TREND MICRO

InterScan™ for Microsoft Exchange 14.0

管理者ガイド

Messaging 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: SMEM148567/190103_JP_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。

InterScan for Microsoft Exchange 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。InterScan for Microsoft Exchange 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

第 2 章：InterScan の使用開始

第 6 章：検索の設定

第 7 章：セキュリティリスク検索の設定

第 8 章：添付ファイルブロックの設定

第 9 章：コンテンツフィルタの設定

第 10 章：情報漏えい対策の設定

第 11 章：スパムメール対策の設定

第 17 章：隔離領域の管理

第 18 章：InterScan の監視

第 19 章：管理タスクの実行

パート IV：ヘルプの参照

第 20 章：セキュリティリスクについて

第 21 章：よくある質問

付録 A：InterScan の Windows イベントログコード

付録 B：最適な運用のために

索引

はじめに

はじめに

本書では、Exchange サーバを保護する InterScan for Microsoft Exchange (以下、InterScan) のインストールとアップグレードを行う際に、実行する必要があるタスクに関する情報が記載されています。

この章の内容は次のとおりです。

ドキュメント

本製品には、次のドキュメントが付属しています。

- オンラインヘルプ: 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
- 最新の情報については弊社の「最新版ダウンロード」サイトをご参照ください。

  https://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

対象読者

InterScan のドキュメントは、以下を含むセキュリティシステムについて基本的な知識があることを前提としています。

- ウイルス対策およびコンテンツセキュリティ保護
- スパムメール保護
- ネットワークに関する概念 (IP アドレス、ネットマスク、トポロジ、LAN 設定など)
- ネットワークトポロジ
- Microsoft Exchange Server 管理
- Microsoft Exchange Server 2019、2016、2013 サーバの役割の設定
- メッセージ形式

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
 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

パート I

InterScan の概要と使用開始

第 1 章

Trend Micro InterScan for Microsoft Exchange の概要

Trend Micro™ InterScan for Microsoft Exchange は、Exchange メールサーバを保護します。InterScan をインストールすることによって、ウイルス/不正プログラム、トロイの木馬、ワーム、スパイウェア/グレーウェア、および不正な URL からサーバを保護できます。また、InterScan は、スパムメールや望ましくないコンテンツを含むメッセージを排除することにより、業務効率やネットワークの整合性を維持します。InterScan の通知は、重大なシステムイベントまたは大規模感染が発生するたびに、管理者またはその他の指定したユーザにタイムリーに警告を送信します。

この章の内容は次のとおりです。

システム要件

最新のシステム要件については、次の Web サイトを参照してください。

https://success.trendmicro.com/dcx/s/solution/000296865?language=ja

注意

システム要件に記載されている OS の種類やハードディスク容量などは、OS のサポート終了、弊社製品の改良などの理由により、予告なく変更される場合があります。

新機能

本バージョンの InterScan では、次の新機能が提供されます。

表 1-1. 14.0 の新機能

機能	説明
Exchange Server 2019 のサポート	本バージョンは、Windows Server 2019 または Windows Server 2022 で実行されている Microsoft Exchange Server 2019 の保護に対応しています。
SIEM へのログ転送	一般的なセキュリティ情報/イベント管理 (SIEM) プラットフォームに、セキュリティリスク、ポリシー違反、スパムメール、および監査のログを送信できるようになりました。
Time-of-Click フィルタのアップデート	Time-of-Click プロテクションの対象に、特定の受信者を指定することができるようになりました。
概要画面の改善	[概要] 画面がアップデートされ、詳細を一目で確認したり、初期設定で過去 30 日間の [概要] データおよびグラフを表示したりできるようになりました。過去 7 日間または当日を選択して、より直近のデータを表示することも可能です。
添付ファイルブロックフィルタのアップデート	パスワードで保護された Microsoft Office ドキュメントと圧縮ファイルをすべてブロック対象に含めることが可能となりました。

機能	説明
Apex Central のサポート	プログラムの物理的な場所またはプラットフォームを問わずウイルス対策およびコンテンツセキュリティプログラムを一元的に管理する機能として、本バージョンでは、Trend Micro Control Manager に代わって Trend Micro Apex Central が使用されます。

機能と利点

InterScan には次の機能と利点があります。

Web ベースの製品コンソール

SSL を使用して、セキュリティで保護された製品コンソールからリモートサーバにアクセスできます。

インストールとサポート

表 1-2. インストールとサポート

機能	利点
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 Microsoft Exchange サーバにインストールできます。 • クラスタ環境へのインストールをサポートしています。

クラスタのサポート	クラスタのサポート
	• Exchange 2019:
	  • データベース可用性グループ (DAG)
	• Exchange 2016:
	  • データベース可用性グループ (DAG)
	• Exchange 2013:
	  • データベース可用性グループ (DAG)

ウイルス対策機能と検索の種類

表 1-3. ウイルス対策機能と検索の種類

機能	利点
強力な独自のウイルス対策機能	• SMTP 検索 (トランスポート検索) とストアレベルの検索をサポートしています。 • メモリ上での検索をマルチスレッドで実行することによって、メッセージを素早く検索できます。 • ウイルス/不正プログラム、トロイの木馬、およびワームを検出し、処理できます。 • スパイウェア/グレーウェアを検出し、処理できます。 • 実際のファイルタイプを識別して、拡張子を偽ったファイルも適切に検出できます。 • ウイルス/不正プログラムに対してトレンドマイクロの推奨処理を使用したり、処理をカスタマイズしたりできます。 • すべてのマクロウイルス/不正プログラムを検出して削除したり、ヒューリスティックルールを使用してこれらを処理できます。
• 高度な脅威検索エンジン (ATSE)	高度な脅威検索エンジン (ATSE) は、パターンベースの検索とヒューリスティック検索を組み合わせて、標的型攻撃で使用されるドキュメントエクスプロイトやその他の脅威を検出します。
• IntelliTrap	本バージョンの InterScan では、IntelliTrap テクノロジが導入されています。IntelliTrap では、パッキングアルゴリズムの検索によってパックされたファイルが検出されます。IntelliTrap を有効にすると、InterScan が感染した添付ファイルに対してユーザ定義の処理を実行し、送信者、受信者、または管理者へ通知を送信します。
• 検索不能メッセージ部分に対応するカテゴリ	InterScan では、検索不能なメッセージ件数とウイルス/不正プログラム件数を区別します。検索不能ファイルには、暗号化されたメールメッセージ、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、[検索の制限条件] の範囲外のファイル、またはサポートされていないか、破損しているファイルが含まれます。

機能	利点
手動検索と予約検索	パターンファイルや検索エンジンのアップデートによって、手動検索または予約検索が中断されることはありません。 これらのページは、メールボックスサーバの役割でのみ表示されます。InterScan では、3 種類の差分検索オプションを使用できます。 • 特定の期間に配信されたメッセージの検索 • 添付ファイルを含むメッセージの検索 • InterScan でまだ検索されていないメッセージの検索
スマートスキャン	スマートスキャンは、セキュリティ機能をサーバからクラウドに移行します。 Trend Micro Smart Protection Network の中核をなす機能のスマートスキャンは、次の利点を提供します。 • クラウド内での高速かつリアルタイムのセキュリティステータス検索機能 • 新たな脅威に対する保護の開始までの時間の短縮 • エンドポイントでのメモリ消費の低減
アップデート	• 予約または手動でコンポーネントをアップデートできます。また、ダウンロード元をカスタマイズできます。

複数の検索フィルタ

表 1-4. 複数の検索フィルタ

機能	利点
添付ファイルブロック	• 指定した添付ファイルをブロックしたり、実際のファイルタイプ、ファイル拡張子、またはファイル名に基づいて添付ファイルをブロックできます。 • Active Directory 統合除外ルールをサポートしています。

機能	利点
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メッセージの内容を選別して除去します。 • Active Directory 統合ポリシー • コンテンツフィルタログ 本バージョンの InterScan では、キーワードが一致した場合にコンテンツフィルタログ内にキーワードが表示されます。 注意 キーワードまたは正規表現が長すぎる場合、情報の一部はログに表示されません。
情報漏えい対策	• ルールベースのフィルタを使用して、機密データがネットワーク外部に送信される前に検出、フィルタ、およびマスクします。 • 事前に定義されたテンプレートとデータ識別子が 100 個以上用意されており、その中から選択できます。また、企業固有の必須要件が満たされるように、カスタマイズしたパターンとキーワードリストを作成することもできます。 • ルールベースのテンプレートにより、ネットワーク外部へ転送される機密データの検出、フィルタ、およびマスクなどの処理を行うことができます。 • 情報漏えい対策ポリシーを作成し、Apex Central から InterScan サーバに配信して、すべてのサーバで全社的なポリシーの一貫性が保たれるようにします。

機能	利点
スパムメール判定ルール	• 検出レベルを調整できるスパムメール対策フィルタを使用して、スパムメールを排除できるとともに、メッセージの誤検出を削減できます。 • Outlook 迷惑メール対策との統合とエンドユーザメール隔離との統合のサポート 本バージョンの InterScan では、「Outlook 迷惑メール対策との統合」ソリューションと「エンドユーザメール隔離との統合」ソリューションを提供します。インストール時にどちらかのソリューションを選択できます。 • 迷惑メールフォルダ 本バージョンの InterScan では、検出されたスパムメールを標準の Outlook フォルダに送信することを選択できます。独立したスパムメールフォルダを作成する必要はなくなりました。
高度なスパムメール対策	高度なスパムメール対策には、高プロファイルユーザ (企業の経営陣など) を装ったメールによる潜在的な詐欺や攻撃を行うビジネスメール詐欺 (BEC) を検出するテクノロジが含まれています。

機能	利点
Web レピュテーション	• 本バージョンの InterScan では、Web レピュテーションテクノロジを利用して、リクエストされたすべての Web ページの整合性を評価しています。 • Web レピュテーション機能により、ユーザのアクセスするページが安全であることがチェックされ、不正プログラムやスパイウェア、ユーザの個人情報を盗むために仕掛けたフィッシング詐欺などの Web 上の脅威から保護されるようになります。 • 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 Web ページがブロックされます。Web レピュテーションはトレンドマイクロのサーバにレーティングを照会します。レーティングは、Web ページのリンク、ドメインと IP アドレスの関係、スパムメールの送信元、スパムメール内のリンクなどの複数の情報から決定されます。これらのレーティングをオンラインで取得することで、Web レピュテーションは常に最新の情報を基に危険性のあるページをブロックします。 • Web レピュテーション機能を有効にすることで、ユーザが不正 URL にアクセスすることを阻止できます。本文に URL を含むメールを受信すると、Web レピュテーションは、そのレピュテーションレーティングについてトレンドマイクロのサーバにクエリを実行します。Web レピュテーションでは、設定に応じて、URL を含むメールを隔離または削除したり、対象メールにタグを付加することができます。
Time-of-Click プロテクション	Time-of-Click プロテクションでは、メッセージの検索時にメールメッセージ本文に含まれる URL を書き換え、メッセージの受信者がそれらの URL をクリックしたときに URL を分析します。

機能	利点
Search & Destroy	Search & Destroy は、Exchange メールボックスサーバにある、望ましくないコンテンツが含まれるメールボックスコンポーネント (メール、会議、タスクなど) の検索とそれらの削除に使用できます。 注意 Search & Destroy メニューは、Search & Destroy 管理者または Search & Destroy オペレータの役割を設定した後に表示されます。
仮想アナライザの統合	Deep Discovery Advisor または Deep Discovery Analyzer の仮想アナライザを使用して、ファイルと URL を評価できます。不審ファイルまたは URL は InterScan から仮想アナライザに送信された後、隔離された仮想環境でコンテンツのシミュレーションと解析が実行され、多くの不正プログラムに共通する特性が識別されます。 仮想アナライザでの解析が完了すると、ファイルまたは URL のリスクレベルを記載したレポートが InterScan に送信されます。管理者は、組織のセキュリティレベルポリシーに基づいて、解析されたファイルまたは URL に対して特定の処理を実行するように InterScan を設定できます。

表 1-5. メールメッセージフローの保護

機能	受信メール	送信メール	内部メール	詳細
セキュリティリスク検索				初期設定では、受信メッセージと送信メッセージの両方に対して有効になっています。
添付ファイルブロック				特定の送信者や特定の受信者の設定をサポートしています。
コンテンツフィルタ				特定の送信者や特定の受信者の設定をサポートしています。

機能	受信メール	送信メール	内部メール	詳細
情報漏えい対策				送信メッセージに対して設定可能で、初期設定では有効になっています。特定の送信者や特定の受信者の設定をサポートしています。
スパムメール対策				
高度なスパムメール対策				ライティングスタイル機能によるビジネスメール詐欺 (BEC) 対策は、受信メッセージに対してのみ機能します。
Web レピュテーション				
Time-of-Click プロテクション				特定の受信者に対して設定できます。
受信メッセージディスクレーマー				
仮想アナライザの統合				受信メッセージに対して設定可能で、初期設定では有効になっています。

役立つ監視ツール

表 1-6. 役立つ監視ツール

機能	利点
通知	InterScan では、次の処理を実行するときに自動的に通知を送信できます。 • メールからウイルスやその他の脅威を検出して処理を実行 • 感染した添付ファイルをブロック • 不審 URL を検出 • メールから望ましくないコンテンツを除去 • 重大なシステムイベントを検出 • ウイルス/不正プログラムの大規模感染を検出 • 通知は、リアルタイム検索、手動検索、または予約検索中に、指定したユーザ宛てに送信できます。 注意 InterScan の通知が簡易ネットワーク管理プロトコル (SNMP) で正しく解決されるようにするには、InterScan インストールディレクトリから MIB (Management Information Base) ファイル「trend_smex_v2.mib」をネットワーク管理ツールにインポートします。
タイムリーで役立つレポートとログ	• 重要なイベントの詳細が記録されたアクティビティログを使用して最新の状態を把握できます。 • グラフィカルなレポートを送信または印刷できます。
隔離	• 不審メールを隔離するように InterScan を設定できます。 • 隔離イベントのログを照会し、安全と判断した隔離メッセージを再送信できます。

バージョンの比較

次の表に、前のバージョンと比較した InterScan の機能を示します。

表 1-7. バージョンの比較

サポート	InterScan 12.x	InterScan 14.x
OS バージョン	• Microsoft Windows Server 2008 R2 Standard Service Pack 1 以上 (64 ビット) • Microsoft Windows Server 2008 R2 Enterprise Service Pack 1 以上 (64 ビット) • Microsoft Windows Server 2008 R2 Datacenter RTM 以上 (64 ビット) • Microsoft Windows Server 2012 Standard または Datacenter (64 ビット) • Microsoft Windows Server 2012 R2 Standard または Datacenter (64 ビット) • Microsoft Windows Server 2016 Standard または Datacenter (64 ビット)	• Microsoft Windows Server 2008 R2 Standard Service Pack 1 以上 (64 ビット) • Microsoft Windows Server 2008 R2 Enterprise Service Pack 1 以上 (64 ビット) • Microsoft Windows Server 2008 R2 Datacenter RTM 以上 (64 ビット) • Microsoft Windows Server 2012 Standard または Datacenter (64 ビット) • Microsoft Windows Server 2012 R2 Standard または Datacenter (64 ビット) • Microsoft Windows Server 2016 Standard または Datacenter (64 ビット) • Microsoft Windows Server 2019 Standard または Datacenter (64 ビット) • Microsoft Windows Server 2022 Standard または Datacenter (64 ビット)
Exchange バージョンの最小要件	• Microsoft Exchange Server 2007 Service Pack 1 • Microsoft Exchange Server 2010 • Microsoft Exchange Server 2013	• Microsoft Exchange Server 2013 Service Pack 1 • Microsoft Exchange Server 2016 • Microsoft Exchange Server 2019

サポート	InterScan 12.x	InterScan 14.x

検索メカニズム	• Microsoft Exchange Server 2010:
	  • VSAPI 2.6
	  • トランスポートエージェント
	• Microsoft Exchange Server 2013/2016:
	  • Exchange Web サービス
	  • トランスポートエージェント
		• Microsoft Exchange Server 2013/2016/2019:
		  • Exchange Web サービス
		  • トランスポートエージェント

トランスポートレベルのリアルタイム検索	可	可
隔離フォルダ設定	可	可
メッセージフィルタ	受信および送信メッセージの削除機能として統合	受信および送信メッセージの削除機能として統合
通知	• CDO (Collaborative Data Object) • CDO (Collaborative Data Object) EX • Exchange Web サービス	• CDO (Collaborative Data Object) • CDO (Collaborative Data Object) EX • Exchange Web サービス
手動検索/予約検索	可	可

InterScan による Microsoft Exchange 環境の保護方法

トレンドマイクロでは、Microsoft Exchange サーバを標的としたセキュリティの脅威の危険性を認識しています。InterScan は、多種多様なセキュリティリスクから Exchange を保護します。InterScan では、Exchange を保護するために複数のフィルタを使用します。メールは次の順序で各フィルタにかけられます。

- スパムメール対策
- 高度なスパムメール対策
- 情報漏えい対策
- コンテンツフィルタ
- 添付ファイルブロック
- セキュリティリスク検索 (高度な脅威検索)
- Web レピュテーション

さらに、InterScan は、管理者がセキュリティリスクを監視し、それに対処する上で役立つ、通知機能とログクエリ機能を備えています。

表 1-8. InterScan による Microsoft Exchange 環境の保護方法

機能	説明
スパムメール対策	メールレピュテーション InterScan のメールレピュテーションを使用すると、スパムメールをネットワークへの侵入前にブロックできます。 コンテンツ検索 InterScan では、トレンドマイクロのスパムメール対策エンジンおよびスパムメール判定ルールを使用することで、スパムメールを、インフォメーションストアに配信される前に排除します。エンドユーザメール隔離が有効になっている場合、管理者は、承認する送信者リストおよびブロックする送信者リストを作成できます。エンドユーザメール隔離が有効になっている場合、エンドユーザは、承認する送信者の独自のリストを作成できます。

機能	説明
高度なスパムメール対策	高度なスパムメール対策では、InterScan でビジネスメール詐欺 (BEC) を使用して高プロファイルユーザ (企業の経営陣など) を装ったメールによる潜在的な詐欺や攻撃を検出するように設定することができます。送信者の内部ドメイン全体を BEC による潜在的な詐欺や攻撃の検索の対象に含めるように設定することもできます。 また、高度なスパムメール対策では、検索モードとしてコンサバティブモードとアグレッシブモードを選択できます。アグレッシブモードでは隔離された仮想環境でコンテンツを検索するために仮想アナライザが必要であるのに対し、コンサバティブモードでは仮想アナライザを使用せずにコンテンツを検索します。
情報漏えい対策	InterScan では、管理者が設定したポリシーに基づいて、さまざまなメッセージ部分の内容を機密情報でフィルタできます。また、送信メールをフィルタし、機密情報が含まれているメールに対して特定の処理を実行できます。
コンテンツフィルタ	InterScan では、管理者が設定したポリシーに基づいて、メッセージのヘッダ、件名、本文、添付ファイルの内容をフィルタできます。受信するメールと送信するメールをフィルタし、メッセージ本文または添付ファイルに望ましくない内容が含まれているメールに対して特定の処理を実行できます。
添付ファイルブロック	InterScan では、管理者が定義した種類や特定の名前に従って、望ましくない添付ファイルをブロックできます。検索時に、InterScan は検出したファイルをテキストメッセージで置き換えてから、そのメッセージを対象の受信者へ配信します。

機能	説明
セキュリティリスク検索	セキュリティリスク検索では、次のいずれかの検索エンジンを使用します。 • セキュリティリスク検索では、トレンドマイクロの最新バージョンの VSAPI 検索エンジンを使用して、ウイルス/不正プログラム、スパイウェア/グレーウェア、ワーム、トロイの木馬、およびその他の不正コードを検出します。トレンドマイクロの検索エンジンは、パターン認識およびルールベースのテクノロジを使用しています。すべての受信メールと送信メールに対して、リアルタイムまたはオンデマンドでウイルス/不正プログラムおよびその他のセキュリティリスクを検索します。 • セキュリティリスク検索では、パターンベースの検索とヒューリスティック検索の組み合わせを採用した高度な脅威検索エンジン (ATSE) を使用して、標的型攻撃で使用されるドキュメントの不正利用などの脅威を検出します。管理者は、詳しい分析のために不審ファイルを仮想アナライザに送信するように InterScan を設定できます。 高度な脅威検索エンジンでは、Windows の実行可能ファイル (PE) やスクリプトファイルなど、一部のファイルのウイルス検索の実行時に、機械学習型検索を使用します。機械学習型検索では、従来のシグネチャベースの不正プログラム検出に比べ、より多くの不正プログラムの亜種を検出できます。
Web レピュテーション	InterScan は、件名、本文、または添付ファイルに URL を含むメールを受信すると、これらのメールがインフォメーションストアに配信される前に、その URL のレピュテーション値についてトレンドマイクロのレーティングサーバを照会します。 InterScan では、メールに含まれる URL をトレンドマイクロのレーティングサーバで評価できなかった場合、高度な脅威を検出するために Trend Micro Deep Discovery Analyzer サーバに送信できます。 ただし、管理者は除外リストを設定して内部ドメインの信頼される URL を検索しないようにすることができます。

機能	説明
Time-of-Click プロテクション	Time-of-Click プロテクションでは、InterScan での検索時にメールメッセージ本文に含まれる URL を書き換え、メッセージの受信者がそれらの URL をクリックしたときに URL を分析するように設定することができます。
リアルタイム検索	InterScan は、すべての受信/送信メッセージ、SMTP メッセージ、パブリックフォルダに投稿されたドキュメント、および他の Microsoft Exchange サーバから複製されたファイルに対してリアルタイム検索を実行し、潜在的なウイルス/不正プログラムの侵入を防止します。リアルタイム検索では、InterScan は、管理者の設定に基づいてセキュリティリスクに対する処理を行います。
手動検索/予約検索	InterScan は、手動での起動または予約に応じて、オンデマンドで手動検索および予約検索を実行します。オンデマンド検索により、インフォメーションストアデータベース内からウイルス/不正プログラムを排除し、古いウイルス/不正プログラムの感染を撲滅し、再感染の可能性を最小化します。手動検索または予約検索を実行するときには、InterScan は、管理者の設定に従って、セキュリティリスクに対する処理を実行します。 InterScan では、個々のストアを検索対象に指定できます。たとえば、このオプションを使用して、すべてのストレージグループではなく、特定のストレージグループのデータベースに対してセキュリティリスク検索機能およびコンテンツセキュリティ機能を提供できます。
警告および通知	InterScan では、大規模感染および重要なシステムイベントに関する警告を送信できます。アウトブレークアラートは、設定数を超えるセキュリティリスクが検出された場合に管理者に通知します。これにより、管理者は Exchange 環境におけるセキュリティ違反に素早く対応できます。

機能	説明
レポートおよびログ	InterScan には、管理者が最新のセキュリティリスクおよびシステムの状態を常に把握できるようにするログ機能とレポート機能があります。コンポーネントのアップデートや検出時の処理などの重要なイベントはログに記録されます。管理者はこれらのイベントに対してクエリを実行し、Exchange 環境のセキュリティに関する最新の詳細情報を提供するログレポートを作成できます。 InterScan では、システム分析のためのレポートを生成して、印刷またはエクスポートすることができます。

駆除できないファイルについて

InterScan では、ファイルを正常に駆除できない場合、そのファイルに「駆除不能」のラベルを付け、駆除不能ファイルに対してユーザが定義した処理を実行します。初期設定の処理は「テキスト/ファイルで置換」です。InterScan では、すべてのウイルス/不正プログラムイベントと関連する処理の経過をログファイルに記録します。

InterScan で駆除処理を実行できない一般的な理由は、以下のとおりです。

- ファイルにトロイの木馬、ワーム、またはその他の実行可能プログラムが含まれていた場合。実行可能ファイルが実行されないようにするには、InterScan でプログラムを完全に削除する必要があります。
- そのファイルの圧縮に使用された圧縮形式がサポートされていない場合。InterScan では、`pkzip` を使用して圧縮され、圧縮の 1 階層目が感染しているファイルに対してのみ、駆除を行います。
- 予期せぬ問題により、駆除が妨げられた場合。

InterScan のテクノロジ

トレンドマイクロのウイルス検索エンジンとスパムメール対策エンジンは、ウイルス/不正プログラムおよびその他のセキュリティ上の脅威を検出し、スパムメールを排除します。このエンジンでは、最新のパターンファイルが必要です。このパターンファイルは、TrendLabs^{SM} によって提供され、アクティブ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から配信されます。

トレンドマイクロ検索テクノロジ

InterScan を使用すると、管理者は自社のセキュリティポリシーに適する不正プログラム検出のレベルを選択できます。InterScan で提供されるセキュリティレベルは、検索エンジンや必要な詳細分析を設定することによって選択できます。

次の表に、InterScan で使用できる検索テクノロジの概要を示します。

表 1-9. 検索テクノロジ

検索テクノロジ	説明
ウイルス検索エンジン	InterScan で使用できる標準の不正プログラム検索エンジン。 このウイルス検索エンジンでは、パターンマッチングとヒューリスティック検索テクノロジを使用して、不正プログラムがシステムに感染する前に脅威を特定できます。
高度な脅威検索エンジン (ATSE)	ATSE では、積極的なヒューリスティック検索を実行してファイルをチェックし、従来型でない脅威 (ドキュメントの不正利用など) が存在しないか確認できます。検出されるファイルによっては安全なものもありますが、仮想環境でさらに観察および分析する必要があります。 ATSE には、ウイルス検索エンジンが提供する機能を強化します。 ATSE 設定の詳細については、109 ページの「セキュリティリスク検索の対象の設定」を参照してください。

検索テクノロジ	説明
仮想アナライザ	仮想アナライザは、隔離された仮想環境でコンテンツのシミュレーションと解析を実行して多くの不正プログラムに共通する特性を識別します。仮想アナライザでは、たとえば、メッセージに添付されているファイルや URL にエクスプロイトコードが含まれているかどうかを確認します。多くのファイルまたは URL には実行可能データが含まれませんが、攻撃者はそのようなファイルまたは URL を媒介にして、プログラムやプログラムを実行するオペレーティングシステムの脆弱性を突く方法を見つけ出します。このため、狙ったユーザに不正なファイルまたは URL を送信するという方法は、攻撃者にとってシステムを危険にさらすのに効果的な方法となっています。 **注意** 仮想アナライザは、トレンドマイクロ独自の脅威分析エンジンと推奨エンジンに基づいてユニークな方法でセキュリティを可視化する製品で、別途ライセンスが必要です。 仮想アナライザの設定の詳細については、229 ページの仮想アナライザの設定を参照してください。

ウイルス検索エンジンのアップデート

トレンドマイクロでは、新しいバージョンのウイルス検索エンジンを定期的に提供しています。新しいエンジンは、たとえば次の場合にリリースされます。

- トレンドマイクロのソフトウェアに、新しい検出テクノロジが組み込まれた場合
- 現在のウイルス検索エンジンでは処理できない、危険度の高いウイルス/不正プログラムが新たに発見された場合
- 検索性能が強化された場合
- 別のファイル形式、スクリプト言語、エンコード、または圧縮形式に対するサポートが追加された場合

最新のウイルス検索エンジンのバージョン番号を確認するには、次のサイトを参照してください。

https://www.trendmicro.com

InterScan が現在使用しているウイルス検索エンジンのバージョンを調べるには、製品コンソールを開き、[概要] > [システム] を表示します。

ヒント

トレンドマイクロではウイルス検索エンジンを頻繁にアップデートすることをお勧めします。予約アップデートを使用すると、InterScan のコンポーネントを簡単に定期的にアップデートできます。

パターンファイル

トレンドマイクロのウイルス検索エンジンは、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、最新のセキュリティリスクを特定します。

次の Web サイトで、最新バージョン、リリース日、およびファイルに記載された新しいすべてのウイルス定義を確認できます。

https://downloadcenter.trendmicro.com/index.php?regs=jp&clk=jp_patterns

InterScan サーバ上で InterScan が現在使用しているパターンファイルのバージョンを調べるには、製品コンソールを開き、[概要] > [システム] の順に選択します。

ヒント

トレンドマイクロではパターンファイルを頻繁にアップデートすることをお勧めします。予約アップデートを使用すると、InterScan のコンポーネントを簡単に定期的にアップデートできます。

パターンファイルの番号

お使いのソフトウェア製品内のパターンファイルがトレンドマイクロから提供されている最新のパターンファイルであるか比較するために、パターンファイルにはバージョン番号があります。

パターンファイルの表示には、xxxxx.xxx.xx というフォーマットが使用されています。

パターンファイル番号が 1.786.01 の場合を例にとります。

- 最初の桁 (1) はパターンファイル番号が 999 を超えた回数を示すロール番号です。最大 5 桁です。
- 次の 3 桁 (786) は従来のパターンファイル番号を示します。
- 最後の 2 桁 (01) は、ビルド番号です。

ウイルス検索エンジンでのウイルスパターンファイルの使用方法

ウイルス検索エンジンは、パターンファイルと連携し、パターンマッチングというプロセスを使用して検出の第 1 レベルを実行します。ウイルス検索エンジンによって一致するものが検出された場合、システム管理者にメールで通知が送られます。

注意

ウイルス検索エンジンには、ディスク領域管理用に古いパターンファイルの自動クリーンナップルーチンが含まれています。

アップデートについて

アップデート機能を使用することにより、InterScan のすべてのコンポーネントの最新版をインターネットからダウンロードできます。

アップデートでは、ネットワークサービスの中断やコンピュータの再起動は必要ありません。InterScan では、あらかじめ決めておいた間隔で定期的に最新コンポーネントを受信するか、手動アップデートを実行することができます。

パターンファイルの差分アップデート

アップデートではパターンファイルの差分アップデートをサポートしています。毎回、パターンファイルをすべてダウンロードするのではなく、新しい部分のみをダウンロードし、既存のパターンファイルに追加できます。この効率的な方法により、ネットワーク帯域幅の消費を大幅に削減できます。

アップデートおよび差分アップデートを使用するように InterScan を設定すると、アップデートに費やす時間が短縮されます。

InterScan でのアップデートの使用方法

InterScan は、アクティブアップデートサーバを手動アップデートと予約アップデートのダウンロード元として使用するように設定できます。コンポーネントアップデートの時間になると、InterScan はアクティブアップデートサーバに直接ポーリングします。アップデートプログラムは新しいコンポーネントを利用できるかどうかを確認し、利用できる場合は、InterScan がアップデートをダウンロードします。

ヒント

複数のサーバ環境で効率よくダウンロードするには、1 つの InterScan サーバに対して、他のサーバがこのサーバから最新版をダウンロードできるように設定します。この設定によって、その InterScan サーバは、差分アップデートを受け取る環境内の他のサーバに対して、仮想アクティブアップデートサーバとして機能します。

トレンドマイクロの推奨設定

トレンドマイクロの推奨設定では、ファイルのヘッダから実際のファイルタイプを識別して、不正プログラムのリスクを伴うファイルタイプのみを検索することで、検索パフォーマンスを最適化します。トレンドマイクロの推奨設定では、実際のファイルタイプの認識機能を使用することで、偽のファイル拡張子を使用して偽装されたファイルを識別します。

トレンドマイクロの推奨設定には次の利点があります。

- パフォーマンスの最適化: トレンドマイクロの推奨設定では、使用するシステムリソースを最小限に抑えているため、ホスト上で実行されている重要なアプリケーションのパフォーマンスに影響を与えません。
- 検索時間の短縮: トレンドマイクロの推奨設定では、実際のファイルタイプの認識機能を使用するため、感染の恐れがあるファイルのみを検索することで検索時間を大幅に短縮してします。

IntelliTrap

ウイルス作成者は、リアルタイム圧縮の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あります。IntelliTrap は、リアルタイムの圧縮済み実行ファイルを遮断し、他の不正プログラムの特性とファイルを組み合わせて、ユーザのネットワークに入り込むというようなウイルスのリスクを減らすのに役立っています。IntelliTrap は、このようなファイルをセキュリティリスクと見なし、安全なファイルを誤ってブロックする場合があるため、IntelliTrap を有効にするときは、ファイルを削除または消去せずに隔離することを検討してください。ユーザが定期的にリアルタイムの圧縮された実行ファイルをやりとりする場合は、IntelliTrap を無効にします。

IntelliTrap では、以下のコンポーネントを使用します。

- 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

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。ウイルスまたは不正プログラムの脅威が検出されると、そのウイルス/不正プログラムに対応した推奨処理が実行され、環境内の攻撃されやすいポイントが保護されます。

ヒント

トレンドマイクロでは、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切な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利点は、次のとおりです。

- 時間の節約と容易な保守 – 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るため、検出時の処理を設定する手間が省けます。

- 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。

HotFix、Patch、および Service Pack について

Critical Patch / Security Patch — 至急対策の必要がある問題のみを修正する目的で一般公開されるプログラムです。トレンドマイクロでは通常、正式な製品リリースの後に、HotFix、Patch、および Service Pack を開発して、未解決の問題への対処、製品のパフォーマンスの向上、および新しい機能の追加を行います。

トレンドマイクロがリリースする可能性のあるアイテムは次のとおりです。

- HotFix — 特定の問題を修正するために提供されるプログラムです。通常は一般公開されません。
- Patch — 既知の問題に対する修正(HotFix / Critical Patch / Security Patch)を累積的に含み、一般公開されるプログラムです。
- Service Pack — 既知の問題に対する累積的な修正に加え、製品の挙動変更や機能変更を盛り込んで一般公開されるプログラムです。

ベンダーやサポートプロバイダは、これらのアイテムがリリースされるとユーザに連絡する場合があります。トレンドマイクロの Web サイトを参照して、新しい Patch または Service Pack のリリース情報を確認してください。

https://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

すべてのリリースには、インストール、配信、および設定の情報が記載された Readme ファイルが含まれています。この Readme ファイルをよく読んでからインストールを実行してください。

第 2 章

InterScan の使用開始

この章では、InterScan for Microsoft Exchange (以下、InterScan) のアクティベートとアップデートの方法について説明します。

内容は次のとおりです。

使用開始

InterScan のインストールを完了したら、いくつかの作業を実行して、すべてが適切に設定されて正しく動作していることを確認します。

手順

1. InterScan 製品コンソールを開きます。
2. セットアップで既存のプロキシサーバを認識するように InterScan を設定していない場合は、ここで設定します。
3. その他のインストール済みの InterScan モジュールをアクティベートします。
4. セットアップで Trend Micro Apex Central に InterScan を登録していない場合は、ここで登録します。
5. InterScan パターンファイルおよび検索エンジンのアップデートを実行します。
6. パターンファイルおよび検索エンジンの自動アップデートを予約します。
7. EICAR テストファイルを使用して、インストール後の動作確認を行います。

製品コンソールについて

InterScan のアクセスおよび制御は、直感的に使用できる製品コンソールから行います。製品コンソールを使用すると、ネットワーク上の任意のエンドポイントから複数の Exchange サーバおよびリモートサーバを管理することができます。InterScan 製品コンソールは、パスワードで保護されており、許可された管理者のみが InterScan の設定を変更できます。製品コンソールは、サポートされているブラウザを使用してネットワーク上の任意のエンドポイントで表示できます。

ローカルサーバでの製品コンソールの起動

手順

1. [スタート] > [すべてのプログラム] > [Trend Micro InterScan for Microsoft Exchange] > [InterScan 管理コンソール] の順にクリックします。

   注意

   Windows 2012 プラットフォームでは、デスクトップショートカットのみを使用できます。

2. ユーザ名とパスワードを入力します。
3. [ログオン] をクリックします。

   注意

   インストールされた InterScan にログオンするには、セットアップ時に設定した管理グループに属するアカウントを使用します。

リモートサーバでの製品コンソールの起動

手順

1. サポートされているブラウザを使用して、以下にアクセスします。

   `<https>://<サーバ名>:<ポート番号>/smex`

   「サーバ名」は InterScan がインストールされているサーバの名前、「ポート番号」はそのサーバへのアクセスに使用されるポート番号です。

   注意

   初期設定では、HTTPS にはポート 16373 が使用されます。

2. ユーザ名とパスワードを入力します。

3. [ログオン] をクリックします。

製品コンソールのメインビュー

InterScan の Web コンソールには直感的に使用できるユーザインタフェースが採用されているため、InterScan の設定および管理に必要なすべての機能に簡単にアクセスできます。

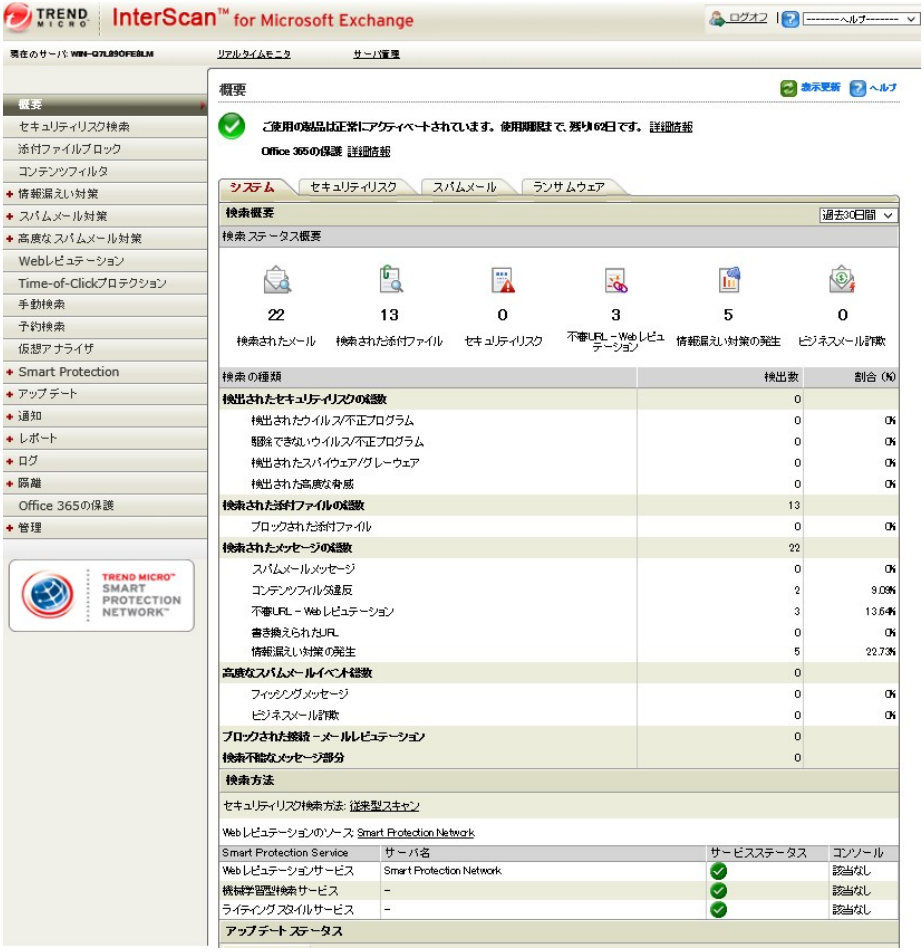


図 2-1. 製品コンソール

製品コンソールの構成要素

バナー

InterScan のバナー領域には製品名やサーバ情報、各種リンクが含まれます。

図 2-2. 製品コンソールのバナー領域

バナーには、次のものが表示されます。

- 現在のサーバ — このコンソールの管理対象サーバです。
- リアルタイムモニタ — クリックすると、リアルタイムモニタにアクセスします。

  詳細については、58 ページの「リアルタイムモニタの概要」を参照してください。
- サーバ管理 — クリックすると、サーバ管理コンソールにアクセスします。

  詳細については、58 ページの「サーバ管理コンソールの概要」を参照してください。
- ログオフ — クリックすると、セッションが終了し、製品コンソールが閉じます。

  注意
  製品コンソールをログオフすることで、許可されていないユーザが設定を変更するのを防ぐことができます。
- ヘルプ — ドロップダウンリストからオプションを選択すると、サポート情報を表示できます。

  ヘルプオプションには、次のものがあります。

  - 目次と索引 — オンラインヘルプの目次および索引を表示します。
  - 製品 Q&A — 製品のトラブルシューティングの最新情報を確認できる製品 Q&A ページを表示します。

- セキュリティ情報 — 最新のセキュリティリスク情報を掲載するトレンドマイクロのセキュリティ情報ページを表示します。
- 購入情報 — 最寄りの販売代理店およびサービスプロバイダを検索できるトレンドマイクロの Web ページを表示します。
- サポート情報 — トレンドマイクロのテクニカルサポート Web サイトにアクセスします。
- バージョン情報 — InterScan とコンポーネントのバージョン番号、および InterScan のシステム情報を表示します。

サイドメニュー

サイドメニューからは、InterScan のメインメニュー項目にアクセスできます。

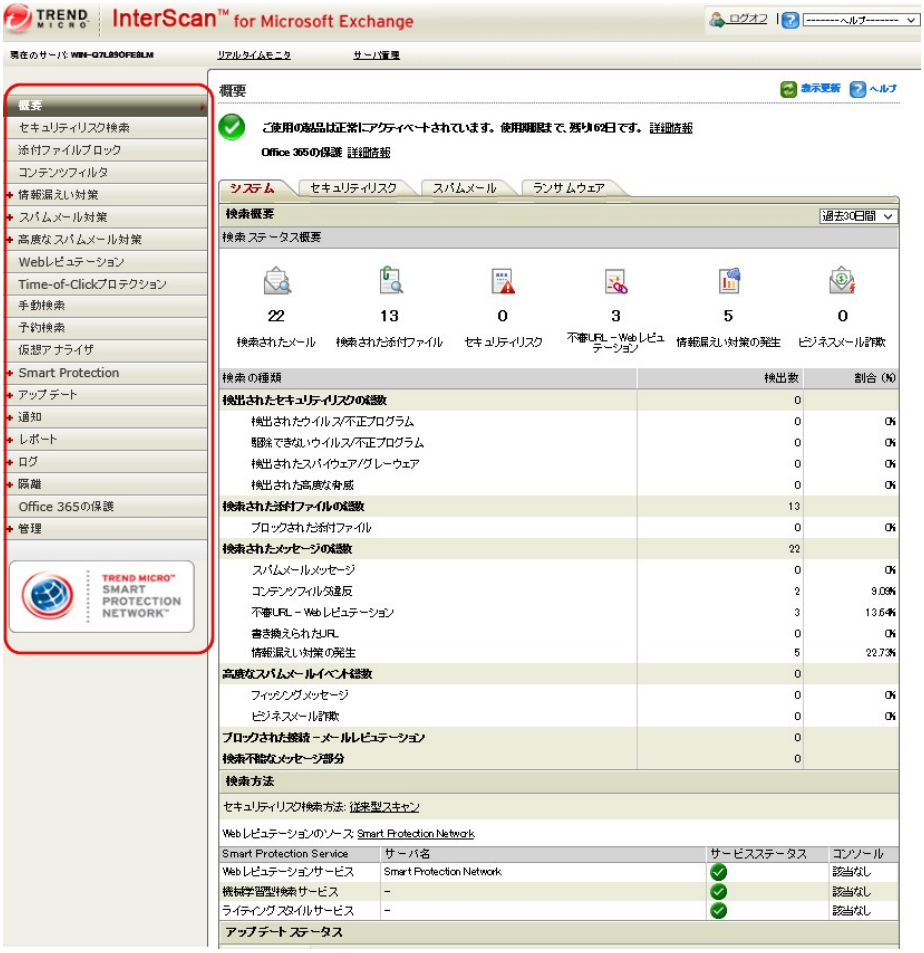


図 2-3. 製品コンソールのサイドメニュー

設定領域

設定領域では、InterScan のすべての設定とオプションを設定および変更することができます。

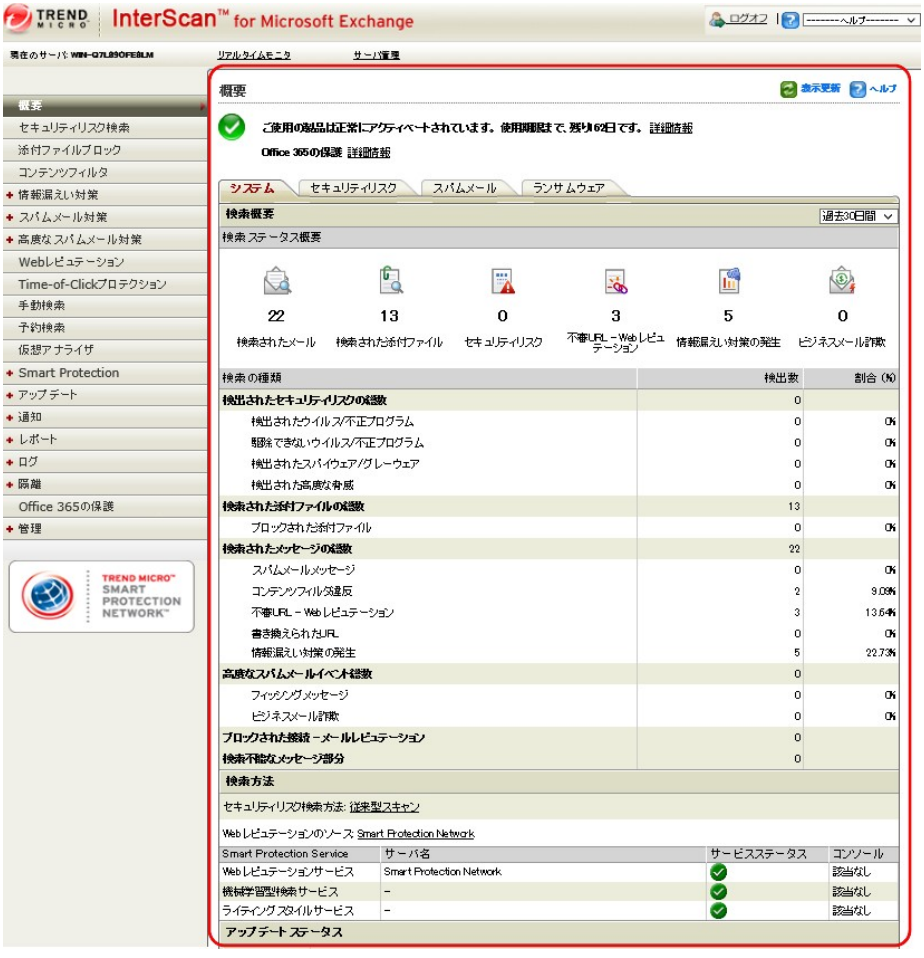


図 2-4. 製品コンソールの設定領域

InterScan 製品コンソール使用中のヘルプの参照

InterScan には、次のタイプのヘルプが用意されています。

手順

- InterScan の各機能の使用方法については、オンラインヘルプを参照してください。オンラインヘルプにアクセスするには、ヘルプアイコン (ヘルプ) をクリックするか、バナー領域の [ヘルプ] ドロップダウンリストから [目次と索引] を選択して目次を開きます。
- トラブルシューティングおよび Q&A 情報にアクセスするには、バナー領域のリストボックスから [製品 Q&A] を選択します。
- コンピュータセキュリティの脅威や警告に関する一般的な情報にアクセスするには、バナー領域のリストボックスから [セキュリティ情報] を選択します。
- トレンドマイクロ販売代理店またはサービスプロバイダへの問い合わせ方法を確認するには、バナー領域のリストボックスから [購入情報] を選択します。

InterScan のアクティベーション

次の場合にはアクティベーションを実行する必要があります。

- InterScan を初めてインストールする場合

  たとえば、トレンドマイクロの販売代理店からある製品バージョンを購入し、アクティベーションコードを入手した場合です。

- バージョンタイプを変更する場合

  たとえば、トレンドマイクロの担当者から新しいアクティベーションコードを入手し、製品コンソールを使用して新しいバージョンをアクティベートする場合です。

注意

体験版では、InterScan の全機能を 30 日間使用できます。30 日を過ぎても InterScan のタスクは引き続き実行されますが、アップデートは実行されなくなります。

InterScan のアクティベーションは、インストール時に実行するか、インストール後に製品コンソールから実行します。

インストール中の InterScan のアクティベーション

手順

1. インストールプログラムを起動します。
2. [製品のアクティベーション] 画面にアクティベーションコードを入力します。
3. インストールを完了し、InterScan をアクティベートします。

製品コンソールを使用した InterScan のアクティベーション

手順

1. [管理] > [製品ライセンス] の順にクリックします。
2. [アップグレード方法] をクリックして InterScan を登録します。

   オンライン登録用のトレンドマイクロの Web サイトが表示されます。
3. [製品ライセンス] 画面で [新しいコード] をクリックします。
4. 所定の欄にアクティベーションコードを入力します。
5. [アクティベート] をクリックします。

アクティベーションコード

InterScan には、通常版と DLP Edition の 2 種類があります。また、DLP Edition のみ体験版と製品版があります。

注意

トレンドマイクロでは、Exchange サーバの保護が途切れないように、体験期間またはサポート契約期間が終了するまでに新しいアクティベーションコードを取得するか、サポート契約を更新することをお勧めします。詳細については、購入先にお問い合わせください。

通常版アクティベーションコード

通常版アクティベーションコードを使用すると、InterScan がアクティベートされます。

表 2-1. 通常版アクティベーションコードの機能

製品の種類	通常版の機能
製品版	製品版アクティベーションコードでは、サポートサービスが提供され、通常版アクティベーションで使用可能な InterScan のすべての機能を実装できます。サポート契約の有効期限が近づくと、InterScan の画面にメッセージが表示されます。

DLP Edition アクティベーションコード

DLP Edition アクティベーションコードを使用すると、InterScan 通常版のすべての機能に加えて、情報漏えい対策機能も使用可能になります。

表 2-2. DLP Edition アクティベーションコードの機能

製品の種類	DLP EDITION の機能
体験版	体験版アクティベーションコードを使用することにより、有効期間内において、製品版と同様の機能を使用できます。有効期間内は、すべてのコンポーネントのアップデート、セキュリティリスク検索、添付ファイルブロック、コンテンツフィルタ、スパムメール対策、エンドユーザメール隔離、Web レピュテーションの機能を利用できます。 有効期限が切れたコードは使用できなくなります。コードの使用中に作成されたルールその他の設定はすべて、そのコードの有効期限が切れると無効になります。1 つのアクティベーションコードの有効期限が切れても、他のコードに影響することはありません。たとえば、スパムメール対策のライセンスが別途に設定されている製品の体験版を使用している場合、1 つのライセンスが期限切れになっても、それが別のライセンスの有効期限に影響することはありません。
製品版	製品版アクティベーションコードでは、サポートサービスが提供され、InterScan のすべての機能を実装できます。サポート契約の有効期限が近づくと、InterScan の画面にメッセージが表示されます。 製品版アクティベーションコードの有効期限が切れると、エンジンやパターンファイルのアップデートをダウンロードできなくなり、最新の状態での保護を行うことができなくなります。ただし、体験版アクティベーションコードとは異なり、製品版アクティベーションコードでは、既存の設定やその他の設定がすべて有効のまま維持されます。

DLP Edition アクティベーションコードの追加機能

InterScan の追加機能を使用するには、DLP Edition を購入するか、または体験版をお試しください。追加機能は次のとおりです。

- 情報漏えい対策 — トレンドマイクロの情報漏えい対策は、企業の情報を予期せぬ漏えいおよび計画的な盗難から保護する、包括的なソフトウェアソリューションです。詳細にカスタマイズ可能な企業固有のポリシー作成、および組み込みの規制テンプレートを使用して、機密情報を管理、制御、および監視することができます。

アクティベーションコードの比較

次の表に、それぞれのタイプのアクティベーションコードで利用できる機能を示します。

表 2-3. 種類別アクティベーションコードの利用可能な機能

機能	DLP Edition アクティベーションコード		通常版アクティベーションコード
	製品版	体験版	製品版
製品コンソール	可	可	可
レポート、ログ、および隔離ファイル管理におけるスパムメール対策項目、コンテンツフィルタ項目、および Web レピュテーション項目	可	可	可
セキュリティリスク検索	可	可	可
高度な脅威検索エンジン	可	可	可
添付ファイルブロック	可	可	可
スパムメール対策: コンテンツ検索	可	可	可
高度なスパムメール対策	可	可	可
情報漏えい対策	可	可	不可
スパムメール対策: メールレピュテーション	可	可	可
コンテンツフィルタ	可	可	可
Web レピュテーション	可	可	可
Time-of-Click プロテクション	可	可	可
手動検索/予約検索	可	可	可
Smart Protection	可	可	可
アップデート	可	可	可

機能	DLP Edition アクティベーションコード		通常版アクティベーションコード
	製品版	体験版	製品版
エンドユーザメール隔離 注意 エンドユーザメール隔離は、Exchange Server 2013 でのみ使用できます。	可	可	可
Apex Central のサポート	可	可	可
Search & Destroy	可	可	可
仮想アナライザ	可	可	可

InterScan の再アクティベート

製品バージョンを変更した場合、InterScan の再アクティベートが必要となることがあります。再アクティベートするには、新しいアクティベーションコードを入力します。[新しいコード] をクリックし、新しいアクティベーションコードを入力することで、新しいバージョンの InterScan の機能を利用できるようになります。

手順

1. [管理] > [製品ライセンス] の順にクリックします。

   [製品ライセンス] 画面が表示されます。

2. [新規入力] をクリックします。

   [製品ライセンス > 新しいコード] 画面が表示されます。

3. 新しいアクティベーションコードを入力するか、貼り付けます。

4. [アクティベート] をクリックします。

これによって新しいバージョンの InterScan がアクティベートされ、そのライセンスに基づいて使用できるすべての機能が有効になります。

InterScan のアップデートについて

セキュリティソフトウェアは、最新の技術を使用していないと効力を発揮しません。新しいウイルス/不正プログラムやその他の不正コードは絶えず出現しています。そのため、InterScan のコンポーネントを定期的にアップデートして、新しいセキュリティ上の脅威に対して防御することが極めて重要です。

アップデート可能な InterScan のコンポーネントは次のとおりです。

- ウイルスパターンファイル
- スパイウェアパターンファイル
- IntelliTrap パターンファイル
- IntelliTrap 除外パターンファイル
- ウイルス検索エンジン
- CI クエリハンドラ
- スパムメール対策パターンファイル
- スパムメール対策エンジン
- URL フィルタエンジン
- スマートスキャンエージェントパターンファイル
- 高度な脅威検索エンジン
- 高度な脅威相関パターンファイル

最新のコンポーネントを使用しているかどうかを調べるには、InterScan 製品コンソールから [概要] 画面を表示します。この画面には、現在のバージョンと、ダウンロードできる最新バージョンのリストが表示されます。

InterScan のアップデート - 要件となるタスク

手順

1. 製品をアクティベートします。
2. プロキシサーバでネットワーク上のインターネットトラフィックが処理されている場合、プロキシサーバ情報を設定します。
3. アップデート方法とダウンロード元を設定します。
   - アップデートの方法には、手動アップデートおよび予約アップデートがあります。

- ダウンロード元には、アクティブアップデートサーバ、インターネット、イントラネット UNC パス、および Apex Central があります。

プロキシの設定

プロキシサーバは、セキュリティを強化して、帯域幅を効率的に利用するために使用されます。ネットワークでプロキシサーバを使用している場合、インターネットへ接続して、InterScan を最新の状態に維持するために必要な最新コンポーネントをダウンロードし、ライセンスステータスをオンラインでチェックするようにプロキシ設定値を設定します。

プロキシサーバは次の機能で使用されます。

- Trend Micro Smart Protection Network
- アップデート
- 製品ライセンスの確認
- Web レピュテーション

手順

1. [管理] > [プロキシ] の順にクリックします。
2. [Web レピュテーション、Time-of-Click プロテクション、機械学習型検索、アップデート、および製品ライセンスの確認にプロキシサーバを使用する] を選択します。このチェックボックスをオンにすると、以下の設定がオンになります。

   トレンドマイクロのレピュテーションサーバへの Web レピュテーションクエリの実行

   Time-of-Click プロテクション

   機械学習型検索

   アップデート

   プロキシサーバを使用しての製品ライセンスの通知
3. プロキシサーバの名前または IP アドレスを入力します。

4. ポート番号を入力します。
5. (任意) [SOCKS 5 を使用する] をオンにします。
6. プロキシサーバで認証を必要とする場合は、ユーザ名とパスワードを指定します。

手動アップデートの設定

InterScan をインストールした直後、および大規模感染が発生した場合は、ウイルス検索エンジンとパターンファイルを手動でアップデートすることをお勧めします。

手順

1. [アップデート] > [手動] の順に選択します。
2. アップデートするコンポーネントを選択します。
3. [アップデート] をクリックします。

   InterScan がコンポーネントのダウンロードを開始し、経過時間とダウンロードの残りの割合を示す進行状況バーが表示されます。指定したダウンロード元から最新のコンポーネントがダウンロードされます。

予約アップデートの設定

アクティブアップデートサーバを定期的にチェックし、使用可能なコンポーネントがあれば自動的にダウンロードするように InterScan を設定します。予約アップデート中、InterScan は、指定されたダウンロード元に最新のコンポーネントが存在するかどうかをチェックします。

ヒント

大規模感染が発生した場合、トレンドマイクロはパターンファイルを即座にアップデートします (1 週間に何度もアップデートする場合もあります)。また、ウイルス検索エンジンと他のコンポーネントは定期的にアップデートされます。トレンドマイクロでは、コンポーネントを毎日 (大規模感染時はより頻繁に) アップデートして、コンポーネントを常に最新の状態に維持することを推奨します。

手順

1. アップデートのダウンロード元を選択します。
   a. [アップデート] > [ダウンロード元] の順に選択します。

      [ダウンロード元] 画面が表示されます。

   b. ダウンロード元を選択します。
   c. [保存] をクリックします。
2. スケジュールを設定します。
   a. [アップデート] > [予約] の順に選択します。
   b. [予約アップデートを有効にする] チェックボックスをオンにして、InterScan がスケジュールに従ってアップデートを開始するように設定します。
   c. [アップデートスケジュール] を設定します。
      1. アップデートの頻度を選択します。分ごと、時間ごと、日ごと、週ごとがあります。
      2. 時間および分を選択することによって、アップデートの [開始時間] を設定します。アップデートが発生すると、この時間にダウンロードが開始されます。
3. ダウンロード元からダウンロードするコンポーネントを選択します。
   a. 予約アップデート時にダウンロードするコンポーネントを選択します。

      ヒント

      表の最上部にあるチェックボックスをオンにすると、すべてのコンポーネントが選択されます。

   b. [保存] をクリックします。

      選択したコンポーネントのダウンロードは、設定したスケジュールに従って開始されます。

ダウンロード元の設定

InterScan を最新の状態に維持するには、最新のコンポーネントをダウンロードする必要があります。この画面を使用して、InterScan が最新コンポーネントをダウンロードする元を設定します。初期設定の場所は、トレンドマイクロのアクティブアップデートサーバです。手動ダウンロードまたは予約ダウンロード中、InterScan はここで設定した場所をチェックし、その場所から最新のコンポーネントをダウンロードします。

重要

[ダウンロード元] メニューは、トレンドマイクロのアクティブアップデートサーバ以外の [ダウンロード元] を使用して InterScan を旧バージョンからアップグレードする場合にのみ使用できます。InterScan の新規インストールでは、[ダウンロード元] メニューは使用できません。

手順

- トレンドマイクロのアクティブアップデートサーバ – 初期設定のアクティブアップデートサーバからダウンロードする場合に選択します。

  トレンドマイクロは、新しいコンポーネントが使用可能になり次第、そのコンポーネントをアクティブアップデートサーバにアップロードします。アップデートを頻繁かつタイムリーに実行する必要がある場合は、ダウンロード元としてトレンドマイクロのアクティブアップデートサーバを選択します。

- イントラネット上のリソース – イントラネット上の特定の場所からダウンロードする場合に選択します。

  最新のコンポーネントが格納されているイントラネット上の場所からコンポーネントをダウンロードします。

  ネットワーク上の別のサーバの UNC パスを入力します。

注意

集中管理型のイントラネット上の場所を 1 つ以上設定することによって、ネットワークトラフィックを大幅に削減し、アップデート時間を大幅に短縮できます。この方法は、メールサーバをインターネットに直接接続したくない場合にも有効です。また、フロントエンドサーバをインターネット上のトレンドマイクロのアクティブアップデートサーバに接続し、フロントエンドサーバからアップデートを受信するようにバックエンドサーバを設定することも可能です。

- 他のサーバがこのサーバからアップデートをダウンロードできるようにする — 他の InterScan サーバがこのサーバからアップデートをダウンロードできるようにするには、このオプションを選択します。

  現在のサーバにあるアップデートパッケージのコピーを作成するように InterScan を設定するには、他のサーバがこのサーバからアップデートをダウンロードできるようにする をクリックします。通常、InterScan では、ダウンロードするよう設定されたコンポーネントまたは必要とされるコンポーネントの差分だけをダウンロードします。アップデートパッケージをコピーするように InterScan を設定した場合、ダウンロードできるすべてのコンポーネントがダウンロードされます。

  たとえば、2 つの Exchange サーバ「a」と「b」が存在し、それぞれに InterScan がインストールされているとします。InterScan は、サーバ「a」を毎日アップデートし、すべてのコンポーネントをダウンロードするように設定されています。InterScan は、サーバ「b」を毎週アップデートし、スパムメール判定ルールコンポーネントだけをダウンロードするように設定されています。両方のサーバは、必要に応じてトレンドマイクロのアクティブアップデートサーバからコンポーネントを受信します。このため、この 2 つのサーバ上のコンポーネントは必ずしも同じであるとは限らず、この 2 つのサーバがアクティブアップデートサーバにポーリングしたとき、異なる差分アップデートが必要になります。より効率的なサーバの構成方法は、アップデートパッケージをコピーするようにサーバ「a」を設定することです。これによって、サーバ「a」をサーバ「b」のダウンロード元に設定し、サーバ「b」は、アクティブアップデートサーバから受信するのと同じようにサーバ「a」からアップデートの差分を受信できるようになります。

注意

クラスタ環境では、コンポーネントを同期させるため、このオプションが初期設定で有効になっており無効にできません。

Trend Micro Cloud App Security による Office 365 の保護

トレンドマイクロでは、Office 365 Exchange Online、OneDrive for Business および SharePoint Online を保護する「Cloud App Security」と呼ばれるセキュリティサービスを提供しています。

InterScan で保護できない場合でも、Cloud App Security を併せてご利用いただくことで、オンプレミスサーバとオンラインの Exchange サービスを保護することができます。

詳細については、「Trend Micro Cloud App Security」および Cloud App Security のオンラインドキュメントを参照してください。

第 3 章

Exchange サーバのセキュリティの確立と維持

InterScan for Microsoft Exchange (以下、InterScan) は、Exchange 環境全体の包括的なセキュリティを実現するために設計されました。ここでは、InterScan の主要なセキュリティ機能の概要およびセキュリティベースラインを迅速に確立し、維持する方法について説明します。

内容は次のとおりです。

セキュリティの確立

InterScan をアクティベートすると、InterScan の機能を設定できます。次の手順に従って Exchange サーバのセキュリティを設定することをお勧めします。

手順

1. InterScan をアップデートします。

   InterScan のリリース時には、その時点で利用可能なスマートスキャンエージェントパターンファイル、ウイルス検索エンジン、ウイルスパターンファイル、スパムメール対策エンジン、およびスパムメール判定ルールが組み込まれています。しかし、トレンドマイクロではエンジンとパターンファイルを継続的にアップデートしています。InterScan によって最適に保護できるよう、インストール後すぐにコンポーネントをアップデートします。44 ページの「InterScan のアップデートについて」を参照してください。

2. InterScan が正常に実行および機能していることを確認します。

   InterScan 管理コンソールから、[リアルタイムモニタ] をクリックします。[リアルタイムモニタ] 画面が開き、InterScan の動作がリアルタイムで表示されます。「リアルタイム検索の実行開始日時」と表示されれば、InterScan が実行されていることが分かります。58 ページの「リアルタイムモニタの概要」を参照してください。

3. インフォメーションストア全体の手動検索を実行します。

   インストール後、インフォメーションストア全体の手動検索を実行することをお勧めします。InterScan では、ウイルス/不正プログラムまたはその他の不正コードを検出すると、トレンドマイクロの初期設定に従ってこれらに対して処理を実行します。ウイルス/不正プログラムに対する初期設定の処理は「駆除」であり、駆除不能な場合は「隔離」です。

手動検索が完了すると、Exchange 環境の基本的なセキュリティが確立されます。

注意

インストールとアクティベーションが完了すると、InterScan は Exchange サーバの保護を開始します。InterScan はトレンドマイクロの初期設定値を使用し、望ましくないコンテンツのフィルタリング、害を及ぼす可能性のある添付ファイルのブロック、およびウイルス/不正プログラムやその他のセキュリティ上の脅威に関する検索をリアルタイムで実行します。準備が完了したら、ネットワークに対する最適な保護および効果が得られるよう、InterScan の設定をカスタマイズします。

セキュリティの維持

Exchange サーバのセキュリティを維持するには、次のことをお勧めします。

表 3-1. セキュリティの維持

処理	利点
予約アップデートの設定	InterScan を常に最新の状態に保つために、InterScan のコンポーネントを定期的にアップデートします。このアップデートを容易にするため、InterScan では予約アップデートを設定できます。予約アップデートでは、設定したスケジュールに従ってトレンドマイクロのアクティブアップデートサーバをチェックし、利用可能なコンポーネントを自動的にダウンロードします。
予約検索	ウイルス/不正プログラムおよびその他のセキュリティ上の脅威は、保護されていないローカルなコンピュータやサーバなどの予期しない感染元から、または非常に緩い設定をすり抜けて、Exchange サーバを攻撃します。このようなリスクを大幅に削減するには、定期的に予約検索を実行します。
マスメーリング型ウイルスに対する処理を有効にする	[セキュリティリスク検索] 画面で [マスメーリング型ウイルスに対する処理を有効にする] を選択し、早期にウイルス大規模感染を警告します。
アウトブレークアラート	攻撃が発生した場合、その拡大を防ぐため、管理者が早期に通知を受信することは極めて重要です。ネットワークで大規模感染の危険がある場合に主要なネットワークセキュリティ担当者に警告を送信するよう、InterScan を設定することをお勧めします。アウトブレークアラートを使用して、指定したユーザに自動的に通知するよう InterScan を設定できます。

処理	利点
全体的なセキュリティについて検討する	InterScan for Microsoft Exchange は、Exchange メールサーバを保護するように設計されています。InterScan では、Exchange 以外のメールサーバ、ファイルサーバ、デスクトップ、またはゲートウェイデバイスに対する保護は行いません。ファイルサーバおよびデスクトップを保護する Trend Micro Apex One™や、ネットワークの周辺を保護する Trend Micro InterScan VirusWall™、InterScan™ Messaging Security Suite などその他のトレンドマイクロ製品と共に使用すると、InterScan による保護が強化されます。 ネットワークセキュリティのニーズすべてに対応するソリューションのより包括的なリストについては、トレンドマイクロの Web サイトを参照してください。 https://www.trendmicro.com/ja_jp/business.html
InterScan フォルダを検索対象から除外する	ファイルベースのウイルス対策ソフトウェアでは、通常、検索対象から除外するフォルダを設定することができます。InterScan を別のウイルス対策ソフトウェアと併用する場合は、次のフォルダを検索対象から除外するよう設定することをお勧めします。 • `Isme¥storage` • `Isme¥temp` • `Isme¥Debug` 注意 これらのフォルダ名は、インストール時に InterScan が初期設定で使用する名前です。

大規模感染状況の管理

ウイルス/不正プログラム、トロイの木馬、ワーム、またはその他のスパイウェア/グレーウェアが、突然ネットワーク上の多くの Exchange サーバやパーソナルコンピュータを攻撃すると、大規模感染が発生します。セキュリティパッチなどの最新コンポーネントが適用されていないソフトウェア、設定が不十分なウイルス対策ソフトウェア、または、新たに発生してまだパターンファイルのない不正プログラムなど、攻撃が発生する理由はいろいろありま

す。大規模感染時には、組織内の広範囲に分散したグループとの通信が混乱し、対応に時間がかかります。

大規模感染が発生したときに管理者が実行する処理は、4 つの一般的な段階に分けることができます。

1. そのセキュリティイベントが確かな問題であり、誤った警告ではないことの確認
2. セキュリティイベントへの対応
3. セキュリティイベントの分析
4. Exchange サーバおよびメールボックスの回復

InterScan には、大規模感染の各段階で管理者を支援するいくつかの便利な機能があります。大規模感染の脅威が発生した場合、次の機能を検討してください。

1. セキュリティイベントが本当に不正プログラムの大規模感染であることを確認するには、次の手順に従ってください。
   - トレンドマイクロの Web サイトで、ウイルス/不正プログラムの警告と最新のセキュリティ情報を確認します。

     https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/
   - InterScan 通知を確認します。InterScan は、大規模感染の状況が発生すると、自動的に警告を送信するように設定できます。さらに、InterScan は、検出された脅威に対して処理を実行する際に、管理者またはその他の指定したユーザに通知するよう設定できます。
   - セキュリティイベントを素早く分析するには、[概要] 画面を表示するか、手動レポートを作成します。セキュリティイベントの詳細については、InterScan のログのクエリを実行します。
2. 対応
   - コンポーネントの手動アップデートを実行して、すぐに最新の InterScan コンポーネントをダウンロードします。
   - アップデートに続き、インフォメーションストア全体の手動検索を実行します。トレンドマイクロの推奨設定やトレンドマイクロの推奨処理などのトレンドマイクロが推奨する初期設定を使用するか、さらに具体的な検索フィルタを設定します。検索対象が正確に分か

っている場合には、[セキュリティリスク検索] 画面で [指定のファイル] を選択し、InterScan で検出するファイル名を入力します。

3. 分析

   - ログクエリを実行し、攻撃についての情報を取得します。ログには、日時、送信者と受信者、感染した添付ファイルの名前などの有益な情報が含まれています。
   - セキュリティ問題の分析に関するサポートが必要な場合には、トレンドマイクロのテクニカルサポートにお問い合わせください。本ドキュメントの「製品サポート情報」を参照してください。

4. 復旧

   - Exchange 環境を復旧したら、設定とセキュリティポリシーの変更を検討します。次の点について考慮してください。
     - 処理を実行する前にファイルをバックアップするよう InterScan を設定します。これにより、回復不可能な処理を実行することを防ぎます。
     - リアルタイムモニタを使用したり、ログやレポートを生成することにより、結果を監視します。
     - サーバ管理ツールを使用し、テスト済みの安全な InterScan サーバから別のサーバへ、迅速かつ簡単に構成を複製できます。

第 4 章

InterScan の管理

この章では、InterScan for Microsoft Exchange (以下、InterScan) の製品コンソールの開き方、使用方法、および InterScan サーバの管理方法について説明します。

内容は次のとおりです。

リアルタイムモニタの概要

リアルタイムモニタには、1 台の Exchange サーバの情報がリアルタイムに表示されます。管理者は、InterScan の検索メッセージや、サーバで検出されたセキュリティリスクの現在の数を確認することができます。

リアルタイムモニタを使用して、ローカルサーバまたはネットワークに接続されている任意のサーバを監視できます。そのため、管理者は複数の InterScan サーバを集中管理できます。

注意

詳細は、Exchange のバージョン、サーバの役割、およびライセンスのバージョンによって異なります。

オプションの説明を以下に示します。

- 件数のリセット — [検索ステータス] のすべてのカウントと検索済みメッセージ数を 0 にリセットし、[検索済みメッセージ] の情報をクリアします。
- 情報のクリア — [検索済みメッセージ] の情報をクリアします。
- 閉じる — 画面を閉じます。

リモートサーバでのリアルタイムモニタの表示

手順

1. 製品コンソールを使用して、リモートサーバにアクセスします。
2. バナー内の [リアルタイムモニタ] をクリックします。

   [リアルタイムモニタ] 画面が開き、リモートサーバの情報が表示されます。

サーバ管理コンソールの概要

InterScan サーバ管理コンソールを使用すると、ネットワーク上のすべての InterScan サーバを表示できます。ここには、同じタイプのアクティベーショ

ンコードを持つサーバのみが表示されます。InterScan を Exchange 2019、2016、または 2013 にインストールすると、フォレスト内のすべての InterScan サーバを表示できます。

サーバ管理のアクティベーション

サーバ管理コンソールにはリモートサーバの状態も表示されるため、設定をリモートサーバにコピーすることができます。InterScan のインストールプロセスでサーバ管理のアクティベーションを行っていない場合、サーバ管理コンソールを使用するには、まずサーバ管理のアクティベーションを実行する必要があります。

手順

1. ローカル管理者権限を持つアカウントで InterScan サーバにログオンします。
2. 製品コンソールの上部にある [サーバ管理] リンクをクリックします。
3. Active Directory の既存のグループを指定し、アクティベーションウィザード画面の指示に従って、サーバ管理のアクティベーションに必要な処理を実行します

サーバ管理コンソールの使用

サーバ管理コンソールでは、以下の機能を使用することができます。

表 4-1. サーバ管理コンソールの機能

機能	説明
パターンファイルおよびエンジンのバージョンの表示	スマートスキャンエージェントパターンファイル、ウイルスパターンファイル、高度な脅威相関パターンファイル、スパイウェアパターンファイル、ウイルス検索エンジン、CI クエリハンドラ、高度な脅威検索エンジン、スパムメール対策パターンファイル、スパムメール検索エンジン、IntelliTrap パターンファイル、IntelliTrap 除外パターンファイル、URL フィルタエンジンに関する情報を表示します。
検索結果の表示	リモート InterScan サーバに対して検索されたメッセージの合計数、および検索結果を表示します。検索結果には、次の検出数も表示されます。

機能	説明
	• セキュリティリスク • 駆除不能なウイルス/不正プログラム • 高度な脅威 • ブロックされた添付ファイル • スパムメール • 高度なスパムメール • 情報漏えい対策 • コンテンツ違反 • 不審 URL • 書き換えられた URL • 検索されたメッセージ • 検索不能なメッセージ部分
検索ステータスの表示	検索の種類が有効になっているのか無効になっているのかを示します。 リモート InterScan サーバに対する次の種類の検索のステータスが表示されます。 • ストアセキュリティリスク検索 • トランスポートセキュリティリスク検索 • ストア添付ファイルブロック • トランスポート添付ファイルブロック • ストアコンテンツフィルタ • トランスポートコンテンツフィルタ • スパムメール対策 • 高度なスパムメール対策 • 情報漏えい対策 • Web レピュテーション • Time-of-Click プロテクション • 仮想アナライザ
前回の複製の表示	前回の複製のサーバ名、ステータス、および期間を表示します。
リモートサーバへの設定の複製	設定を、リスト内の単一または複数のリモートサーバに複製します。複製する設定として、[すべての設定] または [サーバに依存する設定 (隔離ディレクトリやバックアップディレクトリなど) を上書きする] を選択するか、[指定の設定] で次の設定を選択できます。

機能	説明
	• セキュリティリスク検索 • 添付ファイルブロック • コンテンツフィルタ • スパムメール対策 • 高度なスパムメール対策 • Web レピュテーション • Time-of-Click プロテクション • 情報漏えい対策 • 情報漏えい対策テンプレート • 手動検索 • 予約検索 • Smart Protection • 仮想アナライザ • アップデート • 警告 • レポート • ログ • 特定グループ • サーバグループ • 内部ドメイン • 製品ライセンス • 管理 (プロキシ、受信メッセージディスクレーマー、通知設定、リアルタイム検索設定、アクセス管理、Apex Central)
Trend Micro Smart Protection のステータスの表示	サーバ名、検索サービス、検索設定、Trend Micro Smart Protection ソース、およびサーバステータスを含む、スマートスキャンサーバに関する情報を表示します。

製品コンソールの起動

InterScan 製品コンソールでは、一度に 1 台ずつサーバを管理できます。

注意

ローカル管理者権限を持つアカウントまたは InterScan 管理グループに属するアカウントを使用します。Active Directory グループ、またはサーバ管理のアクティベーションで使用した Exchange フォレストに含まれる任意の Active Directory グループに属するアカウントを使用できます。

手順

- ローカルサーバの場合:

a. [スタート] > [すべてのプログラム] > [Trend Micro InterScan for Microsoft Exchange] > [InterScan 管理コンソール] の順にクリックします。

注意

Windows 2012 プラットフォームでは、デスクトップショートカットのみを使用できます。

b. ユーザ名とパスワードを入力します。

c. [ログオン] をクリックします。

- リモートサーバの場合:

  フレームをサポートしている Web ブラウザを使用して、次の URL にアクセスします。

  `https://<サーバ名>:<ポート番号>/smex`

  説明:

  - サーバ名は、InterScan をインストールしたサーバの名前です。
  - ポート番号は、そのコンピュータにアクセスするために使用するポート番号です。

注意

初期設定では、HTTPS にはポート 16373 が使用されます。

サーバ管理を使用した設定の複製

サーバ管理を使用すると、異なる InterScan サーバ間で、任意の設定またはすべての設定を複製できます。この方法によるサーバの複製は、個別にサーバを設定するよりも非常に速く簡単にできます。また、同様の保護を行うすべての InterScan サーバ内で、同じ設定を共有できます。

手順

1. [サーバ管理] をクリックして、[サーバ管理] 画面を開きます。

2. 複製先のサーバを選択します。
3. [複製] をクリックします。

   [複製の設定] 画面が表示されます。
4. 複製する設定を選択します。
   - 複製先のサーバにすべての構成を複製する場合は、[すべての設定] をクリックします。
   - 各構成を個別に複製する場合は、[指定した設定] をクリックします。

注意

現在ログオンしているサーバが、複製元となります。

5. サーバに依存する設定を上書きする場合は、[サーバに依存する設定 (隔離ディレクトリやバックアップディレクトリ) を上書きする] チェックボックスをオンにします。このチェックボックスをオンにすると、隔離フォルダやバックアップフォルダなどに対して設定したディレクトリパスをコピーできます。
6. [配信] をクリックします。

   進行状況バー、および複製の進捗状況を示す画面が表示されます。

サービスの開始と停止

手動ロールバックなどの操作を行うためには、InterScan のサービスを開始または停止することが必要になる場合があります。サービスの開始と停止は、Windows の [サービス] コンソールで実行できます。

InterScan をインストールすると、次のサービスが追加されます。

- InterScan for Microsoft Exchange Master Services: InterScan のメインサービスです。
- InterScan for Exchange Remote Configuration Server: リモート設定用です。

注意

エッジトランスポートサーバの役割を持つ Microsoft Exchange Server 2019、2016、2013 で InterScan を使用する場合、このサービスは追加されません。

- InterScan for Microsoft Exchange System Watcher: システムイベントのログを監視します。
- InterScan EUQ Monitor: このサービスは、インストール時に [エンドユーザメール隔離] が選択された場合に追加されます。

InterScan のアイコンについて

次の表では、InterScan のアイコンを説明しています。

表 4-2. InterScan のアイコン

アイコン	説明
 ヘルプ	クリックすると InterScan のヘルプが表示されます。
 有効	クリックするとルールまたはポリシーが無効になります。このアイコンが表示されているときは、そのルールまたはポリシーが有効になっています。
 無効	クリックするとルールまたはポリシーが有効になります。このアイコンが表示されているときは、そのルールまたはポリシーが無効になっています。
 表示更新	クリックすると画面上の情報が更新されます。
 警告	警告ステータスを示します。
 有効	有効ステータスを示します。
 無効	無効ステータスを示します。
 削除	クリックするとテンプレートが削除されます。

アイコン	説明
 ツールチップ	このアイコンをポイントすると機能に関するヘルプ情報が表示されます。
 詳細の表示	クリックするとドロップダウンが展開されます。
 詳細非表示	クリックするとドロップダウンが閉じられます。

パート II

検索と検索フィルタの設定

第 5 章

Smart Protection の概要

この章では、Trend Micro Smart Protection ソリューションについて説明するとともに、このソリューションを使用するために必要な環境の設定方法についても説明します。

内容は次のとおりです。

Trend Micro Smart Protection について

Trend Micro Smart Protection は、顧客をセキュリティリスクや Web の脅威から保護する目的で設計された、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。クラウド上に統合されたメールレピュテーション、Web レピュテーション、およびファイルレピュテーションの各テクノロジおよび脅威データベースに軽量のエージェントを使用してアクセスすることで、ローカルソリューションとホステッドソリューションの両方を活用し、社内ネットワーク、自宅、外出先を問わず、ユーザを保護します。ネットワークにアクセスする製品、サービス、ユーザが増えるにつれて顧客への保護機能は自動的に更新および強化され、リアルタイムな相互監視保護システムが構築されていきます。

インターネットクラウドで提供されているレピュテーションテクノロジ、検索テクノロジ、および相関分析テクノロジを組み込むことで、Trend Micro Smart Protection ソリューションは、パターンファイルのダウンロードに依存していた従来の負担を軽減し、デスクトップのアップデートに伴う一般的な延期を解消します。

新規ソリューションの必要性

従来のファイルベースの脅威処理方法では、エンドポイントの保護に必要なパターン (定義) のほとんどが定期的に配信されます。パターンファイルは、トレンドマイクロからエージェントにバッチで配信されます。エージェントのウイルス/不正プログラム予防ソフトウェアが新しいアップデートを受信すると、新しいウイルス/不正プログラムのリスクに対する一連のパターン定義がメモリに再ロードされます。新しいウイルス/不正プログラムのリスクが発生した場合には、保護を継続するために、このパターンファイルをもう一度部分的または全体的にアップデートして、エージェントに再ロードする必要があります。

長い間に、出現する脅威の絶対数は大幅に増加してきました。脅威の量の増加は、近年、指数級数的な伸びを示しています。この増加のペースは今日の既知のセキュリティリスクの量を大きく上回り、今後は、このセキュリティリスクの量が新種のセキュリティリスクになると予想されます。セキュリティリスクの量は、サーバやワークステーションのパフォーマンス、ネットワーク帯域幅の使用率、また一般に、適切な保護を提供するまでの全体的な時間や「保護にかかる時間」に影響する可能性があります。

ユーザがウイルス/不正プログラムの量の脅威にも対抗できることを目指した新しい手法がトレンドマイクロによって開拓されています。この先駆的な技術で使用されるテクノロジとアーキテクチャには、ウイルス/不正プログラムのシグネチャやパターンファイルの保存をクラウドに移行するテクノロジが採用されています。ウイルス/不正プログラムのシグネチャの保存をクラウドに移行することにより、将来出現する量のセキュリティリスクからユーザをより強固に保護できます。

Trend Micro Smart Protection サービス

Trend Micro Smart Protection 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。

Trend Micro Smart Protection サービスの内容は次のとおりです。

- ファイルレピュテーションサービス:ファイルレピュテーションサービスは、これまでエージェントコンピュータ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を Trend Micro Smart Protection ソースに移行します。

  詳細については、71 ページの「ファイルレピュテーションサービス」を参照してください。

- Web レピュテーションサービス:Web レピュテーションサービスは、これまでトレンドマイクロのみでホストされていた URL レピュテーションデータの、ローカル Trend Micro Smart Protection ソースでのホストを可能にします。両方のテクノロジにより、パターンファイルのアップデートや URL の妥当性の確認で消費される帯域幅を減らすことができます。

  詳細については、72 ページの「Web レピュテーションサービス」を参照してください。

ファイルレピュテーションサービス

ファイルレピュテーションサービスは、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、すべてのユーザがそれを使用できます。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-エージェント型のアーキ

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、エージェントの全般的なフットプリントを大幅に削減します。

ファイルレピュテーションサービスを使用するには、InterScan をスマートスキャンモードにする必要があります。

Web レピュテーションサービス

世界最大規模のドメインレピュテーションデータベースであるトレンドマイクロの 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。Web レピュテーション機能により、ユーザがアクセスするページが安全で、ユーザの個人情報を引き出すよう設計された不正プログラム、スパイウェア、およびフィッシング詐欺などの Web の脅威が存在しないことを確認できます。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。

Web レピュテーション機能を有効にすることで、ユーザが不正 URL にアクセスすることを阻止できます。本文や添付ファイルに URL を含むメールを受信すると、Web レピュテーションは、そのレピュテーションレーティングについて、割り当てられている Web レピュテーションサーバを照会します。Web レピュテーションでは、設定に応じて、URL を含むメールを隔離または削除したり、対象メールにタグを付加することができます。

ヒント

ネットワーク帯域幅を節約するために、[内部ドメインの URL を放置する] の設定は初期設定のままにして、社内 Web サイトを検索対象から除外することをお勧めします。

Trend Micro Smart Protection ソース

トレンドマイクロは、ファイルレピュテーションサービスと Web レピュテーションサービスを InterScan および Trend Micro Smart Protection ソースに配信します。

Trend Micro Smart Protection ソースは、ウイルス/不正プログラムパターン定義の大部分をホストすることによってファイルレピュテーションサービスを提供します。Apex One エージェントは、それ以外の定義をホストします。自身のパターン定義でファイルの危険性を判定できない場合には、エージェントから Trend Micro Smart Protection ソースに検索クエリが送信されます。Trend Micro Smart Protection ソースは、識別情報を使用してリスクを判定します。

Trend Micro Smart Protection ソースは、これまでトレンドマイクロがホストするサーバを介してのみ利用可能であった Web レピュテーションデータをホストすることによって、Web レピュテーションサービスを提供します。エージェントから Trend Micro Smart Protection ソースに Web レピュテーションクエリが送信され、ユーザがアクセスしようとしている Web サイトの評価が確認されます。エージェントは、Web サイトのレピュテーションを、エンドポイントに適用される特定の Web レピュテーションポリシーに関連付けて、対象サイトへのアクセスを許可するかブロックするかを判定します。

Trend Micro Smart Protection Network

Trend Micro Smart Protection Network は、顧客をセキュリティリスクや Web の脅威から保護する目的で設計された、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基盤です。オンプレミスのソリューションとトレンドマイクロのホステッドソリューションの両方の機能を強化して、企業ネットワーク内、自宅、または外出先などどこでもユーザを保護します。Smart Protection Network は、軽量エージェントを使用して、 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、および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、それだけ顧客の保護機能が自動的に更新および強化され、ユーザにとってのリアルタイムのネイバーフッドウォッチ (近隣監視活動) 保護サービスが形成されます。

Trend Micro Smart Protection Network 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

Trend Micro Smart Protection Server

Trend Micro Smart Protection Server は、ファイルレピュテーションのウイルス/不正プログラムの脅威、および確認済みの Web レピュテーションの脅威のリポジトリを格納します。Trend Micro Smart Protection Server を実装することで、帯域幅の使用量を抑制し、企業に高度なプライバシーを提供します。Trend Micro Smart Protection Server は、ローカルのレピュテーションデータに照らしてすべてのクエリを検証します。

Trend Micro Smart Protection Server には次の 2 つの種類があります。

- 統合 Trend Micro Smart Protection Server: 統合 Trend Micro Smart Protection Server は、他のトレンドマイクロ製品と共にインストールされます。InterScan ではこれらの既存のサーバリソースが活用されるため、リソースが追加で消費されることはありません。
- スタンドアロン Trend Micro Smart Protection Server: スタンドアロン Trend Micro Smart Protection Server は VMware または Hyper-V サーバにインストールされます。スタンドアロンサーバには専用の管理コンソールがあり、InterScan Web コンソールでは管理されません。

Trend Micro Smart Protection ソースの比較

次の表に、Trend Micro Smart Protection Network と Smart Protection Server の相違点を示します。

表 5-1. Trend Micro Smart Protection ソースの比較

比較基準	Smart Protection Server	Trend Micro Smart Protection Network
使用可否	内部エージェント、つまり Web コンソールで指定した位置の条件に一致するエージェントで使用可能。	主に外部エージェント、つまり Web コンソールで指定した位置の条件に一致しないエージェントで使用可能。

比較基準	SMART PROTECTION SERVER	TREND MICRO SMART PROTECTION NETWORK
目的	効率性を最適化するために、Trend Micro Smart Protection サービスを企業ネットワーク内に配置するよう設計されている。	企業ネットワークに直接アクセスできないエージェントに Trend Micro Smart Protection 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。
管理	InterScan 管理者がこれらの Trend Micro Smart Protection ソースをインストールおよび管理する。	トレンドマイクロがこのソースを管理する。
パターンアップデート元	トレンドマイクロのアップデートサーバ	トレンドマイクロのアップデートサーバ
エージェント接続プロトコル	HTTP および HTTPS	HTTPS

Trend Micro Smart Protection パターンファイル

ファイルレピュテーションサービスおよび Web レピュテーションサービスは、Trend Micro Smart Protection パターンファイルを使用します。このパターンファイルは、トレンドマイクロのアクティブアップデートサーバからリリースされます。

表 5-2. Trend Micro Smart Protection パターンファイル

パターンファイル	説明
スマートスキャンエージェントパターンファイル	InterScan はスマートスキャンエージェントパターンファイルにアップデートを毎日ダウンロードします。 InterScan がスマートスキャンモードの場合、セキュリティリスク検索ではスマートスキャンエージェントパターンファイルが使用されます。このパターンでファイルのリスクを判別できない場合、InterScan はスマートスキャンパターンと呼ばれる別のパターンを利用します。

パターンファイル	説明
スマートスキャンパターン	Trend Micro Smart Protection ソースは、スマートスキャンパターンにアップデートを毎時間ダウンロードします。InterScan は、検索クエリを Trend Micro Smart Protection ソースに送信することによって、スマートスキャンパターンに照らして潜在的な脅威を確認します。
Web ブロックリスト	Trend Micro Smart Protection ソースは Web ブロックリストをダウンロードします。InterScan は、Web レピュテーションクエリを Trend Micro Smart Protection ソースに送信することによって、Web ブロックリストに照らして Web サイトのレピュテーションを確認します。InterScan は Trend Micro Smart Protection ソースから受信したレピュテーションデータを、そのコンピュータに適用されている Web レピュテーションポリシーと関連付けます。InterScan は、ポリシーに基づいてサイトへのアクセスを許可またはブロックします。

ローカルソースの設定

セキュリティリスク検索でスマートスキャンを使用するには、ローカルソースを設定します。

手順

1. メインメニューで [Smart Protection] > [ローカルソース] をクリックします。

   [ローカルソース] 画面が表示されます。

2. [追加] をクリックします。

   [Smart Protection Server の追加] 画面が表示されます。

3. 追加するサーバの [サーバの名前またはアドレス] を入力します。

4. [ファイルレピュテーションサービスのポート] を選択し、ファイルレピュテーションサービスを提供する Trend Micro Smart Protection Server のポート番号を入力します。[Web レピュテーションサービスのポート] を選択し、Web レピュテーションサービスを提供する Trend Micro Smart Protection Server のポート番号を入力します。

ヒント

Trend Micro Smart Protection Server のポート番号を確認するには、サーバの Web コンソールを開き、[レピュテーションサービスの概要] 画面を表示します。

5. ファイルレピュテーションサービスを提供する Trend Micro Smart Protection Server の場合、必要に応じて、SSL (Secure Sockets Layer) プロトコルを有効にします。
6. 該当する [接続テスト] ボタンをクリックして、サーバに正常に接続されていることを確認します。
7. [追加] をクリックします。

   Trend Micro Smart Protection Server リストの一番下に Trend Micro Smart Protection Server が表示されます。
8. [参照順序] を指定します。
   - 表示順 — サーバに対するクエリを優先度順に実行します。

     上矢印または下矢印をクリックして、Trend Micro Smart Protection Server の優先度を指定します。このリストの優先度に基づいて Trend Micro Smart Protection Server にクエリが送信されます。
   - ランダム — サーバに対するクエリをランダムに実行します。
9. Trend Micro Smart Protection Server との通信にプロキシが必要な場合は、[プロキシ設定] をクリックしてプロキシを設定します。
10. [保存] をクリックします。

検索サービス設定

検索サービス設定 ([Smart Protection] > [検索サービス設定]) の説明を以下に示します。

表 5-3. 検索サービス設定

検索の種類	オプション
セキュリティリスク検索	• 従来型スキャン —以前のバージョンの InterScan で使用されていた検索方法を選択します。セキュリティリスク検索に使用されるすべてのコンポーネントがローカルの InterScan サーバに格納されます。 • スマートスキャン - ファイルレピュテーションサービス —次世代のクラウド型の保護ソリューションを選択します。このソリューションの中核をなすのは、クラウドに格納された脅威のシグニチャを利用する高度な検索アーキテクチャです。Trend Micro Smart Protection Server をネットワークにインストールすれば、検索効率をさらに高めることができます。
Smart Protection ソースの設定	• Trend Micro Smart Protection Network —すべての Web レピュテーションクエリをトレンドマイクロのサーバに送信して確認します。 • Trend Micro Smart Protection Server —すべての Web レピュテーションクエリをローカルで確認します。ローカルサーバでクエリを確認できない場合は、トレンドマイクロのサーバにクエリが送信されて詳細に分析されます。

第 6 章

検索の設定

この章では、Exchange 環境を保護するためのリアルタイム検索、手動検索、予約検索を設定する方法について説明します。

内容は次のとおりです。

検索について

InterScan は、リアルタイム検索、手動検索、および予約検索という 3 種類の検索をサポートしています。Exchange 環境を保護するために、InterScan はメッセージとその添付ファイルを検索して、セキュリティリスクや望ましくないデータが含まれていないか確認します。InterScan によってこれらが検出されると、設定された処理が検出された項目に対して自動的に実行されます。

InterScan 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、対象のメッセージやファイルでセキュリティリスクや望ましくないデータを検出したときに実行する処理を指定したりできます。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 InterScan を設定することもできます。

バックアップフォルダにファイルをバックアップしてから、そのファイルに対する処理を実行するように InterScan 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。

注意

トレンドマイクロでは、元のファイルに対する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。ファイルが破損または使用できなくなった場合、今後の分析のためにトレンドマイクロにそのファイルを送信してください。

InterScan 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。

初期設定では、InterScan は Exchange 環境の検索可能なすべての送信/受信メッセージと保管メッセージを検索します。検索可能なファイルは、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、およびユーザが定義した検索制限の範囲外のファイルを除くすべてのファイルです。すべてのファイルを検索すると、最大限のセキュリティが確保されます。その反面、すべてのメッセージを検索すると、多大な時間とリソースが消費されるため、状況

によっては無駄な場合があります。そのような場合は、InterScan で検索するファイルを制限します。

リアルタイム検索

以下のデータがリアルタイムで検索されます。

- 受信または送信するすべてのメール
- インターネットから Exchange に送信されてくる SMTP メッセージ
- パブリックフォルダへの投稿
- サーバ間のすべての複製

手動検索

InterScan では、手動検索を実行することで、保護されていないメールサーバや不適切な構成などの予期しないソースからの感染の可能性を最小限に抑えることができます。クラスタの場合、InterScan では 1 つのノード上の各仮想サーバを検索できます。

注意

複数のストレージグループが存在する場合は、複製データベースの検索を無効にすることをお勧めします。[手動検索] に移動し、検索対象として選択されたデータベースを変更します。

手動検索では、セキュリティリスク検索、添付ファイルブロック、コンテンツフィルタ、および情報漏えい対策を実行できます。これらのフィルタは、リアルタイム検索で使用されるフィルタと似ていますが、一部の処理は手動検索や予約検索では実行できません。

手動検索の実行中は、新しい手動検索プロセスを開始することはできません。また、アップデートによって手動検索が中断されることはありません。ただし、予約検索の実行中は、手動検索を開始すると予約検索が停止します。予約検索は、スケジュールに従って再開されます。

予約検索

予約検索は指定した日時に自動的に実行され、設定した経過時間後に一時停止します。完了する前に検索が一時停止した場合は、次回の指定日時に検索

が再開されます。予約検索を使用すると、定期的な検索を自動化して、検索の管理を効率化できます。

すでに進行中の予約検索は、別の予約検索を開始しても中断されません。予約検索がアップデートによって中断されることもありません。

予約検索リスト

オプションの説明を以下に示します。

- 追加 ─リストに新しい予約検索を追加します。
- 削除 ─リストから選択した予約検索タスクを削除します。
- すべてのスケジュールを停止 ─ 現在検索が実行中か、キューに入っているかにかかわらず、すべての予約検索を停止します。
- 有効 ─ 予約検索を有効または無効にします。

クラスタ環境での手動検索および予約検索について

ノードベースでの検索

手動検索および予約検索はノードベースで実行します。つまり、手動検索または予約検索は 1 つのノードで同時に 1 つしか実行できません。

フェイルオーバー時またはリアルタイム検索の変更後の検索

クラスタでフェイルオーバーが実行されている間に、インフォメーションストアのデータベースはアンマウントされ別のノードにマウントされます。フェイルオーバー後、手動または予約検索のタスクは停止されます。また、同じノード上でリアルタイム検索のステータスが変更された場合も、ウイルス検索、添付ファイルブロック、あるいはコンテンツフィルタを有効/無効に変更することにより、手動または予約検索のタスクが停止されます。

手動検索と予約検索の設定

オプションの説明を以下に示します。

表 6-1. 手動検索と予約検索の設定

セクション	設定
予約 注意 予約検索にしか使用できません。	検索頻度: • 毎日 –検索を毎日特定の時刻に実行します。 検索の一時停止 – • [01]〜[23] 時間の中から、検索を一時停止させるまでの経過時間を選択します。InterScan は次回の指定時刻に現在の検索を再開します。 • 検索を一時停止せず、完了するまで実行し続ける場合は、[00] 時間を選択します。 • 毎週 –検索を毎週特定の曜日の特定の時刻に実行します。 • 毎月 –検索を毎月特定の日時に実行します。
データベースの選択	• すべてのデータベース –このオプションの指定後に追加したデータベースも含めて、すべてのデータベースを検索します。 • 指定のデータベース –指定したデータベースを検索します。 • 表示更新 –最新のメールボックスデータベースを表示します。
フォルダ選択	• すべてのフォルダ –すべてのフォルダを検索する場合に選択します。 • 指定したフォルダ –指定したデータベースを検索します。 • パブリックフォルダ検索を有効にする –パブリックフォルダを検索する場合に選択します。

セクション	設定
検索の種類の選択	• セキュリティリスク検索 —設定に基づいて、ウイルスまたは不正プログラムと高度な脅威を検索します。 • 添付ファイルブロック —添付ファイルブロックの設定に基づいて検索を実行します。 • コンテンツフィルタ —コンテンツフィルタの設定に基づいて検索を実行します。 • 情報漏えい対策 —情報漏えい対策の設定に基づいて検索を実行します。
差分検索オプション —複数のチェックボックスをオンにすると、それらのチェックボックス間に「AND」の関係が作成されます。	注意 すべてのチェックボックスをオフにすると、指定したデータベース内のすべてのメッセージが検索されます。 • 次の期間に配信されたメッセージを検索 —特定の期間に配信されたメッセージを検索します。 • 添付ファイルを含むメッセージを検索 —ファイルが添付されているメッセージのみを検索します。 • 検索されていないメッセージを検索 —InterScan でまだ検索されていないメッセージのみを検索します。
CPU 使用率 —この機能を使用すると、手動検索と予約検索で使用するリソースを制限することによりパフォーマンスを管理できます。	• CPU 使用率の制限を有効にする —CPU 使用率を制限して、使用される最大 CPU 使用率を指定します。

圧縮ファイルの処理

圧縮ファイルには、特殊なセキュリティ上の懸念が数多くあります。圧縮ファイルは、パスワードによって保護されたり、暗号化されている場合があります。また、「Zip of Death」と呼ばれるセキュリティリスクを含んでいたり、何層にも圧縮されている場合があります。

圧縮形式

InterScan のウイルス検索エンジンは、次に示す代表的な圧縮形式で圧縮されたファイルを抽出して検索できます。InterScan は、何重にも圧縮されたファイル内に「隠された」ウイルス/不正プログラムを検出することもできます。たとえば、感染ファイルが ZIP で圧縮されて、さらに ARJ で圧縮され、MS で圧縮され、再び ZIP で圧縮された場合でも検出できます。

再帰的検索の最大階層数は 20 です。この制限値は、[セキュリティリスク検索] > [対象] > [検索の制限条件] で設定できます。

表 6-2. サポートされている圧縮形式

- LZH アーカイブ (`.lzh`)
- ZIP アーカイブ (`.zip`)
- RAR アーカイブ (`.rar`)
- TAR アーカイブ (`.tar`)
- ARJ アーカイブ (`.arj`)
- BINHEX (`.hqx`)
- GNU Zip (`.gz`; `.gzip`)
- LZW/圧縮 16 ビット (`.Z`)
- MacBinary (`.bin`)
- Microsoft Cabinet (`.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 (`.u`)
- WinAce (`.ace`)

すべての圧縮添付ファイルをブロック

クライアントに送信される圧縮されたファイルをすべてブロックするように InterScan を設定することを検討してください。InterScan が添付ファイルをブロックしたことを、メールクライアント経由でユーザに通知できます。

手順

1. [添付ファイルブロック] の [対象]タブに移動します。
   - 手動検索または予約検索の場合:

     [検索の種類] > [添付ファイルブロック] > [対象]
   - リアルタイム検索の場合:

     [添付ファイルブロック] > [グローバルポリシー] > [対象]

2. [指定の添付ファイル] をクリックし、次に [添付ファイルの種類] をクリックして、カテゴリを展開します。
3. [圧縮ファイル] をクリックします。
4. [処理] をクリックして処理を選択します。
5. [通知] をクリックして通知方法を選択します。

セキュリティリスク検索時の圧縮ファイルの制限

以下の表に、InterScan で指定できる圧縮ファイルの制限を示します。

表 6-3. セキュリティリスク検索時の圧縮ファイルの制限

設定	説明
解凍ファイルの数が次を超える場合	InterScan で検索する解凍されたファイル数の上限を入力します。圧縮ファイル内の解凍対象ファイル数がこの数値を超える場合は、このオプションで設定した数のファイルのみが検索されます。
解凍ファイルのサイズが次を超える場合	最大サイズを MB 単位で入力します。解凍後のサイズが指定した値以下になる圧縮ファイルだけが検索されます。
圧縮階層の数が次を超える場合	1〜20 の数値を入力します。圧縮階層の数が指定した数値以下の圧縮ファイルだけが検索されます。たとえば、圧縮階層の制限を 5 に設定した場合、5 階層までの圧縮ファイルは検索されますが、6 階層以上に圧縮されたファイルは検索されません。
解凍ファイルのサイズが圧縮ファイルのサイズの「x」倍以上である場合	圧縮ファイルのサイズに対する解凍されたファイルのサイズの割合がこの数値以下の場合のみ、InterScan によって圧縮ファイルが検索されます。 この機能により、InterScan は DoS (Denial-of-Service) 攻撃の原因となり得る圧縮ファイルの検索を回避します。DoS (Denial-of-Service) 攻撃は、不要なタスクによりメールサーバのリソースに負担をかけることで実行されます。解凍されると非常に大きなサイズになるファイルを InterScan が検索しないようにすることで、この問題の発生を回避できます。

InterScan の処理について

InterScan の検索でウイルス/不正プログラム、不審 URL、または望ましくないコンテンツが検出された場合の処理を次に示します。

注意

検索の種類によって実行できる処理が異なります。それぞれの検索で実行できる処理の詳細については、検索の設定、または 89 ページの「検索設定による検出時の処理」を参照してください。

表 6-4. InterScan の処理

処理	説明
駆除	感染したメッセージ本文と添付ファイルからウイルスコードを削除します。残りのメールテキスト、感染していないファイル、および駆除済みのファイルが、対象の受信者に配信されます。  ヒント ウイルス/不正プログラムに対しては、初期設定の検出時の処理「駆除」を使用することをお勧めします。 InterScan でファイルを駆除できない場合もあります。このようなファイルを駆除不能ファイルと呼びます。駆除不能ファイルが検出されたときにこのファイルに対して特別な処理を実行するように、InterScan を設定できます。 手動検索または予約検索では、InterScan によってインフォメーションストアがアップデートされ、ファイルは駆除されたファイルに置き換えられます。

処理	説明
テキスト/ファイルで置換	添付ファイル、感染したコンテンツ、不正なコンテンツ、または望ましくないコンテンツを削除して、テキストまたはファイルに置き換えます。メールは対象の受信者に配信されますが、元のコンテンツがコンテンツフィルタルールに違反していたためコンテンツが置き換えられたことが通知されます。  注意 情報漏えい対策およびコンテンツフィルタでは、検出された違反がメールのヘッダまたは件名に含まれている場合、トランスポートレベルの検索ではこの処理は実行されません。
メッセージ全体の隔離	アクセスが制限されたフォルダにメールを移動し、そのメールを Exchange 環境に対するセキュリティリスクとして削除します。このオプションは、手動検索および予約検索では使用できません。
メッセージ部分の隔離	アクセスが制限されたフォルダにメール本文または添付ファイルを移動し、そのメールを Exchange 環境に対するセキュリティリスクとして削除します。 メッセージ部分が、指定したテキスト/ファイルに置き換えられます。  注意 情報漏えい対策およびコンテンツフィルタでは、検出された違反がメールのヘッダまたは件名に含まれている場合、トランスポートレベルの検索ではこの処理は実行されません。
バックアップ	メッセージをバックアップして、配信し、検出内容をログに記録します。  注意 この処理の動作は以前のバージョンの InterScan の「アーカイブ」と同じです。

処理	説明
メッセージ全体の削除	リアルタイム検索中、InterScan によってメール全体が削除されます。
放置	検出内容をログに記録して、メッセージ部分を配信します。
メッセージ全体の放置	検出内容をログに記録して、メッセージ部分を配信します。
メッセージ部分の放置	検出内容をログに記録して、メッセージ部分を配信します。 注意 情報漏えい対策およびコンテンツフィルタでは、優先度の低いポリシーには適用されません。
タグを付加して配信	メールがスパムメールであることを示すためのタグをそのメールの件名に追加して、対象の受信者に配信します。
ユーザのスパムメールフォルダにメッセージを隔離	インフォメーションストアのサーバ側にあるスパムメールフォルダにメールを移動します。
送信者の管理者に転送する	送信者の管理者にメールを転送します。
特定のメールアドレスに転送する	特定のメールアドレスにメールを転送します。

検索設定による検出時の処理

次の表に、それぞれの検索フィルタの種類により利用可能な検出時の処理を示します。

表 6-5. 検索設定による検出時の処理

検索設定	利用可能な処理
セキュリティリスク検索	
• トレンドマイクロの推奨処理	• 通知しない • 通知 • 駆除不能時に通知

検索設定	利用可能な処理
• マスメーリング型ウイルス	• 駆除 • テキスト/ファイルで置換 • メッセージ全体の隔離 注意 手動検索および予約検索では実行できません。 • メッセージ全体の削除 • 放置 • メッセージ部分の隔離
• すべてのセキュリティリスク	• 駆除 • テキスト/ファイルで置換 • メッセージ全体の隔離 注意 手動検索および予約検索では実行できません。 • メッセージ全体の削除 • 放置 • メッセージ部分の隔離
• ウイルス	• 駆除 • テキスト/ファイルで置換 • メッセージ全体の隔離 注意 手動検索および予約検索では実行できません。 • メッセージ全体の削除 • 放置 • メッセージ部分の隔離

検索設定	利用可能な処理
• ワーム/トロイの木馬	• テキスト/ファイルで置換 • メッセージ全体の隔離  注意 手動検索および予約検索では実行できません。 • メッセージ全体の削除 • 放置 • メッセージ部分の隔離
• 高度な脅威	• メッセージ全体の隔離  注意 手動検索および予約検索では実行できません。 • メッセージ全体の削除 • 放置 • テキスト/ファイルで置換  注意 手動検索および予約検索でのみ実行できます。 • メッセージ部分の隔離  注意 手動検索および予約検索でのみ実行できます。

検索設定	利用可能な処理
• パックされたファイル	• テキスト/ファイルで置換 • メッセージ全体の隔離 注意 手動検索および予約検索では実行できません。 • メッセージ全体の削除 • 放置 • メッセージ部分の隔離
• 不正コード	• 駆除 • テキスト/ファイルで置換 • メッセージ全体の隔離 注意 手動検索および予約検索では実行できません。 • メッセージ全体の削除 • 放置 • メッセージ部分の隔離
• スパイウェア/グレーウェア	• テキスト/ファイルで置換 • メッセージ全体の隔離 注意 手動検索および予約検索では実行できません。 • メッセージ全体の削除 • 放置 • メッセージ部分の隔離

検索設定	利用可能な処理
• 駆除できないファイル	• テキスト/ファイルで置換 • メッセージ全体の隔離  注意 手動検索および予約検索では実行できません。 • メッセージ全体の削除 • 放置 • メッセージ部分の隔離
添付ファイルブロック	• 添付ファイルをテキスト/ファイルで置換 • メッセージ全体の隔離  注意 手動検索および予約検索では実行できません。 • メッセージ部分の隔離 • メッセージ全体の削除 • 通知 • 通知しない

検索設定	利用可能な処理
コンテンツフィルタ	• テキスト/ファイルで置換 • メッセージ全体の隔離 注意 手動検索および予約検索では実行できません。 • メッセージ部分の隔離 • メッセージ全体の削除 • バックアップ • メッセージ部分の放置 • メッセージ全体の放置 注意 「すべての条件に一致」したポリシーでのみ実行できます。 • 送信者の管理者に転送する 注意 手動検索および予約検索では実行できません。 • 特定のメールアドレスに転送する 注意 手動検索および予約検索では実行できません。 • 通知 • 通知しない

検索設定	利用可能な処理
情報漏えい対策	• テキスト/ファイルで置換 • メッセージ全体の隔離 注意 手動検索および予約検索では実行できません。 • メッセージ部分の隔離 • メッセージ全体の削除 • バックアップ • メッセージ部分の放置 • 送信者の管理者に転送する 注意 手動検索および予約検索では実行できません。 • 特定のメールアドレスに転送する 注意 手動検索および予約検索では実行できません。 • 通知 • 通知しない
スパムメール対策	
• コンテンツ検索: スパムメール	• ユーザのスパムメールフォルダにメッセージを隔離 • メッセージ全体の削除 • タグを付加して配信 • 放置

検索設定	利用可能な処理
• コンテンツ検索	• メッセージをユーザのスパムメールフォルダに隔離 • メッセージ全体の削除 • タグを付加して配信 • 放置
高度なスパムメール対策	
分析されたカテゴリ	• メッセージをユーザのスパムメールフォルダに隔離 • メッセージ全体の隔離 • メッセージ全体の削除 • 件名に次のタグを付加 • 放置 • 通知 • 通知しない
推定されるカテゴリ	• メッセージをユーザのスパムメールフォルダに隔離 • メッセージ全体の隔離 • メッセージ全体の削除 • 件名に次のタグを付加 • 放置 • 通知 • 通知しない
フィッシング	• メッセージをユーザのスパムメールフォルダに隔離 • メッセージ全体の削除 • タグを付加して配信 • 放置

検索設定	利用可能な処理
Web レピュテーション	• メッセージをユーザのスパムメールフォルダに隔離 • メッセージ全体の隔離 • メッセージ全体の削除 • タグを付加して配信 • 放置 • 通知 • 通知しない
Time-of-Click プロテクション	
危険	• 許可 • 警告 • ブロック
極めて不審	• 許可 • 警告 • ブロック
不審	• 許可 • 警告 • ブロック
未評価	• 許可 • 警告 • ブロック

検出時の処理の詳細オプション

ディレクトリ、メッセージオプション、追加の検索などを指定するには、詳細オプションを設定します。

表 6-6. 検出時の処理: 詳細オプション

設定	説明

マクロ	詳細マクロ検索は定期的なウイルス検索を補足します。ここでは、ヒューリスティック検索を使用してマクロウイルス/不正プログラムを検出するか、検出したマクロコードをすべて削除します。ヒューリスティック検索とは、パターン認識およびルールベースのテクノロジを使用して不正マクロコードを検索する、評価的なウイルス検出方法です。
	• 検出レベル
	  • レベル 1 では最も具体的な基準を使用しますが、検出するマクロコードの数は最も少なくなります。
	  • レベル 4 では最も多くのマクロコードを検出しますが、安全なマクロコードを誤って不正マクロコードとして認識する可能性があります。
	• 詳細マクロ検索で検出されたすべてのマクロを削除: 検出したすべてのマクロコードを削除します。

隔離設定/隔離ディレクトリ	隔離されたメッセージを保存するディレクトリです。 注意 • InterScan では、ディレクトリを設定する際に UNC パスを使用できます (Exchange エッジサーバを除く)。ログオンしているユーザアカウントが、指定した UNC パスに対するフルコントロール権限を持っている必要があります。 • [セキュリティリスク検索] または [高度なスパムメール対策] で高度な脅威検索エンジンを有効化している場合、もしくは [Web レピュテーション] で URL 分析を有効化している場合で、処理に隔離を設定している場合は、検索された高度な脅威は [高度な脅威の隔離ディレクトリ] に隔離されます。

設定	説明
バックアップ設定/バックアップディレクトリ	バックアップメッセージを保存するディレクトリです。 **注意** InterScan では、ディレクトリを設定する際に UNC パスを使用できます (Exchange エッジサーバを除く)。ログオンしているユーザアカウントが、指定した UNC パスに対するフルコントロール権限を持っている必要があります。
置換設定	違反またはイベントが発生した場合に InterScan が使用する [置換ファイル名] と [置換テキスト] です。ファイルまたはテキストは、指定した置換設定に基づいて置き換えられます。
メールメッセージの転送設定	違反またはイベントが検出された後に転送されるメールの転送先メールアドレスとメッセージの内容です。
検索不能メッセージ部分	• 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です。 • 検索不能メッセージを受信した場合に InterScan が使用する [置換ファイル名] と [置換テキスト] です。ファイルまたはテキストは、指定した置換設定に基づいて置き換えられます。

通知

管理者は、セキュリティリスクに対して処理が実行されたときにメールまたは SNMP で通知を送信するように、InterScan を設定できます。また、通知を Windows イベントログに自動的に記録することもできます。

通知を送信する目的は次のとおりです。

- 元のユーザにメールメッセージが改ざんされていることを警告します。
- 管理者などのネットワークセキュリティ担当者にセキュリティリスクを通知します。
- セキュリティリスクおよび実行される処理に関する情報をユーザに表示します。

InterScan ではオプションにより、初期設定のメッセージに InterScan フィールドをさらに追加したり、カスタマイズしたメッセージを作成したりできます。

ヒント

InterScan の通知が SNMP で正しく解決されるようにするために、InterScan のインストールパス(\Isme\trend_smex_v2.mib) から MIB (Management Information Base) ファイルをネットワーク管理ツールにインポートできます。

通知設定

表 6-7. 通知設定

設定	詳細
管理者に通知する	• 送信先 – 管理者のメールアドレスを入力します。 • 件名 – 管理者に送信するメッセージの件名を入力します。 • メッセージ – メッセージ要素をクリックして、その要素を通知に追加します。 例: [時刻] をクリックしてメッセージリストに追加します。通知メッセージには、InterScan によって処理が実行された時刻が追加されます。 • 一括通知を次の間隔で送信する – 指定した期間のすべての通知を 1 つにまとめたメールを送信します。テキストボックスに数値を入力し、時間または日を選択することによって、期間を指定します。 • 一括通知を次の件数ごとに送信する – 指定した件数のフィルタ処理に関する通知を 1 つにまとめたメールを送信します。テキストボックスにまとめて通知するセキュリティリスクの発生件数を指定します。 • 個別通知を送信する – フィルタ処理が実行されるたびにメール通知を送信します。

設定	詳細
送信者に通知する	• 外部送信者に通知しない – 企業ネットワークの外部の送信者にメール通知を送信しないようにします。 • 詐称メールに対して送信者通知を無効にする – 詐称メッセージが検出されたときにメール通知を送信しないようにします。 注意 このオプションは、セキュリティリスク検索の通知でのみ使用できます。 • 件名 – メール送信者に送信するメッセージの件名を入力します。 • メッセージ – メッセージ要素をクリックして、その要素を通知に追加します。 例: [時刻] をクリックしてメッセージリストに追加します。通知メッセージには、InterScan によって処理が実行された時刻が追加されます。 • 内部送信者宛てと同じ通知 – 外部の送信者に内部の送信者と同じメッセージを送信する場合に選択します。内部の送信者用にカスタマイズされたメッセージと同じメッセージが送信されます。 • 別の通知を指定 – 外部の送信者に別のカスタマイズメッセージを送信する場合に選択します。メッセージ要素をクリックして、その要素を通知に追加します。

設定	詳細
受信者に通知する	• 外部受信者に通知しない – 企業ネットワークの外部の送信者にメール通知を送信しないようにします。 • 件名 – 受信者に送信するメッセージの件名を入力します。 • メッセージ – メッセージ要素をクリックして、その要素を通知に追加します。 例: [詳細の表示] をクリックして、メッセージリストに追加します。通知メッセージには、InterScan によって処理が実行された時刻が追加されます。 • 内部受信者宛てと同じ通知 – 外部の送信者に内部の送信者と同じメッセージを送信する場合に選択します。内部の送信者用にカスタマイズされたメッセージと同じメッセージが送信されます。 • 別の通知を指定 – 外部の送信者に別のカスタマイズメッセージを送信する場合に選択します。メッセージ要素をクリックして、その要素を通知に追加します。
SNMP	SNMP で通知を送信します。クリックすると SNMP メッセージをカスタマイズできます。 • IP アドレス – IP アドレスを入力します。 • コミュニティ – コミュニティ名 (Public または Private) を入力します。 • メッセージ – メッセージ要素をクリックして、その要素を通知に追加します。
Windows イベントログに書き込む	Windows のイベントログに通知を記録します。

第 7 章

セキュリティリスク検索の設定

この章では、Exchange 環境を保護するためのセキュリティリスク検索を設定する方法について説明します。

内容は次のとおりです。

セキュリティリスク検索について

InterScan は、送受信されるすべてのメールを検索することによって、Exchange 環境を保護します。検索設定には、インストールプログラムで設定されるトレンドマイクロの初期設定値をそのまま使用できますが、この章で説明するいくつかの項目を設定することによって検索をカスタマイズすることも可能です。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、InterScan を設定できます。検索の設定は、[セキュリティリスク検索] 画面で行います。この画面には、サイドバーから、または [手動検索] 画面や [予約検索] 画面からアクセスできます。

以下に、セキュリティリスク検索の主な特性について説明します。

表 7-1. セキュリティリスク検索の特性

検索の種類	特性
検索方法	セキュリティリスク検索には次の 2 種類の方法があります。 • 従来型スキャン • スマートスキャン 検索方法は、[検索サービス設定] 画面 ([Smart Protection] > [検索サービス設定]) で設定します。検索方法の詳細については、77 ページの「検索サービス設定」を参照してください。
リアルタイム検索	以下のデータがリアルタイムで検索されます。 • 受信または送信するすべてのメール • パブリックフォルダへの投稿 • サーバ間のすべての複製

検索の種類	特性
手動検索と予約検索	手動検索と予約検索では、メールボックスストアとパブリックフォルダストア内のメッセージが検索されます。 すでに進行中の予約検索は、別の予約検索を開始しても中断されません。予約検索がアップデートによって中断されることもありません。 クラスタサーバ上の場合: 各仮想サーバには検索タスクのリストがあります。現在の仮想サーバに属するストアデータベースを指定できます。予約検索タスクが実行中の場合、新しいタスクは待ち行列に追加されます。別のタスクが同時に起動された場合、タスクは待ち行列に追加されますが、最終的には実行されて終了します。

InterScan 検索の階層

管理者は、InterScan でセキュリティリスク検索を設定することにより、多様なレベルのセキュリティを提供できます。仮想アナライザで高度な脅威検索エンジンを有効にすると、不審な不正プログラムの脅威による標的型攻撃を検出および防止できます。

次の表に、InterScan における検索エンジンの階層の概要を示します。

表 7-2. 検索エンジンの階層

検索エンジン	説明
ウイルス検索エンジンによる検索	ウイルス検索エンジンは、パターンベースのヒューリスティック検索によって、従来型の不正プログラムの脅威を検出します。

検索エンジン	説明
ATSE による検索	ATSE を使用すると、ウイルス検索エンジンで提供される従来型の不正プログラムの脅威に対する保護機能が強化されます。ATSE は、ヒューリスティックアルゴリズムを使用して積極的な検索を実行することにより、ドキュメントの不正利用など標的型攻撃の可能性を識別します。 仮想アナライザにファイルを送信せずに ATSE を有効にするという検索設定の場合、InterScan では、ATSE によって高度な脅威として検出された不審メッセージやファイルを対象として、[高度な脅威] に対して設定されている処理を実行します。 注意 安全なファイルが検出されることもあります。ATSE で検出された不審な脅威については [メッセージ全体の隔離] を選択することをお勧めします。仮想アナライザに送信されなかったファイルについては、評価を実行して、隔離ファイルの実際の脅威を判断してください。 仮想アナライザを登録していない場合は、誤検出を少なくするために検索レベルを [低] に設定し、ATSE で検出された不審な脅威に対して [メッセージ全体の隔離] を選択することをお勧めします。
ATSE と仮想アナライザ	ATSE が不審な不正プログラムの脅威を検出すると、InterScan は詳しい分析のために仮想アナライザにメッセージを送信します。 仮想アナライザは、分離された仮想環境でメッセージのリスクレベルを評価し、InterScan サーバに脅威の評価結果を返します。セキュリティの評価結果が、不審な脅威に対して設定されているセキュリティレベルに違反している場合は、InterScan が [高度な脅威] に対して設定されている処理を実行します。 サンドボックスを使用した保護には、トラフィック方向や対象の受信者など、仮想アナライザの設定を適用することができます。たとえば、受信者を経営層や人事担当部門に設定することが可能です。初期設定では、トラフィック方向は受信メッセージのみです。サンドボックスの保護範囲にないメッセージは、検索エンジンやパターンファイルを使用した従来の方法で検索されます。

検索エンジン	説明
ATSE と機械学習	高度な脅威検索エンジンでは、Windows の実行可能ファイル (PE) やスクリプトファイルなど、一部のファイルのウイルス検索の実行時に、機械学習型検索を使用します。機械学習型検索では、従来のシグネチャベースの不正プログラム検出に比べ、より多くの不正プログラムの亜種を検出できます。

高度な脅威検索エンジンについて

高度な脅威検索エンジン (ATSE - Advanced Threat Scan Engine) は、パターンファイルに基づく検索とヒューリスティック検索を組み合わせて、標的型攻撃で使用されるドキュメントの不正利用などの脅威を検出します。

主な機能は次のとおりです。

- ゼロデイ脅威の検出
- 埋め込まれたエクスプロイトコードの検出
- 既知の脆弱性の検出ルール
- ファイルの変形に対応するパーサの機能強化

重要

ATSE 機能では既知と未知の高度な脅威が両方識別されるため、ATSE を有効にすると、正常なファイルが不正なファイルとしてフラグを付けられることが増加するおそれがあります。

機械学習型検索について

トレンドマイクロの機械学習型検索は、高度な機械学習テクノロジを使用して脅威情報を関連付け、デジタル DNA フィンガープリントや API マッピングなどのファイル機能を使用した詳細なファイル分析により、未知のセキュリティリスクを検出します。機械学習型検索は、未知の脅威およびゼロデイ攻撃から環境を保護するのに役立つ強力なツールです。

不明なファイルやあまり普及していないファイルを検出すると、InterScan は、高度な脅威検索エンジンでファイルを検索してファイル特性を抽出し、機械学習型検索エンジンにレポートを送信します。機械学習型検索では、不正プログラムモデリングにより、サンプルを不正プログラムモデルと比較し、

可能性スコアを割り当て、ファイルに含まれる潜在的な不正プログラムの種類を判別します。

セキュリティリスクの検出時の処理

InterScan には、セキュリティリスク検索用に次の 2 つの基本設定が用意されています。1 つはトレンドマイクロの推奨処理、もう 1 つはセキュリティリスクのタイプに基づいてカスタマイズされた処理です。

表 7-3. セキュリティリスクの検出時の処理

設定	説明
トレンドマイクロの推奨処理	トレンドマイクロが推奨する処理を InterScan で実行する場合は、[トレンドマイクロの推奨処理] を選択します。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切な処理を確定できない場合は、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。
指定の処理	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 InterScan を設定する場合は、[指定の処理] 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 InterScan 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。

手順

- マスメーリング型ウイルスから Exchange サーバを保護するには、[マスメーリング型ウイルスに対する処理を有効にする] を選択し、マスメーリング攻撃を検出したときに InterScan が実行する処理を選択します。この処理は、InterScan の他の処理よりも優先して実行されます。リアルタイム検索の初期設定の処理は、[メッセージ全体を削除] です。
- 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 InterScan を設定するには、[すべてのセキュリティリスク] 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。

- InterScan によって検出される脅威のタイプごとに InterScan の処理を設定するには、脅威タイプを個別に選択し、その脅威タイプを検出したときに InterScan が実行する処理を設定します。

リアルタイムセキュリティリスク検索の有効化

手順

1. メインメニューで [セキュリティリスク検索] を選択します。

   [セキュリティリスク検索] 画面が表示されます。

2. [セキュリティリスク検索] 画面で、[トランスポートレベルでのリアルタイムセキュリティリスク検索を有効にする] を選択します。

セキュリティリスク検索の対象の設定

手順

1. 次のいずれかに移動して、[セキュリティリスク検索] 画面を表示します。
   - リアルタイム検索の場合: セキュリティリスク検索
   - 手動検索の場合: [手動検索] > [セキュリティリスク検索]
   - 予約検索の場合: [予約検索] > [追加] または [編集] > [セキュリティリスク検索]
2. [対象] タブに移動します。

   [対象] タブが表示されます。
3. [高度な脅威検索エンジンを有効にする] を選択して従来とは異なる脅威について積極的な検索を実行できるようにし、[検索レベル]を指定します。

ヒント

安全なファイルが検出されることもあります。ATSE で検出された不審な脅威については [メッセージ全体の隔離] を選択することをお勧めします。仮想アナライザに送信されなかったファイルについては、評価を実行して、隔離ファイルの実際の脅威を判断してください。選択した検索レベルが高いほど、誤検出も多くなる可能性があります。

4. [高度な脅威検索エンジンを有効にする] を選択した場合は、[機械学習型検索を有効にする] も選択すると、機械学習テクノロジを使用してより多くの不正プログラムの亜種を検出できます。その場合は次の設定を行います。

   - [承認するファイルハッシュリストを有効にする] を選択して、ハッシュタグがリストに登録されている添付ファイルの検索をスキップします。

5. 検索対象として次のいずれかを選択します。

   - [すべての添付ファイル] — 検索不能なファイルを除くすべてのファイルで、ウイルス/不正プログラム、ワーム、トロイの木馬、およびその他の不正コードを検索します。検索不能なファイルは、暗号化されたメールメッセージ、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、ユーザが定義した検索制限の範囲外のファイル、またはサポートされていないか、破損しているファイルです。その他の不正コードとは、InterScan による処理を設定する必要がある、これまでに知られていなかった種類の脅威です。
   - [トレンドマイクロの推奨設定] — トレンドマイクロが推奨する設定を使用して効率的な検索が実行されます。

注意

トレンドマイクロの推奨設定を使用した検索と、InterScan の実際のファイルタイプの認識機能を使用した他の検索との間には、重要な相違が 1 つあります。InterScan の実際のファイルタイプの認識機能では、ユーザが検索対象のファイルを独自に定義できるのに対し、トレンドマイクロ推奨設定では、検索対象ファイルとして常にトレンドマイクロが推奨するファイルが選択されます。

- [ファイルタイプを指定] — リンクをクリックしてリストを展開し、検索するファイルタイプを選択します。これらは「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チェックして、実際のファイルタイプを判別します。または、[拡張子の指定] を選択して、ファイル拡張子を個別に指定します。

注意

例: [ファイルタイプを指定] をクリックし、[アプリケーションおよび実行可能ファイル] > [実行可能ファイル (.exe; .dll; .vxd)] の順にクリックすると、実行可能ファイル、DLL、および VXD ファイルタイプが、偽のファイル拡張子が使用されている場合も含めて (実際の拡張子は.exe であるのに.txt 拡張子が付いている場合など) 検索されます。それに対し、[拡張子の指定] をクリックして「.exe」と入力した場合、.exe タイプのファイルのみが検索されます。偽の拡張子が付けられたファイルは認識されません。

6. メッセージ本文を検索するには、[メッセージ本文を検索する] を選択します。
7. IntelliTrap テクノロジを使用するには、[IntelliTrap を有効にする] を選択します。

   IntelliTrap 検索の詳細については、26 ページの「IntelliTrap」を参照してください。
8. スパイウェア/グレーウェアを検索するには、[スパイウェア/グレーウェア検索] で [すべてを選択] を選択するか、リストから選択します。
9. パフォーマンスの向上が必要な場合は、[検索の制限条件] をクリックします。

   圧縮ファイルの制限の詳細については、86 ページの「セキュリティリスク検索時の圧縮ファイルの制限」を参照してください。

ヒント

トレンドマイクロでは、検索制限を使用して DoS (Denial of Service) 攻撃から保護することをお勧めします。DoS とは、ネットワーク接続を不能にするためにコンピュータまたはネットワークに対して行われる攻撃です。典型的な DoS 攻撃は、ネットワーク帯域幅に悪影響を及ぼしたり、メモリなどのコンピュータリソースに過度の負荷をかけたりします。

10. [保存] 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

InterScan は、検索設定に一致するファイルを検出すると、Exchange 環境を保護するための処理を実行します。InterScan がどのような処理を実行するかは、実行している検索の種類 (リアルタイム検索、手動検索、または予約検索)、Exchange Server の役割、およびその検索に対して設定されている処理の種類に応じて決まります。

手順

1. 次のいずれかに移動して、[セキュリティリスク検索] 画面を表示します。
   - リアルタイム検索の場合: セキュリティリスク検索
   - 手動検索の場合: [手動検索] > [セキュリティリスク検索]
   - 予約検索の場合: [予約検索] > [追加] または [編集] > [セキュリティリスク検索]
2. [処理] タブをクリックします。

   [処理] タブが表示されます。
3. 次のいずれかを選択します。
   - [トレンドマイクロの推奨処理] — トレンドマイクロが推奨する検出時の処理を実行します。
   - [指定の処理] — 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。

注意

InterScan が [高度な脅威] で実行する検出時の処理を設定するには、管理者が [セキュリティリスク検索: 対象] タブで高度な脅威検索エンジンを有効にする必要があります。

セキュリティリスクの検索時の処理の詳細については、108 ページの「セキュリティリスクの検出時の処理」を参照してください。

4. 感染ファイルをバックアップするには、[処理の前にバックアップを作成する] を選択します。
5. パフォーマンスの向上が必要な場合は、[感染した圧縮ファイルを駆除しない] を選択します。
6. ファイルの内容と検索結果を分析のためにトレンドマイクロに送信する場合は、[機械学習型検索のフィードバックを Trend Micro Smart Protection Network に送信する] を選択します。

注意

このオプションを選択するには、[対象] タブで機械学習型検索を有効にしておく必要があります。

7. 必要に応じて [詳細オプション] を設定します。

注意

詳細検索処理の詳細については、97 ページの「検出時の処理の詳細オプション」を参照してください。

a. [マクロ]をクリックしてマクロ検索を設定します。
   1. [詳細マクロ検索を有効にする] を選択します。
   2. 次のいずれかを選択します。
      - [検出レベル]
      - [詳細マクロ検索で検出されたすべてのマクロを削除]

注意

マクロ検索の設定の詳細については、114 ページの「マクロ検索の設定」を参照してください。

b. [隔離とバックアップ設定] をクリックして、ディレクトリパスを指定します。

c. [置換設定] をクリックして、感染したコンテンツを置換するためのテキストまたはファイル名を設定します。

d. [検索不能メッセージ部分] をクリックして、暗号化されたメールメッセージ、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、検索の制限条件に当てはまらないファイル、およびサポートされていないか、破損しているファイルに対する処理を指定します。また、検索対象から除外するファイル拡張子、および検索不能なコンテンツを置換するためのテキストまたはファイル名を指定できます。

8. [保存] をクリックします。

マクロ検索の設定

InterScan では、ウイルスパターンファイルを使用して、定期的なウイルス検索中に既知の不正マクロコードを特定します。InterScan は、[セキュリティリスク検索] 画面で設定した処理に従って、不正マクロコードに対処します。不正マクロコードに対する保護を強化するには、詳細マクロ検索を使用します。

詳細マクロ検索は定期的なウイルス検索を補足します。ここでは、ヒューリスティック検索を使用してマクロウイルス/不正プログラムを検出するか、検出したマクロコードをすべて削除します。ヒューリスティック検索とは、パターン認識およびルールベースのテクノロジを使用して不正マクロコードを検索する、評価的なウイルス検出方法です。この方法は、既知のシグネチャを持たないウイルスおよびセキュリティリスクの検出に優れています。不正マクロコードがヒューリスティック検索により検出されると、InterScan は [セキュリティリスク検索] 画面で設定した処理に従って、不正コードに対処します。[詳細マクロ検索で検出されたすべてのマクロを削除] を選択すると、検索したファイルからすべてのマクロコードが削除されます。

手順

1. 次のいずれかに移動して、[セキュリティリスク検索] 画面を表示します。
   - リアルタイム検索の場合: [セキュリティリスク検索] > [処理]
   - 手動検索の場合: [手動検索] > [セキュリティリスク検索] > [処理]
   - 予約検索の場合: [予約検索] > [追加] または [編集] > [セキュリティリスク検索] > [処理]
2. [詳細オプション] をクリックし、[マクロ] をクリックします。
3. [詳細マクロ検索を有効にする] を選択します。
4. 検出タイプを選択します。
   a. [検出レベル] を選択し、ヒューリスティックルールのレベルを設定します。
      - レベル 1 では最も具体的な基準を使用しますが、検出するマクロコードの数は最も少なくなります。
      - レベル 4 では最も多くのマクロコードを検出しますが、安全なマクロコードを誤って不正マクロコードとして認識する可能性があります。

      ヒント

      トレンドマイクロでは、レベル 2 のヒューリスティック検索をお勧めします。このレベルでは、マクロウイルスが高いレベルで検出され、かつ高速で検索が行われます。マクロウイルス/不正プログラムの文字列をチェックするのに必要なルールだけが使用されます。レベル 2 では、安全なマクロコード内で誤って不正コードと認識する度合いも低くなっています。

   b. 検出されたすべてのマクロコードが削除されるようには、[詳細マクロ検索で検出されたすべてのマクロを削除] を選択します。
5. [保存] をクリックします。

セキュリティリスク検索の通知の設定

手順

1. 次のいずれかに移動して、[セキュリティリスク検索] 画面を表示します。
   - リアルタイム検索の場合: セキュリティリスク検索
   - 手動検索の場合: [手動検索] > [セキュリティリスク検索]
   - 予約検索の場合: [予約検索] > [追加] または [編集] > [セキュリティリスク検索]
2. [通知] タブをクリックします。

   [通知] 画面が表示されます。
3. InterScan で通知するユーザに対応するチェックボックスをオンにします。
4. [詳細の表示] をクリックして、その受信者の通知をカスタマイズします。
5. 通知オプションの中から選択します。

   詳細については、100 ページの「通知設定」を参照してください。
6. [Windows イベントログに書き込む] チェックボックスをオンにして、Windows のイベントログに通知が記録されるように設定します。
7. [保存] をクリックします。

第 8 章

添付ファイルブロックの設定

この章では、Exchange 環境を保護するための添付ファイルブロックを設定する方法について説明します。

内容は次のとおりです。

添付ファイルブロックについて

添付ファイルブロックは、不審ファイルが添付されたメールが配信されないようにする機能です。次の要素を基準に添付ファイルをブロックできます。

- 添付ファイルの種類
- 添付ファイルの名前
- 添付ファイルの拡張子

InterScan は、不審添付ファイルを検出すると、ポリシールールに一致するすべてのメッセージを置換、隔離、または削除します。ブロックは、リアルタイム検索、手動検索、予約検索時に実行されます。

添付ファイルの種類は、設定に応じて、.doc、.exe、または.dll などの実際のファイルタイプまたは拡張子で識別されます。多くのウイルス/不正プログラムは、特定の種類のファイルに存在します。InterScan でファイルタイプに応じたブロックを設定することにより、管理者は該当する種類のファイルからの Exchange サーバに対するセキュリティリスクを減少させることができます。同様に、多くの場合、特定の攻撃は特定のファイル名と関係があります。

注意

添付ファイルブロックを使用すると、ウイルス/不正プログラムの大規模感染を効果的に抑制できます。高リスクのファイルタイプや、既知のウイルス/不正プログラムに関連する特定の名前を持つファイルタイプをすべて、一時的に隔離できます。大規模感染が終息した後に、隔離フォルダを調べて、検出されたファイルを処理できます。

メッセージの受信者は、1 つの添付ファイルブロック除外設定に一致する場合と、優先度に基づいて添付ファイルブロックグローバルルールに一致する場合があります。受信者が添付ファイルブロック除外設定に一致する場合、その除外設定で選択された対象は、添付ファイルブロックグローバルルールの適用対象から除外されます。受信者がどの添付ファイルブロック除外設定にも一致しない場合は、添付ファイルブロックグローバルルールが適用されます。

指定された受信者をカスタマイズするために、次の 4 種類のアカウントがサポートされています。Active Directory ユーザ、Active Directory 連絡先、Active Directory 配布グループ、および特定グループです。

添付ファイルブロック除外設定ごとに、選択アカウントと除外アカウントを指定できます。除外設定は、選択アカウントに属しているアカウントには適用されますが、除外アカウントに属しているアカウントには適用されません。たとえば、Active Directory グループ 1 に、AD ユーザ 1 と AD ユーザ 2 が含まれているとします。選択アカウントに「AD グループ 1」が含まれており、除外アカウントに「AD ユーザ 1」が含まれている場合は、ポリシーは AD ユーザ 2 のみに適用されます。

リアルタイム添付ファイルブロックの有効化

添付ファイルブロックが有効になっている場合は、添付ファイルブロックの除外を個別に有効または無効にすることができます。緑色のチェックマークアイコン () はその除外が有効になっていることを示し、赤色の×印 () はその除外が無効になっていることを示します。アイコンをクリックして、有効と無効を切り替えられます。

注意

グローバルポリシーを無効にすることはできません。

手順

1. メインメニューで [添付ファイルブロック] を選択します。

   [添付ファイルブロック] 画面が表示されます。

2. [トランスポートレベルでの添付ファイルブロックを有効にする] を選択します。
3. [保存] をクリックします。

添付ファイルブロックのグローバルポリシーについて

添付ファイルブロックのグローバルポリシーは、送受信するすべてのメールに適用されます。添付ファイル付きのメールを、ファイルタイプまたはファイル名で自動的にブロックするようにグローバルポリシーを設定できます。

一部のユーザに異なる権限が求められる場合には、添付ファイルブロックの除外を作成して、グローバルポリシーに指定した添付ファイル付きメールの送受信を特定のアカウントに許可することもできます。

添付ファイルブロックの対象の設定

添付ファイルは、特定の名前または添付ファイルの種類に基づいてブロックできます。InterScan では、ファイル名拡張子と実際のファイルタイプに基づいて添付ファイルの種類を判断します。添付ファイルのブロックには、2 つの方法があります。すべての添付ファイルをブロックしてから、指定した添付ファイルを除外する方法か、またはブロックする添付ファイルを指定する方法です。

手順

1. 次のいずれかに移動して、[添付ファイルブロック] 画面を表示します。
   - リアルタイム検索の場合: [添付ファイルブロック] > [グローバルポリシー]
   - 手動検索の場合: [手動検索] > [添付ファイルブロック]
   - 予約検索の場合: [予約検索] > [追加] または [編集] > [添付ファイルブロック]
2. [対象] タブをクリックします。

   [対象] 画面が表示されます。
3. 次のいずれかを選択します。
   - [すべての添付ファイル]
     - [ファイルの種類による除外設定] と [除外する添付ファイル名] の一方または両方を選択します。[詳細の表示] をクリックして、特定のファイルの種類や名前を指定します。

- [指定の添付ファイル]
  - [添付ファイルの種類] と [添付ファイル名] の一方または両方を選択します。[詳細の表示] をクリックして、特定のファイルの種類や名前を指定します。

4. 選択した圧縮ファイル内の添付ファイルの種類をブロック対象に含める場合は、[圧縮ファイル内の添付ファイルを対象に含める] を選択します。Microsoft Office または OpenDocument ファイルに組み込まれたファイルの検索をスキップする場合は、さらに次のいずれかのオプションを選択します。
   - Microsoft Office 2007 以降のファイル内の組み込みファイルを対象に含めない
   - OpenDocument ファイル内の組み込みファイルを対象に含めない
5. この画面で選択した添付ファイルをブロックするには、[ドキュメント内で特定の添付ファイル (組み込みファイル) が検出された場合にファイルを対象に含める] を選択します。

   [検索する組み込み階層の最大数] オプションで、検索する組み込みファイルの最大圧縮階層数として、1〜20 の数値を入力します。ファイルの組み込み階層の数が、指定された数を超える場合は、そのファイルは検索されません。
6. パスワードで保護された Office ドキュメントと圧縮ファイルをブロック対象に含める場合は、[パスワード保護された Microsoft Office ドキュメントと圧縮ファイルを対象に含める] を選択します。
7. JavaScript が埋め込まれた PDF ファイルをブロック対象に含める場合は、[JavaScript が埋め込まれた PDF ファイルを対象に含める] を選択します。
8. パフォーマンスの向上が必要な場合は、[検索の制限条件] をクリックします。
   - [圧縮階層の数が次を超える場合]: 検索する圧縮ファイルの最大圧縮階層数として、1〜20 の数値を入力します。圧縮階層の数が、指定された数を超える場合は、その圧縮ファイルは検索されません。
9. [保存] をクリックします。

添付ファイルブロックの処理の設定

InterScan では、ブロックする必要がある添付ファイルを検出するたびに、処理を実行します。この画面を使用して、InterScan が実行する処理を設定します。また、通知を送信するかどうかも設定します。

手順

1. 次のいずれかに移動して、[添付ファイルブロック] 画面を表示します。
   - リアルタイム検索の場合: [添付ファイルブロック] > [グローバルポリシー]
   - 手動検索の場合: [手動検索] > [添付ファイルブロック]
   - 予約検索の場合: [予約検索] > [追加] または [編集] > [添付ファイルブロック]
2. [処理] タブをクリックします。

   [処理] 画面が表示されます。
3. 望ましくないコンテンツを検出したときに InterScan が実行する処理を選択します。

   使用できる処理の詳細については、87 ページの「InterScan の処理について」を参照してください。
4. 必要に応じて [詳細オプション] を設定します。

   詳細検索処理の詳細については、97 ページの「検出時の処理の詳細オプション」を参照してください。
5. [保存] をクリックします。

添付ファイルブロックの通知の設定

手順

1. 次のいずれかに移動して、[添付ファイルブロック] 画面を表示します。
   - リアルタイム検索の場合: [添付ファイルブロック] > [グローバルポリシー]

- 手動検索の場合: [手動検索] > [添付ファイルブロック]
- 予約検索の場合: [予約検索] > [追加] または [編集] > [添付ファイルブロック]

2. [通知] タブをクリックします。

   [通知] 画面が表示されます。

3. InterScan で通知するユーザに対応するチェックボックスをオンにします。
4. [詳細の表示] をクリックして、その受信者の通知をカスタマイズします。
5. 通知オプションの中から選択します。

   詳細については、100 ページの「通知設定」を参照してください。

6. [Windows イベントログに書き込む] チェックボックスをオンにして、Windows のイベントログに通知が記録されるように設定します。
7. [保存] をクリックします。

添付ファイルブロックグローバルポリシーへの除外設定の追加

手順

1. メインメニューで [添付ファイルブロック] を選択します。

   [添付ファイルブロック] 画面が表示されます。

2. [除外の追加] をクリックします。

   [アカウントの選択] 画面が表示されます。

3. グローバルポリシーから除外するアカウントを選択します。
   - 特定の送信者から任意の受信者
   - 任意の送信者から特定の受信者
4. [特定の送信者] または [特定の受信者] リンクをクリックします (該当する場合)。

5. 次のいずれかを選択します。
   - すべて — このポリシーまたは除外をすべてのユーザに適用します。
   - 特定のアカウント — Active Directory グループまたは InterScan 特定グループから選択します。
6. Active Directory のユーザ/グループ/連絡先/特定グループ内で検索して、これらを選択して [選択されたアカウント] リストに追加します。
7. Active Directory のユーザ/グループ/連絡先/特定グループを検索して選択し、[アカウントの除外] 画面の [選択されたアカウント] リストに追加します。
8. [保存] をクリックします。

   [アカウントの選択] 画面が表示されます。
9. [次へ>] をクリックします。

   [ポリシーの指定] 画面が表示されます。
10. 次の設定を行います。
    - 添付ファイルの種類 — グローバルポリシーから除外するファイルタイプを選択します。
    - 添付ファイル名 — グローバルポリシーから除外するファイル名または拡張子、あるいはその両方を指定します。

    注意

    [詳細の表示] をクリックして、ファイルタイプまたは名前を指定します。
11. [次へ>] をクリックします。

    [名前と優先度] 画面が表示されます。
12. 次の設定を行います。
    - 次の除外を有効にする — この除外設定を有効にします。
    - 除外名 — この除外設定の名前を入力します。

13. [優先度] に優先度を数字で入力します。
14. [保存] をクリックします。

添付ファイルブロック除外の編集

手順

1. メインメニューで [添付ファイルブロック] を選択します。

   [添付ファイルブロック] 画面が表示されます。
2. [グローバルポリシー] タブで、除外の [アカウント] または [ポリシー] ハイパーリンクをクリックして、除外を編集します。
3. 次の設定を行います。
   - 次の除外を有効にする — この除外設定を有効にします。
   - 除外名 — この除外設定の名前を入力します。
4. [アカウント] タブをクリックします。
   a. グローバルポリシーから除外するアカウントを変更するには、アカウントの種類を選択します。
      - 特定の送信者
      - 特定の受信者

      注意

      選択したアカウントの種類に該当するアカウントにのみポリシーが適用されます。別のアカウントの種類に該当するアカウントを選択した場合、そのアカウントにはポリシーは適用されません。

   b. 表内の [編集] リンクをクリックして、このポリシーを適用するアカウントと除外するアカウントを変更します。
   c. 次のいずれかを選択します。
      - すべて — このポリシーまたは除外をすべてのユーザに適用します。

- 特定のアカウント — Active Directory グループまたは InterScan 特定グループから選択します。

d. Active Directory のユーザ/グループ/連絡先/特定グループ内で検索して、これらを選択して [選択されたアカウント] リストに追加します。

e. Active Directory のユーザ/グループ/連絡先/特定グループを検索して選択し、[アカウントの除外] 画面の [選択されたアカウント] リストに追加します。

f. [保存] をクリックします。

5. 対象とする添付ファイルの設定を変更するには、[対象] タブをクリックします。

- 添付ファイルの種類 — グローバルポリシーから除外するファイルタイプを選択します。
- 添付ファイル名 — グローバルポリシーから除外するファイル名または拡張子、あるいはその両方を指定します。

注意

[詳細の表示] をクリックして、ファイルタイプまたは名前を指定します。

6. [保存] をクリックします。

カスタマイズポリシーの追加

手順

1. メインメニューで [添付ファイルブロック] を選択します。

   [添付ファイルブロック] 画面が表示されます。

2. [カスタマイズポリシー] タブで、[追加] をクリックしてポリシーを追加します。

   [手順 1: アカウントの選択] 画面が表示されます。

3. 次のいずれかを選択します。
   - 特定の送信者から任意の受信者
   - 任意の送信者から特定の受信者
   - 特定の送信者から特定の受信者
4. [特定の送信者] または [特定の受信者] リンクをクリックします (該当する場合)。
5. 次のいずれかを選択します。
   - すべて — このポリシーをすべてのユーザに適用します。
   - 特定のアカウント — Active Directory グループまたは InterScan 特定グループから選択します。
6. Active Directory のユーザ/グループ/連絡先/特定グループ内で検索して、これらを選択して [選択されたアカウント] リストに追加します。
7. Active Directory のユーザ/グループ/連絡先/特定グループを検索して選択し、[アカウントの除外] 画面の [選択されたアカウント] リストに追加します。
8. [保存] をクリックします。

   [手順 1: アカウントの選択] 画面が再度表示されます。
9. [次へ>] をクリックします。

   [手順 2: ポリシーの指定] 画面が表示されます。
10. 画面上で設定を行います。設定の手順と詳細については、120 ページの「添付ファイルブロックの対象の設定」を参照してください。
11. [次へ>] をクリックします。

    [手順 3: 処理の指定] 画面が表示されます。
12. 画面上で設定を行います。設定の手順と詳細については、122 ページの「添付ファイルブロックの処理の設定」を参照してください。
13. [次へ>] をクリックします。

    [手順 4: 通知の指定] 画面が表示されます。

14. 画面上で設定を行います。設定の手順と詳細については、122 ページの「添付ファイルブロックの通知の設定」を参照してください。
15. [次へ>] をクリックします。

    [手順 5: 名前と優先度] 画面が表示されます。
16. [保存] をクリックします。

カスタマイズポリシーの編集

手順

1. メインメニューで [添付ファイルブロック] を選択します。

   [添付ファイルブロック] 画面が表示されます。
2. [カスタマイズポリシー] タブの [ポリシー] 列で、編集するポリシー名をクリックします。
3. 次の設定を行います。
   - [このポリシーを有効にする] — このポリシーを有効にします。
   - [ポリシー名]: このポリシーの名前を入力します。
4. [アカウント] タブをクリックします。
   a. カスタマイズポリシーを適用するアカウントを変更するには、アカウントの種類を選択します。
      - 特定の送信者
      - 特定の受信者
      - 特定の送信者から特定の受信者

      注意

      選択したアカウントの種類に該当するアカウントにのみポリシーが適用されます。別のアカウントの種類に該当するアカウントを選択した場合、そのアカウントにはポリシーは適用されません。

b. 表内の [編集] リンクをクリックして、このポリシーを適用するアカウントと除外するアカウントを変更します。

c. 次のいずれかを選択します。

- すべて — このポリシーをすべてのユーザに適用します。
- 特定のアカウント — Active Directory グループまたは InterScan 特定グループから選択します。

d. Active Directory のユーザ/グループ/連絡先/特定グループ内で検索して、これらを選択して [選択されたアカウント] リストに追加します。

e. Active Directory のユーザ/グループ/連絡先/特定グループを検索して選択し、[アカウントの除外] 画面の [選択されたアカウント] リストに追加します。

f. [保存] をクリックします。

5. [対象] タブを選択して、必要に応じて設定を変更します。設定の手順と詳細については、120 ページの「添付ファイルブロックの対象の設定」を参照してください。

6. [処理] タブを選択して、必要に応じて設定を変更します。設定の手順と詳細については、122 ページの「添付ファイルブロックの処理の設定」を参照してください。

7. [通知] タブを選択して、必要に応じて設定を変更します。設定の手順と詳細については、122 ページの「添付ファイルブロックの通知の設定」を参照してください。

8. [保存] をクリックします。

第 9 章

コンテンツフィルタの設定

この章では、Exchange 環境を保護するためのコンテンツフィルタを設定する方法について説明します。

内容は次のとおりです。

コンテンツフィルタについて

コンテンツフィルタは、受信および送信メッセージをユーザ定義ポリシーに基づいて評価します。各ポリシーには、キーワードおよび語句のリストが含まれています。コンテンツフィルタでは、メッセージをキーワードのリストと比較することにより、メッセージのヘッダとコンテンツ、またはそのいずれかを評価します。InterScan では、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 Exchange クライアントに配信されないようにする処理を実行できます。また InterScan で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、通知を送信することもできます。

InterScan では、[コンテンツフィルタ] 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メールに適用します。ポリシーを適用する順序は変更できます。InterScan では、実際に各ポリシーによって処理が行われるまで、各ポリシーに従ってすべてのメールをフィルタします。これらのポリシーの順序を変更して、コンテンツフィルタを最適化できます。

コンテンツフィルタにより、管理者はメッセージのテキストそのものに基づいてメールの配信を制限することができます。コンテンツフィルタを使用することで、受信および送信メッセージを監視して、不快なメッセージコンテンツやその他の好ましくないメッセージコンテンツが含まれていないかチェックできます。

たとえば、以下の内容が含まれていないかチェックするポリシーを作成できます。

- 性的嫌がらせに該当する言葉
- 人種差別に該当する言葉
- メールの本文に埋め込まれたスパムメール

注意

本機能は、InterScan 通常版では使用できません。

Active Directory 統合ポリシー

Active Directory 統合ポリシーでは、選択アカウントと除外アカウントを指定できます。ポリシーは、選択アカウントに属しているが除外アカウントには属していないアカウントに適用されます。たとえば、AD グループ 1 に、AD

ユーザ 1 と AD ユーザ 2 が含まれているとします。選択アカウントに「AD グループ 1」が含まれており、除外アカウントに「AD ユーザ 1」が含まれている場合は、ポリシーは AD ユーザ 2 のみに適用されます。

情報漏えい対策

InterScan には初期設定のコンテンツフィルタ情報漏えい対策ポリシーが用意されています。初期設定では、10 個の情報漏えい対策ポリシーが地域別に設定されています。標準のコンテンツフィルタポリシーとは異なり、情報漏えい対策ポリシー内のキーワードは、実際のキーワードではなく正規表現の記述文字列です。

たとえば、IBAN は、

`「[^\w](([A-Z]{2}\d{2}\s?)([A-Za-z0-9]{11,27}|([A-Za-z0-9]{4}\s){3,6}[A-Za-z0-9]{0,3}|([A-Za-z0-9]{4}\s){2}[A-Za-z0-9]{3,4}))[^\w]」`という正規表現の記述です。

「IBAN」という文字列が含まれたメッセージは、このポリシー内で定義された処理をしません。「BE68 5390 0754 7034」などの文字列は、この正規表現に一致して、このポリシー内で定義された処理をします。

リアルタイムコンテンツフィルタの有効化

コンテンツフィルタを有効にすると、個別のコンテンツフィルタポリシーを有効または無効にできます。緑色のチェックマークアイコン () はそのポリシーが有効になっていることを示し、赤色の×印 () はそのポリシーが無効になっていることを示します。アイコンをクリックして、有効と無効を切り替えられます。

手順

1. メインメニューで [コンテンツフィルタ] を選択します。

   [コンテンツフィルタ] 画面が表示されます。

2. [トランスポートレベルでのコンテンツフィルタを有効にする] を選択します。

3. [保存] をクリックします。

グローバル設定

InterScan では、隔離を使用して、該当するメッセージを隔離ディレクトリに移動し、対象のファイルを置き換え、残りのメッセージを元の受信者に配信します。

InterScan では、ポリシーイベントが検出されたときに、メールを隔離またはバックアップするように設定できます。[処理設定] 画面から隔離またはバックアップ用のフォルダを各ポリシーに対して個別に設定するか、またはグローバルディレクトリを指定できます。

隔離またはバックアップ用のグローバルディレクトリを指定すると、InterScan では、ポリシーイベントの結果として隔離またはバックアップするすべてのファイルを、指定したディレクトリに移動します。

グローバルな詳細検索処理の詳細については、97 ページの「検出時の処理の詳細オプション」を参照してください。

[グローバル設定] を設定するには、[コンテンツフィルタ] > [グローバル設定] の順にクリックします。

注意

[すべてのルールに適用] をクリックして、新しいディレクトリを設定する必要があります。[保存] をクリックしても、InterScan では入力したディレクトリパスが保存されるだけで、適用されません。

コンテンツフィルタポリシーの設定

コンテンツフィルタポリシーを作成するには、ポリシーウィザードの指示に従って一連の手順を実行します。各手順で内容を追加して、ポリシーを完成させます。ポリシーの作成後、InterScan ではそのポリシーに従って、すべての受信および送信メッセージのフィルタを開始します。

次のことを実行するポリシーを作成できます。

表 9-1. コンテンツフィルタポリシー

ポリシー	説明
いずれかに一致/すべてのルールに適用	この種類のポリシーでは、リアルタイム検索で、または手動検索や予約検索の際に、すべてのメッセージのコンテンツをフィルタできます。 注意 Active Directory 統合は、Microsoft Exchange Server 2019、2016 または 2013 メールボックスサーバの役割で使用できます。
すべての条件に一致	この種類のポリシーでは、InterScan がメールメッセージの送信者、送信先、Cc、件名、サイズおよび添付ファイル名のフィールド内で特定の内容を検出すると、処理を実行します。
いずれかの条件に一致	この種類のポリシーでは、特定のメールアカウント (複数可) のメッセージコンテンツを検索します。これらのポリシーは、一般的なコンテンツフィルタポリシーに似ていますが、指定されたメールアカウントからのコンテンツのみをフィルタする点が異なります。
除外	この種類のポリシーでは、特定のメールアカウント (複数可) を除外します。

送信者リストと受信者リストの設定 (いずれかに一致/すべてのルールに適用)

注意

ポリシーを編集する場合、アカウントを変更できるのはいずれかに一致/すべてのルールに適用ポリシーのみです。それ以外の種類のポリシーでは、「すべてのアカウント」が初期設定のアカウントとなります。

手順

1. [コンテンツフィルタ] を選択して [コンテンツフィルタ] 画面を表示します。

2. いずれかに一致/すべてのルールに適用ポリシーを追加または編集します。

   - 新規ポリシーの作成中:

     [追加] > [いずれかに一致/すべてのルールに適用] の順にクリックします。

   - ポリシーの編集中:

     a. ポリシー名をクリックします。

     b. [アカウント] タブをクリックします。

3. ポリシー検索の対象とする送信者または受信者を選択します。

   - 新規ポリシーの作成中:

     a. アカウントの種類を選択します。

        - 任意の送信者から任意の受信者
        - 特定の送信者から任意の受信者
        - 任意の送信者から特定の受信者

     b. [特定の送信者] または [特定の受信者] リンクをクリックします (該当する場合)。

   - ポリシーの編集中:

     a. アカウントの種類を選択します。

        - すべて
        - 特定の送信者
        - 特定の受信者

        選択したアカウントの種類に該当するアカウントにのみポリシーが適用されます。別のアカウントの種類に該当するアカウントを選択した場合、そのアカウントにはポリシーは適用されません。

     b. 表内の [編集] リンクをクリックして、このポリシーを適用するアカウントと除外するアカウントを変更します。

4. 次のいずれかを選択します。
   - すべて — このポリシーまたは除外をすべてのユーザに適用します。
   - 特定のアカウント — Active Directory グループまたは InterScan 特定グループから選択します。
5. Active Directory のユーザ/グループ/連絡先/特定グループ内で検索して、これらを選択して [選択されたアカウント] リストに追加します。
6. Active Directory のユーザ/グループ/連絡先/特定グループを検索して選択し、[アカウントの除外] 画面の [選択されたアカウント] リストに追加します。
7. [保存] をクリックします。

コンテンツフィルタの対象の設定

次の対象を設定して InterScan でフィルタするコンテンツを指定します。

手順

1. 次のいずれかに移動して、[コンテンツフィルタ] 画面を表示します。
   - リアルタイム検索の場合: コンテンツフィルタ
   - 手動検索の場合: [手動検索] > [コンテンツフィルタ]
   - 予約検索の場合: [予約検索] > [追加] または [編集] > [コンテンツフィルタ]
2. ポリシーの追加または編集:
   - 新規ポリシーの場合:
     a. [追加] > [ポリシーの種類] をクリックします。
     b. [ポリシーの指定] 画面に移動します。
   - 既存のポリシーの場合:
     a. ポリシー名をクリックします。
     b. [対象] タブをクリックします。

3. 対象の設定を指定します。

表 9-2. コンテンツフィルタの対象の設定

セクション	設定
メールアカウント (いずれかの条件ポリシーに一致)	次のフィールド内で検索するメールアカウントを指定します。 • 送信者 • 送信先 • Cc
対象	次のフィールド内でキーワードを検索します。 • いずれかに一致/すべてのルールに適用ポリシーの場合 – [ヘッダ]、[送信元]、[送信先]、[Cc]、[件名]、[本文]、[添付ファイル] • いずれかの条件に一致ポリシーの場合 – [件名]、[本文]、[添付ファイル] すべての条件に一致ポリシーの場合 – • 次のフィールド内で検索するキーワードを指定します。[送信元]、[送信先]、[Cc]、[件名]、[添付ファイル名] • 大文字/小文字を区別する – キーワードの検索で大文字と小文字を区別します。 • サイズ – [次より大きい]、[次より小さい]、[次と同じ]、または [次と異なる] を選択して、バイト数を指定します。

セクション	設定
キーワードを追加 (いずれかに一致、すべてのルールに適用、いずれかの条件に一致)	• 一致 – [指定したすべてのキーワード] または [指定したいずれかのキーワード] を選択します。 • キーワードを入力 – リストに追加するキーワードを入力します。 • 追加 – キーワードをリストに追加します。 • 削除 – 選択したキーワードをリストから削除します。 • エクスポート – キーワードをファイルにエクスポートします。 • インポート – キーワードをファイルからインポートします。 • 大文字/小文字を区別する – キーワードの検索で大文字と小文字を区別します。 • キーワードの同義語を含める – 同義語も一致対象とします。 • 詳細の表示 – 同義語を管理します。

インポートするキーワードリスト

キーワードファイルをインポートすると、インポートされたキーワードがキーワードリストに表示されます。インポートするファイルは、テキスト (`.txt`) ファイルである必要があります。インポートされたキーワードは、テキストファイルに含まれていたときと同じ形式で表示されます。以下に例を示します。

表 9-3. コンテンツフィルタ用のインポートするテキストファイル

インポートするテキストファイルに含まれる内容	キーワードリストの表示
win cash prize	win cash prize
win cash prize	win cash prize

注意

リストが完成したらキーワードをエクスポートしてください。これにより、他の InterScan サーバで使用するためのキーワードのコピーを保持したり、後でキーワードをインポートできます。

コンテンツフィルタの処理の設定

InterScan では、望ましくないコンテンツを検出するたびに、処理を実行します。この画面を使用して、InterScan が実行する処理を設定します。また、InterScan が通知を送信するかどうかを設定します。

手順

1. 次のいずれかに移動して、[コンテンツフィルタ] 画面を表示します。
   - リアルタイム検索の場合: コンテンツフィルタ
   - 手動検索の場合: [手動検索] > [コンテンツフィルタ]
   - 予約検索の場合: [予約検索] > [追加] または [編集] > [コンテンツフィルタ]
2. ポリシーの追加または編集:
   - 新規ポリシーの場合:
     a. [追加] > [ポリシーの種類] をクリックします。
     b. [処理の指定] 画面に移動します。
   - 既存のポリシーの場合:
     a. ポリシー名をクリックします。
     b. [処理] タブをクリックします。
3. 望ましくないコンテンツを検出したときに InterScan が実行する処理を選択します。
4. 指定したユーザに通知するには、次の操作を行います。
   - [送信者の管理者に転送する] チェックボックスをオンにします。

- [特定のメールアドレスに転送する] チェックボックスをオンにし、受信者のメールアドレスを入力します。

5. 処理が実行されたときの動作として、[通知する] または [通知しない] を選択します。
6. 必要に応じて [詳細オプション] を設定します。

コンテンツフィルタの通知の設定

手順

1. 次のいずれかに移動して、[コンテンツフィルタ] 画面を表示します。
   - リアルタイム検索の場合: コンテンツフィルタ
   - 手動検索の場合: [手動検索] > [コンテンツフィルタ]
   - 予約検索の場合: [予約検索] > [追加] または [編集] > [コンテンツフィルタ]
2. 通知の設定を行う前にポリシーを追加または編集します。
   - 新規ポリシーの場合:
     a. [追加] > [ポリシーの種類] をクリックします。
     b. [通知の指定] 画面に移動します。
   - 既存のポリシーの場合:
     a. ポリシー名をクリックします。
     b. [通知] タブをクリックします。
3. InterScan で通知するユーザに対応するチェックボックスをオンにします。
4. [詳細の表示] をクリックして、その受信者の通知をカスタマイズします。
5. 通知オプションの中から選択します。

   詳細については、100 ページの「通知設定」を参照してください。

6. [Windows イベントログに書き込む] チェックボックスをオンにして、Windows のイベントログに通知が記録されるように設定します。

コンテンツフィルタポリシーの有効化

個々のポリシーを有効にし、検索時に使用する優先度を各ポリシーに指定します。

手順

1. 次のいずれかに移動して、[コンテンツフィルタ] 画面を表示します。
   - リアルタイム検索の場合: コンテンツフィルタ
   - 手動検索の場合: [手動検索] > [コンテンツフィルタ]
   - 予約検索の場合: [予約検索] > [追加] または [編集] > [コンテンツフィルタ]
2. ポリシーを有効にする前に、追加または編集します。
   - 新規ポリシーの場合:
     a. [追加] > [ポリシーの種類] をクリックします。
     b. [名前と優先度] 画面に移動します。
   - 既存のポリシーの場合:

     ポリシー名をクリックします。
3. このポリシーまたは除外を有効にします。
4. このポリシーの名前を [ポリシー名] に入力します。
5. 優先度を指定します。
   - 新規ポリシーの場合:

     このポリシーの優先度を [優先度] に入力します。
   - 既存のポリシーの場合:
     a. リスト内のポリシー名または除外名の横にあるチェックボックスをオンにします。

b. [優先度の再設定] をクリックします。

c. [優先度] フィールドに、優先度を数字で入力します。

d. [優先度を保存] をクリックします。

6. [保存] をクリックします。

コンテンツフィルタの除外ポリシーの設定

除外ポリシーの動作は、他のコンテンツフィルタポリシーと同じ優先順位に従います。除外ポリシーは、優先順位の低いコンテンツフィルタポリシーのメールアドレス除外リストを指定します。

注意

除外メールアドレスは、SMTP アドレスであっても表示名であってもかまいません (InterScan がインストールされているドメイン内のユーザが対象)。除外メールアドレスでは、正規表現を使用できません。

手順

1. 次のいずれかに移動して、[コンテンツフィルタ] 画面を表示します。
   - リアルタイム検索の場合: コンテンツフィルタ
   - 手動検索の場合: [手動検索] > [コンテンツフィルタ]
   - 予約検索の場合: [予約検索] > [追加] または [編集] > [コンテンツフィルタ]
2. ポリシーの追加または編集:
   - 新規ポリシーの場合:

     [除外の > 追加]をクリックします。
   - 既存のポリシーの場合:

     ポリシー名をクリックします。
3. [アドレスを入力] にメールアドレスを入力します。

4. [追加] をクリックします。

   そのメールアドレスがリストに表示されます。

5. リストを保存します。

コンテンツフィルタポリシーの編集

編集オプションの説明を以下に示します。

手順

1. メインメニューで [コンテンツフィルタ] を選択します。

   [コンテンツフィルタ] 画面が表示されます。

2. 編集するポリシーの名前をクリックします。
3. 次のオプションを設定します。
   - このポリシーを有効にする: このポリシーを有効にします。
   - ポリシー名 – 新しい名前を入力してポリシー名を編集します。
   - アカウント – 現在のポリシーが適用されているアカウントを表示します。
   - 対象 – ポリシーの種類に基づいて対象を編集します。
   - 処理 – このポリシーで使用できる処理の中から選択して、処理を編集します。
   - 通知 – このポリシーで使用できるオプションの中から選択して、通知を編集します。
4. [保存] をクリックします。

第 10 章

情報漏えい対策の設定

この章では、Exchange 環境を保護するための情報漏えい対策を設定する方法について説明します。

内容は次のとおりです。

情報漏えい対策について

データ侵害の流行や悪影響により、現在の組織は、デジタル資産保護をセキュリティインフラストラクチャの必須要素と見なしています。

情報漏えい対策は、組織の機密データを不慮の流失や意図的な漏えいから守ります。情報漏えい対策により、管理者は次のことを実行できます。

- データ識別子を使用して保護する必要がある機密情報の識別
- メールや外部デバイスなどの一般的な転送チャネルを通したデジタル資産の転送を制限または阻止するポリシーの作成
- 制定されたプライバシー標準へのコンプライアンスの実施

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。
- セキュリティの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、通常は、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、データ識別子と企業ポリシーの定義を始めることができます。

データ識別子の種類

デジタル資産とは、組織で保護する必要のあるファイルやデータを意味します。デジタル資産は次のデータ識別子を使用して定義することができます。

- パターン: 特定の構造を持つデータ。

  詳細については、147 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: 特別な単語や語句のリスト。

  詳細については、152 ページの「キーワード」を参照してください。

注意

情報漏えい対策テンプレートで使用されているデータ識別子を削除することはできません。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、147 ページの「事前定義済みのパターン」および 147 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

情報漏えい対策には、事前定義済みのパターンが付属しています。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、次の Web サイトを参照してください。

https://success.trendmicro.com/dcx/s/solution/1312344?language=ja

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、利用する事が出来ます。

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、148 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 10-1. 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

パターンの追加と編集

事前に定義されたパターンがどれも会社の要件を満たさない場合は、独自のパターンを作成します。

手順

1. 左側のナビゲーションバーで、[情報漏えい対策] > [データ識別子] の順にクリックします。

   データ識別子のリストが表示されます。

2. [パターン] タブをクリックします。

3. [追加] をクリックするか、パターンの名前をクリックしてパターンを編集します。

   新しい画面が表示されます。

4. パターンの名前を入力します。

   名前の長さは、512 バイトを超えることはできません。

5. 2,048 バイト以内で説明を入力します。

6. パターンを入力し、大文字/小文字を区別するかどうかを指定します。

7. 表示されるデータを入力します。

   たとえば、ID 番号に使用するパターンを作成する場合は、サンプルの ID 番号を入力します。このデータは参照用としてのみ使用されるため、製品のどこにも表示されません。

8. 次のいずれかの条件を選択し、選択した条件に対して追加の設定を行います。

   - なし
   - 特定の文字
   - サフィックス
   - 単一の区切り文字

9. 必要に応じて追加の検証方法を選択します。

   これらの追加のバリデータは、特に高度に専門化されたデジタル資産を検出するように設計されています。

10. 実際のデータと照らし合わせてパターンをテストします。

たとえば、国民識別番号のパターンの場合は、[データのテスト] テキストボックスに有効な ID 番号を入力し、[テスト] をクリックして結果を確認します。

11. [保存] をクリックします。

ヒント

テストが成功した場合にのみ、設定を保存します。データを何も検出できないパターンは、システムリソースを無駄に消費するため、パフォーマンスに影響することがあります。

パターンのインポート

このオプションを使用するためには、パターンを含む正しい形式の .dat ファイルが必要です。現在のサーバ上にある InterScan サーバ、または別の InterScan サーバから、パターンをエクスポートしてファイルを生成してください。

手順

1. 左側のナビゲーションバーで、[情報漏えい対策] > [データ識別子] の順にクリックします。

   データ識別子のリストが表示されます。

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、パターンを含む .dat ファイルを探します。
4. [開く] をクリックします。

   インポートのステータスを示すメッセージが表示されます。

注意

各パターンには一意の ID 値が含まれています。同じ ID のパターンがすでに存在する場合は、InterScan により、既存のパターンが上書きされます。同じ表示名のパターンがすでに存在する場合は、既存のパターンに「Original」というサフィックスが付加され、新しいパターンがリストに追加されます。

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、152 ページの「事前定義済みのキーワードリスト」および 153 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。

https://success.trendmicro.com/dcx/s/solution/1312344?language=ja

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、153 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 10-2. 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追加と編集

キーワードとは特別な意味を持つ語または句のことです。特定の種類のデータを識別するには、関連するキーワードをキーワードリストに追加します。

事前に定義されたキーワードリストがどれも会社の要件を満たさない場合は、独自のキーワードリストを作成できます。

手順

1. 左側のナビゲーションバーで、[情報漏えい対策] > [データ識別子] の順にクリックします。

   データ識別子のリストが表示されます。

2. [キーワードリスト] タブをクリックします。
3. [追加] をクリックするか、キーワードリストの名前をクリックしてキーワードリストを編集します。

   新しい画面が表示されます。

4. キーワードリストの名前を入力します。

   名前の長さは、512 バイトを超えることはできません。

5. 2,048 バイト以内で説明を入力します。
6. 次のいずれかの条件を選択し、選択した条件に対して追加の設定を行います。
   - 任意のキーワード
   - すべてのキーワード
   - <x> 文字以内のすべてのキーワード
   - 合計スコアがしきい値を超えるキーワード
7. リストに手動でキーワードを追加するには
   a. 長さが 3～512 バイトのキーワードを入力し、大文字/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. キーワードを削除するには、キーワードを選択し、[削除] をクリックします。
9. [保存] をクリックします。

パターンのインポート

このオプションを使用するためには、パターンを含む正しい形式の.dat ファイルが必要です。現在のサーバ上にある InterScan サーバ、または別の InterScan サーバから、パターンをエクスポートしてファイルを生成してください。

手順

1. 左側のナビゲーションバーで、[情報漏えい対策] > [データ識別子] の順にクリックします。

   データ識別子のリストが表示されます。

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、パターンを含む.dat ファイルを探します。
4. [開く] をクリックします。

   インポートのステータスを示すメッセージが表示されます。

注意

各パターンには一意の ID 値が含まれています。同じ ID のパターンがすでに存在する場合は、InterScan により、既存のパターンが上書きされます。同じ表示名のパターンがすでに存在する場合は、既存のパターンに「Original」というサフィックスが付加され、新しいパターンがリストに追加されます。

情報漏えい対策テンプレートについて

情報漏えい対策テンプレートを使用して、一連のデータ識別子を組み合わせることにより、機密コンテンツをタグ付けして検出します。テンプレートは、データ識別子と演算子 (および/または) を条件文で組み合わせます。データのセットがポリシーの条件に一致した場合、情報漏えい対策によってポリシー内で定義された処理が実行されます。たとえば、すべて - Names from US Census Bureau AND US - HICN (Health Insurance Claim) テンプレートに一致するデータを含むファイルは HIPAA ポリシー内で定義された処理が適用されます。

情報漏えい対策に組み込みのテンプレートを使用して、GLBA、PCI-DSS、SB-1386、US PII、HIPAA などの規制コンプライアンスに対応することができます。企業独自のカスタムテンプレートを作成したり、既存のテンプレートを変更して、ビジネス要件に合わせることもできます。既存のユーザ定義テンプレートがある場合は、テンプレートをインポートおよびエクスポートして、企業全体でポリシーの一貫性を維持することができます。

情報漏えい対策データ識別子を設定した後、会社固有のテンプレートを作成したり、事前に定義されたテンプレートを使用できます。

事前定義済みの情報漏えい対策テンプレート

情報漏えい対策には、次のように、さまざまな規制基準に準拠するために使用可能な事前定義済みのテンプレートが付属しています。これらのテンプレートは、変更や削除ができません。

- GLBA:Gramm-Leach-Billey Act
- HIPAA:Health Insurance Portability and Accountability Act (医療保険の相互運用性と説明責任に関する法律)
- PCI-DSS:Payment Card Industry Data Security Standard (PCI-DSS: カード会員データや取引情報を保護することを目的に作成されたクレジット業界のセキュリティ基準)
- SB-1386:US Senate Bill 1386
- US PII:United States Personally Identifiable Information (米国で個人を特定できる情報)

すべての事前定義済みのテンプレートの目的の一覧、および保護されるデータの例については、次の Web サイトを参照してください。

https://success.trendmicro.com/dcx/s/solution/1312344?language=ja

情報漏えい対策テンプレートの定義

情報漏えい対策テンプレートは、キーワードリストおよびパターンを使用して組織の機密データを定義します。定義したテンプレートを情報漏えい対策ポリシーで使用することで、企業固有の機密情報を保護できます。情報漏えい対策テンプレートの詳細については、156 ページの「情報漏えい対策テンプレートについて」を参照してください。

注意

組み込みのテンプレートは変更できません。組み込みのテンプレートを新しいテンプレートのベースとして使用するには、テンプレート名の横にあるチェックボックスをオンにして、[情報漏えい対策テンプレート] のツールバーで [コピー] をクリックします。末尾に「コピー」というサフィックスが付いた新しいテンプレートが作成されます。

手順

1. 左側のナビゲーションバーで、[情報漏えい対策] > [情報漏えい対策テンプレート] の順にクリックします。

   テンプレートのリストが表示されます。

2. 情報漏えい対策テンプレートを作成または変更します。

   - テンプレートを作成するには、[情報漏えい対策テンプレート] のツールバーで [追加] をクリックします。
   - テンプレートを変更するには、テンプレート名をクリックします。

3. [名前] にテンプレート名を入力します。

4. (オプション) [説明] にテンプレートの説明を入力します。

5. [条件文] の ⊞ コントロールの横にあるドロップダウンボックスから、条件の [パターン] または [キーワードリスト] を選択します。

6. 選択した条件の横にあるドロップダウンボックスから、パターンまたはキーワードリストを選択します。

7. 条件として [パターン] を追加する場合は、[出現件数] に、テンプレートの処理を実行する条件となる件数を入力します。指定したパターンがメール内にこの件数以上検出されると、InterScan で処理が実行されます。

   注意

   [出現件数] の値は必ず指定する必要があります。0 や空白にすることはできません。

8. 条件を追加するには、[+] コントロールをクリックします。条件を削除するには、[−] コントロールをクリックします。
9. テンプレート定義を複数追加する場合は、[条件文] リストの条件の横にあるドロップダウンボックスから [および] または [または] を選択します。
10. [テンプレート定義] リストに条件を追加するには、[追加] をクリックします。条件文をクリアするには、[クリア] をクリックします。
11. 条件を複数追加する場合は、[テンプレート定義] リストのテンプレート定義の横にあるドロップダウンボックスから [および] または [または] を選択します。
12. [テンプレート定義] リストから定義を削除するには、定義の右にある削除アイコン ( ) をクリックします。
13. [保存] をクリックします。

    [情報漏えい対策テンプレート] 画面が表示され、情報漏えい対策テンプレートリストの一番下に新しいテンプレートが表示されます。

情報漏えい対策テンプレートの削除

注意

組み込みの情報漏えい対策テンプレートや、企業のポリシーに関連付けられているテンプレートは削除できません。テンプレートを削除する前に、すべてのポリシーからそのテンプレートを削除してください。

手順

1. 左側のナビゲーションバーで、[情報漏えい対策] > [情報漏えい対策テンプレート] の順にクリックします。

   テンプレートのリストが表示されます。
2. 削除するテンプレートの横にあるチェックボックスをオンにします。
3. [情報漏えい対策テンプレート] のツールバーで [削除] をクリックします。

情報漏えい対策テンプレートのインポート

管理者は、事前に定義されたルールの一貫性を組織全体で維持するために、情報漏えい対策テンプレートを他の InterScan サーバや他のトレンドマイクロ製品からインポートすることができます。

手順

1. 左側のナビゲーションバーで、[情報漏えい対策] > [情報漏えい対策テンプレート] の順にクリックします。

   テンプレートのリストが表示されます。

2. [情報漏えい対策テンプレート] のツールバーで [インポート] をクリックします。

   注意

   各テンプレートには一意の ID 値が含まれています。同じ ID のテンプレートがすでに存在する場合は、InterScan により、既存のテンプレートが上書きされます。同じ表示名のテンプレートがすでに存在する場合は、既存のテンプレートに「Original」というサフィックスが付加され、新しいテンプレートがリストに追加されます。

   [情報漏えい対策テンプレートのインポート] 画面が表示されます。

3. [参照...] ボタンをクリックし、インポートするテンプレートファイルを探して選択します。[開く] をクリックします。

   注意

   テンプレートファイルは DAT 形式で保存されます。

4. [インポート] をクリックしてテンプレートファイルをインポートします。

情報漏えい対策テンプレートのエクスポート

事前に定義されたルールの一貫性を組織全体で維持するために、テンプレートを他の InterScan サーバや他のトレンドマイクロ製品にエクスポートすることができます。

手順

1. 左側のナビゲーションバーで、[情報漏えい対策] > [情報漏えい対策テンプレート] の順にクリックします。

   テンプレートのリストが表示されます。

2. エクスポートするテンプレートの名前の横にあるチェックボックスをオンにします。

3. [情報漏えい対策テンプレート] のツールバーで [エクスポート] をクリックします。

   [ファイルのダウンロード] ダイアログが表示されます。

4. [保存] をクリックします。

   [名前を付けて保存] ダイアログが表示されます。

5. エクスポートファイルの名前と場所を選択します。[保存] をクリックします。

注意

テンプレートファイルは DAT 形式で保存されます。

情報漏えい対策ポリシーについて

情報漏えい対策ポリシーでは、ネットワーク上の機密情報のフローを監視できます。情報漏えい対策テンプレートを使用して、ポリシールールでネットワーク上の機密データの配信を管理することができます。管理者はポリシーを、企業全体、グループ、または特定のエンドポイントに適用できます。

ポリシーは受信と送信の両方のメールトラフィックに適用できます。また、メッセージの特定の部分を指定することもできます。ポリシー設定では、特定のグループまたはユーザを検索から除外したり、特定のインシデント対応処理を定義したりできます。

InterScan では、情報漏えい対策ポリシー管理が Apex Central に統合されています。管理者は、Apex Central コンソールから会社の情報漏えい対策ポリシ

ーを作成および管理して、その設定を Apex Central に登録されたすべての InterScan サーバに配信できます。

リアルタイム情報漏えい対策の有効化

情報漏えい対策が有効になっている場合、個々の情報漏えい対策ポリシーを有効または無効にすることができます。緑色のチェックマークアイコン () はそのポリシーが有効になっていることを示し、赤色の×印 () はそのポリシーが無効になっていることを示します。アイコンをクリックして、有効と無効を切り替えられます。

手順

1. メインメニューで [情報漏えい対策] > [情報漏えい対策ポリシー] の順にクリックします。

   [情報漏えい対策ポリシー] 画面が表示されます。

2. [トランスポートレベルでの情報漏えい対策を有効にする] を選択します。

3. [ポリシーの適用先] ドロップダウンで、ポリシーの適用先として [送信メッセージ] または [すべてのメッセージ] を選択します。

4. [デジタル資産の検出] ドロップダウンで、デジタル資産の照合方法を選択します。

   - 単一のメッセージ部分 – 各メッセージ部分で別々にデジタル資産が識別されます。

     たとえば、「カナダ: カード名義人情報」というテンプレートのトリガの 1 つが、クレジットカード番号が 5 件検出されることであるとします。[単一のメッセージ部分] を選択すると、同じメッセージ部分でクレジットカード番号が 5 件検出された場合にポリシーがトリガされます。

   - 複数のメッセージ部分 – 選択したすべてのメッセージ部分でデジタル資産が識別されます。

     たとえば、「カナダ: カード名義人情報」というテンプレートのトリガの 1 つが、クレジットカード番号が 5 件検出されることであるとします。[複数のメッセージ部分] を選択すると、選択したすべてのメッセージ部分でクレジットカード番号が照合され、たとえばメッセ

ージ本文で 2 件、メッセージの添付ファイルで 3 件のクレジットカード番号が検出された場合に、テンプレートがトリガされます。

5. [保存] をクリックします。

グローバル設定

InterScan では、隔離を使用して、該当するメッセージを隔離ディレクトリに移動し、対象のファイルを置き換え、残りのメッセージを元の受信者に配信します。

InterScan では、ポリシーイベントが検出されたときに、メールを隔離またはバックアップするように設定できます。[処理設定] 画面から隔離またはバックアップ用のフォルダを各ポリシーに対して個別に設定するか、またはグローバルディレクトリを指定できます。

隔離またはバックアップ用のグローバルディレクトリを指定すると、InterScan では、ポリシーイベントの結果として隔離またはバックアップするすべてのファイルを、指定したディレクトリに移動します。

グローバルな詳細検索処理の詳細については、97 ページの「検出時の処理の詳細オプション」を参照してください。

[グローバル設定] を設定するには、[情報漏えい対策] > [情報漏えい対策ポリシー] > [グローバル設定] の順にクリックします。

注意

[すべてのルールに適用] をクリックして、新しいディレクトリを設定する必要があります。[保存] をクリックしても、InterScan では入力したディレクトリパスが保存されるだけで、適用されません。

情報漏えい対策ポリシーの設定

情報漏えい対策ポリシーは、メールに機密情報が見つかったときに InterScan で実行する処理を定義します。

新規ポリシーを作成する場合は、[情報漏えい対策] > [情報漏えい対策ポリシー] > [追加] を順にクリックします。

既存のポリシーを変更する場合は、[情報漏えい対策] > [情報漏えい対策ポリシー] > [情報漏えい対策ポリシー名] を順にクリックします。

情報漏えい対策ポリシーを設定するには、次の 5 つの手順を実行します。

1. 164 ページの「アカウントの選択」
2. 166 ページの「情報漏えい対策対象の設定」
3. 167 ページの「情報漏えい対策処理の設定」
4. 168 ページの「情報漏えい対策通知の設定」
5. 169 ページの「情報漏えい対策ポリシーの有効化」

アカウントの選択

手順

1. [情報漏えい対策] > [情報漏えい対策ポリシー] を順に選択して、[情報漏えい対策ポリシー] 画面に移動します。
2. ポリシーまたは除外を追加または編集します。
   - 新規のポリシーまたは除外の場合:

     [追加] をクリックします。
   - 既存のポリシーまたは除外の場合:
     a. ポリシー名または除外名をクリックします。
     b. [アカウント] タブをクリックします。
3. ポリシー検索の対象とする送信者または受信者を選択します。
   - 新規ポリシーの作成中:
     a. アカウントの種類を選択します。
        - 任意の送信者から任意の受信者
        - 特定の送信者から任意の受信者
        - 任意の送信者から特定の受信者

- 特定の送信者から特定の受信者

b. [特定の送信者] または [特定の受信者] リンクをクリックします (該当する場合)。

- ポリシーの編集中:

a. アカウントの種類を選択します。

- すべて
- 特定の送信者
- 特定の受信者
- 特定の送信者と受信者

選択したアカウントの種類に該当するアカウントにのみポリシーが適用されます。別のアカウントの種類に該当するアカウントを選択した場合、そのアカウントにはポリシーは適用されません。

b. 表内の [編集] リンクをクリックして、このポリシーを適用するアカウントと除外するアカウントを変更します。

4. 次のいずれかを選択します。
   - すべて — このポリシーまたは除外をすべてのユーザに適用します。
   - 特定のアカウント — Active Directory グループまたは InterScan 特定グループから選択します。
5. Active Directory のユーザ/グループ/連絡先/特定グループ内で検索して、これらを選択して [選択されたアカウント] リストに追加します。
6. Active Directory のユーザ/グループ/連絡先/特定グループを検索して選択し、[アカウントの除外] 画面の [選択されたアカウント] リストに追加します。

情報漏えい対策対象の設定

手順

1. 次のいずれかに移動して、[情報漏えい対策ポリシー] 画面を表示します。
   - リアルタイム検索の場合: [情報漏えい対策] > [情報漏えい対策ポリシー]
   - 手動検索の場合: [手動検索] > [情報漏えい対策]
   - 予約検索の場合: [予約検索] > [追加] または [編集] > [情報漏えい対策]
2. ポリシーまたは除外を追加または編集します。
   - 新規のポリシーまたは除外の場合:
     a. [追加] をクリックします。
     b. [ルールの指定] 画面に移動します。
   - 既存のポリシーまたは除外の場合:
     a. ポリシー名または除外名をクリックします。
     b. [対象] タブをクリックします。
3. 検索対象に含めるメール領域のチェックボックスをオンにします。

   選択可能な対象は次のとおりです。
   - ヘッダ ([送信者]、[送信先]、および [Cc])
   - 件名
   - 本文
   - 添付ファイル
4. 利用可能なテンプレートのリストからテンプレートを選択し、[追加 >>] をクリックしてテンプレートをポリシーに適用します。

注意

情報漏えい対策ポリシーを有効にするには、テンプレートを少なくとも 1 つは選択する必要があります。

5. 新しいテンプレートを作成するには、[使用可能な情報漏えい対策テンプレート] ツールバーで [追加] をクリックします。テンプレートファイルをインポートするには、[インポート] をクリックします。

   テンプレートの追加の詳細については、157 ページの「情報漏えい対策テンプレートの定義」を参照してください。

   テンプレートのインポートの詳細については、160 ページの「情報漏えい対策テンプレートのインポート」を参照してください。

情報漏えい対策処理の設定

手順

1. 次のいずれかに移動して、[情報漏えい対策ポリシー] 画面を表示します。
   - リアルタイム検索の場合: [情報漏えい対策] > [情報漏えい対策ポリシー]
   - 手動検索の場合: [手動検索] > [情報漏えい対策]
   - 予約検索の場合: [予約検索] > [追加] または [編集] > [情報漏えい対策]
2. ポリシーまたは除外を追加または編集します。
   - 新規のポリシーまたは除外の場合:
     a. [追加] をクリックします。
     b. [処理の指定] 画面に移動します。
   - 既存のポリシーまたは除外の場合:
     a. ポリシー名または除外名をクリックします。
     b. [処理] タブをクリックします。
3. 望ましくないコンテンツを検出したときに InterScan が実行する処理を選択します。
4. 指定したユーザに通知するには、次の操作を行います。
   - [送信者の管理者に転送する] チェックボックスをオンにします。

- [特定のメールアドレスに転送する] チェックボックスをオンにし、受信者のメールアドレスを入力します。

5. 処理が実行されたときの動作として、[通知する] または [通知しない] を選択します。
6. 必要に応じて [詳細オプション] を設定します。

情報漏えい対策通知の設定

手順

1. 次のいずれかに移動して、[情報漏えい対策ポリシー] 画面を表示します。
   - リアルタイム検索の場合: [情報漏えい対策] > [情報漏えい対策ポリシー]
   - 手動検索の場合: [手動検索] > [情報漏えい対策]
   - 予約検索の場合: [予約検索] > [追加] または [編集] > [情報漏えい対策]
2. ポリシーまたは除外を追加または編集します。
   - 新規のポリシーまたは除外の場合:
     a. [追加] をクリックします。
     b. [通知の指定] 画面に移動します。
   - 既存のポリシーまたは除外の場合:
     a. ポリシー名または除外名をクリックします。
     b. [通知] タブをクリックします。
3. InterScan で通知するユーザに対応するチェックボックスをオンにします。
4. [詳細の表示] をクリックして、その受信者の通知をカスタマイズします。
5. 通知オプションの中から選択します。

   詳細については、100 ページの「通知設定」を参照してください。

6. [Windows イベントログに書き込む] チェックボックスをオンにして、Windows のイベントログに通知が記録されるように設定します。

情報漏えい対策ポリシーの有効化

手順

1. 次のいずれかに移動して、[情報漏えい対策ポリシー] 画面を表示します。
   - リアルタイム検索の場合: [情報漏えい対策] > [情報漏えい対策ポリシー]
   - 手動検索の場合: [手動検索] > [情報漏えい対策]
   - 予約検索の場合: [予約検索] > [追加] または [編集] > [情報漏えい対策]
2. ポリシーを有効にする前に、追加または編集します。
   - 新規ポリシーの場合:
     a. [追加] をクリックします。
     b. [名前と優先度] 画面に移動します。
   - 既存のポリシーの場合:

     ポリシー名をクリックします。
3. このポリシーまたは除外を有効にします。
4. このポリシーの名前を [ポリシー名] に入力します。
5. 優先度を指定します。
   - 新規ポリシーの場合:

     このポリシーの優先度を [優先度] に入力します。
   - 既存のポリシーの場合:
     a. リスト内のポリシー名または除外名の横にあるチェックボックスをオンにします。

b. [優先度の再設定] をクリックします。

c. [優先度] フィールドに、優先度を数字で入力します。

d. [優先度を保存] をクリックします。

6. [保存] をクリックします。

第 11 章

スパムメール対策の設定

この章では、Exchange 環境を保護するためのスパムメール対策を設定する方法について説明します。

内容は次のとおりです。

スパムメール対策について

トレンドマイクロのスパムメール対策サービスは、スパムメールを阻止して、スパムメールがメールクライアントに届くのを防ぎます。スパムメール対策の仕組みは次のとおりです。

- 受信メールを既知のスパムメールのリストとリアルタイムで照合します。
- 一連の論理的推測に基づいて、そのメールがスパムメールの特性を持っているかどうかを判断します。

スパムメールの送信者が手法を変更した場合でも、スパムメール対策はスパムメールと正当なメールを見分けることができます。トレンドマイクロのスパムメール対策では、特許出願中のヒューリスティックテクノロジを使用して、複数のメール特性に基づいて既存のメールと新しいメールを評価、識別、および監視することで、極めて正確にスパムメールを検出できます。誤検出を少なくするために、高度な動作評価アルゴリズムを使用して、特定のメールがスパムメールである確率を計算します。

InterScan には、スパムメールをフィルタするために、メールレピュテーションとコンテンツ検索という 2 つの強力な機能が備わっています。

スパムメールフォルダの設定

重要

エンドユーザメール隔離のスパムメールフォルダは、Exchange Server 2013 環境でのみ使用できます (迷惑メールフォルダも使用可能)。Exchange Server 2016 および 2019 では、迷惑メールフォルダのみを使用できます。

- トレンドマイクロのスパムメールフォルダ

  InterScan をインストールした Exchange サーバ上のすべてのメールボックスに、スパムメールフォルダが作成されます。InterScan のインストール時に、インストールプログラムによって、このフォルダの名前を指定するように指示され、指定した名前のフォルダが作成されます。

  インストール後に、Microsoft Outlook を使用してスパムメールフォルダの名前を変更できます。トレンドマイクロでは、このフォルダをフォルダ名ではなく ID で識別しています。

- スパムメール検出レベル

  InterScan では、スパムメール検出レベルの初期設定も行われます。スパムメール検出レベルは、Exchange サーバに着信するスパムメールをフィルタ処理するレベルです。

  - 高 — 最も厳しいスパムメール検出レベルです。InterScan は不審ファイルやテキストについてすべてのメールを監視しますが、誤検出の可能性が高くなります。誤検出とは、実際は正当なメールが InterScan によってスパムメールとしてフィルタされることです。
  - 中 — InterScan は高いスパムメール検出レベルで監視し、誤検出となる可能性は中程度になります。
  - 低 — これが初期設定になります。これは最も緩やかなスパムメール検出レベルです。InterScan は最も明確で一般的なスパムメールだけをフィルタします。誤検出の可能性は非常に低くなります。

メールレピュテーションについて

InterScan は、スパムメール対策の一部としてメールレピュテーション機能を提供しています。トレンドマイクロのメールレピュテーションは、防御の最前線でスパムメールを阻止することで、スパムメールがネットワークに氾濫してシステムリソースに負荷をかけることを防止します。

メールサーバは、別のメールサーバからの初期接続を受け入れると、その接続の要求元コンピュータの IP アドレスを記録します。メールサーバはその DNS サーバに照会し、それを受けて DNS サーバはレピュテーションデータベースに照会して、要求元コンピュータの IP アドレスの記録が存在するかどうかを確認します。このホストがデータベースに登録されている場合、メールレピュテーションは適切な処理を推奨します。処理をカスタマイズすることもできます。

トレンドマイクロのメールレピュテーション (標準)

このサービスは、要求された IP アドレスをトレンドマイクロのレピュテーションデータベースと照合して検証することで、スパムメールをブロックします。このレピュテーションデータベースは、トレンドマイクロの Threat Prevention Network によって運用されています。このデータベースは絶えず拡張され、現時点で 10 億件を超える IP アドレスが登録されており、各 IP アドレスにスパムメール活動に基づいてレピュテーションレーティングが割り

当てられています。トレンドマイクロのスパムメール調査担当者は、これらのレーティングを継続的に確認および更新することでレーティングの精度を維持しています。

メールレピュテーション標準サービスは、DNS シングルクエリベースのサービスです。指定されたメールサーバは、不明なホストからメールを受信するたびに、標準評価データベースサーバに DNS クエリを送信します。このホストが標準評価データベースに登録されている場合、メールレピュテーションはそのメールをスパムメールとして報告します。メールレピュテーションから提供されるスパムメール識別情報に基づいて、そのメールに適切な処理を実行するように、メッセージ転送エージェント (MTA) を設定できます。

ヒント

トレンドマイクロ標準評価データベースに登録されている IP アドレスからのメールはすべて、受信せずにブロックするようにメッセージ転送エージェント (MTA) を設定することをお勧めします。

トレンドマイクロのメールレピュテーション (詳細)

このサービスは、スパムメールの送信元が何百万通ものメールを送信しようとしている段階で、これらの送信元を特定してスパムメールを阻止します。これは、動的なリアルタイムのスパムメール対策ソリューションです。このサービスを提供するために、トレンドマイクロはネットワークとトラフィックパターンを絶えず監視して、新たなスパムメール送信元が発生するたびに、スパムメールの最初の兆候から通常数分以内に動的評価データベースをアップデートします。スパムメール活動の形跡が見られなくなると、動的評価データベースはそれに応じてアップデートされます。

メールレピュテーション標準と同様に、メールレピュテーション詳細は DNS クエリベースのサービスですが、2 つのクエリを標準評価データベースと動的評価データベース (リアルタイムで動的にアップデートされるデータベース) という 2 種類のデータベースに発行できる点が異なります。これらの 2 つのデータベースにはそれぞれ異なるエントリが格納されているため (重複する IP アドレスはありません)、トレンドマイクロは、次々と変わるスパムメール送信元に素早く対応できる非常に効率的で効果的なデータベースを維持できます。メールレピュテーション詳細サービスは、お客さまのネットワーク内の総受信接続 (すべて不正な接続) のうち 80%超をブロックしています。結果は、受信メールメッセージストリームに占めるスパムメールの比率に応じて

異なります。受信するスパムメールが多いほど、ブロックされる接続の比率が高まります。

メールレピュテーションの有効化

メールレピュテーションでは、世界でも有数の規模を誇る信頼性の高い評価データベースおよび動的評価データベースとの照合によって受信メールの IP アドレスをチェックし、新しいスパムメールやフィッシングの送信元を特定します。さらに、感染ファイルやボットネットを最初の出現時にブロックします。

手順

1. [スパムメール対策] > [メールレピュテーション] を順に選択して、[メールレピュテーション] 画面に移動します。
2. [メールレピュテーションを有効にする] を選択します。
3. [保存] をクリックします。

メールレピュテーションの対象の設定

手順

1. [スパムメール対策] > [メールレピュテーション] を順に選択して、[メールレピュテーション] 画面に移動します。
2. 次の設定を行います。
   - Trend Micro Smart Protection Network ポータル — グローバルスパムメール情報とレポートの表示、承認するおよびブロックする送信者 IP アドレスリストの作成または管理、管理タスク、およびトレンドマイクロのメールレピュテーション Web サイトからのサービスの設定を実行します。
   - 追加 —IP アドレスを入力してこのボタンをクリックすると、その IP アドレスが承認する IP アドレスのリストに追加されます。
3. [保存] をクリックします。

メールレピュテーションの処理の設定

[対象] タブの [サービスレベル] で [標準] を選択した場合は、[標準評価データベース処理] のオプションのみが表示されます。[対象] タブの [サービスレベル] で [詳細] を選択した場合は、両方のデータベースが使用されるため、[標準評価データベース処理] と [動的評価データベース処理] が表示されます。両方の処理のボックスが表示された場合は、各データベースで検出される内容に対して別々の処理を指定します。

手順

1. [スパムメール対策] > [メールレピュテーション] を順に選択して、[メールレピュテーション] 画面に移動します。
2. [処理] タブをクリックします。
3. [標準評価データベース処理] で次のいずれかを選択します。
   - 推奨処理 — 標準評価データベースで一致した IP アドレスからの接続を拒否。

     (任意) SMTP エラーコードを入力して、カスタムエラーメッセージを入力します。
   - エラーメッセージのない接続を閉じる — 接続を終了します。
   - 放置 — ログに記録せずに放置します。
4. (任意) [詳細] を選択した場合は、[動的評価データベースの処理] に次のいずれかを選択します。
   - 推奨処理 — 動的評価データベースで一致した IP アドレスからの接続を拒否。

     (任意) SMTP エラーコードを入力して、カスタムエラーメッセージを入力します。
   - エラーメッセージのない接続を閉じる — 接続を終了します。
   - 放置 — ログに記録せずに放置します。
5. [保存] をクリックします。

コンテンツ検索について

InterScan では、望ましくないコンテンツを検索するときや、メールを自動的に承認またはブロックするときに、トレンドマイクロのスパムメール対策エンジンを使用してヒューリスティックベースのポリシーを適用します。InterScan のインストール時にエンドユーザメール隔離ツールをインストールすることを選択した場合は、InterScan のインストール先の Exchange サーバにあるすべてのメールボックスにスパムメールフォルダが作成されます。

コンテンツ検索では、承認する送信者リスト、ブロックする送信者リスト、スパムメールフィルタを使用して、メッセージがスパムメールであるかどうかを検査します。

スパムメール対策エンジンとスパムメール判定ルール

InterScan では、トレンドマイクロスパムメール対策エンジンおよびトレンドマイクロスパムメール判定ルールを使用してスパムメールを検出し、これに対処します。トレンドマイクロは、エンジンとパターンファイルを頻繁にアップデートし、これらをダウンロードできるようにしています。InterScan では、手動アップデートまたは予約アップデートによりこれらのコンポーネントをダウンロードできます。

スパムメール対策エンジンは、スパムメールシグネチャおよびヒューリスティックルールを使用してメールを検査します。ここではメールを検索し、ルールのパターンにどれだけ一致しているかにより、それぞれのメッセージにスコアを割り当てます。InterScan はスパムメールスコアをユーザが定義したスパムメール検出レベルと比較します。スパムメールスコアが検出レベルを超えた場合、InterScan はそのスパムメールに対して処理を実行します。ユーザは、スパムメール対策エンジンがスパムメールスコアの割り当てに使用する方法を変更できませんが、スパムメールであるかどうかを判定するために InterScan で使用される検出レベルを調整することはできます。

たとえば、多くのスパムメール送信者は、そのメール内に多くの感嘆符、または複数の連続した感嘆符 (!!!!) を使用します。InterScan は、このように感嘆符を多用するメッセージを検出すると、そのメールのスパムメールスコアを上げます。

エンドユーザメール隔離

インストールの際、Microsoft Exchange 用に各エンドユーザのサーバ側のメールボックスにフォルダを追加できます。インストール時にスパムメールフォルダに名前を付け、保存期限を設定します。スパムメールフォルダの名前は「スパムメール」とすることをお勧めします。スパムメールが検出されると、システムは InterScan であらかじめ定義されているスパムメールフィルタルールに従って、メッセージをこのフォルダに隔離します。エンドユーザはこのスパムメールフォルダを参照して、不審メールを開いたり、参照したり、削除したりすることができます。

エンドユーザはスパムメールフォルダに隔離されたメールを開くことができます。このようなメッセージを開くと、実際のメール上に [送信者の承認] と [承認済み送信者リストの表示] の 2 つのボタンが表示されます。[送信者の承認] をクリックすると、InterScan はメッセージをローカルの受信トレイに移動し、メッセージの送信者アドレスを個人の [承認済み送信者リスト] に追加し、ログにイベントを記録します (管理者は後からレポート内でこのログを参照可能)。[承認済み送信者リストの表示] をクリックすると、別の画面が表示され、エンドユーザはここで承認する送信者リストを名前またはドメイン別に表示および変更できます。Exchange サーバはエンドユーザの承認する送信者リストにあるアドレスからのメッセージを受信すると、メッセージのヘッダまたは内容にかかわらず、これらをエンドユーザの受信トレイに配信します。

InterScan は、管理者にも承認する送信者とブロックする送信者リストを提供します。InterScan では、エンドユーザのリストを確認する前に、管理者の承認する送信者とブロックする送信者リストを適用します。

承認する送信者リストおよびブロックする送信者リスト

InterScan では、承認する送信者リストのアドレスは、フィッシングが検出された場合を除き、スパムメールとして分類されることはなく、このリストのメッセージがスパムメールとしてフィルタされることもありません。また InterScan では、ブロックする送信者リストのアドレスはフィルタされ、常にスパムメールとして分類されます。そして管理者により設定されたルールに応じて処理が実行されます。

注意

Exchange 管理者は、Exchange サーバに対して個別に承認する送信者とブロックする送信者のリストを管理します。エンドユーザが承認する送信者を作成しても、その送信者が管理者のブロックする送信者リストに記載されている場合は、InterScan はこのブロックする送信者からのメッセージをスパムメールとして検出し、これらのメッセージに対する処理を実行します。

スパムメールフィルタ

管理者は、スパムメールをフィルタで排除するためのスパムメール検出レベルを設定します。検出レベルが高いほど、より多くの不審メッセージがスパムメールとして分類されます。

検出レベルにより、InterScan が不審メールに対してどれだけ寛容であるかが決定されます。検出率が高い場合、ほとんどのメールがスパムメールとして隔離されるため、誤って正当なメールをスパムメールとして特定および隔離し、「誤検出」スパムメールを生成してしまう場合もあります。検出率が低い場合、厳密にメールを検査することはありませんが、多くの「誤検出」スパムメールを生成することもありません。

新しいスパムメール送信元

コンテンツ検索では、Web レピュテーションサービスを併用することで、新しいスパムメール送信元を識別できます。[新しいスパムメール送信元の検出を有効にする] を有効にした場合、URL を含むメールを受信すると次の処理が実行されます。

1. Web レピュテーションサービスによって URL のレピュテーションスコアが特定されます。
2. 設定済みの内部ゲートウェイ MX レコードまたは IP アドレスリストを使用して、メールの送信者 IP アドレスが特定されます。
3. メールレピュテーションサービスによって、送信者 IP アドレスのレピュテーションスコアが特定されます。

コンテンツ検索では、メールに含まれている URL と送信者 IP アドレスの両方のレピュテーションスコアを使用して、メールのリスクレベルが特定されます。

重要

新たなスパムメール送信元を検出するには、Web レピュテーションサービスを有効にする必要があります。

コンテンツ検索の有効化

InterScan は、リアルタイムでスパムメールを検出し、Exchange クライアントを保護するための処理を実行します。承認する送信者リストには、ブロックする送信者リストよりも高い優先度が割り当てられています。あるメールアドレスが、承認する送信者リストとブロックする送信者リストの両方に含まれている場合、InterScan では、そのメールアドレスからのメールはスパムメールとして分類されません。

手順

1. [スパムメール対策] > [コンテンツ検索] の順に選択して、[コンテンツ検索] 画面に移動します。
2. [コンテンツ検索を有効にする] を選択します。
3. [保存] をクリックします。

コンテンツ検索の対象の設定

手順

1. [スパムメール対策] > [コンテンツ検索] の順に選択して、[コンテンツ検索] 画面に移動します。
2. [対象] タブをクリックします。
3. 検出レベルを選択します。
   - 高 — 最も厳しいスパムメール検出レベルです。InterScan は不審ファイルやテキストについてすべてのメールを監視しますが、誤検出の可能性が高くなります。誤検出とは、実際は正当なメールが InterScan によってスパムメールとしてフィルタされることです。
   - 中 — InterScan は高いスパムメール検出レベルで監視し、誤検出となる可能性は中程度になります。

- 低 – これが初期設定になります。これは最も緩やかなスパムメール検出レベルです。InterScan は最も明確で一般的なスパムメールだけをフィルタします。誤検出の可能性は非常に低くなります。

4. 新たなスパムメール送信元の可能性がある URL を含むメールを検索するには、[新しいスパムメール送信元の検出を有効にする] を選択します。

重要

新たなスパムメール送信元を検出するには、Web レピュテーションサービスを有効にする必要があります。詳細については、196 ページの「Web レピュテーションの有効化」を参照してください。

新たなスパムメール送信元の詳細については、179 ページの「新しいスパムメール送信元」を参照してください。

- 会社の MX レコードを特定し、[組織の MX レコード] リストに追加します。
- 会社のメールゲートウェイ IP アドレスを特定し、[組織のメールゲートウェイ IP アドレス] リストに追加します。

5. スパムメールとして処理しないメールメッセージの送信元の IP アドレスを追加します。
6. [承認する送信者] および [ブロックする送信者] のリストにメールアドレスまたはドメイン名を追加します。
7. [保存] をクリックします。

コンテンツ検索の処理の設定

手順

1. [スパムメール対策] > [コンテンツ検索] の順に選択して、[コンテンツ検索] 画面に移動します。
2. [処理] タブをクリックします。
3. スパムメールに対する処理として次のいずれかを選択します。

- ユーザのスパムメールフォルダにメッセージを隔離
  - メールがユーザのスパムメールフォルダに隔離されたときに他のフィルタを使用して検索を続ける: メールがスパムとして検出され、ユーザのスパムメールフォルダに隔離された場合も、他のフィルタを使用してメールの検索を続けるには、このオプションを選択します。
- メッセージ全体の削除
- タグを付加して配信
- 放置

使用できる処理の詳細については、87 ページの「InterScan の処理について」を参照してください。

4. [保存] をクリックします。

第 12 章

高度なスパムメール対策の設定

この章では、Exchange 環境を保護するための高度なスパムメール対策を設定する方法について説明します。

内容は次のとおりです。

高度なスパムメール対策について

高度なスパムメール対策では、検索モードと InterScan のビジネスメール詐欺 (BEC) 機能の設定が可能です。

高度なスパムメール対策の検索モードには、コンサバティブモードとアグレッシブモードがあります。アグレッシブモードでは隔離された仮想環境でコンテンツを検索するために仮想アナライザが必要であるのに対し、コンサバティブモードでは仮想アナライザを使用せずに他の方法でコンテンツを検索します。

InterScan のビジネスメール詐欺 (BEC) 機能は、高プロファイルユーザ (企業の経営陣など) を装ったメールによる潜在的な詐欺や攻撃を検出します。

ビジネスメール詐欺について

ビジネスメール詐欺 (BEC) は、同一または類似のアカウント名を使用し、高プロファイルユーザの識別情報を詐称して不正に電信送金を行う詐欺攻撃です。通常、攻撃者は企業の経営幹部を装い、標的が攻撃者の口座に送金するように仕向けます。BEC 詐欺はメールの中間者詐欺とも呼ばれ、国外のクライアントに定期的に電信送金を行う企業がよく標的となります。この攻撃には、不正プログラム、ソーシャルエンジニアリング、またはその両方が利用されることがあります。詳細については、FBI による情報サイトの記事を参照してください。

InterScan for Microsoft Exchange は、スパムメール対策エンジンとの統合により、次の方法で組織を BEC 詐欺から効果的に保護します。

- 指定された高プロファイルユーザのアカウント名を含む外部ネットワークからの受信メールを検索してソーシャルエンジニアリング攻撃をブロックする

InterScan のライティングスタイル検証について

ライティングスタイル検証機能を使用すると、企業のメールのセキュリティが向上します。トレンドマイクロでは、個人のライティングスタイルを固有の「ID」としてデータ処理上扱っています。ライティングスタイルに基づく「ID」は、ユーザのメールデータの履歴に基づいて生成されます。トレンドマイクロは対象ユーザのメールを検索して固有のライティングスタイルを学習し、各ユーザ毎にライティングスタイルモデルを作成します。この情報は本人から送信されたものであるかどうかの判断に利用されます。

注意

このリリースでは、ライティングスタイル検証機能は英語で書かれたメールにのみ適用されます。

高度なスパムメール対策の設定

高度なスパムメール対策の有効化

手順

1. メインメニューで [高度なスパムメール対策] > [高度なスパムメール対策] を選択します。

   [高度なスパムメール対策] 画面が表示されます。

2. [高度なスパムメール対策] 画面で [高度なスパムメール対策を有効にする] を選択します。

3. [保存] をクリックします。

高度なスパムメール対策検索の対象の設定

手順

1. メインメニューで [高度なスパムメール対策] > [高度なスパムメール対策] を選択します。

2. [対象] タブに移動します。

   [対象] タブが表示されます。

3. 不審なメッセージを仮想アナライザに送信して潜在的な脅威をより多く検出したい場合は、[高度なスパムメールに対してアグレッシブモードを有効にする] リンクをクリックして機能の設定を行います。

   この機能を使用するには、仮想アナライザを設定して登録しておく必要があります。詳細については、230 ページの「仮想アナライザの設定」を参照してください。

4. BEC 詐欺に対する保護を有効にするには、[ビジネスメール詐欺チェック] を選択し、次の手順を実行します。
   a. [Active Directory のユーザアカウント] フィールドで、Active Directory の高プロファイルユーザを検索します。
   b. [追加] をクリックして、ユーザを右側の [高プロファイルユーザ] リストに追加します。
5. InterScan でフィッシングの検出を有効にする場合は、[フィッシングの検出を有効にする] オプションを選択します。
6. [保存] をクリックします。

高度なスパムメール対策検索の処理の設定

手順

1. メインメニューで [高度なスパムメール対策] > [高度なスパムメール対策] を選択します。

   [高度なスパムメール対策] 画面が表示されます。
2. [処理] タブをクリックします。
3. 望ましくないコンテンツを検出したときに InterScan が実行する処理を選択します。
   - 分析されたカテゴリ
     - メッセージをユーザのスパムメールフォルダに隔離
       - メールがユーザのスパムメールフォルダに隔離されたときに他のフィルタを使用して検索を続ける: メールがスパムとして検出され、ユーザのスパムメールフォルダに隔離された場合も、他のフィルタを使用してメールの検索を続けるには、このオプションを選択します。
     - メッセージ全体の隔離
     - メッセージ全体の削除
     - 件名に次のタグを付加

- 放置
- 推定されるカテゴリ
  - メッセージをユーザのスパムメールフォルダに隔離
  - メッセージ全体の隔離
  - メッセージ全体の削除
  - 件名に次のタグを付加
  - 放置
- フィッシング活動
  - メッセージをユーザのスパムメールフォルダに隔離
  - メッセージ全体の削除
  - タグを付加して配信
  - 放置

使用できる処理の詳細については、87 ページの「InterScan の処理について」を参照してください。

4. 処理が実行されたときの動作として、[通知する] または [通知しない] を選択します。
5. 検索結果を分析のためにトレンドマイクロに送信する場合は、[Trend Micro Smart Protection Network にフィードバックを送信する] を選択します。

注意

このオプションを選択するには、高度なスパムメール対策機能を有効にしておく必要があります。

6. 必要に応じて [詳細オプション] を設定します。

注意

検出時の処理の詳細オプションについては、97 ページの「検出時の処理の詳細オプション」を参照してください。

7. [保存] をクリックします。

高度なスパムメール対策検索の通知の設定

手順

1. メインメニューで [高度なスパムメール対策] > [高度なスパムメール対策] を選択します。

   [高度なスパムメール対策] 画面が表示されます。

2. [処理] タブをクリックし、通知を受け取る内容に応じて、[分析されたカテゴリ] または [推定されるカテゴリ] で [通知する] を選択します。

3. [通知] タブをクリックします。

4. InterScan で通知するユーザに対応するチェックボックスをオンにします。

5. [詳細の表示] をクリックして、その受信者の通知をカスタマイズします。

6. 通知オプションの中から選択します。

   詳細については、100 ページの「通知設定」を参照してください。

7. [Windows イベントログに書き込む] チェックボックスをオンにして、Windows のイベントログに通知が記録されるように設定します。

8. [保存] をクリックします。

ライティングスタイルトレーニングの設定

高プロファイルユーザのライティングスタイル検証を行うには、各ユーザに固有のパターンを分析して学習するために InterScan が必要となります。ライティングスタイル検証機能を使用する前に、InterScan のトレーニングを行う必要があります。

重要

トレンドマイクロは各ユーザに固有のライティングスタイルパターンを学習するためだけにメールを検索しており、実際のメールやそのコンテンツを収集することは一切ありません。

ライティングスタイルの手動トレーニングの実行

手順

1. メインメニューで [高度なスパムメール対策] > [ライティングスタイルトレーニングの設定] を選択します。

   [ライティングスタイルトレーニングの設定] 画面が表示されます。

2. [手動トレーニング] セクションで、[トレーニングの開始] をクリックします。

   InterScan により、設定したユーザのメールのライティングスタイル分析が開始され、画面に進行状況が表示されます。

   対象ユーザを設定するには、トピック 185 ページの「高度なスパムメール対策検索の対象の設定」を参照してください。

   完了する前に処理を停止する場合は、[トレーニングの停止] をクリックします。

ライティングスタイルの通常トレーニングの設定

ユーザのライティングスタイルは時間の経過とともに変化する場合があります。そのため、ユーザのライティングスタイルモデルを定期的にアップデートすることが重要となります。

手順

1. メインメニューで [高度なスパムメール対策] > [ライティングスタイルトレーニングの設定] を選択します。

   [ライティングスタイルトレーニングの設定] 画面が表示されます。

2. [通常トレーニング] セクションで [このサーバで通常トレーニングを有効にする] を選択し、スケジュールを選択します。

   対象ユーザを設定するには、トピック 185 ページの「高度なスパムメール対策検索の対象の設定」を参照してください。

3. [保存] をクリックします。

InterScan が、設定されたスケジュールに従って、設定されたユーザのライティングスタイルを分析します。

ライティングスタイル検証の設定

ライティングスタイル検証の有効化

重要

[ライティングスタイル検証の設定] を設定する前に、[高度なスパムメール対策] 画面で [高度なスパムメール対策] と [ビジネスメール詐欺] 設定を行う必要があります。

手順

1. メインメニューで [高度なスパムメール対策] > [ライティングスタイル検証の設定] をクリックします。

   [ライティングスタイル検証の設定] 画面が表示されます。

2. [ライティングスタイル検証の設定] 画面で [ライティングスタイル検証設定を有効にする] を選択します。

3. [保存] をクリックします。

ライティングスタイル検証の設定

手順

1. メインメニューで [高度なスパムメール対策] > [ライティングスタイル検証の設定] をクリックします。

[ライティングスタイル検証の設定] 画面が表示されます。

2. [通知設定] セクションで、次の通知を設定します。
   - [偽装された可能性のある送信者に通知する]: [詳細の表示] をクリックし、目的の送信者に通知メッセージを送信するために使用するアカウントの設定を行います。
   - [メールメッセージ受信者のディスクレーマーを追加する]: [詳細の表示] をクリックし、外部ドメインから受信したすべての不審メールの先頭に表示するディスクレーマーメッセージを設定します。
   - [セキュリティ/IT 部門に通知する]: [詳細の表示] をクリックし、InterScan が不審メールを検出したときに通知するセキュリティ/IT 部門メンバーのメールアドレスを設定します。
3. [承認する送信者] セクションで、InterScan によるライティングスタイル検証の検索対象から除外する外部ドメインのメールアドレスを設定します。

重要

承認する送信者を設定する際には、特別な注意が表示されます。承認する送信者は InterScan によるメッセージ検索対象から除外されるので、このセクションで設定したメールアドレスが安全で、本当に目的の人物のものであることを確認してください。

第 13 章

Web レピュテーションの設定

この章では、Exchange 環境を保護するための Web レピュテーションサービスを設定する方法について説明します。

内容は次のとおりです。

Web レピュテーションサービスについて

Web レピュテーションサービスは、Web サイトの経過期間、場所の変更履歴、不正プログラムの動作分析で見つかった不審な活動の兆候などの要因に基づいてレピュテーションスコアを割り当てることで、Web ドメインの信頼性を追跡します。その上でサイトの検索を継続的に行い、感染したサイトにユーザがアクセスしないようにブロックします。

不審 Web サイトから組織を保護するために、Web レピュテーションのソース、対象、処理、および通知を設定する必要があります。

C&C コンタクトアラートサービス

トレンドマイクロのコマンド&コントロール (C&C) コンタクトアラートサービスでは、検出およびアラート機能が向上し、APT (標的型サイバー攻撃)やターゲット攻撃によるダメージを軽減できます。C&C コンタクトアラートサービスは Web レピュテーションサービスと統合され、Web レピュテーションのセキュリティレベルに基づいて、検出されたコールバックアドレスに対して実行される処理を決定します。

Web レピュテーションサービスのセキュリティレベル設定の詳細については、196 ページの「Web レピュテーションの対象の設定」を参照してください。

機能	説明
グローバルインテリジェンスリスト	Trend Micro Smart Protection Network は、世界各地のソースからのグローバルインテリジェンスリストを集め、各 C&C コールバックアドレスのリスクレベルをテストし、評価します。Web レピュテーションサービスは、グローバルインテリジェンスリストを不正な Web サイトのレピュテーションスコアとともに使用し、高度な脅威に対するセキュリティを強化します。Web レピュテーションのセキュリティレベルにより、割り当てられたリスクレベルに基づいて不正な Web サイトや C&C サーバに対して実行される処理が決定されます。

機能	説明
仮想アナライザリスト	InterScan は、仮想アナライザからリストを取得し、グローバルインテリジェンスとローカル仮想アナライザリストの両方に照らしてすべての C&C 脅威を評価します。 Deep Discovery Advisor に統合 Smart Protection Server を接続する処理の詳細については、「Smart Protection Server Administrator's Guide」を参照してください (最新版をダウンロードセンターからダウンロードできます)。
C&C のカテゴリ	Web レピュテーションサービスのログに、検出された脅威のカテゴリに関する情報が表示されます。C&C コンタクトアラートサービスで使用されるカテゴリは次のとおりです。 • C&C サーバ: コマンド&コントロール (C&C) サーバやスパイウェアが収集したデータを保管するサーバ (ドロップゾーン) です。 • 不正ドメイン: 悪質な実行コードをホストするドメインです。 • 新規ドメイン: 使い捨てドメインなどの新しく検出されたトレンドマイクロによる分類がまだ行われていないドメインです。 • C&C サーバ (仮想アナライザ): Deep Discovery Analyzer の C&C サーバリストのサーバ/リポジトリです。

Web レピュテーション検索サービスの設定

InterScan では、Web レピュテーションクエリのサーバとして、Trend Micro Smart Protection Network と Trend Micro Smart Protection Server の 2 つを選択できます。

Trend Micro Smart Protection Network と Trend Micro Smart Protection Server の詳細については、73 ページの「Trend Micro Smart Protection ソース」を参照してください。

手順

1. 左側のナビゲーションペインで、[Smart Protection] > [検索サービス設定] の順にクリックします。

   [検索サービス設定] 画面が表示されます。

2. [Web レピュテーションサービス] で、以下を選択します。

a. Trend Micro Smart Protection Network —すべての Web レピュテーションクエリをトレンドマイクロのサーバに送信して確認します。

b. Trend Micro Smart Protection Server —すべての Web レピュテーションクエリをローカルで確認します。ローカルサーバでクエリを確認できない場合は、トレンドマイクロのサーバにクエリが送信されて詳細に分析されます。

3. ローカルソースを設定するには、関連するリンクをクリックします。76 ページの「ローカルソースの設定」を参照してください。

4. [保存] をクリックします。

Web レピュテーションの有効化

手順

1. メインメニューで [Web レピュテーション] を選択します。

   [Web レピュテーション] 画面が表示されます。

2. [Web レピュテーションを有効にする] を選択します。

3. [保存] をクリックします。

Web レピュテーションの対象の設定

手順

1. メインメニューで [Web レピュテーション] を選択します。

   [Web レピュテーション] 画面が表示されます。

2. [対象] タブをクリックします。

3. 次のいずれかのセキュリティレベルを選択します。

   - 高 — Web からの脅威をより多くブロックしますが、誤検出のリスクも高くなります。
   - 中 — Web からの脅威のほとんどをブロックする一方で、誤検出の件数を低く抑えます。

- 低 – ブロックする Web からの脅威の件数は減少しますが、誤検出のリスクも低くなります。

4. [不審 URL がないかメッセージ添付ファイルのコンテンツを検索する] を選択して、メールの添付ファイル内の Web レピュテーション検索を追加します。
5. [URL 分析を有効にする] を選択して、[仮想アナライザ] 画面で URL 分析を設定します。
6. [内部ドメインの URL を放置する] を選択して、組織内のサーバから生成された URL の検索をスキップします。
7. [承認する URL リストを有効にする] を選択して、現在のセキュリティポリシーで安全とみなされる URL の検索を回避します。
8. 承認する URL をリストに追加します。
9. [承認する送信者] のリストにアドレスを追加します。
10. [保存] をクリックします。

Web レピュテーションの処理の設定

手順

1. メインメニューで [Web レピュテーション] を選択します。

   [Web レピュテーション] 画面が表示されます。
2. [処理] タブをクリックします。
3. 望ましくないコンテンツを検出したときに InterScan が実行する処理を選択します。
   - ユーザのスパムメールフォルダにメッセージを隔離

注意

[ユーザのスパムメールフォルダにメッセージを隔離] は、Outlook 迷惑メール対策と統合している場合に外部のネットワークからのメールのみを隔離する処理です。内部のメールは、「不審 URL」のタグが付けられてユーザの受信トレイに配信されます。

- メッセージ全体の隔離
- メッセージ全体の削除
- タグを付加して配信
- 放置

使用できる処理の詳細については、87 ページの「InterScan の処理について」を参照してください。

4. [トレンドマイクロの Web レピュテーションサービスで評価されていない URL に対して処理を実行する] を選択して、不審 URL と分類されていない URL に対して、指定された処理を実行します。

注意

このオプションは、InterScan で [URL 分析] オプションが有効になっている場合は使用できず無効になります。

5. 処理が実行されたときの動作として、[通知する] または [通知しない] を選択します。
6. 必要に応じて [詳細オプション] を設定します。

注意

詳細検索処理の詳細については、97 ページの「検出時の処理の詳細オプション」を参照してください。

7. [保存] をクリックします。

Web レピュテーションの通知の設定

手順

1. メインメニューで [Web レピュテーション] を選択します。

   [Web レピュテーション] 画面が表示されます。

2. [通知] タブをクリックします。

3. InterScan で通知するユーザに対応するチェックボックスをオンにします。
4. [詳細の表示] をクリックして、その受信者の通知をカスタマイズします。
5. 通知オプションの中から選択します。

   詳細については、100 ページの「通知設定」を参照してください。
6. [Windows イベントログに書き込む] チェックボックスをオンにして、Windows のイベントログに通知が記録されるように設定します。

第 14 章

Time-of-Click プロテクションの設定

この章では、Exchange 環境を保護するための Time-of-Click プロテクション機能を設定する方法について説明します。

内容は次のとおりです。

Time-of-Click プロテクションについて

InterScan for Microsoft Exchange では、メールメッセージに含まれる不正な URL に対する Time-of-Click プロテクション機能を利用できます。この機能を有効にすると、InterScan for Microsoft Exchange により、詳しい分析のためにメールメッセージ内の不審な URL が書き換えられます。この URL がクリックされるたびに、書き換えられた URL が Trend Micro Smart Protection Network (SPN) で分析され、URL のリスクレベルに基づいて指定された処理が適用されます。

Time-of-Click プロテクションを有効にする

手順

1. メインメニューで [Time-of-Click プロテクション] を選択します。

   [Time-of-Click プロテクション] 画面が表示されます。

2. [Time-of-Click プロテクション] 画面で [受信メールに対する Time-of-Click プロテクションを有効にする] を選択します。

Time-of-Click プロテクションの設定

[Time-of-Click プロテクション] 画面で、Time-of-Click プロテクションを有効にし、URL の評価に応じた処理を指定します。

手順

1. メインメニューで [Time-of-Click プロテクション] を選択します。
2. [受信メールに対する Time-of-Click プロテクションを有効にする] を選択して、この機能を有効にします。
3. URL 書き換え設定を選択します。
   - [トレンドマイクロの推奨 URL に適用] (初期設定): このオプションを選択すると、メールメッセージ本文に含まれる URL のうち、トレンドマイクロの Web レピュテーションサービスによる評価が「未評価」または「不正」である URL のみが InterScan for Microsoft Exchange で書き換えられます。

- [すべての URL に適用]: : このオプションを選択すると、メールメッセージ本文に含まれるすべての URL が InterScan for Microsoft Exchange によって書き換えられます。

重要

初期設定では、[デジタル署名されたメールメッセージを放置する] 設定は有効になっています。そのため、デジタル署名されたメッセージは Time-of-Click プロテクションで書き換えられません。この設定を無効にした場合、デジタル署名されたメッセージ内の URL が壊れる可能性があります。

4. URL の評価に応じた処理を指定します。

フィールド	説明
危険	危険な URL に対する処理 ([許可]、[警告]、または [ブロック]) を選択します。初期設定の処理は [ブロック] です。 「危険」に分類されるのは、不正であるか脅威の既知の発信源であることが確認されている URL です。
極めて不審	極めて不審な URL に対する処理 ([許可]、[警告]、または [ブロック]) を選択します。初期設定の処理は [ブロック] です。 「極めて不審」に分類されるのは、不正であるか脅威の発信源であることが疑われる URL です。
不審	不審な URL に対する処理 ([許可]、[警告]、または [ブロック]) を選択します。初期設定の処理は [警告] です。 「不審」に分類されるのは、スパムに関連付けられているか、感染している可能性がある URL です。
未評価	未評価の URL に対する処理 ([許可]、[警告]、または [ブロック]) を選択します。初期設定の処理は [警告] です。 トレンドマイクロでは URL の安全性の評価を積極的に進めていますが、ユーザが新しい Web サイトやあまり利用されない Web サイトにアクセスすると未評価のページに遭遇することがあります。未評価のページへのアクセスをブロックすると、安全性は向上しますが、安全なページへのアクセスもブロックされる場合があります。

5. [メッセージ受信者] セクションで、次に挙げた [次の受信者に送信されたメッセージを分析] のオプションのいずれかを選択します。
   - すべて:
     - すべての受信者に送信されたメッセージを分析する場合は、このオプションを選択します。
   - [特定のアカウント]:
     - このオプションを選択した場合は、[詳細の表示] をクリックして、分析対象にする受信者アカウントを検索して指定します。
6. ネットワークの内部ドメインを対象から除外する場合は、[承認する URL リスト] で、[内部ドメインの URL を放置する] を選択します。[内部ドメイン] リストを確認またはアップデートするには、下のリンクをクリックします。

   注意
   [内部ドメインの URL を放置する] オプションは、初期設定では有効になっています。
7. メールメッセージに含まれる特定の URL を [Time-of-Click プロテクション] による検索の対象から除外する場合は、それらの URL を [承認する URL リスト] に追加します。
8. 特定のアドレスまたはドメインから送信されたメールメッセージを InterScan for Microsoft Exchange による検索の対象から除外する場合は、それらのアドレスまたはドメイン名を [承認する送信者] リストに追加します。
9. [保存] をクリックします。

第 15 章

Search & Destroy の設定

この章では、Exchange 環境を保護するための Search & Destroy を設定する方法について説明します。

内容は次のとおりです。

Search & Destroy について

Search & Destroy は、Exchange メールボックスサーバにあるメールボックスコンポーネント (メール、会議、タスクなど) の検索とそれらの削除に使用できます。管理者は、特定のキーワードに一致するユーザ、メールボックス、コンポーネント作成日付などを検索する詳しい検索条件を指定できます。

InterScan では、Search & Destroy 固有のアクセス管理の役割が管理者に用意されています。Search & Destroy にアクセスできるのは、次のいずれかの役割が割り当てられたユーザだけです。

- Search & Destroy 管理者: ユーザのメールボックスと Exchange サーバの両方にある望ましくないコンテンツを検索、監視、および削除できます。
- Search & Destroy オペレータ: ユーザのメールボックスと Exchange サーバの両方にある望ましくないコンテンツを検索および監視できます。

注意

InterScan の初期設定では、管理者を含めどのユーザも Search & Destroy 管理者の役割には割り当てられていません。管理者は、Search & Destroy に対するアクセス権限をユーザに手動で割り当てる必要があります。詳細については、206 ページの「Search & Destroy アクセスアカウントの設定」を参照してください。

Search & Destroy では、管理者が設定した検索基準に基づいてメールボックスコンポーネントのキーワード一致検索を実行し、条件に一致したもののコピーを Exchange 検出メールボックスに保存する Exchange サービスアカウントが採用されています。管理者は、条件に一致したコンポーネントを確認し、そのコンテンツが望ましいものかを判断できます。望ましくないものは、検出メールボックスと、原因となったユーザのメールボックスから削除できます。

Search & Destroy アクセスアカウントの設定

Search & Destroy を使用するためには、使用前に 2 つのアクセスアカウント、Active Directory サービスアカウント、および InterScan の Search & Destroy 管理者を設定する必要があります。

Active Directory サービスアカウントを作成し、Exchange の Discovery Management グループに追加します。InterScan では、このサービスアカウントを使用してバックエンドのメールボックス検索を実行します。

InterScan の Search & Destroy 管理者は、すべての Search & Destroy 機能へのアクセスをユーザに許可する特殊なアカウントです。Search & Destroy 管理者でないユーザ (管理者またはオペレータ) には、Search & Destroy は表示されません。

注意

Search & Destroy 機能は、Exchange 2013、Exchange 2016、または Exchange 2019 が実行されているメールボックスサーバにのみ対応しています。

Search & Destroy オペレータは、メールボックス検索の設定と結果の確認のみを実行できます。

手順

1. [管理] > [アクセス管理] の順に移動します。
2. 設定する Search & Destroy の役割をクリックします。
3. 必要に応じて、Search & Destroy の説明を変更します。
4. Search & Destroy の役割に追加するユーザまたはグループを検索します。
5. [使用可能なアカウント] リストで、この役割に追加するアカウントを選択し、[追加 >>] をクリックします。
6. [保存] をクリックします。

   [アクセス管理] 画面が表示されます。
7. Search & Destroy の役割の右にある [ステータス] アイコンをクリックして、この役割を有効にします。

   アイコンが赤色の×印 () から緑のチェックマーク () に変わります。
8. [保存] をクリックします。
9. InterScan コンソールからログオフし、機能を使用するために Search & Destroy の役割のアカウントでログオンします。

左側のナビゲーションメニューに、Search & Destroy のメニュー項目が表示されます。ユーザが複数の役割を持つ場合は、Search & Destroy のメニュー項目が既存のメニューと統合されます。

Search & Destroy のアクティベーション

Search & Destroy を初めて使用する場合、管理者はまず Active Directory サービスアカウントと、検索結果を格納する検出メールボックスを指定する必要があります。

注意

- アクティベーション処理が表示されるのは、Search & Destroy 機能に初めてアクセスする場合だけです。
- Search & Destroy 機能は、Exchange 2013、Exchange 2016、または Exchange 2019 が実行されているメールボックスサーバにのみ対応しています。

手順

1. [Search & Destroy] > [メールボックス検索] または [Search & Destroy] > [設定] をクリックします。

   Search & Destroy のアクティベーションウィザードが表示されます。

2. [次へ] をクリックします。

   [要件となる Exchange Server の設定] 画面が表示されます。

3. 要件となる項目の説明をよく読んで、作業を進める前に、要件となる Exchange 環境の設定を行います。

   Exchange 環境の設定の詳細については、356 ページの「Search & Destroy の事前要件」を参照してください。

4. 必要な設定がすべて完了したら、[要件となる Exchange Server の設定がすべて適切に設定されています] を選択します。

5. [次へ] をクリックします。

サービスアカウントのログオン資格情報画面が表示されます。

6. 以前に設定したサービスアカウントのユーザ名を[ユーザ名] に入力します。

注意

サービスアカウントの形式は次のとおりです。

domain\user name

7. このサービスアカウントのパスワードを [パスワード] に入力します。
8. [次へ] をクリックします。

   検出メールボックスの選択画面が表示されます。
9. [使用可能な検出メールボックス] リストから、Search & Destroy の検索結果を格納する検出メールボックスを選択します。
10. [次へ] をクリックします。

    PST 検索結果の生成に関する画面が表示されます。
11. [すべての検索結果を含む.pst ファイルの生成を Search & Destroy ユーザに許可する]オプションを選択します。これにより、InterScan で `<InterScan のインストールパス>¥SmexSDPst` フォルダが作成され、Exchange Trusted Subsystem で共有されるようになります。

注意

このアカウントは Exchange の役割である Mailbox Import Export のメンバーに設定する必要があります。

12. [次へ] をクリックします。

    Search & Destroy アクティベーションの詳細画面が表示されます。

注意

サービスアカウントまたは検出メールボックスが無効になっている場合、アクティベーション処理を続行できません。Search & Destroy のアクティベーションが失敗した理由については、226 ページの「Search & Destroy のトラブルシューティング」を参照してください。

13. Search & Destroy の設定を確認し、[完了] をクリックします。

メールボックス検索について

メールボックス検索は、指定したキーワードが含まれる、Exchange 環境内のメール、メールボックスコンポーネント (会議、連絡先など)、および特殊な項目を検出する機能です。

次の表は、Search & Destroy のメールボックス検索の種類の一覧を示しています。

表 15-1. メールボックス検索の種類

種類	説明
一致の推定	InterScan によって Exchange 環境が検索され、検索条件に一致したメールボックスコンポーネントの推定数および推定サイズが返されます。一致した項目が検出メールボックスにコピーされることはありません。 推定検索を実行すると、管理者は大量のデータを検出メールボックスにコピーする前に検索条件の効果を評価できます。推定検索によってあまりにも多くの一致結果が返される場合には、検索条件を見直して一致を絞り込んでください。 ヒント [すぐに検索] または [後で検索] を実行する場合は、事前に推定検索を実行することをお勧めします。大量のデータを検出メールボックスにコピーするには多くのシステムリソースが必要なため、パフォーマンスが低下する可能性があります。

種類	説明
すぐに検索	InterScan によって Exchange 環境が検索され、検索条件に一致するメールボックスコンポーネントが、指定された検出メールボックスにコピーされます。
後で検索	管理者は、特定の時刻に実行されるようにメールボックス検索を予約し、トラフィックがピークになるときのシステムリソース使用量を低減できます。

キーワード文字列に使用する構文

管理者は、いくつかの方法で検索キーワードを指定できます。正しい形式のキーワード検索文字列を指定すると、一致する項目の数を減らして検索の効率と成果を高めることができます。InterScan では、論理演算子、ワイルドカード、高度なクエリ構文 (AQS)、およびキーワードクエリ言語 (KQL) を使用してキーワード検索の範囲を絞り込むことができます。

表 15-2. キーワード構文

構文の種類	説明	例
論理演算子	複数のキーワードを区切る場合は、大文字の論理演算子 (AND、OR、NOT) を使用します。	• administrator AND password 「administrator」という単語と「password」という単語の両方を含むメールボックスコンポーネントを検索します。 • administrator OR salary 「administrator」という単語または「salary」という単語を含むメールボックスコンポーネントを検索します。 • administrator AND NOT payroll 「administrator」という単語を含むが「payroll」という単語は含まないメールボックスコンポーネントを検索します。

構文の種類	説明	例
カッコ	キーワードを特定のパターンでグループ化する場合は、カッコ () を使用します。	• (administrator OR password) AND NOT salary 「administrator」または「password」という単語を含み、かつ「salary」という単語を含まないメールボックスコンポーネントを検索します。 • (administrator AND NOT password) OR salary 「administrator」という単語を含むが「password」という単語は含まないメールボックスコンポーネント、または「salary」という単語を含むメールボックスコンポーネントを検索します。
二重引用符	二重引用符 ("") は語句を検索する場合に使用します。	• "administrator salary" "administrator salary"という語句を含むメールボックスコンポーネントを検索します。 • "administrator salary" AND "year ending" "administrator salary"という語句と"year ending"という語句の両方を含むメールボックスコンポーネントを検索します。 • ("administrator salary" OR payroll) AND "year ending") "administrator salary"という語句または"payroll"という単語を含み、かつ"year ending"という語句も含むメールボックスコンポーネントを検索します。

構文の種類	説明	例
ワイルドカード (アスタリスク)	特定の文字列で始まる、ある長さのキーワードを検索する場合は、アスタリスク (*) をワイルドカード演算子として使用します。 **注意** InterScan では、文字列の最後でのワイルドカード記号の使用のみサポートされます。	• admin* "admin"で始まる単語を含むメールボックスコンポーネントを検索します。 例: admin、administrator、administration、administrative
キーワードクエリ言語 (KQL)	KQL は、Exchange 2013/2016/2019 環境のプログラム検索が可能な検索クエリ言語です。	KQL の詳細および KQL を使用するコードの例については、次の Web サイトを参照してください。 http://msdn.microsoft.com/ja-jp/library/ee558911.aspx

メールボックス検索のオプション

InterScan には、メールボックス検索の範囲を絞り込むための検索オプションが複数あります。メールボックス検索を適切に設定すると、システムリソースの使用量が減少し、関連する検索結果だけが返されます。

ヒント

[すぐに検索] または [後で検索] を実行する場合は、事前に推定検索を実行することをお勧めします。大量のデータを検出メールボックスにコピーするには多くのシステムリソースが必要なため、パフォーマンスが低下する可能性があります。

次の検索オプションを設定し、メールボックス検索の照合を効率化します。

表 15-3. メールボックス検索のオプション

オプション	説明
キーワード	InterScan では、管理者が指定するキーワードまたは語句を検索できます。検索パラメータを絞り込むには、論理演算子、カッコ、二重引用符、ワイルドカード、または KQL 表現 (Exchange 2013、2016、および 2019 の場合) を使用します。 キーワード検索の詳細については、211 ページの「キーワード文字列に使用する構文」を参照してください。  注意 [キーワード] フィールドに入力できる最大文字数は 8192 字です。

オプション	説明
メールボックス	管理者は、Exchange 環境内のすべてのメールボックスを検索することも、特定のユーザまたは配布グループを選択することもできます。  注意 メールボックス検索は、対象とするユーザまたは配布グループ数を限定して実行することをお勧めします。大量のデータを検出メールボックスにコピーするには多くのシステムリソースが必要なため、パフォーマンスが低下する可能性があります。 [特定のユーザまたは配布グループのメンバーのメールボックス] を選択するには、次の手順を実行します。 1. テキストボックスに検索テキストを入力して使用可能なユーザ、配布グループ、またはデータベースを検索し、[検索] をクリックします。 2. 使用可能なリストで検索するアカウントまたはデータベースを選択し、[追加>>] をクリックします。 または、正しい形式の .txt ファイルから既存のリストをインポートすることもできます。  注意 検索できる最大メールアドレス数は 500 です。ファイルをインポートする場合、[選択されたメールボックス] リストに追加されるアドレスの上限は 500 件です。

オプション	説明
メールボックスコンポーネント	InterScan では、Exchange 環境内のすべてのメールボックスコンポーネントを検索するか、特定のコンポーネントだけを検索するよう管理者が選択することができます。特定のコンポーネントを選択するときには、次のオプションから選択できます。 • メール • 会議 • ジャーナル • タスク • 連絡先 • 備考 • インスタントメッセージングの会話 注意 [すべてのメールボックスコンポーネント (以下の一覧にないコンポーネントも含む)] を選択すると、Exchange メールボックス内のすべてのコンポーネントで見つかった検索結果が表示されます。
特定の送信者または受信者	特定の受信者宛てのメールメッセージまたは特定の送信者からのメールメッセージが検索されます。 注意 InterScan では、表示名、メールアドレス、またはドメイン名を使用して特定の送信者および受信者を検索できます。
日付	管理者は、Exchange 環境内のすべてのコンポーネントを検索することも、特定の日付範囲内で作成されたコンポーネントだけを検索することもできます。
検出メールボックス	管理者は、検索に特定の検出メールボックスを使用することも、以前に設定した初期設定の Search & Destroy 検出メールボックスを受け入れることもできます。

オプション	説明
処理	InterScan には、2 種類の検索処理があります。 • [検索してコンパイル]: 一致するすべての結果が確認用にコンパイルされます (推奨) • [検索して削除]: 一致するすべての結果が自動的に削除されます (非推奨) 注意 メッセージを自動的に削除するのはセキュリティが高い環境だけにすることをお勧めします。

メールボックス検索の設定

手順

1. [Search & Destroy] > [メールボックス検索] に移動します。

   [メールボックス検索] 画面が表示されます。

2. [新規] をクリックします。

   [新規メールボックス検索] 画面が表示されます。

3. メールボックス検索の名前を [名前] に入力します。

4. 見つける InterScan のキーワードを [キーワード] に指定します。

   キーワード検索の詳細については、211 ページの「キーワード文字列に使用する構文」を参照してください。

   注意
   [キーワード] フィールドに入力できる最大文字数は 8192 字です。

5. 検索するメールボックスを [メールボックス] に指定します。

ヒント

メールボックス検索ごとに特定のメールボックスを選択することをお勧めします。[すべてのメールボックスを検索] を選択すると、多くのシステムリソースが使用されるため、パフォーマンスが低下する可能性があります。

6. 必要に応じて、次の追加検索オプションを設定します。
   - メールボックスコンポーネント
   - 特定の送信者または受信者
   - 日付
   - 検出メールボックス
   - 処理

   検索条件の詳細については、213 ページの「メールボックス検索のオプション」を参照してください。
7. 次のいずれかのボタンをクリックします。
   - 一致の推定 – 指定した条件の検索が開始され、検索条件に一致したメールボックスコンポーネントの推定数および推定サイズが返されます。

     ヒント

     [すぐに検索] または [後で検索] を実行する場合は、事前に推定検索を実行することをお勧めします。大量のデータを検出メールボックスにコピーするには多くのシステムリソースが必要なため、パフォーマンスが低下する可能性があります。
   - すぐに検索 – 指定した条件の検索が開始され、検索条件に一致するメールボックスコンポーネントが、指定した検出メールボックスにコピーされます。
   - 後で検索

     [メールボックス検索の予約] 画面が表示されます。

a. 検索に使用する [時間帯] を選択します。

b. 検索の [日時] を指定します。

c. [OK] をクリックして検索のスケジュールを設定します。

- 保存 — Exchange 環境を検索せずに検索条件オプションを保存します。
- キャンセル — すべての変更を破棄します。

注意

メールボックスの検索が完了するまでにしばらく時間がかかることがあります。この間、管理者は引き続き InterScan を使用でき、検索を中断することなく Search & Destroy 機能から移動できます。

メールボックス検索を開始または保存すると、[メールボックス検索] 画面の表に検索内容が表示されます。

メールボックス検索の変更

InterScan では、管理者は、検索が完了した後でもメールボックス検索の検索条件を変更できます。多数の検索結果が返される場合、検索の範囲を小さくして、より正確な結果を取得したいと思うことがあるはずです。

警告!

すでに完了した検索の検索条件を変更すると、Exchange 検出メールボックスと InterScan データベースに保存されている元の検索結果が自動的にすべて削除されます。

手順

1. [Search & Destroy] > [メールボックス検索] をクリックします。
2. 変更する検索の [名前] をクリックします。

   [メールボックス検索の表示] 画面が表示されます。

3. [検索オプションに対する変更を許可する] を選択します。

   すべての検索条件フィールドのロックが解除され、編集できる状態になります。

4. 必要な設定を変更します。

   キーワード文字列の修正の詳細については、211 ページの「キーワード文字列に使用する構文」を参照してください。検索条件オプションの詳細については、213 ページの「メールボックス検索のオプション」を参照してください。

5. 次のいずれかのボタンをクリックします。

   - 一致の推定 — 指定した条件の検索が開始され、検索条件に一致したメールボックスコンポーネントの推定数および推定サイズが返されます。

     ヒント

     [すぐに検索] または [後で検索] を実行する場合は、事前に推定検索を実行することをお勧めします。大量のデータを検出メールボックスにコピーするには多くのシステムリソースが必要なため、パフォーマンスが低下する可能性があります。

   - すぐに検索 — 指定した条件の検索が開始され、検索条件に一致するメールボックスコンポーネントが、指定した検出メールボックスにコピーされます。
   - 後で検索

     [メールボックス検索の予約] 画面が表示されます。

     a. 検索に使用する [時間帯] を選択します。

     b. 検索の [日時] を指定します。

     c. [OK] をクリックして検索のスケジュールを設定します。

   - 保存 — Exchange 環境を検索せずに検索条件オプションを保存します。
   - キャンセル — すべての変更を破棄します。

注意

メールボックスの検索が完了するまでにしばらく時間がかかることがあります。この間、管理者は引き続き InterScan を使用でき、検索を中断することなく Search & Destroy 機能から移動できます。

メールボックス検索を開始または保存すると、[メールボックス検索] 画面の表に検索内容が表示されます。

メールボックス検索の削除

管理者は、InterScan からのみメールボックス検索を削除することも、InterScan の結果と検出メールボックスに格納された結果の両方を削除することもできます。

注意

メールボックス検索を削除しても、ユーザのメールボックスに格納されたメールボックスコンポーネントは削除されません。

手順

1. [Search & Destroy] > [メールボックス検索] に移動します。

   [メールボックス検索] 画面が表示されます。

2. 削除するメールボックス検索の横にあるチェックボックスをオンにします。

3. [削除] ボタンをクリックし、次のいずれかを選択します。

   - 検索のみ削除: メールボックス検索と検索条件だけを削除します。
   - 検索および検出メールボックスの結果を削除: メールボックス検索、検索条件、および Exchange の検出メールボックスに格納されている関連メッセージをすべて削除します。

メールボックス検索結果の表示

InterScan でメールボックス検索が完了すると、管理者は取得されたメッセージの詳細なリストを表示できます。

手順

1. [Search & Destroy] > [メールボックス検索] をクリックします。

   [メールボックス検索] 画面が表示されます。

2. 検索結果の完全なリストを表示する前に検索操作の概要を表示するか、検索結果の完全なリストを直接表示するかを選択します。

   - 最初に検索操作の概要を表示するには、次の手順を実行します。

     a. 検索の [名前] をクリックします。

     b. [ステータス] セクションで概要情報を表示します。

        検索で一致する項目の数が多い場合は、検索条件を見直すことを検討してください。詳細については、219 ページの「メールボックス検索の変更」を参照してください。

     c. [検索結果の表示] をクリックします。

   - 検索結果を直接表示するには、検索の名前の横にある表の [検索結果] 列にある [表示] リンクをクリックします。

   [メールボックス検索の結果] 画面が表示されます。

3. すべての検索結果を含む PST ファイルを作成、コピー、および削除するための管理者向けのオプションがあります。管理者が使用できるオプションは、[検索結果パッケージ (.pst ファイル)] のステータスに応じて異なります。

   - 未生成: [生成] ボタンをクリックして、`<InterScan のインストールパス>¥SmexSDPst` フォルダに PST パッケージを作成できます。
   - サーバで利用可能
     - [ダウンロード] ボタンをクリックして、ローカルの場所に PST ファイルをコピーできます。

- [削除] ボタンをクリックして、<InterScan のインストールパス >¥SmexSDPst フォルダから PST ファイルを削除できます。

注意

管理者が同じメールボックス検索を再度実行すると、PST ファイルが自動的に削除されます。

4. 管理者は、検索結果に対して次のタスクを実行できます。
   - 検索結果をフィルタします。
     a. メッセージのどの部分を検索するかを、[フィルタ基準] ドロップダウンボックスから選択します。
     b. テキストボックスに検索テキストを入力します。
     c. [フィルタ] をクリックします。

注意

[すべて表示] をクリックし、フィルタ条件をリセットします。

   - 選択された結果を [削除] します。
   - 検索結果を [すべて削除] します。

注意

メッセージを削除する際、削除対象として選択したメッセージがエンドユーザによって他の場所に移動されている、または既に削除されている場合には、InterScan ではそのメッセージは見つからず、正常に削除されたことが報告されます。

   - CSV ファイルに結果をエクスポートします。
   - マウスポインタをメッセージの [件名] に移動して、個々のメッセージについての詳細を表示します。

Search & Destroy の設定

Active Directory サービスアカウントと、検索結果を格納する検出メールボックスを指定します。

注意

Search & Destroy の設定を変更する前に、適切に設定された Active Directory サービスアカウントと検出メールボックスが Exchange 組織内に存在することを確認します。

手順

1. [Search & Destroy] > [設定] の順にクリックします。

   [Search & Destroy の設定］ 画面が表示されます。

2. バックエンド検索を実行するサービスアカウントの [ユーザ名］を入力します。

   注意

   サービスアカウントの形式は次のとおりです。

   domain\user name

3. このサービスアカウントのパスワードを [パスワード] に入力します。
4. [使用可能な検出メールボックス] リストから、Search & Destroy の検索結果を格納する検出メールボックスを選択します。
5. 必要に応じて、[すべての検索結果を含む.pst ファイルの生成を Search & Destroy ユーザに許可する] オプションを選択します。[メールボックス検索の結果] 画面に PST 生成オプションが表示されます。

注意

- フォルダ<InterScan のインストールパス>¥SmexSDPst が自動的に作成され、Exchange Trusted Subsystem で共有されます。
- このアカウントは Exchange の役割である Mailbox Import Export のメンバーに設定する必要があります。
- このアカウント用のメールボックスを作成します (Exchange 2013 のみ)。

6. [保存] をクリックします。

Search & Destroy イベントログの表示

InterScan では、Search & Destroy の詳細なイベント追跡ログが記録されます。Search & Destroy では、管理者はユーザのメールボックスにある Exchange コンポーネントを確認して削除できるため、ユーザに誤解があった場合には、Search & Destroy 操作の包括的な監査記録が役立つことがあります。

手順

1. [ログ] > [クエリ] に移動します。

   [ログクエリ] 画面が表示されます。

2. 検索する日付を指定します。
3. [種類] ドロップダウンから、[イベント追跡] を選択します。
4. 探す InterScan のユーザアカウントを選択し、[追加] をクリックします。
5. [ログの種類] の横にある [Search & Destroy のログ] を選択します。
6. [Search & Destroy のログ] の横にあるドロップダウンから、次のいずれかのイベントを選択します。
   - すべて
   - 設定変更

- 操作
- タスクステータス変更

7. 必要に応じ、ログの説明を入力します。
8. [並べ替え基準] と [表示件数] オプションを指定します。
9. [ログの表示] をクリックします。

Search & Destroy のトラブルシューティング

次の表は、Search & Destroy の検索タスクが失敗した理由として考えられるものの一覧を示しています。Exchange サーバからはエラー結果が返されるため、InterScan ではすべての理由を予測することはできません。

表 15-4. 検索処理の失敗の考えられる理由

エラー	考えられる理由	失敗するメールボックス検索処理
Search & Destroy サービスアカウントが無効です	• サービスアカウントの期限が切れています • 指定されたパスワードが正確ではありません • サービスアカウントが Exchange 検出管理グループのメンバーではありません	• 一致の推定/検索 • 削除 (メッセージ) • タスクと検出メールボックス内のメールの削除 • 検索の中止
検出メールボックスの接続エラー	• Exchange システムの検出メールボックスに到達できません	• 一致の推定/検索 • 検索の中止
	• 選択されている検出メールボックスに到達できません	• 一致の推定/検索 • 削除 (メッセージ) • タスクと検出メールボックス内のメールの削除
	• 選択されている検出メールボックスがいっぱいです	• 一致の推定/検索

エラー	考えられる理由	失敗するメールボックス検索処理
エンドユーザメールボックスの接続エラー	エンドユーザメールボックスに到達できません	• 一致の推定/検索 • 削除(メッセージ)
Exchange Web サービスを使用できません	• WinRM エラー • CAS サーバエラー	• 一致の推定/検索 • 削除 (メッセージ) • タスクと検出メールボックス内のメールの削除 • 検索の中止
検索結果の解析に失敗しました	• Exchange の検出管理グループに、選択した検出メールボックスに対するフルアクセス権限がありません • Exchange Web サービスを使用できません • 検出メールボックスにアクセスできません	• 検索
Exchange の現在の設定で、検索できるメールボックスの数が 1〜%N 個に制限されています。有効な数のメールボックスを選択するか、Exchange の現在の設定を変更して、再度実行してください。	• 選択したデータベース内にメールボックスがありません • 選択したデータベース内のメールボックスの数が、Exchange の調整ポリシーで定義されている上限を超えています	一致の推定/検索

第 16 章

仮想アナライザの設定

この章では、Exchange 環境を保護するための仮想アナライザを設定する方法について説明します。

内容は次のとおりです。

仮想アナライザについて

仮想アナライザは、トレンドマイクロ製品から送信されたサンプルを管理および分析するための安全な仮想環境です。サンドボックスイメージを使用することで、実際の設定でのファイルとネットワークの動作を、ネットワークを危険にさらすことなく観察できます。仮想アナライザは、静的分析と動作シミュレーションを実行して、悪意のある要素を特定します。仮想アナライザの分析では、状況に応じて特性が評価され、累積されたレーティングに基づいてサンプルにリスクレベルが割り当てられます。

仮想アナライザには次の機能があります。

- 脅威の実行と評価の概要
- 不正プログラムの動作とシステムへの影響の詳細な検証
- ネットワーク接続の開始
- システムファイル/レジストリの変更
- システムインジェクション動作の検出
- 悪意のある宛先およびコマンド&コントロール (C&C) サーバの特定
- エクスポート可能なフォレンジックレポートと PCAP ファイル
- 包括的な不正プログラムインテリジェンスの生成によるローカルにおける迅速な保護

InterScan は、検索エンジンで検出されない不審添付ファイル、実行可能ファイル、およびスクリプトファイルを分析のために仮想アナライザに送ります。

InterScan は、別途ライセンスが必要なトレンドマイクロ製品である Deep Discovery Analyzer 5.0 に含まれる仮想アナライザと統合することができます。

仮想アナライザの設定

仮想アナライザの設定を行う前に、[セキュリティリスク検索: 対象] 画面で [高度な脅威検索エンジンを有効にする] オプションを選択してください。高度な脅威の検出に必要な検索は、高度な脅威検索エンジンで実行されます。

重要

- 仮想アナライザは、高度な脅威検索エンジンを有効にするまで設定できません。
- 仮想アナライザの統合を有効にする前に、Exchange の再生フォルダを有効にする必要があります。

  Exchange の再生フォルダを有効にする方法については、363 ページの「仮想アナライザ - 統合の事前要件」を参照してください。

  警告!

  仮想アナライザの統合を有効にした後に Exchange の再生フォルダを無効にすると、予期しない問題が生じる可能性があります。Exchange の再生フォルダを無効にする場合は、事前に仮想アナライザの統合を無効にすることをお勧めします。

手順

1. [仮想アナライザ] に移動します。
2. [仮想アナライザにメールメッセージを送信] を選択します。
3. 仮想アナライザの動作モードを選択します。初期設定では [インラインモード] が選択されています。

   328 ページの「仮想アナライザの動作モードとそれぞれの使用基準を教えてください」を参照してください。
4. Deep Discovery Analyzer サーバを設定します。
   - IP アドレスを入力します。

     注意

     IP アドレスは IPv4 形式をサポートします。
   - ポート番号を入力します。
   - API キーを入力します。

注意

IP アドレス、ポート番号、有効な API キーを確認するには、仮想アナライザの管理者に問い合わせてください。

5. InterScan で仮想アナライザとのサーバ通信にプロキシが必要な場合は、[Deep Discovery Analyzer サーバへの接続にプロキシサーバを使用する] を選択します。
   a. 展開ボタン ( ) をクリックしてプロキシの設定を表示します。
   b. プロキシサーバのサーバ名または IP アドレスと、ポート番号を入力します。
   c. プロキシサーバにパスワードが必要な場合は、表示されるフィールドにユーザ名とパスワードを入力します。
6. 次のいずれかのボタンをクリックします。
   - 登録: Deep Discovery Analyzer サーバへの接続を確立します。
   - 接続テスト: Deep Discovery Analyzer サーバへの接続設定を確認しますが、サーバに InterScan を登録しません。

注意

仮想アナライザにメッセージを送信できるようにするには、接続設定を保存する前に仮想アナライザを登録してください。

7. 分析するメッセージのトラフィックの方向を選択します。
8. Active Directory のユーザ/グループ/連絡先/特定グループを検索して選択し、[選択されたアカウント] リストに追加することにより、分析対象から除外する送信者を選択します。
9. Active Directory のユーザ/グループ/連絡先/特定グループ内で検索し、これらを選択した、[選択されたアカウント] リストに追加することにより、分析するメッセージの受信者を選択します。
10. 分析する添付ファイルの種類を選択します。

ヒント

高度な脅威に関して最大の脅威となるのはアプリケーションと実行可能ファイルであるため、それらのファイルタイプのみを分析対象として選択することをお勧めします。

注意

InterScan の初期設定では、推奨されるファイルタイプが詳しい検索のために仮想アナライザに送信されます。特定のファイルタイプを検索対象として選択することもできます。

11. 不審なメッセージを分析して潜在的な脅威をより多く検出できるようにするには、[高度なスパムメールに対してアグレッシブモードを有効にする] を選択します。
12. 次の操作を実行します。
    a. [仮想アナライザのサポートの確認] をクリックして、現在の仮想アナライザで URL 分析がサポートされているかどうかを確認します。確認が完了したら、前の画面に戻ります。
    b. [URL 分析を有効にする] を選択します。

注意

このオプションは、URL 分析がサポートされていない場合は有効になりません。

13. 仮想アナライザが分析するメッセージとファイルに対する [セキュリティレベル] を設定します。
    - セキュリティレベル ― セキュリティレベルにより、仮想アナライザで分析、評価されたメッセージやファイルに対して InterScan が処理を実行するかどうかが決まります。使用できるセキュリティレベルの設定は次のとおりです。[高]、[中]、[低] のいずれかを選択します。

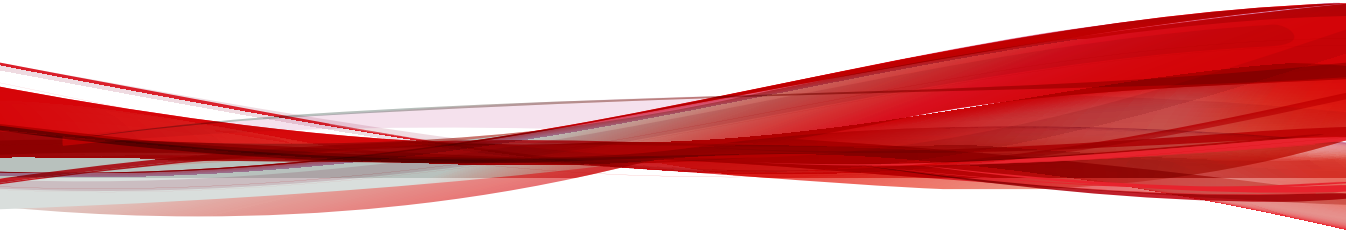
注意

メッセージやファイルの評価結果が、設定したセキュリティレベルに違反していると、InterScan は、[セキュリティリスク検索] の [処理] タブ ([セキュリティリスク検索] > [処理]) で [高度な脅威] に設定された処理を実行します。詳細については、112 ページの「セキュリティリスクの検出時の処理の設定」を参照してください。

- [分析の評価の最大待ち時間] — 仮想アナライザによるリスク分析中にメッセージを一時的に隔離する最大時間を選択します。
- [未解析のリスクに対する処理] — 仮想アナライザで解析できなかった添付ファイルを含むすべてのメールメッセージに対して、この処理が適用されます。仮想アナライザでファイルを解析できなかった理由として、サポートされていないファイルタイプ、接続の問題、解析エラーなどの原因が考えられます。

パート III

InterScan の管理



第 17 章

隔離領域の管理

この章では、隔離領域を管理する方法について説明します。隔離は、メッセージが特定のルールに一致した場合に InterScan で実行できる処理の 1 つです。

内容は次のとおりです。

隔離について

InterScan では、隔離を使用して、感染したメッセージを隔離ディレクトリに移動し、感染したファイルを置き換え、残りのメッセージを元の受信者に配信します。

InterScan では、コンテンツフィルタ違反が検出されたときに、メールを隔離またはバックアップするように設定できます。[処理の選択] 画面から隔離またはバックアップ用のフォルダを各コンテンツフィルタルールに対して個別に設定するか、またはグローバルディレクトリを設定できます。

隔離フォルダ/ディレクトリの設定

隔離またはバックアップ用のグローバルディレクトリを指定すると、InterScan では、コンテンツルール違反の結果として隔離またはバックアップされるすべてのファイルを、指定したディレクトリに移動します。

隔離ディレクトリは、検索フィルタごとに指定します。

表 17-1. 検索フィルタの隔離ディレクトリに関する参考情報

検索フィルタ	参考情報
セキュリティリスク検索	112 ページの「セキュリティリスクの検出時の処理の設定」
添付ファイルブロック	122 ページの「添付ファイルブロックの処理の設定」
コンテンツフィルタ	• ポリシー別ディレクトリの場合: 140 ページの「コンテンツフィルタの処理の設定」 • グローバルディレクトリの場合: 134 ページの「グローバル設定」
情報漏えい対策	• ポリシー別ディレクトリの場合: 167 ページの「情報漏えい対策処理の設定」 • グローバルディレクトリの場合: 163 ページの「グローバル設定」
高度なスパムメール対策	186 ページの「高度なスパムメール対策検索の処理の設定」
Web レピュテーション	197 ページの「Web レピュテーションの処理の設定」

隔離クエリの実行

実行する処理を決定する前に、隔離されたメッセージにクエリを実行できます。メッセージの詳細を確認したら、それらの隔離メッセージをリリースするか削除するかを選択できます。

手順

1. [隔離] > [クエリ] をクリックします。

   [隔離クエリ] 画面が表示されます。
2. 期間を選択します。
3. [すべて] または [指定の理由] を選択します。
   - セキュリティリスク検索
   - 添付ファイルブロック
   - コンテンツフィルタ
   - 情報漏えい対策
   - 検索不能メッセージ部分
   - Web レピュテーション
   - 高度なスパムメール対策
4. 再送信ステータスを選択します。
   - 再送されていない
   - 1 回以上再送信されている
   - 任意のステータス
5. (任意) メールの送信者、受信者、または件名を指定します。
6. 並べ替え基準のオプションを指定します。
7. 1 ページあたりに表示する項目数を指定します。
8. [クエリ対象] でクエリの対象を選択します。

- ローカルサーバ
- リモートサーバ
  a. ドロップダウンから [サーバグループ] を選択します。
  b. [選択可能なサーバ] の一覧でサーバ名をクリックし、[追加 >>] をクリックして [選択されたサーバ] の一覧に追加します。

9. [検索] をクリックします。

隔離ファイルの自動削除設定

[隔離ファイルの削除設定] 画面から、隔離メッセージの予約削除を設定するか、手動で隔離メッセージを削除します。

手順

1. [隔離] > [削除設定] をクリックします。

   [隔離ファイルの削除設定] 画面が表示されます。

2. [自動] タブをクリックします。
3. [自動削除を有効にする] を選択してログが自動的に削除されるようにします。
4. 削除するファイルを選択します。
   - すべての隔離ファイル —隔離されているすべてのファイルを削除します。
   - 再送信されていない隔離ファイル —1 回も再送信されていない隔離ファイルを削除します。
   - 1 回以上再送信された隔離ファイル —少なくとも 1 回は再送信された隔離ファイルを削除します。
5. ファイルを削除するまで保持する日数を指定します。
6. [保存] をクリックします。

隔離ファイルの手動削除設定

手順

1. [隔離] > [削除設定] をクリックします。

   [隔離ファイルの削除設定] 画面が表示されます。

2. [手動] タブをクリックします。
3. 削除するファイルを選択します。
   - すべての隔離ファイル —隔離されているすべてのファイルを削除します。
   - 再送信されていない隔離ファイル —1 回も再送信されていない隔離ファイルを削除します。
   - 1 回以上再送信された隔離ファイル —少なくとも 1 回は再送信された隔離ファイルを削除します。
4. ファイルを削除するまで保持する日数を指定します。
5. [削除] をクリックします。

隔離されたメッセージの再送信

安全と判断したメッセージは元の受信者に再送信できます。メッセージを再送信すると、メール全体またはメッセージ部分が再送信されます。

手順

1. [隔離] > [クエリ] をクリックします。

   [隔離クエリ] 画面が表示されます。

2. 再送信するメッセージの種類のクエリを設定して、実行します。

   クエリが実行され、画面の下部に結果が表示されます。

3. クエリの結果から再送信するメールを選択します。
4. 次のいずれかを実行します。

- 隔離されたメールを通知メールの添付ファイルとして送信する場合は、[再送] をクリックします。
- 隔離されたメールをメール本文に含めて送信する場合は、[元のメッセージを再送信] をクリックし、表示されるポップアップメッセージで処理を確認します。

[隔離 > 再送信] 画面が開き、再送信のオプションが表示されます。

5. [元の受信者を追加する] チェックボックスをオンにし、InterScan によってメールが元の受信者に送信されるように設定します。
6. [転送先] にメールアドレスを入力します。これによって、元の受信者に加えて、または元の受信者の代わりに、このメールアドレスに隔離されたメールが送信されます。

注意

Microsoft Exchange Server 2019、2016、2013 エッジトランスポートサーバの役割で使用している InterScan の場合、[転送先] に受信者のメールアドレスを入力します。

---

7. 元のメールに追加を行います。
   a. [元のメールの件名を付加する] チェックボックスをオンにします。

      これによって、メールの再送信時に件名行に表示されるメッセージが InterScan によって追加されます。

   b. [件名] に再送信するメールの新しい件名を入力するか、または初期設定値を使用する場合はそのままにします。

      初期設定の件名行には、再送信するメールの開封に関する警告が記載されます。
8. 再送信するメールの本文として使用するメッセージを InterScan の [本文] に入力します。
9. 再送信後に元の隔離されたメッセージが削除されるようにする場合は、[再送信の完了後、関連する隔離ファイルをすべて削除する] チェックボックスをオンにします。

   初期設定では、メールは再送信後も保持されます (上記のチェックボックスはオフ)。

10. [今すぐ再送信] をクリックします。

    InterScan によってメールがすぐに送信されます。進行状況バーが表示され、再送信処理の進行状況が表示されます。

11. 再送信処理が完了したら、[OK] をクリックして [隔離クエリ] 画面に戻ります。

注意

再送信後にメッセージが削除されると、データベースの隔離レコードは自動的に削除されます。

第 18 章

InterScan の監視

この章では、ネットワークの監視に役立つ通知、レポート、およびログについて説明します。

内容は次のとおりです。

概要画面の表示

[概要] 画面には、InterScan システムと機能に関する簡単な最新のレポートが表示されます。各機能の現在のステータスと、InterScan で検出されたセキュリティの脅威の件数を監視できます。詳細を確認するには、[レポート] メニューからレポートを生成します。

概要: システム

表 18-1. システム概要画面の情報

項目	説明
検索の概要: 検索ステータス概要	
検索ステータス概要	検索されたメール、検索された添付ファイル、セキュリティリスク、不審 URL、Web レピュテーション、情報漏えい対策、およびビジネスメール詐欺などの検索ステータスを確認できます。
検索の概要: 検索の種類	
検出されたウイルス/不正プログラム	ウイルス/不正プログラムの検出数は、一意のウイルス/不正プログラムの数ではありません。ウイルス/不正プログラムの検出数は、InterScan で 1 つのウイルス/不正プログラムが検出された回数です。
駆除できないウイルス/不正プログラム	検出されたウイルス/不正プログラムのうち駆除できなかったものの数を表示します。
検出されたスパイウェア/グレーウェア	検出されたスパイウェア/グレーウェアの数を表示します。
検出された高度な脅威	検出された高度な脅威の数を表示します。
ブロックされた添付ファイル	添付ファイルブロックポリシーによってブロックされた添付ファイルの数を表示します。
スパムメールメッセージ	コンテンツ検索によって検出されたスパムメールメッセージの数を表示します。
コンテンツフィルタ違反	検出されたコンテンツフィルタルール違反の数を表示します。

項目	説明
不審 URL - Web レピュテーション	Web レピュテーションによって検出された不審 URL の数を表示します。
書き換えられた URL	Time-of-Click プロテクションで書き換えられた URL の数を表示します。
情報漏えい対策の発生	検出された情報漏えい対策ポリシーイベントの数を表示します。
フィッシングメッセージ	コンテンツ検索によって検出されたフィッシングメッセージの数を表示します。
ビジネスメール詐欺	ビジネスメール詐欺フィルタで検出されたメールメッセージの数を表示します。
ブロックされた接続 - メールレピュテーション	スパムメール送信元からのメッセージのメールレピュテーション検出数を表示します。メールレピュテーションによって、スパムメール送信元からメッセージがネットワークに侵入しないようブロックされるため、検索対象のメッセージはありません。
検索不能メッセージ部分	検索の制限条件で指定されているとおりには検索されなかったメッセージ本文と添付ファイルの数を表示します。
検索方法	
セキュリティリスク検索方法	このセクションには、セキュリティリスク検索方法が表示されます。
Web レピュテーションのソース	このセクションには、Web レピュテーションのソースが表示されます。
Smart Protection Service	実行中のそれぞれの Trend Micro Smart Protection サービスについて、現在のサーバのアドレスとステータスが表示されます。
アップデートステータス	
アップデート	選択したコンポーネントをアップデートします。
コンポーネント	コンポーネントの現在のバージョン、利用可能なバージョン、およびアップデートステータスが表示されます。手動でアップデートするコンポーネントを選択できます。

注意

InterScan 通常版には、スパムメール対策、コンテンツフィルタ、情報漏えい対策の機能はありません。

概要: セキュリティリスク

表 18-2. 概要: セキュリティリスク情報

項目	説明
今日のセキュリティリスク概要	検索されたセキュリティリスクの総数と、駆除不能なセキュリティリスク、スパイウェア/グレーウェア、および高度な脅威の割合を表示します。
ウイルス/不正プログラムのグラフ	検索されたメッセージの総数と検出されたウイルス/不正プログラムの数をグラフで表示します。
スパイウェア/グレーウェアのグラフ	検索されたメッセージの総数と検出されたスパイウェア/グレーウェアの数をグラフで表示します。
高度な脅威のグラフ	検索されたメッセージの総数と検出された高度な脅威の数をグラフで表示します。
ウイルス/不正プログラムのトップ	最も多く検出されたウイルス/不正プログラムを表示します。
スパイウェア/グレーウェアのトップ	最も多く検出されたスパイウェア/グレーウェアを表示します。
高度な脅威のトップ	最も多く検出された高度な脅威を表示します。

概要: スパムメール

[概要] 画面には、InterScan システムと機能に関する簡単な最新のレポートが表示されます。詳細を確認するには、[レポート] メニューからレポートを生成します。

表 18-3. スパムメール情報の概要

項目	説明
今日の検索ステータス	現在のスパムメール検出レベルをクリックすると、設定を変更できます。

項目	説明
今日のスパムメール概要	メッセージ、スパムメール、フィッシング、および報告された誤検出の総数を表示します。
スパムメールメッセージ検出グラフ	検索されたメッセージの総数、報告された誤検出、および検出されたスパムメールに関するグラフを表示します。
ビジネスメール詐欺検出グラフ	検索されたメッセージの総数、報告された誤検出、および検出されたビジネスメール詐欺メッセージに関するグラフを表示します。
フィッシング検出グラフ	検索されたメッセージの総数、報告された誤検出、および検出されたフィッシングメッセージに関するグラフを表示します。
レポートされたトップ誤検出	最も多く報告された誤検出を表示します。

注意

InterScan 通常版には、スパムメール対策、情報漏えい対策、コンテンツフィルタの機能はありません。

概要: ランサムウェア

表 18-4. 概要: ランサムウェア情報

項目	説明
今日のランサムウェア概要	検出されたランサムウェアの総数と、その中でセキュリティリスク検索、Web レピュテーション、および仮想アナライザによる検出が占める割合を表示します。
セキュリティリスク検索	検索されたメッセージの総数とセキュリティリスク検索で検出されたランサムウェアの数を表示します。
Web レピュテーション	検索されたメッセージの総数と Web レピュテーションで検出されたランサムウェアの数を表示します。
仮想アナライザ	検索されたメッセージの総数と仮想アナライザで検出されたランサムウェアの数を表示します。

項目	説明
ランサムウェア検出グラフ	検索されたメッセージの総数と検出されたランサムウェア数のグラフを表示します。

警告について

管理者は、重大なシステムイベントまたはセキュリティにかかわる大規模感染が発生したときに、指定したユーザに通知を送信するように、InterScan を設定できます。通知は、メールおよび簡易ネットワーク管理プロトコル (SNMP) で送信するか、Windows イベントログに書き込むことができます。

システムイベント

システムイベントのオプションを以下で簡単に説明します ([通知] > [システムイベント])。

イベントリンクをクリックして警告通知を設定します。通知設定の詳細については、253 ページの「警告通知の設定」を参照してください。

表 18-5. システムイベント

イベント	説明
InterScan サービス	
InterScan サービスの開始に失敗した場合	InterScan for Microsoft Exchange Master Service が正常に開始されなかったとき。
InterScan サービスが使用できない場合	InterScan for Microsoft Exchange Master Service が予想外の状況で停止したとき。
InterScan イベント	
Smart Protection Server: ファイルレピュテーションサービスが次の場合	Trend Micro Smart Protection Server が使用可能または使用不可になったときに通知を受け取ります。
Smart Protection Server: Web レピュテーションサービスが次の場合	Trend Micro Smart Protection Server が使用可能または使用不可になったときに通知を受け取ります。

イベント	説明
仮想アナライザ: 仮想アナライザが次の場合	アナライザサーバが使用可能または使用不可になったときに通知を受け取ります。
アップデート結果が次の場合	アップデートに成功または失敗したときに通知を受け取ります。
前回のアップデート実行日時から次を経過した場合	前回のアップデート実行日時から指定した時間が経過したときに、通知を受け取ります。
手動/予約検索の結果が次の場合	検索処理に成功または失敗したときに通知を受け取ります。
手動/予約検索の実行時間が指定の時間を超えた場合	検索処理の実行時間が指定した時間を超えたときに通知を受け取ります。
Search & Destroy: 検索に成功または失敗した場合	Search & Destroy のメールボックス検索に成功または失敗したときに通知を受け取ります。
バックアップ/隔離/アーカイブディレクトリの含まれるドライブの空き容量が次の値を下回った場合	利用可能なディスク容量が指定した最小容量まで減少したときに通知を受け取ります。
隔離、ログ、およびメールボックス検索結果用のデータベースのサイズが指定の値を超えた場合	データベースのサイズが指定したサイズより大きくなったときに通知を受け取ります。
機械学習型検索が次の場合	機械学習型検索サービスが使用可能または使用不可になったときに通知を受け取ります。
ライティングスタイルサービスが次の場合	ライティングスタイルサービスが使用可能または使用不可になったときに通知を受け取ります。
Exchange イベント	
待機中の SMTP メッセージが指定の時間内に継続的に次の数を超える場合	待機中の SMTP メッセージの数が一定の時間枠の指定した数を超えたときに通知を受け取ります。

イベント	説明
トランザクションログの含まれるドライブのディスク空き容量が次の値を下回った場合	利用可能なディスク容量が指定した最小容量まで減少したときに通知を受け取ります。
メールストアのサイズが指定の値を超えた場合	メールストアのサイズが指定したサイズを超えたときに通知を受け取ります。

注意

System Center Operations Manager (SCOM) を使用するには、InterScan のインストールパッケージから管理パックをインストールして、個々の通知設定ごとに [Windows イベントログに書き込む] を選択します。Exchange のイベントは、System Center Operations Manager (SCOM) には統合されません。

アウトブレークアラート

この画面で利用できるオプションの説明を以下に示します ([通知] > [アウトブレークアラート])。

イベントリンクをクリックして警告通知を設定します。通知設定の詳細については、253 ページの「警告通知の設定」を参照してください。

表 18-6. アウトブレークイベント

イベント	説明
検出済みウイルス/不正プログラムが指定の時間内に次の数に達した場合	検出したウイルス/不正プログラムの数および期間を設定することによって、アウトブレークの条件を設定します。検出されたウイルス/不正プログラムの数がこの制限値に達すると、InterScan から通知が送信されます。
駆除不能のウイルス/不正プログラムが指定の時間内に次の数に達した場合	検出された駆除不能ウイルス/不正プログラムの数および期間を設定することによって、アウトブレークの条件を設定します。検出された駆除不能ウイルス/不正プログラムの数がこの制限値に達すると、InterScan から通知が送信されます。

イベント	説明
検出済みスパイウェア/グレーウェアが指定の時間内に次の数に達した場合	検出したスパイウェア/グレーウェアの数および期間を設定することによって、アウトブレークの条件を設定します。検出されたスパイウェア/グレーウェアの数がこの制限値に達すると、InterScan から通知が送信されます。
ブロック済み添付ファイルが指定の時間内に次の数に達した場合	ブロックされた添付ファイルの数および期間を設定することによって、アウトブレークの条件を設定します。ブロックされた添付ファイルの数がこの制限値に達すると、InterScan から通知が送信されます。

警告通知の設定

警告の条件をクリックすると、警告の通知画面が表示されます。

表 18-7. 通知の設定

設定	説明
管理者への通知	
メール	メールで通知を送信する場合に選択します。
送信先	管理者のメールアドレスを入力します。
件名	管理者に送信するメッセージの件名を入力します。
メッセージ	メッセージ要素をクリックして、その要素を通知に追加します。 たとえば、[時刻] をクリックして、メッセージリストに時刻を追加します。通知メッセージには、InterScan によって処理が実行された時刻が追加されます。
その他の通知	
SNMP	SNMP で通知を送信する場合に選択します。
IP アドレス	SNMP の IP アドレスを指定します。
コミュニティ	SNMP のコミュニティ名を指定します。

設定	説明
メッセージ	メッセージ要素をクリックして、その要素を通知に追加します。 たとえば、[時刻] をクリックして、メッセージリストに時刻を追加します。通知メッセージには、InterScan によって処理が実行された時刻が追加されます。
Windows イベントログに書き込む (このチェックボックスをオンにすると、Microsoft™ System Center Operations Manager がアラート用に Windows イベントログを取り込みます)	Windows のイベントログに通知を送信する場合に選択します。 **注意** System Center Operations Manager (SCOM) を使用するには、InterScan のインストールパッケージから管理パックをインストールして、個々の通知設定ごとに [Windows イベントログに書き込む] を選択します。Exchange のイベントは、System Center Operations Manager (SCOM) には統合されません。

レポートについて

InterScan では、レポートを生成して、ログイベントを整理されたグラフィカルな表示形式で確認できます。レポートは、印刷するか、指定したアドレスにメールで送信できます。また、保存するレポートの数を [レポートの削除設定] 画面で設定できます。レポート数が設定した数を超えた場合は、最も古いレポートから順に超過した分のレポートが削除されます。

例: 15 件のレポートがあり、保存するレポートの最大数が 10 件である場合は、最も古いものから順に 5 件のレポートが削除され、新しく保存された 10 件のレポートが残ります。

手動レポート

手動レポートを生成して、InterScan 情報の概要を確認します。レポートが生成されるとすぐに、管理コンソールにレポートが表示されます。手動レポートは印刷したりメールで送ることができます。

生成されたレポートは、後ですぐに表示できるようにキャッシュに保存されます。レポートは、手動で削除するか、レポート保存期間の設定に従って自動的に削除されるまで、保持されます。

手動レポートの生成

手順

1. [レポート] > [手動レポート] の順にクリックして、[手動レポート] 画面を開きます。
2. [レポートの生成] をクリックします。
3. [レポート名] を入力します。
4. 日付を入力するか、カレンダーアイコンをクリックして日付を選択し、期間を設定します。

   指定した期間について、レポートの対象とするデータが収集されます。
5. レポートに含めるサーバを選択します。
   - ローカルサーバ
   - リモートサーバ
     a. ドロップダウンから [サーバグループ] を選択します。
     b. [選択可能なサーバ] の一覧でサーバ名をクリックし、[追加 >>] をクリックして [選択されたサーバ] の一覧に追加します。
6. レポートの対象とする情報の種類をクリックします。

   レポートの種類の横にある [詳細の表示] アイコンをクリックすると、レポートの詳細なオプションが表示されます。
7. [生成] をクリックします。

予約レポート

InterScan では、指定した日時に予約レポートが生成されます。管理者または他の受信者にメールでレポートを配信するように InterScan を設定できます。

予約レポートは、テンプレートに基づいて生成されます。テンプレートを定義すると、そのテンプレートに基づいて予約レポートが生成されます。レポ

ートテンプレートには、スケジュールと、各レポートに含める内容を指定します。テンプレートに指定した時刻になると、レポートが生成されます。各テンプレートには複数のレポートが含まれ、[予約レポート] 画面の [レポート一覧] をクリックして表示することができます。テンプレートの内容を表示するには、そのテンプレートの名前をクリックします。

予約レポートの生成

手順

1. [レポート] > [予約レポート] の順に選択して [予約レポート] 画面を開きます。
2. [追加] をクリックします。

   [予約レポート > レポートの追加] 画面が表示され、レポートを設定できます。
3. レポートテンプレートの名前を入力します。
4. テンプレートで個別レポートの生成に使用するスケジュールを指定します。

   テンプレートでは、日次、週次、または月次ベースでレポートを生成できます。
5. [レポート生成時刻] に、テンプレートに基づいて個別レポートを生成する時刻を指定します。

   注意

   InterScan では、時刻の設定すべてに 24 時間形式が使用されています。

   例: スケジュールを毎週日曜日に指定し、レポートの生成時刻を 02:00 に設定すると、InterScan では、テンプレートを使用して、毎週日曜日の 02:00 に個別レポートが生成されます。
6. レポートに含めるサーバを選択します。
   - ローカルサーバ

- リモートサーバ

  a. ドロップダウンから [サーバグループ] を選択します。

  b. [選択可能なサーバ] の一覧でサーバ名をクリックし、[追加 >>] をクリックして [選択されたサーバ] の一覧に追加します。

7. InterScan でスケジュールに従って生成するレポートの種類を選択します。
8. テンプレートでレポートを生成するたびにそのレポートを受け取る受信者を設定します。
9. [メールアドレスに送信:] をクリックします。
10. 受信者のメールアドレスを入力します。
11. [保存] をクリックします。

    ブラウザが [予約レポート] 画面に戻ります。レポートテンプレートのリストに新しいテンプレートが追加されます。

レポートの削除設定

[レポートの削除設定] 画面で、InterScan で保存するレポートの数を指定します。手動レポートおよび予約レポートについて、それぞれ数値を入力します。レポート数が指定した最大数を超えると、古いレポートから順に削除されます。各テンプレートに保存される予約レポートについては、指定した最大数はテンプレートごとに保存されるレポート数に適用されます。

たとえば、保存されているレポートテンプレートが 5 つあり、テンプレートに保存する予約レポート数を 4 に設定したとします。その場合、各テンプレートで 4 つのレポート、合計で 20 個のレポート (5 テンプレート×4 レポート) を生成できます。あるテンプレートでもう 1 つレポートが生成されると、そのテンプレートで生成された一番古いレポートが削除されて、レポートの合計数が 20 に維持されます。

[レポートの削除設定] 画面 ([レポート] > [削除設定]) で利用できるオプションの簡単な説明を以下に示します。

- 手動レポート —保存するレポートの最大数を指定します。
- 各テンプレートで作成された予約レポート —保存するレポートの最大数を指定します。

- レポートテンプレート — 保存するレポートテンプレートの最大数を指定します。

ログについて

InterScan では詳細なログが記録されます。管理者は、システムセキュリティの分析時や InterScan の設定時にこれらのログを参照して、Exchange 環境に対する保護を最適化できます。InterScan で記録されるログは次のとおりです。

- セキュリティリスク検索
- 添付ファイルブロック
- コンテンツフィルタ
- アップデート
- 検索イベント
- セキュリティリスクの検索時のバックアップ
- コンテンツフィルタの実行時のバックアップ
- 検索不能メッセージ部分
- イベント追跡
- 情報漏えい対策
- 情報漏えい対策のバックアップ
- Web レピュテーション
- URL クリック追跡
- 高度なスパムメール対策
- 仮想アナライザへの送信

ログ情報を表示するには、ログクエリを実行します。クエリの設定および実行には、[ログクエリ] 画面を使用します。

ログの種類

次の表は、ログの種類を示しています。

種類	説明
セキュリティリスク検索	セキュリティリスクが検出されたメッセージに関する情報
添付ファイルブロック	InterScan で検索されブロックされたファイルが添付されていたメッセージに関する情報
コンテンツフィルタ	InterScan で望ましくないコンテンツがフィルタされたメッセージに関する情報
アップデート	コンポーネントが正常にアップデートされたかどうかに関する情報 注意 コンポーネントには、検索エンジンとパターンファイルが含まれます。
検索イベント	手動検索および予約検索が正常に実行されたか、または失敗したかに関する情報
セキュリティリスクの検索時のバックアップ	処理が実行される前にセキュリティリスク検索によってバックアップフォルダに移動されたファイルに関する情報
コンテンツフィルタの実行時のバックアップ	処理が実行される前にコンテンツフィルタによってバックアップフォルダに移動されたファイルに関する情報
検索不能メッセージ部分	検索の制限条件で指定されているとおりには検索されなかったメッセージ部分に関する情報
イベント追跡	次を含む、製品コンソールにおけるすべての操作に関する情報: • システムおよび脆弱性のログ • Search & Destroy のログ
情報漏えい対策	情報漏えい対策ポリシーイベントが検出されたメッセージに関する情報
情報漏えい対策のバックアップ	処理が実行される前に情報漏えい対策によってバックアップフォルダに移動されたファイルに関する情報
Web レピュテーション	不正 URL が検出されたメッセージに関する情報
URL クリック追跡	InterScan で書き換えられた URL に関する情報

種類	説明
高度なスパムメール対策	不審メッセージとして検出されたメッセージに関する情報
仮想アナライザへの送信	InterScan から仮想アナライザに分析のために送信されたメッセージに関する情報

ログのクエリ

手順

1. [ログ] > [クエリ] の順にクリックします。

   [ログクエリ] 画面が表示されます。

2. 期間を選択します。
3. エントリの種類を選択します。
4. (任意) 選択したエントリの種類に応じて、次のいずれかの条件を指定します。
   - 検出場所
   - 送信者
   - 受信者
   - 件名
   - 添付ファイル名
   - キーワード
   - 名前
   - IP アドレス
   - ログの種類
   - 説明
   - ソースの種類
   - ファイル名または URL

- URL
- 脅威の名前

5. [並べ替え基準] のオプションを指定します。
6. 1 ページあたりに表示する項目数を指定します。
7. [クエリ対象] でクエリの対象を選択します。
   - ローカルサーバ
   - リモートサーバ
     a. ドロップダウンから [サーバグループ] を選択します。
     b. [選択可能なサーバ] の一覧でサーバ名をクリックし、[追加 >>] をクリックして [選択されたサーバ] の一覧に追加します。
8. [ログの表示] をクリックします。

ログの削除設定

InterScan では、セキュリティリスク検索、コンテンツフィルタ、添付ファイルブロック、スパムメール対策、アップデート、検索イベント、バックアップ、およびイベント追跡の詳細なログが記録されます。これらのログは、システム情報に関する貴重な情報源になります。ログの削除設定を実行して、ディスクの使用量を管理します。

ログの手動削除設定の実行

手順

1. [ログ] > [削除設定] をクリックします。
   [ログの削除設定] 画面が表示されます。
2. [手動] タブをクリックします。
3. 削除するログの種類を選択します。
4. ログを削除するまで保持する日数を指定します。
5. イベント追跡ログを削除するまで保持する日数を指定します。

6. [削除] をクリックしてログおよびイベントを削除します。

ログの予約削除設定の実行

手順

1. [ログ] > [削除設定] をクリックします。

   [ログの削除設定] 画面が表示されます。
2. [自動] タブをクリックします。
3. [自動削除を有効にする] を選択します。
4. 削除するログの種類を選択します。
5. ログを削除するまで保持する日数を指定します。
6. イベント追跡ログを削除するまで保持する日数を指定します。
7. [保存] をクリックします。

ログの転送設定

InterScan の設定により、外部の Syslog サーバまたはセキュリティ情報/イベント管理 (SIEM) サーバにイベントを転送することができます。イベントはすべて、クリアテキストで転送されます。

手順

1. [ログ] > [ログ転送設定]の順に選択します。

   [ログ転送設定] 画面が表示されます。
2. ログ転送を有効にするには、[ログ転送設定を有効にする] を選択します。
3. [ログ転送先の設定] セクションで、次の設定を行います。
   - [IP アドレス]: ログ転送先サーバの IP アドレス。
   - [ポート]: ログ転送先サーバのポート番号。
   - [転送の種類]: ログ転送先サーバにログを転送する際に使用するプロトコル。

[TCP] を選択した場合、[SSL を有効にする] を選択するとログコンテンツを暗号化できます。

- [ファシリティ]: Syslog イベントを作成したコンピュータのプロセス。
- [重要度]: Syslog メッセージの重要度レベル。

4. [ログ転送の設定] セクションで、次の設定を行います。
   - [件数]: ログの収集と転送の頻度。
   - [イベント形式]: イベントログの形式。
   - [ログの種類]: InterScan から転送するログの種類。
5. [ネットワーク接続テスト] をクリックしてログ転送先サーバとの接続を確認します。
6. [保存] をクリックします。

第 19 章

管理タスクの実行

この章では、管理タスクについて説明します。

内容は次のとおりです。

プロキシの設定

プロキシサーバは、セキュリティを強化して、帯域幅を効率的に利用するために使用されます。ネットワークでプロキシサーバを使用している場合、インターネットへ接続して、InterScan を最新の状態に維持するために必要な最新コンポーネントをダウンロードし、ライセンスステータスをオンラインでチェックするようにプロキシ設定値を設定します。

手順

1. [管理] > [プロキシ] の順にクリックします。
2. [Web レピュテーション、Time-of-Click プロテクション、機械学習型検索、アップデート、および製品ライセンスの確認にプロキシサーバを使用する] を選択します。このチェックボックスをオンにすると、以下の設定がオンになります。

   トレンドマイクロのレピュテーションサーバへの Web レピュテーションクエリの実行

   Time-of-Click プロテクション

   機械学習型検索

   アップデート

   プロキシサーバを使用しての製品ライセンスの通知
3. プロキシサーバの名前または IP アドレスを入力します。
4. ポート番号を入力します。
5. (任意) [SOCKS 5 を使用する] をオンにします。
6. プロキシサーバで認証を必要とする場合は、ユーザ名とパスワードを指定します。

グローバル承認済みリストの設定

グローバル承認済みリストを使用すると、リアルタイム検索のすべてのフィルタのメール検索がスキップされます。

手順

1. [管理] > [グローバル承認済みリスト] の順にクリックします。

   [グローバル承認済みリスト] 画面が表示されます。

2. 次のいずれかを選択します。

   - 特定の送信者から任意の受信者
   - 任意の送信者から特定の受信者
   - 特定の送信者から特定の受信者

3. [特定の送信者] または [特定の受信者] リンクをクリックします (該当する場合)。

4. 次のいずれかを選択します。

   - すべて — このポリシーをすべてのユーザに適用します。
   - 特定のアカウント — Active Directory グループまたは InterScan 特定グループから選択します。

5. Active Directory のユーザ/グループ/連絡先/特定グループ内で検索して、これらを選択して [選択されたアカウント] リストに追加します。

6. Active Directory のユーザ/グループ/連絡先/特定グループを検索して選択し、[アカウントの除外] 画面の [選択されたアカウント] リストに追加します。

7. [保存] をクリックします。

   [グローバル承認済みリスト] 画面が再度表示されます。

8. 画面上部の [リアルタイム検索のすべてのフィルタにグローバル承認済みリストを使用してメールの検索をスキップする] を選択して、グローバル承認済みリストを有効にします。

9. [保存] をクリックします。

メールの設定

メールヘッダサイズを設定したり、すべての外部ドメインからの受信メッセージの本文の先頭にディスクレーマーテキストを追加するように InterScan を設定できます。

手順

1. [管理] > [メール設定] の順にクリックします。

   [メール設定] 画面が表示されます。

2. [メール制限] セクションで、次の操作を実行します。

   - 各メールヘッダの最大サイズ: ヘッダサイズを 1〜10MB の間で指定します。
   - ヘッダサイズが制限を超えたときの処理: ドロップダウンメニューから処理を選択します。

3. [受信メッセージディスクレーマー] セクションで、[受信メッセージディスクレーマーを有効にする] を選択します。

4. 必要に応じて、[受信メッセージディスクレーマーの内容] フィールドのテキストを変更します。

5. [保存] をクリックします。

グローバル通知の設定

処理を実行した後に通知を送信するように InterScan を設定します。通常、通知は、InterScan 管理者のメールアドレスに対するグローバル初期設定を使用して、Exchange 管理者に送信されます。

管理者は、通知を受信するユーザ、および通知の送信者として表示されるユーザを設定できます。つまり、InterScan で通知が送信される際に、[通知設定] 画面で設定したアドレスがメッセージの送信者として表示されます。そのため、メッセージの受信者はこの送信者に問題を問い合わせることができます。

この画面で管理者のアドレスを設定して適用すると、次の通知で管理者アドレスが変更されます。

- セキュリティリスク検索
- 添付ファイルブロック
- コンテンツフィルタ
- 情報漏えい対策
- 高度なスパムメール対策
- スパムメール対策
- Web レピュテーション
- システム警告
- アウトブレークアラート

注意

上記の機能ごとの通知アドレスは、初期設定のアドレスを適用した後でカスタマイズできます。

InterScan では、メールトラフィックは、内部と外部の 2 つのネットワークカテゴリに分けられます。InterScan は Exchange サーバにクエリを実行して、内部アドレスと外部アドレスがどのように定義されているかを確認します。すべての内部アドレスは共通のドメインを使用し、すべての外部アドレスはそのドメインには属しません。

たとえば、内部ドメインアドレスが「@host.com」の場合、「abc@host.com」や「xyz@host.com」などは内部アドレスとして分類されます。「abc@host.com」や「jondoe@otherhost.com」など、その他のすべてのアドレスは外部アドレスとして分類されます。

InterScan では、次の状況で自動的に通知を送信できます。

- セキュリティリスクの検出と検出時の処理の実行、またはメールからのその他の不正プログラムの検出
- 感染した添付ファイルのブロック
- 不審 URL の検出
- 望ましくないコンテンツのメールからの除去
- 情報漏えい対策イベントを検出して処理を実行
- 重大なシステムイベントを検出
- ウイルス/不正プログラムの大規模感染を検出

注意

InterScan の通知が簡易ネットワーク管理プロトコル (SNMP) で正しく解決されるようにするには、InterScan パッケージの次のパスから MIB (Management Information Base) ファイルをネットワーク管理ツールにインポートします。

```
tool¥admin¥trend.mib
```

グローバル通知の設定

手順

1. [管理] > [通知設定] の順にクリックします。
2. 通知を受信する管理者のメールアドレスを入力します。
3. 通知を送信する送信者のメールアドレスを入力します。
4. SNMP の IP アドレスおよびコミュニティを指定します。
5. [初期設定] および [内部メール定義のカスタマイズ] を選択して、[内部メールの定義] を指定します。

   これによって、InterScan でメールを内部として分類する方法をカスタマイズできるようになります。
6. [保存] をクリックします。

スパムメールの管理の設定

[スパムメールの管理] 画面には、Exchange のメールボックスに作成するスパムメールフォルダの名前と、エンドユーザメール隔離ツールでスパムメールを保持する日数が表示されます。エンドユーザは、Microsoft Outlook を使用してスパムメールフォルダの名前を変更できます。このフォルダは、フォルダ名ではなく ID によって識別されます。

注意

[スパムメールの管理] は、Exchange Server 2013 でのみ使用できます。

手順

- Exchange サーバのすべてのメールボックスに対してエンドユーザメール隔離を有効にするには、[エンドユーザメール隔離を有効にする] を選択します。

注意

エンドユーザメール隔離を有効にして [保存] をクリックすると、確認用メッセージが表示されます。クライアントアカウントからスパムメールフォルダ (およびその内容) を削除する場合は、[すべてのクライアントからエンドユーザメール隔離スパムメールフォルダを削除します] を選択します。

- エンドユーザメール隔離で Exchange サーバに追加された新しいユーザごとに新しいスパムメールフォルダを作成するには、[エンドユーザメール隔離設定] セクションで、[メールフォルダを作成し、スパムメールを削除する] をクリックします。[メールフォルダを作成し、スパムメールを削除する] をクリックすると、新規ユーザのスパムメールフォルダが即座に作成されます。
- [クライアントのスパムメールフォルダ設定] セクションで、スパムメールの削除スケジュールを設定します。
- [エンドユーザメール隔離の除外リスト] セクションで、除外リストのユーザを追加または削除します。このリストに追加したユーザに対してはエンドユーザメール隔離が有効になりません。

アクセス管理について

役割ベースの管理機能を使用して、InterScan 製品コンソールのメニューおよびサブメニューの項目に対するアクセスを許可したり制御したりすることができます。組織に InterScan 管理者が複数いる場合は、この機能を利用して、管理タスクを管理者に委任したり、各管理者がアクセスできるメニュー項目を管理したりすることができます。また、管理者以外のユーザに製品コンソールへの「表示専用」アクセスを許可することができます。

注意

アクセス管理は、リモートデスクトップを使用している場合の非コンソールモードでは使用できません。

アクセス管理権限

アクセス管理権限 ([管理] > [アクセス管理] > [権限]) の説明を以下に示します。

- すべて ― 対象のグループ内のユーザに、対象の機能の有効化、無効化、および設定を許可します。
- 読み取り ― 対象のグループ内のユーザに、対象の機能の表示および次の操作の実行を許可します。

表 19-1. 読み取り権限

権限	説明
アップデート	オペレータは手動アップデートを設定できます。
ログ	オペレータはログをクエリできます。
レポート	オペレータはレポートを生成できます。
隔離	オペレータは、隔離されたメッセージおよびファイルをクエリできます。

- なし ― 対象のグループのユーザに対して、対象の機能を非表示にします。

アクセス管理の有効化

手順

1. [管理] > [アクセス管理] の順にクリックします。

   [アクセス管理] 画面が表示されます。

2. [ステータス] の下のアイコンをクリックして、アクセス管理が有効になっていることを示す緑のチェックアイコン ( ) を表示します。赤色の×アイコン ( ) は、そのポリシーが無効になっていることを示します。

3. [シングルサインオンを有効にする] を選択して、Microsoft™ Windows™ 認証を使用したログオンを許可します。

   この機能は、Microsoft™ Internet Explorer™でのみサポートされています。Internet Explorer セキュリティ強化を有効にしている場合、この機能を使用するには InterScan 製品コンソールサイトをローカルイントラネットゾーンに追加する必要があります。

4. [保存] をクリックします。

アクセス管理の設定

手順

1. [管理] > [アクセス管理] の順にクリックします。

   [アクセス管理] 画面が表示されます。

2. 次のいずれかのアクセス管理の役割をクリックします。
   - 管理者
   - オペレータ
   - Search & Destroy 管理者
   - Search & Destroy オペレータ
3. [認証情報] タブをクリックします。
4. グループの説明を指定します。
5. [検索] を使用して、Active Directory からアカウントを追加します。
6. [保存] をクリックします。
7. [権限] タブをクリックします。
8. グループに付与する権限を選択します。
9. [保存] をクリックします。

特定グループについて

特定グループを作成すると、ネットワークのセグメントにポリシーを簡単に適用できます。管理者は、特定グループを簡単に管理できるようにインポートしたりエクスポートしたりできます。特定グループに他の特定グループを含めることはできません。

ある特定グループに属する Active Directory ユーザを削除すると、その特定グループの [選択されたアカウント] リストに通知メッセージが表示されます。

特定グループの設定

ルールとポリシーを作成するときに管理が簡単になるように特定グループを設定します。

手順

1. [管理] > [特定グループ] の順にクリックします。

   [特定グループ] 画面が表示されます。

2. 特定グループを追加または編集します。

   - 新しい特定グループの場合

     [追加] をクリックします。

   - 既存の特定グループの場合

     グループ名をクリックします。

3. 特定グループの名前を入力して、説明を指定します。
4. Active Directory (AD) ユーザを検索して特定グループに追加するか、SMTP アドレスを指定します。
5. アカウントを追加するには [追加 >>] をクリックし、この特定グループからアカウントを削除するには [<< 削除] をクリックします。
6. [保存] をクリックします。

サーバグループについて

サーバグループを作成すると、[サーバ管理] 画面から複数の InterScan サーバを簡単に管理できます。

また、サーバグループを使用して、ログや隔離されたメッセージをクエリし、任意の InterScan サーバからレポートを作成することで、複数の InterScan サーバを監視できます。

注意

初期設定のサーバグループ (「すべてのサーバ」、「メールボックスサーバ」、および「トランスポートサーバ」) を変更または削除することはできません。

サーバグループの設定

手順

1. [管理] > [サーバグループ] の順にクリックします。

   [サーバグループ] 画面が表示されます。

2. サーバグループを追加または編集します。

   - 新しいサーバグループの場合

     [追加] をクリックします。

   - 既存のサーバグループの場合

     グループ名をクリックします。

3. サーバグループの名前を入力し、説明を指定します。
4. サーバを追加する場合は [追加 >>] をクリックし、このサーバグループからサーバを削除する場合は [<< 削除] をクリックします。
5. [保存] をクリックします。

内部ドメインについて

組織の内部ドメインは、送信メールトラフィックと区別されるように設定します。情報漏えい対策ポリシーは、内部ドメインを通じて送信されるメール

をポリシーの設定に従って無視します。情報漏えい対策ポリシーを送信メッセージのみに適用した場合、内部ドメインのポリシー違反については処理が実行されません。

InterScan では、アスタリスク (*) のワイルドカードを使用して内部ドメインを指定できます。ワイルドカード演算子の使用に際しては、次のルールが適用されます。

- アスタリスクはドメイン名の先頭に使用できます。
- アスタリスクの後ろにはピリオド (.) が必要です。

表 19-2. ワイルドカードの例

有効なワイルドカードの例:	無効なワイルドカードの例:
• *.example.com	• *example.com • example.*.com • example.*

内部ドメインの設定

手順

1. 左側のナビゲーションペインで、[管理] > [内部ドメイン] の順にクリックします。

   [内部ドメイン] 画面が表示されます。

2. 検索対象から除外する内部ドメインの名前を入力します。
3. [追加 >>] をクリックして、[内部ドメイン] リストにドメインを移動します。
4. 内部ドメインのリストをインポートするには、[インポート] をクリックします。内部ドメインのリストを TXT ファイルにエクスポートするには、[エクスポート] をクリックします。
5. [保存] をクリックします。

製品ライセンス

[製品ライセンス] 画面 ([管理] > [製品ライセンス]) には、ライセンスの有効期限、ステータス、バージョン、およびアクティベーションコードに関する情報が表示されます。

次のオプションを使用して製品ライセンスを管理できます。

- ステータスの更新 –製品ライセンスをアップデートします。
- 新しいコード –新しいアクティベーションコードを使用します。

Trend Micro Apex Central について

Trend Micro Apex Central™は、プログラムの物理的な場所またはプラットフォームとは関係なく、ウイルス対策およびコンテンツセキュリティプログラムを一元的に管理できるソフトウェア管理ソリューションです。このアプリケーションを使用することにより、企業のウイルス/不正プログラムおよびコンテンツセキュリティポリシーの管理を簡略化できます。

- Apex Central サーバ: Apex Central サーバは、Apex Central アプリケーションがインストールされたコンピュータです。Web ベースの Apex Central 管理コンソールは、このサーバ上に作成されます。
- エージェント: エージェントとは、Apex Central が製品を管理できるようにする、製品サーバ上にインストールされるアプリケーションです。エージェントは、Apex Central サーバからのコマンドを受信し、管理下の製品に適用します。また、製品からログを収集して、Apex Central に送信します。Apex Central エージェントが Apex Central サーバと直接通信することはありません。その代わりにエージェントは、コミュニケータと呼ばれるコンポーネントを介して通信します。
- コミュニケータ: コミュニケータは、Apex Central システムの通信バックボーンであり、Trend Micro Management Infrastructure の一部です。Apex Central サーバから管理下の製品へのコマンド、および製品から Apex Central サーバへのステータスレポートは、すべてこのコンポーネントを経由します。各製品サーバにインストールされるコミュニケータは 1 つだけです。コミュニケータは、上記サーバのすべてのエージェントの要求を処理します。

- エンティティ: エンティティとは、[製品ディレクトリ] リンクに表示される管理下の製品を指します。これらのアイコンは、[エンティティ] セクションのディレクトリツリーで確認できます。ディレクトリツリーは、Apex Central コンソールに格納されている、管理対象のエンティティすべてを、構造で示したものです。

Trend Micro Management Communication Protocol について

Trend Micro™ Management Communication Protocol (以下、MCP) は、トレンドマイクロの管理下の製品用のエージェントです。Apex Central と Trend Micro InterScan for Microsoft Exchange との通信に使用されており、次のような利点があります。

- ネットワーク負荷とパッケージサイズの低減
- NAT およびファイアウォール環境のサポート
- HTTPS サポート
- 一方向および双方向の通信のサポート
- シングルサインオン (SSO) サポート
- クラスタノードのサポート

InterScan と Apex Central の連携

- Apex Central または Control Manager を使用すると、複数の InterScan サーバに同じ設定を適用できます。
- Apex Central では、管理者は、情報漏えい対策ポリシー (ルール) を設定して、Apex Central 管理コンソールから InterScan サーバにそのルールを直接配信することができます。
- また、Apex Central で、ウイルスパターンファイルや他のダウンロードを同期することもできます (Apex Central はインターネットを使用してトレンドマイクロにアクセスし、その後、イントラネットを使用して InterScan のさまざまなインスタンスにアップデートを配信します)。
- Apex Central のドメインに含まれていない、ネットワーク上の各 InterScan インスタンスは、ウイルスパターンファイルや他のアップデートのダウンロードをそれぞれ個別に実行します。

詳細については、Apex Central のドキュメントを参照してください。

Apex Central または Control Manager への登録

管理者は、Apex Central を使用して InterScan を管理できます。

Apex Central の製品管理の詳細については、「Trend Micro Apex Central 管理者ガイド」を参照してください。

手順

1. [管理] > [Apex Central の設定] の順にクリックします。

   [Apex Central の設定] 画面が表示されます。

2. [接続設定] の [エンティティ表示名] フィールドに、InterScan サーバの名前を入力します。

3. [Apex Central サーバの設定] で、次の項目を指定します。

   a. Apex Central サーバの IP アドレスまたはホスト名を [サーバの FQDN または IP アドレス] フィールドに入力します。

   b. Apex Central のセキュリティを「中」(Apex Central と、管理下の製品の MCP エージェントとの間で、HTTPS 通信および HTTP 通信を許可) に設定した場合は、[HTTPS による接続] を選択します。

   c. ネットワークで認証が必要な場合は、IIS サーバのユーザ名とパスワードを [ユーザ名] および [パスワード] フィールドに入力します。

4. [MCP プロキシの設定] で、次の設定を行います。

   a. Apex Central との通信にプロキシサーバを使用する場合は、[Apex Central サーバとの通信にプロキシサーバを使用する] を選択します。

   b. MCP エージェントが Apex Central との通信に使用するポート番号を入力します。

   c. プロキシプロトコルを選択します。

   d. プロキシサーバの IP アドレスまたはホスト名を [サーバの FQDN または IP アドレス] フィールドに入力します。

e. Apex Central のセキュリティを「中」(Apex Central と、管理下の製品の MCP エージェントとの間で、HTTPS 通信および HTTP 通信を許可) に設定した場合は、[HTTPS による接続] を選択します。

f. プロキシサーバで認証が必要な場合は、プロキシサーバのユーザ ID とパスワードを [ユーザ ID] および [パスワード] フィールドに入力します。

5. NAT デバイスを使用する場合は、[双方向通信ポート転送] で [双方向通信ポート転送を有効にする] を選択して、NAT デバイスの IP アドレスを [IP アドレス] に、ポート番号を [ポート] に入力します。

6. Apex Central にスパムメールログを送信する場合は、[スパムメールログ] で [スパムメールログを Apex Central に送信する] を選択します。

注意

他のフィルタログは、Apex Central が登録されると初期設定でアップロードされます。

---

7. [不審オブジェクト] で、次の設定を行います。

a. InterScan で Apex Central の不審オブジェクトのリストを利用する場合は、[不審オブジェクトリストを有効にする] を選択します。InterScan が、統合された不審オブジェクトのリスト (仮想アナライザとユーザ定義オブジェクトを含む) を同期して、セキュリティリスク検索に適用します。

b. 不審オブジェクトの検出に関する通知を受信するには、[不審オブジェクトの検出通知を有効にする] を選択します。セキュリティリスク検索による検出の詳細は、通知設定に準拠します。

InterScan は Smart Protection Network を利用して URL 内の不審オブジェクトを検出します。ファイル内の不審オブジェクトの検索と判定の処理は、次の優先順位に従って行われます。

ユーザ定義の不審オブジェクト > パターンファイルに基づくローカル検索 > 仮想アナライザがレポートした不審オブジェクト

InterScan の処理と Apex Central の設定のマッピングは、次の表に定義されています。

表 19-3. 不審オブジェクトに対する処理のマッピング表

種類	APEX CENTRAL の処理設定	INTERSCAN の処理
不審オブジェクトのファイリング	ログ	放置
	ブロック	テキスト/ファイルで置換
	隔離	メッセージ全体の隔離 (リアルタイム検索) メッセージ部分の隔離 (手動検索/予約検索)

注意

不審オブジェクトと不審オブジェクトのリストの詳細については、Trend Micro Apex Central 管理者ガイドの「Connected Threat Defense」の章を参照してください。

Apex Central からの InterScan の登録解除

手順

1. [管理] > [Apex Central の設定] の順にクリックします。

   [Apex Central の設定] 画面が表示されます。

2. [接続ステータス] で、[登録解除] をクリックします。

   進行状況を示す画面が表示されます。

システムデバッグの使用

InterScan の [システムデバッグ] 画面から、デバッグを行ったり、InterScan の処理ステータスをレポートしたりできます。予期しない問題が発生した場合、InterScan を使用してデバッグログを生成し、トレンドマイクロのサポートセンターに送信して解析を依頼できます。

手順

1. メインメニューで [管理] > [システムデバッグ] を選択します。

   [システムデバッグ] 画面が表示されます。

2. デバッグするモジュールを選択します。
   - InterScan for Microsoft Exchange Master Service
   - InterScan for Microsoft Exchange Remote Configuration Server
   - InterScan for Microsoft Exchange System Watcher
   - ストアレベルの検索 (Exchange Server 2013、2016、および 2019)
   - トランスポートサービス
   - CGI (Common Gateway Interface)
   - エンドユーザメール隔離 (Exchange Server 2013)
   - Apex Central
3. [デバッグログ数] フィールドで、作成するデバッグログファイルの数を指定します。
4. [適用] をクリックします。

注意

デバッグを有効または無効にした後にサービスを再起動する必要はありません。

パート IV

ヘルプの参照

第 20 章

セキュリティリスクについて

この章では、ネットワークに対して考えられるリスクを把握するのに役立つように、セキュリティリスクについて説明します。

内容は次のとおりです。

用語の理解

コンピュータセキュリティは急速に変化しています。コンピュータおよびネットワークに対する潜在的な危険または好ましくない活動を説明するために、さまざまな用語や語句が管理者や情報セキュリティの専門家によって考案および採用されています。本書で使用するそれらの用語とその意味を次で説明します。

ここで説明する用語には、実際のセキュリティリスクを表すものと、迷惑な、歓迎されない活動を表すものとがあります。トロイの木馬、ウイルス/不正プログラム、ワームなどは、実際のセキュリティリスクを表す用語の一例です。ジョークプログラム、スパイウェア/グレーウェアなどの用語は、害を及ぼす可能性はあっても、単に迷惑で歓迎されないという程度の活動を表すのに使用されます。InterScan は、この章で説明するすべての事象からの保護を実現します。

インターネット上の脅威について

存在を確認されているウイルス/不正プログラムだけでも数千にのぼり、さらに多くのウイルス/不正プログラムが毎日作成されています。ウイルス/不正プログラムに加えて、企業のメールシステムや Web サイトの脆弱性を突いた、新たな脅威の存在が次々に明らかになっています。こうした脅威には、スパイウェア/グレーウェア、フィッシングサイト、ネットワークウイルス/不正プログラム、トロイの木馬、ワームなどがあります。

これらの脅威は、セキュリティリスクと総称されます。セキュリティリスクの主な種類は、次のように要約できます。

表 20-1. インターネット上の脅威

脅威の種類	特性
高度な脅威	高度な脅威は、従来とは異なる方法でシステムを攻撃またはシステムに感染します。ヒューリスティック検索を使用すると、高度な脅威を検出して企業のシステムへの損傷を低減できます。ATSE が検出する高度な脅威の代表的なものを次に示します。 • APT (Advanced Persistent Threats): APT は、企業やリソースを標的とした攻撃です。一般に、従業員へのソーシャルエンジニアリング攻撃が、その企業を重大なリスクに直面させる一連の活動へと発展します。 • 標的型攻撃: 標的型攻撃とは、攻撃者が特定の対象を強引に追跡して危険にさらす、計画的なコンピュータ侵入を指します。この攻撃では、横方向に移動して機密情報を抜き出せるように、攻撃者は標的のネットワーク内に居続けようします。 • エクスプロイト: エクスプロイトとは、ソフトウェアの脆弱性を悪用するまたは狙うために攻撃者が作成したコードです。このコードは、一般に、不正プログラムに組み込まれます。 • ゼロデイ攻撃: ゼロデイ攻撃とは、ソフトウェアの今まで知られていなかった脆弱性を突いて行われる攻撃です。
DoS (Denial of Service) 攻撃	DoS 攻撃は、不要なタスクによりメールサーバのリソースに負担をかけることで実行されます。解凍されると非常に大きなファイルになるファイルを InterScan が検索しないようにすることにより、この問題の発生を回避できます。
フィッシング	クレジットカードや銀行口座番号などの個人情報の確認をユーザに求める、詐欺を目的とした一方的に送りつけられるメール。
スパイウェア/グレーウェア	個人や組織に関する情報を当人が知らないうちに収集するのを助ける技術。

脅威の種類	特性
トロイの木馬型プログラム	多くの場合は不正な、予期しない、または権限のない処理を実行する不正プログラム。トロイの木馬はシステムに損害を与え、予期しないシステム動作を引き起こし、システムのセキュリティを危険にさらしますが、ウイルス/不正プログラムと違って増殖しません。
ウイルス/不正プログラム	破壊的なペイロードを伝送し、増殖して、他のシステムへの感染を急速に拡大するプログラム。ウイルス/不正プログラムはコンピュータにとって最も有力な脅威と言えます。
ワーム	自己完結型のプログラムまたはプログラムのセットで、多くの場合ネットワーク接続またはメール添付ファイルを通じて、自己の機能の複製または自己の一部を他のコンピュータシステムに感染させます。
その他の不正コード	InterScan は、分類が困難であっても Exchange にとって著しい脅威となる不正コードを検出します。このカテゴリは、明確に分類されない種類の脅威に対して InterScan で処理を実行させるときに便利です。
パックされたファイル	パックされたファイルとは、メールに添付されて届く、圧縮されたリアルタイムの実行可能ファイル内に潜む不正コードです。IntelliTrap では、パックされたファイルを検出すると、そのファイルに対してパッキングアルゴリズムを検索します。IntelliTrap を有効にすると、InterScan が感染した添付ファイルに対してユーザ定義の処理を実行し、送信者、受信者、または管理者へ通知を送信します。
ランサムウェア	感染したシステムの画面やファイルをロックすることによって使用不能にしたのち、元に戻すことと引き換えに「身代金」を要求する不正プログラムです。暗号化型ランサムウェアと総称される最近のランサムウェアは、感染したシステム上の特定の種類のファイルを暗号化し、暗号化解除キーと引き換えにオンラインの決済システムで金銭を支払うよう要求します。

ウイルス/不正プログラム

コンピュータウイルス/不正プログラムとは、ファイルを感染させることによって複製する能力を持ったコードのセグメントです。ファイルがウイルス/不正プログラムに感染すると、ファイルが実行されるときにウイルス/不正プロ

グラムも実行され、ウイルス/不正プログラムのコピーがファイルに添付されます。このことによって、感染したファイルがさらに他のファイルを感染させるようになります。生物学上のウイルスと同様に、コンピュータウイルス/不正プログラムは急速に広がり、多くの場合、撲滅するのが困難です。

一部のコンピュータウイルス/不正プログラムは、増殖することに加えて、別の共通点も持っています。それは、ペイロード (発病機能を担う部分) を運ぶダメージルーチンです。ウイルスのペイロードは、メッセージや画像を表示するだけの場合もありますが、ファイルを破壊したり、ハードディスクを再フォーマットしたり、その他の被害を引き起こしたりする可能性もあります。ウイルスにダメージルーチンが含まれていない場合でも、ストレージ領域やメモリを消費し、コンピュータの全体的なパフォーマンスを低下させて、問題を引き起こすことがあります。

一般にウイルス/不正プログラムは次の 3 つに大別されます。

表 20-2. ウイルス/不正プログラムの種類

種類	説明
ファイル感染型	ファイル感染型ウイルス/不正プログラムには、DOS ウイルス/不正プログラム、Windows ウイルス/不正プログラム、マクロウイルス/不正プログラム、およびスクリプトウイルス/不正プログラムなどさまざまな種類があります。これらすべてにはウイルス/不正プログラムとしての共通の特徴がありますが、感染するホストファイルまたはプログラムの種類が異なります。
システム領域感染型	システム領域感染型ウイルス/不正プログラムはハードディスクのパーティションテーブルやハードディスクおよびフロッピーディスクのブートセクタに感染します。

種類	説明
スクリプト	スクリプトウイルス/不正プログラムはスクリプトプログラミング言語で記述されたウイルス/不正プログラムです。Visual Basic スクリプト、JavaScript などで記述され、通常は HTML ドキュメントに埋め込まれています。 VBScript (Visual Basic Script) および Jscript (JavaScript) ウイルス/不正プログラムは Microsoft の Windows Scripting Host を利用して動作し、他のファイルに感染します。Windows Scripting Host は Windows 98 および Windows 2000 などの Windows OS に含まれるので、単に Windows のエクスプローラから `*.vbs` や`*.js` ファイルをダブルクリックするだけでウイルス/不正プログラム活動が実行されます。 ではスクリプトウイルス/不正プログラムのどこが特別なのでしょうか。スクリプトウイルス/不正プログラムは、アセンブリタイプのプログラミング知識を必要とするバイナリウイルス/不正プログラムとは異なり、テキストでプログラミングされます。スクリプトウイルスは、下位レベルのプログラミングを必要とせず、可能な限りコンパクトなコードで機能を実現します。また Windows に事前に定義されているオブジェクトを使用して、感染したシステムの多くの部分に容易にアクセスすることもでき、たとえばファイルを感染させたり、マスメーリングを実行したりします。さらに、コードがテキストで記述されるので、他者がそのコードの枠組みを簡単に解読し模倣できます。そのため、多くのスクリプトウイルス/不正プログラムには改変された亜種がいくつか存在します。 たとえば「I love you」ウイルスの出現直後、ウイルス対策ベンダーは、件名やメールの本文が改変されて広まった、オリジナルのコードのコピーを発見しました。

どのような種類のウイルスであっても、その基本的な仕組みは同じです。ウイルスには自己の複製を明示的に作成するコードが含まれます。ファイル感染型ウイルス/不正プログラムの場合は通常、感染したプログラムをユーザが誤って実行したときに、制御を取得するための改変が加えられています。ウイルスコードの実行が終了すると、多くの場合、感染しているファイルには何も問題がないように見せるためにオリジナルのホストプログラムに制御が戻されます。

また、異なるプラットフォーム間で活動するウイルス/不正プログラムもあります。この種のウイルス/不正プログラムは、たとえば Windows と Linux などのように、異なるプラットフォームに属するファイルにも感染します。ただし、このようなウイルス/不正プログラムは非常にまれで、その機能が 100% 実現されることはほとんどありません。

ウイルス/不正プログラム作成者

従来は、高い技術を持つ個人が単独でウイルス/不正プログラムを作成し、コンピュータ、ネットワークサーバ、またはインターネットにそれを持ち込んでいました。その動機としては、エゴ、復讐、妨害行為、不満などが挙げられてきました。

現在では、マクロウイルス/不正プログラム、大量メール送信ソフト、潜在的に高い破壊力を持つその他のウイルス/不正プログラムの作成に特殊な技術は必要ありません。「ウイルスキット」がインターネット上でまん延しているため、インターネットや企業の通信を混乱させて自分の力を試したいと思う者が、それを自由に入手できるからです。

これに加え、高度なスパイウェア/グレーウェアプログラムやフィッシングサイトを作成する、国外からの組織犯罪が増えています。これらはスパムメールを大量に配信することによって実行されるため、パスワードやクレジットカード番号などの個人情報を少ない労力で引き出すことが可能です。

不正プログラムの名前付け

システム領域感染型ウイルスおよび一部のファイル感染型ウイルスを除き、不正プログラムは、次の形式に従って名前を付けられます。

<プレフィックス>_<脅威名>.<サフィックス>

名前付け規則で使用されるサフィックスは、脅威の変種を示しています。新しい脅威 (脅威のバイナリコードが既存のセキュリティリスクのいずれにも似ていないという意味) に割り当てられるサフィックスは、アルファベット文字「A」です。さらに新しい変種が見つかった場合は、「B」、「C」、「D」というように、サフィックスが順に割り当てられます。場合によっては、特別なサフィックス (一般的な検出を示す「.GEN」や、変種が壊れたり機能しない場合の「.DAM」など) が脅威に割り当てられることがあります。

プレフィックス	説明
プレフィックスなし	システム領域感染型ウイルスまたはファイル感染型ウイルス
1OH	ファイル感染型ウイルス
ADW	アドウェア

プレフィックス	説明
ALS	LISP 自動スクリプト不正プログラム
ATVX	ActiveX の不正コード
BAT	バッチファイルのウイルス
BHO	ブラウザヘルパーオブジェクト - 破壊的ではないツールバーアプリケーション
BKDR	バックドア型ウイルス
CHM	不正な Web サイトで見つかったコンパイル済み HTML ファイル
COOKIE	データ収集目的で、ユーザの Web での行動を追跡するために使用される Cookie
COPY	自分自身をコピーするワーム
DI	ファイル感染型ウイルス
DIAL	ダイヤラープログラム
「DOS、DDOS」	セキュリティ保護されウイルス対策が施された企業 Web サイトへのアクセスを妨げるウイルス
ELF	実行可能なリンク形式のウイルス
EXPL	他のカテゴリに該当しないセキュリティホール
FLOODER	遠隔地にいる悪意のあるハッカーが、特定の IP でデータを氾濫させ、ターゲットシステムを停止させるツール
FONO	ファイル感染型ウイルス
GCAE	ファイル感染型ウイルス
GENERIC	メモリに常駐する、システム領域感染型ウイルス
HKTL	ハッキングツール
HTML	HTML ウイルス
IRC	インターネットリレーチャットの不正プログラム
JAVA	Java の不正コード

プレフィックス	説明
JOKE	ジョークプログラム
JS	JavaScript のウイルス
NE	ファイル感染型ウイルス
NET	ネットワークウイルス
PALM	Palm PDA ベースの不正プログラム
PARITY	システム領域感染型ウイルス
PE	ファイル感染型ウイルス
PERL	PERL で作成されたファイル感染型ウイルスなどの不正プログラム
RAP	リモートアクセスプログラム
REG	システムレジストリを変更する脅威
SPYW	スパイウェア
SYMBOS	Symbian OS を使用した電話に影響を与えるトロイの木馬
TROJ	トロイの木馬
UNIX	Linux/UNIX スクリプトの不正プログラム
VBS	VBScript のウイルス
WORM	ワーム
W2KM、W97M、X97M、P97M、A97M、O97M、WM、XF、XM、V5M	マクロウイルス

圧縮ファイル

圧縮とアーカイブは、特にメール添付ファイル、FTP、HTTP などのファイル転送では、最も一般的なファイル保存方法です。ただし、圧縮ファイルでウイルス/不正プログラム検出を行う前には、まず解凍する必要があります。サポートしていないタイプの圧縮ファイルについては、圧縮ファイル内の個々

のファイルにではなく、圧縮ファイル全体に対して検出時の処理が実行されます。

InterScan では現在、次の圧縮形式をサポートしています。

- 抽出: 複数のファイルが、次の種類の 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、および ACE
- 展開: ファイルが 1 つだけ、次の種類の 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、および Petite
- 復元: ファイルがバイナリから ASCII に変換されている場合に使用します。メールシステムで広く使われている方法です。UUENCODE および BINHEX

注意

InterScan では、サポートしていない圧縮形式については、第 1 圧縮階層より下の階層に含まれるウイルス/不正プログラムを検出できません。

InterScan では、圧縮ファイルを検出すると、次の操作を実行します。

1. 圧縮ファイルを抽出し、検索します。

   InterScan では、最初の圧縮階層の抽出から開始します。第 1 階層の抽出後、第 2 階層に進み、それ以降も最大 20 階層までのユーザが設定したすべての圧縮階層を検索します。

2. 感染ファイルに対してユーザが設定した処理を実行します。

   InterScan では、圧縮形式で検出された感染ファイルに対しても、その他の感染ファイルと同じ処理を実行します。たとえば、感染ファイルに対する処理として [メッセージ全体の隔離] を選択すると、InterScan は感染ファイルが検出されたメッセージ全体を隔離します。

   InterScan では、PKZIP と LHA の 2 種類の圧縮ルーチンからファイルを駆除できます。ただし、InterScan では、これらの圧縮ルーチンを使用して圧縮されたファイルの第 1 階層のみを駆除できます。

ジョークプログラム

ジョークプログラムとは、一般的には悪意のない、通常の実行可能プログラムです。ジョークプログラムはコンピュータユーザをからかう目的で作成されます。データを破壊する意図はありませんが、場合によっては、データの損失を招く可能性のある操作 (古いバックアップからのファイルの復元、ドライブのフォーマット、ファイルの削除など) をユーザが誤ってしてしまうことがあります。

ジョークプログラムは通常の実行可能プログラムであるため、他のプログラムに感染したり、コンピュータシステムやデータに損傷を加えたりすることはありません。時折、一時的にマウスやキーボードなどのデバイスの設定を変更することはあります。しかし、ジョークプログラムが終了するか、コンピュータを再起動すれば、コンピュータは元の状態に戻ります。ジョークプログラムは、一般には無害ですが、組織にとっては大きな損害となる可能性があります。

マクロウイルス/不正プログラム

マクロウイルス/不正プログラムは、アプリケーション固有のものです。Microsoft Word (`.doc`) や Microsoft Excel (`.xls`) などのアプリケーションに含まれるマクロユーティリティに感染します。したがって、`.doc`、`.xls`、`.ppt` など、マクロ対応のアプリケーションに共通する拡張子の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、アプリケーションのデータファイル間で伝染するため、阻止できない場合、最終的に膨大な数のファイルが感染するおそれがあります。

これらのファイルタイプはメールに添付されることが多いので、マクロウイルス/不正プログラムはメールの添付ファイルに入り込み、インターネットを利用して簡単にまん延します。

InterScan では、次の方法でサーバをマクロウイルス/不正プログラムの感染から守ります。

- 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とは、評価的なウイルス/不正プログラム検出方法です。この方法は、既知のウイルスシグネチャを持たないウイルス/不正プログラムおよび脅威の検出に優れています。

- 検索されたファイルのすべてのマクロコードを削除します。

マスメーリング型ウイルス

メールを標的としたウイルス/不正プログラム、たとえば悪名高い Melissa、Loveletter、AnnaKournikova などは、感染したコンピュータのメールクライアントを自動化することで、メールを通じてウイルスを増殖させる能力を持ちます。マスメーリング型の活動とは、Exchange 環境内でクライアントやサーバの間に感染が急速に拡大する状況を表しています。マスメーリング型ウイルスは、駆除に費用がかかり、ユーザの間でパニックを引き起こす可能性があります。トレンドマイクロでは、マスメーリング型ウイルスが一般的に示す活動を検出するウイルス検索エンジンを設計しました。その活動は、トレンドマイクロのアクティブアップデートサーバを使用してアップデートされる、ウイルスパターンファイルに記録されます。

InterScan では、マスメーリング型の活動を検出するたびに、マスメーリング型ウイルスに対して特別な処理を実行できます。マスメーリング型の活動に対して設定される処理は、その他すべての処理に優先されます。マスメーリング攻撃に対する初期設定の処理は、[メッセージ全体の削除] です。

たとえば、メール内にワームまたはトロイの木馬を検出した場合に、そのメッセージを隔離するように InterScan を設定します。また、マスメーリング型ウイルスの検索を有効にして、マスメーリング型の活動を示すすべてのメッセージを削除するように InterScan を設定します。InterScan が、MyDoom の変種などのワームを含むメッセージを受信します。このワームは、独自の SMTP エンジンを使用して、感染したコンピュータから収集したメールアドレスに自身を送信します。InterScan は MyDoom ワームを検出し、マスメーリング型の活動を認識すると、そのワームを含むメールを削除します。それに対して、マスメーリング型の活動を示さないワームには、隔離処理を実行します。

トロイの木馬型プログラム

トロイの木馬は、ギリシャ神話のトロイの木馬にちなんで命名された脅威の一種です。ギリシャ神話のトロイの木馬と同じように、ネットワークを脅かすトロイの木馬は、そのコード内に悪意のある不正コードを隠し持っています。トロイの木馬は表面上は無害のように見えますが、実行すると、厄介なシステムの動作障害を発生させたり、データの損失や機密情報の漏えいを招いたりします。

たとえば、「happy birthday」というトロイの木馬は、歌を再生し、画面にダンスのアニメーションを表示するかたわら、バックグラウンドでポートを開

き、ファイルを投下します。そして悪意のあるハッカーが、このファイルを介してコンピュータを操作し、何らかの企みを実行しようとします。よくある企みの 1 つは、コンピュータを支配して、スパムメールをばらまくことです。また、キーストロークを収集し、キーストロークに保管されたすべてのデータと共に悪意のあるハッカーに送る、という企みもあります。

トロイの木馬はウイルスや不正プログラムとは異なります。ウイルスや不正プログラムと違って、ファイルへの感染や増殖は起こしません。ウイルス検索エンジンは、このような脅威を検出してログに記録し、指定された処理を実行します。

ただし、トロイの木馬の場合、その影響をシステムから除去するには、単なる削除や隔離だけでは十分ではありません。その後にクリーンナップを実行する必要があります。つまり、システムにコピーされた可能性があるプログラムを削除し、ポートを閉じ、レジストリのエントリを削除します。

ワーム

自己完結型のプログラムまたはプログラムのセットで、自己の機能の複製または自己の一部を他のコンピュータシステムに感染させます。通常、ネットワーク接続またはメールの添付ファイルを介してまん延します。ワームはウイルス/不正プログラムとは異なり、自身をホストプログラムに添付する必要がありません。ワームは、多くの場合、Microsoft™ Outlook™などのメールアプリケーションを使用してまん延します。また、ユーザがダウンロードすることを想定して、自己の複製を共有フォルダに作成したり、Kazaa などのファイル共有システムを利用して感染します。場合によっては、ICQ、AIM、mIRC などのチャットアプリケーションやその他のピアツーピア (P2P) プログラムを使用して、自己の複製を感染させます。

Zip of Death

「Zip of death」は、ウイルス対策ソフトウェアやネットワークトラフィックをチェックするセキュリティアプリケーションに大きな負荷を与え、ネットワークをダウンさせるように設計された不正行為です。

ハッカーは、特殊な技法を用いて、解凍後 15GB 以上に達する場合もあるファイルを 500KB のファイルサイズまで圧縮します。別の手口として、解凍するとシステムをクラッシュさせるほどの大量の数のファイルを圧縮するというものもあります。

InterScan では、解凍する圧縮ファイルのサイズおよびファイル数に制限を設定できます。制限値に達すると、InterScan では解凍を中止し、検索の制限条件外のファイルに対して指定された処理が実行されます。

スパイウェア/グレーウェアについて

クライアントは、ウイルス/不正プログラム以外の潜在的な脅威の危険にもさらされています。グレーウェアは、ネットワーク上のコンピュータのパフォーマンスに悪影響を与え、セキュリティ上、機密保持上、および法律上の重大なリスクを組織にもたらします。

表 20-3. グレーウェアの種類

種類	説明
スパイウェア	アカウントユーザ名やパスワードなどのデータを収集し、そのデータを第三者に送信します。
アドウェア	広告を表示し、ユーザのネットサーフィンの好みなどのデータを収集して、そのユーザを対象とする広告を Web ブラウザに表示します。
ダイヤラー	コンピュータのインターネット設定を変更して、あらかじめ設定された電話番号にモデムを通じて電話をかけさせることができます。
ジョークプログラム	CD-ROM トレイを開閉したり、おびただしい数のメッセージボックスを表示したりするなど、コンピュータの異常な動作を引き起こします。
ハッキングツール	ハッカーがコンピュータに侵入できるようにします。
リモートアクセスツール	ハッカーがリモートでコンピュータにアクセスし、制御できるようにします。
パスワード解読アプリケーション	ハッカーがアカウントユーザ名とパスワードを解読できるようにします。
その他	上記以外の種類のグレーウェア。

潜在的なリスクと脅威

スパイウェア/グレーウェアがネットワーク上に存在すると、以下の事態を招く可能性があります。

表 20-4. リスクの種類

種類	説明
コンピュータのパフォーマンスの低下	スパイウェアまたはグレーウェアアプリケーションは、多くの場合、タスクを実行するために、CPU およびシステムメモリのリソースを大量に必要とします。
Web ブラウザ関連のクラッシュの増加	アドウェアなど、ある種のグレーウェアは、多くの場合、ポップアップウィンドウを作成したり、ブラウザのフレームまたはウィンドウに情報を表示したりするように設計されています。そのアプリケーションのコードがシステムのプロセスとやり取りする方法によっては、グレーウェアがブラウザのクラッシュやフリーズを引き起こす場合や、システムの再起動が必要になる場合があります。
ユーザの能率の低下	頻繁に表示されるポップアップ広告を閉じたり、ジョークプログラムの悪影響に対処したりする必要があるために、ユーザが重要な仕事に集中できなくなる可能性があります。
ネットワーク帯域幅の減少	スパイウェアまたはグレーウェアアプリケーションは、多くの場合、ネットワーク内で実行されている別のアプリケーションやネットワーク外の場所に、収集したデータを定期的に送信します。
個人情報および企業情報の損失	スパイウェアまたはグレーウェアアプリケーションが収集するデータは、ユーザが閲覧する Web サイトのリストのように無害なものばかりではありません。スパイウェアまたはグレーウェアは、ユーザが入力するユーザ名とパスワードを収集して、銀行口座などの個人アカウントや、ネットワーク上のリソースにアクセスする企業アカウントにアクセスすることもあります。
法的責任のリスクの上昇	ハッカーがネットワークのコンピュータリソースにアクセスできるようになれば、クライアントコンピュータが使用されて、ネットワーク外のコンピュータに対して攻撃が開始されたり、スパイウェアやグレーウェアがインストールされる可能性があります。その種の活動にネットワークリソースが否応なしに参加させられることにより、他者による被害に対して企業が法的責任を負うことになる場合があります。

スパイウェア/グレーウェアがネットワークに侵入する方法

スパイウェア/グレーウェアが企業のネットワークに侵入するのは、多くの場合、インストールパッケージの中にグレーウェアアプリケーションが組み込まれた正規のソフトウェアを、ユーザがダウンロードするときです。

ほとんどのソフトウェアプログラムには、使用許諾契約書 (EULA) が含まれており、ユーザはダウンロードする前にこれを受け入れる必要があります。通常、EULA には、個人データを収集するためのアプリケーションとその用途に関する情報が記載されていますが、多くの場合、ユーザは、この情報を見過ごすか、法律用語を理解していません。

エンコード形式

InterScan でサポートされているエンコード形式は、次のとおりです。

- BINHEX
- UUencode
- Base64
- Quoted-printable

検索を欺いたりウイルス対策製品を回避したりするために、不正な形式のメールの中に入り込もうとする悪質なセキュリティリスクがますます多くなっています。InterScan 検索エンジンの MIME 解析アルゴリズムでは、MIME 形式のメールを正しく解析し、不正な形式の MIME 形式メールを検出できます。検索エンジンでは、7 ビットと 8 ビットのエンコーディングおよびデコーディングもサポートされています。

MIME (Multipurpose Internet Mail Extensions) タイプ

最上位のメディアタイプです。

サブタイプが指定されていない場合、InterScan では自動的にすべてのサブタイプが含められます。

- application/
- audio/
- image/
- text/
- video/

実際のファイルタイプ

ファイル名を変更して実際のファイルタイプを偽るのは容易です。Microsoft Word などのプログラムは拡張子に依存しないため、ファイル名とは無関係に、そのプログラムで処理できるドキュメントを認識し、開きます。ここに問題があります。たとえば、マクロウイルス入りの Word ドキュメントに「benefits form.pdf」という名前が付けられていたとします。実際のファイルタイプを確認するよう InterScan を設定していないと、このファイルがウイルス検索されていない可能性があるにもかかわらず Word で開いてしまいます。

トレンドマイクロの推奨設定を設定している場合、InterScan はファイルヘッダを開き、内部登録されているデータタイプをチェックして、ファイルの実際のタイプを確認します。

検索対象となるのは、実際にウイルスに感染する可能性があるタイプのファイルに限られます。たとえば、.mid ファイルはすべての Web トラフィックのかなりの部分を占めますが、このタイプのファイルはウイルスを伝播しないことが分かっています。実際のファイルタイプの確認を選択した場合、実際のファイルタイプが判定された後は、この種の不活性なファイルタイプは検索されません。

不正サイト

「不正サイト」とは、スパイウェア/グレーウェア、パスワード解読アプリケーション、キーストロークトラッカー、ウイルス/不正プログラムキットのダウンロードなど、インターネットセキュリティリスクを配布することが分かっている Web サイトまたは URL です。

一見問題のないように見えるサイトで、表面下では、リンクやデータ送信などの「バックエンド」機能すべてをハッカー自身の場所に転送するサイトもあります。

トレンドマイクロでは、LAN クライアントがウイルス/不正プログラムをダウンロードしたり、偽のサイトにだまされることがないように、フィッシングおよびスパイウェアのパターンファイルに確認済みの不正サイトを速やかに追加します。

フィッシング

フィッシングとは、急速に広まっている詐欺の一種で、正当な Web サイトを装って、Web ユーザから個人情報をだまし取るものです。

一般的には、疑いを持たないユーザに、「アカウントに問題がありただちに修正が必要です」または「アカウントが閉鎖されます」というような内容の、緊急を装った本物のようなメールが送信されます。そのメールには、本物によく似た Web サイトへの URL が含まれています (正当なメールおよび正当な Web サイトをコピーするのは簡単ですが、さらに収集したデータを実際に送信する場所、いわゆるバックエンドが変更されています)。

メールには、ユーザにそのサイトにログオンして、いくつかのアカウント情報を確認するように記載されています。そのサイトに入力されるデータは、すべて悪意のあるハッカーに送信されます。ハッカーは、ログオン名、パスワード、クレジットカード番号、またはその他の要求データを盗みます。

フィッシングは、速攻で、安上がりで、簡単に長続きする詐欺です。これらの詐欺の犯人がたくさんもうける可能性もあります。フィッシングは、コンピュータに精通しているユーザでさえも見破ることが難しく、また、法的処置として追跡することも困難です。まして、起訴することは、ほとんど不可能です。

第 21 章

よくある質問

この章では、InterScan の設定に関するよくある質問と、その状況に対処するための手順について説明します。

内容は次のとおりです。

検索とアップデート

パターンファイルまたは Service Pack が最新かどうか、どうすれば分かりますか?

インストールされているモジュールに応じて、InterScan では、次のアップデート可能なファイルを使用できます。

- スマートスキャンエージェントパターンファイル
- ウイルスパターンファイル
- スパイウェアパターンファイル
- IntelliTrap パターンファイル
- IntelliTrap 除外パターンファイル
- ウイルス検索エンジン
- スパムメール対策パターンファイル
- スパムメール対策エンジン
- URL フィルタエンジン
- 高度な脅威検索エンジン
- CI クエリハンドラ
- 高度な脅威相関パターンファイル

利用可能な最新パターンは、手動アップデートの設定または予約アップデートの設定画面で確認できます。

InterScan のバージョンの確認方法

手順

1. InterScan のメインメニューから、[概要] をクリックします。
2. インストール済みのコンポーネント、現在の InterScan のバージョン、およびアップデートのスケジュールの一覧が表示されます。

InterScan のアップデートに使用する最新の Patch の入手先を教えてください

トレンドマイクロでは、これまでに報告された問題に対処するため、またはアップグレード用に、お使いの製品の Patch をリリースすることがあります。利用可能な Patch があるかどうか確認するには、次の URL にアクセスしてください。

https://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

最新版ダウンロードの画面が表示されます。この画面上のリンクからお使いの製品を選択します。Patch には日付が記載されています。まだ適用していない Patch があったら、Readme ドキュメントを開いて、その Patch がお使いの製品に該当するものかどうか確認します。該当する場合は、Readme ファイルに記載されているインストール手順に従ってください。

パターンとキーワード

正規表現とはどのようなものですか?

正規表現は、文字列の照合を実行するために使用します。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。

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。分かりにくい正規表現はパフォーマンスに影響することがあります。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始め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、そのルールを使用した InterScan でのメッセージの管理状況を観察します。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。

表 21-1. 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。

要素	意味	例
+	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。
{}	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。

表 21-2. 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、a、ab、a1 に一致しますが、!&には一致しません。\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、*、&に一致しますが、ace または a1 には一致しません。\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。
\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 vegetables in my soup」という文は検索されませんが、「I like a vegetable in my soup」は検索されます。
\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。

表 21-3. 文字クラス

要素	意味	例
[:alpha:]	任意のアルファベット文字。	`.REG.[[:alpha:]]` は、abc、def、xxx に一致しますが、123 や@#$には一致しません。
[:digit:]	任意の 10 進数文字。\d と機能的には同等です。	`.REG.[[:digit:]]` は、1、12、123 などに一致します。
[:alnum:]	任意の「文字」、つまり、任意の英数字。\w と機能的には同等です。	`.REG.[[:alnum:]]` は、abc、123 に一致しますが、~!@には一致しません。
[:space:]	任意の空白文字。スペース、改行、タブ、改行禁止スペースなどです。\s と機能的には同等です。	`.REG.(vegetable)[[:space:]]` は、「vegetable」の後に任意の空白文字が続く文字列に一致します。したがって、「I like a vegetable in my soup」という文は検索されますが、「I like vegetables in my soup」は検索されません。
[:graph:]	空白、制御文字、または同様のものを除く任意の文字。	`.REG.[[:graph:]]` は、123、abc、xxx、><"に一致しますが、空白または制御文字には一致しません。
[:print:]	任意の文字 ([:graph:] と似ています)。ただし、空白文字が含まれます。	`.REG.[[:print:]]` は、123、abc、xxx、><"、および空白文字に一致します。
[:cntrl:]	任意の制御文字 (例: CTRL + C、CTRL + X)。	`.REG.[[:cntrl:]]` は、0x03、0x08 に一致しますが、abc、123、!@#には一致しません。
[:blank:]	スペースおよびタブ文字。	`.REG.[[:blank:]]` は、スペースおよびタブ文字に一致しますが、123、abc、!@#には一致しません。
[:punct:]	句読点文字。	`.REG.[[:punct:]]` は;:?!~@#$%&*'r;"r;などに一致しますが、123、abc には一致しません。

要素	意味	例
[: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。	`.REG.[[: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。	`.REG.[[: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)。	`.REG.[[:xdigit:]]` は、0a、7E、0f などに一致します。

表 21-4. 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。

要素	意味	例
$	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。
\	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。	• `.REG.C\\C\+\+`は「C\C++」に一致します。 • `.REG.\*`は*に一致します。 • `.REG.\?`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。
\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。

要素	意味	例
\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。

キーワードの使用方法を教えてください

[コンテンツフィルタ] > [ポリシー名] > [ルールの編集]

キーワードは、単語だけに限定されていません。以下のすべてがキーワードに該当します。

- 数字
- 記号
- 短い語句
- 論理演算子で結合された語句
- 正規表現を使用する語句

キーワードを効果的に使用するには

InterScan は、非常に詳細なフィルタを作成する、簡単かつ強力な機能を備えています。コンテンツフィルタルールを作成する際には、次の点に注意してください。

- 初期設定では、InterScan はキーワードに完全一致するものを検索します。正規表現を使用して、キーワードに部分的に一致するものを検索するように InterScan を設定します。
- InterScan では、1 行で複数のキーワードを指定する場合と、別個の行で複数のキーワードを指定する場合では、解析が異なります。

- 実際のキーワードの同義語を検索するように InterScan を設定できます。
- 完全一致、正規表現、キーワードを使用した演算子を使用して、キーワードを以前の設定からキーワードリストへインポートします。

表 21-5. 複数行のキーワードと完全一致を使用する

状況	例	一致/不一致
同じ行に 2 つの語がある場合	bare sexy	一致例: "Click here to see bare sexy beauties." 一致しない例: "Click here to see bare naked sexy hotties."
2 語をカンマで区切った場合	bare, sexy	一致例: "Click here to see hot, bare, sexy beauties." 一致しない例: "Click here to see hot, bare, and sexy beauties."
複数行にわたって複数の語がある場合	nude sexy bare naked	[指定したいずれかのキーワード] を選択する場合 一致例: "This is a nude picture" その他の一致例: "See young, hot, and sexy beauties" [指定したすべてのキーワード] を選択する場合 一致例: "This is a nude picture of sexy buff and bare naked" 一致しない例: "This is a nude picture of sexy buff bare and naked"
同じ行に複数のキーワードがある場合	sex bare nude naked buff	一致例: "Click here for sex bare nude naked buff" 一致しない例: "Click here to see sex that's bare and buff"

キーワードを使用した演算子の使用方法を教えてください

演算子を使用するキーワードをフォーマットするには、以下を参照してください。

演算子を含むキーワードまたはフレーズを入力するには、次のフォーマット例に従ってください。

例: `.WILD. valu*`

注意

演算子の直前および直後にはドットを付けます。最後のドットとキーワードの間にはスペースを入れます。

表 21-6. キーワードを使用した演算子の使用

サポートされているキーワード	仕組み	使用方法
任意のキーワード	その語に一致する内容が検索されます。	その語をキーワードリストに入力して追加します。
OR	OR で区切られているすべてのキーワードが検索されます。 たとえば、apple .OR. orange とします。InterScan は apple または orange を検索します。内容にいずれかが含まれる場合、一致することになります。	含めるすべてのキーワードの間に「.OR.」を入力します。 たとえば、 apple .OR. orange
AND	AND で区切られているキーワードがすべて検索されます。 たとえば、apple .AND. orange とします。InterScan は apple と orange の両方を検索します。両方が内容に含まれていない場合、一致しないことになります。	含めるすべてのキーワードの間に「.AND.」を入力します。 例: apple .AND. orange

サポートされているキーワード	仕組み	使用方法
NOT	検索から NOT 以降のキーワードが除外されます。 例: .NOT. juice とします。「juice」を含まない内容が検索されます。メッセージに「orange soda」とある場合、一致することになりますが、「orange juice」の場合、一致しないことになります。	除外する語の前に「.NOT.」と入力します。 例: .NOT. juice
WILD	WILD はワイルドカードを意味します。ワイルドカードの記号は、語の欠落している部分の代わりです。ワイルドカードの残りの部分が使用されているすべての語が一致することになります。 たとえば、「valu」を含むすべての語を検出する場合、「.WILD. valu*」と入力します。Valumart、valucash、および valubucks はすべて一致となります。 **注意** InterScan では、ワイルドカードコマンド「.WILD.」内での「?」の使用をサポートしていません。	含める語の部分の前に「.WILD.」と入力します。
REG	正規表現を指定するには、たとえば「.REG. a.*e」というように、パターンの前に「.REG.」演算子を追加します。	検出する語のパターンの前に「.REG.」と入力します。 例: 「.REG. a.*e」は、「ace」、「ate」、および「advance」に一致しますが、「all」、「any」、または「antivirus」には一致しません。

ファイルの処理

サイズの大きいファイルの処理方法を教えてください

[セキュリティリスク検索] 画面の [検索の制限条件] には、サイズの大きいファイルの検索遅延に対処するための方法が用意されています。

- メッセージ本文のサイズが次を超える場合 — 指定されたサイズを超えるメールは検索されません。
- 添付ファイルのサイズが次を超える場合 — 指定されたサイズを超える添付ファイルは検索されません。

警告!

これらのオプションによりサイズの大きいファイルは検索されないため、結果的に Web のセキュリティホールとなる可能性があります。トレンドマイクロでは、このオプションは一時的な使用のみに留めることをお勧めします。

圧縮率とはどのようなものですか?

圧縮率は、未圧縮のファイルサイズ/圧縮ファイルサイズの比率です。次の表に、圧縮率の例を示します。

表 21-7. 圧縮率の例

ファイルサイズ (圧縮なし)	ファイルサイズ (圧縮)
500 KB	10KB (圧縮率 50:1)
1,000 KB	10KB (圧縮率 100:1)
1,001 KB	10KB (圧縮率 100:1 超)
2,000 KB	10KB (圧縮率 200:1)

解凍後のファイルのサイズはどのように見積もるのですか?

圧縮されたファイルについて、「x」の値をどのように計算すれば、[解凍ファイルのサイズが圧縮ファイルのサイズの x 倍以上である場合] オプションで効果的に使用できますか?

この機能により、InterScan は DoS (Denial of Service) 攻撃の原因となり得る圧縮ファイルの検索を回避します。DoS 攻撃は、不要なタスクによりメールサーバのリソースに負担をかけることで実行されます。解凍されると非常に大きなファイルになるファイルを InterScan が検索しないようにすることにより、この問題の発生を回避できます。

例: 次の表では、「x」値は 100 です。

表 21-8. 解凍ファイルの例

ファイルサイズ (圧縮なし)	ファイルサイズ (圧縮)	結果
500 KB	10KB (圧縮率 50:1)	検索可
1,000 KB	10KB (圧縮率 100:1)	検索可
1,001 KB	10KB (圧縮率 100.1:1)	検索不可 *
2,000 KB	10KB (圧縮率 200:1)	検索不可 *

* InterScan は検索不能なファイルに対して設定した処理を実行します。

隔離およびログ管理

隔離フォルダとバックアップフォルダでは UNC パスがサポートされますか?

InterScan では、隔離フォルダとバックアップフォルダを設定する際に、Universal Naming Convention (UNC) パスを使用することができます (`¥¥fileserver¥directory` など)。

UNC の隔離フォルダまたはバックアップフォルダを設定するには

1. Exchange サーバと同じドメインにあるリモートエンドポイント上に必要なフォルダを作成します。
2. Exchange サーバのコンピュータアカウントに、UNC パスに対する読み取り/書き込みアクセス許可があることを確認します。

重要

- Exchange Edge サーバでは UNC パスはサポートされません。
- UNC パスには空白を含めることができません。
- クラスタ環境の場合、コンピュータアカウントで選択できるのはクラスタノードのみで、仮想サーバ名は選択できません。

隔離フォルダとバックアップフォルダではマップされたネットワークドライブがサポートされますか?

InterScan では、マップされたネットワークドライブを隔離フォルダとバックアップフォルダに使用できません。リモートの保存場所を使用する場合は、UNC パスを使用してください。

リモートサーバの「検索時間」または「配信時間」はどのように表示されますか?

InterScan は、時間データを変換し、データベースをポーリングするサーバのローカルな時間設定に基づいて表示します。

たとえば、GMT+9 の時間帯にあるリモートサーバが、GMT+8 の時間帯にあるサーバのログをクエリするとします。GMT+8 の時間帯にあるサーバからクエリされると、ログ時間 2014-12-15 13:10:21 GMT+9 が 2014-12-15 12:10:21 GMT+8 に変換されます。

複数のサーバのレポートデータはどのように生成されますか?

InterScan は、時間帯の設定には関係なく、指定された期間に基づいてデータを取得します。サーバが配置されている地域が指定された時間になっていない場合、取得されるデータは「レコード数ゼロ」です。

注意

たとえば、現在の時刻が 14:00 GMT+8 で、GMT+8 の時間帯にあるリモートサーバが、GMT+4 の時間帯にあるサーバの 13:00 から 14:00 までのログをクエリするとします。GMT+4 の時間帯にあるサーバの現在時刻は 10:00 であるため、レコードは返されません。

InterScan は、指定されたサーバから収集した指定された期間のすべてのデータを 1 つのレポートに表示します。指定された期間について、サーバ A に 4 個のログ項目、サーバ B に 5 個のログ項目がある場合、InterScan はその期間について 9 個のエントリを表示します。

ログクエリまたは隔離クエリを一括で生成する前に、InterScan Web サービスポートをファイアウォールのポート除外リストに追加する必要はありますか?

ログクエリや隔離クエリを一括で実行するには、InterScan Web サービスポートをファイアウォールのポート除外リストに追加する必要があります。

注意

初期設定の InterScan Web サービスポートは、HTTPS 用の 16373 です。

エンドユーザメール隔離のスパムメールフォルダを削除した後、再作成することはできますか?

[すべてのクライアントからエンドユーザメール隔離スパムメールフォルダを削除します] オプションを無効にした後、[管理] > [スパムメールの管理] 画面で [エンドユーザメール隔離を有効にする] オプションを有効にするとスパムメールフォルダを再作成することができます。

InterScan によって高度な脅威の分析のために一時的に隔離されたメールを削除するにはどうすればよいですか?

多数のメールが高度な脅威の分析のために隔離されている状態で InterScan のインストール/アンインストールが開始された場合、それらのメールは削除されません。InterScan は「toolDDAnQuarantinedMailsCleaner.exe」という別のツールを自動的に起動し、該当するメールを処理します。通常このツールは正常に実行され、問題は発生しません。ただし、インストール/アンインストール中に例外が発生した場合は、このツールを手動で実行することが必要になる場合があります。

手順

1. ローカル管理者権限で `CMD.exe` を実行します。

2. InterScan のホームディレクトリに切り替えます。
3. 次のいずれかを実行します。
   - インストール時にツールの実行に失敗した場合は、次のコマンドを使用してツールを実行します。

     ```
     toolDDAnQuarantinedMailsCleaner.exe install
     [SMEX_TEMP_QUARANTINE_PATH]
     ```

     注意

     ここで、

     - [SMEX_TEMP_QUARANTINE_PATH]を不審ファイルの隔離パスに置き換えます。

     例:

     ```
     toolDDAnQuarantinedMailsCleaner.exe install "C:\Program
     Files\Trend Micro\Isme\storage\quarantine\Advanced
     threats\temp"
     ```

   - アンインストール時にツールの実行に失敗した場合は、次のコマンドを使用してツールを実行します。

     ```
     toolDDAnQuarantinedMailsCleaner.exe uninstall
     [SMEX_TEMP_QUARANTINE_PATH]
     [SMEX_WTP_TEMP_QUARANTINE_PATH]
     ```

     注意

     ここで、

     - [SMEX_TEMP_QUARANTINE_PATH]を不審ファイルの隔離パスに置き換えます。
     - [SMEX_WTP_TEMP_QUARANTINE_PATH]を不審 URL の隔離パスに置き換えます。

     例:

```
toolDDAnQuarantinedMailsCleaner.exe uninstall
"C:\Program Files\Trend
Micro\Isme\storage\quarantine\Advanced threats\temp"
"C:\Program Files\Trend
Micro\Isme\storage\quarantine\Advanced
threats\SuspiciousURLs"
```

ログ、隔離レコード、およびサーバグループ

リモートサーバあたりのクエリ結果数を増やす方法を教えてください

InterScan では、リモートサーバあたりの結果数が初期設定で最大 3000 レコードに設定されています。ログクエリや隔離クエリの一括実行時に、リモートサーバあたりのクエリ結果数を 3000 レコードより増やしたい場合は、次の隠しレジストリキーを追加します。

パス: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion`

キー: MaxRemoteQuery

タイプ: DWORD

注意

レジストリ値を追加したら、InterScan for Microsoft Exchange Master Service を再起動します。

新しく InterScan をインストールしたサーバをサーバグループリストに反映させる方法を教えてください

[サーバグループ] 画面を初めて開くときに、[表示更新] ボタンをクリックします。ネットワークが自動的にポーリングされ、使用可能なすべての InterScan サーバのリストが返されます。画面を開くときに [表示更新] をクリックしなかった場合は、各グループを開く際にデータの読み込みに多少の時間がかかります。

既存の InterScan サーバをアップグレードするたびに、[表示更新] をクリックしてリストをアップデートしてください。

ログオンと登録

アクティベーションコードはどこで入手できますか?

[管理] > [製品ライセンス]

InterScan は、インストールプロセス中にアクティベートすることも、後で InterScan コンソールを使用してアクティベートすることもできます。InterScan をアクティベートするには、アクティベーションコードを取得している必要があります。

アクティベーションコードの取得

- トレンドマイクロの Web サイトから InterScan をダウンロードした場合は、体験版のアクティベーションコードが自動的に与えられます。
- アクティベーションコードは 37 文字で、次のような形式になっています。

  xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx

- 使用許諾契約書 (製品購入後に取得したもの)

InterScan をアクティベートすると、次のような利点が得られます。

- InterScan パターンファイルおよび検索エンジンのアップデート
- テクニカルサポート
- サポート契約の更新、登録情報とライセンス情報、およびサポート契約更新のお知らせを表示する際の簡単なアクセス

サポート契約の有効期限が切れると、セキュリティアップデートが無効になります。体験版の有効期限が切れると、セキュリティアップデートと検索機能の両方が無効になります。[製品ライセンス] 画面では、アクティベーションコードをオンラインで取得したり、サポート契約更新手順を参照したり、製品の状態を確認したりできます。

リモート SQL Server のデータベースアカウントのパスワードを変更するとどうなりますか?

リモート SQL Server を使用して InterScan をインストールする場合、リモート SQL Server への接続にアカウントが必要です。このアカウントのパスワードを変更した場合、InterScan の設定ファイルでパスワードを手動でアップデートする必要があります。

リモート SQL Server のアカウントのパスワードを手動でアップデートするには

手順

1. コマンドラインインタフェースを開き、InterScan インストールパスのツールフォルダに進みます。

   初期設定のパスは、`C:¥Program Files¥Trend Micro¥Isme¥tools` です。

2. `toolChangeRemoteDBPWD.exe` を使用して次のコマンドを入力し、新しいパスワードを暗号化します。

   ```
   toolChangeRemoteDBPWD.exe -p <出力フォルダのパス> -c <パスワード>
   ```

3. `dbcfg_SQLPassword.txt` を、新しく生成されたファイルに置き換えます。暗号化されたパスワードファイルは、次の場所にあります。

   - `<InterScan インストールパス>¥config¥dbcfg_SQLPassword.txt`

4. InterScan for Microsoft Exchange Master Service を再起動します。

リモート Windows 認証のデータベースアカウントのパスワードを変更するとどうなりますか?

リモート SQL Server を使用して InterScan をインストールする場合、リモート SQL Server への接続にアカウントが必要です。このアカウントのパスワードを変更した場合、InterScan の設定ファイルでパスワードを手動でアップデートする必要があります。

リモート SQL Server のアカウントのパスワードを手動でアップデートするには

手順

1. すべての InterScan サーバのすべてのホスト名を取得し、テキスト (.txt) ファイルに保存します。

   ホスト名の例:

   ```
   ExchangeMailbox01
   ExchangeMailbox02
   ExchangeMailbox03
   ... (など)
   ```

   ファイル名の例:`Server.txt`

2. コマンドラインインタフェースを開き、InterScan インストールパスのツールフォルダに進みます。

   初期設定のパスは、`C:¥Program Files¥Trend Micro¥Isme¥tools` です。

3. 次のコマンドを使用して、InterScan に関連するすべてのサービスをまとめて停止します。

   - for /F %i in (Server.txt) do sc %i stop ScanMail_RemoteConfig
   - for /F %i in (Server.txt) do sc %i stop ScanMail_Master
   - for /F %i in (Server.txt) do sc %i stop ScanMail_SystemWatcher

   注意

   (Server.txt) は実際のファイル名に置き換えます。

4. 次のコマンドを使用して、すべてのホスト名のパスワードをまとめて変更します。

   - for /F %i in (Server.txt) do sc %i config ScanMail_RemoteConfig password=[新しいパスワード]
   - for /F %i in (Server.txt) do sc %i config ScanMail_Master password=[新しいパスワード]
   - for /F %i in (Server.txt) do sc %i config ScanMail_SystemWatcher password=[新しいパスワード]

注意

(Server.txt) は実際のファイル名に置き換えます。

5. 次のコマンドを使用して、InterScan に関連するすべてのサービスをまとめて開始します。

   - for /F %i in (Server.txt) do sc %i start ScanMail_RemoteConfig
   - for /F %i in (Server.txt) do sc %i start ScanMail_Master
   - for /F %i in (Server.txt) do sc %i start ScanMail_SystemWatcher

注意

(Server.txt) は実際のファイル名に置き換えます。

セキュリティの脅威

スパイウェア/グレーウェアとはどのようなものですか?

スパイウェアには、ひそかにデータを収集し、ソースホストに送り返そうとするソフトウェアプログラムやテクノロジが含まれます。このようなプログラムやテクノロジは「ボット」と呼ばれます。

スパイウェアや他のグレーウェアによるセキュリティリスクのカテゴリとして、アドウェア、インターネット cookie、トロイの木馬、監視ツールなどがあります。スパイウェアによって収集される情報の種類は、比較的無害なもの (アクセスした Web サイトの履歴) から、厳重な警戒を要するもの (クレジットカード番号、銀行口座、パスワード) までさまざまです。

スパイウェア/グレーウェアの大半は、ユーザが Web サイトで見つけてダウンロードするスマートなソフトウェアパッケージに含まれています。スパイウェアプログラムには、正規のプログラムに含まれているものもあれば、違法なものもあります。ネットワーク管理者は、特定のクラスのソフトウェアについて、ネットワークに取り込むか、またはブロックするかを判断する必要があります。

スパイウェアは次のようなさまざまな方法でインストールされます。

- ソフトウェアのインストール時に副製品としてインストールされる。
- ポップアップウィンドウで何かをクリックすることによってインストールされる。
- 正規のダウンロードをインストールしたときに、目に見えない「追加プログラム」としてインストールされる。
- トロイの木馬、ワーム、ウイルスを介してインストールされる。

その結果、通常、バックグラウンドでインターネット接続が確立され、この接続によってユーザのコンピュータへの監視経路が開かれます。複数の接続が確立されると、ネットワークのパフォーマンスが低下することもあります。

InterScan では、スパイウェア/グレーウェアを検出したときに次の処理を実行できます。

- テキスト/ファイルで置換 — 感染したコンテンツ、不正なコンテンツ、または望ましくないコンテンツを削除して、テキストまたはファイルに置き換えます。
- メッセージ全体の隔離 — アクセスが制限されたフォルダにメールを移動します。
- メッセージ全体の削除 — メール全体を削除します。
- 放置 — 検出内容をログに記録して、メッセージ部分をそのまま配信します。
- メッセージ部分の隔離 — アクセスが制限されたフォルダにメール本文または添付ファイルを移動します。

増大する危険

「自動ダウンロード」によって、または偽装ポップアップウィンドウの何らかのオプションのクリックによって、不正なスパイウェアと知らずにユーザがインストールしてしまうケースが増加しています。企業のセキュリティ部門が懸念していることは、より機能性の高いスパイウェアによって、キーストロークの監視、ファイルの検索、追加スパイウェアのインストール、Web ブラウザの設定変更、メールやその他のアプリケーションデータの収集などが行われることです。場合によって、スパイウェアで画面ショットを取り込んだり、Web カメラを起動させたりすることも可能です。

企業はその規模の大小を問わず、機密情報の盗難、従業員の生産性の低下、帯域幅の無駄な消費、企業内のデスクトップコンピュータへの被害、スパイウェアに関連したヘルプデスクの呼び出し件数の急増といった問題に取り組む必要があります。スパイウェアはセキュリティ管理とシステム管理の両面を脅かすおそれがあります。

フィッシング詐欺とはどのようなものですか?

フィッシングとは、送信元を実在する正規の企業に偽装したメールのことです。このメッセージは、受信者にリンクをクリックするよう促します。リンクをクリックすると偽の Web サイトに誘導され、パスワード、クレジットカード番号などの個人情報を更新するよう指示されます。これによって受信者から個人情報を盗み、その情報をなりすましに使用しようとしています。

InterScan のコンテンツフィルタ機能では、フィッシングメッセージを検出したときに次の処理を実行できます。

- メッセージ全体の削除

  InterScan によってメッセージ全体が削除されるため、そのメッセージは Exchange から配信されません。

- タグを付加して配信

  メールがフィッシングメールであることを示すためのタグがメールの件名に追加されて、対象の受信者に配信されます。

EICAR テストウイルスとはどのようなものですか?

EICAR (European Institute for Computer Antivirus Research) では、InterScan のインストールと設定のテストに使用できるテスト用「ウイルス」を開発しています。このファイルは、ほとんどのウイルス対策ベンダーのウイルスパターンファイルに含まれるバイナリパターンを含む、感染源とはならないテキストファイルです。これはウイルスではなく、プログラムコードをまったく含みません。

EICAR テストウイルスは、次の URL からダウンロードできます。

https://downloadcenter.trendmicro.com/index.php?regs=jp&prodid=1424

または、次の文字列をテキストファイルに入力し、そのファイルに「`eicar.com`」という名前を付けることにより、独自の EICAR テストウイルスを作成できます。

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!
$H+H*
```

注意

テストの前に、キャッシュサーバとローカルブラウザのキャッシュを消去してください。

誤検出とはどのようなものですか?

誤検出は、Web サイト、URL、「感染した」ファイル、またはメールメッセージが、フィルタソフトウェアにより望ましくない種類のものであると誤って判断されることです。たとえば、「転職/就職」カテゴリのフィルタで、「resume」(再開) と「résumé」(履歴書) が区別されない場合、同僚間の正当なメールが、スパムメールとして検出される場合があります。

次の方法で、今後の誤検出の数を減らすことができます。

1. 最新のパターンファイルにアップデートします。
2. 除外リストに追加して、そのアイテムを検索から除外します。
3. 誤検出の問題をトレンドマイクロに連絡します。

隔離フォルダまたはバックアップフォルダにあるファイルには危険性があるのでしょうか?

隔離フォルダまたはバックアップフォルダにあるファイルには危険性があるのでしょうか?

隔離フォルダおよびバックアップフォルダにあるファイルはすべて、拡張子が削除された特別な形式のファイル名に変更されています。このようにすることで、ファイルが Windows で直接起動されないようになります。ファイルの上でダブルクリックしたり、別の方法で開こうとするなど、実行可能ファイルを誤って起動するのを防ぎます。

ただし、Microsoft™ Office 2003 などのアプリケーションを持っているユーザの場合は、実際のファイルの種類でファイルを認識できるため、危険性があります。このような場合は、拡張子名のないバックアップファイルでも、ユーザが意図せずに起動する可能性があります。

不審なインターネット上の脅威の報告方法を教えてください

フィッシングサイト、または他のいわゆる「不正サイト」(セキュリティリスクの発信源) と思われる不審 Web サイトがある場合は、その URL の評価値を次のポータルで確認したりトレンドマイクロに通知したりできます。

https://global.sitesafety.trendmicro.com/

仮想アナライザ

仮想アナライザの動作モードとそれぞれの使用基準を教えてください

InterScan を仮想アナライザと統合する場合の動作モードには次の 2 つがあります。

- インラインモード: 不審メッセージまたは指定されたメッセージを隔離し、分析のために仮想アナライザに送信します。メッセージは、仮想アナライザで高度な脅威が検出されなければ配信されます。

  実際の環境では、このモードを設定し、[添付ファイルの種類] オプションを [推奨されるファイルタイプ] に設定することをお勧めします。

- 監視モード: 不審メッセージまたは指定されたメッセージをコピーし、分析のために仮想アナライザに送信します。メッセージは、そのまますぐにエンドユーザに配信されます。

  高度な脅威の監視や監査だけが目的の場合は、このモードを設定することをお勧めします。

InterScan が仮想アナライザと統合されている場合、旧バージョンに加えて最新バージョンの InterScan をインストールすることはできますか?

InterScan が仮想アナライザと統合されている場合は、組織のすべての Exchange サーバに同じバージョンの InterScan を導入することを強くお勧めします。

最新バージョンの InterScan では、最新の検索ロジックを利用できるほか、メールのセキュリティ機能も旧バージョンより強化されています。そのため、

旧バージョンの InterScan では、仮想アナライザによる分析後に新しいバージョンからルーティングされるメッセージを認識できない場合があります。

第 22 章

トラブルシューティング

この章では、管理者が手動で実行できる一般的なトラブルシューティング作業について説明します。

内容は次のとおりです。

検索エンジンの手動アップデート

トレンドマイクロでは、InterScan で検索エンジンの自動アップデートをスケジュールすることをお勧めしていますが、検索エンジンは次の手順で手動でアップデートすることもできます。

手順

1. トレンドマイクロの Web サイトから最新の検索エンジンをダウンロードします。

   https://downloadcenter.trendmicro.com/index.php?clk=tbl&clkval=5381&regs=jp&lang_loc=13#fragment--2

2. Windows の [スタート] ボタンをクリックして、[プログラム] > [管理ツール] > [サービス] の順に選択して、次の InterScan サービスを停止します。
   - InterScan for Microsoft Exchange Remote Configuration Server
   - InterScan for Microsoft Exchange Master Service
3. 次の検索エンジンファイルのバックアップを作成します。
   - `¥Program Files¥Trend Micro¥Isme¥engine¥vsapi¥latest¥vsapi64.dll`
4. 新しい検索エンジンファイルを次のディレクトリに展開します

   `¥Program Files¥Trend Micro¥Isme¥engine¥vsapi¥latest¥`
5. InterScan サービスを開始します。
   a. Windows の [スタート] ボタンをクリックして、[プログラム] > [管理ツール] > [サービス] の順に選択します。
   b. 次の各 InterScan サービスを右クリックし、表示されるポップアップメニューから [開始] を選択します。
      - InterScan for Microsoft Exchange Remote Configuration Server
      - InterScan for Microsoft Exchange Master Service

パターンファイル (lpt$vpn.xxx) の手動アップデート

手順

1. トレンドマイクロの Web サイトから最新のパターンファイルをダウンロードします。

   https://appweb.trendmicro.com/ecs/Default.aspx

2. 法人カスタマーサイトより、パターンファイルをダウンロードします。
3. Windows の [スタート] ボタンをクリックして、[プログラム] > [管理ツール] > [サービス] の順に選択して、すべての InterScan サービスを停止します。
4. ダウンロードした圧縮ファイルの内容を次のフォルダに抽出します。

   ```
   ¥Program Files¥Trend Micro¥Isme¥engine¥vsapi¥latest
   ```

5. すべての InterScan サービスを再開してから、InterScan コンソールを更新します。

既知の問題

既知の問題では、一時的な回避方法が必要となる可能性のある、InterScan の予期しない動作について示します。

システム要件、およびインストールやパフォーマンスに影響を与える可能性のある既知の問題については Readme ファイルも確認してください。Readme ファイルには、特定のリリースでの新機能や、その他の役立つ情報も含まれています。

トレンドマイクロ製品の Readme ファイルおよびその他のドキュメントは、次の Web サイトで入手できます。

https://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

既知の問題および考えられる回避方法も、次の製品 Q&A Web サイトに掲載されています。

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

第 23 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

InterScan の Windows イベントログコード

InterScan を監視する際には、Windows のイベントログに記録される通知のイベント ID を参照することがあります。Windows のイベントログについては、次の表を参照してください。

表 A-1. InterScan の Windows イベントログコード

イベント ID	機能	種類/重要度	カテゴリ	説明
3	アプリケーション	エラー	なし	アラート。InterScan のサービス開始に失敗
4	アプリケーション	エラー	なし	アラート。InterScan サービスが使用できない
5	アプリケーション	警告	なし	セキュリティリスク検索の通知
6	アプリケーション	警告	なし	添付ファイルのブロックの通知
7	アプリケーション	警告	なし	コンテンツフィルタの通知
16	アプリケーション	警告	なし	アラート。手動アップデートの失敗

イベント ID	機能	種類/重要度	カテゴリ	説明
17	アプリケーション	情報	なし	アラート。手動アップデートの完了
18	アプリケーション	警告	なし	アラート。最後のアップデート時期が指定時期以前
19	アプリケーション	情報	なし	アラート。手動検索の完了
20	アプリケーション	エラー	なし	アラート。手動検索の失敗
21	アプリケーション	警告	なし	アラート。検索時間が指定時間を超過
22	アプリケーション	警告	なし	アラート。バックアップまたは隔離ディレクトリが含まれるドライブ (ボリューム) 上のディスク空き容量が指定サイズ未満
23	アプリケーション	警告	なし	アラート。隔離およびログ用のデータベースサイズが指定サイズを超過
24	アプリケーション	情報	なし	アラート。予約検索の完了
25	アプリケーション	エラー	なし	アラート。予約検索の失敗
32	アプリケーション	エラー	なし	アラート。予約アップデートの失敗
33	アプリケーション	情報	なし	アラート。予約アップデートの完了
34	アプリケーション	警告	なし	Web レピュテーションの通知
35	アプリケーション	警告	なし	情報漏えい対策の通知

イベント ID	機能	種類/重要度	カテゴリ	説明
257	アプリケーション	警告	なし	アウトブレークアラート、ウイルス/不正プログラムの検出
258	アプリケーション	警告	なし	アウトブレークアラート、駆除不能なウイルス/不正プログラムの検出
259	アプリケーション	警告	なし	アウトブレークアラート、添付ファイルのブロック
260	アプリケーション	警告	なし	アウトブレークアラート、スパイウェア/グレーウェアの検出
513	アプリケーション	エラー	なし	フィルタロードの例外
514	アプリケーション	エラー	なし	アダプタロードの例外
4097	アプリケーション	警告	なし	アラート。Exchange のトランザクションログの含まれるドライブ上のディスク空き容量が指定サイズ未満
4098	アプリケーション	警告	なし	アラート。Exchange のメールストアのサイズが指定サイズを超過
4099	アプリケーション	警告	なし	アラート。連続して待ち行列に格納される Exchange の SMTP メールが指定数を超過
4112	アプリケーション	エラー	なし	ディスク領域が不足しているため、InterScan for Microsoft Exchange Master Service が停止しました。空きディスク領域を増やして、InterScan for Microsoft Exchange Master Service を再開してください。
8193	アプリケーション	情報	なし	(エンドユーザメール隔離)手動管理タスクの処理が開始
8194	アプリケーション	情報	なし	(エンドユーザメール隔離)手動管理タスクの処理が終了

イベント ID	機能	種類/重要度	カテゴリ	説明
8195	アプリケーション	情報	なし	(エンドユーザメール隔離)予約管理タスクの処理が開始
8196	アプリケーション	情報	なし	(エンドユーザメール隔離)予約管理タスクの処理が終了
8197	アプリケーション	情報	なし	(エンドユーザメール隔離)有効化タスクの処理の開始。
8198	アプリケーション	情報	なし	(エンドユーザメール隔離)有効化タスクの処理の終了。
8199	アプリケーション	情報	なし	(エンドユーザメール隔離)無効化タスクの処理の開始。
8200	アプリケーション	情報	なし	(エンドユーザメール隔離)無効化タスクの処理の終了。
20480	アプリケーション	情報	なし	InterScan 製品コンソールにログオンまたはログオフします。
20481	アプリケーション	情報	なし	InterScan の設定変更
20482	アプリケーション	情報	なし	InterScan の管理操作
28672	アプリケーション	情報	なし	セキュリティリスク検索方法の切り替え
28673	アプリケーション	警告	なし	スマートスキャン: ファイルレピュテーションサービスが使用できなかった場合
28675	アプリケーション	情報	なし	スマートスキャン: ファイルレピュテーションサービスが復元された場合
28676	アプリケーション	警告	なし	スマートスキャン: Web レピュテーションサービスが使用できなかった場合

イベント ID	機能	種類/重要度	カテゴリ	説明
28677	アプリケーション	情報	なし	スマートスキャン: Web レピュテーションサービスが復元された場合
28678	アプリケーション	情報	なし	Search & Destroy: 検索に成功した場合
28679	アプリケーション	エラー	なし	Search & Destroy: 検索に失敗した場合
28681	アプリケーション	警告	なし	仮想アナライザ: 仮想アナライザが使用できなかった場合
28682	アプリケーション	情報	なし	仮想アナライザ: 仮想アナライザが復元された場合
28684	アプリケーション	エラー	なし	InterScan データベースにアクセスできません。メールトラフィックは引き続き保護されています。
24578	アプリケーション	情報	なし	InterScan サービスとデータベースの間の接続が復旧しました。
28687	アプリケーション	警告	なし	機械学習型検索サービスを使用できませんでした。
28688	アプリケーション	情報	なし	機械学習型検索サービスが復元されました。
28690	アプリケーション	警告	なし	ライティングスタイルサービスを使用できませんでした。
28691	アプリケーション	情報	なし	ライティングスタイルサービスが復元されました。

付録 B

最適な運用のために

この付録では、最適な運用のための情報を提供します。

内容は次のとおりです。

Microsoft Windows 認証を使用したインストールのためのアカウントの設定

リモート SQL Server へのアクセス時と対象サーバへのログオン時は、同じ Windows アカウントを使用することをお勧めします。

Windows アカウントに最小限必要な権限は次のとおりです。

- ドメインユーザ
- ローカル管理者
- Organization Management
- Exchange の ApplicationImpersonation の役割
- ドメイン管理者 (エンドユーザメール隔離を Exchange 2013 プラットフォームで使用する場合に一時的に必要)
- SQL Server の dbcreator の役割

添付ファイルブロックポリシー

次の表は、推奨される添付ファイルブロック設定を示しています。

表 B-1. 推奨される添付ファイルブロック設定

サーバの役割	設定
エッジサーバ	無効
トランスポートレベルのリアルタイム検索	有効

除外ルールの複製

サーバ管理コンソールを使用して除外ルールを複製します。

表 B-2. 添付ファイルブロック除外ルールの制限事項

リソース	制限事項
プラットフォーム	除外設定は以下のみでサポートされています。 • Exchange Server 2019 • Exchange Server 2016 • Exchange Server 2013 SP1 以上
サーバの役割	• エッジサーバでは、InterScan は、添付ファイルブロックポリシーを実装するための十分な情報を Windows Active Directory から取得できません。 • 除外ルールは、ストアレベルの手動検索および予約検索では適用されません。 • エッジサーバでは、グローバルポリシーのみが適用されます。

サンプル使用シナリオ

シナリオ 1

- シナリオ:

  企業のポリシーでは、すべてのユーザが [音声] という添付ファイルの種類を受信することを禁止している一方で、音楽クラブに属するユーザが mp3 ファイルを受信することを許可しています。

- 解決策:

  1. [指定したものをブロック] > [音声] の順に選択して、グローバルルールを設定します。
  2. 「音楽クラブ」に適用される除外ルールを作成します。
  3. mp3 に対する除外ルールターゲットを設定します。
  4. 一般的なユーザシナリオ 2 (AB 除外設定)。

シナリオ 2

- シナリオ:

企業のポリシーでは、.mp3 ファイル、.doc ファイル、および.exe ファイルをブロックしています。ただし、音楽クラブには.mp3 ファイルの受信を許可して、InterScan には.exe ファイルの受信を許可しています。

- 解決策:

  1. .mp3 ファイル、.doc ファイル、および.exe ファイルをブロックするようにグローバルポリシーを設定します。
  2. 「音楽クラブ」という名前の除外ルールを作成し、.mp3 ファイルを放置するようにこのルールを設定して、優先度を 1 に設定します。
  3. 「InterScan」という名前の除外ルールを作成し、.exe ファイルを放置するようにこのルールを設定して、優先度を 2 に設定します。

既知の問題

あるユーザが「音楽クラブ」グループと「InterScan」グループの両方に属している場合に、メールメッセージに.mp3、.doc、および.exe ファイルが含まれているときは、このユーザは.doc ファイルと.exe ファイルを受信します。

コンテンツフィルタの Active Directory 統合ポリシー

次の表は、推奨されるコンテンツフィルタ設定を示しています。

表 B-3. 推奨されるコンテンツフィルタ設定

サーバの役割	設定
エッジサーバ	無効
トランスポートレベルのリアルタイム検索	有効

コンテンツフィルタポリシーの複製

サーバ管理を使用して、異なる Exchange サーバ間で設定を複製します。同じサーバの役割の間でのみ設定を複製します。

表 B-4. コンテンツフィルタポリシーの制限事項

リソース	制限事項
プラットフォーム	ポリシーは以下のみでサポートされています。 • Exchange Server 2019 • Exchange Server 2016 • Exchange Server 2013 SP1 以上
サーバの役割	• コンテンツフィルタポリシーは、トランスポートレベルのリアルタイム検索のみに適用されます。 • エッジサーバでは、グローバルポリシーのみが適用されます。

情報漏えい対策ポリシー

次の表は、リアルタイム検索に対して推奨される情報漏えい対策設定を示しています。

表 B-5. 推奨される情報漏えい対策設定

サーバの役割	設定
ハブサーバ	ポリシーを [送信メッセージ] に適用
エッジサーバ	無効

注意

情報漏えい対策ポリシーを送信メッセージのみに適用すると、内部ドメインのポリシー違反については検索されません。これにより、情報漏えい対策のリアルタイム検索のパフォーマンスが大幅に向上します。

データ識別子とテンプレートの作成

情報漏えい対策には、管理者が情報漏えい対策ポリシーの作成に使用できる、事前に定義されたテンプレートとデータ識別子が 100 個以上含まれています。これらの事前に定義されたテンプレートとデータ識別子で、企業のデータ保護ニーズの大半に対応できます。ポリシーを作成するときは、ビルトインのアイテムを使用することをお勧めします。

事前に定義されたアイテムが企業の特定のニーズを満たさない場合、管理者は既存のアイテムをコピーして適宜変更できます。使用するテンプレートまたはデータ識別子を選択し、[コピー] をクリックします。新しく作成されたアイテム (<情報漏えい対策アイテム>_Copy) をクリックし、コンテンツを編集します。

注意

事前に定義された情報漏えい対策テンプレートとデータ識別子は変更も削除もできません。

まったく新しいパターンが必要な場合、管理者は Web コンソールを使用して一意のパターンを作成できます。InterScan の情報漏えい対策のパターンには、Perl 互換正規表現 (PCRE) 形式を使用します。ユーザの定義した新しいパターンを情報漏えい対策ポリシーに実装する前に、そのパターンをテストすることをお勧めします。

ヒント

テストが成功した場合にのみ、パターンを保存します。データを何も検出できないパターンは、システムリソースを無駄に消費するため、パフォーマンスに影響することがあります。

InterScan では、情報漏えい対策テンプレートとデータ識別子を DAT ファイル形式でインポートおよびエクスポートできます。DAT ファイルのコンテンツを編集するには、まずアイテムを InterScan 環境にインポートして戻します。エクスポートされた DAT ファイルのコンテンツを変更すると、データが破損して使用できなくなることがあります。

情報漏えい対策ポリシーの複製

サーバ管理コンソールを使用してサーバ間で設定を複製する際、情報漏えい対策ポリシーの設定は同じサーバの役割間で複製することをお勧めします。

情報漏えい対策ポリシーの整合性を維持するには、現在の情報漏えい対策テンプレートのコピーをそれぞれの Exchange サーバに保存します。

情報漏えい対策 – 隠しキー

情報漏えい対策は次の隠しキーを使用して設定できます。

表 B-6. 情報漏えい対策の設定で使用する隠しキー

名前	種類	説明
EmMaxEntitySize	REG_DWORD	情報漏えい対策の検索対象外とする添付ファイルサイズをカスタマイズする場合に使用します。この隠しキーは、検索するファイルの最大サイズ (MB) を示します。
DmcDisableMask	文字列	指定した種類のファイルを検索対象外とする場合に使用します。初期設定では、すべての種類のファイルが情報漏えい対策の検索対象になります。この隠しキーを使用すると、検索対象から除外するファイルの種類を選択できます。この設定はすべての種類の検索に適用されます。

注意

隠しキーの設定は、InterScan のメインサービスの再起動後に反映されます。63 ページの「サービスの開始と停止」を参照してください。

Web レピュテーションの最適化

Web レピュテーションの検索のパフォーマンスは、いくつかの方法で設定を行うことで最適化することができます。ネットワークや検索のパフォーマンスを最適化するには、次の Web レピュテーション設定を検討してください。

- [内部ドメインの URL を放置する] オプションを有効にします。これにより、内部ドメインの URL を含むメッセージが除外されるため、[URL 分析] を有効にした場合のネットワーク帯域幅の消費が減少し、仮想アナライザの負荷が軽減されます。
- 組織の内部 URL を [承認する URL リスト] に追加します。これにより、内部 URL を含むメッセージが除外されるようになるため、ネットワーク帯域幅の消費が減少し、パフォーマンスが向上します。
- Trend Micro Smart Protection Server を使用してネットワーク帯域幅の消費を削減します。Web レピュテーションサービスは、外部の Trend

Micro Smart Protection Network またはローカルの Trend Micro Smart Protection Server のいずれかに URL クエリを送信します。Trend Micro Smart Protection Network にクエリを送信する場合、インターネット接続が低速だと、ネットワークパフォーマンスに悪影響をもたらすことがあります。管理コンソールを使用して Trend Micro Smart Protection Server を設定し、[Smart Protection] > [検索サービス設定] をクリックして Web レピュテーションのソースを変更します。

- Trend Micro Smart Protection Server のパフォーマンスを最適化するには、InterScan 専用の Trend Micro Smart Protection Server を使用することを検討してください。たとえば、InterScan と Apex One で同じ Trend Micro Smart Protection Server を使用している場合、サーバのパフォーマンスが低下することがあります。
- 添付ファイル内の URL を検索すると、システムのパフォーマンスに影響することがあります。コンテンツフィルタまたは情報漏えい対策ポリシーで既に添付ファイル検索を使用している場合は、添付ファイル内の URL 検索によるシステムへの影響はそれほど大きくありません。コンテンツフィルタまたは情報漏えい対策ポリシーで添付ファイル検索を使用していない場合は、添付ファイル内の URL 検索を使用することでパフォーマンスに大きく影響する可能性があります。

Web レピュテーションのパフォーマンス問題のトラブルシューティング

Web レピュテーションサービスのパフォーマンスに問題がある場合は、次の方法で Web レピュテーションの設定をテストしてください。

- ネットワーク接続が安定していることを確認します。

  InterScan では、Web レピュテーションサービスを提供する Trend Micro Smart Protection Network および Trend Micro Smart Protection Server への接続のステータスを監視しています。Web レピュテーションのソースに接続できない場合に通知を受け取るには、[Smart Protection Server: Web レピュテーションサービスが使用不可になった/復旧した場合] を有効にします。この通知を頻繁に受信する場合は、ネットワーク接続が不安定になっている可能性があります。

- Web レピュテーションクエリの速度をテストします。

Web レピュテーションのパフォーマンスログで Web レピュテーションクエリの速度を確認することができます。レジストリキー DebugModule に行 wtp_performance:1 を追加します。レジストリキーのパスは次のとおりです。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥ScanMail for Exchange¥CurrentVersion
```

InterScan のデバッグフォルダ (<InterScan のインストールパス>¥Debug) に、ファイル wtp_performance.log が生成されます。初期設定のデバッグフォルダのパスは次のとおりです。

```
C:¥Program Files¥Trend Micro¥Isme¥Debug
```

このログに、クエリにかかった時間 (ミリ秒) が URL ごとに記録されます。

注意

このチェックは InterScan のデバッグログを有効にしなくても実施されます。

Search & Destroy のベストプラクティス

Search & Destroy 機能を設定するときは、次のベストプラクティスに留意してください。

- 356 ページの「Search & Destroy の事前要件」
- 359 ページの「複数データセンター環境での Search & Destroy の設定」
- 357 ページの「バージョンが混在した Exchange 環境での Search & Destroy の使用」
- 359 ページの「検索条件の最適化」
- 360 ページの「メールボックス検索の最適化」
- 360 ページの「メールボックス検索の削除」
- 361 ページの「Exchange 管理シェルのコマンド」

Search & Destroy の事前要件

Exchange 環境で Search & Destroy を使用する場合は、あらかじめ次の事前要件を確認してください。

表 B-7. 機能

機能	説明
サービスアカウント	このアカウントは、Exchange 環境内でバックエンドの検索を実行します。組織全体で必要なサービスアカウントは 1 つだけです。サービスアカウントは次のように設定します。 • このアカウントは Exchange の検出管理グループのメンバーに設定する必要があります。 • このアカウントは期限切れにならないようにする必要があります。 • 検索結果を .pst ファイルにエクスポートする場合、このアカウントは Exchange の役割である Mailbox Import Export のメンバーに設定する必要があります。 • このアカウント用のメールボックスを作成します (Exchange Server 2013/2016 のみ)。 Exchange 管理シェルのサービスアカウント関連のコマンドの詳細については、361 ページの「サービスアカウントの設定」を参照してください。

機能	説明
検出メールボックス	このメールボックスには、検索結果メッセージが保存されます。InterScan によって、エンドユーザのメールボックスから検出メールボックスにメッセージがコピーされます。検出メールボックスは次のように設定します。 • 検出管理グループには各検出メールボックスに対するフルアクセス権限を割り当てる必要があります。 • 組織内の各データセンターに 1 つ以上の検出メールボックスを割り当てます。 **注意** DAG (Database Availability Group) ソリューションには検出メールボックスを配置しないことをお勧めします。検出メールボックスは、DAG ソリューションで使用すると、より多くのデータベース領域を消費します。 Exchange 管理シェルの検出メールボックス関連のコマンドの詳細については、362 ページの「検出メールボックスの設定」を参照してください。

バージョンが混在した Exchange 環境での Search & Destroy の使用

Search & Destroy 機能で検索して処理できるのは、InterScan のインストールに関連付けられた Exchange 環境と同じバージョンの Exchange 環境にあるメールボックスだけです。複数の InterScan サーバで複数のバージョンの Exchange を管理している場合は、Search & Destroy のタスクをそれぞれの InterScan サーバで別々に実行する必要があります。

例:

Exchange 2010 環境にインストールされた InterScan サーバでは、Exchange 2013 データベースに対して Search & Destroy のタスクを実行することはできません。Exchange 2010 と Exchange 2013 の両方のデータベースを検索するには、Exchange 2010 にインストールされた InterScan サーバで Search & Destroy の検索タスクを実行してから、Exchange 2013 にインストールされた InterScan サーバで Search & Destroy の検索タスクを別途実行する必要があります。

注意

InterScan サーバが関連付けられた Exchange Server と同じバージョンであれば、複数の Exchange サーバに対して Search & Destroy のタスクを実行することができます。

バージョンが混在した Exchange 環境向けの Exchange Server 2013/2016/2019 の準備

Exchange Server 2013/2016 では、バージョンが混在した Exchange 環境で検索を実行する場合、開始前に Exchange サーバに SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9}メールボックスを用意しておく必要があります。Exchange Server 2013/2016 にこのメールボックスがない場合は、Exchange 管理シェルのコマンドを使用して設定します。

手順

1. 次のコマンドを実行します。`Get-Mailbox -Arbitration`

   現在のシステムメールボックスの情報を取得します。

2. 次のコマンドを実行します。`Get-Mailbox -Arbitration "SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9}" | New-MoveRequest -Targetdatabase "Exchange2013/2016 DB Name"`

   Exchange Server 2013/2016 のメールボックスデータベースに SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9}メールボックスを移動します。

3. 次のコマンドを実行します。`Get-MoveRequest`

   移動処理のステータスを確認します。

   注意

   移動処理が完了するまでに数分かかることがあります。

複数データセンター環境での Search & Destroy の設定

手順

1. すべてのデータセンターのすべての Search & Destroy タスクを実行するための、専用の Exchange メールボックスサーバを選択します。
2. InterScan コンソールを使用して Search & Destroy 管理者を設定します。

   詳細については、206 ページの「Search & Destroy アクセスアカウントの設定」を参照してください。
3. すべての Search & Destroy タスクを管理する 1 つのサービスアカウントを準備します。
4. 組織内のデータセンターごとに個別の検出メールボックスを準備します。
5. Search & Destroy をアクティベートし、最も使用頻度の高い検出メールボックスを初期設定のメールボックスとして割り当てます。

   詳細については、208 ページの「Search & Destroy のアクティベーション」を参照してください。
6. データセンターごとに、検索タスクを作成して単一のデータセンターに配置されているメールボックスのみを検索します。

   詳細については、213 ページの「メールボックス検索のオプション」を参照してください。
7. 検索タスクごとに、対象メールボックスと同じレベルに配置されている検出メールボックスを選択します。

検索条件の最適化

メールボックス検索を実行する場合は、次の検索条件を定義して検索範囲を絞り込んでください。

- メッセージの件名、本文、または添付ファイルの検索:
  - 管理者は KQL を使用して、特定のメッセージ部分にしか存在しないテキストを検索できます。次に、シンプルな KQL 検索文字列の例をいくつか示します。

- 例 1: メッセージの件名に「test」という単語が含まれるメッセージを検索するには、「`Subject:test`」と入力します。
- 例 2:「test.xslx」という添付ファイルが含まれるメッセージを検索するには、「`attachment:'test.xslx'`」と入力します。

KQL の詳細については、http://msdn.microsoft.com/ja-jp/library/ee558911.aspx を参照してください。

- 特定のメールボックスサーバ内のユーザの検索:

  InterScan には、特定のメールボックスサーバを直接検索する方法はありません。ただし、特定のメールボックスサーバ上の全ユーザが含まれる配布グループを作成し、その配布グループを検索することは可能です。

メールボックス検索の最適化

メールボックス検索では、サービスアカウントによってメッセージがエンドユーザのメールボックスから Exchange 検出メールボックスにコピーされ、続いて検索結果が解析されて InterScan データベースに送られます。これは、時間がかかり、リソースを多く消費するタスクです。実際の検索を実行する前に、検索結果の見積もりを行うことをお勧めします。

検索結果の見積もりのためにサービスアカウントがメッセージをコピーする必要はなく、Exchange サーバに与える影響もそれほど大きくありません。見積もりを行うと、管理者は実際の検索を実行する前に検索条件を最適化できます。

メールボックス検索が Exchange サーバのパフォーマンスに影響すると思われる場合は、[後で検索] 機能を使用してピーク時間帯以外に検索を実行するようにスケジュールを設定することをお勧めします。

メールボックス検索の削除

- 検索条件を削除することなくエンドユーザのメールボックスから検索結果のメッセージを削除するには

  検索結果画面に移動し、エンドユーザのメールボックスから削除するメッセージを手動で選択します。この操作により、Exchange サーバ検出メールボックスと InterScan データベースに保存されている、選択された検索結果も削除されます。

注意

管理者は、Exchange 管理シェルのコマンドを使用して Exchange 検索タスクを手動で削除できます。

- [タスクのみを削除] 機能を使用する場合
  - 検索条件、タスク名、および検索結果のみが InterScan データベースから削除されます。
  - Exchange 検索タスク、および検出メールボックスに保存されているすべての検索結果はそのまま残ります。
  - エンドユーザのメールボックス内のメッセージは削除されません。

注意

アーカイブのために検索結果を残す場合は、[タスクのみを削除] を使用してください。

Exchange 管理シェルのコマンド

管理者は、Exchange 管理シェルのコマンドを使用して、Exchange サーバに対するさまざまなタスクを実行できます。以下の必要なタスクと便利なタスクについて確認することをお勧めします。

- 361 ページの「サービスアカウントの設定」
- 362 ページの「検出メールボックスの設定」
- 362 ページの「バックエンドの検索タスク」

サービスアカウントの設定

Exchange 環境でバックエンドの検索を実行するには、Exchange サービスアカウントが必要です。管理者は、Exchange 管理シェルの次のコマンドを使用してサービスアカウントを設定できます。

表 B-8. サービスアカウントのコマンド

コマンド	説明
`Add-RoleGroupMember -Identity “Discovery Management” -Member “SERVICE_ACCOUNT_NAME”`	Exchange の Discovery Management グループに「SERVICE_ACCOUNT_NAME」アカウントを追加します。
`New-ManagementRoleAssignment -Role "mailbox import export" -User “SERVICE_ACCOUNT_NAME”`	Exchange の Mailbox Import Export の役割に「SERVICE_ACCOUNT_NAME」アカウントを追加します。

検出メールボックスの設定

メールボックス検索の結果のメッセージを格納するには、Exchange 検出メールボックスが必要です。管理者は、Exchange 管理シェルの次のコマンドを使用して検出メールボックスを設定できます。

表 B-9. 検出メールボックスのコマンド

コマンド	説明
`Get-Mailbox -Filter {RecipientTypeDetails -eq "DiscoveryMailbox"}`	Exchange サーバにあるすべての検出メールボックスが返されます。
`New-Mailbox “NEW_DISCOVERY_MAILBOX_NAME” -Discovery -database "MAILBOX_DATABASE_NAME“`	「MAILBOX_DATABASE_NAME」という名前のデータベースに「NEW_DISCOVERY_MAILBOX_NAME」という名前の新しい検出メールボックスを作成します。
`Add-MailboxPermission -Identity “DISCOVERY_MAILBOX_NAME” -user "Discovery Management" -AccessRights FullAccess`	「DISCOVERY_MAILBOX_NAME」に Exchange の Discovery Management グループのフルアクセス権限を割り当てます。

バックエンドの検索タスク

管理者がメールボックス検索を作成すると、バックエンドの検索を実行する Exchange 検索タスクが InterScan によって作成されます。この Exchange 検索タスクは、次の形式で命名されます。

[task_name][server_name][time_stamp]

たとえば、2012 年 9 月 12 日、午前 4 時 30 分に「serverA」で実行されるメールボックス検索「task1」の場合、Exchange 検索タスク名は次のようになります。

task1serverA20120912043000

管理者は、次のシェルコマンドを使用してバックエンドの検索タスクに対する処理を実行できます。

表 B-10. バックエンドの検索のコマンド

EXCHANGE のバージョン	コマンド	説明
Exchange Server 2013/2016/2019	`get-mailboxsearch |fl name`	完全な検索タスク名が返されます。
	`get-mailboxsearch -identity [task name] |fl`	タスクステータスが返されます。
Exchange Server 2013/2016/2019	`remove-mailboxSearch-identity [task_name]`	Exchange サーバからメールボックス検索を削除し、関連するすべての検索結果を検出メールボックスから削除します

仮想アナライザ - 統合の事前要件

仮想アナライザの統合を有効にする前に、Exchange の再生フォルダを有効にする必要があります。

警告!

仮想アナライザの統合を有効にした後に Exchange の再生フォルダを無効にすると、予期しない問題が生じる可能性があります。Exchange の再生フォルダを無効にする場合は、事前に仮想アナライザの統合を無効にすることをお勧めします。

Exchange 管理シェルを使用して Exchange の再生フォルダを有効にするには、次のコマンドレットを使用します。

表 B-11. Exchange 管理シェルのコマンドレット

コマンドレット	説明
`Get-TransportService | fl replay*`	このコマンドレットは、現在の再生フォルダ属性を返します。 ReplayDirectoryPath 属性が NULL の場合は、Exchange 管理者によって再生フォルダが無効にされています。Exchange 管理者は、`Set-TransportService` コマンドを使用して再生フォルダを有効にする必要があります。
`Set-TransportServer -Identity {server name} -ReplayDirectoryPath "E:\Program Files\Microsoft\Exchange Server\TransportRoles\Replay"`	このコマンドレットは、指定されたディレクトリ内の再生フォルダを有効にします。
`Set- TransportService - Identitiy {Server name} - PickupDirectoryMaxMessages PerMinute 1000`	1 分あたり 3,600 メッセージを処理するなど、Exchange サーバのメッセージ処理量が多く、この状況が数時間続く場合、管理者は URL サンドボックスを有効にする前に、ピックアップディレクトリと再生ディレクトリのメッセージ処理の最大速度を上げる必要があります。

内部ドメイン

- 内部ドメインの設定は、InterScan のインストール時に、Exchange サーバの承認済みドメインと同期されます。この情報はインストールの完了後は更新されません。Exchange サーバで承認済みドメインの設定が更新されたときは、対応する設定を同期することをお勧めします。
- InterScan では、アスタリスク (*) のワイルドカードを使用して内部ドメインを指定できます。あるドメインとその下位ドメインを対象外とする場合、上位ドメインにプレフィックスとしてワイルドカードを使用します。たとえば、`example.com`、`child1.example.com`、および `child2.example.com` を対象外とする場合は、次のように入力します。

  ```
  *.example.com
  ```

一方、あるドメインだけを対象外とし、下位ドメインは検索対象とする場合は、次のように入力します。

```
example.com
```

推奨設定

InterScan は自由に設定できますが、トレンドマイクロでは、次の設定を推奨します。

- コンテンツ検索 — [メッセージをユーザのスパムメールフォルダに隔離] に設定します。
- コンテンツフィルタ — [メッセージ全体の隔離] に設定します。
  - いずれかに一致/すべてのルールに適用
  - すべての条件に一致
  - いずれかの条件に一致

  特定のメールアカウントの除外設定を作成する場合は、[放置] に設定します。
- 添付ファイルブロック — 不審添付ファイルは、[放置] に設定します。
- セキュリティリスク検索 — 駆除
- 情報漏えい対策 — [メッセージ全体の隔離] に設定します。
- その他 —
  - パスワードで保護されているか、暗号化されたメッセージまたはファイルは、[放置] に設定します。
  - 検索制限を超える圧縮ファイルは、[放置] に設定します。

索引

アルファベット

あ

か

さ

た

な

は

ま

や

ら

わ