Bit9 Security Platform の使用

Bit9 Platform バージョン：7.2.3

ドキュメント日付：２０１７年３月３日

著作権表示

『Bit9 Security Platform の使用』
ドキュメント バージョン：7.2.3.b
ドキュメント改定日付：２０１７年３月３日
製品バージョン：7.2.3

Carbon Black, Inc.
1100 Winter Street, Waltham, MA 02451 USA
電話：617.393.7400
FAX：617.393.7499

会社の Web サイト：http://www.carbonblack.com
サポートの E メール：support@carbonblack.com
支援を受けるためにユーザー アカウントを使用して User eXchange にログインすることもできます。

始める前に

この序文では、『Bit9 Security Platform の使用』について簡単に紹介します。

重要: Bit9, Inc., の名前は Carbon Black, Inc. に変更されました。Bit9 Security Platform の名前は Carbon Black Enterprise Protection に変更されました。ただし、本文書はユーザー インターフェイスでBit9の識別子を維持するリリースを対象としているため、文中でもその識別子が使用されます。名前の変更を除き、継続的なサポートや機能の開発に変更はありません。詳細については、当社の Web サイト (www.carbonblack.com) を参照してください。

セクション

対象ユーザー

本文書の内容は、Bit9 コンソールを扱う管理者を対象としています。Bit9 Security Platformのアクティビティを管理するスタッフは、Microsoft Windowsオペレーティング システム、Web アプリケーション、デスクトップ インフラストラクチャ（特に、ソフトウェア展開、パッチ管理、およびウイルス対策ソフトウェア メンテナンスの社内手順）、意図しないソフトウェアの影響にも精通していることが求められます。また、Bit9 Security Platform と Active Directory を統合する機能を使用する場合、Active Directory の概念とその使用方法も熟知している必要があります。日常業務で Bit9 コンソールを扱うユーザーには不要ですが、社内の Bit9 Security Platform データベース サーバーをメンテナンスする担当者には SQL Server の管理に関する知識が必須です。

また、Bit9 Security Platform の管理者は、Bit9 Security Platform で管理されるクライアントのオペレーティング システムと、そこにインストールされるソフトウェアについても熟知する必要があります。

Bit9 の用語

Bit9 Security Platformとその機能を理解するために必要になる主な用語の定義を次の表に示しています。

用語	定義
Bit9 Server	サポート対象の Windows プラットフォームで Bit9 Server ソフトウェアを実行するコンピューター。
Bit9 エージェント	ネットワーク上のコンピューターにインストールされるエージェント ソフトウェア。エージェントは Bit9 Server とは独立して動作しますが、Bit9 Server によって管理されます。
Bit9 コンソール	コンソールは、Bit9 のすべての管理アクティビティを一括して行える管理用ユーザー インターフェイスであり、Web ブラウザーを使ってリモートから表示できます。
適用レベル	Bit9 エージェントが実行されるコンピューターに適用される保護レベル。High (Block Unapproved) から None (Disabled) までのレベルを使って、必要なファイル ブロック レベルを指定できます。
コンピューター	Bit9 エージェントが実行されているコンピューター。Bit9 で管理されるコンピューターはエージェントによって保護されます。エージェントは Bit9 Server に接続すると、情報を送信すると同時に、保護用の更新データを受け取ります。仮想マシンも、Bit9 Security Platform にコンピューターとして追加することができます。
テンプレート	Bit9 エージェントがあらかじめインストールされたコンピューター。1 つ以上の「クローン」コンピューターを作成するときに使用されます。

用語	定義
ポリシー	Bit9 Security Platform で保護される各コンピューターに、そのコンピューターのセキュリティ特性を定義するポリシーが関連付けられます。セキュリティ要件が同じコンピューターには、同じポリシーを適用できます。
コンピューターの初期化	Bit9 システムに新しく接続したコンピューターに対するファイル初期化プロセス。初期化の際に、新しいコンピューターの固定ドライブ上のファイルが Bit9 Server によって個別に評価され、分類されます。
ログイン アカウント	ユーザーが Bit9 コンソールを使用するにはログイン アカウントが必要です。ユーザーの職務に応じたロール ベースのアカウントによって、そのユーザーがシステムで実行できる操作が決まります。 Bit9 エージェントが実行されるコンピューターのユーザーには、Bit9 コンソール アカウントは不要です。Bit9 の監視対象コンピューターのユーザーがサーバーを直接操作する必要はありません。
実行可能ファイルとスクリプト	実行可能ファイルとは、実行可能コードが含まれたファイルを意味します。Bit9 Security Platform では、ネットワーク内のコンピューターに存在するすべての不明ファイルの内容を検査し、ファイルに実行可能コードが含まれているかどうか確認します。実行可能コードが含まれていた場合は、実行可能ファイルとして分類します。 Bit9 Security Platform には、スクリプトを識別して管理するための特殊なルールが用意されており、スクリプト識別用の新しいルールを定義することもできます。 Bit9 Server には実行可能ファイルとスクリプトを格納するインベントリがあり、その実行を許可するかどうかを管理するルールが設定されています。実行可能ファイルやスクリプトとして認識されなかったファイルは登録されませんが、「ファイル整合性ルール」などのカスタム ルールを使用すると、そのようなファイルへのアクセスを制御できます。
ファイルの状態	実行可能ファイルをどのように追跡するか、および実行を許可するかどうかを決定する、Bit9 Security Platform での分類。最上位のファイルの状態としては、承認、禁止、未承認（承認も禁止もされていない）などがあります。ファイルの状態にはグローバル状態とローカル状態があり、状況によって変化します。
ソフトウェアの承認	正規のソフトウェアとして承認する、Bit9 Security Platform の機能。承認済みソフトウェアは、厳重に保護され「ロックダウン」されているコンピューターでも、ユーザーや管理者の承認を得ずに実行することが許可されます。
レピュテーション	ファイルを承認するか禁止するかを判断する材料となる情報です。Bit9 Server に統合されている Bit9 Software Reputation Service によって、ファイルの大規模データベースやファイル公開者のレピュテーション データが提供されます。

用語	定義
通知	Bit9 ルールによってアクションがブロックされたときに表示される場合がある、ダイアログ ボックスまたは一時的なパネル。通知には、そのアクションがブロックされた理由に関する情報に加えて、ユーザーがそのアクションを許可するオプションや、管理者に承認を求めるオプションが表示される場合があります。通知を設定して名前を付けて保存し、別の Bit9 ルールに追加することができます。
承認要求	ファイルやデバイスへのアクセスがブロックされたユーザーによる要求。承認要求は、Bit9 Security Platform を使用せずに E メールや外部 Web サイトを使って非公式に処理することも、Bit9 の承認要求管理機能を使用して処理することもできます。
ドリフト レポート	1 つ以上のコンピューターが（ファイルの追加、削除、変更によって）ファイルのベースラインからどれだけ「ドリフト」しているかを把握するために役立つレポート。ドリフト レポートは、リスク レベルの把握や、許可されるファイルでの企業ポリシーの適用状況の把握に役立つだけでなく、更新されたベースラインに対して承認して追加する必要があるファイルの特定にも役立ちます。
ライブ インベントリ	Bit9 エージェントが稼動している全コンピューター上のすべての「関心対象」ファイルに関する、ほぼリアルタイムの Bit9 データベース。
ベースラインとスナップショット	コンピューター上に現在存在するファイルと比較し、基準からのドリフトの程度を把握するための参照データ。ベースラインとして使用できるのは、スナップショットと呼ばれる名前付きファイル テーブルか、参照コンピューター上の現在のファイルです。
痕跡セット	「痕跡」と呼ばれるルールのグループ。Bit9 Server の配下にあるシステムにおいて特に脅威となるアクティビティや疑わしいアクティビティの検出に役立ちます。
正常性の痕跡	Bit9 Server と SQL Server の特定のパラメーターが Bit9 の運用要件を満たしているかチェックするためのルール。正常性の痕跡の結果は、[System Health（システム正常性）] ページに表示されます。
イベント	Bit9 のアクティビティに関連するアクションの記録（ファイルのブロック、未承認ファイルの実行、システム管理プロセス、コンソール ユーザーのアクションなど）。Bit9 コンソールで調査したイベントを、Syslog サーバーやデータ解析システムなどの他の解析ツールにエクスポートすることができます。
イベント ルール	指定されたイベントが Bit9 Server で記録されたときに特定のアクションを実行するルール。ファイルの状態の変更、エンドポイントからのファイルのアップロード、サードパーティのデトネーション エンジンへのファイル送信などのアクションを実行できます。

本ドキュメントの対象範囲

『Bit9 Security Platform の使用』では、Bit9 Security Platform を使用したネットワーク上の実行可能ファイルの監視、Bit9 Server の構成、Bit9 エージェントが実行されているコンピューターの管理、Bit9 コンソールのユーザーの管理などのタスクについて解説しています。各章は次のような内容になっています。

	章	説明
1	Bit9 Security Platform の概要	Bit9 Security Platform のアーキテクチャ、管理に関する主要な概念、運用の戦略について説明します。
2	Bit9 コンソールの使用	Bit9 コンソールを使用してシステムにログインする方法と、Bit9 Security Platform の操作方法について説明します。一般的なメニューやボタンの説明も含まれます。
3	コンソール ログイン アカウントの管理	ログイン アカウントを作成、管理、削除する方法について説明します。また、さまざまな種類のユーザー アカウントの権限についてと、Active Directory アカウントを Bit9 コンソールのアカウントとして使用する方法についても説明します。
4	ポリシーの作成と構成	一連のコンピューターの保護方法を定義するポリシーについて説明します。ポリシーの設定と適用レベル、およびその変更方法についても説明します。
5	コンピューターの管理	Bit9 エージェントを設定、導入、およびインストールする方法について説明します。また、Bit9 Security Platform で管理されるコンピューターの情報を取得する方法についても説明します。
6	仮想マシンの管理	テンプレート コンピューターから作成した仮想マシンの管理に関する特別な考慮事項について説明します。
7	ファイル情報と公開者情報	Bit9 Security Platformで認識されるファイルの情報が得られる場所とその方法について説明します。Bit9 Security Platformで得られるファイルのグローバル状態とローカル状態の詳細情報についても説明します。
8	ソフトウェアの承認と禁止	ファイルを承認または禁止するさまざまな方法と、その方法を使用する状況について説明します。
9	レピュテーション承認ルール	Bit9 Software Reputation Serviceの信頼設定を使用して、ファイルと公開者を自動的に承認する方法について説明します。
10	ファイル署名証明書の管理	公開者に関連付けられている特定の証明書を承認または禁止することで、ファイルを承認または禁止する方法について説明します。
11	デバイスの管理	コンピューターに接続されたデバイス上のファイルへのアクセスを制限するルールの設定方法について説明します。

	章	説明
12	カスタム ソフトウェア ルール	指定されたパスにあるファイルに対して実行または書き込みが試みられたときの動作を制御する「カスタム ルール」の作成方法について説明します。また、ルールをサーバーからエクスポートして別のサーバーにインポートする方法についても説明します。
13	スクリプト ルール	Bit9 Security Platform のスクリプト ルールによって制御されるファイルとして、ファイルを追加する方法について説明します。
14	レジストリ ルール	指定されたパスにある Windows レジストリの変更が試みられたときの動作を制御する、レジストリ ルールの作成方法について説明します。
15	メモリ ルール	あるプロセスが別のプロセスへのアクセスまたは変更を試みたときの動作を制御するルールの作成方法について説明します。
16	イベント ルール	指定したイベントが Bit9 Server に報告されたときに指定されたアクションを実行するルールを作成する方法について説明します。
17	ブロック通知と承認要求	エージェント コンピューターでのブロック ファイル通知の動作と、通知をカスタマイズする方法について説明します。ユーザーからの承認要求の設定と管理についても説明します。
18	イベント、アラート、およびメーター	一般的な監視作業を行う方法について説明します。Bit9 Security Platformのレポートとイベントを使用してネットワーク ファイルのアクティビティの変化を識別し、適切に対応する方法についても説明しています。さらに、Bit9 によって監視されるアクティビティの E メール アラートを設定する方法や、特定のファイルの実行回数を計測する方法についても説明します。
19	変更の監視：ベースライン ドリフト レポート	ベースライン ドリフト レポート機能を使用してファイル インベントリの長期的な変化を監視する方法について説明します。
20	高度な脅威検出	Bit9 の高度な脅威の痕跡について説明します。これを使用すると、Bit9 Server の配下にあるシステムにおいて脅威となるアクティビティや疑わしいアクティビティを検出できます。
21	ダッシュボードの使用とカスタマイズ	Bit9 ダッシュボードについて説明します。この特別なユーザー インターフェイスには、Bit9 Security Platform で管理されるコンピューターと、そこに保存されているファイルに関する重要情報が要約して表示されます。

	章	説明
22	ファイルの検索	ファイルの検索機能について説明します。この機能を使用すると、ネットワーク上に存在する、Bit9 エージェントが実行されているコンピューターで、特定の実行可能ファイルを検索できます。
23	システム構成	他のサーバー（Carbon Black Response を含む）との統合、バックアップの手順、製品の更新手順、オプションの Bit9 Software Reputation Service ハッシュ識別サービス、エージェントとサーバー間の通信セキュリティ、その他の構成オプションなど、さまざまな設定について説明します。
23	システム正常性の監視	[System Health（システム正常性）] ページについて説明します。このページには、ハードウェア要件とソフトウェア要件への準拠状況、SQL Server の構成、その他の正常性データとパフォーマンス データなど、Bit9 Security Platform 環境の正常性に影響する要素に関する情報が表示されます。
A	ライブ インベントリ SDK：データベース ビュー	Bit9 で管理されるコンピューターに保存されているファイルの「ライブ インベントリ」データベースに対して使用できる、読み取り専用のビューについて説明します。
B	Bit9 API	Bit9 API と呼ばれる RESTful API について説明します。この API を使用すると、カスタム スクリプトを使用したり、ネットワーク セキュリティ プラットフォームなどの他のアプリケーションを使用したりして Bit9 Platform とやりとりするコードを作成できます。
C	Bit9 Connector for Network Security Devices	サードパーティのネットワーク セキュリティ デバイスやセキュリティ サービス（Check Point、Palo Alto Networks、FireEye、SCEP など）を Bit9 Security Platform と統合するための、オプションのコネクター（別ライセンス）について説明します。
D	診断ファイル	エージェント診断ファイルのアップロード方法とアクセス方法について説明します。さらに、コンソールを使って入手できるサーバー診断ファイルについても説明します。
E	エージェントからのファイルのアップロード	エージェントからサーバーにファイルをアップロードするためのオプション機能（別ライセンス）について説明します。
F	外部分析のための Bit9 データのエクスポート	Bit9 Server によって収集されたエンドポイント データを Splunk などの外部の解析ツールに送信するオプション機能（別ライセンス）について説明します。

その他の Bit9 ドキュメント

『Bit9 Security Platform の使用』に記載されていないタスクを行うには、次の Bit9 ドキュメントの一部またはすべてが必要になります。次のドキュメントは、Bit9 Server のインストーラーと同時にダウンロードされる場合があります。Bit9 カスタマー ポータルからもダウンロードできます。

一部のドキュメントは新規リリース版のビルドごとに更新されますが、その他のドキュメントはマイナー バージョンまたはメジャー バージョンの変更時にのみ更新されます。

- 『**運用環境の要件**』– Bit9 Server、Bit9データが保存されるSQL Serverデータベース、および Bit9 エージェントのハードウェアとソフトウェア プラットフォームの要件について説明します。
- 『**Supported Agent Operating Systems**（サポートされているエージェントのオペレーティング システム）』– Bit9 エージェントの現在のバージョンでサポートされているオペレーティング システムについて説明します。
- 『**Installing Bit9 Server**（Bit9 Server のインストール）』– Bit9 Server の新規インストールの方法と、以前のリリースの Bit9 Server をアップグレードする方法について説明します。Bit9「エージェント」のインストール方法については本ドキュメント（『Bit9 Security Platform の使用』）を参照してください。
- 『**Bit9 Security Platform Release Notes**（Bit9 Security Platform リリース ノート）』– インストールした Bit9 Server のバージョンとビルドに固有のドキュメントです。そのリリースにおける新機能、修正内容、既知の問題に関する情報が記載されています。
- 『**Bit9 Events Integration Guide**（Bit9 イベント統合ガイド）』– Bit9 Server に記録されるイベントのインベントリ詳細と、Syslog を介したサードパーティの SIEM システムと Bit9 イベント データを統合する手順について説明します。

高度な脅威環境を初めて扱う方は、『Next Generation Endpoint Security For Dummies (Carbon Black Edition)（ダミーに対する次世代エンドポイント セキュリティ（Carbon Black 版））』（Mike Chapple 著）を参照すると、概要を把握できます。このドキュメントは次の URL から PDF として無料でダウンロードできます。

https://www.carbonblack.com/files/ebook-next-generation-endpoint-security-for-dummies/

コミュニティ リソース

Carbon Black User eXchange の Web サイト (https://community.carbonblack.com) では、Carbon Black のユーザー、社員、およびパートナーが共有する情報にアクセスできます。これには、Bit9 Security Platform (Carbon Black Enterprise Protection)やCarbon Black Enterprise Response を含む全 Carbon Black 製品に関する情報とユーザーのコミュニティへの参加が含まれます。

このリソースにログインすると、次のことができます。

- 他のユーザーに質問したり、他のユーザーの質問に回答したりする
- 「投票」によって製品アイデアのステータスを格上げする
- 最新のユーザー ドキュメントをダウンロードする

- 開発者コミュニティに参加し、アイデアや解決策を投稿したり、他の参加者の投稿について話し合ったりする
- Carbon Black 製品で利用可能なトレーニング リソースを見る

User eXchange にアクセスするにはログイン アカウントが必要です。アカウントが必要な場合は、テクニカル サポートの担当者にお問い合わせください。

サポートへのお問い合わせ

テクニカル サポートでは、複数の方法でお客様からの Bit9 Platform に関するお問い合わせを受け付けています。

テクニカル サポートへの問い合わせ方法
Carbon Black User eXchange：https://community.carbonblack.com
E メール：support@carbonblack.com
電話：877.248.9098
FAX：617.393.7499

問題の報告

テクニカル サポートに電話またはメールで連絡する際は、サポート担当者に以下の情報を提供してください。

必要な情報	説明
連絡先	名前、会社名、電話番号、メール アドレス
製品バージョン	製品名およびバージョン番号
ハードウェア構成	製品を実行するサーバーまたはコンピューターのハードウェア構成（プロセッサー、メモリ、および RAM）
ドキュメント バージョン	ドキュメントの問題の場合、使用しているドキュメントのバージョンを指定してください。ドキュメントの日付とバージョンは表紙に記載されています。大きなドキュメントの場合は、「著作権表示」セクションの後に記載されています。
問題	問題の原因となったアクション、返されたエラー メッセージ、その他の該当する出力
問題の深刻度	重大、深刻、マイナー、または改善

目次

第 1 章

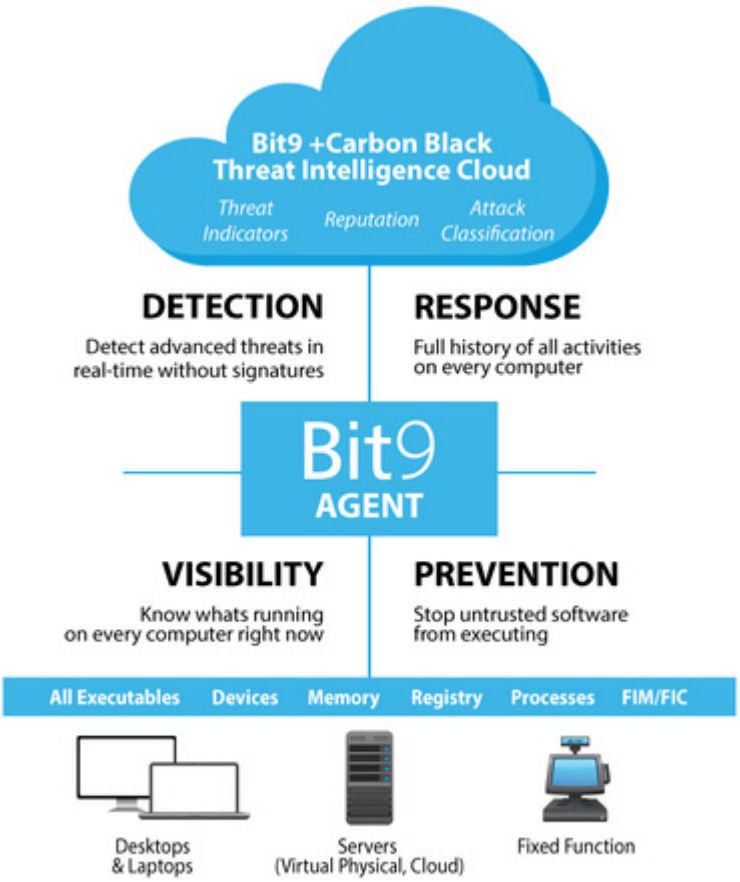
Bit9 Security Platform の概要

この章では、Bit9 Security Platform とその主要概念を示し、許可されない、または悪意のあるファイルの実行がエンドポイントで行われるのを避けるための運用戦略を提案します。

セクション

Bit9 Security Platform とは

Bit9 Security Platform は、包括的なエンドポイント脅威保護ソリューションであり、広く導入されているホワイトリスト化製品です。信頼ベースとポリシー ベースの手法によるアプリケーション制御と、リアルタイムの脅威インテリジェンスとを組み合わせることで、Bit9 はエンドポイントとサーバーのアクティビティを継続的に監視、記録して、従来のセキュリティ防御をかいくぐるサイバー脅威を検出し、対応します。オープン API と幅広いパートナー エコシステムを備えた Bit9 は非常に柔軟性が高く、社内とサードパーティのどちらのツールともシームレスに統合できます。



即時の可視化 – Bit9 エージェントをインストールするだけで、管理者は環境全体のすべての実行可能型ファイルに関してリアルタイムの可視性が得られます。Bit9 エージェントでは、Bit9 脅威インテリジェンス クラウドとの連携によって信頼度および実用的なインテリジェンスが得られるため、悪意のある可能性の高いファイルを容易に発見して、自動的にアクションをとることができます。

柔軟性のある保護防御 – Bit9 Security Platform では、管理者は攻撃を発生前に防ぐことができます。Bit9 のプロアクティブな「デフォルト拒否」、「検出して拒否」、または「デトネート拒否」防御機能を活用することで、Bit9 Security Platform では管理者が必要とする防御とアクセスの適切なバランスを確保する柔軟性を実現しつつ、組織の攻撃対象領域を大幅に減らすことができます。

高度な検出 – Bit9 Security Platform は、強力で自動化された、クラウドで提供される高度な脅威検出技術を備えており、攻撃をすばやく発見して阻止できます。Bit9 + Carbon Black 脅威インテリジェンス クラウドから高度な脅威の痕跡を利用することで、組織の環境内にあるすべてのエンドポイント デバイスについてエンドポイントを継続的に監視、調査して、侵入の潜在的なパターンを発見し、悪意のあるアクティビティを検出します。

リアルタイムのエンドポイント データを使用することにより、Bit9 の高度な脅威の痕跡は単なる「侵入の痕跡」を超えるものになっています。エンドポイント アクティビティ、クラウドから得られる脅威インテリジェンス、ヒューリスティックを組み合わせることで、イベントベースの侵入の痕跡ではなく、パターンに基づいて脅威を識別します。検出を組み合わせるというこの方法により、Bit9 では偽陽性アラートの数を減らすことができ、また、発生してからでなければ侵入を検出できないポールベースの検出方法とは異なり、初期段階と進行中の両方で脅威を検出できるようになっています。

迅速な対応 – 攻撃が検出されると、Bit9 からはセキュリティ インシデントへの迅速な対応、ログ、調査のためのさまざまなツールが提供されます。Bit9 独自の「Detect-and-Deny」保護機能により、管理者はアクティブなプロセスを終了し、その後は攻撃が一切実行されないよう直ちに禁止することで、悪意のあるアクティビティに迅速に対応することができます。さらに、Bit9 ではすべてのエンドポイント アクティビティの履歴が記録されるため、どこでマルウェアが実行されたか、どこが起点か、どのように広がったか、最終的に影響を受けたシステム、実施されたアクション、取得されたデータなどの全面的な影響評価が直ちに管理者に提供されます。

Open API アーキテクチャー – Bit9 はオープン アーキテクチャーを備えているため、セキュリティ スタック全体と統合して、セキュリティ プロセスを自動化、簡素化することができます。Bit9 の RESTful API と広範なパートナー統合エコシステムにより、Bit9 Security Platform はオープンであることと拡張性の点で突出しており、それによってセキュリティ ソリューションを統合して、サードパーティのセキュリティ製品（SIEM、ネットワーク、エンドポイント、運用）や独自の社内ツールによって自動化やレポートを促進したり、セキュリティ応答時間を短縮したりすることができます。

Bit9 Security Platform を使用すると、以下のことが可能です。

- 既知のウイルス、トロイの木馬、アプリケーション侵害、カスタムおよびターゲット型の攻撃をブロックすることによる、悪意のあるソフトウェアの阻止
- 承認済みソフトウェアの実行のみを許可することによる、ゼロデイ脅威の阻止
- Windows レジストリへのアクセスを監視、制御するカスタム ルールの作成
- Windowsコンピューターの特定のプロセスへのアクセスを監視、制御するメモリ ルールの作成
- 重要な非実行システム構成ファイルへのアクセスを禁止またはレポートする、ファイル整合性の監視と制御ルールの作成
- 監査、アクティビティ監視、違反通知、ポリシー適用の簡素化によるコンプライアンスの負担の軽減
- Bit9 Software Reputation Service (SRS) により、環境内で見つかったソフトウェアに関連するリスクをレピュテーション サービスを利用して識別、分類して、

Bit9 + Carbon Black 脅威インテリジェンス クラウドで信頼できると考えられるファイルおよび公開者を自動的に承認

- Windows コンピューターで、付属ストレージ デバイスへの機密データの転送を監査、制御することにより、データの盗難および流出を阻止
- Windows コンピューターで、モデルまたはシリアル番号によってストレージ デバイス上のファイルの実行を承認または禁止するルールを作成
- リスクの最小化、必要な修復、コンプライアンスの維持、サポート コストの削減のために、ファイルのベースラインからの逸脱を監視
- 高度な脅威の痕跡、Bit9 イベント、ファイルの詳細、アラートを使用した脅威の監視
- 受信したイベントに基づく、ファイルおよびコンピューター関連アクションの自動化
- Bit9 OpenAPI を使用してサードパーティ ネットワーク、エンドポイント、SIEM、分析セキュリティ製品およびサービスと Bit9 Server を統合することによる通知と分析
- Bit9 データをエクスポートして Splunk などの外部の分析製品で使用

コンピューター上のファイルに関する情報の提供、許可されていないソフトウェアおよびハードウェアの制御、サイトのコンピューターの柔軟な管理を可能にする Bit9 の補足的な機能を表 1 に示します。

表 1：Bit9 Security Platform の機能

機能	説明
ライブ ファイル インベントリおよびベースライン ドリフト追跡	Bit9 Security Platform では、必要に応じてすべてのコンピューター上のすべてのファイルを常時追跡することができます。ほぼリアルタイムのこのインベントリにより、Bit9 Security Platform はこれらのファイルについて幅広い種類の情報、および組織全体にわたって変更の頻度と種類を提供できます。この情報を利用した結果の 1 つが、1 台または複数のコンピューター上にあるファイル インベントリ内の変更をレポートするベースライン ドリフト レポートです。もう 1 つは、管理対象コンピューターから、指定した実行可能ファイルのすべてのインスタンスを見つける機能です。
Bit9 Software Reputation Service (SRS) ファイル識別およびレピュテーション サービス	Bit9 Software Reputation Service (SRS) では、ファイルの識別および分類が行われます。ファイルのソース、Bit9 エージェントが実行されているコンピューターでのファイルの普及度、ウイルス対策製品によるスキャンの結果、正規のデジタル署名の有無など、さまざまなソースに基づいてファイルに**信頼要因**が割り当てられます。一定の信頼しきい値を満たしたファイルや公開者を自動的に承認することができます。

機能	説明
イベント追跡	Bit9 Security Platform では、ファイル関連イベント、および Bit9 Server または管理対象コンピューターに関係するその他のアクティビティについて、最新状態のデータベースが保持されます。このデータに基づいて、事前定義された、またはカスタムのレポートを表示して、環境の変更や大きな Bit9 Server 操作を把握することができます。特定のイベントに基づいてアラートをトリガーすることもできます。Bit9 イベントは、Syslog にエクスポートして SIEM システムと統合したり、データ分析システム向けや CSV ファイルとしてエクスポートしたりすることができます。
モード	アクティブな Bit9 エージェントは、次の 2 つのモードのいずれかで操作することができます。**可視性モード**では、Bit9 Security Platform のファイルおよびイベント追跡機能は提供されますが、ファイルやデバイスの禁止などのセキュリティ制限は行われません。**制御モード**では、禁止ファイルはブロックされ、未承認ファイル（承認も禁止もされていないファイル）は、その取り扱いを決定するために 3 つの適用レベルから 1 つを選ぶことができます。また、制御ポリシーを設定して、他のファイルおよびデバイスにセキュリティ ルールを適用できます。
適用レベルとポリシー	適用レベルとポリシーを組み合わせて使用することにより、特定のコンピューター上のファイルおよびデバイスのアクティビティを制御します。選択した適用レベルによっては、禁止ファイルおよび未承認（承認も禁止もされていない）ファイルの実行がブロックされることがあります。適用レベルは、強い制限から適用なしまでの幅があります。 ポリシーは、適用レベルのほか、Windows コンピューターで一部のリムーバブル デバイスの動作をブロックまたは制御する機能などの設定を含むルール セットです。Bit9 Security Platform によって管理されるすべてのコンピューターには、ポリシーが 1 つ割り当てられます。
柔軟な緊急ロックダウン	コンピューターを複数のグループに分けて、それぞれ異なるセキュリティ レベルで実行することができます。たとえば、一部のコンピューターは高適用レベルで実行して、Bit9 エージェントがインストールされたときに存在していなかった未承認ファイルが実行されることを禁止し、他のコンピューターにはそれよりも多くの特権を許可することができます。 必要であれば、攻撃や高い脅威が発生している間は緊急ロックダウンを行って、すべてのコンピューターを高適用レベルに移行することができます。脅威が抑制されたと判断したら、システムを元のセキュリティ レベルに戻します。
ファイル整合性の監視と制御	Bit9 Security Platform では、指定したファイルまたはパスに適用するカスタム ソフトウェア ルールを作成することができます。これには、ファイル整合性ルールも含まれます。これにより、特定のフォルダー、または指定条件に一致する複数のフォルダーに対する変更を監視し、必要に応じて変更を制限できます。

機能	説明
ソフトウェア ルール：禁止	禁止は、サイトにある一部またはすべてのコンピューターで禁止されるファイルを（名前またはハッシュによって）指定することができます。ファイルを個別に禁止することも、作成したハッシュのリストで識別されるすべてのファイルを禁止することもできます。また、指定した公開者からのすべてのファイルを禁止することもできます。
ソフトウェア ルール：承認	いくつかの補足的なソフトウェア承認方法により、正当なソフトウェアがすべてのコンピューターまたはコンピューターのグループで実行されることを（ポリシーによって）承認、または単一のコンピューターで実行されることを「ローカルに」承認できます。承認ルールを Bit9 Software Reputation Service (SRS) と統合して、サービスによる分析に基づいて特定の信頼レベルを満たすファイルを自動的に承認することができます。
レジストリ ルール	Windows コンピューターで、レジストリ キーと値の特定の組み合わせパターンが変更されないように保護するルールを指定できます。
メモリ ルール	Windows コンピューターで、プロセスが他のすべての（または特定の）プロセスやユーザーによってアクセスまたは変更されないように保護するルールを指定できます。
デバイス ルール： 承認と禁止	Windows コンピューターで、検出されたストレージ デバイス上のファイルの実行および書き込みを承認または禁止することができます。デバイスのモデルまたは具体的な個々のデバイスを承認、禁止することも、一部またはすべてのコンピューターにルールを適用することもできます。
通知、および ユーザーが開始した承認要求	Bit9 ルールによってファイル アクセスがブロックされたときに、ブロックについて説明する通知をユーザーに表示することができます。この通知では、オプションでファイル承認の要求方法を伝えることができ、要求は Bit9 コンソールで直接追跡し、対応することが可能です。
検出：高度な脅威の痕跡	高度な脅威の痕跡を有効にすると、疑わしい状況が発生したときにイベントをトリガーできます。また、問題がないと考えられるイベントについては例外を作成して痕跡を微調整できます。
イベントトリガー型のアクション	イベント ルールを作成すると、ファイルまたはコンピューターに関連するイベントが発生したとき、それが定義したフィルターに一致する場合に実行されるアクションを指定することができます。また、指定されたイベント ルールがトリガーされたときにレポートするアラートを作成することもできます。
ネットワーク セキュリティ デバイスとの統合	Bit9 Server は、Check Point、Palo Alto Networks、FireEye、Microsoft EMET などのサードパーティが提供する 1 つ以上のネットワーク セキュリティ デバイスまたはサービスと統合することができます。
Bit9 API 経由のアクセス	Bit9 Platform で RESTful API を使用することにより、カスタム スクリプトで、または他のアプリケーションから Bit9 Platform とやりとりするコードを作成することができます。API コードは、get URI 要求、post/put JSON 要求、および interpret JSON 応答を作成できる任意の言語を使用して、HTTPS プロトコルを通じて処理できます。

機能	説明
外部データ分析との統合	Bit9 イベント、ファイル操作データ、ファイル カタログ データをエクスポートして、Splunk などの外部の分析製品で使用することができます。
システム正常性の監視	システム正常性の痕跡をオプトインすると、運用環境の要件への準拠など、Bit9 Server の運用に影響する要因が監視され、レポートされます。

Bit9 Security Platform の動作

Bit9 Security Platform は、実行可能ファイルを追跡し、その普及度と実行を監視します。Bit9 エージェントをコンピューターにインストールすると、Bit9 によるファイルのインベントリである初期化が直ちに始まります。初期インベントリ中にコンピューターで見つかったすべてのファイルは、事前に Bit9 Server で禁止されていなければ、そのコンピューターで「ローカルに」承認されます。ローカルに承認されても、ファイルのグローバルな状態は変更されません。

初期化の後で、Bit9 によって管理されているコンピューター上に新しい、存在を認識されていないファイルが見つかると、グローバルとそれが見つかったコンピューターのローカルの両方で、「未承認」という状態であると分類されます。ファイルの「未承認」状態は、「承認」または「禁止」になるまで維持されます。ファイルは承認されると実行可能になりますが、引き続き追跡されます。

Bit9 Security Platform は、いくつかの承認方法（信頼できるディレクトリ、承認済みの公開者、信頼できるユーザー、Windows コンピューターにおける事前設定されたアップデーター、レビュテーション承認、ハッシュ リストによるファイルの一括承認）を備えており、これによって新しいソフトウェアを簡単に承認でき、個々のファイルごとに承認する必要がありません。また、手動で個別のファイルを承認または禁止とマークすることもできます。

Bit9 の他の機能によって監視されるコンピューター上のアクティビティも、ファイルを承認するか禁止するかを判断するのに役立つ可能性があります。Bit9 Server からは、以下の情報が提供されます。

- あるファイルがコンピューター上に存在するかどうか
- そのファイルがどのコンピューターに存在するか
- そのファイルは環境内のどこに、いつ、初めて出現したか
- ファイルのソース、カテゴリ、信頼度、脅威
- ファイルが実行されたかどうか、いつ実行されたか、およびどのコンピューターで実行されたか
- ファイルが伝播したかどうか、伝播した場合は名前が変更されたかどうか
- Windows コンピューターで、接続されているストレージ デバイス（USB、SCSI など）がネットワーク上に存在するかどうか、最初に認識されたのはいつか、どのコンピューターに接続されているか
- コンピューター上のファイルのインベントリが時間の経過によってどのように変化したか

Bit9 Security Platform によるファイルの追跡

Bit9 コンソールと本文書では、「ファイル」という用語が使われます。「ファイル」が何を意味するかは、Bit9 の機能によって次のように異なります。

- Bit9 のライブ インベントリでは、「ファイル」は実行可能ファイルまたはスクリプト ファイルのことです。Bit9 エージェントをコンピューターにインストールすると、システム上のすべてのファイルが分析され、実行可能ファイルやスクリプトは特定されて、それらのファイルのインベントリが維持されます。非実行可能ファイルは、いったん識別された後は無視されます。
  Bit9 Security Platform は、ファイルの拡張子ではなく内容に基づいて、ファイルが実行可能であることを判断します。Bit9 Security Platform がファイルをスクリプトであると判断するのは、いくつかの要因の組み合わせに基づいており、ユーザーはこのスクリプト定義に追加、変更を加えることができます。承認または禁止できるのは、実行可能ファイルとスクリプト ファイルだけです。特定の構成設定により、これらのファイルを特殊ケースとして追跡とインベントリから除外することができます。
- ファイル整合性の監視では、ファイル整合性の制御ルールによってファイルを登録すると、実行可能でないデータおよび構成ファイルへのアクセスを追跡できます。ファイルまたはパスをそのようなルールの対象にすると、そのファイルにアクセスしようとしたときに Bit9 Security Platform で監査可能なイベントが生成され、必要に応じてそのアクセスをブロックすることができます。

システム アーキテクチャ

Bit9 Security Platform のアーキテクチャは、以下のコンポーネントで構成されています。

- Bit9 Server ソフトウェア – すべてのエージェント システムで、ファイルのセキュリティ管理、イベント監視、注目するファイルのライブ インベントリの中心的な存在です。
- Bit9 エージェント ソフトウェア – サーバー、デスクトップ、ラップトップ、仮想マシン、および固定機能デバイスで実行されます。ファイルを監視し、セキュリティ ポリシー設定に基づいてその実行をブロックまたは許可します。また、新しい実行可能ファイルおよびスクリプト フィルを Bit9 Server にレポートし、設定された他のルールを適用します。
- Bit9 Software Reputation Service (SRS) – Bit9 エージェントが実行されているコンピューターに導入された新しいファイルを既知のファイルのデータベースと比較して、脅威レベル、信頼要因、ソフトウェア分類に関する情報を提供します。必要に応じて、信頼情報を使用して自動的にファイルを承認することもできます。
- Bit9 は、サードパーティ製品と統合することもできます。これには、Splunk などの外部の分析製品や、Check Point、FireEye、Palo Alto Networks などが提供するネットワーク セキュリティ製品が含まれます。

Bit9 Server

Bit9 Server ソフトウェアは、標準的な Windows コンピューターで実行されます。専用のシステムで実行することも、仮想マシンとして実行することもできます。Bit9 Server は、ソフトウェアおよびデバイスの承認と禁止などに関するポリシーとルールを管理し、Bit9 エージェントが実行されているコンピューターでのイベントおよびファイルのアクティビティに対する可視性を提供します。Bit9 Console は Web ベースの使いやすいユーザー インターフェイスであり、接続されているすべてのコンピューターから Bit9 Server へのアクセスを実現します。

Bit9 Server データベースは、Bit9 Server と同じマシン、または別のハードウェア上の SQL Server を使用します。Bit9 Security Platform の中心的なデータは、Live Inventory SDK の一部として公開されている一連のデータベース ビューを通じて、Bit9 Security Platform 外からアクセスできます。Bit9 Security Platform イベントは、Syslog サーバーまたはデータ分析システムに出力して、さらに分析することもできます。

Bit9 Security Platform と Active Directory の統合

ユーザー、コンピューター、グループは、既に Microsoft Active Directory を使用して定義し、命名してあることも考えられます。Bit9 Server は Active Directory 環境を利用して、Bit9 コンソールのユーザーへのアクセス権限の設定、コンピューターへのセキュリティ ポリシーの割り当て、ユーザーおよびコンピューターのメタデータの提供のほか、Bit9 Security Platform で管理されるコンピューターに特定のグループまたはユーザーがソフトウェアをインストールできる（さらに、ソフトウェアが自動的に承認される）ように指定することが可能です。

Bit9 エージェント

Bit9 エージェント ソフトウェアは、クライアント コンピューターで実行されます。ファイルとプロセス アクティビティを監視し、必要に応じて Bit9 Server と通信します。Windows コンピューターでは、接続されているストレージ デバイスとレジストリ アクティビティも監視します。サーバーから切断されても、エージェントは引き続き、最後に受信した禁止ポリシーとセキュリティ ポリシーの指定を適用します。Bit9 エージェントが実行されているコンピューターが切断状態から再度接続されると、エージェントはポリシーとルールの更新をサーバーから受信し、ネットワークに接続されていない間に発生した、関係するファイル アクティビティを伝えます。

Bit9 エージェントはバックグラウンドでサイレントに実行されていますが、ファイルがブロックされるときには、そのファイルの実行が許可されない理由をコンピューターのユーザーに説明するメッセージを表示することができます。ファイルの状態、エージェントのセキュリティ レベル、および構成に関するその他の選択項目に応じて、クライアント コンピューターのユーザーはブロックされたファイルでも Bit9 Security Platform によって実行を許可される可能性があります。また、ブロックされたファイルの承認をユーザーが要求するメカニズムを有効にすることもできます。これには、E メールによる非公式な方法と、Bit9 Security Platform に組み込まれ、追跡される公式の要求プロセスがあります。

Bit9 Software Reputation Service に基づく信頼度

Bit9 Software Reputation Service (SRS) は Bit9 によってホストされる Web サービスで、コンピューター上に見つかったソフトウェアを既知のファイルに関する大規模なデータベースと比較して、識別、分類するために使用されます。さらに Bit9 SRS は、重み付け分析に基づいて各ファイルに脅威レベル（悪意がある、悪意がある可能性がある、未知、クリーン）と信頼度（0 ～ 10、および未知）を割り当てます。Bit9 Server はライブ ファイル インベントリにこの情報を保存できるため、システム上のファイルについて、脅威ステータスなどの重要な情報がすぐにわかります。Bit9 SRS を有効にしておけば、Bit9 Server インベントリにあるどのファイルも「分析」でき、利用可能なすべての情報を取得できます。

ファイルの信頼度は、1 回のウイルス対策製品によるスキャンで得られる情報を上回るものです。ファイルの存在がどれだけの期間、何台のコンピューターで確認されてきたか、信頼できるデジタル署名があるか、複数のウイルス対策プログラムによるスキャンの結果など、一連の要因に基づいています。

たとえば、ウイルス対策プログラムによるスキャンからクリーンであるとされ、既知の公開者からの信頼できるデジタル署名があり、多くのコンピューター上に長期間存在してきたファイルは、Bit9 の信頼度 10 という高い信頼度が与えられる可能性があります。同じようにウイルス対策プログラムによるスキャンからクリーンであるとされたファイルでも、出現してからの期間が短く、わずかな台数のコンピューターにしか存在せず、デジタル署名がなければ、信頼度 2 という低い信頼度になる可能性があります。

Bit9 SRS による信頼度を使用すると、独自の信頼度または発行者の信頼度に基づいて、自動的にファイルを承認することができます。管理者はレピュテーション承認を使用することで、ファイルまたは公開者の信頼度に応じて選択したセキュリティ対策を適用して、信頼度の高いソフトウェアを管理オーバーヘッドなしで承認することができます。

ファイルの状態、ホワイトリスト、ブラックリスト

Bit9 Security Platform のいくつかの主要機能は、組み合わされることで機能し、ネットワーク上のコンピューターを保護します。このセキュリティ機能の中核にあるのは、ファイルをその状態に基づいて分類する機能です。ポリシーはセキュリティ ルールをグループ化したものであり、それぞれの状態のファイルがコンピューターのさまざまなグループによってどのように扱われるかを制御します。ここでは、ファイルの主な状態、すなわち承認（ホワイトリスト化）、禁止（ブラックリスト化）、未承認と、それらがどのように変化するかを説明します。

グローバル状態

Bit9 Server には、Bit9 エージェントが実行されているコンピューター上で追跡されるすべての実行可能ファイルに関して、一意の（ハッシュによって特定される）ファイルの一元的なデータベースが保持されます。これらのファイルの「グローバル状態」は、ファイル カタログで確認できます。グローバル状態は、エージェントによって管理されているコンピューターで、それぞれの適用レベルの下でファイルに何が許可されるかを決定します。

グローバル状態は、以下の組み合わせです。

- ファイルの状態 – ファイル自体の承認または禁止状態
- 公開者の状態 – ファイルの公開者の状態（わかっている場合）

ファイルのグローバル状態は、次のいずれかです。

- 承認 – すべてのコンピューター
- ポリシーにより承認 – 一部のコンピューターで承認され、他のコンピューターでは未承認
- 禁止 – すべてのコンピューター
- ポリシーにより禁止 – 一部のコンピューターで禁止され、他のコンピューターでは未承認
- 未承認 – すべてのコンピューター
- 混在 – 一部のコンピューターで禁止され、他のコンピューターでは承認済み

グローバル状態を直接変更することはできません。ファイルの状態または公開者の状態を変更することによって変更します。Bit9 Security Platform には、ファイルの状態を変更するさまざまな方法が用意されています。詳細については、第 8 章「ソフトウェアの承認と禁止」を参照してください。第 7 章「ファイル情報と公開者情報」では、Bit9 Security Platform によって追跡されるファイルについて、さらに詳細を説明しています。

ローカル状態

Bit9 Server にはファイルのグローバル状態が保持される一方で、Bit9 エージェントが実行されているコンピューターに存在するファイルの各インスタンスには、独自の「ローカル状態」があります。これは、ファイルが存在するコンピューターで、その適用レベルに応じてファイルに何が許可されるかを示します。

グローバル状態が未承認のファイルの場合は、ローカル状態が異なることがあります。特に、グローバルに禁止されていないファイルは、さまざまな方法によってローカルで承認することができます。Bit9 Security Platform では、ファイルのローカル状態の情報が、追跡されているすべてのファイル インスタンスの［Files on Computers（コンピューター上のファイル）］インベントリに保持されます。

ファイルのローカル状態は、次のいずれかです。

- 承認
- 禁止
- 未承認
- 削除（ファイルは最近削除され、次の更新時にデータベースから削除されます）

各ファイル インスタンスには、主な状態のほかにローカル ファイル詳細（第 7 章「ファイル情報と公開者情報」を参照）があります。これは、Bit9 Security Platform で行われた承認などの判断の根拠を示していることがあります。これらの詳細は、主に Bit9 サポートが利用します。

ファイルの承認方法

ソフトウェアを承認すると、Bit9 エージェントが実行されているコンピューターのユーザーは、有効な Bit9 Security Platform 設定と適用レベルに関係なく、問題がないことがわかっているアプリケーションを自由にインストールおよび実行できます。ファイルを承認することは「ホワイトリスト化」とも呼ばれ、懸念する必要がないファイルの追跡にかかる時間の節約にもなります。Bit9 Security Platform には、コンピューター上のソフトウェアを承認する補足的な方法がいくつか用意されています。

- すべてのコンピューターで実行するアプリケーションを事前承認する必要がある場合は、信頼できるディレクトリ、公開者、またはアップデーターを指定することで、自動的に承認を生成できます。
- 高度な脅威から保護し、個別に承認する必要があるファイルの数を減らすには、Bit9 Software Reputation Service (SRS) のファイルまたは公開者の信頼に基づく自動レピュテーション承認を有効にします。
- すべてのコンピューターを対象にする場合もポリシーごとの場合も、個別のファイルはハッシュごとに承認できます。また、承認するファイル ハッシュのリストをインポートすることで、複数の個別のファイルに対する承認を作成することもできます。
- 特定のコンピューターでソフトウェアのインストールを承認する必要がある場合は、インストールを実行する信頼できるユーザー（またはグループ）を指定するか、Bit9 Security Platform のローカル承認方法の 1 つを選択します。

詳細については、「Bit9 ソフトウェアの承認とは」（272 ページ）を参照してください。

ファイルの禁止方法

Bit9 Security Platform の制御モードでは、すべてのコンピューター、または特定のポリシーによって指定されるコンピューターで、特定のファイルの実行を禁止することができます。ファイルの禁止は、「ブラックリスト化」とも呼ばれます。ファイルを禁止するには、次の方法があります。

- ファイル名による禁止 – プラットフォーム（Windows、Mac、Linux）に固有です。指定したプラットフォームごとに、指定したファイルの実行を Bit9 エージェントが実行されているすべてのシステムで禁止するか、指定したポリシーを満たすすべてのシステムで禁止します。
- ハッシュによる禁止 – ファイル名に関係なく、一意のハッシュに一致するファイルを禁止します。すべてのプラットフォームが対象で、Bit9 エージェントが実行されているすべてのシステム、または指定したポリシーを満たすシステムに適用されます。ハッシュのリストをインポートすることで、1 回の操作で複数のファイルを禁止できます。
- 発行者による禁止 – 指定した発行者からのものと識別されたファイルの実行を禁止します。すべての Windows システムが対象で、Bit9 エージェントが実行されているすべてのシステム、または指定したポリシーを満たすシステムに適用されます。

詳細については、第 8 章「ソフトウェアの承認と禁止」の「Bit9 ソフトウェアの禁止とは」を参照してください。

カスタム ルール

ここまでに説明した各種の禁止ルールと承認ルールに加えて、Bit9 Security Platform には、コンピューターの保護、必要なソフトウェアの実行の許可、パフォーマンスの最適化のために他の手段も用意されています。

カスタム ルールを使用すると、特定のアクティビティを許可またはブロックする 1 つまたは複数のパスを、ディレクトリまたはファイルのレベルで指定できます。これは、ファイルの状態が変更される場合もありますが、それ以外の場合はグローバルなルールは変更されず、個別の状況に応じて特定の動作を許可、ブロック、または無効にするだけです。カスタム ルールは、ファイル整合性の制御に使用したり、インストール ディレクトリへの信頼済みパスを作成して安全であることがわかっている、または関心のないディレクトリ内のファイルを追跡する手間を節約したりできるほか、それ以外にもさまざまな目的で設定できます。

詳細については、第 12 章「カスタム ソフトウェア ルール」を参照してください。

セキュリティ ポリシーとセキュリティ レベル

Bit9 Security Platform ポリシーは、Bit9 エージェントが実行されているコンピューターのターゲット グループによって共有される保護ルールの名前付きグループです。Bit9 エージェントを実行しているすべてのコンピューターは、1 つのポリシーに属す必要があります。ポリシーは、個々のセキュリティ要件と組織上の要件に基づいて作成できます。たとえば、機能別のグループ（マーケティング、顧客サービス、IT など）、場所、またはコンピューターの種類（ラップトップ、デスクトップ、サーバーなど）に基づいてポリシーの所属を決定します。

各ポリシーには固有の Bit9 エージェント インストーラーがあります。これは、ポリシーを作成すると自動的にサーバー上に生成されます。インストーラーはエージェントをインストールし、そのエージェントに自動的にポリシーを割り当てます。ただし、Bit9 エージェントが実行されているコンピューターがサーバーに接続するたびに、エージェントを実行しているユーザーやコンピューターの Active Directory データに基づいて Bit9 Server がポリシーを割り当てるようにすることもできます。

ポリシーの詳細については、第 5 章「ポリシーの作成と構成」を参照してください。

ポリシー設定

ポリシー設定は、Bit9 Security Platform がコンピューターの特定のグループをどのように管理するかを定義します。設定には次の 3 つのカテゴリがあります。

- 基本ポリシー定義 – ポリシー名のほか、説明的な情報として、このポリシーが対象にするコンピューターでエージェントのアップグレードが許可されるか、それらのコンピューターでライブ インベントリが有効か、およびポリシーの基本セキュリティ レベル（モードと適用レベル）が含まれます。モードと適用レベルの詳細については、この後で説明します。
- デバイス設定 – デバイス設定は、Bit9 Security Platform ポリシーが Windows コンピューター上のリムーバブル デバイスをどのように扱うかを制御します。数種類のルールを作成することで、デバイスに対する読み取り、書き込み、お

よび実行操作を制御したり、承認または禁止されているデバイスと分類されていないデバイスの扱いを変えるように指定したりできます。

- 高度な設定 – 高度なポリシー設定では、主にポリシーが対象にするコンピューターで特定のファイル タイプをブロックするかどうかを制御します。使用できる値は、Active（アクティブ）、Off（オフ）、Report Only（レポートのみ）です。

ポリシー設定の詳細については、第 5 章「ポリシーの作成と構成」を参照してください。

モードと適用レベル

セキュリティ ポリシー内の適用レベルは、未承認ファイル（存在を確認されていない、または承認も禁止もされていないアプリケーション）の実行を許可するかどうかを制御します。複数の適用レベルを使用できるため、ポリシーごとに、そのポリシーが関連付けられているコンピューターのグループのセキュリティ要件とユーザー要件に適した設定を選択できます。

Bit9 Security Platform には、次の 3 種類の操作モードがあります : エージェント無効、可視性、制御。無効にされたエージェントは、ルールを適用することも、コンピューターからの情報をレポートすることもありません。可視性モードのエージェントは、情報を収集し、レポートしますが、ルールは適用しません。

制御モードでは、ファイルおよびデバイスのアクティビティの追跡、禁止などのルールの適用を含め、コンピューターを保護する Bit9 Security Platform のすべての機能が提供されます。禁止されているファイルは、制御モードですべての適用レベルについてブロックされています。制御モードの適用レベルは、主に未承認ファイルの扱いに関して次のように異なります。

- 高（未承認をブロック）– 承認されたファイルだけが実行を許可されます。
- 中（未承認に対してプロンプトを表示）– 承認されたファイルは実行を許可されます。未承認ファイルを実行しようとすると、通知ダイアログが表示され、許可するかブロックするかを選択できます。
- 低（未承認を監視）– 承認ファイルと未承認ファイルはプロンプトなしで実行を許可されます。ただし、これらのファイルのアクティビティは Bit9 Security Platform に監視されます。

場合によっては、コンピューターが接続されているかどうかによって適用レベルが変わることがあります。

Bit9 Security Platform のライセンスとモード

Bit9 Server のライセンスには、前のセクションで説明した使用可能なモードに応じて 2 つの機能レベルがあります。

- 可視性 – すべての Bit9 Security Platform のファイルおよびイベント追跡およびレポート機能が提供されますが、ファイル ブロックやデバイス ブロックなどの制御機能は提供されません。
- スイート – Bit9 Security Platform の可視性と制御の機能が提供されます。

ライセンス キーによって、各モードで実行可能なエージェントの数が決まります。たとえば、可視性ライセンスを 20、スイート ライセンスを 20 のように、同じサーバー上でライセンスを混合させることができます。さらに、いつでもアップグレードを購入して可視性ライセンスをスイートのレベルまで引き上げることができます。スイート ライセンスを「まったく」お持ちでない場合、制御の機能

は使用できず、本文書で記述されている Bit9 コンソールの要素の一部は表示されないことにご注意ください。

Bit9 Security Platform でのライセンスの機能の詳細については、「Bit9 Platform ライセンスの管理」（783 ページ）を参照してください。

運用戦略

Bit9 Security Platform の総合的な運用戦略は、ネットワーク上のファイルのアクティビティに対する「可視性」を得ることにのみ関心があるのか、ソフトウェアおよびデバイスの利用に対してある程度の「制御」を行う必要があるかによって決まります。また、すべてのコンピューターを同じセキュリティ レベルで運用するか、一部のコンピューターを他のコンピューターよりも高いレベルで制御する必要があるかによっても変わります。さらに、Bit9 Security Platform に関する経験の蓄積、新たな脅威レベル、IT が管理していない新しいソフトウェアをユーザーが実行する必要がある頻度などによって、時間の経過とともに戦略が変わる可能性もあります。

運用戦略が異なれば、必要な準備とメンテナンスの量も変わります。参考システムを作成することも考えられます。これは、ユーザーにとって承認されることが望ましいすべてのアプリケーションを含み、ユーザーのコンピューターで実行されることを避けるアプリケーションは含まない 1 台のコンピューターです。このシステムを使用することで、他のコンピューターにあるファイルが時間の経過によってどのようにドリフトするかを分析するためのベースラインを作成できます。

Bit9 テクニカル サポートまたはサービスの担当者が、環境に適した運用戦略の構築をお手伝いできます。

第 2 章

Bit9 コンソールの使用

この章では、Bit9 コンソールの基本的な使用法について説明します。具体的には、ログインとログアウトの方法、ホーム ページおよびメニュー システムからユーザー インターフェイスを操作する方法、Bit9 Security Platform がテーブル、詳細ページ、ダッシュボードを通じて提供する情報の表示方法です。この章の情報とタスクを習得すれば、本ガイドで説明している他のすべての Bit9 Security Platform アクティビティを理解しやすくなります。

セクション

ログイン

Bit9 Security Platform では「Bit9 コンソール」というブラウザー ベースのユーザー インターフェイスを使用します。このコンソールへは、Bit9 Server 自体も含むサーバーにアクセスできるすべてのコンピューター上の Web ブラウザーからログインできます。HTML フレーム サポートを使用するその他のブラウザーも動作するはずですが、次の Bit9 認定のブラウザーを推奨します。

- Microsoft Internet Explorer バージョン 10.0 以上
- Mozilla Firefox 最新バージョン
- Chrome 最新バージョン
- Safari 最新バージョン（OS X 上のみ）

Internet Explorer の場合、Bit9 コンソールにアクセスするには、セキュリティ設定全体を調整するか、Bit9 コンソール アドレスをローカル イントラネットまたは信頼済みサイト ゾーンの一部として設定しなければならない場合があります。セキュリティ設定は、Internet Explorer で［**ツール**］>［**インターネット オプション**］を選択し、［**セキュリティ**］タブをクリックして選択します。

Bit9 コンソールへのログイン手順：

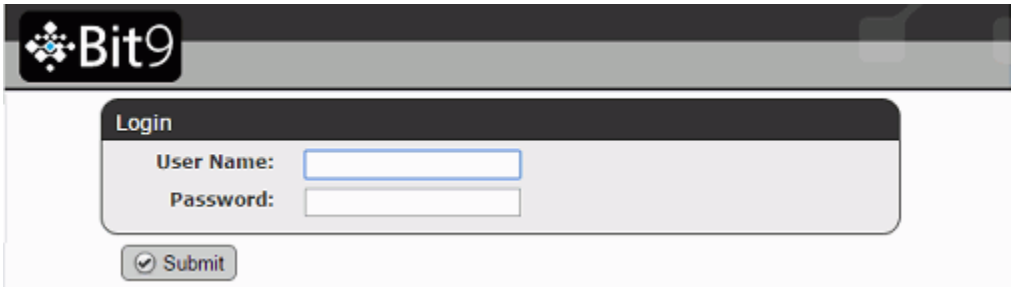
1. サポートされている Web ブラウザーから、インストール時に選択した Bit9 Server の名前を入力します。これは通常、サーバーの完全修飾ドメイン名、または設定した別名です。
   `https://server_name.domain.extension`
2. 証明書ダイアログが表示されたら、サーバーについて提示されたデジタル署名を受け入れます。Web ブラウザーで SSL および HTTPS 接続をサポートするためには、証明書が必要です。
   a. インストール時に提供した場合は、貴社の証明書が表示されます。そうでない場合は、サーバーのインストール時に作成された自己署名証明書が表示されます。Bit9 証明書を受け入れてもセキュリティが侵害されることはありません。
   b. ブラウザーから証明書に関する警告が表示された場合、この警告は無視しても問題ありません。残りの確認画面をクリックして進みます。

注意

証明書の警告が表示されないようにするには、次の手順を実行します。

- Firefox で証明書を永続的に承認します。
- Internet Explorer の場合、警告をクリックして IE ツールバーの［証明書エラー］ボタンをクリックし、自己署名証明書をインストールします。
- Safari の場合、警告上で［**証明書を表示**］をクリックし、Bit9 コンソールの証明書の［常に信頼］ボックスをオンにしたら、［**続ける**］をクリックします。

Bit9 コンソールのログイン画面が表示されます。



3. ユーザー名とパスワードを入力します。初回ログインでは、デフォルトのユーザー名 (admin) とパスワード (admin) を入力します。セキュリティのために、「アカウントのパスワードおよびその他の詳細の変更」（99 ページ）の指示に従ってパスワードをデフォルトから変更してください。
4. ［**Submit**（送信）］ボタンをクリックします。
5. Bit9 コンソールのホーム ページが表示されます。インストール後に初めていずれかのユーザーがログインするときは、ホーム ページが表示されるまで時間がかかる可能性があります。その後のログインにかかる時間は、すべてのユーザーで短縮されます。

ログイン、サーバー、バージョン、アラート情報

Bit9 コンソール ページの右上隅には、次の情報が表示されます。

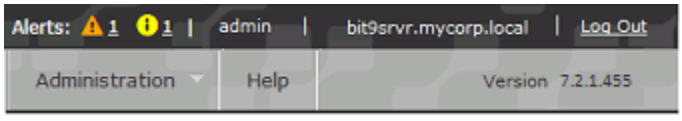
- 現在ログインしているコンソール ユーザーの名前
- Bit9 Server の名前（条件によっては IP アドレス）
- 実行している Bit9 ソフトウェアのバージョン番号
- 現在トリガーされている Bit9 Security Platform アラートがある場合は、3 つのカテゴリごとにその数と、それぞれの色の記号が表示されます：高（赤）、中（オレンジ）、低（黄）。記号または数の上にカーソルを置くと、そのカテゴリのアラートが 1 つだけの場合はアラート名が表示され、複数ある場合はアラート レベルが表示されます。

ログアウト

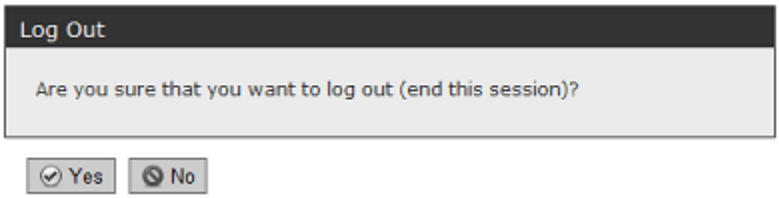
Bit9 コンソールのすべてのページには、［Log Out（ログアウト）］リンクが Web ページ右上隅のバナー領域に表示されます。ログアウトすると Bit9 コンソール セッションは終了します。

Bit9 コンソールからログアウトするには、次の手順を実行します。

1. コンソール バナーで［**Log Out**（ログアウト）］リンクをクリックします。



2. 確認メッセージに応答します。

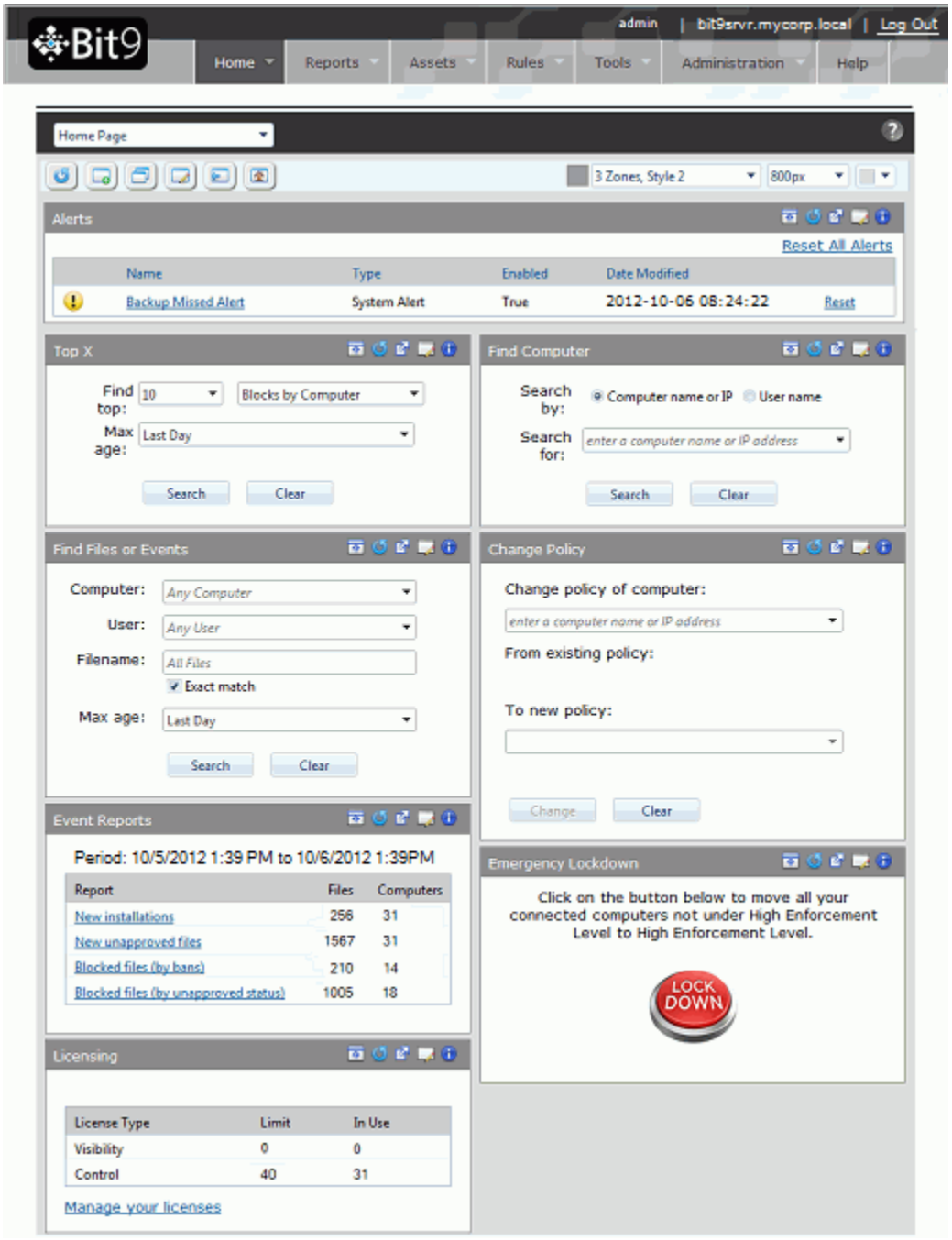


重要

コンソールのユーザー インターフェイスは、ユーザーがすべての権限を持っていることを前提に説明されています。個々のユーザーが利用できる機能は、そのユーザーのアカウント権限に依存します。権限をオフにすると、関連するユーザー インターフェイス要素は表示されません。Bit9 Security Platform のヘルプで説明されている機能が見つからないことによる混乱を避けるために、権限が制限されているユーザーにこのことを伝えることをご検討ください。詳細については、第 3 章「コンソール ログイン アカウントの管理」を参照してください。

ホーム ページ

ホーム ページからは、一般的なタスクと情報にすばやくアクセスすることができます。初めてログインすると、Bit9 Security Platform のホーム ページが表示され、ウィンドウの一番上には Bit9 コンソールのメイン メニューが配置されています。



ホーム ページは「ダッシュボード」です。これは構成可能なページであり、情報やコントロールを含む「ポートレット」を追加、削除することができます。ホーム ページおよび他のダッシュボードの使用方法と変更方法の詳細については、第 21 章「ダッシュボードの使用とカスタマイズ」を参照してください。ホーム ページのデフォルトの内容を次の表 2 に示します。ホーム ページは変更できるので、この表で説明されているものとは異なるポートレットが表示される可能性があることに注意してください。

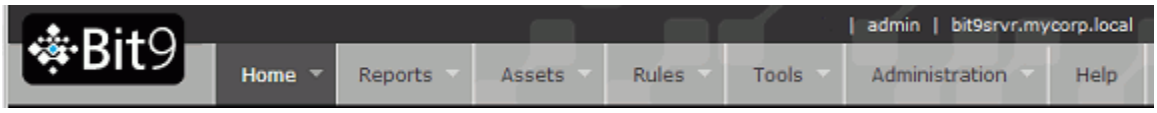
表 2：ホーム ページのクイック アクセス ポートレット

ポートレット	リンク / ボタン	説明
Alerts（アラート）	Reset/Reset All Alerts（リセット / すべてのアラートをリセット）	トリガーされてリセットされていないすべての Bit9 アラートが表示されます。それぞれに [Reset（リセット）] ボタンがあるので、選択してクリアすることができます。また、アラートごとに、そのアラートの詳細を示す［Alerts History（アラート履歴）］ページへのリンクも用意されます。
Top X（上位 X）	Search/Clear（検索 / クリア）	さまざまなカテゴリにおける上位のアイテムを示します。たとえば、前の日にブロックされたファイルの数が多かった上位 10 台のコンピューターなどです。表示するアイテムの数（デフォルトは 10）と、アイテムを検索する期間（デフォルトは 1 日）を指定できます。結果の中で名前（たとえばコンピューター名）をクリックすると、そのアイテムの詳細ページが開きます。数字をクリックすると、通常は上位 X 件のクエリに一致するイベントだけを示す［Events（イベント）］ページが表示されます。
Find Files or Events（ファイルまたはイベントの検索）	Search/Clear（検索 / クリア）	指定したコンピューター、ユーザー、またはファイルの名前に関連するファイルとイベント（ファイルのブロック、未承認ファイル、すべてのイベントなど）を検索します。ファイル名の検索では、[Exact Match（完全一致）] チェックボックスがオンになっていると、その 1 つのファイルだけが結果に表示されます（見つかった場合）。オフになっていると、入力ボックスに入力した文字列を含むすべてのファイルが結果に一覧表示されます。[Max Age（最長期間）] ドロップダウンでは、検索を実施する期間を決定できます。デフォルトは [Last Day（過去 1 日）] です。

ポートレット	リンク / ボタン	説明
Event Reports（イベント レポート）	New Installations（新規インストール）	この Bit9 Server によって管理されている Windows コンピューターで過去 1 日（ページを表示した時点の 24 時間前まで）に行われた、すべての新規ファイルのインストールを示すテーブルが表示されます。 **プラットフォームに関する注意**：この［New installations（新規インストール）］テーブルには、Mac システムでのインストールは含まれません。ただし、インストールされたファイルは、「新しいファイル」を示すテーブルには表示されます。
	New unapproved files（新しい未承認ファイル）	この Bit9 Server によって管理されているコンピューターに過去 1 日（ページを表示した時点の 24 時間前まで）の間に出現した、すべての新しい未承認ファイルを示すテーブルが表示されます。
	Blocked files (by bans)（ブロックされたファイル（禁止））	この Bit9 Server によって管理されているコンピューターで過去 1 日（ページを表示した時点の 24 時間前まで）の間にブロックされた、すべての禁止ファイルを示すテーブルが表示されます。
	Blocked files (by unapproved status)（ブロックされたファイル（未承認））	［Unapproved Executables（未承認実行可能ファイル）］設定の結果としてブロックされた、すべての新しい未承認ファイルが表示されます。レポートの対象は、過去 1 日（ページを表示した時点の 24 時間前まで）です。
Licensing（ライセンス）	Manage your licenses（ライセンスの管理）	サーバーで使用可能な Bit9 エージェント ライセンスの総数と、使用中のライセンスの数が表示されます。ライセンスの一部が可視性、一部が制御である場合は、タイプごとの数が示されます。 ［**Manage your licenses**（ライセンスの管理）］リンクをクリックすると、［System Configuration（システム構成）］ページの［Licensing（ライセンス）］パネルが開きます。ここで、Bit9 Security Platform ライセンスを入力し、Bit9 Software Reputation Service (SRS) を構成、有効化することができます。

ポートレット	リンク / ボタン	説明
Find Computer（コンピューターの検索）	Search/Clear（検索 / クリア）	文字列を入力すると、Bit9 エージェントが実行されているコンピューターのうち、名前または IP アドレスの全体または一部が一致するものが一覧表示されます。結果の中でコンピューター名をクリックすると、その［Computer Details（コンピューターの詳細）］ページが開きます。コンピューターの詳細には、現在の適用レベルと接続ステータスが含まれます。ページのタブ付きビューには、最終ログイン ユーザー、エージェントのバージョン、システムの詳細（取得できる場合）などの詳細情報も示されます。 コンピューター名の検索では、大文字と小文字は区別されません。
Change Policy（ポリシーの変更）	Change/Clear（変更 / クリア）	指定したコンピューターの現在のセキュリティ ポリシーを変更します。ポリシーを変更するコンピューターの名前または IP アドレスを上のボックスに入力します。そのコンピューターの現在のポリシーが表示されます。「変更後」のポリシーを下のボックスに入力します。［**Change**（変更）］をクリックすると、コンピューターは新しいポリシーに移行し、再び明示的に変更するまで維持されます。
Emergency Lockdown（緊急ロックダウン）	Lockdown/ Restore（ロックダウン / 復元）	［**Lockdown**（ロックダウン）］は、Bit9 Server によって管理され、接続されているすべてのコンピューターの適用レベルを、［High（Block Unapproved）（高（未承認をブロック））］に切り換えます。脅威が高まっているときにコンピューターを高適用レベルにすると、新しい実行可能ファイルの実行を確実に禁止できます。 コンピューターが緊急ロックダウン中のとき、［**Restore**（復元）］によってロックダウン前の状態に戻すことができます。緊急ロックダウン前に高適用レベルだったコンピューターは、その状態が維持されます。 **注意**：ロックダウンは、ローカル承認モードのシステムには影響しません。 制御ライセンスをまったくお持ちでない場合、［Lockdown（ロックダウン）］は無効化されますが、［Restore（復元）］は引き続き使用できます。これは、過去にフル ライセンスをお持ちだったときにマシンがロックダウンされた場合のためです。

メイン メニューの使用



各ページの一番上にある Bit9 コンソールのメイン メニューを使用すると、他のコンソール ページに容易に移動できます。このメニューは、論理的なタスク分類に基づいていくつかのセクションに整理されており、そのほとんどは、最上位のラベルの上にカーソルを置くとサブメニューが表示されます。最上位のアイテムをクリックすると、最初のサブ選択のためのページが表示されます。

表 3：Bit9 コンソール メイン メニューの選択項目

セクション	説明
Home（ホーム）	デフォルトでは、コンソールにログインするとホーム ページが表示されます。他のページでメニュー バーの［**Home**（ホーム）］をクリックすると、このページに戻ることができます。 ホーム ページからは、ファイル、イベント、コンピューター、ライセンスに関する情報にすばやくアクセスすることができます。また、必要に応じてコンピューターのポリシーを変更したり、ネットワーク全体のロックダウンを実行したりすることもできます。 ホーム ページは「ダッシュボード」です。そのため、提供される情報や情報の表示形式をカスタマイズによって変更できます。詳細については、第 21 章「ダッシュボードの使用とカスタマイズ」を参照してください。 ホーム ページにあるドロップダウン メニューには、アクセスできる他のダッシュボードが一覧表示されます。 コンソールにログインしたときに最初に表示されるページを変更できます。「コンソール ユーザーの設定」（83 ページ）を参照してください。

セクション	説明
Reports（レポート）	［**Events**（イベント）］は、Bit9 Security Platform によって監視されている、または Bit9 Security Platform に関係するアクティビティによるメッセージです。［Events（イベント）］ページの［Saved Views（保存済みビュー）］を使用すると、特定のタイプのイベントに関するカスタム レポートを表示できます。また、どのビューでもフィルターによって独自のレポートを作成できます。イベントには、ブロックされたファイル、実行された未承認ファイル、コンソール ユーザーによるシステム変更などがあります。ファイル関連のイベントの場合は、イベントから直接ファイルの詳細にリンクすることができます。 ［**Dashboards**（ダッシュボード）］では、［Dashboard List（ダッシュボード一覧）］ページが表示されます。ダッシュボードには、Bit9 Security Platform インストールと、そこから一連の小さな「ポートレット」を通じて管理する対象であるアセットに関する情報が表示されます。ファイル、コンピューター、イベント、アラートについて詳細を調べることができます。ホーム ページは特殊なダッシュボードです。各 Bit9 インストールには、それ以外に 1 つまたは複数のダッシュボードが存在します。ユーザーは、それぞれ独自のダッシュボードやポートレットを作成でき、オプションでそれを共有することもできます。 ［**Baseline Drift**（ベースライン ドリフト）］では、2 つのタブを持つページが表示されます。 • ［**Baseline Drift**（ベースライン ドリフト）］タブでは、指定したベースライン ファイル インベントリからの「ドリフト」を分析するレポートが使用可能であれば、それが表示され、レポートを実行でき、また、新しいレポートを作成、設定できます。 • ［**Baseline Drift**（ベースライン ドリフト）］ページの［Snapshot（スナップショット）］タブには、ベースライン ドリフト分析に使用するために作成した名前付きファイル、すなわち「スナップショット」が一覧表示されます。Bit9 コンソールでは、いくつかの画面からスナップショットを作成できます。 ［**External Notifications**（外部通知）］では、［External Notifications（外部通知）］ページが表示されます。このページには、Check Point、FireEye、Palo Alto Networks などのネットワーク セキュリティ デバイスからの通知のテーブルが表示されます。通知に示されているファイルまたはコンピューターが Bit9 エンドポイント データにもある場合は、そのデータを通知と結び付けることができます。

セクション	説明
Assets（アセット）	[**Computers**（コンピューター）] には、Bit9 Security Platform によって管理されるコンピューターのテーブルが表示されます。コンピューターのテーブルは、さまざまなカテゴリによってフィルターできます。テーブル内のコンピューターは、適用するセキュリティ ポリシーを変更する、ローカル承認にする、または通常のポリシーによって決まる適用レベルに戻すことができます。 [**Files**（ファイル）] では、[Files（ファイル）] ページが表示されます。このページには、Bit9 Security Platform で管理されるコンピューター上のファイルが 2 つのタブ付きリストに表示されます。 • [**File Catalog**（ファイル カタログ）] は、Bit9 Server にレポートするエージェントによって発見されたすべての「一意な」ファイルのリストです。 • [**Files on Computers**（コンピューター上のファイル）] は、Bit9 Server にレポートするエージェントによって発見された、追跡されているファイルのすべてのインスタンスのリストです。 また、[Saved Views（保存済みビュー）] メニューを使用して、表示するファイルをさらに指定することもできます。ビューには、[Banned Files（禁止ファイル）]、[New Unapproved Files（新しい未承認ファイル）]、[Malicious Files（悪意のあるファイル）]、[Categorized Files（分類済みファイル）]、[Installed Programs（インストール済みプログラム）] があります。 **プラットフォームに関する注意**：[Installed Programs（インストール済みプログラム）] ビューに表示されるのは、Windows プログラムのみです。 [Files（ファイル）] ページでカスタム フィルターを使用すると、特定のファイルを検索して、必要に応じて禁止または承認（ローカルまたはグローバルに）することができます。 [**Devices**（デバイス）] では、[Devices（デバイス）] ページが表示されます。このページには、Bit9 Security Platform によって Windows コンピューター上で検出されたリムーバブル デバイスが 2 つのタブ付きリストに表示されます。 • [**Device Catalog**（デバイス カタログ）] には、2 つのビューがあります。1 つは、Bit9 Server にレポートするエージェントによって発見されたすべての一意なデバイス モデルのリストです。もう 1 つは、発見されたすべてのインスタンス（一意のシリアル番号）のリストです。 • [**Devices on Computers**（コンピューター上のデバイス）] は、すべての一意な接続のリストで、ここでの接続は 1 台のコンピューターと 1 台のデバイスの組み合わせとして定義されます。 これらのデバイスのいずれかをグローバルに承認または禁止することで、他のデバイスが制限されているときでも承認されたデバイス上のファイルにはクライアント コンピューターがアクセスできるように、または特定の禁止されたデバイス上のファイルは絶対に実行を許可されないようにすることができます。 **プラットフォームに関する注意**：デバイスの発見と制御は、現在、Windows 上のエージェントでのみ使用できます。

セクション	説明
Rules（ルール）	［**Policies**（ポリシー）］では、既存のポリシー（セキュリティ ルールの名前付きセット）のテーブルが表示され、それらのポリシーを編集したり、新しいポリシーを作成したりできます。Bit9 エージェントのダウンロード ページへのリンクも表示されます。 ポリシーを作成すると、自動的にそれぞれに独自のエージェント インストール ファイルが生成されます。エージェントをインストールするためのインストール ファイルによってコンピューターの初期ポリシーが決まりますが、コンピューターは別のポリシーに移行したり、サービスの終了に伴ってポリシーから削除することもできます。 Bit9 Security Platform と Active Directory の統合を構成してある場合は、［Policies（ポリシー）］ページに［**Mappings**（マッピング）］タブが表示されます。これをクリックすると、［Active Directory Policy Mappings（Active Directory ポリシー マッピング）］ページが表示され、Bit9 エージェントが実行されているコンピューターを、コンピューター（またはユーザー）が属している Active Directory グループの 1 つに従って Bit9 ポリシーに割り当てるためのルールを設定できます。 ［Mappings（マッピング）］オプションは、Bit9 Server と Active Directory サーバーが同じ Active Directory フォレストに存在し、［System Configuration（システム構成）］ページで Active Directory ポリシー マッピングを有効にしてある場合にのみ表示されます。Bit9 Server が、ユーザーおよびシステムを認識するために使用される Active Directory サーバーのフォレストに存在しない場合は、Bit9 サポートにご連絡ください。 ［**Notifiers**（通知）］では、現在ブロックされているファイルまたはアクションの通知のうち、ポリシーおよびその設定に関連付けることができるものがテーブルに表示されます。このページでは、通知を追加、削除、変更できます。Bit9 エージェントが実行されているエンドポイントでアクションがブロックされたときに、そのエンドポイントに通知が表示されるように設定することができます。 ［**Software Rules**（ソフトウェア ルール）］では、ファイルを承認または禁止するため、およびコンピューターの重要な機能へのアクセスを制御するための Bit9 Security Platform ルールが、いくつかのカテゴリ別に表示されます。それぞれのタブに既存のルールが表示され、タブに応じて編集、削除、作成、ルールの有効化または無効化ができます。 • ［**Updaters**（アップデーター）］タブには、Bit9 Server で把握されているアップデーターが一覧表示されます。アップデーターを有効にすると、アプリケーションの更新がダウンロードできるようになった場合は常に、エンドユーザーがそのアプリケーションの更新プログラムを通じてインストールすることが許可されます。**プラットフォームに関する注意**：アップデーターは、プラットフォームに固有です。 • ［**Publishers**（公開者）］タブには、Bit9 Security Platform が 1 つまたは複数の有効なデジタル署名を確認できるソフトウェア ベンダーが一覧表示されます。公開者は、このページで承認または禁止することができます。

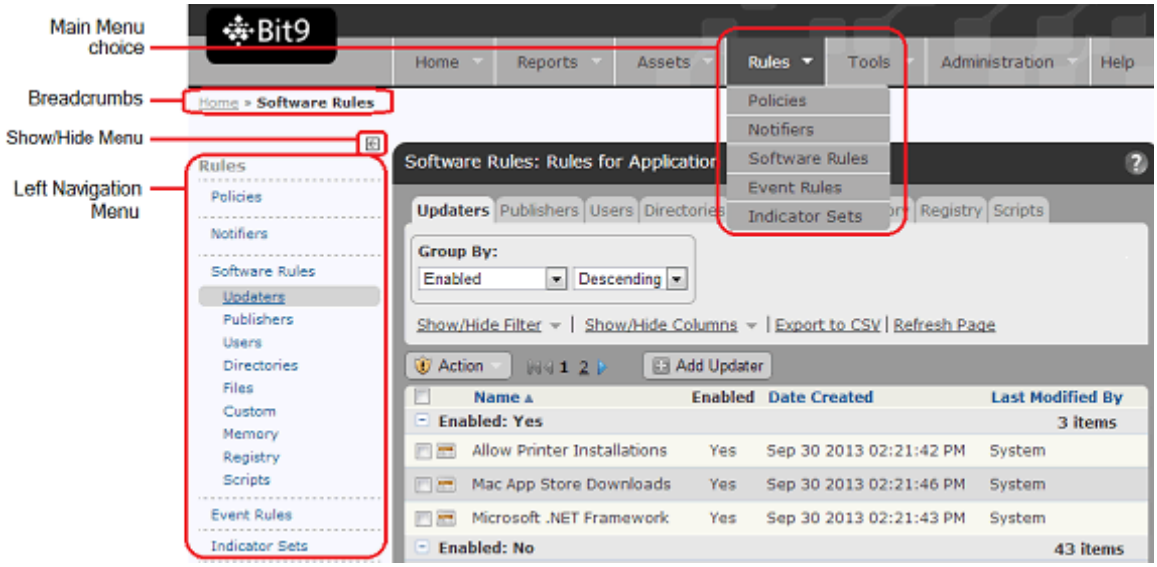
セクション	説明
Rules（ルール）（続き）	• [**Users**（ユーザー）] タブには、認証情報を使用してログインしたすべてのコンピューターにファイルをインストールする許可を持っている、信頼できるユーザーまたはグループが一覧表示されます。 • [**Directories**（ディレクトリ）] タブには、すべてのソフトウェアが承認される、認証された承認ディレクトリが一覧表示されます。 • [**Files**（ファイル）] タブには、個別のファイルの承認と禁止が一覧表示されます。 • [**Custom**（カスタム）] タブには、ファイルの実行や書き込みが許可される方法と場所の指定、ファイルが Bit9 Security Platform によって追跡されるかどうか、変更が許可されないディレクトリなどのカスタム ルールが一覧表示されます。 • [**Memory**（メモリ）] タブには、指定したプロセスに関して情報の取得、変更、および実行（または終了）を制御する Bit9 Security Platform ルールが一覧表示されます。 **プラットフォームに関する注意**：この機能は、Windows 上のエージェントでのみ有効です。 • [**Registry**（レジストリ）] タブには、Windows レジストリの作成、変更、編集を制御する Bit9 Security Platform ルールが一覧表示されます。 **プラットフォームに関する注意**：この機能は、Windows 上のエージェントでのみ有効です。 • [**Scripts**（スクリプト）] タブには、Bit9 Security Platform でスクリプトとして追跡、制御するファイルを定義するルールが一覧表示されます。 • [**Reputation**（レピュテーション）] タブは、[System Configuration（システム構成）] の [Licensing（ライセンス）] ページで Bit9 Software Reputation Service が有効にされている場合に表示されます。レピュテーション ベースのファイルおよび公開者の承認は、このタブで有効または無効にすることができます。 [**Event Rules**（イベント ルール）] では、[Event Rule（イベント ルール）] テーブルが表示されます。イベント ルールは、定義したフィルターにイベントが一致する場合に実行されるアクションを指定します。 [**Indicator Sets**（痕跡セット）] では、[Indicator Set（痕跡セット）] テーブルが表示されます。痕跡セットは、高度な脅威検出ルールをグループ化したもので、有効にすることで疑わしいアクティビティの可視性を高めることができます。
Tools（ツール）	[**Meters**（メーター）] では、指定したファイルの実行回数と、実行したユーザーおよびコンピューターを監視することができます。 [**Alerts**（アラート）] では、一定の条件が成立したときに Bit9 コンソールおよび E メールによって通知を提供します。アラートは、ポリシー固有にすることができます。

セクション	説明
Tools（ツール）（続き）	［**Find Files**（ファイルの検索）］では、ネットワーク上に存在する、Bit9 エージェントが実行されているコンピューターで、実行可能ファイルのすべてのインスタンスが検索されます。同様の検索は［Files（ファイル）］ページでフィルターを使用して実行することもできますが、［Find Files（ファイルの検索）］はこの目的のために事前構成されています。 ［**Approval Requests**（承認要求）］では、Bit9 エージェントが実行されているコンピューター上のユーザーから受け取ったファイル承認要求が表示されます。要求は、ユーザーがファイル アクションをブロックされたとき、そのファイルの承認を要求すると作成されます。［Approval Requests（承認要求）］ページには、要求のステータスがファイルおよび要求者の情報とともに表示されます。 ［**Requested Files**（要求されたファイル）］では、それぞれがファイルのテーブルを含む 3 つのタブを持つページが表示されます。それぞれのタブは次のとおりです。 • ［**Uploaded Files**（アップロードされたファイル）］– このテーブルは、コンソール ユーザーがエージェント コンピューターからサーバーへのアップロードを要求したファイルのリストとステータスを示します。 • ［**Analyzed Files**（分析されたファイル）］– このテーブルは、コンソール ユーザーまたはルールが分析のために外部デバイスへの送信を要求したファイルのリストとステータスを示します。 • ［**Diagnostic Files**（診断ファイル）］– このテーブルは、コンソール ユーザーがエージェント コンピューターからサーバーへのアップロードを要求した診断ファイルのリストとステータスを示します。 ［**Preferences**（設定）］では、各ユーザー（読み取り専用ユーザーも含む）がパスワードの変更、ログイン時に最初に表示されるページの選択、テーブル ページのデフォルト行数の決定、列のサイズ変更可能の有効化、次回のログイン時にコンソールのページへのカスタマイズが維持されるかどうかの指定を行うことができます。
Administration（管理）	［**Login Accounts**（ログイン アカウント）］では、Bit9 コンソールのユーザーを作成および管理する［Login Accounts（ログイン アカウント）］ページが表示されます。Bit9 エージェントが実行されているコンピューターのユーザーには、ログイン アカウントは不要です。 ［**System Configuration**（システム構成）］では、サーバー構成、ログ ファイルの管理、エージェントとの通信の保護、バックアップの構成、ソフトウェア更新のダウンロード、さらに Active Directory との統合など、オプションの Bit9 Security Platform サービスの構成などのタスクを行うページにアクセスできます。システム構成機能は、管理者レベルのログイン アカウントでのみ使用できます。 ［**System Health**（システム正常性）］では、［System Health（システム正常性）］ページが表示されます。ここでは、Bit9 Server の動作に影響する要素の状態の概要と、サーバーの運用環境要件への準拠など、特定の要素の詳細が示されます。

セクション	説明
Help（ヘルプ）	[**Using the Bit9 Security Platform**（Bit9 Security Platform の使用）] では、Bit9 Security Platform のユーザーガイドがブラウザーの別ウィンドウに表示されます。また、コンソールの他のページで［Help（ヘルプ）］ボタンをクリックすると、ヘルプ システムが起動して、該当するページやダイアログ ボックスに関する状況依存の情報が表示されます。

左側のナビゲーション メニューとパンくず機能

ダッシュボード以外のコンソール ページでは、ナビゲーション メニューがページの左端に表示されます。このナビゲーション メニューには、現在の Bit9 コンソール メイン メニュー内のセクションから選択できるページが表示されます。たとえば、トップ メニューで［**Rules**（ルール）］をクリックし、メニューから［**Software Rules**（ソフトウェア ルール）］を選択すると、［Software Rules（ソフトウェア ルール）］ページが開き、デフォルト タブの［Updaters（アップデーター）］が表示されます。アップデーター テーブルの左には、［Rules（ルール）］のすべての選択項目を示すメニューがあります。ここで選択項目をクリックすると、関連するページが表示されます。左側のナビゲーションは、メニューの右上にある四角形で囲まれた矢印ボタンをクリックすることで、縮小または展開することができます。



いずれかのコンソール ページに移動すると、現在のページまでの経路を示す「パンくず」がページの左上に表示されます。上の図では、［**Home**（ホーム）］>［**Software Rules**（ソフトウェア ルール）］が、現在表示されているページへの経路です。これをクリックすることで、経路上の前の場所に戻ることができます。

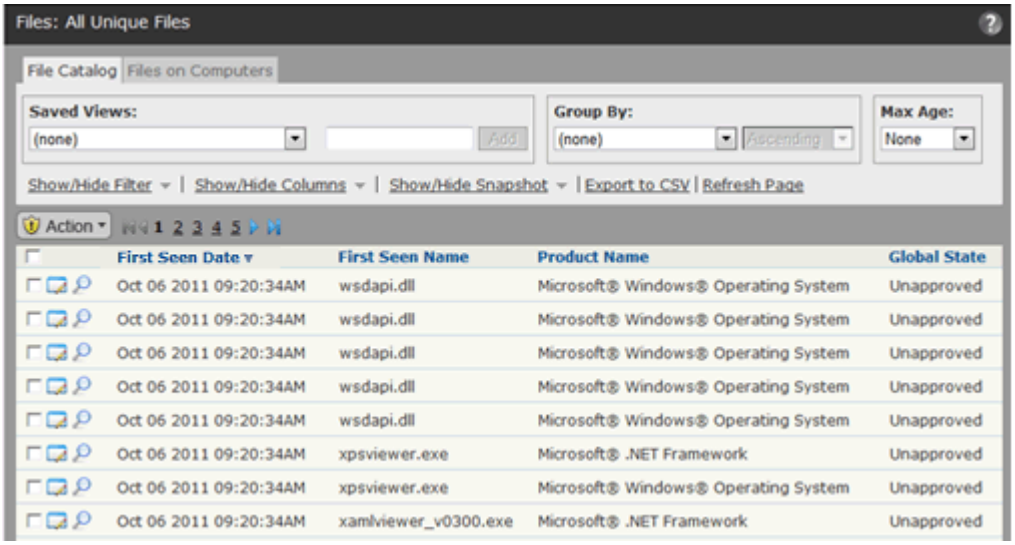
Bit9 コンソールのテーブル

Bit9 コンソールの使用中に表示されるファイルとコンピューターの情報の多くは、テーブル形式です。Bit9 コンソールのテーブルには、そのページの中心的なアイテム（たとえば、[Files（ファイル）] ページならば各ファイル）が 1 つにつき 1 行を使って、そのアイテムに関連するデータとともに表示されます。これらのテーブルに含まれる情報の「ビュー」をさまざまな面から制御できます。また、特定のビューに名前を付けて保存することもできます。このセクションでは主に表示を扱っていますが、Bit9 コンソールのテーブルにはファイルやコンピューターに対するアクションを実行するためのコントロールも数多く用意されています。これらのアクションについては、この後の章で説明します。

注意

このセクションでは、現在多くの Bit9 コンソール ページで使用されているテーブルについて説明します。ダッシュボード ページは、レイアウトとボタンが他と異なります。ダッシュボードの要素の説明については、第 21 章「ダッシュボードの使用とカスタマイズ」を参照してください。

[Files（ファイル）] ページには、Bit9 コンソールのテーブルによく表示される要素の多くが含まれています。



テーブルにはさまざまなボタンとメニューがあり、結果や実行アクションを構成することができます。すべてのページに表示される [Help（ヘルプ）] ボタンに加えて、テーブルが表示される Bit9 コンソール ページには次の要素があります。

- テーブル データ制御リンク
- テーブル列のサイズ変更
- 列のアクション ボタン
- チェックした行のアクション メニュー
- 「追加」ボタン

テーブル データ制御リンク

Bit9 コンソールのテーブル ページの多くには、テーブル見出しの上にテキスト リンクが 1 行あり、そこからテーブル データに対してアクションを実行できます。利用できるテーブル データ制御リンクを表 4 に示します（これが表示されないページもあります）。

表 4：テーブル データ制御リンク

リンク テキスト	アクション
Show/Hide Filter（フィルターの表示 / 非表示）	[Filters（フィルター）] パネルを表示または非表示にします。ここでは、テーブルに返される結果の数を絞り込むことができます。
Show/Hide Columns（列の表示 / 非表示）	[Column Settings（列の設定）] パネルを表示または非表示にします。ここでは、表示する列とその順番を指定することができます。
Show/Hide Snapshot（スナップショットの表示 / 非表示）	[Snapshot（スナップショット）] パネルを表示または非表示にします。ここでは、選択したファイルをファイルの既存の「スナップショット」に追加したり、新しいスナップショットを作成したりできます。スナップショットを使用すると、ベースライン ドリフトを計測できます。詳細については、「スナップショットの管理」（661 ページ）を参照してください。
Export to CSV（CSV へのエクスポート）	現在のブラウザーの標準的なダウンロード方法を使用して、現在のテーブルに表示されている情報をファイルに保存します。エクスポートされるデータの形式は、スプレッドシートとして開くのに適した CSV（コンマ区切り値）ファイルです。CSV ファイルに出力される時刻値は、UTC 時刻で記録されます。
Refresh Page（ページの更新）	ページの表示を更新して、Bit9 Server から取得できる最新のデータを表示します。これは、1 つのページを長時間表示したままのときや、変更頻度が高い情報を含むページを表示しているときに便利です。

テーブル列のサイズ変更

テーブルの幅を制御する方法の 1 つは、[Show/Hide Columns（列の表示 / 非表示）] リンクを使用して列を追加または削除することです。それ以外に、テーブル列のサイズを変更する方法もあります。この機能は、列の間に垂直の境界線が表示されている場合に使用できます。列のサイズ変更を有効または無効にするには、コンソール メニューで［**Tools**（ツール）］>［**Preferences**（設定）］を選択して、[Preferences（設定）] ページで行います。

列の幅を変更するには、マウス カーソルを列の境界線の上に置き、マウスの左ボタンを押したままマウスを動かします。列の幅をその内容よりも狭くすると、文字の末尾が省略記号 (…) で表示されます。

列のアクション ボタン

動的テーブルの行には、クライアント コンピューター、デバイス、イベント、レポート、ファイルなどのオブジェクトに関する情報が含まれます。多くのテーブルでは、各行の左端にボタンがあり、その行に対する操作を実行できます。

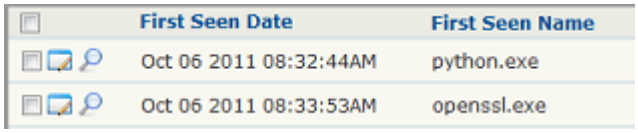


表 5：一般的な列のアクション ボタン

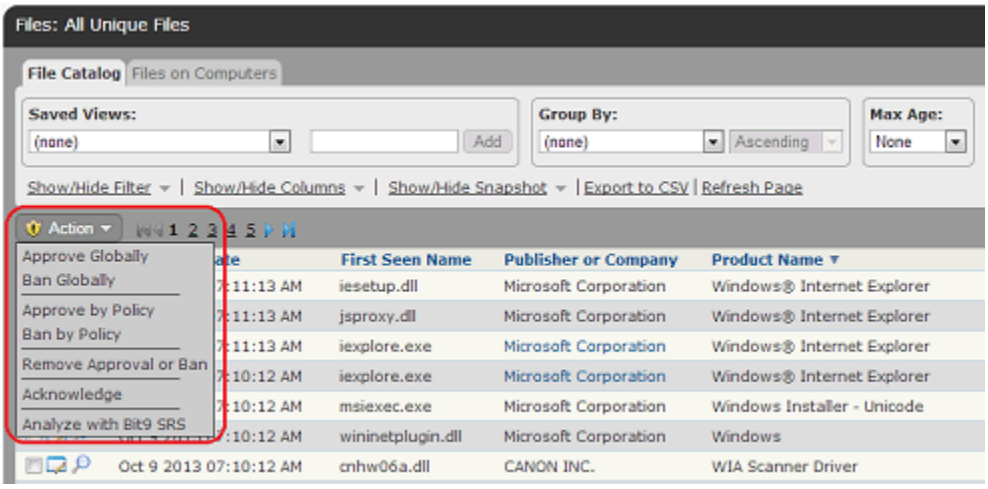
ボタン	ラベル	アクション
	詳細の表示	その行のアイテムの詳細が表示されます。アイテムに編集可能なプロパティがある場合、このボタンをクリックするとプロパティのエディターが起動します。
	削除	その行がテーブルおよび Bit9 データベースから削除されます。
	レポートの表示	行のアイテムに対応するレポート、履歴、その他の情報が表示されます。
	ファイルの検索	[Find Files（ファイルの検索）] ページが表示され、検索パラメーターとして現在の行のファイルの名前またはハッシュが自動的に使用されます。

注意

テーブルによって、表示される情報の種類に合わせて行のアクション ボタンの組み合わせは異なります（すべてのボタンが表示されないことがあります）。テーブルによっては、ここに示されていない、ページ固有のボタンが表示されます。

チェックした行のアクション メニュー

多くのページには［Action（アクション）］メニューがあり、そのページのテーブルでチェックした行に対してアクションを実行するためのコマンドが含まれています。たとえば、［Files（ファイル）］ページの［File Catalog（ファイル カタログ）］タブで「abc.exe」の隣のボックスをオンにすると、［Action（アクション）］メニューからファイルのグローバルな承認または禁止、既存の承認または禁止の削除、ファイルの確認、Bit9 Software Reputation Service でのファイルの分析を実行できます。



［Action（アクション）］メニューの選択項目は、現在のページと、場合によっては構成したオプションによって変わります。

注意

チェックしたアイテムに対するアクションは、現在のページに「表示されている」チェック済みアイテムにのみ有効です。たとえば、Bit9 コンソールのテーブルが 3 ページにわたっており、2 ページでアイテムをチェックしてから 1 ページに戻ると、2 ページでのチェックマークはクリアされます。1 ページでいくつかのアイテムをチェックしてから［Action（アクション）］メニューで［Approve Globally（グローバルに承認）］を選択すると、その前に他のページでアイテムをチェックしていても、1 ページ目に表示されているチェック済みのアイテムだけが承認されます。

また、テーブルの先頭のチェックボックスをオンにすると、現在表示されているページのすべてのアイテム（またはアクションを実行できるすべてのアイテム）だけがチェックされ、他のページの行はチェックされません。

同様に、あるページでアイテムをグループ化しても、チェックしたりアクションを実行したりできるのはグループ内の表示されているアイテムだけです。グループが縮小されている（グループ名だけが表示されている）ときは、グループ内のいずれのアイテムもチェックされているとしては扱われません。

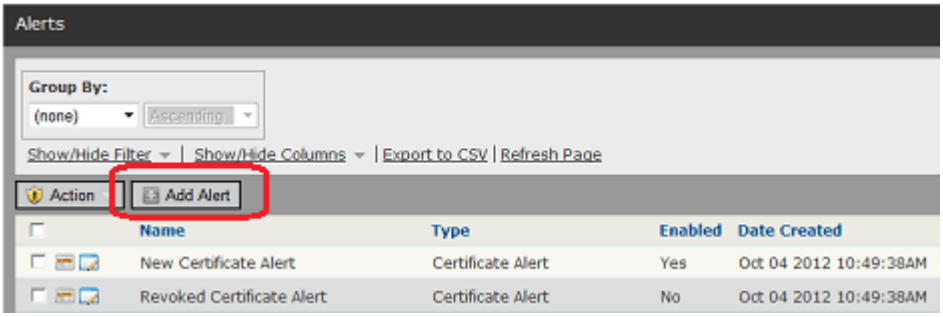
行ランク矢印

一部のテーブルでは、行のランキングが Bit9 Security Platform によるルールの処理に影響します。たとえば、［Custom Rules（カスタム ルール）］ページでルール番号 1 はルール番号 2 の前に処理される、などです。これらのテーブルでは、各行の前にランク番号が表示され、ランク順にソートすることができます。

ランクが意味を持つテーブルでは、各行に（特殊な場合を除いて）矢印が表示され、ルールを移動してランクを高く、または低くすることができます。また、このようなテーブルでは通常、ドラッグアンドドロップによって行のランクを変更することもできます。

「追加」ボタン

ポリシーやアラートなど、何かの新しいインスタンスを作成することができるページには、そのアイテムを追加するためのボタンがあります。たとえば、新しいアラートを作成する場合は、[Alerts（アラート）] ページに移動し、[**Add Alert**（アラートの追加）] ボタンをクリックして、新しいアラートを設定できるフォームを開きます。これらの追加ボタンは通常、ページの左上の領域に表示されます。



ページ、タブ、保存済みビュー

テーブルが表示される Bit9 コンソール ページには、ファイルのテーブル、コンピューターのテーブル、イベントのテーブルなど、それぞれ特定のタイプの情報が含まれています。多くのページでは、数種類の中から「ビュー」を選択することができます。ビューは、そのページ上のデータを一定のパラメーターに制限するもので、必要に応じて新たに作成することもできます。テーブル ページには、以下の機能のうち 1 つまたは複数が用意されています。

- 「タブ」は、ページ上の情報を大きなサブセット間で切り換えるためのものです。たとえば、[Files（ファイル）] ページでは、1 つのタブには Bit9 Security Platform によって見つかったすべての一意なファイルの [Files Catalog（ファイル カタログ）] が示され、別のタブには各コンピューターで追跡されるファイルのインスタンスを含む [Files on Computers（コンピューター上のファイル）] リストが示されます。
- 「フィルター」を使用すると、指定した条件に一致するアイテムだけがテーブルに表示されるようにデータを限定できます。たとえば、ファイル テーブルにフィルターを適用して、特定の承認または禁止状態のファイルだけを表示したり、特定の脅威レベルのファイルだけを表示することができます。フィルターは、それによって作成されたビューを保存するかどうかに関係なく使用できます。
- 「列コントロール」を使用すると、テーブルの各アイテムに関するさまざまな情報を表示できます。たとえば、ファイルが作成された日を示す列を除外し、誰かがそのファイルを実行したかどうかを示す列を追加することができます。フィルターと同様に、特殊な列設定を [Saved Views（保存済みビュー）] に組み込むことも、一時的にのみ使用することもできます。
- 「保存済みビュー」では、フィルターによって不要なアイテムをテーブルから除外したり、各アイテムについて表示されるデータのタイプ（列）を変更したりすることができます。Bit9 には事前構成された保存済みビューが用意されており、また、自分で作成することもできます。保存済みビューのないページもあります。

- 「グループ別」は、テーブル内の情報をグループ化するさまざまな方法をメニューから選択できます。たとえば、[Computers（コンピューター）] ページでポリシーによってグループ化すると、ポリシーのリストが作成され、各ポリシーをクリックすると、そのポリシーに含まれるすべてのコンピューターが表示されます。
- 「最長期間」を使用すると、テーブルに表示される結果を、メニューで選択した期間内のものに制限できます。

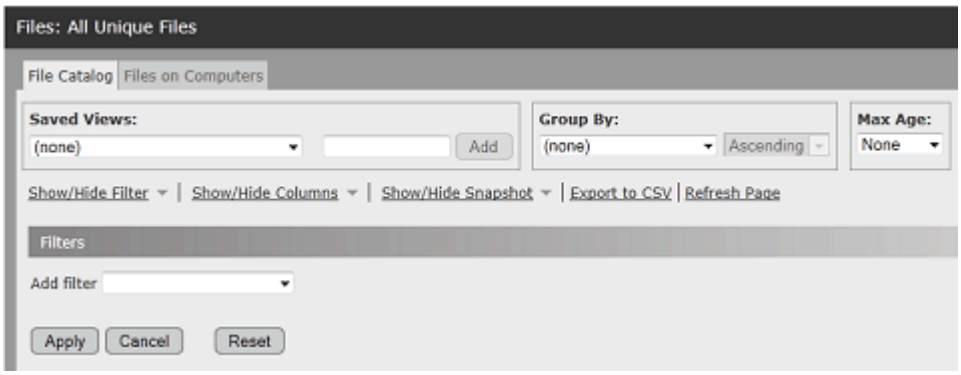
Bit9 コンソールのあるページから離れてから戻ってきたときに各ページをデフォルト ビューに戻すか、最新のページ ビューの選択を「記憶」しておき、次にそのページを表示したときに適用するかを選択できます。詳細については、「コンソール ユーザーの設定」（83 ページ）を参照してください。

フィルターのオプション

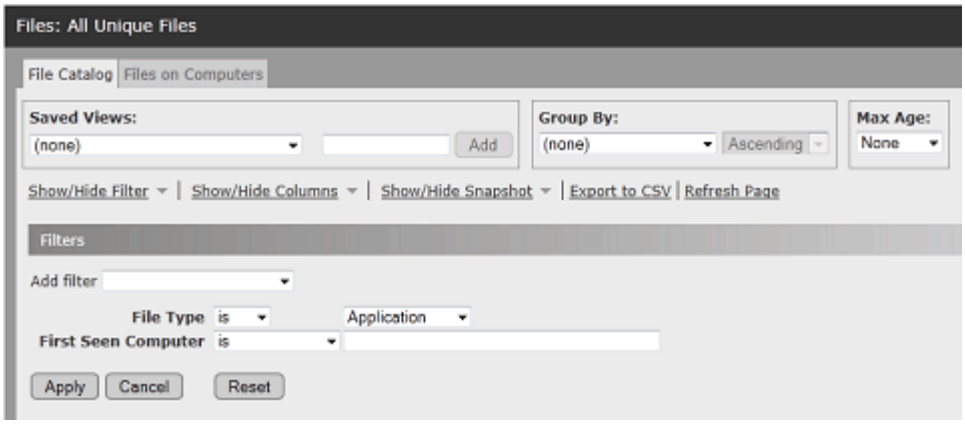
フィルターを使用すると、テーブルに表示される情報を絞り込んで、必要なデータを見つけやすくすることができます。それぞれがテーブル列の情報に対応する 1 つまたは複数の属性を選択し、検索する属性値を入力します。フィルターに対して使用できる演算子は、選択した属性によって異なります。選択したフィルターに基づいて、値はテキスト、数値、日付のいずれかになります。日付値を受け入れる属性の場合、Bit9 コンソールでは日付ボックスが表示されます。

テーブルの結果にフィルターを適用する手順：

1. [**Show/Hide Filters**（フィルターの表示 / 非表示）] をクリックして [Filters（フィルター）] ダイアログを開きます。



2. ［Add Filter（フィルターの追加）］メニューで、テーブルに表示される情報を制限するために使用する 1 つまたは複数のフィルター属性を選択します。



3. 各フィルター属性について、適切な演算子を選択し、値を（必要に応じて）入力します。
4. 選択した属性によって結果にフィルターを適用するには、［**Apply**（適用）］ボタンをクリックします。
5. フィルターが適用される前の結果に表示を戻すには、［**Reset**（リセット）］ボタンをクリックします。

デフォルトの演算子は選択した属性によって異なり、場合によってはパフォーマンス上の理由から決定されます。たとえば、「is」が［File Name（ファイル名）］のデフォルトの演算子になっているのは、フィルターに一致するデータの量を制限するためです。

通常は、同じタイプの複数のフィルターを追加することができます。同じタイプの 2 つのフィルターは、either/or 操作として扱われます。たとえば、［File Name（ファイル名）］フィルターとして、「alpha」を含むファイル名のフィルターと「beta」を含むファイル名のフィルターを追加すると、テーブルには「alpha」または「beta」を名前に含むファイルが表示されます。

「value（値）」フィールドは、一致させるデータを表します。多くのフィルターでは、文字を入力する際に「オートコンプリート」が機能します。たとえば、「contains」演算子を指定した［Product Name（製品名）］フィルターに対して「Abc」と入力すると、Bit9 コンソールには「Abc」を含むすべての製品名のメニューが表示されるため、名前をすべて入力することなく、そこから 1 つを選ぶことができます。

フィルターは、現在テーブルに表示されているレベルの情報にのみ適用されます。たとえば、個別のファイルでなくファイル グループのリストを表示している場合（デフォルト）、［First Seen Name（最初に発見された名前）］が「abc」を含むものを検索するフィルターは、この文字列を含むインストーラー ファイルにのみ一致します。他のファイルによってインストールされた個別のファイルには一致しません。一方、同じフィルターが有効な状態で［Show individual files（個別のファイルを表示）］ボックスをオンにすると、フィルターの文字列を含み、インストーラーによってインストールされたすべてのファイルがテーブルに表示されます。

注意

- ［Show/Hide Filters（フィルターの表示 / 非表示）］ボタンと［Show/Hide Columns（列の表示 / 非表示）］ボタンをクリックすると、両方のパネルを同時に表示できます。この組み合わせによって、特定のテーブルをどのように変更するかについてアイデアが得られる可能性があります。
- 定期的に使用するビューを保存するには、新しい保存済みビューを作成します。「デフォルト ビューと保存済みビュー」（77 ページ）を参照してください。

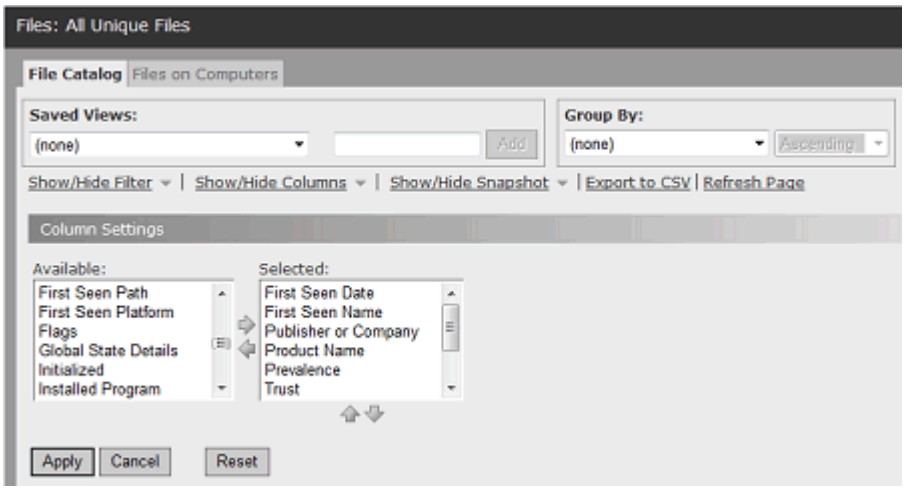
［Show/Hide Columns（列の表示 / 非表示）］のオプション

［Show/Hide Columns（列の表示 / 非表示）］リンクをクリックすると、［Column Settings（列の設定）］パネルが開きます。ここには、表示する列と、特定のテーブルでの表示の順番が表示されます。

- ［Selected（選択済み）］列の項目はテーブルに表示されます。
- ［Available（使用可能）］列の項目はテーブルに表示されません。
- ほとんどのページでは、表示できる列の数が非常に多いため、デフォルトではすべての列は表示されていません。また、Bit9 コンソールのページによってデフォルトの列は異なります。いずれのテーブルも、初期状態のデフォルトの列にリセットすることができます。

テーブル列に表示される情報の表示 / 非表示 / 並べ替え手順：

1. ［**Show/Hide Columns**（列の表示 / 非表示）］をクリックします。［Column Settings（列の設定）］パネルが表示されます。



2. 現在表示されている列の非表示手順：
   a. ［Selected（選択済み）］リストで、列見出しを選択します。
   b. 左向き矢印のアイコンをクリックすると、選択した列見出しが［Available（選択可能）］リストに移動します。

c. 変更を受け入れてテーブルの表示を更新するには、[**Apply**（適用）] ボタンをクリックします。

3. 現在非表示の列の表示手順：
   a. [Available（選択可能）] リストで、列見出しを選択します。
   b. 右向き矢印のアイコンをクリックすると、選択した列見出しが [Selected（選択済み）] リストに移動します。
   c. 変更を受け入れてテーブルの表示を更新するには、[**Apply**（適用）] ボタンをクリックします。
4. 列の順番の変更手順：
   a. [Selected（選択済み）] リストで、列見出しを選択します。
   b. [Selected（選択済み）] リストの下にある上向きまたは下向き矢印をクリックすると、テーブル内での列の位置を変更できます。リストでの上から下への順番が、テーブルでの列の左から右への並びに対応しています。移動できるのは、テーブルに表示されるアイテム（[Selected（選択済み）] リストに表示される列）だけです。
   c. 変更を受け入れてテーブルの表示を更新するには、[**Apply**（適用）] ボタンをクリックします。
5. 現在のビューでテーブルをデフォルト設定に戻すには、[**Reset**（リセット）] ボタンをクリックします。

注意

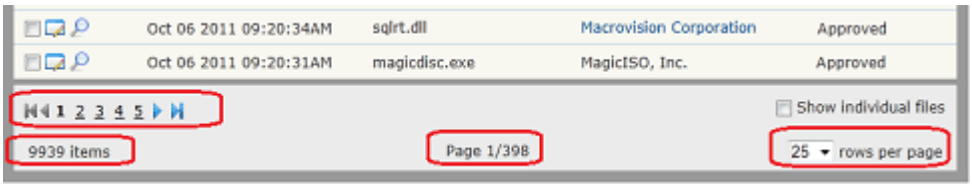
- [Show/Hide Filters（フィルターの表示/非表示）] ダイアログと [Show/Hide Columns（列の表示 / 非表示）] ダイアログは、両方を同時に開くことができます。この 2 つの組み合わせによって、特定のテーブルをどのように変更するのが最適か、アイデアが得られる可能性があります。
- 列コントロールを使用して構成したビューを定期的に使用すると考えられる場合は、ビューに名前を付けると、保存済みビューとしてアクセスできるようになります。「デフォルト ビューと保存済みビュー」（77 ページ）を参照してください。

タブ

「タブ」は、同一ページ内の情報を大きなグループに分けて切り換えるためのものです。たとえば、[Files（ファイル）] ページで [File Catalog（ファイル カタログ）] タブをクリックすると、ネットワーク上の Bit9 エージェントで制御されているコンピューターで見つかった、すべての一意なファイル（同じファイルの各インスタンスではなく）が示されます（変更されていない場合）。同じページの別のタブ [Files on Computer（コンピューター上のファイル）] では、お使いのコンピューターで見つかった追跡対象ファイルのすべてのインスタンスが示されます。場合によっては、同じページでもタブを切り替えることで別のアクションが利用可能になることがあります。

テーブルの長さ

テーブル ページの最下部には、テーブル内のアイテムの総数と、テーブルのページ数が表示されます。ここには、テーブルのページ間を移動するためのページ ナビゲーション ボタンと、1 ページあたりの行数を変更するためのメニューも用意されています。



極端に大きなテーブルを要求すると、テーブルのアイテム総数（現在表示されているページだけでなく、すべてのページに含まれるアイテムの数）の概数が、たとえば「More than 10000 items（10000 アイテム以上）」と示され、テーブルの最初のページが表示されます。これによって Bit9 コンソールによるページの読み込み時間を節約できるとともに、扱いやすいサイズのデータ セットを含むテーブルを要求することを考慮する機会が得られます。［Group By（グループ別）］の選択項目を変更したり、別の列でソートするなど、ビューの変更を考慮してください。

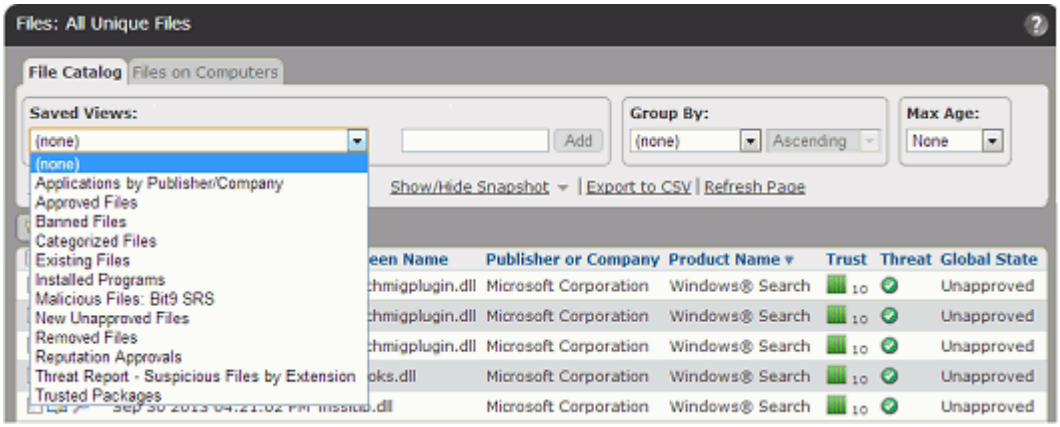
通常は発生しませんが、Bit9 エージェントが大量に存在する場合やデータベース サーバーの処理能力が低い場合などに、膨大な数のデータを含むテーブルを要求すると、Bit9 Server がタイムアウトする可能性があります。これまでに説明した手法を使って、データ セットのサイズを小さくしてください。

デフォルト ビューと保存済みビュー

ページとタブにはそれぞれデフォルト ビューがあります。これはフィルターが適用されていない状態であり、関心の対象になることが最も多いと考えられるデータ列が表示されます。意図したとおりのビューを表示するには、いくつかのテーブル パラメーターを変更します。ページを表示するたびにそのような変更を加えなくて済むように、Bit9 コンソールのほとんどのページでは、ビューに名前を付けて保存することができます。ビューに名前を付けると、［Saved Views（保存済みビュー）］メニューから選択するだけで、再度そのビューを表示できます。［Saved View（保存済みビュー）］メニューで「(none)（(なし)）」を選択すると、ページはシステムのデフォルト ビューにリセットされます。

読み取り専用アカウントでは、新しい保存済みビューを作成することはできません。事前構成された、または他のユーザーが作成した保存済みビューにアクセスできるだけです。

ほとんどの Bit9 コンソール ページには、「(none)（(なし)）」以外に事前構成された保存済みビューが用意されています。事前構成されたビューは変更できませんが、それをテンプレートとして使用して独自の新しい保存済みビューを作成できます。

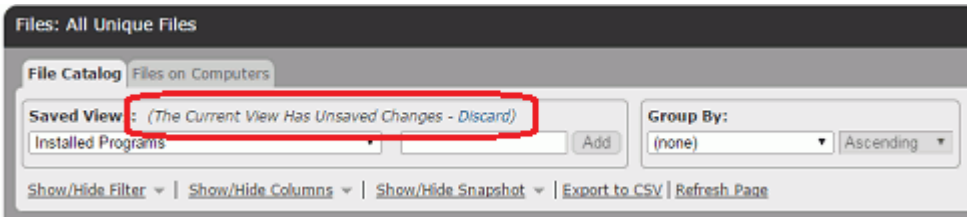


事前構成された保存済みビューの表示手順：

1. 表示するページとタブ（指定する場合）に移動します。
2. ［Saved View（保存済みビュー）］パネルで、［Saved Views（保存済みビュー）］メニューからビューを選択します。マウス ボタンを放すとすぐにビューが表示されます。

選択したビューに応じて、テーブルに表示される列が異なる、またはフィルターに一致する情報だけ（たとえば、ステータスが「禁止」であるファイルだけ）が表示される可能性があります。

［(none)（(なし)）］を含むすべてのビューで、フィルターと列コントロールを使用して、または期間、ページあたりの最大アイテム数、グループを設定できるページ上のさまざまな手段によって、独自の変更を加えることができます。ビューを最初の形式から変更すると、変更を保存するかビューを別の保存済みビューにリセットするまで、未保存の変更があることが［Saved Views（保存済みビュー）］パネルに示されます。システムによって提供されるビューに対する変更は、別の名前で保存する必要があります。



Bit9 コンソール テーブルのビューの変更および保存手順：

1. 表示するページとタブ（指定する場合）に移動します。
2. 既存のビューをテンプレートとして使用して開始する場合は、［Saved Views（保存済みビュー）］メニューからそのビューを選択します。
3. ［**Show/Hide Columns**（列の表示 / 非表示）］を使用して、目的の列を表示します。
4. ［**Show/Hide Filter**（フィルターの表示 / 非表示）］を使用して、テーブルに含める、またはテーブルから除外するアイテムを決定します。

5. 特定の日付または時刻よりも新しいアイテムだけを表示するには、[Maximum Age（最長期間）] メニューを使用します（[Filters（フィルター）] メニューを使用して、さらに複雑な日付 / 時刻フィルターを作成することもできます）。
6. アイテムの一覧表示をアイテム名ではなくグループ名によって行うには、[Group By（グループ別）] メニューで [Group（グループ）] を選択し、表示の順番として [Ascending（昇順）] または [Descending（降順）] を選択します。たとえば、公開者によってグループ化する場合は [Publisher（公開者）] を選択します。初期状態では、テーブルにはグループが表示されていますが、グループ名をクリックすると展開されて、そのグループに含まれる個別のアイテムが表示されます。
7. ファイルのテーブルが表示されるページで、インストール ファイルの名前だけでなく、インストーラーによってインストールされた個々のファイルを確認するには、ページの右下にある [Show individual files（個別のファイルを表示）] チェック ボックスをオンにします。
8. ページに表示する行数を減らす場合は、ページ右下の [rows per page（ページあたりの行数）] メニューで現在と異なる数値を選択します。この行の右側のメニューで [page（ページ）] を選択すると、変更は現在のページ（たとえば、[Computers（コンピューター）] ページ）に対してのみ有効になります。この行の右側のメニューで [all pages（すべてのページ）] を選択すると、変更はコンソールのページのうち、長さを指定していないすべてのページに対して有効になります。
9. 意図したとおりのビューが表示されたら、そのビューを表す名前を [Saved View（保存済みビュー）] パネルの右側のボックスに入力し、[**Add**（追加）] ボタンをクリックします。これで新しいビューが保存され、[Saved Views（保存済みビュー）] メニューから利用できるようになります。

保存済みビューを作成しなくても、Bit9 コンソールではページごとに最新のビュー（フィルターと列の選択）が記憶されるため、ページから離れた後で戻ってくると、別のビューを選択するまで最新のビューで表示されます。ただし、別のビューを選択すると、現在のビューへの変更はすべて失われます。

必要に応じてユーザー設定を使用して、ページの最新の表示状態を記憶せず、ページから離れるとBit9コンソールのデフォルト ビューにリセットされるように設定することもできます。詳細については、「コンソール ユーザーの設定」（83 ページ）を参照してください。また、変更を記憶するように設定してある場合でも、ページに対する特定のアクセスで行った変更が記憶されないようにするには、未保存の変更に関するメッセージの隣にある [**Discard**（破棄）] リンクをクリックします。これにより、ビューは保存済みの形式に戻ります。

ファイルへの Bit9 Server データのエクスポート

Bit9 コンソールのファイル エクスポート ツールを使用すると、データをコンマ区切り形式でダウンロードできます。ダウンロードされたデータは、オンライン表示に関する現在の列とフィルターの設定に従って表示されます。

ファイルを Windows システムにダウンロードすると、拡張子は .CSV になります。Safari ブラウザーを使用している Mac システムでは、ダウンロードしたファイルは標準的な CSV 形式ですが、拡張子は .CSV.XLS になります。

テーブル データからファイルへのダウンロード手順：

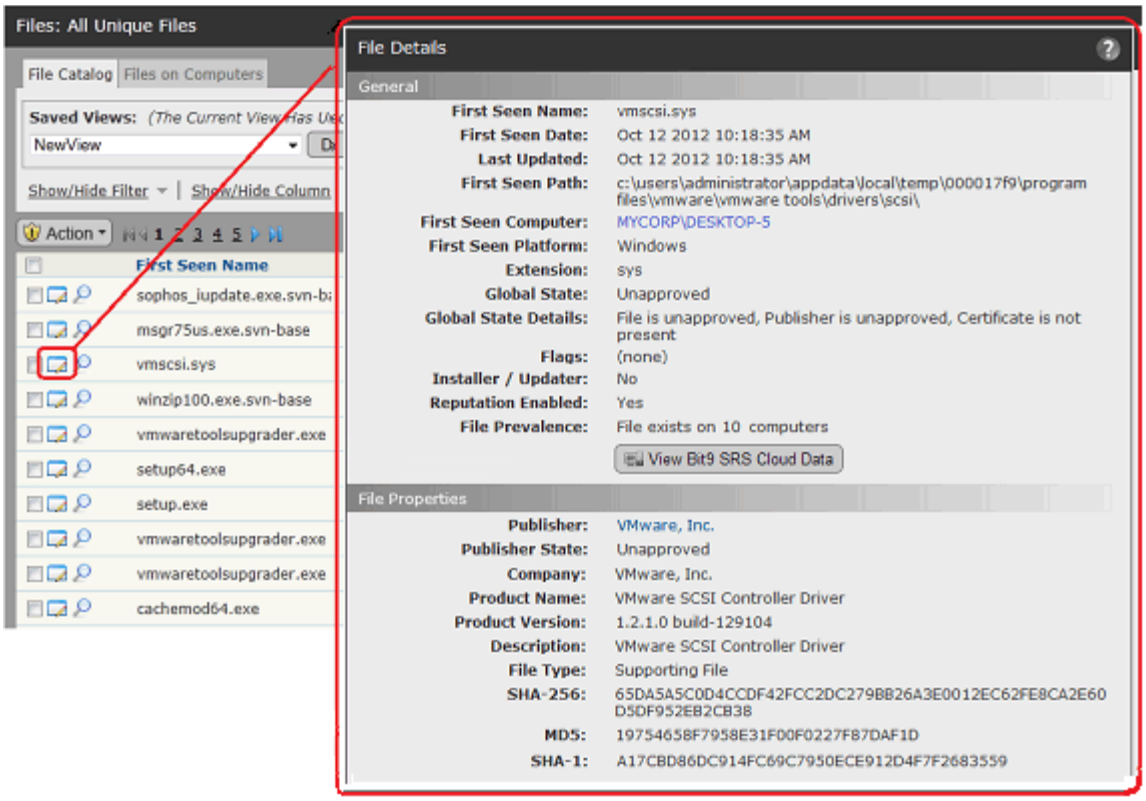
1. ［**Export to CSV**（CSV へのエクスポート）］をクリックします。お使いのブラウザーの標準ダウンロード ダイアログ ボックスが表示されます。
2. ダイアログ ボックスに表示される指示に従って、ファイルをダウンロードします。
   a. ファイルを選択して開くか、ディスクに保存します。
   b. ディスクに保存する場合は、場所を選択し、オプションでファイル名を変更します。

詳細ページとオブジェクト プレビュー

Bit9 コンソールの多くのテーブルでは、［View Details（詳細の表示）］ボタン、またはテーブル内でオブジェクトの名前（青でハイライト表示されている場合）をクリックすることで、行のアイテムの詳細を取得できます。詳細ページには、以下のページがあります。

- ［File Details（ファイルの詳細）］ページ
- ［Computer Details（コンピューターの詳細）］ページ
- ［Publisher Details（公開者の詳細）］ページ
- ［Certificate Details（証明書の詳細）］ページ
- ［Device Details（デバイスの詳細）］ページ
- ［External Notification Details（外部通知の詳細）］ページ
- ［Indicator Set Details（痕跡セットの詳細）］ページ
- ［Approval Request Details（承認要求の詳細）］ページ

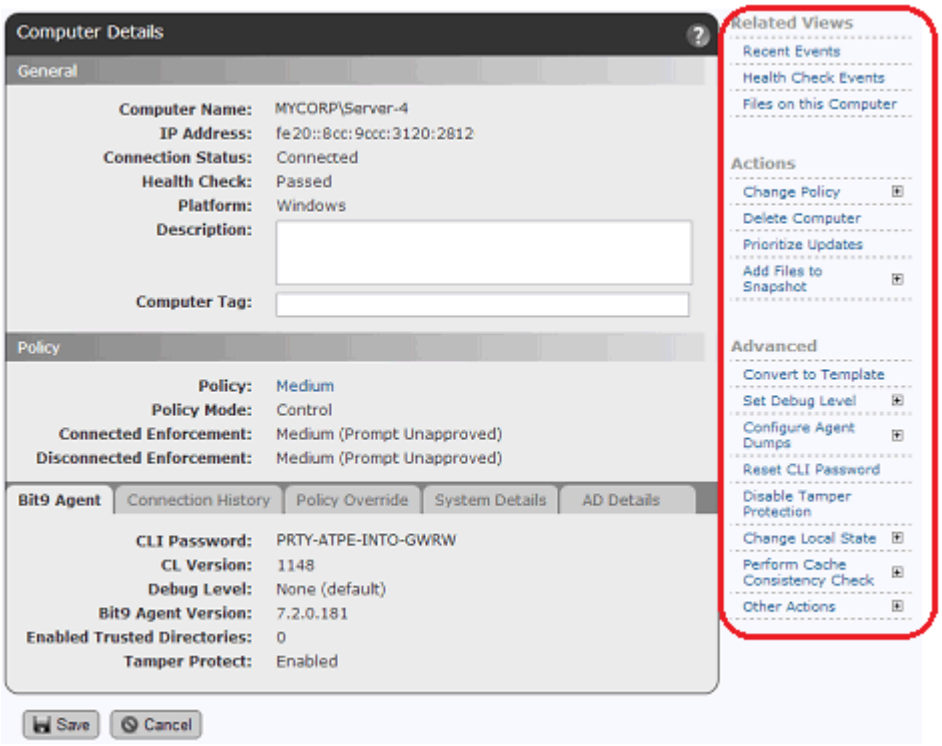
たとえば、ファイル カタログでファイル名の隣の詳細ボタンをクリックすると、［File Details（ファイルの詳細）］ページが表示され、ファイルの詳細情報が示されます。Bit9 コンソールで得られるファイルの詳細については、第 7 章「ファイル情報と公開者情報」を参照してください。



詳細ページのメニュー

Bit9 コンソールの一部のページでは、主要コンテンツの右側にメニューがあります。このメニューには、以下のセクションの 1 つまたは複数が含まれている可能性があります。

- ［**Related Views**（関連ビュー）］セクションのリンクからは、現在のページに関係するページに移動できます。たとえば、［Computer Details（コンピューターの詳細）］ページには、そのコンピューターで追跡されているすべてのファイルを示すテーブルへのリンクがあります。
- ［**Actions**（アクション）］セクションのコマンドでは、ページの内容に関係するアクションを実行できます。たとえば、［File Instance Details（ファイル インスタンスの詳細）］ページには、現在のファイルを禁止または承認するコマンドがあります。
- ［**Advanced**（詳細）］セクションのコマンドは、あまり一般的ではなく、正しく使用するためには Bit9 サポートに相談していただく必要があります。たとえば、［Computer Details（コンピューターの詳細）］ページには、現在の Bit9 エージェントを管理するために使用するパスワードをリセットするコマンドがあります。
- ［**External Pages**（外部ページ）］セクションのリンクは、他の製品がサーバーと統合され、Bit9 コンソールからその情報に直接リンクできるように構成されている場合に表示されます。たとえば、条件によっては［Computer Analytics（コンピューターの分析）］リンクから Splunk コンソールに移動できます。



テーブル データのオブジェクト プレビュー

これまでのセクションで説明したように、詳細ページには Bit9 データベースに登録されているオブジェクトに関する大量の情報が表示され、詳細ページにアクセスする方法の 1 つは、テーブルでハイライト表示されている情報をクリックすることです。場合によっては、ハイライト表示されているオブジェクトの名前以外の情報が必要で、しかし詳細ページで提供されるすべての情報は不要であるという状況が考えられます。オブジェクト プレビューを使用すると、現在のページから移動することなく、ハイライト表示されている多くのオブジェクトのサマリー情報を確認できます。

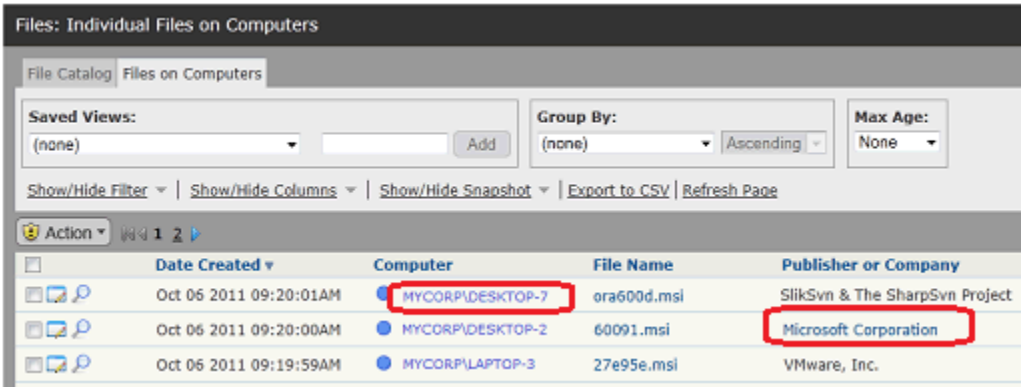
オブジェクト プレビューを表示するには、ハイライト表示されているアイテムの上にマウス カーソルを置き、クリックはしません。たとえば、ここに示したのは、[Events（イベント）] ページでファイル名の上にカーソルを置いたときの [File Instance（ファイル インスタンス）] プレビューです。

テーブル内の次のアイテムには、オブジェクト プレビューがあります（ハイライト表示されている場合）。

- カタログ内のファイル
- ファイル インスタンス
- 証明書
- コンピューター
- デバイス
- 公開者
- ポリシー

ショートカット リンク

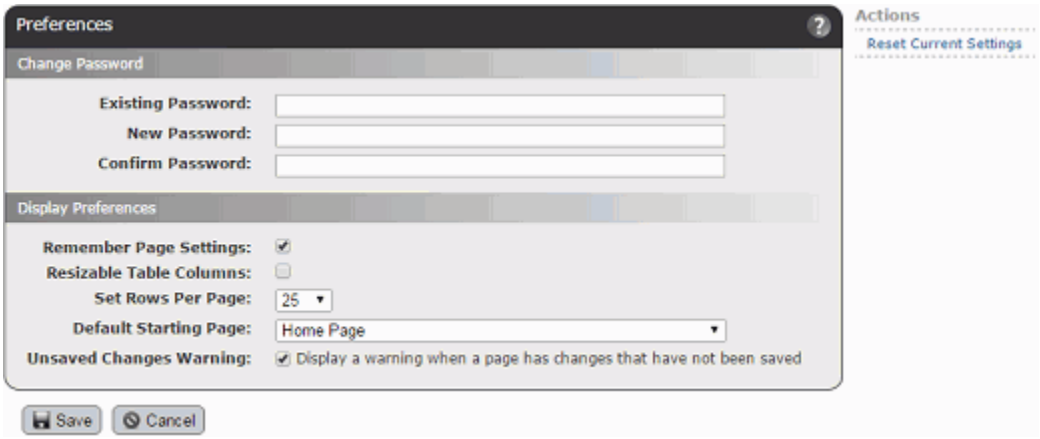
Bit9 コンソールの多くのページには、青色でハイライト表示されたショートカット リンクがあり、それを使用して、現在のページに関係する情報を示すページに移動できます。たとえば、[Computers（コンピューター）] ページでコンピューター名をクリックすると、そのシステムの［Computer Details（コンピューターの詳細）］ページに移動します。また、ポリシー名をクリックすると、[Edit Policy（ポリシーの編集）] ページに移動します。



一部のページでは、別のページで複雑なクエリを作成することなく情報を簡単に検索できる手段として、リンクを使用できます。たとえば、[Edit Policy（ポリシーの編集）] ページには、ポリシーに含まれるすべてのコンピューターを示すリンクがあります。

コンソール ユーザーの設定

［Preferences（設定）］ページでは、Bit9 コンソールのユーザーが各自のパスワード、ログインしたときに最初に表示されるページ、およびページを離れてから戻ってきたときにページ ビューへの変更が維持されているかどうかを変更できます。［Preferences（設定）］ページを表示するには、メイン メニューで［**Tools**（ツール）］>［**Preferences**（設定）］を選択します。



［Preferences（設定）］ページでの変更は、現在ログインしている Bit9 コンソール ユーザーに適用され、読み取り専用アクセスのユーザーも含めすべてのユーザーが指定できます。このページで指定する変更の効果を表 6 に示します。

表 6：ユーザー アカウントの設定ページでの選択項目

パネル：フィールド	説明
Change Password（パスワードの変更）	現在のユーザーが、Bit9 コンソールで作成したアカウントの新しいコンソール ログイン パスワードを入力できます。Active Directory から作成したアカウントに対しては使用できません。
Display Preferences（表示設定）：Remember Page Settings（ページ設定の記憶）	現在のユーザーが、ページ設定が（セッション内で、およびセッション間で）保存されるかどうかを選択できます。この設定は、現在のユーザーが表示する Bit9 コンソールのすべてのページに適用されます。 オンにした場合、フィルター、列、およびグループ化の設定を含むすべてのページ設定は、ページから離れた（またはログアウトした）後に戻ってくると記憶されています。 オフにした場合、ページを離れるとページは Bit9 コンソールのデフォルトに戻り、適用した特殊なレイアウトは失われます。 ［Action（アクション）］メニューの［**Reset Current Settings**（現在の設定をリセット）］を使用すると、このチェック ボックスをオフにすることなくデフォルトに戻すことができます。
Display Preferences（表示設定）：Resizable Table Columns（テーブル列のサイズ変更）	現在のユーザーが、Bit9 コンソール テーブルに対して、サイズ変更可能なテーブル列を有効または無効にできます。デフォルトで有効化されています。詳細については、「テーブル列のサイズ変更」（69 ページ）を参照してください。

パネル：フィールド	説明
Display Preferences（表示設定）：Set Rows per Page（ページあたりの行数の設定）	現在のユーザーが、情報のテーブルが表示されるページでの標準のページあたり行数を設定できます。これを変更すると、Bit9 コンソールのすべてのテーブル ページで行数が再設定されます。ただし、全体の設定の後で、各ユーザーはページごとにページあたり行数をカスタマイズできます。デフォルト設定は 25 です。
Display Preferences（表示設定）：Default Starting Page（デフォルトの開始ページ）	現在のユーザーが、ログイン時に最初に表示される Bit9 コンソール ページを（メニューから）選択できます。以下の選択肢があります。 • ホーム ページ • [Events（イベント）] ページ • [Computers（コンピューター）] ページ • [File Catalog（ファイル カタログ）] ページ • [Policies（ポリシー）] ページ • [Find Files（ファイルの検索）] ページ • [Approval Requests（承認要求）] ページ
Display Preferences（表示設定）：Unsaved Changes Warning（未保存の変更の警告）	これをオンにした場合、このユーザーが変更を保存しないままページから離れようとすると、警告ダイアログが表示されます。このダイアログで、希望どおりにページを離れるか、移動をキャンセルして現在のページにとどまるかを選択できます。これをオフにした場合、このユーザーが変更を保存しないままページから移動しようとしても、警告ダイアログは表示されません。
[Save（保存）] / [Cancel（キャンセル）] ボタン	**[Save（保存）]** は、ユーザーの設定の変更を保存します。**[Cancel（キャンセル）]** は、変更を保存せずに、前に表示していたページに戻ります。

状況依存のヘルプの使用

Bit9 コンソールには状況依存のヘルプ システムが組み込まれており、現在のビューに適した情報が提供されますが、そこから他のトピックに移動することもできます。[Help（ヘルプ）] リンクまたはボタンをクリックすると、現在のブラウザーの新しいタブ、または新しいポップアップ ブラウザーに、新しい [Help（ヘルプ）] ウィンドウが開きます。タブとして表示された場合は、現在のブラウザーからそのタブをドラッグして、独立したウィンドウにヘルプを表示できます。

Microsoft Internet Explorer では、ポップアップ ブロックが有効化されている可能性があります。その場合、ヘルプをポップアップとして表示するには、Bit9 Server からのポップアップ表示を許可する必要があります。また、初めてヘルプを表示するときには証明書エラーが表示される可能性があります。証明書の受け入れについては、「ログイン」（54 ページ）を参照してください。

Bit9 コンソールからオンライン ドキュメントを表示するには、次の手順を実行します。

1. 次のいずれかの方法で［Help（ヘルプ）］を起動します。
   - メイン メニューの［**Help**（ヘルプ）］をクリックして、Bit9 Security Platform ヘルプの目次を開きます。
   - すべてのページにあるヘルプ（疑問符）ボタンをクリックして、そのページのトピックを表示します。
2. ヘルプが表示されたら、目次の中で本のアイコンかその隣の名前をクリックすると、目次のツリーが展開されて詳しいトピックが表示されます。
3. アルファベット順のトピック リストを表示するには、［**Index**（索引）］ボタンをクリックします。
4. キーワードを検索するには、左側の［Help（ヘルプ）］フレームで［Search（検索）］ボタンをクリックし、検索するキーワードを［**Search**（検索）］ダイアログに入力します。

注意

- ［Help（ヘルプ）］タブまたはブラウザーを閉じるまで、要求したヘルプ トピックは同じウィンドウに表示されたままです。ただし、Internet Explorer と Firefox ではセキュリティ機能として、新しいトピックを読み込んでも、開いているヘルプ ウィンドウは前面に表示されません。タブをクリックするか、**Alt + Tab** キー などのデスクトップ ナビゲーション ツールを使用して、ヘルプを前面に表示してください。
- Chrome ではナビゲーションの問題があり、状況依存のヘルプ ページは、要求したトピックの見出しの「直下」（たとえば、トピックの最初の段落）にコンテンツが表示されます。正しいトピックが表示されているかどうかを確認するには、見出しまでスクロールアップします。

第 3 章

コンソール ログイン アカウントの管理

この章では、Bit9 コンソールへのアクセスと特定の機能への権限を管理する方法について説明します。

セクション

ログイン アカウントの管理

Bit9 コンソールの各ユーザーは、ユーザー名とパスワードを使用してシステムにログインする必要があります。ログイン アカウントにより、システム管理の担当者や Bit9 コンソールを使用する他のユーザーは、Bit9 の機能を利用、管理したり、Bit9 エージェントが実行されているコンピューターを管理または監視することができます。

Bit9 コンソールには、組み込みのログイン アカウントが 1 つ用意されています。これは admin というアカウントで、コンソールへの初期ログインに使用され、削除できません。デフォルトでは、このアカウントにはすべての要素に対して、File Uploads（ファイルのアップロード）を除くすべての管理者権限があります。

admin としてログインした直後に実行する必要があることは、パスワード（同じく admin）の変更です。「アカウントのパスワードおよびその他の詳細の変更」（99 ページ）を参照してください。

追加の Bit9 コンソール アカウントを作成するには、次の 2 つの方法があります。

- コンソールでアカウントを作成します。この方法で作成したアカウントはコンソールから管理でき、適切な権限を持つログイン アカウントを持つユーザーが削除できます。
- ユーザーが特定の「マップ済み」グループに属している場合は、Active Directory 認証情報を使用してログインすることをそのユーザーに許可できます。AD ベースの Bit9 コンソール ログインは「外部アカウント」として表示され、アカウントの詳細は AD でのみ変更でき、Bit9 コンソールでは変更できません。セキュリティのベスト プラクティスを必要とする環境の場合、Bit9 は AD ベースのアカウントを使用することを推奨しています。

AD ベースのログイン アカウントとコンソールで作成したログイン アカウントの両方を混在させることはできますが、新しいアカウントの作成を開始する前に、優先するアカウント管理戦略を検討する必要があります。Bit9 コンソールのすべてのアカウントを AD ベースか Bit9 コンソールのどちらか 1 つの同じ方法で生成する方が、混乱を避けることができます。そうしない場合、文字どおりの意味でのアカウント名の重複は発生しませんが、たとえば、コンソールで作成したアカウント名「fred」と、AD ベースのアカウント「fred@somedomain」が存在可能です。

アカウント グループとアクセス権限

ユーザーの権限は、ユーザーが属している「ログイン アカウント グループ」によって決まります。ユーザーのアカウント グループは［Add Login Account（ログイン アカウントを追加）］ページで設定し、［Edit Login Account（ログイン アカウントを編集）］ページで変更できます。組み込みアカウント グループのデフォルトの権限を表 7 に示します。

表 7：組み込みのログイン アカウント グループとデフォルトの機能

ログイン アカウント グループ	機能のまとめ
Administrator（管理者）	ファイルのアップロード、API によるコネクタの拡張、プロセス コマンド ラインの表示を除く、Bit9 コンソールのすべての機能への完全なアクセス。自身も含むすべてのユーザーに対して、権限の追加、削除ができます。
PowerUser（パワーユーザー）	以下の点を除く、すべての機能へのアクセス： • 自身のログイン アカウントは編集できますが、他のユーザーのログイン アカウント、またはいずれかのアカウント グループを作成、編集、削除することはできません。 • [System Configuration（システム構成）] ページでの変更、[File Upload（ファイルのアップロード）] 機能へのアクセス、分析のためのファイルの送信はできません。
ReadOnly（読み取り専用）	• Bit9 コンソールのテーブル、レポート、詳細ページで、ビュー、ルール、設定を表示することはできますが、作成や変更はできません。 • 独自のダッシュボードを作成することはできますが、既存のポートレットを使用する必要があります。編集または削除できるアセットは、それだけです。 • 自分のパスワードおよびページ ビューのデフォルトを [Preferences（設定）] インターフェイスから変更できます。 • [Computer Details（コンピューターの詳細）] ページの [Advanced Options（高度なオプション）] にはアクセスできません。 • [Approval Request（承認要求）]、[Login Account（ログイン アカウント）]、[System Configuration（システム構成）] の各ページなど、管理者ページにはアクセスできません。
Unauthorized（未承認）	Bit9 コンソールにアクセスできません。

組み込みのアカウント グループは削除できませんが、Administrator、PowerUser、ReadOnly の各グループの権限を編集して、アクセス機能を有効または無効にすることができます。また、管理者はカスタムの権限（新しいアカウントとグループを作成する機能を含めて）を持つ新しいアカウント グループを作成できます。アカウント グループの作成とアカウント権限のカスタマイズの手順については、「コンソール アカウント グループの管理」（104 ページ）を参照してください。

AD アカウントを通じたコンソール アクセスの有効化

Active Directory を使用していて、Bit9 Server が Active Directory ドメインに参加している場合、AD アカウントを使って Bit9 コンソールにログインできます。デフォルトでは、Active Directory アカウントは 3 種類の AD セキュリティ グループのいずれかから、表 8 に示すように Bit9 コンソール アカウント グループにマップされます。この表には、それ以外の AD グループがどのようにマップされるかも示されています。

表 8 : AD グループから Bit9 コンソール アカウント グループへのデフォルトのマッピング

Active Directory のセキュリティ グループ	Bit9 コンソール アカウント グループ
cn = "Bit9 Administrators"	Administrator
cn = "Bit9 Power Users"	PowerUser
cn = "Bit9 ReadOnly Users"	ReadOnly
cn =（任意の AD グループを選択）	（対応するカスタム Bit9 アカウント グループ）
（マップされていないグループの名前）	Unauthorized

ユーザーが AD ベースのアカウントで Bit9 コンソールにログインすると、そのアカウントは Bit9 コンソール アカウントとして追加されます。有効な AD アカウントを持ち、マップ済みグループ（Administrators、Power Users、Read Only、またはカスタム グループ）のメンバーではないユーザーが Bit9 コンソールへのログインを試みると、Bit9 コンソール アカウント テーブルには追加されますが、そのアカウントは Unauthorized とされます。そのため、Bit9 コンソールにはログインできません。

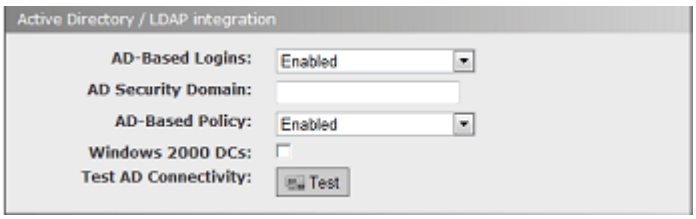
Bit9 に関連する AD セキュリティ グループへの AD アカウントの割り当ては、1 つに限定することをお勧めします。ただし、AD グループは間接的に割り当てることができるため、意図しないまま 1 つの AD アカウントを複数の Bit9 セキュリティ グループに割り当ててしまうことも考えられます。その場合は、Bit9 コンソール エージェント グループのうちランキング リストの中で最上位（番号が最小）のものによって、アカウントの Bit9 Server アクセス権が決まります。詳細については、「コンソール アカウント グループの管理」（104 ページ）を参照してください。

注意

- マップされた標準的な Active Directory グループ名を使用できない、またはしない場合は、別の AD グループをいずれかの Bit9 コンソール アカウント グループにマップすることが考えられます。詳細については、「コンソール アカウント グループの管理」（104 ページ）を参照してください。
- Windows 2000 ドメイン コントローラーを使用している場合を除き、ユーザー アカウントのログイン ドメインとは無関係にセキュリティ ドメインを指定できます。これにより、各ユーザーのドメインではなく指定したセキュリティ ドメイン内に、Bit9 アカウント グループを作成できます。

Bit9 コンソールで AD ログインを有効化する手順：

1. Bit9 コンソール アクセスを許可しようとしている各 AD ユーザー アカウントについて、マップ済み AD セキュリティ グループに割り当ててあることを確認します。
2. admin、または作成済みの他の管理者アカウントでBit9コンソールにログインします。
3. Bit9 コンソール メニューで、[**Administration**（管理）] > [**System Configuration**（システム構成）] の順に選択します。[System Configuration（システム構成）] ページが開きます。
4. [システム構成] ページで [**General**（全般）] タブをクリックします。初期状態では、このページの設定は灰色で表示されます。



5. [Active Directory/LDAP integration（Active Directory/LDAP 統合）] ウィンドウを確認します。既に [AD-Based Logins（AD ベースのログイン）] が [Enabled（有効）] と表示されている場合、変更は一切不要で、残りの手順は省略できます。
6. [AD-Based Logins（AD ベースのログイン）] が [Disabled（無効）] の場合は、ページの下部にある [**Edit**（編集）] ボタンをクリックして設定を編集可能にします。
7. [AD-Based Logins（AD ベースのログイン）] のドロップダウン メニューで、[**Enabled**（有効）] を選択します。
8. Windows 2000 ドメイン コントローラーを使用している場合は、[Windows 2000 DCs (Windows 2000 DC)] チェック ボックスをオンにします。これによって、クロスドメイン メンバーシップ機能が使用できないことを Bit9 Server に伝えます。
9. Bit9 コンソールにログインするユーザーのために、ログイン ドメイン以外のドメインに Bit9 用の AD セキュリティ グループを作成した場合は、そのドメインを [AD Security Domain（AD セキュリティ ドメイン）] フィールドに入力します（この機能は、Windows 2000 ドメイン コントローラーを使用している場合は使用できません）。
10. [Update（更新）] ボタンをクリックし、[Confirmation（確認）] ダイアログが表示されたら [Yes（はい）] をクリックします。これで、Active Directory ログイン アカウントを使用して（マップ済みグループの 1 つに属していれば）Bit9 コンソールにアクセスすることができます。

AD ベースのログインの使用を無効化するには、同じ手順に従いますが、[AD-Based Logins（AD ベースのログイン）] 設定で [Disabled（無効）] を選択します。

AD ベースのログインを無効化すると、ユーザーは自分の AD アカウント名とパスワードを使用して Bit9 コンソールにアクセスできなくなります。

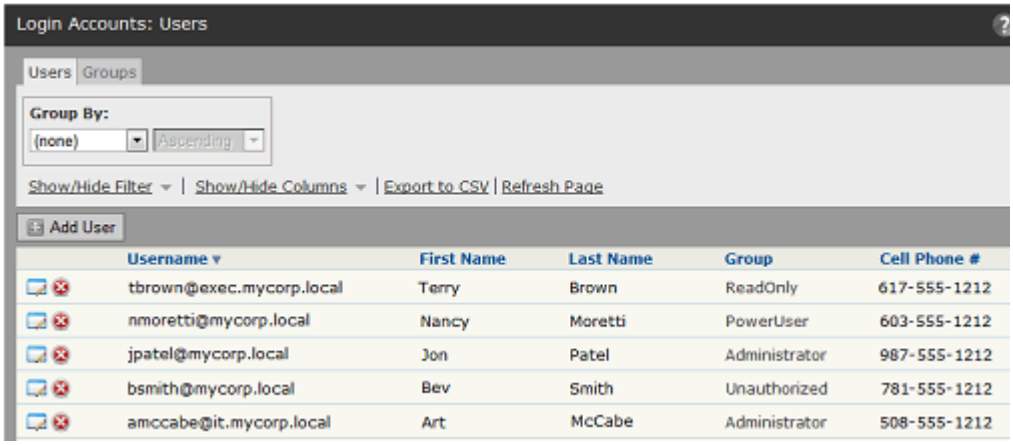
AD ログイン アカウントの形式

Bit9 コンソールにログインする Active Directory アカウント名の形式は、そのアカウント名が Bit9 Server と同じドメインのものか別のドメインのものかによって決まります。

- AD　　アカウントが別のドメインのものである場合は、完全修飾された名前（`NTDOMAIN\Username` または `Username@dnsDomain` の形式）にする必要があります。
- Bit9 Server と同じドメイン内の AD アカウントは、完全修飾されたユーザー名とユーザー名のみのどちらでも（ユーザー名が Bit9 コンソールを使用して直接作成したログイン アカウントと同じでない限り）ログインできます。

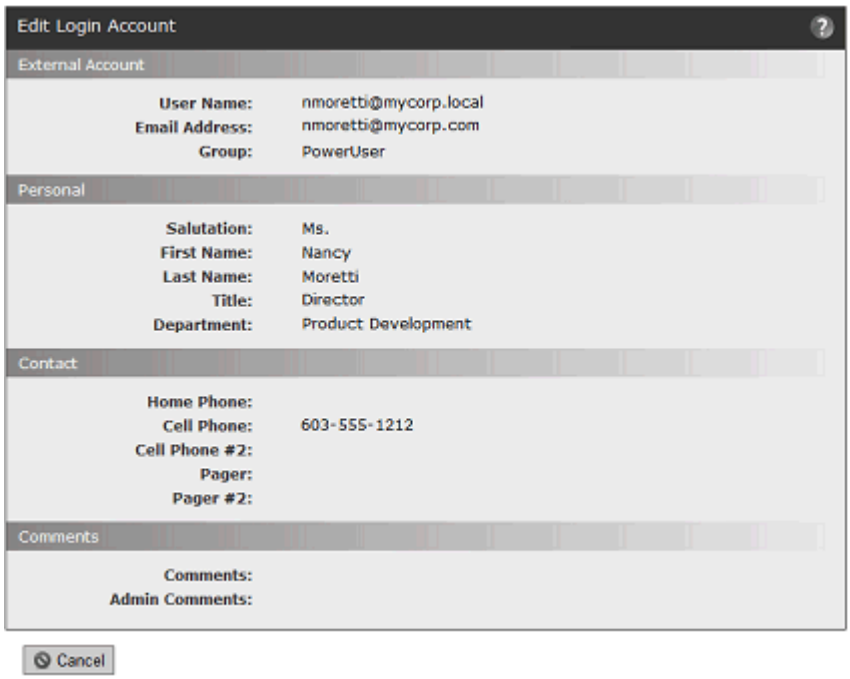
AD ベースのアカウントとコンソールで作成されたアカウントの間には、いくつかの細かい違いがあります。

- ADベースのアカウントを持っているユーザーがBit9コンソールにログインすると、［Login Accounts（ログイン アカウント）］ページと［User Details（ユーザーの詳細）］ページに表示されるユーザー名は、ユーザーとドメインの両方の名前が「`user@dnsDomain`」という形式で表示されます。



- ［View Details（詳細の表示）］ボタンをクリックして［User Details（ユーザーの詳細）］ページを開くと、詳細パネルの一番上のボックスには、AD ユーザー

に対して［External Account（外部アカウント）］というラベルが付けられています。



- このアカウントの詳細を　Bit9　コンソールで編集することはできないため、［Login Account Details（ログイン アカウントの詳細）］ページに［Save（保存）］ボタンはありません。

AD ログイン アカウントの追加、削除、変更

Bit9 Server には、コンソールにログインした AD アカウントのユーザー情報が保管されますが、ログインが試行されるたびに、その情報が正しいかどうか検証されます。ユーザーがコンソールにログインしている間に AD アカウントに対して行われた変更は、そのユーザーがログアウトして再度ログインするまで反映されません。また、アカウントの更新は、ネットワーク上の AD ドメイン コントローラーが変更を送信する頻度に依存します。AD アカウントの変更のうち、Bit9 コンソール ログイン アカウントに影響するものは、次のとおりです。

- AD に追加されたユーザー アカウントは、セキュリティ グループおよびフォレストの基準を満たしていればBit9コンソール ログイン アカウントとして使用可能になります。
- AD から削除されたユーザー アカウントは､Bit9 コンソールにはログインできません。
- ADベースのユーザー セキュリティ グループの割り当てをADで変更すると、Bit9 コンソールでのユーザーのアクセス レベルは次回のログイン時から変更されます。
- AD ベースのユーザーの Bit9 コンソールにおけるユーザー詳細（連絡先情報など）は、AD で変更でき、そのユーザーが次にコンソールにログインしたときに反映されます。

注意

- AD ベースのログイン機能はすべて、Bit9 Server が AD システムと通信できることと、ドメインに存在していることが前提です。何らかの理由（ネットワーク設定の変更、ネットワーク障害、AD システムが利用できないなど）で Bit9 Server が AD システムと通信できなくなると、AD ベースのログインは、その状態が修正されるまで機能しなくなります。
- また、AD ベースのログイン機能には、Bit9 Server にアクセスするユーザーが存在する各フォレストでADセキュリティ グループが定義されていることと、Bit9 Server へのアクセスを許可するユーザーがフォレスト固有のセキュリティ グループに追加されていることも要件です。

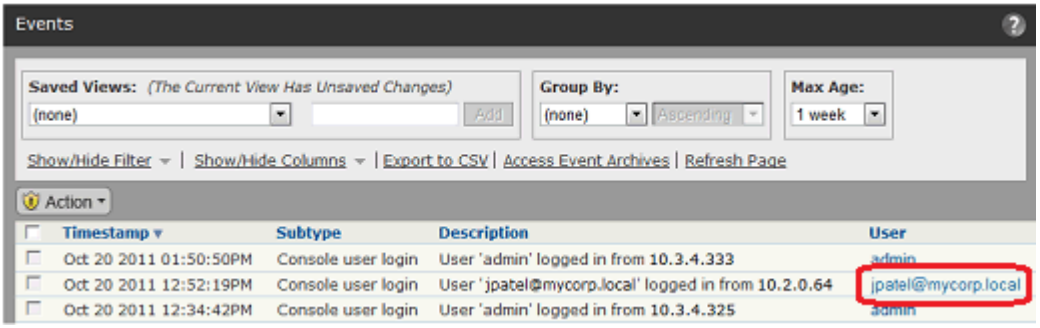
AD グループのマッピングおよびランクの変更

AD マッピングを有効にしてある場合、AD セキュリティ グループから Bit9 コンソール ログイン グループへのマッピングは、各ログイン グループの［Group Details（グループの詳細）］ページで指定します。AD マッピングは、組み込みのグループも含めてすべてのログイン グループに関して変更できます。詳細については、「ログイン アカウント グループの編集」（113 ページ）を参照してください。

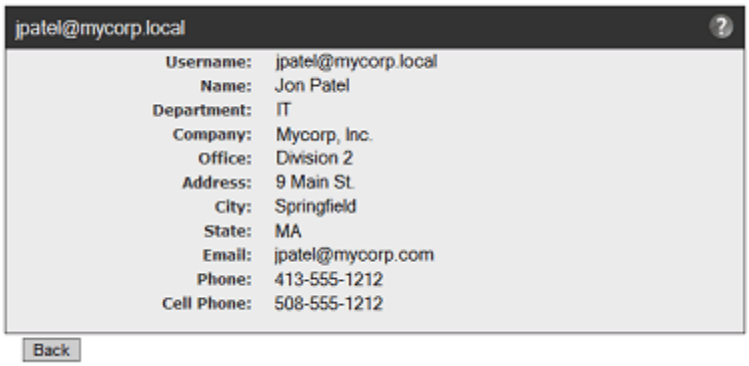
原則として、AD アカウントは 1 つのログイン アカウント グループのマッピング ルールにのみ一致する必要があります。しかし、複数の一致が発生した場合、マッピング ルールは［Login Accounts: Groups（ログイン アカウント : グループ）］ページに基づいてランクが指定されます。AD マッピング ルールのランクを変更することで、優先させるルールに他のルールよりも高いランクを与えることができます。詳細については、「グループの AD マッピングおよびランクの変更」（104 ページ）を参照してください。

Bit9 コンソールに表示される AD ユーザーの詳細の変更

AD ユーザー アカウントが Bit9 コンソールのテーブルに表示されているときは（[Login Accounts（ログイン アカウント）] ページを除き）、AD ユーザーが Bit9 コンソール ログイン アカウントを持っているかどうかに関係なく、そのユーザー名をクリックして追加情報を表示できます。たとえば、[Events（イベント）] ページを表示しているとき、一部のイベントには、そのイベントに関係するユーザーが存在します。



その名前が AD のユーザー名である場合、名前は青色でハイライト表示され、それをクリックすると [User Details（ユーザーの詳細）] ウィンドウが表示されます（これは、[Login Accounts（ログイン アカウント）] ページで名前をクリックしたときに表示される [User Details（ユーザーの詳細）] ページとは異なることに注意してください）。



このページのフィールドは、`UserProps.txt` ファイルを編集することによって変更、追加、または削除できます。このファイルは、Bit9 Server インストール ディレクトリの「Scripts」サブディレクトリ置かれています。たとえば、デフォルトのインストール ディレクトリを受け入れた場合は、`C:\Program Files\Bit9\Parity Server\Scripts` にあります。

このファイルは、2 つの列がコロンで区切られたリストです。Bit9 コンソールのラベル（「Name（名前）」など）が左側に、そのフィールドに表示される AD プロパティが右側に配置されます。このファイルを編集する際、コロンの右側の単語には、必ず実際の AD オブジェクト プロパティを使用してください。

同様のカスタマイズは、Bit9 コンソールでコンピューターに関して表示される AD の詳細についても行うことができます。

Bit9 コンソールでのログイン アカウントの作成

次に示す手順は、Bit9 コンソールでログイン アカウントを作成するためのものです。Bit9 コンソールへのアクセスに既存の Active Directory アカウントを使用する場合は、「AD アカウントを通じたコンソール アクセスの有効化」（89 ページ）を参照してください。

注意

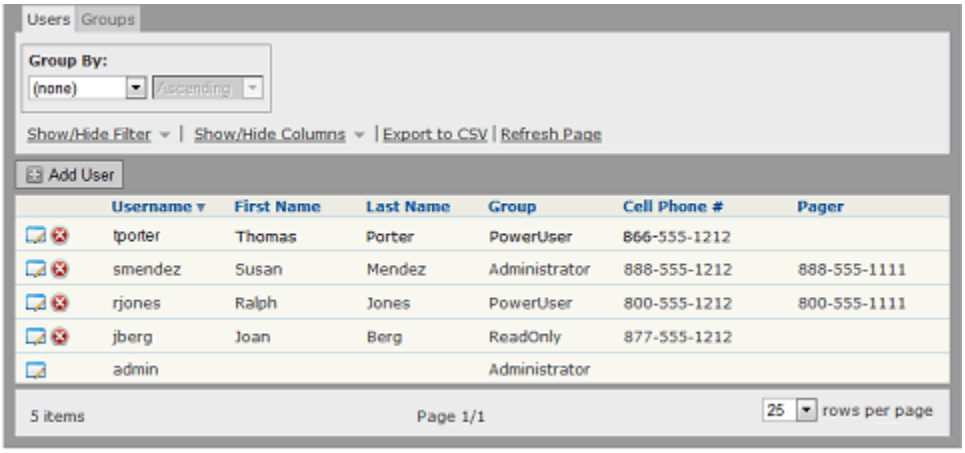
ログイン アカウントは、Bit9 コンソールにアクセスするためのものです。Bit9 関連のロールが、Bit9 エージェントがインストールされているコンピューターのユーザーとしてのロールだけである場合、ログイン アカウントは不要であり、設定することも不適切です。

ログイン アカウントの作成権限は、次のようにアカウント グループによって決まります。

- デフォルトでは、Administrators グループのアカウントはすべてのレベルのアカウントを作成できます。
- デフォルトでは、PowerUsers および ReadOnly グループのアカウントは新しいアカウントを作成できません。
- カスタムのアカウント グループには、[Add/Edit Group（グループの追加 / 編集）] ページの [View login accounts and groups（ログイン アカウントとグループの表示）]、[Manage login accounts（ログイン アカウントの管理）]、および [Manage groups（グループの管理）] 設定に示されるすべてのアカウント作成権限があります。

コンソール ログイン アカウントの作成手順：

1. コンソール メニューから、[**Administration**（管理）] > [**Login Accounts**（ログイン アカウント）] の順に選択します。[Login Accounts（ログイン アカウント）] ページが表示されます。



2. [Login Accounts: Users（ログイン アカウント：ユーザー）] ページが表示されない場合は、[**Users**（ユーザー）] タブをクリックします。

3. ［Login Accounts: Users（ログイン アカウント：ユーザー）］ページで、［**Add User**（ユーザーの追加)］をクリックします。
4. ［Add Login Account（ログイン アカウントを追加)］ページで、新しいアカウントに関する、表 9 に示したカテゴリの情報を入力します。
5. フォームに記入したら、ページの下部にある［**Add User**（ユーザーの追加）］ボタンをクリックします。

表 9：ログイン アカウントの詳細フィールド

フィールド	説明
User Name（ユーザー名） （必須）	Bit9 コンソールにログインするためにユーザーが入力する名前。 文字、数字、または英語キーボード文字の任意の組み合わせを 32 文字未満の長さで入力します。ユーザー名では大文字と小文字は区別されません。 **注意**：ユーザー名に使用できるのは、標準のラテン文字です。記号や句読点は使用できません。特に、Bit9 コンソールで作成するユーザー名には「\」、「@」を使用できないことに注意してください。これは、`user@domain` または `domain\user` という形式を使用している AD ベースのユーザー名と競合するのを避けるためです。禁止されている文字を使用してユーザー アカウントを作成しようとすると、Bit9 コンソールに警告ダイアログが表示されます。
Password（パスワード） （必須）	このユーザーを認証するパスワード。 文字、数字、または英語キーボード文字の任意の組み合わせを 32 文字未満の長さで入力します。パスワードでは大文字と小文字が区別されます。既存のアカウントを編集する際には、このフィールドは［New Password（新しいパスワード)］に変わります。
Confirm password（パスワード確認） （必須）	パスワードの確認です。 パスワードを再入力して、目的のパスワードであることを確認します。
Email address（E メール アドレス）	ユーザーの E メール アドレス。

フィールド	説明
Group（グループ）	このユーザーに対して想定される責任に応じて付与するシステム権限。4 つの組み込みグループが用意されています。また、機能ベースの詳細なアクセス制御を指定してカスタム グループを作成することもできます。詳細については、「コンソール アカウント グループの管理」（104 ページ）を参照してください。 組み込みのアカウント オプションと、そのデフォルトの権限： **Administrator –** Bit9 コンソールのすべての標準的な機能へのフル アクセス。アカウント、レポート、ビュー、ポリシー、ルールなどを作成、変更、削除できます。また、すべてのシステム構成機能を使用できます。自身の権限を変更できます。 **PowerUser** – Bit9 コンソールのほとんどの機能へのアクセス。コンソールの［System Configuration（システム構成）］、［Login Account（ログイン アカウント）］（自身のアカウントを除く）、［Approval Request（承認要求）］の各セクションへの読み取り専用アクセス。ファイルのアップロードおよび分析の送信機能にはアクセスできません。 **ReadOnly** – 非管理機能への読み取り専用アクセス。ReadOnly グループのユーザーは、Bit9 Server システム構成を一切変更できず、Bit9 のリソースを作成、編集、削除することはできません。すべての管理メニューの選択項目は、ReadOnly ユーザーに対しては非表示になります。 **Unauthorized** – このグループのユーザーが持つ既存のアカウントは使用できません。ユーザーによるシステムへのアクセスは禁止し、アカウントは削除しない場合に、Unauthorized を指定します。Unauthorized グループのアカウントに権限を追加することはできません。
Salutation（敬称）	ユーザーの敬称または肩書き（Mr.、Ms.、Dr. など）
First name（名）	ユーザーの名。
Last name（姓）	ユーザーの姓。
タイトル	ユーザーの役職。
Department（部門）	このユーザーが属する組織内のグループ。
Home phone（自宅電話）	ユーザーの自宅の電話番号。
Cell phone（携帯電話）	主に使用する携帯電話の番号。
Cell phone #2（携帯電話 2）	2 番目に使用する携帯電話の番号。
ポケットベル	主に使用するポケットベルの番号。
Pager #2（ポケットベル 2）	2 番目に使用するポケットベルの番号。

フィールド	説明
Comments（コメント）	ユーザーが変更または入力できる追加的な説明情報。ログイン アカウントの一部として表示する任意のテキストを指定できます。
Admin comments（管理コメント）	ユーザーに関する追加的な管理情報。ログイン アカウントの一部として表示する任意のテキストを指定できます。
Show API Token（API トークンの表示）	このチェック ボックスをオンにすると、現在のユーザー アカウント用の API トークンを生成できるインターフェイスが公開されます。この処理のためには、専用のユーザー アカウントを作成することをお勧めします。詳細については、「API 認証とアクセス制御」（836 ページ）を参照してください。

アカウントのパスワードおよびその他の詳細の変更

Bit9 コンソールに初めて「admin」としてログインするときは、デフォルトのパスワード（同じく「admin」）を独自のものに変更する必要があります。「admin」を含むログイン アカウントを保有するすべてのユーザーは、パスワードを定期的に変更する必要があります。

Active Directory ベースのアカウントの場合、パスワードなどのアカウント情報は Active Directory で変更する必要があります。Bit9 コンソールから編集することはできません。

Bit9コンソールで作成されたログイン アカウントの場合は、次のようになります。

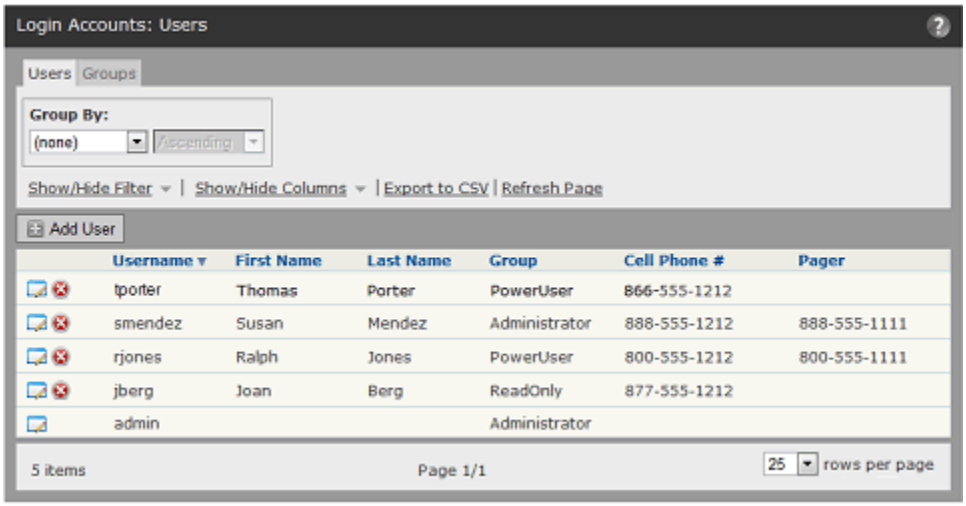
- デフォルトでは、Administrators グループのアカウントは、コンソールで作成されたすべてのアカウントのパスワード、連絡先情報、およびグループを変更できます。「admin」アカウントのグループを変更することはできません。
- デフォルトでは、PowerUsers グループのアカウントは、自身のアカウントのパスワードと連絡先情報を変更できます。
- カスタム グループのアカウント編集権限はさまざまです。

注意

このセクションでは、アカウントの詳細を変更するための［Login Accounts（ログイン アカウント）］管理インターフェイスについて説明しています。これよりもインターフェイスが少ない［Preferences（設定）］ページもあり、そこでは ReadOnly ユーザーを含むすべてのアカウント ユーザーが「自分自身」のアカウントにのみ、パスワードの変更などの変更を行うことができます。詳細については、「コンソール ユーザーの設定」（83 ページ）を参照してください。

ログイン アカウントの Bit9 コンソール パスワードおよびその他の詳細を変更する手順：

1. コンソール メニュー バーから、[Administration（管理）] > [Login Accounts（ログイン アカウント）] の順に選択します。[Login Accounts（ログイン アカウント）] ページが表示されます。



2. [Login Accounts: Users（ログイン アカウント：ユーザー）] ページが表示されない場合は、[Users（ユーザー）] タブをクリックします。
3. [Login Accounts（ログイン アカウント）] ページの [Login Accounts: Users table（ログイン アカウント：ユーザー）] テーブルで、パスワードを変更するユーザーのアカウントを特定します。
4. [Username（ユーザー名）] の隣にある左端の列で、[View Details（詳細の表示）] アイコンをクリックします。[Edit Account Details（アカウントの詳細の編集）] ページが表示されます（フィールドの説明については、表 9、「ログイン アカウントの詳細フィールド」を参照してください）。
5. [Edit Login Account Details（ログイン アカウントの詳細の編集）] ページで、次のように操作します。
   a. [New Password（新しいパスワード）] フィールドに新しいパスワードを入力します。
   b. 確認のために、[Confirm Password（パスワード確認）] フィールドにもう一度パスワードを入力します。
   c. オプションで、ログイン アカウントの他の詳細を変更します。
   d. [Save（保存）] ボタンをクリックします。

注意

［Login Account Details（ログイン アカウントの詳細）］ページの上部にあるボックスのラベルが「External Account（外部アカウント）」である場合、このユーザーは Active Directory アカウントで Bit9 コンソールにアクセスしており、その詳細は編集できません。コンソールで作成されたアカウントは、上部のボックスのラベルに「Account（アカウント）」と表示されます。

6. 他のユーザーのパスワードを変更する場合は、必ず変更を伝えてください。

ログイン アカウントの削除

従業員が Bit9 コンソールにアクセスする必要がなくなった場合や退職した場合などは、ログイン アカウントをシステムから削除できます。Bit9 コンソール ユーザーは、作成が許可されているタイプのアカウントを削除できます。

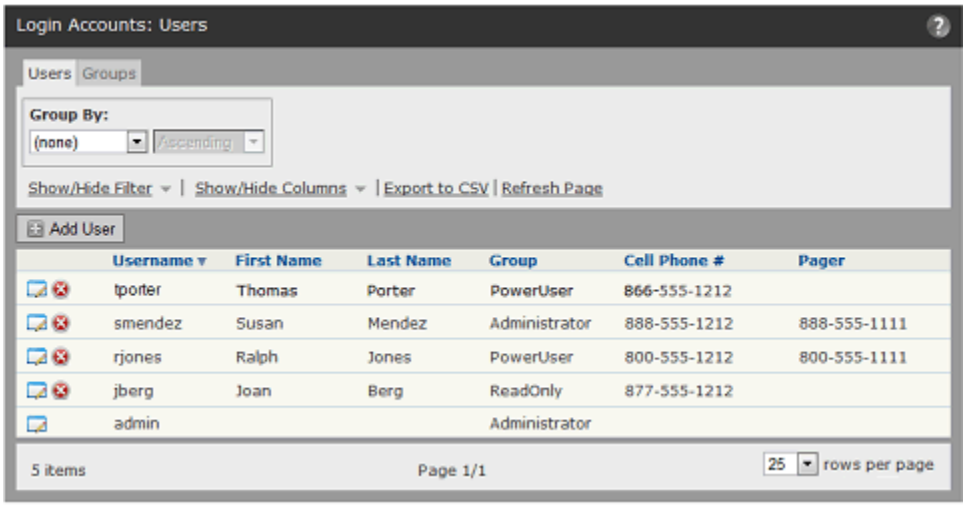
- デフォルトでは、Administrators グループに属するアカウントは、自分自身のアカウントを除くすべてのアカウントを削除できます。
- デフォルトでは、PowerUsers グループに属するアカウントは、ReadOnly のアカウントは削除できますが、PowerUsers と Administrators のアカウントは削除できません。
- カスタム グループのアカウントのアカウント削除権限はさまざまです。

注意

デフォルトの「admin」管理者アカウントを削除することはできません。

ログイン アカウントを削除する手順：

1. コンソール メニュー バーから、［**Administration**（管理）］>［**Login Accounts**（ログイン アカウント）］の順に選択します。［Login Accounts（ログイン アカウント）］ページが表示されます。



2. ［Login Accounts: Users（ログイン アカウント：ユーザー)］ページが表示されない場合は、［**Users**（ユーザー)］タブをクリックします。
3. ［Login Accounts: Users（ログイン アカウント：ユーザー)］テーブルで、ユーザー名を特定します。
4. ユーザー名の隣にある左端の列で、［Delete（削除)］アイコンをクリックします。
5. 確認メッセージに応答します。アカウントを削除する場合は、[**OK**] をクリックします。

ログイン アカウントの無効化

ユーザーが Bit9 コンソールにアクセスする必要がなくなった場合、ログイン アカウントを削除せずにコンソールへのアクセスを制限することができます。これは、アカウントを **Unauthorized** グループに移動することによって行います。特定のログイン アカウントを作成する許可を与えられたユーザーは、そのアカウントを無効にすることもできます。

- デフォルトでは、Administrators グループに属するアカウントは、自分自身のアカウントを除くすべてのアカウントを無効化できます。
- デフォルトでは、PowerUsers グループに属するアカウントは、ReadOnly のアカウントは無効化できますが、Administrators と PowerUsers のアカウント、および自身のアカウントは無効化できません。

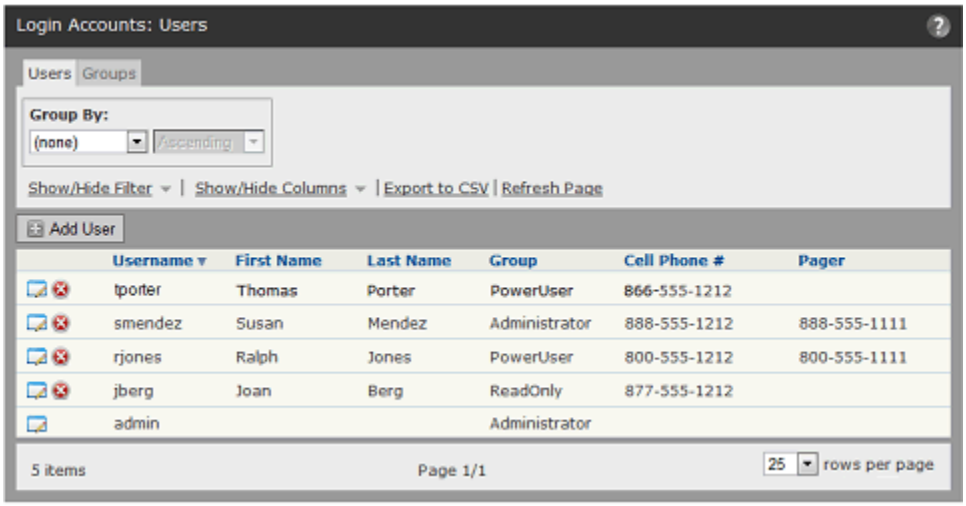
- カスタム グループのアカウントのアカウント無効化権限はさまざまです。

注意

AD マッピングによって作成された Bit9 コンソール ログイン アカウントは、直接無効化することはできません。AD アカウントを無効化する唯一の方法は、その AD セキュリティ グループのマッピング ルールを変更して、Unauthorized ログイン アカウント グループにマップされるようにすることです。

ログイン アカウントを無効化する手順：

1. コンソール メニュー バーから、[**Administration**（管理）] > [**Login Accounts**（ログイン アカウント）] の順に選択します。[**Login Accounts**（ログイン アカウント）] ページが表示されます。



2. [Login Accounts: Users（ログイン アカウント：ユーザー）] ページが表示されない場合は、[**Users**（ユーザー）] タブをクリックします。
3. [Login Accounts: Users（ログイン アカウント：ユーザー）] テーブルで、ユーザー名を特定します。
4. 無効化するアカウントのユーザー名の隣にある [View Details（詳細の表示）] アイコンをクリックします。
5. [Group（グループ）] ドロップダウン メニューから、[**Unauthorized**] を選択します。
6. ページ下部の [Save（保存）] ボタンをクリックします。

コンソール アカウント グループの管理

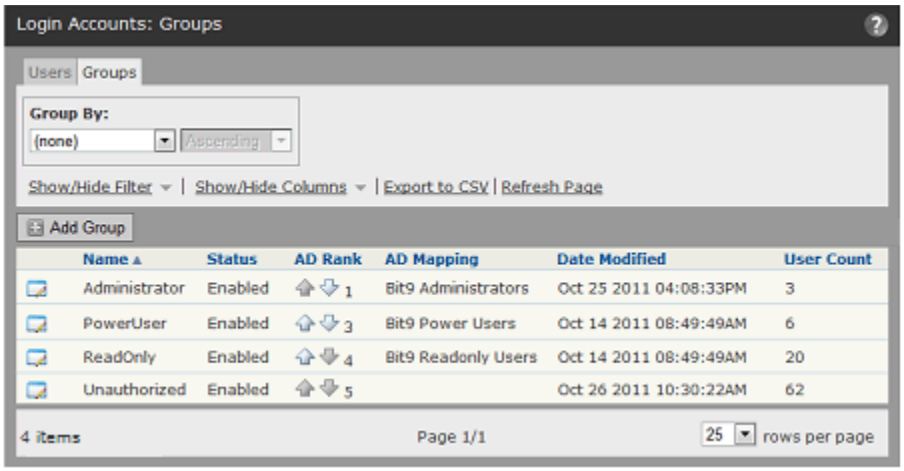
Bit9 コンソール ログイン アカウントの機能は、属しているアカウント グループによって決まります。コンソール アカウント グループを管理する権限を持っているユーザーは、以下のタスクを実行できます。

- カスタム権限を持つ新しいログイン アカウント グループを作成する。
- 組み込みのログイン アカウント グループ（組み込みの Unauthorized グループ以外）の機能を変更する。
- アカウント グループ（組み込みの Administrator グループ以外）を無効化する。
- カスタムで作成した任意のアカウント　グループを削除する（組み込みのグループは削除できません）。
- ADセキュリティ グループからBit9コンソール ログイン アカウント グループへのマッピングと、マッピング ルールが評価される順番を変更する。

現在のログイン アカウント グループは、[Login Accounts: Groups（ログイン アカウント：グループ）] ページで確認できます。このページから、他のグループ管理機能にもアクセスできます。

[Login Accounts: Groups（ログイン アカウント：グループ）] ページの表示手順：

1. コンソール メニュー バーから、[**Administration**（管理）] > [**Login Accounts**（ログイン アカウント）] の順に選択します。[Login Accounts（ログイン アカウント）] ページが表示されます。
2. [Login Accounts: Groups（ログイン アカウント：グループ）] ページが表示されない場合は、[**Groups**（グループ）] タブをクリックします。[Login Accounts: Groups（ログイン アカウント：グループ）] ページが表示されます。



グループの AD マッピングおよびランクの変更

AD 統合を有効にしてある場合は、[Groups（グループ）] タブに Bit9 コンソール ログイン アカウント グループの AD マッピングと AD ランクが表示されます。ランクは、AD マッピング ルールが評価される順番を決定します。この順番は、AD セキュリティ グループが複数のマッピング ルールに一致する場合に意味を持ち

ます。ランクは、[Login Accounts: Groups（ログイン アカウント：グループ）] ページで矢印キーを使用して変更できます。

「Unauthorized」には常に一番下のランクが割り当てられます。これは、このグループが、他のいずれの Bit9 コンソール ログイン アカウント グループのマッピングとも一致しない AD セキュリティ グループ用のデフォルトのグループであるためです。

新しいログイン アカウント グループの作成

組み込みのアカウント グループによってユーザーのアクセス レベルには複数のオプションが用意されていますが、Bit9 コンソールでは、カスタムのログイン アカウント グループを作成および変更するための十分な権限がユーザーに与えられます。アクセスのレベルが 2 つの組み込みオプションの中間に位置する、特別なユーザー グループを作成することもできます。特別なログイン アカウント グループを作成すると、重要な機能への不正アクセスを防げるだけでなく、限定的なロールしか持たないユーザーは、使用しない機能が目に入らないため、そのロールを理解しやすくなります。

たとえば、ヘルプデスク チームのメンバーの場合は、Bit9 コンソールのすべての情報をコンソールに表示できるようにし、それ以外はコンピューターのポリシーの変更、コンピューターをローカル承認にすること、およびデバッグ機能へのアクセスに限定することが考えられます。このような特性を持ったアカウント グループを作成することができます。

表 10 に、ログイン アカウント グループを定義するために使用する情報を示します。

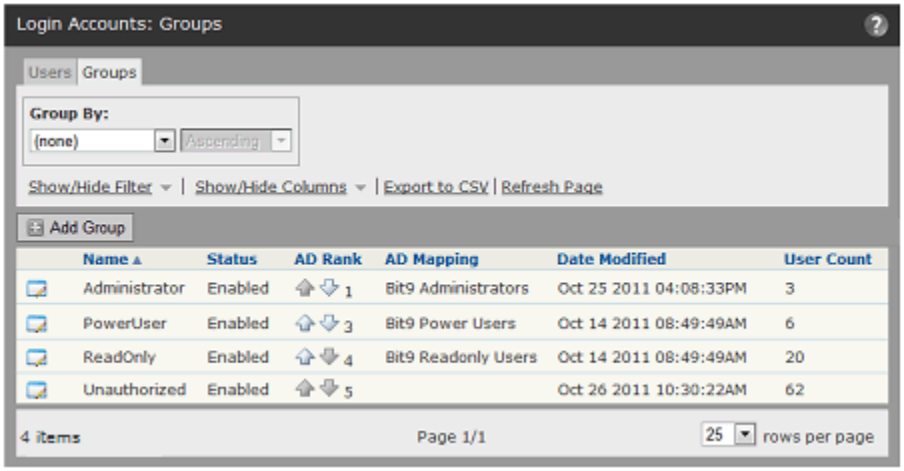
表 10：ログイン アカウント グループのパラメーター

フィールド	説明
Name（名前） （必須）	[Login Accounts: Groups（ログイン アカウント：グループ）] リストに表示され、ログイン アカウントへのグループの割り当て時に使用される名前。 文字、数字、または英語キーボード文字の任意の組み合わせを 32 文字未満の長さで入力します。グループ名では大文字と小文字は区別されません。 **注意**：Bit9 コンソールで作成するユーザー名には「\」、「@」を使用できません。これは、`user@domain` または `domain\user` という形式を使用している AD ベースのユーザー名と競合するのを避けるためです。
Description（説明）	このグループに関するオプションの説明情報。誰が含まれるかのほか、権限に関する大まかな要約などが考えられます。
AD Mapping Name（AD マッピング名）	AD ベースのログイン マッピングを有効にしてある場合に、この Bit9 コンソール ログイン グループにマップする AD セキュリティ グループ。

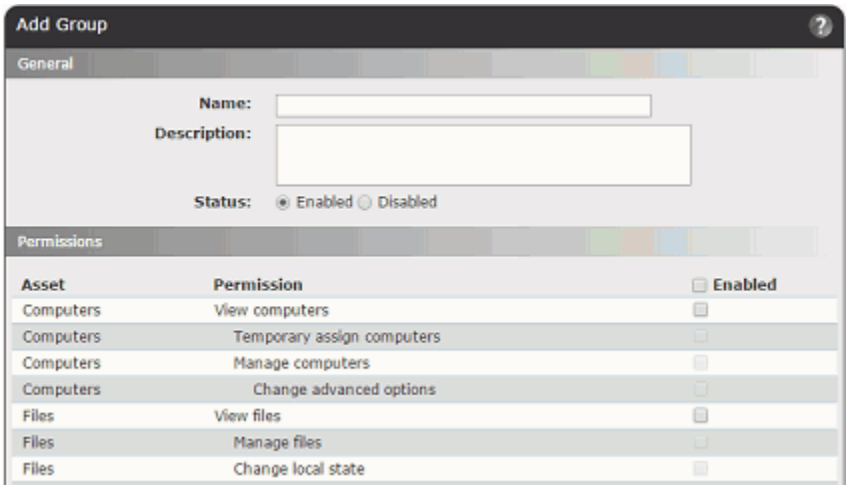
フィールド	説明
Status（ステータス）	このグループを有効化するか無効化するかを決定します。グループを無効化すると、それに含まれるアカウントも無効化され、AD マッピングでこのグループは一致しなくなります。
Permissions（権限）	このグループのメンバーがBit9コンソールで実行を許可される項目を表すチェック ボックスのテーブル。詳細については、109 ページの表 11、「ログイン アカウント グループの権限の設定」を参照してください。

新しい Bit9 コンソール ログイン アカウント グループの作成手順：

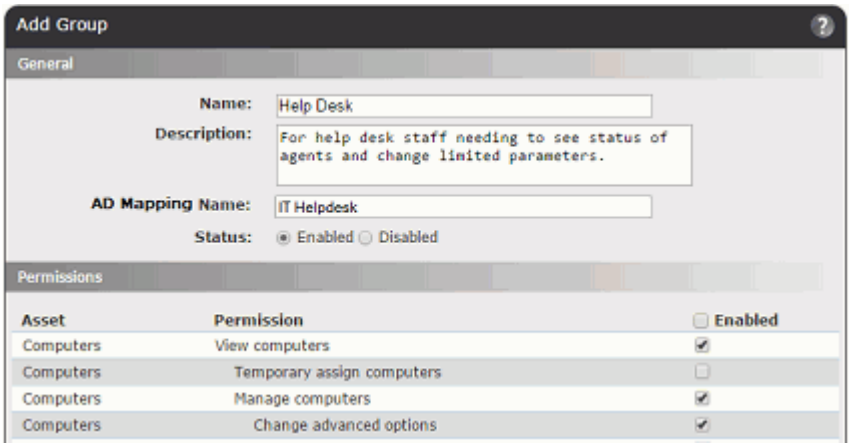
1. コンソール メニュー バーから、［**Administration**（管理）］>［**Login Accounts**（ログイン アカウント）］の順に選択します。［Login Accounts（ログイン アカウント）］ページが表示されます。
2. ［**Groups**（グループ）］タブをクリックします。



3. ［Login Accounts: Groups（ログイン アカウント：グループ）］ページで、［**Add Group**（グループの追加）］をクリックします。［Add Group（グループの追加）］ページが表示されます。

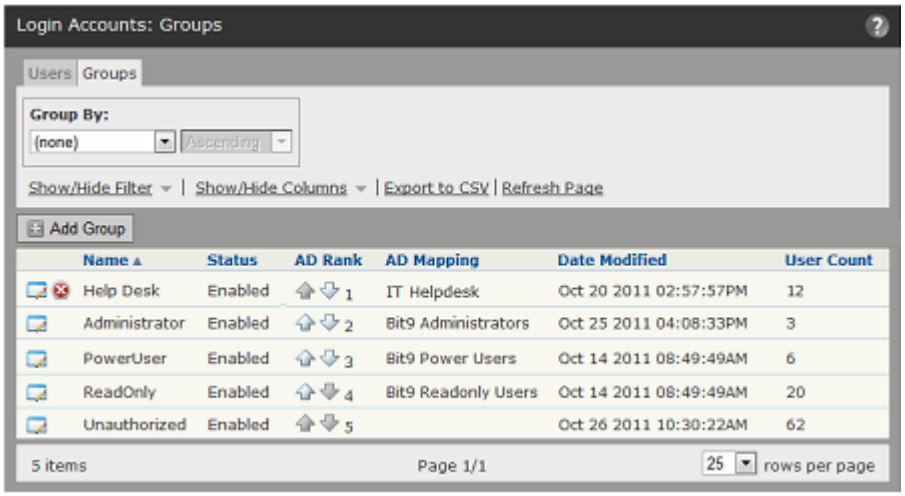


4. 新しいグループの名前と、オプションで目的、想定されるメンバーを明確にする説明や、グループに関するその他の情報などを入力します。
5. このグループをログイン　　アカウントから直接使用できるようにするには、［Status（ステータス）］ラジオ ボタンを［Enabled（有効）］に設定します。
6. AD アカウントのマッピングを有効にしてある場合、AD セキュリティ グループのメンバーを自動的にこの Bit9 コンソール グループにマップするには、その AD セキュリティ グループの名前を［AD Mapping Name（AD マッピング名）］ボックスに入力します。



7. このグループで有効にする各権限の隣のボックスをオンにし、このグループに与えない権限のボックスをオフにします。すべての権限のリストを表 11 に示します。
   注意：Bit9 コンソールのほとんどのアクティビティを実行する権限をこのグループに与える場合は、テーブルのヘッダーにある［Enabled（有効）］ボックスをオンにしてすべてのボックスをオンにしてから、「与えない」権限を削除する方が効率的である可能性があります。

8. このグループの設定が終了したら、ウィンドウの下部にある［**Save**（保存）］ボタンをクリックします。新しいグループが［Login Accounts: Groups（ログイン アカウント：グループ）］テーブルに表示されます。組み込みのグループとは異なり、ユーザー作成のグループは削除できるため、ここには削除ボタンがあります。



9. AD マッピングを有効にしてある場合、新しいグループがマッピング ランクの最上位に置かれます。つまり、この新しいアカウントのマッピング名に一致するすべての AD アカウントは、これよりもランクが低い他のコンソール アカウントと一致する場合でも、このアカウントに割り当てられます。新しいアカウントのランクを下げるには、［AD Rank（AD ランク）］列の矢印を使用して、新しいグループのランクを下げるか他のグループを上げます。
10. AD マッピングを使用してコンソール ログイン アカウントを割り当てていない場合は、この新しいグループに割り当てるアカウントを手動で割り当てます。

アカウント グループの権限

グループの［Add/Edit Group（グループの追加 / 編集）］ページにある［Permissions（権限）］テーブルには、機能が示されており、グループのメンバーについて有効化または無効化することができます。オンにした項目は有効化され、オフにした項目は無効化されます。権限をカスタマイズすることで、グループにとって必要なレベルのアクセスを正確に実現できます。権限を変更できないグループは、Unauthorized グループだけです。

権限は、大きく次の 2 つのカテゴリに分けられます。1 つは Bit9 コンソールの特定のページまたはダイアログを見るための表示権限で、もう 1 つは管理対象のアセット、ルール、コンソール ユーザーを作成、編集、削除するための管理権限です。一部の権限は他の権限に依存しており、表示できないものを管理することはできません。たとえば、［View System Configuration（システム構成の表示）］を無効化すると、［Manage system configuration（システム構成の管理）］も自動的に無効化されます。

他の権限に依存している権限のチェック ボックスは、有効化されていない場合、灰色で（白でなく）表示されます。また、他の権限に依存している権限は、その間の関係を明らかにするためにインデント表示されています。

注意

- 権限の変更は、特に組み込みの Administrator グループの場合、慎重に検討してください。中でも、ユーザー アカウントとグループの表示と管理の権限を削除することは避けてください。削除した場合、これらの機能を復元するためには特殊な復旧コマンドを使用する必要があります。
- Bit9 コンソールのページ、メニュー、リンクなどのユーザー インターフェイスは、ユーザーがすべての管理者権限を持っていることを前提に説明されています。権限をオフにすると、関連するユーザー インターフェイス要素は表示されません。Bit9 Security Platform のヘルプで説明されている機能が見つからないことによる混乱を避けるために、権限が制限されているユーザーにこの可能性を伝えることを検討してください。

表 11：ログイン アカウント グループの権限の設定

アセット	権限名	説明
コンピューター	View computers（コンピューターの表示）	コンピューターのページを表示できます。
コンピューター	Temporary assign computers（コンピューターの一時的な割り当て）	一時的な適用レベル無効化コードを生成できます。View computers（コンピューターの表示）権限が必要です。
コンピューター	Manage computers（コンピューターの管理）	手動でコンピューターをポリシーに割り当て、適用レベルを変更できます。テンプレート コンピューターを管理できます。
コンピューター	Change advanced options（高度なオプションの変更）	コンピューターの診断のコレクションや再同期など、コンピューターの高度なオプションを変更できます。
ファイル	View files（ファイルの表示）	ファイルのページを表示できます。
ファイル	Manage files（ファイルの管理）	ファイルを承認、禁止、確認できます。ファイルをインストーラーとしてマークできます。これには、ローカル ファイルの状態を直接変更する機能は含まれていません。
ファイル	Change local state（ローカル状態の変更）	コンピューター上のファイルのローカル状態を変更できます。

アセット	権限名	説明
デバイス	View devices（デバイスの表示）	デバイスのページを表示できます。
デバイス	Manage device rules（デバイス ルールの管理）	デバイス ルールを管理できます。
ポリシー	View policies（ポリシーの表示）	ポリシーのページを表示できます。
ポリシー	Manage policies（ポリシーの管理）	ポリシーを管理できます（モード、適用レベルなどの変更）。
ポリシー	Manage policy mappings（ポリシー マッピングの管理）	自動ポリシー マッピングのルールを管理できます。
ソフトウェア ルール	View software rules pages（ソフトウェア ルール ページの表示）	ソフトウェア ルールのページを表示できます。Bit9 Connector for Network Security Devices のライセンスが付与されているサーバーの [Event Rules（イベント ルール）] ページの表示も許可されます。
ソフトウェア ルール	Manage event rules（イベント ルールの管理）	イベント ルールを管理できます。Bit9 Connector for Network Security Devices のライセンスが別途必要です。 **注意**：一部のイベント ルールではファイルのアップロードや分析、ファイルの承認などのアクションが指定されており、そのための権限が必要です。
ソフトウェア ルール	Manage trusted directories（信頼できるディレクトリの管理）	信頼できるディレクトリを管理できます。
ソフトウェア ルール	Manage publisher rules（公開者ルールの管理）	信頼できる公開者を管理できます。
ソフトウェア ルール	Manage trusted users（信頼できるユーザーの管理）	信頼できるユーザーを管理できます。
ソフトウェア ルール	Manage custom/registry/memory rules（カスタム / レジストリ / メモリ ルールの管理）	カスタム ルール、レジストリ ルール、およびメモリ ルールを管理できます。
ソフトウェア ルール	Manage updaters（アップデーターの管理）	ソフトウェア アップデーターを有効化、無効化、追加できます。
ソフトウェア ルール	Manage custom scripts（カスタム スクリプトの管理）	Bit9 Server が何をスクリプトとして扱うかのカスタム定義を管理できます。

アセット	権限名	説明
ソフトウェア ルール	Manage indicator sets（痕跡セットの管理）	高度な検出で使用される痕跡セットに対して、有効化、無効化、例外の作成を実行できます。
レポート	View events（イベントの表示）	イベントのページを表示できます。
レポート	View process command lines（プロセス コマンド ラインの表示）	イベントのプロセス コマンド ラインを表示できます。 **重要**：コマンド ラインには、パスワードなどの機密情報が含まれていることがあります。この権限は、デフォルトでは管理者アカウントでも有効化されていません。必要なユーザーのみに限定してください。
レポート	Manage shared dashboards（共有ダッシュボードの管理）	共有ダッシュボードを管理できます。
レポート	View drift reports and snapshots（ドリフト レポートおよびスナップショットの表示）	スナップショット、ドリフト レポート、およびドリフト レポートの結果を表示できます。
レポート	Manage drift reports（ドリフト レポートの管理）	ベースライン ドリフト レポートを管理できます。
レポート	Manage snapshots（スナップショットの管理）	ドリフト レポートで使用されるスナップショットを管理できます。
レポート	Manage saved views（保存済みビューの管理）	すべてのページの保存済みビューを管理できます。
ツール	View alerts（アラートの表示）	アラートのページを表示できます。
ツール	Manage alerts（アラートの管理）	アラートを管理できます。
ツール	View meters（メーターの表示）	メーターおよびメーターの結果を表示できます。
ツール	Manage meters（メーターの管理）	メーターを管理できます。
ツール	View approval requests（承認要求の表示）	ブロック ファイルに対してユーザーから生成された承認要求、およびユーザーが承認したファイルの根拠を表示できます。
ツール	Manage approval requests（承認要求の管理）	ブロック ファイルに対してユーザーから生成された承認要求、およびユーザーが承認したファイルの根拠を管理できます。

アセット	権限名	説明
ツール	View file uploads（ファイルのアップロードの表示）	[Requested Files（要求されたファイル）] ページでアップロードされたファイルを表示できます。
ツール	Manage uploads of inventoried files（登録済みファイルのアップロードの管理）	エージェント コンピューターからファイルの手動アップロードを開始できます。また、ファイルをアップロードするイベント ルールを作成できます。この権限は、Bit9 によって追跡の対象と見なされたファイル（実行可能ファイルおよびスクリプト）のみに適用されます。ファイルのアップロードには別途ライセンスが必要です。
ツール	Manage uploads of files by pathname（パス名によるファイルのアップロードの管理）	エージェント コンピューターからファイルの手動アップロードを開始できます。また、ファイルをアップロードするイベント ルールを作成できます。この権限は、Bit9 インベントリに含まれていないファイルも含めて、エージェント コンピューター上の「すべての」ファイルに適用されます。ファイルのアップロードには別途ライセンスが必要です。
ツール	Access uploaded files（アップロードされたファイルへのアクセス）	サーバーにアップロードされたフィルをダウンロードできます。ファイルのアップロードには別途ライセンスが必要です。
ツール	Submit files for analysis（分析のためのファイルの送信）	手動で、またはイベント ルールを作成することによって、ネットワーク セキュリティ デバイスによる分析のためにファイルを送信できます。API によって実装されている場合を除き、Bit9 Connector for Network Security Devices のライセンスが別途必要です。
通知	View notifiers（通知の表示）	ブロック ファイルの通知の詳細を表示できます。
通知	Manage notifiers（通知の管理）	ブロック ファイルの通知を編集、または新規作成できます。
分析	View external analytics reports（外部分析レポートの表示）	Bit9 コンソールから外部分析レポートへのリンクを表示し、使用できます（外部分析が有効化され、構成されている場合）。
管理	View system configuration（システム構成の表示）	システム構成のページを表示できます。

アセット	権限名	説明
管理	Manage system configuration（システム構成の管理）	システム構成を管理できます。
管理	View login accounts and groups（ログイン アカウントおよびグループの表示）	ログイン アカウントおよびグループを表示できます。
管理	Manage login accounts（ログイン アカウントの管理）	ログイン アカウントを管理できます。
管理	Manage groups（グループの管理）	ユーザー グループを管理できます。
管理	View System Health Indicators（システム正常性の痕跡の表示）	システム正常性のページおよびシステム正常性のアラートを表示できます。
管理	Extend connectors through API（API によるコネクタの拡張）	通知を送信し、（機能セットに含まれている場合は）ファイルを分析できるように、Bit9 API を通じてコネクタを Bit9 Server に登録および登録解除できます。

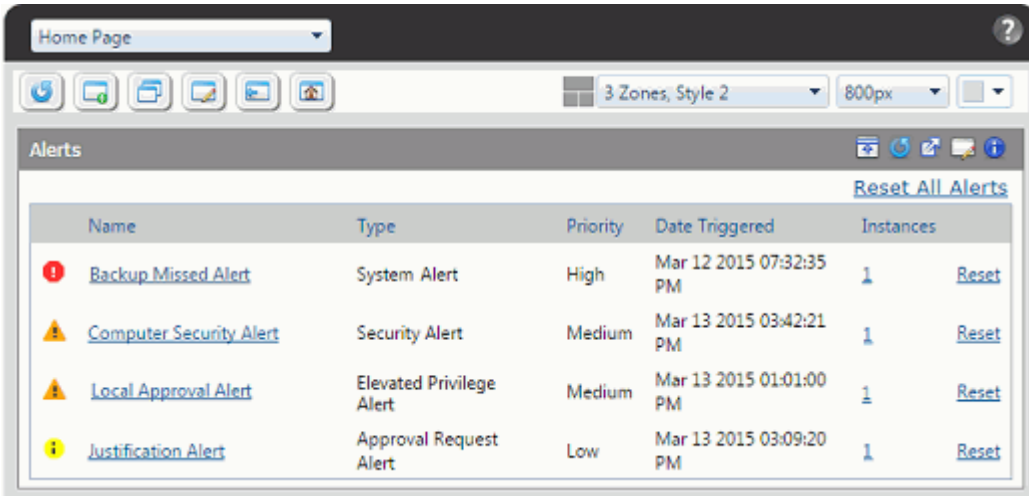
ログイン アカウント グループの編集

Bit9 コンソール ログイン アカウント グループは、次の方法で編集できます。

- 組み込みの Administrator、PowerUser、および ReadOnly コンソール ログイン アカウント グループと、[Login Accounts: Groups（ログイン アカウント：グループ）] タブに表示されるカスタム グループに対しては、機能レベルで権限を追加および削除できます。
- AD マッピングを有効にしてある場合は、コンソール ログイン グループにマップされている AD セキュリティ グループを変更できます。
- アカウント グループを有効化すると、グループに属するアカウントは Bit9 コンソールにアクセスできるようになり、グループを無効化すると、メンバーはコンソールにアクセスできなくなります。
- オプションで、グループの［Description（説明）］を編集することもできます。

Bit9 コンソール ログイン アカウント グループの権限やその他のプロパティを変更する手順：

1. コンソール メニュー バーから、［**Administration**（管理）］>［**Login Accounts**（ログイン アカウント）］の順に選択します。［Login Accounts（ログイン アカウント）］ページが表示されます。
2. ［**Groups**（グループ）］タブをクリックします。
3. ［Login Accounts: Groups page（ログイン アカウント：グループ）］ページで、権限を変更するアカウント グループの［View Details（詳細の表示）］ボタンをクリックします。［Edit Group（グループの編集）］ページが表示されます。



4. ［Edit Group（グループの編集)］ページで、表示されている各機能の現在の権限を確認します。右側の列にチェックマークが付いている機能は有効化されています。チェック ボックスが空の機能は無効化されています。ステータスを変更する機能のチェック ボックスをクリックします。
5. 必要に応じて［AD Mapping Name（AD マッピング名）］や［Description（説明)］などの他のグループ プロパティを変更し、ページ下部にある［Save（保存)］ボタンをクリックして変更を保存します。

グループの無効化

Administrator 以外のグループは無効化することができます。グループを無効化すると、関連付けられたすべてのログイン名は（他のコンソール ログイン グループとも一致する AD ベースのログイン名を除いて）無効になります。アカウントを無効にする方法については、「ログイン アカウントの無効化」（102 ページ）を参照してください。

グループの削除

カスタム ログイン アカウント グループは、関連付けられたアカウントが存在しない状態ならば削除できます。組み込みのアカウント グループは削除できません。

Bit9 コンソール ログイン アカウント グループの削除手順：

1. コンソール メニュー バーから、［Administration（管理）］>［Login Accounts（ログイン アカウント)］の順に選択します。［Login Accounts（ログイン アカウント)］ページが表示されます。
2. ［Groups（グループ)］タブをクリックします。
3. 削除するグループの隣にある［Delete（削除)］(x) ボタンをクリックし、削除を確認します。

第 4 章

コンピューターの管理

この章では、Bit9 コンソールを使用してクライアント コンピューターを管理する方法について説明します。ここでは、第 5 章「ポリシーの作成と構成」の説明に従ってポリシーを設定済みであることを前提にしています。

コンピューター構成タスクには、各コンピューターをセキュリティ ポリシーに割り当てる方法の選択、Bit9エージェントのダウンロード、クライアント コンピューターへのエージェントのインストールがあります。この章では、新しいファイルがネットワークに入ってきたときの参照ポイントとしてファイルのスナップショットを提供するように、コンピューターを設定する方法も説明しています。

仮想マシンを管理する予定がある場合は、この章に加えて第 6 章「仮想マシンの管理」も参照してください。

セクション

コンピューター構成の概要

クライアント コンピューター システムに Bit9 エージェントをインストールして実行すると、そのシステムは Bit9 Server から認識されるようになります。エージェントをダウンロードしてインストールすると、初期化プロセスが開始され、コンピューターとその上のファイルに関する情報が Bit9 Server に送信されます。

インストール前の作業

エージェントをインストールする前に、コンピューター構成に関して以下に示すいくつかの重要な決定を行います。

- **ポリシーの作成** は、コンピューターで使用できるセキュリティ設定のグループを決定します。まだポリシーを作成していない場合は、第 5 章「ポリシーの作成と構成」を参照してください。
- **CLI管理**の構成オプションでは、Bit9テクニカル サポートと連絡を取りながら特定のエージェント管理アクティビティを実行するときのために、ユーザーまたはグループ、または誰もが使用できるパスワードを指定できます。特に、恒久的にオフラインにするシステムがある場合は、ポリシーの作成とエージェント インストール パッケージの配布の前に、ここでいずれかのオプションを選んでおくことをお勧めします。詳細については、「高度な構成オプション」（766 ページ）を参照してください。
- **（オプション）期限切れの証明書の検証設定を確認**します。これは、オフライン システムを実行する場合に重要です。期限切れの証明書でファイルを承認する場合は、恒久的にオフラインのシステムにエージェントをダウンロードしてインストールする前に、これを選択する必要があります。それ以外の方法では、期限切れの証明書は使用できません。詳細については、「期限切れの証明書での承認」（297 ページ）を参照してください。
- コンピューターへの**初期ポリシーの割り当て**は、「Active Directory マッピングによるポリシーの割り当て」（120 ページ）で説明されているように Active Directory データによって、または「エージェント インストーラーのダウンロード」（131 ページ）で説明されているように、使用するエージェント インストーラーによって決まります。
- **（オプション）ファイルのスナップショットのための参照コンピューターを用意する**と、環境内のファイルのベースラインが得られます。望ましいのは、クリーンなコンピューターを用意し、システムの一部または全体で実行するアプリケーションだけをそこにインストールすることです。このコンピューターを用意したら、Bit9 エージェントをインストールします。初期化が完了したら、第 19 章「変更の監視：ベースライン ドリフト レポート」の説明に従ってスナップショット プロセスを実行します。

インストールと初期化

作成したセキュリティ ポリシーごとに、サポートされているプラットフォーム（Windows、Mac、Linux）用のエージェント インストーラーが作成されます。各エージェント インストーラーには、コンピューターに割り当てられるポリシーと、Bit9 Server アドレスが含まれています。AD ベースのポリシー割り当てを使用しない場合、各コンピューターのエージェント インストーラーは、コンピューターのプラットフォームとそのコンピューターを制御するポリシーに基づいて選択します。インストーラーについては、「エージェント インストーラーのダウン

ロード」（131 ページ）および「Bit9 エージェントのインストール」（133 ページ）を参照してください。

Bit9 エージェントのソフトウェアがインストールされると、直ちにファイルの初期化が始まります。エージェントは、クライアント コンピューターの固定ドライブ（リムーバブル ドライブは対象外）にあるすべての実行可能ファイルのインベントリを取得して、各ファイルのハッシュを作成します。コンピューターが最初にサーバーに接続すると、そのエージェントは、各ハッシュを Bit9 Server に送信して、サーバーのファイル インベントリを更新します。初期化中のコンピューター上のファイルは、Bit9 Server で確認済みでないか、グローバルまたはポリシーで禁止されていない限り、「ローカル」承認済み状態になります。初期化の際、コンピューターは割り当てられたセキュリティ ポリシーがあればそれによって保護され、ファイル アクティビティはそのポリシーに従って許可またはブロックされます。

注意

テンプレート コンピューターからクローンされる仮想マシンは、インベントリ内の初期（クローンされた）ファイルを含むかどうかを設定できます。詳細については、「クローン インベントリの構成」（223 ページ）を参照してください。

Bit9 ルールによってあらかじめ禁止または承認されていない限り、Bit9 Server にとって新規のファイルは「グローバル」状態が未承認になり、カタログに追加されます。初期化の「後」でファイルがこのエージェントに初めて認識された場合、エージェントにとってファイルの「ローカル」状態は未承認になります。ファイルの状態の詳細については、「ファイルの状態、ホワイトリスト、ブラックリスト」（46 ページ）を参照してください。

インストール後の作業

Bit9 エージェントをコンピューターにインストールし、初期化が完了した後、次のようにさまざまな方法でコンピューターを監視および管理できます。

- **コンピューターの詳細の表示** – Bit9 Server には、Bit9 エージェントが実行されている各コンピューターの詳細が保持されています。具体的には、コンピューターの IP アドレス、現在サーバーに接続されているかどうか、割り当てられているポリシー、モード、適用レベル、コンピューターのモデルおよびシステムの詳細、接続履歴などです。「コンピューターのテーブルの表示」（153 ページ）を参照してください。
- **コンピューター関連イベントの表示** – 特定のコンピューターに関連するイベントを監視できます。「イベント レポート」（590 ページ）を参照してください。
- **ポリシーの変更** – 必要に応じて、コンピューターに割り当てられているセキュリティ ポリシーを変更できます。「別のポリシーへのコンピューターの移動」（173 ページ）および「デフォルト ポリシーからのコンピューターの復元」（174 ページ）を参照してください。
- **クローンの作成** – コンピューターをテンプレートとして使用して他のコンピューターをクローン作成する場合は、第 6 章「仮想マシンの管理」を参照してください。

- **ファイルのローカル承認** – コンピューターを一時的にローカル承認モードにすることで、Bit9 Server 上でグローバル状態が未承認のファイルをローカルにインストールし、このコンピューターでローカルに承認することができます。「ローカル承認モードへのコンピューターの移行」（176 ページ）を参照してください。
- **接続されているデバイスの詳細の表示** – エージェントで管理する Windows コンピューターに接続されている固定およびリムーバブル ストレージ デバイスを追跡、管理できます。詳細については、「コンピューター上のデバイスの表示」（402 ページ）を参照してください。
- **（オプション）スナップショットの保存** – エージェントのインストールと初期化が完了したら、その時点で Bit9 に登録されているすべての（ハッシュに基づく）ファイルの名前付きスナップショットを保存するように Bit9 Server に指示することができます。これにより、そのコンピューター、他のコンピューター、またはネットワーク全体のファイル インベントリの変化を分析するための参照ポイントが得られます。詳細については、「スナップショットの作成と変更」（661 ページ）を参照してください。
- **コンピューターの削除** – ネットワークから、または Bit9 Security Platform の制御からコンピューターを除外するときは、エージェントをアンインストールし、サーバー上のコンピューターのテーブルからそのコンピューターを削除します。これには、「コンピューターの削除」（177 ページ）に示した一連のアクションが必要です。

コンピューター管理機能へのアクセス

コンピューター管理機能にアクセスできるかどうかは、アクセスを試みるユーザーのログイン アカウント グループの権限によって決まります。

- デフォルトの権限を持つ Administrator および PowerUser のアカウントは、これらの機能にフル アクセスできます。
- デフォルトの権限を持つReadOnlyユーザーは、Bit9エージェントが実行されているコンピューターの詳細を表示することはできますが、設定の追加、削除、変更はできません。
- カスタムのログイン アカウント グループに属するユーザーのアクセス レベルは、［Add/Edit Group（グループの追加 / 編集）］ページの［Computers（コンピューター）］アセット行に示される、グループの権限によって決まります。ここで説明する機能の一部には、追加の権限が必要であることに注意してください。

ログイン アカウント グループの権限の表示と変更の詳細については、「アカウント グループの権限」（108 ページ）を参照してください。

一部またはすべてのユーザーは、標準的なコンピューター管理機能に加えて、エージェント管理コマンドにもアクセスできます。これは、通常は Bit9 テクニカル サポートと連絡を取りながら、特殊な状況で使用します。詳細については、「エージェント管理権限の構成」（750 ページ）を参照してください。

ポリシーへのコンピューターの割り当て

Bit9 エージェントが実行されている各コンピューターには、セキュリティ ポリシーが割り当てられます。コンピューターにポリシーを割り当てる標準的な方法は、次の 3 つです。

- **エージェント インストーラー**– ポリシーを作成すると、Bit9 がサポートされているプラットフォームごとにポリシー固有の Bit9 エージェント インストーラーが生成されます。これにより、コンピューターにエージェントをインストールするとポリシーが割り当てられます。インストールされたエージェントが Bit9 Server に接続すると、そのコンピューターはコンソール上でコンピューターのテーブルに追加されます。AD ベースのポリシー割り当てを設定していない場合、手動で再割り当てを行わない限り、エージェントのポリシーはインストーラーに組み込まれているものが維持されます。
  コンピューターのポリシーを変更するために Bit9 エージェントを再インストールすることは不要であり、実行すべきでもありません。通常、エージェントは各コンピューターに 1 回インストールするだけで済みます。
- **Active Directory (AD) グループ マッピングによる自動** – コンピューターの AD グループ（または、そのコンピューターにログインしているユーザー）情報に基づいて、新規の、および設定によっては既存のコンピューターをセキュリティ ポリシーに割り当てるスクリプトを実行するように、Bit9 Server を設定できます。コンピューターの初期ポリシーは、エージェント インストーラーによって決まります。その初期ポリシーでポリシーの自動割り当てが許可されている場合、この AD ベースのポリシー割り当てが優先されます。AD マッピングによるポリシー割り当てについては、このセクションで後ほど説明します。
- **手動** – どのコンピューターも、インストーラーまたは AD マッピング機能によって割り当てられたものとは異なるポリシーに移動させることができます。これは、間違ったインストーラーが使用されたコンピューターを発見した場合や、ポリシーのマッピングに使用される AD グループ内の他のコンピューターとは異なるセキュリティ ポリシーが必要な場合に有効です。また、手動の割り当ては、コンピューターおよびそのユーザーに対する制限を一時的に強く、または弱くする必要がある状況でも使用できます。コンピューターのポリシーを手動で変更する場合は、後から元のポリシーに復元（または自動割り当て）できます。手動のポリシー割り当てについては、「別のポリシーへのコンピューターの移動」（173 ページ）を参照してください。

コンピューターは、ポリシー割り当てを手動から自動、または自動から手動に変更できます。

注意

場合によっては、ここに示した以外の理由でポリシーを変更することも考えられます。以下に例を示します。

- コンピューターがオフラインの間に、そのコンピューターが属しているポリシーを削除すると、コンピューターはデフォルト ポリシー グループに移動します。詳細については、「デフォルト ポリシーからのコンピューターの復元」（174 ページ）を参照してください。
- オプションのイベント ルール アクションによって、指定したイベントが発生したときにコンピューターを別のポリシーに移動することができます。この機能を有効化するには、Bit9 テクニカル サポートによるサポートが必要です。詳細については、「イベント ルールの作成と編集」（524 ページ）を参照してください。

AD ベースのポリシー割り当てを使用していない場合は、次のセクションを省略して、「エージェント インストーラーのダウンロード」（131 ページ）で説明しているポリシー固有のインストーラーを選択する手順に直接進むことができます。

Active Directory マッピングによるポリシーの割り当て

各コンピューターを Active Directory (AD) データに基づいて特定のポリシーにマップするルールを作成することができます。AD ベースのポリシー割り当ては、エージェントが初めて Bit9 Server に接続したときに行われ、サーバーとエージェントの間の再接続が確立されるか、エージェント コンピューター上のログイン ユーザーが変わったときは、そのたびに確認されます（マッピングが変わる可能性のある場合の詳細については、「コンピューターの登録と AD マッピング」（130 ページ）を参照してください）。

AD ポリシー マッピングの概要

AD ベースのポリシー割り当てを利用するには、次の条件を満たす必要があります。

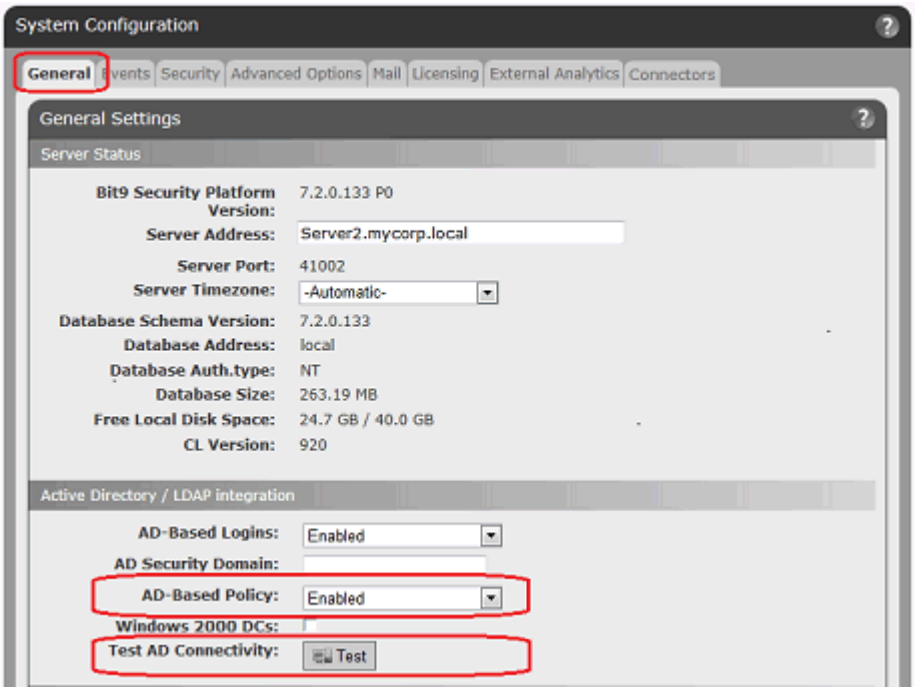
- **AD ドメインへの Bit9 Server のインストール** – Active Directory ドメインのメンバーであるコンピューターに Bit9 Server をインストールします。デフォルトでは、Bit9 Server はマップするコンピューターおよびユーザーと同じ AD フォレストに存在する必要があります。クロス フォレスト統合が必要な場合は、Bit9 サポートの担当者にご連絡ください。
- **AD マッピング インターフェイスの有効化** – [System Configuration（システム構成）] ページの [General（全般）] タブにある [Active Directory/LDAP integration（Active Directory/LDAP 統合）] パネルで、AD ベースのポリシー マッピング インターフェイスを有効化します。
- **AD マップ可能なターゲット ポリシーの作成** – AD マッピングによるコンピューターの割り当て先となるセキュリティ ポリシーを作成し、そのポリシーで必ず自動ポリシー割り当てを許可します。

- **マッピングの作成** – [Policies（ポリシー）] ページの [Mappings（マッピング）] タブで、AD データを使用してコンピューターを別のセキュリティ ポリシーに割り当てる AD ポリシー マッピング ルールを作成します。
- **AD マップ可能なポリシーへのエージェントのインストールまたは移動** – エージェントの新規インストールの際は、エージェントのインストール パッケージのポリシーで必ず自動ポリシー割り当てを許可します。マッピングが正常に実行されるためには、エージェントの現在のポリシーとマップされるポリシーの両方で自動ポリシー割り当てが有効になっている必要があります。既存のエージェントは、必要に応じてインストール後にポリシーを手動から自動に変更したり、エージェントを AD マップ可能なポリシーに移動したりすることができます。

プラットフォームに関する注意：Bit9 Server は、Active Directory サーバーを通じて設定したすべてのコンピューターに対して、それが Windows 以外のプラットフォームであっても AD マッピングを実行します。

AD マッピング インターフェイスを有効化する手順：

1. コンソール メニューで、[**Administration**（管理）] > [**System Configuration**（システム構成）] の順に選択します。[System Configuration（システム構成）] ページが表示されます。
2. [General Settings（全般設定）] ビューが表示されていない場合は、[General（全般）] タブをクリックします。[**General**（全般）] タブには、2 番目のパネルとして [Active Directory/LDAP integration（Active Directory/LDAP 統合）] があります。



3. ［Active Directory/LDAP integration（Active Directory/LDAP 統合）］パネルで、［Test AD Connectivity（AD 接続のテスト)］の隣にある［**Test**（テスト)］ボタンをクリックします。「Success（成功）」というメッセージが表示されたら、次のステップに進みます。「Error（エラー）」というメッセージが表示された場合、Bit9 Server が AD にアクセスできない状態です。この問題を解決するまで、AD マッピングは実行できません。
4. AD 接続が成功した場合は、ウィンドウ下部にある［**Edit**（編集)］ボタンをクリックします。
5. ［AD-Based Policy（AD ベースのポリシー）］のドロップダウン メニューで、［**Enabled**（有効)］を選択します。
6. 変更を送信するには、［**Update**（更新）］ボタンをクリックし、確認ダイアログで［**Yes**（はい)］をクリックします。

AD マッピング ルールの作成

AD ベースのポリシーのインターフェイスを有効にすると、［Policies（ポリシー)］ページを開いたときに新しく［Mappings（マッピング)］タブが表示されます。このタブでクリックすると、［Active Directory Policy Mappings（Active Directory ポリシー マッピング)］ページが開きます。そこで、指定した AD データを持つコンピューターを特定のポリシーにマップするルールを作成します。

マッピング ルールの設定を開始する前に、コンピューターをマップするポリシーをすべて作成しておく必要があります。

マッピング ルールを作成して、組織の部門、ドメイン、セキュリティ グループ、コンピューター名、ユーザー名などの AD データの一致をテストすることができます。マッピング ルールを作成するときは、次の点を考慮する必要があります。

- AD セキュリティ グループのデータは､ユーザーとコンピューターのどちらの一致も利用できますが、コンピューター ベースのルールをお勧めします。1 台のコンピューターに複数のユーザーが存在し､同時にログオンすると､ユーザー ベースの AD マッピングから想定外の結果が発生する可能性があります。
- Bit9 Security Platform では、二重引用符を含む AD オブジェクト名をポリシー マッピングで扱うことはできません。二重引用符を含むオブジェクト名は、マッピング ルールの作成に使用するディレクトリ オブジェクト ブラウザーでは適切に処理できません。
- 原則として、作成するルールの数はできるだけ少なくし、個別のオブジェクトではなくグループをテストします。

マッピング ルールで使用するルール パラメーターを表 12 に示します。

表 12：AD マッピング ルール パラメーター

パラメーター	説明
Computer Object to Test（テストするコンピューター オブジェクト）	ルールに一致するかどうかを調べるためにテストされるオブジェクト。選択肢は、[Computer（コンピューター）]、[User（ユーザー）]、[User or Computer（ユーザーまたはコンピューター）] です。
Relationship（関係）	評価の対象となる関係。ルールで指定されるディレクトリ オブジェクトと、ポリシーを割り当てるコンピューターの AD データの間の関係です。以下の選択肢があります。 • is member of group（グループのメンバー） • is in OU or domain（OU またはドメインに含まれる） • is（等しい） • is not in any domain（どのドメインにも含まれない）
Directory Object（ディレクトリ オブジェクト）	テストされるオブジェクトのデータと一致が確認される AD 内のオブジェクト。このフィールドの右端をクリックすると AD ブラウザーが開き、そこから AD 環境内のオブジェクトを検索できます。 [Directory Object（ディレクトリ オブジェクト）] フィールドの選択肢は、[Relationship（関係）] での選択によって変化します。「is not in any domain」を選択した場合、ディレクトリ オブジェクトは不要です。
Policy to Apply（適用するポリシー）	テストされたオブジェクトがルールに一致した場合にコンピューターに適用するポリシー。選択できるすべてのポリシーがドロップダウン メニューに表示されます。 **注意**：Active Directory ポリシー マッピングを実装する前に作成されているポリシーに対しては、「Automatic policy assignment（自動ポリシー割り当て）」はデフォルトでオフになっています。AD ポリシー マッピングを実装し、以前から存在するポリシーが適用対象になる新しいマッピング ルールを設定した場合は、自動マッピングが実行されるようにポリシー自体の設定を変更する必要があります。自動割り当てを選択することの詳細については、「ポリシーの作成」（183 ページ）を参照してください。

これらのパラメーターを指定すると、ルールは文のように読むことができます。ルールを設定する例を次に示します。

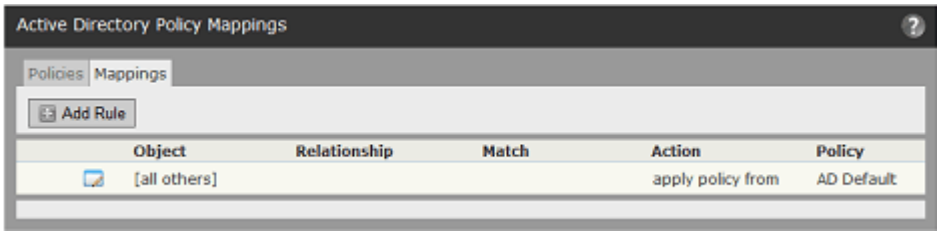
パラメーター	例（太字部分は値）
Computer Object to Test（テストするコンピューター オブジェクト）	If a **Computer**…
Relationship（関係）	… **is in OU or domain** …

パラメーター	例（太字部分は値）
Directory Object（ディレクトリ オブジェクト）	…matching **OU = Marketing,DC=hq,DC=xyzcorp,DC=local** …
Policy to Apply（適用するポリシー）	… assign that computer to the **Standard Protection** policy.

マッピング ルールを設定する手順を次に示します。ほとんどのパラメーターの入力は難しくありませんが、特殊な AD ブラウザーを使用する必要がある［Directory Object（ディレクトリ オブジェクト）］フィールドは特別な注意が必要です。

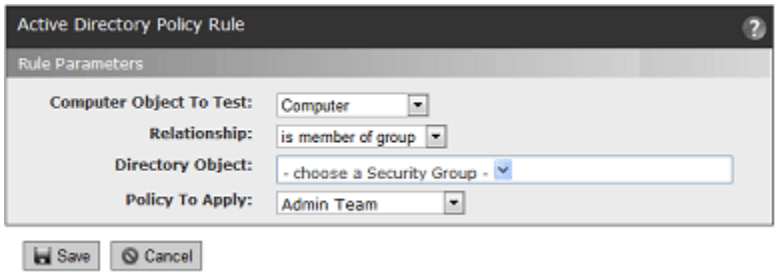
AD ポリシー マッピング ルールの作成手順：

1. コンソール メニューで、［**Rules**（ルール）］>［**Policies**（ポリシー）］の順に選択します。［Policies（ポリシー）］ページが開き、使用可能なすべてのポリシーのリストが表示されます。
2. ［**Mappings**（マッピング）］タブをクリックします。［Active Directory Policy Mappings（Active Directory ポリシー マッピング）］ページが開き、初期状態ではデフォルトのルールのみを含む［Policy Mappings（ポリシー マッピング）］テーブルが表示されます。



注意：［Mapping（マッピング）］タブが表示されない場合は、AD マッピング インターフェイスが有効化されていません。［System Administration（システム管理）］ページの［General（全般）］タブに移動して、この機能を有効にしてください。

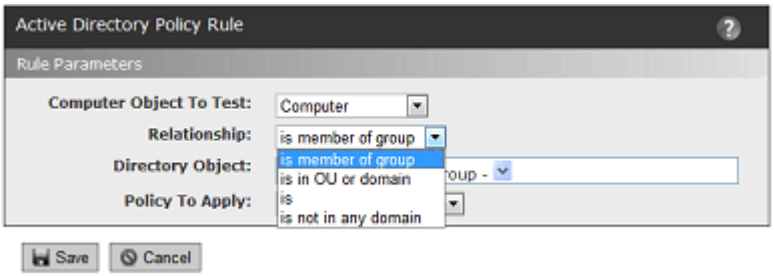
3. ［Active Directory Policy Mappings（Active Directory ポリシー マッピング）］ページで、［**Add Rule**（ルールの追加）］をクリックします。［Active Directory Policy Rule（Active Directory ポリシー ルール）］パネルが表示されます。ここにルール パラメーターを入力します。



4. ［Computer Object to Test（テストするコンピューター オブジェクト）］ドロップダウン メニューで、［Computer（コンピューター）］、［User（ユーザー）］、または［Computer and User（コンピューターおよびユーザー）］を選択します。ほとんどの場合、［**Computer**（コンピューター）］が最適な選択肢です。

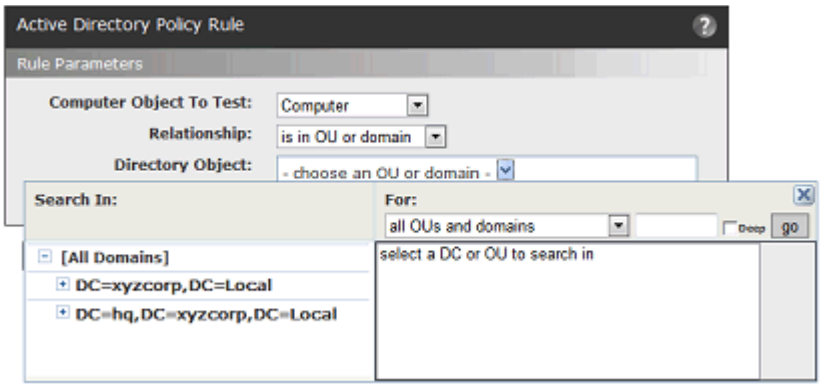
5. テストされるオブジェクトのデータと、ルールで指定されるディレクトリ オブジェクトの間の関係を選択します。このフィールドでの選択によって他のフィールドの選択肢が変わります。

   このフィールドでは、オブジェクトが OU またはドメインに含まれているか、セキュリティ グループの中に含まれているか、どのドメインにも含まれていないか、または選択したディレクトリ オブジェクトと完全に一致する（［Relationship（関係）］メニューの「is」選択肢）必要があるかを指定します。原則として、個別のコンピューターやユーザーを特定するのではなく、複数のコンピューターをポリシーにマップする関係を指定してください。



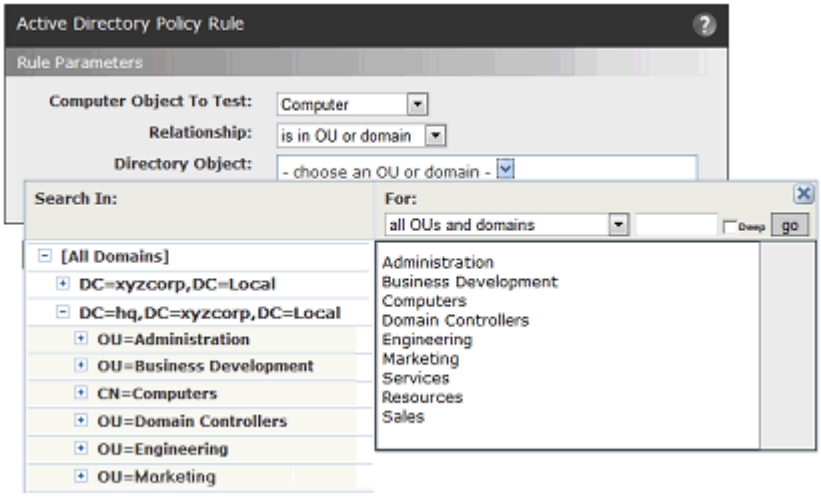
6. テストされるコンピューターのデータと一致が確認されるディレクトリ オブジェクトを選択します。

   a. ［Directory Object（ディレクトリ オブジェクト）］フィールドをクリックして AD ブラウザーを開きます。［Directory Object（ディレクトリ オブジェクト）］フィールドの直下にブラウザーが開きます。左パネルには「Search in（検索する場所）」というラベルと、AD ドメインのツリーが表示されます。

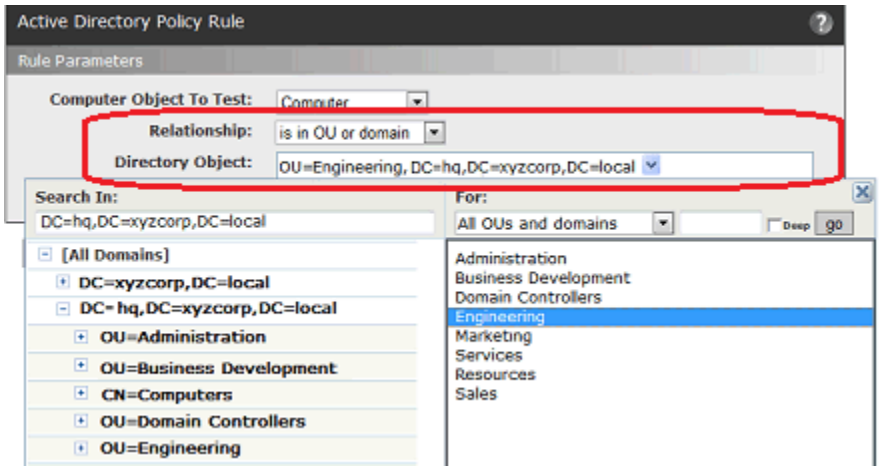


b. 左パネルの AD ツリーを展開するには、展開するノードの隣にあるプラス記号のボタンをクリックします。左パネルのビューを縮小するには、縮小するノードの隣にあるマイナス記号のボタンをクリックします。

c. 左パネルで、検索の範囲を定義するオブジェクトをクリックします。たとえば、2 つのドメインがある場合は、上の例のようにそのうちの 1 つ「DC=hq,DC=xycorp,DC=Local」をクリックすることが考えられます。



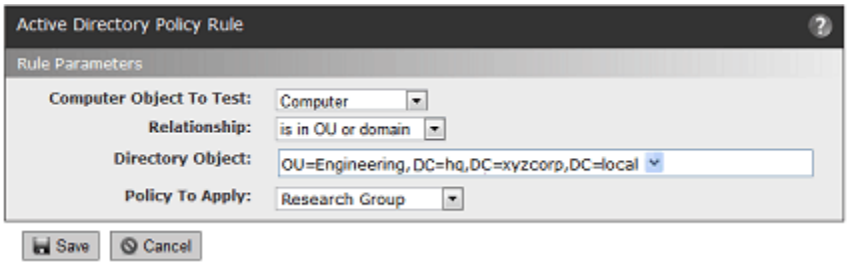
d. このルールに使用するオブジェクトが右パネルにある場合は、それをダブルクリックします。オブジェクト、および AD オブジェクト ツリー内でのオブジェクトの場所に関する詳細な情報が［Rule Parameters（ルール パラメーター）］パネルの［Directory Object（ディレクトリ オブジェクト）］フィールドに表示され、ブラウザーが閉じます。



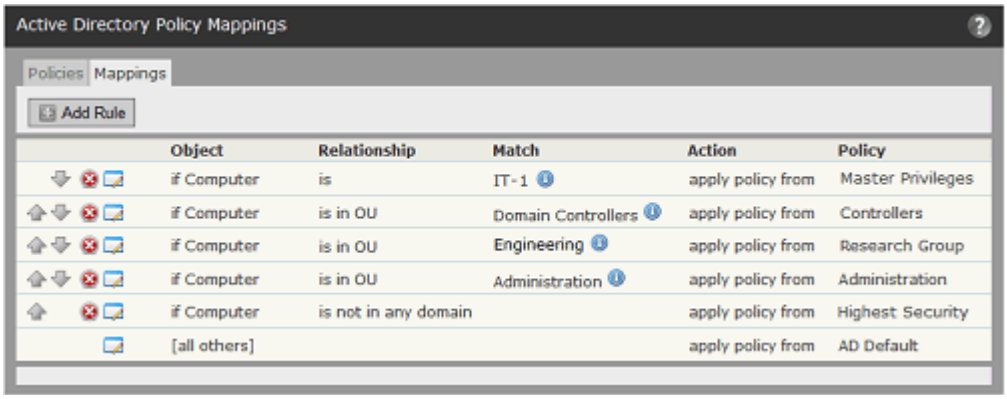
e. ブラウザーが自動的に閉じない場合は、右上の [X] ボタンをクリックして閉じます。

注意：ディレクトリ オブジェクト ブラウザーを使用する際には、さらに別のオプションもあります。詳細については、「AD オブジェクト ブラウザーのオプション」（128 ページ）を参照してください。

7. ［Policy to Apply（適用するポリシー）］ドロップダウン メニューで、このルールの要件に一致するコンピューターに割り当てるポリシーを選択します。ドロップダウンに既存のポリシーのみが表示される場合、つまりこのルールに対応するポリシーがまだ作成されていない場合は、このルールの作成をキャンセルし、［Policies（ポリシー）］ページに移動して新しいポリシーを作成します。



8. ルールのパラメーターをすべて入力したら、［**Save**（保存）］をクリックします。新しく作成されたルールは AD ルールのテーブルの下部、デフォルトのルールの 1 つ上に表示され、それよりも上にあるすべてのルールが優先されます。この例のルールは、Engineering OU に属し hq.xyzcorp.local ドメイン内に存在するすべてのコンピューターを Research Group ポリシーに割り当てるように、Bit9 Server に指示しています。



［Match（一致）］列に表示されているオブジェクトの隣の **[i]** ボタンの上にマウス カーソルを置くと、そのオブジェクトの説明が表示されます。

9. 必要に応じて左端にある上向きと下向き矢印のボタンを使用して（またはドラッグアンドドロップによって）、コンピューターに対してルールが評価される順番を変更します。「［all others（その他すべて）］」ルールは、常にテーブルの一番下に置かれます。
10. ステップ 3 からここまでの手順を、作成する必要がある各ルールについて繰り返します。

マッピング ルールのランキング

AD マッピング ルールは、［Mappings（マッピング）］ページでの上から下の順番でスキャンされ、リストの中で最初に一致したルールだけが適用されます。現在とは異なるポリシー割り当てが望ましいと判断した場合は、ルールの順番を変更します。

デフォルトの AD マッピング ルールは削除できず、［Policy Mappings（ポリシー マッピング）］ルール テーブルの一番下から移動させることもできません。これは「［all others（その他すべて）］」にマップされます。つまり、テーブル内の他のルールのどれにも一致しなかったコンピューターはすべて、ここで選択したポリシーに割り当てられます。これがテーブルの一番下に固定されているため、自動的にマップされるすべてのコンピューターは必ず何らかのポリシーにマップされます。これは、初期状態ではデフォルト ポリシーにマップされますが、変更することができます。他のルールに一致しないコンピューターに、希望するデフォルトのセキュリティ レベルを的確に反映したポリシーが割り当てられるように、「AD Default Policy」を作成することをお勧めします。

AD オブジェクト ブラウザーのオプション

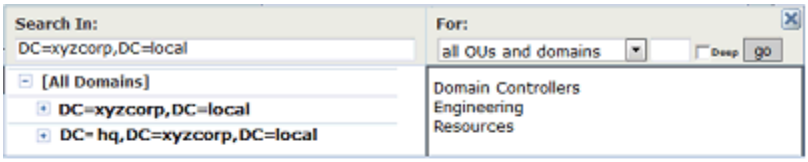
このセクションでは、AD マッピング ルールを定義する際に使用する AD オブジェクト ブラウザーについて、詳しく説明します。

AD オブジェクト ブラウザーの左パネルでは、検索の範囲を決定します。ここには AD ツリーが表示されます。一番上には「［All Domains（すべてのドメイン）］」があり、その下にはツリーの内容が標準的なブラウザーの形式で表示されます。他のオブジェクトを含むノードには [+] ボタンと [-] ボタンがあり、そこからツリーを展開、縮小できます。

右パネルには、[Active Directory Policy Rule（Active Directory ポリシー ルール）] パラメーターに入力した「Relationship（関係）」の値に基づいて検索対象が示されます。左パネルでツリー内のノードをクリックすると、そのノードの直下で「Relationship（関係）」（「OUs and domains」など）に一致するすべてのオブジェクトが右パネルに表示されます。右パネルでオブジェクトをクリックして選択し、[Rule Parameters（ルール パラメーター）] パネルに入力します。

オブジェクトの検索深度

ブラウザーの右上の領域に、「Deep（全階層）」と書かれたチェック ボックスがあります。[Deep（全階層）] ボックスをオンにしてから [**Go**（実行）] をクリックすると、複数レベル階層が実行され、選択したノードの直下だけでなく、そこに含まれるすべてのノードが階層の数に関係なく検索されます。次の B の例では、右パネルに表示されている結果の数が増えていることに注意してください。

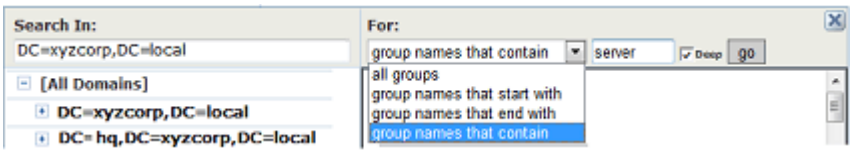


A. Results of a standard search in an AD domain

B. Results of a Deep search in the same domain

オブジェクトの文字列一致

AD オブジェクト ブラウザーのもう 1 つのオプションは、文字列一致による検索です。[Deep（全階層）] チェック ボックスのすぐ左にあるボックスに文字列を入力すると、選択したノード内にある、特定の文字列で始まる、終わる、またはそれを含む AD オブジェクトを検索できます。この文字列をどのように使用するかは、このテキスト ボックスの左にあるドロップダウン メニューで選択します。たとえば、テキスト ボックスに「eng」と入力し、この文字列を「group names that contain（グループ名に含む）」として検索すると、左パネルで選択したノードに「Engineering」および「System Engineering」グループがあった場合、この 2 つが一致します。



コンピューターの登録と AD マッピング

一部のイベントでは、Bit9 Server が実行されているコンピューターへのエージェントの登録がトリガーされます。その場合、次の条件が AD ポリシー マッピングに影響する可能性があります。

- Bit9 Agent が初めてインストールされたとき、コンピューターは、その時点でログオンしているユーザーを使用してサーバーに初めて登録されます。そのコンピューターが前回起動されてから誰もログオンしていない場合、Bit9 Server の作成するユーザー リストで、そのエージェント コンピューターの部分は空になります。
- エージェント コンピューターが再起動され、いずれかのユーザーがログインする前に Bit9 エージェントがサーバーに再接続すると、その登録のユーザー リストは空になります。
- すべてのエージェント コンピューターは（自動ポリシー割り当てを使用しているかどうかに関係なく）、ユーザー セッションのリストが変更されると再登録されます。
  プラットフォームに関する注意：Windows におけるセッションの取り扱い方法のために、Windows コンピューターにおけるユーザーのセッションは、ログアウトによって終了するとは限りません。他のユーザーのセッションに置き換えられるまで継続します。
- エージェント　コンピューターは、サーバーが再起動するたびにサーバーによって切断され、サーバーに再接続すると再登録されます。
- エージェント コンピューターのポリシー割り当てが手動で変更されるか、手動から自動に変更されると、サーバーは必ずコンピューターを切断（して再登録を強制）します。

サーバーの AD キャッシュのクリア

エージェント コンピューターをポリシーにマップするための AD 情報は、Bit9 Server にキャッシュされ、4 時間ごとに更新されます。また、AD マッピングに関係する Bit9 Security Platform ルールに変更が発生したときにも更新されます。

コンピューターまたはユーザーが属するグループの変更やコンピューターの追加などにより、AD サーバー上でこの AD 情報を変更した場合、通常は、次のスケジュールされたキャッシュ更新まで、その情報は Bit9 Server で利用可能になりません。重要な変更を行ったと考えられる場合や、ポリシー マッピングに誤りを発見した場合は、サーバーのキャッシュをクリアすることで、直ちに Bit9 Server で AD 情報の更新を開始することができます。

サーバーのキャッシュをクリアし、AD 情報を更新する手順：

- ［Policies（ポリシー）］ページの［Mappings（マッピング）］タブにある［Actions（アクション）］メニューで、［**Clear Server Cache**（サーバー キャッシュのクリア）］をクリックします。

Bit9 コンソールでの AD コンピューターの詳細の表示

AD と Bit9 Server を統合してある場合、AD ドメイン内のコンピューター名が Bit9 コンソールのテーブルに表示されているときは、そのコンピューター名をクリックして追加情報を表示できます。たとえば、［Events（イベント）］ページを表示

しているとき、一部のイベントには、そのイベントに関係するコンピューターが存在します。

その名前が AD コンピューター名ならば、青色でハイライト表示されます。これをクリックすると、[Computer Details（コンピューターの詳細）] ページが表示されます。このページで［**AD Details**（AD の詳細）］タブをクリックすると、そのコンピューターで取得できる AD 情報が表示されます。

コンソールのテーブルでハイライト表示されている AD ユーザー名をクリックすると、ユーザーに関する同様の情報が表示されます。

エージェント インストーラーのダウンロード

新しいポリシーを作成すると、Bit9 Server によってポリシー固有のエージェント インストーラーがエージェントのプラットフォームごとに作成され、エージェント ダウンロード領域に置かれます。各インストーラーでは、ポリシー、ポリシー設定、適用レベル、およびエージェントを管理するサーバーのアドレスが指定されます。

Bit9 Server をアップグレードすると、エージェント インストーラーも新しいバージョンにアップグレードされます。アップグレード計画に応じて、新しいバージョンのエージェントをダウンロードするか、Bit9 Server がアップグレードを管理することを許可します。詳細については、「Bit9 エージェントのアップグレード」（141 ページ）を参照してください。

注意

すべてのコンピューターに Active Directory を使用してポリシーを割り当てている場合、使用するインストーラーのポリシーで、[Automatic Policy Assignment for New Computers（新しいコンピューターへの自動ポリシー割り当て）] ボックスをオンにしてある必要があります。エージェントをコンピューターにインストールし、Bit9 Server に接続すると、そのコンピューターの正しい AD ベースのポリシーが自動的に割り当てられます。コンピューターが Bit9 Server に接続できないときは、エージェント インストーラーによるポリシーが引き続き適用されます。

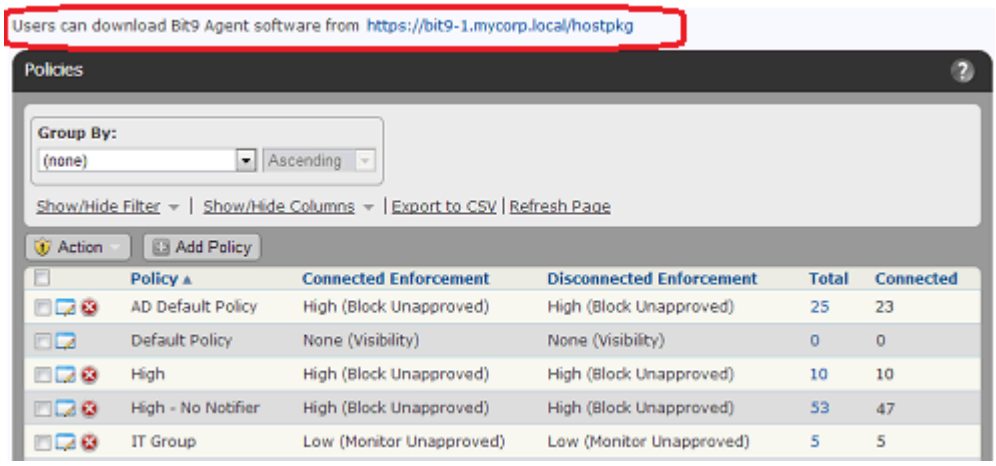
Bit9 エージェント インストーラーは、各プラットフォームに合わせて以下のファイル形式で作成されます。

- Windows: MSI（Microsoft インストーラー）パッケージ
- Mac OS X: DMG ファイル
- Linux: TGZ アーカイブ

これらのパッケージのダウンロード ページには、サーバーの URL を通じてアクセスします。この URL をブックマークしておくと、Bit9 コンソールにログインすることなくページにアクセスできます。

エージェント インストーラーのダウンロード手順：

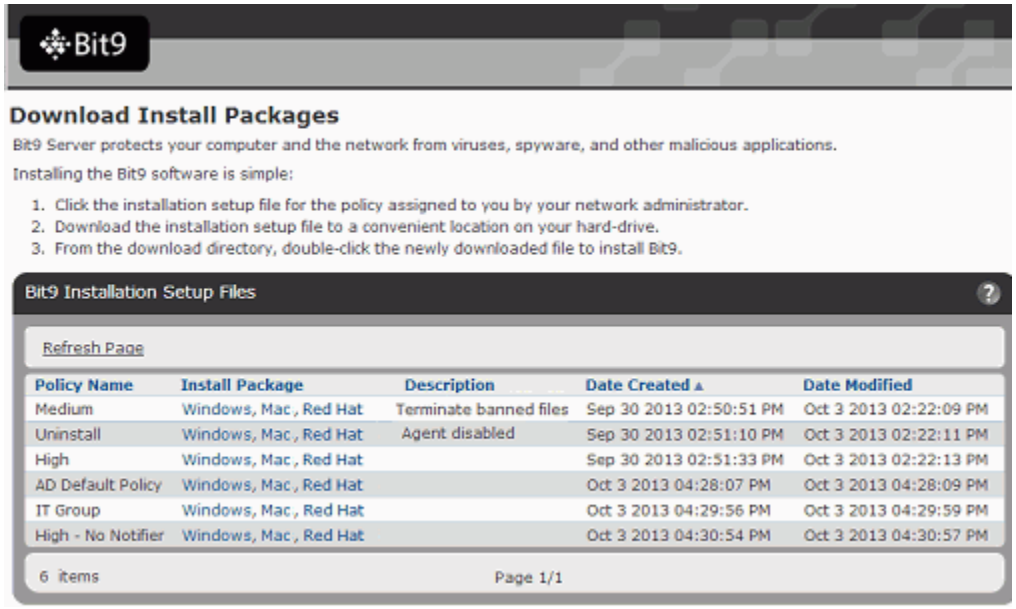
1. コンソール メニューで、[**Rules**（ルール）] > [**Policies**（ポリシー）] の順に選択します。[Policies（ポリシー）] ページが表示されます。



2. [Policies（ポリシー）] ページで、**Bit9 エージェント ソフトウェアをダウンロードする**ためのリンクをクリックします。このページの誰でもアクセスできる URL は、次のような形式です。

   `https://` サーバー名 `/hostpkg`

   [Download Install Packages（インストール パッケージのダウンロード）] ページが開きます。



3. [Bit9 Installation Setup Files（Bit9 インストール設定ファイル）] テーブルで、ポリシー名を使ってインストーラー ファイルを特定します。

4. インストーラーをダウンロードするには、エージェントをインストールするコンピューターのプラットフォーム名（Mac など）をクリックし、ファイルを保存します。
5. ダウンロードが完了し、エージェントをインストールする準備ができたら、次のセクション「Bit9 エージェントのインストール」の指示に従います。

Bit9 エージェントのインストール

Bit9 Agent のインストール プロセスは対話型ではなく、ユーザー入力は不要です。インストールが完了した直後から Bit9 エージェントは機能を開始します。追加の設定や再起動は不要です。

新しいエージェントのインストールの準備

どのプラットフォームでも、Bit9 エージェントをインストールする前に次の点を確認します。

- Bit9 エージェントがインストールされると、コンピューターは直ちにセキュリティ ポリシーによって保護され、エージェントはサーバーに接続してファイルの初期化を開始します。初期化によって Bit9 Server とその新しいクライアントとの間を流れるデータが増える可能性があるため、ネットワーク容量とファイルの数を考慮してエージェントの展開計画を立てます。大規模なネットワークで、すべてのコンピューターに同時にエージェントをインストールすることはお勧めしません。
- 初めて Bit9 Server を構成するときは、グローバルに承認する必要があるすべてのファイルを含む、参照コンピューターを設定することを検討してください。このコンピューターは、ファイル インベントリのドリフトを把握するためのベースラインとしても使用できます。
- Bit9 エージェントは、ユーザー単位ではなくシステム単位のアプリケーションです。
- エージェントをインストールするコンピューターとオペレーティング システムが、Bit9 エージェントでサポートされていることを確認します。エージェントのハードウェア要件については別途提供されている『運用環境の要件』ドキュメントを、現在のエージェントでサポートされている OS のバージョンについては『Supported Agent Operating Systems（サポートされているエージェントのオペレーティング システム）』を参照してください。
- システムにエージェントをインストールする方法を決定します。次に示すように、いくつかのオプションがあります。
  - 既存のソフトウェア展開メカニズムを利用する。　通常、新しいエージェントのインストールは非対話型モードで実行されますが、対話型のインストールをエンド ユーザーに提供することもできます。サードパーティの配布システムを使用して Bit9 エージェントをインストールする場合は、推奨されている手順に従います。Windows でのインストールでは、配布システム（SCCM など）内での MSI または MSP の変換をすべて無効にします。
  - システム管理者、または権限を与えられたその他の従業員が、エージェント ソフトウェアをユーザーの各コンピューターに手動でインストールする。

  - ユーザーに、自分自身でエージェント ソフトウェアをインストールすることを許可する。各ポリシーに関係するユーザーに、エージェントをダウンロードするための URL またはその他の共有場所にアクセスし、そのポリシー用のインストーラー ファイルをダウンロードして、各自のコンピューターでインストールを実行するようにメールで伝えます。操作は一切不要です。インストールはプロンプトなしで実行され、エージェントによるファイルの初期化が開始されます。

- Bit9 エージェント インストーラーは、適切な管理者権限を持つユーザーが実行する必要があります。Windows では、Local System アカウントか、管理者権限とロード可能なユーザー プロファイルを持つユーザー アカウントと考えられます。Mac と Linux では、sudo を使用できるユーザーである必要があります。
- ポリシーとプラットフォームに適合する正しいインストール パッケージをダウンロードするように注意します。「エージェント インストーラーのダウンロード」（131 ページ）を参照してください。AD ベースのポリシー割り当てを利用している場合、自動ポリシー割り当てを許可しているすべてのポリシーに対して、プラットフォーム固有の Bit9 エージェント インストーラーを使用できます。
- コンソールで作成するポリシーの名前には、無効であることが一般的に知られている文字は使用できませんが、各プラットフォームで特殊な処理（コマンド ラインでのエスケープなど）を必要とする文字がポリシー名に含まれていないことを確認してください。

Windows コンピューターへのエージェントのインストール

Bit9 エージェントの Windows インストーラーは MSI パッケージです。そのため、インストール ディレクトリなど、さまざまな設定を環境に合わせて変更することができます。構成オプションの詳細については、Microsoft MSI のドキュメントを参照してください。Windows 用のインストーラーは、次のようにポリシーによって異なる名前が付けられます。

- *policyname*.**msi**

注意

- Windows インストーラー トランスフォーム ファイル (.mst) は、Windows クライアント上の Bit9 エージェント インストーラーでは「サポートされません」。
- バージョン 7.2.3 から、Windows インストーラー パッチ ファイル (.msp) はビルド間のエージェント アップグレードには使用されなくなりました。
- Bit9 エージェント 7.2.3 は、Windows 2000、SP1 よりも前の Windows 2003 Server、または SP2 よりも前の Windows XP が実行されているシステムにはインストールできません。

Bit9 エージェントを Windows コンピューターに新規インストールする手順：

1. クライアント コンピューターで、選択した Windows Bit9 エージェント インストーラーを実行します。以下を考慮した上で、MSI ファイルをインストールするための標準的な方法のいずれかを使用します。

   a. Bit9 エージェント アプリケーションのデフォルトのディレクトリは、32 ビット システムでは **C:\Program Files\Bit9\Parity Agent**、64 ビット システムでは **C:\Program Files (X86)\Bit9\Parity Agent** です。インストール ディレクトリを変更するには、適切な MSI コマンド ライン オプションを使用して、コマンド ラインからインストールを実行します。

   b. デフォルトのアプリケーション　ディレクトリを受け入れる場合は、MSI ファイルの名前をダブルクリックするだけなど、すべての MSI インストール方法を使用できます。

2. Windows エージェントのインストール中は Bit9 インストーラーによってメッセージ ボックスが表示され、インストールが完了すると閉じられます。このボックスには［Cancel（キャンセル）］ボタンがあり、必要に応じて完了前にインストールを終了させることができます。

3. ウイルス対策ソフトウェアを実行している場合は、そのスキャン対象から Bit9 インストール ディレクトリを除外してください。セキュリティ強化のために、Bit9 にはアプリケーション ディレクトリを自己保護する機能があります。パフォーマンスの問題を避けるために、ウイルス対策ソフトウェア ベンダーから提供されているメカニズムを使用して、以下のファイルおよびディレクトリがスキャンまたはブロックされないように指定してください。

   - Bit9 エージェント プロセス **(Parity.exe)**
   - エージェント プログラムのディレクトリ（デフォルトは、32 ビット システムでは **Program Files\Bit9**、64 ビット システムでは **Program Files (x86)\Bit9**）
   - エージェント データ ディレクトリ（デフォルトは、Vista、Windows 7、Windows 2008 システムでは **ProgramData\Bit9\Parity Agent**、その他のサポート対象システムでは **\Documents and Settings\All Users\Application Data\Bit9\Parity Agent**）

4. Zone Alarm などのパーソナル ファイアウォールによって Bit9 エージェントが新しいアプリケーションと認識され、ネットワークへのアクセスがブロックされる可能性があります。Bit9 エージェントを実行するユーザーに対して、各自のコンピューターでアクセスを恒久的に許可するように指示してください。

Bit9 エージェントによって保護されているシステムでユーザーに対して何が表示されるかについては、第 17 章「ブロック通知と承認要求」を参照してください。

重要

- DFS を使用して Windows 2003 または Windows XP システムにエージェントをインストールする場合、Bit9 ファイルのルールをすべて適用するには、エージェント システムを再起動する必要があります。オペレーティング システムの制限により、システムを再起動するまで Bit9 エージェントは DFS の操作（ファイルの実行を含む）を検出できません。この場合は、［Computers（コンピューター）］ページの［Upgrade Status（アップグレード ステータス）］列に［Reboot Required（再起動が必要）］と表示されます。
- すべてのバージョンの Windows で、エージェント インストーラーが書き込みを試みたファイルが他のアプリケーションによって使用中の場合、システムはそのファイルを次の再起動時に置き換えるようにスケジュールし、コンソールではそのコンピューターに［Reboot Required（再起動が必要）］と表示されます。

エージェントがインストールされている Windows オペレーティング システムの更新

エージェントが実行されているシステムでオペレーティング システムの変更がサポートされるかどうかは、アップグレード前後の Windows のバージョンによって決まります。

- **Windows 10 よりも前のバージョンにおけるメジャー バージョンとマイナー バージョンの変更** – エージェントがインストールされているシステムで使用している Windows のメジャー バージョンまたはマイナー バージョンの変更は、Windows 10 よりも前のバージョンへのアップグレードではサポートされていません。たとえば、Windows 8.0 から Windows 8.1 へのアップグレードを、エージェントをアンインストールしてアップグレード後に再インストールすることなく実行することはサポートされていません。実行すると、正常性チェックが失敗し、場合によっては Windows のアップグレードが失敗します。
- **Windows 10 よりも前のバージョンにおけるサービス パック** – Windows 10 よりも前のリリースに対するサービス パックによるアップグレードは、エージェントがインストールされたままでもサポートされ、正常性チェックは失敗しません。
- **Windows 10** – Windows 10 へのアップグレード、および Windows 10 のいずれかのバージョンから別のバージョンへのアップグレードに関する現在の要件については、下記の『Carbon Black User eXchange』を参照してください。

  https://community.carbonblack.com/thread/3367

Mac コンピューターへのエージェントのインストール

Mac コンピューターでは、適切なインストーラー DMG ファイルを使用して Bit9 エージェントをインストールします。Mac 用のインストーラーは、次のようにポリシーによって異なる名前が付けられます。

- *policyname*-***mac.dmg***

> **注意**
>
> Bit9 では、このリリースの『Supported Agent Operating Systems（サポートされているエージェントのオペレーティング システム）』にリストされているシステムにのみエージェントをインストールできます。

「エージェント インストーラーのダウンロード」（131 ページ）で説明されているとおりに、オペレーティング システムとポリシーに適合する正しいエージェント インストール パッケージをダウンロードしてください。AD ベースのポリシー割り当てを利用している場合、自動ポリシー割り当てを許可しているすべてのポリシーに対してエージェント インストーラーを使用できます。ダウンロードした同じエージェント インストーラーを複数のエンドポイントに対して使用できます。また、SSH や Casper などの配布メカニズムを利用してエンドポイントに配布することもできます。

Bit9 エージェントを Mac コンピューターに新規インストールする手順：

1. ターミナル ウィンドウを開き、インストールをダウンロードしたディレクトリ（デフォルトでは各ユーザーのダウンロード ディレクトリ）に移動します。

   ```
   cd ~/Downloads
   ```

2. インストールを開始するには、ダウンロードしたエージェント インストール ファイル、*policyname*`-mac.dmg` をダブルクリックします。標準のパッケージ インストール ダイアログが開きます。

3. インストール ダイアログのプロンプトに応答し、インストールが成功したとダイアログに表示されたら［**Close**（閉じる）］をクリックします。直ちにエージェントが動作を開始します。

4. ウイルス対策ソフトウェアを実行している場合は、そのスキャン対象から Bit9 インストール ディレクトリを除外してください。セキュリティ強化のために、Bit9 にはアプリケーション ディレクトリを自己保護する機能があります。パフォーマンスの問題を避けるために、ウイルス対策ソフトウェア ベンダーから提供されているメカニズムがあれば、それを使用して、以下のディレクトリがスキャンまたはブロックされないように指定してください。

   - **/Applications/Bit9/Daemon/b9daemon** – Bit エージェント プロセス
   - **/Applications/Bit9** – Bit9 プログラム ディレクトリ
   - **/Library/Caches/com.bit9.agent** – Bit9 データ ディレクトリ
   - **/Library/Extensions/b9kernel.kext** – バージョン 10.9 (Mavericks) 以降の OS X での Bit9 ドライバーの場所
     または

/System/Library/Extensions/b9kernel.kext – バージョン 10.9 よりも前の OS X での Bit9 ドライバーの場所

5. Mac ファイアウォールによって Bit9 エージェントが新しいアプリケーションと認識され、ネットワークへのアクセスがブロックされる可能性があります。ユーザーに対して、**b9daemon** への接続を恒久的に許可するように指示してください。

Bit9 エージェントによって保護されているシステムでユーザーに対して何が表示されるかについては、第 17 章「ブロック通知と承認要求」を参照してください。

Linux コンピューターへのエージェントのインストール

注意

Linux の場合、このリリースの『Supported Agent Operating Systems (サポートされているエージェントのオペレーティング システム)』にリストされているバージョンとカーネルにのみエージェントをインストールできます。場合によっては、最新リリースのサーバー用のバージョンが開発中で、以前のバージョンのエージェントが推奨されることもあります。使用する Bit9 Platform のバージョンのリリース ノートとエージェントを参照して、特別な考慮事項を確認してください。

Linux コンピューターでは、適切な TGZ アーカイブを解凍し、スクリプトを実行することによって Bit9 エージェントをインストールします。Bit9 7.2.3 では、Red Hat バージョンまたは CentOS バージョンを実行している Linux コンピューターで、エージェントのインストールがサポートされます。この 2 つには同じインストール ファイルが使用されます。インストール ファイルは、次に示すようにポリシーとオペレーティング システムによって名前が決定される tarball です。

- *policyname-**redhat.tgz***

RedHat および CentOS コンピューターでは、エージェントをインストールする前に Prelinking を無効にすることをお勧めします。Prelinking は Bit9 機能のパフォーマンスを低下させます（リリース ノートを参照してください）。RedHat または CentOS システムで Prelinking を有効にする必要がある場合は、エージェントをインストールする前に RedHat Prelinking アップデーターを有効にします。アップデーターを有効にする手順については、「アップデーターによる承認」(300 ページ) を参照してください。

注意

エージェントの初期インストールでは不要ですが、Linux で Bit9 Server がエージェントのアップグレードを実行するには、**gawk** と **unzip** が必要です。必要に応じて、これらを含めるためにエージェントのインストール前に Linux ディストリビューションをアップデートしてください。

Bit9 エージェントの通常のインストールでは、GUI ベースのブロック ファイルの通知が設定されます。この通知は、Bit9 によって完全にブロックされているアクション、または続行するためにはユーザーの判断が必要なアクションをユーザーが実行しようとしたときに表示されます。グラフィック インターフェイス パッケージが実行されていない Linux システムの場合、または何らかの理由でユーザーによる介入を避ける場合は、通知なしで Linux 用の Bit9 エージェントをインストールすることができます。この **-n** オプションは、エージェントのインストール スクリプト コマンドに対するフラグとして追加でき、この後の手順で説明します。

通知なしで実行することを選択したシステムでは、ポリシーの適用レベルを低または高にしてエージェントをインストールする必要があります。ポリシーの適用レベルを中にすると、さまざまなアクションの許可またはブロックをユーザーに求めるプロンプトが発生しますが、このプロンプトには通知が必要です。

「エージェント インストーラーのダウンロード」で説明されているとおりに、オペレーティング システムとポリシーに適合する正しいエージェント インストール パッケージをダウンロードしてください。AD ベースのポリシー割り当てでは、自動ポリシー割り当てを有効にしてあるポリシーに対しては、必ずエージェント インストーラーを使用します。

Bit9 エージェントを Linux コンピューターに新規インストールする手順：

1. エージェントをインストールするユーザーのアカウントに管理者権限があるか、そのユーザーが **sudo** を使用できることを確認します。
2. このコンピューター用に選択したポリシーのエージェントの tarball アーカイブを解凍、展開します。スペースや括弧など、コマンド引数で受け入れられない文字がポリシー名に含まれている場合は、円記号でエスケープします。

   ```
   tar -xvzf <policyname>-redhat.tgz
   ```

3. ダウンロードした tarball の名前のディレクトリに移動します。

   ```
   cd <policyname>-redhat
   ```

4. 任意のシェルを使用して、sudo でエージェントのインストール シェル スクリプトを実行します。ブロック ファイルの通知をインストールしない場合は、**-n** オプションを追加します。たとえば、Bourne シェルを使用してエージェントをインストールするには、次のようにします。

   ```
   sudo sh ./b9install.sh
   ```
   – 通知なしでインストールする場合は、次のようにします。–
   ```
   sudo sh ./b9install.sh -n
   ```

5. ウイルス対策ソフトウェアを実行している場合は、そのスキャン対象から Bit9 インストール ディレクトリを除外してください。セキュリティ強化のために、Bit9 にはアプリケーション ディレクトリを自己保護する機能があります。パフォーマンスの問題を避けるために、ウイルス対策ソフトウェア ベンダーから提供されているメカニズムがあれば、それを使用して、以下のディレクトリおよびファイルがスキャンまたはブロックされないように指定してください。
   - **/opt/bit9/bin** – Bit9 エージェントのアプリケーションおよびアンインストール スクリプト
   - **/srv/bit9/data** – Bit9 エージェントのデータベースおよび診断ログ

- **/lib/modules/***kernelversion***/kernel/lib/b9kernal.ko** – Bit9 エージェント カーネル
- **/etc/rc*/*b9daemon** および **/etc/init.d/b9daemon** – Bit9 エージェント起動スクリプト
- **/etc/X11/xinit/xinitrc.d/90b9notifier.sh** – Bit9 ブロック ファイル通知

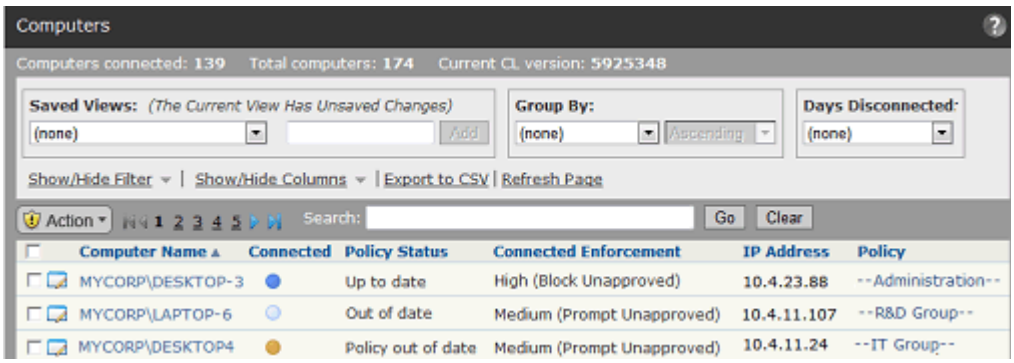
6. ファイアウォールによって Bit9 ソフトウェアが新しいアプリケーションと認識され、ネットワークへのアクセスがブロックされる可能性があります。Bit9 エージェントを実行するユーザーに対して、アクセスを恒久的に許可するように指示してください。

Bit9 エージェントによって保護されているシステムでユーザーに対して何が表示されるかについては、第 17 章「ブロック通知と承認要求」を参照してください。

インストールの検証

接続されているコンピューターでエージェントが実行され、サーバーから認識できることを検証する手順：

1. コンソール　メニューで、[**Assets**（アセット）] > [**Computers**（コンピューター)] の順に選択します。
2. エージェント ソフトウェアが実行されているすべてのコンピューターが一覧表示されている［Computers（コンピューター）］ページで、確認するそれぞれのシステムの名前または IP アドレスを調べます。［Search（検索)］ボックスを使用して、目的のコンピューターを見つけることができます。



3. コンピューターのポリシーに注目します。Active Directory によって割り当てられたポリシーには、名前の前後にダッシュが置かれています。また、[Connected（接続済み)］および［Policy Status（ポリシー ステータス)］列を見て、マシンが最新状態になっているかどうかを判断します。

> **注意**
> 新しくインストールしたエージェントに関するファイル初期化の実行中も、コンピューターは既にそのポリシーの適用レベルで保護されています。

エージェント コンピューターへのインストールの検証

Bit9 エージェントが存在していることは、エージェント コンピューターでローカルに検証することもできます。

- Windows コンピューターでは、**タスク マネージャー**を開いて［**サービス**］タブをクリックします。**B9Daemon** が実行されていることを確認できるはずです。
- Mac コンピューターでは、**アクティビティモニタ**を実行し、［**すべてのプロセス**］を表示します。**b9daemon** が実行されていることを確認できるはずです。
- Linux コンピューターでは、コマンド ウィンドウで **ps aux | grep b9** を使用します。**b9daemon** が実行されていることを確認できるはずです。

Bit9 エージェントのアップグレード

Bit9 Server のアップグレードには、新しいバージョンの Bit9 エージェントも含まれています。エージェントのアップグレードには、次のように示すようにいくつかの方法があります。

- ポリシー単位でエージェントの自動アップグレードを有効にして、サーバーによるアップグレード プロセスの管理を許可する。
- 1 台または複数の特定のコンピューターで、Bit9 コンソールからエージェントのアップグレードを実行する。
- エージェント マシンで、エージェントを手動でアップグレードする。
- 標準的なソフトウェア配布システムを使用してアップグレードを管理する。

注意

サーバーから Linux エージェントのアップグレードを実行するには、エージェント システムに **gawk** と **unzip** が存在していることが必要です。インストール済みでない場合は、エージェントのアップグレードを有効化または開始する前に、これらを含めるために Linux ディストリビューションを更新してください。

アップグレードしないエージェントの機能上の制約

以前の Bit9 エージェントも、バージョン 6.0 以降であれば引き続き実行することができ、全面的にパッチが提供されます。ただし、できるだけ早くエージェントをアップグレードする必要があります。6.x のエージェントをアップグレードしないと、Bit9 Security Platform 7.2.3 の機能の一部は完全には機能せず、次のように過渡的な機能が使用されます。

- **カスタム スクリプト ルール**は、7.0 よりも前のエージェントでは機能しません。
- 書き込み無視ルールに対して**書き込み追跡の例外**を指定する**カスタム ルール**は、7.0 よりも前のエージェントでは機能しません。
- 7.0 よりも前のエージェントが実行されているコンピューター上のブロック ファイルの通知には、**承認要求**機能が含まれません。7.0 のエージェントが実

行されている場合は、この機能により、ブロック ファイルの承認要求を送信できます。

- **ファイル レピュテーションに基づく承認**は、7.0 よりも前のエージェントでは直接利用することはできません。ただし、レピュテーションに基づく承認が有効なファイルへのアクセスを 7.0 エージェントが要求すると、Bit9 Server は承認リストを更新し、「すべての」エージェント（7.0 よりも前のエージェントも含む）は、その構成リストがサーバーによって更新されたとき、その承認を受け取ります。
- **公開者のレピュテーションに基づく承認**は、7.0 よりも前のエージェントでは利用できません。
- 一部の**デバイス管理機能**は、7.0 よりも前のエージェントでは使用できません。たとえば、7.0 よりも前のエージェントでは特定のデバイス タイプを禁止することはできません。また、7.0 よりも前のエージェントで検出されたデバイスは、［Device Catalog（デバイス カタログ）］には表示されますが（一意の場合）、［Devices on Computers（コンピューター上のデバイス）］リストには表示されません。さらに、7.0 以降のエージェントではマウントされている「すべての」デバイスがサーバーにレポートされますが、7.0 よりも前のエージェントでレポートされるのは、そのバージョンの Bit9 によって検出がサポートされているデバイスのみです。これは、主に USB デバイスと iPod（iPod でファイルシステムの検出が有効になっている場合）を意味します。
- **カタログ ベースの（デタッチされた証明書）公開者の承認**は、7.0 よりも前のエージェントが管理するファイルでは使用できません。レピュテーション ベースの承認と同じように、カタログから承認されるファイルに 7.0 エージェントがアクセスすると、その承認は 7.0 よりも前のエージェントにも有効になります。
- 証明書を個別に追跡、承認、および禁止する機能など、一部の**証明書管理機能**は、7.0.1 よりも前のエージェントでは利用できません。
- **禁止イメージを含むプロセスを終了する**、すなわち禁止イメージの実行を防ぐだけでなく、現在実行中のものがあれば終了するようにポリシーを構成する機能は、7.2 よりも前のエージェントでは無効です。
- その他にも、パフォーマンスおよびセキュリティに関する拡張が Bit9 Security Platform の各リリースに実装されていますが、その一部は 7.2.3 よりも前のエージェントでは利用できません。

Bit9 コンソールでは、以前のバージョンのエージェントが存在することで、そのページで表示されるデータや実行できるアクションが影響を受ける場合、メッセージが表示されます。

自動エージェント アップグレードの有効化

Bit9 Server のアップグレード プロセスでは、エージェントの自動アップグレードをトリガーするフラグは［Disabled（無効）］に設定されています。これにより、クライアント コンピューター上のエージェントをアップグレードする前にサーバーのアップグレードを検証することができます。サーバーをアップグレードしたら、次の手順に従って、サーバーに接続されているシステム上のエージェントの自動アップグレードを有効化します。

- 今すぐエージェントをアップグレード「しない」すべてのポリシーについて、［Add/Edit Policy（ポリシーの追加 / 編集）］ページの［Options（オプション）］

セクションで［**Allow upgrades**（アップグレードを許可)］ボックスが「オフ」になっていることを確認します。

- メンバーのエージェントをアップグレードするすべてのポリシーについて、［Add/Edit Policy（ポリシーの追加 / 編集)］ページの［Options（オプション)］セクションで［**Allow upgrades**（アップグレードを許可)］ボックスをオンにします。これは、大量のエージェントに対して同時に実行しないでください（下記の注意を参照)。
- ［System Configuration（システム構成)］ページの［Advanced Options（高度なオプション）］タブで、［**Automatic Agent Upgrades**（自動エージェント アップグレード)］をオンにします。

重要

- システム全体に対してエージェントのアップグレードを再有効化する場合は、今すぐアップグレードしないポリシーのアップグレードをあらかじめ無効にしておきます。
- 大量のエージェントを同時にアップグレードすると、システムのパフォーマンスが低下する可能性があります。エージェントをまとめてアップグレードする際のベスト プラクティスについては、サポートにご相談ください。
- Bit9 Server をあるメジャー バージョンから別のメジャー バージョン（たとえば、v7.0.0 から v7.2.3）にアップグレードすると、追跡対象ファイルの識別機能に対する継続的な機能強化により、エージェントで管理するすべてのコンピューターの固定ドライブの再スキャンが必要になります。このようなアップグレードでは、以前は無視され、現在は追跡の対象と見なされているファイルがあるかどうかを判断するために、信頼できるディレクトリに新しいファイル インベントリを作成することも必要になります。このプロセスにはエージェントの初期化のときと同じアクティビティが必要であり、大量の入出力アクティビティが発生することがあるため、エージェントとファイルの数によって数分から数時間かかる可能性があります。
  Bit9 Server によって管理されるアップグレードとサードパーティの配布方法を使用するアップグレードでは、ネットワークおよびサーバーのパフォーマンスに対する容認できない影響を回避するために、エージェントを段階的にアップグレードすることを推奨します。

Bit9 コンソールからの直接アップグレード

サーバーの定期的なメンテナンスの一部としてエージェントの自動アップグレードが行われるように、コンソールで「有効化」できますが、コンソールからエージェントのアップグレードを「強制的に」実行することもできます。この機能を使用するには、次の条件が必要です。

- ［System Administration（システム管理)］ページの［Advanced Options（高度なオプション)］タブで、［Automatic Agent Upgrades（自動エージェント アップ

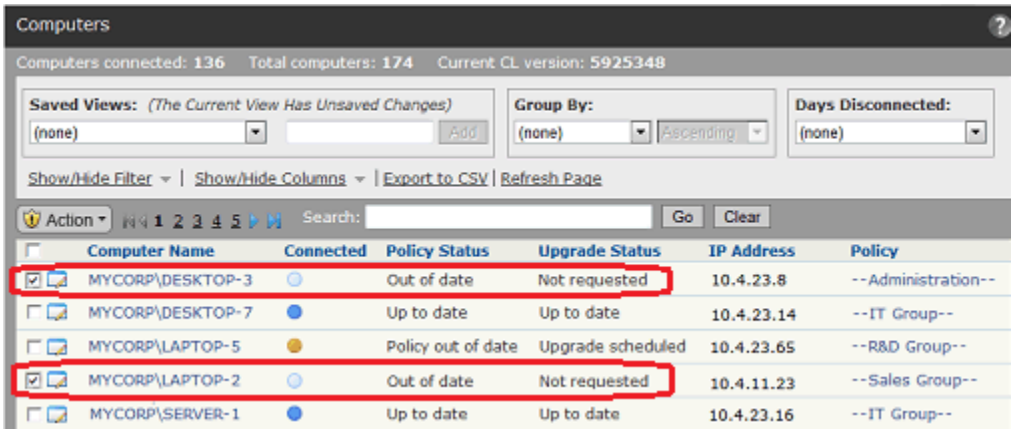
グレード）］が有効になっていること。［Upgrade Computers（コンピューターのアップグレード)］という選択肢は、有効にしない限りメニューに表示されません。

- エージェントは少なくともバージョン 6.0.0 である必要があります。これよりも以前のバージョンからのアップグレードはサポートされていません。

この方法は、接続済みのエージェントに関しては、インストーラー ファイルからアップグレードを実行するのと同じ意味を持ちます。コンソール ベースの「即時」アップグレードの際に接続されていないエージェントは、次に接続したときにアップグレードされます。

コンソールから 1 つ以上のエージェントを直ちにアップグレードする手順：

1. コンソールで、［**Administration**（管理)］>［**System Configuration**（システム構成）］の順に選択し、［**Advanced Options**（高度なオプション）］タブをクリックします。
2. ［Advanced Options（高度なオプション）］タブで［Automatic Agent Upgrades（自動エージェント アップグレード)］フィールドが［Disabled（無効)］の場合は、［**Edit**（編集)］ボタンをクリックし、［Automatic Agent Upgrades（自動エージェント アップグレード)］メニューから［**Enabled**（有効)］を選択してから、［**Update**（更新)］をクリックして変更します。
3. コンソール　メニューで、［**Assets**（アセット）］>［**Computers**（コンピューター)］の順に選択します。
4. アップグレードするコンピューターを特定し、名前の隣のチェック ボックスをオンにします。［Upgrade Status（アップグレード ステータス)］で、そのコンピューターがアップグレード可能であり、まだ最新状態になっていないことを確認します。



5. ［Action（アクション）］メニューで、［**Upgrade Computers**（コンピューターのアップグレード)］コマンドを選択します。

6. 確認ダイアログで [**OK**] をクリックしてアップグレードを開始します。テーブルに表示されているコンピューターの説明を見て、変更の完了を確認します。

エージェントの手動アップグレード

接続されていないシステムの場合、または SCCM や Altiris などのソフトウェア配布システムを使用してアップグレードを配布している場合は、エンドポイントまたは配布サーバーに Bit9 エージェント インストール ファイルを配布する必要があります。

Bit9 エージェントのインストール ファイルは、32 ビット システムでは **Program Files\Bit9\Parity Server\hostpkg**、64 ビット システムでは **Program Files (x86)\Bit9\Parity Server\hostpkg** の Bit9 Server に置かれます。

Windows エージェントの手動アップグレード

バージョン 7.2.3 から、Windows エージェントの「すべての」手動アップグレードには **ParityHostAgent.msi** を使用します。これには、6.0.0 から 7.2.2 までのバージョンからのアップグレードも、以前の 7.2.3 リリースのビルド間アップグレード（7.2.3.546 から 7.2.3.760 など）も含まれます。7.2.3 以前は、ビルド間アップグレードには MSP が使用されていましたが、今後は不要であり、サポートもされません。

重要

- 手動アップグレードは、Local System アカウントか、管理者権限とロード可能なユーザー プロファイルを持つユーザー アカウントによって実行する必要があります。
- 手動アップグレードでは、MSIEXEC　コマンドの中でインストーラーへの完全なパスを使用する必要があります。

以前のバージョンから v7.2.3 へのエージェントのアップグレードを Bit9 Server で管理すると、エージェントはルールの新しいリストを受け取ります。手動アップグレードで、リリース バージョン番号の上位 3 つの数字のいずれかが変更される場合、新しいルールを含むファイル **configlist.xml** を、エージェント インストーラーがアクセスできる場所にコピーする必要があります。これには、サードパーティの配布方法を利用するインストールも含まれます。Bit9 Server では、このファイルはエージェント インストーラーと同じ **hostpkg** フォルダーにありますが、［Downloads（ダウンロード）］ページにリンクはありません。インストーラー内で、URL またはパスを使用してコピーまたは参照する必要があります。

次の手順は、エージェントのメジャー アップグレード（番号の上位 3 つの数字のいずれかが変わる）の場合に適用されます。7.2.3 リリースのビルド間アップグレードでは、configlist.xml ファイルをコピーする必要はありません。ビルド間アップグレードの場合は、「Windows エージェントのビルド間アップグレード」（147 ページ）に進んでください。

Windows エージェントのメジャー アップグレードを手動で、またはソフトウェア配布によってインストールする手順：

1. インストーラーをダウンロードする先のコンピューターのコンソールにログインします。
2. コンソール メニューで、［**Rules**（ルール）］>［**Policies**（ポリシー）］の順に選択し、［Policies（ポリシー）］ページ上部で、エージェント ソフトウェアをダウンロードするためのリンクをクリックします。
3. Bit9 エージェントのアップグレード インストーラー ファイル **ParityHostAgent.msi** を、アップグレードを実行または配布するための場所にダウンロードします。

   このインストーラーは、Bit9 コンソールの［Downloads（ダウンロード）］ページのリストには含まれていません。パスの末尾のファイル名を置き換えることで、URL、UNC パスなど、ファイルを取得するための標準的な手段を使用してダウンロードを実行できます。

   たとえば URL を使用するには、コンソールで［**Rules**（ルール）］>［**Policies**（ポリシー）］の順に選択し、ページ上部にあるダウンロード リンクをクリックして、次のようにダウンロード ページの URL を編集します。
   https://<*bit9servername*>**/hostpkg/pkg.php?pkg=**<*installerfile*>
4. ブラウザーの［保存］オプションを選択します。
5. 同じ手順を使用して、エージェント インストーラーがアクセスできる場所に v7.2.3 のルール リスト **configlist.xml** をダウンロードします。または、エージェント インストール システムが Bit9 Server の hostpkg フォルダーにアクセスできることを確認します。URL を使用するには、ファイルをダウンロードする先のコンピューターのブラウザーで次のように入力します。
   https://<*bit9servername*>**/hostpkg/pkg.php?pkg=configlist.xml**

   注意：エージェントのアップグレードにコマンド ライン引数を使用する場合、configlist.xml をダウンロードする必要はありません。上記の URL をコマンド ラインの引数として使用します。ステップ 7 を参照してください。
6. 1 台のコンピューターを手動でアップグレードする場合は、configlist.xml ファイルを Bit9 エージェントのデータ フォルダー（通常は **C:\ProgramData\Bit9\Parity Agent**）に移動し、**ParityHostAgent.msi** などのインストーラーを実行します。

7. サードパーティの配布システムを通じてエージェントをアップグレードする場合は、そのシステムを使用して configlist.xml ファイルをすべてエージェントのエージェント フォルダーに配布するか、MSIEXEC でコマンド ライン引数を使用することで新しいルール ファイルをアップグレード インストールに含めます。ParityHostAgent.msi を使用したこのようなアップグレードの場合、コマンド ラインは次のようになります。

   ```
   msiexec /i <path>\ParityHostAgent.msi B9_CONFIG=
   https://<bit9serverIP>/hostpkg/pkg.php?pkg=
   configlist.xml /L*v+ c:\ParityHostAgentUpgrade.log
   ```

   コマンドの中で URL、UNC パス、またはローカルの完全パスを使用して configlist.xml の場所を指定できます。相対パスや、パスのないファイル名のみは使用できません。

Windows エージェントのビルド間アップグレード

ビルド間アップグレードは、バージョンの上位 3 つの数字がいずれも変わらないアップグレードです。たとえば、7.2.3.345 から 7.2.3.678 はビルド間アップグレードです。このようなアップグレードは、「ホット フィックス」と呼ばれることもあり、通常は 1 つまたは複数の特定の問題に対処するために、計画されたリリースの間に行われます。特定の顧客のみに提供されることもあります。

このタイプのエージェント データを受け取る場合は、標準的なインストール指示よりも優先される、またはそれを補足する特別な指示が付属していることがあります。以下のステップでは、Windows エージェントのビルド間アップグレードの一般的な手順を説明します。

Windows エージェントのビルド間アップグレードを手動で、またはソフトウェア配布によってインストールする手順 :

1. 受け取ったエージェントのアップグレード インストーラー ファイルを、アップグレードを実行または配布するための場所にダウンロードまたはコピーします。
2. 1 台のコンピューターを手動でアップグレードする場合は、新しいエージェント用に提供されたインストーラーを実行します。インストーラーは、必ずLocal System アカウントか、管理者権限とロード可能なユーザー プロファイルを持つユーザー アカウントで実行します。次のコマンドを使用します。

   ```
   msiexec /fvamus <fullpath>\<agentinstallername>.msi /L*v
   <fullpath>\<logfilename>
   ```

   MSIEXEC コマンドを使用したインストールでは、ローカルの完全なパスを使用する必要があります。
3. サードパーティの配布システムを通じてエージェントをアップグレードする場合は、前のステップで示したように MSIEXEC でコマンド ライン引数を使用できます。

Mac エージェントの手動アップグレード

Bit9 Server のアップグレードが完了したら、v7.2.0 以降の Mac エージェントをダウンロードして、手動で新しいバージョンにアップグレードできます。

注意

v7.0.1 エージェントから v7.2.3 エージェントへの手動アップグレードはサポートされていません。v7.0.1からのアップグレードで、サーバー管理によるアップグレードを使用できない場合は、v7.0.1 エージェントをアンインストールしてから、新しい v7.2.3 エージェントをインストールします。

7.2.0 以降の Mac エージェントを手動アップグレードする手順：

1. エージェントの［Tamper Protection（改ざんからの保護)］を無効にするか、無効モードのポリシーにエージェントを移動します。
2. Bit9 コンソールで、［**Rules**（ルール)］>［**Policies**（ポリシー)］の順に選択し、［Policies（ポリシー）］ページ上部で、エージェント ソフトウェアをダウンロードするためのリンクをクリックします。
3. Mac エージェントのアップグレード インストーラー**Bit9MacInstall.bsx** をダウンロードします。

   これには、URL、UNC パスなど、ファイルを取得するための標準的な手段を使用します。このインストーラーは、Bit9 コンソールの［Downloads（ダウンロード)］ページのリストには含まれていません。

   URL を使用するには、コンソールで［**Rules**（ルール）］>［**Policies**（ポリシー）］の順に選択し、ページ上部にあるダウンロード リンクをクリックして、次のようにダウンロード ページの URL を編集します。

   https://<*bit9serverIPaddress*>**/hostpkg/pkg.php?pkg=Bit9MacInstall.bsx**
4. ターミナル ウィンドウを開き、インストールをダウンロードしたディレクトリ（デフォルトでは各ユーザーのダウンロード ディレクトリ）に移動します。

   ```
   cd ~/Downloads
   ```
5. 次のコマンドを入力してエージェントをインストールします。

   ```
   sudo bash Bit9MacInstall.bsx
   ```

Linux エージェントの手動アップグレード

Bit9 Server のアップグレードが完了したら、アップグレードされた Bit9 エージェントを Linux システムにダウンロードしてインストールできます。ほとんどのエンドポイントでは、通知アップグレード インストーラーもダウンロードして実行する必要があります。

Linux エージェントを手動アップグレードする手順：

1. エージェントの［Tamper Protection（改ざんからの保護)］を無効にするか、無効モードのポリシーにエージェントを置きます。

2. Bit9 コンソールで、[**Rules**（ルール）] > [**Policies**（ポリシー）] の順に選択し、[Policies（ポリシー）] ページ上部で、エージェント ソフトウェアをダウンロードするためのリンクをクリックします。
3. Linux 用のエージェント アップグレード インストーラー **bit9redhat6install.bsx** または **bit9redhat6install.bsx** をクライアント コンピューターにダウンロードします。

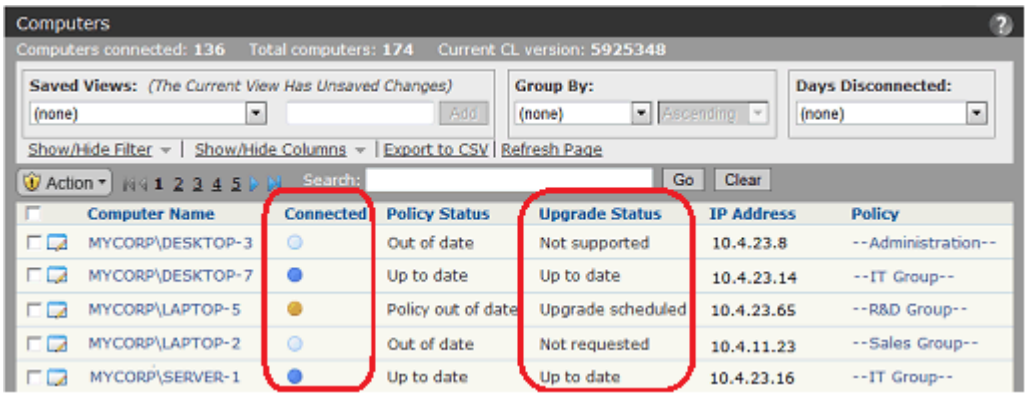
   このインストーラーは、Bit9 コンソールの [Downloads（ダウンロード）] ページのリストには含まれていません。ダウンロードには、URL、UNC パスなど、ファイルを指定するための標準的な構文を使用します。URL を使用するには、コンソールで [**Rules**（ルール）] > [**Policies**（ポリシー）] の順に選択し、ページ上部にあるダウンロード リンクをクリックして、次のようにダウンロード ページの URL を編集します。

   https://*<bit9servername>***/hostpkg/pkg.php?pkg=bit9redhat***{6,7}***install.bsx**
4. クライアント コンピューターで、コマンド ラインからエージェント アップグレード インストーラーを実行します。

   ```
   sudo bash -U bit9redhat{6,7}install.bsx
   ```

エージェント アップグレード ステータス

アップグレード プロセスを簡単に管理できるように、Bit9 コンソールの [Computers（コンピューター）] ページには [Upgrade Status（アップグレード ステータス）] 列が用意されています。このページではさらに、最新のエージェントを実行しているコンピューターと前のバージョンを実行しているコンピューターを視覚的に識別することもできます。このページでは、以前のエージェント バージョンを実行しているコンピューターはオレンジのドットが、最新のエージェントを実行しているコンピューターは青のドットがそれぞれ [Connected（接続済み）] 列に表示されます。



また、[Computers（コンピューター）] テーブルの [Upgrade Status（アップグレード ステータス）] 列には、各エージェントのアップグレード プロセスの進行とともに、そのステータスに関するより詳細な説明が表示されます。クライアントのアップグレード プロセスがすべて完了すると、クライアントの [Upgrade Status（アップグレード ステータス）] と [Policy Status（ポリシー ステータス）] が [Up to Date（最新）] に変わります。[Upgrade Status（アップグレード ステータス）] で使用できる値を表 13 に示します。

アップグレードされた Bit9 エージェントは直ちに実行を開始します。通常、エージェント コンピューターを再起動する必要はありませんが、[Upgrade Status（アップグレード ステータス）] に［Reboot Required（再起動が必要）］と表示されることもあります。

- 一部の Windows XP/2003 システムは、プロセスの順序を整え、DFS を使用しているシステムでルールが確実に適用されるように、アップグレード後に再起動する必要があります。
- すべてのバージョンの Windows で、エージェント インストーラーが書き込みを試みたファイルが他のプロセスによって使用中の場合、コンピューターが前のバージョンのファイルを最新バージョンに置き換えられるように、コンピューターを再起動する必要があります。

表 13：アップグレード ステータス メッセージ

アップグレード ステータス	説明
Not Requested（要求なし）	エージェントはアップグレード可能ですが、このポリシーのアップグレードは有効化されていないか、アップグレードがグローバルに無効化されています。
Upgrade waiting（アップグレード待機中）	エージェントはアップグレード可能であり、アップグレードが許可されたポリシーに属しています。サーバーによるスケジュールを待機中です。
Upgrade scheduled（アップグレード スケジュール済み）	エージェントのアップグレードがスケジュールされているか、コンピューターにアップグレード パッケージがダウンロードされて実行はされていない状態です。サーバーでは、エージェント アップグレード パッケージが「いつ」ダウンロードされ実行されるかは追跡されません。
Upgrade requested（アップグレード要求済み）	このコンピューターのエージェント アップグレードが Bit9 コンソールから要求されました。
Reboot required（再起動が必要）	エージェントはアップグレードされ、再起動を待機中です。再起動は、一定の条件の下でのみ必要とされます（上記の注意を参照）。
Not supported（サポート外）	Windows 2000、または 7.2 をサポートしていないその他のオペレーティング システムでエージェントが実行されているため、エージェントをアップグレードできません。

アップグレード ステータス	説明
Upgrade blocked（アップグレード禁止）	エージェントの構成リストに問題があります。最新状態になっていないか、アップグレードを実行するために必要な値が少なくとも 1 つ不足しています。たとえば、Bit9 Server との通信に使用されるポートの番号が期限切れになっている場合です。構成が最新状態になっていない場合、サーバーからエージェントをアップグレードすることはできませんが、他の手段でアップグレードすることはできます。ほとんどの場合は、ユーザーが介入しなくても一定の時間が経過すれば、接続されているエージェントの構成リストは必要なバージョンになります。エージェントのアップグレードに高い優先順位を与える（[Action（アクション）] メニューの［Computer Details（コンピューターの詳細）］ページ）ことで、構成リストの更新を早くすることができます。それでもエージェントが長時間［Upgrade blocked（アップグレード禁止）］のままである場合は、Bit9 テクニカル サポートにご連絡ください。
Up to date（最新）	エージェントのアップグレード（または新規インストール）は完了しています。
Agent uninstalled（エージェント アンインストール済み）	このコンピューターにはエージェントが存在していましたが、アンインストール済みです。

Bit9 エージェントのアンインストール

標準的なアンインストール手順により、通知プログラムやドライバーも含めて Bit9 ファイルが削除されています。コンピューターのユーザーは、「エージェント管理権限の構成」（750 ページ）の説明に従って特別なエージェント管理者アクセスを与えられない限り、有効な Bit9 エージェントをアンインストールすることはできません。

アンインストールするには、［Computers（コンピューター）］ページで無効モードのポリシーにコンピューターを置くことで、Bit9 エージェントを無効にします。まだ実行していない場合は、エージェントをアンインストールする前に Bit9 コンソールにログインし、［Mode（モード）］を［**Disabled**（無効）］に設定したポリシーを 1 つ作成します。アンインストールのためにポリシーを（「agent disabled policy」などの名前で）作成すると、サーバーによってそれに対応するエージェント インストーラーが自動的に作成され、［Download Install Packages（インストール パッケージのダウンロード）］ページのリストに追加されます。

Windows コンピューターからのエージェントのアンインストール

Bit9 エージェントをアンインストールするには、次の手順を実行します。

1. Bit9 コンソールの［Computers（コンピューター）］ページでコンピューターを特定し、エージェント無効ポリシーに移動します。
2. クライアント コンピューターで、他のアプリケーションをすべて終了します。

3. クライアント コンピューターで、次のように Windows のコントロール パネルから標準的なプログラム削除手順を実行します。

   a. Windows のコントロール パネルで、[**プログラムの追加と削除**]（Vista または Windows 7 システムでは［**プログラムと機能**］）を選択します。

   b. プログラムのリストから、**Bit9 Agent** を選択します。

   c. オペレーティング システムに応じて［**削除**］ボタンまたは［**アンインストール**］ボタンをクリックして、アンインストールが完了するまで待ちます。

4. Bit9 コンソールの［Computers（コンピューター）］ページで、コンピューターを削除します。これにより、そのコンピューターが使用されなくなった（一時的にネットワークから切断されているのではなく）ことが Bit9 Server に伝えられ、アクティブなコンピューターのテーブルから名前が削除されます。

Mac コンピューターからのエージェントのアンインストール

1. Bit9コンソールで、エージェント無効ポリシーにコンピューターを移動します。
2. ターミナル、または他のシェル インターフェイスで、次のコマンドを実行します。

   ```
   sudo /Applications/Bit9/uninstall.sh
   ```

   Bit9 エージェントとそのデータが削除されます。

3. Bit9 コンソールの［Computers（コンピューター）］ページで、コンピューターを削除します。これにより、そのコンピューターが一時的にネットワークから切断されているのではなく、使用されなくなったことが Bit9 Server に示され、アクティブなコンピューターのテーブルから名前が削除されます。

Linux コンピューターからのエージェントのアンインストール

1. Bit9 コンソールで、エージェント無効ポリシーにコンピューターを移動します。
2. 管理者権限で、または sudo を実行できるアカウントでクライアント コンピューターにログインします。
3. シェル ウィンドウで、Bit9 エージェント アプリケーションのディレクトリに移動します。
   - `cd /opt/bit9/bin`
4. アンインストール スクリプトを実行します。
   - エージェントとそのすべてのデータを削除する手順：
     ```
     sudo sh ./b9uninstall.sh
     ```
   - エージェントを削除し、**/srv/bit9** にある Bit9 エージェントのデータは保持する手順：
     ```
     sudo sh ./b9uninstall.sh -d
     ```

5. コンソールの［Computers（コンピューター）］ページで、コンピューターを削除します。これにより、そのコンピューターが（一時的にネットワークから切断されているのではなく）使用されなくなったことが Bit9 Server に示され、アクティブなコンピューターのテーブルから名前が削除されます。

コンピューターのテーブルの表示

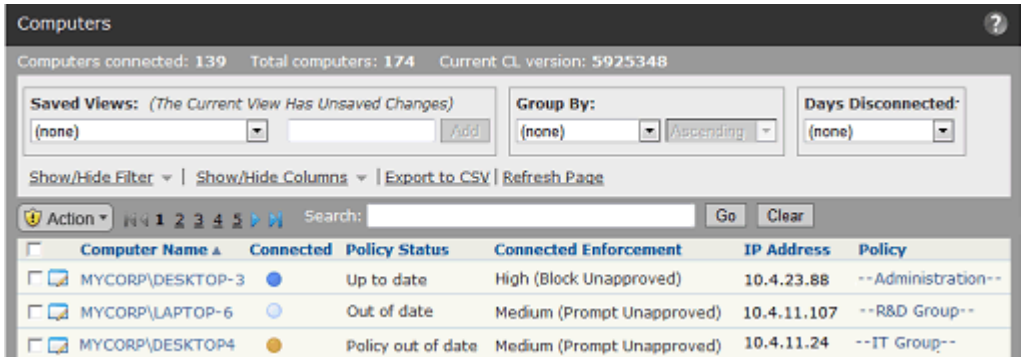
［Computers（コンピューター)］ページのテーブルでは、コンピューターと、そのコンピューターのプラットフォーム、ポリシー、適用レベル、サーバーに接続されているかどうかなど、コンピューターに関する情報を確認できます。ほとんどのコンソール テーブルと同様に、［Columns（列）］ボタンを使用することでテーブルに詳細を追加または削除できます。また、［Search（検索）］フィールドを使用することで、注目するコンピューターだけがページに表示されるように絞り込むこともできます。ビューのカスタマイズの詳細については、第 2 章「Bit9 コンソールの使用」の「Bit9 コンソールのテーブル」を参照してください。

エージェントで管理するコンピューターのテーブル以外に、［Computers（コンピューター)］ページには次の情報も表示されます。

- **Computers connected**（接続済みコンピューター数）– Bit9 エージェントが実行され、現在サーバーに接続されているコンピューターの数が示されます。
- **Total computers**（合計コンピューター数）– サーバーによって管理されているセキュリティ ポリシーの現在のメンバーであるコンピューターの総数が示されます。
- **Current CL version（最新の CL バージョン）**– サーバーが利用できる最新の構成リスト (CL) のバージョン番号が示されます。これは、特定のエージェントの CL が期限切れであるかどうかを判断するときの参考になります。ただし、一部の CL バージョンはエージェントに固有なので、エージェントの CL バージョンがここに表示される CL バージョンと完全に一致しなくても、そのエージェントが期限切れであるとは限りません。

Bit9 Server によって管理されているコンピューターのテーブルを表示する手順：

1. コンソール　メニューで、［**Assets**（アセット）］>［**Computers**（コンピューター）］の順に選択します。［Computers（コンピューター）］ページが表示されます。



2. ［Search（検索）］フィールドを使用すると、コンピューターを名前（またはその一部）、IP アドレス、またはポリシーで検索することによって［Computers（コンピューター）］テーブルのサイズを小さくし、目的のシステムを見つけやすくすることができます。コンピューター名に一致させる文字列を入力し、［**Go**（実行）］をクリックします。［**Clear**（クリア）］をクリックすると、コンピューターのリストは検索の前に表示されていた状態に戻ります。
3. ［Saved Views（保存済みビュー）］は、一定の特性に一致するシステムだけを［Computers（コンピューター）］テーブルに表示するもう 1 つの方法です。
   - ［**Carbon Black Deployments**（Carbon Black の展開）］を選択すると、Carbon Black エージェントがインストールされているかどうかを基準としてグループ化されたコンピューターが表示されます。
   - ［**Cloned Computers**（クローン コンピューター）］を選択すると、テンプレート コンピューターからクローンされたコンピューターが表示されます。詳細については、第 6 章「仮想マシンの管理」を参照してください。
   - ［**Computers in Local Approval**（ローカル承認のコンピューター）］を選択すると、ソフトウェアをローカル承認モードでインストールする承認をサーバーから受け取り済みで、ロックダウンされているコンピューターが表示されます。
   - ［**Computers Requiring Upgrade**（アップグレードが必要なコンピューター）］を選択すると、最新バージョンに更新されていない Bit9 エージェントが実行されているコンピューターが表示されます。
   - ［**Computers connected**（接続済みコンピューター）］を選択すると、現在サーバーに接続されているBit9エージェントが実行されているコンピューターだけが表示されます。
   - ［**Disconnected Computers**（接続されていないコンピューター）］を選択すると、現在サーバーに接続されていない Bit9 エージェントが実行されているコンピューターだけが表示されます。
   - ［**Duplicate Computers**（重複コンピューター）］を選択すると、Bit9 データベース上の他のコンピューターと同じ名前を持つコンピューターが表示されます。詳細については、「重複コンピューター」（179 ページ）を参照してください。
   - ［**Template Computers**（テンプレート コンピューター）］を選択すると、クローン コンピューターのテンプレートであるコンピューターが表示されます。詳細については、第 6 章「仮想マシンの管理」を参照してください。
   - ［**(none)**（(なし)）］を選択すると、このコンピューターによって管理されているすべてのコンピューターが表示される状態に戻ります。
   - 自分で、または他のコンソール ユーザーが保存済みビューを作成済みであれば、それらも使用できます。
4. ［**Show/Hide Filter**（フィルターの表示 / 非表示）］や［**Show/Hide Columns**（列の表示 / 非表示）］をオンにすると［Filters（フィルター）］または［Columns（列）］インターフェイスが表示され、［Computers（コンピューター）］テーブルの表示をさらにカスタマイズできます。

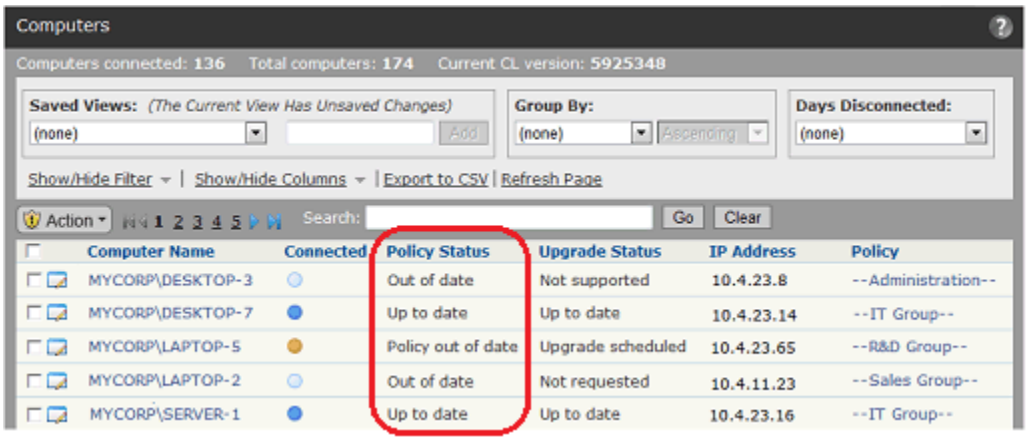
［Computer Details（コンピューターの詳細）］ページで使用できるフィールドの説明を表 15 に示します。これらのほとんどは、［Computers（コンピューター）］テーブルでもデフォルトで、またはカスタマイズによって使用できます。

エージェント ポリシー ステータス

［Computers（コンピューター）］テーブルには［Policy Status（ポリシー ステータス）］という列があり、リスト内の各コンピューターのエージェントが、それに対して適用される Bit9 Server ルールにとって最新状態であるかどうかが示されます。このフィールドは、［Computer Details（コンピューターの詳細）］ページには表示されません。

注意

システム初期化の実行中も、コンピューターは既にそのセキュリティ ポリシーの適用レベルで保護されています。



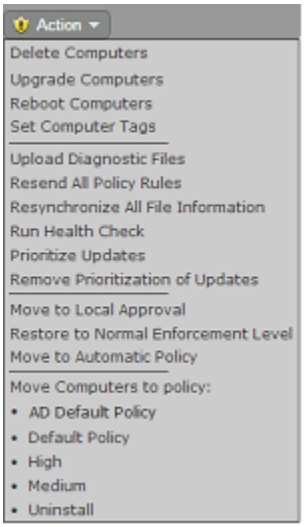
ポリシー ステータスとして使用できる値を表 14 に示します。

表 14：ポリシー ステータス メッセージ

ポリシー ステータス	説明
Up to date（最新）	エージェントの適用レベル、ポリシー、ルールはすべて最新です。
Policy out of date（ポリシーが期限切れ）	エージェントは、そのポリシーの変更を反映していません。
Approvals out of date（承認が期限切れ）	エージェント ルール（ファイルの承認または禁止、信頼済みユーザー、公開者ルール、アップデーター ルール、デバイス ルール、メモリ ルール、およびレジストリ ルールを含む）が期限切れです。
Enforcement Level out of date（適用レベルが期限切れ）	エージェントの適用レベルが期限切れです。
Out of date（期限切れ）	エージェントは、次の複数に関して期限切れです。適用レベル、ポリシー、ルール。

選択したコンピューターに対するアクション

［Computers（コンピューター）］ページの［Action（アクション）］メニューには、1 つまたは複数のコンピューターに適用できるコマンドが用意されています。各コンピューターの行の左側にあるボックスをオンにすることで、アクションの対象を選択することができます。



アクションには、削除、アップグレード、タグ付け、再起動、および別のポリシーへの移動が含まれます。このメニューで実行可能なその他のコマンドについては、表 17、「[Computer Details（コンピューターの詳細）] ページのメニュー」（168 ページ）の［Actions（アクション）］セクションと［Advanced（詳細）］セクションで説明します。

1 台のコンピューターの詳細を表示する手順：

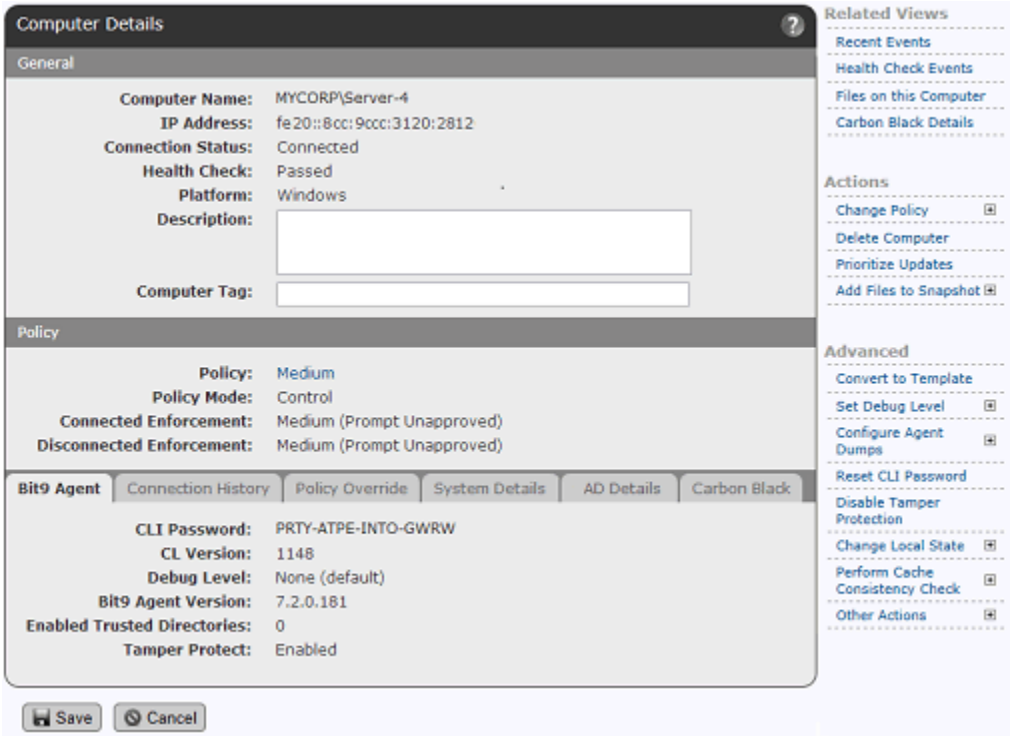
コンピューターを特定し、その詳細を表示する方法は複数あります。ホーム ページの［Find Computer（コンピューターの検索）］ポートレットを使用すると、コンピューターを特定し、その詳細を確認することができます。ここでは、[Computer（コンピューター）］ページでコンピューターを特定し、その詳細情報を取得する方法について説明します。

注意

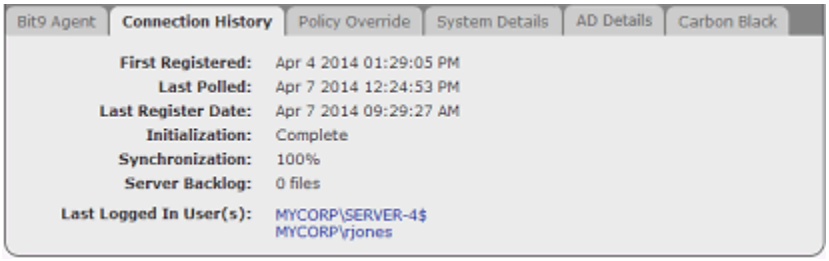
詳細を要求するコンピューターがテンプレート コンピューターである場合、[View Details（詳細の表示）] ボタンをクリックすると、[Computer Details（コンピューターの詳細）] ページではなく［Template Details（テンプレートの詳細）］ページが開きます。詳細については、第 6 章「仮想マシンの管理」を参照してください。

コンピューターの［Computer Details（コンピューターの詳細）］ページを表示する手順：

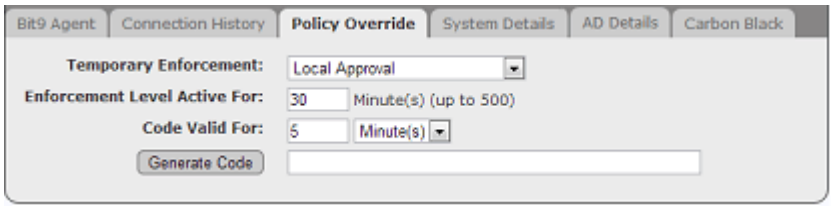
1. コンソール メニュー バーで、［**Assets**（アセット）］>［**Computers**（コンピューター）］の順に選択します。［Computers（コンピューター）］ページが表示されます。
2. ［Computers（コンピューター）］テーブルで、詳細情報が必要なコンピューターを（［Computer filters（コンピューター フィルター）］パネルなどを使用して）特定します。
3. テーブルで、コンピューターの名前、または名前の横にある［View Details（詳細の表示）］ボタンをクリックします。［Computer Details（コンピューターの詳細）］ページが表示されます。



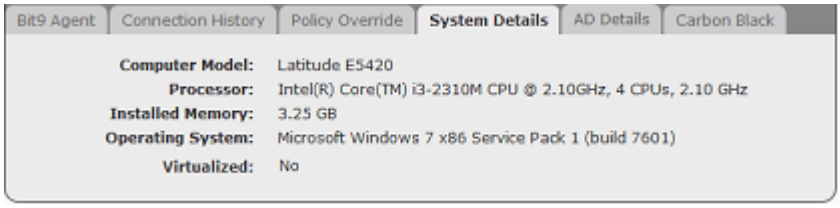
4. ［Computer Details（コンピューターの詳細）］ページの［General（全般）］セクションと［Policy（ポリシー）］セクションは、すべてのビューで表示されます。ページ下部のパネルは、クリックするタブによって次のように変わります。
   - ［**Bit9 Agent**（Bit9 エージェント）］（デフォルト、上記）をクリックすると、現在詳細が表示されているコンピューターのエージェントのバージョン、パスワード、その他の設定情報が表示されます。
   - ［**Connection History**（接続の履歴）］をクリックすると、エージェントと Bit9 Server の間の通信ステータスが、初期化やサーバーとの同期が完全に行われたかどうかを含めて表示されます（初期化が完了した場合のみ［Synchronized（初期化済み）］と表示されます）。



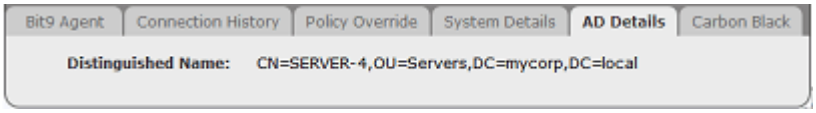
- ［**Policy Override**（ポリシーの無効化）］をクリックすると、一時変更コードが生成され、それを使用することでエージェントを一時的に別の適用レベルに割り当てることができます。



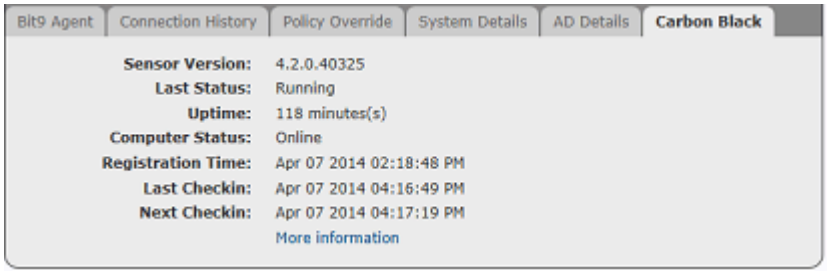
- ［**System Details**（システムの詳細）］をクリックすると、コンピューターの CPU、メモリ、オペレーティング システムに関する情報が取得可能な場合、表示されます。



- ［**AD Details**（AD の詳細）］をクリックすると、このコンピューターに関して Active Directory から得られる情報が表示されます（AD 統合を有効にしてある場合のみ）。



- [**Carbon Black**] をクリックすると、このコンピューターに関して Carbon Black サーバーからレポートされる詳細が表示されます。このサーバーは、Bit9 の［System Configuration（システム構成）］ページの［Licensing（ライセンス）］タブで設定されます。Carbon Black サーバーが構成されていない場合、またはコンピューターで Carbon Black センサーが実行されていない場合、このタブには［Not installed（インストールされていない）］というステータスだけが表示されます。デフォルトでは、Bit9 Server は Carbon Black のステータスを 30 分ごとに確認します。



- [**Microsoft SCEP**] をクリックすると、このコンピューターでの Microsoft SCEP 保護のステータスが表示されます。このタブは、Bit9 Server に SCEP が統合されている場合にのみ表示されます。デフォルトでは、Bit9 Server は SCEP のステータスを 60 分ごとに確認します。

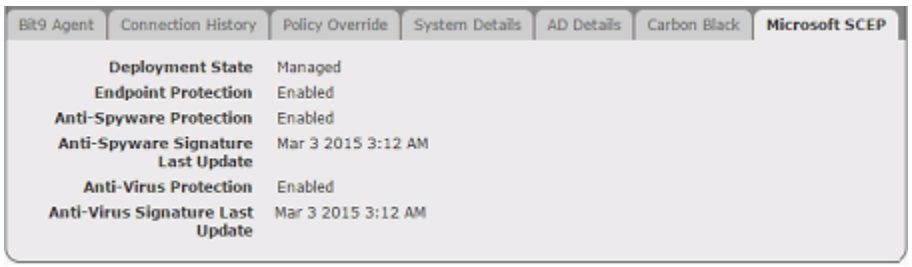


表 15：コンピューターの詳細（［Details（詳細）］ページと［Computers（コンピューター）］テーブル）

フィールド	説明
Computer name（コンピューター名）	コンピューターのネットワーク名。
IP address（IP アドレス）	コンピューターの IP アドレス。IPv4 または IPv6 のアドレスを使用できます。Bit9 Server を IPv6 用に構成すると、Bit9 エージェントは最初に IPv6 で接続を試みます。
Identifier（識別子）	コンピューターの MAC アドレス。（テーブルのみで使用）
Connection status（接続ステータス）	コンピューターと Bit9 Server の間の通信ステータス。 • **Connected**（接続済み）– Bit9 Server との通信が確立されています。 • **Disconnected**（接続されていない）– Bit9 Server との通信が確立されていません。 ［Computers（コンピューター）］テーブルには、［Connection（接続）］ステータス フィールドに円形のアイコンもあり、接続とエージェントのステータスを示しています。 ●（青色）– 接続、最新 ●（明るい青色）– 切断、最新 ●（オレンジ）– 接続、サポート外（エージェントが期限切れ、または再起動が必要） ○（灰色の線で囲まれた透明）– テンプレート コンピューター ●（赤色）– 接続、正常性チェック失敗。エージェントは直ちに確認が必要な状態です。このコンピューターの正常性チェック イベントを収集し、Bit9 テクニカル サポートにご連絡ください。

フィールド	説明
Health Check（正常性チェック）	エージェントの正常性ステータス。正常性チェックには、エージェントが適切に機能しているかどうかを確認する一連のテストが含まれています。値が Passed の場合、このコンピューター上のエージェントに既知の正常性の問題はありません。値が Failed の場合、エージェントの正常性には少なくとも 1 つの面で問題があります。この場合は、[Computers Details（コンピューターの詳細）] ページで [Health Check Events（正常性チェックイベント）] をクリックし、Bit9 テクニカル サポートにご連絡ください。 **注意**：正常性チェックは自動的に実行されますが、エージェントの問題に対処した後で正常であるかどうかを確認するには、[Computer Details（コンピューターの詳細）] ページの [Other Actions（その他のアクション）] メニューで [**Run health check**（正常性チェックの実行）] コマンドを使用して、正常性チェックを実行できます。
Platform（プラットフォーム）	このコンピューターの基本的なオペレーティング システム プラットフォーム。値は Windows、Mac、Linux のいずれかです。[Computer Details（コンピューターの詳細）] ページの [System Details（システムの詳細）] タブに追加の情報が表示されます。
Days Offline（オフライン日数）	コンピューターが切断されている場合、この列を [Computers（コンピューター）] テーブルに追加すると、切断されている期間が表示されます。また、この日数をフィルターとして使用できます。
Upgrade status（アップグレード ステータス）	このコンピューターのエージェント アップグレード ステータス。ステータスのオプションについては、「エージェント アップグレード ステータス」（149 ページ）を参照してください。[Computer Details（コンピューターの詳細）] ページでは、アップグレードが必要なコンピューターについてのみ表示されます。
Upgrade error time（アップグレード エラー時刻）	エージェント アップグレードでエラーが発生した場合、そのエラーの時刻。[Computer Details（コンピューターの詳細）] ページでは、アップグレードが試みられたコンピューターについてのみ表示されます。
Policy status（ポリシー ステータス）	このコンピューターのポリシー保護のステータス（最新かどうかなど）。詳細については、「エージェント ポリシー ステータス」（155 ページ）を参照してください。
Description（説明）	[Computer Details（コンピューターの詳細）] ページに表示される、このコンピューターに関するオプションの情報。詳細ページでこのテキストを入力または編集するには、[**Update Computer**（コンピューターの更新）] ボタンをクリックして保存します。

フィールド	説明
Computer tag（コンピューター タグ）	コンピューターのグループを識別するために追加するオプションのテキスト文字列。このグループを対象に、特定のレポート作成や処理を行うことができます。タグは、コンピューターのグループを識別するために、ポリシーの代替手段として使用できます。たとえば、オフィスのすべてのコンピューターに「Low (Monitor Unapproved)（低（未承認を監視））」ポリシーを適用する一方で、ファイルのアクティビティについては、営業部門や会計部門などのサブグループにタグ付けしたコンピューターごとに、より具体的なレポートで追跡することができます。 タグは［Computer Details（コンピューターの詳細）］ページで 1 台のコンピューターに、または［Computers（コンピューター）］ページの［Action（アクション）］メニューで複数のコンピューターに設定することができます。
Policy（ポリシー）	現在コンピューターに割り当てられているポリシー。
Policy Mode（ポリシー モード）	このポリシーが動作しているセキュリティ モード。選択肢は、可視性、制御、無効です。
Connected Enforcement（接続済み適用）	コンピューターが Bit9 Server と通信しているときに割り当てられる適用レベル。このコンピューターおよび他のポリシー メンバーのこの設定を変更するには、ポリシーを編集します。適用レベルがサーバー上でポリシーの変更を反映した最新状態になっていない場合は、「(out of date)（(期限切れ)）」が付加されます。
Virtualized（仮想化済み）	このコンピューターが仮想マシンであるかどうかを示します（Yes（はい）、No（いいえ））。［Computer Details（コンピューターの詳細）］ページでは、［Virtual Platform（仮想プラットフォーム）］と組み合わされて［System Details（システムの詳細）］タブの 1 つのフィールドになります。
Virtual Platform（仮想プラットフォーム）	これが仮想マシンの場合に、生成するために使用される仮想プラットフォーム。現在の値は、空白、VMware、Unknown（不明）です。［Computer Details（コンピューターの詳細）］ページでは、［Virtual（仮想）］と組み合わされて［System Details（システムの詳細）］タブの 1 つのフィールドになります。
Clone Inventory（クローン インベントリ）	このコンピューターがクローンを作成するためのテンプレートである場合に、そのテンプレートから作成されるクローンのインベントリにすべてのファイル（テンプレート イメージのファイルを含む）が含まれるか、新規または変更された（各クローンの作成後）ファイルのみが含まれるかを示します。テンプレートでないコンピューターの場合、このフィールドは空白です。詳細については、第 6 章「仮想マシンの管理」を参照してください。
Inventory（インベントリ）	このコンピューターが仮想マシンである場合に、そのクローンのインベントリにすべてのファイル（テンプレート イメージのファイルを含む）が含まれるか、新規または変更された（クローンの作成後）ファイルのみが含まれるかを示します。クローンでないコンピューターの場合、このフィールドは空白です。詳細については、第 6 章「仮想マシンの管理」を参照してください。

フィールド	説明
SCEP Status（SCEP ステータス）	Microsoft SCEP が Bit9 Server と統合されている場合に、このコンピューター上の SCEP エージェントのステータスを示します。以下の値があります。 • Unknown（不明）– SCEP 統合は有効化されていません。 • Not Present（なし）– このコンピューターに SCEP エージェントはインストールされていません。 • Disabled（無効）– 1 つまたは両方の SCEP エージェント コンポーネントが無効になっています。 • Outdated（期限切れ）– SCEP はインストールされていますが、1 つまたは両方のコンポーネントの署名が 3 日よりも前の日付です。 • Active（アクティブ）– SCEP はインストールされており、両方のコンポーネントとも有効で、すべての署名は最新です。
Save（保存）（ボタン）	[Description（説明）] および [Computer tag（コンピューター タグ）] に加えた変更が、[Computer Details（コンピューターの詳細）] ページの [General（全般）] パネルに適用されます。
Cancel（キャンセル）（ボタン）	[**Save**（保存）] ボタンをクリックする前にクリックすると、[Description（説明）] および [Computer tag（コンピューター タグ）] に対する変更のうち保存されていない部分がクリアされます。ページは、編集を開始する前に有効だった設定に戻ります。

表 16：[Computer Details（コンピューターの詳細）] ページ：タブ化されているセクション

フィールド	説明
[Bit9 Agent（Bit9 エージェント）] タブ	
CLI Password（CLI パスワード）（CLI Code（CLI コード）（テーブル内））	このコンピューターにインストールされているBit9エージェント用のコマンド ライン診断ユーティリティを有効化するためのコード。Bit9 テクニカル サポートの担当者が使用します。

フィールド	説明
CL Version（CL バージョン）	構成リストのバージョン番号。コンピューターとサーバー ルールが同期しているかどうかを判断するために使用されます。最新でない場合、番号とともに「(out of date)（(期限切れ)）」と表示されます。コンピューターの CL バージョンを、[Computers（コンピューター）] ページに表示される Bit9 Server の最新の CL バージョンと比較してください。また、多くの Bit9 Security Platform ルールの詳細ページには CL バージョンが示されており、ルールの最新の定義がわかります。Bit9 サポートが使用します。 **注意**：まれに、CL バージョンの隣に次のメッセージが表示されることがあります。 Agent did receive but is not enforcing all the rules yet（エージェントはルールを受け取りましたが、まだすべてのルールを適用していません。） これは、エージェントが受け取ったルールを処理中であり、一部のルールが完全に機能しない可能性があることを意味します。このメッセージ（およびメッセージが示す状態）は、数分以内に解消されます。
Debug Level（デバッグ レベル） （**Agent Debug Level**（エージェント デバッグ レベル）（テーブル内））	このエージェントの現在のデバッグ レベル。収集されるデバッグ情報の量を表します。これは、[Advanced（詳細）] メニューで変更できます。Bit9 サポートが使用します。
Bit9 Agent Version（Bit9 エージェントのバージョン）	このコンピューターにインストールされているBit9エージェントのバージョン番号。
Enabled Trusted Directories（有効な信頼済みディレクトリ）	このコンピューターで現在有効になっている信頼済みディレクトリの数。詳細については、「信頼済みディレクトリによる承認」（277 ページ）を参照してください。
Tamper Protect（改ざんからの保護）	エージェントの改ざんから保護する機能のステータス。値は Enabled（有効）または Disabled（無効）です。
[Connection History（接続の履歴）] タブ	
First Registered（初回登録）	このコンピューターが初めて Bit9 Server に登録された日時。
Last Polled（最終ポーリング）	このエージェントが最後に最新情報を求めて Bit9 Server にポーリングし、最新のファイル情報をサーバーに提供した日時。エージェントは 30 秒ごとにポーリングを実行する可能性がありますが、ポリシーの変更や承認などに関する新しい情報がサーバーにない場合は「スリープ」状態になり、10 分ごとに頻度が低下します。
Last Register Date（最終登録日）	エージェントが最後に Bit9 Server に接続した日時。

フィールド	説明
Synchronization（同期） （**%Synchronization**（同期率）（テーブル内））	このエージェントと Bit9 Server の間での、ファイル情報の同期率。初期化が完了した後でのみ表示されます。
Initialization（初期化） （**% Initialization**（初期化率）（テーブル内））	初期化中に、初期化が完了した割合が表示されます。初期化が 100% に到達すると「Complete（完了）」と表示されます。
Server Backlog（サーバー バックログ）	このコンピューターから受信したが、サーバー上での処理がまだ完全には完了していないファイルの数。バックログ ファイルは［File Catalog（ファイル カタログ）］に表示されますが、［Files on Computers（コンピューター上のファイル）］タブまたは［Find Files（ファイルの検索）］ページには表示されません。
Last logged in user(s)（最終ログイン ユーザー）	コンピューターが最後に Bit9 Server に接続したときにログインしていたユーザー。AD 統合を有効にしてある場合、このフィールドをクリックするとユーザーに関する詳細情報が得られます。
［Policy Override（ポリシーの無効化）］タブ	切断されているコンピューターの適用レベルを一時的に変更するためのコードを生成できます。「期限付きポリシーへの一時変更の使用」（318 ページ）を参照してください。
［System Details（システムの詳細）］タブ	
Computer Model（コンピューターのモデル）	このコンピューターのモデル。仮想マシンも識別されます。
Processor（プロセッサー）	このコンピューターのプロセッサーのモデル、速度、数。
Installed Memory（内蔵メモリ）	このコンピューターに内蔵されているメモリの量。
Operating System（オペレーティング システム）/ Operating System Details（オペレーティング システムの詳細）	このコンピューターのオペレーティング システムのバージョン。 ［Computers（コンピューター）］テーブルでは、 • ［Operating System（オペレーティング システム）］には基本的な OS（Windows 7 など）が示されます。 • ［Operating System Details（オペレーティング システムの詳細）］には、完全な名前、ビルド、サービス パックのレベルが示されます。 ［Computer Details（コンピューターの詳細）］ページの［Operating System（オペレーティング システム）］フィールドには、完全な詳細が示されます。

フィールド	説明
Virtualized（仮想化済み）	このコンピューターが仮想マシンであるかどうかと、仮想マシンである場合はそのプラットフォーム。次のいずれかの値になります。No（いいえ）、Yes（VMware）（はい（VMware））、Yes (Unknown)（はい（不明））
［AD Details（AD の詳細）］タブ	
	このタブをクリックすると、コンピュータに関して Active Directory から得られる追加の情報がある場合、それが表示されます。AD との統合が有効でないか、AD サーバーにアクセスできない場合、追加される情報はありません。
［Carbon Black］タブ	
Sensor Version（センサー バージョン） （**Carbon Black Version**（Carbon Black のバージョン）（テーブル内））	このコンピューターにインストールされている Carbon Black センサーのバージョン。

フィールド	説明
Carbon Black Status（Carbon Black のステータス）（テーブル内） **Last Status（最終ステータス）**（[Details（詳細）] ページの場合）	このフィールドには、Bit9 エージェントが Bit9 Server にレポートした、このコンピューターの Carbon Black センサーの最終ステータスが示されます。Bit9 Server は Carbon Black のステータスを 30 分ごとに確認するため、最大で 30 分間はステータスの変化が同期していない可能性があります。 このテーブルでの Carbon Black のステータス値は次のいずれかです。 • Unknown（不明） • Installed, initializing（インストール済み、初期化中）– センサーがインストールされていますが、初期化は完了していません • Installed, running（インストール済み、実行中） • Installed, not running（インストール済み、実行中でない） • Not installed（インストールされていない） • Stopped（停止済み） [Details（詳細）] ページの [Carbon Black] タブにある [Last Status（最終ステータス）] フィールドは、テーブルの Carbon Black のステータスと類似しています。ただし、センサー ステータスが [Unknown（不明）] である場合、このフィールドは表示されません。このフィールドの値は次のいずれかです。 • Running（実行中） • Service not running（サービスは実行中でない） • Kernel not running（カーネルは実行中でない） • Stopped（停止済み） **注意**：センサーのインストールから Bit9 による Carbon Black のステータスのポーリングまでの最大 30 分の遅れだけでなく、Carbon Black センサーが Carbon Black サーバーに接続してセンサー ID を受信するまでは、[Not installed（インストールされていない）] のステータスがレポートされ続けます。また、Bit9 エージェントがオフラインであるか、またはコンピューターからアンインストールされている場合は、センサー ステータスが変化していても、エージェントによってレポートされた Carbon Black センサーの最終ステータスが Bit9 コンソールに表示されます。
Uptime（稼働時間）	Carbon Black センサーが直近の起動以降に実行中である分数と時間数。
Computer Status（コンピューター ステータス）	Carbon Black サーバーによってレポートされた、このコンピューターのステータス。
Registration Time（登録日時）	このコンピューター上の Carbon Black センサーがサーバーに登録された日時。
Last Checkin（最終チェックイン）	このコンピューター上の Carbon Black センサーがサーバーに最後にチェックインした日時。
Next Checkin（次回チェックイン）	このコンピューター上の Carbon Black センサーでスケジュールされている、サーバーへの次回のチェックイン日時。

フィールド	説明
More Information（詳細情報）	[System Configuration（システム構成）] ページの [Licensing（ライセンス）] タブで構成されている Carbon Black サーバーのログイン ページに接続します。ログインすると Carbon Black の [Sensors（センサー）] ページが開き、このコンピューターに関する追加の詳細を確認できます。 **注意**：Carbon Black コンソールを正常に開くには、Carbon Black サーバーに対する有効なログイン認証情報を持っている必要があります。
[Microsoft SCEP] タブ	
Deployment State（展開状態）	このコンピューターの SCEP エージェントの状態。値は、Managed（手動）または Unmanaged（非管理）です。
Endpoint Protection（エンドポイント保護）	このコンピューターの Microsoft エンドポイント保護のステータス。Enabled（有効）または Disabled（無効）。
Anti-Spyware Protection（スパイウェア対策保護）	このコンピューターの Microsoft スパイウェア対策保護のステータス。Enabled（有効）または Disabled（無効）。
Anti-Spyware Signature Last Update（スパイウェア対策署名最終更新）	このコンピューターにおける Microsoft スパイウェア対策の署名の最終更新日時。
Anti-Virus Protection（ウイルス対策保護）	このコンピューターの Microsoft ウイルス対策保護のステータス。Enabled（有効）または Disabled（無効）。
Anti-Virus Signature Last Update（ウイルス対策署名最終更新）	このコンピューターにおける Microsoft ウイルス対策の署名の最終更新日時。
Last Infection（最終感染）	SCEP に検出された最後のマルウェア感染の日時。

表 17：[Computer Details（コンピューターの詳細）] ページのメニュー

メニュー / オプション	説明
[Related Views（関連ビュー）] メニュー	
Recent Events（最近のイベント）	[Events（イベント）] ページが開き、このコンピューターがソースとなった最近のイベント（発生した場合）が表示されます。
Health Check Events（正常性チェック イベント）	[Events（イベント）] ページが開き、このコンピューターの正常性チェック イベントが表示されます。この情報は、エージェント正常性チェックが失敗した場合に、Bit9 テクニカル サポートによるトラブルシューティングで使用します。必要に応じてイベントページで [**Export to CSV**（CSV にエクスポート）] ボタンを使用することにより、発生したイベントを保存できます。
Files on this Computer（このコンピューター上のファイル）	[Find Files（ファイルの検索）] ページが開き、このコンピューター上の追跡されているファイルがすべて一覧表示されます。
Carbon Black Details（Carbon Black の詳細）	ブラウザーの新しいウィンドウまたはタブが開き、[System Configuration（システム構成）] ページの [Licensing（ライセンス）] タブで構成されている Carbon Black サーバーのログインページが表示されます。ログインすると Carbon Black の [Sensors（センサー）] ページが開き、このコンピューターに関する追加の詳細を確認できます。リンクは Carbon Black サーバーが構成されている場合にのみ表示されます。 **注意**：Carbon Black コンソールを正常に開くには、Carbon Black サーバーに対する有効なログイン認証情報を持っている必要があります。
[Actions（アクション）] メニュー	
Change Policy（ポリシーの変更）	コンピューターを別のポリシーに移動する手段として、ドロップダウン メニューが提供されます。このメニューから使用できるポリシーの 1 つである [Local Approval（ローカル承認）] を使用すると、このコンピューターを一時的にローカル承認モードにすることができます。 [**Go**（移動）] ボタンをクリックすると変更が適用されます。 このコンピューターのポリシーが自動的に割り当てられた場合は、[Go（移動）] ボタンの隣に [Automatic（自動）] と表示され、メニューは無効になります。[Automatic（自動）] チェックボックスをオフにして自動割り当てを解除すると、メニューからポリシーを選択できます。

メニュー / オプション	説明
Prioritize Updates（更新の優先）/ Remove Prioritization of Updates（更新の優先の解除）	このコンピューターがエージェントと構成リストのアップグレードを Bit9 Server から受け取る優先順位を一時的に高くします。接続されていないホストも、接続されていないまま優先順位を高くすることができ、その状態は次にエージェントがオンラインになったときに反映されます。 コンピューターが優先されると、このリンクは［Remove prioritization of updates（更新の優先の解除）］に変わります。［Remove prioritization of updates（更新の優先の解除）］をクリックすると、優先されていたコンピューターは直ちに順位が下がります。すべての面で最新状態になると、［Prioritize Updates（更新の優先）］が適用されていたエージェントは自動的に通常の優先順位に戻ります。 エージェントの優先順位を恒久的に高くすることもできます。これは、［Trusted Directories（信頼済みディレクトリ）］をホストしているコンピューターに対して自動的に行われます。恒久的な優先は、［Advanced/Other Actions（詳細 / その他のアクション）］メニューのコマンドによって割り当てることもできます。 ［Remove prioritization of updates（更新の優先の解除）］コマンドを選択すると、恒久的な優先と一時的な優先の両方が解除されます。
Request Agent Upgrade（エージェント アップグレードの要求）/ Remove Agent Upgrade Request（エージェント アップグレードの要求の削除）	［Request Agent Upgrade（エージェント アップグレードの要求）］は、このエージェントを直ちにアップグレードするようにスケジュールします。Bit9 エージェントがアップグレード可能な場合にのみ表示されます。 ［Remove Agent Upgrade Request（エージェント アップグレードの要求の削除）］は、アップグレード要求を削除して、エージェントへのアップグレードの適用を中止します。これは、直ちにエージェントをアップグレードするようにスケジュールしてある場合にのみ表示されます。 このオプションは、エージェントの自動アップグレードが有効なポリシーにのみ適用されます（「高度な構成オプション」（766 ページ）を参照）。

メニュー / オプション	説明
Add files to Snapshot（スナップショットへのファイルの追加）	このコンピューター上にあるファイルのリスト（Bit9 Server のデータベースに保管されている）を、ファイルのスナップショットに追加します。スナップショットを使用すると、Bit9 Server ネットワーク上の各コンピューターが、既知のファイルのベースラインからどれだけドリフトしているかを把握できます。スナップショット内のファイルにはさまざまなステータスがあります。スナップショットに禁止ファイルが含まれている場合、そのファイルは禁止されたままです。詳細については、「スナップショットの管理」（661 ページ）を参照してください。 このメニューには、次の 2 つのオプションがあります。 Choose existing snapshot（既存のスナップショットを選択）– このコンピューター上のファイルのリストが、メニューから選択したスナップショットに追加されます。 Create a new snapshot（新しいスナップショットを作成）– 新しいスナップショット名の入力が要求され、このコンピューター上のファイルのリストが、そのスナップショットに保存されます。
[Advanced（詳細）] メニュー	
Convert to Template（テンプレートに変換）	現在のコンピューターを Bit9 Security Platform コンピューターの「テンプレート」に変換します。その後、このテンプレートのイメージから（サードパーティの仮想化 / イメージ ソリューションを使用して）作成されるクローン コンピューターを適切に管理することができます。詳細については、第 6 章「仮想マシンの管理」を参照してください。
Set Debug Level（デバッグ レベルの設定）	このコンピューター上のエージェントから収集するデバッグ情報の量を変更します。Bit9 サポートと連絡を取りながら使用します。
Configure Agent Dumps（エージェント ダンプの設定）	このコンピューター上のエージェントから取得するダンプに含まれる情報の量を変更します。Bit9 テクニカル サポートが使用します。
Reset CLI Password（CLI パスワードのリセット）	CLI 有効化コードを手動でリセットします。Bit9 サポート担当者と連絡を取りながら有効化コードを使用した後、これを使って有効化コードを変更することで、サポート対象のユーザーのみにアクセスを許可できます。
Disable（改ざんからの保護の無効化）/Enable Tamper Protection（改ざんからの保護の有効化）	エージェントの改ざんからの保護が有効なとき、[Disable Tamper Protection（改ざんからの保護の無効化）] をクリックすると無効になります。保護が無効なとき、[Enable Tamper Protection（改ざんからの保護の有効化）] をクリックすると有効になります。改ざんからの保護を無効にすることは、特定の問題を解決する必要がある場合を除いて推奨されません。また、できるだけ早く再度有効化する必要があります。

メニュー / オプション	説明
Change local state（ローカル状態の変更）	コンピューター上の未承認ファイルをすべてローカルで承認できます。初期化後に、問題がないことがわかっている大量のファイルをコンピューターに追加した後で実行することが考えられます。
Perform Cache Consistency Check（キャッシュ整合性チェックの実行）	キャッシュ整合性チェックは、このコンピューター上のエージェントが保持する情報が、実際に存在するファイルに関する正確な情報であることを確認するためのものです。ファイルがコンピューターに書き込まれたときにエージェントが実行されていなかった場合にのみ必要です。整合性チェックのためにエージェントの更新が必要な場合、差異があればそれもサーバーに送信されます。 ファイル キャッシュの変更は、ファイルが承認されるかどうかに影響する可能性があります。次に示すキャッシュ整合性チェックの 3 つのレベルのうち 1 つをメニューから選択できます。 • **Quick　Verification（クイック検証）**：エージェントのキャッシュ内のファイルがすべて存在することと、追跡する必要がある実行可能ファイルのままであることが確認され、ディスク上の各ファイルのサイズが、前回ファイルが分析されたときにキャッシュに保存されたサイズと比較されます。ファイルが存在しない場合は、キャッシュから削除されます。他のチェックが失敗する場合は、ファイルが再分析されます。 • **Rescan Known Files（既知のファイルを再スキャン）**：[Quick Verification（クイック検証）] の内容のすべてに加えて、ディスク上の各ファイルのハッシュが、エージェントのキャッシュ内にある同じファイルのハッシュと比較されます。ハッシュが一致しない場合は、ファイルが再分析されます。 • **Full Scan for New Files（新規ファイルを完全スキャン）**：前の 2 つの内容すべてに加えて、ディスク全体が再スキャンされ、エージェントのキャッシュ内に存在する必要があって実際は存在していないものがないか調査されます。見つかったファイルが分析されます。

メニュー / オプション	説明
	メニュー オプションのほかに、次の 3 つのチェック ボックスによって整合性チェックの内容を変えることができます。 • **Preserve state of changed files（変更されたファイルの状態を保持する）**：エージェントのキャッシュにハッシュが記録されていない場合、名前によってファイルが検索されます。ファイルが見つかると、この記録から得られたファイルの状態が現在のファイルに使用されます。 • **Re-evaluate publishers（公開者を再評価する）**：各ファイルが再検査され、その証明書情報が正確であることと、証明書が期限切れでなく、取り消されてもいないことが確認されます。また、信頼済み公開者の承認が再評価されます。 • **Approve new files（新しいファイルを承認する）**：完全スキャン中に見つかった新しいファイルがローカルで承認されます。 **注意**：この整合性チェックはトラブルシューティング機能であり、通常は Bit9 テクニカル サポートと連絡を取りながら使用します。キャッシュ整合性チェックは、選択するオプションによっては長時間かかることがあります。
[Other Actions（その他のアクション）] サブメニュー	エージェント管理機能のうち、必要とされる頻度が低く、Bit9 テクニカル サポートと連絡を取りながら使用されることの多いもの。以下のオプションを選択できます。 • Reboot computer（コンピューターの再起動） • Upload diagnostic files（診断ファイルのアップロード） • Delete diagnostic files on computer（コンピューター上の診断ファイルの削除） • Make local copy of agent cache（エージェント キャッシュのローカル コピーの作成） • Rescan installed applications（インストール済みアプリケーションの再スキャン） • Resend all policy rules（すべてのポリシー ルールの再送信） • Resynchronize all file information（すべてのファイル情報の再同期） • Upload statistics（統計のアップロード） • Run health check（正常性チェックの実行） • Restore database（データベースの復元） • Delete database（データベースの削除） • Restart service（サービスの再起動） • Permanently prioritize updates（更新の恒久的な優先）

別のポリシーへのコンピューターの移動

コンピューターを別のポリシーに移動することは、新しいポリシーを作成することなく保護を変更できる便利な方法です。[Computers（コンピューター）] テーブルでコンピューターを選択し、別のポリシーに移動します。AD ベースのポリシー割り当てを有効にしてある場合、コンピューターのポリシー割り当てを手動から自動、または自動から手動に変更できます。

注意

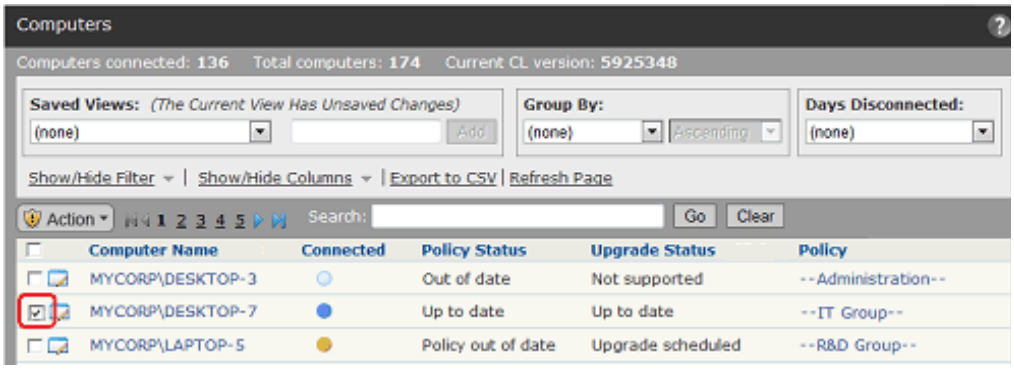
AD マッピング ルールを変更しても、対象のコンピューターのポリシーが直ちに変更されることはありません。変更は、そのコンピューターが次に Bit9 Server に再登録されるときに行われます。エージェント コンピューターの登録が発生するイベントの一覧は、セクション「ポリシーへのコンピューターの割り当て」（119 ページ）に示してあります。

このセクションで説明されている方法のほかに、Bit9 コンソールのホーム ページで [Change Policy（ポリシーの変更）] ポートレットを使用することもできます。

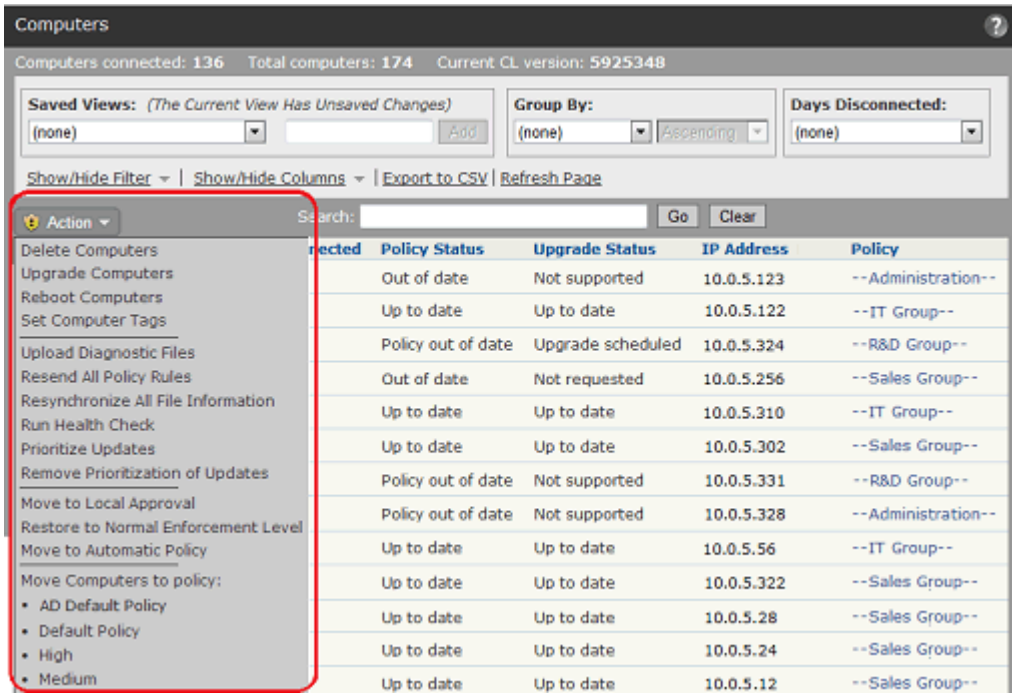
コンピューターを別のポリシーに移動する手順：

1. コンソール メニューで、[**Assets**（アセット）] > [**Computers**（コンピューター）] の順に選択します。[Computers（コンピューター）] ページが表示されます。

2. [Computers（コンピューター）] テーブルで、移動するコンピューターを特定し（必要に応じて保存済みビューを使用して）、目的のコンピューターのチェック ボックスをオンにします。



3. ［**Action**（アクション）］ボタンをクリックして［Action（アクション）］メニューを表示します。



4. ［Action（アクション）］メニューから、実行する移動のオプションを選択します。確認ダイアログで**[OK]**をクリックすると、選択したポリシーにコンピューターが割り当て直されます。選択したポリシーにコンピューターが移動し、［Automatic（自動）］から移動した場合はポリシーの割り当てが手動になります。

注意

コンピューターのポリシーの変更は、［Computer Details（コンピューターの詳細）］ページのテーブルでコンピューター名をクリックし、［Change Policy（ポリシーの変更）］メニューを使用して実行することもできます。

また、イベント ルールを作成することにより、特定のイベントが発生したときにコンピューターのポリシーを自動的に変更することもできます。

デフォルト ポリシーからのコンピューターの復元

デフォルト ポリシーは、Bit9 Server にレポートするコンピューターのうち、他のポリシーと関連付けられていないコンピューターのためのものです。そのようになる原因は、次のようにいくつか考えられます。

- AD マッピングが有効になっており、デフォルトの AD マッピング ルール（リストの最後のルール）ではポリシーがデフォルト ポリシーにマップされていて、エージェントが他のルールに一致しない。

- コンピューターへのBit9エージェントの初期インストールに、削除されたポリシーに関連付けられている古いインストーラーが使用されている。
- ポリシー内の最後のエージェントがBit9 Serverから切断され、ポリシーに含まれるコンピューターがなくなったため、コンソールの操作者が削除する判断をし、コンソールで［Computers（コンピューター）］テーブルから削除された。その後、エージェントがBit9 Serverに再接続した。

どのケースでも、コンピューターは自動的にデフォルト ポリシーに移動されます。Bit9 は、デフォルト ポリシーの適用レベルをサイトの適切な保護レベルに設定することをお勧めします。ファイルの実行を追跡し、ブロックはしない可視化モードにデフォルト ポリシーを設定している場合、［Default Policy（デフォルト ポリシー）］に表示されたすべてのコンピューターは、できるだけ早く、必要な設定と適用レベルを備えたポリシーに移動する必要があります。

注意

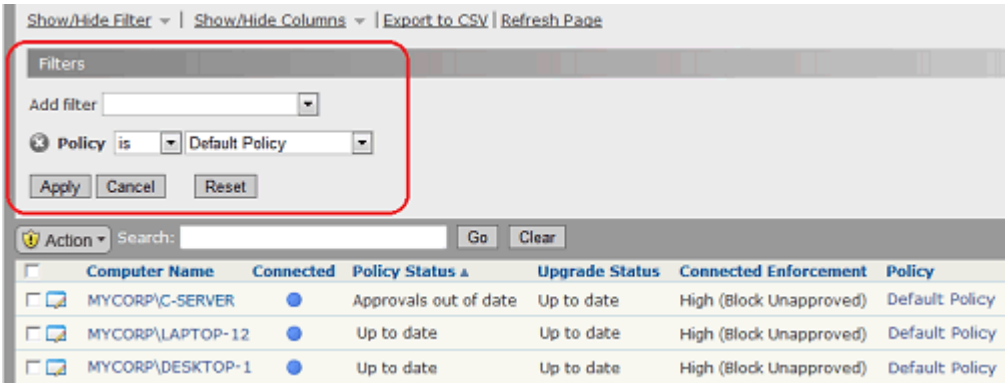
- フル スイート ライセンス（可視性と制御）をまったくお持ちでない場合、デフォルト ポリシーの適用レベルの選択肢は［Visibility（可視性）］と［Disabled（無効）］だけです。
- デフォルト ポリシーはシステムによって予約されているため、削除することはできません。

コンピューターをデフォルト ポリシーから復元する手順は、フィルターを適用する手順が追加されている以外、本質的にはコンピューターを別のポリシーに移動することと同じです。

デフォルト ポリシー内のコンピューターを別のポリシーに移動する手順：

1. コンソール メニューで、［**Assets**（アセット）］>［**Computers**（コンピューター）］の順に選択します。［Computers（コンピューター）］ページが表示されます。
2. 表示内容が現在の選択でない場合は、［Saved View（保存済みビュー）］として［**(none)**（(なし)）］を選択します。
3. ［**Show/Hide Filters**（フィルターの表示 / 非表示）］リンクをクリックし、［Add filter（フィルターの追加）］メニューで［**Policy**（ポリシー）］を選択します。

4. ［Policy（ポリシー）］フィルターで、演算子が「is」であることを確認し、右端のメニューから［**Default Policy**（デフォルト ポリシー）］を選択して、［**Apply**（適用）］ボタンをクリックしてフィルターを適用します。デフォルト ポリシーのすべてのコンピューターが表示されます。



5. ［Computers（コンピューター）］テーブルで、移動するコンピューターのチェック ボックスをオンにします。デフォルト ポリシーからデフォルトでない同じポリシーに複数のコンピューターを移動する場合は、一度にオンにすることができます。
6. ［Action（アクション）］メニューから、オンにしたコンピューターを移動する先のポリシーを選択します。AD ベースのポリシー割り当てを使用していて、目的のコンピューターがマッピング ルールの 1 つに一致することが確かである場合は、［**Move to Automatic Policy**（自動ポリシーに移動）］を選択します。
7. 確認ダイアログで **[OK]** をクリックすると、新しいポリシーにコンピューターが割り当て直されます。これにより、チェック ボックスをオンにしたコンピューターのエージェントと Bit9 Server は一時的に接続が切断され、再接続が行われます。再接続されると、コンピューターは移動先のポリシーに割り当てられます。

ローカル承認モードへのコンピューターの移行

新しいソフトウェアをインストールする必要がある場合に、Bit9 の信頼済み承認方法（ディレクトリ、ユーザー / グループ、公開者、およびアップデーター）が適していない状況では、ユーザーのコンピューターを一時的にローカル承認モードにすることができます。これは、ソフトウェアのインストールが許可される特殊なポリシーです。ローカル承認モードのコンピューターに置かれた実行可能ファイルは、あらかじめ禁止されていない限り、そのコンピューターでローカルに承認されます。ローカル承認モードを有効にする前にコンピューターに存在していたファイルは、承認するための他の方法も存在しますが、ローカルで承認されることはありません。

コンピューターのローカル承認モードを有効にするには、［Computers（コンピューター）］ページでコンピューター名の隣のチェック ボックスをオンにし、［Action（アクション）］メニューの［**Move to Local Approval**（ローカル承認に移行）］を選択するか、［Computer Details（コンピューターの詳細）］ページの［Change Policy

（ポリシーの変更）］メニューで［**Local Approval**（ローカル承認）］を選択します。詳しい手順については、「ローカル承認モードへのコンピューターの移行」（314 ページ）を参照してください。

コンピューターの追加

コンピューターは、Bit9 エージェントをインストールすると［Computers（コンピューター）］テーブルに追加されます。特別な「コンピューターを追加する」操作は不要です。AD ベースのポリシー割り当てを使用している場合、新しいコンピューターには、コンピューター（またはそのユーザー）の AD データをセキュリティ ポリシーにマッピングするために設定したルールに基づいて、ポリシーが割り当てられます。それ以外の場合、コンピューターには、選択されたエージェント インストール パッケージで指定されているポリシーが割り当てられます。

コンピューターの削除

使用しなくなった、またはエージェントでの管理を停止したコンピューターは、Bit9 Server から削除できます。Bit9 コンソールの［Computers（コンピューター）］テーブルからコンピューターを削除する前に、コンピューターの適用レベルを無効に変更し、その後、Bit9 エージェントをアンインストールします。詳細については、「Bit9 エージェントのアンインストール」（151 ページ）を参照してください。

コンピューターを削除する前にエージェントをインストールせず、そのコンピューターを Bit9 Server と同じネットワークに接続したままの場合、コンピューターは Bit9 Server によってポーリングされると再度［Computer（コンピューター）］テーブルに表示されます。ネットワークに接続されているコンピューターは直ちにテーブルに表示され、オフラインの場合は再接続されたときに表示されます。削除されたコンピューターでエージェントが引き続き実行されていると、最後に記録されたポリシーに戻ります。エージェント インストーラーによってコンピューターに適用されていたポリシーを削除済みの場合、サーバーはコンピューターをデフォルト ポリシーに移動します。

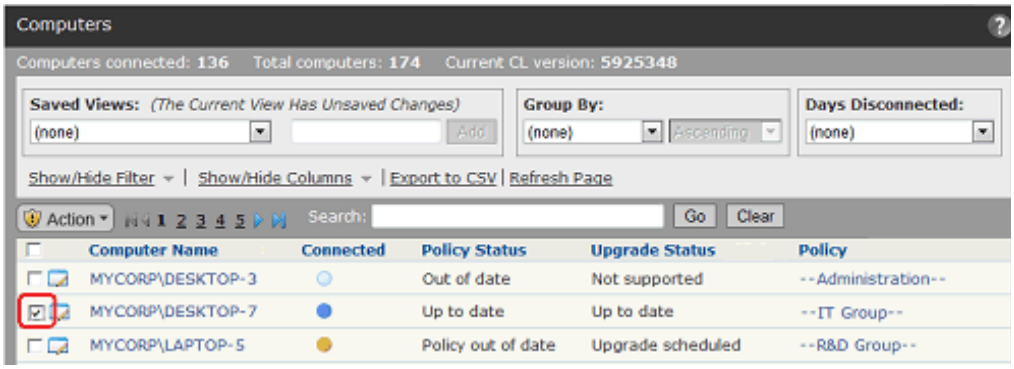
注意

Bit9 エージェントが実行されているコンピューターが Bit9 Server に接続できない状態で、そのエージェントを削除するには、Bit9 テクニカル サポートにご連絡ください。

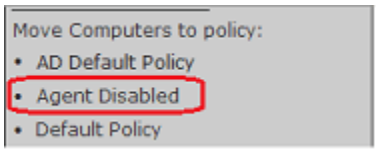
削除されたコンピューター上のファイルは、デフォルトでは 24 時間の短期間、［Files on Computers（コンピューター上のファイル）］インベントリに残ります。これらのファイルがどのように検索結果に表示されるかについては、「削除されたコンピューター上のファイル」（739 ページ）を参照してください。

Bit9 Server からコンピューターを削除する手順：

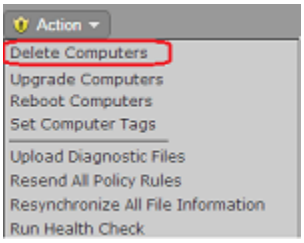
1. コンソール メニューで、[**Assets**（アセット）] > [**Computers**（コンピューター）] の順に選択します。[Computers（コンピューター）] ページが表示されます。
2. 削除するコンピューターを特定し、名前の隣のチェック ボックスをオンにします。



3. [Action（アクション）] メニューで、メニューからエージェント無効ポリシー（下に「Agent Disabled（エージェント無効）」と表示されていますが、任意の名前を使用できます。適用レベルとモードは「無効」である必要があります）の［Move（移動）］コマンドを選択します。



4. 確認ダイアログで、[**OK**] をクリックしてポリシーの変更を開始します。テーブルに表示されているコンピューターの説明を見て、変更の完了を確認します。
5. このコンピューターのエージェントがエージェント無効ポリシーに割り当てられ、「無効」の適用レベルが表示されたら、コンピューターからエージェントのソフトウェアを削除します。
6. [Computers（コンピューター）] ページで、エージェントを削除したコンピューターの名前を特定し、名前の隣のチェック ボックスをオンにします。
7. ［Action（アクション）］メニューで、［**Delete Computers**（コンピューターの削除）］を選択します。

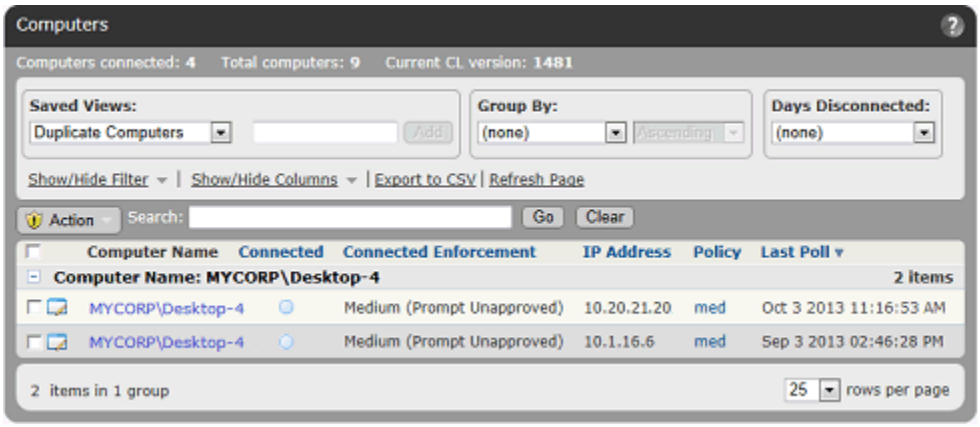


8. 確認ダイアログで [**OK**] をクリックして削除を完了します。

重複コンピューター

［Computers（コンピューター）］テーブルに、コンピューター名が重複して表示されることがあります。これは、エージェントで管理するコンピューターをオフラインにするか、再構成または修理した後で、以前のエージェントをアンインストールしてエントリをテーブルから削除しないまま、エージェントを再インストールした場合に発生する可能性があります。これはアセット管理の問題につながり、多くのコンピューターを定期的に再構成している大規模な組織では問題も大きくなります。

コンピューター名の重複を発見および排除しやすくするために、［Computers（コンピューター）］ビューには［Duplicate Computers（重複コンピューター）］という保存済みビューがあります。このビューのリストには、エージェントで管理するコンピューターのうち、エージェントで管理する別のコンピューターと名前が同じで、どちらも Bit9 で削除されていないものが含まれます。



［Duplicate Computers（重複コンピューター）］ビューには、コンピューターが名前でグループ化されて表示され、［Last Poll（最終ポーリング）］（エージェントとサーバーが最後に通信を行った日時）が示されているため、どのエントリのコンピューターが現在アクティブなエージェントに対応しているかがわかります。

注意

また、任意の［Computers（コンピューター）］テーブル ビューに［Duplicate（重複）］列を追加して、コンピューター名が重複している（値が［Yes（はい）］）か重複していないか（値が［No（いいえ）］）を区別できます。

第 5 章

ポリシーの作成と構成

この章では、ポリシーを作成し、そのポリシーの設定（適用レベルなど）を変更する方法について説明します。

セクション

ポリシーと適用レベルの概要

Bit9 エージェントが実行されている各コンピューターには、Bit9 Security Platform「ポリシー」が関連付けられています。ポリシーにより、そのポリシーのコンピューターすべてに共通のファイル制御定義が作成されます。各ポリシーは、一連の設定と全体的な適用レベルで構成されています。

「ポリシー設定」では、Bit9 エージェントの制御対象となるファイルや操作のタイプのほか、ポリシーを割り当てる方法や、ポリシーが適用されるコンピューター上のエージェントを自動アップグレードするかどうかなどを指定できます。

「適用レベル」では、ポリシー設定によって定義されたアクション、特にファイルへの書き込みやファイルの実行を、どの程度厳密に制御するかを定義します。以下の選択肢があります。

- High (Block Unapproved)（高（未承認をブロック））
- Medium (Prompt Unapproved)（中（未承認に対してプロンプトを表示））
- Low (Monitor Unapproved)（低（未承認を監視））
- None (Visibility)（なし（可視性））
- None (Disabled)（なし（無効））

注意

高、中、および低適用は、表示機能と制御機能の両方を備えた完全な Bit9 Security Platform でのみ使用できます。サイトのライセンスすべてが可視性のみの操作を対象としている場合、そのサイトは適用なしの可視性モードとエージェント無効モードに制限されます。

可視性モードでは、他の適用レベルを実施しているときにアクティビティをブロックする設定を選択できますが、こうした設定によってブロックや禁止が適用されることはありません。

ポリシーの作成

ポリシーを使用すると、Bit9 エージェントが実行されているコンピューターを、一般的なセキュリティ要件に応じてグループ化することができます。たとえば、営業、マーケティングなどの部門や、その他の組織的関係に基づいてポリシーを作成できます。また、特別なドメイン コントローラー ポリシーなど、コンピューターの目的固有のポリシーを作成することも可能です。すべてのコンピューターを対象とする会社全体の運用基準が1つだけ必要な場合は、作成するのはポリシーは 1 つでかまいませんが、通常は、複数のポリシーを作成します。

ポリシーの割り当て先は、通常、ユーザーではなくコンピューターですが、Active Directory データを使用すると、ユーザーごとにポリシーを割り当てることができます。各コンピューターには、現在のログオン ユーザー数に関係なく、一度に 1 つのポリシーしか指定できません。

ポリシーが作成されたら、そのポリシーには、さまざまな方法（Active Directory グループに基づいた自動的割り当てなど）でコンピューターを割り当てることができます。ポリシー割り当ての詳細については、第 4 章「コンピューターの管理」を参照してください。

重要

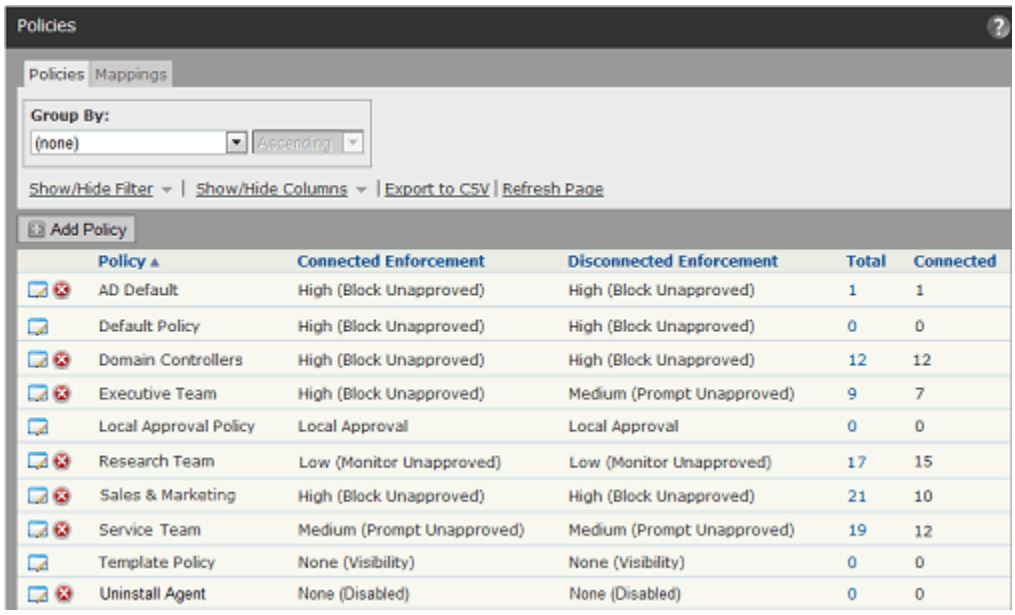
ポリシー名には、英数字と ISO-8559-1 セットの記号を使用できます。ISO-8559-1 セットの 32 ～ 127 の記号を使用できます。ただし、次の記号は例外になります。< > : " / \ | ? * # @

Unicode 文字またはポリシー名で予約されている記号を入力すると、警告ダイアログが表示されます。ポリシーを保存するには、禁止されている文字を名前から削除する必要があります。

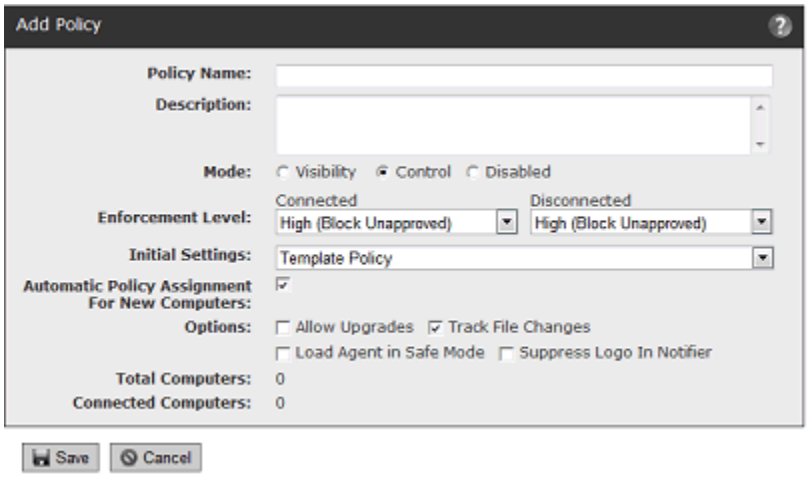
文字によっては、ポリシー名で許可されていても、その文字を使うことで、ポリシーのエージェント インストーラーの実行中にエラーが発生することがあります。Mac コンピューターに適用されるポリシーでは、名前に括弧とスペースを使用しないようにするか、インストーラーを実行するときは、これらの文字を「エスケープ」するようにしてください。

ポリシーの作成手順：

1. コンソール メニューで、[**Rules**（ルール）] > [**Policies**（ポリシー）] の順に選択します。[Policies（ポリシー）] ページが表示されます。



2. [Policies（ポリシー）] ページで、[**Add Policy**（ポリシーの追加）] ボタンをクリックします。[Add Policy（ポリシーの追加）] ページが表示されます（制御ポリシーについては、以下を参照）。



3. [Add Policy（ポリシーの追加）] ページで、ポリシー名を入力し、他のポリシー パラメーターを選択して定義します（表 18 を参照）。表示されるパラメーターは、ポリシーの設定や構成の選択内容によって異なります。

表 18：ポリシーの定義： メイン パネル

フィールド	説明
Policy name（ポリシー名）	ポリシーの名前。 このポリシーを使用するコンピューターまたはユーザーに対して使用する、セキュリティ レベル、機能、またはその他の共通要素を示す名前を選択します。 **注意**：一度ポリシーを作成すると、その名前を変更することはできないため、必ず有用でわかりやすい名前を選択してください。
Description（説明）	ポリシーのオプション情報。任意のテキストを入力できます
Mode（モード）	このポリシーのコンピューターが Bit9 Server と連携するときのモード。 [**Visibility**（可視性）]：ファイル追跡のみを指定します。Bit9 Server は、ファイルのアクティビティとイベントを追跡します。ファイルの実行と書き込みが、適用されているポリシー設定またはファイル禁止の影響を受けることはありません。可視性モードを選択すると、適用レベル メニューは表示されません。 制御ライセンスを購入していない場合、無効モード以外で選択できるのは、可視性モードだけです。 セキュリティ機能がコンピューターの動作を妨げている場合、または妨げる可能性がある場合は、可視性モードを使用します。たとえば、すべてのコンピューターにインストールできるファイル用の信頼済みディレクトリを構成するコンピューターに対して可視性モードを選択します。 [**Control**（制御）]：適用レベル メニューを有効にします。このメニューから、未承認ファイルおよび禁止ファイルの実行の制御レベルを選択できます。 [**Disabled**（無効）]：パススルー モードを指定します。ファイルのアクティビティが、エージェントによってブロックされることはなく、サーバーにレポートされることもありません。実行可能ファイルは、エージェントがインストールされていない場合と同じように実行されます。この設定は、エージェントをアンインストールするときに使用します。 無効モードの場合、サーバー上のコンピューターのファイル インベントリが最新の状態に維持されません。エージェントが後から有効になった場合にファイル情報とプロセス情報の間に差ができないように、一部の操作は監視されます（ただし、サーバーにはレポートされません）。

フィールド	説明
Connected Enforcement Level（接続済み適用レベル）	コンピューターがネットワークに接続されているときの、このポリシーのコンピューター保護レベル（制御モードではメニューのみが表示されます）。 [**High (Block Unapproved)**（高（未承認をブロック））]：設定可能な最高保護レベル。Bit9 Security Platform で追跡されているカテゴリの未承認ファイルまたは禁止ファイルは実行できません。イベント ログには、ブロックされたファイル実行が記録されます。 [**Medium (Prompt Unapproved)**（中（未承認に対してプロンプトを表示））]：エージェント コンピューターでは未承認の実行可能ファイルがブロックされますが、ファイルの実行を許可またはブロックするオプションが示されたダイアログ ボックスがユーザーに表示されます。明示的に禁止されたファイルの実行については、ユーザーが許可することはできません。 [**Low (Monitor Unapproved)**（低（未承認を監視））]：未承認の実行可能ファイルの実行が許可されますが、追跡されません。実行が許可されたファイルには、実行中の非実行可能ファイル（dll、com オブジェクト、ロード可能なリソースなど）、未承認スクリプト、未承認実行可能ファイルなどがあります。許可されたファイル実行の最初のインスタンスと、ブロックされたすべての実行に対して、イベントが記録されます。 高、中、低の各適用レベルでどのファイルがブロックされるかは、各ポリシー内の高度な設定の影響も受けます。 [Mode（モード）] 行で [**Visibility**（可視性）] と [**Disabled**（無効）] を設定すると、適用レベルが [**None**（なし）] になります。
Disconnected Enforcement Level（接続されていない適用レベル）	コンピューターと Bit9 Server が通信していないときの、このポリシーのコンピューター保護レベル。接続済み適用レベルが「低」（または「なし」）の場合、接続されていない適用レベルはオンラインと同じで、直接変更することはできません。接続済み適用レベルが「高」または「中」の場合、接続されていない適用レベルとして「高」または「中」を選択できます。接続済み適用レベルと異なっていてかまいません。
Initial Settings（初期設定）	新しいポリシーのテンプレートとして使用する既存のポリシー。ポリシーの作成時は表示されませんが、選択したポリシーのデバイス設定と高度な設定（のみ）が新しいポリシーに転送されます。詳細については、「テンプレート ポリシー」（194 ページ）を参照してください。
Automatic Policy Assignment for New Computers（新しいコンピューターへの自動ポリシー割り当て）	このボックスがオンの場合、AD ベースのポリシー割り当てが有効で、かつ構成されていると、エージェントのインストールに使用されたインストール パッケージに埋め込まれているポリシーに関係なく、このポリシーのインストーラーを使用した新しいコンピューターが AD マッピング ルールに従ってそのポリシーを取得します。オフの場合、インストール パッケージは、ポリシーと AD のマッピングは何の影響も及ぼさないと判断します。詳細については、「Active Directory マッピングによるポリシーの割り当て」（120 ページ）を参照してください。

フィールド	説明
Set automatic policy for existing computers（既存のコンピューターに対して自動ポリシーを設定する）	このチェックボックスは、[Automatic policy assignment for new computers（新しいコンピューターへの自動ポリシー割り当て）] ボックスがオンになっている場合にのみ表示されます。オンにすると、コンピューターが手動（自動以外）で現在のポリシーに割り当てられた場合に、その割り当てが自動ポリシー割り当てに変更されます。
Set manual policy for existing computers（既存のコンピューターに対して手動ポリシーを設定する）	このチェックボックスは、[Automatic policy assignment for new computers（新しいコンピューターへの自動ポリシー割り当て）] ボックスがオンになっている場合にのみ表示されます。オンにすると、コンピューターがポリシーに自動的に割り当てられた場合に、その割り当てが手動割り当てに変更されます。
オプション：Allow Upgrades（アップグレードを許可）	Bit9 Server が Bit9 エージェントの自動アップグレード用に構成されている場合、このボックスをオンにすると、ポリシーのコンピューターで Bit9 エージェントのアップグレードが通知およびスケジュールされます。（手動または Active Directory マッピングのいずれかによって）このポリシーに移動されたコンピューターもアップグレードされます。詳細については、「高度な構成オプション」（766 ページ）および「Bit9 Server のインストール」のアップグレード セクションを参照してください。Bit9 Server アップグレード中にのみ使用します。
オプション：Track File Changes（ファイル変更の追跡）	オンにすると（デフォルト）、コンピューター上のファイル変更（ファイルの追加、削除、または変更）が追跡され、この Bit9 Server のデータベースに追加されます。 SQL Express からフルバージョンの SQL Server にアップグレードされるのを待っている場合や、ファイル アクティビティを追跡したくないコンピューターを対象とした特別なポリシーでは、このオプションをオフにすると、パフォーマンスに関する問題が解決されることがあります。 **重要**：この機能をオフにすると、1 日後に、このポリシーの対象となるエージェントのファイル インベントリ情報が削除されます。[Computers on Files（コンピューター上のファイル）] テーブル、ファイルの検索、およびベースライン ドリフト レポートでは、こうしたコンピューターに関する正確な情報を確認できません。また、この機能をオフにした後にオンにすると、影響を受けるエージェントが強制的に再同期され、ファイル データベースが更新されるため、パフォーマンスに影響を及ぼすことがあります。

フィールド	説明
Load Agent in Safe Mode（セーフ モードでエージェントをロード）	このポリシーのコンピューターがセーフ モードでブートされたときに、セーフ モードでそのコンピューターの Bit9 エージェントをロードします。この場合、システムがセーフ モードであっても、エージェントはすべての適用アクティビティを実行します。完全保護には、ブート時にロードを行うエージェント カーネルと、ブート後にサービスとして実行されるエージェント自体が必要です。 **警告**：セーフ モードでの復旧操作はエージェントによって妨げられる可能性があるため、このオプションを使用するのは、セーフ モードを使用せずに復旧する手段が用意されている場合だけにしてください。エージェントをセーフ モードで実行できるようにする方法について不明な点がある場合は、Bit9 テクニカル サポートにお問い合わせください。
Suppress Logo in Notifier（通知のロゴの抑止）	いずれかの Bit9 ルールによってこのポリシーのエージェントで通知が表示されるときに、そのルールの通知定義にロゴが含まれていても、そのロゴを表示しません。
Total/Connected Computers（合計 / 接続済みコンピューター数）	[**Total Computers**（合計コンピューター数）] – Bit9 Server 上で、このポリシーによって管理されているコンピューターの合計数。プラットフォーム別のコンピューター数は括弧内に表示されます。 [**Connected Computers**（接続済みコンピューター数）] – Bit9 Server に現在接続され、このポリシーによって管理されているコンピューターの合計数。プラットフォーム別のコンピューター数は括弧内に表示されます。

4. このページでポリシー構成パラメーターを指定したら、[**Save**（保存）] ボタンをクリックします。[Policies（ポリシー）] ページの表に新しいポリシーが表示されます。
5. ポリシーのデバイス設定または高度な設定を変更するには、新しいポリシー名の横にある [View Details（詳細の表示）]（鉛筆）ボタンをクリックし、変更してから、[**Save**（保存）] をクリックします。こうした設定の編集の詳細については、「ポリシーの編集手順：」（197 ページ）を参照してください。デバイス設定と高度な設定は [Add Policy（ポリシーの追加）] ページには表示されません。この設定を表示するには、まずポリシーを保存する必要があります。

注意

Bit9 Security Platform のデバイス設定とその他のデバイス監視および制御機能の詳細については、第 11 章「デバイスの管理」を参照してください。

ポリシーと禁止の設定の適用時にクライアント コンピューターに表示される通知のカスタマイズについては、第 17 章「ブロック通知と承認要求」を参照してください。

ポリシー設定

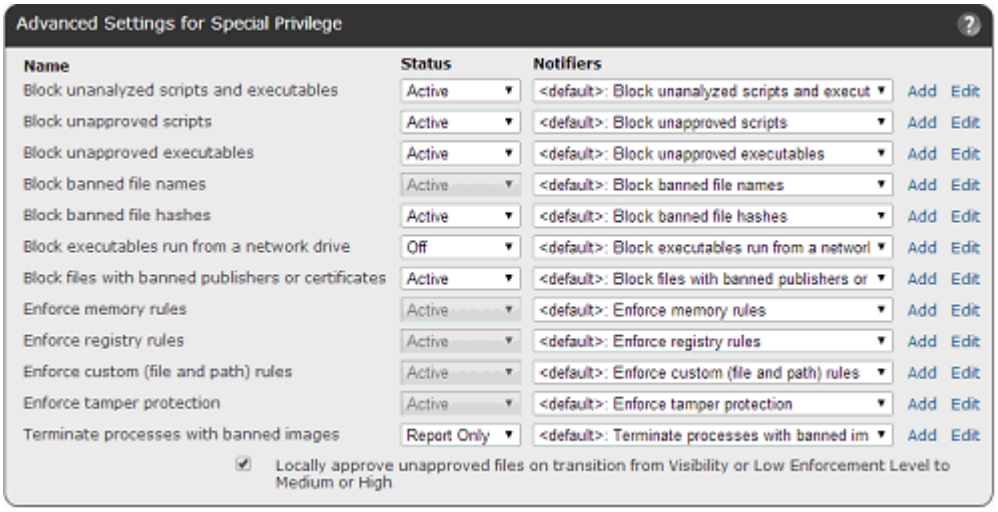
ポリシーの適用レベルは、全体的なセキュリティ レベルを設定し、ポリシーが未承認のファイルの実行をブロックするように構成されているか、許可するように構成されているかを確認します。動作をさらに細かく制御するには、詳細なポリシー設定を使用します。この設定はデバイス設定と高度な設定に分類されます。デバイス設定については、第 11 章「デバイスの管理」を参照してください。

重要

可視性モードでは、ファイルをブロックする設定を有効にできますが、この設定は、可視性モードのコンピューターには効果がありません。ファイルのブロックおよびその他の制御機能を有効にするには、ポリシーを制御モードにする必要があります。可視性モードではこの設定を情報提供の目的で、または今後制御モードに変更する予定があるときに引き続き有効にします。

高度な設定

アクティブの場合、高度な設定によって、指定したファイル アクティビティがブロックされ、他のルールが適用されます。



ファイルやアクティビティは、通常、複数のルールに影響されるため、設定をオフにした場合の結果はさまざまです。高度な設定には 3 つのオプションが用意されています。

表 19：ポリシーの高度な設定のオプション

設定のオプション	説明
Active（アクティブ）	設定が有効です。指定した適用レベルに従って、ファイルがブロックまたは許可されます。
Off（オフ）	設定が無効で、どの適用レベルも適用されません。ファイルの一致と設定は引き続き追跡されますが、ブロックされません。

設定のオプション	説明
Report Only（レポートのみ）	設定がアクティブになっていればブロックされていたはずであるアクションを許可するテスト状態で、「ブロックしていたはず」というイベントが［Events（イベント）］テーブルに記録されます。このオプションを使用すると、ファイルを実際にブロックせずに、ポリシーの設定と適用レベルが意図したとおりに動作することを確認できます。

アクションまたはファイルを「ブロック」する設定をオフにしても、そのアクションまたはファイルが「許可」されるとは限りません。同様に、アクションを「許可」する設定をオフにしても、そのアクションまたはファイルが「ブロック」されるとは限りません。［Events（イベント）］ページには、許可される予定だったファイルがブロックされた理由が示されています。

表 20 は、高度な設定と、その設定を［Active（アクティブ）］または［Off（オフ）］に設定した場合の影響を示しています。設定の中にはオフにできないものがありますが、ファイルの実行をブロックしたときに表示される「通知」を変更または無効にできるように、こうした設定についても説明します。

注意

- 「実行可能ファイル」と「スクリプト」については異なる設定があります。Bit9 Security Platform は、コンテンツに基づいてファイルが実行可能かどうかを判断します。一方、スクリプトはファイル拡張子で識別されます。Bit9 エージェントは、ファイルを確認した後、そのファイルのコンテンツに基づいて適切なポリシー設定を適用します。Bit9 Security Platform でのスクリプトの定義方法については、第 13 章「スクリプト ルール」を参照してください。
- 各設定に［Notifier（通知）］メニューがあり、このポリシーの設定がアクションがブロックをブロックしたときにエージェント コンピューターに表示される通知を選択できます。通知の選択と定義については、第 17 章「ブロック通知と承認要求」を参照してください。
- ソフトウェア禁止の詳細については、「ソフトウェアの承認と禁止」（271 ページ）を参照してください。特定のパスの特別なファイル処理に対するカスタム ルール作成の詳細については、第 12 章「カスタム ソフトウェア ルール」を参照してください。

表 20：高度な設定の動作

設定	Active（アクティブ）	Off（オフ）
Block unanalyzed scripts and executables（未分析のスクリプトおよび実行可能ファイルをブロック）	まだ分析されていない実行可能ファイル（.exe、.dll、.com など）とスクリプト ファイル（.bat、.vbs など）を追跡し、そのファイルを、ローカル承認モードで高、中、低の各適用レベルに従ってシステムに対してブロックします。 ユーザーまたはプロセスがスクリプトと実行可能ファイルを実行しようとした場合に、Bit9 Security Platform が想定した時間でファイル状態のランタイム チェックを完了できないと、そのスクリプトと実行可能ファイルは未分析としてレポートされます。これは、通常、ファイルのルート証明書の期限が切れたときや、その証明書を確認できないときに発生します。	実行を妨げる設定がない限り、未分析の実行可能ファイルとスクリプト ファイルの実行を許可します。この設定はお勧めしません。
Block unapproved scripts（未承認スクリプトをブロック）	未承認ステータスのスクリプト ファイル（.bat、.vbs など）を追跡し、次のように適用レベルに従ってブロックします。 • 高適用レベルでは、未承認スクリプトがブロックされます。 • 中適用レベルでは、未承認スクリプトがブロックされますが、ファイルを特定するダイアログが表示され、ユーザーはそのファイルを実行することを選択できます。 • 低適用レベルでは、ファイルの実行が許可されます。実行可能ファイルが最初に実行されたときにイベントが記録されます。 **注意**：第 13 章「スクリプト ルール」の表 54 は、Bit9 Security Platform によるファイル タイプが考慮されたスクリプトを示しています。	実行を妨げる設定がない限り、明示的に禁止されていないスクリプト ファイルの実行を許可します。

設定	Active（アクティブ）	Off（オフ）
Block unapproved executables（未承認実行可能ファイルをブロック）	未承認ステータスの実行可能ファイル（.exe、.dll、.com など）を追跡し、次のように適用レベルに従ってブロックまたは許可します。 • 高適用レベルでは、すべての未承認実行可能ファイルがブロックされます。 • 中適用レベルでは、未承認実行可能ファイルがブロックされますが、ファイルを特定するダイアログが表示され、ユーザーはそのファイルを実行することを選択できます。 • 低適用レベルでは、ファイルの実行が許可されます。ファイルが最初に実行されたときにイベントが記録されます。	実行を妨げる設定がない限り、明示的に禁止されていない未承認ファイルの実行を許可します。
Block banned file names（禁止ファイル名をブロック）	制御モードの場合、コンピューターでファイル名によって禁止されたファイルの実行をブロックします。	ポリシー ページでは無効にできませんが、個別の禁止を、ポリシー固有の禁止として構成できます。
Block banned file hashes（禁止ファイル ハッシュをブロック）	制御モードの場合、コンピューター上のすべての禁止ハッシュをブロックします。	禁止ハッシュ設定を無効にして、実行を妨げる設定がない限り、禁止ハッシュの実行を許可します。
Block executables run from a network drive（ネットワーク ドライブからの実行可能ファイルの実行をブロック）	制御モードの場合、ネットワーク経由で実行されるコンピューター上のファイル（承認ファイルを含む）の実行をブロックします。 **プラットフォームに関する注意**：この設定は、Windows エージェントに対してのみ有効です。	実行を妨げる設定がない限り、未承認でない、または明示的に禁止されていないネットワーク実行可能ファイルの実行を許可します。
Block files with banned publishers or certificates（公開者または証明書が禁止されているファイルをブロック）	制御モードの場合、公開者（または証明書）が禁止されているファイルの実行をブロックします。	実行を妨げる設定がない限り、公開者 / 証明書が禁止されているファイルの実行を許可します。

設定	Active（アクティブ）	Off（オフ）
Enforce memory rules（メモリ ルールを適用）	有効なすべてのメモリ　アクセス ルール、制御ルール、およびレポート作成ルールを適用します。 **プラットフォームに関する注意**：この設定は、Windows エージェントに対してのみ有効です。	ポリシー ページでは無効にできませんが、個別のルールを、ポリシー固有のルールとして構成できます。
Enforce registry rules（レジストリ ルールを適用）	有効なすべてのレジストリ アクセス ルールとレポート作成ルールを、このポリシーに適用します。 **プラットフォームに関する注意**：この設定は、Windows エージェントに対してのみ有効です。	ポリシー ページでは無効にできませんが、個別のルールを、ポリシー固有のルールとして構成できます。
Enforce custom (file and path) rules（カスタム（ファイルおよびパス）ルールを適用）	有効なすべてのカスタム ルール（定義されたパスの特別なファイル処理）をこのポリシーに適用します。カスタム ルールを構成するには、コンソール メニューで［Software Rules（ソフトウェア ルール）］を選択し、［Custom（カスタム）］タブをクリックします。	ポリシー ページでは無効にできませんが、個別のルールを、ポリシー固有のルールとして構成できます。
Enforce tamper protection（改ざんからの保護を適用）	Bit9 エージェントで改ざんを回避するためのルールを適用します。	ポリシーに対して無効にすることはできません。特定のコンピューターで改ざんからの保護をオフにする必要がある場合は、Bit9 テクニカル サポートにご連絡ください。
Terminate processes with banned images（禁止イメージを含むプロセスを終了）	ファイルが禁止されている場合は、そのファイルと一致する現在実行中のプロセスを終了します。	実行中に禁止されたファイルが引き続き実行できます。
Locally approve unapproved files on transition from Visibility or Low Enforcement Level to Medium or High（可視性または低適用レベルから中適用レベルまたは高適用レベルへの移行中に未承認ファイルをローカルで承認）	オンにすると、ポリシーの適用レベルが「低」（または「なし」）から「中」または「高」に変更されるときに、特定の未承認ファイルがローカルで承認されます。これは、低（または「なし」）適用レベル ポリシーのコンピューターに最初に未承認として見つかったファイルにのみ適用されます。こうしたファイルのローカル状態の詳細は「未承認」です。 ローカル承認方法の詳細については、「ファイルのローカル承認」（308 ページ）を参照してください。	オフにすると、適用レベルを変更しても、このポリシーのファイルのローカル状態は影響を受けません。

テンプレート ポリシーとデフォルト ポリシー

デフォルト ポリシー

Bit9 Security Platform には、デフォルト ポリシーというポリシーが組み込まれています。このポリシーにコンピューターが割り当てられる状況を次に示します。

- ポリシーの割り当てに AD マッピングを使っている場合、Bit9 Security Platform の最初の構成では、デフォルト ポリシーには、その他のマッピング ルールと一致しないコンピューターが割り当てられます。ただし、一致しないコンピューターの割り当て先のポリシーは変更することができるため、一般的には、「AD デフォルト」ポリシーを別に作成することをお勧めします。詳細については、「Active Directory マッピングによるポリシーの割り当て」（120 ページ）を参照してください。
- 存在しない（削除された）ポリシーのコンピューターが Bit9 Server にレポートされると、そのコンピューターはデフォルト ポリシーに自動的に移動され、デフォルト設定に基づいて適用されます。この状況に対処する方法については、「デフォルト ポリシーからのコンピューターの復元」（174 ページ）を参照してください。

制御機能のライセンスが付与されている場合、デフォルト ポリシーの適用レベルを「高」（未承認をブロック）に設定して、コンピューターをデフォルト ポリシーに切り替えると、禁止ファイルと未承認ファイルは両方とも実行できません。未承認ファイルに関する懸念は少ないけれども、こうしたファイルをユーザーの介入なしで実行できるようにしたくない場合は、適用レベルを「中」に設定します。また、デフォルト ポリシーの他の設定を編集することもできます。

注意

コンピューターが予期せずデフォルト ポリシーに割り当てられることがあります。このため、［Locally approve unapproved files on transition from Visibility or Low Enforcement Level to Medium or High（可視性または低適用レベルから中適用レベルまたは高適用レベルへの移行中に未承認ファイルをローカルで承認）］の最初のポリシー設定はオフに設定されています（ボックスがオフになっています）。オフでない場合、予期せずデフォルト ポリシーへの移行が行われたときに、多くのファイルが意に反してローカルで承認される可能性があります。この設定の詳細については、「適用レベル変更時の自動ローカル承認」（309 ページ）を参照してください。

テンプレート ポリシー

組み込みテンプレート ポリシーの目的は、他のポリシーを作成するときの「テンプレート」として使用することです。デフォルトでは、作成した最初のポリシーの初期デバイス設定と高度な設定は、このテンプレート ポリシーの設定に基づいています。ただし、デフォルト ポリシーなどの他の既存のポリシーに基づいて設定されるように変更することもできます。

注意

ポリシーが継承するのは、テンプレート ポリシーの「デバイス設定」と「高度な設定」だけです。適用レベルなど、[Add/Edit Policy（ポリシーの追加 / 編集）] ページの最上位パネルの設定は継承されません。新しいポリシーを保存すると、[Edit Policy（ポリシーの編集）] ページにデバイス設定と高度な設定が表示されます。

よく使用されるデバイス設定と高度な設定をテンプレート ポリシーに追加することで、簡単にポリシーを作成できるようになります。一度作成したポリシーとテンプレート ポリシーは関連付けられていないため、作成した新しいポリシーのすべての設定を変更することができます。

ポリシーの構成で重要なのは、アクションをブロックする可能性があるポリシー設定に通知を割り当てることです。ポリシー設定ごとに 1 つの通知（「通知なし」を選択することも可能）が割り当てられ、メッセージは、ブロックを発生させた設定によって異なります。デフォルトのメッセージを変更する場合は、他のポリシーを作成する「前に」テンプレート ポリシーを変更することをお勧めします。詳細については、「通知のカスタマイズと作成」(553 ページ) を参照してください。

テンプレート ポリシーとデフォルト ポリシーの主な違いは、[Locally approve unapproved files on transition from Visibility or Low Enforcement Level to Medium or High（可視性または低適用レベルから中適用レベルまたは高適用レベルへの移行中に未承認ファイルをローカルで承認）] と呼ばれる高度な設定です。この設定は、通常、新しく作成されたポリシーに対して有効にするため、テンプレート ポリシーではデフォルトで有効になっています（また、表示されていません）。

テンプレート ポリシーの特性を次に示します。

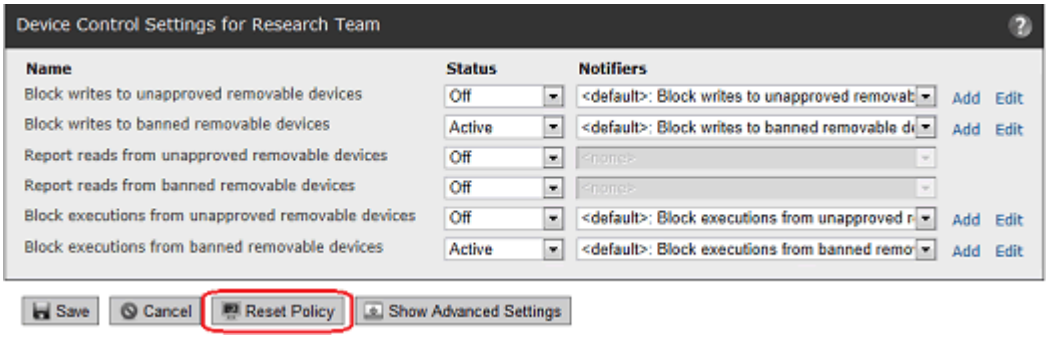
- [Policies（ポリシー）] ページとその [Edit（編集）] ページにのみ表示されます
- コンピューターに割り当てることはできません
- テンプレート ポリシーを指定する AD マッピング ルールを作成することはできません
- テンプレート ポリシーに対応するエージェント インストール パッケージはありません
- デフォルト ポリシーと同様、テンプレート ポリシーは削除できません
- [Locally approve unapproved files on transition from Visibility or Low Enforcement Level to Medium or High（可視性または低適用レベルから中適用レベルまたは高適用レベルへの移行中に未承認ファイルをローカルで承認）] 設定は表示されませんが、自動的に有効になります

重要

新しいポリシーを作成するときは、そのポリシーを作成するときに基にした既存のポリシーから継承した設定値を必ず確認し、必要に応じて変更してください。

ポリシーをテンプレート ポリシーの設定にリセット

各ポリシーの［Edit Policy（ポリシーの設定）］ページでは、［Device Settings（デバイスの設定）］テーブルのすぐ下に［**Reset Policy**（ポリシーのリセット）］ボタンがあります。



このボタンを押して、確認ダイアログで [**OK**] をクリックすると、デバイス設定と高度な設定がテンプレート ポリシーの「現在」の設定にリセットされます。

重要

リセット ダイアログ ボックスで [**OK**] をクリックすると、ポリシー設定がリセットされます。［**Save**（保存）］をクリックする必要はありません。リセットされないようにするには、「確認ダイアログ ボックス」でキャンセルする必要があります。［Edit Policy（ポリシーの編集）］ページの［**Cancel**（キャンセル）］をクリックしても、変更を防ぐことはできません。

改ざんからの保護設定

改ざんからの保護設定により、クライアント コンピューターで Bit9 アプリケーション ディレクトリに書き込もうとしたり、Bit9 エージェント ファイルを変更しようとしたりする試みがブロックされます。改ざんからの保護はポリシーごとに無効にできませんが、［Computer Details（コンピューターの詳細）］ページの［Advanced（詳細）］メニューを使用すれば、システムに対して無効にできますが、この設定を変更する前に、Bit9 テクニカル サポートにご連絡ください。

コンピューターがエージェント無効モードでない限り、コンピューター ユーザーがエージェントをアンインストールすることはできません。

注意

独自のディレクトリ保護ポリシーを指定できます。第 12 章「カスタム ソフトウェア ルール」を参照してください

コンピューターからの Bit9 エージェントの削除の詳細については、「Bit9 エージェントのアンインストール」（151 ページ）を参照してください。

ポリシーの編集

ポリシーの基本的な定義（説明を含む）と適用レベルは、[Edit Policy（ポリシーの編集）] ページの上部のパネルで編集できます。ポリシーの「名前」は変更できません。

デバイス設定と高度な設定のほとんどで、次の操作を行うことができます。

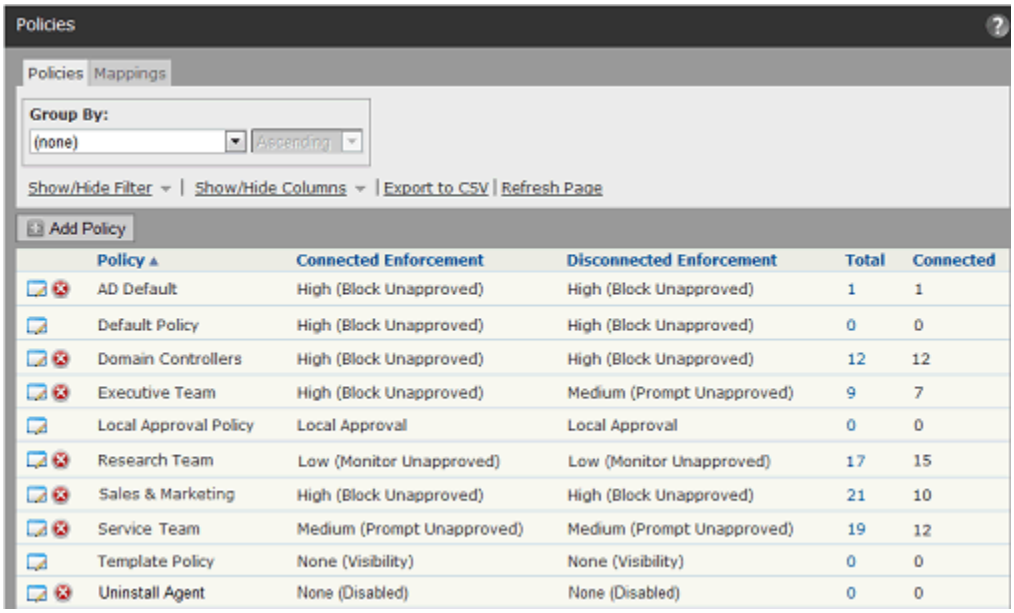
- オンまたはオフにする
- レポートのみの状態に切り替える。この状態の場合は、有効化されていれば実行していたはずである処理をレポートする
- 別の「通知」（または通知なし）を選択する。この通知は、アクティブなポリシー設定の結果としてアクションがブロックされたときに表示されるダイアログ ボックスです。この通知については、第 17 章「ブロック通知と承認要求」を参照してください

設定の中にはオプションが少なかったり、このリスト以外のオプションが示されたりするものがあります。

> **注意**
>
> ポリシー設定は無効にできますが、作成または削除することはできません。すべてのポリシーの基準設定名（「Block unapproved scripts（未承認スクリプトをブロック）」など）は変更できません。

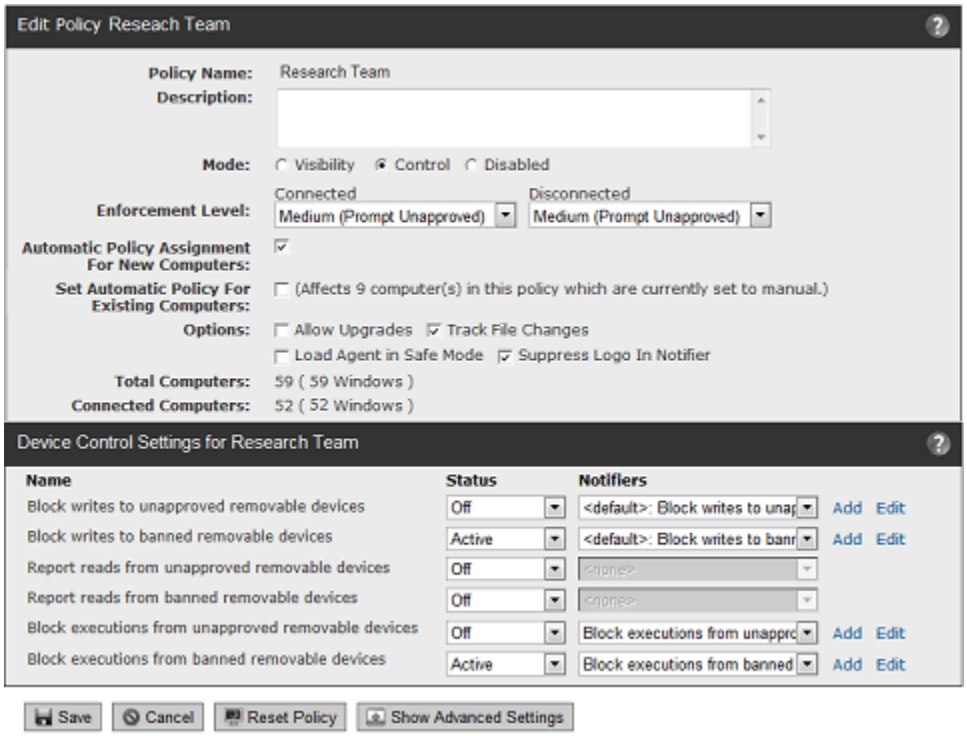
ポリシーの編集手順：

1. コンソール メニューで、[**Rules**（ルール）] > [**Policies**（ポリシー）] の順に選択します。[Policies（ポリシー）] ページが表示されます。



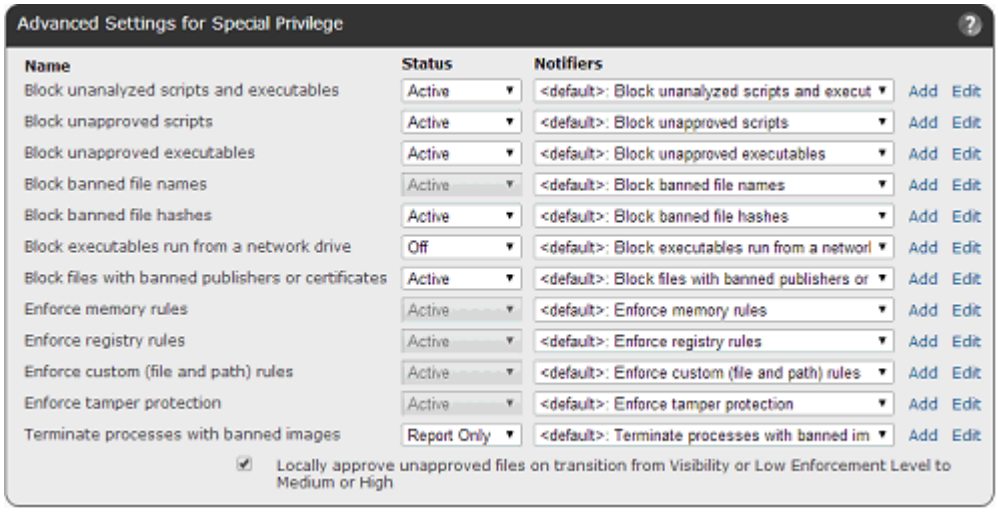
Policy	Connected Enforcement	Disconnected Enforcement	Total	Connected
AD Default	High (Block Unapproved)	High (Block Unapproved)	1	1
Default Policy	High (Block Unapproved)	High (Block Unapproved)	0	0
Domain Controllers	High (Block Unapproved)	High (Block Unapproved)	12	12
Executive Team	High (Block Unapproved)	Medium (Prompt Unapproved)	9	7
Local Approval Policy	Local Approval	Local Approval	0	0
Research Team	Low (Monitor Unapproved)	Low (Monitor Unapproved)	17	15
Sales & Marketing	High (Block Unapproved)	High (Block Unapproved)	21	10
Service Team	Medium (Prompt Unapproved)	Medium (Prompt Unapproved)	19	12
Template Policy	None (Visibility)	None (Visibility)	0	0
Uninstall Agent	None (Disabled)	None (Disabled)	0	0

2. [Policies（ポリシー）] ページで、編集するポリシー名の隣の [View Details（詳細の表示）]（ファイルと鉛筆）ボタンをクリックします。[Edit Policy（ポリシーの編集）] ページが表示されます。



3. メイン パネルで詳細を編集します。それには、適切なボックスをオンまたはオフにして、テキストを入力し、他のモードや適用レベルを選択します。表示されるパラメーターは、他のポリシー設定や構成の選択内容によって異なる場合があります。こうした設定の詳細については、表 18、「ポリシーの定義：メイン パネル」185 ページを参照してください。

4. ［Edit Policy（ポリシーの編集）］ページで、［**Show Advanced Settings**（高度な設定の表示）］ボタンをクリックして、このポリシーに関連付けられている残りの設定を表示します。



5. ［Device Control Settings（デバイス制御設定）］テーブルのドロップダウン メニューを使用して、変更する設定の状態として、［**Off**（オフ）］、［**Active**（アクティブ）］、［**Report Only**（レポートのみ）］のいずれかを選択します（読み取り設定の場合、［Active（アクティブ）］は選択できません）。これらの設定については、表 43、「デバイス制御設定の動作」386 ページを参照してください。
プラットフォームに関する注意：このデバイスの可視性および制御機能は、Windows コンピューターに対してのみ有効です。

6. ［Advanced Settings（高度な設定）］テーブルのドロップダウン メニューを使用して、変更する設定の状態として、［**Active**（アクティブ）］（オン）、［**Report Only**（レポートのみ）］（オン、ただし実施されない）、［**Off**（オフ）］のいずれかを選択します。これらの設定については、表 20、「高度な設定の動作」191 ページを参照してください。
注意：高度な設定の中には変更できないものがあります。固定された設定の場合、メニュー ボックスの値は灰色で表示されます。

7. ［Locally approve unapproved files on transition from Visibility or Low Enforcement Level to Medium or High（可視性または低適用レベルから中適用レベルまたは高適用レベルへの移行中に未承認ファイルをローカルで承認）］の設定を変更するには、このボックスをオンまたはオフにします。

8. エージェント コンピューター上でデバイス設定または高度な設定によってアクションがブロックされたときに表示される通知をカスタマイズするには、その設定の横にある［Notifiers（通知）］メニューから別の通知を選択して、通知を**編集**するか（この通知が使用されるすべての場所に影響します）、新しい通知を**追加**して定義します。詳細については、「通知のカスタマイズと作成」（553 ページ）を参照してください。

9. ポリシー設定の変更が完了したら、［**Save**（保存）］をクリックします。変更が保存され、［Policies（ポリシー）］テーブルが再表示されます。

ポリシー詳細の関連ビュー

［Edit Policy（ポリシーの編集）］ページには［Related Views（関連ビュー）］メニューがあり、ポリシーに関連するファイルとファイル ルールの情報を提供するリンクが設定されています。

- ［All files on computers in this policy（このポリシー内のコンピューター上のすべてのファイル）］により、ポリシーに割り当てられたコンピューター上の、追跡済みファイルのインスタンスすべてが表示される［Find Files（ファイルの検索）］ページが開きます。
- ［Unapproved files on computers in this policy（このポリシー内のコンピューター上の未承認ファイル）］により、このポリシーに割り当てられたコンピューター上の、ローカル状態が未承認のすべてのインスタンスが示された［Find Files（ファイルの検索）］ページが開きます。これは、ポリシー設定がそのコンピューター上のファイルに実際にどのように影響するかを確認するうえで役立ちます。
「ローカル状態の詳細」が「未承認」のファイルのみが表示されるように、他のフィルターを結果に追加できます。このポリシーに対して自動承認ボック

スがオンになっている場合、このファイルは、適用レベルが「低」から「中」または「高」のいずれかに変更されることで承認されます。

- [File bans and approvals that apply to this policy（このポリシーに適用されるファイルの禁止と承認）] により、[Software Rules/Files（ソフトウェア ルール / ファイル）] タブのフィルター処理されたビューが開きます。このビューには、すべてのポリシーに適用する、またはこのポリシーに適用することを指定する、ファイル禁止とファイル承認が表示されています。これは、このポリシーの適用レベルを変更するか、他の設定を変更するかを決めるときに役に立つ場合があります。
- [Computers manually assigned to this policy（このポリシーに手動で割り当てられたコンピューター）] により、[Computers（コンピューター）] ページのフィルター処理されたビューが開きます。このビューには、ポリシーに手動で割り当てられた（つまり、AD マッピングに割り当てられなかった）コンピューターが表示されています。

適用レベル

適用レベルはBit9エージェントが実行されているコンピューターに適用される保護レベルで、ポリシーごとに指定されます。適用レベルはそれぞれ制限が異なっています。ファイル アクションがポリシー設定に対してどのように制御されるかは、適用レベルの影響を受けます。Bit9 Security Platform のファイル ブロック機能およびその他の制御機能は、適用レベルと、有効になっているより具体的なポリシー設定（ポリシー固有の禁止など）の両方によって異なります。

制御モードで、適用レベルとして [High (Block Unapproved)（高（未承認をブロック））]、[Low (Monitor Unapproved)（低（未承認を監視））]、または [Medium (Prompt Unapproved)（中（未承認に対してプロンプトを表示））] をメニューから選択します。[None (Visibility)（なし（可視性））] モードと [None (Disabled)（なし（無効））] モードの場合、適用レベルは自動的に [None（なし）] が指定されます。

表 21：適用レベル

適用レベル	使用する状況：
High (Block Unapproved)（高（未承認をブロック））	最高保護レベルが必要な場合や、ポリシーのコンピューターで実行するアプリケーションを事前承認するのが現実的であるときに、高適用レベルを使用します。 高適用レベルでは、実行が明示的に承認されたファイルのみが許可されます。 アプリケーション構成がほとんど変わらないコンピューター、たとえばサーバー、専用システムなどに、高適用レベルを使用することをお勧めします。アプリケーション構成が動的に変化するコンピューターについては、信頼済みディレクトリ、信頼済みユーザー、承認済みの公開者、有効なアップデーター、またはレピュテーション承認によってファイルを事前承認する場合に、高適用レベルを使用できることがあります。 Bit9 Server で既に特定され禁止されているファイルを除き、コンピューター上のすべてのファイルが、Bit9 エージェントをインストールする前にローカルで承認され、そのコンピューター上での高適用レベルに基づいて実行できます。 制御モードの場合に、高適用レベルをポリシーで使用できます。

適用レベル	使用する状況：
Medium (Prompt Unapproved)（中（未承認に対してプロンプトを表示））	未承認ファイルがそのまま実行されるのを防ぐ必要があるが、こうしたファイルを完全にはブロックしたくない、という条件で動作させるには、中適用レベルを使用します。 中適用レベルでは、すべての未承認ファイル実行がブロックされますが、クライアント コンピューターにダイアログが表示され、ユーザーがそのファイルを実行するかどうかを決めることができます。ユーザーがファイルの実行を許可すると、ファイルはそのコンピューターでローカル承認され、常に実行できるようになります。未承認ファイルがネットワーク共有またはリムーバブル デバイスからリモートで実行されている場合、実行の承認は一時的なものです（3 日間だけ承認されます）。 **プラットフォームに関する注意**：リムーバブル ドライブまたはネットワーク ドライブの中には、特に Windows 以外のシステムでは Bit9 Security Platform によって認識されないものがあります。こうしたドライブから実行されたファイルは、ローカル ファイルのように処理されます。 明示的に禁止されたファイルを、中適用レベルで実行することはできません。 制御モードの場合に、中適用レベルをポリシーで使用できます。
Low (Monitor Unapproved)（低（未承認を監視））	不明ファイルに関する懸念がなく、ブロックする必要があるのが明示的に禁止されているファイルだけの場合は、低適用レベルを使用します。 低適用レベルでは、禁止されたファイルがブロックされますが、ユーザーは承認または未承認（禁止も承認もされていない）ソフトウェアをインストールできます。未承認ファイルについては、実行が許可されていますが、監視が可能で、必要に応じて緊急ロックダウンで対応できます。 制御モードの場合に、低適用レベルをポリシーで使用できます。
None (Visibility)（なし（可視性））	ブロックせずにファイルのアクティビティを追跡するには、適用レベルを［None (Visibility)（なし（可視性））］に設定します。 可視性モードでは、Bit9 のレポート作成およびアセット管理機能（ドリフト レポート、イベント レポート、ファイル インベントリなど）によって、コンピューター上での実行可能ファイルのアクティビティが追跡されますが、ルールは適用されません。ここから、より制御された環境を実装していくことができます。 ［Mode（モード）］行で［Visibility（可視性）］をクリックして、このレベルを選択します。

適用レベル	使用する状況：
None (Disabled)（なし（無効））	すべての適用と追跡アクティビティを停止するには、[None (Disabled)（なし（無効））] モードを選択します。この選択は、次の場合に実行します。 • システム障害をデバッグできるように、Bit9 サポート スタッフからエージェントを無効にするよう指示された。 • コンピューターから Bit9 エージェントを削除する予定である。エージェントを削除し、Bit9 Server からコンピューターを削除するには、コンピューターを [None (Disabled)（なし（無効））] モードにしておく必要があります。 コンピューターのエージェントを無効にした場合、そのコンピューターのファイル データベースは、エージェント コンピューターから削除されますが、サーバーには 1 日残ります。ファイルを他の適用レベルのポリシーに移動すると、エージェント無効モードのコンピューターにより、そのファイルは再初期化されます。 **注意**：エージェントが後から有効になった場合にファイル情報とプロセス情報の間に差ができないように、操作の中には、[None (Disabled)（なし（無効））] モードのエージェントによって引き続き監視されるものもあります（ただし、こうした操作はサーバーにレポートされません）。通常、エージェント コンピューターでのこの処理に必要なリソースはわずかですが、書き込み数が膨大だと、その影響が顕著になる可能性があります。 [Mode（モード）] 行で [Disabled（無効）] をクリックして、このレベルを選択します。

ポリシー設定への適用レベルの影響

適用レベルは、ポリシー設定およびその他のルールと連携して、さまざまなタイプのファイル アクションが許可される条件を制御します。表 22 は、ファイル アクティビティが、適用レベルと次の設定の組み合わせによってどのような影響を受けるかを示しています。

- 「アクティブ」な高度なポリシー設定とネットワーク全体のファイル禁止
- 「アクティブ」に設定されたデバイス制御の設定

表 22：適用レベル別のアクティブなポリシー設定の影響

アクティブなポリシーの設定	適用レベル				
	None (Disabled)（なし（無効））	None (Visibility)（なし（可視性））	Low (Monitor Approved)（低（承認を監視））	Medium (Prompt Unapproved)（中（未承認に対してプロンプトを表示））	High (Block Unapproved)（高（未承認をブロック））
Block unanalyzed scripts & executables（未分析のスクリプトおよび実行可能ファイルをブロック）	オフ	許可	ブロック	ブロック	ブロック
Block unapproved scripts（未承認スクリプトをブロック）	オフ	許可	許可	プロンプト	ブロック
Block unapproved executables（未承認実行可能ファイルをブロック）	オフ	許可	許可	プロンプト	ブロック
Block banned file names（禁止ファイル名をブロック）（無効化できません）	オフ	許可して報告	ブロック	ブロック	ブロック
Block banned file hashes（禁止ファイル ハッシュをブロック）	オフ	許可して報告	ブロック	ブロック	ブロック
Enforce memory rules（メモリ ルールを適用）（無効化できません）**	オフ	非ブロック アクションおよび報告	ブロック（指定した場合）	ブロック（指定した場合）	ブロック（指定した場合）
Enforce registry rules（レジストリ ルールを適用）（無効化できません）**	オフ	非ブロック アクションおよび報告	ブロック（指定した場合）	ブロック（指定した場合）	ブロック（指定した場合）
Enforce custom (file and path) rules（カスタム（ファイルおよびパス）ルールを適用）（無効化できません）**	オフ	非ブロック アクションおよび報告	ブロック（指定した場合）	ブロック（指定した場合）	ブロック（指定した場合）
Enforce tamper protection（改ざんからの保護を適用）（無効化できません）	基本	フル	フル	フル	フル
Terminate processes with banned images（禁止イメージを含むプロセスを終了）	オフ	続行して報告	終了	終了	終了
Block executables run from a network drive（ネットワーク ドライブからの実行可能ファイルの実行をブロック）*	オフ	許可して報告	ブロック	ブロック	ブロック
Block writes to unapproved removable devices（未承認リムーバブル デバイスへの書き込みをブロック）*	オフ	許可して報告	ブロック	ブロック	ブロック
Block files with banned publishers or certificates（公開者または証明書が禁止されているファイルをブロック）	オフ	許可して報告	ブロック	ブロック	ブロック
Block writes to unapproved removable devices（未承認リムーバブル デバイスへの書き込みをブロック）*	オフ	許可して報告	ブロック	ブロック	ブロック
Block writes to banned removable devices（禁止リムーバブル デバイスへの書き込みをブロック）*	オフ	許可して報告	ブロック	ブロック	ブロック
Report reads from unapproved removable devices（未承認リムーバブル デバイスからの読み取りを報告）*	オフ	許可して報告	許可して報告	許可して報告	許可して報告
Report reads from banned removable devices（禁止リムーバブル デバイスからの読み取りを報告）*	オフ	許可して報告	許可して報告	許可して報告	許可して報告
Block execution from unapproved removable devices（未承認リムーバブル デバイスからの実行をブロック）*	オフ	許可して報告	ブロック	ブロック	ブロック
Block execution from banned removable devices（禁止リムーバブル デバイスからの実行をブロック）*	オフ	許可して報告	ブロック	ブロック	ブロック

* デバイスとネットワーク ドライブのルールは Windows コンピューターにのみ適用されます。
** メモリ、レジストリ、およびカスタム ルールで実行可能なアクションには、多数の非ブロック オプションが含まれます。

注意

- 未承認ファイルを実行しようとして、中適用レベルによってダイアログが生成されるとき、いずれかのオプション（ブロックまたは許可）がイベントとして記録されます。また、低適用レベルの場合は、未承認ファイルを実行すると、イベントが生成されます。
- ［Edit Policy（ポリシーの編集）］ページの［Related Views（関連ビュー）］メニューには［Unapproved files on computers in this policy（このポリシー内のコンピューター上の未承認ファイル）］リンクがあります。未承認ファイルの処理方法は適用レベルの影響を受けるため、このリンクは、適用レベルの設定方法や、特定のコンピューターを現在のポリシーに割り当てたままにするかどうかを決めるうえで役立ちます。

ローカル承認用の特別な適用レベル

Bit Security Platform により、ローカル承認のコンピューターに対して特別な適用レベルが設定されます。この適用レベルはシステム用に予約されており、直接選択することはできません。ソフトウェアのローカル承認は、特に高適用レベルのコンピューターを対象としています。

ポリシー適用レベルの変更

コンピューター グループのルールの適用レベルを変更するには、そのグループを別のポリシーに移動します。コンピューターの移動については、「別のポリシーへのコンピューターの移動」（173 ページ）を参照してください。

また、次のいずれかの方法を使用して、現在のポリシーに適用されている適用レベルを引き上げたり引き下げたりすることもできます。

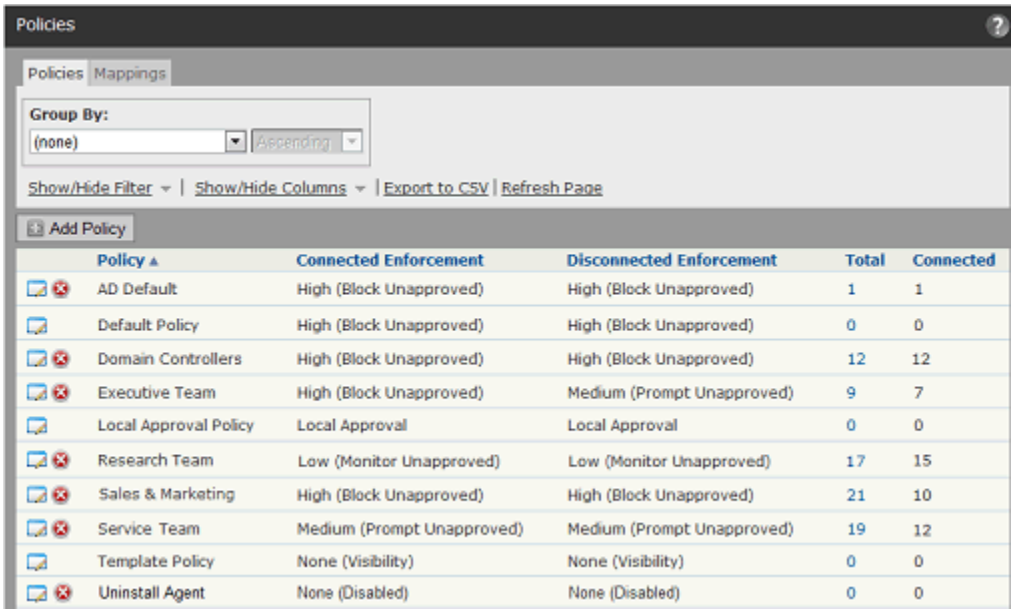
- 制御モードのまま適用レベルを変更する場合は、ポリシーの接続済み適用レベルと接続されていない適用レベルのメニューを編集することで、制御適用レベルを切り替えます。たとえば、保護を強化するには、低（未承認を監視）適用レベルまたは中（未承認に対してプロンプトを表示）適用レベルのポリシーを、高（未承認をブロック）適用レベルに切り替えます。
- 制御モードの場合に制御を解除するには、可視性モードに切り替えます。これにより、適用レベルが［None (Visibility)（なし（可視性））］に変更されます。
- 可視性モードの場合は、制御モードに切り替えて、メニューから新しい適用レベルを選択します。

重要

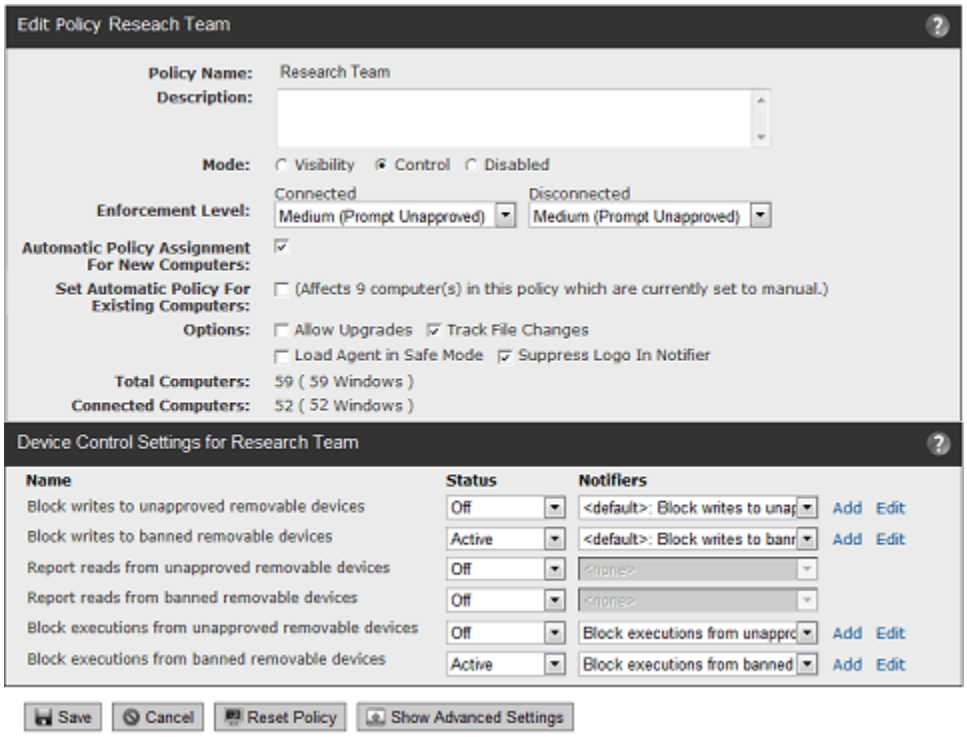
1 回の操作で多くのエージェントを無効または再度有効にすることはお勧めしません。エージェント無効モードに切り替えると、Bit9 エージェントによって提供されている適用、レポート作成、および追跡が解除されます。エージェント無効モードから切り替えると、ポリシー内のエージェント数によっては、パフォーマンスに大きな影響が及ぶことがあります。エージェント無効モードから切り替わった各エージェントで再初期化が行われ、新しくインストールされたエージェントと同じプロセスが実行されます。

制御モードの場合に、ポリシーの適用レベルを変更する手順：

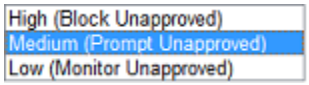
1. コンソール メニューで、[**Rules**（ルール）] > [**Policies**（ポリシー）] の順に選択します。[Policies（ポリシー）] ページが表示されます。



2. [Policies（ポリシー）] ページで、編集するポリシー名の隣の [View Details（詳細の表示）]（ファイルと鉛筆）ボタンをクリックします。[Edit Policy（ポリシーの編集）] ページが表示されます。



3. モードを切り替えるには、目的のモードの横にあるボタンをクリックします。
4. 制御モードで適用レベルを変更するには、ドロップダウン　　メニューから［Connected Enforcement Level（接続済み適用レベル）］を選択します。



5. 接続済み適用レベルとして「高」または「中」を選択した場合は、ドロップダウン メニューから、別の接続されていない適用レベルを選択できます。
6. ポリシーに対して必要な変更を行います。ポリシー設定の詳細については、「ポリシー設定」（189 ページ）を参照してください。
7. 変更を保存するには、ページ下部の［Save（保存）］ボタンをクリックします。

すべてのコンピューターのロックダウン

Bit9 コンソールのホーム ページには、Bit9 Security Platform 管理対象コンピューターすべての適用レベルを「高」に変更する、緊急ロックダウン ボタンがあります。緊急ロックダウン中、適用設定が無効になっていないポリシーを含むアクティブなエージェントは次のように動作します。

- 禁止ファイルがブロックされます。
- 緊急ロックダウンの「後」に現れたすべての未承認ファイルがブロックされます。
- 未承認のままの既存の未承認ファイルすべてがブロックされます。

- 以下で説明するように、一部のファイルがローカルで承認され、実行できます。
- 緊急ロックダウンが開始されたときにオフラインだったコンピューターについては、Bit9 Server への再接続時に、ロックダウンが有効のままの場合はロックダウンします。
- ロックダウンはすべてのアクティブ エージェント（可視性のみモードのエージェントを含む）に影響します。エージェントが無効なコンピューターは影響を受けません。

場合によっては、コンピューターをロックダウンすることで、一部の未承認ファイルがローカルで承認されることがあります。[Edit Policy（ポリシーの編集）] ページの[Advanced Settings（高度な設定）]パネルには、「Locally approve unapproved files on transition from Visibility or Low Enforcement Level to Medium or High（可視性または低適用レベルから中適用レベルまたは高適用レベルへの移行中に未承認ファイルをローカルで承認）」というチェックボックスがあります。この影響を受けるのは、適用レベルが「低」または「なし」から「高」または「中」に変更されるコンピューターです。

- ボックスがオンになっている場合、低（または「なし」）適用レベルだったコンピューターで最初に見つかった既存の未承認ファイルが、ロックダウン時にローカルで承認されます。
- ボックスがオフになっている場合、そのポリシーのコンピューター上の未承認ファイルは、ロックダウン後も未承認のままで、実行が許可されません。

デフォルトの読み取り専用権限が付与されている Bit9 コンソールのユーザーは、緊急ロックダウン中にアクセスできません。ログイン アカウント グループには、そのメンバーが緊急ロックダウンを実行できるように「コンピューター管理」権限を付与する必要があります。

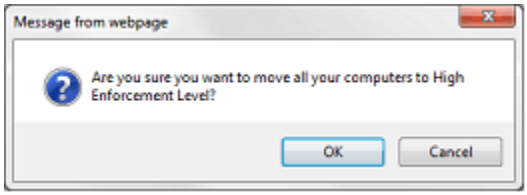
注意

緊急ロックダウンにより変更されるのは、コンピューターの「適用レベル」だけです。高度な設定が「オフ」または「レポートのみ」のポリシーでは、ロックダウンのときでも、一部の脅威がブロックされない可能性があります。

すべてのコンピューターのロックダウン手順：

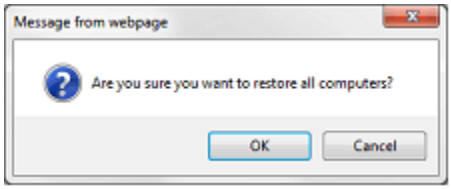
1. コンソール メニューから［**Home**（ホーム）］を選択します。ホーム ページが表示されます。[Emergency Lockdown（緊急ロックダウン）]ポートレットは、デフォルトでページ右下のポートレットに表示されますが、管理者が移動または削除できます。

2. ［Emergency Lockdown（緊急ロックダウン）］ポートレットで、［**Lock Down**（ロックダウン）］ボタンをクリックします。ロックダウンの確認ページが表示されます。



3. 確認ダイアログで、[**OK**] をクリックして、すべてのコンピューターをロックダウンします。無効モードのエージェントを除き、すべてのエージェントがロックダウンされます。ホーム ページが表示され、［**Lock down computers**（コンピューターをロックダウン）］ボタンが［**Restore computer**（コンピューターを復元）］に切り替わります。

4. ロックダウンの原因となった問題を解決したら、［**Restore computers**（コンピューターを復元）］ボタンをクリックして、すべてのコンピューターを前の適用レベルに戻します。復元の確認ページが表示されます。



5. 確認ダイアログで、［**Yes**（はい）］をクリックして、すべてのコンピューターを復元します。

ポリシーの削除

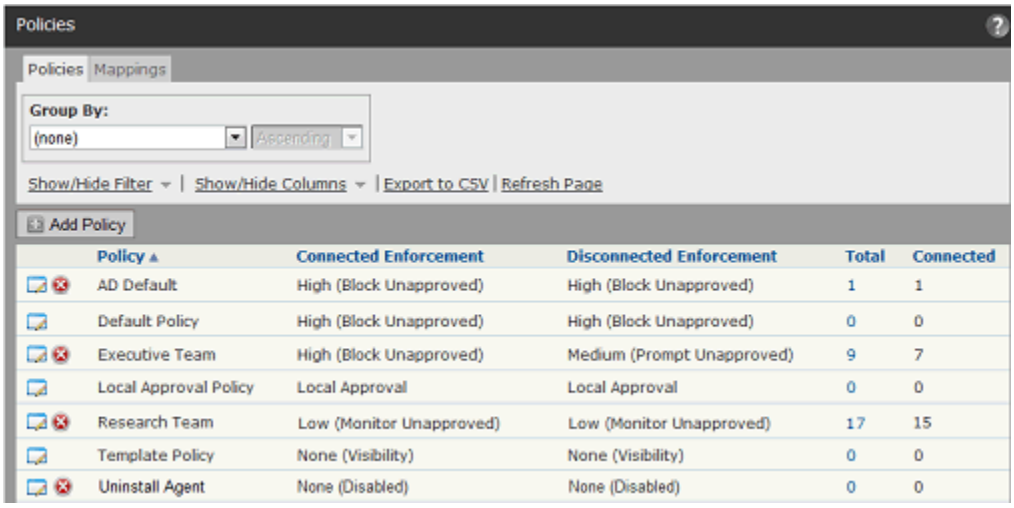
不要になったポリシーは削除できます。ただし、コンピューターが割り当てられているポリシーを削除することはできません。削除するポリシーがコンピューターに関連付けられている場合は、そのコンピューターから Bit9 エージェントをアンインストールするか、コンピューターを他のポリシーに移動します。移動した場合、そのコンピューターは Bit9 によって引き続き保護されます。「Bit9 エージェントのアンインストール」(151 ページ) および「別のポリシーへのコンピューターの移動」（173 ページ）を参照してください。ポリシーを削除すると、関連付けられているエージェント インストーラーも Bit9 Server から削除されます。

次の組み込みポリシーは削除できません。

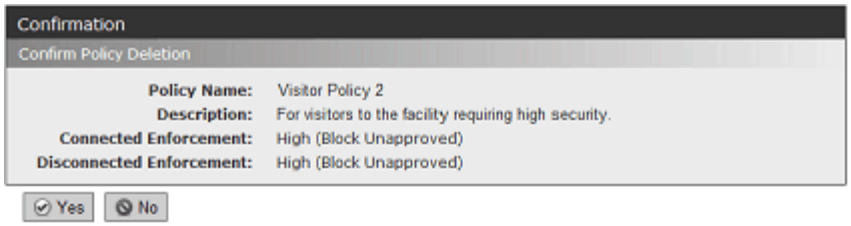
- デフォルト ポリシー
- ローカル承認ポリシー
- テンプレート ポリシー

ポリシーの削除手順：

1. コンソール メニューで、[**Rules**（ルール）] > [**Policies**（ポリシー）] の順に選択します。[Policies（ポリシー）] ページが表示されます。



2. [Policies（ポリシー）] ページで、削除するポリシー名の隣の [Delete（削除）] (x) ボタンをクリックします。確認ダイアログが表示されます。



3. [**Yes**（はい）] をクリックします。[Policies（ポリシー）] ページに戻ります。

注意

ポリシーにコンピューターが含まれる場合、確認ダイアログで [Yes（はい）] をクリックすると、[Policies（ポリシー）] ページに削除失敗メッセージが表示されます。そのコンピューターは、ポリシーを削除する前に、([Computer（コンピューター）] ページで) 他のポリシーに移動するか削除する必要があります。

第 6 章

仮想マシンの管理

この章では、Bit9 コンソールで「クローン」と呼ばれる仮想マシンと、そのクローンのベースとなっている「テンプレート」コンピューターを、Bit9 Security Platform で効率的に管理する方法について説明します。仮想マシンを管理するには、第 4 章「コンピューターの管理」についてよく理解しておく必要があります。

セクション

概要

仮想マシンに Bit9 エージェントがインストールされている場合、Bit9 Security Platform では、物理的に異なるコンピューターを管理するように仮想マシンを管理できます。ただし、この仮想マシンの管理方法は、特別なステップによって「改善」することができます。

Bit9 エージェントが含まれる仮想化ソフトウェア プラットフォームでコンピューターをプロビジョニングし、そのコンピューターを Bit9 コンソールを使用してテンプレートに変換するとき、このテンプレートに基づいたクローンでは、ファイル インベントリ処理のほとんどを最適化できます。Bit9 Server では、クローンのインベントリを、そのテンプレートに基づいて自動的に初期化できます。また、オプションで、クローンの作成後に発生したファイル変更のみを、サーバーが追跡するように選択することもできます。

こうしたオプションによって、クローン コンピューターに関連付けられたネットワーク トラフィックとサーバー負荷が軽減するため、仮想マシンのほとんどを Bit9 Server で管理できるようになる可能性もあります。さらに、テンプレートをベースにしたコンピューターを簡単に検出し、適宜管理できるように、サーバーには、テンプレートとそのクローンの間の関連付けが維持されます。

注意

- この章では、主に、仮想マシンをクローンとして管理する方法について説明しますが、その手順は、物理コンピューターの再イメージ（「非実体化」など）にも使用できます。この場合、クローンは、実際にはテンプレートの共通のディスク イメージを持つ物理マシンです。
- Bit9 テクニカル サポートと協力してカスタム ソリューションを実装し、7.0 Bit9 (Parity) より前のリリースでテンプレートとクローンを管理していた場合、そのソリューションはバージョン 7.2.3 でも引き続き動作しますが、新しい標準テンプレート管理機能には統合されません。

この章と Bit9 コンソールにおける、仮想マシンと非実体化されたマシン管理コンポーネントの説明で使用されている主な用語を次に示します。

- **テンプレート コンピューター** – Bit9 エージェントなど、必要なソフトウェアが事前インストールされたコンピューター。VMware または他のメカニズムによって 1 台以上のコンピューターのクローン（共通イメージからの複数コンピューターのハード ドライブの「非実体化」など）を実行するときに使用されます。Bit9 テンプレート コンピューターとして使用するコンピューターは、オフラインにしておく必要があります。
- **クローン コンピューター**– テンプレート コンピューターのクローンとして作成されたコンピューター。Bit9 Server には新しいコンピューターとして登録されますが、特定の親テンプレートのクローンとして引き続き特定されます。
- **親テンプレート** – 各クローン コンピューターは親テンプレート コンピューターを参照します。このマッピングは、クローンまたはテンプレートのいずれかが削除されるまで保持されます。

Bit9コンソールへのログインに使用されるログイン アカウントでテンプレートおよびクローンを管理できるようにするには、そのアカウントにコンピューターの管理権限が必要です。

テンプレート コンピューターの作成

Bit9 Platform には、仮想マシンを作成したり、物理マシンのクローン ディスク イメージを管理したりするためのソフトウェア（VMware View など）が含まれないため、この章では、こうしたシステムの使用手順については説明しません。ここで説明する機能を使用するには、マスター イメージからクローンを作成する製品があり、その使用方法がわかっている必要があります。Bit9 Server では、こうしたシステムによって生成されたクローンを管理できますが、この Bit9 Server はシステム自体には統合されません。

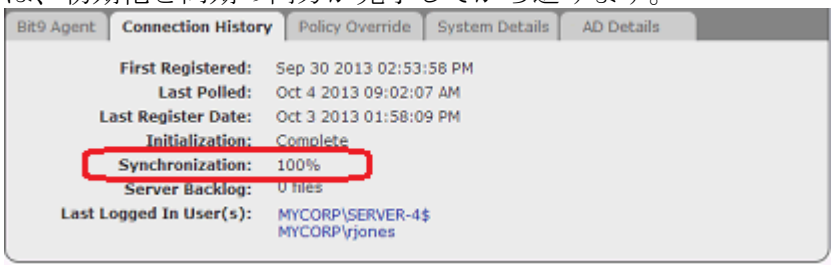
Bit9 がテンプレート コンピューターに求める要件を次に示します。

- Bit9 (Parity) エージェント 7.0.0 以降がインストールされている
- Bit9 Server によって使用されている信頼済みディレクトリのホームではない
- 完全に初期化されている
- 物理コンピューターまたは仮想マシンのいずれかである
- Bit9 テンプレート コンピューターになる前にシャットダウンされ、コンソールで「オフライン」として表示される。また、その後もオフラインとして保持される

テンプレート コンピューターの作成手順：

1. テンプレートとして使用するコンピューターで、プラットフォーム、アプリケーション、およびテンプレート イメージに必要なその他のファイルをインストールします。
2. コンピューターでBit9エージェント7.2.1以降をインストールするか、Bit9エージェント 7.2.1 以降にアップグレードします。
3. エージェントのインストール後、コンピューターが Bit9 Server に接続されていることを確認し、完全に初期化します。初期化の進捗状況を監視するには、Bit9 コンソール メニューで、[**Assets**（アセット）] > [**Computers**（コンピューター）] の順に選択し、コンピューター名の横にある［View Details（詳細の表示）］（鉛筆とファイル）ボタンをクリックします。初期化の進捗状況が［Computer Details（コンピューターの詳細）］ページの［**Connection History**（接続の履歴）］タブに表示されます。

4. 初期化が「完了」と表示されたら、同期が 100% になっていることも確認します。Bit9 エージェントのインストール後にテンプレート コンピューターに追加されたファイルが、初期化ではなく、同期に含まれます。次のステップには、初期化と同期の両方が完了してから進みます。



5. コンピューターをシャットダウンします。

> **注意**
>
> v7.2.3 より前では、sysprep を使ってテンプレートを準備していたときは、シャットダウンの前にコンピューターで改ざんからの保護を無効にする必要がありました。これはもう不要です。

6. コンピューターの［Computer Details（コンピューターの詳細）］ページに移動し、［Advanced（詳細）］メニューで［**Convert to Template**（テンプレートに変換）］をクリックします。［Computer Details（コンピューターの詳細）］ページが［Template Details（テンプレートの詳細）］ページに変わります。
7. デフォルトでは、テンプレート名は、テンプレートの作成元コンピューターの名前になりますが、［Template Settings（テンプレートの設定）］タブで、この名前を変更し、説明を追加して、クリーンアップおよびインベントリ パラメーターを変更できます（詳細については、「クローンの削除」と「クローン インベントリの構成」を参照）。
8. ［Template Details（テンプレートの詳細）］ページの構成に問題がなければ、［**Save**（保存）］をクリックします。［Computers（コンピューター）］テーブルにコンピューターがテンプレートとして表示されます。
   注意：この章で後述する特定のタスクを除き、テンプレートとして変換したコンピューターはオンラインに戻さないでください。テンプレート コンピューターをオンラインにすると、そのコンピューター自体のクローンとして表示されます。
9. 仮想化ソフトウェアを使用して、コンピューターからクローンを作成します。クローンは、Bit9 コンソールでは新しいコンピューターとして表示されます。

［Computers（コンピューター）］テーブルでのテンプレートの表示

［Computers（コンピューター）］ページのテーブルでは、コンピューターと、そのコンピューターのポリシー、適用レベル、サーバーに接続されているかどうかなど、コンピューターに関する情報を確認できます。デフォルトでは、完全な［Computers（コンピューター）］テーブルには［Connected（接続済み）］列があり、

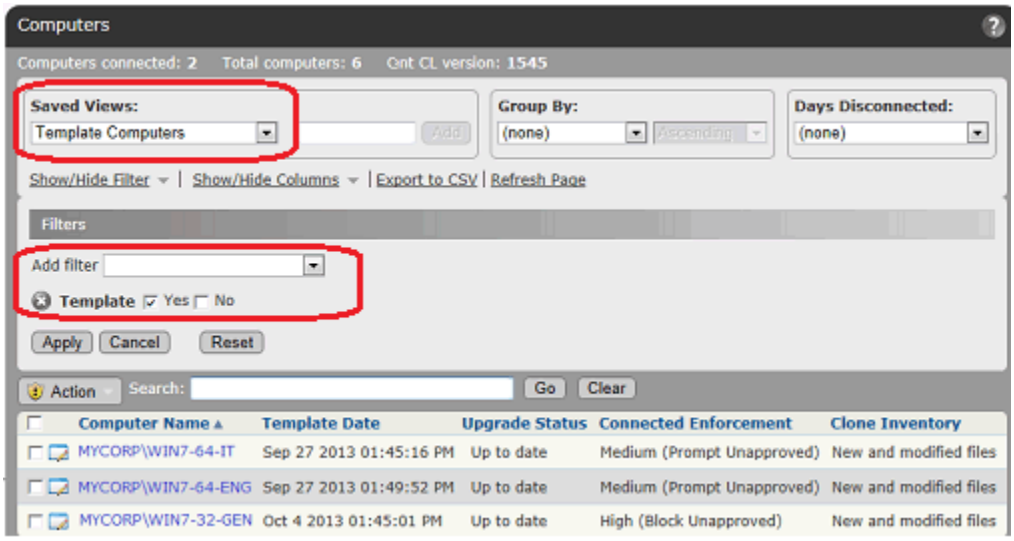
テンプレート　コンピューターは灰色の枠線の白い丸で示されています。

○［Show/Hide Columns（列の表示 / 非表示）］ボタンを使用して、［Template（テンプレート）］列を［Computers（コンピューター）］テーブルに追加することもできます。この列では、テンプレートには［Yes（はい）］が、テンプレートではないコンピューターには［No（いいえ）］が示されます。

表示したいコンピューターがすべてテンプレート コンピューターの場合は、［Saved View（保存済みビュー）］の［Template Computers（テンプレート コンピューター）］を使用します。

コンピューターのテーブルにテンプレート コンピューターを表示する手順：

1. コンソール メニューで、［**Assets**（アセット）］>［**Computers**（コンピューター）］の順に選択します。［Computers（コンピューター）］ページが表示されます。
2. ［Saved Views（保存済みビュー）］メニューで［**Template Computers**（テンプレート コンピューター）］を選択して、クローン コンピューターのテンプレートであるコンピューターを表示します。



3. ［Saved View（保存済みビュー）］では、フィルターの［Template（テンプレート）］の［Yes（はい）］チェックボックスが使用されます。［Saved View（保存済みビュー）］ではなく、または［Saved View（保存済みビュー）］の他に［**Show/Hide Filter**（フィルターの表示 / 非表示）］をクリックすると、［Computers（コンピューター）］テーブルのビューをさらにカスタマイズできます。

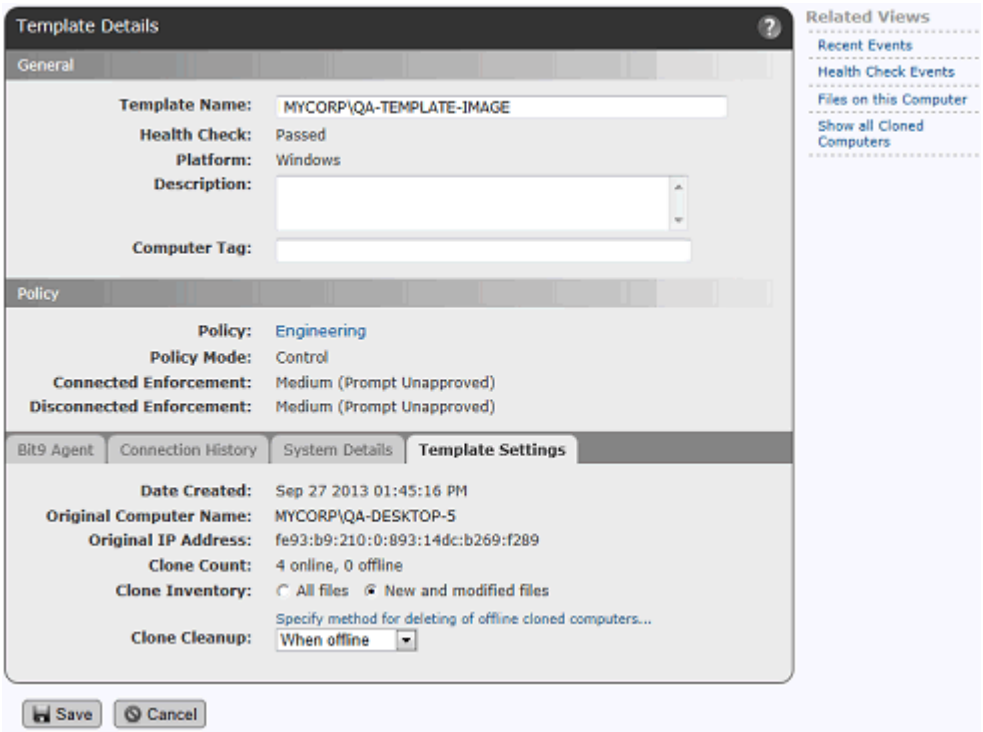
デフォルトの［Template Computers（テンプレート コンピューター）］ビューには、［Clone Inventory（クローン インベントリ）］列があり、このテンプレートのクローンのファイル インベントリに、クローン コンピューターのすべてのファイルが含まれるか、クローン作成後に追加または変更されたファイルのみが含まれるかが示されます。ファイル インベントリは、Microsoft 署名サポート ファイルの追跡除外の影響を受ける可能性があることにも注意してください。詳細については、「Microsoft サポート ファイルの追跡の除外」（239 ページ）を参照してください。

テンプレート詳細の表示と編集

テンプレート以外のコンピューターと同様、テンプレート コンピューターを見つけ、その詳細を表示する方法は複数あります。ホーム ページの［Find Computer（コンピューターの検索）］ポートレットを使用すると、テンプレート コンピューターを見つけ、その詳細を確認することができます。ここでは、［Computer（コンピューター）］ページでテンプレート コンピューターを見つけ、その詳細情報を取得する方法について説明します。

コンピューターの［Template Details（テンプレートの詳細）］ページを表示する手順：

1. コンソール メニュー バーで、［**Assets**（アセット）］>［**Computers**（コンピューター）］の順に選択します。［Computers（コンピューター）］ページが表示されます。
2. ［Computers（コンピューター）］テーブルで、詳細情報が必要なテンプレート コンピューターを見つけます（たとえば、名前で検索したり、［Saved View（保存済みビュー）］の［Template Computers（テンプレート コンピューター）］や［Computer filters（コンピューター フィルター）］パネルを使用したりします）。
3. テーブルで、テンプレート コンピューターの名前またはその名前の横にある［View Details（詳細の表示）］ボタンをクリックします。［Template Details（テンプレートの詳細）］ページが開きます。



情報のほとんどが［Computer Details（コンピューターの詳細）］ページと同じですが（表 15、159 ページ）、表 23 に示すように重要な違いがあります。

表 23：[Template Details（テンプレートの詳細）] と [Computer Details（コンピューターの詳細）] の違い

フィールド / メニュー / タブ	[Template Details（テンプレートの詳細）] ページの説明
Template Name（テンプレート名）	詳細ページのコンピューター名を置き換えます。デフォルトでは、テンプレートの作成元コンピューターの名前です。一意である必要があります。
IP Address（IP アドレス）	[Template Details（テンプレートの詳細）] にはありません（オフラインにする必要があるコンピューターには不要です）。
Connection Status（接続ステータス）	[Template Details（テンプレートの詳細）] にはありません（オフラインにする必要があるコンピューターには不要です）。
Health Check（正常性チェック）	[Template Details（テンプレートの詳細）] ページでは、これが、コンピューターがテンプレートになる前に実行された最後の正常性チェックです。
[Policy Override（ポリシーの無効化）] タブ	[Template Details（テンプレートの詳細）] ページにはありません。
[Template Settings（テンプレートの設定）] タブ	テンプレートの詳細。以下が含まれます。 • [**Date Created**（作成日）] – Bit9 コンソールでテンプレートが作成された日付。 • [**Original Computer Name**（元のコンピューター名）] – コンピューターがテンプレートに変換されたときのコンピューター名。 • [**Original IP Address**（元の IP アドレス）] – コンピューターがテンプレートに変換されたときの、そのコンピューターの IP アドレス。 • [**Clone Count**（クローン数）] – このテンプレートからの現在のクローン数。 • [**Clone Inventory**（クローン インベントリ）] – 各クローンのファイル インベントリに、テンプレート コンピューターからクローンされたファイルを含め、すべてのファイルを保存するか、新しいファイルと変更されたファイルのみを保存するか。「クローン インベントリの構成」（223 ページ）を参照してください。 • [**Clone Cleanup**（クローン クリーンアップ）] – オフラインのとき、このテンプレートのクローンを削除するタイミング。「クローンの削除」（225 ページ）を参照してください。

フィールド / メニュー / タブ	[Template Details（テンプレートの詳細）] ページの説明
[Related Views（関連ビュー）] メニュー	以下が含まれます。 • [**Show All Cloned Computers**（すべてのクローン コンピューターを表示）] – このテンプレートのクローンで、Bit9 Server に接続され、まだ削除されていないものをすべて表示します。 • [**Health Check Events**（正常性チェック イベント）] – このコンピューターがテンプレートになる前の正常性チェック イベントの表を表示します。 • [**Files on this Computer**（このコンピューター上のファイル）] – テンプレート コンピューター上のすべての追跡済みファイル インスタンスの表が含まれる [Find Files（ファイルの検索）] ページが表示されます。
[Actions（アクション）] メニュー	このメニューの項目は状況によって異なります。 [**Delete Offline Clones**（オフライン クローンを削除）] – コンソールに示されているクローンがテンプレートに含まれる場合に表示されます。このテンプレートのクローンで、現在オフラインのものをすべて削除します。 [**Convert to Computer**（コンピューターに変換）] – Bit9 Server によって管理されているクローンがテンプレートにない場合に表示されます。この場合、テンプレート コンピューターを通常のコンピューターに変換し、必要に応じてサーバーに再接続できます。このオプションの主な目的は、意図しないテンプレート変換を元に戻せるようにすることです。 どちらの状況も当てはまらない場合、メニューは表示されません。
[Advanced（詳細）] メニュー	[Template Details（テンプレートの詳細）] ページにはありません。

クローンの展開

コンピューターをテンプレートとして登録すると、そのテンプレートのすべてのクローンが Bit9 Server によって自動的に認識されます。クローンの初期化は、クローン以外のコンピューターよりもはるかに高速に行われます。

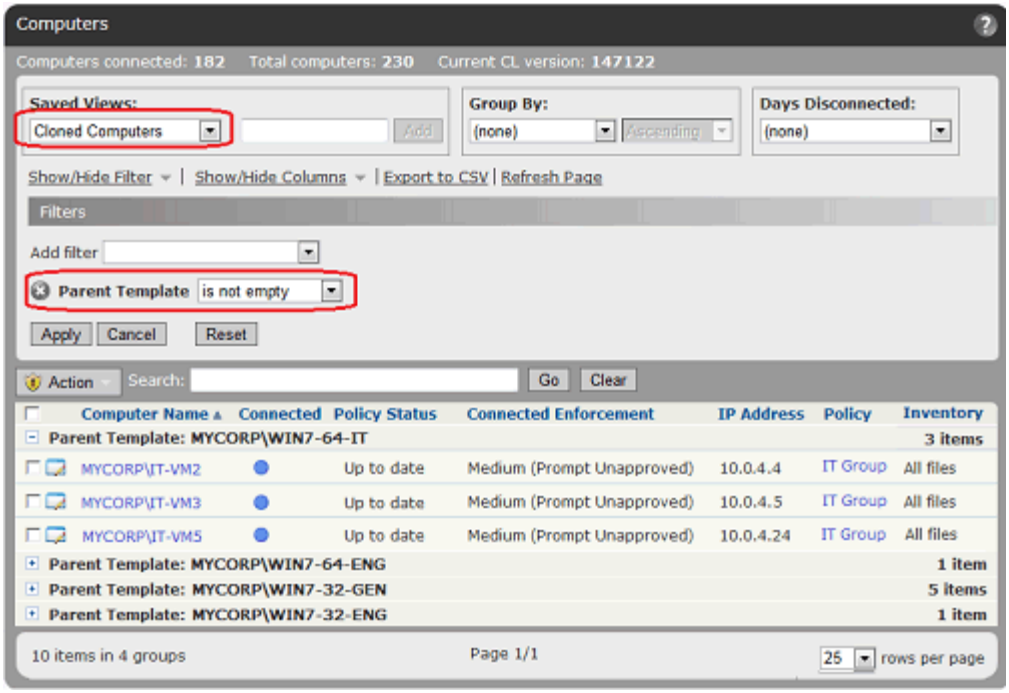
クローンが手動または自動でスナップショット イメージに戻ると、新しいクローンが作成され、コンソールのコンピューター リストに追加されます。これはまだ同じテンプレートに関連付けられています。Bit9 Server に関しては、「古い」クローンはオフラインになり、どの方法を選択してもクリーンアップできます（「クローンの削除」（225 ページ）を参照）。

[Computers（コンピューター）] テーブルでのクローンの表示

[Computers（コンピューター）] ページのテーブルでは、コンピューターと、そのコンピューターのポリシー、適用レベル、サーバーに接続されているかどうかな

ど、コンピューターに関する情報を確認できます。[Show/Hide Columns（列の表示 / 非表示）] ボタンを使用して、[Parent Template（親テンプレート）] 列を [Computers（コンピューター）] テーブルに追加することもできます。この列に値が含まれているコンピューターはすべてクローンです。クローンでないコンピューターの場合、この列には何も表示されません。

クローンのみを確認するには、[Computers（コンピューター）] ページの [Saved View（保存済みビュー）] で [Cloned Computers（クローン コンピューター）] を選択して、Bit9 Server で認識されているすべてのクローン コンピューターを表示します。デフォルトでは、このビューは親テンプレートごとにグループ化されているため、クローンの基になっているテンプレートがわかります。



[Cloned Computers（クローン コンピューター）] の [Saved View（保存済みビュー）] では、「親テンプレートが空ではない」フィルターが適用されています。[Saved View（保存済みビュー）] ではなく、または [Saved View（保存済みビュー）] の他に [Show/Hide Filter（フィルターの表示 / 非表示）] をクリックすると、クローン コンピューターのビューをさらにカスタマイズできます。

デフォルトの [Cloned Computers（クローン コンピューター）] ビューには、[Inventory（インベントリ）] 列があり、このクローンのファイル インベントリに、すべてのファイル（テンプレート イメージのファイルなど）が含まれるか、クローン作成後に追加または変更されたファイルのみが含まれるかが示されます。

テンプレートのクローンを検索

テンプレートから作成されたクローンを特定する方法はいくつかあります。

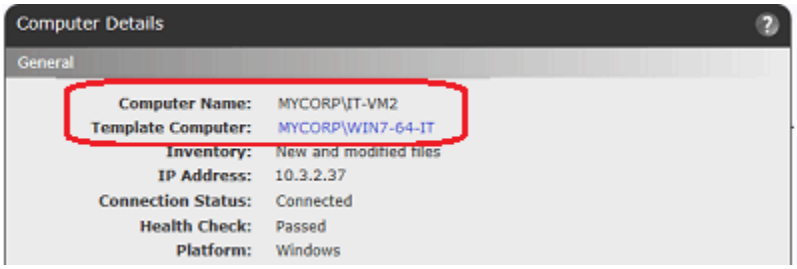
- [Computers（コンピューター）] ページの [Saved View（保存済みビュー）] で [Cloned Computers（クローン コンピューター）] を選択します。これにより、親テンプレートごとにグループ化されたクローンが表示されます。

- ［Template Details（テンプレートの詳細）］ページで、［Related Views（関連ビュー）］メニューの［Show All Cloned Computers（すべてのクローン コンピューターを表示)］を選択します。
- ［Computers（コンピューター）］ページで、［Parent Template（親テンプレート）］フィルターを使用すると、特定のテンプレートに基づいたすべてのクローンを特定できます。名前の一部を入力すると、入力した文字列を含む名前が表示されるため、正確なテンプレート名がわからない場合にも役に立ちます。

クローンのテンプレートを検索

クローン コンピューターのテンプレートは、次の方法で見つけることができます。

- ［Computers（コンピューター)］ページの［Saved View（保存済みビュー)］で［Cloned Computers（クローン コンピューター)］を選択します。これにより、親テンプレートごとにグループ化されたクローンが表示されます。
- ［Computer Details（コンピューターの詳細）］ページに表示されているクローンの情報は、他のコンピューターの情報とほぼ同じですが、コンピューターがクローンの場合は、標準的な情報のほかに［Template Computer（テンプレート コンピューター)］フィールドが表示されます。



クローンのサーバー バックログ

［Computer Details（コンピューターの詳細)］ページの［Connection History（接続の履歴)］タブには、［Server Backlog（サーバー バックログ)］フィールドがあります。これは、コンピューターから受信したが、サーバー上での処理がまだ完全には完了していないファイルの数を示します。バックログのファイルは、［File Catalog（ファイル カタログ)］に表示されますが、［Files on Computers（コンピューター上のファイル)］タブおよび［Find Files（ファイルの検索)］ページには表示されません。

これは、テンプレート イメージのファイルを含め、すべてのファイルをインベントリに保存するように構成されているクローンで特に役立ちます。Bit9 Server によって検出されたクローンが、すべてのファイルをインベントリに保存するように構成されている場合、親テンプレートからのファイル インベントリは、そのコンピューターのバックログにコピーされます。この場合、［Server Backlog（サーバー バックログ）］フィールドに示されるファイル数はかなり多くなります。クローン マシンのファイル インベントリは、このバックログが消去されるまで使用できません。

テンプレートの変更

オペレーティング システムの新しい更新プログラムをインストールする場合などに、すべてのユーザーを対象とした既存のテンプレートの変更が必要になることがあります。また、元のテンプレート イメージを維持しながら、別の目的や別のユーザー グループに合わせて若干の変更を加えて新しいテンプレートを作成する場合も、既存のテンプレートを変更する必要があります。

既存のテンプレートを変更するには、テンプレート コンピューターをオンラインに戻す必要があります。オンラインのコンピューターは、元のテンプレートの新しいクローン コンピューターとして扱われます。コンピューターがクローンとして認識されている間は、更新をインストールして、他の必要な変更を加えることができます。変更が完了したら、その「クローン」をテンプレートに変換します。既存のテンプレート コンピューターから作成された新しいテンプレートは、クローン クリーンアップ パラメーターを元のテンプレートから自動的に継承します。

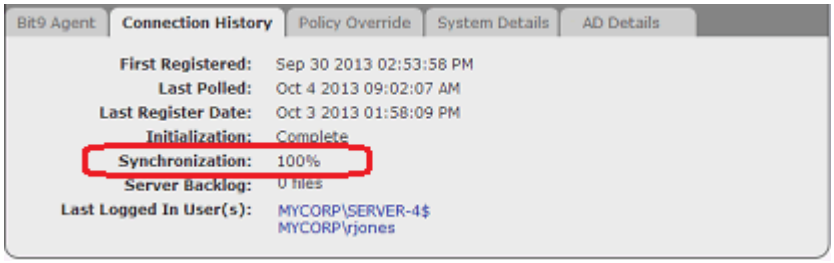
元のテンプレートのクローンは自動削除されず、オンラインである限り有効です。こうしたクローンは、初期化またはイメージ インフラストラクチャを使用して適宜管理できます。

古いテンプレートで実行できることは、そのテンプレートを更新した理由と、テンプレートに関連付けられているオンライン クローンがまだ存在するかどうかによって異なります。新しいテンプレートが本当の意味での更新版で、今後古いバージョンを使用することがない場合、古いテンプレートは削除します。その際、そのテンプレートのクローンはオフラインにすることをお勧めします。詳細については、「テンプレートの削除」を参照してください。

新しいテンプレートがバリエーションの 1 つで、必ずしも古いテンプレートを置き換える必要がない場合は、両方のテンプレートを使用可能な状態のまま維持できます。

テンプレート コンピューターの更新手順：

1. テンプレート コンピューターをオンラインに戻します。そのコンピューターは、元のテンプレートのクローンとしてコンソールに表示されます。
2. この「クローン」コンピューターでは、更新テンプレートに必要なファイルの追加、削除、および変更を行うことができます。
3. 初期化またはイメージ　ソフトウェアを使用して、このコンピューターのイメージを更新するか、新しいイメージを作成します。
4. クローンのファイル インベントリが完全に同期されるまで待ちます。同期の進捗状況を監視するには、Bit9 コンソール メニューで、[**Assets**（アセット）] > [**Computers**（コンピューター）] の順に選択し、コンピューター名の横にある［View Details（詳細の表示）］（鉛筆とファイル）ボタンをクリックします。同期の進捗状況が［Computer Details（コンピューターの詳細）］ページの［**Connection History**（接続の履歴）］タブに表示されます。



5. 同期が100%になったら、コンピューターをシャットダウンするか、ネットワークから削除します。
6. 「更新したクローン コンピューター」（元のテンプレートではありません）の［Computer Details（コンピューターの詳細）］ページに移動し、［Advanced（詳細）］メニューで［**Convert to Template**（テンプレートに変換）］をクリックします。［Computer Details（コンピューターの詳細）］ページが［Template Details（テンプレートの詳細）］ページに変わります。
7. 更新されたテンプレートには、デフォルトで、古いテンプレート名と数値が組み合わされた名前が付けられます。この数値は、テンプレートが更新された回数を表します。たとえば、元のテンプレートが MYCORP\WIN7-64-IT の場合、編集されたテンプレートの名前は MYCORP\WIN7-64-IT (1) になります。また、次の編集バージョンの名前は MYCORP\WIN7-64-IT (2) になり、以降同じように名前が付けられます。この名前は、必要に応じて変更できます。
8. 仮想化ソフトウェアを使用して、新しいテンプレート コンピューターからクローンを作成します。

テンプレートの削除

テンプレートはいつでも削除できます。クローンを持つテンプレートを削除すると、そのクローンは独立したコンピューターになります。つまり、テンプレートとの関連付けが解除されます。テンプレート コンピューターを同じ名前で後から復元しても、テンプレートとクローンは再接続されません。

Bit9 コンソールからテンプレート コンピューターを削除する手順：

1. コンソール　メニューで、［**Assets**（アセット）］>［**Computers**（コンピューター）］の順に選択します。
2. ［Template Computers（テンプレート コンピューター）］ビューまたはその他の方法を使用して、テンプレート コンピューターを見つけます。
3. ［Computers（コンピューター）］テーブルで、テンプレート コンピューターの横にあるボックスをオンにし、［Action（アクション）］メニューから［**Delete Computers**（コンピューターの削除）］を選択して、削除を確認します。

注意

テンプレートにクローンがない場合は、そのテンプレートを通常（テンプレートなし）のコンピューターに変換し、Bit9 Server で管理することもできます。「通常のコンピューターへのテンプレートの変換」（228 ページ）を参照してください。

クローン インベントリの構成

Bit9 の仮想マシン管理機能を使用する主な理由として、テンプレート コンピューターから今後作成されるクローンでの、ファイル インベントリ処理の最適化が挙げられます。クローン ファイル インベントリ管理には 2 つのオプションがあります。

- ［**All files**（すべてのファイル）］– テンプレートに存在するファイルに基づいてクローンのファイル インベントリが自動的に初期化されます。クローンが検出されると、そのテンプレートのインベントリはクローンのインベントリにコピーされます。その後のファイルの追加や変更もクローン インベントリに反映されます。これはデフォルトの設定です。
- ［**New and modified files**（新しいファイルと変更されたファイル）］– 空のファイル インベントリでクローンを開始し、クローンの作成後に発生した各クローンに対するファイルの追加と変更のみをサーバーが追跡するように選択できます。

このオプションはテンプレートごとに設定されます。「クローン」に対するコンピューター インベントリ上のファイルがどのように管理されるかは、このオプションの影響を受けます。ここで選択した内容に関係なく、テンプレート イメージからのファイルはすべて、サーバー上のBit9ファイル カタログに保存されます。

［New and modified files（新しいファイルと変更されたファイル）］を選択すると、クローン インベントリにより、次の変更がベースライン テンプレート インベントリから追跡されます。

- ファイルの作成
- ファイルの変更
- ファイルの削除
- ファイル名の変更
- ファイルの Bit9 状態（承認と禁止）の変更

ファイルの「パス」の変更（ファイル名自体の変更以外）によって、テンプレート インベントリにあったファイルがクローン インベントリの一部として追跡されることはありません。

インベントリ オプションの選択

クローン インベントリの最適な設定は、それぞれの環境と優先事項によって異なります。新しいファイルと変更されたファイルのみがインベントリを保存するように選択した場合の利点として最も明らかなのは、ネットワークおよびサーバー トラフィックが軽減され、関係ないと思われるデータ量を最小限に抑えられる点です。これは、ご利用の環境で数千台のクローン コンピューターと大きなベース ファイル イメージを使用している場合に特に重要です。

このインベントリ オプションと、クローン インベントリの制限による影響とのバランスをうまく保つ必要があります。［New and modified files（新しいファイルと変更されたファイル）］を選択すると、次のようになります。

- ［Find Files（ファイルの検索）］ページにも［Files on Computers（コンピューター上のファイル）］ページにも、クローン コンピューターのすべてのファイルを表示しきれなくなります。

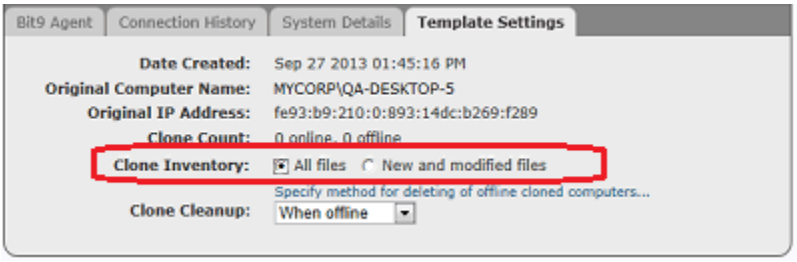
- クローン マシンが含まれるドリフト レポートが不完全になります。適切に動作する唯一のドリフト レポート タイプはセルフ ドリフトです（クローン コンピューター上の現在のファイルと、そのファイルの以前のインベントリとの比較）。初期テンプレート イメージからの変更されていないファイルは、このレポートに含まれません。
- クローン コンピューターから作成されたスナップショットには、新しいファイルと変更されたファイルのみが追加されます。
- テンプレート イメージからの変更されていないファイルについては、クローンのインスタンスがカウントされないため、ファイルの普及度が正確ではありません（元のイメージからのファイルの削除も考慮されません）。
- クローン コンピューターのインベントリには、テンプレート イメージの変更されていないファイルが表示されないため、こうしたファイルを直接ローカルで承認するには、（特定のクローン コンピューターの）特定のファイル インスタンスがイベントに表示されている必要があります。それ以外の場合、グローバル承認が必要になる場合があります。

注意

Bit9 には、特定の Microsoft 署名オペレーティング システムとアプリケーション ファイルの追跡を除外するオプションも用意されており、これにより、トラフィックとデータベースの要求を大幅に軽減することができます。これは、クローンだけではなく、すべてのコンピューターに影響します。詳細については、「Microsoft サポート ファイルの追跡の除外」（239 ページ）を参照してください。

テンプレートのクローン インベントリ設定を構成する手順：

1. コンソール メニューで、[**Assets**（アセット）] > [**Computers**（コンピューター）] の順に選択します。
2. [Template Computers（テンプレート コンピューター）] ビューまたはその他の方法を使用して、テンプレート コンピューターを見つけ、[View Details（詳細の表示）] ボタンまたはコンピューター名をクリックします。
3. [**Template Settings**（テンプレートの設定）] タブをクリックします。



4. [Clone Inventory（クローン インベントリ）] フィールドで、[**All files**（すべてのファイル）] と [**New and modified files**（新しいファイルと変更されたファイル）] のどちらかのボタンを選択します。

5. 他に構成の変更がない場合は［**Save**（保存）］をクリックします。

注意

インベントリ オプションとして［New and modified files（新しいファイルと変更されたファイル）］を選択しても、クローンがオフラインになった後に、同じ名前のクローンが接続された場合、そのファイルが既に削除済みとしてマークされていると、テンプレート イメージの一部として提供されたファイルを含め、すべてのファイルがインベントリに保存されます。

クローンの削除

Bit9 Security Platformの管理環境で仮想マシンを必要に応じて作成したり削除したりする場合は、使用しない古いクローンが［Computers（コンピューター）］ページに残らないようにします。たとえば、仮想マシンが時間ベースまたはログインのたびにスナップショットに自動的に戻るように設定したり、クローンのテンプレート イメージを頻繁に更新したりします。Bit9 Security Platform には、古いクローンをクリーンアップする方法が複数用意されています。

- **手動クリーンアップ** – この方法では、すべてのクリーンアップ方法を手動のままにして、［Template Details（テンプレートの詳細）］ページで、オフライン クローンを定期的に削除できます。
- **すべてのクローンを自動クリーンアップ** – オフラインのクローン コンピューターを、スケジュールに従って削除するクリーンアップ ルールを構成できます。「すべて」のオフライン クローン コンピューターを削除するか、特定のフィルターに一致するものだけを削除できます。たとえば、仮想化環境で実行されているコンピューターで、オフラインになってから 5 日を超えるものをすべて削除することができます。
- **テンプレートごとに自動クリーンアップ** – さまざまなテンプレートに対してさまざまなクリーンアップ ルールを構成できます。

通常のクローン以外のコンピューターと同様、削除されたクローンのファイル インベントリは、クローンが削除されてから 24 時間後に削除されます。

クローンの手動クリーンアップ

手動クリーンアップには 2 つの方法があります。

- ［Saved View（保存済みビュー）］の［Cloned Computers（クローン コンピューター）］を使用して目的のクローンを見つけ、他のコンピューターのように削除できます。
- テンプレートの［Template Details（テンプレートの詳細）］ページに移動し、［Action（アクション）］メニューの［Delete Offline Clones（オフライン クローンを削除）］コマンドを使用します。

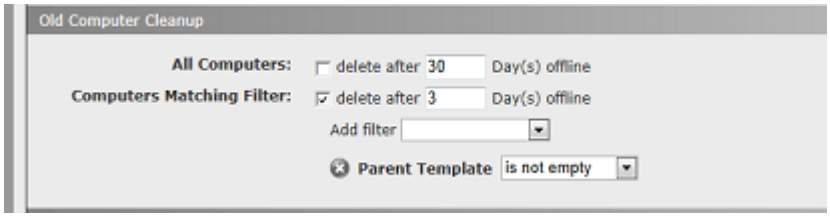
すべてのクローンを自動クリーンアップ

［System Configuration（システム構成）］ページの［Advanced（詳細）］タブには、管理されているコンピューターのリストからオフライン コンピューターを削除する設定があります。オフライン状態が一定期間続いた「すべて」のコンピューターをコンソールから削除することや、選択したコンピューターを削除するフィルターを設定することができます。

各テンプレートのクローン クリーンアップ構成を手動のままにしておく場合は、フィルターされたグローバル クリーンアップ方法を使って、オフライン クローンを削除できます。1 つ以上のテンプレートに対して自動クリーンアップ方法を設定し、グローバル削除方法を設定すると、「どちらか」のルールを満たした場合に必ずオフライン クローンが削除されます。

オフライン クローンのグローバル クリーンアップ ルールを作成する手順：

1. コンソール メニューで、［**Administration**（管理）］>［**System Configuration**（システム構成）］の順に選択します。［System Configuration（システム構成）］ページが表示されます。
2. ［**Advanced Options**（高度なオプション）］タブをクリックします。［Advanced Options（高度なオプション）］構成ページが表示されます。
3. ［**Edit**（編集）］ボタンをクリックします。
4. ［Old Computer Cleanup（古いコンピューターのクリーンアップ）］パネルで、指定した期間が経過した後にクローン コンピューターが削除されるように［Computers Matching Filter（フィルターに一致したコンピューター）］を構成します。
   a. ［Computers Matching Filter（フィルターに一致したコンピューター）］の右側にあるボックスをオンにします。
   b. コンソールの［Computers（コンピューター）］ページからコンピューターが削除されるまでの、コンピューターのオフライン日数を入力します。
   c. ［Add Filter（フィルターを追加）］メニューで、適切なフィルターを選択します。たとえば、［**Parent Template**（親テンプレート）］を選択し、その［Parent Template（親テンプレート）］の横に表示されたメニューで［**is not empty**（空でない）］を選択します。これにより、テンプレートがあるコンピューターすべてが確実に削除されます。［**Virtualized**（仮想化）］を選択し、［Yes（はい）］ボックスをオンにして、すべての仮想マシンを（クローンかどうかに関係なく）クリーンアップすることもできますが、この場合、他の手段で作成されたクローンはクリーンアップされません。また、［**Virtual Platform**（仮想プラットフォーム）］を選択し、フィールドに「VMware」と入力すると、**VMware** コンピューターをクリーンアップできます。



5. 変更を保存するには、［**Update**（更新）］ボタンをクリックし、確認ダイアログで［**Yes**（はい）］をクリックします。

1 つのテンプレートの自動クローン クリーンアップ

クローンのクリーンアップはテンプレートごとに設定されます。手動クリーンアップを選択することも、2 つの自動設定のいずれかを選択することもできます。システム構成ページでグローバル クローン クリーンアップ ルールを設定すると、そのルールもテンプレートに適用されます。

特定のテンプレートの自動クローン クリーンアップを構成する手順：

1. コンソール メニューで、[**Assets**（アセット）] > [**Computers**（コンピューター）] の順に選択します。
2. クローン削除を構成するテンプレート　　コンピューターを見つけ、[View Details（詳細の表示）] ボタンをクリックして、[Template Details（テンプレートの詳細）] ページを開きます。
3. [**Template Settings**（テンプレートの設定）] タブをクリックします。テンプレートがいつ作成されたか、コンピューターの元の名前と IP アドレス、および Bit9 Server で確認されたテンプレートのクローン数が表示されます。また、このテンプレートのクローン コンピューターをクリーンアップする方法を選択するためのメニューもあります。
4. [Clone Cleanup（クローン クリーンアップ）] メニューで、次のいずれかを選択できます。
   - [**Manual**（手動）] – 自動クリーンアップは行われません。このテンプレートに基づくクローンは、手動で削除するか、[System Configuration（システム構成）] の [Advanced（詳細）] タブで定義したグローバル クリーンアップ ルールで削除する必要があります。
   - [**When offline**（オフライン時）] – このテンプレートに基づくクローンは、オフラインになった時点で削除されるようにスケジュールされます。実際には、他のサーバー アクティビティに基づいて 10 ～ 15 分以内に削除されます。
   - [**Based on time**（時間基準）] – このテンプレートに基づくクローンは、このオプションを選択した場合に表示されるフィールドに設定したオフライン時間が経過した時点で削除されます。テンプレートとグローバル クリーンアップで異なる時間が定義されている場合は、早い方の期限に達した時点でクリーンアップがトリガーされます。
   - [**Based on name**（名前基準）] – このテンプレートに基づくクローンが Bit9 Server に新しく登録されると、同じ名前の「オフライン」クローンすべてが自動的に削除されます。オンライン クローンには影響がありません。この方法は、元に戻された古いコンピューター データを分析する必要がない限り、安全に使用できます。新しいクローンに常に新しい名前が付けられる場合、オフライン クローンはクリーンアップされません。

   注意：使用中のクローンが誤って削除されないように、クローンがオフラインとして検出されても、サーバーと通信していない状態が 10 分以上続かない限り、そのクローンが削除されることはありません。これは、ネットワーク中断によってクローンが誤って未使用のように見える状況を緩和するうえで役に立ちます。
5. [Template Details（テンプレートの詳細）] ページで必要な変更すべてを行ったら、[**Save**（保存）] をクリックします。

通常のコンピューターへのテンプレートの変換

テンプレートを通常のコンピューターに戻すことができます。この機能の主な目的は、コンピューターを誤ってテンプレートに変換したときに修復することですが、どのような状況でも使用できます。テンプレートとして実際に使用されているコンピューターを変換する必要がある場合は、変換前に、Bit9 コンソールの［Computers（コンピューター)］ページで、そのテンプレートにクローンがないことを確認する必要があります。

テンプレート コンピューターを通常のエージェント管理コンピューターに戻す手順：

1. このテンプレートの［Template Details（テンプレートの詳細)］ページで、［Related Views（関連ビュー）］メニューの［**Show All Cloned Computers**（すべてのクローン コンピューターを表示)］をクリックします。
2. このコンピューターにクローンがある場合は、クローンを Bit9 Server から削除するか、そのテンプレートをテンプレートとして残します（「コンピューターの削除」（177 ページ）を参照）。それ以外の場合、クローンは独立したコンピューターになります（テンプレートには接続されません)。
3. テンプレートに確実にクローンがない場合は、［Template Details（テンプレートの詳細）］ページに戻り、［Action（アクション）］メニューで［**Convert to Template**（テンプレートに変換)］をクリックします。コンピューターが Bit9 Server管理に戻り、［Template Details（テンプレートの詳細)］ページが［Computer Details（コンピューターの詳細)］ページに変換されます。
4. 変換の完了後、サーバーで管理できるようにコンピューターを再接続します。

第 7 章

ファイル情報と公開者情報

この章では、Bit9 Security Platform で検出および管理されるファイルで使用できる情報の場所と内容、およびこうしたファイルに関連付けられている公開者に関する情報について説明します。また、特定のファイルの追跡を除外するオプションや、特定のファイルが存在する、または存在しないコンピューターをすべて表示するオプションについても説明します。

セクション

概要

Bit9 Security Platform は、コンピューターで追跡の対象となるファイルに関するさまざまな情報を収集します。追跡対象となるファイルは、Bit9 Platform によって実行可能ファイルと見なされたファイル（.EXE ファイル、.DLL ファイルなど）、またはスクリプトとして定義されたファイル拡張子と一致するファイルです。こうした情報は、単にファイル アクティビティを認識したり、特定のファイルまたはファイル クラスの実行や書き込みの制御方法を決めたりするときに使用できます。

Bit9 エージェントで認識されるファイルの多くに、確認済み「公開者」が指定されています。他のファイル情報と同様、公開者は、ファイルのソースを認識するうえで役に立ちます。また、この公開者を使って、ファイルを自動的に承認または禁止することもできます。

注意

ファイルおよび公開者情報の中には、Bit9 Software Reputation Service (SRS) によって提供されるものがあります。こうした情報を取得するには、Bit9 SRS を有効にしておく必要があります。詳細については、「Bit9 SRS の有効化」（787 ページ）を参照してください。

ファイルおよび公開者情報を使用したファイルの承認または禁止については、第 8 章「ソフトウェアの承認と禁止」を参照してください。

ファイル情報は、Bit9 コンソールの複数の場所にテーブル形式で表示されますが、情報を確認する際の主な開始点となるのが［Files（ファイル）］ページです。このページにアクセスするには、コンソール メニューの［Assets（アセット）］>［Files（ファイル）］の順に選択します。［Files（ファイル）］ページには次の 2 つのタブがあります。

- ［**File Catalog**（ファイル カタログ）］タブには、コンピューターで検出された一意の追跡対象ファイルが表示されます。カタログ登録されたファイルには、エージェント コンピューターに現在存在している追跡済みファイル、追跡対象ファイルとして見なされたがインベントリで追跡されていないファイル、および以前エージェント システムに存在していたが削除されたファイルが含まれます。
- ［**Files on Computers**（コンピューター上のファイル）］タブには追跡済みファイル インスタンスが表示されます。これには、（すべてのファイル処理の完了後）Bit9 Server にレポートする、すべてのエージェント管理コンピューター上にあるすべての追跡対象ファイルの全インスタンスが含まれます。ただし、次の例外があります。
  - Microsoft オペレーティング　システムおよびアプリケーションの共通サポート ファイルをファイル インベントリから除外して、追跡のオーバーヘッドとデータベース サイズを減らすことができます。詳細については、「Microsoft サポート ファイルの追跡の除外」（239 ページ）を参照してください。
  - VDI 製品で使用されるテンプレートのファイル インスタンスを除外して、クローンを作成できます。詳細については、「クローン インベントリの構成」（223 ページ）を参照してください。

- ポリシー単位でファイル追跡を無効にできます。

いずれかの状況がコンピューターのファイルに影響する場合、そのファイルの普及度の値は不正確になります。普及度に反映されるのは、追跡済みファイルだけだからです。

テーブル内のファイルの完全な情報は、そのファイルの詳細ページで確認できます。

- ［**File Details**（ファイルの詳細）］ページには、固有のファイルに関するグローバル情報と、そのファイルのインスタンス一覧へのリンクが表示されます。
- ［**File Instance Details**（ファイル インスタンスの詳細）］ページには、特定のコンピューターの特定のファイル インスタンスに関する情報が表示されます。

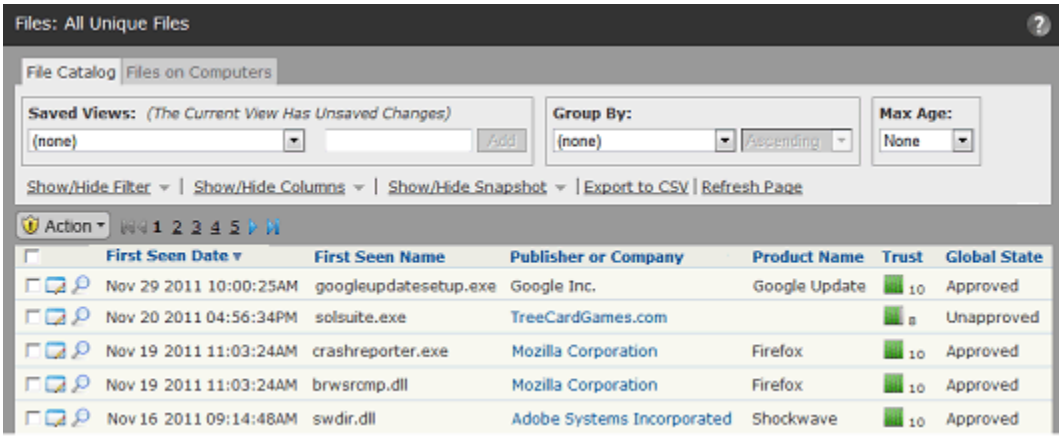
［Publisher rules（公開者ルール）］ページのテーブルには、Bit9 Server によって管理されているエージェントで検出されたファイルの公開者が表示されます。このページにアクセスするには、［**Rules**（ルール）］>［**Software Rules**（ソフトウェア ルール）］の順に選択し、コンソール メニューで［**Publishers**（公開者）］タブをクリックします。テーブル内の公開者の完全な情報は、その公開者の詳細ページで確認できます。

ファイル テーブルの表示

ファイル カタログ

［Files（ファイル）］ページの［File Catalog（ファイル カタログ）］タブには、組織の Bit9 エージェントが実行されているコンピューターで検出された一意のファイルが表示されます。［File Catalog（ファイル カタログ）］ページには、ファイルとその詳細のテーブルのほか、［Action（アクション）］メニューが表示されます。このメニューを使用すると、Bit9 Software Reputation Service でのファイルに関する情報の承認、禁止、検索など、ファイルに関連するさまざまなアクションを実行できます。こうしたアクションについては、他の章で説明します。

［File Catalog（ファイル カタログ）］で、ファイル名の横にある［View Details（詳細の表示）］（ファイルと鉛筆）ボタンをクリックすると、［File Details（ファイルの詳細）］ページが開きます。［File Catalog（ファイル カタログ）］の列見出しのほとんどが、1 つのファイルの［File Details（ファイルの詳細）］ページのフィールドと対応しています。この情報の説明については、表 25、「［File Details（ファイルの詳細）］および［File Catalog（ファイル カタログ）］ページのフィールド」（246 ページ）を参照してください。



デフォルトでは、[File Catalog（ファイル カタログ）] には一意の「最上位レベル」ファイル（他のファイルによってインストールされたり、他のファイルからコピーされたりしたものではないファイル）すべてが表示されます。カタログの別の保存済みビューを選択することや、独自のビューを作成して、特定のファイルの種類に焦点を当てたり、1 つのファイルを検索したりすることもできます。コンソール テーブルでのビューの変更にまだ慣れていない場合は、「Bit9 コンソールのテーブル」（68 ページ）を参照してください。最上位レベルのファイルだけでなく、一意の個々のファイルすべてを表示することもできます。このオプションを選択する前に、「個別のファイルの表示」（235 ページ）を参照してください。

注意

[File Catalog（ファイル カタログ）] では、一意のファイルに対して [First Seen Name（最初に確認された名前）] が表示され、一意のファイルはハッシュによって特定されます。「特定のコンピューター」のファイル インスタンスに使用されている名前は、[Files on Computers（コンピューター上のファイル）] タブに表示されていても、[File Catalog（ファイル カタログ）] には表示されない場合があります。特定のインスタンスを名前で見つけるには、[Find Files（ファイルの検索）] または [Files on Computers（コンピューター上のファイル）] タブを使用してください。

表 24 は、[File Catalog（ファイル カタログ）] タブの [Saved Views（保存済みビュー）] を示しています。

表 24：[File Catalog（ファイル カタログ）] タブの [Saved Views（保存済みビュー）]

保存済みビュー	説明
Applications by Publisher/Company（アプリケーション（公開者 / 会社別））	アプリケーションまたはパッケージとして特定されたファイル。このビューでは、公開者（可能な場合）または会社別にグループ化されます。
Approved Files（承認済みファイル）	Bit9 のグローバル承認方法で承認されたすべての実行可能ファイル。
Banned Files（禁止ファイル）	ハッシュによって明示的に禁止されたすべてのファイル。名前によって禁止されたファイルは、[File Catalog（ファイル カタログ）] タブのテーブルに表示されません。あるポリシーでは禁止され、あるポリシーでは禁止されていないファイルについては、[Banned Files（禁止ファイル）] テーブルには表示されません。こうしたファイルを見つけるには、[File Catalog（ファイル カタログ）] タブで [File State（ファイルの状態）] フィルターを使用します。
Categorized Files（分類済みファイル）	少なくとも 1 台のコンピューターに存在し、Bit9 SRS で特定できるアプリケーション カテゴリのいずれかに分類されるファイル（ハッキング ツール、インスタント メッセージなど）。このビューでは、ファイルはカテゴリごとにグループ化されます。
Existing Files（既存のファイル）	ネットワーク上にある 1 台以上のエージェント管理コンピューターに存在するファイル。
Installed Programs（インストール済みプログラム）	関連付けられたインストール済みプログラム別にグループ化されたファイル。このビューには、インストール済みプログラムの完全なパッケージまたはアプリケーション名が表示されます。 **プラットフォームに関する注意**：インストール済みプログラムとして特定されるのは Windows ファイルだけです
Malicious Files（悪意のあるファイル）	少なくとも 1 台のコンピューターに存在し、Bit9 SRS により脅威レベル「1- 危険な可能性あり」または「2- 悪質」として特定されたファイル。
New Unapproved Files（新しい未承認ファイル）	ファイルの初期化「後」にコンピューター上で見つかったファイル。確認されておらず、少なくとも 1 台のコンピューター上にまだ存在します。
Removed Files（削除済みファイル）	Bit9 Server にレポートするエージェント管理コンピューターに存在しなくなったファイル。
Reputation Approvals（レピュテーション承認）	Bit9 SRS のファイルまたはその公開者の信頼度によって承認されたファイル。

保存済みビュー	説明
Trusted Packages（信頼済みパッケージ）	信頼済みディレクトリの最上位レベルのファイル。他のファイルの共通のソースまたはインストーラー ファイルです。[View Details（詳細の表示）] ボタンをクリックすると、パッケージ自体の［File Details（ファイルの詳細）］ページが表示されます。パッケージ名をクリックすると、パッケージによって書き込まれた関連ファイルのテーブルが表示されます。各パッケージのルート ファイルは、他のタブにも表示される場合があることに注意してください。

Files on Computers（コンピューター上のファイル）

［Files on Computers（ファイル上のコンピューター)］タブには、エージェント コンピューター上のファイルのテーブルが表示されます。また、接続されていないコンピューターについては、エージェントが Bit9 Server と最後に通信したときに、そのコンピューター上に存在していたファイルが表示されます。削除されたコンピューターのファイルについては、削除後 1 日は削除済みコンピューターのファイルとしてマークされ、引き続き表示されますが、その期間が終了すると表示されなくなります。

デフォルトでは、［Files on Computers（コンピューター上のファイル)］テーブルには、すべてのコンピューターにある「すべて」の最上位レベル ファイル（他のファイルによってインストールされたり、他のファイルからコピーされたりしたものではないファイル）と、一連の初期化済みファイル（Bit9 エージェントがインストールされたときにコンピューターに存在していたファイル）が表示されます。ただし、カタログの別の［Saved View（保存済みビュー）］を選択することや、独自のビューを作成して、特定のファイルの種類に焦点を当てたり、1 つのファイルを検索したりできます。コンソール テーブルでのビューの変更にまだ慣れていない場合は、「Bit9 コンソールのテーブル」（68 ページ）を参照してください。最上位レベルのファイルだけでなく、コンピューター上の個別のファイルを表示することもできます。このオプションを選択する前に、「個別のファイルの表示」を参照してください。

［Files on Computers（コンピューター上のファイル）］タブには、表 24、「［File Catalog（ファイル カタログ）］タブの［Saved Views（保存済みビュー）］」（233 ページ）に示す次の保存済みビューが含まれています。

- Applications by Publisher/Company（アプリケーション（公開者 / 会社別））
- Banned Files（禁止ファイル）
- Categorized Files（分類済みファイル）
- Installed Programs（インストール済みプログラム）
- Malicious Files（悪意のあるファイル）
- Unapproved Files（未承認ファイル）

表 25 は、［File Catalog（ファイル カタログ)］テーブルのフィールドを示しています。このフィールドのほとんどが、［Files on Computer（コンピューター上のファイル)］テーブルにも表示されます。表 26 は、［Files on Computers（コンピューター上のファイル)］タブで使用できる追加フィールドを示しています。デフォルトでは、一部のフィールドは表示されません。

個別のファイルの表示

［Show individual files（個別のファイルを表示）］チェックボックスは、両方の［Files（ファイル）］ページ タブの右下にあり、表示されるファイルに大きな影響を及ぼします。

オンになっていない場合（デフォルト）、［File（ファイル）］ページには「最上位レベル」ファイル（他のファイルによってインストールされたり、他のファイルからコピーされたりしたものではないファイル）のみが表示されます。［Files on Computers（コンピューター上のファイル）］ページには、各コンピューターの一連の初期化済みファイルも表示されます。

このボックスがオンの場合、［Files（ファイル）］ページには、最上位レベルのファイルと、他のファイルによってインストールされたファイルが表示されます。Bit9 Server にレポートされた完全なファイル カタログ リストに表示される一意のファイル数が 1 億にのぼることもあります。［Files on Computers（コンピューター上のファイル）］は、コンピューター上に実際にあるファイルのインベントリで、さらに大きくなる場合があります。通常は発生しませんが、Bit9 エージェントが大量に存在する場合やデータベース サーバーの処理能力が低い場合などに、個別のファイルすべてを表示しようとすると、Bit9 Server がタイムアウトする可能性があります。この場合は、ビューを変更することを検討します。たとえば、［Show individual files（個別のファイルを表示）］をオフにして、［Group by（グループ別）］の選択を変更するか、別の列を基準に並べ替えます。フィルターを使用して、表示する合計ファイル数を制限することもできます。

かなり多くのファイルが含まれるテーブルを要求すると、左下に表示される、テーブルのすべてのページに含まれるアイテムの数が、「More than 10000 items（10000 アイテム以上）」のように概数で表示されます。また、結果数がそれほど大きくならなくても、要求したビューに Bit9 Server による追加処理が必要な場合は、このように表示されます。結果が表示された後に［**Refresh Page**（ページの更新）］をクリックすると、ほとんどの場合、正確な数字が表示されます。

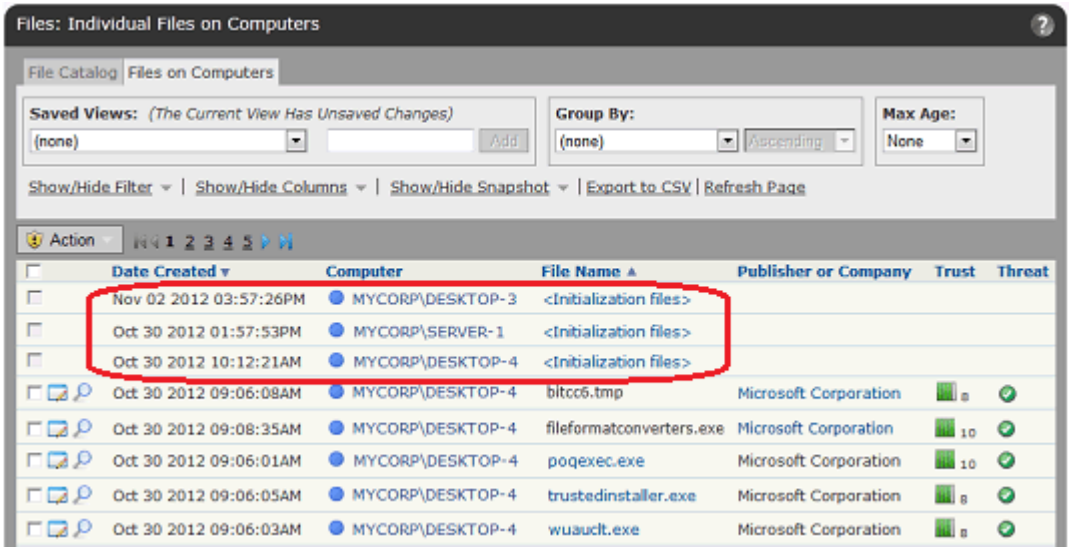
［File Catalog（ファイル カタログ）］ページまたは［Files on Computers（コンピューター上のファイル）］ページの最上位レベル ファイルの名前をクリックすると、そのファイルに関連付けられている個別のファイルのリストが表示されます。

プラットフォームに関する注意: この Bit9 Security Platform リリースでは、Windows ファイルのみがインストーラーごとにグループ化されます。したがって、［Show individual files（個別のファイルを表示）］をオンにしても、［File Catalog（ファイル カタログ）］の Windows 以外のコンピューターのファイルは変更されません。ただし、［Files on Computers（コンピューター上のファイル）］タブでは、初期化済みファイルが Mac パッケージ（適切にマークされたヘッダーが含まれる .pkg ファイル）のファイルとしてグループ化されるため、［Show individual files（個別のファイルを表示）］をオンにすると、テーブルに表示されるファイル数が多くなります。

初期化済みファイル

Bit9 エージェントをコンピューターにインストールすると、ファイルのインベントリであるファイルの「初期化」が直ちに始まります。エージェントは、クライアント コンピューターの固定ドライブにあるすべての実行可能ファイルのインベントリを取得して、各ファイルのハッシュを作成します。コンピューターが最初にサーバーに接続すると、そのエージェントは、各ハッシュを Bit9 Server に送信して、サーバーのファイル インベントリを更新します。初期化中のコンピューター上のファイルは、Bit9 Server で確認済みでないか、グローバルまたはポリシーで禁止されていない限り、「ローカル」承認済み状態になります。

［Show individual files（個別のファイルを表示）］をオンにしないと、各エージェント管理コンピューターの［Files on Computers（コンピューター上のファイル）］テーブルに、ファイル名「<**Initialization files**（初期化ファイル）>」の行が示されます。［<Initialization files（初期化ファイル）>］をクリックすると、コンピューターのすべての初期化済みファイルが表示されたテーブルが開きます。この方法は、エージェントのインストール前に各システムに存在していたファイルを確認する際に役立ちます。

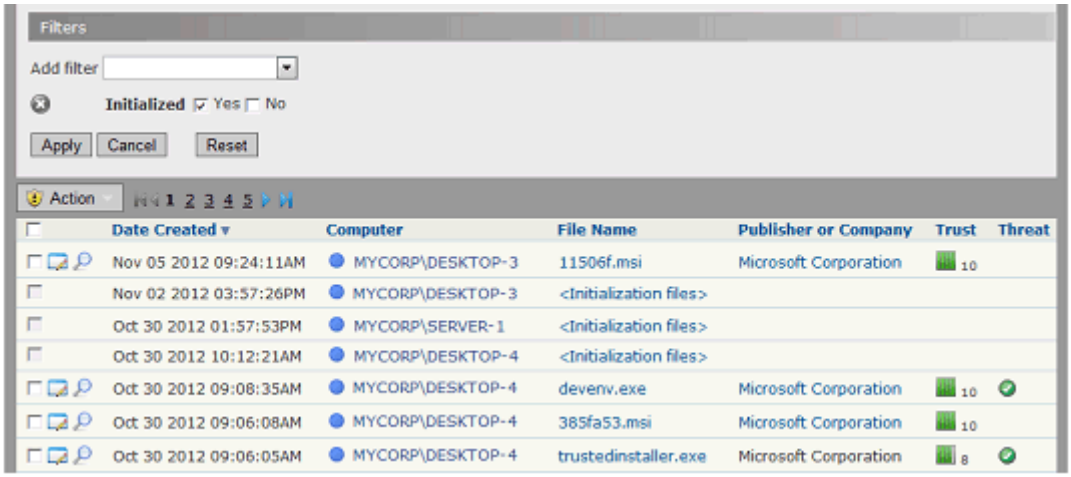


エージェントを無効にしてから、再度有効にすると、新しい初期化プロセスが開始され、［<Initialization files（初期化ファイル）>］グループは変更されます。それ以外の場合、このグループは、エージェントで問題が発生しない限り変わりません。エージェントをアップグレードしても、初期化済みファイルのリストは変更されません。

［Files on Computers（コンピューター上のファイル）］ページで［<Initialization files（初期化ファイル）>］をクリックすると、そのコンピューターのファイル リストがテーブルに表示されます。いずれかのファイルをクリックすると、そのファイルを含むグループのリストが表示されますが、現在のコンピューターでは、そのファイルを含むグループは特定されません。これは、エージェントよりも前に存在していたファイルが、さまざまな場所からインストールまたはコピーされた可能性があるからです。

［Files on Computers（コンピューター上のファイル）］ページで、［Show individual（個別に表示）］ボックスがオンになっていない場合、［Initialized（初期化済み）］が［Yes（はい）］に設定されているフィルターを使用すると、［<Initialization files

（初期化ファイル）>］と、通常は、他の複数ファイルに対する行がテーブルに表示されます。他のファイルは既知のインストーラーですが、［<Initialization files（初期化ファイル）>］グループにも追加されます。



ファイル テーブル ページのメニュー

［File Catalog（ファイル カタログ）］テーブルおよび［Files on Computers（コンピューター上のファイル）］テーブルの左上には［Action（アクション）］メニューがあります。表 27、「ファイル テーブルおよび詳細ページのメニュー」258 ページは、ファイル ページのメニューで使用できるオプションを示しています。オプションの中には、一部のファイル状態でしか使用できないものがあることに注意してください。

指定したファイルが存在する、または存在しないコンピューターの検索

使用している環境にアプリケーションを追加する場合、または新しいファイルで既存のプログラムを更新する場合に、この変更に関連するファイルが不足しているコンピューターがないかどうかを確認する必要があることがあります。一方、1 つ以上のファイルを環境から削除しなければならない場合は、こうしたファイルが存在するコンピューターの一覧を取得できると便利です。Bit9 コンソールのファイル ページには、ファイル ハッシュを検索パラメーターとして使用することで、この情報を入手できるメニューがあります。

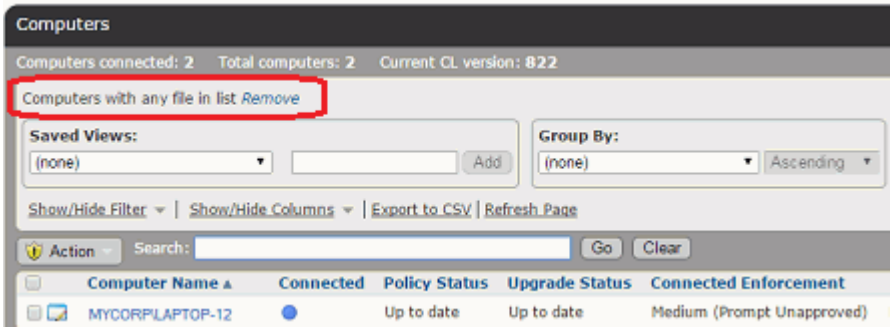
［File Details（ファイルの詳細）］ページと［File Details（ファイルの詳細）］ページの両方の［Related Views（関連ビュー）］メニューに、次のコンピューター検索オプションが用意されています。

- ［**Computers with this file**（このファイルが存在するコンピューター）］– 詳細ページで示したファイルが存在するコンピューターの一覧が含まれている［Computers（コンピューター）］テーブルを表示します。
- ［**Computers without this file**（このファイルが存在しないコンピューター）］– 詳細ページで示したファイルが存在しないコンピューターの一覧が含まれている［Computers（コンピューター）］テーブルを表示します。

［File Catalog（ファイル カタログ）］ページ、［Files on Computers（コンピューター上のファイル）］ページ、および［Find Files（ファイルの検索）］結果ページのテーブルで複数のファイルをオンにして、［Action（アクション）］メニューのコマンドをそのファイルすべてに適用することができます。他にもコンピューター検索オプションが用意されています。

- ［**Find computers with at least one of the selected files**（選択したファイルの少なくとも 1 つが存在するコンピューターを検索）］–［Files（ファイル）］ページでオンにしたファイルのうち、少なくとも 1 つのファイルが存在するコンピューターの一覧が含まれている［Computers（コンピューター）］テーブルを表示します。
- ［**Find computers with all of the selected files**（選択したファイルすべてが存在するコンピューターを検索）］–［Files（ファイル）］ページでオンにした「すべて」のファイルが存在するコンピューターの一覧が含まれている［Computers（コンピューター）］テーブルを表示します。
- ［**Find computers missing at least one of the selected files**（選択したファイルの少なくとも 1 つが存在しないコンピューターを検索）］–［Files（ファイル）］ページでオンにしたファイルのいずれかが存在しないコンピューターの一覧が含まれている［Computers（コンピューター）］テーブルを表示します。
- ［**Find computers missing all of the selected files**（選択したファイルすべてが存在しないコンピューターを検索）］–［Files（ファイル）］ページでオンにした「すべて」のファイルが存在しないコンピューターの一覧が含まれている［Computers（コンピューター）］テーブルを表示します。

［Computers（コンピューター）］ページでは、これらのコマンドの結果と一緒に［Saved View（保存済みビュー）］メニューの上に凡例が表示され、どのコマンドが使用されたかが示されます。こうした結果を生成したフィルターを解除して、通常の［Computers（コンピューター）］ページ ビューに戻すには、この凡例の横にある［**Remove**（削除）］リンクをクリックします。



注意

［Files on Computers（コンピューター上のファイル）］インベントリからファイルが除外されている場合、これらのコマンドを使用して、そのファイルが存在するコンピューターを特定することはできません。たとえば、［System Configuration（システム構成）］ページの［Advanced（詳細）］タブで、Microsoft サポート ファイルの追跡がオフになっている場合は、コンピューターの検索コマンドで、それらのファイルに対する正確な結果を取得することはできません。

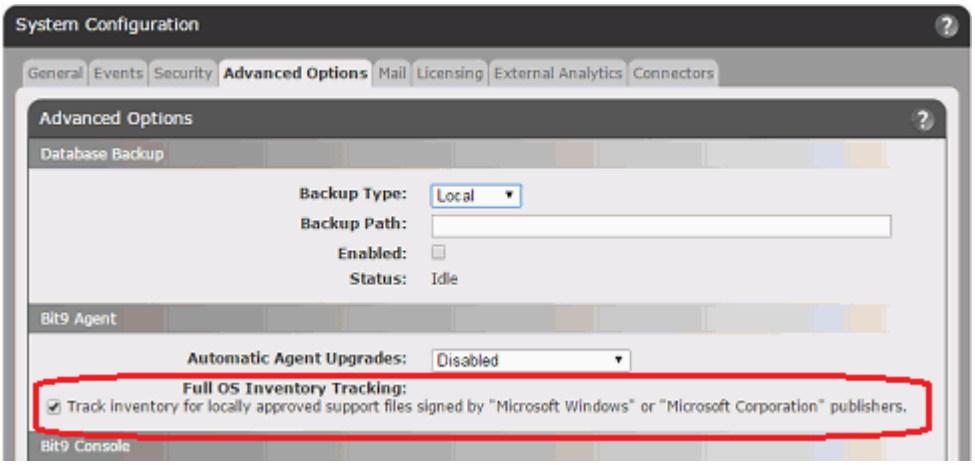
Microsoft サポート ファイルの追跡の除外

Bit9 では、デフォルトで、サーバーに接続されているすべてのエージェント上にある追跡対象ファイルのインスタンスすべてがインベントリに保存され、追跡されます。こうしたファイルの多くが、Windows オペレーティング システム ファイルと Microsoft アプリケーションのファイル、そして関連するシステム更新プログラムです。Windows のアップグレードに伴い、オペレーティング システム ファイルの数が増え、その数は Windows XP の数倍になっています。さらに、アプリケーションのファイルも同じように増えます。Windows 更新プログラムのサイズもかなり大きくなっています。こうした増大により、Windows コンピューターのインベントリにあるすべてファイルに対して、Microsoft ファイルが占める割合が半分、場合によっては 4 分の 3 以上になることもあります。

Microsoft のファイルを信頼し承認している場合、そのファイルは追跡したくないこともあります。Bit9 Platform には、公開者「Microsoft Windows」または「Microsoft Corporation」によって署名されている一部のファイルに対して、ファイル追跡を除外するオプションが用意されています。システム上のファイル インスタンスの大部分に対してファイル追跡をオフにすることで、指定したエージェント数に対して必要なデータベースのサイズを減らし、こうしたファイルの処理に必要なサーバーの負荷を軽減できます。

こうしたファイルの追跡をオフにすると、[Files on Computers（コンピューター上のファイル）] インベントリからそのファイルの「インスタンス」が除外され、そのファイルに関連するイベントが制限されます。その場合、こうしたファイルはエンドポイントで表示されなくなりますが、ファイルのハッシュと情報は、それがエージェント管理コンピューターに存在している限り、[File Catalog（ファイル カタログ）] に表示されます。また、こうしたファイルに関連する承認、禁止などのイベントについては、引き続きレポートされます。

Microsoft 署名サポート ファイルのインスタンスの追跡は、[System Configuration（システム構成）] ページの [Advanced Options（高度なオプション）] タブで制御します。デフォルトでは、これらのファイルは追跡されます。



Microsoft 署名サポート ファイルのインスタンスを無効または再度有効にする手順：

1. コンソール メニューで、[**Administration**（管理）] > [**System Configuration**（システム構成）] の順に選択します。[System Configuration（システム構成）] ページが表示されます。
2. [**Advanced Options**（高度なオプション）] タブをクリックし、ページ下部の [**Edit**（編集）] ボタンをクリックします。
3. [Bit9 Agent（Bit9 エージェント）] パネルで、[Full OS Inventory Tracking（OS インベントリの詳細追跡）] チェックボックスを「オフ」にします。「Microsoft Windows」または「Microsoft Corporation」によって署名されたサポート ファイルの追跡が無効になります。
4. ページ下部の [**Update**（更新）] ボタンをクリックします。サポート ファイルの追跡が無効になります。
5. これらのファイルの追跡を再度有効にするには、[Full OS Inventory Tracking（OS インベントリの詳細追跡）] チェックボックスをオンにして、[Update（更新）] ボタンをクリックします。この変更を確定するには、確認ダイアログで [**Yes**（はい）] をクリックします。
   注意：[Full OS Inventory Tracking（OS インベントリの詳細追跡）] の確認ダイアログには、製品のパフォーマンスへの影響に関する警告が表示されます。この設定を長い間オフにしていた場合は、ファイル トラフィックの大幅な増加に伴う要件を作業環境が満たしているかどうかを確認してください。

影響を受けるファイル インスタンス

[Full OS Inventory Tracking（OS インベントリの詳細追跡）] をオフにすると、次の「すべての」の条件を満たすファイルのインスタンスが追跡されなくなります。

- 公開者が「Microsoft Windows」または「Microsoft Corporation」である。これには直接署名されたファイルと、デタッチされた公開者によって署名されたファイルが含まれます。他の Microsoft 公開者によって署名されたファイルは、正規なファイルであっても追跡対象となります。
- ファイルが .DLL などのサポート ファイルである。これは、通常は追跡対象と見なされるため、Bit9 によって追跡されます。.EXE ファイルまたはそのファイルに関連するイベントの追跡は、このオプションの影響を受けません。
- ファイルが、直接または承認ルールによってローカルで承認されている。

OS インベントリ追跡に影響する変更

他のルールと同様、Bit9 Platform では、OS インベントリの詳細追跡ルールとその他のルールや条件が相互に作用します。

- [**File State Transitions**（ファイル状態の移行）] – ファイル除外が有効の場合（つまり、[Full OS Inventory Tracking（OS インベントリの詳細追跡）] が「無効」の場合）、除外の条件を満たす未承認ファイルのインスタンスが登録され、追跡されます。こうしたファイルは、後で承認された時点で追跡されなくなりますが、サーバーにはファイルの状態の変更は組み込まれません。つまり、

ファイルは、普及度が 0 として表示されても、インベントリに残ったままになります。このようになる条件を次に示します。

- Microsoft サポート ファイルがローカルで「未承認」だったため、インベントリから除外されず、後でローカルで承認された。
- ［Full OS Inventory Tracking（OS インベントリの詳細追跡）］が無効になっているときの公開者の信頼度の条件が高く（たとえば、承認のための最小キー サイズが 2048）、Microsoft サポート ファイルが「除外されなかった」が、その後、公開者の信頼度が低くなり（たとえば、最小 1024 ビット）、サポート ファイルのほとんどが承認された。

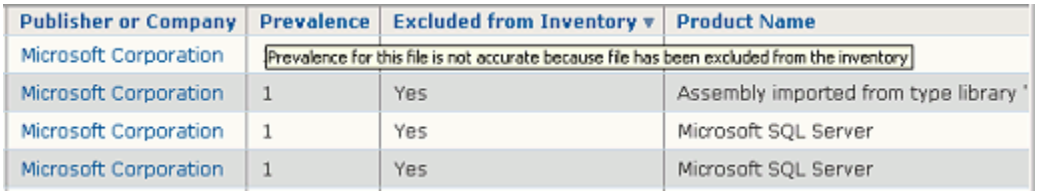
- ［**Disabling Tracking**（追跡の無効化）］–［Full OS Inventory Tracking（OS インベントリの詳細追跡）］を無効にすると、次が発生します。
  - 影響を受けるすべてのファイルが、［Files on Computers（コンピューター上のファイル）］ページのファイル インベントリから削除されます。削除は、サーバーの負荷が高くないときにバックグラウンドで行われ、インベントリのサイズにもよりますが、数日かかることがあります。イベントによって、インベントリから削除されたファイル数がレポートされます。
  - こうしたファイルの新しい承認済みインスタンスとファイルへの変更は、登録も追跡もされません。
- ［**Re-Enabling Tracking**（追跡の再有効化）］–［Full OS Inventory Tracking（OS インベントリの詳細追跡）］を無効にした後に再度有効にした場合は、Microsoft 署名ファイルが、エージェント コンピューターからインベントリに自動的に再保存されることはなく、新しいインスタンス、または関連ファイルのアクティビティが追跡されます。前から存在するすべての Microsoft サポート ファイルのインベントリを収集する必要がある場合は、コンピューターごとにすべてのファイル情報を再同期します。このオプションは、［Computers（コンピューター）］ページの［Action（アクション）］メニューにあります。
- ［**Agent Version**（エージェント バージョン）］– エージェント 7.2.1 以降では Microsoft サポート ファイルの追跡をオフにできます。こうしたエージェントは、ドキュメントで説明されているとおりに動作します。その前の（サポートされている）エージェントでも追跡をオフにできますが、動作が異なります。以前のエージェントでは必要な情報がいくつか不足しているため、サーバーはそのエージェントから即座にファイルを除外できるとは限りません。たとえば、ファイルがサポート ファイルであること、またはファイルが Microsoft によって署名されていることを、検出できないことがあります。ただし、こうしたファイルは、毎日行われるファイル情報の定期更新中にバックグラウンドで削除されます。

除外されたファイル インスタンスに関する情報

承認済み Microsoft サポート ファイルのインスタンスの追跡をオフにしても、その情報は使用できます。情報の中には、ファイルの特定のインスタンスではなく、ファイル自体の一般的な情報であるものがあります。

2 つの関連 Microsoft 公開者によって署名されたローカル承認済みサポート ファイルの追跡をオフにしても、ハッシュが含まれるファイルが任意のエージェント監視コンピューターに表示されていれば、サポート ファイルは引き続き［File Catalog（ファイル カタログ）］に表示されます。インスタンス追跡がオフになっているため、ファイルの普及度（ファイルが見つかったコンピューターの数）の

値は信頼できず (ゼロの場合があります)、普及度を計算できないというヒントが表示されます。



通常はこうしたファイルの追跡はオフにしますが、特定のインスタンスの追跡が必要になることがあります。たとえば、特定の Microsoft DLL バージョンによって脆弱性がレポートされたため、それを変更する場合などです。こうしたファイルの負荷を軽減しながら、特定のファイルの実行を追跡できるように、全般設定を管理する方法はいくつかあります。

- **禁止のレポート** – ファイルに対してレポートのみの禁止を作成できます。すべてのコンピューター上にあるこのファイルのインスタンスすべてがインベントリに追加されます。
- **メーター** – ファイル ハッシュに対してメーターを作成すると、除外されたファイルのすべての実行がイベントとしてメーターによってレポートされますが、そのインスタンスは［Files on Computers（コンピューター上のファイル)］インベントリに追加されません。
- **分析ツールへのデータのエクスポート** – Bit9 Platform を、Splunk などの外部分析ツールに統合すると、除外されたファイル インスタンスのデータが、他のファイルやイベント データすべてと一緒に追加されます。外部ツールを使用すると、これまでにすべてのコンピューターに現れ、除外されたファイルのすべてのインスタンスを見つけることができます。また、外部ツールに提供されたデータでは、こうしたファイルの実行も追跡されます。
- **［File Catalog（ファイル カタログ)］の［Inventory（インベントリ)］列からの除外** – ［File Catalog（ファイル カタログ)］ではオプションの［Excluded from Inventory（インベントリからの除外)］列を使用できます。この列をテーブルに追加すると、除外された OS サポート ファイルであることが理由でインスタンスがファイル インベントリにないファイルを特定できます。
  注意：Microsoft サポート ファイル除外を有効にした後にローカルで承認されたファイルは、引き続き「未承認」ファイルとして表示されるため、［Files on Computers（コンピューター上のファイル)］インベントリに表示されます。

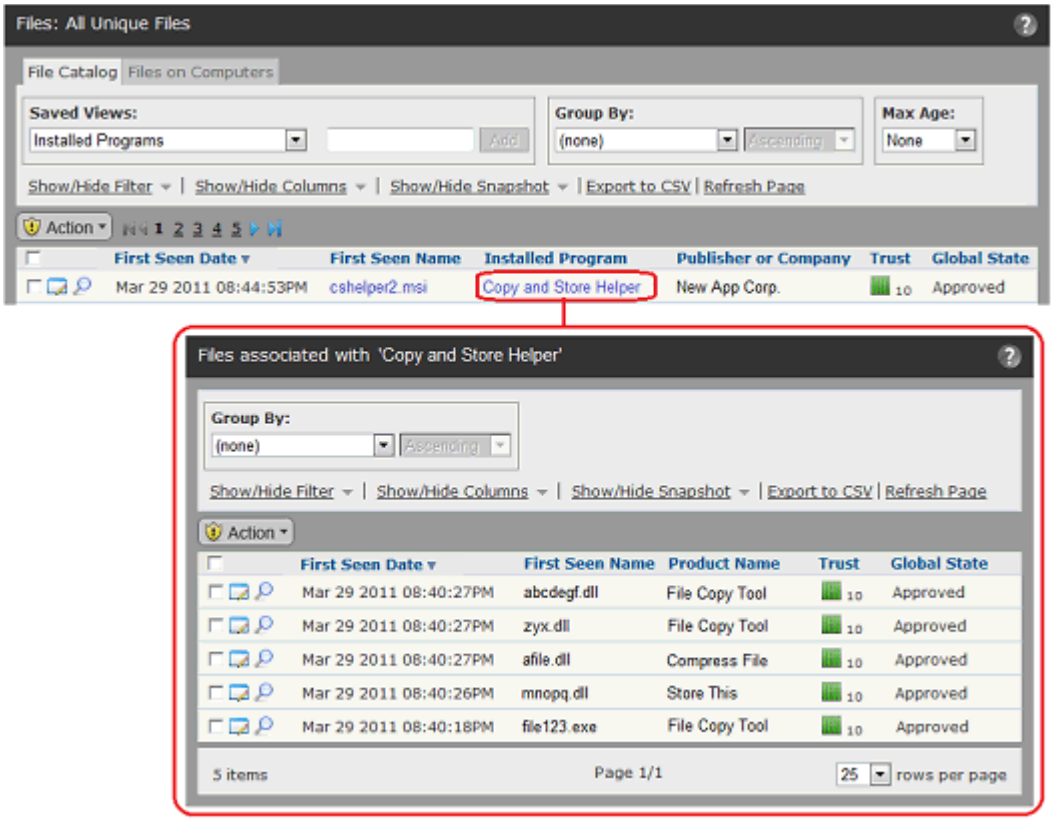
Bit9 エージェントのほか、Carbon Black センサーがコンピューターにインストールされている場合は、Carbon Black が、こうしたファイルの実行を引き続き検出してレポートします。

ファイル グループ

プラットフォームに関する注意: このBit9 Security Platform リリースでは、Windows コンピューターのファイルのみがインストーラーごとにグループ化されます。したがって、このセクションは他のプラットフォームには適用されません。

コンピューターへのファイルのインストール中、ファイルはそのインストール プロセスの分析に従ってグループ化されます。このグループには一意の名前や、複数のグループに共通のインストーラー名（「setup.exe」など）が付けられる場合があります。

インストールが完了すると、エージェントは、Windows プログラムのデータベースをスキャンして、そのファイルを「プログラムと機能」エントリに関連付けることができるかどうかを確認します。関連付けられる場合、ファイルは、対応するプログラムの変更または削除に使用されるファイルの下で再グループ化されます。「プログラムと機能」エントリが見つからない場合は、インストール済みファイルの最初のグループ名が保持されます。



ファイルがBit9 コンソールに表示される場合は必ず、グループ名が使用されます。次に例を示します。

- ［File Catalog（ファイル カタログ）］ページと［Files on Computers（コンピューター上のファイル）］ページで、［Installed Programs（インストール済みプログラム）］の［Saved View（保存済みビュー）］を選択して、アプリケーションのリストを表示できます。
- ［Baseline Drift Report Results（ベースライン ドリフト レポートの結果）］の［Files（ファイル）］ビューでは、インストール済みプログラムごとにグルー

プ化して、各アプリケーションの属性となっているドリフトの大きさを確認できます。

- ［File Catalog（ファイル カタログ）］でハイライト表示されているファイル名をクリックすると、クリックしたファイルに関連付けられているファイルの一覧と、通常は、関連付けられているファイルが含まれるアプリケーションが［File Group Details（ファイル グループの詳細）］ページに表示されます。ここには、Bit9 エージェントが実行されているすべてのコンピューター上の、ハイライト表示されたファイルによってインストールされた一意のファイルすべてがまとめられています。
- ［Files on Computers（コンピューター上のファイル）］ページでハイライト表示されているファイル名をクリックすると、クリックしたファイル インスタンスに関連付けられているファイルの一覧が［File Group details（ファイル グループの詳細）］ページに表示されます。
- ［Files on Computers（コンピューター上のファイル）］ページの［<Initialization files（初期化ファイル）>］行をクリックすると、Bit9 エージェントが最後に初期化された時点で（通常は、エージェントがインストールされたときに）その行で指定されていた、コンピューター上のファイルの一覧が表示されます。

詳細ページの表示

Bit9 コンソールには、管理しているファイルを対象とした 2 つの詳細ページが用意されています。

- ［**File Details**（ファイルの詳細）］– Bit9 エージェントが実行されているコンピューターで検出された「一意のファイルごと」に、ファイルのグローバル情報が表示される［File Details（ファイルの詳細）］ページを開くことができます。このページでは、ファイルのさまざまなグローバル パラメーターを変更できます。［File Details（ファイルの詳細）］ページには、［File Catalog（ファイル カタログ）］テーブルに表示されている一意のファイルに関する詳しい情報が表示されます。
- ［**File Instance Details**（ファイル インスタンスの詳細）］– Bit9 エージェントが実行されているコンピューターで検出された「一意のファイル インスタンスごと」に、［File Instance Details（ファイル インスタンスの詳細）］ページを開くことができます。このページには、［File Details（ファイルの詳細）］ページに表示されているグローバル情報の一部のほか、そのインスタンスに固有の情報が表示されます。また、このページで、ファイルのインスタンスとグローバル属性の両方を変更することもできます。［File Instance Details（ファイル インスタンスの詳細）］ページには、［Computers on Files（コンピューター上のファイル）］テーブルに表示されているファイル インスタンスに関する詳しい情報が表示されます。

次のセクションでは、ファイル詳細ページの概要について説明します。また、これらのページで使用できるメニュー コマンドの表もあります。ファイル詳細ページで実行できるアクティビティについては、『Bit9 Security Platform の使用』の他の場所で詳しく説明しています。特に、第 8 章「ソフトウェアの承認と禁止」を参照してください。

［File Details（ファイルの詳細）］ページ

［File Details（ファイルの詳細）］ページには、ファイルのグローバル状態の詳細が表示されます。一意のファイルが表示される［File Catalog（ファイル カタログ）］などのテーブルで［View Details（詳細の表示）］（鉛筆）ボタンをクリックすると、［File Details（ファイルの詳細）］ページが開きます。

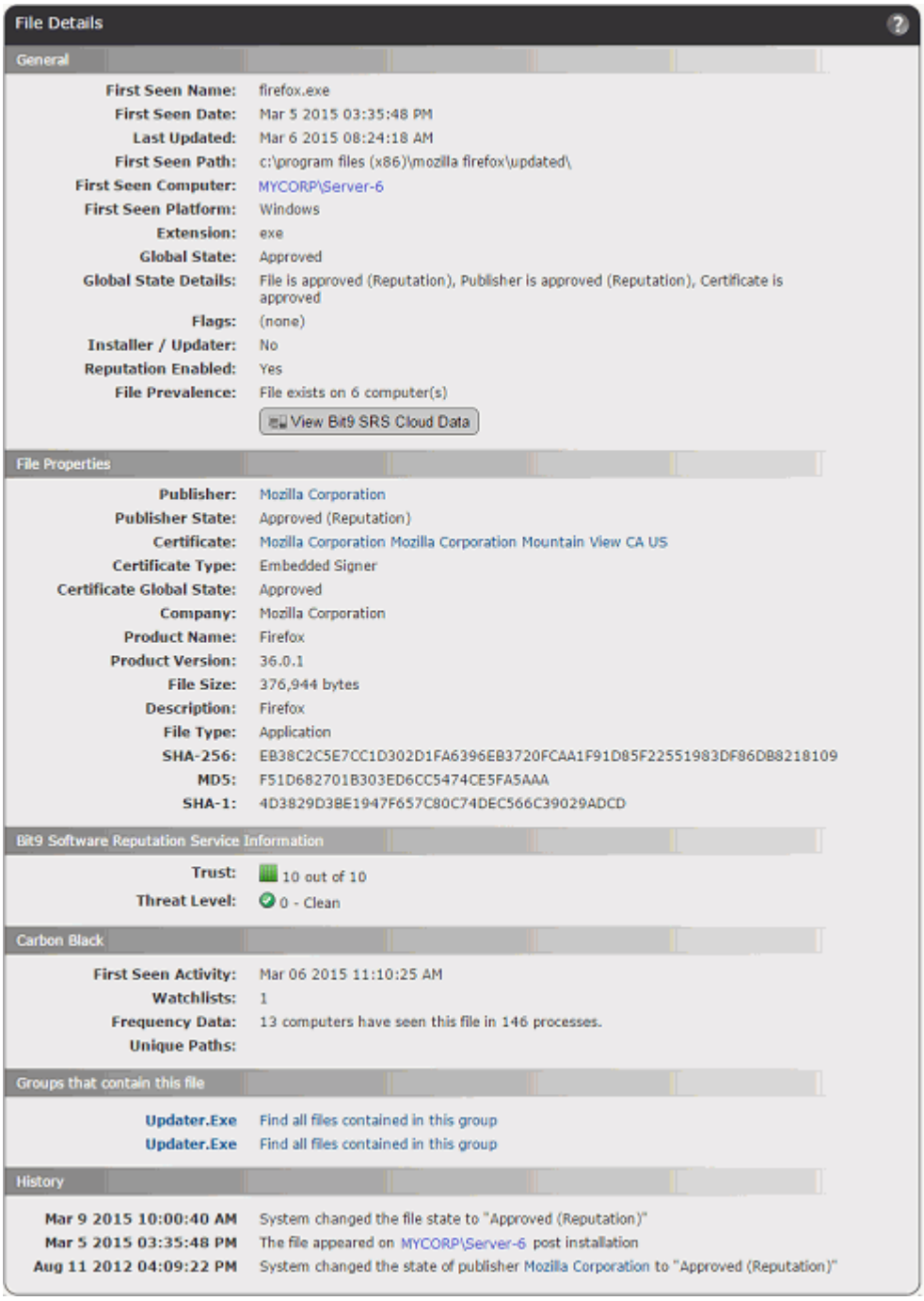


表 25 は、［File Details（ファイルの詳細）］ページで使用できる情報とアクションを示しています。一部のグローバル ファイル属性は、Bit9 エージェントが参照す

るファイルの「最初に確認された」インスタンスに対してのみ捕捉されます。これには、[File Details（ファイルの詳細）] ページと同様のラベルが付けられます。

表 25：[File Details（ファイルの詳細）] および [File Catalog（ファイル カタログ）] ページのフィールド

フィールド	説明
[General（全般）] パネル	
First Seen Name（最初に確認された名前）	この Bit9 Server によって管理されているエージェントによってこのハッシュが検出された最初のファイルの名前。
First Seen Date（最初に確認された日付）	このハッシュが含まれる最初のファイルがネットワーク コンピューターで確認された日時。表示形式は、MM DD YYYY hh:mm:ss(AM/PM) です。
Last Updated（最終更新日）	このファイルのメタデータが更新された最終更新日時（普及度、信頼度など、Bit9 提供のデータに影響されません）。
First Seen Path（最初に確認されたパス）	このサーバーにこのハッシュがレポートされた最初のファイルのパス。
First Seen Computer（最初に確認されたコンピューター）	ファイルが最初に確認されたコンピューターの名前。この名前をクリックすると、このコンピューターの [Computer Details（コンピューターの詳細）] ページが表示されます。 最初に確認されたコンピューターを後でシステムから削除すると、ファイルとの関連性が解除され、このフィールドは空白になります。
First Seen Platform（最初に確認されたプラットフォーム）	この Bit9 Server によってこのファイルが最初に確認されたプラットフォーム（Windows または Mac）。
Extension（拡張子）	このハッシュが含まれる最初に確認されたファイルの拡張子。
Global State（グローバル状態）	[File State（ファイルの状態）] と [Publisher State（公開者の状態）] が組み合わされた [Global State（グローバル状態）] は、すべてのシステムまたはポリシーごとの全体的な承認状態を示します。ファイルのグローバル承認は、ハッシュまたは公開者によって行うことができ、[Approved（承認）]、[Banned（禁止）]、[Unapproved（未承認）]、[Approved By Policy（ポリシーにより承認）]、[Banned By Policy（ポリシーにより禁止）]、[Mixed（混在）] のいずれかの値になります。ファイルの承認状態がポリシーによって異なるファイルについては、[Global State（グローバル状態）] は [Mixed（混在）] になります。たとえば、あるポリシーでハッシュによって禁止されているファイルが、残りのすべてのポリシーで公開者によって承認されていることがあります。

フィールド	説明
Global State Details（グローバル状態の詳細）	[Global State（グローバル状態）] に影響しているファイルの状態と公開者の状態。
Flags（フラグ）	Bit9 サポート エンジニアが使用するファイル状態のメタデータ。この情報の提供をサポート担当者から求められる場合があります。
Installer/Updater（インストーラー / アップデーター） （[File Details（ファイルの詳細）]） **Installer（インストーラー）** （[File Catalog（ファイル カタログ）]）	このファイルが、Bit9 の分析ツールまたはコンソール ユーザーによってインストーラーまたはアップデーターとして特定されているかどうかを示します（ファイルが承認されると、そのファイルによって作成されたすべてのファイルが承認されることを示します）。 **Yes**（はい）– インストーラーとして処理されます。拡張され、さらに多くのファイルを作成します。このファイルが承認されると、このファイルによって作成されたファイルは、ローカルで承認されます。 **No**（いいえ）– 拡張できないファイルとして処理されます。
Reputation Enabled（レピュテーション有効）	このファイルに対してレピュテーションに基づく承認が有効かどうかを示します（[Yes（はい）] または [No（いいえ）]）。
File Prevalence（ファイル普及度）	このファイルが存在するコンピューターの数。 [Actions（アクション）] メニューの [**Add Alert**（アラートの追加）] コマンドを使用すると、ファイルの普及度が所定のレベルに達したときにトリガーされるアラートを追加できます。詳細については、「Bit9 アラートの使用」（606 ページ）を参照してください。
View Bit9 SRS Cloud Data（Bit9 SRS Cloud データの表示）（ボタン）	クリックすると、Bit9 SRS からこのファイルの詳細な分析結果（使用できる場合）を取得できます。Bit9 SRS を有効にすると、[File Details（ファイルの詳細）] ページに表示されます。詳細については、「Bit9 SRS の有効化」（787 ページ）を参照してください。
[File Properties（ファイル プロパティ）] パネル	
Publisher（公開者）	ファイルがデジタル署名されているか、デジタル署名されたパッケージに含まれていた場合に、アプリケーションに関連付けられている公開者（ソフトウェア製造業者）が表示されます。
Publisher State（公開者の状態）	公開者の承認状態。[Approved（承認）]、[Approved By Policy（ポリシーにより承認）]、[Banned（禁止）]、[Banned By Policy（ポリシーにより禁止）]、[Unapproved（未承認）] のいずれかの値になります。公開者が不明の場合は表示されません。
Certificate（証明書）	このファイルに署名した証明書のサブジェクト名。

フィールド	説明
Certificate Type（証明書の種類）	リーフ証明書の場合、証明書の種類は、そのリーフ証明書の用途と、ファイルにどのように関連付けられているかを示します。次の語句の組み合わせが表示されます。[Embedded（埋め込み）]、[Detached（デタッチ）]、[Signer（署名者）]、[Cosigner（副署者）] のいずれかになります。
Certificate Global State（証明書のグローバル状態）	証明書の現在の状態。[Unapproved（未承認）]、[Approved（承認）]、[Banned（禁止）]、[Approved By Policy（ポリシーにより承認）]、[Banned By Policy（ポリシーにより禁止）]、[Mixed（混在）] のいずれかの値になります。
Company（会社）	ファイル メタデータの会社名（指定されている場合）。
Product Name（製品名）	ファイル メタデータの製品名（指定されている場合）。
Product Version（製品バージョン）	ファイル メタデータの製品バージョン（指定されている場合）。
File Size（ファイル サイズ）	ファイルのサイズ（バイト単位）
Description（説明）	ファイル メタデータの説明（指定されている場合）。
File Type（ファイル タイプ）	次のいずれかになります。 [**Application**（アプリケーション）] – パッケージを除くすべての実行可能ファイル（.exe、.com など） [**Supporting File**（サポート ファイル）] – 実行可能ファイルによってロードされた任意のライブラリ（.dll、.ocx、.sys） [**Package**（パッケージ）] – 任意のインストーラー（コンテンツを含む .exe。自己解凍 zip、セットアップ プログラムなど） [**Script File**（スクリプト ファイル）] – 任意のスクリプトまたはバッチ ファイル（.bat、.vbs、.wsf など） [**Other**（その他）] – 今後使用するために予約されているタイプ [**Unrecognized Executed File**（未確認の実行済みファイル）] – 初期化中にもその後の分析でも Bit9 によって実行可能ファイルとして特定されなかったが、特定のプロセスによって実行が試みられたファイル。実行が試行されたことで、そのファイルは、Bit9 Server および Bit9 エージェントによって追跡および管理されたファイルのリストに追加されます。 [**Unknown**（不明）] – ファイル タイプ情報を提供しない古い Bit9 エージェントによってレポートされたファイル

フィールド	説明
SHA-256	Bit9 独自の SHA-256 アルゴリズムを使用して作成されたファイルのハッシュ（データ署名）。SHA-256 は、Bit9 によって追跡されるファイルの優先ハッシュとして内部的に使用されます。 Bit9 アルゴリズムによって作成された SHA-256 ハッシュが、他の手段で作成されたハッシュと同じ場合もありますが、ファイルには、日付、場所、または追跡目的とは関係ないコンテキスト固有の情報が含まれているため、一部のファイルではインストールのたびにハッシュが変わります。このように動作するファイルでは、特別な**ファジー ハッシュ**アルゴリズムによってこの無関係の「ゆれ」が排除され、Bit9 エージェントが実行されているコンピューター上の、こうしたファイルのインスタンスすべてが同じものとして表示されます。このアルゴリズムを使用すると、ハッシュは、「SHA-256（正規化済み）」として特定されます。 ハッシュによってファイルを検索するには、[Files（ファイル）] ページまたは［Find Files（ファイルの検索）］ページのフィルターを使用します。[Related Views（関連ビュー）] の［**All File Instances**（すべてのファイル インスタンス）］を使用すると、[File Details（ファイルの詳細）] ページからこの操作を直接行うことができます。
MD5	MD5 は、広く使用されているハッシュ アルゴリズムです。Bit9 には、公開済み MD5 ハッシュのリストを使ってファイルを特定できるように、この代替ハッシュが用意されています。
SHA-1	SHA-1も広く使用されているハッシュ アルゴリズムの1つです。Bit9 には、公開済み SHA-1 ハッシュのリストを使ってファイルを特定できるように、この代替ハッシュが用意されています。
[Bit9 Software Reputation Service Information（Bit9 Software Reputation Service 情報）] パネル	
Trust（信頼度）	ファイル ソース、証明書などの Bit9 Software Reputation Service (SRS) 情報に基づくファイルの信頼度を示します。信頼度は、0（信頼できない）から 10（最も信頼できる）の数値で表され、この数値を示すメーターがグラフィック表示されます。ファイルの信頼度が不明の場合もあります。この場合、そのファイルに対する列のこのフィールドは空白で、その詳細ページには「(unknown)（(不明)）」と表示されます。 このフィールドの値は、ファイル整合性の主観評価です。ファイルが安全かどうかは Bit9 SRS 分析による情報に基づいており、信頼度の値は、Bit9 Server における実際の承認を示すものではありません。ただし、レピュテーション ルールを使用すると、ファイルの信頼度または公開者の信頼度に基づいてファイルを自動的に承認できます。

フィールド	説明
Threat level（脅威レベル）	Bit9 SRS が構成されている場合は、検出されたファイルが自動的に脅威分析に送信されます。既知のマルウェアには、赤色の「x」アイコンでフラグが設定されます。フラグが設定されていないファイルは、マルウェアとして認識されませんでしたが、必ずしも安全だとは限りません。脅威レベルを次に示します。 **0** – クリーン **1** – 危険な可能性あり **2** – 悪質 **Unknown（不明）** – 特定できません
Category（カテゴリ）	Bit9 SRS を構成した場合は、このファイルのカテゴリ（エンターテイメント、ハッキング ツール、インスタント メッセージ、メディア プレーヤー）が表示されます。カテゴリがわからない場合もあります。この場合、カテゴリは詳細ページに表示されません。
Policy Specific States（ポリシー固有の状態）	ポリシー固有のファイル処理方法を示します。たとえば、ファイルのハッシュがポリシー固有の方法で禁止または許可されている場合、そのポリシー名がここに表示されます。ポリシー固有のファイル処理がない場合は、表示されません。
[Carbon Black] パネル（すべてのデータが Carbon Black Server から提供されます）	
First Seen Activity（最初に確認されたアクティビティ）	このファイルに関するアクティビティが Carbon Black サーバーに最初にレポートされた日時。
Watchlists（ウォッチリスト）	このファイルが含まれる Carbon Black ウォッチリストの数が表示されます。
VirusTotal Score（VirusTotal スコア）	このファイルの VirusTotal スコアが表示されます。
Frequency Data（頻度データ）	この MD5 ハッシュ値を持つバイナリを確認したホストの数が表示されます。
Unique Paths（一意のパス）	このファイルが確認された一意のパスの数が表示されます。
Network Connections（ネットワーク接続）	このプロセスの実行時に試行または確立したネットワーク接続の数が表示されます。
Registry Modifications（レジストリ変更）	このファイルを実行したために行われたレジストリ変更の数が表示されます。
File Icon（ファイル アイコン）	このファイルに関連付けられているデスクトップ アイコンが表示されます（存在する場合）。
More information（詳細情報）	Carbon Black コンソールに戻って、ファイルの追加情報を入手します。

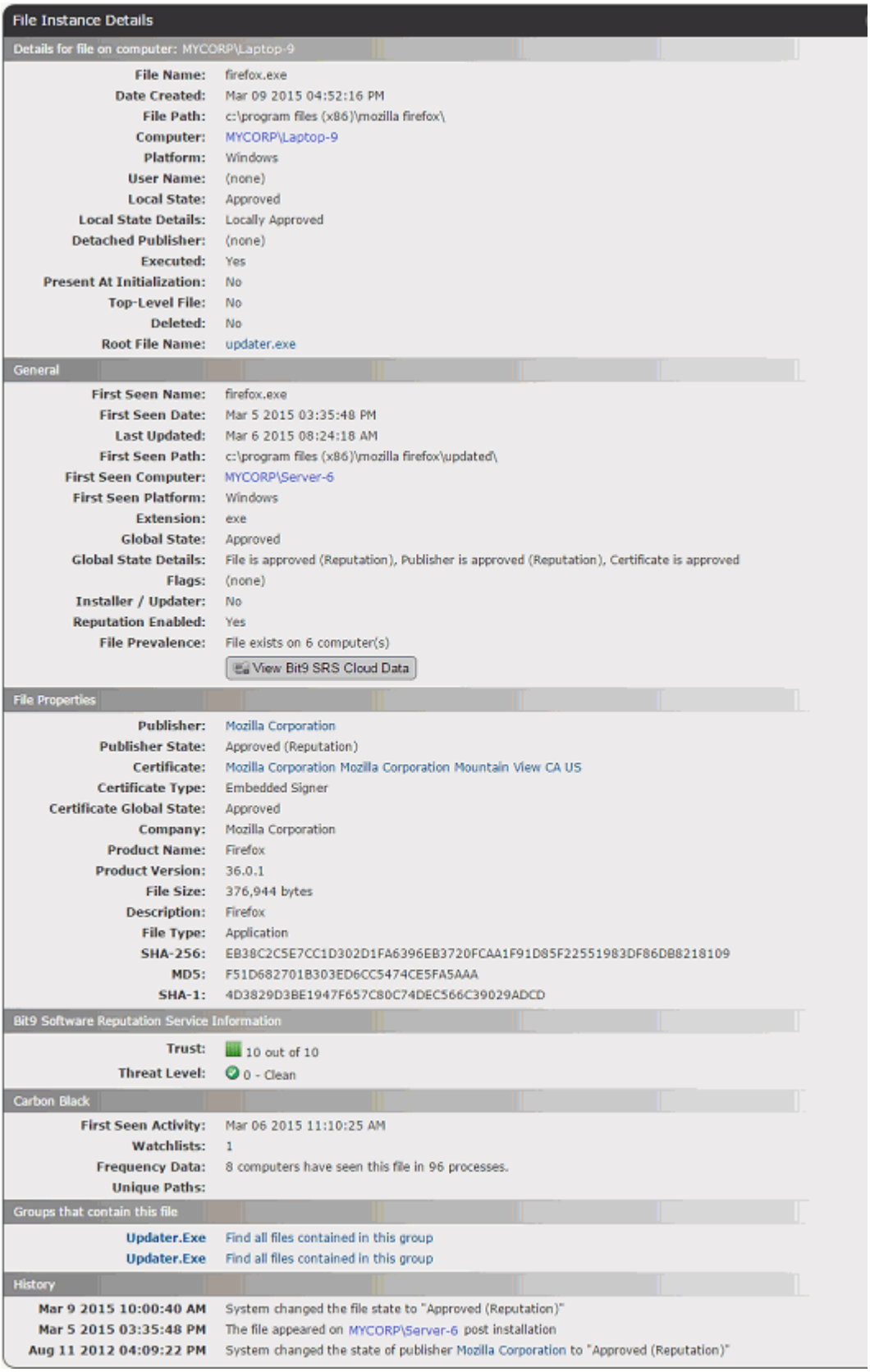
フィールド	説明
[External Analysis Results（外部分析結果）] パネル	
< 製品名 >	Bit9 Connector を使用して、Bit9 Platform と、サポートされているネットワーク セキュリティ デバイスまたはサービスを統合し、そのソースからの通知と Bit9 ファイル カタログを関連付けた場合、ファイルが、サードパーティ ソースからの悪意のある通知または危険な可能性がある通知と一致すると、その結果がこのパネルに表示されます。使用できるオプションを次に示します。 • Check Point • FireEye • Microsoft SCEP • Palo Alto Networks WildFire
[Group Information（グループ情報）] パネル	
< グループ名 >	ファイルがグループのルートの場合は、グループ名（通常はファイル名）とそのグループ内にあるファイル数を示します。ファイルをダウンロードするブラウザーなどのツールが、グループのルートとして表示される場合もあります。こうしたファイルは、他の方法でツールに関連付けられていなくても、グループ メンバーとして表示される場合があります。
[Groups that contain this file（このファイルが含まれるグループ）] パネル	
< グループ名 >	ファイルがグループに関連付けられている場合、このパネルには、そのファイルが関連付けられているグループと、そのグループのルート ファイル（わかっている場合）が表示されます。ファイルの中には、複数のルート ファイルによってインストールされるもの（または他のファイルのコピー）である場合があります。こうしたファイルの場合は、複数のグループがここに表示されます。 表示される各グループに［Find all files contained in this group（このグループに含まれるすべてのファイルを検索）］リンクがあり、このリンクをクリックすると、［File Group Details（ファイル グループの詳細）］ページが開き、結果が表示されます。
[History（履歴）] パネル	
< 日時 >	初期化中または初期化後の検出中、最初に確認されたコンピューターでファイルが特定されたかどうかを示します。 また、ファイルに適用されている承認または禁止も示します。 初期化「後」に検出されたファイルは、承認または禁止されるまで未承認ファイルとして追跡され、［Files（ファイル）］ページの［File Catalog（ファイル カタログ）］タブにある［New Unapproved（新しい未承認）］ビューで確認できます。

フィールド	説明
[File Catalog（ファイル カタログ）] テーブルのみのフィールド	
Acknowledged（確認済み）	コンソール ユーザーがこのファイルを確認したかどうかを示します（[Yes（はい）] または [No（いいえ）]）。ファイルの確認には、[File Catalog（ファイル カタログ）] タブの [Action（アクション）] メニューを使用できます。これは、既知のファイルと新しいファイルを区別するときに役立ちます。ファイルを確認すると、そのファイルは [New Unapproved Files（新しい未承認ファイル）] ビューから削除されますが、その状態は変更されません。
Approved by Reputation（レピュテーションに基づいて承認済み）	ファイルが独自のレピュテーションまたは公開者のレピュテーションのいずれかによって承認されたかどうかを示します（[Yes（はい）] または [No（いいえ）]）。
CL Version（CL バージョン）	個別のファイルについては、このファイルの現在のグローバル状態が定義された構成リストの番号。この CL バージョン以降のエージェントに、ファイルの正しいグローバル状態が指定されています。
File Size（ファイル サイズ）	各ファイルのサイズ（バイト単位）が表示されます。
File State（ファイルの状態）	ファイル ハッシュの承認 / 禁止状態（[Unapproved（未承認）]、[Approved（承認）]、[Banned（禁止）]、[Approved By Policy（ポリシーにより承認）]、または [Banned By Policy（ポリシーにより禁止）]）。ファイルのグローバル状態は、ファイルの状態と公開者の状態を組み合わせたものです。 ファイルの状態を変更するには、[Files（ファイル）] ページにある任意のテーブルの [Action（アクション）] メニュー、またはファイルの詳細ページのいずれかを使用します。詳細ページでは、既存の承認または禁止を編集できます。
File State Reason（ファイルの状態の理由）	承認済みファイルまたは禁止ファイルのハッシュについては、その状態が指定された方法。値は、[Manual（手動）]、[Trusted Directory（信頼済みディレクトリ）]、[Reputation（レピュテーション）]、[Imported（インポート）]、[External（API）（外部（API））]、[Unknown（不明）] のいずれかになります。
Initialized（初期化済み）	エージェントの初期化中にこのファイルが存在したかどうかを示します（[Yes（はい）] または [No（いいえ）]）。
Installed Program（インストール済みプログラム）	このファイルが関連付けられているインストール済みプログラム（存在する場合）の完全なパッケージまたはアプリケーションの名前。 **プラットフォームに関する注意**：インストール済みプログラムとして特定されるのは Windows ファイルだけです。

フィールド	説明
Marked as Installer（インストーラーとしてマーク済み）	Bit9 によってインストーラーとして特定されていないファイルが、コンソール ユーザーによってインストーラーとしてマークされているかどうかを示します。 [**Yes**（はい）] – ユーザーによってファイルがインストーラーとしてマークされました。 [**No**（いいえ）] – ユーザーによってファイルがインストーラーとしてマークされませんでした（ただし、Bit9 によってインストーラーとして特定されている可能性があります）。
Publisher or Company（公開者または会社）	ファイルの公開者（表示可能な場合）または会社（表示可能で、公開者情報がない場合）。
Trusted Package（信頼済みパッケージ）	このファイルのパッケージが信頼できるかどうかを示します（[Yes（はい）] または [No（いいえ）]）。信頼済みパッケージは、信頼済みディレクトリに配置されている共通のソースまたはインストーラーです。 **プラットフォームに関する注意**：信頼済みパッケージに含めることができるのは Windows ファイルだけです。

[File Instance Details（ファイル インスタンスの詳細）] ページ

[File Instance Details（ファイル インスタンスの詳細）] ページには、コンピューター上のファイル インスタンスに関する情報と、[File Details（ファイルの詳細）] ページのグローバル ファイル情報の一部が表示されます。ファイル インスタンスが表示されるテーブル、たとえば [Files on Computers（コンピューター上のファイル）] ページや [Find File Results（ファイル検索の結果）] で [View Details（詳細の表示）]（鉛筆）ボタンをクリックすると、[File Details（ファイルの詳細）] ページが開きます。



File Instance Details

Details for file on computer: MYCORP\Laptop-9

File Name:	firefox.exe
Date Created:	Mar 09 2015 04:52:16 PM
File Path:	c:\program files (x86)\mozilla firefox\
Computer:	MYCORP\Laptop-9
Platform:	Windows
User Name:	(none)
Local State:	Approved
Local State Details:	Locally Approved
Detached Publisher:	(none)
Executed:	Yes
Present At Initialization:	No
Top-Level File:	No
Deleted:	No
Root File Name:	updater.exe

General

First Seen Name:	firefox.exe
First Seen Date:	Mar 5 2015 03:35:48 PM
Last Updated:	Mar 6 2015 08:24:18 AM
First Seen Path:	c:\program files (x86)\mozilla firefox\updated\
First Seen Computer:	MYCORP\Server-6
First Seen Platform:	Windows
Extension:	exe
Global State:	Approved
Global State Details:	File is approved (Reputation), Publisher is approved (Reputation), Certificate is approved
Flags:	(none)
Installer / Updater:	No
Reputation Enabled:	Yes
File Prevalence:	File exists on 6 computer(s)
	View Bit9 SRS Cloud Data

File Properties

Publisher:	Mozilla Corporation
Publisher State:	Approved (Reputation)
Certificate:	Mozilla Corporation Mozilla Corporation Mountain View CA US
Certificate Type:	Embedded Signer
Certificate Global State:	Approved
Company:	Mozilla Corporation
Product Name:	Firefox
Product Version:	36.0.1
File Size:	376,944 bytes
Description:	Firefox
File Type:	Application
SHA-256:	EB38C2C5E7CC1D302D1FA6396EB3720FCAA1F91D85F22551983DF86DB8218109
MD5:	F51D682701B303ED6CC5474CE5FA5AAA
SHA-1:	4D3829D3BE1947F657C80C74DEC566C39029ADCD

Bit9 Software Reputation Service Information

Trust:	10 out of 10
Threat Level:	0 - Clean

Carbon Black

First Seen Activity:	Mar 06 2015 11:10:25 AM
Watchlists:	1
Frequency Data:	8 computers have seen this file in 96 processes.
Unique Paths:	

Groups that contain this file

Updater.Exe	Find all files contained in this group
Updater.Exe	Find all files contained in this group

History

Mar 9 2015 10:00:40 AM	System changed the file state to "Approved (Reputation)"
Mar 5 2015 03:35:48 PM	The file appeared on MYCORP\Server-6 post installation
Aug 11 2012 04:09:22 PM	System changed the state of publisher Mozilla Corporation to "Approved (Reputation)"

［File Instance Details（ファイル インスタンスの詳細）］フィールドの多くが［File Details（ファイルの詳細）］ページのフィールド（表 25）と同じで、同じアクションの多くを［File Instance Details（ファイル インスタンスの詳細）］ページで実行できます。表 26 は、［File Instance Details（ファイル インスタンスの詳細）］ページと［Files on Computers（コンピューター上のファイル）］テーブルで使用できる追加フィールドを示しています。詳細ページでは、これらのフィールドは上部の［**Details for file on computer**: *<computername>*（コンピューター上のファイルの詳細：< コンピューター名 >）］パネルに表示されます。

表 26：追加のフィールド：［File Instance Details（ファイル インスタンスの詳細）］と［Files on Computers（コンピューター上のファイル）］

フィールド	説明
［File Instance Details: File on Computers（ファイル インスタンスの詳細：コンピューター上のファイル）］パネル	
File Name（ファイル名）	このインスタンスのファイル名。
Date Created（作成日）	このインスタンスが現在の場所に作成された正確な日時。表示形式は、MM DD YYYY hh:mm:ss(AM/PM) です。
File Path（ファイル パス）	このファイル インスタンスのパス。
Computer（コンピューター）	このインスタンスがあるコンピューターの名前。
Platform（プラットフォーム）	インスタンスがあるシステムのプラットフォーム（Windows、Mac）。
User Name（ユーザー名）	このファイルが作成されたときにログインしていたユーザーの名前。
Local State（ローカル状態）	ファイル インスタンスのローカル状態（［Unapproved（未承認）］、［Approved（承認）］、［Banned（禁止）］、［Deleted（削除済み）］）。 ローカル状態が「未承認」の場合は、［Actions（アクション）］メニューで［**Approve Locally**（ローカルで承認）］を選択できます。「承認」の場合は、**ローカル承認を削除**することができます。「禁止」の場合、変更することはできません。
Local State Details（ローカル状態の詳細）	Bit9 サポート エンジニアが使用するファイル状態のメタデータ。必要に応じて、この情報の提供をサポート担当者から求められる場合があります。詳細については、表 32 を参照してください。

フィールド	説明
Detached Publisher（デタッチされた公開者）	このファイルに独自の証明書がなく、「デタッチされた証明書」によって間接的に署名された場合に、このフィールドが表示され、公開者の名前が示されます。一部の公開者は、更新を、未署名のファイルのコレクションを「カタログ」と共に配布します。このカタログには、間接的に署名されたファイルすべてのハッシュが含まれており、カタログ自体も署名されています。Bit9 はこのカタログを使用して公開者を確認し、この方法で署名されたファイルの、公開者ベース承認を許可することができます。
Detached Publisher State（デタッチされた公開者の状態）	（デタッチされた公開者がある場合）このオプションは［Publisher State（公開者の状態）］と同じで、［Approved（承認）］、［Approved By Policy（ポリシーにより承認）］、［Banned（禁止）］、［Banned By Policy（ポリシーにより禁止）］、［Unapproved（未承認）］のいずれかの値になります。
Executed（実行）	このファイル インスタンスが実行されたことがあるかどうかを示します。
Present at Initialization（初期化時に存在）	Bit9 エージェントがインストールされたときに、このファイル インスタンスが、コンピューターに存在していたファイルの 1 つであったかどうか、または、インストール後に現れたかどうかを示します。
Top-Level File（最上位レベル ファイル）	ファイルが最上位レベル ファイル（他のファイルによってインストールされたり、他のファイルからコピーされたりしたものではないファイル）かどうかを示します。 **プラットフォームに関する注意**：Windows システムでは、初期化中に検出されたファイルに、後で、つまりそのファイルがインストーラーであることがわかった時点で最上位レベル ステータスを適用できます。
Deleted（削除済み）	このファイル インスタンスが存在していたコンピューターからそのインスタンスが削除されたかどうかを示します。これはファイル削除の直後から、そのファイルがこの Bit9 Server のデータベースから削除されるまでの間の一時的な状態です。
Root File Name（ルート ファイル名）	現在のファイルを作成したファイル。最上位レベル ファイルの場合は、ルート ファイルがないため、名前は「(none)（(なし)）」になります。
［File on Computer（コンピューター上のファイル）］テーブルのみのフィールド	
Computer tag（コンピューター タグ）	該当ファイルが存在するコンピューターについては、オプションのコンピューター タグが表示されます（指定されている場合）。
IP Address（IP アドレス）	ファイルが存在するコンピューターの IP アドレス。
Operating System（オペレーティング システム）	ファイルが存在するコンピューターのオペレーティング システム。
Policy（ポリシー）	ファイルが存在するコンピューターの Bit9 セキュリティ ポリシー。

ファイル ページのメニュー

[File Details（ファイルの詳細）] ページのメニュー

[File Details（ファイルの詳細）] ページには、ファイル情報の右側に [Related Views（関連ビュー）]、[Actions（アクション）]、[Advanced（詳細）] という 3 つのメニューがあります。[File Catalog（ファイル カタログ）] タブおよび [Files on Computers（コンピューター上のファイル）] タブのテーブルの左上に [Action（アクション）] メニューがあります。表 27、「ファイル テーブルおよび詳細ページのメニュー」は、ファイル ページのメニューで使用できるオプションを示しています。オプションの中には、一部のファイル状態でしか使用できないものがあることに注意してください。

[File Instance Details（ファイル インスタンスの詳細）] ページのメニュー

[File Instance Details（ファイル インスタンスの詳細）] ページには、ファイル情報の右側に [Related Views（関連ビュー）]、[Actions（アクション）]、[Advanced（詳細）] という 3 つのメニューがあります。[File Details（ファイルの詳細）] ページのメニューと似ていますが、ローカル承認のオプションが含まれている点が異なります。表 27、「ファイル テーブルおよび詳細ページのメニュー」は、ファイル ページ メニューで使用できるオプションを示しています。

注意

- メニューのオプションの中には、一部のファイル状態でしか使用できないものがあることに注意してください。
- ビューにファイル関連のイベントが含まれるときは、このコマンドの多くを、[Events（イベント）] ページの [Action（アクション）] メニューでも使用できます。

表 27：ファイル テーブルおよび詳細ページのメニュー

メニュー オプション	File Catalog（ファイル カタログ）	Files on Computers（コンピューター上のファイル）	File Details（ファイルの詳細）	File Instance Details（ファイル インスタンスの詳細）
[Related Views（関連ビュー）] メニュー				
All File Instances（すべてのファイル インスタンス）			X	X
File Events（ファイル イベント）			X	X
Carbon Black Details（Carbon Black の詳細）			X	X
Computers with this file（このファイルが存在するコンピューター）			X	X
Computers without this file（このファイルが存在しないコンピューター）			X	X
[Actions（アクション）] メニュー				
Approve Locally（ローカルで承認）		X	X	X
Remove Local Approval（ローカル承認を削除）		X		X
Approve Globally（グローバルに承認）	X	X	X	X
Ban Globally（グローバルに禁止）	X	X	X	X
Approve by Policy（ポリシーにより承認）	X	X	X	X
Ban by Policy（ポリシーにより禁止）	X	X	X	X
Edit Global Approval/Ban（グローバル承認 / 禁止を編集） **Edit Approval/Ban by Policy（ポリシーによる承認 / 禁止を編集）**			X	X
Remove Approval or Ban（承認または禁止を削除）	X	X	X	X
Acknowledge（確認）	X			

メニュー オプション	File Catalog（ファイル カタログ）	Files on Computers（コンピューター上のファイル）	File Details（ファイルの詳細）	File Instance Details（ファイル インスタンスの詳細）
Find computers with at least one of the selected files（選択したファイルの少なくとも 1 つが存在するコンピューターを検索）			X	X
Find computers with all of the selected files（選択したファイルすべてが存在するコンピューターを検索）			X	X
Find computers missing at least one of the selected files（選択したファイルの少なくとも 1 つが存在しないコンピューターを検索）			X	X
Find computers missing all of the selected files（選択したファイルすべてが存在しないコンピューターを検索）			X	X
Add/Edit Meter（メーターを追加 / 編集）			X	X
Add/Edit Alert（アラートを追加 / 編集）			X	X
［Advanced（詳細）］メニュー				
View Bit9 SRS Data（Bit9 SRS データの表示）	X	X	X	X
Enable/Disable Reputation for this File（このファイルのレピュテーションを有効化 / 無効化）			X	X
Mark as Installer/Not Installer（インストーラー / インストーラー以外としてマーク）			X	X
［External Pages（外部ページ）］メニュー				
File Analytics（ファイル分析）			X	X

ファイル ビューの概要

前のセクションでは、Bit9 コンソールにおけるファイル情報のメイン ビューについて詳しく説明しました。表 28 では、この情報が示されているビューにアクセスする方法を簡単に説明します。

表 28：Bit9 コンソールのファイル ビューとファイルの詳細

表示される内容	手順
Bit9 Server で管理されているコンピューターで検出された、一意の「最上位レベル」ファイル（他のファイルによってインストールされていないファイル）すべてが表示されるテーブル。	[**Assets**（アセット）] > [**Files**（ファイル）] に移動し、[**File Catalog**（ファイル カタログ）] タブをクリックして、[Show individual files（個別のファイルを表示）] ボックスがオンになっていないことを確認します。
	注意：最上位レベル ファイルは、インストーラーに関連付けられていない、またはインストーラーが不明なファイルです。最上位レベル ファイルがインストーラーの場合、その名前は、その関連ファイルへのリンクとしてハイライト表示されます。
Bit9 Server で管理されているコンピューターで検出された、一意の個別のファイルすべてが表示されるテーブル。	[**File Catalog**（ファイル カタログ）] タブをクリックし、[Show individual files（個別のファイルを表示）] ボックスをオンにします。
	注意：このビューには、他のファイルによってインストールされたファイルと、最上位レベルのファイルの両方が表示されます。既知のインストーラーの名前はハイライト表示されます。 **重要**：Bit9 Server によって膨大な数の一意のファイルが検出されることがあります。処理能力の低いサーバーを使用している場合、このビューにより、パフォーマンスの問題が発生する可能性があります。
一意のファイルのグローバル ファイルの詳細。	[**File Catalog**（ファイル カタログ）] タブをクリックし、詳細を表示するファイルの横にある [View Details（詳細の表示）] ボタンをクリックします。

表示される内容	手順
最上位レベル ファイルに関連付けられている（通常は、そのファイルによってインストールされている）、Bit9 Server で管理されているすべてのコンピューターのファイルすべてが表示されるテーブル。	[**File Catalog**（ファイル カタログ）] タブをクリックし、[Show individual files（個別のファイルを表示）] ボックスがオンになっていないことを確認して、関連ファイルのリストを表示するファイルの名前をクリックします。
	注意：これは関連ファイルのリストです。特定のコンピューターで確認されたインストールには限定されません。たとえば、インストーラー X がファイル A と B をあるコンピューターにインストールし、ファイル B と C を別にコンピューターにインストールしていることが確認された場合、インストールされたすべてのファイル（A、B、および C）が、インストーラー X の [File Group Details（ファイル グループの詳細）] ページに表示されます。 テーブルのファイルの詳細については、そのファイルの横にある [View Details（詳細の表示）] ボタンをクリックします。 **プラットフォームに関する注意**: この Bit9 リリースでは、インストーラーごとにグループ化されるのは Windows コンピューターのファイルだけです。
Bit9 Server で管理されているすべてのコンピューター上の、(他のファイルによってインストールされていない）「最上位レベル」ファイル インスタンスすべてが表示されるテーブル。	[**Files on Computers**（コンピューター上のファイル）] タブをクリックし、[Show individual files（個別のファイルを表示）] ボックスがオンになっていないことを確認します。
	注意：最上位レベル ファイルは、インストーラーに関連付けられていない、またはインストーラーが不明なファイルです。最上位レベル ファイルがインストーラーの場合、その名前は、その関連ファイルへのリンクとしてハイライト表示されます。 このテーブル ビューにも、エージェントごとに [<Initialization files（初期化ファイル）>] という名前のエントリがあります。これは、エージェントがインストールされたときにコンピューターで見つかったファイルのグループです。
エージェントが最初にインストールされるとき、または無効なエージェントが再度有効になるときに行われる「初期化」時に、コンピューターで見つかったファイル インスタンスすべてが表示されるテーブル。	[**Files on Computers**（コンピューター上のファイル）] タブをクリックし、[Show individual files（個別のファイルを表示）] ボックスがオンになっていないことを確認します。次に、対象のコンピューターの名前が含まれる行の [<Initialized files（初期化ファイル）>] をクリックします。

表示される内容	手順
Bit9 Serverで管理されているすべてのコンピューター上の、個別のファイル インスタンス「すべて」が表示されるテーブル。	[**Files on Computers**（コンピューター上のファイル）] タブをクリックし、[Show individual files（個別のファイルを表示）] ボックスをオンにします。
	注意：このビューには、エージェント管理コンピューター上の最上位レベル ファイルと、その最上位レベル ファイルによってインストールされた「個別」ファイルの両方が表示されます。エージェントの分析によってコンテンツが確認された最上位レベル ファイルは、ハイライト表示されたリンクとして表示されます。 **重要**：このボックスは、特にエージェント管理コンピューターの数が多いときは、不必要にオンにしないでください。個別のファイルの合計数は、数千万から数億にのぼる可能性があります。これだけ多くのファイルが含まれるリストをロードしようとすると、Bit9 Server がタイムアウトする可能性があります。
1 台のコンピューター上にある 1 つのファイル インスタンスの詳細。	[**Files on Computers**（コンピューター上のファイル）] タブをクリックし、詳細を表示するファイル インスタンスの横にある［View Details（詳細の表示）］ボタンをクリックします。
	注意：[File Instance Details（ファイル インスタンスの詳細）] ページが開きます。 このインスタンスのローカル状態とその他の情報、およびファイルのグローバルな詳細情報の両方が表示されます。 最上位レベル ファイルは、存在しなくなっている場合でも、引き続き［Files on Computers（コンピューター上のファイル）］テーブルに表示されることがあります。コンピューター上に存在しない削除されたファイルの［View Details（詳細の表示）］をクリックすると、グローバルな詳細情報のみが表示されます。
1 つの最上位レベル ファイルに関連付けられている、1 台のコンピューター上のファイルすべてが表示されるテーブル。	[**Files on Computers**（コンピューター上のファイル）] タブをクリックし、関連ファイルのリストを表示するハイライト表示された最上位レベルのファイル インスタンスの名前をクリックします。
	注意：名前がクリックされたファイルに関連付けられている、「指定されたコンピューター」行のファイルすべてを対象にしたファイルの検索結果が表示されます。 テーブルのファイルの詳細については、そのファイルの横にある［View Details（詳細の表示）］ボタンをクリックします。

ファイルのグローバル状態

［Files（ファイル）］ページの［File Catalog（ファイル カタログ）］タブに表示されるファイルの状態を次に示します。

- ［**File State**（ファイルの状態）］– ファイル自体の承認または禁止状態です。
- ［**Publisher State**（公開者の状態）］– ファイルの公開者の状態です（わかっている場合）。値は、［Approved（承認）］、［Approved By Policy（ポリシーにより承認）］、［Unapproved（未承認）］のいずれかのみです。
- ［**Global State**（グローバル状態）］– ファイルの状態と公開者の状態を組み合わせて、エージェント管理コンピューターにおけるファイルの処理方法を特定します。ファイルの状態とグローバル状態は、次の両方が該当する場合を除いて同じになります。
  - 公開者の状態が未承認でない。
  - ファイルの状態が、公開者と同じポリシーで承認または禁止ではない。

グローバル状態を直接変更することはできません。表 29 は、グローバル状態の一覧を示しています。

表 29：Bit9 Server によってカタログ登録されている（ファイルの）グローバル状態

状態	説明
承認	すべてのコンピューターでの実行が許可されています。
禁止	ハッシュによって禁止されており、制御モードで実行されているコンピューターでの実行は許可されません。
ポリシーにより承認	1 つ以上のポリシーによりコンピューターでの実行が許可されています。
ポリシーにより禁止	（制御モードの場合）1 つ以上のポリシーによりコンピューターでの実行がハッシュによって禁止されています。
未承認	（グローバルおよびポリシーによって）承認も禁止もされていません。未承認ファイルの実行は、その実行が試みられたコンピューターのポリシーの適用レベルに基づいてブロックまたは許可されます。
混在	あるポリシーでファイルの状態が「禁止」で、別のポリシーまたはすべてのポリシーで公開者の状態が「承認」になっているため、有効な状態がポリシーによって異なります。

フラグ

グローバル状態は、ファイル カタログの一意のファイルそれぞれに対する有効な Bit9 の分類で、ファイルの状態と、ファイルに対する公開者の状態を組み合わせたものです。「フラグ」は、主に、Bit9 テクニカル サポートによって使用されますが、ファイルが Bit9 環境でどのようにラベル付けまたは処理されているかを判断するうえで役に立つことがあります。

表 30：ファイルのフラグ

フラグ	説明
レポートのみの禁止	Bit9 コンソール ユーザーによってファイルが特定されたため、ファイル実行の試みが禁止されているかのようにレポートされますが、ファイルの実行はブロックされません。
インストーラー	Bit9 によってファイルがインストーラーとして特定され、実行が許可されています。そのファイルによって作成された実行可能ファイルはローカルで承認されます。 **プラットフォームに関する注意**：この Bit9 リリースの場合、Mac コンピューターでは、ネイティブ Mac アップデーターに関連付けられているファイル（.pkg ファイル）のみがインストーラーとして特定されます。
インストーラー（無効化）	ファイルが Bit9 によってインストーラー「以外」として特定されましたが、Bit9 コンソール ユーザーがそのファイルを「インストーラー」に変更しました。実行が許可されている場合は、そのファイルによって作成された実行可能ファイルがローカルで承認されます。
インストーラー以外（無効化）	ファイルが Bit9 によって「インストーラー」として特定されましたが、Bit9 コンソール アカウント ユーザーがそのインストーラー ステータスを「インストーラー以外」に変更しました。

ファイルのローカル状態

グローバルに禁止または承認されたファイルでは、ローカル状態とグローバル状態が同じになります。グローバル状態が未承認のファイルの場合は、ローカル状態が異なることがあります。特に、グローバルに禁止されていないファイルは、さまざまな方法でローカルで承認することができます。ファイルのローカル状態は、［Files（ファイル）］ページの［Files on Computers（コンピューター上のファイル）］タブで確認できます。

表 31：ローカル状態

状態	説明
承認	このファイル インスタンスは実行が許可されています。ローカル承認は、ポリシーのすべてのコンピューターまたは Bit9 Server によって管理されているすべてのコンピューターに対して、名前またはハッシュによって行われます。また、グローバルな承認方法、適用レベルの変更のほか、この 1 つのファイル インスタンスの明示的なローカル承認によって行われることもあります。ローカルで承認されたファイルの「グローバル状態」は「未承認」または「承認」で、「禁止」にはなりません。

状態	説明
禁止	このファイル インスタンスは実行が禁止されています。ローカル状態が「禁止」のファイルは、特定のポリシーのすべてのコンピューター、またはBit9 Serverで管理されているすべてのコンピューターで禁止されている可能性があります。名前によってファイルを禁止しても、そのローカル状態は変更されないことに注意してください。
未承認	このファイル インスタンスは承認も禁止もされていません。そのファイル インスタンスの実行は、そのインスタンスがあるコンピューターの適用レベルに基づいてブロックまたは許可されます。
削除済み	このファイルのインスタンスは削除されていますが、レコードがこのBit9 Server のデータベースにまだ存在します。

ローカル状態の詳細

ローカル状態は、特定のコンピューターにおける特定のファイル インスタンスに対して使用される Bit9 の分類です。この情報は、主に、Bit9 テクニカル サポートによって使用されますが、ファイルに最上位レベルのローカル状態が割り当てられた理由を判断するうえで役に立つことがあります。

表 32：ローカル（ファイル）状態の詳細

状態	説明
承認	[File Catalog（ファイル カタログ）] でグローバルに承認されたファイルの、ローカル コンピューター上の承認状態。
承認（非永続的）	バージョン 6.0 以前の方法で承認されたが、[File Catalog（ファイル カタログ）] でグローバルに承認されていないファイルの、ローカル コンピューター上の承認状態。この状態のファイルを削除しても、新しいインスタンスがローカルで承認されるとは限りません。
インストーラーとして承認	最上位レベル インストーラーの承認状態（Windows の場合）。インストーラーとそのインストーラーに含まれるファイルが、ハッシュ化、分析、および Bit9 によってグローバルに承認されていることを示します。これらのファイルは、ユーザーが実行すると、グローバルに承認されたファイルとして実行が Bit9 エージェントによって許可されます。この状態は一般的ではなく、インストーラーによって生成されたファイルのローカル承認には不要です。
インストーラーとして承認（最上位レベル）	最上位レベル インストーラーの承認状態。インストーラーはグローバルに承認され、実行すると、インストーラーによって生成されたファイルはローカルで承認されます。 **プラットフォームに関する注意**：この Bit9 リリースの場合、Mac コンピューターでは、ネイティブ Mac アップデーターに関連付けられているファイル（.pkg ファイル）のみがインストーラーとして特定されます。

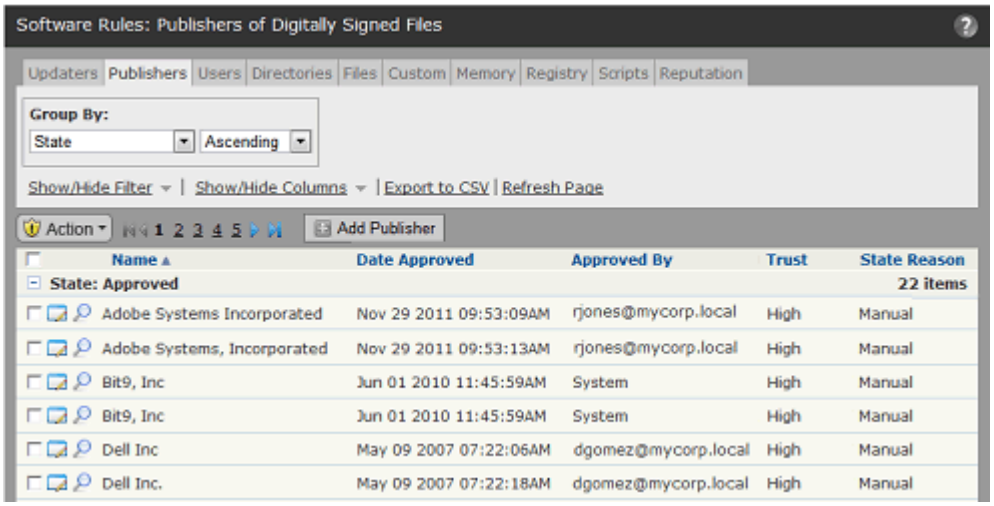
状態	説明
禁止	指定したハッシュに一致するファイルの実行が、すべてのコンピューターまたはポリシーによって指定されたコンピューターで許可されていません。
禁止（レポートのみ）	ハッシュによって禁止されるファイルのテスト ファイル状態。レポートのみの禁止状態のファイルは、実行が許可されますが、「ブロックしていたはず」というメッセージがイベント ログに記録され、禁止がアクティブだった場合にファイルがどのように処理されたはずかを示します。
ローカルで承認	ファイルは、ローカル コンピューターでの実行が承認されていますが、[File Catalog（ファイル カタログ）] では（グローバルまたは現在のポリシーに対して）承認されていません。ローカルで承認されているファイルは 1 台のコンピューターにインストールできます。その際に、Bit9 エージェントが実行されている他のコンピューターに対して承認する必要はありません。
ローカルで承認（自動）	信頼済みインストーラーまたはアップデーターによって作成されたファイルであるため、ローカル コンピューターでの実行が承認されています。承認のソース以外は、「ローカルで承認」と同じです。
未承認	エージェントの初期化後に現れたファイルで、承認されていません。ファイルは、各コンピューターの適用レベルに応じてブロックされるか、実行が許可されます。こうしたファイルは、コンピューターの適用レベルが、ポリシー設定に応じて「低」（または「なし」）から「中」または「高」に変更された場合に、ローカルで承認されることがあります。適用レベルが「低（未承認を監視）」または「なし（可視性のみ）」のときに、最初のローカル インスタンスが見つかると、ファイルには未承認のローカル状態の詳細が割り当てられます。この動作の詳細については、「適用レベル変更時の自動ローカル承認」（309 ページ）を参照してください。
未承認（永続的）	エージェントの初期化後に現れたファイルで、承認されていません。未承認（永続的）ファイルは、コンピューターの適用レベルが「低」または「なし（可視性）」から「高」または「中」に変更されてもローカルで承認されません。コンピューターの適用レベルが「高」または「中」のときに、最初のローカル インスタンスが見つかると、ファイルには未承認（永続的）のローカル状態の詳細が割り当てられます。

公開者情報

[Software Rules（ソフトウェア ルール）] ページの [Publishers（公開者）] タブには、組織の Bit9 エージェントが実行されているコンピューターで検出されたファイル公開者が表示されます。また、Bit9 Server のファイル カタログに手動で追加された公開者もすべて表示されます。このページには [Action（アクション）] メニューがあり、公開者を承認または禁止したり、承認または禁止を削除したり、公開者を確認することでその公開者が確認済みであることを示したりできます。こうしたアクションについては、「公開者による承認または禁止」（288 ページ）を参照してください。

検出または追加された公開者のリストを表示する手順：

1. コンソール メニューで、[**Rules**（ルール）] > [**Software Rules**（ソフトウェア ルール）] の順に選択します。[Software Rules（ソフトウェア ルール）] ページが表示されます。
2. [**Publishers**（公開者）] タブをクリックします。[Publishers（公開者）] テーブルには、サーバーにレポートするエージェント管理コンピューターにインストールされている署名済みソフトウェアのすべての公開者と、証明書を使用して手動で追加したすべての公開者が表示されます。



[Publishers（公開者）] テーブルに表示されている公開者の [Publishers Details（公開者の詳細）] ページを表示するには、その公開者の名前の横にある [View Details（詳細の表示）]（鉛筆とファイル）ボタンをクリックします。[Publisher Details（公開者の詳細）] ページには、詳細オプション（表 33 を参照）のほか、公開者を承認する、または承認を削除するためのショートカットもあります。[Related Views（関連ビュー）] メニューには、公開者のすべてのファイルを表示するコマンドと、この公開者の承認状態が最新になっているコンピューターを表示するコマンドもあります。

1 つの公開者の詳細を表示する手順：

1. コンソール メニューで、[**Rules**（ルール）] > [**Software Rules**（ソフトウェア ルール）] の順に選択します。[Software Rules（ソフトウェア ルール）] ページが表示されます。
2. [**Publishers**（公開者）] タブをクリックします。[Publishers（公開者）] テーブルには、ネットワーク上のエージェント管理コンピューターにインストールされている署名済みソフトウェアのすべての公開者が表示されます。
3. 公開者のテーブルから、アクセス許可を与える公開者を見つけ、[View Details（詳細の表示）] ボタン（鉛筆とファイル）をクリックします。[Publisher Details（公開者の詳細）] ページが開きます。

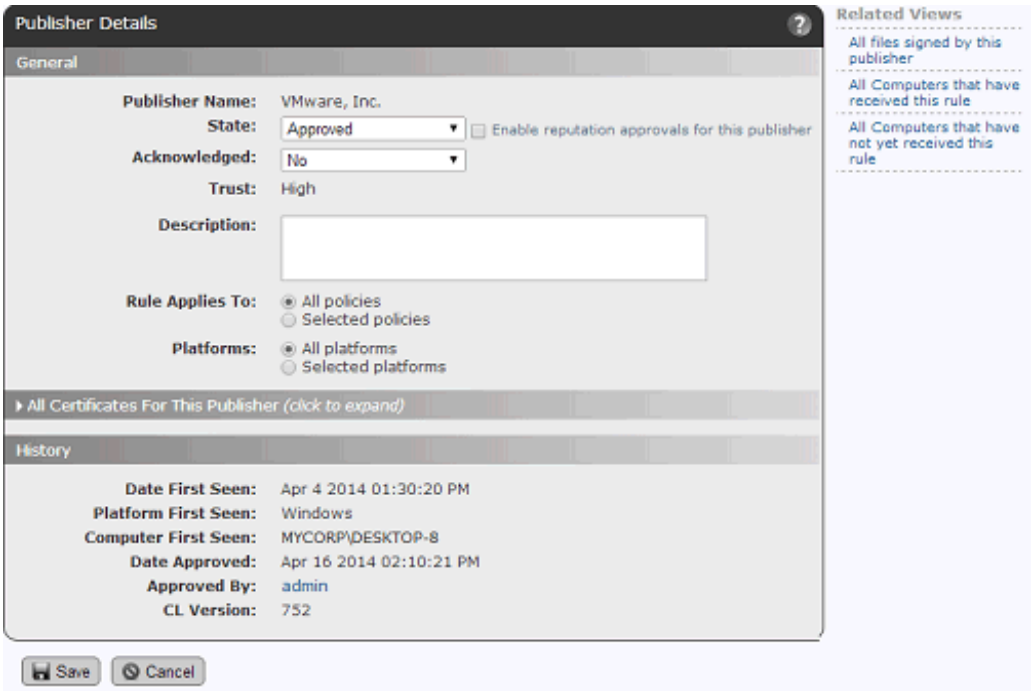


表 33：公開者の詳細

フィールド	説明
[General（全般）] パネル	
Publisher Name（公開者名）	証明書に表示されている、この公開者の名前。
State（状態）	[Approved（承認）]、[Unapproved（未承認）]、[Banned（禁止）] のいずれかです。
Enable reputation approvals…（… レピュテーション承認の有効化）	このチェックボックスは、レピュテーション承認を有効にした場合に表示されます。[Enable reputation approvals for this publisher（この公開者のレピュテーション承認の有効化）] はデフォルトでオンになっており、この公開者をレピュテーションで承認できます。オフにすると、この公開者のレピュテーション承認が無効になりますが、レピュテーション承認がグローバルで有効になっている場合、オフの設定が反映されるのは、変更後最初に確認されたファイルだけです。
Acknowledged（確認済み）	公開者を確認できます。これは、公開者が既に確認済みであることを示します。これは、新しい公開者と既知の公開者を区別するときに役立ちます。
Trust（信頼度）	このフィールドは、Bit9 SRS を有効にした場合に表示されます。この公開者の信頼度が表示されます。[High（高）]、[Medium（中）]、[Low（低）]、[Not Trusted（信頼できない）] のいずれかになります。

フィールド	説明
Description（説明）	この公開者とその状態のオプションの説明です。
Rule Applies To（ルールの適用先）	レピュテーション承認が有効になっていない公開者については、公開者の状態を、すべてのポリシーのコンピューターまたは一部のポリシーのコンピューターにのみ適用できます。
Approved Platforms（承認済みプラットフォーム）	公開者の状態を、すべてのプラットフォームのコンピューターを適用したり、プラットフォーム（Windows、Mac）を選択して適用したりできます。 **プラットフォームに関する注意**：公開者の承認は Windows でのみ動作します。
Date First Seen（最初に確認された日付）	サーバーにレポートするエージェント管理コンピューターで、この公開者が最初に確認された日時。
[History（履歴）] パネル	
Platform First Seen（最初に確認されたプラットフォーム）	この公開者が最初にサーバーにレポートされたコンピューターのプラットフォーム（Mac または Windows）。
Computer First Seen（最初に確認されたコンピューター）	この公開者が最初にサーバーにレポートされたコンピューター。
Date Approved（承認日）	公開者が承認されている場合は、承認が行われた日時。
Approved By（承認者）	公開者を承認した Bit9 コンソール ユーザー。レピュテーションによって承認された公開者の場合、このフィールドには「System（システム）」と表示されることがあります。
Date Acknowledged（確認日）	公開者が確認されている場合は、確認された日時。
Acknowledged by（確認者）	公開者が確認されている場合は、その公開者を確認した Bit9 コンソール ユーザー。
CL Version（CL バージョン）	現在の公開者の状態が含まれる Bit9 Platform ルールのバージョン。エージェントにルールが適用されているかどうかを判断するうえで役立ちます。

第 8 章

ソフトウェアの承認と禁止

この章では、Bit9 Security Platform を使用してソフトウェアを承認または禁止する方法について説明します。ここで提供するのは、グローバル ファイル承認とローカル ファイル承認の両方に関する情報です。ソフトウェアを承認および禁止する方法の多くは、[Software Rules（ソフトウェア ルール）] ページのタブのいずれかで確認できます。

Bit9 Security Platform では、明示的な承認および禁止のほか、カスタム ルールを定義することで、ファイル実行の許可やブロック、指定した場所での書き込み、指定したユーザーやプロセスによる書き込み（選択した場合）を行うことができます。第 12 章「カスタム ソフトウェア ルール」を参照してください。

セクション

Bit9 ソフトウェアの承認とは

ソフトウェアを承認すると、Bit9 エージェントが実行されているコンピューターのユーザーが、有効な Bit9 セキュリティ設定と適用レベルに関係なく、「既知の良好な」アプリケーションを自由にインストールして実行できます。Bit9 Security Platform には、コンピューター上のソフトウェアを承認する補足的な方法がいくつか用意されています。選択した方法に基づいて、承認されたソフトウェアのインストールを、すべてのコンピューター、選択したポリシーのコンピューター、または個別に選択したコンピューターで許可できます。

既存の設定と手順、特にサイトで既に実施されているソフトウェア配布プロセスに最も適した方法を組み合わせて選択することができます。

- アプリケーションをすべてのコンピューター（または選択したポリシーのすべてのコンピューター）で実行するために事前承認する必要がある場合は、信頼済みディレクトリを指定するか、指定した公開者を承認してそのアプリケーションのインストールを許可するか、特定のアップデーターを有効にしてアプリケーションを自動的に更新します。
- 脅威レベルが低いアプリケーションを、すべてのコンピューター（または選択したポリシーのすべてのコンピューター）で実行するために事前承認する場合は、Bit9 SRS によってレポートされた特定のファイルおよび公開者の信頼度に基づいて、レピュテーション ルールを有効にします。
- すべてのコンピューター、または選択したポリシーのすべてのコンピューターで実行できるようにする個別のファイルまたはインストーラーを検出したら、ファイル承認ルールを作成します。
- 承認するファイルのハッシュのリストがある場合は、1 回の操作でそのリスト全体に対する承認を作成できます。
- 選択した特定のコンピューターでソフトウェアのインストールを承認する必要がある場合は、インストールを実行する信頼済みユーザー（またはグループ）を指定するか、ローカル承認方法を選択します。
- 特定の場所や、特定のユーザーまたはプロセス別にファイルのインストールや実行を許可する特別なルールが必要な場合は、カスタム ルールを作成します。

ヒント

高適用レベルを除くすべての適用レベルでは、ユーザーは未承認ソフトウェアをインストールできます。必須ではありませんが、広く使用されているソフトウェアについては、低適用レベルで実行する場合でも承認（少なくとも確認）しておくことをお勧めします。承認することにより、未承認ステータスのファイル数が少なくなり、懸念されるファイルに焦点を当てることができます。たとえば、既知の良好なファイルを承認すると通常はベースライン ドリフト レポートのサイズが小さくなり、読みやすくなります。

同様に、コンピューターが可視性モードで動作している場合は、「すべて」のソフトウェアをその承認状態に関係なく実行できます。しかし、可視性モードですべてのコンピューターを実行している場合でも、既知の良好なファイルを承認して、そのファイルに関して収集されるイベント データ量を減らしたいことがあります。これは、一部またはすべてのコンピューターを、将来的に高適用レベルまたは中適用レベルに移行する可能性に備えて、準備するときにも役立ちます。

内部的な基準や手順、および必要な承認範囲（ネットワーク全体またはコンピューター固有）に基づいて、表 34 に示されているいずれかの方法でファイルを承認できます。

表 34：Bit9 ファイル承認方法

承認方法	ソフトウェアの承認対象	使用する状況
信頼済みディレクトリによる承認	すべてのコンピューター（グローバル）	安全な信頼済みサーバーが（たとえば、ソフトウェア展開用として）用意されており、そこに認証済み承認ディレクトリを作成する場合。
信頼済みユーザーまたはグループによる承認	インストール コンピューターのみ（ローカル）	無制限インストール権限を Windows ユーザー アカウントまたは Windows または AD グループのすべてのユーザーに付与する場合。信頼済みユーザーが、自身の認証情報を使用してログインしているすべてのコンピューターにインストールすることができます。
公開者による承認または禁止	インストール コンピューターのみ（ローカル）。ただし、すべてのコンピューターがオンデマンドでインストールできます	Bit9 が有効なデジタル証明書を確認できるベンダーのソフトウェアをすべて承認する場合。公開者を特定する証明書を承認または禁止することもできます。これはファイルの状態に影響します。「適用のための証明書の使用」（369 ページ）を参照してください。
公開者のレピュテーションによる承認（第 9 章「レピュテーション承認ルール」を参照）	インストール コンピューターのみ（ローカル）。ただし、どのコンピューターにでもオンデマンドでインストールできます	Bit9 Software Reputation Service (SRS) によって信頼できると見なされた、すべての公開者のソフトウェアをすべて自動的に承認する場合。
アップデーターによる承認	インストール コンピューターのみ（ローカル）。ただし、どのコンピューターにでもオンデマンドでインストールできます	指定したアプリケーション更新プログラムを通じてアプリケーションの更新がダウンロードできるようになった場合に、その更新のインストールを許可する場合。
適用レベル変更時の自動ローカル承認	インストール コンピューターのみ（ローカル）	コンピューターの適用レベルを「中」または「高」に上げるとき、「低適用以上の状態で見つかった未承認ファイル」をローカルで承認する場合。
ローカル承認モードへのコンピューターの移行	インストール コンピューターのみ（ローカル）	高適用ポリシーのコンピューターでユーザーによるソフトウェアのインストールを許可する場合。このモードでユーザーが未承認ファイルをインストールすると、ローカル承認が行われます。

承認方法	ソフトウェアの承認対象	使用する状況
コンピューター上にあるすべての未承認ファイルのローカル承認	インストール コンピューターのみ（ローカル）	特定のコンピューターに存在するすべての未承認ファイルをローカルで承認する場合。
個別のファイルのローカル承認	インストール コンピューターのみ（ローカル）	コンピューター上の特定のファイルを選択してローカルで承認する場合。ファイルをローカルで承認するか、ローカル承認を削除できます。
ファイル承認ルール	すべてのコンピューター、または選択したポリシーのコンピューターに対して承認	任意のコンピューターで既知の良好なアプリケーションを確実に実行し、ハッシュによって承認できるようにする場合。
ファイル レピュテーションによる承認（第 9 章「レピュテーション承認ルール」を参照）	すべてのコンピューター、または選択したポリシーのコンピューターに対して承認	Bit9 SRS が信頼できると見なしたすべてのソフトウェアを（ハッシュによって）自動的に承認する場合。
イベント ルールによる承認（第 16 章「イベント ルール」を参照）	ルールによって異なる	ファイルがレポート イベントに含まれるときに、そのファイルをローカルまたはグローバルに自動承認する場合。

ルールの仕様に関するプラットフォームの考慮事項

Bit9 Security Platform ルールの多くに、ファイル名やパスの仕様のほか、手動で入力するその他の情報（ユーザー名、グループ名、コンピューター名など）が含まれています。Mac コンピューターと Windows コンピューターのどちらでも、ルールのファイル名、パス、ユーザー名は、通常、大文字と小文字が区別されません。Linux コンピューターのルールのファイル名とユーザー名は、通常、大文字と小文字が区別されます。たとえば、*/temp/myfile.exe* を禁止するルールを作成した場合、このルールでは *MyFile.exe* や */TEMP/myfile.exe* はブロックされません。ルール パラメーターに対して大文字と小文字が区別されるかどうかを判断するには、さらに次の 2 つの点を考慮します。

- オペレーティング システムの大文字と小文字を区別するかどうかの一般的なルールに関係なく、大文字と小文字の区別を実際に決定するのはファイル システムです。大文字と小文字が区別されるファイル システムが、大文字と小文字が区別されない標準のファイル システムのコンピューターにアタッチされている場合、Bit9 ルールでは大文字と小文字が区別されます。その逆も同様です。外部ドライブを接続する場合、またはネットワーク ファイル システムを Bit9 管理コンピューターにマウントする場合は、この点に気を付けてください。
- ルール フィールドに入力されたテキストの大文字と小文字は、その時点で区別されていなくても保持されます。これは、情報をコピーしたとき、コピー先でその情報が別のプラットフォームに適用される場合に重要となることがあります。

パスを入力するときは、必ず適用先プラットフォーム向けの正しいディレクトリ区切り文字と、選択されたプラットフォームのパスに適した文字と形式のみを使

用します。Bit9 Server ではプラットフォーム間でパスを変換できません（たとえば、「\」を「/」に変換することはできません）。ただし、区切り文字がプラットフォームに合っていない場合は、警告が表示されることがあります。

Bit9 ソフトウェアの禁止とは

Bit9 ファイル禁止は、Bit9 エージェントが実行されているコンピューターで特定のファイルが実行されるのを、エージェントの適用レベルに基づいてブロックするルールです（表 35 を参照）。毎日の操作で Bit9 エージェントによってレポートされたファイルを禁止できます。また、コンピューター上でまだ確認されていないものの、サードパーティから既に情報を入手しているファイルをあらかじめ禁止することもできます。Bit9 では、ファイル名またはハッシュによる禁止がサポートされます。制御モードで実行されているすべてのエージェントを禁止したり、選択したポリシーのコンピューターのみを禁止の対象にしたりできます。また、プロセスのファイル イメージを禁止したときに、既に実行中のプロセスを終了するように Bit9 を構成することもできます。

次の表で示すように、ファイルを禁止しても、可視性モードで動作しているコンピューター上のソフトウェアの実行は継続されます。ただし、可視性モードでも、禁止ファイルの実行頻度の監視に使用できるイベントが生成されます。また、可視性モードで望ましくないファイルを禁止すると、将来的に完全制御モードに移行する準備を行ううえで役立ちます。

表 35：ファイルの実行に対するファイル禁止の影響（適用レベル別）

ポリシー設定	適用レベル				
アクティブな禁止	なし（エージェント無効）	なし（可視性のみ）	低	中	高
（ハッシュまたは名前による）禁止ファイル	オフ / 許可	許可してレポート	ブロック	ブロック	ブロック

名前またはハッシュによって特定のファイルを禁止すると、その禁止は、[Software Rules（ソフトウェア ルール）] ページの [Files（ファイル）] タブにルールとして表示されます。

ファイルを禁止する際に基本的に行わなければならないのは、名前によって禁止するかハッシュによって禁止するかを決めることです。表 36 は、この 2 つの違いを示しています。

表 36：名前による禁止とハッシュによる禁止

禁止タイプ	説明
ファイル名による禁止	すべての場所（ファイル名のみを入力した場合）または指定した場所（パスを入力した場合）、およびすべてのコンピューターまたは選択したポリシーのコンピューターにある、指定したファイルの実行をブロックします。ファイル名による禁止では、ファイルのグローバル状態は変更されませんが、指定した名前のファイルのインスタンスについては、どこにあってもすべてが確実にローカルで禁止されます。 特に (*) ワイルドカード文字を使用してパスを指定するときは、システムまたはアプリケーションの操作に必要なファイルを禁止しないように気を付けてください。 安全のため、ファイル名による禁止を「レポートのみ」状態で実行すると、禁止の影響をテストできます。禁止（レポートのみ）は、その状態を「禁止されているファイルのブロック」に変更するまで適用されません。 名前およびハッシュの両方によって禁止されているファイルを状態で検索すると、ファイルは禁止状態のファイルのリストに表示されますが、［Banned by Name（名前による禁止）］の［Local State Details（ローカル状態の詳細）］のファイルには表示されません。 **プラットフォームに関する注意**：ファイル名による禁止はそれぞれ、1 つのプラットフォームにのみ適用されます。パスを入力するときは、必ず正しいディレクトリ区切り文字と、選択されたプラットフォームのパスに適した文字と形式のみを使用します。
ハッシュによる禁止	すべてのコンピューターまたは選択したポリシーのコンピューターのすべての場所で、指定したハッシュの実行をブロックします。ハッシュによる禁止はプラットフォームに固有ではありません。 外部ソースからハッシュをコピーして貼り付けることはできますが、ファイルが一覧表示されているコンソール ページからエージェントによって直接検出されたハッシュを禁止する方が簡単です。ハッシュが表示されているコンソール ページのほとんどから、禁止を直接作成することができます。こうしたページから禁止の作成を開始すると、［Add File Rule（ファイル ルールの追加）］ページが自動的に表示されます。このページにはハッシュが入力され、タイプには「禁止」が設定されています。また、禁止を作成する前に、他の禁止プロパティを変更することもできます。

ファイル禁止のオプション

特定のファイルに禁止を直接適用して今後の実行をブロックする以外にも、Bit9 にはさまざまな方法やオプションが用意されています。ソフトウェアを禁止するオプションを次のリストにまとめます。

- すべてのコンピューターまたは選択したポリシーのすべてのコンピューターで、特定のソフトウェアが実行されないようにするには、ファイルごとにファイル禁止ルールを作成します。これにより、制御モードで実行されているすべてのコンピューターでそのソフトウェアがブロックされます（高適用で実

行している場合は、単純に承認しないようにします)。こうした禁止の作成方法の詳細については、「ファイル固有のルール：承認と禁止」(324 ページ)を参照してください。

- 禁止する不要なファイルのハッシュのリストがある場合は、1 回の操作でそのリスト全体に対する禁止を作成できます。こうした禁止の作成方法の詳細については、「ファイル リストの承認または禁止」(337 ページ)を参照してください。
- 特定の公開者のファイルをすべて禁止する場合は、公開者を禁止します。詳細については、「公開者による承認または禁止」(288 ページ)を参照してください。公開者の禁止をさらに細かく調整するには、公開者の特定の証明書を禁止します。詳細については、「適用のための証明書の使用」(369 ページ)を参照してください。
- 特定の場所や、特定のユーザーまたはプロセス別にファイルのインストールや実行をブロックまたは許可する特別なルールが必要な場合は、実行をブロックするカスタム ルールを作成します。このルールは禁止ではなく、条件に一致したときに禁止と同じように機能します。詳細については、第 12 章「カスタム ソフトウェア ルール」を参照してください。
- 禁止イメージが含まれる現在実行中のプロセスのほか、今後のファイル実行の試みを禁止する必要がある場合は、ポリシーをそのように構成します。詳細については、「禁止による実行中のプロセスの停止」(339 ページ)を参照してください。
- 外部通知からのマルウェア レポートなど、特定のイベントでファイルが参照されるときに、そのファイルを禁止する必要がある場合は、イベント ルールを作成します。詳細については、第 16 章「イベント ルール」を参照してください。

信頼済みディレクトリによる承認

組織でソフトウェア展開ツールを使用している場合、またはソフトウェア承認用のコンピューターを確保する必要がある場合は、信頼済みディレクトリを使用して、通常の展開中にソフトウェアを自動的に承認できます。信頼済みディレクトリ承認は、既存のソフトウェア展開プロセスに容易に統合できます。展開サーバーの指定された信頼済みディレクトリのソフトウェアはすべて、自動的に承認されます。信頼済みディレクトリによる承認レベルは、そのディレクトリがあるプラットフォームによって異なります。

Bit9 では、一般的な展開技術による信頼済みディレクトリ承認をテストし、完全にサポートしています。ご自身の展開方法がサポートされているかどうか、および、それを Bit9 Security Platform に統合する際の特別な考慮事項に関するガイダンスについては、Bit9 テクニカル サポートにお問い合わせください。

ディレクトリの有効化直後またはそのディレクトリへのファイルの追加直後に、信頼済みディレクトリ承認がエージェントに送信されることはありません。エンドポイントに信頼済みディレクトリ ファイル承認が送信される状況には次の 3 種類があります。

- 「いずれかのエンドポイント」でブロックされているファイルの記録が Bit9 Server 上にあり、そのファイルが後で信頼済みディレクトリによって承認された場合、サーバーはエージェントに対してそのファイルが承認されたことを直ちに通知します。

- 信頼済みディレクトリによって承認されたファイルのインスタンスを Bit9 Server に接続されたコンピューター上でユーザーが実行しようと試みた場合、サーバーはエージェントに対してそのファイルの実行を直ちに許可し、そのファイルが承認されたことを他のエージェントにも通知します。
- 信頼済みディレクトリによって承認されたファイルがインストーラーであると特定された場合、Bit9 Server はエージェントに対してそのファイルが承認されたことを直ちに通知します。

ファイルが信頼済みディレクトリによって承認され、他のルールによりブロックされなかった場合でも、上記いずれかの状況が発生してファイルの承認がエージェントに通知されない限り、そのファイルのインスタンスはローカルで承認されません。その場合、ファイルの承認が送信される前にエージェント コンピューターがサーバーから切断されると、インスタンスがブロックされる可能性があります。

注意

リムーバブル メディアは、信頼済みディレクトリには使用しないことをお勧めします。リムーバブル デバイスが一度切断されてから再接続された場合、再スキャンは行われないため、新しいコンテンツはすべて未処理になり、信頼されません。新しいコンテンツを信頼するには、信頼済みディレクトリを無効にしてから、再度有効にする必要があります。永続的にアタッチされた固定メディアで信頼済みディレクトリを、エージェントが変更や追加を監視し、新しいコンテンツすべてを処理できるように構成します。

Windows の信頼済みディレクトリ

Windows コンピューターでは、信頼済みディレクトリで見つかったファイル（およびそのサブフォルダー）自体は承認されます。

信頼済みディレクトリのインストーラーとアーカイブ

アーカイブとインストーラーは、他のファイルを生成できるファイル タイプです。両方のファイル タイプを信頼済みディレクトリに配置して、ファイル承認をさらに効率化すると便利ですが、この 2 つはそれぞれ異なる方法で処理されることに注意してください。

- **インストーラー** – Bit9 によって「インストーラー」として認識される共通の Windows 形式は、NullSoft、Wise、InstallShield、および MSI です。ファイルをインストーラーとして手動でマークすることもできます。

  信頼済みディレクトリでは、インストーラー ファイルはグローバルに承認され、ファイル カタログに追加されます。信頼済みディレクトリをホストしているシステムでエージェントが実行されている場合、インストーラーは［Files on Computers（コンピューター上のファイル）］リストにも追加されます。インストーラー ファイルの実行時に、書き込まれるファイルを確認するインストーラー ファイル分析は実行されません。また、インストーラーによって書き込まれるファイルは、インストーラーが実際に実行されるまで、［File Catalog（ファイル カタログ）］リストまたは［Files on Computers（コンピューター上のファイル）］リストに追加されません。インストーラーによって書き

込まれるファイルのインスタンスはローカルで承認されます。これらのファイルが、ファイル カタログでグローバルに承認されることはありません。

- **アーカイブ** – Bit9 によって「アーカイブ」として認識される Windows 形式は、7Zip、BZip2、CAB、GZip、ISCab、ISO、MSCompress、RAR、ZIP、および TAR です。

  信頼済みディレクトリでは、アーカイブ ファイルの展開時に、書き込まれるファイルを確認するアーカイブ ファイル分析は Bit9 によって実行されません。アーカイブ ファイルによって書き込まれるファイルは、そのファイルのインスタンスがまだ存在しなくてもグローバルに承認され、ファイル カタログに追加されます。ただし、アーカイブが他のコンピューターで展開されるまで、[Files on Computers（コンピューター上のファイル）] インベントリにファイルは追加されません。最上位レベルのアーカイブ ファイル（myfiles.ZIP など）はファイル カタログに追加されません。

  Windows イメージ (WIM) ファイルは、オペレーティング システム ファイルをパッケージ化するためによく使用されます。デフォルトでは、Bit9 によってアーカイブとして認識されませんが、信頼済みディレクトリをホストしているシステムごとに次の手順を実行して、WIM ファイルのコンテンツを分析して承認できます。

WIM ファイルの内容の信頼済みディレクトリ承認を有効にする手順：

1. WIM ファイルの内容を承認できるようにする信頼済みディレクトリを選択または作成します。信頼済みディレクトリがあるシステムで、Microsoft Windows 自動インストール キット (AIK) をダウンロードします。このキットには **imagex.exe** が含まれています。これが WIM の承認に必要です。

   https://www.microsoft.com/en-us/download/details.aspx?id=10333

   Windows 7、8、10（および同等のサーバー）は、サポートされているオペレーティング システムのリストに含まれていませんが、このキットを使用できます。
2. ImageX.exe をエージェント フォルダーに追加できるように、エージェントで改ざんからの保護を無効にします。
3. Windows AIK をダウンロードした場所にある ImageX.exe をエージェント インストール ディレクトリ（通常は C:\Program Files (x86)\Bit9\Parity Agent）にコピーします。
4. Bit9 コンソールで、信頼済みディレクトリがあるエージェントで ImageX.exe ファイルを承認します。
5. エージェントの改ざんからの保護を再度有効にします。
6. コンソールで、[Support（サポート）] ページの URL を入力します。

   `https://<サーバーのアドレス>/support.php`
7. [**Advanced Configuration**（高度な構成）] タブをクリックし、[Agent Configuration（エージェント構成）] パネルで [**Enable Deep Crawl**（深いクロールの有効化）] ボックスをオンにします。
8. [**Deep Crawl Files**（深いクロール ファイル）] 行で、ファイル拡張子リストの末尾に「*.wim」を追加します（まだ、追加されていない場合）。リスト内では、コンマを使用して、新しい拡張子と以前に拡張子を区切ります。完了したら、[**Update**（更新）] をクリックします。

Mac および Linux の信頼済みディレクトリ

Mac および Linux コンピューターでは、信頼済みディレクトリの最上位レベル ファイル（および、そのすべてのサブフォルダー）が承認されますが、内容は分析されることや承認されることはありません。たとえば、インストーラーによってインストールされるファイル、またはアーカイブ ファイルから抽出された可能性があるファイルについては、その最上位レベル ファイルが信頼済みディレクトリに配置されているときは、分析も承認も行われません。

ただし、Mac コンピューターで、PKG ファイルが信頼済みディレクトリに配置されている場合、その PKG ファイルは承認済み「インストーラー」になります。つまり、PKG ファイルが分析されていなくても、インストーラー プロセスによって PKG から書き込まれたファイルはすべて承認されます。

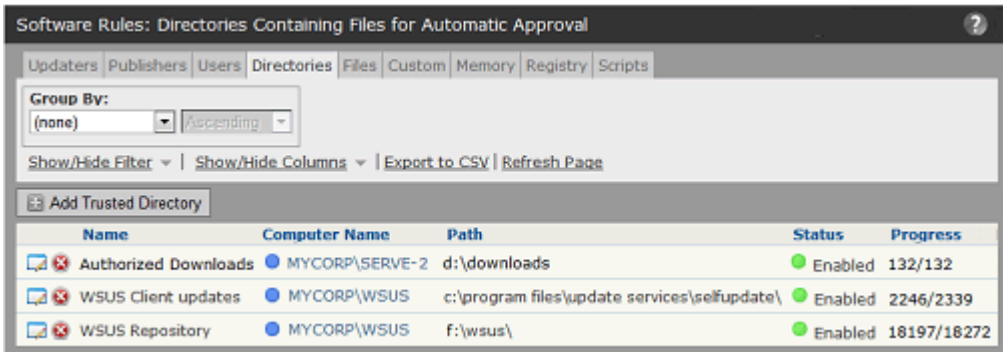
Mac と Linux の両方の信頼済みディレクトリについては、アプリケーションまたはアーカイブのファイルをグローバルに承認するには、インストールまたは解凍されるファイルが実際に信頼済みディレクトリに配置されるようにパッケージを展開または解凍します。

信頼済みディレクトリの作成

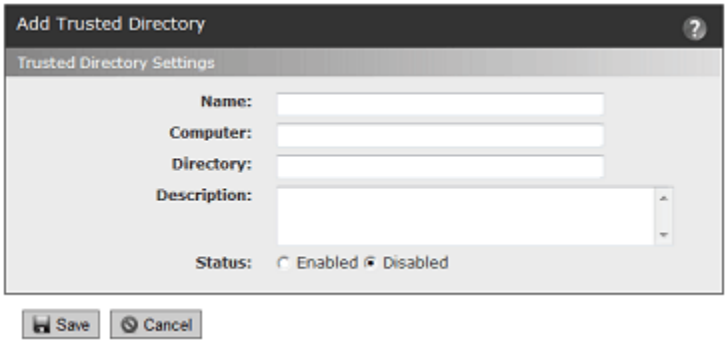
信頼済みディレクトリは、Bit9 エージェントがインストールされているコンピューターに配置する必要があります。Bit9 コンソールから、展開サーバーの名前とディレクトリを指定して、そのサーバーを信頼します。

信頼済みディレクトリを使用して、ソフトウェアを展開するために自動的に承認する手順：

1. 展開サーバーにBit9エージェントがまだインストールされていない場合は、インストールします。サーバーのファイルの初期化が完了するまで待ちます。展開サーバーの初期化ステータスは、［Computers（コンピューター）］ページまたは［Computer Details（コンピューターの詳細）］ページで監視できます（「1台のコンピューターの詳細を表示する手順：」（156 ページ）を参照）。
2. コンソール メニューで、［**Rules**（ルール）］>［**Software Rules**（ソフトウェア ルール）］の順に選択します。［Software Rules（ソフトウェア ルール）］ページが表示されます。デフォルトでは、［Updaters（アップデーター）］タブが表示されます。
3. ［**Directories**（ディレクトリ）］タブをクリックします。［Trusted Directories（信頼済みディレクトリ）］テーブルが表示されます。



4. ［**Add Trusted Directory**（信頼済みディレクトリを追加）］ボタンをクリックします。［Add Trusted Directory（信頼済みディレクトリの追加）］ページが表示されます。



5. 展開サーバーに関する情報と、信頼済みディレクトリのステータスを入力します。次の表は、信頼済みディレクトリのフィールドと、使用できる値を示しています。

表 37：信頼済みディレクトリのパラメーター

フィールド	説明
Name（名前）	［Trusted Directories（信頼済みディレクトリ）］テーブルで自動承認インスタンスを特定するときに使用される名前。任意のテキストを指定できます。
Computer（コンピューター）	ソフトウェア展開サーバーとして使用している、または今後使用するエージェント管理コンピューター。この名前は、［Computers（コンピューター）］ページに表示されているコンピューター名と一致している必要があります。ドメイン内のコンピューターについては、ドメインとコンピューター名の両方を次のいずれかの形式で指定します。 • `DOMAIN_NAME\computer_name`（Windows のみ） • `computer_name.domain.extension`（すべてのプラットフォーム） **注意**：既存の信頼済みディレクトリのコンピューター名を編集する場合、新しい名前と一致するコンピューターが Bit9 Server によって複数検出されると、それぞれのコンピューターに対して信頼済みディレクトリが作成されます。

フィールド	説明
Directory（ディレクトリ）	展開サーバーの展開ディレクトリ。展開技術によっては、複数のディレクトリを個別に指定しなければならないことがあります。たとえば、Microsoft WSUS には次のディレクトリが必要です（実際のドライブ文字に置き換えてください）。 C:\WSUS\WsusContent\ C:\Program Files\Update Services\Selfupdate\ **注意**：リムーバブル メディアを信頼済みディレクトリに使用することはお勧めしません。リムーバブル ドライブを取り外してから再アタッチした場合、再スキャンは実行されません。そのため、新しいソフトウェアが信頼されない可能性があります。 **プラットフォームに関する注意**：パスを入力するときは、必ず正しいディレクトリ区切り文字と、選択されたプラットフォームのパスに適した文字と形式のみを使用します。Bit9 Server ではプラットフォーム間でパスを変換できません（たとえば、「\」を「/」に変換することはできません）。また、Linux のファイルとパスでは、通常、大文字と小文字が区別されることに注意してください。
Description（説明）	この信頼済みディレクトリのオプションの説明です。
Status（ステータス）	次のいずれかを選択します。 ［**Enabled**（有効）］– 展開サーバー上の信頼済みディレクトリに存在するソフトウェアは、すべてのコンピューターにインストールすることが承認されます。 ［**Disabled**（無効）］– 展開サーバー上の信頼済みディレクトリに存在するソフトウェアは、他のコンピューターに対して承認されません。このディレクトリからインストールされたソフトウェアは、展開サーバーのポリシーの設定に従って処理されます。

6. ［**Save**（保存）］ボタンをクリックします。承認コンピューターと指定した構成情報が、［Trusted Directories（信頼済みディレクトリ）］テーブルに表示されます。

> **注意**
> 信頼済みディレクトリを作成したときに有効にしなかった場合は、そのディレクトリを使用する前に有効にする必要があります。

7. 既にある手順に従ってソフトウェアを展開します。信頼済みディレクトリを使用して Mac または Linux アプリケーションを承認する場合は、「Mac および Linux の信頼済みディレクトリ」（280 ページ）を参照してください。

信頼済みディレクトリを有効にすると、次のようになります。

- 信頼済みディレクトリを有効にしたときに存在していたすべてのファイル（サブフォルダーのファイルを含む）がグローバルに承認されます。また、信頼済みディレクトリを有効にした後に追加するファイルも承認されます。

- Windows の信頼済みディレクトリでインストーラーとして特定されたファイルがグローバルに承認されます。インストーラーによって書き込まれたファイルは、書き込まれた場所で、書き込まれたときにローカルで承認されます。同様に、アーカイブ ファイルはグローバルに承認され、展開時にそのファイルによって書き込まれるファイルもグローバルに承認されます。
- ディレクトリが存在するコンピューターは、ルールの変更ができるだけ早く適用されるように、更新の永続的な優先順位が構成されます。このステータスは、[Computer Details（コンピューターの詳細）] ページで変更できます。

> **注意**
>
> 既存の Windows 展開フォルダーを信頼済みディレクトリにした場合、そのフォルダーに大量のソフトウェアが保存されていると、ディレクトリの内容を分析して承認する Bit9 スキャン プロセスに数時間かかることがあります。

信頼済みディレクトリの検証

信頼済みディレクトリが機能していること、およびそのディレクトリ内のファイルが承認されていることを確認する方法は複数あります。

信頼済みディレクトリのステータスを確認する手順：

1. コンソール メニューで [**Rules**（ルール）] > [**Software Rules**（ソフトウェア ルール）] の順に選択し、[Software Rules（ソフトウェア ルール）] ページで [**Directories**（ディレクトリ）] タブをクリックします。[Trusted Directories（信頼済みディレクトリ）] テーブルが表示され、各信頼済みディレクトリのステータスと、これまでに分析された（合計）ファイル数が示されます。
2. 必要に応じて、信頼済みディレクトリの横にある [View Details（詳細の表示）]（ファイルと鉛筆）ボタンをクリックして、そのディレクトリの詳細を確認できます。この詳細ページには、追加のステータス情報が含まれる場合があります。

[Events（イベント）] ページで、信頼済みディレクトリ関連のイベントを確認することもできます。ディレクトの作成と変更アクティビティのほか、信頼済みディレクトリで行われたファイル分析の結果が表示されるイベント サブタイプもあります。

展開サーバーでファイルが承認されていることを確認するには、[File Catalog（ファイル カタログ）] タブの [Saved Views（保存済みビュー）] メニューから [**Approved Files**（承認済みファイル）] を選択し、承認済みであると思われるファイルのいずれかを検索します。信頼済みディレクトリの新しく承認されたファイルが [Approved Files（承認済みファイル）] テーブルに表示されるまでの時間は、ディレクトリ内のファイル数と、Bit9 Server 上の他のアクティビティの量によって異なります。[Approved Files（承認済みファイル）] テーブルを更新するには、[File Catalog（ファイル カタログ）] ページの [Refresh Page（ページの更新）] ボタンを使用します。

フィルターを [Approved Files（承認済みファイル）] ビューに追加して、信頼済みディレクトリであるために承認されたファイルをすべて表示することもできます。[Add filter（フィルターを追加）] メニューで [**File State Reason**（ファイルの

状態の理由)］を選択し、［File State Reason（ファイルの状態の理由)］メニューから［is（等しい)］と［**Trusted Directory**（信頼済みディレクトリ)］を選択して、フィルターを完成させます。

Windows パッケージの承認の確認

Windows インストーラーの場合、Bit9 が信頼済みディレクトリでインストーラーを認識して承認したこと（そして、インストールしたファイルをローカルで承認すること）を確認できます。［File Catalog（ファイル カタログ）］タブにある［**Trusted Packages**（信頼済みパッケージ)］という［Saved View（保存済みビュー)］には、信頼済みディレクトリに保存されていることが理由でグローバルに承認されたインストーラーが一覧表示されます。このリストには、Bit9 エージェントのインストーラーも含まれます。このテーブルには、インストーラーとして認識されていないファイルは表示されません。

［Trusted Packages（信頼済みパッケージ）］ビューで、パッケージ名の横にある［View Details（詳細の表示)］ボタン（鉛筆とファイル）をクリックすると、その［File Details（ファイルの詳細）］ページが表示されます。パッケージ名をクリックすると、パッケージによって書き込まれた関連ファイルのテーブルが表示されます。

インストーラー アクセスのカスタム ルール

Bit9 Security Platform では、「信頼済みパス」を作成するカスタム ルールがサポートされます。信頼済みパスは、インストーラーを配置するネットワークの場所として便利です。そのインストーラーは、一部またはすべてのポリシーのコンピューターが実行することができます。

信頼済みパスのファイルによって書き込まれたファイルのローカル状態は、使用された［Execute Action（実行アクション)］コマンドによって異なります。［Execute Action（実行アクション）］が［Allow（許可）］に設定されている場合、インストーラーによるファイルの書き込みは許可されますが、そのファイルがアクションによってローカルで承認されることはありません。［Execute Action（実行アクション)］が［Allow and Promote（許可と昇格)］に設定されている場合は、インストーラーによるファイルの書き込みが許可され、そのファイルは（禁止されていない限り）ローカルで承認されます。いずれの場合も、書き込まれたファイルのグローバル状態は、信頼済みパスの影響を受けません。詳細については、「［Trusted Paths（信頼済みパス)］」（451 ページ）を参照してください。

ディレクトリの信頼の削除または無効化

信頼済みディレクトリから信頼を削除することにした場合は、次の 2 つのいずれかを実行します。

- 信頼済みディレクトリを「無効」にして、無効にした後に追加されたファイルが信頼されないよう指定します。これを行うには、名前の横にある［View Details（詳細の表示)］（鉛筆とファイル）ボタンをクリックし、［**Disabled**（無効)］ステータス ラジオ ボタンをクリックして、［**Save**（保存)］をクリックします。展開サーバーからインストールを一時的にサスペンドする場合にこれを検討します。（削除するのではなく）無効にすることで、後で必要になったときに、プロパティを再入力することなくディレクトリを再度有効にできます。

- ディレクトリを［Trusted Directories（信頼済みディレクトリ）］リストから削除するには、名前の横にある **[X]** ボタンをクリックします。この操作で削除されるのは、Bit9 のディレクトリの「信頼済みステータス」です。実際のフォルダーではありません。展開サーバーでフォルダーの内容が不要になった場合は、フォルダー自体を削除します。

注意

- 信頼済みディレクトリのステータスを無効化または削除しても、ディレクトリ内の既存のファイルから承認は削除されません。
- コンピューターから削除された、またはネットワークの問題により Bit9 エージェントにアクセスできない信頼済みディレクトリ フォルダーは、［Trusted Directories（信頼済みディレクトリ）］テーブルに［Enabled, Inaccessible（有効、アクセス不可）］と表示されます。

信頼済みユーザーまたはグループによる承認

Bit9 Security Platform では、コンピューターの適用保護が「高」のときに、ソフトウェアを自身のコンピューターまたは他の人のコンピューターにインストールする必要があるユーザーを対象としたインストール権限がサポートされます。ユーザーを個別に信頼したり、メンバーを信頼済みユーザーにする信頼済みグループを指定したりできます。

信頼済みユーザーおよび信頼済みグループのユーザーには、自身の認証情報でログインできる、アクセス可能なすべてのコンピューターにソフトウェアをインストールするためのフル権限が付与されます（禁止されていない限り）。信頼済みユーザーによってインストールされたアプリケーションは、インストールされた場所でローカル承認されます。

グループを指定する方法

Mac および Linux の場合は、名前を入力してグループを指定します。

Windows の場合は、次の方法でグループを指定できます。

- AD が実装されている場合は、AD グループを指定できます。グループとドメイン名、または SID を入力します。
- 組み込みの Windows グループをメニューから選択できます。

AD ユーザーまたはグループを選択する場合：

- Bit9 Server が信頼済みユーザーまたはグループの AD 情報にアクセスできる場合は、その AD ユーザーまたはグループを指定できます。
- AD ベースの権限が決まるのは、ユーザーのログイン時です。AD グループに対して Bit9 権限に影響する変更を行った場合、そのグループのログイン ユーザーは、「次回」のログインまで、その変更の影響を受けません。

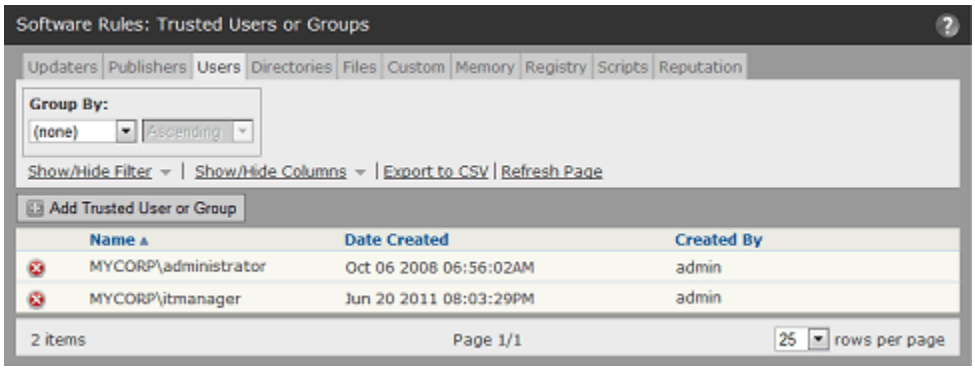
組み込み Windows グループを選択した場合、オペレーティング システムのバージョンによっては、意図したとおりにアクセスが提供されないことがあります。

Windows Vista 以降でアプリケーションを実行する場合、事前定義されたセキュリティ グループ（Administrators など）のメンバーシップを指定するには、管理者としてアプリケーションを実行する必要があります。ルールに対してグループを定義する必要がある場合は、事前定義されたグループではなく、自身で定義したセキュリティ グループを使用することを検討してください。

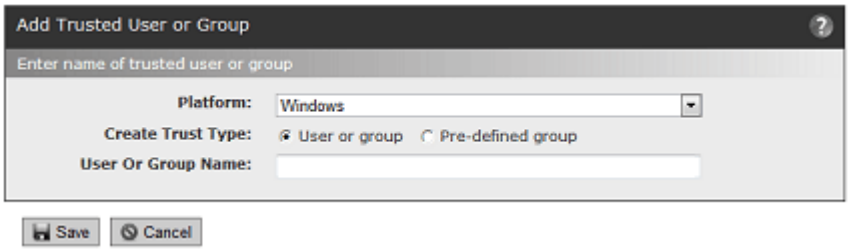
信頼済みユーザーまたはグループの作成

高適用レベルのコンピューターにソフトウェアをインストールできるユーザーを指定する手順：

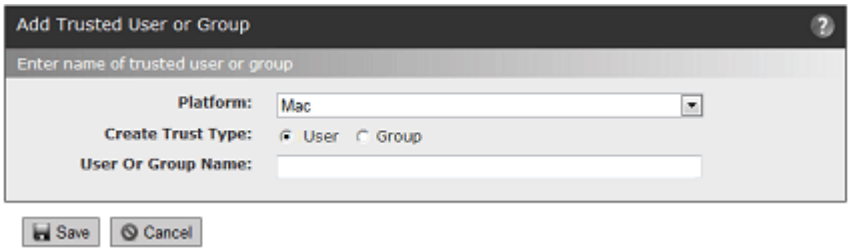
1. コンソール メニューで［**Rules**（ルール）］>［**Software Rules**（ソフトウェア ルール）］の順に選択し、［Software Rules（ソフトウェア ルール）］ページで［**Users**（ユーザー）］タブをクリックします。［Trusted Users or Groups（信頼済みユーザーまたはグループ）］ビューが表示されます。



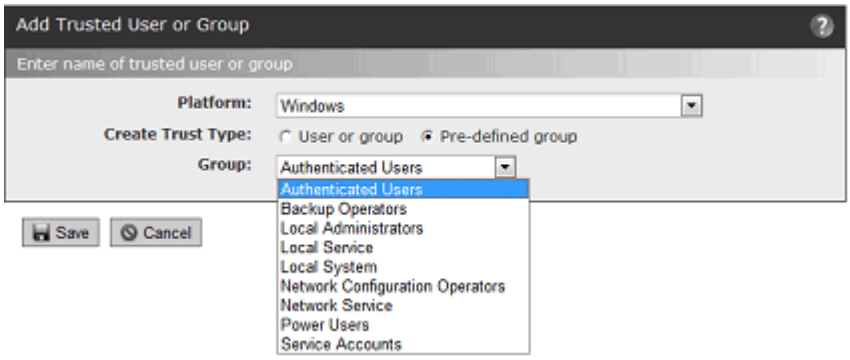
2. ［**Add Trusted User or Group**（信頼済みユーザーまたはグループを追加）］ボタンをクリックします。［Add Trusted User or Group（信頼済みユーザーまたはグループの追加）］ページが表示されます。



3. プラットフォームを選択します。このプラットフォームから、ユーザーまたはグループを選択します。Windows ではなく Mac または Linux を選択した場合、一部のフィールドが異なります。



4. Windows をプラットフォームとして選択した場合は、次の「**いずれか**」の方法で、信頼済み権限を付与するユーザーまたはグループの名前を入力します。
   - ［**User or group**（ユーザーまたはグループ）］をオンのままにして、次のいずれかの形式で有効なドメインおよびユーザー名を入力します。*DOMAIN_NAME\user_name* または *user_name@DOMAIN_NAME*
   - ［**User or group**（ユーザーまたはグループ）］をオンのままにして、次のいずれかの形式で有効な AD グループ名を入力します。*DOMAIN_NAME\group_name* または *group_name@DOMAIN_NAME*
   - ［**User or group**（ユーザーまたはグループ）］をオンのままにして、有効なユーザーまたはグループ SID を入力します。
   - ［**Pre-defined group**（事前定義グループ）］ボタンをクリックし、メニューから Windows グループを選択します。



5. Mac または Linux をプラットフォームとして選択した場合は、次の「**いずれか**」の方法で、信頼済み権限を付与するユーザーまたはグループの名前を入力します。
   - ［**User**（ユーザー）］を選択したままにして、選択したプラットフォームに対する有効なユーザー名を入力します。
   - ［**Group**（グループ）］をクリックし、選択したプラットフォームに対する有効なグループ名を入力します。
6. ［**Save**（保存）］ボタンをクリックします。ユーザーまたはグループが［Trusted Users（信頼済みユーザー）］テーブルに表示されます。

ユーザーまたはグループからの信頼の削除

ロックダウンされたコンピューターでユーザーまたはグループのインストール権限が不要になった場合は、［Trusted Users or Groups（信頼済みユーザーまたはグループ）］テーブルからそのユーザーまたはグループを削除できます。これを行うには、そのユーザーまたはグループのエントリの横にある［Delete（削除）］(X) ボタンをクリックします。

重要

- Bit9 の信頼をユーザーまたはグループから削除し、Bit9 エージェントがその変更を受け取ると、ほぼ直後にそのユーザーまたはグループの信頼済みステータスは失われます。つまり、ユーザーは信頼されなくなり、新しいインストールを実行できません。ただし、ユーザーが信頼されていたときに作成されたプロセスは、そのプロセスが存在する限り信頼された状態が維持されます。
- Bit9 によって信頼された AD グループからユーザーを削除しても、そのユーザーの状態は、ログアウトするまで信頼されたままです。

公開者による承認または禁止

プラットフォームに関する注意

公開者の承認と禁止は、現在 Windows コンピューターでのみ機能します。他のプラットフォームのファイルには影響しません。

ファイルの多くがデジタル証明書で署名されています。このデジタル証明書は、ファイルの整合性と ID（ファイルの公開者の名前など）を確認します。[Software Rules（ソフトウェア ルール）] ページの [Publishers（公開者）] タブには、Bit9 エージェントによって検出されたファイル用の有効な証明書で特定された、一意の公開者が一覧表示されます。Windows でファイル上のデジタル証明書が見つかると、Bit9 コンソールで公開者が検出され、表示されます。

Bit9 コンソールに表示された公開者は、承認または禁止できます。未承認のままにしておくこともできます。公開者の承認と禁止は、すべてのコンピューターまたは特定のポリシーのコンピューターに適用できます。公開者を確認して、既に確認済みのため、詳しく追跡する必要がないことを指定できます。公開者を確認しても、その公開者の状態は変わりません。

公開者の禁止と承認の要件はそれぞれ異なります。

- **禁止** – 公開者を禁止すると、その公開者を特定する証明書によって署名されたファイルすべてが禁止されます。
- **承認** – 公開者を承認すると、その公開者を特定する証明書によって署名されたファイルが承認されます。ただし、ファイルが承認されるには、その証明書が追加の Bit9 検証要件を満たしている必要があります。この要件の詳細については、この後のセクション「ファイルを承認できる証明書の確認」（295 ページ）で説明します。

注意

Bit9 Platform では、証明書自体を承認または禁止することもできます。この方法を使用すると、ソースを特定することで、さらに安全にファイルを特定および制御できますが、この方法は複雑です。詳細については、第 10 章「ファイル署名証明書の管理」を参照してください。

公開者の承認

信頼済みディレクトリを使用したアプリケーション承認が現実的ではなく、特定のソースのすべてのソフトウェアをすべてのユーザーがインストールできるようにする場合は、公開者によってファイルを承認できます。承認済み公開者のアプリケーションは、承認が適用されているポリシーのコンピューターにインストールして実行できます。公開者によって承認されたファイルのグローバル状態は（必要に応じて）変更されますが、ファイルの状態は変更されません（「ファイルのグローバル状態」（263 ページ）を参照）。こうしたファイルのインスタンスはそれぞれローカルで承認されるため、そのファイルが存在するコンピューターで実行できます。

公開者による承認では、信頼済みソースの新しいファイルが、エージェント管理コンピューターに届いたときには事前承認されています。また、必ずしもファイルごとに個別のルールを送信する必要がないため、エージェントに送信されるルールのトラフィック量を削減することもできます。

公開者を承認する方法は 2 つあります。

- **手動承認** – ［Publishers（公開者）］タブのリストから公開者を選択して承認できます。手動承認については、このセクションで説明します。
- **レピュテーション承認** – Bit9 SRS でレポートされた特定の信頼しきい値を満たす、すべての公開者の自動承認を有効にできます。「既存」のファイルに対する、レピュテーションによる公開者の承認の影響は、手動でそのファイルを承認した場合と同じです。また、新しい公開者が Bit9 SRS で認識されており、選択した信頼度を満たしている場合、その公開者は、自身のファイルがいずれかのコンピューターで検出されるとすぐに承認されます。レピュテーション承認の手順と考慮事項については、第 9 章「レピュテーション承認ルール」を参照してください。

重要

公開者を承認する前に、その公開者から派生する可能性のあるすべてのファイルについて検討してください。承認が追加されると、その公開者の「すべて」の実行可能ファイルとスクリプト ファイルがローカルで承認されます。公開者は［Approved（承認済み）］リストから削除できますが、これは、変更時にネットワークになかった新しいファイルにのみ影響します。つまり、公開者を承認したことでローカルで承認されたファイルから、「ファイル」の承認を削除する操作はありません。

公開者の禁止

公開者を禁止すると、その禁止の影響を受けるポリシーのエージェント コンピューターでは、その公開者のソフトウェアを実行できなくなります。公開者によってファイルを禁止するのは、ご自身の環境で実行したくない悪意のあるファイルまたはアプリケーションのソースがその公開者であることがわかっている場合です。公開者の禁止を作成すると、その公開者のファイルのローカル状態が「禁止」に変更されます。

ファイルの署名が無効な場合や、公開者による承認の他の要件をファイルが満たしていない場合でも、公開者によってファイルを禁止できます。

公開者の禁止は、Bit9 コンソールを使用して手動で作成します。

重要

承認と同様、公開者の禁止の影響を受ける可能性があるすべてのファイルについて検討し、公開者の禁止により、環境に必要なファイルが誤って禁止されないようにしてください。

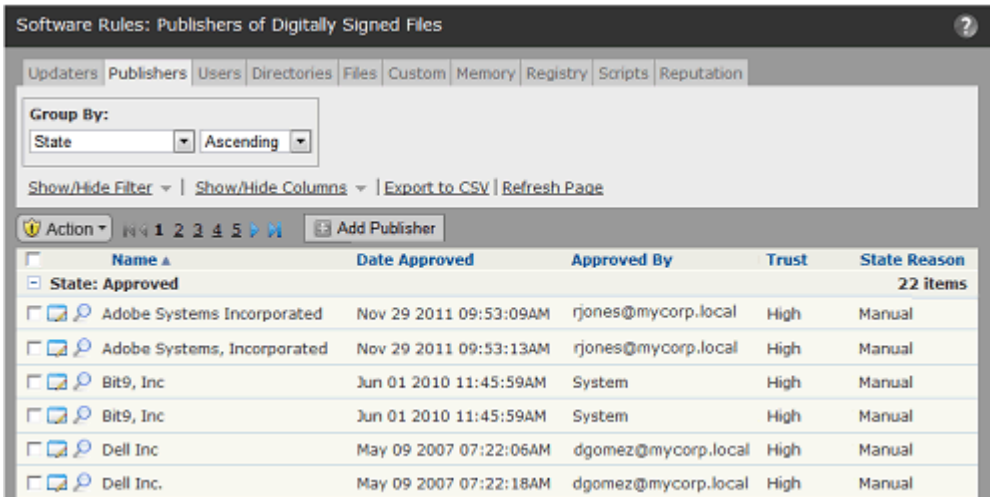
［Publishers（公開者）］タブでの禁止と承認の管理

［Publishers（公開者）］タブでは、承認や禁止のほか、複数の公開者から禁止や承認を一度に削除できます。テーブルから行った公開者の状態の変更は、すべてのポリシーに適用されます。

テーブルで複数の公開者のボックスをオンにすると、それらの公開者の状態が同じように変更されます。つまり、オンにしたすべての公開者に対して禁止、承認、禁止または承認の削除が適用されます。ある公開者を禁止して、ある公開者を承認するという処理を 1 回の操作で行うことはできません。

すべてのポリシーに対して 1 つ以上の公開者のソフトウェアを承認または禁止する手順：

1. コンソール メニューで、［**Rules**（ルール）］>［**Software Rules**（ソフトウェア ルール）］の順に選択します。［Software Rules（ソフトウェア ルール）］ページが表示されます。
2. ［**Publishers**（公開者）］タブをクリックします。［Publishers（公開者）］テーブルには、サーバーにレポートするエージェント管理コンピューターで検出され、適切に署名されたソフトウェアのすべての公開者と、証明書が手動で追加されているすべての公開者が表示されます。



3. 公開者のテーブルで、承認または禁止する公開者を見つけます。テーブルが複数ページにわたる場合があることに注意してください。

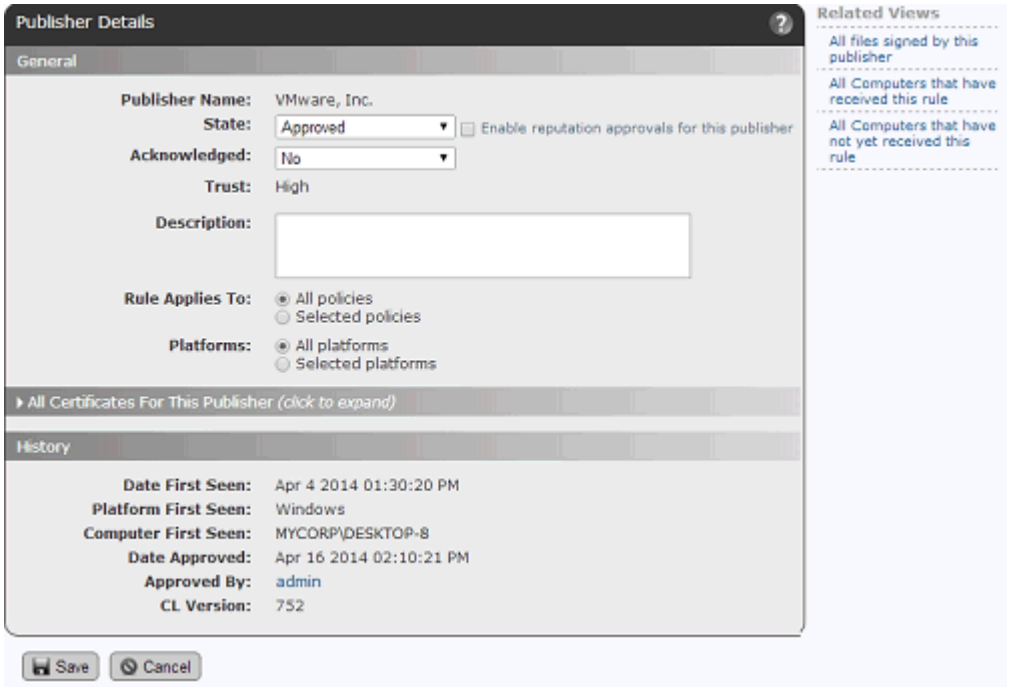
注意

同じ会社のファイルが、句読点などの小さな違いにより、異なる公開者のファイルとして特定されることがあります。このようなファイルは、[Publishers（公開者）] テーブルでは別個の行に表示されます。たとえば、「Adobe Inc.」と「Adobe, Inc.」の両方がテーブルに表示される場合があります。この場合は、インスタンスごとに個別に承認（または、未承認のままに）できます。公開者によって署名されたファイルが [Files（ファイル）] ページに未承認として表示されており、そのファイルを承認する必要がある場合は、必ず正しい公開者の証明書を承認してください。

4. 承認または禁止する公開者を確認します。特定の公開者についてさらに詳しい情報が必要な場合は、[Publisher Details（公開者の詳細）] ページを開きます。
5. 状態を変更する公開者の名前の横にあるチェックボックスをそれぞれオンにします。ページ内で変更する名前のチェックボックスをいくつでもオンにできます。承認および禁止アクションは、現在表示されているページにのみ適用されることに注意してください。
6. （現在のページで）状態を変更する公開者すべてをオンにしたら、[Action（アクション）] メニューで次の操作を行います。
   a. 選択した公開者すべてを承認するには、[**Approve Publishers**（公開者を承認）] を選択します。
   b. 選択した公開者すべてを禁止するには、[**Ban Publishers**（公開者を禁止）] を選択します。
   c. 選択した公開者すべての状態を「未承認」に戻すには、[**Remove Approval or Ban**（承認または禁止を削除）] を選択します。

［Publishers Details（公開者の詳細）］ページでの禁止と承認の管理

公開者が 1 つの場合は、［Publisher Details（公開者の詳細）］ページを使用して、公開者を承認または禁止したり、承認や禁止を削除したりできます。また、承認または禁止が適用されているポリシーを変更することもできます。



一部またはすべてのポリシーの 1 つの公開者を承認または禁止する手順（［Publisher Details（公開者の詳細）］ページ）：

1. コンソール メニューで、［**Rules**（ルール）］>［**Software Rules**（ソフトウェア ルール）］の順に選択します。［Software Rules（ソフトウェア ルール）］ページが表示されます。
2. ［**Publishers**（公開者）］タブをクリックします。［Publishers（公開者）］テーブルには、サーバーにレポートするエージェント管理コンピューターで検出され、適切に署名されたソフトウェアのすべての公開者と、証明書が手動で追加されているすべての公開者が表示されます。
3. 公開者のテーブルから、状態を変更する公開者を見つけ、［View Details（詳細の表示）］ボタン（鉛筆とファイル）をクリックします。［Publisher Details（公開者の詳細）］ページが開きます。
4. ［State（状態）］フィールドで、［**Approved**（承認済み）］または［**Banned**（禁止）］を選択します。
5. 必要に応じて、［Acknowledged（確認済み）］状態を［**Yes**（はい）］に変更します。こうすると、この公開者が確認済みであることを指定して、まだ確認していない公開者に焦点を当てることができます。これを行うには、［Acknowledged（確認済み）］フィールドを使用して、［Publishers（公開者）］テーブルにフィルターを適用します。公開者を確認しても、その公開者の状態には影響しません。

6. ［Rule Applies To（ルールの適用先）］フィールドで、［**All policies**（すべてのポリシー）］または［**Selected policies**（選択済みポリシー）］ラジオ ボタンをクリックします。
7. ［Selected policies（選択済みポリシー）］を選択した場合は、公開者の承認または禁止を有効にするポリシーの横にあるボックスをそれぞれオンにします。
8. ［Platform（プラットフォーム）］フィールドで、［**All platforms**（すべてのプラットフォーム）］または［**Selected platforms**（選択済みプラットフォーム）］ラジオ ボタンをクリックします。
   プラットフォームに関する注意：公開者の承認と禁止は、現在 Windows エージェントにのみ影響します。
9. 承認または禁止の構成が終了したら、［**Save**（保存）］ボタンをクリックします。

公開者の追加

［Publishers（公開者）］テーブルには、Bit9 エージェントが実行されているコンピューター上のファイルを通じて既に特定された公開者すべてが表示されますが、そのファイルがコンピューターに届く前に、公開者を承認しておく必要があります。たとえば、Bit9 エージェントが実行されていないコンピューターを使用して、ソフトウェアを配信する場合などです。これに対応するには、公開者を「手動」でテーブルに追加します。

公開者の追加手順：

1. 追加する公開者のファイルにアクセスできるコンピューターでブラウザーを開き、Bit9 コンソールにログインします。この操作は、ファイルが含まれるコンピューターで行うと便利です。
2. ［Publishers（公開者）］タブで［**Add Publisher**（公開者を追加）］ボタンをクリックして、［Add Publisher（公開者の追加）］ダイアログを表示します。

3. ［**Browse**（参照）］ボタンをクリックして、公開者によって適切に署名されたアプリケーション ファイルを見つけます。適切に署名された実行可能ファイルを参照して、その公開者を追加することができます。
4. Windows で、ファイルが署名されていることを確認するには、そのファイルを右クリックし、メニューから［プロパティ］を選択します。［プロパティ］ウィンドウに［デジタル署名］タブがある場合、ファイルは署名されており、その証明書を調査できます。
5. ファイル名をダブルクリックして、［File Name（ファイル名）］フィールドに名前を入力します。
6. ［**Save**（保存）］ボタンをクリックします。公開者情報が抽出され、その公開者がテーブルに追加されます。公開者の状態は最初は「未承認」です。

7. この新しい公開者をすべてのポリシーに対して承認または禁止する必要がある場合は、[Publisher（公開者）] テーブルの新しいエントリの横にあるボックスをオンにして、[Action（アクション）] メニューから [**Approve Publishers**（公開者を承認）] または [**Ban Publishers**（公開者を禁止）] を選択します。公開者を承認して、状態別にテーブルをグループ化すると、その公開者は該当する [State（状態）] セクションに移動します。これで、この公開者のファイルは、エージェント管理コンピューターのいずれかに現れた時点で、指定したとおりに処理されます。

[Publisher Details（公開者の詳細）] ページで、ポリシーによって公開者を承認または禁止することもできます。

> **注意**
>
> 手動で公開者を追加するとき、特定したファイルの一時コピーが Bit9 Server により作成されます。その一時コピーは、公開者が追加された後に削除されます。エージェントがサーバー コンピューターで実行されている場合、ファイルは [File Catalog（ファイル カタログ）] に表示されますが、普及度はゼロになります。

公開者の承認の削除

「承認済み」公開者の状態を「未承認」に変更するには、[Software Rules（ソフトウェア ルール）] ページの [Publisher（公開者）] タブに移動し、名前の横にあるボックスをオンにして、[Action（アクション）] メニューの [**Remove Publisher Approval**（公開者の承認の削除）] を選択します。これにより承認が削除されますが、公開者は禁止されません。[Publisher Details（公開者の詳細）] ページを使用して、承認を削除することもできます。

公開者が承認されたときに、この公開者のソフトウェアを既にインストールまたは実行していたコンピューターでは、そのソフトウェアを引き続き実行できます。承認済み公開者の既存のソフトウェア インスタンスはすべてローカルで承認されており、Bit9 Server 上の公開者のステータスが変更されてもローカル承認が削除されることはありません。

公開者の禁止の削除

「禁止」された公開者の状態を「未承認」に変更するには、[Software Rules（ソフトウェア ルール）] ページの [Publisher（公開者）] タブに移動し、名前の横にあるボックスをオンにして、[Action（アクション）] メニューの [**Remove Publisher Approval or Ban**（公開者の承認または禁止の削除）] を選択します。これにより禁止が削除されますが、公開者は承認されません。[Publisher Details（公開者の詳細）] ページの [State（状態）] メニューで [**Unapproved**（未承認）] を選択して、禁止を削除することもできます。

公開者の禁止が削除されると、公開者のファイルは、公開者の禁止が適用されていなかったときの状態に戻ります。

公開者のすべてのファイルを検索

［Software Rules（ソフトウェア ルール）］の［Publishers（公開者）］タブでは、指定した公開者からのファイルとして特定された、コンピューター上のファイル インスタンスすべてを検索できます。これを行うには、公開者の名前の横にある［Find Files（ファイルの検索）］ボタンをクリックします。このリストは、［Publisher Details（公開者の詳細）］ページの［Related Views（関連ビュー）］メニューを使用して表示することもできます。

ファイルを承認できる証明書の確認

公開者の特定と、公開者の承認によるファイル承認は両方とも、デジタル証明書に基づいています。証明書について詳しくない場合は、次の Web サイトで有用な背景情報を入手できます。

http://msdn.microsoft.com/en-us/library/ms537361(v=vs.85).aspx

https://sites.google.com/site/ddmwsst/digital-certificates

公開者の承認と、その公開者のファイルとして特定されたファイルの承認を区別することが重要です。［Software Rules（ソフトウェア ルール）］ページの［Publishers（公開者）］タブに表示される公開者はすべて承認することができます。公開者がこのリストに表示されるのは、ファイルにその公開者を特定する証明書があり、Windows によって署名が有効であると見なされた場合です。

ただし、この公開者の「ファイル」として特定されたファイルを、公開者によって承認できるのは、そのファイルの証明書チェーンにあるすべての証明書が Windows によって有効であると見なされている場合だけです。たとえば、証明書を受け入れるには、現在のルート証明書をインストールする必要があります。

注意

マイクロソフト セキュリティ情報 MS13-098 では、リモート コードを実行できる可能性がある Authenticode シグネチャ検証の脆弱性について説明しています。これに応じて、Microsoft では、Windows Authenticode シグネチャ フォーマットで署名されたバイナリに対するシグネチャ検証方法を変更する、サポートされているすべての Windows リリースを対象とした更新プログラムを発表しました。この変更を有効にすると、Windows Authenticode シグネチャ検証で WIN_CERTIFICATE 構造の外部情報が許可されず、Windows で非準拠バイナリが署名済みとして認識されることがなくなります。この新しい動作を有効にすると、前に公開者によって承認されたファイルが、Bit9 管理システムでブロックされる可能性があります。

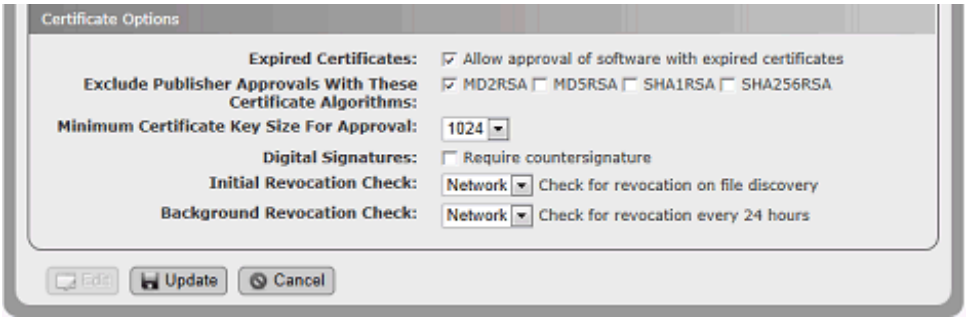
この変更はセキュリティ情報 MS13-098 に含まれますが、(2014 年 7 月時点では) オプトイン ベースでのみ有効になります。ただし、Microsoft は、Microsoft Windows の今後のリリースでこれをデフォルトの動作にすると発表しています。
この変更の詳細については、https://technet.microsoft.com/library/security/2915720 を参照してください。

また、ファイルのチェーン内にあるすべての証明書が Bit9 の追加要件も満たす必要があります。この設定は、[System Configuration（システム構成）] ページの [Advanced Options（高度なオプション）] タブで構成できます。こうした証明書の設定に関しては次の点に注意してください。

- エージェント インストール パッケージを生成する前（つまり、Bit9 Server のインストール直後）に、証明書構成オプションを設定することをお勧めします。これにより、サーバーに接続されていないエージェントを含め、すべてのエージェントによって、意図したとおりに証明書が確実に処理されます。また、エージェントのインストール後に証明書の設定を変更した場合は、各エージェントで証明書の再評価を行う必要があります。エージェントを展開する前に正しく設定しておくことで、大量の処理が実行されるのを避けることができます。
- 以前の設定を満たしていた証明書を持ち、公開者によって既に承認されているファイルのローカル承認については、構成可能な証明書設定を変更しても削除されません。
- 証明書設定の変更は、Microsoft サポート ファイルの追跡とインベントリに影響する可能性があります。「OS インベントリ追跡に影響する変更」（240 ページ）を参照してください。

構成可能な証明書の承認オプションを表示および変更する手順：

1. コンソール メニューで、[**Administration**（管理）] > [**System Configuration**（システム構成）] の順に選択します。
2. [システム構成] ページで、メニューの [**Advanced Options**（高度なオプション）] をクリックします。[Advanced Options（高度なオプション）] ページが表示されます。下部には [Certificate Options（証明書オプション）] パネルがあります。



3. ページ下部で、[**Edit**（編集）] ボタンをクリックします。
4. **[Expired Certificates（期限切れの証明書）]**：[Certificate Options（証明書オプション）] パネルでは、期限切れの証明書の使用がデフォルトで有効になっています。このオプションの構成に役立つ情報については、「期限切れの証明書での承認」（297 ページ）を参照してください。
   a. 期限切れの証明書の使用を「無効」にするには、[Expired Certificates（期限切れの証明書）] チェックボックスを「オフ」にします。
   b. 無効にした期限切れの証明書の使用を「再度有効」にするには、そのボックスをオンにします。

5. **[Exclude Publisher Approvals With These Certificate Algorithms（これらの証明書アルゴリズムで公開者の承認を除外する）]：**このフィールドで現在オンになっているチェックボックスを確認します。このオプションの構成に役立つ情報については、「証明書アルゴリズムの除外」（298 ページ）を参照してください。
   a. 特定のアルゴリズムを使用している証明書によって署名されたファイルに対して、公開者の承認を「禁止」するには、そのアルゴリズム名の横にあるボックスをオンにします。
   b. 特定のアルゴリズムを使用している証明書によって署名されたファイルに対して、公開者の承認を「許可」するには、そのアルゴリズム名の横にあるボックスを「オフ」にします。
6. **[Minimum Certificate Key Size For Approval（承認用の証明書キーの最小サイズ）]：**公開者によるファイルの承認に必要な証明書キーの最小の長さを変更するには、メニューから新しい値を選択します。このオプションの構成に役立つ情報については、「最小キー サイズ」（298 ページ）を参照してください。
7. **[Digital Countersignatures（デジタル連署）]：**各証明書のデジタル署名に連署を要求するには、[Require countersignature（連署が必要）] ボックスをオンにします。連署を求めない場合は、このボックスを「オフ」にします。このオプションの構成に役立つ情報については、「連署オプション」（298 ページ）を参照してください。
8. **[Initial/Background Revocation Check（初期 / バックグラウンドでの失効検査）]：**証明書失効検査を制御する設定は 2 つあります。「初期」の失効検査では、ファイルが最初に検出されたときに行われる失効検査が制御されます。「バックグラウンド」での失効検査では、（有効の場合に）24 時間ごとに行われる現行の検査が制御されます。これらの設定については、「失効検査」（299 ページ）を参照してください。
9. いずれかの設定を変更した場合は、ページ下部の［**Update**（更新）］をクリックし、[Confirm Server Setting Change（サーバー設定の変更の確認）] ダイアログで［**Yes**（はい）］をクリックして、変更を保存します。

期限切れの証明書での承認

Bit9 Security Platform では、デフォルトで、期限が切れているものの（確認可能な）タイムスタンプが証明書の有効期間内である証明書を使用して、公開者によるファイル承認を行うことができます。タイムスタンプがないか、無効であるか、証明書の有効期間の前または後である場合、ソフトウェアを公開者により承認することはできません。

期限切れの証明書による承認は無効にできます。無効にしない場合、その証明書は Bit9 Security Platform により信頼されます。これによりセキュリティが向上しますが、期限切れになった有効な証明書を持つ適切なファイルが承認されないことがあります。

[Allow approval of software with expired certificates（期限切れの証明書でのソフトウェアの承認を許可）] を無効にすると、すべての公開者が再評価されます。ただし、期限切れの証明書が許可されていたときに、その証明書によってファイルが

公開者によりローカルで承認された場合は、設定を無効にしても、ファイルはローカルで承認されたままになります。

［Expired Certificates（期限切れの証明書）］の設定は、公開者の「禁止」には影響しません。したがって、ファイルで無効な署名や期限切れの証明書が使用されていても、公開者によってファイルを禁止することは可能です。

重要

最初または永続的にサーバーに接続されないエージェントについては、インストール パッケージを生成する前に、期限切れの証明書オプションを設定することが特に重要です。これにより、接続されていないエージェントによって、意図したとおりに期限切れの証明書が確実に処理されます。

証明書アルゴリズムの除外

［Exclude Publisher Approvals With These Certificate Algorithms（これらの証明書アルゴリズムで公開者の承認を除外する）］オプションを使用すると、特定のアルゴリズムを使用している証明書を持つファイルに対して、公開者ベースのファイル承認を無効にできます。アルゴリズムのボックスがオンになっている場合、そのアルゴリズムを使用する証明書を持つファイルについては、公開者による承認が許可されません。オフの場合、そのアルゴリズムを使用する証明書を使用して、公開者によるファイル承認を行うことができます。選択肢は、MD2RSA、MD5RSA、SHA1RSA、および SHA256RSA です。7.0.1 Patch 11 以降の新しい Parity インストールでは、デフォルトで、リストされたアルゴリズムのいずれかを使用している証明書を使用して承認できます。また、以前のリリースのアップグレードやパッチでも、アップグレード前にコンソールから設定が変更されていない限り、リストされたアルゴリズムのいずれかを使用している証明書を使用して承認できます。

最小キー サイズ

［Minimum Certificate Key Size for Approval（承認用の証明書キーの最小サイズ）］オプションを使用すると、ファイル承認に使用される証明書のキーの最小長を指定できます。512 ～ 4096 の範囲内の値を選択でき、キー サイズが選択した値以上の証明書をファイルの承認に使用することができます。キー サイズが選択した値を下回る証明書は、ファイルの承認に使用できません。7.0.1 Patch 11 以降の新しい Parity インストールのデフォルト値は 512 です。以前のリリースのアップグレードやパッチでも、アップグレード前にコンソールから設定が変更されていない限り、この値が使用されます。

連署オプション

Bit9 が署名済みファイルを公開者によって承認できるように、証明書のデジタル署名の連署を要求することができます。これにより、署名のタイム スタンプの操作に対するセキュリティが強化されます。デフォルトでは、ボックスはオフになっています（つまり、連署は不要です）。ボックスをオンにすると、連署されていない証明書は有効とは見なされず、公開者による承認に使用できません。

また、連署処理に関する次の詳細情報にも注意してください。

- ボックスがオフの場合、連署がない署名は、署名証明書の有効期間の間のみ有効です。
- この設定に関係なく、連署が存在する場合、その連署が有効と見なされるためには、デジタル署名に対して有効である必要があります。

失効検査

ファイルの証明書が失効しているかどうかをエージェントが検査するかどうかと、その検査方法を制御する設定は 2 つあります。

- ［**Initial Revocation Check**（初期の失効検査)］– エージェントで最初にファイルが検出されたときに、証明書の失効検査を実行するかどうかと、実行する場合はその方法を指定します。
- ［**Background Revocation Check**（バックグラウンドでの失効検査)］– 24 時間ごとにバックグラウンドで証明書の失効検査を実行するかどうかと、実行する場合はその方法を指定します。

失効設定それぞれに設定できる値が 3 つあります。

- ［**Network**（ネットワーク)］– 失効情報がローカルで提供されていない場合は、ネットワークを使用して、証明書の失効ステータスを取得します。
- ［**Cache**（キャッシュ)］– 証明書の失効を実行するときに、ローカルで提供されている失効ステータス情報を使用します（ネットワークは使用しません)。
- ［**None**（なし)］– 証明書の失効検査を実行しません。

エージェントのパフォーマンスに影響が及ぶ可能性があるため、これらの値を設定するときは、エージェントの展開シナリオを考慮してください。たとえば、オフライン エージェントがある場合は、特に［Initial Revocation Check（初期の失効検査)］で［Network（ネットワーク)］オプションを使用しないようにします。また、毎日の失効検査はバックグラウンドで行われ、エージェントのパフォーマンスに悪影響を及ぼす可能性はそれほど高くありませんが、初期の失効検査の設定は、エージェントのパフォーマンスに大きく影響する場合があることにも注意してください。

注意

エージェント ベースの証明書の失効検査が有効かどうかに関係なく、Bit9 Server はインベントリの証明書を繰り返し検証して、その証明書が失効していないことを確かめます。この検証は通常毎週行われ、証明書失効リスト (CRL) を登録機関からダウンロードしたり、OCSP (Online Certificate Status Protocol) 応答者に対して OCSP 呼び出しを行ったりします。ネットワーク トラフィックを監視している場合は、このようなダウンロードに、さまざまな国のさまざまなサイトが含まれている可能性があることに注意してください。

サーバー ベースの検証検査では、証明書の状態が変わったときに管理者に通知されますが、ルールの適用はこの影響を受けません。ルールの動作が失効の影響を受けるようにするには、エージェント ベースの失効検査を有効にします。

アップデーターによる承認

アップデーター承認ルールでは、アプリケーション更新プログラムがダウンロード可能になったときに、適用保護が「高」のコンピューターのユーザーが、承認済みソースからそのプログラムをインストールできるようにします。承認できるのは、ウイルス対策、スパイウェア対策、パーソナル ファイアウォール、デスクトップ生産性向上プログラムなど、よく使用されるエンタープライズ アプリケーションのアップデーター プログラムです。すべてのコンピューターが承認済みアップデーターを実行できますが、こうしたアップデーターにより Web 経由でインストールされたアプリケーションは、インストール コンピューターでのみ使用されるように、Bit9 エージェントによってローカルで承認されます。

プラットフォームに関する注意：アップデーターは、プラットフォームに固有です。アップデーターのほとんどがデフォルトで無効になっていますが、有効にできます。バージョン 7.2.1 より前では、Mac および Linux の組み込みアップデーターはリストされていませんでしたが、自動的に有効になっていました。こうしたアップデーターは現在個別のアップデーターとしてリストされ、デフォルトで無効になっているため、環境を制御しやすくなりました。Mac App Store Downloads はデフォルトで有効になっている数少ないアップデーターの 1 つですが、これも無効にできます。

標準の［Updaters（アップデーター）］タブには、3 つのタイプの「アップデーター」が表示されます。

- 特定の製品または製品ファミリー向けアップデーター（「Google Chrome」など）。
- 専用アイテム。ソフトウェア配布システムからのファイルの書き込みを許可する「アップデーター」など（例：「Microsoft SCCM」）。
- 「アップデーター」の中には、実際は特別な Bit9 機能の配信メカニズムであるものがあります。たとえば、Bit9 Server と Carbon Black センサーそれぞれに対する、一連の改ざんからの保護ルールである「アップデーター」があります。こうしたアップデーターは追加保護を実現するために有効にしたり、サーバーやエンドポイントで実行する必要があるアクティビティを妨げている場合は無効にしたりできます。

製品固有のアップデーターを有効にした場合、承認されるのはその製品の「アップグレード手順」のみであることに注意してください。アプリケーションのインストール パッケージ全体が承認されるわけではありません。

新しいアプリケーションまたは新しいアプリケーション バージョンが導入され、前の製品やバージョンが古くなると、必要なアップデーターのリストも変わる場合があります。使用可能なアップデーターのリストは、次の方法で更新されます。

- 新しいバージョンの Bit9 Security Platform をインストールすると、アップデーターのリストが更新され、新しいアップデーターが追加されます。また、古いアップデーターが削除され、既存のアップデーターは必要に応じて変更されます。
- アップデーターを常に最新の状態に保つには、Bit9 SRS によるアップデーターの自動更新を有効にします（Bit9 SRS が有効の場合は、デフォルトで有効になっています）。
- 現在サポートされていない更新プログラムについては、リストに追加するよう Bit9 にリクエストしてください。承認され使用可能になった新しいアップ

データーは、手動で Bit9 Server に追加するか、Bit9 SRS で自動ダウンロードできます。

注意

不要なファイル ブロックが行われないように、Bit9 エージェントをインストールする前に、組織で実行されているアプリケーションすべてに対して、サポートされているすべてのアップデーターを有効にすることをお勧めします。有効になっていないアップデーターがファイルを変更しようとして、アプリケーションがブロックされた場合は、グローバル承認またはローカル承認方法を使用して、ブロックされたファイルを手動で承認できます。

サーバーで使用できるアップデーターの一覧を表示するには、コンソールで［Software Rules Updaters（ソフトウェア ルール アップデーター）］ページを開きます。このページには、サポートされている v7.2.3 アップデーターのほか、手動で追加されたアップデーターや、前に有効にした古いアップデーター（前の Bit9 (Parity) バージョンからアップグレードした場合）が表示されます。

表 38 は、名前によって用途を判断できないアップデーターや、特別な実装情報が必要なアップデーターに関する情報を示しています。Bit9 コンソールにアクセスできない場合、サポートされているアップデーターの一覧が必要なときは、Bit9 テクニカル サポートにお問い合わせください。

表 38：アップデーターに関する情報

アップデーター	プラットフォーム	説明
注意：この表は、追加説明が必要なアップデーターについてのみ説明しています。アップデーターの一覧については、コンソールの［Software Rules/Updaters（ソフトウェア ルール / アップデーター）］ページを確認してください。		
Adobe Application Manager	Windows	Adobe Application Manager で「管理」されている製品の更新を許可します。
Adobe Products Not Listed	Windows	特定の Bit9 アップデーターが表示されない、特定の Adobe 製品に対する更新の自動承認を許可します。
Allow Printer Installations	Windows	現在エージェント コンピューターにないプリンター ドライバーの自動インストールを印刷サーバーに許可します（Windows 2003 以降）。このアップデーターは、ローカルに接続されたプリンターのドライバーのインストールを許可する手段として有効にしないでください。
Bit9 Server Tamper Protection	Windows	この「アップデーター」は Bit9 Server を改ざんから保護する一連のルールです。デフォルトで無効になっていますが、追加保護のために有効にすることをお勧めします。トラブルシューティングの目的で、必要に応じて、後で無効にすることもできます。

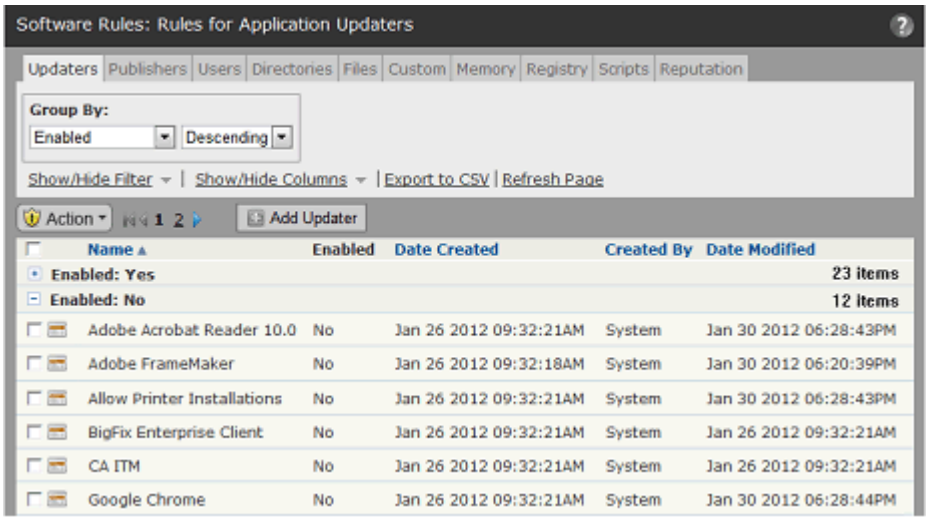
アップデーター	プラットフォーム	説明
Carbon Black	Mac	OS X が実行されているエンドポイントで Carbon Black センサーに対する更新を許可します。
Carbon Black Tamper Protection	Windows	この「アップデーター」は Carbon Black センサーを改ざんから保護する一連のルールです。Bit9 エージェントと Carbon Black センサーの両方がエンドポイントにインストールされている場合、このアップデーターを有効にすると、追加保護が実現します。
CSC.exe Temporary Files - Do Not Report	Windows	このアップデーターは、一時ファイル専用の場所で Microsoft Visual C# Compiler (CSC.exe) によって DLL が作成または変更されるときに、サーバー上の新しいファイルのレポート数を大幅に減らします。この「アップデーター」を有効にしても、その場所で引き続きファイルを承認または禁止できます。このプロセスの一時ファイルのトラフィックすべてを確認する必要がある場合は、このアップデーターを無効にします。
Java	Windows	Java 仮想マシンに対する更新と、一部の Java バージョンに含まれるアドオン（検索バー、サード パーティ アプリケーションなど）をインストールまたはアップデートする更新を許可します。これは、以前のリリースの Java and Bundled Software アップデーターと同等です。
Mac System Updates	Mac	OS X オペレーティング システムに対する更新を許可します。 **注意 :** 7.2.1 より前のリリースでは、Mac System Updates は自動的に許可され、アップデーターはありませんでした。これらの更新を許可するかどうかを制御できるようになりました。
Microsoft .NET Framework	Windows	.NET Just-In-Time コンパイラの実行を許可します。.NET を必要とするアプリケーションを実行する場合に、有効にする必要があります。 **Windows Update** は **Windows Defender** と **Microsoft .NET** の両方の更新プログラムを提供しますが、いずれかの製品の更新プログラムを適切にインストールするには、Windows Update のほかに、固有のアップデーターを信頼する必要があります。
Microsoft Office 2013	Windows	Microsoft クイック実行ストリーミング技術に基づいた更新を許可します。クイック実行を有効にせずに、Office の MSI インストーラーを使用した場合は、Windows Update によって Office の更新が提供されます。このアップデーターを有効にする必要はありません。

アップデーター	プラットフォーム	説明
Red Hat Prelinking	Linux	RedHat および CentOS コンピューターでは、エージェントをインストールする前にPrelinkingを無効にすることをお勧めします。Prelinking は Bit9 機能のパフォーマンスを低下させます（リリース ノートを参照してください）。RedHat または CentOS システムでPrelinkingを有効にする必要がある場合は、エージェントをインストールする前に RedHat Prelinking アップデーターを有効にします。
Red Hat Software Update	Linux	サポートされている RedHat および CentOS オペレーティング システムに対する自動更新を許可します。
Symantec Endpoint Protection for Mac	Mac	環境で SEP が実行されている場合に、**Symantec Endpoint Protection for Mac** アップデーターを有効にします。SEP 更新が許可され、ファイル操作のパフォーマンスが向上します。SEP Auto Protect Preferences Pane を使用して、次のエンドポイント SafeZone を含めるように SEP を構成します。**/Library/Application Support/com.bit9.Agent**
Ubuntu Software Update	Linux	サポートされているUbuntuオペレーティング システムに対する自動更新を許可します。
Windows 8, 10 and Server 2012 Updates	Windows	7.0.1 より前の Patch 11 エージェントで、これらのプラットフォームに対する更新を許可します。この更新プログラムは、すべての 7.2.x エージェントと、7.0.1 の場合は Patch 11 以降のエージェントで自動的に有効になります。
Windows Defender	Windows	**Windows Update** は **Windows Defender** と **Microsoft .NET** の両方の更新プログラムを提供しますが、いずれかの製品の更新プログラムを適切にインストールするには、Windows Update のほかに、固有のアップデーターを信頼する必要があります。 **注意 :** 他の AV 製品がインストールされていない限り、Windows 10 では Windows Defender がデフォルトで有効になっています。

アップデーター	プラットフォーム	説明
Windows Update（6.0.2 より前のエージェント）	Windows	このアップデーターによって、6.0.2 より前のエージェントでの Windows Updates の実行が許可されます。v6.0.2 以降のエージェントでは、Windows Updates がデフォルトで有効になっています。
Windows Update Temporary Files - Do Not Report	Windows	このアップデーターは、Windows の更新が適用されるときに、サーバー上の新しいファイルのレポート数を大幅に減らします。レポートされないファイルは一時的な場所にあり、Microsoft によって提供されるため、追跡や調査の対象にはなりません。この「アップデーター」を有効にしても、その場所で引き続きファイルを承認または禁止できます。アップデーター ファイルのトラフィックすべてを確認する必要がある場合は、このアップデーターを無効にします。

アプリケーション アップデーターによってインストールされたソフトウェアの自動承認を指定する手順：

1. コンソール メニューで、[**Rules**（ルール）] > [**Software Rules**（ソフトウェア ルール）] の順に選択します。[Software Rules（ソフトウェア ルール）] ページが表示されます。
2. [**Updaters**（アップデーター）] タブをクリックします。さまざまなアプリケーションのアップデーター プログラムのテーブルが表示されます。デフォルトでは、アップデーターは有効かどうかに基づいてグループ化されています。



3. 現在無効になっているアップデーターのうち、有効にするアップデーターの行の左端にあるボックスをオンにして、[Action（アクション）] メニューの [**Enable Updaters**（アップデーターを有効にする）] を選択します。そのアップデーターが有効になり、デフォルトのグループ化が適用されている場合、[Enabled: Yes（有効化：はい）] セクションに移動されます。Bit9 エージェントが実行されているコンピューターが、そのアプリケーションの自動アップデーターを使用して、ソフトウェアをインストールできるようになります。

   注意

   ソフトウェア メーカーによっては、同じ製品ファミリーに複数の製品が含まれていることがあります。選択したアップデーターが、使用しているアプリケーションに適した製品とバージョンに対応しているかどうかを確認してください。

4. アップデーターの変更、追加、および削除に合わせてアップデーター リストを更新し、常に最新の状態が維持されるようにするには、「アップデーターのオプション」を有効のままにしておきます。「アップデーターの自動更新の有効化または無効化」（305 ページ）を参照してください。
5. 必要なアップデーターがテーブルに表示されていない場合は、Bit9 テクニカル サポートに新しいアップデーターのリクエストを送信できます。アップデーター追加の詳細については、「アップデーターの追加」（306 ページ）を参照してください。
6. アップデーターを無効にするには、無効にするアップデーターの名前の横にあるボックスをそれぞれオンにして、[Action（アクション）] メニューの [**Disable Updaters**（アップデーターを無効にする）] を選択します。

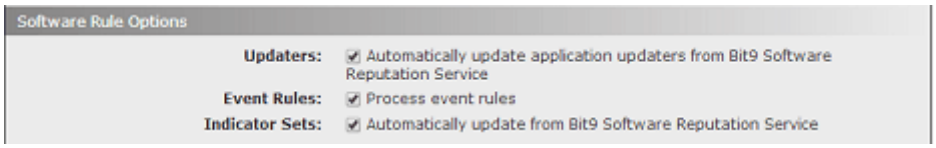
アップデーターの自動更新の有効化または無効化

ソフトウェア プロバイダーによる製品または製品バージョンの変更により、必要なアップデーターのリストが変更される可能性があります。Bit9 は、サポートされる製品のアップデーターに対する変更と、製品独自のアップデーターを含む新製品のリリースを追跡します。新しいバージョンの Bit9 Security Platform をインストールすると、その変更を適用するためにアップデーター リストが変更されますが、そのアップデーター リストは、リリース間で更新しなければならないこともあります。

Bit9 SRS にアップデーター リストの管理を許可すると、新しいアップデーターと変更されたアップデーターは、Bit9 から使用できるようになった時点で入手することができます。また、Bit9 SRS の更新を有効にすることで、古いアップデーターがアップデーター リストから削除されます。自動更新により、アップデーター リストを常に最新の状態に維持できるほか、リスト上のアップデーターを手動で更新する必要がほとんどなくなります。Bit9 SRS が有効の場合、この機能はデフォルトで有効になっていることに注意してください。

Bit9 SRS によるアップデーターの自動更新を有効または無効にする手順：

1. コンソール メニューで、[**Administration**（管理）] > [**System Configuration**（システム構成）] の順に選択します。
2. [システム構成] ページで、メニューの [**Advanced Options**（高度なオプション）] をクリックします。[Advanced Options（高度なオプション）] ページが表示されます。下部には [Software Rules Options（ソフトウェア ルール オプション）] パネルがあります。
3. ページ下部で、[**Edit**（編集）] ボタンをクリックします。
4. [Software Rule Options（ソフトウェア ルール オプション）] パネルでは、Bit9 SRS updater オプションがデフォルトで有効になっています。
   a. Bit9 SRS でアップデーターを常に最新の状態に保つ必要がない場合は、[Automatically update application updaters from Bit9 SRS（Bit9 SRS からアプリケーション アップデーターを自動更新）] ボックスをオフにして、ページ下部の [**Update**（更新）] ボタンをクリックします。
   b. 無効にした Bit9 SRS からの自動更新を再度有効にするには、このボックスをオンにして、[**Update**（更新）] ボタンをクリックします。



5. [Confirm Server Setting Change（サーバー設定の変更の確認）] ダイアログで、[**Yes**（はい）] をクリックして変更を保存します。

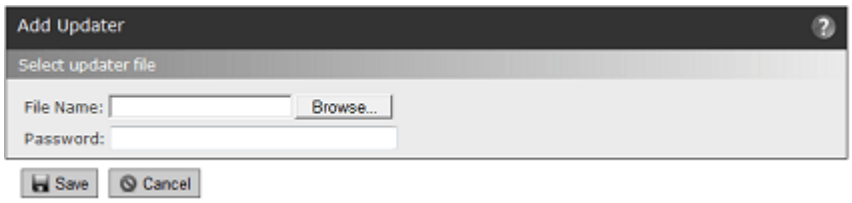
アップデーターの追加

現在の [Updaters（アップデーター）] テーブルにないアプリケーションまたはソフトウェア配布アップデーターが必要な場合は、Bit9 テクニカル サポートに新しいアップデーターのリクエストを送信できます。リクエストが受理されると、新しいアップデーターは次のいずれかの方法で提供されます。

- アップデーターの Bit9 SRS 更新が有効になっている場合は、準備ができた時点で Bit9 Server に自動的にインストールされます。
- 更新ファイルとして Bit9 により提供されます。

Bit9 提供のファイルから新しいアップデーターをインストールする手順：

1. サポート エンジニアの指示に従ってアップデーター ファイルをダウンロードし、Bit9 Server がアクセスできる場所に配置します。
2. コンソール メニューで [**Rules**（ルール）] > [**Software Rules**（ソフトウェア ルール）] の順に選択し、[**Updater**（アップデーター）] タブをクリックします。
3. [**Add Updater**（アップデーターを追加）] ボタンをクリックします。[Add Updater（アップデーターの追加）] ページが表示されます。



4. ［**Browse**（参照）］ボタンをクリックして、新しいアップデーターを見つけ、ファイル選択ツールで［**Open**（開く）］をクリックします。ファイルのパス名が［File name（ファイル名）］ボックスに表示されます。
5. ［**Save**（保存）］ボタンをクリックします。新しいアップデーターがインストールされますが、有効にはなりません。
6. 新しいアップデーターを有効にするには、名前の左側にあるボックスをオンにし、［Action（アクション）］メニューの［**Enable Updaters**（アップデーターを有効にする）］を選択します。アップデーターは、［Enabled: Yes（有効：はい）］セクションに移動されます。ユーザーはこのアプリケーションのアップデーターを使用して、ソフトウェアをインストールできるようになります。

アップデーターの履歴

アップデーターの履歴を表示すると、そのアップデーターが最新かどうか、および変更がいつ行われたかを確認できます。たとえば、履歴の［Date Created（作成日）］フィールドは、Bit9 SRS によって新しいアップデーターが追加されたことを示している可能性があります。

アップデーターの履歴を表示する手順：

- ［Updaters（アップデーター）］タブで、アップデーターの名前の横にある［View History（履歴を表示）］ボタンをクリックします。［**Return**（戻る）］ボタンをクリックすると、アップデーターの一覧に戻ります。

履歴ページには、次のアップデーター情報が表示されます。

- アップデーター名
- プラットフォーム
- 有効かどうか（はい / いいえ）
- アップデーターのバージョン番号
- （この Bit9 Server での）作成日
- （この Bit9 Server での）作成者
- アップデーターに対する変更の履歴

［Updater History（アップデーターの履歴）］の［Related Views（関連ビュー）］メニューを使用すると、どのエージェント管理コンピューターに、このアップデーターの最新ルールが適用されているかを確認できます。

ファイルのローカル承認

Bit9 エージェントが初めてコンピューターにインストールされるとき、そのコンピューター上のすべてのファイルは、グローバル承認または禁止されていない限り、「初期化」プロセス中に「ローカル承認」されます。つまり、適用レベルに関係なく、そのコンピューターでのファイルの実行が許可されます。ただし、ローカル承認は、ファイルの「グローバル状態」には影響しません。エージェントの初期化中にファイルがローカルで承認されるため、実行する必要があるファイルを使ってコンピューターを設定し、そのファイルに関するグローバルな決定は後で Bit9 Security Platform を使用してファイルとコンピューターの詳細を収集し終わってから行うことができます。

Bit9 エージェントの初期化後にコンピューターに現れたファイルは、明示的に禁止または承認されていなければ、「未承認」状態が割り当てられます。未承認のファイルは、低適用レベルおよび（ユーザー介入を伴う）中適用レベルで実行されているコンピューターでの実行が許可されますが、高適用レベルのコンピューターでは実行できません。

特定のコンピューターのみが新しいアプリケーションを実行できるように指定できます。その際、ネットワーク上の他のコンピューターでそのアプリケーションを承認する必要はありません。1 台以上のコンピューターを高適用レベルに変更する前に、そのコンピューター上のファイルの状態を未承認からローカル承認に変更することもできます。これを実現するために、Bit9 Security Platform には次のオプションが用意されています。

- コンピューターをさらに安全な適用レベルに移行するときに、特定の未承認ファイルをポリシー単位でローカル承認に変更可能
- 特定のコンピューターにある個別のファイルをローカル承認
- 特定のコンピューターにあるすべての未承認ファイルをローカル承認
- インストールされているファイルがローカルで承認されているときに、高適用レベルまたは中適用レベルのコンピューターを、ローカル承認ポリシーに一時的に再割り当て
- Bit9 分析で特定できなくてもファイルをインストーラーとして指定(その逆も同様)。インストーラーをローカル承認すると、そのインストーラーによってインストールされたすべてのファイルがローカルで承認されます

注意

- こうした方法では、グローバルに禁止されたファイル、またはコンピューター上でポリシーによって禁止されたファイルをローカル承認することはできません。また、グローバルに承認されたファイル、またはコンピューター上でポリシーによって承認されたファイルのローカル承認を削除することもできません。
- 公開者の承認など、承認方法によっては、ファイルのすべてのインスタンスがローカルで承認されます。これについては、このセクションでは説明しません。ファイル状態への公開者承認の影響の詳細については、「公開者による承認または禁止」（288 ページ）を参照してください。
- コンピューターをローカル承認ポリシーに再割り当てするにはフル スイート ライセンス（可視性と制御）が必要です。可視性のみのライセンスのサイトでは再割り当てを実行できません。

適用レベル変更時の自動ローカル承認

Bit9 セキュリティ ポリシーには［Advanced Setting（高度な設定）］があり、これはデフォルトで有効になっています。つまり、Bit9 エージェントのポリシーが低適用レベルまたは適用レベルなし（可視性）のときに検出された未承認ファイルが、そのポリシーの適用レベルが「中」または「高」になったときにローカル承認されます。

未承認ファイルの自動ローカル承認により、低適用レベルのときに新しいファイルをインストールし、その後、より厳しい適用レベルに変更できます。移行時に存在していたファイルの実行が制限されることはありません。明示的に禁止したファイルは禁止されたままになり、中または高適用レベルの際に検出された未承認ファイルについては、適用レベルの移行中は未承認のままです。

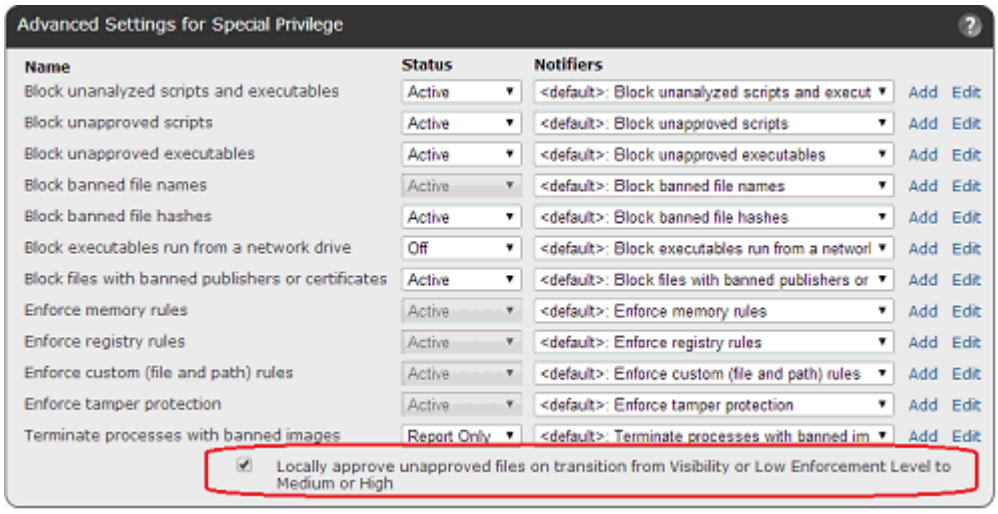
この機能は、必要に応じて、ポリシー単位で無効にできます。これにより、移行前にエージェントに既にある未承認ファイルの意図しない実行に対するセキュリティが強化されますが、移行後に低リスクのソフトウェアがブロックされることが多くなる可能性もあります。自動ローカル承認を有効にしない場合は、承認しなければならない個別のファイル数を減らすことができる、他の一括承認方法を検討してください。

注意

適用レベルの変更は、コンピューターがポリシーを変更したり、ポリシー自体の適用レベルが変わったりしたときに発生します。コンピューターがポリシーを変更した場合、移行の承認を行うかどうかを判断する基準となるのは、「変更元のポリシー」の設定です。「変更先のポリシー」の設定ではありません。

適用レベル変更時の未承認ファイルの自動ローカル承認を無効にする手順：

1. コンソール メニューで、［**Rules**（ルール）］>［**Policies**（ポリシー）］の順に選択します。［Policies（ポリシー）］ページが表示されます。
2. 変更するポリシーの名前の横にある［View Details（詳細の表示）］（鉛筆）ボタンをクリックします。そのポリシーの［Edit Policy（ポリシーの編集）］ページが表示されます。
3. ［**Show Advanced Settings**（高度な設定の表示）］ボタンをクリックします。［Advanced Settings（高度な設定）］パネルが表示されます。



4. ［Advanced Settings（高度な設定）］パネルの下部にある［Locally approve unapproved files on transition from Visibility or Low Enforcement Level to Medium or High（可視性または低適用レベルから中適用レベルまたは高適用レベルへの移行中に未承認ファイルをローカルで承認)］チェックボックスをオフにします。
5. ［**Save**（保存)］ボタンをクリックします。
6. 変更する他のポリシーについて、手順 2 ～ 5 を繰り返します。

自動ローカル承認を再度有効にするには、このチェックボックスをオンにします。

移行中にローカル承認されるファイル

ローカル「未承認」ファイルには 2 つのタイプがあり、ローカル状態の詳細がそれぞれ異なります。

- ローカル状態の詳細が「未承認」のファイルは、適用レベルが「なし（可視性)」または「低」のシステムで検出されました。このファイルは、適用レベルを「中」または「高」に変更することでローカル承認されます。
- ローカル状態の詳細が「未承認（永続的)」のファイルは、適用レベルが「中」または「高」のシステムで検出されました。このファイルは、移行中も未承認のままです。

ローカル状態の詳細は、［Files（ファイル)］ページか、［Find File（ファイルの検索)］の結果（複数ファイルの場合）または［File Instance Details（ファイル インスタンスの詳細)］ページ（1 つのファイルの場合）で確認できます。いずれかのテーブルに［Local State Details（ローカル状態の詳細)］列が表示されていない場合は、その列を追加します。

ポリシーについては、［Edit Policy（ポリシーの編集）］ページの［Related Views（関連ビュー）］メニューに、［**Unapproved files from computers in this policy**（こ

のポリシーのコンピューターの未承認ファイル)］リンクがあり、このリンクをクリックすると、［Find Files（ファイルの検索)］ページが開き、そのファイルの検索結果が表示されます。このリストを表示しておくと、未承認ファイルのローカル承認に影響するアクションを実行するときに役に立つ場合があります。

個別のファイルのローカル承認

Bit9 エージェントの初期化中に存在していたと思っていたファイルがなく、その結果、そのファイルがローカル承認されていないことがわかったとします。見つからないファイルは、スタンドアロンの実行可能ファイルである場合があります。そのファイルがないために、アプリケーションを実行できない可能性もあります。見つからないファイルを特定できる場合は、そのファイルをコンピューターに配置すれば、インスタンス単位でローカル承認できます。

ローカル承認は、ファイル インスタンスが表示されている次のコンソール テーブルから実行できます。

- ［Files（ファイル)］ページの［Files on Computer（コンピューター上のファイル)］タブ。このタブには、ネットワーク上のすべてのエージェント管理コンピューターにある、追跡対象ファイルのインスタンスが表示されます
- ［Baseline Drift Report Results（ベースライン ドリフト レポートの結果)］ページのファイル ビュー
- 検索結果が表示されている［Find Files（ファイルの検索)］ページ

注意

1 台のコンピューターで特定のファイルを検索している場合は、コンピューター フィルターをファイルの検索クエリに追加し、そのコンピューターの名前を入力します。これにより、探しているファイルは、入力したコンピューターでのみ検索されます。

これらのページのいずれかでフィルターを使用すると、必要なファイルの正確なリスト、または特定のファイルを取得できます。

ファイル テーブルから個別のファイル インスタンスをローカル承認する手順：

1. ファイル テーブルでローカル承認するファイル インスタンスを見つけます。
2. テーブルで、ローカル承認するファイル インスタンスの左側にあるボックスをそれぞれオンにします。各ファイルの横にあるコンピューター名が対象のコンピューターであることを確認します。
3. ［Action（アクション)］メニューで、［**Approve Locally**（ローカルで承認)］を選択します。オンにした各ファイルのローカル状態は、そのファイルが現れたコンピューターに対して［Locally Approved（ローカルで承認済み)］になります。

注意

ファイルをローカル承認する前に、そのファイルの詳細を確認するには、ファイル テーブルの［View Details（詳細の表示）］（鉛筆）ボタンをクリックして、［File Instance Details（ファイル インスタンスの詳細）］ページを表示します。ファイルがまだグローバルまたはローカル承認されていない場合は、このページの［Actions（アクション）］メニューにも［**Approve Locally**（ローカルで承認）］が表示されます。

ローカル承認の削除

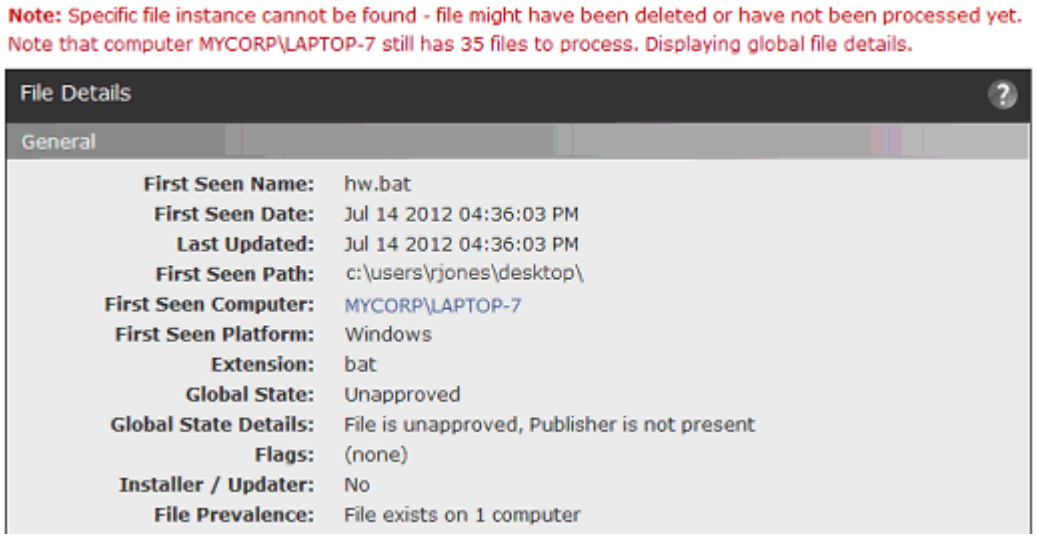
個別のファイルをローカル承認できるように、ローカルで承認されたファイルからローカル承認を「削除」することができます。この操作は、Bit9 エージェントの初期化時にコンピューター上で本当はファイルを承認する必要がなかった場合、または初期化後のいずれかの方法でファイルを誤って承認した場合に行うことができます。承認が必要だったときと同じ方法でファイルを見つけ、次のいずれかの操作を行います。

- ファイル テーブル（［Files（ファイル）］ページ、［Find Files（ファイルの検索）］ページ、［Baseline Drift Report Results（ベースライン ドリフト レポートの結果）］）で、削除するローカル承認が含まれるファイルの横にあるボックスをそれぞれオンにし、［Action（アクション）］メニューの［Remove Local Approval（ローカル承認を削除）］を選択します。
- ［File Instance Details（ファイル インスタンスの詳細）］ページで、［**Remove Local Approval**（ローカル承認を削除）］リンクをクリックします。

ファイル カタログ インベントリにないファイルのローカル承認

エージェントによって新しいファイルが検出されると、サーバーとコンソールが効率的に動作できるように、サーバーへのファイル インスタンス追加がバックグラウンドで処理されます。このため、ファイルがファイル インスタンスとして実際に［Files on Computers（コンピューター上のファイル）］ページに表示される前に、［Events（イベント）］ページが、コンピューターで新しいファイルが検出されたことをレポートする可能性があります。

［Event（イベント）］ページからファイルをローカル承認するには、そのページの［Action（アクション）］メニューで［Approve Locally（ローカルで承認）］を選択します。［Event Description（イベントの説明）］でハイライト表示されているファイル パスをクリックして、［File Details（ファイルの詳細）］ページに移動することもできます。完全に処理されていないファイルに対してこの操作を行うと、［File Details（ファイルの詳細）］ページの上部にコメントが表示されます。



ファイルが見つかっていなくても、[File Details（ファイルの詳細）] ページの [Actions（アクション）] メニューから [Approve Locally（ローカルで承認）] コマンドを使用できます。

一時ファイルまたは削除済みファイルのローカル承認

特定のタスクを実行するために、コンピューター上にファイルが短い間だけ現れる場合があります。たとえば、プリンター ドライバーをインストールしている場合は、ドライバーをインストールしている間だけ一時ファイルが現れ、その後このファイルは消えます。このファイルは [Files on Computers（コンピューター上のファイル）] ページに表示されませんが、特定のコンピューターでこのドライバーのインストールが Bit9 によってブロックされないように、ハッシュによってローカル承認できます。

エージェント コンピューターに存在するのに、完全には登録されていないファイルと同様、一時ファイルまたは削除済みファイルをローカルで承認するには、[Events（イベント）] ページの [Action（アクション）] メニューまたはファイルの [File Details（ファイルの詳細）] ページの [Actions（アクション）] メニューを使用します。手動でローカル承認されたファイルについては、そのローカル承認は、今後同じコンピューターに現れるそのファイルのすべてのインスタンスに対して無期限に、つまりインスタンスが削除された後も保持されます。他のルール（公開者の承認など）でローカル承認されたファイルのローカル承認は数日後に期限切れになります。

注意

コンピューターに現在存在していないファイルのローカル承認は「削除」できません。

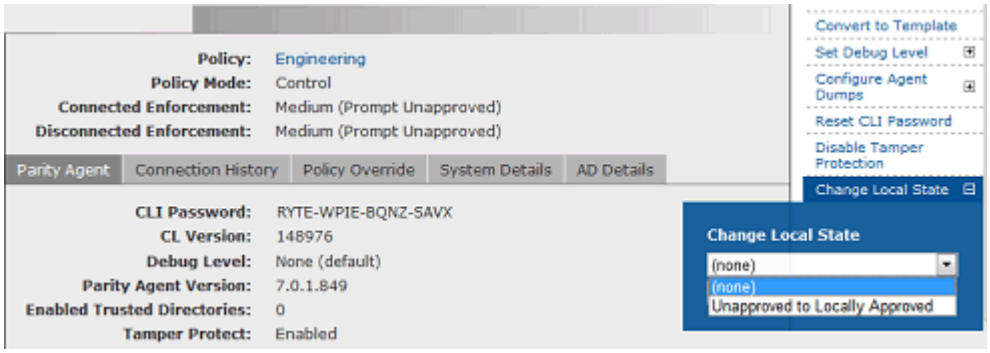
コンピューター上にあるすべての未承認ファイルのローカル承認

Bit9 Security Platform には、選択したコンピューター上にあるすべての未承認ファイルをローカルで承認するためのメカニズムが用意されています。この操作は、初期化後、コンピューターに既知の良好なファイルを多数追加した場合に行うこ

とができます。追加したファイルは、(明示的に禁止またはグローバルで承認されていなければ) 未承認状態になります。

コンピューター上にあるすべての未承認ファイルを「ローカルで承認済み」に変更する手順：

1. コンソール　メニューで、[**Assets**（アセット）] > [**Computers**（コンピューター)] の順に選択します。
2. 変換する未承認ファイルがあるコンピューターの名前をクリックします。そのコンピューターの [Computer Details（コンピューターの詳細)] ページが表示されます。
3. ページの右下にある [Advanced (詳細)] メニューで [**Change Local State** (ローカル状態を変更)] をクリックし、[Change Local States (ローカル状態の変更)] メニューから [**Unapproved to Locally Approved**（未承認からローカル承認)] を選択して、[Go (実行)] ボタンをクリックします。コンピューター上のローカル状態が「未承認」だったすべてのファイルが「ローカルで承認済み」になります。



ローカル承認モードへのコンピューターの移行

> **注意**
> コンピューターをローカル承認モードに再割り当てするにはフルスイート ライセンス（可視性と制御）が必要です。可視性のみのライセンスのサイトでは再割り当てを実行できません。

高適用レベルで選択したコンピューターに新しいアプリケーションをインストールできるようにするには、一時的に保護を緩め、禁止されていないすべてのファイルをコンピューターで実行できるようにします。これを行う方法は、コンピューターが Bit9 Server に接続されているかどうかによって異なります。

- **オンライン コンピューターの場合**：Bit9 コンソールを使用して、ソフトウェアのインストールが完了するまでコンピューターを他の適用レベルに移行し、完了した時点で戻すことができます。このオプションについては、セクション「ローカル承認モードへのオンライン コンピューターの移行」(315 ページ)で説明しています。
- **オフライン コンピューターの場合**：Bit9 コンソールを使用して、コンピューターで使用するシステム固有のパスワードを生成し、指定した期間だけその

コンピューターを他の適用レベルに移行できます。このオプションについては、セクション「期限付きポリシーへの一時変更の使用」（318 ページ）で説明しています。

いずれの場合も、ローカル承認モードは一時的なもので、期限付き適用レベルに一時的に変更できる時間は指定されています。ただし、オンライン コンピューターについては、「ローカル承認モードからのオンライン コンピューターの復元」（318 ページ）で説明するように手動で戻す必要があります。

コンピューターを元の適用レベルに戻した後は、コンピューターがローカル承認モードになる前に未承認で、「ローカル承認モードで実行されなかった」ファイルはすべて未承認のままです。以前に未承認で、コンピューターがローカル承認モードの間に実行またはインストールされたファイルは、コンピューター上でローカル承認されていますが、「グローバル」状態は引き続き未承認です。

高適用レベルと中適用レベルの両方からローカル承認に移行できます。中適用レベルでも未承認ファイルを実行できますが、ローカル承認を使用することで、未承認ファイルを実行しようとするときに通知に応答する必要がなくなります。

ローカル承認モードへのオンライン コンピューターの移行

ローカル承認モードを使用すると、モード変更の前にコンピューターに存在していたファイルや、コンピューターが通常のポリシーに戻った後にインストールされたファイルのローカル状態に影響を与えずに、新しいファイルをインストールしてローカル承認できます。これは、コンピューターにインストールする必要がある新しいファイルをまだ導入していない場合に役に立ちます。

Bit9 コンソールを使用して、ソフトウェアのインストールが完了するまで、「オンライン」コンピューターを事前定義されたローカル承認ポリシーに移行できます。ローカル承認ポリシーでは、コンピューター ユーザーが、高適用レベルまたは中適用レベルのために以前ブロックされていた未承認アプリケーションをインストールし、実行できます。ただし、禁止されたファイルについては、実行は引き続き禁止およびブロックされます。

インストールが完了したら、コンピューターを元のポリシーに復元できます（復元する必要があります）。復元しても、適用レベルを緩めたときにインストールされローカル承認されたファイルはすべて、引き続き実行することができます。

注意

- 未承認ソフトウェアをインストールできるのは、低適用レベル ポリシーのコンピューターです。ただし、特にコンピューターを後で高適用レベルに後で移行する場合は、コンピューターをローカル承認に移行して、既知の良好なファイルを承認することをお勧めします。
- ローカル承認で唯一アクティブな［Device Control（デバイス制御）］設定は、［Block writes to banned removable devices（禁止リムーバブル デバイスへの書き込みをブロック）］と［Block executes from banned removable devices（禁止リムーバブル デバイスからの実行をブロック）］です。他の設定はすべて［Off（オフ）］になっています。

コンピューターをローカル承認モードに移行する方法は複数あり、いずれの方法でもコンピューターを前のポリシーに復元できます。

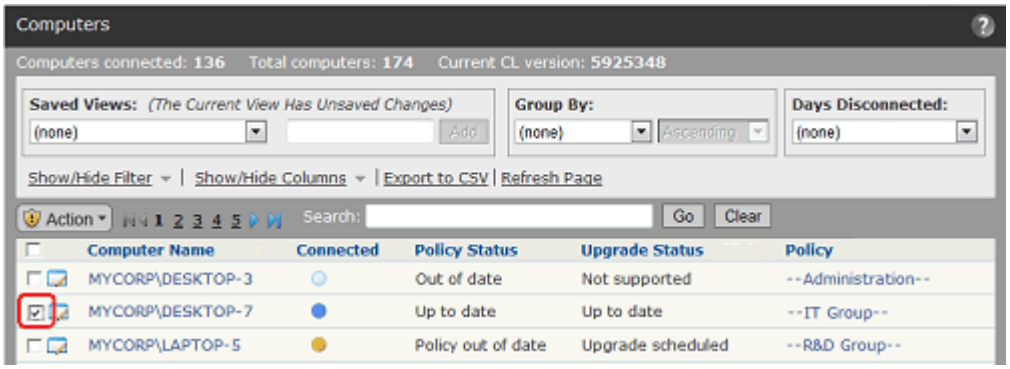
- ［Computers（コンピューター）］ページでは、1 台以上のコンピューターをまとめてローカル承認モードに移行できます。
- ［Computer Details（コンピューターの詳細）］ページの［Action（アクション）］メニューを使用すると、高適用または中適用からローカル承認に 1 台のコンピューターを移行できます。
- コンソールのホーム ページ（または他のダッシュボード）の［Change Policy（ポリシーの変更）］ポートレットを使用して、1 台のコンピューターをローカル承認モードに移行できます。

ローカル承認モードには、監視および制御の特別な機能がいくつか用意されています。

- どのマシンがローカル承認モードになっているかを追跡するには、［Computers（コンピューター）］ページの［Saved View（保存済みビュー）］で［Computers in Local Approval（ローカル承認のコンピューター）］を選択します。
- コンピューターがローカル承認されている時間が、指定した時間を超えたときにトリガーするアラートを設定できます。詳細については、「Bit9 アラートの使用」（606 ページ）を参照してください。
- ［Computers（コンピューター）］ページの［Action（アクション）］メニューで［Restore to Normal Enforcement Level（標準の適用レベルに復元）］コマンドを使用すると、ローカル承認モードに手動で移行したコンピューターを、そのコンピューターの標準の適用レベルに簡単に戻すことができます。

1 台以上のオンライン コンピューターをローカル承認モードに移行する手順：

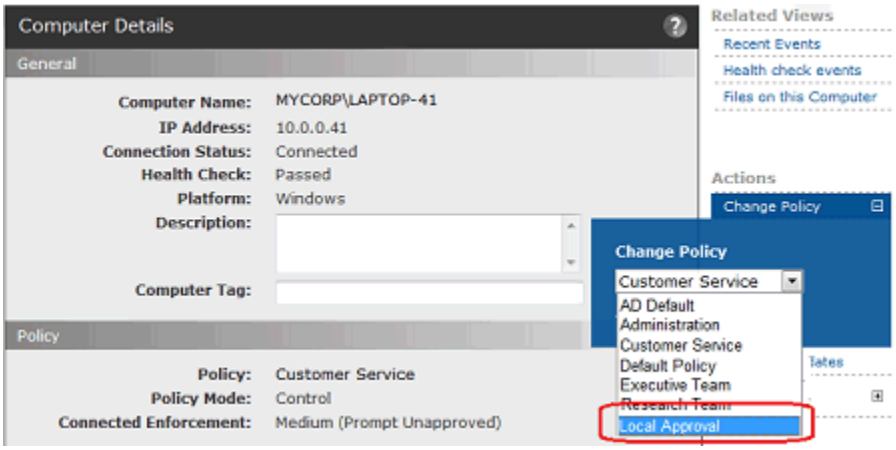
1. コンソール メニューで、［**Assets**（アセット）］>［**Computers**（コンピューター）］の順に選択します。［Computers（コンピューター）］ページが表示されます。
2. ［Computers（コンピューター）］テーブルで、ローカル承認モードに移行するコンピューターを見つけます。表示されるコンピューターの数を減らすには、［Show/Hide Filters（フィルターを表示 / 非表示）］ボタンを使用して、ポリシーまたはその他の関連フィールドにフィルターを適用します。［Search（検索）］ボックスに、コンピューター名の全体または一部を入力することもできます。
3. ローカル承認モードに移行するコンピューターの名前の横にあるチェックボックスをオンにします。



4. ［Action（アクション）］メニューで、［**Move to Local Approval**（ローカル承認に移行）］を選択します。コンピューターがローカル承認ポリシーに移行します。未承認ファイルを実行でき、デバイス制御は無効になります。ただし、ブロックされている禁止デバイスへの書き込みは除きます。
選択したコンピューターに低適用レベルのコンピューターが含まれていると、操作は失敗し、エラー メッセージが表示されます。
5. ［Computers（コンピューター）］ページの［Saved View（保存済みビュー）］で［**Computers in Local Approval**（ローカル承認のコンピューター）］を選択します。コンピューターがローカル承認ポリシーの一部としてテーブルに表示されていることを確認します。確認できた場合、コンピューター ユーザーはソフトウェアをそのシステムにインストールし、ローカル承認できます（グローバルに禁止または承認されていない場合）。唯一アクティブな［Device Control（デバイス制御）］設定は、［Block writes to banned removable devices（禁止リムーバブル デバイスへの書き込みをブロック）］です。

オンライン コンピューターをローカル承認モードに移行する手順（［Computer Details（コンピューターの詳細）］ページ）：

1. ［Computer Name（コンピューター名）］フィールドが表示されている任意のページで、名前をクリックします。そのコンピューターの［Computer Details（コンピューターの詳細）］ページが表示されます。
2. ［Actions（アクション）］メニューで、［**Change Policy**（ポリシーを変更）］をクリックします。［Change Policy（ポリシーの変更）］ダイアログが表示されます。
3. ［Change Policy（ポリシーの変更）］メニューで、［**Local Approval**（ローカル承認）］を選択し、［Go（実行）］ボタンをクリックします。コンピューターがローカル承認ポリシーに移行します。未承認ファイルが実行されます。唯一アクティブな［Device Control（デバイス制御）］設定により、リムーバブル デバイスへの書き込みとそのデバイスでの実行がブロックされます（高適用レベルおよび中適用レベルのコンピューターについてのみ、メニューに［Local Approval（ローカル承認）］が表示されます）。



4. ［Computer Details（コンピューターの詳細）］ページで、ポリシーがローカル承認に変更されていることを確認します。確認できた場合、コンピューターユーザーはソフトウェアをそのシステムにインストールし、ローカル承認できます（グローバルに禁止または承認されていない場合）。

ローカル承認モードからのオンライン コンピューターの復元

コンピューターをローカル承認モードに移行し、新しいアプリケーションをインストールしたら、通常、そのコンピューターはすぐに前のポリシーに復元する必要があります。ローカル承認への移行と同様、前のポリシーへの復元は、［Change Policy（ポリシーの変更）］ポートレット、［Computer Details（コンピューターの詳細）］ページ、または［Computers（コンピューター）］ページから行うことができます。ここでは［Computers（コンピューター）］ページを使う方法について説明します。

注意

以下で説明する方法は、オンライン コンピューターでのみ有効です。期限付き適用レベルに一時的に変更して、オフライン コンピューターをローカル承認モードに移行した場合、その期間が終了すると、コンピューターは自動的に標準の適用レベルに戻ります。その詳細については、「期限付きポリシーへの一時変更の使用」（318 ページ）を参照してください。

ローカル承認モードのコンピューターを前のポリシーに復元する手順：

1. コンソール メニューで、［**Assets**（アセット）］>［**Computers**（コンピューター）］の順に選択します。［Computers（コンピューター）］ページが表示されます。
2. ［Computers（コンピューター）］ページの［Saved View（保存済みビュー）］メニューで［**Computers in Local Approval**（ローカル承認のコンピューター）］を選択し、ローカル承認ポリシーにコンピューターが表示されていることを確認します。
3. テーブルで、復元するコンピューターの横にあるボックスをオンにします。複数のコンピューターを復元する場合は、1 つずつ選択します。
4. ［Action（アクション）］メニューで、［**Restore to Normal Enforcement Level**（標準の適用レベルに復元）］を選択します。コンピューターが前のポリシーに戻ります。そのコンピューターは、［Computers in Local Approval（ローカル承認のコンピューター）］ビューに表示されなくなります。

期限付きポリシーへの一時変更の使用

新しいアプリケーションを、高適用レベルで保護されている特定のコンピューターにインストールしなければならないことがあります。これを行うには、一時的に保護を緩めて、禁止されていないファイルを実行する許可をコンピューターに付与します。つまり、コンピューターにソフトウェアをインストールする間だけ、そのコンピューターを事前定義されたローカル承認ポリシーに移行します。

接続されていないコンピューターを Bit9 Server から直接制御することはできないため、他の方法で、他の適用レベルに移行するようエージェントに指示する必要

があります。エージェント管理コンピューターに入力できる特別なコードを生成すると、指定した時間だけ適用レベルを切り替えることができます。コードは 1 つのエージェントに固有で、使用できるのは 1 回だけです。生成したコードで、「なし（無効）」を除く任意の適用レベルにコンピューターを切り替えることができますが、この機能の主な目的は、ローカル認証モードへの一時的な移行です。

適用レベルの変更時間として指定できるのは最大 500 分です。

一時的に変更する期間として指定した時間が経過すると、コンピューターは自動的に元のポリシーに復元されます。一時的にローカル承認に移行していた間にインストールされたファイルはすべて、そのまま実行し続けることができます。ローカル承認ポリシーが適用されていたコンピューターで実行またはインストールされたファイルは、（グローバル、またはそのコンピューターのポリシーで禁止されていない限り）ローカル承認されていますが、「グローバル」状態は引き続き未承認です。

この期限付きポリシーへの一時的な変更は、特にオフラインのコンピューターで役立ちますが、オンラインのコンピューターでも使用できます。一時的に変更している間、エージェントの接続は切断されます。Mac および Linux コンピューターでは、一時的に変更されているときにエージェントまたはコンピューターが再起動されても、その状態は、指定した時間が経過するまで保持されます。

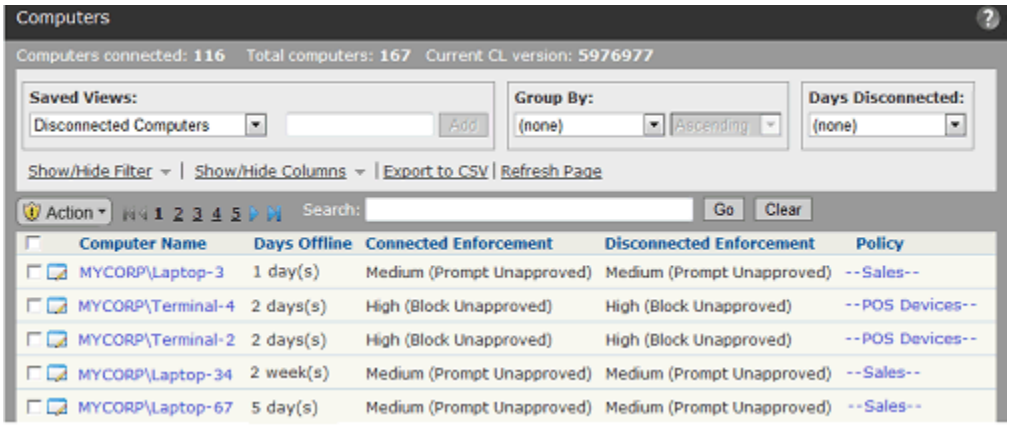
プラットフォームに関する注意：Bit9 Server に現在接続されている Windows コンピューターの場合、期限付き適用レベルに一時的に変更することはお勧めしません。一時的に変更されている間に Windows コンピューターまたはエージェントを再起動すると、その一時変更期間は終了します。一時変更機能を使ってアプリケーションをインストールしてローカル承認していた場合は、これによりインストールが中断され、必要なファイルのローカル承認が妨げられるため、アプリケーションが使用できなくなることがあります。この予期せぬ結果を避けるため、期限付き適用レベルに一時的に変更する場合、Windows クライアントと Bit9 Server の接続は物理的に切断してください。

警告

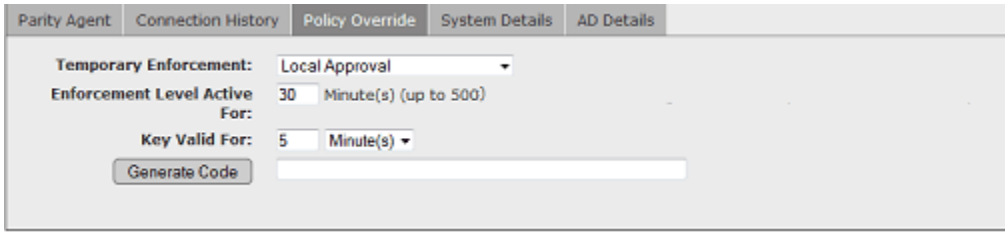
一時的なポリシー変更コードを使用してコンピューターの適用レベルを「低」または「なし（可視性のみ）」に切り替えた場合、エージェントは、元の適用レベルに戻るときに、そのコンピューターの適用レベルを緩めたときに検出された一部の未承認ファイルをローカル承認する場合があります。これは、ローカル状態の詳細が「未承認」のファイルに影響し、コンピューターが割り当てられているポリシーの［Advanced Settings（詳細設定）］の［Locally approve unapproved files on transition from Visibility or Low Enforcement Level to Medium or High（可視性または低適用レベルから中適用レベルまたは高適用レベルへの移行中に未承認ファイルをローカルで承認）］がオンかどうかによって異なります。Bit9 では、この自動ローカル承認設定が「オフ」になっていることを確認できない場合は、「ローカル承認」、「中適用レベル」、または「高適用レベル」への一時的な移行には、適用レベルの一時変更機能だけを使うことをお勧めします。

コンピューターを一時的なローカル承認モードに移行するためのコードを生成する手順：

1. コンソール メニューで、[**Assets**（アセット）]>[**Computers**（コンピューター）]の順に選択します。[Computers（コンピューター）]ページが表示されます。



2. テーブルで、コードを生成するコンピューターを見つけ、その名前をクリックします。そのシステムの［Computer Details（コンピューターの詳細）］ページが表示されます。
3. ページ下部にあるパネルで［**Policy Override**（ポリシーの一時変更）］タブをクリックします。



4. 別の適用レベルに移行する必要がない場合は、[Temporary Policy Override Code（一時的なポリシー変更コード）]パネルの［Temporary Enforcement（一時的な適用レベル）］は、デフォルトの［**Local Approval**（ローカル承認）］のままにします。
5. ［Enforcement Level Active For（適用レベルの有効期間）］に、適用レベルの変更をアクティブにする時間を分単位で入力します（最大 500）。
6. ［Key Valid For（キーの有効期間）］ボックスに、一時変更コードを有効にする時間を入力します。このフィールドを指定するときは、キーを必要とするコンピューター ユーザーにキーが提供されるまでの時間と、そのユーザーがどのタイミングでキーを入力できるようになるかを考慮する必要があります。

7. すべてのパラメーターをすべて入力したら、[**Generate Code**（コードを生成）] ボタンをクリックします。ボタンの横にあるボックスに、ハイフンで区切られた 9 文字の文字列が表示されます。

8. オフライン　コンピューターに新しいソフトウェアをインストールするユーザーに配布できるように、ボックスのコードをコピーして保存します（さらに、コンピューター名をメモします）。コードは、[Computer Details（コンピューターの詳細）] ページには保存されないため、記録しておく必要があります。

一時変更コードを適用する手順は、エージェント コンピューターのプラットフォーム（Windows、Mac、Linux）によって異なります。

Windows エージェントでの一時的な変更

Windows コンピューターでは、一時変更を開始する前にエージェントと Bit9 Server の接続を切断することを強くお勧めします。

Windows コンピューターで期限付きポリシーへの一時変更コードを使用する手順：

1. オフライン コンピューターで、**TimedOverride.exe** プログラムを見つけて実行します。このプログラムは、Bit9 エージェント インストール ディレクトリにあります。認証ダイアログ ボックスが表示されます。
2. ダイアログ ボックスにこのエージェントの一時変更コードを入力し、[**OK**] をクリックします。
   - 入力したコードが無効または期限切れの場合、あるいは TimedOverride.exe が何らかの理由で Bit9 エージェントと通信できない場合は、エラー メッセージが表示されます。誤ったコードを 3 回入力すると、プログラムは自動的に終了します。
   - 有効なコードが入力され、適用レベルの移行が適切に行われた場合は、メッセージなしでダイアログ ボックスが閉じます。
3. エラー コードがなく、ダイアログ ボックスが表示されていない場合は、このマシンに必要な新しいソフトウェアのインストールを開始できます（一時変更コードの目的がローカル承認だったことを前提としています）。適用レベルは、コードが生成されたときに設定した期間が経過すると、元の適用レベルに戻ります。

Mac および Linux エージェントでの一時的な変更

Mac および Linux コンピューターについては、一時変更を開始する前に、必ずしも Bit9 Server から接続を切断する必要はありません。エージェントが Bit9 Server に接続されている場合、一時変更を実行することで自動的に切断され、一時変更期間が終了した時点で再接続されます。マシンの再起動またはエージェントの再起動によって、期限付き一時変更がキャンセルされることはありません。

Mac および Linux コンピューターでは、特別なエージェント管理コマンドで一時変更コードを使用して、期限付きポリシーへの一時変更に適用します。

Mac および Linux コンピューターで期限付きポリシーへの一時変更コードを使用する手順：

1. 一時変更を適用するコンピューターで、ターミナル ウィンドウを開き、次のディレクトリに移動します。
   - Linux の場合：**`cd /opt/Bit9/bin`**
   - Mac の場合：**`cd /Applications/Bit9/Tools`**
2. 次のコマンドを入力して、生成した一時変更コードを引数として指定します。

   `./b9cli -timedoverride` *<code>*

   - 入力したコードが無効または期限切れの場合は、エラー メッセージが表示されます。誤ったコードを 3 回入力すると、その後 1 時間またはエージェントが再起動されるまで、プログラムはロックされます。
   - 有効なコードが入力され、適用レベルの移行が適切に行われた場合は、「Timed override set（期限付きの一時変更が設定されました）」というメッセージが表示されます。
3. 一時変更が設定されると、エージェントがサーバーから切断され（接続されていた場合）、このマシンに必要な新しいソフトウェアのインストールを開始できます（一時変更コードの目的がローカル承認だったことを前提としています）。

構成した一時変更が期限切れになると、適用レベルは元の設定に戻ります。Mac および Linux コンピューターでは、一時変更コードが適用されたときにコンピューターが接続されていた場合は、その Bit9 Server に再接続されます。すぐに再接続されても、後から再接続されたとしても、エージェントは、適用レベルの変更に関連付けられているイベントをサーバーにレポートします。

ファイルをインストーラーまたはインストーラー以外としてマーク

Bit9 Security Platform では、ファイルの分析時に、ファイルが「インストーラー」の可能性が高いかどうか、つまり実行時に追加のファイルが生成されるかどうかを判断します。インストーラーとして特定されたファイルをローカルで承認すると、そのインストーラーによってインストールされたファイルもローカル承認されます。インストーラーとして特定されていないファイルについては、そのファイルが生成するファイル（存在する場合）に承認ステータスが転送されることはありません。

ファイルが誤って分類されることや、最上位ファイルをローカルで承認しても、そのファイルによってインストールされたファイルはローカル承認したくないこともあります。ファイルの詳細ページのメニューを使用すると、ファイルをインストーラーとして設定することも、インストーラーとしての設定を解除することもできます。いずれの場合も、メニューには、現在のステータスを変更するためのオプションしか表示されません。

注意

このリリースでは、Linux ファイルはインストーラーとして認識されません。また、インストーラーとして認識される唯一の Mac ファイルはパッケージ、つまり、拡張子が .PKG で、適切に定義された「アーカイブ」ヘッダーを持つファイルです。このため、「インストーラーとしてマーク」機能は、このプラットフォームで特に役立つ可能性があります。

ファイルをインストーラーとしてマークする手順：

- ［File Details（ファイルの詳細）］ページまたは［File Instance Details（ファイルインスタンスの詳細）］ページで、［Actions（アクション）］メニューの［**Mark as Installer**（インストーラーとしてマーク）］をクリックします。

ファイルをインストーラー以外としてマークする手順：

- ［File Details（ファイルの詳細）］ページまたは［File Instance Details（ファイルインスタンスの詳細）］ページで、［Actions（アクション）］メニューの［**Mark as Not Installer**（インストーラー以外としてマーク）］をクリックします。

注意

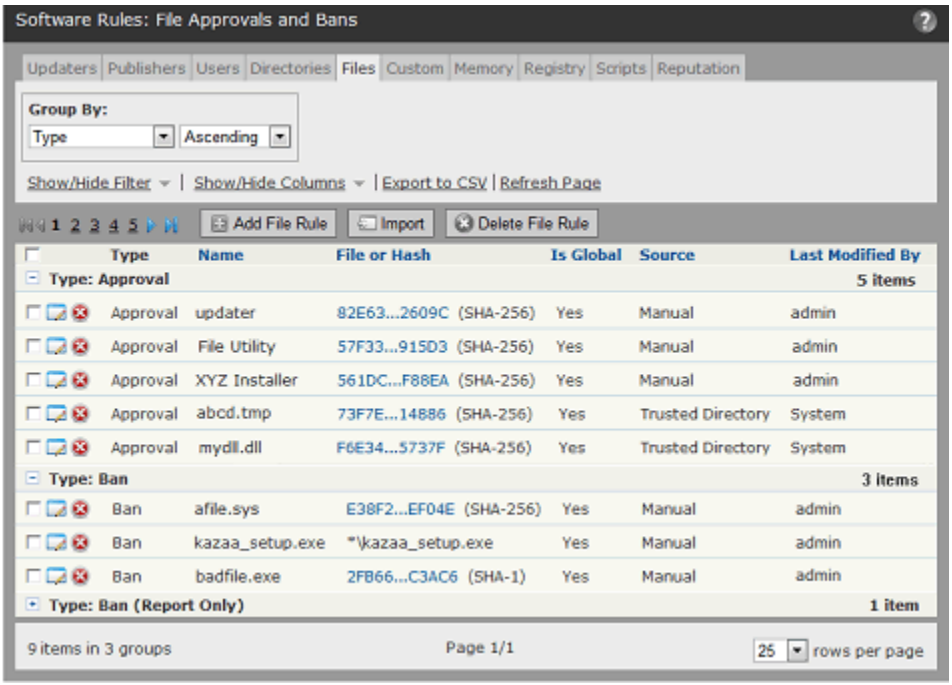
- ファイルのインストーラーのステータスを上書きすると、ファイルの［Local State Details（ローカル状態の詳細）］には新しいステータスが表示されます。
- ファイル　テーブルで、インストーラーとして特定されていないファイルの横にあるボックスをオンにして、［Action（アクション）］メニューの［Approve by Policy（ポリシーにより承認）］を選択すると、承認ルールの一環として、そのファイルをインストーラーとしてマークすることができます。これにより、このファイルによって作成された新しいファイルが、確実にローカルで承認されます。既に作成されているファイルについては、現在の状態が保持されます。
- ルールの仕様を満たすファイルを「昇格」するカスタム ルールを作成できます。この場合、こうしたファイルは、ルールの条件に従ってインストーラーとして処理されますが、グローバル ステータスがインストーラーまたはインストーラー以外に変更されることはありません。第 12 章「カスタム ソフトウェア ルール」を参照してください。

ファイル固有のルール：承認と禁止

［Software Rules（ソフトウェア ルール）］ページの［Files（ファイル）］タブには、特定の個別のファイルに対してご自身のサイトで作成されたすべての承認と禁止が表示されます。こうしたルールでは、ハッシュまたはファイル名（オプション、禁止のみ）によってファイルが特定されます。

承認と禁止がグローバルの場合は、その承認と禁止はすべてのコンピューターに適用されます。また、選択したポリシーのコンピューターに承認と禁止を適用することもできます。アクティブな禁止は、制御モードでは、影響を受けるコンピューターでのファイルの実行をブロックします。可視性モードではコンピューターのイベントをレポートし、エージェント無効モードではコンピューターに何も行いません。アクティブになっていれば実行していたはずである処理をレポートするだけの禁止を作成することもできます。

［Files（ファイル）］タブには承認と禁止の両方が表示されるため、すべてのファイル ルールを 1 か所で管理できます。特定のファイルが何らかの承認または禁止の影響を受けていないかどうかを確認し、確認された1つ以上のファイルからルールを削除できます。



デフォルトでは、ファイル ルールは「タイプ」に基づいてグループ化され、すべての承認、禁止、レポートのみの禁止をまとめて確認できます。ほとんどのコンソール テーブルと同様、グループ化を変更（または解除）するには、［Group by（グループ別）］メニューで別のオプションを選択します。

プロパティ ページにファイル ハッシュまたは名前を手動で入力する場合は、［Software Rules（ソフトウェア ルール）］ページの［Files（ファイル）］タブを使用して、承認と禁止を直接作成できますが、ファイル ハッシュが既に用意されているテーブルまたは［File Details（ファイルの詳細）］ページを使うと、禁止をさらに簡単に作成できます。いずれの場合も、作成した承認または禁止は、このページに表示されます。

新しい禁止または承認を作成すると、既に承認または禁止が設定されているファイルが影響を受けることがあります。その場合は、警告が表示され、新しいルールを保存すると古いルールが削除されることが通知されます。この通知は、ファイル グループを選択したことで、あるファイルの承認が禁止によって誤って置き換えられる場合、または禁止が承認によって誤って置き換えられる場合に特に便利です。

作成した禁止によって、以降のファイルの実行だけでなく、そのファイルに一致する現在実行中のプロセスが停止されることもあります。詳細については、「禁止による実行中のプロセスの停止」（339 ページ）を参照してください。

注意

［Files（ファイル）］タブの承認と禁止は、（名前またはハッシュによって）指定されたファイルに対して特別に作成されたルールです。このページには、レピュテーション ルール、カスタム ルールなど、他のルールにより有効になっている承認や禁止が「すべて」表示されるわけではありません。また、グローバルな「ファイル状態」の包括的なリストでもありません。「グローバル状態」が「承認」のすべてのファイルを表示するには、［File Catalog（ファイル カタログ）］を使用します。

［File Rules（ファイル ルール）］ページに表示される承認と禁止を作成する方法を次に示します。

- ［Software Rules（ソフトウェア ルール）］の［Files（ファイル）］タブから、［Add File Rule（ファイル ルールの追加）］ページを開き、1 つのファイルのハッシュを入力します。禁止の場合は、ファイル名または特定のパスを使用することもできます
- ［File Details（ファイルの詳細）］ページまたは［File Instance Details（ファイル インスタンスの詳細）］ページで、［Actions（アクション）］メニューの承認コマンドまたは禁止コマンドのいずれかを選択して、1 つのファイルに対してルールを作成します。
- ファイルのテーブル（［File Catalog（ファイル カタログ）］など）で 1 つ以上のファイルをオンにして、［Action（アクション）］メニューの承認コマンドまたは禁止コマンドのいずれかを選択し、1 つ以上のルールを作成します。
- ［Events（イベント）］テーブルで、説明にファイル参照が含まれる 1 つ以上のイベントをオンにして、［Action（アクション）］メニューの承認コマンドまたは禁止コマンドのいずれかを選択し、1 つ以上のルールを作成します。
- ［Software Rules（ソフトウェア ルール）］の［Files（ファイル）］タブで、ファイル ハッシュのリストをインポートして、複数のルールを作成します。
- ［Software Rules（ソフトウェア ルール）］の［Directories（ディレクトリ）］タブで、信頼済みディレクトリを作成します。信頼済みディレクトリに配置されているファイルごとに、そのファイル用に作成された承認ルールがあります。
- 外部 API によって承認または禁止が作成されていることがあります。また、ルールが古いバージョンのBit9 Security Platform (Parity)で作成されている場合など、ルールのソースが不明な場合もあります。［Files（ファイル）］タブまたは［Edit File Rule（ファイル ルールの編集）］ページの［Source（ソース）］フィールドには、ルールがどのように作成されたかが示されています。

一度作成したルールは、[File Rules（ファイル ルール）] ページで管理できます。また、ルールを削除するときは、ほとんどの場合、作成するときに使用したページのコマンドを使用できます。

警告

誤ったファイルを禁止すると、意図しない有害な結果につながることがあります。たとえば、適切なシステム ファイルを誤って禁止すると、直ちにコンピューターがクラッシュする場合があります。ファイルを禁止する前に、正しい名前またはハッシュが入力されていることを必ず確かめてください。安全のため、最初にファイルの検索機能でファイル名またはハッシュを検索して、それが禁止するファイルであることを確認し、さらに、そのファイルの [File Details（ファイルの詳細）] ページを確認します。また、禁止する前に、Bit9 Software Reputation Service (SRS) を使用して、ファイルの詳細を確認することも検討してください。詳細については、第 23 章「システム構成」の「Bit9 SRS の有効化」を参照してください。

ファイルを実際にブロックせずに禁止の影響をテストする方法として、レポートのみの禁止を作成するというものがあります。

レポートのみの禁止のテストは、実行中のプロセスの停止を有効にして禁止を作成したときに特にお勧めです。「禁止による実行中のプロセスの停止」（339 ページ）を参照してください。

レポートのみの禁止

「禁止（レポートのみ）」ルールを作成すると、ユーザーへの禁止の影響を確認できます。レポートのみ禁止を使用すると、ファイルはブロックされず、「ブロックしていたはず」および「終了していたはず」という警告がイベント ログに書き込まれます。これが確実に実行をブロックするファイルである場合は、ルールを完全な禁止に変更できます。Bit9 イベント レポートの詳細については、「イベント レポート」（590 ページ）を参照してください。

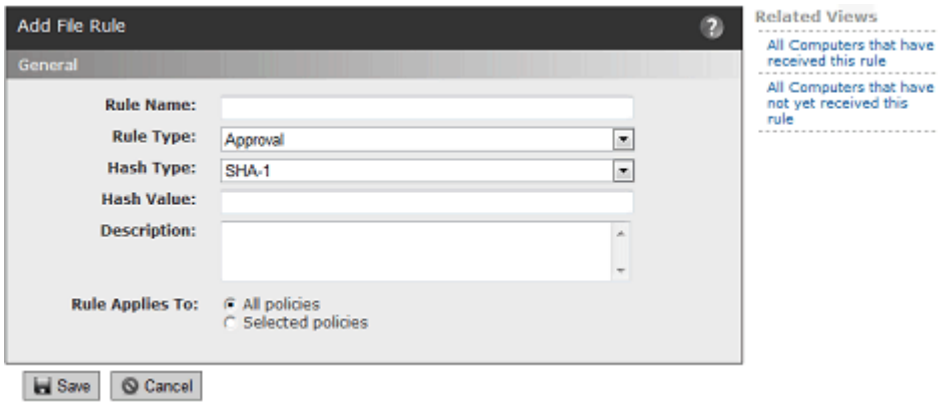
[Software Rules（ソフトウェア ルール）] ページでの承認または禁止の作成

承認または禁止に対してすべてのパラメーターを指定する場合は、[Add File Rule（ファイル ルールの追加）] ページで作成します。

1 つのファイルの承認または禁止を作成および構成する手順：

1. コンソール メニューで、[**Rules**（ルール）] > [**Software Rules**（ソフトウェア ルール）] の順に選択します。[Software Rules（ソフトウェア ルール）] ページが表示されます。
2. [**Files**（ファイル）] タブをクリックします。[File Approvals and Bans（ファイルの承認と禁止）] テーブルが表示されます。

3. ［**Add File Rule**（ファイル ルールを追加）］ボタンをクリックします。［Add File Rule（ファイル ルールの追加）］ページが表示されます。このページでは、デフォルトのルール タイプとして［Approval（承認）］が指定されています。



4. ルールと、承認または禁止するファイルに関する情報を指定します（表 39 は、指定できるパラメーターの一覧と作成後に使用できるルール情報を示しています）。
   a. テーブル内でルールを識別できるようにルール名を指定します。
   b. ルール タイプ（［Approval（承認）］、［Ban（禁止）］、［Ban（Report Only）（禁止（レポートのみ））］）を選択します。［Ban（禁止）］を選択すると、現在実行されている一致ファイルが停止される可能性があることを通知する警告が表示されます。詳細については、「禁止による実行中のプロセスの停止」（339 ページ）を参照してください。
   c. ルールが「禁止」の場合は、タイプ（ハッシュまたはファイル名）を選択します。
   d. ハッシュ ルールについては、使用するハッシュのタイプ（MD5、SHA-1、または SHA-256）を指定します。
   e. ファイル名による禁止の場合は、ルールが適用されるプラットフォーム（Windows、Mac、または Linux）を選択します。
   f. ファイルを特定するハッシュ値またはファイル名を入力します。
   g. オプションで説明を入力します。
   h. ［Rule Applies To（ルールの適用先）］フィールドで、ルールの適用先として、［All policies（すべてのポリシー）］を選択するか［Selected policies（選択済みポリシー）］を指定します。
5. 承認または禁止を作成するには、［**Save**（保存）］をクリックします。ルールは［File Rules（ファイル ルール）］テーブルに表示されます。禁止、レポートのみの禁止、承認ごとにまとめて表示するには、「タイプ」（デフォルト）に基づいてテーブルをグループ化します。

ルールを保存すると、ルールとその追加情報を定義するパラメーターが、詳細ページで使用できるようになります。表 39 は、［Edit File Rule（ファイル ルールの編集）］ページに表示される情報を示しています。ページでどのフィールドを編集できるかは、ルールの作成方法によって異なります。

表 39：ファイル ルールのパラメーター

フィールド	説明
Rule Name（ルール名）	承認または禁止するファイルの説明テキスト。ファイル名、またはルールの管理に役立つその他の識別情報です（ルールは、名前を入力しなくても作成されます）。 **注意**：これはただのルール名です。ここにファイル名を入力しても、ファイル名ベースのルールは作成されません。
Rule Type（ルール タイプ）	[Approval（承認）]、[Ban（禁止）]、[Ban (Report Only)（禁止（レポートのみ））] のいずれかを選択できます。[Ban (Report Only)（禁止（レポートのみ））] では、ルールが「完全禁止」の場合にファイルがブロックされていたはずである状況をイベントとしてレポートします。
Source（ソース） （読み取り専用）	ルールがどのように作成されたか。値は、[Manual（手動）]（ゼロから、または［Action（アクション）］メニューのコマンドにより作成）、[Trusted Directory（信頼済みディレクトリ）]、[Imported（インポート）]（アップロードされたファイル リストから）、[External (API)（外部（API））]、および［Unknown（不明）］です。ルールが作成された後に表示されます。
Type（タイプ） （禁止のみ）	ファイルを禁止するには、ファイルの名前またはそのハッシュ（データ署名）を把握している必要があります。どちらか適切な方を選択します。名前を選択した場合は、特定の場所のファイルにのみルールが適用されるようにパスを入力できます。承認は常にハッシュによって行われるため、承認の場合、[Type（タイプ）] フィールドは表示されません。名前による禁止はプラットフォームに固有です。
File Name（ファイル名） （禁止のみ）	（禁止に対してのみ、またタイプとしてファイル名を選択した場合にのみ表示されます）ファイルとその拡張子の名前。msblast.exe など。 特定の場所にある一致するファイルのみを禁止する場合は、ディレクトリ パスを指定します。パスを使用した場合、他のディレクトリに存在する同じ名前のファイルは、名前による禁止の対象になりません。 **プラットフォームに関する注意**：パスを入力するときは、必ず正しいディレクトリ区切り文字と、選択されたプラットフォームのパスに適した文字と形式のみを使用します。Bit9 Server ではプラットフォーム間でパスを変換できません（たとえば、「\」を「/」に変換することはできません）。また、Linux のファイル名は、通常、大文字と小文字が区別されます。
Platform（プラットフォーム） （名前による禁止のみ）	（禁止に対してのみ、またタイプとしてファイル名を選択した場合にのみ表示されます）このルールが有効なプラットフォーム（Mac、Linux、Windows）。名前による禁止はプラットフォームに固有です。
Hash Type（ハッシュ タイプ）	承認または禁止するハッシュの作成に使用する暗号化アルゴリズム。値を貼り付ける場合は、MD5、SHA-1、および SHA-256 を選択できます。ファイル テーブルまたは詳細ページから作成されたルールでは SHA-256 が使用されます（使用できる場合）。

フィールド	説明
Hash Value（ハッシュ値）	ファイルのハッシュ（データ署名）。この Bit9 Server でまだ認識されていないハッシュをルールで使用できます。 コンピューターで既に認識されているファイルのハッシュを確認するには、[File Catalog（ファイル カタログ）] ページまたは [Find Files（ファイルの検索）] ページを使用できます。
Description（説明）	ファイルの承認または禁止について詳しく説明するオプションのテキスト。 この情報は、[File Rules（ファイル ルール）] テーブルの [Description（説明）] 列（表示されている場合）に表示されます。
Rule Applies To（ルールの適用先）	承認が実施される対象のポリシー： すべてのコンピューターのファイルを承認または禁止するには、[**All policies**（すべてのポリシー）] を選択します。 ルールを適用するポリシーを選択するには、[**Specified policies**（指定されたポリシー）] を選択します。このボタンをクリックすると、ポリシーのリストが表示され、各ポリシーにチェックボックスが示されています。すべてのボックスをオンまたはオフにするには、リストの最上部にあるチェックボックスを使用します。ただし、どのポリシーにも適用しないルールを作成することはできません。
History（履歴） （読み取り専用）	ルールの作成日、最終更新日、作成者、および最終更新者が表示されます。また、現在のバージョンのルールが存在する CL バージョン（Bit9 ルールのバージョン）も表示されます。これは、ルールがエージェントに存在しているかどうかを判断するときに使用できます。

ファイル ルールの編集と削除

既存のファイル ルールを変更または削除できます。表 39、「ファイル ルールのパラメーター」328 ページは、変更できるパラメーターと読み取り専用のパラメーターをいくつか示しています。

承認または禁止のルールを編集する手順：

1. [Software Rules（ソフトウェア ルール）] ページの [Files（ファイル）] タブで、ルールの横にある [View Details（詳細の表示）]（鉛筆とファイル）ボタンをクリックします。[Edit File Rule（ファイル ルールの編集）] ページが表示されます。
2. 変更する詳細を編集します。タイプ（ハッシュまたはファイル）、ハッシュ タイプ、およびハッシュ値を除く、すべてのルール パラメーターを変更できます。また、ページに追加された [Source（ソース）] フィールドと [History（履歴）] フィールドは読み取り専用で、ルールに関連するアクティビティが反映されます。

3. 変更が完了したら、[**Save**（保存）] をクリックします。ルールが更新されます。

注意

既存の承認または禁止を無効にすることはできません。ただし、ルール タイプは変更できます。たとえば、禁止を「アクティブな禁止」から「レポートのみ」に変更し、実際にブロックせずに、ブロックしていたはずのファイル実行をレポートできます。

禁止から承認、または承認から禁止に変更することもできます。ただし、こうした変更は、その影響を必ず理解したうえで行うようにしてください。また、絶対に有効にしないルールは削除します。

ファイルのルールを削除するには、ファイル テーブル ページの［Action（アクション）］メニューで［**Remove Approval or Ban**（承認または禁止を削除）］コマンドを使用するか、詳細ページで適切な［Remove（削除）］コマンドを使用します。［Software Rules（ソフトウェア ルール）］ページの［Files（ファイル）］タブが表示されている場合は、次の手順でルールを削除します。

1 つ以上の承認または禁止ルールを削除する手順：

1. ［Software Rules（ソフトウェア ルール）］ページの［Files（ファイル）］タブで、削除する承認および禁止の横にあるボックスをオンにします。
2. ［**Delete File Rule**（ファイル ルールを削除）］ボタンをクリックします。
3. 確認ダイアログ ボックスで **[OK]** をクリックします。ルールが削除されます。

［Edit Rule（ルールの編集）］ページで［**Remove Rule**（ルールを削除）］ボタンをクリックして、1 つの承認または禁止を削除することもできます。

テーブル ページでのファイルの承認と禁止の作成

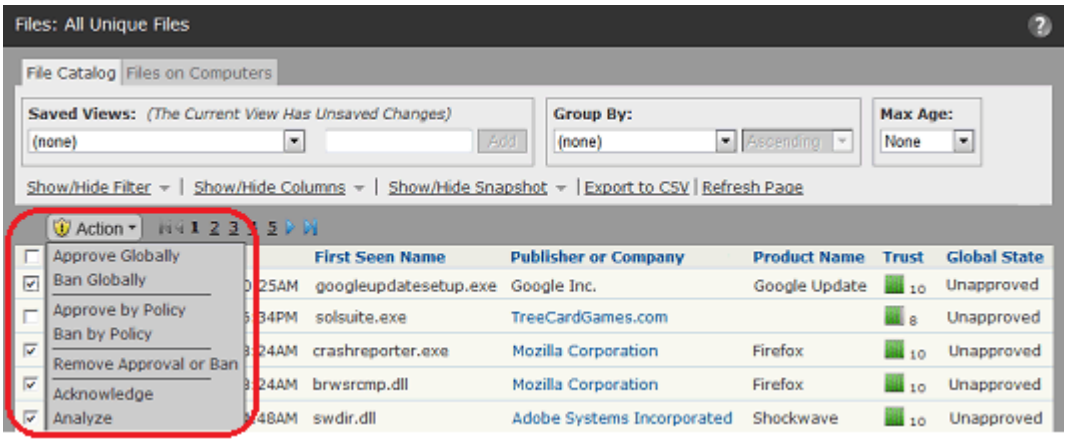
ここでは、［Files（ファイル）］ページ（［File Catalog（ファイル カタログ）］または［Files on Computers（コンピューター上のファイル）］）からルールの承認または禁止を作成する方法について説明します。ただし、この説明は、ファイルの一覧が表示される他のコンソール ページや、ファイルが主要情報ではないページ、つまりファイルが他のオブジェクトの詳細にリンクとして表示されることがあるページにも適用されます。一般的には、ファイル名の横にチェックボックスがある行の［Action（アクション）］メニューから禁止および承認を作成できます。たとえば次のようなページです。

- ［Files（ファイル）］ページ（［Files Catalog（ファイル カタログ）］と［Files on Computers（コンピューター上のファイル）］の両方）
- ファイルが表示されている［Baseline Drift Report Results（ベースライン ドリフト レポートの結果）］ページ
- ［Snapshot Content（スナップショット コンテンツ）］ページ
- ［Events（イベント）］ページ（ファイル ハッシュが含まれるイベントのみ）
- ［Find Files（ファイルの検索）］ページ（結果が表示されている場合）

［Action（アクション）］メニューでは、テーブル ページから承認と禁止を管理するためのオプションを選択できます。

- ［**Approve Globally**（グローバルに承認）］– すべてのコンピューターのファイルをグローバルに承認するハッシュ ベースのルールを直ちに作成します。構成は不要です。
- ［**Ban Globally**（グローバルで禁止）］– すべてのコンピューターに適用するアクティブなハッシュ禁止を直ちに作成します。構成は不要です。
- ［**Approve by Policy**（ポリシーにより承認）］–［Add Rule（ルールの追加）］ページが開きます。このページでは、ルール名がファイル名、ルール タイプが承認に設定され、ファイル ハッシュが既に準備できています。ルールは選択したポリシーまたはすべてのコンピューターに適用できます。また、ルール名を編集して、説明を追加することもできます。
- ［**Ban by Policy**（ポリシーにより禁止）］–［Add Rule（ルールの追加）］ページが開きます。このページでは、ルール名がファイル名、ルール タイプが禁止に設定され、ファイル ハッシュが既に準備できています。ルールは選択したポリシーまたはすべてのコンピューターに適用できます。また、ルール名を編集し、説明を追加できるほか、ルールをアクティブな禁止やレポートのみの禁止にすることもできます。
- ［**Remove Approval or Ban**（承認または禁止を削除）］– 承認と禁止が混在して選択されているものを含め、オンになっているすべてのボックスのルールを直ちに削除します。

コンソール ファイル テーブルから承認や禁止を作成するメリットは、複数のファイルを一度に承認または禁止できることです。たとえば、ファイル ページでフィルタリング ツールを使用すると、特定の基準を満たすファイルの一覧を取得し、各ファイル名の横にあるボックスをオンにして、1 回の操作でグローバルに禁止できます。



テーブルからルールを作成する場合、指定したルールの定義は、選択した各ファイルに適用されます。定義を保存すると、選択したファイルごとに個別にルールが作成され、名前が付けられます。テーブルのオンになっている行から作成されたルールは必ずハッシュ禁止で、SHA-256 ハッシュを使用します（使用できる場合）。

注意

- 最初は、共通のソースに由来するファイルは、ソースまたはインストーラー ファイル名でグループ化されています。承認または禁止するファイルを探している場合、「個々」のファイルを表示および検索できるように、インストーラーでグループ化されているすべてのファイルをテーブルに含めるには、[Files（ファイル）] ページの右下にある [**Show Individual Files**（個別のファイルを表示）] ボックスをオンにします。これにより、テーブルが自動的に更新されます。
- [Files（ファイル）] ページでファイル リストにフィルターしたり、列を並べ替えて表示したり、結果をコンマ区切り形式でダウンロードしたりできます。詳細については、第 2 章「Bit9 コンソールの使用」の「Bit9 コンソールのテーブル」を参照してください。

グローバル承認と禁止の作成

ファイル ページの [Action（アクション）] メニューには 2 つのショートカット コマンドがあります。1 つはグローバル禁止を作成し、もう 1 つはページでオンにしたファイルに対してグローバル承認を作成します。作成するルールに対して特別な構成を作成する必要がない限り、このコマンドで 1 つ以上のファイルをすばやく承認または禁止できます。

この方法で作成されたルールは、すべてのポリシーに適用されます。[Globally Approve（グローバル承認）] を選択すると、オンにしたファイルが、すべてのコンピューターに対してグローバルに承認され、各ファイルには [Software Rules（ソフトウェア ルール）] ページで個別の承認ルールが指定されます。同様に、[Globally Ban（グローバル禁止）] を選択すると、制御ポリシーのすべてのコンピューターでファイルが禁止され、各ファイルには [Software Rules（ソフトウェア ルール）] ページで個別の禁止ルールが指定されます。

承認と禁止の両方について、ファイルをオンにすると、そのファイル名がルール名として使用されます。複数のファイルをオンにすると、名前は空白になります。

注意

既にルールが設定されているファイルを選択し、別のタイプのルールを適用した場合は、古いルールの名前が維持されたままでルール タイプが変更されます。そのため、「Approve Files for My Project（自分のプロジェクトのファイルを承認）」といった名前を付けたルールのルール タイプを「禁止」に変更すると混乱が生じる可能性があります。

［Files（ファイル）］ページで 1 つ以上のファイルに対してグローバル承認またはグローバル禁止を作成する手順：

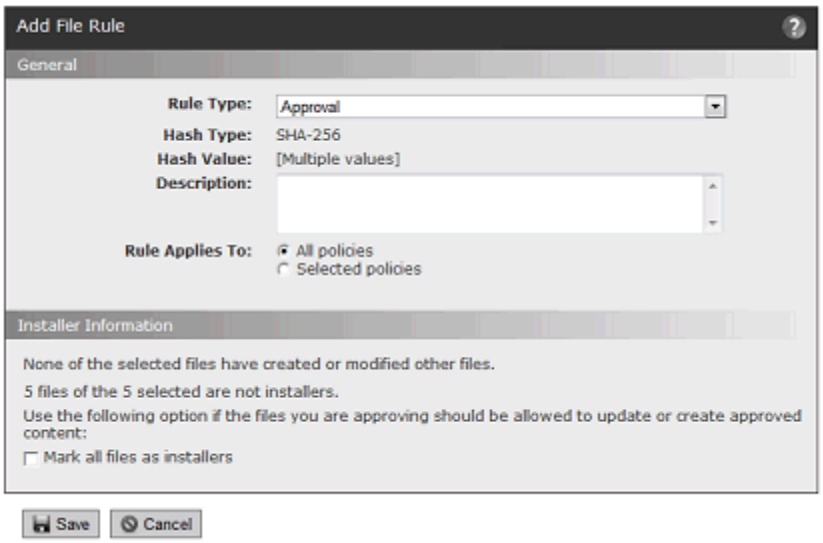
1. コンソール メニューで、［**Assets**（アセット）］>［**Files**（ファイル）］の順に選択します。［Files（ファイル）］ページが表示されます。
2. 承認または禁止するファイルを見つけ、その名前の横にあるボックスをオンにします。
3. ［Action（アクション）］メニューで、［**Globally Approve**（グローバル承認）］または［**Globally Ban**（グローバル禁止）］を選択します。
4. 確認ダイアログ ボックスで [**OK**] をクリックします。

カスタム承認と禁止

ファイル テーブルの［Action（アクション）］メニューで［Approve by Policy（ポリシーにより承認）］または［Ban by Policy（ポリシーにより禁止）］を選択すると、［Add File Rule（ファイル ルールの追加）］ダイアログが表示されます。このダイアログには、選択したファイルのハッシュが既に入力されています。グローバル オプションを選択した場合とは異なり、このオプションでは、ルールを作成する前に他のパラメーターをカスタマイズできます。

［Files（ファイル）］ページに表示されている 1 つ以上のファイルに対してカスタム承認または禁止を作成する手順：

1. コンソール メニューで、［**Assets**（アセット）］>［**Files**（ファイル）］の順に選択します。［Files（ファイル）］ページが表示されます。
2. 承認または禁止するファイルを見つけ、その名前の横にあるボックスをオンにします。
3. ［Action（アクション）］メニューで、［**Approve by Policy**（ポリシーにより承認）］または［**Ban by Policy**（ポリシーにより禁止）］を選択します。［Add File Rule（ファイル ルールの追加）］ページが開きます。



4. ルール タイプを変更できます。たとえば、[**Ban**（禁止）]（実行をアクティブにブロック）から［**Ban (Report Only)**（禁止（レポートのみ））］（禁止が完全に有効化されていればファイルがブロックされていたはずであることをレポート）に変更できます。
5. オプションでルールの説明を追加できます（承認済みファイルの共通事項、ファイルを禁止した理由など）。
6. ［Rule applies to（ルールの適用先）］フィールドで次の操作を行います。
   a. ルールをすべてのコンピューターに適用するには、［All policies（すべてのポリシー）］ボタンを選択したままにします。
   b. ルールを選択したポリシーにのみ適用するには、［Selected policies（選択したポリシー）］ボタンをクリックします。
7. ルール タイプが「承認」の場合は、［Installer Information（インストーラー情報）］パネルがページ下部に表示されます。「承認」として選択されているいずれかのファイルが現在インストーラーとして認識されていない場合は、［Mark all files as installers（すべてのファイルをインストーラーとしてマーク）］チェックボックスがパネルに表示されます。ファイルを承認してインストーラーとしてマークする場合は、そのボックスをオンにします。

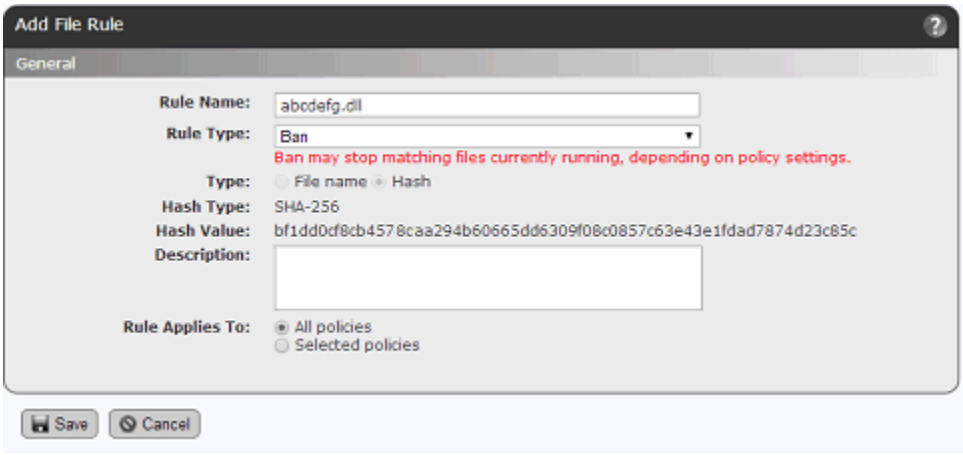
重要

特にルールに対して複数のファイルが選択されている場合は、［Mark all files as installers（すべてのファイルをインストーラーとしてマーク）］ボックスをオンにする前に、必ず「すべて」のファイルをインストーラーにする必要があることを確かめます。インストーラーによって作成されたファイルはローカル承認され、この承認を自動的には削除する方法はありません。［Installer Information（インストーラー情報）］パネルには、選択したファイルのうち、いくつのファイルがこのオプションの影響を受けるか、また、選択したファイルの中に、他のファイルを作成または変更したファイルがあるかどうかを示すメッセージが表示されます。

8. 意図したとおりにルールを構成したら、［**Save**（保存）］ボタンをクリックします。プロセスの開始時にオンにした各ファイルが、［Software Rules（ソフトウェア ルール）］ページの［Files（ファイル）］タブに個別の承認として表示されます。［File Approvals and Bans（ファイルの承認と禁止）］テーブルには、承認または禁止がグローバルかどうかが示されます。

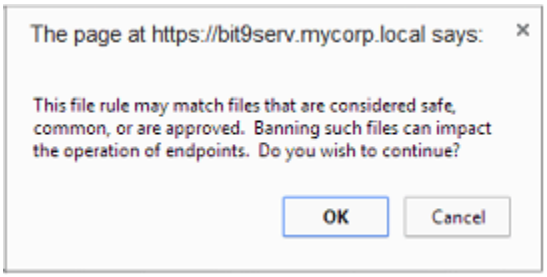
禁止の作成または編集時の警告

禁止を作成または編集するとき、[File Rule details（ファイル ルールの詳細）] ダイアログには、ルールによって現在実行中のファイルが停止される可能性があることを示す警告が赤色で表示されます。これは、プロセスの停止が有効になっているポリシーがなくても、念のため表示されます。



さらに、ファイルの禁止を追加または編集して、[File Rule details（ファイル ルールの詳細）] ダイアログで［Save（保存）］をクリックすると、確認ダイアログに警告の内容が詳しく表示されることがあります。名前による禁止の場合、この警告は、名前にワイルドカードが含まれているときに表示されます。さらに、名前による禁止とハッシュによる禁止の両方について、ルールで指定されたファイルの Bit9 SRS 脅威レベルが「0 – クリーン」または「不明」で、次の条件のいずれかが当てはまる場合にも表示されます。

- 禁止で指定されているファイルが Microsoft によって署名されている（キー システム ファイルを含む）
- 禁止で指定されているファイルが他の信頼済み公開者によって署名されている
- 禁止で指定されているファイルの Bit9 SRS 信頼レベルが 7 を超える。
- 禁止で指定されているファイルが、10% を超えるレポート エージェント コンピューターに表示されている。



いずれかの条件が当てはまる場合、禁止で示されているファイルを終了することで、コンピューターのシャットダウンなど、望ましくない動作につながることがあります。このダイアログではデフォルトで禁止が許可されるため、禁止に関して懸念がある場合は、必ず［**Cancel**（キャンセル）］をクリックしてください。

［File Details（ファイルの詳細）］ページでのファイルの承認と禁止

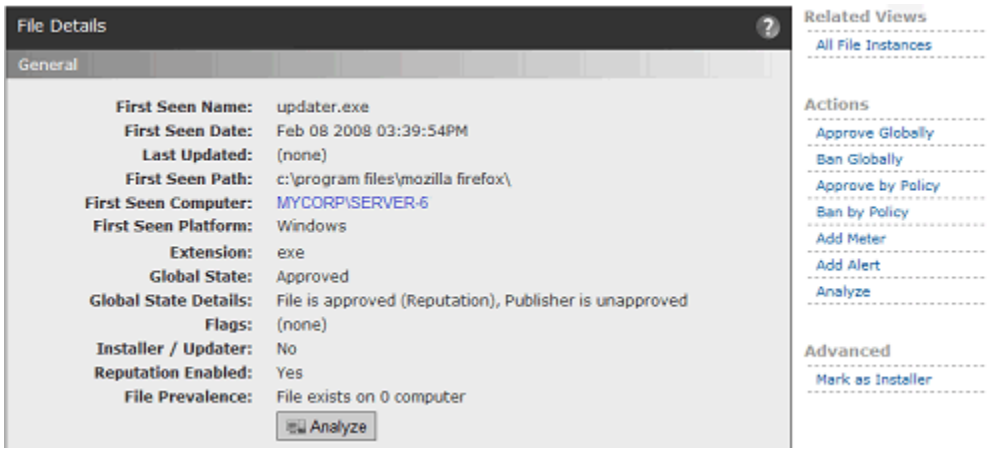
テーブルからファイルを承認または禁止できますが、禁止するかどうかを決める前に、そのファイルの詳細情報を確認することもできます。この操作を行うには、［File Details（ファイルの詳細）］ページに移動します。

注意

［File Instance Details（ファイル インスタンスの詳細）］ページでこれと同じ手順を実行して、グローバルまたはポリシーによってファイルを承認したり禁止したりできます。また、このページには、個別のファイルのローカル承認を適用または削除するオプションも用意されています。

［File Details（ファイルの詳細）］ページを使用して 1 つのファイルを承認または禁止する手順：

1. 承認または禁止するファイルを見つけたら、テーブルでそのファイルの横にある［View Details（詳細の表示）］（鉛筆）ボタンをクリックします。［Events（イベント）］テーブルの場合は、そのハッシュまたは名前をクリックします。［File Details（ファイルの詳細）］ページが表示されます（ここでは上部パネルのみ）。



2. ［File Details（ファイルの詳細）］ページの情報を確認して、それが承認または禁止する必要があるファイルであることを確かめます。たとえば、［File Prevalence（ファイル普及度）］行では、そのファイルが現在保存されているコンピューターがないかどうかを確認できます。ファイルを承認または禁止する前に、どのコンピューターにそのファイルがあるかを確かめるには、［Related Views（関連ビュー）］メニューで［**All File Instances**（すべてのファイル インスタンス）］リンクをクリックします。

3. Bit9 SRS が有効になっている場合、[Bit9 Software Reputation Service Information（Bit9 Software Reputation Service 情報）] パネルには、信頼、脅威など、そのファイルに関する情報が表示されます（表示可能な場合）。[**Analyze**（分析）] ボタンをクリックすると、Bit9 SRS で情報を検索したり（[none（なし）] が表示されている場合）、更新された情報がないかどうかをチェックしたりできます。

   注意

   ファイルを分析する必要があるのに、[Analyze（分析）] ボタンが表示されていない場合は、「Bit9 SRS の有効化」（787 ページ）を参照してください。

4. [Action（アクション）] メニューで、このファイルに対して作成するルールを選択します。既に承認または禁止されているファイルがある場合、反対のルールを作成するときは、（[**Remove Approval**（承認を削除）] または [**Remove Ban**（承認を禁止）] を使用して）現在のルールを削除しておく必要があります。

   注意

   [Software Rules（ソフトウェア ルール）] ページの [Files（ファイル）] タブでのハッシュ承認または禁止の詳細については、「[Software Rules（ソフトウェア ルール）] ページでの承認または禁止の作成」（326 ページ）を参照してください。

ファイル リストの承認または禁止

ファイルのハッシュ リストがある場合は、そのリストをテキスト ファイルでインポートして Bit9 コンソールに入力し、ファイルの状態を 1 回の操作で変更できます。ファイルの状態は「承認済み」、「禁止」、「禁止（レポートのみ）」のいずれかに変更できます。また、この操作は、一部またはすべてのポリシーに対して行うことができます。

ハッシュ リストを承認または禁止するための要件と推奨事項を次に示します。

- ハッシュ リストが含まれるファイルは、Bit9 Server からアクセスできる必要があります。
- ファイルには MD5、SHA-1、SHA-256 のいずれかのハッシュ リストを含める必要があります。ハッシュは 1 行につき 1 つだけ指定します。
- ファイルごとに 1 つのハッシュ タイプを使用します。1 つのファイルに複数のタイプを混在させると、予期しない結果につながる可能性があります。
- リスト内のすべてのファイルに対して同じアクションを実行します。つまり、承認、禁止、レポートのみの禁止の作成は、リスト全体に対して行う必要があります。
- このバージョンの Bit9 コンソールは、Internet Explorer 10 以降でサポートされています。高度なセキュリティ設定を備えた一部の以前のバージョンの IE では、[**インターネット オプション**]、[**セキュリティ**]、[**信頼済みサイト**]、[**サイ**

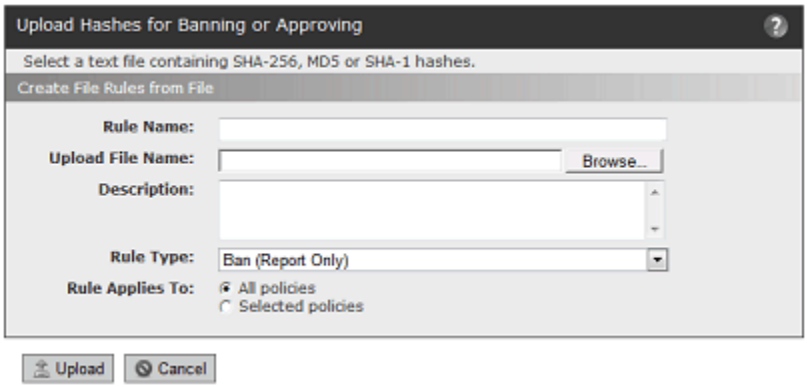
ト］の順に選択して、https://<bit9servername>/ を信頼済みサイトに設定します。それ以外の場合、一括ハッシュ ファイルは処理できません。

- 処理が完了したことが［Upload Hashes（ハッシュのアップロード)］ページに表示されるまで、そのページから移動しないでください。移動すると、ハッシュの処理が中断されます。その場合は、ファイルをもう一度アップロードできます。これにより、まだ承認または禁止されていないハッシュが処理されます。

この方法を使用して、ハッシュによってファイルのリストを承認または禁止すると、各ファイルが個別のルールとして表示されますが、ルール名はそれぞれ同じになります。

ハッシュ リストの承認または禁止を作成する手順：

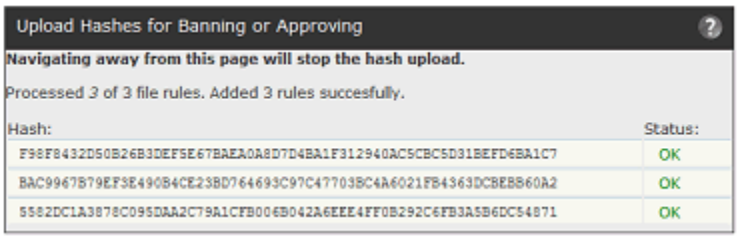
1. ハッシュが含まれるファイルを、Bit9 Server からアクセスできる場所にコピーまたは移動します。
2. コンソール メニューで、［**Rules**（ルール)］>［**Software Rules**（ソフトウェア ルール）］の順に選択します。［Software Rules（ソフトウェア ルール）］ページが表示されます。
3. ［**Files**（ファイル）］タブをクリックします。［File Rules（ファイル ルール）］ページが開き、承認済みファイルと禁止ファイルの一覧が表示されます。
4. ［**Import**（インポート)］ボタンをクリックします。［Upload Hashes for Banning or Approving（禁止または承認のハッシのアップロード）］ページが表示されます。



5. 次のように、ルール パラメーターを入力します。
   a. ［File Rules（ファイル ルール）］ページに表示されるルール名を入力します。
   b. ［**Browse**（参照）］ボタンを使用して、ハッシュ リストが含まれるファイルを見つけ、［Choose file（ファイルの選択）］ダイアログで［**Open**（開く）］をクリックします。ハッシュが含まれるファイルへのパスが［File name（ファイル名)］ボックスに表示されます。
   c. （オプション）ルールの説明を入力します。
   d. ［Rule Type（ルール タイプ)］メニューで、［**Approve**（承認)］、［**Ban**（禁止)］、または［**Ban (Report Only)**（禁止（レポートのみ))］を選択します。

e. ［**All policies**（すべてのポリシー）］または［**Selected policies**（選択したポリシー）］に対してルールを有効にします。

6. すべてのルール パラメーターに問題がなければ、［**Upload**（アップロード）］をクリックします。ハッシュの処理中、2 列の進行状況テーブルが表示され、ルールの成功または失敗がファイルごとにレポートされます。また、リスト上のハッシュが既に選択した状態になっている場合も通知されます。



7. コンソール メニューで、［**Rules**（ルール）］>［**Software Rules**（ソフトウェア ルール）］の順に選択します。［Software Rules（ソフトウェア ルール）］ページの［Files（ファイル）］タブにあるテーブルの個別の行に、承認または禁止を作成したハッシュが同じ名前で表示されます。リスト上のすべてのファイルに対してルールを作成すると、各ルールを個別に変更することができます。

禁止による実行中のプロセスの停止

デフォルトでは、ファイルを禁止すると、以降のファイル実行は停止されますが、エージェント管理システムで既に実行されているプロセスは停止されません。つまり、実行が許可されているファイルは、後で悪質であると見なされても、Bit9 ルール以外の何らかの理由で終了されるか、システムを再起動して終了されない限り実行され続けます。こうした状況は特に、明示的に禁止されていないファイルを実行できる低適用ポリシーと中適用ポリシーでよく起こります。

v.7.2.0 以降では、このようなポリシーのコンピューターが、現在実行中のソフトウェアを禁止するルールを受け取ったときに、そのソフトウェアが停止されるようにポリシーを構成できます。この機能により、環境内のソフトウェアをさらに細かく制御することができます。ただし、この機能を使うときは、重要なプロセスを中断したり、コンピューターの実行を妨げたりすることがないように気を付ける必要があります。また、ポリシーに対して有効になっている場合は、プロセスの停止が「すべて」の禁止ファイルに適用されることにも注意してください。この設定の影響を確認できるように、v7.2.0 で新しく作成されたポリシーは、禁止によって終了されるプロセスを、実際に終了せずにレポートするように構成されています。

注意

- 7.2.0 より前のエージェントは、この機能の影響は受けず、禁止ファイルに一致するプロセスを終了できません。
- Bit9 Platform v7.2.3 では、禁止イメージを含むプロセスの終了は Windows エージェントでのみサポートされています。

禁止プロセスを終了するシステム上にある禁止でも、終了しないシステム上にある禁止でも、ユーザーのシステムを中断したり、他の依存アプリケーションのエラーや進行中の作業の消失を発生させたりする可能性があります。一方で、禁止によってプロセス実行を終了できるようにすると、禁止の結果に関するフィードバックが直ちに提供されます。マルウェアに感染した正規のプロセスを終了して、感染なしで再開することもできます。次の例は、プロセス終了を有効にすることで起こる潜在的な影響を示しています。

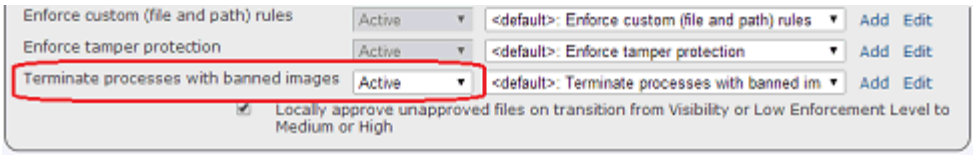
- **個別の単一アプリケーション** – skype.exe が禁止されます。禁止の影響を受けるシステムで、Skype の実行中のインスタンスすべてが突然終了し、ユーザーが Skype を再起動しようとするとブロックされます。
- **Windows エクスプローラー拡張機能** – Windows エクスプローラー拡張機能として登録され、エクスプローラーの実行中のインスタンスすべてに存在する malware.dll と呼ばれるファイルが禁止されます。禁止の影響を受けるシステムで、エクスプローラーのインスタンスすべてが終了され、その後エクスプローラーが自動的に再起動されます。再起動すると、エクスプローラーは引き続きロードされ、実行されますが、禁止ファイル malware.dll はブロックされます。つまり、禁止により、意図しないプロセスだけが実行されないようになり、重要なエクスプローラー プロセスはブロックされません。プロセス終了設定を行わないと、意図しないプロセスが、禁止された後も、すべてのアクティブ エクスプローラーで実行され続けます。
- **動的にロードされた DLL** – wsock32.dll が禁止されます。また、特定のネットワーク操作を実行する必要があるときは、application xyz.exe によって wsock32.dll が動的にロードされ、操作が完了したら、アンロードされることが想定されます。禁止の影響を受けるシステムで、wsock32.dll ファイルがアンロード中に禁止されると、その wsock32.dll ファイルは xyz.exe によって次回ロードされるときにブロックされ、操作が失敗する可能性があります。このファイルがロードされているときに禁止が有効になると、process xyz.exe は終了します。
- **共有サービス** – ネットワーク サービスとしてインストールされ、svchost のインスタンスを他の実行中のサービスと共有する malware.dll が禁止されます。ファイルが禁止されると、svchost のインスタンスと、同じプロセスのすべてのサービスが終了します。
- **重要なプロセスへの挿入** – 重要なシステム プロセスである csrss.exe に挿入される malware.dll が禁止されます。禁止の影響を受けるシステムで、csrss.exe が終了します。Windows は重要なシステム プロセスの終了を検出すると、直ちにシャットダウンします。起動時に csrss.exe が再ロードされると、Bit9 によってイメージ挿入が阻止され、システムは通常どおりブートできます。マルウェアはインストールされません。
- **ブート時のドライバー** – ブート時のドライバーとしてインストールされる malware.sys が禁止されます。Bit9 エージェントの前にドライバーがロードされた場合、そのドライバーは実行され続け、マシンがクラッシュしない限り停止できません。唯一の修復方法として考えられるのが、セーフ モードに切り替えて駆除するか、以前の時点に復元することです。

これ以外にもさまざまな影響を考慮して、ポリシーでプロセス終了を有効にするかどうかを検討してください。

禁止プロセスの即時終了を有効または無効にする手順：

1. コンソール メニューで、[**Rules**（ルール）] > [**Policies**（ポリシー）] の順に選択します。

2. プロセス終了を構成するポリシーの横にある［View Details（詳細の表示）］ボタンをダブルクリックします。
3. ［Edit Policy（ポリシーの編集）］ページで、［**Show Advanced Settings**（高度な設定の表示）］ボタンをクリックします。
4. ポリシーの［Advanced Settings（高度な設定）］パネルで、最後の設定である［Terminate processes with banned images（禁止イメージを含むプロセスを終了）］に移動します。［Status（ステータス）］メニューで、次のいずれかを選択します。
   - ［**Off**（オフ）］– 禁止を作成しても、実行中のプロセスは終了されません。また、禁止によって終了される実行中のプロセスもレポートされません。
   - ［**Report Only**（レポートのみ）］– 禁止を作成しても、実行中のプロセスは終了されませんが、この設定が［Active（アクティブ）］になっていれば終了されていたはずである実行中のプロセスがレポートされます。
   - ［**Active**（アクティブ）］– 禁止を作成することで、禁止イメージに一致する実行中のプロセスが終了されます。



5. ［Advanced Settings（高度な設定）］パネルの上にある［**Save**（保存）］ボタンをクリックします。
6. この設定を変更する他のポリシーについて、この手順を繰り返します。

第 9 章

レピュテーション承認ルール

この章では、レピュテーション承認ルールについて説明します。これらのルールを使用すると、Bit9 Software Reputation Service (SRS) によって設定されるファイルおよび公開者の信頼度に基づいて自動的にファイルを承認できるようになります。

注意

レピュテーション承認ルールを使用するには Bit9 SRS のアクティベーションが必要です。「Bit9 SRS の有効化」（787 ページ）を参照してください。

その他のファイル承認方法については第 8 章「ソフトウェアの承認と禁止」を参照してください。

セクション

概要

Bit9 Software Reputation Service (SRS) は既知のファイルに関するクラウドベースのデータベースで、Bit9 によりホストされています。このサービスは、ディストリビューション パートナー、Web クローラー、ハニーポット、Bit9 ユーザー コミュニティなどからファイル データを収集します。Bit9 SRS はデータベース内のファイルに関するコンテキスト情報（ファイルの公開者やファイルに関連付けられている製品など）を提供します。また、複数のマルウェア対策ツールを使用してソフトウェアを選別し、サードパーティの脆弱性データベースとの照合も行います。

Bit9 SRS は各ファイルの情報を使用して、各ファイルの脅威レベルと信頼度を設定します。また、公開者の信頼度も設定します。

レピュテーション承認ルールを使用すると、これらの信頼度に基づいて自動的にファイルを承認できます。レピュテーション承認ルールの作成時には次のようにオプションを設定します。

- ファイルのレピュテーションに基づいて承認するか、公開者のレピュテーションに基づいて承認するかを選択します（両方のオプションを同時に有効にすると、ルールの適用対象と効果が最大化されます）。
- ファイルと公開者を承認する際の信頼度のしきい値を設定します。
- すべてのエージェント管理コンピューターに対してレピュテーション承認を有効にするか、ポリシーごとにレピュテーション承認を有効にするかを選択します。
- 自動的に承認したくない特定の公開者またはファイルに対してレピュテーション承認を無効にすることもできます。

高度な脅威が懸念される場合、レピュテーション承認は信頼できるファイルのみを承認する方法として有効な選択肢であると言えます。レピュテーションに基づく自動承認を使用するとエンド ユーザーがより柔軟にファイルを使用できるようになり、承認済みファイルのホワイトリストを管理するための労力を軽減できます。ただし、レピュテーション承認はファイルの信頼度（そのファイルがどの程度安全と考えられるか）のみに基づく承認方式であり、各ファイルがビジネス環境に適しているかどうかは考慮されない点に注意してください。

レピュテーション承認を有効にしても、各ファイルまたは各公開者に手動で割り当てられている状態は引き続き有効であり、レピュテーションよりも優先されます。たとえば、名前やハッシュに基づいて禁止されているファイルはレピュテーションに基づいて承認された場合でも引き続きブロックされます。レピュテーション承認ルールがコンピューター上のファイルに適用されるタイミングと方法についてはこの章の後半で説明します。

ファイルと公開者の信頼度

ファイルの信頼度

Bit9 SRS は次の要素を考慮し、独自のアルゴリズムに基づいてファイルの信頼度を設定します。

- ［**Source Trust**（ソース信頼度）］– ファイルの出所
- ［**Publisher Trust**（公開者の信頼度）］– ファイルがデジタル証明書で署名されていて、その証明書が信頼できるものであるかどうか

- ［**Malware Severity**（マルウェアの深刻度）］– ウイルス対策製品によって悪意のあるファイルまたは悪意の疑いがあるファイル（ウィルスやマルウェア）と判断されたかどうか（Bit9 SRS データベース内のファイルは複数のウイルス対策製品によってスキャンされます）
- ［**Vulnerability Severity**（脆弱性の深刻度）］– そのファイルに既知の脆弱性（特にマイクロソフトから報告された脆弱性）が存在するかどうか。存在する場合はどの程度深刻な脆弱性か
- ［**Duration Seen**（認識期間）］– Bit9 SRS によりこのファイルが環境内で監視されている期間
- ［**First Seen**（最初の認識日時）］– Bit9 SRS によりこのファイルが環境内で最初に発見された日時
- ［**Prevalence**（普及度）］– このファイルが環境内でどの程度普及しているものとして Bit9 SRS にレポートされているか

各ファイルの信頼度は、これらの要素を組み合わせて計算されます。Bit9 SRS は各ファイルの信頼度を **0（信頼度最低）**から **10（信頼度最高）**の間で設定します。たとえば、既知の脆弱性が存在しない署名済みオペレーティング システム ファイルの信頼度はおよそ 10 に設定されるのに対し、広く知られていない Web サイトから配布された未署名のサードパーティ アプリケーションの信頼度はおよそ 3 に設定されます。また、既知のマルウェアや、既知のマルウェアを拡散するアプリケーションの信頼度はほぼ 0 に設定されます。

公開者の信頼度

公開者の信頼度は、その公開者から配布されたすべてのファイルに対するユーザー エクスペリエンスや、公開者の一般的なレピュテーションなど、さまざまな要素に基づいて設定されます。公開者の信頼度として設定される値には、［High（高）］、［Medium（中）］、［Low（低）］、［Not Trusted（信頼できない）］の 4 種類があります。公開者の信頼度が［Not Trusted（信頼できない）］に設定されている場合は、その公開者に関する情報がまったく存在しないか、その公開者の信頼レベルを昇格させる要素が存在しないことを意味します。

レピュテーション承認戦略

レピュテーション承認を有効にすると、信頼度の高いソフトウェアをエージェント管理コンピューターで自動的に実行できるため、管理作業の負荷を軽減することができます。レピュテーション承認をどのように導入するかは各組織の目標（特に利便性と安全性のバランス）に基づいて検討する必要があります。ファイルのレピュテーションに基づく承認と公開者のレピュテーションに基づく承認は別々に有効化することもできますが、両方を同時に有効にするとレピュテーション承認の利点を最大化することができます。

- **ファイルのレピュテーションに基づく承認** – 一部のファイルには公開者の署名が追加されていない場合があります。ファイルのレピュテーションに基づく承認を有効にすると、各ファイルが既知の公開者から配布されたものかどうかにかかわらず、Bit9 SRS で認識されているファイルに関するレピュテーション データを活用できます。
- **公開者のレピュテーションに基づく承認** – 公開者のレピュテーションに基づく承認を有効にすると、まだレピュテーションが設定されていない新しい

ファイルを含め、信頼できる公開者によって署名されたすべてのファイルが承認され、それらのファイルをエージェント管理コンピューター上で実行できるようになります。承認済みの公開者から配布されたファイルは、サーバーに接続されているエージェント管理コンピューター上でローカルに承認されます。

レピュテーション承認はすべてのコンピューターに対して有効にすることも、特定のポリシーに含まれるコンピューターのみに対して有効にすることもできます。レピュテーション承認の対象を特定のポリシーのみに限定してもパフォーマンスには影響しないため、どのファイルの実行を許可するかを厳密に管理する必要があるポリシーを除き、すべてのポリシーに対してレピュテーション承認を有効にすることをお勧めします。

注意

Bit9 SRS のアクティベーションを行うと、[Publishers（公開者）] タブに公開者の信頼度が表示されます。この情報を確認することで、公開者のレピュテーションに基づく承認を有効にした場合の結果を予測することができます。公開者のレピュテーションに基づく承認を有効にすると、信頼度が [High（高）] に設定されている公開者からのファイルはすべて承認されます。

承認する信頼レベルの設定

承認するファイルと公開者の信頼レベルは自由に設定できますが、推奨される 2 通りの組み合わせを以下に示します。

目標	ファイルの信頼度	公開者の信頼度
資産の保護を最優先する場合 – 知的財産や機密情報などを厳重に保護する必要がある場合	8	[High（高）]
資産の保護に柔軟性を持たせる場合 – コンピューターを危険なファイルから保護しつつ、脅威レベルが比較的低いファイルを自動的に承認する場合	6	[Medium（中）]

ファイルのレピュテーションに基づく承認と公開者のレピュテーションに基づく承認を両方とも有効にすると、ファイル自体のレピュテーション、または公開者のレピュテーションのいずれかがしきい値を超えている場合にファイルが承認されます。

これらの設定はバランスを考慮して適宜調整できますが、承認の基準とする信頼度を極端に低く設定することは推奨されません。承認の基準とする信頼度を変更した場合の影響は、コンソールの [File Catalog（ファイル カタログ）] と [Publishers（公開者）] リストを確認することで予測できます。これらのリストは信頼度別にグループ化されています。

信頼カテゴリーごとにファイルを表示するには、コンソール メニューで [**Assets**（アセット）] > [**Files**（ファイル）] を選択して、[**File Catalog**（ファイル カタログ）] タブをクリックし、[Group By（グループ別）] メニューで [**Trust**（信頼）] を選択します。

信頼カテゴリーごとに現在の公開者を表示するには、コンソール メニューで［**Rules**（ルール）］>［**Software Rules**（ソフトウェア ルール）］の順に選択して、［**Publishers**（公開者）］タブをクリックし、［Group by（グループ別）］メニューで［**Trust**（信頼）］を選択します。このリストに表示されるのは、エージェント管理コンピューターに登録されているファイルの公開者、またはエージェントがインストールされていないコンピューター上でファイルから証明書をインポートすることによって追加された公開者のみが表示されます。

ファイルのレピュテーションに基づく承認の仕組み

ファイルのレピュテーションに基づく承認は Bit9 SRS で認識されているファイルについての情報に基づいて実行されます。レピュテーションのしきい値を満たすファイルごとに（グローバルまたはポリシー別の）レピュテーション承認ルールが Bit9 Server 上に作成されます。レピュテーション承認の範囲はレピュテーションが有効になっているポリシーのリストに基づいて決定されます。他のファイル承認方法と同様に、レピュテーション承認はレピュテーションの設定に応じてポリシーごとの承認またはグローバルな承認と同様に動作します。

ファイル レピュテーション ルールのリストは Bit9 Server に表示されませんが、レピュテーションに基づいて承認されたファイルのリストは表示できます。「レピュテーション承認に関連するビュー」（354 ページ）を参照してください。

他の承認方法とは異なり、ファイルのレピュテーションに基づく承認はエンドポイントへ自動的にプッシュされません。レピュテーション承認が有効になっているエンドポイントに、レピュテーションに基づくファイルの承認がプッシュされる状況には次の 3 種類があります。

- いずれかのエンドポイントでブロックされているファイルの記録が Bit9 Server 上にあり、そのファイルが後でレピュテーションに基づいて承認された場合、サーバーはエージェントに対してそのファイルが承認されたことを即座に通知し始めます。
- レピュテーションに基づいて承認されたファイルのインスタンスを Bit9 Server に接続されたコンピューター上でユーザーが実行しようと試み、そのファイルがレピュテーション信頼度のしきい値を満たしていることがサーバーによって検出された場合、サーバーはエージェントに対してそのファイルの実行を即座に許可し、そのファイルが承認されたことを他のエージェントにも通知し始めます。
- レピュテーションに基づいて承認されたファイルがインストーラーであると判断された場合、Bit9 Server はエージェントに対してそのファイルが承認されたことを即座に通知し始めます。

ファイルがレピュテーションに基づいて承認され、他のルールによりブロックされなかった場合でも、上記いずれかの状況が発生してファイルの承認がエージェントに通知されない限り、そのファイルのインスタンスはローカルで承認されず、ファイルの承認が通知される前にエージェント コンピューターがサーバーに接続されていなかった場合はブロックされる可能性があります。

ファイルのレピュテーションに基づく承認の取り消し

ファイルのレピュテーションに基づく承認ルールが変更され、特定のファイルのレピュテーション承認が取り消された場合（レピュテーション承認が完全に無効化されたり、レピュテーション承認がポリシーごとに無効化されたり、承認のしきい値が引き上げられたり、ファイル自体のレピュテーションが下がった場合）

は、サーバーに接続されているコンピューター上でそのファイルのグローバルな承認が取り消され、[File Catalog（ファイル カタログ）] に表示されるファイルの状態が未承認に戻されます。レピュテーションに基づいて承認されたときにそのファイルのインスタンスが実行されていた場合、そのインスタンスは、承認時に実行されていたコンピューター上でローカルに承認され続けます。

ファイルまたは公開者に明示的に割り当てられている禁止や承認の状態はレピュテーション承認よりも優先されます。

注意

ファイルのレピュテーションに基づく承認を有効にすると、信頼レベルに基づいて各ファイルを承認するかどうかが最初に分析されるため、Bit9 Server のパフォーマンスに大きく影響する可能性があります。また、ファイルの承認を無効にしたり、承認のしきい値を変更した場合も、同様の影響が生じる可能性があります。ファイル レピュテーション ルールの設定は不必要に変更しないようにしてください。

公開者のレピュテーションに基づく承認の仕組み

公開者のレピュテーションに基づく承認を有効にすると、信頼できる公開者（指定されたしきい値を満たす公開者）のリストがすべてのコンピューターに送信されます。この承認済み公開者リストを受信した Bit9 エージェントは、承認済み公開者から新しいファイルが配布されたときにサーバーに接続されていなくても、検出されると同時にそれらのファイルを承認することができます。また、承認済み公開者から配布された既存のファイルは、明示的に禁止されていない限り、未承認のファイルも含めてすべて承認されます。

公開者のレピュテーションに基づく承認は Bit9 Server およびネットワーク トラフィックにほとんど影響を及ぼしません。

公開者を手動で承認する場合と同様に、公開者のレピュテーションに基づく承認の対象となるファイルは、「公開者による承認または禁止」で説明されている要件をすべて満たす証明書を使用して署名されたファイルのみです。

公開者のレピュテーションに基づく承認の取り消し

公開者のレピュテーションに基づきローカルで承認されたファイルがある場合、その公開者の承認が後で取り消されても、そのファイルのローカルでの承認は取り消されません。公開者のレピュテーションが変わったり、レピュテーション承認の設定が変更されたり、レピュテーション承認が完全に無効化されるなどして、公開者の承認が取り消された場合でも、その影響が及ぶのは以後に検出されたファイルのみです。

レピュテーションに基づく承認が取り消された公開者のファイルを未承認の状態に戻すには、[Files on Computers（コンピューター上のファイル）] または [File Instance Details（ファイル インスタンスの詳細）] ページでインスタンスごとにローカルでの承認を取り消します。特定の公開者が禁止の対象になった場合は、公開者のレピュテーションに基づいてローカルで承認されたファイルが自動的に未承認の状態に戻されるため、ローカルでの承認をインスタンスごとに手動で取り消す必要はありません。

公開者の承認に基づいてローカルで承認されたファイルを明示的に禁止すると、そのファイルのローカルでの承認が取り消されます。

レピュテーション承認とその他の Bit9 ルール

レピュテーション ルールはコンソールから実行される他のアクションの影響を受ける場合があります。

- 名前やハッシュに基づいて特定のファイルを識別するファイル ルールが明示的に設定されると、そのファイルに対するレピュテーション承認が自動的に無効になります。これにはグローバルおよびポリシー固有のファイル ルール（ブロックと承認）、承認または禁止するハッシュのインポート済みリストに含まれるファイル、信頼済みディレクトリ、手動でブロックまたは承認された公開者などが含まれます。レピュテーションに基づく制御の対象から除外されたファイルは、レピュテーションの設定やしきい値に基づいて自動的に承認されなくなります。
- レピュテーションが無効になっているファイルの状態をレピュテーションに基づいて制御できるようにするには、明示的なルール（承認または禁止）を削除し、そのファイルのレピュテーションを再度有効にする必要があります。
- ファイルへのアクセスを直接ブロックまたは許可するカスタムルールは、ファイルまたは公開者のレピュテーションに基づく承認よりも優先されます。

ファイルと公開者の例外の作成

レピュテーション承認を有効にすると、Bit9 SRS の情報を利用して信頼済みファイルが不必要にブロックされないようにすることができるため、通常はこの機能を有効にしておくことをお勧めします。ただし、Bit9 SRS でのレピュテーションにかかわらず特定のファイルや公開者が承認されないようにする必要が生じる場合があります。そのため、個々のファイルまたは公開者ごとにレピュテーション承認を無効にするオプションが用意されています。

注意

Bit9 Server でレピュテーション機能を有効にする前にファイルまたは公開者の例外を作成すると、指定されたファイルや公開者はレピュテーション ルールの影響を受けなくなります。レピュテーション ルールが有効化された後に例外を追加すると、新しく検出されたファイルのレピュテーション承認が無効になり、ファイルのレピュテーションに基づくグローバルな承認が取り消されますが、レピュテーションに基づいて承認された公開者のファイルに対するローカルでの承認は取り消されません。

ファイルごとのレピュテーション承認の無効化

レピュテーション承認はファイルごとに無効化できます。サーバー上でレピュテーション ルールを有効にする前に例外を作成すると、指定されたファイルのインスタンスに対するレピュテーション承認が無効になります。レピュテーション ルールを有効にした後に例外を作成すると、他の承認が適用されていない限り、

レピュテーションに基づいて承認されたファイルは（グローバルとローカルの両方で）未承認の状態に戻されます。ただし、何らかの方法で（公開者の承認やカスタム ルールに基づいて）既にローカルで承認されているファイルは引き続きローカルで承認されます。

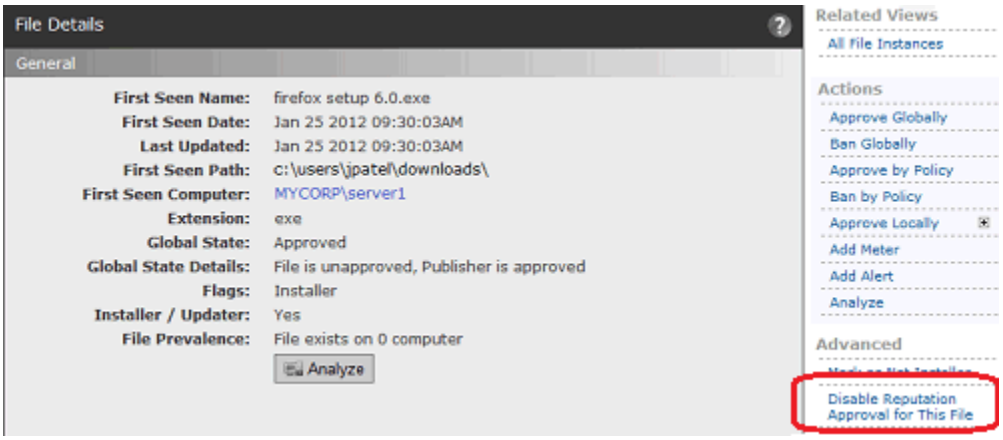
特定のファイルのレピュテーションを無効にした場合、そのファイルがインストーラーであっても、レピュテーションが無効になるのはそのファイルのみです。

ファイルのレピュテーション承認の無効化手順：

1. 設定を変更するファイルの［File Details（ファイルの詳細）］ページまたは［File Instance Details（ファイル インスタンスの詳細）］ページを開きます。
2. メイン ページの右にある［Advanced（詳細）］メニューで［**Disable Reputation Approval for this File**（このファイルのレピュテーション承認の無効化）］をクリックします。そのファイルのレピュテーション承認が無効になります。

ファイルのレピュテーション承認の再有効化手順：

- ［File Details（ファイルの詳細）］ページまたは［File Instance Details（ファイル インスタンスの詳細）］ページにある［Advanced（詳細）］メニューで［Enable Reputation Approval for this File（このファイルのレピュテーション承認の有効化）］をクリックします。



公開者ごとのレピュテーション承認の無効化

レピュテーション承認は公開者ごとに無効化できます。サーバー上でレピュテーション ルールを有効にする前に例外を作成すると、指定された公開者からのファイルのインスタンスに対するレピュテーション承認が無効になります。レピュテーション ルールを有効にした後に例外を作成すると、その公開者を無効にする前にエージェント管理コンピューター上で検出された承認済み公開者からのファイルは既にレピュテーションに基づいてローカルで承認されているため、公開者が無効にされてもそれらのファイルは未承認の状態に戻されません。公開者の承認を無効にした後にこの Bit9 Server で初めて検出されたファイルのみが公開者のレピュテーションの影響を受けなくなります。

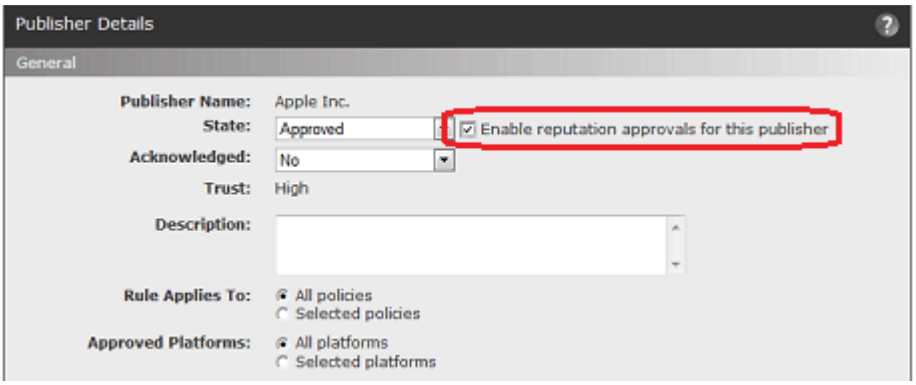
公開者のレピュテーション承認の無効化手順：

1. 設定を変更する公開者の［Publisher Details（公開者の詳細）］ページを開きます。

2. ［Enable reputation approvals for this publisher（この公開者のレピュテーション承認の有効化）］の隣にあるチェックボックスをオンにします。
3. ［**Save**（保存）］ボタンをクリックします。その公開者のレピュテーション承認が無効になります。

公開者のレピュテーション承認の再有効化手順：

- ［Publisher Details（公開者の詳細）］ページで［Enable reputation approvals for this publisher（この公開者のレピュテーション承認の有効化）］をオンにします。



レピュテーション承認の有効化

このセクションでは、Bit9 Server でレピュテーション承認機能を有効にする方法について説明します。レピュテーション承認を有効にする前に：

- レピュテーション承認の対象から除外する必要があるファイルや公開者の例外を検討してください。これらの例外は、レピュテーション承認機能を有効にする前に作成する必要があります。詳細については、「ファイルと公開者の例外の作成」（349 ページ）を参照してください。
- レピュテーション承認をすべてのエージェント管理コンピューターで使用できるようにするか、特定のポリシーに含まれるエージェント管理コンピューターのみで使用できるようにするかを検討してください。この選択は下記の手順にも含まれています。

Bit9 Server でレピュテーションを有効にした後でもファイルや公開者の例外を追加することは可能ですが、公開者のレピュテーションに基づいて既にローカルで行われた承認は公開者の例外を作成しても取り消されません。

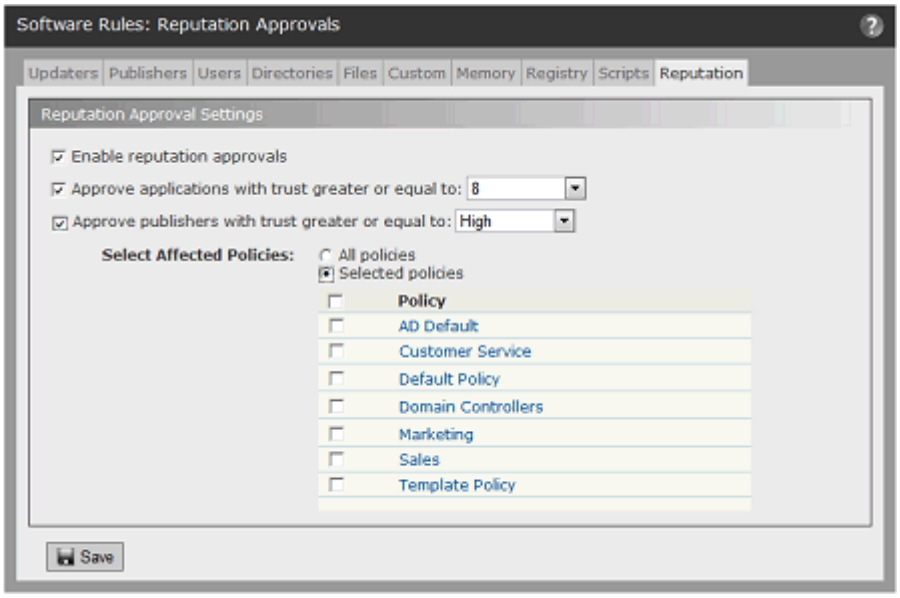
レピュテーション承認の有効化手順：

1. コンソール メニューで、［**Rules**（ルール）］>［**Software Rules**（ソフトウェア ルール）］の順に選択します。［Software Rules（ソフトウェア ルール）］ページが表示されます。
2. ［Software Rules（ソフトウェア ルール）］ページで［**Reputation**（レピュテーション）］タブをクリックします。［Reputation Approvals（レピュテーション承認）］ページが表示されます。

注意

レピュテーション承認を有効にする前に Bit9 SRS のアクティベーションを行う必要があります。Bit9 SRS のアクティベーションが行われていない場合は［Software Rules（ソフトウェア ルール）］ページに［Reputation（レピュテーション）］タブが表示されません。その場合は、次の手順に進む前に「Bit9 SRS の有効化」（787 ページ）の手順に従ってください。

3. ［Enable reputation approvals（レピュテーション承認の有効化）］チェックボックスをオンにします。ページ内のフィールドが編集可能になります。



4. ファイルのレピュテーション承認を有効にするには、［Approve applications with a trust greater or equal to（次の信頼度以上のアプリケーションを承認）］チェックボックスがオンになっていることを確認し、メニューから信頼レベルを選択します。ファイルの信頼レベルは 1（信頼度最低）から 10（信頼度最高）の間で選択できます。推奨される設定については、「承認する信頼レベルの設定」（346 ページ）を参照してください。

5. レピュテーションに基づく公開者の承認を有効にするには、［Approve publishers with a trust greater or equal to（次の信頼度以上の公開者を承認）］チェックボックスがオンになっていることを確認し、メニューから公開者の信頼レベルを選択します。公開者の信頼レベルには、［Low（低）］、［Medium（中）］、［High（高）］の 3 種類があります。

6. レピュテーション承認を有効にするポリシーを選択します。
   a. すべてのポリシーに対してルールを有効にするには、[All policies（すべてのポリシー）] ラジオ ボタンをクリックします。
   b. 特定のポリシーのみに対してルールを有効にするには、[Selected policies（選択されたポリシー）] ラジオ ボタンをクリックし、ルールを有効にする各ポリシーの隣にあるチェックボックスをオンにします。

   注意

   [Edit Policy（ポリシーの編集）] ページでもポリシーごとにレピュテーション承認を有効または無効にすることができます。

7. レピュテーション承認の設定が完了したら、ページの下部にある [**Save**（保存）] ボタンをクリックし、確認ダイアログで **[OK]** を選択します。レピュテーション承認が有効になります。

   注意

   ファイルのレピュテーション承認を有効にすると、膨大な数のファイルの状態を再評価する必要が生じる可能性があります。ファイル状態の変更はコンソールですぐには確認できませんが、これらの変更は新しい承認ルールに基づいてすべてのファイル状態が更新されるまでバックグラウンドで継続されます。承認の処理が完全に終わるまでに数分以上かかる場合があります。

レピュテーション承認の変更と無効化

レピュテーション承認機能を変更または無効化するには、それらの機能を有効にした場所から設定を変更する必要があります。変更には、ファイルや公開者の信頼度しきい値の変更や、レピュテーション承認の対象となるポリシーの変更などが含まれます。一方の種類（公開者またはファイル）のレピュテーション承認のみを無効にして他方のレピュテーション承認を有効にしておくこともできます。

レピュテーション承認の変更または無効化の影響は、有効化されている承認の種類によって異なります。また、レピュテーション承認を変更するとルールの再評価が行われるため、ネットワークにも影響します。

- ファイルのレピュテーション承認のしきい値を変更すると変更の処理中にサーバーやネットワーク トラフィックに 1 回限りの多大な影響が生じることがあります。ファイル カタログの評価と更新は数分で完了しますが、エージェント数とファイル カタログのサイズによっては、新しいファイル状態情報がすべてのエージェントに送信されるまでに数時間から数日かかる場合があります。
- 承認しきい値を変更する場合と同様に、ファイルの承認を無効にする場合もネットワークに多大な影響が生じることがあり、新しいファイル状態情報がすべてのエージェントに送信されるまでに数時間から数日かかる場合があります。

- 公開者承認ルールまたはポリシーの適用範囲の変更は特に大きな影響を及ぼしません。
- 公開者の承認を無効にしても、公開者のレピュテーションに基づいて既にローカルで承認されたファイルの承認が取り消されることはありません。

レピュテーション承認機能の変更および無効化手順：

1. コンソール メニューで［**Rules**（ルール）］>［**Software Rules**（ソフトウェア ルール）］を選択し、［**Reputation**（レピュテーション）］タブをクリックします。［Reputation Approvals（レピュテーション承認）］ページが表示されます。
2. 必要な変更を加え、［**Save**（保存）］をクリックします。

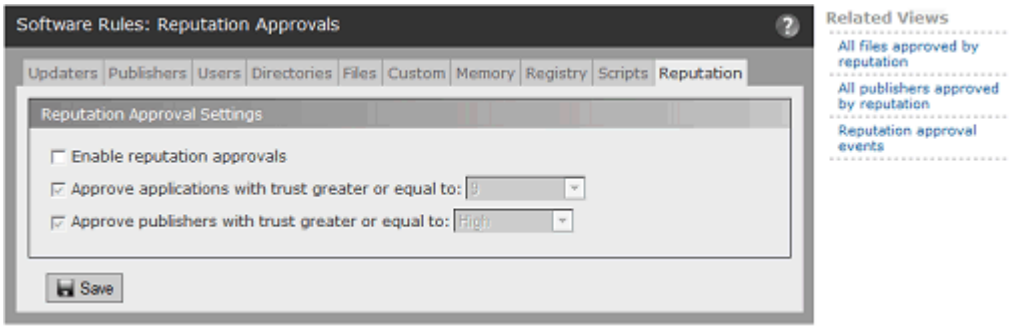
注意

- ［Edit Policy（ポリシーの編集）］ページでもポリシーごとにレピュテーション承認を有効または無効にすることができます。
- レピュテーション承認の対象から除外する必要があるファイルや公開者に関しては例外を作成できます。「ファイルと公開者の例外の作成」（349 ページ）を参照してください。

レピュテーション承認に関連するビュー

［Reputation Approvals（レピュテーション承認）］ページの右側にある［Related Views（関連ビュー）］メニューには、コンソール内で確認できる承認関連の追加情報へのリンクが表示されます。

- ［**All files approved by reputation**（レピュテーションに基づいて承認されたすべてのファイル）］– このリンクをクリックすると［File Catalog（ファイル カタログ）］ページが表示され、レピュテーションに基づいてグローバルに承認されたすべてのファイルが表示されるようにフィルターが適用されます。
- ［**All publishers approved by reputation**（レピュテーションに基づいて承認されたすべての公開者）］– このリンクをクリックすると［Software Rules（ソフトウェア ルール）］ページの［Publishers（公開者）］タブが表示され、レピュテーションに基づいて承認されたすべての公開者が表示されるようにフィルターが適用されます。
- ［**Reputation approval events**（レピュテーション承認イベント）］– このリンクをクリックすると［Events（イベント）］ページが表示され、（公開者とファイルの）レピュテーション承認に関連するすべてのイベントが表示されるようにフィルターが適用されます。



これらのビューには、レピュテーション承認が各コンピューターにどのような影響を与え、レピュテーション承認の設定または各ファイルおよび各公開者の状態をどのように変更する必要があるかを把握する際に役立つ情報が表示されます。

ファイルや公開者を表示するその他のビューには次のフィールドがあり、これらを確認することでファイルや公開者がレピュテーション承認の影響を受けているかどうかを把握できます。

- ［**File State Reason**（ファイルの状態の理由）］– ファイルのレピュテーションに基づいてファイルが承認された場合は、このフィールドに［Reputation（レピュテーション）］と表示されます。承認された公開者がファイルに関連付けられている場合は、［File State Reason（ファイルの状態の理由）］に［Reputation（レピュテーション）］以外の理由が表示されていても、［File State（ファイルの状態）］に［Approved by Reputation（レピュテーションに基づいて承認済み）］と表示されることがあります。
- ［**Publisher State Reason**（公開者の状態の理由）］– レピュテーションに基づいてファイルの公開者が承認された場合は、このフィールドに［Reputation（レピュテーション）］と表示されます。
- ［**Reputation Enabled**（レピュテーション有効）］（ファイル）– ［File Details（ファイルの詳細）］および［File Instance Details（ファイル インスタンスの詳細）］ページにある［Reputation Enabled（レピュテーション有効）］フィールドには、現在のファイルに対してファイルのレピュテーション承認が有効になっているかどうかが表示されます。このフィールドは［Files Catalog（ファイル カタログ）］ページと［Files on Computers（コンピューター上のファイル）］ページにも追加できます。このフィールドに［Yes（はい）］と表示されている場合は、ファイルが承認されたことを意味するのではなく、そのファイルに対してレピュテーション承認が有効になっていることを意味します。
- ［**Reputation Enabled**（レピュテーション有効）］（公開者）– ［Software Rules（ソフトウェア ルール）］ページの［Publishers（公開者）］タブでは、表示されている各公開者に対してレピュテーション承認が有効になっているかどうかを示す列を追加できます。ファイルの場合と同様に、このフィールドに［Yes（はい）］と表示されている場合は、公開者が承認されたことを意味するのではなく、その公開者に対してレピュテーション承認が有効になっていることを意味します。

第 10 章

ファイル署名証明書の管理

この章では、Bit9 ファイル監視および適用アクティビティでファイル署名証明書を使用するための高度な機能について説明します。これらの機能では、以下のことができます。

- **証明書の検出およびインベントリ** – エージェントで検出されるファイル署名証明書に関する情報とチェーン内のすべての証明書は、Bit9 Server データベースに収集および格納されます。
- **証明書の状態による適用** – 証明書チェーン内の証明書は、特定の公開者に対して承認または禁止できます。また、証明書の状態を使用し、Bit9 Platform で管理されているファイルを承認または禁止できます。

プラットフォームに関する注意

これらの証明書の可視性および制御機能は Windows オペレーティングシステムを実行しているコンピューターでのみ使用できます。

セクション

概要

Bit9 Platform では、証明書で特定された発行者の「名前」により、公開者を承認または禁止できます。証明書の公開者名が承認されている公開者と一致する場合、その証明書で署名されたファイルは、他のルールによって禁止されていない限り承認されます。証明書の公開者名が禁止されている公開者と一致する場合、その証明書で署名されたファイルは禁止されます。証明書内に特定の公開者名があるファイルはすべて、Bit9 Server で定義されているその公開者の状態の影響を受けます。こうしたルールについては、「公開者による承認または禁止」（288 ページ）を参照してください。

この章で説明する証明書の管理機能により、公開者の承認にセキュリティと情報のレイヤーがもう 1 つ追加されることになります。証明書内の公開者名は、各中央当局によって制御されるものではありません。一方、証明書そのものは制御されます。証明書は、個人、サーバー、会社、またはその他のエンティティを特定し、その ID を公開鍵と関連付けます。証明書は、公開鍵暗号に基づいて身元を証明するものとして、一般的に認識されています。証明書によって認証された公開鍵だけが、その証明書により特定されるエンティティが持つ対応した秘密鍵と連携します。ここではエンティティはファイルです。

ファイル署名証明書は、証明書チェーンまたはパスの終端にあるリンクです。ルート証明書は、最初の信頼を付与するエンティティを特定します。この証明書は、中間証明書に署名するために使用される場合があります。続いてこの中間証明書が、ファイルを具体的に特定する最終的なリーフ証明書に対して信頼を付与します。パス内には複数の中間証明書がある場合もあります。

Bit9 エージェントは、Bit9 で検出される署名済みファイルの信頼のパス内にある、特定可能で有効な証明書をすべてレポートします。署名証明書のパス内の証明書は、いずれも承認または禁止できます。証明書に承認または禁止の状態が指定されている（または未承認のままの）場合、その状態はリーフ証明書の特定の公開者に対してのみ適用されます。同じ証明書が、別の発行者が署名したファイルの証明書チェーン内に偶然存在する場合、そのファイルに影響を与えるには、証明書を別個に承認または禁止する必要があります。

注意

2013 年後半に Microsoft はセキュリティ情報 MS13-098 を公開し、そこでリモート コードを実行できる可能性がある Authenticode シグネチャ検証の脆弱性について説明しています。これに応じて、Microsoft では、Windows Authenticode シグネチャ フォーマットで署名されたバイナリに対するシグネチャ検証方法を変更する、サポートされているすべての Microsoft Windows リリースを対象とした更新プログラムを発表しました。

この変更を有効にすると、Windows Authenticode シグネチャ検証で WIN_CERTIFICATE 構造の外部情報が許可されず、Windows で非準拠バイナリが署名済みとして認識されることがなくなります。この新しい動作を有効にすると、前に公開者によって承認されたファイルが、Bit9 管理システムでブロックされる可能性があります。

この変更はセキュリティ情報 MS13-098 に含まれますが、（2014 年 7 月時点では）オプトイン ベースでのみ有効になります。ただし、Microsoft は、Microsoft Windows の今後のリリースでこれをデフォルトの動作にすると発表しています。

この変更の詳細については、https://technet.microsoft.com/library/security/2915720 を参照してください。

証明書管理機能の概要

Bit9 証明書管理機能には、以下の固有の機能が含まれています。

- コンソール メニューで、[**Assets**（アセット）] > [**Certificates**（証明書）] の順に選択し、[**Certificates**（証明書）] テーブルを開きます。[Certificates（証明書）] テーブルには、エージェント管理コンピューターで見つかった、ファイルの署名または連署に使用されるすべてのリーフ証明書と、これらのリーフ証明書のパス内のすべての証明書が表示されます。
- テーブル内の証明書の横にある [View Details（詳細の表示）] ボタンをクリックすると、その証明書の [**Certificate Details**（証明書の詳細）] ページが開きます。[Certificate Details（証明書の詳細）] ページには、1 つの証明書の全詳細が表示されます。また、その証明書によって署名されたすべてのファイルのテーブルなど、その証明書に関係する関連ビューへのリンクがあります。
- 各公開者の [**Publisher Details**（公開者の詳細）] ページには、[**All Certificates for This Publisher**（この公開者のすべての証明書）] パネルがあります。このパネルには、証明書のサブジェクト名の CN 部分にこの公開者名を含んでいる証明書がすべて表示されます。またこのパネルには、この公開者に関連付けられているリーフ証明書の証明書パス内の各証明書の承認や禁止の状態が表示され、各証明書の承認や禁止を追加または削除できます。
- 証明書関連フィールドは、[**File Details**（ファイルの詳細）] と [**File Instance Details**（ファイル インスタンスの詳細）] ページにあります。
- [**System Configuration**（システム構成）] ページの [**Advanced Options**（高度なオプション）] タブにある [**Certificate Options**（証明書オプション）] パネルには、ファイルの承認に使用される場合に証明書が満たす必要のある要件 (鍵の長さやアルゴリズムなど) を決定する設定があります。エージェントが独自の証明書の失効検査を実行できるようにするルールを構成できます。
- エージェント　ベースの証明書の失効検査が有効かどうかに関係なく、Bit9 Server はインベントリの証明書を繰り返し検証して、その証明書が失効していないことを確かめます。この検証は通常毎週行われ、証明書失効リスト (CRL) を登録機関からダウンロードしたり、OCSP (Online Certificate Status Protocol) 応答者に対して OCSP 呼び出しを行ったりします。ネットワーク トラフィックを監視している場合は、このようなダウンロードに、さまざまな国のさまざまなサイトが含まれている可能性があることに注意してください。
  サーバー ベースの検証検査では、証明書の状態が変わったときに管理者に通知されますが、ルールの適用はこの影響を受けません。ルールの動作が失効の影響を受けるようにするには、エージェント ベースの失効検査を有効にします。
- トリガー条件が発生すると証明書関連の [**Events**（イベント）] や [**Alerts**（アラート）] が表示されることがあります。

証明書情報の表示

証明書情報は Bit9 コンソールの複数の場所で利用できます。この情報は特定の証明書を承認または禁止するかどうかを決定するときに役立ちます。

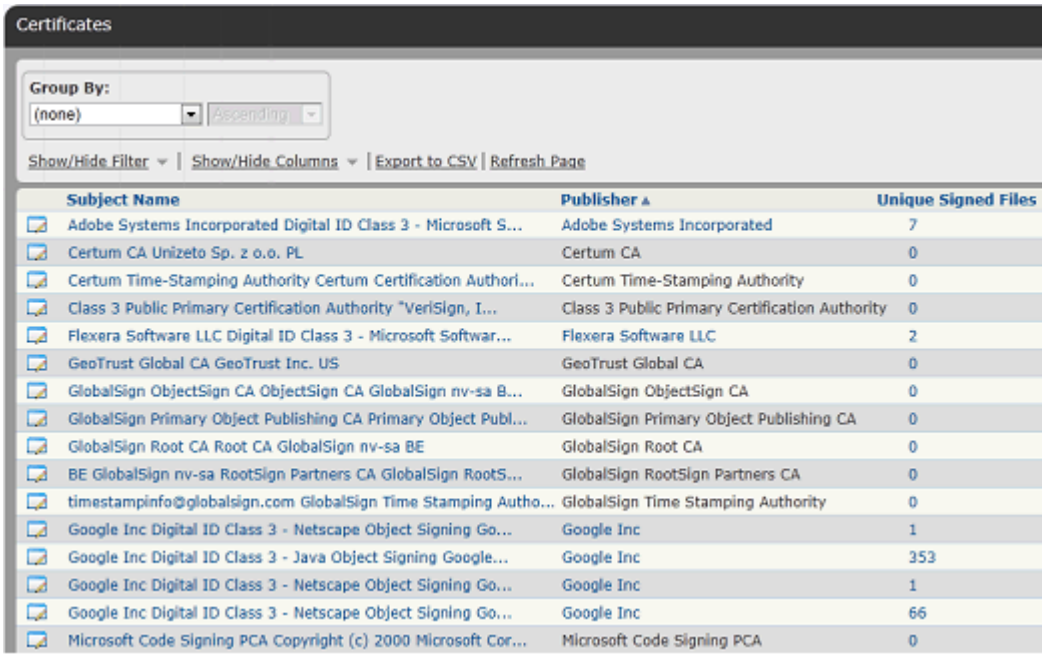
証明書テーブル

［Certificates（証明書）］テーブルには、エージェント管理コンピューターで見つかった、ファイルの署名または連署に使用されるすべてのリーフ証明書と、これらのリーフ証明書のパス内のすべての証明書が表示されます。このテーブルでは、各証明書の［Certificate Details（証明書の詳細）］ページにアクセスできます。［View Details（詳細の表示）］ボタンまたはテーブル内のサブジェクト名をクリックすると、証明書の詳細を確認できます。

［Certificate（証明書）］テーブルは読み取り専用ページです。［Action（アクション）］メニューはありません。証明書の状態は、［Publisher Details（公開者の詳細）］ページで、公開者ごとにのみ変更できます。詳細については、「公開者の証明書の承認または禁止」（372 ページ）を参照してください。

証明書テーブルを表示する手順：

- コンソール メニューで、［**Assets**（アセット）］>［**Certificates**（証明書）］の順に選択します。



Subject Name	Publisher	Unique Signed Files
Adobe Systems Incorporated Digital ID Class 3 - Microsoft S...	Adobe Systems Incorporated	7
Certum CA Unizeto Sp. z o.o. PL	Certum CA	0
Certum Time-Stamping Authority Certum Certification Authori...	Certum Time-Stamping Authority	0
Class 3 Public Primary Certification Authority "VeriSign, I...	Class 3 Public Primary Certification Authority	0
Flexera Software LLC Digital ID Class 3 - Microsoft Softwar...	Flexera Software LLC	2
GeoTrust Global CA GeoTrust Inc. US	GeoTrust Global CA	0
GlobalSign ObjectSign CA ObjectSign CA GlobalSign nv-sa B...	GlobalSign ObjectSign CA	0
GlobalSign Primary Object Publishing CA Primary Object Publ...	GlobalSign Primary Object Publishing CA	0
GlobalSign Root CA Root CA GlobalSign nv-sa BE	GlobalSign Root CA	0
BE GlobalSign nv-sa RootSign Partners CA GlobalSign RootS...	GlobalSign RootSign Partners CA	0
timestampinfo@globalsign.com GlobalSign Time Stamping Autho...	GlobalSign Time Stamping Authority	0
Google Inc Digital ID Class 3 - Netscape Object Signing Go...	Google Inc	1
Google Inc Digital ID Class 3 - Java Object Signing Google...	Google Inc	353
Google Inc Digital ID Class 3 - Netscape Object Signing Go...	Google Inc	1
Google Inc Digital ID Class 3 - Netscape Object Signing Go...	Google Inc	66
Microsoft Code Signing PCA Copyright (c) 2000 Microsoft Cor...	Microsoft Code Signing PCA	0

デフォルトのテーブルには、各証明書に関する重要な情報が含まれている特定の列が表示されます。Bit9 のテーブルでは、［Show/Hide（表示 / 非表示）］パネルを使用して、テーブル ビューの列を追加または削除できます（テーブル ビューのカスタマイズに関する詳細については、「Bit9 コンソールのテーブル」（68 ページ）を参照）。表 40 には、［Certificate（証明書）］テーブルと［Certificate Details（証明書の詳細）］ページで利用できるフィールドについて示します。これらのフィールドの一部は、デフォルトではテーブルに表示されないことに注意してください。

表 40：[Certificate（証明書）] テーブルと [Certificate Details（証明書の詳細）] ページのフィールド

フィールドまたは列	ソース	表示場所	説明
注意：表示場所の列の T はテーブル ページ、D は詳細ページを表します。			
Subject Name（サブジェクト名）	証明書	T、D	証明書を識別できるサブジェクト名。この場合はファイルの署名者です。 テーブルでは名前は短縮されていますが、ツールチップには完全なサブジェクト名が表示されます。テーブル内の名前をクリックすると、その証明書の詳細ページが表示されます。
Publisher（公開者）	証明書	T、D	証明書のサブジェクト名の CN 部分で特定された公開者名。 公開者がファイル カタログ内のファイルに署名している場合、名前をクリックすると Publisher Details（公開者の詳細）] ページが開きます。表示されている一部の「公開者」は、実際のソフトウェア公開者ではなく認証局であるため、名前にリンクがありません。
Unique Signed Files（一意の署名済みファイル）	Bit9	T、D	この証明書によって署名されているファイル カタログ内の一意のファイルの数。1 以上の場合、数字をクリックすると、フィルターされた File Catalog（ファイル カタログ）] が開き、これらのファイルが表示されます。
Path Position（パスの位置）	証明書	T	サーバーにカタログ登録されている証明書パス内のこの証明書の位置。値は、[Root（ルート）]、[Intermediary（中間）]、[Leaf（リーフ）] のいずれかです。 証明書パスの位置、エージェントの違い、および証明書管理への影響に関する詳細については、「パスの位置とエージェントの差異」（371 ページ）を参照してください。
Root Certificate（ルート証明書）	証明書	D	ルート証明書であるかどうかです。値は、[Yes（はい）]、[No（いいえ）] のどちらかです。
Global State（グローバル状態）	Bit9	T、D	この証明書の有効な状態です。この証明書で特定された公開者の状態、証明書の状態、証明書パスの状態、および証明書の構成設定により決定されます。証明書のグルーバル状態の決定方法、値、および他のオブジェクトの状態との相互影響については、「証明書のグローバル状態」（374 ページ）を参照してください。

フィールドまたは列	ソース	表示場所	説明
Certificate State（証明書の状態）	Bit9	T	この公開者の証明書に指定されている状態。 値は、[Approved（承認）]、[Unapproved（未承認）]、[Banned（禁止）] のいずれかです。この状態が証明書のグローバル状態とファイル状態にどのような影響を及ぼすかについては、「証明書のグローバル状態」（374 ページ）を参照してください。
Certificate State Details（証明書の状態の詳細）（詳細ページ内） Global State Details（グローバル状態の詳細）（テーブル内）	Bit9 と証明書	T、D	証明書のグローバル状態に影響しているすべての要素の詳細な説明。 詳細については、「証明書のグローバル状態」（374 ページ）を参照してください。
Valid From（有効開始日）	証明書	T、D	この証明書が有効になる日付です。形式は、MMM DD YYYY HH:MM:SS AM/PM (UTC) です。
Valid To（有効期限日）	証明書	T、D	この証明書の有効期限日です。形式は、MMM DD YYYY HH:MM:SS AM/PM (UTC) です。
Signature Algorithm（署名アルゴリズム）	証明書	T、D	証明書の署名の作成に使用されたアルゴリズムです。一般的な値は、MD2RSA, MD5RSA, SHA1RSA, SHA256RSA です。 このフィールドに関係する構成設定については、「証明書の承認構成の選択項目」（370 ページ）を参照してください。
Thumbprint（拇印）	証明書	T、D	この証明書の SHA1 ハッシュ値。
Certificate ID（証明書 ID）	Bit9	T、D	この証明書の一意のBit9生成ハッシュ識別子。
First Seen Date（最初に確認された日付）	Bit9	T、D	この Bit9 Server でこの証明書が最初に確認され、登録された日時。
Last Modified Date（最終変更日）（詳細ページ内） Date Modified（変更日）（テーブル内）	Bit9	T、D	この Bit9 Server でこの証明書のレコードが最後に変更された日時。
Description（説明）	Bit9	T、D	コンソールのユーザーがこの証明書についてのコメントを追加または変更できる編集可能なフィールド。

フィールドまたは列	ソース	表示場所	説明
Last Validation Date（最終検証日）	Bit9	T、D	この証明書が Bit9 サーバーで最後に検証された日時。証明書は検出時に検証され、定期的に再検査されます。
Public Key Algorithm（公開鍵アルゴリズム）	証明書	T、D	公開鍵の作成に使用されたアルゴリズム。
Public Key Size（公開鍵サイズ）	証明書	T、D	この証明書の公開鍵のサイズ。 サイズの設定については、「証明書の承認構成の選択項目」（370 ページ）を参照してください。
Serial Number（シリアル ナンバー）	証明書	T、D	その発行認証局の証明書の中で一意の数字を含んでいる、証明書内のフィールド。
Type（タイプ）	???	T?D	証明書が埋め込まれているかデタッチされているか、またはその両方か、ファイルに署名するために署名が使用されているか、または署名に連署するために署名が使用されているか（通常はタイムスタンプの検証用）。リーフ証明書のみ。 値は、[Embedded（埋め込み）]、[Detached（デタッチ）]、[Signer（署名者）]、[Cosigner（副署者）] のいずれかになります。各証明書にはこれらの値が 2 つ以上あります。 種類と証明書管理への影響に関する詳細については、「証明書の種類」（371 ページ）を参照してください。
Validation Error（検証エラー）（テーブル内） Validation Message（検証メッセージ）（詳細ページ内）	証明書	T、D	証明書が検査されたときにエラー メッセージが返された場合に表示されます。証明書の検査でエラーが発生しなかった場合、このフィールドは空白です。返される可能性のあるメッセージのリストについては、http://msdn.microsoft.com/en-us/library/windows/desktop/aa377590(v=vs.85).aspx を参照してください。 多くの証明書で、必ずしも重大なリスクではない理由を示す検証エラーが表示されます。たとえば、認証局が古い証明書の情報の提供を（したがって検証を）中止する可能性があることなどです。

フィールドまたは列	ソース	表示場所	説明
History（履歴）	Bit9	D	パネルには以下の項目があります。 • [First Seen Date（最初に確認された日付）] - Bit9 環境でこの証明書が最初に確認された日時。 • [Last Modified By（最終変更者）] – この証明書の状態に対して最新の変更を行ったコンソール ユーザー（テーブルでは表示されません）。 • [Last Modified Date（最終変更日）] – この証明書の状態に対して最新の変更が行われた日時。
Certificate Path（証明書パス）	証明書	D	この証明書の証明書パスがパネルに表示されます。リスト内の各項目（現在の証明書を除く）は、パス内の他の証明書の詳細へのリンクになっています。

[Certificate（証明書）] テーブルの検索、並べ替え、およびグループ化

標準のテーブルのカスタマイズ方法を使用して、特定の証明書を表示または検索できます。たとえば、[Show/Hide Filters（フィルターの表示 / 非表示）] メニューを使用してサブジェクト名やハッシュで特定の証明書を検索したり、[Group by（グループ別）] メニューを使用して証明書を特定のフィールドごとに整理したりすることが可能です。[Group by（グループ別）] メニューには次の選択肢があります。

- Subject Name（サブジェクト名）
- Publisher（公開者）
- Unique Signed Files（一意の署名済みファイル）
- Path Position（パスの位置）
- Global State（グローバル状態）
- Certificate State（証明書の状態）
- Valid From（有効開始日）
- Valid To（有効期限日）
- Signature Algorithm（署名アルゴリズム）
- Thumbprint（拇印）

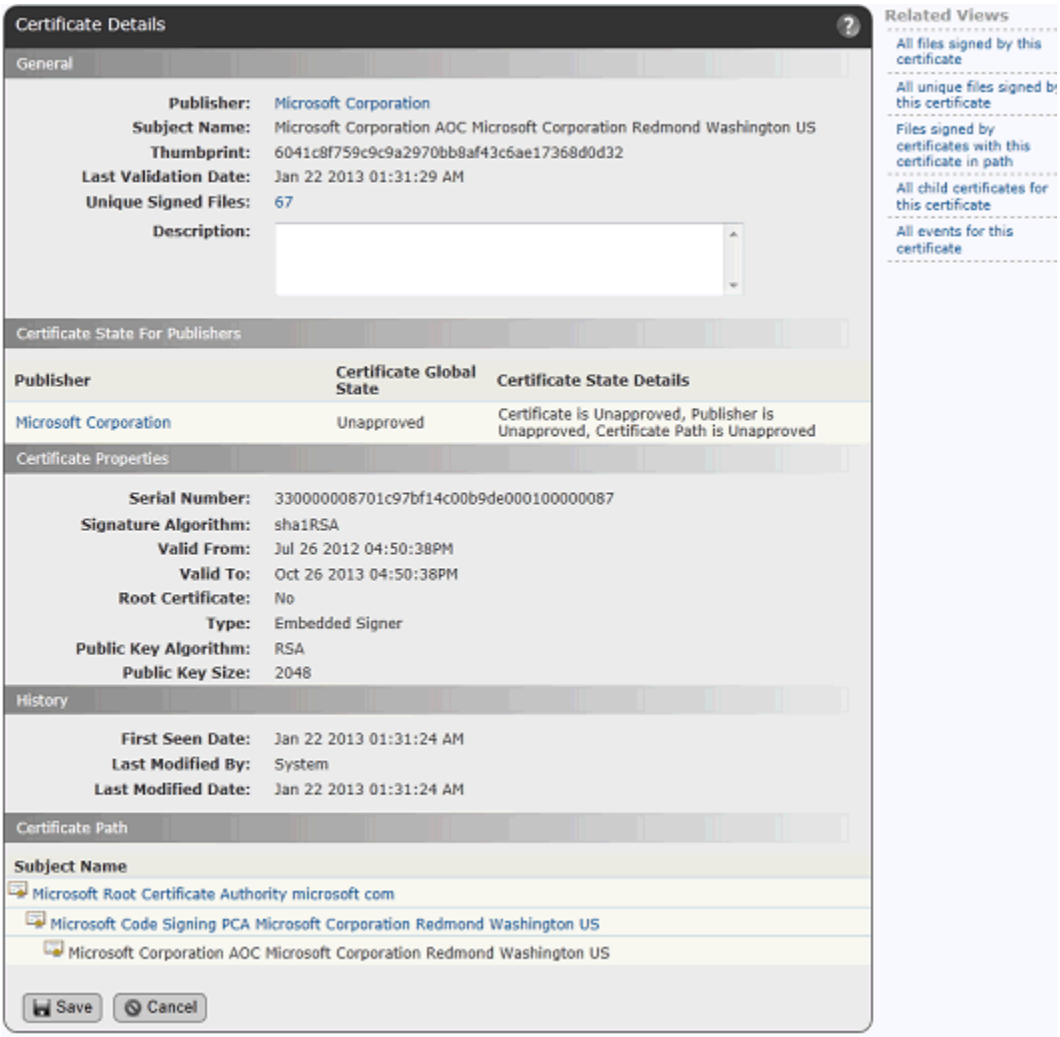
証明書の詳細

[Certificate Details（証明書の詳細）] ページには、1 つの証明書の全詳細が表示されます。また、その証明書に関係する関連ビューへのリンクもあります。表 40 でこのページに表示されるフィールドについて説明します。

1 つの証明書の［Certificates Details（証明書の詳細）］ページを表示する手順：

- ［Certificates（証明書）］テーブルまたは［Publisher Details（公開者の詳細）］ページの証明書セクションで、［View Details（詳細の表示）］ボタンまたは証明書のサブジェクト名をクリックします。

［Events（イベント）］テーブルなど、証明書の情報が表示されるその他の場所で、証明書のサブジェクト名をクリックするとその詳細を確認できます。



［Certificate Details（証明書の詳細）］で発行者名がリンクとしてハイライト表示されている場合、そのリンクをクリックするとこの証明書の公開者の詳細ページに移動できます。［Certificate Path（証明書パス）］パネルでハイライト表示されている証明書名をクリックして、その詳細を表示することもできます。この証明書に署名済みのファイルがある場合、［Unique Signed Files（一意の署名済みファイル）］フィールドの横にある数字をクリックすると、フィルターされた［File Catalog（ファイル カタログ）］ビューが表示され、これらのファイルが表示されます。「中間」および「ルート」証明書の場合、中間およびルート証明書の公開者名はリンクになりません。

［Certificate Details（証明書の詳細）］の［Related Views（関連ビュー）］メニュー

［Certificate Details（証明書の詳細）］メニューには、証明書に関する追加情報と環境内での使用方法を表示できる［Related Views（関連ビュー）］メニューがあります。すべての証明書で［Related Views（関連ビュー）］のすべての選択肢が使用できるわけではありません。ビューオプションを次に示します。

- ［**All files signed by this certificate**（この証明書で署名されたすべてのファイル）］– フィルターされた［Find Files（ファイルの検索）］ページが表示され、この証明書で署名されたすべてのファイル インスタンス（つまり、この証明書が「リーフ」証明書であるファイル）が表示されます。
- ［**All unique files signed by this certificate**（この証明書で署名されたすべての一意のファイル）］– フィルターされた［File Catalog（ファイル カタログ）］ページが表示され、この証明書で署名されたすべての一意のファイルが表示されます。
- ［**Files signed by certificates with this certificate in path**（証明書で署名され、パス内にこの証明書があるファイル）］– フィルターされた［Find Files（ファイルの検索）］ページが表示され、証明書パス内にこの証明書があるファイル インスタンスが表示されます。
- ［**All child certificates for this certificate**（この証明書のすべての子証明書）］– フィルターされた［Certificates（証明書）］ページが表示され、この証明書より下のレベルの子証明書が表示されます。
- ［**All events for this certificate**（この証明書のすべてのイベント）］– フィルターされた［Events（イベント）］ページが表示され、この証明書に関連するイベントが表示されます。イベントには、禁止と承認の作成または削除、証明書の検出または追加、および証明書の検査が含まれます。

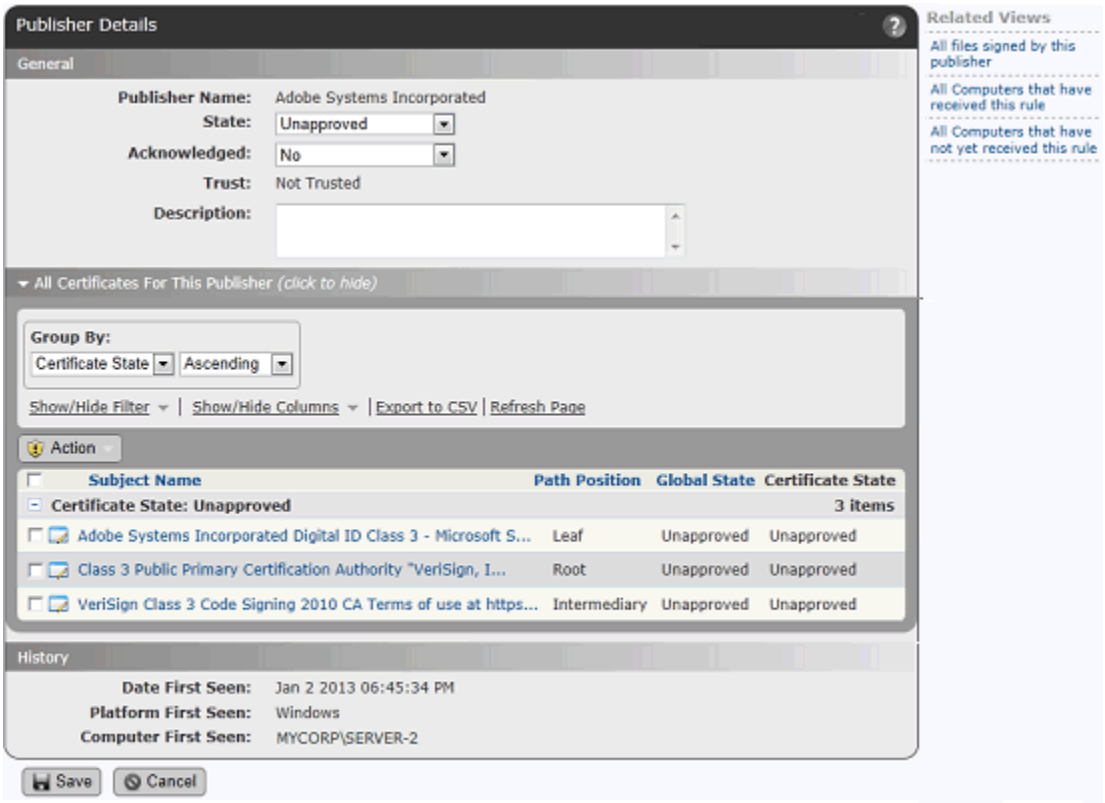
公開者の証明書の表示

［Publisher Details（公開者の詳細）］ページには、［All Certificates for This Publisher（この公開者のすべての証明書）］パネルがあります。このパネルは長くなる可能性があるため、パネル名をクリックすることでページ上で縮小および展開できるようになっています。

［Publisher Details（公開者の詳細）］ページで証明書を表示する手順：

1. ハイライト表示されている公開者名をクリックします。

   注意：イベント、ファイルの詳細、証明書の詳細など、公開者名はさまざまな場所に表示されます。公開者名がハイライト表示されていない場合、その公開者はファイルに直接署名するソフトウェア公開者ではなく、ファイル署名用の証明書に署名する認証局である可能性があります。
2. 公開者の証明書が表示されない場合、［**All Certificates for This Publisher**（この公開者のすべての証明書）］をクリックします。



このパネルには、この公開者のすべてのリーフ証明書と、このリーフ証明書に関連付けられているすべてのルートおよび中間証明書が表示されます。パネルは［Certificates（証明書）］テーブルに似ており、テーブル用の標準のフィルター、列、およびグループ化ツールを使用して変更できます。表示されている証明書については、［View Details（詳細の表示）］ボタンまたはサブジェクト名をクリックすることで、その詳細ページに移動できます。

［Publisher Details（公開者の詳細）］ページの証明書のテーブルには、［Action（アクション）］メニューがあります。このメニューを使用して、現在の公開者に対して証明書の禁止、承認、承認または禁止の削除を実行できます。詳細については、「公開者の証明書の承認または禁止」（372 ページ）で説明します。

ファイルとファイル インスタンスの詳細の証明書フィールド

コンソールの［File Catalog（ファイル カタログ）］、［Files on Computers（コンピューター上のファイル）］、および［File Instance Details（ファイル インスタンスの詳細）］ページには、証明書関連のフィールドがあります。ほとんどの場合、証明書名やハッシュは、ファイル情報から、そのファイルに署名した証明書に関する詳細情報へのリンクになっています。証明書情報は、これらすべてのページの［Global State Details（グローバル状態の詳細）］にも含まれています。詳細については、第 7 章「ファイル情報と公開者情報」を参照してください。

表 41 には、ファイル ページに表示される証明書関連のフィールドを示します。

表 41：ファイル テーブルと詳細ページの証明書関連のフィールド

フィールド	File Catalog（ファイル カタログ）	Files on Computers（コンピューター上のファイル）	File Details（ファイルの詳細）	File Instance Details（ファイル インスタンスの詳細）
Certificate（証明書）			リンク	X
Certificate Type（証明書の種類）			X	X
Certificate Global State（証明書のグローバル状態）	X	X	X	X
Certificate Hash（証明書ハッシュ）	リンク			
Certificate State（証明書の状態の理由）	X	X		
Certificate Subject Name（証明書のサブジェクト名）	X	X		
Detached Certificate Subject Name（デタッチされた証明書のサブジェクト名）（詳細ページでは、Detached Certificate（デタッチされた証明書））		X		リンク
Detached Certificate Type（デタッチされた証明書の種類）				X
Detached Certificate State（デタッチされた証明書の状態）				X

証明書のアラート

証明書関連のアラートは 2 つあります。証明書をセキュリティ実施計画の一環として利用している場合、これらが特に役立つ場合があります。

- [**New Certificate Alert**（新しい証明書アラート）] – Bit9 コンソールにまだリストされていない公開者の証明書を含むファイルが検出されるか、Bit9 Server に新しい証明書が直接インポートされたときに、サブスクライバーにアラートを送信します。デフォルトでは、このアラートはすべての公開者の新しい証明書が検出されたときにトリガーされます。ただし、特定の公開者の新しい証明書に対してのみトリガーするように設定できます。
- [**Revoked Certificate Alert**（証明書取り消しアラート）] – この Bit9 Server で認識されている証明書が取り消されたときに、サブスクライバーにアラートを送信します。デフォルトでは、このアラートはいずれかの公開者の証明書が取り消されたときにトリガーされます。ただし、特定の公開者の証明書に対してのみトリガーするように設定できます。

証明書の検出や取り消しに関する情報をユーザーに知らせる特別なメール テンプレートがあります。

アラートの構成、有効化、およびアラートへの対応の詳細については、「Bit9 アラートの使用」（606 ページ）を参照してください。

証明書のイベント

Bit9 ではファイル署名証明書に関連するイベントがレポートされます。イベントはコンソールの［Events（イベント）］ページに表示され、Syslog 出力でも利用できます。証明書関連のイベントの説明には、サブジェクト名が含まれています。コンソールの［Events（イベント）］ページ上のサブジェクト名は、［Certificate Details（証明書の詳細）］ページへのリンクになっています。

証明書のイベント サブタイプ（イベントの一意の Bit9 識別子）の詳細については、別途提供されている『Bit9 Events Integration Guide（Bit9 イベント統合ガイド）』を参照してください。サブタイプは次の 2 種類があります。

- **検出イベント** – Bit9 での証明書の状態とは無関係の、証明書自体と関係のあるイベントです。
- **ポリシー適用イベント** – Bit9 での証明書の禁止または承認の追加または削除をレポートするイベントです。

Bit9 コンソールでのイベントの表示に関する詳細については、「イベント レポート」（590 ページ）を参照してください。別のドキュメントを参照してください。

外部ビューでの証明書

Bit9 では、コンソールの代替手段として、ファイルとイベントのデータベースのパブリック ビューを使用できます。これらのパブリック ビューを使用することにより、独自のレポート作成ソリューションやデータ分析ソリューションを作成することが可能になります。前のセクションで説明した証明書関連のイベント サブタイプは、ExEvents ビューに含めることが可能です。加えて、証明書のメタデータがファイルの情報とともに以下のビューに含まれます。

- **ExFileCatalog** – すべての一意のハッシュのメタデータ
- **ExFileInstances** – すべてのコンピューター上の全ファイル インスタンスのメタデータ
- **ExDeletedFileInstances** – すべての削除されたファイル インスタンスのメタデータ

Bit9 データベースの外部ビューへのアクセス方法の詳細については、付録 A、「ライブ インベントリ SDK：データベース ビュー」を参照してください。

適用のための証明書の使用

この章の前のセクションでは、Bit9 が証明書について提供する情報について主に扱いました。このセクションでは、証明書の承認と禁止、およびファイル状態に対するその影響について説明します。証明書の承認と禁止機能の概要を以下に示します。

- **証明書の承認設定** – [System Configuration（システム構成）] ページには、特定の証明書をグローバルに承認できるかどうかを決定する [Advanced Options（高度なオプション）] があります。
- **管理可能な証明書の種類** – 選択した構成にかかわらず、検出されたすべての証明書を承認または禁止できるわけではありません。
- **パスの位置とエージェントの差異** – 証明書や公開者の組み合わせが同じでも、各エージェントで証明書パスが異なる場合があります。また、サーバーのパスが、エージェントの現在のパスと部分的にだけ一致している場合や、まったく一致していない場合があります。
- **証明書の状態** – 証明書を承認または禁止（または承認と禁止を削除）することで、特定の公開者の、特定の証明書の状態が決まります。
- **証明書のグローバル状態** – その他の要因が証明書の状態と影響し合って、証明書の有効な状態である証明書のグローバル状態が決まります。
- **ファイルの状態への影響** – 証明書のグローバル状態がその他のルールおよび状態と影響し合って、特定の証明書またはその子証明書の 1 つで署名されたファイルの状態が決まります。
- **証明書の禁止設定** – 各コンピューターのポリシーには、証明書の禁止を有効にするかどうかを決定する高度な設定があります。

証明書の承認や禁止を準備する際に重要なことは、「状態を有効にする公開者ごとに」状態を指定する必要があるという点です。

証明書の承認構成の選択項目

ファイルの承認を有効にするには、そのファイルの証明書チェーンにあるのすべての証明書が Windows によって有効であると見なされる必要があります。たとえば、証明書を受け入れるには、現在のルート証明書をインストールする必要があります。

加えて、[System Configuration（システム構成）] ページの [Advanced（詳細）] タブには、証明書で署名されたファイルの状態を決定する際にその証明書の承認を有効にするかどうかを決定する構成設定があります。この構成オプションの詳細については、「ファイルを承認できる証明書の確認」（295 ページ）を参照してください。

証明書は、証明書自体を承認および禁止できるほか、名前で公開者を承認または禁止するために使用することもできます。[Advanced Options（高度なオプション）] ページの [Certificate Options（証明書オプション）] を設定または表示するときは、以下のことに注意してください。

- これらの設定の要件を満たしていない証明書を承認できます。その場合、証明書自体の [Certificate State（証明書の状態）] には [Approved（承認）] と表示されます。ただし、そのような証明書のグローバル状態（有効な状態）を承認にすることはできません。
- [Certificate Options（証明書オプション）] の選択項目は、副署者証明書には影響しません。
- [Certificate Options（証明書オプション）] の選択項目では、証明書の禁止を防ぐことも、[Certificate Global State（証明書のグローバル状態）] の値が [Banned（禁止）] にならないようにすることもできません。詳細については、「証明書のグローバル状態」（374 ページ）を参照してください。

- ［System Configuration（システム構成）］ページの［Advanced Options（高度なオプション）］タブの［Expired Certificates（期限切れの証明書）］オプションは、「証明書」をグローバルに承認する機能には影響しません。このオプションは、「公開者」によるファイルの承認に期限切れの証明書を使用できるかどうかを決定するものです。ボックスをオンにすると、期限が切れているものの有効期間中にはファイルの署名に使用されていた証明書がファイルにある場合、その証明書を公開者による承認に使用できます。オフにすると、期限切れの証明書を公開者によるファイルの承認に使用できません。この設定は、証明書のグローバル状態には影響しません。

証明書の種類

［Certificate Details（証明書の詳細）］ページには、［Certificate Type（証明書の種類）］フィールドがあります。このフィールドにはリーフ証明書の場合にだけ値が表示されます。証明書の種類は、そのリーフ証明書の用途と、ファイルにどのように関連付けられているかを示します。次の語句の組み合わせが表示されます。

- ［**Embedded**（埋め込み）］– ファイルのデジタル署名が、ファイル自体の実行可能でない部分に埋め込まれています。
- ［**Detached**（デタッチ）］– 署名対象のファイルがダイジェストにハッシュされています。また、デジタル署名がダイジェストに適用され、複数のファイル用の証明書を含めることができる別のカタログ ファイルに収められています。
- ［**Signer**（署名者）］– 証明書は、その証明書が署名するファイルのコード署名証明書です。
- ［**Cosigner**（副署者）］– 証明書は、その証明書が署名するファイルの副署者（または「連署者」）証明書です。副署者証明書は通常、タイム スタンプに使用されます。

リーフ証明書の各インスタンスは、埋め込みとデタッチのどちらかである必要があり、また署名者と副署者のどちらかである必要があります。そのため、どの証明書でも、［Type（種類）］のフィールド内のディスクリプターは少なくとも 2 つあります。同じ証明書は異なる方法で使用できるので、複数の種類を持つことが可能です。したがってディスクリプターが 3 つ以上になる場合もあります。［Certificates（証明書）］テーブル内の 1 つの証明書の［Type（種類）］には、たとえば［Embedded Detached Signer（埋め込み デタッチ 署名者）］や上記の語句の別の組み合わせが表示されます。

重要

承認または禁止できるのは、あるファイルの署名者として特定および使用されている証明書だけです。副署者証明書の状態が Bit9 によって指定されることはありません。

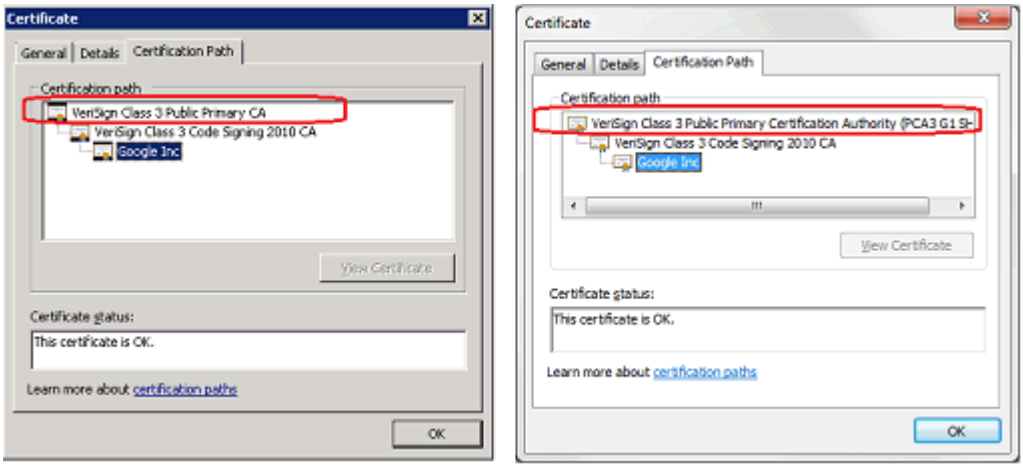
パスの位置とエージェントの差異

［Publisher Details（公開者の詳細）］ページを表示すると、［All Certificates for This Publisher（この公開者のすべての証明書）］パネルにパス内のすべての証明書が表示されます。これらの証明書は、承認または禁止することが可能です。ただしそ

れを実行する前に、パス上のさまざまなポイントで承認または禁止することにより生じる各種の影響を考慮してください。

同じリーフ証明書の証明書パスが、エージェント間や、エージェントとサーバー間で異なる場合があります。異なる供給元から同じファイルを受け取った場合や、1 つのコンピューターのアップデーターが有効でも別のコンピューターでは無効な場合にこれは発生します。これらの差異を最小化するよう、時間の経過に伴いエージェントが証明書パスを更新します。

パスの差異がある可能性があるため、中間またはルート証明書の承認や禁止は、期待どおりの結果が得られない場合があります。リーフ証明書（同じ発行者とシリアル ナンバー）が同じでルート証明書が異なる場合の例を以下に示します。



これらのルートの 1 つを承認して、そのリーフ証明書のすべてのインスタンスを処理できたと考えても、すべてのエージェントで目的の結果が得られるとは限りません。証明書パス全体を制御できる、内部で署名した証明書に関しては、パスの差異はそれほど問題ではない場合があります。

証明書パスのばらつきを減らすには、エージェントとサーバー上の証明書ストアを最新の状態に保ちます。また、署名済みファイルの最新バージョンを入手するために、オペレーティング システムのアップデーターとその他の重要なアプリケーション アップデーターの実行が許可されていることを確認します。

公開者の証明書の承認または禁止

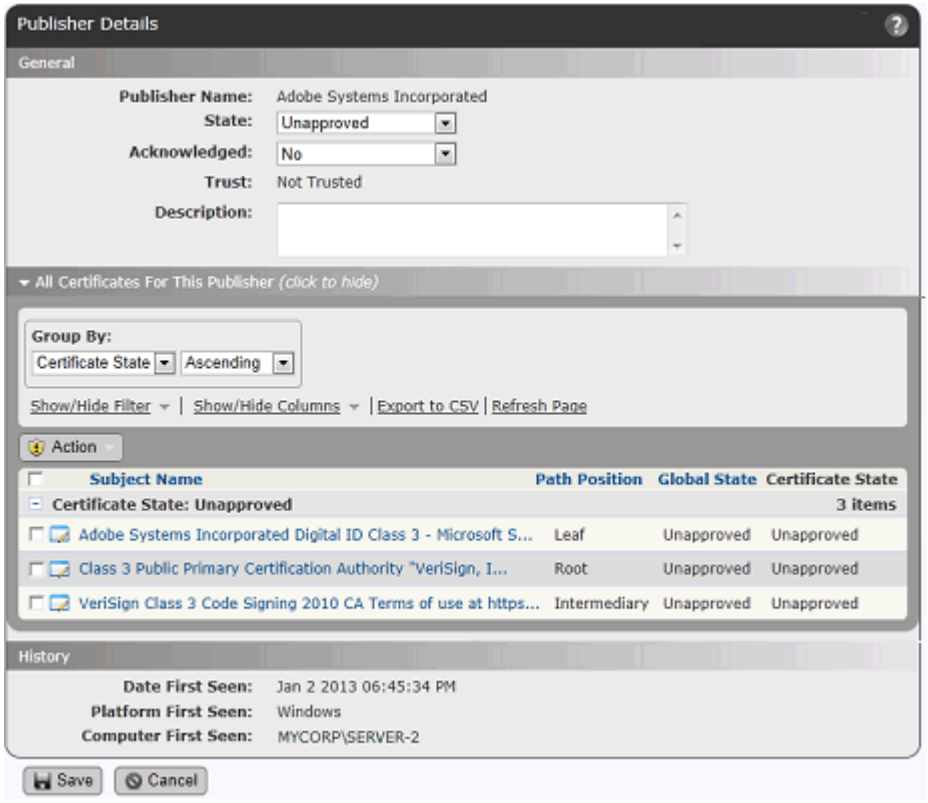
証明書は公開者ごとに承認または禁止します。証明書の状態は、その公開者の中でのみ有効です。証明書が複数の公開者によって使用されている場合、それぞれの公開者について状態を指定する必要があります。

証明書を承認または禁止することにより、証明書の状態が規定されます。状態は［Approved（承認）］、［Banned（禁止）］、［Unapproved（未承認）］のいずれかです。有効な証明書の状態は［Certificate Global State（証明書のグローバル状態）］と呼ばれ、その証明書で署名されたファイルに適用されます。証明書のグローバル状態は、証明書の状態、証明書パス内の他の証明書の状態、公開者の状態、および（承認の場合は）証明書の構成設定の選択によって決まります。各種の証明書のグローバル状態がどのように生成されるのかについては、「証明書のグローバル状態」（374 ページ）を参照してください。

証明書を承認または禁止する手順：

1. ［System Administration（システム管理）］ページの［Advanced Options（高度なオプション）］タブで、適切な［Certificate Options（証明書オプション）］を設定していること確認します。この設定により、承認に使用できる証明書が決定されます。「ファイルを承認できる証明書の確認」（295 ページ）を参照してください。
2. 承認または禁止する証明書を見つけ、承認または禁止を適用する公開者の［Publisher Details（公開者の詳細）］ページを開きます。

   注意：最初に証明書を見つけてからその公開者名をクリックすることができます（［File Details（ファイルの詳細）］ページ、［Events（イベント）］ページ、［Certificates（証明書）］テーブルなど）。または、証明書の公開者を知っている場合、その詳細ページを直接開きます。
3. 公開者の証明書がまだ表示されていない場合、［**All Certificates for This Publisher**（この公開者のすべての証明書）］をクリックします。



4. ［All Certificates for this Publisher（この公開者のすべての証明書）］パネルで、承認または禁止する証明書の横にあるボックスをオンにします。オンにしたすべての証明書には、同じ状態を適用する必要があります。つまり同時に一部の証明書を承認しつつ別の証明書を禁止にすることはできません。
5. ［Action（アクション）］メニューで、［**Approve Certificates**（証明書を承認）］または［**Ban Certificates**（証明書を禁止）］を選択します。オンにした証明書の証明書の状態が、選択した状態に変わります。

承認、未承認、または禁止の証明書の状態が、他の状態およびルールとどのように影響し合って証明書のグローバル状態が決定されるかについては、「証明書のグローバル状態」（374 ページ）を参照してください。

証明書の承認または禁止を削除する手順：

1. ［Publisher Details（公開者の詳細）］ページで、状態を変更する証明書のボックスをオンにします。この操作では、禁止されている証明書と承認されている証明書を組み合わせて選択できます。
2. ［Action（アクション）］メニューで、［**Remove Approval or Ban**（承認または禁止を削除）］を選択します。オンにした証明書の証明書の状態が、すべて未承認に変わります。

証明書のグローバル状態

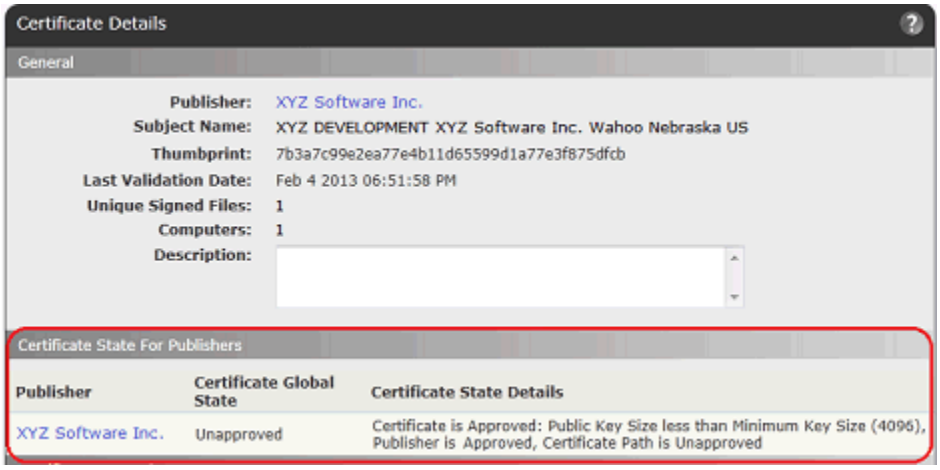
証明書のグローバル状態は証明書の有効な状態です。証明書のグローバル状態は次のいずれかの値になります。

- Unapproved（未承認）
- Approved（承認）
- Banned（禁止）
- Approved By Policy（ポリシーにより承認）
- Banned By Policy（ポリシーにより禁止）
- Mixed（混在）

証明書のグローバル状態は以下の要因で決まります。

- **証明書の状態** – 値は［Unapproved（未承認）］、［Approved（承認）］、［Banned（禁止）］のいずれかです。
- **公開者の状態** – 値は［Unapproved（未承認）］、［Approved（承認）］、［Banned（禁止）］、［Approved By Policy（ポリシーにより承認）］、［Banned By Policy（ポリシーにより禁止）］のいずれかです。
- **証明書パスの状態** – 値は［Unapproved（未承認）］、［Approved（承認）］、［Banned（禁止）］、［Mixed（混在）］（チェーン内に承認されている証明書と禁止されている証明書がある場合）のいずれかです。
- **証明書のキーの長さとアルゴリズム** – この証明書が［System Configuration（システム構成）］ページの［Advanced Settings（高度な設定）］の要件を満たしているかどうか。

どの証明書についても、［Certificates（証明書）］（テーブル）ページまたは［Certificate Details（証明書の詳細）］ページで、［Certificate Global State（証明書のグローバル状態）］に影響している要因を確認できます。この詳細ページの［Certificate State for Publishers（公開者の証明書の状態）］パネルに、関係する要因がまとめられています。



上記の例では、[Certificate Global State（証明書のグローバル状態）] は [Unapproved（未承認）] になっています。[Certificate Global State（証明書の状態の詳細）] を見ると、証明書自体の状態は [Approved（承認）] ですが、その公開鍵のサイズが [System Configuration（システム構成）] ページの [Advanced Options（高度なオプション）] ページで指定されている最小長に満たないため、グローバル状態は承認になっていません。証明書が複数の設定の要件（最小キー サイズと許可されているアルゴリズムの仕様など）を満たしていない場合、2 つの原因のうちの 1 つだけが [Certificate State Details（証明書の状態の詳細）] に表示されます。

以下の例は、これらの値がお互いにどのように影響し合って証明書のグローバル状態が決定されるかを把握するうえで役立ちます。可能なすべての組み合わせを表 42、「証明書のグローバル状態の決定」（377 ページ）に示します。

例 1：すべての状態と構成で承認が許可されている場合

条件	例またはコメント
証明書が最小キー サイズ構成を満たしている	証明書の最小キー サイズ：1024 この証明書のキーの長さ：2048
その証明書のアルゴリズムのタイプを無視するよう構成されていない	無視する証明書の署名アルゴリズム：MD2RSA だけがオン この証明書の署名アルゴリズム：SHA1RSA
証明書に連署がある（必要な場合）	
構成した失効検査で、証明書が失効の対象として検出されなかった …	
リーフ証明書の状態が承認である	コンソール ユーザーが証明書を承認しました。
公開者の状態が承認である	公開者はコンソール ユーザーまたはレピュテーションにより承認されました。
この証明書のパス内の他の証明書が 1 つも禁止されていない	証明書パスの状態は [Certificate Details（証明書の詳細）] に表示されます。
以上の条件に該当する場合、証明書のグローバル状態は承認になります。	この状態が、証明書で署名されるファイルに影響する状態です。

例 2：証明書が構成の要件を満たしていない場合

条件	例またはコメント
証明書が最小キー サイズ構成を満たしている	証明書の最小キー サイズ：1024 この証明書のキーの長さ：2048
その証明書のアルゴリズムのタイプを無視するよう構成されている	無視する証明書の署名アルゴリズム：MD2RSA と SHA1RSA がオン この証明書の署名アルゴリズム：SHA1RSA
証明書の状態が承認である	
公開者の状態が承認である	
この証明書のパス内の他の証明書が 1 つも禁止されていない	
以上の条件に該当する場合、証明書のグローバル状態は未承認になります。	承認のための他のすべての条件は満たされていますが、証明書アルゴリズムだけは承認のために許可されていません。

例 3：パス内に禁止されている証明書がある場合

条件	例またはコメント
証明書が最小キー サイズを満たしている、または満たしていない	
証明書が他の高度なオプションの要件を満たしている、または満たしていない	
公開者の状態が承認または未承認であり、ポリシー制限がない	
この証明書またはパス内のいずれかの証明書が禁止されている	
以上の条件に該当する場合、証明書のグローバル状態は禁止になります。	証明書のグローバル状態は禁止ですが、各エージェントに対する禁止の有効性は、エージェントのポリシーの［Advanced Settings（高度な設定）］の［Block files with banned publishers or certificates（公開者または証明書が禁止されているファイルをブロック）］によって決まります。この設定は、デフォルトでアクティブになっています。

例 4：グローバル状態が混在になる場合

条件	例またはコメント
公開者の状態がポリシーにより承認である	
この証明書またはパス内のいずれかの証明書が禁止されている	

以上の条件に該当する場合、証明書のグローバル状態は混在になります。	公開者が承認されるポリシーでは、証明書のグローバル状態は未承認になります。 公開者の承認に含まれていないポリシーでは、証明書ごとの禁止がポリシーで許可されている場合、証明書のグローバル状態は禁止になります。

表 42 には、証明書、発行者、証明書パスの状態のさまざまな組み合わせにより、証明書のグローバル状態がどのように決定されるかを示します。これらの結果はすべて、パス内のすべての証明書が、[System Configuration（システム構成）] の [Advanced Options（高度なオプション）] ページで指定されている設定の要件を満たしていることを前提としています。「(ポリシーにより)」のように表中で括弧が表示されている箇所については、証明書の状態は、表示上、ポリシーによるものとは「明示」されませんが、公開者の状態がポリシーにより承認またはポリシーにより禁止であるため、「実質上」は「ポリシーにより」決定されています。

表 42：証明書のグローバル状態の決定

#	証明書の状態	公開者の状態	証明書パスの状態	証明書のグローバル状態
1	未承認	未承認	未承認	未承認
2	承認	未承認	未承認	承認
3	禁止	未承認	未承認	禁止
4	未承認	承認	未承認	承認
5	承認	承認	未承認	承認
6	禁止	承認	未承認	禁止
7	未承認	禁止	未承認	禁止
8	承認	禁止	未承認	禁止
9	禁止	禁止	未承認	禁止
10	未承認	ポリシーにより承認	未承認	ポリシーにより承認
11	(ポリシーにより) 承認	ポリシーにより承認	未承認	ポリシーにより承認
12	(ポリシーにより) 禁止	ポリシーにより承認	未承認	混在
13	未承認	ポリシーにより禁止	未承認	ポリシーにより禁止
14	(ポリシーにより) 承認	ポリシーにより禁止	未承認	混在
15	(ポリシーにより) 禁止	ポリシーにより禁止	未承認	ポリシーにより禁止

#	証明書の状態	公開者の状態	証明書パスの状態	証明書のグローバル状態
16	未承認	未承認	承認	承認
17	承認	未承認	承認	承認
18	禁止	未承認	承認	禁止
19	未承認	承認	承認	承認
20	承認	承認	承認	承認
21	禁止	承認	承認	禁止
22	未承認	禁止	承認	禁止
23	承認	禁止	承認	禁止
24	禁止	禁止	承認	禁止
25	未承認	ポリシーにより承認	（ポリシーにより）承認	ポリシーにより承認
26	承認	ポリシーにより承認	（ポリシーにより）承認	ポリシーにより承認
27	（ポリシーにより）禁止	ポリシーにより承認	（ポリシーにより）承認	混在
28	未承認	ポリシーにより禁止	（ポリシーにより）承認	混在
29	（ポリシーにより）承認	ポリシーにより禁止	（ポリシーにより）承認	混在
30	（ポリシーにより）禁止	ポリシーにより禁止	（ポリシーにより）承認	混在
31	未承認	未承認	禁止	禁止
32	承認	未承認	禁止	禁止
33	禁止	未承認	禁止	禁止
34	未承認	承認	禁止	禁止
35	承認	承認	禁止	禁止
36	禁止	承認	禁止	禁止
37	未承認	禁止	禁止	禁止
38	承認	禁止	禁止	禁止
39	禁止	禁止	禁止	禁止
40	未承認	ポリシーにより承認	（ポリシーにより）禁止	混在
41	（ポリシーにより）承認	ポリシーにより承認	（ポリシーにより）禁止	混在
42	（ポリシーにより）禁止	ポリシーにより承認	（ポリシーにより）禁止	混在

#	証明書の状態	公開者の状態	証明書パスの状態	証明書のグローバル状態
43	未承認	ポリシーにより禁止	（ポリシーにより）禁止	ポリシーにより禁止
44	（ポリシーにより）承認	ポリシーにより禁止	（ポリシーにより）禁止	混在
45	（ポリシーにより）禁止	ポリシーにより禁止	（ポリシーにより）禁止	ポリシーにより禁止
46	未承認	未承認	混在 *	禁止
47	承認	未承認	混在 *	禁止
48	禁止	未承認	混在 *	禁止
49	未承認	承認	混在 *	禁止
50	承認	承認	混在 *	禁止
51	禁止	承認	混在 *	禁止
52	未承認	禁止	混在 *	禁止
53	承認	禁止	混在 *	禁止
54	禁止	禁止	混在 *	禁止
55	未承認	ポリシーにより承認	（ポリシーにより）混在 *	混在
56	（ポリシーにより）承認	ポリシーにより承認	（ポリシーにより）混在 *	混在
57	（ポリシーにより）禁止	ポリシーにより承認	（ポリシーにより）混在 *	混在
58	未承認	ポリシーにより禁止	（ポリシーにより）混在 *	混在
59	（ポリシーにより）承認	ポリシーにより禁止	（ポリシーにより）混在 *	混在
60	（ポリシーにより）禁止	ポリシーにより禁止	（ポリシーにより）混在 *	混在

混在の状態と「ポリシーにより」が付く状態

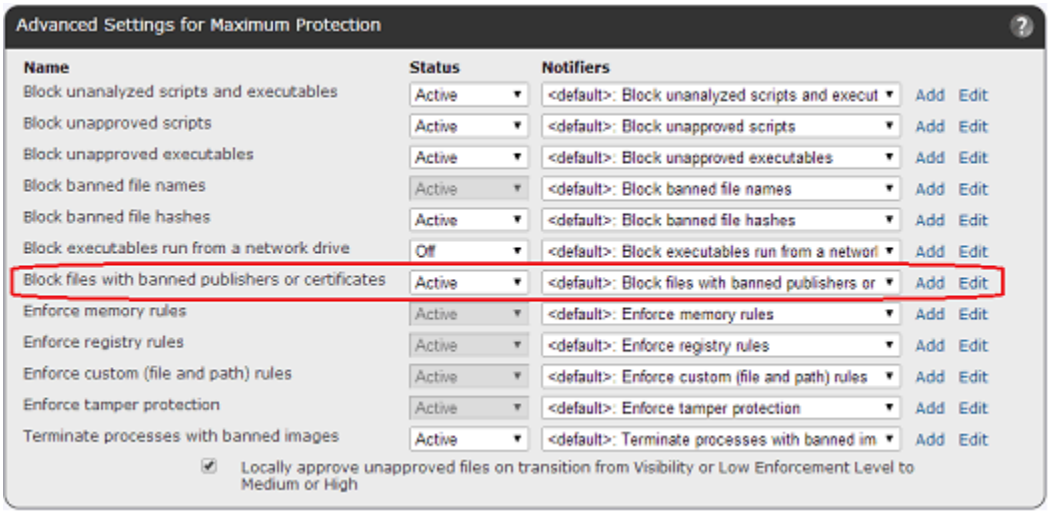
表 42 に示されているとおり、証明書のグローバル状態は、混在、ポリシーにより承認、またはポリシーにより禁止という状態になる場合があります。表には各ケースが示されていますが、以下の一般的なルールに注意してください。

- **混在のパスの状態** – 承認されている証明書と禁止されている証明書がある場合、証明書のパスの状態は混在と見なされます。ただし、混在のパスの状態は、情報の提供のみを目的としたものです。証明書のグローバル状態への影響という意味では、混在状態のパスは禁止状態のパスと同じです。
- **「ポリシーにより」が付く公開者の状態** – 公開者の状態がポリシーにより禁止またはポリシーにより承認である場合、パス内の証明書に対する禁止または

承認は、公開者のポリシーの選択によってフィルターされます。たとえば、証明書の状態が禁止であり、その公開者の状態がポリシーにより承認である場合、証明書のグローバル状態は混在になります。

ポリシーでの証明書の禁止設定

各ポリシーの［Advanced Settings（高度な設定）］パネルには、［Block files with banned publishers or certificates（公開者または証明書が禁止されているファイルをブロック）］設定があります。証明書の禁止をファイルのブロックに反映させるには、この設定を［Active（アクティブ）］（デフォルト）にする必要があります。証明書の設定は、高、中、および低の適用レベルのポリシーでのみ有効です。また、この設定は証明書の禁止の「適用」にのみ影響します。証明書に対して禁止を指定できるかどうかには影響しません。ここでの選択で、証明書が「承認」されないようにしたり、ファイルに対する承認の有効化を防いだりすることもできません。



他のルールとの相互影響

証明書のグローバル状態は、他のルールおよび状態と影響し合いながら、ファイルの状態に関係します。証明書のグローバル状態に影響する構成ルールは、「証明書のグローバル状態」（374 ページ）で説明しました。関係する可能性のある他のルールを以下に示します。

- **適用レベル** – 証明書のグローバル状態が禁止の場合、高、中、および低の適用レベルでファイルを実行できるかどうかに影響することがあります。証明書のグローバル状態が承認の場合、高および中の適用レベルでのファイルの実行に影響することがあります。
- **レピュテーション ルール** – レピュテーション ルールは公開者の状態に影響することがあります。それにより、証明書のグローバル状態に影響することがあります。個々の証明書に状態を指定し終わってから、レピュテーション ルールを有効または変更する場合は、このことに注意してください。詳細については、第 9 章「レピュテーション承認ルール」を参照してください。

証明書のグローバル状態がファイルのグローバル状態に及ぼす影響

ファイルのグローバル状態は、ファイルの状態、公開者の状態、および証明書のグローバル状態の組み合わせで決定されます。パス内のすべての証明書が未承認の場合、証明書はファイルのグローバル状態に影響しません。証明書のグローバル状態が未承認以外の場合、その証明書はファイルのグローバル状態の決定に影響することがあります。最も簡単な例を 2 つ示します。

- 「ポリシーにより」が付く状態の設定がなく、ファイルの状態、公開者の状態、または証明書のグローバル状態が禁止の場合、ファイルのグローバル状態は禁止になります。
- 「ポリシーにより」が付く状態の設定がなく、かつ証明書のグローバル状態に影響を与える 3 つの要素がいずれも禁止ではなく、少なくとも 1 つが承認の場合、ファイルのグローバル状態は承認になります。

エージェントのバージョンとファイルのグローバル状態

v7.0.1 Patch 3 以降のエージェント（v7.2 のすべてのエージェントを含む）では、ファイルのグローバル状態は実質上、証明書のグローバル状態とファイルの状態の組み合わせで決定されます。公開者の状態は、証明書のグローバル状態の計算で既に考慮されているためです。

v7.0.1 Patch 3 より前のエージェントでは、ファイルのグローバル状態は公開者の状態とファイルの状態の組み合わせで決定されます。証明書のグローバル状態は、ファイルのグローバル状態の決定には影響しません。

ファイルのグローバル状態の決定方法の詳細については、第 7 章「ファイル情報と公開者情報」を参照してください。

第 11 章

デバイスの管理

この章では、Bit9 エージェントを実行中のコンピューター上で検出されたストレージ デバイスを追跡および制御するための機能について説明します。

セクション

概要

Bit9 Security Platform では、エージェントで管理する Windows コンピューターの固定およびリムーバブル ストレージ デバイスを追跡できます。また、これらのリムーバブル デバイスでユーザーが実行できるファイル操作を制御することもできます。Bit9 のデバイス管理は以下の要素で構成されています。

- **ポリシー別のデバイス制御設定**では、Bit9 のルールによりポリシー内のコンピューターに接続されているデバイスに対する書き込みおよび操作の実行を制御するかどうかを決定します。また、この制御を未承認のデバイス、禁止されているデバイス、その両方のいずれに適用するかを決定します。
- **デバイス固有のルール**では、「モデル」と「個々のデバイス」のどちらかで特定のリムーバブル デバイスを明示的に承認または禁止して、承認されたデバイスでファイルへの書き込みまたはファイルの実行を許可するとともに、ポリシー設定により禁止または未承認のデバイスを制限することができます。これらの承認および禁止ルールの動作は、Bit9 Platform でのファイルの承認および禁止の動作に似ています。
- **デバイス インベントリ**テーブルでは、Bit9 エージェントによって検出された各デバイスが表示され、デバイス固有のルールを実装できます。このインベントリには、デバイス モデルのリスト、個々のデバイスのリスト、個々のデバイスと個々のコンピューターの一意の「接続」のリストが含まれています。これらのリスト内のインスタンスはいずれもドリルダウンすることができます。

この章では「個々のデバイス」という用語は、同時に 1 つのコンピューターにのみ接続できる 1 つの具体的なデバイスを指します。一般的に、これは特定のモデルと一意（少なくともそのモデルで一意）のシリアル ナンバーで表されます。

プラットフォームに関する注意

リリース 7.2.3 では、デバイスの可視性および制御機能は「Windows」を実行しているコンピューターでのみ使用できます。デバイス管理は、現在 Mac または Linux コンピューターでは使用できません。

Bit9 によって管理されるデバイス

Bit9 エージェントは、Windows コンピューター上のさまざまな種類のデバイスを検出できます。通常、デバイスが識別可能なファイル システムを持っている場合、［Devices（デバイス）］テーブルに追加されます。検出されたデバイスの管理方法は、固定デバイスとして認識された場合とリムーバブル デバイスとして認識された場合とで異なります。

- **固定デバイス**は、デバイス インベントリに含まれますが、Bit9 ルールで承認、禁止、ブロックすることはできません。
- **リムーバブル デバイス**は、デバイス インベントリに含まれ、Bit9 ルールで承認、禁止、ブロックすることができます。

Bit9 は、デバイスが固定かリムーバブルかを判断するために、デバイスから提供される情報を利用する必要がありますが、その情報が誤っている場合があることに注意してください。

Bit9 エージェントによって検出されるデバイスの具体的なカテゴリを以下に示します。

- IDE デバイス
- SATA デバイス
- SCSI デバイス
- USB デバイス
- FireWire (IEEE 1394) デバイス
- シリアル バス プロトコル 2 デバイス
- フロッピー ディスク ドライブ

検出される USB デバイスには、「スティック」タイプのソリッドステート ドライブ、CD/DVD ドライブ、メディア カード リーダーが含まれます。リムーバブル メディアを扱うドライブの場合、ドライブが読み取るメディアではなく、ドライブ自体がデバイス テーブルに表示されることに注意してください。

注意

ここで説明するデバイス設定とルールに加えて、デバイスでできることとできないことを制御するカスタム パス ルールを作成できます。詳細については、第 12 章「カスタム ソフトウェア ルール」「Windows ルールのパスでのデバイスの指定」（422 ページ）を参照してください。

ポリシー単位のデバイス制御の有効化

Bit9 Platform のデバイス制御機能を有効にするには、ポリシーのデバイス制御設定をアクティブ化する必要があります。ポリシーごとに、独自のデバイス制御設定を指定できます。この設定により、以下を任意に組み合わせたブロック機能をアクティブ化することが可能です。

- 禁止されているデバイスや未承認のデバイス
- 書き込みや実行操作

デバイスでの読み取り操作をブロックすることはできませんが、レポート機能を有効にして、禁止または未承認のデバイスでファイルが読み取られたときにイベントを生成することができます。

［Edit Policy（ポリシーの編集）］ページで、既に作成されているポリシーに対してデバイス制御を有効にします。デバイス制御設定は、新しいポリシーを作成するために使用する［Add Policy（ポリシーの追加）］ページには表示されません。

可視性モードのポリシーについては、どのデバイス制御設定も選択できますが、デバイス操作はブロックされません。デバイスのアクティビティをブロックするには、ポリシーが制御モードである必要があります。

注意

CD/DVD ドライブなど、リムーバブル「メディア」を扱うドライブに対する設定の効果は、リムーバブル メディアを扱わないデバイスに対する効果とは異なります。CD または DVD を焼くことは、「書き込み」操作には含まれません。CD/DVD メディアを焼くことをブロックする場合は、メディア作成ソフトウェア アプリケーションを禁止してください。

表 43 に、デバイス制御設定を具体的に選択した場合の効果を示します。

表 43：デバイス制御設定の動作

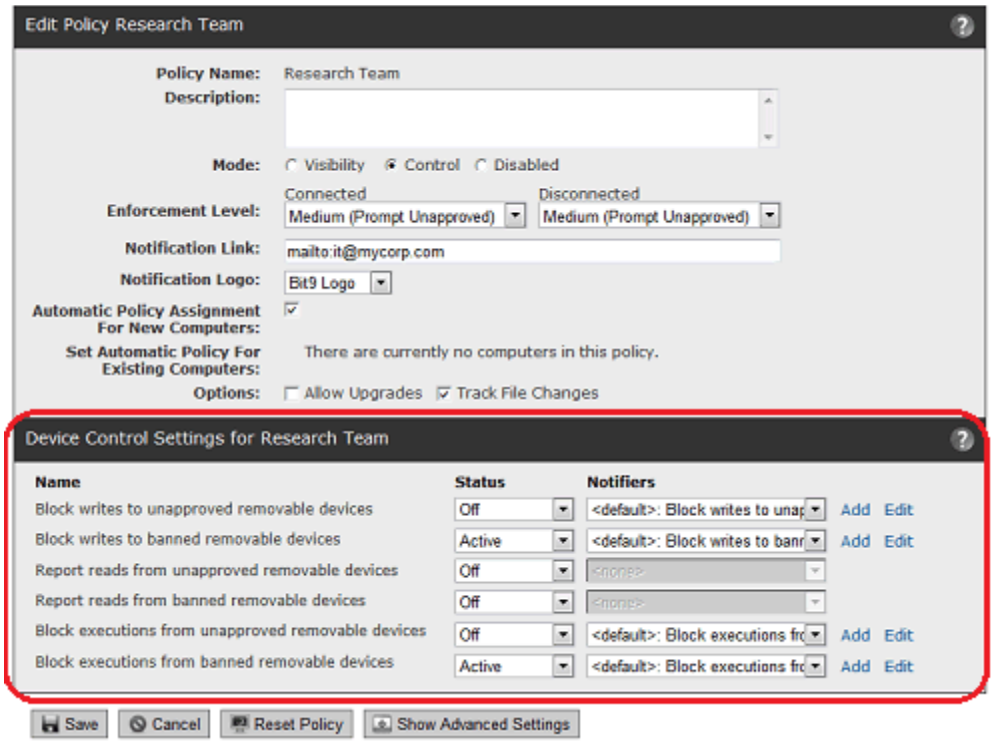
設定	Active（アクティブ）	Off（オフ）	Report Only（レポートのみ）
Block writes to unapproved removable devices（未承認リムーバブル デバイスへの書き込みをブロック）	未承認リムーバブル デバイスへの書き込み操作を追跡し、制御モードのすべてのポリシー（高、中、および低の適用レベル）でこの操作をブロックします。 **注意**： • どのデバイスもデフォルトでは未承認です。そのため、この設定をアクティブ化する前に、明示的に承認していないデバイスをすべてブロックする必要があるのかどうかを確認してください。 • リムーバブル デバイスへの書き込みをブロックしても、CD/DVD メディアへの書き込みはブロックされません。	リムーバブル デバイスへの書き込み操作を許可します。イベントはレポートされません。	書き込み操作を許可し、操作をイベントとしてレポートします。
Block writes to banned removable devices（禁止リムーバブル デバイスへの書き込みをブロック）	禁止リムーバブル デバイスへの書き込み操作を追跡し、制御モードのすべてのポリシー（高、中、および低の適用レベル）でこの操作をブロックします。 **注意**：リムーバブル デバイスへの書き込みをブロックしても、CD/DVDメディアへの書き込みはブロックされません。	禁止リムーバブル デバイスへの書き込み操作を許可します。イベントはレポートされません。	書き込み操作を許可し、操作をイベントとしてレポートします。

設定	Active（アクティブ）	Off（オフ）	Report Only（レポートのみ）
Report reads from unapproved removable devices（未承認リムーバブル デバイスからの読み取りを報告）	選択できません。	未承認リムーバブル デバイスからの読み取りを許可します。イベントはレポートされません。	読み取りを許可し、操作をイベントとしてレポートします。
Report reads from banned removable devices（禁止リムーバブル デバイスからの読み取りを報告）	選択できません。	禁止リムーバブル デバイスからの読み取りを許可します。イベントはレポートされません。	読み取りを許可し、操作をイベントとしてレポートします。
Block execution from unapproved removable devices（未承認リムーバブル デバイスからの実行をブロック）	未承認リムーバブル デバイスでのファイルの実行を追跡し、制御モードのすべてのポリシー（高、中、および低の適用レベル）でこの操作をブロックします。 **注意**：どのデバイスもデフォルトでは未承認です。そのため、この設定をアクティブ化する前に、明示的に承認していないデバイスをすべてブロックする必要があるのかどうかを確認してください。	ファイル自体が別のルールで禁止されていない限り、未承認リムーバブル デバイスでのファイルの実行を許可します。イベントはレポートされません。	実行を許可し、操作をイベントとしてレポートします。
Block execution from banned devices（禁止デバイスからの実行をブロック）	禁止リムーバブル デバイスでのファイルの実行を追跡し、制御モードのすべてのポリシー（高、中、および低の適用レベル）でこの操作をブロックします。	ファイルが別のルールで禁止されていない限り、禁止リムーバブル デバイスでのファイルの実行を許可します。イベントはレポートされません。	実行を許可し、操作をイベントとしてレポートします。

デフォルト、テンプレート、およびローカル承認ポリシーでは、デバイス制御はすべて［Off（オフ）］に設定されています（ブロックおよびレポートなし）。ただし、禁止デバイスでの書き込みと実行をブロックする設定は［Active（アクティブ）］です。ローカル承認ポリシーを除き、すべてのポリシーでこの設定は変更できます。他のポリシーを作成する「前に」テンプレート ポリシーの設定を変更することで、ポリシー設定にかかる時間を節約できます。

ポリシーのデバイス制御を有効にする手順：

1. コンソール メニューで、[**Rules**（ルール）] > [**Policies**（ポリシー）] の順に選択します。[Policies（ポリシー）] ページが開きます。
2. [Policies（ポリシー）] ページで、デバイス設定を編集するポリシー名の隣の [View Details（詳細の表示）]（鉛筆とファイル）ボタンをクリックします。[Edit Policy（ポリシーの編集）] ページが開きます。



3. [Device Control Settings（デバイス制御設定）] パネルで、有効にする設定については [**Active**（アクティブ）] を、無効にする設定については [**Off**（オフ）] を選択します。また、Bit9 Server にデバイス上でのファイルのアクティビティをレポートさせる（ただし実施はしない）設定については [**Report Only**（レポートのみ）] を選択します。デバイスへの読み取りアクセスはブロックできません。そのため、2 つある読み取りに関する設定では [Active（アクティブ）] を選択できません。各設定の効果の詳細については、表 43、「デバイス制御設定の動作」386 ページを参照してください。
4. デバイス設定によりファイルアクセスがブロックされたときに表示される通知を変更（または削除）できます。これを実行するには、通知を変更する設定の横にある [Notifier（通知）] メニューでそれぞれ選択します。その他のオプションと詳細については、第 17 章「ブロック通知と承認要求」を参照してください。
5. デバイス設定とその通知を必要に応じて編集したら、[Edit Policy（ポリシーの編集）] ページの下部にある [Save（保存）] ボタンをクリックします。そのポリシーに対する変更が保存されます。
6. デバイス設定を変更する各ポリシーに対してこの手順を繰り返します。

特定のデバイスの管理

Bit9 Security Platform は、コンピューターで検出されたデバイスに関するさまざまな情報を収集します。この情報を使用して、デバイスでのファイルのアクティビティの処理方法を決定することができます。

デフォルトでは、すべてのデバイスが未承認の状態です（承認も禁止もされていません）。モデルとシリアル ナンバーのどちらかで、特定のリムーバブル デバイスを明示的に承認または禁止できます。他のルールでブロックされていないファイルは、承認されているデバイスで常に実行および書き込みを行うことが可能です。未承認および禁止ファイルの処理は、各ポリシーのデバイス制御設定によって異なります。

注意

禁止されているデバイスは、可視性モードに設定されているポリシーではブロックされません。ただし、デバイス設定で［Report Only（レポートのみ）］を選択すると、制御モードの場合はブロックされるデバイス関連アクティビティのイベントを生成できます。

同様に、特定のデバイスを禁止および承認しても、ポリシーでデバイス設定が［Active（アクティブ）］に設定されていない場合、アクセスはブロックまたは許可されません。

デバイス情報の表示

デバイス情報は［Devices（デバイス）］ページにテーブルの形で表示されます。このページにアクセスするには、コンソール メニューで、［**Assets**（アセット）］>［**Devices**（デバイス）］の順に選択します。それぞれのデバイス テーブルで、項目の横にある［View Details（詳細の表示）］ボタン（ファイルと鉛筆）をクリックすると、ページ上の各項目（モデル、デバイス インスタンス、または接続）の詳細ページを確認できます。これらのビューにそれぞれ表示される情報の種類を以下のテーブルに示します。

デバイス情報	情報が表示されるテーブル	各テーブル行の詳細ページ
検出されたデバイス モデル（ベンダーと名前）	Device Catalog（デバイス カタログ）（［Show Individual devices（個々のデバイスを表示）］ボックスが**オフ**）	Device Model Details（デバイス モデルの詳細）（1 つのモデルについて）
検出された個々のデバイス（一意のシリアル ナンバー）	Device Catalog（デバイス カタログ）（［Show Individual devices（個々のデバイスを表示）］ボックスが**オン**）	Device Details（デバイスの詳細）（1 つのシリアル ナンバーについて）
個々のコンピューターに接続されている個々のデバイス	Devices on Computers（コンピューター上のデバイス）	Device Attachment Details（デバイス接続の詳細）（デバイスとコンピューターの 1 つのペアについて）

デバイス テーブルには［Saved Views（保存済みビュー）］はありませんが、［Group By（グループ別）］メニューを使用することで、さまざまなフィールドで情報をグループ化できます。たとえば、「ベンダー」でグループ化されたデバイスをすべて表示したり、モデルのルールに対する「例外」となるルールに当てはまる特定のシリアル ナンバーのデバイス モデルをすべて表示したりすることが可能です。［Group By（グループ別）］メニューには、これらの各ケースに対応するオプションがあります。ビューの変更にまだ慣れていない場合は、「Bit9 コンソールのテーブル」（68 ページ）を参照してください。

モデル別のデバイスの管理

コンピューターに接続されているデバイスは、モデル別に監視および管理できます。モデル別にデバイスを管理することで、1 つのルールで多くのデバイスを制御できます。実行できる操作は以下のとおりです。

- ［Device Catalog（デバイス カタログ）］でデバイス モデルの完全なリストを表示できます。
- ［Device Model Details（デバイス モデルの詳細）］ページで 1 つのデバイス モデルに関する全情報を表示できます。［Related Views（関連ビュー）］メニューを使用して、デバイス モデルに「関連」するその他の情報を表示できます。
- ［Device Catalog（デバイス カタログ）］ページまたは［Device Model Details（デバイス モデルの詳細）］ページで、承認、禁止、承認または禁止の削除を実行できます。

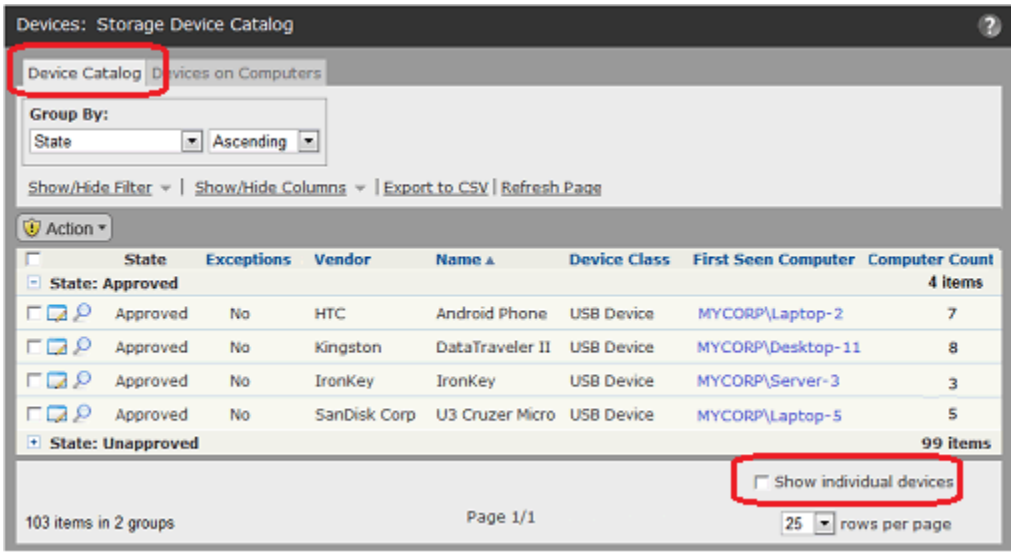
［Device Catalog（デバイス カタログ）］でのデバイス モデルの表示

デバイス モデルは、ベンダーと製品名の固有の組み合わせにより識別されます。［Device Model（デバイス モデル）］テーブルには、コンピューターに接続されているデバイスの種類に関する一般的な情報が表示され、デバイス モデルのすべてのインスタンスを承認または禁止できます。

Bit9 によって検出されたすべてのデバイス モデルを表示する手順：

1. コンソール メニューで、［**Assets**（アセット）］>［**Devices**（デバイス）］の順に選択します。［Devices（デバイス）］ページが表示されます。
2. ［**Device Catalog**（デバイス カタログ）］タブをクリックします。［Device Catalog（デバイス カタログ）］テーブルがページに表示されます。

3. ページ下部にスクロールし、[Show individual devices（個々のデバイスを表示）] チェックボックスがオンの場合、クリックしてオフにします。[Device Catalog（デバイス カタログ）] にデバイス モデルのテーブルが表示されます。



このテーブルに表示できる列の説明については、表 44、「デバイス モデルの詳細」393 ページを参照してください。

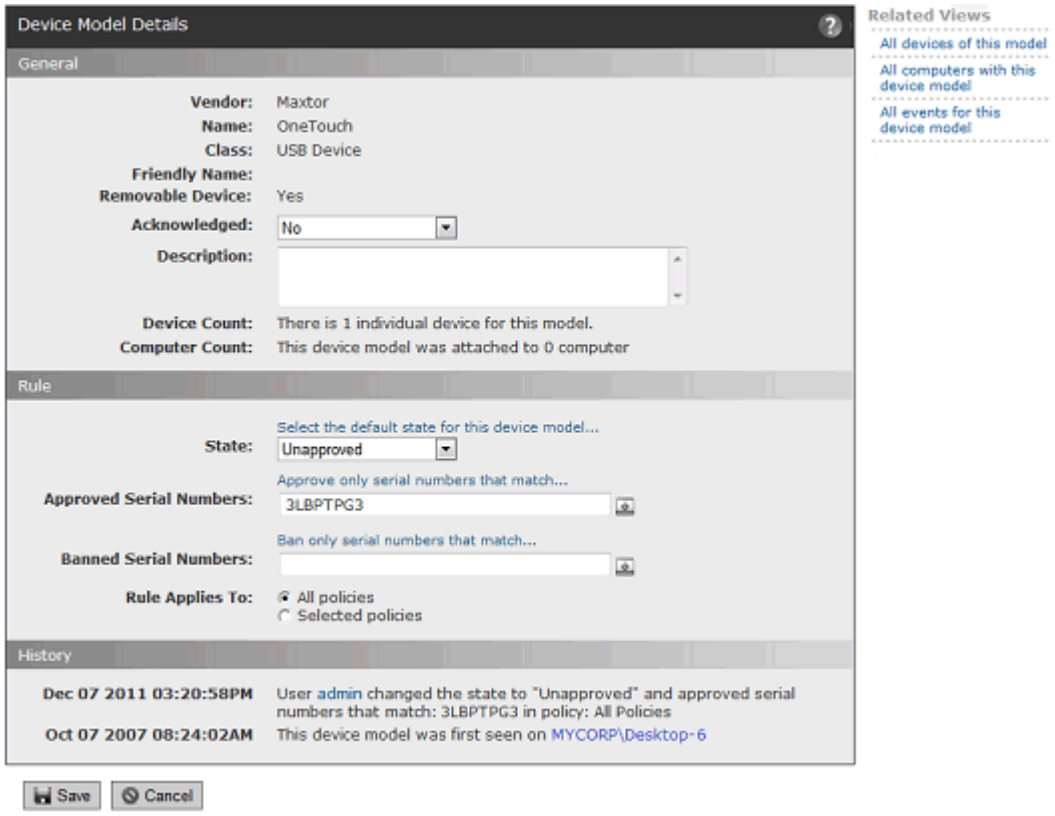
[Device Catalog（デバイス カタログ）] 内のモデルに対する [Action（アクション）] メニューは、テーブル内のボックスがオンの行に対して適用されます。メニューには以下のコマンドがあります。

- Globally Approve（グローバル承認）
- Globally Ban（グローバル禁止）
- Remove Approval or Ban（承認または禁止を削除）
- Acknowledge（確認）

承認および禁止コマンドについては、「デバイス モデルの承認と禁止」（394 ページ）で説明されています。[Acknowledge（確認）] コマンドは、特定のモデルを確認し、そのステータスに対して所定のアクションを実行したことを示すために使用できます。その後に、未確認のデバイス モデルが見やすくなるよう、テーブルを並べ替えることやフィルターすることができます。

1 つのデバイス モデルの詳細の表示

[Device Model Details（デバイス モデルの詳細）] ページには、モデルに関する情報が表示されます。表 44、「デバイス モデルの詳細」でこのページに表示されるフィールドについて説明します。



また［Device Model Details（デバイス モデルの詳細）］ページでは、このモデルのデバイスを扱う方法に関するルールを構成できます。この操作はメニューではなくページ自体で行います。ルールには、モデルの全体的な状態や、特定のシリアル ナンバーに対する例外を含めることができます。

［Related Views（関連ビュー）］メニューには、以下の情報へのリンクがあります。

- ［**All devices of this model**（このモデルのすべてのデバイス）］–［Device Catalog（デバイス カタログ）］をフィルターして、エージェント管理コンピューターに接続されている、このデバイス モデルのすべてのインスタンスを表示します。
- ［**All computers with this device model**（このデバイス モデルが接続されているすべてのコンピューター）］–［Devices on Computers（コンピューター上のデバイス）］テーブルをフィルターして、このモデルのデバイスが接続されているすべてのコンピューターを表示します。
- ［**All events for this device model**（このデバイス モデルのすべてのイベント）］–［Events（イベント）］ページに移動し、ページをフィルターして、このデバイス モデルに関連するすべてのイベントを表示します。イベントには、各インスタンスの最初の検出や、このモデルのデバイスがコンピューターに接続された日時またはコンピューターから取り外された日時が含まれます。

表 44：デバイス モデルの詳細

フィールド	説明
Vendor（ベンダー）	デバイスのブランド（「SanDisk」など）。デバイスに検出可能なベンダー情報がない場合、このフィールドには［USB DISK（USB ディスク）］や［Flash（フラッシュ）］などと表示されることがあります。
Name（名前）	デバイス モデルの名前です。商品名（「Jumpdrive Pro」など）やモデル名（「c30w」など）が表示されます。デバイスに検出可能なモデル名がない場合、このフィールドには［USB Storage Device（USB ストレージ デバイス）］や［Unnamed Product（無名の製品）］などと表示されることがあります。
Class（クラス）	これは主にデバイスのインターフェイスの説明です。値は、［IDE Device（IDE デバイス）］、［SATA Device（SATA デバイス）］、［SCSI Device（SCSI デバイス）］、［USB Device（USB デバイス）］、［FireWire (IEEE 1394) Device（FireWire (IEEE 1394) デバイス）］、［Serial Bus Protocol 2（シリアル バス プロトコル 2）］、［Floppy Disk（フロッピー ディスク）］、および［Unknown（不明）］です。
Removable Device（リムーバブル デバイス）	デバイスがリムーバブルであるかどうかが表示されます。値は［**Yes**（はい）］または［**No**（いいえ）］です。デバイスによっては、このフィールドに正確な情報が表示されない場合があります。
Friendly Name（わかりやすい名前）	このデバイスの共通の名前です。たとえば、デバイス接続時に Windows エクスプローラーに表示される名前です。
Acknowledged（確認済み）*	デバイスを確認して、既に確認済みのため、詳しく追跡する必要がないことを指定できます。デバイスを確認しても、そのデバイスの承認状態は変わりません。［Action（アクション）］メニューと詳細ページのドロップダウン メニューで、このフィールドに対して［**Yes**（はい）］または［**No**（いいえ）］を選択できます。
Description（説明）	編集可能なテキストで、このデバイス モデルのレコードに任意の情報を追加できます。
Device Count（デバイス数）	コンピューター上で Bit9 によって検出されたこのモデルの一意のデバイス（つまり、一意のシリアル ナンバー）の数。
Computer Count（コンピューター数）	このモデルのデバイスが接続されているコンピューターの数。
First Seen Platform（最初に確認されたプラットフォーム）	このデバイス　　モデルが確認された最初のプラットフォーム（Windows、Mac、または Linux）。リリース 7.2.3 では、このフィールドは必ず Windows になります。
State（状態）	このデバイス モデルのデフォルトの状態。値は、［Approved（承認）］、［Banned（禁止）］、［Unapproved（未承認）］です。デバイス モデルの特定のインスタンス（シリアル ナンバー）に対して、デフォルトのモデルの状態とは異なる状態を指定できます。

フィールド	説明
Approved Serial Numbers（承認するシリアル ナンバー）	デバイス モデルのデフォルトの状態が［Unapproved（未承認）］または［Banned（禁止）］の場合、［Approved（承認）］状態にするシリアル ナンバーを指定できます。特定のシリアル ナンバーを 1 つ以上入力することや、ある範囲の数字が含まれるようにワイルドカードを使用したパターンを入力することができます。
Banned Serial Numbers（禁止するシリアル ナンバー）	デバイス モデルのデフォルトの状態が［Unapproved（未承認）］または［Approved（承認）］の場合、［Banned（禁止）］状態にするシリアル ナンバーを指定できます。特定のシリアル ナンバーを 1 つ以上入力することや、ある範囲の数字が含まれるようにワイルドカードを使用したパターンを入力することができます。
Rule Applies To（ルールの適用先）	デバイス モデルのルールは、すべてのポリシーのコンピューターに対して、または特定のポリシーのコンピューターのみに対して適用できます。
History（履歴）	デバイスが検出された日時と、デバイスに影響を及ぼすルールが適用または変更された日時が記録されます。

デバイス モデルの承認と禁止

デバイス モデルの承認と禁止の管理には次の 2 つの方法があります。

- ［Device Catalog（デバイス カタログ）］で、テーブル内の 1 つ以上のデバイス モデルのボックスをオンにし、［Action（アクション）］メニューで、オンにしたすべてのアイテムに対して承認、禁止、承認または禁止の削除を実行できます。
- ［Device Model Details（デバイス モデルの詳細）］ページで、ページ上に表示されているデバイス モデルに対して承認、禁止、承認または禁止の削除を実行できます。モデルに対するデフォルト ルールの例外（シリアル ナンバーを使用）を表示、追加、および削除することもできます。また、すべてのポリシーまたは特定のポリシーにのみ適用するルールを作成できます。

［Device Catalog（デバイス カタログ）］で 1 つ以上のデバイス モデルを承認する手順：

1. コンソール メニューで、［**Assets**（アセット）］>［**Devices**（デバイス）］の順に選択します。［Devices（デバイス）］ページが表示されます。
2. ［Device Catalog（デバイス カタログ）］タブをクリックし、カタログ ページの右下隅にある［Show individual devices（個々のデバイスを表示）］ボックスが「オフ」になっていることを確認します。表示されるテーブルのタイトルは、［Devices: Storage Device Catalog（デバイス：ストレージ デバイス カタログ）］です。
3. 承認する各デバイス　モデルの横にあるボックスをオンにし、［Action（アクション）］メニューで［**Globally Approve**（グローバル承認）］を選択します。
4. 確認ダイアログで **[OK]** を選択します。デバイス モデルが承認され、デバイス モデルのすべてのインスタンスがデフォルトで承認されるようになります。

1 つ以上のモデルを禁止するには、上記の手順を使用し、ステップ 3 の［Action（アクション）］メニューで［**Globally Ban**（グローバル禁止）］を代わりに選択します。

1 つ以上のモデルから承認または禁止を削除するには、上記の手順を使用し、ステップ 3 の［Action（アクション）］メニューで［**Remove Approval or Ban**（承認または禁止を削除）］を代わりに選択します。

注意

- 承認または禁止できるのは、リムーバブルとして認識されたデバイスだけです。［Device Catalog（デバイス カタログ）］でモデルを承認または禁止するときに、「固定」デバイスのチェックボックスがオンになっている場合、エラー メッセージが表示され、リムーバブル以外のドライブは影響を受けません。「リムーバブル」デバイスが選択の中に含まれている場合、他のデバイスがリムーバブルでなくても、そのデバイスはコマンドの影響を受けます。テーブル内の［Removable Device（リムーバブル デバイス）］の列のボックスをオンにすることで、デバイスを承認または禁止するかどうかを決定できます。
- ［Device Catalog（デバイス カタログ）］で実行する承認および禁止のアクションはすべてグローバルであるため、すべてのデバイス インスタンスとすべてのポリシーのコンピューターが影響を受けます。承認または禁止を特定のポリシーのコンピューター上のデバイスに限定する場合、または特定のデバイスのシリアル ナンバーに対するルールの例外を追加する場合は、［Device Model Details（デバイス モデルの詳細）］ページを使用します。
- ［Remove Approval or Ban（承認または禁止を削除）］コマンドを使用するときは、禁止されているモデルと承認されているモデルを組み合わせて選択できます。状態はすべて［Unapproved（未承認）］に変更されます。

［Device Model Details（デバイス モデルの詳細）］ページで 1 つのデバイス モデルを承認する手順：

1. コンソール メニューで、［**Assets**（アセット）］>［**Devices**（デバイス）］の順に選択します。［Devices（デバイス）］ページが表示されます。
2. ［Device Catalog（デバイス カタログ）］タブをクリックし、カタログ ページの右下隅にある［Show individual devices（個々のデバイスを表示）］ボックスが「オフ」になっていることを確認します。表示されるテーブルのタイトルは、［Devices: Storage Device Catalog（デバイス：ストレージ デバイス カタログ）］です。
3. 承認するデバイス モデルの隣の［View Details（詳細の表示）］ボタン（ファイルと鉛筆）をクリックします。［Device Model Details（デバイス モデルの詳細）］ページが表示されます。

4. この承認を特定のポリシーに限定する場合、[**Selected policies**（選択されたポリシー)] ラジオ ボタンをクリックし、有効にするポリシーの横にあるボックスをオンにします。
5. [State（状態)] メニューで [**Approved**（承認)] を選択します。
6. モデル自体を承認していても、このデバイス モデルの特定のインスタンスを禁止する場合、[Banned Serial Numbers（禁止するシリアル ナンバー)] フィールドに 1 つ以上のシリアル ナンバー（または、ワイルドカードを使用したシリアル ナンバーのパターン）を入力します。

   [Device Catalog（デバイス カタログ）] または [Devices on Computers（コンピューター上のデバイス)] テーブル内のデバイス インスタンスを承認または禁止するか、または [Device Instance Details（デバイス インスタンスの詳細)] ページまたは [Device Attachment Details（デバイス接続の詳細)] ページで承認または禁止コマンドを使用することで、例外を後から追加することもできます。
7. ページ下部の [Save（保存)] ボタンをクリックし、確認ダイアログで **[OK]** をクリックします。デバイス モデルが承認され、作成した例外が適用されるインスタンスを除き、すべてのインスタンスが承認されます。

詳細ページでモデルを禁止するには、上記の手順を使用し、ステップ 5 の [State（状態)] メニューで [**Banned**（禁止)] を選択します。例外を作成する必要があり、シリアル ナンバーがわかっている場合、[Approved Serial Numbers（承認するシリアル ナンバー)] フィールドに一致する数字またはパターンを入力します。

詳細ページを使用してモデルから承認または禁止を削除するには、上記の手順を使用し、ステップ 3 の [Action（アクション)] メニューで [**Unapproved**（未承認)] を代わりに選択します。

注意

承認または禁止できるのは、リムーバブルとして認識されたデバイスだけです。リムーバブル以外のデバイスの場合、[Device Model Details（デバイス モデルの詳細)] ページに [Rules（ルール)] セクションが表示されません。

デバイス インスタンスの管理

シリアル ナンバーで識別される個々のデバイスを監視および管理できます。インスタンス別にデバイスを管理することで、同じモデルの他のデバイスとは処理が異なる特定のデバイスを制御できます。実行できる操作は以下のとおりです。

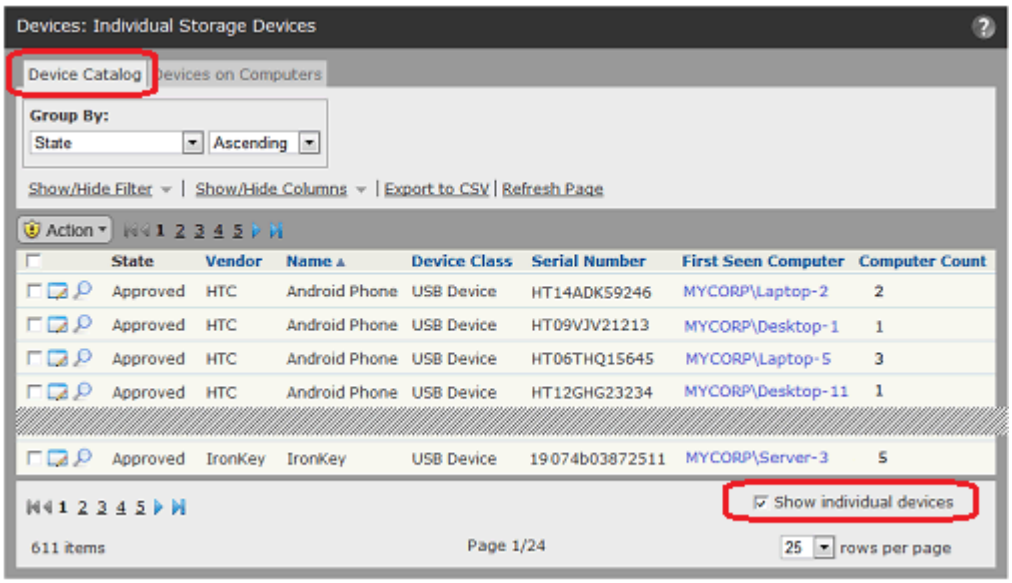
- [Device Catalog（デバイス カタログ)] でデバイス インスタンスの完全なリストを表示できます。
- [Device Details（デバイスの詳細)] ページで 1 つのデバイス インスタンスに関する全情報を表示できます。[Related Views（関連ビュー)] から、デバイスに関連するその他の情報を確認することもできます。
- [Device Catalog（デバイス カタログ)] ページまたは [Device Details（デバイスの詳細)] ページで、承認、禁止、承認または禁止の削除を実行できます。

[Device Catalog（デバイス カタログ）] でのインスタンスの表示

デバイス インスタンスは、シリアル ナンバー、ベンダー、および名前によって識別されます。デバイス インスタンス ビューは、コンピューター上のデバイスの数に関する情報を確認したり、特定のデバイス インスタンスを承認または禁止したりする場合に便利です。

Bit9 によって検出されたすべての一意のデバイス インスタンスを表示する手順：

1. コンソール メニューで、[**Assets**（アセット）] > [**Devices**（デバイス）] の順に選択します。[Devices（デバイス）] ページが表示されます。
2. [**Device Catalog**（デバイス カタログ）] タブをクリックします。[Device Catalog（デバイス カタログ）] テーブルがページに表示されます。
3. ページ下部にスクロールし、[Show individual devices（個々のデバイスを表示）] チェックボックスがオフの場合、クリックしてボックスをオンにします。[Device Catalog（デバイス カタログ）] に、一意のシリアル ナンバーを持つデバイス インスタンスのテーブルが表示されます。



このテーブルに表示できる列の説明については、表 45、「デバイスの詳細（一意のシリアル ナンバー）」 399 ページを参照してください。

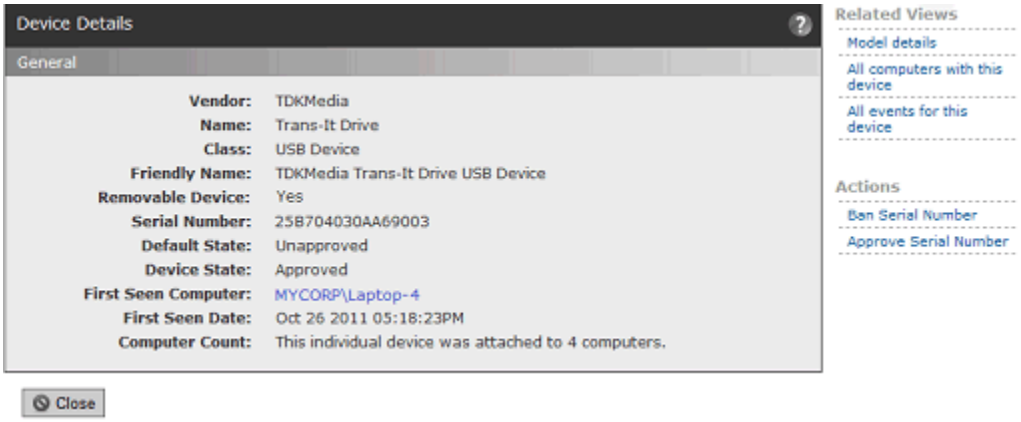
[Device Catalog（デバイス カタログ）] 内のインスタンスに対する [Action（アクション）] メニューは、テーブル内のボックスがオンの行に対して適用されます。メニューには以下のコマンドがあります。

- Globally Approve（グローバル承認）
- Globally Ban（グローバル禁止）
- Remove Approval or Ban（承認または禁止を削除）
- Acknowledge（確認）

承認および禁止コマンドについては、「デバイス インスタンスの承認または禁止」（400 ページ）で説明されています。[Acknowledge（確認）] コマンドは、特定のデバイス インスタンスを確認し、そのステータスに対して所定のアクションを実行したことを示すために使用できます。その後に、未確認のデバイス モデルが見やすくなるよう、テーブルを並べ替えることやフィルターすることができます。

1 つのデバイス インスタンスの詳細の表示

［Device Details（デバイスの詳細）］ページには、（一意のシリアル ナンバーを持つ）1 つの一意のデバイスに関する情報が表示されます。表 45、「デバイスの詳細（一意のシリアル ナンバー）」399 ページでこのページに表示されるフィールドについて説明します。



［Device Details（デバイスの詳細）］ページには、［Actions（アクション）］メニューと［Related Views（関連ビュー）］メニューがあります。

［Actions（アクション）］メニューには、このデバイスを承認および禁止するためのコマンドと、承認または禁止を削除するためのコマンドが含まれています。表示されるコマンドは、デバイスの現在の状態によって異なります。これらのコマンドを使用する方法の詳細については、「デバイス インスタンスの承認または禁止」（400 ページ）を参照してください。

［Related Views（関連ビュー）］メニューには、以下の情報へのリンクがあります。

- ［**Model details**（モデルの詳細）］– このデバイスの［Device Model Details（デバイス モデルの詳細）］ページに移動します。このページには、モデル自体とそのモデルに対するデフォルトのルールの定義に関する情報が表示されます。
- ［**All computers with this device**（このデバイスが接続されているすべてのコンピューター）］–［Devices on Computers（コンピューター上のデバイス）］テーブルをフィルターして、このデバイス インスタンスが接続されているすべてのコンピューターを表示します。
- ［**All events for this device**（このデバイスのすべてのイベント）］–［Events（イベント）］ページに移動し、ページをフィルターして、（シリアル ナンバーで識別される）このデバイス インスタンスに関連するすべてのイベントを表示します。イベントには、インスタンスの最初の検出や、このモデルのデバイスがコンピューターに接続された日時またはコンピューターから取り外された日時が含まれます。

表 45：デバイスの詳細（一意のシリアル ナンバー）

フィールド	説明
Vendor（ベンダー）	デバイスのブランド（「SanDisk」など）。デバイスに検出可能なベンダー情報がない場合、このフィールドには［USB DISK（USB ディスク）］や［Flash（フラッシュ）］などと表示されることがあります。
Name（名前）	デバイス モデルの名前です。商品名（「Jumpdrive Pro」など）やモデル名（「c30w」など）が表示されます。デバイスに検出可能なモデル名がない場合、このフィールドには［USB Storage Device（USB ストレージ デバイス）］や［Unnamed Product（無名の製品）］などと表示されることがあります。
Class（クラス）	これは主にデバイスのインターフェイスの説明です。値は、［IDE Device（IDE デバイス）］、［SATA Device（SATA デバイス）］、［SCSI Device（SCSI デバイス）］、［USB Device（USB デバイス）］、［FireWire (IEEE 1394) Device（FireWire (IEEE 1394) デバイス）］、［Serial Bus Protocol 2（シリアル バス プロトコル 2）］、［Floppy Disk（フロッピー ディスク）］、および［Unknown（不明）］です。
Removable Device（リムーバブル デバイス）	デバイスがリムーバブルであるかどうかが表示されます。値は［**Yes**（はい）］または［**No**（いいえ）］です。デバイスによっては、このフィールドに正確な情報が表示されない場合があります。
Friendly Name（わかりやすい名前）	このデバイスの共通の名前です。たとえば、デバイス接続時に Windows エクスプローラーに表示される名前です。ベンダーと名前を組み合わせたものや変形させたものがよく表示されます。
Serial Number（シリアル ナンバー）	この一意の個別のデバイスを識別するシリアル ナンバー。
Default State（デフォルトの状態）	このデバイスのデフォルトの状態（デバイスの「モデル」の状態）。値は、［Approved（承認）］、［Banned（禁止）］、［Unapproved（未承認）］です。この特定のインスタンスは、デフォルトの状態とは異なる状態になる場合があります。
Device State（デバイスの状態）	（シリアル ナンバーで識別される）この個別のデバイスの実際の状態。値は、［Approved（承認）］、［Banned（禁止）］、［Unapproved（未承認）］です。
First Seen Computer（最初に確認されたコンピューター）	Bit9 エージェントによってこの個別のデバイスが最初に検出されたコンピューター。
Platform（プラットフォーム）	デバイスが最初に検出されたコンピューターのプラットフォーム（Windows、Mac、または Linux）。リリース 7.2.3 では、このフィールドは必ず Windows になります。
First Seen Date（最初に確認された日付）	Bit9 エージェントによってこの個別のデバイスが最初に検出された日時。
Computer Count（コンピューター数）	この個別のデバイスが接続されている個別のコンピューターの数。

デバイス インスタンスの承認または禁止

デバイス インスタンス（シリアル ナンバー）の承認と禁止の管理には次の 2 つの方法があります。

- ［Device Catalog（デバイス カタログ）］ページまたは［Devices on Computers（コンピューター上のデバイス）］ページで、テーブル内の 1 つ以上のデバイス インスタンスのボックスをオンにし、［Action（アクション）］メニューで、オンにしたすべてのアイテムに対して承認、禁止、承認または禁止の削除を実行できます。
- ［Device Details（デバイスの詳細）］ページまたは［Device Attachment Details（デバイス接続の詳細）］ページで、ページ上に表示されているデバイス インスタンスに対して承認、禁止、承認または禁止の削除を実行できます。

インスタンスをデバイス モデルのデフォルトの状態とは異なる状態にする場合、必要な操作はインスタンスの承認、禁止、インスタンスからの承認または禁止の削除を実行することだけです。インスタンス別の例外は、デバイス モデルの［Device Model Details（デバイス モデルの詳細）］ページに表示されます。

［Device Catalog（デバイス カタログ）］で 1 つ以上のデバイス インスタンスを承認する手順：

1. コンソール メニューで、［**Assets**（アセット）］>［**Devices**（デバイス）］の順に選択します。［Devices（デバイス）］ページが表示されます。
2. 以下のいずれかを実行します。
   - ［**Device Catalog**（デバイス カタログ）］タブをクリックし、カタログ ページの右下隅にある［Show individual devices（個々のデバイスを表示）］ボックスがオンになっていることを確認します。表示されるテーブルのタイトルは、［Devices: Individual Storage Devices（デバイス：個々のストレージデバイス）］です。
     または
   - ［**Devices on Computers**（コンピューター上のデバイス）］タブをクリックします。
3. 承認する各デバイス　インスタンスの横にあるボックスをオンにし、［Action（アクション）］メニューで［**Globally Approve**（グローバル承認）］を選択します。
4. 確認ダイアログで [**OK**] を選択します。デバイスがシリアル ナンバー別に承認されます。

1 つ以上のインスタンスを禁止するには、上記の手順を使用し、ステップ 3 の［Action（アクション）］メニューで［**Globally Ban**（グローバル禁止）］を代わりに選択します。

1 つ以上のインスタンスから承認または禁止を削除するには、上記の手順を使用し、ステップ 3 の［Action（アクション）］メニューで［**Remove Approval or Ban**（承認または禁止を削除）］を代わりに選択します。

注意

- 承認または禁止できるのは、リムーバブルとして認識されたデバイスだけです。デバイスを承認または禁止するときに、「固定」デバイスのチェックボックスがオンになっている場合、エラー メッセージが表示され、リムーバブル以外のドライブは影響を受けません。「リムーバブル」デバイスが選択の中に含まれている場合、他のデバイスがリムーバブルでなくても、そのデバイスはコマンドの影響を受けます。テーブル内の［Removable（リムーバブル）］の列のボックスをオンにすることで、デバイスを承認または禁止するかどうかを決定できます。
- デバイス「インスタンス」に対して実行した承認および禁止のアクションは、いずれもそのデバイス「モデル」のルール内の例外として扱われ、そのモデルのルールで指定されているすべてのポリシーまたは選択されたポリシーに対して適用されます。
- ［Remove Approval or Ban（承認または禁止を削除）］コマンドを使用するときは、禁止されているデバイスと承認されているデバイスを組み合わせて選択できます。状態はすべて［Unapproved（未承認）］に変更されます。

［Device Details（デバイスの詳細）］ページまたは［Device Attachment Details（デバイス接続の詳細）］ページでインスタンスを承認する手順：

1. コンソール メニューで、［**Assets**（アセット）］>［**Devices**（デバイス）］の順に選択します。［Devices（デバイス）］ページが表示されます。
2. 以下のいずれかを実行します。
   - ［**Device Catalog**（デバイス カタログ）］タブをクリックし、カタログ ページの右下隅にある［Show individual devices（個々のデバイスを表示）］ボックスがオンになっていることを確認します。表示されるテーブルのタイトルは、［Devices: Individual Storage Devices（デバイス：個々のストレージデバイス）］です。
     または
   - ［**Devices on Computers**（コンピューター上のデバイス）］タブをクリックします。
3. 承認するデバイス インスタンスの隣の［View Details（詳細の表示）］ボタン（ファイルと鉛筆）をクリックします。［Device Details（デバイスの詳細）］ページまたは［Device Attachment Details（デバイス接続の詳細）］ページが表示されます。

4. ページ右側の［Actions（アクション）］メニューで、［**Approve Serial Number**（シリアル ナンバーを承認）］を選択します。デバイスが承認され、デバイスのシリアル ナンバーがそのモデルの［Device Model Details（デバイス モデルの詳細）］ページ上で例外として追加されます。

詳細ページでデバイス インスタンスを禁止するには、上記の手順を使用し、ステップ 4 の［Action（アクション）］メニューで［**Ban Serial Number**（シリアル ナンバーを禁止）］を代わりに選択します。

詳細ページでデバイス インスタンスの承認または禁止を削除するには、同じ手順を使用し、適切な削除コマンドを代わりに使用します。

注意

承認または禁止できるのは、リムーバブルとして認識されたデバイスだけです。固定デバイスの承認または禁止を試みると、エラー メッセージが表示されます。

コンピューターとデバイス間の接続の管理

特定のデバイス インスタンスと特定のコンピューターとの間の接続を監視し、個々のデバイスを管理できます。実行できる操作は以下のとおりです。

- ［Devices on Computers（コンピューター上のデバイス）］テーブルでデバイスとコンピューター間の接続の完全なリストを表示できます。
- ［Device Attachment Details（デバイス接続の詳細）］ページで、1 つの特定のデバイスと 1 つの特定のコンピューターとの間の接続に関する全情報を表示できます。［Related Views（関連ビュー）］から、この接続または個々のデバイスに関連するその他の情報を確認することもできます。
- ［Devices on Computers（コンピューター上のデバイス）］テーブルまたは［Device Attachment Details（デバイス接続の詳細）］ページで、承認、禁止、承認または禁止の削除を実行できます。

コンピューター上のデバイスの表示

［Devices on Computers（コンピューター上のデバイス）］タブには、個々のコンピューターに接続されている個々のデバイスのテーブルが表示されます。1 つのデバイスと 1 つのコンピューターとの間の関係は、接続された回数と取り外された回数にかかわらず、テーブル内で 1 つの「接続」としてカウントされます。特定のコンピューター上でのリムーバブル デバイスの使用が懸念される場合、［Devices on Computers（コンピューター上のデバイス）］ページでそのような接続が存在するかどうかを確認できます。このテーブルで個々のデバイスを承認または禁止できます。

特定のデバイスと特定のコンピューターとの間のすべての接続を表示する手順：

1. コンソール メニューで、[**Assets**（アセット）] > [**Devices**（デバイス）] の順に選択します。[Devices（デバイス）] ページが表示されます。
2. [**Devices on Computers**（コンピューター上のデバイス）] タブをクリックします。[Devices on Computers（コンピューター上のデバイス）] ページが表示されます。ページには、（一意のシリアル ナンバーを持つ）デバイス インスタンスと特定のコンピューターとの組み合わせがそれぞれ表示されます。

このテーブルに表示できる列の説明については、表 46、「デバイス接続の詳細」405 ページを参照してください。

[Devices on Computers（コンピューター上のデバイス）] テーブル内のインスタンスに対する [Action（アクション）] メニューは、テーブル内のボックスがオンの行に対して適用されます。メニューには以下のコマンドがあります。

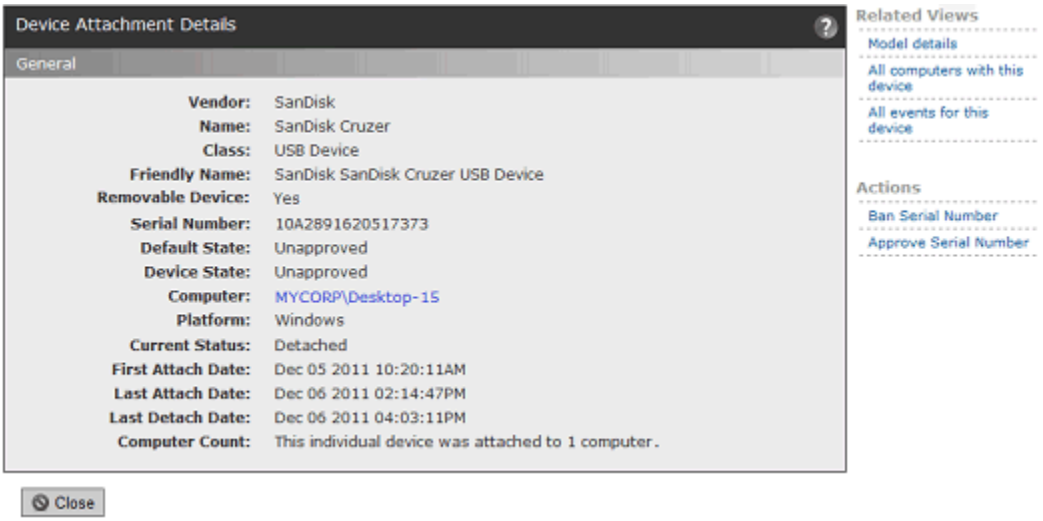
- Globally Approve（グローバル承認）
- Globally Ban（グローバル禁止）
- Remove Approval or Ban（承認または禁止を削除）
- Acknowledge（確認）

[Devices on Computers（コンピューター上のデバイス）] テーブルとインスタンスの [Device Catalog（デバイス カタログ）] の承認および禁止コマンドは、ボックスがオンの行の（シリアル ナンバーで定義される）インスタンスに適用されます。特定の「接続」が承認または禁止されるわけではありません。詳細については、「デバイス インスタンスの承認または禁止」（400 ページ）を参照してください。

[Acknowledge（確認）] コマンドは、特定のデバイス インスタンスを確認し、そのステータスに対して所定のアクションを実行したことを示すために使用できます。その後に、未確認のデバイス モデルが見やすくなるよう、テーブルを並べ替えることやフィルターすることができます。

コンピューターとデバイス間の 1 つの接続の詳細の表示

［Device Attachment Details（デバイス接続の詳細）］ページには、1 つのデバイス インスタンスと 1 つのコンピューターとの間の接続の履歴に関する情報が表示されます。表 46、「デバイス接続の詳細」405 ページでこのページに表示されるフィールドについて説明します。



［Device Attachment Details（デバイス接続の詳細）］ページには、［Action（アクション）］メニューと［Related Views（関連ビュー）］メニューがあります。

［Action（アクション）］メニューには、このデバイス インスタンスを承認および禁止するためのコマンドと、承認および禁止を削除するためのコマンドが含まれています。表示されるコマンドは、デバイスの現在の状態によって異なります。これらのコマンドを使用する方法の詳細については、「デバイス インスタンスの承認または禁止」（400 ページ）を参照してください。

［Related Views（関連ビュー）］メニューには、以下の情報へのリンクがあります。

- ［**Model details**（モデルの詳細）］– このデバイスの［Device Model Details（デバイス モデルの詳細）］ページに移動します。このページには、モデル自体とそのモデルに対するデフォルトのルールの定義に関する情報が表示されます。
- ［**All computers with this device**（このデバイスが接続されているすべてのコンピューター）］–［Devices on Computers（コンピューター上のデバイス）］テーブルをフィルターして、このデバイス インスタンスが接続されているすべてのコンピューターを表示します。
- ［**All events for this device**（このデバイスのすべてのイベント）］–［Events（イベント）］ページに移動し、ページをフィルターして、「このコンピューター上の」（シリアル ナンバーで識別される）このデバイス インスタンスに関連するすべてのイベントを表示します。イベントには、インスタンスの最初の検出や、このモデルのデバイスがコンピューターに接続された日時またはコンピューターから取り外された日時が含まれます。

表 46：デバイス接続の詳細

フィールド	説明
Vendor（ベンダー）	デバイスのブランド（「SanDisk」など）。デバイスに検出可能なベンダー情報がない場合、このフィールドには［USB DISK（USB ディスク）］や［Flash（フラッシュ）］などと表示されることがあります。
Name（名前）	デバイス モデルの名前です。商品名（「Jumpdrive Pro」など）やモデル名（「c30w」など）が表示されます。デバイスに検出可能なモデル名がない場合、このフィールドには［USB Mass Storage Device（USB 大容量ストレージ デバイス）］や［Unnamed Product（無名の製品）］などと表示されることがあります。
Class（クラス）	これは主にデバイスのインターフェイスの説明です。値は、［IDE Device（IDE デバイス）］、［SATA Device（SATA デバイス）］、［SCSI Device（SCSI デバイス）］、［USB Device（USB デバイス）］、［FireWire (IEEE 1394) Device（FireWire (IEEE 1394) デバイス）］、［Serial Bus Protocol 2（シリアル バス プロトコル 2）］、［Floppy Disk（フロッピー ディスク）］、および［Unknown（不明）］です。
Removable Device（リムーバブル デバイス）	デバイスがリムーバブルであるかどうかが表示されます。値は［**Yes**（はい）］または［**No**（いいえ）］です。デバイスによっては、このフィールドに正確な情報が表示されない場合があります。
Friendly Name（わかりやすい名前）	このデバイスの共通の名前です。たとえば、デバイス接続時に Windows エクスプローラーに表示される名前です。ベンダーと名前を組み合わせたものや変形させたものがよく表示されます。
Serial Number（シリアル ナンバー）	コンピューターに接続されている一意の個別のデバイスを識別するシリアル ナンバー。
Default State（デフォルトの状態）	このデバイス モデルのデフォルトの状態。値は、［Approved（承認）］、［Banned（禁止）］、［Unapproved（未承認）］です。この特定のインスタンスは、モデルのデフォルトの状態とは異なる状態になる場合があります。
Device State（デバイスの状態）	（シリアル ナンバーで識別される）この個別のデバイスの実際の状態。値は、［Approved（承認）］、［Banned（禁止）］、［Unapproved（未承認）］です。
Computer（コンピューター）	デバイスが接続されているコンピューターの名前。
Platform（プラットフォーム）	デバイスが接続されているコンピューターのプラットフォーム（Windows、Mac、または Linux）。リリース 7.2.3 では、このフィールドは必ず Windows になります。

フィールド	説明
Current Status（現在の状態）	この接続を定義するデバイスとコンピューターが現在接続されているか取り外されているか。 **注意**：Bit9 Server に接続していないコンピューターのデバイス接続の状態は、コンピューターが接続されていたときの最後の既知の状態です。
First Attach Date（最初に接続された日付）	デバイスとコンピューターが最初に接続された日時。
Last Attach Date（最後に接続された日付）	デバイスとコンピューターが最後に接続された日時。
Last Detach Date（最後に取り外された日付）	デバイスがコンピューターから最後に取り外された日時。
Computer Count（コンピューター数）	（シリアル ナンバーで識別される）この個別のデバイスが接続されている個別のコンピューターの数。

第 12 章

カスタム ソフトウェア ルール

この章では、指定したパスに一致するファイルに対して特別な処理を実行するカスタム ルールについて説明します。カスタム ルールはパフォーマンスの最適化、ファイル整合性の制御、ソフトウェア配布元として信頼できるファイル パスの作成など、特殊な状況で使用できます。また、承認や禁止など、その他のルールに対する例外を作成する目的にも使用できます。

注意

ファイルを承認または禁止する標準的な方法については下記を参照してください。第 8 章「ソフトウェアの承認と禁止」

Bit9 Security Platform には次のようなルールもあります。

- スクリプトの定義を追加または変更するルールについては、第 13 章「スクリプト ルール」を参照してください。
- Windows レジストリを保護するルールについては、第 14 章「レジストリ ルール」を参照してください。
- 実行中のプロセスに他のプロセスがアクセスして変更を加えられないように保護するルールについては、第 15 章「メモリ ルール」を参照してください。
- 特定のイベントが発生したときにファイルの承認や禁止などのアクションを実行するルールについては、第 16 章「イベント ルール」を参照してください。

セクション

概要

カスタム ルールを作成すると、指定したファイル パスに一致するファイルに対して特別な処理を実行できます。カスタム ルールでは、パスの指定やその他のルール パラメーターに一致した場合に、ファイルの実行や書き込み操作をブロックしたり、許可したり、レポートしたり、無視するなどの具体的なアクションを実行するように指定することができます。

ルール タイプ

Bit9 Security Platformには特定の目的を達成できるように一部設定済みのカスタム ルールがいくつか用意されています。

- ［**File Integrity Control**（ファイル整合性の制御）］– 指定されたフォルダーやファイルの変更をブロックまたはレポートします。
- ［**Trusted Path**（信頼済みパス）］– ファイルの実行を常に許可するフォルダーやファイルを定義します。
- ［**Execution Control**（実行の制御）］– 指定された条件に一致するファイルの実行が試みられたときの動作を制御するルールを作成します。
- ［**File Creation Control**（ファイル作成の制御）］– 指定された条件に一致するファイルの書き込みが試みられたときの動作を制御するルールを作成します。
- ［**Performance Optimization**（パフォーマンスの最適化）］– ファイルの作成、変更、削除を無視するフォルダーとファイルを指定します（ただし、ファイルの実行は引き続き監視されます）。

ルールの種類として［**Advanced**（詳細）］を選択すると、すべてのパラメーターを手動で設定できます。

カスタム ルールは、ネットワーク ログイン スクリプトやソフトウェア配布システムを利用できるようにしたり、Bit9 Server によるファイル アクティビティの監視やルール適用の対象から除外してソフトウェア開発者が実行可能ファイルを実行できる場所を指定する目的などに使用できます。また、カスタム ルールを使用してアプリケーションのディレクトリへの変更をブロックすることにより、ユーザーがアプリケーションをアンインストールできないようにすることもできます。

ルールの適用範囲

特定のプラットフォーム上で稼働するすべてのコンピューター（すべての Windows コンピューターなど）にあらゆる状況下で適用されるカスタム ルールを作成することもできますが、次の条件を 1 つ以上指定してルールの適用範囲を限定することもできます（ルールの種類によっては、ここに示されているすべてのオプションを指定できない場合があります）。

- **プロセス別** – 特定のプロセスが指定された場所でファイルの書き込みまたは実行を試みた場合にのみルールを適用できます。
- **ユーザー別またはグループ別** – 特定のユーザーまたはユーザー グループのみに対してルールを適用できます。
- **ポリシー別** – 指定されたポリシーに含まれるコンピューターのみにルールを適用できます。

- **ルール ランキング** – カスタム ルールはランク順に評価されます。各ルールのランクはデフォルトで［Custom Rules（カスタム ルール）］テーブルに表示されます。ランクが「1」に設定されているルールが最優先され、「2」に設定されているルールがその次に優先されます。1 つの例外（ファイルの書き込みを無視するルール）を除き、各ファイルに最初に一致したルールのみが評価されます。ルールの順序は変更できます。たとえば、フォルダー内の特定のファイルのみに適用されるルールをリスト内の上位に配置し、同じフォルダーの全ファイルに適用される別のルールをリスト内の下位に配置することで、上位のルールを優先することができます。

ユーザーが作成したカスタム ルールはプラットフォーム固有のルールとなり、Bit9 エージェントをインストールできるプラットフォーム（Windows、Mac、または Linux）のうち、いずれか 1 種類のみに適用されます。

ファイルおよびプロセスとの一致

アクションを実行しようとしたファイルやプロセスがカスタム ルールに一致するかどうかを確認するために、ファイル名またはプロセス名で使用されている文字列と、ルール内で指定されている条件の文字列との間で比較が行われます。ハッシュ値はカスタム ルールの処理では使用されません。

パスやプロセスの指定にワイルドカードや特定のマクロを含めるとルールの適用範囲を拡張でき、エージェント コンピューターごとに異なる場所にあるファイルやプロセスに対してもルールを適用できるようになります。詳細については、「パスとプロセスの指定」（420 ページ）を参照してください。

事前構成済みのルール

Bit9 Server の新規インストールを実行すると、パフォーマンスを向上させたり、不要な追跡処理を避けるために、事前構成済みのさまざまなカスタム ルールが作成されます。これらのルールはデフォルトで有効になっています。これらのルールは必要に応じて削除または無効化できます。Bit9 Security Platform をアップグレードした場合、これらのルールは既存のルールの下に（既存ルールよりも下位のランクに）追加されます。

ルールのテーブルには［**Sample**（サンプル）］と書かれたルールも含まれ、これらのルールはデフォルトで無効になっています。これらのルールの大部分はアプリケーション固有のルールで、一般的なアプリケーションやスイートで必要とされるファイルの実行や書き込みを許可することを目的としています。これらのルールはそのまま有効にすることも、カスタマイズしてから有効にすることもできます。

［Custom Rules（カスタム ルール）］テーブルに表示される内部ルール

［Custom Rules（カスタム ルール）］テーブルには［Internal（内部）］と書かれたルールが含まれています。これらのルールはコンソールの別の部分（［Edit Policy（ポリシーの編集）］ページの［Device Settings（デバイス設定）］や［Advanced Settings（高度な設定）］など）で有効にできます。たとえば、ポリシーの［Advanced Settings（高度な設定）］テーブルに表示される［Block banned file hashes（禁止ファイル ハッシュをブロック）］は［Custom Rules（カスタム ルール）］ページに内部ルールとして表示されます。

いずれかのポリシーで有効になっている内部ルールのステータスは、ルール テーブル内で［Enabled（有効）］と表示されます。［Custom Rules（カスタム ルール）］テーブルで内部ルールを有効化、無効化、変更、移動することはできませんが、内部ルール以外のその他のカスタム ルールを内部ルールよりも上位または下位に移動することにより各ルールの優先順位を調整することは可能です。詳細については、「ルールのランキングと内部ルール」（438 ページ）を参照してください。

すべてのプラットフォームに適用されるカスタム ルールは内部ルールのみです。

カスタム ルールの通知の指定

Bit9 Security Platform には、ルールによってアクションがブロックされた場合、またはアクションを許可するかブロックするかの選択をユーザーに促す場合に通知を表示する機能があります。カスタム ルールごとに、次の 2 種類の通知ソースからいずれかを選択できます。

- ［**Use Policy Specific Notifier**（ポリシー固有の通知を使用）］– 各ポリシーの［Advanced Setting（高度な設定）］には［Enable custom (file and path) rules（カスタム（ファイルおよびパス）ルールを有効化）］が含まれ、この項目は常にオンになっています。このポリシー設定の［Notifier（通知）］フィールドでは、カスタム ルールによってアクションがブロックされたときにエージェント コンピューターに表示する通知を指定できます。また、このポリシー設定で［<none>（なし）］を選択すると、そのポリシーでカスタム ルールの通知を表示しないようにすることができます。ポリシー固有のカスタム ルール通知はすべてのカスタム ルールに割り当てることができます。詳細については、「高度な設定」（189 ページ）を参照してください。
- ［**Custom Notifier**（カスタム通知）］– ポリシー固有の通知を使用しない場合は、カスタム ルールごとに通知を選択（または作成）できます。選択肢は、［Add/Edit Custom Rule（カスタム ルールの追加 / 編集）］ページのメニューに表示されます。

カスタム ルール通知の設定については、下記の表 47 を参照してください。通知の詳細については、第 17 章「ブロック通知と承認要求」を参照してください。

ルール アクションとして［Prompt（プロンプト）］を選択した場合、プロンプト ルールは通知を表示する必要があるため、［Custom Notifier（カスタム通知）］メニューのオプションに［<none>（なし）］は表示されません。

ブロック ルールの場合は通知を表示せずにアクションをブロックすることもできるため、ルール アクションとして［Block（ブロック）］を選択した場合は［Custom Write Notifier（カスタム書き込み通知）］メニューから［<none>（なし）］を選択できます。

ルールの設定で［Use Policy Specific Notifier（ポリシー固有の通知を使用）］を選択する場合は、［Enforce custom (file and path) rules（カスタム（ファイルおよびパス）ルールを適用）］に関する通知として［<none>（なし）］をポリシーで指定できます。これを指定すると、プロンプト ルールに対しても通知は表示されなくなります。ルールの動作に関してユーザーに選択を促す必要がまったくない場合を除き、ポリシーのカスタム ルール通知として［<none>（なし）］を選択することは推奨されません。

可視性モードのカスタム ルール

可視性モード ポリシーの場合、カスタム ルールの効果はルールの種類によって異なります。

- 可視性モードの場合、ファイルをブロックするように設定されたカスタム ルールが条件に一致すると Bit9 イベントが生成されますが、実際の効果は現れません。
- 可視性モードの場合、ファイルを承認するように設定されたカスタム ルールが条件に一致するとファイル状態が変更されますが、ファイルの実行には影響しません。
- ［Write（書き込み）］メニューで［Ignore（無視）］が指定されているカスタム ルール（下記を参照）は可視性モードでも通常どおりに適用されます。

カスタム ルールの作成

カスタム ルールを一から作成するには、左の列に太字で表示されている情報を入力する必要があります。

概要	［Add/Edit Custom Rule（カスタム ルールの追加 / 編集）］ページのフィールド
この（これらの）ソース プロセス …	［Process（プロセス）］
… および / または**この（これらの）ユーザー**が …	［User or Group（ユーザーまたはグループ）］
… **この（これらの）操作**を …	［Operation（操作）］（［Execute（実行）］、［Write（書き込み）］、または両方）
… **この（これらの）ファイル**に対して …	［Path or File（パスまたはファイル）］
… **この（これらの）ポリシー**に含まれるコンピューター上で …	［Rule applies to:（ルールの適用先：）］
… **このプラットフォーム**上で稼働しているコンピューター上で実行しようと試みた場合 …	［Platform（プラットフォーム）］
… **この（これらの）アクション**を適用します。	［Execute Action（実行アクション）］および / または［Write Action（書き込みアクション）］

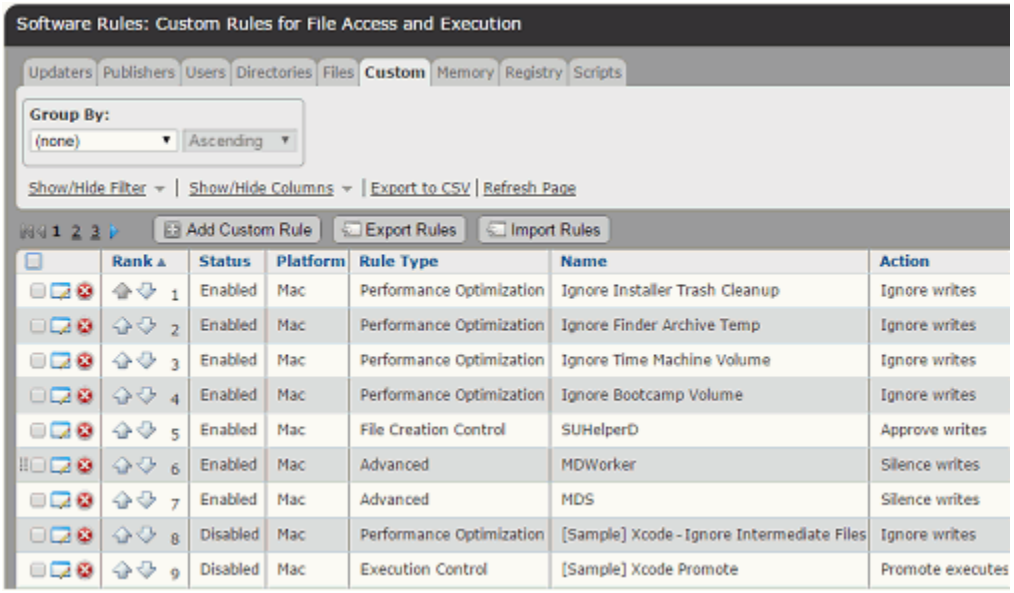
プラットフォーム以外のパラメーターでは複数の項目を指定でき、そのクラスに含まれるすべての項目を指定することもできます（たとえば、すべてのユーザー、すべてのポリシー、またはすべてのソース プロセスにルールを適用できます）。また、上記の説明とは逆に、指定と異なるプロセスがアクションを試みた場合や、指定と異なるファイルに対してアクションが試みられた場合にルールを適用するように指定することもできます。

［Add Custom Rule（カスタム ルールの追加）］ページで［Rule Type（ルール タイプ）］を選択するとその他のパラメーターが自動的に変更されるため、ルールを定義するためにすべての情報を指定しなくてもよい場合があります。

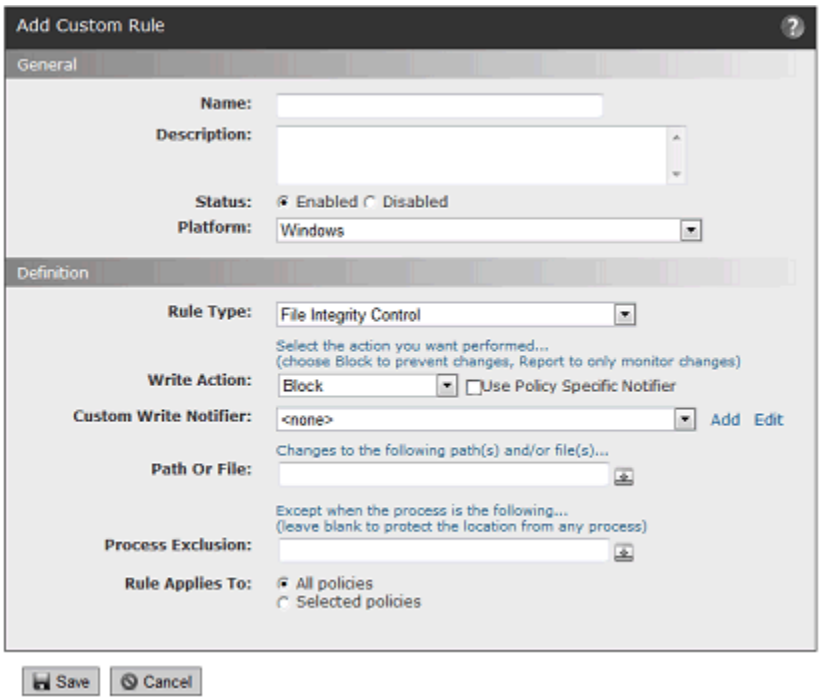
- 選択したルール タイプに関係しないフィールドや、有効な値が 1 つしかないフィールドはページ上に表示されません。
- また、選択したルール タイプに関係しないメニュー オプションも表示されません。
- ［Add Custom Rule（カスタム ルールの追加）］ページで設定可能な各フィールドのインライン ヘルプ テキストは、そのルール タイプに適した値を選択できるように自動的に変更されます。

カスタム ルールの追加（作成）手順：

1. コンソール メニューで、［**Rules**（ルール）］>［**Software Rules**（ソフトウェア ルール）］の順に選択します。［Software Rules（ソフトウェア ルール）］ページが表示されます。
2. ［Software Rules（ソフトウェア ルール）］ページで［**Custom**（カスタム）］タブをクリックします。［Custom Rules（カスタム ルール）］テーブルが表示されます。



3. ［**Add Custom Rule**（カスタム ルールの追加）］ボタンをクリックします。［Add Custom Rule（カスタム ルールの追加）］ページが表示されます。



4. ［Name（名前）］フィールドにこのルールを識別するための名前を入力します。
5. ルールの目的や他のルールとの関係など、ルールに関するコメントを追加する場合は、［Description（説明）］を入力することもできます。
6. デフォルトでは、新しいカスタム ルールを定義して［**Save**（保存）］をクリックすると、そのカスタム ルールのステータスは［**Enabled**（有効）］になります。作成したルールを後で適用する場合は、［Status（ステータス）］フィールドで［**Disabled**（無効）］をクリックします。
7. メニューからルール　タイプを選択します。デフォルトでは［File　Integrity Control（ファイル整合性の制御）］が選択されていますが、一部設定済みのルール タイプがその他にもいくつか用意されています。目的に合ったルール タイプが表示されていない場合は、［Rule Type（ルール タイプ）］メニューで［**Advanced**（詳細）］を選択すると、最も多くの設定オプションが表示されます。表 47 で、各ルール タイプとその他のカスタム ルール パラメーターについて説明します。
8. このカスタム ルールに必要なその他のパラメーター（表 47 を参照）を入力して、［**Save**（保存）］をクリックします。新しく作成されたルールが［Custom Rules（カスタム ルール）］テーブルの先頭に表示されます。
9. このルールを最優先しない場合は、［Rank（ランク）］列の矢印を使用して適切なランクに下げます。詳細については、「ルールのランキング」（436 ページ）を参照してください。

カスタム ルールのパラメーター

表 47 に、[Add/Edit Custom Rule（カスタム ルールの追加 / 編集）] ページで設定可能なパラメーターを示します。

表 47：カスタム ルールのパラメーター

フィールド	説明
[Name（名前）]	このルールを識別するための名前。（必須）
[Description（説明）]	カスタム ルールに関する追加情報。任意のテキストを入力できます。（オプション）
[Status（ステータス）]	このルールを有効または無効にするラジオ ボタン。これらのラジオ ボタンを使用することで、特定の場合にのみ使用するルールを作成したり、定義を維持したままルールを一時的に無効にしたりできます。
[Platform（プラットフォーム）]	このルールが適用されるプラットフォーム（Windows、Mac、または Linux）。あらかじめ組み込まれている「内部」ルールを除き、カスタム ルールは1種類のプラットフォームのみに適用されます。
[Rule Type（ルール タイプ）]	ルール タイプを選択すると、[Add/Edit Custom Rule（カスタム ルールの追加 / 編集）] ページにあるその他のオプションやデフォルト値が変更され、一般的なシナリオに合わせてルールの一部が事前に構成されます。ルール タイプのオプションには、[**File Integrity Control**（ファイル整合性の制御）]、[**Trusted Path**（信頼済みパス）]、[**Execution Control**（実行の制御）]、[**File Creation Control**（ファイル作成の制御）]、[**Performance Optimization**（パフォーマンスの最適化）]、[**Advanced**（詳細）] があります。詳細と例については、「カスタム ルールの種類と例」（449 ページ）を参照してください。
[Operation（操作）]	ルールを適用する操作の種類。このメニューのオプションには、[**Execute**（実行）]、[**Write**（書き込み）]、および [**Execute and Write**（実行と書き込み）] があります。
[Execute Action（実行アクション）]	このルールに一致するファイルの実行が試みられた場合に適用するアクション。このメニューは [Operation（操作）] フィールドで [Execute（実行）] または [Execute and Write（実行と書き込み）] が選択されている場合にのみ表示されます。このメニューのオプションについては、表 48 を参照してください。
[Write Action（書き込みアクション）]	このルールに一致するファイルの作成、変更、または削除が試みられた場合に適用するアクション。このメニューは [Operation（操作）] フィールドで [Write（書き込み）] または [Execute and Write（実行と書き込み）] が選択されている場合にのみ表示されます。このメニューのオプションについては、表 49 を参照してください。

フィールド	説明
[Use Policy Specific Notifier（ポリシー固有の通知を使用）]	[Action（アクション）] として [Block（ブロック）] または [Prompt（プロンプト）] を選択した場合は、このチェックボックスが [Action（アクション）] オプションの右に表示され、デフォルトでオンになります。このチェックボックスがオンになっている場合、カスタム ルールによってアクションがブロックされたときに表示される通知は、アクションがブロックされたコンピューターのポリシーの [カスタム（ファイルおよびパス）ルールを有効化)] 設定で指定されている通知と同じになります。このチェックボックスがオフになっている場合は、[Custom Notifier（カスタム通知）] メニューからカスタム通知を選択できます。
[Custom Execute/Write Notifier（カスタム実行 / 書き込み通知）]	このメニューは、[Action（アクション）] として [Block（ブロック）] または [Prompt（プロンプト）] を選択し、[Use Policy Specific Notifier（ポリシー固有の通知を使用）] チェックボックスがオンになっている場合にのみ表示されます。 [Action（アクション）] として [Block（ブロック）] を選択した場合は、このメニューから通知を選択できます。このメニューには [<none>（なし）] オプションも表示され、このオプションを選択するとこのルールに関する通知が無効になります。 [Action（アクション）] として [Prompt（プロンプト）] を選択した場合は、このメニューから通知を選択できます。ただし、プロンプトを表示するように設定されたルールの場合は必ず通知を表示する必要があるため、[<none>（なし）] オプションは表示されません。
[Path or File（パスまたはファイル）]	このルールを適用するパス。ここではフォルダーまたは特定のファイルを指定できます。ローカル パスまたは UNC パスを指定できますが、マップされたドライブ（Z:\application など）は指定できません。パスを指定する方法の詳細については、「パスとプロセスの指定」（420 ページ）を参照してください。
[Process（プロセス）]	このメニューを使用すると、指定したパスに一致するファイルの実行または書き込みが特定のプロセスによって試みられた場合にのみルールを適用できます。プロセスを指定する方法については、「パスとプロセスの指定」（420 ページ）を参照してください。プロセス メニューのオプションについては、表 52 を参照してください。
[User or Group（ユーザーまたはグループ）]	このルールを適用するユーザーまたはグループ。ユーザーまたはグループを指定する方法については、「ユーザーまたはグループの指定」（435 ページ）を参照してください。
[Rule applies to（ルールの適用先）]	ラジオ ボタンを使用して、ルールを [**All policies**（すべてのポリシー）] に適用するか、[**Selected policies**（選択されたポリシー）] のみに適用するかを選択できます。[**Selected policies**（選択されたポリシー）] を選択すると、Bit9 Server 上の各ポリシーがチェックボックスとともに表示されます。
[History（履歴）]	既存ルールの場合は [History（履歴）] パネルが表示され、ルールの作成日、作成者、最終更新日、最終更新者が表示されます。

実行アクションおよび書き込みアクションの指定

カスタム ルールで制御できるアクションには 2 種類あります。実行アクションと書き込みアクションです。

実行アクションはルールに一致するファイルの実行が試みられたときに適用されるアクションです。[Execute Action（実行アクション）] メニューは［Operation（操作）］フィールドで［Execute（実行）］または［Execute and Write（実行と書き込み）］が選択されている場合にのみ表示されます。表 48 に、このメニューのオプションを示します。

表 48：[Execute Action（実行アクション）] のオプション

メニュー オプション	説明
[Default（デフォルト）]	このルールに一致するファイルの実行が試みられた場合、既存のポリシー設定と他の非カスタム ルールを適用し、その他のカスタム ルールを処理しません。
[Allow（許可）]	ルールに一致するファイルの実行が指定されたパスで試みられた場合、（他のルールで禁止されている場合でも）実行を許可します。 **注意**：昇格状態（ファイルがインストーラーとして処理されるかどうか）は、アクションを試みたプロセスに応じて決定されます（アクションを試みたプロセスが昇格されている場合は、新たに作成されたプロセスも昇格されます）。
[Block（ブロック）]	ルールに一致するファイルの実行をブロックします。 [Block（ブロック）] が選択されている場合は、[Use Policy Specific Notifier（ポリシー固有の通知を使用）] チェックボックスが表示され、デフォルトでオンになります。このチェックボックスをオフにすると、ルールによってアクションがブロックされたときにユーザーに表示されるカスタム通知を無効にすることができます。詳細については、表 47 を参照してください。
[Promote（昇格）]	このルールに一致するファイルを昇格させます（インストーラーとして処理します）。ファイルが昇格されている場合でも、そのファイルを実行できるかどうかは既存のファイル状態と実行が試みられたマシンの適用レベルに基づいて決定されます。ファイルの実行が許可された場合、そのファイルによって書き込まれたファイルは既に禁止されていない限りローカルで承認され、書き込みを行ったプロセスがそれらのファイルの実行を試みた場合は書き込まれたファイルも昇格されます。
[Allow and Promote（許可と昇格）]	ファイルの状態にかかわらず、[Path or File（パスまたはファイル）] の指定と一致するファイルの実行を許可し、そのファイルを昇格させます（インストーラーとして処理します）。[Allow and Promote（許可と昇格）] ルールに一致するファイルによって書き込まれたファイルは、既に禁止されていない限りローカルで承認されます。ファイルの実行をパス名に基づいて信頼する方法については、「[Trusted Paths（信頼済みパス）]」を参照してください。

メニュー オプション	説明
[Prompt（プロンプト）]	このルールに一致するファイルの実行が試みられたときに、ユーザーに通知ダイアログを表示します。 [Prompt（プロンプト）] が選択されている場合は、[Use Policy Specific Notifier（ポリシー固有の通知を使用）] チェックボックスが表示され、デフォルトでオンになります。このチェックボックスをオフにすると、ルールによってアクションがブロックされたときにユーザーに表示されるカスタム通知を無効にすることができます。詳細については、表 47 を参照してください。 ユーザーは、実行をブロックするか、実行を許可するか（許可された場合、そのファイルはローカルで承認されます）、ファイルを昇格させるか（さらに実行を許可するか）を選択できます。ユーザーの選択に基づいて実行される動作は、ルール自体で [Block（ブロック）]、[Allow（許可）]、または [Allow and Promote（許可と昇格）] が指定されている場合の動作と同じです。ユーザーが [Allow（許可）] または [Promote（昇格）] を選択した場合、以降に同じアクションが試みられると、プロンプトを表示せずに許可または昇格されます。 **注意**：カスタム ルールのプロンプトから実行がブロックまたは許可されても、グローバルな承認または禁止状態には影響しません。
[Report（レポート）]	ファイルの状態にかかわらず、このルールに一致するファイルの実行を（イベントとして）レポートします。
[Report Process Create（プロセスの作成をレポート）]	このルールで指定されているファイルとパスに一致し、ルールで指定されているプロセスによって開始されたプロセスの作成を（イベントとして）レポートします。
[Block Silently（サイレント ブロック）]	実行の条件がこのルールに一致する場合にファイルの実行をブロックします。通知は表示されず、Bit9 イベントも生成されません。
[Report Process Exit（プロセスの終了をレポート）]	このルールで指定されているファイルとパスに一致し、ルールで指定されているプロセスによって開始されたプロセスの終了を（イベントとして）レポートします。
[Report Image Load（イメージのロードをレポート）]	このルールで指定されているファイルとパスに一致するDLLまたは EXE が、ルールで指定されているプロセスによってロードされたときに（イベントとして）レポートします。

書き込みアクションは、ルールに一致するファイルの作成、変更、または削除が試みられたときに適用されるアクションです。[Write Action（書き込みアクション）] メニューは [Operation（操作）] フィールドで [Write（書き込み）] または [Execute and Write（実行と書き込み）] が選択されている場合に、[Add/Edit Custom Rule（カスタム ルールの追加 / 編集）] ページに表示されます。表 49 に、このメニューのオプションを示します。

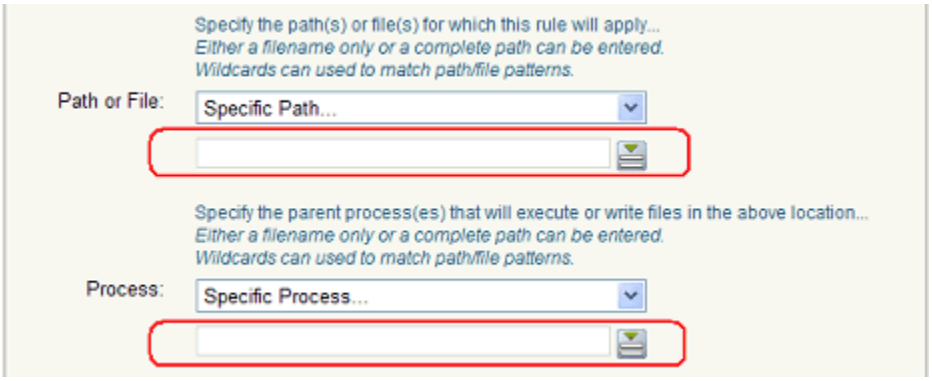
表 49：[Write Action（書き込みアクション）] のオプション

メニュー オプション	説明
[Silence（サイレンス）]	このルールとその他のルール（システムに組み込み済みのルールやユーザーが作成したルール）に一致するアクションが試みられた場合、他のルールの実行を妨げることなく、通知、メーター、およびイベントの生成をブロックします。通常はプロンプト（許可するかブロックするかを尋ねる）通知が表示されるアクションがサイレンス ルールと一致した場合、そのアクションはブロックされます。このオプションはルール タイプとして［Advanced（詳細）］が選択されている場合にのみ表示されます。
[Default（デフォルト）]	このルールに一致するファイルの書き込みが試みられたときに既存のポリシー設定と非カスタム ルールを適用します。このルールに一致したファイルに関しては、他のカスタム ルールは処理されません。
[Ignore（無視）]	このルールに一致するファイルの作成、変更、または削除の追跡を無効にします。無視ルールに一致するファイルは追跡の対象から除外されますが、ファイルの状態や適用レベルに基づいてブロックが適用された場合、ファイルの書き込みはブロックされます。 ［Ignore（無視）］を選択してもルールの処理は停止されません。無視ルールと下位にランクされた別のルールに一致する書き込み操作が試みられた場合は、2 番目に一致したルールが処理されます。
[Track（追跡）]	このルールに一致するファイルの作成、変更、または削除を追跡します。このアクションを使用すると無視ルールに対する例外を作成できます。このオプションはルール タイプとして［Advanced（詳細）］が選択されている場合にのみ表示されます。
[Block（ブロック）]	このルールに一致するファイルの書き込みをブロックします。このオプションを選択した場合は、ファイルの作成、削除、および変更がブロックされます。 ［Block（ブロック）］が選択されている場合は、［Use Policy Specific Notifier（ポリシー固有の通知を使用）］チェックボックスが表示され、デフォルトでオンになります。このチェックボックスをオフにすると、ルールによってアクションがブロックされたときにユーザーに表示されるカスタム通知を無効にすることができます。詳細については、表 47 を参照してください。
[Approve（承認）]	このルールに一致するファイルの作成（書き込み）を許可し、可能な場合は（グローバルにまたはポリシーで禁止されていない場合は）ローカルでそのファイルを承認します。

メニュー オプション	説明
[Approve as Installer（インストーラーとして承認）]	このルールに一致するファイルの作成（書き込み）を指定されたディレクトリ内で許可し、可能な場合は（グローバルにまたはポリシーで禁止されていない場合は）そのファイルをローカルで承認し、インストーラーとしてマークします。 **注意**：カスタム ルールによって適用される［Approve as Installer（インストーラーとして承認）］アクションは、あくまでもローカルで一時的に適用されるアクションです。このアクションは同じファイルの別インスタンスには適用されず、そのファイルがグローバルに「インストーラー以外」としてマークされている場合は初期状態が上書きされているため、このインスンタンスに対しても適用されません。このルールは、Bit9 による初期分析の結果「インストーラー以外」としてマークされたファイルに対して適用されます。 このオプションを選択した場合、ファイル ハッシュは確認されず、名前のみに基づいてファイルがインストーラーとして承認されるため、このオプションを使用する場合は注意が必要です。
[Prompt（プロンプト）]	ルールに一致するファイルの書き込みを試みたユーザーに対して、書き込みをブロックするか許可するかを尋ねる通知が表示されます。 ［Prompt（プロンプト）］が選択されている場合は、［Use Policy Specific Notifier（ポリシー固有の通知を使用）］チェックボックスが表示され、デフォルトでオンになります。このチェックボックスをオフにすると、ルールによってアクションがブロックされたときにユーザーに表示されるカスタム通知を無効にすることができます。詳細については、表 47 を参照してください。 ユーザーが通知から［Approve（承認）］を選択した場合はファイルの書き込みが行われ、実行可能ファイルの場合は承認されます。以後、同じ操作（ルールに一致する別のファイルではなく、同じパスにある同一ファイルに対する操作）が試みられた場合はプロンプトなしで承認されます。ただし、ファイルを実行できるかどうかは引き続き、名前またはハッシュに基づくグローバルな禁止の設定に基づいて制御されます。
[Allow（許可）]	このルールに一致するファイルの作成、変更、または削除を許可します。この選択は書き込まれるファイルの状態には影響しません。
[Report（レポート）]	通常は Bit9 Server で追跡されないファイルも含め、このルールに一致したすべてのファイルの書き込みを（イベントとして）レポートします。これには実行可能ファイルとして分析されないファイルや、初めて検出されたハッシュのインスタンスではないファイルも含まれます。
[Never Report（レポートしない）]	このルールに一致するアクションをサーバーにレポートしません。アクションの記録は引き続きエージェント上で保持されます。

パスとプロセスの指定

カスタム ルールで［Path or File（パスまたはファイル）］を指定する場合は、パラメーターの文字列を定義するためのオプションがいくつかあります。これらのオプションは、パスの入力を必要とする 2 つのプロセス オプション（［Specific Process…（特定のプロセス）］または［Any Process Except…（以下を除くすべてのプロセス …）］）を選択した場合にも使用できます。



これらのオプションには以下のものがあります。

- **ディレクトリまたはファイル/プロセスを指定** – 特定のファイルのみがルールに一致するように、そのファイルを厳密に識別するパスまたはプロセスを入力できます。ディレクトリを指定した場合は、そのディレクトリとサブディレクトリ内にあるすべてのファイルとプロセスにルールが適用されます。
- **ローカル ドライブまたは UNC パスを指定（Windows のみ）** – *C:\folder1\subfolder\application.exe* のようにローカル ドライブ名を使用してローカルのパスまたはプロセスを指定できます。リモートのパスやプロセスを指定する場合は *\\computer\dir\application.exe* のように UNC パスを使用します。マップされたドライブがパスまたはプロセスの指定で使用されている場合は正しく認識されません。
- **ワイルドカードを使用** – ワイルドカード（任意の 1 文字を表す「?」と 0 個以上の文字を表す「*」）を使用することにより、パスまたはプロセスの指定範囲を広げたり、正確な場所が分からないファイルやフォルダーにも一致するルールを作成できます。ワイルドカードはパスの先頭、末尾、または中間で使用できます。
- **マクロを使用** – エージェント コンピューター上の正確な場所が分からない場合でも、特別なマクロを使用することにより、特定の既知のフォルダーを指定できます。マクロはプラットフォーム固有であり、現在のリリースでは Windows に対してのみ使用できます。
- **複数のパスまたはプロセスを指定** – 1 つのルールに複数のパスやプロセスを追加できます。

ファイルまたはディレクトリの指定

パスの指定では、ディレクトリまたは特定のファイルを入力できます。ディレクトリを指定した場合は、そのディレクトリとサブディレクトリ内にあるすべてのファイルにルールが適用されます（ただし、上位にランクされた別のルールが特定のファイルやサブディレクトリに一致した場合は除く）。

［Path or File（パスまたはファイル）］または［Process（プロセス）］の定義がディレクトリであることを示すには、定義の末尾にルール プラットフォームで使用されるフォルダー区切り文字（スラッシュまたは円記号）を付けるか、区切り文字とアスタリスクを付けます。区切り文字を付けないと、ディレクトリではなく、指定された名前を持つファイルがルールの適用対象と見なされます。たとえば、Windows のパスを定義する場合は、次のいずれかの形式を使用して、ルールの適用対象がディレクトリであることを示します。

```
c:\folder1\subfolder2\
c:\folder1\subfolder2\*
```

一方、次の形式はディレクトリとして認識されません。

```
c:\folder1\subfolder2
```

パスまたはプロセスの定義でパス マクロを使用する場合は、マクロの後に円記号を付けなくても Bit9 Server は自動的にディレクトリとして処理します。「ルールでのマクロの使用」を参照してください。

プラットフォーム固有の構文

ルールで指定されているパスは、そのルールで選択されたプラットフォームでのパス ルールに従って解釈されます。具体的には、次のように解釈されます。

- ルール内のパスやファイル名で大文字と小文字が区別されるかどうかはオペレーティング システムによって異なります。通常、Mac と Windows では大文字と小文字が区別されないのに対して、Linux では大文字と小文字が区別されます。ただし、大文字 / 小文字の識別方法が異なるファイル システムがコンピューターに接続されている場合（たとえば、外付けドライブが接続されている場合や、ネットワーク上のファイル システムがマウントされている場合）は、ファイル システムの大文字 / 小文字識別方法に基づいてルールが有効かどうかが決定されます。
- 大文字 / 小文字が区別されないプラットフォームであっても、パスやファイル名の大文字 / 小文字は入力されたとおりに維持されます。
- パスの指定では、ルールの適用対象となるプラットフォームのディレクトリ区切り文字を使用する必要があります。Mac と Linux ではスラッシュ (/) を使用し、Windows では円記号 (\) を使用します。ルールの適用対象となるプラットフォームが変更された場合、区切り文字は自動的に変換されませんが、正しくない区切り文字はルールに入力できません。
- その他にも、パスの指定では、ファイル システムで禁止されている文字を使用しないなど、選択したプラットフォームの要件が満たされていることを確認する必要があります（たとえば、Mac のパスではコロン (:) を使用できません）。
- パスで使用されているマクロは、ルールの適用対象となるプラットフォームに固有のものである必要があります。現在のところ、マクロを使用できるのは Windows プラットフォームに対してのみです。

ルールでのワイルドカードの使用

［Path（パス）］および［Process（プロセス）］フィールドではワイルドカード文字を使用できます。アスタリスク (*) は 0 個以上の文字を表し、疑問符 (?) は任意の 1 文字を表します。ワイルドカードを使用すると、複数のコンピュータ上で複数

の場所に存在するディレクトリのパスを部分的に指定したり、複数のパスを指定することができます（ただし、マクロのほうが同じ目的をより効果的に達成できることもあります。「ルールでのマクロの使用」を参照してください）。マクロ内ではワイルドカードを使用できません。

パスまたはプロセスの指定で使用できるワイルドカードの数に制限はありません。たとえば、次のようにパスを指定できます。

```
*\Win*\folder?\
```

警告

ワイルドカードを使用するとルールの適用範囲が広くなりすぎ、他のアプリケーションやオペレーティング システムによる正常な動作に必要なディレクトリ内のアクティビティにも影響する可能性があるため注意が必要です。エージェント コンピューター上で必要な操作に影響しないことが分かっている場合を除き、パス フィールドでアクタリスク ワイルドカードを単独で使用しないようにしてください（特に、実行や書き込みをすべてブロックするルールを作成する場合）。また、他のルールによって作成された制約に対する例外を作成する場合も同様の注意をもってワイルドカードを使用してください。

自動パス変換

プロセス フィールドのファイル パスに特定の記号が含まれている場合は、ルールを処理する際に自動パス変換が次のように実行されます。

- 円記号で終わるパス (Windows) またはスラッシュで終わるパス（Mac および Linux）の末尾にはワイルドカード文字の「*」が追加されます。
- スラッシュまたはドライブ文字を含まないパスの先頭には「*\」（Windows の場合）または「*/」（Mac および Linux の場合）が追加されます。
- Windowsルールでは、ローカルの固定ボリュームを表している場合に限りパスの指定でドライブ文字を使用できます。マップされたボリュームに割り当てられたドライブ文字は、すべてのコンピューターで同じマッピングになっていない可能性があるため使用できません。
- Windows ルールの場合、「*:\」は、接続されているすべてのストレージ ボリューム（フロッピー ディスクと CD-ROM を除く）を表します。

Windows ルールのパスでのデバイスの指定

Windows ルールでは、パスの指定に *\device* を含めることで、エージェント コンピューター上の一部のデバイスまたはすべてのデバイス上のプロセスに適用されるルールを作成できます。以下に例を示します。

\device* はすべてのデバイスを表します。

\device\harddisk* は、コンピューターに接続されているすべてのストレージ ボリューム（フロッピー ディスクと CD-ROM を除く）を表します。

\device\cdrom* は CD-ROM デバイスを表します。

プラットフォームに関する注意：現在のリリースでは、デバイスの可視性および制御機能は Windows コンピューターに対してのみ使用できます。

ルールでのマクロの使用

カスタム ルールの［Path（パス）］および［Process（プロセス）］フィールドでは特定のマクロがサポートされています。これらのフィールドで左山括弧 (<) 文字を入力するとマクロのメニューが表示されます。カスタム ルールでは次のマクロがサポートされていますが、その大部分はメモリ ルール、レジストリ ルール、スクリプト ルール、ファイル（名）による禁止など、他のルールでもサポートされています。

- **パス マクロ** – Windows の一般に知られているフォルダーのサブセットです(一部のパスは他のプラットフォームでも機能する場合があります)。これらのパスはすべて、特定のファイルではなく場所を表します。
- **OnlyIf マクロ** – 特定のルールを展開するための条件の指定に使用できるマクロです。
- **レジストリ マクロ** – Windows レジストリ内の文字列を指定するマクロです。

パス マクロとレジストリ マクロを使用すると、ルールの適用対象となるファイルがコンピューターごとに異なる場所に存在している場合でも、指定したプラットフォームを実行しているすべてのコンピューター上のパスを動的に指定するルールを効果的に定義できます。OnlyIf マクロは、ルールの適用対象を特定のコンピューターのみに制限する場合に役立ちます。無効なマクロを入力すると、コンソールにエラー メッセージが表示されます。

注意

パス マクロは、ルールの［Path or File（パスまたはファイル）］フィールドの先頭でのみ使用できます（パス マクロの前にその他の文字列を置くことはできません）。OnlyIf マクロとレジストリ マクロは、Windows ルールの［Path or File（パスまたはファイル）］フィールド内のどこでも使用できます。

ほとんどのマクロは Windows プラットフォーム専用です。

パス マクロ

パス マクロは一般に知られている Windows プラットフォーム フォルダーのサブセットに基づいています（CSIDLs は Vista より古いバージョンの Windows 用で、KNOWNFOLDERIDs は Vista 以降のバージョンの Windows 用です）。パス マクロは山括弧で囲まれた一意の文字列で構成されています。たとえば、Windows ルールで <MyDocuments> マクロを使用すると、各コンピューター上での実際の場所にかかわらず、各 Windows コンピューターの各ユーザーの My Documents フォルダーを指定できます。CSIDLs および KNOWNFOLDERIDs の詳細については、次のリンクを参照してください。

http://msdn.microsoft.com/en-us/library/windows/desktop/bb762494(v=vs.85).aspx

http://msdn.microsoft.com/en-us/library/windows/desktop/dd378457(v=vs.85).aspx

パス マクロは常にディレクトリを表すため、末尾にディレクトリ区切り文字（スラッシュまたは円記号）がない場合でも、末尾にディレクトリ区切り文字があるものとして処理されます。たとえば、Windows ルールに含まれる <AppData> は <AppData>\ と解釈されてから展開されるため、そのルールは Application Data ディ

レクトリとその中にあるすべてのファイル、サブディレクトリ、サブサブディレクトリなどに適用されます。同様に、<AppData>myapp\ は <AppData>\myapp\ と解釈されます。円記号を明示的に付けた場合、ルールの処理時に新たな円記号は追加されません。

マクロのメニューを表示するには、ルールの追加ページで［Path or File（パスまたはファイル）］ボックスまたは［Process（プロセス）］ボックスの 1 文字目に左山括弧 (<) を入力します。入力を進めると、選択したプラットフォーム上に存在し、それまでに入力した文字列に一致する選択肢のみが自動補完メニューに表示されます。表 50 に Windows ルールで使用できるパス マクロを示します。

この表の「ユーザー別」列は、ログインしているユーザーに基づいてマクロが展開されるかどうかを示しています。ユーザーがログインしてから、そのユーザーに適用されるルールが有効になるまでの間にはわずかな遅れがあり、その時間は設定されているルールの数や、ルールに含まれるマクロとグループ メンバーシップの展開にかかる時間によって異なります。そのため、ユーザー固有のマクロを含むルールや、ユーザーグループが指定されているルールは、ユーザーのログイン後すぐには適用されない可能性があります。

重要

ユーザーのログイン後にできるだけ早くルールを有効にする必要がある場合は、この表の「ユーザー別」列に「はい」と記載されているマクロをルール内で使用しないようにし、ユーザー グループも指定しないようにしてください。ユーザー名や SID が指定されているルールは常に有効で、この遅れによる影響を受けません。

表 50：Windows ルールで使用可能なパス マクロ

マクロ	ユーザー別	説明
<AppData>	はい	アプリケーション固有のデータの共通レポジトリとして機能するディレクトリ。このマクロは次の値にマッピングされます。 • CSIDL_APPDATA • FOLDERID_RoamingAppData
<CommonAppData>	いいえ	すべてのユーザーによって使用され、すべてのユーザーがアクセスできるアプリケーション データを格納するディレクトリ。このフォルダーは全ユーザーに共通するアプリケーション データを保存するために使用されます。たとえば、スペルチェック辞書、クリップ アートのデータベース、ログ ファイルなどがアプリケーションによってこの場所に保存されます。このマクロは次の値にマッピングされます。 • CSIDL_COMMON_APPDATA • FOLDERID_ProgramData

マクロ	ユーザー別	説明
<CommonDesktopDirectory>	いいえ	すべてのユーザーのデスクトップに表示されるファイルとフォルダーを格納するディレクトリ。このマクロは次の値にマッピングされます。 • CSIDL_COMMON_DESKTOPDIRECTORY • FOLDERID_PublicDesktop
<CommonDocuments>	いいえ	すべてのユーザーに共通するドキュメントを格納するディレクトリ。このマクロは次の値にマッピングされます。 • CSIDL_COMMON_DOCUMENTS • FOLDERID_PublicDocuments
<CommonPrograms>	いいえ	すべてのユーザーの［スタート］メニューに表示される共通のプログラム グループのフォルダーを格納するディレクトリ。このマクロは次の値にマッピングされます。 • CSIDL_COMMON_PROGRAMS • FOLDERID_CommonPrograms
<CommonStartMenu>	いいえ	すべてのユーザーの［スタート］メニューに表示されるプログラムとフォルダーを格納するディレクトリ。このマクロは次の値にマッピングされます。 • CSIDL_COMMON_STARTMENU • FOLDERID_CommonStartMenu
<CommonStartup>	いいえ	すべてのユーザーの［スタートアップ］フォルダーに表示されるプログラムを格納するディレクトリ。このマクロは次の値にマッピングされます。 • CSIDL_COMMON_STARTUP • FOLDERID_CommonStartup
<Cookies>	はい	インターネット Cookie の共通レポジトリとして機能するディレクトリ。このマクロは次の値にマッピングされます。 • CSIDL_COOKIES • FOLDERID_Cookies
<DesktopDirectory>	はい	（デスクトップ フォルダー自体ではなく）デスクトップ上のファイル オブジェクトを物理的に格納するために使用されるディレクトリ。 • CSIDL_DESKTOPDIRECTORY • FOLDERID_Desktop

マクロ	ユーザー別	説明
<InternetCache>	はい	インターネット一時ファイルの共通レポジトリとして機能するディレクトリ。このマクロは次の値にマッピングされます。 • CSIDL_INTERNET_CACHE • FOLDERID_InternetCache
<LocalAppData>	はい	ローカル（非ローミング）アプリケーションのデータレポジトリとして機能するディレクトリ。このマクロは次の値にマッピングされます。 • CSIDL_LOCAL_APPDATA • FOLDERID_LocalAppData
<MyDocuments>	はい	マイ ドキュメント フォルダーを表す仮想フォルダー。ユーザーのドキュメントの共通レポジトリを物理的に格納するために使用されるファイル システム ディレクトリ。このマクロは次の値にマッピングされます。 • CSIDL_PERSONAL • FOLDERID_Documents
<Profile>	はい	ユーザーのプロファイル フォルダー。このマクロは次の値にマッピングされます。 • CSIDL_PROFILE • FOLDERID_Profile
<ProgramFiles>	いいえ	Program Files フォルダー。このマクロは次の値にマッピングされます。 • CSIDL_PROGRAM_FILES • FOLDERID_ProgramFiles
<ProgramFilesx86>	いいえ	32 ビットの Program Files フォルダー。このマクロは次の値にマッピングされます。 • CSIDL_PROGRAM_FILESX86 • FOLDERID_ProgramFilesX86
<ProgramFilesCommon>	いいえ	アプリケーション間で共有されるコンポーネントのフォルダー。このマクロは次の値にマッピングされます。 • CSIDL_PROGRAM_FILES_COMMON • FOLDERID_ProgramFilesCommon
<ProgramFilesCommonx86>	いいえ	32 ビットの Program Files フォルダー。このマクロは次の値にマッピングされます。 • CSIDL_PROGRAM_FILES_COMMONX86 • FOLDERID_ProgramFilesCommonX86

マクロ	ユーザー別	説明
<Programs>	はい	ユーザーのプログラム グループを格納するディレクトリ（各プログラム グループ自体がファイル システム ディレクトリ）。このマクロは次の値にマッピングされます。 • CSIDL_PROGRAMS • FOLDERID_Programs
<RecycleBin>	はい	ごみ箱ディレクトリ。このディレクトリの場所はオペレーティング システムとファイル システムの種類によって異なります。このマクロは次の値にマッピングされます。 • CSIDL_BITBUCKET • FOLDERID_RecycleBinFolder
<StartMenu>	はい	［スタート］メニューの項目を格納するディレクトリ。このマクロは次の値にマッピングされます。 • CSIDL_STARTMENU • FOLDERID_StartMenu
<Startup>	はい	ユーザーのスタートアップ プログラム グループに対応するディレクトリ。このマクロは次の値にマッピングされます。 • CSIDL_STARTUP • FOLDERID_Startup
<System>	いいえ	Windows プラットフォーム固有の System フォルダー。このマクロは次の値にマッピングされます。 • CSIDL_SYSTEM • FOLDERID_System
<Systemx86>	いいえ	32 ビットおよび 64 ビット オペレーティング システムの両方に存在する 32 ビットの System フォルダー。このマクロを使用すると、32 ビット版のユーティリティのみにルールを適用できます。このマクロは次の値にマッピングされます。 • CSIDL_SYSTEMX86 • FOLDERID_SystemX86
<Windows>	いいえ	Windows ディレクトリまたは SYSROOT。これは %windir% 環境変数または %SYSTEMROOT% 環境変数に対応します。このマクロは次の値にマッピングされます。 • CSIDL_WINDOWS • FOLDERID_Windows

OnlyIf マクロ

［Custom Rules（カスタム ルール）］ページには、ルールの適用条件を指定するためのコントロール（特定のポリシーに含まれるコンピューターのみにルールの適用対象を制限するフィールドなど）が用意されています。OnlyIf マクロはこれらのユーザー インターフェイス コントロールを補足する機能であり、OnlyIf マクロを使用するとその他の条件もルール内で指定できます。

OnlyIf マクロはカスタム ルール、レジストリ ルール、メモリ ルール、スクリプト ルール、および（名前に基づく）ファイル ルールで使用できます。OnlyIf マクロはルール内でパスを指定するフィールドに入力できます。カスタム ルールの場合は、［Path or File（パスまたはファイル）］フィールドと［Process（プロセス）］フィールドがこれに該当します。

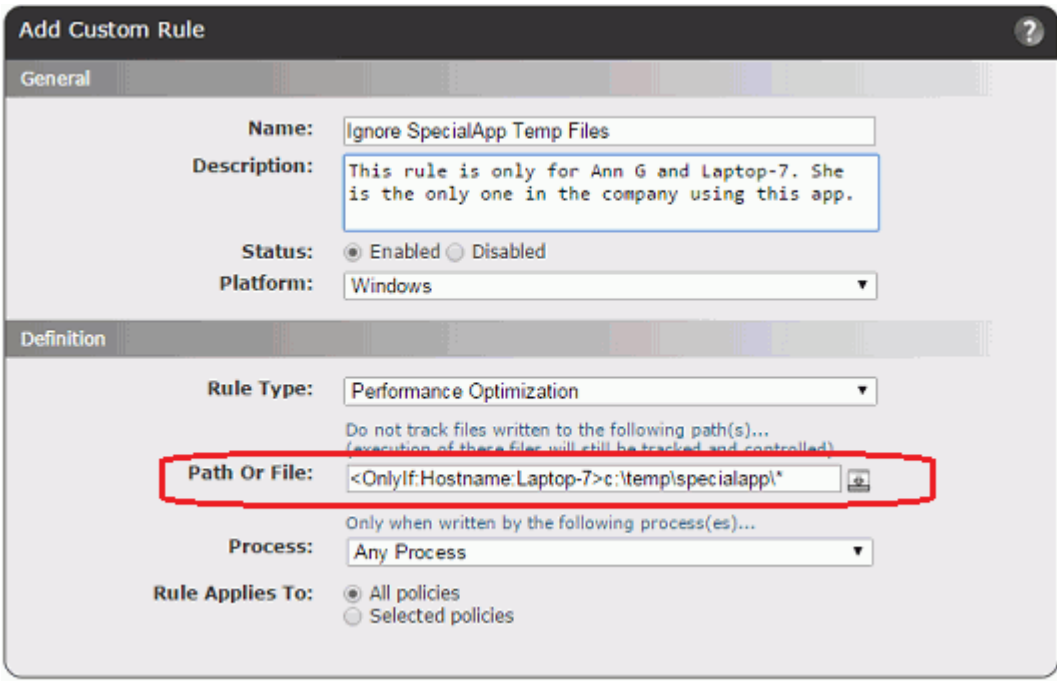
注意

OnlyIf マクロは v7.2.0 以降の Bit9 エージェントで機能します。以前のエージェントでは機能しません。

OnlyIf マクロの構文は次のとおりです。

<OnlyIf: 条件 : 値 **>**

たとえば、**<OnlyIf:Hostname:Laptop-7>** と指定されている場合は、アクションが試みられたシステムが Laptop-7 である場合にのみルールが適用されます。この指定はカスタム ルールの［Path or File（パスまたはファイル）］フィールドで行います。



パスとプロセスがそれぞれ 1 つずつ指定されているルールの場合は、どちらのフィールドで OnlyIf マクロを使用しても同じ結果になります。複数のパスまたは複数のプロセスが指定されているルールの場合は、OnlyIf マクロを使用するフィールドによって結果が異なる場合があります。たとえば、パスが 3 つ指定されていて、プロセスが 1 つだけ指定されているルールの場合、プロセス フィールドに OnlyIf 句を追加すると、すべてのパスにルールが適用されます。OnlyIf の条件を 1 つのパスのみに適用する必要がある場合は、該当するパスのフィールドのみに OnlyIf マクロを追加します。

Onlyif マクロで使用されるワイルドカード比較ロジックは、カスタム ルールのターゲット名またはプロセス名で使用される比較ロジックと同じです。マクロ内の大文字と小文字は区別されず、「*」と「?」をワイルドカードとして使用できます。

表 51 に OnlyIf マクロで使用できる条件と、それぞれの使用例を示します。

注意

特に記載がない限り、これらのマクロは Windows でのみサポートされます。

表 51：ルール内の OnlyIf マクロ

OnlyIf 条件	説明と例
ProductName	指定された名前を持つ製品がインストールされている場合にのみルールが展開されます。下の例では、ワイルドカード文字のアスタリスクを使用して、「Microsoft Office 2007」という文字列を含む製品名を指定しています。 **例**：<OnlyIf:ProductName:*Microsoft Office 2007*>
ProductCode	一致するGUIDを持つ製品がインストールされている場合にのみルールが展開されます。 **例**：<OnlyIf:ProductCode:{F1D61F7C-6E4C-4902-9278-0F93131BE2D2}> **注意**：マイクロソフトの製品コードについては、http://blogs.msdn.com/b/pusu/archive/2009/06/10/understanding-msi.aspx を参照してください。
UpgradeCode	指定されたアップグレード コードに一致する製品がインストールされている場合にのみルールが展開されます。 **例**：<OnlyIf:UpgradeCode:{F1D61F7C-6E4C-4902-9278-0F93131BE2D2}> **注意**：マイクロソフトのアップグレード コードについては、http://blogs.msdn.com/b/pusu/archive/2009/06/10/understanding-msi.aspx を参照してください。
PackageCode	指定されたパッケージ コードに一致する製品がインストールされている場合にのみルールが展開されます。 **例**：<OnlyIf:PackageCode:{F1D61F7C-6E4C-4902-9278-0F93131BE2D2}> **注意**：マイクロソフトのパッケージ コードについては、http://blogs.msdn.com/b/pusu/archive/2009/06/10/understanding-msi.aspx を参照してください。

OnlyIf 条件	説明と例
HostName	NETBIOS マシン名が指定された文字列と一致する場合にのみルールが展開されます。 **例**：<OnlyIf:HostName:*BSMITH-1*> **プラットフォームに関する注意**：この条件は Windows、Mac、および Linux エージェントに対して有効です。
DomainName	エージェント コンピューターが指定されたドメインに属している場合にのみルールが展開されます。 **例**：<OnlyIf:DomainName:*mycompany.local> **プラットフォームに関する注意**：この条件は Windows、Mac、および Linux エージェントに対して有効です。
HardwareManufacturer	コンピューターの製造元が指定された文字列と一致する場合にのみルールが展開されます。 **例**：<OnlyIf:HardwareManufacturer:*Dell*>
HardwareModel	コンピューターのモデルが指定された文字列と一致する場合にのみルールが展開されます。 **例**：<OnlyIf:HardwareModel:*XPS>
ServiceName	指定された文字列と一致する名前を持つサービスが存在する場合にのみルールが展開されます。 **例**：<OnlyIf:ServiceName:*Parity Server*>
ServiceDisplayName	指定された文字列と一致する表示名を持つサービスが存在する場合にのみルールが展開されます。 **例**：<OnlyIf:ServiceDisplayName:*Parity Server*>
Driver	指定されたドライバーがロードされている場合にのみルールが展開されます。 **例**：<OnlyIf:Driver:mfehidk>
Virtualized	エージェントが仮想マシン上で実行されている場合（値が 1 の場合）、またはエージェントが仮想マシン上で実行されていない場合（値が 0 の場合）にのみルールが展開されます。 **例**：<OnlyIf:Virtualized:1>
DEPSupported	このシステムで DEP がサポートされている場合（値が 1 の場合）、または DEP がサポートされていない場合（値が 0 の場合）にのみルールが展開されます。 **例**：<OnlyIf:DEPSupported:0>
RegKeyExists	指定されたレジストリ キーが存在する場合にのみルールが展開されます。 **例**：<OnlyIf:RegKeyExists:HKLM\Software\Foo>
RegValueExists	指定されたレジストリ値が存在する場合にのみルールが展開されます。 **例**：<OnlyIf:RegValueExists:HKLM\Software\Foo>
RegValueIs	指定されたキーに含まれるデータが指定されたパターンに一致する場合にのみルールが展開されます。この例では、Foo がキーに相当し、*Bar* がパターンに相当します。 **例**：<OnlyIf:RegValueIs:HKLM\Software\Foo:*Bar*>

OnlyIf 条件	説明と例
HostId	HostID が指定された値に一致するコンピューターに対してのみルールが展開されます。 **例**：<OnlyIf:HostId:5> **プラットフォームに関する注意**：この条件は Windows、Mac、および Linux エージェントに対して有効です。
FileExistsOnDisk	指定された名前を持つファイルがディスク上に存在する場合にのみルールが展開されます。Bit9 で追跡されているかどうかにかかわらず、ローカル システム ユーザーがアクセス可能なすべてのファイルを指定できます。下の例では、c:\windows\system32\foo.txt が存在する場合、d:\foo.exe を対象とするルールが作成されます。OnlyIf 句では完全なパスを指定する必要があります。 **例**：<OnlyIf:FileExistsOnDisk:<System>\foo.txt>d:\foo.exe
FileIsTracked	指定された名前を持つファイルが存在し、そのファイルが Bit9 エージェントによる追跡の対象になっている場合にのみルールが展開されます。完全なパスを指定する必要があります。 **例**：<OnlyIf:FileIsTracked:<System>\calc.exe>
HashExists	指定されたハッシュを持つファイルが存在し、そのファイルが Bit9 エージェントによる追跡の対象になっている場合にのみルールが展開されます。 **例**：<OnlyIf:HashExists:1c94cd9e3ee959ff6002eca3c5e7e7fdb9158657>
Bit9Version:Is	Bit9 エージェントのバージョンが指定されたバージョンと一致する場合にのみルールが展開されます。 **例**：<OnlyIf:Bit9Version:Is:7.2.0.233> **プラットフォームに関する注意**：この条件は Windows、Mac、および Linux エージェントに対して有効です。
Bit9Version:Atleast	Bit9 エージェントのバージョンが指定されたバージョン以上である場合にのみルールが展開されます。 **例**：<OnlyIf:Bit9Version:Atleast:7.2.0.233> **プラットフォームに関する注意**：この条件は Windows、Mac、および Linux エージェントに対して有効です。
Bit9Version:AtMost	Bit9 エージェントのバージョンが指定されたバージョン以下である場合にのみルールが展開されます。 **例**：<OnlyIf:Bit9Version:AtMost:7.2.0.233> **プラットフォームに関する注意**：この条件は Windows、Mac、および Linux エージェントに対して有効です。
OSVersionIs	エージェント システムのオペレーティング システム バージョン (major.minor.point) が指定されたバージョンと一致する場合にのみルールが展開されます。 **例**：<OnlyIf:OSVersionIs:10.6.8> **プラットフォームに関する注意**：この条件は Windows、Mac、および Linux エージェントに対して有効です。

OnlyIf 条件	説明と例
OSVersionAtleast	エージェント システムのオペレーティング システム バージョン (major.minor.point) が指定されたバージョン以上である場合にのみルールが展開されます。 **例**：<OnlyIf:OSVersionAtleast:10.6.8> **プラットフォームに関する注意**：この条件は Windows、Mac、および Linux エージェントに対して有効です。
OSVersionAtMost	エージェント システムのオペレーティング システム バージョン (major.minor.point) が指定されたバージョン以下である場合にのみルールが展開されます。 **例**：<OnlyIf:OSVersionAtMost:10.6.8> **プラットフォームに関する注意**：この条件は Windows、Mac、および Linux エージェントに対して有効です。
OSVersionString	エージェント システムのオペレーティング システムの詳細な説明が指定されたパターンと一致する場合にのみルールが展開されます。 **例**：<OnlyIf:OSVersionString:*Windows Server 2008*> **プラットフォームに関する注意**：この条件は Windows、Mac、および Linux エージェントに対して有効です。
ServerEdition	オペレーティング システムがサーバー エディションである場合（値が 1 の場合）、またはサーバー エディションでない場合（値が 0 の場合）にのみルールが展開されます。 **例**：<OnlyIf:ServerEdition:1>

Windows レジストリ マクロ

Windows ルールでは、パスまたはプロセスの指定でレジストリ (Reg) マクロを使用することにより、Windows レジストリの値を指定できます。パス マクロとは異なり、reg マクロの山括弧の間には変数の内容が入ります。reg マクロはキーではなく値を示している必要があります。

reg マクロの入力手順：

1. 最初に左山括弧 (<) を入力し、その直後に **Reg:** を入力します。
2. **<Reg:** の後に次のいずれかを入力します。
   a. **HKLM** (HKEY_LOCAL MACHINE を表します)
   b. **HKCU** (HKEY_CURRENT_USER を表します)
   c. **HKLM-SoftwareX86**
   d. **HKLM-SoftwareX64**
   e. **HKCU-SoftwareX86**
   f. **HKCU-SoftwareX64**
3. このルールを適用するパスの残り部分を入力します。キーではなく値を指定する必要があります。ただし、キーのデフォルト値を使用する場合のみ、キーを指定した後に円記号を入力します。

4. reg マクロには変数の内容が入るため、自動補完は行われません。マクロに入れるパスを完全に入力して、最後に右山括弧 (>) を入力する必要があります。完全なマクロは次のような形式になります（この例では HKLM を最上位のレジストリ ノードとして使用しています）。

   ```
   <Reg:HKLM\ 特定のパス >
   ```

reg マクロは各エージェントでそのルールが最初に利用可能になったときに評価されます。ルールがそのコンピューターに該当する場合は有効になります。たとえば、レジストリに書き込まれるパス値を使用して、「MyApp」というアプリケーションのアップデーターを昇格させるルールを作成した場合、MyApp のアップデーターがインストールされているシステムでは、<Reg:HKLM\Software\MyApp\Update\path> が C:\Program Files (x86)\MyApp\Update\MyAppUpdate.exe などに展開されます。この更新プログラムがインストールされていないシステムの場合、このルールは作成されません。

特定の状況が発生しない限り、reg マクロが使用されているルールが一度評価された後に再評価されることはありません。したがって、セッション中にレジストリが変更された場合、その変更によってルールが有効または無効になる可能性がある場合でも、ルールの動作には影響しません。エージェント上でルールの「再展開」が行われる状況は次のとおりです。

- エージェントが停止されて再起動された場合（コンピューターがシャットダウンされて再起動された場合など）
- 新しいユーザーがログインした場合
- 異なるルールを含むポリシーにエージェントが割り当て直された場合
- サーバー上でルールが作成、編集、または削除された場合
- エージェントが MSI のインストールまたはアップグレードの終了を検出した場合
- 特別な Bit9 Support コマンドを使用して手動で再評価が開始された場合

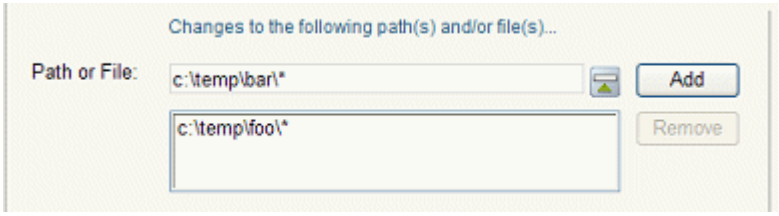
重要

HKCU から始まるレジストリ マクロが指定されているルールは、ユーザーがログオンしてからしばらく経つまで有効になりません。ルールが有効になるまでの時間は、設定されているルールの数と、レジストリ マクロやその他のユーザー固有パラメーターの展開に必要な時間によって異なります。ログイン後すぐにルールを有効にする必要がある場合は、HKCU から始まるマクロを使用しないでください。

複数のパスまたはプロセスの入力

ルールの［Path or File（パスまたはファイル）］と［Process（プロセス）］では、複数の文字列を入力できます。ルールの対象となる最初のプロセスを入力した後に、ボックスの右にある［Expand（展開）］ボタンをクリックします。

その後、ボックス内に別のパスまたはファイルを入力し、項目を 1 つ入力するたびに［**Add**（追加）］をクリックします。



ファイルまたはパスを削除するには、［Path or File（パスまたはファイル）］ボックスの下にあるリストでファイルまたはパスを選択して、［**Remove**（削除）］ボタンをクリックします。

1 つのルールで複数のパスまたはプロセスを入力した場合は、［Custom Rules（カスタム ルール）］ページの該当列に最初のパスが表示され、その後ろに［**(multiple)**（複数）］と表示されます。値の上にマウス ポインターを置くと、そのルールのパスまたはプロセスの完全なリストがヒントとして表示されます。

プロセスの指定

［Process（プロセス）］で文字列を指定する際には、［Path or File（パスまたはファイル）］で使用できるものと同じオプションを使用できます。詳細については、「パスとプロセスの指定」（420 ページ）を参照してください。

1 つのルールで［User or Group（ユーザーまたはグループ）］と［Process（プロセス）］が両方とも指定されている場合は、両方の条件が適用されます。たとえば、［Specific Process（特定のプロセス）］が選択されている場合は、条件に一致するユーザーまたはグループが、条件に一致するプロセスの実行を試みた場合にルールが適用されます。［Any Process Except（以下を除くすべてのプロセス）］が選択されている場合は、［User or Group（ユーザーまたはグループ）］と［Process（プロセス）］の両方がルールの定義と一致する場合を除いてルールが適用されます。

表 52：[Process（プロセス）] メニューのオプション

メニュー オプション	説明
[Any Process（すべてのプロセス）]	ルールに一致するファイルの実行または書き込みが何らかのプロセスによって試みられた場合、どのプロセスかにかかわらずルールを適用します。
[Any Promoted Process（昇格されたすべてのプロセス）]	ルールの評価時に昇格されていたプロセスがルールに一致するアクションを試みた場合にルールを適用します。昇格されたプロセスとは、インストーラーとしてマーキングされたファイルによって生成された承認済みのプロセス、カスタム ルールの結果として昇格されたプロセス、または昇格されたプロセスによって開始された承認済みのプロセスのいずれかを指します。
[Any System Process（すべてのシステム プロセス）]	Local System ユーザーのセキュリティ コンテキストで実行されているプロセスがルールに一致するアクションを試みた場合にルールを適用します。このオプションの効果は [User or Group（ユーザーまたはグループ）] メニューで Local User を選択した場合の効果と同じですが、こちらのオプションを選択するほうがより効率的です。
[Specific Process...（特定のプロセス ...）]	指定された文字列に一致するプロセスがルールに一致するアクションを試みた場合にルールを適用します。メニューの下にあるテキスト ボックスには複数のプロセスを入力できます。
[Any Process Except...（以下を除くすべてのプロセス ...）]	指定された文字列に一致するプロセスを除く任意のプロセスがルールに一致するアクションを試みた場合にルールを適用します。メニューの下にあるテキスト ボックスには複数のプロセスを入力できます。

ユーザーまたはグループの指定

ルールの種類によっては、特定のユーザーまたは特定のグループに属するユーザーがアクションを試みた場合にのみ適用されるルールを作成できます。[Add/Edit Custom Rule（カスタム ルールの追加 / 編集）] ページの [User or Group（ユーザーまたはグループ）] で選択できるオプションは次のとおりです。

- [**Any Users**（すべてのユーザー）] – すべてのユーザーにルールを適用します。
- [**Specific User or Group...**（特定のユーザーまたはグループ ...）] – メニューの下にテキスト ボックスが表示され、次の形式を使用して AD ユーザーまたはグループを入力できます。ユーザーまたはグループ名 @ ドメイン または ドメイン \ ユーザーまたはグループ名
  プラットフォームに関する注意：Mac または Linux のグループを指定するには、グループ名の前に「group」という単語とコロンを付ける必要があります。たとえば、「consoleusers」グループを指定する場合は、「group:consoleusers」と入力します。この接頭辞を付けないと、グループ名ではなくユーザー名と見なされます。
- Windows ルールの場合は、**Authenticated Users** や **Local Administrators** など、組み込み済みの Windows グループもメニュー オプションとして表示されます。

注意

- Windows Vista 以降でアプリケーションを実行する場合、事前定義されたセキュリティ グループ（Administrators など）のメンバーシップを指定するには、管理者としてアプリケーションを実行する必要があります。ルールに対してグループを定義する必要がある場合は、事前定義されたグループではなく、自身で定義したセキュリティ グループを使用することを検討してください。
- ユーザーがログインした後にグループのメンバーシップが確立されてグループベースのルールが有効になるまでの間にはわずかな遅れがあります。設定されているルールが多い場合はこの遅れが長くなる可能性があります。ユーザーのログイン後にできるだけ早くルールを有効にする必要がある場合は、ルール内でユーザー グループを指定しないようにしてください。ユーザー名や SID が指定されているルールは常に有効で、この遅れによる影響を受けません。
- ユーザーまたはグループの指定は、パスに含まれるマクロを展開するかどうかも決定します。指定されたユーザーまたはグループと一致するマクロを含むパスのみが展開されるため、ユーザーまたはグループがアクションを試みた場合でも、ユーザー関連のマクロがパスに含まれている場合は、指定されたユーザー以外のユーザーに関連するパスは展開されず、ルールは適用されません。

ルールのランキング

カスタム ルールには「ランク」番号が割り当てられ、最もランク番号が小さいルールから最もランク番号が大きいルールに向かって順番に評価されます。最小のランク番号は「1」です。デフォルトではランク順にルールが表示されますが、必要に応じて他の列を基準にテーブルを並べ替えることもできます。アクションをブロックするルールとアクションを許可するルールの両方に一致するファイルが存在する場合は、ランキングが高いほうのルール（ランク番号が小さいほうのルール）が優先され、ランキングが低いほうのルール（ランク番号が大きいほうのルール）は適用されません。特定のルールを現在の優先順位よりも上げる必要がある場合は、ルールのランキングを変更できます。

重要

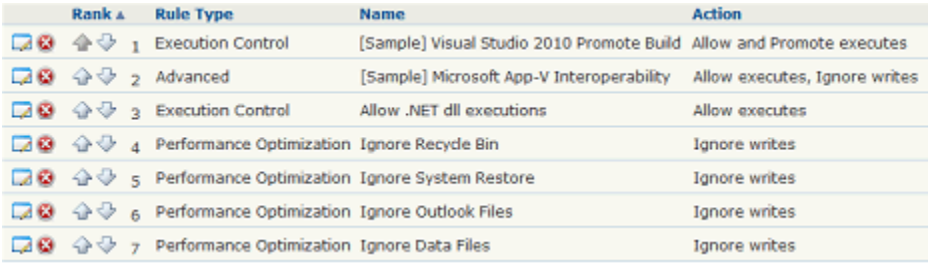
ルールのランキングは、アクションをブロックするルール、アクションを許可するルール、またはユーザーにプロンプトを表示してアクションをブロックするか許可するかを尋ねるルールに関してのみ意味を持ちます。ファイルに対して試みられたアクションに一致するブロック ルール、許可ルール、またはプロンプト ルールの中で最もランキングが高いルールが優先され、下位にランクされたルールの処理は停止されます。

ただし、下位にランクされている場合でも、アクションとして［Approve（承認）］、［Approve as Installer（インストーラーとして承認）］、［Track（追跡）］、［Report（レポート）］、［Promote（昇格）］、または［Ignore（無視）］が指定されているルールの処理は停止されません。たとえば、特定の書き込みアクションが無視ルールに一致し、下位にランクされている別のルール（ランク番号が大きいルール）にも一致した場合は、2 番目に一致したルールも処理されます。

カスタム ルールではありませんが、［Custom Rules（カスタム ルール）］テーブルには、禁止されているファイルのブロックなど、Bit9 Security Platform での基本的なアクションに関する内部ルールも表示されます。内部ルールとの関係においてそれ以外のルールの順位を変更する方法とその必要がある状況に関連する推奨事項については、「ルールのランキングと内部ルール」を参照してください。

カスタム ルールのランクの変更手順：

1. ［Custom Rules（カスタム ルール）］ページでルールがランク順に表示されていない場合は、［Rank（ランク）］列の見出しをクリックして並べ替えます。
2. ランクを変更するルールを探します。
3. ルールのランクを上げるには、適切な位置に来るまでルールの隣にある上矢印ボタンをクリックします。
   または
   移動するルールの上にマウス ポインターを置き、左マウス ボタンを押しながら新しい位置にルールをドラッグしてマウス ボタンを放します。
4. ルールのランクを下げるには、適切な位置に来るまでルールの隣にある下矢印ボタンをクリックするか、ドラッグアンドドロップでルールを移動します。



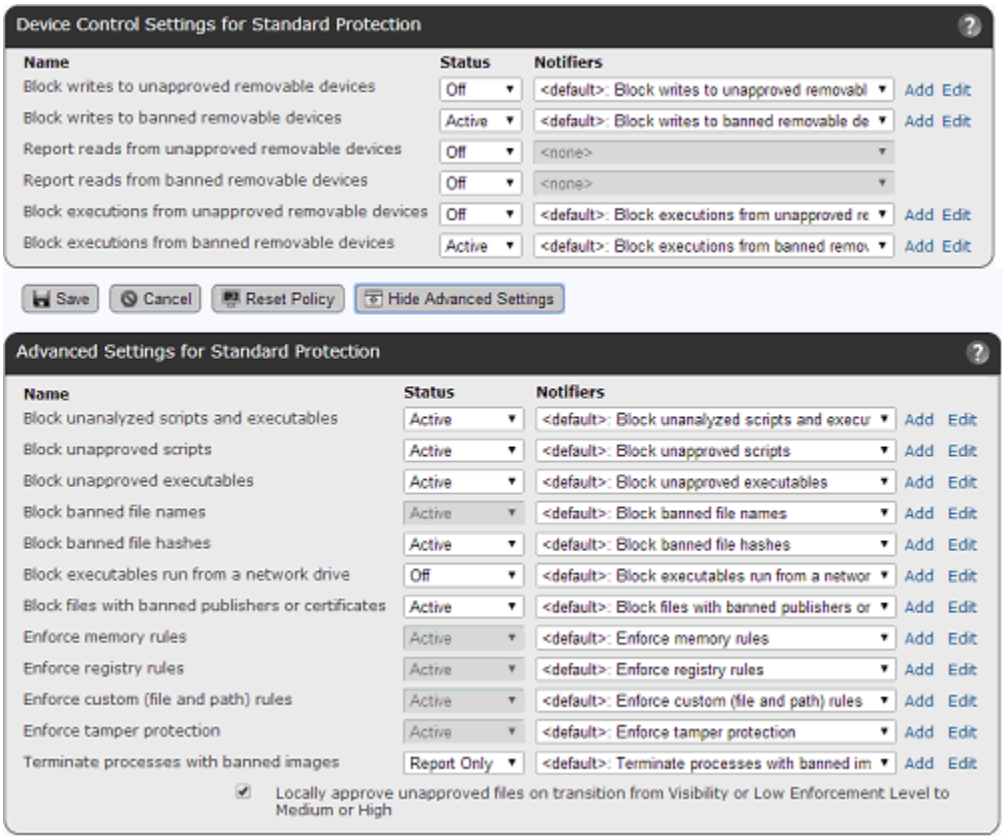
Rank ▲	Rule Type	Name	Action
1	Execution Control	[Sample] Visual Studio 2010 Promote Build	Allow and Promote executes
2	Advanced	[Sample] Microsoft App-V Interoperability	Allow executes, Ignore writes
3	Execution Control	Allow .NET dll executions	Allow executes
4	Performance Optimization	Ignore Recycle Bin	Ignore writes
5	Performance Optimization	Ignore System Restore	Ignore writes
6	Performance Optimization	Ignore Outlook Files	Ignore writes
7	Performance Optimization	Ignore Data Files	Ignore writes

注意

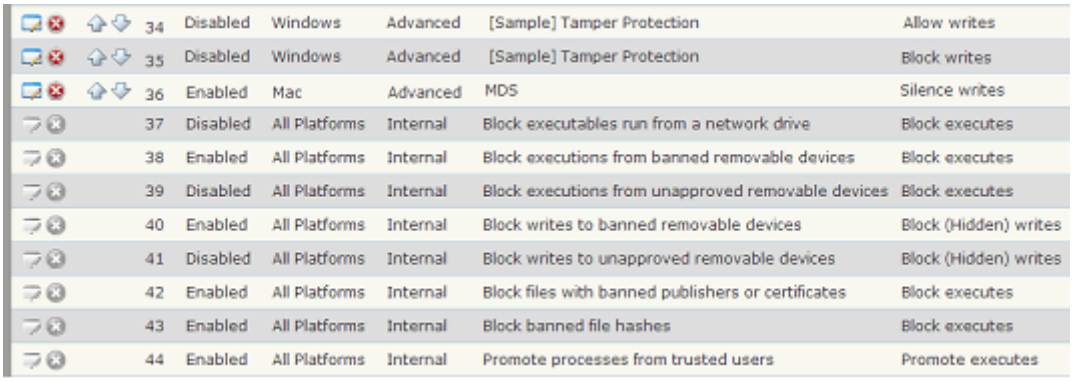
ドラッグアンドドロップを使用する場合、前後のページにルールをドラッグすることはできません。現在表示されていないランキングにルールを移動する必要がある場合は、［Custom Rules（カスタム ルール）］ページの右下にあるメニューを使用して 1 ページごとに表示される行数を増やすことができます。

ルールのランキングと内部ルール

［Custom Rules（カスタム ルール）］テーブルには、コンソールの他の部分に存在する機能に関連する内部ルールも表示されます。これらの内部ルールは［Edit Policy（ポリシーの編集）］ページの［Device Settings（デバイス設定）］や［Advanced Settings（高度な設定）］に表示される設定にほぼ対応しています。



たとえば、［Block banned file hashes（禁止ファイル ハッシュをブロック）］は、［Custom Rules（カスタム ルール）］ページに内部ルールとして表示され、［Edit Policy（ポリシーの編集）］ページの［Advanced Settings（高度な設定）］セクションの設定項目としても表示されます。



［Custom Rules（カスタム ルール）］ページで内部ルールを有効化、無効化、変更、または移動することはできないため、内部ルールの削除ボタンや編集ボタンはグ

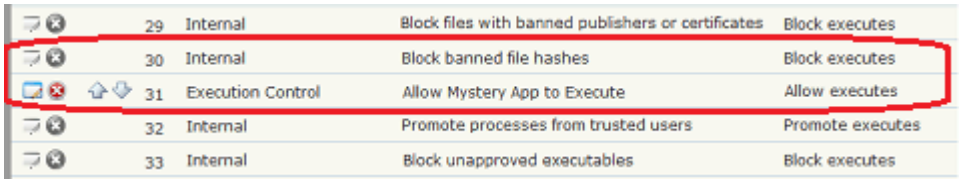
レーで表示され、上下矢印ボタンも表示されません。内部ルール間の優先順位を変更することはできません。ただし、内部ルール以外のカスタム ルールを内部ルールよりも上位または下位に移動することにより各ルールを適用する方法や状況を制御することは可能です。これを行うには、内部ルール以外のルールを移動します。

他のルールとの関係において内部ルールの優先順位を変更する必要がある主な状況は次のとおりです。

- デフォルトでは、禁止されているファイルの実行を許可するカスタム ルールが作成されると、そのルールは禁止ハッシュの実行をブロックする内部ルールよりも上位にランクされます。したがって、そのファイルに対しては、禁止ハッシュをブロックする内部ルールよりも、カスタム ルールのほうが優先されます。禁止されているファイルの実行を許可するカスタム ルールのランクを内部ルール［Block banned file hashes（禁止ファイル ハッシュをブロック）］よりも下位に下げると、ファイルの実行は許可されなくなります。
- デフォルトでは、ファイルの書き込みを許可するカスタム ルールが作成されると、そのルールは書き込みをブロックする内部ルールよりも上位にランクされるため、書き込みを許可するルールが優先されます。たとえば、デバイスへの書き込みを許可するルールを作成すると、そのルールはデバイスへの書き込みをブロックする内部ルールよりも上に表示されます。デバイスへの書き込みを許可するカスタム ルールを［Block writes to unapproved removable devices（未承認リムーバブル デバイスへの書き込みをブロック）］ルールよりも下に移動すると、書き込みをブロックするルールが優先され、それよりも下位にある許可ルールやプロンプト ルールに一致する場合でも未承認デバイスへのファイルの書き込みがブロックされます。

実行を許可するカスタム ルールよりもファイルのハッシュに基づく禁止を優先させる手順：

1. ［Custom Rules（カスタム ルール）］ページでルールがランク順に表示されていない場合は、［Rank（ランク）］列の見出しをクリックして並べ替えます。
2. 禁止されているファイルの実行を許可するルールを探します。
3. 下矢印を使用して許可ルールの位置を［Block banned file hashes（禁止ファイル ハッシュをブロック）］ルールよりも下に下げます。



カスタム ルールの無効化と削除

不要になったカスタム ルールはカスタム ルール テーブル内に残したまま無効化することも、テーブルから削除することもできます。無効化または削除されたルールは、新たに検出されたファイルに対しては適用されません。ただし、ルールを無効にする前にそのルールによって適用されたファイル状態はそのまま維持されます。

同じルールを将来再び使用する可能性がある場合は、一時的に無効にすることをお勧めします。

カスタム ルールの無効化手順：

1. コンソール メニューで［**Rules**（ルール）］>［**Software Rules**（ソフトウェア ルール）］を選択し、［Software Rules（ソフトウェア ルール）］ページが表示されたら［**Custom**（カスタム）］タブをクリックします。［Custom Rules（カスタム ルール）］テーブルが表示されます。
2. 無効にするルールの隣にある［Edit（編集）］ボタン（鉛筆とファイル）をクリックします。［Edit Custom Rule（カスタム ルールの編集）］ページが表示されます。
3. ［Status（ステータス）］行にある［**Disabled**（無効）］ラジオ ボタンをクリックし、ページの下部にある［**Save**（保存）］ボタンをクリックします。ルールが無効になります。

ルールを完全に削除した場合、削除を取り消したり、削除したルールを復元することはできません。本当にルールを削除してもよいかどうかを事前に必ず確認してください。Bit9 コンソールに表示される事前構成済みのルールを削除することは推奨されません。

カスタム ルールの削除手順：

1. コンソール メニューで［**Rules**（ルール）］>［**Software Rules**（ソフトウェア ルール）］を選択し、［Software Rules（ソフトウェア ルール）］ページが表示されたら［**Custom**（カスタム）］タブをクリックします。［Custom Rules（カスタム ルール）］テーブルが表示されます。
2. 削除するルールの隣にある［Delete（削除）］ボタン（X と書かれている赤い丸）をクリックし、設定ダイアログで［**OK**］をクリックします。ルールが削除されます。

コンピューターでのルール ステータスの表示

Bit9 Server で管理されているエージェントの数と接続されていないエージェントの数によっては、すべてのエージェントに新しいルールや更新されたルールがすぐに配信されない場合があります。有効になっているルールの［Edit（編集）］ページにある［Related Views（関連ビュー）］メニューには、［Computers（コンピューター）］ページの 2 種類のフィルター済みビューへのリンクがあり、エージェント管理コンピューターでのルールのステータスを確認できます。以下の選択肢があります。

- **[All Computers that have received this rule（このルールを既に受信したすべてのコンピューター）]**
- **[All Computers that have not yet received this rule（このルールをまだ受信していないすべてのコンピューター）]**

一度も有効化されたことがないルールの場合、このメニューは表示されません。

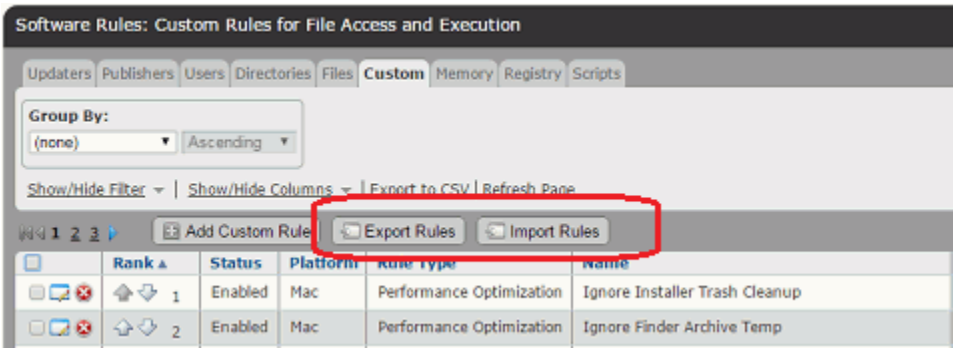
ルールのエクスポートとインポート

Bit9 Server 上で作成された特定のルールはファイルにエクスポートすることができ、そのファイルを他の Bit9 Server にインポートすることもできます。エクスポート可能な種類のルールは次のとおりです。

- カスタム ルール
- レジストリ ルール
- メモリ ルール

ルールのエクスポートとインポートは次のような状況で役立つ場合があります。

- **テスト環境から実稼働環境への移行** – ラボ環境でルールを作成してテストと調整を行ってから実稼働環境にルールを適用する場合、ルールのエクスポートとインポートを使用すれば、ルールの動作に問題がないことが確認された時点でテスト サーバーからルールをエクスポートし、ルール ファイルを実稼働サーバーにインポートできるので、ルール パラメーターを手動で再入力する手間やその際に起こりうる間違いを避けることができます。
- **Bit9 コミュニティでのルールの共有** – 便利なルールを作成したときに他のコミュニティ メンバーがインポートできるように、それらのルールをファイルにエクスポートして共有することができます。
- **Bit9 サポートからのソリューションの提供** – お客様が特定の目的を達成するためのルールを作成する際にサポートを必要とする場合、Bit9 サポートが適切なルールを作成し、お客様のサーバーにインポートできるようにルールをエクスポートして提供する場合があります。



ルールのエクスポートとインポートは、エクポートする種類のルールが表示される［Software Rules（ソフトウェア ルール）］ページのタブで行います。エクスポート ファイルには同じ種類のルールをいくつでも書き込めますが、異なる種類のルールを同じファイルに書き込むこともできます。たとえば、カスタム ルールとレジストリ ルールを 1 つのファイルにエクスポートできます。

エクスポートされたルール ファイルは、コンソールを表示しているブラウザーの標準ダウンロード方法とダウンロード先を使用してダウンロードされます。ルール ファイルの拡張子は **.rules** です。新しいルールを作成したり、既存のルールを変更したときに、必要に応じて新しいエクスポート ファイルを生成できます。

改ざんを防ぐためにルール ファイルは暗号化されています。エクスポートしたファイルに任意でパスワードを設定することにより、セキュリティをさらに強化することもできます。

注意

ルールのエクスポートとインポートを実行できるのはバージョン 7.2.1 以降の Bit9 Server のみです。

ルールのエクスポート

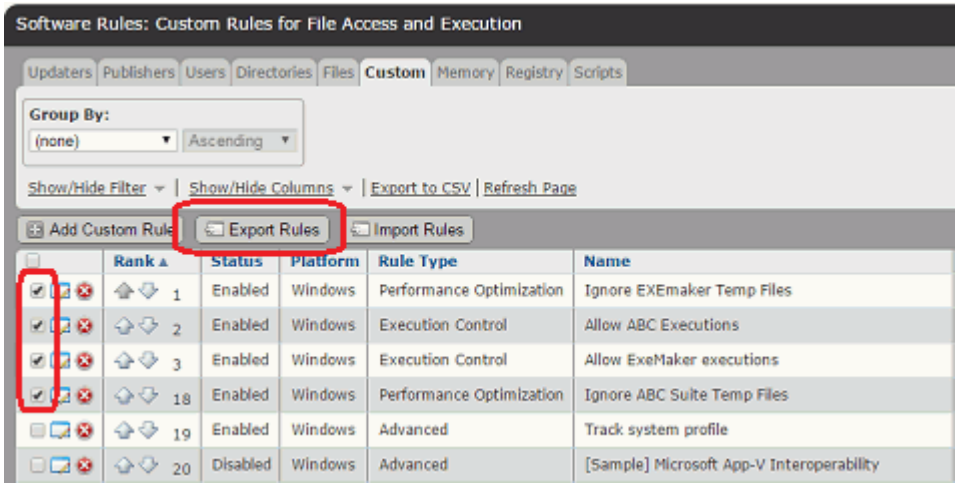
ルールをエクスポートする際には、ルールがどこにインポートされるかを考慮する必要があります。たとえば、社内で使用するルールをエクスポートする場合や、Bit9 コミュニティのメンバーと共有するルールをエクスポートする場合は、それぞれ次のような点を考慮する必要があります。

- **機密情報** – ルールを共有した結果、社外に公表すべきでない情報が漏洩してしまう可能性もあります。このような情報には、パス、ユーザー名、ルールの［Description（説明）］フィールドに書き込まれたコメントなどが含まれます。一般に知られている SID 以外のユーザーやグループの指定をエクスポートしないようにすることもできます。
- **環境に依存する設定** – 社外に共有するルールの場合、自社環境に固有のパスが指定されているとルールの有用性が制限される可能性があります。一般に、マクロが使用されているルールのほうが移植性に優れています。

ファイルへのルールのエクスポート手順：

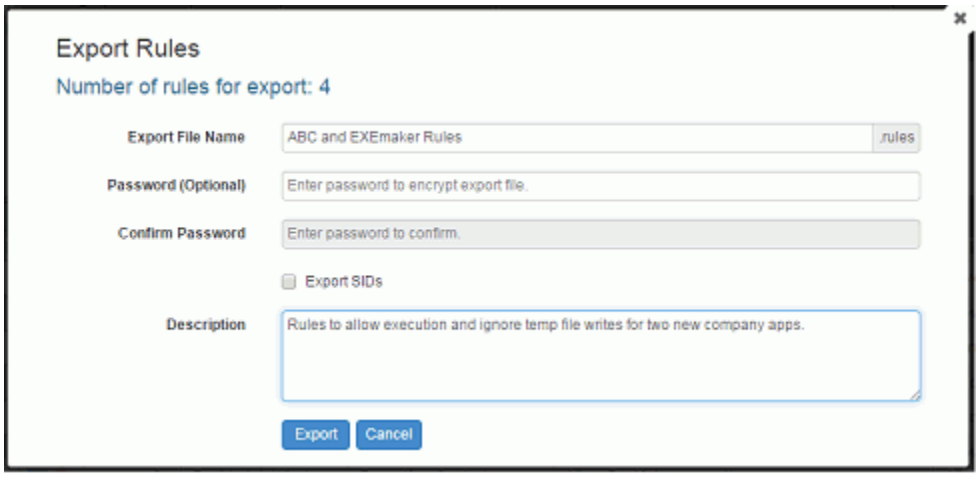
1. コンソール メニューで［**Rules**（ルール）］>［**Software Rules**（ソフトウェア ルール）］を選択し、エクスポートする種類のルールが表示されるタブ（［Custom（カスタム）］、［Registry（レジストリ）］、または［Memory（メモリ）］）をクリックします。
2. 1 つのファイルにエクスポートするすべてのルールが現在のページに表示されている必要があります。必要な場合は、フィルター、グループ化、または保存済みビューを使用してページの内容を変更します。大量のルールをエクスポートする場合は、必要に応じて、コンソール ページの右下にあるメニューを使用して 1 ページごとに表示される行数を増やします。

3. エクスポートする各ルールの隣にあるチェックボックスをオンにして、［**Export Rules**（ルールのエクスポート）］ボタンをクリックします。



［Export Rules（ルールのエクスポート）］ダイアログが表示されます。エクポートされるルールの数が表示され、ファイル名を入力するためのフィールドと、その他のエクポート オプションが表示されます。

4. 新しいエクスポート　ファイルのファイル名を（拡張子なしで）入力します。これが唯一の必須フィールドです。



5. エクスポートされたルール ファイルはテキストとして読み取れないように暗号化されていますが、安全性をさらに強化する必要がある場合はパスワードを入力し、確認のためにもう一度パスワードを入力します。このパスワードはファイルをインポートする際に必要になります。

6. 次のすべてに当てはまる場合は、［**Export SIDs**（SID のエクスポート）］チェックボックスをオンにします。

   - エクスポートするルールの中に、特定のユーザーまたはグループのみに適用されるルールが含まれている。
   - それらのユーザーまたはグループは、一般に知られている Windows システムのセキュリティ識別子 (SID) ではない。

- これらのルールのインポート先サーバーに、ルール内で指定されている SID が存在している。このケースは、同じ組織内でルールを移行する場合などに該当します。

7. このファイルをインポートするユーザーがルールの目的を理解しやすいように、任意で［Description（説明）］を追加できます。
8. エクスポート ファイルを保存する準備ができたら、［**Export**（エクスポート）］ボタンをクリックします。
   ダイアログが閉じ、ルール ファイルが作成され、Bit9 コンソールを実行しているブラウザーの標準ダウンロード方法を使用してルール ファイルがダウンロードされます。たとえば、［Export File Name（エクスポート ファイル名）］フィールドに「New Custom Rules」と入力すると、[Downloads] フォルダーに「New Custom Rules.rules」という名前のファイルが書き込まれます。

エクスポートしたルール ファイルは、他の Bit9 Server のホストにコピーしたり、ネットワーク経由でインポートできるように共有することができます。

ルールのインポート

他のサーバーからルールをインポートするには、ルール ファイルにアクセスする必要があります。また、ファイルがパスワードで保護されている場合は、インポート ダイアログでファイルを開いてインポートするルールを選択するために、パスワードの入力も必要になります。

ルールをインポートする手順については、「ファイルからのルールのインポート手順：」（448 ページ）を参照してください。インポートを実行する前に、次のセクションを参照することを強く推奨します。

インポートするルールの選択

［Import Rules（ルールのインポート）］ダイアログでルール ファイルの名前を入力すると、そのファイルが適切な形式で作成されているかどうかが確認され、インポートを行おうとしているページとルールの種類が一致しているかどうかも確認されます。ファイルがパスワードで保護されている場合は、パスワードの入力を求められます。これらのチェックに合格すると、ファイルに含まれるルールのリストがダイアログ ボックスに表示されます。

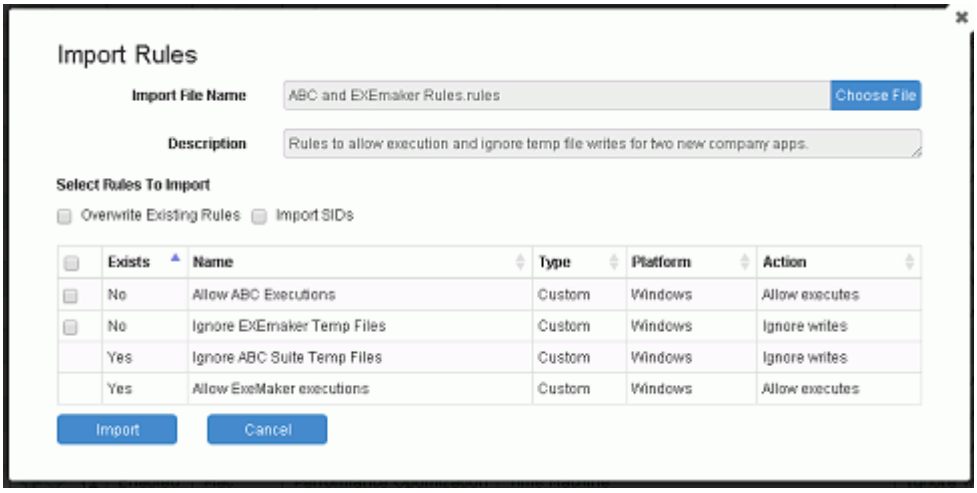


表 53 で［Import Rules（ルールのインポート）］ダイアログ内のフィールドについて説明します。大部分のフィールドについては、このセクションの後半でさらに詳しく説明します。

表 53：［Import Rules（ルールのインポート）］ダイアログのフィールド

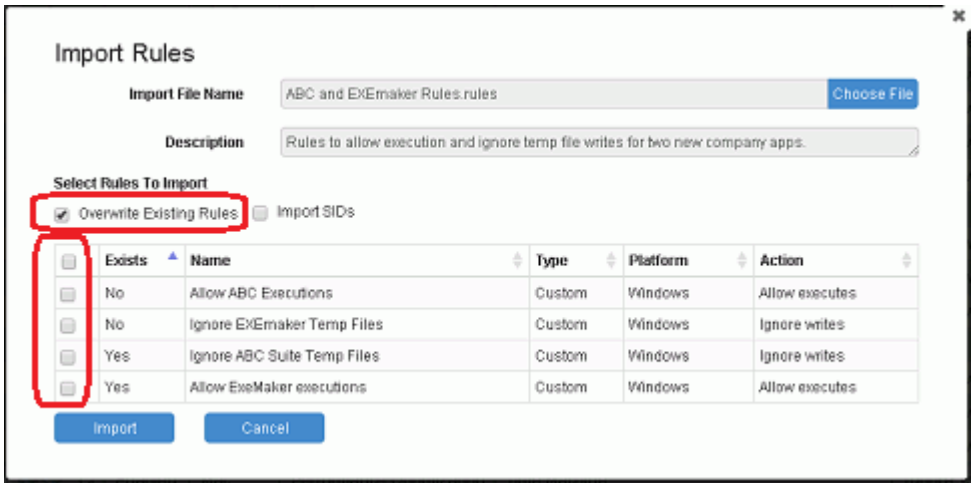
フィールド	説明
[Import File Name（インポート ファイル名）]	このサーバーにインポートされるルール ファイルの名前が表示されます。ファイル名は［Choose File（ファイルの選択）］ボタンとファイル選択ダイアログを使用して入力します。
[Description（説明）]	ルールをエクスポートするときに説明が追加されていた場合は、その説明が表示されます。
[Overwrite Existing Rules（既存ルールを上書き）]	このチェックボックスがオフになっている場合（デフォルト）、インポート先のサーバー上に既に存在するルールの隣にはチェックボックスが表示されません。このチェックボックスがオンになっている場合は、テーブル内のすべてのルールの隣にチェックボックスが表示され、既存のルールを上書きするかどうかを選択できます。
[Import SIDs（SID のインポート）]	このチェックボックスをオフにすると、Local Administrator のように一般に知られているセキュリティ ID (SID) ではないユーザーやグループがルール内で指定されている場合に、それらの指定がインポートされなくなります。このチェックボックスをオンにすると、ルール内のユーザーとグループの指定がすべてインポートされます。ルールをエクスポートする際には一致オプションが適用されるため、元のルールに含まれていたユーザーやグループの指定がエクスポートされたファイル内のルールでは削除されている場合もあります。
[Enter Password（パスワードの入力）]	このフィールドは、ルールのエクスポート時にパスワードが指定された場合にのみ表示されます。パスワードが指定されている場合は、このファイルを開くためのパスワードを入力するフィールドと［Open Import File with Password（パスワードを使用してインポートファイルを開く）］ボタンが表示されます。

フィールド	説明
ルール テーブル	インポート ファイルに含まれるすべてのルールがテーブルに表示されます。各ルールの行には次の列があります。 • （チェックボックス） – インポートの対象として選択できる各ルールの隣にチェックボックスが表示されます。 • [Exists（既存）] – そのルールがインポート先のサーバーに既に存在しているかどうかを示します。 • [Name（名前）] – ルール ページに表示されるとおりのルール名。 • [Type（種類）] – 表示されるタブ（[Custom（カスタム）]、[Memory（メモリ）]、または [Registry（レジストリ）]）によって示されるルールの種類。 • [Platform（プラットフォーム）]–ルールが適用されるオペレーティング システム / プラットフォーム（Windows、Mac、Linux）。 • [Action（アクション）] – ルールによって適用されるアクションの種類。

Bit9 Server 上の各ルールにはグローバルに一意の識別子 (GUID) が割り当てられ、エクスポートされたルール ファイルにはそれらの ID も書き込まれています。インポートするルール ファイルを選択すると、インポート ファイルに含まれるルールの GUID が既存ルールの GUID と比較され、同じルールがサーバー上に既に存在している場合は［Import Rules（ルールのインポート）］ダイアログにメッセージが表示されます。

ルールのエクポート元（組織内、Bit9 コミュニティ、Bit9 サポートなど）によっては、どのルールをインポートするかに関して異なる判断が必要になる場合があります。ファイル内のルールをすべてインポートする必要はありません。各ルールの隣にあるチェックボックスを使用してインポートするルールを選択できます。

デフォルトでは、インポート ファイルに含まれるルールのうち、インポート先サーバーに既に存在するルールの隣にはチェックボックスが表示されません。[Overwrite Existing Rules（既存ルールを上書き）] と名付けられたマスター チェックボックスをオンにすると、そのようなルールの隣にもチェックボックスが表示され、(既に存在するルールを含め) ページに表示されているすべてのルールをインポートできるようになります。



インポートされたルールの設定に生じる差異

ルールには、プロセス、パス、適用するアクション、ブロックに関連する通知など、さまざまな種類のパラメーターがあります。インポートされたルールの設定はエクポート元のサーバー上での設定とほぼ同じですが、次の要因により一部違いが生じる場合があります。

- インポートされたルールがインポート先のサーバー上に今まで存在していなかった新規のルールであるか、インポート先のサーバー上に既に存在するルールを更新するものであるか
- 特定のポリシーのみに適用されるルールであるか
- 特定のユーザーまたはグループに適用されるルールであるか

サーバー上に今まで存在していなかった新規のルールであるか、既に存在するルールであるかに応じて、設定に次の違いが生じます。

- **有効か無効か** – 新規ルールはインポート時に無効化されるため、手動で有効にする必要があります。これは、ルールを有効にする前に、サイト固有のポリシーやユーザー パラメーターを追加するなどのカスタマイズを行えるようにすることを目的としています。既存のルールはインポート時に上書きされ、インポート先サーバー上での有効 / 無効の設定はそのまま維持されます。
- **ランク** – 新規ルールはインポート時に最高レベルにランクされます。インポートによって上書きされた既存ルールのランクは、インポート先サーバー上で以前に設定されていた相対順位のまま維持されます（新規ルールも同時にインポートされた場合は、それに応じて下位のランクに移動されます）。
- **通知** – 通知を必要とする新規ルール（特定のアクションをブロックするルール）がインポートされた場合は、デフォルトの通知が使用されます。インポートされたルールによって既存ルールが上書きされた場合は、既存ルールで指定されていた通知が維持されます。

特定のポリシーに含まれるコンピューターに対してのみ適用されるルールも存在する可能性がありますが、同じポリシーが他のサーバーにも存在しているとは限りません。インポートされたルールが今までに存在していなかった新規のルールである場合は、既存のポリシー指定が削除され、そのルールがすべてのポリシーに適用されます。インポートされたルールによって既存ルールが上書きされた場合は、インポート先サーバー上の既存ルールのポリシー設定が維持され、エクポート元サーバー上のルールに含まれるポリシー設定は適用されません。

特定のグループに属する特定のユーザーまたはメンバーがアクションを試みた場合にのみ適用されるルールも存在する可能性があります。通常、一般に知られているセキュリティ ID (SID) を使用するユーザー名およびグループ名は、すべての Windows コンピューター上に存在します。一方、一般に知られていないユーザーやグループはルールのインポート先となるコンピューター上に存在していない可能性があります。エクポートされたルールでユーザーやグループが指定されている場合は、それらのユーザーやグループが一般に知られているかどうかなどの要因に基づき、インポートの結果が変わります。

- 一般に知られた SID がルール内で指定されている場合、それらの指定は常にエクスポートされ、すべてインポートされます。
- ［Export Rules（ルールのエクスポート）］ダイアログで［Export SIDs（SID のエクスポート）］チェックボックスがオンになっていた場合は、一般に知られていないユーザーやグループの指定もルールとともにエクスポートされます。

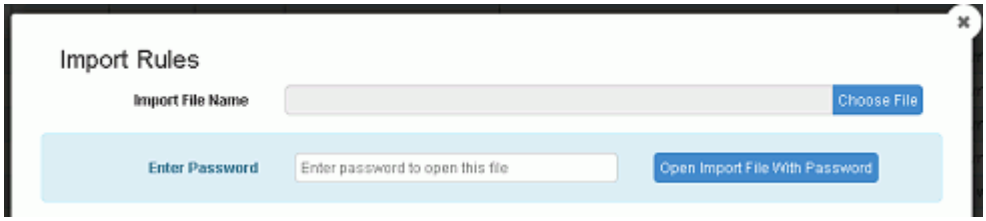
- 一般に知られていないユーザーやグループの指定がルールとともにエクスポートされている場合は、[Import Rules（ルールのインポート）] ダイアログで [Import SIDs（SID のインポート）] チェックボックスがオンにすると、それらの指定もインポートされます。

- エクスポートされたルールで一般に知られている SID と一般に知られていない SID が両方とも指定されていて、[Import SIDs（SID のインポート）] チェックボックスをオフにした場合は、一般に知られているユーザーまたはグループのみがルールとともにエクスポートされます。一般に知られていないユーザーまたはグループのみがルール内で指定されている場合はユーザーまたはグループの指定がルールから削除され、そのルールはすべてのユーザーに適用されます。

ファイルからのルールのインポート手順：

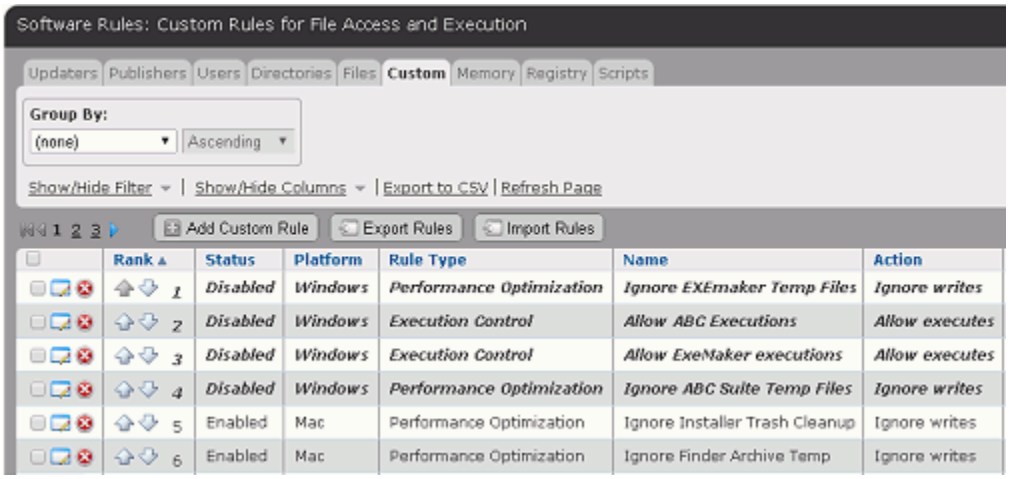
1. コンソール メニューで [**Rules**（ルール）] > [**Software Rules**（ソフトウェアルール）] を選択し、インポートする種類のルールのタブ（[Custom（カスタム）]、[Registry（レジストリ）]、または [Memory（メモリ）]）をクリックします。
2. [**Import Rules**（ルールのインポート）] ボタンをクリックします。

   [Import Rules（ルールのインポート）] ダイアログが表示されます。
3. [**Choose File**（ファイルの選択）] ボタンをクリックして Windows 標準のファイル選択ダイアログを開き、インポートするルール ファイルを選択します。パスワードが不要な場合は、「インポートするルールの選択」（444 ページ）に示すように、ファイルに含まれるルールの一覧が [Import Rules（ルールのインポート）] ダイアログに表示されます。
4. ファイルを開くためにパスワードの入力が必要な場合は、ルール名が表示される前に、パスワードの入力フィールドがダイアログに表示されます。その場合は、パスワードを入力して [Open Import File with Password（パスワードを使用してインポート ファイルを開く）] をクリックします。



   パスワードが確認されると、「インポートするルールの選択」（444 ページ）に示すように、ファイルに含まれるルールの一覧がダイアログに表示されます。
5. 一般に知られていない SID を使用しているユーザーやグループのパラメーターも含めてインポートする場合は、[**Import SIDs**（SID のインポート）] チェックボックスをオンにします。これらの機能の詳細については、「インポートするルールの選択」（444 ページ）を参照してください。

6. デフォルトでは、インポート先のサーバー上に既に存在するルールの隣にはチェックボックスが表示されません。既存のルールを上書きするかどうかを選択する必要がある場合は、[**Overwrite Existing Rules**（既存ルールを上書き）] チェックボックスをオンにします。既存ルールを上書きした場合の結果については、「インポートされたルールの設定に生じる差異」（447 ページ）を参照してください。
7. ダイアログに表示されている各ルールの情報を確認し、インポートする各ルールの隣にあるチェックボックスをオンにして、[**Import**（インポート）] ボタンをクリックします。
ダイアログが閉じ、ルールがサーバーにインポートされます。現在のセッションが継続されている間、インポートされたルールは斜体の太字でルール ページ上に表示されます。



カスタム ルールの種類と例

[Add/Edit Custom Rule（カスタム ルールの追加 / 編集）] ページの [Rule Type（ルール タイプ）] メニューには、次のオプションが表示されます。

- [**File Integrity Control**（ファイル整合性の制御）] – 指定されたフォルダーやファイルの変更をブロックします。
- [**Trusted Path**（信頼済みパス）] – ファイルの実行を常に許可するフォルダーやファイルを定義します。
- [**Execution Control**（実行の制御）] – ルールに一致するファイルの実行が試みられたときの動作を制御します。
- [**File Creation Control**（ファイル作成の制御）] – ルールに一致するファイルの書き込みが試みられたときの動作を制御します。
- [**Performance Optimization**（パフォーマンスの最適化）] – 監視の対象から除外する（ただし、実行は引き続き監視する）フォルダーとファイルを指定します。
- [**Advanced**（詳細）] – このオプションを選択すると、ファイルの実行、作成、および追跡を最も詳細に制御することができます。

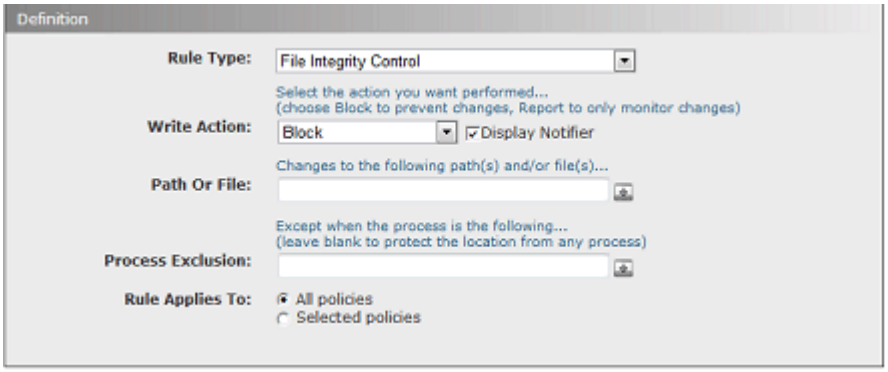
［Custom Rules（カスタム ルール）］テーブルには［Sample（サンプル）］と書かれたルールも含まれ、これらのルールはデフォルトで無効になっています。たとえば、［[Sample］Developer - Visual Studio Ignore Intermediate Files（[サンプル］開発者 – Visual Studio 中間ファイルを無視）］は、多くのビルド環境で一般的に見られる特定の中間ファイルを無視するパフォーマンス最適化ルールです。［Custom Rules（カスタム ルール）］テーブルでこれらのサンプルの隣にある［Edit（編集）］ボタン（鉛筆）をクリックすると、同様の結果を達成するために適用されるパラメーターの種類を確認できます。

以下のセクションでは、各種ルールの一般的な設定例を紹介します。

［File Integrity Control（ファイル整合性の制御）］

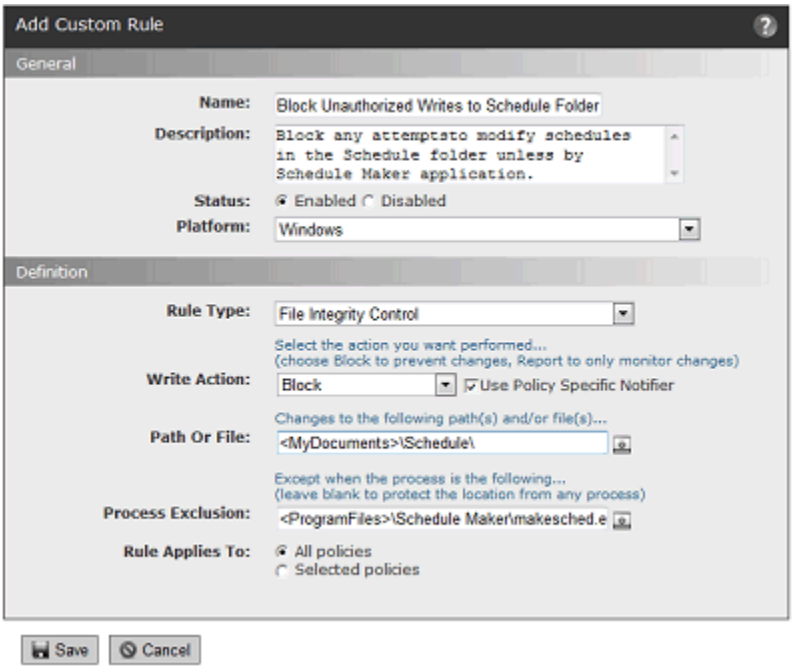
［Write Action（書き込みアクション）］オプション : ［Block（ブロック）］、［Report（レポート）］
［Execute Action（実行アクション）］: この種類のルールには該当しません（ダイアログに表示されません）
［User（ユーザー）］: すべてのユーザーに適用されます（この種類のルールの固定値で、ダイアログに表示されません）

［File Integrity Control（ファイル整合性の制御）］ルールを使用すると、特定のフォルダー（またはファイル）、または指定に一致する複数のフォルダー（またはファイル）に対する変更を制御できます。［Write Action（書き込みアクション）］として［Block（ブロック）］を選択するとフォルダーへの書き込みをブロックでき、［Write Action（書き込みアクション）］として［Report（レポート）］を選択すると変更を（ブロックせずに）監視できます。



たとえば、ScheduleCreator というアプリケーションによって全社員のスケジュールが生成され、各ユーザーのコンピューターの［**マイ ドキュメント**］フォルダー内にある［**Schedule**］フォルダーにその結果が保存されているとします。また、ScheduleCreator の実行可能ファイルは **makesched.exe** と名付けられているとします。そして、各ユーザーのスケジュールの生成を許可し、指定された場所に生成されたスケジュールを誰も変更できないようにする必要があるとします。この場合は、ルールの種類として［**File Integrity Control**（ファイル整合性の制御）］を選択し、［Write Action（書き込みアクション）］を［**Block**（ブロック）］に設定します。次に、［Path or File（パスまたはファイル）］を **<MyDocuments>\Schedule** に設定します。<MyDocuments> は、エージェントが稼働するコンピューター上の各ユーザーの「マイ ドキュメント」フォルダーにマッピングされるマクロです。最後に、［Process Exclusion（除外するプロセス）］ボックスに「***\makesched.exe**」

と入力して、このプロセスがルールで指定されているパスへの書き込みを行えるように設定します。**<ProgramFiles>\Schedule Maker\makesched.exe** のように、[Process Exclusion（除外するプロセス）] ボックスでマクロを使用すると、許可の対象となるプロセスを、特定の場所から実行されるプロセスのみに制限できます。



[Trusted Paths（信頼済みパス）]

[Execute Action（実行アクション）]：[Allow（許可）]、[Allow and Promote（許可と昇格）]、[Promote（昇格）]
[User（ユーザー）]：すべてのユーザーに適用されます（この種類のルールの固定値で、ダイアログに表示されません）

カスタム ルールの使用方法の 1 つとして、信頼済みパスの指定があります。ネットワーク上の場所を信頼済みパスとして指定し、その場所にインストーラーを配置すると、特定のポリシーまたはすべてのポリシーに含まれるコンピューターがそれらのインストーラーを実行できるようになります。

信頼済みパスはアクセス方式の 1 つであり、グローバルな承認を適用するための手段ではありません。信頼済みパスを設定すると、実行可能ファイルによって生成されたファイルをグローバルに承認することなく、特定の場所でのファイルの実行を許可できます。

信頼済みパス上のファイルは指定された場所で実行される必要がありますが、実行の結果として生成されるファイルの保存先は別のコンピューター上（信頼済みパス経由で実行可能ファイルにアクセスする別のコンピューター上）でもかまいません。信頼済みパス上のファイルにアクセスできるコンピューターが、自身のローカル ドライブにインストール パッケージをコピーして実行することはできません。

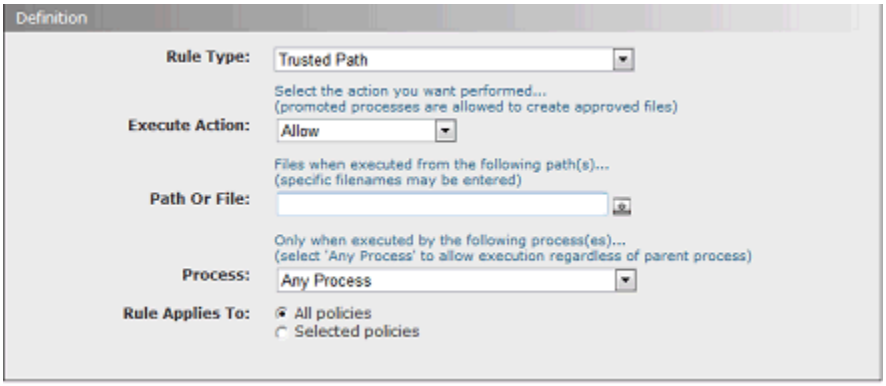
信頼済みパスのファイルによって書き込まれたファイルのローカル状態は、使用された [Execute Action（実行アクション）] コマンドによって異なります。[Execute Action（実行アクション）] が [Allow（許可）] に設定されている場合、インス

トーラーによるファイルの書き込みは許可されますが、そのファイルがアクションによってローカルで承認されることはありません。この場合、Bit9 Server によって今までに検出されたことがないファイルが新たに書き込まれると、[Files（ファイル）] ページの［File Catalog（ファイル カタログ）］タブに［Unapproved（未承認）］ステータスのファイルとして追加されます。［Execute Action（実行アクション）］が［Allow and Promote（許可と昇格）］に設定されている場合は、インストーラーによるファイルの書き込みが許可され、そのファイルは（禁止されていない限り）ローカルで承認されます。

重要

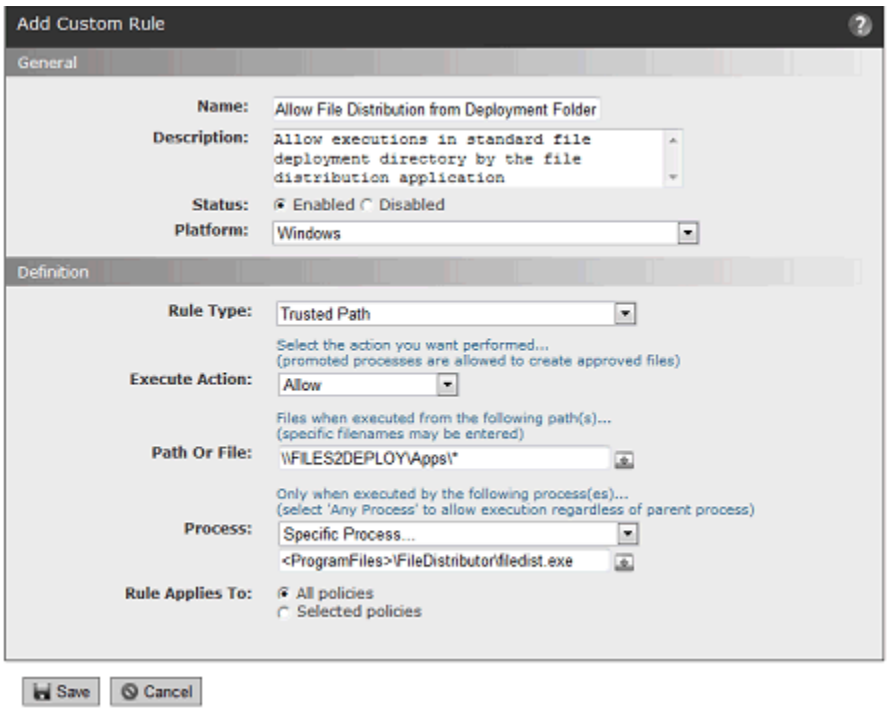
- 信頼済みパスに実行可能ファイルやスクリプトを書き込むことができるユーザーは、(a) その場所にアクセスして、(b) リモート ドライブからの実行が許可されているコンピューターに対して任意のアプリケーションを共有することができます。信頼済みパスを有効にする前に、プラットフォームのセキュリティ設定を確認して、その場所が適切に保護されていることを確認してください。
- Bit9 コンソールで、ユーザー固有の［File Integrity Control（ファイル整合性の制御）］ルールまたは［File Creation Control（ファイル作成の制御）］ルールを信頼済みパスに対して作成すると、信頼済みパスの安全性を強化することができます。新しいルールのランクを［Trusted Path（信頼済みパス）］ルールより高く設定すると、そのパスをソフトウェア配布場所として使用することを許可すると同時に、同じ場所への書き込みを制御できます。

インストーラー用の信頼済みパスを作成するには、「カスタム ルールの作成」（411 ページ）の説明に従い、［Rule Type（ルール タイプ）］として［**Trusted Path**（信頼済みパス）］を選択します。［Trusted Path（信頼済みパス）］を選択すると、それに応じてページ内の他のフィールドが変更されます。［Execute Action（実行アクション）］メニューに［**Allow**（許可）］と表示され、このルールに一致するファイルの実行が許可されます。



たとえば、FileDistributor というアプリケーションを使用して特定の配布サーバーから社内ソフトウェアを配布するとします。また、FileDistributor アプリケーションの実行可能ファイルは **filedist.exe** と名付けられていて、社内ソフトウェアは **\\FILE2DEPLOY\Apps** にある配布サーバーから配布されるとします。この場合は、ルールの種類として［**Trusted Path**（信頼済みパス）］を選択し、［Path or File（パスまたはファイル）］に **\\FILES2DEPLOY\Apps*** と入力します。

このルールの［Process（プロセス）］フィールドが［Any Process（すべてのプロセス）］に設定されている場合は、ルールの影響を受けるクライアント上のすべてのプロセスがその場所からアプリケーションやインストーラーを実行できます。このセキュリティ ギャップを軽減するには、このディレクトリ内のファイルを実行できるプロセスを FileDistributor のみに制限することにより、指定されたディレクトリからインストール　　アプリケーションを実行できるプロセスを FileDistributor だけに制限します。この制約を作成するには、［Process（プロセス）］に「***\filedist.exe**」と入力します。また、**<ProgramFiles>\FileDistributor\filedist.exe** のようにマクロを使用してファイルの場所を指定すると、さらに詳細にプロセスを制限できます。ユーザーが同じファイルを手動で実行しようとした場合はブロックされます。



さらに、［Rule applies to（ルールの適用先）］ボタンを使用すると、信頼済みパスやその他のカスタム ルールを特定のポリシーに含まれるコンピューターだけに適用できます。これらのパラメーターをすべて組み合わせると、システムのセキュリティ リスクを最小限に抑えながら、必要な操作を許可するルールを定義できます。

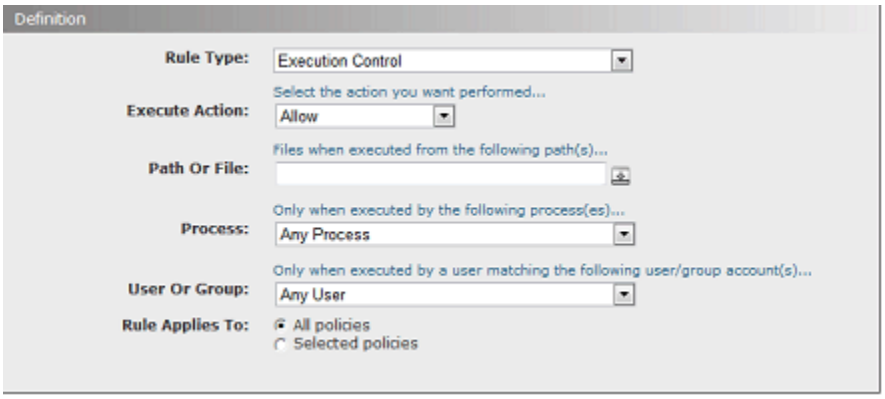
［Execution Control（実行の制御）］

［**Execute Action**（実行アクション）］**オプション** – ［Allow（許可）］、［Block（ブロック）］、［Allow and Promote（許可と昇格）］、［Promote（昇格）］、［Prompt（プロンプト）］、［Report（レポート）］

［**Write Action**（書き込みアクション）］– この種類のルールには該当しません（ダイアログに表示されません）

［Execution Control（実行の制御）］ルールは、その名が示すとおりのルールです。この種類のルールでは、特定の条件に一致するファイルの実行が試みられたときに適用するアクションを指定できます。条件に一致するファイルの書き込み（作成、変更、削除）には影響しません。

［Execution Control（実行の制御）］ルールは［Trusted Path（信頼済みパス）］ルールに似ていますが、ユーザーまたはグループを指定でき、［Execute Action（実行アクション）］で指定できるオプションの種類が信頼済みパス ルールよりも多い点が異なります。



たとえば、MyDevTool というツールを使用して DLL の開発とコンパイルを行っている開発者がいるとします。また、MyDevTool アプリケーションは、このアプリケーションで作成された DLL を実行するように設定されているとします。そして、このアプリケーションによる実行がブロックされないようにするためのルールを作成する必要があるとします。

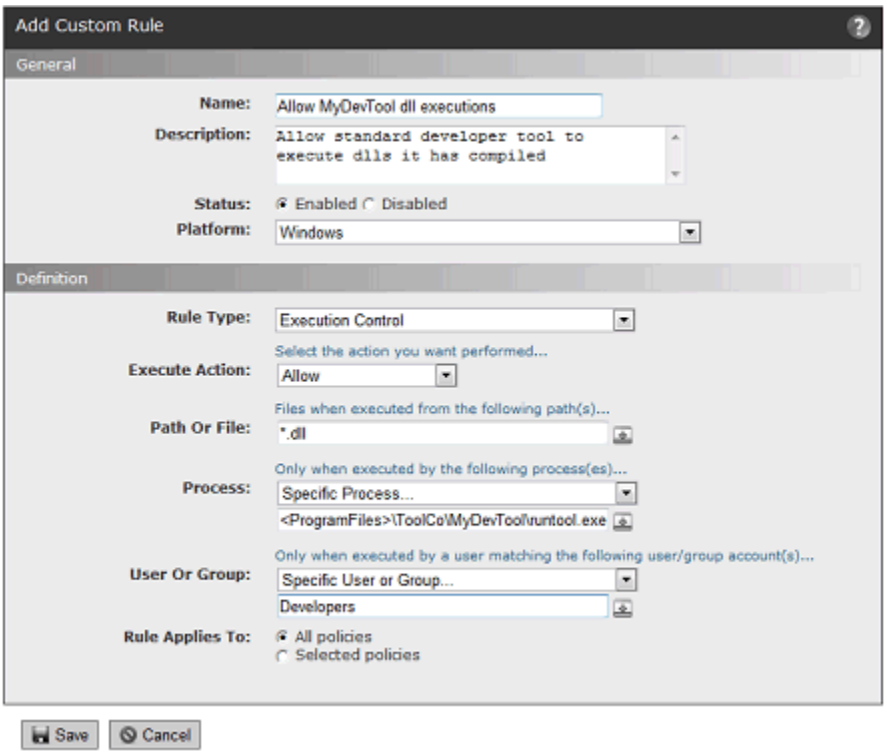
MyDevTool によって作成されるファイルは DLL であるため、［Path or File（パスまたはファイル）］に「***.dll**」と入力します。これらのファイルの場所が分かっている場合はパスも指定できますが、この例では場所を指定していません。

このルールの［Process（プロセス）］フィールドが［**Any Process**（すべてのプロセス）］に設定されている場合は、ルールの影響を受けるクライアント上のすべてのプロセスが任意の DLL を実行できます。このルールをより安全にするには、このディレクトリ内のファイルを実行できるプロセスをMyDevToolアプリケーションだけに制限します。これを行うには、**<ProgramFiles>\ToolCo\MyDevTool\runtool.exe** のようにマクロを使用してツールの正確な場所を指定します。

Active Directory グループが定義されている場合は、このツールを使用する権限を持つグループのみがこれらの DLL を実行できるように制限することもできます。これを行うには、［User or Group（ユーザーまたはグループ）］メニューで［**Specify**

User or Group…（ユーザーまたはグループを指定）］を選択し、ツールの実行を許可するグループの AD グループ名（**Developers** など）を入力します。

これにより、Developers グループに属するユーザーであればどこにある DLL ファイルでも MyDevTool を使用して実行できるルールが作成されます。



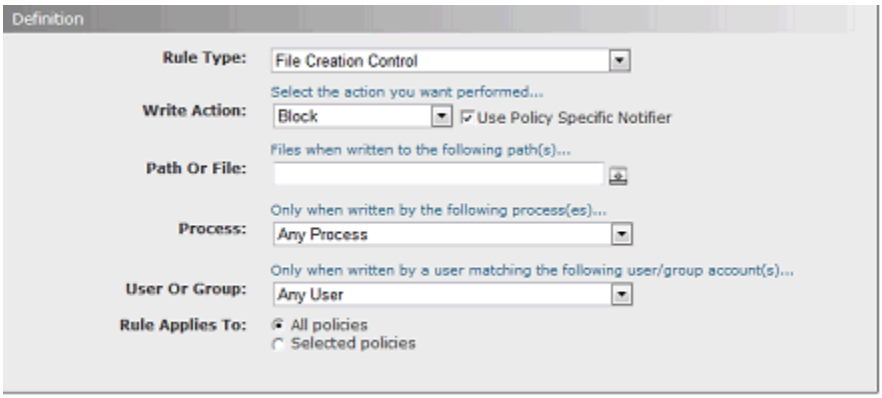
［File Creation Control（ファイル作成の制御）］

［**Write Action**（書き込みアクション）］**オプション** – ［Ignore（無視）］、［Block（ブロック）］、［Approve（承認）］、［Approve as installer（インストーラーとして承認）］、［Prompt（プロンプト）］、［Allow（許可）］

［**Execute Action**（実行アクション）］– この種類のルールには該当しません（ダイアログに表示されません）

［File Creation Control（ファイル作成の制御）］ルールを作成すると、特定の条件に一致するファイルの書き込み（作成）が試みられたときの動作を制御できます。ファイルの実行には影響しません。

［File Integrity Control（ファイル整合性の制御）］ルールと同様に、［File Creation Control（ファイル作成の制御）］ルールでも書き込みをブロックできます。ただし、［File Creation Control（ファイル作成の制御）］ルールでは、ユーザーまたはグループを指定でき、ファイルの書き込みをブロックしないケースとして指定できる［Write Action（書き込みアクション）］オプションの種類が多くなっています。



[Performance Optimization（パフォーマンスの最適化）]

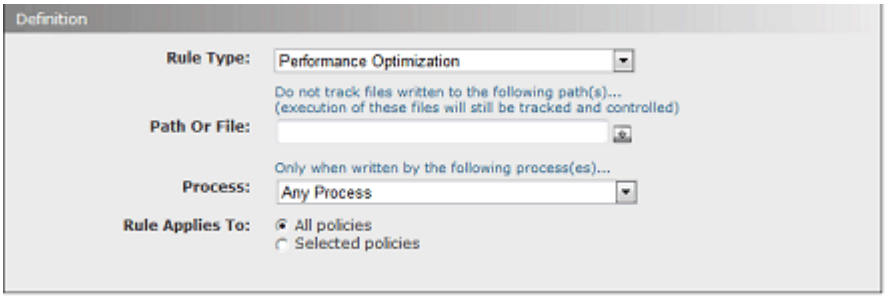
[**Write Action**（書き込みアクション）] – [Ignore（無視）]（この種類のルールの固定値で、ダイアログに表示されません）

[**Execute Action**（実行アクション）] – この種類のルールには該当しません（ダイアログに表示されません）

[**Users**（ユーザー）] – [Any User（すべてのユーザー）]（この種類のルールの固定値で、ダイアログに表示されません）

特に指示され限り、Bit9 Server は Bit9 エージェントを実行しているコンピューターに書き込まれるすべてのファイルを追跡し続けます。通常、この動作は監視の目的に役立ちますが、通常の処理の一環として同じディレクトリに大量のファイルを書き込むプロセスがある場合、これらの書き込み動作を監視するためにシステム リソースやネットワーク リソースが不必要に使用され、重要な情報は何も入手できません。このような場合は、[Performance Optimization（パフォーマンスの最適化）] カスタム ルールを作成して監視の対象から除外するディレクトリを指定できます。

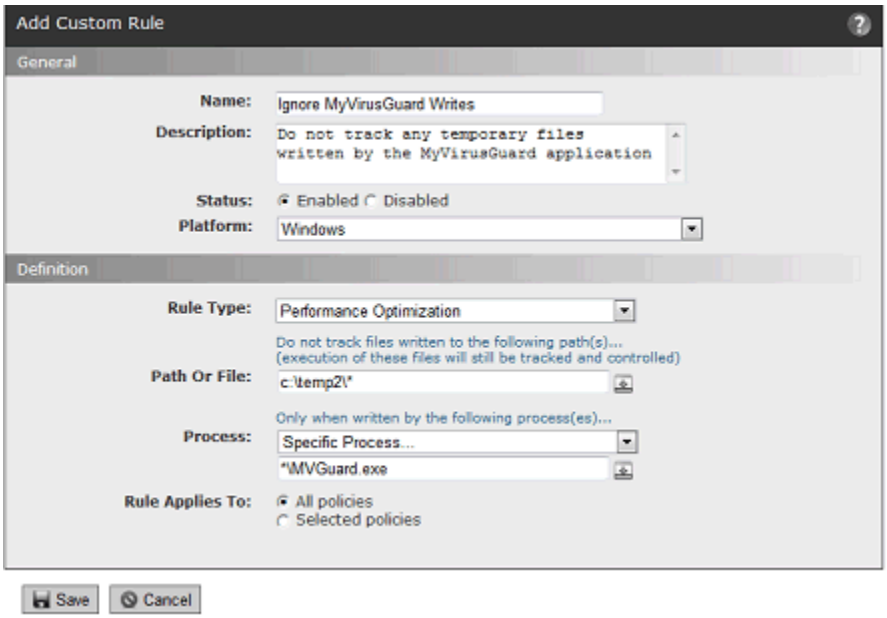
特定のファイルを監視の対象から除外するルールを作成するには、「カスタム ルールの作成」（411 ページ）の説明に従い、[Rule Type（ルール タイプ）] として [**Performance Optimization**（パフォーマンスの最適化）] を選択します。[Performance Optimization（パフォーマンスの最適化）] を選択すると、それに応じてページ内の他のフィールドが変更されます。[Write Action（書き込みアクション）] は [**Ignore**（無視）] に設定され（ただしダイアログには表示されません）、ルールに一致するファイルの書き込みは Bit9 Server によって追跡されなくなります。



たとえば、大量の一時ファイルを **c:\temp2** に書き込む MyVirusGuard というアプリケーションがあるとします。

その場合は、[Performance Optimization（パフォーマンスの最適化）] ルールを作成し、[Path or File（パスまたはファイル）] フィールドで **c:\temp2*** を指定します。ファイルの書き込み、変更、または削除がどのユーザーによって行われたかにかかわらず、その場所にあるファイルは Bit9 Server による追跡の対象から除外されます。これにより、サーバーで実行される処理や情報収集の量を削減できますが、それと同時に、そのディレクトリに書き込まれるすべてのファイルが追跡の対象から除外されることになります。

MyVirusGuard の実行可能ファイルが MVGuard.exe と名付けられている場合、このルールの [Process（プロセス）] フィールドに ***\MVGuard.exe** を追加すると、追跡を受けずに MyVirusGuard がこのディレクトリに書き込めるようになります。その他のプロセスによって c:\temp2\ に書き込まれたファイルは、引き続きサーバーによって追跡されます。プロセスを指定することにより、安全性を可能な限り維持したままこの目的を達成することができます。[Process (プロセス)] フィールドに入力されたプロセス名の前にアスタリスク ワイルドカードとスラッシュが付いているため、MVGuard.exe はどこにインストールされているかにかかわらず、追跡を受けずに指定されたディレクトリへいつでも書き込むことができます。



[Performance Optimization（パフォーマンスの最適化）] ルールの（表示されない）実行アクションは [**Default**（デフォルト）] であるため、c:\temp2 での「実行」は引き続き追跡され、他のルールによってブロックされている場合はブロックされます。つまり、指定されたプロセスによって試みられたファイルの「書き込み」のみが追跡を受けずに許可されます。

無視ルールとブロック ルールの組み合わせ

先ほどの例では、[Process Exclusion（除外するプロセス）] を使用して、通常はブロックされる場所への書き込みを特定のプロセスに対して許可していました。この方法に加え、2 つのルールを組み合わせて、例外ルールの優先順位をメイン ルールよりも高く設定することにより、特定のルールに対する例外を作成することもできます。

たとえば、**logs** サブフォルダーに **superapp.log** という名前のログ ファイルを作成する、Super App というプログラムがあるとします。この場合、プロセスの例外を作成する代わりに、アプリケーション フォルダーの残り部分を保護したままこのサブフォルダーへのファイルの書き込みを許可することができます。これを行うには、次のように設定された 2 つのルールを作成します。

- **無視ルール – <ProgramFiles>\superapp\logs*** への書き込みを無視して許可する [Performance Optimization（パフォーマンスの最適化）] ルールを作成します（自動的に選択されるアクションです）。
- **ブロック ルール**–パスとして<ProgramFiles>\superapp*を指定し、[Write Action（書き込みアクション）] として [Block（ブロック）] を指定した [File Integrity Control（ファイル整合性の制御）] ルールを作成し、許可ルールよりもランクを低く設定します。

[Performance Optimization（パフォーマンスの最適化）] ルールがブロック ルールよりも高くランクされているため、変更が試みられると、例外に一致するかどうかが最初に確認され、例外に一致した場合、ブロック ルールの評価は行われません。

第 13 章

スクリプト ルール

この章では、Bit9 Security Platform でスクリプトとして追跡、管理するファイルを識別するスクリプト ルールについて説明します。Bit9 Server にはさまざまなスクリプト ルールがあらかじめ用意されていますが、カスタム ルールを作成して他のスクリプトを指定することもできます。

セクション

概要

Bit9 Security Platform による追跡および管理の対象となるファイルには 2 種類あります。実行可能ファイルとスクリプトです。実行可能ファイルは Bit9 によるファイル内容の分析に基づいて識別されます。スクリプトは名前に基づいて識別されます。

スクリプトとは

スクリプトとは、スクリプト プロセッサーのコンテキストにおいてのみ実行または解釈が可能なコンテンツを含むファイルです。特定のホスト プロセスに依存する点で、スクリプトは一般的な実行可能ファイルと異なります。スクリプトでは次の 2 つの指定を行う必要があります。

- スクリプト タイプ: スクリプト ファイルの識別に必要なファイル パターン定義を指定します。
- スクリプト プロセッサー : スクリプト タイプに基づいて識別されたスクリプトを処理するファイルを指定します。プロセッサーに一致する文字列を指定することもできますが、Windows の場合は各エージェント コンピューターで管理されているファイルの関連付けリストを介して特定のスクリプト タイプに一致したファイルを処理するデフォルトのプロセッサーを決定することもできます。互換性のあるプロセッサーが複数存在する場合でも、各スクリプト タイプに対して指定できるプロセッサーは 1 つのみです。

スクリプト ファイルの例には、VisualBasic スクリプト（*.vbs）、バッチ スクリプト（*.bat、*.cmd）、シェル スクリプト（*.sh、*.csh など）があります。スクリプトは FireFox の XPI プラグインや Chrome の CRX 拡張機能のようにブラウザーのアドオンや拡張機能として追加される場合もあり、Word ドキュメント（*.docx）などのアプリケーション データ ファイルとして追加される場合もあります。スクリプト プロセッサーの例には、cmd.exe（バッチ スクリプト）、bash（シェル スクリプト）、wscript.exe（VisualBasic スクリプト）などに加え、firefox.exe、chrome.exe、word.exe のように一見スクリプト プロセッサーではないプロセスも含まれます。

スクリプト ファイルとプロセッサーは、文字列の一致によってルール内の指定と比較されます。

注意

- スクリプトの識別にファイル ハッシュは使用されません。スクリプト ファイルはハッシュ化されていますが、スクリプト ルールではファイル拡張子に基づいてスクリプトの識別が行われます。
- Bit9 Security Platformによる監視と制御の対象になるスクリプトは、ルール内での指定および定義が可能なスクリプト名とプロセッサー ファイル名を使用するスクリプトのみです。ブラウザー メモリー内で実行されるスクリプト処理（JavaScript など）は Bit9 スクリプト ルールによる制御の対象になりません。
- 一部のスクリプトは内容に基づいて識別され、スクリプト ルールではなく実行可能ファイル用のルールによって制御される場合があります。詳細については、「内容に名前に基づいて識別されるシェル スクリプト」（464 ページ）を参照してください。

Bit9 スクリプト ルールの動作

スクリプト ルールに一致したファイルに対して実行されるアクションには次の 2 種類があります。

- **可視性：**新しいファイルがエージェント コンピューターに追加されるか、新しいルールが作成されたことにより、ルールで指定されているスクリプト タイプに一致するファイルが新たに検出されると、そのファイルは［File Catalog（ファイル カタログ）］テーブルおよび［Files on Computers（コンピューター上のファイル）］テーブルに追加され、その時点から追跡されるようになります。スクリプト ファイルは名前に基づいて識別されますが、Bit9 による監視の対象として識別される他のファイルと同様にハッシュ化され、スクリプト ファイルのハッシュはファイル データベースに保存されます。
- **制御：**ルール内で指定されているスクリプト プロセッサーに一致するファイルが、同じルール内で指定されているスクリプト タイプとして識別されるファイルへのアクセスを試みると、スクリプトの実行が試みられているものと見なされます。有効なスクリプト ルールに一致するスクリプトの実行は、実行が試みられたコンピューターのポリシー設定と、その他の適用可能な Bit9 ルールに従って制御されます。

Bit9 によって識別されたスクリプトのファイル状態は、そのファイルが発見されたタイミングと、［Rescan Computers: Check to approve all existing scripts matching this definition（コンピューターの再スキャン：この定義に一致するすべての既存スクリプトを承認する場合はオンにします）］の設定によって異なります。［Rescan Computers（コンピューターの再スキャン）］チェックボックスがオフの場合、ルールで指定されているタイプのスクリプトが実行されると、それらのファイルはすべて未承認として扱われます。［Rescan Computers（コンピューターの再スキャン）］チェックボックスがオンの場合は、再スキャン時にエージェント管理コンピューター上に存在しているすべてのスクリプト ファイルがローカルで承認され、（明示的に禁止されていない限り）すべての適用レベルで実行が許可されま

す。再スキャン後に発見されたスクリプト ファイルは未承認と見なされ、適用レベルが［High（高）］または［Medium（中）］の場合は実行がブロックされます。

事前構成済みのスクリプト ルール

Bit9 Security Platform にはさまざまな標準スクリプト ルールが含まれ、その一部はデフォルトで有効になっています。［Script Rules（スクリプト ルール）］ページでは、既存のルールを有効化、無効化、または編集することができ、新しいカスタム スクリプト ルールを作成することもできます。

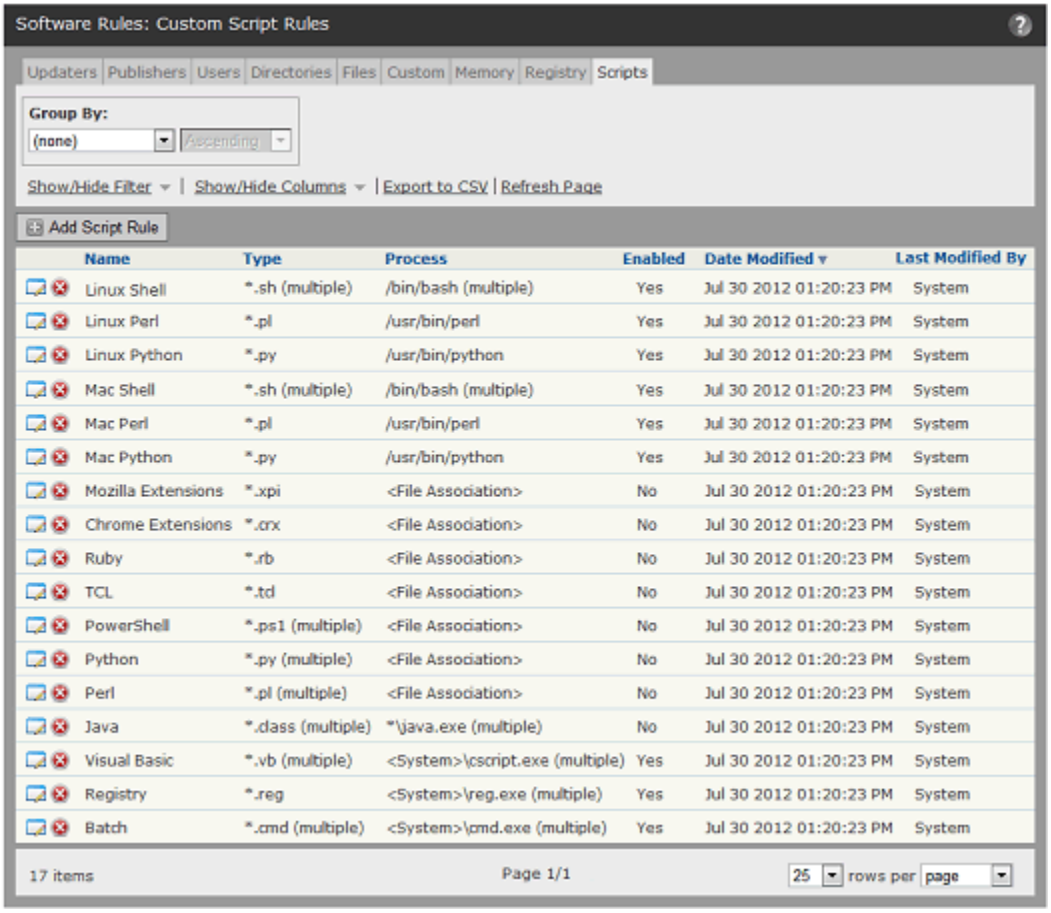


表 54 に標準のスクリプト ルールを示します。異なるルール間でファイル拡張子が共通している場合、ファイル拡張子の隣に記載されているプロセス名またはプロセス パスが異なります。

表 54：標準のスクリプト ルールとファイル拡張子

アプリケーションまたはカテゴリ	スクリプト拡張子	プロセス	プラットフォーム	デフォルトの状態
Linux シェル	.sh、.csh、.zsh、.ksh	/bin/bash、/bin/csh、/bin/ksh、/bin/sh、/bin/tcsh、/bin/zsh /bin/dash、/bin/static-sh、/bin/busybox	Linux	有効
Linux Perl	.pl	/usr/bin/perl	Linux	有効
Linux Python	.py	/usr/bin/python	Linux	有効
Mac シェル	.sh、.csh、.zsh、.ksh	/bin/bash、/bin/csh、/bin/ksh、/bin/sh、/bin/tcsh、/bin/zsh	Mac	有効
Mac Perl	.pl	/usr/bin/perl	Mac	有効
Mac Python	.py	/usr/bin/python	Mac	有効
バッチ	.cmd、.bat	<System>\cmd.exe <Systemx86>\cmd.exe	Windows	有効
レジストリ	.reg	<System>\reg.exe <Systemx86>\reg.exe <System>\regedt32.exe <Systemx86>\regedt32.exe <Windows>\regedit.exe <Systemx86\regedit.exe>	Windows	有効
Visual Basic	.vbs、.vb、.vbe、.wsf、.wsh	<System>\cscript.exe、 <Systemx86>\cscript.exe <System>\wscript.exe、 <Systemx86>\wscript.exe	Windows	有効
Java	.jar、.class	*\java.exe、*\javaw.exe	Windows	無効
Perl	.pl、.pm	< ファイルの関連付けに依存 >	Windows	無効
Python	.py、.pyc、.pyo	< ファイルの関連付けに依存 >	Windows	無効
PowerShell	.ps1、.psm1	< ファイルの関連付けに依存 >	Windows	無効
TCL	.tcl	< ファイルの関連付けに依存 >	Windows	無効

アプリケーションまたはカテゴリ	スクリプト拡張子	プロセス	プラットフォーム	デフォルトの状態
Ruby	.rb	< ファイルの関連付けに依存 >	Windows	無効
Chrome 拡張機能	.crx	< ファイルの関連付けに依存 >	Windows	無効
Mozilla 拡張機能	.xpi	< ファイルの関連付けに依存 >	Windows	無効

スクリプト ルールの優先順位と他の Bit9 ルールとの関係

スクリプト ルールで定義されているスクリプト ファイルには、一致する（スクリプト ルール以外の）カスタム ルールも適用され、書き込みを無視、実行または書き込みをブロック、プロンプト、許可、などのアクションが適用される可能性があります。たとえば、[Write Action（書き込みアクション）] が [Ignore（無視）] に設定されているカスタム ルールに一致したスクリプト ファイルのファイル状態は未承認に設定され、適用レベルが [High（高）] または [Medium（中）] の場合は実行がブロックされます。また、[Execute Action（実行アクション）] が [Allow（許可）] に設定されているカスタム ルールにスクリプト ファイルとそのプロセッサーが一致した場合は、ファイルの状態に関係なく実行が許可されます。

さらに、スクリプト ファイルはハッシュに基づいて禁止または承認することもできます。

内容に名前に基づいて識別されるシェル スクリプト

[Custom Script Rules（カスタム スクリプト ルール）] テーブルには、Mac および Linux 固有のシェル スクリプト ファイルに関するルールも含まれ、それらはデフォルトで有効になっています。通常、スクリプトは明示的なルールで指定されたファイル拡張子とプロセッサーに基づいて識別されますが、Mac および Linux のシェル スクリプトに関しては例外があります。

一部のシェル スクリプトでは、それらのスクリプトの処理に使用するデフォルトのインタープリターを指定する特殊なマークアップが 1 行目に含まれています。このマークアップは一般にハッシュバングまたはシェバンと呼ばれ、シャープ記号 (#) と感嘆符 (!) で構成されています。以下に例を示します。

```
#!/bin/bash
```

これは、このスクリプト ファイルの処理に /bin/bash インタープリターを使用する必要があることを示しています。

シェバン マークアップを含むファイルはBit9で追跡する必要があることが明らかであるため、一致するスクリプト ルールがあるかどうかにかかわらず、このマークアップを含むシェル スクリプトは内容に基づいて識別され、追跡されます。つまり、このマークアップが検出されると、そのファイルをスクリプトとして識別

し、シェバン マークアップで指定されているインタープリターをプロセッサーとして識別する不可視のスクリプト ルールが作成されます。

シェバン パターンを含む Mac および Linux シェル スクリプトに Bit9 ルールがどのように適用されるかは、スクリプトがどのように実行され、一致するカスタム スクリプト ルールが効力を持つかどうかによって異なります。

- **スクリプトがコマンドとして使用された場合 –** スクリプト ファイルがコマンドとして実行された場合は、シェバンで指定されているプロセッサーが使用され、スクリプトではなく実行可能ファイルを制御するポリシー設定に基づいて制御されます。次に例を示します。

  ```
  $ ./foo.sh
  ```

  この方法でスクリプトを実行するには、オペレーティング システム内でスクリプト自体に実行許可が与えられている必要があります。
- **定義されているプロセッサーとスクリプトの組み合わせがコマンドとして使用された場合 –** プロセッサーをコマンドとして使用し、スクリプト ファイルを引数として使用してスクリプト ファイルが実行され、その組み合わせがシェバンまたはカスタム スクリプト ルールで定義されている場合、そのアクションはスクリプト用のポリシー設定に基づいて制御されます。次に例を示します。

  ```
  $ csh ./foo.sh
  ```

  この場合、スクリプト ファイル自体の実行許可は必要ありません。
- **定義されていないプロセッサーとスクリプトの組み合わせがコマンドとして使用された場合 –** ファイルのシェバン パターンとカスタム スクリプト ルールで定義されていないプロセッサーを使用してスクリプト ファイルが実行された場合、そのファイル自体が追跡の対象となるスクリプトとして識別されているかどうかにかかわらず、そのスクリプト アクションはスクリプト用のポリシー設定に基づく制御を受けません。これには、シェバン パターンを含むスクリプト ファイルが他のプロセッサーを使用して実行された場合も含まれます。

スクリプト ルールのポリシー設定

カスタム ルール、レジストリ ルール、メモリ ルールとは異なり、スクリプト ルールではアクションの指定を行いせん。スクリプト ルールは主に、既に Bit9 Security Platform での追跡とアクション ルールの対象になっているカテゴリのファイルに対して機能します。各ポリシーには、そのポリシーに含まれるコンピューター上でスクリプト ファイルをどのように制御するかを指定する高度な設定が 2 種類あります。

- **［Block unanalyzed scripts and executables（未分析のスクリプトおよび実行可能ファイルをブロック）］:** この設定では、Bit9 Security Platform でまだ分析されていないスクリプトと実行可能ファイルをブロックするかどうか指定します（コンピューター上で初期化がまだ完了していない場合など）。また、この設定には、そのようなファイルがブロックされたときに表示される通知を変更または無効にするためのメニューとリンクがあります。
- **［Block unapproved scripts（未承認スクリプトをブロック）］:** この設定では、適用レベルが［High（高）］または［Medium（中）］に設定されているコンピューター上でファイルの状態が未承認に設定されているスクリプトの実行

を許可するかどうかを指定します。また、この設定には、そのようなファイルがブロックされたときに表示される通知を変更または無効にするためのメニューとリンクがあります。

スクリプトは、スクリプト用のポリシー設定ではなく、実行可能ファイル用のポリシー設定によって制御される場合があることに注意してください。詳細については、「内容に名前に基づいて識別されるシェル スクリプト」を参照してください。

関連トピック

ポリシー内のスクリプト固有の設定項目については、表 20「高度な設定の動作」191 ページを参照してください。

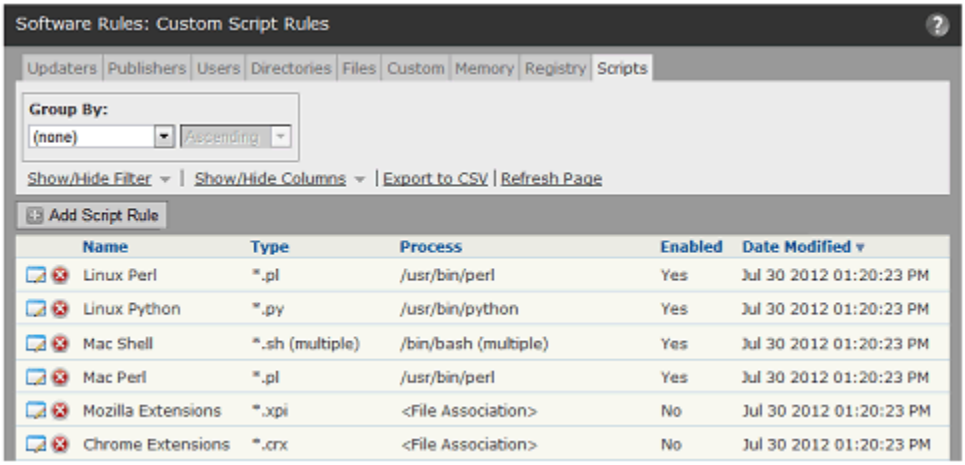
スクリプトがブロックされたときに表示される通知の設定については、第 17 章「ブロック通知と承認要求」を参照してください。

カスタム スクリプト ルールの作成

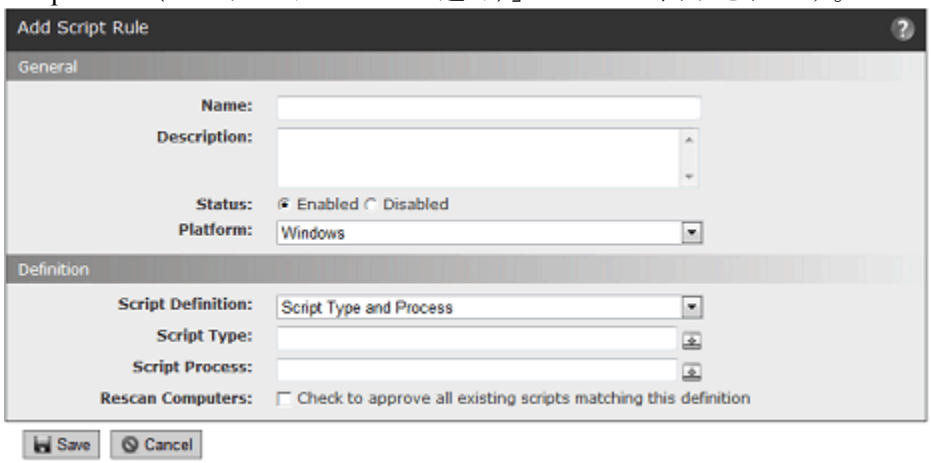
以下の手順は、カスタム スクリプト ルールの作成方法に関する説明です。ルールのパラメーターについては、表 55 を参照してください。

カスタム スクリプト ルールの追加（作成）手順：

1. コンソール メニューで［**Rules**（ルール）］>［**Software Rules**（ソフトウェア ルール）］を選択し、［Software Rules（ソフトウェア ルール）］ページで［**Scripts**（スクリプト）］タブをクリックします。［Custom Script Rules（カスタム スクリプト ルール）］テーブルが表示されます。



2. ［**Add Script Rule**（スクリプト ルールの追加）］ボタンをクリックします。［Add Script Rule（スクリプト ルールの追加）］ページが表示されます。



3. ［Name（名前）］フィールドに名前を入力します。この名前はルールのリストに表示されます。任意で［Description（説明）］フィールドに詳細な説明を入力することもできます。
4. 新しいスクリプト ルールを設定して［Save（保存）］をクリックすると、そのスクリプト ルールのステータスはデフォルトで［**Enabled**（有効）］になります。作成したルールを後から有効にする場合は、［Status（ステータス）］フィールドで［**Disabled**（無効）］をクリックします。
5. ［Platform（プラットフォーム）］フィールドで、［**Windows**］、［**Mac**］、または［**Linux**］を選択します。スクリプト ルールはすべて 1 種類のプラットフォームのみに適用されます。
6. ［Script Definition（スクリプト定義）］でスクリプト プロセッサーの識別方法を選択します。選択肢については、表 55 を参照してください。
プラットフォームに関する注意：Mac または Linux スクリプトの場合、選択できるオプションは［**Script Type and Process**（スクリプト タイプとプロセス）］のみです。
7. 各スクリプト ルールでは、［Script Types（スクリプト タイプ）］を 1 つまたは複数入力できます。［Script Type（スクリプト タイプ）］フィールドには、そのスクリプト タイプのファイル名定義を入力します（通常はアスタリスクの後にドットを入力し、その後にファイル拡張子を入力します）。スクリプト タイプを追加するには、［Script Types（スクリプト タイプ）］フィールドにパターンを入力し、フィールドの右にある［**Add**（追加）］ボタンをクリックして新しいパターンを追加していきます。
8. ［Script Type and Process（スクリプト タイプとプロセス）］を指定するルール（Window のみ）の場合は 、スクリプト プロセスも 1 つ以上追加する必要があります。ルール内のプロセスごとに［Script Process（スクリプト プロセス）］フィールドにプロセス定義を入力し、フィールドの右にある［**Add**（追加）］ボタンをクリックします。

9. この定義に一致するすべての既存スクリプトが Bit9 Security Platform による追跡と制御の対象となるファイルのリストに確実に追加されるようにするには、[**Rescan Computers**（コンピューターの再スキャン）] チェックボックスをオンにします。
10. [**Save**（保存）] ボタンをクリックしてルールを保存します。作成されたルールが [Script Rules（スクリプト ルール）] ページに表示されます。

表 55：スクリプト ルールのパラメーター

フィールド	説明
[Name（名前）]	[Script Rules（スクリプト ルール）] ページに表示されるこのルールの名前。（必須）
[Description（説明）]	ルールに関する追加情報。任意のテキストを入力できます。（オプション）
[Status（ステータス）]	このルールを有効または無効にするラジオ ボタン。これらのラジオ ボタンを使用することで、特定の場合にのみ使用するルールを作成したり、定義を維持したままルールを一時的に無効にしたりできます。
[Platform（プラットフォーム）]	このスクリプト ルールが適用されるプラットフォーム（Windows、Mac、または Linux）。各スクリプト ルールは、1 種類のプラットフォームのみに適用されます。
[Script Definition（スクリプト定義）]	スクリプト ルールの定義方法。メニューには以下の選択肢があります。 [**File Association**（ファイルの関連付け）] – エージェント コンピューターのファイルの関連付けリストを使用してスクリプト プロセスを決定する場合はこの定義を選択します。このオプションを選択した場合でも [Script Type（スクリプト タイプ）]（ファイル名）を指定することは可能です。 一般的なスクリプト タイプを対象とするルールの場合は、さまざまなバージョンのスクリプト エンジン（異なるバージョンの Perl など）が環境内にインストールされている可能性があるため、[File Association（ファイルの関連付け）] を選択したほうがよい場合があります。ただし、個々のコンピューター上に複数のバージョンのスクリプト エンジンがインストールされている場合は、ファイルの関連付けで指定されているバージョンのみが Bit9 によって管理されることになるため、このオプションが必ずしも最善の選択であるとは限りません。この選択を行う前に、環境内の現状を十分に確認してください。 **プラットフォームに関する注意**：[File Association（ファイルの関連付け）] を使用できるのは Windows スクリプトのみです。 [**Script Type and Process**（スクリプト タイプとプロセス）] – スクリプトを定義するファイル パターンとスクリプトを実行するプロセスを両方とも指定する場合はこの定義を選択します。

フィールド	説明
[Script Type（スクリプト タイプ）]	このルールに一致したファイルをスクリプトと見なすかどうかを決定するファイル名パターン。大半の標準ルールでは、スクリプトと見なすファイルの拡張子（*.vbs など）を使用してスクリプト タイプが定義されています。スクリプト タイプの指定では、パス、ワイルドカード、およびマクロを使用できます。Bit9 ルールのパターン定義オプションの概要については、「パスとプロセスの指定」（420 ページ）を参照してください。
[Script Process（スクリプト プロセス）]	指定されたスクリプト タイプに一致するファイルを処理する際の動作を制御する必要がある実行可能ファイル。スクリプト プロセッサーの例には、wscript.exe（Visual Basic スクリプト）、cmd.exe（バッチ スクリプト）、ps.exe（PowerShell スクリプト）などに加え、firefox.exe、chrome.exe、word.exe のように一見スクリプト プロセッサーではないプロセスも含まれます。スクリプト プロセスの指定では、パス、ワイルドカード、およびマクロを使用できます。Bit9 ルールのパターン定義オプションの概要については、「パスとプロセスの指定」（420 ページ）を参照してください。
[Rescan Computers（コンピューターの再スキャン）]	このチェックボックスがオンになっている場合は、サーバーに接続されているすべての Bit9 エージェント コンピューターの再スキャンが実行され、このスクリプト ルールに一致するファイルが検索されます。一致するファイルが見つかった場合は［File Catalog（ファイル カタログ）］に追加され、ファイルの状態が承認済みに設定されます。このチェックボックスがオフになっている場合、ルールに一致するスクリプト ファイルはすべて未承認になります。接続されていないコンピューターは再接続されたときに「再スキャン」ルールを受信し、再スキャンが実行されます。次の点に注意してください。 • 新規ルールまたは既存ルールで［Rescan Computers（コンピューターの再スキャン）］を有効にすると遅延が発生し、その間はローカルのスクリプトが承認されない可能性があります。 • Bit9 エージェントに対してルールを無視するように指示するカスタム ルールに一致したスクリプト ファイルは引き続き無視されます。
[History（履歴）]	既存ルールの場合はページの下部に［History（履歴）］パネルが表示され、ルールの作成日、作成者、最終更新日、最終更新者が表示されます。

重要

パフォーマンスに悪影響が及ぶため、きわめて広範囲に適用される定義を［Script Type（スクリプト タイプ）］または［Script Process（スクリプト プロセス）］フィールドで使用することは推奨されません。ルール内のいずれかのフィールドで * または *.* が使用されている場合はページ上に警告が表示されます。スクリプト ルールでファイル パターンを定義する際には、できるだけ狭い範囲に限定されたパターンを使用してください。

スクリプト ルールの編集

スクリプト ルールの編集は次のような場合に必要になることがあります。

- スクリプトを有効または無効にする場合（スクリプトを有効または無効にした場合の効果については、「スクリプト ルールの無効化と削除」（470 ページ）を参照してください）
- スクリプトまたはプロセッサーの識別に使用するパターンを追加、削除、または変更する場合
- スクリプト プロセッサーの識別にファイルの関連付けを使用するようにスクリプト定義を変更する場合、またはファイルの関連付けではなく特定のプロセッサー パターンを使用するようにスクリプト定義を変更する場合

スクリプト ルールの編集手順：

1. コンソール メニューで、[**Rules**（ルール）] > [**Software Rules**（ソフトウェア ルール）] の順に選択します。[Software Rules（ソフトウェア ルール）] ページが表示されます。
2. [Software Rules（ソフトウェア ルール）] ページで [**Scripts**（スクリプト）] タブをクリックします。[Custom Script Rules（カスタム スクリプト ルール）] テーブルが表示されます。
3. 編集するルールの左にある [View Details（詳細の表示）] アイコン（鉛筆とファイル）をクリックします。[Edit Custom Script Rule（カスタム スクリプト ルールの編集）] ページが表示されます。
4. 必要に応じてルールを編集し（パラメーターの詳細については、表 55 を参照してください）、[Save（保存）] をクリックします。[Edit Custom Rule（カスタム ルールの編集）] ページが閉じ、[Custom Script Rules（カスタム スクリプト ルール）] ページが表示されます。

スクリプト ルールの無効化と削除

不要になったスクリプト ルールはスクリプト ルール テーブル内に残したまま無効化することも、テーブルから削除することもできます。無効化または削除されたスクリプト ルールは、新たに検出されたファイルに対しては適用されません。ただし、ルールが有効化されていた間に検出されたスクリプト ファイルは引き続き Bit9 によって追跡され、ルールが有効化されていたときに適用されたファイル状態はそのまま維持されます。

スクリプト定義を無効にしても、ルールに一致するファイルは、Bit9 によって追跡されているファイルのインベントリからはすぐに削除されません。この動作は、ルール変更などのアクションが誤って行われた場合などに情報の消失を防ぐことを目的としています。ただし、無効化されたルールに一致するスクリプト ファイルがインベントリ内に残される期間は、そのファイルが実際にエージェントから削除されたり変更されるなどの要因に基づいて変化します。

一度無効化された定義が後で有効化され、再スキャンが有効になっている場合は、新たに検出されたスクリプトのみがローカルで承認されます。インベントリ内に残っていたスクリプトの状態は以前の状態のまま維持されます。

同じルールを将来再び使用する可能性がある場合は、一時的に無効にすることをお勧めします。

スクリプト ルールの無効化手順：

1. コンソール メニューで［**Rules**（ルール）］>［**Software Rules**（ソフトウェア ルール）］を選択し、［Software Rules（ソフトウェア ルール）］ページが表示されたら［**Scripts**（スクリプト）］タブをクリックします。［Custom Script Rules（カスタム スクリプト ルール）］テーブルが表示されます。
2. 無効にするルールの隣にある［Edit（編集）］ボタン（鉛筆とファイル）をクリックします。［Edit Script Rule（スクリプト ルールの編集）］ページが表示されます。
3. ［Status（ステータス）］行にある［**Disabled**（無効）］ラジオ ボタンをクリックし、ページの下部にある［Save（保存）］ボタンをクリックします。ルールが無効になります。

ルールを完全に削除した場合、削除を取り消したり、削除したルールを復元することはできません。本当にルールを削除してもよいかどうかを事前に必ず確認してください。Bit9 で事前構成済みのルールを削除することは推奨されません。

スクリプト ルールの削除手順：

1. コンソール メニューで［**Rules**（ルール）］>［**Software Rules**（ソフトウェア ルール）］を選択し、［Software Rules（ソフトウェア ルール）］ページが表示されたら［**Scripts**（スクリプト）］タブをクリックします。［Custom Script Rules（カスタム スクリプト ルール）］テーブルが表示されます。
2. 削除するルールの隣にある［Delete（削除）］ボタン（X と書かれている赤い丸）をクリックし、確認ダイアログで **[OK]** をクリックします。ルールが削除されます。

コンピューターでのルール ステータスの表示

Bit9 Server で管理されているエージェントの数と接続されていないエージェントの数によっては、すべてのエージェントに新しいルールや更新されたルールがすぐに配信されない場合があります。有効になっているルールの［Edit（編集）］ページにある［Related Views（関連ビュー）］メニューには、［Computers（コンピューター）］ページの 2 種類のフィルター済みビューへのリンクがあり、エージェント管理コンピューターでのルールのステータスを確認できます。以下の選択肢があります。

- **［All Computers that have received this rule（このルールを既に受信したすべてのコンピューター）］**
- **［All Computers that have not yet received this rule（このルールをまだ受信していないすべてのコンピューター）］**

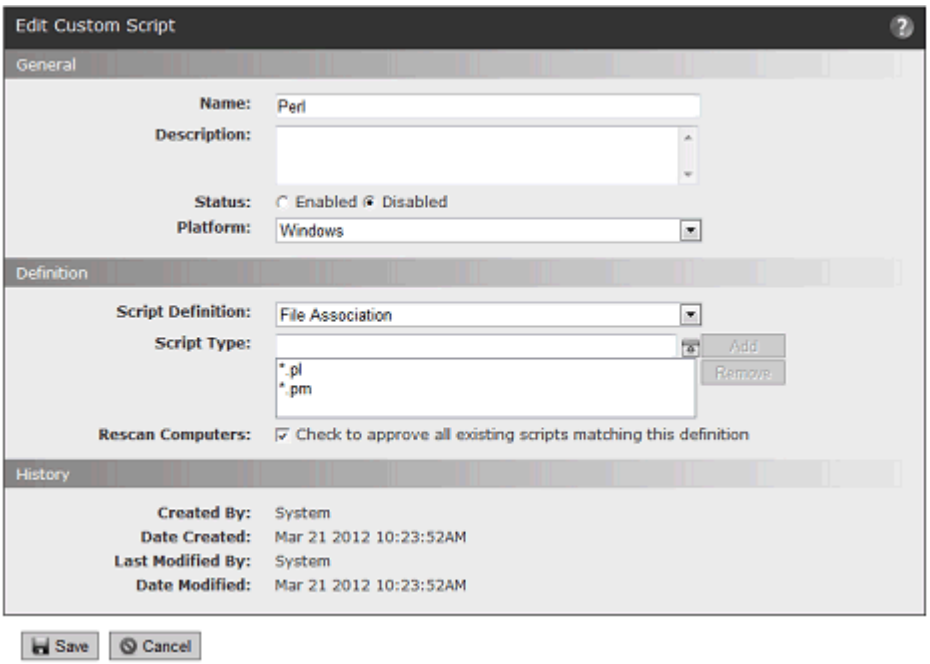
一度も有効化されたことがないルールの場合、このメニューは表示されません。

スクリプト ルールの例

Bit9 Security Platform にはさまざまな事前構成済みのスクリプト ルールが含まれています。これらは他のルールを作成する際の例として役立ちます。

例：Windows Perl スクリプト

Perl スクリプトの実行を追跡して制御する Windows スクリプト ルールがあらかじめ用意されています。[Software Rules（ソフトウェア ルール）] ページの [Scripts（スクリプト）] タブで Perl ルールの隣にある [Edit（編集）] ボタン（鉛筆とファイル）をクリックすると、このルールがどのように定義されているかを確認できます。



[Script Type（スクリプト タイプ）] フィールドでは 2 つのパターン（*.pl と *.pm）が指定されています。これらの拡張子で終わるファイルは Perl スクリプト ファイルと見なされ、検出されると Bit9 によって追跡されます。

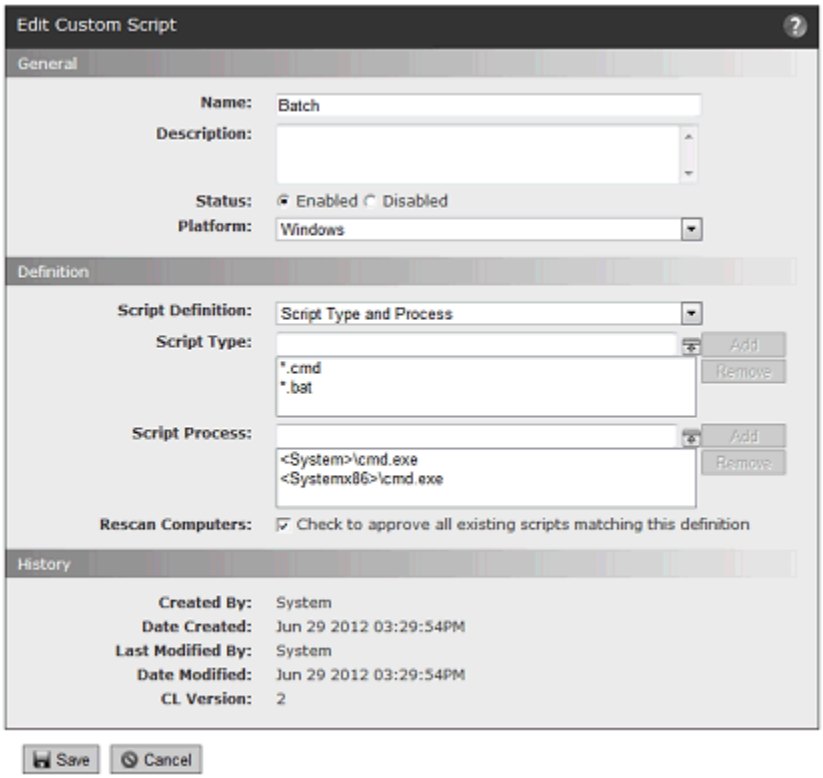
[Script Definition（スクリプト定義）] フィールドでは [File Association（ファイルの関連付け）] が選択されています。そのため、スクリプト プロセッサーの一致パターンを指定する必要はありません。このルールでは、各エージェント コンピューター上で Perl プロセッサーとして指定されているアプリケーション ファイルがスクリプト プロセッサーとして使用されます。*.pl または *.pm ファイルに関連付けられたアプリケーションがそれらのファイルへのアクセスを試みるたびに、エージェントは、スクリプト ファイルの現在の状態、実行が試みられたコンピューターのポリシー設定、およびスクリプト ファイルに影響するその他のルールに基づいてスクリプトの実行を制御します。

このルールでは [Rescan Computers（コンピューターの再スキャン）] チェックボックスがオンになっています。そのため、このルールが有効になると、Bit9 Server で管理されているすべてのコンピューターが再スキャンされ、このルール

で指定されているスクリプト タイプに一致するファイルがローカルで承認されて［File Catalog（ファイル カタログ）］と［Files on Computers（コンピューター上のファイル）］リストに追加されます。このチェックボックスをオフにすると、指定されているスクリプト タイプに一致するすべてのファイルが未承認として扱われます。ルールに一致する他のスクリプト ファイルは、実行が試みられたときに「発見」され、ローカルで承認されないため、ブロックされる可能性があります。

例：Windows バッチ スクリプト

Bit9 Security Platform には、Windows バッチ スクリプトの実行を識別して制御するスクリプト ルールが用意されています。［Software Rules（ソフトウェア ルール）］ページの［Scripts（スクリプト）］タブでバッチ ルールの隣にある［Edit（編集）］ボタン（鉛筆とファイル）をクリックすると、このルールがどのように定義されているかを確認できます。



バッチ ルールの［Script Type（スクリプト タイプ）］フィールドでは 2 つのパターン（*.cmd と *.bat）が指定されています。これらの拡張子で終わるファイルはバッチ スクリプト ファイルと見なされ、検出されると Bit9 によって追跡されます。

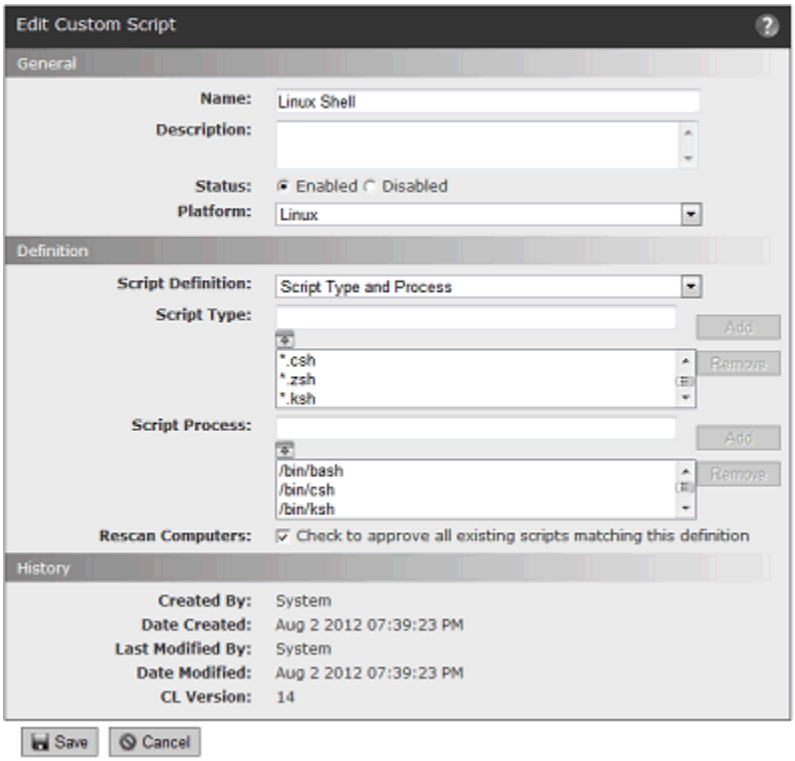
［Script Definition（スクリプト定義）］フィールドでは［Script Type and Process（スクリプト タイプとプロセス）］が選択されているため、［Script Process（スクリプト プロセス）］でパターンを少なくとも 1 つ指定する必要があります。このルールでは、*cmd.exe* が 32 ビット システムと 64 ビット システムの両方でこのスクリプトのプロセッサーとして識別されるように2つのプロセスが指定されています。

このルールを有効にすると、(指定された場所にある) cmd.exe が .cmd または .bat 拡張子を持つファイルへのアクセスを試みるたびに、エージェントは、スクリプト ファイルの現在の承認状態、実行が試みられたコンピューターのポリシー設定、およびスクリプト ファイルに影響するその他のルールに基づいてスクリプトの実行を制御します。

このルールでは［Rescan Computers（コンピューターの再スキャン）］チェックボックスがオンになっているため、このルールが有効になると、Bit9 Server で管理されているすべてのコンピューターの再スキャンが実行されて、このルールで指定されているスクリプト タイプに一致するファイルがローカルで承認され、［File Catalog（ファイル カタログ）］と［Files on Computers（コンピューター上のファイル）］リストに追加されます。

例：Linux シェル スクリプト

Bit9 Server には Linux コンピューター上でのネイティブ シェル スクリプトの実行を識別して制御するスクリプト ルールが用意されています。［Software Rules（ソフトウェア ルール）］ページの［Scripts（スクリプト）］タブで Linux シェル ルールの隣にある［Edit（編集）］ボタン（鉛筆とファイル）をクリックすると、このルールがどのように定義されているかを確認できます。



Linux シェル ルールの［Script Type（スクリプト タイプ）］フィールドではいくつかのパターン（*.sh、*.csh、*.zsh、*.ksh）が指定されています。これらの拡張子で終わるファイルはシェル スクリプト ファイルと見なされ、検出されると Bit9 Server によって追跡されます。

［Script Definition（スクリプト定義）］フィールドでは［Script Type and Process（スクリプト タイプとプロセス）］が選択されています（Mac および Linux 用のルールで選択できるのは、このオプションのみです）。このルールでは、サポートされている Linux プラットフォームでのネイティブ スクリプトの処理をサポートする多数のプロセスが指定されています。必要な場合は、このルールのプロセッサー（またはスクリプト タイプ）を追加または削除できます。

このルールを有効にすると、指定されているプロセッサーが、指定されている拡張子（.sh など）を持つファイルへのアクセスを試みるたびに、Bit9 Server は、スクリプト ファイルの現在の承認状態、実行が試みられたコンピューターのポリシー設定、およびスクリプト ファイルに影響するその他のルールに基づいてスクリプトの実行を制御します。

このルールでは［Rescan Computers（コンピューターの再スキャン）］チェックボックスがオンになっているため、このルールが有効になると、Bit9 Server で管理されているすべてのコンピューターの再スキャンが実行されて、このルールで指定されているスクリプト タイプに一致するファイルがローカルで承認され、［File Catalog（ファイル カタログ）］と［Files on Computers（コンピューター上のファイル）］リストに追加されます。

第 14 章

レジストリ ルール

この章では、指定されたパスに一致する Windows レジストリの場所で変更が試みられた場合の動作を制御するレジストリ ルールについて説明します。レジストリ ルールの適用対象は、特定のユーザーや特定のプロセスのみに制限することもできます。

プラットフォームに関する注意：レジストリ ルールは Windows オペレーティング システムを実行しているコンピューターのみに適用されます。

セクション

概要

レジストリ ルールを使用すると、指定されたパスに一致する Windows レジストリ内の場所への書き込みが試みられたときに、書き込みをブロック、レポート、または許可するか､ユーザーに選択を促すプロンプトを表示することができます。キーまたは値の作成、変更、削除はすべて「書き込み」と見なされます。

レジストリ ルールに関連するイベント（レジストリ ルールによる書き込みのブロックなど）のリストを表示するには、[Events（イベント）] ページに移動し、[Saved Views（保存済みビュー)] メニューから [Registry（レジストリ)] を選択します。

注意

可視性モード ポリシーに含まれるコンピューターの場合、書き込みをブロックするレジストリ ルールまたはユーザーにプロンプトを表示するレジストリ ルールはレポートのみを行うルールとして扱われ､書き込みのブロックまたはプロンプトの表示は行われません。

ルールの適用範囲

Windows コンピューター上でレジストリの変更を試みたすべてのユーザーおよびプロセスに適用されるレジストリ ルールを作成できます。また、次の条件を指定して、適用範囲を絞り込んだルールを作成することもできます。

- **プロセス別** – 特定のプロセスが指定された場所への書き込みを試みた場合にのみルールを適用できます。
- **ユーザー別またはグループ別** – 特定のユーザーまたはユーザー グループのみにルールを適用できます。
- **ポリシー別** – 指定されたポリシーに含まれるコンピューターのみにルールを適用できます。
- **ルールの順序** – レジストリ ルールは[Registry Rules（レジストリ ルール)]テーブルにデフォルトで表示される [Rank（ランク）] 列の値順に評価されます。ランクが「1」に設定されているルールが最優先され､「2」に設定されているルールがその次に優先されます。ルールの順番は変更できます。たとえば、特定のユーザーが特定のレジストリ パスへのアクセスを試みたときに適用されるルールを作成し、その他のユーザーがそのパスへのアクセスを試みたときに適用されるルールよりも上に置くことができます。

重要

予期しない影響を防ぐため、レジストリ ルールの適用範囲はできるだけ狭い範囲に限定することを推奨します。

サンプル ルール

新規にインストールされたBit9 Serverには事前構成済みのレジストリ ルールが含まれ、デフォルトでは無効になっています。これらのルールを表示するには、

［Software Rules（ソフトウェア ルール）］ページの［Registry（レジストリ）］タブをクリックします。これらのルールの一部はそのまま有効にすることもできますが、独自のルールを作成するための見本としても使用できます。自動起動ルール（このルールもデフォルトでは無効になっています）は、起動時に影響を受ける可能性があるレジストリ内のさまざまな場所を保護します。ルールの設定方法の例については、「サンプル レジストリ ルール」（494 ページ）を参照してください。

レジストリ ルールのエクスポートとインポート

レジストリ ルールはサーバーからエクスポートして別のサーバーにインポートできます。［Registry Rules（レジストリ ルール）］ページには、この目的に使用できるボタンがあります。詳細については、「カスタム ルール」の章で「ルールのエクスポートとインポート」（441 ページ）を参照してください。

レジストリ ルールの通知の指定

Bit9 エージェントには、ルールによってアクションがブロックされた場合、またはアクションを許可するかブロックするかの選択をユーザーに促す場合に通知を表示する機能があります。レジストリ ルールごとに、次の 2 種類の通知ソースからいずれかを選択できます。

- ［**Use Policy Specific Notifier**（ポリシー固有の通知を使用）］– 各ポリシーの［Advanced Setting（高度な設定）］には［Enable registry rules（レジストリ ルールを有効化）］が含まれ、この項目は常にオンになっています。この設定の［Notifier（通知）］フィールドでは、レジストリ ルールによってアクションがブロックされたときにエージェント コンピューター上で表示する通知を指定できます。また、このポリシー設定で［<none>（なし）］を選択すると、プロンプトを表示するように設定されたルールも含め、特定のポリシー内でレジストリ ルールに関する通知を表示しないようにすることができます。ポリシー固有の通知はすべてのレジストリ ルールに割り当てることができます。詳細については、「高度な設定」（189 ページ）を参照してください。
- ［**Custom Notifier**（カスタム通知）］– ポリシー固有の通知を使用しない場合は、レジストリ ルールごとに通知を選択（または作成）できます。選択肢は、［Add/Edit Registry Rule（レジストリ ルールの追加 / 編集）］ページのメニューに表示されます。プロンプトを表示するように設定されたルールで［Custom Notifier（カスタム通知）］を選択した場合は、必ず通知を表示する必要があります。書き込みをブロックするように設定されたルールで［Custom Notifier（カスタム通知）］を選択した場合は、［<none>（なし）］を選択して通知を表示しないようにすることもできます。

レジストリ ルール通知の設定項目については、下記の表 56 を参照してください。通知の詳細については、第 17 章「ブロック通知と承認要求」を参照してください。

レジストリ ルールの作成

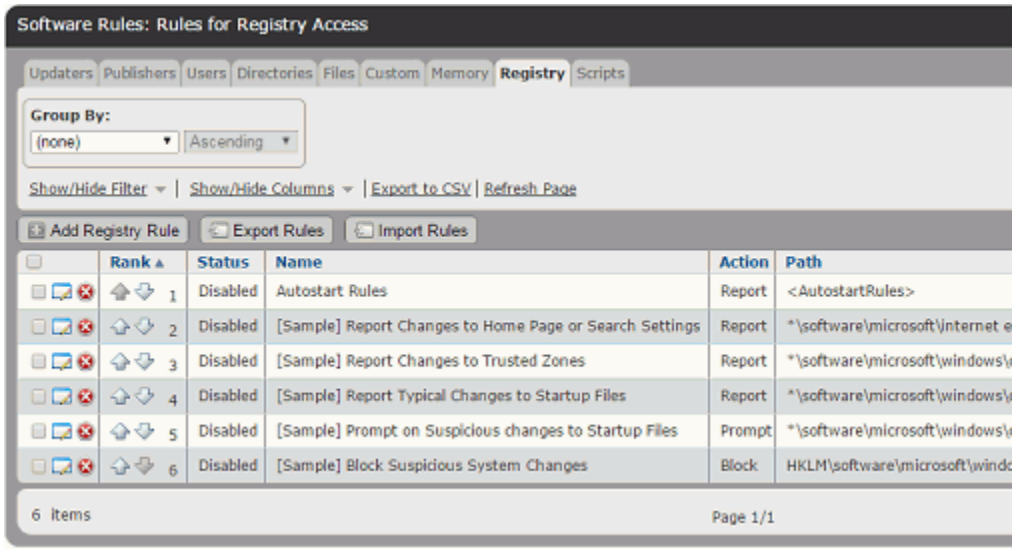
レジストリ ルールを作成するには、ルール名を指定した後、下の表の左列に太字で示されている情報を、右列に示されている［Add Registry Rule（レジストリ ルールの追加）］ページ内の場所に入力する必要があります。

概要	［Add/Edit Registry Rule（レジストリ ルールの追加 / 編集）］ページのフィールド
この（これらの）ソース プロセス …	［Process（プロセス）］
… および / または**この（これらの）ユーザー**が …	［User or Group（ユーザーまたはグループ）］
…Windows レジストリ内の**この（これらの）場所**に対して …	［Registry Path（レジストリ パス）］
… **この（これらの）ポリシー**に含まれるコンピューター上で変更を試みた場合 …	［Rule applies to:（ルールの適用先：）］
… **このアクション**を実行します。	［Write Action（書き込みアクション）］

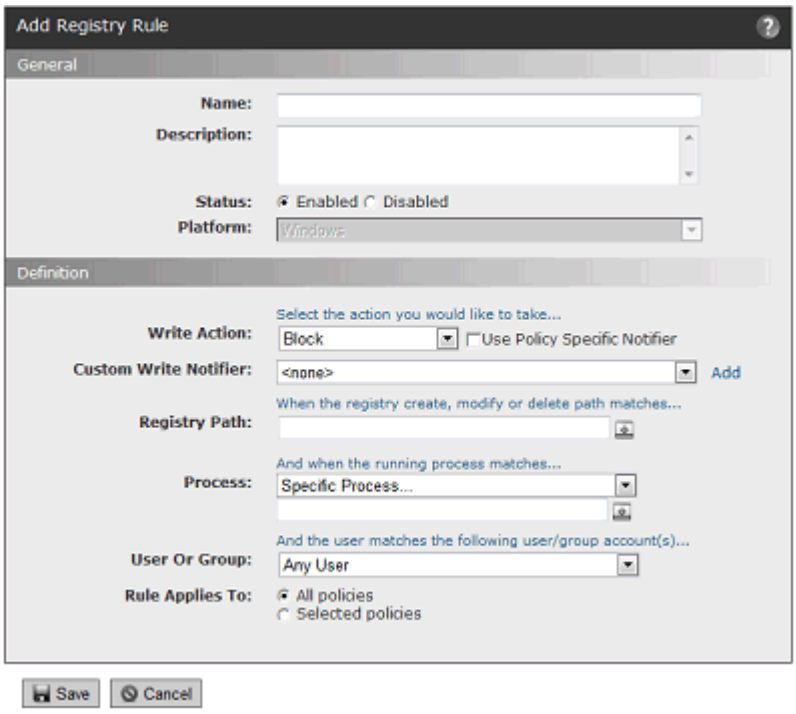
これらのパラメーターでは複数の項目を指定でき、そのクラスに含まれるすべての項目を指定することもできます（たとえば、すべてのユーザー、すべてのポリシー、またはすべてのソース プロセスにルールを適用できます）。

レジストリ ルールの追加（作成）手順：

1. コンソール メニューで、[**Rules**（ルール）] > [**Software Rules**（ソフトウェア ルール）] の順に選択します。[Software Rules（ソフトウェア ルール）] ページが表示されます。
2. レジストリ タブ、またはページの左にあるメニューで [**Registry Rules**（レジストリ ルール）] をクリックします。[Registry Rules（レジストリ ルール）] ページが表示されます。



3. 新しいルールを作成するには、[**Add Registry Rule**（レジストリ ルールの追加）] ボタンをクリックします。[Add Registry Rule（レジストリ ルールの追加)] ページが表示されます。



4. [Name（名前)] フィールドに名前を入力します。この名前はルールのリストに表示されます。
5. ルールの目的や他のルールとの関係など、ルールに関するコメントを追加する場合は、[Description（説明)] を入力することもできます。
6. 新しいルールはデフォルトで [**Enabled**（有効）] になっています。ルールを後から有効にする場合は、[Status（ステータス)] フィールドで [**Disabled**（無効)] をクリックします。
7. このルールに必要なその他の情報(表 56、「レジストリ ルールのパラメーター」483 ページを参照）を入力して、[Save（保存)] をクリックします。新しく作成されたルールが [Registry Rules（レジストリ ルール)] テーブルの末尾に表示されます。[Registry Rules（レジストリ ルール）] テーブルが複数ページにわたる場合は、新しいルールを確認できるように最後のページが表示されます。
8. このルールの優先順位を変更する場合は、[Rank（ランク）] 列の矢印を使用するかドラッグアンドドロップを使用して適切なランクに移動します。詳細については、「ルールのランキング」（492 ページ）を参照してください。

レジストリ ルールのパラメーター

表 56 に、[Add/Edit Registry Rule（レジストリ ルールの追加 / 編集）] ページで設定可能なパラメーターを示します。

表 56：レジストリ ルールのパラメーター

フィールド	説明
[Name（名前）]	[Registry Rules（レジストリ ルール）] ページに表示されるこのルールの名前。（必須）
[Description（説明）]	レジストリ ルールに関する追加情報。任意のテキストを入力できます。
[Status（ステータス）]	このルールを有効または無効にするラジオ ボタン。これらのラジオ ボタンを使用することで、特定の場合にのみ使用するルールを作成したり、ルールの作成時に使用した情報を維持したままルールを一時的に無効にしたりできます。
[Platform（プラットフォーム）]	このルールが適用されるプラットフォーム。このフィールドの値は変更できず、常に [Windows] が選択されています。レジストリ ルールは Windows 以外のプラットフォームには影響を与えません。
[Write Action（書き込みアクション）]	このルールに一致する書き込みが試みられた場合に適用するアクション。選択できるアクションについては、表 57 を参照してください。書き込みルールはすべての Windows プラットフォーム（ただし 64 ビット版の Windows Server 2003 を除く）におけるレジストリへのアクセス許可の変更も制御します。
[Use Policy Specific Notifier（ポリシー固有の通知を使用）]	[Write Action（書き込みアクション）] として [Block（ブロック）] または [Prompt（プロンプト）] を選択した場合は、このチェックボックスが [Write Action（書き込みアクション）] オプションの右に表示されます。このチェックボックスがオンになっている場合、レジストリ ルールによってアクションがブロックされたときに表示される通知は、アクションがブロックされたコンピューターのポリシーの [Enable Registry Rules（レジストリ ルールを有効化）] 設定で指定されている通知と同じになります。このチェックボックスがオフになっている場合は、[Custom Write Notifier（カスタム書き込み通知）] メニューからカスタム通知を選択できます。

フィールド	説明
[Custom Write Notifier（カスタム書き込み通知）]	このメニューは、[Write Action（書き込みアクション）] として [Block（ブロック）] または [Prompt（プロンプト）] を選択し、[Use Policy Specific Notifier（ポリシー固有の通知を使用）] チェックボックスをオフにした場合にのみ表示されます。 [Write Action（書き込みアクション）] として [Block（ブロック）] を選択した場合は、このメニューから通知を選択できます。このメニューには [<none>（なし）] オプションも表示され、このオプションを選択するとこのルールに関する通知が無効になります。 [Write Action（書き込みアクション）] として [Prompt（プロンプト）] を選択した場合は、このメニューから通知を選択できます。プロンプトを表示するにより設定されたルールの場合は必ず通知を表示する必要があるため、[<none>（なし）] オプションは表示されません。
[Registry Path（レジストリ パス）]	このルールを適用するレジストリ パス。パスを指定する際のオプションについては、「レジストリ パスの指定」（486 ページ）を参照してください。
[Process（プロセス）]	このメニューを使用すると、指定したパスに一致するファイルの実行または書き込みが特定のプロセスによって試みられた場合にのみルールを適用できます。プロセスを指定する方法については、「レジストリ ルールでのプロセスの指定」（487 ページ）を参照してください。プロセス メニューのオプションについては、表 58 を参照してください。
[User or Group（ユーザーまたはグループ）]	このメニューでは、このルールを適用するユーザーまたはグループを指定できます。ユーザーまたはグループを指定する方法については、「ユーザーまたはグループの指定」（491 ページ）を参照してください。
[Rule applies to（ルールの適用先）]	ラジオ ボタンを使用して、このルールを [**All policies**（すべてのポリシー）] に適用するか、[**Selected policies**（選択されたポリシー）] のみに適用するかを選択できます。[**Selected policies**（選択されたポリシー）] を選択すると、Bit9 Server 上で設定されているすべてのポリシーがチェックボックスとともに表示されます。ポリシーのチェックボックスはいくつでもオンにすることができます。
[History（履歴）]	既存ルールの場合は [History（履歴）] パネルに、ルールの作成日、作成者、最終更新日、最終更新者が表示されます。

書き込みアクションの指定

レジストリ ルールの [Write Action（書き込みアクション）] フィールドでは、そのルールに一致するレジストリへの書き込みが試みられた場合に適用するアクションを指定します。オプションについては、表 57 を参照してください。書き込みアクションには、すべてのプラットフォームにおけるレジストリ キーの作成、

削除、および変更が含まれます。また、すべての Windows プラットフォーム（ただし 64 ビット版の Windows Server 2003 を除く）におけるレジストリへのアクセス許可の変更も含まれます。

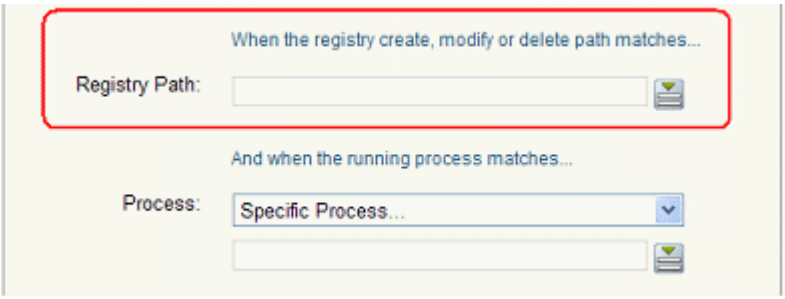
表 57：[Write Action（書き込みアクション）] メニューのオプション

オプション	説明
[Block（ブロック）]	このルールに一致する場所でのレジストリ キーおよび値の作成、削除、および変更をブロックします。 [Block（ブロック）] が選択されている場合は、[Use Policy Specific Notifier（ポリシー固有の通知を使用）] チェックボックスと [Custom Write Notifier（カスタム書き込み通知）] メニューが表示されます。これらを使用すると、このルールによってアクションがブロックされたときに表示する通知を指定できます。詳細については、表 56 を参照してください。
[Prompt（プロンプト）]	指定された場所でレジストリの変更が試みられたときにコンピューター ユーザーに通知ダイアログを表示します。通知ダイアログでは [Block（ブロック）] または [Allow（許可）] を選択できます。一度ユーザーが通知ダイアログで選択を行った後に、同じユーザーが同じコンピューター上で同じプロセスを使用して同じルールに一致する書き込みを試みた場合は常に同じ選択が適用され、プロンプトは再度表示されません。 [Prompt（プロンプト）] が選択されている場合は、[Use Policy Specific Notifier（ポリシー固有の通知を使用）] チェックボックスと [Custom Notifier（カスタム通知）] メニューが表示されます。これらを使用すると、ユーザーに選択を求める通知を表示できます。詳細については、表 56 を参照してください。
[Report（レポート）]	このレジストリ パスでの変更をブロックせずに Bit9 イベントとしてレポートします。

[Allow（許可）]	このルールに一致する場所でのレジストリ キーおよび値の作成、削除、および変更を許可します。これは適用されるルールが存在しないパスにおけるデフォルトの動作です。
	[Allow（許可）] を使用すると、特定の場所への書き込みをブロックする一般ルールの例外を作成できます。たとえば、
	`*\Software\MyApp\*`
	上記パスへの書き込みをすべてブロックするルールを作成した後、下記パスへの書き込みを許可する別のルールを作成し、許可ルールのランクをブロック ルールより上位に設定することでブロック ルールに対する例外を作成できます。
	`*\Software\MyApp\SpecialKey`

レジストリ パスの指定

［Registry Path（レジストリ パス）］では、ルールを適用する Windows レジストリ内の場所を指定します。



レジストリ パスの先頭では次のいずれかの文字列を使用する必要があります。

- **HKLM**
- **HKCU**
- **HKLM-SoftwareX86**
- **HKLM-SoftwareX64**
- **HKCU-SoftwareX86**
- **HKCU-SoftwareX64**
- *\

注意

- レジストリ パスの指定ではマクロを使用できません。
- 実際には他のキーへのリンクであるキーを含むパスが入力された場合、そのルールは機能しません。たとえば、*CurrentControlSet* を含むパスが指定されたルールは機能しません。リンクされた項目の代わりにワイルドカード（この例では *ControlSet**）を使用することを検討してください。

ワイルドカードの使用

［Registry Path（レジストリ パス）］ではワイルドカード（0 個以上の文字を表す「*」と、任意の 1 文字を表す「?」）を使用できます。ワイルドカードを使用すると、レジストリ パスを部分的に指定したり、複数のレジストリ パスを指定することができます。パスの指定で使用できるワイルドカードの数に制限はありません。

ワイルドカードを使用すると、レベルを省略したり、サブキーの名前を知らなくてもサブキーの値（またはそのサブキー）にルールを適用できます。以下に例を示します。

```
*\myapp\*\*
```

上記のように指定すると、下記のような *myapp* のサブキーの下にあるキーまたは値のみにルールが適用されます。

HKLM\myapp\apprunner\4.0

ただし、下記のような *myapp* 自体のサブキーまたは値には適用されません。

HKLM\myapp\sharedfiles

警告

ワイルドカードを使用する場合は、ルールの適用範囲が広くなりすぎて他のアプリケーションやオペレーティング システムの正常な動作が妨げられることがないように注意してください。エージェント コンピューター上での必要な操作に影響しないことが分かっている場合を除き、[Registry Path（レジストリ パス）] フィールドでアクタリスク ワイルドカードを単独で使用しないようにしてください（特に、書き込みをすべてブロックするルールを作成する場合）。レジストリ ルールはアプリケーションやシステムのパフォーマンスに深刻な影響を及ぼす場合があります。

キーまたは値の指定

パスの末尾に「\」がある場合は、そのパスにあるキーのみにルールが適用されます。パスの末尾に「*」がある場合は、そのパスの下にあるすべてのキー、サブキー、および値にルールが適用されます。

パスの末尾に円記号またはワイルドカードがない場合は、そのパスに一致する（キーではなく）値のみにルールが適用されます。以下に例を示します。

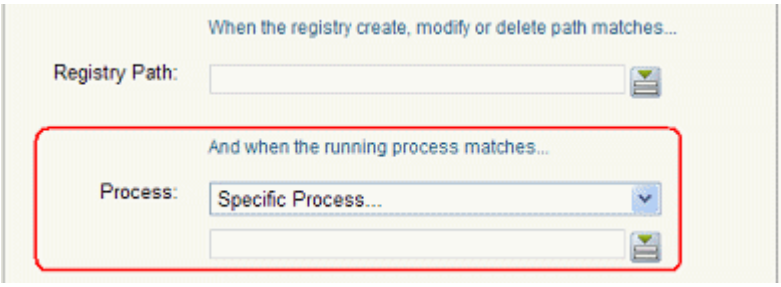
HKLM\SOFTWARE\FileReader\9.0\ViewOutput

上記の指定は、ViewOutput というキーではなく、ViewOutput という値に一致します。

レジストリ ルールには複数のパスを追加できます。詳細については、「複数のパスまたはプロセスの入力」（491 ページ）を参照してください。ルール内で複数のパスが指定されている場合は、[Registry Rule（レジストリ ルール）] テーブルの [Registry Path（レジストリ パス）] フィールドに最初のパスが表示され、その後ろに「(**multiple**)」（複数）と表示されます。

レジストリ ルールでのプロセスの指定

[Add/Edit Registry Rule（レジストリ ルールの追加 / 編集）] ページの [Process（プロセス）] フィールドを使用すると、レジストリの変更を試みたプロセス（実行中のファイル）に基づいてルールを細かく調整できます。



すべてのプロセス、特定のプロセス タイプ、特定のプロセス、または指定されたものを除くすべてのプロセスに適用されるようにルールを設定できます。表 58 に、[Process（プロセス）] フィールドのオプションを示します。

表 58：[Process（プロセス）] メニューのオプション

メニュー オプション	説明
[Any Process（すべてのプロセス）]	レジストリへの書き込みを試みたすべてのプロセスにルールを適用します。
[Any Promoted Process（昇格されたすべてのプロセス）]	ルールの評価時に昇格されていたすべてのプロセスにルールを適用します。昇格されたプロセスとは、インストーラーとしてマーキングされたプロセス、カスタム ルールの結果として昇格されたプロセス、または昇格されたプロセスによって開始された承認済みのプロセスのいずれかを指します。
[Any System Process（すべてのシステム プロセス）]	Local System ユーザーのセキュリティ コンテキストで実行されているすべてのプロセスにルールを適用します。このオプションの効果は [User or Group（ユーザーまたはグループ）] メニューで Local User を選択した場合の効果と同じですが、こちらのオプションを選択するほうがより効率的です。
[Specific Process...（特定のプロセス...）]	メニューの下にテキスト ボックスが表示され、このルールを使用して制御するプロセスの名前を入力できます。プロセスの指定に関するガイドラインと要件については、「レジストリ ルールでのプロセスの指定」（487 ページ）を参照してください。
[Any Process Except...（以下を除くすべてのプロセス ...）]	メニューの下にテキスト ボックスが表示され、このルールの適用対象から除外するプロセスを入力できます。プロセスの指定に関するガイドラインと要件については、「レジストリ ルールでのプロセスの指定」（487 ページ）を参照してください。 **注意**：[User or Group（ユーザーまたはグループ）] を指定し、[Process（プロセス）] メニューから [Any Process Except...（以下を除くすべてのプロセス ...）] も選択した場合、そのルールは、指定された例外プロセスが指定されたユーザーまたはグループによって実行されている場合を除いて適用されます。

パスの入力を必要とする [Process（プロセス）] メニューのオプション（[Specific Process...（特定のプロセス）] または [Any Process Except...（以下を除くすべてのプロセス ...）]）を選択した場合は、次のような方法でパスを定義できます。

- **特定のプロセスまたはディレクトリを指定** – 特定のプロセスのみがルールに一致するように、そのファイルを正確に特定するパスまたはプロセスを入力

できます。ディレクトリを指定した場合は、そのディレクトリとサブディレクトリ内にあるすべてのプロセスにルールが適用されます。

- **ローカル ドライブまたは UNC パスを指定** – *C:\folder1\subfolder\application.exe* のようにローカル ドライブ名を使用してローカルのプロセスを指定できます。また、*\\computername\dir\application.exe* のように UNC パスを使用して、リモートのプロセスを指定することもできます。マップされたドライブがパスまたはプロセスの指定で使用されている場合は正しく認識されません。
- **ワイルドカードを使用** – ワイルドカード（任意の 1 文字を表す「?」と 0 個以上の文字を表す「*」）を使用することによりプロセスの指定範囲を広げたり、正確な場所が分からないファイルやフォルダーにも一致するルールを作成できます。ワイルドカードはパスの先頭、末尾、または中間で使用できます。
- **マクロを使用** – エージェント コンピューター上の正確な場所が分からない場合でも、特別な Bit9 マクロを使用することにより、Microsoft Windows 環境内の一般に知られているフォルダーを指定できます。
- **複数のプロセス パスを指定** – 1 つのルールで複数のプロセス定義を指定できます。

プロセスまたはディレクトリの指定

プロセス パスの指定では、ディレクトリまたは特定のファイルを入力できます。ディレクトリを指定した場合は、そのディレクトリまたはサブディレクトリ内にあるプロセスによって指定されたレジストリ内の場所への書き込みが試みられたときにルールが適用されます（ただし、上位にランクされた別のルールが現在のプロセスに一致した場合は除く）。

プロセス定義がディレクトリであることを示すには、定義の末尾に円記号 (\) または円記号とアスタリスク (*) を付ける必要があります。円記号を付けないと、ディレクトリではなく、指定された名前を持つファイルがルールの適用対象と見なされます。たとえば、次のいずれかの形式を使用してパスを定義すると、「subfolder2」がディレクトリとして正しく認識されます。

```
c:\folder1\subfolder2\
c:\folder1\subfolder2\*
```

一方、次の形式はディレクトリとして認識されません。

```
c:\folder1\subfolder2
```

プロセスの定義でパス マクロを使用する場合は、マクロの後に円記号を付けなくても、展開されたマクロはディレクトリとして扱われます。「マクロの使用」を参照してください。

ワイルドカードの使用

［Process（プロセス）］フィールドではワイルドカード文字を使用できます。アスタリスク (*) は 0 個以上の文字を表し、疑問符 (?) は任意の 1 文字を表します。ワイルドカードを使用すれば、複数のコンピュータ上で複数の場所に存在するプロセスを指定することもできます（ただし、マクロのほうが同じ目的をより効果的に達成できることもあります。「マクロの使用」を参照してください）。

プロセスの指定で使用できるワイルドカードの数に制限はありません。たとえば、次のようにパスを指定できます。

```
*\Win*\folder?\
```

プロセス パスの自動変換

［Process（プロセス）］フィールドに特定の記号が含まれている場合は、次のように自動パス変換が行われます。

- スラッシュで終わるプロセス パスの末尾にはワイルドカード文字の「*」が追加されます。
- スラッシュとドライブ文字を含まないプロセス パスの先頭には「*\」が追加されます。
- ドライブ文字は、ローカルの固定ボリュームを表している場合に限り、パスの指定で使用できます。マップされたボリュームに割り当てられたドライブ文字は、すべてのコンピューターで同じマッピングになっていない可能性があるため使用できません。
- 「*:\」は、接続されているすべてのストレージ ボリューム（フロッピー ディスクと CD-ROM を除く）を表します。

プロセス パスでのデバイスの指定

パスの指定に *\device* を含めると、エージェント コンピューター上の一部のデバイスまたはすべてのデバイスから実行されているプロセスによって書き込みが試みられたときにルールを適用するように指定できます。以下に例を示します。

- **\device**** はすべてのデバイスを表します。
- **\device\harddisk*** は、コンピューターに接続されているすべてのストレージ ボリューム（フロッピー ディスクと CD-ROM を除く）を表します。
- **\device\cdrom*** は CD-ROM デバイスを表します。

マクロの使用

レジストリ ルールの［Process（プロセス）］フィールドでは特定のマクロを使用できます。［Process（プロセス）］フィールドに左山括弧 (<) 文字を入力するとマクロのメニューが表示されます。レジストリ ルールの［Process（プロセス）］フィールドでサポートされているマクロには次の 2 種類があります。

- **パス マクロ** – Microsoft Windows 環境の一般に知られているフォルダーのサブセットです。このパスはすべて、特定のファイルではなく場所を表します。パス マクロを使用できる場所は、ルールの［Path or File（パスまたはファイル）］フィールドの先頭のみです（パス マクロの前にその他の文字列を置くことはできません）。
- **レジストリ マクロ** – Windows レジストリ内の文字列を指定するマクロです。レジストリ マクロは［Path or File（パスまたはファイル）］フィールド内のどこでも使用できます。

マクロを使用すると、ルールの適用対象となるファイルがコンピューターごとに異なる場所に存在している場合でも、すべての Windows コンピューター上で機能するルールを効果的に定義できます。

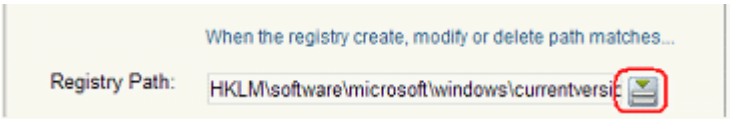
パス マクロとレジストリ マクロの詳細については、「カスタム ルール」の章で「ルールでのマクロの使用」（423 ページ）を参照してください。これらのマクロはレジストリ ルールの［Process（プロセス）］フィールドで使用できます。

注意

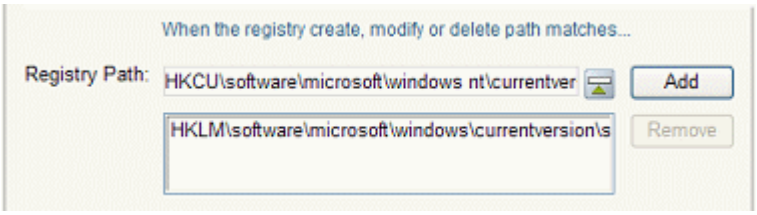
マクロはレジストリ ルールの［Process（プロセス）］フィールドで使用できますが、［Registry Path（レジストリ パス）］フィールドでは使用できません。

複数のパスまたはプロセスの入力

ルールの［Registry Path（レジストリ パス）］と［Process（プロセス）］フィールドでは、複数の文字列を入力できます。たとえば、ルールの適用対象となる最初のレジストリ パスを入力した後に、ボックスの右にある［Expand（展開）］ボタンをクリックします。

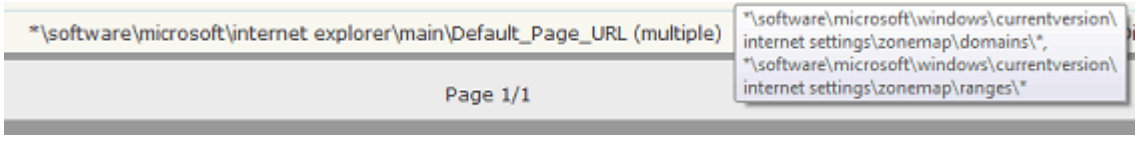


その後、ボックス内に別のパスを入力し、項目を 1 つ入力するたびに［Add（追加）］をクリックします。



パスを削除するには、［Expand（展開）］ボタンをクリックし、［Registry Path（レジストリ パス）］ボックスの下にあるリストでファイルまたはパスを選択して、［**Remove**（削除）］ボタンをクリックします。［Process（プロセス）］フィールドでの項目の追加と削除も同様の方法で行えます。

1 つのルールで複数のパスまたはプロセスを指定した場合は、［Registry Rules（カスタム　ルール）］ページの該当列に最初のパスが表示され、その後ろに「(**multiple**)」（複数）と表示されます。値の上にマウス ポインターを置くと、そのルールのパスまたはプロセスの完全なリストがヒントとして表示されます。



ユーザーまたはグループの指定

特定のユーザーまたは特定のグループに属すユーザーがアクションを試みた場合にのみ適用されるルールを作成できます。［Add/Edit Custom Rule（カスタム ルー

ルの追加 / 編集)］ページの［User or Group（ユーザーまたはグループ)］で選択できるオプションは次のとおりです。

- ［**Any Users**（すべてのユーザー)］– すべてのユーザーにルールを適用します。
- ［**Specific User or Group…（特定のユーザーまたはグループ …)**］– メニューの下にテキスト ボックスが表示され、次の形式を使用して AD ユーザーまたはグループを入力できます。ユーザーまたはグループ名 @ ドメインまたはドメイン \ ユーザーまたはグループ名
- ［**Authenticated Users**］や［**Local Administrators**］など、組み込み済みの Windows グループもメニュー オプションとして表示されます。

注意

- Windows Vista 以降でアプリケーションを実行する場合、事前定義されたセキュリティ グループ（Administrators など）のメンバーシップを指定するには、管理者としてアプリケーションを実行する必要があります。ルールに対してグループを定義する必要がある場合は、事前定義されたグループではなく、自身で定義したセキュリティ グループを使用することを検討してください。
- ユーザーがログインした後にグループのメンバーシップが確立されてグループベースのルールが有効になるまでの間にはわずかな遅れがあります。設定されているルールが多い場合はこの遅れが長くなる可能性があります。ユーザーのログイン後にできるだけ早くルールを有効にする必要がある場合は、ルール内でユーザー グループを指定しないようにしてください。ユーザー名や SID が指定されているルールは常に有効で、この遅れによる影響を受けません。

ルールのランキング

レジストリ ルールには「ランク」番号が割り当てられ、最もランク番号が小さいルールから最もランク番号が大きいルールに向かって順番に評価されます。最小のランク番号は「**1**」です。デフォルトではランク順にルールが表示されますが、必要に応じて他の列を基準にテーブルを並べ替えることもできます。同じパスが複数のルールで指定されている場合は、ランキングが高いほうのルール（ランク番号が小さいほうのルール）が優先され、ランキングが低いほうのルール（ランク番号が大きいほうのルール）は適用されません。ただし、この動作には 1 つだけ例外があり、アクションとして［Report（レポート)］が指定されているルールが先に一致した場合は、下位にランクされているルールも引き続き処理されます。

ルールのランキングは変更できます。

レジストリ ルールのランクの変更手順：

1. ［Registry Rules（レジストリ ルール)］ページでルールがランク順に表示されていない場合は、［Rank（ランク)］列の見出しをクリックして並べ替えます。
2. ランクを変更するルールを探します。

3. ルールのランクを上げるには、適切な位置に来るまでルールの隣にある上矢印ボタンをクリックします。
   または
   移動するルールの上にマウス ポインターを置き、左マウス ボタンを押しながら新しい位置にルールをドラッグしてマウス ボタンを放します。
4. ルールのランクを下げるには、適切な位置に来るまでルールの隣にある下矢印ボタンをクリックするか、ドラッグアンドドロップでルールを移動します。

Rank ▲	Name	Path
1	[Sample] Block Suspicious System Changes	HKLM\software\microsoft\windows nt\currentversion\image file
2	[Sample] Report Changes to Trusted Zones	*\software\microsoft\windows\currentversion\internet settings\
3	[Sample] Prompt on Suspicious changes to Startup Files	*\software\microsoft\windows\currentversion\policies\explorer\
4	[Sample] Tamper Protection	HKLM-SoftwareX86\microsoft\windows nt\currentversion\image
5	[Sample] Tamper Protection	HKLM-SoftwareX86\microsoft\windows nt\currentversion\image
6	[Sample] Tamper Protection	HKLM-SoftwareX86\microsoft\windows nt\currentversion\image

注意

ドラッグアンドドロップを使用する場合、前後のページにルールをドラッグすることはできません。現在表示されていないランキングにルールを移動する必要がある場合は、[Custom Rules（カスタム ルール）] ページの右下にあるメニューを使用して 1 ページごとに表示される行数を増やすことができます。

レジストリ ルールの無効化と削除

不要になったレジストリ ルールはレジストリ ルール テーブル内に残したまま無効化することも、テーブルから削除することもできます。無効化または削除されたルールは、新たに検出されたファイルに対しては適用されません。ただし、ルールを無効にする前にそのルールによって適用されたファイル状態はそのまま維持されます。

同じルールを将来再び使用する可能性がある場合は、一時的に無効にすることをお勧めします。

レジストリ ルールの無効化手順：

1. コンソール メニューで [**Rules**（ルール）] > [**Software Rules**（ソフトウェア ルール）] を選択し、[Software Rules（ソフトウェア ルール）] ページが表示されたら [**Registry**（レジストリ）] タブをクリックします。[Registry Rules（レジストリ ルール）] テーブルが表示されます。
2. 無効にするルールの隣にある [Edit（編集）] ボタン（鉛筆とファイル）をクリックします。[Edit Registry Rule（レジストリ ルールの編集）] ページが表示されます。
3. [Status（ステータス）] 行にある [**Disabled**（無効）] ラジオ ボタンをクリックし、ページの下部にある [Save（保存）] ボタンをクリックします。ルールが無効になります。

ルールを完全に削除した場合、削除を取り消したり、削除したルールを復元することはできません。本当にルールを削除してもよいかどうかを事前に必ず確認してください。

レジストリ ルールの削除手順：

1. コンソール メニューで［**Rules**（ルール）］>［**Software Rules**（ソフトウェア ルール）］を選択し、［Software Rules（ソフトウェア ルール）］ページが表示されたら［**Registry**（レジストリ）］タブをクリックします。［Registry Rules（レジストリ ルール）］テーブルが表示されます。
2. 削除するルールの隣にある［Delete（削除）］ボタン（X と書かれている赤い丸）をクリックし、確認ダイアログで **[OK]** をクリックします。ルールが削除されます。

コンピューターでのルール ステータスの表示

Bit9 Server で管理されているエージェントの数と接続されていないエージェントの数によっては、すべてのエージェントに新しいルールや更新されたルールがすぐに配信されない場合があります。有効になっているルールの［Edit（編集）］ページにある［Related Views（関連ビュー）］メニューには、［Computers（コンピューター）］ページの 2 種類のフィルター済みビューへのリンクがあり、エージェント管理コンピューターでのルールのステータスを確認できます。以下の選択肢があります。

- **［All Computers that have received this rule（このルールを既に受信したすべてのコンピューター）］**
- **［All Computers that have not yet received this rule（このルールをまだ受信していないすべてのコンピューター）］**

一度も有効化されたことがないルールの場合、このメニューは表示されません。

サンプル レジストリ ルール

Bit9 Security Platform には一連のサンプル レジストリ ルールが含まれ、デフォルトでは無効になっています。これらのルールの設定を確認してそのまま有効にすることもできますが、適切にレジストリを保護できるようにカスタマイズしてから使用することもできます。

重要

サンプル レジストリ ルールを有効にする場合は、レジストリ パスや適用されるアクション（ブロック、プロンプト、レポート、許可）など、設定されているパラメーターを必ず確認してください。ルールのアクションを［Report（レポート）］に設定してしばらく様子を見てからルールを完全に有効化（つまり、アクションをブロック、プロンプト、または許可に変更する）こともできます。

例：Internet Explorer の信頼済みゾーンの変更をレポート

ここでは最初の例として「[Sample] Report Changes to Trusted Zones（［サンプル］信頼済みゾーンの変更をレポート）」と名付けられたサンプル ルールのパラメーターについて説明します。このサンプルはコンソールに表示されるルールに含まれていますが、デフォルトでは無効になっています。このルールは Bit9 エージェントを実行しているマシン上で Internet Explorer の信頼済みゾーンのサイトまたは IP アドレスが変更されたときにレポートを行います。信頼済みゾーンに含まれるサイトには強力な権限が与えられるため、信頼済みゾーンの変更はセキュリティ リスクにつながるおそれがあります。

最初に、［**Registry**（レジストリ）］タブに移動し、「[Sample] Report Changes to Trusted Zones（［サンプル］信頼済みゾーンの変更をレポート）」ルールの隣にある［View Details（詳細の表示）］ボタン（鉛筆とファイル）をクリックします。

説明に書かれているように、このルールは Internet Explorer の信頼済みゾーンのサイトまたは IP アドレスに変更を加えるレジストリの変更が行われたときに Bit9 イベントを生成します。パラメーターは次のように設定されています。

- ［**Write Action**（書き込みアクション）］:［**Report**（レポート）］– ルールに一致する変更のレポートのみを行います。書き込みのブロック、または通常ブロックされる書き込みの許可などは行われません。より規制的なルールを作成する必要がある場合は、この設定を［**Prompt**（プロンプト）］に変更することもできます。その場合は、Bit9 エージェントを実行しているコンピューター上の各ユーザーに対して、ルールに一致するレジストリの変更をブロックするか許可するかの選択を求めるプロンプトが表示されます。あるいは、ルールに一致する変更をすべて**ブロック**することもできます。

- ［Registry Path（レジストリ パス）］:
  \software\microsoft\windows\currentversion\internet settings\zonemap\domains
  \software\microsoft\windows\currentversion\internet settings\zonemap\ranges
  – このルールには 2 つのパスが含まれています。これらのパスは ***** から始まるため、先頭が HKCU であるか、HKCU であるか、サポートされているその他の接頭辞であるかにかかわらず、以降の部分に一致するパスへの書き込みはすべてこのルールに一致します。また、これらのパスはスラッシュとアスタリスクで終わるため、**domains** および **ranges** と同じ階層またはその下にあるキーと値がこのルールに一致します。

- ［**Process**（プロセス）］:［**Any Process**（すべてのプロセス）］– 他のパラメーターに一致するレジストリへの書き込みを試みたすべてのプロセスにルールを適用します。
- ［**User or Group**（ユーザーまたはグループ）］:［**Any User**（すべてのユーザー）］– 他のパラメーターに一致するレジストリへの書き込みを試みたすべてのユーザーにルールを適用します。
- ［**Rule applies to**（ルールの適用先）］:［**All policies**（すべてのポリシー）］– すべてのポリシー（したがって、Bit9 エージェントを実行しているすべての Windows コンピューター）にルールを適用します。

このルールが有効になっている場合、ルールに一致するレジストリへの書き込みが試みられると、［Events（イベント）］ページにイベントとして表示されます。これらのイベントを検索するには、［Events（イベント）］ページで［Show/Hide Filters（フィルターの表示/非表示）］ボタンをクリックし、「Subtype is Report write (registry rule)（サブタイプがレポートの書き込み（レジストリ ルール））」のフィルターを作成します。このルールに一致するイベント レポートが見つかった場合は、次のような方法で処理できます。

- その変更が望ましくない場合は、（Bit9 の外部で）変更を元に戻し、同じ変更が再び発生しないように（単にレポートするだけでなく）その変更をブロックする新しいルールを作成します。ルールの適用範囲を狭める必要がある場合、または広げる必要がある場合は、ワイルドカードや複数のパスを使用します。
- その変更に特に問題がない場合は変更を許可します。
- Bit9 Server のファイル情報を使用すると、変更を試みたプロセスに関する情報を入手できます。

自動起動ルール

Bit9 Security Platform v7.2.3 の［Registry Rules（レジストリ ルール）］テーブルには自動起動ルールが含まれています。このルールは、実際には複数のルールで構成されています。このルールはデフォルトで無効になっています。このルールセットを有効にすると、コンピューターの起動時の動作を制御するレジストリ内の場所の変更が試みられたときにサーバーにレポートされ、オプションで変更をブロックすることもできます。たとえば、自動起動ルールの対象となる数多くのパスには、次のパスが含まれます。

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

このルール セットを有効にする前に影響をテストする必要がある場合は、このルールの［Write Action（書き込みアクション）］メニューで［Report（レポート）］を選択します。ある程度の期間が経過したら［Events（イベント）］ページに移動し、フィルターを「Rule name contains Autostart（ルール名に Autostart を含む）」に設定して、このルール セットによってトリガーされたイベントを確認します。このルールを有効にしても問題がないと判断した場合は、［Write Action（書き込みアクション）］の値を［Block（ブロック）］（または［Prompt（プロンプト）］）に変更できます。

［Edit Registry Rule（レジストリ ルールの編集）］ページに表示される自動起動ルールのレジストリ パスは <AutostartRules> です。このマクロは、このルールによって制御される場所の現在のリストへの参照です。このリストは Bit9 Server 内で管理され、ルール定義には列挙されません。このリストは将来のリリースで更新および拡張される予定です。現在使用しているバージョンでこのルールが適用される場所の詳細については、Bit9 テクニカル サポートにお問い合わせください。

注意

リリース 7.0 より前の Bit9 (Parity) には、新しい自動起動ルール セットに含まれる場所の一部のみに適用されるレジストリ ルールが組み込まれていました。これらの自動起動ルールを使用していた場合は、起動時の安全性をさらに強化するため、代わりに新しい自動起動ルールを使用することをお勧めします。

第 15 章

メモリ ルール

この章では、実行中のプロセスに他のプロセスがアクセスして変更を加えられないように保護するメモリ ルールについて説明します。

プラットフォームに関する注意：メモリ ルールは Windows オペレーティング システムを実行しているコンピューターのみに適用されます。

セクション

概要

メモリ ルールを使用すると Windows コンピューター上のプロセスへのアクセス試行を監視し、必要な場合は特定のプロセスが他のプロセスやユーザーによってアクセスまたは変更されないように保護することができます。メモリ ルールでは、指定された条件に一致するプロセスへの読み取りアクセス、書き込みアクセス、または実行アクセスをブロックしたり、そのようなアクセスをレポートしたり、そのようなアクセスをブロックするか許可するかの選択を求めるプロンプトをエージェント システム上のユーザーに表示することができます。また、特殊なケースに対処できるように高度なオプションも用意されています。

Bit9 エージェントによって保護されているシステムのメモリ内で悪意のある攻撃が発生した場合、メモリ ルールが適切に設定されていれば、他のプロセスに攻撃が広がることを防止でき、他のプロセス内の情報へのアクセスをブロックすることもできます。メモリ ルールを作成すると、保護されているコンピューターの脆弱性による影響を制限することができます。また、特定のアプリケーションやプロセスがユーザーや悪意のあるコードによって不正に終了されたり操作されないように保護することもできます。

メモリ ルールに関連するイベント（メモリ ルールによってブロックされたアクションなど）のリストを表示するには、[Events（イベント）] ページに移動し、[Saved Views（保存済みビュー）] メニューから [**Memory**（メモリ）] を選択します。

重要

エージェント コンピューターを保護できるように、Bit9 には [Tamper Protection（改ざんからの保護）] と名付けられた 2 つのルールが組み込まれ、これらのルールのランクはデフォルトで 1 および 2 に設定されています。Bit9 サポートからの指示がない限り、これらのルールを編集したり、無効化したり、順序を入れ替えたりしないようにしてください。ルールに変更を加える場合は、事前に説明フィールドを確認してください。

ルールの適用範囲

どのユーザーまたはどのプロセスが指定されたプロセスへのアクセスを試みたかにかかわらず、すべての Windows コンピューターに適用されるメモリ ルールを作成できます。また、次の条件を指定して、適用範囲を絞り込んだルールを作成することもできます。

- **ソース プロセス別** – 特定のソース プロセスが監視対象または保護対象のターゲット プロセスへのアクセスを試みた場合にのみルールを適用できます。
- **ユーザー別またはグループ別** – 特定のユーザーまたはユーザー グループのみにルールを適用できます。
- **ポリシー別** – 指定されたポリシーに含まれるコンピューターのみにルールを適用できます。
- **ルールの順序** – メモリ ルールは [Memory Rules（メモリ ルール）] テーブルにデフォルトで表示される [Rank（ランク）] 列の値順に評価されます。ランクが「1」に設定されているルールが最優先され、「2」に設定されているルールがその次に優先されます。ルールの順番を変更して、適用範囲が広いルール

よりも先に適用範囲が狭いをルールを評価させることもできます。たとえば、特定のユーザーが特定のプロセスへのアクセスを試みたときに適用されるルールを作成し、その他のユーザーがそのプロセスへのアクセスを試みたときに適用されるルールよりも上に置くことができます。詳細については、「ルールのランキング」（514 ページ）を参照してください。

メモリ ルールの適用対象に関しては次のような制約があります。

- メモリ ルールを使用して特定のプロセスをそれ自身から保護することはできません。たとえば、プロセスが自身を終了できないようするルールや、プロセスが自身のメモリを変更できないようにするルールは作成できません。
- メモリ ルールは Mac、Linux、および 64 ビット版 Windows Server 2003 を実行しているコンピューターではサポートされていません。
- ［Kernel Memory Access（カーネル メモリ アクセス）］ルールは Windows XP または SP1 が適用されていない Windows Server 2003 を実行しているコンピューターのみでサポートされています。
- ［Dynamic Code Execution（動的コード実行）］ルールは 32 ビット版の Windows XP、Windows 2003、Windows Vista、および Windows 7 のみでサポートされ、これらの Windows オペレーティング システムの 64 ビット版ではサポートされていませんが、Windows 8 および 10 に関してはすべてのバージョンでサポートされています。
- 可視性モード ポリシーに含まれるコンピューターの場合、書き込みをブロックするメモリ ルールまたはユーザーにプロンプトを表示するメモリ ルールはレポートのみを行うルールとして動作し、書き込みのブロックやプロンプトの表示は行われません。

メモリ ルールのエクスポートとインポート

メモリ ルールはサーバーからエクスポートして別のサーバーにインポートできます。［Memory Rules（メモリ ルール）］ページにはこれらの機能を使用するためのボタンがあります。詳細については、「カスタム ルール」の章で「ルールのエクスポートとインポート」（441 ページ）を参照してください。

メモリ ルールの通知の指定

Bit9 エージェントには、ルールによってアクションがブロックされた場合、またはアクションを許可するかブロックするかの選択をユーザーに促す場合に通知を表示する機能があります。メモリ ルールごとに、次の 2 種類の通知ソースからいずれかを選択できます。

- ［**Use Policy Specific Notifier**（ポリシー固有の通知を使用）］– 各ポリシーの［Advanced Setting（高度な設定）］には［Enforce memory rules（メモリ ルールを適用）］が含まれ、この項目は常にオンになっています。このポリシー設定の［Notifier（通知）］フィールドでは、メモリ ルールによってアクションがブロックされたときにエージェント コンピューター上で表示する通知を指定できます。また、このポリシー設定で［<none>（なし）］を選択すると、（プロンプトを表示するように設定されているルールに一致した場合を含め）そのポリシーに含まれるコンピューター上でメモリ ルールの通知を一切表示しないようにすることができます。ポリシー固有のメモリ ルール通知はどのメモリ ルールにでも割り当てることができます。詳細については、「高度な設定」（189 ページ）を参照してください。

- ［**Custom Notifier**（カスタム通知）］– ポリシー固有の通知を使用しない場合は、メモリ ルールごとに通知を選択（または作成）できます。選択肢は、［Add/Edit Memory Rule（メモリ ルールの追加 / 編集）］ページのメニューに表示されます。プロンプトを表示するように設定されたルールで［Custom Notifier（カスタム通知）］を選択した場合は、必ず通知を表示する必要があります。書き込みをブロックするように設定されたルールで［Custom Notifier（カスタム通知）］を選択した場合は、［<none>（なし）］を選択して通知を表示しないようにすることもできます。

メモリ ルール通知の設定項目については、下記の表 59 を参照してください。通知の詳細については、第 17 章「ブロック通知と承認要求」を参照してください。

メモリ ルールの作成

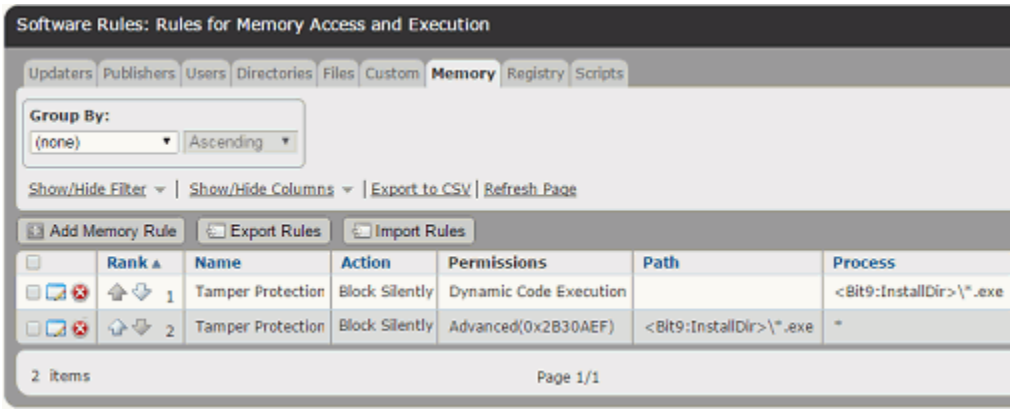
メモリ ルールを作成するには、ルール名を指定した後、下の表の左列に太字で示されている情報を、右列に示されている［Add Memory Rule（メモリ ルールの追加）］ページ内のフィールドに入力する必要があります。

概要	［Add/Edit Memory Rule（メモリ ルールの追加 / 編集）］ページのフィールド
この（これらの）ソース プロセス …	［Source Process（ソース プロセス）］
… および / または**この（これらの）ユーザー**が …	［User or Group（ユーザーまたはグループ）］
… 次の**タイプのメモリ アクセス**を …	［Permissions（権限）］
… **この（これらの）場所にあるプロセス**に対して …	［Target Process（ターゲット プロセス）］
… **この（これらの）ポリシー**に含まれるコンピューター上で試みた場合 …	［Rule applies to:（ルールの適用先：）］
… **このアクション**を実行します。	［Action（アクション）］

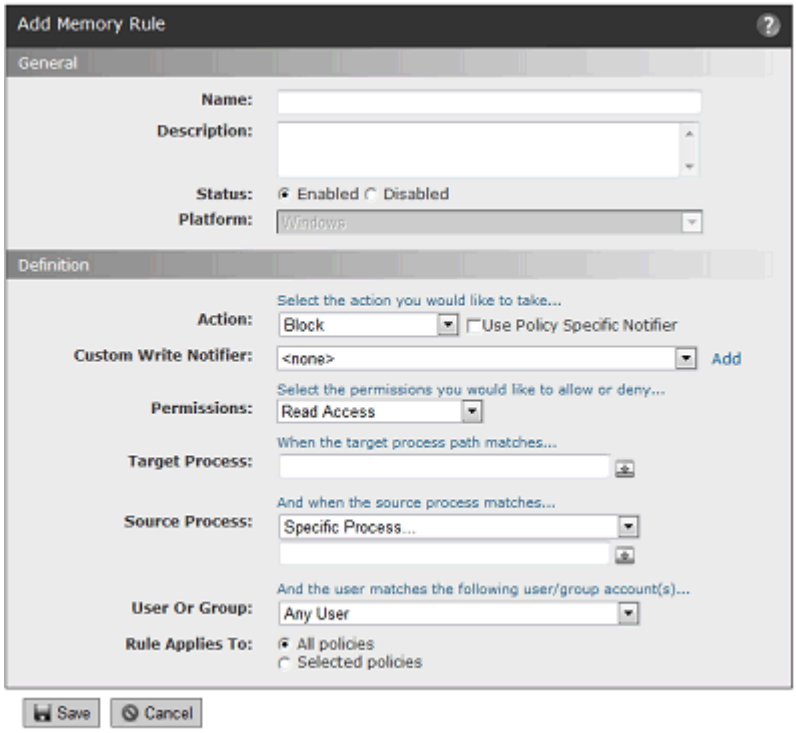
これらのパラメーターでは複数の項目を指定でき、そのクラスに含まれるすべての項目を指定することもできます（たとえば、すべてのユーザー、すべてのポリシー、またはすべてのソース プロセスにルールを適用できます）。

メモリ ルールの追加（作成）手順：

1. コンソール メニューで、［**Rules**（ルール）］>［**Software Rules**（ソフトウェア ルール）］の順に選択します。［Software Rules（ソフトウェア ルール）］ページが表示されます。
2. ページの左メニューまたはタブにある［**Memory**（メモリ）］をクリックします。［Memory Rules（メモリ ルール）］テーブルが表示され、組み込み済みのルールとサーバー上で作成されたその他のメモリ ルールが表示されます。



3. ［**Add Memory Rule**（メモリ ルールの追加)］ボタンをクリックします。［Add Memory Rule（メモリ ルールの追加)］ページが表示されます。



4. ［Name（名前)］フィールドに名前を入力します。この名前はルールのリストに表示されます。任意で［Description（説明）］フィールドに詳細な説明を入力することもできます。
5. 新しいメモリ ルールはデフォルトで［**Enabled**（有効)］になっています。ルールを後から有効にする場合は、［Status（ステータス)］フィールドで［**Disabled**（無効)］をクリックします。

6. このルールに必要なその他の情報（表 59、「メモリ ルールのパラメーター」504 ページを参照）を入力して、[**Save**（保存）] をクリックします。新しく作成されたルールが［Memory Rules（メモリ ルール）］テーブルの最後に表示されます。［Memory Rules（メモリ ルール）］テーブルが複数ページにわたる場合は、新しいルールを確認できるように最後のページが表示されます。
7. このルールの優先順位を変更する場合は、［Memory Rules（メモリ ルール）］テーブルをランク順に並べ替え、［Rank（ランク）］列の矢印を使用するかドラッグアンドドロップを使用して適切な位置にルールを移動します。詳細については、「ルールのランキング」（514 ページ）を参照してください。

メモリ ルールのパラメーター

表 59 に、［Add/Edit Memory Rule（メモリ ルールの追加 / 編集）］ページで設定可能なパラメーターを示します。

表 59：メモリ ルールのパラメーター

フィールド	説明
[Name（名前）]	［Memory Rules（メモリ ルール）］ページに表示されるこのルールの名前。（必須）
[Description（説明）]	メモリ ルールに関する追加情報。任意のテキストを入力できます。
[Status（ステータス）]	このルールを有効または無効にするラジオ ボタン。これらのラジオ ボタンを使用することで、特定の場合にのみ使用するルールを作成したり、ルールの作成時に使用した情報を維持したままルールを一時的に無効にしたりできます。
[Platform（プラットフォーム）]	このルールが適用されるプラットフォーム。このフィールドの値は変更できず、常に [Windows] が選択されています。メモリ ルールは Windows 以外のプラットフォームには適用されません。
[Action（アクション）]	このルールに一致するプロセスへのアクセスまたはプロセスの変更が試みられた場合に Bit9 エージェントで適用するアクション。このフィールドのオプションについては、表 60 を参照してください。
[Use Policy Specific Notifier（ポリシー固有の通知を使用）]	［Action（アクション）］として［Block（ブロック）］または［Prompt（プロンプト）］を選択した場合は、このチェックボックスが［Action（アクション）］オプションの右に表示されます。このチェックボックスがオンになっている場合、メモリ ルールによってアクションがブロックされたときに表示される通知は、アクションがブロックされたコンピューターのポリシーの［Enforce Memory Rules（メモリ ルールを適用）］設定で指定されている通知になります。このチェックボックスがオフになっている場合は、［Custom Write Notifier（カスタム書き込み通知）］メニューからカスタム通知を選択できます。

フィールド	説明
[Custom Write Notifier（カスタム書き込み通知）]	このメニューは、[Action（アクション）] として [Block（ブロック）] または [Prompt（プロンプト）] を選択し、[Use Policy Specific Notifier（ポリシー固有の通知を使用）] チェックボックスをオフにした場合にのみ表示されます。 [Action（アクション）] として [Block（ブロック）] を選択した場合は、このメニューから通知を選択できます。このメニューには [<none>（なし）] オプションも表示され、このオプションを選択するとこのルールに関する通知が無効になります。 [Action（アクション）] として [Prompt（プロンプト）] を選択した場合は、このメニューから通知を選択できます。ただし、プロンプトを表示するように設定されたルールの場合は必ず通知を表示する必要があるため、[<none>（なし）] オプションは表示されません。
[Permissions（権限）]	このルールを適用するアクセスのタイプ。[Permissions（権限）] フィールドのオプションについては、表 61 を参照してください。
[Target Process（ターゲット プロセス）]	このルールを通じてアクセスを制限、監視、または許可するプロセス。ターゲット プロセスを定義する方法については、「ターゲット プロセスとソース プロセスの指定」（509 ページ）を参照してください。
[Source Process（ソース プロセス）]	このメニューを使用すると、指定されたソース プロセスがターゲット プロセスへのアクセスを要求した場合にのみルールを適用できます。このメニューのオプションについては、表 62、「[Source Process（ソース プロセス）] メニューのオプション」512 ページを参照してください。パスを入力する際のオプションについては、「ターゲット プロセスとソース プロセスの指定」（509 ページ）を参照してください。 **注意**：[Kernel Memory Access（カーネル メモリ アクセス）] ルールおよび [Dynamic Code Execution（動的コード実行）] ルールの場合は、ソース プロセス自体がルールの適用対象になるため、ターゲット プロセスを指定する必要はありません。
[User or Group（ユーザーまたはグループ）]	このメニューでは、このルールを適用するユーザーまたはグループを指定できます。ユーザーまたはグループを指定する方法については、「ユーザーまたはグループの指定」（513 ページ）を参照してください。
[Rule applies to（ルールの適用先）]	ラジオ ボタンを使用して、このルールを [All policies（すべてのポリシー）] に適用するか、[Selected policies（選択されたポリシー）] のみに適用するかを選択できます。[Selected policies（選択されたポリシー）] を選択すると、Bit9 Server 上で設定されているすべてのポリシーがチェックボックスとともに表示されます。ポリシーのチェックボックスはいくつでもオンにすることができます。
[History（履歴）]	既存ルールの場合はページの下部に [History（履歴）] パネルが表示され、ルールの作成日、作成者、最終更新日、最終更新者が表示されます。

ルールのアクションの指定

メモリ ルールの［Action（アクション）］フィールドでは、ルールに一致するメモリ アクセスが試みられた場合にBit9エージェントで実行するアクションを定義します。このフィールドのオプションについては、表 60 を参照してください。

表 60：［Action（アクション）］ メニューのオプション

フィールド	説明
［Block（ブロック）］	このルールに一致するプロセスへのアクセス、プロセスの終了、またはプロセスの変更をブロックします。 ［Block（ブロック）］が選択されている場合は、［Use Policy Specific Notifier（ポリシー固有の通知を使用）］チェックボックスと［Custom Write Notifier（カスタム書き込み通知）］メニューが表示されます。これらを使用すると、このルールによってアクションがブロックされたときに表示する通知を指定できます。詳細については、表 59 を参照してください。
［Block Silently（サイレント ブロック）］	このルールに一致するプロセスへのアクセス、プロセスの終了、またはプロセスの変更をブロックします。通知は表示されず、Bit9 イベントも生成されません。
［Prompt（プロンプト）］	このルールに一致するプロセスへのアクセス、プロセスの終了、またはプロセスの変更が試みられたときにエンドポイント ユーザーに通知ダイアログを表示します。通知ダイアログでは［Block（ブロック）］または［Allow（許可）］を選択できます。一度ユーザーが通知ダイアログで選択を行った後に同じコンピューター上で同じプロセスが同じルールに一致した場合は同じ選択が自動的に適用され、プロンプトは再度表示されません。 ［Prompt（プロンプト）］が選択されている場合は、［Use Policy Specific Notifier（ポリシー固有の通知を使用）］チェックボックスと［Custom Write Notifier（カスタム書き込み通知）］メニューが表示されます。これらを使用すると、ユーザーに選択を求める通知を表示できます。詳細については、表 59 を参照してください。 **注意**：［Dynamic Code Execution（動的コード実行）］ルールの［Action（アクション）］フィールドで［Prompt（プロンプト）］を選択すると Bit9 エージェントを実行しているコンピューターの動作が不安定になる可能性があるため、この組み合わせは推奨されません。
［Report（レポート）］	ルールに一致するプロセスへのアクセス、プロセスの終了、またはプロセスの変更をブロックせず、それらのアクションを Bit9 イベントとしてレポートします。

フィールド	説明

[Allow（許可）]	このルールに一致するすべてのメモリ操作またはプロセス操作を許可します。これは特定のターゲット プロセスまたはソース プロセスに適用されるルールが存在しない場合のデフォルトの動作です。
	[Allow（許可）] を使用すると、特定の場所への書き込みをブロックする一般ルールの例外を作成できます。たとえば、
	`c:\Program Files\InterestingApp\*`
	上記パスでのメモリ操作をすべてブロックするルールを作成した後、下記パスでのメモリ操作を許可する別のルールを作成し、許可ルールのランクをブロック ルールより上位に設定することでブロック ルールに対する例外を作成できます。
	`c:\Program Files\InterestingApp\Subfolder\`

ルールの権限の指定

[Permissions（権限）] フィールドでは、このルールを適用するアクセスのタイプ（読み取り、書き込み、実行など）を定義します。複数のタイプのアクセスを制御できるオプションもあります。[Permissions（権限）] メニューのオプションについては、表 61 を参照してください。

表 61：[Permissions（権限）] メニューのオプション

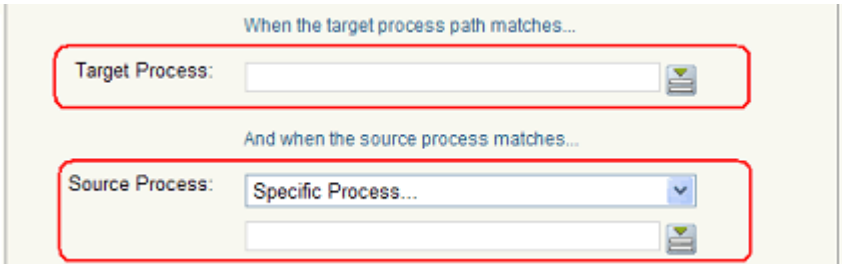
フィールド	説明
[Control Process（プロセスの制御）]	プロセスまたはスレッドの実行を制御するために必要なアクセス（プロセスを終了する機能など）。
[Read Access（読み取りアクセス）]	プロセスまたはスレッドに関する特定の情報の取得、コピー、または複製に必要なアクセス。データの損失や盗難のみが懸念される場合は、[Action（アクション）] を [Block（ブロック）] に設定してこのオプションを選択することを推奨します。
[Write Access（書き込みアクセス）]	プロセスまたはスレッドおよびその属性の変更に必要なアクセス。

フィールド	説明
[Dynamic Code Execution（動的コード実行）]	実行可能イメージに関連付けられていないコードの実行をアプリケーションに許可するかどうかを制御します。この保護を適用することにより、さまざまな形式のマルウェアによる恣意的なコード実行や浮動的なコード実行がブロックされます。また、動的実行保護 (DEP) を無効化しようとする試みもブロックされます。これは、32 ビット版の Windows XP、Windows 2003、Windows Vista、および Windows 7 のみに適用されます。 **重要**：[Dynamic Code Execution（動的コード実行）] ルールの［Action（アクション）］メニューでは［**Prompt**（プロンプト）］オプションを指定しないようにしてください。そのようなルールを作成するとエージェント コンピューター上で望ましくない結果が生じる可能性があります。
[Kernel Memory Access（カーネル メモリ アクセス）]	ユーザーモード プロセスによるカーネル メモリへのアクセスを許可するかどうかを制御します。このオプションを使用すると、適正なアプリケーションによるアクセスを許可し、その他すべてのアプリケーションによるアクセスを拒否するルールを作成できます。これは、Windows XP および（SP1 が適用されていない）Windows Server 2003 のみに適用されます。
[Write + Control（書き込み + 制御）]	書き込みと制御の権限。［Permission（権限）］メニューでこのオプションを選択し、[Action（アクション）] メニューで［Block（ブロック）］を選択すると、プロセスに対する攻撃（悪意のあるコードによる挿入、終了、改ざんなど）をブロックできます。
[Read + Control（読み取り + 制御）]	読み取り、書き込み、および制御の権限。このオプションを選択して、［Action（アクション）］を［Block（ブロック）] に設定すると、攻撃だけでなくデータの損失や盗難も防止することができます。これには［Dynamic Code Execution（動的コード実行）］と［Kernel Memory Access（カーネル メモリ アクセス）］は含まれません。
[Advanced...（詳細 ...）]	このオプションを選択するとメモリ アクセスをさらにきめ細かく制御できます。[Advanced（詳細）] オプションを使用する場合は、Bit9 テクニカル サポートまでご連絡ください。

ターゲット プロセスとソース プロセスの指定

通常、メモリ ルールでは次の 2 つのプロセスを指定します。

- ［**Target Process**（ターゲット プロセス）］– このフィールドで指定されたプロセスへのアクセスがルールによって制限、監視、または許可されます。
- ［**Source Process**（ソース プロセス）］– このフィールドで指定されたプロセスがターゲット プロセスへのアクセスを要求したときにルールが適用されます。



メモリ ルールで［Target Process（ターゲット プロセス）］を指定する際には、パラメーターの文字列を定義するためのオプションがいくつか用意されています。これらのオプションは、パスの入力を必要とする 2 つの［Source Process（ソース プロセス）］オプション（［Specific Process…（特定のプロセス）］または［Any Process Except…（以下を除くすべてのプロセス …）］）を選択した場合にも使用できます。これらのオプションには以下のものがあります。

- **ディレクトリまたはプロセスを指定** – 特定のファイルのみがルールに一致するように、そのファイルを厳密に特定するプロセス指定を入力できます。ディレクトリを指定した場合は、そのディレクトリとサブディレクトリ内にあるファイルから実行されているプロセスにルールが適用されます。
- **ローカル ドライブまたは UNC パスを指定** – *C:\folder1\subfolder\application.exe* のようにローカル ドライブ名を使用してプロセスを指定できます。また、*\\computer\dir\application.exe* のように UNC パスを使用して、リモートのプロセスを指定することもできます。マップされたドライブがパスまたはプロセスの指定で使用されている場合は正しく認識されません。
- **ワイルドカードを使用** – ワイルドカード（任意の 1 文字を表す「?」と 0 個以上の文字を表す「*」）を使用することによりプロセスの指定範囲を広げたり、正確な場所が分からないファイルやフォルダーにも一致するルールを作成できます。ワイルドカードはパスの先頭、末尾、または中間で使用できます。
- **マクロを使用** – エージェント コンピューター上の正確な場所が分からない場合でも、特別な Bit9 マクロを使用することにより、Microsoft Windows 環境内の一般に知られているフォルダーを指定できます。
- **複数のパスまたはプロセスを指定** – 1 つのルールで複数のプロセス パス定義を指定できます。

ファイルまたはディレクトリの指定

ターゲット プロセスまたはソース プロセスのパスを定義する際には、ディレクトリまたはファイルを指定できます。ディレクトリを指定した場合は、そのディレクトリとサブディレクトリ内にあるプロセスにルールが適用されます（ただし、

上位にランクされた別のルールがそのディレクトリ内のプロセスやサブディレクトリに一致した場合は除く)。

プロセス定義がディレクトリであることを示すには、定義の末尾に円記号 (\) または円記号とアスタリスク (*) を付ける必要があります。円記号を付けないと、ディレクトリではなく、指定された名前を持つファイルがルールの適用対象と見なされます。たとえば、次のいずれかの形式を使用してパスを定義すると、ディレクトリとして正しく認識されます。

```
c:\folder1\subfolder2\
c:\folder1\subfolder2\*
```

一方、次の形式はディレクトリとして認識されません。

```
c:\folder1\subfolder2
```

プロセスの定義でパス マクロを使用する場合は、マクロの後に円記号を付けなくてもディレクトリとして扱われます。「マクロの使用」を参照してください。

ワイルドカードの使用

プロセス フィールドではワイルドカード文字を使用できます。アスタリスク (*) は 0 個以上の文字を表し、疑問符 (?) は任意の 1 文字を表します。ワイルドカードを使用すると、複数のコンピュータ上で複数の場所に存在するディレクトリのパスを部分的に指定したり、複数のパスを指定することができます（ただし、マクロのほうが同じ目的をより効果的に達成できることもあります。「マクロの使用」を参照してください)。マクロ内ではワイルドカードを使用できません。

プロセスの指定で使用できるワイルドカードの数に制限はありません。たとえば、次のようにパスを指定できます。

```
*\Win*\folder?\
```

警告

ワイルドカードを使用する場合は、ルールの適用範囲が広くなりすぎて他のアプリケーションやオペレーティング システムの正常な動作が妨げられることがないように注意してください。エージェント コンピューター上で必要な操作に絶対に影響しないことが分かっている場合を除き、[Target Process（ターゲット プロセス）] フィールドでアクタリスク ワイルドカードを単独で使用しないようにしてください (特に、複数のタイプのアクセスをブロックするルールを作成する場合)。

自動パス変換

プロセス フィールドのファイル パスに特定の記号が含まれている場合は、ルールを処理する際に自動パス変換が次のように実行されます。

- スラッシュで終わるパスの末尾にはワイルドカード文字の「*」が追加されます。
- スラッシュとドライブ文字を含まないパスの先頭には「*\」が追加されます。
- ドライブ文字は、ローカルの固定ボリュームを表している場合に限り、パスの指定で使用できます。マップされたボリュームに割り当てられたドライブ

文字は、すべてのコンピューターで同じマッピングになっていない可能性があるため使用できません。

- 「*:\」は、接続されているすべてのストレージ ボリューム（フロッピー ディスクと CD-ROM を除く）を表します。

パスでのデバイスの指定

パスの指定に *\device* を含めることで、エージェント コンピューター上の一部のデバイスまたはすべてのデバイス上に存在するプロセスに適用されるルールを作成できます。以下に例を示します。

- **\device**** はすべてのデバイスを表します。
- **\device\harddisk**** は、コンピューターに接続されているすべてのストレージ ボリューム（フロッピー ディスクと CD-ROM を除く）を表します。
- **\device\cdrom**** は CD-ROM デバイスを表します。

マクロの使用

プロセス フィールドでは特定のマクロを使用できます。プロセス フィールドで左山括弧 (<) 文字を入力するとマクロのメニューが表示されます。メモリ ルールのプロセス フィールドでサポートされているマクロには次の 2 種類があります。

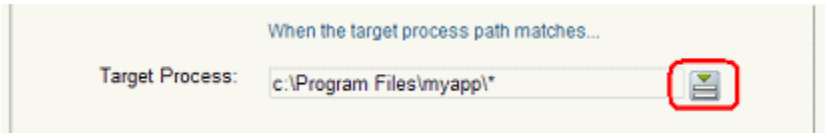
- **パス マクロ** – Microsoft Windows 環境の一般に知られているフォルダーのサブセットです。このパスはすべて、特定のファイルではなく場所を表します。パス マクロを使用できる場所は、ルールの［Path or File（パスまたはファイル）］フィールドの先頭のみです（パス マクロの前にその他の文字列を置くことはできません）。
- **レジストリ マクロ** – Windows レジストリ内の文字列を指定するマクロです。レジストリ マクロは［Path or File（パスまたはファイル）］フィールド内のどこでも使用できます。

マクロを使用すると、指定する必要があるプロセスがコンピューターごとに異なる場所に存在している場合でも、すべてのエージェント コンピューター上で機能するルールを効果的に定義できます。

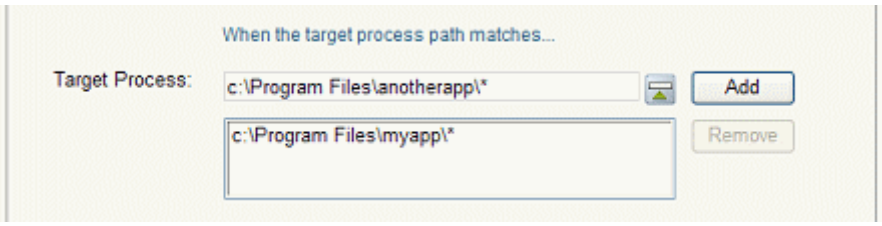
パス マクロとレジストリ マクロの詳細については、「カスタム ルール」の章で「ルールでのマクロの使用」（423 ページ）を参照してください。メモリ ルールのプロセス フィールドでは、そこで説明されているマクロを使用できます。

複数のターゲット プロセスまたはソース プロセスの入力

メモリ ルールの各プロセス フィールドでは、複数の文字列を入力できます。たとえば、ルールの適用対象となる最初のメモリ パスを入力した後に、ボックスの右にある［Expand（展開）］ボタンをクリックします。

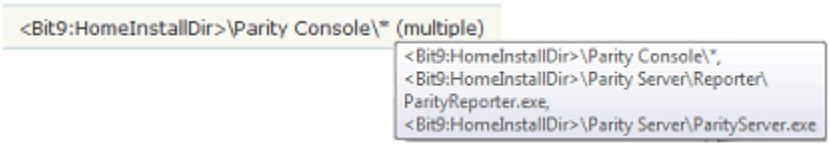


その後、ボックス内に別のプロセス パスを入力し、項目を 1 つ入力するたびに［**Add**（追加）］をクリックします。



プロセス パスを削除するには、［Expand（展開）］ボタンをクリックし、ボックスの下にあるリストでパスを選択して、［**Remove**（削除）］ボタンをクリックします。

ルール内のいずれかのプロセス フィールドに複数のパスを入力した場合は、［Memory Rules（メモリ ルール）］テーブルの該当列に最初のパスが表示され、その後ろに「(multiple)」（複数）と表示されます。値の上にマウス ポインターを置くと、そのルールのプロセスの完全なリストがヒントとして表示されます。



［Source Process（ソース プロセス）］メニュー

メモリ ルールの［Source Process（ソース プロセス）］フィールドでは、ターゲット プロセスへのアクセスを要求する側のプロセスを指定します。［Source Process（ソース プロセス）］メニューには、メニュー選択だけで完全に定義されるオプション（［**Any Process**（すべてのプロセス）］など）と、プロセス パスの入力を必要とするオプションが含まれます。

表 62：［Source Process（ソース プロセス）］メニューのオプション

フィールド	説明
［Any Process（すべてのプロセス）］	ターゲット プロセスへのアクセスを試みたすべてのプロセスにルールを適用します。
［Any Promoted Process（昇格されたすべてのプロセス）］	ルールの評価時に昇格されていたすべてのソース プロセスにルールを適用します。昇格されたプロセスとは、インストーラーとしてマーキングされたプロセス、カスタム ルールの結果として昇格されたプロセス、または昇格されたプロセスによって開始された承認済みのプロセスのいずれかを指します。
［Any System Process（すべてのシステム プロセス）］	Local System ユーザーのセキュリティ コンテキストで実行されているすべてのソース プロセスにルールを適用します。このオプションの効果は［User or Group（ユーザーまたはグループ）］メニューで Local User を選択した場合の効果と同じです。

フィールド	説明
[Specific Process…（特定のプロセス …)]	メニューの下にテキスト ボックスが表示され、このルールを通じて制御するソース プロセスを入力できます。
[Any Process Except…（以下を除くすべてのプロセス …)]	メニューの下にテキスト ボックスが表示され、このルールの適用対象から除外するソース プロセスを入力できます。 **注意 :** [User or Group（ユーザーまたはグループ）] を指定し、[Process（プロセス)] メニューから [Any Process Except…（以下を除くすべてのプロセス …)] も選択した場合、そのルールは、指定された例外プロセスが指定されたユーザーまたはグループによって実行されている場合を除いて適用されます。

ユーザーまたはグループの指定

特定のユーザーまたは特定のグループに属すユーザーがアクションを試みた場合にのみ適用されるルールを作成できます。[Add/Edit Memory Rule（メモリ ルールの追加 / 編集)] ページの [User or Group（ユーザーまたはグループ)] で選択できるオプションは次のとおりです。

- [**Any Users**（すべてのユーザー)] – すべてのユーザーにルールを適用します。
- [**Specific User or Group…**（特定のユーザーまたはグループ …)] – メニューの下にテキスト ボックスが表示され、次の形式を使用して AD ユーザーまたはグループを入力できます。ユーザーまたはグループ名 @ ドメインまたはドメイン \ ユーザーまたはグループ名
- [**Authenticated Users**] や [**Local Administrators**] など、組み込み済みの Windows グループもメニュー オプションとして表示されます。

注意

- Windows Vista 以降でアプリケーションを実行する場合、事前定義されたセキュリティ グループ（Administrators など）のメンバーシップを指定するには、管理者としてアプリケーションを実行する必要があります。ルールに対してグループを定義する必要がある場合は、事前定義されたグループではなく、自身で定義したセキュリティ グループを使用することを検討してください。
- ユーザーがログインした後にグループのメンバーシップが確立されてグループベースのルールが有効になるまでの間にはわずかな遅れがあります。設定されているルールが多い場合はこの遅れが長くなる可能性があります。ユーザーのログイン後にできるだけ早くルールを有効にする必要がある場合は、ルール内でユーザー グループを指定しないようにしてください。ユーザー名や SID が指定されているルールは常に有効で、この遅れによる影響を受けません。

ルールのランキング

メモリ ルールには「ランク」番号が割り当てられ、最もランク番号が小さいルールから最もランク番号が大きいルールに向かって順番に評価されます。最小のランク番号は「**1**」です。[Memory Rules（メモリ ルール）] ページでは、デフォルトでランク順にルールが表示されますが、必要に応じて他の列を基準にテーブルを並べ替えることもできます。

メモリに関連するアクションがいずれかのルール定義に一致した場合は、そのルールが評価されます。ルールの処理はランク順に従って続行され、他のルールが現在のメモリ関連アクションに一致するかどうかが確認されます。一致するルールがこれ以上見つからなくなったときにどうなるかは、一致したルールの [Permissions（権限）] 設定によって異なります。

- アクションが 2 つのルールに一致し、それらのルールで異なる権限が設定されている場合は（たとえば、一方は [Read Access（読み取りアクセス）] に適用され、他方は [Write Access（書き込みアクセス）] に適用される場合は）、両方のルールが評価されます。このようなケースで、[Control Process（プロセス制御）] に適用される 3 つ目のルールも一致する場合は、そのルールも評価されます。
- アクションが 2 つ（以上）のルールに一致し、すべてのルールで同じ権限が設定されている場合は（たとえば、両方のルールが [Write Access（書き込みアクセス）] に適用される場合は）、最初のルールのみが評価されます。ただし、この動作には 1 つだけ例外があり、アクションとして [Report（レポート）] が指定されているルールが先に一致した場合は、同じ権限が設定されている下位のルールも引き続き処理されます。

特定のルールを現在のランク位置よりも上げる必要がある場合は、ルールのランキングを変更できます。

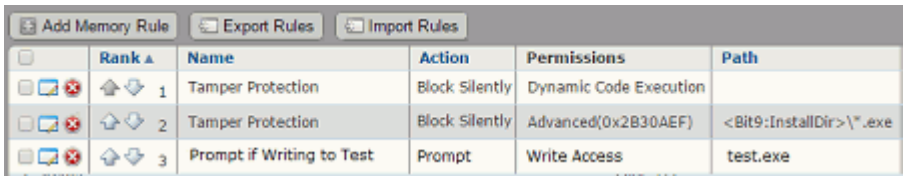
重要

サーバーを保護できるように、Bit9 には [Tamper Protection（改ざんからの保護）] と名付けられた 2 つのルールが組み込まれ、これらのルールのランクはデフォルトで 1 および 2 に設定されています。Bit9 テクニカル サポートからの指示がない限り、他のルールのランクをこれらのルールよりも上にしないようにしてください。

メモリ ルールのランクの変更手順：

1. [Memory Rules（メモリ ルール）] ページでルールがランク順に表示されていない場合は、[Rank（ランク）] 列の見出しをクリックして並べ替えます。
2. ランクを変更するルールを探します。
3. ルールのランクを上げるには、適切な位置に来るまでルールの隣にある上矢印ボタンをクリックします。
   または
   移動するルールの上にマウス ポインターを置き、左マウス ボタンを押しながら新しい位置にルールをドラッグしてマウス ボタンを放します。

4. ルールのランクを下げるには、適切な位置に来るまでルールの隣にある下矢印ボタンをクリックするか、ドラッグアンドドロップでルールを移動します。



メモリ ルールの無効化と削除

不要になったメモリ ルールはメモリ ルール テーブル内に残したまま無効化することも、テーブルから削除することもできます。無効化または削除されたルールは、以後、効果を持たなくなります。

同じルールを将来再び使用する可能性がある場合は、一時的に無効にすることをお勧めします。

メモリ ルールの無効化手順：

1. コンソール メニューで［**Rules**（ルール）］>［**Software Rules**（ソフトウェア ルール）］を選択し、［Software Rules（ソフトウェア ルール）］ページが表示されたら［**Memory**（メモリ）］タブをクリックします。［Memory Rules（メモリ ルール）］テーブルが表示されます。
2. 無効にするルールの隣にある［Edit（編集）］ボタン（鉛筆とファイル）をクリックします。［Edit Memory Rule（メモリ ルールの編集）］ページが表示されます。
3. ［Status（ステータス）］行にある［**Disabled**（無効）］ラジオ ボタンをクリックし、ページの下部にある［Save（保存）］ボタンをクリックします。ルールが無効になります。

ルールを完全に削除した場合、削除を取り消したり、削除したルールを復元することはできません。本当にルールを削除してもよいかどうかを事前に必ず確認してください。

メモリ ルールの削除手順：

1. コンソール メニューで［**Rules**（ルール）］>［**Software Rules**（ソフトウェア ルール）］を選択し、［Software Rules（ソフトウェア ルール）］ページが表示されたら［**Memory**（メモリ）］タブをクリックします。［Memory Rules（メモリ ルール）］テーブルが表示されます。
2. 削除するルールの隣にある［Delete（削除）］ボタン（X と書かれている赤い丸）をクリックし、確認ダイアログで **[OK]** をクリックします。ルールが削除されます。

コンピューターでのルール ステータスの表示

Bit9 Server で管理されているエージェントの数と接続されていないエージェントの有無によっては、すべてのエージェントに新しいルールや更新されたルールがすぐに配信されない場合があります。有効になっているルールの［Edit（編集）］ページにある［Related Views（関連ビュー）］メニューには、［Computers（コンピューター)］ページの 2 種類のフィルター済みビューへのリンクがあり、エージェント管理コンピューターでのルールのステータスを確認できます。以下の選択肢があります。

- **［All Computers that have received this rule（このルールを既に受信したすべてのコンピューター)］**
- **［All Computers that have not yet received this rule（このルールをまだ受信していないすべてのコンピューター)］**

一度も有効化されたことがないルールの場合、このメニューは表示されません。

第 16 章

イベント ルール

この章では、定義したフィルターに一致するイベントが発生したときに特定のアクションを実行するイベント ルールについて説明します。

セクション

概要

イベント ルールでは、定義したフィルターに一致するファイル関連のイベントまたはコンピューター関連のイベントが発生したときに実行するアクションを指定できます。この機能を使用するには、[Manage event rules（イベント ルールの管理）] 権限を持つユーザーとしてコンソールにログインする必要があります。「アカウント グループの権限」（108 ページ）を参照してください。

指定されたイベント ルールがトリガーされたときに表示されるアラートを作成することもできます。「アラートの作成」（611 ページ）を参照してください。

ルール アクションをトリガーできるアクション

イベント ルールのトリガーとして使用できるイベントはファイルに関連するイベントのみです。各ルールではイベント サブタイプを少なくとも 1 つ指定する必要があります。たとえば、[New file on network（ネットワーク上の新規ファイル）] サブタイプに関連するイベントが発生したときにアクションをトリガーするようにルールを設定します。異なるイベント状況でルール アクションが実行されるように、複数のサブタイプを追加することもできます。また、その他の条件（イベントに特定の IP アドレスへの参照が含まれている、など）をルールに追加することもできます。

あるいは、イベントまたはその親プロセスで参照されているターゲット ファイルが特定のプロパティを持つ場合にのみルールを実行するように指定することもできます。たとえば、新規の未承認ファイルに対して Bit9 SRS によるレピュテーション承認が有効になっていない場合にのみ、それらのファイルを分析サービスにアップロードするように指定することができます。

ルールを通じて実行できるアクション

イベント ルールでは次のアクションを実行できます。

- [**Change global file state**（ファイルのグローバル状態を変更）] – イベントで参照されているファイルのグローバルな承認または禁止（レポートのみ）を作成したり、グローバルな承認または禁止を削除するイベント ルールを作成できます。このルールはすべてのコンピューターに適用することも、ポリシーごとに適用することもできます。さらに、イベント ルールを使用した高度な禁止を作成するオプション機能を有効にすることもできます。また、グローバル状態を変更するルールを構成することで、エンドポイント ユーザーからの承認要求を解決することもできます。
- [**Change global process state**（プロセスのグローバル状態を変更）] – イベントで参照されているプロセスのファイルのグローバルな承認または禁止（レポートのみ）を作成したり、グローバルな承認または禁止を削除するイベント ルールを作成できます。このルールはすべてのコンピューターに適用することも、ポリシーごとに適用することもできます。さらに、イベント ルールを使用した高度な禁止を作成するオプション機能を有効にすることもできます。また、グローバル状態を変更するルールを構成することで、エンドポイント ユーザーからの承認要求を解決することもできます。
- [**Change global file state**（ファイルのローカル状態を変更）] – イベントで参照されているファイルのローカル承認を作成したり、ローカル承認を削除するイベント ルールを作成できます。また、ローカル状態を変更するルールを構

成することで、エンドポイント ユーザーからの承認要求を解決することもできます。

- ［**Upload file**（ファイルをアップロード）］– イベントで参照されているファイルを Bit9 Server にアップロードするイベント ルールを作成できます。
- ［**Analyze file**（ファイルを分析）］– Bit9 Connector で設定された分析サービスにファイルをアップロードするイベント ルールを作成できます。
- ［**Move computer**（コンピューターを移動）］– 必要に応じて、ファイル関連のイベントで参照されているコンピューターを別のポリシーと適用レベルに移動することもできます。

ユーザーには、与えられている権限に基づくアクション オプションのみが表示されます。たとえば、［Analyze file（ファイルを分析）］オプションは、分析サービスにファイルを送信する権限を持たないユーザーに対しては表示されません。

ルールの効果のシミュレーション

イベント ルールの重要な機能の 1 つとして、指定されたアクションを実際には実行せずに、ルールを有効にした場合の効果のシミュレーションのみを実行する機能があります。イベント ルールは Bit9 Server に重大な影響を及ぼす可能性があるため、正しく設定しないと望ましくない結果や予期せぬ結果が生じる場合があります。そのため、新しいルールを作成した際には、完全に有効にする前に、［Simulate only（シミュレーションのみ）］モードで実行することを強く推奨します。このオプションは［Add Event Rule（イベント ルールの追加）］ページと［Edit Event Rule（イベント ルールの編集）］ページから選択できます。［Simulate only（シミュレーションのみ）］を使用する推奨ワークフローについては、「ルールを有効化する前のテスト」（522 ページ）を参照してください。

過去のイベントへのルールの再適用

Bit9 には、新しいルールを過去のイベントに適用する機能があります。この機能を［Simulate only（シミュレーションのみ）］モードと組み合わせて使用すると、過去に発生した大量のイベントにルールを適用して、実際にそのルールが有効だった場合にどのイベントが処理されていたかを確認できます。結果を確認した後、ルールを微調整して、そのルールがトリガーされる状況を絞り込むこともできます。また、新しいルールが完全に有効になったときに、そのルールを過去のイベントに遡って適用することもできます。この機能を利用すると、たとえば先週新たに発見されたすべての未承認ファイルを外部の分析サービスに送信するといった処理が可能になります。

イベント ルールの有効化、無効化、および削除

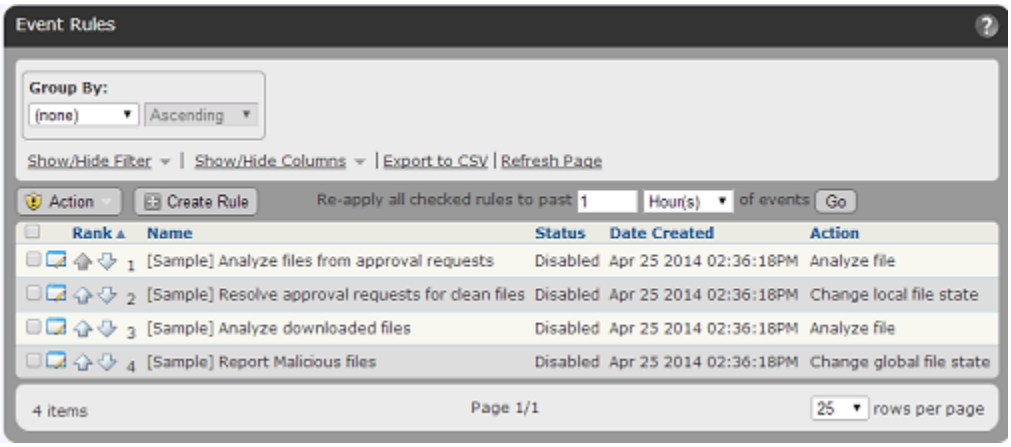
特定のイベント ルールを有効化、無効化、または削除するには、［Event Rules（イベント ルール）］（テーブル）ページまたは［Edit Event Rule（イベント ルールの編集）］ページを使用します。

［Event Rules（イベント ルール）］ページを使用する場合は、1 つ以上のルールを選択し、［Action（アクション）］メニューを使用してそれらのルールを有効化または無効化できます。このメニューでは［Simulate Only（シミュレーションのみ）］オプションを選択できません。［Simulate Only（シミュレーションのみ）］モード

でルールを有効にするには、[Edit Event Rule（イベント ルールの編集）] ページを使用します。

[Event Rules（イベント ルール）]テーブルでのルールの有効化または無効化手順:

1. コンソール メニューで、[**Rules**（ルール）] > [**Event Rules**（イベント ルール）] の順に選択します。[Event Rules（イベント ルール）] ページが表示され、作成済みのルールとそれらのステータスが表示されます。

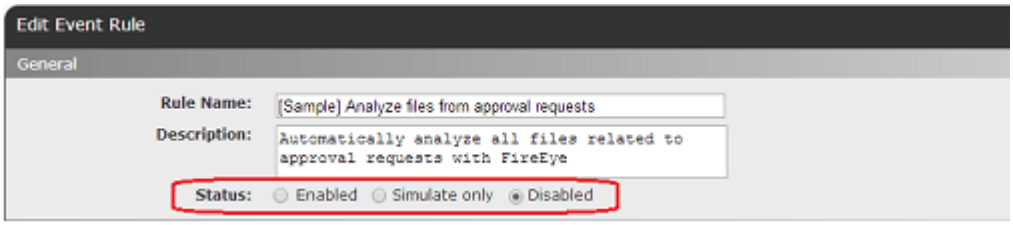


2. テーブル内でルールの隣にあるチェックボックスをオンにします（複数選択することもできます）。
3. [Action（アクション）] メニューから [**Enable**（有効化）] または [**Disable**（無効化）] を選択し、確認ダイアログで選択を確認します。メニューから選択したオプションに応じて、チェックボックスがオンになっているルールが有効または無効になります。

1 つのイベント ルールだけを有効または無効にする場合は、[Edit Event Rule（イベント ルールの編集）] ページを使用できます。また、このページでは、[Simulate only（シミュレーションのみ）] モードを有効にして、ルール内で指定されているアクションを実際には実行せずにイベント ルールの効果を確認することができます。

イベント ルールの有効化、無効化、または効果のシミュレーション手順：

1. コンソール メニューで、[**Rules**（ルール）] > [**Event Rules**（イベント ルール）] の順に選択します。[Event Rules（イベント ルール）] ページが表示され、作成済みのルールとそれらのステータスが表示されます。
2. ステータスを変更するルールの隣にある [View Details（詳細の表示）] ボタンをクリックします。[Edit Event Rule（イベント ルールの編集）] ページが表示されます。



3. ［Status（ステータス）］フィールドでいずれかのラジオ ボタン（［**Enable**（有効化）］、［**Simulate Only**（シミュレーションのみ）］、または［**Disable**（無効化）］）をクリックします。
4. 必要に応じてその他のルール プロパティを変更した後、そのルールによって処理されたイベントを同じページ内で監視するには［**Save**（保存）］をクリックし、ページを閉じるには［**Save & Exit**（保存して終了）］をクリックします。［Simulate only（シミュレーションのみ）］のルールを使用する推奨ワークフローについては、「ルールを有効化する前のテスト」（522 ページ）を参照してください。

注意

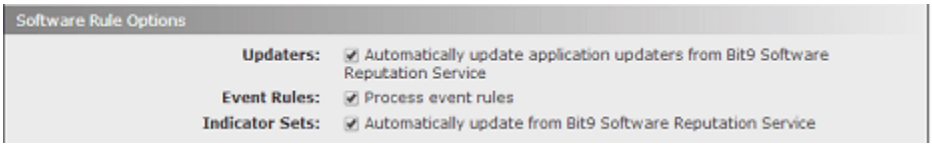
分析ツールの環境（特定のオペレーティング システムを実行している分析環境など）に依存するイベント ルールを作成し、その環境が利用できなくなった場合、その環境が再び利用可能になるまで数分間待機した後、そのイベント ルールは自動的に無効になります。

［Event Rules（イベント ルール）］テーブルでのルールの削除手順：

1. コンソール メニューで、［**Rules**（ルール）］>［**Event Rules**（イベント ルール）］の順に選択します。［Event Rules（イベント ルール）］ページが表示され、作成済みのルールとそれらのステータスが表示されます。
2. テーブル内でルールの隣にあるチェックボックスをオンにします（複数選択することもできます）。
3. ［Action（アクション）］メニューから［**Delete**（削除）］を選択し、ダイアログで選択を確認します。チェックボックスがオンになっているルールが削除されます。

すべてのイベント ルールの処理の無効化

Bit9 Server は有効化されているすべてのルールを処理するようにデフォルトで設定されています。そのため、各ルールがどのように動作し、各ルールが機能するかどうかは、有効化、無効化、およびシミュレーションの設定によって決定されますが、イベント ルール機能自体を無効にしてすべてのイベント ルールの処理を停止することもできます。イベント ルールの処理を無効化または再有効化するためのチェックボックスは、［System Configuration（システム構成）］ページの［Advanced Options（高度なオプション）］タブにあります。すべてのイベント ルールを無効にすると、イベント ルールに基づくアラートがトリガーされなくなります。



すべてのイベント ルールの処理の無効化手順：

1. コンソール メニューで、[**Administration**（管理）] > [**System Configuration**（システム構成）] の順に選択し、[**Advanced Options**（高度なオプション）] タブをクリックします。
2. ページ下部にある [**Edit**（編集）] ボタンをクリックします。
3. [Software Rule Options（ソフトウェア ルールのオプション）] パネルで [Event Rules（イベント ルール）] チェックボックスをオフにし、[**Update**（更新）] ボタンをクリックします。

イベント ルールを再有効化する手順も上記と同じです（ただし、[Event Rules（イベント ルール）] チェックボックスをオフにするのではなくオンにします）。イベント ルールを再有効化すると、停止された時点から各ルールの処理が再開されます。この機能はインフラストラクチャの休止などによってイベント ルールのアクションを実行できない場合などに役立つことがあります。たとえば、接続されているアプライアンスへのアクセスを必要とする分析ルールが大量にあり、メンテナンスのためにアプライアンスを一時的にシャットダウンする必要がある場合は、メンテナンスが完了するまでそれらのルールの処理を無効にすることができます。

ルールを有効化する前のテスト

イベント ルールのアクション（禁止、承認、別のポリシーへのコンピューターの移動など）が適切に設定されていない場合は、セキュリティや運用に関わる深刻な問題につながるおそれがあります。そのため、新しいルールを作成した際には、完全に有効にする前に、[Simulate only（シミュレーションのみ）] モードで実行することを強く推奨します。このオプションは [Add Event Rule（イベント ルールの追加）] ページと [Edit Event Rule（イベント ルールの編集）] ページから選択できます。

イベント ルールを [Simulate only（シミュレーションのみ）] モードで実行すると、過去の通知にルールを適用して、実際にそのルールが有効だった場合にどのイベントが処理されていたかを確認できます。結果を確認した後、ルールのフィルターを追加または変更して、そのルールがトリガーされる状況を絞り込むこともできます。サンプル ルールの [Edit Event Rule（イベント ルールの編集）] ページを開くと、それらのルールによって処理されるイベントを制限するために、どのようにフィルターが使用されているか確認できます。これらのルールの詳細については、「サンプル イベント ルール」（539 ページ）を参照してください。

[Simulate only（シミュレーションのみ）] モードでのルールの効果のテスト手順：

1. コンソール メニューで、[**Rules**（ルール）] > [**Event Rules**（イベント ルール）] の順に選択します。[Event Rules（イベント ルール）] ページが表示され、作成済みのルールとそれらのステータスが表示されます。
2. テストするルールの隣にある [View Details（詳細の表示）] ボタンをクリックします。そのルールの [Edit Event Rule（イベント ルールの編集）] ページが表示されます。
3. ルールの設定を確認し、必要に応じて変更を加えます。

4. ［Status（ステータス）］フィールドで［**Simulate Only**（シミュレーションのみ)］ラジオ ボタンをオンにします。
5. 必要に応じてさらにルールを修正し、［Save（保存)］ボタンをクリックします。**注意：**このプロセスを完了するにはイベント ルールの詳細ページで引き続き作業する必要があるため、［Create & Exit（作成して終了)］ボタンを押さないようにしてください。
6. ページの右にある［Advanced（詳細)］メニューで［**Re-apply rule**（ルールの再適用)］をクリックし、ダイアログ ボックスで期間を選択します。これにより、ルールが適用される過去のイベントの期間が決定されます。一致するイベントの量によっては、最初のテストで短めの期間（［**1 day**（1 日)］など）を選択することを推奨します。期間を選択して［**Go**（実行)］をクリックします。
7. ［History（履歴）］パネルの［Last Processed Event（最後に処理されたイベント）］フィールドに未処理のイベントが表示されなくなるまで、定期的に［Processed Events（処理されたイベント)］パネルの［**Refresh Page**（ページの更新)］ボタンをクリックしてページの内容をしばらく観察します。［Processed Events（処理されたイベント)］パネルに表示される情報の例については、「イベント ルールの履歴と［Processed Events（処理されたイベント）］リスト」（537 ページ）を参照してください。
8. 予想していたイベントが［Processed Events（処理されたイベント)］パネルに表示されない場合や、予想よりも多くのイベントまたは予想と異なるイベントが表示されている場合は、適切にルールを修正し、再び［**Save**（保存)］をクリックして、ルールを再適用します。そのルールに関連するイベントがテーブルに表示され、［Status（ステータス）］フィールドに［Simulated（シミュレート済み)］と表示されます。
9. ルールのシミュレーション期間を長くする場合は、［Re-apply rule（ルールの再適用)］の値を変更して［**Go**（実行)］をクリックします。
10. 予想どおりのイベントが表示され、ルールを有効にしても問題がないと判断できたら、ルールの［Status（ステータス)］フィールドを［**Enabled**（有効)］に変更して、［**Save & Exit**（保存して終了)］をクリックします。以後、新しいイベントに対して、実際にこのルールが実行されるようになります。過去のイベントに対して実際にルールを実行する必要がある場合は、再適用メニューを使用します。

イベント ルールの作成と編集

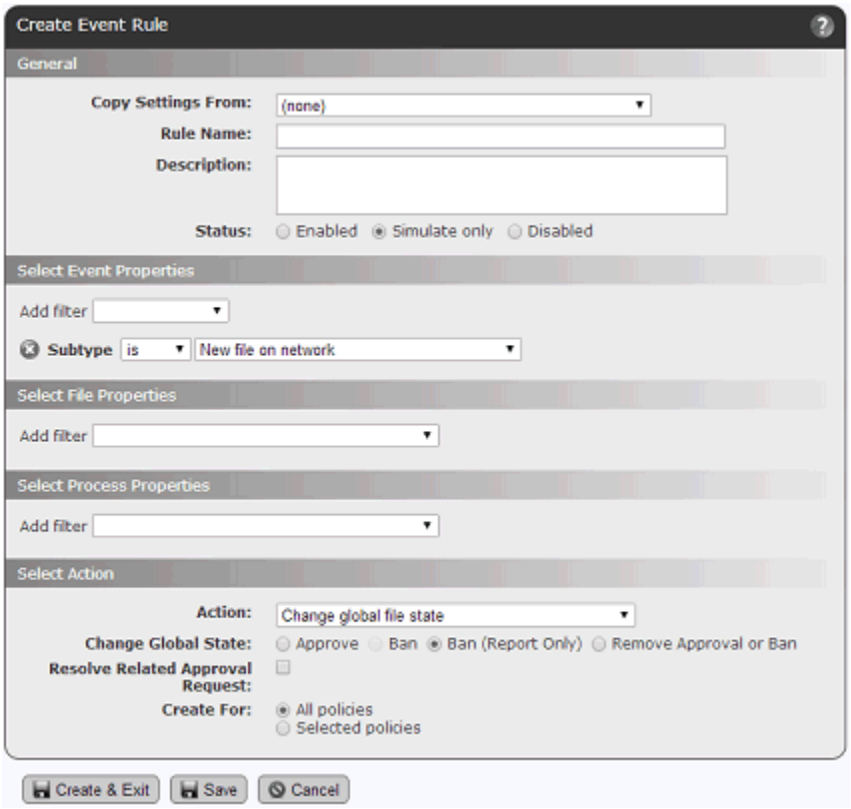
新しいルールを作成するには、既存ルールの設定をコピーして修正するか、新しいルールを一から作成します。少なくとも、下の表の左列に太字で表示されている必須の情報は、いずれの場合も入力する必要があります。

概要	[Add/Edit Event Rule Page（イベント ルールの追加 / 編集）] ページのセクション
ファイル関連のイベントがこの（これらの）基準に一致した場合、…	[Select Event Properties（イベント プロパティの選択）]
… さらに、**イベントで参照されているファイルがこの（これらの）基準に一致**した場合（オプション）、…	[Select File Properties（ファイル プロパティの選択）]
… さらに、**イベントで参照されているプロセスがこの（これらの）基準に一致**した場合（オプション）、…	[Select Process Properties（プロセス プロパティの選択）]
… **次のアクション**を …	[Select Action（アクションの選択）]
… **この（これらの）ポリシー**に含まれるコンピューター上で実行します …	[Select Action（アクションの選択）] / [Create For:（作成の対象：）]

[Select Event Properties（イベント プロパティの選択）]、[Select File Properties（ファイル プロパティの選択）]、および [Select Process Properties（プロセス プロパティの選択）] セクションでは、ルールをトリガーするための基準を複数指定できます。選択するアクションによっては、[Select Action（アクションの選択）] セクションで複数のパラメーターを指定します。

イベント ルールの追加（作成）手順：

1. Bit9 コンソール メニューで、[**Rules**（ルール）] > [**Event Rules**（イベント ルール）] の順に選択します。[Event Rule（イベント ルール）] ページが表示されます。
2. [Event Rule（イベント ルール）] ページで [**Create Rule**（ルールの作成）] を選択します。[Create Event Rule（イベント ルールの作成）] ページが表示されます。このページに表示される設定項目の詳細については、表 63、「イベント ルールのパラメーター」（528 ページ）を参照してください。



3. 新しく作成するルールに似た既存のルールがある場合は、[Copy Settings From（設定のコピー元）] メニューからそのルールを選択します。このメニューで [(none)（なし）] 以外のオプションを選択すると、選択した既存ルールからパラメーターが読み込まれるので、コピー元のルールと異なるパラメーターを変更するだけで新しいルールを作成できます。
4. [Rule Name（ルール名）] フィールドに、そのルールの一意の名前を入力します。既存ルールから設定をコピーした場合、デフォルトの名前はコピー元のルール名の後に「(Copy)」を付けた名前になります。
5. 必要に応じて [Description（説明）] フィールドにルールの説明を入力することもできます（このフィールドへの入力は任意です）。
6. [Status（ステータス）] フィールドで、次のいずれかを選択します。
   - [**Enabled**（有効）] – ルールで指定されているアクションが指定されているとおりに実行されます。

- ［**Simulate only**（シミュレーションのみ）］– ルールで指定されているアクションがシミュレートされます。ルールが有効化されていた場合にどのようにアクションが実行されていたかを示すイベントが生成されますが、指定されているアクションは実際には実行されません。
- ［**Disabled**（無効）］– ルールと設定は維持されますが、指定されているアクションは実行またはシミュレートされません。

重要

新しいイベント ルールの場合は、［Simulate only（シミュレーションのみ）］を選択することを強く推奨します。［Status（ステータス）］フィールドのオプションについては、「ルールを有効化する前のテスト」（522 ページ）を参照してください。

7. ［Select Event Properties（イベント プロパティの選択）］パネルで［Add filter（フィルターの追加）］メニューを使用してイベント プロパティを少なくとも 1 つ選択します。これらのフィルターには次の要件があります。
   - ［Subtype（サブタイプ）］フィルターを少なくとも 1 つ追加する必要があります。
   - イベント ルールのトリガーとして使用できるイベントはファイルまたはコンピューターに関連するイベントのみであるため、このメニューの選択項目もそれに応じて限定されています。
   - イベントで出現する一部のファイル関連プロパティは［File Properties（ファイル プロパティ）］メニューに表示されるため、ここには表示されません。
   - イベント ルールのフィルターでファイル名またはパス名を使用するには、［File Properties（ファイル プロパティ）］のフィルターではなく［Event Properties（イベント プロパティ）］のフィルターを使用してファイル名またはパス名を指定する必要があります。通常、［Event Properties（イベント プロパティ）］の［File name（ファイル名）］は、［File Property（ファイル プロパティ）］の［First Seen Name（最初に確認された名前）］よりも多くのイベントに一致します。
8. ［Select File Properties（ファイル プロパティの選択）］パネルの［Add filter（フィルターの追加）］メニューで、このルールがトリガーされる状況をさらに絞り込むためのファイル プロパティを 1 つまたは複数選択します。ここに表示される選択肢は Bit9 ファイル カタログのフィールドとほぼ同じですが、ファイル カタログにはないフィールドもいくつかあります。このパネルに表示される選択肢の一部については、「イベント ルール定義のファイル プロパティとプロセス プロパティ」を参照してください。

注意

［Select File Properties（ファイル プロパティの選択）］および［Select Process Properties（プロセス プロパティの選択）］で拡張子フィルターを選択する場合は、（*.bat* ではなく *bat* のように）先頭にドットを付けずにファイル拡張子を指定する必要があります。この規則に従わないと、ルールが正しく機能しません。

9. ［Select Process Properties（プロセス プロパティの選択）］パネルの［Add filter（フィルターの追加）］メニューで、このルールがトリガーされる状況をさらに絞り込むためのプロセス プロパティを 1 つまたは複数選択します。ここに表示される選択肢は Bit9 ファイル カタログのフィールドとほぼ同じですが、ファイル カタログにはないフィールドもいくつかあります。このパネルに表示される選択肢の一部については、「イベント ルール定義のファイル プロパティとプロセス プロパティ」を参照してください。

注意

この設定オプションが適用されるプロセスは、ファイルの実行時にオペレーティング システムのタスク マネージャーに表示されるプロセスではなく、イベントまたはイベント ルールで参照されているファイルの親プロセスです。

10. ［Select Action（アクションの選択）］パネルの［Action（アクション）］メニューで、イベントとファイルがこのルールに一致したときに実行するアクションを選択します。このメニューに表示されるオプションは、ルールの作成または編集を行っているコンソール ユーザーの権限によって異なります。「アカウント グループの権限」（108 ページ）を参照してください。表示される可能性があるオプションには以下のものがあります。

- ［**Change global file state**（ファイルのグローバル状態を変更）］– ルールに一致したファイルのグローバル状態を自動的に変更します。ルールに一致したファイルに対して、承認、「レポートのみの禁止」の作成、承認の削除、または禁止を実行できます。また、状態の変更をすべてのポリシーに適用するか、選択されたポリシーのみに適用するかを指定することもできます。

  注意：イベント ルールを通じて（レポートのみではなく）実際の禁止を適用する機能はデフォルトで無効になっています。この機能を有効にする必要がある場合は、Bit9 サポートにお問い合わせください。

- ［**Change local file state**（ファイルのローカル状態を変更）］– ルールに一致したファイルのローカル状態を自動的に変更します。ルールに一致したファイルをローカルで承認するか、ローカル承認を削除することができます。

- ［**Upload file**（ファイルをアップロード）］– Bit9 によって管理されているコンピューター上でルールに一致するファイルが見つかった場合、そのコンピューターから Bit9 Server にそれらのファイルをアップロードします。デフォルトのアップロード先を使用することもできますが、サーバーまたはアクセス可能な他のコンピューター上の適切な場所をアップロード先として定義することもできます。たとえば、新しく発見されたすべてのファイルを特定のシステムにアップロードして手動で調査したり、特定のシステム上に存在するツールでスキャンすることができます。

  このアクションを選択するには、ログイン中のユーザー アカウントに［Manage uploads of inventoried files（登録済みファイルのアップロードの管理）］権限が付与されている必要がありますが、デフォルトでこの権限を与えられている標準のアカウント グループはありません。

- ［**Analyze file**（ファイルを分析）］– 接続されている分析用デバイスにファイルを送信します。Bit9 Connector で設定されている任意の分析サービスを選択することができ、複数のサービスにファイルを送信することもできます。
- ［**Move computer**（コンピューターを移動）］– ルールに一致するイベントが発生したときに、イベントで参照されているコンピューターを他のポリシーに移動します。

  ［Move computer（コンピューターを移動）］オプションはデフォルトで無効になっています。この機能を使用する必要がある場合は、Bit9 テクニカル サポートにお問い合わせください。

11. ［Action（アクション）］メニューでの選択がファイル状態の変更に関係する場合は、ファイルに関連する承認要求を自動的に解決できるように設定することもできます。これを行うには、［**Resolve Related Approval Request**（関連する承認要求を解決）］チェックボックスをオンにします。このチェックボックスがオフになっている場合は、手動で解決されるまで、関連するファイルの承認要求は未解決のままになります。関連する承認要求が存在しない場合、このチェックボックスは効果を持ちません。承認要求がどのように送信されて解決されるかについては、「承認要求と根拠」（572 ページ）を参照してください。
12. ルールの定義が完了したら［Save（保存）］をクリックし、同じページ内で「イベント ルールの有効化、無効化、および削除」の手順に進みます。

    または

    ルールを作成した後に［Create Event Rule（イベント ルールの作成）］ページを閉じるには、［**Create & Exit**（作成して終了）］をクリックします。

表 63 に、［Create/Edit Event Rule（イベント ルールの作成 / 編集）］ページで設定可能なパラメーターを示します。

表 63：イベント ルールのパラメーター

パネル：フィールド	説明
［Copy Settings From:（設定のコピー元：）］	初期設定のコピー元として使用する既存ルール。設定をコピーしない場合は、デフォルト値の［(none)（なし）］を選択します。
［Rule Name（ルール名）］	このルールを識別するための名前。（必須）
［Description（説明）］	ルールに関する追加情報。任意のテキストを入力できます。（オプション）

パネル：フィールド	説明
[Status（ステータス）]	このルールを有効にするかどうかを決定し、どのように有効化するかを決定するラジオ ボタン。 • [**Enabled**（有効）] – ルールで指定されているアクションが指定されているとおりに実行されます。 • [**Simulate only**（シミュレーションのみ）] – ルールで指定されているアクションがシミュレートされます。ルールが有効化されていた場合にどのようにアクションが実行されていたかを示すイベントが生成されますが、指定されているアクションは実際には実行されません。新規に作成するルールの場合は、このオプションがデフォルト値になります。 • [**Disabled**（無効）] – ルールと設定は維持されますが、指定されているアクションは実行またはシミュレートされません。サンプル ルールではこのオプションがデフォルトで選択されています。
[Select Event Properties（イベント プロパティの選択）]：[Add Filter（フィルターの追加）]	このルールをトリガーするイベントのプロパティ。 • [**Subtype**（サブタイプ）] – このフィルターではイベント サブタイプ フィルター（ [New file on network（ネットワーク上の新規ファイル）] など）を少なくとも 1 つ指定する必要があります。複数のサブタイプを追加することもできます。たとえば、[New file on network（ネットワーク上の新規ファイル）] イベントまたは [New unapproved file to computer（コンピューターに追加された新規の未承認ファイル）] イベントのいずれかが発生したときにルールをトリガーできます。 • **[Other Event properties（その他のイベント プロパティ）]** – このフィルターにはその他のプロパティも追加できます。イベントで出現する一部のファイル関連プロパティは [File Properties（ファイル プロパティ）] メニューに表示されるため、ここには表示されません。
[Select File Properties（ファイル プロパティの選択）]：[Add Filter（フィルターの追加）]	このルールがトリガーされる状況をさらに絞り込むためのファイル プロパティ。ここに表示される選択肢は Bit9 ファイル カタログのフィールドとほぼ同じです。このパネルに表示される選択肢の一部については、「イベント ルール定義のファイル プロパティとプロセス プロパティ」（534 ページ）を参照してください。イベント ルールでのファイル プロパティの指定は必須ではありません。 **注意**：指定したファイル プロパティを利用できない場合はルールが実行されず、ルールに一致したイベントはそのプロパティが利用可能になるまで保留状態になります。たとえば、Bit9 SRS レピュテーションの信頼レベルが 5 以下のファイルに一致するルールを作成しても、Bit9 SRS が設定されていないためにファイルの信頼度情報を利用できなければ、その他すべてのルール パラメーターに一致した場合でもそのルールは実行されません。これはファイルの普及度やメタデータにも当てはまります。

パネル：フィールド	説明
[Select Process Properties（プロセス プロパティの選択）]：[Add Filter（フィルターの追加）]	このルールがトリガーされる状況をさらに絞り込むためのプロセス プロパティ。 ここに表示される選択肢は Bit9 ファイル カタログのフィールドとほぼ同じです。このパネルに表示される選択肢の一部については、「イベント ルール定義のファイル プロパティとプロセス プロパティ」（534 ページ）を参照してください。イベント ルールでのプロセス プロパティの指定は必須ではありません。 **注意**：指定したプロセス プロパティを利用できない場合はルールが実行されず、ルールに一致したイベントはそのプロパティが利用可能になるまで保留状態になります。たとえば、Bit9 SRS レピュテーションの信頼レベルが 5 以下のファイルに一致するルールを作成しても、Bit9 SRS が設定されていないためにファイルの信頼度情報を利用できなければ、その他すべてのルール パラメーターに一致した場合でもそのルールは実行されません。これはファイルの普及度やメタデータにも当てはまります。

パネル：フィールド	説明
[Select Action（アクションの選択）]：[Action（アクション）]	[Actions（アクション）] メニューには次のオプションが表示されます。 • [**Change global file state**（ファイルのグローバル状態を変更）] – ルールに一致したファイルのグローバル状態を自動的に変更します。ルールに一致したファイルに対して、承認、「レポートのみの禁止」の作成、承認の削除、または禁止を実行できます。また、状態の変更をすべてのポリシーに適用するか、選択されたポリシーのみに適用するかを指定することもできます。 **注意**：イベント ルールを使用して（レポートのみではなく）実際の禁止を適用する機能はデフォルトで無効になっています。この機能を有効にする必要がある場合は、Bit9 サポートにお問い合わせください。 • [**Change global process state**（プロセスのグローバル状態を変更）] – ルールに一致したプロセスのファイルのグローバル状態を自動的に変更します。ルールに一致したプロセスに対して、承認、「レポートのみの禁止」の作成、承認の削除、または禁止を実行できます。また、状態の変更をすべてのポリシーに適用するか、選択されたポリシーのみに適用するかを指定することもできます。 • [**Change local file state**（ファイルのローカル状態を変更）]– ルールに一致したファイルのローカル状態を自動的に変更します。ルールに一致したファイルをローカルで承認するか、ローカル承認を削除することができます。 • [**Upload file**（ファイルをアップロード）] – Bit9 によって管理されているコンピューター上でルールに一致するファイルが見つかった場合、そのコンピューターから Bit9 Server にそれらのファイルをアップロードします。デフォルトのアップロード先を使用することもできますが、サーバーまたはアクセス可能な他のコンピューター上の適切な場所をアップロード先として選択することもできます。たとえば、新しく発見されたすべてのファイルを別のコンピューターにアップロードして手動で調査したり、特定のシステム上に存在するツールでスキャンすることができます。 **注意**：このオプションは、一方または両方の［Manage uploads of inventoried files（登録済みファイルのアップロードの管理）］権限を持つコンソール ユーザーに対してのみ表示されます。「アカウント グループの権限」（108 ページ）を参照してください。 • [**Analyze file**（ファイルを分析）] – ルールの条件が満たされたときに、接続されている分析用デバイスにファイルを送信します。Bit9 Connector を介して Bit9 Server に統合され、現在有効になっている分析サービスのチェックボックスを 1 つ以上オンにします。設定されているサービスがない場合、このオプションは表示されません。

パネル：フィールド	説明
	• [**Move computer**（コンピューターを移動）] – ルールに一致するイベントが発生したときに、イベントで参照されているコンピューターを他のポリシーに移動します。このメニューには次のオプションがあります。 [**Specify policy**（ポリシーを指定）] – このオプションを選択すると、Bit9 Server 上で設定されているポリシーのメニューが表示されます。 [**Restore to normal enforcement level**（通常の適用レベルに戻す）] – このオプションを選択すると、[Local Approval（ローカル承認）] モードで動作しているコンピューターが以前のポリシーに戻されます。コンピューターが [Local Approval（ローカル承認）] モードで動作していない場合、この設定は効果を持ちません。 [**Local approval**（ローカル承認）] – このオプションを選択すると、コンピューターが [Local Approval（ローカル承認）] モードに移行されます。詳細については、「ローカル承認モードへのコンピューターの移行」（314 ページ）を参照してください。 [**Automatic policy**（自動ポリシー）] – このオプションを選択すると、Active Directory マッピングによって割り当てられるポリシーにコンピューターが移動されます。AD マッピングが有効になっていない場合、この設定は効果を持ちません。 **注意**：[**Move computer**（コンピューターを移動）] オプションはデフォルトで無効になっています。このアクションを使用する必要がある場合は、Bit9 サポートにお問い合わせください。
[Resolve Related Approval Request（関連する承認要求を解決）]	このチェックボックスは、ルールの [Action（アクション）] メニューで [Change global file state（ファイルのグローバル状態を変更）] または [Change local file state（ファイルのローカル状態を変更）] が選択されている場合に表示されます。このチェックボックスをオンにすると、このファイルで参照されているファイルに関連する承認要求のステータスが [Resolved（解決済み）] に変更されます。
[Priority（優先度）]	ルールの [Action（アクション）] メニューで [Upload file（ファイルをアップロード）] または [Analyze file（ファイルを分析）] が選択されている場合は、アップロードまたは分析の優先度を [Low（低）]、[Medium（中）]、または [High（高）] に設定できます。これにより、指定されているアクションを他のアップロード要求または分析要求よりも先に実行するか後に実行するかが決定されます。要求の処理が進行中の場合は、[Requested Files（要求されたファイル）] ページで優先度を変更できます。

イベント ルールの編集

既存のルールを編集するには、表 63、「イベント ルールのパラメーター」（528 ページ）で説明されているパラメーターを変更します。ただし、一度作成したルールのアクション設定は変更できません。別のアクションを指定するには、別の権限を持つ Bit9 コンソール ユーザー アカウントでログインしなければならない場合があります。また、1 つのルールで別々の種類のアクションが記録されると、

ルールの履歴が役に立たなくなります。アクションを変更する場合は、新しいルールを作成する必要があります。［Copy Settings from（設定のコピー元）］フィールドを使用して既存ルールのパラメーターの多くをコピーし、アクションだけを変更して保存すれば、新しいルールを簡単に作成できます。［Action（アクション）］の下にある一部のオプション（適用対象のポリシーや承認要求に関する設定）は変更できます。

［Edit Event Rule（イベント ルールの編集）］ページのメニュー

［Edit Event Rule（イベント ルールの編集）］ページの右側には 2 つのメニューがあります。［Related Views（関連ビュー）］メニューには次のコマンドが 1 つ以上表示されます（ルールで選択されている［Action（アクション）］によって異なります）。

- ［**All file rules created by this rule**（このルールによって作成されたすべてのファイル ルール）］–［Software Rules: Files Approvals and Bans（ファイルの承認と禁止）］ページが表示され、このイベント ルールによって作成されたファイル ルールが表示されます（ローカルのファイル承認はこのページで追跡されないため表示されません）。
- ［**All file uploads created by this rule**（このルールによって開始されたすべてのファイル アップロード）］–［Requested Files: Uploaded Files（要求されたファイル：アップロードされたファイル）］ページが表示され、このルールによって開始されたアップロードが表示されます。
- ［**All file analysis submissions created by this rule**（このルールによって開始された分析サービスへのファイル送信）］–［Requested Files: Analyze file（要求されたファイル：分析されたファイル）］ページが表示され、Bit9 Connector で設定されている分析サービスへのファイル送信が表示されます。
- ［**Related events**（関連イベント）］–［Events（イベント）］ページが表示され、このルールに関連するイベントが表示されます。

［Action（アクション）］メニューには次のコマンドが 1 つ以上表示されます。

- ［**Cancel all file analysis submissions created by this rule**（このルールによって開始された分析サービスへのファイル送信をすべてキャンセル）］– ファイル分析ルールの場合、Bit9 Connector で設定されている分析サービスへのファイル送信がすべてキャンセルされます（ただし、未完了の送信タスクだけが対象になります）。このルールによって開始された分析サービスへのファイル送信が既に完了している場合、この設定は効果を持ちません。
- ［**Cancel all file uploads created by this rule**（このルールによって開始されたファイルのアップロードをすべてキャンセル）］– ファイル アップロード ルールの場合、このルールによって開始されたファイル アップロードがすべてキャンセルされます（ただし、未完了のアップロード タスクだけが対象になります）。ファイルのアップロードが既に完了している場合、この設定は効果を持ちません。
- ［**Create Alert**（アラートの作成）］–［Add Alert（アラートの追加）］ページが開き、イベント ルールの情報に基づいてアラートが部分的に設定されます。すべての項目を設定して保存すると、このイベント ルールがトリガーされるたびにアラートが表示されるようになります。

［Advanced（詳細）］メニューには次のコマンドが 1 つ以上表示されます。

- ［**Re-apply rule**（ルールの再適用）］– 過去の開始点を選択して、その時点から現在までに発生したすべてのイベントにこのルールを再適用できます。このアクションは新しいルールや編集済みのルールを［Simulate only（シミュレーションのみ）］モードでテストしてから［Enabled（有効）］モードに切り替える場合に役立ちます。また、有効モードに切り替える前に発生したイベントにルールを再適用する場合にも使用できます。
- ［**Clear processed events**（処理済みのイベントをクリア）］– シミュレートされたイベント、実行されたイベント、およびスキップされたイベントが［Processed Events（処理されたイベント）］パネルから消去されます。保留中のイベントは消去されません。

イベント ルールのランキング

イベント ルールは最も高いランクのプロセス（ランク番号が最も小さいプロセス）から順番に処理されます。処理の順序はテーブル内での現在の並び順ではなくルールのランク番号のみに基づいて決定されます。一致したルールのうち、現在有効になっているものだけがすべて処理されます。ルールのランクを変更するには、［Event Rule（イベント ルール）］ページのテーブルをランク順に並べ替え、各ルールの隣にある上矢印と下矢印を使用します。

イベント ルール定義のファイル プロパティとプロセス プロパティ

［Add/Edit Event Rule Page（イベント ルールの追加 / 編集）］ページの［Select File Properties（ファイル プロパティの選択）］パネルと［Select Process Properties（プロセス プロパティの選択）］パネルに表示されるオプションの中には、ルールの評価に影響する特殊な動作を伴うものがあります。たとえば、イベント ルールのフィルターで指定されているデータが欠落したイベントが発生した場合の動作が問題となります。そのようなイベントの評価は、指定されているデータが利用可能になるまで保留されます。以降のセクションでは、ルールの評価に影響するこのような状況について説明します。

Bit9 SRS の信頼度データと脅威データ

ルールの［File or Process Properties（ファイルまたはプロセスのプロパティ）］でいずれかの Bit9 SRS パラメーター（［Trust（信頼度）］または［Threat（脅威）］）が選択されている場合、そのルールはこれらのフィールドで指定された値を持つイベントが発生した場合にのみトリガーされます。［Trust（信頼度）］または［Threat（脅威）］の値がまだ存在していないファイルに関連するイベントは、Bit9 SRS の情報が利用可能になるまで保留状態になります（イベントの状態は一致したルールの［Processed Events（処理されたイベント）］リストに表示されます）。それらのイベントは、該当するデータが利用可能になって時点で、ルールに基づき評価されます。

［Trust（信頼度）］の値が（存在しないのではなく）不明である場合の動作にも注意が必要です。Bit9 SRS と Bit9 Server の間でファイル情報が同期されているものの、各ファイルの信頼度情報が存在していない場合は、Bit9 コンソールに［Trust（信頼度）］の値が何も表示されません。一方、信頼度が不明なファイルに関しては、［Trust（信頼度）］の値として -1 が割り当てられます。したがって、一定の信頼度を下回るファイルに対してアクションを実行するように設定されたイベントルールは、指定された信頼度に満たないファイルだけでなく、信頼度が不明なファイルに対してもトリガーされます。信頼度が（不明ではなく）一定の値を下回る

ファイルにのみルールのアクションを実行するには、さらに条件を追加して、信頼度が 0 以上である場合にルールをトリガーするように指定します。

ファイル普及度

フィルターのパラメーターとしてファイルの普及度が選択されている場合、そのルールは関連するファイルの普及度が計算されているイベントが発生した場合にのみトリガーされます。普及度の値がまだ設定されていないファイルに関連するイベントは、普及度の値が利用可能になるまで保留状態になります。また、特定の設定（Microsoft サポート ファイルを追跡の対象から除外する設定や、特定のポリシーを追跡の対象から除外する設定など）を使用すると、普及度を正確にレポートできなくなることに注意してください。

ファイル メタデータ

ファイル フィルターまたはプロセス フィルターの一部としていずれかのファイル メタデータ フィールド（ファイル タイプ、ファイル サイズ、会社、公開者、製品など）が使用されている場合、その他の条件に一致するイベントが発生しても、フィルターで指定されているメタデータがそのファイルに関してエージェントからレポートされるまでそのイベントは評価されません。通常、イベントがレポートされてから関連するファイル メッセージが届くまでの時間は数秒間です。ただし、エージェントからレポートするファイルが大量に残っている場合や、イベントが送信された直後にエージェントがオフラインになった場合はこの時間が長くなり、イベント ルールの評価が保留されることがあります。

ファイル拡張子

［Select File Properties（ファイル プロパティの選択）］および［Select Process Properties（プロセス プロパティの選択）］でファイル拡張子をフィルターとして選択する場合は、先頭にドットを付けずにファイル拡張子を指定する必要があります。たとえば、*bat* 拡張子を持つバッチ ファイルに対してルールがトリガーされるように指定するには、*.bat*（ドット付きの bat）ではなく、*bat* のみを使用します。この規則に従わないと、ルールが正しく機能しません。

分析結果オプション

［Select File Properties（ファイル プロパティの選択）］および［Select Process Properties（プロセス プロパティの選択）］フィルターのメニューには、Bit9 ファイル カタログには存在しないファイル分析オプションが含まれています。それらのオプションを使用すると、外部デバイスによる分析の結果に基づいてアクションを実行できます。これに該当するオプションは［Analysis Result: Check Point（分析結果：Check Point）］、［Analysis Result:Palo Alto Networks Wildfire（分析結果：Palo Alto Networks Wildfire）］、［Analysis Result: FireEye（分析結果：FireEye）］および［Analysis Result: Microsoft SCEP（分析結果：Microsoft SCEP）］で、これらを選択すると、各デバイスから返された最新のファイル分析結果が表示されます。表示される可能性がある値は次のいずれかになります。

- ［**Unknown**（不明）］– 対象ファイルがまだこのサービスで分析されていないことを示します。
- ［**Clean**（クリーン）］– 対象ファイルがこのプロバイダーで分析されていて、疑わしいコンテンツが見つからなかったことを示します。

- [**Potential Risk**（危険な可能性あり）] – 対象ファイルがこのプロバイダーで分析されていて、危険の可能性が見つかっていることを示します。現在のところ、この状態が設定される可能性があるのは、FireEye でユーザーが作成した脅威マッピングに対象ファイルが一致した場合のみです。
- [**Malicious**（悪質）] – 対象ファイルがこのプロバイダーで分析されていて、悪意のあるファイルとしてレポートされていることを示します。
- [**Analysis Pending**（分析中）] – 対象ファイルがこのプロバイダーでまだ分析中であることを示します。
- [**Analysis Error**（分析エラー）] – 対象ファイルの分析時にエラーが返されたことを示します。

Bit9 SRS や普及度フィルターと同様に、分析フィルターが指定されているルールに一致するイベントが発生した場合でも、そのイベントで参照されているファイルの分析結果がまだ存在していない場合は、ルールの評価が保留されます。

注意

- SCEP 通知にはファイル　ハッシュが含まれていません。Bit9 は、SCEP 通知に含まれるその他のデータ（プロセス名、ファイル名、書き込み時間、ユーザー名、コンピューター名）とデータベース内のファイルを比較し、相関関係が見つかった場合は、[File Catalog（ファイル カタログ）] に登録されているハッシュを SCEP 通知に関連付けます。そのため、Bit9 エージェント システム上のクリーンなファイルが SCEP で悪意のあるファイルとして認識される場合があります。したがって、SCEP 通知のみに基づくイベント ルールはクリーンなファイルに対してもトリガーされる可能性があり、ルールで指定されているアクションによっては悪影響が生じるおそれがあります。SCEP 分析結果をプロパティで使用するすべてのイベント ルールで、ファイルの信頼度やファイルの普及度などの追加の要素を使用することを推奨します。
- 作成済みの脅威マッピング ルールがある場合は、FireEye 通知に基づくイベント ルールを作成する前に、脅威マッピング ルールの内容を確認してください。脅威マッピングが分析結果に影響して、イベント ルールがトリガーされる状況が変わる場合があります。「FireEye 脅威レベル マッピング」(872 ページ) を参照してください。

カタログ登録されていないファイルのグローバル禁止

イベント ルールでは、Bit9 エージェントからサーバーにまだレポートされていないファイルについてもグローバル禁止を作成できます。このアクションは、ルールの [Event Properties（イベント プロパティ）] で特定のイベント サブタイプ（[Malicious File Detected（悪意のあるファイルの検出）] など）が指定されていて、そのルール定義に一致するイベントをトリガーしたファイルが Bit9 Server に接続されている分析サービスからレポートされている場合に実行されます。ルール内でその他のプロパティが定義されていない場合は、該当するファイルの「事前禁止」が直ちに作成されるため、そのファイルがいずれかのエージェント コンピューター上に出現したときには既に禁止されています。

一方、ルールの定義に［File Properties（ファイル プロパティ）］フィルターが追加されている場合は、レポート済みのファイルがエージェント管理コンピューター上に実際に出現し、ルール内で指定されているプロパティに基づいて評価できるようになるまで、そのルールは保留状態になります。［Process Properties（プロセス プロパティ）］フィルターが定義されている場合、どのプロセスにも関連しないイベントはスキップされ、イベント ビューに記録されません。

イベント ルールによる承認がエンドポイントに与える影響

イベント ルールによるローカル承認は直ちに（またはエージェントがサーバーに接続されると同時に）適用されます。ただし、他の大部分の承認とは異なり、イベント ルールによるグローバル承認およびポリシーごとの承認はエンドポイントへ自動的にはプッシュされません。レピュテーション ルールと同様に、イベント ルールによるファイル承認がエンドポイントにプッシュされる状況には次の 3 種類があります。

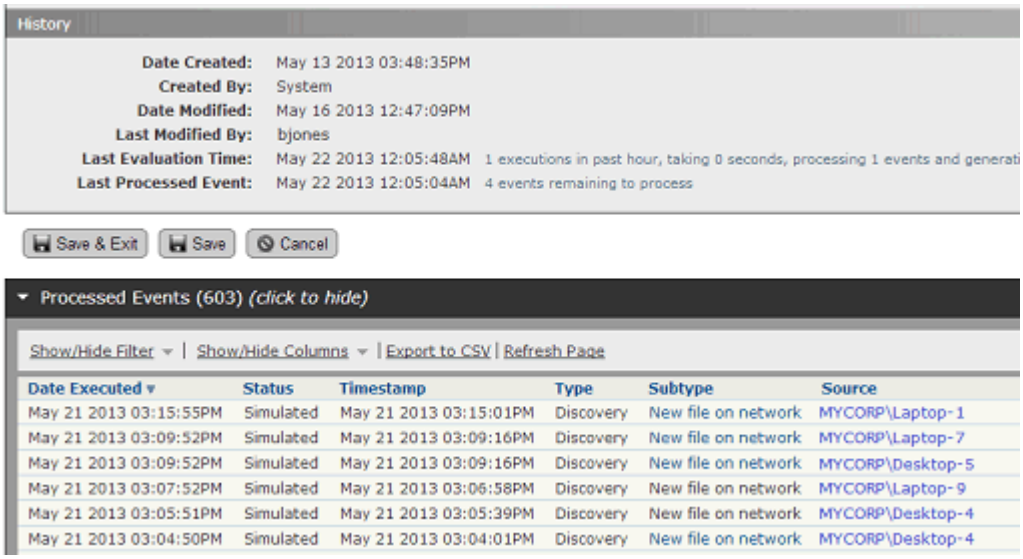
- いずれかのエンドポイントでブロックされているファイルの記録が Bit9 Server 上にあり、後でそのファイルがイベント ルールによって承認された場合、サーバーは接続されているエージェントに対してそのファイルが承認されたことを直ちに通知し始めます。
- イベント ルールによって承認されたファイルのインスタンスを Bit9 Server に接続されたコンピューター上でユーザーが実行しようと試みた場合、サーバーはエージェントに対してそのファイルの実行を直ちに許可し、そのファイルが承認されたことを他のエージェントにも通知し始めます。
- イベント ルールによって承認されたファイルがインストーラーとして識別された場合、Bit9 Server はエージェントに対してそのファイルが承認されたことを直ちに通知し始めます。

ファイルがイベント ルールによって承認され、他のルールによりブロックされなかった場合でも、上記いずれかの状況が発生してファイルの承認がエージェントに通知されない限り、そのファイルのインスタンスはローカルで承認されず、ファイルの承認が通知される前にエージェント コンピューターがサーバーに接続されていなかった場合はブロックされる可能性があります。

イベント ルールによってファイルがグローバルまたはポリシーごとに承認された後、イベント ルールによってその承認が取りされた場合、そのファイルの承認はサーバーに接続されているコンピューター上でも取り消され、［File Catalog（ファイル カタログ）］でのファイル状態は未承認に戻されます。ただし、イベント ルールによって承認されたときにそのファイルのインスタンスが実行されていた場合、承認時にサーバーに接続されていたコンピューター上のインスタンスはすべてローカルで承認され続けます。

イベント ルールの履歴と［Processed Events（処理されたイベント）］リスト

各ルールによって処理されたイベントの履歴はイベント ルールの詳細（［Edit Event Rule（イベント ルールの編集）］）ページの［History（履歴）］パネルに表示されます。Bit9 データベースからイベントがトリミングされると、この履歴も自動的にトリミングされます。



［History（履歴）］には次の情報が表示されます。

- ［**Date Created**（作成日）］– このルールが作成されたときのタイム スタンプ。
- ［**Created By**（作成者）］– このルールを作成したユーザーの Bit9 コンソール ログイン アカウント。
- ［**Date Modified**（変更日）］– このルールが最後に変更されたときのタイム スタンプ。
- ［**Last Modified By**（最終変更者）］– このルールを最後に変更したユーザーの Bit9 コンソール ログイン アカウント。
- ［**Last Evaluation Time**（最終評価時刻）］– 一致するイベントによってこのルールが最後にトリガーされたときのタイム スタンプ。このフィールドには、過去 1 時間に発生したこのルールの処理に関する統計（ルールがトリガーされた回数、処理されたイベントの数、処理の所要時間など）も表示されます。
- ［**Last Processed Event**（最後に処理されたイベント）］– このルールによって最後に処理されたイベントのタイム スタンプ。この値は処理中のイベントが大量に残っているかどうかをイベント ログで確認したり、次に処理されるイベントを確認するときに役立ちます。「処理中」とは、ルールが処理されていることを示しますが、最終的なアクションが完了したことを示すわけではないことに注意してください。

［Edit Event Rule（イベント ルールの編集）］ページの［History（履歴）］パネルの下には、現在のルールによって処理されたイベントを示す［Processed Events（処理されたイベント）］テーブルが表示されます。この情報はルールの影響を監視するときに役立ちます。このテーブルには、処理された各イベントのステータスとして次のいずれかが表示されます。

- ［**Pending**（保留中）］– このイベントはルールに一致しましたが、ルールのアクションがまだ完了していません。アクションがまだ完了していない理由に関して何らかの情報がある場合は、［Status（ステータス）］の上にマウス ポインターを置くとツールチップにそれらの情報が表示されます。
- ［**Simulated**（シミュレート済み）］– このイベントは［Simulate only（シミュレーションのみ）］モードで処理されました。この処理はイベントとして記録

されていますが、実際のアクションは実行されていません。詳細については、「イベント ルールの有効化、無効化、および削除」を参照してください。

- ［**Executed**（実行済み）］– このイベントはルールによって処理され、指定されたアクションが実行されました。
- ［**Skipped**（スキップ済み）］– ルールで指定されているアクションが禁止されているか、ルールの定義が現在の状況に一致しないため、ルールがスキップされました。たとえば、禁止済みのファイルをグローバルに承認しようとするルールはスキップされます。

サンプル イベント ルール

Bit9 コンソールのメニューから［**Rules**（ルール）］>［**Event Rules**（イベント ルール）］を選択してアクセスできる［Event Rules（イベント ルール）］ページには、さまざまなサンプル ルールが含まれています。これらのルールの隣にある［View Details（詳細の表示）］ボタンをクリックすると詳細ページが表示され、各ルールがどのように定義されているかを確認できます。新しいルールを作成する際には、これらのサンプル ルール（またはその他の既存ルール）をテンプレートとして使用することもできます。たとえば、サンプル ルールに変更を加え、［Carbon Black watchlist（Carbon Black のウォッチリスト）］サブタイプに一致するイベントがレポートされたときに、イベントで参照されているファイルとプロセスを禁止または分析するルールを作成できます。

注意

分析ツールの環境（特定のオペレーティング システムを実行している分析環境など）に依存するイベント ルールを作成し、その環境が利用できなくなった場合、その環境が再び利用可能になるまで数分間待機した後、そのイベント ルールは自動的に無効になります。

サンプル ルール：［Analyze files from approval requests（承認要求の対象ファイルを分析）］

このルールは、承認要求の対象ファイルを 1 つ以上の分析サービスに送信します。デフォルトのファイル送信先は WildFire ですが、［System Administration（システム管理）］ページの [Bit9 Connector] タブで設定されている他の分析サービスにファイルを送信するようにルールを変更することもでき、複数のサービスから分析結果を要求することもできます。選択したサービスから分析結果が既にレポートされているファイルは送信されません。承認要求の詳細については、「承認要求と根拠」（572 ページ）を参照してください。Bit9 Connector を使用して Bit9 Platform に分析サービスを統合する方法については、第章「Bit9 Connector for Network Security Devices」を参照してください。

このルールのデフォルトのプロパティは次のとおりです。

- **［Event Properties（イベント プロパティ）］**：［Subtype（サブタイプ）］が［Approval request created（承認要求の作成）］である

- ［**File Properties（ファイル プロパティ）**］：［Analysis Result: Palo Alto Networks WildFire（分析結果：Palo Alto Networks WildFire）］が［**Unknown（不明）**］である
- ［**Process Properties（プロセス プロパティ）**］：なし
- ［**Action（アクション）**］：［Analyze file（ファイルを分析）］
  - ［**Priority（優先度）**］：［Medium（中）］
  - （分析サービスの選択）：未選択

サンプル ルール：［Resolve approval requests for clean files（クリーンなファイルの承認要求を解決）］

承認要求の対象ファイルが WildFire で既に分析されていてクリーンであると判定されている場合、このルールはそれらのファイルをローカルで承認した後で、関連する承認要求を解決します。このルールを使用する場合は、ファイルの分析が行われてから承認要求が解決されるようにするために、［Analyze files from approval requests（承認要求の対象ファイルを分析）］ルールと一緒に有効化する必要があり、こちらのルールを分析ルールよりも低いランクに設定する必要があります。

このルールのデフォルトのプロパティは次のとおりです。

- ［**Event Properties（イベント プロパティ）**］：［Subtype（サブタイプ）］が［Approval request created（承認要求の作成）］である
- ［**File Properties（ファイル プロパティ）**］：［Analysis Result: Palo Alto Networks WildFire（分析結果：Palo Alto Networks WildFire）］が［**Clean（クリーン）**］である
- ［**Process Properties（プロセス プロパティ）**］：なし
- ［**Action（アクション）**］：［Change local file state（ファイルのローカル状態を変更）］
  - ［**Change local state（ローカル状態の変更）**］：［Approve（承認）］
  - ［**Resolve Related Approval Request（関連する承認要求を解決）**］：未選択

このルールは、接続されている複数のデバイスまたはサービスの分析結果に基づいてアクションを実行するように変更することもできますが、すべての分析要求が完了するまでは保留状態になります。

サンプル ルール：［Analyze downloaded files（ダウンロードされたファイルを分析）］

このルールは Web ブラウザーから Bit9 で管理されているコンピューターにダウンロードされた特定のファイルを Palo Alto Networks WildFire に送信して分析を行います。信頼できることを示すプロパティを持っているファイル、WildFire によって分析結果が既にレポートされているファイル、WildFire での分析の要件を満たしていないファイルは除外されます。また、一部分しかダウンロードされていないファイルも除外されます。

このルールのデフォルトのプロパティは次のとおりです。

- ［**Event Properties（イベント プロパティ）**］:
  - ［**Subtype**（サブタイプ）］が［New file on network（ネットワーク上の新規ファイル）］である
  - ［**Process**（プロセス）］の末尾に *iexplore.exe*、*firefox.exe*、または *chrome.exe* がある
  - ［**File Name**（ファイル名）］に *.crdownload* または *.part* が含まれていない
- ［**File Properties（ファイル プロパティ）**］:
  - ［**File Size**（ファイル サイズ）］が *10240000* より小さい
  - ［**File State**（ファイルの状態）］が［Approved（承認済み）］でない
  - ［**File Type**（ファイル タイプ）］が［Application（アプリケーション）］である
  - ［**Analysis Result: Palo Alto Networks WildFire**（分析結果：Palo Alto Networks WildFire）］が［Unknown（不明）］である
- ［**Process Properties（プロセス プロパティ）**］: なし
- ［**Action（アクション）**］:［Analyze file（ファイルを分析）］
  - ［**Priority（優先度）**］:［Medium（中）］
  - （分析サービスの選択）：未選択

サンプル ルール：［Report malicious files（悪意のあるファイルをレポート）］

このルールは、Bit9 SRS によって検出された悪意あるファイル、および Bit9 Connector の一部として Bit9 に統合されている任意のアプライアンスまたはサービスによって検出された悪意あるファイルに対して、「レポートのみの禁止」をグローバルに適用します。

このルールのデフォルトのプロパティは次のとおりです。

- ［**Event Properties（イベント プロパティ）**］:［Subtype（サブタイプ）］が［Malicious File Detected（悪意のあるファイルの検出）］である
- ［**File Properties**（ファイル プロパティ）］: なし
- ［**Process Properties（プロセス プロパティ）**］: なし
- ［**Action（アクション）**］:［Change global file state（ファイルのグローバル状態を変更）］
  - ［**Change Global State（グローバル状態を変更）**］:［Ban (Report only)（禁止（レポートのみ））］
  - ［**Resolve Related Approval Request（関連する承認要求を解決）**］: 未選択
  - ［**Create For（作成の対象）**］:［All policies（すべてのポリシー）］

これはレポートしか行わないルールであるため、最初に［Simulate only（シミュレーションのみ）］モードでテストする必要はありません。

第 17 章

ブロック通知と承認要求

この章では、Bit9 ルールによってファイルへのアクセスや関連するアクションがブロックされたときに、エージェントが管理するコンピューターに表示される通知について説明します。さまざまなルールへの通知の割り当て方法、標準の通知の動作、通知への対応としてユーザーが利用可能なオプション、通知のカスタマイズ方法、Bit9 承認要求管理機能の有効化および使用方法についても説明します。

セクション

通知：動作

Bit9 エージェントは、画面に表示されることなくバックグラウンドで稼働し、ブロック ルールで指定されているアクションを検出およびブロックします。エージェントはアクションをブロックすると、このアクションが試行されたコンピューター上に「通知」を表示し、アクションがブロックされた理由をユーザーに知らせます。ブロックされたアクションと Bit9 Server で選択された設定に応じて、通知内でユーザーにブロックに対応するためのオプションを提供することもできます。

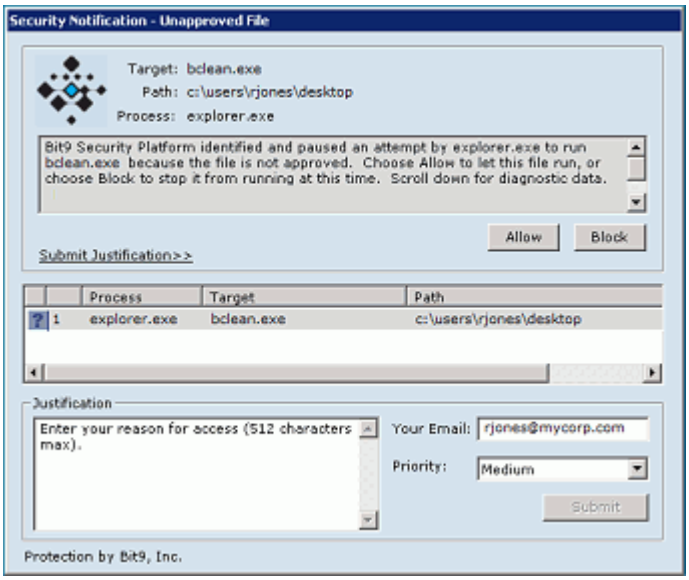
以下の説明はすべて、すべてのルールと設定に対して通知が有効化されていることを前提としています。

注意

バージョン 7.2.3 では、Windows 8 および Windows 8 Pro に対して通知をサポートしていますが、通知が利用できるのはこれらのシステムが従来のデスクトップ モードで実行されている場合のみです。Metro インターフェイスでは、通知はサポートされません。

プロンプト通知

「プロンプト」通知は、試行されたアクションとそのアクションが中断された理由をユーザーに知らせるだけでなく、そのアクションを許可またはブロックするオプションも提供します。

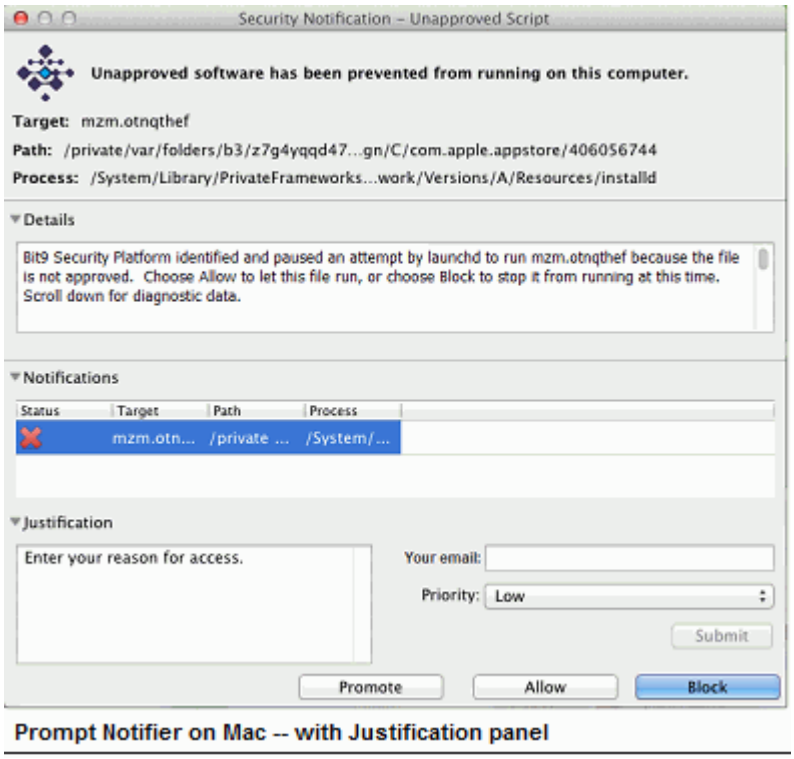


プロンプト通知は、次の状況でユーザーに表示されます。

- 中適用レベル（未承認に対してプロンプトを表示）のコンピューター上で、ユーザーが未承認ファイルの実行を試みたとき。
- ユーザーがカスタム（ファイルまたはパス）ルール、レジストリ ルール、またはメモリ ルールで管理されるアクションの実行を試み、そのルールがユーザーに決定を促すように設定されているとき。

プロンプト通知はユーザーからの応答を必要とするため、カスタム ルール、レジストリ ルール、メモリ ルールの定義によって無効化することはできません。また、ユーザーに入力を促すルールを定義するポリシー設定でも無効化しないでください。

承認要求機能の一部である［根拠 (Justification)］オプションが有効化されている場合、ユーザーは通知に対応して行った選択の「根拠」を送信できます。根拠は、アクションの許可またはブロックを選択する「前」に送信する必要があります。この機能の詳細については、「承認要求と根拠」(572 ページ) を参照してください。



Prompt Notifier on Mac -- with Justification panel

プロンプト通知に表示される選択肢は、ブロックが発生した状況によって異なります。

- ［**Block** (ブロック)］を選択すると、アクションはそのままブロックされ、ファイルやデバイスの状態は変更されず、通知が終了します。
- ［**Allow** (許可)］を選択すると、アクションが実行されます。コンピューターの適用レベルが中であるために未承認ファイルがブロックされた場合、このファイルはローカルで承認され、実行が許可されます。このファイルがインストーラーとして認識された場合、このファイルによって書き込まれたファイルはローカルで承認されます。インストーラーとして認識されない場合、このファイルによって書き込まれたファイルはローカルで承認されません。
- アクションがファイル実行ルールによってブロックされた場合は、Shift キーを押すと Mac および Linux 上では［**Promote** (昇格)］ボタンが有効になり、Windows では［**Allow** (許可)］に代わって［**Promote** (昇格)］が表示されます。［Promote (昇格)］を選択すると、そのファイルは昇格プロセスとして実行されます。つまり、このプロセスによって書き込まれたファイルはローカルで承認されます。この機能は、他のファイルをインストールするにもかか

わらず Bit9 にインストーラーとして認識されないファイルがあるとき、それを実行する試みによって通知が表示されたときに有益です。

- 10 分経過してもユーザーがプロンプト通知に対してアクションを取らない場合、ファイルはブロックされ、ブロック イベントが Bit9 Server に記録されて通知が終了します。ただし、ダイアログを操作（ダイアログのクリックや移動など）するとタイムアウトを防止できます。

ブロック専用通知

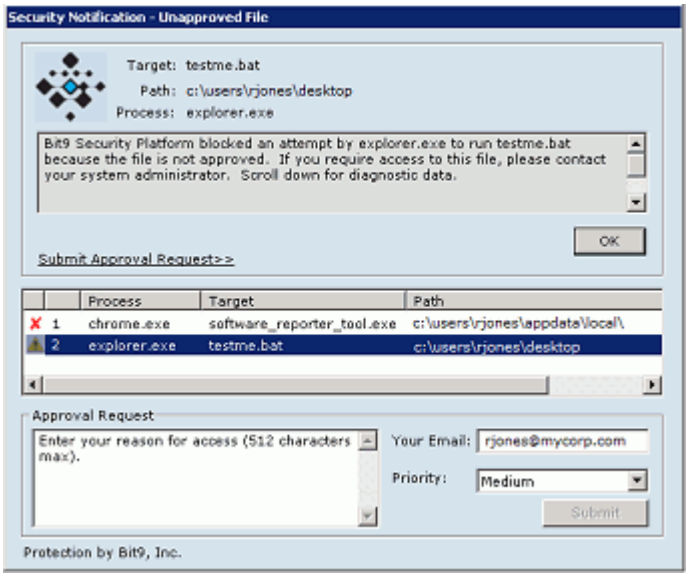
「ブロック専用」通知は、ユーザーが実行したアクションがブロックされたこととその理由をユーザーに知らせますが、アクションを許可するオプションはユーザーに提供されません。ブロック専用通知は、有効化されている場合、次の状況で表示されます。

- ユーザーが、禁止されているファイルの実行を制御モードのコンピューター上で試みたとき。
- ユーザーが、高適用レベル（未承認をブロック）のコンピューター上で未承認ファイルの実行を試みたとき。
- ユーザーが、カスタム ルール、レジストリ ルール、またはメモリ ルールで管理されるアクションの実行を試み、そのルールがそのアクションをブロックするように設定されているとき。
- ユーザーが、ファイル アクションをブロックするデバイス ルールで管理されるデバイスに対してそのファイル アクションを試みたとき。

ブロック専用通知の外観とオプションは、通知が表示されるプラットフォームによって異なります。

Windows コンピューター上のブロック通知

Windows コンピューターでは、ブロック通知はフルサイズ ダイアログとして表示されます。ブロックされたファイルやデバイスに対してアクションを実行できるオプションはありません。通知を終了するには、**[OK]** をクリックするか **Esc** キーを使用します。

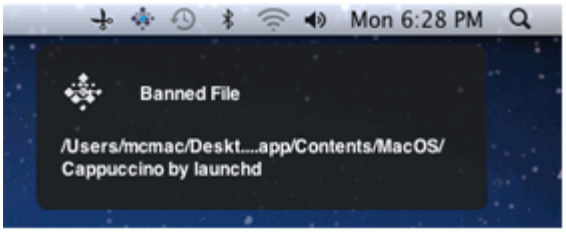


承認要求機能が有効化されている場合、ユーザーは現在アクセスできないファイルまたはデバイスに対する正式なアクセス要求を送信できます。承認要求は、v7.0.0 以降の新しい Bit9 インストールではデフォルトで有効化されています。この機能の詳細（以前のリリースからアップグレードしている場合に承認要求を有効化する方法を含む）については、「承認要求と根拠」（572 ページ）を参照してください。

ブロック専用通知は、それに対応するルールを無効化しなくても無効化できます。

Mac および Linux コンピューター上のブロック通知

Mac (OS X) および Linux コンピューター上のブロック通知は、ブロックされた操作やアクションに関する情報が表示される小さい半透明の通知パネルです。この通知はアクションを要求しないため、ユーザーがクリックしない限り、通知パネルは 5 秒で画面から消えます。この通知が表示されている間に新しいブロックが発生した場合、新しいブロックによってタイマーがリセットされ、さらに 5 秒間通知が表示されます。



画面から消える前にブロック通知をクリックすると、[Bit9 Notifier history（Bit9 通知履歴）] ウィンドウが開き、そのコンピューター上で発生した通知イベントの履歴が表示されます。この情報の詳細および [Bit9 Notifier history（Bit9 通知履歴）] ウィンドウで実行できるアクションについては、「Bit9 通知トレイと履歴ウィンドウ」（548 ページ）を参照してください。

通知コンポーネント

フルサイズの通知（すべての Windows 通知と、Mac および Linux 上のプロンプト通知）には、以下のコンポーネントを含めることができます。常に表示されるか、オプションか、カスタマイズ可能かはコンポーネントによって異なります。

- このウィンドウの上部には、タイトルが表示されます。（例：[Security Notification – Unapproved File（セキュリティ通知 – 未承認ファイル）]）
- アクションのターゲット（ユーザーが実行を試みたファイルなど）、そのパス、その実行を試みたプロセスに関する情報が表示されます。
- 通知の左上には、ブロックのソースの特定に役立つロゴが表示されます。デフォルトでは、Bit9 のロゴが表示されます。このロゴは非表示にもできます。
- Mac および Linux コンピューターでは、補足的なサブタイトル（例：「Unapproved software has been prevented from running on this computer.（このコンピューター上で未承認のソフトウェアの実行が阻止されました。）」が表示されます。）
- 通知の一番上のテキスト ボックスに表示される通知テキストには、ブロックされた要素とその理由の説明が表示されます。たとえば、「Bit9 blocked an attempt by explorer.exe to run calc.exe because the file is not approved. If you require access to this file, please contact your system administrator.」（Bit9 は explorer.exe に

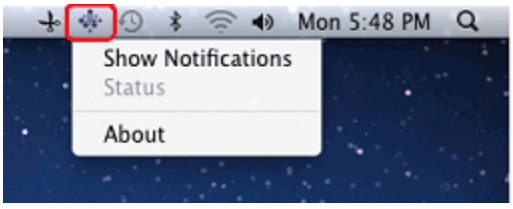
よる calc.exe の実行をブロックしました。このファイルは承認されていません。このファイルへのアクセスが必要な場合は、システム管理者に連絡してください。）と表示されます。Mac および Linux コンピューターでは、［Bit9 Notifier history（Bit9 通知履歴）］ウィンドウに各通知イベントに対する同様の詳細情報が表示されます。「Bit9 通知トレイと履歴ウィンドウ」（548 ページ）を参照してください。

- Windows コンピューターでは、オプションの通知リンクによって、セキュリティ ポリシーを説明するサイトをポイントする URL へのリンクや、ブロックされたオブジェクトへのアクセスを要求する機会を提供できます。このリンクは、アクセスを要求するメール メッセージが送信されるようにも設定できます。
- Windows コンピューターでは、通知の履歴パネル自体に、このコンピューター上でブロックされたファイルが表示されます。緑色のチェックマークは、ファイルの実行または書き込みが許可されたことを示します。赤の「x」は、Bit9 ルールかユーザーの選択によってファイルまたはアクションがブロックされたことを示します。黄色の三角は、ユーザーがアクションを実行する前に通知がタイムアウトしたこと（そのためアクションがブロックされたこと）を示します。疑問符は、現在のブロック イベント（現在の通知を表示させたイベント）を示します。Linux および Mac コンピューターでは、［Bit9 Notifier history（Bit9 通知履歴）］ウィンドウに同様の履歴情報が表示されます。「Bit9 通知トレイと履歴ウィンドウ」（548 ページ）を参照してください。
- ［Approval Request（承認要求）］パネルでは、ユーザーは現在アクセスできないファイルやデバイスの正式な承認要求を送信できます。［Justification（根拠）］パネルでは、通知で許可の選択肢が与えられている場合にアクションを許可する根拠を送信できます。この機能の詳細については、「承認要求と根拠」（572 ページ）を参照してください。

Bit9 通知トレイと履歴ウィンドウ

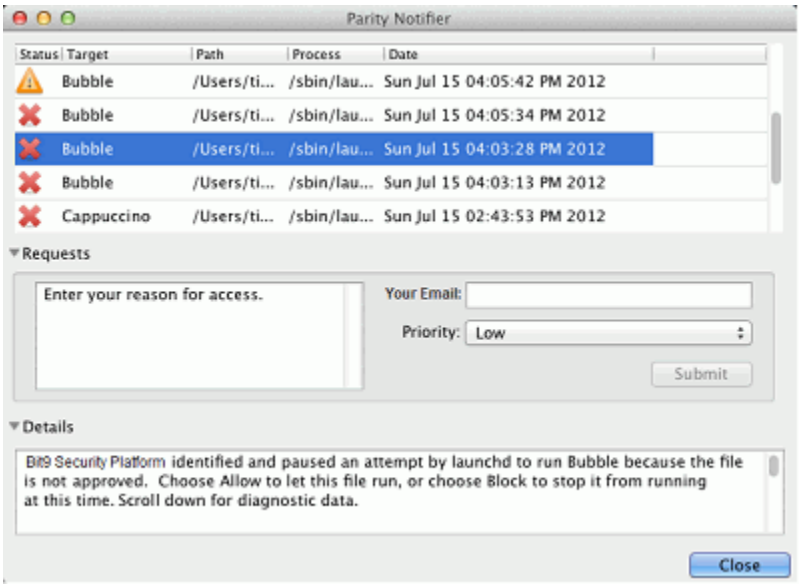
Linux および Mac コンピューターでは、Bit9 エージェントをインストールすると、以下のオプションを含むメニューへのアクセスに使用できるトレイやパネル アイコンが追加されます。

- ［**Show Notifications**（通知の表示）］– ［Bit9 Notifier history（Bit9 通知履歴）］ウィンドウが開き、過去のブロック イベントと、それに関する通知情報が表示されます。過去にブロックされたファイルの承認要求を送信するためのインターフェイスへのアクセスも提供します。
- ［**About**（バージョン情報）］– Bit9 エージェントのバージョンと著作権情報が表示されます。



［Bit9 Notifier History（Bit9 通知履歴）］ウィンドウ

Linux および Mac コンピューターでは、［Bit9 Notifier history（Bit9 通知履歴）］ウィンドウに過去のブロック イベントが表示されます。ブロック イベントを選択すると、その詳細情報を表示し、ブロックされたファイルやアクションの承認要求を送信できます。



Windows コンピューターでは、各通知自体に Mac または Linux 通知の履歴リストと同様に機能する履歴パネルが含まれています。大きな違いは、Windows では通知が表示された場合にのみ履歴を確認できる点です。それ自体としてアクセスできる［Bit9 Notifier history（Bit9 通知履歴）］ウィンドウはありません。

ブロック イベントのリストには、以下の情報が表示されます。

- ［**Status**（ステータス）］– アイコンで表示されます。赤の X はブロックされたファイルまたはアクション、緑のチェックマークは通知上でのユーザーの選択によって許可されたファイルまたはアクション、黄色の三角はユーザーがアクションを実行する前に通知がタイムアウトしたこと（そのためにアクションがブロックされたこと）を示します。
- ［**Path**（パス）］– ブロックされたファイルの完全なパス。
- ［**Process**（プロセス）］– アクションを試みたプロセスの完全なパス。
- ［**Date**（日付）］– ファイルまたはアクションがブロックされた日時。

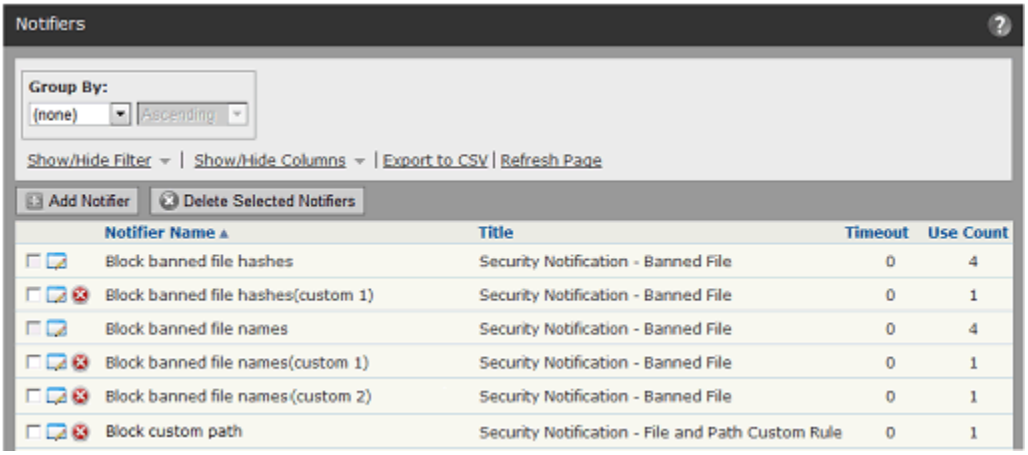
履歴リストの下に表示される［Request（要求）］パネルでは、リストで選択したブロック ファイルの承認を要求できます。このパネルは、パネル名の隣の矢印をクリックすると表示と非表示を切り替えられます。

［Requests（要求）］パネルの下の［Details（詳細）］パネルには、ブロックされたファイルやアクションのさらに詳しい説明が表示されます。このパネルは、パネル名の隣の矢印をクリックすると表示と非表示を切り替えられます。

Bit9 コンソールの［Notifiers（通知）］ページ

Bit9 エージェントに使用可能な通知は、Bit9 コンソールの［Notifiers（通知）］ページのテーブルに表示されます。このページには、現在の Bit9 リリースで提供されているデフォルトの通知と、管理者が追加したすべての通知が表示されます。また、以前の Bit9 (Parity) バージョンからアップグレードし、通知を変更してある場合、通知のテーブルには 7.2.3 のデフォルトの通知と変更された通知の両方が表示されます。6.0.2 通知の最初の変更版は名前に「(custom 1)」が付加され、2 番目の変更版には「(custom 2)」が付加されます。

このページではすべての通知を編集できますが、デフォルト通知の削除はできません。



設定とルールへの通知の割り当て

Bit9 コンソールでは、以下の 2 つの場所で通知を割り当てられます。

- ［Edit Policy（ポリシーの編集）］ページ（各ポリシー設定に対する割り当て）
- ［Add/Edit Rule（ルールの追加 / 編集）］ページ（カスタム ルール、レジストリ ルール、メモリ ルールへの割り当て）。ルールは、コンピューターのポリシーによって割り当てられた通知、またはルールの詳細で指定されたカスタム通知を使用するように設定できます。

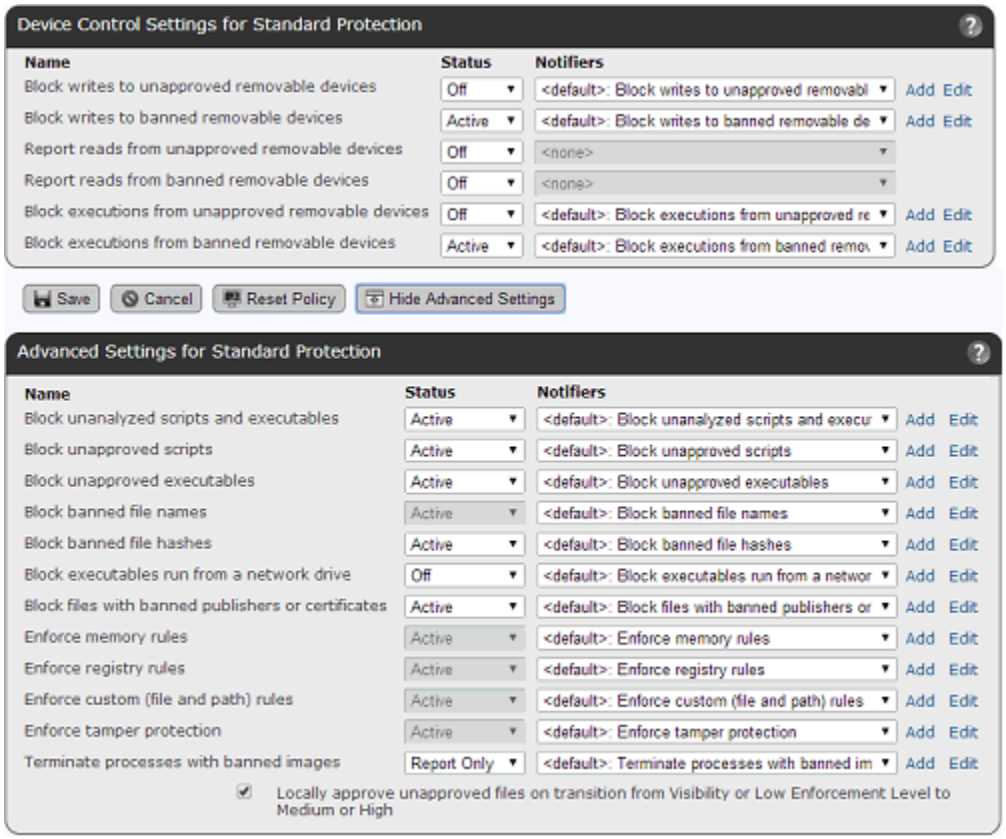
ポリシー設定への通知の割り当て

各ポリシー設定には、デフォルトで設定固有の通知が割り当てられているため、通知の構成は不要です。ただし、メニューを使用してルールや設定ごとに異なる通知を選択することができます。このセクションでは、設定に既存の通知を割り当てる方法を説明します。通知の変更や新規作成の方法の詳細については、「通知のカスタマイズと作成」（553 ページ）を参照してください。

ポリシー設定への通知の割り当て手順：

1. コンソール メニューで、［**Rules**（ルール）］>［**Policies**（ポリシー）］の順に選択します。［Policies（ポリシー）］ページが表示されます。

2. ［Policies（ポリシー）］ページで、通知割り当てを変更するポリシー名の隣の［View Details（詳細の表示）］ボタンをクリックします。［Edit Policy（ポリシーの編集）］ページが表示されます。
3. ［Advanced Setting（高度な設定）］の通知を変更する場合は、［**Show Advanced Settings**（高度な設定の表示）］をクリックします。



4. 通知を変更する設定に対して、［Notifiers（通知）］メニューから新しい通知を選択します。
［<none>（なし）］を選択すると、設定によってアクションがブロックされたときに通知を非表示にできます。ただし、通知を［<none>（なし）］に変更する前に、この設定が適用されるあらゆる状況を考慮してください。たとえば、［Block unapproved executables（未承認の実行可能ファイルをブロック）］に対して［<none>（なし）］を選択すると、未承認ファイルの実行のブロックまたは許可を選択する必要がある中適用レベルのポリシーのユーザーは、その決定を下す機会を得られません。このファイルは、エージェントからの通知なしでブロックされます。
5. ［**Save**（保存）］ボタンをクリックして変更を保存します。［Policies（ポリシー）］ページが表示されます。
6. このポリシーで変更する設定に対して、手順 3 ～ 5 を繰り返します。
7. 通知を変更する各ポリシーに対してこの手順を繰り返します。

ポリシー設定と通知

［Edit Policy（ポリシーの編集）］ページの［Device Settings（デバイス設定）］および［Advanced Settings（高度な設定）］リストに表示される以下の各ポリシー設定には、通知が個別に割り当てられています。

デバイス設定と通知：

- Block writes to unapproved removable devices（未承認リムーバブル デバイスへの書き込みをブロック）
- Block writes to banned removable devices（禁止リムーバブル デバイスへの書き込みをブロック）
- Block executions from unapproved removable devices（未承認リムーバブル デバイスからの実行をブロック）
- Block executions from banned removable devices（禁止リムーバブル デバイスからの実行をブロック）
- Report reads from unapproved devices（未承認デバイスからの読み取りを報告）（通知は表示されません）
- Report reads from banned devices（禁止デバイスからの読み取りを報告）（通知は表示されません）

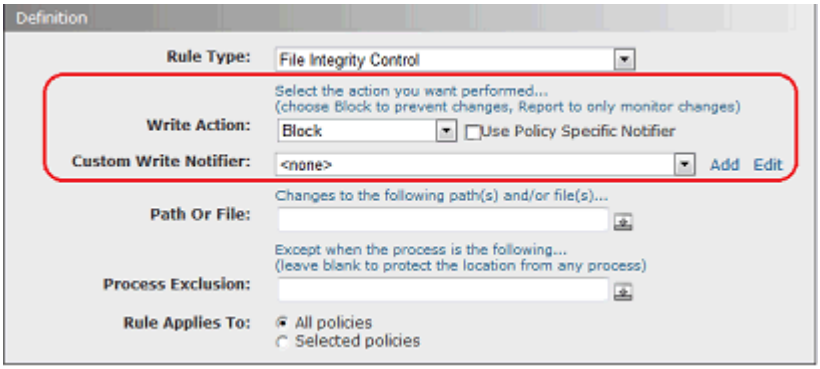
高度な設定と通知：

- Block unanalyzed scripts and executables（未分析のスクリプトおよび実行可能ファイルをブロック）
- Block unapproved scripts（未承認スクリプトをブロック）
- Block unapproved executables（未承認実行可能ファイルをブロック）
- Block banned file names（禁止ファイル名をブロック）
- Block banned file hashes（禁止ファイル ハッシュをブロック）
- Block executables run from a network drive（ネットワーク ドライブからの実行可能ファイルの実行をブロック）
- Enforce memory rules（メモリ ルールを適用）
- Enforce registry rules（レジストリ ルールを適用）
- Enforce custom (file and path) rules（カスタム（ファイルおよびパス）ルールを適用）
- Enforce tamper protection（改ざんからの保護を適用）
- Terminate processes with banned images（禁止イメージを含むプロセスを終了）

カスタム ルール、レジストリ ルール、およびメモリ ルールへの通知の割り当て

通知は、カスタム ルール、レジストリ ルール、またはメモリ ルールがアクションをブロックしたときや、これらのルールがユーザーにアクションの許可またはブロックの決定を促すときに表示できます。各ルールには、2 つの通知ソースのいずれか 1 つを選択できます。

- ［**Use Policy Specific Notifier**（ポリシー固有の通知を使用）］– 各ポリシーには、ルールのタイプごとの［Advanced Setting（高度な設定）］が含まれています。各ポリシー設定の［Notifier（通知）］フィールドでは、そのタイプのルールがアクションをブロックしたときにエージェント コンピューターに表示される通知を指定できます。［<none>（なし）］を選択すると、ルールは通知を表示することなくアクションをブロックできます。デフォルトでは、アクションをブロックするルールと、ユーザーに決定を促すルールは、ポリシー固有の通知を使用します。
- ［**Custom Notifier**（カスタム通知）］– ポリシー固有の通知を使用しない場合は、使用可能な任意の通知をルールに割り当てられます。通知の選択肢は、ルールの［Add/Edit（追加 / 編集）］ページのメニューに表示されます。また、新しい通知を追加することも、既存の通知を編集することもできます。詳細については、「通知のカスタマイズと作成」（553 ページ）を参照してください。



ルール アクションとして［Prompt（プロンプト）］を選択した場合、プロンプト ルールは通知を表示する必要があるため、［Custom Notifier（カスタム通知）］メニューのオプションに［<none>（なし）］は表示されません。

ルール アクションとして［Block（ブロック）］を選択した場合、ルールは通知を行わずにアクションをブロックできるため、［Notifier（通知）］メニューで［<none>（なし）］を選択できます。

ルールに［Use Policy Specific Notifier（ポリシー固有の通知を使用）］を選択すると、そのルール タイプに対する通知の 1 つとして［<none>（なし）］を指定できます。これを指定すると、プロンプト ルールに対しても通知は表示されなくなります。ルールに対する応答をユーザーに求めなくても問題がないことが確実な場合を除き、ポリシーのルール通知として［<none>（なし）］を選択することは推奨しません。

通知のカスタマイズと作成

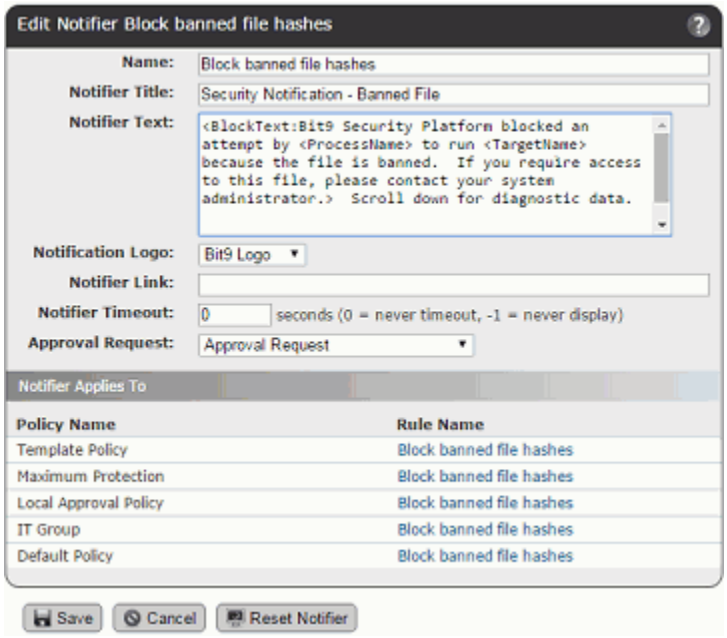
通知は既存のものを編集することも、新規作成することもできます。デフォルトの通知を編集する場合は、変更した通知を後で元の状態にリセットできます。

通知テキスト、通知リンク、通知名、カスタム ロゴのパスを組み合わせた長さは、1,900 文字以内にする必要があります。この制限を超えると警告が表示されます。

既存の通知のカスタマイズ手順：

1. ［Edit Notifier（通知の編集）］ページは、3 つの方法で開くことができます。

- コンソール メニューで、[**Rules**（ルール）] > [**Notifiers**（通知）] の順に選択します。通知のテーブルで、編集する通知名の隣にある [View Details（詳細の表示）]（ファイルと鉛筆）ボタンをクリックします。
- [Edit Policy（ポリシーの編集）] ページの [Device Settings（デバイス設定）] または [Advanced Settings（高度な設定）] パネルで、編集する通知名の右端列の [**Edit**（編集）] をクリックします。
- カスタム ルール、レジストリ ルール、またはメモリ ルールの [Edit（編集）] ページで、[Custom Notifier（カスタム通知）] メニューが表示されている場合に、通知名の隣の [**Edit**（編集）] をクリックします。



2. 変更する通知設定を確認し、変更を加えます（表 64 を参照）。
3. [**Save**（保存）] ボタンをクリックして変更を保存します。

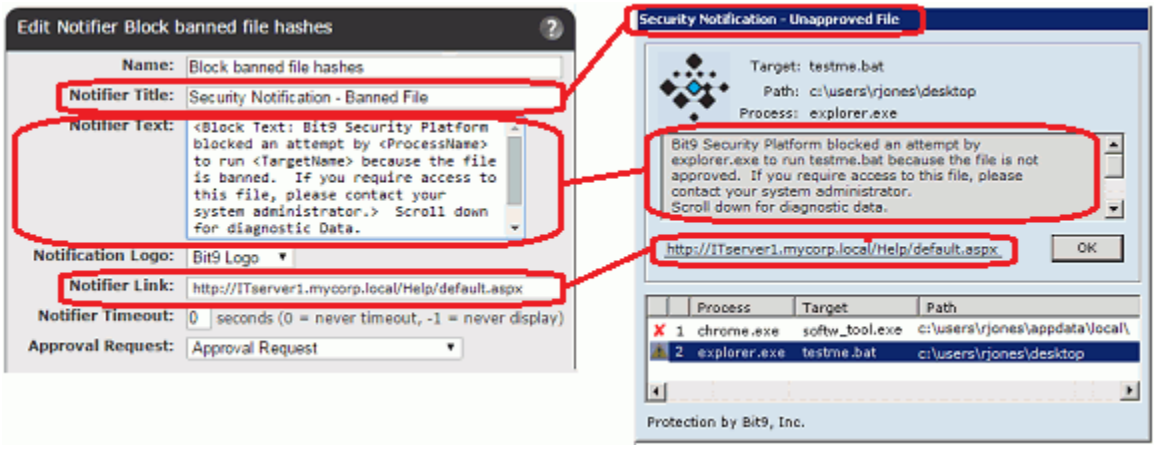
表 64：通知設定の追加 / 編集

フィールド	説明
[Copy Settings From（設定のコピー元）]	（[Add Notifier（通知の追加）] ページのみ）新しい通知の初期設定をコピーする元になる既存の通知。この情報を使用して新しい通知のすべてのフィールドにデータを入力し、変更が必要な箇所だけを変更できます。すべての通知フィールドに一から情報を入力する場合は、[(none（なし))] を選択します。
[Name（名前）]	[Policy（ポリシー）] および [Rule（ルール）] ページの通知のテーブルに表示される通知名。この名前は、コンピューター ユーザーに表示される通知には表示されません。
[Notifier Title（通知のタイトル）]	エージェントがこの設定に基づいてファイル実行をブロックしたときに、コンピューター ユーザーに表示される通知メッセージのウィンドウのタイトル。

フィールド	説明
[Notifier Text（通知テキスト）]	エージェントがこの設定に基づいてファイル実行をブロックしたときに、Windows コンピューターの通知に表示される説明メッセージ。管理者は、このメッセージの変更、ブロックのみを行う状況とブロックおよびプロンプトを行う状況に対する異なるメッセージのタグ付け、イベント固有の情報を提供するタグの追加、その他の条件テキストの追加を行えます。ここで使用するタグによって、承認要求機能を変更することもできます。 タグの説明については、「通知テキストの編集」（557 ページ）を参照してください。承認要求のアクティブ化と設定の詳細については、「承認要求と根拠」（572 ページ）を参照してください。 **プラットフォームに関する注意**：通知テキストは Windows 通知でのみ表示されます。
[Notifier Logo（通知ロゴ）]	デフォルトでは、Bit9 設定によってファイルがブロックされたとき、[Notifier（通知）] ダイアログ ボックスには Bit9 ロゴが表示されます。[Notifier Logo（通知ロゴ）] メニューには、次のオプションがあります。 • [**Bit9 logo**（Bit9 ロゴ）] を選択したままにする。 • [**Custom**（カスタム）] を選択し、別のイメージの URL またはファイル パスを指定する。イメージの形式とファイル パスの要件の詳細については、「カスタム通知ロゴの指定」（565 ページ）を参照してください。 • [**None**（なし）] を選択し、通知にロゴやイメージを表示しない。
[Notifier Link（通知リンク）]	以下のいずれかを指定します。 • コンピューター ユーザーが、ブロック ファイルに対応するためのセキュリティ設定や手順に関する情報を取得できる Web ページへのリンク • ユーザーが E メールで質問を送信するための mailto: リンク ここに指定する URL または mailto リンクは、通知にそのまま表示することも、「FriendlyText」の記述を表示することもできます。 URL も mailto リンクも表示しない場合は、このフィールドは空白のままにします。 **プラットフォームに関する注意**：このリリースでは、通知リンクは Windows 通知でのみ表示されます。
[Notifier Timeout（通知タイムアウト）]	Windows コンピューターの画面にブロック専用通知が表示される秒数。指定された時間が経過すると、通知は自動的に終了します。 デフォルト タイムアウト値のゼロ (0) では、ユーザーが通知に対応するまで画面に通知が表示されます。この値を マイナス 1 (-1) にすると、通知は表示されません。ブロック アクション通知の有効化と無効化の詳細については、「Bit9 通知の無効化」（568 ページ）を参照してください。 **プラットフォームに関する注意**：この値は、Windows コンピューターにのみ影響します。Mac および Linux では、ブロック専用通知のタイムアウトはデフォルトで 5 秒です。

フィールド	説明
[Approval Request（承認要求）]	この通知に対して承認要求機能を有効化するかどうかと、その方法を指定します。以下の選択肢があります。 • [**None**（なし）] – [Approval Request（承認要求）] パネルを表示しません。 • [**Approval Request**（承認要求）] – ルールによってファイルへのアクセスが完全にブロックされたときに [Approval Request（承認要求）] パネルを表示します。 • [**Justification**（根拠）] – ルールによってユーザーがアクションの許可またはブロックを促されたときに [Justification（根拠）] パネルを表示します。 • [**Approval Request and Justification**（承認要求と根拠）] – ブロックされたときとユーザーに決定を促すときの両方で [Approval Request/Justification（承認要求 / 根拠）] パネルを表示します。 詳細については、「承認要求と根拠」（572 ページ）を参照してください。
[Notifier Applies to（通知の適用先）]	（この通知が 1 つ以上の設定またはルールに割り当てられている場合にのみ表示されます）このパネルには、この通知が割り当てられているすべてのルールと設定が一覧表示されます。これらすべての割り当てを削除するには、[Advanced（高度）] メニューで [**Remove Association**（関連付けの削除）] をクリックします。この操作を行うと、関連するポリシー設定はデフォルト通知に戻り、関連するルールはそのルール タイプのポリシー固有通知に戻ります。

次の図に、[Add/Edit Notifier（通知の追加 / 編集）] ダイアログでの変更が反映された通知の内容を示します。



新しい通知の作成

新しい通知の作成方法は、既存の通知の編集方法に似ていますが、最初の手順が異なります。

新しい通知の追加（作成）手順：

1. ［Add Notifier（通知の追加）］ページは 3 つの方法で開くことができます。
   a. コンソール メニューで、［**Rules**（ルール）］>［**Notifiers**（通知）］の順に選択し、通知のテーブルで［**Add Notifier**（通知の追加）］ボタンをクリックします。
   b. ［Edit Policy（ポリシーの編集）］ページの［Device Settings（デバイス設定）］または［Advanced Settings（高度な設定）］パネルで、編集する通知名の右端列の［**Add**（追加）］をクリックします。
   c. カスタム ルール、レジストリ ルール、またはメモリ ルールの［Edit（編集）］ページで、［Custom Notifier（カスタム 通知）］メニューが表示されている場合に、通知名の隣の［**Add**（追加）］をクリックします。
2. 既存の通知の設定を開始点にする場合は、［Copy Settings From（設定のコピー元）］メニューから通知を選択します。
3. 必要に応じて設定を編集または入力します（表 64 を参照）。
4. ［**Save**（保存）］ボタンをクリックして変更を保存します。

   注意：［Add Notifier（通知の追加）］ページで［Save（保存）］をクリックすると、通知が保存されて［Notifier（通知）］リストに追加されます。ポリシーから［Add Notifier（通知の追加）］ページに移動した場合は、新しい通知は［Edit Policy（ポリシーの編集）］ページで［Save（保存）］をクリックしなくても保存されます。

通知テキストの編集

Bit9 ルールによってアクションがブロックされたときにユーザーに表示される通知テキストは、カスタマイズできます。たとえば、［Promote（昇格）］オプションを目立たせないようにする場合でなければ、既存のポリシーの通知にその説明を追加することが考えられます。Bit9 通知では、エンド ユーザーに提供する情報のカスタマイズに使用できる条件タグ、メタタグ、およびレポート タグがサポートされています。

プラットフォームに関する注意：通知テキストは、すべてのプラットフォームのプロンプト通知、Windows のブロック専用通知、および［Bit9 Notifier history（Bit9 通知履歴）］ダイアログに表示されます（履歴ダイアログの場合は、履歴で選択された項目に対する通知テキスト）。通知メッセージは Windows イベント ログにも記録されます。

通知テキストでのタグの使用

通知テキストおよびリンクには、通知を発生させたイベントに固有の情報（イベントが発生したコンピューター名、適用されていたポリシーなど）を提供するタグを含めることができます。表 65 に、通知メッセージに追加できる情報タグを示します。ただし、Bit9 サポート専用のその他のタグが使用されることもあります。

注意

通知テキスト ボックスのタグは、ユーザーに状況情報を提供するだけでなく、Bit9 承認要求機能のカスタマイズにも使用できます。これらのタグと使用方法の詳細については、「承認要求と根拠」(572 ページ) を参照してください。

表 65：通知の情報タグ

タグ	説明	値の例
<ComputerName>	ブロック イベントが発生したコンピューターのローカル名。	「RJONES-LAPTOP」
<DebugInfo>	イベントを生成したルールとポリシーに関する技術情報。これはメタタグ（他のタグによって表される情報を含むタグ）です。	
<DomainName>	ブロック イベントが発生したコンピューターの NetBIOS ドメイン名。	「MYCORP」
<EnforcementLevel>	ブロックが発生した時点でのエージェントの適用レベル。	「High (Block Unapproved)（高（未承認をブロック））」、「Medium (Prompt Unapproved)（中（未承認に対してプロンプトを表示））」、「Low (Monitor Unapproved)（低（未承認を監視））」
<Operation>	ブロックされた操作のタイプ。	「Execute（実行）」、「Write（書き込み）」、「Read（読み取り）」など。
<OsVersion>	エージェント コンピューターの Windows のバージョン、ビルド、リリース。	「Microsoft Windows 7 x64 (build 7600)」
<Bit9AgentVersion>	操作がブロックされたシステム上で稼働しているエージェントのバージョン。	「7.2.1.256 (Patch 3)」
<Policy>	エージェント コンピューターに適用されているポリシー。	「Research Team」、「Sales Group」、「Guests」など。
<ProcessName>	ブロックされたプロセス名（パスなし）。	「explorer.exe」

タグ	説明	値の例
<ProcessPath>	ブロックされたプロセスのパス（名前を含まない）。	「c:\windows\system32\」
<ProcessPathName>	ブロックされたプロセスの完全なパス（名前を含む）。	「c:\windows\system32\explorer.exe」
<ProcessPublisher>	ソース プロセスの公開者名（署名がある場合）。	「Bit9, Inc」、「Google Inc.」、「Microsoft Corporation」など。
<ProcessSha256>	ソース プロセスの SHA256 ハッシュ（16 進数）	
<RuleType>	トリガーされたルールのタイプ。	「File and Path（ファイルおよびパス）」、「Registry（レジストリ）」、「Memory（メモリ）」、「Process（プロセス）」など。
<TargetName>	アクセスが試みられたターゲット ファイル、レジストリ キー、またはプロセスの名前（パスなし）。	「foo.bat」
<TargetPath>	ターゲットになったファイル、キー、またはプロセスのパス（名前なし）。	「c:\test\」
<TargetPathName>	ターゲットの完全なパスと名前。	「c:\test\foo.bat」
<TargetPublisher>	ターゲット ファイルの公開者名（署名がある場合）。	「Bit9, Inc」、「Google Inc.」、「Microsoft Corporation」など。
<TargetDevice>	アクションがブロックされたデバイスのドライブ文字。マップされていないデバイスは \\device\<name> と表示されます。	
<TargetShare>	ファイルへのアクセスがブロックされたリモート ドライブのネットワーク パス（ファイル名なし）。	「\\SERVER3\temp\mydir」
<TargetSha256>	ターゲット ファイルの SHA256 ハッシュ（16 進数）。	
<TargetSha1>	ターゲット ファイルの SHA1 ハッシュ（16 進数）。	
<TargetMD5>	ターゲット ファイルの MD5 ハッシュ（16 進数）。	
<UserName>	ブロック操作が開始されたコンテキストのユーザー名。	「\MYCORP\rjones」

ブロック用とプロンプト用の条件メッセージ

1 つの通知テキスト内で条件タグを使用すると、アクションが Bit9 ルールによってブロックされたときのブロック専用通知と、ユーザーにアクションをブロックまたは許可を促すプロンプト通知に、異なるメッセージを表示できます。たとえば、1 つの通知テキスト ブロックを作成し、高適用レベルのポリシーのユーザーが未承認ファイルの実行を試みた場合には「block」メッセージを表示し、中適用レベルのポリシーのユーザーが同じファイルの実行を試みた場合には「ask」メッセージを表示できます。アクションをブロックまたは許可するオプションをユーザーに提供するカスタム ルール、レジストリ ルール、メモリ ルールでも、同様のプロンプト メッセージを使用できます。表 66 に、さまざまなブロック条件用のタグを示します（「message」は、メッセージ内で使用されるさまざまなテキストを表します)。

表 66：通知の条件タグ

	説明
<BlockText:*message*>	ルールによってアクションがブロックされ、ユーザーにアクションを許可する選択肢がない場合に表示されるテキスト。
<AskText:*message*>	ユーザーにアクションをブロックするか続行するかの決定を促す場合に表示されるテキスト。大半の「プロンプト」ケースで使用されるテキストです。
<AskAllowText:*message*>	ユーザーに「ファイルの実行をブロックするか許可するか」の決定を促す場合に表示されるテキスト。
<AskRestrictText:*message*>	ユーザーに「メモリ アクセスを許可するか制限するか」の決定を促す場合に表示されるテキスト。
<AskApproveText:*message*>	ユーザーに「ファイルの書き込みをブロックするか、ファイルを承認して書き込みを許可するか」の決定を促す場合に表示されるテキスト。

たとえば、未承認のファイルがブロックされたときに、通知テキストに以下の内容を含めることができます。

```
このコンピューター上で未承認ファイルの実行が試行されました
<BlockText:。この試みはブロックされました。このファイルへのアクセスが
必要な場合は、システム管理者に連絡してください。><AskText:。このファイ
ルの実行を許可する場合は［Allow（許可)］を選択してください。今回の実行
を阻止する場合は［Block（ブロック)］を選択してください。>
```

エージェント コンピューターに、この通知テキストが設定されている高適用レベルのポリシーが割り当てられている場合、未承認ファイルの実行が試行されると、通知メッセージでは「BlockText:」が使用されます。

```
このコンピューター上で未承認ファイルの実行が試行されました。この試みはブロックされました。このファイルへのアクセスが必要な場合は、システム管理者に連絡してください。
```

一方、これと同じ通知テキストが設定されている中適用レベルのポリシーが割り当てられているエージェント コンピューターで、未承認ファイルを開こうとすると、通知メッセージでは「AskText:」が使用されます。

```
このコンピューター上で未承認ファイルの実行が試行されました。このファイルの実行を許可する場合は［Allow（許可)］を選択してください。今回の実行を阻止する場合は［Block（ブロック)］を選択してください。
```

表 66 に示した block/ask 条件タグの内側には、他のタグをネストできます。例として、以下に「ブロックされた未承認」ファイルに対するデフォルトの通知メッセージを示します。

```
<BlockText:Bit9 は <ProcessName> による <TargetName> の実行の試行をブロックしました。このファイルは未承認です。このファイルへのアクセスが必要な場合は、システム管理者に連絡してください。><AskText:Bit9 は、<ProcessName> による <TargetName> の実行の試行を特定し、停止しました。このファイルは未承認です。このファイルの実行を許可する場合は［Allow（許可)］を選択してください。今回の実行を阻止する場合は［Block（ブロック)］を選択してください。>
```

BlockText および AskText 両方の条件タグの内側に、他のタグがネストされているのがわかります。block/ask 条件タグは、内側に他のタグをネストできる唯一の通知「テキスト」タグです。通知「リンク」では、「FriendlyText」タグの内側にタグをネストできます。

注意

以前のリリースから Bit9 Server にアップグレードした場合、既存の通知メッセージ（デフォルト ポリシーおよびテンプレート ポリシーの通知メッセージを含む）は保持されます。Bit9 (Parity) の 6.0.2 よりも前のバージョンから使用を開始している場合は、「block」条件と「ask」条件に異なるメッセージを提供する条件テキストや、その他の特殊タグは通知に含まれていない可能性があります。

条件演算子としての情報タグ

通知メッセージには、特別な「block-and-ask」条件演算子に加え、表 65 に示されているすべての情報タグ（< DebugInfo> などのメタタグを除く）に基づいて他の条件テキストも含めることができます。条件テキスト タグは、以下のように作成します。

```
<tagnameText:pattern-to-match:message-text>
```

タグ名の直後に単語「Text」を追加する必要があります。追加しないと、このタグは機能しません。

たとえば、アクションが試行されたコンピューター上で Bit9 エージェント 7.0.0 が稼働している場合にのみ表示される通知テキストを設定するには、以下の例のように **<Bit9AgentVersion>** タグを使用します。

```
<Bit9AgentVersionText:7.0.0.*: これは 7.0.0 エージェントにのみ表示されます。>
```

「7.0.0.*」でワイルドカード文字のアスタリスクが使用されているため、Bit9 Agent 7.0.0 の任意のビルド番号がこの条件に一致します。アスタリスクは 0 文字以上の任意の文字に一致します。疑問符は任意の 1 文字に一致します（0 文字には一致しません）。

もう 1 つ例をあげると、ターゲット ファイルのハッシュが特定の SHA-256 ハッシュと一致する場合に表示される通知テキストは、**<TargetSha256>** タグを使用して設定できます。この条件テキストは、以下に示すように汎用の「ファイル ブロック」通知内にネストできます。

```
Bit9 は、<ProcessName> による <TargetName> の実行の試みをブロックしました。このファイルは禁止されています。
<TargetSha256Text:c1c4eacd1fe39c93df477f335644902b3b83cc437bfe4b641960f874af1e0708: この MyFavoriteApp のバージョンには、重大なセキュリティの欠陥があります。>
このブロックを解決する必要がある場合は、システム管理者に連絡してください。下にスクロールすると診断データが表示されます。

<DebugInfo>
```

通知リンクの編集

通知リンクとは、アクションがブロックされたときにユーザーが社内のサポート デスクに連絡したり、アクションがブロックされた詳しい理由を説明する Web ページを開いたりするためにクリックできるリンクです。通知リンクは、Bit9 がファイル アクションをブロックするすべての状況で同一ものを使用できますが、通知ごとに異なるリンクを設定するオプションがあります。また通知テキストと同様に、リンク内でタグを使用してイベントに関する詳細情報を提供することもできます。

通知リンクは、ファイルやデバイスへのアクセス要求を管理する手段の 1 つで、アクセス要求の収集および対応用のITポリシーを設定している場合に有効に活用できます。Bit9 には独自の承認要求機能も装備されており、この機能を利用すると、ユーザーが Bit9 コンソール上で直接承認要求を作成、送信、管理するために必要なフィールドを通知に含めることができます。詳細については、「承認要求と根拠」（572 ページ）を参照してください。

プラットフォームに関する注意: 通知リンクはWindows通知でのみ表示されます。

通知リンクのタグ

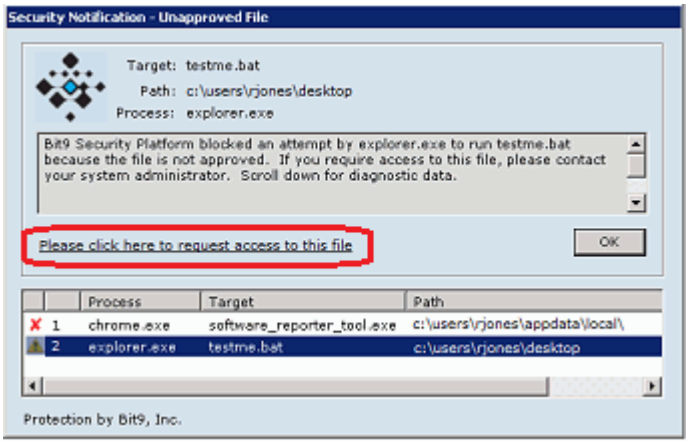
［Add/Edit Notifier（通知の追加 / 編集）］ページの［**Notifier link**（通知リンク）］フィールドでは、2 つの目的で通知タグを利用できます。

- タグを使用して通知メール メッセージやサイト URL をカスタマイズできます。自動ワークフロー要求を作成するときや、通知の原因になったファイルに関する情報を自動的に表示する Web サイト リンクを作成するときに便利です。タグの完全なリストは、表 65、「通知の情報タグ」（558 ページ）を参照してください。
- URL 自体の代わりに通知ダイアログに表示する「FriendlyText」を作成できます。FriendlyText タグは、通知リンク テキスト内の任意の場所に配置できます。

以下に、上記の両方の目的でタグが使用されている通知リンクの例を示します。

```
mailto:it@mycorp.com?subject=<TargetName> の承認要求
&body=<UserName>(<DomainName>\<ComputerName>) により
<TargetName> へのアクセスが要求されました。%0A ファイルの詳細の入手
先：https://bit9server1/file-details.php?hash=<TargetSha256>
<FriendlyText: このファイルへのアクセスを要求するには、ここをクリック
してください。>
```

上記の通知テキストが「Block unapproved executables」（未承認実行可能ファイルのブロック）通知で使用される場合、高適用レベルのポリシーが割り当てられているエージェント コンピューターで未承認ファイルの実行が試行されると、以下のような通知が表示されます。



この通知リンクには、通知リンク URL（「mailto:mycorp.com…」）の代わりに、ユーザーにこのリンクをクリックする理由を示す「FriendlyText」（「このファイルへのアクセスを要求するには、ここをクリックしてください。」）が表示されます。

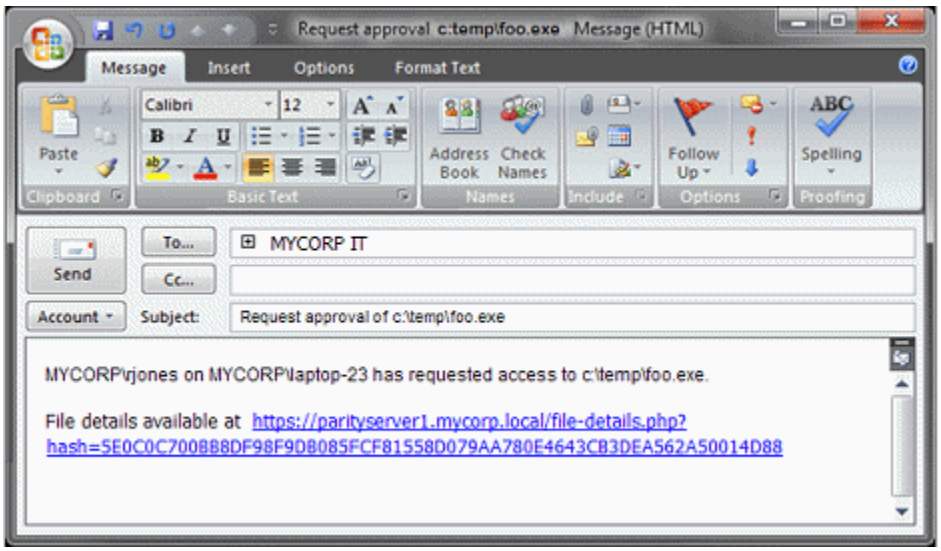
FriendlyText タグの内側には、他のタグをネストできます。たとえば、上記のような汎用リンク テキストの代わりに、次のようなリンクを作成できます。

```
<FriendlyText:<TargetName> へのアクセスを要求するには、ここをクリックしてください。>
```

その結果、ブロックされたファイルの名前がリンク テキスト内に挿入されます。

URL と Friendly Text のどちらを表示する場合も、生成されるリンク テキストは 1 ～ 2 行で表示されます。このテキストはアクション ボタン（[OK]、[Allow（許可）]、[Block（ブロック）]）に干渉しません。リンク テキストが長すぎる場合は、ダイアログ ボックスに収まるように切り詰められます。

この例では、ユーザーがリンクをクリックすると、ユーザーのデフォルト メール クライアントで以下のようなメール メッセージが作成されます。



上記で定義された通知リンクでは、以下のようなカスタマイズのためにタグが使用されています。

- 未承認ファイルへのアクセスを組織の IT グループに要求する E メール メッセージを生成する。
- メッセージ ヘッダーにファイル名を指定する。
- メッセージ本文で、ユーザー、コンピューター、ファイルを特定する。
- 要求されたファイルに関するBit9コンソールの[File Details（ファイルの詳細）]ページを直接ポイントする URL を、メール メッセージ内で提供する。

ユーザーが自分でファイルに関する決定を下す「block-and-ask」の状況に対しては、（メール メッセージを生成せずに）ファイルの詳細に関する URL を直接開く、以下のようなシンプルな通知リンクを作成できます。

```
https://bit9server1/file-details.php?hash=<TargetSha256>
<FriendlyText: このファイルの情報を入手するには、ここをクリックしてください。>
```

通知ソース行の編集

通知の最下部には、通知のソースを識別する行が表示されます。デフォルトでは「Protection by Bit9, Inc.」が表示されます。この行を変更するには、[Notifier Text（通知テキスト）] フィールドに以下のタグを挿入し、*text* の代わりにソースを識別する独自のテキストを入力します。

```
<NotifierComment:text>
```

通知からこの行を削除するには、*text* として 1 つのスペース文字を使用します。

プラットフォームに関する注意 : 通知ソース行は Windows 通知でのみ表示されます。

カスタム通知ロゴの指定

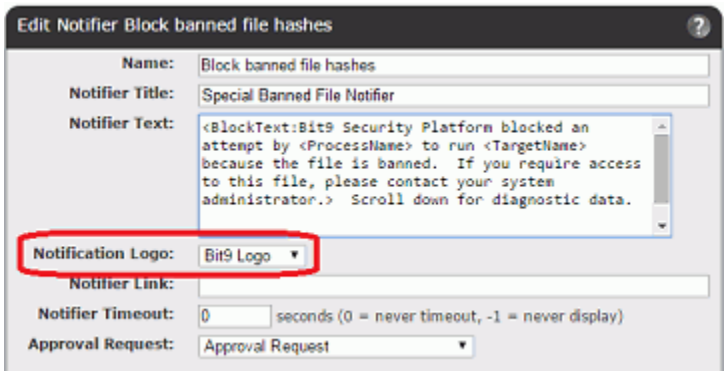
デフォルトでは、エージェント コンピューターでファイルがブロックされたときに表示される通知にはBit9 ロゴが表示されます。通知にロゴを表示しないことも、カスタム ロゴを指定することもできます。ロゴは通知ごとに指定します。

重要

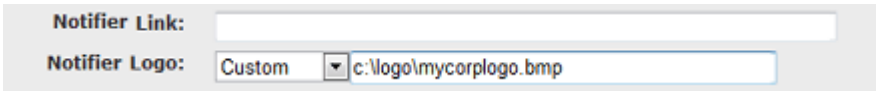
- 7.0.0 以前に導入されたカスタム ロゴは（Bit9 テクニカル サポートから提供される特別なソリューションと、Bit9 (Parity) 6.0.2 に用意されている標準カスタマイズのどちらも）、v7.2.3 にアップグレードするときに保持されません。カスタム ロゴを導入するには、以下の方法を使用する必要があります。v7.0.0 以降で指定したカスタム ロゴは、アップグレード後も保持されます。
- 6.0.2 以前の Bit9 エージェントは、アップグレードされるまで新たに設定されたカスタム ロゴを表示できません。

通知のカスタム ロゴの指定手順：

1. コンソール メニューで、[**Rules**（ルール）] > [**Notifiers**（通知）] の順に選択します。[Notifiers（通知）] ページが表示されます。
2. [Notifiers（通知）] ページで、以下のいずれかを実行します。
   - 新しい通知を作成する場合は、[**Add Notifier**（通知の追加）] をクリックします。[Add Notifier（通知の追加）] ページが表示されます。
     または
   - 編集する既存の通知名の隣にある [View Details（詳細の表示）]（ファイルと鉛筆）ボタンをクリックします。[Edit Notifier（通知の編集）] ページが表示されます。



3. ［Notifier Logo（通知ロゴ）］メニューで［**Custom**（カスタム）］を選択します。メニューの隣にテキスト ボックスが表示されます。



4. 使用するロゴを含むファイルをアクセス可能な場所に保存し、［Notifier Logo（通知ロゴ）］テキスト ボックスにその場所を入力します。ロゴ ファイルの場所を指定する方法には、以下の 3 つがあります。

   - **UNC：*\\server\share\path\imagefile.gif*** 形式でロゴ ファイルのネットワーク ベース パスを指定できます。Bit9 エージェントはローカル コピーの作成を試みます。ファイルがダウンロードできない場合、エージェントは新しいイメージを取得できるまで以前のイメージ（デフォルトの Bit9 イメージなど）を使用します。エージェントは、イメージをダウンロードできるまで、またはイメージが明示的に変更または無効化されるまで、1 時間ごとにイメージのダウンロードを試みます。
     注意：エージェント コンピューターからこのイメージにアクセスできるように、**LocalSystem** アカウントには指定された UNC パスへのアクセス権が必要です。また、アクセスにパスワードが要求される場所にはロゴを配置しないでください。
   - **URL：http*://path/imagefile.gif*** の形式で Web ベースのパスを指定できます。Bit9 エージェント プロセスによってアクセス可能で、匿名未承認アクセスを許可するパスを指定する必要があります。上記の説明と同様に、Bit9 エージェントはこのファイルのローカル コピーを作成します。
   - **ローカル：*d:\path\imagefile.gif*** の形式で（ローカル コンピューターの）ローカル ファイル パスを指定できます。ターゲット ファイルは、Bit9 エージェント プロセスからローカルでアクセスできる必要があります。ロゴ ファイルは、ロゴを使用する各エージェント コンピューター上に配置する必要があります。このファイルの更新は、次回通知が表示されるときに行われます。指定されたファイルにアクセスできない場合は、代わりに Bit9 ロゴが表示され、ローカル パス以外の場合と同様に Bit9 エージェント セッションごとにイベントが生成されます。

5. ［**Save**（保存）］をクリックします。変更が保存され、［Notifiers（通知）］ページが表示されます。
6. カスタム ロゴを表示する各通知に対して上記の手順を繰り返します。

イメージ ファイルの要件

Bit9 エージェントがインストールされている Windows システムには、**GenericLogo.gif** という名前の空白のサンプル通知イメージが含まれています。保存場所は Bit9 データ ディレクトリ（デフォルトでは **ProgramData\Bit9\Parity Agent\images**）です。Bit9 Server にエージェントがインストールされている場合は、サーバー上でこのフォルダーを開き、自社のロゴ イメージを作成する開始点として GenericLogo.gif を使用できます。それ以外の場合は、エージェントがインストールされている別のシステムにこのイメージをコピーします。

指定するカスタム イメージは、以下の要件を満たしている必要があります。

- イメージ サイズが 60 x 60 ピクセルである。
- ファイル形式が GIF、JPG、または BMP である。
- GenericLogo.gif と同じ背景を使用している。透明の背景は使用できません。

ロゴ関連イベント

Bit9 エージェントがカスタム ロゴを正常に取得しても、ロゴ関連のイベントは生成されません。ただし、エージェントがロゴ ファイルの取得に失敗すると、サブタイプ「Agent Error」のイベントが生成され、コンピューター名とイメージ ファイル名が通知されます。ロゴの取得に失敗した場合、コンピューターがその後カスタム ロゴを正常に取得すると別のイベントが生成されます。

ロゴ イメージの変更

通知ロゴとして非ローカル イメージを指定する（UNC または URL パスを使用する）場合、そのイメージは各エージェント システムに（エージェントがインストールされていればサーバーであっても）コピーされます。非ローカルのイメージを変更しても名前を変更しない場合は、Bit9 エージェントは変更後のイメージに更新しません。

通知のロゴ イメージを更新するには、イメージ ファイル名を変更し、そのポリシーの通知ロゴ パスを更新します。たとえば、カスタム ロゴ ***\\server\share\mylogo.gif*** を設定した後にこのロゴを変更した場合は、ファイル名を **mynewlogo.gif** に変更し、通知の詳細でそのパスを **\\server\share\mynewlogo.gif** に編集します。これで、そのポリシーのエージェントによって新しいイメージに更新されます。

エージェントにダウンロードされたイメージ ファイルは、更新も削除もできません。そのため、mylogo.gif から mynewlogo.gif に変更した後で mylogo.gif に戻すと、ソース イメージ ファイルを変更してあっても、最初にダウンロードされたバージョンの mylogo.gif が使用されます。

ポリシーでの通知ロゴの抑止

ポリシーのすべての通知の通知ロゴは、非表示にできます。［Add/Edit Policy（ポリシーの追加 / 編集）］ページの［Suppress Logo in Notifier（通知のロゴの抑止）］チェックボックスをオンにすると、各通知で指定されている通知構成に関わらず、通知ロゴが抑止されます。

初期設定への通知のリセット

すべてのデフォルト通知は、初期設定にリセットできます。初期設定にリセットすると、その通知に対して行ったすべてのカスタマイズが失われます。リセットを取り消すことはできません。通知をリセットするには、[Edit Notifier（通知の編集）] ページを開き、[**Reset Notifier**（通知のリセット）] をクリックします。このページに [Reset Notifier（通知のリセット）] ボタンが表示されない場合、その通知はデフォルト通知ではありません。

初期通知へのポリシーのリセット

[Edit Policy（ポリシーの編集）] ページには [Reset Policy（ポリシーのリセット）] ボタンがあります。このボタンをクリックし、確認ダイアログで **[OK]** をクリックすると、[Device Settings（デバイス設定）] および [Advanced Settings（高度な設定）] がテンプレート ポリシーの「初期」設定（Bit9 Server のインストール直後に有効になった設定）にリセットされます。ポリシーの各設定がデフォルト通知に戻ります。

Bit9 通知の無効化

一部またはすべてのエージェント コンピューターで、通知の無効化が必要になることがあります。たとえば、専用デバイスを高適用レベルで運用している場合、不正なアクションはフィードバックなしでそのままブロックすることが考えられます。ブロック専用通知は、通知を表示するルールを無効化しなくても無効化できます。通知は、各ポリシーの設定ごとに無効化できます。また、特定のカスタム ルール、メモリ ルール、またはレジストリ ルールの通知も無効化できます。

無効化できるのは、「ブロック専用」ルールの通知のみです。ユーザーに対応を「促す」プロンプト ルールは、常に通知を表示する必要があります。

Bit9 通知を無効化しても、アクションが常に通知なしでブロックされるとは限りません。一部の Bit9 ブロックは、発生時にオペレーティング システムの通知が表示されます。また、通知を無効化しても、アクションとして「サイレント ブロック」が定義されているカスタム ルール、レジストリ ルール、またはメモリ ルールによるブロックである場合を除き、イベントによるブロックの記録は継続されます。

ポリシーの通知設定の無効化手順：

1. 通知を無効化するポリシーの [Edit Policy（ポリシーの編集）] ページを開きます。
2. [Advanced Setting（高度な設定）] の通知を無効化する場合は、[**Show Advanced Settings**（高度な設定の表示）] をクリックします。
3. 無効化する通知の設定に対して、[Notifiers（通知）] メニューで [<none>（なし）] を選択します。
   通知を [<none>（なし）] に変更する前に、この設定が適用されるあらゆる状況を考慮してください。たとえば、[Block unapproved executables（未承認の実行可能ファイルをブロック）] に対して [<none>（なし）] を選択すると、未承認ファイルの実行のブロックまたは許可を選択する必要がある中適用レベルのポリシーのユーザーは、その決定を下す機会を得られません。このファイルは、Bit9 からの通知なしでブロックされます。

4. ［**Save**（保存）］ボタンをクリックして変更を保存します。［Policies（ポリシー）］ページが表示されます。
5. このポリシーで変更する設定に対して、手順 3 ～ 5 を繰り返します。
6. 通知を変更する各ポリシーに対してこの手順を繰り返します。

特定のカスタム ルール、レジストリ ルール、またはメモリ ルールの通知の無効化手順：

1. コンソール メニューで、［**Rules**（ルール）］>［**Software Rules**（ソフトウェア ルール）］の順に選択します。
2. ［Software Rules（ソフトウェア ルール）］ページで、変更するルール タイプのタブをクリックします。
3. ルールのテーブルで、通知を無効化するルールの隣の［View Details（詳細の表示）］（ファイルと鉛筆）ボタンをクリックします。
4. ［Edit Rule（ルールの編集）］ページで、ルールで設定されているアクションの隣の［Use Policy Specific Notifier（ポリシー固有の通知を使用）］ボックスを「オフ」にします。
5. ［Custom Notifier（カスタム通知）］メニューで［<none >（なし）］を選択します。ただし、ユーザーに決定を促すルールでは［<none>（なし）］オプションを選択できません。
6. ［**Save**（保存）］をクリックして変更を保存します。

通知が無効化されても、アクションがブロックされると、イベントによる記録は行われます。一部のルールでは、アクション メニューから［Block Silently（サイレント ブロック）］を選択することで、通知とイベント記録の両方を無効化できます。

注意

（設定で通知なしを選択するのではなく）通知が表示されるすべての場所について無効化することもできます。その場合は、［Add/Edit Notifier（通知の追加 / 編集）］ページの［Notifier Timeout（通知のタイムアウト）］に値としてマイナス 1 **(-1)** を入力します。

Windows セッション仮想化の通知

Bit9 Security Platform は、Citrix XenApp、Windows Server リモート デスクトップ サービス、Windows Server ターミナル サービスなどによって提供されるセッション仮想化環境向けに通知の特別処理をサポートしています。これらの環境では、次のように特別な通知タグを追加して、通知を転送するように Bit9 サーバーに指示できます。1 名のユーザーが複数のセッションにログインしており、通知をトリガーするアクションを試みた場合、そのユーザーのすべてのログイン セッションに通知を表示する。プロンプト通知の場合は、ユーザーがこれらの通知のいずれかに対応すると、すべての通知を終了する。ブロック通知の場合は、各セッションで通知を終了する必要がある。

- 複数のユーザーが 1 つのセッションにログインしており、そのいずれかのユーザーが通知をトリガーするアクションを試みた場合、ブロックをトリガーしたユーザーにのみ通知を表示する。
- 通知をトリガーするアクションが、特定のユーザーではなくシステムによって開始された場合は、通知を特定のユーザーかグループ、またはすべてのユーザーに表示するか、どのユーザーにも表示しないかを選択できる。どのオプションを設定しても、Bit9 によって［Event（イベント）］ページにブロック イベントは記録される。
- 特別な通知動作を有効化していても、セッション仮想化を使用していないエージェント管理コンピューターのユーザーには、通常のルールに従って通知を表示する。

注意

- 通知の特別処理は、ターミナル サーバーまたはアプリケーション サーバー上で「ホストされているセッション」（セッション仮想化）にのみ適用されます。つまり、単一のシステムと、そのシステム上のユーザーおよびアプリケーションに適用されます。アプリケーションをローカルで実行するアプリケーション仮想化には、この機能は適用されません。
- 通知は常に、ブロックされるアクションを実行したユーザーのセッションにダイレクトされます。アクションの実行元のセッションとは限りません。たとえば、ユーザー A がユーザー B のコマンド プロンプトにアクセスでき、ユーザー A が `runas /user:A cmd.exe` を実行してから未承認ファイルを実行した場合、通知はユーザー A が未承認ファイルを実行したように見えるセッションではなく、ユーザーA のリモート セッションに表示されます。
- **プラットフォームに関する注意：**ブロードキャスト通知は Windows セッションでのみ利用できます。

セッション仮想化の通知動作は、次の 2 つのタグでアクティブ化できます。

- **<NotifierBroadcastMessage>** は、特別な通知転送を有効化するために必要です。このタグがある場合、通知はアクションを開始したユーザーのすべての

セッションに表示されるか、システム　　アクションの場合は NotifierBroadcastSystem の指定どおりに表示されます。

- **<NotifierBroadcastSystem:*user*|*group*|*blank*>** は、システムによって開始されたアクションが Bit9 ルールにブロックされたときの動作を決定するために使用されます。デフォルトは **<Notifier BroadcastSystem>**（引数なし）です。通知からこのタグを削除し、<NotifierBroadcastMessage> を残す場合、通知はすべてのログイン セッション ユーザーに表示されます。

以下の手順は、1 つのポリシー内のすべての設定の通知動作を変更することを前提としています。これらのタグは、［Notifier（通知）］ページで個別の通知に追加することもできます。

セッション仮想化の特別な通知転送を有効化する手順：

1. コンソール メニューで、［**Rules**（ルール）］>［**Policies**（ポリシー）］の順に選択します。
2. 通知を編集するポリシーの隣の［View Details（詳細の表示）］（ファイルと鉛筆）ボタンをクリックします。
3. 変更する通知の設定を選択し、［Notifier（通知）］フィールド右の［**Edit**（編集）］ボタンをクリックします。
4. ［Edit Notifier（通知の編集）］ダイアログで、［Notifier Text（通知テキスト）］フィールドに **<NotifierBroadcastMessage>** を入力します。
5. ［Notifier Text（通知テキスト）］フィールドに、**<NotifierBroadcastSystem:>** タグと必要なオプションを入力します。
   - システムによって開始されたアクションのブロックに対する通知を 1 名のユーザーに転送するには、コロンの後にユーザー名を入力します。例：**<NotifierBroadcastSystem:MYCORP\jsmith>**
   - システムによって開始されたアクションのブロックに対する通知をグループのメンバーに転送するには、コロンの後に特定のグループ名または組み込みグループ名を入力します。例：**<NotifierBroadcastSystem:MYCORP\itgroup>**
   - システムによって開始されたアクションのブロックに対する通知を抑止するには、コロンの後に何も入力しません（その場合、コロンは省略できます）。例：**<NotifierBroadcastSystem>**
     このケースで通知を抑止する場合、中適用レベルのポリシーのユーザーには、未承認のソフトウェアを許可するオプションは与えられません。このソフトウェアは常にブロックされます。
   - 通知テキスト領域から **<NotifierBroadcastSystem>** タグを削除し、**<NotifierBroadcastMessage>** を残す場合、通知はすべてのログイン セッション ユーザーに表示されます。
6. ［**Save**（保存）］をクリックして、通知への変更を保存します。
7. ポリシーの各通知（および変更する他の要素）に対してこの手順を繰り返します。

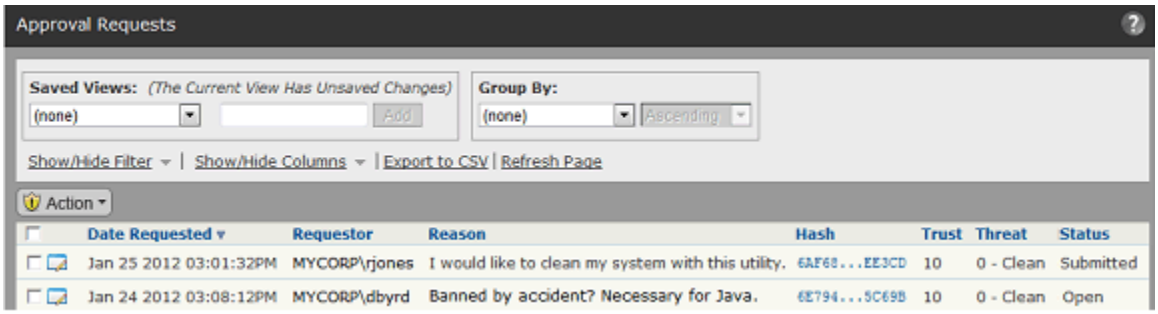
承認要求と根拠

Bit9 ルールによってアクションがブロックされると、通常はアクションがブロックされたコンピューター上に通知が表示されます。承認要求機能を利用すると、ユーザーは通知が表示されたときに管理者にフィードバックを送信できます。

- **承認要求** – アクションが「ブロック」され、許可するオプションが与えられない場合でも、ユーザーはブロックされたファイルやデバイスへのアクセスを必要とすることがあります。Bit9 通知は、ブロックされたファイルやデバイスに対する正式の「承認要求」をユーザーが送信できるように設定できます。
- **根拠** – アクションによって「プロンプト」通知がトリガーされ、アクセスをブロックまたは許可するオプションをユーザーに提供する場合、ユーザーがアクションを許可する理由の説明を可能にする（または求める）必要が生じることがあります。承認要求機能には、このような「根拠」を送信するためのインターフェイスも含まれています。

送信された承認要求と根拠は、ともに Bit9 コンソールの［Approval Request（承認要求）］テーブルに表示されるため、容易に管理および対応できます。承認要求と根拠は Bit9 イベント データベースに記録されます。必要に応じて、承認要求が送信された場合にトリガーされる組み込みアラートを有効化できます。根拠用のアラートも用意されています。

この章では「承認要求」という用語は、承認要求と根拠の両方を含む機能を表す一般的な用語として使用されます。必要な場合には区別して説明します。



注意

- 7.0以前のエージェントが稼働するコンピューターでは、承認要求や根拠は送信できません。
- 承認要求と根拠は、カスタム ルール、レジストリ ルール、またはメモリ ルールでの使用を想定していません。
- 承認要求機能の代用として「通知リンク」を、「Bit9 コンソール外部」で管理される承認要求プロセスとして使用できます。通知リンクを使用すると、ファイル承認の責任者またはグループ向けの空白の E メールを自動的に開いたり、管理者が IT 要求処理に使用する Web ページにユーザーを移動させたりできます。これらのリンクの設定方法の詳細については、「通知テキストの編集」（557 ページ）を参照してください。
  プラットフォームに関する注意：通知リンクは Windows コンピューターでのみ表示されます。

承認要求と根拠の有効化

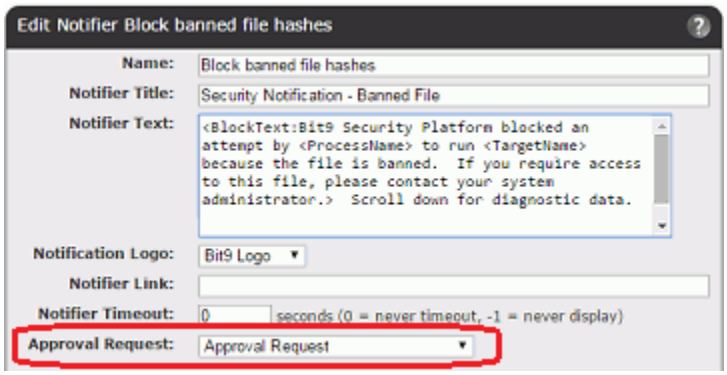
承認要求と根拠は、通知ごとに有効化します。有効化のための操作（必要な場合）は、7.0 以前のリリースからアップグレードしているか、およびこの機能の外観と動作をカスタマイズするかによって異なります。

- **新規インストール**– バージョン 7.0.0 以降の Bit9 Security Platform の新規インストールでは、承認要求はデフォルト ポリシーとテンプレート ポリシーのすべてのファイルおよびデバイスのブロック設定で有効化されています。これらのポリシーから作成する新しいポリシーにも承認要求と根拠が設定され、通知インターフェイスではこの 2 つが区別されます。通知をカスタマイズしない場合は、以下で説明する手順を実行する必要はありません。
- **アップグレード**– Bit9 (Parity) の 7.0 以前のバージョンからのアップグレードでは、承認要求は有効化されません。承認要求は、各通知の［Approval Request（承認要求）］メニューを使用して有効化できます。通知テキストにタグを追加すると、外観をさらにカスタマイズできます。アップグレードの場合、v7.0.1 以前にカスタマイズした通知では、通知ラベルで「承認要求」と「根拠」が区別されません。

プラットフォームに関する注意：承認要求や根拠を無効化すると、プロンプト通知と Windows のブロック専用通知で関連パネルが表示されなくなります。Mac および Linux では、承認要求や根拠が無効化されているブロック イベントを選択すると、［Bit9 Notifier History（Bit9 通知履歴）］ウィンドウの［Justification（根拠）］パネルがグレー表示になります。

通知の承認要求や根拠を有効化する手順：

1. 通知を選択し、その［Edit（編集）］ページを開きます。



2. ［Approval Request（承認要求）］メニューで、目的のオプションを選択します。以下のオプションを選択できます。
   - **Approval Request（承認要求）**
   - **Justification（根拠）**
   - **Approval Request and Justification（承認要求と根拠）**
   - **None（なし）**
3. ［**Save**（保存）］ボタンをクリックします。

注意

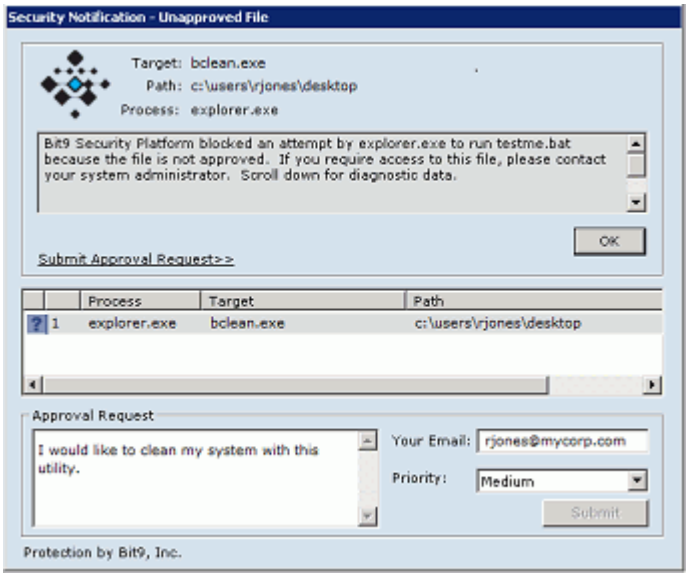
承認要求が閉じられている場合、要求者への自動 E メール通知を有効化できます。「要求と根拠の解決」(577ページ) を参照してください。

承認要求と根拠の送信

ファイル アクションがブロックされ、ファイルを許可するオプションがない場合でも、承認要求が有効化されていれば、ユーザーはファイルの承認を要求できます。この要求を入力する場所はプラットフォームによって異なります。

Windows コンピューターでは、承認要求はブロック通知を通じて送信します。ユーザーは、通知内でブロックとその理由の説明を確認できます。理由を確認してもブロックされたファイルやデバイスにアクセスする必要がある場合、ユーザーは通知の左下に表示されている［Approval Request（承認要求）］ボックスに承認要求を入力できます（最大 512 文字）。必要に応じて、E メール アドレスを入力して要求に含めることができます。［Priority（優先度）］も設定できます（デフォルトは［Medium（中）］）。承認を要求するテキストを入力すると、［**Submit**（送信）］ボタンが有効化されます。このボタンをクリックすると Bit9 Server に要求が送信されます。

Windows 通知では、［Submit Approval Request（承認要求を送信）］リンクではなく［Submit（送信）］ボタンによって要求を送信します。［Submit Approval Request（承認要求を送信）］リンクは、通知の下部に表示される［Approval Request（承認要求）］パネルの開閉に使用します。



要求を送信しても Windows 通知は終了しません。ブロック専用通知を閉じるには、[**OK**] をクリックする必要があります。

Mac および Linux コンピューターでは、アクションが完全にブロックされた場合、ユーザーは［Bit9 Notifier history（Bit9 通知履歴）］ウィンドウで履歴からブロック イベントを選択し、上記の Windows の説明と同様に情報を入力（最大 512 文字）することによって承認を要求できます。Windows とは異なり、Mac および Linux ユーザーは［Bit9 Notifier history（Bit9 通知履歴）］ウィンドウを閉じずに、複数のファイルの承認を要求できます。

どのプラットフォームでも、ファイルに対するアクションの許可またはブロックの選択を通知によって促された場合、ユーザーはファイルに対するアクションの許可を選択する「根拠」を送信できます。この情報は、承認要求と同じようにして送信されます。次にユーザーは、［**Block**（ブロック）］ボタンか、アクションを

発生させるいずれかのボタン（[**Allow**（許可）]または［**Promote**（昇格）]）をクリックする必要があります。

ユーザーが要求または根拠を送信すると、エージェントから要求への正式な接続はなくなります。ただし、ユーザーは同じファイルまたはデバイスに対して別の要求を送信でき、再送信の際はコメントや優先度（ファイルにアクセスできないためにタスクを実行できないなど）を変更できます。要求に対応するかどうかは、要求を確認する Bit9 Security Platform 管理者が判断します。

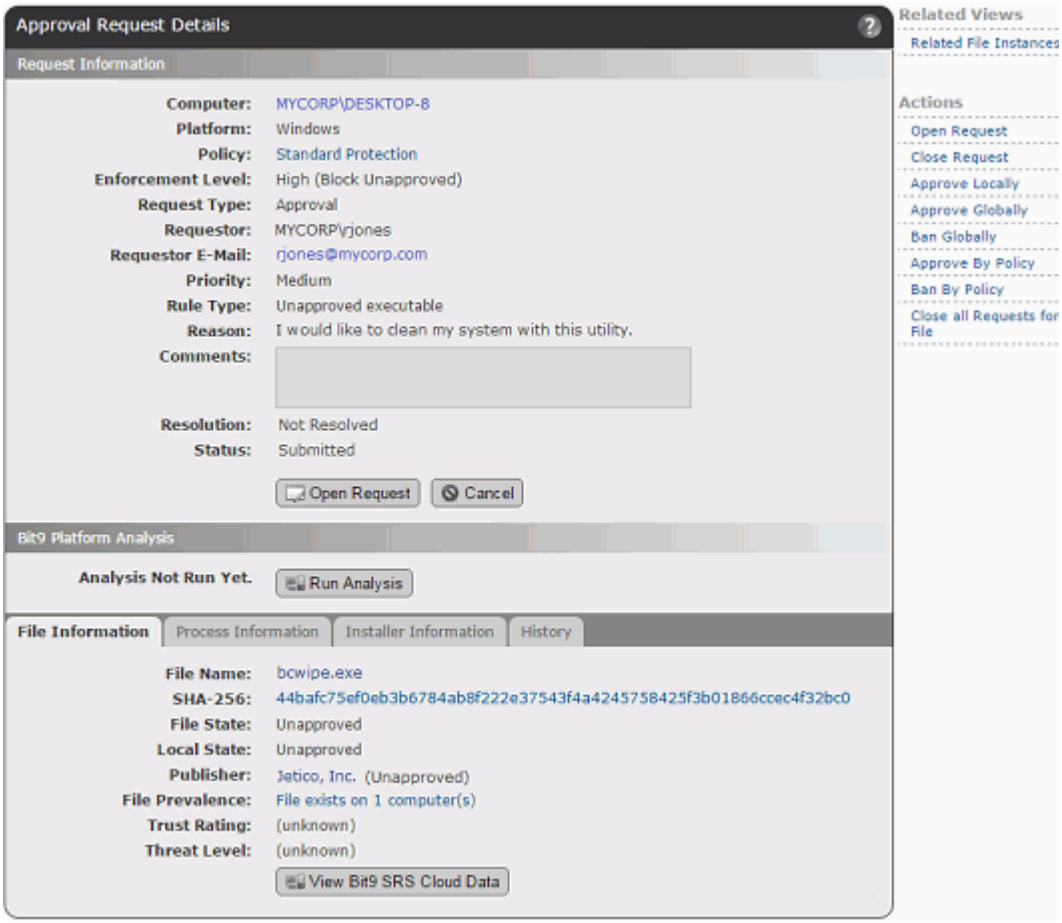
承認要求と根拠の表示

承認要求は、デフォルトの Administrator および PowerUser 権限を持つ Bit9 コンソール ユーザーが管理できます。また、承認要求の表示および管理権限を持つカスタム グループを作成できます。

送信された要求と根拠は、[Approval Request（承認要求）]ページに表示されます。このページにアクセスするには、Bit9 コンソール メニューで、［**Tools**（ツール）] > ［**Approval Requests**（承認要求）］を選択します。初期状態では、要求または根拠の［Status（ステータス）]は［Submitted（送信済み）]、［Resolution（解決）]は［Not Resolved（未解決）］です。［Preferences（設定）］ページ（［**Tool**（ツール）] > ［**Preferences**（設定）］）で、ログイン時に表示されるデフォルトの開始ページとして［Approval Request（承認要求）]ページを設定できます。

要求の［Status（ステータス）]を「オープン」に変更して、この要求への対応を開始したことを示すことができます。要求の編集可能フィールドを変更するためには、この変更が必要です。要求をオープンするには、[Approval Requests（承認要求）]ページのテーブルの［Actions（アクション）]メニュー、または［Approval Request Details（承認要求の詳細）]ページの［Actions（アクション）]メニューを使用します。

特定の承認要求の詳細を表示するには、その要求の隣の［View Details（詳細の表示）]（ファイルと鉛筆）ボタンをクリックします。



[Approval Request Details（承認要求の表示）]ページでは、要求と要求されたファイルまたはデバイスの詳細を確認できます。また、要求の編集（コメントの追加、要求に対して行った対応の入力など）も実行できます。このページの右側の[Actions（アクション）]メニューからは、ブロックされたファイルやデバイスへのアクセスを許可する場合に変更が必要なBit9ルールの一部に簡単にアクセスできます。

[Approval Request Details（承認要求の詳細）]ページは、以下のパネルに分かれています。

- [**Request Information**（要求情報）]パネルには、主に要求自体に関する情報（要求元のコンピューターとユーザー、要求に関連する Bit9 ルールと設定など）が表示されます。ユーザーが入力した要求の説明や、管理者が対応を入力するフィールドも表示されます。このパネルに含まれるフィールドの詳しい説明については、表 67、「要求 / 根拠情報」582 ページを参照してください。
- [**Bit9 Analysis**（Bit9 分析）]パネルは、初期状態では空白です。[**Run Analysis**（分析の実行）]ボタンをクリックすると、ブロックされたファイルまたはデバイスや、承認を要求するユーザーに関連する情報、その他の要求関連情報が表示されます。この分析で提供される情報の詳しい説明については、表 68、「Bit9 要求および根拠分析」582 ページを参照してください。分析を実行済みの場合は、[Rerun Analysis（分析の再実行）]をクリックすると情報を更新できます。これは Bit9 Software Reputation Service 分析ではありません。この分

析データを取得するには、[File information（ファイル情報）] タブ パネルで [Analyze（分析）] をクリックします。

- [**File Information**（ファイル情報）] パネルには、ブロックされたファイルの名前、ハッシュ、普及度、公開者、状態、(Bit9 SRS がアクティブでファイルが既知の場合は）信頼度および脅威レベルが表示されます。このパネルで [**Analyze**（分析）] ボタンをクリックすると、このファイルに関する詳しい Bit9 SRS 情報を取得できます。このパネルの各フィールドの説明については、表 69、「承認要求 / 根拠の詳細のファイル情報」 585 ページを参照してください。ただし、デバイスと、非実行可能ファイルの書き込みブロックについては、すべての情報の説明は提供されません。
- [**Process Information**（プロセス情報）] パネルには、アクションの開始を試みたプロセスに関する情報が表示されます。このパネルの各フィールドの説明については、表 70、「要求 / 根拠の詳細のプロセスおよびインストーラー情報」 586 ページを参照してください。
- [**Installer Information**（インストーラー情報）] パネルには、ブロック ファイルをインストールしたインストーラー（既知の場合）に関する情報が表示されます。このパネルの各フィールドの説明については、表 70、「要求 / 根拠の詳細のプロセスおよびインストーラー情報」 586 ページを参照してください。
- [**History**（履歴）] パネルには、承認要求に対する変更日時（作成、オープン、変更、クローズの日時を含む）が表示されます。要求に対応して Bit9 ルールに加えた変更の履歴は表示されません。

要求と根拠の解決

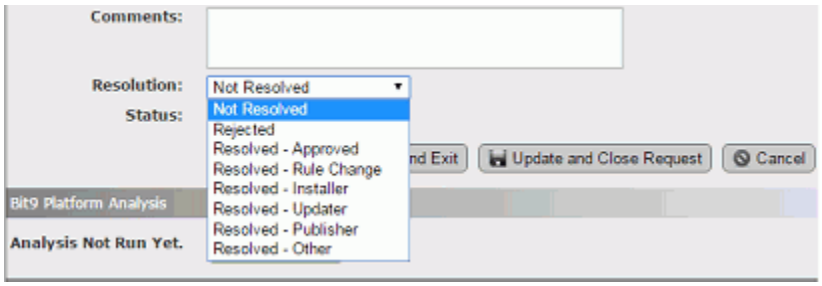
要求または根拠に入力された情報を確認し、どのような対応を行うかを決定する準備ができた場合に行う主な手順を以下に示します。

- 要求をオープンして、対応を開始したことを示します。
- 要求を拒否しない場合は、ファイル状態やルールに対して必要な変更を加えます。
- 要求自体のステータスを更新し、必要に応じて自分の決定やアクションに関するコメントを入力します。コメントは監査目的で入力しますが、要求者へのフィードバックの提供のためにも使用できます。
- 要求をクローズして、対応が完了したことを示します。自動 E メール応答が有効化されている場合、要求をクローズすると要求元のユーザーへの E メール送信も行われ、決定内容が通知されます。
- 自動応答が有効化されていない場合に応答を送信するときは、承認要求元のユーザーに要求への対応を説明するメールを送信します。

承認要求を確認して解決する手順：

1. コンソール メニューで、[**Tools**（ツール）] > [**Approval Requests**（承認要求）] の順に選択し、確認する要求の隣の［View Details（詳細の表示）］ボタンをクリックします。[Approval Request Details（承認要求の詳細）]ページが開きます。
2. ［Approval Request Details（承認要求の詳細）］ページで、［Actions（アクション）］メニューから［**Open Request**（要求のオープン）］を選択するか、最初のパネルの下部の［Open Request（要求のオープン）］ボタンをクリックします。［Comments（コメント）］、［Resolution（解決）］、［Response E-mail（応答 E メール）］フィールドがアクティブになります。

3. ブロックされたファイルまたはデバイスへのアクセスを許可する場合は、［Actions（アクション）］メニューのコマンド ショートカットを使用して、ブロックを発生させた 1 つまたは複数の Bit9 ルールを変更します。たとえば、ファイルをローカルで承認するか、禁止を編集または削除するか、ファイルをグローバルで承認します。
［Action（アクション）］メニューのコマンドには、制限なくアクセスできます。要求に対応するには、他のルールの変更も必要になる可能性があります。
注意：どのような変更を行っても、要求自体の［Resolution（解決）］および［Status（ステータス）］フィールドには影響しません。これらのフィールドは個別に変更する必要があります。
4. ［Approval Request Details（承認要求の詳細）］の［Resolution（解決）］メニューから項目を選択して、要求への対応として行ったこと（または行わなかったこと）を示します。このフィールドは情報の提供のみを目的としており、ファイルやデバイスの状態には影響しません。要求されたアイテムへのアクセスを許可しない場合は、[**Reject**（拒否）] を選択します。[Resolution（解決）] メニューをアクティブにするには、要求のステータスが「オープン」である必要があります。



5. 要求への対応とその理由について詳しい情報を入力するには、[Comments（コメント）] を追加または変更します。
6. [Response E-mail（応答 E メール）] のアドレスが空の場合や誤っている場合、要求者に要求への対応を通知するには、要求がオープン状態の間にアドレスを追加または修正します。
7. 要求への対応が完了したら、[Action（アクション）] メニューから [**Close Request**（要求のクローズ）] を選択します。1 つのファイルに対して複数の要求がある場合は、[**Close All Requests for this file**（このファイルに対するすべての要求をクローズ）] を選択できます。要求をクローズすると、要求のステータスの把握に役立ちますが、自動 E メール応答が有効化されている場合には、要求を送信したユーザーに E メールで要求のステータスが通知されます。

   要求は必要に応じて再度オープンできます。
8. 要求者への自動 E メール通知が有効化されていない場合は、[Response E-mail（応答 E メール）] アドレス フィールドをクリックすると、宛先に要求者が指定されたメッセージがデフォルトの E メール クライアントで開きます。この操作を行う場合は、通知する応答の詳細を入力してから送信してください。

ユーザーへの承認要求への対応の通知

承認を要求したユーザーに、要求が解決したことを通知することができます。Bit9 は、E メールを介して通知する 2 つの方法を備えています。

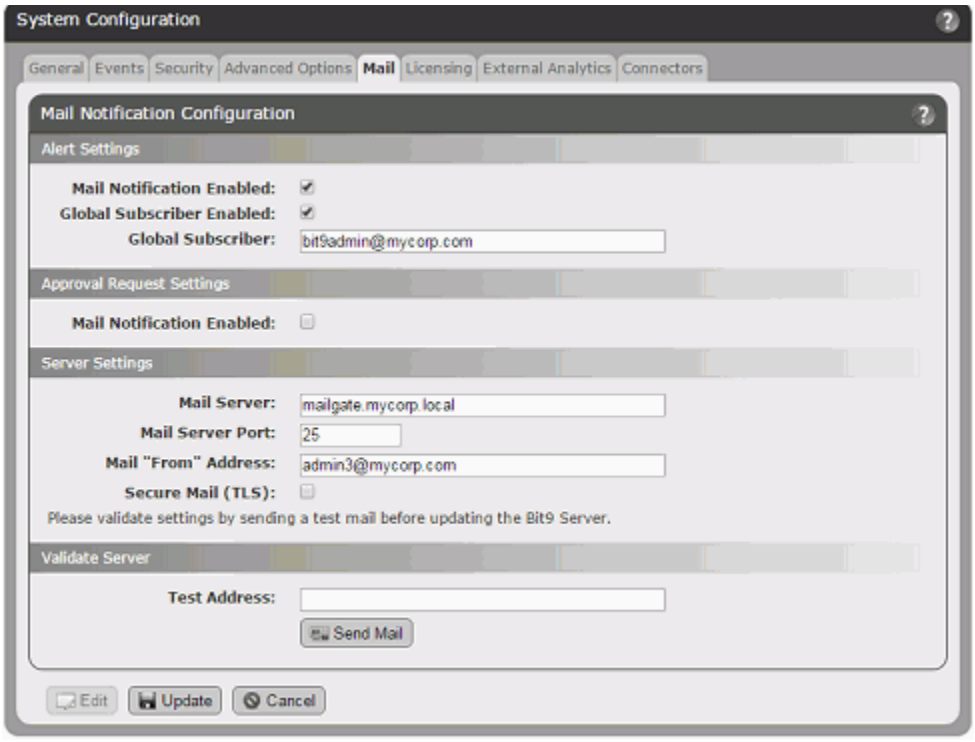
- **手動** – [Approval Request Details（承認要求の詳細）] ページの [Response E-mail（応答 E メール）] フィールドをクリックすると、事前設定された E メール フォームがデフォルトのメーラーで開きます。
- **自動** – 要求ワークフローに自動通知を追加できます。自動 E メール通知は、[System Configuration（システム構成）] ページの [Mail（メール）] タブで有効化します。この機能はデフォルトで無効になっています。

どちらの方法でも、応答メールは要求者が要求で指定した E メール アドレスに送信されます（指定されている場合）。

> **注意**
>
> 自動応答機能は、承認要求に対してのみ有効です。根拠に対しては E メールは自動送信されません。

承認要求への自動応答 E メールを有効化する手順：

1. コンソール メニューで、[**Administration**（管理）] > [**System Configuration**（システム構成）] の順に選択し、[System Configuration（システム設定）] ページで [**Mail**（メール）] タブをクリックします。
2. [Approval Request Settings（承認要求設定）] パネルで、[**Mail Notification Enabled**（メール通知の有効化）] チェックボックスをオンにします。



3. Bit9 Security Platform 用のメール サーバーを設定していない場合は、[Server Settings（サーバー設定）] パネルに必要な情報を入力し、テスト アドレスにメッセージを送信してサーバーを検証します。メール サーバー構成の詳細については、「アラート メールおよび承認要求メールの構成」（777 ページ）を参照してください。
4. ページ下部の［**Update**（更新）］ボタンをクリックして設定を保存します。

通知が送信されるタイミング

サーバーのメール構成を正しく設定し、承認要求通知を有効化してある場合、以下の状況で［Approval Request（承認要求）］を「閉じる」とメール通知が送信されます。

- ［Resolution（解決）］フィールドが［Not Resolved（未解決）］または［Rejected（拒否）］から、［Resolved（解決済み）］オプションに変更された。
- ［Resolution（解決）］フィールドが、他の何らかのオプションから［Rejected（拒否）］に変更された。
- オープンしていた要求がクローズされたときの［Resolution（解決）］フィールドが［Not Resolved（未解決）］である。

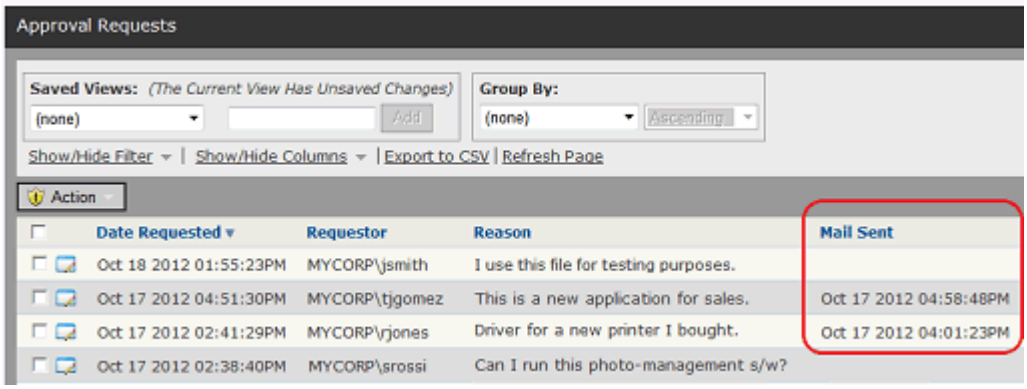
［Resolution（解決）］フィールドが 1 つの［Resolved（解決済み）］オプションから別の［Resolved（解決済み）］オプション（例：［Resolved - Approved（解決済み – 承認）］から [Resolved - Updater（解決済み – アップデーター）]）に変更された場合、通知メールは送信されません。

また、［Status（ステータス）］が［Closed（クローズ）］に変更されない限り、通知メールは送信されません。

承認要求通知を有効化するときに、すでにクローズされていた要求の通知は送信されません。ただし、通知が有効化された後に要求が初めてオープン（または再度オープン）された場合、[Status（ステータス）] および [Resolution（解決）] フィールドが上記の要件を満たしていれば要求者に通知が送信されます。

Bit9 Server には、要求対応メールの記録（サーバーからの送信時のタイムスタンプなど）が保持されます。この記録は、受信メールではなく、送信メールの記録です。受信者の E メール アドレスが正しくない場合でも、サーバーにはメッセージが送信されたことが記録されます。要求者の E メール アドレスがない場合、サーバーにメール送信の記録は保持されません。

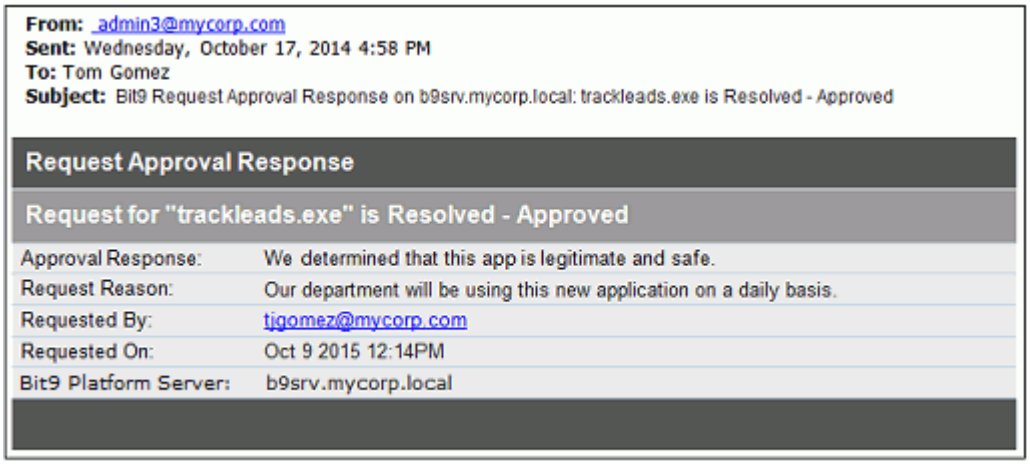
要求対応メールの送信日時の記録は、[Mail Sent（送信済みメール）] フィールドに表示されます。承認要求のテーブルでは、この列は [Show/Hide Columns（列の表示 / 非表示）]機能を使用して追加できるオプションの列です。[Approval Request Details（承認要求の詳細）] ページでは、メッセ ― ジが送信された場合は常に表示されます。



通知メールの内容

承認要求への対応メールが送信される際、メールには次の情報が含まれます。

- 承認が要求されたファイル名
- 対応（[Resolution（解決）] メニューで選ばれた項目）
- [Approval Request Details（承認要求の詳細）] ページで Bit9 Platform 管理者によって追加されたコメント
- 要求の理由（要求者が入力した場合）
- 要求者の E メール アドレス
- 要求日
- Bit9 Server のホスト名


From: admin3@mycorp.com
Sent: Wednesday, October 17, 2014 4:58 PM
To: Tom Gomez
Subject: Bit9 Request Approval Response on b9srv.mycorp.local: trackleads.exe is Resolved - Approved

Request Approval Response

Request for "trackleads.exe" is Resolved - Approved

Approval Response:	We determined that this app is legitimate and safe.
Request Reason:	Our department will be using this new application on a daily basis.
Requested By:	tjgomez@mycorp.com
Requested On:	Oct 9 2015 12:14PM
Bit9 Platform Server:	b9srv.mycorp.local

承認要求と根拠の詳細

次の表に、[Approval Request Details（承認要求の詳細）] ページのフィールドの説明を示します。[Approval Request（承認要求）] テーブルでは、オプションとして他のフィールドも利用できます。

表 67：要求 / 根拠情報

フィールド	説明
[Computer（コンピューター）]	ブロックが発生したコンピューター名。
[Policy（ポリシー）]	ブロック時にエージェント コンピューターで有効だったポリシー。
[Platform（プラットフォーム）]	ブロックが発生したコンピューターのプラットフォーム。
[Enforcement Level（適用レベル）]	ブロック時にエージェント コンピューターで有効だったポリシーの適用レベル。
[Request Type（要求タイプ）]	[Approval（承認）] または [Justification（根拠）]。
[Requestor（要求者）]	要求を行ったユーザー。
[Response E-Mail（応答 E メール）]	ブロックされたユーザーが入力した E メール アドレス（入力されている場合）。
[Priority（優先度）]	（ユーザーが設定した）要求の優先度。[High（高）]、[Medium（中）]（デフォルト）、[Low（低）] を選択できます。

フィールド	説明
[Rule Type（ルール タイプ）]	アクションをブロックしたルールのタイプ。たとえば、[Unapproved executable（未承認の実行可能ファイル）] は、未承認ファイルの実行をブロックするポリシーが適用されているコンピューター上で、未承認のファイルの実行がブロックされたことを示します。
[Reason（理由）]	通知に入力された承認要求テキストまたは根拠テキスト。
[Comments（コメント）]	要求を確認した管理者からのコメント。いつでも変更および更新できます。
[Resolution（解決）]	要求がどのように解決されたかを示します。メニューには以下の選択肢があります。 • Not Resolved（未解決） • Rejected（拒否） • Resolved-Approved（解決済み - 承認） • Resolved-Rule Change（解決済み - ルール変更） • Resolved-Installer（解決済み - インストーラー） • Resolved-Updater（解決済み - アップデーター） • Resolved-Publisher（解決済み - 公開者） • Resolved-Other（解決済み - その他） このフィールドの選択肢は情報の提供のみを目的としています。この選択によってルールやファイルの状態は変更されません。このフィールドは、要求または根拠がオープンされているときにのみ変更できます。
[Status（ステータス）]	要求のステータス。以下の値があります。 • Submitted（送信済み）– ユーザーが要求を送信済みです。 • Open（オープン）– 要求は管理者によってオープンされています。送信済みの要求とクローズされた要求の両方をオープンできます。[Resolution（解決）] フィールドを変更するには、要求をオープンする必要があります。 • Closed（クローズ）–（おそらく何らかの方法で解決されたため）要求はクローズされています。要求に対応するアクションを実行していなくても、要求はクローズできます。
[Mail Sent（送信済みメール）]	要求への自動対応が有効化されており、この要求に対してメールが送信された場合、このフィールドにはそのメールのタイムスタンプが表示されます。

[Bit9 Analysis（Bit9 分析）] パネルには、[**Run Analysis**（分析の実行）] ボタンをクリックして得られた情報が表示されます。このパネルは、ブロック ファイルとアクセスを要求するユーザーに関する統計情報を提供します。

表 68：Bit9 要求および根拠分析

リンク / ボタン	コメント
<number >blocks seen by this computer within 1 hour(s).（このコンピューターで 1 時間以内にブロックが <number> 回発生しました。）	分析の実行開始までの 1 時間に、このコンピューターで発生したブロック数。このリンクをクリックすると、フィルターされた［Event（イベント）］ページが開き、このコンピューターに関連するすべてのタイプのブロック イベントが表示されます。
<number> blocks from this process on this computer. within 1 hour(s).（1 時間以内にこのコンピューターのこのプロセスが <number> 回ブロックされました。）	分析の実行開始までの 1 時間に、このコンピューター上で特定のプロセスをブロックした回数。このリンクをクリックすると、フィルターされた［Event（イベント）］ページが開き、このコンピューターでブロックされているアクションの実行を試みたプロセスに関連するブロック イベントが表示されます。
<number> files written by <the process that tried to execute this file> on this machine.（このコンピューター上で < このファイルの実行を試みたプロセス > によって <number> 件のファイルが書き込まれました。）	このリンクをクリックすると、フィルターされた［Find Files（ファイルの検索）］ページが開き、このマシン上でこのプロセスによって書き込まれたファイルが表示されます。 **プラットフォームに関する注意**：このフィールドは、Windows コンピューター上のファイルに対してのみ表示されます。
<number> files written by <the process that tried to execute this file> on the network. (ネットワーク上で < このファイルの実行を試みたプロセス > によって <number> 件のファイルが書き込まれました。	このリンクをクリックすると、フィルターされた［Find Files（ファイルの検索）］ページが開き、任意のコンピューター上でこのプロセスによって書き込まれたファイルのすべてのインスタンスが表示されます。 **プラットフォームに関する注意**：このフィールドは、Windows コンピューター上のファイルに対してのみ表示されます。
File appears on <number> computers with <number> different hashes.（ファイルが <number> 個の異なるハッシュで <number> 台のコンピューターに出現しました。）	Bit9 Server で管理されているすべてのコンピューターで、要求されたファイルの名前とパスを検索した結果。このリンクをクリックすると、フィルターされた［Find Files（ファイルの検索）］ページが開き、このファイルの名前およびパスと一致するすべてのインスタンスが表示されます。
<number> approval requests for this file.（このファイルに対する承認要求は <number> 個です。）	「ハッシュ」によって識別されたこのファイルに対する要求数。このリンクをクリックすると、フィルターされた承認要求のテーブルが開き、このファイル ハッシュに対するすべての要求が表示されます。

リンク / ボタン	コメント
<number> total approval requests by this user.（このユーザーからの承認要求は合計 <number> 件です。）	このリンクをクリックすると、フィルターされた承認要求のテーブルが開き、このユーザーからのすべての承認要求が表示されます。
<number> open requests by this user.（このユーザーからのオープン要求は <number> 件です。）	このリンクをクリックすると、フィルターされた承認要求のテーブルが開き、このユーザーからのすべての「オープン状態」の承認要求が表示されます。
Last Analysis Completed On <datetime>（最後の分析は <datetime> に完了）（読み取り専用）	この要求に対する最後の分析の実行日時、または分析がまだ実行されていないことを示します。
Run/Rerun Analysis（分析の実行 / 再実行）（ボタン）	このパネルに情報を提供する分析が実行されます。分析が実行済みの場合は再実行されて、変更された情報（ユーザーからの要求の回数、ブロック ファイルの書き込みを試みたプロセスによって書き込まれたファイル数など）が更新されます。

表 69：承認要求 / 根拠の詳細のファイル情報

フィールド	説明
[File Name（ファイル名）]	リンクをクリックすると、ブロック ファイルの［File Instance Details（ファイル インスタンスの詳細）］ページが表示されます。
[SHA-256]	リンクをクリックすると、ブロック ファイルの［File Instance Details（ファイル インスタンスの詳細）］ページが表示されます。
[File State（ファイルの状態）]	Bit9 ファイル カタログでのこのファイルのグローバル状態。
[Local State（ローカル状態）]	このコンピューターでのブロックされたファイル インスタンスのローカル状態。
[Publisher（公開者）]	公開者名と公開者の承認状態。公開者名をクリックすると、ブロック ファイルの公開者の［Publisher Details（公開者の詳細）］ページが開きます。
[File Prevalence（ファイル普及度）]	ブロック ファイルが存在するコンピューターの数。
[Trust Rating（信頼度）]	ブロック ファイルの Bit9 SRS での信頼度（既知の場合）。範囲は 0（信頼度低）～ 10（信頼度高）です。
[Threat Level（脅威レベル）]	ブロック ファイルの Bit9 SRS での脅威レベル（既知の場合）。値は 0（クリーン）、1（危険な可能性あり）、2（悪質）です。

［Process（プロセス）］タブおよび［Installer（インストーラー）］タブは、それぞれについて同様の情報を提供します。

表 70：要求 / 根拠の詳細のプロセスおよびインストーラー情報

フィールド	説明
［Process（プロセス）］	ブロック ファイルの書き込みまたは実行を試みたプロセスの完全なパス。
［Installer（インストーラー）］	ブロック ファイルのインストーラーの完全なパス。
[SHA-256]	プロセスまたはインストーラーの SHA-256 ハッシュ。
［Trust Rating（信頼度）］	ブロック ファイルの実行を試みたプロセス、またはファイルをインストールしたインストーラーの Bit9 SRS での信頼度（既知の場合）。範囲は 0（信頼度低）～ 10（信頼度高）です。
［Threat Level（脅威レベル）］	ブロック ファイルの実行を試みたプロセス、またはそのファイルをインストールしたインストーラーの Bit9 SRS での脅威レベル（既知の場合）。値は 0（クリーン）、1（危険な可能性あり）、2（悪質）です。

変更可能な他の項目の詳細については、「通知の要求 / 根拠インターフェイスのカスタマイズ」を参照してください。

通知の要求 / 根拠インターフェイスのカスタマイズ

［Approval Request（承認要求）］パネルのヘッダー テキスト、リンク、指示テキストは変更できます。これらを変更する理由の 1 つは、以前のリリースで変更された通知の承認要求と根拠に異なるラベルを表示するためです。

注意

- カスタマイズしたタグを承認要求や根拠に追加するには、［Edit Notifier（通知の編集）］ページの［Approval Request（承認要求）］メニューを使用して承認要求 / 根拠機能を有効化する必要があります。
- **プラットフォームに関する注意：**［Bit9 Notifier History（Bit9 通知履歴）］ウィンドウの承認要求 / 根拠インターフェイスは、Windows コンピューターでのみカスタマイズできます。

表 71、「承認通知と根拠のカスタマイズ用タグ」に、通知の承認要求の変更に使用できるタグを示します。以下の例は、テンプレート　ポリシーの［Block unapproved executables（未承認実行可能ファイルのブロック）］の通知テキストです。ここでは、タグの挿入場所とそれぞれに表示するさまざまなラベルを示しています。

```
<BlockText:Bit9 は <ProcessName> による <TargetName> の実行の試行をブロックしました。このファイルは未承認です。このファイルへのアクセスが必要な場合は、システム管理者に連絡してください。><AskText:Bit9 は、<ProcessName> による <TargetName> の実行の試行を特定し、停止しました。このファイルは未承認です。このファイルの実行を許可する場合は［Allow（許可）］を選択してください。今回の実行を阻止する場合は［Block（ブロック）］を選択してください <NotifierRequestLink: 根拠を送信
><NotifierRequestText: アクセスを必要とする理由を入力してください。
><NotifierRequestHeading: 根拠 ><NotifierRequestProcessed: 根拠が送信されました。> 下にスクロールすると診断データが表示されます。
```

表 71：承認通知と根拠のカスタマイズ用タグ

タグ	説明
<NotifierRequestLink:*text*>	このテキストは、通知の［Approval Request（承認要求）］パネルを開閉するリンクに表示されます。
<NotifierRequestHeading:*text*>	このテキストは、ユーザーが要求を入力するテキスト ボックスの上に表示されます。
<NotifierRequestText:*text*>	このテキストは、ユーザーが要求を入力するテキスト ボックス内に表示されます。ユーザーが実際の要求の入力を開始すると、このテキストは消去されます。
<NotifierRequestProcessed:*text*>	ユーザーが要求を送信すると、テキスト ボックス内にこのテキストが表示されて、要求が処理されたことを示します。
<NotifierRequireSubmitOnAllow>	ユーザーが根拠を送信するまで、通知の［Allow（許可）］または［Approve（承認）］ボタンは（存在する場合）無効になります。
<NotifierRequireSubmitOnBlock>	ユーザーが根拠を送信するまで、プロンプト通知の［Block（ブロック）］ボタンは（存在する場合）無効になります。
<NotifierRequestMinLength:*n*>	ユーザーが要求 / 根拠テキスト ボックスに n 文字以上入力するまで、承認要求または根拠の［Submit（送信）］ボタンは（存在する場合）無効になります。

第 18 章

イベント、アラート、およびメーター

この章では、Bit9 イベント レポートおよびアラートを使用して、ネットワーク内のファイルのアクティビティやその他の重要な Bit9 操作を監視する方法を説明します。また、ネットワーク内で増殖するファイルの検出や、特定のファイルが実行された回数の追跡に活用できるツールについても説明します。

これらの機能は、単独でも組み合わせても多くの用途で使用できます。たとえば、ネットワーク内のコンピューターに未承認ファイルの実行を許可している場合、ファイル、コンピューター、コンピューター ユーザーごとに実行回数を追跡できます。環境全体を高適用レベルのみで運用している場合は、Bit9 監視機能を使用して確実に意図したとおりにファイルをブロックまたは許可できます。また、他の監視機能と「アラート」を組み合わせると、特定のアクションの発生時やしきい値の超過時に自動的に通知を受けることができます。

システム内のファイルのインベントリ全体について変更を追跡する Bit9 の機能の詳細については、第 19 章「変更の監視：ベースライン ドリフト レポート」を参照してください。

独自のツールを使用して Bit9 イベントとファイル情報を分析する方法については、付録 A、「ライブ インベントリ SDK：データベース ビュー」、および Bit9 テクニカル サポートが別途提供している『Bit9 Events Integration Guide（Bit9 イベント統合ガイド）』を参照してください。Bit9 イベントを外部データ分析ツールにエクスポートする方法については、付録 F、「外部分析のための Bit9 データのエクスポート」も参照してください。

セクション

監視の前提条件

Bit9 イベントを正確に監視するには、クライアント コンピューター（ラップトップ、デスクトップ、サーバー）がオンラインで、Bit9 エージェントによってアクティブに監視されている必要があります。この章では、以下のことを前提にしています。

- Bit9 ポリシーが作成および構成されている。
- Bit9 エージェントが監視対象のコンピューターにインストール済みで、これらのコンピューターの初期化が完了している。
- すべての Bit9 エージェントのバージョンが 7.0.0 以上である。

これらのタスクの詳細については、第 5 章「ポリシーの作成と構成」および第 4 章「コンピューターの管理」を参照してください。

監視の前提条件ではありませんが、外部イベント ロギング サーバーを使用する場合は、外部サーバーでできるだけ早くイベントの取得を開始できるように、外部サーバー システムに SQL Server をインストールし、Bit9 Server とこの外部サーバーとの接続を設定してください（「外部イベント ロギングの設定」（756 ページ）を参照）。

イベント レポート

Bit9 の［Events（イベント）］ページは、Bit9 のアクティビティに関連して記録されたすべてのイベント（ブロックされたファイル、実行された未承認ファイル、システム管理プロセス、コンソール ユーザーによるアクションなど）へのアクセスを提供します。Bit9 Server は、イベント ボリュームの影響をほとんど受けることなく、接続されているコンピューターのイベント データをほぼリアルタイムで更新します。

定義済みの Bit9 レポートを［Saved View（保存済みビュー）］メニューから利用できます。また、既存のビューをテンプレートとして使用するか、完全なイベント テーブルを開始点にして、独自の保存済みビューを作成して保存することもできます。どのイベント レポートも、新しい保存済みビューを作成せずに、期間を変更して結果を表示できます。

［Events（イベント）］ページには、指定した期間のイベントがページあたり最大 200 個表示されます。テーブルに表示されるイベント数を調節するには、このページの右下部分にある［**rows per page**（ページあたりの行数）］パラメーターを変更します。

注意

Bit9 の Syslog イベントを出力して、他のシステムで処理することもできます。その場合でも、イベント出力は Bit9 コンソールのイベント ログにも表示されます。詳細については、Bit9 の設定に関する章の「イベント管理のオプション」を参照してください。

Bit9 イベントは、外部データ分析製品によって使用されるフォルダーにエクスポートすることもできます。詳細については、付録 F、「外部分析のための Bit9 データのエクスポート」を参照してください。

イベントの完全なリストと、サポートされる Syslog 形式に出力をマッピングする方法については、Bit9 が別途提供するドキュメント『Bit9 Events Integration Guide（Bit9 イベント統合ガイド）』を参照してください。

［Home Page（ホーム ページ）］の［Event Report（イベント レポート）］ポートレットの使用

イベントを監視する手段の 1 つは、Bit9 コンソールの［Home Page（ホーム ページ）］の［Event Report（イベント レポート）］ポートレットを使用する方法です。このサマリー ポートレットは、［Events（イベント）］ページの以下の 4 つの事前定義された保存済みビューからの基本データ、およびこれらのビューへのリンクを提供します。ビューの詳細については、「［Events（イベント）］ページでのレポートの表示」（593 ページ）を参照してください。

- New installations（新規インストール）（Windows のみ）
- New unapproved files（新しい未承認ファイル）
- Blocked files (Banned)（ブロックされたファイル（禁止））
- Blocked files (Unapproved)（ブロックされたファイル（未承認））

このポートレットには、過去 24 時間に各タイプのイベントに関与したファイルやコンピューターの数が表示されます。このデータは、ページを表示または再表示すると更新されます。レポート名をクリックすると、完全なレポートを表示できます。

［Home Page（ホーム ページ)］の日次イベント サマリーを表示する手順：

1. コンソール メニューで、［**Home Page**（ホームページ)］をクリックします。デフォルトでは、［Event Reports（イベント レポート)］ポートレットはこのページの左下部分に表示されます。

2. ［Event Reports（イベント レポート）］ポートレットでレポート名をクリックすると、［Events（イベント)］ページの［Saved View（保存済みビュー)］が開き、完全なレポートが表示されます。詳細については、「［Events（イベント)］ページでのレポートの表示」を参照してください。

注意

カスタム イベント ポートレットを作成し、［Home Page（ホーム ページ)］や他のダッシュボードに表示することができます。詳細については、「ダッシュボードの使用とカスタマイズ」(693 ページ)を参照してください。

[Events（イベント）] ページでのレポートの表示

Bit9 Server 上で使用できるすべてのイベント レポートは、Bit9 が提供するレポートか、ユーザーが作成したレポートかを問わず、[Events（イベント）] ページに保存済みビューとして表示されます。表 72 に、事前定義済みの保存済みビューのリストと、それぞれに含まれるイベントを示します。

表 72：[Events（イベント）] ページの保存済みビュー

メニュー オプション	説明
(none)（なし）	選択された期間中のすべてのBit9イベントをフィルターせずに示すレポートが、デフォルト列を使用して表示されます。
Alerts and Meters（アラートとメーター）	アラートまたはメーターのすべての作成、変更、削除と、アラートをトリガーしたかメーターを増加させたすべての（選択した期間中の）アクティビティを含むレポートが表示されます。
Approval Requests（承認要求）	ブロック ファイルに対する承認要求の（エージェント コンピューター上での）作成、および（Bit9 コンソールでの）要求のオープンまたはクローズをすべて含むレポートが表示されます。
Blocked Files (All)（ブロックされたファイル（すべて））	選択した期間中に、何らかの理由でブロックされた（またはブロックされるはずだったが [Report Only（レポートのみ）] 状態だった）すべてのファイルを含むレポートが表示されます。このレポートには、明示的に禁止されているファイル、特定のコンピューターの適用レベルまたはポリシーによってブロックされた未承認状態のファイル、まだ分析されていないファイル、ブロックされたデバイス上のファイル、カスタム ルールによってブロックされたファイルが含まれます。 レジストリ ルールまたはメモリ ルール、および特定の組み込み内部 Bit9 保護によってブロックされたアクションは、このリストには表示されません。
Blocked Files (Banned)（ブロックされたファイル（禁止））	選択した期間中に、明示的に禁止されているために Bit9 エージェントが稼働するコンピューター上でブロックされたすべてのファイルを含むレポートが表示されます。
Blocked Files (Report Only)（ブロックされたファイル（レポートのみ））	選択した期間中に、ブロックされるはずだったが、ファイルを実行したコンピューターのポリシー設定とポリシー適用レベルの組み合わせによって [Report Only（レポートのみ）] 状態になっていたすべてのファイルを含むレポートが表示されます。
Blocked Files (Unapproved)（ブロックされたファイル（未承認））	選択した期間中に、ポリシーの未承認実行可能ファイル設定または未承認のスクリプト設定、およびその適用レベルによってブロックされた、すべての未承認ファイルを含むレポートが表示されます。

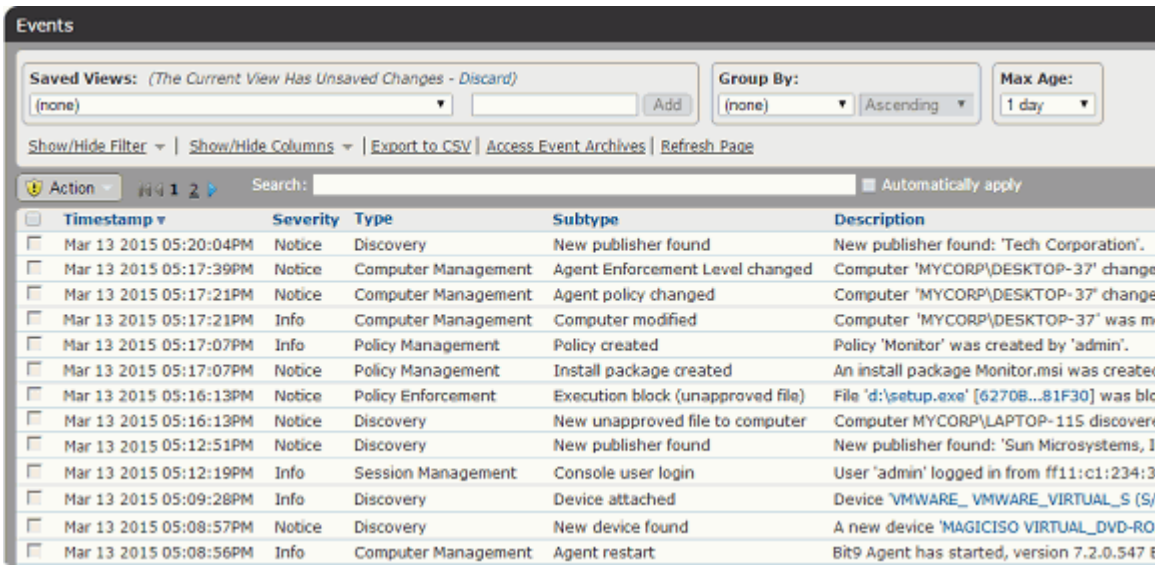
メニュー オプション	説明
Carbon Black	Carbon Black サーバーが Bit9 Server と統合されている場合、Carbon Black サーバーからのすべてのウォッチリスト イベントと Carbon Black センサーからのステータス イベントを含むレポートが表示されます。
Computer Management（コンピューター管理）	Bit9 エージェントが稼働するコンピューターに関連する、選択された期間中のイベント（新しいコンピューターと削除されたコンピューター、エージェントの起動とシャットダウン、別のポリシーに移行されたコンピューター、ポリシー設定または適用レベルの変更、AD ポリシー マッピング ルールの変更（順番の変更を含む）など）を含むレポートが表示されます。
Connectors（コネクター）	ネットワーク セキュリティ コネクター関連のイベント（外部通知、悪意のあるファイルの検出、ファイル分析アクティビティ、コネクター統合の追加、設定、削除など）を示すレポートが表示されます。
Console Access（コンソール アクセス）	選択された期間中のユーザーのログインとログアウト、コンソール ログイン アカウントの作成、編集、削除を含むレポートが表示されます。
Device Control（デバイス制御）	選択された期間中のデバイス関連のイベントを含むレポートが表示されます。これらのイベントには、デバイスの承認、禁止、または承認や禁止の削除、ネットワーク内の新しいデバイスの検出、ネットワーク内のデバイスの接続と接続解除の検出、デバイス関連のポリシー設定の対象になるすべてのデバイス アクセスが含まれます。 **プラットフォームに関する注意**：デバイス制御は Windows コンピューターでのみ有効です。
Duplicate Computer Registrations（コンピューターの重複登録）	同一のエージェント ID で複数のコンピューターを登録しようとする試みに関連するすべてのイベントを含むレポートが表示されます。
File Analysis（ファイル分析）	外部ツールによるファイル分析に関連するすべてのイベントを含むレポートが表示されます。これには、外部通知、ファイル アップロード イベントのほか、悪質または危険な可能性があるファイルに関する Bit9 SRS またはサードパーティ ツールからのレポートが含まれます。
Memory（メモリ）	メモリ（プロセス保護）ルールに関連するすべてのイベントを含むレポートが表示されます。 **プラットフォームに関する注意**：メモリ ルールは Windows システムにのみ影響します。
New Files (All)（新しいファイル（すべて））	選択された期間中にサイト内のコンピューターに現れたすべての新しいファイル（今までファイル カタログに含まれていなかったファイル）を含むレポートが表示されます。

メニュー オプション	説明
New Files (Approved)（新しいファイル（承認済み））	選択された期間中にさまざまな理由で承認されたすべてのファイルのレポートが表示されます。初期化によって承認されたファイルは含まれません。
New Files (Banned)（新しいファイル（禁止））	ネットワークで見つかったすべての新しい禁止ファイルのリストが表示されます。
New Files (Unapproved)（新しいファイル（未承認））	選択された期間中にサーバーで見つかった、承認も禁止もされていないすべての新しいファイルを含むレポートが表示されます。
New Installations（新規インストール）	選択された期間中に、ファイルによって 1 つまたは複数のファイルが書き込まれた（新しいファイル グループを作成した）各インスタンスを含むレポートが表示されます。 **プラットフォームに関する注意**：含まれるのは Windows インストールのみです。
Registry（レジストリ）	Windows レジストリ ルールに関連するすべてのイベントを含むレポートが表示されます。 **プラットフォームに関する注意**：レジストリ ルールは Windows コンピューターにのみ適用されます。
Reputation（レピュテーション）	すべてのレピュテーション関連イベント（レピュテーションに基づいたファイルまたは公開者の承認の追加や削除、ファイルまたは公開者のレピュテーションのプロパティの変更など）を含むレポートが表示されます。
Security Alert Events（セキュリティ アラート イベント）	セキュリティ アラート関連イベントのレポートが表示されます。これらのイベントには、アップグレードが失敗したために Bit9 によって保護されていないエージェント コンピューター、エージェント改ざんの検出または阻止、コンピューターの時計のずれ（セキュリティ対策を阻止するために変更された可能性）が含まれます。
Server Management（サーバー管理）	選択された期間中の [System Configuration（システム構成）] ページのデータ、Bit9 データベース バックアップに関するデータ（成功、失敗、変更）、サーバー エラー データ、Bit9 SRS エラー データ、データベース エラー データ、および Bit9 Server の起動またはシャットダウンのデータへのあらゆる変更を含むレポートが表示されます。
System Health History（システム正常性履歴）	正常性の痕跡の深刻度へのすべての変更、および正常性の痕跡のすべての作成、変更、または検出を含むレポートが表示されます。
Temporary Policy Overrides（一時的なポリシー無効化）	エージェントに対して作成されたすべての一時的なポリシー無効化コードを含むレポートが生成されます。

メニュー オプション	説明
Threat Indicators（脅威の痕跡）	Bit9 が管理するコンピューター上で痕跡セット内の ATI によって検出された脅威が表示されます。有効化された痕跡セットがない場合、このビューは空になります。このイベントおよびその他の脅威関連のイベントのビューの詳細については、第 20 章「高度な脅威検出」を参照してください。
Threat Indicators - Legacy（脅威の痕跡 – 従来）	v7.2.0 以前のリリースでインストールされた ATI によって検出された脅威が表示されます。以前のリリースで Detection Enhancement をインストールしなかった場合、このビューは空になります。
Threat Report - Suspicious executable created by shell（脅威レポート – シェルによって作成された疑わしい実行可能ファイル）	システム ディレクトリ、ごみ箱、AppData などの場所に cmd.exe または powershell.exe によって特定の実行可能ファイルを作成するイベントが表示されます。
Threat Report – Suspicious Files by Location（脅威レポート – 場所が疑わしいファイル）	いずれかのコンピューターの通常とは異なる疑わしい場所で最初にファイルが確認または実行されたイベント、または 1 台以上のコンピューターの通常とは異なる疑わしい場所に最初に（未承認の状態で）ファイルが出現したイベントが表示されます。例としては、ごみ箱での予期しないファイルのアクティビティがあります。
Threat Report - Suspicious Files by Name（脅威レポート – 名前が疑わしいファイル）	いずれかのコンピューターで疑わしい名前のファイルが最初に確認または実行されたイベント、または 1 台以上のコンピューターで最初に（未承認の状態で）疑わしい名前のファイルが出現したイベントが表示されます。多くの場合、名前は正規の Windows ファイルの名前に類似しています。たとえば、svch0st.exe（svchost.exe の 小文字の 'o' の代わりにゼロを使用）という名前のファイルが検出されると、このイベント ビューに表示されます。
Threat Report – Suspicious Files by Parent（脅威レポート – 親が疑わしいファイル）	不明な、または普及度の低い実行可能ファイルが、通常はそれらのファイルを作成しないはずのプログラムによって書き込まれるイベントが表示されます。この例には、Adobe Reader によって作成される実行可能ファイルがあります。多くの場合、このファイルは形式が異常で、悪意のある PDF 形式による攻撃の兆候と考えられます。

既存の Bit9 イベント レポートの表示手順：

1. コンソール メニューで、[**Reports**（レポート）] > [**Events**（イベント）] の順に選択します。[Events（イベント）] ページに、過去 1 時間のすべてのイベントを示すデフォルト ビューが表示されます。



2. [Saved Views（保存済みビュー）] メニューからビューを選択します。選択したビューが表示されます。多くの列や幅が広い列を含むビューでは、イベントのすべてのデータを確認するために左右にスクロールする必要があります。

レポートの変更および保存方法の詳細については、「イベント レポートのカスタマイズ」（598 ページ）を参照してください。

注意

- イベントのテーブルは CSV 形式でダウンロードできます。
- イベントのテーブルまたは説明に IP アドレスが表示されている場合、それはエージェント コンピューターのイベントが報告された時点での IP アドレスで、現在の IP アドレスとは限りません。

イベント テーブルのオブジェクト プレビュー

他のテーブルと同様に、イベントのテーブル内でハイライト表示されている項目は、クリックすると詳細を表示できます。ハイライト表示される項目の多くは、カーソルを上に乗せるとオブジェクト プレビューが表示され、ページから移動しなくてもサマリー情報を確認できます。

イベント レポートでのファイルへのアクションの実行

イベントの詳細からファイルが特定される場合は、[Events（イベント）] ページから直接そのファイルに対してアクションを実行できます。アクションを実行するには、イベント テーブルで該当のイベントの左にあるチェックボックスをオンにし、[Action（アクション）] メニューからアクションを選択します。ボックスをオンにできるのは、ファイル情報を含むイベントのみです。

[Events（イベント）] ページからファイルに対して実行できるアクションは、[Files（ファイル）] ページから実行できる以下のようなアクションと同じです。

- ファイル インスタンスをローカルで承認する、またはローカル承認を削除する
- すべてのコンピューターでグローバルにファイルを承認または禁止する
- 特定のポリシーでコンピューターに適用するカスタム承認または禁止を作成する
- 完全に有効化されていればファイルを「ブロックしていたはず」であることをレポートするのみの、レポートのみの禁止を作成する
- 承認または禁止を削除する
- Bit9 Software Reputation Service (SRS) 情報を取得してファイルを分析する

これらのファイル アクションの詳細については、第 8 章「ソフトウェアの承認と禁止」を参照してください。

Bit9 Connector オプションがインストールされ、ライセンスが付与されている場合は、ファイルをアップロードすることも、サードパーティ製ネットワーク セキュリティ アプライアンスで分析することもできます。詳細については、付録 C、「Bit9 Connector for Network Security Devices」および付録 E、「エージェントからのファイルのアップロード」を参照してください。

イベント レポートのカスタマイズ

[Events（イベント）] ページでは、複数の [Saved Views（保存済みビュー）] を利用できます。どのビューでも、[Show/Hide Filter（フィルターの表示 / 非表示）] および [Show/Hide Columns（列の表示 / 非表示）] ボタンを使用して、特定のプラットフォームのイベントだけを表示するなど、表示をカスタマイズできます。また [Show/Hide（表示 / 非表示）] ボタンは、表示しているテーブルに変更が加えられているかどうかの確認にも使用できます。

一度だけ使用する特別なレポートが必要な場合は、カスタマイズし、結果を確認した後、変更を保存しません。保存されていない変更がある場合は、[Saved Views（保存済みビュー）] メニューの隣に表示されるメッセージで、変更が未保存であることが通知され、変更を破棄するオプションが提供されます。Bit9 コンソールの［Preferences（設定）］ページの［Remember Page Settings（ページ設定の記憶）］の設定によっては、［Events（イベント）］ページから移動して再度戻ったときに、保存していないカスタマイズでフィルターされたビューが表示されます。

カスタム レポートを保存するには、［Saved View（保存済みビュー）］パネルを使用し、既存の保存済みビュー名（組み込み Bit9 レポート以外の場合）、または新しい名前で保存します。

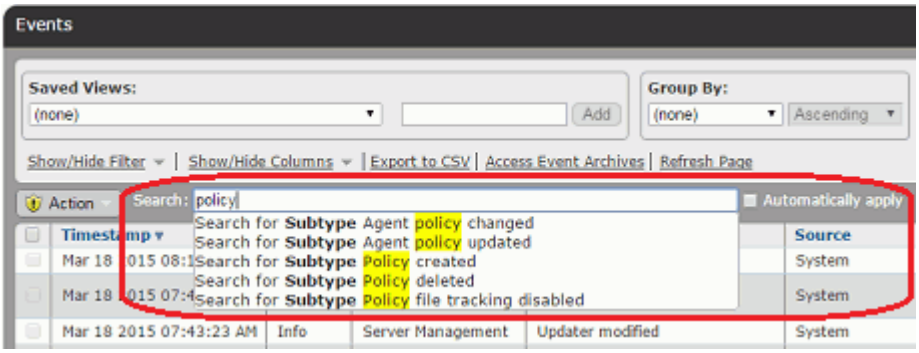
コンソールのテーブルの機能の詳細については、第 2 章「Bit9 コンソールの使用」の「Bit9 コンソールのテーブル」を参照してください。

イベント検索ボックスの使用

［Events（イベント）］ページには、入力した文字列に一致するイベントを迅速に検索できる検索ボックスがあります。検索文字列は、以下のフィールドのデータに対してマッチングされます。

- ［File Hash（ファイル ハッシュ）］
- ［Source（ソース）］
- ［Subtype（サブタイプ）］
- ［Platform（プラットフォーム）］
- ［IP Address（IP アドレス）］

イベント データベース内のこれらのフィールドのデータが文字列と一致する場合、オートコンプリート メニューによってリストが表示され、確認する項目を選択できます。



リストから項目を選択するときに、テーブルは次の 2 つのいずれかの方法でフィルターされます。

- 検索画面に入力する前に［Automatically apply（自動的に適用）］をオンにした場合、メニュー内のオプションをクリックすると即座にテーブルがフィルターされ、適切なフィールドでその文字列に一致するイベントのみが表示されます。
- ［Automatically apply（自動的に適用）］をオンにしていない場合、メニュー内のオプションをクリックすると［Show/Hide Filters（フィルターの表示 / 非表示）］パネルが開きます。ここには、適切なフィールドでその文字列に一致す

るイベントのみを表示するフィルターが設定されています。テーブル ビューに変更を適用する前に、必要に応じて他のフィルターを追加できます。

表 73：イベント レポートのパラメーター

フィールド	説明
[Saved View（保存済みビュー）]	このレポートの名前。 新しいレポートを作成する場合は、[Saved View（保存済みビュー）] の「右」のテキスト ボックスにレポートの目的を示すテキストを入力してから［**Add**（追加）］をクリックします。このレポートは新しい名前で保存され、他のレポートとともに［Saved View（保存済みビュー）］メニューに表示されます。
[Maximum age（最長期間）]	関心のある期間。レポートには、レポートの実行時点までの過去の指定した期間（時間、日、週、月）に発生したイベントが表示されます。選択した値は即座に有効になります。 ［Filters（フィルター）］パネルを使用すると、開始日や終了日に現在の日時以外を使用する［**Timestamp**（タイムスタンプ）］など、期間の設定に関するオプションが増えます。
[Rows per page（ページあたりの行数）]	［Events（イベント）］テーブルの 1 ページに表示されるイベントの最大数。この値は、テーブルの右下の［rows per page（ページあたりの行数）］メニューによってユーザーごとに制御されます。 デフォルトは 25 です。レポートに［rows per page（ページあたりの行数）］設定を超える項目が含まれている場合、コンソールは追加のページと、移動用のページ番号パネルを作成します。
[Group by（グループ別）]	デフォルト表示の結果などをグループ化する基準の列と、並べ替えの順番（昇順または降順）。［Group by（グループ別）］を使用すると、展開可能なリストが作成されます。このリストには、初期状態ではグループ名（セキュリティ ポリシーなど）とグループあたりの項目数のみが表示されますが、グループ名をクリックするとグループのメンバー（コンピューターなど）を表示できます。グループ化にはすべての列名を使用できるわけではありません。

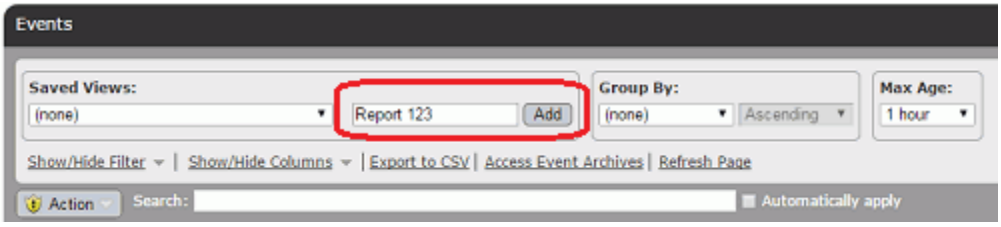
フィールド	説明
[Filters（フィルター）]	レポートに適用するイベント パラメーター。任意のフィルターの組み合わせを指定して、レポートに含めるイベントを決定できます。 フィルターのほとんどは、イベント内のファイルまたはコンピューターと関連していることが明らかなデータのものですが、以下のような特別のケースもあります。 [**Subtype**（サブタイプ）] – すべての Bit9 イベント タイプのイベントのサブカテゴリ。表示する 1 つまたは複数のイベント サブタイプを指定できます。サブタイプが選択されていないとき、コンソールはすべてを検索します。 [**Severity**（深刻度）] – フィルターを使用して、標準の Syslog メッセージ深刻度ガイドラインに基づいてイベントを表示または非表示にできます。カテゴリは以下のとおりです。 [**Critical**（重大）] – 重大な状態 [**Debug**（デバッグ）] – デバッグ レベル メッセージ [**Error**（エラー）] – エラー状態 [**info**（情報）] – 情報メッセージ [**Notice**（通知）] – 正常だが重要な状態 [**Warning**（警告）] – 警告状態 各ログ メッセージの深刻度のステータスは、[Severity（深刻度）] 列に表示されます。 **注意**：以前のリリースでは、現在 [Severity（深刻度）] とラベルされている列とフィルターは「Priority（優先度）」と呼ばれていました。
[Columns（列）]（Show/Hide（表示 / 非表示））	[Events（イベント）] テーブルに列として含める情報。矢印を使用して、表示する列と順番を指定します。 [Selected（選択済み）] リストの項目がテーブルに表示されます。 [Available（使用可能）] リストの項目はテーブルに表示されません。

イベント レポートをカスタマイズして [**Saved View（保存済みビュー）**] として保存する手順：

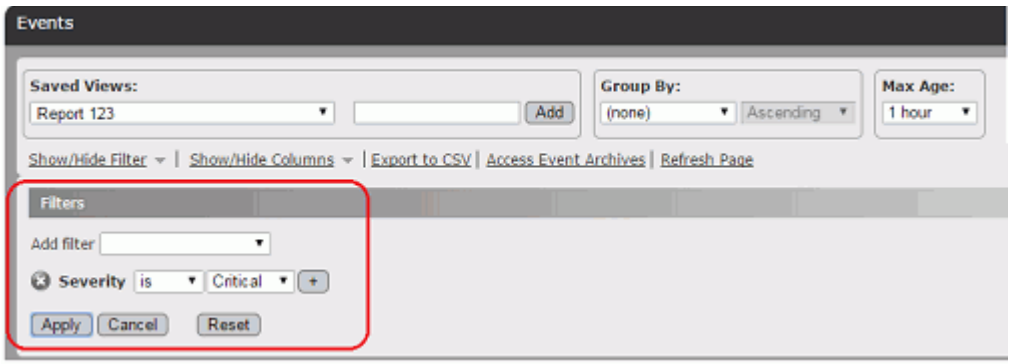
1. コンソール メニューで、[**Reports**（レポート）] > [**Events**（イベント）] を選択します。[Events（イベント）] ページが表示されます。

2. [Saved View（保存済みビュー）] 内に、必要とするレポートに似ている既存レポートがある場合は、[Saved View（保存済みビュー）] メニューからそのレポートを選択します。ない場合は [(**none**（なし）)] を選択します。

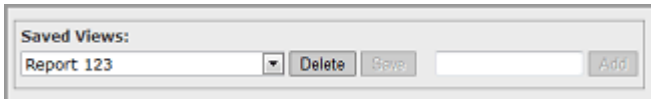
3. [Saved View（保存済みビュー）] パネルの右のボックスをクリックし、レポート名を入力してから [**Add**（追加）] をクリックします。新しいレポートが現在の [Saved View（保存済みビュー）] として表示され、メニューに追加されます。すべての変更を行ってから、新しいビューを作成することもできます。



4. ［**Show/Hide Filters**（フィルターの表示 / 非表示）］リンクをクリックし、1 つまたは複数のフィルターを選択して、レポートのパラメーターを指定します。フィルターは必要な数だけ追加できます。フィルターの設定が完了したら、［**Apply**（適用）］をクリックします。



5. ［**Show/Hide Columns**（列の表示 / 非表示）］リンクをクリックし、矢印ボタンを使用して、レポートに表示するデータのタイプ、および表示する順番を選択します。列の追加と削除が完了したら、［**Apply**（適用）］をクリックします。
6. フィルター設定中にレポートの期間を選択しなかった場合は、［Maximum Age（最長期間）］メニューから期間を選択します。
7. 1 ページに表示する行数を現在の値から変更する場合は、ページ右下の［rows per page（ページあたりの行数）］ドロップダウン メニューを使用します。
8. レポートのデータを縮小および展開可能なグループに配置するには、［Group by（グループ別）］メニューでグループと並び替えの方向（［ascending（昇順）］または［descending（降順）］）を選択します。たとえば、［Group by（グループ別）］として［Policy（ポリシー）］を選択すると、［Events（イベント）］ページでは最初にポリシー名が表示されます。ポリシー名をクリックすると、そのポリシー内のコンピューターのイベントが表示されます。
9. 意図したとおりにレポートの形式を設定したら、そのレポートに使用する名前が［Saved Views（保存済みビュー）］メニューに表示されていることを確認し、［Saved Views（保存済みビュー）］パネルで［Save（保存）］をクリックします。指定した変更が適用されたレポートが保存されます。



イベント レポートの編集

レポートの編集方法はレポートの作成方法に似ていますが、編集では同じレポート名を維持します。

> **注意**
>
> Bit9 Server で提供されている事前定義済みの［Saved Views（保存済みビュー）］は読み取り専用です。これらのビューは、変更して同じ名前で保存することはできません。変更したら別の名前で保存する必要があります。

既存のイベント レポートの編集手順：

1. コンソール メニューで、［**Reports**（レポート）］>［**Events**（イベント）］を選択します。［Events（イベント）］ページが表示されます。
2. ［Saved Views（保存済みビュー）］メニューから、編集するレポートを選択します。レポートが表示されます。
3. レポートに必要なすべての変更を加えたら（表 73、「イベント レポートのパラメーター」 600 ページを参照）、［Save（保存）］ボタンをクリックします。

イベント レポートへのコマンド ライン情報の追加

Bit9エージェントによって生成されたイベントに関連するプロセスのコマンド ライン情報が必要になる場合があります。［Command Line（コマンド ライン）］列はデフォルトの［Event（イベント）］ページ ビューには含まれていませんが、［Show/Hide Columns（列の表示 / 非表示）］パネルを使用して［Event（イベント）］ページに追加することができます。また、コマンド ライン データには Bit9 Live Inventory SDK を通じてアクセスできます。現在コマンド ライン データは、Bit9 Server からの Syslog 出力には含まれていません。

7.2 エージェントによって生成されたイベントに関連するプロセスがある場合、［Command Line（コマンド ライン）］フィールドにはプロセス コマンド ラインの最初の 512 文字が表示されます。7.2.0 以前のエージェントでは、この情報は提供されません。

Subtype	Command Line
Execution block (unapproved file)	"C:\Windows\system32\cmd.exe"
Execution block (unapproved file)	C:\Windows\Explorer.EXE
Execution block (unapproved file)	C:\Windows\SysWOW64\inetsrv\w3wp.exe -ap "DefaultAppPool" -v "v2.0"
File approved (publisher)	"C:\Program Files (x86)\Bit9\Parity Console\php\php-cgi.exe"

［Command Line（コマンド ライン）］には、影響を受けたファイルではなく、アクションを試行したプロセスが表示されます。上記の例では、最初の 2 行はスクリプトの実行がブロックされたことを示しています。最初のケースでは、ユーザーがコマンド プロンプトからスクリプトの実行を試みました。2 番目のケースでは、ユーザーがスクリプトをダブルクリックしました。

通常はイベントを生成しないアクションのコマンド ライン データを取得するには、それらのアクションをレポートするカスタム ルールを追加します。［Add

Custom Rule（カスタム ルールの追加）］ページで、［Rule Type（ルール タイプ）］として［Advanced（高度）］、［Operation（操作）］として［Execute（実行）］（または［Execute and Write（実行と書き込み）］）、［Execute Action（実行アクション）］として［Report Process Create（プロセスの作成をレポート）］を選択します。次に、アクションを開始したプロセスによって作成されるプロセスの［Process（プロセス）］および［Path or File（パスまたはファイル）］情報を入力します。このルールに一致するアクションが発生すると、プロセスの作成時にイベント（コマンド ライン情報を含む）がレポートされます。

重要

- コマンド ライン データには、パスワードなどの機密情報が含まれていることがあります。［Command Line（コマンド ライン）］列がビューに追加されると、この列の見出しはすべてのユーザーに表示されますが、この列内のデータや CSV ファイルにエクスポートされたデータは、特定の権限を持つユーザーにのみ表示されます。「View process command lines（プロセス コマンド ラインの表示）」と呼ばれるこの権限は、デフォルトではどのコンソール ログイン アカウント グループに対しても有効化されていません。この権限は、この情報を必要とするユーザーに対してのみ有効化する必要があります。ユーザー アカウントの権限変更の詳細については、「アカウント グループとアクセス権限」（88 ページ）を参照してください。
- この権限は、Syslog または Live Inventory SDK 出力のイベントには影響しません。これらでは、利用可能な場合は常にコマンド ライン データが含まれます。
- Bit9 エージェント管理コマンドを使用する際は、このフィールドのパスワード データが公開される可能性を考慮する必要があります。これらのコマンドに（「エージェント管理権限の構成」（750 ページ）で説明しているように）パスワードを設定してある場合、1 つの行にコマンドとパスワードを入力すると、パスワードがイベントのコマンド ライン フィールドに含まれることになります。Bit9 は、エージェント管理コマンドを単独で入力し、その後のプロンプトでパスワードを入力することを推奨します。

［Install Event Details（インストール イベントの詳細）］の表示

イベント サブタイプがハイライト表示されている場合、そのイベントには他のイベントが関連付けられています。ハイライト表示されているイベント サブタイプをクリックすると［Install Event Details（インストール イベントの詳細）］レポートが開き、クリックしたイベントに関連付けられているすべてのサブイベントが

（コンピューター別に）表示されます。この詳細レポートは、主にルート イベントとルート イベントによって生成されたイベントの間の「関係」を確認する上で役立ちます。

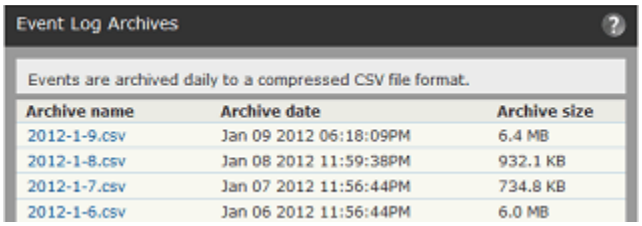
注意

ここでレポートされるのは、ルート インストール「イベント」によって生成された「イベント」です。「インストーラー」によって「インストールされたファイル」ではありません。ファイルのインストール時にイベントが生成されるかどうかは、インストーラーの承認ステータスによって決まります。ファイルがインストールされるコンピューターのセキュリティ ポリシーや、ファイルの追跡を除外できるその他のルールと設定にも影響を受けることがあります。イベントには、プロセス名、プロセスを実行中のユーザーなどの情報が含まれます。

承認済みインストーラーは、ローカルで承認されたファイルを生成します。承認されたファイルは［Install Event Details（インストール イベントの詳細）］ページにサブイベントを生成しません。「未承認」インストーラーは（以前に他の手段で承認されていない限り）未承認ファイルを生成し、未承認ファイルはサブイベントを生成します。また、新たにインストールされてブロックされたファイルも［Install Event Details（インストール イベントの詳細）］にサブイベントを生成します。

イベント アーカイブの表示

［Events（イベント）］ページの［**Access Event Archives**（イベント アーカイブにアクセス）］リンクをクリックすると、Bit9 イベントの日次アーカイブのテーブルが開きます。これらのイベントは、CSV ファイルにアーカイブされています。



この CSV ファイル名をクリックし、ダイアログ ボックスから実行するアクションを選択すると、任意の日付のイベント アーカイブを開いたりダウンロードしたりすることができます。これらのアーカイブは、Bit9 Server インストール ディレクトリの「archivelogs」フォルダーに保存されています。

［Events（イベント）］ページに戻るには、コンソール メニューで［**Reports**（レポート）］>［**Events**（イベント）］を選択します。

注意

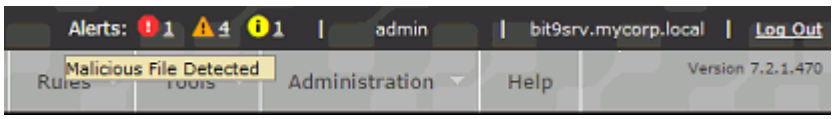
- アーカイブは、［System Configuration（システム構成）］ページの［Events（イベント）］タブで有効化または無効化できます。詳細については、「Bit9 イベント データベースの管理」（754 ページ）を参照してください。
- Bit9 コンソールのイベント時間とは異なり、CSV ファイル内で示されるアーカイブ イベントのタイムスタンプは UTC 時間で表示されます。

Bit9 アラートの使用

アラートは、コンピューターへのリスクの高いファイルの出現や拡散など、Bit9 が監視する重要なアクティビティを通知します。アラートに指定した条件が満たされた場合は、以下の方法で通知を提供できます。

- **コンソール バナーでの通知** – アラートがトリガーされると、すべてのコンソール ページのコンソール メニューの右上にインジケーターが表示されます。バナーに表示される記号は 3 つあり、それぞれが異なるアラート優先度を示しています。記号の右には、各カテゴリでトリガーされているアラートの数が表示されます。優先度の詳細については、「アラートの優先度」（619 ページ）を参照してください。

  記号または数字の上にマウス カーソルを移動すると、アラートのタイプを説明するツールチップ（その優先度のアラートが 1 つのみの場合）またはその優先度が表示されます。記号または数字をクリックすると、その優先度レベルでトリガーされているアラートが 1 つの場合は［Alert Instances（アラート インスタンス）］ページが開き、複数の場合はこれらのアラートが表示されるようにフィルターされた［Alerts（アラート）］ページが開きます。



- **E メール通知** – アラートをトリガーしたイベントに関する E メール通知が一連のサブスクライバーに送信されます。
- **［Alerts（アラート）］ページの行のハイライト表示** – ［Alerts（アラート）］ページで、トリガーされている各アラートの行がハイライト表示されます。ハイライト表示の色はアラートの優先度（高は赤、中はオレンジ、低は黄色）を示します。
- **［Home Page（ホームページ）］とその他のダッシュボード** – 現在トリガーされているすべてのアラートは、デフォルトの Bit9 コンソール［Home Page（ホームページ）］に含まれる［Triggered Bit9 Alerts（トリガーされた Bit9 アラート）］ポートレットに表示されます。このポートレットは他のダッシュボードにも追加できます。またこのポートレットは、色と記号を使用してアラートの優先度を表します。

アラートの通知が不要になったときは、そのアラートを「リセット」できます。アラートをリセットすると、[Alerts（アラート）] ページと [Home Page（ホームページ）]（および [Triggered Bit9 Alerts（トリガーされた Bit9 アラート）] ポートレットが含まれるすべてのダッシュボード）の警告バナーが削除されます。また、アラート E メールの自動再送信を有効化している場合は、その送信が停止されます。そのアラートのトリガー条件が再度発生すると、新たなアラートがトリガーされます。アラートを発生させる条件が消滅した場合、そのアラートは非トリガー状態に自動リセットされます（詳細については、「アラートのトリガー方法」（620 ページ）を参照してください）。

アラート履歴はアラートごとに保持され、この履歴はアラートがトリガーおよびリセットされると更新されます。

注意

アラート機能へのアクセス権は、[Login Accounts（ログイン アカウント）] の [Add/Edit Group（グループの追加 / 削除）] ページの「View alerts（アラートの表示）」および「Manage Alerts（アラートの管理）」権限によって決定されます。

Bit9 アラートには、2 つの最上位クラスがあります。

- **組み込みアラート** – 表 74 に、コンソールにデフォルトで表示される事前設定済みアラートを示します。
- **ユーザー作成アラート** – [Alerts（アラート）] ページでアラートを作成および編集できます。方法については、「アラートの作成」（611 ページ）を参照してください。

[Alerts（アラート）] ページには、組み込みアラートとユーザー作成アラートを含む現在利用可能なすべてのアラート（有効化されているものと無効化されているものの両方）のリストが表示されます。

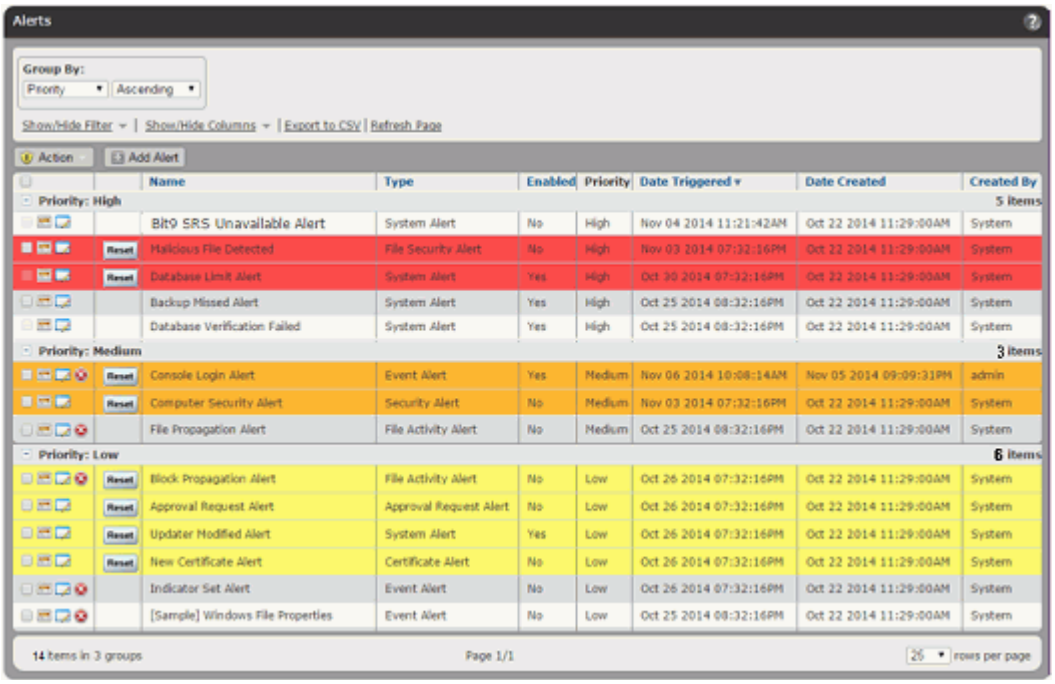


表 74：組み込みアラート

アラート	説明
Database Limit Alert（データベース上限アラート）	SQL Expressデータベースのサイズが指定された上限を超えた場合に、サブスクライバーにアラートを送信します（上限はSQL のエディションによって異なります）。（完全な SQL バージョンでなく）SQL Server Express エディションをインストールしてある場合にのみ有効です。常に有効です（無効化できません）。
Backup Missed Alert（バックアップ失敗アラート）	スケジュールされていたバックアップが失敗したときにサブスクライバーにアラートを送信します。デフォルトで有効化されていますが、無効化できます。
Database Verification Failed（データベース検証失敗）	Bit9 データベースの破損が見つかったときにサブスクライバーにアラートを送信します。トリガーされた場合は、Bit9 サポートにご連絡ください。常に有効です（無効化できません）。
Potential Risk File Detected（危険な可能性があるファイルの検出）	Bit9 エージェントによって監視されるコンピューター上のファイルが、Bit9 SRS によって、または接続されているセキュリティ デバイスやサービスによって悪意のあるファイルである可能性があると判断されたときに、サブスクライバーにアラートを送信します。デフォルトでは無効化されています。
Malicious File Detected（悪意のあるファイルの検出）	Bit9 エージェントによって監視されるコンピューター上のファイルが、Bit9 SRS によって、または接続されているセキュリティ デバイスやサービスによって悪意のあるファイルであると判断されたときに、サブスクライバーにアラートを送信します。禁止ファイルや承認済みファイルは無視するように設定できます。デフォルトでは無効化されています。
Elevated Privilege: Install Mode（権限昇格 : インストール モード）	任意のコンピューターで、ローカル承認モードが指定を超える期間継続されると、サブスクライバーにアラートを送信します。デフォルトは 1 時間ですが、変更できます。すべてのコンピューターは、ソフトウェアのインストールに必要な時間を超えて承認モードを継続させないようにする必要があります。
Bit9 Software Reputation Service Unavailable Alert（Bit9 Software Reputation Service使用不能アラート）	アラートで指定された期間中に、予定されていた Bit9 SRS タスクが実行されなかったときに、サブスクライバーにアラートを送信します。デフォルトの期間は 3 時間ですが、変更できます。Bit9 SRS が有効化されている場合は、デフォルトで有効化されています（無効化できません）。Bit9 SRS が有効化されていない場合は無効です。 このアラートは、一度トリガーされると、Bit9 SRS のすべての標準的なタスクが通常の動作に復元されるまで有効のままです。手動でリセットできますが、アラートを発生させた条件が解消していない場合は、指定された時間の経過後に再度トリガーされます。 また、このアラートを発生させた条件により、[System Configuration（システム構成）] の [Licensing（ライセンス）] ページには Bit9 SRS が利用できないという通知が追加されます。

アラート	説明
Approval Request Alert（承認要求アラート）	指定された数を超える承認要求が［Submitted（送信済み）］または［Open（オープン）］状態のときに、サブスクライバーにアラートを送信します。このアラートがトリガーされる際、1 週間以上経過した要求とクローズされた要求は考慮されません。このアラートは、一度トリガーされると、手動でリセットされるか、十分な数の要求がクローズされてオープン状態の要求の合計がしきい値を下回るまで有効のままです。デフォルトで有効化されています。
Justification Alert（根拠アラート）	エンドポイント ユーザーが実行の許可を求めて作成した根拠が、指定された数を超えたときに、サブスクライバーにアラートを送信します。このアラートがトリガーされる際、1 週間以上経過した根拠は考慮されません。このアラートは、一度トリガーされると、手動でリセットされるか、十分な数の根拠がクローズされて合計数がしきい値を下回るまで有効のままです。デフォルトで有効化されています。
Updater Modified Alert（アップデーター変更アラート）	Bit9 SRS によってアップデーターが作成、変更、または削除されると、サブスクライバーにアラートを送信します。常に有効です（無効化できません）。 **注意**：［System　Configuration（システム構成）］ページの［Advanced Options（高度なオプション）］タブで、Bit9 SRS による自動アップデーター管理を有効にしておく必要があります。
Computer Security Alert（コンピューター セキュリティ アラート）	コンピューター上で疑わしい動作が検出されると、サブスクライバーにアラートを送信します。トリガーを発生させる条件には、アップグレード障害のために保護されていないコンピューターの検出、エージェントの改ざんの検出または阻止、Bit9 Server とのコンピューター クロックの非同期などがあります。常に有効です（無効化できません）。 これらのアラートと、その原因となる条件の詳細については、「［Computer Security Alerts（コンピューター セキュリティ アラート）］でのエージェントの問題の検出」（628 ページ）を参照してください。

アラート	説明
New Certificate Alert（新しい証明書アラート）	Bit9 コンソールにまだリストされていない公開者の証明書を含むファイルが検出されるか、Bit9 Server に新しい証明書が直接インポートされたときに、サブスクライバーにアラートを送信します。デフォルトでは、このアラートはすべての公開者の新しい証明書が検出されたときにトリガーされます。ただし、特定の公開者の新しい証明書に対してのみトリガーするように設定できます。 特定の公開者に対して設定する場合は、アラートを発生させる公開者の名前のすべてまたは一部に一致する文字列を指定する必要があります。たとえば、文字列として「Apple」を指定すると、「Apple」、「Apple, Inc.」、「Big Apple, Ltd.」などと識別される公開者の新しい証明書についてアラートが送信されます。 アラートには、複数の公開者（または名前の一部）を追加できます。 このアラートを使用するには、v7.0.1 以上のエージェントが必要です。デフォルトでは無効化されています。
Revoked Certificate Alert（証明書取り消しアラート）	この Bit9 Server で把握されている証明書が取り消されたときに、サブスクライバーにアラートを送信します。デフォルトでは、このアラートは「いずれかの」公開者の証明書が取り消されたときにトリガーされます。ただし、特定の公開者の証明書に対してのみトリガーするように設定できます。 特定の公開者に対して設定する場合は、アラートを発生させる公開者の名前のすべてまたは一部に一致する文字列を指定する必要があります。たとえば、文字列として「Apple」を指定すると、「Apple」、「Apple, Inc.」、「Big Apple, Ltd.」などと識別される公開者の証明書の取り消しについてアラートが送信されます。 アラートには、複数の公開者（または名前の一部）を追加できます。 このアラートを使用するには、v7.0.1 以上のエージェントが必要です。デフォルトでは無効化されています。
Indicator Set Alert（痕跡セット アラート）	検出の痕跡セットが作成、更新、または削除されたときに、サブスクライバーにアラートを送信します。
System Health OER Alert（システム正常性 OER アラート）	このサーバーの環境がBit9 Platform運用環境の要件に従っていないときに、サブスクライバーにアラートを送信します。この状況は、パフォーマンスの問題が直ちに、または潜在的に発生する可能性を示しています。 **注意**：このアラートは、［System Configuration（システム構成）］ページの［Advanced（高度）］タブで、システム正常性の痕跡が有効化され、この痕跡がサーバーにダウンロードされている場合にのみ表示およびトリガーできます。痕跡が存在する場合、常に有効です。

アラート	説明
System Health Infrastructure Configuration Alert（システム正常性インフラストラクチャ構成アラート）	サーバー環境の条件によって［System Health（システム正常性）］ページの［Infrastructure Configuration（インフラストラクチャ構成）］タブの正常性の痕跡がトリガーされたときに、サブスクライバーにアラートを送信します。 **注意**：このアラートは、［System Configuration（システム構成）］ページの［Advanced（高度）］タブで、システム正常性の痕跡が有効化され、この痕跡がサーバーにダウンロードされている場合にのみ表示およびトリガーできます。痕跡が存在する場合、常に有効です。
[Sample] Windows File Properties（[サンプル] Windows ファイル プロパティ）	「書き込みのレポート」（カスタム ルール）が発生し、脅威検出のための Windows ファイル プロパティ痕跡セットがトリガーされたときに、サブスクライバーにアラートを送信します。 デフォルトでは無効化されています。

アラートの作成

アラートは、次のタイプのものを作成および構成できます。

表 75：ユーザーが作成可能なアラートのタイプ

アラートのタイプ	説明
File Activity: Propagating File（ファイル アクティビティ：ファイルの増殖）	指定された期間中に、「ローカルで未承認」のファイルがポリシーで設定されている割合を超えるコンピューターに出現すると、サブスクライバーにアラートを送信します。高適用レベルで運用していない場合は、ファイルの増殖はウイルスの拡散を示している可能性があります。
File Activity: Blocked File（ファイル アクティビティ：ファイルのブロック）	指定された期間中に、同一のファイルがポリシーで設定されている割合を超えるコンピューターでブロックされたときに、サブスクライバーにアラートを送信します。
Baseline Drift Alert（ベースライン ドリフト アラート）	ファイルのベースライン ドリフトが指定されたしきい値に達すると、サブスクライバーにアラートを送信します。
File Prevalence Alert（ファイル普及度アラート）	指定された数を超えるコンピューターに「指定された」ファイルが存在するときに、サブスクライバーにアラートを送信します。
Event Alert（イベント アラート）	指定されたイベントが発生したとき、または指定されたイベント ルールが指定された期間中にしきい値を超える回数発生したときに、サブスクライバーにアラートを送信します。

アラートの作成手順：

1. コンソール メニューで、[**Tools**（ツール）] > [**Alerts**（アラート）] を選択します。[Alerts（アラート）] ページに、現在使用可能なすべてのアラート（有効化されているものと無効化されているものの両方）のリストが表示されます。

2. [Alerts（アラート）] ページで、[**Add Alert**（アラートの追加）] ボタンをクリックします。[Alert Information（アラート情報）] ページが表示されます。

3. [Alert Information（アラート情報）] パネルで、必要な情報を入力します。指定可能なパラメーターの詳細については、以下の表 76 を参照してください。

4. すべてのアラート パラメーターの入力が終了したら、[**Create**（作成）] をクリックして新しいアラートを作成し、このページに留まるか、[**Create & Exit**（作成して終了）] をクリックしてアラートのテーブルに戻ります。このアラートにサブスクライバーを追加するときは、[Create（作成）] を使用します。

   作成された新しいアラートは、[Alerts（アラート）] ページに表示されます。アラートは、有効化されるとネットワーク上でアクティビティの監視を開始し、設定された定義に一致する条件を発見するとトリガーされます。

表 76：アラートのパラメーター

セクション	フィールド	説明
[General（一般）]	**[Alert name（アラート名）]**	[Alert（アラート）] テーブルに表示されるアラート名。
	[Message（メッセージ）]	アラートのトリガー時に送信されるメッセージ。イベント アラート用のメッセージにタグを追加することにより、そのアラート インスタンスに固有のデータを提供できます。「イベント アラート メッセージ用の情報タグ」（617 ページ）を参照してください。
	[Priority（優先度）]	このアラートに割り当てる優先度。選択肢は、[High（高）]、[Medium（中）]、[Low（低）] です。優先度によって、ユーザー インターフェイスでアラートに割り当てられる色が決まります。また、優先度によってアラートをグループ化し、最も重大な項目をハイライト表示できます。
	[Status（ステータス）]	アラートを有効化（オン）するか無効化（オフ）するかを指定します。アラートがトリガーされた後に無効化しても、アラートは自動的にリセットされません。
[Type（タイプ）]	**[Type（タイプ）]**	構成するアラートのタイプ。 • File Activity: Propagating File（ファイル アクティビティ：ファイルの増殖） • File Activity: Blocked File（ファイル アクティビティ：ファイルのブロック） • Baseline Drift Alert（ベースライン ドリフト アラート） • File Prevalance Alert（ファイル普及度アラート） • Event Alert（イベント アラート）
	[Description（説明）]	指定されたアラート タイプを詳しく説明する読み取り専用テキスト。

セクション	フィールド	説明
	[Mail Template（メール テンプレート）]	このアラートのサブスクライバーに送信する E メールの形式と内容を決定するために使用するテンプレート。デフォルト テンプレートはあらゆるアラートに使用できますが、各タイプのアラートに合わせた他の標準テンプレートも用意されています。 • Default（デフォルト） • Template for File（ファイル用テンプレート） • Template for Elevated Privilege（権限昇格用テンプレート） • Template for Approval（承認用テンプレート） また、必要に応じてカスタム テンプレートを作成できます。カスタム テンプレートを作成する場合は、Bit9 テクニカル サポートにお問い合わせください。
[Criteria（条件）]：File Activity/ Prevalence alerts（ファイル アクティビティ / 普及度アラート）	**[Threshold（しきい値）]**	アラートのトリガーに必要な、影響を受けたコンピューターのしきい値。アラート タイプに適用される場合にのみ表示されます。この値は、割合または実際の数値です。
[Criteria（条件）]：File Activity alerts（ファイル アクティビティ アラート）	**[Time Period（期間）]**	アラートのトリガーのために、アクティビティが発生する必要がある最低期間。アラート タイプに適用される場合にのみ表示されます。
[Criteria（条件）]：Baseline Drift alerts（ベースライン ドリフト アラート）	**[Drift Report（ドリフト レポート）]**	アラートをトリガーするために分析するデータが含まれるドリフト レポートの名前。アラート タイプに適用される場合にのみ表示されます。
	[Alert When（アラートのタイミング）]	測定するドリフト パラメーターと、アラートをトリガーするしきい値。アラート タイプに適用される場合にのみ表示されます。

セクション	フィールド	説明
[Criteria（条件）]：File Prevalence alerts（ファイル普及度アラート）	**[Specify File By（ファイルの指定基準）]**	ファイルを識別する基準。選択肢は［Hash（ハッシュ）］と［Filename（ファイル名）］です。
	[File Name（ファイル名）]	アラートのために監視するファイルの名前。［Specify File By（ファイルの指定基準）］として［Filename（ファイル名）］を選択している場合にのみ表示されます。 **注意**：普及度アラートのファイル名にワイルドカードは使用できません。
	[Publisher Contains（公開者を含む）]（オプション）	ファイルのソースとして特定されている公開者の名前（特定されている場合）。［Specify File By（ファイルの指定基準）］として［Filename（ファイル名）］を選択している場合にのみ表示されます。
	[Hash Type（ハッシュ タイプ）]	ファイルの特定に使用するハッシュのタイプ（MD5、SHA-1、または SHA-256）。［Specify File By（ファイルの指定基準）］として［Hash（ハッシュ）］を選択している場合にのみ表示されます。
	[Hash Value（ハッシュ値）]	ファイルのハッシュ値。［Specify File By（ファイルの指定基準）］の値のタイプとして［Hash（ハッシュ）］を選択している場合にのみ表示されます。
[Criteria（条件）]：Event Alerts（イベントアラート）	**[Threshold（しきい値）]**	アラートをトリガーするために、指定された期間中にイベントまたはイベント ルールがこのルールで定義されているプロパティに一致する必要がある回数。
	[Time Period（期間）]	アラートのトリガーのために、このルールに定義された条件が満たされる必要がある期間。
	[Trigger On（トリガー基準）]	アラートを［Event(s)（イベント）］によってトリガーするか［Event Rule（イベント ルール）］によってトリガーするかを指定します。
	[Select Event Properties（イベント プロパティの選択）]	イベントによるトリガーを選択した場合、このアラートをトリガーするイベントのプロパティ。以下のプロパティがあります。 • ［Subtype（サブタイプ）］– イベントによってトリガーされるルール セットには、少なくとも 1 つのサブタイプを含める必要があります。複数のサブタイプを含めることができます。 • その他のプロパティ – ［Add filter（フィルターの追加）］メニューに、アラートをトリガーする条件を絞り込んで指定するために追加できるその他のイベント パラメーターがあります。

セクション	フィールド	説明
	[Select File Properties（ファイル プロパティの選択）]	イベントによるトリガーを選択した場合、イベントに関連するファイルがアラートをトリガーするために満たす必要があるプロパティをオプションで追加できます。ファイルのプロパティを指定する必要はありませんが、指定した場合は、そのプロパティがルールに一致しないとき、またはイベントでそのプロパティの値が利用できないとき、アラートはトリガーされません。
	[Select Process Properties（プロセス プロパティの選択）]	イベントによるトリガーを選択した場合、ファイル プロパティで指定されたファイルの親プロセスが、このアラートをトリガーするために満たす必要があるプロパティをオプションで追加できます。プロセスのプロパティを指定する必要はありませんが、指定した場合は、そのプロパティがルールに一致しないとき、またはイベントでそのプロパティの値が利用できないとき、アラートはトリガーされません。
	[Event Rule（イベント ルール）]	イベント ルールによるトリガーを選択した場合、[Event Rule（イベント ルール）] メニューに既存のルールのリストが表示されます。
[Policies（ポリシー）] （適切なアラート タイプに対してのみ表示）	**[Rule Applies To（ルールの適用先）]**	ラジオ ボタンをクリックして、このアラートを [All policies（すべてのポリシー）] または [Selected policies（選択済みポリシー）] に対して有効化します。 [Selected policies（選択済みポリシー）] の場合は、アラートを有効化する各ポリシーの隣のチェックボックスをオンにします。
	[Selected（選択済み）]	このアラートの対象になるポリシー。 ポリシーを選択し、矢印ボタンを使用して適切な列に移動します。

セクション	フィールド	説明
[Subscribers（サブスクライバー）]	**[Email（E メール）]**	**注意**：サブスクライバーは、アラートが作成されるまで追加できません（このフィールドは表示されません）。 アラート通知を送信するEメール アドレスを追加します。[Email address（E メール アドレス）] ボックスにアドレスを 1 件入力するたびに［Add（追加）］ボタンをクリックして、サブスクライバー リストを作成します。[Add（追加）] ボタンは、有効なEメール アドレスを入力すると有効になります。 アドレス ボックスの右のドロップダウン メニューで、通知 E メールの形式を指定します。選択肢は、[text（テキスト）]、[HTML]、[Auto（オート）] です。[Auto（オート）] を選択すると、受信者のメール サーバーによって形式が決定されます。
[Reminder Mail（リマインダー メール）]	**[Status（ステータス）]**	[Reminder Mail（リマインダー メール）] の [Status（ステータス）] では、指定期間の経過後にアラートがリセットされていない場合に、アラート E メールを再送信するかどうかを決定します。選択肢は、[Enabled（有効）] または［Disabled（無効）］です。
	[Remind Every（リマインド間隔）]	[Reminder Mail（リマインダー メール）] が有効な場合に、リセットされていないアラートに対するアラート E メール再送信の間隔。
[Auto Reset（自動リセット）]	**[Status（ステータス）]**	[Auto Reset（自動リセット）] では、指定した期間の経過後、または一部のアラートについて、トリガーした条件が有効でなくなったときにアラートを自動的にリセットするかどうかを決定します。[Enabled（有効）] に設定すると、アラートを自動リセットできます。[Disabled（無効）] に設定した場合は、アラートを手動でリセットする必要があります。
	[Reset After（リセットまでの期間）]	[Auto Reset（自動リセット）] が有効な場合、別の理由によってアラートがリセットされていないときに、トリガーされたアラート インスタンスを自動リセットするまでの期間を決定します。デフォルト値は 4 週間です。この値は別の期間に変更できます（単位は分から週）。

イベント アラート メッセージ用の情報タグ

アラート メッセージでは、アラートをトリガーした条件に関する追加情報を提供できます。イベント アラートの場合は、メッセージにタグを追加し、アラート インスタンスに固有のデータを提供できます。表 77 に、利用可能なタグを示します。

表 77：イベント アラート メッセージ用の情報タグ

タグ	説明
<FileName>	アラートを開始したイベントから取得したファイル名。複数のファイルがアラートを引き起こした場合は、コンマ区切りリストになります。
<Sha256>	アラートを開始したイベントから取得したファイルの SHA-256 ハッシュ。複数のファイルがアラートを引き起こした場合は、コンマ区切りリストになります。
<Md5>	アラートを開始したイベントから取得したファイルの MD5 ハッシュ。複数のファイルがアラートを引き起こした場合は、コンマ区切りリストになります。
<Sha1>	アラートを開始したイベントから取得したファイルの SHA-1 ハッシュ。複数のファイルがアラートを引き起こした場合は、コンマ区切りリストになります。
<RootSha256>	アラートを開始したイベントから取得したファイルの Root SHA-256 ハッシュ。複数のファイルがアラートを引き起こした場合は、コンマ区切りリストになります。
<HostName>	アラートを開始したイベントから取得したコンピューター名。複数のコンピューターがアラートを引き起こした場合は、コンマ区切りリストになります。
<UserName>	アラートを開始したイベントから取得したユーザー名。複数のユーザーがアラートを引き起こした場合は、コンマ区切りリストになります。
<EventRuleName>	イベント ルールによってアラートが開始された場合は、ルール名。
<EventRuleDescription>	イベント ルールによってアラートが開始された場合は、ルールの説明。
<EventSubtype>	アラートを開始したイベントのサブタイプ。複数のイベントがアラートを引き起こした場合は、コンマ区切りリストになります。
<EventDescription>	アラートを開始したイベントから取得した説明フィールド。
<AntibodyId>	アラートを開始したイベントから取得したファイルの ID。複数のイベントがアラートを引き起こした場合は、コンマ区切りリストになります。
<HostId>	アラートを開始したイベントから取得したホストの ID。複数のイベントがアラートを引き起こした場合は、コンマ区切りリストになります。

アラートの編集

アラートは、しきい値、期間、サブスクライバー、その他のパラメーターを変更するために変更が必要になる場合があります。アラートの有効化または無効化が

必要なこともあります。これらの操作は、[Alert Information（アラート情報）] ページで行うことができます。

アラートの編集、有効化、無効化の手順：

1. [Alerts（アラート）] ページを開いていない場合は、Bit9 コンソール メニューで [**Alerts**（アラート）] をクリックします。
2. 変更するアラートの隣にある [View Details（詳細の表示）]（鉛筆とファイル）ボタンをクリックします。[Alert Information（アラート情報）] ページが表示されます。
3. アラートの有効化または無効化のみを行う場合は、[Alert Information（アラート情報）] パネルの [General（一般）] セクションの適切なボタンをクリックし、ページ下部の [**Save**（保存）] ボタンをクリックします。
4. 他の変更も行う場合は、適切なパラメーターを編集し（表 76 を参照）、[**Save**（保存）] ボタンをクリックします。アラートが更新され、[Alerts（アラート）] ページに戻ります。

組み込みアラートの新しいインスタンスは作成できませんが、一部の設定は編集できます。たとえば、承認要求アラートのトリガーに必要な承認要求数を変更することができます。また、アップデーター変更アラートをトリガーするアクション（作成、編集、削除）も変更できます。

アラートの優先度

各 Bit9 アラートには、優先度（高、中、または低）が割り当てられています。アラートの優先度によって、コンソール バナーとダッシュボードでのアラート アイコンの形と色、および [Alerts（アラート）] ページでのトリガーされたアラートの行に使用される色が決まります。

表 78：アラートの優先度

アラートの優先度	アイコン	行の色
高		**赤**
中		**オレンジ**
低		**黄色**

アラート優先度は、アラートごとの重要性の違いを視覚的に表すだけでなく、[Alerts（アラート）] ページでのグループ化にも利用できます。グループ化を行うと、最も重要性の高いアラートに最初に注意が向きやすくなります。[Group by（グループ別）] メニューで [Priority（優先度）] を選択すると、アラートはまず [Priority（優先度）]、次に [Date Triggered（トリガー日）] によって降順で並び替えられます。

システム アラートには、変更不可能な優先度が事前に定義されています。

- Database Limit Alert（データベース上限アラート）– 高

- Database Verification Alert（データベース検証アラート）– 高
- Bit9 SRS Unavailable Alert（Bit9 SRS 使用不能アラート）– 高

他のアラートに関しては、[Alerts（アラート）] ページの [Action（アクション）] メニュー、または [Add/Edit Alert（アラートの追加 / 編集）] ページの [Priority（優先度）] メニューを使用して優先度を変更できます。

アラートの削除

アラートを削除するときは、アラートの定義を削除し、そのアラートで実施していたすべての監視を終了します。また、現在は有効化しないものの将来使用する可能性があるアラートの場合は、無効化することもできます。Bit9 Server が提供する事前定義アラートの一部は削除できません。これらのアラートには [Delete（削除）] ボタンがありません。

アラートの削除手順：

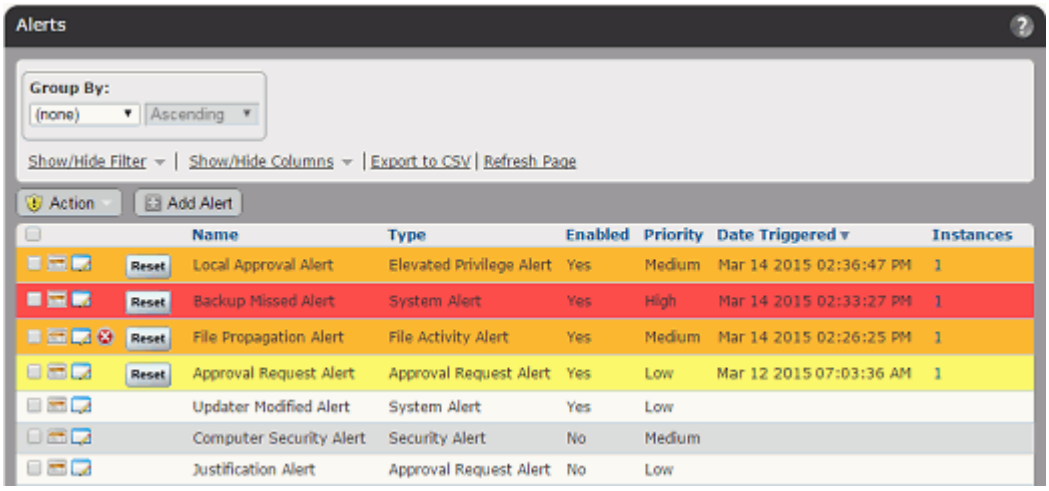
1. [Alerts（アラート）] ページで、削除するアラートの名前の隣にある [Delete（削除）] (x) ボタンをクリックします。
2. 確認のダイアログ ボックスで [**Yes**（はい）] をクリックします。

アラートのトリガー方法

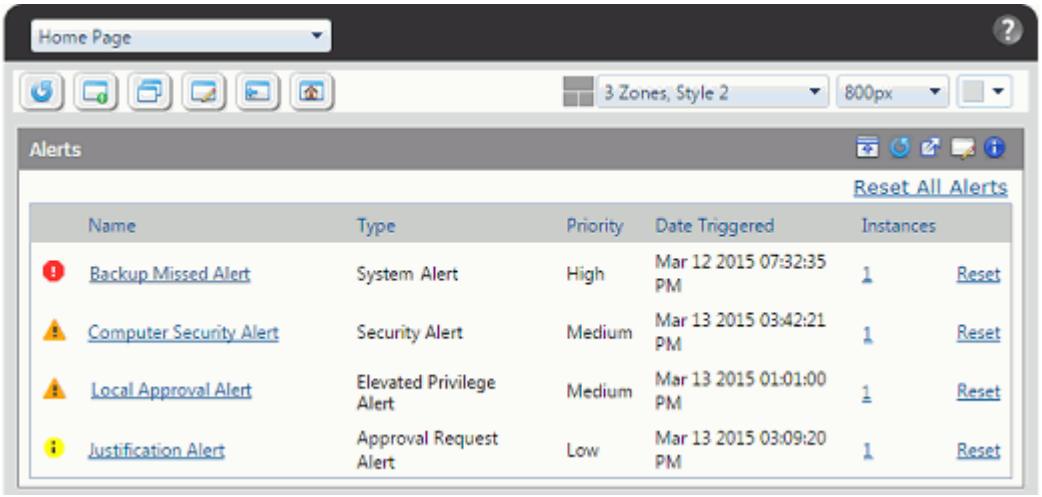
組み込みアラートも作成したアラートも、[Alerts（アラート）] ページに表示されるアラートはすべて、1 つの「アラート クラス」と考えることができます。アラート クラスのトリガー条件を満たす状況が発生するたびに、「アラート インスタンス」が発生します。一部のアラート クラスでは、発生可能なインスタンスは 1 つのみです。たとえば、Bit9 Server 用のデータベースは 1 つだけなので、Bit9 データベース制限アラートでは一度に 1 つのインスタンスしか発生しません。その他のクラスは、同時に多くのインスタンスが発生する可能性があります。たとえば、1 つのネットワーク内に複数の悪意のあるファイルが存在することも考えられるため、複数の悪質ファイル検出アラート インスタンスが発生する可能性があります。

アラート クラスのトリガーされたインスタンスが存在する場合、そのアラートは [Alerts（アラート）] ページで色別の深刻度レベルを使用してハイライト表示され、アラート名の隣に [Reset（リセット）] ボタンが追加されます。[Date Triggered（トリガー日）] 列にはアラートがトリガーされた日時が表示され、[Instances（インスタンス）] 列にはトリガーされているインスタンスの数と [Alert Instances（アラート インスタンス）] ページへのリンクが表示されます。デフォルトでは、トリガーされているアラートはこのページ上部に表示され、トリガー日時の降順に並んでいます。

コンソール ログイン セッション中は、コンソールに各アラート「インスタンス」の新しいバナーは表示されませんが、インスタンス数は表示されます。以下に示すトリガーされたアラートのビューは、グループ化されず、[Date Triggered（トリガー日）] によって並び替えられています。



また、トリガーされたアラートは、デフォルト［Home Page（ホーム ページ）］に含まれる［Alerts（アラート）］ポートレットにも表示され、トリガーされたアラートの数はコンソール バナーに表示されます。

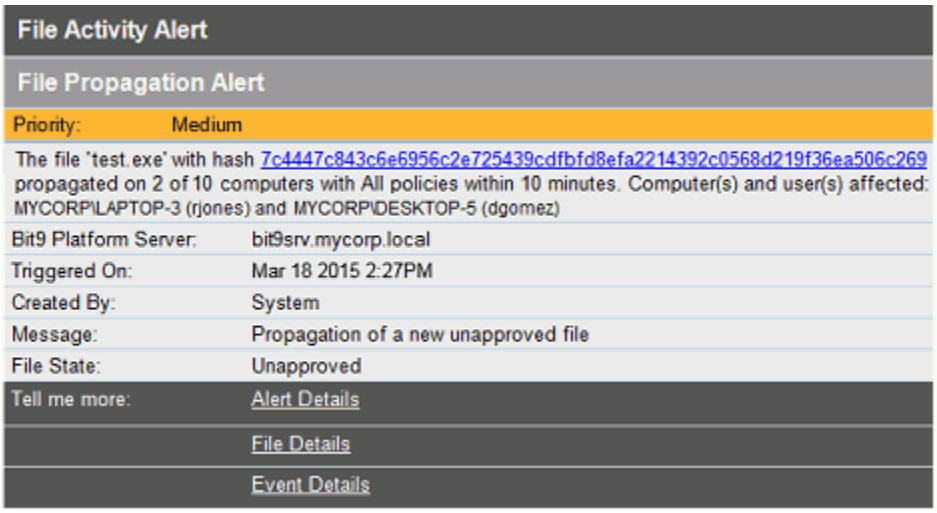


トリガーされたアラートのメール通知

アラートがトリガーされると、そのアラートの各サブスクライバーに通知メールが送信されます。設定してある場合は、グローバル アラート サブスクライバーにも送信されます。

Bit9 コンソールには、トリガーされたアラート「クラス」ごとに 1 つのバナーが表示されますが、Bit9 Server は各「インスタンス」ごとにアラート E メールを送信します。インスタンスは、アラート条件に一致する個別のケースとして定義されます。たとえば、悪意のあるファイルの場合、アラートをリセットするまでに同一の悪意のあるファイルが 20 回出現しても、単純に 1 つのインスタンスとしてカウントされます。しかし、アラートをリセットするまでに 20 の「異なる」悪意のあるファイルが出現すると、各ファイルが 1 つのインスタンスとしてカウントされ、サブスクライバーへのアラートのためにインスタンスごとに新しい E メール メッセージが生成されます。

メール通知には、このインスタンス アラートに対するアクションの実行時間、アクションが実行されたシステム、ログイン ユーザー、ファイル ハッシュなど、アラートの基本情報が含まれます。以下の［File Propagation Alert（ファイル増殖アラート）］通知は、典型的なファイル関連アラートです。実際に提供される情報は、アラートのタイプによって異なります。



File Activity Alert

File Propagation Alert

Priority:	Medium
The file 'test.exe' with hash 7c4447c843c6e6956c2e725439cdfbfd8efa2214392c0568d219f36ea506c269 propagated on 2 of 10 computers with All policies within 10 minutes. Computer(s) and user(s) affected: MYCORP\LAPTOP-3 (rjones) and MYCORP\DESKTOP-5 (dgomez)	
Bit9 Platform Server:	bit9srv.mycorp.local
Triggered On:	Mar 18 2015 2:27PM
Created By:	System
Message:	Propagation of a new unapproved file
File State:	Unapproved
Tell me more:	Alert Details
	File Details
	Event Details

上記の例で示されているように、メール通知にはアラート関連情報が表示されるコンソール ページへのリンクも含まれています。このケースでは、このアラートのインスタンスのリストを示す［Alert Details（アラートの詳細）］、トリガーしたファイルを示す［File Details（ファイルの詳細）］ページ、および該当する場合は、アラートの対象になったファイル（ハッシュ）に関連する［Event Details（イベントの詳細）］です。［File Details（ファイルの詳細）］と［Event Details（イベントの詳細）］は、ファイル以外のアラートには含まれません。コンピューターのポリシーなどの Bit9 設定が関与するイベントの場合には、［Computers（コンピューター）］テーブルへの［Manage Computers（コンピューターの管理）］リンクが含まれることもあります。

同一のアラート クラスの新しいインスタンスによって生成される各 E メールは、同一の［Alert History（アラート履歴）］で追跡されます。この E メールには、アラートの該当インスタンスへのリンクが含まれています。アラートをリセットすると、そのインスタンスの履歴はクリアされますが、このセッション中に初めてトリガーされた日時の記録は残されます。トリガーされたアラートの履歴とインスタンス リストの例については、「アラートのインスタンスと履歴の表示」（625 ページ）を参照してください。

注意

アラート通知 E メールに含まれる詳細は、そのアラートの特定の「インスタンス」の説明です。E メールの［Alert Details（アラートの詳細）］リンクをクリックすると、［Alert Instances（アラート インスタンス）］ページが開き、トリガーされたアラートの「すべて」のインスタンスの詳細が表示されます。

トリガーされたアラートのリマインダー メール

アラートのリマインダー メールを有効化すると、アラートが手動または自動でリセットされていない限り、指定したスケジュールでそのアラートに対する新しい E メール通知が生成されます。たとえば、Bit9 SRS Unvailable Alert（Bit9 SRS 使用不能アラート）がトリガーされると、E メールが即座に送信されます。リマインダー メールを有効化していない場合は、このアラートをリセットした後にトリガー条件が再度発生しない限り、このアラートに関する E メールはその後送信されません。

一方、リマインダー メールを「有効化」し、間隔を 30 分に設定している場合は、このアラートのサブスクライバーは接続が回復するかアラートがリセットされるまで、30 分間隔でこのアラートに関する新しい E メールを受信します。

アラートの手動および自動リセット

アラートをリセットすると、アラートは「トリガーされている」状態でなくなり、アラートのトリガーを発生させたすべての現在のインスタンスの履歴がクリアされます。アラートは、リセットされると［Triggered Alerts（トリガーされたアラート）］ポートレットに表示されなくなり、［Alerts（アラート）］ページでもハイライト表示項目ではなくなります。このアラートに一致する条件が再度発生すると、新しいアラートがトリガーされ、新しい E メールがサブスクライバーに送信され、このアラートがコンソールの定位置に表示されます。

アラートは手動または自動でリセットできます。

- **手動リセット** – アラートを手動でリセットするには、［Triggered Alerts（トリガーされたアラート）］ポートレット、［Alerts（アラート）］ページ、または［Alert History（アラート履歴）］ページで、該当するアラートの［Reset（リセット）］ボタンをクリックします。この操作を行うと、アラートがリセットされることに加え、アラート履歴に「Reset（リセット）」イベントが追加され、タイムスタンプ、リセットを行った Bit9 コンソール ユーザーのアカウント名が記録されます。
- **時間制限による自動リセット** – アラートの自動リセットを有効化してある場合、自動リセットの期間を設定できます。この期間が経過するまでにアラートが手動、または条件の変化によってリセットされない場合、アラートは自動でリセットされます。デフォルト値は 4 週間です。アラート条件の変化に対しては自動リセットを許可し、期間に基づいた自動リセットは行わない場合は、このフィールドの値として非常に長い期間（週）を設定します。時間ベースの自動リセットが発生すると、「Auto-Reset（自動リセット）」イベントが履歴に追加され、タイム スタンプが記録されます。自動リセットが行われても、アラート E メールは送信されません。
- **条件の変化による自動リセット** – アラートの自動リセットを有効化している場合、アラートをトリガーした条件が変化するとアラートが自動的にリセットされることがあります。あるアラート インスタンスをトリガーした条件が存在しなくなると、そのインスタンスは、所属するアラート クラスのトリガーされたインスタンスのリストから削除されます。その時点で、トリガーされたインスタンスがアラート クラスから「なくなった」場合、アラート通知は自動的にリセットされます。リセットがトリガーされる条件は、アラートのタイプごとに異なります。一部のタイプのアラートは、この方法では自動リセットされません（期間による自動リセットは発生します）。
  アラートが自動リセットされると、履歴に「Auto-Reset（自動リセット）」イベントが追加され、タイムスタンプ、変更したユーザーが記録されます。ただし、自動リセットが行われてもアラート E メールは送信されません。

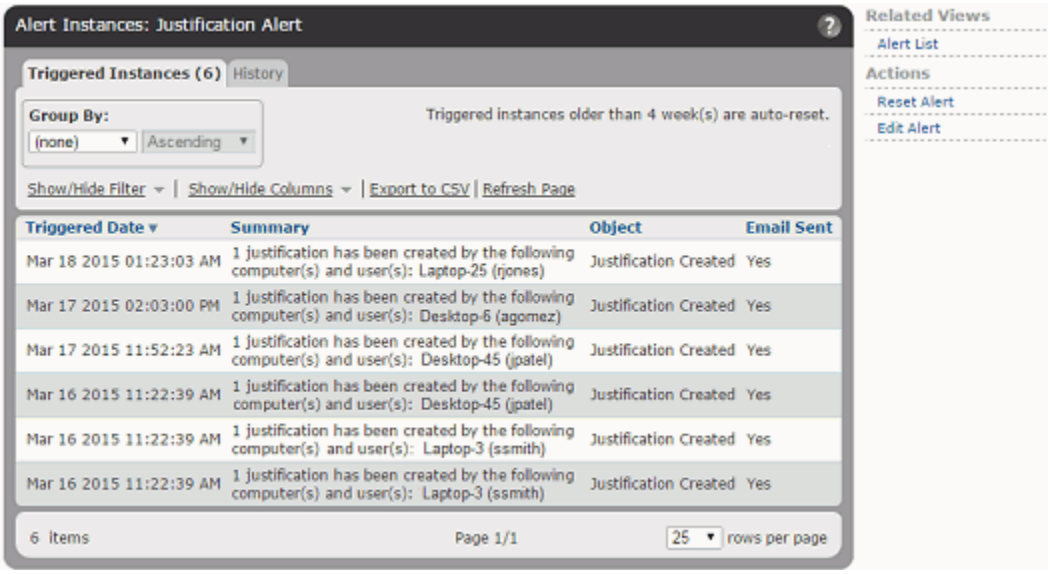
表 79：さまざまなアラート タイプのリセット条件

アラートのタイプ	リセットの条件
Backup Missed Alert（バックアップ失敗アラート）	バックアップが成功したときにリセットされます。
Database Limit Reached（データベース制限到達）	データベース サイズがしきい値を下回るとリセットされます。
Database Verification Failed（データベース検証失敗）	データベース検証が成功するとリセットされます。
Potential Risk or Malicious File Detected（危険な可能性がある、または悪意のあるファイルの検出）	アラートをトリガーした（または先に検出されていたらトリガーしていた）ファイルが「なくなる」とリセットされます。
Bit9 SRS Unavailable Alert（Bit9 SRS 使用不能アラート）	Bit9 Server が Bit9 SRS に正常に再接続し、Bit9 SRS データとサーバーの同期が正常に動作するとリセットされます。これによりイベントが生成されます。
Local Approval Alert（ローカル認証アラート）	ローカル認証モードのマシンがなくなるとリセットされます。
File Prevalence（ファイル普及度）	特定のファイルの普及度が、指定したしきい値を下回るとリセットされます。
Baseline Drift（ベースライン ドリフト）	指定したドリフト レポートのドリフトが、指定したパラメーター（ユーザー、コンピューター、またはポリシー）のしきい値を下回るとリセットされます。
Computer Security（コンピューター セキュリティ）	アラートを発生させた条件が満たされなくなると（この変化が検出可能な場合）リセットされます。
Approval Request Alert（承認要求アラート）	十分な数の［Submitted（送信済み）］または［Open（オープン）］状態の承認要求がクローズされ、トリガーしきい値を下回るとリセットされます。
Justification Alert（根拠アラート）	十分な数の［Submitted（送信済み）］または［Open（オープン）］状態の根拠がクローズされ、トリガーしきい値を下回るとリセットされます。
File Propagation and Block Alert（ファイルの増殖 / ブロック アラート）	これらのアラートは時間ベースなので、条件ではリセットされません。たとえば、特定のファイルが 1 時間に 20 パーセントのマシンに増殖したとアラートが判断した場合、その後どのようなイベントが発生しても過去の 1 時間に発生した事象は変わらないため、アラートはトリガーされたままです。［Auto Reset（自動リセット）］期間による自動リセットのみが適用されます。

アラートのタイプ	リセットの条件
Updater Modified Alert（アップデーター変更アラート）	変更されたアップデーターは変更された状態が維持されるため、条件ではリセットされません。[Auto Reset（自動リセット）] 期間による自動リセットのみが適用されます。
New Certificate Alert（新しい証明書アラート）	条件ではリセットされません。[Auto Reset（自動リセット）] 期間による自動リセットのみが適用されます。
Revoked Certificate Alert（証明書取り消しアラート）	条件ではリセットされません。[Auto Reset（自動リセット）] 期間による自動リセットのみが適用されます。
Event Alert（イベント アラート）	条件ではリセットされません。[Auto Reset（自動リセット）] 期間による自動リセットのみが適用されます。
System Health OER Alert（システム正常性 OER アラート）	[System Health（システム正常性）] ページの OER 痕跡に問題が表示されなくなるとリセットされます。

アラートのインスタンスと履歴の表示

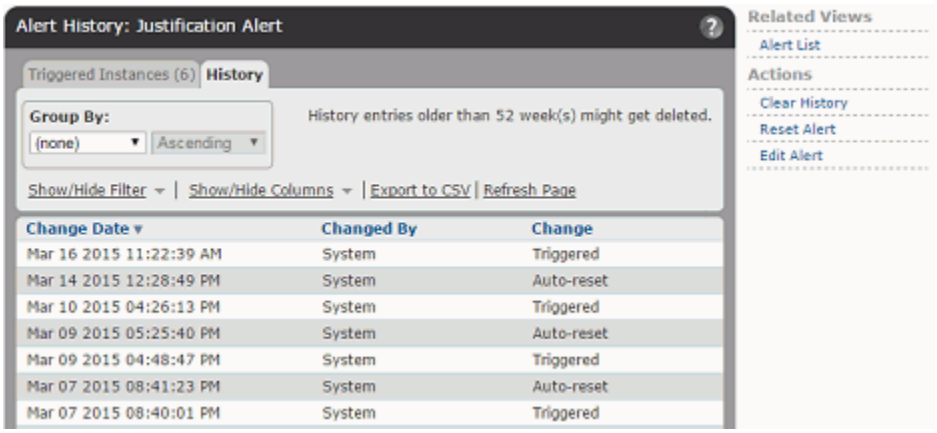
アラートが現在トリガーされている場合、[Alerts] ページでそのアラートの［View Instances（インスタンスの表示）］ボタン（ ）をクリックすると、アラートをトリガーしたインスタンスを表示できます。［Alert Instances（アラート インスタンス）］ページには、インスタンスごとにアラートの日付、サマリー説明、オブジェクト（オブジェクトと実行されたアクション（作成、変更、削除など））、E メール送信の有無が表示されます。



アラートをリセットすると、そのアラートをトリガーしたインスタンスの詳細は削除されます。

アラートの履歴を表示するには、[Alerts（アラート）] ページで [View Instances（インスタンスの表示）] ボタン（ ）をクリックし、[History（履歴）] タブをクリックするか、[Alert Instances（アラート インスタンス）] ページで [History（履歴）] タブをクリックします。アラートがトリガーされていない場合、[View Instances（インスタンスの表示）] ボタンをクリックしたときに利用できるタブは [History（履歴）] タブのみです。

アラート インスタンスの [History（履歴）] ページには、アラートの作成および変更の日時とそのユーザー、トリガーおよびリセットの日時、追加されたサブスクライバー、有効か無効かなどの情報があります。



[Alert Instances（アラート インスタンス）] と [Alert History（アラート履歴）] のどちらのビューにも、アラートに対するアクション実行用のメニューがあります。以下に示すこれらのメニューのコマンドのほとんどは、両方のタブに表示されます。

- [**Alert List**（アラートの一覧表示）] – [Alerts（アラート）] テーブル ページに戻ります。
- [**Clear History**（履歴のクリア）] – ([History（履歴）] ページのみ）このアラートのすべての履歴をクリアします。
- [**Reset Alert**（アラートのリセット）] – （トリガーされているアラートのみ）トリガー状態のアラートをリセットし、現在のインスタンスを削除します。
- [**Delete Alert**（アラートの削除）] – （アラートが削除可能な場合のみ）操作可能なアラートのリストからそのアラートを削除します。
- [**Edit Alert**（アラートの編集）] – アラートの設定を編集できる [Edit Alert（アラートの編集）] ページが開きます。

重要

［**Reset Alert**（アラートのリセット）］を実行すると、アラートの最新のトリガーから前回のアラートのリセットまでの間について「インスタンス」の詳細な履歴は削除されますが、アラートがトリガーされた日時などの他のすべての情報は残ります。［**Clear History**（履歴のクリア）］を実行すると、アラートの作成および変更の日時、サブスクライバー、すべてのトリガー、およびリセット イベントを含む「すべて」のアラートの履歴が削除されます。アラートの履歴は、これらの情報が不要であることを確認してからクリアしてください。

アラート E メール サブスクリプションの管理

アラート E メールには 2 つのタイプのサブスクリプションがあります。

- **特定のアラート** – ［Alert Information（アラート情報）］ページで、そのアラートに対する E メール通知のサブスクライバーを追加できます。
- **すべてのアラート** – ［System Configuration（システム構成）］ページで、アラート E メールのグローバル サブスクライバーを「1 名」設定できます。「グローバル アラート サブスクライバーの指定」（782 ページ）を参照してください。

重要

サブスクライバーは、［System Configuration（システム構成）］ページでアラート E メールが正しく設定され、有効化されている場合にのみ通知 E メールを受信します。詳細については、Bit9 の設定に関する章の「アラート メールおよび承認要求メールの構成」を参照してください。

E メール通知の一般的な設定方法は、個別のアラートのサブスクリプションです。この方法では、特定のユーザーにとって重要なアラートを決定できるため、重要なアラートが他のアラート E メールに埋もれてしまう事態を回避できます。ユーザーは、［Triggered Alerts（トリガーされたアラート）］ポートレットまたは［Alerts（アラート）］ページで、E メール通知が必要なほど重要ではない通知を常に監視できます。

特定のアラートの E メール通知リストにサブスクライバーを追加する手順：

1. ［Alerts（アラート）］ページで、変更するアラートの隣にある［View Details（詳細の表示）］（鉛筆とファイル）ボタンをクリックします。
2. ［Alert Information（アラート情報）］ページで、［Subscribers（サブスクライバー）］パネルまで下にスクロールし、［**Email Address**（E メール アドレス）］テキスト ボックスをクリックして、サブスクライバー名を貼り付けるか入力します。

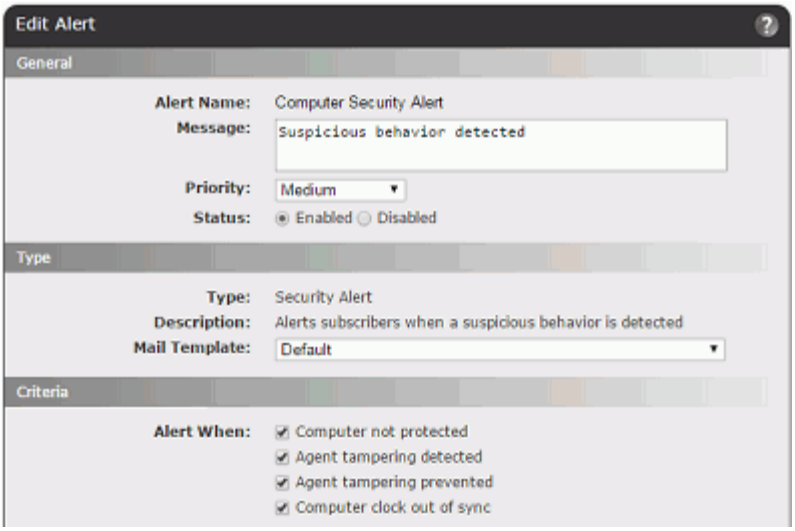
3. ドロップダウン メニューから E メールのタイプ（[**Auto**（オート）]、[**Text**（テキスト）]、または [**HTML**]）を選択します。デフォルトの［Auto（オート）］では、受信者の E メール システムに関する情報に基づいて、サーバーが受信者に最適な形式を決定します。
4. ［**Add**（追加）］をクリックしてサブスクライバーを追加します。新しいサブスクライバー名が、サブスクライバー エントリ行の下のリストに表示されます。
5. アラートがトリガーされたときに通知を受信する他のすべてのサブスクライバーを追加します。
6. ［Alert Information（アラート情報）］ページ下部の［**Save**（保存）］をクリックします。新しいサブスクライバーがこのアラートの配布リストに追加されます。

既存のサブスクライバーの E メール アドレスまたは送信形式を編集するには、サブスクライバーの追加のときと同様に［Alert Information（アラート情報）］ページを開き、サブスクライバー名の隣の［**Edit**（編集）］をクリックします。サブスクライバー情報の編集が完了したら、名前の隣の［Update（更新）］をクリックし、次に［Alert Information（アラート情報）］ページ下部の［Save（保存）］をクリックします。必ず両方のボタンをクリックしてください。

E メール通知のリストからサブスクライバーを削除するには、［Alert Information（アラート情報）］ページを開き、名前の隣の［**Remove**（削除）］をクリックします。このアクションに対しては、削除の確認メッセージは表示されません。名前は即座に削除されます。

［Computer Security Alerts（コンピューター セキュリティ アラート）］でのエージェントの問題の検出

Bit9 のアラートの多くはコンピューター セキュリティに関連していますが、特にこの目的のために設計されている組み込みアラートがあります。［Computer Security Alert（コンピューター セキュリティ アラート）］（デフォルトでは無効）は、疑わしい行動を示す可能性があるイベントによってトリガーされます。



セキュリティ アラートのトリガー条件

［Computer Security Alert（コンピューター セキュリティ アラート）］で有効化できるトリガー条件は 4 つあります。デフォルトでは、このアラートを有効化するとすべての条件が有効化されます。これらのうちどの条件によってセキュリティ アラートがトリガーされたかは、［Alert instance（アラート インスタンス）］ページの［Summary（サマリー）］フィールド、およびこのアラートによって送信された E メール通知（有効な場合）で特定できます。

セキュリティ アラートのトリガー条件を以下に示します。

- **Computer not protected（コンピューターが保護されていない）** – この条件は、エージェント アップグレードが失敗すると発生します。つまり、特定されたコンピューター上でBit9エージェントが稼働していないため、コンピューターが Bit9 エージェントによって保護されていない状態です（［Computers（コンピューター）］ページで、このコンピューターの［Connection status（接続ステータス）］インジケーターが赤になります）。この条件によってアラートがトリガーされた場合、エージェントが正常な動作を再開するとアラートは自動的にリセットされます。
- **Agent tampering detected（エージェントの改ざんの検出）** – Bit9 エージェントの改ざんからの保護が Bit9 コンソールで誤って無効化され、Bit9 エージェントが稼働するコンピューター上のユーザーが（新規ファイルの追加などによって）エージェント フォルダーを変更すると、［Computer Security Alert（コンピューター セキュリティ アラート）］がトリガーされ、サマリー説明に「Agent tampering detected（エージェントの改ざんを検出）」と示されます。管理者がBit9エージェントの改ざんからの保護を再度有効化すると、このアラートは自動的にリセットされます。
- **Agent tampering prevented（エージェント改ざんの阻止）** – エージェントが管理するコンピューター上のユーザーがエージェントの改ざんを試み、失敗すると、［Computer Security Alert（コンピューター セキュリティ アラート）］がトリガーされ、サマリー説明に「Agent tampering prevented（エージェントの改ざんの阻止）」と示されます。たとえば、ユーザーがエージェント フォルダー (Bit9\Parity Agent) へのファイルのコピーを試み、改ざんからの保護のために失敗した場合や、特別なエージェント管理コマンドの不正な実行（正しいパスワードなし）を試みた場合です。この条件がアラートをトリガーした場合、アラートは手動でリセットする必要があります。
- **Computer clock out of sync（コンピューター クロックの非同期）** – マルウェアやその他の不正なファイルの実行を検出されずに試みる手段の 1 つに、ターゲット システムのクロックを変更して無効なタイムスタンプを作成するという方法があります。Bit9 エージェントは、そのような状況でもファイルの実行を検出してレポートしますが、Bit9 Serverのクロックとエージェント クロック間に相違があるとすぐに［Computer Security Alert（コンピューター セキュリティ アラート）］が生成され、サマリー説明に「Computer clock out of sync（コンピューター クロックの非同期）」と示されます。不正なアクティビティの開始元コンピューター上のシステム時間を修正すると、Bit9 Server が受信する次のイベントによってこのアラートがリセットされます。

［Computer Security Alert（コンピューター セキュリティ アラート）］が有効化されている場合は、いずれかのコンピューター上で有効化されている「いずれか」の条件が発生すると、このアラートがトリガーされます。このアラートがトリガーされている間に、同じコンピューター上でこのトリガー条件が追加で発生すると、履歴には記録されますが、新たなアラート インスタンスは生成されません。ただ

し、同じコンピューターで「異なる」トリガー条件を満たすイベントがレポートされると、新たなインスタンスが表示されます。たとえば、改ざんの試行が 2 回失敗した場合、その 2 回の間にアラートがリセットされない限り、2 つのアラート インスタンスは生成されません。一方、1 台のコンピューター上で改ざんの試行の後にクロックの非同期が発生した場合、2 つの異なるアラート インスタンスが生成されます。

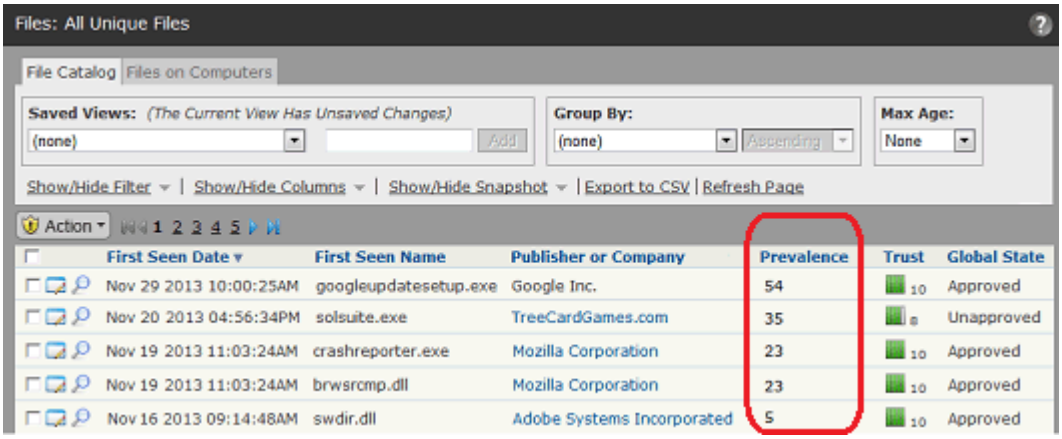
すべてのアラートと同様に、通知が有効化され、正しく設定されていれば、インスタンス発生のたびに E メール通知が送信されます。Bit9 コンソールに表示される［Alert Instance（アラート インスタンス）］とアラートの E メール通知の両方に、セキュリティ イベントの詳細、イベントが発生したコンピューターの名前、インスタンスのトリガー日時が含まれます。

注意

［Computer Security Alert（コンピューター セキュリティ アラート）］は Bit9 エージェントに基づいているため、アラートのトリガー条件が満たされたときにエージェントが接続されていないと、アラートは生成されません。また、多数のエージェント、ファイル、変更が存在する環境では、エージェントがセキュリティ イベントをレポートしたときに Bit9 Server で多数のイベントが処理されていると、そのアラートは遅延することがあります。

ファイル普及度のアラート

［File（ファイル）］ページの［File Catalog（ファイル カタログ）］タブには、特定のファイルが存在するコンピューターの数を（定期的なアップデートに基づいて）示す［Prevalence（普及度）］列があります。



［Prevalence（普及度）］列がテーブルに含まれている場合は、普及度を基準にテーブルを並び替えることができます。また、ページでフィルターを設定して、指定した数以上の普及度を持つファイルのみを示すレポートを表示することもできます。過去にエージェントによって検出され、この Bit9 Server にレポートされたファイルでも、現在の普及度がゼロの場合はこのテーブルから削除されます。ただし、［Files（ファイル）］ページの［Saved Views（保存済みビュー）］から［Removed Files（削除済みファイル）］を選択すると、このファイルを表示できます。

普及度アラート

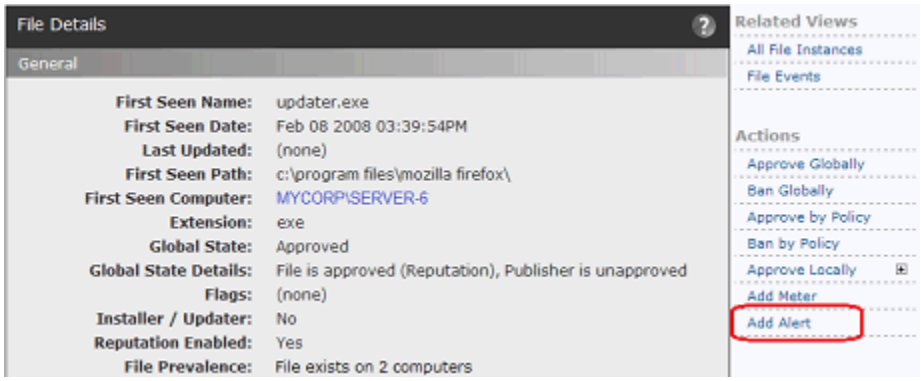
普及度アラートは、特定のファイルの普及度が設定済みのしきい値に到達するとトリガーされます。ファイル普及度アラートは、[Alert（アラート）]ページを開いて、アラートの対象ファイルに関する情報を入力することで作成できますが、追跡するファイルの［File Details（ファイルの詳細）］ページを使用すると簡単に作成できます。アラートの詳細については、「Bit9 アラートの使用」（606 ページ）を参照してください。

注意

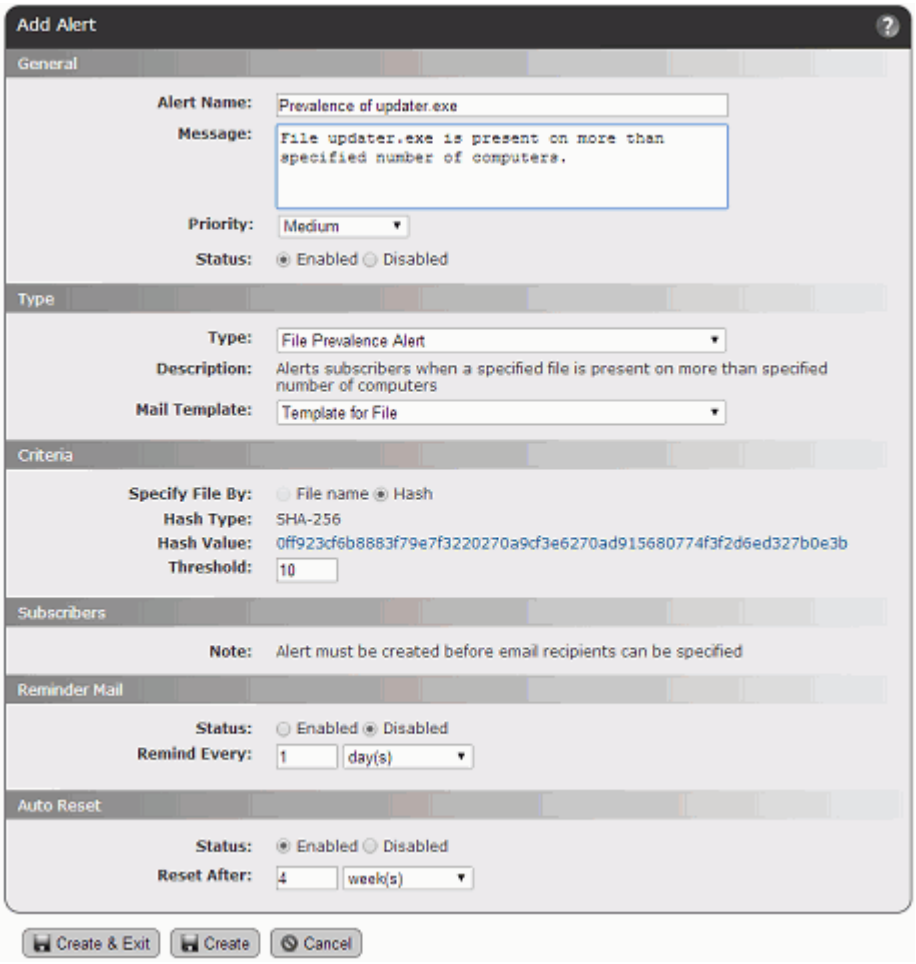
- 普及度アラートのファイル名にワイルドカードは使用できません。
- 普及度アラートには、パスではなく名前を指定します。

［File Details（ファイルの詳細）］ページからファイル普及度のアラートを作成する手順：

1. ［Files（ファイル）］ページで、増殖を追跡するファイルの名前の隣にある［View Details（詳細の表示）］（ファイルと鉛筆）ボタンをクリックします。［File Details（ファイルの詳細）］ページが開きます



2. このファイルの［File Details（ファイルの詳細）］ページで、［Action（アクション）］メニューの［**Add Alert**（アラートの追加）］をクリックします。ファイル名とそのハッシュが入力された状態で［Alert Information（アラート情報）］ページが開きます。



3. このアラートに、以下を含む残りのパラメーターを設定します。
   a. このアラートがトリガーされるために、このファイルが出現する必要があるコンピューターの数のしきい値。
   b. 一定時間の経過後にアラートがリセットされていない、または条件が改善されないとき、定期的に E メール リマインダーを再送信する場合のリマインダー メールの指定。
4. このページに留まる場合は［**Create**（作成）］をクリックします。［Alerts（アラート）］テーブル ページに移動する場合は［**Create & Exit**（作成して終了）］をクリックします。このファイルの普及度アラートが［Alerts（アラート）］ページに表示されます。
5. E メール　アラートのサブスクライバーを追加するには、アラートの［View Details（詳細の表示）］ボタン（ファイルと鉛筆）をクリックし、［Alert Information（アラート情報）］ページの［Subscribers（サブスクライバー）］セクションでアドレスを追加します。

特定のファイル実行の監視

ソフトウェア メーター機能を使用すると、ユーザーが特定のファイルを実行した回数を追跡できます。メーターを作成するときは、追跡するファイルを指定します。指定したファイルがコンピューター上で実行されるたびに、サーバーがその実行を記録します。構成可能なレポートには、実行時間、ユーザー、コンピューター、およびポリシー別に累積の実行イベントを表示できます。メーターは必要な数だけ作成し、一元的に管理（レポート表示、編集、削除）できます。監視は、メーターを作成するとほぼ同時に開始されます。

ソフトウェア メーターは、以下の目的に役立ちます。

- アプリケーションの使用頻度に関するデータの収集
- アプリケーションを実行しているコンピューターの特定
- アップグレードが必要な古いバージョンのソフトウェアを実行しているコンピューターの特定、または古くなったアプリケーションの完全な廃止

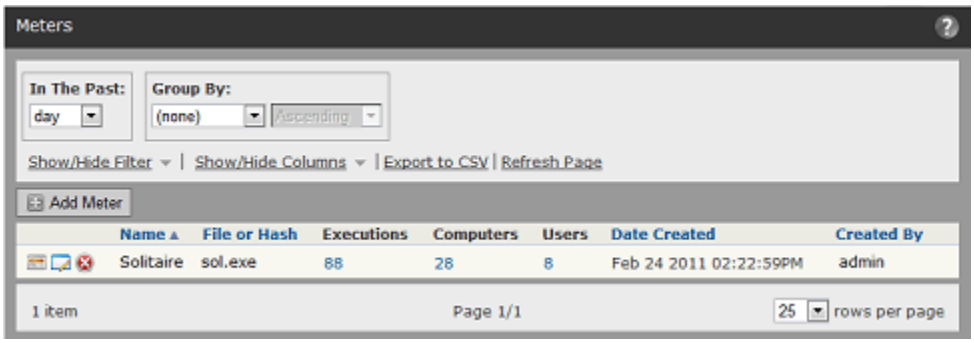
注意

- Bit9 エージェントは、コンピューターを起動したときに最初に開始されるプロセスの 1 つです。通常、エージェントが起動するまで、または一定のタイムアウト時間が経過するまで、ユーザーはエージェント管理コンピューターにログインできないように設定されます。ただし、エージェントよりも前に起動するように設定されているサービスまたはプロセスがある場合、そのアクティビティは、エージェントが起動するまで監視や制御が行われません。
- ネットワーク上、またはコンピューターのサブセット上で実行された「すべて」のファイルは、[Find Files（ファイルの検索）] ページの［Filters（フィルター）］、または［Files（ファイル）］ページの［Files on Computers（コンピューター上のファイル）］タブを使用して検索できます。「[Find Files（ファイルの検索）] ページでの検索の定義」を参照してください。

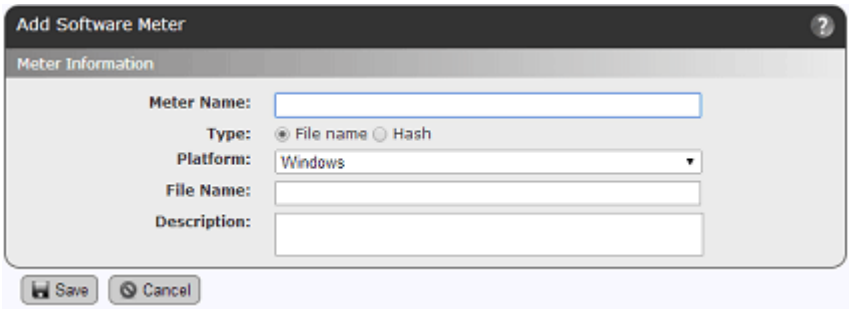
メーターは、以下に示す手順で一から作成できます。または［File Details（ファイルの詳細）］ページからファイル用のメーターを直接作成できます。「［File Details（ファイルの詳細）］ページからのメーターの作成」（637 ページ）を参照してください。

指定したファイルの実行をメーターする手順：

1. コンソール メニューで、[**Tools**（ツール）] > [**Meters**（メーター）] の順に選択します。[Meters（メーター）] ページが表示されます。



2. [Meters（メーター）] ページで [**Add Meter**（メーターの追加）] をクリックします。



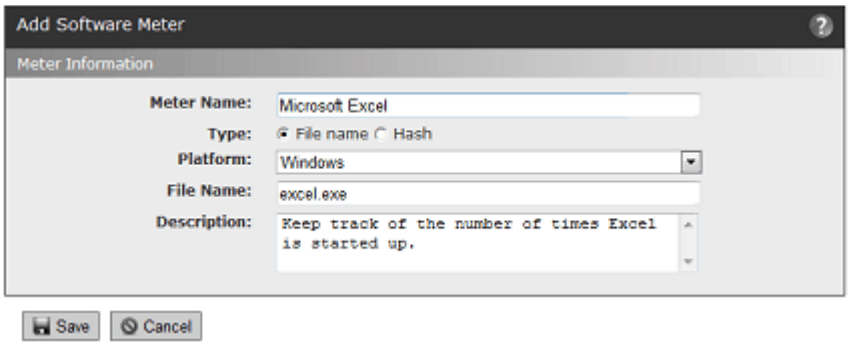
3. [Add Software Meter（ソフトウェア メーターの追加）] ページで、このファイルに使用する識別のタイプ（[File name（ファイル名）] または [Hash（ハッシュ）]）を選択します。選択したタイプに応じて追加フィールドが表示されます。
4. [Software Meter（ソフトウェア メーター）] パネルで、監視するファイルに関する情報を指定します。

表 80：ソフトウェア メーターのパラメーター

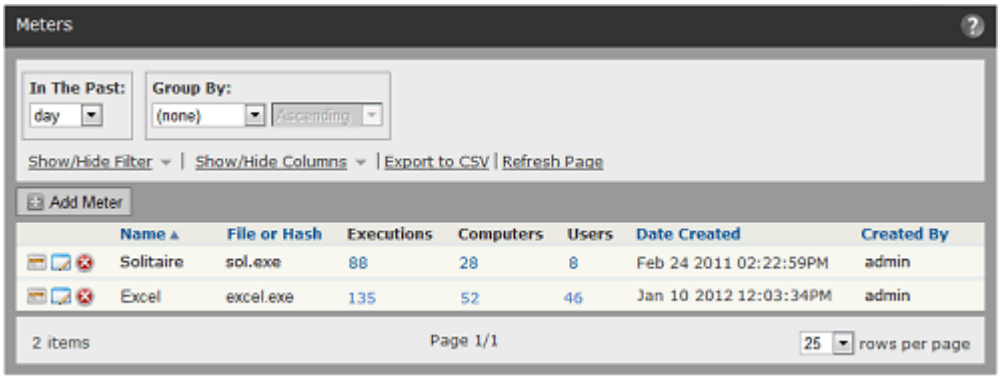
フィールド	説明
[Meter name（メーター名）]	メーターするソフトウェアの説明テキスト。
[Type（タイプ）]	ファイルをメーターするには、ファイルの名前またはハッシュ（データ署名）を把握している必要があります。どちらか適切な方を選択します。ファイル名メーターはプラットフォームに固有であり、ハッシュ メーターはすべてのプラットフォームに適用されます。 [File Details（ファイルの詳細）] ページから直接作成されたメーターには、ファイル識別子としてそのファイルのSHA-256ハッシュが自動的に入力されます（利用可能な場合）。

フィールド	説明
[Platform（プラットフォーム）]	ファイル名メーターの場合、メーターを適用するプラットフォーム（Windows、Mac、または Linux）。ファイル名メーターは、1 つのプラットフォームでのみ使用できます。 （ハッシュ メーターにはこのフィールドは表示されません。）
[File Name（ファイル名）]	このメーターを適用するファイル名（またはパス）。ファイル名のみを指定すると、あらゆる場所でのこのファイルの実行がメーターされます。ファイル名で終了するパスを指定すると、指定された場所でのこのファイルの実行のみがメーターされます。 指定したパスがディレクトリで終了している場合、このディレクトリとそのすべてのサブディレクトリでのすべての実行がメーターされます。 **プラットフォームに関する注意：** • Windows のパスでは、ローカル ドライブ名（例：C:\dir\subdir\application）または UNC パス（例：\\dir\subdir\application）を指定できます。ネットワーク アクセス用のマップされたドライブ（例 Z:\application）は指定できません。 • すべてのパスで、選択したプラットフォームで定められている正しいディレクトリ区切り文字を使用してください。 • メーターの作成後にプラットフォームを切り替えることができますが、ディレクトリ区切り文字やドライブ レターなど、プラットフォームの差異を考慮する必要があります。プラットフォームの違いによってパスが無効になる可能性があります。
[Hash Type（ハッシュ タイプ）]	監視するハッシュの作成に使用する暗号化アルゴリズム（MD5、SHA-1、または SHA-256）。[Files（ファイル）] または [Find Files（ファイルの検索）] の検索では、Bit9 はデフォルトで SHA-256 ハッシュを返しますが、他のハッシュ タイプで監視、承認、または禁止できるように相互参照します。[File Details（ファイルの詳細）] ページからメーターを直接作成する場合、ファイル識別子としてこのファイルの SHA-256 ハッシュが自動的に利用されます（利用可能な場合）。
[Hash Value（ハッシュ値）]	ファイルのハッシュ（データ署名）。 このハッシュが過去に指定されたことがある場合でも、コンピューター上でのファイルの実行を監視します。外部ソースに基づくハッシュを入力した場合、Bit9 エージェントが稼働するコンピューターは、最初にこのハッシュに遭遇したときにその実行を登録します。 ネットワーク上のハッシュを特定するには、[Files（ファイル）] ページか [Find Files（ファイルの検索）] ユーティリティを使用します。Bit9 Server 上で特定されたファイルに対しては、[File Details（ファイルの詳細）] ページから直接メーターを作成できます。
[Description（説明）]	メーターされるファイルを詳しく説明するオプションのテキスト。この情報を表示するには、[Meter（メーター）] テーブルに [Description（説明）] 列を追加します。

たとえば、Microsoft Excel の実行をファイル名で監視するメーターは、以下のスクリーンショットに示すように指定できます。



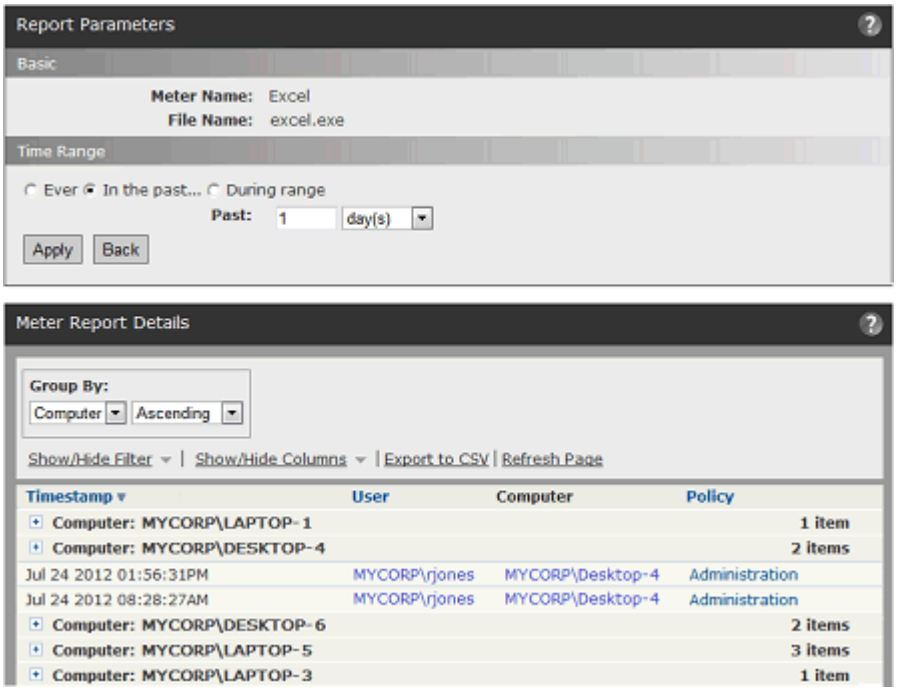
5. メーターされるファイルのテーブルにこのファイルを追加するには、[Save（保存）] をクリックします。メーターが作成されて有効化され、メーターの名前、メーターされるファイル、実行情報が［Software Meter（ソフトウェアメーター)］ページの［Meter（メーター)］テーブルに表示されます。



6. メーター情報を変更するには、メーター名の隣にある［View Details（詳細の表示)］（鉛筆とファイル）ボタンをクリックします。
7. メーター イベントのレポートを表示するには、レポート名の左端にある［View Report（レポートの表示)］ボタンをクリックします。

注意

デフォルトでは、メーター イベントはコンピューターによってグループ化されます。そのコンピューター上でのすべてのファイルの実行を表示するには、コンピューター名を展開します。または、[Group by（グループ別)］メニューで［None（なし)］を選択すると、このグループ化を削除できます。



8. メーターを削除するには、[Meter（メーター）] ページで、削除するメーターの隣にある [Delete（削除）] (x) アイコンをクリックします。

[File Details（ファイルの詳細）] ページからのメーターの作成

1 つの特定のファイルの実行を監視する場合は、[File Details（ファイルの詳細）] ページから直接メーターを作成できます。この方法には、メーター作成に必要なほとんどの情報（ハッシュ値を含む）が事前に設定されるというメリットがあります。この方法で作成されたメーターは、自動的に [Hash（ハッシュ）] タイプのメーターになります。

[File Details（ファイルの詳細）] ページから直接ソフトウェア実行メーターを作成する手順：

1. メーターするファイルの [File Details（ファイルの詳細）] ページを開きます。
2. [File Details（ファイルの詳細）] ページの右にある [Action（アクション）] メニューで、[**Add Meter**（メーターの追加）] をクリックします。[Add Software Meter（ソフトウェア メーターの追加）] ページが表示されます。ファイルのハッシュ値がすでに入力され、ファイル名がデフォルト メーター名になっています。
3. 必要に応じてメーター名を変更し、説明を追加します。
4. [Save（保存）] をクリックしてメーターを保存し、有効化します。

第 19 章

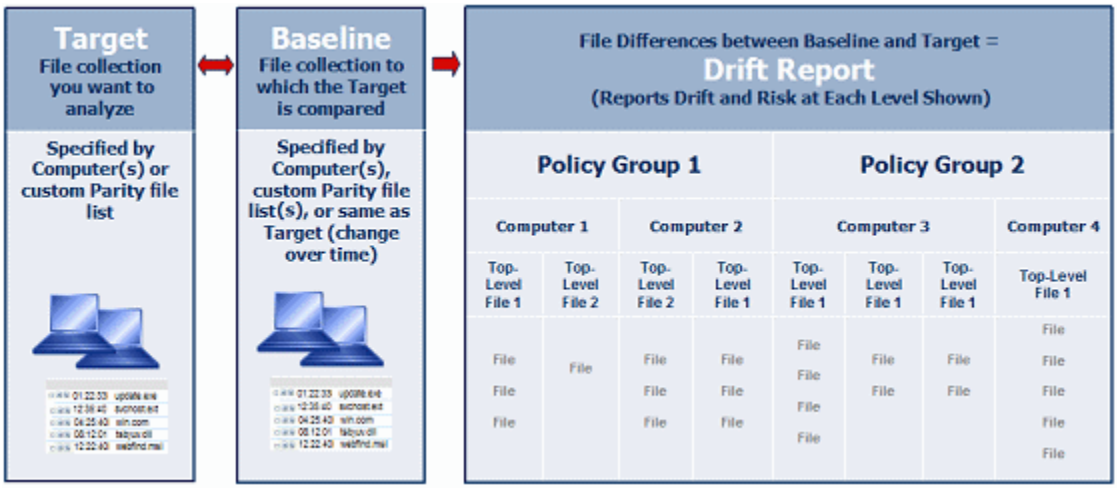
変更の監視：ベースライン ドリフト レポート

この章では、ベースライン ドリフト レポートの使用方法を説明します。このレポートでは、Bit9 エージェントが稼働するシステム上のファイル インベントリの変更を追跡できます。他の監視機能の説明については、第 18 章「イベント、アラート、およびメーター」を参照してください。

セクション

ベースライン ドリフトの概要

Bit9 Server にレポートしているコンピューター上のファイルの Bit9 ライブ インベントリを使用して、ベースライン ドリフト（ファイルのベースラインと、指定したターゲット上の現在のファイルとの差異）を測定することができます。この差異はベースライン ドリフト レポートとして取得可能で、動的なテーブルに詳細を表示することも、Bit9 ダッシュボード上にグラフィック チャートとして表示することもできます。ベースライン ドリフト レポートは、ファイルの差異を単純な数値として提供するだけでなく、そのような変化に関連するリスク分析も提供します。



ドリフト レポートは、一度設定すると自動的に数時間ごとに実行され、ファイル インベントリの変更に関する最新の記録を提供します。さまざまなターゲットとベースラインを使用してさまざまなベースライン ドリフト レポートを作成することができます。また、すぐに利用できる事前構成済みのレポートが用意されています。デフォルトでは、このレポートを作成、変更、および削除できるのは PowerUser と Administrator のみです。ただし、ドリフト レポートとスナップショットの表示のみ、または表示と管理が許可されるカスタム アカウント グループを構成することができます。

表 81：ベースライン ドリフトの用語

用語	説明
ターゲット	分析の対象とする現在のファイルの集合。特定のコンピューター上のすべてのファイル、特定のセキュリティ ポリシーが適用されたコンピューター上のすべてのファイル、またはすべてのコンピューター上のすべてのファイルを指定できます。テーブルにカスタム フィルターを適用して、1 台以上のコンピューター上のファイルを指定することもできます。

用語	説明
ベースライン	ターゲットを比較する基準。1 つの「スナップショット」として取得されたファイルのセット、複数のスナップショット、1 台以上のコンピューターのセット、定義したフィルターやその他のパラメーターによって生成されたカスタム ベースラインを指定できます。ベースラインを使用しないことも可能です。その場合は、時間の経過とともに出現する新しいファイルがレポートされます。
スナップショット	1 台以上のコンピューターから収集したファイルのセット。選択した 1 台以上のコンピューターの「すべて」のファイル、カスタム定義フィルターに基づいて選択されたファイル、Bit9 コンソールの他のページから取得されたファイルのリストを指定できます。各スナップショットには名前が付けられ、ドリフト レポートのベースラインとして使用できます。
ベースライン ドリフト レポート	ベースラインとターゲットの間の差異に関する情報が含まれるレポート。ドリフト レポートでは、変更されたファイルの数だけでなく、その変更に起因するリスク面での差異も把握できます。

ドリフトとリスクの測定方法

ベースライン ドリフト レポートは、指定されたターゲットについて、コンピューターやファイルに関するさまざまなタイプのデータを提供できます。表 82、「基本的なドリフト値」にこれらの情報の説明を示します。

表 82：基本的なドリフト値

用語	説明
ドリフト	ターゲットへのファイルの追加、変更、および（レポートで設定されている場合）削除の観点から単純に測定されたドリフト量。ファイルはハッシュ値で識別されます。1 回のファイルの追加、変更、変更のドリフト値は、それぞれ 1 です。ファイルが変更されたどうかを Bit9 が判断する方法の詳細については、「ベースライン ドリフト レポートの高度なオプション」（656 ページ）を参照してください。
重み付きドリフト	ドリフト値をベースとし、各ファイルのドリフトの重要性を増減させる可能性がある複数の要因によって調整した値。調整要因には、信頼度、脅威レベル、ファイルのタイプ、他のファイルとの関連性などがあります。たとえば、有効なデジタル署名があるファイル、信頼度が高いファイル、または信頼度の高いファイルによってインストールされたファイルの重み付きドリフト値は、これらの要因を考慮しない場合の値よりも低くなります。
リスク	重み付きドリフトに類似する値ですが、脅威ではないと判明したファイルのリスクはゼロになるように調整されます。
重み付きドリフトの割合	現在のレポートにおける重み付きドリフトの合計に占める、行に示されている項目の割合。
リスクの割合	現在のレポートにおけるリスクの合計に占める、行に示されている項目の割合。

ベースライン ドリフト レポートでレポートされるドリフトおよびリスクの合計を決定する、他の重要な要因を以下に示します。

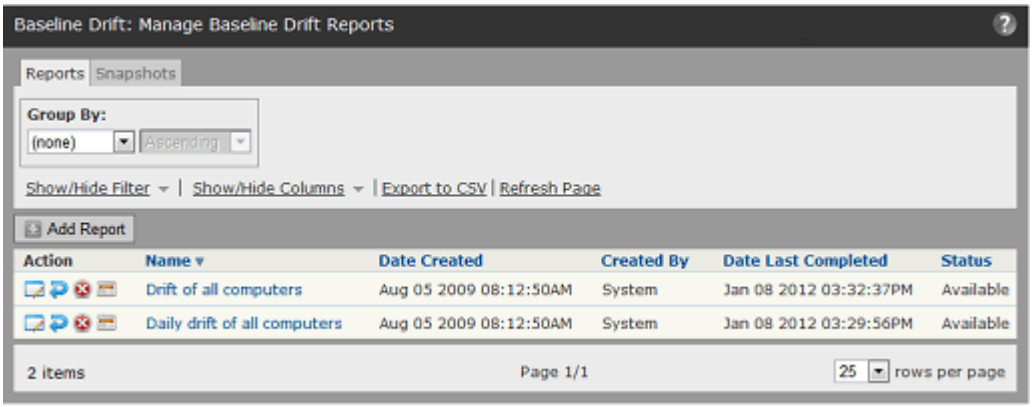
- **ファイル フィルタリング：**ベースラインとターゲットのどのファイルを比較対象にするかを決定できます。たとえば、事前構成済みドリフト レポートでは、未承認ファイルは比較され、禁止ファイルや承認ファイルは無視されますが、必要に応じてこの設定を変更できます。他にもいくつかのファイル カテゴリを比較に含めたり比較から除外したりできます。詳細については、以下の「ターゲットおよびベースラインの定義でのフィルターの使用」および「[Advanced Options（高度なオプション）]：[File Filter Options（ファイル フィルター オプション）]」のセクションを参照してください。
- **ファイル比較メソッド：**デフォルトでは、ベースラインで見つかったファイル ハッシュがターゲットでも「いずれかの場所」で見つかった場合、これは一致するファイルと見なされ、ドリフトはレポートされません。これは「ファイル コンテンツ」メソッドと呼ばれます。もう 1 つの比較メソッドである「ファイルの場所」メソッドでは、ハッシュが同一でもベースラインとターゲットで異なる場所にある場合はドリフトと見なされます。詳細については、「[Advanced Options（高度なオプション）]：[File Comparison Method（ファイル比較メソッド）]」を参照してください。

ベースライン ドリフト レポートの表示と管理

ベースライン ドリフト レポートはすべて、[Manage Baseline Drift Reports（ベースライン ドリフト レポートの管理）] ページに表示されます。このコンソールに表示される事前構成済みのベースライン ドリフト レポートは、[Drift of all computers（すべてのコンピューターのドリフト）] と [Daily drift of all computers（すべてのコンピューターの日次ドリフト）] の 2 つです。これらはデフォルトで無効になっています。これらの事前構成済みレポートを活用することで、ベースライン ドリフトの構成オプションを確認したり、レポートに結果を表示したりできます。既存のレポートは、コピーして新しいレポートの開始点として活用できます。

ベースライン ドリフト レポートのテーブルの表示手順：

- コンソール メニューで、[**Reports**（レポート）] > [**Baseline Drift**（ベースライン ドリフト）] の順に選択します。
  [Manage Baseline Drift Reports（ベースライン ドリフト レポートの管理）] ページが表示されます。



[Manage Baseline Drift Reports（ベースライン ドリフト レポートの管理）] ページでは、既存のレポート、およびレポートの新規作成機能にアクセスできます。またこのページでは、フィルター、列の追加と削除、テーブルの項目のグループ化など、コンソール テーブル ページで使用可能なすべての標準的なボタンとツールを使用できます。以下の表に、ドリフト ページのボタン、列、タブの説明を示します。

表 83: [Manage Baseline Drift Reports（ベースライン ドリフト レポートの管理）] ページのパラメーター

項目	説明
[**Report**（レポート）] タブおよび [**Snapshot**（スナップショット）] タブ	[Report（レポート）] タブ（デフォルト）には、使用可能なすべてのドリフト レポートのテーブルと、それらのレポートについての重要情報が表示されます。また、新しいレポートを作成するための [Add Report（レポートの追加）] ボタンも表示されます。 [Snapshot（スナップショット）] タブには、使用可能なすべてのスナップショットのテーブルと、それらのスナップショットについての重要情報が表示されます。詳細については、「スナップショットの管理」を参照してください。
[**Add Report**（レポートの追加）] ボタン	[Add Baseline Drift Report（ベースライン ドリフト レポートの追加）] ページが開き、新しいベースライン ドリフト レポートの詳細を入力できます。
[View Report Results（レポート結果の表示）] ボタン	この行のレポートの最新結果を表示します。
[View Details（詳細の表示）] ボタン	この行のレポートの [Baseline Drift Report Details（ベースライン ドリフト レポートの詳細）] ページが開きます。このページでは、レポートの詳細を表示および編集できます。
[Schedule Run（実行のスケジュール）] ボタン	通常のレポート期間まで待たずに、この行のレポートができるだけ早く実行されるようにスケジュールできます。
[Delete（削除）] ボタン	この行のレポートを削除します。
[**Name**（名前）] フィールド	レポートの名前。この名前をクリックすると、その行のレポートの最新結果が表示されます。
[**Date Created**（作成日）] フィールド	このレポートが作成された日時。
[**Created by**（作成者）] フィールド	このレポートを作成したコンソール ユーザー。[Created by（作成者）] フィールドに [System（システム）] が表示されているレポートは、Bit9 によって提供されています。

項目	説明
［**Date Last Completed**（最終完了日）］フィールド	このレポートが最後に実行された日時。空白の場合、このレポートは無効化されているか、新規作成されたレポートで最初の実行が完了していません。
［**Status**（ステータス）］フィールド	レポートの現在のステータスを示します。次のいずれかの値になります。 • ［**Available**（使用可能）］– 更新されたレポートを表示できます。 • ［**Available (Updating)**（使用可能（更新中））］– 現在新しいレポートを作成中です。レポートが完了するまでは、前回のレポートを表示できます。 • ［**Disabled**（無効）］– レポートは無効化されており、結果は生成されていません。最後に作成された結果は削除されています。 • ［**Not available**（使用不能）］– レポートは新規です。結果はまだ生成されていません。

ベースライン ドリフト レポート結果の表示

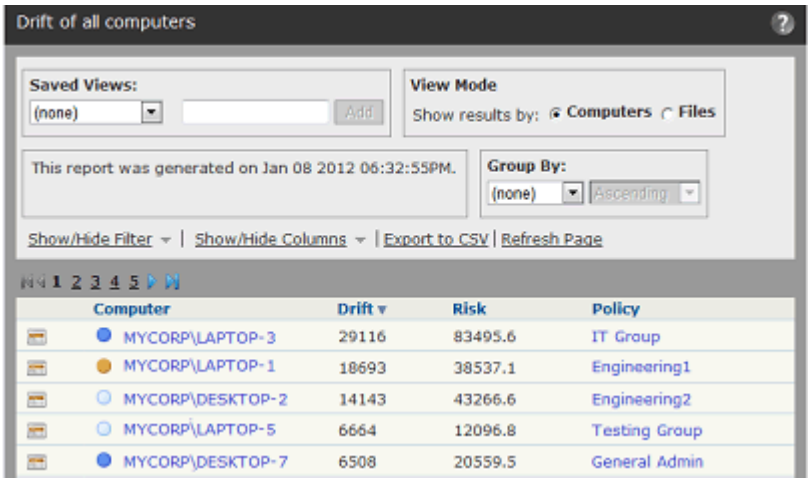
［Manage Baseline Drift Reports（ベースライン ドリフト レポートの管理）］ページのリストに表示されているレポートが［Available（使用可能）］の場合は、最新のレポート結果を表示できます。

ベースライン ドリフト レポートの表示手順：

1. コンソール メニューで、［**Reports**（レポート）］>［**Baseline Drift**（ベースライン ドリフト）］の順に選択します。
2. ［Baseline Drift（ベースライン ドリフト）］ページの［Manage Baseline Drift Reports（ベースライン ドリフト レポートの管理）］テーブルで、表示するレポート名をクリックします。デフォルトでは、最初のビューにはドリフトがコンピューター別に表示されます。

レポート結果：コンピューター ビュー

以下の図は、最初に表示される組み込みの［Drift of all computers（すべてのコンピューターのドリフト）］レポートです。この結果には、過去 24 時間にエージェントが追跡するファイルが追加または変更された（デフォルトではファイルの削除は追跡されません）すべてのコンピューターと、各コンピューターにおけるドリフト量のテーブルが表示されます。［View Mode（ビュー モード）］パネルでは［Computers（コンピューター）］が選択されています。



レポート結果：ファイル ビュー

ドリフトの主要な要素はファイル自体から得られるため、ベースライン ドリフト レポートのファイル ビューは、コンピューター ビューよりも詳しい情報を提供します。ドリフト レポートでは、以下の 3 つの主要なファイル ビューを使用できます。

- **すべての最上位ファイル** – 選択したドリフト　レポートのメイン　ファイル ビューです。レポートの各最上位ファイルのドリフト、リスク、その他のデータが表示されます。
- **1 つの最上位ファイルに関連するファイル** – 1 つの最上位ファイルに関連するファイルのドリフト レポートです。最上位ファイル レポートでハイライト表示されている名前をクリックすると、関連ファイルのレポートを表示できます。
- **1 台のコンピューターのファイル** – ドリフトの原因になった 1 台のコンピューターのすべてのファイルのドリフト レポートです。コンピューター ビューでコンピューター名をクリックすると、コンピューター固有のファイル レポートを表示できます。

これらの主要ビューに加えて、ファイル別のドリフト テーブルの情報を別の視点から提供する、事前構成済みの［Saved Views（保存済みビュー）］が用意されています。

- ［**Drift Contributing to Risk**（リスクの原因となったドリフト）］ – （最上位）ファイルごとの標準レポートを表示します。ただし、ドリフト リスクが 0 のファイルは除外されます。
- ［**Drift by Category**（カテゴリ別のドリフト）］ – ［Group by（グループ別）］メニュー、または［Filters（フィルター）］リストで［Category（カテゴリ）］を選択した場合と同じビューです。Bit9 Software Reputation Service (SRS) によってレポートされたファイル カテゴリのリストがテーブルの左列に表示されます。カテゴリの隣のプラス記号をクリックすると、ビューが展開され、そのカテゴリのすべてのファイルと、各ファイルのドリフトおよびリスク レベルが表示されます。
- ［**Drift by Publisher/Company**（公開者 / 会社別のドリフト）］ – ［Group by（グループ別）］メニュー、または［Filters（フィルター）］リストで［Publisher（公開者）］または［Company（会社）］を選択した場合と同じビューです。ファ

イルで識別された公開者名 / 会社名のリストがテーブルの左列に表示されます。公開者名 / 会社名の隣のプラス記号をクリックすると、ビューが展開され、その公開者または会社に関連するすべてのファイルと、各ファイルのドリフトおよびリスク レベルが表示されます。

- ［**Drift by Installed Program**（インストール済みプログラム別のドリフト）］– ［Group by（グループ別）］メニューで［Installed Program（インストール済みプログラム）］を選択した場合と同じビューです。1 つのインストーラー プログラムに関連するすべてのファイルの合計ドリフトが表示されます。
  プラットフォームに関する注意：このビューは、Windows エージェントの場合にのみ有効です。

次の表に、ドリフト レポートのファイル ビューのコントロールとデフォルト フィールドを示します。

表 84：ドリフト レポート結果の要素

項目	説明
 ［View Report Results（レポート結果の表示）］ボタン	コンピューター ビュー モードのときに、この行のコンピューターのベースライン ドリフト レポートにドリル ダウンします。
 ［View Details（詳細の表示）］ボタン	ファイル ビューのときに、この行のファイルの［File Instance Details（ファイル インスタンスの詳細）］ページを開きます。
 ［Find Files（ファイルの検索）］ボタン	（ファイル ビューのみ）［Find Files（ファイルの検索）］ページが開き、この行のファイルのハッシュに一致する、すべてのコンピューター上のすべてのファイル インスタンスが表示されます。
［File Name（ファイル名）］	ドリフトの原因になっているターゲット上のファイルの名前が表示されます。青でハイライト表示されているファイルはリンクになっており、関連するファイルが存在する最上位ファイルであることを示しています。このリンクをクリックすると、この最上位ファイルに関連するファイルのベースライン ドリフト レポートにドリル ダウンします。
［Publisher or Company（公開者または会社）］	公開者（表示可能な場合）または会社（表示可能で、公開者情報がない場合）が表示されます。
［Drift（ドリフト）］	コンピューター ビュー モードでは、この行のコンピューター上のすべてのドリフト ファイルのドリフトの合計。 ファイル ビューでは、このファイルのドリフトの合計（関連するファイルがない場合）、または、このファイルに関連するファイルのドリフトの合計（最上位ファイルの場合）。 グループ化された情報を含むビューでは、グループ パラメーターの各インスタンスのドリフトの合計。グループを展開すると、グループの各メンバーのドリフトが表示されます。

項目	説明
[Risk（リスク）]	この行の項目のすべてのドリフト ファイルのリスクの合計。詳細については、「ドリフトとリスクの測定方法」（641 ページ）を参照してください。
[Threat（脅威）]	Bit9 SRS で認識されているマルウェア脅威の重み付け分析に基づいた、この行のファイルの脅威レベル。脅威レベルは、悪質（赤の！アイコン）、悪質な可能性あり（黄色の！アイコン）、未知（アイコンなし）、またはクリーン（緑の √ アイコン）です。
[Trust（信頼度）]	この行のファイルの信頼度レベル（0 ～ 10）。0 が最低、10 が最高の信頼度です。信頼度は、ファイルのソース、公開者、Bit9 SRS での認識（マルウェア、またはその他の望ましくないファイル カテゴリなど）を含むさまざまな要因に基づいて算出されます。
[Computer（コンピューター）]	この行のファイルが含まれるコンピューターが表示されます。名前をクリックすると、このコンピューターの［Computer Details（コンピューターの詳細）］ページが表示されます。
[User Name（ユーザー名）]	インストールの開始時、または最上位ファイルの作成時における、このコンピューターのログイン ユーザー。
[View Mode（ビュー モード）]	［View Mode（ビュー モード）］ボックスで［**Files**（ファイル）］をクリックすると、コンピューター別ドリフトからファイル別ドリフトにビューが変更され、レポートには最上位ファイルの一覧が示されます。［View Mode（ビュー モード）］ボックスで［**Computers**（コンピューター）］をクリックすると、ファイル別ドリフトからコンピューター別ドリフトにビューが変更され、ドリフト レポートにはすべてのコンピューターの一覧が表示されます。 **注意**：テーブルの右下の［Show individual files（個別のファイルを表示）］をクリックすると、ファイル ビューには最上位ファイルとそのすべての関連ファイルの両方が表示されます。
[Saved Views（保存済みビュー）]	ファイル ビュー モードには、3 つの保存済みビューがあります。レポートのファイルの完全なリストに戻るには、［Saved Views（保存済みビュー）］で［**none**（なし）］を選択します。
[Action（アクション）] メニュー	ドリフト レポートでチェックボックスをオンにしたファイルに対してアクションを実行できます。詳細については、「ドリフト レポート結果への対応」（650 ページ）を参照してください。

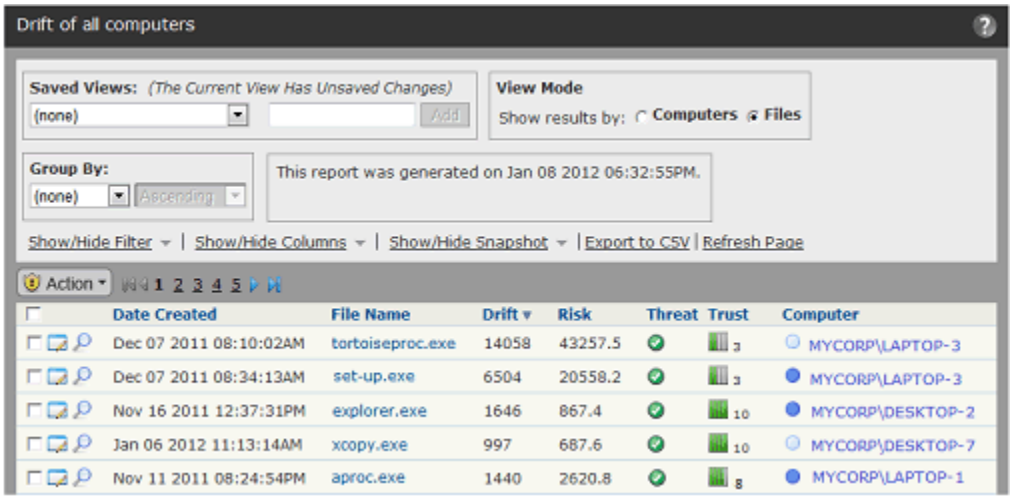
ファイル別ドリフト：すべてのコンピューター上の最上位ファイル

最上位ファイルの多くは、コンピューターに他のファイルをインストールするファイルなので、多くの場合、最上位ファイルのレポートはドリフトとリスクを追跡する上で最も役立ちます。これらのファイルは、レポート内の他のファイルによって生成されていないという意味で「最上位」です。

ベースライン ドリフト レポートの最上位ファイル ビューの表示手順：

1. コンソール メニューで、［**Reports**（レポート）］>［**Baseline Drift**（ベースライン ドリフト）］の順に選択します。

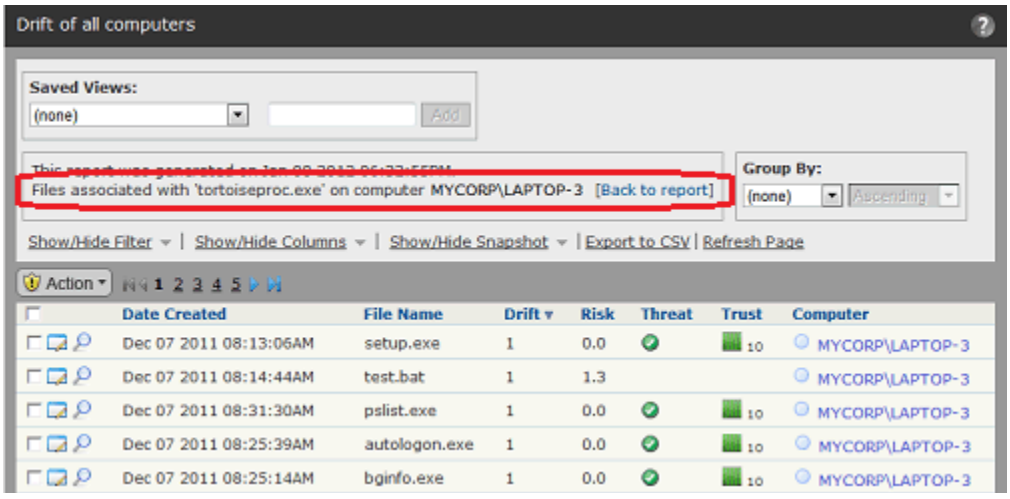
2. ［Baseline Drift（ベースライン ドリフト）］ページの［Manage Baseline Drift Reports（ベースライン ドリフト レポートの管理）］テーブルで、表示するレポート名をクリックします。
3. ［View Mode（ビュー モード）］ボックスで［**Files**（ファイル）］をクリックします。
   最上位ファイル ビューが表示されます。



4. 最上位ファイル ビューとこれらのファイルによって生成されたファイルの両方をレポート結果に表示するには、ページの右下隅の［Show individual files（個別のファイルを表示）］チェックボックスをオンにします。

ファイル別ドリフト：関連ファイルのレポート

青でハイライト表示されている名前は、その名前をクリックすると詳細情報を確認できることを示しています。最上位ファイル レポートでは、ファイル名をクリックすると、クリックしたファイルに「関連する」ファイルの［Baseline Drift Report Results（ベースライン ドリフト レポートの結果）］ページが表示されます。関連するファイルとは、最上位ファイルによってインストールされたファイルか、最上位ファイルのコピー（ハッシュが同一）です。



関連ファイルのレポートから最上位ファイル ビューに戻る手順：

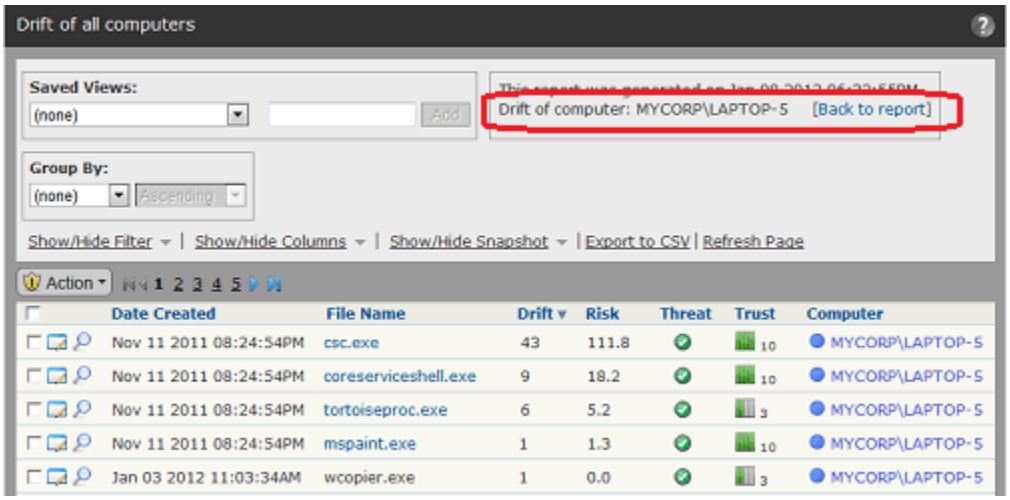
- テーブルの上の「Files associated with（関連ファイル）」行にある［**Back to report**（レポートに戻る）］をクリックします。

1 台のコンピューターのファイル別ドリフト

1 台のコンピューターのファイル別ドリフト レポートを取得できます。このレポートは、さまざまな状況で役立ちます。たとえば、他のコンピューターよりもドリフトが著しく多いコンピューターを見つけて、修復手順を実行することができます。

1 台のコンピューターのファイル別ドリフトの表示手順：

1. コンソール メニューで、［**Reports**（レポート）］>［**Baseline Drift**（ベースライン ドリフト）］の順に選択します。
2. ［Baseline Drift（ベースライン ドリフト）］ページの［Manage Baseline Drift Reports（ベースライン ドリフト レポートの管理）］テーブルで、表示するレポート名をクリックします。
3. コンピューター ビュー モードが表示されていない場合は、［View Mode（ビューモード）］ボックスで［**Computers**（コンピューター）］をクリックします。
4. ファイル レポートを表示するコンピューターの名前の隣にある［View Details（詳細の表示）］ボタンをクリックします。そのコンピューターのドリフト ファイルのみを表示するレポートが表示されます。



コンピューター ドリフトの詳細ビューから最上位コンピューター ビューに戻る手順：

- テーブルの上の「Drift of computer（コンピューターのドリフト）」行にある［**Back to report**（レポートに戻る）］をクリックします。

ドリフト レポート結果への対応

ベースライン ドリフト レポートの結果は、ドリフトのレベルの把握から、一部またはすべてのコンピューターのセキュリティ ポリシーの変更まで、幅広い目的で使用できます。講じるアクションのほとんどは Bit9 コンソールで操作できます。ただし、見つからないファイルの復元などの一部のアクションは、手動で行う必要があります。通常は、アクションの対象になるファイルの隣のチェックボックスをオンにしてから、［Action（アクション）］メニューを使用してさまざまな対応を行います。

以下にドリフトの修復方法を示します。

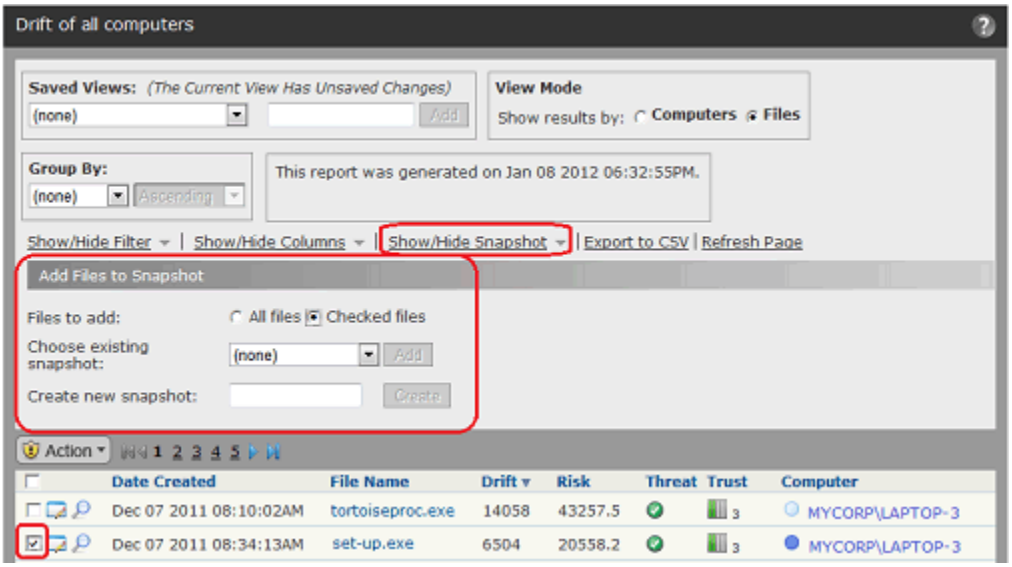
- **スナップショットへのファイルの追加：**ベースライン ドリフト レポートが 1 つ以上のスナップショットに基づいている場合は、［**Show/Hide Snapshots**（スナップショットの表示 / 非表示）］リンクをクリックすると、レポートに示されているすべてのファイル、または選択したファイルのみをスナップショットに追加できます。この場合、追加するファイルは即座にレポートから削除され、今後のレポートでは使用されなくなります。ファイル グループのチェックボックスをオンにすると、グループ内のすべてのファイルが選択したスナップショットに追加されます。
- **ファイルのローカル承認：**［Action（アクション）］メニューを使用して、ドリフト レポートでチェックボックスをオンにしたファイルに対して［**Approve locally**（ローカルで承認）］を選択できます。その結果、発見されたコンピューター上でのこのファイルの実行が許可されるだけでなく、すべての承認済みファイルを除外する（デフォルト設定）ドリフト レポートでは、今後このファイルが除外されます。
- **ローカル承認の削除：**［Action（アクション）］メニューを使用して、ドリフト レポートでチェックボックスをオンにしたローカル承認済みファイルに対して［**Remove Local Approval**（ローカル承認を削除）］を選択できます。
- **ファイルのグローバル承認または禁止：**［Action（アクション）］メニューを使用して、ドリフト レポートでチェックボックスをオンにしたファイルに対して［Globally Approve（グローバル承認）］または［Globally Ban（グローバル禁止）］を選択できます。
- **カスタム承認または禁止の作成：**［Action（アクション）］メニューを使用して、ドリフト レポートでチェックボックスをオンにしたファイルに対して［Approve by Policy（ポリシーにより承認）］または［Ban by Policy（ポリシーにより禁止）］を選択し、カスタム承認または禁止を作成できます。承認の場合は、ポリシーで承認することも、チェックボックスをオンにしたファイルをインストーラーとしてマークすることもできます。禁止の場合は、ポリシーによって禁止した上で、禁止されたファイルをブロックするか、禁止を完全に適用すればブロックされたはずのファイルをレポートするのみかを選択できます。
- **ファイル グループのメンバーの表示とメンバーへのアクション**：ファイル グループの詳細を表示する場合は、ファイル名か［View Details（詳細の表示）］ボタンをクリックして、グループ内のドリフトの原因になったファイルを含むページを表示します。このページで、ファイルを個別に承認または禁止できます。
- Bit9 コンソールの他のページと同様に、ドリフト レポートから［File Details（ファイルの詳細）］ページにドリル ダウンし、上記で説明されている多くのアクションにアクセスできます。

- **グループまたは信頼メソッドごとのファイルの承認または禁止：**ファイルを個別に承認または禁止する代わりに、ファイルのグループをインストールする元のパッケージを承認できます。ドリフト レポートにソースが同じ多くのファイルが含まれており、そのソースを信頼している場合は、公開者、アップデーター、またはユーザー別に（[Software Rules（ソフトウェア ルール）]ページで）ファイルを承認することもできます。このタイプの変更を行っても現在のレポートに影響はありませんが、レポートに承認済みファイルを含めない限り、今後生成されるこのレポート（またはその他の同様のレポート）には、この変更の対象になったファイルは表示されなくなります。
- **ファイルの追加または削除：**コンソール以外の方法で、ドリフト レポートの情報に基づいてシステムの 1 つ以上のファイルの追加または削除を行い、今後のレポートに表示されるドリフトを減らすことができます。

スナップショットへのドリフト結果の追加

[Baseline Drift Report Results（ベースライン ドリフト レポートの結果）]を表示したときに、ドリフトの追跡が不要なファイルがレポートに含まれていることがあります。ドリフト レポートで、1 つ以上のスナップショットがベースラインとして使用されている場合、ドリフト レポートに含まれているファイルをベースライン スナップショットの 1 つに追加できます。また、新しいスナップショットを作成して、このスナップショットをベースラインに追加することもできます。

このタイプの修復を行うことは、実質的に特定のドリフト結果を「今後」無視することを意味します。このドリフトを削除する（ファイル インベントリを変更する）ためにエージェントに送信されるものはなく、既存のレポート結果は変更されません。ただし、スナップショットに追加したファイル、またはベースラインに追加する新しいスナップショットに追加したファイルは、今後のドリフト レポート結果には含まれません。



ベースライン ドリフト レポートからスナップショットへのファイルの追加手順:

1. レポートで、(スナップショットにすべてのファイルを追加する場合以外は) 追加する各ファイルのチェックボックスをオンにします。
2. [**Show/Hide Snapshot**(スナップショットの表示 / 非表示)] リンクをクリックして [Add Files to Snapshot(スナップショットへのファイルの追加)] パネルを表示します。
3. [Add Files to Snapshot(スナップショットへのファイルの追加)] パネルで、[Files to add(追加するファイル)] 行の [**All files**(すべてのファイル)] または [**Checked files**(チェック済みファイル)] ラジオ ボタンをクリックします。
4. 対象のファイルを追加するスナップショットを指定します。
   a. 既存のスナップショットにファイルを追加する場合は、[Choose existing snapshot(既存のスナップショットの選択)] メニューからスナップショットを 1 つ選択し、[**Add**(追加)] をクリックします。このメニューには、現在のレポートでベースラインとして使用されているスナップショットだけでなく、使用可能なすべてのスナップショットが含まれています。
   b. 新しいスナップショットにファイルを追加する場合は、[Create new snapshot(新しいスナップショットの作成)] ボックスに名前を入力し、[**Create**(作成)] ボタンをクリックします。
5. このレポートが複数のページで構成されている場合に、チェックボックスをオンにしたファイルを追加する場合は、追加するファイルが含まれるすべてのページでこの手順を繰り返します。

注意

上記の手順は、「最新の」ドリフト レポートの実行時に、今後の結果に反映させるようにスナップショットを追加することを想定していますが、スナップショットの使用方法に制限はありません。他の目的でもスナップショットにファイルを保存できます。

レポートの作成と編集

[Add Baseline Drift Report(ベースライン ドリフト レポートの追加)] ページと [Edit Baseline Drift Report(ベースライン ドリフト レポートの編集)] ページのどちらでも、[Baseline Drift Report Details (ベースライン ドリフト レポートの詳細)] ウィンドウが使用されます (内容には多少の違いがあります)。ここでは、レポートの作成方法を説明します。レポートの編集方法も基本的に同じですが、編集の場合は既存のレポートを使用します。

ベースライン ドリフト レポートの作成手順：

［Manage Baseline Drift Reports（ベースライン ドリフト レポートの管理）］ページで、［**Add Report**（レポートの追加）］をクリックし、［Add Baseline Drift Reports（ベースライン ドリフト レポートの追加）］ページを開きます。ここで、作成するレポートの詳細を入力します。

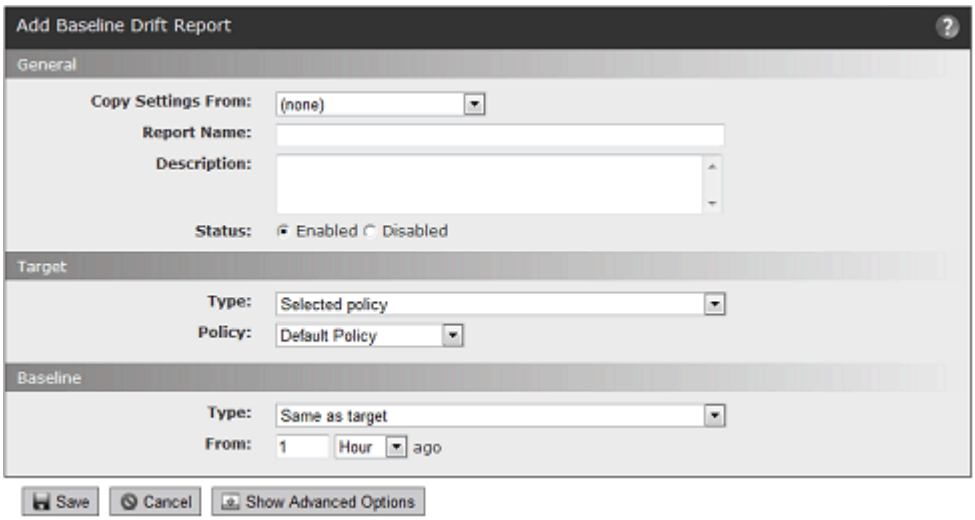
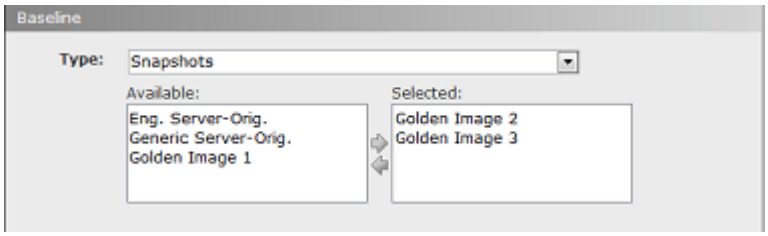


表 85：［Add/Edit Baseline Drift Report（ベースライン ドリフト レポートの追加 / 編集）］の詳細

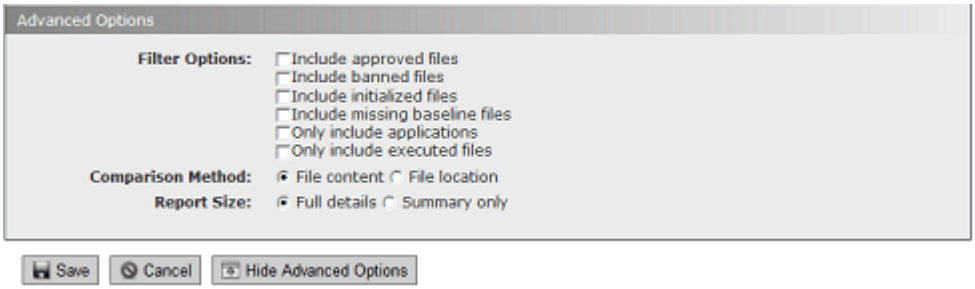
項目	説明
［Copy Settings From（設定のコピー元）］メニュー	（［Add（追加）］ページのみ）新しいレポートの詳細として入力するために、既存のレポートの設定をコピーします。このコピーには必要に応じて変更を加えることができます。このメニューでレポートを選択した場合、新しいレポートのデフォルト名は「Copy of < 既存のレポート名 >」です。
［Report name（レポート名）］	［Manage Baseline Reports（ベースライン レポートの管理）］ページ、およびこのレポートのウィンドウ バナーに表示される名前。
［Description（説明）］	（オプション）このレポートの目的を表すテキスト。
［Status（ステータス）］ラジオ ボタン	［**Enabled**（有効）］にすると、自動的にレポート結果が生成されます。［**Disabled**（無効）］にすると、レポート生成は無効になり、レポートの履歴はすべて削除されます。

項目	説明
[Target（ターゲット）] メニュー	レポートでの分析の対象。ターゲットの［Type（タイプ）］のオプションを以下に示します。 ［**Computer**（コンピューター）］– 選択されたコンピューターのすべての変更を追跡します。 ［**Computer in policy**（ポリシーのコンピューター）］– 選択されたポリシー内のすべてのコンピューターのすべてのファイル変更を追跡します。 ［**Computer Filter**（コンピューター フィルター）］– フィルターで指定された基準に一致するコンピューターのすべてのファイル変更を追跡します。 ［**Advanced Filter**（高度なフィルター）］– フィルターで指定された基準に一致するすべてのファイル変更を追跡します。この基準には、ファイルの基準とコンピューターの基準の両方を含めることができます。 ［**All Computers**（すべてのコンピューター）］– ネットワーク上のすべてのコンピューターのすべてのファイル変更を追跡します。 ［**All Computers**（すべてのコンピューター）］以外の各ターゲットタイプでは、ターゲットの指定に必要な追加のフィールドが表示されます。
[Baseline（ベースライン）] メニュー	ターゲットと比較する対象。ベースラインのオプションを以下に示します。 ［**Computer**（コンピューター）］– 指定されたコンピューターでレポートの実行時に見つかったファイルをターゲットと比較します。 ［**Computer in policy**（ポリシーのコンピューター）］– このメニューで選択されたポリシー内のすべてのコンピューターで（レポートの実行時に）見つかったファイルをターゲットと比較します。 ［**Computer Filter**（コンピューター フィルター）］– フィルターで指定された基準に一致するコンピューターのファイルをターゲットと比較します。 ［**Advanced Filter**（高度なフィルター）］– フィルターで指定された基準に一致するファイルをターゲットと比較します。この基準には、ファイルの基準とコンピューターの基準の両方を含めることができます。 ［**Snapshot**（スナップショット）］– 選択された 1 つ以上のスナップショット内のファイルをターゲットと比較します。 

項目	説明
	[**Same as target**（ターゲットと同じ）] – ターゲット コンピューター上のファイルを、過去の指定された時点の同一のコンピューター上のファイルと比較します。  [**None**（なし）] – ベースラインとの比較を行わずに、すべてのコンピューターの合計ドリフトを算出します。この選択肢の場合は、エージェントのインストール以降にターゲット マシン セットで発生したすべての変更のみを監視したレポートが生成されます。このオプションでは、見つからないファイルは追跡できません。[Advanced Options（高度なオプション）] をデフォルトのままにしている場合、このオプションを選択すると、ターゲット システム上のすべての未承認ファイルのテーブルと、ベースライン ドリフト レポートでのみ把握できる補足的なドリフトおよびリスク情報が表示されます。これらの未承認ファイルに対してアクションが必要かどうかを判断する場合や、特定のグループ、ユーザー、またはコンピューターがリスクの合計の中で過度の割合を占めていないか判断する場合は、リスクによってフィルターしたり並べ替えたりできます。 [None（なし）] 以外の各 [Type（タイプ）] オプションでは、ベースラインの指定に必要な追加のフィールドが表示されます。
[Save（保存）] ボタン	入力されたパラメーターを保存し、ベースライン ドリフト レポートを作成します。一度作成されたレポートは、無効化されない限り、スケジュールどおりに実行されます。
[Cancel（キャンセル）] ボタン	レポートの作成または編集をキャンセルします。
[Show/Hide Advanced Options（高度なオプションの表示 / 非表示）] ボタン	レポートの追加のパラメーターを表示または非表示にします。詳細については、「ベースライン ドリフト レポートの高度なオプション」を参照してください。

ベースライン ドリフト レポートの高度なオプション

［Advanced Options（高度なオプション）］セクションには、ベースライン ドリフト分析の対象にするファイルのタイプ、ベースラインとターゲットの比較メソッド、生成されるレポートの詳細レベル、およびそれに伴って決まるサイズを変更するためのオプションが含まれています。これらのオプションを変更すると、パフォーマンスに影響が及ぶ場合や、検証に必要とする以上の非常に詳細なレポートが生成される場合があります。



[Advanced Options（高度なオプション）]：[File Filter Options（ファイル フィルター オプション）]

フィルター オプションを使用すると、さまざまなタイプのファイルを選択してドリフト レポートに含めることができます。これらのオプションはすべて、デフォルトでオフになっています。これらのオプションは、ベースラインまたはターゲットの［Type（タイプ）］メニューで［Advanced Filters（高度なフィルター）］を選択して設定できるオプションのうち、よく使用する一部のオプションのショートカットとして使用できます。以下の選択肢があります。

- ［**Include approved files**（承認済みファイルを含める）］– ローカル状態が「承認済み」のファイルをベースライン ドリフト比較に含めます。
- ［**Include banned files**（禁止ファイルを含める）］– ローカル状態が「禁止」のファイルをベースライン ドリフト比較に含めます。
- ［**Include initialized files**（初期化済みファイルを含める）］– 新たにインストールされたエージェントで初期化されたファイルをベースライン ドリフト比較に含めます。
- ［**Include missing baseline files**（見つからないベースライン ファイルを含める）］– ベースライン ドリフト分析に、ベースラインには存在するがターゲット システムで見つからない（ベースラインが［Same as target（ターゲットと同じ）］のときに表示されない）ファイルの追跡を含めます。
- ［**Only include applications**（アプリケーションのみを含める）］– ネットワーク内の実行可能なファイル（.exe や .com、パッケージは除く）のみをベースライン ドリフト比較に含めます。
- ［**Only include executed files**（実行済みファイルのみを含める）］– ネットワーク内で実際に実行済みのファイルのみをベースライン ドリフト比較に含めます。

どのフィルター オプションを使用するかは、ベースライン ドリフト レポートを実行する目的によって決まります。デフォルトで含まれるのは未承認ファイルのみですが、ローカルで承認したファイルや禁止したファイルを含むベースライン ドリフト レポートを実行することもできます。この両方のオプションを使用した

場合は、関心の対象である「すべて」の新しいファイルがドリフト レポートに表示されるため、システムがゴールデン イメージまたは既知のベースラインから「ドリフトした」かどうかを確認する上で非常に役立ちます。承認した一部のファイルが承認すべきではなかったことや、禁止ファイルが大量に増殖していることが判明することがあります。禁止ファイルは実行できませんが、大量の増殖は問題です。

ローカルで禁止したファイルと承認したファイル、および見つからないベースライン ファイルを比較に含めることが役立つもう 1 つの例は、販売時点管理システムなど、システムが完全に標準に準拠する必要がある環境です。ドリフト レポートを使用して、すべてのシステムがゴールデン ディスク イメージと「厳密に」一致しているかどうかを確認することができます。

[Advanced Options（高度なオプション）]：[File Comparison Method（ファイル比較メソッド）]

ベースライン ドリフト レポートは、ファイルのコンテンツ（ハッシュ）とファイルの場所（完全なパス名）の両方を使用して、追加されたファイル、見つからないファイル、変更済みファイルを識別します。[Baseline Drift Report Details（ベースライン ドリフト レポートの詳細）] の [Advanced Options（高度なオプション）] では、これらの比較メソッドの「方法」を変更できます。

- [**File Content**（ファイル コンテンツ）] – デフォルトでは、ベースライン ドリフト レポートは比較メソッドとして「ファイル コンテンツ」を使用します。このオプションが有効になっている場合、ベースラインのファイルとターゲットのファイルのハッシュが同じであれば、2 つのファイルのパス名（場所）にかかわらずドリフトはレポートされません。場所が同じ（ベースラインとターゲットでパスおよびファイル名が同じ）でも、ハッシュが異なるファイルは、ターゲット上で変更されたと見なされ、ドリフトとしてカウントされます。ターゲットのどこにも見つからないベースラインのハッシュは「見つからないファイル」としてレポートされ、ベースラインで見つからないターゲットのハッシュは「追加されたファイル」と見なされます。
- [**File location**（ファイルの場所）] –「ファイルの場所」を選択した場合、ベースラインとターゲットの両方で同じパスとファイル名で見つかった同一のハッシュに対しては、ドリフトはレポートされません。同一の場所（パスおよびファイル名）で見つかった異なるハッシュは、「変更されたファイル」と見なされ、ドリフト数に追加されます。異なる場所で同一のハッシュが見つかっても、一致とは「見なされません」。このケースでは、ベースライン ドリフト レポートは新しいファイル（ターゲットでファイルが含まれている場所に、ベースラインではファイルが含まれていない場合）、見つからないファイル（ベースラインでファイルが含まれている場所に、ターゲットではファイルが含まれていない場合）、または変更されたファイル（ベースラインとターゲットに同一名だがハッシュが異なるファイルがある場合）をレポートします。

一部のケースでは、比較メソッドが変わっても合計ドリフトには影響しません。たとえば、ドリフト レポートで、見つからないファイルの追跡を有効化している場合です。ただしデフォルト設定のままにしてあり、かつ見つからないファイルを追跡しない場合は、異なる比較メソッドを使用すると表 86 の例に示すように異なるドリフト結果が生成される可能性があります。

表 86：例：比較メソッドの違いによるドリフトへの影響

ベースラインのファイル	ターゲットのファイル	コンテンツによるドリフト	場所によるドリフト
C:\folder1\file1（ハッシュ A）	C:\folder1\file1（ハッシュ A）	なし	なし
C:\folder1\file2（ハッシュ B）	C:\folder1\file2（ハッシュ F）	新規 1（ハッシュF）	変更 1 (file2)
C:\folder2\file3（ハッシュ C）	C:\folder2\file3（ハッシュ B）	変更 1 (file3)	見つからない 1（ハッシュ C）
C:\folder2\file4（ハッシュ D）		見つからない 1	見つからない 1
	C:\folder2\file5（ハッシュ G）	新規 1	新規 1
ドリフト合計（見つからないファイルを含む）		**4**	**4**
ドリフト合計見つからないファイルを除く（デフォルト）		**3**	**2**

[Advanced Options（高度なオプション）]：レポート詳細レベル

［Advanced Options（高度なオプション）］では、ベースライン ドリフト レポートのサイズを選択できます。デフォルトの選択肢は［Full details（完全な詳細）］で、最上位ファイルと関連するすべての個別ファイルの詳細を含むドリフト レポートが生成されます。もう一方の［Summary only（サマリーのみ）］オプションでは、最上位（ファイル グループ）の詳細を含むレポートが生成され、要求されたとき（ユーザーが詳細を表示するためにファイル グループをクリックしたとき）にのみ個別ファイルの詳細が表示されます。以下の表に、これらのオプションを選択するための考慮事項を示します。

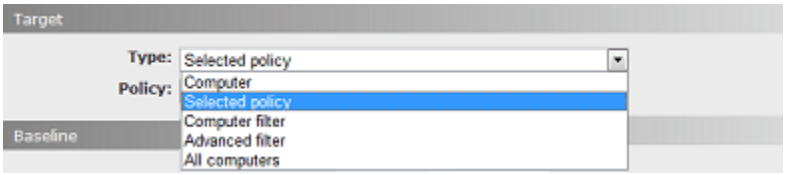
表 87：［Report Size（レポート サイズ）］オプション

違い	［Summary Only（サマリーのみ）］レポート	［Full Details（完全な詳細）］レポート
詳細レベル	最初は、ファイル グループ別の結果がレポートされます。個別ファイル レベルのレポートは、ユーザーがファイル グループをクリックしたときにオンデマンドで生成されます。	個別のファイルの詳細が含まれます。
データベース サイズ	データベース内で小さいサイズ	大きいサイズ（サマリーの約 10 倍）
作成速度	作成が速い	作成が遅い

違い	[Summary Only（サマリーのみ）] レポート	[Full Details（完全な詳細）] レポート
レポートへのアクセス速度	表示が遅い	表示が速い
ダッシュボードとの親和性	脅威、信頼度、公開者 / 会社などのファイル レベルの詳細が含まれていないため、グラフィック（ポートレット）および包括的な分析には適さない	グループ、フィルターなどを使用したグラフィック表示と分析に適している

ターゲットおよびベースラインの定義でのフィルターの使用

[Target（ターゲット）] および [Baseline（ベースライン）] の定義で使用する [Type（タイプ）] メニューには、[Computer Filters（コンピューター フィルター）] と [Advanced Filters（高度なフィルター）] の 2 種類のフィルターがあります。[Advanced Filters（高度なフィルター）] には、[Computer Filters（コンピューター フィルター）] のすべてのフィルター タイプが含まれます。タイプを選択すると、そのメニューから必要なだけ異なるフィルターを追加できます。また、同じタイプの複数のフィルターを追加することもできます。



[**Computer Filters**（コンピューター フィルター）] は、ベースラインまたはターゲットの指定に使用する唯一の基準がコンピューター関連の場合に便利です。[Computer Filter（コンピューター フィルター）] には以下のオプションがあります。

- [Computer（コンピューター）]
- [Computer tag（コンピューター タグ）]
- [IP Address（IP アドレス）]
- [Platform（プラットフォーム）]
- [Policy（ポリシー）]

このうち 2 つは [Type（タイプ）] メニューで選択肢が重複しますが、[Computer Filters（コンピューター フィルター）] タイプを使用すると、コンピューターに対して複数のフィルターを設定できます。たとえば、ポリシーが低適用レベルで、コンピューター タグが「Sales」または「Marketing」のすべてのコンピューターをベースラインに含めるように指定できます。

[**Advanced Filters**（高度なフィルター）] は、[Computer Filters（コンピューター フィルター）] メニューでは使用できない基準をベースラインまたはターゲットに含める必要があるときに便利です。[Advanced Filters（高度なフィルター）] にはコンピューター フィルターも含めることができますが、ハッシュ値、ファイル普及度、脅威レベルなど多くのファイル基準セットを使用できます。

大半のフィルターの選択肢は名前から意味がわかりますが、[File Type（ファイル タイプ）] は説明が必要です。[File Type（ファイル タイプ）] フィルターでは、ターゲットまたはベースラインに以下の選択肢を含めるか「除外する」ように指定できます。

- **[Application（アプリケーション）]:** パッケージを除くすべての実行可能ファイル（.exe、.com など）
- **[Supporting File（サポート ファイル）]:** 実行可能ファイルによってロードされた任意のライブラリ（.dll、.ocx、.sys など）
- **[Package（パッケージ）]:** 任意のインストーラー（コンテンツを含む .exe。自己解凍 zip、セットアップ プログラムなど）
- **[Script File（スクリプト ファイル）]:** 任意のスクリプトまたはバッチ ファイル（.bat、.vbs、.wsf など）
- **[Other（その他）]:** 今後使用するために予約されているタイプ
- **[Unrecognized Executed File（未確認の実行済みファイル）]:** 初期化中にもその後の分析でも Bit9 によって実行可能ファイルとして特定されなかったが、特定のプロセスによって実行が試みられたファイル。この実行の試みによって、このファイルは追跡および管理のために Bit9 コンソールのファイル リストに追加されました。
- **[Unknown（不明）]:** ファイル タイプ情報を提供しない古い Bit9 エージェントによってレポートされたファイル

マルチプラットフォーム環境でのドリフト

Bit9 Security Platform は、Windows、Mac、および Linux コンピューターへのエージェントのインストールをサポートしています。異なるオペレーティング システムでは異なるプラットフォーム ソフトウェアやアプリケーションが見つかるため、ドリフトの計測にこうした異なるコンピューターを混在させても意味がありません。この「ノイズ」レベルによって、有益なデータの抽出が難しくなります。すべてのコンピューター、または 1 つのポリシー内のすべてのコンピューターを（ポリシーがプラットフォーム固有の場合を除き）ドリフト レポートでターゲットにすることは推奨しません。

マルチプラットフォーム環境を運用している場合は、以下の方法で有益な結果を生成するレポートを定義できます。

- [Baseline（ベースライン）] の [Type（タイプ）] として [**None**（なし）] を選択します。この選択肢の場合は、エージェントのインストール以降にターゲット マシン セットで発生したすべての変更を監視したレポート（見つからないファイルは追跡しない）が生成されます。デフォルトでは、ターゲット システム上のすべての未承認ファイルの一覧と、補足的なドリフトおよびリスク情報が表示されます。
- [Baseline（ベースライン）] の [Type（タイプ）] として [**Same as Target**（ターゲットと同じ）] を選択します。この選択肢の場合は、各コンピューターをそれ自体と比較したドリフトのみを表示するレポートが生成されます。
- 他のベースライン タイプを選択する場合は、[Target（ターゲット）] メニューで [Advanced Filter（高度なフィルター）] または [Computer Filter（コンピューター フィルター）] を選択し、そのフィルターにプラットフォームを指定することによって、プラットフォームごとに 1 つのドリフト レポートを生成できます。

ドリフト レポートのパラメーターの指定方法の詳細については、「ベースライン ドリフト レポートの作成手順：」（653 ページ）を参照してください。

スナップショットの管理

スナップショットは、1 台以上のコンピューターから取得したファイルのリスト（名前、ハッシュ、場所など）です。ドリフト レポートのベースラインとして、1 つのスナップショット、またはスナップショットの組み合わせを使用できます。フィルターを使用して必要なファイルの正確なリストを作成してから、そのファイル リストのスナップショットを作成します。Bit9 コンソールでは、いくつかの場所でスナップショットを作成できます。スナップショットを作成した後で、必要に応じてスナップショットへのファイルの追加や削除を行うことができます。

スナップショットの作成、変更、削除を実行できるのは、PowerUser、Administrator、およびスナップショットの表示および管理権限を持つカスタム グループのユーザーのみです。

プラットフォームに関する注意：単一のスナップショットに複数のオペレーティング システム プラットフォーム（Windows、Mac、Linux など）のファイルを混在させることは推奨されません。

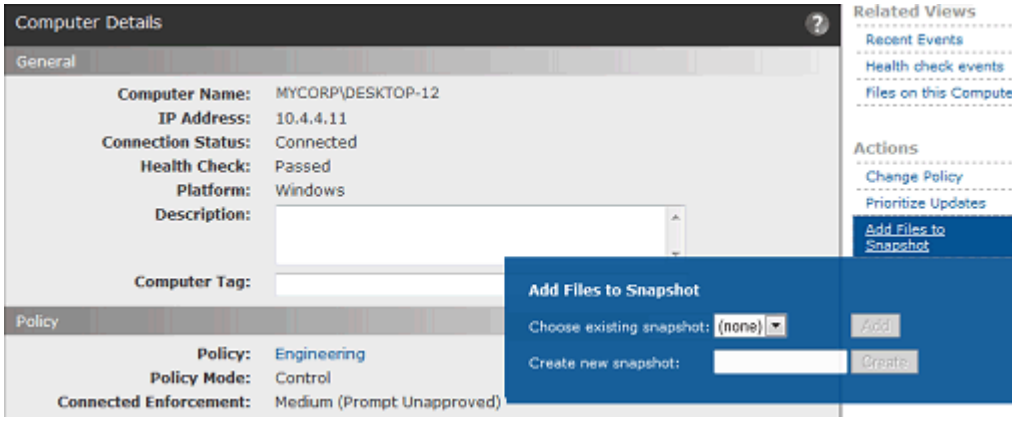
スナップショットの作成と変更

新しいスナップショットは、主に次の 2 つの方法で作成できます。

- 特定のコンピューターのすべてのファイルを使用する
- ［Snapshot（スナップショット）］ボタンがあるコンソール ページ上の、フィルター済みまたは未フィルターのファイル テーブルを使用する

1 台のコンピューターのすべてのファイルからスナップショットを作成する（またはスナップショットに追加する）手順：

1. コンソール　メニューで、［**Assets**（アセット）］>［**Computers**（コンピューター)］の順に選択します。
2. ［Computers（コンピューター)］テーブルで、スナップショットとして使用するファイルが含まれるコンピューターの名前をクリックします。そのコンピューターの［Computer Details（コンピューターの詳細)］ページが開きます。
3. この詳細ページの右にある［Action（アクション)］メニューで、［Add Files to Snapshot（スナップショットへのファイルの追加)］をクリックします。［Add Files to Snapshot（スナップショットへのファイルの追加)］ダイアログが表示されます。



4. 「新しいスナップショットを作成」する場合は、このダイアログで［Create new snapshot（新しいスナップショットの作成）］ボックスにスナップショットの名前を入力し、［**Create**（作成）］をクリックします。
   または
   このコンピューターのすべてのファイルを既存のスナップショットに「追加」する場合は、［Choose existing snapshot（既存のスナップショットの選択）］メニューから既存のスナップショットを選択し、［**Add**（追加）］をクリックします。

   スナップショットの作成または追加を確認するメッセージが表示されます。
5. スナップショットの内容を表示するには、コンソール メニューから［**Reports**（レポート）］>［**Baseline Drift**（ベースライン ドリフト）］を選択し、［Snapshot（スナップショット）］タブをクリックします。
   スナップショットのテーブルに新しい、または変更されたスナップショットが表示されます。

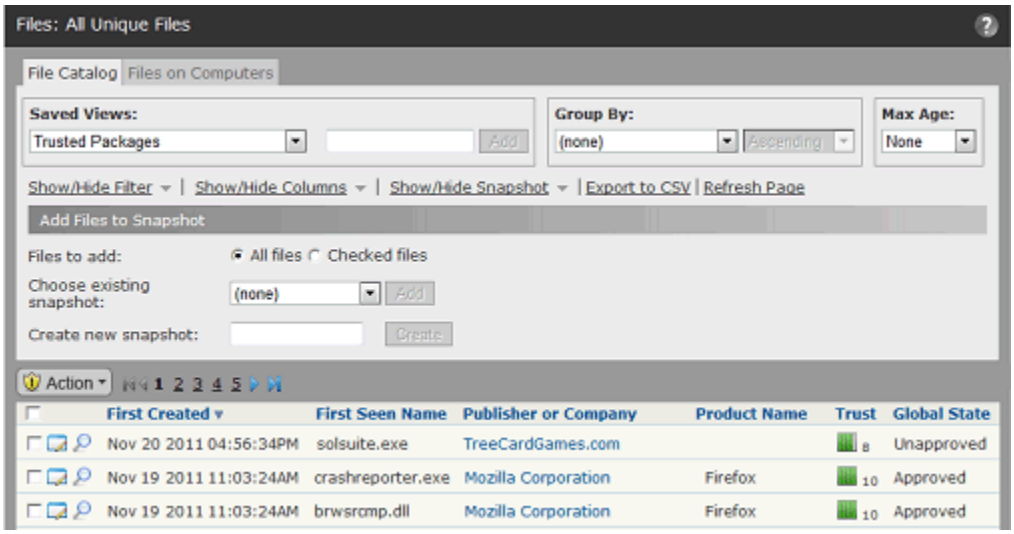
注意

コンピューター上のファイルの「スナップショット」は静的で、スナップショットが作成された時点でコンピューター上に存在したファイルのリストです。コンピューター自体を比較のベースラインとして使用することもできます。その場合は、「レポートを実行した時点」でのコンピューター上のファイルがベースラインになります。

ファイル テーブルからスナップショットを作成する（またはファイルをスナップショットに追加する）手順：

1. スナップショットの作成を実行するコンンソール ページに移動します。
   たとえば、コンソール メニューで［**Assets**（アセット）］>［**Files**（ファイル）］を選択して［Files（ファイル）］ページに移動し、［**File Catalog**（ファイル カタログ）］をクリックします。
2. スナップショットに含めるファイルのリストを取得するために、必要に応じてタブ、フィルター、列、保存済みビューを選択します。

3. ［**Show/Hide Snapshot**（スナップショットの表示 / 非表示）］リンクをクリックして［Snapshot（スナップショット）］パネルを表示します。



4. スナップショットに追加するファイルを個別に選択する場合は、追加する各ファイルの左のチェックボックスをオンにし、［Add Files to Snapshot（スナップショットにファイルを追加）］パネルの［Files to add（追加するファイル）］行で［**Checked files**（チェック済みファイル）］ラジオ ボタンをクリックします。このラジオ ボタンをクリックしないと、このページのすべてのファイルがスナップショットに追加されます。

5. 新しいスナップショットを作成するには、［Create new snapshot（新しいスナップショットの作成）］ボックスにスナップショットの名前を入力し、［**Create**（作成）］をクリックします。現在のファイル テーブルから新しいスナップショットが作成されます。現在表示中のページだけでなく、このテーブルの「すべて」のページのファイルがスナップショットに含まれます。
または
現在のテーブルのすべてのファイルを「既存」のスナップショットに追加するには、［Choose existing snapshot（既存のスナップショットの選択）］メニューから該当のスナップショットを選択し、［**Add**（追加）］をクリックします。.

6. ［Checked files（チェック済みファイル）］を選択する場合は、テーブルの各ページでファイルを確認して追加する必要があります。そうしない場合、現在表示されているページでチェック済みのファイルのみが追加されます。

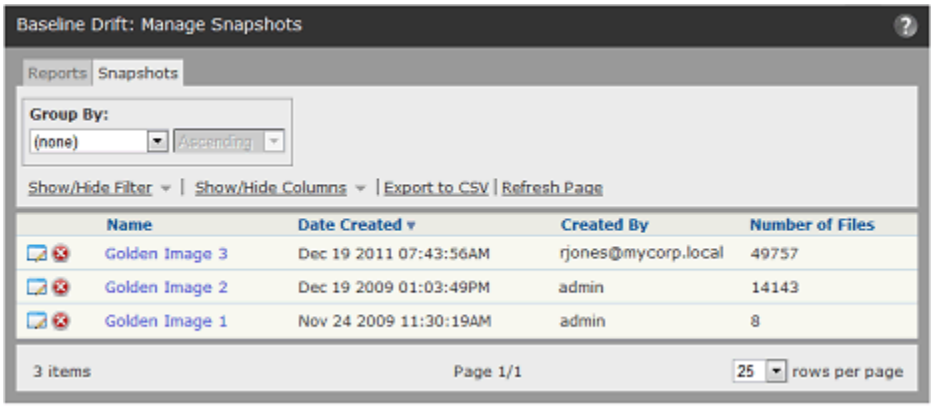
7. 新しいスナップショットが作成されたことを確認するには、コンソール メニューから［**Reports**（レポート）］>［**Baseline Drift**（ベースライン ドリフト）］を選択し、次に［**Snapshot**（スナップショット）］タブをクリックします。スナップショットのテーブルに新しいスナップショットが表示されるはずです。

スナップショットの表示と編集

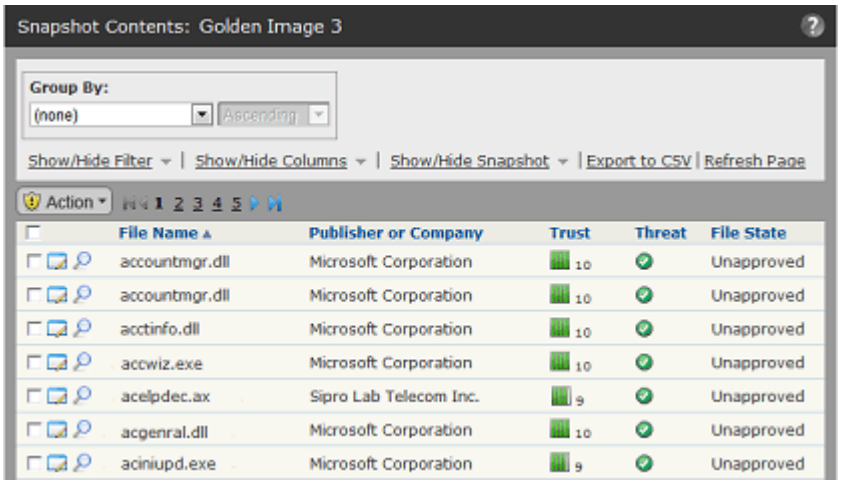
作成されたスナップショットは、[Baseline Drift（ベースライン ドリフト）] ページの [Snapshot（スナップショット）] タブに表示されます。

スナップショットの表示手順：

1. コンソール メニューで、[**Report**（レポート）] > [**Baseline Drift**（ベースライン ドリフト）] の順に選択します。
2. [Baseline Drift（ベースライン ドリフト）] ページで [**Snapshot**（スナップショット）] タブをクリックします。



3. 表示するスナップショットの名前、またはその行の [View Details（詳細の表示）] ボタンをクリックします。 [Snapshot Contents（スナップショットの内容）] ページが開き、スナップショット内のすべてのファイルを示すテーブルが表示されます。



[Snapshot Contents（スナップショットの内容）] ページから、任意の標準テーブル ツール（フィルター、列コントロールなど）を使用してスナップショット内のファイルのビューを変更できます。

スナップショット内のファイルの管理

スナップショット内の 1 つ以上のファイルのチェックボックスをオンにして、以下のアクションを実行することができます。

- **チェックボックスがオンのファイルをスナップショットから削除する**–［Action（アクション）］メニューから［**Remove from Snapshot**（スナップショットからの削除）］を選択したときにチェックボックスがオンのファイルは、スナップショットから削除されますが、ネットワーク内のコンピューターからは削除されません。
- **ファイルの承認または禁止** –［Action（アクション）］メニューから、スナップショット内のチェックボックスがオンのファイルに対するグローバルまたはカスタムの承認または禁止を作成するコマンドを使用できます。ただし、特定のファイルを処理する場合は、さらに効率的かつ柔軟に承認する方法があります。たとえば、その公開者、またはファイルを生成したインストーラーによってファイルを承認できます。
- **Bit9 SRS で分析** –［Action（アクション）］メニューから［**Analyze**（分析）］を選択したときにチェックボックスがオンのファイルについて、Bit9 SRS が提供するこれらのファイルに関する情報が取得されます。

スナップショットの削除

［Baseline Drift（ベースライン ドリフト）］ページの［Snapshot（スナップショット）］タブで、不要になったスナップショットを削除できます。削除する前に、そのスナップショットが不要かどうか、ファイルの追加や削除によって活用できないかどうかを十分に検討してください。削除したスナップショットは復元できません。

スナップショットの削除手順：

1. コンソール メニューで、［**Reports**（レポート）］>［**Baseline Drift**（ベースライン ドリフト）］の順に選択します。
2. ［Baseline Drift（ベースライン ドリフト）］ページで、［**Snapshot**（スナップショット）］タブをクリックします。
   ［Snapshot（スナップショット）］タブは、少なくとも 1 つのスナップショットが保存されるまで表示されません。
3. 削除するスナップショットの行の［Delete（削除）］ボタンをクリックし、確認ボックスで **[OK]** をクリックします。

グラフでのベースライン ドリフト レポートの表示

［Baseline Drift（ベースライン ドリフト）］ページのテーブルには、ドリフト結果のすべての詳細を柔軟に表示できますが、ネットワーク内のファイル変更を手軽に参照できる指標として、ドリフトをグラフィック表示することもできます。ベースライン ドリフト レポートのグラフは、コンソールの「ダッシュボード」ページにグラフィック「ポートレット」として表示できます。

Bit9 コンソールには、ダッシュボードとして個別のグラフを表示し、ベースライン ドリフト情報を提供する事前構成済みのポートレットが含まれています。

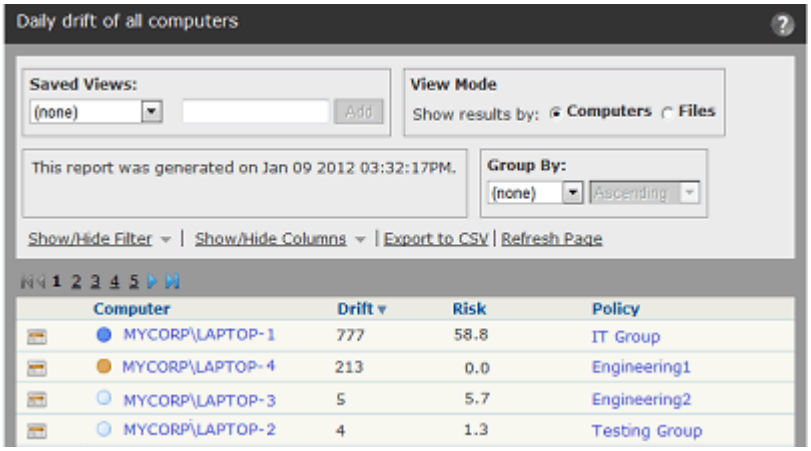
「Drift（ドリフト）」がタイトルに含まれるいずれかのポートレットを選択すると、ドリフト情報のグラフィック表示の例を確認できます。

独自のドリフト ポートレットを作成する場合は、有益な情報を表示できるように、以下のヒントを参考にしてください。

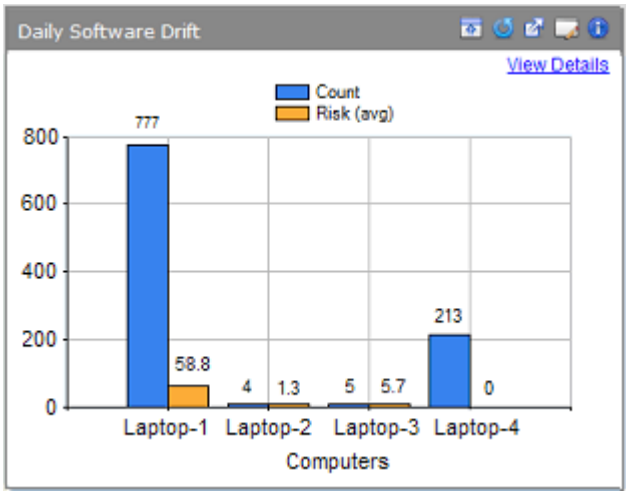
- ポートレットの横のサイズは、ポートレットが表示されるダッシュボードのレイアウトによって変化します。ベースライン ドリフト ポートレットにデータを収めるために、ダッシュボード上でポートレットを移動したり、ダッシュボードのレイアウトを変更したりすることが必要になることもあります。このポートレットがプレゼンテーションに適した形式になるように、表示するデータやグラフのタイプを選択することもできます。
- X 軸に表示する項目数を考慮してください。Portlet Editor では、X 軸に表示する項目を最大値または最小値から 5、10、または 15 個に制限できますが、制限するとレポートのすべてのデータを確認することはできません。そのため、たとえば 1000 台のコンピューターが存在する場合には、「コンピューター」別でなく「ポリシー」別のドリフトの表示を選択します。コンソール テーブルでは、いつでもさらに詳細なデータにドリル ダウンできます。（ポートレットの［Split by（分割の基準）］機能を使用する場合は、ポートレット内の棒、列、またはその他の要素を分割する項目数を同様に制限する必要があります。）
- Portlet Editor のプレビュー機能を使用して、データがどのように表示されるかを確認します。ポートレットを保存する前に、表示オプションを必要なだけ試すことができます。
- ベースライン ドリフト レポートのサイズが［Summary Only（サマリーのみ）］（レポートの作成または編集時の［Advanced Options（高度なオプション）］）のオプション）の場合、ドリフト レポートにはダッシュボードで必要な量のデータが得られません。グラフを表示できるのは、レポート サイズが［Full Details（完全な詳細）］のレポートのみです。

以下の例は、同一の情報を［Baseline Drift Report Results（ベースライン ドリフト レポートの結果）］テーブルとグラフィック ポートレットに表示したものです。Bit9 エージェント コンピューターが 5 台以下のデモンストレーション システムならば、コンピューター別ドリフトを容易にグラフで表示できます。ただし、これは本番環境には適しません。

テーブル形式では、ドリフト レポートは以下の図のようになります。



上記と同じ情報が、ダッシュボードには以下の図のように表示されます。[View Details（ビューの詳細）] ボタンをクリックすると、完全なレポート テーブルに戻ります。



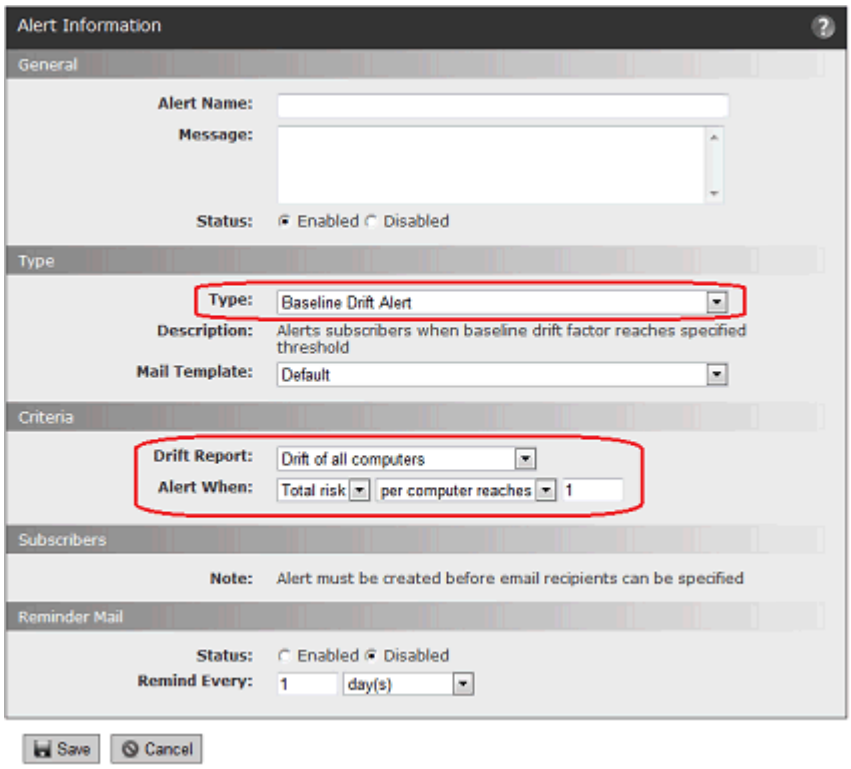
ダッシュボードの詳細については、「ダッシュボードの使用とカスタマイズ」（693 ページ）を参照してください。

ベースライン ドリフト アラートの作成

アラートを作成して、ベース ドリフトが設定済みのしきい値を超えたときに管理者や他のコンソール ユーザーに通知することができます。ベースライン ドリフト アラートを有効化すると、レポート生成が完了するたびにトリガー条件が検証されます。

ベースライン ドリフト アラートの作成手順：

1. コンソール メニューで、[**Tools**（ツール）] > [**Alerts**（アラート）] の順に選択します。[Alerts（アラート）] ページが開き、すべての構成済みアラートのリストが表示されます。
2. [Alerts（アラート）] ページで、[**Add Alert**（アラートの追加）] ボタンをクリックします。[Alert Information（アラート情報）] ページが表示されます。



3. ［Alert Information（アラート情報）］ウィンドウの［General（一般）］パネルで、［Alert name（アラート名）］と［Message（メッセージ）］（アラートがトリガーされたときにサブスクライバーに送信する内容）を入力します。
4. ［Type（タイプ）］パネルで、［Type（タイプ）］メニューの［**Baseline Drift Alert**（ベースライン ドリフト レポート）］を選択します。
5. ［Criteria（基準）］パネルで、このアラートでデータを監視するドリフト レポートを選択します。
   注意：ドリフト レポートがまだ作成されていない場合、［Drift Report（ドリフト レポート）］行にメニューは表示されず、レポートが未作成であることを知らせるメッセージが表示されます。
6. ［Alert When（アラートのタイミング）］行で、アラートをトリガーするしきい値パラメーターを選択します。
7. ［**Save**（保存）］をクリックしてアラートを作成します。
8. ［Alerts（アラート）］ページで、新しいアラート名の隣にある［View Details（詳細の表示）］（鉛筆とファイル）ボタンをクリックします。
9. ［Alert Information（アラート情報）］ページの［Subscribers（サブスクライバー）］セクションで、アラート E メールを送信する E メール アドレスを入力します。1 つのアドレスごとに［**Add**（追加）］をクリックします。
10. Eメール形式を指定する場合は、アドレス ボックスの右のメニューから選択します。

11. アラートがリセットされていない限りアラートを定期的に再送信する場合は、[Reminder Mail（リマインダー メール）] を [**Enabled**（有効）] に設定し、間隔を選択します。
12. [**Save**（保存）] をクリックします。

トリガー条件を満たすベースライン ドリフト条件が発生するたびに、[Home Page（ホームページ）] ダッシュボードと [Alerts（アラート）] ページの両方で該当のアラートが色でハイライト表示され、[Reset（リセット）] ボタンが追加されます。また、このアラートのすべてのサブスクライバーに、この状況に関する E メールが送信されます。アラートを手動でリセットするには、[Alerts（アラート）] ページで、該当するアラート名の隣の [Reset（リセット）] ボタンをクリックします。ベースライン ドリフト アラートは、指定したドリフト レポートのドリフトが、指定したパラメーター（ユーザー、コンピューター、またはポリシー）のしきい値を下回ると自動的にリセットされます。

アラートの動作の詳細については、「Bit9 アラートの使用」（606 ページ）を参照してください。

第 20 章

高度な脅威検出

この章では、Bit9 の高度な脅威の痕跡を有効にして使用する方法と、Bit9 イベント、ファイル詳細、およびアラートによる脅威の監視方法について説明します。

セクション

概要

Bit9 Security Platform は、エンドポイントでのアクティビティの監視を支援する多くの機能を備えています。これらの機能を拡張するために、Bit9 では、次のような高度な検出機能を用意しています。

- **高度な脅威の痕跡 (ATI)**。Bit9 Server にレポートしているシステムにおいて特に脅威となるアクティビティや疑わしいアクティビティの検出を支援する、痕跡セット内でグループ化されたルール。
- **検出ビュー**。Bit9 データベースの内容を表示し、ATI およびその他の Bit9 Security Platform 機能によって提供される検出関連データに注目することができます。

高度な脅威の痕跡は、エンドポイントでのイベントまたは一連の条件に基づいて、悪意のあるアクティビティを示すことができます。これにより、ファイルやレジストリ設定が存在しているという事実を後からレポートするだけの侵入の痕跡 (IOC) など、ある一時点でのスナップショットだけに頼る検出システムよりも、対象範囲を広げて早期に警告を出すことができます。高度な検出では実装の一部として動的イベントも使用するため、疑わしいファイルの作成など、疑わしいアクティビティの兆候をリアルタイムで示し、関連するイベントのメタデータを取得できます。

ATI はレポート目的にのみ使用できますが、他の Bit9 機能や Bit9 コンソール以外のアクションを使用して、検出された脅威から修復することができます。たとえば、脅威としてレポートされたファイルをブロックしたり、特定の場所で特定のプロセスによって実行されたアクションをブロックするカスタム ルールを作成したりすることができます。また、Bit9 イベント ルール機能を使用すると、脅威関連イベントで出現する「あらゆる」ファイルを直ちにブロックすることができます。

次に、高度な脅威検出を使用する手順の要約を示します。

- **検出用の痕跡セットの有効化** – コンソールの［Indicator Sets（痕跡セット）］ページ（［Rules（ルール）］>［Indicator Sets（痕跡セット）］の順に選択）で、使用する痕跡セットを有効にします。サーバーで痕跡セットを有効にすると ATI がすべてのエージェントにコミットされ、いずれかの ATI によって指定された条件が発生すると新しいイベントがサーバーに送信されます。「脅威検出のための痕跡セット」（673 ページ）を参照してください。
- **脅威レポートの監視** –［Events（イベント）］ページおよび［Files（ファイル）］ページの［Saved Views（保存済みビュー）］を使用して、疑わしいまたは脅威となるイベントやファイルがないか定期的に確認します。「脅威レポートの監視」（683 ページ）を参照してください。
- **レポートの微調整** – レポートが不要な検出関連イベントが表示される場合は、そのイベントを検出した痕跡セットを無効にするか（その痕跡セットからのレポートが一切不要であることが確かな場合）、イベントでレポートされた特定のファイルについて痕跡の例外を作成します。「痕跡セットの例外」（677 ページ）を参照してください。一方、優先度が高いと考えられる検出関連イベントが表示される場合は、そのイベントに対するアラートの作成を検討します。「脅威関連アラート」（688 ページ）を参照してください。
- **脅威からの修復** – 修復を必要とする脅威が表示される場合は、脅威によって悪意のあるアクションが実行されないように Bit9 ルール（禁止、カスタム ルール、またはイベント ルールなど）の作成を検討するか、Bit9 の範囲外でアク

ション（ファイルの削除、ファイアウォールの作成など）を実行するか、あるいはその両方によって脅威に対応します。「脅威への対応」（689 ページ）を参照してください。

ATI は（無効でなければ）どの適用レベルでもエージェントと連動しますが、高適用レベルでは、脅威検出の原因となる条件が発生する可能性は低くなります。

アップグレードに関する注意

Bit9 7.0.0 または 7.0.1 で高度な検出機能を別途インストールして使用していた場合、Bit9 Security Platform v7.2.3 では ATI がアップデーターではなく痕跡セットにグループ化されていることに注意してください。つまり、痕跡の表示、有効化、または無効化は［Indicator Sets（痕跡セット）］ページで行います。また、このような以前の 7.0.x リリースで ATI 関連のイベント ルールを作成してある場合は、7.2.3 の実装を反映した新しいイベント ルールを作成する必要があります。ただし、以前の ATI によってレポートされた脅威は、［Events（イベント）］ページの保存済みビュー（［Threat Reports - Legacy（脅威レポート – 従来）］）で表示されます。

新しいバージョンの検出に変換するために必要なすべての手順の説明と、使用可能な最新の ATI を使用しているかどうかを確認する手順については、このリリースの『Bit9 Security Platform Release Notes（Bit9 Security Platform リリース ノート）』を参照してください。

脅威検出のための痕跡セット

痕跡セットとは、その名前が示すカテゴリに属する、またはプラットフォーム用の ATI のグループ（検出ルール）です。痕跡セットを表示し、管理するには、コンソール ユーザーの Manage indicator sets（痕跡セットの管理）権限が有効である必要があります。この権限は、Administrator と PowerUser ではデフォルトで有効です。ユーザー権限の有効化の詳細については、「アカウント グループの権限」（108 ページ）を参照してください。

v7.2.0 の最初のリリースで提供されたデフォルトの痕跡セットと、それに含まれる ATI のタイプを以下に示します。クラウドベースの更新または Bit9 Security Platform の将来のバージョンで、痕跡セットは追加、削除、変更される可能性があります。詳細については、「痕跡セットに対する更新」（682 ページ）を参照してください。

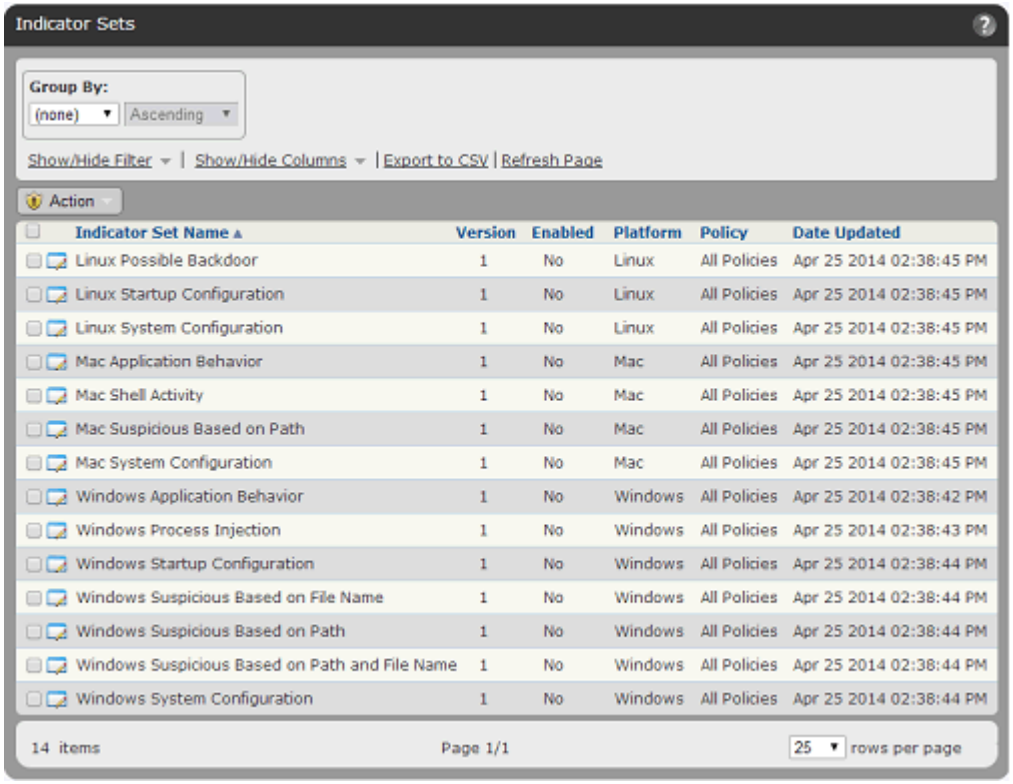
- ［**Windows Application Behavior**（Windows アプリケーションの動作）］– このグループの ATI では、特定のアプリケーションのタイプでは通常予想されない動作が検出されます。たとえば、このグループにある「Possible exploit of document handling application（文書処理アプリケーションの悪用の可能性）」という ATI では、Microsoft Excel などのアプリケーションによって未知の実行可能ファイル（foo.exe など）が作成される場合に、イベントがレポートされます。
- ［**Windows Process Injection**（Windows プロセス挿入）］– このグループの ATI では、特定のシステム プロセスへの疑わしいコードの挿入が検出されます。たとえば、このグループにある「Possible password hash tool execution（パスワー

ド ハッシュ ツール実行の可能性)」という ATI では、システムでキャッシュに保存されたパスワード ハッシュをプロセスが収集しようとする場合に、イベントがレポートされます。この痕跡セットでは通常、メモリ ルールに関連する問題がレポートされます。

- [**Windows Startup Configuration**(Windows スタートアップ構成)]– このグループの ATI では、Windows スタートアップ構成に対する疑わしい変更が検出されます。
- [**Windows Suspicious Based on File Name**(Windows 疑わしいファイル名)]– このグループの ATI では、疑わしいファイルまたは悪意のあるファイルを示すファイル名が検出されます。たとえば、ファイルの名前や拡張子が、正規のファイル(「iexplore.exe」など)に類似していて多少変更されている(「Lexplore.exe」など)場合、このグループの ATI によってそのファイルがレポートされます。既知のマルウェアの名前や拡張子を持つファイルもレポートされます。
- [**Windows Suspicious Based on Path**(Windows 疑わしいパス)] – このグループの ATI では、ごみ箱またはシステム ボリュームでのファイルの実行など、疑わしい場所でのファイルのアクティビティが検出されます。
- [**Windows Suspicious Based on Path and File Name**(Windows 疑わしいパスとファイル名)] – このグループの ATI では、ファイルのパスとファイル名の両方に基づいて、疑わしいアクティビティが検出されます。たとえば、システム フォルダー以外で実行されているシステム ファイルをレポートする ATI があります。このグループの別の痕跡では、ほとんど使用されないシステム ユーティリティの実行がレポートされます。
- [**Windows System Configuration**(Windows システム構成)] – このグループの ATI では、ファイアウォールや名前解決の改ざん、言語パックのインストールなど、疑わしいシステム構成アクティビティが検出されます。
- [**Mac Application Behavior**(Mac アプリケーションの動作)] – このグループの ATI では、特定のアプリケーションのタイプでは通常予想されない動作が検出されます。たとえば、このグループの ATI には、Microsoft Excel などのアプリケーションによって未知の実行可能ファイルが作成される場合に、イベントをレポートするものがあります。このグループの別の ATI では、ブラウザーからのシェルの生成を検出します。
- [**Mac Shell Activity**(Mac シェル アクティビティ)]– このグループの ATI では、コマンド シェルの疑わしい使用が検出されます。
- [**Mac Suspicious Based on Path**(Mac 疑わしいパス)] – このグループの ATI では、ゴミ箱フォルダーからの実行の試行など、アクティビティが試行される場所に基づいて、疑わしいアクティビティが検出されます。
- [**Mac System Configuration**(Mac システム構成)] – このグループの ATI では、権限の昇格の試行など、システム構成に対する疑わしい変更が検出されます。
- [**Linux Possible Backdoor**(Linux バックドアの可能性)] – このグループの ATI では、Linux セキュア シェルへのバックドアに関連するファイルが検出されます。
- [**Linux Startup Configuration**(Linux スタートアップ構成)] – このグループの ATI では、Linux スタートアップ構成に対する疑わしい変更が検出されます。
- **Linux System Configuration**(Linux システム構成) – このグループの ATI では、名前解決の改ざんなど、Linux スタートアップ構成に対する疑わしい変更が検出されます。

痕跡セットの表示、有効化、無効化の手順：

1. コンソール メニューで、[**Rules**（ルール）] > [**Indicator Sets**（痕跡セット）] の順に選択します。[Indicator Sets（痕跡セット）] ページが表示されます。



2. 有効にする各痕跡セットの名前の横にあるチェックボックスをオンにし、[**Enable Indicator Sets**（痕跡セットの有効化）] を選択します。
   または
   無効にする各痕跡セットの名前の横にあるチェックボックスをオンにし、[**Disable Indicator Sets**（痕跡セットの無効化）] を選択します。

3. 1 つの痕跡セットの詳細および例外を表示するには、テーブルで痕跡セットの名前の横にある［View Details（詳細の表示）］ボタンをクリックします。

最初は、すべての痕跡セットが無効になっています。これらのルール グループを選択して、有効または無効にすることができます。たとえば、使用中の環境で、ある痕跡セットによって関心のないイベントがあまりにも多く生成される場合は、［Indicator Sets（痕跡セット）］ページでその痕跡セットをオフにすることができます。また、セットの痕跡をすべて無効にはしないで、痕跡セットの例外を作成することもできます。詳細については、「痕跡セットの例外」（677 ページ）を参照してください。

他の Bit9 テーブルと同様に、［Group By（グループ別）］メニュー、［Show/Hide Filter（フィルターの表示 / 非表示）］リンク、および［Show/Hide Columns（列の表示 / 非表示）］リンクを使用して、［Indicator Sets（痕跡セット テーブル）］のビューを変更できます。表 88、「痕跡セットのパラメーター」（677 ページ）では、すべての使用可能な列について説明しています。

痕跡セットの詳細

［Indicator Sets（痕跡セット）］テーブルで、セットの名前の横にある［View Details（詳細の表示）］ボタンをクリックすると、そのセットの［Indicater Set Details（痕跡セットの詳細）］ページが開きます。このページには、次の項目があります。

- 名前、バージョン、履歴など、痕跡セットについての重要な詳細
- 痕跡セットを有効および無効にしたり、痕跡セットをアクティブにするポリシーを指定したりするラジオ ボタンおよびチェックボックス
- 痕跡セットの例外を表示し、有効化、無効化、削除を実行できる［Exceptions（例外）］パネル
- この痕跡セットに関連する最近のイベントを表示するようにフィルターされた［Events（イベント）］ページを開く、［Related Views（関連ビュー）］メニューの［Recent Events（最近のイベント）］リンク

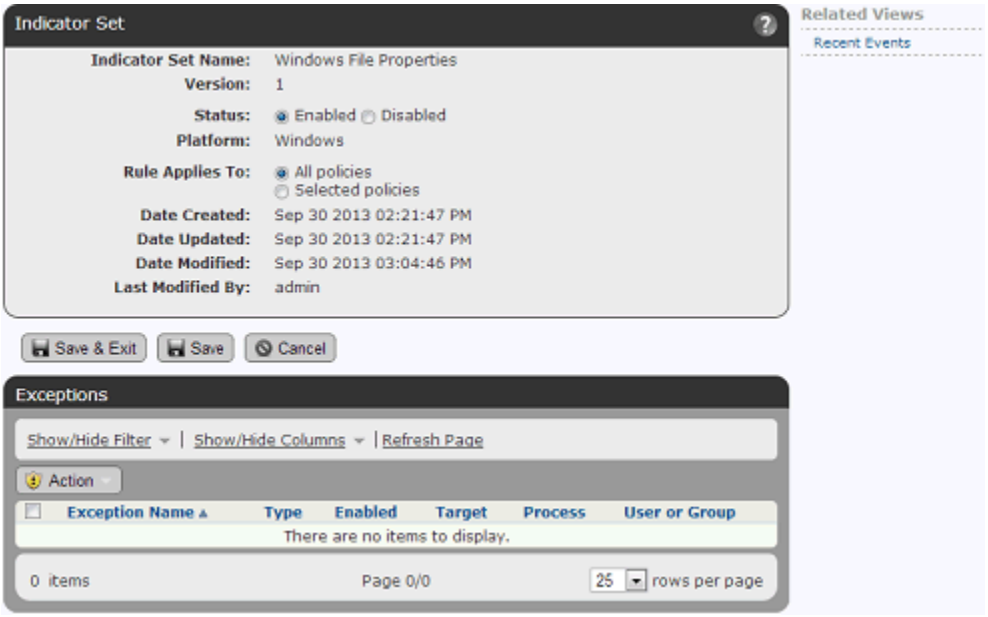


表 88 に、［Indicator Sets（痕跡セット）］テーブルと［Indicator Set Details（痕跡セットの詳細）］ページで使用可能なフィールドを示します。

表 88：痕跡セットのパラメーター

フィールド	説明
[**Indicator Set Name（痕跡セット名）**]	痕跡セットの名前。名前は Bit9 によって割り当てられ、プラットフォームと、セット内の ATI の一般的な目的で構成されます。
[**Version（バージョン）**]	この痕跡セットのバージョン。新しいバージョンが Bit9 クラウドからダウンロードされている場合は、バージョン番号が大きくなることでそれが示されます。
[**Status（ステータス）**]（[Details（詳細）] ページ） [**Enabled**（有効化）]（テーブル）	[Details（詳細）] ページで［Status（ステータス）］ラジオ ボタンを使用して、この痕跡セットを有効または無効にすることができます。［Indicator Sets（痕跡セット）］テーブルでは、［Enabled（有効化）］フィールドに［Yes（はい）］または［No（いいえ）］が表示されます。
[**Platform（プラットフォーム）**]	この痕跡セットが有効となるプラットフォーム（Windows、Mac、または Linux）。
[**Rule Applies To（ルールの適用先）**]（[Details（詳細）] ページ） [**Policy（ポリシー）**]（テーブル）	[Details（詳細）] ページでラジオ ボタンを使用すると、ルールを［All policies（すべてのポリシー）］または［Selected policies（選択されたポリシー）］に適用できます。［Selected policies（選択されたポリシー）］を選択すると、Bit9 Server 上の各ポリシーがチェックボックスとともに表示されます。 ［Indicator Sets（痕跡セット）］テーブルでは、［Policy（ポリシー）］フィールドに、セットが有効になっているポリシーが表示されます。
[**Date Created（作成日）**]	この Bit9 Server でこの痕跡セットが最初に確認された日時。
[**Date Updated（更新日）**]	この痕跡セットが最後に新しいバージョンに更新された日時。この痕跡セットに対して更新がなかった場合は、［Date Created（作成日）］と同じです。
[**Date Modified（変更日）**]	痕跡セット構成に対して最後に「ユーザーが実行した」変更の日時。これには、痕跡セットの有効化または無効化、および痕跡セットの適用先のポリシーに対する変更が含まれます。
[**Last Modified By（最終変更者）**]	この痕跡セットの編集可能なパラメーターに対して最新の変更を行った Bit9 コンソール ユーザー。
[**Exceptions（例外）**] パネル （[Details（詳細）] ページのみ）	[Details（詳細）] ページのこのパネルには、この痕跡セットに対して適用された例外の一覧が表示されます。例外の詳細については「痕跡セットの例外」（677 ページ）を、痕跡セットの例外のパラメーターに関する説明については表 89、「例外の詳細（痕跡セット内）」（681 ページ）を参照してください。

痕跡セットの例外

痕跡セットの例外とは、例外と一致するアクションについてのレポートを生成しないために痕跡セットに加える変更です。関心のないイベントに関するレポートを減らす、または停止する一方で、残りの痕跡セット機能は引き続き有効にして

おくことができます。痕跡セットの例外を作成するには、[Events（イベント）] ページで今後のレポートから除外する ATI 関連イベントを特定します。そのイベントに固有の例外を自動で作成するか、例外を変更して適用する対象、プロセス、またはユーザーの範囲を広げたり狭めたりすることができます。

痕跡セットの例外は、例外を作成するために使用するイベントを生成した痕跡セットに固有です。同時に複数の例外を作成できますが、ATI に基づかないイベントを使用して例外を作成することはできません。

痕跡セットの例外の作成手順（デフォルトの方法）：

1. 例外を作成する対象のイベントが表示されない場合は、コンソール メニューで［**Reports**（レポート）］>［**Events**（イベント）］の順に選択し、［**Threat Indicators**（脅威の痕跡）］保存済みビューを選択します。別のビューからイベントを選択することもできますが、[Threat Indicators（脅威の痕跡)] を使用すると、表示されているすべてのイベントには必ず痕跡セットが関連付けられています。
   注意：[Indicator Set Details（痕跡セットの詳細）] ページの［**Recent Events**］リンクを選択して、そのセットの最近のイベントをすべて表示することもできます。
2. 必要に応じて、[Max Age（最長期間)] の値を変更して以前のイベントを表示します。
3. 例外を作成するイベントが 1 つ以上表示されているときは、それぞれのイベントの横にあるチェックボックスをオンにし、[Action（アクション)] メニューで［**Create Indicator Set Exceptions**（痕跡セットの例外の作成）］を選択します。ページ上部のステータス メッセージは、例外が正常に作成されたかどうかを示します。または、正常に作成されない場合はエラーを表示します。一般的なエラーとして、痕跡セットがないイベントを選択するエラーがあります。

   このように作成されたそれぞれの例外には、痕跡セットの名前と増加する番号からなる名前が使用されます。たとえば、Windows System Configuration（Windows システム構成）セットに対する最初の例外は、「Windows System Configuration Exception 1」という名前になります。

作成した痕跡セットの例外は（名前も含めて）編集できます。または、[Create an advanced Indicator Set Exception（高度な痕跡セットの例外の作成）] を選択して、作成時に特別なパラメーターを指定します。高度な痕跡セットの例外は、同時に 1 つのイベントに対してのみ作成できます。

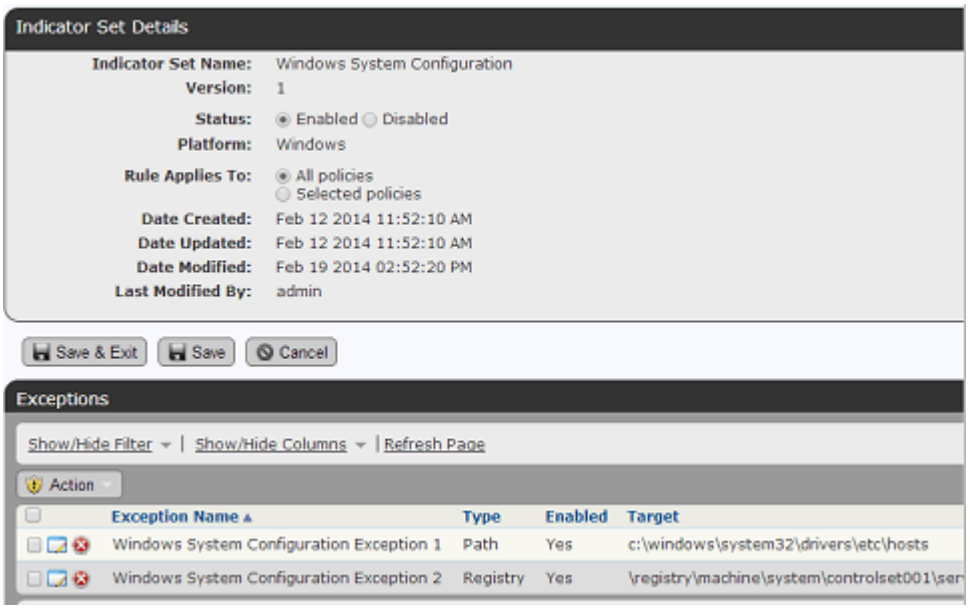
高度な痕跡セットの例外の作成手順：

1. 例外を作成する対象のイベントが表示されない場合は、コンソール メニューで［**Reports**（レポート）］>［**Events**（イベント）］の順に選択し、［**Threat Indicators**（脅威の痕跡）］保存済みビューを選択します。別のビューからイベントを選択することもできますが、［Threat Indicators（脅威の痕跡)］を使用すると、表示されているすべてのイベントには必ず痕跡セットが関連付けられています。
   注意：［Indicator Set Details（痕跡セットの詳細）］ページの［**Recent Events**］リンクを選択して、そのセットの最近のイベントをすべて表示することもできます。
2. 必要に応じて、［Max Age（最長期間)］の値を変更して以前のイベントを表示します。
3. 高度な例外を作成するイベントが表示されているときは、イベントの横にあるチェックボックスをオンにし、［Action（アクション)］メニューで［**Create an advanced Indicator Set Exception**（高度な痕跡セットの例外の作成)］を選択します。［Add Indicator Set Exception（痕跡セットの例外の追加)］ダイアログが表示されます。痕跡セットとプラットフォームは読み取り専用フォームで入力されており、その他のパラメーターは編集可能になっています。複数のチェックボックスをオンにすると、エラー メッセージが表示されます。
4. ［Add Indicator Set Exception（痕跡セットの例外の追加)］ダイアログ ボックスで、例外名と、オプションで説明を入力します。
5. その他のパラメーターを編集して、必要なルールを作成します。これらのパラメーターは、表 89、「例外の詳細（痕跡セット内)」（681 ページ）で説明されています。
6. 例外の構成が終了したら、そのページから移動しない場合は［**Save**（保存）］ボタンをクリックし、［Events（イベント)］ページに戻る場合は［**Save & Exit**（保存して終了)］ボタンをクリックします。

   新しい例外が［Indicator Set Details（痕跡セットの詳細)］ページの［Exceptions（例外)］パネルに表示されます。

痕跡セットの例外の詳細

すべての［Indicator Set Details（痕跡の例外の詳細）］ページに［Exceptions（例外）］パネルがあります。このセットに対して例外が作成されると、このパネルのテーブルに表示されます。



テーブルには、例外名と例外のその他の詳細が表示されます。このテーブルは、他の Bit9 テーブルと同じように、［Show/Hide Filter（フィルターの表示 / 非表示）］リンクおよび［Show/Hide Columns（列の表示 / 非表示）］リンクを使用して変更できます。［Action（アクション）］メニューを使用すると、例外を有効化、無効化、および削除することができます。

テーブルに表示されている例外の［View Details（詳細の表示）］ボタンをクリックすると、［Indicator Set Exception Details（痕跡セットの例外の詳細）］ページが表示されます。

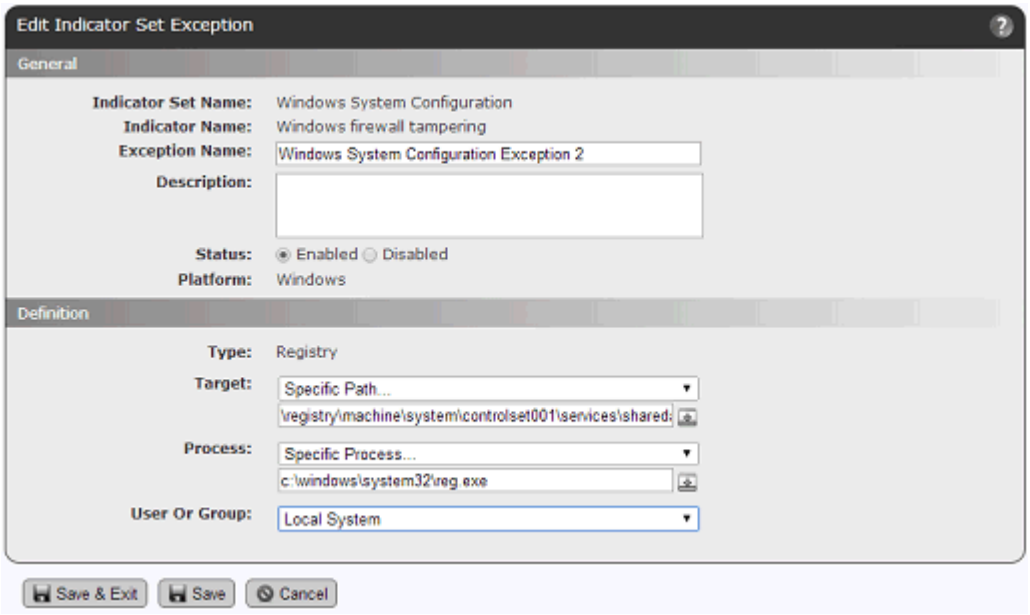


表 89：例外の詳細（痕跡セット内）

フィールド	説明
[Indicator Set Name（痕跡セット名）]	この例外が適用される痕跡セットの名前。名前は Bit9 によって割り当てられ、プラットフォームと、セット内の ATI の一般的な目的で構成されます。
[Indicator Name（痕跡名）]	例外を作成する痕跡セット内の特定の ATI の名前。
[Exception Name（例外名）]	例外の名前。[Action（アクション）] メニューの [**Create Indicator Set Exceptions**（痕跡セットの例外の作成）] コマンドを使用して例外を作成する場合は、自動的に入力されます。自動的な名前付けでは、痕跡セットの名前と増加する番号からなる名前が使用されます。たとえば、Windows System Configuration（Windows システム構成）セットに対する最初の例外は、「Windows System Configuration Exception 1」という名前になります。[**Create an advanced Indicator Set Exception**（高度な痕跡セットの例外の作成）] を使用して例外を作成する場合は、コンソール ユーザーが名前を入力します。どちらの場合でも、名前は後で変更できます。
[Description（説明）]	例外の追加情報。任意のテキストを入力できます（オプション）。
[Status（状態）]	この例外を有効または無効にするラジオ ボタン。
[Platform（プラットフォーム）]	この例外を適用するプラットフォーム（Windows、Mac、または Linux）。
[Type（タイプ）]	この例外の作成時に割り当てられるタイプ（編集不可）。使用できる値は、Path（パス）、Process（プロセス）、Registry（レジストリ）です。
[Target（ターゲット）]	例外が作成されたアクションのターゲット。このフィールドには複数の値を使用でき、使用される値は例外タイプによって次のように異なります。 • パス – ファイル パスまたはファイル名 • プロセス – プロセス • レジストリ – レジストリ パス Bit9 ルールのパスおよびプロセスの指定については、カスタム ルールに関する章で説明しています。Bit9 ルールのページでプロセスを指定する方法については、「パスとプロセスの指定」（420 ページ）で詳しく説明しています。プロセス メニューのオプションについては、表 52 で説明しています。
[Process（プロセス）]	このメニューを使用すると、指定したターゲットに一致するアクションを特定のプロセスが試みるときにのみ例外を適用するように、例外を制限します。「パスとプロセスの指定」（420 ページ）で、Bit9 ルールのページでプロセスを指定する方法について詳しく説明しています。

フィールド	説明
[User or Group（ユーザーまたはグループ）]	この例外を適用するユーザーまたはグループ。ユーザーおよびグループの指定方法は、カスタム ルールに関する章のセクション「ユーザーまたはグループの指定」（435 ページ）で説明しています。
[Date Created（作成日）] （テーブルのみ）	この例外が作成された日時。
[Date Modified（変更日）] （テーブルのみ）	この例外が最後に変更された日時。
[Created By（作成者）] （テーブルのみ）	この例外を作成した Bit9 コンソール ユーザー。
[Last Modified By（最終変更者）] （テーブルのみ）	この例外を最後に変更した Bit9 コンソール ユーザー。

痕跡セットに対する更新

Bit9 は、痕跡セットに対して定期的な自動更新を行うメカニズムを備えています。この更新では、まったく新しい痕跡セットの作成、既存のセットへの新しい痕跡の追加、痕跡セットの再編成、または既存の痕跡への変更が行われます。Bit9 SRS が有効で、[System Configuration（システム構成）] の [Advanced Options（高度なオプション）] ページで痕跡セットの自動更新も有効な場合に、これらの変更は使用可能になった時点で自動的に配信されます。Bit9 SRS の有効化の詳細については、「Bit9 SRS の有効化」（787 ページ）を参照してください。痕跡セットの自動更新の有効化の詳細については、「高度な構成オプション」（766 ページ）を参照してください。

常に自動更新を有効にしておくことも、定期的に更新を一時的に有効にすることもできます。更新は 24 時間以内に配信されるようにスケジュールされ、多くの場合 24 時間よりも早く使用可能になります。

自動更新を受信すると、痕跡セットの状態は次のようになります。

- 新しい痕跡セットは、無効な状態で追加されます。
- 既存の痕跡セットは、更新前の状態に従って引き続き有効または無効になります。このことは、アップグレードによって既存の痕跡セットに対して脅威の痕跡が追加または変更される場合にも当てはまります。

痕跡セットの更新の追跡

組み込みの**痕跡セット アラート**が用意されており、有効にすると次の痕跡セットの変更が通知されます。

- 痕跡セットの更新

- 痕跡セットの作成
- 痕跡セットの削除

このアラートが特に役立つのは、自動更新を一時的にのみ有効にしている場合です。いつ更新を無効にすればよいかを判断できます。アラートの有効化と構成の詳細については、「Bit9 アラートの使用」（606 ページ）を参照してください。

［Indicator Set Details（痕跡セットの詳細）］ページ、または［Indicator Sets（痕跡セット）］テーブルの［Version（バージョン）］、［Date Created（作成日）］、および［Date Updated（更新日）］フィールドを確認することでも、検出の痕跡セットが更新されたかどうかがわかります。

脅威レポートの監視

疑わしいアクティビティまたは脅威となるアクティビティは、Bit9 コンソールの［Events（イベント）］ページおよび［Files（ファイル）］ページの保存済みビューでレポートされます。脅威を監視する活動の一環として、これらのビューを定期的に確認する必要があります。これらの脅威レポートを監視すると、情報が得られるだけでなく、次のようにレポートおよび脅威からの修復のアクションを向上させる上で役立ちます。

- **痕跡セットの例外の作成** – 特定の脅威に関連するイベントのレポートを受け取る必要がない場合は、痕跡セットの例外を作成することで、そのレポートを除外することができます。「痕跡セットの例外」（677 ページ）を参照してください。
- **痕跡セットの無効化** – 特定の痕跡セットによってレポートされるすべてのイベントが関心のないものである場合は、その痕跡セットを無効にすることができます。「脅威検出のための痕跡セット」（673 ページ）を参照してください。
- **痕跡セットの有効化** – 一部の痕跡セットを有効にしていない状態で、特定の重要なアクティビティがレポートされていないと考えられる場合は、そのアクティビティをレポートする痕跡セットが無効になっているかどうかを確認します。「脅威検出のための痕跡セット」（673 ページ）を参照してください。
- **アラートの作成** – 優先度が高いと考えられる検出関連イベントが表示される場合は、そのイベントに対するアラートの作成を検討します。「脅威関連アラート」（688 ページ）を参照してください。
- **脅威からの修復** – 脅威を監視しているときに、修復が必要なイベントが発生する場合があります。この修復には、Bit9 の範囲外でのアクションの実施、Bit9 ルールの作成、またはこれら 2 つの組み合わせが必要な場合があります。「脅威への対応」（689 ページ）を参照してください。

［Events（イベント）］ページの脅威のビュー

Bit9 コンソールの［Events（イベント）］ページでは、疑わしいアクティビティまたは脅威となるアクティビティがいくつかの保存済みビューでレポートされます。これらの保存済みビューには、痕跡セットの有効化が必要なものと、その他のデータを使用するものがあります。次の保存済みビューは脅威に関連しています。

- ［**Threat Indicators**（脅威の痕跡）］– このビューには、Bit9 が管理するコンピューター上で痕跡セット内の ATI によって検出された脅威が表示されます。

有効化された痕跡セットがない場合、このビューは空になります。これらのレポートの詳細については、以降のセクション「脅威イベント レポートの確認」（685 ページ）で説明します。

- ［**Threat Indicators - Legacy**（脅威の痕跡 – 従来）］– このビューには、v7.2.0 以前のリリースでインストールされた ATI によって検出された脅威が表示されます。以前のリリースで Detection Enhancement をインストールしなかった場合、このビューは空になります。
- ［**Threat Report - Suspicious executable created by shell**（脅威レポート – シェルによって作成された疑わしい実行可能ファイル）］– このビューには、システム ディレクトリ、ごみ箱、AppData などの場所に cmd.exe または powershell.exe によって特定の実行可能ファイルを作成するイベントが表示されます。
- ［**Threat Report – Suspicious Files by Location**（脅威レポート – 場所が疑わしいファイル）］– このビューには、いずれかのコンピューターの通常とは異なる疑わしい場所で最初にファイルが確認または実行されたイベント、または 1 台以上のコンピューターの通常とは異なる疑わしい場所に最初に（未承認の状態で）ファイルが出現したイベントが表示されます。例としては、ごみ箱での予期しないファイルのアクティビティがあります。
- ［**Threat Report – Suspicious Files by Name**（脅威レポート – 名前が疑わしいファイル）］– このビューには、いずれかのコンピューターで疑わしい名前のファイルが最初に確認または実行されたイベント、または 1 台以上のコンピューターで最初に（未承認の状態で）疑わしい名前のファイルが出現したイベントが表示されます。多くの場合、名前は正規の Windows ファイルの名前に類似しています。たとえば、svch0st.exe（svchost.exe の 小文字の 'o' の代わりにゼロを使用）という名前のファイルが検出されると、このイベントビューに表示されます。
- ［**Threat Report – Suspicious Files by Parent**（脅威レポート – 親が疑わしいファイル）］– このビューには、不明な、または普及度の低い実行可能ファイルが、通常はそれらのファイルを作成しないはずのプログラムによって書き込まれるイベントが表示されます。この例には、Adobe Reader によって作成される実行可能ファイルがあります。多くの場合、このファイルは形式が異常で、悪意のある PDF 形式による攻撃の兆候と考えられます。

［Events（イベント）］ページでの脅威レポートの表示手順：

1. コンソール メニューで、［**Reports**（レポート）］>［**Events**（イベント）］の順に選択します。
2. ［Saved Views（保存済みビュー）］メニューで、調査する**脅威**のビューを選択します。

脅威関連イベントのビューのフィールド

脅威のビューでは、［Events（イベント）］テーブルにあるいくつかのフィールドが他よりも重要な意味を持っています。一部のフィールドはデフォルトで表示され、一部のフィールドは追加することができます。次にこれらのフィールドを示します。

- ［**Indicator Set**（痕跡セット）］– イベントをトリガーした痕跡を含む痕跡セットの名前。
- ［**Rule Name**（ルール名）］– イベントをトリガーしたルールの名前。検出イベントの場合は、検出された疑わしいアクティビティを表します。

- ［**Indicator Name**（痕跡名）］– このフィールドはオプションで、脅威イベントの［Rule Name（ルール名）］と同じです。Syslog 出力で脅威イベントを識別しやすくするために含まれています。
- ［**Process Threat**（プロセスの脅威）］– このイベントでアクションを試行するプロセスの脅威レベル。Bit9 Software Repurtation Service (SRS) によってレポートされる場合に示されます。
- **Process Trust**（プロセスの信頼度）– このイベントでアクションを試行するプロセスの信頼度。Bit9 SRS によってレポートされる場合に示されます。
- ［**Process Prevalence**（プロセス普及度）］– イベントの［Process（プロセス）］フィールドに関連付けられたファイルの普及度。普及度は、プロセス ファイルのインスタンスが少なくとも 1 つ存在するコンピューターの数で示されます。
- ［**File Threat**（ファイルの脅威）］– このイベントで影響を受けたファイルの脅威レベル。Bit9 SRS によってレポートされる場合に示されます。
- ［**File Trust**（ファイルの信頼度）］– このイベントで影響を受けたファイルの信頼度。Bit9 SRS によってレポートされる場合に示されます。
- ［**File Prevalence**（ファイル普及度）］– このイベントで影響を受けたファイル（［File Name（ファイル名）］フィールドのファイル）の普及度。普及度は、ファイルのインスタンスが少なくとも 1 つ存在するコンピューターの数で示されます。

注意

脅威、信頼度、および普及度のデータの初期値とその後の更新は、Bit9 SRS へのアクセスと Bit9 タスクのスケジュールに基づいて提供されるため、更新は遅れる場合があります。

脅威イベント レポートの確認

イベント ビューごとに、提供される情報のタイプも対象期間も異なります。

［**Threat Indicator**（脅威の痕跡）］ビューでは多くの場合、最新の、または最も影響が大きい潜在的な脅威が表示されます。このため、最初にこのビューに注意を向けることをお勧めします。ただし、［Threat Indicators（脅威の痕跡）］ビューに表示されるのは、1 つ以上の痕跡セットを有効にした後に発生した、一致するイベントのみです。

［Threat Indicators（脅威の痕跡）］ビューに表示されるイベントの場合、そのイベントをトリガーした ATI の痕跡セットとルール名の両方が表示されます。これによって、ルールで識別された脅威のタイプが示されます。また、過剰なレポートや偽陽性のソースも識別できるため、痕跡セットの無効化や、痕跡セットの特定のルールに対する例外の作成について判断する場合にも役立ちます。

［**脅威レポート**］ビューでは、拡張機能を追加する前に存在したイベントなど、標準の Bit9 イベントを使用します。これらによって、有効にしてある痕跡セットがあるかどうかに関係なく、［Max Age（最長期間）］メニューで選択する任意の期間に発生した一致するイベントがレポートされます。すべてのイベント ビューと同じように、脅威のイベントを表示できる最長期間は、Bit9 データベースで有効なデータベースの抽出オプションに従って区切られます。

［Description（説明）］フィールドも、イベントを確認するときに役立ちます。イベントによっては、書き込み、変更、または削除が行われたファイル、ファイルに影響を与えたプロセス、その他の関連データを特定できることがあります。ここでは、次の ATI によって生成されたイベントの説明の例を示します。

ルール名	説明の例
名前が疑わしい実行可能ファイル	ファイル'c:\documents and settings\user\temp\lexplore.exe' が変更または削除されました。
スタートアップ構成に対する異常な変更	レジストリ '\registry\machine\software\microsoft\windows nt\currentversion\winlogon\shell' の変更が許可されました。

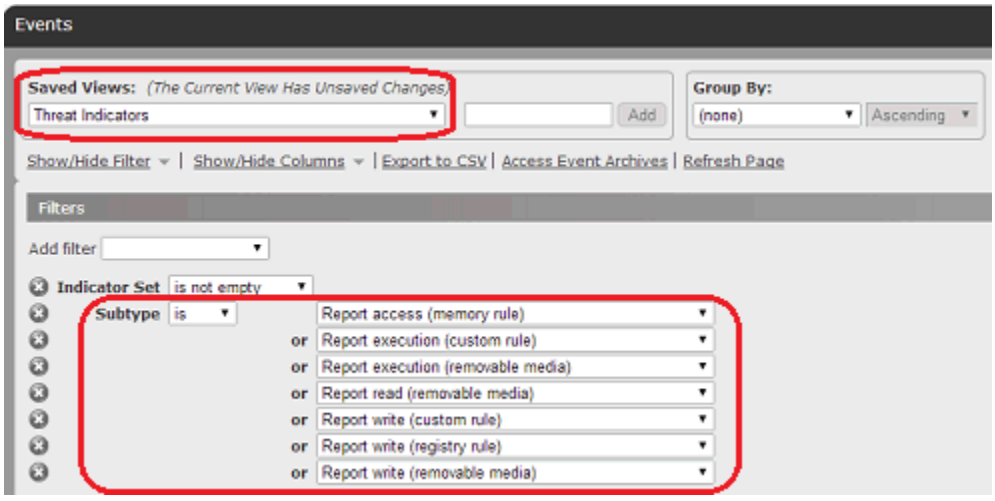
説明の情報の一部は、ビューに追加可能な特定のフィールドにも表示されます。

注意

イベント ビューとは違い、［File Catalog（ファイル カタログ）］ビューでは、ファイル インベントリ内に現在存在するファイルと過去のファイルの両方についてレポートされます。ビューのパラメーターに一致するファイルが、サーバーにレポートするエージェント管理のコンピューターに一度でも存在したことがある場合は、このビューに表示されます。

ビューのパラメーターの表示と変更

脅威関連イベントのビューを作成するために使用するフィルターを表示するには、ビューが表示されているときに［Show/Hide Filter（フィルターの表示 / 非表示）］ボタンをクリックします。次の例は、［Threat Indicators（脅威の痕跡）］ビューを作成するために使用するフィルターを示しています。



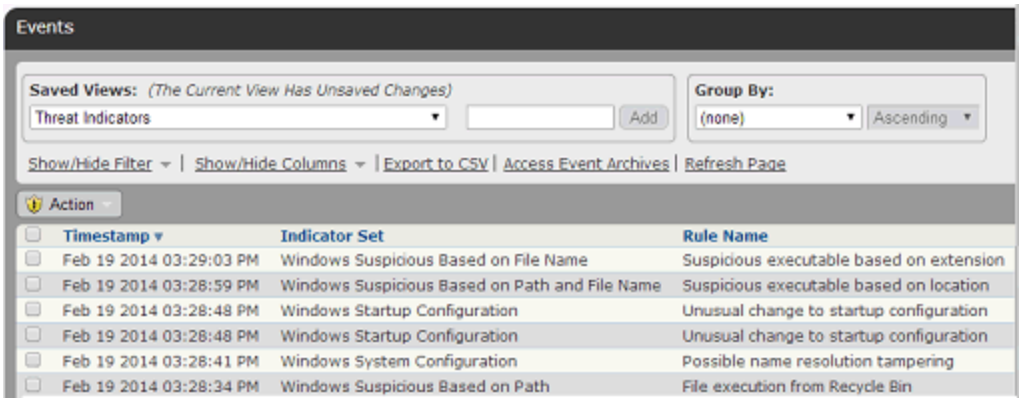
フィルター条件を追加、削除、または変更して細かく調整し、重要でないイベントを除外したり、表示するイベントの範囲を広げたりして、これらのビューを変

更することができます。デフォルトの保存済みビューに対する変更は保存できませんが、変更したビューに新しい名前を付けて保存できます。

デフォルトでは、脅威のビューには過去 1 日のイベントが表示されます。[Events（イベント）] の [Max Age（最長期間）] メニューで別の期間を選択できます。

Syslog 出力の脅威イベント

脅威関連イベントは、他の Bit9 イベントとともに Syslog にエクスポートされます。Syslog でフィルターまたは検索の対象を決定するために、脅威のビューの 1 つを選択し、テーブルに表示されているルール名を確認して、イベントを生成した特定のルールを確認できます。また、[Indicator Name（痕跡名）] フィールド（未加工の出力では「indicatorName」ですが、フォーマットに応じてさまざまな文字列にマップされます）を含むイベントを Syslog 内で検索することで、イベントを脅威検出イベントとして識別できます。これらのイベントでは、[Indicator Name（痕跡名）] は [Rule Name（ルール名）] と同じです。



その他の検索方法として、イベント サブタイプが「Report」（「Report execution block」以外）で始まるイベントのみを表示するように Syslog 出力をフィルターすることができます。これらは、脅威関連イベントのサブタイプです。[Events（イベント）] ページ ビューの特定のイベント サブタイプの一覧を表示するには、[Saved Views（保存済みビュー）] メニューからビューを選択し、[**Show/Hide Filter**（フィルターの表示 / 非表示）] をクリックします。

Bit9 Server で使用可能な Syslog 出力の詳細については、別のドキュメント『Bit9 Events Integration Guide（Bit9 イベント統合ガイド）』を参照してください。

CSV ファイルへの脅威イベント データのエクスポート

Bit9 コンソールの他のテーブルと同様に、[Events（イベント）] ページの脅威関連テーブルのデータを CSV ファイルにエクスポートできます。これは、外部ツールで脅威を分析するのに役立ちます。この情報をエクスポートする場合は、コンソール ページの [Show/Hide Columns（列の表示 / 非表示）] 機能を使用してすべての列をテーブルに追加することを検討してください。このようにすると、脅威イベントに関して役立つ可能性があるすべての情報がエクスポートに含まれます。

CSV ファイルに脅威イベントをエクスポートするには、必要なビュー、列、および［Max Time（最長期間）］の値を使用してテーブルを設定し、［**Export to CSV**（CSV にエクスポート)］をクリックします。

［Files（ファイル)］ページの脅威のビュー

ATI などの脅威監視に関連付けられたイベントが表示される［Events（イベント)］ページ ビュー以外にも、［Files（ファイル)］ページに、疑わしいファイルまたは脅威となるファイルの存在がレポートされます。Bit9 エージェントがエンドポイントにインストールされる前に作成されていたファイルもレポートされます。

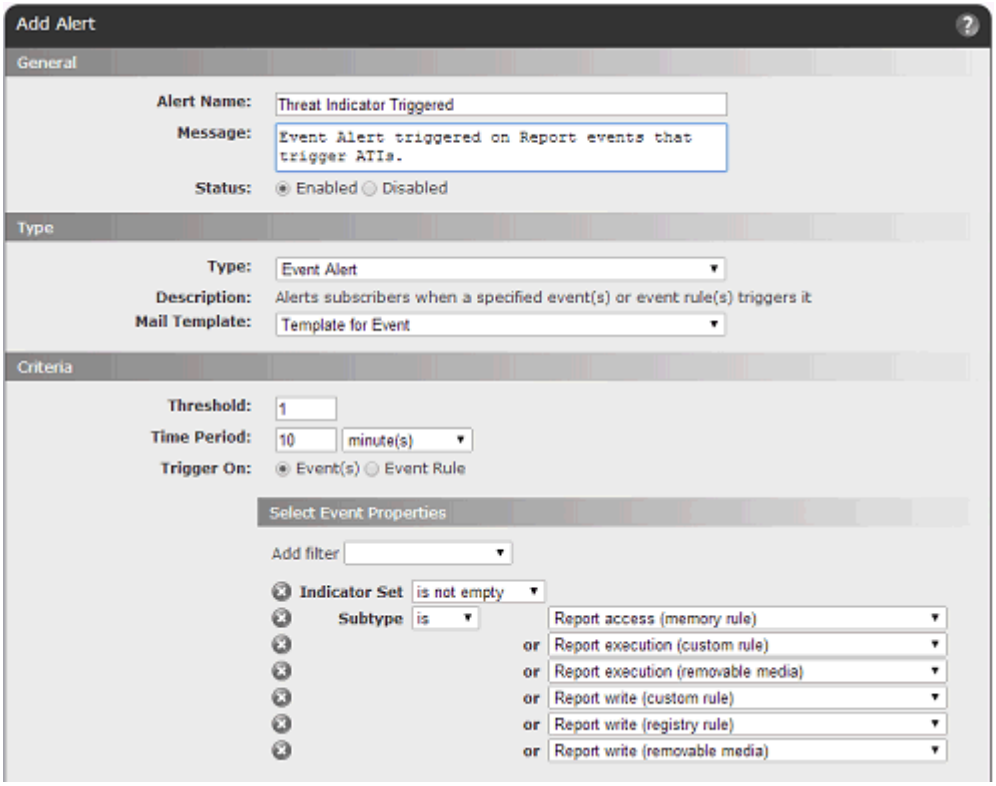
［Files（ファイル)］ページを表示するには、コンソール メニューで［**Assets**（アセット）］>［**Files**（ファイル）］の順に選択し、［File Catalog（ファイル カタログ)］または［**Files on Computers**（コンピューター上のファイル)］のいずれかのタブを選択します。これらのタブでは、次の脅威関連の保存済みビューを使用できます。

- ［**Threat Report - Suspicious Files by Extension**（脅威レポート – 拡張子が疑わしいファイル)］（ファイル カタログのみ）– このビューでは、Bit9 によって分析されて実行可能ファイルであると判断されたものの、拡張子が実行可能ファイルのタイプではないファイルが識別されます。ほとんどのマルウェアは、「.gif」や「.jpg」など、通常は問題とならないファイル拡張子を使用して自身を偽装しようとします。
- ［**Threat Report - Suspicious Files by Name**（脅威レポート–名前が疑わしいファイル）］–（コンピューター上のファイルのみ）このビューには、インベントリに登録されているファイルのうち、一般的なファイル（オペレーティング システムのファイルなど）の名前に類似し、Bit9 SRS の信頼度がゼロで、未承認のファイル状態のものが表示されます。

［Event（イベント)］ビューと同様に、［Files（ファイル)］ページでも［**Show/Hide Filter**（フィルターの表示 / 非表示)］ボタンをクリックすると、これらのビューの作成に使用される拡張子とその他のパラメーターを表示できます。これらのビューでは、多くの「偽陽性」が作成される可能性があります。結果の数を減らすために、このビューではファイル信頼度、サイズ、公開者などの追加の要素を使用しています。ファイルの脅威レポートの独自のバージョンを作成するために、ビューをさらに変更して、別の名前で保存することができます。

脅威関連アラート

ATI によって潜在的な脅威の発生が判断された場合に必ずトリガーされるアラートを作成できます。この目的に使用するアラートはイベント アラートで、特定のタイプの脅威イベントを含める、または除外するように細かく調整することができます。すべてのイベント アラートには、［Select Event Properties（イベント プロパティの選択)］パネルで少なくとも 1 つのサブタイプを含める必要があります。次の例では、［Events（イベント)］ページの［Threat Indicator（脅威の痕跡)］ビューと同じプロパティを使用したアラートを作成しています。そのため、［Threat Indicator（脅威の痕跡)］ビューに表示されるイベントが発生すると、必ずこのイベントがトリガーされます。



アラートを使用すると特定のイベントを容易に監視でき、トリガーされたときに 1 人以上の受信者に E メールを送信するようにアラートを構成することができます。アラートの作成と構成の手順については、「Bit9 アラートの使用」（606 ページ）を参照してください。

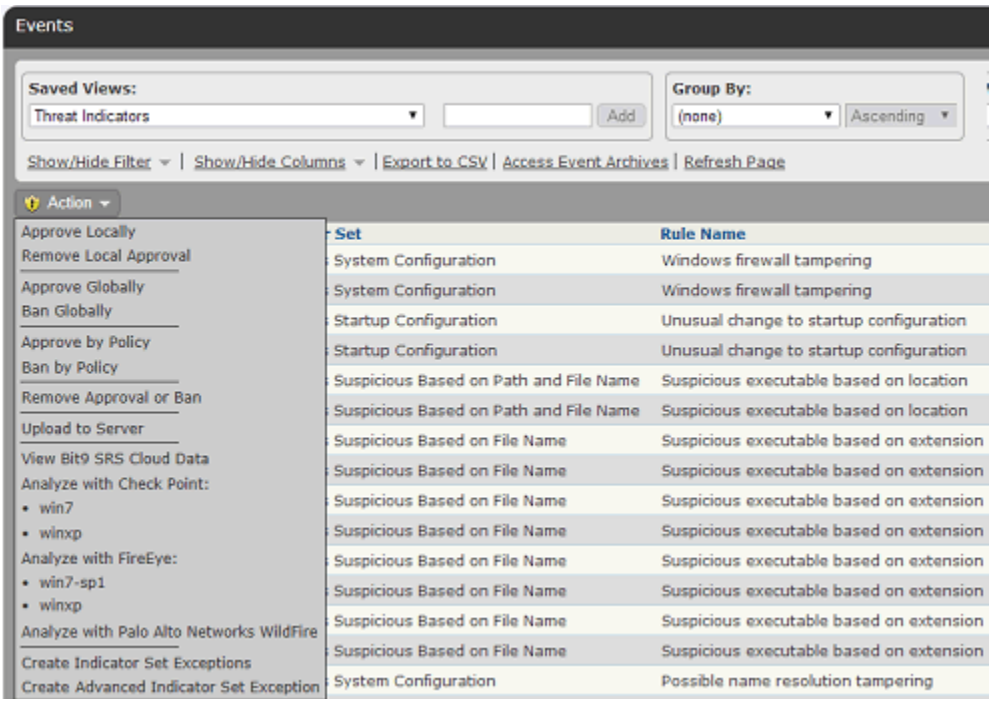
脅威への対応

修復や追加的な注意が必要な脅威が確認された場合には、さまざまな方法で対応できます。対策を講じる前の手順として、レポートに示されているファイル、プロセス、ユーザーなどの情報を調査することが重要です。

対応が必要であると判断した場合には、疑わしいファイルのインスタンスの削除や新しいファイアウォール ルールの作成など、Bit9 の範囲外で対策を講じることもあります。Bit9 Security Platform では、脅威のビューにレポートされたイベントの横にあるチェックボックスをオンにし、[Action（アクション）] メニューの次のコマンドを使用して、イベントでレポートされたファイルに対して操作を行うことができます。

- [**View Bit9 SRS Cloud Data**（Bit9 SRS Cloud データの表示）] – Bit9 SRS を有効にしている場合は、Bit9 SRS サイトを開いて、Bit9 が監視するコンピューターでのファイルの最初の確認日と普及度など、ファイルの追加情報を表示できます（情報が利用できる場合）。
- [**Send Suspicious Files for Analysis**（分析用に疑わしいファイルを送信）] – Bit9 Connector を使用して外部の分析アプライアンスまたは分析サービスを統合した場合は、レポートされたファイルを外部での分析用に脅威として送信できます。このオプションで分析用に送信できるのは、脅威イベントで示されたターゲット ファイルで、プロセスではありません。

- [**Ban Globally**（グローバルに禁止）] / [Ban by Policy（ポリシーによる禁止）] – いずれかの脅威のビューの［Action（アクション）］メニューで直接、疑わしいファイルまたは悪意のあるファイルを禁止できます。脅威レポートでレポートされるファイルは、それを受け入れる目的と受け入れない目的のどちらでも使用されることがあるため、禁止を使用する際は注意が必要です。禁止を使用するかどうか判断するために、まず「レポートのみの禁止」を実行することをお勧めします。このオプションは［Ban by Policy（ポリシーによる禁止）］ページから使用できます。

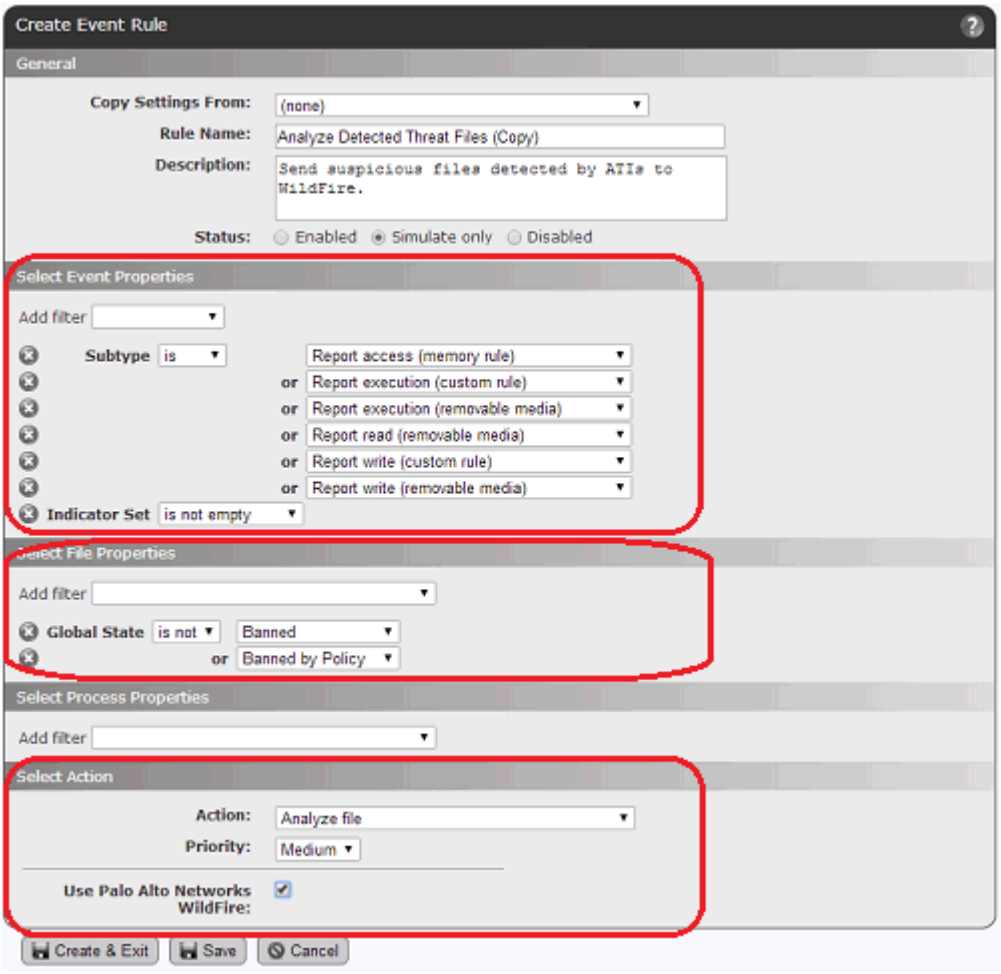


［Action（アクション）］のオプション以外にも、状況に応じてカスタム ルールやレジストリ ルールなどのさまざまなタイプのルールを作成して、脅威を軽減できます。これらのルールには、手動でパラメーターを入力する必要があります。脅威のビューでイベントからファイルの情報、レジストリの情報、またはプロセスの情報をコピーしてから、何らかの方法でその他のルール パラメーターを構成します。その際、ブロックまたはレポートの対象であることが確かなアクションだけをルールの対象とし、重要なファイルやプロセスをブロックしないように注意します。これらのルールを作成する方法の詳細については、第 12 章「カスタム ソフトウェア ルール」、第 14 章「レジストリ ルール」および第 15 章「メモリ ルール」を参照してください。

イベント ルールによる脅威への対応

Bit9 イベント ルールを使用すると、ルール定義に一致するイベントが発生したときに特定のアクションを実行できます。これにより、［Events（イベント）］ページで脅威を確認していない場合でも、脅威に自動的に対応できます。イベント ルールを使用してファイルを自動的に禁止することはできませんが、次のように、レポートされた脅威に対して役立つ可能性がある他のアクションを実行できます。

- **疑わしいファイルの承認の取り消し** – イベント ルールを使用して、ルール パラメーターに一致するファイルに対するローカル承認またはグローバル承認を自動的に取り消すことができます。
- **分析用に疑わしいファイルを送信** – Bit9 Connector を使用して外部の分析アプライアンスまたは分析サービスを統合した場合は、レポートされたファイルを外部での分析用に脅威として送信するイベント ルールを作成できます。たとえば次の図では、脅威のイベントでレポートされて、まだ禁止されていないファイルが分析用に WildFire に送信されます。これによって、ファイルをブロックするかどうかの判断に影響する可能性がある追加の情報が得られます。
- **禁止の作成**– ATIによってトリガーされた脅威イベントに含まれるファイルに関して、レポートのみの禁止を作成するイベント ルールを定義できます。レポートのみの禁止によって生成されるイベントにより、禁止のすべての機能が有効になっていればファイルがブロックされていたことが示されます。デフォルトでは使用できませんが、Bit9 テクニカル サポートにご相談いただくことで、イベント ルールによる高度な禁止を作成するオプションを有効にすることができます。



イベント ルールの作成および編集方法の詳細については、第 16 章「イベント ルール」を参照してください。

第 21 章

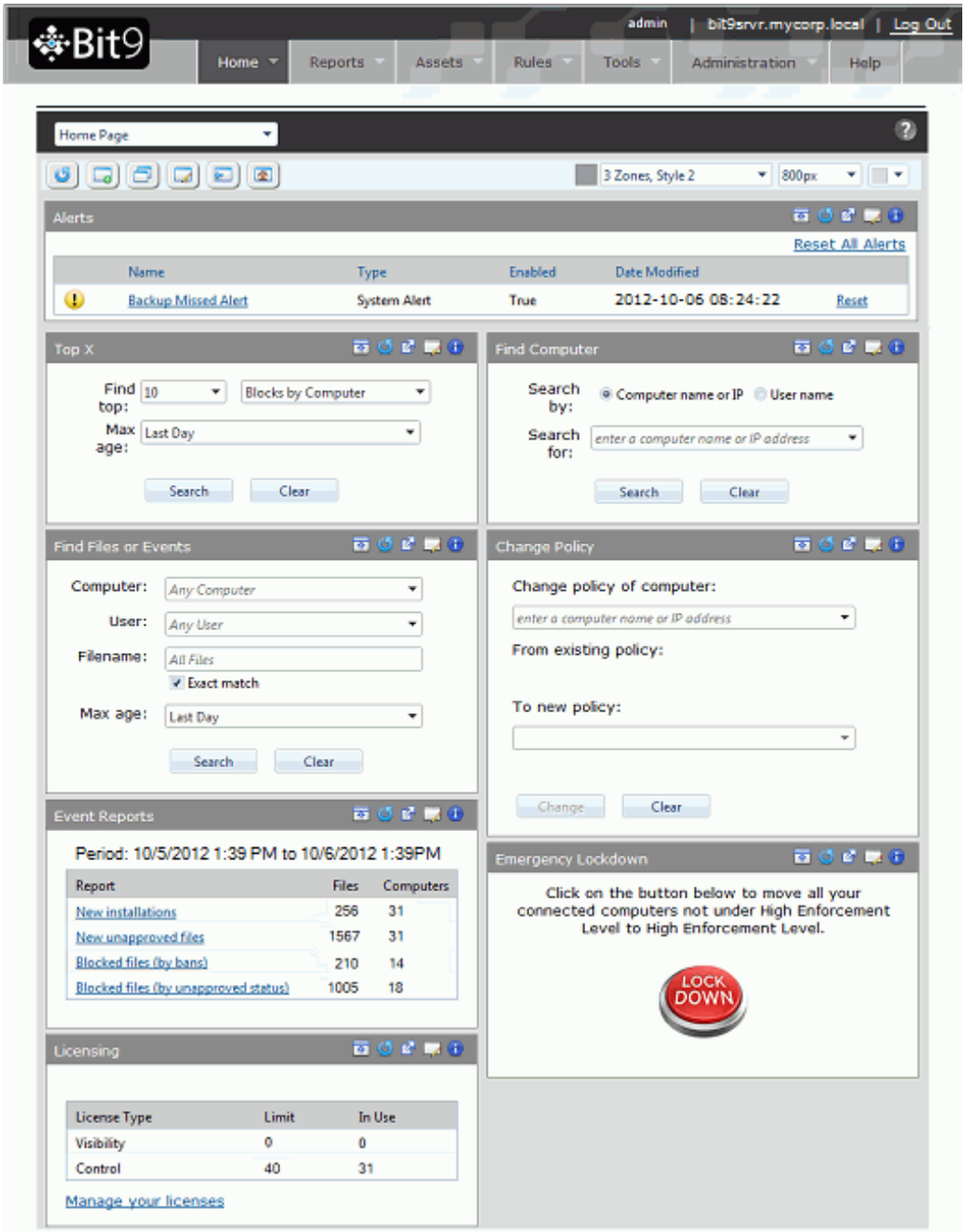
ダッシュボードの使用とカスタマイズ

Bit9 ダッシュボードは、「ポートレット」と呼ばれるコンパクトなウィンドウを備えた構成可能なページです。それぞれのポートレットによって Bit9 関連の情報やコントロールにアクセスできます。

セクション

ダッシュボードの概要

デフォルトの開始ページを変更していない場合、Bit9 コンソールにログインしたときに表示される最初のページは［Home Page（ホーム ページ）］ダッシュボードです（表示されないときは、コンソール メニューで［Home（ホーム）］をクリックします）。



ダッシュボードは、一連の「ポートレット」で構成され、それぞれのポートレットからコンピューターおよびファイルのセキュリティの管理に役立つ概要情報や

コントロールを利用できます。一部のポートレットには、イベントやベースライン ドリフトなど、Bit9 データベースに含まれる特定のタイプの情報が表示されます。また、一部のポートレットでは外部の URL からのニュース フィードやその他の情報が表示される場合があります。

注意

この章では、ホーム ページを例に使用して、ダッシュボードの機能を説明します。ホーム ページ ポートレットの完全なリストと説明については、表 2、「ホーム ページのクイック アクセス ポートレット」58 ページを参照してください。

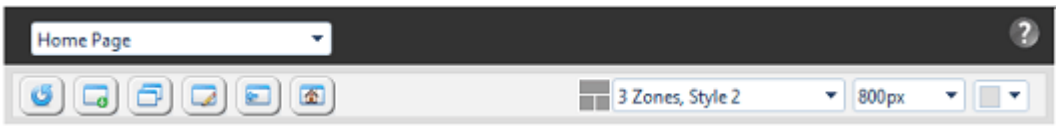
- この章の最初のセクションでは、ダッシュボードの基本要素とその使用方法について説明します。Bit9 が提供するダッシュボードのみを提供された状態のまま使用する場合、読む必要があるのはこのセクションだけです。
- この章の 2 つ目の主要セクションでは、ダッシュボードの「外観」のカスタマイズについて説明します。既存のダッシュボードのみを使用し、その表示の一部を変更する場合は、このセクションが役立ちます。
- この章の 3 つ目の主要セクションでは、ダッシュボードとダッシュボード上の情報やコントロールを作成する方法とカスタマイズする方法について説明します。他のユーザーとダッシュボードを共有する方法も説明します。
- この章の最後のセクションでは、ダッシュボードを構成するポートレットの作成および編集方法について説明します。

ダッシュボードで実行できる操作は、コンソール ログイン アカウントの権限レベルによって異なります。次の説明は、各グループにデフォルトの権限があることを前提としています。

- Administrator と PowerUser は、自分自身のダッシュボードおよび他のユーザーと共有しているダッシュボードの表示、作成、変更、削除を行い、その機能を使用することができます。作成したダッシュボードを共有し、Bit9 コンソールの新しいユーザーに対して別のデフォルトのホーム ページを選択できます。
- Administrator と PowerUser はポートレットの表示、作成、変更、削除を行い、その機能を使用することができます。
- ReadOnly ユーザーは、自分自身のダッシュボードの機能、ホーム ページとシステム ダッシュボードなどの Bit9 が提供するダッシュボードの機能、および他のユーザーが作成し、共有しているダッシュボードの機能にアクセスして使用できます。また、自分自身のダッシュボードを作成、変更、削除することができます。その他のダッシュボードの変更や削除、作成したダッシュボードの共有、新しい Bit9 コンソール ユーザーに対する別のデフォルトのホーム ページの選択は行うことができません。
- ReadOnly ユーザーは、ポートレットの機能を表示し、使用できます。ただし、コンピューターの緊急ロックダウンおよびポリシー変更など、使用権限のない機能にアクセスするポートレットは除きます。ポートレットを作成、変更、削除することはできません。
- ［Group Details（グループの詳細）］ページの［Manage Shared Dashboards（共有ダッシュボードの管理）］チェックボックスを使用して、ダッシュボードへのアクセス権限を有効または無効にすることができます（「コンソール アカウント グループの管理」（104 ページ）を参照）。

ダッシュボードの要素

ダッシュボードによって表示されるポートレットはさまざまですが、すべてのダッシュボード ページの基本構造は標準的なものです。2 つの主要な領域として、ダッシュボード ツールバーとポートレットがあります。このうちダッシュボード ツールバーは現在のダッシュボードの名前が表示されており、管理のためのボタンとメニューを備えています。



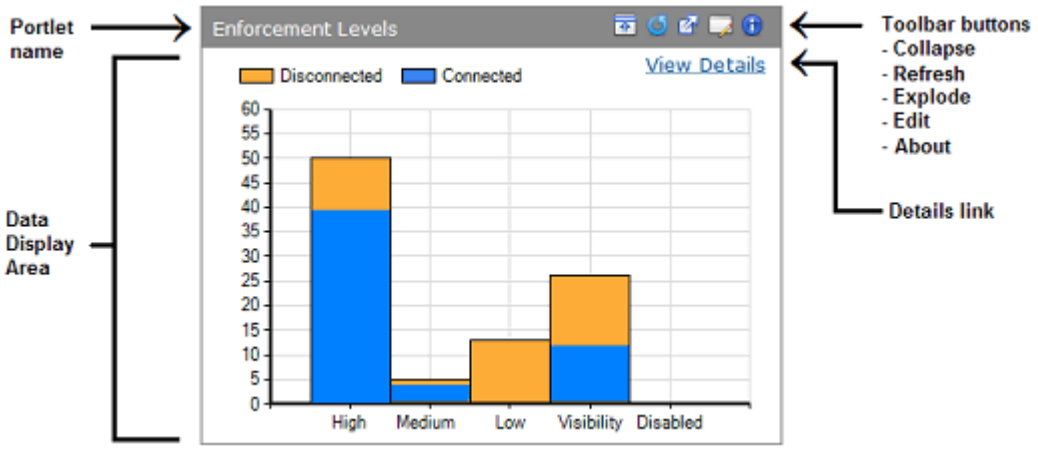
ダッシュボード ツールバーには以下の項目があります。

- 現在のダッシュボードの名前 – ツールバーの左上に表示されます。
- ダッシュボード メニュー – ダッシュボード名の横にあるドロップダウン矢印をクリックすると、ダッシュボード メニューが開き、別のダッシュボードを選択して表示できます。
- ダッシュボード ヘルプ ボタン – ダッシュボード ページの右上の領域にある疑問符ボタンをクリックすると、ダッシュボードに関する一般的なヘルプが開きます。個々のポートレットでは、右上隅の情報ボタンを使用すると、そのポートレットの説明が表示されます。
- ダッシュボード アクション ボタン – [Reload（再ロード）] ボタンによって現在のダッシュボードを再ロードできます。 他のボタンはセクション「ダッシュボードの作成、編集、管理」（705 ページ）で説明する、より高度なアクティビティに使用されます。
- ダッシュボードの外観オプション メニュー – ツールバーの右側半分にあるこれらのオプションの詳細については、「ダッシュボードの外観の変更」（702 ページ）を参照してください。

ポートレットの使用

ダッシュボードのポートレットにはファイル、コンピューター、またはイベントの情報が表示されることがあります。ポートレットには Bit9 エージェントによって管理されているコンピューターの数とタイプ、適用されているセキュリティ ポリシーの数とタイプ、またはコンピューター上のソフトウェアのカテゴリが表示されることがあります。ダッシュボードには、イベントやファイルの検索などの問い合わせを実行するポートレットや、すべてのコンピューターをロックダウンするなどのアクションを実行するポートレットが含まれる場合もあります。

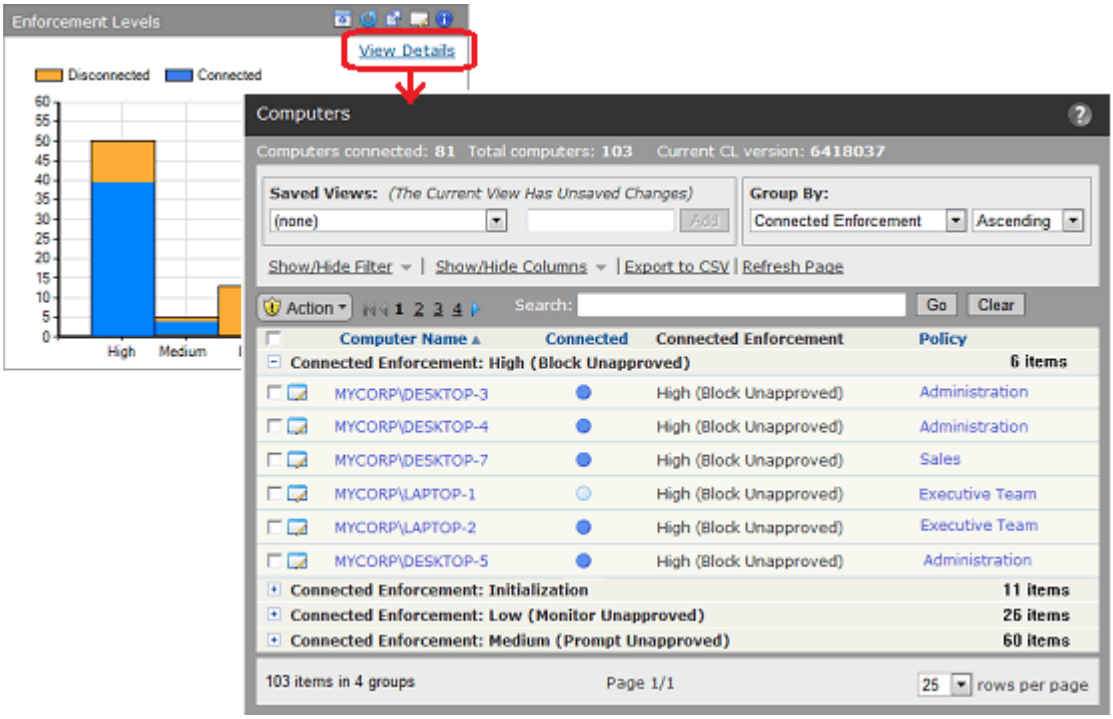
各ポートレットには、左上にポートレット名を表示したツールバー、右上に一連のボタンがあります。ポートレットの主な内容はツールバーの下に表示されます。データはテーブル、図、グラフ、RSS クロール、または HTML ページの形式でこの内容領域に表示されます。アクションを行うポートレットやクエリを実行できるポートレットには、入力フィールドやクリックしてアクションを実行するためのボタンがあります。また、データを伝達するための他の手段を備えたポートレットを追加することもできます。



多くのポートレットでは、棒グラフの棒など、グラフの要素の上にマウス カーソルを移動するとその要素の説明が表示されます。たとえば、グラフの棒が表すコンピューターの数などが表示されます。

詳細なデータの取得

多くのポートレットでは、最上部に重要な情報が表示されるだけでなく、詳細な情報に「ドリル ダウン」することもできます。詳細を表示するには、ポートレットでグラフィックやデータ（マウス カーソルが手の形に変わる場所）をクリックします。ポートレットに［View Details（詳細の表示）］ボタンがある場合は、そのボタンをクリックすることもできます。ダッシュボードの下には、最初の詳細レベルとして、ポートレットが表示する内容についての追加情報を示す Bit9 Server ページが表示される場合があります。ポートレットによっては、詳細ページの情報はデータ タイプごとにグループ化されて（適用レベルによってコンピューターをグループ化するなど）ポートレットに表示されます。



詳細への「ドリルダウン」からダッシュボードに戻るには、コンソールの［Home（ホーム）］メニューで、以前表示していたダッシュボードの名前を選択します。戻るボタンを使用してダッシュボードに戻ると、予期しない結果となる可能性があります。

ポートレット ツールバーのボタン

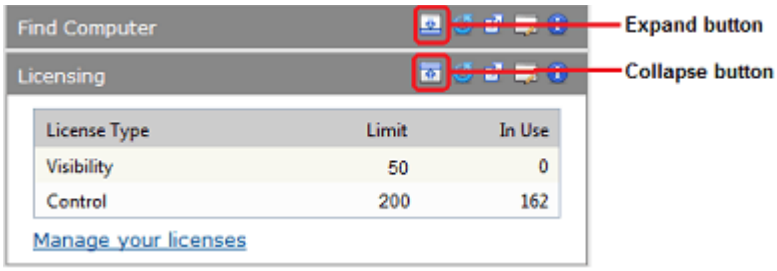
ポートレット ツールバーには、さまざまなオプションがあり、一部のオプションではポートレットの表示を変更できます。表 90 に、ツールバーのボタンと実行するアクションを示します。

表 90：ポートレット ツールバーのボタン

ボタン	説明
［Collapse（縮小）］	ポートレットのビューを縮小し、ツールバーのみを表示します。
［Expand（展開）］	縮小したポートレットを通常の表示に戻します。
［Reload（再ロード）］	ポートレットを再ロードして、使用可能な最新のデータを示します。
［Explode（拡大）］	ポートレットのビューを拡大して、ポートレットをダッシュボード全体に表示します。拡大したポートレットの右上隅にある [X] をクリックすると、通常のサイズに戻ります。
［Edit（編集）］	このポートレットの［Portlet Details（ポートレットの詳細）］ページを開きます。このページでは、編集可能なパラメーターにアクセスできます。編集可能なパラメーターは、ポートレットのタイプとソースによって異なります。組み込みのポートレットの一部では、編集可能なパラメーターは、ユーザーが［Information（情報）］ボタンをクリックしたときに表示される名前と説明だけです。 「ポートレットの詳細の編集」（715 ページ）を参照してください。
［Information（情報）］	このポートレットの情報ウィンドウを開きます。情報ウィンドウには、ポートレットの目的と使用方法の簡単な説明が示されます。この情報は編集可能です。

ポートレットの縮小、展開、拡大

ダッシュボードでのポートレット ウィンドウの表示方法を変更するための機能は 2 つあります。1 つ目の機能では、ポートレットを「縮小」して名前とツールバーのみを表示することができます。また、ポートレットを「展開」して通常の状態に戻すことができます。この［Collapse（縮小）］または［Expand（展開）］ボタン（現在のポートレットの状態によって切り替わります）は、各ポートレットのツールバーの右側にあります。



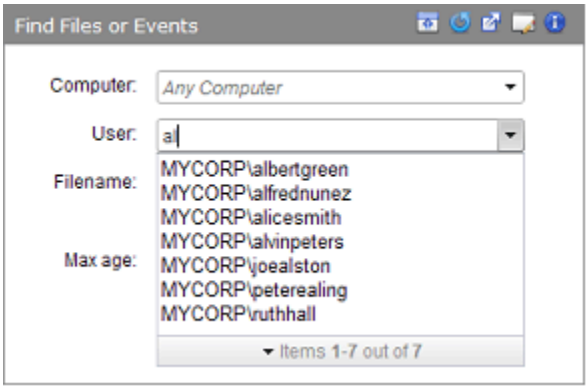
また、一時的な表示オプションとしてポートレットの拡大があり、ダッシュボードの表示領域全体に 1 つのポートレットを表示することができます。拡大されたビューでの作業が終わったら、ポートレットの右上の領域にある [X] ボタンをクリックすると通常の表示に戻ります。

「拡大された」ポートレットのサイズは、[Explode（拡大）] ボタンをクリックした時点での Bit9 コンソールのブラウザー ウィンドウのサイズによって変わります。

ポートレットへの情報の入力

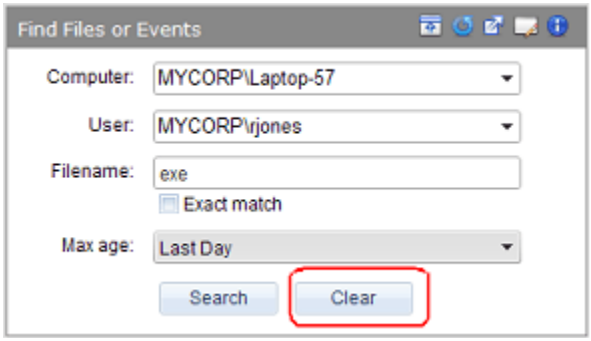
Bit9 Security Platform にはシステム ポートレットが付属していますが、これらのすべてがオリジナルのホーム ページに表示されるわけではありません。システム ポートレットの一部はコンピューター名、ファイル名、ユーザー名などのデータを入力するフィールドを備えており、情報を検索したり、データで識別された項目に対してアクションを実行したりすることができます。これらのポートレットには、いくつかの便利な機能があります。

Bit9 Server のデータベースに保存されているデータの名前を入力する場所では、「オートコンプリート」機能を使用できます。入力中に、それまでに入力した内容と一致する候補のリストがメニューに表示されます。目的の項目がメニューに表示されている場合は、その項目をポイントしてクリックするだけで名前の入力が完了します。以下の例で示されているように、オートコンプリートでは、選択したカテゴリに含まれる、入力した文字列を含むオブジェクト（この例ではユーザー）が表示されます。入力した文字列で始まるオブジェクトだけが表示されるのではありません。ただし、ファイル名については、入力した文字列を含むすべてのファイルを検索するデフォルトの動作ではなく、「完全一致」オプションを選択できます。



データをポートレットに入力すると、通常、入力したデータは変更しない限りそのフィールドに保持されます（デフォルトになります）。この動作は、最初の入力

と類似した情報で何度も検索（またはその他のアクション）を行うときに便利です。ポートレットにデータが入力されていない状態で操作をやり直す場合は、[Clear（クリア）] ボタンをクリックします。



ポートレットのその他のコントロール

ポートレットでは詳細を表示したり、アクションを実行したりする特別なコントロールを使用できます。たとえば、[Emergency Lockdown（緊急ロックダウン）] ポートレットには、ロックダウン用と復元用の大きなボタンがあります。[Alerts（アラート）] ポートレットには、一部またはすべてのリンクをリセットするテキスト リンクがハイライト表示されています。特別なコントロールが用意されている場所では、ポートレット自体のテキストによってその用途が明確に示されます。

他のダッシュボードの表示

ホーム ページは、いつでも Bit9 コンソール メニューから使用できます。Bit9 (Parity) 6.0 以降の新しいインストールには、各適用レベルのコンピューターの数、システム上で確認された新しいソフトウェア、およびベースライン ドリフト レポートなど、システムに関するさまざまなレポートを表示するポートレットを備えたシステム ダッシュボードも含まれています。以前のリリースから Bit9 v7.2.3 へのアップグレードには、以前のバージョンで作成して使用できるようになっているその他のダッシュボードも含めることができます。

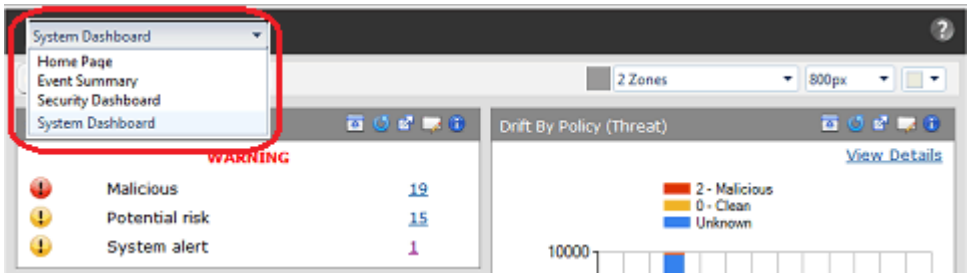
次の図は、システム ダッシュボードに表示されるポートレットの種類を示しています（使用中のシステム ダッシュボードでは、ポートレットの数や種類が異なる場合があります）。


System Dashboard
2 Zones
800px
System Alerts
WARNING
Malicious 19
Potential risk 15
System alert 1
Enforcement Levels
View Details
Disconnected
Connected
High
Medium
Low
Visibility
Disabled
New Software
Max age: 1 day
View Details
File Count
Moving Average
1/6/2012
1/7/2012
1/7/2012
1/7/2012
Software Categorization
View Details
Browsers [11]
Entertainment [13]
Hacking Tools [7]
Instant Messaging [23]
Media Players [16]
P2P Applications [2]
Toolbars [2]
Utilities [79]
Emergency Lockdown
Click on the button below to move all your connected computers not under High Enforcement Level to High Enforcement Level.
LOCK DOWN
Drift By Policy (Threat)
View Details
2 - Malicious
0 - Clean
Unknown
Drift
Policy
Drift by Computer (Drift vs. Risk)
View Details
Risk
Drift
Daily Software Drift
View Details
Drift
Risk
Computer
Operating Systems
View Details
Mac
Windows 7
Windows 8
Windows Server 2003
Windows Server 2008
17 (9.1%)
32
3 (1.6%)
9 (4.8%)
126

別のダッシュボードを選択して開くには、いくつかの方法があります。

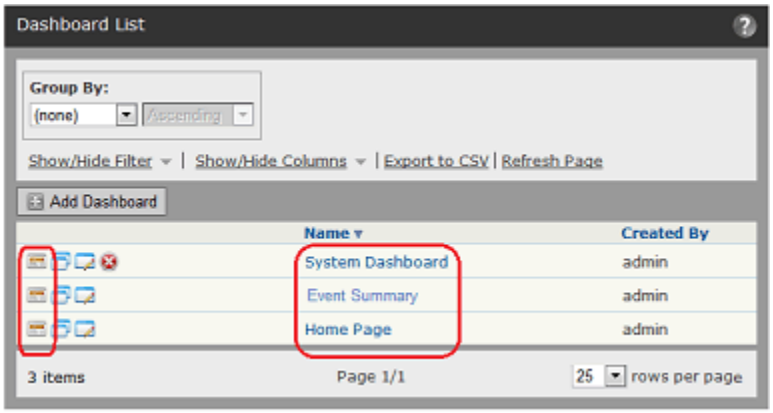
ダッシュボードを開く手順：

- ダッシュボードを表示しているときは、次のようにツールバーの左上にあるメニューで別のダッシュボードを選択します。



- または、任意のコンソール ページで、コンソール メニューの［**Home**（ホーム）］の上にカーソルを移動すると、選択できる他のダッシュボードが表示されます。すべてのダッシュボードがメニューに追加されているとは限りません。

- または、コンソール メニューで［**Reports**（レポート）］>［Dashboards（ダッシュボード）］を選択し、［Dashboard List（ダッシュボード リスト）］でダッシュボード名の横にある［View Dashboard（ダッシュボードの表示）］ボタンをクリックするか、名前自体をクリックします。



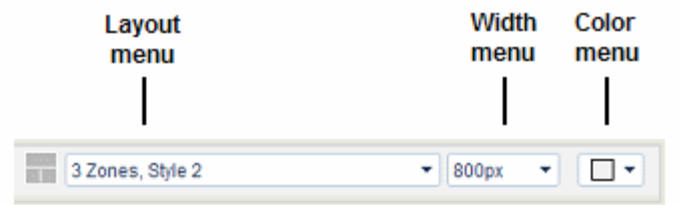
ダッシュボードの外観の変更

次のオプションを使用して、ダッシュボードの外観を変更できます。

- ダッシュボードでのポートレットのレイアウトの変更
- ダッシュボードの幅の変更
- ダッシュボードの背景色の変更
- ポートレット ウィンドウの縮小と展開

- ダッシュボードでのポートレットの移動

これらのオプションのうち、3 つがツールバーの右半分にあるメニューに表示されます。

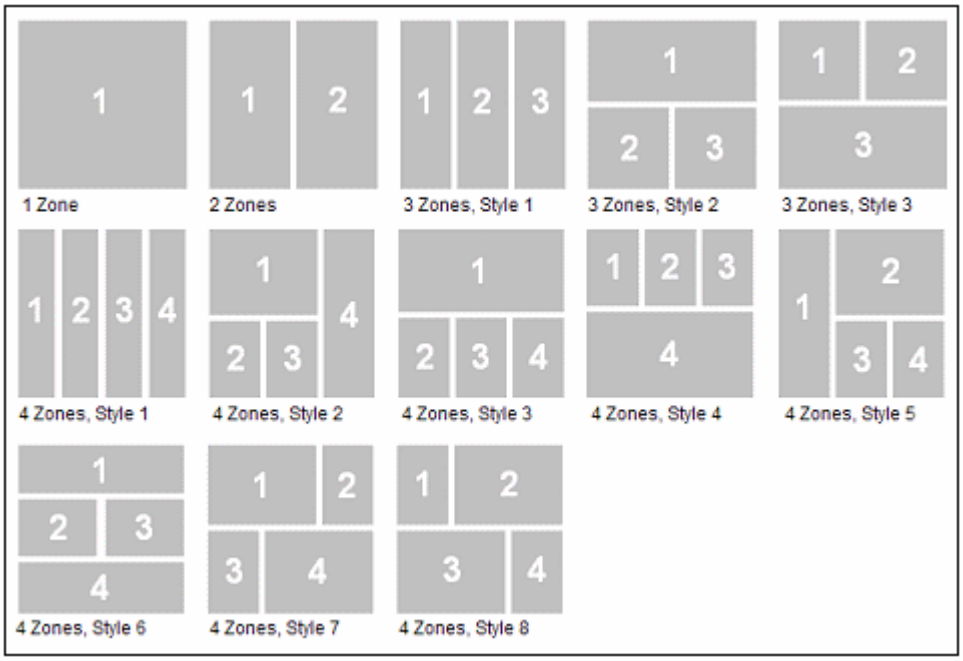


このセクションでは、既存のポートレットを含む既存のダッシュボードの外観とレイアウトを変更する操作について説明します。ポートレットの追加と削除については、セクション「ダッシュボードの編集」（710 ページ）で説明しています。

これらの外観のオプションは、現在のダッシュボードにのみ影響し、現在ログインしているユーザーに固有です。

ダッシュボードのレイアウトの変更

ダッシュボードのレイアウト メニューには現在のダッシュボード レイアウトが示され、13 種類のテンプレート セットから別のレイアウトを選択できます。テンプレートを使用すると、ポートレットを配置するゾーンを作成できます。一部のレイアウトでは、ゾーンの幅が異なります。レイアウトを選択したら、ポートレットを現在のゾーンから内容に適した幅のゾーンに移動することができます。



レイアウトにはゾーンの数で名前が付けられ、ゾーンの数が同じスタイルが複数ある場合は「スタイル」番号が含まれます。デフォルトのレイアウトは大きさが等しい 2 列構成のレイアウトで、唯一の「2 ゾーン」レイアウトです。ゾーンの数はポートレットの数を表しません。各ゾーンには複数のポートレットを配置することができ、通常は複数配置されます。

レイアウトでのポートレットの配分

レイアウトを切り替えたり、ポートレットを追加したりすると、ポートレットは次のルールに従ってゾーンに割り当てられます。

- ゾーンの数が現在のレイアウトと同じか多いレイアウトに切り替えた場合、ポートレットは割り当てられているゾーンに残ります。たとえば、「2 ゾーン」から「3 ゾーン、スタイル 1」に切り替えた場合、ポートレットを移動するまでは、ゾーン 1 のポートレットはすべてゾーン 1 に残り、ゾーン 2 のポートレットはすべてゾーン 2 に残ります。あるレイアウトで広いゾーンにあったポートレットが、別のレイアウトでも広いゾーンにマップされるということはありません。
- 現在のレイアウトよりもゾーンの数が少ないレイアウトに切り替えた場合、ポートレットは新しいゾーンにマップし直されます。ポートレットが以前のレイアウトで偶数ゾーンにあった場合は、そのポートレットは新しいレイアウトの偶数ゾーンに移動し、奇数ゾーンにあった場合は、奇数ゾーンに移動します。ただし、1 ゾーンのレイアウトに移動する場合は例外で、ポートレットはすべて 1 つのゾーンに移動します。
- ダッシュボードにポートレットを追加すると、ポートレットはゾーン 1 から順次、各ゾーンに配分されます。1 つの編集セッションで 3 つのポートレットを追加すると、それぞれゾーン 1、2、3 に配分されます。
- コンソールでは、使用したレイアウトでのポートレットの配分が「記憶」されます。レイアウトの変更後に以前使用したレイアウトに戻すと、ポートレットは追加も削除もされなかったものとして扱われ、以前と同じ場所に表示されます。

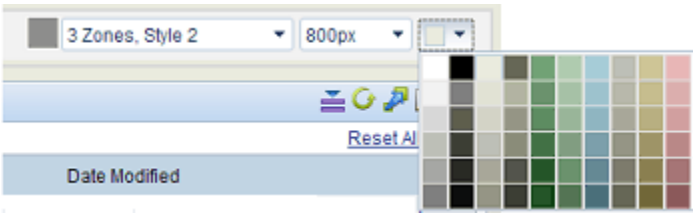
レイアウトの変更後にポートレットの並べ替えが必要になることはよくあります。

ダッシュボードの幅の変更

ダッシュボードの幅メニューには、現在のダッシュボードの幅がピクセル単位で表示され、600 ～ 1700 ピクセルの幅を選択できます。ダッシュボードの幅を変更すると、現在のレイアウト内でのゾーンの幅に比例してポートレットの幅のサイズが変更されます。幅を選択するときは、画面サイズと解像度、および Bit9 コンソールに割り当てる画面の領域を考慮します。ダッシュボードのデフォルトの幅は 800 ピクセルです。

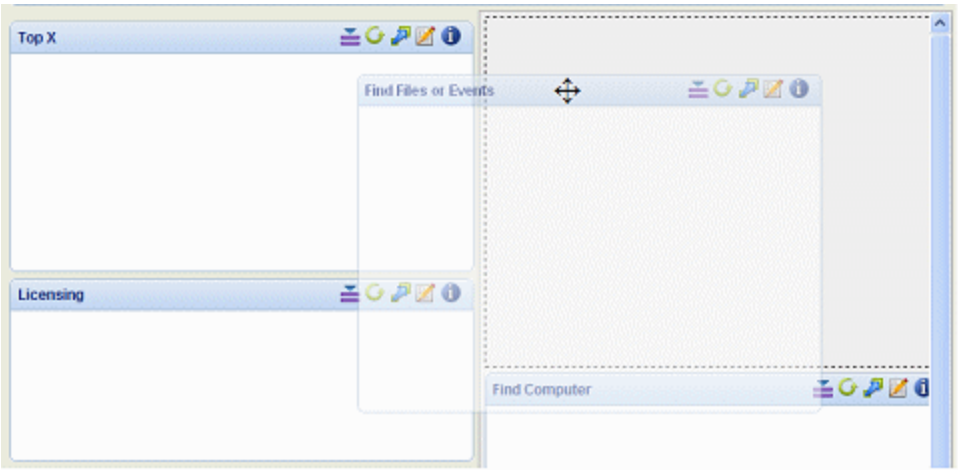
ダッシュボードの背景色の変更

ダッシュボードの色メニューでは、ダッシュボードの背景色を変更できます。メニューをクリックするとパレットが表示され、パレット上の色をクリックすると色が変更されます。背景色の変更はポートレットの色に影響しません。デフォルトの背景色は薄い灰色です。



ポートレットの移動

ポートレットを移動するには、ポートレット内のツールバーをクリックし、左マウス ボタンを押したままマウスを動かします。ポートレットを移動するとき、移動しているポートレットは透明になり、他のポートレットは境界のみが表示されます。ポートレットの移動中は、マウス ボタンを離したときにドロップされる場所が点線のボックス（移動先領域）として表示されます。1 つのレイアウト ゾーンから別のレイアウト ゾーンに移動する場合は、ポートレットの幅に変更があれば、移動先領域のボックスによって示されます。ポートレットを新しい場所にドロップすると、ポートレットはすべて通常の表示に戻ります。



ダッシュボードの作成、編集、管理

このセクションでは、ダッシュボードの作成と編集、およびその他のダッシュボード管理タスクについて説明します。ダッシュボードは、次の基本パラメーターによって定義されます。

- 名前
- ダッシュボードに表示するポートレット
- このダッシュボードを他のユーザーと共有するかどうか
- このダッシュボードを Bit9 コンソール メニューのリストに表示するかどうか

新しいダッシュボードを最初から作成するか、または既存のダッシュボードをコピーして新しい名前を付け、コピー後に変更することができます。ダッシュボードを作成、コピー、編集するいずれの場合も、[Edit Dashboard（ダッシュボードの編集）] ページで基本構成情報を入力するか編集します。それぞれの場合の主な違いは、使用開始時に［Edit Dashboard（ダッシュボードの編集）］ページに入力されている情報（情報がある場合）の種類です。

ダッシュボードの作成と編集以外にも、以下の操作を行うことができます。

- デフォルトのダッシュボードの設定と再ロード。「デフォルトのホーム ページの管理」（711 ページ）で説明しています。
- ダッシュボードの削除。「ダッシュボードの削除」（712 ページ）で説明しています。

注意

このセクションでは、ダッシュボードとその内容の定義および管理方法について説明しています。ダッシュボードの外観のカスタマイズ方法については、セクション「ダッシュボードの外観の変更」（702 ページ）で説明しています。

ここで説明しているダッシュボード管理タスクのほとんどは、[Dashboards list (ダッシュボード リスト)] ページまたは各ダッシュボードのツールバーから実行できます。[Dashboards list（ダッシュボード リスト）] ページの機能の概要については、「[Dashboards（ダッシュボード）] ページでのダッシュボードの管理」（713 ページ）を参照してください。表 91 に、ダッシュボード ツールバーのボタンで実行されるアクションを示します。

表 91：ダッシュボード ツールバーのボタン

ボタン	説明
[Reload（再ロード）]	使用可能な最新のデータが反映されるように、ダッシュボードとそのポートレットを再ロードします。
[New Dashboard（新しいダッシュボード）]	[Edit Dashboard（ダッシュボードの編集）] ページを開きます。このページでは、新しいダッシュボードの名前を入力し、このダッシュボードを他のユーザーが使用できるようにするかどうかと、コンソール メニュー（[Home（ホーム）] の下）に表示するかどうかを選択できます。また、このページでダッシュボードのポートレットを選択すると、[New Portlet（新しいポートレット）] ボタンを使用して新しいポートレットを作成できます。
[Copy Dashboard（ダッシュボードのコピー）]	現在のダッシュボードの [Edit Dashboard（ダッシュボードの編集）] ページを開きます。現在のポートレットがすべて含まれるように選択され、新しいダッシュボードの名前が「Copy of < 表示していたダッシュボード >」という形式で入力されています。任意の名前に変更できます。独自のバージョンの共有ダッシュボードを作成する必要がある場合、または既存のダッシュボードに含まれるポートレットのいくつかは使用しつつニーズに合わせてポートレットを追加または削除する場合、ダッシュボードのコピーを保存すると便利です。また、これによってコンソール メニューにダッシュボードを追加して、すべてのユーザーと共有することもできます。
[Edit Dashboard（ダッシュボードの編集）]	[Edit Dashboard（ダッシュボードの編集）] ページを開きます。ここで、新しいポートレットの作成や表示されるポートレットの変更など、現在のダッシュボードを変更できます。
[Delete Dashboard（ダッシュボードの削除）]	（確認ボックスで [OK] が選択された後で）現在のダッシュボードを削除します。「ダッシュボードの削除」（712 ページ）を参照してください。ホーム ページでは使用できません。

ボタン	説明
 [Reset to Default（デフォルトにリセット）]	システムが提供するダッシュボード（現在はホーム ページとシステム ダッシュボード）を、現在保存されているデフォルト設定にリセットします（次の「[Set as Default（デフォルトとして設定）]」を参照）。ユーザーが作成したダッシュボードに対しては使用できません。
 [Set as Default（デフォルトとして設定）]	この設定の保存後に作成されたアカウントを持つユーザーに対して、現在のダッシュボードをデフォルトのホーム ページとして設定します。「デフォルトのホーム ページの管理」（711 ページ）を参照してください。

共有ダッシュボード

自分だけが使用できる専用のダッシュボードも作成できますが、[Edit Dashboard（ダッシュボードの編集）] ページの [Share with all users（すべてのユーザーと共有）]チェックボックスをオンにすると、作成したダッシュボードを共有できます。

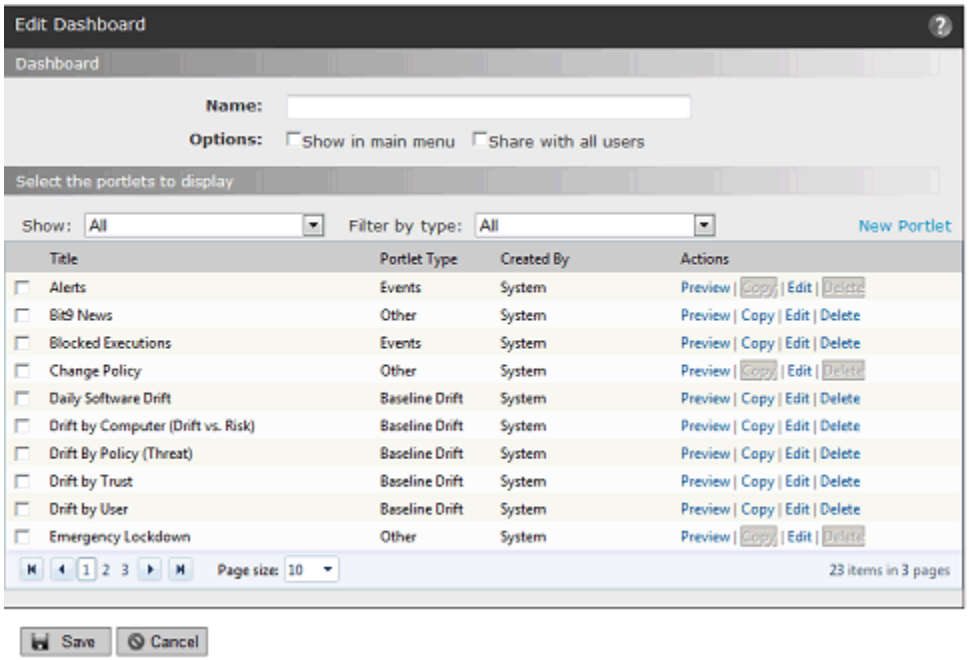
ダッシュボードが共有されている場合、Administrator グループまたは PowerUser ユーザー グループのコンソール ユーザー、共有ダッシュボードの管理権限を持つカスタム グループのコンソール ユーザーは、ダッシュボードを変更できます。また、削除することもできます。

共有したダッシュボードが他のユーザーにとって重要なものになっている可能性があることに注意してください。ダッシュボードの共有を無効にしたり、ダッシュボードを削除したりすると、他のユーザーはそのダッシュボードにアクセスできなくなります。原則として直ちにアクセスできなくなりますが、ダッシュボードを表示している場合は、そこから移動するとアクセスできなくなります。

新しいダッシュボードの作成

新しいダッシュボードの作成手順：

1. 次のいずれかの操作によって、新しいダッシュボードを作成して [Edit Dashboard（ダッシュボードの編集）] ページを開きます。
   - コンソール メニューで [**Reports**（レポート）] > [**Dashboards**（ダッシュボード）] の順に選択し、[Dashboards（ダッシュボード）] ページで [**Add Dashboard**（ダッシュボードの追加）] ボタンをクリックします。
     または
   - 任意のダッシュボードで、[Create New Dashboard（新しいダッシュボードの作成）] ボタンをクリックします。 



2. ［Name（名前）］ボックスで、新しいダッシュボードの名前を入力します。この名前は、このダッシュボードを表示すると左上に表示され、［Dashboards（ダッシュボード）］ページのダッシュボードのリストでも使用されます。
3. コンソール メニューの［Home（ホーム）］セクションにこのダッシュボードを追加するには、次の操作を行います。
   a. ［Options（オプション）］行で、［Show in main menu（メイン メニューに表示）］チェックボックスをオンにします。このチェックボックスをオンにしなくても、ダッシュボードは［Dashboards（ダッシュボード）］ページと、他のダッシュボードの［Dashboards（ダッシュボード）］メニューから使用できます。
   b. ダッシュボードに対して選択した名前とは別の（通常は短い）名前をメニューに表示するには、［Show（表示）］チェックボックスをオンにすると表示される［Menu name（メニュー名）］フィールドにその名前を入力します。
4. 他のユーザーがこのダッシュボードを使用できるようにするには、［Share with all users（すべてのユーザーと共有）］をオンにします。
5. このダッシュボードに追加する各ポートレットの左にあるチェックボックスをオンにします。ポートレット リストの下部にあるページ ボタン、またはリストの最上部にあるフィルターを使用して、関心のある使用可能なポートレットをすべて表示します。
   注意：ダッシュボードにポートレットを追加する前にポートレットの外観を確認するには、ポートレット名の右にある［**Preview**（プレビュー）］をクリックします。

6. リストに表示されていないポートレットが必要な場合は、「ポートレットの作成とカスタマイズ」（714 ページ）を参照してください。新しいポートレットが作成されたら、その名前の横にあるチェックボックスをオンにしてこのダッシュボードに追加します。
7. ［Save（保存）］をクリックします。新しいダッシュボードが保存され、［Dashboards（ダッシュボード）］ページのリストに追加されます。適切なチェックボックスをオンにした場合は、そのダッシュボード名がコンソール メニューの［Home（ホーム）］メニューに表示されます。

ダッシュボードのコピー

ダッシュボードをコピーすると、次のようなさまざまな状況で役立つことがあります。

- 他のユーザーが作成した共有ダッシュボードのコピーを自分で保持する場合
- 希望に近いダッシュボードがあるが、自分のニーズに合わせてポートレットを追加または削除、あるいは編集する場合

別の名前で既存のダッシュボードを保存する手順：

1. 次のいずれかの操作によって、ダッシュボードをコピーして［Edit Dashboard（ダッシュボードの編集）］ページを開きます。
   - コンソール メニューで［**Reports**（レポート）］>［**Dashboards**（ダッシュボード）］の順に選択し、［Dashboards（ダッシュボード）］ページでコピーするダッシュボードの横にある ボタンをクリックします。
     または
   - コピーするダッシュボードで、［Copy Dashboard（ダッシュボードのコピー）］ボタン をクリックします。
2. コピー元のダッシュボードと名前以外のすべてのパラメーターが同じ状態で、［Edit Dashboard（ダッシュボードの編集）］ページが開きます。名前は「Copy of < コピーしたダッシュボードの名前 >」という形式で表示されます。「Copy of」で始まるデフォルトの名前を、ダッシュボードで使用する名前に置き換えます。
3. 必要に応じて他のダッシュボード パラメーターを変更します。詳細については、「新しいダッシュボードの作成」（707 ページ）を参照してください。
4. このダッシュボードに表示しないポートレットを削除する場合は、ポートレット名の左にあるチェックボックスをオフにします。

   警告

   ポートレット名の右にある［Delete（削除）］リンクはクリックしないでください。クリックすると現在のダッシュボードからだけでなく、Bit9 Server からも完全に削除されます。

5. このダッシュボードに表示するポートレットを追加するには、ポートレット名の左にあるチェックボックスをオンにします。

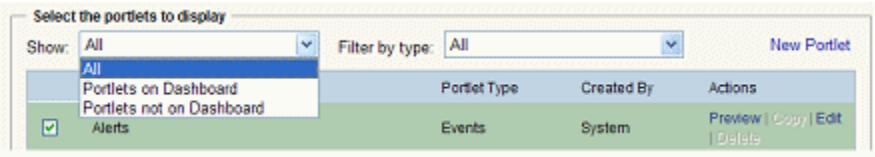
6. 新しいタイプのポートレットが必要な場合は、「ポートレットの作成とカスタマイズ」（714 ページ）を参照してください。新しいポートレットが作成されたら、その名前の横にあるチェックボックスをオンにしてこのダッシュボードに追加します。
7. ［**Save**（保存）］をクリックします。
コピーされたダッシュボードが、新しい名前とすべての変更内容が反映された状態で［Dashboards（ダッシュボード）］ページに表示されます。

ダッシュボードの編集

ダッシュボードを編集して、ポートレットの追加または削除、名前の変更、共有およびメニューオプションの変更を行うことができます。

ダッシュボードの編集手順：

1. 編集するダッシュボードを表示します。
2. ダッシュボード ツールバーの［Edit this dashboard（このダッシュボードの編集）］ボタン（鉛筆）をクリックします。［Edit Dashboard（ダッシュボードの編集）］ページが表示されます。
3. 必要に応じて、次のようなダッシュボード パラメーターを変更します。
   a. ポートレット名
   b. ［Show in main menu（メイン メニューに表示）］の選択
   c. メニュー名（［Show in main menu（メイン メニューに表示）］がオンの場合）
   d. ［Share with all users（すべてのユーザーと共有）］の選択
4. ［Edit Dashboard（ダッシュボードの編集）］ページのポートレット リストには、現在のダッシュボードにすでにあるポートレットを含め、すべてのポートレットが表示されます。このリストは、いくつかのオプションを使用してフィルターできます。
   a. 現在このダッシュボードにないポートレットのみをリストで表示するには、［Show（表示）］メニューで［**Portlets not on the dashboard**（ダッシュボードにないポートレット）］を選択します。



   b. リストに特定のタイプのポートレットのみを表示するには、［Filter by type（タイプでフィルター）］メニューでタイプを選択します。たとえば、［Computer（コンピューター）］ポートレットのみを表示するよう選択できます。ポートレット タイプの説明については、「ポートレット タイプとサブタイプ」（715 ページ）を参照してください。

［Show（表示）］メニューでの選択と［Filter（フィルター）］メニューでの選択を組み合わせることができます。これらのメニューでの選択は、［Edit Dashboard（ダッシュボードの編集）］ページの表示内容にも影響しますが、ダッシュボードの表示内容には影響しません。

c. リスト全体が表示されているか、フィルターされているかどうかに関係なく、複数のページにわたっている場合は、リスト下部のページ番号または矢印をクリックして他のページに移動できます。リストの右下隅の凡例に、現在のリストの項目数とページ数が示されます。

5. リスト内の各ポートレットの横にある［**Preview**（プレビュー）］ボタンを使用して、ダッシュボードでリストがどのように表示されるかを確認できます。
6. 各ポートレットの名前の左にあるチェックボックスをオンにすると、ダッシュボードに追加されます。
現在リストで見つからないポートレットを作成する必要がある場合は、「ポートレットの作成とカスタマイズ」（714 ページ）を参照してください。
7. 各ポートレットの名前の横にあるチェックボックスをオフにすると、ダッシュボードから削除されます。
注意：ポートレット名の右にある［Delete（削除）］リンクはクリックしないでください。クリックすると現在のダッシュボードからだけでなく、Bit9 Server からも完全に削除されます。
8. 追加するすべてのポートレットをオンにしたら、［**Save**（保存）］ボタンをクリックします。新しいポートレットが追加された状態で、ダッシュボードが再表示されます。
9. 新しいポートレットを表示するためにダッシュボード全体のレイアウトを変更する必要がある場合は、［Dashboard Layout（ダッシュボード レイアウト）］メニューを使用して変更します。詳細については、「ダッシュボードのレイアウトの変更」（703 ページ）を参照してください。
10. 必要に応じて、新しいポートレットを表示できるようにダッシュボード上のポートレットを移動します。ポートレットの移動方法がわからない場合は、「ポートレットの移動」（705 ページ）を参照してください。

デフォルトのホーム ページの管理

次のように、ダッシュボードには 2 つのホーム ページ管理ボタンがあります。

- ［Reset to Default（デフォルトにリセット）］ボタン  を使用すると、変更されている可能性がある現在のホーム ページをデフォルトのホーム ページにリセットできます。
- ［Set as Default（デフォルトとして設定）］ボタン  を使用すると、Administrator 権限または PowerUser 権限（あるいはカスタムの共有ダッシュボードの管理権限）を持つユーザーは、現在のダッシュボードを新しいユーザーのデフォルトのホーム ページとして保存できます。

別のデフォルトのホーム ページを設定すると、［Reset to Default（デフォルトにリセット）］ボタンを使用するすべてのユーザーにとって、そのページがホーム ページとなります。このページは、デフォルトの変更後に初めてログインする新しい

コンソール ユーザーにとっても、デフォルトのホーム ページになります。デフォルトのホーム ページが変更される前にすでにログインしていたユーザーについては、この変更を行う権限があるユーザーが［Reset to Default（デフォルトにリセット）］ボタンをクリックした場合を除いて、既存のホーム ページが保持されます。

注意

確実に元のホーム ページに戻せるようにするには、自分（または他のユーザー）が変更する前に、［Copy Dashboard（ダッシュボードのコピー）］コマンドを使用してホーム ページをコピーし、コピーの名前を変更してバックアップを保持します。必要に応じて、［Set as Default（デフォルトとして設定）］を使用してバックアップからホーム ページを復元できます。

ダッシュボードの削除

作成したダッシュボードと、（ReadOnly ユーザーとしてログインしていない場合は）使用可能な共有ダッシュボードは削除できます。どのユーザーも削除できないダッシュボードは、ホーム ページのみです。

共有ダッシュボードの削除を選択すると、ダッシュボードが共有されていることがダイアログ ボックスで警告され、削除を確認するかキャンセルすることができます。他の Bit9 コンソール ユーザーが共有ダッシュボードを使い続ける必要がある可能性があるため、共有ダッシュボードを削除するときは注意してください。削除したときに別のユーザーがダッシュボードを使用している場合、そのダッシュボードはユーザーが移動するまで表示され続け、移動した時点で使用できなくなります。

ダッシュボードの削除手順：

1. 次のいずれかの方法で削除処理を開始します。
   - コンソール メニューで［**Reports**（レポート）］>［**Dashboards**（ダッシュボード）］の順に選択し、［Dashboards（ダッシュボード）］ページで、削除するダッシュボードの名前の横にある削除 (x) ボタンをクリックします。
     または
   - 削除するダッシュボードで、［Delete Dashboard（ダッシュボードの削除）］ボタン  をクリックします。
2. 表示される確認ダイアログで、このダッシュボードを削除して問題がなければ［**Yes**（はい）］をクリックします。ダッシュボードが削除されます。削除したときにそのダッシュボードを表示していた場合は、ホーム ページに置き換えられます。

[Dashboards（ダッシュボード）] ページでのダッシュボードの管理

[Dashboards（ダッシュボード）] ページには、使用可能なすべてのダッシュボードのリストと、ダッシュボードを管理するためのコントロールが表示されます。この章の他のセクションで説明する手順の多くでは、タスクを実行する代替手段に関連して [Dashboards（ダッシュボード）] ページに言及しています。

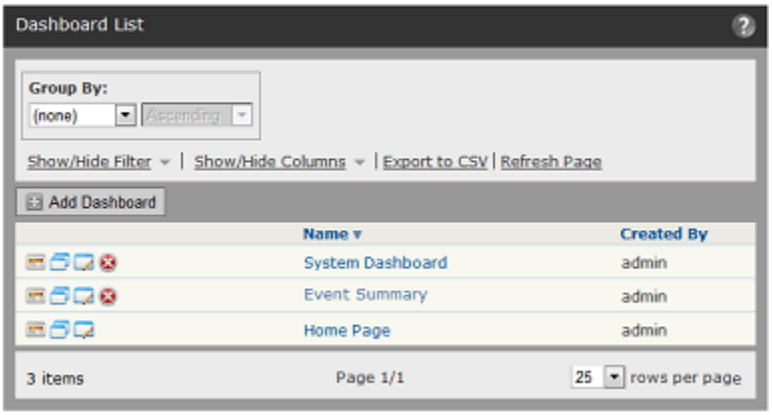


表 92 に、このページで使用できるダッシュボード固有のアクションを示します。ダッシュボードをすでに表示しているときに使用できる同様のコマンドについて、表 91 も参照してください。

表 92：ダッシュボード リストのボタンとリンク

ボタン / リンク	説明
[Add Dashboard（ダッシュボードの追加）]	[Edit Dashboard（ダッシュボードの編集）] ページを開きます。ここでデータを入力して、新しいダッシュボードを作成、構成できます。詳細については、「新しいダッシュボードの作成」（707 ページ）を参照してください。
 [View Dashboard（ダッシュボードの表示）]	このボタンをクリックすると、この行にダッシュボードが表示されます。概要については、「ダッシュボードの概要」（694 ページ）を参照してください。
 [Copy Dashboard（ダッシュボードのコピー）]	現在のダッシュボードのポートレットとその他の設定を「Copy of <現在のダッシュボード>」という名前の新しいダッシュボードにコピーし、[Edit Dashboard（ダッシュボードの編集）] ページを開きます。任意の名前に変更できます。独自のバージョンの共有ダッシュボードが必要な場合、または既存のダッシュボードがテンプレートに適している場合は、ダッシュボードのコピーを保存することが役立ちます。詳細については、「ダッシュボードのコピー」（709 ページ）を参照してください。
 [Edit Dashboard（ダッシュボードの編集）]	この行のダッシュボードの［Edit Dashboard（ダッシュボードの編集）］ページを開きます。ここで、新しいポートレットの作成や表示されているポートレットの変更など、ダッシュボードを変更できます。詳細については、「ダッシュボードの編集」（710 ページ）を参照してください。
 [Delete Dashboard（ダッシュボードの削除）]	（確認ボックスで [OK] が選択された後で）この行のダッシュボードを削除します。詳細については、「ダッシュボードの削除」（712 ページ）を参照してください。ホーム ページでは使用できません。
ダッシュボード名のリンク	リスト内のダッシュボード名をクリックすると、ダッシュボードが表示されます。

ポートレットの作成とカスタマイズ

ダッシュボード管理機能以外にも、[Edit Dashboard（ダッシュボードの編集）] ではポートレット管理機能を使用して、次の操作を実行できます。

- 既存のポートレットの編集
- 新しいポートレットの作成
- 既存のポートレットのコピーと変更
- ポートレットの削除

Administrator 権限または PowerUser 権限を持つユーザー、またはダッシュボード管理権限を持つカスタム グループのユーザーが、これらの機能を使用できます。作成や削除など、ポートレットに対する変更はすべて、あらゆる Bit9 コンソール ユーザーに影響します。つまり「個人用の」ポートレットはありません。

ポートレット タイプとサブタイプ

ポートレットは、タイプとサブタイプによって整理されます。タイプとサブタイプごとにポートレットの機能は異なります。また、作成や編集の際に使用できる入力パラメーターも異なります。タイプは次のとおりです。

- **イベント：**これらのポートレットには、一定期間にブロックされたファイル拡張子の数や、トリガーされたアラートなど、Bit9 データベースから得られるイベント情報が表示されます。
- **ベースライン ドリフト**：これらのポートレットには、日次でのソフトウェアのベースラインからのドリフトや、ベースラインから最も逸脱したコンピューターのリストなど、ベースライン ドリフト分析の結果が表示されます。
- **コンピューター：**これらのポートレットには、実行中のオペレーティング システム別のコンピューターの数や適用レベル別のコンピューターの数など、システム上のコンピューターについて Bit9 Server で入手可能な情報が表示されます。
- **ファイル：**これらのポートレットには、時間の経過とともに新しく確認されたファイルの数やシステム上のファイルのカテゴリ（ブラウザー、ユーティリティ、メッセージングなど）など、エージェントが管理するコンピューターのファイルの情報が表示されます。
- **その他:** これらのポートレットでは、外部の URL からの RSS フィードや情報が表示されることがあります。また、指定した HTML ページが表示されることもあります。このカテゴリには、緊急ロックダウン ボタンなど、システム作成の特殊な「アクション」ポートレットや、Bit9 データベースから得られるさまざまなタイプの情報の組み合わせも含まれています。

システム ポートレット

Bit9 コンソールのインストールには、多くの事前構成されたポートレットが付属しています。これらの一部はホーム ページに表示されます。また、使用するサイトの他のダッシュボードに表示されることもあります。システム ポートレットは、[Edit Dashboard（ダッシュボードの編集）] ページの［Created By（作成者）］列に表示される「System（システム）」という名前で識別できます。

［Emergency Lockdown（緊急ロックダウン）］ポートレットや［Change Policy（ポリシー変更）］ポートレットなど一部のポートレットは、特殊なポートレットとして設計されていて、コピーしたり編集したりすることはできません（この行の［Copy（コピー）］リンクや［Edit（編集）］リンクはグレー表示になります）。これらのポートレットは、名前と説明のみを変更できます。

ポートレットの詳細の編集

ポートレットを編集して、外観や表示されるデータを変更できます。たとえば、必要なデータを確認するには、縦棒グラフよりも円グラフのほうが見やすいと判断したとします。ポートレットを編集するには、ダッシュボードに現在表示されているポートレットから、または［Edit Dashboard（ダッシュボードの編集）］ページのポートレット リストから、［Portlet Details（ポートレットの詳細）］ページを開きます。

編集可能な個々のパラメーターの詳細については、「カスタム ポートレットの作成」（717 ページ）を参照してください。

現在表示されているダッシュボードでのポートレットの編集手順：

1. 編集するポートレットの右上にある［Edit（編集）］ボタン  をクリックします。
   ［Portlet Details（ポートレットの詳細）］ページが表示されます。
2. ［Portlet Details（ポートレットの詳細）］ページで、設定に対するすべての必要な変更を行います。必要に応じて、［**Show Advanced Details**（高度な詳細を表示）］ボタンをクリックして、追加の編集オプションを使用します。
3. ページ下部の［**Preview**（プレビュー）］リンクを使用すると、変更の効果を確認できます。［Preview（プレビュー）］パネルを表示するために、ブラウザー ウィンドウを下方向にスクロールする必要がある場合があります。プレビューを表示したまま引き続き変更を行い、［**Refresh**（更新）］をクリックして結果を確認することができます。プレビューを終えたら、［**Close**（閉じる）］をクリックします。
4. 加えた変更に問題がなければ、［Portlet Details（ポートレットの詳細）］ページの下部にある［Save（保存）］をクリックします。加えたすべての変更がポートレットに反映された状態で、現在のダッシュボードが表示されます。

ポートレット カタログを使用すると、現在のダッシュボードのいずれかにポートレットが表示されるかどうかに関係なく、ポートレットを編集できます。

［Edit Dashboard（ダッシュボードの編集）］テーブルでのポートレットの編集手順：

1. ［Edit Dashboard（ダッシュボードの編集）］ページで、編集するポートレットを見つけます。
2. ポートレットのリストで、編集するポートレットの名前の右にある［**Edit**（編集）］リンクをクリックします。［Portlet Details（ポートレットの詳細）］ページが表示されます。
3. 前の手順の説明に従って編集します。

ポートレットの削除

警告

コンソール ユーザーは、Administrators グループまたはダッシュボード管理権限を持つカスタム グループのメンバーであれば、［Edit Dashboard（ダッシュボードの編集）］ページでポートレットを削除できます（一部のシステム ポートレットを除く）。この機能は、すべてのユーザーが使用するすべてのダッシュボードからポートレットを削除するため、注意して使用してください。

ポートレットを恒久的に削除する手順：

1. 任意のダッシュボードまたは［Dashboards（ダッシュボード）］ページで、［Edit Dashboard（ダッシュボードの編集）］（鉛筆）ボタンをクリックします。［Edit Dashboard（ダッシュボードの編集）］ページが表示されます。
2. ポートレットのリストで、削除するポートレットの横にある［**Delete**（削除）］をクリックします。確認ダイアログが表示され、このポートレットを使用するダッシュボードの数に関する情報などが示されます。このポートレットを Bit9 環境から削除してよいかどうかを確認してください。このポートレットは、すべてのユーザーにとって恒久的に削除されます。
3. このポートレットを削除してよいことが間違いない場合は、確認ダイアログで [**OK**] をクリックします。［Edit Dashboard（ダッシュボードの編集）］ページのポートレット リストからポートレットが削除されます。このポートレットを含むすべてのダッシュボードから削除されます。

ユーザーがこのポートレットを含むダッシュボードを表示している場合は、ユーザーが再ロードするか、ダッシュボードから移動するまでポートレットは引き続き表示されます。

カスタム ポートレットの作成

ダッシュボードでは、Bit9 が作成したポートレットを使用できるだけでなく、独自のポートレットを作成して使用することもできます。さまざまなポートレット タイプのリストから、Bit9 が管理するアセットおよびルールのデータを表示するのに適したものを選択し、そのレポートのデータの外観を必要に合わせて構成できます。

カスタム ポートレットは、その作成者に関係なく、すべてのコンソール ユーザーが［Edit Dashboard（ダッシュボードの編集）］ページから使用できます。ただし、ReadOnly ユーザーは、ポートレットを作成したり変更したりすることはできません。

ポートレットの詳細を入力するときには、［Portlet Details（ポートレットの詳細）］ページでさまざまな設定を試して［**Preview**（プレビュー）］ボタンをクリックすることをお勧めします。プレビュー機能は、そのポートレットに対して互換性のない設定を選択したときに通知するデバッガーとして、また、ダッシュボードにカスタム ダッシュボードを追加する前にさまざまなグラフやデータ群を試すための手段として役立ちます。

カスタム ポートレットの作成手順：

1. 現在表示されているダッシュボードで、または［Dashboards list（ダッシュボード リスト）］で任意のダッシュボードの名前の横にある、［Edit Dashboard（ダッシュボードの編集）］ボタンをクリックします。
2. ［Edit Dashboard（ダッシュボードの編集）］ページで、［**New Portlet**（新しいポートレット）］をクリックします。［New Portlet（新しいポートレット）］ページが表示されます。

3. ［New Portlet（新しいポートレット）］ページで、［Select portlet type（ポートレット タイプの選択）］メニューからタイプを選択します。ポートレット タイプの説明については、「ポートレット タイプとサブタイプ」（715 ページ）を参照してください。
4. 複数の選択肢がある場合は、［Select subtype（サブタイプの選択）］メニューからサブタイプを選択します。
5. ［**Next**（次へ）］をクリックします。［Portlet Details（ポートレットの詳細）］ページが表示されます。これは、ポートレットを編集するときに表示されるのと同じ［Portlet Details（ポートレットの詳細）］ページです。

注意

ポートレットのタイプとサブタイプによって、ポートレットの基本構造と、［Portlet Details（ポートレットの詳細）］ページで使用可能な選択肢の多くが決定されます。これらは、一度選択すると編集できません。ポートレットの作成中にタイプまたはサブタイプの変更が必要になった場合は、［**Cancel**（キャンセル）］をクリックしてやり直してください。

ポートレットの詳細の追加

6. ［Portlet Details（ポートレットの詳細）］ページで、以下を含む全般的な詳細を入力します。
   a. ［**Title（タイトル）**］: ポートレット上、および［Edit Dashboard（ダッシュボードの編集）］ページのポートレット リストに表示するタイトルを入力します。
   b. ［**Description（説明）**］: ポートレットの目的の短い説明や使用方法など、このポートレットの情報ボタンをユーザーがクリックしたときに表示される情報を入力します。
7. ［Portlet Details（ポートレットの詳細）］ページに、［Baseline Drift details（ベースライン ドリフトの詳細）］や［RSS details（RSS の詳細）］など、ポートレット タイプに固有のパネルが表示される場合は、必要な情報をパネルに入力してから［**Next**（次へ）］をクリックします。
   ［Next（次へ）］リンクの代わりに［**Save**（保存）］リンクが表示されている場合は、クリックすると新しいポートレットは保存され、カタログと現在のダッシュボードに追加されます。ポートレット タイプによっては、これ以上の構成は不要です。
8. ［Data Presentation（データ表示）］パネルが表示される場合は、グラフ タイプとして［Table（テーブル）］を選択できます。
   - ［**Table**（テーブル）］を選択した場合は、列と列の順序を選択し、手順 14. に進みます。テーブル ポートレットの構成方法の詳細については、「ポートレットでのテーブルの使用」（722 ページ）を参照してください。
   - その他のデータ表示タイプを選択した場合は、手順 9. に進みます。

9. ［Graph Settings（グラフ設定）］パネルがページに表示される場合は、このポートレットのデータの表示方法について詳細を指定します。使用可能な選択肢はポートレットのタイプとサブタイプによって異なりますが、表 93 に示しているものが一般的です。
10. グラフ設定の選択を終了したら、［**Preview**（プレビュー）］をクリックしてポートレットの外観を確認します。グラフ タイプを変えるなど、さまざまな設定を試して最適な設定を見つけることができます。設定を変更したときは、［**Refresh**（更新）］を使用してプレビューを更新します。
11. このポートレットのグラフの基本的な外観を指定したら、次の 2 つのうちのいずれかを実行できます。
    a. 高度なグラフィックの詳細の表示と変更を行わない場合は、［Save（保存）］をクリックして［Edit Dashboard（ダッシュボードの編集）］ページにポートレットを追加します。
    b. 追加のグラフィック設定を表示する場合は、［**Show Advanced Settings**（高度な設定の表示）］ボタンをクリックします。
12. 高度なグラフィック設定を確認するときは、表 94 に示された選択肢を使用できます。高度な設定の一部は、グラフ タイプによっては適切（または使用可能）ではありません。
13. 高度な詳細を入力した場合は、保存する前に［**Preview**（プレビュー）］リンクをもう一度クリックしてポートレットを確認できます。
14. 作成するポートレットの［Portlet Details（ポートレットの詳細）］ページにフィルター パネルがあり、ポートレット（グラフィック ポートレットとテーブルのみのポートレットの両方）で使用するデータをフィルターする場合は、必要なフィルターを構成します。詳細については、「ポートレットでのフィルターの使用」（726 ページ）を参照してください。
15. ポートレットの外観とデータに問題がなければ、［Save（保存）］をクリックしてポートレット カタログと現在のダッシュボードにポートレットを追加し、ポートレット エディターを閉じます。

表 93：ポートレットのグラフィック設定

設定	説明
[Chart type（グラフ タイプ）]	このメニューは、選択したポートレット タイプとサブタイプのデータの表示方法をリストで示します。リストには、点、棒、円の各グラフなどの選択肢があります。
[X-axis（X 軸）]	選択したポートレット タイプやサブタイプに使用できる属性のタイプをリストで示します。グラフの X 軸上に配置する属性のタイプ（コンピューター名など）を選択します。グラフのタイプによっては、ここでの選択によって決定されるのは X 軸に表示されるデータではなく、円グラフの各スライスが表すデータなど、別の形式での基礎データです。
[Limit to the 5|10|15 highest|lowest values（最大値または最小値から 5、10、15 個に制限）]	個々のコンピューターなどのデータを X 軸に配置すると、データの数が多すぎるためポートレット内に効果的に表示できない可能性があります。[Limit to（制限）] チェックボックスとメニューを使用すると、表示する項目（ドリフトなど）を最大値または最小値からの 5、10、または 15 個に制限してデータを表示できます。これらの制限を使用すると、最も重要な情報が表示され、狭いスペースに大量の情報が配置されることがなく、実用的なグラフィックを表示できます。散布図や「自動分割」機能を使用する列など、グラフ タイプによってはこのボックスは表示されません。
[Group by（グループ別）]	グラフ タイプに [Scatter（散布図）] を選択した場合にのみ表示されます。[Group by（グループ別）] の値を選択した場合、散布図の点は各グループ メンバーの値ではなく、指定したグループの合計値を表します。たとえば、[Group by（グループ別）] の値に [Policy（ポリシー）] を選択すると、点は個々のコンピューターの Y 値を表すのではなく、ポリシーのすべてのコンピューターの Y 値を表します。
[Exclude "Unknown" X-axis values（「未知の」X 軸の値を除外）]	このチェックボックスをオンにすると、未知の X 軸の値を持つデータは図またはグラフに表示されません。この方法でも、有用性の低い情報がポートレットに表示されるのを避けることができます。

設定	説明
[Split by（分割する基準）]	X 軸データを分割する値を持つ情報のタイプを指定します。たとえば、未加工のドリフトをポリシー別に表示するポートレットを作成することができます。[Split by（分割する基準）] を使用すると、選択した列の一意の値ごとに系列（棒、列、またはセグメント）を作成できるため、あるポリシーに含まれるすべてのコンピューターを表す棒を（色によって）分割して、各コンピューターがドリフトにどれだけの影響を与えているか示すことができます。
[Metrics（メトリック）]	グラフの Y 軸に表示できる属性の選択肢をリストで表示します。作成するポートレット タイプで選択できる値が 1 つだけの場合は、ドロップ ダウン メニューになります。複数のタイプを選択できる場合は、複数選択メニューとなり、[Available（使用可能）] 列から [Selected（選択済み）] 列に、またはその逆に複数の項目を移動できます。使用可能と示されているメトリックは、どれでも追加できます。たとえば、グローバル状態別に一意のファイルを示す棒グラフの場合、[Count（件数）] を追加して各状態のファイル数を表示し、さらに [Prevalence（普及度）] を追加してコンピューター上の各タイプのファイル数を表示することができます。
[Show table below graph（グラフの下にテーブルを表示）]	オンにすると、このポートレットで使用できるテーブル列のリストが表示されます。表示する列を [Selected（選択済み）] 列に移動します。詳細については、「ポートレットでのテーブルの使用」（722 ページ）を参照してください。

表 94：ポートレットの高度な設定

設定	説明
[Height（高さ）]	ピクセル単位でポートレットの高さを選択するか、ダッシュボードによるポートレットのサイズ設定（自動）を使用します。[Auto（自動）] 以外の値を選択すると、ポートレットが適切に表示されない場合があります。
[Show X axis title（X 軸のタイトルを表示）] / [Show axis titles（軸のタイトルを表示）]	チェックボックスがオンの場合、ポートレットのグラフに X 軸のタイトル（グラフの詳細の X 軸のボックスに表示されるタイトル）が表示されるか、X 軸と Y 軸が表示されている場合は、それぞれにタイトルが表示されます。
[X-axis labels（X 軸のラベル）]	[None（なし）] 以外を選択した場合は、位置や方向の選択に基づいてグラフ上のデータ ポイント（棒グラフの棒など）にラベルが追加されます。[Auto（自動）] を選択すると、ダッシュボードによって最適な位置にラベルが配置されます。
[Legend（凡例）]	[None（なし）] 以外のボタンをクリックすると、グラフ要素を説明する凡例が指定した場所に表示されます。たとえば、全体システムと接続システムにそれぞれ異なる色を使用することで、凡例によって識別できます。
[Include tooltips（ツールチップを含める）]	（凡例の代替機能）このチェックボックスが使用可能でオンになっている場合は、マウス カーソルをグラフ要素の上に置くと、要素が表す内容を説明するツールチップが表示されます。
[Show Data Point Values（データ ポイントの値の表示）]	ボックスがオンの場合は、ポートレットのグラフに Y 値（または同等の値）が表示されます。たとえば、ある列が 3 台のコンピューターを表している場合は、3 という数字がその列の上に表示されます。
[Draw 3D（3D を描画）]	チェックボックスがオンの場合、表示されるグラフには 3D 効果が適用されます。
[Use logarithmic scale（対数目盛りの使用）]	チェックボックスがオンの場合は、表示されているデータの目盛りが均等から対数に変更されます。

ポートレットでのテーブルの使用

ポートレットの内容がテーブルでの表示に適している場合は、[Portlet Details（ポートレットの詳細）] ページに表示される 2 つのテーブル オプションを使用できます。

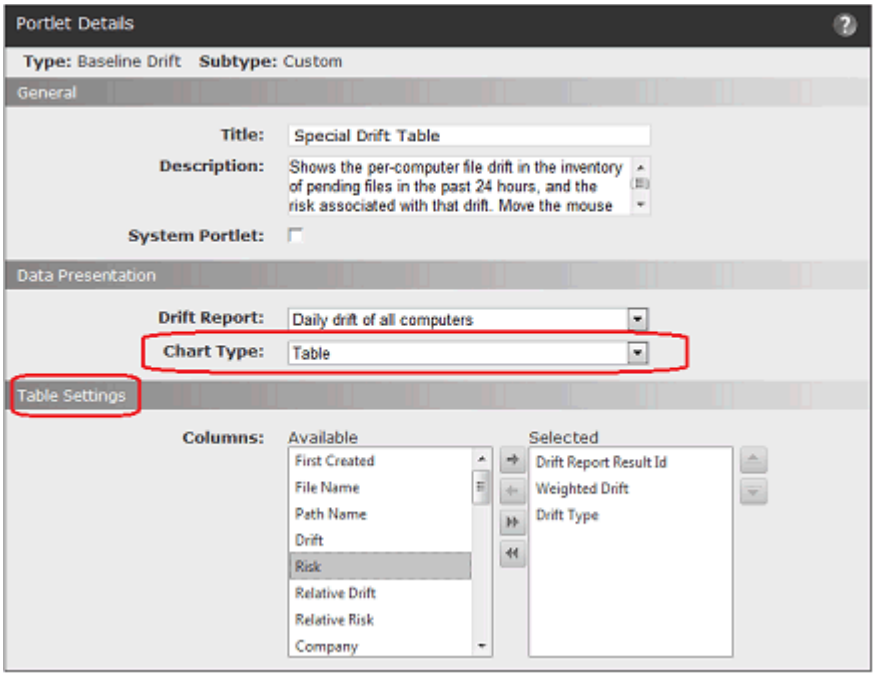
- **テーブルのみ**：[Portlet Details（ポートレットの詳細）] ページの [Chart type（グラフ タイプ）] メニューでテーブル オプションを使用できます。これは、ポートレットにグラフィックのグラフを表示しない場合に選択するオプションです。
- **補足テーブル**：主要なグラフ タイプがテーブル以外の場合は、[Show table below graph（グラフの下にテーブルを表示）] チェックボックスが [Graph

Settings（グラフ設定）］パネルの下部に表示されます。このチェックボックスをオンにすると、グラフィックとテーブルの両方が表示されます。

テーブルのみのポートレット

グラフィック表示に適さない Bit9 データをダッシュボードに表示する場合は、テーブルのみのポートレットを選択することをお勧めします。たとえば、何らかの基準を満たすコンピューターやファイルの数には関心がなく、各コンピューターや各ファイルごとにさまざまな種類のデータを詳細に把握することに関心がある場合などです。

テーブルのみの表示が可能な場合は、［Portlet Details（ポートレットの詳細）］ページに［Data Presentation（データ表示）］パネルが表示されます。このパネルでは、グラフ タイプに［**Table**（テーブル）］を選択できます。このオプションを選択すると、［Portlet Details（ポートレットの詳細）］ページの［Graph Settings（グラフ設定）］パネルは［Table Settings（テーブル設定）］パネルに置き換えられます。ここで、テーブルに含めるデータを選択し、順序を指定します。

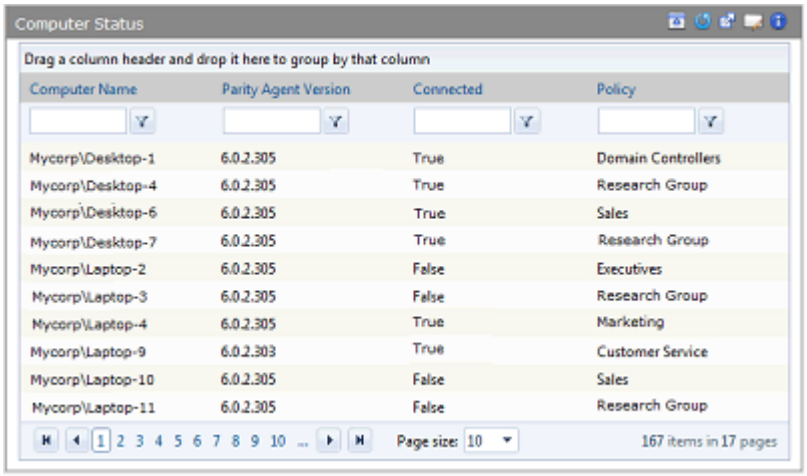


テーブルに表示する列は、選択する必要があります。データ要素をダブルクリックすることによって、［Available（使用可能）］列と［Selected（選択済み）］列の間で相互に移動することができます。また、矢印ボタンを使用して項目を［Available（使用可能）］と［Selected（選択済み）］の間で移動したり、テーブルのデータの順序を変更したりすることもできます。

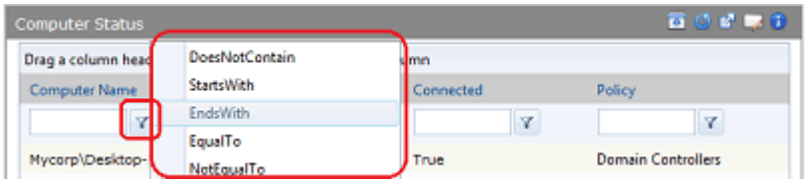
次のようにテーブル ポートレットには、表示するデータを並べ替えるさまざまな機能があります。

- テーブルが複数ページにわたる場合は、ポートレットの左下にあるページ ボタンや矢印ボタンを使用してページ間を移動することができます。
- テーブルに表示する列の数は、選択するページ サイズを変更することで決定できます（10 行単位）。

- 列の上をクリックして、テーブルの別の場所に列をドラッグできます。
- 列見出しの上をクリックして、ポートレットの最上部にあるラベル付きのゾーンにドラッグすると、列見出しで指定されたデータでテーブルをグループ化することができます。
- 列見出しでテーブルの内容をフィルターして、関心のあるデータを表示できます（［Portlet Details（ポートレットの詳細）］ページのフィルターを使用して、データを事前にフィルターすることもできます）。
- 列見出しをクリックして、その列のデータを並べ替えることができます。



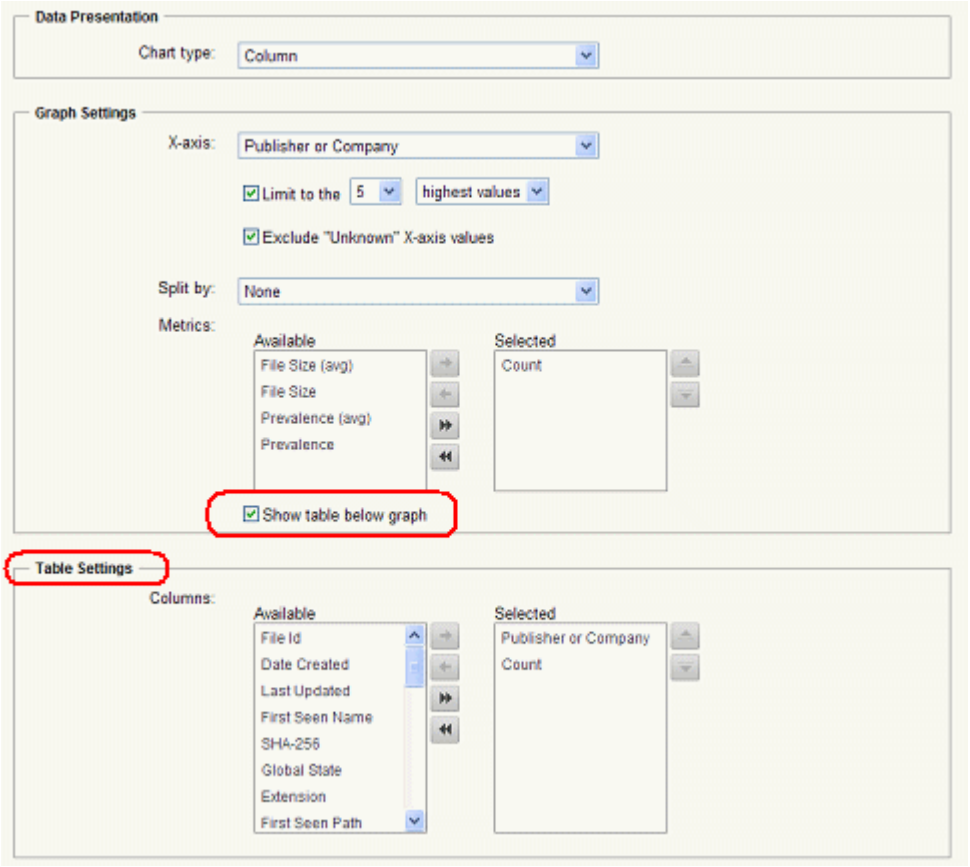
列でフィルターするには、列の下のボックスに文字列を入力します。たとえば、「Laptop」という文字列を［Computer Name（コンピューター名）］列に入力します。次にフィルター ボタンをクリックして演算子メニューを表示します。このメニューでは、データをフィルターするために、入力した文字列をどのように使用するかを選択できます。



ポートレットの補足テーブル

グラフィック ポートレット内に補足テーブルを追加できます。スペースが共有されているため、複雑な補足テーブルを作成することはあまり考えられません。

補足テーブルを使用できる場合は、［Graph Settings（グラフ設定）］パネルの下部に［Show table below graph（グラフの下にテーブルを表示）］チェックボックスが表示されます。このチェックボックスをオンにすると、［Table Settings（テーブル設定）］パネルが表示されます。



テーブルに表示する列を選択する必要があります。[Graph Settings（グラフ設定）]で選択したメトリックはテーブルにはインポートされません。データ要素をダブルクリックすることによって、[Available（使用可能）]列と[Selected（選択済み）]列の間で相互に移動することができます。また、矢印ボタンを使用して項目を[Available（使用可能）]と[Selected（選択済み）]の間で移動したり、テーブルのデータの順序を変更したりすることもできます。

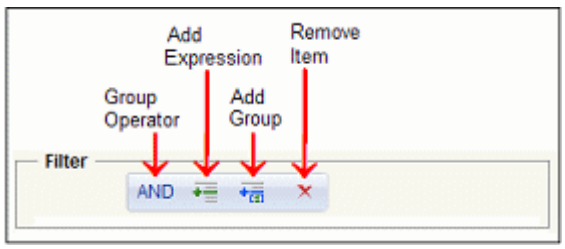
Publisher or Company	Count
Apple Inc.	4005
Business Objects	4327
Mercury Interactive Corp.	3838
Microsoft Corporation	50543
Sun Microsystems Inc.	8145

テーブルのみのポートレットと同様に、列をドラッグアンドドロップして並べ替えたり、列見出しをクリックしてデータを並べ替えたりすることができます。列でグループ化したり、テーブル自体にあるデータをフィルターしたりすることはできません。

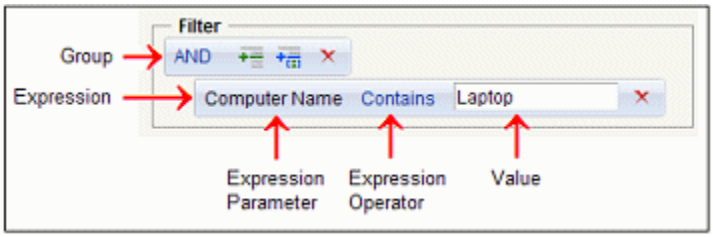
ポートレットでのフィルターの使用

一部のポートレットでは、フィルターを使用することにより、ポートレットに表示される情報を制限したり、ポートレットに表示される情報に焦点を絞ったりすることができます。たとえば、コンピューターの接続ステータスを表示するポートレットを作成し、可視性モード ポリシーのステータスは除外することができます。

フィルターは RSS フィードや HTML ページなどの一部のポートレットでは無効で、Bit9 Server とともにインストールされる事前構成済みのポートレットでは使用されません。作成または編集するポートレットにフィルター機能がある場合は、[Portlet Details（ポートレットの詳細）] ページに［Filters（フィルター）］パネルが表示されます。次の図は、ポートレット フィルターの初期状態の構成要素を示しています。



この初期状態のフィルター ビューには、最上位のグループ演算子が表示されます。フィルターで実際に処理を行うには、少なくとも 1 つの式を追加する必要があります。式とはパラメーターのセットで、Bit9 データに対して true（真）または false（偽）と評価されます。たとえば、ポートレット データのコンピューターの名前に「Laptop」を含むコンピューターのみをフィルターに指定するには、次のフィルターを作成します。



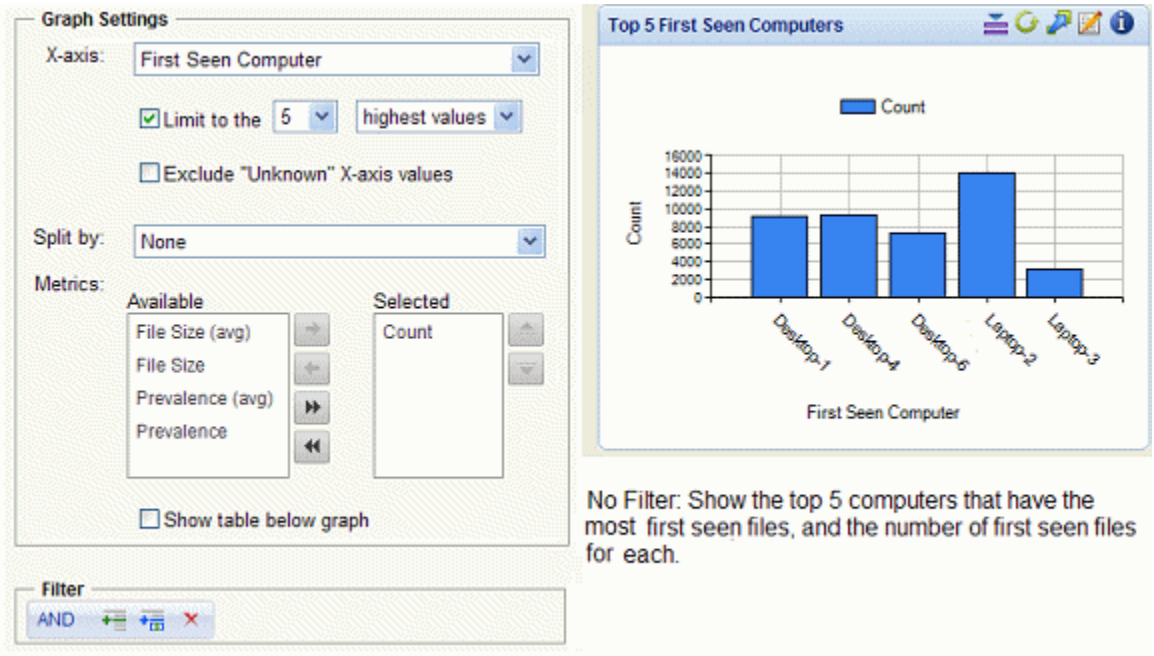
それぞれの式は、Bit9 データベースで使用可能なデータの種類であるパラメーター、式演算子、および値で構成されます。パラメーターと演算子はメニューから選択しますが、ポートレットのタイプとサブタイプによってメニューは異なります。一致対象となる値は入力します。

グループに式が 1 つしかない場合でも、すべての式はグループに属します。式はそれ自体で true と評価される場合もありますが、グループ演算子は表 95 に示すように、グループが true であるかどうかが判断されます。

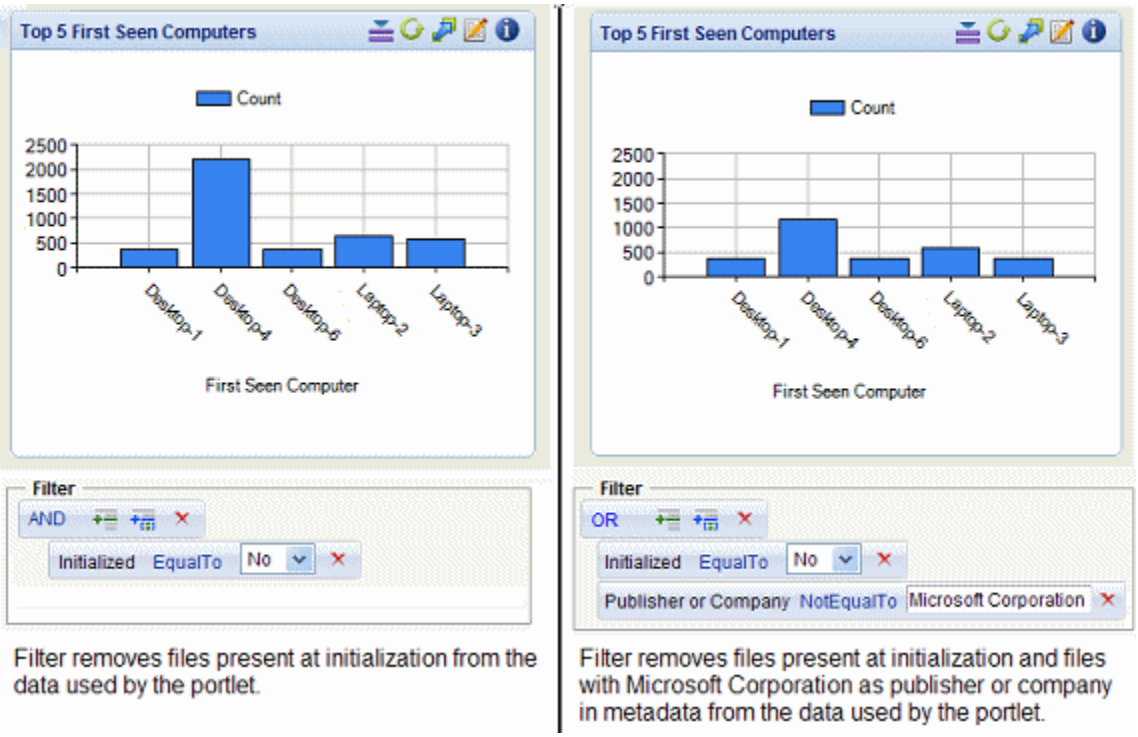
表 95：ポートレット フィルターのグループ演算子

演算子	効果
AND	グループのすべての式が true の場合、そのグループは true となります。最上位のグループの場合は、グループ内のすべての式が true となるデータがポートレットに表示されます。
OR	グループの 1 つ以上の式が true の場合、そのグループは true となります。最上位のグループの場合は、グループ内の 1 つ以上の式が true となるデータがポートレットに表示されます。
NOTAND	グループの 1 つ以上の式が false の場合、そのグループは true となります。最上位のグループの場合は、グループ内の 1 つ以上の式が false となるデータがポートレットに表示されます。
NOTOR	グループのすべての式が false の場合、そのグループは true となります。最上位のグループの場合は、グループ内のすべての式が false となるデータがポートレットに表示されます。

AND をグループ演算子として使用し、式が 1 つのみの場合、式が true であればグループは true となり、その式に一致するデータがポートレットに表示されます。ただし、表で説明しているように、式を追加し、他の演算子を使用すると、より効果の高い詳細なフィルターを作成できます。次の図にいくつかの例を示します。



上で詳しく示している［Top 5 First Seen Computers（初めて発見されることが多い上位 5 台のコンピューター）］ポートレットを作成すると、初めて発見されるファイルの数が最も多い 5 台のコンピューターが表示されます。このデータにはフィルターがないことに注意してください。そこで、Bit9 エージェントがインストールされた時点にコンピューターに存在したファイルについてはデータを除外し、その後に発見されたファイルに注目することが考えられます。これを行うために、左下の図のように、式を追加して「初期化済み」ファイルを除外するフィルターを作成できます。



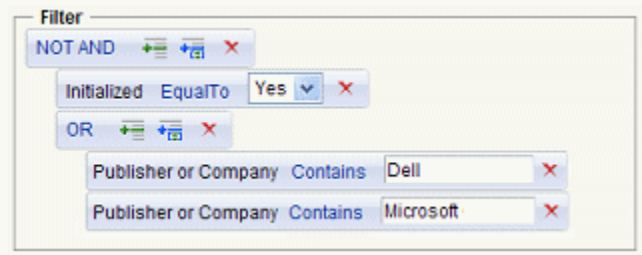
ポートレットをより細かく調整するには、初期化済みのファイル以外に、発行者が「Microsoft Corporation」と識別されるすべてのファイルを除外することができます。これは、初期化後に複数のMicrosoftアプリケーションがすべてのコンピューターにインストールされていて、ポートレットでこれらのファイルを追跡する必要がないと判断できるためです。これを行うために、グループ演算子を OR に変更し、新しい式を作成して右下の図のようなフィルターを作成できます。

目的のために必要なグループ演算子が同じである限り、1 つのグループに式を追加し続けることができます。

式のグループのネスト

フィルター内に式のグループをネストすることができます。フィルター グループ内のそれぞれの式は、最上位の演算子（AND、OR、NOT AND、NOT OR）が同じであり、グループの結果は、その上位のグループからは 1 つの式のように扱われます。グループおよびグループの式にインデントを設定することによってグループ レベルを決めることができます。左側にあるグループは、右側にあるグループよりも上位のグループになります。

次のフィルターは、ポートレットにデータが表示されているファイルが、初期化済みであることと、Dell または Microsoft のいずれのファイルであることの両方は満たさないことを指定しています。OR グループは Initialized の式と同じレベルにあり、NOT AND グループにはフィルター内のすべてが含まれています。



注意

式またはグループの各構成要素を選択するとき、フィルターでは前処理が実行されるため、フィルターを作成する操作の後に数秒の待ち時間が発生する場合があります。

第 22 章

ファイルの検索

この章では、[Find Files（ファイルの検索）] ページを使用して、Bit9 エージェントが稼動しているコンピューター上の実行可能ファイルを検索したり、そのファイルの存在を確認したりする方法を説明します。[Find Files（ファイルの検索）] では、ファイルの「インスタンス」が検索されます。ファイル カタログのファイル リストは検索されません。

セクション

［Find Files（ファイルの検索）］の概要

Bit9 Server では、Bit9 エージェントが稼動しているコンピューターのうち、現在サーバーに接続しているすべてのコンピューター上のすべての追跡対象ファイルが、ほぼリアルタイムで追跡されます。この「ライブ インベントリ」により、Bit9 Server 用のデータベースにある名前やハッシュなどの条件に一致するファイルまたはファイル グループを迅速に検索することが可能です。コンピューターがオフラインの場合、ファイル インベントリには、コンピューターが前回接続したときに検出されたすべてのファイルが含まれています。

この章では、［Find Files（ファイルの検索）］ページについて説明します。［Find Files（ファイルの検索）］ページは、デフォルトで開くページであり、ファイルを名前で検索するフィルターが含まれています。［Files on Computers（コンピューター上のファイル）］タブと同様、フィルターを追加して、検索結果を絞り込むことができ、多くの検索から保存済みビューを作成できます。また、コンソール ページによっては、［Find Files（ファイルの検索）］ボタンまたはリンクを使用して、テーブル行または詳細ページ内の特定のファイルを対象に検索を実行し、その結果を表示できるものもあります。

注意

- ［Files（ファイル）］ページの［Files on Computers（コンピューター上のファイル）］タブでは、ファイル インスタンスを検索することもできますが、その場合は、ファイル名フィルターを含むすべてのフィルターを手動で追加する必要があります。
- ファイル　インベントリから特定のファイルを除外する機能もあり、除外されたファイルは検索結果に表示されない場合があります。詳細については、第 7 章「ファイル情報と公開者情報」の「概要」セクションを参照してください。

他のページからのファイルの検索

［Find Files（ファイルの検索）］ページに直接移動するほかに、他のページのテーブルで、ファイル名またはハッシュの隣にある［Find File（ファイルの検索）］ボタン  をクリックして、ファイル インスタンスを検索することも可能です。この方法では、そのファイルのすべてのインスタンスに対して、ハッシュによる検索が開始されます。この操作は、次のページから実行できます。

- ［Files（ファイル）］ページ（［Files Catalog（ファイル カタログ）］タブと［Files on Computers（コンピューター上のファイル）］タブの両方）
- ［File Group Details（ファイル グループの詳細）］ページ
- ［Baseline Drift Report Results（ベースライン ドリフト レポートの結果）］ページ（ファイル ビュー）
- ［Snapshot Content（スナップショット コンテンツ）］ページ
- ［Find Files（ファイルの検索）］ページ（結果を特定の 1 つのファイルのインスタンスのみに絞り込みます）

- ［Software Rules/Publishers（ソフトウェア ルール / 公開者）］ページ（特定の公開者からのすべてのファイルを検索します）
- ［Approval Request Details（承認要求の詳細）］ページ（承認が要求されたファイルのすべてのインスタンスを検索します）

コンソール ページによっては、リンクをクリックすることにより、事前に構成されたファイル検索を開始して、現在のページに関係のあるファイルを検索できるものもあります。例を次に示します。

- ［Files（ファイル）］ページのファイル名リンク – ［Files（ファイル）］ページでハイライトされたファイル名をクリックすると、指定したファイルに関連するすべてのファイル（指定したファイルによってインストールされたファイル、または指定したファイルのコピーであるファイル）に関する［Find Files（ファイルの検索）］レポートがコンソールに表示されます。
- ［File Details（ファイルの詳細）］ページおよび［File Instance Details（ファイル インスタンスの詳細）］ページ – ［Related Views（関連ビュー）］メニューの［All File Instances（すべてのファイル インスタンス）］リンクをクリックすると、詳細が表示されているファイルの検索が開始されます。
- ［Add/Edit Policy（ポリシーの追加 / 編集）］ページ – このページの［Related Views（関連ビュー）］メニューでは、［All Files on computers in this policy（このポリシー内のコンピューター上のすべてのファイル）］および［Unapproved files on computers in this policy（このポリシー内のコンピューター上の未承認ファイル）］という 2 つのファイル検索方法を選択できます。
- ［Computer Details（コンピューターの詳細）］ページ – ［Related Views（関連ビュー）］メニューに［Files on this Computer（このコンピューター上のファイル）］が含まれています。この項目を選択すると、コンピューター上のすべてのファイルについての［Find Files（ファイルの検索）］レポートが表示されます。

これらのいずれかのクエリに対して［Find Files（ファイルの検索）］の結果が表示されたら、他のコンソール テーブルと同様、列を表示または非表示にしたり、追加のフィルターを適用したりして、結果をさらに絞り込むことができます。［Filters（フィルター）］パネルが表示されていない場合は、［Show/Hide Filters（フィルターの表示 / 非表示）］リンクをクリックします。

［Home Page（ホーム ページ）］ダッシュボードには、ファイル検索用の別のツール、たとえば、［Find Files（ファイルの検索）］ポートレットや［Events（イベント）］ポートレットなどが表示されます。

[Find Files（ファイルの検索）] ページでの検索の定義

[Find Files（ファイルの検索）] ページでは、[Filters（フィルター）] メニューで使用可能なパラメーターを基にファイル クエリを作成できます。他のすべてのページと同様、同じ検索でフィルターを組み合わせることができます(場合によっては、同じタイプのフィルター、たとえば、「ファイル名が calc.exe」や「ファイル名が add.exe」を複数組み合わせることもできます)。

特定の 1 つのファイルを検索する場合は、ファイル名またはハッシュ識別子で検索できます。

ヒント

別のファイル名を装いつつも、その内部データは変わらない、悪意のあるプログラムによる攻撃を検出するには、ファイル名とハッシュに基づく組み合わせ検索が役立ちます。このような攻撃は、比較によって判別できます。

名前によるファイルの検索

ハッシュによる検索は、ファイルのすべてのインスタンスを確実に検索する方法として優れていますが、名前による検索は、最も簡単にゼロから検索を作成できます。ファイル名による検索では、さまざまな演算子を使用して、検索で得られる一致項目を増やしたり、絞り込んだりできます。表 96 を参照してください。

表 96：ファイル名フィルターの演算子

フィールド	説明
contains（含む）	ボックス内のテキストが名前に含まれるすべてのファイル。
does not contain（含まない）	ボックス内のテキストが名前に含まれないすべてのファイル。
begins with（で始まる）	ボックス内のテキストで名前が始まるすべてのファイル。
ends with（で終わる）	ボックス内のテキストで名前が終わるすべてのファイル。
is（等しい）	入力したテキストに完全に一致するファイルのみ。[is（等しい）] を選択したときは、拡張子を含むファイル名全体が [File Name（ファイル名）] テキスト ボックスに入力されていることを確認してください。
is not（等しくない）	入力したテキストに名前が完全に一致しないすべてのファイル。たとえば、ファイル名として「calc」と入力した場合、[**is not**（等しくない）] の結果には、「calc.exe」や「mycalc」などが含まれることに注意してください。
is empty（空）	名前が欠落している、または空白のすべてのファイル。
is not empty（空でない）	名前が欠落しておらず、空白でもないすべてのファイル。

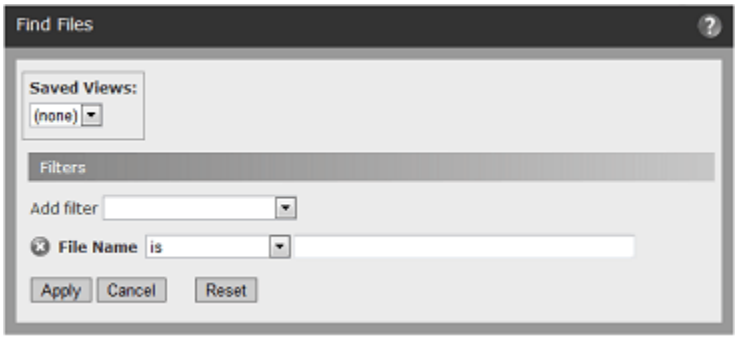
デフォルトでは、[Find Files（ファイルの検索）] ページが開くと、ファイル名フィルターに演算子［is（等しい）］が設定されています。つまり、ボックスに入力したテキストに完全に一致するファイル インスタンスが結果に表示されます。

ファイルを検索するときは、次のベスト プラクティスを考慮してください。

- **ワイルドカードを使用しない** – ファイル名の検索文字列にワイルドカード（* や？など）を使用しないでください。Bit9 Server では、検索文字列が文字通りに照合されるため、期待どおりの結果が得られない場合があります。代わりに、演算子メニューを使用して同じ処理を実行してください。特殊記号を入力する必要はありません。
- **大文字と小文字の区別、およびプラットフォーム** – 大文字と小文字の区別はオペレーティング システムによって異なりますが、Bit9 Platform でのファイル検索では、大文字と小文字は区別されません。たとえば、「Myfile.exe」、「myFiLE.exe」、または「myfile.exe」を検索すると、同じ結果が返されます。
- **結果の制限** – 検索結果が適切な数のファイルに制限されるように検索パラメーターを定義してください。コンソール上で返される一致ファイルの数は制限されています。結果の数が 1 つのテーブルに確実に挿入できる数を超えた場合は、検索を絞り込むように指示するメッセージが表示されます。
- **オートコンプリート** – [File Name（ファイル名）] フィールドなど、[Find Files（ファイルの検索）] ページの多くのフィールドでは、文字列を入力していくと、一致する文字列が自動的に選択項目としてメニューに表示されます。

ファイルのインスタンスを名前で検索する手順：

1. コンソール メニューで、[**Tools**（ツール）] > [**Find Files**（ファイルの検索）] の順に選択します。[File Name（ファイル名）] フィルターと［is（等しい）］演算子がデフォルトで選択された状態で［Find Files（ファイルの検索）］ページが表示されます。



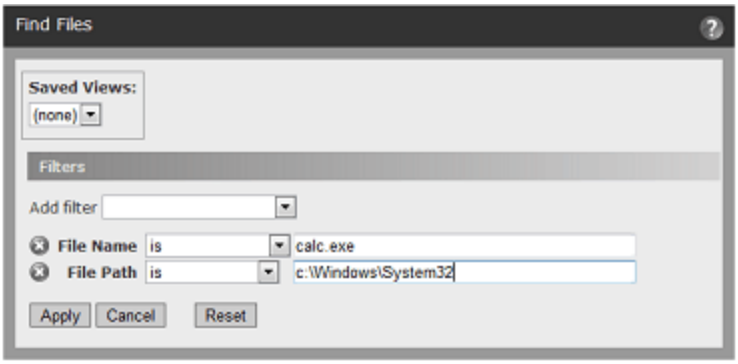
2. 検索で使用するファイル名、またはファイル名の一部を指定します。ファイル名を入力していくと、それまでに入力した文字列に一致するファイルのリストがコンソールに表示されます。
3. ファイルの照合に使用する演算子を選択します（表 96 を参照してください）。たとえば、入力した文字列をファイル名の一部として含むファイルをすべて表示する場合は、演算子として［contains（含む）］を選択します。入力したファイル名に完全に一致するファイルのみを検索する場合は、［is（等しい）］を選択します。

4. ［**Apply**（適用）］をクリックします。入力したファイル名と演算子の組み合わせに一致する（すべてのコンピューター上の）すべてのファイルが［Find Files（ファイルの検索）］テーブルに表示されます。
5. 必要な場合は、別のフィルターを追加して検索を実行できます。別のフィルターを追加して［Filters（フィルター）］パネルの［**Apply**（適用）］をクリックすると、そのたびに、新しい結果が表示されます。

ファイル検索時のパス名の追加

名前でファイルを検索するときは、ファイル パスを追加できます。ファイル パスは、他の検索でも役立ちます。たとえば、特定のディレクトリとそのサブディレクトリにある、特定の公開者からのすべてのファイルを検索する場合などに役立ちます。

パス名を指定するときは、検索するファイルの名前は指定しません。たとえば、「c:\windows\system32」にある「calc.exe」を検索する場合は、次のフィルターを指定します。

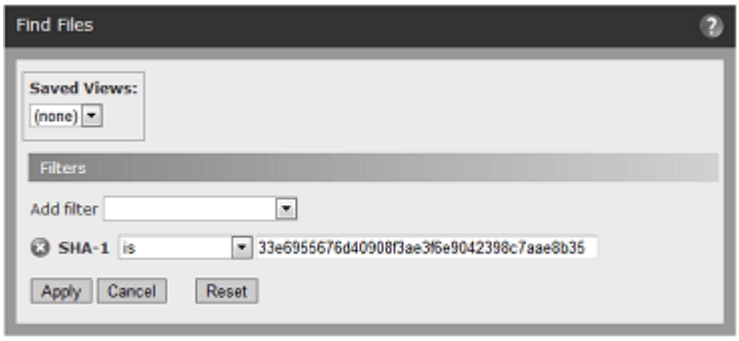


［File Path（ファイル パス）］に「c:\windows\system32」を指定した場合は、このフォルダー内のファイルのみが検索されます。サブフォルダー内のファイルは検索されません。指定したフォルダーとそのサブフォルダー内にあるすべてのファイルを検索する場合は、演算子として［**contains**（含む）］を使用します。たとえば、［File Name（ファイル名）］に「calc.exe」、［File Path（ファイル パス）］に「**contains** c:\windows\system32」を指定した場合は、「system32」とその下のすべてのレベルにある「calc.exe」のインスタンスがすべて検索されます。

プラットフォームに関する注意：ファイル検索でパス名を指定すると検索対象が制限され、使用するプラットフォーム固有の区切り文字（「\」または「/」）とその他の特殊なパス文字に一致するコンピューターのみが検索されます。

ハッシュによるファイルの検索

Bit9 では、SHA-256、SHA-1、および MD5 という 3 つのハッシュ タイプがサポートされます。Bit9 以外のソースからのハッシュがあり、そのハッシュを検索する場合は、［Filters（フィルター）］メニューからハッシュ タイプを選択し、フィルター フィールドにハッシュを入力します。これにより、［Find Files（ファイルの検索）］ページから、環境内のコンピューター上でそのファイルを検索できます。



ファイルによっては、同一のファイルに対して同一になる SHA-256 ハッシュを作成するために Bit9 で特殊な処理が施されます。このため、外部で作成された SHA-256 ファイルは、使用しないことをお勧めします。

ハッシュで検索する場合、最も良い方法は、いずれかの［Files（ファイル）］タブで対象のファイルを見つけてから、そのファイルの隣にある［Find File（ファイルの検索）］ボタンをクリックする方法です。そうすることで、ハッシュ文字列の入力やコピーを行わなくてもファイル検索を行えます。

ファイル名の場合と同様、ハッシュの数字を入力していくと、一致するハッシュのリストがコンソールに表示されます。リストの項目が 1 つのみの場合は、ハッシュ文字列全体を入力しなくても、その項目を選択できます。

［Find Files（ファイルの検索）］の結果の使用

［Find Files（ファイルの検索）］の結果ページには、［Files（ファイル）］ページで使用可能なすべてのツールがあり、詳細情報を取得したり、テーブルの 1 つ以上のファイルに対してアクションを実行したりできます。

- 最初の検索範囲が広いために、（異なるインスタンスだけではなく）異なるファイルが結果に含まれている場合、特定の 1 つのファイルの隣にある［Find File（ファイルの検索）］ボタン をクリックすると、そのファイルのすべてのインスタンスに対する検索を新たに開始できます。
- 検索されたファイル インスタンスの隣にある［View Details（詳細の表示）］ボタン をクリックすると、そのインスタンスに関する詳細情報を確認できます。
- 結果からファイルを選択し、［Action（アクション）］メニューの承認コマンドまたは禁止コマンドを使用して、ファイルを承認または禁止することができます。たとえば、結果内のいずれかのファイルを「**ローカルで承認**」したり、「**ローカル承認を削除**」するには、ファイル名の左側にあるボックスをオンにして、該当するボタンをクリックします。
- Bit9 Software Reputation Service (SRS) を有効にした場合は、結果内のすべてのファイルの追加情報を表示できます（追加情報がある場合）。追加情報を表示するには、ファイル名の左側にあるボックスをオンにして、［Action（アクション）］メニューから［**View Bit9 SRS Cloud Data**（Bit9 SRS Cloud データの表示）］を選択します。

- Bit9 Connector によるサードパーティ分析ツールの統合を有効にした場合は、［Action（アクション）］メニューに［**Analyze with…**（… で分析）］コマンドが表示されます。用意されているコマンドを使用して、検索した 1 つ以上のファイルを分析のために送信できます。
- ［Action（アクション）］メニューには、［Find Files（ファイルの検索）］の結果にある 1 つ以上のファイルが存在するコンピューター、またはそれらのファイルが存在しないコンピューターを検索するコマンドも含まれています。

注意

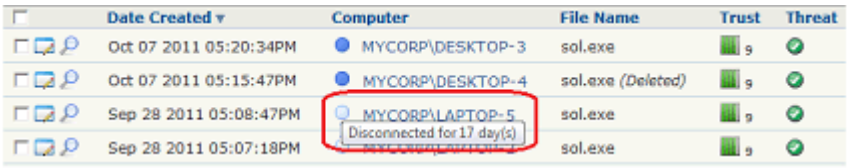
- 各ファイルに対して［View Bit9 SRS Cloud Data（Bit9 SRS Cloud データの表示）］コマンドを使用すると、結果が新しいタブに表示されます。Internet Explorer で複数のファイルを要求したときは、最初の結果が表示された後、ポップアップ ブロッカーにより、各ファイルの結果がブロックされる場合があります。
- 他のコンソール テーブルと同様、［Find Files（ファイルの検索）］の結果のテーブルの見出しにあるボタンを使用すると、表示列を並べ替えたり、結果をコンマ区切り値形式でダウンロードしたり、［Find File（ファイルの検索）］の結果をスナップショットに追加したりできます。詳細については、第 2 章「Bit9 コンソールの使用」の「Bit9 コンソールのテーブル」を参照してください。

結果に関する特別なケース

オフライン コンピューター上のファイル

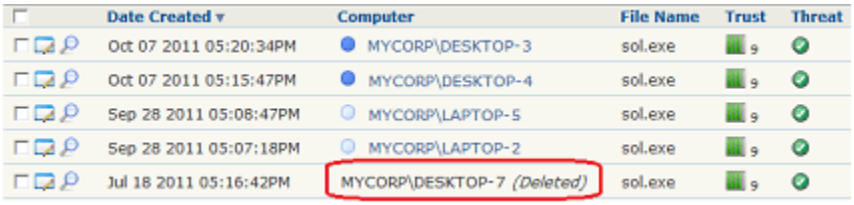
コンピューターがオフラインの場合、［Find Files（ファイルの検索）］の検索結果には、そのコンピューターが最後に Bit9 Server と同期されたときに検出されたファイルの中で、指定した条件に一致するファイルが表示されます。次回、そのコンピューターが Bit9 Server に接続すると、条件に一致したファイルの情報が短時間で更新され、更新された情報が［Find File（ファイルの検索）］で使用可能になります（更新時間は、ネットワーク トラフィックや更新するコンピューター数の影響を受けます）。

［Computer（コンピューター）］列を含む［Find File（ファイルの検索）］の結果テーブルでは、コンピューター名の左側にインジケーターがあり、現在そのコンピューターがサーバーに接続されていて最新の状態になっているかどうかがわかります。濃い青色の円が表示されている場合、そのコンピューターは現在接続されており、最新の状態になっています。オレンジ色の円が表示されている場合、そのコンピューターはアップグレードを待機しています。明るい青色の円が表示されている場合、そのコンピューターは切断されています。ステータスを示す円の上にマウス カーソルを移動すると、そのコンピューターのステータスに関する詳細情報（コンピューターがオフラインになってからの日数など）がコンピューター名の下に表示されます。



削除されたコンピューター上のファイル

[Computers（コンピューター)］リストからコンピューターを削除しても、そのコンピューター上のファイルは[Files on Computers（コンピューター上のファイル)］データベースに 1 日間残ります。つまり、[Find Files（ファイルの検索)］で検索を実行したときに、削除されたコンピューターからの結果が含まれる場合があります。削除されたコンピューターには、[Find Files（ファイルの検索)］の結果と同様のラベルが表示されます。



削除されたファイル

[Find Files（ファイルの検索）］での検索に一致するファイルが最近コンピューターから削除された場合でも、必要があれば、そのファイルを［Find File（ファイルの検索)］の結果に含めることができます。ただし、この動作は、デフォルトでは実行されません。削除されたファイルを含めるには、[Find Files（ファイルの検索)］ページの右下にある［Show deleted files（削除されたファイルの表示)］ボックスをオンにします。これにより、テーブルが直ちに更新され、削除されたファイルのうち、検索パラメーターに一致するものが表示されます。削除されたファイルには、[Find Files（ファイルの検索)］の結果と同様のラベルが表示されます。

削除されたファイルは、古いイベントと同じスケジュールでデータベースから除去されます。この期間の構成については、「高度な構成オプション」（766 ページ）を参照してください。

注意

- フィルターを使用して、削除されたファイルを検索する場合は、一致する結果が表示される前に、ページ右下隅にある［Show deleted files（削除したファイルの表示）］ボックスをオンにする必要があります。
- 削除されたファイルを検索に含めると、検索速度が低下し、リソースの使用量が増加します。したがって、この機能を使用するのは、必要なときのみにしてください。

初期化中または同期中のコンピューター上のファイル

Bit9 エージェントをインストールしたコンピューターがまだ初期化中の場合、［Find Files（ファイルの検索）］では、そのコンピューター上のファイルの一部を検索できますが、ファイル インベントリ全体は初期化が完了するまで検索できません。コンピューターがまだ初期化中であるかどうかを確認するには、［Computers（コンピューター）］ページに移動して、そのコンピューターを探します。

同様に、エージェントとサーバーの再同期が行われている場合は、同期が終了するファイル情報の変更が完了しません。同期の進行状況は、［Computer Details（コンピューターの詳細）］ページで確認でき、テーブルに［Synchronization（同期）］列を追加した場合は［Computers（コンピューター）］ページでも確認できます。

ファイル検索用の保存済みビュー

頻繁に使用すると思われる複雑な検索条件がある場合は、その検索条件を［Saved View（保存済みビュー）］として保存できます。

注意

- ［Find Files（ファイルの検索）］ページから検索を再実行するとコンテキストが変わる可能性があるために保存できないビューもあります（たとえば、他のページの［Find File（ファイルの検索）］ボタンから開始された検索など）。その場合、［Saved Views（保存済みビュー）］パネルは表示されません。代わりに、［Files（ファイル）］ページの［Files on Computers（コンピューター上のファイル）］タブでフィルターを使用すれば、必要な検索を複製して保存できる場合があります。
- 読み取り専用権限のみを持つユーザーはビューを保存できません。また、カスタム ログイン アカウント グループによっては、ビューを保存する権限がないものもあります。

［Find Files（ファイルの検索）］ページで保存済みビューを作成する手順：

1. コンソール メニューで、［**Tools**（ツール）］>［**Find Files**（ファイルの検索）］の順に選択します。［File Name（ファイル名）］フィルターと［is（等しい）］演算子がデフォルトで選択された状態で［Find Files（ファイルの検索）］ページが表示されます。
2. 検索条件に追加する各フィルターを選択した後、フィルターの構成に必要なテキストを指定して、［**Apply**（適用）］をクリックします。
3. フィルターの追加が終了したら、テーブルの上にある［Saved Views（保存済みビュー）］ボックスに名前を入力して、［**Add**（追加）］をクリックします。以後、必要なときはいつでも、作成した保存済みビューを［Saved View（保存済みビュー）］メニューから選択して、同じ検索に対する結果を取得できます。

第 23 章

システム構成

この章では、Bit9 Server 環境を構成および保守するための設定について説明します。［System Configuration（システム構成）］ページにアクセスできるのは、Administrators グループ、または［View System Configuration（システム構成の表示）］ボックスと［Manage System Configuration（システム構成の管理）］ボックスがオンになっているカスタマイズ済みのグループに属すログイン アカウントのみです。

セクション

概要

［System Configuration（システム構成）］ページには、読み取り専用のステータス情報と構成設定の両方が表示されます。これらの情報と設定は、Bit9 Security Platform 管理者によって使用されます。構成情報は一連のタブ付きビューで編成されています。これらのビューの中には、複数のパネルを持つものもあります。

- ［**General**（全般）］タブ – サーバー ステータス情報、Bit9 を Active Directory または LDAP に統合するためのオプション、および［Bit9 Agent Management（Bit9 エージェント管理）］のオプション。
- ［**Events**（イベント）］タブ – Bit9 専用のデータベースを管理するための構成設定、および補足用の外部イベント ロギング（Syslog など）をセットアップするためのオプション。
- ［**Security**（セキュリティ）］タブ – Bit9 エージェントと Bit9 Server 間のセキュア通信の現在のステータスが表示されます。また、これらの通信で証明書の検証を有効にするオプションを選択できます（検証がまだ有効になっていない場合）。
- ［**Advanced Options**（高度なオプション）］タブ – データベースのバックアップ、エージェントの自動アップグレード、Bit9 コンソールのログイン タイムアウト、Bit9 で無視するファイル、Bit9 API へのアクセス、オフライン コンピューターの削除、公開者の期限切れ証明書の使用許可、Bit9 Software Reputation Service (SRS) による検出の痕跡セット、システムの正常性の痕跡、およびアップデーター定義の更新などのオプション。
- ［**Mail**（メール）］タブ – Bit9 アラートのトリガー時、または承認要求の解決時に E メールを送信するための構成設定。
- ［**Licensing**（ライセンス）］タブ – サーバーに接続するためのライセンスが付与された Bit9 エージェントの数とタイプが表示され、ライセンス キーの更新を行えます。また、Bit9 Software Reputation Service を有効にしたり、構成したりすることもできます。
- ［**Connectors**（コネクター）］タブ – 1 つ以上のネットワーク セキュリティ デバイスまたはサービスに Bit9 Server を統合するための構成設定。このタブの設定項目については、付録 C「Bit9 Connector for Network Security Devices」を参照してください。
- ［**External Analytics**（外部分析）］タブ – エンドポイントで収集されたデータを Bit9 Server から外部の分析ツールにエクスポートするための、Bit9 External Analytics の構成設定。このタブの設定項目については、付録 F「外部分析のための Bit9 データのエクスポート」を参照してください。

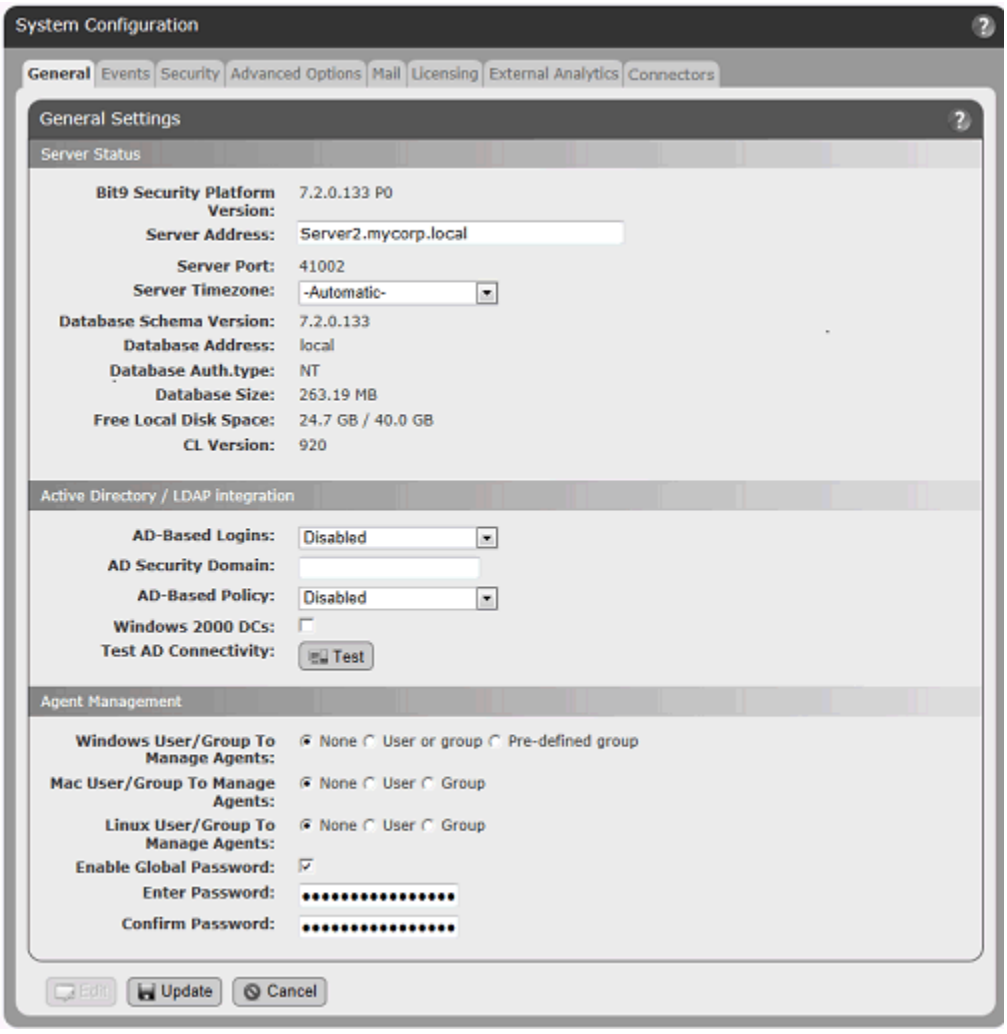
［System Configuration（システム構成）］ページを表示する手順：

1. コンソール メニューで、［**Administration**（管理）］>［**System Configuration**（システム構成）］の順に選択します。［System Configuration（システム構成）］ページが表示されます。
2. Bit9 コンソールには、デフォルトで［System Configuration（システム構成）］ページの［General（全般）］タブが表示されます。このタブにない情報を表示または変更する場合は、別のタブを選択します。

［General Configuration（全般構成）］タブ

［System Configuration（システム構成）］ページの［General（全般）］タブでは、構成フィールドが次の 3 つのパネルに配置されています。

- ［Server Status（サーバー ステータス）］パネル – Bit9 Server とデータベース サーバーに関する情報（サーバーのアドレスなど）が表示されます。
- ［Active Directory/LDAP Integration（Active Directory/LDAP 統合）］パネル – AD または LDAP と Bit9 Server との統合を構成できます。
- ［Agent Management（エージェント管理）］パネル – ユーザー、グループ、またはパスワードを指定して、特別なエージェント管理コマンドへのアクセス権を設定できます。



サーバー ステータスおよびオプションの表示

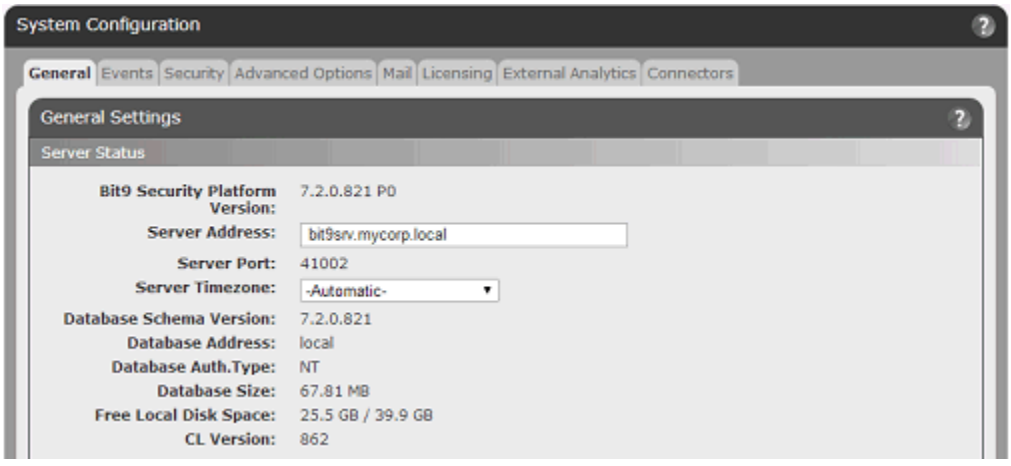
［System Configuration（システム構成）］ページの［General（全般）］タブの最上部には、［Server Status（サーバー ステータス）］というパネルがあります。このパネルには、Bit9 Server のパラメーターが表示され、一部のパラメーターは編集することできます（詳細については、表 97 を参照してください）。

重要

［Server Status（サーバー ステータス）］パネルのパラメーターを見ると、Bit9 データベースのサイズや Bit9 Server を実行しているコンピューターの空き容量がわかります。ただし、外部 SQL データベースの容量が不足しているかどうかはわかりません。選択したデータベース オプションにかかわらず、Bit9 データベースを定期的に監視し、Bit9 データベースが空き容量をオーバーして Bit9 Server の動作が妨げられないように注意してください。データベース構成の詳細については、『Installing Bit9 Server（Bit9 Server のインストール）』ドキュメントを参照してください。また、データベース関連のアラートについては、「アラートの作成」（611 ページ）を参照してください。

サーバー ステータス情報を表示する手順：

1. コンソール メニューで、［**Administration**（管理）］>［**System Configuration**（システム構成）］の順に選択します。
2. 他のタブが表示されている場合は、［**General**（全般）］タブをクリックします。［General（全般）］構成オプションが表示され、このタブの上部に［Server Status（サーバー ステータス）］パネルがあります。



3. タイムゾーンを変更するには、［**Edit**（編集）］ボタンをクリックして、設定を変更します。次に、［**Update**（更新）］ボタンをクリックし、確認ダイアログで［**Yes**（はい）］をクリックします。他の設定の詳細については、表 97 を参照してください。

表 97：サーバー ステータス情報と構成オプション

フィールド	説明
Bit9 Version（Bit9 のバージョン）	インストールされている Bit9 Server ソフトウェアのバージョン番号。（読み取り専用）
Server Address（サーバー アドレス）	Bit9 Server の IP アドレスまたは完全修飾 DNS 名。 サーバー アドレスを変更した場合は、Bit9 エージェントをすべてのコンピューターに再インストールする必要があります（ただし、IP アドレスを対応する DNS 名に変更した場合、またはその逆の場合は不要です）。エージェントをインストールすると、コンピューターが直ちに再初期化され、サーバーで明示的に禁止されたファイルを除くすべてのファイルがローカルで承認され、実行が許可されます。同じポリシーを使用できるようにするため、Bit9 Security Platform では、既存のエージェント インストール パッケージが新しい IP アドレスで自動的に更新され、コンピューターがオンラインに戻ったときに正しいサーバーに対してレポートを送信するように構成されます。 **注意**：Bit9 Server との通信には IPv6 を使用できますが、Firefox ブラウザーを使用する場合、バージョンによっては、数値形式の IPv6 アドレスが受け入れられないことがあります。この問題を避けるには、サポートされている他のブラウザーを使用するか、完全修飾 DNS 名を使用してください。
サーバー ポート（Server Port）	Bit9 エージェントが稼動しているコンピューターと通信するための専用の Bit9 Server ポート。この設定をサーバーのインストール後に変更することはできません。（読み取り専用）
Server Timezone（サーバーのタイムゾーン）	Bit9 Server で使用されるタイムゾーン。通常、このフィールドは［Automatic（自動）］に設定され、Bit9 Server のオペレーティング システムと同じタイムゾーンが使用されます。ただし、特定地域の夏時間を標準以外の方法で処理する必要がある場合は、ここにあるドロップダウン メニューを使用してサーバー タイムゾーンを明示的に設定できます。
Database Schema Version（データベース スキーマのバージョン）	通常、データベース スキーマのバージョンは、Bit9 Server のバージョンと同じです。ただし、サーバーをアップグレードまたは再インストールする場合は、既存のデータベースを使用できます。この場合、データベース スキーマのバージョンは異なることがあります。この情報は、Bit9 サポートを利用する際に必要になることがあります。（読み取り専用）

フィールド	説明
Database Address（データベース アドレス）	データベースが**ローカル**にあるのか、別のサーバーにあるのかが示されます。後者の場合は、そのアドレスが表示されます。（読み取り専用）
Database Auth. Type（データベース認証のタイプ）	Bit9 Server のインストール時に選択したデータベース認証のタイプが示されます。[**NT** (NT)] の場合は、Windows NT のアカウントまたはグループに基づいてデータベース アクセスが制御されます。[**SQL** (SQL)] の場合は、SQL Server 固有のログインおよびパスワードが使用されます。（読み取り専用）
Database Size（データベース サイズ）	Bit9 データベースによって現在使用されているディスク容量。（読み取り専用）
Free Local Disk Space（ローカル ディスクの空き容量）	Bit9 Server 上のローカル ディスクの空き容量。Bit9 データベースが Bit9 Server と同じシステムにある場合は、この値を定期的に監視することにより、イベントがどのくらいの早さで蓄積されるかを確認して、イベント ログを削除する間隔の調整が必要かどうかを判断できます。（読み取り専用） **重要**：このフィールドでは、Bit9 Server システムの空き容量のみが報告されます。リモート データベースを使用している場合は、そのシステム上で直接、空き容量を確認してください。
CL Version（CL バージョン）	これは、現在の一連のポリシー ルールが反映された構成リストのバージョン番号です。Bit9 コンソール ユーザーが禁止の作成やポリシーの変更などのアクションを実行して Bit9 Server の構成を変更すると、この数値が増加します。Bit9 サポートを利用する際、トラブルシューティングの状況によっては、この CL バージョン情報が必要になることがあります。（読み取り専用）

Active Directory 統合の構成

Bit9 Server では、Active Directory (AD) 環境を利用して、Bit9 コンソール ユーザーのアクセス権限の設定、コンピューターへのセキュリティ ポリシーの割り当て、およびユーザーとコンピューターのメタデータの提供を行うことができます。また、特定のグループまたはユーザーを指定して、Bit9 で管理されるコンピューターへのソフトウェアのインストール（および、ソフトウェアの自動承認）を行えるようにすることもできます。AD 統合の構成は、[General（全般）] タブで行います。

AD 統合構成オプションを表示する手順：

1. コンソール メニューで、[**Administration**（管理）] > [**System Configuration**（システム構成）] の順に選択します。

2. 他のタブが表示されている場合は、[**General**（全般）] タブをクリックします。[General（全般）] 構成オプションが表示され、中央のパネルに AD/LDAP 統合オプションがあります。

3. AD または LDAP 統合を構成するには、ページ下部にある [**Edit**（編集）] ボタンをクリックし、[Active Directory/LDAP integration（Active Directory/LDAP 統合）] パネルで必要に応じて変更を行います。変更が終了したら、[**Update**（更新）] ボタンをクリックし、確認ダイアログで [**Yes**（はい）] をクリックします。これらの設定の詳細については、表 98 を参照してください。

表 98：Active Directory/LDAP 統合オプション

フィールド	説明
AD-based logins（AD ベースのログイン）	このフィールドで [**Enabled**（有効）] を選択すると、ユーザーは、AD のアカウントとパスワードを使用して、Bit9 コンソールにログインできます。詳細については、第 3 章「コンソール ログイン アカウントの管理」の「AD アカウントを通じたコンソール アクセスの有効化」（89 ページ）を参照してください。
AD security domain（AD セキュリティ ドメイン）	このフィールドで AD セキュリティ ドメインを指定すると、Bit9 Server は、Bit9 コンソール ユーザーのログインを検証する際、そのドメインを参照して、Bit9 セキュリティ グループが存在するかどうかを確認します。セキュリティ ドメインを指定しない場合は、各コンソール ユーザーのログイン ドメインが使用されます。そのため、各コンソール ユーザーがログインするには、Bit9 セキュリティ グループが各ユーザーのドメインに存在する必要があります。
AD-based policy（AD ベースのポリシー）	このフィールドで [**Enabled**（有効）] を選択すると、AD または LDAP に基づいて Bit9 ポリシーを自動的にコンピューターに割り当てることができます。詳細については、第 4 章「コンピューターの管理」を参照してください。
Windows 2000 DCs (Windows 2000 DC)	このボックスをオンにすると、ネットワークで Windows 2000 ドメイン コントローラーが使用されます。その場合、指定した AD セキュリティ ドメインの値は無効になります（値を指定していた場合）。これは、AD セキュリティ ドメインが、Windows 2003 SP2 ドメイン コントローラーでのみ使用可能なクロスドメイン メンバーシップ テストに依存しているためです。
Test AD Connectivity（AD 接続のテスト）	[**Test**（テスト）] ボタンをクリックすると、Bit9 Server と Active Directory 間の接続がテストされます。テストが成功した場合は、Bit9 の Active Directory 統合機能を使用できます。エラーが報告された場合、Bit9 Server は Active Directory にアクセスできません。そのため、統合機能を使用する前に、その問題を解決する必要があります。

エージェント管理権限の構成

Bit9 テクニカル サポート担当者からの支援を受けながら、Bit9 エージェントを管理するための特別なエージェント管理コマンドを使用できます。各エージェントには、コマンドを有効にする固有の「CLI」パスワードがあります。このパスワードは、［Computer Details（コンピューターの詳細）］ページの［Bit9 Agent（Bit9 エージェント）］タブで調べることができます。ただし、グローバルなアクセス方法を作成すれば、エージェントごとにパスワードを調べなくても済むようになります。

Bit9 エージェントは、コンピューターの管理や保護において重要な役割を果たします。そのため、これらのコマンドへのアクセスは制限する必要があります。［General（全般）］タブの［Agent Management（エージェント管理）］セクションでは、次のいずれかまたは両方の方法を選択して、エージェント コマンドへのアクセスを制御できます。

- クライアント プラットフォームごとに、コマンドを実行できるユーザーまたはグループを指定する
- コマンドの実行に必要なパスワードを指定する

ユーザー / グループとパスワード両方を定義する場合は、いずれかのアクセス方法だけで十分です。エージェントにはエージェント インストール パッケージを作成した時点で最新のエージェント管理構成が組み込まれています。パスワードを変更した場合、Bit9 Server では、新しいパスワードを使用してオンライン中のエージェントが更新されますが、オンラインでないエージェントは、古いパスワードを引き続き使用する必要があります。同様に、オフラインのエージェントでは、古いエージェントをアンインストールして、新しいエージェントを特定の方法でインストールしない限り、ユーザーまたはグループのアクセス定義の変更は有効になりません。

注意

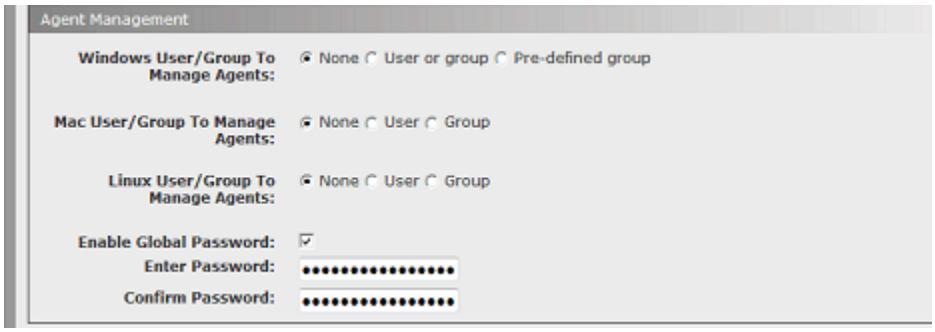
グローバルなエージェント パスワードまたはアクセスを許可するユーザー / グループを設定するときは、［Agent Management（エージェント管理）］のオプションを構成してから、エージェント インストール パッケージを生成するのが最も効率的な方法です。

Bit9 Server を新規インストールする場合は、インストール中にエージェント管理コマンドへのアクセス方法を指定するように求められます。このタイミングでオプションを選択するのが最適です。

［Agent Management（エージェント管理）］の構成オプションを表示する手順：

1. コンソール メニューで、［**Administration**（管理）］>［**System Configuration**（システム構成）］の順に選択します。

2. 他のタブが表示されている場合は、[**General**（全般）] タブをクリックします。[General（全般）] 構成オプションが表示され、下部のパネルに [Agent Management（エージェント管理）] のオプションがあります。



3. エージェント管理コマンドへのアクセス方法を構成するには、ページ下部にある [**Edit**（編集）] ボタンをクリックし、必要に応じて変更を行います。変更が終了したら、[**Update**（更新）] ボタンをクリックし、確認ダイアログで [**Yes**（はい）] をクリックします。これらの設定の詳細とオプション選択のガイダンスについては、表 99 および「接続の状況と [Agent Management（エージェント管理）] での選択」（752 ページ）を参照してください。

表 99：[Agent Management（エージェント管理）] の構成オプション

フィールド	説明
Windows User/ Group to Manage Agents（エージェントを管理する Windows ユーザー / グループ）	定義されている場合、ここで指定された Windows ユーザーまたはグループは、そのユーザーまたはグループを認識するコンピューター上で、Bit9 エージェント管理用の特別なコマンドを実行できます。 • [User or group（ユーザーまたはグループ）] ラジオ ボタンをクリックし、ユーザーまたはグループの名前を手動で入力します。このボックスには、ユーザーまたはグループの SID を入力することもできます。 • [Predefined group（事前定義グループ）] ボタンをクリックし、メニューから Windows グループ（[Local Administrators（ローカル管理者）] など）を選択します。
Mac User/ Group to Manage Agents（エージェントを管理する Mac ユーザー / グループ）	定義されている場合、ここで指定された Mac ユーザーまたはグループは、そのユーザーまたはグループを認識するコンピューター上で、Bit9 エージェント管理用の特別なコマンドを実行できます。[User（ユーザー）] ラジオ ボタンまたは [Group（グループ）] ボタンをクリックし、ボックスに名前を入力します。

フィールド	説明
Linux User/ Group to Manage Agents（エージェントを管理する Linux ユーザー / グループ）	定義されている場合、ここで指定された Linux ユーザーまたはグループは、そのユーザーまたはグループを認識するコンピューター上で、Bit9 エージェント管理用の特別なコマンドを実行できます。[User（ユーザー）] ラジオ ボタンまたは [Group（グループ）] ボタンをクリックし、ボックスに名前を入力します。
Enable Global Password（グローバル パスワードの有効化）	定義されている場合、どのユーザーでもクライアント コンピューターから、ここで指定されたパスワードを使用して Bit9 エージェント管理用の特別なコマンドを実行できます。チェックボックスをオンにして、パスワードを入力します。 パスワードと、エージェント管理用のユーザーまたはグループの両方を定義した場合は、いずれか一方のみを指定することで管理コマンドへのアクセスが可能になります。

接続の状況と［Agent Management（エージェント管理）］での選択

エージェント管理コマンドへのアクセス方法を選択する際には、Bit9 エージェントを実行しているクライアント システムを Bit9 Server に接続するかどうかや、その接続頻度を考慮することを推奨します。

コンピューターをサーバーに全く接続しない場合は、[Agent Management（エージェント管理）] でパスワードを設定してからインストール パッケージを生成することにより、管理コマンドへのアクセスが可能になります。このパスワードはエージェントに組み込まれ、パスワードの変更は、次のいずれかの方法によってのみ行うことができます。

- パスワードの変更後に生成された新しいエージェント　パッケージをインストールする。
- グローバル パスワードの変更後に Bit9 Server から新しい構成リストをインポートする。構成リストのインポート手順については、Bit9 テクニカル サポートの担当者にお問い合わせください。

システムを Bit9 Server に全く接続しない場合は、すべてのマシン上に確実に存在するグループ（Windows コンピューターの場合は Local Administrators など）を指定するという方法もあります。この方法が適切かどうかは、組織内で管理アカウントがどのように管理されているかによって決まりますが、この方法を使用すると、Bit9 Security Platform の変更に関係なく、指定したグループのユーザーを追加または削除することにより、エージェント管理コマンドへのアクセスを制御できます。

コンピューターを Bit9 Server にときどき接続する場合は、クライアント管理コマンドへのアクセス方法をより柔軟に選択したり、変更したりできます。パスワード、ユーザー定義、またはグループ定義を変更すると、エージェントがサーバーに次回接続されたときにその内容が伝達されます。

すべてのコンピューターを Bit9 Server に常に接続する場合（または、必要に応じて接続できる場合）は、エージェント管理コマンドへのアクセス方法を最も柔軟に構成できます。これは、エージェントがサーバーが接続すると、行った変更が

直ちにエージェントに送信されるからです。この場合は、既知のグループを選択するか、新しいグループ（「Bit9 Local Administrators」など）を定義し、そのメンバーに管理コマンドへのアクセス権を付与するほうが便利な場合もあります。また、グループ単位でアクセス権を設定すると、runas、psexec、sudo などのツールを使い、別の認証情報を使用してコマンドを実行することも可能になります。必要に応じて、パスワードを使用することもできます。

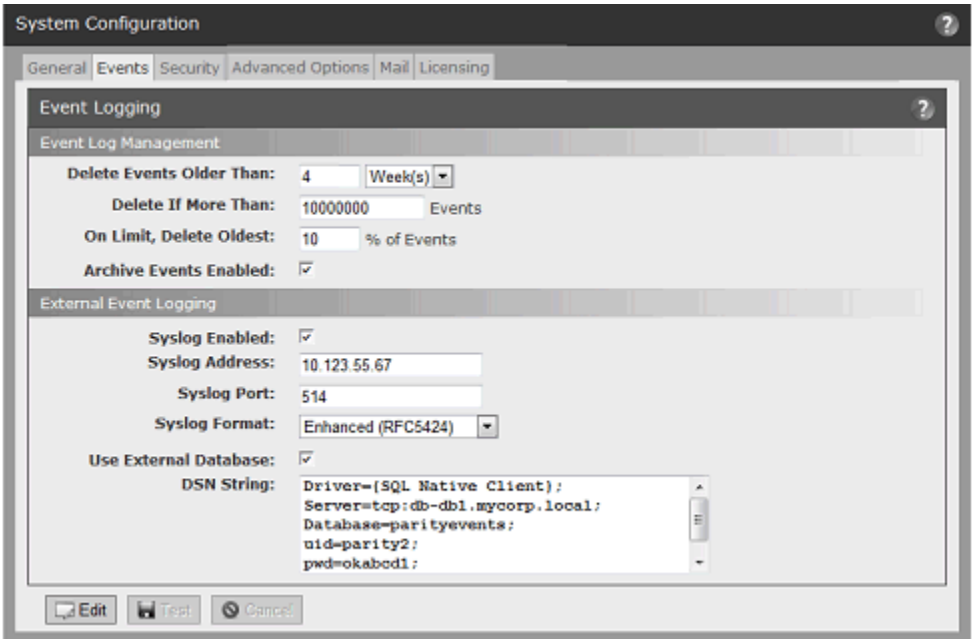
注意

Windows Vista 以降でアプリケーションを実行する場合、事前定義されたセキュリティ グループ（Administrators など）のメンバーシップを指定するには、管理者としてアプリケーションを実行する必要があります。Vista または Windows 7 を実行しているコンピューターを使用する場合、ユーザーにこの権限が与えられているかどうかが不明なときは、［Agent Management（エージェント管理）］で事前定義されたグループを指定するのが適切な選択とならない場合があります。

イベント管理のオプション

Bit9 イベント データは、SQL Server データベースに保存されます。このイベント データは、ネットワーク上のファイル アクティビティの量に応じて時間とともに増大します。［Events（イベント）］タブには、Bit9 Security Platform で生成されたイベント データを管理するための 2 組のオプションがあります。

- ［Event Log Management（イベント ログの管理）］パネルには、プライマリ Bit9 データベースのサイズとイベントのアーカイブを管理するためのオプションがあります。
- ［External Event Logging（外部イベント ロギング）］パネルには、補足用の外部ロギングを有効にするためのオプションがあります。このオプションを有効にすると、Bit9 イベントを別の SQL Server または Syslog 管理サーバーのログに記録できます。補足用の外部ロギングを使用すると、プライマリ データベースに保存されるデータの量を削減できる場合があります。



重要

イベント ログの管理方法を選択する際には、Bit9 データを保存するディスクの容量と外部 SQL Server データベースの空き容量を考慮することを推奨します。ロギング構成を変更する場合は、事前にこれらの点を確認してください。

Bit9 イベント データベースの管理

［Event Log Management（イベント ログ管理）］タブには、Bit9 データベースの増大を制限し、イベント アーカイブを設定するためのオプションが含まれています。

イベント削除のしきい値の設定

データ削除のしきい値を設定すると、Bit9 データベースを常に適切なサイズに維持することができます。Bit9 Server は、このデータ量を処理するためのメカニズムをいくつか備えています。Bit9 では、次の 2 種類のパラメーターに基づいて、イベント データを自動的に削除できます。

- ［**Delete Events Older Than**（次より古いデータを削除）］– Bit9 はデフォルトで 4 週間前より古いイベントを自動的に削除します。それらのイベント データはシステム上で削除され、Bit9 Server によって生成されるレポートに表示されなくなります。この期間は、［Management Configuration（管理構成）］テーブルで変更できます。
- ［**Delete if More Than**（次を超える場合に削除）］– このしきい値はデフォルトで 100 万（SQL Server Express の場合）および 1000 万（SQL Server の他のエディションの場合）に設定されます。これは、2 番目のパラメーターである［**On Limit Delete Oldest**（制限に達したら最も古いデータを削除）］と連携しており、設定済みの制限に達したときに削除するイベントの割合を定義できます。デフォルトの割合は 10% です。

イベント データは、いずれかの条件が満たされると削除されます。これらの自動削除パラメーターは、SQL Server 上のディスク空き容量と、履歴情報をどの程度まで保持する必要があるかに基づいて構成できます。ご使用のネットワークに適した値を判断するには、サーバー上のディスク使用量を監視し、それに応じてイベント データベースの削除パラメーターを調整します。

日次イベント アーカイブの有効化

［System Configuration Events（システム構成イベント）］タブで［Archive Events Enabled（イベントのアーカイブを有効にする）］がオンになっている場合は、Bit9 Server により、毎日のイベント データを記録した CSV ファイルの圧縮ファイルが個々に生成されます。日次イベント ファイルは、1 年分保存され、［Event Log Archives（イベント ログ アーカイブ）］を通じてアクセスできます。［Event Log Archives（イベント ログ アーカイブ）］には、日付の付いたファイルが時系列でリストされています。このログを通じて、リストされているイベント ログ ファイルをクリックし、開くことができます（別の場所に保存することもできます）。［Event Log Archives（イベント ログ アーカイブ）］を開くには、イベント ログのヘッダーにある［Archives（アーカイブ）］ボタン をクリックします。

［Archive Events Enabled（イベントのアーカイブを有効にする）］をオフにすると、その時点からイベント アーカイブが生成されなくなります。

外部サーバーへのデータベースの移動

Bit9 Server をインストールする際の選択項目の一つとして、Bit9 データベースを Bit9 Server と同じコンピューターに配置するかどうかがあります。場合によっては、Bit9 のデータ ボリュームを共有データベース サーバーから専用データベース サーバーに移行することが必要となります。

プライマリ Bit9 データベースを移行するには、Bit9 コンソールの外部での操作が必要になります。たとえば、Bit9 Server のインストール プログラムを実行して、新しいサーバーに再接続する作業が必要です。このような移行が必要な場合は、Bit9 テクニカル サポートにお問い合わせください。

注意

［System Configuration Events（システム構成イベント）］タブの［External Event Logging（外部イベント ロギング）］のオプションは、補足用のイベント ロギングを有効にするためのもので、プライマリ データベースを移行するためのものではありません。

外部イベント ロギングの設定

Bit9 Security Platform では、イベント データを外部にある追加の SQL Server にコピーできます。また、イベントをさまざまな出力形式で Syslog サーバーに出力するように構成することもできます。外部イベント ロギングの設定項目については、表 100（760 ページ）を参照してください。

Syslog サーバーへのイベントのロギング

Bit9 Server では、複数の形式を使用して Bit9 イベント情報を Syslog サーバーに統合する機能がサポートされています。Syslog 統合の構成は、［Events（イベント）］タブの［External Event Logging（外部イベント ロギング）］パネルで行います。

サポートされる形式を次に示します。

- **基本(RFC3164)** – 6.0.1より前のバージョンのBit9 (Parity)からv7.2.3にアップグレードする場合のデフォルトです。
- **拡張 (RFC5424)** – より新しい標準であり、Bit9 (Parity) v6.0.1 以降を新規にインストールする場合のデフォルトです。
- **CEF (ArcSight)** – Bit9 イベント ログを HP ArcSight ESM または HP ArcSight Logger に統合する場合に使用する形式です。
- **LEEF (Q1 Labs)** – Bit9 イベント ログを QRadar Log Manager または QRadar SIEM に統合する場合に使用する形式です。

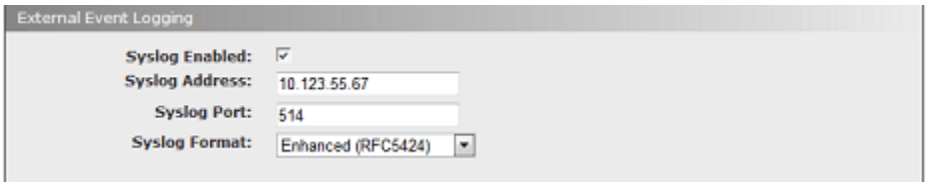
注意

- Bit9 でサポートされる syslog 形式と、Bit イベントをそれらの形式にマッピングする方法の詳細については、別のドキュメント『Bit9 Events Integration Guide（Bit9 イベント統合ガイド）』を参照してください。
- HP ArcSight 製品または Q1Labs 製品を以前のバージョンの Bit9 とともに使用していた場合は、統合ガイドを参照し、統合環境を Bit9 Security Platform v7.2.3 にアップグレードする手順を確認する必要があります。
- 6.0.2 より前のリリースで、Bit9 テクニカル サポートの支援を受けながら特別な Syslog 形式を手動で有効にした場合は、v7.2.3 にアップグレードしたときに変更が上書きされます。［Syslog format（Syslog 形式）］メニューを使用して、形式を選択してください。

Syslog サーバーへのイベント ロギングを有効にする手順：

1. Bit9 イベントを記録する Syslog サーバーを準備します。サーバーの準備の詳細については、『Bit9 Events Integration Guide（Bit9 イベント統合ガイド）』を参照してください。

2. Bit9 コンソール メニューで、[**Administration**（管理）] > [**System Configuration**（システム構成）] の順に選択し、[System Configuration（システム構成）] ページで［**Events**（イベント）］タブをクリックします。
3. ［Events（イベント）］タブで、ページ下部にある［**Edit**（編集）］ボタンをクリックします。
4. ［External Event Logging（外部イベント ロギング）］パネルで、[**Syslog Enabled**（Syslog を有効にする）］ボックスをオンにします。



5. Syslog サーバーのアドレス（IP アドレスまたは FQDN）とポート番号をそれぞれ［Syslog Address（Syslog アドレス）］ボックスおよび［Syslog Port（Syslog ポート）］ボックスに入力します。
6. ［Syslog Format（Syslog 形式）］メニューから出力形式を選択します。
7. ［**Update**（更新）］ボタンをクリックし、確認ダイアログで［**Yes**（はい）］をクリックすると、構成が保存されます。

補足用の SQL Server へのイベントのロギング

外部ロギングを使用すると、カスタム レポートの実装を SQL で直接作成できます。外部サーバーを使用すると、Bit9 Server データベースに短期間イベントを保持しながら、フォレンジック要件やコンプライアンス要件を満たすためにイベントを長期間保存できます。また、パフォーマンス上の理由から外部イベント ロギングの実装が必要になる場合もあります。

外部ロギングを有効にしたときの動作の要点を次にいくつか示します。

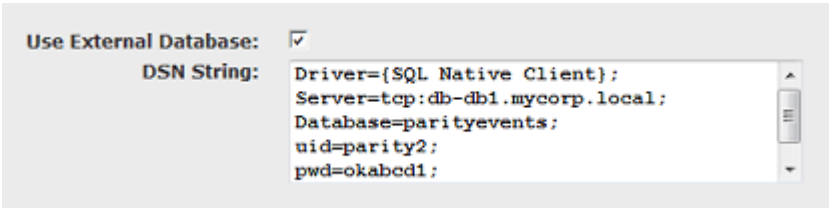
- 外部ロギングを使用しても、プライマリ SQL Server データベースのローカル ロギングは停止されません。イベント ロギングは続行され、指定した任意の期間のイベント（または指定した総数のイベント）が保存されます。
- システム パフォーマンスを向上させるため、プライマリ SQL Server データベースから外部のイベント SQL Server データベースへのイベント データのコピーは、連続的にではなく、約 30 秒おきに実行されます。
- 外部ロギングを有効にする前に発生したイベントは、外部ログにコピーされません。そのため、外部ロギングを設定し、すべてのイベントを記録する場合は、Bit9 Server のセットアップ時に外部ロギングも一緒にセットアップするのが一番よい方法です。
- 外部サーバーにアクセスできなくなった場合は、エラーがログに記録されますが、Bit9 Server の動作に変化はありません。外部サーバーが再び使用可能になると、ログに記録されていなかったイベントがコピーされます。

表 100、「外部イベント ロギングのオプション」（760 ページ）は、［Events（イベント）］タブの［External Event Logging（外部イベント ロギング）］パネルの各パラメーターを示しています。詳細については、Bit9 サポート Web サイトを参照するか、Bit9 サポートにお問い合わせください。

補足用の SQL データベースへの外部イベント ロギングを設定する手順の概要を次に示します。外部データベースで NT 認証を使用する場合は、次の手順に示す特別な DSN を使用してください。

追加の SQL Server への外部イベント ロギングを有効にする手順：

1. Bit9 イベントを記録するための十分な容量を備えたマシンに SQL Server をインストールします。DSN（データ ソース名）文字列の情報を控えておきます。この情報は、後から Bit9 コンソールで使用する必要があります。
2. 外部イベント スクリプト **external_events.sql** を実行し、Bit9 イベントを正しく保存できるように SQL データベースを構成します。このスクリプトは、**Bit9 Server\sql** フォルダーにあります。外部イベント ロギングを使用するには、新規にインストールした SQL Server 上でこのスクリプトを実行する必要があります。
3. コンソール メニューで、［**Administration**（管理）］>［**System Configuration**（システム構成）］の順に選択します。［System Configuration（システム構成）］ページが表示されます。
4. ［**Events**（イベント）］タブをクリックします。［External Event Logging（外部イベント ロギング）］パネルが表示されます。
5. ［**Edit**（編集）］ボタンをクリックし、［Use External Database（外部データベースの使用）］ボックスをオンにします。これにより、パネル上で［**Test**（テスト）］ボタンが有効になり、データ フィールドの編集が可能になります。
6. このデータベースの DSN を［DSN String（DSN 文字列）］フィールドに入力します。
   a. 手動認証の場合は、次のように入力します。各項目を 1 行ずる入力し、セミコロンで区切ります（下の図は例を示しています）。
      - Driver={SQL Native Client};
      - Server=**tcp:***yourfullyqualifiedservername\instancename*;
      - Database=**bit9Events;**
      - Uid=*usernameforSQLadmin;*
      - Pwd=*password;*



   b. NT 認証を使用する場合は、Bit9 Server のインストール時に指定したドメイン認証情報を入力することにより、外部イベント ロギング サーバーにアクセスできます。この場合は、次のように、上記の「Uid」行から「Pwd」行までを「Trusted_Connection」行に置き換えます。
      - Driver={SQL Native Client};

- Server=**tcp:***yourfullyqualifiedservername**instancename*;
- Database=**bit9Events**;
- Trusted_Connection=**Yes**;

注意

DSN 文字列がわからない場合は、Bit9 Server のホーム ディレクトリにある shepherd.dsn ファイルを参照してください。

7. DSN が機能することを確認するために、[**Test**（テスト）] ボタンをクリックします。DSN が適切に構成されている場合は、[DSN String（DSN 文字列）] ボックスの下に「Testing: Success（テスト：成功）」というメッセージが表示されます。DSN が適切に構成されていない場合は、エラー メッセージが表示されます。
8. DSN のテストが成功したら、[**Update**（更新）] ボタンをクリックし（テストが成功し、なおかつチェックボックスがオンになっている場合、[Update（更新）] ボタンをクリックすると、[Test（テスト）] ボタンが [Update（更新）] ボタンに置き換えられます）、確認ダイアログで [**Yes**（はい）] をクリックします。これにより、外部ロギングが有効になります。

外部イベント ロギングを無効にする手順：

1. コンソール メニューで、[**Administration**（管理）] > [**System Configuration**（システム構成）] の順に選択します。[System Configuration（システム構成）] ページが表示されます。
2. [**Events**（イベント）] タブをクリックします。[External Event Logging（外部イベント ロギング）] パネルが表示されます。
3. [**Edit**（編集）] ボタンをクリックします。これにより、パネル上のデータ フィールドの編集が可能になります。
4. [**Use External Database**（外部データベースの使用）] ボックスをクリックしてオフにします。これにより、[Test（テスト）] ボタンが [Update（更新）] ボタンに変化します。
5. [**Update**（更新）] ボタンをクリックし、確認ダイアログで [**Yes**（はい）] をクリックします。外部イベント ロギングが無効になります。

表 100：外部イベント ロギングのオプション

フィールド	説明
Syslog Enabled（Syslog を有効にする）	Syslog 管理ツールで詳細に分析するために Bit9 イベント情報を別のサーバーに出力するかどうかを指定するチェックボックス。オンにした場合は、Syslog サーバーのアドレスとリッスン ポートも指定する必要があります。デフォルトでは、このオプションはオフになっています。 **注意**：Syslog 管理ツールで Bit9 イベント出力を使用する方法については、Bit9 テクニカル サポートにお問い合わせください。
Syslog Address（Syslog アドレス）	Syslog サーバーの IP アドレス（オプション）。Syslog アドレスを指定した場合は、Syslog サーバーのポートも入力する必要があります。 **注意**：設定した Syslog のアドレスやポートに誤りがあっても、エラーは報告されません。Syslog アドレスが正しく設定されたことを確認するには、この構成が完了した後、Syslog サーバーで Bit9 イベントが受信されることを確認してください。
Syslog Port（Syslog ポート）	Syslog サーバーのポート番号。 リッスン ポートに送信される Bit9 イベントには、ブロックされたファイル、システム上の新しいファイル、ログイン アカウントの変更などのアクティビティ メッセージが含まれます。 イベント データをエクスポートしても、イベントは引き続き［Events（イベント）］ページに書き込まれます。［Events（イベント）］ページには、Bit9 コンソールからアクセスできます。Syslog ポートを指定した場合は、Syslog サーバーのアドレスも入力する必要があります。
Syslog Format（Syslog 形式）	次のいずれかを指定します。 • **基本(RFC3164)** – 6.0.2より前のバージョンのBit9からアップグレードする場合のデフォルトです。 • **拡張 (RFC5424)** – より新しい標準であり、Bit9 v7.0.1 以降を新規にインストールする場合のデフォルトです。 • **CEF (ArcSight)** – Bit9イベント ログをHP ArcSight ESMまたは HP ArcSight Logger に統合する場合に使用する形式です。 • **LEEF (Q1Labs)** – Bit9 イベント ログを QRadar SIEM または QRadar Log Manager に統合する場合に使用する形式です。 Bit9 Security Platform でサポートされる syslog 形式と、Bit イベントをそれらの形式にマッピングする方法の詳細については、『Bit9 Events Integration Guide（Bit9 イベント統合ガイド）』を参照してください。 **注意**：6.0.2 より前のリリースで、Bit9 テクニカル サポートの支援を受けながら特別な Syslog 形式を手動で有効にした場合は、v7.2.3 にアップグレードしたときに変更が上書きされます。［Syslog format（Syslog 形式）］メニューを使用して、形式を選択してください。

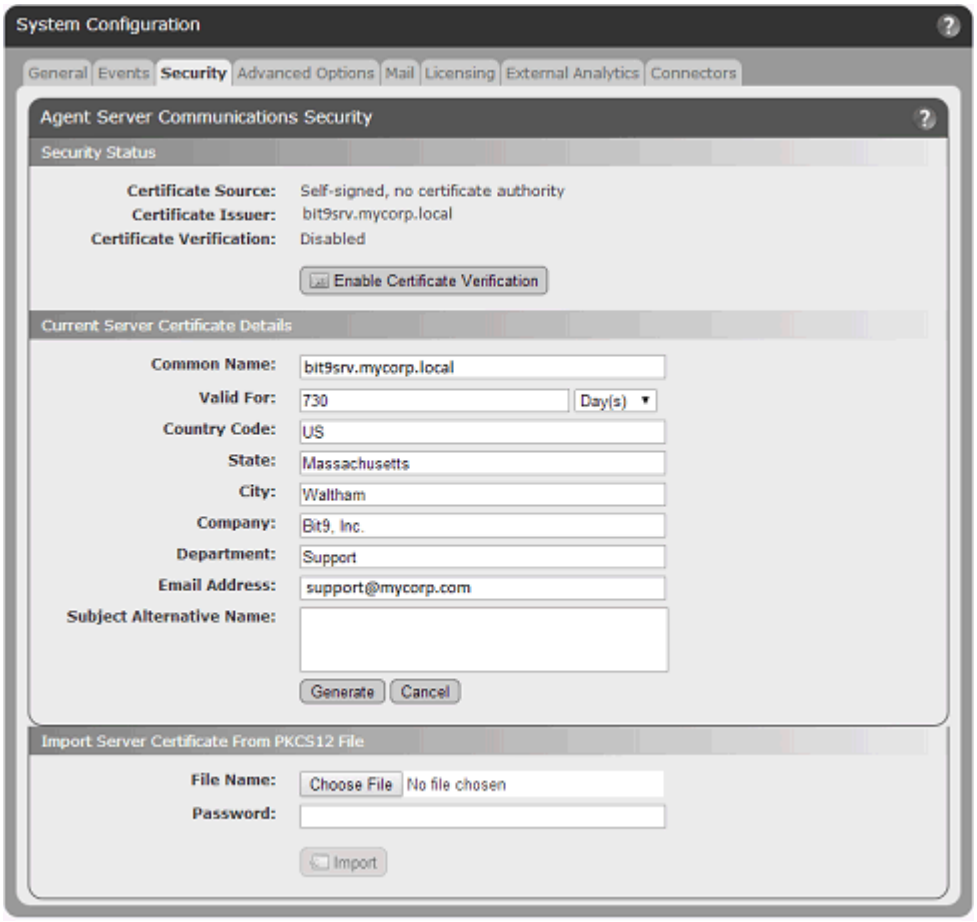
フィールド	説明
Use External Database（外部データベースの使用）	このボックスをオンにすると、外部 SQL データベースを使用できるようになります。オフにすると、Bit9 イベントが外部データベースに報告されなくなります。
DSN String（DSN 文字列）	使用する外部データベースを識別する DSN 文字列。手動認証と NT 認証のどちらを使用するかによって異なります。この項目の構成方法については、「追加の SQL Server への外部イベント ロギングを有効にする手順：」（758 ページ）を参照してください。

エージェント – サーバー間通信の保護

Bit9 Security Platform では、サーバーとエージェント間の通信に SSL セキュリティが使用されます。デフォルトでは、Bit9 Server のインストール時に生成された自己署名 Bit9 セキュリティ証明書が使用されますが、インストール時に別の証明書を指定することもできます。

［System Configuration（システム構成）］の［**Security**（セキュリティ）］タブには、エージェント – サーバー間通信の構成ページが表示されます。このページでは、次のような変更を行えます。

- 現在、エージェント – サーバー間通信で自己署名証明書が使用されている場合は、証明書の詳細を編集できます。
- PKCS#12 ファイルから別の証明書をインポートできます（自己署名証明書、または認証局から）。
- 証明書の検証を有効にして、セキュリティを向上させることができます。これにより、Bit9 エージェントが稼動しているコンピューターで、Bit9 Server に正しい証明書が存在するかどうかが常に検査されるようになります。これを変更できるのは 1 回のみで、取り消すことはできません。証明書の検証は既知の認証局に対してのみ行う必要があり、自己署名証明書に対しては検証を有効にしないでください。



セキュリティ ステータス

このページの上部のパネルには、エージェント – サーバー間通信のセキュリティ ステータスが表示されます。具体的には、(1) 証明書のソース（自己署名証明書かインポートされた証明書か）、(2) 証明書の発行者が証明書に関連付けられているかどうか、(3) エージェントがサーバーに問い合わせて証明書の正当性を検証するように Bit9 Security Platform が構成されているかどうかが報告されます。自己署名証明書の場合、証明書の発行者は Bit9 Server の名前であり、証明書に既知の認証局はありません。このパネルには、証明書の検証を有効にするボタンも含まれています。

現在の証明書の詳細

［Current Server Certificate Details（現在のサーバー証明書の詳細）］パネルには、セキュリティ証明書から得られる標準的な詳細が表示されます。証明書が自己署名証明書の場合は、詳細を編集して証明書を再生成できます。

自己署名された通信セキュリティ証明書の詳細を編集する手順：

1. コンソール メニューで、[**Administration**（管理）] > [**System Configuration**（システム構成）] の順に選択します。[System Configuration（システム構成）] ページが表示されます。
2. [**Security**（セキュリティ）] タブをクリックします。[Agent Server Communications Security（エージェント – サーバー間通信のセキュリティ）] ページが表示されます。
3. [Current Server Certificate Details（現在のサーバー証明書の詳細）] パネルで、[**Edit**（編集）] ボタンをクリックします。詳細パネルのフィールドが編集可能になり、[Edit（編集）] ボタンが [Generate（生成）] ボタンと [Cancel（キャンセル）] ボタンに置き換えられます。
4. 証明書の詳細を必要に応じて変更した後、[**Generate**（生成）] ボタンをクリックすると、新しい詳細を含む証明書が生成されます。変更をキャンセルするには、代わりに [**Cancel**（キャンセル）] ボタンをクリックします。

表 101：エージェント – サーバー間通信の証明書の詳細

フィールド / ボタン	説明
Common Name（コモン ネーム）	エージェントが接続する Bit9 Server の完全修飾ドメイン名を指定する必要があります。
Expiration Date（有効期限）/ Valid For（有効期間）	証明書が期限切れになる日時が表示されます。証明書の詳細を編集するときに、このフィールドは [**Valid For**（有効期間）] に変わり、ボックスが表示されます。表示されたボックスに、証明書を有効にする日数または年数を入力します。 **注意**：自己署名証明書の場合、[Valid For（期間）] に 20 年または 7300 日を超える値を入力することはできません。
Country Code（国コード）	証明書に責任を持つ組織の標準的な 2 文字の国コード。
State（状態）	状態（情報がある場合）。
City（市区町村）	市区町村。
Company（会社）	証明書に責任を持つ会社。
Department（部門）	会社内の部門（情報がある場合）。
Email Address（E メール アドレス）	証明書に関する詳細情報を必要としているユーザーのための連絡先情報。

フィールド / ボタン	説明
Subject Alternative Name（サブジェクトの別名）	サブジェクトの別名 (SAN) は、サーバー ホスト名を基準として証明書を検証する代替の手段です。SAN では、単一のサーバーに対して複数の DNS 名や IP アドレスをコンマで区切って指定できます。これにより、さまざまなネットワーク ルートからのアクセスがあるときでも証明書の検証が可能であり、また、同じ証明書を複数のサーバーで使用することができます。 デフォルトでは、[Subject Alternative Name（サブジェクトの別名）] フィールドは空です。必要な形式は、ツールチップに表示されます。SAN エントリの形式の例を次に示します。 DNS=bit9platform.mycorp.com, DNS=bit9platform.mycorp.local,IP=10.0.8.123 DNS 名には、ワイルドカードを使用できます（例：*.mycorp.com）。

サーバー名と証明書の一致の検証

サーバー名と証明書が一致するかどうかがエージェントによってどのように検証されるかは、サーバー証明書に含まれているサーバー情報によって異なります。

- 証明書のDNSエントリにサブジェクトの別名(SAN)が含まれている場合は、そのエントリと、エージェントが使用するサーバー アドレスとが比較され、両方が一致する必要があります。
- DNS エントリに SAN が含まれていない場合は、エージェントが使用するサーバー アドレスと、サーバー証明書のコモン ネーム (CN) とが比較検証され、両方が一致する必要があります。

エージェントとサーバー証明書間でアドレス / 名前の形式が一致しないと、たとえ名前が IP アドレスに解決されても検証に失敗します。たとえば、エージェントで IPv6 アドレスが使用されていて、SAN で IPv6 アドレスが使用されていない場合は、検証に失敗します。この問題を解決するには、もう 1 つのアドレス（IPv6 アドレス）を DNS=[IPv6] 形式で SAN に追加します。

証明書のインポート

必要な場合は、新しい SSL 証明書をインポートできます。証明書をインポートするときには、次の点に注意してください。

- 期限切れの証明書はインポートできません。
- サポートされるのは、PKCS#12 証明書のみです。別のバージョンの PKCS を使用することはできません。別の形式の証明書を使用するには、最初に PKCS#12 ファイル形式に変換する必要があります。
- 証明書をインポートする場合、インポートした証明書は編集できないため、[Current Certificate Details（現在の証明書の詳細）] パネルに［Edit（編集）］ボタンは表示されません。

- Bit9 Security Platform では、複数レベルの証明書の使用がサポートされます。実際の証明書は、PKCS#12 コンテナー ファイルの「最後」で指定されている必要があります。
- インポートできのは、Bit9 Server のホスト名または IP アドレスに一致する証明書のみです。

注意

Bit9 Server のインストール時には、自己署名証明書を生成するか、Bit9 コンソール用の実際の証明書をインポートする必要があります。実際の証明書をインポートする場合は、エージェント – サーバー間通信用にも同じ証明書を使用できます。このオプションを選択した場合は、次の手順を実行する必要はありません。

エージェント – サーバー間で安全に通信するための新しい証明書をインポートする手順：

1. コンソール メニューで、[**Administration**（管理）] > [**System Configuration**（システム構成）] の順に選択します。[System Configuration（システム構成）] ページが表示されます。
2. [**Security**（セキュリティ）] タブをクリックします。[Agent Server Communications Security（エージェント – サーバー間通信のセキュリティ）] ページが表示されます。
3. [Import Server Certificate（サーバー証明書のインポート）] パネルで [Browse（参照）] をクリックし、新しい証明書ファイルの場所に移動します。ファイル選択ダイアログでファイルを見つけたら、[**Open**（開く）] をクリックします。
4. 証明書ファイルのパスワードを入力します。
5. 必要な情報を入力したら、[**Import**（インポート）] をクリックします。変更の影響を説明するダイアログ ボックスが表示されます。
6. 証明書のインポートを完了するには、確認ダイアログで **[OK]** をクリックします。インポートの成否を示すステータス メッセージが表示されます。インポートが成功した場合は、新しい証明書が証明書リポジトリにインストールされ、[Current Server Certificate Details（現在のサーバー証明書の詳細）] パネルのすべてのフィールドが更新されます。

証明書の検証の有効化

証明書の検証を有効にすると、すべての Bit9 エージェントは、認証局またはそのルート証明書と比較して Bit9 Server 証明書が本物かどうかを検証するようになります。これにより、エージェントとサーバー間の通信をスプーフィングできなくなるため、通信セキュリティのレベルが向上します。

重要

証明書の検証は、一度有効にすると取り消すことができません。したがって、必要な証明書が所定の場所にあり、検証機能を実装しても問題がないことを確認してから、ボタンをクリックしてください。自己署名証明書は既知の認証局で生成されたものではないため、自己署名証明書を使用する場合は証明書の検証を有効にしないでください。

エージェントがサーバーに対して通信証明書の検証を要求するように設定する手順：

1. コンソール メニューで、[**Administration**（管理）] > [**System Configuration**（システム構成）] の順に選択します。[System Configuration（システム構成）] ページが表示されます。
2. [**Security**（セキュリティ）] タブをクリックします。[Agent Server Communications Security（エージェント – サーバー間通信のセキュリティ）] ページが表示されます。
3. 必要に応じて証明書の変更（自己署名証明書の詳細の編集や、ファイルからの新しい証明書のインポートなど）を行います。
4. [Security Status（セキュリティ ステータス）] パネルで、[**Enable Certificate Verification**（証明書の検証の有効化）] ボタンをクリックします。変更を適用しても問題がない場合は、確認ダイアログで **[OK]** をクリックします。Bit9 コンソールでこの変更を取り消すことはできません。[OK] をクリックすると、[Enable Certificate Verification（証明書の検証の有効化）] ボタンが消え、[Certificate Verification（証明書の検証）] フィールドが [Enabled（有効）] に変わります。

高度な構成オプション

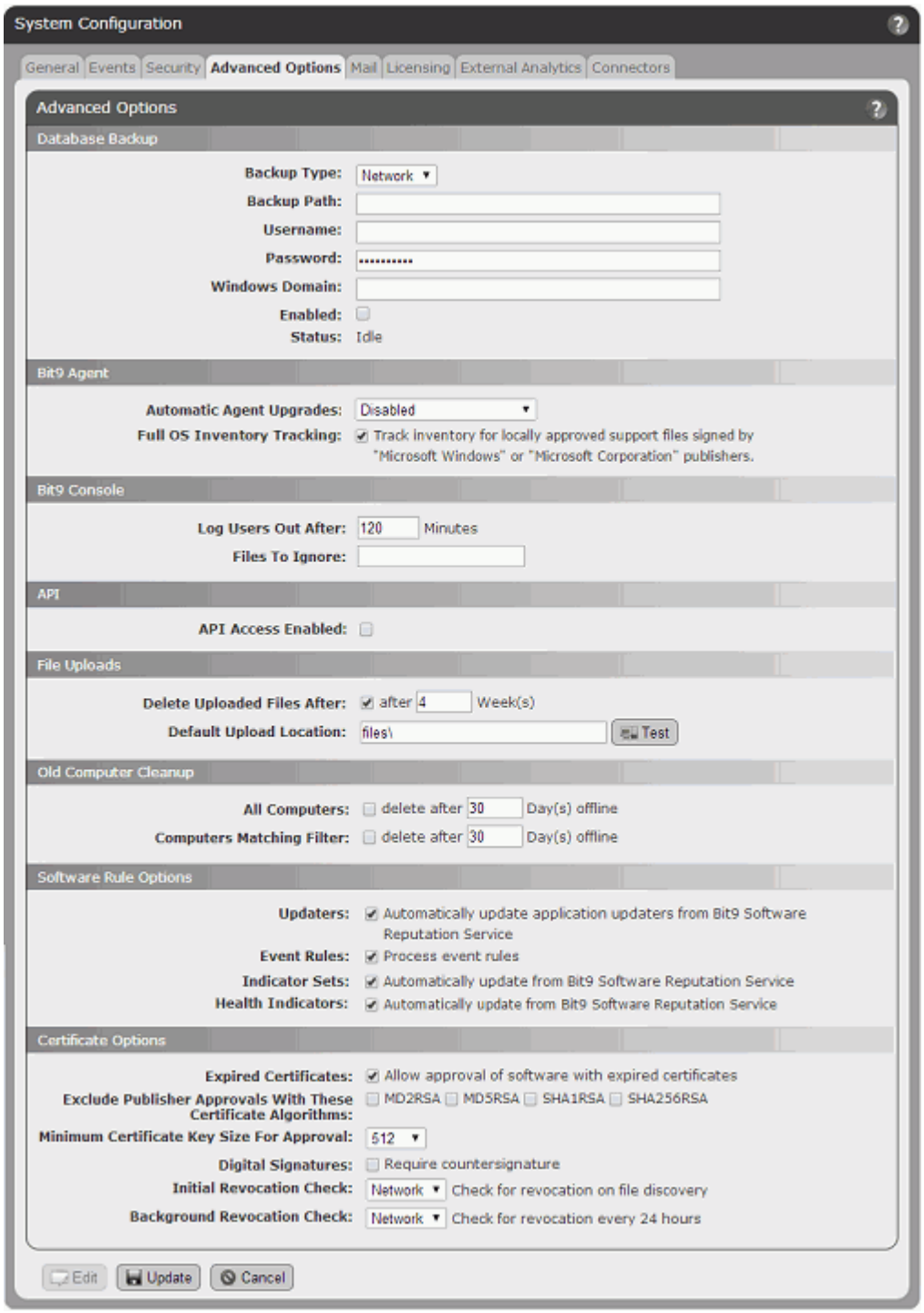
[System Configuration（システム構成）] ページの [Advanced Options（高度なオプション）] タブには、データベースのバックアップ、コンピューターとエージェントの管理、証明書とアップデーターのルール、コンソール全般の管理に関するオプションが含まれています。また、オプション機能の設定項目も含まれている場合があります。

[Database Backup（データベース バックアップ）] のオプション（およびバックアップと復元の手順）については、「Bit9 Server のバックアップ」（772 ページ）と「Bit9 Server の復元」（775 ページ）を参照してください。

このセクションでは、その他の高度なオプションの概要を説明します。表 102 は、このページのパラメーターを説明したものです（[Database Backup（データベース バックアップ）] のパラメーターについては、上記のセクションで説明しています）。

高度な構成オプションを表示および編集する手順：

1. コンソール メニューで、［**Administration**（管理）］>［**System Configuration**（システム構成）］の順に選択します。［System Configuration（システム構成）］ページが表示されます。
2. ［**Advanced Options**（高度なオプション）］タブをクリックします。［Advanced Options（高度なオプション）］構成ページが表示されます。



3. いずれかの構成情報を変更する必要がある場合は、[**Edit**（編集）] をクリックし、必要な変更を行います。
4. 変更を適用するには、[**Update**（更新）] ボタンをクリックし、確認ダイアログで [**Yes**（はい）] をクリックします。

表 102：高度な（構成）オプション

セクション：フィールド	説明
Database Backup（データベース バックアップ）	これらのオプションの説明については、「Bit9 Server のバックアップ」（772 ページ）を参照してください。
Bit9 Agent（Bit9 エージェント）：Automatic Agent Upgrades（エージェントの自動アップグレード）	[**Enabled**（有効）] にした場合、新しいバージョンのエージェントが入手可能になると Bit9 エージェントに通知がプッシュされます（ただし、そのエージェントが属しているポリシーでもエージェントのアップグレードが有効になっている場合のみ）。このフィールドは Bit9 Server をアップグレードするときに使用するためのものであり、通常は [**Disabled**（無効）] に設定されています。新しくインストールされた Bit9 Server には影響しません。エージェント アップグレードの詳細な手順については、『Installing Bit9 Server（Bit9 Server のインストール）』ガイドを参照してください。
Bit9 Agent（Bit9 エージェント）：Full OS Inventory Tracking（OS インベントリの完全追跡）	このボックスをオンにした場合は、このサーバーのファイル インベントリで、Microsoft からのすべてのファイルが追跡されます。オフにした場合は、Bit9 データベースにある、ローカルで承認されたサポート ファイルのうち、公開者が「Microsoft Windows」または「Microsoft Corporation」であるファイルが追跡の対象から除外されます。これにより、サーバーの負荷を大幅に削減できます。詳細については、「Microsoft サポート ファイルの追跡の除外」（239 ページ）を参照してください。
Bit9 Console（Bit9 コンソール）：Log Users Out After（ユーザーがログアウトされるまでの時間）	何の操作も行われないまま指定された時間が経過すると、ユーザーは Bit9 コンソールから自動的にログアウトします。
Bit9 Console（Bit9 コンソール）：Files to ignore（無視するファイル）	[Files（ファイル）] ページのリストから除外するファイルをコンマで区切って指定します。必要に応じて、ワイルドカード文字 (*) も使用できます。無視されたファイルに関連するイベントは引き続き [Events（イベント）] テーブルに表示され、アラートをトリガーできます。無視されたファイルは、[Find Files（ファイルの検索）] の結果として確認できます。基本的に、これらのファイルが Bit9 Server の通常の操作で使用されることありません。

セクション：フィールド	説明
API	[API Access Enabled（API アクセスを有効にする）] をオンにすると、このサーバーで Bit9 API が使用可能になります。Bit9 API を使用すると、さまざまな言語による自動化やスクリプトを通じてBit9 Platformとそのデータベースにアクセスできます。詳細については、付録 B「Bit9 API」を参照してください。
File Uploads（ファイルのアップロード）	（オプション）エージェント コンピューターからファイルをアップロードするための機能。利用には別途ライセンスが必要です。ファイルのアップロード先とファイルをサーバーに残しておく期間を指定します（この期間が経過すると、ファイルが削除されます）。詳細については、「エージェントからのファイルのアップロード」（913 ページ）を参照してください。
Old Computer Cleanup（古いコンピューターのクリーンアップ）：All Computers（すべてのコンピューター）	オフラインの状態のままこの期間が経過すると、切断されているすべてのコンピューターが、Bit9 Security Platform で管理されるコンピューターのリストから削除されます。このボックスをオンにしてクリーンアップを有効にし、オフラインのコンピューターを削除するまでの日数を入力します。 削除されたコンピューターが再接続されたときに、そのコンピューターで Bit9 エージェントがまだ実行されている場合は、そのコンピューターのファイル リストが再同期され、最後に構成されたポリシー（存在する場合）またはデフォルト ポリシーに戻ります。詳細については、「コンピューターの削除」（177 ページ）を参照してください。
Old Computer Cleanup（古いコンピューターのクリーンアップ）：Computers Matching Filter（フィルターに一致するコンピューター）	一定期間が経過すると、Bit9 で管理されるコンピューターのリストからフィルターに一致するコンピューターが自動的に削除されます。このボックスをオンにしてクリーンアップを有効にし、オフラインのコンピューターを削除するまでの日数を入力します。 1 つまたは複数のフィルターを追加して、指定した条件に一致するコンピューターのみを削除することもできます。たとえば、時間制限に達したときに、仮想コンピューターのみを削除することが可能です。また、特定のタグ（「Visitor」など）に一致するすべてのコンピューターを削除することも可能です。フィルターのオプションを次に示します。 • Computer name（コンピューター名） • Computer tag（コンピューター タグ） • IP Address（IP アドレス） • Identifier（MAC address）（識別子（MAC アドレス）） • Parent Template（親テンプレート） • Platform（プラットフォーム） • Policy（ポリシー） • Virtualized（仮想化済み） • Virtual Platform（仮想プラットフォーム） すべてのフィルター条件に一致したコンピューターのみが削除されます。

セクション：フィールド	説明
Software Rule Options（ソフトウェア ルールのオプション）：Updaters（アップデーター）	[Automatically update application updaters from Bit9 SRS（Bit9 SRS からアプリケーション アップデーターを自動更新）] をオンにすると、Bit9 SRS は、Bit9 Server の［Software Rules（ソフトウェア ルール）］セクションにある［Updaters（アップデーター）］リストを、確認した新しいバージョンで常に最新の状態に維持します。 オフにした場合、リストされるアップデーターは、サーバーのインストール時に指定されたアップデーターのままとなります。アップデーターを手動で定義した場合は、そのアップデーダーがリストに補足されます。
Software Rule Options（ソフトウェア ルールのオプション）：Event Rules（イベント ルール）	[Process event rules（プロセス イベント ルール）] をオン（デフォルト）にすると、[Event Rules（イベント ルール）] ページで定義および有効化されたイベント一致ルールにより、ファイルの分析やファイルの禁止などのアクションをトリガーできます。詳細については、「イベント ルール」（517 ページ）を参照してください。
Software Rule Options（ソフトウェア ルールのオプション）：Indicator Sets（痕跡セット）	[Automatically update from Bit9 Software Reputation Service（Bit9 Software Reputation Service から自動更新）] をオン（デフォルト）にすると、Bit9 SRS は、脅威検出に使用される痕跡セットを常に最新の状態に維持します。痕跡セットの詳細については、第 20 章「高度な脅威検出」を参照してください。
Software Rule Options（ソフトウェア ルールのオプション）：Health Indicators（正常性の痕跡）	[Automatically update from Bit9 Software Reputation Service（Bit9 Software Reputation Service から自動更新）] をオン（デフォルト）にすると、Bit9 SRS は、システム正常性の監視および報告に使用される正常性の痕跡をダウンロードし、必要に応じて更新します。オフにした場合、[System Health（システム正常性）] 機能は使用できません。正常性の痕跡の詳細については、第 24 章「システム正常性の監視」を参照してください。
Certificate Options（証明書オプション）：Expired Certificates（期限切れの証明書）	[Allow approval of software with expired certificates（期限切れの証明書でのソフトウェアの承認を許可）] をオンにすると、期限切れの証明書を公開者ベースのファイル承認に使用できます（ただし、その証明書が過去に有効であった場合に限られ、なおかつ、証明書が有効であった期間内に証明書のタイムスタンプが付与されている場合に限られます）。詳細については、「期限切れの証明書での承認」（297 ページ）を参照してください。 オフにした場合、証明書の期限が切れているソフトウェアは公開者に基づく承認の対象から除外されます。

セクション：フィールド	説明
Certificate Options（証明書オプション）：Exclude Publisher Approvals With These Certificate Algorithms（これらの証明書アルゴリズムで公開者の承認を除外する）	このオプションによりは、公開者に基づく承認の対象から除外される証明書が決定されます。証明書アルゴリズムのボックスがオンになっている場合、そのアルゴリズムの証明書を使用して公開者が署名したファイルは、公開者に基づく承認の対象から除外されます。詳細については、「証明書アルゴリズムの除外」（298 ページ）を参照してください。 以下のオプションを選択できます。 • MD2RSA • MD5RSA • SHA1RSA • SHA256RSA
Certificate Options（証明書オプション）：Minimum Certificate Key Size For Approval（承認用の証明書キーの最小サイズ）	このオプションでは、公開者に基づくファイルの承認で使用する証明書のキーの最小長を指定します。キー サイズが指定した値以上である証明書のみを、公開者に基づく承認に使用できます。キー サイズが選択した値を下回る証明書は、承認に使用できません。デフォルト値は **512** です。詳細については、「最小キー サイズ」（298 ページ）を参照してください。
Certificate Options（証明書オプション）：Digital Signatures（デジタル署名）	[Require countersignature（連署が必要）] がオンの場合は、公開者を識別するために使用される各証明書のデジタル署名に連署が必要です。このオプションの構成に役立つ情報については、「連署オプション」（298 ページ）を参照してください。
Certificate Options（証明書オプション）：Initial Revocation Check（初期の失効検査）	エージェント上で最初にファイルが検出されたときに、証明書の失効検査を実行するかどうかと、その方法を指定します。次の 3 つの値があります。 • **Network**（ネットワーク）– 失効情報がローカルで提供されていない場合は、ネットワークを使用して、証明書の失効ステータスを取得します。 • **Cache**（キャッシュ）– 証明書の失効を実行するときに、ローカルで提供されている失効ステータス情報を使用します（ネットワークは使用しません）。 • **None**（なし）– 証明書の失効検査を実行しません。 エージェントのパフォーマンスに影響が及ぶ可能性があるため、これらの値を設定するときは、エージェントの展開シナリオを考慮してください。詳細については、「失効検査」（299 ページ）を参照してください。

セクション：フィールド	説明
Certificate Options（証明書オプション）：Background Revocation Check（バックグラウンドでの失効検査）	24 時間ごとにエージェント上で既存のファイルに対して証明書の失効検査を実行するかどうかと、その方法を指定します。有効にした場合、これらの検査はバックグラウンドで実行されます。指定できる値は、[Initial Revocation Check（初期の失効確認）]（上記）と同じです。 詳細については、「失効検査」（299 ページ）を参照してください。 **注意**：通常、証明書の失効検査は、1 週間ごとにサーバーでも実行されます。サーバー ベースの失効検査は、初期またはバックグラウンドの失効検査の設定には影響されません。ネットワーク接続を監視している場合、表示されるトラフィックの一部は、これらの失効検査のものとなり、さまざまな国のサイトが含まれる場合があることに注意してください。

Bit9 Server のバックアップ

SQL Server管理者が標準的なバックアップ計画とバックアップ メカニズムをすでに実装している場合は、そのメカニズムを使用して Bit9 データベースをバックアップすることを推奨します。

別個のデータベース バックアップ メカニズムがない場合や、既存のバックアップ メカニズムを使用しない場合のために、Bit9 には、Bit9 Security Platform システムを完全にバックアップし、現在の構成（コンピューターの構成、システム設定、ファイル データベース、イベント ログなど）をそのまま復元するメカニズムが用意されています。Bit9 バックアップ メカニズムでは、重要な変更（ポリシーの変更など）が行われると、6 時間以内にデータベースのすべての変更がバックアップされます。完全バックアップは、1 日 1 回実行されます。継続的に自動バックアップが行われるため、サーバーとそれに接続されているコンピューターは、バックアップ構成を復元した後も引き続き同期されます。

バックアップ フォルダーの空き容量は、Bit9 Server データベースのサイズの 2 倍以上に保つ必要があります。バックアップ フォルダーとメインの SQL データベースの両方について、ディスク容量を定期的に監視し、容量超過にならないように注意してください。

Bit9 Server のバックアップ機能では、Bit9 データベースをホストしている SQL Server インスタンス上で **xp_cmdshell** のサポートを有効にする必要があります。xp_cmdshell を有効にする手順については、SQL Server のドキュメントを参照してください。このタスクに関する情報が得られるリンクを次に示します。

- SQL Server 2008: http://www.mssqltips.com/sqlservertip/1673/where-is-the-surface-area-configuration-tool-in-sql-server-2008/
- SQL Server 2012: http://msdn.microsoft.com/en-us/library/ms190693.aspx

重要

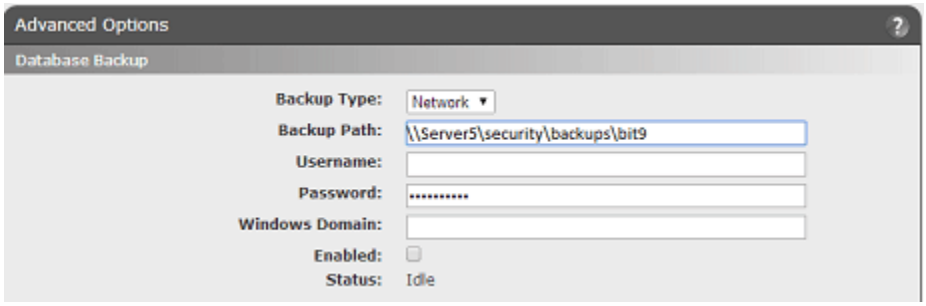
xp_cmdshell を有効にするとセキュリティに影響が及びます。そのため、サイトの SQL Server 管理者は、機密漏れを制限するために、すべてのベスト プラクティスに従う必要があります。これには、次の推奨事項が含まれますが、この内容に限定されるわけではありません。

- sysadmin 以外のプリンシパルにアクセス権を付与しないこと。
- SQL Serverのsysadmin権限は、信頼できるSQL Serverシステム管理者にのみ付与すること。

Bit9 バックアップ　　メカニズムの使用を中止する場合は、xp_cmdshell を無効にしてください。

Bit9 Security Platform のデータベース バックアップ メカニズムを使用する手順：

1. SQL Server で xp_cmdshell が有効になっていることを確認します。
2. コンソール メニューで、[**Administration**（管理）] > [**System Configuration**（システム構成）] の順に選択します。
3. [**Advanced Options**（高度なオプション）] タブをクリックします。[Advanced Options（高度なオプション）] ページが表示されます。ページ上部に、[Database Backup（データベース バックアップ）] パネルがあります。
4. ページ下部にある [**Edit**（編集）] ボタンをクリックし、バックアップ先と構成オプションを指定します（表 103 を参照）。



5. [**Update**（更新）] ボタンをクリックし、確認ダイアログで [**Yes**（はい）] をクリックします。バックアップを有効にしてバックアップ構成を保存するたびに、Bit9 Server は、バックアップ設定をテストし、構成が失敗した場合はエラー メッセージを表示します。また、[Events（イベント）] ページにメッセージを書き込み、バックアップの成否や問題があるかどうかを通知します。

表 103：[Database Backup（データベース バックアップ）] のオプション

フィールド	説明
Backup Type（バックアップ タイプ）	[Network（ネットワーク）] または [Local（ローカル）]。ローカル バックアップには、Bit9 Server ドライブと異なる物理ドライブを使用する必要があります。
Backup Path（バックアップ パス）	Bit9 データベースおよび構成のバックアップが保存される、コンピューターまたはストレージ メディアの完全なパス。バックアップ ディレクトリは、Bit9 Server 管理者のみがアクセスできるようにして保護してください。最高のパフォーマンスを得るために、不要なサブディレクトリの作成は避け、できるだけサーバーのルート ディレクトリから近い階層にバックアップ ディレクトリを作成してください。以下に例を示します。 \\server_name\bit9_backup **注意**： • ローカル バックアップの場合は、ローカル パスを使用することを推奨します。ローカル ドライブの場合は、UNC パス（上記の形式）を使用できますが、[Local（ローカル）] オプションには、ユーザー名、パスワード、Windows ドメインの情報が含まれないため、このパスを作成する際に権限は使用されません。 • Bit9 Server がリモート データベースに接続されている場合、ここで指定するバックアップ パスは、データベース サーバーを基準とした相対パスになり、ユーザー名、パスワード、および Windows ドメインの各フィールドは表示されません。
Username（ユーザー名）（ネットワーク バックアップ）	ネットワーク バックアップ ディレクトリへの書き込み権限を持つユーザーの名前。
Password（パスワード）（ネットワーク バックアップ）	ネットワーク バックアップ ディレクトリへの書き込みを行うユーザー アカウントのドメイン パスワード。セキュリティを確保するために、パスワードは Bit9 データベース内で暗号化されます。
Windows domain（Windows ドメイン）（ネットワーク バックアップ）	ネットワーク上のバックアップ先にアクセスするユーザー アカウントが属している Windows ドメイン。
Enabled（有効）	指定した保存先へのバックアップを 2 分間隔で開始するには、このボックスをオンにします。 自動バックアップを中止するには、このチェックボックスをオフにします。
Status（ステータス）（読み取り専用）	次回のバックアップ予定時刻、または最新のバックアップのステータス（エラーがある場合は、エラーを含む）。

重要

バックアップ ディレクトリを構成した後、そのディレクトリ内でファイルの追加、削除、編集は行わないでください。更新は継続的に行われているため、そのような変更は、ファイルの同期やバックアップの整合性に影響を与えます。

Bit9 Server の復元

Bit9 Security Platform システムを直近の状態に復元することが可能です。Bit9 データベースおよび設定の復元には、手動による手順が必要で、Bit9 Server を再インストールする必要があります。安全のため、Bit9 の復元手順では、自動バックアップが無効にされ、バックアップ コピーが上書きされなくなります。これにより、バックアップ コピーを安全な場所にコピーすることが可能になります。

Bit9 エージェントは、Bit9 Server とは独立して動作します。Bit9 Server を再インストールし、バックアップ構成を復元している間、コンピューターは、前回のポーリング時に Bit9 Server から受信した構成設定に従って、保護され続けます。

Bit9 Security Platform を直近の構成に復元する手順：

1. Windows システムが破損している場合は、Bit9 Server ハードウェアにオペレーティング システムを再インストールします。インストールのガイドラインについては、『Installing Bit9 Server（Bit9 Server のインストール）』ガイドを参照してください。
2. Bit9 Server を再インストールします。

   重要

   再インストール時に、インストール先のコンピューターの IP アドレスが検出されます。DNS 名を使用して Bit9 Server をインストールした場合は、名前が同じで IP アドレスが異なるコンピューターに Bit9 Server を再インストールできる場合があります。それ以外の場合、IP アドレスが異なるコンピューターに Bit9 Server を再インストールするには、Bit9 エージェントもすべてのコンピューターに再インストールする必要があります。インストール時、コンピューターはファイルを再初期化し、以前未承認だったファイルをローカルで承認します。この復元手順により、新しいサーバー IP アドレスを使用するように、既存のエージェント インストール パッケージが自動的に更新されます。

   a. 指定されたサーバーに接続されているドライブにBit9 CD（Bit9の実行可能イメージ）を挿入します。

b. メッセージに従ってインストーラーを実行します。サーバーIP アドレスの変更、ターミナル サービスを使用したインストール、DNS 名の使用など、各種インストール オプションについては、『Installing Bit9 Server（Bit9 Server のインストール）』ガイドを参照してください。

c. ［Install Type Option（インストール タイプ オプション）］画面で、［**Restore from backup**（バックアップから復元）］オプションを選択します。

d. バックアップ ディレクトリに移動します。

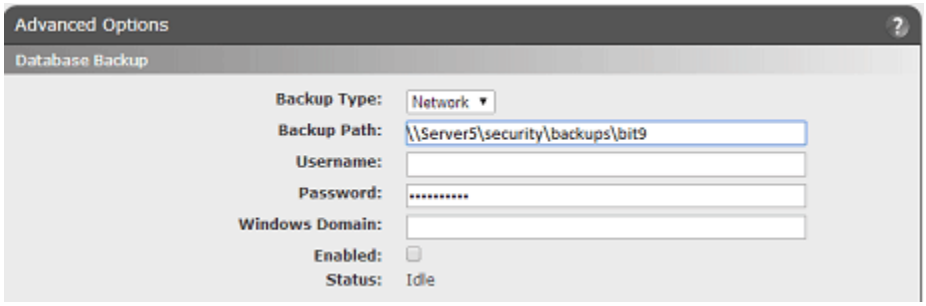
e. 標準的なインストール手順を示す残りのメッセージに従ってインストールが完了したら、手順を終了します。

3. 復元手順の間は、継続バックアップが自動的に無効になります。次の手順に従って自動バックアップを再開します。

a. バックアップ　フォルダー内のすべてのファイルを新しい場所にコピーして、上書きされないようにします（または、新しいバックアップ フォルダーを指定して、既存のバックアップ ファイルはそのままにしておきます）。

b. 現在指定されているバックアップ　ディレクトリが空であることを確認します。これにより、古いファイルによってデータが破損することなくフレッシュ バックアップが完了します。

c. Bit9 コンソール メニューで、［**Administration**（管理）］>［**System Configuration**（システム構成）］を選択し、［**Advanced Options**（高度なオプション）］タブをクリックします。［Advanced Options（高度なオプション）］ページの上部に、［Database Backup（データベース バックアップ）］パネルがあります。



d. ［**Enabled**（有効）］チェック ボックスをオンにします。

e. 指定された場所へのバックアップを開始するには、ページ下部にある［**Update**（更新）］ボタンをクリックし、確認ダイアログで［**Yes**（はい）］をクリックします。

アラート メールおよび承認要求メールの構成

Bit9 にはメール サーバーの構成を必要とする機能があります。これは、特定の状況で管理者またはエンドポイント ユーザーにメッセージを送信できるようにするためです。現在、メール サーバーの構成が必要な機能は、次のとおりです。

- **アラート** – Bit9 アラートがトリガーされたときに、E メールで管理者に通知します。アラートの詳細については、「アラートの作成」（611 ページ）を参照してください。
- **承認要求** – 承認要求がクローズされたときに、E メールでユーザーに通知します。承認要求への応答の詳細については、「要求と根拠の解決」（577 ページ）を参照してください。

これらの E メール通知を有効にするには、SMTP (Simple Mail Transport Protocol) サーバーへのアクセス権を Bit9 Security Platform に付与し、通知条件が満たされたときにメッセージを送信できるようにする必要があります。これの設定は、[System Configuration（システム構成）] ページの［Mail（メール）］タブで行います。このタブでは、次のことが可能です。

- 通知用のメール サーバーを指定します。
- 標準メールとセキュア メールのとちらで通知を行うかを選択します。
- 特定のアラートのサブスクライバーに対して、アラート メールの送信を有効または無効にします。
- 必要に応じて、すべてのアラートEメールを受信するグローバル サブスクライバーを指定します。
- 承認要求への応答 E メールの自動配信を有効または無効にします。

表 104 に、これらのオプションのすべてのフィールドを示します。

表 104：メールの構成設定

パネル：フィールド	説明
Alert Settings（アラート設定）：Mail Notification Enabled（メール通知の有効化）	Bit9 アラートがトリガーされたときに Bit9 アラートの E メール サブスクライバーへ E メールを送信するかどうかを指定するチェックボックス。Bit9 コンソールでアラートを綿密に監視している場合、またはアクティビティのテストもしくは監視のために大量のアラートを生成している場合は、このボックスをオフにすることを推奨します。デフォルトで有効化されています。
Alert Settings（アラート設定）：Global Subscriber Enabled（グローバル サブスクライバーの有効化）	E メール アラートのグローバル サブスクライバーを有効にするかどうかを指定するチェックボックス。この設定を有効にし、[Global subscriber（グローバル サブスクライバー）] フィールドにサブスクライバーを入力すると、そのサブスクライバーは、何らかの Bit9 アラートがトリガーされるたびに E メールを受信します。この設定は、必要に応じて有効化または無効化できます。

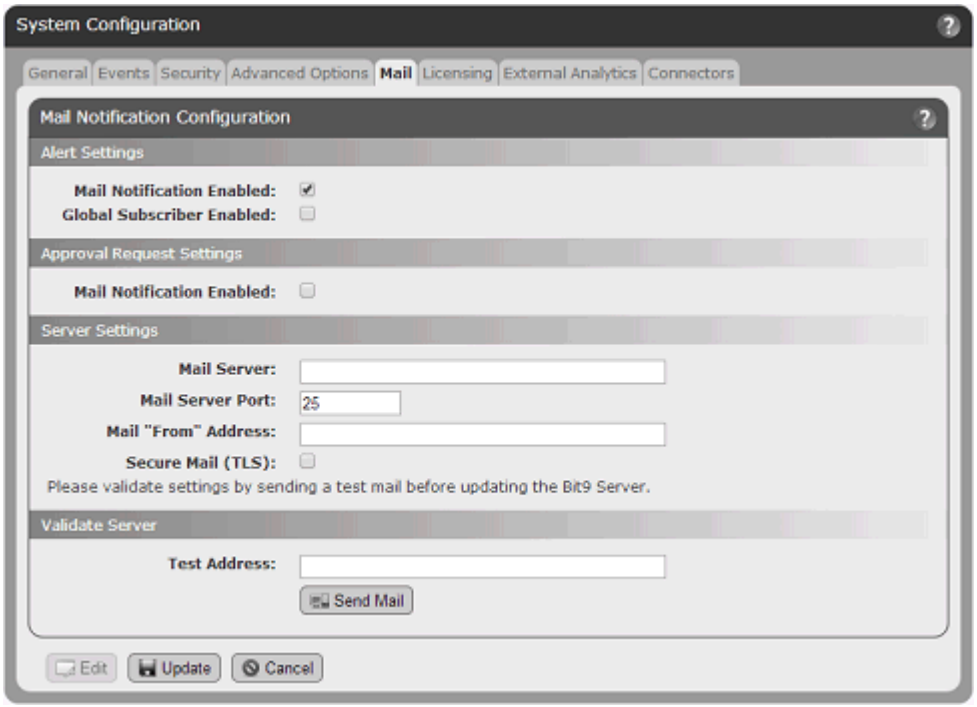
パネル：フィールド	説明
Alert Settings（アラート設定）： Global Subscriber（グローバル サブスクライバー）	グローバル アラート サブスクライバーの E メール アドレス。[Global Subscriber Enabled（グローバル サブスクライバーの有効化）] がオンの場合にのみ表示されます。
Approval Request Settings（承認要求設定）： Mail Notification Enabled（メール通知の有効化）	承認要求を行っているユーザーに対して要求のクローズ時に自動 E メールを送信するかどうかを指定するチェックボックス。デフォルトでは無効化されています。
Server Settings（サーバー設定）： Mail Server（メール サーバー）	メール サーバーのアドレス。IP アドレスを指定することも、完全修飾ドメイン名を指定することもできます。
Server Settings（サーバー設定）： Mail Server Port（メール サーバーのポート）	メール サーバーのポート。使用するサーバーのポートを指定します。標準の SMTP メールではデフォルトで 25 が使用されます。セキュア メールではデフォルトで 587 が使用されます。使用するポートが送信トラフィックで使用可能であることを確認してください。
Server Settings（サーバー設定）： Mail “From” Address（メールの「送信元」アドレス）	通知 E メールで送信元アドレスとして使用するアドレス。 送信元アドレスは、実際に機能する E メール アドレスでなくても問題ありません。ただし、E メール アドレスとして適切な構文でなければなりません（例：info@mycorp.com）。そうしないと、イベント ログにエラーが記録されます。また、メール サーバーによっては、送信元アドレスが適切でない E メールは、スパムとして自動的に破棄される場合があります。
Server Settings（サーバー設定）： Secure Mail (TLS)（セキュア メール（TLS））	通知をセキュア メールで送信するかどうかを指定するチェックボックス。セキュア メールでは、ユーザー名とパスワードを指定して、E メール サーバーとの通信を認証する必要があります。 **注意**：多要素認証が必要なアカウントでセキュア メールを使用することはできません。そのようなアカウントを使用すると、Bit9 通知の送信に失敗します。
Server Settings（サーバー設定）： Secure Mail Username（セキュア メールのユーザー名）	メール サーバーへのアクセス認証に使用するユーザー名。[Secure Mail (TLS)（セキュア メール（TLS））] がオンの場合にのみ表示されます。

パネル：フィールド	説明
Server Settings（サーバー設定）：Secure Mail Password/ Confirm Password（セキュア メールのパスワード / パスワードの確認）	メール サーバーへのアクセス認証に使用するパスワード。両方のフィールドにパスワードを入力する必要があります。[Secure Mail (TLS)（セキュア メール（TLS））] がオンの場合にのみ表示されます。
Validate Server（サーバーの検証）：Test Address（テストアドレス）	E メール サーバー構成のテストに使用する E メール アドレス。たとえば、自身で使用している E メール アドレスを指定して、[**Send Mail**（メールの送信）] ボタンをクリックすると、メール サーバー構成が機能しているかどうかを直ちに確認できます。このテストは、このページの設定を更新する前に行う必要があります。そうすれば、すべての問題を表示して解決することが可能です。

標準 E メールで通知を行うための構成

標準（非セキュア）メールを使用して E メールを構成する手順：

1. コンソール メニューで、[**Administration**（管理）] > [**System Configuration**（システム構成）] の順に選択します。[System Configuration（システム構成）] ページが表示されます。
2. [**Mail**（メール）] タブをクリックします。[Mail Notification Configuration（メール通知構成）] テーブルが表示されます。



3. ［**Edit**（編集）］ボタンをクリックすると、E メール構成フィールドが編集可能になります。有効または無効にしたオプションに応じて、フィールドが追加または削除されます。オプションを有効にすると、そのオプションの必須フィールドのうち、未入力のフィールドが赤で表示されます。
4. デフォルトでは、［Alerts Settings Mail Notification Enabled（アラート設定メール通知の有効化）］ボックスがオンになっています。アラート通知 E メールを送信する場合は、このボックスをオンのままにします。
   注意：グローバル サブスクライバーを有効にするかどうかを決定する前に、「グローバル アラート サブスクライバーの指定」（782 ページ）を参照してください。
5. 承認要求が解決されたときに自動　E　メールを要求者に送信する場合は、［Approval Request Settings（承認要求設定）］パネルの［Mail Notification Enabled（メール通知の有効化）］ボックスをオンにします。
6. ［Server Settings（サーバー設定）］パネルで、メール サーバーのアドレスを完全修飾ドメイン名または IP アドレスで入力します。
7. 標準メールを使用する場合、［Mail Server Port（メール サーバーのポート）］は、デフォルトで 25 に設定されます。別のポートを使用する場合は、フィールドの値を変更します。
8. ［Mail “From” Address（メールの「送信元」アドレス）］を入力します。これは、通知 E メールの送信元として受信者に表示されるアドレスです。
9. セキュア メールで通知を行う場合は、「セキュア E メールで通知を行うための構成」（780 ページ）で説明されている情報を入力します。
10. メール サーバー構成をテストするには、自身でメールを受信できるテスト E メール アドレスを入力して、［**Send Mail**（メールの送信）］ボタンをクリックします。Bit9 コンソールからテスト E メールがそのアドレスに送信されます。
11. ［Validate Server（サーバーの検証）］セクションでメール サーバー構成をテストしてエラーが報告された場合は、問題を解決します。続行するには、［Validate Server（サーバーの検証）］のテストが成功する必要があります。
12. ［**Update**（更新）］ボタンをクリックし、確認ダイアログで［**Yes**（はい）］をクリックします。更新されたメール構成が［Mail Notification Configuration（メール通知構成）］ページに表示されます。

セキュア E メールで通知を行うための構成

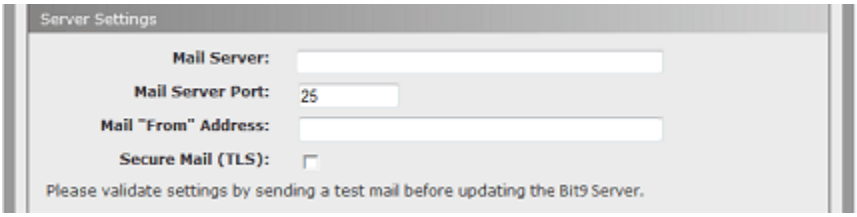
Bit9 Security Platform では、Bit9 通知を送信する際に、標準メールではなく、セキュア メールを使用するオプションを選択できます。セキュア メールでは、メール サーバーにアクセスする際にユーザー名とパスワードを指定する必要があります。セキュア メールでは Transport Layer Security（トランスポート レイヤー セキュリティ）が使用され、メール サーバーへの通信が明示的に保護されます。デフォルトではポート 587 が使用され、**–BEGINTLS** をプレーン テキストで送信することにより通信が開始されます。

重要

多要素認証が必要なアカウントでセキュア メールを使用することはできません。そのようなアカウントを使用すると、Bit9 通知の送信に失敗します。

通知で SMTP/TLS を使用するように Bit9 Security Platform を構成する手順：

1. コンソール メニューで、[**Administration**（管理）] > [**System Configuration**（システム構成）] を選択し、[**Mail**（メール）] タブをクリックします。[Mail Notification Configuration（メール通知構成）] ページが開きます。
2. [**Edit**（編集）] ボタンをクリックし、[Secure Mail (TLS)（セキュア メール (TLS)）] ボックスをオンにします。セキュア メールのオプションが表示されます。



3. [Mail Server（メール サーバー）] と [Mail “From” Address（メール「送信元」アドレス）] を指定します（まだ指定していない場合）。
4. セキュア メールを選択した場合、[Mail Server Port（メール サーバーのポート）] はデフォルトで **587** に設定されます。別のポートを使用する場合は、このフィールドの値を変更します。
5. セキュア メール サーバーでの認証に使用するユーザー名を [Security Mail Username（セキュリティ メール ユーザー名）] フィールドに入力します。

   注意

   - Exchange Server の場合、ユーザー名は、「ドメイン \ ユーザー名」の形式で入力する必要があります。また、[From address（送信元アドレス）] フィールドには、ユーザーの E メール返信先アドレスを入力する必要があります。
   - Gmail の場合、ユーザー名は、Gmail ユーザー名をドメインなしで入力する必要があります。[From address（送信元アドレス）] の値は無視されます。

6. メール サーバーのパスワードを [Secure Email Password（セキュア E メール パスワード）] フィールドに入力し、同じパスワードを [Confirm Password（パスワード確認）] フィールドに再び入力します。

7. ［Validate Server（サーバーの検証）］パネルで［**Test Address**（テスト アドレス）］に値を入力します。次に、［**Send Mail**（メールの送信）］をクリックして、メール サーバーの設定をテストします。構成に問題がない場合は、テスト メールが送信されたことを確認するメッセージが表示されます。指定したアドレスにメールが届いていることを確認します。

8. 指定したとおりに E メールを受信したことを確認したら、［**Update**（更新）］ボタンをクリックして構成を保存します。次に、確認ダイアログで変更を確認し、問題がなければ［**Yes**（はい）］をクリックします。

グローバル アラート サブスクライバーの指定

グローバル アラート サブスクライバーとして指定できるユーザーは 1 人です。そのユーザーには大量のメールが送信される可能性があるため、この機能を有効にする際は、慎重に検討してください。場合によっては、アラート追跡専用の特別なアドレスを使用することも検討してください。グローバル サブスクライバーの有効化は、［System Configuration（システム構成）］ページの［Mail Notification Configuration（メール通知構成）］パネルで行います。

1 人のサブスクライバーがすべてのアラート E メールを受信できるようにする手順：

1. コンソール メニューで、［**Administration**（管理）］>［**System Configuration**（システム構成）］の順に選択します。
2. ［**Mail**（メール）］タブをクリックします。［Mail Notification Configuration（メール通知構成）］ページが表示されます。
3. ［Settings（設定）］パネルで［**Edit**（編集）］をクリックします。
4. ［**Global Subscriber Enabled**（グローバル サブスクライバーの有効化）］ボックスをオンにします。［Global Subscriber（グローバル サブスクライバー）］テキスト ボックスが表示されます。
5. ［Global Subscriber（グローバル サブスクライバー）］テキスト ボックスにサブスクライバーの名前を入力します。
6. ［**Update**（更新）］ボタンをクリックし、確認ダイアログで［**Yes**（はい）］をクリックします。

注意

グローバル サブスクライバーを無効にするには、［Global Subscriber Enabled（グローバル サブスクライバーの有効化）］ボックスをオフにして、［Update（更新）］ボタンをクリックします。

Bit9 Platform ライセンスの管理

［System Configuration（システム構成）］ページの［Licensing（ライセンス）］パネルでは、Bit9 ライセンスの管理や Bit9 Software Reputation Service (SRS) の有効化、無効化、構成が可能です。Bit9 SRS のオプションについては、「Bit9 SRS の有効化」（787 ページ）を参照してください。

Bit9 Security Platform のライセンス付与は、次の 2 つの機能レベルで行えます。

- **可視性** – Bit9 のすべてのファイル追跡機能、イベント追跡機能、レポート機能が有効になりますが、ファイルの禁止やデバイスのブロックなどの制御機能は含まれません。
- **スイート** – 可視性機能と制御機能の両方が有効になります。

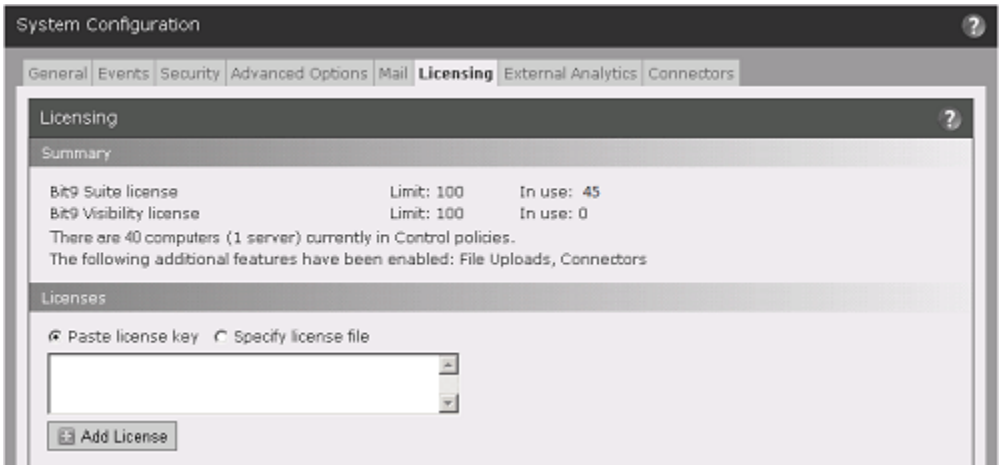
各モードで実行可能なエージェントの数はライセンス キーの数で決定されます。たとえば、可視性ライセンスを 20、スイート ライセンスを 20 のように、同じサーバー上で両方のライセンスを併用することもできます。さらに、いつでも制御アップグレードを購入して可視性ライセンスをスイート レベルまで引き上げることができます。また、オプション機能の中には、ライセンス キーによって制御されるものもあります。

Bit9 ライセンスの上限および使用状況の表示

［System Configuration（システム構成）］の［Licensing（ライセンス）］パネルには、所有している各レベルのライセンスと、使用中の各タイプのライセンス数が表示されます。また、このパネルでは、新しいライセンスを追加することもできます。このパネルには、オプション機能やカスタム機能が有効であることが表示される場合もあります。たとえば、Bit9 Connector にライセンスが付与されている場合は、その旨が表示されます。

Bit9 のライセンス構成ページを表示する手順：

1. コンソール メニューで、［**Administration**（管理）］>［**System Configuration**（システム構成）］の順に選択します。［System Configuration（システム構成）］ページが表示されます。
2. ［**Licensing**（ライセンス）］タブをクリックします。［Licensing（ライセンス）］オプションが表示されます。



［Licensing（ライセンス）］ウィンドウの［Summary（概要）］パネルには、次の情報が表示されます。

- ［**Bit9 Suite license**（Bit9 スイート ライセンス）］– 完全制御モードでの実行が許可されるエージェント数の**上限**と（存在する場合）、**現在使用中**のスイート ライセンスの数が表示されます。
- ［**Bit9 Visibility license**（Bit9 可視性ライセンス）］– 可視性モードでのみ実行が許可されるエージェント数の**上限**と（存在する s 場合）、**現在使用中**の可視性ライセンスの数が表示されます。
- ［**There are x computer(s) currently in Visibility policies**（現在、x 台のコンピューターが可視性ポリシーに含まれています）］および［**There are y computer(s) currently in Control policies**（現在、y 台のコンピューターが制御ポリシーに含まれています）］– 各モードで現在動作しているシステムの数が表示されるだけではなく、それぞれのリストへのアクセスも可能です。各行のハイライト表示された数値をクリックすると、［Computers（コンピューター）］ページが開き、クリックしたカテゴリのコンピューターのみが表示されます。たとえば、上の図で、[40] をクリックすると、制御ポリシーに含まれるコンピューターのリストが表示されます。この行には、この Bit9 Server で管理されているコンピューターのうち、何台がサーバーであるかも表示されます。
- 現在のライセンスにオプション機能が含まれている場合は、それらの機能も［Summary（概要）］パネルに表示されます。

注意

- 各カテゴリで実行可能なエージェント（コンピューター）の数は Bit9 ライセンスによって決まります。ライセンスは特定のエージェントに固定されません。各レベルで実際に稼動しているエージェントの数は、エージェントを制御しているポリシーの［Add/Edit Policy（ポリシーの追加 / 編集）］ページにある［Mode（モード）］設定で制御されます。Bit9 スイートのライセンス数に余裕がある場合は、コンピューターまたはコンピューター グループを可視性モードから制御モードに、またはその逆に移行することが可能です。
- 可視性モード ポリシーに含まれるエージェントに対しては、最初に可視性のみのライセンスが購入済みの数まで使用された後（存在する場合）、必要に応じて Bit9 スイート ライセンスが使用されます。

［Licensing（ライセンス）］ポートレットが表示されている場合、Bit9 Security Platform の管理者は、Bit9 コンソールのホーム ページでライセンス情報を確認することもできます。このポートレットには［**Manage your licenses**（ライセンスの管理）］リンクがあり、このリンクから［Licensing（ライセンス）］構成ページに移動できます。

ライセンスに関する警告

ポリシーを作成または編集する際や、ポリシーにコンピューターを追加する際には、使用している各タイプのライセンスの数を変更できます。制御モードのエージェント数が所有している Bit9 スイート ライセンスの数を超える場合は、コンソールに警告メッセージが表示されます。エージェントの総数がライセンスの総数を超えた場合も警告が表示されます。いずれかの警告が表示された場合は、次のいずれかのアクションを実行します。

- Bit9 営業担当者に連絡して、追加のライセンスを購入します。
- 所有している Bit9 スイート ライセンスの上限数に従い、十分な数のエージェントを制御ポリシーから移動します。これを行うには、いくつかのコンピューターを別のポリシーに移動するか、1 つ以上のポリシーを可視性モードに変更します。
- 所有しているライセンスの上限数に従い、十分な数のエージェントをエージェント無効モードに移行します（また、ライセンスをさらに取得する予定がない場合は、エージェントをアンインストールします）。

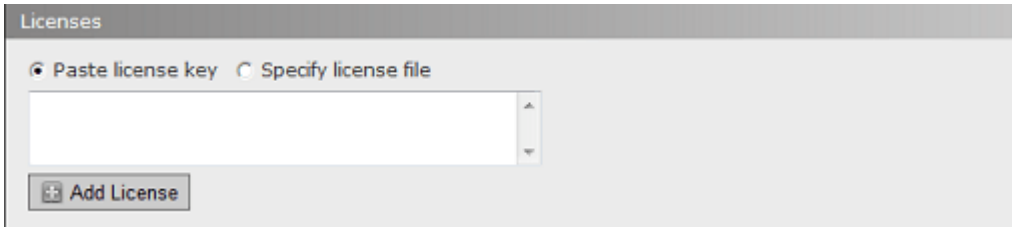
ライセンスの追加

使用できるエージェントの数を増やすためにいずれかのレベルのライセンス キーを新しく取得した場合は、[Licensing（ライセンス）] ページで新しいライセンスを有効にします。新しい Bit9 ライセンスを追加する方法には、次の 2 つがあります。

- 文字列をテキスト ボックスに入力する
- ライセンス キーを含むファイルの場所を指定する

キーを入力して新しい Bit9 ライセンスを追加する手順：

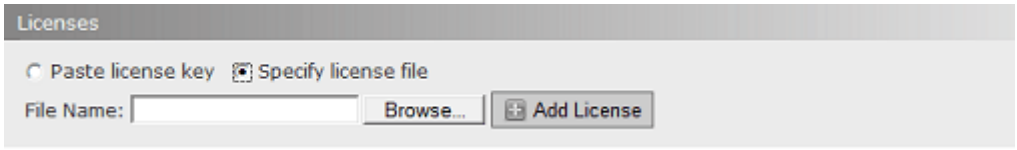
1. コンソール メニューで、[**Administration**（管理）] > [**System Configuration**（システム構成）] の順に選択します。[System Configuration（システム構成）] ページが表示されます。
2. [**Licensing**（ライセンス）] タブをクリックします。[Licensing（ライセンス）] オプションが表示されます。
3. [Licenses（ライセンス）] パネルで、[**Paste license key**（ライセンス キーの貼り付け）] ラジオ ボタンをクリックします。



4. Bit9 から受け取ったライセンス キーをテキスト ボックスに貼り付けるか入力します。
5. [**Add License**（ライセンスの追加）] ボタンをクリックします。

ファイル名を指定して新しい **Bit9** ライセンスを追加する手順：

1. コンソール メニューで、［**Administration**（管理）］>［**System Configuration**（システム構成）］の順に選択します。［System Configuration（システム構成）］ページが表示されます。
2. ［**Licensing**（ライセンス）］タブをクリックします。［Licensing（ライセンス）］オプションが表示されます。
3. ［Licenses（ライセンス）］パネルで、［**Specify license file**（ライセンス ファイルの指定）］ラジオ ボタンをクリックします。



4. ［**Browse**（参照）］ボタンをクリックしてファイル選択ダイアログを開き、ライセンス ファイルを参照して［**Open**（開く）］をクリックします。
5. ［**Add License**（ライセンスの追加）］ボタンをクリックします。

ライセンス追加の確認

ライセンスが正常に追加されると、［Add License（ライセンスの追加）］パネルに次のメッセージが表示されます。「Bit9 License has been successfully added.（Bit9 ライセンスが正常に追加されました。）」

ライセンスが正常に追加されなかった場合は、次のメッセージが表示されます。「Bit9 License has not been added:（Bit9 ライセンスは追加されませんでした。）」。このメッセージとともに、追加に失敗した理由も表示されます。可能な場合は問題を解決し、問題を解決できない場合は、Bit9 サポート担当者にお問い合わせください。

Bit9 SRS の有効化

Bit9 Software Reputation Service (SRS) は、Bit9 Server の価値を高める機能を提供する Web サービスです。Bit9 SRS を有効にすると、次のことが可能になります。

- Software Reputation Service 自体を使用して、既知のファイルに関する大規模なデータベースとコンピューター上で検出されたソフトウェアを比較し、識別、分類することができます。SRS データベース内のファイルには脅威レベルと信頼度が割り当てられています。
- Bit9 からサーバーにリモート アクセスして、診断やトラブルシューティングを行えます。
- 信頼できるアップデーターと高度な脅威の痕跡の更新をクラウドベースで行えます。

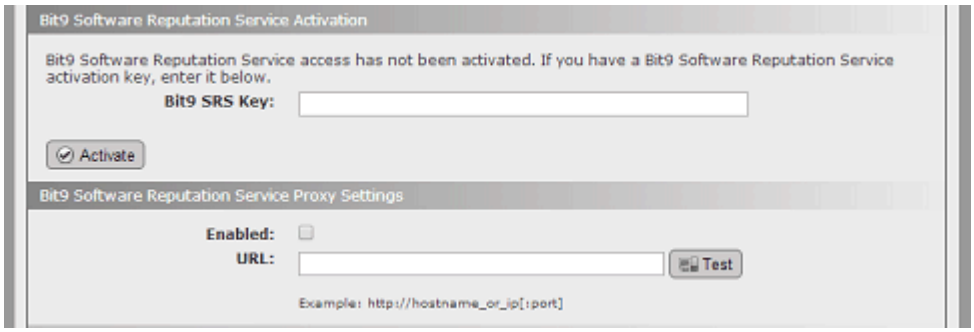
Bit9 SRS を有効にしたときに大部分の機能はデフォルトで有効になっていますが、特定の機能グループを手動で有効または無効にすることもできます。

注意

Bit9 Security Platform のライセンス キーに Bit9 SRS サブスクリプションが含まれていた場合は、[Licensing（ライセンス）] ページに SRS のキーが表示されます。SRS の使用に関する契約条件に同意してサービスを有効にするには、次の手順に従う必要があります。

Bit9 SRS を有効にして構成する手順：

1. コンソール メニューで、[**Administration**（管理）] > [**System Configuration**（システム構成）] の順に選択します。[System Configuration（システム構成）] ページが表示されます。
2. [**Licensing**（ライセンス）] タブをクリックします。[Licensing（ライセンス）] 構成オプションが表示されます。ページ下部に [Bit9 SRS Activation（Bit9 SRS アクティベーション）] パネルと [Bit9 SRS Proxy Settings（Bit9 SRS プロキシ設定）] パネルがあります。

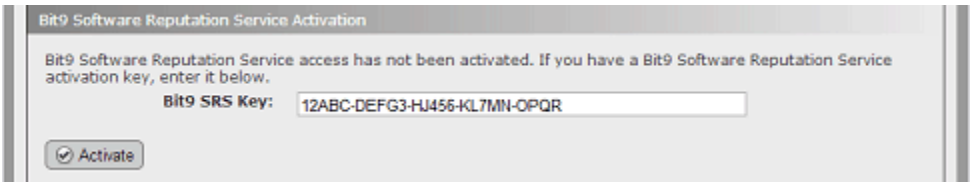


3. Bit9 SRS との通信にプロキシ サーバーを使用する場合は、[Bit9 SRS Proxy Settings（Bit9 SRS プロキシ設定）] パネルに移動して [**Edit**（編集）] をクリックし、次の表の説明に従って設定を構成します。プロキシ サーバーで認証が必要な場合は、「Bit9 SRS 用のプロキシ サーバーの使用」（791 ページ）を参照してください。

表 105：SRS プロキシ設定

フィールド / ボタン	説明
Proxy Settings（プロキシ設定）：Enabled（有効）	オンにした場合は、プロキシ サーバーを使用して Bit9 SRS と通信できるようになります。[URL (URL)] ボックスにその URL を入力する必要があります。
Proxy Settings（プロキシ設定）：URL	Bit9 SRS との通信でプロキシとして使用する URL。ホスト名または IP アドレスを使用できます。また、必要に応じて、ポートの指定を追加することもできます。

4. ［**Update**（更新）］ボタンをクリックし、確認ダイアログで［**Yes**（はい）］をクリックします。
5. ［Bit9 SRS Activation（Bit9 SRS アクティベーション）］ボックスに Bit9 SRS キーがすでに表示されている場合は、次のステップに進みます。
   または
   ［Bit9 SRS key（Bit9 SRS キー）］フィールドが空の場合は、所有しているキーを入力するか、Bit9 サポート担当者に連絡してアクティベーション キーを入手します。



   注意：この手順の残りのステップを実行するには、ブラウザーと Bit9 SRS サイトが接続されている必要があります。
6. Bit9 SRS キーが表示されている場合は、［**Activate**（有効化）］をクリックします。ページの［Activation（アクティベーション）］パネルが更新され、新しいボタンが表示されます。
7. ［**Accept Terms and Activate**（条件を受け入れて有効化）］ボタンをクリックします。［Bit9 SRS Terms and Conditions（Bit9 SRS 使用条件）］ページが新しいブラウザー ウィンドウに表示されます。
8. Bit9 SRS の使用条件を確認します。同意する場合は、条件を読んだことを示すためにボックスをオンにし、［**Submit**（送信）］ボタンをクリックします。これにより、サブスクリプションが有効になり、Bit9 SRS に接続できるようになります。
9. ［Bit9 SRS Activation（Bit9 SRS アクティベーション）］ブラウザー ウィンドウを閉じ、Bit9 コンソールの［System Configuration（システム構成）］に戻ります。
10. ［**Verify Activation**（アクティベーションの確認）］ボタンをクリックし、Bit9 Server と通信できるように Bit9 SRS が正常に構成されたかどうかを確認します。

11. アクティベーションの完了後に表示される［**Options**（オプション）］ボタンをクリックし、特定の Bit9 SRS パラメーターを変更するための Web ページを開きます。次のチェック ボックスがオプションとして表示されます（どのオプションがデフォルトで有効になっているかに注意してください）。

    - ［**Enable file metadata sharing for Reputation and Threat results from Bit9**（ファイル メタデータの共有を有効にして Bit9 からレピュテーションと脅威の結果を取得する）］– 分析のため、エージェントから収集したファイルの（コンテンツではなく）メタデータを Bit9 Software Reputation Service に転送します。このオプションは、デフォルトで有効になっています。Bit9 が提供するレピュテーション サービスにアクセスするには、有効のままにしておく必要があります。
    - ［**Enable remote diagnostic analysis by Bit9 Support**（Bit9 サポートによるリモート診断分析を有効にする）］– 最適なパフォーマンスを得られるように、診断データと環境全体の使用状況に関する情報を Bit9 Server から Bit9 に継続的に転送します。このオプションは、デフォルトで有効になっています。
    - ［**Enable direct file transfer to Bit9 Support for troubleshooting**（トラブルシューティングのためにファイルを直接 Bit9 サポートに転送する）］– Bit9 Server のサポート ディレクトリ内のすべてのファイル（ログ ファイル、エージェント キャッシュ ファイルなど）が Bit9 に送信されます。これらのファイルは、Bit9 環境に関する質問や問題に Bit9 サポートが対処するために役立てられます。このオプションは、デフォルトで無効になっています。
    - ［**Enable automatic updates of Trusted Updaters and Advanced Threat Indicators**（信頼できるアップデーターと高度な脅威の痕跡を自動更新する）］– Bit9 Server 上の信頼できるアップデーターと高度な脅威の痕跡（検出用）がリモートから更新または追加されます。このオプションは、デフォルトで有効になっています。
    - ［**Enable Health Indicators**（正常性の痕跡を有効にする）］– 正常性の痕跡がリモートから配信され、Bit9 環境の正常性を監視および報告できます。また、既存の正常性の痕跡を更新することもできます。このオプションは、デフォルトで有効になっています。この機能の詳細については、第 24 章「システム正常性の監視」を参照してください。
    - ［**Enable VirusTotal Lookup**（VirusTotal ルックアップを有効にする）］– この統合により、まだ SRS に報告されていないマルウェアやアドウェアが環境内のエンドポイントで発見された場合に警告が表示されます。Bit9 Platform Server は新しく見つかったハッシュを SRS で検索してレピュテーション スコアを取得する際、まだ SRS に報告されていないハッシュをキューに入れ、VirusTotal (VT) で非同期検索を行います。VT の検索結果の分析に基づいてマルウェアまたはアドウェアであると判断されたファイルは SRS データベースに取り込まれ、悪意のあるファイル イベントまたは危険な可能性のあるファイル イベントがプラットフォーム サーバーに送信されます。
      注意：SRS が実際のファイルにアクセスすることはなく、VirusTotal で分析を行うためにファイルをアップロードすることはありません。ハッシュの検索のみが行われます。

12. ［Bit9 SRS Options（Bit9 SRS のオプション）］を確認します。処理内容がわからないオプションがある場合は、Bit9 サポートに連絡し、詳細を確認してください。有効または無効にするオプションを確認したら、［**Edit Settings**（設定の編集）］ボタンをクリックし、変更する各オプションの隣にあるボックスをオンまたはオフにします。作業が完了したら、［**Save Settings**（設定を保存）］ボタンをクリックします。

    注意：［Bit9 SRS Options（Bit9 SRS のオプション）］ページにアクセスする際に、Bit9 カスタマー ポータルのログイン認証情報の入力を求められる場合があります。オプションの表示や編集を行うときは、ログイン認証情報を手元に用意しておいてください。

13. ご使用のサーバーの Bit9 SRS 構成の変更履歴を表示するには、［**View Log**（ログの表示）］リンクをクリックします。Bit9 SRS の構成が完了したら、ブラウザー ウィンドウを閉じます。

Bit9 SRS を有効にすると、サーバー上のファイルと Bit9 SRS との同期が開始されます。Bit9 SRS でハッシュを基準に特定のファイルの検索を開始するには、［Files（ファイル）］ページまたは［File Details（ファイルの詳細）］ページで［**Analyze**（分析）］ボタンをクリックします。各ファイルの分析結果は、ブラウザーの新しいタブに表示されます。Internet Explorer で複数のファイルを要求したときは、最初の結果が表示された後、ポップアップ ブロッカーにより、各ファイルの結果がブロックされる場合があります。

Bit9 SRS の可用性ステータス

Bit9 Server では、Bit9 SRS への接続が絶えず検査されています。Bit9 SRS が使用可能でない場合は、サービスが中断した理由を示すエラーが［Licensing（ライセンス）］タブに表示されます。

また、アラートで指定された期間中（デフォルトは 3 時間）に所定の Bit9 SRS タスクが実行されないときは、組み込みの［Bit9 SRS Unavailable Alert（Bit9 SRS 使用不能アラート）］がトリガーされます。このアラートがトリガーされたときに、特定のアラート サブスクライバーへ E メール通知を送信することもできます。

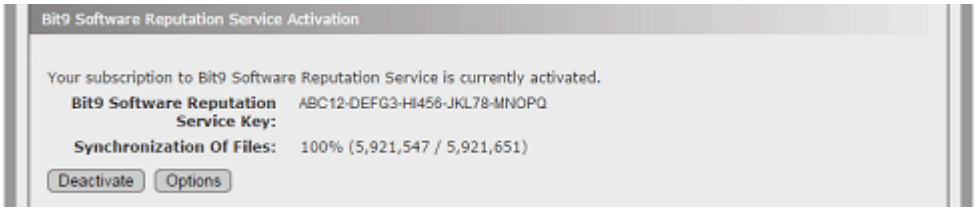
通常、ネットワークに関連する一時的な問題は Bit9 SRS ユーザーに重大な影響が及ぶ前に解決されるため、［Bit9 SRS Unavailable（Bit9 SRS 使用不能アラート）］がトリガーされるまでの時間はデフォルトで 3 時間に設定されています。これにより、不要なアラートが表示される可能性を防止できますが、どのくらいの時間、Bit9 SRS が使用不能であった場合にアラートをトリガーするかの設定は変更できます。アラートが表示される場所など、アラートの詳細については、「Bit9 アラートの使用」（606 ページ）を参照してください。

Bit9 SRS に関連するもう一つの接続は、コンソール ユーザーのブラウザーと Bit9 SRS 間の接続です。この接続は Bit9 SRS を有効にするときに必要となり、Bit9 コンソールのファイルの詳細ページで［Analyze（分析）］を選択したときに発生する Bit9 SRS ファイル評価ページへのリダイレクトでもこの接続が必要になります。ユーザーが［Licensing（ライセンス）］タブに移動すると、Bit9 Server は、そのユーザーが Bit9 SRS サイトにアクセスできるかどうかを検査し、接続に問題がある場合は、次のエラーを表示します。「Bit9 SRS is currently not accessible. Please

check back later.（現在、Bit9 SRS にアクセスできません。後で再度確認してください。）」

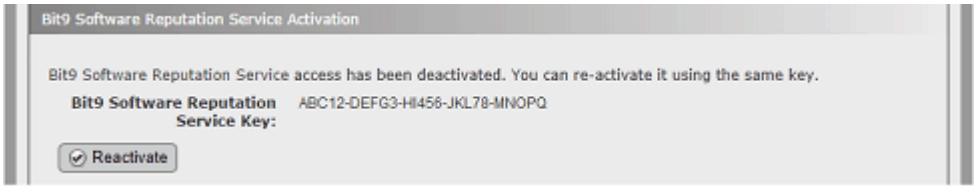
Bit9 SRS の無効化

何らかの理由で Bit9 SRS を無効にする必要がある場合は、[System Configuration（システム構成）] ページの［Licensing（ライセンス）］タブで、アクティベーションに使用したときと同じパネルを使用します。



［**Deactivate**（無効化）］ボタンをクリックするとダイアログが表示され、信頼と脅威に関する情報が提供されなくなることを示す警告が表示されます。このダイアログで無効化を確定します。

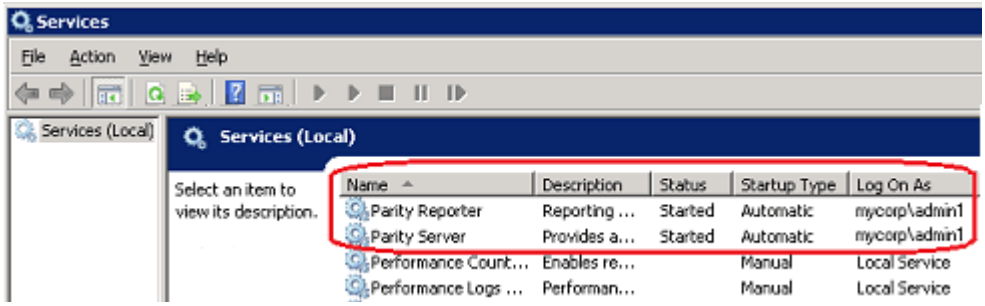
サービスを有効にするときに指定したキーは保存されます。これにより、［**Reactivate**（再有効化）］ボタンをクリックするだけで、Bit9 SRS 接続を再び有効にすることができます。



Bit9 SRS 用のプロキシ サーバーの使用

Bit9 SRS との通信の処理にはプロキシ サーバーを使用できます。認証が不要なプロキシ サーバーを使用する場合は、表示されたフィールドに URL を入力し、プロキシを使用可能にするためのボックスをオンにします。

認証が必要なプロキシ サーバーを使用する場合は、Bit9 Server のインストール時に構成した Bit9 Security Platform サービスのユーザー アカウントに対してプロキシ サーバーへのアクセスを許可する必要があります。このアカウントの名前を確認するには、Windows タスク マネージャーを開き、右下隅の［**Services**（サービス）］ボタンをクリックします。[Bit9 Reporter] の隣にある［Log On As（ログオン名）］フィールドの名前に対して、プロキシ サーバーへのアクセスを許可する必要があります。

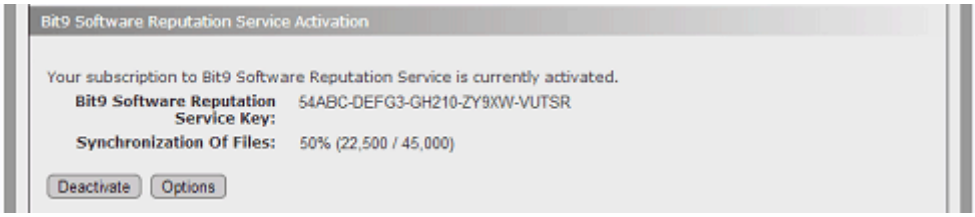


Bit9 SRS の同期

Bit9 SRS を有効にすると、Bit9 Server との間でファイル情報の同期が開始されます。この同期により、Bit9 SRS に登録されている情報と一致するサーバー上のファイルに対して、信頼度と脅威レベルが割り当てられます。 この処理に要する時間は、同期するファイルの数に応じて異なります。

最初の同期後も Bit9 SRS と Bit9 Server は通信を継続します。サーバーで検出された新しいファイルは Bit9 SRS に同期され、信頼度と脅威レベルが変更されるとサーバー上の情報も更新されます。その他のファイル メタデータ（公開者や証明書のデータなど）も更新される場合があります。

［Bit9 SRS Activation（Bit9 SRS アクティベーション）］パネルには、同期のステータスが表示されます。これには、サーバー上で検出された一意のファイルの総数、現在までに同期されたファイルの数と割合、および同期が完了するまでの推定時間が含まれます。 これは最初の同期の際に特に役立ちますが、多数の新しいファイルがサーバー上に出現したときにサーバー上の信頼度情報と脅威情報がすでに同期されているかを追跡する場合にも役立ちます。



注意

データベースに技術的な問題が発生した場合や、Bit9 SRS へのネットワーク接続が中断した場合は、推定時間どおりに同期が完了しない場合があります。同期中にエラーが発生した場合は、通常の動作に戻るまでプロセスが一時的に停止され、エラー メッセージに一時停止の長さが示されます。

Carbon Black サーバー統合の有効化

Bit9 Server と Carbon Black サーバーの両方でエンドポイントを管理している場合は、Carbon Black サーバーに接続するように Bit9 Server を構成し、ファイルおよびCarbon Black ウォッチリスト イベントに関する情報を受信および表示することが可能です。表 106 に、この統合の構成設定を示します。Carbon Black サーバーに関する構成項目は、[System Configuration（システム構成）] ページの [Licensing（ライセンス）] タブにあります。

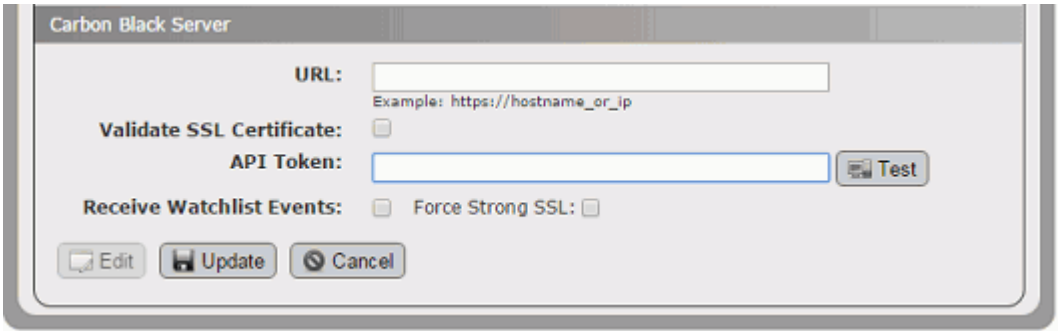


表 106：Carbon Black との統合に関する構成設定

フィールド / ボタン	説明
URL	Bit9 Server にリンクする Carbon Black サーバーの URL。必要に応じて、ポートも指定できます。
Validate SSL Certificate（SSL 証明書の検証）	このボックスをオンにすると、Carbon Black サーバーの証明書の有効性チェックが行われます。このチェック ボックスをオンにする必要があるのは、Carbon Black サーバーの証明書が署名されていない場合のみです。
API Token（API トークン）	Bit9統合に使用するCarbon Blackサーバー ユーザーのAPIトークンをここに入力します。[**Test**（テスト）] ボタンをクリックして、サーバーにアクセスできること、およびキーが動作することを確認します。テスト結果として次のいずれかの値が返されます。 • **Success, version:（成功、バージョン：）**<Carbon Black 製品のバージョン > • **Invalid API Token（API トークンが無効です）** • **Server not accessible（サーバーにアクセスできません）** **重要**：このフィールドの詳細については、「統合用の Carbon Black ユーザーの作成」を参照してください。

フィールド / ボタン	説明
Receive Watchlist Events（ウォッチリスト イベントの受信）	このボックスをオンにすると、構成されたサーバーから Bit9 Server に Carbon Black ウォッチ リスト イベントが配信されます。
Force Strong SSL（強力な SSL の強制）	このボックスをオンにすると、Carbon Black サーバーはイベントを送信する前に Bit9 Server の証明書を確認します。IIS 上にある Bit9 の自己署名証明書がサーバーで使用されている場合は、このボックスをオンにしないでください。

重要

これらの設定項目は、Carbon Black コンソールにも表示されます。Carbon Black コンソールにある Bit9 Platform との統合に関する設定は編集可能ですが、そこで行った変更は適用されません。Bit9 と Carbon Black の統合に関する設定を編集する場合は、必ず Bit9 コンソールを使用してください。

統合用の Carbon Black ユーザーの作成

Carbon Black と Bit9 Platform 間の統合を構成するときに入力できる API トークンは 1 つのみです。そのため、これを目的とした新しい Carbon Black ユーザーを作成し、そのユーザーの API トークンを使用する必要があります。その Carbon Black ユーザーは、Administrators グループに含まれている必要があり、なおかつグローバル管理者でなければなりません。基本的な手順の概要を次に示します。

Carbon Black と Bit9 の統合に使用するユーザーおよび API トークンを作成する手順（概要）:

1. 他の管理ユーザーを作成できるユーザーとして Carbon Black サーバーにログインします。
2. Carbon Black コンソールで、[**Administration**（管理）] > [**Users**（ユーザー）] の順に選択した後、[**Add User**（ユーザーの追加）] をクリックし、Bit9 との統合に使用する新しいユーザーを作成します。このユーザーを Administrators チームに割り当てるとともに、[Global administrator（グローバル管理者）] ボックスをオンにしてください。
3. ログアウトし、作成した新規ユーザーとして Carbon Black コンソールに再ログインします。
4. Carbon Black コンソールのメニューで、***username*** > [**My Profile**（マイ プロファイル）] の順に選択します。

5. ［My Account（マイ アカウント）］ページの左側のメニューで［**API Token**（API トークン）］を選択し、［**Your API Token**（自分の API トークン）］ボックスの文字列をコピーします。この文字列を使用して、Bit9 Platform コンソールの［System Configuration（システム構成）］ページにある［Licensing（ライセンス）］タブで Carbon Black との統合を構成します。

詳細な手順については、『Carbon Black ユーザー ガイド』の「Carbon Black と Bit9 Server の統合」を参照してください。

第 24 章

システム正常性の監視

この章では、[System Health（システム正常性）] ページについて説明します。Bit9 管理者は、[System Health（システム正常性）] ページを使用して、Bit9 Server の正常性とパフォーマンスを監視できます。

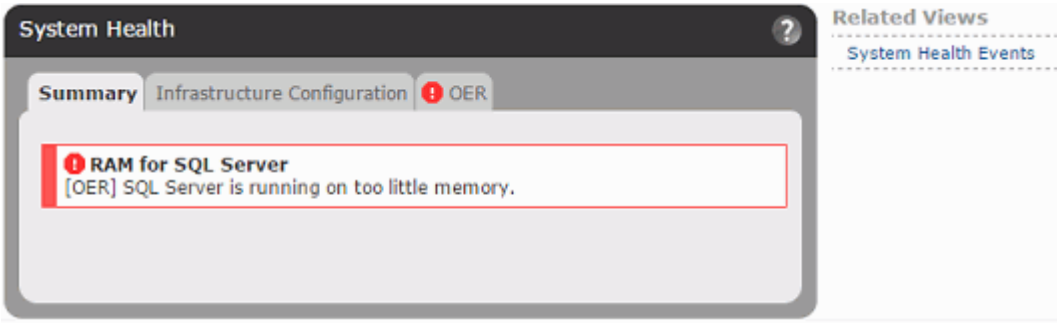
セクション

概要

Bit9 管理者は、[System Health（システム正常性）] ページを使用して、Bit9 Server のパフォーマンスに影響を与える要素を監視できます。このページでは、[Health Indicators（正常性の痕跡）] の出力が表示され、Bit9 Server、SQL Server、または環境全体に関する問題を発見するのに役立ちます。

たとえば、サーバーで管理されているルールやエンドポイントの数が Bit9 運用環境の要件のガイドラインに準拠していない場合があります。この状況は、Bit9 エージェントがインストールされたエンドポイントを環境に追加した場合などに発生します。システム正常性が低下するもう一つの原因として、ハードウェア環境の変更（ディスク容量や RAM の変更など）があります。

[System Health（システム正常性）] ページでは、問題が深刻になる前にこのような傾向を確認できます。これにより、自分自身でその状況に対処したり、Bit9 サポートに連絡して支援を受けることができます。また、監視されているすべての要素が正常かどうかがわかる点も便利です。



[System Health（システム正常性）] ページには、さまざまなタブ ビューが含まれ、各種の正常性の痕跡による分析結果が表示されます。最初のタブには、全体的な正常性の概要が表示されます。トリガーされた正常性の痕跡がある場合は、それに関する簡潔な概要も表示されます。その他のタブには、関連する 1 つ以上の痕跡が含まれます。各タブの情報は、グラフ形式、表形式、テキスト形式、またはこれらを組み合わせた形式で表示できます。

正常性の痕跡では、深刻な状態や境界状態に関するフィードバックが次のような方法で提供されます。

- [**System Health**（システム正常性）] **ページでトリガーされた痕跡** – 正常性に影響する問題がサーバーに存在していることがいずれかの痕跡によって検出されると、上図のように [System Health（システム正常性）] ページに赤色のアイコンとハイライト枠が表示されます。黄色のアイコンとハイライト枠がいずれかの痕跡で表示されている場合、そこで報告されている要素は境界状態にありますが、深刻な状態ではありません。
- **アラート** – [System Health（システム正常性）] ページの各タブには、アラートが組み込まれており、システムが Bit9 Platform 運用環境の要件やその他の必要な構成に準拠していない場合は警告が表示されます。また、これらのタブでは、正常性の痕跡の深刻度レベルが変化したときにトリガーされるアラートの作成も可能です。
- **イベント** – 正常性の痕跡の深刻度レベルが変化するとイベントがサーバーに記録され、Syslog 出力を通じて確認することができます。

［System Health（システム正常性）］ページに表示される正常性の痕跡は、Carbon Black 脅威インテリジェンスを通じて Bit9 Server に提供されます（Carbon Black 脅威インテリジェンスは、以前は Bit9 Software Reputation Service (SRS) と呼ばれ、今回のリリースの Bit9 コンソールでは引き続き従来の名称が使用されています）。このクラウド サービスを使用すると、［System Health（システム正常性）］ページを有効にするために必要な一連の痕跡を最初にダウンロードできるだけでなく、既存の痕跡の変化や、システム正常性のビューに追加された新しい痕跡を反映して、サーバーを常に最新の状態に保つことができます。［System Health（システム正常性）］の痕跡が機能するためには、Bit9 SRS がサーバーに接続されている必要があります。

システム正常性の痕跡の有効化

システム正常性の痕跡は、Carbon Black 脅威インテリジェンス (Bit9 SRS) によって提供されます。クラウドから正常性の痕跡を最初にダウンロードするときは、SRS を有効にする必要があります。SRS は、必要に応じて既存の痕跡を更新したり、新しく作成された痕跡を追加したりするために使用されます。

また、Bit9 Server で Bit9 SRS を有効にするだけではなく、［System Configuraiton（システム構成）］ページの［Advanced Options（高度なオプション）］タブで、正常性の痕跡の「更新」設定を有効にする必要もあります。この切り替えにより、正常性の痕跡の最初のダウンロードと以後の更新の両方が可能になります。

Bit9 Server でシステム正常性の痕跡を有効にする手順：

1. コンソール メニューで、［**Administration**（管理）］>［**System Configuration**（システム構成）］の順に選択し、［**Licensing**（ライセンス）］タブをクリックします。
2. ［Licensing（ライセンス）］タブの［Bit9 Software Reputation Service Activation（Bit9 Software Reputation Service のアクティベーション）］パネルに SRS が有効化されていることが表示されているかどうかを確認します。有効になっていない場合は、「Bit9 SRS の有効化」（787 ページ）のアクティベーション手順に従ってください。
3. Bit9 SRS が有効になったら、［System Configuration（システム構成）］ページの［**Advanced Options**（高度なオプション）］タブをクリックし、ページ下部にある［**Edit**（編集）］ボタンをクリックします。
4. ［Software Rule Options（ソフトウェア ルールのオプション）］パネルで、［**Health Indicators**（正常性の痕跡）］ボックスをオンにします。ページを保存すると、正常性の痕跡が Bit9 SRS から自動的にダウンロードされ、必要に応じて更新されます。
5. ページ下部の［**Update**（更新）］ボタンをクリックします。正常性の痕跡のダウンロードがスケジュールされ、しばらくすると開始されます。この機能を有効にすると表示される項目の説明については、「［System Health（システム正常性）］ページの表示」を参照してください。

システム正常性の痕跡を有効にすると、Bit9 SRS からサーバーへの痕跡のダウンロードが開始されます。接続速度や他のサーバー アクティビティにもよっては、この処理に 1 ～ 2 時間かかる場合があります。

システム正常性の痕跡の無効化

正常性の痕跡の更新を無効にする必要がある場合は、[System Configuration（システム構成）] ページの［Advanced Options（高度なオプション）］タブに移動して、［**Edit**（編集）］ボタンをクリックします。次に、［**Health Indicators**（正常性の痕跡）］ボックスをオフにして、［**Update**（更新）］ボタンをクリックします。痕跡を無効にした後に［System Health（システム正常性）］ページに移動すると、その機能が無効になっていることを示すメッセージが表示されます。

［System Health（システム正常性）］ページの表示

このページを表示するには、［View system health indicators（システム正常性の痕跡の表示）］権限を備えたログイン アカウントが必要です。Administrators グループのアカウントは、デフォルトでこの権限を備えています。別のユーザーがこのページにアクセスできるように構成する必要がある場合は、「コンソール アカウント グループの管理」（104 ページ）を参照してください。

注意

ここに示す［System Health（システム正常性）］ページの図は、本書が発行された時点では正確な内容となっています。ただし、正常性の痕跡は Bit9 クラウドから提供および更新されるため、ご使用のバージョンの Bit9 コンソールでは、タブ上の痕跡とその外観や内容が異なる場合があります。

［System Health（システム正常性）］ページを表示する手順：

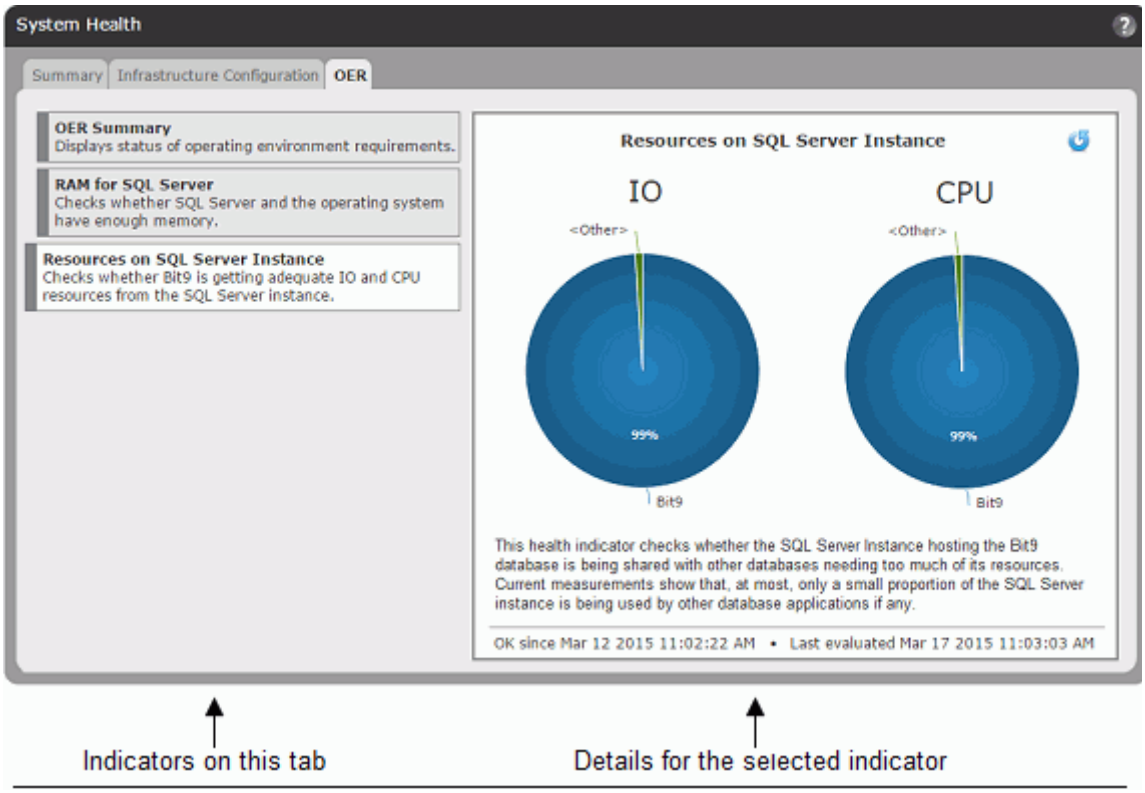
- コンソール メニューで、［**Administration**（管理）］>［**System Health**（システム正常性）］の順に選択します。

痕跡の最初のダウンロードが未完了の場合は、［System Health（システム正常性）］ページに［Summary（概要）］タブのみが表示され、ダウンロード中であることを示すメッセージが表示されます。

ダウンロードが完了すると、使用可能な正常性のビューごとにタブが表示されます。最初のタブには全体的な正常性の概要が表示されます。トリガーされた正常性の痕跡がある場合、また正常性の痕跡の正しい動作を妨げる条件がある場合は、それらも表示されます。トリガーされた痕跡がない場合も、［Summary（概要）］

タブには、その旨が表示されます。

その他のタブには、各種の正常性の痕跡による分析結果が表示されます。表示されるタブは、SRS を通じて新しい痕跡が使用可能になるにつれて変化します。



［System Health（システム正常性）］タブ ビューには、上の例のように複数の痕跡が表示される場合があります。痕跡はページの左側に表示され、タブの右側には選択した痕跡の詳細が表示されます。選択した痕跡は、左側にずれた状態で表示されます。

［System Health（システム正常性）］ページに痕跡が表示されない状況を次にいくつか示します。

- Bit9 Software Reputation Service (SRS) が無効であるために正常性の痕跡が使用不可である。
- ［System Health（システム正常性）］機能が無効である。

- SRS からの正常性の痕跡のダウンロードがまだ進行中である。

注意

ご使用の環境に関係がないと Bit9 Server で判断された痕跡は表示されません。また、タブ上のどの痕跡もご使用の環境に関係がないと判断された場合は、そのタブ自体が表示されません。環境が変更されると、痕跡、またはタブ全体が［System Health（システム正常性）］ページに表示されなくなる場合があります。

［System Health（システム正常性）］ページ上での移動

［System Health（システム正常性）］ページでビューを変更したり、ドリルダウンで追加情報を確認したりする方法は、いくつかあります。

- **タブ ビューを変更する**–いずれかのタブをクリックすると、表示されている一連の痕跡が変更されます。
- **タブに表示されている痕跡を変更する**– 1つのタブに複数の痕跡が表示されている場合、左側にある他のいずれかの痕跡をクリックすると、右側に表示される詳細が変更されます。
- **詳細に含まれているリンク** – 痕跡の詳細によっては、追加情報へのリンクが含まれている場合があります。たとえば、［OER Summary（OER の概要）］詳細ビューには、Bit9 カスタマー ポータル上にある、Bit9 Platform 運用環境の要件に関する最新ドキュメントへのリンクが含まれています。このリンクに移動するには、ポータル ログインが必要です。
- **痕跡の詳細を再ロードする** – 最新の情報を確実に表示するには、痕跡の詳細ビューの右上隅にある再ロード ボタンをクリックします。 大部分の痕跡は、24 時間ごとに再評価されます。［OER Summary（OER の概要）］痕跡は、15 分ごとに再評価されます。
- **システム正常性イベント** –［System Health（システム正常性）］ページの［Related Views（関連ビュー）］メニューには、［Events（イベント）］ページへのリンクが含まれています。このページは、正常性の痕跡に関連するイベントのみを表示するようにフィルタリングされた状態で表示されます。これらのイベントの詳細については、「システム正常性イベント」（804 ページ）を参照してください。

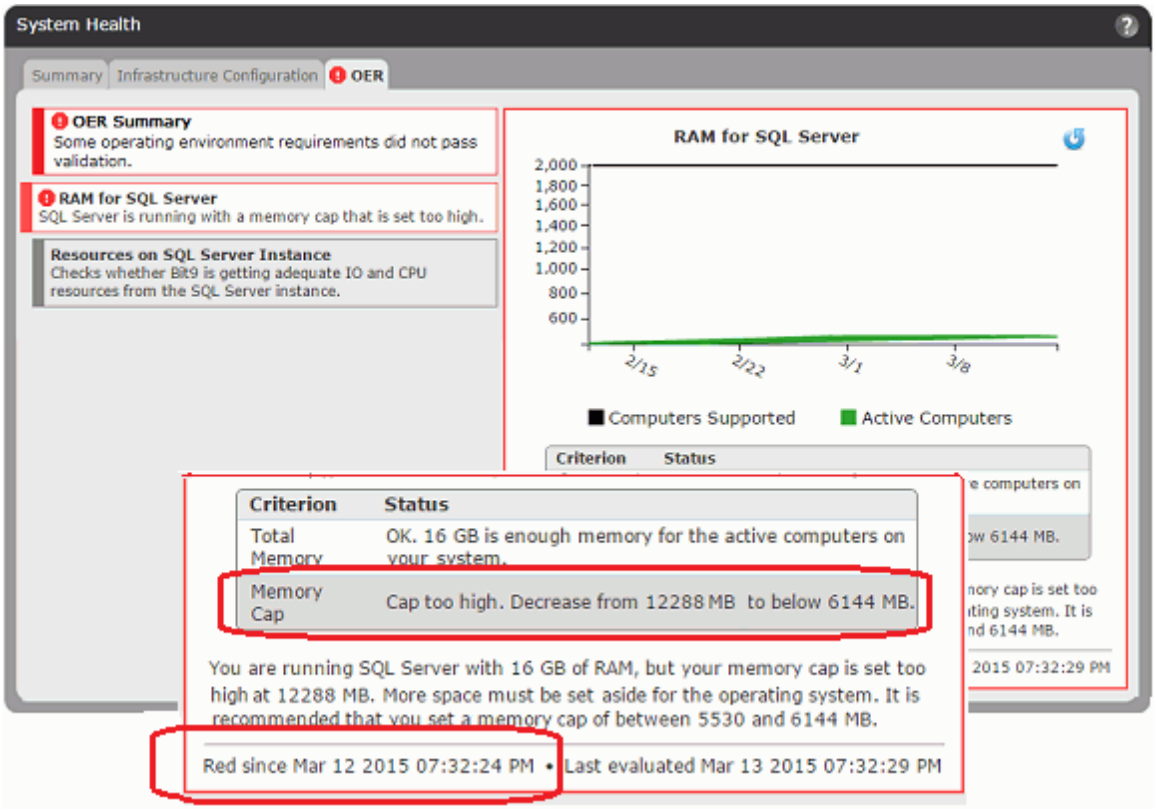
正常性の痕跡の状態

正常性の痕跡は、監視対象のパラメーターまたはリソースの状態を示すために色分けされます。それぞれの色とその状態を次に示します。

- **灰色** – 痕跡が灰色の場合、監視されている状況は正常で（通知のみを目的としており、正常性の評価はありません）、アクションは不要です。
- **黄色** – 痕跡が黄色の場合、監視されている状況は境界状態で、追跡調査と必要に応じてアクションが必要です。
- **赤色** – 痕跡が赤色の場合、監視されている状況は深刻な状態で、アクションが必要です。

正常な状態よりも低い状態を示している痕跡は「トリガーされた」ものと見なされます。痕跡がトリガーされると、その状態が複数の場所、たとえば、［Summary（概要）］タブ ビューの痕跡のリスト、タブ自体の痕跡のリスト、その痕跡が表示

されているビューの痕跡のリストなどに表示されます。タブ ビューの詳細セクションには、問題の説明とその問題が存続している時間が表示されます。また、問題について警告するためにアラートがトリガーされます。



システム正常性アラート

アラートにより、システム正常性の問題を通知できます。これらの通知は、Bit9 コンソールに表示され、（有効になっている場合は）サブスクライバーに E メールで送信されます。アラートの詳細については、「Bit9 アラートの使用」（606 ページ）を参照してください。システム正常性の問題は次のアラートによって通知されます。

- **System Health OER Alert**（システム正常性 OER アラート）– この組み込みアラートには、コンソール アラートが表示されます。Bit9 Platform 運用環境の要件で定められている特定の仕様にサーバーの環境が準拠していない場合は、サブスクライバーに E メールが送信されます。このアラートは常に有効になっていますが、[Health Indicators（正常性の痕跡）] が有効でない場合はトリガーされません。
- **System Health Infrastructure Configuration Alert**（システム正常性インフラストラクチャ構成アラート）– この組み込みアラートには、コンソール アラートが表示されます。[System Health（システム正常性）] ページの [Infrastructure Configuration（インフラストラクチャ構成）] タブで報告されるいずれかの要素が要件に準拠していない場合は、サブスクライバーに E メールが送信され

ます。このアラートは常に有効になっていますが、[Health Indicators（正常性の痕跡）] が有効でない場合はトリガーされません。

注意

システム正常性アラートは、[System Configuration（システム構成）] ページの［Advanced（高度）］タブでシステム正常性の痕跡が有効化され、関連する痕跡がサーバーにダウンロードされている場合にのみ表示およびトリガーできます。痕跡が存在する場合、常に有効です。

システム正常性イベント

Bit9 Server では、正常性の痕跡に関連するさまざまなイベントが記録されます。Bit9 コンソールでこれらのイベントを表示したり、これらのイベントに応答する SIEM のルールを設定したりできます。また、これらのイベントに基づいて、Bit9 アラートやイベント ルールをトリガーすることもできます。痕跡自体の変更を通知するイベント サブタイプとして、[Health indicator created（正常性の痕跡の作成）]、[Health indicator changed（正常性の痕跡の変更）]、および［Health indicator deleted（正常性の痕跡の削除）］があります。

多くの場合、システム正常性を監視するときに最も重要になるイベントは、[Health indicator severity change（正常性の痕跡の深刻度の変化）] サブタイプです。深刻度が比較的低い状態から比較的高い状態に変化したことを示すイベントが発生した場合は、Bit9 環境の特定の要素に注意が必要です。これに対して、深刻度が低下した場合は、行った修復が成功したことを示しています。深刻度が上昇すると、深刻度が［Warning（警告）］に設定されたイベントがトリガーされます。深刻度が低下すると、深刻度が［Info（通知）］に設定されたイベントがトリガーされます。

深刻度変更イベントの［Description（説明）］フィールドには、そのイベントがトリガーされた理由の詳細が表示されます。また、新規作成された痕跡の状態の説明も表示されます。表 107 は、[Health indicator severity change（正常性の痕跡の深刻度の変化）] イベントがトリガーされる条件を示しています。

表 107：[Health Indicator Severity Change（正常性の痕跡の深刻度の変化）] イベントの条件

条件	説明
痕跡の状態が正常でなくなった	正常性の痕跡 <name> が深刻度 <severity level> に変化しました。詳細については、正常性の痕跡を確認してください。
深刻度が上昇して黄色から赤色に変化した	正常性の痕跡 <name> の深刻度が <old severity> から <new severity> に上昇しました。詳細については、正常性の痕跡を確認してください。
深刻度が低下して黄色に変化した	正常性の痕跡 <name> の深刻度が <old severity> から <new severity> に低下しました。
トリガーされた痕跡が正常になった	正常性の痕跡 <name> が正常に戻りました。
新しい痕跡の状態が異常である	新規に作成された正常性の痕跡 <name> の深刻度が <severity level> です。詳細については、正常性の痕跡を確認してください。
新しい痕跡の状態が正常である	新規に作成された正常性の痕跡 <name> は正常です。

Bit9 コンソールで正常性の痕跡イベントを表示する手順：

1. コンソールの [Events（イベント）] ページで、[**Reports**（レポート）] > [**Events**（イベント）] の順に選択します。
2. [Saved View（保存済みビュー）] メニューで、[**System Health History**（システム正常性履歴）] を選択します。
3. 必要に応じて、テーブル ビューのその他のパラメーター（[Max Age（最長期間）] など）を調整します。

付 録 A

ライブ インベントリ SDK：データベース ビュー

Bit9 Security Platform には、コンソールのユーザー インターフェイスを通じてファイルとコンピューターのライブ インベントリにアクセスする機能だけでなく、データベース内の情報を外部から参照するためのパブリック ビューも用意されています。これらのパブリック ビューを使用することにより、独自のレポート作成ソリューションやデータ分析ソリューションを作成することが可能になります。この付録では、これらの読み取り専用データベース ビューについて説明します。

外部データベース ビューを使用して独自のレポートを作成すると、ファイルやコンピューターのインベントリ データを使って複雑な分析を行えます。また、この SDK には次のような利点もあります。

- Bit9 コンソールでは利用できない特別なフィルターの組み合わせやファイルのグループ化が可能です。
- コンソールのユーザー インターフェイスを介さずデータベースに直接アクセスするため、クエリを高速で実行できます。
- 特定のスケジュールに従ってレポートを実行したり、サードパーティ ツールと統合するためのデータをレポートとして出力することができます。

注意

Bit9 Platform には Bit9 API と呼ばれる RESTful API も含まれ、この API を使用することにより、カスタム スクリプトや他のアプリケーションを通じて Bit9 Platform とやりとりするコードを作成できます。詳細については、付録 B「Bit9 API」を参照してください。

パフォーマンスの考慮事項

外部ビューはデータベースに対して読み取り専用アクセスを行い、Bit9 Server の他のタスクに影響しないように最適化されています。データベース サーバーは共有リソースですが、外部ビューから過剰にクエリを実行すると Bit9 Server 全体のパフォーマンスに影響に及ぼす可能性があります。次の一般的注意事項を守ってください。

- 完了までに 2 分以上かかるクエリは実行しないようにしてください。
- 外部データベースのクエリ所要時間が合計時間の5%を超えないようにしてください（1 時間あたり数分程度を目安としてください）。
- できる限り、Bit9 エージェントで大量のタスクが処理されている時間帯（特にエージェントの初期化が行われている時間帯）を避けてクエリを実行するようにしてください。

パフォーマンスの問題に関してサポートが必要な場合は、Bit9 テクニカル サポートまでご連絡ください。

旧バージョンからのアップグレード

以前のリリースでこれらのデータベース ビューを使用していた場合は、このリリースでの変更に合わせてクエリの修正が必要になることがあります。以下にある各ビューの表では、Bit9 (Parity) 6.0.2 以降の変更が次のように示されています。

- **追加**されたフィールドに関しては、**7.0.0** で新しく追加されたフィールド名の前に黒い三角形 (▲) を記し、**7.0.1** で新しく追加されたフィールド名の前に黒いひし形 (♦) を記し、**7.2.0** で新しく追加されたフィールド名の前に黒い星 (★) を記しています。ただし、同じバージョンで追加されたフィールドであっても、最初に導入されたビルドやパッチが異なる場合もあります。
- **変更**されたフィールド（フィールド名および値）に関しては、**7.0.0** で変更されたフィールド名の前に白抜きの三角形 (Δ) を記し、**7.0.1** で変更されたフィールド名の前に白抜きのひし形 (◊) を記しています。変更の内容は、コメント欄の「変更に関する注意」で説明されています。ただし、同じバージョンで変更されたフィールドであっても、最初に変更されたビルドやパッチが異なる場合もあります。
- **削除**されたフィールドに関しては、各表の前で述べられています。

Bit9 v7.2.3 では Mac、Linux、および Windows コンピューター上のエージェントがサポートされているため、パスに関連するすべてのフィールドで各オペレーティング システムに固有の構文（区切り文字など）が使用されます。

また、v6.0.2 以前のバージョンからアップグレードする場合は、次のようにグローバルな用語変更が行われるため、それに応じて SDK の値も大幅に変更されます。

表 108： 6.0.2 以降のリリースでのグローバルな用語変更

カテゴリ	6.0.2 での用語	7.2.3 での用語
ファイルの状態	Pending（保留中）	Unapproved（未承認）
	Approved (Custom)（承認（カスタム））	Approved by Policy（ポリシーにより承認）
	Banned (Custom)（禁止（カスタム））	Banned by Policy（ポリシーにより禁止）
コンピューターの保護レベル	SecCon	Enforcement Level（適用レベル）
適用レベルの値	20-Lockdown（20- ロックダウン）	High (Block Unapproved)（高（未承認をブロック））
	30-Block-and-Ask（30- ブロックして確認）	Medium (Prompt Unapproved)（中（未承認に対してプロンプトを表示））
	40-Monitor（40- 監視）	Low (Monitor Unapproved)（低（未承認を監視））
	60-Visibility Only（60- 可視性のみ）	None (Visibility)（なし（可視性））
	80-Agent Disabled（80- エージェント無効）	None (Disabled)（なし（無効））

スキーマの概要：bit9_public

外部ビューは Bit9 Server ライブ インベントリの非正規化ビューです。これらのビューはデータ キューブを使用したレポート作成や分析に適しています。公開されている各ビュー名の先頭には「external（外部）」を意味する「Ex」が付き、**Das** データベース内の **bit9_public** スキーマに含まれています。

スキーマ ユーザーの指定

bit9_public スキーマへのアクセス権を付与するユーザーのログイン名を指定する必要があります。（Bit9 Server をインストールした後に）このログイン名を追加して手動でログインするには、次のスクリプトを使用します。*Domain* および *bit9user* の部分を、該当する Windows ユーザーの値に置き換えて使用してください。

```
CREATE LOGIN [Domain\bit9user] FROM WINDOWS WITH
DEFAULT_DATABASE=[Das]
GO
CREATE USER [Domain\bit9user] FOR LOGIN [Domain\bit9user]
GO
USE [Das]
GO
GRANT SELECT ON SCHEMA :: dbo TO [Domain\bit9user]
GO
GRANT EXECUTE ON SCHEMA :: dbo TO [Domain\bit9user]
GO
ALTER AUTHORIZATION ON SCHEMA::bit9_public TO
[Domain\bit9user]
GO
```

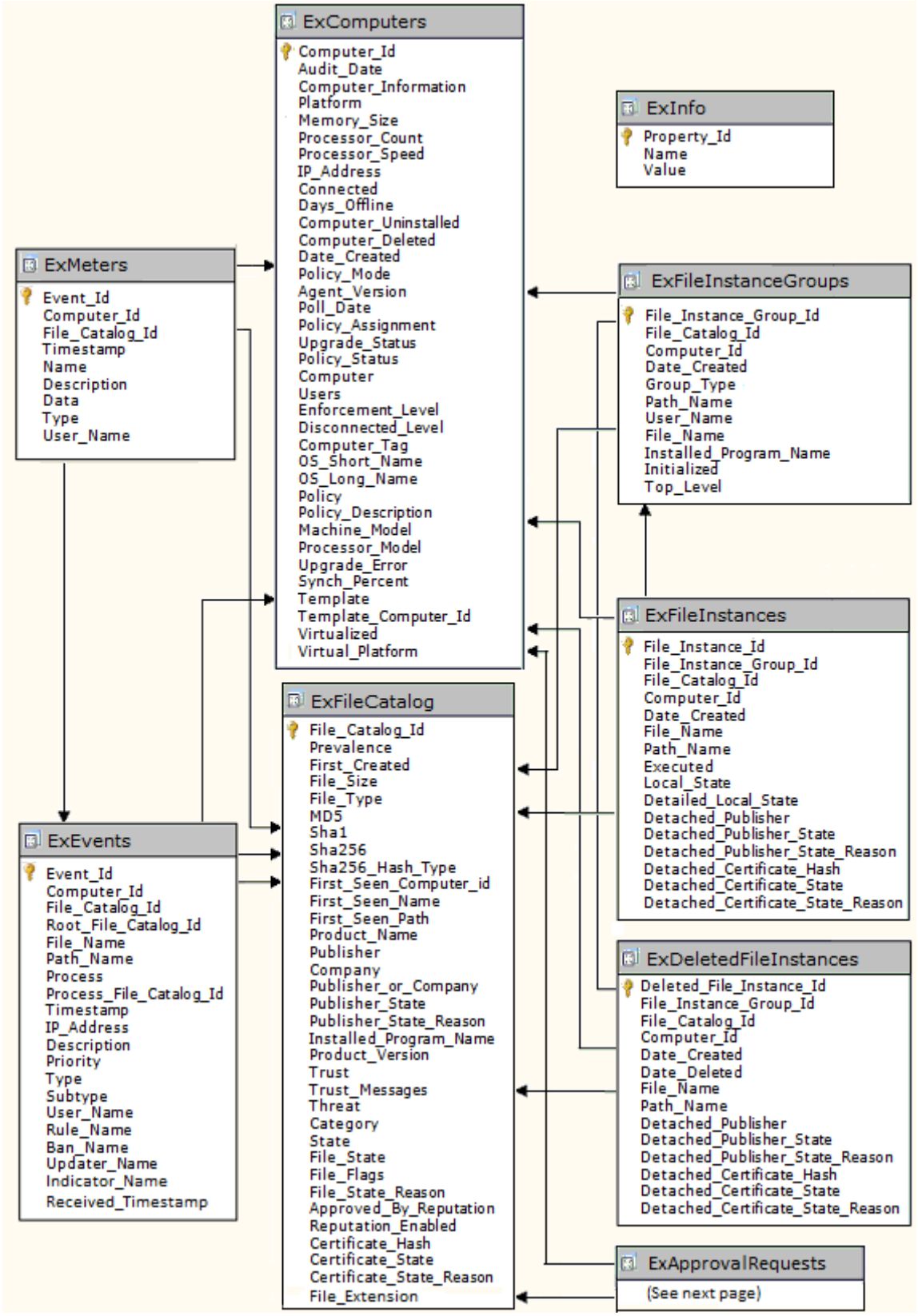
スキーマ ビューとダイアグラム

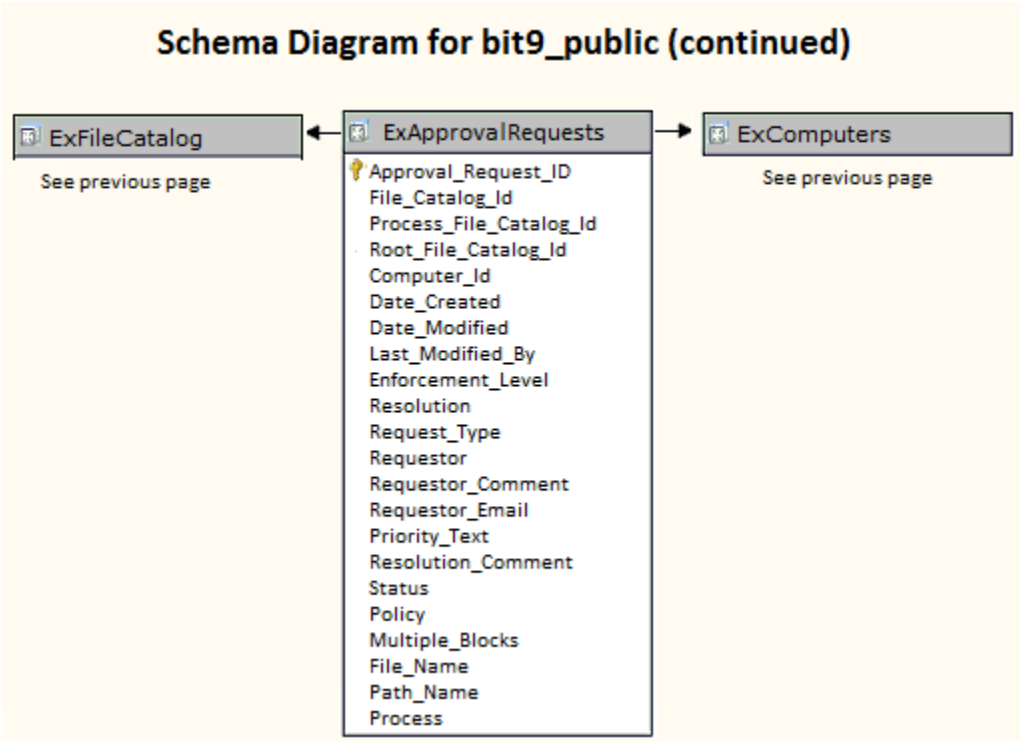
表 109 に、このスキーマで使用できるビューを示します。各ビュー内のデータの詳細については、このトピックの後半にあるテーブルを参照してください。bit9_public の完全なスキーマ ダイアグラムは、次の表のすぐ後に掲載されています。

表 109：bit9_public のスキーマ ビュー

ビュー名	説明	主キー	外部キー
ExInfo	Bit9 Server 環境内のサーバーとスキーマのパブリック プロパティ	Property_Id	（なし）
ExEvents	[Events（イベント）] ページに表示されるすべてのイベント	Event_Id	File_Catalog_Id、Root_File_Catalog_Id、Computer_Id
ExMeters	メーターされているファイルのすべての実行	Event_Id	Computer_Id、File_Catalog_Id
ExComputers	すべてのコンピューターのメタデータ	Computer_Id	（なし）
ExFileCatalog	すべての一意のハッシュのメタデータ	File_Catalog_Id	（なし）
ExFileInstances	すべてのコンピューター上の全ファイル インスタンスのメタデータ	File_Instance_Id	File_Instance_Group_Id、Computer_Id、File_Catalog_Id
ExDeletedFileInstances	すべての削除済みファイル インスタンスのメタデータ	Deleted_File_Instance_Id	File_Instance_Group_Id、Computer_Id、File_Catalog_Id
ExFileInstanceGroups	すべてのファイル インスタンス グループのメタデータ	File_Instance_Group_Id	Computer_Id、File_Catalog_Id
ExApprovalRequests	[Approval Requests（承認要求）] ページに表示されるすべての承認要求	Approval_Request_Id	File_Catalog_Id、Process_File_Catalog_Id、Root_File_Catalog_Id、Computer_Id

bit9_public のスキーマ ダイアグラム




Schema Diagram for bit9_public (continued)
ExFileCatalog
See previous page
ExApprovalRequests
Approval_Request_ID
File_Catalog_Id
Process_File_Catalog_Id
Root_File_Catalog_Id
Computer_Id
Date_Created
Date_Modified
Last_Modified_By
Enforcement_Level
Resolution
Request_Type
Requestor
Requestor_Comment
Requestor_Email
Priority_Text
Resolution_Comment
Status
Policy
Multiple_Blocks
File_Name
Path_Name
Process
ExComputers
See previous page

データベース ビューの詳細

ExComputers

ExComputers ビューを使用すると、サイト内で Bit9 エージェントを実行しているすべてのコンピューターのメタデータにアクセスできます。Bit9 コンソールですべてのコンピューターのメタデータを一覧表示するには、コンソール メニューで［**Assets**（アセット）］>［**Computers**（コンピューター）］の順に選択します。1 台のコンピューターのメタデータを表示するには、［Computers（コンピューター）］ページでコンピューター名をクリックします。

表 110：ExComputers ビューの詳細

フィールド名	データ型	特殊な値	コメント
Computer_Id	**int**		**主キー**
Audit_Date	nvarchar		コンピューターの情報が収集された日時
Computer_Information	XML		各コンピューターのドライブ数と空き容量、プロセッサーの数とモデルと速度、システム上の合計 RAM など、コンピューターに関する（XML 形式の）データを含むメタフィールド
▲ Platform	varchar	'Windows'、'Mac'、'Linux'	
Memory_Size	int		このコンピューターに搭載されているメモリのサイズ（メガバイト）
Processor_Count	int		このコンピューターのプロセッサーの数
Processor_Speed	float		コンピューター プロセッサーの速度 (MHz)
IP_Address	varchar		最後に記録されたこのコンピューターの IP アドレス。IPv4 または IPv6 アドレスのいずれかになります。
Connected	varchar	'Yes'（はい）、'No'（いいえ）	このコンピューター上のエージェントが Bit9 Server に接続されている場合は 'Yes'（はい）
Days_Offline	int		このコンピューターがオフラインになってからの日数
Computer_Uninstalled	varchar	'Yes'（はい）、'No'（いいえ）	このコンピューターからエージェントがアンインストールされている場合は 'Yes'（はい）

フィールド名	データ型	特殊な値	コメント
Computer_Deleted	varchar	'Yes'（はい）、'No'（いいえ）	このコンピューターが Bit9 Server の［Computers（コンピューター）］リストから削除されている場合は 'Yes'（はい）
Date_Created	datetime		このコンピューターが初めて Bit9 Server に接続した日時
Policy_Mode	varchar	'Control'（制御）、'Visibility'（可視性）、'Agent Disabled'（エージェント無効）	このコンピューターが属しているポリシーのモード
Agent_Version	varchar		このコンピューターにインストールされているエージェントのバージョン
Poll_Date	varchar		このコンピューターが最後に Bit9 Server に接続した日時
Policy_Assignment	varchar	'Manual'（手動）、'Automatic'（自動）	このコンピューターにポリシーがどのように割り当てられたか（ポリシーが Active Directory によって自動的に割り当てられた場合は 'Automatic'（自動））。
Δ Upgrade_Status	varchar	'Up to date'（最新）、'Completed'（完了済み）、'Not supported'（サポート外）、'Scheduled'（スケジュール済み）、'Waiting'（待機中）、'Not requested'（要求なし）、'Agent uninstalled'（エージェント アンインストール済み）、'Reboot required'（再起動が必要）'Blocked'（ブロック済み）、'Upgrade requested'（アップグレード要求済み）、'Unknown'（不明）	このエージェントの現在のアップグレード ステータス **変更に関する注意**：'Upgrade requested'（アップグレード要求済み）は 7.0.0 で追加されました。

フィールド名	データ型	特殊な値	コメント
ΔPolicy_Status	varchar	'Policy out of date'（ポリシーが期限切れ）、'Approvals out of date'（承認が期限切れ）、'Enforcement Level out of date'（適用レベルが期限切れ）、'Out of date'（期限切れ）、'Up to date'（最新）	このコンピューターの現在のポリシー ステータス **変更に関する注意**：6.0.2 では、'Enforcement Level out of date'（適用レベルが期限切れ）が 'SecCon out of date'（SecCon が期限切れ）となっていました。
Computer	nvarchar		このコンピューターの名前
Users	nvarchar		現在までにこのコンピューターにログオンしたことがあるユーザーのカンマ区切りリスト
Δ Enforcement_Level	nvarchar	'High (Block Unapproved)'（高（未承認をブロック））、'Medium (Prompt Unapproved)'（中（未承認に対してプロンプトを表示））、'Low (Monitor Unapproved)'（低（未承認を監視））、'None (Visibility)'（なし（可視性））、'None (Disabled)'（なし（無効））	このコンピューターがオンラインのときに使用される適用レベル **変更に関する注意**：6.0.2 では、Enforcement_Level が Online_SecCon となっていました。7.0.0 以降では、すべての値が変更されています。
Δ Disconnected_Level	nvarchar	'High (Block Unapproved)'（高（未承認をブロック））、'Medium (Prompt Unapproved)'（中（未承認に対してプロンプトを表示））、'Low (Monitor Unapproved)'（低（未承認を監視））、'None (Visibility)'（なし（可視性））、'None (Disabled)'（なし（無効））	このコンピューターがオフラインのときに使用される適用レベル **変更に関する注意**：6.0.2 では、Disconnected_Level が Offline_SecCon となっていました。7.0.0 以降では、すべての値が変更されています。
Computer_Tag	nvarchar		このコンピューターに割り当てられているオプションのカスタム タグ
OS_Short_Name	nvarchar		このコンピューターにインストールされている OS の短い名前

フィールド名	データ型	特殊な値	コメント
OS_Long_Name	nvarchar		このコンピューターにインストールされている OS の長い名前
Policy	nvarchar		このエージェントが最後に参加したポリシーの名前
Policy_Description	nvarchar		このエージェントが最後に参加したポリシーの説明
Machine_Model	nvarchar		このコンピューターのマシン モデル
Processor_Model	nvarchar		このコンピューターのプロセッサー モデル
Upgrade_Error	nvarchar		エージェント アップグレード時のエラー（発生した場合のみ）
Synch_Percent	int		このコンピューターと Bit9 Server の同期の進捗状況（パーセント）
▲ Template	varchar	'Yes'（はい）、'No'（いいえ）	このコンピューターがテンプレートである場合は 'Yes'（はい）。そうでない場合は 'No'（いいえ）（クローン コンピューターとクローンでないコンピューターの両方を含みます）
▲ Template_Computer_Id	int		親テンプレート コンピューターの ID。値が 0 の場合、このコンピューターは親テンプレートを持たず、クローンでないことを意味します。値が 0 以外の場合、このコンピューターはクローンであることを意味します。
▲ Virtualized	varchar	'Yes'（はい）、'No'（いいえ）	このコンピューターが仮想マシンである場合は 'Yes'（はい）。そうでない場合は 'No'（いいえ）。
▲ Virtual_Platform	varchar		Virtualized が 'Yes'（はい）の場合は、仮想マシンのプラットフォームを示します。現在のところ、このフィールドの値は 'VMware'、'Unknown'（不明）、または空白のいずれかになります。

ExInfo

ExInfo ビューを使用すると、Bit9 Server や環境内の他のサーバーのアドレスに加え、Bit9 Server とパブリック スキーマ（このスキーマ）のバージョンに関するデータにアクセスできます。

表 111：ExInfo ビューの詳細

フィールド名	データ型	特殊な値	コメント
Property_Id	**int**		**主キー**
Name	nvarchar	'RPCServerAddress'、'Bit9ServerVersion'、'WebServerAddress'、'DBPublicSchemaVersion'、	プロパティの名前
Value	nvarchar		プロパティの値

ExMeters

ExMeters ビューを使用すると、Bit9 メーターの全実行に関するデータにアクセスできます。Bit9 メーターを設定すると、指定されたファイルが環境内で実行されるたびに監視が行われます。Bit9 コンソールでこれらの情報を表示するには、コンソール メニューで［**Tools**（ツール）］>［**Meters**（メーター）］の順に選択して、各メーターの隣にある［View Details（詳細の表示）］ボタンをクリックします。

表 112：ExMeters ビューの詳細

フィールド名	データ型	特殊な値	コメント
Event_Id	bigint		このメーター エントリに対応するイベントの ExEvents テーブルの外部キー。この値は常に一意であるため、主キーとしても使用できます。
Computer_Id	int		このメーター エントリに対応するコンピューターの ExComputers テーブルの外部キー
File_Catalog_Id	int		このメーター エントリに対応するファイルの ExFileCatalog テーブルの外部キー
Timestamp	datetime		このメーター エントリが生成された日時
Name	nvarchar		メーターの名前
Description	nvarchar		メーターの説明

フィールド名	データ型	特殊な値	コメント
Data	nvarchar		メーターに関連付けられたデータ（このフィールドの解釈については、「Type」を参照してください）
ΔType	int	2 = sha1 ハッシュ、 3 = md5 ハッシュ、 4 = ファイル名、 5 = sha256 ハッシュ 6 = sha256 ファジー ハッシュ	Data フィールドのタイプ。メーターがどのような方法で作成されたかを示します。 **変更に関する注意**：旧バージョンの一部マニュアルでは、このフィールドの値が正しく記載されていませんでした。
User_Name	nvarchar		このメーターを作成したユーザーの名前

ExEvents

ExEvents ビューを使用すると、［Events（イベント）］ページで表示可能なすべてのイベントにアクセスできます。これにはファイルの発見、ファイルのブロック、ファイルの承認、未承認ファイルの実行、システム管理プロセス、およびコンソール ユーザーによるアクションに関連するイベントが含まれます。Bit9 コンソールでイベント データを表示するには、コンソール メニューで［**Reports**（レポート）］>［**Events**（イベント）］の順に選択して［Events（イベント）］ページを開きます。

表 113：ExEvents ビューの詳細

フィールド名	データ型	特殊な値	コメント
Event_Id	**bigint**		**主キー**
Computer_Id	int		このイベントを送信したコンピューターの ExComputers テーブルの外部キー
File_Catalog_Id	int		このイベントに関連付けられたファイルの ExFileCatalog テーブルの外部キー
Root_File_Catalog_Id	int		このイベントに関連付けられたルート ファイルの ExFileCatalog テーブルの外部キー
▲ File_Name	nvarchar		このイベントに関連するファイルの名前
▲ Path_Name	nvarchar		このイベントに関連するファイルのパス。パスの表記には、ファイルが存在するエージェントの OS に固有の区切り文字が使用されます。
Process	nvarchar		このイベントに関連付けられたプロセスの名前

フィールド名	データ型	特殊な値	コメント
▲ Process_File_Catalog_ID	int		このイベントに関連付けられたプロセスの ExFileCatalog テーブルの外部キー
Timestamp	datetime		このイベントが生成された日時 (UTC)
IP_Address	varchar		このイベントを開始したエンドポイントの IP アドレス
Description	nvarchar		イベントの説明
Priority	nvarchar	'Debug'（デ バ ッグ）、 'Info'（情報）、 'Notice'（通知）、 'Warning'（警告）、 'Error'（エラー）、 'Critical'（重大）	イベントの優先度
Type	nvarchar		イベント タイプ
Subtype	nvarchar		イベント サブタイプ
User_Name	nvarchar		このイベントに関連付けられたユーザーの名前
▲ Rule_Name	nvarchar		このイベント（ブロック、プロンプト、レポート、承認）をトリガーした Bit9 ルールの名前
♦ Ban_Name	nvarchar		このイベントに関連付けられたハッシュまたはファイル名に基づく禁止の名前（禁止に名前が付けられていない場合は空）。7.0.1 Patch 3 で導入されました
♦ Updater_Name	nvarchar		このイベントに関連付けられたアップデーターの名前。7.0.1 Patch 3 で導入されました
★ Indicator_Name	nvarchar		このイベントに脅威の痕跡が関連付けられている場合は、脅威の痕跡の名前
★ Received_Timestamp	datetime		Bit9 Server がこのイベントを受信した日時 (UTC)
Command_Line	nvarchar		このイベントによって記録されたアクションを試みたプロセスのコマンド ライン

ExFileCatalog

ExFileCatalog ビューを使用すると、環境内のコンピューター上で発見されたファイルの一意のハッシュのメタデータにアクセスできます。Bit9 コンソールでこれらのファイル データを表示するには、コンソール メニューで［**Assets**（アセット）］>［**Files**（ファイル）］の順に選択して［File Catalog（ファイル カタログ）］タブをクリックします。

表 114：ExFileCatalog ビューの詳細

フィールド名	データ型	特殊な値	コメント
File_Catalog_Id	**int**		**主キー**
Prevalence	int		このファイルの普及度（現在このファイルが存在しているコンピューターの数）
First_Created	datetime		このファイルが最初に作成された日時
File_Size	bigint		このファイルのサイズ（バイト単位）
File_Type	varchar	'Application'（アプリケーション）、'Package'（パッケージ）、'Script File'（スクリプト ファイル）、'Supporting File'（サポート ファイル）、'Other'（その他）、'Unknown'（不明）、'Unrecognized Executed File'（未確認の実行済みファイル）	このファイルの種類
MD5	char		このファイルの MD5 ハッシュ
Sha1	char		このファイルの SHA1 ハッシュ
Sha256	char		このファイルの SHA256 ハッシュ（このフィールドの解釈については、Sha256_Hash_Type を参照してください）
Sha256_Hash_Type	int	5 = 通常ハッシュ 6 = MSI ファジー ハッシュ	Sha256_Hash のタイプ。詳細については、「SHA-256」（249 ページ）を参照してください。

フィールド名	データ型	特殊な値	コメント
First_Seen_Computer_id	int		このファイルが最初に発見されたコンピューターの ExComputers テーブルの外部キー
First_Seen_Name	nvarchar		このファイルがいずれかのコンピューター上で最初に発見されたときのファイル名
First_Seen_Path	nvarchar		このファイルがいずれかのコンピューター上で最初に発見されたときのパス。最初に発見されたコンピューターの OS に固有のパス区切り文字が使用されます。
Product_Name	nvarchar		このファイルの製品名
Product_Version	nvarchar		このファイルの製品バージョン
Publisher	nvarchar		このファイルの公開者（ファイルが証明書で署名されている場合）
▲ ◊Publisher_State	nvarchar	'Approved'（承認済み）、'Approved by Policy'（ポリシーにより承認）、'Unapproved'（未承認）、'Banned'（禁止）、'Banned by Policy'（ポリシーにより禁止）	この公開者の状態（情報がある場合）。署名されていないファイルの場合は「none」（なし） **変更に関する注意**：'Banned'（禁止）および 'Banned by Policy'（ポリシーにより禁止）は 7.0.1 で追加されました。
▲ Publisher_State_Reason	nvarchar	'Manual'（手動）、'Reputation'（レピュテーション）、'Imported'（インポート）、'External (API)'（外部（API））、'Unknown'（不明）	ファイルの公開者が承認された理由
Publisher_or_Company	nvarchar		このファイルの公開者（情報がある場合）または会社（公開者情報がない場合）
Company	nvarchar		このファイルの会社名

フィールド名	データ型	特殊な値	コメント
Installed_Program_Name	nvarchar		このファイルがインストーラーであった場合は、このファイルによりインストールされたプログラムの名前（Windows の［プログラムの追加と削除］ページに表示される名前）。Mac または Linux 用ファイルの場合は値なし。
Trust	int	-1 = 不明、 [0 – 10] 有効な値	このファイルの信頼度（最大値 = 10）
Trust_Messages	nvarchar		このファイルの信頼度に関連付けられた追加情報
Threat	nvarchar	'0 - Clean'（0 – クリーン）、 '1 - Potential risk'（1 – 危険な可能性あり）、 '2 - Malicious'（2 – 悪質）、 'Unknown'（不明）	このファイルの脅威レベル
Category	nvarchar		このファイルのカテゴリ
▲ State	nvarchar	'Unapproved'（未承認）、'Approved'（承認済み）、'Banned'（禁止）、'Approved by Policy'（ポリシーにより承認）、'Banned by Policy'（ポリシーにより禁止）、'Mixed'（混在）	このファイルに対して有効なグローバル状態
Δ File_State	nvarchar	'Unapproved'（未承認）、'Approved'（承認済み）、'Banned'（禁止）、'Approved by Policy'（ポリシーにより承認）、'Banned by Policy'（ポリシーにより禁止）、'Mixed'（混在）	このファイルのグローバル状態 **変更に関する注意**：6.0.2 での名称は Global_State でした。7.0.0 以降では値も変更されています。

フィールド名	データ型	特殊な値	コメント
Δ File_Flags	nvarchar	次の値で構成されるカンマ区切りリスト 'Installer'（インストーラー）、 'Not installer (Override)'（インストーラー以外（無効化））、 'Installer (Override)'（インストーラー（無効化））、 'Report Only Ban'（レポートのみの禁止）	このファイルのグローバル ファイル フラグ **変更に関する注意**：6.0.2 では、File_Flags が Global_Flags となっていました。また、6.0.2 では 'Report Only Ban'（レポートのみの禁止）が 'Test Banned'（テスト禁止）という値になっていました。
▲ File_State_Reason	nvarchar	'Manual'（手動）、'Trusted Directory'（信頼済みディレクトリ）、'Reputation'（レピュテーション）、'Imported'（インポート）、'External (API)'（外部（API））、'Unknown'（不明）	このファイルの承認状態が割り当てられた理由
▲ Approved_By_Reputation	varchar	'Yes'（はい）、'No'（いいえ）	Bit9 SRS でのファイルまたは公開者の信頼度と脅威レベルに基づいてこのファイルが承認されたかどうか
Reputation_Enabled	varchar	'Yes'（はい）、'No'（いいえ）	このファイルに対してレピュテーションに基づく承認が有効になっているか
♦ Certificate_Hash	char		この証明書を一意に識別する Bit9 独自のハッシュ
♦ Certificate_State	nvarchar	'Unapproved'（未承認）、'Approved'（承認済み）、'Banned'（禁止）、'Approved by Policy'（ポリシーにより承認）、'Banned by Policy'（ポリシーにより禁止）	このファイルの証明書のグローバル状態 **注意**：証明書が無効な場合、このフィールドは 'Unapproved'（未承認）になります。証明書が署名されていない場合、このフィールドは空になります。
♦ Certificate_State_Reason	nvarchar	'Manual'（手動）、'External (API)'（外部（API））	証明書の状態が割り当てられた理由（Publisher_State_Reason と同じ）
★ File_Extension	nvarchar		このハッシュを含むファイルが最初に見つかったときの拡張子

ExFileInstances

ExFileInstances ビューを使用すると、サイト内の各コンピューター上で見つかった各ハッシュの各インスタンスに関するメタデータにアクセスできます。Bit9 コンソールでこれらのファイル データを表示するには、コンソール メニューで［**Assets**（アセット）］>［**Files**（ファイル）］の順に選択して、［File on Computers（コンピューター上のファイル）］タブをクリックします。個々のファイルのインスタンスに関する完全な詳細を表示するには、［Files on Computers（コンピューター上のファイル）］タブで、ファイルの隣にある［View Details（詳細の表示）］ボタンをクリックします。

変更に関する注意：v7.0.1 以降では、**Initialized** および **Top_Level** フィールドがこのビューから削除されて、**ExFileInstanceGroups** ビューに移動されています。

表 115：ExFileInstances ビューの詳細

フィールド名	データ型	特殊な値	コメント
File_Instance_Id	**bigint**		**主キー**
File_Instance_Group_Id	int		このファイルを含むグループの ExFileInstanceGroups テーブルの外部キー
File_Catalog_Id	int		このファイルに関する詳細の ExFileCatalog テーブルの外部キー
Computer_Id	int		このファイルが存在するコンピューターの ExComputers テーブルの外部キー
Date_Created	datetime		このファイルが作成された日時 (UTC)
File_Name	nvarchar		このファイルの名前
Path_Name	nvarchar		このファイルのパス。ファイルが存在するエージェントの OS に固有の区切り文字が使用されます。
Executed	varchar	'Yes'（はい）、'No'（いいえ）	このファイルがこれまでに実行されたことがある場合は 'Yes'（はい）
Δ Local_State	nvarchar	'Unapproved'（未承認）、'Approved'（承認）、'Banned'（禁止）	このファイルのローカル状態 **変更に関する注意**：6.0.2 では、'Unapproved'（未承認）が 'Pending'（保留中）となっていました。

フィールド名	データ型	特殊な値	コメント
Δ Detailed_Local_State	nvarchar	'Approved (Not Persisted)'（未承認（非永続的））、'Unapproved (Persisted)'（未承認（永続的））、'Banned by Hash'（ハッシュに基づいて禁止）、'Locally Approved'（ローカルで承認）、'Banned by Name'（名前に基づいて禁止）、'Banned by Name (Report Only)'（名前に基づいて禁止（レポートのみ））、'Locally Approved (Auto)'（ローカルで承認（自動））、'Approved as Installer'（インストーラーとして承認）、'Approved'（承認）、'Approved as Installer (Top Level)'（インストーラーとして承認（トップ レベル））、'Banned by Hash (Report Only)'（ハッシュに基づいて禁止（レポートのみ））、'Unapproved'（未承認）	このファイルの詳細なローカル状態 **変更に関する注意**：6.0.2 では、'Unapproved'（未承認）が 'Pending'（保留中）となっていました。6.0.2 では、'Unapproved (Persisted)'（未承認（永続的））が 'Pending (Persisted)'（保留中（永続的））となっていました。
♦ Detached_Publisher	nvarchar		デタッチされた公開者の名前。埋め込まれている公開者は ExFileCatalog との結合によって取得できます。
♦ Detached_Publisher_State	nvarchar	'Approved'（承認済み）、'Approved by Policy'（ポリシーにより承認）、'Unapproved'（未承認）、'Banned'（禁止）、'Banned by Policy'（ポリシーにより禁止）	デタッチされた公開者の状態（情報がある場合）。署名されていないファイルの場合は「none」（なし）
♦ Detached_Publisher_State_Reason	nvarchar	'Manual'（手動）、'Imported'（インポート）、'External (API)'（外部（API））、'Unknown'（不明）	このファイルの公開者の状態が割り当てられた理由

フィールド名	データ型	特殊な値	コメント
Detached_Certificate_Hash	char		デタッチされた証明書の Bit9 独自のハッシュ。埋め込まれている証明書は ExFileCatalog との結合によって取得できます。
♦ Detached_Certificate_State	nvarchar	'Unapproved'（未承認）、'Approved'（承認済み）、'Banned'（禁止）、'Approved by Policy'（ポリシーにより承認）、'Banned by Policy'（ポリシーにより禁止）	デタッチされた証明書のグローバル状態 **注意**：証明書が無効な場合、このフィールドは 'Unapproved'（未承認）になります。証明書が署名されていない場合、このフィールドは空になります。
♦ Detached_Certificate_State_Reason	nvarchar	'Manual'（手動）、'Imported'（インポート）、'External (API)'（外部（API））、'Unknown'（不明）	このファイルからデタッチされた証明書の状態が割り当てられた理由（Publisher_State_Reason と同じ）

ExDeletedFileInstances

ExDeletedFileInstances ビューを使用すると、サイト内の各コンピューター上で削除された各ファイル インスタンスに関するメタデータにアクセスできます。Bit9 Server には、各コンピューター上の一意のファイル名のインスタンスのうち、最後に削除されたインスタンスのみが記録として残ります。したがって、同じファイルの作成と削除が繰り返された場合は、最後に削除されたインスタンスのみが記録されます。

変更に関する注意：Bit9 v7.0.1 以降では、**Initialized** および **Top_Level** フィールドがこのビューから削除されて、**ExFileInstanceGroups** ビューに移動されています。

表 116：ExDeletedFileInstances ビューの詳細

フィールド名	データ型	特殊な値	コメント
Deleted_File_Instance_Id	**bigint**		**主キー**
File_Instance_Group_Id	int		このファイルを含むグループの ExFileInstanceGroups テーブルの外部キー
File_Catalog_Id	int		このファイルに関する詳細の ExFileCatalog テーブルの外部キー
Computer_Id	int		このファイルが存在するコンピューターの ExComputers テーブルの外部キー

フィールド名	データ型	特殊な値	コメント
Date_Created	datetime		このファイルが作成された日時 (UTC)
Date_Deleted	datetime		このファイルが削除された日時 (UTC)
File_Name	nvarchar		このファイルの名前
Path_Name	nvarchar		このファイルのパス。ファイルが存在していたエージェントの OS に固有の区切り文字が使用されます
♦ Detached_Publisher	nvarchar		デタッチされた公開者の名前。埋め込まれている公開者は ExFileCatalog との結合によって取得できます。
♦ Detached_Publisher_State	nvarchar	'Approved'（承認済み）、'Approved by Policy'（ポリシーにより承認）、'Unapproved'（未承認）、'Banned'（禁止）、'Banned by Policy'（ポリシーにより禁止）	デタッチされた公開者の状態（情報がある場合）。署名されていないファイルの場合は「none」（なし）
♦ Detached_Publisher_State_Reason	nvarchar	'Manual'（手動）、'Reputation'（レピュテーション）、'Imported'（インポート）、'External (API)'（外部（API））、'Unknown'（不明）	このファイルの公開者の状態が割り当てられた理由
♦ Detached_Certificate_Hash	char		デタッチされた証明書の Bit9 独自のハッシュ。埋め込まれている証明書は ExFileCatalog との結合によって取得できます
♦ Detached_Certificate_State	nvarchar	'Unapproved'（未承認）、'Approved'（承認）、'Banned'（禁止）、'Approved by Policy'（ポリシーにより承認）、'Banned by Policy'（ポリシーにより禁止）	デタッチされた証明書のグローバル状態。**注意**：証明書が無効な場合、このフィールドは 'Unapproved'（未承認）になります。証明書が署名されていない場合、このフィールドは空になります。

フィールド名	データ型	特殊な値	コメント
♦ Detached_Certificate_State_Reason	nvarchar	'Manual'（手動）、'Imported'（インポート）、'External (API)'（外部（API））、'Unknown'（不明）	このファイルからデタッチされた証明書の状態が割り当てられた理由（Publisher_State_Reason と同じ）

ExFileInstanceGroups

ExFileInstanceGroups ビューを使用すると、環境内のコンピューター上で発見されたファイル インスタンス グループのメタデータにアクセスできます。ファイル インスタンス グループとは、1 個のルート ファイル（通常はインストーラーですが、場合によってはコピー元になったファイル）に関連付けられたファイルのグループです。

表 117：ExFileInstanceGroups

フィールド名	データ型	特殊な値	コメント
File_Instance_Group_Id	**Int**		**主キー**
File_Catalog_Id	Int		このグループのルート ファイルに関する詳細の ExFileCatalog テーブルの外部キー
Computer_Id	Int		このファイル グループが存在するコンピューターの ExComputers テーブルの外部キー
Date_Created	datetime		このファイル グループが作成された日時 (UTC)
Group_Type	int	0 – 初期化済みファイル 1 – 最上位レベル ファイル 2 – プロセスによってインストールされたファイル 3 – インストーラーによりインストールされ、[プログラムの追加と削除] に表示されるファイル	このグループが Bit9 によってどのように認識されたか

フィールド名	データ型	特殊な値	コメント
Path_Name	nvarchar		このグループのルート ファイルに対応するパス。パスの表記には、ファイルが存在するエージェントの OS に固有の区切り文字が使用されます。
User_Name	nvarchar		このグループを作成したユーザー
File_Name	nvarchar		このグループのルート ファイルに対応するファイル名
Installed_Program_Name	nvarchar		このファイルがインストーラーであった場合は、インストールされたプログラムの名前
♦ Initialized	varchar	'Yes'（はい）、'No'（いいえ）	このグループに含まれるファイルが初期化中に発見された場合は 'Yes'
♦ Top_Level	varchar	'Yes'（はい）、'No'（いいえ）	このグループがインストーラーによって生成されたファイルではなく最上位レベルのファイルに相当する場合は 'Yes'。このグループに含まれるファイルがインストールの一部であった場合は 'No'。

ExApprovalRequests

ExApprovalRequests ビューを使用すると、ファイルの実行がブロックされたときに表示される Bit9 通知を介してユーザーが作成した承認要求のワークフローにアクセスできます。これには、実行が完全にブロックされたファイルの承認要求や、ユーザーがプロンプトに応答してファイルの実行を許可した場合の根拠が含まれます。

注意：このビューは v7.2.0 で新しく導入されました。

表 118：ExApprovalRequests

フィールド名	データ型	特殊な値	コメント
Approval_Request_Id	**Int**		**主キー**
File_Catalog_Id	Int		承認要求が作成されたファイルの ExFileCatalog テーブルの外部キー
Process_File_Catalog_Id	Int		承認要求が作成されたファイルに関連付けられているプロセスの ExFileCatalog テーブルの外部キー

フィールド名	データ型	特殊な値	コメント
Root_File_Catalog_Id	Int		承認要求が作成されたファイルに関連付けられているルートファイルの ExFileCatalog テーブルの外部キー
Computer_Id	Int		承認要求を発行したコンピューターの ExComputers テーブルの外部キー
Date_Created	datetime		この承認要求が作成された日時 (UTC)
Date_Modified	datetime		この承認要求が最後に変更された日時 (UTC)
Last_Modified_By	nvarchar		この承認要求を最後に変更したユーザー
Enforcement_Level	nvarchar	有効な適用レベル	ファイルがブロックされたときのエージェントの適用レベル
Resolution	nvarchar	Not Resolved（未解決）、 Resolved - Publisher（解決済み – 公開者）、 Resolved - Installer（解決済み – インストーラー）、 Resolved - Approved（解決済み – 承認）、 Resolved - Rule Change（解決済み – ルール変更）、 Resolved - Other（解決済み – その他）、 Rejected（拒否）	要求の解決
Request_Type	nvarchar	Approval（承認）、 Justification（根拠）	承認要求の種類。ファイルがブロックされた場合は Approval（承認）、ファイルがユーザー選択プロンプトをトリガーした場合は Justification（根拠）
Requestor	nvarchar		エージェント上で承認要求を作成したユーザー
Requestor_Comments	nvarchar		承認要求の作成時に入力されたコメント

フィールド名	データ型	特殊な値	コメント
Requestor_Email	nvarchar		承認要求の作成時に入力された E メール アドレス
Priority_Text	nvarchar	High（高）、Low（低）、Medium（中）	作成者によってこの要求に割り当てられた優先度
Resolution_Comments	nvarchar		承認の解決時に入力されたコメント
Status	nvarchar	Submitted（送信済み）、Closed（クローズ）	要求の現在のステータス
Policy	nvarchar		ブロックが発生したときにエージェントが属していたポリシーの名前
Multiple_Blocks	nvarchar	Yes（はい）、No（いいえ）	このエンドポイントとハッシュで複数のブロックが発生したかどうか
File_Name	nvarchar		エージェント上でブロックされたファイルの名前
Path_Name	nvarchar		エージェント上でブロックされたファイルのパス
Process	nvarchar		エージェント上でブロックされたファイルを書き込もうとしたプロセスの完全なパス

クエリの例

以下に、Live Inventory SDK を使用して実行できるクエリの例を示します。各クエリでは **das** データベースを使用する必要があります。

悪意のあるファイルの一覧表示

Bit9 SRS が有効になっている場合は、次のクエリを使用して、Bit9 エージェントを実行しているシステム上で検出された悪意のあるすべてのファイルの名前と普及度を一覧表示できます。

```
USE das
SELECT First_Seen_Path, First_Seen_Name, Sha256, Threat,
  Trust, Prevalence
FROM bit9_public.ExFileCatalog
WHERE Threat IN ('2 - Malicious', '1 - Potential risk')
ORDER BY First_Seen_Path, First_Seen_Name
```

このクエリに一致するデータが見つかった場合は、次のような出力が表示されます（書式は実際の表示と異なります）。

First_Seen_Path	First_Seen_Name	Sha256	Threat	Trust	Prev.
c:\temp\folder1	myfileapp.exe	46b8d0bc3a4db8433fb66543c1ec03bd1e24e0198228ac7024c0a15658bf04fd	1 - Potential risk	2	1
c:\documents and settings\rjones	numbergen.exe	552e68dcd6c2a4d6bf9c9dbf278967e2904cd624c23c0aad58c430ed7fa75acd	1 - Potential risk	1	1
c:\documents and settings\bsmith	makemess.exe	4d9ab91f5e1efbcb5abcd6ec9a0a6345235a54cf05d6241a304e3bf3b40d4668	1 - Potential risk	3	1
c:\hp\bin	endprocess.exe	1effc62134ab95d297c34959752311e1f7f433d07810da65b233bf7241ada68ad	1 - Potential risk	3	13
c:\program files\mywebapp\	f4dothis.dll	abcdea797736654ae4f74eef7371d018c3463f24cf78aea92dafe51c7a858f19	2 - Malicious	0	1
c:\jobfiles	myway.exe	23451271912da7b68b407c77381ab1ff3b59b37c1e4d9f1e417a1d0fcc9270dd	2 - Malicious	0	1

ポリシーおよび適用レベルごとの Bit9 エージェント システムの一覧表示

次のクエリを使用すると、Bit9 エージェントを実行しているシステムの数を確認して、ポリシーおよび適用レベルごとに結果をグループ化できます。

```
USE das
SELECT Policy, Enforcement_Level, Disconnected_Level,
COUNT(*)
  AS Computer_Count
FROM bit9_public.ExComputers
GROUP BY Policy, Enforcement_Level, Disconnected_Level
ORDER BY Policy
```

このクエリに一致するデータが見つかった場合は、次のような出力が表示されます（書式は実際の表示と異なります）。

Policy	Connected_Enforcement_Level	Disconnected_Enforcement_Level	Count
Agent Disabled	None (Disabled)	None (Disabled)	3
Research Team	Medium (Prompt Unapproved)	Medium (Prompt Unapproved)	6
Default Policy	None (Visibility)	None (Visibility)	1
General Office	High (Block Unapproved)	High (Block Unapproved)	49
Guest Policy	High (Block Unapproved)	High (Block Unapproved)	1
IT Group	Low (Monitor Unapproved)	Low (Monitor Unapproved)	11

ポリシーごとの新しい未承認ファイルの一覧表示

次のクエリを使用すると、過去 24 時間以内に発見された新しい未承認ファイルの数を確認して、ポリシーごとに結果をグループ化できます。

```
USE das
SELECT Policy, COUNT(*) FROM bit9_public.ExFileInstances fi
  JOIN bit9_public.ExComputers c
ON c.Computer_Id = fi.Computer_Id
WHERE fi.Date_Created>DATEADD(day, -1, GetUTCDate()) AND
  Local_State = 'Unapproved'
GROUP BY Policy
ORDER BY COUNT(*) DESC
```

このクエリに一致するデータが見つかった場合は、次のような出力が表示されます（書式は実際の表示と異なります）。

Policy	New Unapproved File Count
Research Team	529
General Office	101
IT Group	257

コンピューターおよびポリシーごとの新しい未承認ファイルの一覧表示

次のクエリを使用すると、過去 24 時間以内に発見された新しい未承認ファイルの数を確認して、コンピューターおよびポリシーごとに結果をグループ化できます。

```
USE das
SELECT c.Computer, c.Policy, COUNT(*) as Unapproved_Count
FROM bit9_public.ExFileInstances fi
  JOIN bit9_public.ExComputers c
  ON c.Computer_Id = fi.Computer_Id
WHERE fi.Date_Created>DATEADD(day, -1, GetUTCDate()) AND
Local_State = 'Unapproved'
GROUP BY c.Computer, c.Policy
ORDER BY COUNT(*) DESC
```

このクエリに一致するデータが見つかった場合は、次のような出力が表示されます（書式は実際の表示と異なります）。

Computer Name	Policy	New Unapproved File Count
MYCORP\DESKTOP-3	Research Team	307
MYCORP\LAPTOP-1	General Office	215
MYCORP\LAPTOP-4	Research Team	32
MYCORP\DESKTOP-8	IT Group	3
MYCORP\DESKTOP-10	General Office	2
MYCORP\LAPTOP-7	General Office	1

付 録 B

Bit9 API

Bit9 API を使用すると、カスタム スクリプトや他のアプリケーションを通じて Bit9 Platform とやりとりするためのコードを作成できます。Bit9 API は、get URI 要求、post/put JSON 要求、および interpret JSON 応答を作成できる任意の言語と HTTPS プロトコルを使用して処理できる RESTful API です。

Bit9 API を通じてアクションを実行すると、コンソールから同じアクションを実行した場合と同等のオーディット トレールが作成されます。イベントでは、アクションを実行した API ユーザー名が参照されます。

この付録には、次の 2 つのセクションがあります。

- **API 認証とアクセス制御** – API ユーザー アカウントの作成方法と、クライアントの API 認証に必要な API トークンを生成する方法について説明します。また、アクセスに必要なログイン アカウントのアクセス許可を設定する方法についても説明します。
- **使用可能なオブジェクト** – Bit9 APIを通じてアクセスできるオブジェクトのリストと簡単な説明が掲載されています。

この付録はあくまでも要約版です。完全版の API ドキュメントは、次の 2 つの場所から入手できます。

- お使いのバージョンの Bit9 Platform がファイナライズされた時点のドキュメントは、Bit9 コンソールから https://< サーバーアドレス >/api/bit9platform/v1 に移動して入手できます。
- 最新版のドキュメントは https://github.com/carbonblack/bit9platform から入手できます。この場所にはサンプルも追加される予定です。

注意

Bit9 Platform には Live Inventory SDK も含まれ、データベースへの読み取り専用アクセスを可能にするパブリック ビューが提供されています。これらのパブリック ビューを使用することにより、独自のレポート作成ソリューションやデータ分析ソリューションを作成することが可能になります。詳細については、付録 A「ライブ インベントリ SDK：データベース ビュー」を参照してください。

概要

現在の Bit9 API のバージョンは v1 です。すべての API 呼び出しで次のアドレスが使用されます。
https://< サーバー名 >**/api/bit9platform/v1**

API 認証とアクセス制御

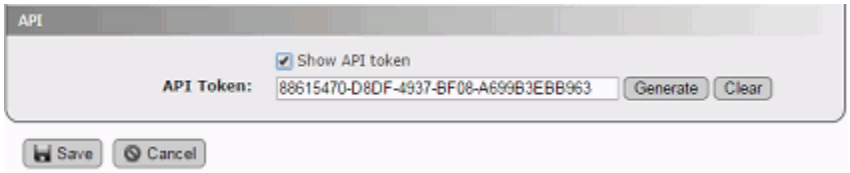
Bit9 API の認証には、現在ログインしているコンソール ユーザーの API トークンが使用されます。各 HTTP 要求の 'X-Auth-Token' ヘッダーにこのトークンが含まれている必要があります。

アクセス制御に関しては、API クライアントごとに別個のコンソール ユーザーを作成して、必要最小限のアクセス許可のみを付与することを推奨します。ただし、API クライアントには、Bit9 コンソールを通じて同じオブジェクトにアクセスする場合に必要となるアクセス許可と同等の権限を付与する必要があります。たとえば、API クライアントから 'event' オブジェクトにアクセスする必要がある場合は、クライアントで使用されている API トークンに関連付けられたユーザーに「View events（イベントの表示）」アクセス許可を付与する必要があります。各オブジェクトを使用するために必要となるアクセス許可については、GitHub で提供されている完全版の API ドキュメントを参照してください。アクセス許可を追加または削除する手順については、「アカウント グループの権限」（108 ページ）を参照してください。API を使用して Bit9 Platform にコネクターを追加する場合は、「Bit9 API を使用したコネクターの追加」（838 ページ）も参照してください。

API ユーザーの作成と API トークンの取得手順：

1. サーバー上または GitHub 上の Bit9 API ドキュメントを参照して、API クライアントに必要なアクセス許可を確認します。
2. コンソール メニューから、［**Administration**（管理）］>［**Login Accounts**（ログイン アカウント）］の順に選択します。
3. ［**Groups**（グループ）］タブをクリックして、［**Add Group**（グループの追加）］ボタンをクリックします。［Add Group（グループの追加）］ページが表示されます。
4. ［Add Group（グループの追加）］ページで、［Name（名前）］フィールドに名前（「API Connector Extensions」など）を入力し、必要に応じて［Description（説明）］フィールドに説明を追加して、クライアントに必要な各アクセス許可のチェックボックスをオンにします。一部のアクセス許可は他のアクセス許可に依存します。たとえば、オブジェクトを変更するためのアクセス許可を付与するには、オブジェクトを表示するためのアクセス許可も付与する必要があります。
5. グループの設定が完了したら、［Status（ステータス）］行にある［**Enabled**（有効）］ボタンをクリックし、ページの下部にある［Save（保存）］ボタンをクリックします。
6. ［**Users**（ユーザー）］タブをクリックし、［Login Accounts: Users（ログイン アカウント：ユーザー）］ページで、［**Add User**（ユーザーの追加）］をクリックします。

7. ［Add User（ユーザーの追加)］ページでユーザー名（「API HashBanScript」など）とパスワードを指定し、先ほど作成したグループを選択します。
8. 必要に応じてその他のフィールドに情報を入力します。
9. ページ下部にある［**Show API token**（API トークンの表示)］チェックボックスをオンにし、［**Generate**（生成)］ボタンをクリックします。［API Token（API トークン)］ボックスに文字列が表示されます。



10. API コード内の適切な場所に API トークンをコピーします。また、ログイン ユーザー名と、ログイン ユーザー名に関連付けられたコードを控えておきます。
11. ページ下部の［**Save**（保存)］ボタンをクリックします。

重要

文字列がそのまま表示される方法で API トークンを使用することは避けてください。API トークンが漏洩した場合は、API ユーザーとしてログインし、［Edit Login Account（ログイン アカウントの編集)］ページで［Generate（生成)］をクリックして新しいトークンを生成し、［Save（保存）］をクリックして、以後の認証に新しいトークンを使用してください。

現在 API へのアクセス権限を持つユーザーの API アクセスを無効にするには、上記の手順に従い、［Generate（生成)］の代わりに［Clear（クリア)］をクリックします。サーバーのセキュリティ強化が必要な場合は、すべての API アクセスを削除する必要があります。

使用可能なオブジェクト

Bit9 API を通じてアクセスできる Bit9 Platform オブジェクトは次のとおりです（API で実際に使用されるオブジェクト名と、どのオブジェクトが読み取り専用かについては、完全版のドキュメントを参照してください)。

- 承認要求と根拠 – 承認要求、およびユーザーが通知に応答したときに作成される根拠にアクセスできます。
- 証明書 – エンドポイントで見つかった公開者の証明書と、それらの状態にアクセスできます。
- コンピューター – Bit9 エージェントのコンピューター関連プロパティにアクセスできます。また、ポリシーの変更、エージェントのアップグレード、コンピューターの VDI テンプレート化、デバッグ プロパティの変更など、高度なアクションを実行することもできます。
- コネクター – Bit9 Platform に統合されているネットワーク セキュリティ コネクターの設定にアクセスできます。

- イベント – Bit9 Platform によって記録されたイベントにアクセスできます。
- ファイル分析 – 分析のためにネットワーク コネクターへ送信されたファイルにアクセスできます。また、ファイルの分析を要求したり、ファイルの分析をキャンセルすることもできます。
- ファイル カタログ – Bit9 エージェントによって発見された一意の全ファイルのレコード（ファイルに関連するメタデータを含む）にアクセスできます。
- ファイル インスタンス – すべての Bit9 エージェント上のファイルのライブ ファイル インベントリ（[Files on Computers（コンピューター上のファイル）]）にアクセスできます。また、ローカルでファイルを承認することもできます。
- 削除済みのファイル インスタンス – すべての Bit9 エージェント上の削除済みファイルのインベントリにアクセスできます。
- ファイル インスタンス グループ – ［Files on Computers（コンピューター上のファイル）］インベントリ内のファイル グループのレコードにアクセスできます。
- ファイル ルール – 一意のファイルに関連するルールにアクセスできます。また、承認と禁止の作成や編集も行えます。
- エージェントからアップロードされたファイル – エージェントから Bit9 Server にアップロードされたファイルのレコードにアクセスできます。また、アップロードを要求したり、アップロードをキャンセルすることもできます。
- メーターされている実行 – Bit9 メーターによって追跡されているファイル実行のレコードにアクセスできます。
- 通知 – ネットワーク コネクター（サービスおよびアプライアンス）から Bit9 Server に通知をプッシュできます。
- 通知 – ファイルに対するアクションがルールによってブロックされたときに使用される通知にアクセスできます。
- 保留中の分析 – 特定の外部コネクターに対する保留中の分析要求にアクセスできます。
- ポリシー – ポリシーの情報にアクセスできます。
- 公開者 – 公開者の情報にアクセスできます。また、公開者の状態（禁止または承認）を変更することもできます。
- サーバー設定 – サーバーの設定プロパティにアクセスできます。
- サーバー パフォーマンス – サーバーのパフォーマンス統計情報にアクセスできます。
- アップデーター – アップデーターの情報にアクセスできます。アップデーターを有効または無効にすることもできます。

Bit9 API を使用したコネクターの追加

Bit9 Connector を使用すると Bit9 Server を 1 つまたは複数のネットワーク セキュリティ デバイスまたはサービスに統合して、脅威に関する通知を外部ソースからサーバーに送信したり、デトネーションや分析のためにサーバーから外部ソースへファイルを送信することが可能になります。Bit9 Server には特定のコネクターとの統合機能があらかじめ組み込まれ、Bit9 コンソールにある設定項目を通じて構成することができます。

Bit9 API を使用すると Bit9 Connector の機能を拡張して、Bit9 Server に現在組み込まれていないデバイスやサービスを統合できるようになります。これらの統合が正しく実装されると通知機能や分析機能が追加され、それらの機能を設定して使用するために必要なユーザー インターフェイス要素も追加されます。新しいコネクターを設定するためのインターフェイスは、Bit9 コンソールの［System Configuration（システム構成）］ページの［Connectors（コネクター）］タブにあります。このタブには、次の設定オプションがあります。

- ［**Integration Enabled**（統合の有効化）］– このコネクターとの通知の統合を有効または無効にするには、このチェックボックスを使用します。このチェックボックスがオフの場合は、ファイル分析も自動的に無効になります。
- ［**File Analysis Enabled**（ファイル分析の有効化）］– このコネクターにファイル分析機能がある場合は、このチェックボックスを使用して、このコネクターによるファイル分析を有効または無効にすることができます。この設定項目はコネクターにファイル分析機能がある場合にのみ表示されます。
- ［**Upload Location**（アップロード先）］– ファイル分析を有効にした場合は、このコネクターで使用するアップロード先をカスタマイズできます。このオプションはコネクターにファイル分析機能がある場合にのみ表示されます。

設定が完了すると、Bit9 コンソールのインターフェイス内で組み込み済みのコネクターが表示されるすべての場所に、新しいコネクターが表示されます。たとえば、接続されているデバイスまたはサービスに分析機能がある場合は、［Files（ファイル）］ページの［Action（アクション）］メニューに新しいコネクターが分析オプションとして表示されます。コネクターの機能とユーザー インターフェイスの詳細については、付録 C「Bit9 Connector for Network Security Devices」を参照してください。

注意

- カスタムのネットワーク セキュリティ デバイスまたはサービスとの統合を追加するには、Bit9 へのアクセスに使用するログイン アカウントに「Extend connectors through API」（API によるコネクタの拡張）アクセス許可を付与する必要があります。また、コネクターの設定を行うには、システム構成の表示と管理を行うためのアクセス許可も必要になります。
- Bit9 API を通じてコネクターを実装した後は、特別なライセンスがなくてもそのコネクターの通知機能にアクセスできます。ただし、Bit9 で管理されているコンピューターからサードパーティ デバイスまたはサービスにファイルを送信して分析を行うには、ファイル アップロード機能を利用するためのライセンスが別途必要になります。

付 録 C

Bit9 Connector for Network Security Devices

この章では、Bit9 Server と 1 つまたは複数のネットワーク セキュリティ デバイスやサービスを統合する Bit9 Connector の構成方法と使用方法について説明します。

セクション

概要

Bit9 Connector を使用すると、以下のような 1 つまたは複数のネットワーク セキュリティ デバイスまたはサービスを Bit9 Server に統合することができます。

- Check Point® Software Technologies ファイアウォール
- Check Point ThreatCloud Emulation サービス
- Check Point Threat Emulation プライベート クラウド アプライアンス
- FireEye™ Email Security および Network Security
- FireEye Forensic Analysis
- Microsoft System Center Endpoint Protection (SCEP)
- Palo Alto Networks™ ファイアウォール
- Palo Alto Networks WildFire™ パブリックおよびプライベート クラウド サービス

注意

Bit9 API を使用すると、サポートされているデバイスおよびサービスだけではなく VirusTotal および Lastline も Bit9 Platform と統合することができます。このような統合は一部の API 機能のみであり、現在サポートの対象とはなりません。API のアクセスおよび認証を有効化する手順については、付録 B、「Bit9 API」を参照してください。API の詳しいドキュメントとサンプル コードの入手方法については、https://github.com/carbonblack/bit9platform を参照してください。

これらのシステムを Bit9 を統合すると、接続中のデバイスまたはサービスが企業ネットワーク上でマルウェアを検出したときに、Bit9 のリアルタイム エンドポイント センサーとレコーダーが脅威の場所と範囲を自動的に確認するようになるため、インシデント対応と修復を迅速に実施できます。また、Bit9 エンドポイント センサーによって検出された疑わしいファイルを、接続中のいずれかのアプライアンスやネットワーク セキュリティ分析プロバイダーにアップロードして詳しく分析することができます。

Bit9 Connector は、Bit9 Server およびネットワーク セキュリティ用のデバイスやサービスが個別に提供している機能に以下の機能を追加します。

- **外部通知** – 接続中のソースによって提供される通知を Bit9 コンソールに「外部通知」として表示し、Bit9 エンドポイント データと相関付けてアラートの優先度および感染範囲に関する可視性を即座に提供します。詳細については、「外部通知」（876 ページ）を参照してください。
- **ファイルの禁止** – 接続中のソースによってレポートされたマルウェアを、Bit9 上で手動または自動的に禁止できます。詳細については、「外部からレポートされたマルウェアの禁止」（893 ページ）を参照してください。
- **レジストリ制御** – 接続中のソースによってレポートされた疑わしいファイルやレジストリ アクティビティを、レポートするか Bit9 カスタム ルールによって制限できます。詳細については、「マルウェアのレポートまたは禁止用の特別ルール」（894 ページ）を参照してください。

- **疑わしいファイルの分析** – Bit9 エージェントによってエンドポイント上で発見された疑わしいファイルを、接続中のサービスに送信して分析できます。詳細については、「エンドポイント上の疑わしいファイルの分析」（896 ページ）を参照してください。
- **統合イベント ロギング** – 外部の通知や分析に関連するイベントや、Bit9 Server にレポートされたイベントが Bit9 イベント ログに統合され、Syslog 出力としても利用できるようになります。詳細については、「Bit9 でのコネクター関連イベントのロギング」（901 ページ）を参照してください。
- **イベント ルール** – ファイル関連の Bit9 イベントを使用してアクションを実行するルールを定義できます。たとえば、Bit9 Server インベントリで新たに見つかったファイルを、ルールによって Check Point Threat Emulation のクラウド サービスやアプライアンス、Palo Alto Networks WildFire クラウド、または FireEye AX に分析のために送信することができます。また、外部通知で悪意があるとしてレポートされたすべてのファイルを自動的に禁止するルールも定義できます。さらに、Microsoft SCEP から繰り返しレポートされるマルウェア感染の親プロセスが同一であることが Bit9 によって検出された場合は、この親プロセスが必要な機能で使用されていなければ禁止するイベント ルールを作成できます。イベント ルールの動作と構成方法の説明については、「イベント ルール」（517 ページ）を参照してください。

コネクターの使用準備

Bit9 Connector は、別途ライセンス付与される Bit9 Security Platform のオプションです。このコネクターを使用するには、次の手順を実行する必要があります。

- 適切な Bit9 Connector のライセンスが付与された Bit9 Server をインストールするか、Bit9 Server のインストール後にこのライセンスを追加します。
- この付録の説明に従って Bit9 Server とすべての接続デバイスを構成し、相互に通信できるようにします。
- 1 つ以上の Bit9 コンソール ユーザー アカウントが Bit9 Connector に関連する権限を持っていることを確認します。Administrator グループのアカウントは、デフォルトでこれらの権限を持っています。詳細については、「アカウント グループの権限」（108 ページ）を参照してください。

注意

Bit9 Connector for Network Security Devices と Bit9 Server のハードウェア要件およびソフトウェア要件に対応する Check Point 製品、Microsoft 製品、Palo Alto Networks 製品、および FireEye 製品のバージョンについては、Bit9 担当者にお問い合わせください。

Microsoft SCEP との統合の有効化

Microsoft System Center Configuration Manager (SCCM) は、ソフトウェアの配布、構成管理、エンドポイントとサーバーのセキュリティ ポリシーの設定に使用できます。SCCM のコンポーネントである System Center Endpoint Protection (SCEP) は、Microsoftプラットフォーム向けのマルウェア対策やその他のセキュリティ機能を提供しています。

Bit9 Connector を使用して SCCM Server を統合することで、Microsoft System Center Endpoint Protection (SCEP) 通知が Bit9 Server に送信されるようになります。これらの SCEP 通知は、マルウェアの場所を特定し、セキュリティ チームの調査や脅威の駆除に役立てるために、Bit9 が管理するエンドポイントのファイルの情報と相関付けることができます。新しい脅威がレポートされると、このファイルが隔離される場合でも、Bit9 はこのファイルのハッシュを取得して Bit9 インベントリに配置することができます。

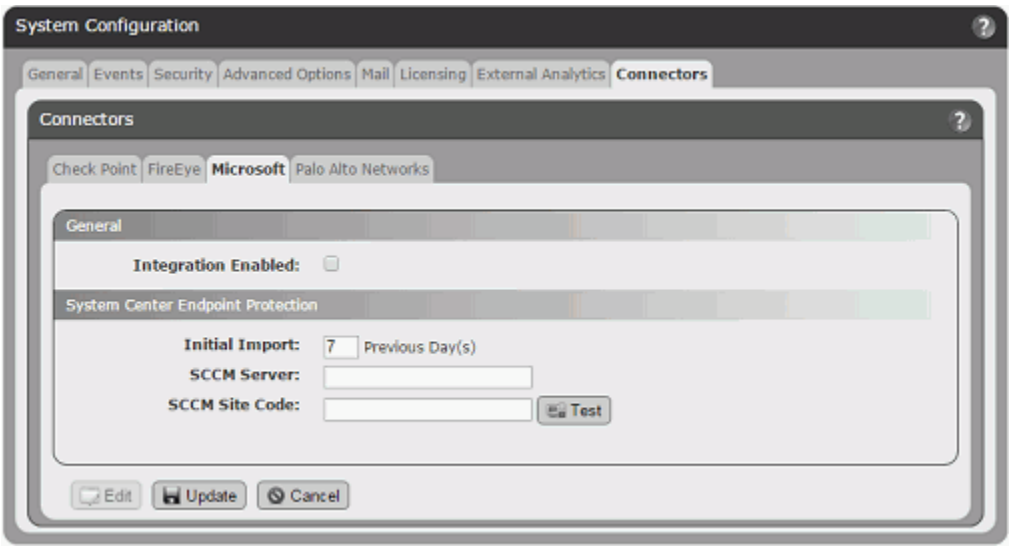
この統合を行うと、脅威のファイル情報を統合できることに加え、Bit9 Server が SCEP 機能（スパイウェア対策、マルウェア対策、エンドポイント保護）のステータスを Bit9 コンソールの［Computer Details（コンピューターの詳細）］ページにレポートできるようになります。

重要

- この統合を成功させるには、「Bit9 Server」サービスを実行するユーザーが SCCM の Read-Only Analyst（読み取り専用アナリスト）アクセス権を持っている必要があります。このユーザーは Bit9 Server インストール中に構成されます。Window タスク マネージャーを開き、右下隅の［サービス］ボタンをクリックするとこのユーザーを確認できます。
- Microsoft Security Essentials 製品ラインとの統合はサポートされていません。

Microsoft SCEP 通知と Bit9 Server との統合を有効化する手順：

1. Bit9 コンソールで、［**Administration**（管理）］>［**System Configuration**（システム構成）］を選択し、［**Connector**（コネクター）］タブ、[**Microsoft**] タブの順にクリックします。
2. ページ下部の［**Edit**（編集）］ボタンをクリックします。



3. ［**Integration Enabled**（統合の有効化）］チェックボックスをオンにします。これは Microsoft SCEP 統合のマスター スイッチです。どの統合機能を有効化するときも、このスイッチをオンにする必要があります。
4. ［Initial Import（初期インポート）］フィールドに、Bit9 にインポートする履歴通知データの日数を入力します。デフォルト値は 7 日間です。この値は、Bit9 Server にまだデータを提供していない SCCM サーバーからのインポートにのみ影響します。Bit9 が既にそのサーバーからデータを提供されている場合、データのインポートは前回のデータの受信日時から再開されます。
5. ［SCCM Server（SCCM サーバー）］フィールドに、サイトの Microsoft SCEP を管理する SCCM サーバー名を入力します。
6. ［SCCM Site Code（SCCM サイト コード）］フィールドに、Configuration Manager 2007 階層でこのサイトの識別に使用される 3 文字のサイト コードを入力します。
7. 初期インポート期間を選択し、サーバー アドレスとサイト コードを入力したら、［**Test**（テスト）］ボタンをクリックして SCCM Server と Bit9 Server が相互に通信できることを確認します。このテストが失敗した場合は、エラー メッセージを使用して構成のトラブルシューティングを行います。
8. テストが成功した場合は、ページ下部の［**Update**（更新）］ボタンをクリックします。
9. SCEP でスキャンしないファイルとして、Bit9 エージェント プロセスと、そのプログラム ディレクトリおよびデータ ディレクトリを必ず追加してください。「Bit9 エージェントのインストール」（133 ページ）を参照した後、特定のプラットフォーム（Windows、Mac、または Linux）におけるインストール手順を読み、除外する特定のファイル名およびディレクトリを確認してください。

統合が完了すると、Bit9 コンソールで SCEP 通知の表示が開始されます。通知を確認するには、Bit9 コンソール メニューで［Report（レポート）］>［External Notification（外部通知）］を選択し、［Saved Views（保存済みビュー）］メニューから［Microsoft Notification（Microsoft 通知）］を選択します。SCEP 通知がまったく表示されない場合は、以下のトラブルシューティング手順を実行できます。

- Bit9 コンソールの［Events（イベント）］ページでサーバー エラーを確認する。
- *Bit9\Parity Server\Reporter\ParityReporter.log* で目的の詳細情報を確認する。
- Bit9 Server サービスを実行しているユーザーが SCCM の Read-Only Analyst（読み取り専用アナリスト）アクセス権を持っていることを確認する。このユーザーは Bit9 Server インストール中に構成されます。Window タスク マネージャーを開き、右下隅の［サービス］ボタンをクリックするとこのユーザーを確認できます。

通知機能の完全な説明（Bit9 コンソールに表示されないように事前にフィルターされる通知のタイプを含む）については、「外部通知」（876 ページ）を参照してください。

SCCM Server が構成され、Bit9 Server と統合されたら、［Connector（コネクター）］ページの [Microsoft] タブを開き、サーバーのステータスを確認できます。ステー

タス インジケーターは［SCCM Server（SCCM サーバー）］フィールドの隣に表示されます。

- 緑の円は統合に問題がないことを示します。
- 赤の円は問題を示し、この場合はインジケーターとともにエラーメッセージが表示されます。
- グレーの円は統合が無効化されていることを示します。

各ステータス インジケーターの円の上にマウスを乗せると、ツールチップに追加情報が表示されます。

SCEP ハッシュ識別の制限

特定の状況下では、SCEP によって隔離または削除された新しいファイルに対して Bit9 がハッシュを生成できない場合があります。つまり、問題のファイルが Bit9 ファイル インベントリに追加されない、または Bit9 ルールの対象にならないことになります。その状況を以下に示します。

- 圧縮ファイルまたは圧縮フォルダーからのマルウェア　　ファイルの抽出に Windows Explorer が使用されたとき
- ファイルがネットワーク共有からエンドポイントにコピーされたとき
- SCEP によってマルウェアとして識別されたファイルが、Bit9 によって実行可能ファイルまたはスクリプトとして追跡されるファイル タイプと異なるとき（たとえば、そのファイルがテキストまたは Word 文書ファイルのとき）。このケースでは、このファイル タイプを Bit9 の追跡対象にするカスタム ルールかスクリプト ルールを作成できますが、このファイル タイプが非常に一般的なものである場合、パフォーマンスに悪影響が及ぶことがあります。

また、他の Bit9 Connector 統合では Bit9 に外部通知が送信されるときにハッシュも提供されますが、SCEP では提供されません。Bit9 イベント ルールでは通常、ファイルへのトリガーやアクション実行のためにハッシュが必要となります。

Bit9 は、ハッシュと SCEP 通知を関連付けるために、通知に含まれる他のデータ（プロセス名、ファイル名、書き込み時間、ユーザー名、コンピューター名など）の相関付けを試みます。この相関付けによって Bit9 ファイル カタログ内のハッシュの特定に成功すると、［External Notification（外部通知）］イベントが処理された後に、このハッシュが［Malicious File Detected（悪意のあるファイルの検出）/ Potential Risk File Detected（危険な可能性があるファイルの検出）］イベントに付加されます。これにより、［Malicious File Detected（悪意のあるファイルの検出）］イベントをベースとするイベント ルールを SCEP 通知によってトリガーできるようになります。

重要

SCEP 通知のファイルと Bit9 ファイル データベースのファイルの相関付けにはハッシュが使用されないため、Bit9 エージェント システム上ではクリーンなファイルが SCEP によって悪質と識別される可能性や、SCEP 通知のみをベースとするイベント ルールがクリーンなファイルに対してトリガーされる可能性があります。そのため、ルールのアクションによっては悪影響が生じることがあります。SCEP 分析結果をプロパティで使用するすべてのイベント ルールで、ファイルの信頼度やファイルの普及度などの追加の要素を使用することを推奨します。

Palo Alto Networks との統合の有効化

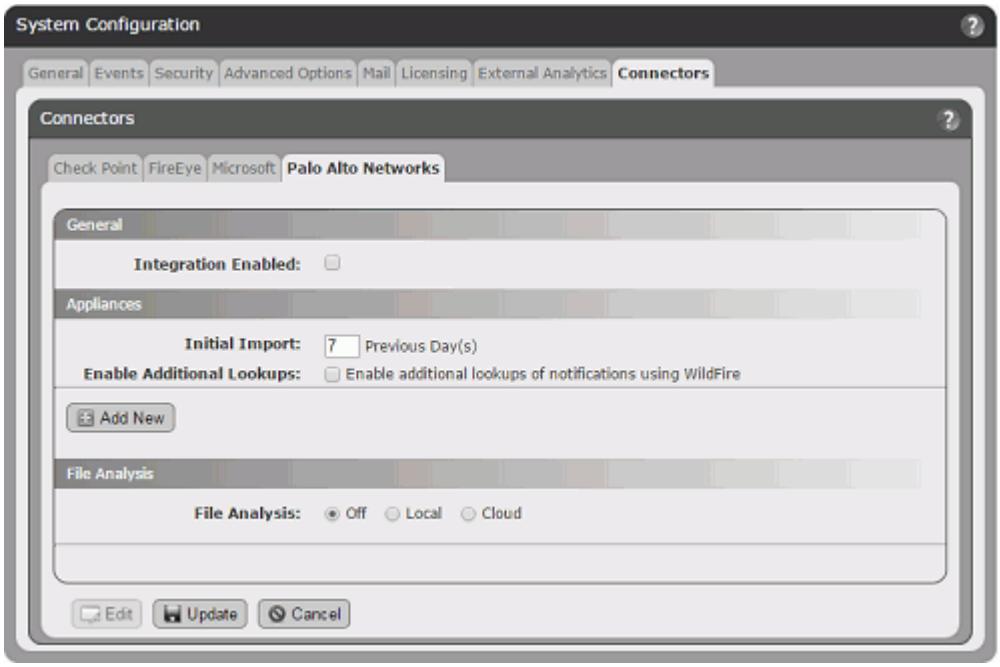
Bit9 Connector for Palo Alto Networks を有効化するには、Bit9 Server と Palo Alto Networks アプライアンスの両方で構成手順を実行する必要があります。通知の統合、WildFire のパブリック クラウドまたはプライベート クラウドによる Bit9 ファイルのファイル分析の統合、または通知と分析両方の統合を有効化できます。

Palo Alto Networks アプライアンスの通知の統合

Palo Alto Networks の複数のアプライアンスの通知を Bit9 Server と統合できます。

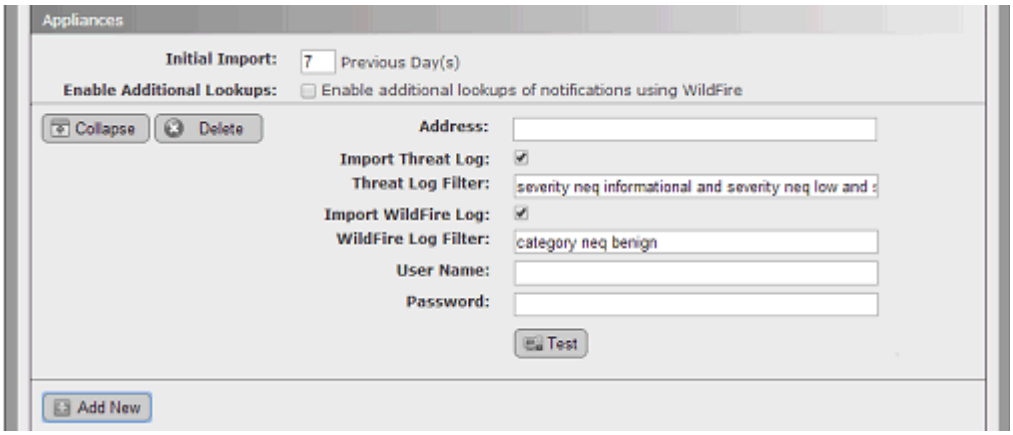
Palo Alto Networks アラートと Bit9 Server との統合を有効化する手順：

1. Palo Alto Networks ファイアウォールと Bit9 Server が相互に通信できることを確認します。
2. Bit9 と統合する各 Palo Alto Networks アプライアンスで、Bit9 統合のための読み取り専用管理権限を持つローカル ユーザー アカウントを作成します。
3. Bit9 コンソールで、[**Administration**（管理）] > [**System Configuration**（システム構成）] を選択し、[**Connector**（コネクター）] タブ、[**Palo Alto Networks**] タブの順にクリックします。
4. ページ下部の［Edit（編集）］ボタンをクリックします。



5. ［**Integration Enabled**（統合の有効化）］チェックボックスをオンにします。このボックスは、Palo Alto Networks 統合のマスター スイッチです。

6. ［Appliances（アプライアンス）］パネルで、［Initial Import（初期インポート）］フィールドに、Bit9 にインポートする履歴通知データの日数を入力します。デフォルト値は 7 日間です。この値は、Bit9 Server にまだデータを提供していないアプライアンスにのみ影響します。Bit9 がすでにそのアプライアンスからデータを提供されている場合、データのインポートは前回のデータの受信日時から再開されます。
7. ファイルの参照が含まれる各通知の完全なマルウェア レポートを取得する場合は、［Enable Additional Lookups（追加検索の有効化）］ボックスをオンにします。
   重要：設定した［Initial Import（初期インポート）］は一度に行われます。［Enable Additional Lookups（追加検索の有効化）］ボックスをオンにした場合は、WildFire クラウド クエリ数がお使いのライセンスの 1 日あたりの限度を超えないように［Initial Import（初期インポート）］期間を選択するようにしてください。
8. ［Palo Alto Networks Integration Settings（Palo Alto Networks 統合設定）］ページの［Appliances（アプライアンス）］セクションで、Bit9 統合にアプライアンスを追加または削除できます。



アプライアンスごとに［Add New（新規の追加）］をクリックし、以下の情報を入力します。

a. ［**Address**（アドレス）］– アプライアンスの IP アドレス。
b. ［**Import Threat Log**（脅威ログのインポート）］– このボックスをオンにすると、このアプライアンスから Bit9 Server の［External Notification（外部通知）］ページへの脅威ログ データのインポートが有効になります。
c. ［**Threat Log Filter**（脅威ログのフィルター）］– このテキスト フィールドは、［External Notification（外部通知）］テーブルに表示されるこのアプライアンスの脅威ログ データを制限するためのフィルターを示しています。デフォルトでは、このフィルターによって、深刻度レベルが「informational（情報）」、「low（低）」、または「medium（中）」の通知が削除されます。このフィルターは、必要な通知を取得するように修正できます。フィルター構文は Palo Alto Networks コンソールで使用されている構文と同じです。

d. ［**Import WildFire Log**（WildFire ログのインポート）］– このボックスをオンにすると、このアプライアンスから Bit9 Server の［External Notification（外部通知）］ページへの WildFire ログ データのインポートが有効になります。

e. ［**WildFire Log Filter**（WildFire ログのフィルター）］– このテキスト フィールドは、［External Notification（外部通知）］テーブルに表示されるこのアプライアンスの WildFire ログ データを制限するためのフィルターを示しています。デフォルトでは、このフィルターによってカテゴリーが「benign（無害）」の通知が削除されます。このフィルターは、必要な通知のみを取得するように修正できます。

f. ［**User Name**（ユーザー名）］および［**Password**（パスワード）］-［User Name（ユーザー名）］および［Password（パスワード）］ボックスに、ステップ 2 で作成した一意のアカウントのユーザー名とパスワードを入力します。
注意：これらのフィールドでは、Palo Alto Networks または Bit9 コンソールのログイン資格情報を使用しないでください。

g. アドレスと資格情報を入力したら、アプライアンスの指定内容を保存する前に、［Test（テスト）］ボタンをクリックして、このアプライアンスがアクセス可能であること、資格情報が適切であること、フィルター構文が有効であることを確認します。

9. 追加のアプライアンスを統合する場合は、［Add New（新規の追加）］をクリックし、他のアプライアンスの必要情報を入力してください。

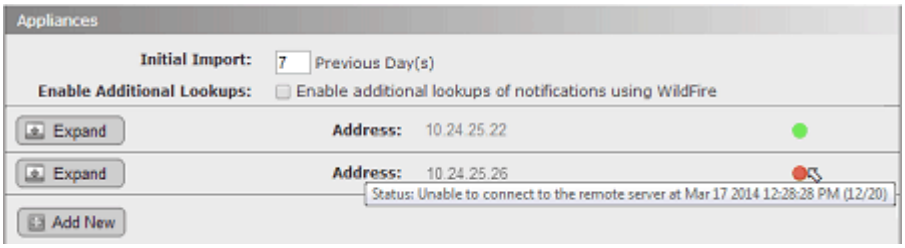
10. ［File Analysis（ファイル分析）］パネルの設定で、Bit9 Server が管理するエージェントのファイルを分析のために WildFire クラウドに送信できるようにするかどうかを決定します。WildFire ファイル分析を有効にする場合、このセクションの構成方法については「分析のための WildFire クラウドとの統合」を参照してください。

11. 統合の構成が終了したら（およびすべてのアプライアンスが上記の［Test（テスト）］に合格したら）、ページ下部にある［**Update**（更新）］ボタンをクリックします。

通知の統合が完了すると、Bit9 コンソールで Palo Alto Networks 通知の表示が開始されます。通知を確認するには、Bit9 コンソール メニューで［**Reports**（レポート）］>［**External Notification**（外部通知）］を選択します。アプライアンス通知の事前フィルターが原因で、通知を即座に確認できない場合があります。通知がまったく表示されない場合は、Bit9 コンソールの［Events（イベント）］ページでサーバー エラーを確認してください。また、
Bit9\Parity Server\Reporter\ParityReporter.log で目的の詳細情報を確認してください。

通知機能の完全な説明（Bit9 コンソールに表示されないように事前にフィルターされる通知のタイプを含む）については、「外部通知」（876 ページ）を参照してください。

Bit9 での Palo Alto Networks 通知アプライアンスのステータス



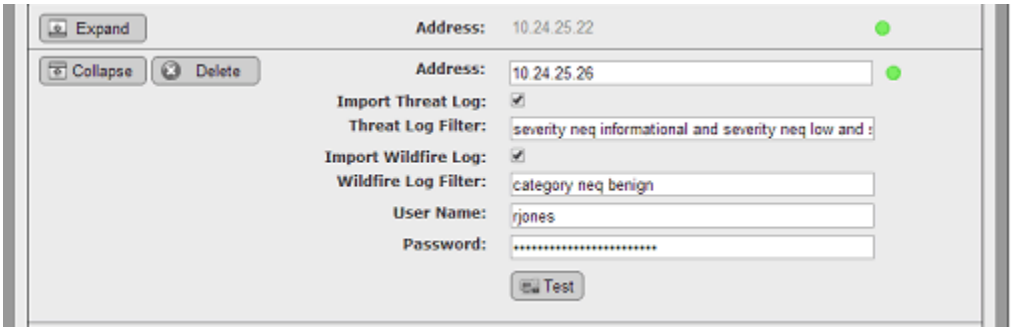
構成が終了すると、Bit9 に通知を送信する各 Palo Alto Networks アプライアンスのステータスが Bit9 コンソールの［System Configuration（システム構成）］/［Connector（コネクター）］/［Palo Alto Networks integration（Palo Alto Networks 統合）］ページに表示されます。［Appliances（アプライアンス）］パネルで、各アプライアンスのアドレスの隣にステータス インジケーターが表示されます。

- 緑の円は、そのアプライアンスの統合に問題がないことを示します。
- 赤の円は問題を示し、この場合はインジケーターとともにエラーメッセージが表示されます。
- 水色の円は、アプライアンスが非アクティブ化されていることを示します。

各ステータス インジケーターの円の上にマウスを乗せると、ツールチップに追加情報が表示されます。

アプライアンス統合の修正または削除

既存の各アプライアンス統合の構成を編集（Bit9 Server への 1 つまたは両方のログのインポートの有効化または無効化など）することができます。また、アプライアンス統合を削除することもできます。



Palo Alto Networks アプライアンス統合の削除または編集手順：

1. ［Connector（コネクター）］/ [Palo Alto Networks] タブで、ページ下部にある［Edit（編集）］ボタンをクリックします。
2. 編集するアプライアンスの隣の［**Expand**（展開）］ボタンをクリックします。そのアプライアンスの構成が表示されます。
3. アプライアンスを統合から削除する場合は、そのアドレスの隣の［**Delete**（削除）］ボタンをクリックします。

4. 脅威ログまたは WildFire ログ データの Bit9 へのインポートを有効化または無効化するには、適切なチェックボックスをオンまたはオフにします。
5. いずれかのログ インポートのフィルターを変更する場合は、対応する［Filter（フィルター）］ボックスのテキストを編集します。
6. インポートの有効化またはフィルターの修正を行った場合は、［**Test**（テスト）］をクリックして、このアプライアンスがアクセス可能であること、およびフィルター構文が有効であることを確認します。
7. ［**Update**（更新）］をクリックして変更を保存します。

分析のための WildFire クラウドとの統合

Bit9 が管理するシステムから、Palo Alto Networks WildFire パブリック クラウド、またはローカルにインストールされた WildFire プライベート クラウド デバイスに、分析のためにファイルをアップロードできるように設定できます。どちらにアップロードした場合も、ファイルは分析され、分析結果が Bit9 コンソールに返されます。

WildFire との統合が完了すると、Bit9 コンソール ページにファイルの表またはファイルの詳細を表示する新しいメニュー選択肢が追加されます。これらの［Analyze with Palo Alto Networks WildFire（Alto Networks WildFire で分析）］コマンドを使用して、WildFire クラウドにファイルをアップロードすることができます。WildFire クラウドへのファイルのアップロード方法と WildFire 分析の結果の表示方法の詳細については、「エンドポイント上の疑わしいファイルの分析」（896 ページ）を参照してください。

注意

Bit9 Server は、1 つまたは複数の WildFire プライベート クラウド アプライアンスまたは WildFire パブリック クラウドに接続できますが、プライベート クラウド分析とパブリック クラウド分析を混在させることはできません。

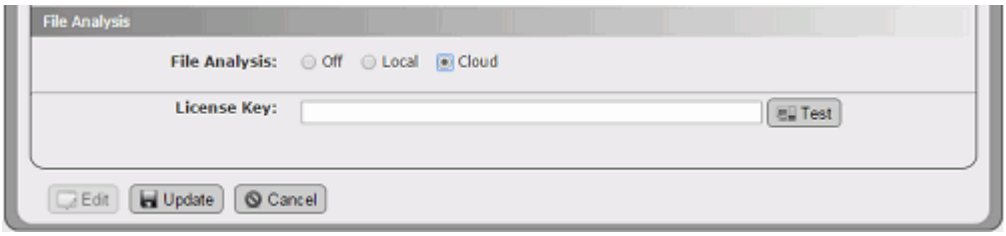
WildFire パブリック クラウドとの統合

Bit9 Platform を WildFire パブリック クラウドと統合する場合は、（プロキシ経由でなく）直接接続する必要があります。

分析のために Palo Alto Networks WildFire パブリック クラウドにファイルをアップロードできるようにする手順：

1. このページをまだ表示していない場合は、Bit9 コンソールで、［**Administration**（管理）］>［**System Configuration**（システム構成）］を選択し、［**Connector**（コネクター）］タブ、[**Palo Alto Networks**] タブの順にクリックします。ページ下部にある［**Edit**（編集）］ボタンをクリックします。

2. ［File Analysis（ファイル分析）］パネルで［Cloud（クラウド）］ボタンをクリックし、［WildFire Key（WildFire キー）］フィールドにお使いの WildFire ライセンス キーを入力します。
   注意：WildFire クラウド サービスでの分析のために Bit9 によって送信されたファイルは、WildFire ライセンス キーの制限の対象になります。



3. ［WildFire Key（WildFire キー）］フィールドの隣の［**Test**（テスト）］ボタンをクリックし、このキー、および WildFire クラウドと Bit9 Server 間の接続を確認します。テストが成功しなかった場合は、失敗メッセージを使用して接続の問題のトラブルシューティングを行います。
4. ［File Analysis（ファイル分析）］パネルで［**File Analysis Enabled**（ファイル分析の有効化）］チェックボックスをオンにします。
5. WildFire　キーのテストに合格し、その他の必要情報の入力（ページ上部の［Integration Enabled（統合の有効化）］）チェックボックスをオンにするなど) が完了したら、［**Update**（更新）］ボタンをクリックして変更を保存します。

WildFire パブリック クラウド クエリの制限

Bit9 で WildFire パブリック クラウド分析を有効化すると、1 日に発生する WildFire クエリ数が増加します。1 日に WildFire に送信されるクエリ数が 1 日あたりの上限を超える場合は、自動ファイル送信を削減または停止するか、送信するファイルを決定するフィルターを修正することを検討してください。

以下の状況では、Bit9 との統合によって WildFire クエリ数が増加します。

- Bit9 が Palo Alto Networks アプライアンスから受信するログでは、WildFire レポートが参照されている場合があります。［Palo Alto Networks Integration（Palo Alto Networks 統合）］ページの［Enable Additional Lookups（追加検索の有効化）］ボックスをオンにすると、参照する必要がある各ログ エントリについて WildFire クラウドにクエリが行われます。クエリ数が上限を超える場合は、この自動クエリを無効化できます。
- 統合を構成した後、Palo Alto Networks アプライアンスから初めて WildFire ログのデータをインポートするときには、［Initial Import（初期インポート）］に設定した日数とその期間内にファイアウォールに存在した WildFire ログ エントリ数によっては、一度に大量のクエリが発生することがあります。
- 分析のために Bit9 からクラウドにファイルを送信するときは、手動の場合もイベント ルールを介した自動送信の場合も、そのファイルのハッシュが既に認識されているかどうかを確認するために 1 つの WildFire クエリが発生します。認識されている場合、そのファイルはアップロードされないため、使用されるのはそのクエリのみです。認識されていない場合は、もう 1 つのクエリを使用してファイルが送信され、さらにもう 1 つのクエリを使用して分析の結果の問い合わせが行われます。

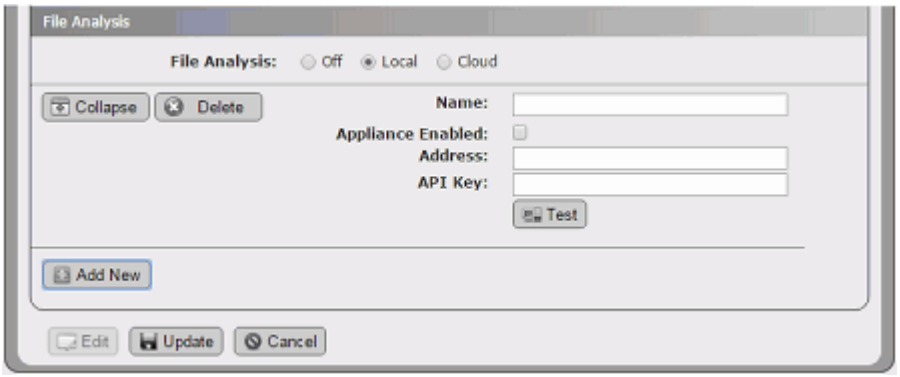
- イベント ルールによって WildFire クラウドへのファイルのアップロードが開始された時点で、既にその日のクエリ上限に到していた場合、そのファイルは処理が翌日まで遅延されます。これによりライセンス カウントをリセットできます。Bit9 は自動的にこの遅延を開始します。[Analyzed file（分析されたファイル）] ページで影響を受けたファイルの [Status（ステータス）] フィールドにマウスを乗せると、この状況がツールチップとしてレポートされます。

WildFire プライベート クラウド デバイスとの統合

分析のためにパブリック クラウド サービスを使用しない、またはできない場合は、Bit9 Platform をローカルにインストールされている WildFire プライベート クラウド デバイスと統合できます。またこの場合は、特定の期間に送信できるクエリ数の上限がなくなります。Bit9 Server には、複数のローカル WildFire アプライアンスを統合することができ、その場合は分析要求が複数のデバイス間に分散されます。

分析のために Palo Alto Networks WildFire プライベート クラウドにファイルをアップロードできるようにする手順：

1. このページをまだ表示していない場合は、Bit9 コンソールで、[**Administration**（管理）] > [**System Configuration**（システム構成）] を選択し、[**Connector**（コネクター）] タブ、[**Palo Alto Networks**] タブの順にクリックします。ページ下部にある [**Edit**（編集）] ボタンをクリックします。
2. [File Analysis（ファイル分析）] パネルで、[Local（ローカル）] ラジオ ボタンをクリックし、次に [Add New（新規の追加）] ボタンをクリックします。ローカル アプライアンスの構成フィールドが表示されます。



3. [Name（名前）] フィールドに、Bit9 構成でのこの WildFire アプライアンスの識別に使用する名前を入力します。
4. [Address（アドレス）] フィールドに、この WildFire アプライアンスの IP アドレスまたはホスト名を入力します。ここには、「http」プレフィックスを持つ URL ではなく、アドレスまたは名前を入力する必要があります。
5. [API Key（API キー）] フィールドにこのアプライアンスの API キーを入力します。
6. [Test（テスト）] ボタンをクリックし、API キー、および WildFire アプライアンスと Bit9 Server 間の接続を確認します。テストが成功しなかった場合は、失敗メッセージを使用して接続の問題のトラブルシューティングを行います。

7. このデバイスの［File Analysis（ファイル分析）］パネルで、［**Appliance Enabled**（アプライアンスの有効化）］チェックボックスをオンにします。
8. ライセンスおよび接続テストに合格し、その他の必要情報の入力（ページ上部の［Integration Enabled（統合の有効化）］）チェックボックスをオンにする、必要に応じて自動検索構成を設定するなど) が完了したら、［**Update**（更新）］ボタンをクリックして変更を保存します。
9. プライベート クラウド アプライアンスをさらに追加する場合は、［**Add New**（新規の追加）］ボタンをクリックし、別のアプライアンスの構成を繰り返します。

Check Point との統合の有効化

Bit9 Connector for Check Point を有効化するには、Bit9 Server と Check Point クラウドまたはアプライアンスの両方で構成手順を実行する必要があります。統合の有効化、ログ サーバーからの通知の構成、Check Point ThreatCloud Emulation Service またはローカル プライベート クラウド アプライアンスによる Bit9 ファイルの分析の有効化を行うことができます。ThreatCloud Emulation Service を使用するには、ライセンス キーが必要です。

Check Point ログ サーバーと Bit9 との統合

複数の Check Point ログ サーバーの通知を Bit9 Server と統合できます。ここで説明する手順を実行するには、Check Point の高度な構成を十分に理解していること、およびその実行権限を持っていることが条件になります。

Check Point ログ サーバーと Bit9 Server との統合の構成手順：

1. Check Point ログ サーバーと Bit9 Server が相互に通信できること、および接続用のポート（デフォルトでは **18184**）がオープンであることを確認します。
2. Check Point ログ サーバー上で LEA サーバーが実行されていることを確認します。実行されていない場合は実行します。
3. Check Point ダッシュボードを使用して、Bit9 Server に接続するための OPSEC アプリケーションを作成します。
   a. 左下のパネルで、［Servers and OPSEC（サーバーと OPSEC）］ボタンをクリックし、［**OPSEC Application**（OPSEC アプリケーション）］を右クリックして［**New OPSEC Application**（新しい OPSEC アプリケーション）］を選択します。
   b. ［Name（名前）］ボックスに、Bit9 接続用のアプリケーションとして明らかに識別できる OPSEC アプリケーション名を入力します（例：**Bit9**、**Bit9_Server**）。
   c. ［Host（ホスト）］メニューで、Bit9 と統合する Check Point ログ サーバーのホスト名を選択します。
   d. ［Client Entities（クライアント エンティティ）］パネルで、[**LEA**] ボックスをオンにします。

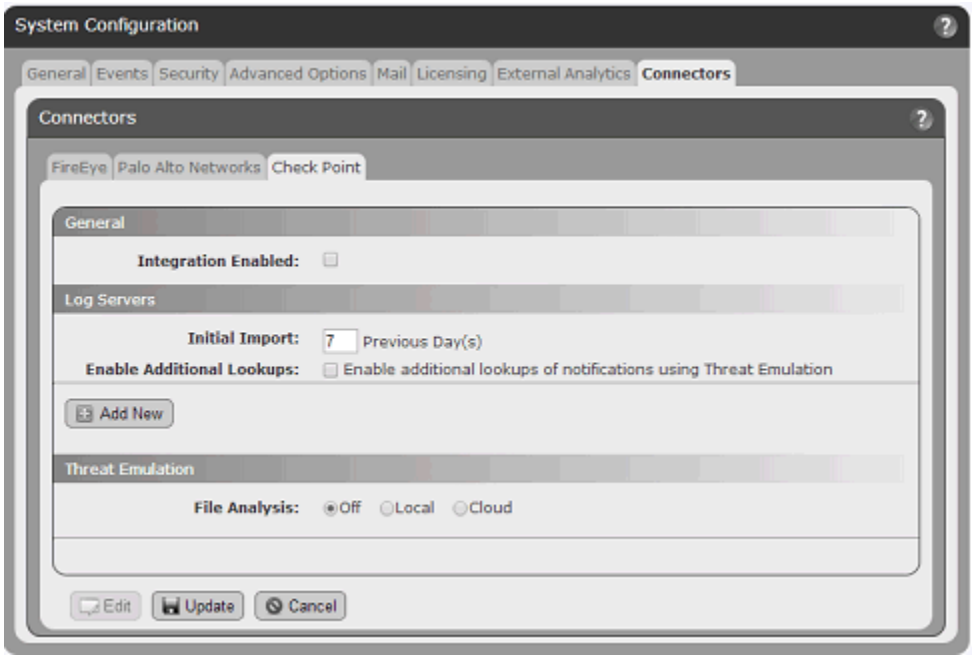
e. ［LEA Permissions（LEA 権限）］タブで、［**Show all log field**（すべてのログ フィールドを表示）］を選択します。

f. ［**Communication**（通信）］ボタンをクリックし、SSLA 証明書ファイルに使用するパスワードを入力します。後で使用するためにこのパスワードのメモを取り、［**Initialize**（初期化）］ボタンをクリックします。初期化が完了したら、［Close（閉じる）］ボタンをクリックしてこのダイアログを閉じます。

g. ［OPSEC Application Properties（OPSEC アプリケーションのプロパティ）］ダイアログで［**Close**（閉じる）］をクリックします。このダイアログは、Bit9 の Check Point の構成ページに [DN] フィールドをコピーするために、後でもう一度開きます。

4. Bit9 コンソールで、［**Administration**（管理）］>［**System Configuration**（システム構成）］を選択し、［**Connector**（コネクター）］タブ、[**Check Point**] タブの順にクリックします。

5. ページ下部の［**Edit**（編集）］ボタンをクリックします。



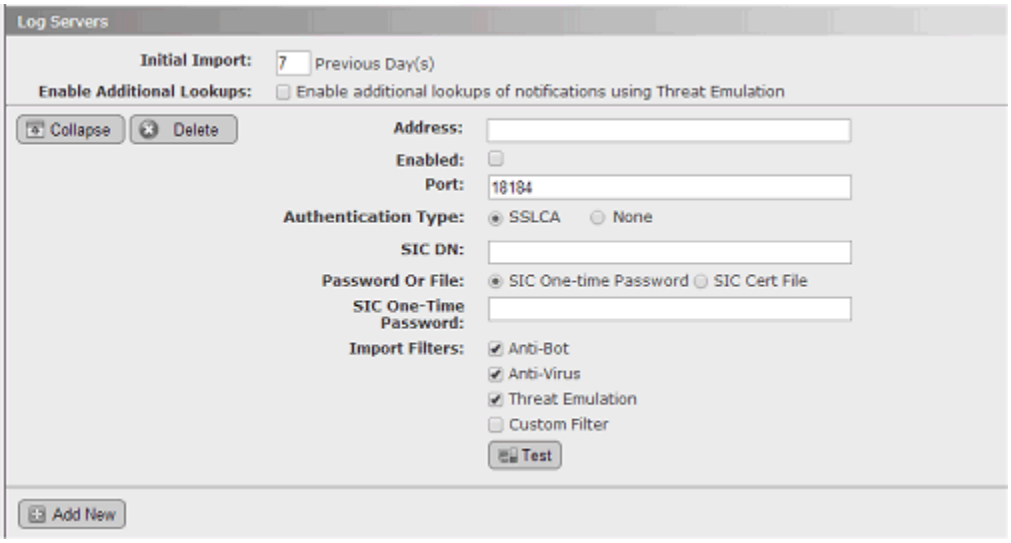
6. ［**Integration Enabled**（統合の有効化）］チェックボックスをオンにします。これは Check Point 統合のマスター スイッチです。どの統合機能を有効化するときも、このチェック ボックスをオンにする必要があります。

7. ［Log Servers（ログ サーバー）］パネルで、［Initial Import（初期インポート）］フィールドに、Bit9 にインポートする履歴通知データの日数を入力します。デフォルト値は 7 日間です。この値は、Bit9 Server にまだデータを提供していないログ サーバーにのみ影響します。Bit9 がすでにそのログ サーバーからデータを提供されている場合、データのインポートは最後のデータの受信時間から再開されます。

8. ［Enable Additional Lookups（追加検索の有効化）］チェックボックスによって、Check Point ログ サーバーから受信する情報量が決まります。脅威エミュレーション通知で参照されている各ファイルの完全なマルウェア レポートを取得する場合は、このボックスをオンにします。この検索は、構成に応じて、ThreatCloud Emulation サービス、またはローカルの Threat Emulation プライベート クラウド アプライアンスで行われます。

   重要：設定した［Initial Import（初期インポート）］は一度に行われます。初期インポート中に［Enable Additional Lookups（追加検索の有効化）］が有効な場合は、パフォーマンスに大きな影響が及ぶことがあります。また追加検索を有効にした場合は、Check Point Threat Emulation クラウド クエリ数がお使いのライセンスの限度を超えないように注意して［Initial Import（初期インポート）］期間を選択してください。詳細については、「ThreatCloud Emulation の検索の制限」（865 ページ）を参照してください。

9. [Check Point] ページの［Log Servers（ログ サーバー）］セクションで、［**Add New**（新規の追加）］をクリックして新しいサーバーの構成パネルを開きます。このパネルでは、Check Point ログ サーバーと Bit9 Server 間の統合と接続の追加、構成、削除を行うことができます。



10. ［Address（アドレス）］フィールドに、ログ サーバーの IP アドレスを入力します。

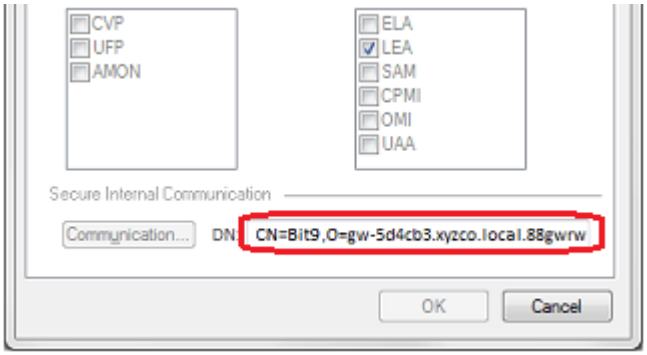
11. ［Enabled（有効化）］ボックスをオンにし、Bit9 Server とこのログ サーバー間の接続を有効化します。この統合は、その他の構成データを失わずに有効化または無効化できます。

12. ［Port（ポート）］フィールドに、Bit9 Server と Check Point ログ サーバーの接続に使用するポートを入力します。デフォルトのポートは **18184** です。

13. ［Authentication（認証）］フィールドで、これらのサーバー間の通信を保護するかしないかを選択します。サーバー間の通信を平文で行うようにするには、［None（なし）］ラジオ ボタンをクリックし、手順 14 をスキップします。

保護された通信を使用する場合は、**[SSLCA]** ラジオ ボタンをクリックして（デフォルト）、以下の情報を入力します。

a. **[SIC DN]** – このセキュリティ内部通信 (SIC) 識別名は、Bit9 Server と Check Point ログ サーバー間の通信を保護するために必要です。Check Point ダッシュボードで、Bit9 用に作成した OPSEC アプリケーションの［Edit（編集）］ダイアログを開きます。［OPSEC Application Properties（OPSEC アプリケーションのプロパティ）］ダイアログの [DN] フィールドを、Bit9 コンソールの [SIC DN] フィールドにコピーします。



b. ［**Password or File**（パスワードまたはファイル）］– Check Point ログ サーバー用の SSL 証明書を Bit9 Server にダウンロードする方法を制御するラジオ ボタンです。

- パスワードを入力してログサーバーから証明書ファイルをダウンロードするには、［**SIC One-time Password**（SIC ワンタイム パスワード）］を選択します。このオプションを選択すると、［**SIC One-Time Password**（SIC ワンタイム パスワード）］ボックスが開きます。ここに Check Point ダッシュボードでBit9 OPSECアプリケーションを作成したときに作成したパスワードを入力します。
- 以前にダウンロードした証明書ファイルを使用するには、［**SIC Cert File**（SIC 証明書ファイル）］を選択します。このオプションを選択すると、［**SIC Cert File**（SIC 証明書ファイル）］ボックスが開きます。ここに証明書ファイル名を入力します。この証明書のデフォルト名は ops1.tmp です。

14. ［Import Filters（インポート フィルター）］セクションでは、Check Point ログ サーバーからインポートするデータを制御します。3 つの Check Point モジュール タイプに対応する **[Anti-bot]、[Anti-Virus]、[Threat Emulation] の 3 つのチェックボックスの選択肢が用意されています。**デフォルトではすべてがオンになっていますが、どのモジュールのデータのインポートも無効化できます。また［Custom Filter（カスタム フィルター）］も選択できます。このオプションを選択すると、3 つの製品固有の選択肢が無効化され、データ インポートを制御する特別なフィルターを作成できます。この機能の使用方法の詳細については、「Check Point 用カスタム インポート フィルター」を参照してください。

15. アドレス、資格情報、フィルターを入力したら、構成を保存する前に［**Test**（テスト）］ボタンをクリックして、このログ サーバーがアクセス可能であること、およびフィルター構文が有効であることを確認してください。［SIC One-Time Password（SIC ワンタイム パスワード）］を入力し、証明書ファイルが正常にダウンロードされた場合は、このファイルが構成の設定に追加されます。
16. 追加のログ サーバーを統合する場合は、［**Add New**（新規の追加）］ボタンをクリックし、手順 10 ～ 15 に従って他のログ サーバーの必要情報を入力してください。
17. Bit9 Server が管理するエージェントのファイルを Check Point に送信して分析できるかどうかは、［File Analysis（ファイル分析）］セクションの構成で決まります。Check Point ファイル分析を有効にする場合、このセクションの構成方法については「分析のための Check Point との統合」を参照してください。
18. 統合の構成が終了したら（およびすべてのログ サーバーが上記のテストに合格したら）ページ下部にある［**Update**（更新）］ボタンをクリックします。

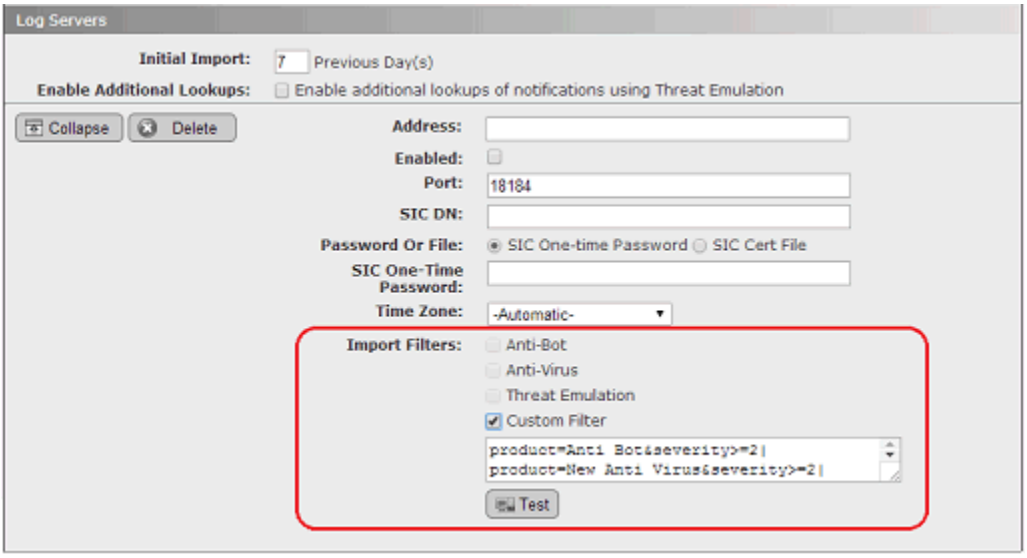
通知の統合が完了すると、Bit9 コンソールで Check Point ログ サーバーからの通知の表示が開始されます。通知を確認するには、Bit9 コンソール メニューで［**Reports**（レポート）］>［**External Notification**（外部通知）］を選択します。ログ サーバー通知の事前フィルターが原因で、通知を即座に確認できない場合があります。通知がまったく表示されない場合は、Bit9 コンソールの［Events（イベント）］ページでサーバー エラーを確認してください。また、以下のログで目的の詳細情報を確認してください。

- *Bit9\Parity Server\Reporter\ParityReporter.log*
- *Bit9\Integrations\CheckPoint\Bin\B9ConnectorCP.bt9*

通知機能の完全な説明（Bit9 コンソールに表示されないように事前にフィルターされる通知のタイプを含む）については、「外部通知」（876 ページ）を参照してください。

Check Point 用カスタム インポート フィルター

Check Point ログ サーバーから Bit9 にインポートするデータを決定するために、[**Anti-bot**]、[**Anti-Virus**]、[**Threat Emulation**] の 3 つの標準オプションが用意されています。特別なフィルターが必要な場合は、［System Configuration（システム構成）］ページで［Connector（コネクター）］タブ、[Check Point] タブの順に選択し、［Import Filters（インポート フィルター）］フィールドで［Custom Filter（カスタム フィルター）］チェックボックスをオンにします。このボックスをオンにすると、他のフィルター チェックボックスがオフになり、［Custom Filter（カスタム フィルター）］テキスト ボックスが開きます。フィルターはすべてログ サーバー側で実行されるため、ログ サーバーと Bit9 Server 間のネットワーク トラフィックが低減されます。



まず［Custom Filter（カスタム フィルター）］ボックスには、[Anti-bot]、[Anti-Virus]、および [Threat Emulation] チェックボックスがオンの場合と同じフィルタリングを実行するフィルターが表示されます。このデフォルトのカスタム フィルターの内容を確認して、フィルター構文を理解するようにしてください。これらのフィルターに追加や編集を行うことも、空白のフィルター ウィンドウから作成を開始することもできます。フィルター ウィンドウのサイズを変更するには、マウスの左ボタンを押しながら右下隅をドラッグします。

フィルターは、Check Point ログの属性、演算子、属性に指定する値で構成されます。以下に例を示します。

```
severity>=medium
```

深刻度「medium（中）」以上の通知が［External Notifications（外部通知）］テーブルにインポートされます。

フィルター条件は、以下の演算子の表で説明されている AND および OR 演算子を使用して組み合わせることができます。以下に例を示します。

```
product=Threat Emulation&verdict=Malicious
```

このフィルターの条件は、製品が「Threat Emulation」で、かつ判定が「Malicious（悪質）」です。

ボックスにカスタム フィルターを入力したら、［Test（テスト）］ボタンを使用してフィルター構文が有効であることを確認します。テストが正常に実行されると、構文が検証され、Bit9 Server と Check Point サーバーとの接続が確認されますが、Check Point データが実際にこのフィルターに一致するかどうかはわかりません。

表 119 に、フィルターの演算子とその使用例を示します。

表 119：Check Point カスタム フィルターの演算子

演算子	説明	例
=	等しい	src=10.0.3.5
=	属性が存在する（パラメーターがない場合）	verdict=
!=	等しくない	verdict!=benign
!=	属性が存在しない（パラメーターがない場合）	verdict!=
>=	以上	severity>=medium
<=	以下	severity<=low
%=	文字列を含む	emulated_on%=Windows 7
~=	文字列を含まない	emulated_on~=Windows XP
= ,	属する（グループに使用）	product=Anti Virus,New Anti Virus
&	AND（フィルターの組み合わせに使用）	severity>medium&verdict=benign **注意**：AND と OR を組みわせる場合、常に AND を内部演算とし、OR を外部演算とする必要があります。以下に例を示します。 product=Anti Malware&severity>=medium| product=New Anti Virus&severity>=medium
|	OR（フィルターの組み合わせに使用）	severity>medium&verdict=benign|verdict=malicious

注意

以下のカスタム フィルターの制限に注意してください。

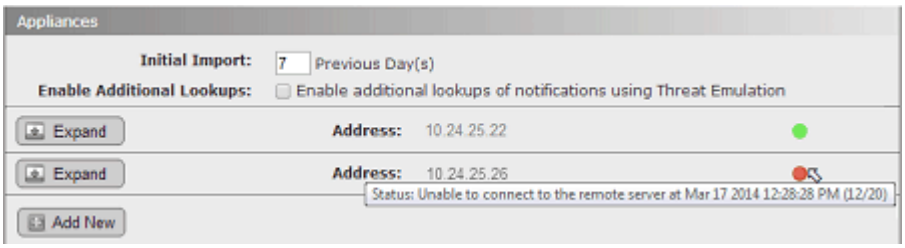
- 引用符はサポートされていません。
- 演算子の優先順位付けや式のグループ化のための括弧はサポートされていません。
- 時間によるフィルタリングはサポートされていません。
- ネットワーク アドレスによるフィルタリングでは、ネットワーク マスクを使用できません。

表 120 に、カスタム フィルターで使用可能な Check Point ログの属性の一部を示します。すべての属性のリストは、Check Point LEA のフィールド ガイドに収録されています。

表 120：フィルターで使用される Check Point ログの属性の例

Check Point ログの属性（大文字と小文字の区別あり）	説明
src	ソース ホスト名または IP アドレス
dst	宛先ホスト名または IP アドレス
orig	ログ エントリを生成するファイアウォールのホスト名
severity	ログ エントリの深刻度（n/a、low（低）、medium（中）、high（高）、critical（クリティカル））
Confidence Level	イベントの信頼レベル
verdict	脅威エミュレーションの判定（benign（無害）、malicious（悪質））
src_user_name	Check Point で Identity Awareness が使用されている場合は、ソース ユーザー名
product	ログ エントリの生成に使用されたソフトウェア製品（ブレード）（Anti Malware、Anti Virus、New Anti Virus、Threat Emulation）
Protection name	Check Point によってレポートされたマルウェア名
file_type	ファイル タイプ（PDF、EXE など）
file_size	ファイルのサイズ（バイト単位）
analyzed_on	脅威エミュレーション分析が実行された場所（Check Point Threat Cloud またはローカル エミュレーション アプライアンスのホスト名）

Bit9 での Check Point ログ サーバーのステータス



構成が終了すると、Bit9 Server と統合された各 Check Point ログ サーバーのステータスが、Bit9 コンソールの［System Configuration（システム構成）］/［Connector（コネクター）］/ [Check Point] ページに表示されます。［Log Servers（ログ サーバー）］パネルで、各アプライアンスのアドレスの隣にステータス インジケーターが表示されます。

- 緑の円は、そのログ サーバーの統合に問題がないことを示します。
- 赤の円は問題を示し、この場合はインジケーターとともにエラーメッセージが表示されます。

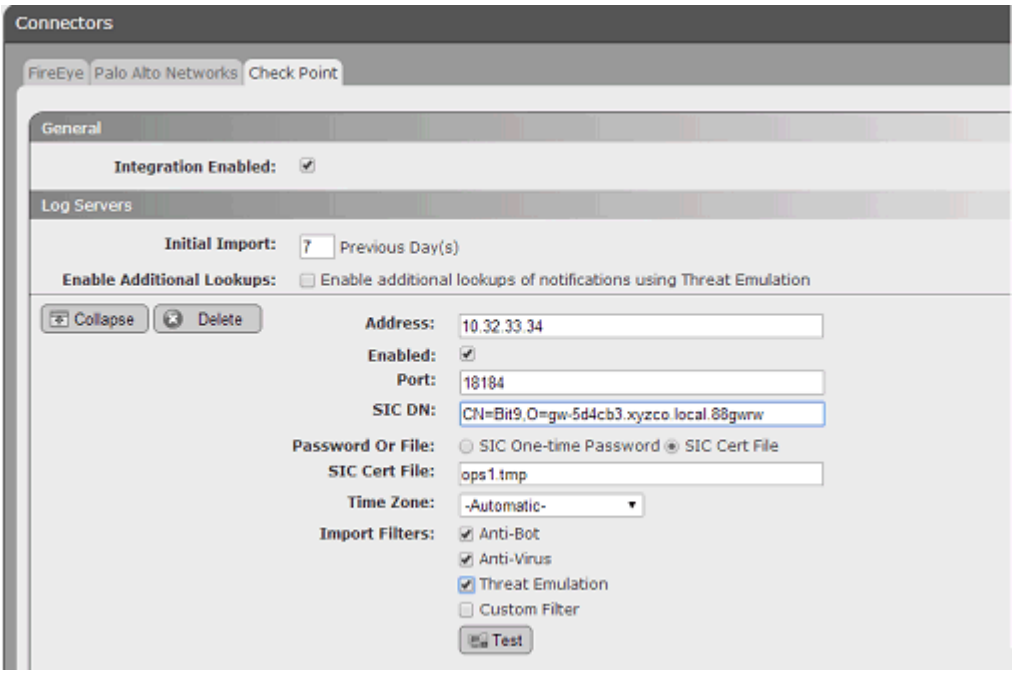
- 水色の円は、ログ サーバーが非アクティブ化されていることを示します。

各ステータス インジケーターの円の上にマウスを乗せると、ツールチップに追加情報が表示されます。

ログ サーバー接続エラーは、Bit9 の［Events（イベント）］ページと［External Notification（外部通知）］ページにも［Server Error（サーバー エラー）］イベントとして表示されます。

ログ サーバー統合の修正または削除

既存の各アプライアンス統合の構成を編集（1 台または複数のログ サーバーから Bit9 Server への通知の有効化または無効化など）することができます。また、統合から 1 台のログ サーバーを削除することも、Check Point との統合全体を無効化することもできます。



Check Point ログ サーバー統合の削除または編集手順：

1. ［Connector（コネクター）］/ [Check Point] タブで、ページ下部にある［**Edit**（編集）］ボタンをクリックします。
2. 編集するアプライアンスの隣の［**Expand**（展開）］ボタンをクリックします。そのアプライアンスの構成が表示されます。
3. アプライアンスを統合から削除する場合は、そのアドレスの隣の［**Delete**（削除）］ボタンをクリックします。
4. Bit9 へのログ　データのインポートを有効化または無効化するには、適切なチェックボックスをオンまたはオフにします。
5. ログ インポートのフィルターを変更する場合は、標準フィルター ボックスをオンまたはオフにするか、［Custom Filter（カスタム フィルター）］ボックスのテキストを編集します。

6. その他の必要な変更を加えます。
7. ［**Test**（テスト）］をクリックして、このアプライアンスがアクセス可能であること、およびフィルターが有効であることを確認します。
8. ［**Update**（更新）］をクリックして変更を保存します。

分析のための Check Point との統合

Bit9 が管理するシステムのファイルを Check Point Threat Emulation サービス、またはローカルの Threat Emulation アプライアンスにアップロードして分析し、結果を Bit9 コンソールに表示するように設定できます。それには、[Check Point] の構成ページの［Threat Emulation（脅威エミュレーション）］パネルを使用します。

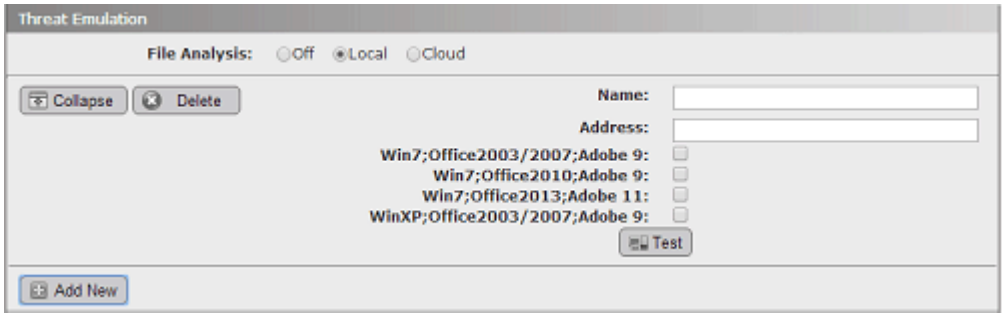
注意

Bit9 は、Check Point HTML レポートの下部に表示される、「unexpected activities by time（時間別の予期しないアクティビティ）」という名前の Check Point レポートの一部のデータのみの相関付けを行います。

Threat Emulation アプライアンスへの接続

Check Point Threat Emulation アプライアンスにファイルをアップロードできるようにする手順：

1. Bit9 コンソールで、［**Administration**（管理）］>［**System Configuration**（システム構成）］を選択し、［**Connector**（コネクター）］タブ、[**Check Point**] タブの順にクリックします。
2. ［**Edit**（編集）］ボタンをクリックします。
3. ［Threat Emulation（脅威エミュレーション）］パネルで、［**Local**（ローカル）］ラジオ ボタンをクリックし、次に［**Add New**（新規の追加）］ボタンをクリックします。



4. この Threat Emulation アプライアンスを Bit9 構成で識別するために使用する名前を入力します。
5. この Threat Emulation アプライアンスの IP アドレスを入力します。

6. Bit9 Server から分析対象のファイルを送信する各分析環境のボックスをオンにします。Threat Emulation アプライアンス上で構成されている分析環境のみを選択するようにしてください。Bit9 は、ローカルの Threat Emulation アプライアンス上でサポートされている環境をプログラム的に特定することができません。
7. ［Test（テスト）］ボタンをクリックし、Threat Emulation アプライアンスのアドレスと、このアプライアンスおよび Bit9 Server 間の接続を確認します。テストが成功しなかった場合は、失敗メッセージを使用して接続の問題のトラブルシューティングを行います。発生しうる問題の 1 つは、ポートの不一致です ThreatCloud Emulation Service への接続のためのデフォルト ポートは 443 ですが、ローカル アプライアンスは **18194** を使用する必要があります。

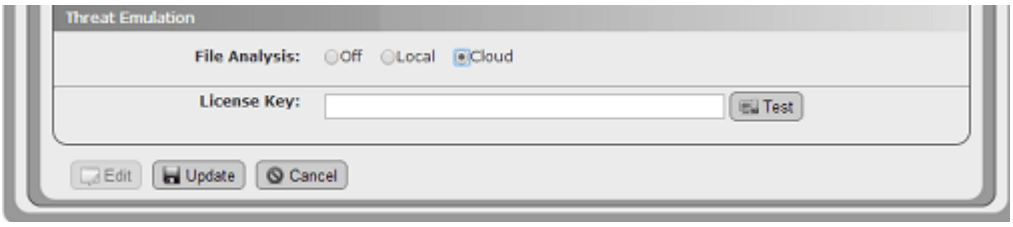
   注意：このページのテストで、Check Point 構成のすべての問題が検出されるわけではありません。たとえば、現存しない環境を構成した場合でも、それがテストで検出されないため、その環境を必要とするアクションは失敗します。
8. テストに合格し、その他の必要情報の入力が完了したら、［**Update**（更新）］ボタンをクリックして変更を保存します。

分析の構成が完了すると、Bit9 コンソールのページにファイル テーブル、またはファイルの詳細を表示する新しいメニューが表示されます。これらの［**Analyze File with Check Point**（Check Point でファイル分析）］コマンドを使用して、Check Point にファイルをアップロードすることができます。Check Point へのファイルのアップロード方法と Check Point 分析の結果の表示方法の詳細については、「エンドポイント上の疑わしいファイルの分析」（896 ページ）を参照してください。

ThreatCloud Emulation Service への接続

分析のために Check Point クラウドにファイルをアップロードできるようにする手順：

1. Bit9 コンソールで、［**Administration**（管理）］>［**System Configuration**（システム構成）］を選択し、［**Connector**（コネクター）］タブ、[**Check Point**] タブの順にクリックします。
2. ［**Edit**（編集）］ボタンをクリックします。
3. ［Threat Emulation（脅威エミュレーション）］パネルで、［**Cloud**（クラウド）］ラジオ ボタンをクリックします。
4. ［Threat Emulation（脅威エミュレーション）］パネルで、お使いの Check Point Threat Emulation クラウド サービスのライセンス キーを入力します。



5. ［License Key（ライセンス キー）］フィールドの隣の［**Test**（テスト）］ボタンをクリックし、このキー、および Check Point と Bit9 Server 間の接続を確認します。テストが成功しなかった場合は、失敗メッセージを使用して接続の問題のトラブルシューティングを行います。

> **注意**
>
> 分析のために Bit9 Server から Check Point Threat Emulation サービスにファイルを送信する際にプロキシ サーバーを使用する必要がある場合は、［System Configuration（システム構成）］ページの［Licensing（ライセンス）］タブを使用してその構成を行えます。［Bit9 SRS Proxy Settings（Bit9 SRS プロキシ設定）］パネルのフィールドに、プロキシ サーバー アドレスを入力できます。この設定は、Check Point に送信されるファイルと Bit9 SRS に使用され、［Test（テスト）］をクリックしたときにプロキシにレポートされます。「Bit9 SRS の有効化」（787 ページ）を参照してください。

6. ライセンス　キーがテストに合格し、その他の必要情報の入力が完了したら、［**Update**（更新）］ボタンをクリックして変更を保存します。

分析の構成が完了すると、Bit9 コンソールのページにファイル テーブル、またはファイルの詳細を表示する新しいメニューが表示されます。これらの［**Analyze File with Check Point**（Check Point でファイル分析）］コマンドを使用して、Check Point にファイルをアップロードすることができます。Check Point へのファイルのアップロード方法と Check Point 分析の結果の表示方法の詳細については、「エンドポイント上の疑わしいファイルの分析」（896 ページ）を参照してください。

ThreatCloud Emulation の検索の制限

ThreatCloud Emulation Service 分析を Bit9-Check Point 統合に追加する場合は、Check Point クエリ数の上限を考慮してください。クエリの増加は、［Enable Additional Lookups（追加検索の有効化）］をオンにすると特に著しくなります。この構成では、外部通知で参照されているファイルが悪質と判定されており、このレポートの検索がまだ行われていない場合に、ThreatCloud Emulation Service にこのファイルに関する完全なレポートが要求されるためです。詳細については、「Threat Emulation の自動検索の有効化」を参照してください。

お使いの Check Point ログ サーバー アプライアンスからの 1 日あたりのクエリ数の合計が ThreatCloud Emulation Service の検索の上限を超えた場合は、Check Point に連絡してライセンス キーを拡張してください。

Threat Emulation の自動検索の有効化

[Check Point] の構成ページで［Enable Additional Lookups（追加検索の有効化）］をオンにすると、返されるレポ ― トの検索数と詳細レベルの両方に影響します。

ThreatCloud Emulation Service を使用している場合、自動検索数はライセンス キーで指定されている毎時および毎月の限度に影響します。通知を初めて有効化したときに自動検索を有効にした場合、特に以前の数日分の通知の入力を要求したときなど、すぐに 1 日あたりの上限に達する可能性があります。

ローカルの Threat Emulation アプライアンスを使用している場合は、検索数の上限はありません。

分析のためにファイルを送信したとき、受信されるレポートの内容は以下のように変化します。

- ［**Enable Additional Lookups**（追加検索の有効化）］が「オフ」の場合（デフォルト）– Threat Emulation ログからの通知には、最上位のマルウェア ファイルと、そのハッシュ、そのファイル サイズが含まれます。
- ［**Enable Additional Lookups**（追加検索の有効化）］が「オン」の場合 – Threat Emulation ログからの通知の判定が悪質で、この通知の検索がまだ実施されていない場合に、自動検索が行われます。検索の結果として、ファイル名、レジストリ エントリに加え、展開されたファイル名とレジストリの変更も返されますが、ファイルのハッシュとファイルのサイズは含まれません。

FireEye 統合の有効化

Bit9 Connector for FireEye を有効化するには、Bit9 Server と FireEye コンソールの両方で構成手順を実行する必要があります。統合には 2 つのレベルがあります。

- 「通知のみ」の統合を有効化できます。
- 通知とファイル分析両方の統合を有効化できます。

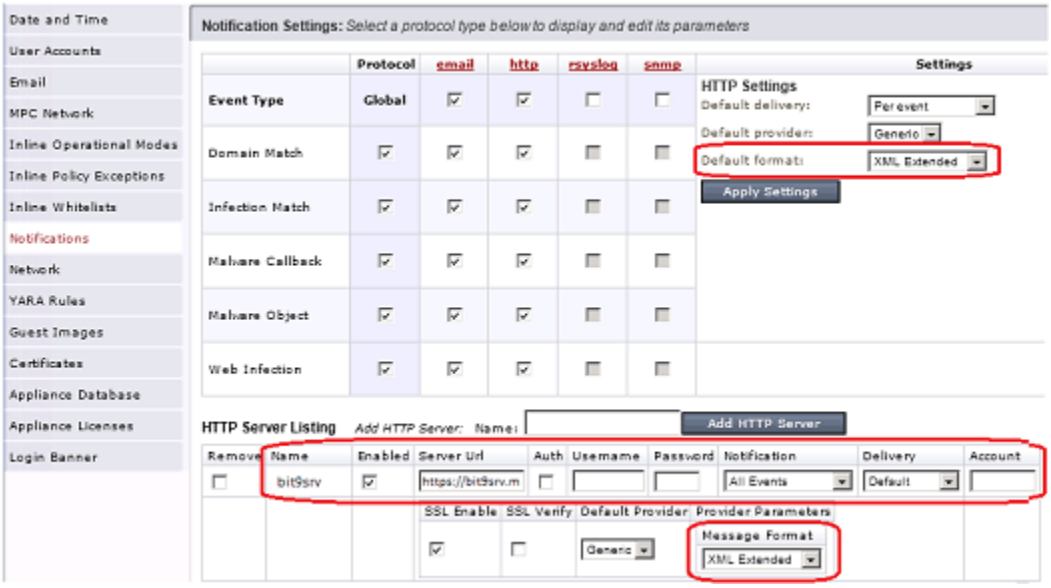
パフォーマンスと帯域幅の考慮事項

FireEye から受信する通知は IIS によって処理され、各データのサイズは 2KB から 20MB 以上まで範囲に幅があります。サイズが大きい通知を頻繁に受信すると、コンソールのパフォーマンスに影響する可能性があります。また、外部通知による大きな負荷は、Bit9 Server とそのデータベースに影響を及ぼすことがあります。

FireEye 通知との統合

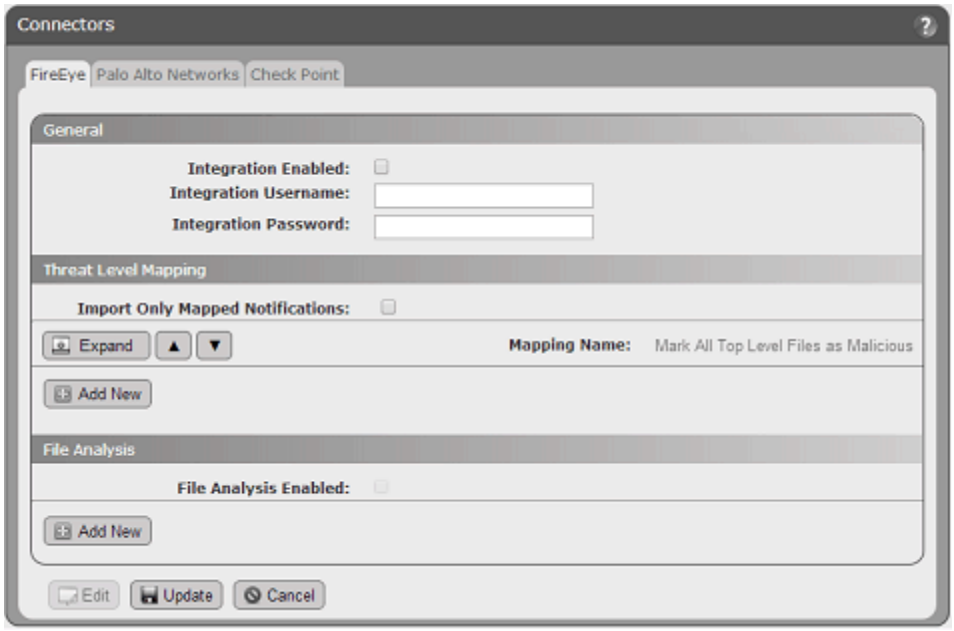
FireEye 通知と Bit9 Server との統合を有効化する手順：

1. FireEye と Bit9 Server が相互に通信できることを確認します。
2. FireEye コンソールで、［**Settings**（設定）］>［**Notifications**（通知）］を選択します。



3. ［Notification Settings（通知の設定）］ページで、新しい HTTP リスナーを追加して構成します。
   a. [**http**] 列ヘッダーをクリックして、[HTTP Server Listing（HTTP サーバー リスト）］を表示します。
   b. ［Add HTTP Server（HTTP サーバーの追加）］ボックスに新しいサーバーの名前を入力し、［**Add HTTP Server**（HTTP サーバーの追加）］ボタンをクリックします。
   c. ［Server URL（サーバー URL）］ボックスに、Bit9 Server 上のリスナー ファイルの URL を入力します。
      https://*<Bit9Server>***/fireeye/listener.ashx**
   d. ［Message Format（メッセージ形式）］メニューで、［**XML Extended**（XML 拡張）］を選択します。
   e. ［**SSL Enable**（SSL 有効）］ボックスがオンになっていることを確認します。
   f. 認証が必要な場合は、［**Auth**（認証）］チェックボックスをオンにし、使用するユーザー名とパスワードを入力します。認証が不要な場合は、両方を空白にして、ボックスをオフにします。
      注意：これらのフィールドでは、FireEye または Bit9 コンソールのコンソール ログイン資格情報を使用しないでください。これはドメイン アカウントではありません。Bit9 コンソールの［System Configuration（システム構成）］ページの [FireEye] タブにも入力する一意のユーザー名とパスワードを使用します。
   g. 右上の［HTTP Settings（HTTP 設定）］セクションで、[Default Delivery（デフォルト提供）］設定が［**Per event**（イベントごと）］になっていることを確認します。
   h. このページの構成が終了したら、［**Update**（更新）］ボタンをクリックします。

4. Bit9 コンソールで、[**Administration**（管理）] > [**System Configuration**（システム構成）] を選択し、[**Connector**（コネクター）] タブ、[**FireEye**] タブの順にクリックします。
5. ページ下部の [**Edit**（編集）] ボタンをクリックします。



6. [**Integration Enabled**（統合の有効化）] チェックボックスをオンにします。このボックスは、FireEye 統合のマスター スイッチです。
7. 認証が必要な場合は、[Integration Username（統合ユーザー名）] ボックスにユーザー名を入力し、[Integration Password（統合パスワード）] ボックスにパスワードを入力します。認証が不要な場合は、両方のボックスを空白にします。

   注意：これらのフィールドでは、FireEye または Bit9 コンソールのコンソール ログイン資格情報を使用しないでください。FireEye コンソールの [FireEye Notification Settings（FireEye 通知設定）] の [Auth（認証）] セクションに入力した、一意のユーザー名とパスワードを使用します。
8. [Threat Level Mapping（脅威レベル マッピング）] で、FireEye から受信する通知深刻度レベルを、Bit9 脅威レベルにどのようにマッピングするかを決定します。デフォルトのマッピングでは、FireEye ファイル通知は深刻度に関係なくすべて Bit9 の「悪質」脅威レベルにマッピングされます。デフォルト マッピング ルールのマッピングは変更でき、ルールを追加して FireEye のさまざまな深刻度を Bit9 のさまざまな深刻度レベルにマッピングすることもできます。詳細については、「FireEye 脅威レベル マッピング」（872 ページ）を参照してください。

9. Bit9 Server が管理するエージェントのファイルを FireEye アプライアンスに送信して分析できるかどうかは、[File Analysis（ファイル分析）] セクションの構成で決まります。FireEye を利用したファイル分析を有効にする場合、このセクションの構成方法については「分析のための FireEye との統合」を参照してください。
10. 統合の構成が終了したら、ページ下部にある［**Update**（更新）］ボタンをクリックします。
11. FireEye コンソールで、［**Settings**（設定）］>［**Notifications**（通知）］を開き、［Malware-object notification type（マルウェア - オブジェクト通知タイプ）］で［**Test-Fire**（テスト - Fire）］を選択します。数分以内に Bit9 に通知が表示されます。この検証の後、Bit9 コンソールの［Administration（管理）］/［System Administration（システム管理）］/［Connector（コネクター）］/ [FireEye] タブページに表示される FireEye 統合ステータスは、緑の円になります。

通知の統合が完了すると、Bit9 コンソールで FireEye 通知の表示が開始されます。通知を確認するには、コンソール メニューで［**Reports**（レポート）］>［**External Notification**（外部通知）］を選択します。通知が表示されない場合は、Bit9 の［Events（イベント）］ページでサーバー エラー イベントを確認してください。また、\Bit9\Integrations\FireEye\listener で、debug.log ファイルにエラーがないかどうかも確認してください。

通知機能の詳しい説明については、「外部通知」を参照してください。

分析のための FireEye との統合

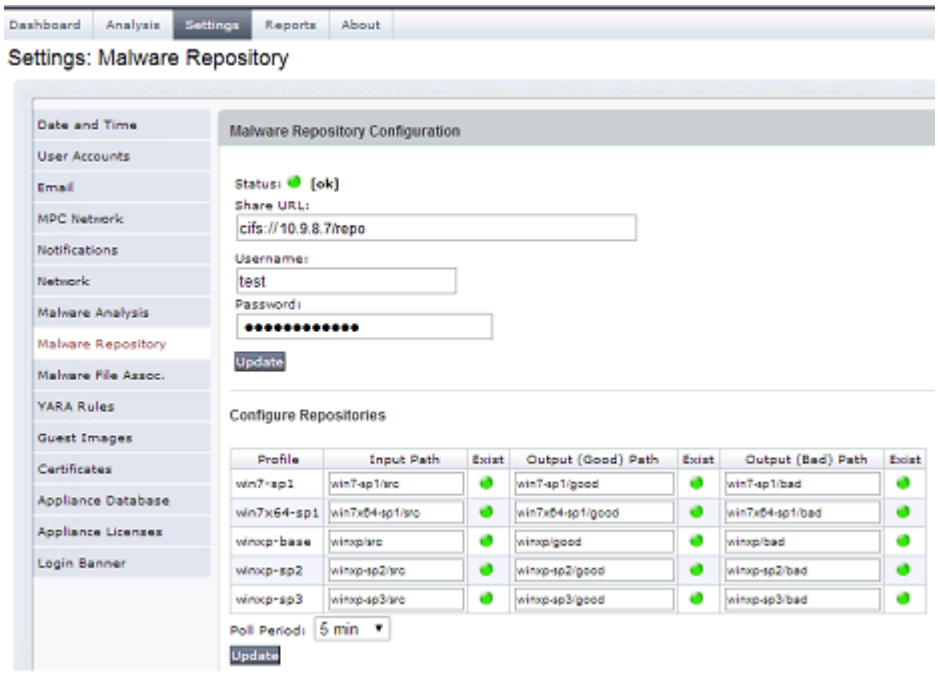
必要に応じて、通知の統合のみを使用できます。また、Bit9 が管理するシステムで見つかったファイルを FireEye アプライアンスにアップロードして分析し、分析結果を Bit9 コンソールに表示するように設定することもできます。

分析のために Bit9 Server から FireEye アプライアンスにファイルをアップロードできるようにする手順：

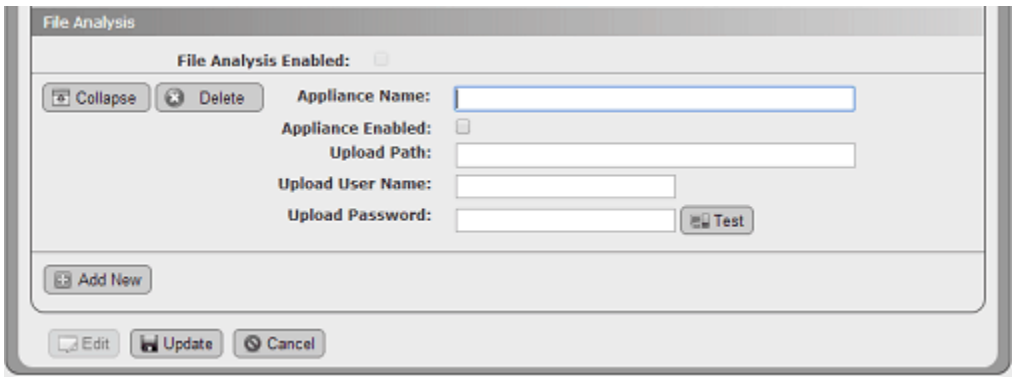
1. FireEyeアプライアンスとBit9 Serverが相互に通信できること、上記の手順で説明されている通りに通知の統合が有効化されていることを確認します。
2. FireEye のドキュメントで説明されているように FireEye Malware Repository 用のファイル共有をセットアップし、FireEye がこの共有への適切なアクセス権を持っていることを確認します。各オペレーティング システム フォルダーは、以下のような構造にする必要があります。

表 121：FireEye 分析のフォルダー構造

フォルダーの内容	パス形式	例
分析のために Bit9 からアップロードされたファイル	-<*OSpath*> または <*OSpath*>**/src**	d/win7sp1/ または d/win7sp1/src
悪意のあるファイルを示す分析結果	<*OSpath*>**/bad**	d/win7sp1/bad
ファイルに**悪意がない**ことを示す分析結果	<*OSpath*>**/good**	d/win7sp1/good



3. Bit9 コンソールで、［**Administration**（管理）］>［**System Configuration**（システム構成）］を選択し、［**Connector**（コネクター）］タブ、**[FireEye]** タブの順にクリックします。
4. ページ下部の［**Edit**（編集）］ボタンをクリックします。

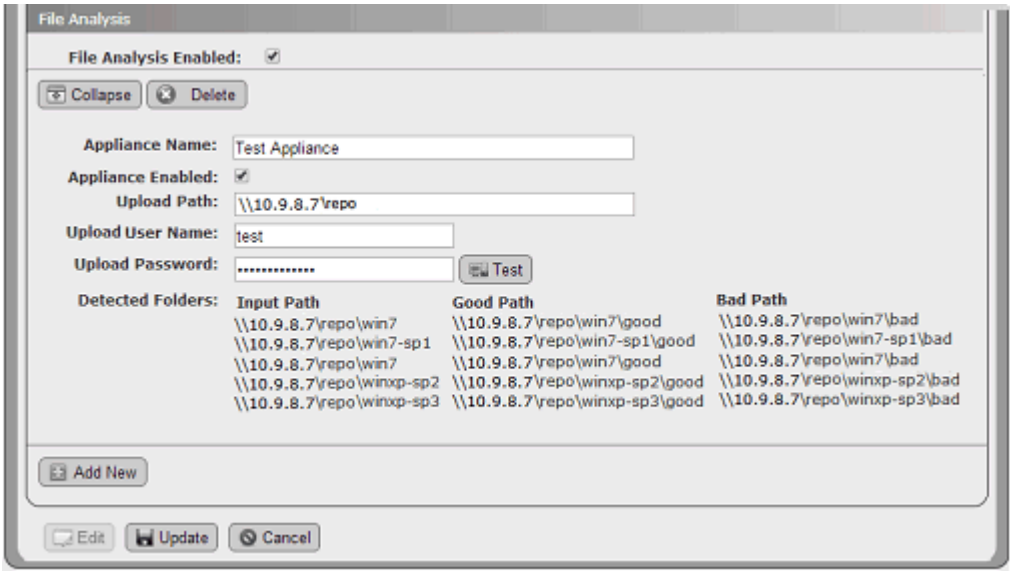


5. ［File Analysis（ファイル分析）］パネルで［**File Analysis Enabled**（ファイル分析の有効化）］ボックスをオンにし、次に［**Add New**（新規の追加）］ボタンをクリックしてアプライアンスの構成に必要なフィールドを表示します。
6. ［Appliance Name（アプライアンス名）］に、ファイルのアップロード先になる FireEye アプライアンスを入力します。この名前は、このページでアプライアンスを識別するためにのみ使用されます。接続の成功や失敗には影響を与えません。
7. ［**Appliance Enabled**（アプライアンスの有効化）］ボックスをオンにし、構成の終了後すぐにこのアプライアンスにファイルをアップロードできるようにします。

8. ［Upload Path（アップロード パス)］フィールドに、FireEye Malware Repository を含む共有フォルダーのパスを入力します。
9. この［Upload Path（アップロード パス)］にアクセスするための［Upload User Name（アップロード ユーザー名）］および［Upload Password（アップロード パスワード)］を入力します。［Upload User Name（アップロード ユーザー名)］フィールドに入力するユーザー名を選択するときは、アップロード パス権限を考慮してください。このアカウントには、アップロード フォルダーの読み取り / 書き込み権限が必要です。

> **注意**
>
> ［Upload User Name（アップロード ユーザー名）］および［Upload Password（アップロード パスワード)］フィールドを空白のままにすると、Bit9 Server をインストールしたアカウントがアップロード ユーザーとして使用されます。

10. ［Test（テスト)］ボタンをクリックし、このページの変更を更新する前に、Bit9 Server がファイル共有にアクセスできることを確認します。ファイル共有にアクセスできない場合は、このファイル共有に対して構成したユーザー アカウントが読み取り / 書き込み権限を持っていることを確認してください。ファイル共有にアクセス可能な場合は、検出された各分析環境の［Detected Folders（検出されたフォルダー)］フィールドに［Input Path（入力パス)］、［Good Path（悪意のないファイル用パス)］、［Bad Path（悪意のあるファイル用パス)］が入力されます。



11. テストが正常に終了したら、［**Update**（更新）］ボタンをクリックして変更を保存します。

12. さらにアプライアンスを追加する場合は、[FireEye] タブ内の［**Edit**（編集）］ボタンをクリックし、次に［File Analysis（ファイル分析）］パネル下部の［**Add New**（新規の追加）］ボタンをクリックして、新しいデバイスの構成およびテスト手順を繰り返します。

分析の統合が完了すると、Bit9 コンソールのファイル テーブルやイベント テーブルが表示されるページや、単一ファイルの詳細を表示するページに新しいメニュー項目が表示されます。これらの［**Analyze File with FireEye**（FireEye でファイル分析）］コマンドを使用して、FireEye アプライアンスにファイルを送信することができます。また、［System Configuration（システム構成）］ページの [FireEye] タブ内にある［File Analysis（ファイル分析）］パネルには、Bit9 Server からファイルを送信できるファイル共有内のすべてのオペレーティング システム固有フォルダーが表示されます。FireEye へのファイルのアップロード方法と FireEye 分析結果の表示方法の詳細については、「エンドポイント上の疑わしいファイルの分析」を参照してください。

注意

［Analyze with FireEye（FireEye で分析）］サブメニューの選択肢は、上記の手順で［Test（テスト）］ボタンをクリックしたときに検出されたフォルダー構造に基づいています。検出されたフォルダー構成が現在の FireEye コンソールの共有構成と一致していない場合、現在構成されていないフォルダーが選択されるとファイル分析は失敗します。

FireEye 脅威レベル マッピング

外部通知を受信するたびに、Bit9 Server イベント ログに［External Notification（外部通知）］イベントが発生します。マルウェアや危険な可能性があるファイルを示している外部通知は、別の Bit9 イベントも生成することができます。脅威レベル マッピング機能を使用すると、FireEye アプライアンスから送信された通知に基づいて Bit9 マルウェア イベントを生成する 1 つまたは複数のマッピングを作成できます。各マッピング定義は、編集、削除、およびランク（評価の順番）を移動することができます。

マルウェアや危険な可能性があることを示す外部通知が Bit9 Server で受信されると、その通知は Bit9 イベントの生成方法を決定するマッピングに渡されます。このマッピングでは深刻度やタイプなどの外部通知に固有のフィールドを使用し、イベントの生成を一部の通知のみに限定することができます。マッピングは、上位から下位へという順番で処理されます。［Assign Threat Level（割り当て通知レベル）］値が［None（なし）］以外のマッピングのうち、通知と最初に一致したマッピングによってイベントが生成され、他のマッピングによる評価が停止されます。

Bit9 コンソールで生成されるイベントのサブタイプは、［Assign Threat Level（割り当て脅威レベル）］値によって決まります。

- ［Assign Threat Level（割り当て脅威レベル）］が［Malicious（悪質）］に設定されている場合、一致する通知によって［Malicious File Detected（悪意のあるファイルの検出）］イベントが生成されます。

- ［Assign Threat Level（割り当て脅威レベル）］が［Potential risk（危険な可能性あり）］に設定されている場合、一致する通知によって［Potential Risk File Detected（危険な可能性があるファイルの検出）］イベントが生成されます。

生成されるのは、通知あたり 1 つの脅威レベル イベントのみです。マッピングが通知と一致しない場合は、［External Notification（外部通知）］イベントのみが生成され、関連する脅威レベル イベントは生成されません。

外部通知から生成される Bit9 マルウェア イベントは、以下を提供します。

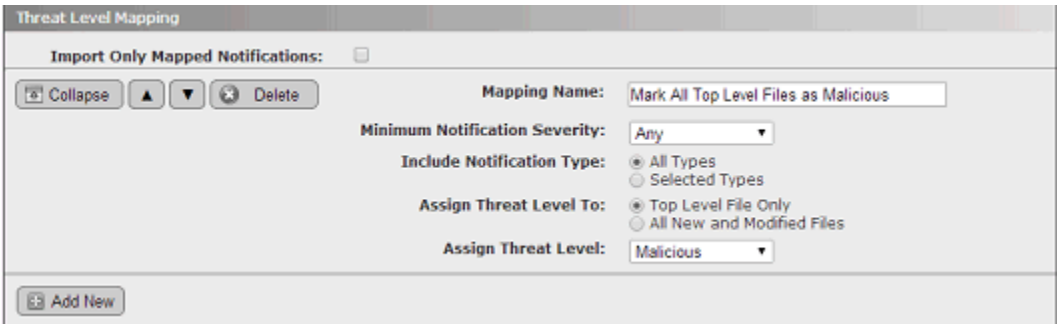
- マルウェア アクティビティの監査証跡（「Bit9 でのコネクター関連イベントのロギング」（901 ページ）を参照してください）。
- イベント ルールのトリガー。これにより、自動的にファイル禁止を生成できます（第 16 章「イベント ルール」）。
- Bit9 の悪意のあるファイル アラートまたは危険な可能性のあるファイル アラートのトリガー。このアラートは E メール通知を送信するように構成することもできます（「Bit9 アラートの使用」（606 ページ）を参照してください）。

注意

脅威レベル マッピングは、マルウェア イベントの生成を制御するだけでなく、対象外のデータに関する初期外部通知を排除するためにも使用できます。「マッピングされている脅威のみへの通知の制限」（875 ページ）を参照してください。

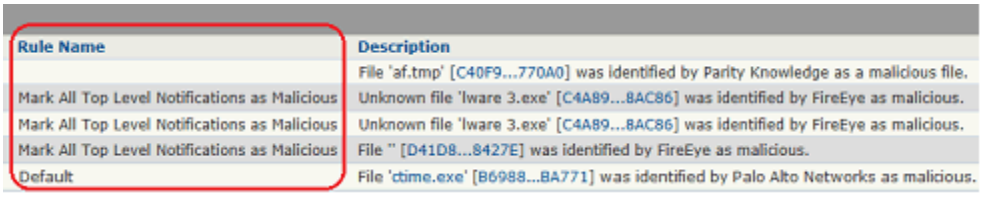
デフォルトの脅威レベル マッピング ルール

最初は、マルウェア関連通知の内容に関わらず、通知があると常に悪意のあるファイル イベントを Bit9 のイベント ログに生成するという、最も一般的なケースに対応する事前定義マッピングが 1 つだけ用意されています。以下にこのマッピングの設定を示します。



脅威レベル マッピングの追加または編集

各脅威レベル マッピングには一意の名前が必要です。以下に示すように、マッピングによって生成された［Malicious File Detected（悪意のあるファイルの検出）］イベントおよび［Potential Risk File Detected（危険な可能性があるファイルの検出）］イベントのマッピング名は、Bit9［Event（イベント）］ページの［Rule Name（ルール名）］として表示されます。



Rule Name	Description
	File 'af.tmp' [C40F9...770A0] was identified by Parity Knowledge as a malicious file.
Mark All Top Level Notifications as Malicious	Unknown file 'Iware 3.exe' [C4A89...8AC86] was identified by FireEye as malicious.
Mark All Top Level Notifications as Malicious	Unknown file 'Iware 3.exe' [C4A89...8AC86] was identified by FireEye as malicious.
Mark All Top Level Notifications as Malicious	File '' [D41D8...8427E] was identified by FireEye as malicious.
Default	File 'ctime.exe' [B6988...BA771] was identified by Palo Alto Networks as malicious.

新しい脅威レベル マッピングの作成手順：

1. Bit9 コンソール メニューで、[**Administration**（管理）] > [**System Configuration**（システム構成）] を選択し、[**Connector**（コネクター）] タブ、[**FireEye**] タブの順にクリックします。
2. ページ下部の［**Edit**（編集）］ボタンをクリックします。
3. ［Threat Level Mapping（脅威レベル マッピング）］パネルで、［**Add New**（新規の追加）］ボタンをクリックします。［Threat Level Mapping（脅威レベル マッピング）］パネルに、新しいマッピング定義セクションが表示されます。
4. ［Mapping Name（マッピング名）］フィールドに、新しいルールの一意の名前を入力します。
5. 受信する通知の［Minimum Notification Severity（通知の最低深刻度）］を選択します。この深刻度以上の通知がマッピングされます。このマッピングでは、これより低い深刻度は無視されます。選択肢（深刻度の高い方から）は、［**Critical**（重大）］、［**Major**（深刻）］、［**Minor**（マイナー）］、［**Any**（すべて）］です。
6. ［Include Notification Type（含める通知タイプ）］フィールドで、このマッピングとマッチングする通知のタイプを選択します。［**All Type**（すべてのタイプ）］または［**Seleted Type**（選択したタイプ）］を選択できます。［Seleted Type（選択したタイプ）］の場合は、［**Malware Object**（マルウェア オブジェクト）］、［**Malware Callback**（マルウェア コールバック）］、［**Web Infection**（Web 感染）］、［**Infection Match**（感染一致）］、［**Domain Match**（ドメイン一致）］から 1 つ以上を含めることができます。
7. このマッピングの脅威レベルは、［**Top Level File Only**（最上位ファイルのみ）］またはこの通知に関連付けられている［**All New and Modified Files**（すべての新規および変更ファイル）］（マルウェア自体とマルウェアによって作成されたファイル）に割り当てることができます。
8. 最後のパラメーターである［Assign Threat Level（割り当て脅威レベル）］では、通知とこのマッピングが一致したときに生成される Bit9 イベント サブタイプが決定されます。選択肢は、［**None**（なし）］（イベントを生成しません）、［**Potential risk**（危険な可能性あり）］、および［**Malicious**（悪質）］です。
9. このマッピングの順番を変更し、他のマッピングの前または後に処理する場合は、上または下の矢印を使用して位置を移動します。マッピングはこのページに表示される順番に処理され、最初に一致したマッピング処理のみが行われます。
10. 定義が終了したら、ページ下部にある［**Update**（更新）］ボタンをクリックします。確認ダイアログを使用して、変更を保存または破棄できます。

既存のマッピングは、パラメーターの変更や、他のルールに対する順番の変更のために編集することができます。

脅威レベル マッピングの編集手順：

1. ［System Configuration（システム構成）］ページの [FireEye] タブにある［**Edit**（編集）］ボタンをクリックします。
2. マッピングの順番のみを変更する場合は、マッピング名の隣の上または下の矢印を使用して位置を変更してから［**Update**（更新）］ボタンをクリックします。
3. その他の変更を加えるには、編集するマッピングの隣にある［**Expand**（展開）］ボタンをクリックします。
4. 新しいマッピングの作成手順の説明に従ってパラメーターを編集したら、［**Update**（更新）］ボタンをクリックし、ダイアログで変更を確認します。

マッピングされている脅威のみへの通知の制限

Bit9 Server は、いずれかのマッピング ルールに一致する通知のみを受け付けるように構成することができます。その結果、サーバーが収集する外部通知数と、これらの通知に対応するイベント数が減少するため、目的の通知を扱いやすくなります。この機能を有効化する前に、マッピング ルールを検証してどの通知が排除されるかを確認してください。

マッピングされていない FireEye 通知を排除する手順：

- [FireEye] の構成ページで、［**Edit**（編集）］をクリックし、［Threat Level Mapping（脅威レベル マッピング）］ボックスで［**Import Only Mapped Notifications**（マッピングされている通知のみをインポート）］ボックスをオンにし、最後に［**Update**（更新）］ボタンをクリックします。

Bit9 での FireEye アプライアンスのステータス

構成が終了すると、Bit9 と FireEye との統合のステータスが、Bit9 コンソールの［System Configuration（システム構成）］/［Connector（コネクター）］/［FireEye Integration Settings（FireEye 統合設定）］ページの［General（一般）］パネルに表示されます。各アプライアンスのアドレスの隣にステータス インジケーターが表示されます。

- 緑の円は、そのアプライアンスの統合に問題がないことを示し、最新の通知のタイムスタンプも表示されます。
- 赤の円は問題を示し、エラー メッセージも同時に表示されます。
- 水色の円は、構成が更新され、Bit9 が次の FireEye 通知を待機していることを示します。

コンソール アカウント権限の有効化

Bit9 コンソール ユーザーが Bit9 Connector 機能を使用するには、各自のユーザー アカウントで特定の権限を有効化する必要があります。構成ページにアクセスするためには一般的な管理権限が必要ですが、Connector 機能にアクセスするにはさ

らに以下の権限が必要です。これらの権限の詳しい説明と、コンソール ユーザー アカウントへの権限の追加方法の詳細については、「アカウント グループの権限」（108 ページ）を参照してください。

- ツール：View file uploads（ファイルのアップロードの表示）（デフォルトでは Administrator アカウントに対して有効化されています）
- ツール：Submit files for analysis（分析のためのファイルの送信）（デフォルトでは Administrator アカウントに対して有効化されています）

外部通知

Bit9 Connector を有効化すると、Bit9 コンソールに［External Notifications（外部通知）］ページが追加されます。このページには、ネットワーク セキュリティ デバイスおよびサービスからの通知のテーブルが表示されます。このテーブルの各行には、ファイル ハッシュやソース IP アドレスなどの重要情報が含まれています。通知に含まれているファイルまたはコンピューターがBit9エンドポイント データにも含まれている場合は、そのデータを通知と相関付けることができます。

このページには、通知に加え、接続中の構成済みデバイスまたはサービスからの通知を受信できない場合にはエラー メッセージも表示されます。

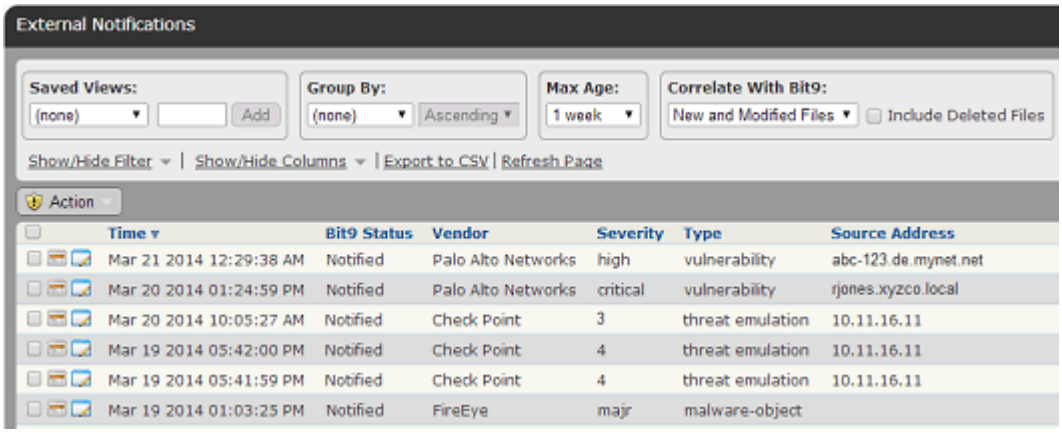
Palo Alto Networks からの通知は、セキュリティ分析という目的との関連性が低い通知が排除されるように事前にフィルターされます。深刻度が「informational（情報）」、「low（低）」、または「medium（中）」の脅威ログ通知は、デフォルトで Bit9 Server に提供される通知に含まれません。また、カテゴリーが「benign（無害）」の WildFire Log 通知は、デフォルトで除外されます。Check Point 通知も事前にフィルターされます。

すべてのソースからの通知合計数は、日次チェックが行われます。日次チェックで合計数が多すぎることが判明すると、ログの一番古い通知がトリミングされます。ただし、トリミングを設定する前に通知数が上限を大幅に上回る可能性があることに注意してください（通知が最初に有効化されたときなど）。

通知数の上限に達すると通知がトリミングされるだけでなく、一定の保存期間を経過した通知も削除されます。デフォルトで、通知数の上限は 200,000、保存期間は 6 か月です。これらの数値は、その後変更できます。

Bit9 コンソールで［External Notifications（外部通知）］テーブルを開く手順：

- Bit9 コンソール メニューで、［**Reports**（レポート）］>［**External Notifications**（外部通知）］を選択します。



Bit9 Server とのデータ相関付けによって、Bit9 エージェントが稼働するシステムへの影響に応じて迅速に外部通知の優先順位を付けることができます。接続中のネットワーク セキュリティ ソースからマルウェア通知を受信すると、以下のことを把握できます。

- 運用するいずれかのシステムにマルウェアが存在するかどうか
- 運用するいずれかのシステムでマルウェアが実行されたか
- どれくらい広まっているか（コンピューターの台数）
- このマルウェアのソースとして特定されたシステムの詳細（システムに対するユーザー アクティビティおよびその他のシステム アクティビティの種類など）

［External Notifications（外部通知）］テーブルでは、さまざまな方法で詳細情報を見ることができます。

- ［View Details（詳細の表示）］（ファイルと鉛筆）ボタンをクリックすると、その行の通知の［External Notification Details（外部通知の詳細）］ページが開きます。この詳細ページには、Bit9 データベースに保管されているこの通知のすべての情報が含まれています。詳細については、「［External Notification Details（外部通知の詳細）］」（884 ページ）を参照してください。またこの表には、通知の完全な XML 詳細ファイルを開くリンクも含まれています。このページの詳細については、「XML 詳細の表示」を参照してください。
- ［Total Files（合計ファイル）］または［New and Modified files（新しいファイルと変更されたファイル）］列の数字が 0 より大きければ、この数字をクリックしても［External Notification Details（外部通知の詳細）］ページを開くことができます。
- [Malware MD5]、[SHA-1]、または [SHA-256] ハッシュがテーブルに表示されており、このハッシュによって Bit9 Server に登録されているファイルが識別できる場合、ハッシュをクリックするとそのファイルの［File Details（ファイルの詳細）］ページが開きます。
- いずれかの［Bit9 Files（Bit9 ファイル）］の列で、ファイル数に 1 が表示されている場合、1 をクリックするとそのファイルの［File Details（ファイルの詳細）］ページが開きます。この数字が 2 以上の場合は、数字をクリックすると［External Notification Details（外部通知の詳細）］ページが開き、［Known Files（既知のファイル）］タブが表示されます。
- ［Bit9 Computers（Bit9 コンピューター）］列で、コンピューター数に 1 が表示されている場合、1 をクリックするとそのコンピューターの［Computer Details（コンピューターの詳細）］ページが開きます。この数字が 2 以上の場合は、数字をクリックすると［Computers（コンピューター）］テーブルが開きます。
- ［Source Address（ソース アドレス）］または［Destination Address（宛先アドレス）］列に Bit9 エージェントがインストールされているシステムのアドレスが表示されている場合、このアドレスをクリックするとそのコンピューターの［Computer Details（コンピューターの詳細）］ページが開きます。
- ［History（履歴）］ボタンをクリックすると、［Notification Details（通知の詳細）］ページが開き、［History（履歴）］タブが表示されます。［History（履歴）］タブには、この通知に関連する最新の 20 のアクションが含まれています。

表 122 に、［External Notifications（外部通知）］テーブルで把握できる情報を示します。デフォルトでは、これらすべての列が表示されるわけではありません。

表 122：[External Notifications（外部通知）] テーブルの列

列	説明
Vendor（ベンダー）	外部通知を送信した製品のベンダー。現在は Check Point、FireEye、または Palo Alto Networks です。
Appliance（アプライアンス）	通知を提供した外部アプライアンスまたはサービスの名前。アプライアンスまたはサービス コンソール URL へのリンクが含まれています。 Check Point の場合は、通知がプライベート脅威エミュレーターから送信されたときは、その名前がここに表示されます。
Product（製品）	（提供されている場合）外部アプライアンスまたはサービス製品の名前。アプライアンス コンソール URL へのリンクが含まれています。
Version（バージョン）	外部アプライアンス、エージェント、またはレポートのバージョン。アプライアンス コンソール URL へのリンクが含まれています。
Time（時間）	ネットワーク上でマルウェアが検出された日時。
Severity（深刻度）	通知の深刻度。ベンダーによって基準が異なります。
Type（タイプ）	通知のタイプ（名前ではありません）。 **Check Point の場合**は、通知を提供できる構成済みのいずれかの Check Point ソフトウェア製品（ブレード）。 **FireEye の場合**は、[domain-match（ドメイン - 一致）]、[malware-callback（マルウェア - コールバック）]、[malware-object（マルウェア - オブジェクト）]、[web-infection（Web- 感染）]、[infection match（感染一致）] になります。 **Microsoft SCEP の場合**は、プレフィックス「malware_」または「potential_risk_」で始まり、SCEP ファイル パス ヘッダーによってレポートされているオブジェクトで終了する文字列（例：「potential_risk_file」、「malware_webscript」）。 **Palo Alto Networks の場合**は、[wildfire（WildFire）]、[spyware（スパイウェア）]、[virus（ウイルス）]、[vulnerability（脆弱性）]、[wildfire-result（WildFire- 結果）]。
Source IP（ソース IP）	マルウェアの発生源の IP アドレス。

列	説明
Source Address（ソース アドレス）	ソース アドレスは、マルウェアの発生源のアドレスで、以下のソースのいずれかです。 • このアドレスが Bit9 Server によって把握されているコンピューターの場合は、Bit9 データベースでこのソースに対してリストされるホスト名が使用されます。この場合、この名前は［Computer Details（コンピューターの詳細）］ページにリンクされます。 • このコンピューターがサーバーに把握されていない場合、サーバーはリバース DNS ルックアップを実行します。このホスト名がこの方法で解決できれば、この名前が使用され、永続化されます。 • Bit9 がホスト名を解決できない場合、プロバイダーによって解決された URL が表示されます。 • 解決が不可能な場合はIPアドレスが表示されます。このケースは、マルウェアがコールバックを試みた場合に発生することがあります。
Source URL（ソース URL）	プロバイダーによって解決された、マルウェアの発生源のコンピューターの URL。
Source Username（ソース ユーザー名）	ソース アドレスでシステムにログインしたユーザーの名前。Active Directory がアプライアンスまたはサービスと統合されている場合に、Check Point、Microsoft、および Palo Alto Networks 統合に対して表示されます。
Destination IP（宛先 IP）	マルウェアのターゲットになった IP アドレス。
Destination Address（宛先アドレス）	「Source Address（ソース アドレス）」で説明したようにして解決された、マルウェアのターゲットになったアドレス。
Destination Username（宛先ユーザー名）	宛先アドレスでシステムにログインしたユーザーの名前。Active Directory がアプライアンスまたはサービスと統合されている場合に、Check Point および Palo Alto Networks 統合に対して表示されます。
Malicious（悪質）	通知が悪意のあるファイルを特定したかどうかを示します（［Yes（はい）］/［No（いいえ）］）。
Malware Name（マルウェア名）	通知でレポートされたマルウェア名（複数になる場合はコンマ区切り）。FireEye および Microsoft SCEP の場合は、マルウェア名の説明を含む各社の外部サイトにリンクされます。
Malware MD5（マルウェア MD5）	通知でレポートされた最上位 MD5 ハッシュ。
Malware SHA1（マルウェア SHA1）	通知でレポートされた最上位 SHA1 ハッシュ。Check Point 通知および Microsoft 通知に対して表示されます。
Malware File（マルウェア ファイル）	通知でレポートされた最上位ファイル名。
Application（アプリケーション）	通知でレポートされたアプリケーション。

列	説明
Analysis Environment（分析環境）	ファイル分析に使用されたオペレーティング システム環境。Palo Alto Networks および Check Point の場合は、環境内の重要アプリケーション（Office など）に関する情報が含まれることもあります。
Registry Keys（レジストリ キー）	通知でレポートされたレジストリ キーの変更数。
Directories（ディレクトリ）	通知でレポートされたディレクトリの変更数。
New and Modified Files（新しいファイルと変更されたファイル）	通知でレポートされた、このマルウェアによって作成または変更されたファイル数。
Total Files（合計ファイル）	この通知に含まれる一意のファイル数の合計。
Received Time（受信時間）	Bit9 Server この通知を受信した日時。
Modified Time（修正時間）	この通知の最終変更（ステータスの変更など）日時。
Bit9 Status（Bit9 ステータス）	Bit9 でのこの通知のステータス（［Notified（通知済み）］、［Escalated（エスカレーション済み）］、［Resolved（解決済み）］、［Closed（クローズ）］）。
Bit9 Known Files（Bit9 に把握されているファイル）	Bit9 Server に把握されているこの通知内の一意のファイル数。［External Notifications（外部通知）］ページの［Correlate with Bit9（Bit9 との相関付け）］オプションに基づいて変更されることがあります。
Bit9 Executed Files（Bit9 実行済みファイル）	Bit9 Server に把握されている、エンドポイントで実行されたこの通知内のファイル数。［External Notifications（外部通知）］ページの［Correlate with Bit9（Bit9 との相関付け）］オプションに基づいて変更されることがあります。
Bit9 Banned Files（Bit9 禁止ファイル）	Bit9 Server に把握されているこの通知内の禁止ファイル数。［External Notifications（外部通知）］ページの［Correlate with Bit9（Bit9 との相関付け）］オプションに基づいて変更されることがあります。
Bit9 Computers（Bit9 コンピューター）	この通知でレポートされた MD5 ハッシュの 1 つに一致する 1 つ以上のファイルが含まれる、Bit9 が管理するコンピューター数。
Bit9 Files on Computers（コンピューター上の Bit9 ファイル）	この通知でレポートされた Bit9 が管理するコンピューターのファイルのインスタンス数。
Bit9 Submitted（Bit9 が送信済み）	ファイル分析のために、この Bit9 Server によってこの通知のファイルが外部デバイスに送信されたかどうかを示します（［Yes（はい）］/［No（いいえ）］）。

[External Notifications（外部通知）]テーブル ページの［Action（アクション）］ メニュー

［External Notifications（外部通知）］テーブル ページの［Action（アクション）］メニューには、テーブルでチェック済みの 1 つまたは複数の通知のステータスの変更や、通知で参照されているファイルに関する詳細情報の取得のためのコマンドが含まれています。通知管理コマンドは、通知の管理を容易にすることのみを目的としており、通知内のファイルには影響を及ぼしません。

- ［**Escalate Notification**（通知のエスカレーション）］– これが注意を要する通知であり、この通知の調査や関連するアクションを実行する必要があることを指定します。
- ［**Resolve Notification**（通知の解決）］– これらの通知への対応が終了したことを指定します。
- ［**Close Notification**（通知のクローズ）］– これらの通知が解決され、［External Notification Details（外部通知の詳細）］ページに必要なコメントが入力されて、通知を追跡する必要がなくなったことを指定します。
- ［**View Bit9 SRS Cloud Data**（Bit9 SRS クラウド データの表示）］– Bit9 SRS が有効で、かつ通知に MD5 ハッシュが含まれている場合に、Bit9 SRS Web サイトを開き、チェック済みの通知内の MD5 ハッシュに関する情報を表示します。

［Notifications（通知）］テーブル ページの［Saved Views（保存済みビュー）］

デフォルトでは、［External Notifications（外部通知）］ページには、ネットワーク セキュリティ デバイスから Bit9 Server に到着したすべての通知が表示されます。事前構成済みの［Saved Views（保存済みビュー）］を使用すると、特定のタイプの通知に注目しやすくなります。

- ［**Active Notifications**（アクティブな通知）］– ステータスが Closed（クローズ）以外で、かつ Bit9 コンソールからの分析要求の結果ではない、すべての通知が表示されます。通知のステータスの説明については、「通知のステータスの管理」を参照してください。これはデフォルトのビューです。
- ［**Check Point Notifications**（Check Point 通知）］– Check Point ログ サーバーから受信したすべての通知が表示されます。
- ［**File Analysis Results**（ファイル分析結果）］– Bit9 コンソールから分析のために送信されたファイルに関するすべての通知が表示されます。
- ［**FireEye Notifications**（FireEye 通知）］– FireEye デバイスから受信した通知のうち、Bit9 コンソールから送信されたファイルに関連しない通知が表示されます。
- ［**Microsoft Notifications**（Microsoft 通知）］– Microsoft SCEP から受信した通知が表示されます。
- ［**Notifications with Files**（ファイルを含む通知）］– 1 つ以上のファイル ハッシュが含まれるすべての通知が（このファイルが Bit9 Server に把握されているかどうかを問わず）表示されます。
- ［**Notifications with Files on Bit9 Computers**（Bit9 コンピューター上のファイルを含む通知）］– エージェントに管理されるシステム上に存在する（または存在した）ために Bit9 Server に把握されている 1 つ以上のファイル ハッシュまたはファイルが含まれるすべての通知が表示されます。

- ［**Palo Alto Networks Notifications**（Palo Alto Networks 通知）］–Palo Alto Networks デバイスから受信した通知が表示されます。

他の Bit9 コンソールのテーブル ページと同様に、このビューは［Show Filters（フィルターの表示）］ボタンと［Show Columns（列の表示）］ボタンを使用してカスタマイズでき、カスタマイズしたビューは保存できます。

［File Details（ファイルの詳細）］ページから通知テーブルへのアクセス

［File Details（ファイルの詳細）］と［File Instance Details（ファイル インスタンスの詳細）］ページには、現在のファイルに対してネットワーク セキュリティ デバイスからの通知がある場合、［Related Views（関連ビュー）］メニューに［**External Notifications**（外部通知）］が選択肢として表示されます。このリンクをクリックすると、このファイルを含む通知のみを表示するようにフィルターされた［External Notifications（外部通知）］テーブル ページが表示されます。

外部通知の相関付けレベルの選択

Bit9 Connector の重要な機能の 1 つは、外部ソースから受信したセキュリティ通知と、Bit9 が管理するコンピューターで使用可能なリアルタイム ファイル データとの相関付けです。［External Notifications（外部通知）］ページには、すべての Bit9 テーブルで利用可能な通常のフィルタリングとテーブル列の選択肢があるだけでなく、通知データと相関付けるファイルを選択するためのメニューも使用できます。

［Correlate with Bit9（Bit9 との相関付け）］パネルには、以下の選択肢があります。

- ［**New and Modified files**（新しいファイルと変更されたファイル）］– この選択肢を選択すると、Bit9 情報と、通知でレポートされたすべてのファイル（最上位マルウェアと、このマルウェアによって書き込みまたは修正されたすべてのファイルを含む）が相関付けされます。
- ［**Only Untrusted Files**（信頼されないファイルのみ）］– この選択肢を選択すると、Bit9 情報と、Bit9 SRS にレポートされた信頼レベルが **5** 以下の通知内のファイルのみが相関付けされます。
- ［**Only Top Level Files**（最上位ファイルのみ）］– この選択肢を選択すると、Bit9 情報と、通知でレポートされた最上位ファイルのみが相関付けされます。最上位ファイルによって書き込みまたは修正されたファイルは相関付けされません。
- ［**Include Deleted Files**（削除済みファイルを含む）］– すべてのメニュー選択肢に適用されるチェックボックスです。オンにした場合、通知データと相関付けるデータに、Bit9 エンドポイントから削除されたファイルが含まれます。非常に多く発生している、実行後に自身を削除するマルウェアを確実に追跡するときに役立つオプションです。

注意

［External Notification Details（外部通知の詳細）］ページの［Known Files and Files on Computer（既知のファイルおよびコンピューター上のファイル）］タブでも、［Correlate with Bit9（Bit9 との相関付け）］の選択肢を変更することができます。これらのどの場所で変更を行っても、すべての通知テーブルに影響があります。

外部通知に含まれている MD5 ハッシュは、Bit9 Server インベントリ内のファイルとの相関付けに使用されます。通知に MD5 ハッシュではなく SHA-256 ハッシュが含まれている場合は、SHA-256 ハッシュが相関付けに使用されます。

少ないケースですが、日付、場所、その他のコンテキスト固有の情報が含まれているためインストールされるたびにハッシュが変更されるファイルについては、ファイル インベントリに「ファジー」ハッシュが作成されます。このハッシュは「SHA-256（正規化済み）」として識別され、外部通知でレポートされた SHA-256 ハッシュと相関付けできない場合があります。このことが関係するのは、通知内に MD5 ハッシュが含まれておらず、通知で特定されたファイルが Bit9 Server のファイル インベントリ内のファジー SHA-256 ハッシュを必要とする場合のみです。

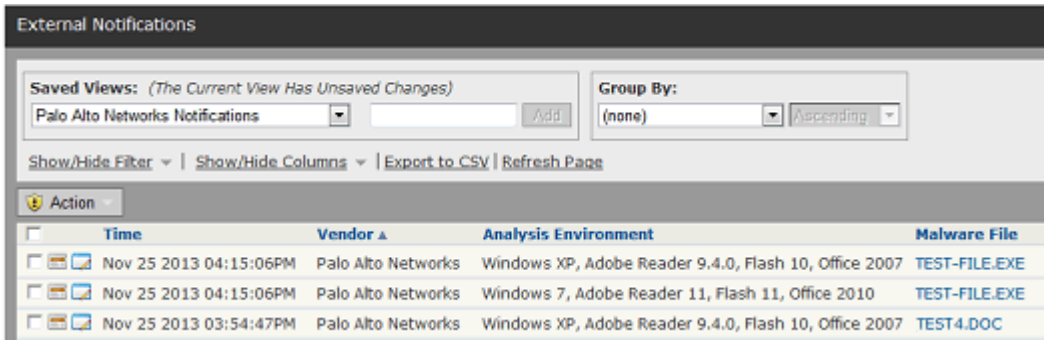
マルウェア ファイルとその親プロセスのどちらについても、ファイルの相関付けは Bit9 Server が通知を受信した直後に開始され、通知を処理して Bit9 ファイル インベントリ処理と同期するために必要な期間、バックグラウンド タスクとして継続されます。ファイルの相関付けはすべての未知のファイルに対して繰り返し実行され、相関付けが完了するか、通知が古くなったとみなされるまで（通常は 24 時間）継続されます。この期間が確保されているため、新しいファイルの通知が Bit9 Server に到着したとき、Bit9 Server がそのファイルを［Files on Computers（コンピューター上のファイル）］インベントリに記録する前に、新しいファイルを大量に相関付けることができます。

ファイルが正常に相関付けされると、［Malicious File Detected（悪意のあるファイルの検出）］イベントまたは［Potential Risk File Detected（危険な可能性があるファイルの検出）］イベントが生成されます。これには、マルウェア ファイルとその親プロセスの両方のハッシュが含まれます。通知に複数のファイルが含まれている場合、イベントは最上位ファイルに対してのみ生成されます。通知テーブルと通知の詳細では、これらのハッシュはそれぞれのファイルの［Bit9 File Details（Bit9 ファイルの詳細）］ページにリンクされます。

注意

ファイルが同一の名前を維持したまま、ファイル自体が変更され、そのハッシュが変更されると、新しいハッシュとの相関付けを試みることができますが、新しいハッシュが通知に含まれていない場合、相関付けは失敗します。

複数の分析環境からの通知



Check Point および WildFire（6.0 以降）は、同一のファイルについて、異なる各分析環境から複数の通知をレポートできます。［Analysis Environment（分析環境）］フィールドは、ファイルのデトネーションまたは分析が行われたテスト環境に関する情報を提供し、ファイルが各環境で悪質とみなされたかどうかを把握できるので特に有益です。ファイルのデトネーションに基づく通知の場合、この環境には基盤のオペレーティング システムだけでなく、その他の重要なソフトウェアも含まれます。ある通知の［Analysis Environment（分析環境）］の例：*Windows 7*、*Adobe Reader 11*、*Flash 11*、*Office 2010*

静的分析に関する WildFire 通知では、このフィールドでアナライザーのタイプがレポートされます。例：*DOC/CDF Analyzer*

注意

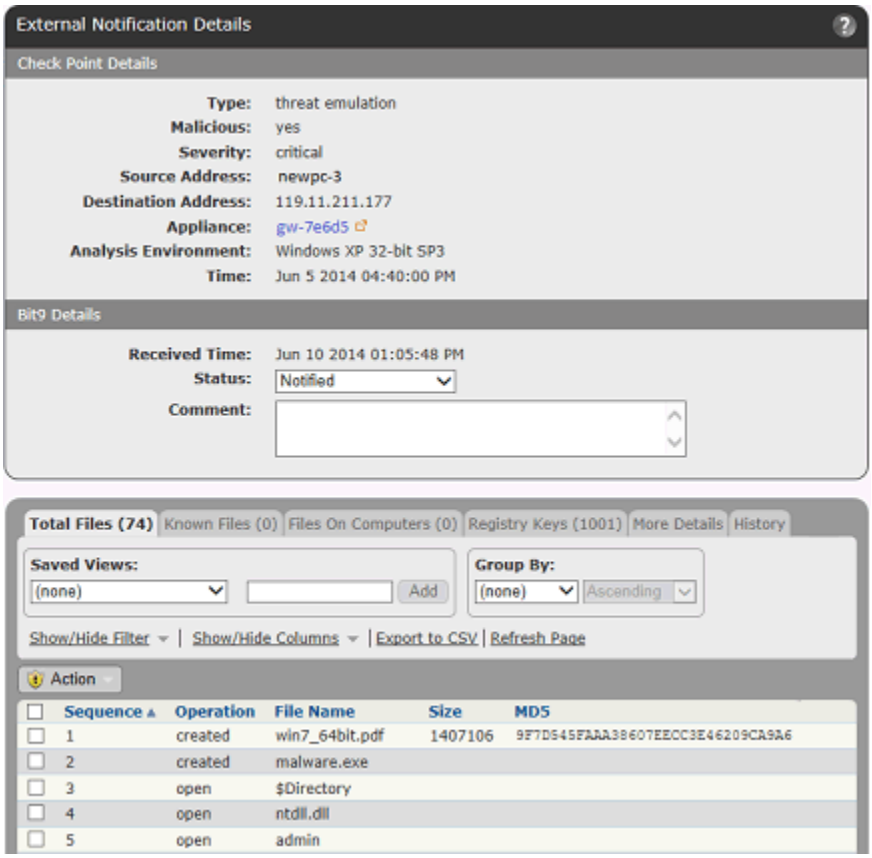
Bit9 から WildFire に分析のためにファイルがアップロードされ、WildFire がこのファイルに関する複数の通知をレポートする場合、このファイルは一部の環境で無害と見なされ、それ以外の環境で悪質と見なされることがあります。［External Notifications（外部通知）］テーブルと［External Notification Details（外部通知の詳細）］ページで、分析環境別の個々の分析結果を確認できます。ただし、WildFire クラウドに送信されたファイルの場合、［Requested Files（要求されたファイル）］ページの［Analyzed Files（分析されたファイル）］タブには、WildFire によって決定されたこのファイルの総合的な結果のみが表示されます。

［External Notification Details（外部通知の詳細）］

［External Notification Details（外部通知の詳細）］ページには、1 つの通知について Bit9 データベースに保管されているすべての情報が表示されます。

1 つの通知の［External Notification Details（外部通知の詳細）］ページを開く手順：

1. Bit9 コンソール メニューで、［**Reports**（レポート）］>［**External Notifications**（外部通知）］を選択します。
2. 通知内の関心がある行で［View Details（詳細の表示）］ボタンをクリックします。



この詳細ページには、通知に関する基本情報が含まれています。ページの下部には、さらに詳しい情報を提供する一連のタブがあります。表示されるタブは、通知のタイプによって異なります。メイン ページとタブの大半のフィールドの詳細については、表 122（878 ページ）で説明されています。タブに関する情報については、以下のセクションで説明します。

[Total Files（合計ファイル）] タブ

このタブには、この通知でレポートされたすべてのファイル（他のファイルに書き込まれたファイルを含む）が表示されます。複数の場所に書き込まれた同一のファイル（同一のハッシュを持つファイル）は、[Total Files（合計ファイル）] リストに複数回表示されます。このテーブルには以下の列が含まれています。

表 123：[Total Files（合計ファイル）] タブの列

列	説明
Sequence（順序）	ネットワーク セキュリティ デバイスによって疑わしいマルウェア インスタンスが分析されたときに、各ファイルが登場した順序。この順序の最初のファイルは最上位プロセスです。
Operation（操作）	ファイルに対して実行された操作（[start（開始）]、[create（作成）]、[close（クローズ）] など）。 Microsoft SCEP 通知の場合は、常に [create（作成）] です。

列	説明
File Name（ファイル名）	ネットワーク セキュリティ デバイスによってレポートされたファイル名。Check Point の場合は、最初のファイルのみレポートされます。
Size（サイズ）	ネットワーク セキュリティ デバイスによってレポートされたファイル サイズ。Check Point の場合は、最初のファイルのみレポートされます。
MD5	ファイルの MD5 ハッシュ。Check Point の場合は、最初のファイルのみレポートされます。
File Path（ファイル パス）	通知でレポートされたファイル名のファイル パス。
Parent File Name（親ファイル名）	このファイルの親プロセスのファイル名。
Parent File Path（親ファイル パス）	このファイルの親プロセスのファイル パス。
SHA1	このファイルの SHA1 ハッシュ（レポートされた場合）。Check Point の場合は、最初のファイルのみレポートされます。
SHA-256	このファイルの SHA-256 ハッシュ（レポートされた場合）。Palo Alto Networks 通知に対してのみ表示されます。
Known File（既知のファイル）	このファイルが Bit9 Server によって把握されているかどうか（[Yes（はい）] / [No（いいえ）]）。

[Operation（操作）] 列は、通知に含まれている各ファイルで行われた操作に関する重要情報を提供します。このフィールドを基準に並べ替えまたはフィルターを行うと、ファイルに行われた操作を把握できます。通知では、「作成された」ファイルや「上書きされた」ファイルがレポートされることがあります。この 2 つの操作が行われたファイルは、[New and Modified files（新しいファイルと変更されたファイル）] リストに含まれています。ファイルは、「オープン」または「終了」されたものもあります。

Bit9 Server によって把握されているファイルの場合、[Total Files（合計ファイル）] タブのリスト内の [View Details（詳細の表示）] ボタンを使って、このファイルの [File Details（ファイルの詳細）] ページを開くことができます。

このタブの [Action（アクション）] メニューには、選択したファイルに対して実行できる以下のコマンドが含まれています。

- [**Ban Globally**（グローバル禁止）] – すべてのポリシーでファイルを禁止します。他の構成は必要ありません。
- [**Ban by Policy**（ポリシーによる禁止）] – ポリシー別の禁止またはレポートのみの禁止を作成するためのダイアログ ボックスが開きます。
- [**Remove Approval or Ban**（承認または禁止を削除）]– 任意の有効な禁止 / 承認を即座に削除します。

- ［**Find By Name**（名前で検索）］– 選択したファイル名でフィルターされた［Find Files（ファイルの検索）］ページにリダイレクトされます。
- ［**Find By Size**（サイズで検索）］– 外部通知のレポートに応じて、選択したファイルのサイズに一致するファイルの検索結果が表示されるようにフィルターされた［Find Files（ファイルの検索）］ページにリダイレクトされます。
- ［**Find By Hash**（ハッシュで検索）］– 外部通知のレポートに応じて、選択したファイルのハッシュの検索結果が表示されるようにフィルターされた［Find Files（ファイルの検索）］ページにリダイレクトされます。
- ［**View Bit9 SRS Cloud Data**（Bit9 SRS Cloud データの表示）］– Bit9 SRS のこのファイルのハッシュ別のレポートにリダイレクトされます（SRS が有効な場合）。

［Known Files（既知のファイル）］タブ

このタブには、Bit9 Server に把握されているこの通知内のすべてのファイルが表示されます。テーブルには、（デフォルトでもカスタマイズした場合も）Bit9 ファイル カタログのすべてのフィールドが含まれます。［Total Files（合計ファイル）］タブに表示されるような、ネットワーク セキュリティ デバイスからのファイル情報を提供する他のフィールドを追加することもできます。［Action（アクション）］メニューには、［Total Files（合計ファイル）］タブ メニューと同じオプションが含まれていますが、使用可能な場合は通知ではなく Bit9 インベントリのファイル情報が使用されます。

このページでは、［Correlation Details（相関付けの詳細）］オプションを変更して、通知と相関付ける Bit9 情報をカスタマイズできます。ここで選択した内容は、相関付けオプションが表示されるすべてのページに影響します。

［Files On Computers（コンピューター上のファイル）］タブ

このタブには、この通知に含まれる Bit9 Server ファイル インベントリ内の全ファイル インスタンスが表示されます。ここには、（デフォルトでもカスタマイズした場合も）Bit9 コンソールの［Files on Computers（コンピューター上のファイル）］）ページのすべてのフィールドを追加できます。また［External File Name（外部ファイル名）］および［External Size（外部サイズ）］列も追加できます。［Action（アクション）］メニューには、［Total Files（合計ファイル）］タブ メニューと同じオプションが含まれます。

このページの［Correlation Details（相関付けの詳細）］オプションを変更して、通知と相関付ける Bit9 データをカスタマイズできます（この変更は、相関付けオプションが表示されるすべてのページに影響します）。

［Directories（ディレクトリ）］タブ

FireEye 通知に対しては、［Directories（ディレクトリ）］タブに、外部通知でレポートされたすべての関連ディレクトリ エントリ（疑わしいアクティビティが検出されたパス）が表示されます。このタブのテーブルには、次の列を含めることができます。

表 124：[Directories（ディレクトリ）] タブの列

列	説明
Sequence（順序）	ネットワーク セキュリティ デバイスによって疑わしいマルウェア インスタンスが分析されたときに、各プロセスが登場した順序。この順序の最初のプロセスは最上位プロセスです。
Directory（ディレクトリ）	ネットワーク セキュリティ デバイスによってレポートされたディレクトリ（一部が省略されて表示されます）
Operation（操作）	ディレクトリで行われた操作（[created（作成）]、[opened（開く）]、[deleted（削除）] など）
Process（プロセス）	ネットワーク セキュリティ デバイスによってレポートされたプロセス。
プロセス MD5	プロセスの MD5 ハッシュ。
Process Path（プロセス パス）	ネットワーク セキュリティ デバイスによってレポートされたプロセスのパスの場所。

ディレクトリへのアクセスを試みたプロセスを Bit9 Server が把握している場合、このリストには [View Details（詳細の表示）] ボタンが含まれており、このプロセスの [File Details（ファイルの詳細）] ページを開くことができます。

このタブの [Action（アクション）] メニューには、選択したファイルに対して実行できる以下のコマンドが含まれています。

- [**Ban Process Globally**（プロセスのグローバル禁止）] – すべてのポリシーでプロセス ファイルを禁止します。他の構成は必要ありません。
- [**Ban by Policy**（ポリシーによるプロセス禁止）] – ポリシー別の禁止またはレポートのみの禁止を作成するためのダイアログ ボックスが開きます。
- [**Remove Process Approval or Ban**（プロセス承認または禁止を削除）] – 任意の有効な禁止 / 承認を即座に削除します。
- [**Create Custom Rule**（カスタム ルールの作成）] – [Add Custom Rule（カスタム ルールの追加）] ページが開きます。このディレクトリへのアクセスを試みたプロセスの禁止を作成するための値が事前に入力されています。詳細については、「ディレクトリ制御用のカスタム ルール」を参照してください。

[Registry Keys（レジストリ キー）]

このタブには、外部通知でレポートされたすべての関連レジストリ値の変更が表示されます。このタブのテーブルには、次の列が含まれています。

表 125：[Registry Keys（レジストリ キー）] タブの列

列	説明
Sequence（順序）	ネットワーク セキュリティ デバイスによって疑わしいマルウェア インスタンスが分析される際の、レジストリ キーへのアクセス試行の順序。
Process（プロセス）	ネットワーク セキュリティ デバイスによってレポートされたプロセス。
プロセス MD5	プロセスの MD5 ハッシュ。
Process Path（プロセス パス）	ネットワーク セキュリティ デバイスによってレポートされたプロセスのパスの場所。
キー	ネットワーク セキュリティ デバイスによってレポートされたレジストリ キー（一部が省略されて表示されます）。
Name（名前）	ネットワーク セキュリティ デバイスによってレポートされたレジストリ キー名。
Value（値）	ネットワーク セキュリティ デバイスによってレポートされたレジストリ キー値。
Operation（操作）	レジストリ キーで行われた操作（setval（値の設定）、added（追加）など）。

レジストリ キーへのアクセスを試みたプロセスを Bit9 Server が把握している場合、このリストには［View Details（詳細の表示）］ボタンが含まれており、このプロセスの［File Details（ファイルの詳細）］ページを開くことができます。

このタブの［Action（アクション）］メニューには、選択したファイルに対して実行できる以下のコマンドが含まれています。

- ［**Ban Process Globally**（プロセスのグローバル禁止）］– すべてのポリシーでプロセス ファイルを禁止します。他の構成は必要ありません。
- ［**Ban by Policy**（ポリシーによるプロセス禁止）］– ポリシー別の禁止またはレポートのみの禁止を作成するためのダイアログ ボックスが開きます。
- ［**Remove Process Approval or Ban**（プロセス承認または禁止を削除）］– 任意の有効な禁止 / 承認を即座に削除します。
- ［**Create Registry Rule**（レジストリ ルールの作成）］–［Add Registry Rule（レジストリ ルールの追加）］ページが開きます。このプロセスから通知でレポートされたレジストリ キーへのアクセスを禁止するルールを作成するための値が事前に入力されています。詳細については、「レジストリ ルール」を参照してください。

[More Details（追加の詳細）] タブ

このタブには、現在の外部通知からの追加の詳細情報が表示されます。このタブに含まれる情報は、通知のタイプに応じて異なります。以下の表に、このタブに含まれる可能性があるフィールドを示します。

表 126：[More Details（追加の詳細）] タブのフィールド

フィールド	説明
Malware type（マルウェア タイプ）	外部通知でレポートされたマルウェアのタイプ。[External Notifications（外部通知）] テーブルの [Type（タイプ）] と同じ場合も、[Backdoor（バックドア）]、[HackTool（ハッカーツール）]、[Trojan（トロイの木馬）] など、より具体的なタイプの場合もあります。
Anomaly（異常）	異常
Application（アプリケーション）	ターゲットにされたアプリケーション
HTTP Header（HTTP ヘッダー）	外部通知によって Web 感染がレポートされた HTTP ヘッダー
Show XML Details（XML 詳細の表示）	外部ネットワーク セキュリティ デバイスからの完全なXML通知を含む新しいブラウザー タブが開きます。このアラートは、Bit9 コンソール Web サイトに保管されているファイル（「store」サブフォルダー内）から読み込まれます。 **注意**：XML ファイルが非常に大きい場合、このリンクを使用して開くと、ブラウザーのパフォーマンスとナビゲーションに問題が発生する場合があります。このリンクを右クリックして [**Save Target As**（ターゲットに名前を付けて保存）] または [**Save Link As**（リンクに名前を付けて保存）] を選択し、ファイルを別の場所に保存すると、別のビューアーでこのファイルを開くことができます。

[History（履歴）] タブ

[History（履歴）] タブは、外部通知ワークフローの監査証跡を提供します。ここには、すべてのステータス変更、その変更に関連するすべてのコメントが含まれています。[Notification Details（通知の詳細）] ページを既に表示している場合はこのタブをクリックしますが、[External Notifications（外部通知）] テーブルの通知の行の [Action（アクション）] 列で [History（履歴）] ボタンをクリックして履歴を表示することもできます。

関連通知の表示

[External Notification Details（外部通知の詳細）] ページに表示されている単一の通知に関連通知がある場合は、[Related Views（関連ビュー）] メニューに [**Show Related Notifications**（関連通知の表示）] コマンドが含まれています。関連通知とは、現在表示されている通知と同じ MD5 ハッシュが含まれている通知です。

このコマンドをクリックすると、リンクのクリック元の通知を含む関連通知が表示されるようにフィルターされた [External Notifications（外部通知）] テーブルが開きます。

XML 詳細の表示

外部通知は XML 形式でレポートされ、分析されたマルウェアの動作に関する情報が含まれています。Bit9 Server は、これらの XML 通知を解析し、データベースに重要情報を効率的に保管します。また各 XML 通知は、コンテンツ全体が、Bit9 Server の Bit9 インストール ディレクトリ の各ネットワーク セキュリティ デバイス ベンダー用の独立した「store」フォルダーに保管されます（Bit9\Integrations\PAN\store、Bit9\Integrations\CheckPoint\store、または Bit9\Integrations\FireEye\listener\store）。

注意

- 非常に大きい XML 詳細ファイルを開くと、ブラウザーのパフォーマンスとナビゲーションに問題が発生する場合があります。このリンクを右クリックして［Save Target As（ターゲットに名前を付けて保存）］または［Save Link As（リンクに名前を付けて保存）］を選択し、ファイルを別の場所に保存すると、別のビューアーでこのファイルを開くことができます。
- Palo Alto Networks からの通知に、複数の「Analysis Environment（分析環境）」タイプのレポートが含まれている場合は、［Show XML（XML を表示）］を使用すると、現在の通知の分析環境の XML 詳細のみが表示されます。
- ［XML Details（XML の詳細）］リンクは、Microsoft SCEP 通知では使用できません。

外部通知の完全な XML 詳細にアクセスする手順：

- 通知の［External Notification Details（外部通知の詳細）］ページで、［External Pages（外部ページ）］メニューの［**Show XML Details**（XML の詳細を表示）］をクリックします。完全な詳細が別のブラウザー ウィンドウに表示されます。

外部コンソールへのアクセス

大半のコネクターの［Notification Details（通知の詳細）］ページでは、［External Pages（外部ページ）］メニューのコマンドをクリックして、通知の提供元のアプライアンスのコンソールを開くことができます。このコンソールは新しいブラウザー ウィンドウで開きます。Bit9 コンソールのユーザーが資格情報を使用して外部アプライアンスの認証を受けていない場合、ブラウザーはログイン ページにリダイレクトされます。

マルウェアの詳細の取得

Microsoft SCEP 通知の場合は、［Notification Details（通知の詳細）］ページの［External Pages（外部ページ）］メニューが Microsoft Malware Protection Center の Threat Encyclopedia へのリンクになっており、［Malware Name（マルウェア名）］フィールドに表示された脅威の情報が表示されます。

通知のステータスの管理

Bit9 コンソールには、[External Notifications（外部通知）] テーブルと [External Notification Details（外部通知の詳細）] ページ両方に、各通知の [Status（ステータス）] フィールドが表示されます。通知のステータスは、通知への対応の進捗を追跡することのみを目的としており、ステータスの変更は通知ソースに返されません。通知のステータスに必須のフローはありませんが、以下のステータス管理ワークフローを参考にしてください。

通知のステータスの管理手順：

1. コンソール メニューで、[**Reports**（レポート）] > [**External Notification**（外部通知）] の順に選択し、確認する通知の隣の [View Details（詳細の表示）] ボタンをクリックします。[**External Notification Details**（外部通知の詳細）] ページが開きます。
2. この通知を検証したり、この通知にアクションを実行したりする場合は、[External Notification Details（外部通知の詳細）] ページの [Actions（アクション）] メニューで [Escalate Notification（通知のエスカレーション）] を選択します。ステータスが [Escalated（エスカレーション済み）] に変更されます。
3. [External Notification Details（外部通知の詳細）] ページ、[File Details（ファイルの詳細）] ページ、[Event（イベント）] ページの情報、ネットワーク セキュリティ デバイスのファイル分析、またはこの通知に適切な他の手段を使用して、通知を調査します。[Comments（コメント）] フィールドにエスカレーションに関連するコメントを入力します。
4. 通知内のファイルに対して講じるアクション（ファイルの禁止、カスタムまたはレジストリ ルールの作成など）を実行します。
   注意：禁止などのルール変更を行っても、要求自体の [Status（ステータス）] フィールドに影響はありません。ステータスは手動で変更する必要があります。
5. [Comments（コメント）] フィールドに解決に関連するコメントを入力します。
6. アクションを実行したら（またはアクションが不要な場合は）、[External Notification Details（外部通知の詳細）] の [Action（アクション）] メニューで [**Resolve Notification**（通知の解決）] を選択します。ステータスが [Resolved（解決済み）] に変更されます。
7. この通知に必要な処理が終了したら、[Comments（コメント）] フィールドに最後のコメントを入力し、[Actions（アクション）] メニューで [**Close Notification**（通知のクローズ）] を選択します。ステータスが [Closed（クローズ）] に変更され、ビューが [External Notifications（外部通知）] テーブルに戻ります。通知をクローズすると、この通知は [**Active Notifications**（アクティブな通知）] ビューから削除されます。ただし、[(**none**（なし）)] の保存済みビューを選択すると表示できます。

上記の説明は、[External Notification Details（外部通知の詳細）] ページの [Actions（アクション）] メニューからステータスを変更する手順です。ステータスは、同じページの [Status（ステータス）] ドロップダウン メニュー、または [External Notification（外部通知）] ページのテーブルの [Action（アクション）] メニューからも変更できます。

外部からレポートされたマルウェアの禁止

Bit9 Server は、外部ネットワーク セキュリティ デバイスによってマルウェア通知の一部としてレポートされたファイルまたはプロセスを禁止できます。これらのファイルやプロセスの禁止は、複数の方法で実行できます。

- 外部通知でレポートされたファイルの**手動でのファイルの禁止**
- 外部通知でレポートされた、レジストリ キーへのアクセスを試みた特定のプロセスを禁止する**レジストリ ルール**
- 外部通知でレポートされたディレクトリでのアクティビティを禁止する**カスタム ルール**
- 特定のファイル関連のイベントの発生時（このケースでは外部通知に起因）に、レポートのみの禁止またはその他のルールを自動的に作成する**イベント ルール**

レジストリ ルール、カスタム ルール、およびイベント ルールは、記述されたアクションを禁止するのではなく、「レポート」するように構成することもできます。

手動でのファイルの禁止

外部通知でレポートされたファイルを手動で禁止する手順は、Bit9 に登録されたファイルを禁止する場合とほぼ同じです。ただし、［External Notification Details（外部通知の詳細）］ページの［Action（アクション）］メニューから直接禁止を適用できるため、Bit9 エージェントが管理するエンドポイントに出現したかどうかを問わず、外部通知で特定されたマルウェアを禁止できます。

外部通知でマルウェアとしてレポートされたファイルを手動で禁止する手順：

1. ファイルを禁止する通知の隣にある［View Details（詳細の表示）］ボタンをクリックします。
2. ［External Notification Details（外部通知の詳細）］ページのいずれかの［Files（ファイル）］タブで、禁止する各ファイルの左のボックスをオンにします。
3. ［Action（アクション）］メニューで、チェック済みファイルに適用する禁止の種類を選択します。
   a. すべてのコンピューターでファイルを禁止するには、［**Ban Globally**（グローバル禁止）］を選択します。他の操作を必要とせずに禁止が作成されます。
   b. 禁止をカスタマイズする場合は、［**Ban by Policy**（ポリシーによる禁止）］を選択します。情報が一部入力された［Add File Rule（ファイル ルールの追加）］ページが開きます。このページで、高度な禁止またはレポートのみの禁止を選択できます。また、禁止を適用する特定のポリシーを選択できます。レポートのみの禁止は、禁止を完全に有効化する前にその動作を監視する必要があるときに有効です。禁止の構成が完了したら、［Save（保存）］をクリックします。

注意：［External Notification Details（外部通知の詳細）］ページの［Files（ファイル）］タブの［Action（アクション）］メニューには、関心のあるファイルを見つけることができるように以下の選択肢が含まれています。

- ［**Find By Name**（名前で検索）］
- ［**Find By Size**（サイズで検索）］
- ［**Find By Hash**（ハッシュで検索）］

［Software Rules（ソフトウェア ルール）］ページの［Files（ファイル）］タブ（コンソール メニューで［**Rules**（ルール）］>［**Software Rules**（ソフトウェア ルール）］を選択）に、作成した禁止が表示されます。外部通知から手動で作成された禁止は、プレフィックス「External_」にファイル名が付加された名前になります。

注意：一部の［External Notification（外部通知）］ページでは、システム上のオブジェクトにアクションの実行（レジストリ キーの変更やディレクトリへの書き込みなど）を試みた「プロセス」を禁止できます。これらのプロセスは、上記の説明と同じ手順で禁止できます。ただし、使用するコマンドは単純な［Ban（禁止）］ではなく［Ban Process（プロセスの禁止）］です。

マルウェアのレポートまたは禁止用の特別ルール

特定の通知では、標準のファイル禁止が最善の修復策ではないことがあります。Bit9 Connector は、疑わしいとして特定されたアクションを制御するための他の複数のルールを提供しています。このようなルールは、禁止と同様に、事前に入力された一部のルール データを使用して［External Notification Details（外部通知の詳細）］ページで作成できます。

レジストリ ルール

通知に疑わしいレジストリ エントリまたはアクティビティが含まれている場合、［External Notification Details（外部通知の詳細）］ページには［Registrty Keys（レジストリ キー）］タブが含まれています。このタブは、侵害された可能性があるキーに関する情報を提供します。レポートされたキーを選択して、以下を実行できます。

- キーへのアクセスを試みたプロセスを禁止する
- 以前に作成されたプロセスの禁止または承認を削除する
- キーへのアクセスを制御するレジストリ ルールを作成する

このコンテキストで作成された禁止は、［Files（ファイル）］タブで作成される禁止に似ています。レジストリ ルール コマンドには、さまざまなオプションがあります。

［Notification Details（通知の詳細）］ページからレジストリ ルールを作成する手順：

1. 目的の［Notification Details（通知の詳細）］ページで［**Registrty Keys**（レジストリ キー）］タブをクリックします。
2. ルールを作成するレジストリ キーの隣にあるボックスをチェックします。
3. ［Action（アクション）］メニューで、［**Create Registry Rule**（レジストリ ルールの作成）］を選択します。［Add Registry Rule（レジストリ ルールの追加）］ページが表示されます。ルール名と設定は、通知の詳細から事前に入力されています。

4. デフォルトでは、この方法で作成されるルールは、通知で特定されたプロセスから指定されたレジストリ キーへの書き込みをブロックし、この動作をすべてのユーザーとすべてのポリシーに対して行います。これらの設定は、ルールを保存する前に変更できます。［Write Action（書き込みアクション）］メニューのオプションで［**Report**（レポート）］を選択すると、このキーのアクティビティをレポートするがブロックは行わないように設定できます。ルールの最適な構成方法がわからない場合は、「レジストリ ルールの作成」（480 ページ）を参照してください。まずはルールのパラメーターの調査のみを行うという場合は、ルールを保存せずに**キャンセル**できます。
重要：ルール メニューには、指定された場所でのアクティビティを許可するオプションや、以前よりもプロセスの権限を昇格させるオプションも用意されています。事前に入力されている値を変更する場合は、これらのメニューでの選択肢に十分注意してください。
5. 必要に応じてルールを変更したら、［Save（保存）］ボタンをクリックします。新しいルールが作成され、Bit9 コンソールの［Software Rules（ソフトウェア ルール）］ページの［Registry（レジストリ）］タブに表示されます。

ディレクトリ制御用のカスタム ルール

疑わしいパス名エントリが含まれる通知では［External Notification Details（外部通知の詳細）］ページに［Directories（ディレクトリ）］タブが表示され、侵害された可能性があるディレクトリに関する情報が表示されます。このタブでは、ディレクトリを選択して、以下を実行できます。

- ディレクトリへのアクセスを試みたプロセスを禁止する
- 以前に作成されたプロセスの禁止または承認を削除する
- この場所へのアクセスを制御するカスタム ルールを作成する

このコンテキストで作成されるプロセス禁止は、［Files（ファイル）］タブで作成されるファイル禁止に似ています。カスタム ルール コマンドには、さまざまなオプションがあります。

［Notification Details（通知の詳細）］ページからカスタム ルールを作成する手順：

1. 目的の［Notification Details（通知の詳細）］ページで［**Directories**（ディレクトリ）］タブをクリックします。
2. ルールを作成するディレクトリの隣にあるボックスをチェックします。
3. ［Action（アクション）］メニューで、［**Create Custom Rule**（カスタム ルールの作成）］を選択します。［Add Custom Rule（カスタム ルールの追加）］ページが表示されます。ルール名と設定は、外部通知の詳細から事前に入力されています。

4. デフォルトでは、この方法で作成されるルールは、通知で特定されたプロセスから指定されたディレクトリへの書き込みをブロックし、この動作をすべてのユーザーとすべてのポリシーに対して行います。これらの設定は、ルールを保存する前に変更できます。[Execute Action（実行アクション）] メニューのオプションで［**Report**（レポート）］を選択すると、この場所のアクティビティをレポートするがブロックは行わないように設定できます。ルールの最適な構成方法がわからない場合は、「カスタム ルールの作成」（411 ページ）を参照してください。まずはルールのパラメーターの調査のみを行うという場合は、ルールを保存せずに**キャンセル**できます。
重要：ルール メニューには、指定された場所でのアクティビティを許可するオプションや、以前よりもプロセスの権限を昇格させるオプションも用意されています。事前に入力されている値を変更する場合は、これらのメニューでの選択肢に十分注意してください。
5. 必要に応じてルールを変更したら、［**Save**（保存）］ボタンをクリックします。新しいルールが作成され、Bit9 コンソールの［Software Rules（ソフトウェア ルール）］ページの［Custom（カスタム）］タブに表示されます。

エンドポイント上の疑わしいファイルの分析

外部デバイスまたはサービスとの間で統合とファイル分析を有効化している場合は、分析のために Bit9 Server ファイル インベントリのファイルを接続中のソースに送信できます。分析を有効化すると、Bit9 コンソールの複数の場所に［**Analyze with…**（… で分析）］コマンドが追加され、Palo Alto Networks、Check Point、または FireEye のアプライアンスかサービスにファイルを送信できるようになります。Check Point および FireEye の場合は、これらのコマンドに Windows のバージョン固有のサブメニューが含まれているため、ファイルを分析する環境を選択できます。これらのコマンドは、以下の場所で使用できます。

- ［File Catalog（ファイル カタログ）］ページ、［Files on Computers（コンピューター上のファイル）］ページ、および［Find Files（ファイルの検索）］結果ページの［Action（アクション）］メニュー（1 つ以上のファイル）
- ［File Details（ファイルの詳細）］ページおよび［File Instance Details（ファイル インスタンスの詳細）］ページの［Advanced（詳細）］メニュー（単一のファイル）
- ［Events（イベント）］ページの［Action（アクション）］メニュー（1 つ以上のファイル）
- ファイルが表示される他のテーブル ページ

注意

Bit9 ファイル インベントリのファイルは、ネットワーク上でアクセスできず一時的に使用できない場合や、一時ファイルや削除済みファイルであるため永続的に使用できない場合があります。分析のために外部デバイスにこのようなファイルの送信を試みたとき、そのファイルが見つからなかった場合には、Bit9 は同じファイルの別のインスタンスを検索し、送信しようとします。別のインスタンスが存在しない場合は、この分析要求によってエラーが発生します。

プラットフォームに関する注意：現在 Bit9 Connector を介したファイル分析は、Windows エージェントからのファイルのみサポートされています。

分析のためにファイルを外部サービスに送信する手順：

1. ファイルが表示されているテーブルで、送信するファイルの隣にあるボックスをオンにします。
2. ［Action（アクション）］メニューで、使用可能な［**Analyze with…**（… で分析）］コマンドを選択します。使用できるコマンドは、コネクターに対して有効化したアプライアンスによって異なります。
   a. Palo Alto Networks - Bit9 間のファイル分析を有効化している場合は、［**Analyze with Palo Alto Networks WildFire**（Palo Alto Networks WildFire で分析）］を選択できます。
   b. ファイル分析のために Check Point - Bit9 間の統合を有効化している場合は、［**Analyze with Check Point**（Check Point で分析）］サブメニューを選択し、その下でファイルを分析する分析環境を指定できます。指定するのは、オペレーティング システムと、Microsoft Office や Adobe Acrobat などの一般的なツールです（例：**win7；Office 2010；Adobe 9**）。
   c. ファイル分析のために FireEye - Bit9 間の統合を有効化している場合は、［**Analyze with FireEye**（FireEye で分析）］サブメニューを選択し、その下でファイルを分析するオペレーティング システムを指定できます（例：**win7**）。オペレーティング システムの正確な名前と選択肢は、FireEye 環境のセットアップ方法によって異なります。

   選択した分析ソースへのファイルのアップロードがスケジュールされたことを示すメッセージが表示されます。
3. または、単一ファイルの［File Details（ファイルの詳細）］ページか［File Instance Details（ファイル インスタンスの詳細）］ページを開き、［Advanced（詳細）］メニューで［**Analyze with…**（… で分析）］コマンドを選択します。

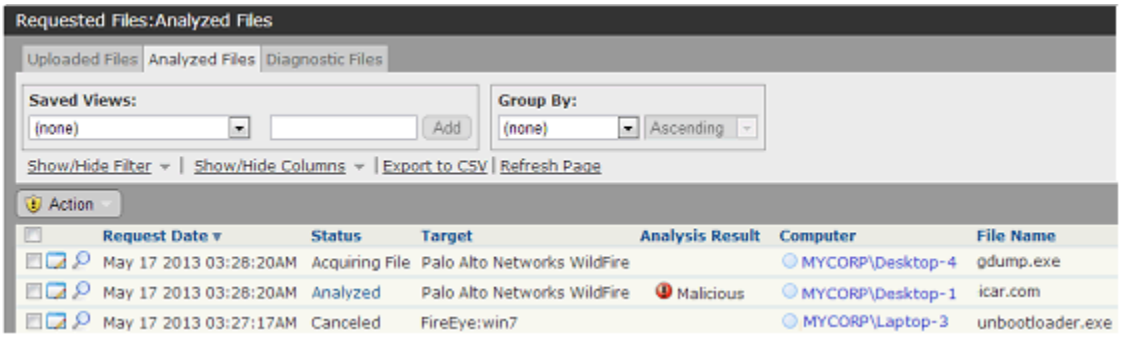
   これらのページでは、同一の分析プロバイダーにすでにファイルが送信されている場合は警告が表示されますが、警告で **[OK]** をクリックすると、ファイルはもう一度アップロードされます。
4. 分析の進捗を監視するには、［**Tools**（ツール）］>［**Requested Files**（要求されたファイル）］を選択し、［**Analyzed Files**（分析されたファイル）］をクリックして送信済みファイルのテーブルを表示します。

分析のために送信されたファイルの監視

Bit9 コンソールの［Requested Files（要求されたファイル）］ページの［Analyzed Files（分析されたファイル）］タブには、分析のために外部サービスに送信されたすべてのファイルのステータスと分析結果（分析が完了している場合）が表示されます。このページのデフォルト ビューでは、すべてのファイルが要求日を基準に並べ替えられて表示されますが、さらに的を絞ったファイル リストを提供する［Saved Views（保存済みビュー）］も利用できます。

- Analysis in Progress（進行中の分析）

- Completed Analysis（完了した分析）
- Analysis Errors（分析エラー）
- Files Submitted to Check Point（Check Point に送信済みのファイル）
- Files Submitted to FireEye（FireEye に送信済みのファイル）
- Files Submitted to WildFire（WildFire に送信済みのファイル）



このテーブルには以下の列を表示できます（デフォルトでは一部のみ表示）。

- ［**Request Date**（要求日）］– このファイルのファイル分析要求が送信された日。
- ［**Requester**（要求者）］– アップロードを要求したユーザー。
- ［**Upload %**（アップロードの割合）］-（分析ではなく）アップロードが完了した割合。
- ［**Status**（ステータス）］– このファイルが分析プロセスのどの時点にあるかを示します。ステータスの値の説明については、「分析のステータス」を参照してください。
- ［**Analysis Results**（分析結果）］– 分析が完了すると、このフィールドは分析の結果（Clean（クリーン）、Potential Risk（危険な可能性あり）、または Malicious（悪質））を示します。
- ［**Computer**（コンピューター）］– ファイルのアップロード元のコンピューター。
- ［**File Name**（ファイル名）］– ファイルがアップロードされた場所でのファイルの名前。
- ［**File Size**（ファイル サイズ）］– Bit9 エージェントが管理するコンピューターに表示される（または表示されていた）ファイル サイズ。
- [**MD5**] – ファイルの MD5 ハッシュ。
- ［**Date Modified**（変更日）］– このファイルのエントリが最後に変更された時間。
- ［**Error**（エラー）］– ファイル分析のためのアップロードまたは送信に関連するエラー。
- ［**File Path**（ファイル パス）］– ファイルがアップロードされた時点でファイルが格納されていた、ソース コンピューター上のディレクトリ。ファイルの現在の場所とは限りません。
- ［**Last Modified by**（最終変更者）］– 関連アクションを実行して、このファイルの［Analyzed Files（分析されたファイル）］エントリを最後に変更したユーザー。

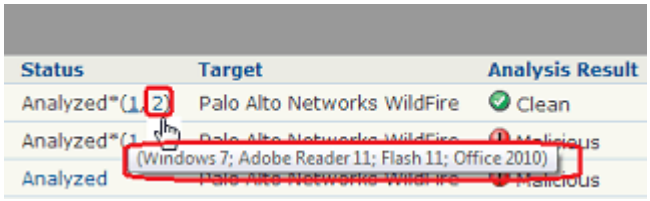
- ［**Prevalence**（普及度）］– Bit9 が管理するコンピューターでのこのファイルの普及度。
- ［**Provider**（プロバイダー）］– Palo Alto Networks または FireEye。
- [**SHA-256**] – このファイルの SHA ハッシュ。
- ［**Source**（ソース）］– この分析要求のソース。［Manual（手動）］または［Event rule（イベント ルール）］になります。
- ［**Source Name**（ソース名）］– ソースが［Event rule（イベント ルール）］の場合は、ルールの名前。
- ［**Target**（ターゲット）］– ファイル分析のターゲット。分析を開始したユーザーに指定された選択肢に応じて、[**Palo Alto Networks WildFire**]、[Check **Point**: <*Target Environment*>]、または [FireEye: <*Windows version*>] になります。ローカル アプライアンスで実行された **Check Point** および FireEye 分析の場合は、このフィールドにアプライアンス名も表示されます例：**Check Point**:win7;Office2010;Adobe9:Appliance1

分析の対象になった Bit9 エージェントからのファイルは、Bit9 Server には保管されず、サーバーにダウンロードすることも、このテーブルから削除することもできません。

分析のステータス

［Analyzed Files（分析されたファイル）］タブの［Status（ステータス）］列は、ファイル分析の進捗状況に関するフィードバックを提供します。テーブルの［Status（ステータス）］の値にマウスを乗せると追加情報が表示されます。値は以下のいずれかになります。

- ［**Acquiring File**（ファイル取得中）］– エンドポイントからアップロードして分析のためにデバイスに送信する必要があるファイルのアップロードが完了していないことを示します。
- ［**Error**（エラー）］– アップロードまたは分析が失敗しました（ファイル名またはパスが存在しないことなどが原因）。このフィールドの上にマウスを乗せると、エラーの詳細を含むツールチップが表示されます。
- ［**Canceled**（キャンセル済み）］– コンソール ユーザーによってアップロードがキャンセルされました。
- ［**Analyzing**（分析中）］– 分析のためにファイルがデバイスに移動されました。
- ［**Analyzed**（分析済み）］– Bit9 Server がデバイスから XML レポートを受信しました。この状況が発生すると、ファイルの［Status（ステータス）］値が［Notification Details（通知の詳細）］へのリンクになります。
- ［**Analyzed* (1,2…)**（分析済み *（1,2…））］–［Analyzed（分析済み）］に括弧で囲われた一連の数字が続く場合は、WildFire から複数のファイル分析結果が返されたことを示しています。異なる「分析環境」から、それぞれの結果が返されます。数字の上にマウスを乗せると、その数字が表している分析環境が表示されます。



数字をクリックすると、その分析環境に固有の［Notification Details（通知の詳細）］が表示されます。値の詳細については、「複数の分析環境からの通知」（884 ページ）を参照してください。

複数の結果が含まれるファイルの［Analysis Results（分析結果）］には、WildFire によって提供された最上位分析値がレポートされます。

注意

ファイルの分析結果が存在する場合は、結果はそのファイルの［File Details（ファイルの詳細）］ページと［File Instance Details（ファイル インスタンスの詳細）］ページの［External Analysis Results（外部分析結果）］パネルに表示されます。

［Analyzed Files（分析されたファイル）］タブでのアクション

［Analyzed Files（分析されたファイル）］タブの［Action（アクション）］メニューは、同一または異なる分析プロバイダーへの分析要求を再試行するオプションを提供します。以下のオプションが含まれています。

- ［**Cancel Analysis**（分析のキャンセル）］– チェック済みの分析エントリをキャンセルします。キャンセルが不可能な 1 つまたは複数のエントリに対しては効力がありません。
- ［**Retry Analysis**（分析の再試行）］– チェック済みの分析エントリを再試行します。再試行が不可能なエントリ（このファイルの分析がすでに保留中の場合など）に対しては、効力がありません。
- ［**View Bit9 SRS Cloud Data**（Bit9 SRS クラウド データの表示）］– Bit9 SRS からチェック済みファイルの情報を取得します（可能な場合）。
- ［**Analyze with…**（… で分析）］– 使用可能な分析プロバイダー（Check Point、Palo Alto Networks WildFire、FireEye）ごとにオプションが表示されます。Check Point および FireEye の場合は、適切なオペレーティング システムを送信先に設定するオプションがあります。

これらのいずれかのアクションが選択されたときに、既存のアップロード済みファイルが使用可能な場合は、分析のための送信でこのファイルが使用されます。使用できない場合は、ファイルがアップロードされた後で送信されます。

注意

［Requested Files（要求されたファイル）］ページには、［Analyzed Files（分析されたファイル）］タブに加え、この付録で説明されていない他の 2 つのタブがあります。

- ［Uploaded Files（アップロード済みファイル）］– Bit9 で管理されるエンドポイントから Bit9 Server にアップロードされて登録されたファイルが表示されます。
- ［Diagnostic Files（診断ファイル）］– Bit9 Server にアップロード済みの診断ファイルが表示されます。

一般的なファイルおよび診断ファイルのアップロードの詳しい詳しい説明については、付録 E、「エージェントからのファイルのアップロード」を参照してください。

Bit9 でのコネクター関連イベントのロギング

Bit9 の［Events（イベント）］ページは、環境内の Bit9 アクティビティに関連して記録されたすべてのイベント（ブロックされたファイル、実行された未承認ファイル、システム管理プロセス、コンソール ユーザーによるアクションなど）へのアクセスを提供します。Bit9 Server は、イベント ボリュームの影響をほとんど受けずに、接続されているコンピューターのイベント データをほぼリアルタイムで更新します。詳細については、「イベント レポート」（590 ページ）を参照してください。

Bit9 の Syslog イベントを出力して、他のシステムで処理することもできます。詳細については、「イベント管理のオプション」（753 ページ）を参照してください。

Bit9 Connector for Network Security Devices が有効化されると、Bit9 イベント ログにコネクター関連のイベントが生成されます。ネットワーク セキュリティ デバイスとの統合により、Bit9 イベントにはいくつかの重要な追加や変更が発生します。

- ［**External Notification**（外部通知）］– このイベント サブタイプ（「サブタイプ」は最も具体的なイベント識別子です）は［Discovery（検出）］タイプに属します。このイベントは、Bit9 Server が受信した（現在は Check Point、Palo Alto Networks、または FireEye からの）外部通知に対して生成されます。ただし、ファイル送信の結果として受信される外部通知に対しては、［File Analysis Complete（ファイル分析完了）］も生成される場合は生成されません。
- **他のイベントのコネクター関連アクション** – コネクター関連のアクティビティをレポートする可能性がある他のイベントを表 127 に示します。ここに示したイベント サブタイプの大半は、他の目的にも使用されます。これらのサブタイプとして発生する可能性はあっても、ネットワーク セキュリティ デバイスのアクティビティに関連していないイベントの説明はここには含まれていません。Bit9 のすべてのイベント タイプおよびサブタイプの完全な説明と、Syslog イベント出力を有効化する方法については、別途提供されている『Bit9 Events Guide（Bit9 イベント ガイド）』を参照してください。

表 127：Bit9 イベント ログのコネクター関連イベント

イベント タイプ	イベント サブタイプ	外部通知関連の説明と例
Discovery（検出）	Malicious File Detected（悪意のあるファイルの検出）	未知のファイル '$filename$' [$param1$] が $param3$ によって悪質と特定されました。 または ファイル '$filename$' [$param1$] が $param3$ によって悪質と特定されました。
Discovery（検出）	Potential Risk File Detected（危険な可能性があるファイルの検出）	$param3$ からの未知のファイル '$filename$' [$param1$] が $param3$ によって危険な可能性があると特定されました。 または $param3$ からのファイル '$filename$' [$param1$] が $param3$ によって危険な可能性があると特定されました。
Discovery（検出）	External Notification（外部通知）	$Provider$ が $src_ip から $target_ip への ファイル '$filename' で、名前 $malware name$ の $malware type$ をレポートしました。
Computer Management（コンピューター管理）	File Upload Requested（ファイル アップロード要求済み）	ユーザー '$username$' がコンピューター '$computer$' からのファイル [$hash$] のアップロードを要求しました。 または ユーザー '$username$' がコンピューター '$computer$' からのファイル '$param1$' のアップロードを要求しました。 または イベント ルール '$ruleName$' によって、コンピューター '$computer$' からのファイル [$hash$] のアップロードが要求されました。 注意：レポートされるアップロードは外部通知と無関係な場合があります。
Computer Management（コンピューター管理）	File Upload Completed（ファイル アップロード完了）	コンピューター '$computer$' からのファイル [$hash$] のアップロードが完了しました。 または コンピューター '$computer$' からのファイル '$param1$' のアップロードが完了しました。

イベント タイプ	イベント サブタイプ	外部通知関連の説明と例
Computer Management（コンピューター管理）	File Upload Canceled（ファイル アップロード キャンセル）	ユーザー '$username$' がコンピューター '$computer$' からのファイル [$hash$] のアップロードをキャンセルしました。 または ユーザー '$username$' がコンピューター '$computer$' からのファイル '$param1$' のアップロードをキャンセルしました。
Computer Management（コンピューター管理）	File Upload Error（ファイル アップロード エラー）	コンピューター '$computer$' からの ファイル [$hash$] のアップロードが エラー '$param2$' のために失敗しました。 または コンピューター '$computer$' からの ファイル '$param1$' のアップロードがエラー '$param2$' のために失敗しました。
Computer Management（コンピューター管理）	File Upload Deleted（ファイル アップロード削除）	ユーザー '$username$' がアップロード済みファイル [$hash$] を削除しました。 または ユーザー '$username$' がアップロード済みファイル '$param1$' を削除しました。
General Management（一般管理）	Event rule created（イベント ルール作成）	イベント ルール '$param1$' が '$userName$' によって作成されました。
General Management（一般管理）	Event rule modified（イベント ルール変更）	イベント ルール '$param1$' が '$userName$' によって変更されました。
General Management（一般管理）	Event rule deleted（イベント ルール削除）	イベント ルール '$param1$' が '$userName$' によって削除されました。
Server Management（サーバー管理）	File analysis requested（ファイル分析要求）	ユーザー '$username$' が '$param1$' によるファイル [$hash$] の分析を要求しました。 または イベント ルール '$ruleName$' によって、$param1$ によるファイル [$hash$] の分析が要求されました。
Server Management（サーバー管理）	File analysis completed（ファイル分析完了）	ファイル '$filename$' [$hash$] が '$param1$' によって正常に分析されました。疑わしい点は見つかりませんでした。 または ファイル '$filename$' [$hash$] が '$param1$' によって正常に分析されました。悪質としてレポートされました。

イベント タイプ	イベント サブタイプ	外部通知関連の説明と例
Server Management（サーバー管理）	File analysis canceled（ファイル分析キャンセル）	ユーザー '$username$' が '$param1$' によるファイル '$filename$' [$hash$] の分析をキャンセルしました。
Server Management（サーバー管理）	File analysis error（ファイル分析エラー）	'$param1$ によるファイル '$filename$' [$hash$] の分析がエラー '$param2$' のために失敗しました。
Server Management（サーバー管理）	Server error（サーバー エラー）	$param1$ **注意**：これはコネクター固有のイベントではありませんが、デバイスとの接続または認証の失敗など、コネクター関連のエラーがレポートされることがあります。
Server Management（サーバー管理）	Connector restart（コネクター再起動）	コネクターが起動されました。ビルド情報：$param1$.
Server Management（サーバー管理）	Connector shutdown（コネクター シャットダウン）	コネクターがクリーンにシャットダウンされました。

追加のログ情報

Bit9 イベント ログだけでなく、コネクター統合のログ ファイルで入手できる情報も有益に活用できることがあります。この情報は、Bit9 インストール フォルダーの以下の場所に保存されています。

- **Check Point** – \Bit9\Integrations\CheckPoint\B9ConnectorCP.bt9
- **FireEye** – \Bit9\Integrations\FireEye\listener\debug.log
- **Palo Alto Networks** – \Bit9\Parity Server\Reporter\ParityReporter.log

付 録 D

診断ファイル

セクション

概要

Bit9 コンソールには、Bit9 Server と Bit9 エージェント用の特定の診断ファイルを表示するページがあります。これらのファイルは、Bit9 サポートと協力して Bit9 環境の問題を調査するときに便利です。

診断ファイルは［Requested Files（要求されたファイル）］ページの［Diagnostic Files（診断ファイル）］タブに表示されます。以下のファイルが含まれます。

- サーバーのインストール ログとダンプ ファイル
- コンソール ユーザーが要求したエージェント診断ファイル

サーバーのインストール ログとダンプファイルは、サーバーのアクティビティによって作成されると、タブに自動的に表示されます。エージェント診断ファイルは［Computers（コンピューター）］ページまたは［Computer Details（コンピューターの詳細）］ページで要求する必要があります。サーバーにアップロード後、これらのファイルは Bit9 コンソールを実行しているコンピューターにダウンロードできます。

エージェントからファイルを選択してアップロードする機能とは異なり、診断ファイルは特別なライセンスや権限がなくてもアクセスできます。

注意

この付録では「診断ファイル」のアップロードについてのみ説明します。エージェントからのその他のファイルのアップロードについては、付録 E、「エージェントからのファイルのアップロード」を参照してください。この機能には、ライセンスが別途必要です。

エージェント診断ファイルのアップロード

エージェント診断ファイルのアップロードは［Computers（コンピューター）］ページまたは［Computer Details（コンピューターの詳細）］ページから開始できます。［Computers（コンピューター）］ページでは、1 つ以上のコンピューターからファイルをアップロードできます。

1 つのエージェントの診断ファイルのアップロードを開始する手順：

1. コンソール　メニューで、［**Assets**（アセット）］>［**Computers**（コンピューター）］の順に選択します。［Computers（コンピューター）］ページが表示されます。
2. 統計情報または診断情報のアップロード元のコンピューターを検索し、その詳細ページを開きます。
3. ［Computer Details（コンピューターの詳細）］ページで、［Advanced（詳細）］メニューの［**Other Actions**（その他のアクション）］を選択してから、［Other Actions（その他のアクション）］メニューで［**Upload diagnostic files**（診断ファイルのアップロード）］を選択します。

   問題が発生しない限り、［Computer Details（コンピューターの詳細）］ページに、選択したファイルのアップロードがスケジュールされたことを示すメッ

セージが表示されます。[Diagnostic Files（診断ファイル）] タブで、このエージェントの新しいzipファイルが利用できるようになったかどうかを確認できます。

1 つ以上のエージェントの診断ファイルのアップロードを開始する手順：

1. コンソール　メニューで、[**Assets**（アセット）] > [**Computers**（コンピューター）] の順に選択します。[Computers（コンピューター）] ページが表示されます。
2. 診断ファイルをアップロードする各コンピューターの横にあるボックスをオンにし、[Action（アクション）] メニューで [**Upload diagnostic files**（診断ファイルのアップロード)] を選択します。確認ダイアログが表示されます。
3. 確認ダイアログで **[OK]** をクリックしてアップロードを開始します。ステータス メッセージには、要求が正常に実行されたかどうかと、何台のコンピューターの診断ファイルがサーバーに送信されるかが表示されます。

アップロードのキャンセルまたは再試行

アップロードが完了しなかった場合、アップロードをキャンセルできます。この操作は、アップロード開始時にコンピューターを誤って必要以上に多く選択した場合や、テーブルに表示されたファイル サイズが大きすぎる場合に実行できます。

診断ファイルのアップロードをキャンセルする手順：

1. コンソール メニューで、[**Tools**（ツール）] > [**Requested Files**（要求されたファイル)] の順に選択します。
2. [**Diagnostic Files**（診断ファイル)] タブをクリックします。アップロードされた診断ファイル、アップロード中のファイル、または要求されたもののアップロードされなかったファイルがテーブルに表示されます。
3. アップロードをキャンセルする各ファイルの横にあるボックスをオンにし、[Action（アクション)] メニューで [**Cancel Uploads**（アップロードをキャンセル)] を選択します。
4. 確認ダイアログで **[OK]** を選択します。

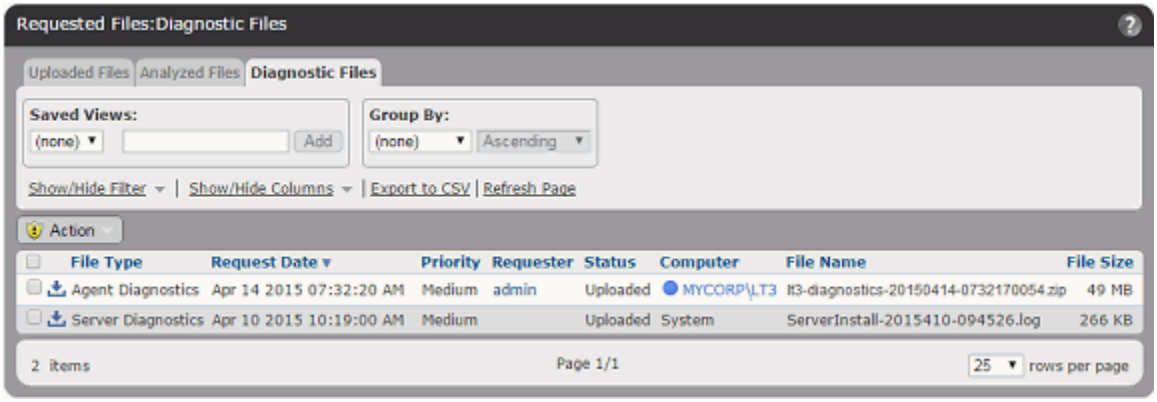
アップロードが失敗した、またはアップロードをキャンセルした場合、[Diagnostic Files（診断ファイル)] ページでそのファイルのボックスをオンにし、[Action（アクション)] メニューで [**Retry Uploads**（アップロードを再試行)] を選択すると、アップロードを再試行できます。

診断ファイルの表示

診断ファイルは、［Requested Files（要求されたファイル）］ページの［Diagnostic Files（診断ファイル）］タブに表示されるテーブルに一覧表示されます。

診断ファイルを表示する手順：

1. コンソール メニューで、［**Tools**（ツール）］>［**Requested Files**（要求されたファイル）］の順に選択します。
2. ［**Diagnostic Files**（診断ファイル）］タブをクリックします。サーバーにアップロードされた診断ファイルがテーブルに表示されます。



エージェントからの診断ファイルのアップロードを要求すると、そのエージェントに関連する診断ファイルとログファイルを含んだ zip ファイルがサーバーにアップロードされます。たとえば Windows システムの場合、zip ファイルには Bit9 エージェントのログ フォルダー (ProgramData\Bit9\Parity Agent\Logs) と Windows フォルダーから選ばれたログ ファイルが含まれます。zipファイルに含まれるファイルの一覧は、オペレーティング システム プラットフォームによって異なります。

アップロードされた診断ファイルは、以下の形式で命名されます。

*<computername>***-diagnostics-***<date>***-***<time>***.zip**

サーバー診断ファイルは「**.log**」、「**.dmp**」、またはその他の形式になる場合があります。

表 128 に［Diagnostic Files（診断ファイル）］ページで使用できる列を示します。デフォルトで表示されるものと、追加する必要があるものとがあります。

表 128：[Diagnostic Files（診断ファイル）] テーブルの列

列	説明
Actions（アクション）	[Action（アクション）] 列には、アクション メニューのコマンドを適用するファイルを選択するためのチェックボックスと、個々のファイルにアクションを実行するためのボタンがあります。このページの [Action（アクション）] メニューには次のコマンドがあります。 • [**Cancel Uploads**（アップロードをキャンセル）] – オンにしたファイルのアップロードをキャンセルします（アップロードが完了していない場合）。 • [**Retry Uploads**（アップロードを再試行）] – オンにしたファイルのアップロードを再試行します。 • [**Delete Uploads**（アップロードを削除）] – オンにしたファイルのテーブル行を削除するとともに、ファイルが正常にアップロードされている場合は、サーバーからファイルを削除します。  Bit9 Server から、コンソールを表示しているコンピューターにファイルをダウンロードします（正常にアップロードされている場合）。
Priority（優先度）	保留中のファイルをサーバーにアップロードする優先度。診断ファイルの場合、優先度は常に [**Medium**（中）] です。
Request Date（要求日）	ファイルのアップロードが要求された日時。
Requester（要求者）	アップロードを要求したコンソール ユーザー。ファイルがサーバー ログの場合は空白です。

列	説明
Status（ステータス）	ファイルのアップロード ステータス。次のいずれかの値になります。 • [**Uploaded**（アップロード済み）] – アップロードが正常に完了し、ファイルをサーバー上で使用できます。 • [**Uploading**（アップロード中）]– アップロードは進行中ですが、まだ完了していません。サーバーによるファイルの受信は一部完了しています。このステータスが表示されるのは、ファイルが非常に大きい場合だけです。 • [**Initiated**（開始済み）] – ファイルが保存されているエージェントがアップロード タスクを受信しました。 • [**Queued**（待機中）] – アップロード タスクがまだエージェントに送信されていません。 • [**Error**（エラー）] – アップロードは失敗しました。このステータスの上にカーソルを合わせると、エラー メッセージが表示されます。エラーには、「No file with hash（ハッシュのあるファイルが存在しない）」、「The system cannot find the path specified（システムが指定したパスを検出できない）」、「The system cannot find the file specified（システムが指定したファイルを検出できない）」などがあります。 • [**Canceled**（キャンセル済み）] – コンソール ユーザーによってアップロードがキャンセルされました。
Computer（コンピューター）	ファイルのアップロード元のコンピューターの名前。
File Name（ファイル名）	アップロードしたファイルの名前。
File Size（ファイル サイズ）	ファイルのサイズ（バイト単位）。
Upload %（アップロードの割合）	アップロードの完了割合。アップロードが完了すると「100%」と表示されます。アップロードが失敗した場合や、アップロードがまだ開始されていない場合は、「0%」と表示されます。
Upload Date（アップロード日）	ファイルがサーバーにアップロードされた日時。
Upload Directory（アップロード ディレクトリ）	ファイルのアップロード先の Bit9 Server のディレクトリ。手動アップロードの場合、値は [(default)（(デフォルト)）] です。この場合、[System Configuration（システム構成）] ページの [Advanced Options（高度なオプション）] タブで構成されているディレクトリが使用されます。イベント ルールによるアップロードの場合、実際のパスが表示されます。
Error（エラー）	ファイルのアップロードを妨げたエラーの説明。デフォルトでは表示されません。
File Path（ファイル パス）	ファイルのアップロード元のエージェント コンピューターの場所。デフォルトでは表示されません。

列	説明
Prevalence（普及度）	サーバーにレポートするBit9管理コンピューターのうち、このファイルが存在するコンピューターの数。
MD5	ファイルの MD5 ハッシュ。
SHA256	ファイルの SHA-256 ハッシュ。
Source（ソース）	アップロードの要求ソース。[Event rule（イベント ルール）] か [Manual（手動）] のどちらかです。
Source Name（ソース名）	イベント ルールによる要求であった場合は、ルール名。手動による要求であった場合は、このフィールドは空白です。

アップロードされた診断ファイルの削除

診断ファイルが不要になった場合、[Diagnostic Files（診断ファイル）] ページでそのファイルの行の横にあるボックスをオンにし、[Action（アクション）] メニューから [Delete Uploads（アップロードを削除）] を選択すると、サーバーからファイルを削除できます。

付 録 E

エージェントからのファイルのアップロード

セクション

概要

Bit9 Security Platform では、すべてのアクティブなモードで、ソフトウェアの増殖を監視してアクティビティのオーディット トレールを生成する機能を使用できます。監視中に確認された情報によっては、特定のアクティビティに関連する実際のファイルにアクセスすることが必要になる場合もあります。オプションのファイル アップロード機能では、Bit9 Agent 7.0.0 以降を実行しているコンピューターから Bit9 Server に任意のファイルのコピーをアップロードできます。

ファイル アップロード機能を利用するには、ファイル アップロード機能だけのために、または Bit9 Connector ライセンスの一部として、特別なライセンス キーを適用する必要があります。Bit9 ライセンスを適用する手順については、「Bit9 Platform ライセンスの管理」（783 ページ）を参照してください。

注意

分析のためにサードパーティのデバイスまたはサービスにファイルを送信するには、ファイル アップロード機能を使用します。ただし、分析の要求によって実行されるアップロードは、ファイル アップロードのユーザー インターフェイスには表示されず、またここでは取り上げません。分析用ファイルのアップロードに関連するプロセスについては、付録 C、「Bit9 Connector for Network Security Devices」を参照してください。

診断ファイルはエージェント コンピューターからアップロードできます。また、特殊なケースではサーバーからアップロードすることも可能です。診断ファイルは通常のファイル アップロードとは別のタブにカタログ登録されていますが、ファイルを操作するためのユーザー インターフェイスはほとんど同じです。

ファイル アップロード機能へのアクセスの有効化

重要

- この機能の権限は、デフォルトでは「admin」アカウントおよび「Administrator」アカウント グループのメンバーに付与されていません。この権限は明示的に追加する必要があります。
- その他の Bit9 の機能では、エージェント管理コンピューター上のファイルに関するデータが得られます。それに対してこの機能では、適切な権限を持つコンソール ユーザーが実際のファイルをアップロードできます。この機能を使用する場合は細心の注意を払い、他のユーザーのコンピューターおよびファイルにアクセスする際に組織のポリシーに完全に準拠する必要があります。機能に絶対にアクセスする必要がある Bit9 コンソール ユーザーにのみ、機能を使用する権限が与えられていることを確認してください。

ファイル アップロード機能へのアクセスは、以下の権限によって制御されます。

- **ツール アセットの View file uploads（ファイルのアップロードの表示）**–［Requested Files（要求されたファイル）］ページでアップロードされたファイルを表示できます。
- **ツール アセットの Manage uploads of inventoried files（登録済みファイルのアップロードの管理）**–エージェント コンピューターからファイルの手動アップロードを開始できます。また、ファイルをアップロードするイベント ルールを作成することもできます。この権限は、Bit9 によって追跡の対象と見なされたファイル（実行可能ファイルおよびスクリプト）のみに適用されます。
- **ツール アセットの Manage uploads of files by pathname（パス名によるファイルのアップロードの管理）** – エージェント コンピューターからファイルの手動アップロードを開始できます。この権限では、Bit9 インベントリに含まれていないファイルも含めて、パス名によるファイルのアップロードを実行できます。
- **ツール アセットの Access uploaded files（アップロードされたファイルへのアクセス）** – サーバーにアップロードされたファイルをダウンロードできます。

機能アクセス権の有効化の詳細については、「アカウント グループの権限」（108 ページ）を参照してください。

アップロードのスケジュール

Bit9 コンソールの複数の場所で、手動でファイルをアップロードするコマンドを使用できます。使用できる場所は以下のとおりです。

- ［Events（イベント）］ページ（コンピューター上に存在するファイルが表示されるイベントのページ）
- ［Approval Requests（承認要求）］ページ
- ［Files Catalog（ファイル カタログ）］テーブルと［Files on Computers（コンピューター上のファイル）］テーブル

- ［Find File Results（ファイル検索の結果）］テーブル
- ［Snapshot Content（スナップショット コンテンツ）］テーブル
- ［File Details（ファイルの詳細）］ページと［File Instance Details（ファイル インスタンスの詳細）］ページ
- ［Computer Details（コンピューターの詳細）］ページ（パスによるファイルのアップロードのみ）

これらのページの大半で、Bit9 によって追跡対象ファイル（つまり、実行可能ファイル）と識別されてライブ インベントリに追加されたファイルのコピーをアップロードできます。［Computer Details（コンピューターの詳細）］ページでは、ファイルが Bit9 ファイル インベントリ内に存在するかどうかにかかわらず、コンピューター上の「すべて」のファイルのコピーをアップロードできます。どのファイルをアップロードしても、元のファイルはエージェント コンピューター上に残ります。インベントリからファイルをアップロードするための権限とパスでファイルをアップロードするための権限は異なることに注意してください。

重要

2 ギガバイトを超えるファイルのアップロードは推奨されません。2 GB を超えるファイルは、アップロードが失敗して「通信エラー」が表示される場合があります。

手動でのアップロードの実行に加えて、特定のイベントが発生したときにファイルをアップロードするイベント ルールを作成できます。詳細については、「イベント ルール」（517 ページ）を参照してください。

アップロード コマンドを正常に実行すると、アップロードがスケジュールされたことを示すメッセージがコンソール ページに表示されます。通常、アップロードはほぼ即座に開始されますが、Bit9 Server の他のアクティビティやアップロードするファイルのサイズによって遅延が生じる場合があります。また、Bit9 Server はファイルをアップロードするために少なくとも読み取り権限を必要とします。他のプログラムによって開かれている一部のファイルはアップロードできません。Bit9 Server がエージェント管理コンピューター上の要求されたファイルに対する読み取り権限を持っていない場合、［Uploaded Files（アップロードされたファイル）］テーブルにそのファイルに関するエラー メッセージが表示されます。

アップロードがスケジュールされているファイルが存在するコンピューターが現在接続されていない場合、アップロードは後で試行されます。また、エージェント側のエラーによりファイルのアップロードが中断された場合、アップロードは再試行されます。

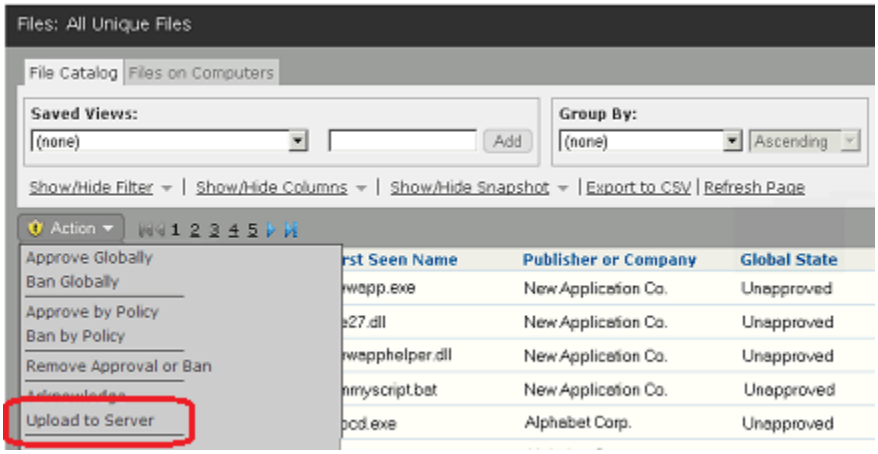
テーブルからの登録済みファイルのアップロードの開始

ファイル リンクがあるテーブル ページ（［File Catalog（ファイル カタログ）］、［Files on Computers（コンピューター上のファイル）］、［Events（イベント）］など）では、1 つ以上のファイルのアップロードを一度にスケジュールできます。アップロードを要求すると、ハッシュに一致するファイルのアップロード元のコンピューターが Bit9 Server によって選択されます。Bit9 Server は現在接続されているコンピューター上のファイルのインスタンスを最初に検索します。ファイルが

存在するコンピューターが複数接続されている場合、コンピューターがサーバーと最後にいつ通信したかと、他のアップロードがスケジュールされているか、または進行中かどうかに基づいて（これらを優先的に回避しつつ）、「最適」なコンピューターが選択されます。接続されているコンピューター上にファイルが存在しない場合、切断されているコンピューターからのアップロードがスケジュールされます。サーバーはそのコンピューターが再接続されるとアップロードを開始します。

ファイル テーブルからファイルのアップロードを開始する手順：

1. ［Files on Computers（コンピューター上のファイル）］など、ファイル テーブルのページに移動します。
2. サーバーにアップロードするファイルの横にあるボックスをオンにします。
3. ［Action（アクション）］メニューで［**Upload to Server**（サーバーにアップロード）］を選択します。



4. 確認のダイアログ ボックスで［**Yes**（はい）］をクリックします。

   アップロードがスケジュールされたことを示すメッセージがページに表示されます。

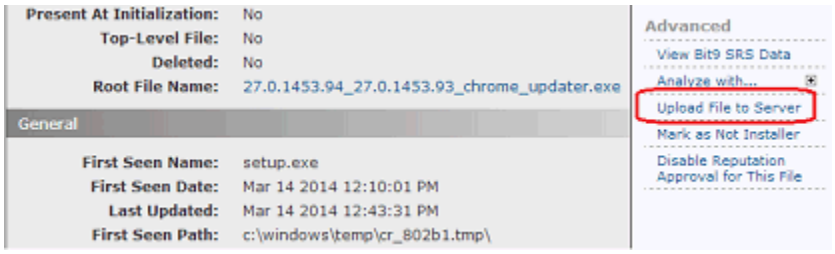
［File Instance Details（ファイル インスタンスの詳細）］ページでのアップロードの開始

［File Instance Details（ファイル インスタンスの詳細）］ページまたは［File Details（ファイルの詳細）］ページでは、1 つのファイルのアップロードをスケジュールできます。手順は共通です。

［File Instance Details（ファイル インスタンスの詳細）］ページでファイルのアップロードを開始する手順：

1. アップロードするファイルの［File Instance Details（ファイル インスタンスの詳細）］ページに移動します。

2. ファイル データの右側にある［Advanced（詳細）］メニューで［Upload File to Server（サーバーにファイルをアップロード）］を選択します。



アップロードがスケジュールされたことを示すメッセージがページに表示されます。

詳細ページでファイルをアップロードすると、［Advanced（詳細）］メニューの［Upload File to Server（サーバーにファイルをアップロード）］コマンドが［**Related File Uploads**（関連ファイルのアップロード）］に変わります。このリンクをクリックすると、［Requested Files（要求されたファイル）］ページの［Uploaded Files（アップロードされたファイル）］タブが開き、このファイルの SHA-256 ハッシュでファイルがフィルターされます。

［Computer Details（コンピューターの詳細）］ページでのパスによるアップロードの開始

［Computer Details（コンピューターの詳細）］ページでは、ファイルが追跡対象ファイルの Bit9 ファイル インベントリ内に存在するかどうかにかかわらず、コンピューター上のすべてのファイルのアップロードをスケジュールできます。その他のコンソール ページからのアップロードとは異なり、ファイルへのパスを入力する必要があります。選択できるファイルのリストは存在せず、アップロードはハッシュに基づいて実行されません。

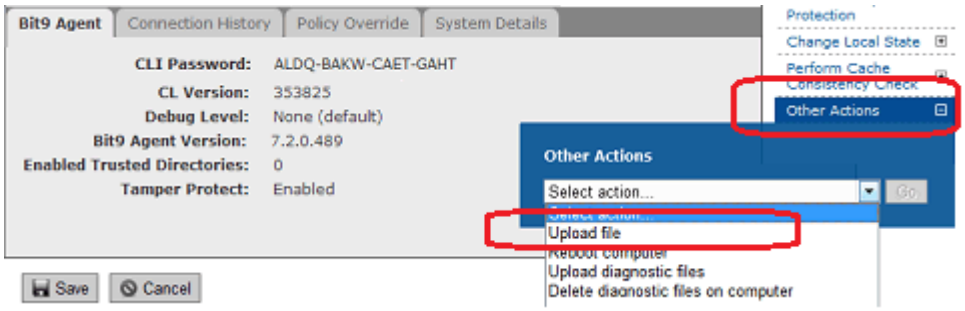
注意

［Computer Details（コンピューターの詳細）］ページからファイルをアップロードするには、「Manage uploads of files by pathname（パス名によるファイルのアップロードの管理）」アカウント権限が別途必要です。この権限を設定する手順については、「アカウント グループとアクセス権限」（88 ページ）を参照してください。

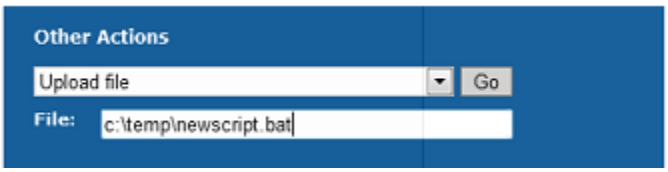
ファイルへのパスにはワイルドカードを使用できませんが、マクロとレジストリキーを使用してパスの場所を指定できます。Bit9 によって認識されるパス マクロのリストについては、「ルールでのマクロの使用」（423 ページ）を参照してください。

［Computer Details（コンピューターの詳細）］ページでファイルのアップロードを開始する手順：

1. アップロードするファイルがあるコンピューターの詳細ページに移動します。
2. ファイル データの右側にある［Advanced（詳細）］メニューで［**Other Actions**（その他のアクション）］を選択します。
3. ［Other Actions（その他のアクション）］メニューで［**Upload File**（ファイルをアップロード）］を選択します。



4. メニューに表示される［File（ファイル）］ボックスにファイルへの完全なパスを入力し、［**Go**（移動）］ボタンをクリックします。



アップロードがスケジュールされたことを示すメッセージがページに表示されます。存在しないファイルやパスを入力してもアップロードは試行されます。その場合、アップロードを開始したページにはエラーは表示されませんが、失敗した試行のレコードが［Requested Files（要求されたファイル）］の［Uploaded Files（アップロードされたファイル）］テーブルに表示されます。

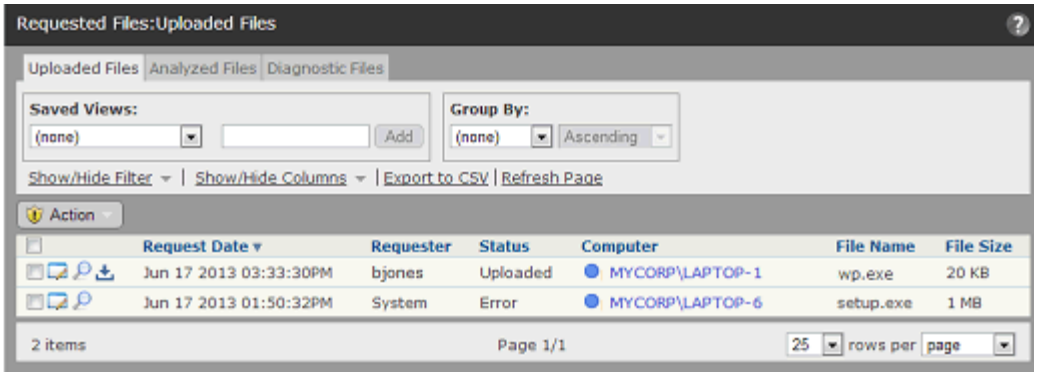
アップロード テーブルの表示

要求された各アップロードは、アップロードが失敗した場合も、［Uploaded Files（アップロードされたファイル）］ページに表示されます。このページでは、アップロードされたファイルに関する情報の表示、リストからのアップロードの削除、アップロードの再試行、進行中のアップロードのキャンセル、およびアップロードされたファイルの表示を実行できます。

［Uploaded Files（アップロードされたファイル）］ページを開く手順：

1. コンソール メニューで、［**Tools**（ツール）］>［**Requested Files**（要求されたファイル）］の順に選択します。

2. ［Requested Files: Uploaded Files（要求されたファイル：アップロードされたファイル)］ビューがまだ表示されていない場合は、［**Uploaded Files**（アップロードされたファイル)］タブをクリックします。



［Uploaded Files（アップロードされたファイル)］ページでは、デフォルトのビューに加えて、以下の保存済みビューが選択できます。

- Uploads in Progress（進行中のアップロード）
- Completed Uploads（完了したアップロード）
- Upload Errors（アップロードエラー）

表 129 に［Uploaded Files（アップロードされたファイル)］ページで使用できる列を示します。デフォルトで表示されるものと、追加する必要があるものとがあります。

表 129：[Uploaded Files（アップロードされたファイル）] テーブルの列

列	説明
Actions（アクション）	[Action（アクション）] 列には、アクション メニューのコマンドを適用するファイルを選択するためのチェックボックスと、個々のファイルにアクションを実行するためのボタンがあります。このページの [Action（アクション）] メニューには次のコマンドがあります。 • [**Cancel Uploads**（アップロードをキャンセル）] – オンにしたファイルのアップロードをキャンセルします（アップロードが完了していない場合）。 • [**Retry Uploads**（アップロードを再試行）] – オンにしたファイルのアップロードを再試行します。 • [**Delete Uploads**（アップロードを削除）] – オンにしたファイルのテーブル行を削除するとともに、ファイルが正常にアップロードされている場合は、サーバーからファイルを削除します。 • [**Change priority to:**（優先度を変更：）] – このアップロード要求の優先度を、メニュー内の選択肢のいずれかに変更します。選択肢は、[**Low**（低）]、[**Medium**（中）]、[**High**（高）]、[**Highest**（最高）] です。優先度を変更すると、保留中のファイルがアップロードされる順序に影響します。 • [**View Bit9 SRS Cloud Data**（Bit9 SRS クラウドデータを表示）] – このファイル（ハッシュで識別）に関して Bit9 SRS データベースから入手できるデータを表示します。 • [**Analyze with…**（… で分析）] – サードパーティの分析デバイスまたはサービスがBit9コネクタによって統合されている場合、選択したファイルを分析のために送信できます。[Uploaded Files（アップロードされたファイル）] ページに正常にアップロードされなかったファイルについては、[Analyze with…（… で分析）] コマンドを選択すると、新しくアップロードが開始されます。アップロードが正常に実行されると、サードパーティ デバイスにファイルが送信されます。 個別にアップロードされたファイルの行は、各行にあるボタンで操作できます。これには、すべてのファイル テーブルにある標準の [File Details（ファイルの詳細）] ボタンと [Find File（ファイルの検索）] ボタンがあります。正常にアップロードされたファイルには、次のボタンがさらに表示されます。  Bit9 Server から指定した場所にファイルをダウンロードします（正常にアップロードされている場合）。これを実行するには、コンソール ユーザーはアップロードされたファイルにアクセスする特定の権限を持っている必要があります。
Priority（優先度）	保留中のファイルをサーバーにアップロードする優先度。優先度の選択肢は、[**Low**（低）]、[**Medium**（中）]、[**High**（高）]、[**Highest**（最高）] です。[Action（アクション）] メニューで変更できます。
Request Date（要求日）	ファイルのアップロードが要求された日時。

列	説明
Requester（要求者）	アップロードを要求したコンソール ユーザー。イベント ルールによる要求であった場合は、[System（システム）]。
Status（ステータス）	ファイルのアップロード ステータス。次のいずれかの値になります。 • [**Uploaded**（アップロード済み）] – アップロードが正常に完了し、ファイルをサーバー上で使用できます。 • [**Uploading**（アップロード中）] – アップロードは進行中ですが、まだ完了していません。サーバーによるファイルの受信は一部完了しています。このステータスが表示されるのは、ファイルが非常に大きい場合だけです。 • [**Initiated**（開始済み）] – ファイルが保存されているエージェントがアップロード タスクを受信しました。 • [**Queued**（待機中）] – アップロード タスクがまだエージェントに送信されていません。 • [**Error**（エラー）] – アップロードは失敗しました。このステータスの上にカーソルを合わせると、エラー メッセージが表示されます。エラーには、「No file with hash（ハッシュのあるファイルが存在しない）」、「The system cannot find the path specified（システムが指定したパスを検出できない）」、「The system cannot find the file specified（システムが指定したファイルを検出できない）」などがあります。 • [**Canceled**（キャンセル済み）] – コンソール ユーザーによってアップロードがキャンセルされました。
Computer（コンピューター）	ファイルのアップロード元のコンピューターの名前。
File Name（ファイル名）	アップロードしたファイルの名前。ほとんどの要求で、Bit9 Server は要求されたファイルの「ハッシュ」に一致するファイルをアップロードします。そのため、ここに表示される名前が選択したファイルの名前と異なる場合があります。 [Computer Details（コンピューターの詳細）] ページからのアップロードでは、アップロード要求中、ファイル名は常に [File（ファイル）] ボックスに入力した名前になります。
File Size（ファイル サイズ）	ファイルのサイズ（バイト単位）。
Upload %（アップロードの割合）	アップロードの完了割合。アップロードが完了すると「100%」と表示されます。アップロードが失敗した場合や、アップロードがまだ開始されていない場合は、「0%」と表示されます。
Upload Date（アップロード日）	ファイルがサーバーにアップロードされた日時。

列	説明
Upload Directory（アップロード ディレクトリ）	ファイルのアップロード先の Bit9 Server のディレクトリ。手動アップロードの場合、値は［(default)（(デフォルト)）］です。この場合、［System Configuration（システム構成）］ページの［Advanced Options（高度なオプション）］タブで構成されているディレクトリが使用されます。イベント ルールによるアップロードの場合、実際のパスが表示されます。
Error（エラー）	ファイルのアップロードを妨げたエラーの説明。たとえば、ファイルが指定した場所に（またはどこにも）存在しなかった場合のエラーは、「**file not found**（ファイルが見つかりません）」です。デフォルトでは表示されません。
File Path（ファイル パス）	ファイルのアップロード元のエージェント コンピューターの場所。デフォルトでは表示されません。
Prevalence（普及度）	サーバーにレポートするBit9管理コンピューターのうち、このファイルが存在するコンピューターの数。
MD5	ファイルの MD5 ハッシュ。
SHA256	ファイルの SHA-256 ハッシュ。
Source（ソース）	アップロードの要求ソース。［Event rule（イベント ルール）］か［Manual（手動）］のどちらかです。
Source Name（ソース名）	イベント ルールによる要求であった場合は、ルール名。手動による要求であった場合は、このフィールドは空白です。

診断ファイル

［Requested Files（要求されたファイル）］ページには［Diagnostic Files（診断ファイル）］タブもあります。このタブには、Bit9 で管理されるエンドポイントから Bit9 Server にアップロードされた診断ファイルが表示されます。サーバーにアップロードできる診断ファイルには、サーバー診断ファイルとエージェント診断ファイルの 2 種類があります。サーバー診断ファイルは、テーブル内のファイルのチェックボックスの横にあるダウンロード ボタンをクリックすることで、コンソール ユーザー自身のコンピューターにダウンロードできます。エージェント診断ファイルはサーバー上に残り、ダウンロード オプションはありません。

［Diagnostic Files（診断ファイル）］タブの情報とアクションは、通常、Bit9 テクニカル サポートと連絡を取りながら使用します。

診断ファイルのアップロードとダウンロードの詳細については、付録 D、「診断ファイル」を参照してください。

アップロードされたファイルのダウンロード

ファイルが Bit9 サーバーにアップロードされると、適切な権限を持つコンソール ユーザーが、選択したファイルをさらに調査するためにローカル コンピューターにダウンロードできるようになります。

重要

この機能を使用する場合は特に細心の注意を払い、他のユーザーのコンピューターおよびファイルにアクセスする際に組織のポリシーに完全に準拠する必要があります。機能に絶対にアクセスする必要がある Bit9 コンソール ユーザーにのみ、機能を使用する権限が与えられていることを確認してください。ファイルをダウンロードする機能については、コンソール ユーザーの権限設定に独自の権限設定（「Access uploaded files（アップロードされたファイルへのアクセス）」）が用意されています。

アップロードされたファイルをダウンロードする手順：

1. ［Uploaded Files（アップロードされたファイル）］テーブルで、ダウンロードするファイルの行のダウンロード ボタン をクリックします。
2. ブラウザーのダイアログに従い、ファイルのダウンロードを選択します。

   コンソールを表示しているコンピューター上のダウンロード場所にzipファイルがコピーされます。zip ファイルには、アップロードされたファイルとエージェント コンピューターのフォルダー パスが含まれています。フォルダーをたどってファイルにアクセスできます。

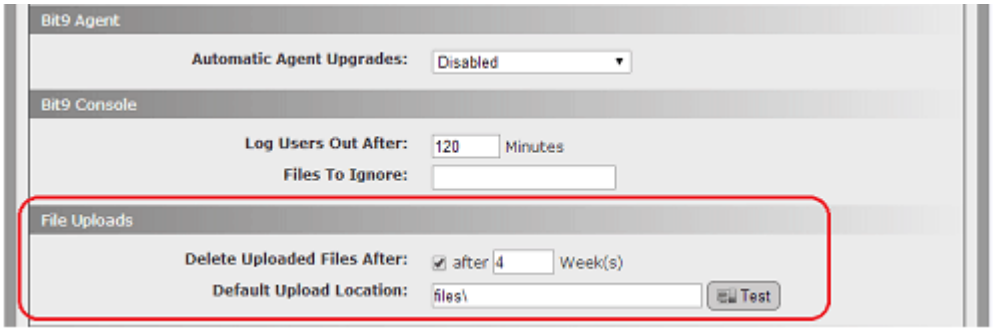
アップロード構成オプション

アップロードされたファイルの削除

［Uploaded Files（アップロードされたファイル）］ページで、削除する各ファイルの列のボックスをオンにし、［Action（アクション）］メニューから［**Delete Uploads**（アップロードを削除）］を選択すると、アップロードされた各ファイルをサーバーから削除できます。また、サーバーにアップロードされたファイルをスケジュールに従って削除するよう、Bit9 Server を構成することもできます。デフォルトでは、ファイルはサーバーにアップロードされてから 4 週間後に削除されます。

アップロードされたファイルの自動検出を構成する手順：

1. コンソール メニューで、［**Administration**（管理）］>［**System Configuration**（システム構成）］の順に選択し、［System Configuration（システム構成）］ページで［**Advanced Options**（高度なオプション）］タブをクリックします。
2. ページ下部の［**Edit**（編集）］ボタンをクリックします。



3. ［File Uploads（ファイルのアップロード）］パネルで［Delete Uploaded Files After（アップロードされたファイルを削除するまでの期間）］ボックスがオンになっていることを確認し、ファイルを削除するまでの週数を入力します。

   注意：アップロードされたファイルの自動検出を無効にすることは推奨されません。

4. ページ下部の［**Update**（更新）］ボタンをクリックします。

> **注意**
>
> ［Uploaded Files（アップロードされたファイル）］テーブルはバックアップされますが、実際にアップロードされたファイルは Bit9 Server のバックアップには含まれません。Bit9 データベースを復元した場合、［Uploaded Files（アップロードされたファイル）］テーブルにファイルがリストされていたなら、テーブルは復元されますが、ファイルは使用できません。

アップロードされたファイルの場所の変更

アップロードされた zip ファイルのデフォルトの場所は、Bit9 インストール ディレクトリの「Parity Server\Files」フォルダーです。アップロードされたファイルは番号付きの zip ファイルに格納されます。たとえば、最初にアップロードしたファイルは次の場所に保存されます。

```
C:\Program Files (x86)\Bit9\Parity Server\Files\1.zip
```

［System Administration（システム管理）］ページの［Advanced Options（高度なオプション）］ページで、［Default Upload Location（デフォルトのアップロード先）］の設定を編集して選択することで、この場所を変更できます（上の図を参照）。以下の方法で場所を指定できます。

- 完全なパスを使用せずにフォルダーを指定した場合、場所は Bit9 Server の「Bit9\Parity Server\」ディレクトリを基準にしていると見なされます。たとえば、上の図の［Advanced Options（高度なオプション）］ページのデフォルトの場所は、簡単に「files\」とだけ指定されています。
- ドライブ文字を含め、Bit9 Server 上の完全なパスを指定できます。
- 完全なUNCパスを使用して、Bit9 Server以外のシステム上の場所を指定できます。

どの方法でアップロード先を指定する場合も、その場所の書き込み権限を持っている必要があります。また、UNC パスを使用する場合は、指定したシステムのネットワーク アクセス権を持っている必要があります。

ファイルのアップロード先を変更する手順：

1. コンソール メニューで、[**Administration**（管理）] > [**System Configuration**（システム構成）] の順に選択し、[System Configuration（システム構成）] ページで [**Advanced Options**（高度なオプション）] タブをクリックします。
2. ページ下部の [**Edit**（編集）] ボタンをクリックします。
3. [File Uploads（ファイルのアップロード）] パネルでファイルのアップロード先となる場所のパスを入力し、[**Test**（テスト）] ボタンをクリックしてその場所が存在することを確認します。

   注意：存在しないディレクトリを指定した場合、[Test（テスト）] ボタンをクリックすると失敗メッセージが表示されます。ただし、指定した場所の上のディレクトリに書き込む権限を持っている場合、フォルダーが作成されてファイルがその場所にアップロードされます。
4. ページ下部の [**Update**（更新）] ボタンをクリックします。

注意

Bit9 Connector のライセンスが付与されている場合は、イベント ルールを使用して、ルールのファイル基準に一致するファイルを自動的にアップロードできます。また、ルールごとに別の場所を定義できます。「イベント ルール」（517 ページ）を参照してください。

付 録 F

外部分析のための Bit9 データのエクスポート

この章では、エンドポイントで収集されたデータを Bit9 Server から外部の分析ツールにエクスポートするために、Bit9 External Analytics を構成して使用する手順について説明します。この統合で Bit9 データを分析する機能を拡張し、外部ツールで他の Bit9 Server をはじめとする複数のソースのデータを分析できます。

注意

このリリースで Bit9 は Splunk との外部分析の統合を実装しました。ここに示す例は Splunk 固有のものです。ただし、他の外部分析ツールを設定する専門知識があれば、この付録のデータ エクスポートの構成に関する一般的な説明を参照することで、それらのツールと統合できます。

セクション

概要

Bit9 Security Platform では複数のさまざまなツールで分析および表示できる Syslog イベントを出力できます。リリース v7.2 以降の Bit9 では、外部分析統合機能により、Bit9 Platform で収集された幅広いデータを別の方法で利用できます。Splunk などの外部データ分析ツールにデータを送信するよう Bit9 Server を構成できます。Bit9 と外部の分析ツールとの統合には、次の利点があります。

- **複数のソースのデータの分析** – 他のデータ セキュリティ プラットフォームまたは複数の Bit9 Server から送信される情報と組み合わせて Bit9 の情報を表示できます。このリリースでは、Splunk にインポートされる Bit9 データを CIM 標準に正規化できます。
- **Bit9 ファイル データの分析への追加** – Syslog ベースの統合とは違い、外部分析の統合は「イベント」ログ出力に制限されません。Bit9 イベント データ、ファイル カタログ、ファイル操作データのいずれかまたはすべてを外部ツールにエクスポートするよう選択できます。送信するデータのタイプと量は Bit9 コンソールで構成できます。
- **新しいレポート機能の使用** – 外部ツールの機能を使用して、新しいタイプのレポートを Bit9 データから生成できます。
- **分析の負荷の移動** – データ分析を別のツールや場所に移動することで、Bit9 データベース サーバーに対する負荷を軽減できます。
- **外部レポート ツールへの Bit9 コンソールのリンク** – 分析の統合を有効にすると、特定の Bit9 コンソール ページから外部分析ツールのコンソールへのリンクを追加できます。

外部分析用にエクスポートされるデータは JSON 形式となります。

注意

Bit9 で使用できるファイル カタログ データについては、第 7 章「ファイル情報と公開者情報」を参照してください。Bit9 Platform で使用できるイベントについては、別冊の『Bit9 Events Integration Guide（Bit9 イベント統合ガイド）』を参照してください。

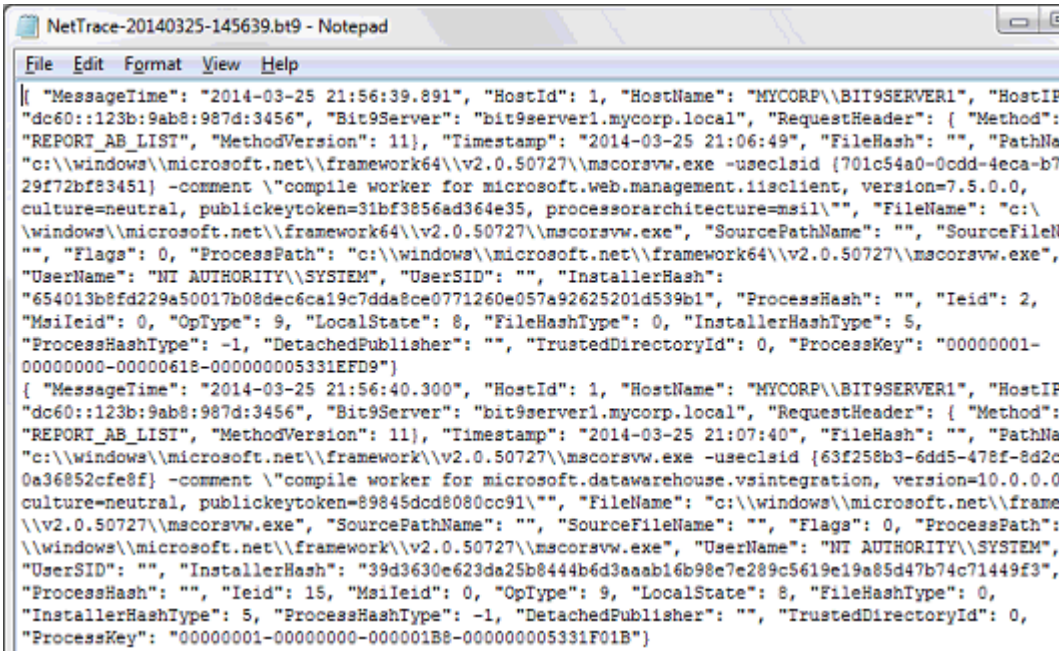
外部分析の使用準備

外部データ分析機能を使用するには、次の操作を実行します。

- 外部分析用のデータをフォルダーに送信するよう Bit9 Server を構成します。
- 外部分析に関連する権限を持っている 1 つ以上の Bit9 コンソール ユーザー アカウントを有効にします。これらの権限は、「View System Configuration（システム構成の表示）」、「Manage System Configuration（システム構成の管理）」、および（Bit9 コンソールから外部ツールへのリンクを表示し、アクセスするための）「View External Analytics Reports（外部分析レポートの表示）」です。ユーザー権限の詳細については、「アカウント グループの権限」（108 ページ）を参照してください。
- Bit9 コンソールから外部ツールに戻るリンクを設定する場合は、分析統合を使用する Bit9 コンソール ユーザーも外部ツールのログイン アカウントを持っていることを確認します。
- 出力を使用するように分析ツールを構成します。

データ形式と管理

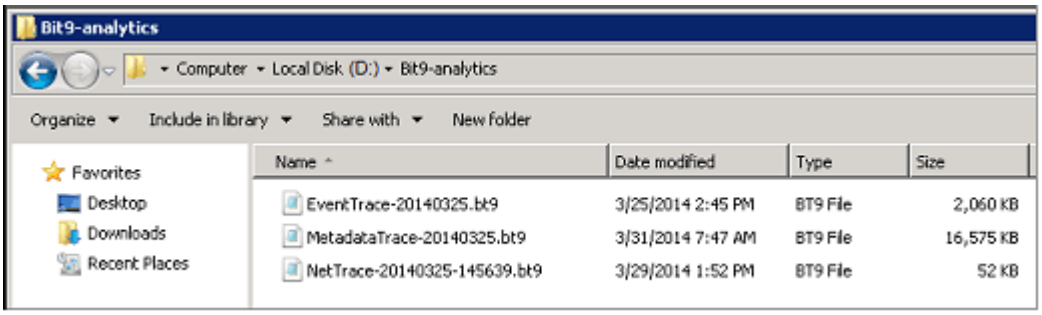
外部分析用のデータは JSON 形式でエクスポートされます。Bit9 Server からの JSON 出力にはフィールド名と各値が含まれているため、未加工の出力を表示することや、後でインデックスの依存関係を作成せずに解析することが簡単にできます。



Bit9 Security Platform 向け Splunk アプリを使用すると、Splunk サーバーによってインポートされた Bit9 データは CIM にマッピングされ、他のデータと統合できます。詳細については、「Bit9 向け Splunk アプリでの CIM へのフィールド マッピング」（950 ページ）を参照してください。

エクスポートに対して有効にしたメッセージに応じて、次の 1 つ以上のファイルが外部分析用に構成したエクスポート ディレクトリに作成されます。

- **イベント データ** – `EventTrace-<YYYYMMDD>.bt9`
- **ファイル カタログ データ** – `MetadataTrace-<YYYYMMDD>.bt9`
- **ファイル操作データ** – `NetTrace-<YYYYMMDD-HHMMSS>.bt9`



各メッセージ ログ ファイルの最大サイズは 512 MB で、最大サイズに達した時点で新しいログ ファイルが作成されます。Bit9 Server プロセスが再起動された場合も、ログが新しく開始されます。

新しいファイル操作データ ファイル (NetTrace) は、上記のように日付と時刻の両方を含む名前が付けられます。

イベント データ ファイルまたはファイル カタログ データ ファイルが同じ日に 2 つ作成される場合は、それぞれの 2 番目のファイルに数字が付加されます。たとえば、2013 年 10 月 29 日に作成された最初のファイル カタログ データのファイルの名前は「MetadataTrace-20131029.bt9」になります。そのファイルが同じ日にサイズの制限に達すると、2 番目のファイルは「MetadataTrace20131029-1.bt9」という名前になります。

注意

エクスポート可能なイベント タイプとサブタイプの詳細については、別冊の『Bit9 Events Integration Guide（Bit9 イベント統合ガイド）』を参照してください。

分析用にエクスポートされるデータの量

- ファイル カタログはコンピューター 1 台あたり 1 日 20 KB
- イベントはコンピューター 1 台あたり 1 日 75 KB
- ファイル操作はコンピューター 1 台あたり 1 日 135 KB（量：高）
- ファイル操作はコンピューター 1 台あたり 1 日 115 KB（量：中）
- ファイル操作はコンピューター 1 台あたり 1 日 100 KB（量：低）

エクスポート ディレクトリのサイズの制限

コンソールの［System Configuration（システム構成）］ページの［External Analytics（外部分析）］タブには、エクスポート ディレクトリのデータの量を制限できるチェックボックスがあります。このボックスをオンにするとフィールドが表示され、エクスポート ディレクトリのデータの最大サイズ（エクスポート ディレクトリ内のすべてのファイルの合計サイズ）を GB 単位で入力して設定できます。制限に達すると、ディレクトリ サイズが制限を下回るまで、古い順にファイルが削除されます。指定可能な最小サイズは 3 GB です。各ディレクトリの最新のファイルは削除されません。上限は 10 PB です。

注意

エクスポート ディレクトリのサイズ制限によって、Bit9 Server 上のディレクトリに保持されるデータの量を制御できますが、外部分析ツールにアップロードされるデータの量は制限されません。ライセンスやパフォーマンス上の理由で外部ツールにアップロードするデータを制限する必要がある場合は、「Bit9 コンソールでの外部分析の有効化」（931 ページ）の説明に従って［External Analytics Settings（外部分析設定）］のチェックボックスと［External Analytics（外部分析）］構成ページのラジオ ボタンを使用します。

ローカル ログ ファイルとネットワーク ログ ファイル

ログ ファイルがローカルにあり、ログの内容を Splunk Universal Forwarder などのデータ分析ツールへの中継機能によって中継する場合は、パフォーマンスに対する影響は最小限に抑えられます。ただし、ログ ファイルをネットワーク上の場所に書き込む場合は、ネットワークの待ち時間が長いとデータが利用できるまでに遅延が発生する可能性があります。

分析データをローカルに書き込む場合は、オペレーティング システムまたは Bit9 SQL データベースが配置されているディスク以外のディスクに書き込む必要があります。

Bit9 コンソールでの外部分析の有効化

次のように Bit9 コンソールで Bit9 分析機能の 3 つの要素を構成します。

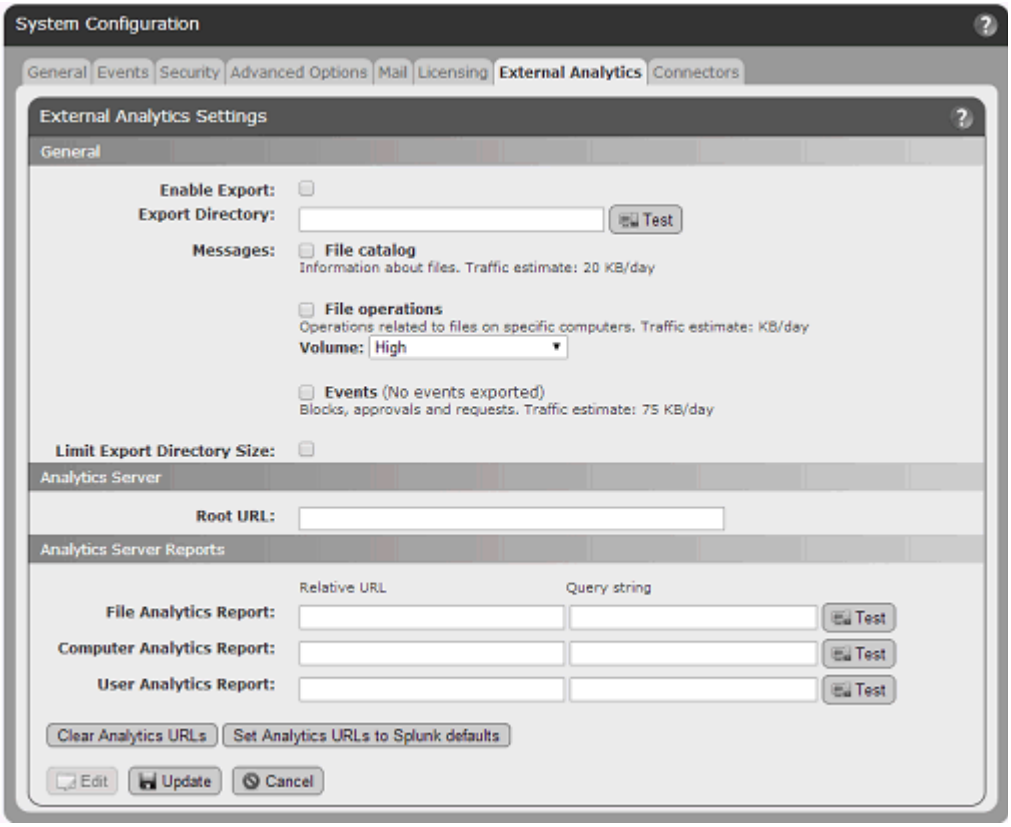
- ［System Configuration（システム構成）］ページの［External Analytics（外部分析）］タブで、Bit9 データをエクスポートするフォルダーの場所、内容、およびサイズ制限（必要な場合）を指定します。
- 同じタブで、Bit9 コンソール ユーザーが外部分析サーバー上の特定のレポートにリンクできるよう URL とクエリを指定できます。
- ［Add Custom Rule（カスタム ルールの追加）］ページで、データ エクスポート ディレクトリに書き込まれたファイルを無視するルールを作成して、データ エクスポートによる Bit9 Server への影響を抑えることができます。

次の手順では、上記の最初の 2 つのタスクを行う方法を説明します。［External Analytics（外部分析）］タブのパラメーターの詳細については、表 130、「外部分析構成オプション」（934 ページ）を参照してください。

Bit9 コンソールで外部分析機能を有効にする手順：

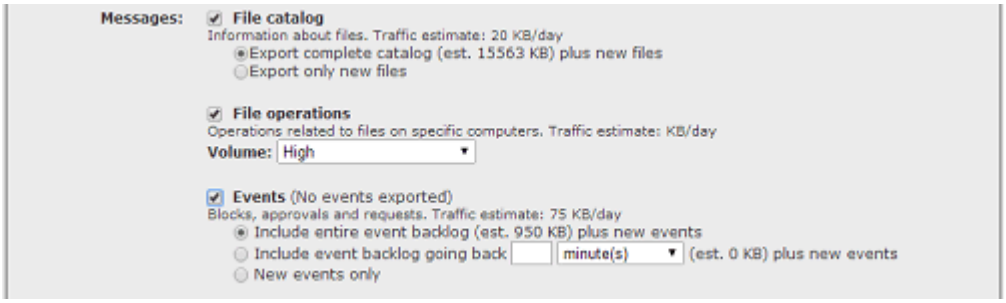
1. コンソール メニューで、［**Administration**（管理）］>［**System Configuration**（システム構成）］の順に選択し、［**External Analytics**（外部分析）］タブをクリックします。

2. ページ下部の［**Edit**（編集）］ボタンをクリックします。



3. ［General（全般）］パネルで、［**Enable Export**（エクスポートの有効化）］ボックスをオンにします。
4. ［Export Directory（エクスポート ディレクトリ）］フィールドで、Bit9 分析ファイルを書き込むディレクトリの名前を入力します。このフォルダーは Bit9 Serverサービス(ParityServer)を実行するユーザーが書き込みアクセス権を持っているフォルダーにする必要があります。
注意 : Bit9 Server をホストしているシステムに、エクスポートされたデータを書き込む場合は、オペレーティング システムまたは SQL Server が使用しているディスク ボリューム以外のディスク ボリュームを使用する必要があります。
5. ［Export Directory（エクスポート ディレクトリ）］フィールドの右側にある［**Test**（テスト）］ボタンをクリックして、ディレクトリが有効で、そのディレクトリにサーバー プロセスが書き込むことができるかどうかをテストします。

6. 次のように［Messages（メッセージ）］のフィールドで、エクスポートする情報のタイプを指定します。



   a. ［**File Catalog**（ファイル カタログ）］– このボックスをオンにした場合、エクスポート ディレクトリにファイル カタログ データがエクスポートされます。このボックスをオンにすると、次の 2 つのラジオ ボタンが表示されます。［**Export complete catalog**（完全なカタログのエクスポート）］では、ファイル カタログの現在の内容全体とカタログへの新しい追加内容がエクスポートされます。［**Export only new files**（新しいファイルのみのエクスポート）］では、このオプションを有効にした後に、Bit9 Server にレポートするエージェントが検出した一意の新しいファイルのみがエクスポートされます。

   b. ［**File Operations**（ファイル操作）］– このボックスをオンにした場合、ファイルに影響する操作に関する、エージェントからのメッセージがエクスポートされます。ドロップダウン メニューではエクスポートするデータの量と、さらにはデータのタイプを決定できます。詳細については、表 130 を参照してください。

   c. ［**Events**（イベント）］– これをオンにした場合、Bit9 イベントがエクスポートされます。エクスポートするイベント データの量を制御し、使用可能な場合にエクスポートの推定サイズを表示するラジオ ボタンのオプションの詳細については、表 130 を参照してください。

> **注意**
>
> これらのメッセージ エクスポート オプションを設定する場合は、各オプションに表示されるトラフィックの推定値と外部分析デバイスに対するトラフィックの制限を考慮します。ただし、有用な分析を実行できるだけの十分な量のデータを必ずエクスポートする必要もあります。

7. ［Analytics Server Reports（分析サーバー レポート）］セクションでは、Bit9 コンソールから外部分析サーバー上のレポートへのリンクを構成できます。これらのリンクを有効にするには、最初に［Root URL（ルート URL）］フィールドに Bit9 Platform と統合する分析ツールのルート URL を入力します。

8. ［Analytics Server Reports（分析サーバー レポート）］パネルで、表示されたレポートの各タイプに対して相対 URL とクエリ文字列を入力し、テストします。分析ツールに渡す情報（ファイル ハッシュ、マシン名、ユーザー名）を表すために、クエリ文字列内ではマーカー **<val>** を使用します。
9. ［**Update**（更新）］をクリックします。

表 130：外部分析構成オプション

フィールド / ボタン	説明
Enable Export（エクスポートの有効化）	このチェックボックスでは、外部分析ツールへのデータ エクスポートやリンクなどの Bit9 の外部分析統合機能の有効化および無効化を行います。
Export Directory（エクスポート ディレクトリ）	このフィールドでは、Bit9 Server が外部分析用のデータをエクスポートするディレクトリを指定します。［Test（テスト）］ボタンを使用すると、ディレクトリが有効であることと、サーバー プロセスがそのディレクトリに書き込み可能であることを確認できます。テスト結果はボタンの横に表示されます（テストに成功すると [OK] が、失敗するとその理由を示すメッセージが表示されます）。
Messages:（メッセージ：） **File Catalog（ファイル カタログ）**	このチェックボックスでは、エクスポート ディレクトリへのファイル カタログ データのエクスポートを有効にします。このボックスをオンにすると、エクスポートするファイル カタログ データの量を制御する次の 2 つのラジオ ボタンが表示されます。 • ［**Export complete catalog**（完全なカタログのエクスポート）］– このオプションでは、ファイル カタログの現在の内容全体がエクスポートされ、カタログへの新しい追加内容が継続してエクスポートされます。 • ［**Export only new files**（新しいファイルのみのエクスポート）］– このオプションでは、Bit9 Server にレポートするエージェントが検出した一意の新しいファイルのみがエクスポートされます。
Messages:（メッセージ：） **File Operations（ファイル操作）**	このチェックボックスでは、ファイルに影響する操作に関する、エージェントからのメッセージのエクスポートを有効にします。ドロップダウン メニューではエクスポートするデータの量と、さらにはデータのタイプを決定できます。 • ［**Low**（低）］– 作成、変更、削除、名前の変更、ディレクトリ名の変更の各操作に関するメッセージがエクスポートされます。 • ［**Medium**（中）］–［Low（低）］の場合のすべてのメッセージと、ファイル状態の変更に関するメッセージ（Approved（承認）、Unapproved（未承認）、Banned（禁止））がエクスポートされます。これには、個々のファイルの状態の変更と、ファイルのグループの状態が変更される操作も含まれます。 • ［**High**（高）］– すべてのファイル操作メッセージがエクスポートされます。

フィールド / ボタン	説明
Messages:（メッセージ：）Events（イベント）	このチェックボックスでは、Bit9 イベント データのエクスポートを有効にします。このボックスをオンにすると、エクスポートするイベント データの量を制御するラジオ ボタンが表示され、使用可能な場合にエクスポートの推定サイズが表示されます。 • [**Include entire event backlog (est.** *value* **KB) plus new events**（イベント バックログ全体（推定「値」KB）と新しいイベントを含む）] – 既存のイベント データベース全体をエクスポートし、継続して新しいイベントをエクスポートできます。 • [**Include event backlog going back** *[time value]* **(est.** *value* **KB) plus new events**（過去［期間の値］のイベント バックログ（推定「値」KB）と新しいイベントを含む)] – エクスポートする過去のイベントの期間（現在を起点とする）を選択し、このオプションが有効になった時点から継続して新しいイベントをエクスポートできます。 • [**New events only**（新しいイベントのみ)] – この設定が有効になった時点からのみ継続して新しいイベントをエクスポートできます。
Limit Export Directory Size（エクスポート ディレクトリのサイズの制限）	このボックスをオンにするとフィールドが表示され、エクスポート ディレクトリのデータの最大サイズ（エクスポート ディレクトリ内のすべてのファイルの合計サイズ）を GB 単位で入力して設定できます。制限に達すると、ディレクトリ サイズが制限を下回るまで、古い順にファイルが削除されます。指定可能な最小サイズは 3 GB です。各ディレクトリの最新のファイルは削除されません。
Root URL（ルート URL）	ここに入力したルート URL（オプションでポートも含む）は Bit9 Server と統合する分析サーバーを参照します。これは、Bit9 コンソール ページから分析サーバー上のレポートに戻るリンクのベース URL として使用されます。 **注意**：Bit9 コンソール ユーザーには外部サーバーにログインするための認証情報が必要です。指定した URL では、ユーザーが Bit9 コンソールを使用して外部サーバーにアクセスする場合でも、これらの認証情報でログインできるようにする必要があります。
File Details Report（ファイル詳細レポート）	分析サーバー上の File Investigation（ファイルの調査）レポートへのリンクを定義します。行を定義する次の 2 つのフィールドがあります。[Relative URL（相対 URL)] は定義したルート URL に付加され、[Query String（クエリ文字列)] はその URL から取得するレポートを定義します。 定義すると、この [**File Analytics**（ファイル分析)] リンクは [File Details（ファイルの詳細)] ページと［File Instance Details（ファイル インスタンスの詳細)] ページの［External Pages（外部ページ)] メニューに表示されます。 この行の右側にある [**Test**（テスト)] ボタンをクリックして、URL とクエリ定義が有効であることを確認します。

フィールド / ボタン	説明
Computer Details（コンピューター詳細レポート）	分析サーバー上の Computer Investigations（コンピューターの調査）レポートへのリンクを定義します。行を定義する次の 2 つのフィールドがあります。[Relative URL（相対 URL）] は定義したルート URL に付加され、[Query String（クエリ文字列）] はその URL から取得するレポートを定義します。 定義すると、この［**Computer Analytics**（コンピューター分析）］リンクは［Computer Details（コンピューターの詳細）］ページの［External Pages（外部ページ）］メニューに表示されます。 この行の右側にある［**Test**（テスト）］ボタンをクリックして、URL とクエリ定義が有効であることを確認します。
User Details Report（ユーザー詳細レポート）	分析サーバー上の Console User Search（コンソール ユーザー検索）（この場合は Bit9 コンソール ログイン アカウント）レポートへのリンクを定義します。行を定義する次の 2 つのフィールドがあります。[Relative URL（相対 URL）] は定義したルート URL に付加され、[Query String（クエリ文字列）] はその URL から取得するレポートを定義します。 定義すると、この［**User Analytics**（ユーザー分析）］リンクは［Edit Login Account（ログイン アカウントを編集）］ページの［External Pages（外部ページ）］メニューに表示されます。 この行の右側にある［**Test**（テスト）］ボタンをクリックして、URL とクエリ定義が有効であることを確認します。
Set Analytics URLs to Splunk defaults（分析 URL に Splunk のデフォルト値を設定）	このボタンをクリックすると、Splunk のデフォルトの相対 URL およびクエリ文字列定義が 3 つのレポート フィールドに挿入されます。さらに、［Root URL（ルート URL）］フィールドに「http://server:8000」が挿入されます（ポート 8000 は Splunk のデフォルト）。 「server」を有効な Splunk サーバーの URL に置き換えると、これらのデフォルト値により、Bit9 コンソールから有効な Splunk レポートにアクセスできます。
Clear Analytics URLs（分析 URL のクリア）	このボタンをクリックすると、[Analytics Server（分析サーバー）] および [Analytics Server Reports（分析サーバー レポート）] フィールドからすべての値がクリアされます。

外部分析統合の編集または無効化

Bit9 Server との外部分析統合を編集または無効にする必要がある場合は、Bit9 コンソールで［System Configuration（システム構成）］ページの［External Analytics（外部分析）］タブを使用できます。エクスポート ディレクトリや統合用にインストールした Splunk Universal Forwarder などの追加のコンポーネントは、Bit9 コンソールから統合を無効にしても、削除されたり、アンインストールされたりすることはありません。

分析ログ ファイルを無視するカスタム ルールの追加

外部分析が有効な場合、エクスポート ディレクトリにファイル書き込み操作が繰り返し継続的に行われます。エージェントがサーバーでアクティブな場合、これにより、通常 Bit9 Server で大きなイベント トラフィックが生成されます。このイベント トラフィックは追跡するほど重要ではないため、カスタム ルールを作成してエクスポート ディレクトリのファイルの追跡を除外することを検討します。これらのルールを構成する方法の詳細については、第 12 章「カスタム ソフトウェア ルール」を参照してください。

エクスポートされた分析ファイルの追跡を除外する方法：

1. コンソール メニューで［**Rules**（ルール）］>［**Software Rules**（ソフトウェア ルール）］の順に選択し、［**Custom**（カスタム）］タブをクリックします。
2. ［**Add Custom Rule**（カスタム ルールの追加）］ボタンをクリックします。
3. ［Add Custom Rule（カスタム ルールの追加）］ページで、必要な情報を入力し、分析データ用のエクスポート ディレクトリへの書き込みを無視するルールを作成します。
   a. ［**Name**（名前）］–「Ignore Data Analytics Log Files（データ分析ログ ファイルを無視）」などルールを識別しやすい名前を選択します。
   b. ［**Description**（説明）］–（オプション）ルールの目的を詳細に示す説明を追加します。
   c. ［**Status**（ステータス）］–［**Enabled**（有効）］ラジオ ボタンをクリックします。
   d. ［**Platform**（プラットフォーム）］– ルールが適用されるプラットフォームを選択します。Bit9 Server システム上のエクスポート ディレクトリでは、これは **Windows**（デフォルト）です。
   e. ［**Rule Type**（ルール タイプ）］–［**Performance Optimization**（パフォーマンスの最適化）］を選択します。
   f. ［**Path or File**（パスまたはファイル）］– `D:\Bit9Analytics` のように、分析ファイルが書き込まれるフォルダーのパスと名前を指定します。
   g. ［**Process**（プロセス）］–［**Specific Process**（特定のプロセス）］を選択し、Bit9がこれらのファイルを書き込むために使用するプロセスを入力して**追加**します。たとえば、64 ビット OS を実行していて、デフォルトの Bit9 インストール ディレクトリを使用する場合は、次を使用します。
      ```
      <ProgramFiles>\Bit9\Parity Server\ParityServer.exe
      <ProgramFiles>\Bit9\Parity Server\Reporter\ParityReporter.exe
      ```
   h. ［**Rule Applies To**（ルールの適用先）］–［**All policies**（すべてのポリシー）］、または必要に応じて書き込み先のシステム（通常は Bit9 Server）が属するポリシーのみを選択します。
4. このルールの構成が終了したら、［**Save**（保存）］ボタンをクリックします。新しいルールが［Custom Rules（カスタム ルール）］テーブルに追加されます。

Bit9 データ分析用の外部ツールの有効化

データをエクスポートし、(オプションで) レポート用に分析サーバーに接続するように Bit9 Server を構成する以外にも、エクスポートした Bit9 データに分析サーバーがアクセスするよう接続を構成する必要があります。外部ツールを Bit9 データにアクセス可能にする厳密な手順はさまざまですが、手順には Bit9 Server システムに対して実行するアクションと分析サーバーに対して実行するアクションを含めることができます。次のセクションでは、Splunk による Bit9 データへのアクセスを有効にする手順を説明します。

Splunk による Bit9 データの収集の有効化

分析用に Splunk サーバーによる Bit9 データのインポートを有効にするには、Bit9 Server をホストするシステムと Splunk サーバーの両方に変更を加える必要があります。これらの手順を要約すると、次のようになります。

- Splunk サーバーを実行し、Bit9 Server とネットワーク経由でアクセス可能にする。
- Splunk Forwarder からのメッセージを受信するよう Splunk サーバーを設定する。
- Bit9 Security Platform向けSplunkアプリをSplunkサーバーにインストールする。
- Splunkweb を実行するマシン上にない Splunk Indexer を実行するマシンに Bit9 Security Platform 向け Splunk アプリをインストールする。
- Bit9 Server に Splunk Forwarder をインストールする。
- Bit9 Security Platform 向け Splunk アプリを Splunk Forwarder にインストールする。

Bit9 にアクセスするための Splunk サーバーの構成

Bit9 データを分析に使用できるようにするには、Splunk サーバーに対していくつかの手順を完了する必要があります。最初に、Splunk サーバーがフォワーダーのデータをポート 9997 で受信するよう構成します。

Splunk Universal Forwarder のメッセージを受信するよう Splunk サーバーを設定する手順：

1. 管理者レベルのユーザーとして Splunk サーバーにログインします。
2. Splunk コンソールの最上部のメニュー バーで、[**Settings** (設定)] (Splunk 6) または [**Management** (管理)] (Splunk 5) > [**Data** (データ)] > [**Forwarding and receiving** (フォワーディングと受信)] の順に選択し、[Forwarding and receiving (フォワーディングと受信)] ウィンドウで [**Configure receiving** (受信の構成)] を選択します。
3. [Receive data (データの受信)] ウィンドウで、ポート 9997 が構成されているかどうかを確認します。構成されていない場合は、[**New** (新規)] ボタンをクリックし、リッスンするポートとして「**9997**」と入力し、[**Save** (保存)] ボタンをクリックします。

4. ファイアウォールで、Splunkがポート9997でデータを確実に受信できるようにルールを作成します。

Bit9 Security Platform 向け Splunk アプリを使用すると、Splunk は Bit9 によって提供されたデータを解釈して、分析および表示できるようになります。

Bit9 Security Platform 向け Splunk アプリを Splunk サーバーにインストールする手順：

1. 管理者レベルのユーザーとして Splunk サーバーにログインします。
2. Splunk コンソールで **Find Apps Online**（アプリのオンライン検索）機能を使用して「Bit9」を検索し、Bit9 Security Platform 向け Splunk アプリが見つかったら、サーバー上の使いやすい場所にそのアプリをダウンロードします。
3. Splunk コンソールの最上部のメニュー バーで［**Apps**（アプリ）］>［**Manage Apps**（アプリの管理）］の順に選択します。
4. 次のように zip ファイルからアプリをインストールします。
   - ［**Install app from file**（ファイルからのアプリのインストール）］をクリックし、［Upload an app（アプリのアップロード）］ダイアログで `bit9-security-platform_20.tgz` ファイルを参照します。次に［**Upload**（アップロード）］をクリックします。ファイル名の末尾の番号はバージョンの変更に合わせて変わることがあります。

注意

Splunkweb を実行しているマシン上にない Splunk Indexer がある場合、これらのインデクサーをホストしているマシンに Bit9 Security Platform 向け Splunk アプリもインストールする必要があります。そのための手順は、Splunk Forwarder にこのアプリをインストールする手順と同じです。「Bit9 Security Platform 向け Splunk アプリを Bit9 Server にインストールする手順：」（940 ページ）を参照してください。

Bit9 Server への Splunk Forwarder とアプリのインストール

Bit9 コンソールで外部分析を構成する以外にも、Splunk との接続を有効にするために、Bit9 Server をホストするシステムに対してコンソール以外から実行する 2 つの追加手順があります。

- Splunk Universal Forwarder をインストールする。
- Bit9 Security Platform向けSplunkアプリをForwarderのサブディレクトリにインストールする。

Splunk Universal Forwarder はシステムにインストールできるパッケージで、Splunk がシステムからデータを収集できるようにします。たとえば、ログ ファイルから収集できます。この場合は、Forwarder と Bit9 向け Splunk アプリがインストールされていると、Forwarder はデータを Bit9 のエクスポート フォルダーから収集し、Splunk インフラストラクチャの適切な場所に転送します。

重要

Splunk Universal Forwarder のインストール処理では、Bit9 Server 上のデータ ファイルの場所の入力を求められても、入力しないでください。これらのファイルの場所は、Bit9 Security Platform 向け Splunk アプリによって指定されます。

Bit9 Server に Splunk Forwarder をインストールする手順：

1. 次の Splunk の Web サイトからフォワーダーをダウンロードします。
   http://www.splunk.com/download/universalforwarder
2. Bit9 Server で使用しているオペレーティング システムに対応するインストーラーを実行します。
3. Splunk サーバーのアドレスを求められたら、入力します。
4. Splunk Forwarder がインストールされたら、次の手順に従って Bit9 Security Platform 向け Splunk アプリを Splunk Forwarder のインストール ディレクトリの下にインストールします。

Bit9 Security Platform 向け Splunk アプリを Bit9 Server にインストールする手順:

1. 次の Splunk アプリの Web サイトで Bit9 Security Platform 向け Splunk アプリを検索し、ダウンロードします。
   http://apps.splunk.com
2. `bit9-security-platform_20.tgz` などのダウンロードしたファイルを Splunk Forwarder インストール ディレクトリの下の `\etc\apps` サブディレクトリにコピーします。たとえば、Bit9 Server 上で 64 ビット OS を実行している場合は、次の場所にコピーします。
   `C:\Program Files\SplunkUniversalForwarder\etc\apps\`

   注意 : ファイル名の末尾に番号が付いています。この番号はアプリのバージョンの変更に合わせて変わることがあります。
3. ファイルを解凍します。
4. `TA-bit9` ディレクトリに移動し、`local` という名前の新しいディレクトリを作成します。
5. `default\inputs.conf` を `local` ディレクトリにコピーします。
6. Bit9 コンソールの［System Configuration（システム構成）］の［External Analytics（外部分析）］ページで構成したエクスポート ディレクトリの場所を参照するよう `local\inputs.conf` の最初の行を編集して、このファイルを保存します。たとえば、Bit9 Server 上のエクスポート ディレクトリが `D:\Bit9\LogFiles` である場合、次のように `inputs.conf` の最初の行を変更する必要があります。

   ```
   [monitor://D:\Bit9\LogFiles\*.bt9]
   ```

7. コマンド プロンプトで、次のように Splunk Forwarder を再起動します。

```
cd \Program Files\SplunkUniversalForwarder\bin
.\splunk.exe restart
```

「Bit9 コンソールでの外部分析の有効化」および「Bit9 データ分析用の外部ツールの有効化」で説明しているタスクをすべて完了すると、Bit9 と Splunk の統合が完了し、Bit9 のデータが Splunk に流れ始めます。

外部分析ツールでの Bit9 データの表示

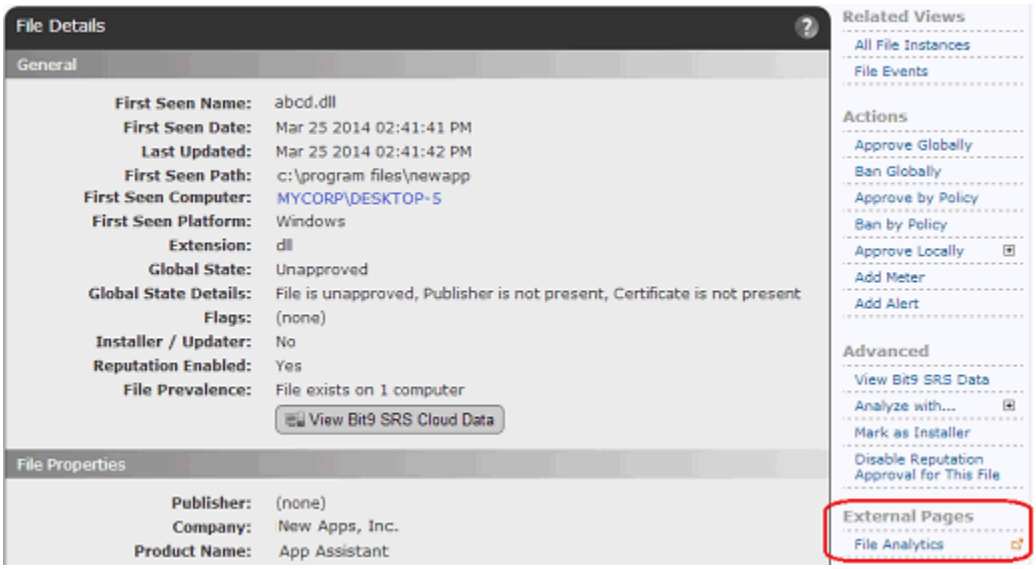
外部分析ツールによる Bit9 データの使用方法は、ツールのレポート機能、および他のデータ セキュリティ プラットフォームから送信される情報と Bit9 情報を統合する機能によって異なります。この統合のユーザーには、使用中の分析ツールにおけるさまざまなソースからのデータの統合方法、および統合した情報を利用するレポートの作成方法について知識が必要です。作成する具体的なレポートは、各ユーザーが決定します。

外部分析ツールでレポートを使用する方法の 1 つとして、Bit9 コンソールからレポートへのリンクがあります。

Bit9 コンソールから外部ツールへのリンク

Bit9 コンソールの［System Configuration（システム構成）］ページの［External Analytics（外部分析）］タブには、外部ツールのレポートへのリンクを定義できるフィールドがあります。このページでルート URL と各カテゴリの分析レポートが構成されている場合は、次のリンクが該当する各ページの右側のメニューに表示されます。

- ［**Computer Analytics**（コンピューターの分析）］–［Computer Details（コンピューターの詳細）］ページに表示されます。
- ［**File Analytics**（ファイル分析）］–［File Details（ファイルの詳細）］と［File Instance Details（ファイル インスタンスの詳細）］ページに表示されます。
- ［**User Analytics**（ユーザー分析）］–［Edit Login Account（ログイン アカウントを編集）］ページに表示されます。



Bit9 コンソール ユーザーがこれらのリンクの 1 つをクリックすると表示されるページの内容は、構成ページで指定した URL とクエリ定義でのみ決定されます。Bit9コンソール ユーザーには外部サーバーにログインするための認証情報が必要です。指定した URL では、ユーザーが Bit9 コンソールを使用して外部サーバーにアクセスする場合でも、これらの認証情報でログインできるようにする必要があります。

これらのリンクを有効にする方法の詳細については、「Bit9 コンソールでの外部分析の有効化」（931 ページ）を参照してください。これらのレポートに表示される内容の例については、「Bit9 Security Platform 向け Splunk アプリの使用」を参照してください。

Bit9 Security Platform 向け Splunk アプリの使用

Bit9 Security Platform 向け Splunk アプリは、Splunk で Bit9 データをより効果的に表示するのに役立ちます。このアプリをインストールして構成すると、Bit9 データの表示に専用で使用できるダッシュボードのセットが追加されます。また、たとえば、Bit9 をデータのソースとして認識すること、キー/ 値のペアの各キーワードの目的を認識すること、Bit9 固有の値を解読することや、Bit9 フィールドを CIM（共通情報モデル）にマッピングして Bit9 データを他のソースからのデータと組み合わせることによって、Splunk の機能を拡張して、その他のビューで Bit9 データを扱うこともできます。

Bit9 向け Splunk アプリのダッシュボード

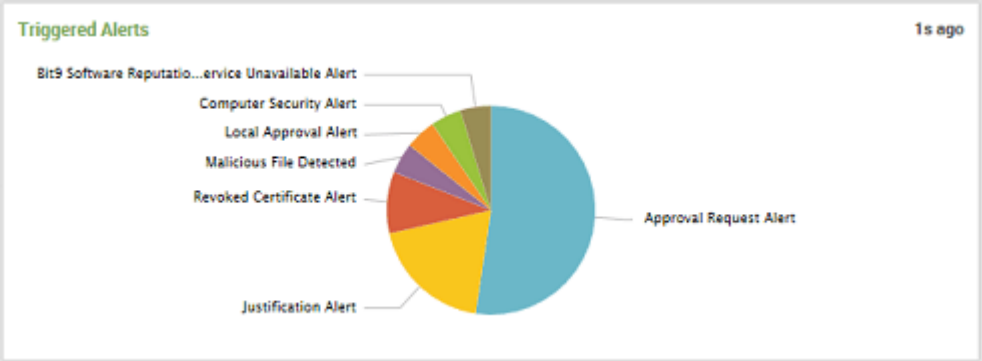
Bit9 Security Platform 向け Splunk アプリには次のダッシュボードがあります。

- ［**Deployment Activity**（展開アクティビティ）］– Bit9 Platform インストールで使用できる情報の概要。
- ［**Activity Details: File Activity**（アクティビティの詳細：ファイル アクティビティ）］– Bit9 が管理するコンピューターでのファイル作成および変更アクティビティに関する情報。

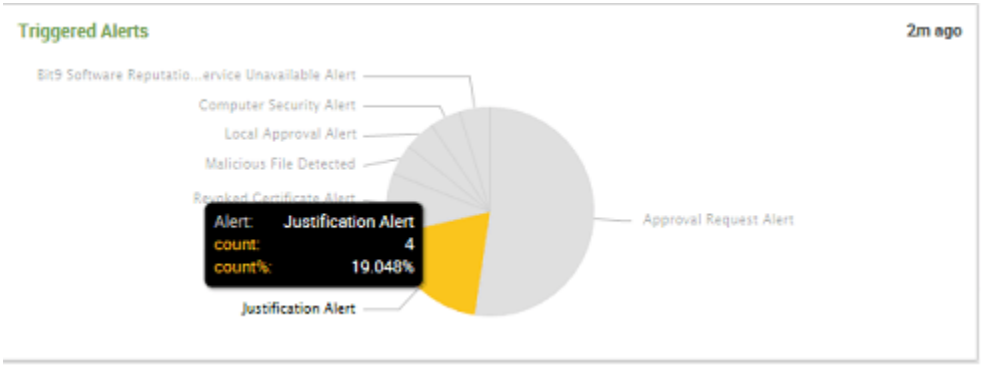
- ［**Activity Details: Blocks**（アクティビティの詳細：ブロック）］– Bit9 が管理するコンピューターでブロックされたファイルに関する情報。
- ［**Activity Details: Approvals**（アクティビティの詳細：承認）］– Bit9 が管理するコンピューターで承認されたファイルに関する情報。
- ［**Activity Details: New Unapproved Files**（アクティビティの詳細：新しい未承認ファイル）］– Bit9 が管理するコンピューターで検出され、承認も禁止もされていない新しいファイルに関する情報。
- ［**Activity Details: Events**（アクティビティの詳細：イベント）］– Bit9 Server で記録されたイベントに関する情報。
- ［**File Investigation**（ファイルの調査）］– 特定のファイルに対象を絞ったマルウェア調査に適した情報。Bit9 コンソールからリンクしている場合、ファイルに関する情報をリンク先のその詳細ページから取得します。
- ［**Computer Investigation**（コンピューターの調査）］– 特定のコンピューターに対象を絞ったマルウェア調査に適した情報。Bit9 コンソールからリンクしている場合、コンピューターに関する情報をリンク先のその詳細ページから取得します。
- ［**Console Users**（コンソール ユーザー）］– 特定の Bit9 コンソール ユーザーによって実行された異常なアクションやリスクの高いアクションを検出するのに適した情報。Bit9 コンソールからリンクしている場合、そのユーザーに関する情報をリンク先のその詳細ページから取得します。
- ［**All Console Users**（すべてのコンソール ユーザー）］– すべての Bit9 コンソール ユーザーに関する情報。

これらのダッシュボードのそれぞれに、Bit9 Server から Splunk にインポートされる情報を表示するパネルがあります。一部のパネルでは、最上部に要約パネルも表示されます。Bit9 コンソールでダッシュボードを使用したことがあれば、似たようなパネルを備えているものもあることがわかります。ただし、ここで利用するのは Splunk の分析機能と複数ソースの統合機能です。表 131 では、Bit9 向け Splunk アプリのダッシュボードで使用できるパネルを示し、それらのパネルが表示されるダッシュボードを紹介します。

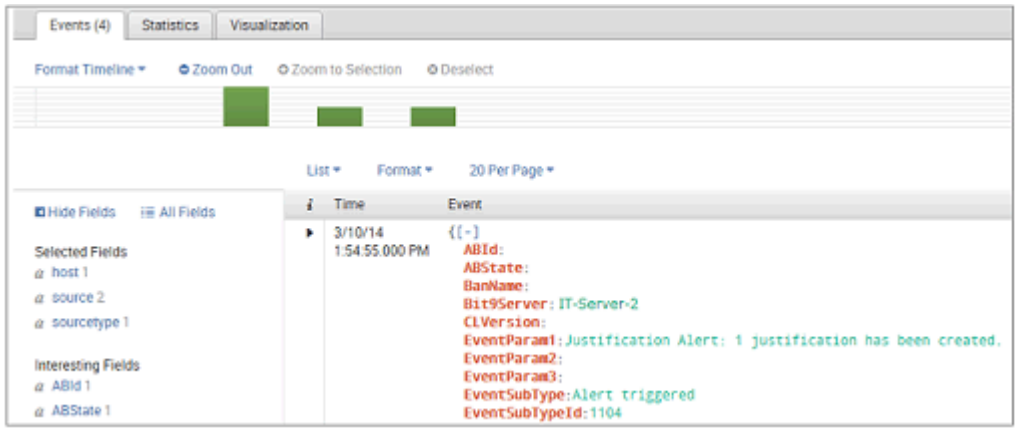
これらのダッシュボードのパネルには、データのテーブル、または次に示す Triggered Bit9 Alerts（トリガーされた Bit9 アラート）のようなデータを視覚的に表現したグラフが表示されます。パネルによっては両方が表示されます。



円グラフのスライスや棒グラフの棒など、グラフのセクションにマウス カーソルを合わせると、そのセクションが表すデータを説明する凡例が表示されます。



これらのセクションのいずれかをクリックすると、基となるデータが表示されます。



これらのパネルでは、データの表示対象期間を変更する機能など、その他の標準的な Splunk 機能が使用できます。

表 131：Bit9 向け Splunk アプリのダッシュボード内のパネル

ダッシュボード	パネル	説明
Deployment Activity（展開アクティビティ）	Host Activity（ホストアクティビティ）	ファイルおよびイベント アクティビティ（エージェント コンピューター別）。
	Triggered Alerts（トリガーされたアラート）	トリガーされたアラートの数（タイプ別）。
	File Blocks（ファイル ブロック）	ブロックされたファイル（日付、コンピューター、および製品名別）。
	New Unapproved Files（新しい未承認ファイル）	エージェント コンピューターに出現した新しい未承認ファイルをレポートするイベント（日付別）。
	New Files in Catalog（カタログ内の新しいファイル）	カタログに追加された一意の新しいファイル（日付別）。
	Approvals（承認）	ファイルの承認（日付、コンピューター、および製品名別）。
	File Activity（ファイル アクティビティ）	Bit9 が管理するシステムでのファイルの作成および変更（日付、コンピューター、製品名、またはファイル名別）。
	Top Event Subtypes（上位のイベント サブタイプ）	イベント サブタイプのリスト（頻度別）。
Activity Details: File Activity（アクティビティの詳細：ファイル アクティビティ）	File Creations（ファイル作成）	ファイル作成（日付、コンピューター、製品名またはファイル名、およびプロセス別）。
	ファイル変更	ファイル変更（日付、コンピューター、製品名またはファイル名、およびプロセス別）。
Activity Details: Blocks（アクティビティの詳細：ブロック）	Blocks（ブロック）	ファイルのブロック（日付、コンピューター、およびファイル名別）。
	Block Distributions（ブロックの分布）	ファイルのブロック（ファイルの信頼度、ファイルの実行を試行したプロセス、および製品名別）。
	Block Sources（ブロックのソース）	ファイルのブロック（アクションをブロックしたルール、理由（イベント サブタイプ）、および公開者別）。

ダッシュボード	パネル	説明
Activity Details: Approvals（アクティビティの詳細：承認）	Approvals（承認）	ファイルの承認（日付、コンピューター、およびファイル名別）。
	Approval Distribution（承認の分布）	ファイルの承認（ファイルの信頼度、ファイルを生成、変更、または実行したプロセス、および製品名別）。
	Approval Sources（承認のソース）	ファイルの承認（ファイルを承認したルール、理由（イベント サブタイプ）、および公開者別）。
Activity Details: New Unapproved Files（アクティビティの詳細：新しい未承認ファイル）	New Unapproved Files（新しい未承認ファイル）	エージェント コンピューターに出現した新しい未承認ファイル（日付別）。
	New Unapproved Files By Product Name（製品別の新しい未承認ファイル）	新しい未承認ファイルのリスト（公開者別）。
	Top New Unapproved File Hashes（上位の新しい未承認ファイルのハッシュ）	新しい未承認ファイルのリスト（ハッシュ別、インスタンスの多い順で順位付け）。
	Top New Unapproved File Names（上位の新しい未承認ファイルの名前）	新しい未承認ファイルのリスト（名前別、インスタンスの多い順で順位付け）。
	Potentially Malicious Files（悪質な可能性のあるファイル）	Bit9 SRSによって悪質な可能性があるファイルとして認識された新しい未承認ファイル。
	Top Computers（上位のコンピューター）	新しい未承認ファイルがあるコンピューター（インスタンスの多い順で順位付け）。
	Known Trust Values（既知の信頼度）	新しい未承認ファイルのリスト（Bit9 SRS 信頼度別（既知である場合））。
	Top Users（上位ユーザー）	新しい未承認ファイルのリスト（ユーザー別、ファイルの多い順で順位付け）。

ダッシュボード	パネル	説明
Activity Details: Events（アクティビティの詳細：イベント）	Events（イベント）	イベント（日付別）。
	Top Event Subtypes（上位のイベント サブタイプ）	イベント（イベント サブタイプ別、インスタンスの多い順に順位付け）
	Errors（エラー）	エラー メッセージ。
	Top Computers（上位のコンピューター）	イベント（イベントで参照したエージェント コンピューター別、インスタンスの多い順に順位付け）。
	Top Users（上位ユーザー）	イベント（イベントで参照したユーザー別、インスタンスの多い順に順位付け）。
	Top Event Types（上位のイベント タイプ）	イベント（イベント タイプ別、多い順）。イベント タイプには、複数のサブタイプが含まれます。
File Investigation（ファイルの調査）	Number of computers on which this file has been created（このファイルが作成されたコンピューターの数）	このサーバーにレポートする Bit9 管理コンピューターでのこのファイルの普及度。
	File Hashes（ファイル ハッシュ）	名前によるファイル検索で、この名前のファイルに対して識別されたハッシュ。
	File Information: First Seen on Network（ファイル情報：ネットワークでの最初の確認）	このサーバーにレポートする Bit9 管理コンピューターで最初に確認されたこのファイルの名前。
	Hash Activity（ハッシュ アクティビティ）	このハッシュを使用したファイルの作成と変更、およびそのファイルによる作成と変更を表す時間に基づいた棒グラフ。
	Other Hashes with First Seen Name（最初に確認された名前を持つ他のハッシュ）	このサーバーにレポートする Bit9 管理コンピューターで最初に確認されたファイル名と同じ名前を持つ他のハッシュ。
	Files Modified By This File（このファイルによって変更されたファイル）	このファイルがプロセスとなっているファイル。新しい順で簡単なイベントのテーブルとして表示されます。

ダッシュボード	パネル	説明
File Investigation（ファイルの調査）（続き）	Top Hashes Modified by This File（このファイルによって変更された上位のハッシュ）	このファイルがプロセスとなっているファイル。特定のファイル / ハッシュによってそのファイル（ハッシュで識別）が変更された回数で並べ替えて表示されます。
	Top Event Subtypes Containing This File（このファイルを含む上位のイベント サブタイプ）	このファイルへの参照を含むイベント サブタイプ。このファイルのインスタンスを最も多く含むサブタイプから順に表示されます。
	Top Rules Containing This File（このファイルを含む上位のルール）	プロセス、インストーラー、または処理対象となるファイルとしてファイル / ハッシュを認識するルールなど、このファイルを参照するルール。指定したファイルの参照回数別に、ルールが降順で表示されます。
Computer Investigation（コンピューターの調査）	Detection Events（検出イベント）	Bit9 高度な脅威の痕跡に関連するイベントのテーブル。
	Risky Behavior（リスクの高い動作）	改ざんからの保護に関する問題や、エージェント コンピューター上の危険または悪質な可能性のあるファイルの検出に関する問題に関連するイベントのテーブル。
	Risky Behavior Timeline（リスクの高い動作のタイムライン）	時間の経過に基づいてグラフ化されたリスクの高い動作の数。
	Blocks（ブロック）	このコンピューターでブロックされたファイル アクションのグラフ（日付別）。
	New Files（新しいファイル）	検索で指定したコンピューター上の新しいファイルのテーブル。
	File Activity（ファイル アクティビティ）	ファイル作成および変更のグラフ（日付別）。
	Approved Files（承認済みファイル）	承認済みのファイルおよび承認に使用されたルールのテーブル。
	Events Chart（イベント グラフ）	検索期間に特定のコンピューターが関与する上位 10 件の頻度の高いイベント サブタイプのグラフ。
	Health Checks（正常性チェック）	Bit9正常性チェック イベントおよび正常性チェックの結果のテーブル。

ダッシュボード	パネル	説明
Console User Search（コンソール ユーザー検索）	Events（イベント）	このユーザーを参照するイベントの日付別のグラフ。
	User Activity（ユーザー アクティビティ）	追加の詳細を含むテーブルに日付順で表示された、このユーザーを参照するイベント。
	New or Removed Console Users（新しいまたは削除されたコンソール ユーザー）	このユーザーによって作成または削除されたコンソール ユーザー。
	Custom Rules Actions（カスタム ルール アクション）	このユーザーによるカスタム ルールの作成と変更。
	File Approvals（ファイルの承認）	このユーザーによるファイルの承認。
	File Bans（ファイル禁止）	このユーザーによるファイルの禁止。
	Policy Management by Subtype（サブタイプによるポリシー管理）	ポリシーの変更と作成、ポリシー アクションによるエージェントのインストーラー ファイルの書き込みなど、このユーザーによって実行されたポリシー管理アクション。
	Global Approval by Trust（信頼によるグローバル承認）	ユーザーと信頼によるグローバル承認。
	Globally Approved Hashes（グローバル承認済みのハッシュ）	このユーザーによってグローバルに承認されたハッシュ。
	Local Approval by Trust（信頼によるローカル承認）	このユーザーと信頼によるローカル承認。
	Top Locally Approved Hashes（上位のローカル承認済みハッシュ）	このユーザーによってローカルで承認されたファイル（ハッシュ別）。多い順に表示されます。

ダッシュボード	パネル	説明
All Console Users（すべてのコンソール ユーザー）	Events（イベント）	日付別にグラフ化したすべてのコンソール ユーザーによるイベント。
	Policy Management（ポリシー管理）	ポリシー管理イベント（日付およびユーザー別）。
	Computer Management（コンピューター管理）	コンピューター管理イベント（日付およびユーザー別）。
	Session and General Management（セッションおよび一般管理）	セッションおよび一般管理イベント（日付およびユーザー別）。
	Top Ten User - Global Approvals（上位 10 ユーザー – グローバル承認）	グローバルのファイル承認が最も多い上位 10 人のユーザー。
	Top Ten User - Local Approvals（上位 10 ユーザー – ローカル承認）	ローカルのファイル承認が最も多い上位 10 人のユーザー。

Bit9 向け Splunk アプリでの CIM へのフィールド マッピング

Splunk のセキュリティ ツールを使用するには、データを正規化してソースに関係なく同じ方法でデータを処理し、分析できるようにする必要があります。Bit9 Security Platform 向け Splunk アプリでは、Bit9 データ分析出力のフィールドは CIM（共通情報モデル）にマッピングされます。共通情報モデルの詳細については、http://www.dmtf.org/standards/cim を参照してください。

表 132 では、Bit9 向け Splunk アプリで行われる CIM マッピングを示しています。

表 132：Splunk での Bit9 データと CIM のマッピング

Bit9 のフィールド	CIM のフィールド
HostName	src_nt_host、dest_nt_host、dest, dvc_nt_host
HostIP	src_ip、dest_ip、dvc_ip
FilePath	file_path
FileHash	file_hash、hash
FileName	file_name
FileSize	file_size、size
Message	change_type
EventSubType	action
Timestamp	modtime

インデックス

A

B

C

D

E

F

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

あ

い

う

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

つ

て

と

ね

は

ひ

ふ

へ

ほ

ま

み

む

め

も

ゆ

よ

ら

り

る

れ

ろ

わ