TREND MICRO

PortalProtect™ 2.6

管理者ガイド

Collaboration Security

※注意事項

複数年契約について

・お客さまが複数年契約（複数年分のサポート費用前払い）された場合でも、各製品のサポート期間については、当該契約期間によらず、製品ごとに設定されたサポート提供期間が適用されます。

・複数年契約は、当該契約期間中の製品のサポート提供を保証するものではなく、また製品のサポート提供期間が終了した場合のバージョンアップを保証するものではありませんのでご注意ください。

・各製品のサポート提供期間は以下の Web サイトからご確認いただけます。

https://success.trendmicro.com/dcx/s/solution/000207383?language=ja

法人向け製品のサポートについて

・法人向け製品のサポートの一部または全部の内容、範囲または条件は、トレンドマイクロの裁量により随時変更される場合があります。

・法人向け製品のサポートの提供におけるトレンドマイクロの義務は、法人向け製品サポートに関する合理的な努力を行うことに限られるものとします。

商標について

TRENDMICRO、TREND MICRO、ウイルスバスター、InterScan、INTERSCAN VIRUSWALL、InterScanWebManager、InterScan Web Security Suite、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、Trend Park、Trend Labs、Network VirusWall Enforcer、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、SPN、SMARTSCAN、Trend Micro Kids Safety、Trend Micro Web Security、Trend Micro Portable Security、Trend Micro Standard Web Security、Trend Micro Hosted Email Security、Trend Micro Deep Security、ウイルスバスタークラウド、スマートスキャン、Trend Micro Enterprise Security for Gateways、Enterprise Security for Gateways、Smart Protection Server、Deep Security、ウイルスバスター ビジネスセキュリティサービス、SafeSync、Trend Micro NAS Security、Trend Micro Data Loss Prevention、Trend Micro オンラインスキャン、Trend Micro Deep Security Anti Virus for VDI、Trend Micro Deep Security Virtual Patch、SECURE CLOUD、Trend Micro VDI オプション、おまかせ不正請求クリーンナップサービス、Deep Discovery、TCSE、おまかせインストール・バージョンアップ、Trend Micro Safe Lock、Deep Discovery Inspector、Trend Micro Mobile App Reputation、Jewelry Box、InterScan Messaging Security Suite Plus、おもいでバックアップサービス、おまかせ！スマホお探しサポート、保険&デジタルライフサポート、おまかせ！迷惑ソフトクリーンナップサービス、InterScan Web Security as a Service、Client/Server Suite Premium、Cloud Edge、Trend Micro Remote Manager、Threat Defense Expert、Next Generation Threat Defense、Trend Micro Smart Home Network、Retro Scan、is702、デジタルライフサポート プレミアム、Air サポート、Connected Threat Defense、ライトクリーナー、Trend Micro Policy Manager、フォルダシールド、トレンドマイクロ認定プロフェッショナルトレーニング、Trend Micro Certified Professional、TMCP、XGen、InterScan Messaging Security、InterScan Web Security、Trend Micro Policy-based Security Orchestration、Writing Style DNA、Securing Your Connected World、Apex One、Apex Central、MSPL、TMOL、TSSL、ZERO DAY INITIATIVE、Edge Fire、Smart Check、Trend Micro XDR、Trend Micro Managed XDR、OT Defense Console、Edge IPS、スマスキャ、Cloud One、Cloud One - Workload Security、Cloud One - Conformity、ウイルスバスター チェック！、Trend Micro Security Master、Worry-Free XDR、Worry-Free Managed XDR、Network One、Trend Micro Network One、らくらくサポート、Service One、超早得、

P/N: PPEM28661/190425_JA_R2 (2024/03)

プライバシーと個人データの収集に関する規定

トレンドマイクロ製品の一部の機能は、お客さまの製品の利用状況や検出にかかわる情報を収集してトレンドマイクロに送信します。この情報は一定の管轄区域内および特定の法令等において個人データとみなされることがあります。トレンドマイクロによるこのデータの収集を停止するには、お客さまが関連機能を無効にする必要があります。

PortalProtect により収集されるデータの種類と各機能によるデータの収集を無効にする手順については、次の Web サイトを参照してください。

https://www.go-tm.jp/data-collection-disclosure

重要

データ収集の無効化やデータの削除により、製品、サービス、または機能の利用に影響が発生する場合があります。PortalProtect における無効化の影響をご確認の上、無効化はお客さまの責任で行っていただくようお願いいたします。

トレンドマイクロは、次の Web サイトに規定されたトレンドマイクロのプライバシーポリシー (Global Privacy Notice) に従って、お客さまのデータを取り扱います。

https://www.trendmicro.com/ja_jp/about/legal/privacy-policy-product.html

目次

はじめに

第 1 章：概要

第 4 章：セキュリティリスク検索

第 5 章：ファイルブロック

第 9 章：手動検索

第 10 章：予約検索

第 11 章：通知、警告、ログ、およびレポート

はじめに

PortalProtect 管理者ガイドへようこそ。本書には、PortalProtect を設定して SharePoint サーバを保護するために必要な情報が記載されています。

本章の内容は次のとおりです。

ドキュメント

PortalProtect には、次のドキュメントが付属しています。

- オンラインヘルプ (英語) — 各種作業を実行するための詳細な手順の説明。
- インストールガイド — 製品の概要、インストール計画、インストール、設定、起動方法に関する説明。
- 管理者ガイド — 製品の概要、インストール計画、インストール、設定、および製品環境を管理するために必要な詳細情報の説明。
- Readme — 基本的なインストール方法と既知の制限事項に関する説明。

注意

ドキュメントおよびプログラムファイルの最新版については、最新版ダウンロードサイト (https://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp) から該当するリンクにアクセスしてチェックすることをお勧めします。

対象読者

PortalProtect のドキュメントは、セキュリティシステムや Microsoft Windows SharePoint サービスの管理について基本的な知識があることを前提としています。インストールガイド、管理者ガイド、およびオンラインヘルプはネットワーク管理者を対象に作成されています。

ドキュメントの表記規則

このドキュメントでは、次の表記規則を使用しています。

表 1. ドキュメントの表記規則

表記	説明
注意	設定上の注意

表記	説明
 ヒント	推奨事項
 重要	必須の設定や初期設定、および製品の制限事項に関する情報
 警告!	避けるべき操作や設定についての注意

第 1 章

概要

Trend Micro PortalProtect (以下、PortalProtect) 2.6 は、Microsoft SharePoint Server 2013/2016/2019/サブスクリプションエディション 用のサーバベースのセキュリティソリューションです。PortalProtect は、ウイルスをはじめとするセキュリティの脅威による攻撃からコラボレーションシステムを 保護します。

PortalProtect は、Microsoft SharePoint Server と統合するように設計され、実績のあるエンタープライズセキュリティテクノロジを 基盤として構築されています。SharePoint Server でコンテンツをチェックイン、チェックアウト、およびパブリッシュするたびに、すべてのコンテンツに対してリアルタイムのバックグラウンド検索が実行されます。また、SharePoint Server の SQL コンテンツストアに格納されているコンテンツに対して手動および予約検索が可能です。

PortalProtect では、広範囲にわたる集中型の管理および通知機能が提供されます。これらの機能を使用することで、通知の送信、レポートの生成、ログクエリの生成などのタスクを実行できます。アウトブレークアラートなどの自動通知機能によって、早期に攻撃を検出し、より的確に対処できるようになります。

本章では、PortalProtect の利点や機能を紹介し、SharePoint 環境におけるセキュリティの 脅威と、PortalProtect がこれらの脅威から環境をどのように保護するかについて説明します。

本章の内容は次のとおりです。

新機能

PortalProtect 2.6 の新機能

本リリースの PortalProtect には、次の新機能が含まれています。

機能	説明
SharePoint Server サブスクリプションエディションのサポート	Microsoft SharePoint Server サブスクリプションエディションをフルサポートします。
Windows Server 2022 デスクトップエクスペリエンスのサポート	Microsoft SharePoint サブスクリプションエディションを実行する Microsoft Windows Server 2022 デスクトップエクスペリエンスをサポートします。
Windows Server 2022 Server Core のサポート	Microsoft SharePoint サブスクリプションエディションを実行する Microsoft Windows Server 2022 Server Core をサポートします。
SQL Server 2019 のサポート	データベースサーバとして Microsoft SQL Server 2019 をサポートします。
SharePoint Server 2019 のサポート	Microsoft SharePoint Server 2019 をフルサポートします。
Windows Server 2019 のサポート	Microsoft SharePoint Server を実行する Microsoft Windows Server 2019 をサポートします。
SQL Server 2017 のサポート	データベースサーバとして Microsoft SQL Server 2017 をサポートします。
トレンドマイクロのアップデートサーバへの HTTPS 接続	初期設定で、トレンドマイクロのアップデートサーバへの接続に HTTPS が使用されます。

グローバル除外リスト

PortalProtect には、グローバル除外リストという情報漏えい対策、コンテンツフィルタ、およびファイルブロック用の追加機能があります。これは、管理者が、情報漏えい対策、ファイルブロック、およびコンテンツフィルタのポリシーから除外する Active Directory ユーザおよびグループを追加できる

除外リストです。リアルタイムコンテンツフィルタは 、ドキュメントと Web コンテンツの両方に使用可能です。

機能と利点

PortalProtect には、次の機能や利点があります。

- 高速で簡単なインストール
  - 1 つのインストールプログラムを使用して 1 台または複数の SharePoint サーバにインストールできます。
- 強力な独自のウイルス対策機能
  - プロアクティブなマルチスレッド 検索を使用して、ドキュメントの作成者がチェックインまたはチェックアウトするときやユーザが参照するためにドキュメントを開くときなど、複数のアクセスポイントからのアクセスに対してリアルタイムのウイルス 検出および駆除を実行できます。
  - トレンドマイクロの推奨設定を使用して、ファイル拡張子が変更されているかどうかに関係なく、実際のファイルタイプの 検出および検索を実行できます。
  - 有害な可能性のあるマクロウイルスを検出して削除します。
  - トレンドマイクロの推奨処理を使用して脅威を、ウイルス、不正マクロコード、およびその他の脅威などに分類できます。
- ファイルブロック
  - ウイルスの大規模感染発生時には、ファイルブロック機能を使用することで、管理者が指定したすべてのファイルタイプを 一時的にブロックできます。
  - Microsoft Active Directory ユーザ/グループまたは SharePoint ユーザ/グループと統合されている、ポリシーベースのファイルブロックを実行します。
- コンテンツフィルタ
  - ルールベースのフィルタを 使用して、不快、または好ましくないと思われるファイルおよび Web コンテンツを選別して除去します。

- Microsoft Active Directory ユーザ/グループまたは SharePoint ユーザ/グループと統合されている、ポリシーベースのコンテンツフィルタを実行します。

- Web レピュテーション
  - Web レピュテーションフィルタを使用して、Web ベースのセキュリティリスクをブロックします。
- 情報漏えい対策
  - 個人を特定可能な情報が、ドキュメントライブラリ、Wiki、ブログ、ディスカッションフォーラムなどに投稿されるか、それらから取得されることを標準テンプレートまたはユーザカスタマイズテンプレートを使用して防止します。
- 隔離
  - 1 つのファーム内の隔離ファイルに対して集中的な隔離管理を実行します。
- 手動検索と予約検索
  - 不正コードやウイルスの脅威に対する追加の保護機能として、リアルタイム検索の他に、SharePoint SQL Server コンテンツストアへの手動および予約検索を実行できます。
- アップデート
  - 手動および予約アップデートによって、最新の保護状態を維持できます。
  - トレンドマイクロのアップデートサーバを使用して、自動的に最新のウイルスパターンファイルや検索エンジンのアップデートを検索し、ダウンロードできます。
- 容易な管理
  - 一元化された設定、レポート、ログ、およびアップデートの機能を備え、管理者やワークスペースコーディネータなどの受信者へ、カスタマイズ可能な警告メッセージをリアルタイムに通知できます。
  - Trend Micro Control Manager との統合がサポートされています。

ウイルスが SharePoint 環境に感染するしくみ

社内ユーザが情報を作成および収集する際に、情報の検索、整理、および管理に費やされる時間が増加しています。SharePoint Server は組織の Web ポータルを短期間で作成するための機能を搭載し、それに検索機能、ドキュメント管理機能、およびコラボレーションオプションが統合されています。SharePoint Server を使用することで、物理的な場所に関係なくユーザ間で簡単に情報を共有できるようになりますが、同時にセキュリティリスクも増大します。ファイル共有やリアルタイムで双方向の情報交換は、侵入用の入口やデータ盗用の機会をサイバー犯罪者に与えているのです。

PortalProtect が SharePoint Server を保護するしくみ

PortalProtect は、SharePoint Server をさまざまな方法で保護します。この中核となる機能がコンテンツの検索とブロックです。ユーザは、PortalProtect がファイルをブロックしたりウイルスを検出したりする際の処理を設定できます。これらのイベントについての通知を管理者やその他の受信者へ送信することもできます。

- PortalProtect では、ファイルまたは Web コンテンツを検索し、そのいずれかがポリシーに違反しているかどうかを判断できます。違反が検出されると、管理者の事前設定に従って隔離や削除などの処理が実行されます。
- PortalProtect では、ファイルまたは Web コンテンツ内の URL を検索して不正な URL を検出できます。不正な URL が検出されると、管理者の事前設定に従ってブロックや放置などの処理が実行されます。
- PortalProtect では、ファイル拡張子、ファイル名、実際のファイルタイプなどに基づいてファイルをブロックできます。PortalProtect が特定のファイルタイプを検出すると、管理者の事前設定に従って隔離や削除などの処理が実行されます。
- 検索では、ウイルスやその他の不正プログラムの検出に最新の検索エンジンが使用されます。PortalProtect がウイルスや不正コードを検出すると、管理者の設定に従って隔離や削除などの処理が実行されます。検索エンジンでは複数のスレッドを管理可能なため、多数の要求を同時に処理できます。要求を優先順位に従って処理することもできます。

PortalProtect には定期的なフィードバックおよびレポート機能があり、最新のセキュリティの脅威やシステムのステータスに関する情報を受信できます。コンポーネントのアップデートや検出時の処理など、重要なイベントがログに記録されます。これらのイベントについてクエリを実行し、ログを作成することで、最新の詳細情報を取得できます。また、印刷およびエクスポート可能な分析用レポートを生成するように設定できます。

検索エンジンは、次の方法ですべてのコンテンツを検索します。

- リアルタイム検索 — リアルタイム検索は、継続的に実行される検索です。SharePoint Server のウイルス対策機能を有効にすると、PortalProtect によってファイルのチェックイン、チェックアウト、保存、および取得ごとにリアルタイム検索が実行されます。すべての受信および送信ファイルがウイルスやその他の不正コードについて検索されます。検索エンジンは、複数のスレッドを管理し、多数の要求を同時に処理する能力を備えています。
- 手動検索 (Scan Now) — 手動検索はオンデマンドの検索であり、検索を実行するとただちに開始され、設定に応じてドキュメントライブラリの全部または一部のファイルが検索されます。データベース内の全部または一部のフォルダを検索するように検索タスクを設定できます。手動検索は、SharePoint サーバの任意のコンテンツをすぐに検索する方法として利用できます。
- 予約検索 — 予約検索は指定された日時や頻度で自動的に実行されます。設定に応じてドキュメントライブラリの全部または一部のファイルを検索します。予約検索によって、SharePoint サーバでの定期的な検索を自動化できるため、ウイルス対策管理の効率化や、ウイルス対策ポリシーのより詳細な管理が可能です。

トレンドマイクロでは、いくつかの検索タスクを組み合わせて安全な SharePoint 環境を構築することをお勧めします。手動検索を設定および実行すると、SQL Server のコンテンツストアに保存されたコンテンツから脅威が除去されます。リアルタイム検索を設定および有効化すると、新しい脅威が発生したときに SharePoint サーバが保護されます。最後に、定期的に予約検索を実行することで安全な SharePoint 環境を維持できます。

PortalProtect のアーキテクチャ

PortalProtect は、SharePoint Server に総合的なセキュリティ機能を提供します。

PortalProtect セキュリティソリューションの中核機能は、トレンドマイクロ独自の検索エンジンです。この検索エンジンは、SharePoint Server によって管理される Antivirus Manager (AVM) と統合されます。リアルタイム検索時、コンテンツが SharePoint Server でチェックイン、チェックアウト、またはパブリッシュされるたびに、Antivirus Manager でトレンドマイクロの検索エンジンが呼び出されます。トレンドマイクロの検索エンジンは、コンテンツを検索することで応答します。手動または予約検索の間、検索エンジンは SharePoint Server SQL データベース内のすべてのコンテンツにアクセスします。

Microsoft Office や Internet Explorer を実行する SharePoint Server クライアントは、Internet Information Services (以下、IIS) を使用して SharePoint Server 環境と通信します。PortalProtect の Web 管理コンソールを使用する SharePoint の管理者も、IIS を使用して SharePoint 環境と通信します。

PortalProtect は、HTTP を介してトレンドマイクロのアップデートサーバやその他のインターネット/イントラネット上のサーバからコンポーネントを受信できます。

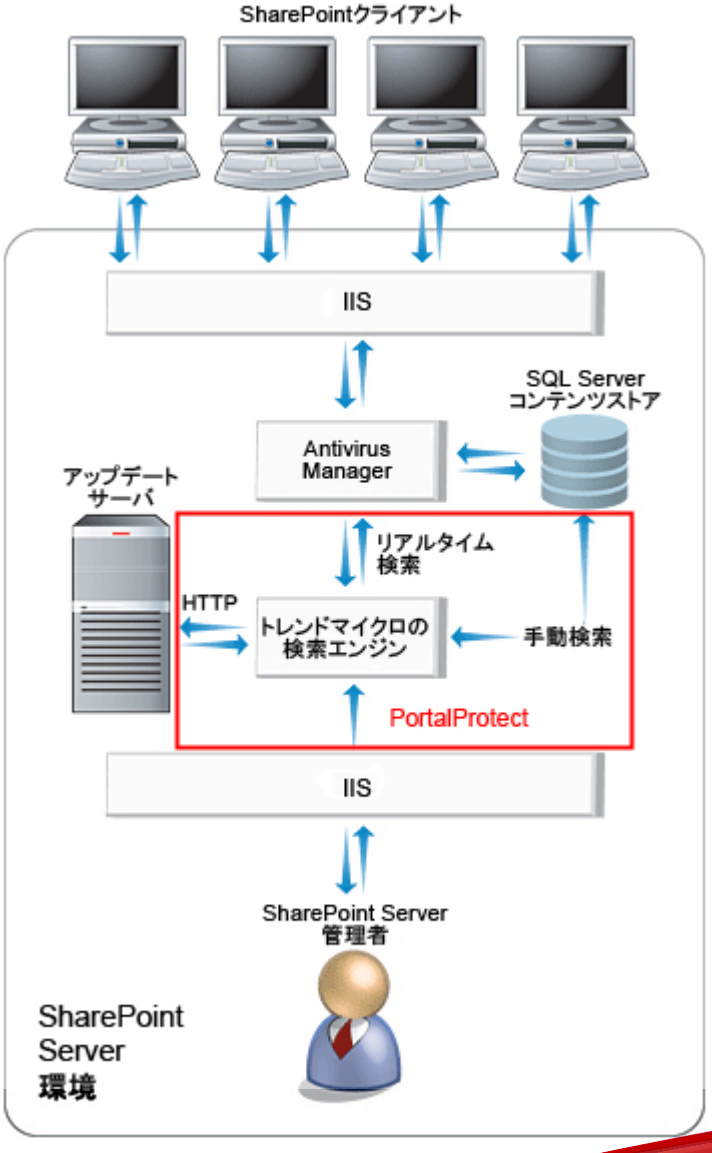


図 1-1. PortalProtect と SharePoint Server との連携

大規模感染の制御

PortalProtect は、ウイルスの大規模感染発生時に、さまざまな方法で SharePoint Server を保護します。ポータル環境の保護には、次の方法を使用できます。

- PortalProtect の通知機能を使用して、管理者や IT 技術者への早期の警告を配信します。
- 手動アップデート (Update Now) を使用して、最新のウイルスパターンファイルと検索エンジンをただちにダウンロードします。手動検索を設定および実行し、ウイルスに対する処理を設定します。早期の効果的な対処を実現するため、トレンドマイクロの推奨設定や推奨処理などの機能を選択し、PortalProtect がウイルスに対して推奨されるブロックおよび処理を行うようにします。
- 手動またはリアルタイム検索のブロックオプションを設定して、特定のファイルタイプまたはファイル名を検出するように設定します。特定のファイルタイプやファイル名について、ブロックや隔離などの処理を実行するように PortalProtect を設定し、SharePoint サーバへの感染を防止します。

注意

この方法は、ウイルスの正確な名前を認識している場合に特に有効です。ウイルスのアラート情報については、以下の脅威データベースを参照してください。

https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/

- リアルタイム検索を設定し、検出されたウイルスに対する処理を設定します。早期の効果的な対処を実現するため、トレンドマイクロの推奨設定や推奨処理などの機能を選択し、PortalProtect がウイルスに対して推奨されるブロックおよび処理を行うようにします。
- 処理結果を分析するためにレポートを生成し、ログのクエリを実行します。感染元または感染を媒介した SharePoint サーバのサイトを特定します。

PortalProtect のテクノロジ

トレンドマイクロの検索エンジンは、ウイルス/不正プログラムなどのセキュリティの脅威を検出して、望ましくないコンテンツを排除できます。このエンジンは、TrendLabs によって提供され、アップデートサーバまたはユーザが設定したアップデート元を経由して配信される最新のパターンファイルに基づいています。

トレンドマイクロの検索エンジンについて

ウイルス検索エンジンは、すべてのトレンドマイクロ製品の中枢です。もともとは、ファイルベースのコンピュータウイルスの対策として開発されました。現在の検索エンジンはより洗練され、不正プログラムやスパイウェアなどの多種多様なセキュリティリスクを検出します。

- 世界中広範囲のコンピュータで確認されているウイルス (IN THE WILD)
- 研究などで開発された、世の中に出回っていないウイルス (IN THE ZOO)

トレンドマイクロの検索エンジンは、すべてのファイルの全領域を検索する代わりに、エンジンとパターンファイルの連携によりウイルスコードの兆候やウイルスが潜む可能性が高いファイル中の領域を特定して検索します。ウイルスが検出されると、そのウイルスを削除して、ファイルの整合性を復元することができます。

検索エンジンは、(ディスクスペース 容量の管理のために) 古いウイルスパターンファイルを自動的にクリーンナップし、(帯域幅を最低限度に抑えるために) パターンファイルの差分アップデートを行う機能を持ちます。

さらに、検索エンジンでは (MIME や BinHex を含む) 主要な暗号形式をすべて復号化できます。検索エンジンは、.Zip、.Arj、.Cab などの一般的な圧縮形式を認識し、検索します。ほとんどのトレンドマイクロ製品では、圧縮ファイル内に含まれる圧縮ファイルについて、検索する圧縮階層数を製品の管理者が指定できます (最大 20 階層)。

検索エンジンは最新の状態を維持することが重要です。トレンドマイクロでは、次の 2 つの方法でこれを可能にしています。

- ウイルスパターンファイル (検索エンジンデータファイル) の頻繁なアップデート。ウイルスパターンファイルはダウンロードしてエンジンで読み取ることができ、エンジンコード自体を変更する必要はありません。

- SQL Slammer のような複合型の脅威が発生した場合など、ウイルスの脅威の性質が変化したことによるエンジンソフトウェアの技術的なアップグレード。いずれの場合も、アップデートが自動的にスケジュールされます。またセキュリティ管理者はこれらの更新を手動で処理できます。

検索エンジンのアップデートについて

最も緊急を要するウイルス情報をウイルスパターンファイルに含めることで、検索エンジンのアップデート回数を最低限に抑えながら、保護状態を最新に保つことができます。ただし、このような場合でも、トレンドマイクロは新しい検索エンジンのバージョンを定期的に作成しています。新しいエンジンは、たとえば次のタイミングでリリースされます。

- トレンドマイクロが新しい検索および検出テクノロジをソフトウェアに導入したとき
- 現在のエンジンでは処理できない、危害を加える可能性がある新しいウイルスが発見されたとき
- 検索機能が強化されたとき
- 新しいファイル形式、スクリプト言語、エンコード、圧縮フォーマットなどのサポートが追加されたとき

最新バージョンの検索エンジンを確認するには、次の URL を参照してください。

https://downloadcenter.trendmicro.com/index.php?regs=jp&clk=result_page&clkval=drop_list&prodid=1321

ウイルスパターンファイルについて

トレンドマイクロの検索エンジンは、ウイルスパターンファイルと呼ばれる外部データファイルを使用して、最新のウイルスや、トロイの木馬、マスメール活動、ワーム、および複合型攻撃 (例: Bagle、NetSky) などのその他のインターネットの脅威に対して最新の状態を維持します。

アップデート機能を使用するすべてのトレンドマイクロウイルス対策プログラムは、トレンドマイクロのサーバでの新しいウイルスパターンファイルの準備状況を検出できます。さらに、サーバを毎週、毎日、または 1 時間ごとに自動的にポーリングし、最新のファイルを取得するように設定できます。

自動アップデートは最低でも 1 日に 1 回予約しておくことをお勧めします。これは PortalProtect の出荷時の初期設定です。

ウイルスパターンファイルは次の Web サイト (英語) から手動でダウンロードできます。ここでは、現在のバージョン、リリース日、さらにこのファイルに含まれているすべての新しいウイルス定義も参照できます。

https://www.trendmicro.com/en_us/business/products/downloads.html?clk=left_nav&clkval=pattern_file&regs=NABU

検索のしくみ

検索エンジンは、ウイルスパターンファイルを利用し、パターンマッチングと呼ばれる処理を使用して最初のレベルの検出を実行します。各ウイルスには、他のコードと区別可能な、特徴を表す固有のシグネチャや文字列が含まれており、TrendLabs のウイルス専門家はパターンファイル内にこのコードの無害なスニペットを入れています。次に、検索エンジンは、検索する各ファイルの特定部分とウイルスパターンファイル内のパターンを比較して、一致を探します。一致が検出されると、システム管理者にメールで通知が送信されます。

アップデートについて

アップデートは、多くのトレンドマイクロ製品に共通の機能です。トレンドマイクロのアップデートサーバに接続し、ウイルスパターンファイル、検索エンジン、スパムメール判定ルール、およびプログラムファイルをダウンロードできるようにします。アップデートを実行しても、ネットワークサービスが妨げられたり、コンピュータを再起動する必要はありません。アップデートは、定期スケジュールに従って利用することも、必要に応じて利用することも可能です。

ウイルスパターンファイルの差分アップデート

アップデートでは、ウイルスパターンファイルの差分アップデートがサポートされています。アップデートでは、毎回すべてのパターンファイルをダウンロードするのではなく、新しいファイルと既存パターンファイルへの追加のみを部分的にダウンロードできます。これは効率的なアップデート方法であり、ウイルス対策ソフトウェアをアップデートするために必要となる帯域幅を大幅に削減できます。

PortalProtect でのアップデートの使用

PortalProtect では、手動および予約によるコンポーネントアップデートのダウンロード元として、トレンドマイクロのアップデートサーバを 使用するように設定できます。コンポーネントのアップデート時には、PortalProtect がアップデートサーバを直接ポーリングし、利用可能なアップデートがあるかどうか判断して、ダウンロードします。

注意

新しい脅威は毎日のように出現しています。アップデートは最低でも 1 日に 1 回実行することをお勧めします。

トレンドマイクロの推奨設定 (Intelliscan) について

ウイルス対策ソリューションの多くは、潜在的な脅威について検索する対象ファイルの特定に 2 つのオプションを用意しています。PortalProtect では、すべてのファイルを検索することも (最も安全な方法)、実際のファイルタイプやファイル拡張子に基づいて対象ファイルを特定し、検索することもできます。ただし、拡張子を変更してファイルを偽装しようとする試みがますます増えているため、拡張子に基づくファイルの特定はあまり有効ではないことに留意してください。

トレンドマイクロの推奨設定は、ファイル名の拡張子に関係なくファイルの実際のファイルタイプを特定するトレンドマイクロのテクノロジです。トレンドマイクロの推奨設定では、対象ファイルを特定して検索を行うため、すべてのファイルを検索する場合に比べて効率的です。

注意

トレンドマイクロの推奨設定は、すべてのファイルでヘッダを調べますが、特定の指標に基づき、セキュリティリスクに感染しやすいと判断されたファイルのみを検索対象として選択します。

トレンドマイクロの推奨設定では感染しやすいと判断されたファイルのみが検索対象となるため、次のような利点があります。

- パフォーマンスの最適化。すべてのファイルを検索する場合に比べて使用するシステムリソースが少なくなります。

- 検索時間の短縮。すべてのファイルを検索する場合に比べて検索時間が短縮されます。

Trend Micro Smart Protection Network について

Trend Micro Smart Protection Network は、セキュリティリスクや Web 上の脅威からお客さまを保護するために設計された、次世代のクラウド-クライアント型コンテンツセキュリティインフラストラクチャです。これによりオンプレミス型ソリューションとホスト型ソリューションの両方が強化され、ユーザは企業ネットワーク内、自宅、外出先などの場所に関係なく保護されます。Trend Micro Smart Protection Network では、軽量クライアントを使用して、独自のインターネットクラウドで提供されているメールレピュテーション、Web レピュテーション、ファイルレピュテーションの相関分析テクノロジおよび脅威データベースにアクセスします。より多くの製品、サービス、およびユーザがネットワークにアクセスすれば、それだけ保護機能が自動的に更新および強化されることになり、利用者自身のリアルタイムな自警システムが構築されていきます。スマートスキャンソリューションでは、クラウド内保護のために Trend Micro Smart Protection Network が利用されます。

Smart Protection サービス

Smart Protection サービスでは、クラウドに保存された不正プログラム対策シグネチャ、Web レピュテーション、および脅威のデータベースが提供されます。Smart Protection では、ファイルレピュテーションテクノロジを使用してセキュリティリスクを検出し、Web レピュテーションテクノロジを使用して不正な Web サイトをブロックします。ファイルレピュテーションテクノロジにより、これまでエンドポイントに保存されていた大量の不正プログラム対策シグネチャの負荷が Trend Micro Smart Protection Network または Smart Protection Server に移行されます。Web レピュテーションテクノロジでは、以前に Trend Micro Smart Protection Network に保存されていた URL が Smart Protection Server に配置されます。両方のテクノロジを併用することにより、パターンファイルのアップデートや URL の妥当性のクエリで消費される帯域幅を削減できます。

さらにトレンドマイクロは、世界各国で使用されているトレンドマイクロ製品から保護された情報を収集し、新しい各種の脅威を積極的に特定しています。

Web レピュテーション

Web レピュテーションテクノロジは、Web サイトの経過日数、配置場所の変更履歴、および不正プログラムの挙動分析により検出された不審な活動の兆候などの要素に基づいてレピュテーションスコアを割り当てることにより、Web ドメインの信頼性を追跡します。サイトは継続的に検索され、感染サイトへのユーザアクセスがブロックされます。

ユーザが URL にアクセスすると、次の処理が実行されます。

- ドメインレピュテーションデータベースを使用して Web サイトやページの信頼性を確認します。
- Web ドメインや個々のページまたはサイト内のリンクにレピュテーションスコアを割り当てます。
- サイトへのユーザのアクセスを許可またはブロックします。

精度を向上させると同時に誤検出を少なくするため、トレンドマイクロの Web レピュテーションテクノロジでは、サイト全体を分類またはブロックするのではなく、サイト内の特定のページまたはリンクにレピュテーションスコアを割り当てています。これは、以前に正規サイトの一部分のみがハッキングされ、長期にわたってレピュテーションが動的に変化したことに対応する処理です。

Smart Protection ソース

Smart Protection ソースは、Smart Protection コンポーネントをダウンロードし、それらのコンポーネントのホストとなります。エンドポイントでは Web サイトの検索および Web サイトへのアクセスを実行するときに、これらのコンポーネントに対してクエリを実行します。クライアントは、次のいずれかの Smart Protection ソースに接続できます。

- Smart Protection Server: Smart Protection Server は、ローカル (社内ネットワーク) の企業ネットワークにアクセス可能なユーザ向けのものです。ローカルサーバは、効率を最適化するために、Smart Protection サービスを企業ネットワーク内で実行します。
- Trend Micro Smart Protection Network: 企業ネットワークに直接アクセスできないユーザにレピュテーションサービスを提供する、グローバル規模のインターネットベースインフラストラクチャです。

実際のファイルタイプ

実際のファイルタイプに基づいて検索を実行するように PortalProtect が設定されている場合、検索エンジンは、ファイル名でなくファイルヘッダを調べて実際のファイルタイプを判定します。たとえば、すべての実行可能ファイルを検索するように設定されている検索エンジンで `family.gif` という名前のファイルが検出された場合、ファイル拡張子からそのファイルがグラフィックのように見えても、検索は続行されます。検索の間に、検索エンジンは、ファイルヘッダを開いて内部に登録されたデータ型を調べ、そのファイルが実際にグラフィックファイルであるのか、または検出を避ける目的で名前が意図的に変更された実行可能ファイルであるのかどうかを確認します。

実際のファイルタイプに基づく検索をトレンドマイクロの推奨設定 (Intelliscan) と併せることで、危険をもたらすと知られているファイルタイプのみが検索されます。これらのテクノロジを使用すると、検索エンジンが検証するファイルの総数は削減されますが (最大で全体の 3 分の 2 程度)、セキュリティリスクが高くなる可能性があります。

たとえば、Web トラフィックの大部分を占める `.gif` ファイルや `.jpg` ファイルでは、ウイルスを潜伏させたり、実行可能ファイルコードを起動したり、既知または理論上のセキュリティホールを攻撃したりすることはできません。だからといって、これらのファイルが本当に安全なのかといえば、そうではありません。悪意のあるハッカーが有害なファイルに安全なファイル名を付け、検索エンジンの検出を逃れてネットワークを通過するように偽装している可能性があります。誰かがこのファイルの名前を変更して実行すると、システムに危害が加えられる可能性があります。

ヒント

最高のセキュリティレベルを確保するには、すべてのファイルを検索することをお勧めします。

IntelliTrap について

ウイルス作成者は、リアルタイム圧縮アルゴリズムを使用してウイルスフィルタを回避しようとすることがよくあります。IntelliTrap は、リアルタイム圧縮された実行可能ファイルをブロックして、これらのファイルを他の不正プログラム特性と組み合わせることで、このようなウイルスがネットワークに侵入するリスクを低減します。IntelliTrap はこのようなファイルをセキュリティリスクと判断して、安全なファイルを誤ってブロックする可能性があ

るため、IntelliTrap を有効にしているときは、ファイルを削除したり駆除したりせずに隔離することをお勧めします。ユーザがリアルタイム圧縮された実行可能ファイルを頻繁に使用する場合は、IntelliTrap を無効にしてください。

IntelliTrap では次のコンポーネントが使用されます。

- ウイルス検索エンジン
- IntelliTrap パターンファイル
- IntelliTrap 除外パターンファイル

トレンドマイクロの推奨処理 (Active Action)

トレンドマイクロの推奨処理では、ウイルス/不正プログラムの種類が識別され、ウイルスのそれぞれの種類がコンピュータシステムや環境に侵入する方法に基づいて処理が推奨されます。トレンドマイクロの推奨処理では、不正コード、複製、およびペイロードの各種類をウイルス/不正プログラムとして分類します。PortalProtect によりウイルス/不正プログラムが検出されると、そのウイルス/不正プログラムの種類に対応した推奨処理 (駆除、隔離、削除) が実行されて、環境内の攻撃されやすいポイントが保護されます。

検出時の処理に詳しくない場合、またはある特定のタイプのウイルス/不正プログラムに適した処理を確定できない場合、トレンドマイクロの推奨処理を使用することをお勧めします。

トレンドマイクロの推奨処理を使用すると、次の利点があります。

- 時間の節約と保守の容易さ — トレンドマイクロの推奨処理では、トレンドマイクロが推奨する処理が使用されます。処理の設定に時間を割く必要はありません。
- アップデート可能 — ウイルス/不正プログラム作成者は、ウイルス/不正プログラムによるコンピュータの攻撃方法を絶えず変えています。トレンドマイクロの推奨処理の設定は、新しいウイルスパターンファイルごとにアップデートされ、最新の脅威や、ウイルス/不正プログラムによる攻撃の最新の方法からユーザを保護します。

カスタマイズされた設定

検出された脅威のタイプに基づいてカスタマイズされた処理を実行するように PortalProtect を設定する場合は、[Customize action for detected threats] を選択します。

画面の下部で、感染したファイルのバックアップを作成してから処理を実行するように PortalProtect を設定できます。これは、元のファイルが破損しないようにするための予防措置です。

カスタマイズされた検出時の処理の使用

ユーザ環境での検索を最適化するには、カスタマイズされた処理を使用します。

- 検出されたすべてのセキュリティリスクに対して同じ処理を使用するよう PortalProtect を設定するには、[All threats] を選択し、初期設定の処理に同意するかまたはカスタマイズされた処理を選択します。
- PortalProtect によって検出される脅威のタイプごとに処理を設定するには、[Specify action per detected threat] を選択し、その脅威タイプを検出したときに PortalProtect が実行する処理を個別に設定します。

脅威の種類

- ウイルス — コンピュータウイルスは、他のファイル (.exe、.com、.dll など) に寄生して、ファイルのオープン時または起動時に実行されることで自己複製するプログラムです。
- マクロ — マクロには不正プログラムコードが含まれている可能性があります。マクロウイルスはアプリケーション固有で、Microsoft Office アプリケーションをターゲットにしています。PortalProtect には、これらのファイルを対象とした 4 レベルのヒューリスティック検索が用意されています。また、検出されたすべてのマクロを削除することもできます。22 ページの「マクロウイルスについて」を参照してください。
- その他の脅威 — その他の脅威には、スパイウェア、ダイヤラー、ハッキングツール、パスワード解読アプリケーション、アドウェア、ジョークプログラム、リモートアクセスツールなどがあります。その他の脅威に対する初期設定の処理は隔離です。これらの脅威の詳細については、セキュリティ情報に関するトレンドマイクロの Web サイト (https://

www.trendmicro.com/vinfo/jp/threat-encyclopedia/) を参照してください。

- 暗号化またはパスワード保護されたファイル — PortalProtect では、これらのファイルタイプを検索しません。代わりに、これらのファイルタイプが SharePoint サーバの脅威にならないように防御する処理を実行します。PortalProtect が実行する処理は設定に応じて異なります。初期設定の処理は放置ですが、隔離、削除、および拡張子変更などの処理も指定できます。詳細については、22 ページの「暗号化ファイルとパスワード保護ファイルについて」および 23 ページの「検索不能ファイルについて」を参照してください。

指定可能な処理

検索の種類	PortalProtect で実行する処理
[Security Risk Scan] (リアルタイム)	駆除、ブロック、または放置 (Clean/Block/Pass)
[File Blocking] (リアルタイム)	ブロックまたは放置 (Block/Pass)
[Content Filtering] (リアルタイム)	ブロックまたは放置 (Block/Pass)
[Web Reputation] (リアルタイム)	ブロックまたは放置 (Block/Pass)
[Data Loss Prevention] (リアルタイム)	ブロックまたは放置 (Block/Pass)
[Manual Scan] > [Security Risk]	駆除、隔離、削除、放置、または拡張子変更 (Clean/Quarantine/Delete/Pass/Rename)
[Manual Scan] > [File Blocking]	隔離、削除、または放置 (Quarantine/Delete/Pass)
[Manual Scan] > [Content Filtering]	隔離、削除、または放置 (Quarantine/Delete/Pass)
[Manual Scan] > [Data Loss Prevention]	隔離、削除、または放置 (Quarantine/Delete/Pass)
[Scheduled Scan] > [Security Risk]	駆除、隔離、削除、放置、または拡張子変更 (Clean/Quarantine/Delete/Pass/Rename)
[Scheduled Scan] > [File Blocking]	隔離、削除、または放置 (Quarantine/Delete/Pass)

[Scheduled Scan] > [Content Filtering]	隔離、削除、または放置 (Quarantine/Delete/Pass)
[Scheduled Scan] > [Data Loss Prevention]	隔離、削除、または放置 (Quarantine/Delete/Pass)

カスタム処理を使用する場合は、それぞれの脅威について検出時の処理を設定できます。PortalProtect で脅威が検出されると、その脅威に関連付けられた処理が自動的に実行されます。PortalProtect が実行するすべての検索処理は、ウイルスログに記録されます。

ウイルスの検出時の処理には次のものがあります。

- 駆除 (Clean) — 感染ファイルからウイルスコードを削除します。ファイルからウイルスを駆除できない場合は、指定された二次処理が実行されます。ウイルスに対しては、初期設定の検出時の処理である駆除を使用することをお勧めします。PortalProtect がファイルからウイルスを駆除できなかった場合に実行する二次処理を選択します。初期設定の二次処理は隔離です。手動検索または予約検索の実行時、PortalProtect はデータベースをアップデートして、ドキュメントのコンテンツを駆除されたものに置き換えます。

注意

駆除処理は、その他の脅威や圧縮されたファイルには使用できません。

- 削除 (Delete) — ファイルを削除してログにイベントを記録します。
- 隔離 (Quarantine) — PortalProtect データベースにファイルを移動することで、そのファイルを SharePoint 環境からセキュリティリスクとして削除します。
- 拡張子変更 (Rename) — ファイル名はそのままで拡張子を `.vir` に変更し、ファイルが開いたり実行されたりしないようにします。たとえば、`virus.exe` というファイル名は `virus.exe.vir` に変更されます。

  リアルタイム検索の実行時、PortalProtect では拡張子変更されたファイルを SharePoint サーバに配置できます。
- ブロック (Block) — そのファイルの SharePoint サーバへのアクセスがブロックされ、ログにイベントが記録されます。

- 放置 (Pass) — ウイルスログにウイルス感染や不正ファイルの情報を記録しますが、そのファイルに対しては処理を行いません。

注意

PortalProtect では、あるファイルの検出時の処理を後から変更しても、そのファイルのダウンロード時には、以前に指定した処理が実行されます。最初に指定した検出時の処理でファイルを検索し、その後、処理を別の値に変更しても、ファイルが PortalProtect に送信されて再検索されることはありません。たとえば、検出時の処理を「放置」から「駆除」に変更してファイルをダウンロードした場合、そのファイルに対する処理は「駆除」でなく「放置」になります。

マクロウイルスについて

マクロウイルスはアプリケーション固有のウイルスです。マクロウイルスは、Microsoft Word (.doc) や Microsoft Excel (.xls) などのアプリケーションで動作するマクロユーティリティに感染します。そのため、これらのウイルスは、マクロの実行が可能なアプリケーションに共通の拡張子 (.doc、.xls、および.ppt など) を持つファイルで検出されます。マクロウイルスは、対象アプリケーションのデータファイル間で広まり、最終的には大量のファイルに感染する可能性があります。

暗号化ファイルとパスワード保護ファイルについて

PortalProtect ではこれらのファイルタイプを検索しない代わりに、これらのファイルタイプが SharePoint サーバの脅威にならないように防御する処理を実行します。PortalProtect が実行する処理は設定に応じて異なります。初期設定の処理は放置ですが、隔離、削除、および拡張子変更などの処理も指定できます。

表 1-1. 暗号化ファイルとパスワード保護ファイルに対する検出時の処理

検索の種類	PortalProtect で実行する処理
リアルタイム検索 (Real-time)	ブロックまたは放置 (Block/Pass)
手動検索 (Manual Scan)	隔離、放置、削除、または拡張子変更 (Quarantine/Pass/Delete/Rename)

予約検索 (Scheduled Scan)	隔離、放置、削除、または拡張子変更 (Quarantine/Pass/Delete/Rename)

注意

PortalProtect が暗号化ファイル、パスワード保護ファイル、および検索不能ファイルを隔離すると、ファイルがウイルス感染したことが SharePoint Server に報告されます。場合によっては、実際には感染していないにも関わらず、感染されたと報告されることがあります。そのため、定期的に隔離ログを確認して、誤検出されたファイルがないかどうか調べることをお勧めします。

検索不能ファイルについて

PortalProtect では、1GB を超えるファイルなど一部のファイルタイプを検索できません。代わりに、これらのファイルが SharePoint サーバの脅威にならないように防御する処理を実行します。PortalProtect が実行する処理は設定に応じて異なります。初期設定は放置ですが、隔離、削除、および拡張子変更などの処理も指定できます。

表 1-2. 検索不能ファイルに対する検出時の処理

検索の種類	PortalProtect で実行する処理
リアルタイム検索 (Real-time)	ブロックまたは放置 (Block/Pass)
手動検索 (Manual Scan)	隔離、放置、削除、または拡張子変更 (Quarantine/Pass/Delete/Rename)
予約検索 (Scheduled Scan)	隔離、放置、削除、または拡張子変更 (Quarantine/Pass/Delete/Rename)

圧縮ファイルの検索

PortalProtect では、検索オプションの設定に従って圧縮ファイルを検索およびブロックできます。PortalProtect でウイルスが検出されると、ファイルをブロックするか、事前設定された処理が実行されします。

注意

圧縮階層が 1 より大きい場合、PortalProtect ではウイルスを駆除できません。ただし、圧縮ファイルをブロックして隔離する、または検索して削除するように PortalProtect を設定できます。

圧縮およびアーカイブはファイルを格納するための最も一般的な方法です。特にメールの添付ファイル、FTP、および HTTP などのファイル転送でよく使用されます。圧縮ファイルのウイルスを検出するには、まず圧縮ファイルを解凍する必要があります。

PortalProtect は現在、次の圧縮タイプをサポートしています。

- 抽出方式 — 複数のファイルが 1 つのファイルに圧縮またはアーカイブされている場合に使用します。PKZIP、LHA、LZH、ARJ、MIME、MSCF、TAR、GZIP、BZIP2、RAR、AMG、ACE
- 展開方式 — 1 つのファイルが 1 つのファイルに圧縮またはアーカイブされている場合に使用します。PKLITE、PKLITE32、LZEXE、DIET、ASPACK、UPX、MSCOMP、LZW、MACBIN、Petite、PEPack、WWPack
- デコード方式 — ファイルがバイナリから ASCII へ変換されている場合に使用します。この方式は、メールシステムで広く採用されています。UUCODE および BINHEX

その他の圧縮ファイルタイプについては、圧縮ファイルに含まれる個々のファイルではなく、圧縮ファイル全体を検索します。

第 2 章

基本設定

本章では、PortalProtect の使用を開始して SharePoint 環境を保護するために必要な基本事項について説明します。さらに、ヘルプの参照方法や、PortalProtect の使用開始時に実行する必要がある作業について説明します。この作業を完了すれば、PortalProtect の機能を最大限活用できるようになります。

本章の内容は次のとおりです。

PortalProtect の Web 管理コンソールの表示

PortalProtect は、直観的な操作が可能な Web 管理コンソールからアクセスおよび制御できます。Web 管理コンソールは、Internet Explorer 7.0 SP1 以上を実行するネットワーク上の任意のコンピュータで表示できます。

手順

1. デスクトップ上の PortalProetct 管理コンソールのショートカットをクリックします。
2. [スタート] > [プログラム] > [Trend Micro PortalProtect for Microsoft SharePoint] > [PortalProtect Management Console] の順に選択します。

   Web 管理コンソールが表示されます。
3. 次のいずれかを実行します。
   - ローカルサーバの Web 管理コンソールを表示するには

     次の URL をアドレスボックスに入力します。

     `https://<ローカルホスト>:<ポートナンバー>/PortalProtect/Login.htm`

     注意

     ポート番号は、インストール時のユーザの入力によって異なります。初期設定のポートは 16373 です。インストール時には SSL が有効になっており、http プロトコルの選択肢はありません。
   - リモートサーバの Web 管理コンソールを表示するには

     Internet Explorer を使用して次の URL にアクセスします。

     `https://[サーバ名]:[サーバポート]/PortalProtect/Login.htm`

     「サーバ名」は、PortalProtect がインストールされたサーバの名前です。「サーバポート」は、そのコンピュータへのアクセスに使用するポート番号です。

主要な要素

Web 管理コンソールは、次の主要な要素で構成されています。

- PortalProtect バナーは、常時画面の上部に表示されています。バナーにはドロップダウンリストがあり、オンラインサポートへのアクセスに使用できます。バナーを使用してログオフすることもできます。
- サイドバーは、管理コンソールの左側にあるメニューです。PortalProtect のすべての設定にすばやくアクセスできます。
- メインの表示領域では、PortalProtect の各種オプションを表示および設定できます。
- メインの表示領域にある画面タブは、各種トピックおよびオプションへアクセスするために使用します。
- ヘルプアイコンは、状況に依存したヘルプや、各種機能についてのポップアップ情報を表示するために使用します。

ログオンとログオフ

ログオン

設定を行うには、PortalProtect にログオンする必要があります。PortalProtect の管理者にログオンを要求することで、さらに保護を強化しています。

ログオフ

Web 管理コンソールのバナーで [Log Off] をクリックしてログオフします。

PortalProtect のアクティベート

PortalProtect の利点を最大限活用するには、製品版をアクティベートする必要があります。これにより、最新の検索エンジンとウイルスパターンファイルのアップデートのダウンロードが可能になります。さらに、アップグレードや HotFix をダウンロードすることもできます。これらの主要コンポーネントがなければ、SharePoint 環境は、新しく出現したウイルスの攻撃から保護されません。

PortalProtect には、2 種類のアクティベーションコード (AC) があります。

バージョン 2.0 以前の PortalProtect の AC を使用時には、PortalProtect のセキュリティリスク検索、ファイルブロック、コンテンツフィルタ、および Web レピュテーションがアクティベートされます。情報漏えい対策機能を使用するには専用の AC が必要ですので、お買い上げの販売店にお問い合わせください。

購入した製品に同梱されているアクティベーションコードを使用して、インストール時に PortalProtect をアクティベートします。

注意

体験版のアクティベーションコードを使用する場合は、30 日間に限り PortalProtect を使用できます。体験期間終了後は、PortalProtect を使用することはできません。体験版を製品版にアップグレードするには、トレンドマイクロの営業部、またはライセンスを受けた販売代理店に連絡して新しいアクティベーションコードを取得してください。

製品版をアクティベートすると次の利点が提供されます。

- PortalProtect の製品版の機能。最新の検索エンジンとサポート契約期間内におけるウイルスパターンファイルのアップデートが可能になり、トレンドマイクロのアップデートサーバを使用することができます。
- サポート契約の範囲内でのトレンドマイクロのサポートサービス

新しいアクティベーションコードを取得するには

- アクティベーションコードが期限切れになった場合は、トレンドマイクロの販売代理店に連絡してサポート契約を更新してください。

管理コンソールから製品版をアクティベートするには

1. サイドバーで、[Administration] > [Product License] の順にクリックします。

   [Product License] 画面が表示されます。

2. [Enter New Activation Code] をクリックします。
3. 新しいアクティベーションコードを該当するフィールドに入力します。
4. [Activate] をクリックします。

PortalProtect のアップデート

新しいウイルスや不正コードは常に拡散されているため、新しいセキュリティの脅威から環境を保護するには、検索エンジンとパターンファイルを定期的にアップデートすることが重要です。

PortalProtect をアップデートできるようにするには、次の作業を完了する必要があります。

- 使用環境のネットワークでインターネットトラフィックをプロキシサーバが処理している場合は、プロキシサーバの情報を入力する必要があります。30 ページの「グローバルプロキシサーバ」参照。
- アップデート方法とアップデート元を設定します。アップデート方法には手動アップデートと予約アップデートがあります。アップデート元には、トレンドマイクロのアップデートサーバ、その他のアップデート元、およびイントラネットの UNC パスがあります。

注意

管理コンソールには、[ActiveUpdate server]、[UNC path]、および [Other Update source] の 3 つのオプションがあります。

ダウンロード元の選択

コンポーネントを最初にアップデートするときには、ダウンロード元を選択する必要があります。

重要

[Download Source] メニューは、アップデートサーバ以外のダウンロード元が設定されている古いバージョンから PortalProtect をアップグレードする場合にのみ使用できます。PortalProtect の新規インストールでは、[Download Source] メニューは使用できません。

手順

1. [Updates] > [Download Source] の順にクリックして、ダウンロード元を選択します。

[Download Source] 画面が表示されます。

- Trend Micro ActiveUpdate server — トレンドマイクロで新しいコンポーネントが準備されると、アップデート機能によってただちにダウンロードされます。適切なタイミングでの頻繁なアップデートが必要な場合には、アップデート元にトレンドマイクロのアップデートサーバを選択してください。
- Intranet location containing a copy of the current file — ネットワークの他のサーバの Universal Naming Convention (UNC) パスを入力します。ユーザ名とパスワードが要求されたら、[User name] と [Password] に入力します。
- Other Update Source — 最新のコンポーネントを受信するインターネットのダウンロード元からコンポーネントをダウンロードします。

2. 同じローカルネットワークの他のサーバからアクセスできる 1 つのサーバにコンポーネントパッケージを作成するには、[Allow other servers to download updates from this server...] を選択します。

注意

選択時には、他のサーバから次の URL を使用してパッケージをダウンロードできます。

https://<サーバ IP>:<ポート>/PortalProtect/Activeupdate

3. [Save] をクリックします。

すべてのダウンロード設定を初期設定値に変更するには、[Reset] をクリックします。

グローバルプロキシサーバ

多くの企業では、セキュリティの強化と帯域幅の使用効率向上のためにプロキシサーバを使用しています。PortalProtect でプロキシサーバを使用している場合は、インターネットへ接続するようにプロキシサーバを設定して、PortalProtect の最新状態を維持するために必要なコンポーネントのダウンロードや、オンラインでのライセンスのステータス確認などを行います。

次の機能はプロキシサーバを使用します。

- アップデート
- Web レピュテーションフィルタ

手順

1. PortalProtect の Web 管理コンソールを開きます。
2. サイドバーで、[Administration] > [Proxy] の順にクリックします。

   [Proxy Settings] 画面が表示されます。
3. Web レピュテーション、アップデート、および製品ラインセンスの通知に対して [Use a proxy server] を選択します。
4. 次の情報を入力してプロキシサーバを設定します。
   - サーバ名または IP アドレス
   - ポート
   - SOCKS 5 プロキシプロトコルを使用するかどうかの選択
5. プロキシサーバがパスワードを要求する場合には、[Proxy Authentication] で次の情報を該当するフィールドに入力します。
   - ユーザ名
   - パスワード
6. [Save] をクリックして、設定を保存します。

コンポーネントの手動アップデート

PortalProtect のインストール直後や、ウイルスの大規模感染発生時には、ただちにコンポーネントを手動でアップデートすることをお勧めします。これにより、SharePoint 環境のセキュリティの基盤を確立できます。

注意

コンポーネントを最初にアップデートするときは、アップデートの前に [Download Source] を選択してください。29 ページの「ダウンロード元の選択」を参照してください。

手順

1. 左側のメニューで、[Updates] > [Manual] の順にクリックします。

   [Manual Update] 画面が表示されます。

2. アップデートするコンポーネントのチェックボックスをオンにします。
3. [Update] をクリックします。

   PortalProtect がアップデートを開始します。

注意

すべてのダウンロード設定を初期設定値に変更するには、[Reset] をクリックします。

予約アップデートの設定

アップデートサーバを定期的に確認し、利用可能なアップデートを自動的にダウンロードするように設定します。この強力な機能によって、PortalProtect とすべてのコンポーネットは最新状態が維持され、最小限の操作で最上の保護状態を実現できます。

注意

コンポーネントを最初にアップデートするときは、アップデートの前に [Download Source] を選択してください。29 ページの「ダウンロード元の選択」を参照してください。

ヒント

ウイルスパターンファイルは定期的にアップデートされます。ウイルスの大規模感染が発生している場合は、1 日に数回アップデートされることもあります。PortalProtect のコンポーネントが最新バージョンになるように、少なくとも 1 日に 1 回アップデートを実行してください。

手順

1. 左側のメニューで、[Updates] > [Scheduled] の順にクリックします。

   [Scheduled Update] 画面が表示されます。

2. [Enable scheduled updates] を選択します。
3. アップデートするコンポーネントのチェックボックスをオンにします。
4. [Update Schedule] で、[Minute(s)]、[Hour(s)]、[Day(s)]、[Weekly] のいずれかのアップデート頻度のオプションを選択します。
5. ドロップダウンを使用して適切な開始予定を選択します。
6. [Save] をクリックします。

注意

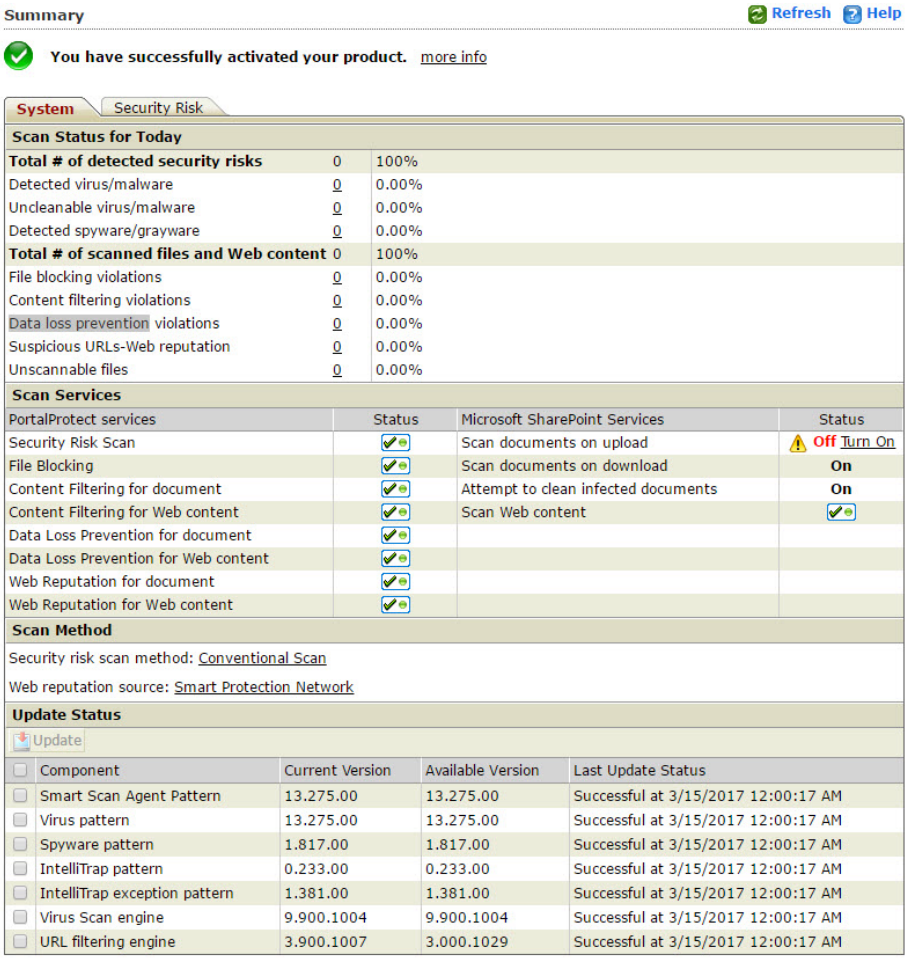
すべてのダウンロード設定を初期設定値に変更するには、[Reset] をクリックします。

PortalProtect の管理

ここでは、PortalProtect のさまざまな管理機能について説明します。

Summary 画面

PortalProtect の [Summary] 画面には、[System] と [Security Risk] の 2 つのタブがあります。ここでは、これらのタブにある機能と表示について簡単に説明します。



Summary

Refresh Help

You have successfully activated your product. more info

System | Security Risk

Scan Status for Today

Total # of detected security risks	0	100%
Detected virus/malware	0	0.00%
Uncleanable virus/malware	0	0.00%
Detected spyware/grayware	0	0.00%
Total # of scanned files and Web content	0	100%
File blocking violations	0	0.00%
Content filtering violations	0	0.00%
Data loss prevention violations	0	0.00%
Suspicious URLs-Web reputation	0	0.00%
Unscannable files	0	0.00%

Scan Services

PortalProtect services	Status	Microsoft SharePoint Services	Status
Security Risk Scan	✓	Scan documents on upload	Off Turn On
File Blocking	✓	Scan documents on download	On
Content Filtering for document	✓	Attempt to clean infected documents	On
Content Filtering for Web content	✓	Scan Web content	✓
Data Loss Prevention for document	✓		
Data Loss Prevention for Web content	✓		
Web Reputation for document	✓		
Web Reputation for Web content	✓		

Scan Method

Security risk scan method: Conventional Scan

Web reputation source: Smart Protection Network

Update Status

Update

Component	Current Version	Available Version	Last Update Status
Smart Scan Agent Pattern	13.275.00	13.275.00	Successful at 3/15/2017 12:00:17 AM
Virus pattern	13.275.00	13.275.00	Successful at 3/15/2017 12:00:17 AM
Spyware pattern	1.817.00	1.817.00	Successful at 3/15/2017 12:00:17 AM
IntelliTrap pattern	0.233.00	0.233.00	Successful at 3/15/2017 12:00:17 AM
IntelliTrap exception pattern	1.381.00	1.381.00	Successful at 3/15/2017 12:00:17 AM
Virus Scan engine	9.900.1004	9.900.1004	Successful at 3/15/2017 12:00:17 AM
URL filtering engine	3.900.1007	3.000.1029	Successful at 3/15/2017 12:00:17 AM

Scan Status for Today

- Total # of detected security risks — 今日検出されたセキュリティリスクの合計数が表示されます。

  Detected virus/malware — ウイルス/不正プログラムの検出数です。表示されるのは、ウイルス/不正プログラムの種類の数ではなく、今日 PortalProtect によって検出されたウイルス/不正プログラムの総数になります。この値とともに、ファイルと Web コンテンツについて検出されたセキュリティリスクの総数に対するこの検出数の比率が表示されます。数値のリンクをクリックすると、ログのクエリが実行され、ログが表示されます。

  Uncleanable virus/malware — 今日検出され駆除できなかったウイルス/不正プログラムの総数と、ファイルと Web コンテンツについて検出されたセキュリティリスクの総数に対するこの検出数の比率が表示されます。数値のリンクをクリックすると、ログのクエリが実行され、ログが表示されます。

  Detected spyware/grayware — 今日検出されたスパイウェア/グレーウェアの総数と、ファイルと Web コンテンツについて検出されたセキュリティリスクの総数に対するこの検出数の比率が表示されます。数値のリンクをクリックすると、ログのクエリが実行され、ログが表示されます。

- Total # of scanned files and Web content — 検索されたファイルと Web コンテンツの総数が表示されます。

  File blocking violations — 今日検出されたファイルブロック違反の総数と、ファイルと Web コンテンツの合計検索数に対するこの検出数の比率が表示されます。数値のリンクをクリックすると、ログのクエリが実行され、ログが表示されます。

  Content filtering violations — 今日検出されたコンテンツフィルタポリシー違反の総数と、ファイルと Web コンテンツの合計検索数に対するこの検出数の比率が表示されます。数値のリンクをクリックすると、ログのクエリが実行され、ログが表示されます。

  Data loss prevention violations — 今日検出された情報漏えい対策違反の総数と、ファイルと Web コンテンツの合計検索数に対するこの検出数の比率が表示されます。数値のリンクをクリックすると、ログのクエリが実行され、ログが表示されます。

Suspicious URLs Web reputation — 今日 Web レピュテーションによって検出された疑わしい URL の総数と、ファイルと Web コンテンツの合計検索数に対するこの検出数の比率が表示されます。数値のリンクをクリックすると、ログのクエリが実行され、ログが表示されます。

Unscannable files — 今日検出された検索不能なファイルの総数と、ファイルと Web コンテンツの合計検索数に対するこの検出数の比率が表示されます。数値のリンクをクリックすると、ログのクエリが実行され、ログが表示されます。

Scan Services — PortalProtect services

- Security Risk Scan — [Status] 列のアイコンをクリックして、セキュリティリスク検索を有効または無効にします。
- File Blocking — [Status] 列のアイコンをクリックして、ファイルブロックを有効または無効にします。
- Content Filtering for document — [Status] 列のアイコンをクリックして、ドキュメントのコンテンツフィルタを 有効または無効にします。
- Content Filtering for Web content — [Status] 列のアイコンをクリックして、Web コンテンツのコンテンツフィルタを 有効または無効にします。
- Data Loss Prevention for document — [Status] 列のアイコンをクリックして、ドキュメントの情報漏えい対策を有効または無効にします。
- Data protection for Web content — [Status] 列のアイコンをクリックして、Web コンテンツの情報漏えい対策を有効または無効にします。
- Web Reputation for document — [Status] 列のアイコンをクリックして、ドキュメントの Web レピュテーションを有効または無効にします。
- Web Reputation for Web content — [Status] 列のアイコンをクリックして、Web コンテンツの Web レピュテーションを有効または無効にします。

注意

緑色のチェックマークはサービスが有効であることを示し、赤い「×」はサービスが無効であることを示します。

Scan Services — Microsoft SharePoint Services

注意

[Turn On] リンクをクリックして [Central Administration] > [Security] > [Antivirus] ウィンドウを開くと、このオプションを有効または無効にするよう選択できます。[OK] をクリックしてウィンドウを閉じ、[Summary] ページの表示を更新して、設定が更新されたことを確認します。

- Scan documents on upload: このサービスを有効にすると、[Status] 列に [On] と表示され、無効にすると感嘆符、[Off]、および [Turn On] リンクが表示されます。
- Scan documents on download: このサービスを有効にすると、[Status] 列に [On] と表示され、無効にすると感嘆符、[Off]、および [Turn On] リンクが表示されます。
- Attempt to clean infected documents: このサービスを有効にすると、[Status] 列に [On] と表示され、無効にすると感嘆符、[Off]、および [Turn On] リンクが表示されます。
- Scan Web content: [Status] 列のアイコンをクリックして、Web コンテンツの検索を有効または無効にします。緑色のチェックマークはサービスが有効であることを示し、赤い「×」はサービスが無効であることを示します。

Scan Method

- Security Risk Scan Method: Conventional Scan — リンクをクリックすると、従来型スキャンまたはスマートスキャンを選択して設定できます。62 ページの「セキュリティリスク検索方法の選択」を参照してください。
- Web Reputation Source: Smart Protection Network — リンクをクリックすると、グローバル (外部ネットワーク) の Trend Micro Smart Protection Network またはローカル (社内ネットワーク) の Smart Protection Server からの検索を選択して設定できます。62 ページの「セキュリティリスク検索方法の選択」を参照してください。

Smart Scan Server

注意

このセクションはスマートスキャンオプションを選択した場合にのみ次の項目とともに表示されます。

- Smart Protection Service — サーバにセキュリティリスク検索と Web レピュテーションを組み込みます。
- Server Name: PortalProtect の検索要求を処理するスマートスキャンサーバの名前です。
- Service Status: このサーバのスマートスキャンサービスのステータスが表示されます。
- Console — リンクをクリックすると、このスマートスキャンサーバの Web コンソールにアクセスできます。

Update Status

次のコンポーネントについて、[Current Version] 列に現在のバージョン、[Available Version] 列に利用可能なバージョン、および [Last Update Status] 列に前回のアップデートステータスが表示されます。(複数の) コンポーネントを選択して [Update] をクリックすると、手動でアップデートするか、すべての履歴を示したアップデートログをクエリできます。

- Smart Scan Agent Pattern
- Virus pattern
- Spyware pattern
- IntelliTrap pattern
- IntelliTrap exception pattern
- Virus scan engine
- URL filtering engine

リアルタイムモニタについて

リアルタイムモニタには、現在の PortalProtect サーバの情報がリアルタイムに表示されます。PortalProtect が検索するコンテンツがアップロードまたは投稿されるたびに表示されます。また、サーバで検出されたウイルス/不正プログラム、スパイウェア/グレーウェア、および疑わしい URL の現在の数も表示されます。

リアルタイムモニタには、サーバに関する次の情報が表示されます。

画面の上部に表示されるグループ

- サーバ名 ([Server name])
- スマートスキャンエージェントパターンファイル ([Smart Scan Agent Pattern])
- ウイルスパターンファイル ([Virus pattern])
- IntelliTrap パターンファイル ([IntelliTrap pattern])
- スパイウェアパターンファイル ([Spyware pattern])
- URL フィルタエンジン ([URL filtering engine])
- リアルタイム検索の実行開始日時: xxxx/xx/xx xx:xx:xx ([Real-time scan has been running since: xxxx/xx/xx xx:xx:xx])
- ウイルス検索エンジン ([Scan engine])
- IntelliTrap 除外パターンファイル ([IntelliTrap exception pattern])

[Scanning Status] グループ

- 検索済みファイルおよび Web コンテンツ ([Files and Web content scanned])
- 検出されたウイルス/不正プログラム ([Virus/Malware found])
- 検出されたスパイウェア/グレーウェア ([Spyware/Grayware found])
- 駆除できないウイルス ([Uncleanable viruses])
- ファイルブロック違反 ([File Blocking violation])
- コンテンツフィルタ 違反 ([Content filtering violation])

- 検出された疑わしい URL - Web レピュテーション ([Detected suspicious URLs - Web Reputation])
- 情報漏えい対策 ([Data loss prevention])

リアルタイムモニタで使用可能なオプションは次のとおりです。

- Reset Count — [Scanning Status] のカウントをすべてゼロにリセットし、[Scanned Contents] のリストもクリアします。
- Clear Content — [Scanned Contents] のリストをクリアします。
- Close — 画面を閉じます。

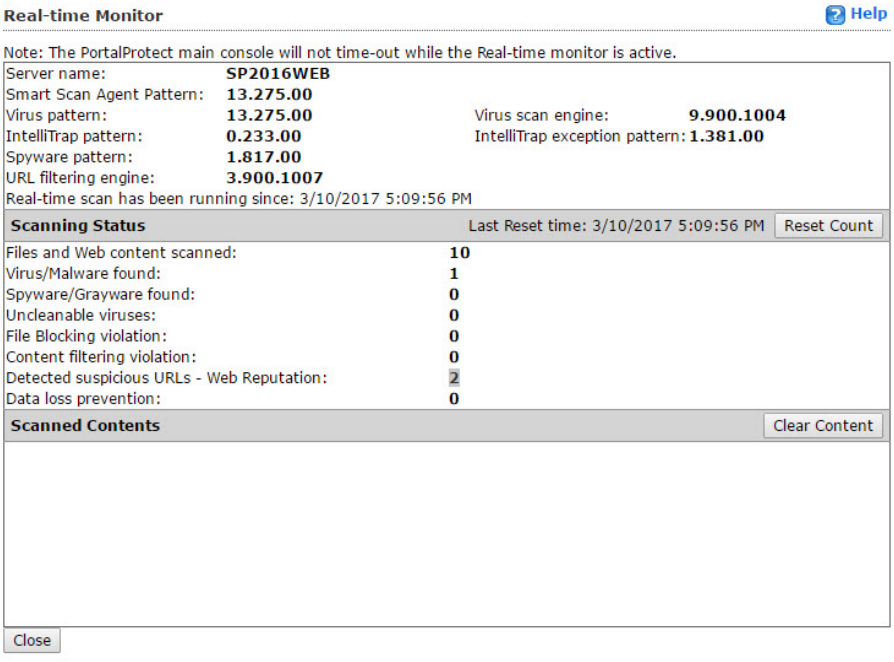


図 2-1. リアルタイムモニタ画面

リアルタイムモニタを表示するには

1. PortalProtect 製品コンソールを開きます。

2. 画面の上部の [Real-time monitor] リンクをクリックします。

サーバ管理コンソールについて

サーバ管理では、情報をクエリする機能や、すべての PortalProtect サーバの設定をファームに複製する機能を利用できます。サーバ管理コンソールには、エンジン/パターンファイルのバージョン、検索ステータス、検索結果、および前回の複製に関する情報が表示されます。

次に、使用可能なオプションについての簡単な説明を示します。

[Query] タブ

次の最新情報が表示されます。

- Pattern and engine version — 各サーバの現在のパターンファイル/エンジンが表示されます。
- Scanning status — セキュリティリスク検索、ファイルブロック、ファイルのコンテンツフィルタ、Web コンテンツのコンテンツフィルタ、ファイルの情報漏えい対策、Web コンテンツの情報漏えい対策、ファイルの Web レピュテーション、および Web コンテンツの Web レピュテーションの検索ステータス ([On] または [Off]) が表示されます。
- Scanning result — 概要ページと同様の最新の検索結果が表示されます。
- Last replication — サーバ名、前回複製した日、ステータスなど、前回の複製に関連する情報が表示されます。

[Replication] タブ

ある PortalProtect サーバからファーム内の別のサーバに自動的に設定を複製できます。この処理を実行するには、画面の下部に表示される [Automatically replicate settings to other servers] を選択します。

注意

[All settings] と [Overwrite server-dependent settings (such as backup directories)] を選択した場合は、サーバに依存する設定が複製されます。[All settings] を選択し、[Overwrite server-dependent settings (such as backup directories)] をオフにした場合は、サーバに依存する設定は複製されません。

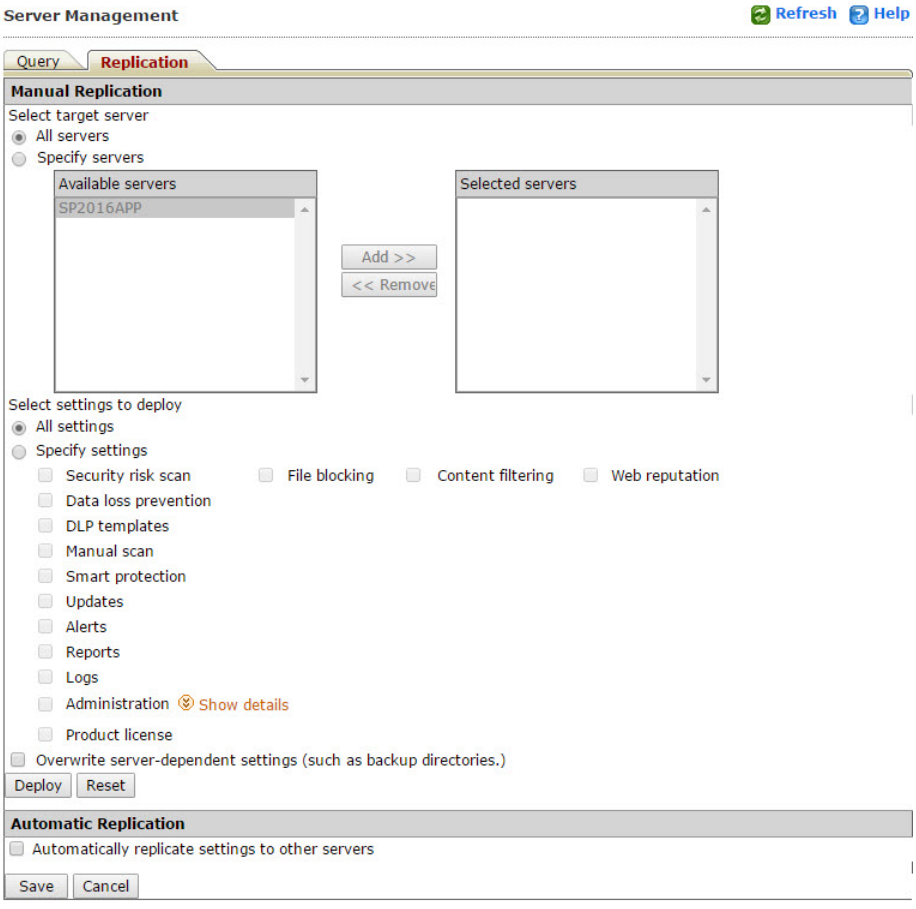


図 2-2. [Server Management] 画面の[Replication] タブ

使用可能なオプションは次のとおりです。

- Select target server

  1. All servers — コピー中のサーバを除く、ファーム内のすべてのサーバが対象となります。
  2. Specify servers — 複製を送信する特定の対象サーバを選択します。

- Select settings to deploy
  1. All Settings — 選択したサーバに、すべての設定が複製されます。
  2. Specify Settings — 複製する設定を次の設定から選択します。

注意

このオプションは、[Specify Setting] を選択した後にのみ使用可能になります。

- Security risk scan
- File blocking
- Content filtering
- Web reputation
- Data loss prevention
- DLP templates
- Manual scan
- Smart protection
- Updates
- Alerts
- Reports
- Logs
- Administration: [Proxy]、[Notification settings]、[Access control]、および [Control manager]
- Product license
- Overwrite server-dependent settings (such as backup directories): このオプションは、[Specify Settings] で [Security Risk Scan] または [Manual Scan] を選択した場合に有効になります。また、[All settings] を選択したときにも有効になります。

注意

[Real-time Security Risk Scan] および [Manual Scan for Security Risk Scan] のバックアップディレクトリは、サーバ依存設定を含みます。詳細については、52 ページの「処理を実行する前のファイルのバックアップ」を参照してください。

- Automatic Replication

  Automatically replicate settings to other servers: 設定を他のサーバに自動的に複製します。

第 3 章

検索とブロックの設定

本章では、PortalProtect の検索オプションとブロックオプションについて 説明します。PortalProtect には、SharePoint 環境で使用可能な以下の検索機能があります。

- リアルタイム検索
- 手動検索
- 予約検索

各検索オプションには、以下に対する独自の検索フィルタおよびブロックフィルタがあります。

- セキュリティリスク検索
- ファイルブロック
- コンテンツフィルタ
- Web レピュテーション
- 情報漏えい対策

より詳細なオプションを設定して、不正なマクロコードを検索したり、圧縮ファイルをブロックおよび検索したりすることもできます。

本章の内容は次のとおりです。

- 47 ページの「検索オプションの設定」
- 59 ページの「高度なマクロ検索について」

検索について

PortalProtect では、次の 3 種類の検索を実行できます。

- リアルタイム検索
- 手動検索
- 予約検索

SharePoint 環境を保護するため、PortalProtect は、コンテンツに対してセキュリティリスクおよび望ましくないデータの検索を行います。これらが検出されると、これらに対して設定された処理が自動的に実行されます。

PortalProtect では、特定の対象に対して検索を実行するよう設定したり、セキュリティリスクや望ましくないデータが検出された場合に実行する処理を指定したりすることができます。また、セキュリティリスクや望ましくないデータに対して処理を実行するときに通知を送信するように PortalProtect を設定することもできます。

さらに、PortalProtect でファイルを処理する前に、バックアップフォルダにファイルを保存するように設定できます。これは、元のファイルが破損しないようにするための予防措置です。

注意

トレンドマイクロでは、元のファイルに処理が実行された後、そのファイルが破損しておらず、使用可能であることを確認したら、バックアップファイルを削除することをお勧めします。ファイルが破損していたり使用できなくなった場合は、トレンドマイクロに送信して詳しい分析を依頼してください。PortalProtect によってウイルス自体が駆除され、削除されている場合でも、ウイルスによって元のファイルのコードが破壊され、修復できなくなることがあります。

検索オプションの設定

検索を指定してそのオプションを設定するには検索メニューを使用します。リアルタイム検索、手動検索、または予約検索を指定できます。さらに、それぞれの検索には異なるオプションを設定できます。検索オプションを設定して保存すると、PortalProtect は、その設定に基づいて検索を開始し、処理

を実行します。検索を無効にすると、設定を変更することなく検索を一時的に停止できます。49 ページの「セキュリティリスクのリアルタイム 検索の有効化と無効化」参照。

検索について

リアルタイム検索は、ファイルを SharePoint サーバに保存するとき (チェックイン)、または SharePoint サーバから取得するとき (チェックアウト) に実行されます。手動検索では SharePoint コンテンツデータベースが検索され、[ScanNow] を手動で選択するとただちに処理が開始されます。予約検索では手動検索と同じ機能が実行されますが、設定したスケジュールに従って検索が行われます。検索にかかる時間は、ファイル数やハードウェアのリソース数によって異なります。

SharePoint 環境のパフォーマンスを最適化するには、手動検索や予約検索をシステム使用率のピーク時間外に実行することをお勧めします。

注意

リアルタイム検索が有効で、さらに SharePoint でウイルス対策オプションの [ダウンロード時にドキュメントをスキャンする] および [アップロード時にドキュメントをスキャンする] が有効な場合、PortalProtect ではファイルのアップロード時に検索が実行され、ダウンロード時には実行されません。これらのファイルは検索済みであるため、ダウンロード時に再度検索されることはありません。これは、Microsoft SharePoint 側の制限によるものです。

ヒント

PortalProtect の管理コンソールを使用して検索を設定および実行する方法の詳細については、オンラインヘルプ (英語) を参照してください。

PortalProtect は、アップロードとダウンロードのどちらの場合も、すべてのコンテンツに対して検索を実行することで、SharePoint 環境を保護します。オンデマンド検索 (手動検索)、スケジュールに基づく検索 (予約検索)、または継続的/永続的な検索 (リアルタイム検索) を実行するよう、PortalProtect を設定できます。検索の設定は、[Security Risk Scan] 画面で行うこともできます。この画面には、サイドバーから、または [Manual Scan] 画面や [Scheduled Scan] 画面からアクセスできます。

注意

リアルタイム検索は、ユーザ操作を妨げることなく SharePoint 環境を保護します。リアルタイム検索を有効にすると、バックグラウンドで継続的にウイルス検索が実行されます。一度に設定できるリアルタイム検索は 1 つのみです。

警告!

リアルタイム検索機能は常に有効にしておくことをお勧めします。リアルタイム検索機能を無効にする必要がある場合は、必ず定期的に手動検索を実行してください。

セキュリティリスクのリアルタイム検索の有効化と無効化

セキュリティリスクのリアルタイム検索を有効にすると、ポータル環境のバックグラウンドで継続的に検索が実行されます。同様に、予約検索が設定されたスケジュールに従って自動的に実行されます。リアルタイム検索と予約検索は、検索設定を変更することなく無効にできます。リアルタイム検索を再開させたい場合は、単純に検索を有効に戻します。

注意

リアルタイム検索を無効にすると、バックグラウンド検索やファイルブロックが実行されず、ポータル環境がウイルスの感染に対して脆弱になります。予約検索を無効にすると、SQL コンテンツストアの検索とブロックが実行されません。これにより、SharePoint サーバに保存されている感染ファイルに対してシステムが脆弱になります。

Smart Protection ソース

Smart Protection ソースのオプションにより、個人の要件に応じてスマートスキャンサーバを追加、削除、インポート、およびエクスポートできます。ここでは、使用可能なさまざまなオプションや設定、およびそれらの設定方法について説明します。

Smart Protection Server が使用不能になった場合、PortalProtect はファイル検索のためにローカル (社内ネットワーク) のウイルスパターンファイルをロードします。Smart Protection が再度利用可能になると、PortalProtect は自

動的にローカル (社内ネットワーク) のウイルスパターンファイルをアンロードし、スマートスキャンパターンファイルをロードして、Smart Protection Server によるファイルの検索を継続します。Smart Protection Server が使用可能または使用不能になるたびに、メール警告を送信するようにシステムを設定できます。詳細については、234 ページの「システムイベント」を参照してください。

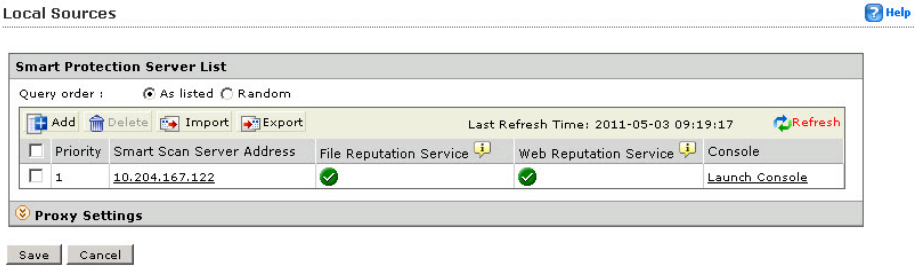


図 3-1. [Local Sources] 画面

Smart Protection ソースの設定

手順

1. [Smart Protection] > [Local Sources] をクリックします。[Local Sources] 画面が表示されます。
2. Smart Protection Server を追加するには、次の手順を実行します。

   [Import] をクリックしてサーバのリストをインポートするか、[Export] をクリックしてエクスポートします。

   a. [Add] をクリックします。[Add Smart Protection Server] 画面が表示されます。

   b. 次の情報を入力します。

      - サーバ名またはアドレス
      - ファイルレピュテーションのサービスポート
      - SSL

- Web レピュテーションのサービスポート

c. [File] または [Web Reputation] テストボタンのいずれかをクリックして、接続をテストします。

3. [Add] をクリックして設定を完了し、保存します。

注意

複数の Smart Protection Server を登録している場合は、PortalProtect がクエリを実行する順序を選択できます。[As listed] の場合、表示されている優先順位に従ってクエリが実行されます。[Random] の場合、リスト内のサーバに対してランダムにクエリが実行されます。システムから Smart Protection Server に接続できない場合は、選択したクエリの順序に従って次のサーバに接続が試行されます。

4. 次の手順で、ローカル Smart Protection ネットワークのプロキシサーバを追加または編集します。

a. [Local Sources] 画面で、[Proxy Settings] の横のアイコンをクリックして内容を展開表示します。

b. [Use a proxy server for PortalProtect and Local Smart Protection Server communication] を選択します。

c. [Server name or IP address] フィールドに IP アドレスまたはサーバ名を入力します。

d. [Port] フィールドにポート番号を入力します。

e. 必要に応じて [User ID] にユーザ ID を入力します。

f. 必要に応じて [Password] にパスワードを入力します。

g. [Save] をクリックします。

注意

このプロキシ設定は、ローカル (社内ネットワーク) の Smart Protection Server のみに影響し、[Administration] > [Proxy] に表示されるグローバルプロキシサーバの設定には影響しません。

処理を実行する前のファイルのバックアップ

PortalProtect でファイルを処理する前に、そのバックアップファイルをバックアップフォルダに作成するように設定できます。これは、元のファイルが破損しないようにするための予防措置です。

バックアップファイルは、処理の実行後、変更されたファイルが使用可能で破損していないことを確認したら、ただちに削除する必要があります。ファイルが破損していたり使用できなくなった場合は、トレンドマイクロに送信して詳しい分析を依頼してください。PortalProtect でウイルスを駆除および削除できても、ウイルスによってファイルコードが修復不能なほど破壊されている場合があるので注意してください。

バックアップフォルダの 場所の設定方法については、次を参照してください。

52 ページの「セキュリティリスク検索のバックアップフォルダの 指定」

54 ページの「手動検索のバックアップフォルダの 指定」

57 ページの「予約検索のバックアップフォルダの 指定」

セキュリティリスク検索のバックアップフォルダの指定

セキュリティリスク検索のバックアップフォルダを 指定するために必要な手順を説明します。

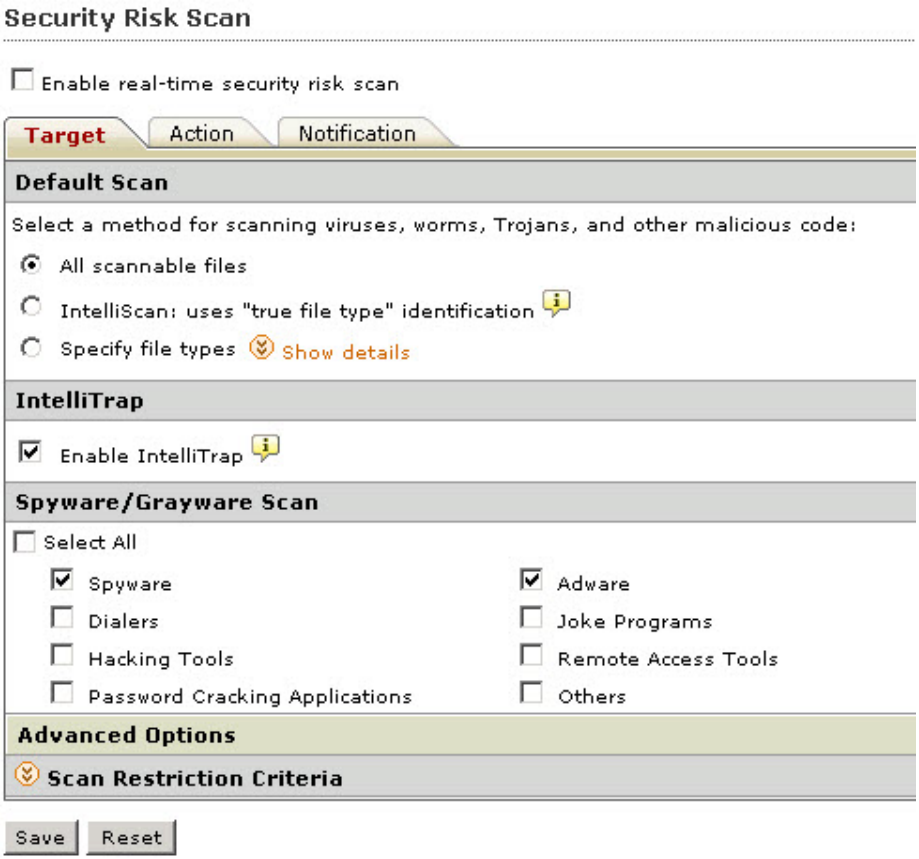


図 3-2. [Security Risk Scan] 画面 ([Target] タブ)

手順

1. 左側のメニューで、[Security Risk Scan] をクリックします。[Security Risk Scan] 画面が表示されます。
2. [Action] タブをクリックし、画面下部の [Backup Setting] を展開します。

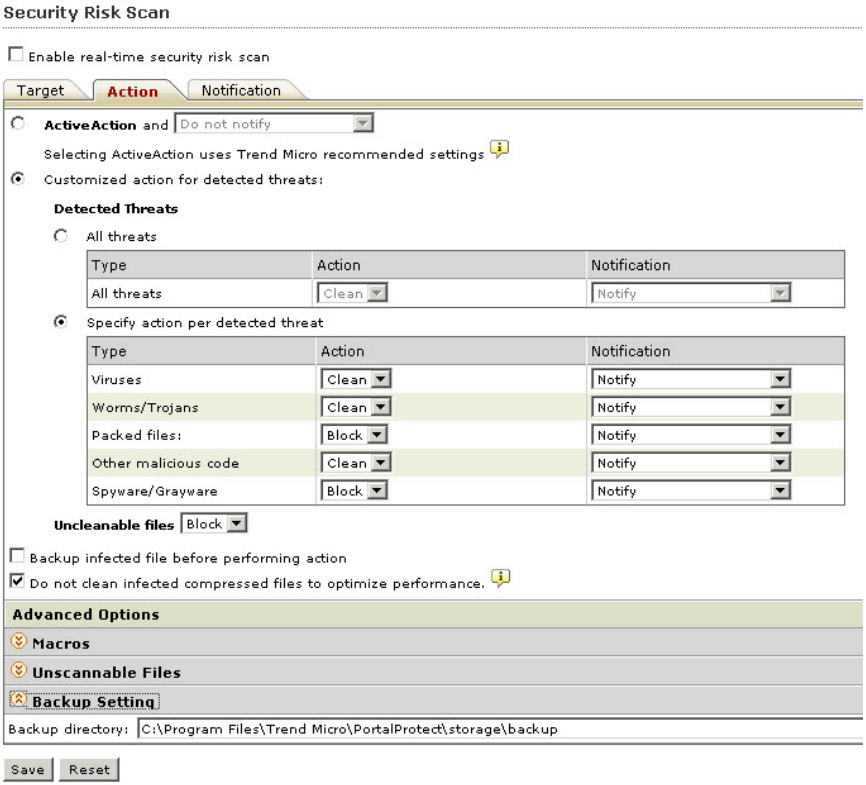


図 3-3. Security Risk Scan ([Action] タブ)

3. [Backup directory] に、バックアップファイルの保存先のフルパスを入力します。ディレクトリパスが存在しない場合は、指定したパスにフォルダが作成されます。

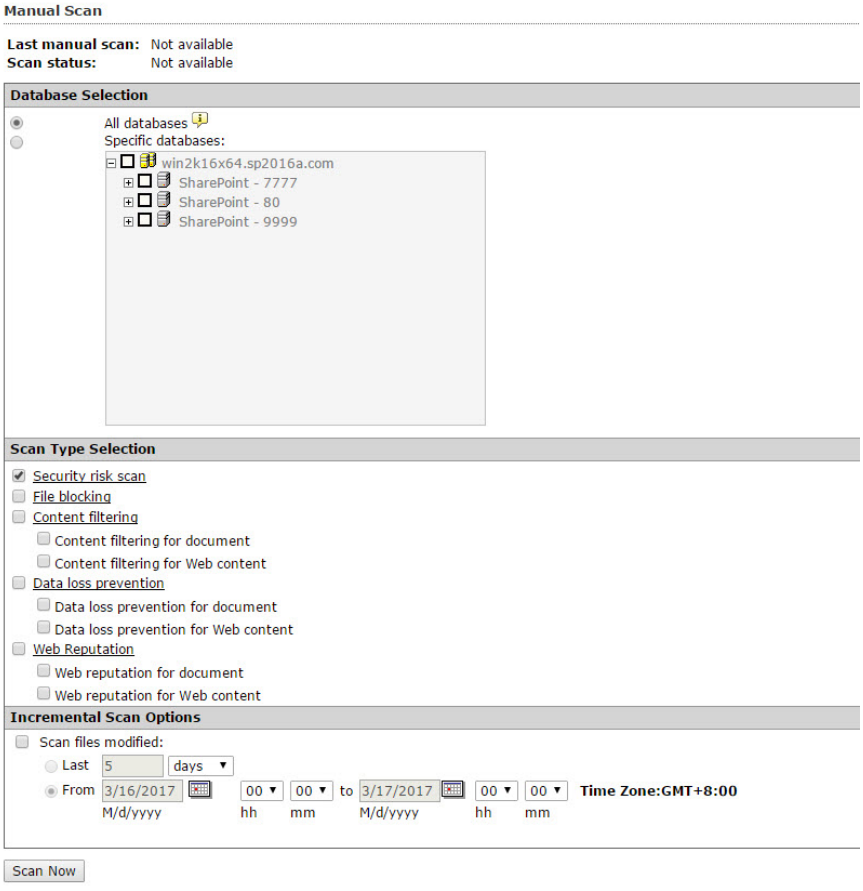
4. この設定を使用する場合は、[Save] をクリックして設定を保存します。

手動検索のバックアップフォルダの指定

手動検索のバックアップフォルダを 指定するために必要な手順を説明します。

手順

1. 左側のメニューで、[Manual Scan] をクリックします。[Manual Scan] 画面が表示されます。
2. [Select the scan type] の下にある [Security risk scan] リンクをクリックします。



3. [Manual Scan] > [Security Risk Scan] 画面が表示されます。

4. [Action] タブをクリックし、画面下部の [Backup Setting] を展開します。

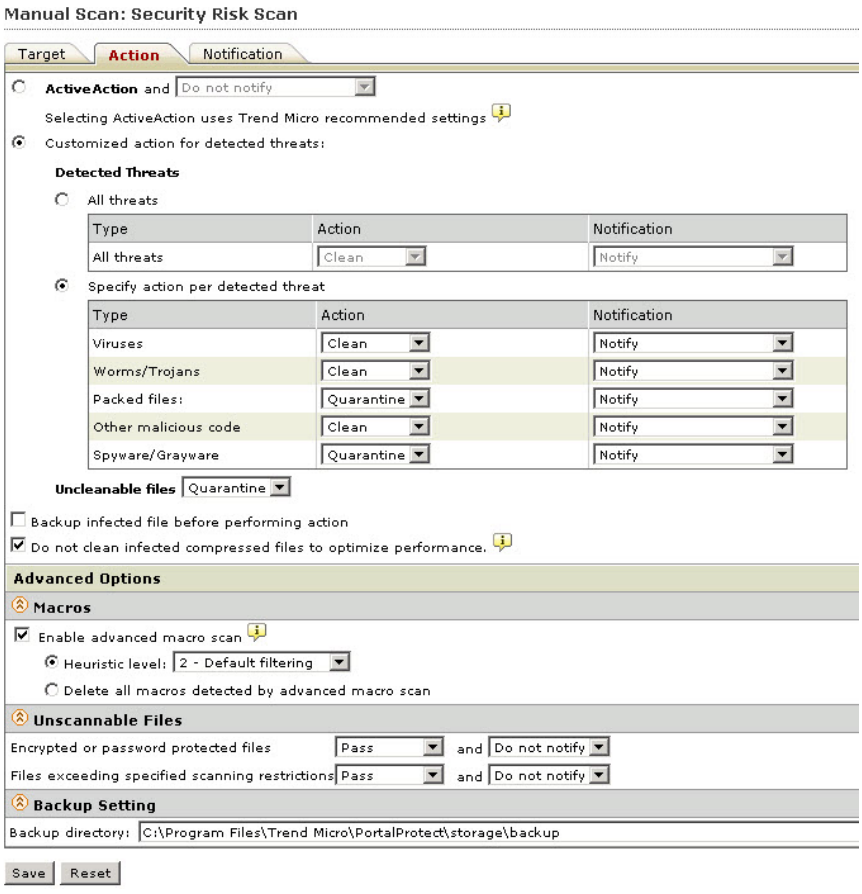


図 3-4. [Manual Scan] > [Security Risk Scan] ([Action] タブ)

5. [Backup directory] に、バックアップファイルの保存先のフルパスを入力します。ディレクトリパスが存在しない場合は、指定したパスにフォルダが作成されます。

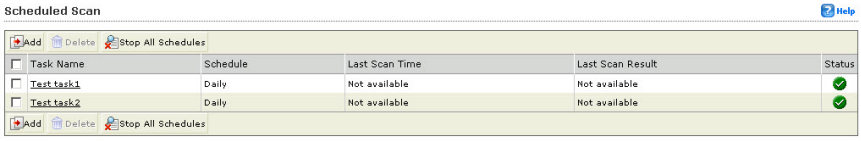
6. この設定を使用する場合は、[Save] をクリックして設定を保存します。

予約検索のバックアップフォルダの指定

予約検索のバックアップフォルダを 指定するために必要な手順を説明します。

手順

1. 左側のメニューで、[Scheduled Scan] をクリックします。[Scheduled Scan] 画面が表示されます。
2. [Add] をクリックして新しい予約検索を追加するか、[Task Name] 列で既存の予約検索をクリックします。



3. 前の選択内容に応じて、[Scheduled Scan: Add Scan Task] または [Scheduled Scan: Edit Scan Task] 画面が表示されます。

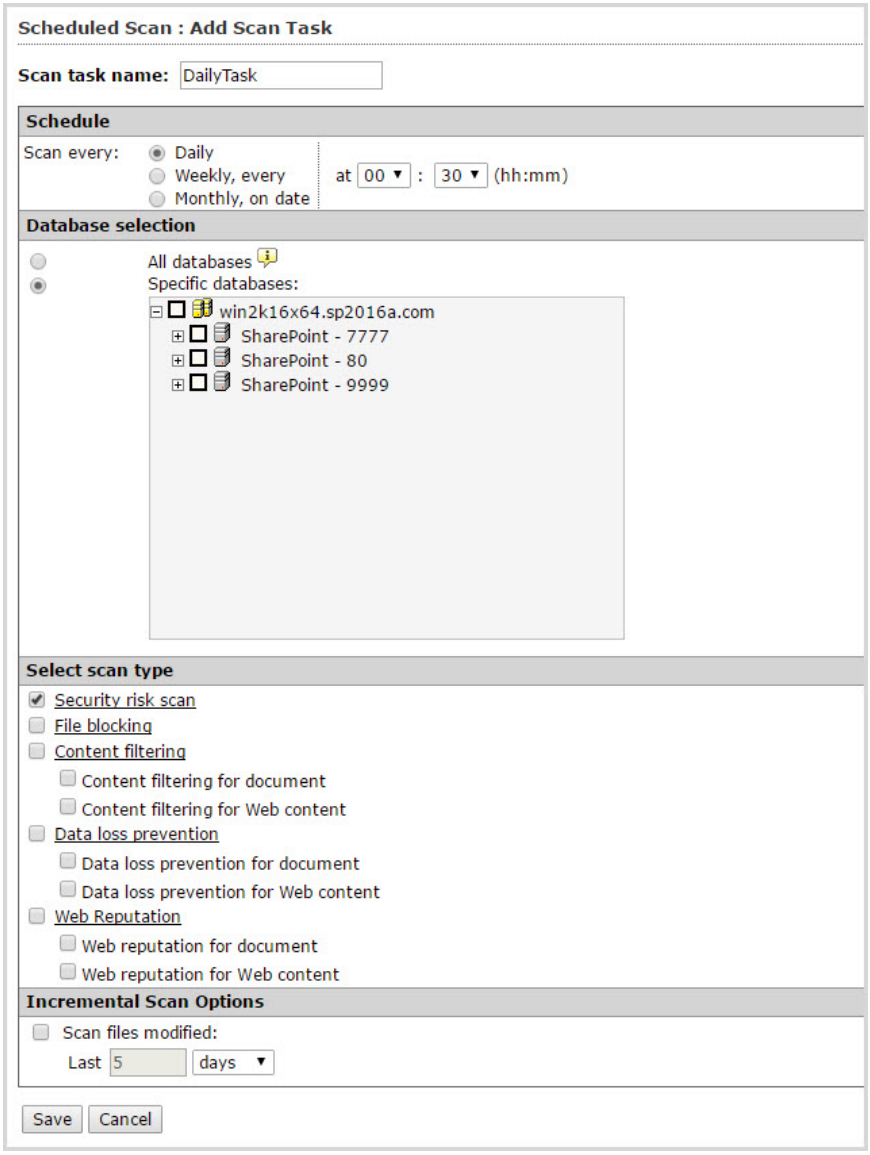


図 3-5. [Scheduled Scan: Add Scan Task] 画面

4. [Select scan type] の下にある [Security risk scan] リンクをクリックします。[Scheduled Scan] > [Security Risk Scan] 画面が表示されます。
5. [Action] タブをクリックし、画面下部の [Backup Setting] を展開します。
6. [Backup directory] に、バックアップファイルの保存先のフルパスを入力します。ディレクトリパスが存在しない場合は、指定したパスにフォルダが作成されます。
7. この設定を使用する場合は、[Save] をクリックして設定を保存します。

高度なマクロ検索について

マクロウイルス/不正プログラムはアプリケーションに依存します。マクロウイルスは、Microsoft Word (`.doc`) や Microsoft Excel (`.xls`) などのアプリケーションで動作するマクロユーティリティに感染します。そのため、これらのウイルスは、マクロの実行が可能なアプリケーションに共通の拡張子 (`.doc`、`.xls`、および`.ppt` など) を持つファイルで検出されます。マクロウイルス/不正プログラムは、対象アプリケーションのデータファイル間で広まり、最終的には大量のファイルに感染する可能性があります。

PortalProtect では、次の方法を使用してマクロウイルス/不正プログラムのサーバへの感染を回避します。

- ヒューリスティック検索を使用して不正なマクロコードを検出します。
- ヒューリスティック検索は、ウイルスや不正プログラムを検出するための評価的な方法であり、既知のウイルスシグネチャを持たない未知のウイルス/不正プログラムや脅威を検出する点で優れています。
- 検索ファイルからすべてのマクロコードを除去します。

詳細については、以下を参照してください。

- 66 ページの「セキュリティリスクのリアルタイム 検索のマクロ検索オプションの設定」
- 160 ページの「手動検索のマクロ検索オプションの設定」
- 188 ページの「予約検索のマクロ検索オプションの設定」

第 4 章

セキュリティリスク検索

本章では、セキュリティリスク検索に必要な背景情報と設定方法について説明します。PortalProtect では、セキュリティリスク検索用に従来型スキャンとスマートスキャンの 2 つのオプションが用意されています。従来型スキャンは、ローカルコンピュータ上の検索エンジンに要求を送信します。スマートスキャンは、セキュリティリスクや Web 上の脅威から SharePoint 環境を保護するために設計された、次世代の顧客専用クラウド-クライアント型コンテンツセキュリティインフラストラクチャである Trend Micro Smart Protection Network を使用します。より多くの製品、サービス、およびユーザがネットワークにアクセスすれば、それだけ保護機能が自動的に更新および強化されることになり、利用者自身のリアルタイムな自警システムが構築されていきます。スマートスキャンソリューションでは、クラウド内保護のために Trend Micro Smart Protection Network が利用されます。

本章の内容は次のとおりです。

ファイルレピュテーション

トレンドマイクロのファイルレピュテーションテクノロジは、ユーザにアクセスを許可する前に、インターネットクラウドに格納されている膨大なデータベースを照会して対象ファイルのレピュテーション (評価) を確認します。不正プログラム情報はクラウドに格納されているので、すべてのユーザがただちに使用できます。パフォーマンスに優れたコンテンツ配信ネットワークとローカル (社内ネットワーク) のキャッシュサーバによって、確認プロセスで発生する待ち時間は最小限に抑えられます。クラウド-クライアント型のアーキテクチャは、より迅速な保護を実現し、パターンファイル配信の負荷を解消することに加えて、クライアントの全般的なフットプリントを大幅に削減します。

セキュリティリスク検索方法の選択

手順

1. 左側のメニューで [Smart Protection] > [Scan Service Settings] をクリックします。

   [Scan Service Settings] 画面が表示されます。

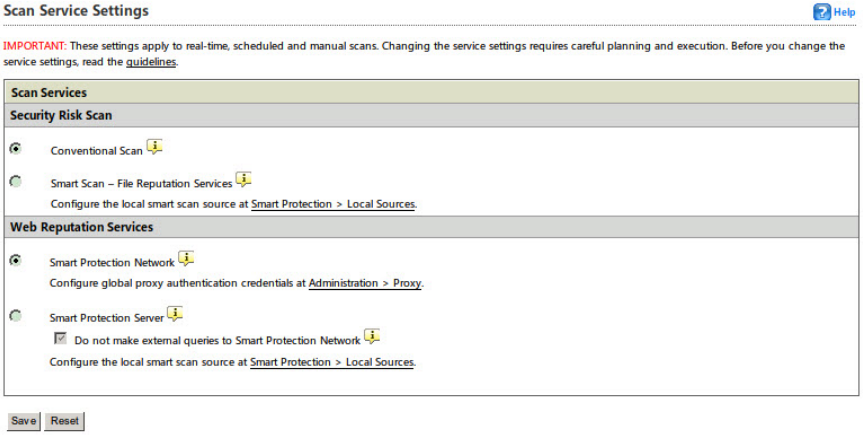


図 4-1. [Scan Service Settings] 画面

2. [Security Risk Scan] で、次のオプションのいずれかを選択します。

   - Conventional Scan — ローカルコンピュータの検索エンジンを使用してファイルのセキュリティリスク検索を実行します。
   - Smart Scan - File Reputation Services — 専用のスマートスキャンサーバを使用してファイルのセキュリティリスク検索を実行します。

     スマートスキャンソースを設定します。スマートスキャンを使用する場合は、[Smart Protection] > [Local Sources] リンクをクリックして Smart Protection Server を設定します。

   注意

   これらの設定方法の詳細については、147 ページの「Web レピュテーションソースの選択」を参照してください。

3. [Save] をクリックします。

セキュリティリスクのリアルタイム検索の有効化と無効化

手順

1. 左側のメニューで、[Security Risk Scan] をクリックします。

   [Security Risk Scan] 画面が表示されます。

2. 検索を有効にするには [Enable real-time security risk scan] をオンにし、無効にするにはオフにします。
3. [Save] をクリックします。

注意

セキュリティリスクのリアルタイム検索は、[Summary] 画面で [Scan Services] の [Status] アイコンをクリックしても 有効化または無効化できます。

セキュリティリスク検索の対象の設定について

ここでは、[Security Risk Scan] > [Target] タブで利用できるオプションについて簡単に説明します。PortalProtect の初期設定では、最大限のセキュリティを実現するため、SharePoint サーバ上のすべてのファイルが検索されます。しかし、すべてのファイルを 1 つ 1 つ検索するには多くの時間とリソースが必要になります。そのため、リアルタイム検索、手動検索、および予約検索の対象ファイルを制限することを検討してください。

PortalProtect では、検索を次のファイルに限定するように設定できます。

- すべての検索可能ファイル — SharePoint 環境を通過する、または SharePoint 環境に保存されているすべてのコンテンツを検索します。
- トレンドマイクロの推奨設定 (Intelliscan) — トレンドマイクロの推奨設定を使用することで効率的な検索を実行できます。14 ページの「トレンドマイクロの推奨設定 (Intelliscan) について」を参照してください。
- 特定のファイルタイプ — ファイル拡張子のリストおよび実際のファイルタイプのリストから検索対象を選択できます。このリストに項目を追加するには、[Specify file extensions configuration] フィールドにファイル拡張子を入力します。

セキュリティリスク検索の対象の設定

[Target] タブでセキュリティリスク検索を設定するために必要な手順を説明します。

手順

1. 製品コンソールにログオンします。
2. [Security Risk Scan] をクリックします。

   [Security Risk Scan] 画面が表示されます。
3. セキュリティリスク検索について、次のいずれかを選択します。
   - All scannable files: 検索可能なファイルをすべて検索するには、このオプションを選択します。
   - IntelliScan: 実際のファイルタイプの識別により、トレンドマイクロの推奨設定を使用して効率的な検索を実行します。

- Specify file types: [Show details] リンクをクリックしてリストを展開し、PortalProtect で検索するファイルを選択します。これらのファイルが「実際のファイルタイプ」です。検索エンジンはファイル名ではなくファイルヘッダを検証して、実際のファイルタイプを判定します。または、ファイルの拡張子のリストを作成するには、[Specify file extensions] を選択します。
- 例: [Specify file types] をクリックして、[Application and executables] > [Executable (.exe、.dll、.vxd)] を選択すると、PortalProtect は実行可能ファイル、DLL、および VXD ファイルタイプを検索します。この場合、これらのファイルで偽のファイル拡張子が使用されていても (実際の拡張子は `.exe` であるにもかかわらず、`.txt` という拡張子が付加されていても)、検索は行われます。ただし、[Specify file extensions] をクリックして「`exe`」と入力した場合は、PortalProtect は `.exe` タイプのファイルしか検索しません。この場合、他のファイルタイプを偽装するために、偽の拡張子が付けられたファイルは PortalProtect で認識されません。

4. IntelliTrap テクノロジを利用するには、[Enable IntelliTrap] を選択します。
5. [Spyware/Grayware Scan] では、[Select All] を選択するか、以下から選択します。
   - Spyware
   - Dialers
   - Hacking Tools
   - Password Cracking Applications
   - Adware
   - Joke Programs
   - Remote Access Tools
   - Others
6. パフォーマンスを調整するには、[Scan Restriction Criteria] をクリックして詳細を展開します。[Do not scan file if...] の下で以下を設定します。
   - File size exceeds — 1〜100MB の値を入力します。

このオプションが選択されていない場合、1GB より大きいファイルは検索されません。

7. [Do not scan compressed files if] の下で、以下に従って値を入力します。
   - Decompressed file count exceeds [xxxxx] — 圧縮ファイル内の最大ファイル数を入力します (1〜10,000)。PortalProtect では、この値以上のファイル数を含む圧縮ファイルは検索されません。
   - Size of Decompressed file exceeds [xxxx] — PortalProtect で検索する圧縮ファイルの最大サイズをメガバイト単位で入力します (1〜2048)。PortalProtect では、このサイズ以上の圧縮ファイルは検索されません。
   - Number of layers of compression exceeds [xx] — PortalProtect で検索する圧縮ファイルの最大階層数を入力します (1〜20)。PortalProtect では、この値以上の圧縮階層を持つ圧縮ファイルは検索されません。
   - Size of decompressed file is "x" times the size of compressed file — 解凍ファイルの最大サイズを示す、圧縮ファイルのサイズに対する倍数を入力します。解凍ファイルが超えてはいけない、圧縮ファイルのサイズに対する倍数 (100〜1,000,000) を入力します。圧縮ファイルのサイズの「x」倍より大きい解凍ファイルは検索されません。
8. [Save] をクリックします。

セキュリティリスクのリアルタイム検索のマクロ検索オプションの設定

セキュリティリスクのリアルタイム 検索のマクロ検索オプションを設定するために必要な手順を説明します。

手順

1. 左側のメニューで [Security Risk Scan] をクリックし、[Action] タブを選択します。
2. [Advanced Options] で、[Macros] をクリックしてコンテンツを開きます。
3. [Enable advanced macro scan] を選択して機能を有効にします。

4. [Heuristic level] で、次のいずれかのオプションを選択します。
   - 1 — Lenient filtering
   - 2 — Default filtering
   - 3 — Sensitive filtering
   - 4 — Rigorous filtering

   または
5. [Delete all macros detected by advanced macro scan] を選択します。
6. [Save] をクリックします。

セキュリティリスクの検出時の処理の設定について

ブロックまたは検索の設定に一致するファイルが検出されると、PortalProtect では SharePoint 環境を保護するための処理が実行されます。実行される処理は、検索の種類 (リアルタイム検索、手動検索、または予約検索) と、その検索に設定した処理の種類によって異なります。PortalProtect が処理を実行するたびに、ログにイベントが記録されます。[Logs] メニューを使用すると、これらのログイベントについてクエリを実行できます。

手順

1. バックアップフォルダを設定するかどうかを選択します。

   バックアップフォルダを設定すると、指定された処理を実行する前に、PortalProtect からファイルのコピーがバックアップディレクトリに送信されます。52 ページの「セキュリティリスク検索のバックアップフォルダの指定」参照。
2. ウイルスまたは不正プログラムコードを検出したときに実行する処理を設定します。

   トレンドマイクロの推奨処理を使用するように設定することも、カスタム処理を設定することもできます。トレンドマイクロの推奨処理では、

脅威の種類に基づいて最適な処理が実行されます。18 ページの「トレンドマイクロの推奨処理 (Active Action)」参照。

セキュリティリスクの検出時の処理の設定

検索の設定に一致するファイルが検出されると、PortalProtect では SharePoint 環境を保護するための処理が実行されます。実行される処理は、検索の種類 (リアルタイム検索、手動検索、または予約検索) と、その検索に設定した処理の種類によって異なります。

次に、使用可能なオプションについての簡単な説明を示します。

- ActiveAction: トレンドマイクロが推奨する検索処理を実行します。

ヒント

トレンドマイクロの推奨処理 (Active Action) は、トレンドマイクロが推奨する一次および二次検索処理を実行します。一次検索処理に失敗した場合は、二次処理が実行されます。ウイルス、トロイの木馬、およびジョークプログラムに対しては、事前に設定された検索処理が使用されます。

- Customized action for detected threats: すべてのセキュリティリスクに対して同じ処理を実行するか、脅威ごとに処理を指定します。
- Advanced Options: マクロ、検索不能なファイル、およびバックアップ設定について、詳細オプションを指定します。

手順

1. 製品コンソールにログオンします。
2. [Security Risk Scan] をクリックします。

   [Security Risk Scan] 画面が表示されます。
3. [Action] タブをクリックします。

   [Action] 画面が表示されます。
4. 次のいずれかを選択します。
   - ActiveAction

[Notify]、[Notify when uncleanable]、または [Do not notify]

- Customized action for detected threats

5. 感染ファイルをバックアップするには、[Backup infected file before performing action] を選択します。
6. パフォーマンスの向上が必要な場合は、[Do not clean infected compressed files to optimize performance] を選択します。
7. 必要に応じて [Advanced Options] を設定します。[Advanced Options] で、[Macros] をクリックしてコンテンツを展開します。
8. [Enable advanced macro scan] を選択して機能を有効にします。
9. [Heuristic level] で、次のいずれかのオプションを選択します。
   - 1 — Lenient filtering
   - 2 — Default filtering
   - 3 — Sensitive filtering
   - 4 — Rigorous filtering
10. [Delete all macros detected by advanced macro scan] を選択します。
11. [Unscannable Files] をクリックして展開し、暗号化されたファイル、パスワードで保護されたファイル、および検索の制限条件に当てはまらないファイルに対する処理を指定します。次のオプションから選択します。
    - Encrypted or password protected files
      a. [Block] または [Pass]

      および

      b. [Notify] または [Do not notify]
    - Files exceeding specified scanning restrictions
      a. [Block] または [Pass]

      および

      b. [Notify] または [Do not notify]

12. 必要に応じて [Backup Setting] を変更します。
13. [Save] をクリックします。

注意

通知の設定方法の詳細については、207 ページの「セキュリティリスク検索通知の設定」を参照してください。

圧縮ファイルの検索

ここでは、セキュリティリスクのリアルタイム検索、手動検索、および予約検索で圧縮ファイルの検索を設定するために必要な手順を説明します。

注意

圧縮ファイルを検索する際の検索パフォーマンスを最適化するには、[Security Risk Scan] > [Action] タブで [Do not clean infected compressed files to optimize performance] をオフにします。

手順

1. 左側のメニューで [Security Risk Scan] をクリックし、[Target] タブを選択します。
2. [Target] タブの [Advanced Options] で、[Scan Restrictions Criteria] を展開します。

注意

検索する項目のチェックボックスをオンにして、適切な値を設定します。

3. [Do not scan file if...] の下で以下を設定します。
   - File size exceeds — 1〜100MB の値を入力します。
4. [Do not scan compressed files if] の下で、以下に従って値を入力します。

- Decompressed file count exceeds [xxxxx] — 圧縮ファイル内の最大ファイル数を入力します (1〜10,000)。PortalProtect では、この値以上のファイル数を含む圧縮ファイルは検索されません。
- Size of Decompressed file exceeds [xxxx] — PortalProtect で検索する圧縮ファイルの最大サイズをメガバイト単位で入力します (1〜2048)。PortalProtect では、このサイズ以上の圧縮ファイルは検索されません。
- Number of layers of compression exceeds [xx] — PortalProtect で検索する圧縮ファイルの最大階層数を入力します (1〜20)。PortalProtect では、この値以上の圧縮階層を持つ圧縮ファイルは検索されません。
- Size of decompressed file is "x" times the size of compressed file — 解凍ファイルの最大サイズを示す、圧縮ファイルのサイズに対する倍数を入力します。解凍ファイルが超えてはいけない、圧縮ファイルのサイズに対する倍数 (100〜1,000,000) を入力します。圧縮ファイルのサイズの「x」倍より大きい解凍ファイルは検索されません。

5. [Save] をクリックします。

第 5 章

ファイルブロック

本章では、タイプや名前に基づいてファイルをブロックするよう PortalProtect を設定し、その設定に一致したすべてのファイルに対して実行する処理を選択する方法について説明します。

本章の内容は次のとおりです。

ファイルブロックについて

タイプや名前に基づいてファイルをブロックするよう PortalProtect を設定し、その設定に一致したすべてのファイルに対して実行する処理を選択できます。ファイルブロックを有効にすると、設定に従ってファイルがブロックされます。ファイルブロックは、リアルタイム検索、手動検索、および予約検索の実行時に、選択した設定に応じて実行できます。

注意

ファイルブロックオプションは、実行する検索の種類によって異なります。セキュリティリスク検索、手動検索、および予約検索のそれぞれで指定可能な処理を確認してください。

ファイルタイプは、.txt、.exe、.dll などのファイル拡張子によって識別され、多くのウイルスがこの特定のファイルタイプと密接に関連しています。ウイルスの中には無害として認知されている拡張子を使用してファイルを偽装するものがあるため、実際のファイルタイプに基づくブロック機能では、ファイルのヘッダを検索してそのタイプを判断しています。ファイルタイプに基づいてブロックするように PortalProtect を設定すると、SharePoint サーバにおいてそれらのファイルタイプに対するセキュリティリスクを低減できます。同様に、特定の攻撃の多くが特定のファイル名に関連しています。感染ファイルの名前がわかれば、PortalProtect を使用してそのファイルを SharePoint 環境から排除できます。ブロック機能はウイルスの大規模感染を制御する効果的な方法です。

ヒント

管理者は、ファイルブロックを使用して、業務に関係のないファイルの共有を制限するポリシーを SharePoint サーバに実施することもできます。

ファイルブロックの処理の設定について

ブロックの設定に一致するファイルが検出されると、PortalProtect では SharePoint 環境を保護するための処理が実行されます。実行される処理は、検索の種類 (リアルタイム検索、手動検索、または予約検索) と、その検索に設定した処理の種類 (ブロックまたは放置) によって異なります。
PortalProtect が処理を実行するたびに、ログにイベントが記録されます。こ

れらのログは、[Logs] メニューから表示できます。詳細については、245 ページの「ログのクエリ」を参照してください。

指定可能な処理

検索の種類	PortalProtect で実行する処理
[File Blocking] (リアルタイム)	ブロックまたは放置 (Block/Pass)
[Manual Scan] > [File Blocking]	隔離、削除、または放置 (Quarantine/Delete/Pass)
[Scheduled Scan] > [File Blocking]	隔離、削除、または放置 (Quarantine/Delete/Pass)

ファイルブロックの設定

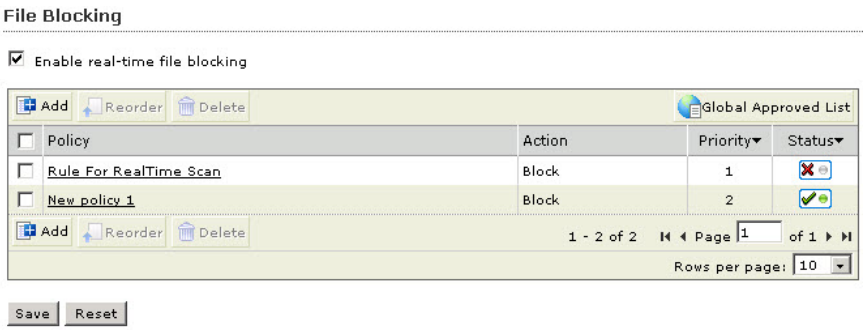
ここでは、PortalProtect のファイルブロックを設定および管理するために必要な情報を示します。[File Blocking] メイン画面から、以下の設定を管理できます。

- リアルタイムでのファイルブロックを有効化/無効化する
- リストされたポリシーを、ポリシー名または有効化/無効化によってフィルタする
- ポリシーの優先順位を変更する
- ポリシーを削除する
- ポリシーを有効化/無効化する
- ポリシーページに表示される行数を変更する
- 新しいポリシーを追加または既存のポリシーを編集する

手順

1. 左側のメニューで、[File Blocking] をクリックします。

[File Blocking] 画面が表示されます。



2. [Enable real-time file blocking] を選択します。

注意

リスト表示されたポリシーは、[Policy name]、[All]、[Enabled]、または [Disabled] によってフィルタできます。フィルタオプションを 選択したら、[Search] をクリックします。すべての検索結果を表示するには、[Display All] をクリックします。

---

3. [Save] をクリックします。

ファイルブロックポリシーの追加

ここでは、新しいファイルブロックポリシーを追加するために必要な手順を説明します。

手順

1. 左側のメニューで、[File Blocking] をクリックします。[File Blocking] 画面が表示されます。
2. [Add] をクリックします。[File Blocking: Add Policy] > [Step 1: Specify Rules] 画面が表示されます。

手順 1. [File Blocking: Add Policy] > [Specify Rules]

手順

1. [Block these files] の下で [Specific files] > [File Types] の以下のオプションから選択し、[Show details] をクリックしてコンテンツを展開します。
   - Application and executables
   - Documents
   - Images
   - Video
   - Audio
   - Compressed files
2. [Specific files] > [File Names] の場合は、[Show details] をクリックしてコンテンツを展開します。
   a. リストに表示されている拡張子をブロックするには、[Specific file extensions to block] を選択します。新しい拡張子を追加するには、拡張子を入力して、[Add] をクリックします。複数のエントリはセミコロン (;) で区切ります。

      注意
      エントリを削除するには、エントリを選択して、[Delete] をクリックします。複数のエントリを選択するには、<Ctrl> キーを押しながらクリックします。

   b. リストに表示されている名前を持つファイルをブロックするには、[File names to block] を選択します。新しいファイル名を追加するには、ファイル名を入力して、[Add] をクリックします。
3. 指定したファイルタイプまたはファイル名が含まれている圧縮ファイルをブロックするには、[Block compressed files containing the specific file types or names] を選択します。
4. [Block OLE containers containing the specific file types or names] を選択し、[Show details] をクリックしてコンテンツを展開します。

a. OLE (Object Linking and Embedding) コンテナをマイクロソフトのドキュメントファイルに制限するには、[Microsoft documents] を選択します。

b. OLE コンテナを PDF ファイルに制限するには、[Adobe Portable Document Format (.pdf)] を選択します。

c. ブロックでサポートする OLE の最大階層数を設定します。

5. [Next] をクリックします。[File Blocking: Add Policy] > [Step 2: Exceptions] 画面が表示されます。

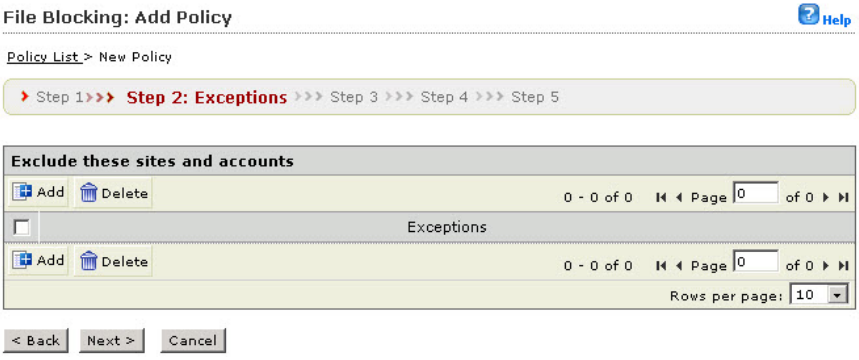


図 5-1. [File Blocking: Add Policy] > [Step 2: Exceptions] 画面

手順 2. [File Blocking: Add Policy] > [Exceptions]

手順

1. 除外設定を追加するには、[Add] をクリックします。[File Blocking: Add Policy] > [Step 2.a: Specify sites to be excluded] 画面が表示されます。

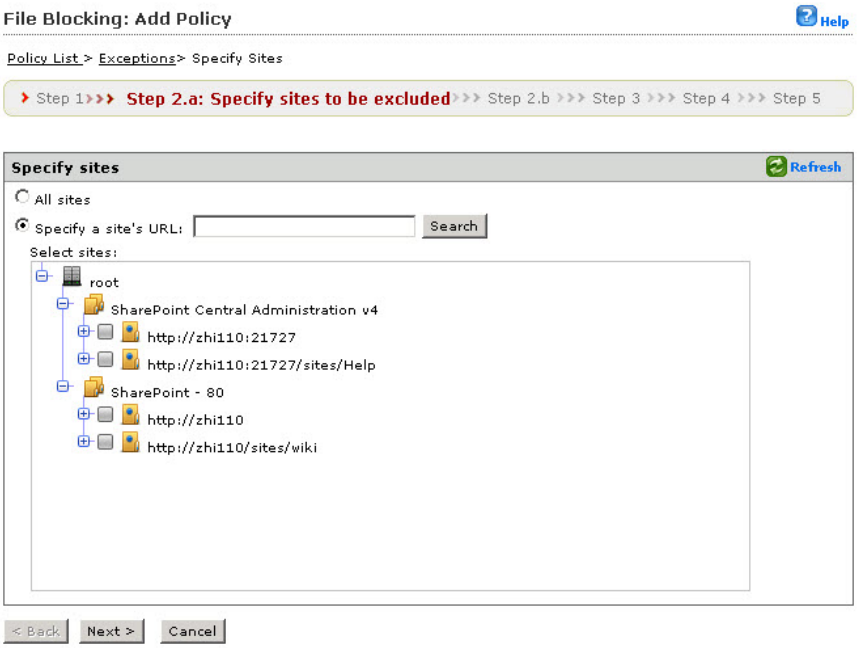


図 5-2. [File Blocking: Add Policy] > [Step 2.a: Specify sites to be excluded] 画面

2. 次のいずれかを選択します。

   • [All sites] を選択した場合

   注意
   [All sites] オプションを指定した場合は、AD ユーザ/グループのみから選択できます。

   • [Next >] をクリックします。

   • [Specify a site's URL] を選択した場合

注意

[Specify a site's URL] オプションを指定した場合は、AD ユーザ/グループと SharePoint ユーザ/グループの両方から選択できます。選択するには、[Search for] ドロップダウンを使用します。

- [Specify a site's URL] フィールドに URL を入力し、[Search] をクリックします。
- [Select sites] のツリーで、このポリシーから除外する特定のサイトを選択します。
- [Next >] をクリックします。

3. [Next >] をクリックします。[Step 2b: Specify accounts to be excluded] 画面が表示されます。

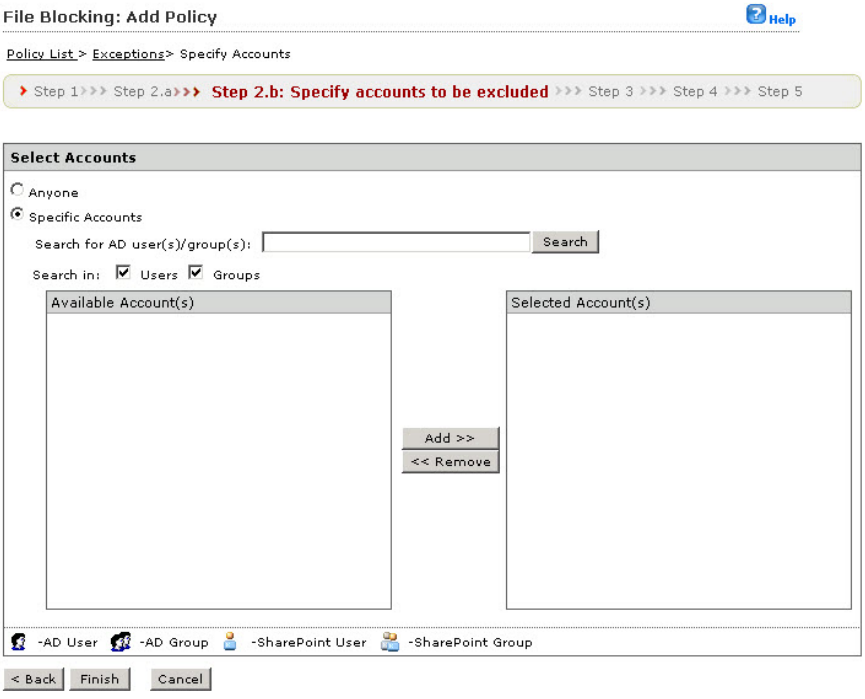


図 5-3. [File Blocking: Add Policy] > [Step 2.b: Specify accounts to be excluded] 画面

4. 次のオプションから選択します。

   - Anyone — すべてのアカウントを除外する場合に選択します。[Finish] をクリックして、次の手順に進みます。
   - Specific accounts — 特定のアカウントを選択する場合に使用し、次の手順に進みます。

5. AD ユーザまたはグループの名前を [Search for AD user(s)/group(s)] フィールドに入力します。

注意

[Specify a site's URL] オプションを指定した場合は、AD ユーザ/グループと SharePoint ユーザ/グループの両方から選択できます。選択するには、[Search for] ドロップダウンを使用します。

6. [Search in] の横にある [Users] または [Groups]、あるいは両方を適宜選択します。
7. [Search] をクリックします。検索の結果は、[Available Account(s)] 画面に表示されます。
8. 必要に応じて検索を繰り返します。
9. 除外対象とするユーザ/グループをすべて選択し、[Add] をクリックして、[Selected Account(s)] 画面に移動します。
10. オプションを選択したら、[Finish] をクリックします。[File Blocking: Add Policy] > [Step 2: Exceptions] 画面に新しく追加した除外設定が表示されます。
11. [Next >] をクリックします。[File Blocking: Add Policy] > [Step 3: Specify Action] 画面が表示されます。

図 5-4. [File Blocking: Add Policy] > [Step 3: Specify Action] 画面

手順 3. [File Blocking: Add Policy] > [Specify Action]

手順

1. 次のオプションから選択します。
   - [Block] または [Pass]

     および

   - [Notify] または [Do not notify]
2. [Next >] をクリックします。[File Blocking: Add Policy] > [Step 4: Specify Notification] 画面が表示されます。

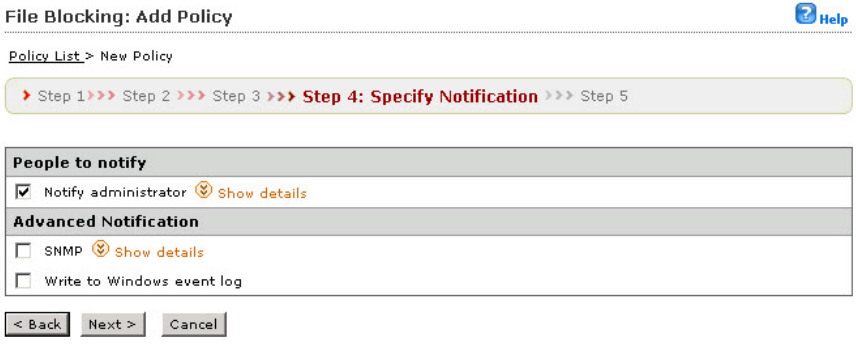


図 5-5. [File Blocking: Add Policy] > [Step 4: Specify Notification] 画面

手順 4. [File Blocking: Add Policy] > [Specify Notification]

手順

1. 209 ページの「ファイルブロック通知の設定」で説明されている基本手順に従います。[Next >] をクリックします。[File Blocking: Add Policy] > [Step 5: Name and Priority] 画面が表示されます。

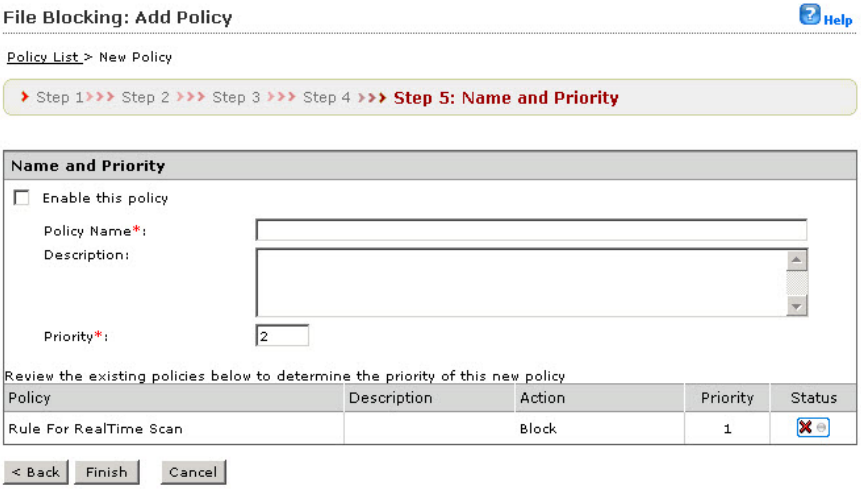


図 5-6. [File Blocking: Add Policy] > [Step 5: Name and Priority] 画面

手順 5. [File Blocking: Add Policy] > [Name and Priority] 画面

手順

1. [Enable this policy] を選択して、有効にします。
2. [Policy name] フィールドにポリシーの名前を入力します。
3. [Priority] フィールドにポリシーの優先順位を入力します。

> **ヒント**
> その他のポリシーの優先順位および設定は、既存のポリシーを確認する画面で確認できます。

4. [Finish] をクリックします。[File Blocking] メイン画面が表示され、指定した優先順位で新しいポリシーが表示されます。

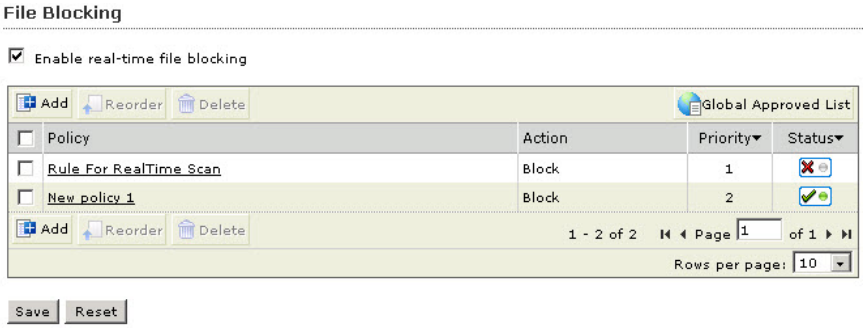


図 5-7. [File Blocking] メイン画面

ファイルブロックポリシーの編集

ここでは、ファイルブロックポリシーを編集するために必要な手順を説明します。

手順

1. 左側のメニューで、[File Blocking] をクリックします。

   [File Blocking] 画面が表示されます。

2. [File Blocking] 画面で、編集するポリシー名をクリックします。

[File Blocking: Edit Policy] 画面が表示されます。

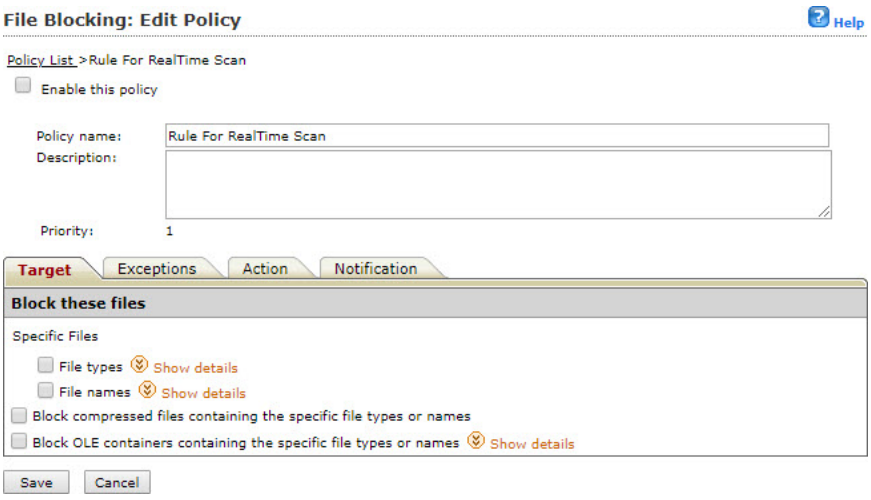


図 5-8. [File Blocking: Edit Policy] 画面 ([Target] タブ)

3. [Enable this policy] チェックボックスをオンまたはオフにして、ポリシーを有効/無効にします。
4. 必要に応じて以下を編集します。
   - Policy name
   - Description
5. [Target] タブをクリックします。
6. [Block these files] の [Specific Files] で [Show details] をクリックして内容を展開し、[File types] と [File names] を選択します。

   詳細については、77 ページの「手順 1. [File Blocking: Add Policy] > [Specify Rules]」を参照してください。
7. [Exceptions] タブをクリックして、必要に応じて除外設定を追加または編集します。

   詳細については、78 ページの「手順 2. [File Blocking: Add Policy] > [Exceptions]」を参照してください。

8. [Action] タブをクリックして、以下から選択します。
   - Block file
   - Pass
   - Notify
   - Do not notify
9. [Notification] タブをクリックして、適切な設定を選択します。

   詳細については、83 ページの「手順 4. [File Blocking: Add Policy] > [Specify Notification]」を参照してください。
10. [Save] をクリックします。

使用可能なファイルタイプについて

ここでは、使用可能なファイルタイプについて説明します。

アプリケーションおよび実行可能ファイル

表 5-1. アプリケーションおよび実行可能なファイルの種類

ファイルタイプ	関連付けられている拡張子
実行可能なリンク形式のファイル	.elf
実行可能ファイル	.exe、.dll、.vxd
Java アプレット	.class
Windows NT/95 のショートカット	.lnk
Windows インストーラパッケージ	.msi

文書ファイル

表 5-2. 文書ファイルの種類

ファイルタイプ	関連付けられている拡張子
Adobe Portable Document Format	.pdf

ファイルタイプ	関連付けられている拡張子
コンパイル済み HTML ヘルプ	.chm
ActiveMime で圧縮された MS Office のマクロ	.mso
Microsoft Access	.mdb、.accdb
Microsoft Excel	.xls、.xlt
Microsoft Office Excel 2007	.xlsx、.xlsm、.xltx、.xltm、.xlsb、.xlam
Microsoft Office PowerPoint 2007	.pptx、.pptm、.potx、.ppam、.ppsx、.ppsm
Microsoft Office Word 2007	.docx、.docm、.dotx、.dotm
Microsoft OLE	.doc (Word 6.0〜2003)、.dot、.vss、.shs
Microsoft PowerPoint	.pps、.ppt
Microsoft プロジェクト	.mpp
Microsoft リッチテキスト形式	.rtf
Microsoft WORD/DOS 4.0/5.0	.wri、.doc
Microsoft ヘルプ	.hlp
MSFT	.msft
WordPerfect	.wp

画像

表 5-3. 画像ファイルの種類

ファイルタイプ	関連付けられている拡張子
Compuserve	.gif
Corel PhotoPaint 画像	.cpt
Corel Global Macro Storage	.gms
JPEG 画像	.jpg、.jpeg、.jpe

ファイルタイプ	関連付けられている拡張子
Macintosh MacPaint グラフィック	.mac
Portable Network Graphics	.png
Tagged image format	.tiff
Windows/ OS/2 ビットマップ	.bmp
Windows メタファイル	.wmf

ビデオ

表 5-4. ビデオファイルの種類

ファイルタイプ	関連付けられている拡張子
Advanced Streaming Format	.asf、.wmv
Macromedia フラッシュ	.swf
Moving Picture Experts Group ビデオ	.mpg、.mpeg
Microsoft Resource Interchange File Format	.avi、.bnd、.wav
Quicktime Movie	.mov、.qt、.qtm
Real Media	.rm

オーディオ

表 5-5. オーディオファイルの種類

ファイルタイプ	関連付けられている拡張子
Musical Instrument Digital Interface	.mid
MPEG Audio Layer 3	.mp3
Real Audio	.ra、.ram

圧縮ファイル

表 5-6. 圧縮ファイルの種類

ファイルタイプ	関連付けられている拡張子
LHA で作成されたアーカイブ	.lzh
Pkzip で作成されたアーカイブ	.zip
RAR で作成されたアーカイブ	.rar
Tar で作成されたアーカイブ	.tar
ARJ 圧縮アーカイブ	.arj
BINHEX	.hqx
GNU Zip	.gz、.gzip
LZW/16 ビット圧縮	.Z
MacBinary	.bin
Microsoft キャビネット	.cab
Microsoft 圧縮	.mscomp
MIME	.eml、.mht
Teledisk フォーマット	.td0
Unix BZ2 Bzip 圧縮ファイル	.bz2
UUEncode	.uu
WinAce	.ace

第 6 章

コンテンツフィルタ

本章では、望ましくないコンテンツが SharePoint に投稿されないように PortalProtect を設定する方法について説明します。

本章の内容は次のとおりです。

コンテンツフィルタについて

PortalProtect では、コンテンツフィルタポリシーのキーワードと一致する言葉を検出すると、望ましくないコンテンツが SharePoint に投稿されないようにする処理を実行できます。望ましくないコンテンツに対する処理を実行するたびに通知を送信するように設定することもできます。

PortalProtect の各コンテンツフィルタポリシーには、キーワード、語句、またはコンプライアンスパターンのリストが含まれています。コンプライアンスパターンは、クレジットカード番号、社会保障番号、および各国特有の識別情報に関連付けられています。PortalProtect は、今回 Active Directory (AD) ユーザ/グループ、および SharePoint ユーザ/グループと統合されました。ポリシーの適用対象は以下のとおりです。

- Active Directory ユーザ/グループ
- SharePoint サイト /SharePoint ユーザ/グループ

コンテンツフィルタは 以下に対して有効化できます。

- ドキュメントに対するリアルタイムコンテンツフィルタ — SharePoint ドキュメントライブラリにアップロードまたはダウンロードされるドキュメントのコンテンツをリアルタイムでフィルタします 。
- Web コンテンツに対するリアルタイムコンテンツフィルタ — タスク、リンク、カレンダ、通知など、新しいアイテムを 作成するときや既存のアイテムを更新するときに SharePoint Lists の Web コンテンツをフィルタします。

PortalProtect では、[Content Filtering] 画面に表示される順序に従ってコンテンツフィルタポリシーを適用します。ポリシーを適用する順序は設定可能です。PortalProtect では、コンテンツ違反が検出され、それ以降の検索が中止される処理 (ブロックまたは放置) が実行されない限り、各ポリシーに従ってフィルタ処理を行います。これらのポリシーの順序を変更することで、コンテンツフィルタを 最適化できます。

注意

ファイルに対するコンテンツフィルタは、アップロードおよびダウンロード中に検索を実行しますが、Web に対するコンテンツフィルタは、リストアイテムが追加または変更されたときに検索を実行します。

ファイルに対するコンテンツフィルタでは、.eml ファイルのコンテンツは検索できません。

たとえば、以下をチェックするポリシーを作成できます。

- クレジットカード番号および各国特有の識別情報
- 性的嫌がらせに該当する言葉
- 人種差別に該当する言葉
- 下品な言葉

コンテンツフィルタの処理の設定について

次の表は、コンテンツフィルタで 使用できる処理を示しています。

表 6-1. コンテンツフィルタの処理

検索の種類	PortalProtect で実行する処理
[Content Filtering] (リアルタイム)	ブロックまたは放置
[Manual Scan] > [Content Filtering] (ドキュメント)	隔離、削除、または放置 (Quarantine/Delete/Pass)
[Manual Scan] > [Content Filtering] (Web)	放置 注意 注意: PortalProtect は、手動検索でポリシーを実行する Web コンテンツを放置し、ログを作成します。
[Scheduled Scan] > [Content Filtering] (ドキュメント)	隔離、削除、または放置 (Quarantine/Delete/Pass)

検索の種類	PortalProtect で実行する処理
[Scheduled Scan] > [Content Filtering] (Web)	放置 注意 注意: PortalProtect は、手動検索でポリシーを実行する Web コンテンツを放置し、ログを作成します。

コンテンツフィルタポリシー

ここでは、コンテンツフィルタポリシーのオプションの 設定に役立つ背景情報について説明します。

ポリシーの除外設定

Active Directory に統合されたポリシーについては、特定の Active Directory ユーザとグループをポリシー除外アカウントとして指定することができます。たとえば、AD Group1 に ADuser1 と ADuser2 の除外設定を含めるとします。この場合、ADUser1 と ADUser2 は AD Group1 ポリシーに従って除外対象となります。

注意

除外設定は AD 環境でのみ機能します。[Exception] リストは、フォレストを超えた AD ユーザ/グループをサポートしません。また、グローバル AD グループもサポートしません。

SharePoint ユーザとグループに統合されたポリシーについては、特定の SharePoint サイトおよびサイト内のユーザ/グループを指定できます。

グローバル除外リスト (リアルタイム)

PortalProtect には、ドキュメントと Web コンテンツの両方に対応したグローバル除外リストという追加のリアルタイム機能があります。これは、管理者が、コンテンツフィルタポリシーから除外する Active Directory ユーザとグル

ープを追加できる除外リストです。3 ページの「グローバル除外リスト」を参照してください。

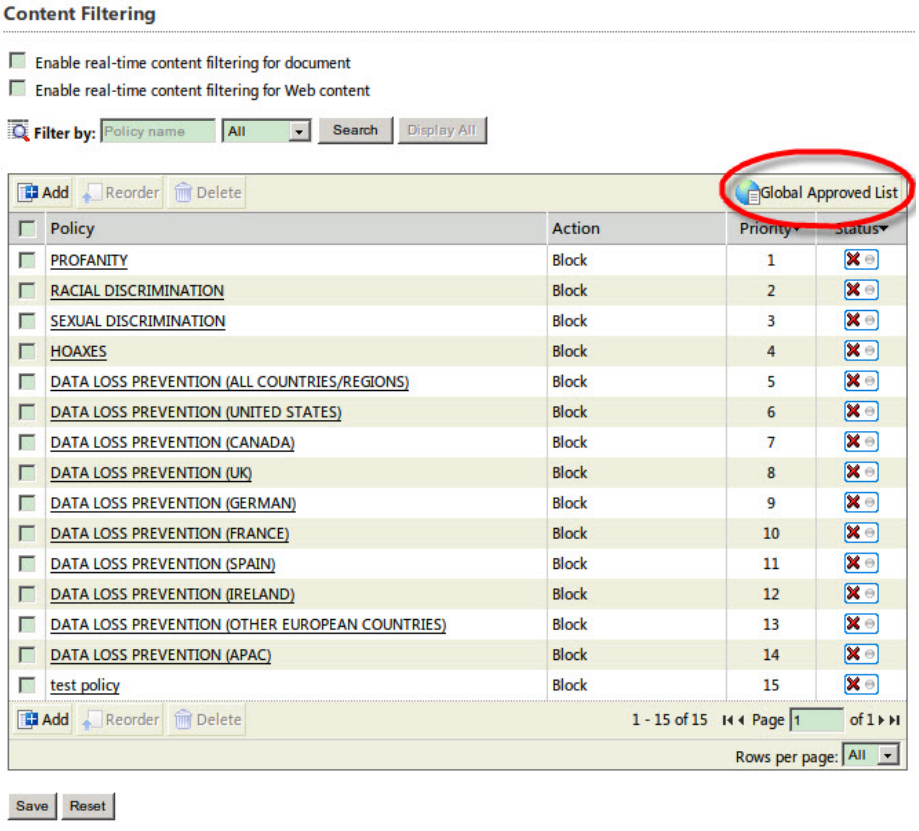


図 6-1. コンテンツフィルタのグローバル除外リスト

手順

1. 左側のメニューで [Content Filtering] をクリックします。

   [Content Filtering] 画面が表示されます。

2. [Global Approved List] をクリックします。

[Content Filtering: Edit Global Approved List] 画面が表示されます。

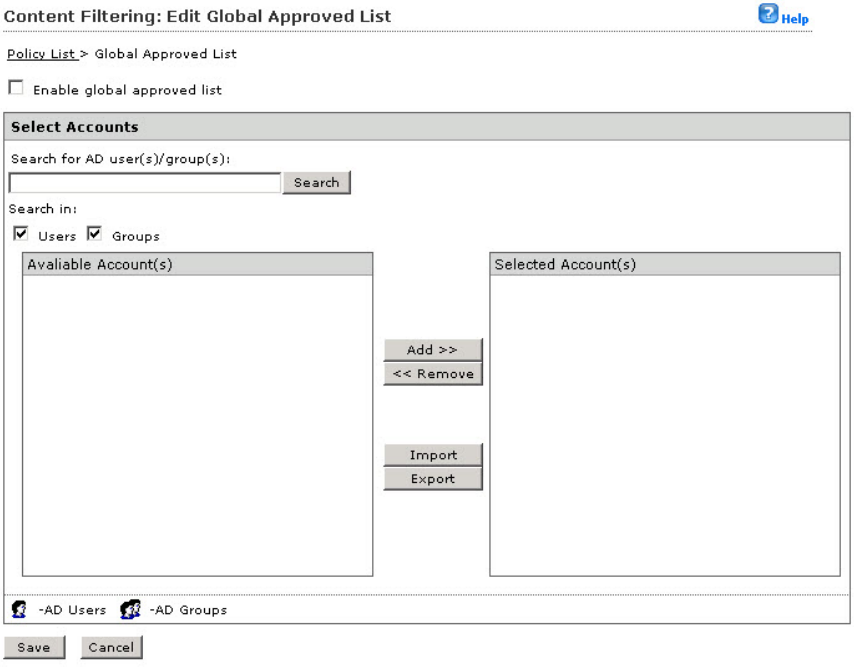


図 6-2. [Content Filtering: Edit Global Approved List] 画面

3. [Enable global approved list] をオンにして機能を有効にします。
4. AD ユーザまたはグループの名前を [Search for AD user(s)/group(s)] フィールドに入力します。
5. [Search in] の下で [Users] または [Groups]、あるいは両方を適宜選択します。
6. [Search] をクリックします。

   検索の結果は、[Available Account(s)] 画面に表示されます。
7. 必要に応じて検索を繰り返します。
8. [Global Approved List] に含めるユーザ/グループをすべて選択し、[Add] をクリックして、[Selected Account(s)] 画面に移動します。

注意

AD ユーザ/グループを外部ファイルからインポートすることや、外部ファイルにエクスポートすることも可能です。

9. [Save] をクリックします。

コンテンツフィルタの設定

ここでは、PortalProtect のコンテンツフィルタを 設定および管理するために必要な情報を示します。[Content Filtering] メイン画面から、以下の設定を管理できます。

- ドキュメントに対するリアルタイムでのコンテンツフィルタを 有効化/無効化する
- Web コンテンツに対するリアルタイムでのコンテンツフィルタを 有効化/無効化する
- リストされたポリシーを、ポリシー名または有効化/無効化によってフィルタする
- ポリシーの優先順位を変更する
- ポリシーを削除する
- ポリシーを有効化/無効化する
- ポリシーページに表示される行数を変更する
- 新しいポリシーを追加または既存のポリシーを編集する

手順

1. 左側のメニューで、[Content Filtering] をクリックします。

[Content Filtering] 画面が表示されます。

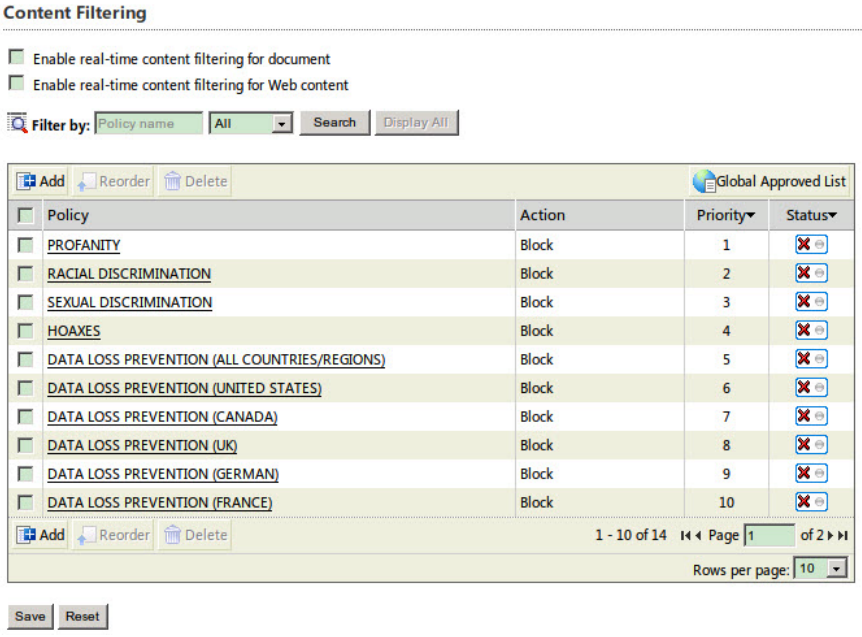


図 6-3. [Content Filtering] メイン画面

2. 次のオプションのいずれかまたは両方を選択します。

   - Enable real-time content filtering for document — ドキュメントに対してリアルタイムコンテンツフィルタを 実行します。
   - Enable real-time content filtering for Web content — Web コンテンツに対してリアルタイムコンテンツフィルタを 実行します。

注意

リスト表示されたポリシーは、[Policy name]、[All]、[Enabled]、または [Disabled] によってフィルタできます。フィルタオプションを 選択したら、[Search] をクリックします。すべての検索結果を表示するには、[Display All] をクリックします。

---

3. [Save] をクリックします。

コンテンツフィルタポリシーの追加

ここでは、新しいコンテンツフィルタポリシーを 作成するために必要なさまざまな手順を説明します。

手順 1. [Content Filtering: Add Policy] > [Specify Rules]

手順

1. 左側のメニューで、[Content Filtering] をクリックします。

   [Content Filtering] 画面が表示されます。

2. [Add] をクリックします。

   [Content Filtering: Add Policy] > [Step 1: Specify Rules] 画面が表示されます。

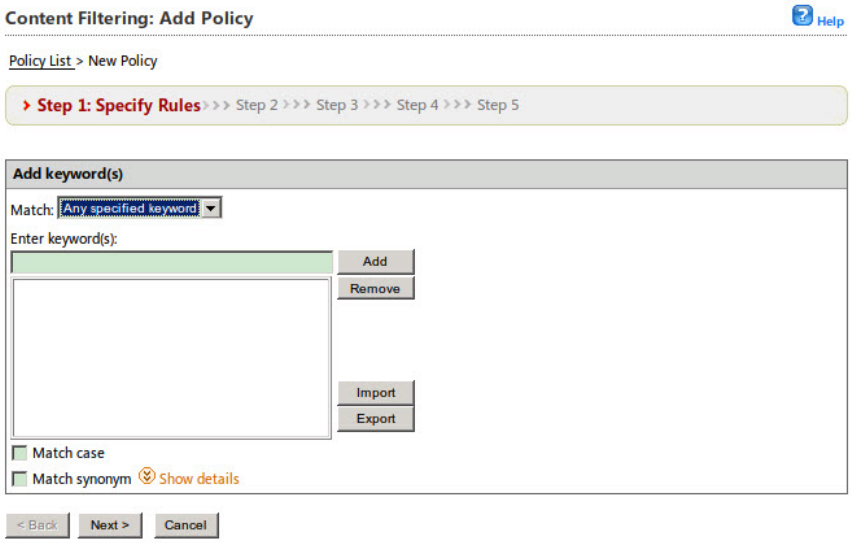


図 6-4. [Content Filtering: Add Policy] > [Step 1: Specify Rules] 画面

3. [Match] ドロップダウンリストから、次のオプションを選択します。
   - Any specified keyword — キーワードのいずれかが検出され一致したときにこのルールが実行されるようにするには、このオプションを選択します。
   - All keyword — すべてのキーワードが検出され一致したときにこのルールが実行されるようにするには、このオプションを選択します。

   注意
   キーワードリストの横にある [Export] または [Import] キーを使用すると、テキストファイル (.txt) との間でキーワードのエクスポートまたはインポートを実行できます。

4. キーワードを追加または削除するには、次の手順を実行します。
   a. [Enter keyword(s)] フィールドにキーワードまたは正規表現を入力して、[Add] をクリックします。

      注意
      PortalProtect での正規表現の使用方法の詳細については、291 ページの正規表現についてを参照してください。

   b. キーワードを削除するには、既存のリストからキーワードを選択し、[Remove] をクリックします。
5. リストされたキーワードの大文字と小文字を区別するには、[Match case] をオンにします。
6. 以下に従って [Match synonym] 設定を指定します。
   a. [Show details] をクリックして、同義語の設定セクションを展開します。
   b. キーワードリストからキーワードを選択して、[Synonyms to exclude] 画面に同義語を表示します。
   c. 1 つ以上の同義語を左側の [Synonyms to include] 画面に移動します。複数を選択するには、<Ctrl> キーを使用します。

7. [Next >] をクリックします。

   [Content Filtering: Add Policy] > [Step 2: Exceptions] 画面が表示されます。

手順 2. [Content Filtering: Add Policy] > [Step 2: Exceptions]

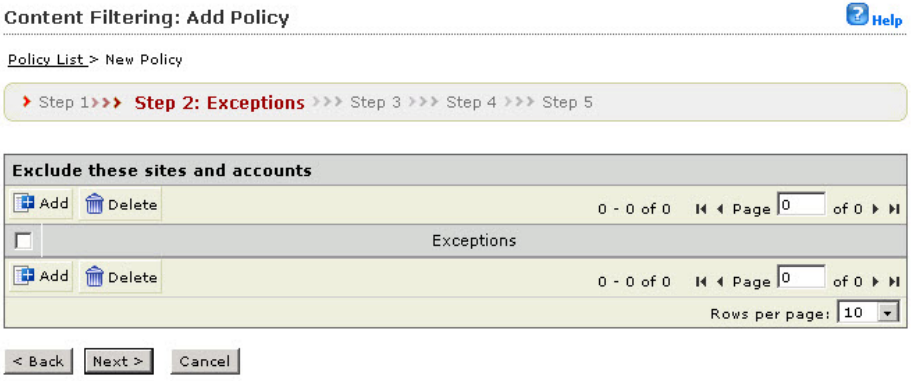


図 6-5. [Content Filtering: Add Policy] > [Step 2: Exceptions] 画面

手順

1. [Step2: Exceptions] 画面で [Add] をクリックします。

[Step 2a: Specify sites to be excluded] 画面が表示されます。

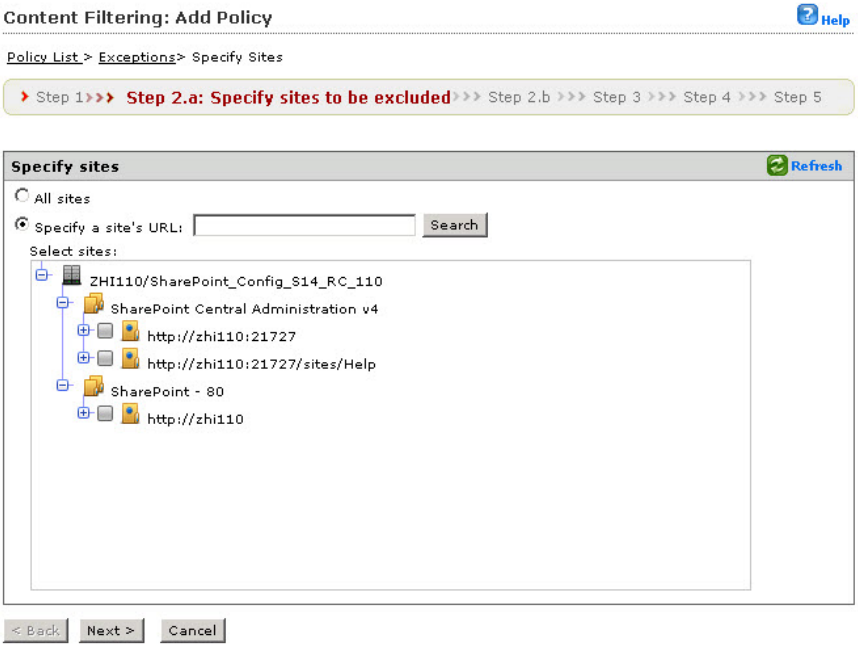


図 6-6. [Content Filtering: Add Policy] > [Step 2.a Specify sites to be excluded] 画面

2. 次のいずれかを選択します。

   • [All sites] を選択した場合

   注意

   [All sites] オプションを指定した場合は、AD ユーザ/グループのみから選択できます。

   [Next >] をクリックして、ステップ 3 に進みます。

   • [Specify a site's URL] を選択した場合

注意

[Specify a site's URL] オプションを指定した場合は、AD ユーザ/グループと SharePoint ユーザ/グループの両方から選択できます。選択するには、[Search for] ドロップダウンを使用します。

a. [Specify a site's URL] フィールドに URL を入力し、[Search] をクリックします。

b. [Select sites] のツリーで、このポリシーから除外する特定のサイトを選択します。

c. [Next >] をクリックして、ステップ 3 に進みます。

3. [Next >] をクリックします。

[Step 2b: Specify accounts to be excluded] 画面が表示されます。

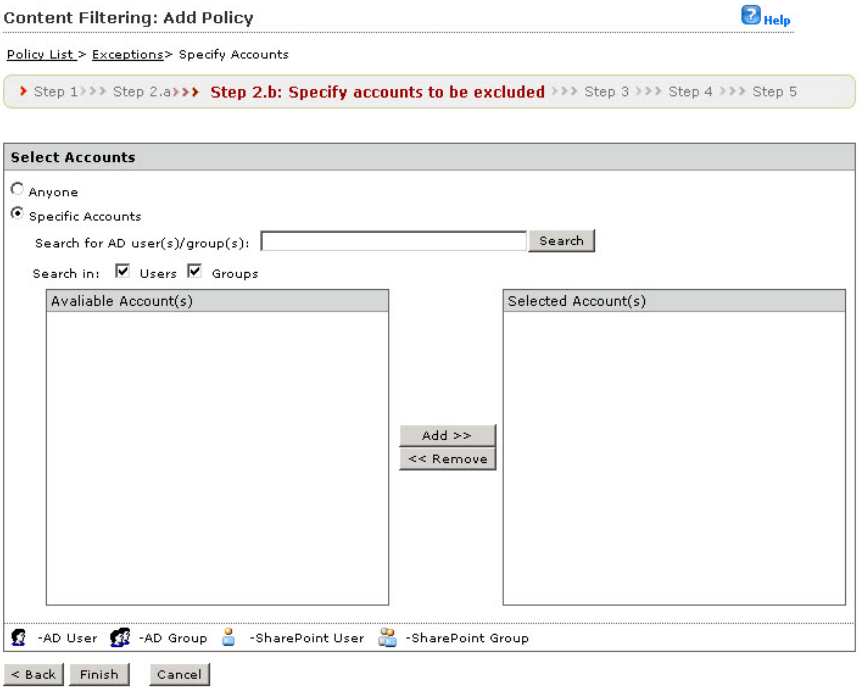


図 6-7. [Content Filtering: Add Policy] > [Step 2.b Specify accounts to be excluded] 画面

4. 次のオプションから選択します。
   - Anyone — すべてのアカウントを除外する場合に選択します。選択し、[Finish] をクリックして、次の手順に進みます。
   - Specific accounts — 特定のアカウントを選択する場合に使用し、次の手順に進みます。
5. AD ユーザまたはグループの名前を [Search for AD user(s)/group(s)] フィールドに入力します。

注意

[Specify a site's URL] オプションを指定した場合は、AD ユーザ/グループと SharePoint ユーザ/グループの両方から選択できます。選択するには、[Search for] ドロップダウンを使用します。

6. [Search in] の横にある [Users] または [Groups]、あるいは両方を適宜選択します。
7. [Search] をクリックします。

   検索の結果は、[Available Account(s)] 画面に表示されます。
8. 必要に応じて検索を繰り返します。
9. 除外対象とするユーザ/グループをすべて選択し、[Add] をクリックして、[Selected Account(s)] 画面に移動します。
10. [Finish] をクリックします。

    [Step 2: Exceptions] 画面が表示されます。
11. 追加または編集した除外設定を選択して、[Next >] をクリックします。

    [Step 3: Action] 画面が表示されます。

手順 3. [Content Filtering: Add Policy] > [Specify Action]

手順

1. 次のいずれかのオプションから、コンテンツフィルタポリシーの処理を選択します。
   - [Block] または [Pass]
   - [Notify] または [Do not notify]
   - [Next >] をクリックします。

手順 4. [Content Filtering: Add Policy] > [Specify Notification]

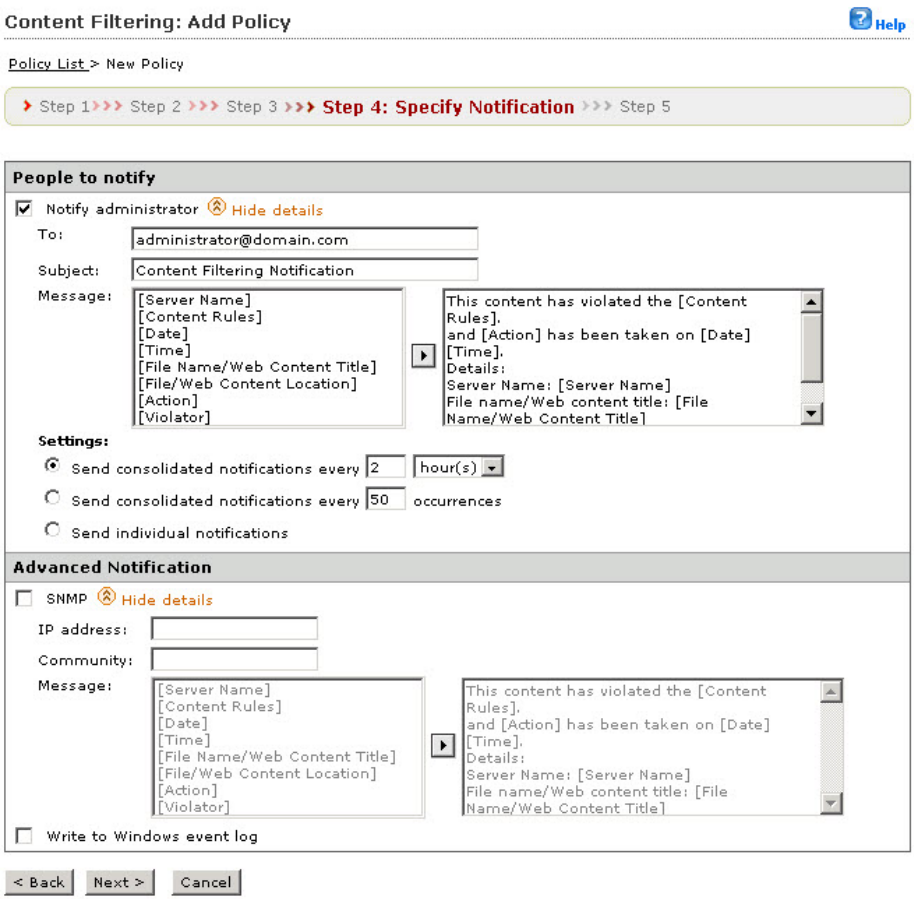


図 6-8. [Content Filtering: Add Policy] > [Step 4: Specify Notification] 画面

手順

1. [Notify administrator] をオンにして、このコンテンツフィルタポリシーの通知を有効にします。

2. [People to notify] の下の [Show details] をクリックして展開し、次を設定します。

   - To — グローバルメールアドレスがこのフィールドに 表示されます。追加のメールアドレスはセミコロンで区切って入力して、独自の通知を作成します。
   - Subject — メールの件名の行に表示される件名を入力します (例: Content Filtering Notification)。
   - Message — 変数を使用して独自のメッセージを作成できます (変数の例: [Server Name]、[Content Rules]、[Date]、[Time]、[File Name/Web Content Title]、[File/Web Content Location]、[Action]、[Violator])。

   注意

   使用可能な変数は左側の画面に表示され、本文は右側の画面に表示されます。

3. [Settings] の下で、次に応じて通知の配信オプションを選択します。

   - Send consolidated notifications every [xx] [hours or days] — 変数フィールドで入力した時間数または日数ごとに通知を送信する場合、このオプションを選択します。
   - Send consolidated notifications every [xx] occurrences — 変数フィールドで入力した回数発生した後に通知を送信する場合、このオプションを選択します。
   - Send individual notifications — イベントが発生するたびに通知を送信する場合、このオプションを選択します。

4. [Advanced Notification] の下で、[SNMP] を選択してこのオプションを有効にします。
5. [Show details] をクリックしてオプションを展開し、次に応じて設定を行います。

   - IP Address
   - Community

- Message — この手順のステップ 2 で説明したメッセージを作成します。

6. [Write to Windows event log] を選択すると、それぞれの通知を Windows イベントログに書き込みます。
7. [Next >] をクリックします。

手順 5. [Content Filtering: Add Policy] > [Name and Priority]

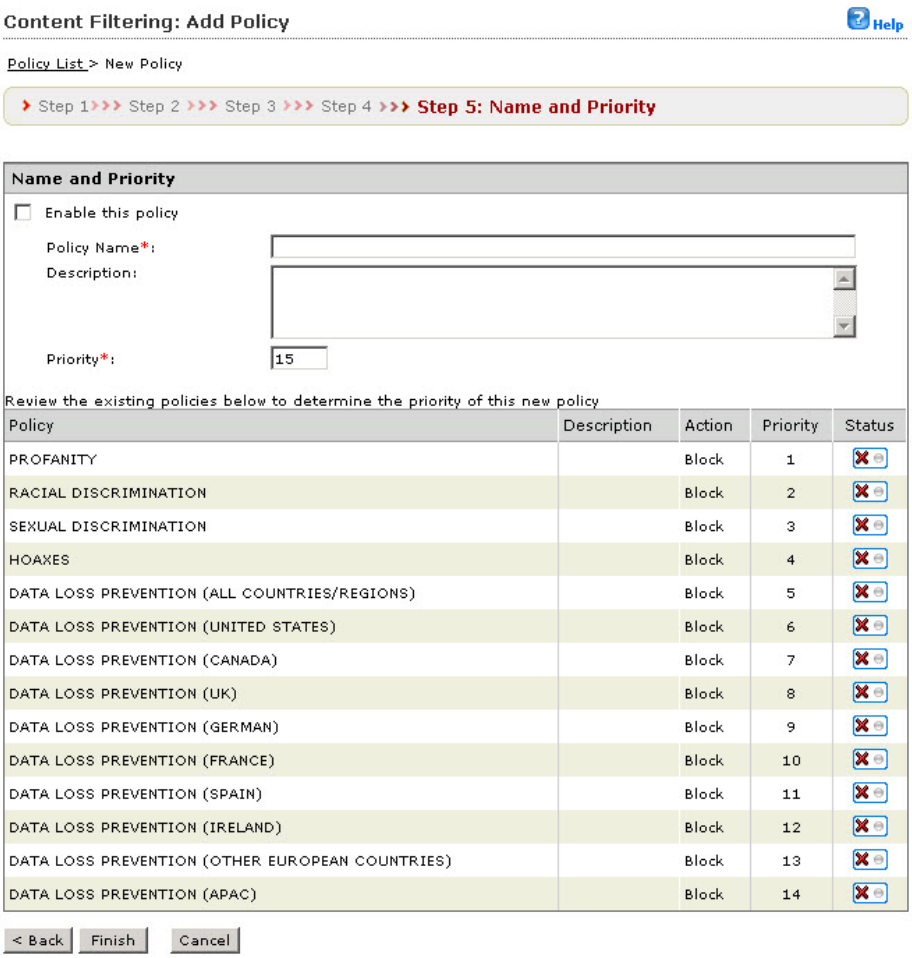


図 6-9. [Content Filtering: Add Policy] > [Step 5: Name and Priority] 画面

手順

1. [Enable this policy] を選択して、有効にします。

2. [Policy name] フィールドにポリシーの名前を入力します。
3. [Priority] フィールドにポリシーの優先順位を入力します。

ヒント

その他のポリシーの優先順位および設定は、既存のポリシーを確認する画面で確認できます。

4. [Finish] をクリックします。

   [Content Filtering] メイン画面が表示され、指定した優先順位で新しいポリシーが表示されます。

コンテンツフィルタポリシーの編集

ここでは、コンテンツフィルタポリシーを編集するために必要な手順を説明します。

手順

1. 左側のメニューで、[Content Filtering] をクリックします。

   [Content Filtering] 画面が表示されます。
2. [Content Filtering] 画面で、編集するポリシー名をクリックします。

[Content Filtering: Edit Policy] 画面が表示されます。

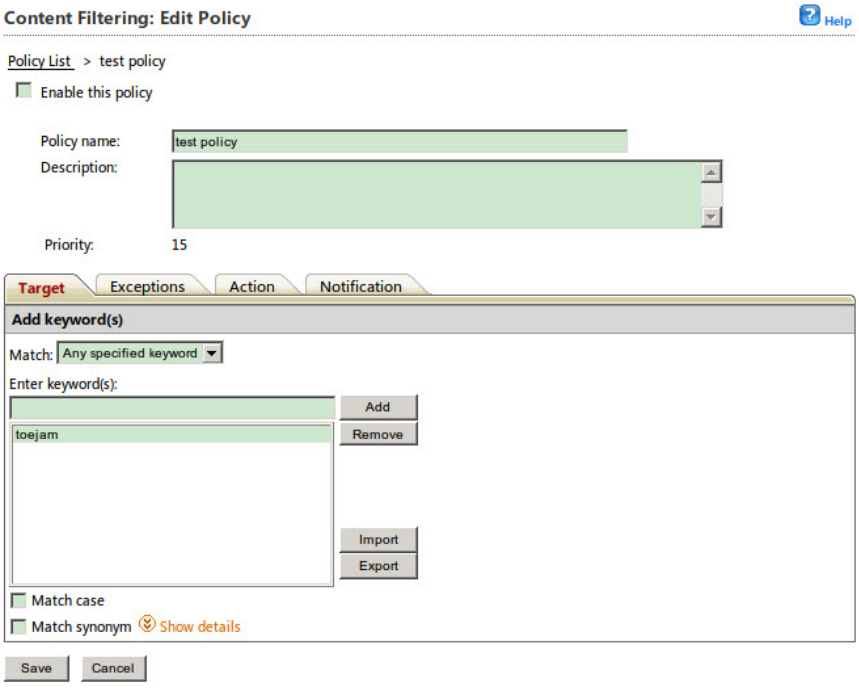


図 6-10. [Content Filtering: Edit Policy] 画面 ([Target] タブ)

3. [Enable this policy] チェックボックスをオンまたはオフにして、ポリシーを有効/無効にします。
4. 必要に応じて以下を編集します。
   - Policy name
   - Description
5. [Target] タブをクリックし、[Match] ドロップダウンから次のオプションを選択します。
   - Any specified keyword — キーワードのいずれかが検出され一致したときにこのルールが実行されるようにするには、このオプションを選択します。

- All keyword — すべてのキーワードが検出され一致したときにこのルールが実行されるようにするには、このオプションを選択します。

注意

キーワードリストの横にある [Export] または [Import] キーを使用すると、テキストファイル (.txt) との間でキーワードのエクスポートまたはインポートを実行できます。

6. キーワードを追加または削除するには、次の手順を実行します。
   a. [Enter keyword(s)] フィールドにキーワードまたは正規表現を入力して、[Add] をクリックします。

注意

PortalProtect での正規表現の使用方法の詳細については、291 ページの正規表現についてを参照してください。

   b. キーワードを削除するには、既存のリストからキーワードを選択し、[Remove] をクリックします。
7. リストされたキーワードの大文字と小文字を区別するには、[Match case] をオンにします。
8. 以下に従って [Match synonym] 設定を指定します。
   a. [Show details] をクリックして、同義語の設定セクションを展開します。
   b. キーワードリストからキーワードを選択して、[Synonyms to exclude] 画面に同義語を表示します。
   c. 1 つ以上の同義語を左側の [Synonyms to include] 画面に移動します。複数を選択するには、<Ctrl> キーを使用します。
9. [Exceptions] タブをクリックして、必要に応じて除外設定を追加または編集します。

   詳細については、101 ページの「手順 2. [Content Filtering: Add Policy] > [Step 2: Exceptions]」を参照してください。

10. [Action] タブをクリックして、以下から選択します。
    - Block
    - Pass
    - Notify
    - Do not notify
11. [Notification] タブをクリックして、適切な設定を選択します。

    詳細については、106 ページの「手順 4. [Content Filtering: Add Policy] > [Specify Notification]」を参照してください。
12. [Save] をクリックします。

第 7 章

情報漏えい対策

本章では、SharePoint 環境を保護するための情報漏えい対策の設定方法について説明します。

本章の内容は次のとおりです。

情報漏えい対策について

データ漏えいの蔓延と悪影響から環境を守るため、現在、各組織はデジタル資産の保護をセキュリティインフラストラクチャの 重要な要素として位置付けています。

情報漏えい対策は、組織の機密データを過失または故意による漏えいから保護します。情報漏えい対策により、次のことが可能になります。

- 保護を必要とする機密情報のデータ識別子を使用した特定
- メールや外部デバイスなどの一般的なチャネルを通じてデジタル資産を伝達することを制限または防止するポリシーの作成
- 制定されたプライバシー基準の遵守

機密情報の漏えいの危険性を監視するには、まず次の点について確認する必要があります。

- どのデータを無許可のユーザから保護する必要があるか。
- 機密データはどこにあるか。
- 機密データはどのような方法で送受信されるか。
- どのユーザが機密データへのアクセスや機密データの送信を許可されているか。
- セキュリティ違反が発生した場合にどのような処理を実行する必要があるか。

この重要な監査では、通常、複数の部署や、組織の機密情報に詳しいユーザを対象にします。

機密情報とセキュリティポリシーをすでに定義している場合は、データ識別子および企業ポリシーの定義を開始できます。

データ識別子の種類

デジタル資産とは、組織が無許可の転送から保護する必要のあるファイルやデータのことです。デジタル資産は次のデータ識別子を使用して管理者が定義します。

- パターン: 一定の構造を持つデータ。

  詳細については、117 ページの「パターン」 を参照してください。

- キーワードリスト: 特殊な語句のリスト。

  詳細については、122 ページの「キーワード」 を参照してください。

注意

情報漏えい対策 (DLP) テンプレートで使用しているデータ識別子は削除できません。データ識別子を削除する前に、テンプレートを削除してください。

パターン

パターンは特定の構造を持つデータです。たとえば、クレジットカード番号の多くは 16 桁の「nnnn-nnnn-nnnn-nnnn」という形式で表現されるため、パターンによる検出に適しています。

事前定義済みのパターンとカスタマイズしたパターンを使用できます。

詳細については、117 ページの「事前定義済みのパターン」および 117 ページの「カスタマイズしたパターン」を参照してください。

事前定義済みのパターン

情報漏えい対策では、あらかじめトレンドマイクロで定義したパターンが用意されています。これらのパターンは、変更や削除ができません。

これらのパターンは、パターンマッチングと数学的な等式を使用して検証されます。機密と考えられるデータがパターンに一致すると、そのデータに対してさらに検証チェックが実行されることもあります。

事前定義済みのパターンの全リストについては、こちらを参照してください。

カスタマイズしたパターン

事前定義済みパターンに該当しないパターンを利用したい場合は、カスタマイズしたパターンを作成し、利用することができます。

パターンは強力な文字列照合ツールです。パターンを作成する前に、以下の注意点をご確認ください。パターンの善し悪しが性能に大きく影響する場合があります。

パターンを作成する際の注意:

- 有効なパターンを定義するための参考として事前定義済みのパターンを参照してください。たとえば、日付を含むパターンを作成する場合は、「日付」に事前定義されたパターンを参照してください。
- 情報漏えい対策は Perl 互換正規表現 (PCRE) で定義されたパターン形式に準拠しています。PCRE の詳細については、次の Web サイトを参照してください。

  http://www.pcre.org/
- 単純なパターンから始めてください。不正なアラームが発生した場合にパターンを修正したり、検出率を高めるためにパターンを調整したりします。

パターンを作成するときには、いくつかの条件の中から選択できます。パターンに選択した条件を満たすデータだけが、情報漏えい対策ポリシーの適用対象となります。各条件オプションの詳細については、118 ページの「カスタマイズしたパターンの条件」を参照してください。

カスタマイズしたパターンの条件

表 7-1. カスタマイズしたパターンの条件オプション

条件	ルール	例
なし	-	すべて : 米国勢調査局発行の名前 • パターン:[^\w]([A-Z][a-z]{1,12}(\s?,\s?[\s]|\s([A-Z])\.\s)[A-Z][a-z]{1,12})[^\w]

条件	ルール	例
特定の文字	パターンには、指定した文字が含まれている必要があります。 さらに、パターンの文字数は、最小文字数以上、最大文字数以下である必要があります。	米国 - ABA 銀行ルーティング番号 • パターン:[^\d]([0123678]\d{8})[^\d] • 文字: 0123456789 • 最小文字数: 9 • 最大文字数: 9
サフィックス	サフィックスはパターンの最終セグメントを意味します。サフィックスには、指定された文字と特定の文字数が含まれている必要があります。 さらに、パターンの文字数は、最小文字数以上、最大文字数以下である必要があります。	すべて - 自宅住所 • パターン:\D(\d+\s[a-z.]+\s([a-z]+\s){0,2} (lane|ln|street|st|avenue|ave|road|rd|place|pl|drive|dr|circle| cr|court|ct|boulevard|blvd)\.?[0-9a-z,#\s\.]{0,30}[\s|,][a-z]{2}\ s\d{5}(-\d{4})?)[^\d-] • サフィックス文字: 0123456789- • 文字数: 5 • パターンの最小文字数: 25 • パターンの最大文字数: 80
単一のセパレータ文字	パターンは 2 つのセグメントで構成し、1 つの文字で区切る必要があります。文字は 1 バイト長にする必要があります。 さらに、セパレータ文字の左側の文字数は下限値と上限値の範囲に収める必要があります。セパレータ文字の右側の文字数は上限値を超えないようにする必要があります。	すべて - メールアドレス • パターン:[^\w.]([\w\.]{1,20}@[a-z0-9]{2,20}[\.][a-z]{2,5}[a-z\.]{0,10})[^\w.] • セパレータ: @ • 左側の最小文字数: 3 • 左側の最大文字数: 15 • 右側の最大文字数: 30

カスタマイズしたパターンの作成

手順

1. Data Loss Prevention > Data Identifiers に移動します。
2. [パターン] タブをクリックします。
3. [追加] をクリックします。

   新しい画面が表示されます。
4. 256 文字以内でキーワードリスト名を入力します。
5. 256 文字以内で説明を入力します。
6. 表示するデータを入力します。

   たとえば、ID 番号に関するパターンを作成する場合は、サンプル ID 番号を入力します。このデータは、参照目的にのみ使用し、製品内の他の場所には表示されません。
7. 次の条件のいずれかを選択して、その条件に合わせて追加の設定値を指定します (118 ページの「カスタマイズしたパターンの条件」を参照)。
   - なし
   - 特定の文字
   - サフィックス
   - 単一のセパレータ文字
8. オプション:パターンの検証機能を選択します。

   注意

   データ単位は意味規則に準拠します。すべての 9 桁の数字が有効な社会保障番号となるわけではなく、すべての 15 桁または 16 桁の数字が有効なクレジットカード番号となるわけではありません。誤検出を少なくするため、パターンの検証ツールでは、抽出されたデータ単位がこのようなルールに準拠するかどうかを確認します。
9. 実際のデータでパターンをテストします。

[テストデータ] テキストボックスに有効な値を入力して [テスト] をクリックし、結果を確認します。

10. 目的の結果であれば、[保存] をクリックします。

注意

テストが成功した場合にのみ設定を保存します。データを検出できないパターンは、システムリソースを浪費し、性能に影響を与える可能性があります。

カスタマイズしたパターンのインポート

このオプションは、パターンを含む正しい形式の `.xml` ファイルがある場合に使用します。このファイルは、PortalProtect 管理コンソールからパターンをエクスポートして生成できます。

手順

1. Data Loss Prevention > Data Identifiers に移動します。
2. [パターン] タブをクリックします。
3. [インポート] をクリックして、パターンが含まれている `.xml` ファイルを指定します。
4. [開く] をクリックします。

   インポートが成功したかどうかを示すメッセージが表示されます。

注意

カスタマイズしたパターンは、すべて.xml ファイルの name フィールドで識別されます。この名前は一意の内部名であり、管理コンソールには表示されません。

ファイルにカスタマイズしたパターンがすでに含まれている場合は、PortalProtect が既存のパターンを上書きします。ファイルに事前定義されたパターンが含まれている場合、PortalProtect は事前定義されたパターンをスキップし、残りのカスタマイズしたパターンをインポートします。

キーワード

キーワードは特殊な単語または語句です。関連するキーワードをキーワードリストに追加することで、特定の種類のデータを識別できます。たとえば、「予後」、「血液型」、「予防接種」、および「医師」は診断書で使用されるキーワードです。診断書ファイルの転送を禁止したい場合は、情報漏えい対策ポリシーでこれらのキーワードを使用し、これらのキーワードを含むファイルをブロックするように情報漏えい対策を設定できます。

よく使用される単語を組み合わせて意味のあるキーワードを形成できます。たとえば、「end」、「read」、「if」、および「at」を組み合わせて、「END-IF」、「END-READ」、「AT END」などのソースコードで見られるキーワードを形成できます。

事前定義済みのキーワードリストとカスタマイズしたキーワードリストを使用できます。詳細については、122 ページの「事前定義済みのキーワードリスト」および 123 ページの「カスタマイズしたキーワードリスト」を参照してください。

事前定義済みのキーワードリスト

情報漏えい対策には、事前定義済みのキーワードリストが付属しています。これらのキーワードリストは、変更や削除ができません。リストにはそれぞれ固有の条件が組み込まれており、テンプレートに照らしてポリシー違反と見なすかどうかを判別します。

情報漏えい対策の事前定義済みキーワードリストの詳細については、次の Web サイトを参照してください。

http://tmqa.jp/dlp_list

カスタマイズしたキーワードリスト

どの事前定義済みのキーワードリストも要件を満たさない場合は、カスタマイズしたキーワードリストを作成します。

キーワードリストを設定するときに選択可能な条件がいくつかあります。キーワードリストは、情報漏えい対策によるポリシーの適用に関係なく、選択した条件を満たす必要があります。キーワードリストごとに次の条件のいずれかを選択します。

- いずれかのキーワード
- すべてのキーワード
- <x> 文字以下のすべてのキーワード
- キーワードの合計スコアがしきい値を超過

条件のルールの詳細については、123 ページの「カスタマイズしたキーワードリストの条件」を参照してください。

カスタマイズしたキーワードリストの条件

表 7-2. キーワードリストに関する条件

条件	ルール
いずれかのキーワードと一致	ファイルには、キーワードリスト内の 1 つ以上のキーワードが含まれている必要があります。
すべてのキーワード	ファイルには、キーワードリスト内のすべてのキーワードが含まれている必要があります。

条件	ルール
<x> 文字以下のすべてのキーワード	ファイルには、キーワードリスト内のすべてのキーワードが含まれている必要があります。さらに、あるキーワードから次のキーワードまでの長さが<x>文字以内である必要があります。 たとえば、WEB、DISK、および USB の 3 つのキーワードがあり、指定した文字数が 20 であるとします。 情報漏えい対策で DISK、WEB、USB の順ですべてのキーワードが検出された場合は、「D」(DISK) から「W」(WEB) までの文字数と「W」から「U」(USB) の文字数が 20 文字以下である必要があります。 次のデータはこの条件を満たします。DISK####WEB############USB 次のデータはこの条件を満たしません。 DISK******************WEB****USB (「D」と「W」の間が 23 文字) この文字数を小さくすると (10 など) 検索時間は短くなりますが、検出範囲は制限される傾向にあります。これは、特に大きなファイルで、機密データが検出される確率が低下します。数字を大きくするほど、対象範囲も広がりますが、検索時間は長くなります。
キーワードの合計スコアがしきい値を超過	ファイルには、キーワードリスト内の 1 つ以上のキーワードが含まれている必要があります。1 つのキーワードしか検出されなかった場合は、そのスコアがしきい値を上回っている必要があります。複数のキーワードが存在する場合は、それらの合計スコアがしきい値を上回っている必要があります。 キーワードごとに 1 ～ 10 のスコアを割り当てます。人事部門での「昇給」など、機密性の高い単語または語句には比較的高いスコアを割り当てる必要があります。それ自体にあまり意味のない単語または語句には低いスコアを割り当てることができます。 しきい値を設定するときに、キーワードに割り当てたスコアを考慮します。たとえば、5 つのキーワードがあり、そのうちの 3 つのキーワードの優先順位が高い場合は、しきい値を優先順位の高い 3 つのキーワードの合計スコア以下にします。これは、ファイルからこの 3 つのキーワードが検出された場合に、機密扱いの対象として十分であることを意味します。

キーワードリストの作成

手順

1. Data Loss Prevention > Data Identifiers に移動します。

2. [キーワードリスト] タブをクリックします。
3. [追加] をクリックします。

   新しい画面が表示されます。
4. 長さが 256 文字を超えないようにキーワードリスト名を入力します。
5. 長さが 256 文字を超えないように説明を入力します。
6. 次の条件のいずれかを選択して、その条件に合わせて追加の設定値を指定します。
   - 任意のキーワード
   - すべてのキーワード
   - <x> 文字以下のすべてのキーワード
   - キーワードの合計スコアがしきい値を超過
7. キーワードを手動でリストに追加するには
   a. 3〜40 文字の長さのキーワードを入力し、大文字と小文字を区別するかどうかを指定します。
   b. [追加] をクリックします。
8. キーワードを編集するには、リスト内のキーワードをクリックし、[キーワード] テキストボックスで編集して、[アップデート] をクリックします。
9. キーワードを削除するには、そのキーワードを選択して、[削除] をクリックします。
10. [保存]をクリックします。

キーワードリストのインポート

このオプションは、キーワードリストを含む正しい形式の.xml ファイルがある場合に使用します。このファイルは、PortalProtect 管理コンソールからキーワードリストをエクスポートして生成できます。

手順

1. Data Loss Prevention > Data Identifiers に移動します。
2. [キーワード] タブをクリックします。
3. [インポート] をクリックして、キーワードリストが含まれている.xml ファイルを指定します。
4. [開く] をクリックします。

   インポートが成功したかどうかを示すメッセージが表示されます。

注意

カスタマイズされたキーワードリストは、すべて.xml ファイルの name フィールドで識別されます。この名前は一意の内部名であり、管理コンソールには表示されません。

ファイルにカスタマイズされたキーワードリストがすでに含まれている場合は、PortalProtect が既存のキーワードリストを上書きします。ファイルに事前定義されたキーワードリストが含まれている場合、PortalProtect は事前定義されたキーワードリストをスキップし、残りのカスタマイズされたキーワードリストをインポートします。

情報漏えい対策コンプライアンステンプレート

情報漏えい対策コンプライアンステンプレートでは 、データ識別子と論理演算子(And、Or、Except) を組み合わせて条件文を作成します。特定の条件文を満たすファイルまたはデータのみ、情報漏えい対策ポリシーの対象になります。

情報漏えい対策データ識別子を設定している場合は、独自にテンプレートを作成することができます。事前定義されたテンプレートを使用することもできます。詳細については、「127 ページの「カスタマイズした情報漏えい対策テンプレート」」および「127 ページの「事前定義された情報漏えい対策テンプレート」」を参照してください。

注意

情報漏えい対策ポリシーで使用されているテンプレートを削除することはできません。削除する前に、ポリシーからテンプレートを削除してください。

事前定義された情報漏えい対策テンプレート

トレンドマイクロでは、さまざまな規制基準への準拠に使用できる、事前定義されたテンプレートのセットが用意されています。これらのテンプレートを変更または削除することはできません。

事前定義されたすべてのテンプレートの目的と、保護されるデータの例を示す詳細なリストについては、こちらを参照してください。

カスタマイズした情報漏えい対策テンプレート

データ識別子の定義が完了したら、独自のテンプレートを作成します。テンプレートは、データ識別子と、条件文を形成する論理演算子 (And、Or、Except) で構成されます。

条件文と論理演算子の働きと例については、127 ページの「条件文と論理演算子」を参照してください。

条件文と論理演算子

情報漏えい対策は左から右に条件文を評価します。条件文を設定する場合は、論理演算子を慎重に使用してください。論理演算子を間違って使用すると、予期せぬ結果をもたらす不正な条件文になります。

次の表の例を参照してください。

表 7-3. サンプル条件文

条件文	説明と例
[データ識別子 1] および [データ識別子 2] 除外 [データ識別子 3]	ファイルは、[データ識別子 1] と [データ識別子 2] の条件を満たすが、[データ識別子 3] の条件を満たしていない必要があります。 次に例を示します。 ファイルは、[Adobe PDF 文書] であり、[メールアドレス] を含むが、[キーワードリスト内のすべてのキーワード] を含まない必要があります。
[データ識別子 1] または [データ識別子 2]	ファイルは [データ識別子 1] または [データ識別子 2] の条件を満たす必要があります。 例: ファイルは、[Adobe PDF 文書] であるか、[Microsoft Word ドキュメント] である必要があります。
除外 [データ識別子 1]	ファイルは [データ識別子 1] の条件を満たしていない必要があります。 例: ファイルは [マルチメディアファイル] 以外である必要があります。

表の最後の例で示したように、ファイルが条件文内のいずれのデータ識別子の条件も満たさないことが必要な場合は、条件文内の最初のデータ識別子に「除外」演算子を使用できます。ただし、ほとんどの場合、最初のデータ識別子に演算子は使用しません。

テンプレートの作成

手順

1. Data Loss Prevention > DLP Templates に移動します。
2. [追加] をクリックします。

   新しい画面が表示されます。
3. 長さが 256 文字を超えないようにテンプレート名を入力します。

4. 長さが 256 文字を超えないように説明を入力します。
5. データ識別子を選択してから、[追加] アイコンをクリックします。
6. パターンを選択した場合は、出現頻度を入力します。情報漏えい対策がパターンをポリシーの対象とするには、指定された回数だけ出現している必要があります。
7. 定義ごとに論理演算子を選択します。

注意

条件文を設定する場合は、論理演算子を慎重に使用してください。論理演算子を間違って使用すると、予期せぬ結果をもたらす不正な条件文になります。正しい使用例については、127 ページの「条件文と論理演算子」を参照してください。

8. 選択したデータ識別子のリストからデータ識別子を削除するには、ごみ箱アイコンをクリックします。
9. [保存]をクリックします。

テンプレートのインポート

このオプションは、テンプレートを含む正しい形式の.xml ファイルがある場合に使用します。このファイルは、PortalProtect 管理コンソールからテンプレートをエクスポートして生成できます。

手順

1. Data Loss Prevention > DLP Templates に移動します。
2. [インポート] をクリックして、テンプレートが含まれている.xml ファイルを指定します。
3. [開く] をクリックします。

   インポートが成功したかどうかを示すメッセージが表示されます。

注意

カスタマイズされたテンプレートは、すべて.xml ファイルの name フィールドで識別されます。この名前は一意の内部名であり、管理コンソールには表示されません。

ファイルにカスタマイズされたテンプレートがすでに含まれている場合は、PortalProtect が既存のテンプレートを上書きします。ファイルに事前定義されたテンプレートが含まれている場合、PortalProtect は事前定義されたテンプレートをスキップし、残りのカスタマイズされたテンプレートをインポートします。

情報漏えい対策ポリシー

ここでは、情報漏えい対策ポリシーを設定するために必要な手順を説明します。

手順

1. 左側のメニューで、[Data Loss Prevention] > [Policy] をクリックします。

[Data Loss Prevention] 画面が表示されます。

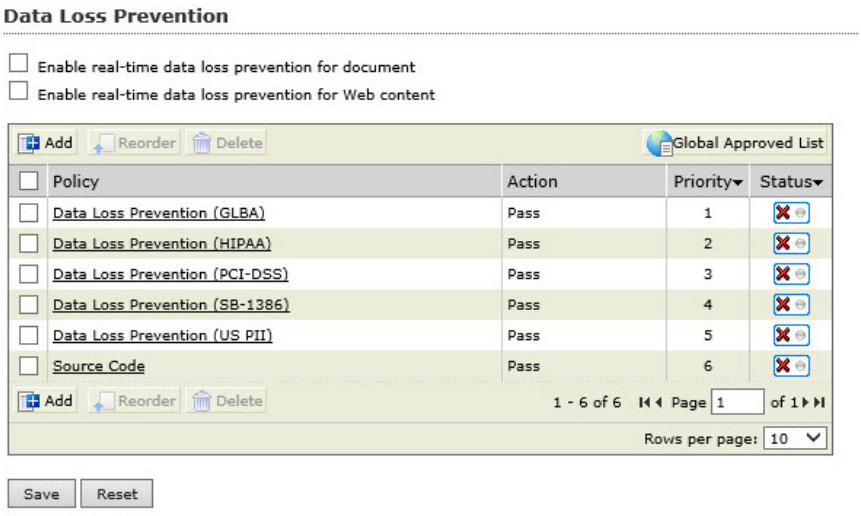


図 7-1. [Data Loss Prevention] メイン画面

2. 次のオプションのいずれかまたは両方を選択します。
   - Enable real-time data loss prevention for document — ドキュメントに対してリアルタイムの情報漏えい対策を実行します。
   - Enable real-time data loss prevention for Web content — Web コンテンツに対して情報漏えい対策を実行します。
3. [Save] をクリックします。

情報漏えい対策ポリシーの追加

ここでは、新しい情報漏えい対策ポリシーを作成するために必要なさまざまな手順を説明します。

手順 1. [Data Loss Prevention: Add Policy] > [Specify Rules]

手順

1. 左側のメニューで、[Data Loss Prevention] > [Policy] をクリックします。

   [Data Loss Prevention] 画面が表示されます。

2. [Add] をクリックします。

   [Data Loss Prevention: Add Policy] > [Step 1: Specify Rules] 画面が表示されます。

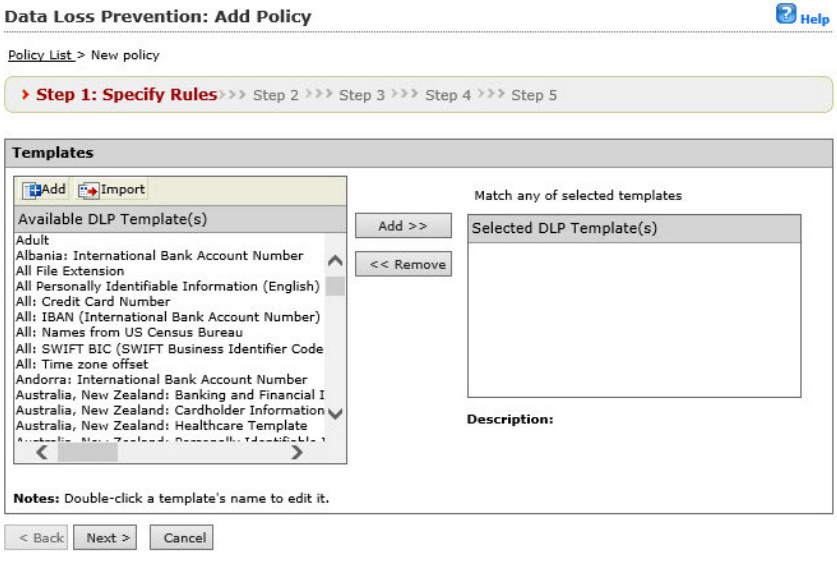


図 7-2. [Data Loss Prevention: Add Policy] > [Step 1: Specify Rules] 画面

3. 追加する情報漏えい対策テンプレートを [Available DLP template (s)] のリストから選択し、[Add >>] をクリックします。情報漏えい対策テンプレートを削除するには、選択して [<< Remove] をクリックします。

注意

複数の情報漏えい対策テンプレートを選択するには、<Ctrl> キーを押しながらクリックします。

情報漏えい対策テンプレートを XML ファイルからインポートするには、[Import] ボタンをクリックします。

4. [Available DLP Template (s)] のリストに情報漏えい対策テンプレートを追加するには、次の手順を実行します。
   a. [Import] ボタンの横にある [Add] ボタンをクリックします。

      [Add Data Loss Prevention Template] 画面が表示されます。
   b. [Name and Description] セクションの [Name:] フィールドに新しいテンプレートの名前を入力します。
   c. [Description] フィールドに必要に応じて新しいテンプレートの説明を入力します。
5. 情報漏えい対策テンプレートを定義するには、次のいずれかの手順を選択して実行します。
   a. [Expressions] を選択した場合

      「US: SSN (Social Security Number)」、「All: Credit Card Number」、または「US: Phone Number」 などリストからパターンを選択します。
   b. [Occurrences] フィールドにポリシーを実行するために必要な出現回数を入力します。
   c. 別の情報漏えい対策テンプレートを追加するには [+] をクリックします。
      1. 適切な演算子 (`[And]` または `[Or]`) を選択します。
      2. [Expressions] を選択し、リストから使用可能な式を 1 つ選択することで前の手順を繰り返します。
      3. [Occurrences] フィールドにポリシーを実行するために必要な出現回数を入力します。
   d. [Keywords] を選択した場合

1. 使用可能なキーワードのリストからいずれかのキーワードを選択します。
2. 別の情報漏えい対策テンプレートを追加するには [+] をクリックします。
3. 適切な演算子 (`[And]` または `[Or]`) を選択します。
4. [Keywords] を選択し、リストから使用可能なキーワードを 1 つ選択することで前の手順を繰り返します。

6. 情報漏えい対策テンプレートの追加が終わったら、[Add] > [Save] の順にクリックします。

   [Data Loss Prevention: Add Policy] > [Step 1: Specify Rules] 画面が表示されます。

7. [Next] をクリックします。

   [Data Loss Prevention: Add Policy] > [Step 2: Exceptions] 画面が表示されます。

手順 2. [Data Loss Prevention: Add Policy] > [Step 2: Exceptions]

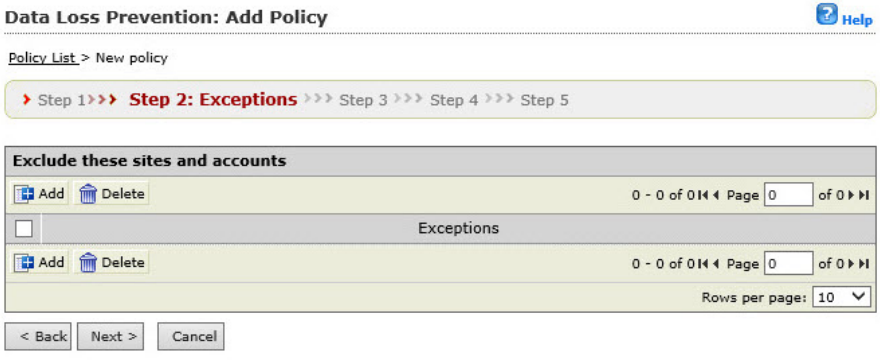


図 7-3. [Data Loss Prevention: Add Policy] > [Step 2: Exceptions] 画面

手順

1. [Step2: Exceptions] 画面で [Add] をクリックします。

   [Step 2a: Specify sites to be excluded] 画面が表示されます。

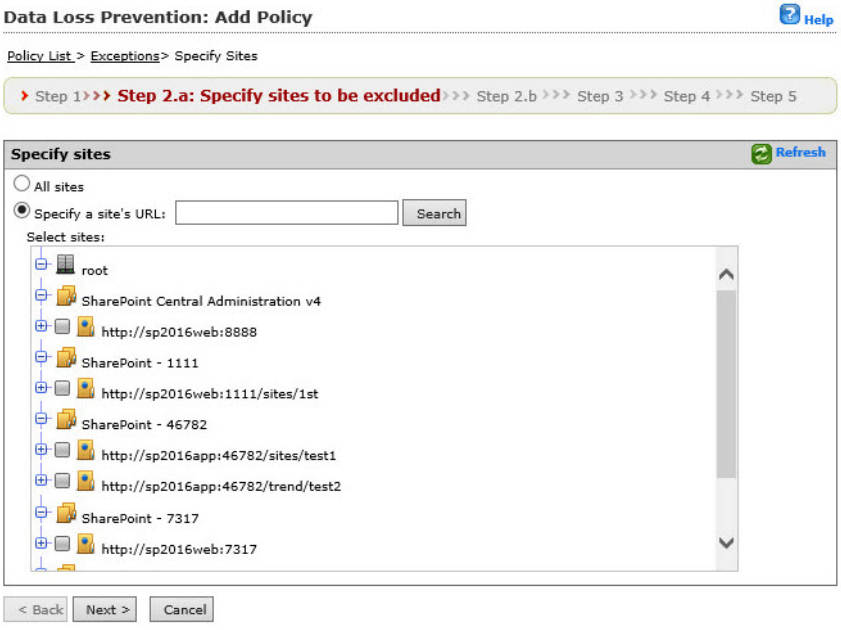


図 7-4. [Data Loss Prevention: Add Policy] > [Step 2.a Specify sites to be excluded] 画面

2. 次のいずれかを選択します。

   [All sites] を選択した場合

> **注意**
> [All sites] オプションを指定した場合は、AD ユーザ/ グループのみから選択できます。

   - [Next] をクリックして、ステップ 3 に進みます。

     [Specify a site's URL] を選択した場合

注意

[Specify a site's URL] オプションを指定した場合は、AD ユーザ/ グループと SharePoint ユーザ/ グループの両方から選択できます。選択するには、[Search for] ドロップダウンを使用します。

- [Specify a site's URL] フィールドに URL を入力し、[Search] をクリックします。
- [Select sites] のツリーで、このポリシーから除外する特定のサイトを選択します。

3. [Next >] をクリックします。

[Step 2b: Specify accounts to be excluded] 画面が表示されます。

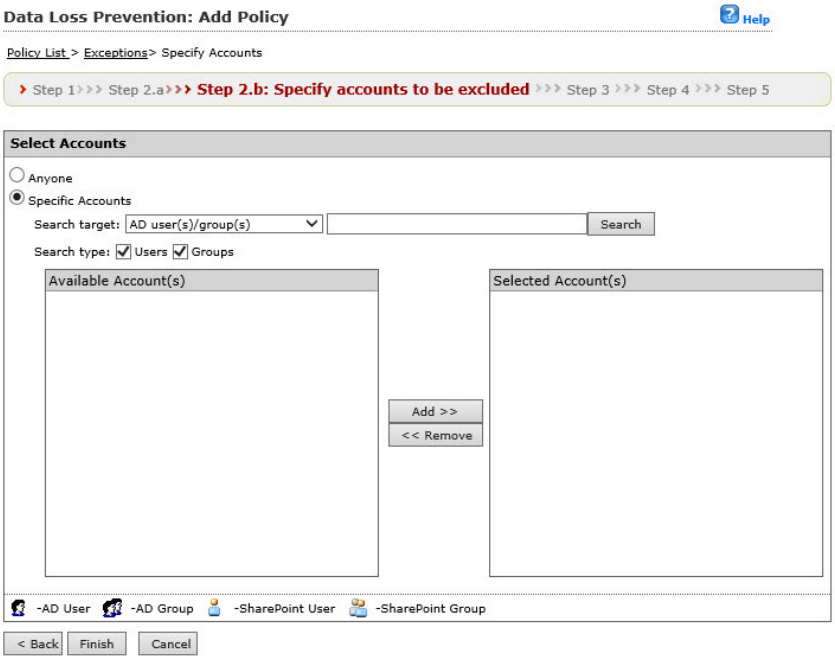


図 7-5. [Data Loss Prevention: Add Policy] > [Step 2.b Specify accounts to be excluded] 画面

4. 次のオプションから選択します。

- Anyone — すべてのアカウントを除外する場合に選択します。[Finish] をクリックして、次の手順に進みます。
- Specific accounts — 特定のアカウントを選択する場合に使用し、次の手順に進みます。

5. AD ユーザまたはグループの名前を [Search for AD user (s) /group (s)] フィールドに入力します。

注意

[Specify a site's URL] オプションを指定した場合は、AD ユーザ/ グループと SharePoint ユーザ/ グループの両方から選択できます。選択するには、[Search for] ドロップダウンを使用します。

6. [Search in] の横にある [Users] または [Groups]、あるいは両方を適宜選択します。
7. [Search] をクリックします。

   検索の結果は、[Available Account (s)] 画面に表示されます。
8. 必要に応じて検索を繰り返します。
9. 除外対象とするユーザ/ グループをすべて選択し、[Add] をクリックして、[Selected Account (s)] 画面に移動します。
10. [Finish] をクリックします。

    [Step 2: Exceptions] 画面が表示されます。
11. 追加または編集した除外設定を選択して、[Next >] をクリックします。

    [Step 3: Action] 画面が表示されます。

手順 3. [Data Loss Prevention: Add Policy] > [Specify Action]

手順

1. 次のいずれかのオプションから、情報漏えい対策ポリシーの処理を選択します。

- [Block] または [Pass]
- [Notify] または [Do not notify]
- [Next >] をクリックします。

手順 4. [Data Loss Prevention: Add Policy] > [Specify Notification]

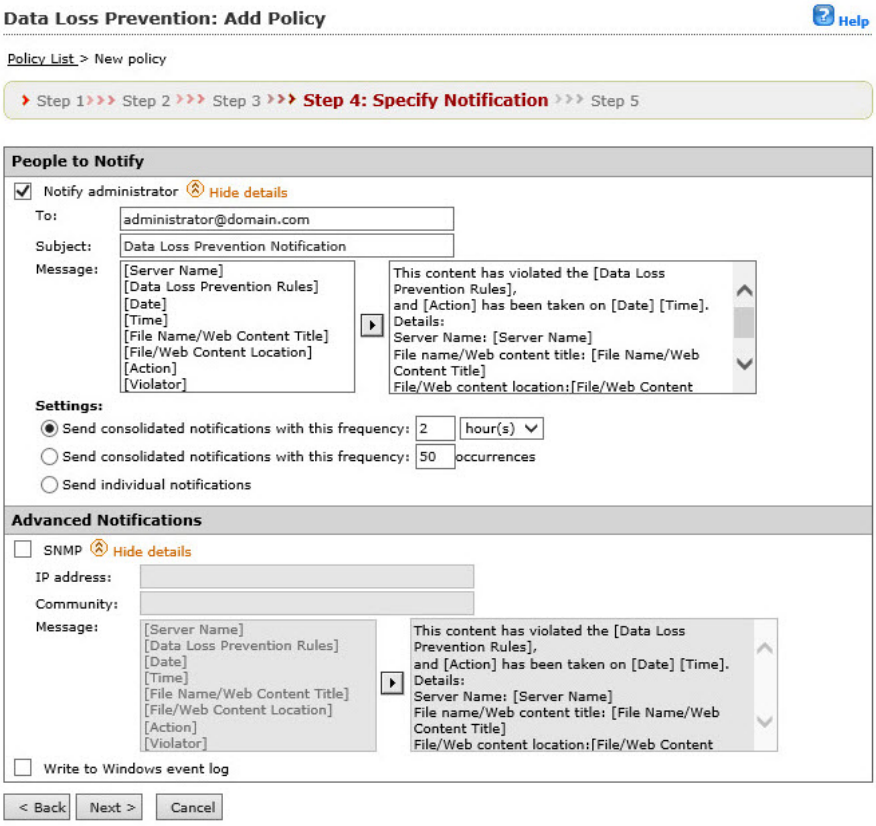


図 7-6. [Data Loss Prevention: Add Policy] > [Step 4: Specify Notification] 画面

手順

1. [Notify administrator] をオンにして、この情報漏えい対策ポリシーの通知を有効にします。
2. [People to notify] の下の [Show details] をクリックして展開し、次を設定します。
   - To — グローバルメールアドレスがこのフィールドに 表示されます。追加のメールアドレスはセミコロンで区切って入力して、独自の通知を作成します。
   - Subject — メールの件名の行に表示される件名を入力します (例: Web Reputation Notification)。
   - Message — 変数を使用して独自のメッセージを作成できます (変数の例: [Server Name]、 [Data Loss Prevention Rules]、[Date]、[Time]、[File Name/Web Content Title]、[File/Web Content Location]、[Action]、[Violator])。

   注意

   使用可能な変数は左側の画面に表示され、本文は右側の画面に表示されます。
3. [Settings] の下で、次に応じて通知の配信オプションを選択します。
   - Send consolidated notifications every [xx] [hours or days] — 変数フィールドで入力した時 間数または日数ごとに通知を送信する場合、このオプションを選択します。
   - Send consolidated notifications every [xx] occurrences — 変数フィールドで入力した回数 発生した後に通知を送信する場合、このオプションを選択します。
   - Send individual notifications — イベントが発生するたびに通知を送信する場合、このオプ ションを選択します。
4. [Advanced Notification] の下で、[SNMP] を選択してこのオプションを有効にします。
5. [Show details] をクリックしてオプションを展開し、次に応じて設定を行います。

- IP Address
- Community
- Message — この手順のステップ 2 で説明したメッセージを作成します。

6. [Write to Windows event log] を選択すると、それぞれの通知を Windows イベントログに書き 込みます。
7. [Next >] をクリックします。

手順 5. [Data Loss Prevention: Add Policy] > [Name and Priority]

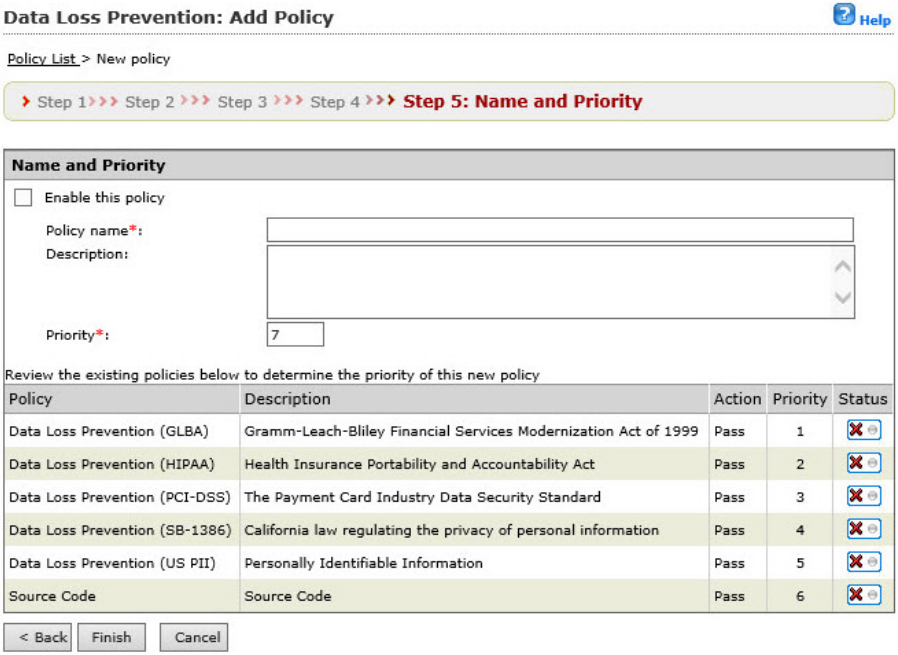


図 7-7. [Data Loss Prevention: Add Policy] > [Step 5: Name and Priority] 画面

手順

1. [Enable this policy] を選択して、有効にします。
2. [Policy name] フィールドにポリシーの名前を入力します。
3. [Priority] フィールドにポリシーの優先順位を入力します。

注意

その他のポリシーの優先順位および設定は、既存のポリシーを確認する画面で確認できます。

4. [Finish] をクリックします。

   [Data Loss Prevention] メイン画面が表示され、指定した優先順位で新しいポリシーが表示されます。

情報漏えい対策ポリシーの編集

ここでは、情報漏えい対策ポリシーを編集するために必要な手順を説明します。

手順

1. 左側のメニューで、[Data Loss Prevention] > [Policy] をクリックします。

   [Data Loss Prevention] 画面が表示されます。
2. [Data Loss Prevention] 画面で、編集するポリシー名をクリックします。

[Data Loss Prevention: Edit Policy] 画面が表示されます。

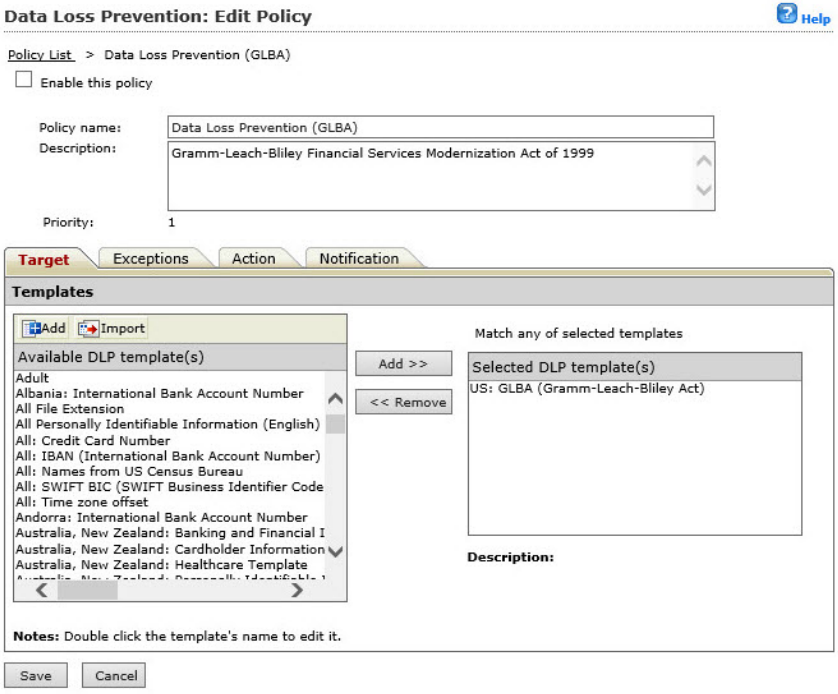


図 7-8. [Data Loss Prevention: Edit Policy] 画面 ([Target] タブ)

3. [Enable this policy] チェックボックスをオンまたはオフにして、ポリシーを有効/ 無効にします。
4. 必要に応じて以下を編集します。
   - Policy name
   - Description
5. [Target] タブをクリックします。
6. 追加する情報漏えい対策テンプレートを [Available DLP template (s)] のリストから選択し、[Add >>] をクリックします。情報漏えい対策テンプレートを削除するには、選択して [<< Remove] をクリックします。

注意

複数の情報漏えい対策テンプレートを選択するには、<Ctrl> キーを押しながらクリックします。

情報漏えい対策テンプレートをテキストファイル (.txt) からインポートするには、[Import] ボタンをクリックします。

7. [Available DLP Template (s)] のリストに情報漏えい対策テンプレートを追加するには、次の手順を実行します。

   a. [Import] ボタンの横にある [Add] ボタンをクリックします。

      [Add Data Loss Prevention Template] 画面が表示されます。

   b. [Name and Description] セクションの [Name:] フィールドに新しいテンプレートの名前を入力します。

   c. [Description] フィールドに必要に応じて新しいテンプレートの説明を入力します。

8. 情報漏えい対策テンプレートを定義するには、次のいずれかの手順を選択して実行します。

   a. [Expressions] を選択した場合

      「US: SSN (Social Security Number)」、「All: Credit Card Number」、または 「US: Phone Number」 などリストからパターンを選択します。

   b. [Occurrences] フィールドにポリシーを実行するために必要な出現回数を入力します。

   c. 別の情報漏えい対策テンプレートを追加するには [+] をクリックします。

      1. 適切な演算子 ([And] または [Or]) を選択します。
      2. [Expressions] を選択し、リストから使用可能な式を 1 つ選択することで前の手順を繰り返します。
      3. [Occurrences] フィールドにポリシーを実行するために必要な出現回数を入力します。

   d. [Keywords] を選択した場合

1. 使用可能なキーワードのリストからいずれかのキーワードを選択します。
2. 別の情報漏えい対策テンプレートを追加するには [+] をクリックします。
3. 適切な演算子 ([And] または [Or]) を選択します。
4. [Keywords] を選択し、リストから使用可能なキーワードを 1 つ選択することで前の手順を繰り返します。

9. 情報漏えい対策テンプレートの追加が終わったら、[Add] > [Save] の順にクリックします。

   [Data Loss Prevention: Edit Policy] > [Target] タブが表示されます。

10. [Exceptions] タブをクリックして、必要に応じて除外設定を追加または編集します。

    詳細については、134 ページの「手順 2. [Data Loss Prevention: Add Policy] > [Step 2: Exceptions]」 を参照してください。

11. [Action] タブをクリックして、以下から選択します。

    - Block
    - Pass
    - Notify
    - Do not notify

12. [Notification] タブをクリックして、適切な設定を選択します。

    詳細については、138 ページの「手順 4. [Data Loss Prevention: Add Policy] > [Specify Notification]」 を参照してください。

13. [Save] をクリックします。

第 8 章

Web レピュテーション

本章では、Web 上の脅威からネットワークとコンピュータを保護するために PortalProtect を設定する方法について説明します。

本章の内容は次のとおりです。

Web レピュテーションについて

このバージョンの PortalProtect は、Web レピュテーションテクノロジを使用して、SharePoint サーバの Web コンテンツとファイルに含まれる URL の整合性を評価します。

Web からの脅威には、インターネットで発生する幅広い脅威が含まれます。Web からの脅威は、単一のファイルやアプローチを利用するのではなく、さまざまなファイルや手法を巧妙に組み合わせて使用しています。たとえば、Web からの脅威の作成者は、使用する脅威のバージョンや種類を絶えず変更しています。Web からの脅威は感染したコンピュータ上ではなく Web サイトの特定の場所に潜んでいるため、作成者は絶えずそのコードを変更して検出を回避しようとします。

Web レピュテーションでは、ページごとのレピュテーションレーティングに基づいてファイルと Web コンテンツがブロックされます。これらのレーティングについて Trend Micro Smart Protection Network にクエリが実行されます。

安全でない URL としてトレンドマイクロが分類した URL を含むファイルや Web コンテンツはブロックされます。また、独自の承認済み URL リストをカスタマイズしたり、このリストに加えたりすることができます。この機能を有効にするには、[Web Reputation] ページで、[Enable real-time Web Reputation for documents] および [Enable real-time Web Reputation for Web content] を選択します。

ローカルおよびグローバル Smart Protection

このバージョンの PortalProtect には、URL のレピュテーションと安全性を判定する 2 つの方法が用意されています。一つはグローバル (外部ネットワーク) の Trend Micro Smart Protection Network、もう一つはローカル (社内ネットワーク) の Smart Protection Server です。グローバル (外部ネットワーク) の Trend Micro Smart Protection Network では、URL のレピュテーションを調べるために Trend Micro Smart Protection Network に要求を送信します。ローカル (社内ネットワーク) の Smart Protection Server では、それらの要求をローカル (社内ネットワーク) の Smart Protection Server に送信します。ローカル (社内ネットワーク) の Smart Protection Server では、守秘性が向上し、さらに処理速度が向上する場合もあります。

ローカル (社内ネットワーク) の Smart Protection Server は、セキュリティリスクや Web 上の脅威から SharePoint 環境を保護するために設計された、次世代の顧客専用クラウド-クライアント型コンテンツセキュリティインフラストラクチャである Trend Micro Smart Protection Network を使用します。より多くの製品、サービス、およびユーザがネットワークにアクセスすれば、それだけ保護機能が自動的に更新および強化されることになり、利用者自身のリアルタイムな自警システムが構築されていきます。スマートスキャンソリューションでは、クラウド内保護のために Trend Micro Smart Protection Network が利用されます。

Web レピュテーションソースの選択

手順

1. 左側のメニューで [Smart Protection] > [Scan Service Settings] をクリックします。

   [Scan Service Settings] 画面が表示されます。

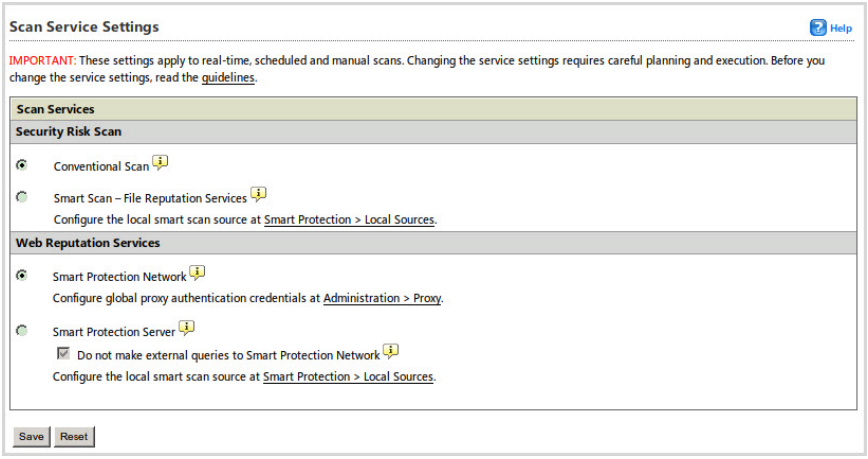


図 8-1. [Scan Service Settings] 画面

2. [Web Reputation] の下で、次のオプションを選択します。

   a. Smart Protection Network: グローバル (外部ネットワーク) の Trend Micro Smart Protection Network からプロキシ経由で URL を検索します。

b. 設定方法の詳細については、[Administration] > [Proxy] のリンクをクリックして 30 ページの「グローバルプロキシサーバ」を参照してください。

c. Smart Protection Server: 専用のスマートスキャンサーバを使用して URL を検索します。

注意

ローカル (社内ネットワーク) の Smart Protection Server で URL のレピュテーションを判定できない場合は、Trend Micro Smart Protection Network へのクエリの実行を許可するオプションを選択できます。[Do not make external queries to Smart Protection Network] チェックボックスをオンにすると、ローカル (社内ネットワーク) のスマートスキャンサーバに対してのみクエリが実行されます。このチェックボックスをオフにすると、PortalProtect から Trend Micro Smart Protection Network へのクエリの実行が可能になります。

d. [Smart Protection] > [Local Sources] リンクをクリックして Smart Protection Server を設定します。この画面での設定方法については、49 ページの「Smart Protection ソース」を参照してください。

3. [Save] をクリックします。

注意

Smart Protection Server が使用できない場合やオンラインに復帰しない場合のアラートを設定する方法の詳細については、234 ページの「警告」を参照してください。

リアルタイム Web レピュテーションの有効化

手順

1. 製品コンソールにログオンします。

2. メインメニューから [Web Reputation] をクリックします。

   [Web Reputation] 画面が表示されます。

3. 次のオプションのいずれかまたは両方を選択します。

   - Enable real-time Web Reputation for document
   - Enable real-time Web Reputation for Web content

4. [Save] をクリックします。

Web レピュテーション: 対象の設定について

ここでは、[Web Reputation] 画面の [Target] タブで利用できるオプションについて簡単に説明します。

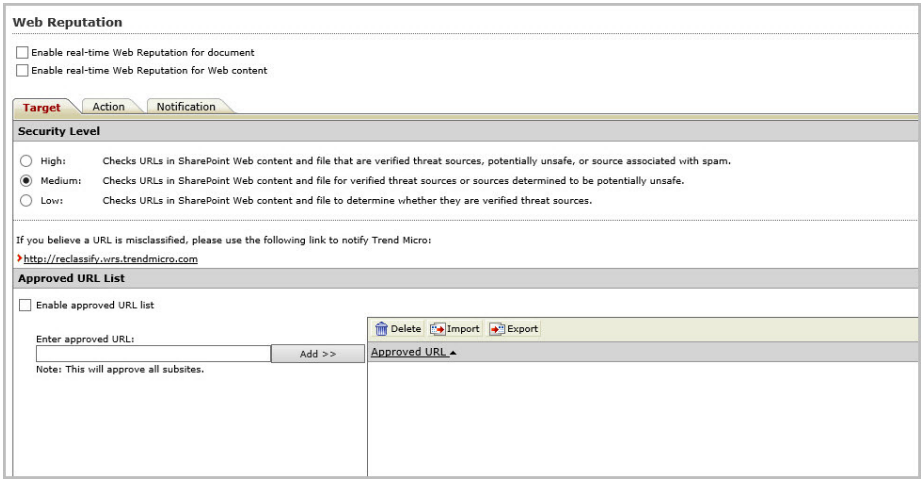


図 8-2. [Web Reputation] の [Target] タブ

- Enable real-time Web Reputation for document: ファイルに対して Web レピュテーションを有効にします。
- Enable real-time Web Reputation for Web content: Web コンテンツに対して Web レピュテーションを有効にします。

- High: Web コンテンツについて、脅威の送信元として検証された URL、安全でない可能性がある URL、またはスパムメールに関連付けられている URL の有無をチェックします。
- Medium: Web コンテンツについて、脅威の送信元として検証された URL または安全でない可能性がある URL の有無をチェックします。
- Low: Web コンテンツについて、脅威の送信元として検証された URL の有無をチェックします。
- https://global.sitesafety.trendmicro.com/index.php?cc=jp: クリックすると、誤って分類されている URL をトレンドマイクロに報告するための新しいページが表示されます。このポータルを使用して、Web サイトのレピュテーションをチェックすることもできます。
- Enable approved URL list: 承認された URL のカスタムリストを使用するには、このチェックボックスをオンにします。
- Enter approved URL: URL を入力します。

ヒント

ネットワーク帯域幅を節約するために、社内 Web サイトを Web レピュテーションの承認 URL リストに追加することをお勧めします。

- Add>>: URL をリストに追加します。
- Delete: URL をリストから削除します。
- Import: URL リストをインポートします。
- Export: URL リストをエクスポートします。
- Approved URL: 昇順または降順で並べ替えます。
- Save: すべての設定を保存します。
- Reset: 初期設定に戻します。

Web レピュテーション: 対象の設定

次に、Web レピュテーションの対象を設定するために必要な手順を示します。

手順

1. 製品コンソールにログオンします。
2. メインメニューから [Web Reputation] をクリックします。

   [Web Reputation] 画面が表示されます。
3. 次のセキュリティレベルのいずれかを選択します。
   - High: Web コンテンツについて、脅威の送信元として検証された URL、安全でない可能性がある URL、またはスパムメールに関連付けられている URL の有無をチェックします。
   - Medium: Web コンテンツについて、脅威の送信元として検証された URL または安全でない可能性がある URL の有無をチェックします。
   - Low: Web コンテンツについて、脅威の送信元として検証された URL の有無をチェックします。
4. [Enable approved URL list] を選択して、現在のセキュリティポリシーで安全と見なされる URL の検索を回避します。
5. 承認する URL をリストに追加します。
6. [Save] をクリックします。

Web レピュテーション: 処理の設定について

ここでは、[Web Reputation] の [Action] タブで利用できるオプションについて簡単に説明します。

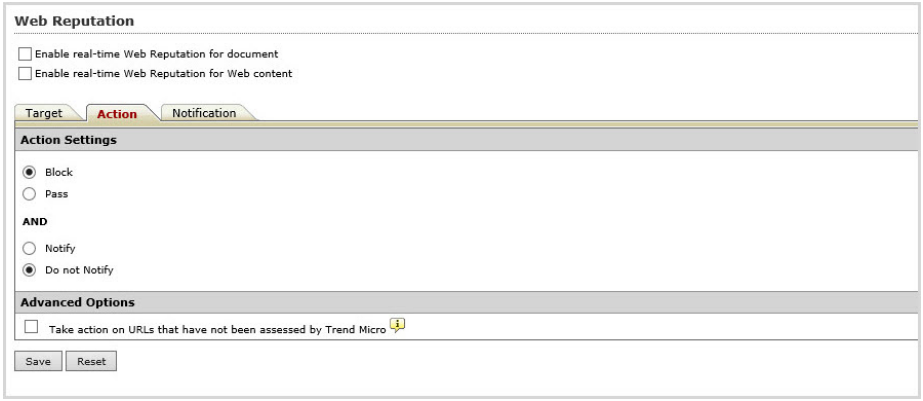


図 8-3. [Web Reputation] の [Action] タブ

- Block
- Pass
- Notify: 通知を送信します。
- Do not notify: 通知を送信しません。
- Take action on URLs that have not been assessed by Trend Micro: 分類されていない URL を疑わしい URL として扱い、指定された処理を実行します。
- Save: 設定を保存します。
- Reset: 初期設定に戻します。

Web レピュテーション: 処理の設定

次に、Web レピュテーションの処理を設定するために必要な手順を示します。

手順

1. 製品コンソールにログオンします。
2. メインメニューから [Web Reputation] をクリックします。

   [Web Reputation] 画面が表示されます。
3. [Action] タブをクリックします。
4. 処理を選択します。
5. 厳密な Web レピュテーションポリシーを適用するには、[Take action on URLs that have not been assessed by Trend Micro] を選択します。
6. [Notify] または [Do not notify] を選択します。
7. [Save] をクリックします。

Web レピュテーション: 通知

ここでは、この画面で使用可能なオプションについて簡単に説明します。

- Notify administrator: 管理者に通知を送信します。
- Show details: 追加のオプションを表示します。
- SNMP: SNMP で通知を送信します。
- Write to Windows event log: Windows のイベントログに通知を記録します。
- Save: 設定を保存します。
- Reset: 初期設定に戻します。

Trend Micro Smart Protection Network

Trend Micro Smart Protection Network はトレンドマイクロが管理するサーバとインターネットクラウドテクノロジで 構成され、Web およびファイルレピュテーションにおいて独自のインターネットクラウド相関分析テクノロジ、および脅威データベースを提供しています。より多くの製品、サービス、およびユーザがネットワークにアクセスすれば、それだけ保護機能が自動的

に更新および強化されることになり、ユーザのリアルタイムな自警システムが構築されていきます。

第 9 章

手動検索

手動検索はいつでも実行できます。予約検索の実行中に手動検索を実行すると、手動検索が優先されます。

本章の内容は次のとおりです。

手動検索の設定

ここでは、手動検索を設定するために必要な手順を説明します。

手順

1. 左側のメニューで、[Manual Scan] をクリックします。

[Manual Scan] 画面が表示されます。

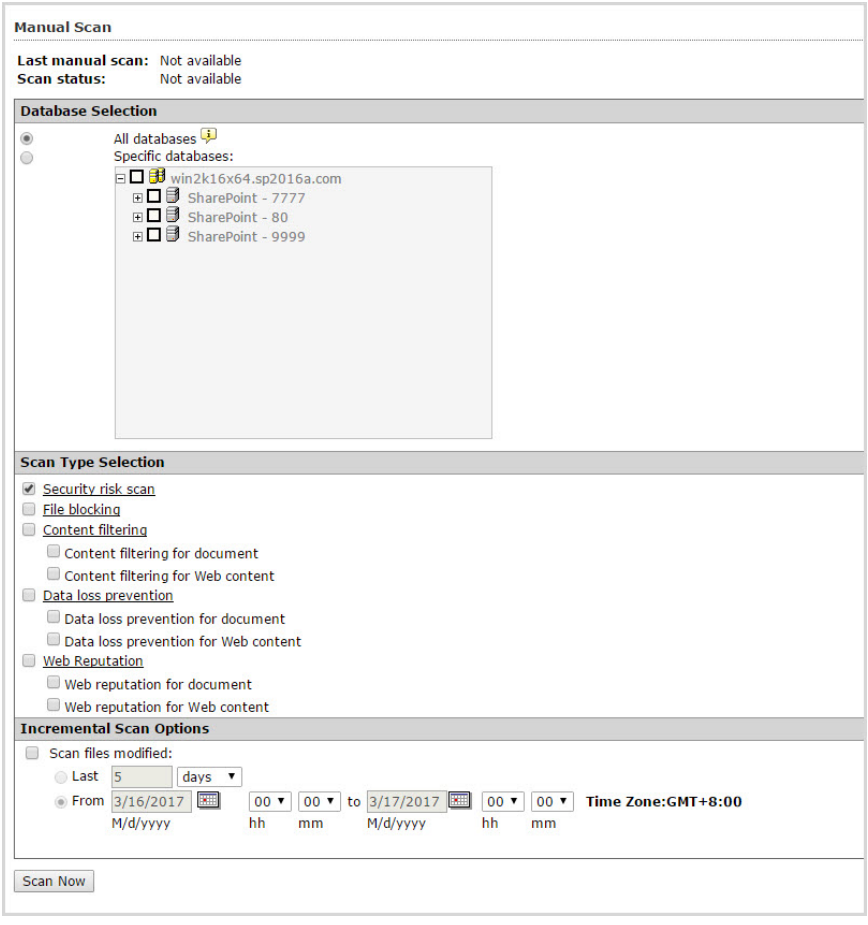


図 9-1. [Manual Scan] メイン画面

2. [Database selection] の下にある次のオプションから選択します。
   - All databases: すべてのデータベースを検索します。
   - Specific databases: 特定のデータベースを指定して検索するには、このオプションを選択して有効にします。

3. [Select the scan type] の下にある次のオプションから選択します。

注意

手動検索のオプションを設定するには、[Security risk scan]、[File blocking]、[Content filtering]、[Data loss prevention]、または [Web Reputation] リンクをクリックします。詳細については、以下を参照してください。

93 ページの「コンテンツフィルタの 処理の設定について」

161 ページの「手動検索: セキュリティリスク 検索の設定」

165 ページの「手動検索: ファイルブロックの設定」

171 ページの「手動検索: コンテンツフィルタの 設定」

177 ページの「手動検索: 情報漏えい対策の設定」

182 ページの「手動検索: Web レピュテーションの設定」

- Security risk scan — セキュリティリスクの手動検索を実行します。
- File blocking — ファイルブロックの手動検索を実行します。
- Content filtering — コンテンツフィルタの 手動検索を実行します。
  a. Content filtering for document: 選択されたコンテンツフィルタのオプションおよびポリシーに従ってドキュメントを検索します。詳細については、97 ページの「コンテンツフィルタの 設定」を参照してください。
  b. Content filtering for Web content: 選択されたコンテンツフィルタのオプションおよびポリシーに従って SharePoint に投稿された Web コンテンツを検索します。
- Data loss prevention — 情報漏えい対策の手動検索を実行します。
  a. Data loss prevention for document — 選択された情報漏えい対策のオプションおよびポリシーに従ってドキュメントを検索します。

b. Data loss prevention for Web content — 選択された情報漏えい対策のオプションおよびポリシーに従って SharePoint に投稿された Web コンテンツを検索します。

- Web Reputation — Web レピュテーションの手動検索を実行します。

a. Web reputation for document — 安全でない URL として分類されている URL を含むファイルを検索およびブロックします。詳細については、146 ページの「Web レピュテーションについて」を参照してください。

b. Web reputation for Web content — SharePoint サーバに投稿された Web コンテンツを検索します。

4. 一定期間の間に変更されたファイルを検索するには、[Scan files modified] を選択して、次の [Incremental Scan Options] を有効にします。

- [Last] を選択して、入力フィールドに数値を入力し、[Hours]、[Days]、または [Weeks] から適切なものを選択します。
- [From] を選択して、[From] および [to] で、適切な日付、時間、および分を選択します。

5. [Scan Now] をクリックします。

手動検索での圧縮ファイルの検索

手動検索で圧縮ファイルを検索するために必要な手順を説明します。

手順

1. 左側のメニューで、[Manual Scan] をクリックします。
2. [Select the scan type] の下にある [Security risk scan] リンクをクリックします。
3. [Target] タブを選択します。[Advanced Options] で、[Scan Restrictions Criteria] を展開します。

注意

検索する項目のチェックボックスをオンにして、適切な値を設定します。

4. [Do not scan file if...] の下で以下を設定します。
   - File size exceeds — 1〜100MB の値を入力します。
5. [Do not scan compressed files if] の値を選択または入力します。
   - Decompressed file count exceeds [xxxxx] — 圧縮ファイル内の最大ファイル数を入力します (1〜10,000)。PortalProtect では、この値以上のファイル数を含む圧縮ファイルは検索されません。
   - Size of Decompressed file exceeds [xxxx] — PortalProtect で検索する圧縮ファイルの最大サイズをメガバイト単位で入力します (1〜2048)。PortalProtect では、このサイズ以上の圧縮ファイルは検索されません。
   - Number of layers of compression exceeds [xx] — PortalProtect で検索する圧縮ファイルの最大階層数を入力します (1〜20)。PortalProtect では、この値以上の圧縮階層を持つ圧縮ファイルは検索されません。
   - Size of decompressed file is "x" times the size of compressed file — 解凍ファイルの最大サイズを示す、圧縮ファイルのサイズに対する倍数を入力します。解凍ファイルが超えてはいけない、圧縮ファイルのサイズに対する倍数 (100〜1,000,000) を入力します。圧縮ファイルのサイズの「x」倍より大きい解凍ファイルは検索されません。
6. [Save] をクリックします。

手動検索のマクロ検索オプションの設定

手動検索のマクロ検索オプションを設定するために必要な手順を説明します。

手順

1. 左側のメニューで、[Manual Scan] をクリックします。
2. [Select the scan type] の下にある [Security risk scan] リンクをクリックし、[Action] タブを選択します。
3. [Advanced Options] で、[Macros] をクリックしてコンテンツを開きます。

4. [Enable advanced macro scan] を選択して機能を有効にします。
5. [Heuristic level] で、次のいずれかのオプションを選択します。
   - 1 — Lenient filtering
   - 2 — Default filtering
   - 3 — Sensitive filtering
   - 4 — Rigorous filtering

   または
6. [Delete all macros detected by advanced macro scan] を選択します。
7. [Save] をクリックします。

手動検索: セキュリティリスク検索の設定

ここでは、手動検索のセキュリティリスク検索を設定するために必要な手順を説明します。

手順 1. 手動検索: セキュリティリスク検索の設定 ([Target] タブ)

手順

1. 左側のメニューで、[Manual Scan] をクリックします。

   [Manual Scan] 画面が表示されます。
2. 前提条件として、156 ページの「手動検索の設定」で説明されているオプションを設定済みであることを確認してください。
3. [Select the scan type] の下にある [Security risk scan] リンクをクリックします。

[Manual Scan: Security Risk Scan] 画面が表示されます。

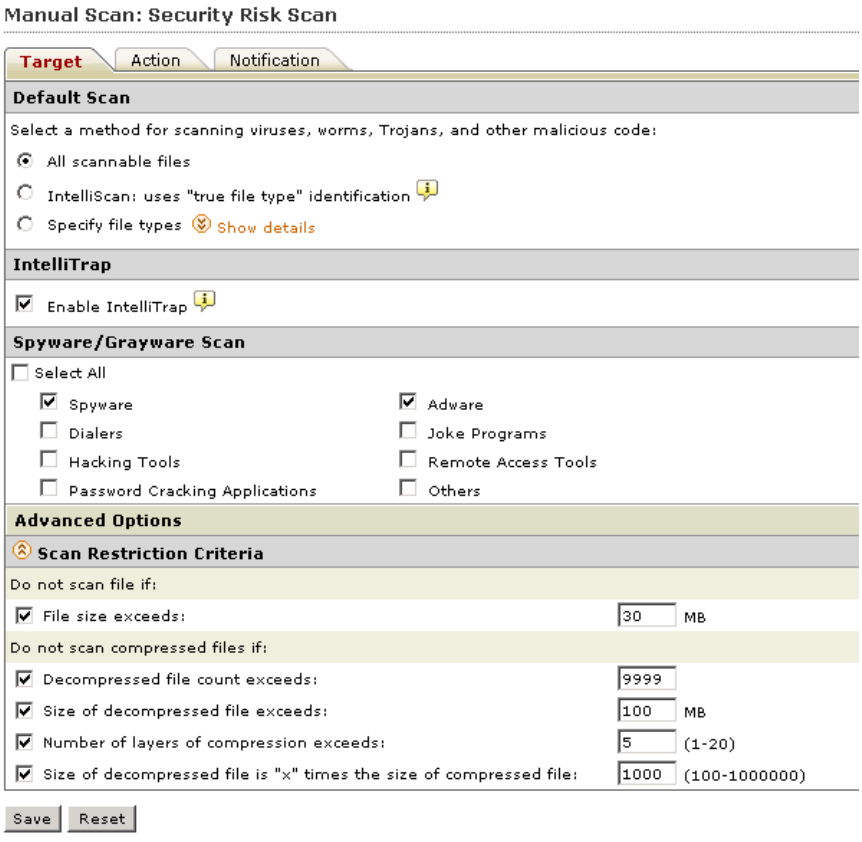


図 9-2. [Manual Scan: Security Risk Scan] 画面 ([Target] タブ)

4. 67 ページの「セキュリティリスクの検出時の処理の設定について」の説明に従って [Target] タブで設定を行います。

手順 2. 手動検索: セキュリティリスク検索の設定 ([Action] タブ)

手順

1. [Target] タブの設定が完了したら、[Action] タブをクリックします。

   [Manual Scan: Security Risk Scan] 画面に [Action] タブが表示されます。

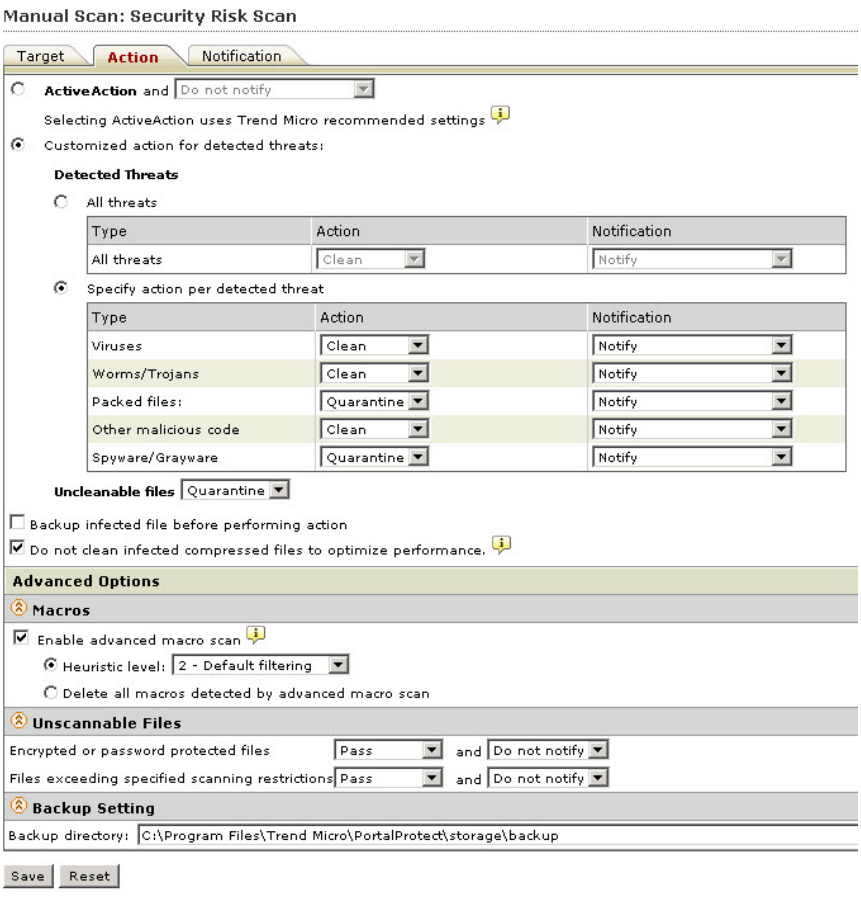


図 9-3. [Manual Scan: Security Risk Scan] 画面 ([Action] タブ)

2. 手動のセキュリティリスク検索で使用可能なオプションから選択します。

   68 ページの「セキュリティリスクの検出時の処理の設定」および次の表を参照してください。

   表 9-1. 手動検索のセキュリティリスク検索で利用可能な処理

脅威の種類	使用可能なオプション
すべての脅威	駆除、隔離、削除、放置、または拡張子変更
ウイルス	駆除、隔離、削除、放置、または拡張子変更
ワーム/トロイの木馬	隔離、削除、放置、または拡張子変更
パックされたファイル	隔離、削除、放置、または拡張子変更
その他の不正プログラムコード	駆除、隔離、削除、放置、または拡張子変更
スパイウェア/グレーウェア	隔離、削除、放置、または拡張子変更
駆除不能なウイルス	隔離、削除、放置、または拡張子変更

手順 3. 手動検索: セキュリティリスク検索の設定 ([Notification] タブ)

手順

1. [Manual Scan: Security Risk Scan] > [Notification] タブをクリックします。
2. この手動のセキュリティリスク検索を、207 ページの「セキュリティリスク検索通知の設定」の説明に従って設定します。
3. [Save] をクリックします。
4. [Scan Now] をクリックして、保存した設定で手動検索を実行します。

手動検索: ファイルブロックの設定

ここでは、手動検索のファイルブロックを設定するために必要な手順を説明します。

手順

1. 左側のメニューで、[Manual Scan] をクリックします。
2. [Select the scan type] の下にある [File blocking] リンクをクリックします。

   [Manual Scan: File Blocking] 画面が表示されます。
3. [Add] をクリックして新しいポリシーを作成します。

[Manual Scan: File Blocking: Add Policy] 画面が表示されます。

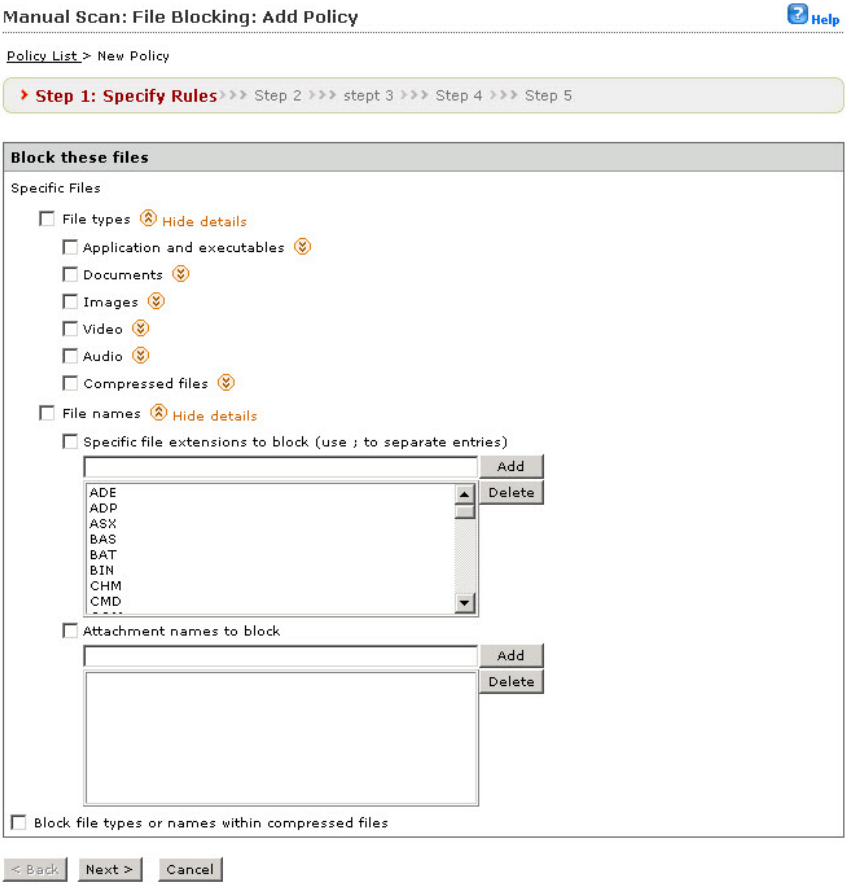


図 9-4. [Manual Scan: File Blocking: Add Policy] > [Step 1. Specify Rules] 画面

4. 後に続く手順に従って、この新しいポリシーの設定を完了します。

手順 1. [Manual Scan: File Blocking: Add Policy] > [Specify Rules]

手順

1. [Block these files] > [Specific Files] の下で次のオプションから選択し、このルールでブロックするファイルを指定します。

   - File types — すべてのファイルタイプを選択します。特定のファイルタイプを選択する場合は、[Show details] をクリックします。87 ページの「使用可能なファイルタイプについて」の表 5-2 から 5-7 を参照してください。

2. 特定のファイル名または拡張子を追加または削除するには、[File names] の横にある [Show details] をクリックして、コンテンツを展開します。

3. 必要に応じて [Add] または [Delete] をクリックして、ファイルまたはファイル拡張子を追加または削除します。

4. [Block file type or name within compressed files] を選択して、処理を実行します。

5. [Next >] をクリックします。

   [Manual Scan: File Blocking: Add Policy Step 2: Exceptions] 画面が表示されます。

手順 2. [Manual Scan: File Blocking: Add Policy] > [Specify sites to be excluded]

手順

1. この新しいポリシーに対する除外設定として任意のサイトおよびアカウントを除外するには、[Add] をクリックします。

   [Manual Scan: File Blocking: Add Policy (Step 2.a: Specify sites to be excluded)] 画面が表示されます。

2. 次のオプションから選択します。

   - All sites

- Specify a site's URL — 特定の URL を入力し、[Search] をクリックするか、ツリーからサイトを選択します。

3. [Next >] をクリックします。

   [Manual Scan: File Blocking: Add Policy (Step 2.b: Specify accounts to be excluded)] 画面が表示されます。

4. 次のオプションから選択します。

   - Anyone
   - Specific accounts — [Search for] ドロップダウンから [AD user(s)/groups] または [SharePoint user(s)/group(s)] を選択します。

5. [Users] または [Groups]、あるいは両方のチェックボックスをオンにします。次に名前を入力し、[Search] をクリックします。

6. 検索が完了したら、含める項目を [Available Account(s)] 画面から選択して、[Add] をクリックします。

7. 必要に応じて項目の検索および追加を続け、完了したら、[Finish] をクリックします。

   [Manual Scan: File Blocking: Add Policy Step 2: Exceptions] 画面が表示され、新しく追加したサイト/アカウントが表示されます。

8. [Next >] をクリックします。

   [Manual Scan: File Blocking: Add Policy Step 3: Specify Action] 画面が表示されます。

手順 3. [Manual Scan: File Blocking: Add Policy] > [Specify Action]

手順

1. 次のオプションから処理を選択します。

   - Quarantine
   - Delete
   - Pass

2. 以下から選択します。
   - Notify
   - Do not notify
3. [Next >] をクリックします。

   [Manual Scan: File Blocking: Add Policy Step 4: Specify Notification] 画面が表示されます。

手順 4. [Manual Scan: File Blocking: Add Policy] > [Specify Notification]

手順

1. [People to notify] の下で、次のオプションを選択します。
   - Notify violator
   - Notify administrator

   注意

   通知の設定方法については、209 ページの「ファイルブロック通知の設定」を参照してください。
2. [Next >] をクリックします。

   [Manual Scan: File Blocking: Add Policy Step 5: Name and priority] 画面が表示されます。

手順 5. [Manual Scan: File Blocking: Add Policy] > [Name and priority]

手順

1. 手動検索のために、[Enable this policy] をオンにして有効にします。無効にするにはオフにします。

2. [Policy name] フィールドに新しいポリシーの名前を入力します (必須)。
3. [Description] フィールドにポリシーの説明を入力します。
4. [Priority] フィールドに処理の優先順位を示す数字を入力します (必須)。

   優先順位を決定する際は、画面の下部に表示される既存のポリシーおよびステータスを参考にします。
5. [Finish] をクリックします。

   [Manual Scan: File Blocking] 画面が表示され、作成したポリシーに関して以下の情報が表示されます。

   - Policy: 名前
   - Action:Quarantine、Block など
   - Priority:1、2、3 など
   - Status: 有効 (緑色のチェックマーク) または無効 (赤色の X)。必要に応じてクリックしてステータスを変更します。

注意

リアルタイム検索のファイルブロックからポリシーをインポートするには、[Import] をクリックします。

ファイルブロックルールのインポート

手動検索のファイルブロックを使用すると、リアルタイム検索からファイルブロックのルールをインポートできますが、リアルタイム検索と手動検索では実行される処理が異なり、次の表に示すようにインポートされます。

表 9-2. ファイルブロックのインポートルールのマッピング

検索のタイプ	リアルタイム検索での処理	手動または予約検索での処理
ファイルに対するファイルブロック	Block	Quarantine
	Pass	Pass

手順

1. 左側のメニューで、[Manual Scan] をクリックします。

   [Manual Scan] 画面が表示されます。

2. [Scan Type Selection] の下にある [File blocking] リンクをクリックします。

   [Manual Scan: File Blocking] 画面が表示されます。

3. [Import] をクリックします。

   [Import from Real-time File Blocking Policy] 画面が表示されます。

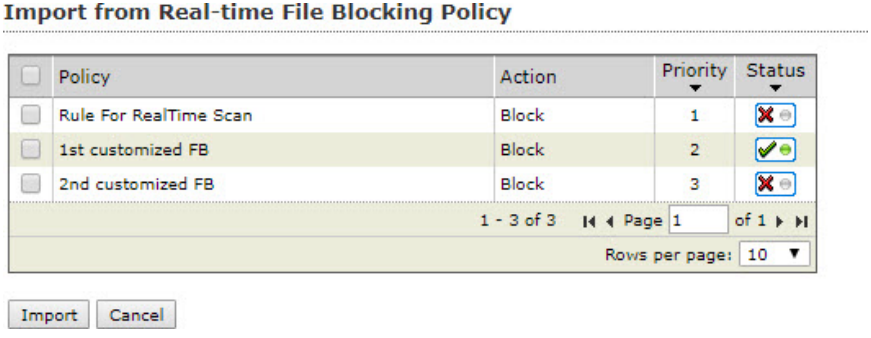


図 9-5. [Import from Real-time File Blocking Policy] 画面

4. インポートするポリシーを選択して、[Import] をクリックします。

手動検索: コンテンツフィルタの設定

ここでは、手動検索のコンテンツフィルタを 設定するために必要な手順を説明します。

コンテンツフィルタルールのインポート

手動検索のコンテンツフィルタを 使用すると、リアルタイム検索からコンテンツフィルタのルールをインポートできますが、リアルタイム検索と手動検索では実行される処理が異なり、次の表に示すようにインポートされます。

表 9-3. コンテンツフィルタのインポートルールのマッピング

検索のタイプ	リアルタイム検索での処理	手動または予約検索での処理
ファイルに対するコンテンツフィルタ	Block	Quarantine
	Pass	Pass
Web コンテンツに対するコンテンツフィルタ	Block	Pass
	Pass	Pass

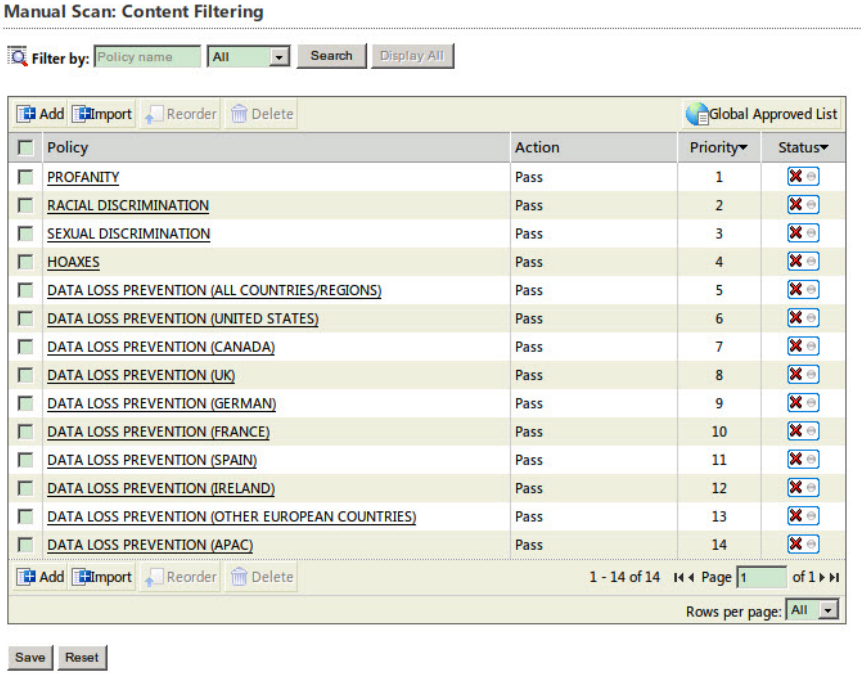
手順

1. 左側のメニューで、[Manual Scan] をクリックします。

   [Manual Scan] 画面が表示されます。

2. [Select the scan type] の下にある [Content filtering] リンクをクリックします。

[Manual Scan: Content Filtering] 画面が表示されます。



3. [Import] をクリックします。

[Import from Real-time Content Filtering Policy] 画面が表示されます。

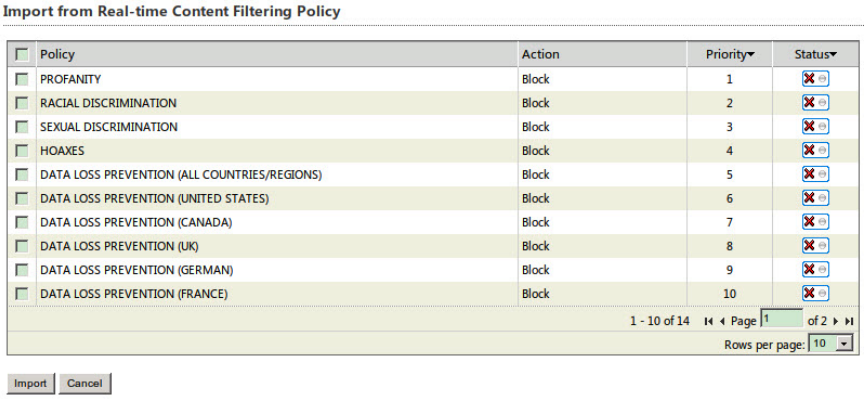


図 9-6. [Import from Real-time Content Filtering Policy] 画面

4. インポートするポリシーを選択して、[Import] をクリックします。

手動検索のコンテンツフィルタ検索の設定

手順

1. 左側のメニューで、[Manual Scan] をクリックします。

   [Manual Scan] 画面が表示されます。

2. [Select the scan type] で、以下に対してコンテンツフィルタを 実行するかどうかを指定します。

   - ドキュメントに対するコンテンツフィルタ
   - Web コンテンツに対するコンテンツフィルタ

3. [Content filtering] リンクをクリックします。

[Manual Scan: Content Filtering] 画面が表示されます。

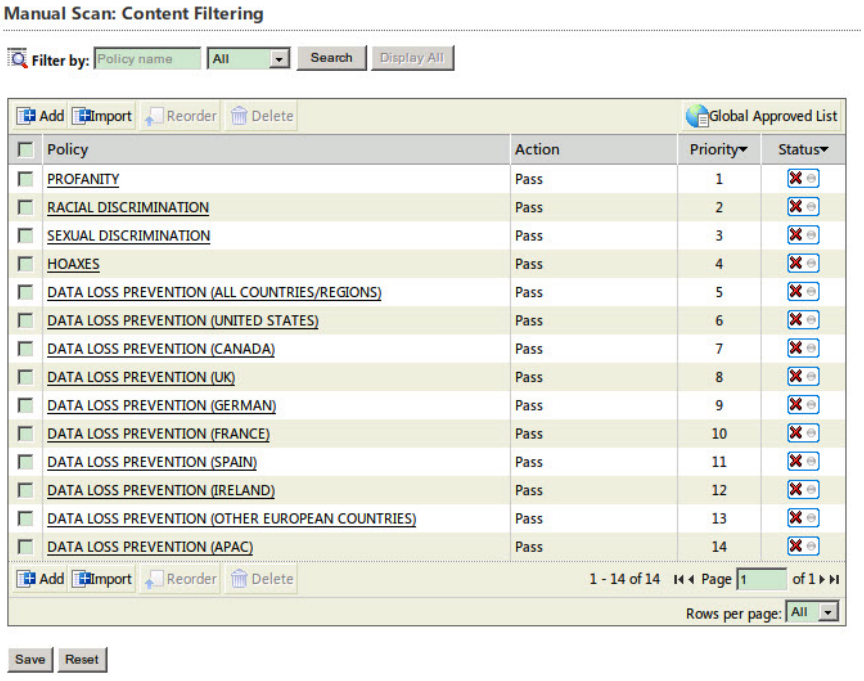


図 9-7. [Manual Scan: Content Filtering] 画面

注意

ポリシーは、[Policy name] や、[Enabled]、[Disabled]、または [All] (有効化されたポリシーと無効化されたポリシーの両方) のいずれかによってフィルタできます。

4. ポリシーを削除または並べ替えるには、リストで選択して、[Delete] または [Reorder] をクリックします。既存のポリシーを編集するには、そのポリシーをクリックします。
5. [Status] 列で、赤色の X、または緑色のチェックマークをクリックして、手動検索の既存のコンテンツフィルタポリシーを 有効または無効にします。

6. 既存のポリシーを選択し、次のオプションを設定します。
   - Enable this policy: ポリシーを有効にします。
   - Policy name: ポリシー名を入力します。
   - Description: ポリシーをさらに詳しく表す説明を追加します。
7. 99 ページの「コンテンツフィルタポリシーの 追加」の説明に従って [Target] タブで設定を行います。
8. [Exceptions] タブをクリックします。
9. 新しい除外設定を作成するには [Add] をクリックします。または既存の除外設定をクリックします。

   [Specify sites] 画面が表示されます。
10. 次のオプションから選択します。
    - All sites: このポリシーからすべてのサイトを除外します。
    - Specify a site's URL: このポリシーから除外する特定のサイトを選択します。
11. [Next >] をクリックします。

    除外するアカウントを選択するための [Select Accounts] 画面が表示されます。
12. 次のオプションから選択します。
    - Anyone — すべてのアカウントを除外する場合に選択します。選択し、[Finish] をクリックして、次の手順に進みます。
    - Specific accounts — 特定のアカウントを選択する場合に使用し、次の手順に進みます。
13. AD ユーザまたはグループの名前を [Search for AD user(s)/group(s)] フィールドに入力します。
14. [Search in] の横にある [Users] または [Groups]、あるいは両方を適宜選択します。
15. [Search] をクリックします。

    検索の結果は、[Available Account(s)] 画面に表示されます。

16. 必要に応じて検索を繰り返します。
17. 除外対象とするユーザ/グループをすべて選択し、[Add] をクリックして、[Selected Account(s)] 画面に移動します。
18. [Finish] をクリックします。

    [Manual Scan: Content Filtering: Edit Policy] > [Exceptions] 画面が表示されます。
19. [Action] タブをクリックし、次のいずれかのオプションから、コンテンツフィルタポリシーの処理を選択します。
    - [Quarantine]、[Delete]、または [Pass]
    - [Notify] または [Do not notify]
20. [Notification] タブをクリックして、219 ページの「手動検索通知 — コンテンツフィルタの 設定」の説明に従って設定を行います。
21. [Save] をクリックします。

手動検索: 情報漏えい対策の設定

ここでは、手動検索の情報漏えい対策を設定するために必要な手順を説明します。

情報漏えい対策ルールのインポート

手動検索の情報漏えい対策を使用すると、リアルタイム検索から情報漏えい対策のルールをインポートできますが、リアルタイム検索と手動検索では実行される処理が異なり、次の表に示すようにインポートされます。

表 9-4. 情報漏えい対策のインポートルールのマッピング

検索のタイプ	リアルタイム検索での処理	手動または予約検索での処理
ファイルに対する情報漏えい対策	Block	Quarantine
	Pass	Pass
Web コンテンツに対する情報漏えい対策	Block	Pass

検索のタイプ	リアルタイム検索での処理	手動または予約検索での処理
	Pass	Pass

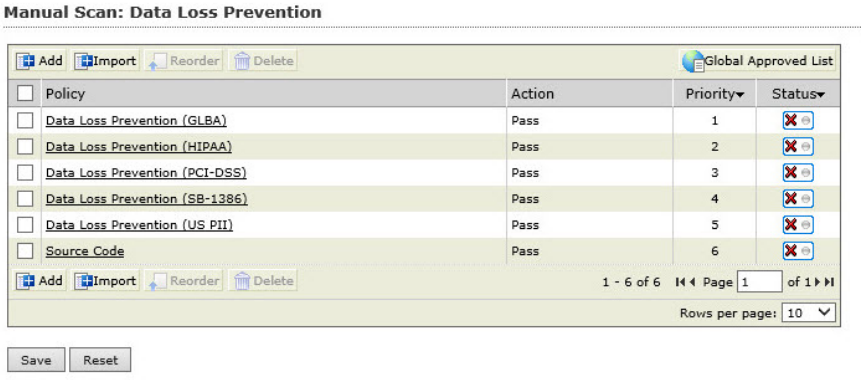
手順

1. 左側のメニューで、[Manual Scan] をクリックします。

   [Manual Scan] 画面が表示されます。

2. [Select the scan type] の下にある [Data loss prevention] リンクをクリックします。

   [Manual Scan: Data Loss Prevention] 画面が表示されます。



3. [Import] をクリックします。

[Import from Real-time Data Protection Policy] 画面が表示されます。

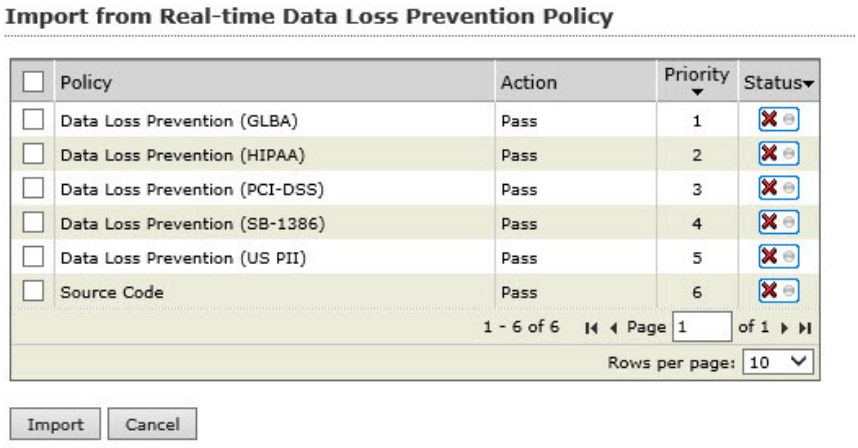


図 9-8. [Import from Real time Data Loss Prevention Policy] 画面

4. インポートするポリシーを選択して、[Import] をクリックします。

手動検索の情報漏えい対策検索の設定

手順

1. 左側のメニューで、[Manual Scan] をクリックします。

   [Manual Scan] 画面が表示されます。

2. [Scan Type Selection] で、以下に対してコンテンツフィルタを実行するかどうかを指定します。

   - ドキュメントに対する情報漏えい対策
   - Web コンテンツに対する情報漏えい対策

3. [Data loss prevention] リンクをクリックします。

[Manual Scan: Data Loss Prevention] 画面が表示されます。

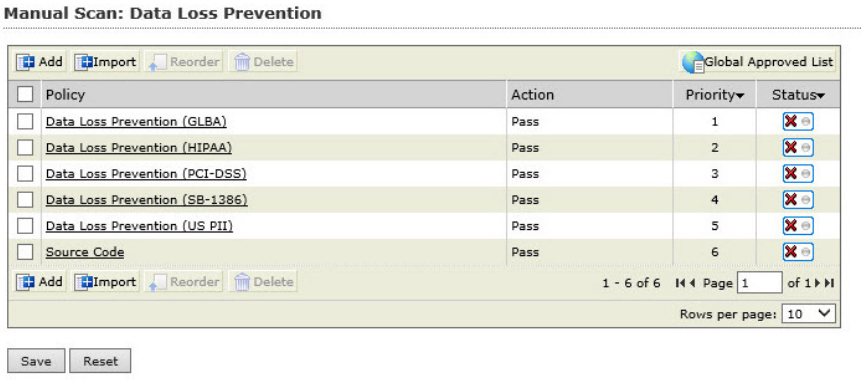


図 9-9. [Manual Scan: Data Loss Prevention] 画面

4. ポリシーを削除または並べ替えるには、リストで選択して、[Delete] または [Reorder] をクリックします。既存のポリシーを編集するには、そのポリシーをクリックします。
5. [Status] 列で、赤色の X、または緑色のチェックマークをクリックして、手動検索の既存のデータ漏えい対策ポリシーを有効または無効にします。
6. 既存のポリシーを選択し、次のオプションを設定します。
   - Enable this policy: ポリシーを有効にします。
   - Policy name: ポリシー名を入力します。
   - Description: ポリシーをさらに詳しく表す説明を追加します。
7. 131 ページの「情報漏えい対策ポリシーの追加」の説明に従って [Target] タブで設定を行います。
8. [Exceptions] タブをクリックします。
9. 新しい除外設定を作成するには [Add] をクリックします。または既存の除外設定をクリックします。

   [Specify sites] 画面が表示されます。

10. 次のオプションから選択します。
    - All sites: このポリシーからすべてのサイトを除外します。
    - Specify a site's URL: このポリシーから除外する特定のサイトを選択します。
11. [Next >] をクリックします。

    除外するアカウントを選択するための [Select Accounts] 画面が表示されます。
12. 次のオプションから選択します。
    - Anyone — すべてのアカウントを除外する場合に選択します。選択し、[Finish] をクリックして、次の手順に進みます。
    - Specific accounts — 特定のアカウントを選択する場合に使用し、次の手順に進みます。
13. AD ユーザまたはグループの名前を [Search for AD user(s)/group(s)] フィールドに入力します。
14. [Search in] の横にある [Users] または [Groups]、あるいは両方を適宜選択します。
15. [Search] をクリックします。

    検索の結果は、[Available Account(s)] 画面に表示されます。
16. 必要に応じて検索を繰り返します。
17. 除外対象とするユーザ/グループをすべて選択し、[Add] をクリックして、[Selected Account(s)] 画面に移動します。
18. [Finish] をクリックします。

    [Manual Scan: Data Loss Prevention: Edit Policy] > [Exceptions] 画面が表示されます。
19. [Action] タブをクリックし、次のいずれかのオプションから、コンテンツフィルタポリシーの処理を選択します。
    - [Quarantine]、[Delete]、または [Pass]
    - [Notify] または [Do not notify]

20. [Notification] タブをクリックして設定します。
21. [Save] をクリックします。

手動検索: Web レピュテーションの設定

ここでは、手動検索の Web レピュテーションを設定するために必要な手順を説明します。

手順

1. 左側のメニューで、[Manual Scan] をクリックします。

   [Manual Scan] 画面が表示されます。
2. 前提条件として、156 ページの「手動検索の設定」で説明されているオプションを設定済みであることを確認してください。
3. [Select the scan type] の下にある [Web Reputation] リンクをクリックします。

   [Manual Scan: Web Reputation] 画面が表示されます。
4. Web レピュテーションの設定方法の詳細については、49 ページの「Smart Protection ソース」、146 ページの「Web レピュテーションについて」、および 147 ページの「Web レピュテーションソースの選択」を参照してください。
5. 設定が完了したら、[Save] をクリックします。

   [Manual Scan] 画面が表示されます。
6. [Scan Now] をクリックして、新しい設定で手動検索を実行します。

第 10 章

予約検索

予約検索を設定すると、ウイルス対策に関する定型業務を自動化できるため、セキュリティポリシーにおける効率性および管理性が向上します。予約検索は、ユーザが設定した時間間隔と時刻に従って実行されます。設定された時刻になると、SharePoint サーバに感染ファイルがないかどうか自動的に検索されます。予約検索を有効にすると、すべての検索が設定したスケジュールに従って実行されます。予約検索を無効にするには、[Scheduled Scan] の [Status] 列にある緑色のチェックマークをクリックします。クリックすると、緑色のチェックマークが赤色の「X」に変わります。

本章の内容は次のとおりです。

予約検索の設定

ここでは、予約検索を設定するために必要な手順を説明します。

手順

1. 左側のメニューで [Scheduled Scan] をクリックして、[Scheduled Scan] 画面を表示します。
2. [Status] 列の緑色のチェックマークをクリックすると、検索が無効になり、赤色の「X」が表示されます

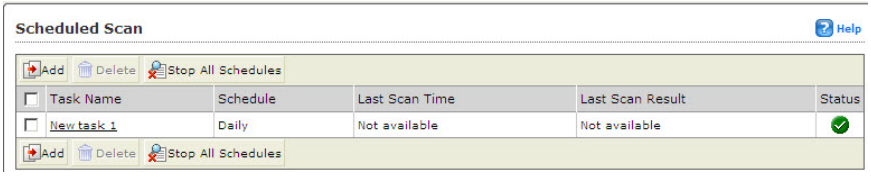


図 10-1. 有効化された予約検索

3. 予約検索を有効にするには、[Status] 列で赤色の「X」をクリックし、緑色のチェックマークを表示します。

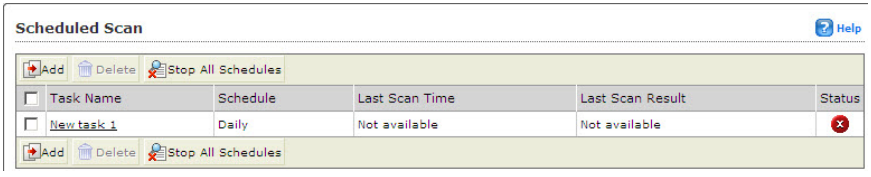


図 10-2. 無効化された予約検索

注意

検索を無効にしても設定は変更されません。予約検索を再開させたい場合は、検索を有効に戻します。

予約検索タスクの追加または編集

ここでは、予約検索タスクを追加または編集するために必要な手順を説明します。

手順

1. 左側のメニューで [Scheduled Scan] をクリックして、[Scheduled Scan] 画面を表示します。
2. [Scheduled Scan] ツールバーで [Add] をクリックします。

[Scheduled Scan: Add Scan Task] 画面が表示されます。

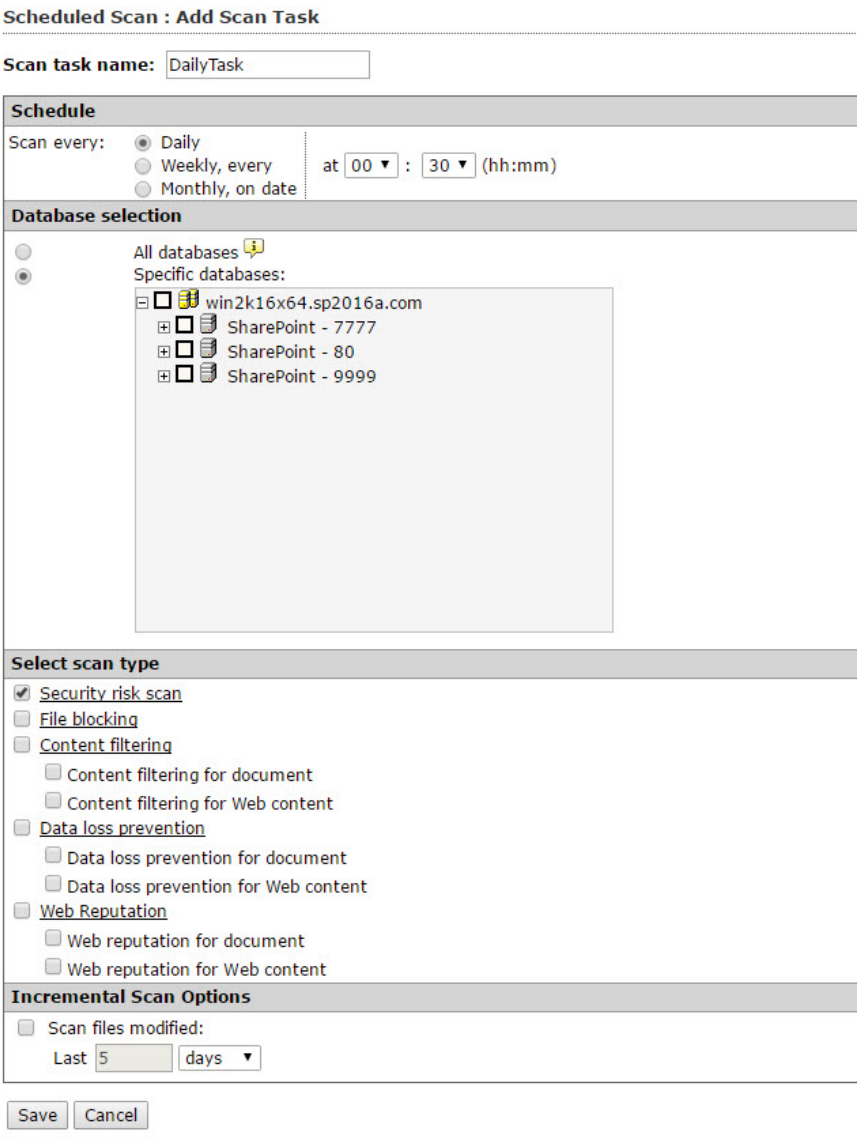


図 10-3. [Scheduled Scan: Add Scan Task] 画面

3. [Scan task name] フィールドで、新しい検索タスクの名前を入力します。
4. [Schedule] で、次のオプションから検索スケジュールを選択します。
   - Daily—at (hh:mm) — 毎日、指定した時刻に検索を実行します。
   - Weekly, every—[day of week] at (hh:mm) — 毎週、指定した曜日と時刻に検索を実行します。
   - Monthly, on date—[day of month] at (hh:mm) — 毎月、指定した日付と時刻に検索を実行します。
5. [Database selection] の下で、次のオプションのいずれかを選択します。
   - All databases — この設定を行った後に追加されたデータベースを含めます。
   - Specific databases — データベースを展開し、画面に表示されたデータベースの中から検索するものを選択します。
6. [Select the scan type] の下にある次のオプションから選択します。

注意

予約検索のオプションを設定するには、[Security risk scan]、[File blocking]、[Content filtering]、[Data loss prevention]、または [Web Reputation] リンクをクリックします。詳細については、以下を参照してください。

190 ページの「予約検索: セキュリティリスク 検索の設定」

192 ページの「予約検索: ファイルブロック検索の設定」

197 ページの「予約検索: コンテンツフィルタの 設定」

200 ページの「予約検索: 情報漏えい対策の設定」

203 ページの「予約検索: Web レピュテーションの設定」

   - Security risk scan — セキュリティリスクの予約検索を実行します。
   - File blocking — ファイルブロックの予約検索を実行します。

- Content filtering — コンテンツフィルタの 予約検索を実行します。[Content filtering for document] または [Content filtering for Web content] を必要に応じてオンまたはオフにします。
- Data loss prevention — 情報漏えい対策の予約検索を実行します。[Data loss prevention for document] または [Data loss prevention for Web content] を必要に応じてオンまたはオフにします。
- Web Reputation — Web レピュテーションの手動検索を実行します。[Web Reputation for document] または [Web Reputation for Web content] を必要に応じてオンまたはオフにします。

7. 一定期間の間に変更されたファイルを検索するには、[Scan files modified] を選択して、次の [Incremental Scan Options] を有効にします。
   - [Last] を選択して、入力フィールドに数値を入力し、[Hours]、[Days]、または [Weeks] から適切なものを選択します。
8. [Save] をクリックします。

予約検索のマクロ検索オプションの設定

予約検索のマクロ検索オプションを設定するために必要な手順を説明します。

手順

1. 左側のメニューで、[Scheduled Scan] をクリックします。
2. [Add] をクリックして新しい予約検索を作成するか、[Task Name] をクリックして既存の予約検索を編集します。
3. [Select scan type] の下にある [Security risk scan] リンクをクリックし、[Action] タブを選択します。
4. [Advanced Options] で、[Macros] をクリックしてコンテンツを開きます。
5. [Enable advanced macro scan] を選択して機能を有効にします。
6. [Heuristic level] で、次のいずれかのオプションを選択します。
   - 1 — Lenient filtering

- 2 — Default filtering
- 3 — Sensitive filtering
- 4 — Rigorous filtering

または

7. [Delete all macros detected by advanced macro scan] を選択します。
8. [Save] をクリックします。

予約検索での圧縮ファイルの検索

予約検索で圧縮ファイルを検索するために必要な手順を説明します。

手順

1. 左側のメニューで、[Scheduled Scan] をクリックします。
2. [Add] をクリックして新しい予約検索を作成するか、[Task Name] をクリックして既存の予約検索を編集します。
3. [Select scan type] の下にある [Security risk scan] リンクをクリックします。
4. [Target] タブを選択します。[Advanced Options] で、[Scan Restrictions Criteria] を展開します。

注意

検索する項目のチェックボックスをオンにして、適切な値を設定します。

5. [Do not scan file if...] の下で以下を設定します。
   - File size exceeds — 1〜100MB の値を入力します。
6. [Do not scan compressed files if] の値を選択または入力します。
   - Decompressed file count exceeds [xxxxx] — 圧縮ファイル内の最大ファイル数を入力します (1〜10,000)。PortalProtect では、この値以上のファイル数を含む圧縮ファイルは検索されません。

- Size of Decompressed file exceeds [xxxx] — PortalProtect で検索する圧縮ファイルの最大サイズをメガバイト単位で入力します (1〜2048)。PortalProtect では、このサイズ以上の圧縮ファイルは検索されません。
- Number of layers of compression exceeds [xx] — PortalProtect で検索する圧縮ファイルの最大階層数を入力します (1〜20)。PortalProtect では、この値以上の圧縮階層を持つ圧縮ファイルは検索されません。
- Size of decompressed file is "x" times the size of compressed file — 解凍ファイルの最大サイズを示す、圧縮ファイルのサイズに対する倍数を入力します。解凍ファイルが超えてはいけない、圧縮ファイルのサイズに対する倍数 (100〜1,000,000) を入力します。圧縮ファイルのサイズの「x」倍より大きい解凍ファイルは検索されません。

7. [Save] をクリックします。

予約検索: セキュリティリスク検索の設定

ここでは、予約検索のセキュリティリスク検索タスクを設定するために必要な手順を説明します。

手順

1. 左側のメニューで、[Scheduled Scan] をクリックします。

   [Scheduled Scan] 画面が表示されます。

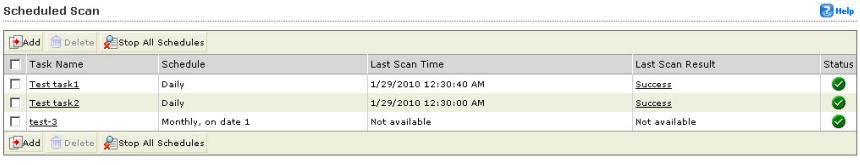


図 10-4. [Scheduled Scan] メイン画面

注意

前提条件として、184 ページの「予約検索の設定」で説明されているオプションを設定済みであることを確認してください。

2. [Add] をクリックします。

   [Scheduled Scan: Add Scan Task] 画面が表示されます。

3. [Scan task name] フィールドに新しい名前を入力します。

4. [Select the scan type] の下にある [Security risk scan] リンクをクリックします。

   [Scheduled Scan: Security Risk Scan] 画面が表示されます。

手順 1. 予約検索: セキュリティリスク検索 ([Target] タブ)

手順

1. 67 ページの「セキュリティリスクの検出時の処理の設定について」の説明に従って [Target] タブで設定を行います。

手順 2. 予約検索: セキュリティリスク検索の設定 ([Action] タブ)

手順

1. [Target] タブの設定が完了したら、[Action] タブをクリックします。

   [Scheduled Scan: Security Risk Scan] 画面に [Action] タブが表示されます。

2. 予約検索のセキュリティリスク検索で使用可能なオプションから選択します。詳細については、163 ページの「手順 2. 手動検索: セキュリティリスク検索の設定 ([Action] タブ)」を参照してください。

3. 必要に応じて [Advanced Options] を設定します。詳細については、188 ページの「予約検索のマクロ検索オプションの設定」を参照してください。

4. 必要に応じて [Unscannable Files] を設定します。詳細については、23 ページの「検索不能ファイルについて」を参照してください。

手順 3. 予約検索: セキュリティリスク検索の設定 ([Notification] タブ)

手順

1. [Scheduled Scan: Security Risk Scan] > [Notification] タブをクリックします。
2. 必要に応じて [Notification] を設定します。

   注意

   この検索の通知の設定方法の詳細については、225 ページの「予約検索通知 — セキュリティリスク検索の設定」を参照してください。

3. [Save] をクリックします。

   [Scheduled Scan: Add Scan Task] 画面が表示されます。

4. [Save] をもう一度クリックします。

   新しく作成したタスクが [Scheduled Scan] タスクリストに表示されます。

予約検索: ファイルブロック検索の設定

ここでは、予約検索のファイルブロック検索タスクを設定するために必要な手順を説明します。

手順

1. 左側のメニューで、[Scheduled Scan] をクリックします。

[Scheduled Scan] 画面が表示されます。

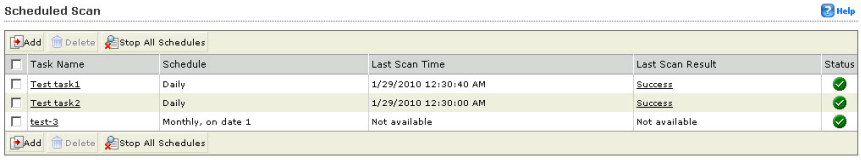


図 10-5. [Scheduled Scan] メイン画面

注意

前提条件として、184 ページの「予約検索の設定」で説明されているオプションを設定済みであることを確認してください。

2. [Add] をクリックします。

   [Scheduled Scan: Add Scan Task] 画面が表示されます。

3. [Scan task name] フィールドに新しい名前を入力します。

4. [Select the scan type] の下にある [File Blocking] リンクをクリックします。

   [Scheduled Scan: File Blocking] 画面が表示されます。

5. [Scheduled Scan: File Blocking] 画面で [Add] をクリックします。

   [Scheduled Scan: File Blocking: Add Policy] 画面が表示されます。後に続く手順に従って、この新しいポリシーの設定を完了します。

手順 1. [Scheduled Scan: File Blocking: Add Policy] > [Specify Rules]

手順

1. [Block these files] > [Specific Files] の下で次のオプションから選択し、このルールでブロックするファイルを指定します。

   - File types — すべてのファイルタイプを選択します。特定のファイルタイプを選択する場合は、[Show details] をクリックします。87 ページの「使用可能なファイルタイプについて」の表 5-2 から 5-7 を参照してください。

2. 特定のファイル名または拡張子を追加または削除するには、[File names] の横にある [Show details] をクリックして、コンテンツを展開します。
3. 必要に応じて [Add] または [Delete] をクリックして、ファイルまたはファイル拡張子を追加または削除します。
4. [Block file type or name within compressed files] を選択して、処理を実行します。
5. [Next >] をクリックします。

   [Scheduled Scan: File Blocking: Add Policy] > [Step 2: Exceptions] 画面が表示されます。

手順 2. [Scheduled Scan: File Blocking: Add Policy] > [Exceptions]

手順

1. この新しいポリシーに対する除外設定として任意のサイトおよびアカウントを除外するには、[Add] をクリックします。

   [Scheduled Scan: File Blocking: Add Policy (Step 2.a: Specify sites to be excluded)] 画面が表示されます。
2. 次のオプションから選択します。
   - All sites
   - Specify a site's URL — 特定の URL を入力し、[Search] をクリックするか、ツリーからサイトを選択します。
3. [Next >] をクリックします。

   [Scheduled Scan: File Blocking: Add Policy (Step 2.b: Specify accounts to be excluded)] 画面が表示されます。
4. 次のオプションから選択します。
   - Anyone
   - Specific accounts — [Search for] ドロップダウンから [AD user(s)/groups] または [SharePoint user(s)/group(s)] を選択します。

5. [Users] または [Groups]、あるいは両方のチェックボックスをオンにします。次に名前を入力し、[Search] をクリックします。
6. 検索が完了したら、含める項目を [Available Account(s)] 画面から選択して、[Add] をクリックします。
7. 必要に応じて項目の検索および追加を続け、完了したら、[Finish] をクリックします。

   [Scheduled Scan: File Blocking: Add Policy Step 2: Exceptions] 画面が表示され、新しく追加したサイト/アカウントが表示されます。
8. [Next >] をクリックします。

   [Scheduled Scan: File Blocking: Add Policy Step 3: Specify Action] 画面が表示されます。

手順 3. [Scheduled Scan: File Blocking: Add Policy] > [Specify Action]

手順

1. 次のオプションから処理を選択します。
   - Quarantine
   - Delete
   - Pass
2. 以下から選択します。
   - Notify
   - Do not notify
3. [Next >] をクリックします。

   [Scheduled Scan: File Blocking: Add Policy Step 4: Specify Notification] 画面が表示されます。

手順 4. [Manual Scan: File Blocking: Add Policy] > [Specify Notification]

手順

1. [People to notify] の下で、次のオプションを選択します。
   - Notify violator
   - Notify administrator

   注意

   この検索の通知の設定の詳細については、217 ページの「手動検索通知 — ファイルブロックの設定」を参照してください。

2. [Next >] をクリックします。

   [Scheduled Scan: File Blocking: Add Policy Step 5: Name and priority] 画面が表示されます。

手順 5. [Scheduled Scan: File Blocking: Add Policy] > [Name and priority]

手順

1. 手動検索のために、[Enable this policy] をオンにして有効にします。無効にするにはオフにします。
2. [Policy name] フィールドに新しいポリシーの名前を入力します (必須)。
3. [Description] フィールドにポリシーの説明を入力します。
4. [Priority] フィールドに処理の優先順位を示す数字を入力します (必須)。

   注意

   優先順位を決定する際は、画面の下部に表示される既存のポリシーおよびステータスを参考にします。

5. [Finish] をクリックします。

   [Scheduled Scan: File Blocking] 画面が表示され、作成したポリシーに関して以下の情報が表示されます。

   - Policy: 名前
   - Action: Quarantine、Block など
   - Priority: 1、2、3 など
   - Status: 有効 (緑色のチェックマーク) または無効 (赤色の X)。必要に応じてクリックしてステータスを変更します。

   注意

   リアルタイム検索のファイルブロックからポリシーをインポートするには、[Import] をクリックします。

予約検索: コンテンツフィルタの設定

ここでは、予約検索のコンテンツフィルタを 設定するために必要な手順を説明します。

コンテンツフィルタの 設定方法に関連する詳細情報については、次を参照してください。

- 92 ページの「コンテンツフィルタについて 」
- 93 ページの「コンテンツフィルタの 処理の設定について」
- 94 ページの「コンテンツフィルタポリシー 」
- 97 ページの「コンテンツフィルタの 設定」

手順

1. 左側のメニューで、[Scheduled Scan] をクリックします。

   [Scheduled Scan] 画面が表示されます。

2. [Add] をクリックします。

   [Scheduled Scan: Add Scan Task] 画面が表示されます。

3. [Scan task name] フィールドに新しいタスクの名前を入力します。

注意

前提条件として、184 ページの「予約検索の設定」で説明されているオプションを設定済みであることを確認してください。

4. [Select the scan type] で、以下に対してコンテンツフィルタを 実行するかどうかを指定します。
   - ドキュメントに対するコンテンツフィルタ
   - Web コンテンツに対するコンテンツフィルタ
5. [Content filtering] リンクをクリックします。

   [Scheduled Scan: Content Filtering] 画面が表示されます。
6. [Add] をクリックして新しいポリシーを作成します。

   [Scheduled Scan: Content Filtering: Add Policy] > [Step 1: Specify Rules] 画面が表示されます。

手順 1. [Scheduled Scan: Content Filtering: Add Policy] > [Specify Rules]

手順

1. 99 ページの「コンテンツフィルタポリシーの 追加」の説明に従って、キーワードおよび同義語を追加します。
2. [Next >] をクリックします。

   [Scheduled Scan: Content Filtering: Add Policy] 画面が表示されます。

手順 2. [Scheduled Scan: Content Filtering: Add Policy] > [Specify Sites to be Excluded]

手順

1. この画面での設定方法の詳細については、101 ページの「手順 2. [Content Filtering: Add Policy] > [Step 2: Exceptions]」を参照してください。
2. 除外の設定が完了したら、[Next >] をクリックします。

   [Scheduled Scan: Content Filtering: Add Policy] > [Step 3: Specify Action] 画面が表示されます。

手順 3. [Scheduled Scan: Content Filtering: Add Policy] > [Specify Action]

手順

1. 処理および通知のオプションを選択します。この画面での設定方法の詳細については、105 ページの「手順 3. [Content Filtering: Add Policy] > [Specify Action]」を参照してください。
2. [Next >] をクリックします。

   [Scheduled Scan: Content Filtering: Add Policy] > [Step 4: Specify Notification] 画面が表示されます。

手順 4. [Scheduled Scan: Content Filtering: Add Policy] > [Specify Notification]

手順

1. 利用可能なオプションから選択します。この画面での設定方法の詳細については、106 ページの「手順 4. [Content Filtering: Add Policy] > [Specify Notification]」を参照してください。
2. [Next >] をクリックします。

[Scheduled Scan: Content Filtering: Add Policy] > [Step 5: Name and Priority] 画面が表示されます。

手順 5. [Scheduled Scan: Content Filtering: Add Policy] > [Name and Priority]

手順

1. 利用可能なオプションを設定します。この画面での設定方法の詳細については、109 ページの「手順 5. [Content Filtering: Add Policy] > [Name and Priority]」を参照してください。
2. [Finish] をクリックします。

   [Scheduled Scan: Content Filtering] 画面に新しく作成したポリシーが表示されます。
3. [Save] をクリックします。

予約検索: 情報漏えい対策の設定

ここでは、予約検索の情報漏えい対策を設定するために必要な手順を説明します。

情報漏えい対策の設定方法に関連する詳細情報については、次を参照してください。

- 115 ページの情報漏えい対策
- 130 ページの「情報漏えい対策ポリシー」
- 126 ページの「情報漏えい対策コンプライアンステンプレート 」

手順

1. 左側のメニューで、[Scheduled Scan] をクリックします。

   [Scheduled Scan] 画面が表示されます。
2. [Add] をクリックします。

   [Scheduled Scan: Add Scan Task] 画面が表示されます。

3. [Scan task name] フィールドに新しいタスクの名前を入力します。

注意

前提条件として、184 ページの「予約検索の設定」で説明されているオプションを設定済みであることを確認してください。

4. [Select the scan type] で、以下に対して情報漏えい対策を実行するかどうかを指定します。
   - ドキュメントに対する情報漏えい対策
   - Web コンテンツに対する情報漏えい対策
5. [Data loss prevention] リンクをクリックします。

   [Scheduled Scan: Data Loss Prevention] 画面が表示されます。
6. [Add] をクリックして新しいポリシーを作成します。

   [Scheduled Scan: Data Loss Prevention: Add Policy] > [Step 1: Specify Rules] 画面が表示されます。

手順 1. [Scheduled Scan: Data Loss Prevention: Add Policy] > [Specify Rules]

手順

1. 131 ページの「情報漏えい対策ポリシーの追加」の説明に従って設定します。
2. [Next >] をクリックします。

   [Scheduled Scan: Data Loss Prevention: Add Policy] 画面が表示されます。

手順 2. [Scheduled Scan: Data Loss Prevention: Add Policy] > [Specify Sites to be Excluded]

手順

1. この画面での設定方法の詳細については、134 ページの「手順 2. [Data Loss Prevention: Add Policy] > [Step 2: Exceptions]」を参照してください。
2. 除外の設定が完了したら、[Next >] をクリックします。

   [Scheduled Scan: Data Loss Prevention: Add Policy] > [Step 3: Specify Action] 画面が表示されます。

手順 3. [Scheduled Scan: Data Loss Prevention: Add Policy] > [Specify Action]

手順

1. 処理および通知のオプションを選択します。この画面での設定方法の詳細については、137 ページの「手順 3. [Data Loss Prevention: Add Policy] > [Specify Action]」を参照してください。
2. [Next >] をクリックします。

   [Scheduled Scan: Data Loss Prevention: Add Policy] > [Step 4: Specify Notification] 画面が表示されます。

手順 4. [Scheduled Scan: Data Loss Prevention: Add Policy] > [Specify Notification]

手順

1. 利用可能なオプションから選択します。この画面での設定方法の詳細については、138 ページの「手順 4. [Data Loss Prevention: Add Policy] > [Specify Notification]」を参照してください。
2. [Next >] をクリックします。

[Scheduled Scan: Data Loss Prevention: Add Policy] > [Step 5: Name and Priority] 画面が表示されます。

手順 5. [Scheduled Scan: Data Loss Prevention: Add Policy] > [Name and Priority]

手順

1. 利用可能なオプションを設定します。この画面での設定方法の詳細については、140 ページの「手順 5. [Data Loss Prevention: Add Policy] > [Name and Priority]」を参照してください。
2. [Finish] をクリックします。

   [Scheduled Scan: Data Loss Prevention] 画面に新しく作成したポリシーが表示されます。
3. [Save] をクリックします。

予約検索: Web レピュテーションの設定

ここでは、予約検索の Web レピュテーションを設定するために必要な手順を説明します。このリリースでは、Web レピュテーションの新しい機能によってファイル内の URL の検索が可能です。Web レピュテーションの設定方法に関連する詳細情報については、次を参照してください。

- 146 ページの「Web レピュテーションについて」
- 146 ページの「ローカルおよびグローバル Smart Protection」
- 153 ページの「Trend Micro Smart Protection Network」

手順

1. 左側のメニューで、[Scheduled Scan] をクリックします。

   [Scheduled Scan] 画面が表示されます。
2. 前提条件として、184 ページの「予約検索の設定」で説明されているオプションを設定済みであることを確認してください。

3. [Select the scan type] の下にある [Web Reputation] リンクをクリックします。

   [Scheduled Scan: Web Reputation] 画面が表示されます。

4. Web レピュテーションの設定方法の詳細については、146 ページの「Web レピュテーションについて」およびその後の手順を参照してください。

5. 設定が完了したら、[Save] をクリックします。

   [Scheduled Scan] 画面が表示されます。

6. [Save] をもう一度クリックします。

第 11 章

通知、警告、ログ、およびレポート

本章では、PortalProtect の通知、警告、ログ、およびレポート機能について説明します。また、通知の種類および通知を送信する方法、アウトブレークの発生時に警告を発するシステムイベントを設定します。さらに、ログを表示して、発生した PortalProtect イベントを確認します。ログは、トラブルシューティングに役立つ重要な情報源です。日次、週次、月次のレポートを使用して、SharePoint 環境のセキュリティに関する情報を共有します。

予防的なセキュリティ戦略の一環として通知を使用し、攻撃を予測してリスクを評価します。対応型のセキュリティ戦略の一環としてログを使用し、損害の原因を評価して解決を試みます。通知とログを組み合わせて使用して、SharePoint 環境の脆弱性を特定し、他のセキュリティチームメンバーと 情報を共有するためにレポートを送信します。

本章の内容は次のとおりです。

通知の設定

通知は、管理者または他の指定された受信者に送信できます。PortalProtect では、メール、SNMP (Simple Network Management Protocol) トラップ、または Windows イベントログを介した通知を設定できます。グローバル通知の設定は、すべての通知に適用されます。次のそれぞれの通知に独自の設定を行うこともできます。

- 207 ページの「セキュリティリスク検索通知の設定」
- 209 ページの「ファイルブロック通知の設定」
- 210 ページの「コンテンツフィルタ 通知の設定」
- 212 ページの「情報漏えい対策通知の設定」
- 213 ページの「Web レピュテーション通知の設定」
- 215 ページの「手動検索通知 — セキュリティリスク検索の設定」
- 217 ページの「手動検索通知 — ファイルブロックの設定」
- 219 ページの「手動検索通知 — コンテンツフィルタの 設定」
- 221 ページの「手動検索通知 — 情報漏えい対策の設定」
- 223 ページの「手動検索通知 — Web レピュテーションの設定」
- 225 ページの「予約検索通知 — セキュリティリスク検索の設定」
- 227 ページの「予約検索通知 — ファイルブロックの設定」
- 229 ページの「予約検索通知 — コンテンツフィルタの 設定」
- 230 ページの「予約検索通知 — 情報漏えい対策の設定」
- 232 ページの「予約検索通知 — Web レピュテーションの設定」

グローバル通知の設定

[Administration] > [Notification Settings] で通知の設定を作成することもできます。この領域で連絡先情報を追加して [Apply All] をクリックすると、そのメールアドレスはセキュリティリスク検索、ファイルブロック、手動検索、予約検索、コンテンツフィルタ、Web レピュテーション、および情報漏えい対策のそれぞれ独自の通知に適用されます。

グローバル通知の設定

手順

1. 左側のメニューで [Administration] > [Notification Settings] をクリックします。
2. [Administrator Notification] の下に、すべての通知を受信する管理者のメールアドレスを入力します。複数のアドレスがある場合はセミコロン (;) を使用して区切ります。[Apply All] をクリックして新しい設定を更新します。
3. [Sender Settings] の下に、警告および通知を送信する送信者のメールアドレスを入力します (例: PortalProtect_Administrator@do.not.reply)。
4. [Email Account Settings] の下に、PortalProtect が次のメールベースの通知の送信に使用する SMTP サーバ (メールサーバ) の設定を入力します。
   - Display name — 一意の識別子 (例: PortalProtect Notification)
   - SMTP Server
   - Port
5. [SNMP] の下に、次を入力します。
   - IP address
   - Community
6. [Save] をクリックします。

イベント通知

PortalProtect では、セキュリティリスク検索、ファイルブロック、コンテンツフィルタ、Web レピュテーション、および情報漏えい対策において一意のイベント通知を送信するためのさまざまなオプションが用意されています。

セキュリティリスク検索通知の設定

セキュリティリスク検索通知を設定するために必要な手順を説明します。

手順

1. 左側のメニューで、[Security Risk Scan] をクリックします。[Security Risk Scan] 画面が表示されます。
2. [Notification] タブをクリックします。
3. [People to notify] で、[Notify administrator] を選択してセキュリティリスク検索通知を有効にします。
4. [People to notify] の下の [Show details] をクリックして次を設定します。
   - To — グローバルメールアドレスがこのフィールドに 表示されます。追加のメールアドレスはセミコロンで区切って入力して、独自の通知を作成します。
   - Subject — メールの件名の行に表示される件名を入力します (例: Security Risk Scan Notification)。
   - Message — 変数を使用して独自のメッセージを作成できます (変数の例: [Server Name]、[Security Risk Name]、[Date]、[Time]、[File Name]、[File Location]、[Action]、[Violator])。

   注意

   使用可能な変数は左側の画面に表示され、本文は右側の画面に表示されます。
5. [Settings] の下で、次に応じて通知の配信オプションを選択します。
   - Send consolidated notifications every [xx] [hours or days] — 変数フィールドで入力した時間数または日数ごとに通知を送信する場合、このオプションを選択します。
   - Send consolidate notifications every [xx] occurrences — 変数フィールドで入力した回数発生した後に通知を送信する場合、このオプションを選択します。
   - Send individual notifications — イベントが発生するたびに通知を送信する場合、このオプションを選択します。
6. [Advanced Notification (SNMP)] の下で、[SNMP] を選択してこのオプションを有効にします。

7. [Show details] をクリックしてオプションを展開し、次に応じて設定を行います。
   - IP Address
   - Community
   - Message — この手順のステップ 4 で説明したメッセージを作成します。
8. [Write to Windows event log] を選択すると、それぞれの通知を Windows イベントログに書き込みます。
9. [Save] をクリックします。

ファイルブロック通知の設定

ファイルブロック通知を設定するために必要な手順を説明します。

手順

1. 左側のメニューで、[File Blocking] をクリックします。[File Blocking] 画面が表示されます。
2. [Notification] タブをクリックします。
3. [People to notify] で、[Notify administrator] を選択してファイルブロック通知を有効にします。
4. [People to notify] の下の [Show details] をクリックして次を設定します。
   - To — グローバルメールアドレスがこのフィールドに 表示されます。追加のメールアドレスはセミコロン (;) で区切って入力して、独自の通知を作成します。
   - Subject — メールの件名の行に表示される件名を入力します (例: File Blocking Notification)。
   - Message — 変数を使用して独自のメッセージを作成できます (変数の例: [Server Name]、[File Blocking Rules]、[Date]、[Time]、[File Name]、[File Location]、[Action]、[Violator])。

注意

使用可能な変数は左側の画面に表示され、本文は右側の画面に表示されます。

5. [Settings] の下で、次に応じて通知の配信オプションを選択します。
   - Send consolidated notifications every [xx] [hours or days] — 変数フィールドで入力した時間数または日数ごとに通知を送信する場合、このオプションを選択します。
   - Send consolidate notifications every [xx] occurrences — 変数フィールドで入力した回数発生した後に通知を送信する場合、このオプションを選択します。
   - Send individual notifications — イベントが発生するたびに通知を送信する場合、このオプションを選択します。
6. [Advanced Notification (SNMP)] の下で、[SNMP] を選択してこのオプションを有効にします。
7. [Show details] をクリックしてオプションを展開し、次に応じて設定を行います。
   - IP Address
   - Community
   - Message
8. [Write to Windows event log] を選択すると、それぞれの通知を Windows イベントログに書き込みます。
9. [Save] をクリックします。

コンテンツフィルタ通知の設定

コンテンツフィルタ 通知を設定するために必要な手順を説明します。

手順

1. 左側のメニューで、[Content Filtering] をクリックします。[Content Filtering] 画面が表示されます。

2. [Add] をクリックして新規ポリシーを追加するか、[Policy] 列の既存のポリシーをクリックします。[Content Filtering: Edit Policy] 画面が表示されます。
3. [Notification] タブをクリックします。
4. [People to notify] で、[Notify administrator] を選択してコンテンツフィルタ通知を有効にします。
5. [People to notify] の下の [Show details] をクリックして次を設定します。
   - To — グローバルメールアドレスがこのフィールドに 表示されます。追加のメールアドレスはセミコロン (;) で区切って入力して、独自の通知を作成します。
   - Subject — メールの件名の行に表示される件名を入力します (例: Content Filtering Notification)。
   - Message — 変数を使用して独自のメッセージを作成できます (変数の例: [Server Name]、[Content Rules]、[Date]、[Time]、[File Name/Web Content Title]、[File/Web Content Location]、[Action]、[Violator])。

   
   注意
   使用可能な変数は左側の画面に表示され、本文は右側の画面に表示されます。
6. [Settings] の下で、次に応じて通知の配信オプションを選択します。
   - Send consolidated notifications every [xx] [hours or days] — 変数フィールドで入力した時間数または日数ごとに通知を送信する場合、このオプションを選択します。
   - Send consolidate notifications every [xx] occurrences — 変数フィールドで入力した回数発生した後に通知を送信する場合、このオプションを選択します。
   - Send individual notifications — イベントが発生するたびに通知を送信する場合、このオプションを選択します。
7. [Advanced Notification (SNMP)] の下で、[SNMP] を選択してこのオプションを有効にします。

8. [Show details] をクリックしてオプションを展開し、次に応じて設定を行います。
   - IP Address
   - Community
   - Message
9. [Write to Windows event log] を選択すると、それぞれの通知を Windows イベントログに書き込みます。
10. [Save] をクリックします。

情報漏えい対策通知の設定

情報漏えい対策通知を設定するために必要な手順を説明します。

手順

1. 左側のメニューで、[Data Loss Prevention] > [Policies] をクリックします。[Data Loss Prevention] 画面が表示されます。
2. [Add] をクリックして新規ポリシーを追加するか、[Policy] 列の既存のポリシーをクリックします。[Data Loss Prevention: Edit Policy] 画面が表示されます。
3. [Notification] タブをクリックします。
4. [People to notify] で、[Notify administrator] を選択して情報漏えい対策通知を有効にします。
5. [People to notify] の下の [Show details] をクリックして次を設定します。
   - To — グローバルメールアドレスがこのフィールドに 表示されます。追加のメールアドレスはセミコロン (;) で区切って入力して、独自の通知を作成します。
   - Subject — メールの件名の行に表示される件名を入力します (例: Data Loss Prevention Notification)。
   - Message — 変数を使用して独自のメッセージを作成できます (変数の例: [Server Name]、[Data Loss Prevention Rules]、[Date]、[Time]、

[File Name/Web Content Title]、[File/Web Content Location]、[Action]、[Violator])。

注意

使用可能な変数は左側の画面に表示され、本文は右側の画面に表示されます。

6. [Settings] の下で、次に応じて通知の配信オプションを選択します。
   - Send consolidated notifications every [xx] [hours or days] — 変数フィールドで入力した時間数または日数ごとに通知を送信する場合、このオプションを選択します。
   - Send consolidate notifications every [xx] occurrences — 変数フィールドで入力した回数発生した後に通知を送信する場合、このオプションを選択します。
   - Send individual notifications — イベントが発生するたびに通知を送信する場合、このオプションを選択します。
7. [Advanced Notification (SNMP)] の下で、[SNMP] を選択してこのオプションを有効にします。
8. [Show details] をクリックしてオプションを展開し、次に応じて設定を行います。
   - IP Address
   - Community
   - Message
9. [Write to Windows event log] を選択すると、それぞれの通知を Windows イベントログに書き込みます。
10. [Save] をクリックします。

Web レピュテーション通知の設定

Web レピュテーション通知を設定するために必要な手順を説明します。

手順

1. 左側のメニューで、[Web Reputation] をクリックします。[Web Reputation] 画面が表示されます。
2. [Notification] タブをクリックします。
3. [People to notify] で、[Notify administrator] を選択して Web レピュテーション通知を有効にします。
4. [People to notify] の下の [Show details] をクリックして次を設定します。
   - To — グローバルメールアドレスがこのフィールドに 表示されます。追加のメールアドレスはセミコロン (;) で区切って入力して、独自の通知を作成します。
   - Subject — メールの件名の行に表示される件名を入力します (例: Web Reputation Notification)。
   - Message — 変数を使用して独自のメッセージを作成できます (変数の例: [Server Name]、[Suspicious URLs]、[Date]、[Time]、[Web Content Title]、[Web Content Location]、[Action]、[Violator])。

   注意

   使用可能な変数は左側の画面に表示され、本文は右側の画面に表示されます。
5. [Settings] の下で、次に応じて通知の配信オプションを選択します。
   - Send consolidated notifications every [xx] [hours or days] — 変数フィールドで入力した時間数または日数ごとに通知を送信する場合、このオプションを選択します。
   - Send consolidate notifications every [xx] occurrences — 変数フィールドで入力した回数発生した後に通知を送信する場合、このオプションを選択します。
   - Send individual notifications — イベントが発生するたびに通知を送信する場合、このオプションを選択します。
6. [Advanced Notification (SNMP)] の下で、[SNMP] を選択してこのオプションを有効にします。

7. [Show details] をクリックしてオプションを展開し、次に応じて設定を行います。
   - IP Address
   - Community
   - Message
8. [Write to Windows event log] を選択すると、それぞれの通知を Windows イベントログに書き込みます。
9. [Save] をクリックします。

手動検索通知

ここでは、手動検索のさまざまな通知を設定する方法について説明します。

手動検索通知 – セキュリティリスク検索の設定

手動検索のセキュリティリスク検索通知を設定するために必要な手順を説明します。

手順

1. 左側のメニューで、[Manual Scan] をクリックします。[Manual Scan] 画面が表示されます。
2. [Select the scan type] の下にある [Security risk scan] リンクをクリックします。
3. [Notification] タブをクリックします。
4. [People to notify] の下で、次のオプションを選択します。
   - Notify violator
   - Notify administrator

注意

[Notify violator] オプションでは、[Subject] と [Message] のみを含めることができます。[Notify administrator] の統合通知 (consolidated notifications) の設定は違反ユーザ (violator) には使用できません。

5. [People to notify] の下の [Notify violator] または [Notify administrator] の横にある [Show details] をクリックして次を設定します。

注意

[Notify violator] オプションでは、[To] フィールドは使用しません。

- To — グローバルメールアドレスがこのフィールドに 表示されます。追加のメールアドレスはセミコロンで区切って入力して、独自の通知を作成します。
- Subject — メールの件名の行に表示される件名を入力します (例: Security Risk Notification)。
- Message — 変数を使用して独自のメッセージを作成できます (変数の例: [Server Name]、[Security Risk Name]、[Date]、[Time]、[File Name]、[File Location]、[Action]、[Violator])。

注意

使用可能な変数は左側の画面に表示され、本文は右側の画面に表示されます。

6. [Settings] の下で、次に応じて通知の配信オプションを選択します。
   - Send consolidated notifications every [xx] [hours or days] — 変数フィールドで入力した時間数または日数ごとに通知を送信する場合、このオプションを選択します。
   - Send consolidate notifications every [xx] occurrences — 変数フィールドで入力した回数発生した後に通知を送信する場合、このオプションを選択します。
   - Send individual notifications — イベントが発生するたびに通知を送信する場合、このオプションを選択します。

7. [Advanced Notification (SNMP)] の下で、[SNMP] を選択してこのオプションを有効にします。
8. [Show details] をクリックしてオプションを展開し、次に応じて設定を行います。
   - IP Address
   - Community
   - Message
9. [Write to Windows event log] を選択すると、それぞれの通知を Windows イベントログに書き込みます。
10. [Save] をクリックします。

手動検索通知 — ファイルブロックの設定

手動検索のファイルブロック通知を設定するために必要な手順を説明します。

手順

1. 左側のメニューで、[Manual Scan] をクリックします。[Manual Scan] 画面が表示されます。
2. [Select the scan type] の下にある [File blocking] リンクをクリックします。
3. 既存のポリシーを選択するか、[Add] をクリックして新しいポリシーを作成します。
4. [Notification] タブをクリックします。
5. [People to notify] の下で、次のオプションを選択します。
   - Notify violator
   - Notify administrator

注意

[Notify violator] オプションでは、[Subject] と [Message] のみを含めることができます。[Notify administrator] の統合通知 (consolidated notifications) の設定は違反ユーザ (violator) には使用できません。

6. [People to notify] の下の [Notify violator] または [Notify administrator] の横にある [Show details] をクリックして次を設定します。
   - To — グローバルメールアドレスがこのフィールドに 表示されます。追加のメールアドレスはセミコロンで区切って入力して、独自の通知を作成します。
   - Subject — メールの件名の行に表示される件名を入力します (例: File Blocking Notification)。
   - Message — 変数を使用して独自のメッセージを作成できます (変数の例: [Server Name]、[File Blocking Rules]、[Date]、[Time]、[File Name]、[File Location]、[Action]、[Violator])。

注意

使用可能な変数は左側の画面に表示され、本文は右側の画面に表示されます。

7. [Settings] の下で、次に応じて通知の配信オプションを選択します。
   - Send consolidated notifications every [xx] [hours or days] — 変数フィールドで入力した時間数または日数ごとに通知を送信する場合、このオプションを選択します。
   - Send consolidate notifications every [xx] occurrences — 変数フィールドで入力した回数発生した後に通知を送信する場合、このオプションを選択します。
   - Send individual notifications — イベントが発生するたびに通知を送信する場合、このオプションを選択します。
8. [Advanced Notification (SNMP)] の下で、[SNMP] を選択してこのオプションを有効にします。
9. [Show details] をクリックしてオプションを展開し、次に応じて設定を行います。

- IP Address
- Community
- Message — この手順のステップ 6 で説明したメッセージを作成します。

10. [Write to Windows event log] を選択すると、それぞれの通知を Windows イベントログに書き込みます。
11. [Save] をクリックします。

手動検索通知 — コンテンツフィルタの設定

手動検索のコンテンツフィルタ通知を設定するために必要な手順を説明します。

手順

1. 左側のメニューで、[Manual Scan] をクリックします。[Manual Scan] 画面が表示されます。
2. [Select the scan type] の下にある [Content filtering] リンクをクリックします。
3. 既存のポリシーを選択するか、[Add] をクリックして新しいポリシーを作成します。
4. [Notification] タブをクリックします。
5. [People to notify] の下で、次のオプションを選択します。
   - Notify violator
   - Notify administrator

> **注意**
> [Notify violator] オプションでは、[Subject] と [Message] のみを含めることができます。[Notify administrator] の統合通知 (consolidated notifications) の設定は違反ユーザ (violator) には使用できません。

6. [Notify Violator] の横の [Show details] をクリックして次の選択をします。
   - Subject — メールの件名の行に表示される件名を入力します (例: Content Filtering Notification)。
   - Message — 変数を使用して独自のメッセージを作成できます (変数の例: [Server Name]、[Content Rules]、[Date]、[Time]、[File Name/Web Content Title]、[File/Web Content Location]、[Action]、[Violator])。
7. [Notify administrator] の横の [Show details] をクリックして次を設定します。
   - To — グローバルメールアドレスがこのフィールドに 表示されます。追加のメールアドレスはセミコロンで区切って入力して、独自の通知を作成します。
   - Subject — メールの件名の行に表示される件名を入力します (例: Content Filtering Notification)。
   - Message — 変数を使用して独自のメッセージを作成できます (変数の例: [Server Name]、[Content Rules]、[Date]、[Time]、[File Name/Web Content Title]、[File/Web Content Location]、[Action]、[Violator])。

   注意

   使用可能な変数は左側の画面に表示され、本文は右側の画面に表示されます。
8. [Settings] の下で、次に応じて通知の配信オプションを選択します。
   - Send consolidated notifications every [xx] [hours or days] — 変数フィールドで入力した時間数または日数ごとに通知を送信する場合、このオプションを選択します。
   - Send consolidate notifications every [xx] occurrences — 変数フィールドで入力した回数発生した後に通知を送信する場合、このオプションを選択します。
   - Send individual notifications — イベントが発生するたびに通知を送信する場合、このオプションを選択します。

9. [Advanced Notification (SNMP)] の下で、[SNMP] を選択してこのオプションを有効にします。
10. [Show details] をクリックしてオプションを展開し、次に応じて設定を行います。
    - IP Address
    - Community
    - Message
11. [Write to Windows event log] を選択すると、それぞれの通知を Windows イベントログに書き込みます。
12. [Save] をクリックします。

手動検索通知 — 情報漏えい対策の設定

手動検索の情報漏えい対策通知を設定するために必要な手順を説明します。

手順

1. 左側のメニューで、[Manual Scan] をクリックします。[Manual Scan] 画面が表示されます。
2. [Select the scan type] の下にある [Data loss prevention] リンクをクリックします。
3. 既存のポリシーを選択するか、[Add] をクリックして新しいポリシーを作成します。
4. [Notification] タブをクリックします。
5. [People to notify] の下で、次のオプションを選択します。
    - Notify violator
    - Notify administrator

注意

[Notify violator] オプションでは、[Subject] と [Message] のみを含めることができます。[Notify administrator] の統合通知 (consolidated notifications) の設定は違反ユーザ (violator) には使用できません。

6. [Notify Violator] の横の [Show details] をクリックして次の選択をします。
   - Subject — メールの件名の行に表示される件名を入力します (例: Data Loss Prevention Notification)。
   - Message — 変数を使用して独自のメッセージを作成できます (変数の例: [Server Name]、[Data Loss Prevention Rules]、[Date]、[Time]、[File Name/Web Content Title]、[File/Web Content Location]、[Action]、[Violator])。
7. [Notify administrator] の横の [Show details] をクリックして次を設定します。
   - To — グローバルメールアドレスがこのフィールドに 表示されます。追加のメールアドレスはセミコロンで区切って入力して、独自の通知を作成します。
   - Subject — メールの件名の行に表示される件名を入力します (例: Data Loss Prevention Notification)。
   - Message — 変数を使用して独自のメッセージを作成できます (変数の例: [Server Name]、[Data Loss Prevention Rules]、[Date]、[Time]、[File Name/Web Content Title]、[File/Web Content Location]、[Action]、[Violator])。

注意

使用可能な変数は左側の画面に表示され、本文は右側の画面に表示されます。

8. [Settings] の下で、次に応じて通知の配信オプションを選択します。
   - Send consolidated notifications every [xx] [hours or days] — 変数フィールドで入力した時間数または日数ごとに通知を送信する場合、このオプションを選択します。

- Send consolidate notifications every [xx] occurrences — 変数フィールドで入力した回数発生した後に通知を送信する場合、このオプションを選択します。
- Send individual notifications — イベントが発生するたびに通知を送信する場合、このオプションを選択します。

9. [Advanced Notification (SNMP)] の下で、[SNMP] を選択してこのオプションを有効にします。
10. [Show details] をクリックしてオプションを展開し、次に応じて設定を行います。
    - IP Address
    - Community
    - Message
11. [Write to Windows event log] を選択すると、それぞれの通知を Windows イベントログに書き込みます。
12. [Save] をクリックします。

手動検索通知 — Web レピュテーションの設定

手動検索の Web レピュテーション通知を設定するために必要な手順を説明します。

手順

1. 左側のメニューで、[Manual Scan] をクリックします。[Manual Scan] 画面が表示されます。
2. [Select the scan type] の下にある [Web Reputation] リンクをクリックします。
3. [Notification] タブをクリックします。
4. [People to notify] の下で、次のオプションを選択します。
    - Notify violator

- Notify administrator

注意

[Notify violator] オプションでは、[Subject] と [Message] のみを含めることができます。[Notify administrator] の統合通知 (consolidated notifications) の設定は違反ユーザ (violator) には使用できません。

5. [People to notify] の下の [Notify violator] または [Notify administrator] の横にある [Show details] をクリックして次を設定します。
   - To — グローバルメールアドレスがこのフィールドに 表示されます。追加のメールアドレスはセミコロンで区切って入力して、独自の通知を作成します。
   - Subject — メールの件名の行に表示される件名を入力します (例: Web Reputation Notification)。
   - Message — 変数を使用して独自のメッセージを作成できます (変数の例: [Server Name]、[Suspicious URLs]、[Date]、[Time]、[Web Content Title]、[Web Content Location]、[Action]、[Violator])。

   注意

   使用可能な変数は左側の画面に表示され、本文は右側の画面に表示されます。

6. [Settings] の下で、次に応じて通知の配信オプションを選択します。
   - Send consolidated notifications every [xx] [hours or days] — 変数フィールドで入力した時間数または日数ごとに通知を送信する場合、このオプションを選択します。
   - Send consolidate notifications every [xx] occurrences — 変数フィールドで入力した回数発生した後に通知を送信する場合、このオプションを選択します。
   - Send individual notifications — イベントが発生するたびに通知を送信する場合、このオプションを選択します。
7. [Advanced Notification (SNMP)] の下で、[SNMP] を選択してこのオプションを有効にします。

8. [Show details] をクリックしてオプションを展開し、次に応じて設定を行います。
   - IP Address
   - Community
   - Message
9. [Write to Windows event log] を選択すると、それぞれの通知を Windows イベントログに書き込みます。
10. [Save] をクリックします。

予約検索通知

ここでは、予約検索のさまざまな通知を設定する方法について説明します。

予約検索通知 – セキュリティリスク検索の設定

セキュリティリスク検索の予約検索通知を設定するために必要な手順を説明します。

手順

1. 左側のメニューで、[Scheduled Scan] をクリックします。[Scheduled Scan] 画面が表示されます。
2. [Add] をクリックして新規タスクを追加するか、[Task Name] 列の既存のタスクをクリックします。[Scheduled Scan: Edit Scan Task] または [Scheduled Scan: Add Scan Task] 画面が表示されます。
3. [Select scan type] の下にある [Security risk scan] リンクをクリックします。
4. [Notification] タブをクリックします。
5. [People to notify] の下で、次のオプションを選択します。
   - Notify violator
   - Notify administrator

注意

[Notify violator] オプションでは、[Subject] と [Message] のみを含めることができます。[Notify administrator] の統合通知 (consolidated notifications) の設定は違反ユーザ (violator) には使用できません。

6. [People to notify] の下の [Notify violator] または [Notify administrator] の横にある [Show details] をクリックして次を設定します。
   - To — グローバルメールアドレスがこのフィールドに 表示されます。追加のメールアドレスはセミコロンで区切って入力して、独自の通知を作成します。
   - Subject — メールの件名の行に表示される件名を入力します (例: Security Risk Notification)。
   - Message — 変数を使用して独自のメッセージを作成できます (変数の例: [Server Name]、[Security Risk Name]、[Date]、[Time]、[File Name]、[File Location]、[Action]、[Violator])。

注意

使用可能な変数は左側の画面に表示され、本文は右側の画面に表示されます。

7. [Settings] の下で、次に応じて通知の配信オプションを選択します。
   - Send consolidated notifications every [xx] [hours or days] — 変数フィールドで入力した時間数または日数ごとに通知を送信する場合、このオプションを選択します。
   - Send consolidate notifications every [xx] occurrences — 変数フィールドで入力した回数発生した後に通知を送信する場合、このオプションを選択します。
   - Send individual notifications — イベントが発生するたびに通知を送信する場合、このオプションを選択します。
8. [Advanced Notification (SNMP)] の下で、[SNMP] を選択してこのオプションを有効にします。
9. [Show details] をクリックしてオプションを展開し、次に応じて設定を行います。

- IP Address
- Community
- Message

10. [Write to Windows event log] を選択すると、それぞれの通知を Windows イベントログに書き込みます。
11. [Save] をクリックします。

予約検索通知 — ファイルブロックの設定

ファイルブロックの予約検索通知を設定するために必要な手順を説明します。

手順

1. 左側のメニューで、[Scheduled Scan] をクリックします。[Scheduled Scan] 画面が表示されます。
2. [Task Name] 列の既存のタスクをクリックします。[Scheduled Scan: Edit Scan Task] 画面が表示されます。
3. [Select scan type] の下にある [File blocking] リンクをクリックします。
4. 既存のポリシーを選択します。
5. [Notification] タブをクリックします。
6. [People to notify] の下で、次のオプションを選択します。
   - Notify violator
   - Notify administrator

   注意

   [Notify violator] オプションでは、[Subject] と [Message] のみを含めることができます。[Notify administrator] の統合通知 (consolidated notifications) の設定は違反ユーザ (violator) には使用できません。
7. [People to notify] の下の [Notify violator] または [Notify administrator] の横にある [Show details] をクリックして次を設定します。

- To — グローバルメールアドレスがこのフィールドに 表示されます。追加のメールアドレスはセミコロンで区切って入力して、独自の通知を作成します。
- Subject — メールの件名の行に表示される件名を入力します (例: File Blocking Notification)。
- Message — 変数を使用して独自のメッセージを作成できます (変数の例: [Server Name]、[File Blocking Rules]、[Date]、[Time]、[File Name]、[File Location]、[Action]、[Violator])。

注意

使用可能な変数は左側の画面に表示され、本文は右側の画面に表示されます。

8. [Settings] の下で、次に応じて通知の配信オプションを選択します。
   - Send consolidated notifications every [xx] [hours or days] — 変数フィールドで入力した時間数または日数ごとに通知を送信する場合、このオプションを選択します。
   - Send consolidate notifications every [xx] occurrences — 変数フィールドで入力した回数発生した後に通知を送信する場合、このオプションを選択します。
   - Send individual notifications — イベントが発生するたびに通知を送信する場合、このオプションを選択します。
9. [Advanced Notification (SNMP)] の下で、[SNMP] を選択してこのオプションを有効にします。
10. [Show details] をクリックしてオプションを展開し、次に応じて設定を行います。
    - IP Address
    - Community
    - Message
11. [Write to Windows event log] を選択すると、それぞれの通知を Windows イベントログに書き込みます。

12. [Save] をクリックします。

予約検索通知 — コンテンツフィルタの設定

コンテンツフィルタの 予約検索通知を設定するために必要な手順を説明します。

手順

1. 左側のメニューで、[Scheduled Scan] をクリックします。[Scheduled Scan] 画面が表示されます。
2. [Task Name] 列の既存のタスクをクリックします。[Scheduled Scan: Edit Scan Task] 画面が表示されます。
3. [Select scan type] の下にある [Content Filtering] リンクをクリックします。
4. 既存のポリシーを選択します。
5. [Notification] タブをクリックします。
6. [People to notify] の下で、次のオプションを選択します。
   - Notify violator
   - Notify administrator

   注意

   [Notify violator] オプションでは、[Subject] と [Message] のみを含めることができます。[Notify administrator] の統合通知 (consolidated notifications) の設定は違反ユーザ (violator) には使用できません。
7. [People to notify] の下の [Notify violator] または [Notify administrator] の横にある [Show details] をクリックして次を設定します。
   - To — グローバルメールアドレスがこのフィールドに 表示されます。追加のメールアドレスはセミコロンで区切って入力して、独自の通知を作成します。
   - Subject — メールの件名の行に表示される件名を入力します (例: Content Filtering Notification)。

- Message — 変数を使用して独自のメッセージを作成できます (変数の例: [Server Name]、[Content Rules]、[Date]、[Time]、[File Name/Web Content Title]、[File/Web Content Location]、[Action]、[Violator])。

注意

使用可能な変数は左側の画面に表示され、本文は右側の画面に表示されます。

8. [Settings] の下で、次に応じて通知の配信オプションを選択します。
   - Send consolidated notifications every [xx] [hours or days] — 変数フィールドで入力した時間数または日数ごとに通知を送信する場合、このオプションを選択します。
   - Send consolidate notifications every [xx] occurrences — 変数フィールドで入力した回数発生した後に通知を送信する場合、このオプションを選択します。
   - Send individual notifications — イベントが発生するたびに通知を送信する場合、このオプションを選択します。
9. [Advanced Notification (SNMP)] の下で、[SNMP] を選択してこのオプションを有効にします。
10. [Show details] をクリックしてオプションを展開し、次に応じて設定を行います。
    - IP Address
    - Community
    - Message
11. [Write to Windows event log] を選択すると、それぞれの通知を Windows イベントログに書き込みます。
12. [Save] をクリックします。

予約検索通知 — 情報漏えい対策の設定

情報漏えい対策の予約検索通知を設定するために必要な手順を説明します。

手順

1. 左側のメニューで、[Scheduled Scan] をクリックします。[Scheduled Scan] 画面が表示されます。
2. [Task Name] 列の既存のタスクをクリックします。[Scheduled Scan: Edit Scan Task] 画面が表示されます。
3. [Select scan type] の下にある [Data loss prevention] リンクをクリックします。
4. 既存のポリシーを選択します。
5. [Notification] タブをクリックします。
6. [People to notify] の下で、次のオプションを選択します。
   - Notify violator
   - Notify administrator

   注意

   [Notify violator] オプションでは、[Subject] と [Message] のみを含めることができます。[Notify administrator] の統合通知 (consolidated notifications) の設定は違反ユーザ (violator) には使用できません。
7. [People to notify] の下の [Notify violator] または [Notify administrator] の横にある [Show details] をクリックして次を設定します。
   - To — グローバルメールアドレスがこのフィールドに 表示されます。追加のメールアドレスはセミコロンで区切って入力して、独自の通知を作成します。
   - Subject — メールの件名の行に表示される件名を入力します (例: Data Loss Prevention Notification)。
   - Message — 変数を使用して独自のメッセージを作成できます (変数の例: [Server Name]、[Data Loss Prevention Rules]、[Date]、[Time]、[File Name/Web Content Title]、[File/Web Content Location]、[Action]、[Violator])。

注意

使用可能な変数は左側の画面に表示され、本文は右側の画面に表示されます。

8. [Settings] の下で、次に応じて通知の配信オプションを選択します。
   - Send consolidated notifications every [xx] [hours or days] — 変数フィールドで入力した時間数または日数ごとに通知を送信する場合、このオプションを選択します。
   - Send consolidate notifications every [xx] occurrences — 変数フィールドで入力した回数発生した後に通知を送信する場合、このオプションを選択します。
   - Send individual notifications — イベントが発生するたびに通知を送信する場合、このオプションを選択します。
9. [Advanced Notification (SNMP)] の下で、[SNMP] を選択してこのオプションを有効にします。
10. [Show details] をクリックしてオプションを展開し、次に応じて設定を行います。
    - IP Address
    - Community
    - Message
11. [Write to Windows event log] を選択すると、それぞれの通知を Windows イベントログに書き込みます。
12. [Save] をクリックします。

予約検索通知 — Web レピュテーションの設定

Web レピュテーションの予約検索通知を設定するために必要な手順を説明します。

手順

1. 左側のメニューで、[Scheduled Scan] をクリックします。[Scheduled Scan] 画面が表示されます。
2. [Task Name] 列の既存のタスクをクリックします。[Scheduled Scan: Edit Scan Task] 画面が表示されます。
3. [Select scan type] の下にある [Web Reputation] リンクをクリックします。
4. [Notification] タブをクリックします。
5. [People to notify] の下で、次のオプションを選択します。
   - Notify violator
   - Notify administrator

   注意
   [Notify violator] オプションでは、[Subject] と [Message] のみを含めることができます。[Notify administrator] の統合通知 (consolidated notifications) の設定は違反ユーザ (violator) には使用できません。
6. [People to notify] の下の [Notify violator] または [Notify administrator] の横にある [Show details] をクリックして次を設定します。
   - To — グローバルメールアドレスがこのフィールドに 表示されます。追加のメールアドレスはセミコロンで区切って入力して、独自の通知を作成します。
   - Subject — メールの件名の行に表示される件名を入力します (例: Web Reputation Notification)。
   - Message — 変数を使用して独自のメッセージを作成できます (変数の例: [Server Name]、[Suspicious URLs]、[Date]、[Time]、[Web Content Title]、[Web Content Location]、[Action]、[Violator])。

   注意
   使用可能な変数は左側の画面に表示され、本文は右側の画面に表示されます。

7. [Settings] の下で、次に応じて通知の配信オプションを選択します。
   - Send consolidated notifications every [xx] [hours or days] — 変数フィールドで入力した時間数または日数ごとに通知を送信する場合、このオプションを選択します。
   - Send consolidate notifications every [xx] occurrences — 変数フィールドで入力した回数発生した後に通知を送信する場合、このオプションを選択します。
   - Send individual notifications — イベントが発生するたびに通知を送信する場合、このオプションを選択します。
8. [Advanced Notification (SNMP)] の下で、[SNMP] を選択してこのオプションを有効にします。
9. [Show details] をクリックしてオプションを展開し、次に応じて設定を行います。
   - IP Address
   - Community
   - Message
10. [Write to Windows event log] を選択すると、それぞれの通知を Windows イベントログに書き込みます。
11. [Save] をクリックします。

警告

警告機能は、システムイベントおよびアウトブレークの 通知を行います。ここでは、次のオプションを有効化および設定する方法について説明します。

システムイベント

システムイベントにより、PortalProtect のさまざまな機能の状態に関する通知を送信できます。これらの通知の内容は、次のとおりです。

- PortalProtect Services
  - PortalProtect service did not start successfully (PortalProtect サービスが正常に起動しませんでした)

- PortalProtect service is unavailable (PortalProtect サービスを使用できません)

- PortalProtect Events
  - Smart Protection Server—Each time File Reputation service was [Unavailable] or [Recovered] (ファイルレピュテーションサービスが使用不能か回復されるたびに通知を送信)
  - Smart Protection Server—Each time Web Reputation service was [Unavailable] or [Recovered] (Web レピュテーションサービスが使用不能か回復されるたびに通知を送信)
  - Update—Each time update was [Unsuccessful] or [Successful] (アップデートが成功または失敗するたびに通知を送信)
  - Update—Last update time is older than [x] [hour(s) or day(s)] (前回のアップデート日時が [x] (時間または日数) より前の場合は通知を送信)
  - Manual/Scheduled scan tasks were [Unsuccessful] or [Successful] (手動/予約検索タスクが失敗または成功した場合に通知を送信)
  - Manual/Scheduled scan time exceeds [x] [hour(s) or day(s)] (手動/予約検索の実行時間が [x] (時間または日数) を超えた場合に通知を送信)
  - The disk space on the local drive (volume) of the backup directory is less than [x-GB/MB] (バックアップディレクトリ用ローカルドライブ (ボリューム) のディスク容量が [x-GB/MB] 未満になった場合に通知を送信)

    Specify time interval to send consecutive alerts if above problem still exists [x] [min(s)/hr(s)] (上記の問題が続く場合、[x] (分/時間) の間隔で連続的に警告を送信)
  - The log database size exceeds [x-GB/MB] (ログデータベースサイズが [x-GB/MB] を超えた場合に通知を送信)

    Specify time interval to send consecutive alerts if above problem still exists [x] [min(s)/hr(s)] (上記の問題が続く場合、[x] (分/時間) の間隔で連続的に警告を送信)

- The size of quarantined files exceeds [x-GB/MB] (隔離ファイルのサイズが [x-GB/MB] を超えた場合に通知を送信)

また、問題が継続的に発生する場合は、連続する警告の送信頻度を設定できます。

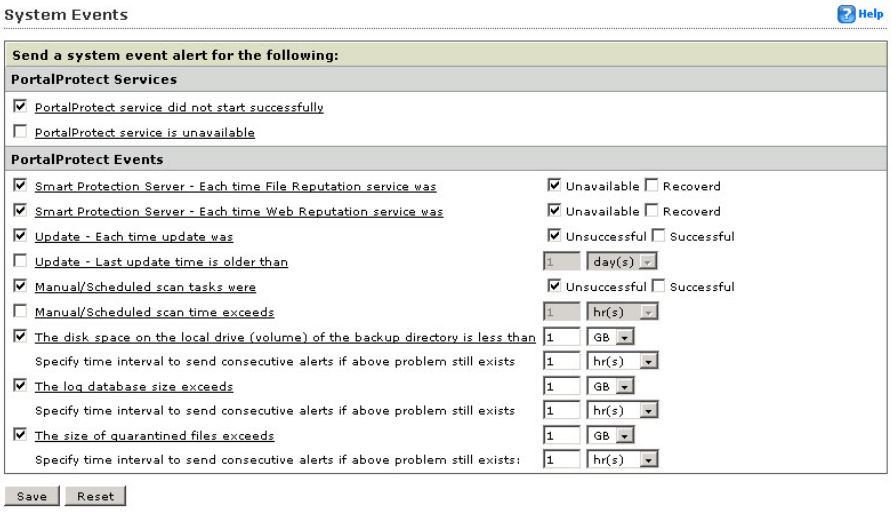


図 11-1. システムイベント設定画面

PortalProtect サービスに関するシステムイベントの設定

手順

1. [Alerts] > [System Events] をクリックします。[System Events] 画面が表示されます。
2. [PortalProtect Services] の下で、次のオプションを選択します。
   - PortalProtect service did not start successfully (PortalProtect サービスが正常に起動しませんでした)
   - PortalProtect service is unavailable (PortalProtect サービスを使用できません)

3. オプションを選択したら、リンクをクリックして [Administrator Notification] 画面を表示します。
4. 207 ページの「セキュリティリスク検索通知の設定」で説明したように、カスタムメッセージおよびメールリストを作成します。
5. [Save] をクリックします。

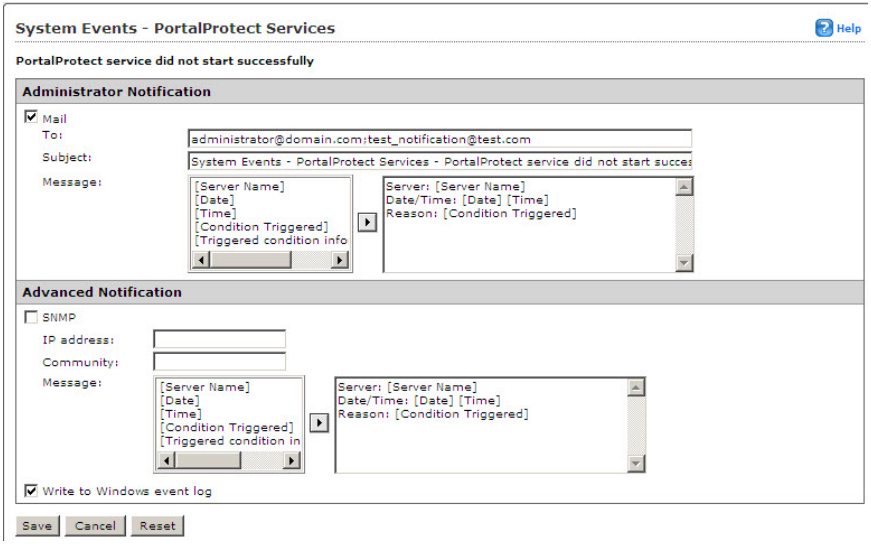


図 11-2. [System Events]、 ([Administrator Notification] 画面)

PortalProtect イベントに関するシステムイベントの設定

手順

1. [Alerts] > [System Events] をクリックします。[System Events] 画面が表示されます。
2. [PortalProtect Events] の下で、次のオプションを選択します。
   - Smart Protection Server - Each time File Reputation service was [Unavailable] or [Recovered] — セキュリティリスク検索サービスが利用できなくなった場合に単一の通知を受信するには [Unavailable]

を選択します。セキュリティリスク検索サービスを利用できるようになったときに単一の通知を受信するには [Recovered] を選択します。

- Smart Protection Server - Each time Web Reputation service was [Unavailable] or [Recovered] — Web レピュテーションサービスが利用できなくなった場合に単一の通知を受信するには [Unavailable] を選択します。Web レピュテーションサービスを利用できるようになったときに単一の通知を受信するには [Recovered] を選択します。
- Update - each time update was [Unsuccessful] or [Successful] — アップデートの成功/失敗の通知を送信するかどうかをこのオプションで選択します。
- Update - Last update is older than [x][hour(s) or day(s)] — フィールドに値を入力して、[day(s)] または [hour(s)] を選択します。前回のアップデート日時からの期間がその値に達すると、通知が送信されます。
- Manual/Scheduled scan tasks were [Unsuccessful] or [Successful] — 手動/予約検索タスクの成功/失敗の通知を送信するかどうかをこのオプションで選択します。
- Manual/Scheduled scan time exceeds [x][hour(s) or day(s)] — フィールドに値を入力して、[day(s)] または [hour(s)] を選択します。検索時間がその値を超えると、通知が送信されます。
- The disk space on the local drive (volume) of the backup directory is less than [x-MB/GB] — フィールドに値を入力して、[MB] (メガバイト) または [GB] (ギガバイト) を選択します。指定された領域のハードディスク空き容量がこの値より小さくなると、通知が送信されます。

  Specify time interval to send consecutive alerts if above problem [available disk space] still exists — フィールドに値を入力して、[minute(s)] または [hour(s)] を選択します。指定された時間に達するごとに、別の通知が送信されます。
- Log database size exceeds [x-GB/MB] — フィールドに値を入力して、[day(s)] または [hour(s)] を選択します。

Specify time interval to send consecutive alerts if above problem still exists — フィールドに値を入力して、[minute(s)] または [hour(s)] を選択します。指定された時間に達するごとに、別の通知が送信されます。

- The size of quarantined files exceeds [x-GB/MB] — フィールドに値を入力して、[day(s)] または [hour(s)] を選択します。

  Specify time interval to send consecutive alerts if above problem still exists — フィールドに値を入力して、[minute(s)] または [hour(s)] を選択します。指定された時間に達するごとに、別の通知が送信されます。

注意

ファーム環境内で警告が重複して発生するのを避けるために、[The size of quarantined file exceeds] の警告は 1 つの PortalProtect サーバのみで有効にし、ファーム内の他のすべての PortalProtect サーバではこのオプションを無効にしてください。

3. オプションを選択して通知を実行するパラメータを設定したら、リンクをクリックして [Administrator Notification] 画面を表示します。
4. 207 ページの「セキュリティリスク検索通知の設定」で説明したように、カスタムメッセージおよびメールリストを作成します。
5. [Save] をクリックします。

アウトブレークアラート

アウトブレークアラートにより、次の場合に管理者に警告するように設定できます。

- 指定された期間内に、検出されたウイルスが指定された数に達した場合
- 指定された期間内に、駆除できないウイルスが指定された数に達した場合
- 指定された期間内に、ブロックされたファイルが指定された数に達した場合

アウトブレークアラートの設定

手順

1. 左側のメニューで [Alerts] > [Outbreak Alert] をクリックします。[Outbreak Alert] 画面が表示されます。
2. [Number] フィールドに、アラートを実行する、検出されたウイルス、駆除できないウイルス、ブロックされたファイルの個数を入力します。さらに、[Time] フィールドに値を入力して、その値の単位が [Hours] か [Minutes] かを選択します。

   注意

   アウトブレークアラートは、指定された期間内に [Number] に達した場合に通知します。たとえば、検出されたウイルスで、[Number] フィールドに 25 を入力し、[Time] に 24 時間と入力した場合、24 時間の期間内に 25 以上のウイルスが検出されるとアウトブレークアラートが通知されます。

3. 次のオプションを設定します。
   - [Virus detected reach the following number within the shown time] — [number] [time value] [hours/minutes] を選択します。
   - [Uncleanable viruses reach the following number within the shown time] — [number] [time value] [hours/minutes] を選択します。
   - [Blocked files reach the following number within the shown time] — [number] [time value] [hours/minutes] を選択します。
4. [Save] をクリックします。

アクセス制御について

PortalProtect 製品コンソールのメニューおよびサブメニュー項目に対するアクセス権の付与や制御を行うには、役割ベースの管理機能を使用します。この機能では、管理者以外のユーザに製品コンソールへの表示のみのアクセス権を付与することもできます。PortalProtect には、Administrator と

Operator の 2 つの役割が用意されています。Operator の役割で使用可能な権限は、組織の要求に合わせて変更できます。

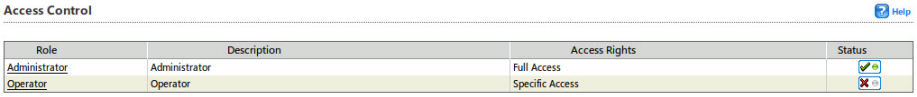


図 11-3. [Access Control] メイン画面

アクセス制御の認証

ここでは、[Access Control] の [Authentication] 設定画面について説明します。この画面では、特定の AD ユーザおよび AD グループを選択して、Administrator または Operator のいずれかの役割に追加できます。

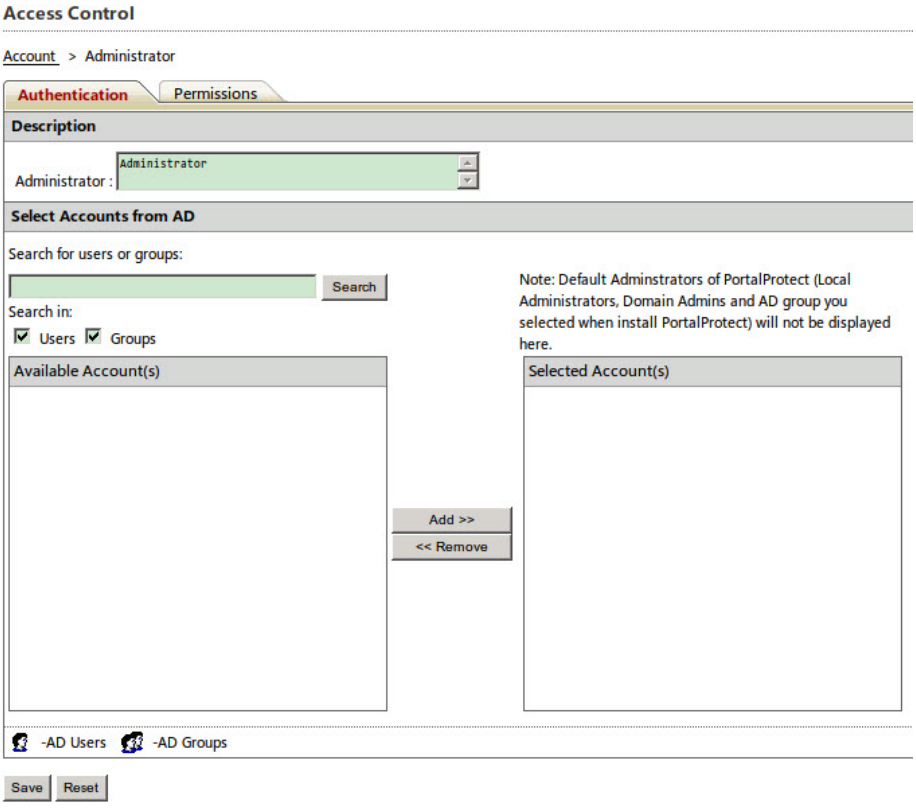


図 11-4. 管理者用の [Access Control]、[Authentication] 画面

[Access Control] の [Authentication] 画面に表示される各種フィールドおよび機能の説明を次に示します。

- Description — このフィールドでは、Administrator または Operator のいずれかに対する説明を変更できます。初期設定の説明は、「Administrator」と「Operator」です。
- Select Accounts from AD — このセクションでは、AD ユーザおよび AD グループを検索し、Administrator または Operator の役割を適用するためにそれらを追加できます。

アクセス制御の権限

PortalProtect では、特定の機能へのアクセスを許可または拒否する権限をカスタマイズできます。Administrator の役割は、すべての権限とアクセス権を有し、それらの権限は変更できません。ただし、業務の要求に従って Operator が権限を利用できるようにカスタマイズできます。

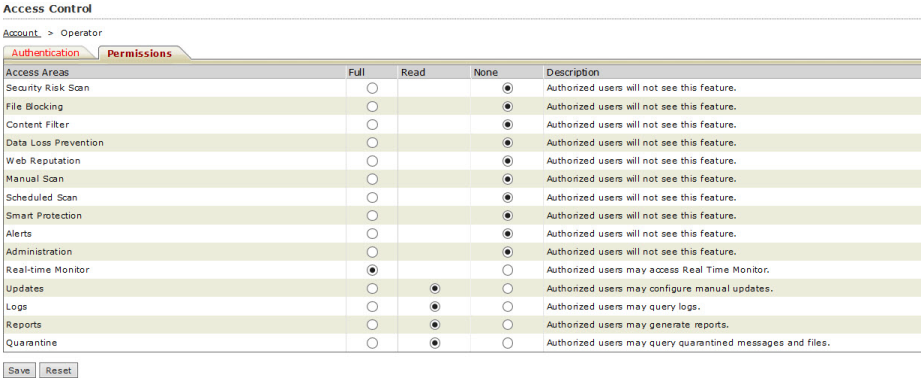


図 11-5. Operator のアクセス制御の権限 ([Access Control]、[Permissions] 画面)

ログの使用

PortalProtect では、ウイルス検索に関する包括的な情報を提供します。これらの情報はデータベースに保存されます。そのデータベースにクエリを実行してログを取得し、分析することができます。たとえば、セキュリティリスク検索ログを分析して最も流行しているウイルスおよび検索処理を確認し、ウイルスをネットワーク内に持ち込んだユーザを特定できます。

ログで得られる情報を使用して、システムの脆弱性を低減させ、セキュリティポリシーの効果を確認することができ、さらに必要に応じてポリシーを修

正できます。また、ログデータを.csv 形式でファイル出力して、詳細な分析を行ったり情報を共有することができます。

次に、各種ウイルスログ内に含まれる情報を示します。

- [Security risk scan] ログ — 日時、違反ユーザ、セキュリティリスク名、処理、ファイル名、場所などの情報が含まれます。セキュリティ検索ログは、次の項目でフィルタできます。
  - All
  - Detected virus/malware
  - Uncleanable virus/malware
  - Detected spyware/grayware
- [File blocking] ログ — 日時、違反ユーザ、ポリシー名、処理、ファイル名、実行される原因となったファイルの種類/名前、場所などの情報が含まれます。
- [Content Filtering] ログ — 日時、違反ユーザ、ポリシー名、処理、ファイル名/Web コンテンツのタイトル、実行される原因となったキーワード、場所などの情報が含まれます。
- [Data loss prevention] ログ — 日時、違反ユーザ、ポリシー名、処理、ファイル名/Web コンテンツのタイトル、テンプレート、場所などの情報が含まれます。
- [Web reputation] ログ — 日時、違反ユーザ、リスクレベル、Web コンテンツのタイトル、疑わしい URL、処理、場所などの情報が含まれます。
- [Update] ログ — 日時、説明などの情報が含まれます。
- [Scan events] ログ — 日時、説明などの情報が含まれます。
- [Backup] ログ — 日時、違反ユーザ、セキュリティリスク名、ファイル名、場所、バックアップパスなどの 情報が含まれます。
- [Unscannable files] ログ — 日時、場所、違反ユーザ、理由、ファイル名、処理などの情報が含まれます。
- [Event tracking] ログ — ユーザ名、イベント時刻、IP アドレス、イベントの種類、ソースの種類、説明などの情報が含まれます。

ログのクエリ

PortalProtect では、さまざまなログを表示し、ファイル出力して印刷することができます。クエリ機能を使用して、表示するログの種類を選択します。イベント、検出されたウイルス、コンポーネントアップデート、ブロックされたファイル、およびバックアップフォルダに配置されたファイルに関してクエリを実行できます。クエリで取得したログ情報は、ファイル出力したり印刷することができます。

ログのクエリの実行

手順

1. 左側のメニューで [Logs] > [Query] をクリックします。[Log Query] 画面が表示されます。
2. [Type] ドロップダウンからログの種類を選択します。
3. 期間を使用してクエリを実行するには、次の手順を実行します。
   - [Dates] フィールドからクエリの期間を選択します。期間は、[from:] の [MM/dd/yyyy] および時刻 [hh] と [mm]、および [to:] の [MM/dd/yyyy] および [hh] と [mm] で指定します。
4. [Violator] についてクエリを実行するには、次の手順を実行します。
   - [All] を選択してすべてのユーザを検索します。
   - または、[Specify user(s)] を選択し、ドロップダウンをクリックして特定の AD ユーザを検索対象として追加します。
5. [Site] についてクエリを実行するには、次の手順を実行します。
   - [All] を選択してすべてのサイトを検索します。
   - または、[Specify site(s)] を選択し、ドロップダウンをクリックして特定のサイトを検索対象として追加します。
6. [File name] を使用してクエリを実行するには、次の手順を実行します。
   - [File name] フィールドにファイル名のすべてまたは一部を入力します。

7. [Sort by] ドロップダウンから並べ替えオプションを選択し、[Ascending] または [Descending] を選択します。
8. [Display] フィールドで、1 ページ当たりに表示するログのエントリ数を入力します。初期設定は 15 です。
9. [Search] をクリックすると、クエリの結果が表示されます。
10. [Export] をクリックすると、クエリの結果が CSV ファイル (Unicode 標準) として出力されます。
11. [Print] をクリックすると、クエリの結果が印刷されます。

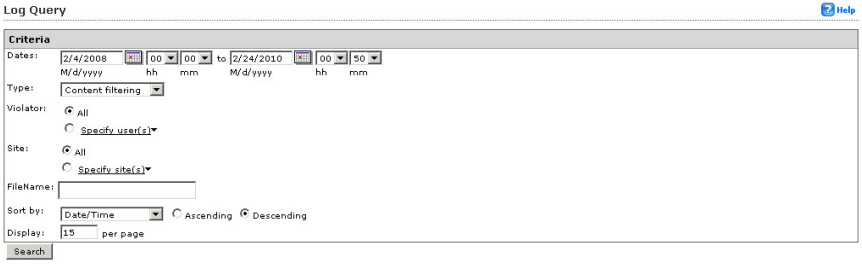


図 11-6. [Log Query] 画面

ログの削除設定

[Log Maintenance] 画面では、ログの履歴を削除する手動および自動のオプションを設定できます。この機能は、ハードディスクの空き容量が問題になっている場合や記録した情報が有用でなくなった場合などに、ハードディスクの容量の節約に役立ちます。ログは自動および手動で削除できます。

ログの手動削除

PortalProtect のログを手動で削除するために必要な手順を説明します。

手順

1. 左側のメニューで、[Logs] > [Maintenance] をクリックして、[Log Maintenance] 画面で [Manual] タブを選択します。
2. [Target] グループで、[All logs] を選択してすべてを削除するか、[Specified logs] を選択して次の基準で削除します。

- Security risk scan
- Web reputation
- Backup
- File blocking
- Updates
- Unscannable files
- Content filtering
- Scan events
- Event tracking
- Data loss prevention

3. [Action] グループの [Delete event tracking logs older than] フィールドおよび [Delete logs older than] フィールドに日数の値を入力します。

注意

[Delete event tracking logs older than] フィールドに入力した日数よりも古いイベントトラッキングログは削除されます。[Delete logs older than] フィールドに入力した日数よりも古いその他のログは削除されます。

4. [Delete Now] をクリックします。

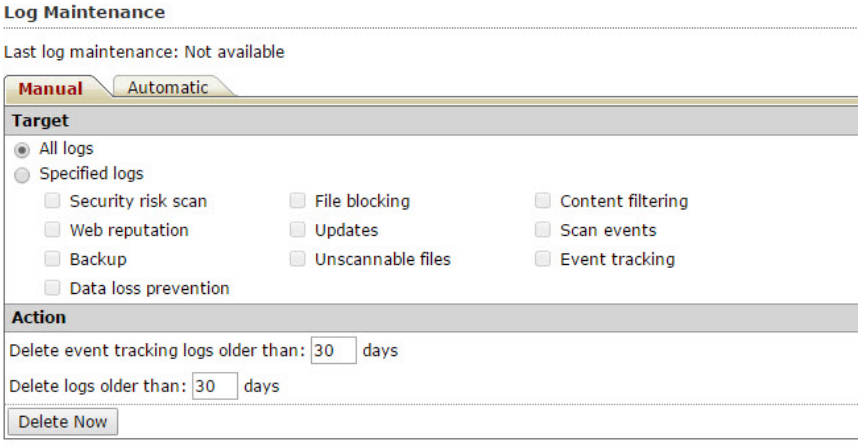


図 11-7. [Log Maintenance] の [Manual] タブ

ログの自動削除

ログを自動的に削除するように PortalProtect を設定できます。指定されたログの日数やサイズを超えたときに PortalProtect でログを自動的に削除するように設定できます。

手順

1. 左側のメニューで、[Logs] > [Maintenance] の順にクリックして、[Automatic] タブを選択します。
2. [Enable automatic maintenance] を選択します。
3. [Target] グループで、[All logs] を選択してすべてを削除するか、[Specified logs] を選択して次の基準で削除します。
   - Security risk scan
   - Web reputation
   - Backup
   - File blocking

- Updates
- Unscannable files
- Content filtering
- Scan events
- Event tracking
- Data loss prevention

4. [Action] グループの [Delete event tracking logs older than] フィールドおよび [Delete logs older than] フィールドに日数の値を入力します。

注意

[Delete event tracking logs older than] フィールドに入力した日数よりも古いイベントトラッキングログは削除されます。[Delete logs older than] フィールドに入力した日数よりも古いその他のログは削除されます。

5. [Save] をクリックします。

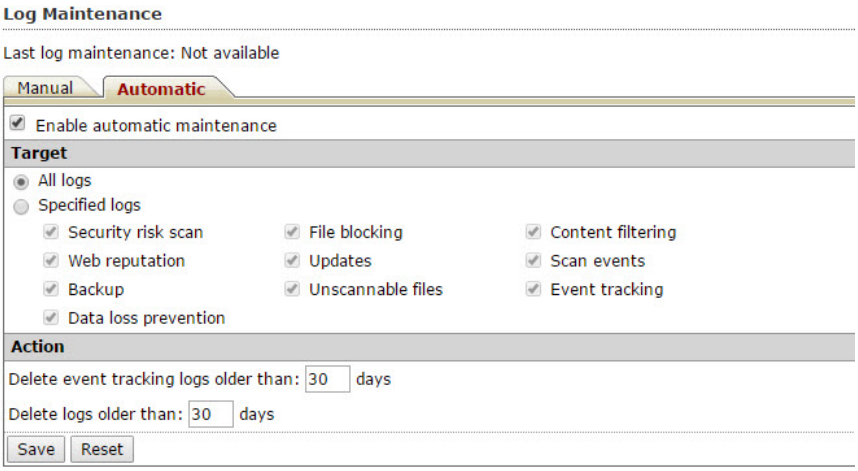


図 11-8. [Log Maintenance] の [Automatic] タブ

隔離の集中管理

隔離の管理では、手動検索と予約検索で隔離されたすべてのファイルを管理できます。PortalProtect 管理者は、ファーム内のすべての PortalProtect システムで隔離された隔離ファイルをクエリ、削除、復元、およびダウンロードすることができます。ここでは、隔離のクエリと削除設定機能について説明します。

隔離のクエリ

PortalProtect では、管理者が次の特定の検索基準を使用して隔離ファイルをクエリできます。

- 日付
- 時刻
- 違反ユーザ ([All] または [Specify user(s)])
- サイト ([All] または [Specify site(s)])
- ファイル名
- 種類 ([Security risk scan]、[File blocking]、[Content filtering]、[Data loss prevention]、[Unscannable files])

さらに、次の基準に従って検索結果を並べ替えて表示できます。

- 日時
- ファイル名
- 違反ユーザ
- 昇順および降順の並べ替え
- ページごとに表示する結果の数

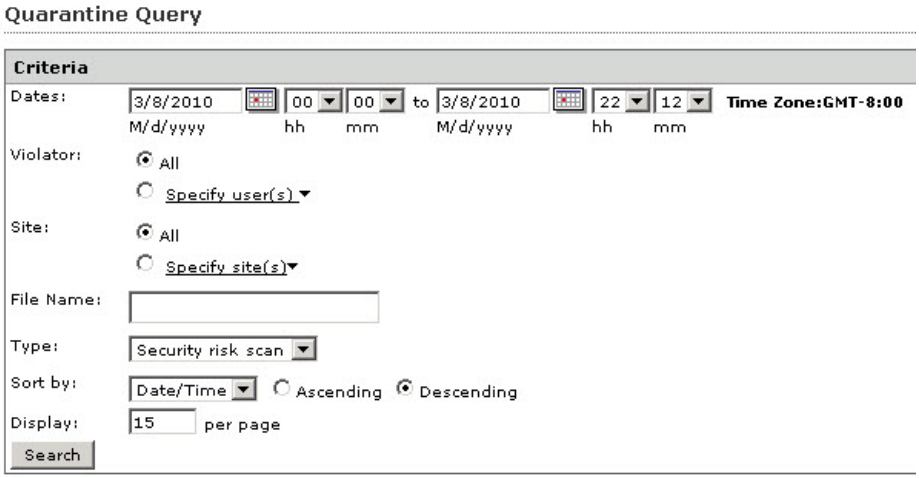


図 11-9. [Quarantine Query] メイン画面

表 11-1. 隔離の初期設定

設定名	初期設定
Date	1 日
Violator	All 注意 Active Directory から特定の違反ユーザを選択します。
Sites	All 注意 サイトツリーから特定のサイトを選択します。

設定名	初期設定
File Name	Null 注意 特定のファイル名を入力するか、空欄にして、すべての隔離ファイルを他の検索基準に従って検索します。
Sort by	Date/Time Descending
Display	ページあたり 15 レコード

管理者が隔離ファイルに対して実行できる機能の一部には、次のようなものがあります。

- 隔離ファイルは、クエリ後に復元または削除できます。
- ファイルブロック、コンテンツフィルタ、または情報漏えい対策によって隔離されたファイルは、クエリ後にダウンロードできます。

隔離のクエリの実行

手順

1. 左側のメニューで [Quarantine] > [Query] をクリックします。
   [Quarantine Query] 画面が表示されます。
2. 期間を使用してクエリを実行するには、次の手順を実行します。
   - [Dates] フィールドからクエリの期間を選択します。期間は、[from:] の [MM/dd/yyyy] および時刻 [hh] と [mm]、および [to:] の [MM/dd/yyyy] および [hh] と [mm] で指定します。
3. [Violator] についてクエリを実行するには、次の手順を実行します。
   - [All] を選択してすべてのユーザを検索します。
   - または、[Specify user(s)] を選択し、ドロップダウンをクリックして特定の AD ユーザを検索対象として追加します。

4. [Site] についてクエリを実行するには、次の手順を実行します。
   - [All] を選択してすべてのサイトを検索します。
   - または、[Specify site(s)] を選択し、ドロップダウンをクリックして特定のサイトを検索対象として追加します。

注意

[Site] の初期設定は [All] です。ユーザは、特定のサイトをサイトツリーから選択できます。URL 検索では、指定した URL の位置が生成されます。すべての URL は、http または https から始まっている必要があります。

5. [File name] を使用してクエリを実行するには、次の手順を実行します。
   - [File name] フィールドにファイル名のすべてまたは一部を入力します。
6. 検索の種類 ([Type]) を使用してクエリを実行するには、次のいずれかを選択します。
   - Security risk scan (初期設定)
   - File blocking
   - Content filtering
   - Unscannable files
   - Data loss prevention
7. [Sort by] ドロップダウンから並べ替えオプションを選択し、[Ascending] または [Descending] を選択します。
8. [Display] フィールドで、1 ページ当たりに表示するログのエントリ数を入力します。初期設定は 15 です。
9. [Search] をクリックすると、クエリの結果が表示されます。

隔離ファイルの削除、復元、またはダウンロード

隔離のクエリを実行した後、必要に応じてそのファイルを削除、復元、またはダウンロードできます。ただし、システムを保護するため、ウイルスに感染したファイルはダウンロードできません。

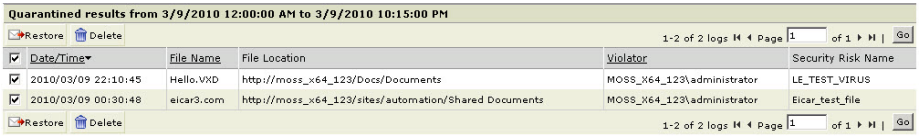


図 11-10. 隔離のクエリの結果画面

次に、隔離のクエリの結果画面で使用可能なオプションについて説明します。

- Restore — クリックすると、[File Location] 見出しの欄に表示されている場所にファイルが復元されます。
- Delete — クリックすると、選択したファイルが削除されます。
- Date/Time — ファイルが隔離された日時です。
- File Name — 隔離されたファイルの名前です。
- File Location — 隔離されたファイルの場所です。
- Violator — ファイルのアップロードを行ったユーザが表示されます。
- Security Risk Name (セキュリティリスク検索の場合のみ) — ファイルに含まれるウイルス/不正プログラム/スパイウェア/グレーウェアの名前が表示されます。
- Policy Name (ファイルブロック、コンテンツフィルタ、および情報漏えい対策の場合のみ) — 隔離が実行される原因となったポリシー名が表示されます。
- Reason (検索不能ファイルの場合のみ) — ファイルを検索できなかった簡単な説明が表示されます。たとえば、「Over restriction (decompressed file count)」などです。

隔離ファイルの削除、復元、またはダウンロード

手順

1. 250 ページの「隔離のクエリ」の説明に従って、隔離クエリを実行します。
2. [Quarantined results] 画面で、削除または復元するファイルを選択して、次のいずれかをクリックします。
   - [Delete] をクリックすると、選択したファイルが削除されます。
   - [Restore] をクリックすると、選択したファイルが元の場所に復元されます。

注意

コンテンツフィルタ、ファイルブロック、情報漏えい対策、および検索不能ファイルの場合は、[File Name] リンクをクリックすると、ファイルのダウンロードが開始されます。ファイルを開くか、選択した場所に保存するオプションを使用できます。

ヒント

列の見出しをクリックすると、見出しのラベル ([Date/Time]、[File Name] など) に従って、隔離の結果が並べ替えられます。

隔離の削除設定

[Quarantine Maintenance] では、選択した期間に従って隔離ファイルを削除する、手動または自動の設定ができます。

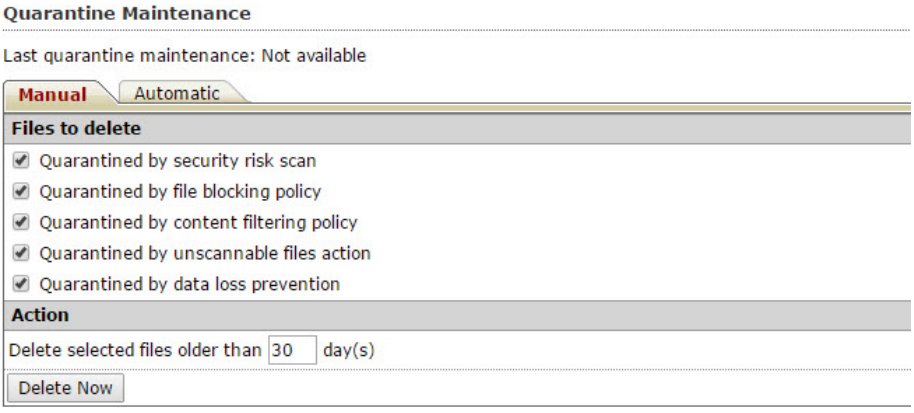


図 11-11. [Quarantine Maintenance] 画面の [Manual] タブ

警告!

隔離の削除設定を定期的に実行し、ファイルの復元や削除を行うことで、重要文書の紛失を防いだり、空きディスク容量の増加を図ったりしてください。

ヒント

ファーム環境内では、1 つの PortalProtect サーバのみで隔離の自動削除設定を有効にし、同じファーム内の他のすべての Web フロントエンドサーバでは無効にしてください。

隔離ファイルの手動削除

手順

1. [Quarantine] > [Maintenance] > [Manual] タブをクリックします。
   [Quarantine Maintenance] 画面の [Manual] タブが表示されます。

2. [Files to delete] の下で、次のオプションを選択します。
    - Quarantined by security risk scan
    - Quarantined by file blocking policy
    - Quarantined by content filtering policy
    - Quarantined by unscannable files action
    - Quarantined by data loss prevention
3. [Action] グループの [Delete selected files older than [xx] days] フィールドに値を入力します。
4. [Delete Now] をクリックします。

隔離ファイルの自動削除

手順

1. [Quarantine] > [Maintenance] > [Automatic] タブをクリックします。
   [Quarantine Maintenance] 画面の [Automatic] タブが表示されます。
2. [Enable automatic maintenance] をオンにしてこの機能を有効にします。
3. [Files to delete] の下で、次のオプションを選択します。
    - Quarantined by security risk scan
    - Quarantined by file blocking policy
    - Quarantined by content filtering policy
    - Quarantined by unscannable files action
    - Quarantined by data loss prevention
4. [Action] グループの [Delete selected files older than [xx] days] フィールドに値を入力します。
5. [Save] をクリックします。

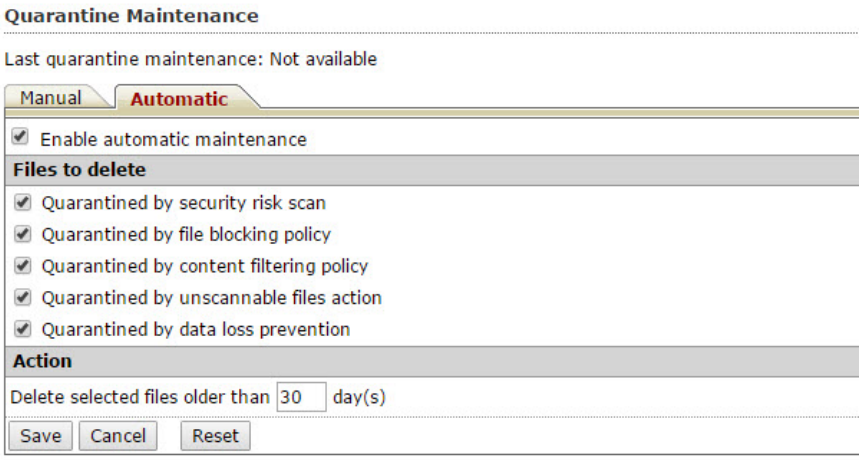


図 11-12. [Quarantine Maintenance] の [Automatic] タブ

レポートの表示および作成

PortalProtect では、1 回限りのレポートまたは予約レポートを作成できます。これらのレポートは、ログイベントのデータを使用して作成されます。管理コンソールから以前に作成したレポートを表示できます。

1 回限りのレポートの作成

手順

1. 左側のメニューで [Reports] > [One-time Reports] をクリックします。[One-time Reports] 画面が表示されます。
2. [One-time Reports] 画面から [Generate report] をクリックします。[One-time Reports: Add/Edit a report] 画面が表示されます。
3. [Report name] フィールドにレポートの名前を入力します。
4. [From] と [To] フィールドで、レポートのデータを収集する期間を選択します。
5. [Content] グループで、レポートに表示する項目を次のオプションから選択します。

- Scan status summary — 検索ステータスの概要を表示します。
- Security risk scan report — セキュリティリスク検索レポートを有効にする場合はこれを選択して、次のオプションを選択します。
  - Security risk scan summary
  - Viruses/malware graph — グラフのデータを、時間、日、週、月のいずれの単位で表示するかをドロップダウンから選択します。
  - Top viruses/malware — レポートで上位何個のウイルス/不正プログラムを表示するかを入力します。
  - Top viruses/malware violators — レポートで上位何人のウイルス/不正プログラムの違反ユーザを表示するかを入力します。
  - Virus/malware action summary — レポートに表示されるすべてのウイルスおよび不正プログラムに対して実行された処理の概要を表示する場合は、これを選択します。
  - Security risk types — レポートでセキュリティリスクタイプを表示する場合は、これを選択します。
  - Spyware/grayware graph — グラフのデータを、時間、日、週、月のいずれの単位で表示するかをドロップダウンから選択します。
  - Top spyware/grayware — スパイウェア/グレーウェアを表示する場合は、これを選択します。
  - Top spyware/grayware violators — スパイウェア/グレーウェアの違反ユーザを表示する場合は、これを選択します。
  - Virus/grayware action summary — レポートに表示されるすべてのウイルスおよびグレーウェアに対して実行された処理の概要を表示する場合は、これを選択します。
- File blocking report — ファイルブロックレポートを有効にする場合はこれを選択して、次のオプションを選択します。
  - File blocking summary — レポートにファイルブロックの概要を表示する場合は、これを選択します。

- Blocked files graph — グラフのデータを、時間、日、週、月のいずれの単位で表示するかをドロップダウンから選択します。
- Top file types blocked — レポートで上位何個のブロックされたファイルの種類を表示するかを入力します。
- Top file names blocked — レポートで上位何個のブロックされたファイル名を表示するかを入力します。
- Top file extensions blocked — レポートで上位何個のブロックされたファイル拡張子を表示するかを入力します。
- Top blocked file violators — レポートで上位何人のブロックされたファイルの違反ユーザを表示するかを入力します。
- Top file blocking policy triggered — レポートで上位何個の、ブロックを実行したファイルポリシーを表示するかを入力します。

- Content filtering report — コンテンツフィルタレポートを 有効にする場合はこれを選択して、次のオプションを選択します。
  - Content filtering summary — レポートにコンテンツフィルタの概要を表示する場合は、これを選択します。
  - Filtered files and Web content graph — グラフのデータを、時間、日、週、月のいずれの単位で表示するかをドロップダウンから選択します。
  - Top filtered files/Web content violators — レポートで上位何人の違反ユーザを表示するかを入力します。
  - Top content filtering policy triggered — レポートで上位何個のポリシーを表示するかを入力します。
- Data loss prevention report — 情報漏えい対策レポートを有効にする場合はこれを選択して、次のオプションを選択します。
  - Data loss prevention summary — レポートに情報漏えい対策の概要を表示する場合は、これを選択します。
  - Filtered files and Web content graph — グラフのデータを、時間、日、週、月のいずれの単位で表示するかをドロップダウンから選択します。

- Top filtered files/Web content violators — レポートで上位何人の違反ユーザを表示するかを入力します。
- Top data loss prevention policy triggered — レポートで上位何個の情報漏えい対策ポリシーを表示するかを入力します。
- Top data loss prevention template triggered — レポートで上位何個の情報漏えい対策テンプレートを表示するかを入力します。

- Unscannable file report — 検出不能ファイルレポートを有効にする場合はこれを選択して、次のオプションを選択します。
  - Unscannable file summary — レポートに検出不能ファイルの概要を表示する場合は、これを選択します。
  - Unscannable file graph — グラフのデータを、時間、日、週、月のいずれの単位で表示するかをドロップダウンから選択します。
- Web reputation report — Web レピュテーションレポートを有効にする場合はこれを選択して、次のオプションを選択します。
  - Web reputation summary — レポートに Web レピュテーションの概要を表示する場合は、これを選択します。
  - Suspicious URLs graph — グラフのデータを、時間、日、週、月のいずれの単位で表示するかをドロップダウンから選択します。
  - Top malicious URLs — レポートで上位何個の不正な URL を表示するかを入力します。
  - Top authors of Web content containing suspicious URLs — レポートで上位何人の、このオプションに対応する作成者を表示するかを入力します。

6. [Generate] をクリックします。

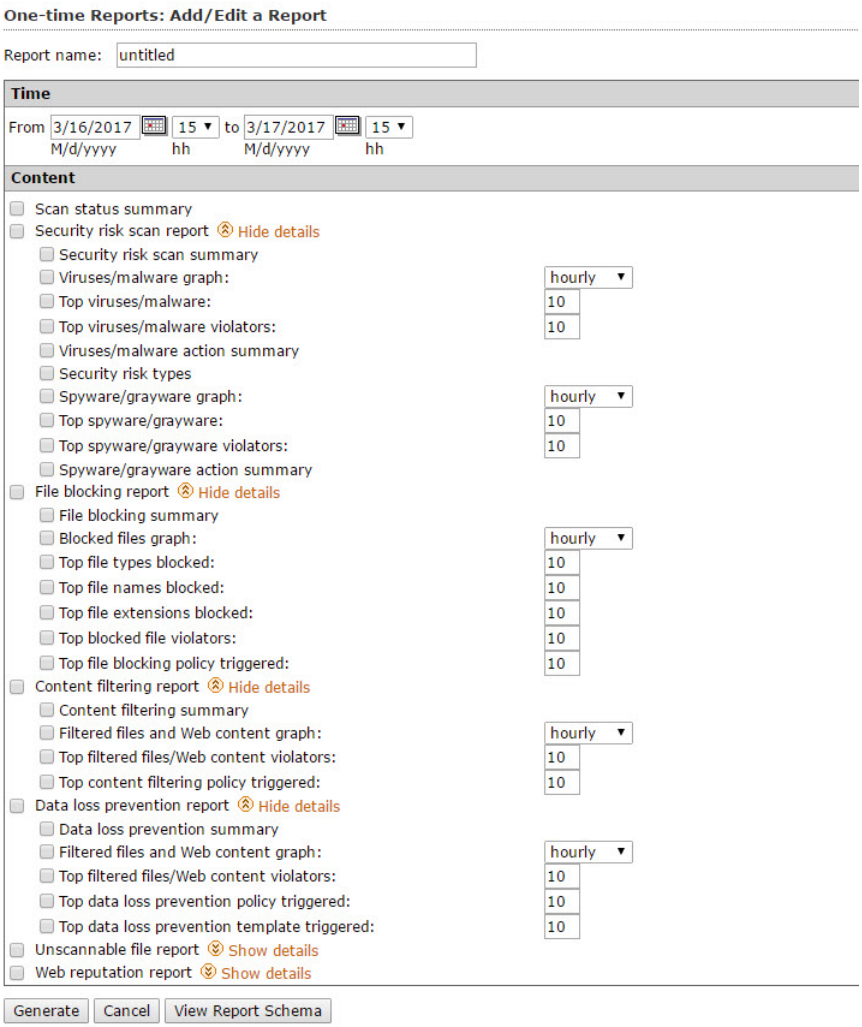


図 11-13. [One-time Reports: Add/Edit a report] 画面

予約レポートの作成

手順

1. 左側のメニューで [Reports] > [Scheduled Reports] をクリックします。[Scheduled Reports] 画面が表示されます。
2. [Scheduled Reports screen] 画面から [Add] をクリックします。[Scheduled Reports: Add Report] 画面が表示されます。
3. [Report name] フィールドに予約レポートの名前を入力します。
4. [Schedule] グループで、次のオプションを選択します。
   - Daily — 毎日レポートを作成する場合はこれを選択します。
   - Weekly, every — 選択された曜日に週次レポートを作成する場合はこれを選択します。
   - Monthly, every — 月の初日、15 日、または最後の日に月次レポートを作成する場合はこれを選択します。
5. [Generate report at] フィールドの [hh] と [mm] からレポートを生成する時刻を選択します。
6. [Content] グループで、次のオプションを選択します。
   - Scanning status summary — 検索ステータスの概要を表示します。
   - Security risk scan report — セキュリティリスク検索レポートを有効にする場合はこれを選択して、次のオプションを選択します。
     - Security risk scan summary
     - Security risk types — レポートでセキュリティリスクタイプを表示する場合は、これを選択します。
     - Viruses/malware graph — グラフのデータを、時間、日、週、月のいずれの単位で表示するかをドロップダウンから選択します。
     - Top viruses/malware — レポートで上位何個のウイルス/不正プログラムを表示するかを入力します。

- Top viruses/malware violators — レポートで上位何人のウイルス/不正プログラムの違反ユーザを表示するかを入力します。
- Viruses/malware action summary — レポートに表示されるすべてのウイルスおよび不正プログラムに対して実行された処理の概要を表示する場合は、これを選択します。
- Spyware/grayware graph — グラフのデータを、時間、日、週、月のいずれの単位で表示するかをドロップダウンから選択します。
- Top spyware/grayware — スパイウェア/グレーウェアを表示する場合は、これを選択します。
- Top spyware/grayware violators — スパイウェア/グレーウェアの違反ユーザを表示する場合は、これを選択します。
- Virus/grayware action summary — レポートに表示されるすべてのウイルスおよびグレーウェアに対して実行された処理の概要を表示する場合は、これを選択します。

- File blocking report — ファイルブロックレポートを有効にする場合はこれを選択して、次のオプションを選択します。
  - File blocking summary — レポートにファイルブロックの概要を表示する場合は、これを選択します。
  - Blocked files graph — グラフのデータを、時間、日、週、月のいずれの単位で表示するかをドロップダウンから選択します。
  - Top file types blocked — レポートで上位何個のブロックされたファイルの種類を表示するかを入力します。
  - Top file names blocked — レポートで上位何個のブロックされたファイル名を表示するかを入力します。
  - Top file extensions blocked — レポートで上位何個のブロックされたファイル拡張子を表示するかを入力します。
  - Top blocked file violators — レポートで上位何人のブロックされたファイルの違反ユーザを表示するかを入力します。

- Top file blocking policy triggered — レポートで上位何個の、ブロックを実行したファイルポリシーを表示するかを入力します。

- Content filtering report — コンテンツフィルタレポートを 有効にする場合はこれを選択して、次のオプションを選択します。
  - Content filtering summary — レポートにコンテンツフィルタの概要を表示する場合は、これを選択します。
  - Filtered files and Web content graph — グラフのデータを、時間、日、週、月のいずれの単位で表示するかをドロップダウンから選択します。
  - Top filtered files/Web content violators — レポートで上位何人の違反ユーザを表示するかを入力します。
  - Top content filtering policy triggered — レポートで上位何個のポリシーを表示するかを入力します。
- Data loss prevention report — データ保護レポートを有効にする場合はこれを選択して、次のオプションを選択します。
  - Data loss prevention summary — レポートにデータ保護の概要を表示する場合は、これを選択します。
  - Filtered files and Web content graph — グラフのデータを、時間、日、週、月のいずれの単位で表示するかをドロップダウンから選択します。
  - Top filtered files/Web content violators — レポートで上位何人の違反ユーザを表示するかを入力します。
  - Top data loss prevention policy triggered — レポートで上位何個のポリシーを表示するかを入力します。
  - Top data loss prevention template triggered — レポートで上位何個のテンプレートを表示するかを入力します。
- Unscannable file report — 検出不能ファイルレポートを有効にする場合はこれを選択して、次のオプションを選択します。
  - Unscannable file summary — レポートに検出不能ファイルの概要を表示する場合は、これを選択します。

- Unscannable file graph — グラフのデータを、時間、日、週、月のいずれの単位で表示するかをドロップダウンから選択します。

- Web reputation report — Web レピュテーションレポートを有効にする場合はこれを選択して、次のオプションを選択します。
  - Web reputation summary — レポートに Web レピュテーションの概要を表示する場合は、これを選択します。
  - Suspicious URLs graph — グラフのデータを、時間、日、週、月のいずれの単位で表示するかをドロップダウンから選択します。
  - Top malicious URLs — レポートで上位何個の不正な URL を表示するかを入力します。
  - Top authors of Web content containing suspicious URLs — レポートで上位何人の、このオプションに対応する作成者を表示するかを入力します。

7. [Delivery] グループで、レポートの配信先メールアドレスを入力します。複数のメールアドレスがある場合はセミコロンを使用して区切ります。
8. [Save] をクリックします。

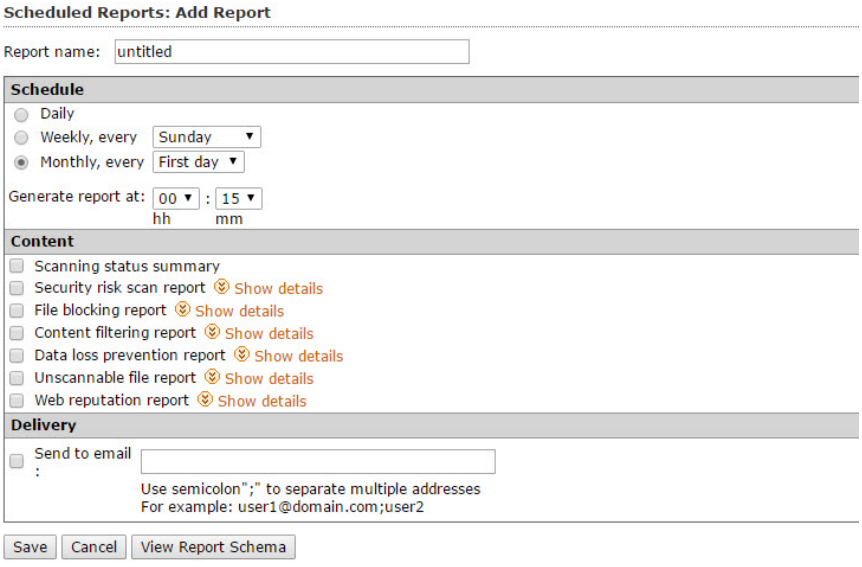


図 11-14. [Scheduled Reports: Add Report] 画面

ヒント

カスタマイズレポートを作成するには、[View Log Schema] をクリックして PortalProtect ログスキーマのコピーを取得します。

レポートの削除設定

[Report Maintenance] では、次のそれぞれの項目について、保存するレポートの最大数を設定できます。

- One-time reports — PortalProtect で保存できる 1 回限りのレポートの最大数を指定します。設定した値を超えた 1 回限りのレポートは、古いものから削除されます。
- Scheduled reports saved in each template — PortalProtect で保存できる予約レポートの最大数を指定します。設定した値を超えた予約レポートは、古いものから削除されます。

- Report templates — PortalProtect で保存できるレポートテンプレートの最大数を指定します。設定した値を超えたレポートテンプレートは、古いものから削除されます。

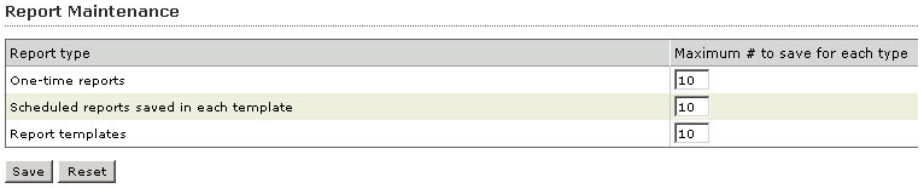


図 11-15. [Report Maintenance] 画面

第 12 章

テクニカルサポート

ここでは、次の項目について説明します。

トラブルシューティングのリソース

トレンドマイクロでは以下のオンラインリソースを提供しています。テクニカルサポートに問い合わせる前に、こちらのサイトも参考にしてください。

サポートポータルの利用

サポートポータルでは、よく寄せられるお問い合わせや、障害発生時の参考となる情報、リリース後に更新された製品情報などを提供しています。

https://success.trendmicro.com/dcx/s/?language=ja

脅威データベース

現在、不正プログラムの多くは、コンピュータのセキュリティプロトコルを回避するために、2 つ以上の技術を組み合わせた複合型脅威で構成されています。トレンドマイクロは、カスタマイズされた防御戦略を策定した製品で、この複雑な不正プログラムに対抗します。脅威データベースは、既知の不正プログラム、スパム、悪意のある URL、および既知の脆弱性など、さまざまな混合型脅威の名前や兆候を包括的に提供します。

詳細については、https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/ をご覧ください。

- 現在アクティブまたは「in the Wild」と呼ばれている生きた不正プログラムと悪意のあるモバイルコード
- これまでの Web 攻撃の記録を記載した、相関性のある脅威の情報ページ
- 対象となる攻撃やセキュリティの脅威に関するオンライン勧告
- Web 攻撃およびオンラインのトレンド情報
- 不正プログラムの週次レポート

製品サポート情報

製品のユーザ登録により、さまざまなサポートサービスを受けることができます。

トレンドマイクロの Web サイトでは、ネットワークを脅かすウイルスやセキュリティに関する最新の情報を公開しています。ウイルスが検出された場合や、最新のウイルス情報を知りたい場合などにご利用ください。

サポートサービスについて

サポートサービス内容の詳細については、製品パッケージに同梱されている「製品サポートガイド」または「スタンダードサポートサービスメニュー」をご覧ください。

サポートサービス内容は、予告なく変更される場合があります。また、製品に関するお問い合わせについては、サポートセンターまでご相談ください。トレンドマイクロのサポートセンターへの連絡には、電話またはお問い合わせ Web フォームをご利用ください。サポートセンターの連絡先は、「製品サポートガイド」または「スタンダードサポートサービスメニュー」に記載されています。

サポート契約の有効期限は、ユーザ登録完了から 1 年間です (ライセンス形態によって異なる場合があります)。契約を更新しないと、パターンファイルや検索エンジンの更新などのサポートサービスが受けられなくなりますので、サポートサービス継続を希望される場合は契約満了前に必ず更新してください。更新手続きの詳細は、トレンドマイクロの営業部、または販売代理店までお問い合わせください。

注意

サポートセンターへの問い合わせ時に発生する通信料金は、お客さまの負担とさせていただきます。

トレンドマイクロへのウイルス解析依頼

ウイルス感染の疑いのあるファイルがあるのに、最新の検索エンジンおよびパターンファイルを使用してもウイルスを検出/駆除できない場合などに、感染の疑いのあるファイルをトレンドマイクロのサポートセンターへ送信していただくことができます。

ファイルを送信いただく前に、トレンドマイクロの不正プログラム情報検索サイト「脅威データベース」にアクセスして、ウイルスを特定できる情報がないかどうか確認してください。

https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/

ファイルを送信いただく場合は、次の URL にアクセスして、サポートセンターの受付フォームからファイルを送信してください。

https://success.trendmicro.com/dcx/s/threat?language=ja

感染ファイルを送信する際には、感染症状について簡単に説明したメッセージを同時に送ってください。送信されたファイルがどのようなウイルスに感染しているかを、トレンドマイクロのウイルスエンジニアチームが解析し、回答をお送りします。

感染ファイルのウイルスを駆除するサービスではありません。ウイルスが検出された場合は、ご購入いただいた製品にてウイルス駆除を実行してください。

メールレピュテーションについて

スパムメールやフィッシングメールなどの 送信元を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

ファイルレピュテーションについて

不正プログラムなどのファイル情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

Web レピュテーションについて

不正な Web サイトや URL などの情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

その他のリソース

製品やサービスについてのその他の情報として、次のようなものがあります。

最新版ダウンロード

製品やドキュメントの最新版は、次の Web ページからダウンロードできます。

https://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

注意

サービス製品、販売代理店経由での販売製品、または異なる提供形態をとる製品など、一部対象外の製品があります。

付録 A

トラブルシューティング

ここでは、PortalProtect の機能に関してよくある質問とその回答について紹介します。

本章では、以下についてのよくある質問とその回答を示しています。

検索

Web コンテンツのコンテンツフィルタや Web レピュテーションが機能しません。原因は何でしょうか。

次の点を確認してください。

1. PortalProtect の Web 管理コンソールにログオンします。
2. [Summary] 画面で、[Scan Web content] が有効になっているかどうかを確認します。[Status] 列のアイコンをクリックして、有効または無効にします。このオプションは、ファーム内のすべての SharePoint サーバに対するグローバルなオン/オフのスイッチです。
3. Web コンテンツ検索が有効なときに、新しい SharePoint リストを作成する場合は、まず [Summary] 画面の [Scan Web content] を無効にしてから、再度有効にする必要があります。これを行わない場合は、新しく作成した SharePoint リストに対する Web コンテンツ検索は 12 時間後に有効になります。
4. [Content Filtering] または [Web Reputation] 画面で、検索オプションが有効になっていることを確認してください。[Content Filtering] では、少なくとも 1 つのルールを有効にする必要があります。

注意

Web コンテンツの作成者がシステムアカウントの場合、ファイルと Web コンテンツの検索は省略されます。

PortalProtect で、「file "x.xxx" contains the following virus: "It has been blocked; final action is:[Block]."」というメッセージが出力されます。しかし、このファイルにはウイルスは含まれていません。なぜ、このファイルにウイルスが含まれているというメッセージが出力されるのですか。

Microsoft SharePoint Server がこのメッセージの形式を提供し、トレンドマイクロが引用符内の内容を修正しています。そのため、PortalProtect のファイルブロックまたはコンテンツフィルタでファイルがブロックされると 、ファイルがウイルスに感染していなくても「contains the following virus」と表示

されてしまいます。メッセージをより正確に理解するには、「contains the following virus」の部分を無視して、引用符内の内容にのみ注目してください。

ファイルブロックを有効にしていませんが、一部のファイルはアップロードもダウンロードもされません。原因は何でしょうか。

SharePoint Server のブロックリスト設定を確認してください。SharePoint Server は、指定された接尾辞を持つファイルをブロックします。SharePoint Server　Central Management Page を使用して、この設定を変更します。

SharePoint Server からファイルブロック設定を削除するには

1. [セキュリティの構成] を選択します。
2. [一般的なセキュリティ] の設定で [ブロックするファイルの種類の定義] を選択します。
3. 拡張子名がダイアログボックスにリストされます。ここに含まれるすべての拡張子名が、アップロード時またはダウンロード時に SharePoint Server でブロックされます。

PortalProtect では、圧縮ファイル内に存在するファイルをブロックできません。圧縮ファイル内に感染ファイルが存在する場合、PortalProtect はどのようにそれを検出するのですか。

ブロック処理では、PortalProtect は圧縮ファイルを単一のファイルとして処理します。検索/隔離/駆除処理では、PortalProtect は圧縮ファイルに含まれるファイルを 1 つずつ処理します。したがって、感染ファイルは PortalProtect で処理されないわけではありません。

PortalProtect では、`.zip` および `.lzh` 圧縮ファイルの検索方法が他の圧縮ファイルの検索方法と異なるのですか。

PortalProtect では、Virus Scanning Application Program Interface (VSAPI) を使用して圧縮ファイルを処理します。VSAPI は、圧縮ファイルを拡張子で区別するのではなく、実際のファイルタイプで区別しています。つまり、VSAPI では、`.zip` ファイルの名前が `.txt` に変更されていてもそれを判別できます。VSAPI は、`.zip` ファイルと `.lzh` ファイルを同様に検索します。

検索には一次処理と二次処理を設定できますが、二次処理は一次処理が失敗した場合にのみ実行されるのでしょうか。それとも両方の処理が実行されるのでしょうか。

二次処理は一次処理が失敗した場合にのみ実行されます。二次処理は、一次処理が駆除の場合のみ選択できます。

PortalProtect でファイルをブロックしたときに作成されるレコードはありますか。

はい。PortalProtect でファイルをブロックすると通知が送信されます (通知が有効な場合)。PortalProtect では、検索時にファイルをブロックするとログが作成されます。

どのようなファイルが検出不能ファイルと見なされるのですか。

検索不能ファイルは、VSAPI で検索できないファイルです。たとえば、暗号化ファイルやパスワード保護ファイルです。

PortalProtect は暗号化ファイルを検索できますか。

いいえ。暗号化ファイルは検索設定で指定する個別の脅威になります。ユーザは暗号化ファイルに対する処理をカスタマイズできます。

PortalProtect サーバでウイルスを検索できるのですが、エンジンとパターンファイルをアップデートできません。原因は何でしょうか。

アクティベーションコードの 有効期限が切れている可能性があります。販売代理店に問い合わせてサポート契約を更新してください。

情報漏えい対策のパターンの発生とは、どういう意味でしょうか。

情報漏えい対策のパターンの発生とは、ドキュメントまたは Web コンテンツの何らかが情報漏えい対策のパターンに一致したことを表します。たとえば、情報漏えい対策ポリシーにパターンが含まれ、発生回数が「3」に設定されているとします。この場合、パターンの発生回数が「3」未満であれば、

SharePoint サイトに投稿されたドキュメントおよび Web コンテンツによって対応する情報漏えい対策ポリシーが実行されることはありません。

PortalProtect にドキュメントまたは Web コンテンツ用の情報漏えい対策機能がないのはなぜでしょうか。

PortalProtect のアクティベーションコード (AC) を確認してください。データ保護機能を使用するには専用の AC が必要ですので、お買い上げの販売店にお問い合わせください。AC を PortalProtect の Web 管理コンソールで変更した場合は、ログオフし、再度ログオンして情報漏えい対策関連の機能を確認してください。

コンテンツフィルタ、情報漏えい対策、および Web レピュテーションによって実行されるファイルタイプ検索は、どのようにすればその一部をスキップできますか。

PortalProtect では、この機能を実装するために次のレジストリキーが提供されています。

- 名前: FileTypeBypassMask
- 種類: string

説明: この隠しキーは、コンテンツフィルタ、情報漏えい対策、および Web レピュテーションのファイル検索で特定のファイルタイプを除外するために使用できます。「docx;pptx」に設定されている場合、コンテンツフィルタ、情報漏えい対策、および Web レピュテーションのファイル検索で `.docx` および `.pptx` ファイルがスキップされます。

注意

この隠しキーの変更は、サービスを再起動したときに適用されます。

コンテンツフィルタ、情報漏えい対策、およびドキュメント内の URL におけるファイル検索サイズは、どのようにすればカスタマイズできますか。

PortalProtect では、この機能を実装するために次のレジストリキーが提供されています。

- 名前: FileSizeThreshold
- 種類: REG_DWORD

説明: 情報漏えい対策、コンテンツフィルタ、および Web レピュテーションのファイル検索サイズのしきい値です。この隠しキーでは、ファイル検索のしきい値をメガバイト単位で指定します。初期設定値は 1000MB です。キーにゼロが設定されている場合、無制限を意味します。

注意

この隠しキーの変更は、サービスを再起動したときに適用されます。

アップデート

アップデートサーバからのアップデートが成功しなかった原因は何でしょうか。

システムでインターネット 接続にプロキシサーバが必要な場合は、設定が正しいかどうか確認してください。

PortalProtect でイントラネットソースを使用してアップデートを受信する場合、共有場所はどのようにアップデートされるのですか。

アップデートでは、イントラネットコンピュータからの最新コンポーネントのダウンロードをサポートします。そのコンピュータにアップデートパッケージを配置して、イントラネットの他のコンピュータがダウンロードするフォルダの共有を有効にします。

コンポーネントパッケージはどのようにアップデートされるのですか。

ダウンロードに成功したら、パッケージを抽出して、PortalProtect に新しいモジュールをロードするように通知します。

別の PortalProtect サーバのコンポーネントパッケージソースを使用してエンジンまたはパターンファイルをアップデートするにはどうしたらよいでしょうか。

[Updates] > [Download Source] の順に選択し、[Other Update Source] を選択して、次の URL を入力します。

https://<サーバ名><:ポート番号>/PortalProtect/activeupdate

ここで、

- サーバ名 は、コンポーネントパッケージソースのあるサーバのホスト 名または IP アドレスです。
- ポート番号 は、PortalProtect Web コンソールのポート番号です。

一般的な問題

警告の問題

「PortalProtect service did not start successfully」と「PortalProtect service is unavailable?」の警告の違いは何ですか。

- PortalProtect service did not start successfully: PortalProtect for Microsoft SharePoint Master Service の起動に失敗すると発生します。
- PortalProtect service is unavailable: PortalProtect_Master サービスがすでに起動しており、突然停止した場合に発生します。

SNMP トラップは受信できるのにメール警告を受信できないのはなぜでしょうか。

PortalProtect では、メール警告を SMTP サーバに送信します。他の警告の種類を受信できてメール警告だけが受信できない場合は、SMTP サーバを調べてポート番号が正しく設定されているか確認してください。また、警告の受信に複数のメールアドレスを設定している場合、それらの区切りにセミコロンが使用されているか確認してください。

通知の問題

ファイルブロックのルールが実行されるようなファイルをアップロードしましたが、メール通知を受信しません。原因は何でしょうか。

ファイルブロックのメール通知は、初期設定で、2 時間ごとにまとめて送信するように設定されています。つまり PortalProtect は、ブロックしたすべてのファイルに関するメール通知を 2 時間ごとに 1 回送信します。この設定は要件に応じて変更できます。

その他の問題

リモートサーバからサーバ管理コンソールで情報をクエリできません。どうすればいいですか。

- 関連する PortalProtect サーバがすべて同じファーム内にあることを確認します。
- PortalProtect がインストールされ、Web フロントエンドサーバで起動されていることを確認します。
- PortalProtect_Master サービスが、ローカル管理者およびドメインユーザの権限を持つユーザによって開始されていることを確認します。
- リモート PortalProtect サーバのファイアウォールをチェックし、TCP に対してポート 139 と 445 が開かれていることを確認します。
- リモートサーバで次の Windows サービスが実行されていることを確認します。
  - リモートプロシージャコール (PRC)
  - サーバ
  - ワークステーション

設定をファーム内の他の PortalProtect サーバへ自動的に複製できません。原因は何でしょうか。

次の手順を実行してください。

- [Server Management] の [Automatically replicate settings to other servers] チェックボックスをオンにします。

- リモート PortalProtect サーバの情報がクエリ可能であることを確認します。
- 製品版 PortalProtect のサポート契約が有効期間中であることを確認します。
- PortalProtect サーバがすべて同じバージョンであることを確認します。
- PortalProtect サーバがすべて OPP (大規模感染予防ポリシー) 状態ではないことを確認します。

PortalProtect で Active Directory ユーザ/グループを検索できません。原因は何でしょうか。

- PortalProtect では、現在のフォレストの Active Directory ユーザ/グループのみが検索可能です。ユーザが現在のフォレスト内に存在するかどうかを確認してください。
- PortalProtect では、Active Directory ユーザ/グループの名前について検索文字列が前方のみから検索されます。

注意

「test」という文字列を検索する場合、「te」と文字を入力すると一致します。ただし、「es」という文字を検索で使用しても、「test」には一致しません。

ローカルサーバからは PortalProtect Web コンソールにアクセスできるのですが、リモートコンピュータからはアクセスできません。原因は何でしょうか。

次の点を確認してください。

- インストール時に指定した HTTPS ポート (初期設定は 16373) を介した PortalProtect Web コンソールへのアクセスをブロックするネットワークファイアウォールがあるか。
- PortalProtect サーバ上の Windows ファイアウォールで、インストール時に指定した HTTPS ポート (初期設定は 16373) をブロックしていないか。

他のトレンドマイクロ製品で検索から除外する必要のあるフォルダはどれでしょうか。

他のトレンドマイクロ製品では、次の 3 つのフォルダを検索から除外する必要があります。

- バックアップフォルダ
- temp フォルダ
- Sharedrespool フォルダ

バックアップフォルダの 場所は変更できます。初期設定の場所は次のとおりです。

- 初期設定のバックアップフォルダ

  ```
  (ドライブ文字):¥Program Files¥Trend Micro¥PortalProtect
  ¥storage¥backup
  ```

- temp フォルダ

  ```
  (ドライブ文字):¥Program Files¥Trend Micro¥PortalProtect¥Temp
  ```

- Sharedrespool フォルダ

  ```
  (ドライブ文字):¥Program Files¥Trend Micro¥PortalProtect
  ¥SharedResPool
  ```

PortalProtect ではどのようにファイルを読み込んで、それに拡張子があることを認識するのですか。

ユーザが SharePoint Server にファイルをアップロードすると、SharePoint Server は PortalProtect を呼び出して、ファイルにウイルスが含まれているかどうかを検出します。PortalProtect は SharePoint Services からファイル名と拡張子を取得します。

PortalProtect で拡張子を読み取った後、一致しているものがあるかどうかをどのように判断するのですか。拡張子を比較するための、すべてのユーザ設定を含むデータベースがあるのですか。

すべてのユーザ設定はデータベースに保存されます。PortalProtect はファイル拡張子を比較して、一致があるかどうかを確認します。

Windows イベントログに「Unable to connect to the PortalProtect database.Check your network settings and make sure the network connection between PortalProtect and the database server is available.」が表示されるのはなぜですか?

PortalProtect は、データベース接続を監視し、接続不能になると PortalProtect サービスを停止します。この問題が発生すると、PortalProtect によって Windows イベントログにエントリが作成されます。PortalProtect は、データベース接続の監視を継続し、接続が回復すると、データベース接続が回復したことを示す別のエントリを Windows イベントログに作成します。

PortalProtect のシングルサインオンでは、Windows Server 2003 の Web コンソールにログオンできませんでした。原因は何でしょうか。

リモートサーバへの接続に `mstsc` を使用している場合は、次の操作を試してください。

- 接続モードを `mstsc/admin` に変更して再接続する
- または、URL を localhost から hostname に変更するか、127.0.0.1 を使用する

Smart Protection Server のクエリ順序は、[As listed] と [Random] で何が違いますか。

クエリ順序は、Smart Protection Server リストのみに使用可能です。クエリ順序が [As listed] の場合、最初の使用可能な Smart Protection Server が使用されます。クエリ順序が [Random] の場合、使用可能な Smart Protection Server の中からランダムに選択されます。

PortalProtect では IPv6 がどのようにサポートされるのですか。

PortalProtect では、次の場合に IPv6 がサポートされます。

- インストールの対象サーバの指定
- PortalProtect の Web 管理コンソールへのアクセス
- Trend Micro Control Manager への PortalProtect の登録
- ダウンロード元の IP アドレスの指定
- SNMP 通知の IP アドレスの設定

- Web レピュテーションレーティングのクエリ

付録 B

Trend Micro Control Manager からの管理

Trend Micro Control Manager (以下、Control Manager) は、トレンドマイクロのウイルス対策製品やサービスを緊密に連携されたウイルスセキュリティ / コンテンツ管理ソリューションに統合する集中管理システムです。

本章の内容は次のとおりです。

Control Manager の概要

Control Manager は、ゲートウェイ、メールサーバ、ファイルサーバ、および企業のデスクトップの各レベルでトレンドマイクロの製品やサービスを管理するための集中管理コンソールです。管理者は、ポリシー管理機能を使用して製品設定を行い、これを管理下の製品やエンドポイントに導入できます。Control Manager の Web ベースの管理コンソールにより、ネットワーク全体のウイルス対策およびコンテンツセキュリティ製品やサービスを単一の場所から監視することができます。

システム管理者は、Control Manager を使用することで、感染、セキュリティ違反、ウイルス/不正プログラムの侵入といった活動を監視してレポートを作成することが可能です。アップデートコンポーネントをダウンロードしてネットワーク全体に配信することで、一貫した最新の保護が適用されます。アップデートコンポーネントには、ウイルスパターンファイル、検索エンジン、スパムメール判定ルールなどが含まれます。Control Manager では、手動アップデートと予約アップデートの両方が可能です。柔軟性向上のため、製品の設定および管理はグループでも個人でも行うことができます。

Control Manager の設定

[Control Manager Settings] 画面では、PortalProtect MCP エージェントと Control Manager サーバ間の通信を設定できます。

手順

1. [Administration] > [Control Manager Settings] の順にクリックし、要件に従って次のオプションを設定します。
   - 画面上部
     - Enable communication between the PortalProtectMCP agent and Control Manager — PortalProtect MCP エージェントと Control Manager 間の通信を有効にします。
   - Connection Status
     - Registered Control Manager server — Control Manager サーバが接続されているかどうかを示します。
   - Connection Settings

- Entity display name — Control Manager の製品ツリーに表示されるエンティティ 名を示します。

- Control Manager Server Settings
  - Server FQDN or IP address — サーバの完全修飾ドメイン名または IP アドレスを入力します。
  - Port — ポート番号を入力し、HTTPS を使用するかどうかを選択します。
  - Web server authentication — IIS サーバで使用するユーザ名とパスワードを [Username] および [Password] に入力します。

注意

Control Manager では、Web サーバ認証に指定した情報は使用されません。

- MCP Proxy Settings
  - Use a proxy server for communication with the Control Manager server — Control Manager サーバとの通信にプロキシサーバを使用する場合に選択します。
  - Proxy protocol — HTTP または SOCKS 5 のいずれかを選択します。
  - Server FQDN or IP address — サーバの完全修飾ドメイン名または IP アドレスを入力します。
  - Port — MCP プロキシで使用するポート番号を入力します。
  - Proxy server authentication — 必要に応じてユーザ ID とパスワードを [User ID] と [Password] に入力します。

- Two Way Communication Port Forwarding
  - Enable two-way communication port forwarding — 管理下の製品と Control Manager 間のリアルタイム接続を有効にする場合に選択します。
  - IP address — ポートフォワーディングで 使用する IP アドレスを入力します。

- Port — ポートフォワーディングで 使用するポート番号を入力します。

注意

現在の接続設定をテストするには [Test Connection] をクリックし、現在の設定を登録するには [Register] をクリックします。変更を保存せずに終了するには [Cancel] をクリックします。

付録 C

正規表現について

正規表現は、文字列の照合を実行するために使用します。

注意

正規表現は、強力な文字列照合ツールです。このため、正規表現の構文に精通し、慣れている管理者が、正規表現を使用することをお勧めします。正規表現の記述が不完全な場合、パフォーマンスに悪影響をもたらす可能性があります。トレンドマイクロでは、複雑な構文を使用しない、単純な正規表現から開始することをお勧めします。新しいルールを導入する際は、バックアップ処理を使用し、PortalProtect がどのようにルールを適用するか観察します。そのルールが予期せぬ結果を引き起こさないことを確認してから、処理を変更します。

一般的な正規表現のいくつかの例については、以下の表を参照してください。

出現回数とグループ化

表 C-1. 出現回数とグループ化

要素	意味	例
.	ドットまたはピリオドの記号は、改行文字以外の任意の文字を表します。	do.は、doe、dog、don、dos、dot などに一致します。d.r は、deer、door などに一致します。
*	アスタリスク記号は、直前の要素が 0 回以上連続することを意味します。	do*は、d、do、doo、dooo、doooo などに一致します。
+	プラス記号は、直前の要素が 1 回以上連続することを意味します。	do+は、do、doo、dooo、doooo などに一致しますが、d には一致しません。
?	疑問符は、直前の要素が 0 または 1 回連続することを意味します。	do?g は、dg または dog に一致しますが、doog、dooog などには一致しません。
( )	丸カッコは、その間にあるものが何であっても、1 つのものと見なしてグループ化します。	d(eer)+は、deer、deereer、deereereer などに一致します。+記号は丸カッコ内のサブ文字列に適用されるので、d の後に「eer」のグループが複数回続く文字列が検索されます。
[ ]	角カッコは、文字のセットまたは範囲を示します。	d[aeiouy]+は、da、de、di、do、du、dy、daa、dae、dai などに一致します。+記号は角カッコ内の集合に適用されるので、d の後に [aeioy] の集合の中の 1 つ以上の文字が続く文字列が検索されます。 d [A-Z] は、dA、dB、dC から dZ までの文字列に一致します。角カッコ内の集合は、A ～ Z の範囲のすべての大文字を表します。
^	角カッコ内のキャレット記号は、指定された集合または範囲を論理的に否定します。つまり、その集合または範囲にない任意の文字が一致します。	d[^aeiouy] は、d の後に母音以外の 1 文字が続く、db、dc、dd、d9、d# に一致します。

要素	意味	例
{ }	中カッコは、直前の要素が特定の回数繰り返されることを設定します。中カッコ内の値が 1 つだけの場合、その回数の繰り返しのみが一致します。2 つの数字がカンマで区切られている場合、直前の文字の繰り返しが有効な回数の集合を表します。1 つの 10 進数字の後にカンマが続く場合は、上限がないことを意味します。	da{3} は、d の後に 3 回だけ「a」が続く、daaa に一致します。da{2,4} は、d の後に 2、3、4 回「a」が続く daa、daaa、および daaaa に一致しますが、daaaaa には一致しません。da{4,} は、d の後に 4 回以上「a」が続く、daaaa、daaaaa、daaaaaa などに一致します。

文字クラス (短縮形)

表 C-2. 文字クラス (短縮形)

要素	意味	例
\d	任意の 10 進数文字。[0-9] または [[:digit:]] と機能的には同等です。	\d は、1 つ以上の任意の 10 進数文字で、1、12、123 などに一致しますが、1b7 には一致しません。
\D	10 進数字以外の任意の文字。[^0-9] または [^[:digit:]] と機能的には同等です。	\D は、0、1、2、3、4、5、6、7、8、9 以外の 1 つ以上の任意の文字で、a、ab、ab&に一致しますが、1 には一致しません。
\w	任意の「単語」となる文字、つまり、任意の英数字。[_A-Za-z0-9] または [_[:alnum:]] と機能的には同等です。	\w は、1 つ以上の大小の英字または 10 進数字で、句読点やその他の特殊文字は含まれません。\w は、a、ab、a1 に一致しますが、!&には一致しません。
\W	英数字以外の任意の文字。[^_A-Za-z0-9] または [^_[:alnum:]] と機能的には同等です。	\W は、1 つ以上の任意の文字で、大小の英字および 10 進数字は含まれません。\W は、*、&に一致しますが、ace または a1 には一致しません。

要素	意味	例
\s	任意の空白文字。スペース、改行、タブ、改行禁止スペースなどです。[[:space]] と機能的には同等です。	vegetable\s は、「vegetable」の後に空白文字が続く文字列に一致します。したがって、「I like a vegetable in my soup」という文は検索されますが、「I like vegetables in my soup」は検索されません。
\S	任意の空白以外の文字。スペース、改行、タブ、改行禁止スペースなど以外のすべての文字です。[^[:space]] と機能的には同等です。	vegetable\S は、「vegetable」の後に空白文字以外の任意の文字が続く文字列に一致します。したがって、「I like vegetables in my soup」という文は検索されますが、「I like a vegetable in my soup」は検索されません。

文字クラス

表 C-3. 文字クラス

要素	意味	例
[:alpha:]	任意のアルファベット文字。	正規表現 [[:alpha:]] は、abc、def、xxx に一致しますが、123 や@#$には一致しません。
[:digit:]	任意の 10 進数文字。\d と機能的には同等です。	正規表現 [[:digit:]] は、1、12、123 などに一致します。
[:alnum:]	任意の「単語」となる文字、つまり、任意の英数字。\w と機能的には同等です。	正規表現 [[:alnum:]] は、abc、123 に一致しますが、~!@には一致しません。
[:space:]	任意の空白文字。スペース、改行、タブ、改行禁止スペースなどです。\s と機能的には同等です。	正規表現(vegetable)[[:space:]] は、「vegetable」の後に任意の空白文字が続く文字列に一致します。したがって、「I like a vegetable in my soup」という文は検索されますが、「I like vegetables in my soup」は検索されません。

要素	意味	例
[:graph:]	空白、制御文字、または同様のものを除く任意の文字。	正規表現 [[:graph:]] は、123、abc、xxx、><"に一致しますが、空白または制御文字には一致しません。
[:print:]	任意の文字 ([:graph:] と似ています)。ただし、空白文字が含まれます。	正規表現 [[:print:]] は、123、abc、xxx、><"、および空白文字に一致します。
[:cntrl:]	任意の制御文字 (例: CTRL + C、CTRL + X)。	正規表現 [[:cntrl:]] は、0x03、0x08 に一致しますが、abc、123、!@#には一致しません。
[:blank:]	スペースおよびタブ文字。	正規表現 [[:blank:]] は、スペースおよびタブ文字に一致しますが、123、abc、!@#には一致しません。
[:punct:]	句読点文字。	正規表現[[:punct:]] は、; : ? ! ~ @ # $ % & * ' " に一致しますが、123、abc には一致しません。
[:lower:]	任意の小文字のアルファベット文字 (注意: [大文字/小文字を区別する] を有効にする必要があります。有効にしない場合、[:alnum:] と同様に機能します)。	正規表現 [[:lower:]] は、abc、Def、sTress、Do などに一致しますが、ABC、DEF、STRESS、DO、123、!@#には一致しません。
[:upper:]	任意の大文字のアルファベット文字 (注意: [大文字/小文字を区別する] を有効にする必要があります。有効にしない場合、[:alnum:] と同様に機能します)。	正規表現 [[:upper:]] は、ABC、DEF、STRESS、DO、Def、Stress、Do などに一致しますが、abc、123、!@#には一致しません。
[:xdigit:]	16 進数で使用できる数字 (0-9a-fA-F)。	正規表現 [[:xdigit:]] は、0a、7E、0f などに一致します。

パターンアンカー正規表現

表 C-4. パターンアンカー正規表現

要素	意味	例
^	文字列の始まりを示します。	^ (notwithstanding) は、「notwithstanding」で始まる任意のテキストのブロックに一致します。「notwithstanding the fact that I like vegetables in my soup」は検索されますが、「The fact that I like vegetables in my soup notwithstanding」は検索されません。
$	文字列の末尾を示します。	(notwithstanding)$は、「notwithstanding」で終わる任意のテキストのブロックに一致します。「The fact that I like vegetables in my soup notwithstanding」は検索されますが、「notwithstanding the fact that I like vegetables in my soup」は検索されません。

エスケープシーケンス正規表現

表 C-5. エスケープシーケンス正規表現

要素	意味	例
\	正規表現で特殊な意味を持つ文字 (たとえば「+」) と一致させます。	(1) 正規表現 C\\C\+\+は「C\C++」に一致します。 (2) 正規表現*は*に一致します。 (3) 正規表現\?は?に一致します。
\t	タブ文字を示します。	(stress)\t は、サブ文字列「stress」を含み、「stress」の直後にタブ (ASCII 0x09) 文字が続く、任意の文字列のブロックに一致します。

要素	意味	例
\n	改行文字を示します。 注意 改行文字は、プラットフォームにより異なります。Windows では、改行は 2 文字で、改行 (CR) に行頭復帰 (LF) が続きます。UNIX および Linux では、1 文字の行頭復帰 (LF) で、Macintosh では、1 文字の改行 (CR) です。	(stress)\n は、サブ文字列「stress」を含み、「stress」の直後に 2 つの改行 (ASCII 0x0A) 文字が続く、任意の文字列のブロックに一致します。
\r	行頭復帰文字 (LF) を示します。	(stress)\r は、サブ文字列「stress」を含み、「stress」の直後に行頭復帰 (ASCII 0x0D) 文字が 1 つ続く、任意の文字列のブロックに一致します。
\b	バックスペース文字を示します。	(stress)\b は、サブ文字列「stress」を含み、「stress」の直後にバックスペース (ASCII 0x08) 文字が 1 つ続く、任意の文字列のブロックに一致します。
\xhh	指定された 16 進数コードの ASCII 文字を示します (hh は任意の 2 桁の 16 進数値を表します)。	\x7E(\w){6} は、先頭が~ (チルダ) 文字でちょうど 6 文字の英数字の「単語」を含む、任意の文字列のブロックに一致します。したがって、「~ab12cd」、「~Pa3499」が一致しますが、「~oops」は一致しません。

索引