



InterScan Messaging Security Suite™ 9.1

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サイトからご確認ください。
<https://esupport.trendmicro.com/ja-jp/support-lifecycle/default.aspx>

著作権について

本ドキュメントに関する著作権は、トレンドマイクロ株式会社へ独占的に帰属します。トレンドマイクロ株式会社が事前に承諾している場合を除き、形態および手段を問わず、本ドキュメントまたはその一部を複製することは禁じられています。本ドキュメントの作成にあたっては細心の注意を払っていますが、本ドキュメントの記述に誤りや欠落があってもトレンドマイクロ株式会社はいかなる責任も負わないものとします。本ドキュメントおよびその記述内容は予告なしに変更される場合があります。

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 InterScan WebManager SCC、Trend Micro NAS Security、Trend Micro Data Loss Prevention、Securing Your Journey to the Cloud、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アップサービス、Deep Discovery、TCSE、おまかせインストーラー・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アップサービス、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、およびTrend Micro Policy-based Security Orchestrationは、トレンドマイクロ株式会社の登録商標です。

本ドキュメントに記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。

Copyright © 2019 Trend Micro Incorporated. All rights reserved.

P/N: MSEM77873_170627_JP_R1 (2019/06)

目次

本書について

本書について	13
新機能	14
対象読者	17
InterScan Messaging Security Suite ドキュメント	17
ドキュメントの表記規則	18

パート I : はじめに

第 1 章 : InterScan Messaging Security Suite の概要

InterScan MSS について	22
InterScan MSS の主な特長と利点	22
クラウドプレフィルタについて	32
スパイウェアと他の種類のグレーウェアについて	33
Web レピュテーションサービスについて	35
メールレピュテーションについて	35
Trend Micro Control Manager について	38
トレンドマイクロの Smart Protection について	42
グレーメールの検索について	45
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について	46

第 2 章 : はじめに

InterScan MSS の管理コンソールを開く	48
管理コンソールのパスワードを変更する	49
スマートスキャンを使用する	50

プロキシを設定する	50
InterScan MSS サービス	52
エンドユーザメール隔離の管理コンソールを開く	53

第 3 章：設定ウィザードの使用

設定ウィザードにより IMSS を設定する	56
通知を設定する	56
アップデート元を設定する	58
LDAP を設定する	60
内部アドレスを設定する	64
Control Manager サーバを設定する	65
製品をアクティベートする	67
設定を確認する	68

第 4 章：コンポーネントのアップデート

エンジンとパターンファイルをアップデートする	70
アップデート元を指定する	71
手動アップデートを実行する	72
コンポーネントのアップデートをロールバックする	74
予約コンポーネントをアップデートする	74

第 5 章：クラウドプレフィルタの導入

クラウドプレフィルタについて	80
クラウドプレフィルタアカウントを作成する	83

第 6 章：ATSE および仮想アナライザの導入

検索テクノロジー	90
高度な脅威検索エンジンについて	90
仮想アナライザについて	92

第 7 章 : Trend Micro Email Encryption の導入

Trend Micro Email Encryption について	100
Trend Micro Email Encryption を使用する	101
Trend Micro Email Encryption を登録する	101
ドメインを管理する	102
ドメインを登録する	103

パート II : InterScan MSS の設定

第 8 章 : クラウドプレフィルタの設定

クラウドプレフィルタポリシーについて	110
クラウドプレフィルタポリシーを作成する	112
クラウドプレフィルタの動作を確認する	122
DNS の MX レコードを設定する	122
クラウドプレフィルタを使用する際に推奨される InterScan MSS の設定	123
クラウドプレフィルタを無効にする	125

第 9 章 : 送信者フィルタの設定

IP フィルタサービス	128
メールレピュテーション管理コンソールを使用する	128
送信者フィルタを設定する	130
不審 IP アドレスおよびドメインを表示する	143

第 10 章 : SMTP を設定する

MTA (Message Transfer Agents)	146
SMTP 接続を有効にする	146
SMTP ルーティングを設定する	146

メッセージ配信について	155

第 11 章：既知のホストの設定

既知のホストについて	160
既知のホストを追加する	161
既知のホストをインポートする	162
既知のホストをエクスポートする	163

第 12 章：POP3 の設定をする

POP3 メッセージを検索する	166
POP3 の検索を有効にする	167
POP3 の設定をする	168
POP3 検索サービスを設定する	169

パート III：InterScan MSS ポリシー

第 13 章：ポリシーの管理

ポリシーについて	174
Policy Manager の仕組み	174
ポリシーリストに表示されるポリシーをフィルタする	176

第 14 章：共通のポリシーオブジェクトの設定

ポリシーオブジェクトの説明	180
アドレスグループ	181
キーワードリストを使用する	192
DLP コンプライアンステンプレート	206
ポリシー通知	226
スタンプ	231
DKIM 承認済みリスト	234

Web レピュテーション承認済みリスト	236
第 15 章 : 内部アドレスの設定	
内部アドレスを設定する	240
ユーザまたはグループを検索する	243
LDAP ユーザまたはグループを検索する	244
第 16 章 : Trend Micro Smart Protection の使用	
トレンドマイクロの Smart Protection について	248
Smart Protection ソース	251
検索方法を選択する	254
Web レピュテーションサービスを使用する	256
第 17 章 : ポリシーの設定	
ポリシーを追加する	260
ルートを指定する	260
検索条件を指定する	267
処理を指定する	297
ポリシーを完成させる	304
第 18 章 : 暗号化の設定	
暗号化を設定する	310
メッセージトラフィックを暗号化する	311
暗号化ポリシーを設定する	311
第 19 章 : 検索除外の設定	
検索除外を設定する	314
セキュリティ設定違反の除外を設定する	315
セキュリティ設定違反の検索処理を設定する	316
正しくない形式のメッセージの検索処理を設定する	317

暗号化されたメッセージの除外を設定する	319
暗号化されたメッセージの検索処理を設定する	320
仮想アナライザの検索の除外の検索処理を設定する	321

第 20 章：既存のポリシーの設定

既存ポリシーを変更する	324
ポリシーの例 1	327
ポリシーの例 2	332
アスタリスクワイルドカードを使用する	337

パート IV：ネットワークの監視

第 21 章：ネットワークの監視

ネットワークを監視する	342
システムステータスを表示する	342

第 22 章：ダッシュボードとウィジェット

ダッシュボードを使用する	346
タブについて	346
ウィジェットについて	351

第 23 章：レポート

レポートを生成する	356
1 回限りのレポートを管理する	359
予約レポート	362

第 24 章：ログ

ログについて	370
ログを設定する	370

ログのクエリを実行する	372

第 25 章 : メール領域とキュー

メール領域とキューについて	390
隔離とアーカイブを設定する	390
隔離領域を管理する	392
アーカイブ領域を管理する	395
メッセージのクエリを実行する	397
隔離されたメッセージを表示する	404
アーカイブされたメッセージを表示する	406
保留されたメッセージを表示する	407
仮想アナライザのキューのメッセージを表示する	408

第 26 章 : 通知

イベント通知	412
通知を設定する	412
イベント条件および通知メッセージを設定する	415
エンドユーザメール隔離通知	418
ログオン通知の設定	420
通知を編集する	421

パート V : InterScan MSS の管理

第 27 章 : 設定のバックアップ、復元、および複製

設定のインポートとエクスポート	426
InterScan MSS をバックアップする	428
InterScan MSS を復元する	430
設定を複製する	432
デバッグログをエクスポートする	434

第 28 章 : エンドユーザメール隔離

エンドユーザメール隔離について	438
EUQ 認証	438
エンドユーザメール隔離を設定する	439
配布リスト EUQ の管理	450
エンドユーザメール隔離を無効にする	452
EUQ データベースを管理する	453

第 29 章 : 管理タスク

管理者アカウントを管理する	458
接続を設定する	462
データベースのメンテナンススケジュールを設定する	475
製品ライセンスを管理する	476
製品のアクティベーションを実行する	480
Smart Protection Network を設定する	482

第 30 章 : システムとアプリケーションのアップデートと復旧

システムとアプリケーションをアップデートする	484

第 31 章 : トラブルシューティングと FAQ

トラブルシューティング	488
FAQ	505
クラウドプレフィルタのトラブルシューティング	524

付録**付録 A : テクニカルサポート**

トラブルシューティングのリソース	530
製品サポート情報	531

サポートサービスについて	531
セキュリティニュース	532
脅威解析・サポートセンター TrendLabs (トレンドラボ)	533

付録 B : InterScan MSS スクリプト

InterScan MSS スクリプトを使用する	536

付録 C : 初期設定のディレクトリ場所

初期設定のメールキュー	542
コンテンツフィルタ、ウイルス、およびプログラムのログ	543
一時フォルダ	543
通知メールキュー	544

索引

索引	545

はじめに

本書について

Trend Micro InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) の管理者ガイドをお読みいただきありがとうございます。本書では、InterScan MSS の特徴、システム要件、および InterScan MSS の設定手順について説明しています。

InterScan MSS のインストールおよびアップグレードについては、*InterScan MSS 9.1 インストールガイド*を参照してください。

この章の内容は次のとおりです。

- ・ 14 ページの「新機能」
- ・ 17 ページの「対象読者」
- ・ 17 ページの「InterScan Messaging Security Suite ドキュメント」
- ・ 18 ページの「ドキュメントの表記規則」

新機能

次の表に、InterScan MSS で利用可能な新機能の概要を示します。

表 1. InterScan MSS の新機能

新機能	説明
クラウドプレフィルタの統合	クラウドプレフィルタは、メールメッセージがネットワークに到達する前にすべてのメールメッセージをフィルタする、ホステッドメールセキュリティサービスです。メールメッセージを事前にフィルタすることで時間とコストを節約できます。
DLP コンプライアンステンプレート	DLP コンプライアンステンプレートでは、組織の機密データ (デジタル資産) を偶発的な開示や意図的な盗用から保護します。
仮想アナライザとの統合	仮想アナライザは、Deep Discovery Analyzer 内でサンプルを管理および分析するために使用される隔離された仮想環境です。InterScan MSS では、添付ファイルを含む不審メッセージを分析用に仮想アナライザに送信するルールを定義できます。 負荷分散とフェイルオーバー機能をさらに効率化するため、InterScan MSS では仮想アナライザに複数のサーバを追加できます。仮想アナライザサーバは InterScan MSS 管理コンソールで有効化、無効化、および削除できます。
エンドユーザメール隔離のシングルサインオン (SSO)	一度ドメインにログオンしたら、ドメイン名とパスワードを再入力せずにエンドユーザメール隔離 (EUQ) を実行できるようになります。
ダッシュボードとウィジェット	リアルタイムサマリの代わりにダッシュボードとウィジェットが使用されるようになります。これにより管理者は、InterScan MSS のデータをより柔軟に表示できます。[概要] 画面の名称は [システムステータス] に変更され、左側のメニューに表示されます。

新機能	説明
Web レピュテーションの強化	Web レピュテーションフィルタが強化され、トレンドマイクロで評価されていない URL を検出できるようになります。これにより、一時的な不正 Web サイトを利用した高度な脅威に対する保護を強化できます。
Smart Protection の強化	InterScan MSS では、Smart Protection ソースに Trend Micro Smart Protection Network と Smart Protection Server の両方を使用できます。Smart Protection Server を使用すると、Smart Protection サービスを企業ネットワークに対してローカライズし、送信トラフィックを削減して、効率を最適化できます。
ソーシャルエンジニアリング攻撃からの保護	ソーシャルエンジニアリング攻撃からの保護では、メールメッセージ内のソーシャルエンジニアリング攻撃に関連する疑わしい動作を検出します。本機能が有効な場合、スパムメール検索エンジンは、送信メール内のメールヘッダ、件名、本文、添付ファイル、SMTP プロトコル情報などに対して不審な動作を検索します。スパムメール検索エンジンは、ソーシャルエンジニアリング攻撃に関連する動作を検出するとメッセージの詳細を InterScan MSS に返し、InterScan MSS は、追加の処理を実行するか、ポリシーを適用するか、またはレポートを作成します。
既知のホストのサポート	既知のホストには、信頼されるメール転送エージェント (MTA) と、ネットワーク上で InterScan MSS の外側に配置されたクラウドプレフィルタが含まれます。InterScan MSS では、既知のホストを指定して、送信者フィルタやグレーメール検索から除外できます。
グレーメール	グレーメールとは、スパムメールではなく、ユーザ自身が過去に受信設定を行ったメールです。InterScan MSS では、管理者が識別できるように、一般のスパムメールとは区別してグレーメールを管理します。グレーメール除外リストに指定された IP アドレスは検索対象外となります。

新機能	説明
複数の LDAP サーバ	InterScan MSS は、複数の LDAP サーバの使用と、より多くの LDAP サーバの種類をサポートしています。
高度な不正プログラム対策保護	高度な脅威検索エンジン (以下、ATSE) では、パターンベースの検索と強力なヒューリスティック検索を組み合わせて使用することにより、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。
Time-of-Click プロテクション	メールメッセージ内の不正 URL に対して Time-of-Click プロテクションが提供されます。Time-of-Click プロテクションを有効にすると、InterScan MSS は、さらなる分析のためにメール内の URL を書き換えます。トレンドマイクロでは、これらの URL をクリック時に分析し、不正なものである場合はブロックします。
Connected Threat Defense(CTD)	Trend Micro Control Manager (以下、Control Manager) サーバの不審オブジェクトリストを利用するように InterScan MSS を設定します。Control Manager コンソールを使用すると、不審オブジェクトリストを基に検出されたオブジェクトに対する処理を指定して、トレンドマイクロ製品により保護されているエンドポイントで特定された脅威に対して環境固有のポリシーを提供できます。 Control Manager は、不審オブジェクトを利用して標的型攻撃や高度な脅威を調査します。これにより、システムに危険やデータ損失をもたらす可能性のあるファイルまたは URL が検出されます。
メールでのレポート配信	InterScan MSS では、新しく生成されたレポートや保存されたレポートをメールで送信できます。レポートの詳細情報が含まれます。
EUQ 配布リストの管理	Web ベースのエンドユーザメール隔離サービスを使用すると、エンドユーザは自分が所属する配布リストのスパムメールの隔離方法を管理できます。
LDAPS のサポート	LDAP over SSL (LDAPS) がサポートされるため、安全で暗号化されたチャネルを使用して LDAP サーバと通信できます。

新機能	説明
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	C&C コンタクトアラートサービスでは、強化された検出およびアラート機能により、持続的標的型攻撃 (APT: Advanced Persistent Threats) や標的型攻撃によるダメージを軽減します。
エンドユーザメール隔離通知のオンライン処理リンク	InterScan MSS を使用すると、エンドユーザメール隔離通知内のリンクを介して隔離されたメッセージに処理を適用できます。

対象読者

InterScan MSS のドキュメントは、中規模から大規模企業の IT 管理者およびメール管理者を対象に書かれています。本書は、読者の方に、次の知識を含め、メールメッセージングネットワークの専門的な知識があることを前提としています。

- ・ SMTP および POP3 プロトコル
- ・ Postfix や Microsoft Exchange などの Message Transfer Agent (MTA)
- ・ LDAP
- ・ データベース管理
- ・ Transport Layer Security

InterScan Messaging Security Suite 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。

- ・ 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
- ・ 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

- ・ 管理者ガイドー 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

**注意**

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。

<http://www.trendmicro.co.jp/download/>

ドキュメントの表記規則

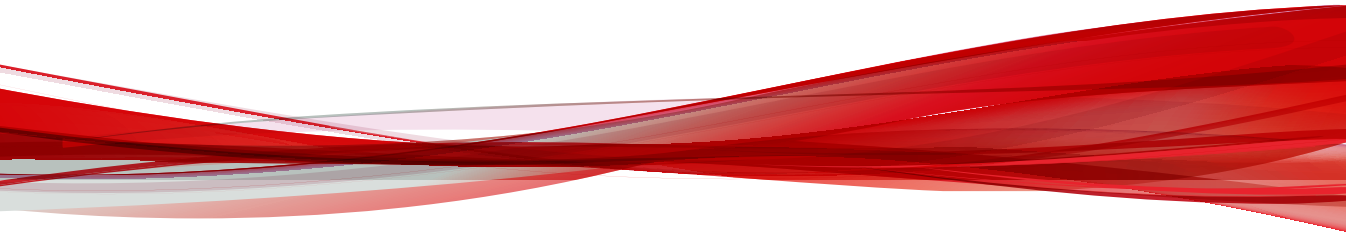
このドキュメントでは、次の表記規則を使用しています。

表 2. 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	必須または初期設定および製品の制限事項に関する情報
 警告!	重要な処理と設定オプション

パートⅠ

はじめに



第 1 章

InterScan Messaging Security Suite の概要

この章では、Trend Micro InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) の特徴、機能、およびテクノロジーについて説明します。また、スパムメール対策機能を強化する他のトレンドマイクロ製品の基本情報も示します。

この章の内容は次のとおりです。

- ・ 22 ページの「InterScan MSS について」
- ・ 22 ページの「InterScan MSS の主な特長と利点」
- ・ 32 ページの「クラウドプレフィルタについて」
- ・ 33 ページの「スパイウェアと他の種類のグレーウェアについて」
- ・ 35 ページの「Web レピュテーションサービスについて」
- ・ 35 ページの「メールレピュテーションについて」
- ・ 38 ページの「Trend Micro Control Manager について」
- ・ 42 ページの「トレンドマイクロの Smart Protection について」
- ・ 45 ページの「グレーメールの検索について」
- ・ 46 ページの「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について」

InterScan MSS について

InterScan MSS は、ウイルス対策、スパムメール対策、フィッシング対策、およびコンテンツフィルタ技術を統合してメールを保護します。この柔軟性の高いソフトウェアソリューションの特長は、既知および潜在的なウイルスをブロックする、実績の高いウイルス対策およびゼロデイ攻撃からの保護です。

多層構造のスパムメール対策では、最初のレベルであるメールレピュテーションテクノロジーの保護と、IP プロファイラや各種要素からなる強力なエンジンを混在させる手法を使用したカスタマイズ可能なトラフィック管理を組み合わせています。多言語のスパムメール対策は、グローバル企業へのさらなるサポートを提供します。高度なコンテンツフィルタにより、規制コンプライアンスおよびコーポレートガバナンスを達成でき、機密情報を保護できます。InterScan MSS は、集中管理されたスケーラビリティの高い単一のプラットフォームを保護し、ゲートウェイでの総合的なメールセキュリティを提供します。

InterScan MSS の主な特長と利点

次の表に、ネットワークにおける InterScan MSS の特長と利点について説明します。

表 1-1. 主な特長と利点

特長	説明	利点
データおよびシステムの保護		

特長	説明	利点
ウイルス対策による保護	InterScan MSS では、トレンドマイクロの検索エンジンおよびパターンマッチングというテクノロジーを使用して、ウイルスの検出を実行します。検索エンジンは、ゲートウェイを通過するファイル内のコードと、パターンファイルに記述された既知のウイルスのバイナリパターンを比較します。パターンの一致を検出すると、検索エンジンはポリシーールルの設定に応じて、処理を実行します。	機能強化されたウイルス/コンテンツ検索サービスにより、メッセージングシステムは最適な状態で稼働し続けることができます。
クラウドベースのメッセージのプレフィルタ	クラウドプレフィルタは、InterScan MSS と統合され、メールトラフィックがネットワークに到達する前にすべてのトラフィックを検索します。	クラウドプレフィルタは、スパムメールや不正なメッセージがネットワークに到達しないように、これらの大量のメッセージをブロックできます (全メッセージトラフィックの最大 90%)。
高度な不正プログラム対策保護	高度な脅威検索エンジン (以下、ATSE) では、パターンベースの検索と強力なヒューリスティック検索を組み合わせて使用することにより、標的型攻撃で使用す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。	ATSE では、既知および未知の高度な脅威を識別し、パターンにまだ追加されていない新型の脅威からシステムを保護します。
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	C&C コンタクトアラートサービスにより、InterScan MSS は、メッセージヘッダの送信者、受信者および返信先アドレスと、メッセージ本文に含まれる URL を調べて、いずれかが既知の C&C オブジェクトに一致しているかどうかを確認できます。	C&C コンタクトアラートサービスでは、強化された検出およびアラート機能により、持続的標的型攻撃 (APT: Advanced Persistent Threats) や標的型攻撃によるダメージを軽減します。

特長	説明	利点
グレーメール	グレーメールとは、スパムメールではなく、ユーザ自身が過去に受信設定を行ったメールです。InterScan MSS では、マーケティングメッセージ、ニュースレター、およびソーシャルネットワークの通知をグレーメールとして検出します。	InterScan MSS では、管理者が識別できるように、一般のスパムメールとは区別してグレーメールを管理します。グレーメール除外リストに指定された IP アドレスは検索対象外となります。
規制コンプライアンス	管理者は、新しい初期設定のポリシー検索条件である [コンプライアンステンプレート] を使用して、行政機関の規制要件に適合させることができます。	管理者は、規制コンプライアンスに対応するコンプライアンステンプレートを使用できます。利用可能なテンプレートのリストについては、 http://esupport.trendmicro.com/solution/ja-JP/1107704.aspx を参照してください。
スマートスキャン	スマートスキャンでは、以前 InterScan MSS サーバに格納されていた脅威のシグネチャをクラウドに格納することで負荷を軽減し、より効率的に検索を実行できるようになります。	スマートスキャンは、Trend Micro Smart Protection Network を利用して次のことを実現します。 ・ クラウド内での高速かつリアルタイムなセキュリティステータス検索機能の提供 ・ 新たな脅威に対する保護に必要な時間の短縮 ・ サーバのメモリ消費量の低減

特長	説明	利点
IntelliTrap	ウイルス作成者は、通常、さまざまなファイル圧縮スキームを使用して、ウイルスフィルタを回避しようとしています。IntelliTrap は、これらの圧縮ファイルのヒューリスティック評価を行います。 IntelliTrap が脅威のないファイルをセキュリティリスクとして識別する可能性があるため、IntelliTrap が有効な場合は、このカテゴリに分類されるメッセージの添付ファイルを隔離することをお勧めします。また、ユーザが定期的に圧縮ファイルを交換する場合は、この機能を無効にしなければならないこともあります。 初期設定では、IntelliTrap は、ウイルス対策ポリシーに対する検索条件の 1 つとして有効になっており、セキュリティリスクとして分類される可能性のあるメッセージの添付ファイルを隔離するように設定されています。	IntelliTrap を使用すると、さまざまなファイル圧縮スキームを使用して圧縮されたウイルスがメールを介してネットワークに侵入するリスクを低減できます。
コンテンツ管理	InterScan MSS は、ネットワークを通じてやりとりされるメールメッセージと添付ファイルの内容が適切かどうかを分析します。	InterScan MSS では、業務に不要なやりとりや巨大な添付ファイルなど、不適切と思われる内容を効果的にブロックまたは保留できます。
リアルタイムの統計情報と監視	管理者は、管理コンソールでグループ内のすべての InterScan MSS デバイスの検索パフォーマンスと送信者フィルタパフォーマンスを監視できます。	InterScan MSS では、管理者がメール処理に関する問題の兆候をすぐに把握できるように、システムの概要を提供します。管理者は、詳細ログを参照して、問題が大きくなる前に対処できます。
その他のメール脅威からの保護		

特長	説明	利点
DoS 攻撃	巨大な添付ファイルでメールサーバを氾濫させたり、複数のウイルスや多重圧縮ファイルが含まれるメッセージを送信したりすることで、悪意のあるユーザがメール処理を妨害することがあります。	InterScan MSS を使用すると、どのような特性を持つメッセージを SMTP ゲートウェイで阻止するかを設定できるため、DoS 攻撃のリスクを低減できます。
不正なメールコンテンツ	実行可能プログラムや、マクロが埋め込まれたドキュメントなど、ウイルスはさまざまな種類の添付ファイルに潜んでいる可能性があります。HTML スクリプトファイル、HTML リンク、Java アプレット、ActiveX コントロールが含まれるメッセージも、有害な処理を実行する可能性があります。	InterScan MSS では、SMTP ゲートウェイの通過を許可するメッセージの種類を設定できます。
生産性の低下	ビジネスに関係のないメールトラフィックは、多くの企業で問題となっています。スパムメールメッセージはネットワーク帯域幅を消費し、従業員の生産性に影響します。従業員の中には、会社のメッセージングシステムから個人的なメッセージを送信したり、巨大なマルチメディアファイルを転送したり、業務時間内に個人的なビジネスを行ったりする人もいます。	ほとんどの企業では、メッセージングシステムの使用許容範囲を示すポリシーを制定しています。InterScan MSS は、企業の既存のポリシーを適用し、準拠させることのできるツールを提供します。

特長	説明	利点
法的責任とビジネスの信頼性	メールが不正に使用されると、企業の法的責任が問われる場合があります。従業員が性的または人種的嫌がらせを行っていたり、他の違法活動に携わっていたりするかもしれません。また、従業員の不正行為により、社内のメッセージングシステムから機密情報が漏えいする可能性もあります。企業のメールサーバから配信される不適切なメッセージは、そのメッセージの内容が企業の持論と異なるものであったとしても、企業の評判を損ねることになります。	InterScan MSS には、コンテンツを監視してブロックするツールが装備されているため、不適切な内容や機密事項が含まれるメッセージがゲートウェイを通過するリスクを低減できます。
マスメーリング型ウイルスの封じ込め	メール送信型ウイルスにより、社内のメッセージングシステムを介して偽装メッセージが自動的に広がる場合があります。そのため、クリーンアップに費用がかかったり、ユーザの間でパニックが発生したりする可能性があります。 InterScan MSS がマスメーリング型ウイルスを検出した場合、このウイルスに対する処理を、他の種類のウイルスに対する処理とは異なったものにすることが可能です。 たとえば、InterScan MSS が重要な情報を含む Microsoft Office ドキュメントにマクロウイルスを検出した場合、重要な情報を失わないようにするために、メッセージ全体を削除するのではなくメッセージを隔離するようにプログラムを設定できます。一方で、マスメーリング型ウイルスを検出した場合は、メッセージ全体を自動的に削除するようにプログラムを設定できます。	マスメーリング型ウイルスを含むメッセージを自動的に削除することにより維持する価値のないメッセージやファイルを検出、隔離、または処理するためにサーバのリソースを削減できます。 既知のマスメーリング型ウイルス ID は、TrendLabsSM (トレンドラボ) アップデートサーバを使用してアップデートされるマスメーリングパターンファイル内にあります。この種類のウイルスとそのメールの自動削除を有効にすることにより、リソースの節約、関連部署へのヘルプデスクコールの回避、および大規模感染後のクリーンアップ作業の排除を実現できます。
スパイウェアと他の種類のグレーウェアからの保護		

特長	説明	利点
スパイウェア と他の種類の グレーウェア	クライアントは、スパイウェア、アドウェア、ダイヤラーなど、ウイルス以外の潜在的な脅威のリスクにもさらされています。詳細については、 33 ページの「スパイウェアと他の種類のグレーウェアについて」 を参照してください。	InterScan MSS を使用すると、スパイウェアや他の種類のグレーウェアから環境を保護できるため、企業のセキュリティ、機密性、法的責任に関わるリスクを大幅に軽減できます。
統合されたスパムメール対策機能		
スパムメール 対策 (コンテ ンツ検索)	InterScan MSS では、オプションでスパムメール対策 (コンテンツ検索) 機能を追加できます。この機能を使用するには、別途アクティベーションコードが必要になります。詳細については、販売店にお問い合わせください。 なお、スパムメール対策機能は、アクティベーションコードを入力してアクティベーションを完了した時点で有効になります。	スパムメール対策 (コンテンツ検索) では、高度なコンテンツ処理と統計分析に基づく検索テクノロジーが使用されています。他の手法によるスパムメールの識別とは異なり、コンテンツ分析機能を採用したことで、パフォーマンスの高いリアルタイムの検出が可能です。スパムメールの送信者が手法を変更した場合でも、容易に対応できます。
IP プロファイ ラとメールレ ピュテーショ ンによるスパ ムメールフィ ルタ	IP プロファイラは、自己学習能力と十分なカスタマイズ性を備えており、スパムメールや他の潜在的な脅威を送信するコンピュータの IP アドレスを能動的にブロックします。メールレピュテーションは、トレンドマイクロのデータベースで管理される既知のスパムメール送信者の IP アドレスをブロックします。  注意 IP プロファイラとメールレピュテーションを設定する前にスパムメール対策 (コンテンツ検索) をアクティベートしてください。	IP プロファイラおよびメールレピュテーションからなる送信者フィルタ機能を統合することで、InterScan MSS は IP レベルでスパムメール送信者をブロックできます。

特長	説明	利点
ソーシャルエンジニアリング攻撃からの保護	ソーシャルエンジニアリング攻撃からの保護機能により、メールに含まれるソーシャルエンジニアリング攻撃を行う可能性のある不審な動作を検出できます。	本機能が有効な場合、スパムメール検索エンジンは、送信メール内のメールヘッダ、件名、本文、添付ファイル、SMTP プロトコル情報などに対して不審な動作を検索します。スパムメール検索エンジンは、ソーシャルエンジニアリング攻撃に関連する動作を検出するとメッセージを InterScan MSS に返し、InterScan MSS は、追加の処理を実行するか、ポリシーを適用するか、またはレポートを作成します。
管理と統合		
LDAP およびドメインベースのポリシー	ユーザグループの定義および管理者権限に Lotus Domino、Microsoft Active Directory などの LDAP ディレクトリサービスを使用している場合は、LDAP を設定できます。	LDAP を使用すると、さまざまなルールを定義して、企業のメールの使用ガイドラインを適用することができます。送信者および受信者のアドレスに基づいて、個人またはグループ用のルールを定義できます。
Web ベースの管理コンソール	管理コンソールを使用すると、InterScan MSS のポリシーおよび設定を簡単に変更できます。	管理コンソールは SSL に準拠しています。SSL に準拠することで、より安全に InterScan MSS にアクセスできます。

特長	説明	利点
エンドユーザメール隔離	InterScan MSS には、スパムメール管理を強化するための Web ベースのエンドユーザメール隔離が用意されています。Web ベースのエンドユーザメール隔離サービスを使用すると、エンドユーザは各自の個人アカウントおよび、自分が所属する配布リストのスパムメールの隔離方法を管理できます。InterScan MSS では、スパムメールと判定されたメッセージを隔離します。これらのメッセージは、エンドユーザメール隔離によってデータベース内でインデックスが付けられます。エンドユーザはメッセージを再確認したり、削除したり、または配信を許可したりできます。	Web ベースのエンドユーザメール隔離管理コンソールを使用すると、エンドユーザは InterScan MSS によって隔離されたメッセージを管理できます。 InterScan MSS ではさらに、エンドユーザメール隔離通知内のリンクを介して隔離されたメッセージに処理を適用でき、送信者を承認済み送信者リストに追加できます。
管理タスクの委任	InterScan MSS には、管理コンソールにさまざまなアクセス権限を作成する機能が用意されています。管理者のログオンアカウントごとに、アクセスを許可するコンソールのセクションを選択できます。	管理ロールをさまざまな従業員に委任することで、管理職務の共有を促進できます。
レポート機能の一元化	一元化されたレポート機能により、レポートを必要に応じてそのつど作成することも、予約して作成することもできます。	InterScan MSS の稼働状況を解析できます。 必要に応じてそのつど作成するレポートでは、レポートのコンテンツを必要に応じて指定できます。また、レポートを日次、週次、および月次ベースで自動生成するように設定することもできます。 InterScan MSS では、1 回限りのレポートと予約レポートをメールで送信できます。

特長	説明	利点
システムの可用性の監視	組み込みエージェントが InterScan MSS サーバの状態を監視し、メールフローを妨害する可能性のある違反状況が発生した場合に、メールまたは SNMP トラップを通じて通知を配信します。	システム障害の検出をメールや SNMP で通知することにより、迅速に修正措置を実行し、停止時間を最小限に抑えられるようにします。
POP3 検索	管理コンソールからの POP3 検索は、任意で有効または無効に設定できます。	SMTP トラフィックの他に、InterScan MSS では、ネットワーク内のメッセージングクライアントがメッセージを受信する際に、ゲートウェイで POP3 メッセージも検索できます。
クラスタ化アーキテクチャ	本バージョンの InterScan MSS は、分散配置が可能になるように設計されています。	各種の InterScan MSS コンポーネントをさまざまなコンピュータ上にインストールできます。一部のコンポーネントは複数のコンピュータに配置できます。たとえば、メッセージの量に応じて、追加サーバ上に追加の InterScan MSS 検索サービスコンポーネントをインストールして、すべてのサーバで同じポリシーサービスを使用することができます。
Control Manager との統合	Control Manager は、ウイルス対策プログラムとコンテンツセキュリティプログラムを、その物理的な位置やプラットフォームに関係なく中央から制御できるようにす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は、企業のウイルス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します。	Control Manager から配信される大規模感染予防サービスにより、大規模感染のリスクを低減できます。トレンドマイクロの製品で新種のメール送信型ウイルスが検出されると、トレンドラボから詳細なコンテンツフィルタを使用するポリシーが発行されるため、InterScan MSS でメッセージ内の不審な特性を識別して、メッセージをブロックすることができます。これらのルールは、最新のパターンファイルが提供されるまでの期間、感染の機会を最小限に抑えるのに役立ちます。

特長	説明	利点
仮想アナライザとの統合	InterScan MSS は仮想アナライザと統合されています。この隔離された仮想環境は、Deep Discovery Analyzer 内でサンプルを管理および分析するために使用されます。	InterScan MSS は、さらなる分析のために、添付ファイルを含む不審メッセージを仮想アナライザに送信します。仮想アナライザは、隔離された仮想環境でコンテンツシミュレーションと分析を実行し、さまざまなタイプの不正プログラムに関連付けられた共通する特性を識別します。特に、仮想アナライザはメッセージに添付されたファイルに不正なコードが含まれているかどうかを確認します。
Time-of-Click プロテクション	メールメッセージ内の不正 URL に対して Time-of-Click プロテクションが提供されます。	Time-of-Click プロテクションを有効にすると、InterScan MSS は、さらなる分析のためにメール内の URL を書き換えます。トレンドマイクロでは、これらの URL をクリック時に分析し、不正なものである場合はブロックします。

クラウドプレフィルタについて

クラウドプレフィルタは、InterScan MSS と統合され、クラウドでの予防的なプライバシーの保護と、ローカルの仮想アプライアンスの制御を可能にするクラウドセキュリティソリューションです。

クラウドプレフィルタは、ネットワークの外側でスパムメールや不正プログラムをブロックすることにより、最大 90% まで受信メールメッセージの量を削減します。クラウドプレフィルタは、ゲートウェイの位置で InterScan MSS と統合され、機密情報の柔軟な制御を可能にします。さらに、メールメッセージはローカルへ隔離されるため、メールメッセージの機密性が維持されます。メールメッセージがクラウド内に保存されることはありません。クラウドプレフィルタを使用することで、複雑さが緩和され、管理工数が削減されるため、大幅な経費の節約が可能です。

スパイウェアと他の種類のグレーウェアについて

企業ユーザは、ウイルスや不正プログラム以外の潜在的な脅威のリスク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、機密性、および法的責任において、企業に深刻なリスクをもたらします。

表 1-2. グレーウェアの種類

種類	説明
スパイウェア	アカウント ID やパスワードなどの情報を収集し、外部へ送信します。
アドウェア	広告を表示したり、Web ブラウザを通じてユーザの Web 閲覧の好みなどの情報を収集したりして、ユーザに対する広告の的を絞ります。
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、あらかじめ設定された電話番号に、コンピュータがモデムを通じて自動的にダイヤルするようにします。
ジョークプログラム	CD-ROM トレイを開閉したり、大量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するのを手助けします。
リモートアクセスツール	ハッカーがコンピュータへリモートアクセスして制御するためのツールです。
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するためのツールです。
その他	上記以外の種類

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/グレーウェアは、ユーザが正規のソフトウェアをダウンロードした場合でも、そのソフトウェアのインストールパッケージにグレーウェアアプリケーションが含まれていて、企業ネットワークに侵入することがあります。

大部分のソフトウェアプログラムには、ダウンロードする前にユーザが同意しなければならない使用許諾契約書 (EULA) が含まれています。多くの場合、使用許諾契約書にはアプリケーションと個人データ収集の使用目的に関する情報が記載されていますが、ユーザはこうした情報を見過ごしたり、法律用語を理解できないことがあります。

潜在的なリスクと脅威

ネットワーク上にスパイウェアやグレーウェアが存在すると、以下の事態が発生する可能性があります。

表 1-3. 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/グレーウェアアプリケーションがタスクを実行するには、CPU と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	アドウェアなど特定の種類のグレーウェアは、ポップアップウィンドウを作成したり、ブラウザフレーム内やウィンドウ内に情報を表示するように設計されているものがあります。こうしたアプリケーションのコードがシステム処理に与える影響の程度によって、グレーウェアはブラウザをクラッシュまたはフリーズさせたりする場合があります、システムの再起動が必要になることもあります。
ユーザ効率の低下	頻繁に表示されるポップアップ広告を閉じて、ジョークプログラムの弊害に対処しなければならないため、ユーザは本来の作業に集中できない場合があります。
ネットワーク帯域幅の効率低下	スパイウェア/グレーウェアアプリケーションは、収集したデータをネットワーク上で実行されている他のアプリケーションやネットワークの外部に定期的に送信することがあります。
個人情報や企業情報の漏えい	スパイウェア/グレーウェアが収集するデータは、ユーザがアクセスする Web サイトの一覧のような無害な情報ばかりではありません。スパイウェア/グレーウェアは、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接続している企業アカウントへのアクセス時に入力したユーザ名やパスワードも収集できます。

種類	説明
法的責任におけるリスクの増大	ネットワーク上のコンピュータリソースにハッカーが侵入した場合、ハッカーはクライアントコンピュータを利用して攻撃を開始したり、ネットワーク外のコンピュータにスパイウェア/グレーウェアをインストールしたりできます。このような活動に社内のネットワークリソースが関与すると、他の組織が被った損害に対して法律上の責任を問われる場合があります。

Web レピュテーションサービスについて

トレンドマイクロの Web レピュテーションテクノロジーでは、ドメインの分析から導き出した URL の信頼度の評価を基に、Web サイトに「評価 (レピュテーション)」を割り当てることで、感染の拡大を防ぐことができます。Web レピュテーションは、ゼロデイ攻撃などの Web ベースの脅威がネットワークに到達する前に、コンピュータをそれらの脅威から保護します。Web レピュテーションテクノロジーにより、大量の Web ドメインのライフサイクルを追跡し、実績のあるトレンドマイクロスパムメール対策の保護範囲をインターネットにまで広げます。

メールレピュテーションについて

メールレピュテーションは、受信メール接続の IP アドレスを Trend Micro Smart Protection Network に転送して、広範なレピュテーションデータベースと照合することで、スパムメールがコンピュータネットワークに侵入する前に検出してブロックすることを目的としたものです。

メールレピュテーションの種類

メールレピュテーションには、[35 ページの「標準」](#)と[36 ページの「詳細」](#)の 2 種類があります。

メールレピュテーション: 標準

このサービスでは、要求された IP アドレスを、Trend Micro Smart Protection Network によって管理されているトレンドマイクロの評価データベースと照

合して検証することにより、スパムメールをブロックします。この拡張を続けるデータベースには、現在 10 億を超える IP アドレスが、スパムメールの活動に基づく評価とともに格納されています。トレンドマイクロのスパムメール調査担当者は、これらの評価の見直しと更新を継続的にを行い、その精度を高めています。

「メールレピュテーション: 標準」サービスは、DNS 単一クエリベースのサービスです。未知のホストからメールメッセージを受信するたびに、指定されたメールサーバは、標準評価データベースサーバに対して DNS クエリを実行します。そのホストが標準評価データベースに存在すれば、メールレピュテーションはそのメールメッセージをスパムメールとしてレポートします



ヒント

標準レピュテーションデータベースのデータに合致した IP アドレスからのメールメッセージは、受信せず、ブロックするように InterScan MSS を設定することをお勧めします。

メールレピュテーション: 詳細

「メールレピュテーション: 詳細」サービスは、膨大な量のスパムメールの送信処理中に、スパムメールの送信元を特定してその送信を停止します。

これは、動的でリアルタイムな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、継続的にネットワークおよびトラフィックパターンを監視し、新しいスパムメールの送信元が現れると、ただちに (通常はスパムメールの最初の兆候の数分以内に) 動的評価データベースを更新します。スパムメールの活動の形跡がなくなると、動的評価データベースもそれに応じて更新されます。

「メールレピュテーション: 詳細」は「メールレピュテーション: 標準」と同様に DNS クエリベースのサービスですが、標準評価データベースと動的評価データベース (動的にリアルタイムに更新されるデータベース) という 2 種類のデータベースに対して 2 つのクエリを発行できます。この 2 つのデータベースには個別のエントリが格納されます (IP アドレスは重複しません)。そのため、トレンドマイクロは極めて動的なスパムメールの送信元にすばやく対応できる、非常に効果的で効率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でこれまで全受信接続 (すべて不正接続) の 80% 以上をブロックしています。この結果は、

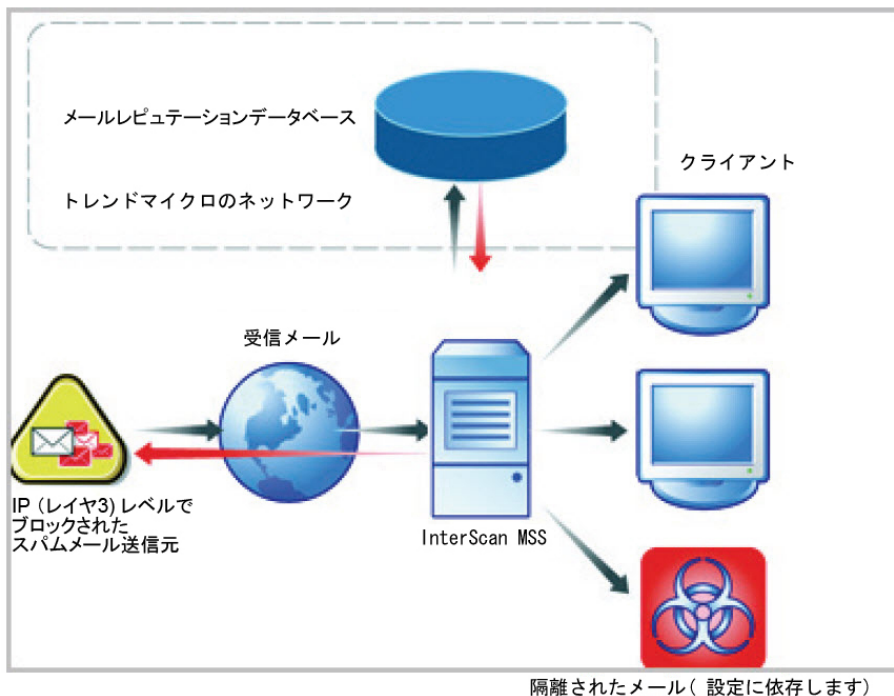
受信メールストリームに占めるスパムメールの量により異なります。受信するスパムメールが多いほど、ブロックされる接続の割合は高くなります。

メールレピュテーションテクノロジーの仕組み

トレンドマイクロのメールレピュテーションテクノロジーは、ドメインネームサービス (DNS) のクエリベースのサービスです。次のプロセスは、InterScan MSS が、送信側メールサーバから接続要求を受信した後に実行されます。

1. InterScan MSS が、接続を要求しているコンピュータの IP アドレスを記録します。
2. InterScan MSS が、その IP アドレスをトレンドマイクロのメールレピュテーション DNS サーバに転送し、評価データベースに問い合わせを行います。IP アドレスがすでにスパムメールとして報告されている場合、そのアドレスは問い合わせの時点ですでにデータベースに存在しています。
3. レコードが存在する場合は、メールレピュテーションが、InterScan MSS に永続的または一時的に接続要求をブロックするよう指示します。要求をブロックするかどうかは、スパムメールのソースの種類、履歴、現在の活動レベル、およびその他の観察パラメータによって決まります。

下記の図は、メールレピュテーションの仕組みを示します。



メールレピュテーションの動作の詳細については、<https://ers.trendmicro.com/>を参照してください。

Trend Micro Control Manager について

Trend Micro Control Manager (以下、Control Manager) は、ウイルス対策プログラムとコンテンツセキュリティプログラムを、その物理的な位置やプラットフォームに関係なく中央から制御できるようにす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は、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します。

- ・ **Control Manager サーバ:** Control Manager サーバは、Control Manager アプリケーションがインストールされるコンピュータです。Control Manager の Web ベースの管理コンソールは、このサーバでホストされます。
- ・ **エージェント:** エージェントは、Control Manager が製品を管理できるように、管理下の製品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 Control Manager サーバからコマンドを受信して、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、Control Manager に送信します。
- ・ **エンティティ:** エンティティは、製品ディレクトリ上の管理下の製品を表します。各エンティティは、ディレクトリツリーにアイコンで表示されます。このディレクトリには、Control Manager 管理コンソールにある、管理下のすべてのエンティティが表示されます。

Control Manager のサポート

次の表では、InterScan MSS でサポートされている Control Manager の機能を示しています。

表 1-4. サポートされる Control Manager の機能

特長	説明	サポートの有無
双方向通信	双方向通信では、InterScan MSS と Control Manager のいずれも通信プロセスを開始できます。	なし InterScan MSS のみが Control Manager との通信プロセスを開始できます。

特長	説明	サポートの有無
大規模感染予防ポリシー	大規模感染予防ポリシー (OPP) は、トレンドラボによって開発され、大規模感染に迅速に対応します。このポリシーには、InterScan MSS サーバまたはそのクライアントの感染確率を減らすために、InterScan MSS で実行する必要のある処理が一覧表示されます。 トレンドマイクロのアップデートサーバは、このポリシーを Control Manager 経由で InterScan MSS に配信します。	あり
クエリ用のログのアップロード	クエリの目的で InterScan MSS のウイルスログ、コンテンツセキュリティログ、およびメールレピュテーションログを Control Manager にアップロードします。	あり
シングルサインオン	InterScan MSS 管理コンソールに最初にログオンせずに、Control Manager から InterScan MSS を直接管理します。	なし Control Manager から InterScan MSS を管理するには、まず InterScan MSS 管理コンソールにログオンする必要があります。
設定の複製	Control Manager で既存の InterScan MSS サーバから新規の InterScan MSS サーバに設定を複製します。	あり
パターンファイルのアップデート	Control Manager から InterScan MSS によって使用されるパターンファイルをアップデートします。	あり

特長	説明	サポートの有無
エンジンのアップデート	Control Manager から InterScan MSS によって使用されるエンジンをアップデートします。	あり
製品コンポーネントのアップデート	Control Manager から Patch や HotFix などの InterScan MSS 製品コンポーネントをアップデートします。	なし 製品コンポーネントのアップデート方法については、Patch または HotFix の Readme を参照してください。
ユーザインタフェースリダイレクトによる設定	Control Manager からアクセス可能な InterScan MSS 管理コンソールを使用して InterScan MSS を設定します。	あり
製品登録の更新	Control Manager から InterScan MSS ライセンスを更新します。	あり
Control Manager のカスタムレポート	Control Manager には、メール関連データについてカスタムレポートを生成したりログクエリを実行したりする機能が用意されています。	あり

特長	説明	サポートの有無
Control Manager エージェントのインストール/アンインストール	Control Manager から InterScan MSS Control Manager エージェントをインストールまたはアンインストールします。	なし InterScan MSS Control Manager エージェントは、InterScan MSS をインストールすると自動的にインストールされます。エージェントを有効または無効にするには、InterScan MSS 管理コンソールから次の操作を行います。 1. [管理] > [接続] の順に選択します。 2. [Control Manager サーバ] タブをクリックします。 3. エージェントを有効または無効にするには、[MCP エージェントを有効にする] の横にあるチェックボックスをオンまたはオフにします。
イベント通知	Control Manager から InterScan MSS イベント通知を送信します。	あり
すべてのコマンドに対するコマンド追跡	Control Manager が InterScan MSS に対して発行するコマンドのステータスを追跡します。	あり

トレンドマイクロの Smart Protection について

トレンドマイクロは、Smart Protection サービスを介した次世代のコンテンツセキュリティを提供します。クラウド内で脅威情報を処理することにより、必要なシステムリソースを減らし、時間のかかる署名のダウンロードをなくします。

Smart Protection サービスには以下が含まれます。

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では、検索エンジンがローカルにあるパターンファイルではなく、Trend Micro Smart Protection Network にパターンファイルを照合してチェックします。パフォーマンスに優れたコンテンツ配信ネットワークにより、確認プロセスで発生する待ち時間が最小限に抑えられ、より迅速な保護が可能となります。

トレンドマイクロは、不正プログラムの検出率を高めるため、ファイルレピュテーションを継続的に強化しています。スマートフィードバックを採用することで、何百万ものユーザからファイルに関するフィードバックを集め、不正ファイルの可能性を判断するうえで役立つ情報を特定しています。

Web レピュテーションサービス

トレンドマイクロの Web レピュテーションでは、世界最大級のレピュテーションデータベースを使用して、Web サイトの存続期間や URL の変更、および不正プログラム挙動分析から検出される不審な活動の兆候といった要素を基に、ドメインの信頼性を判別します。精度を向上させると同時に誤検出を少なくするため、トレンドマイクロでは、サイト全体を分類するのではなく、特定のページにレピュテーションスコアを割り当てています。

Web レピュテーションテクノロジーは、次のことからユーザを守ります。

- ・ 感染サイトへのアクセス
- ・ サイバー犯罪に使用されている C&C サーバとの通信

新しいソリューションの必要性

従来の脅威処理方法では、不正プログラムのパターンファイル（または定義）が定期的にクライアントに配信され、ローカルに保存されます。保護を継続するためには、新しいアップデートを定期的に受信して、不正プログラム対策ソフトウェアに読み込む必要があります。

この方法が有効に機能する一方で、増加し続ける脅威は、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、さらに適切な保護を提供するまでにかかる全体的な時間に影響する可能性があります。急激な脅威の増加に対処するため、トレンドマイクロは、不正プログラム対策

シグネチャをクラウドに格納するアプローチを他に先駆けて開発しました。このアプローチで使用するテクノロジーとアーキテクチャにより、新たに出現する脅威からユーザを適切に保護できます。

Trend Micro Smart Protection Network

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は Trend Micro Smart Protection Network を介して InterScan MSS と連携します。

Trend Micro Smart Protection Network は、Web からの脅威やセキュリティリスクからユーザを保護する、次世代のクラウド-クライアント型コンテンツセキュリティインフラストラクチャです。このソリューションでは、軽量クライアントを使用し、独自のインターネットクラウドで提供されているメールレピュテーション、Web レピュテーション、ファイルレピュテーションの関連分析テクノロジーおよび脅威データベースにアクセスすることで、ローカルソリューションおよびホステッドソリューションの機能を強化して、企業ネットワーク内、自宅、または外出先にいる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、およびユーザが増えるとともに、お客さまのセキュリティ保護対策は自動的にアップデートおよび強化され、ユーザに対するリアルタイムのネイバーフッドウォッチ保護サービスが構築されています。

Smart Protection Network は、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。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、クライアントから Smart Protection Network に検索クエリが送信されます。

Smart Protection Network 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。クライアントから Smart Protection Network 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 サイトのレピュテーションが確認されます。クライアントは、Web サイトのレピュテーションを、コンピュータ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。

Smart Protection Network の詳細については、次のサイトを参照してください。

<http://www.trendmicro.co.jp/spn/>

グレーメールの検索について

グレーメールとは、スパムメールではなく、ユーザ自身が過去に要請した大量のメールメッセージのことを指します。InterScan MSS では、マーケティングメッセージ、ニュースレター、およびソーシャルネットワークの通知をグレーメールとして検出します。InterScan MSS では、次の 2 つの方法でグレーメールメッセージを識別します。

- ・ 送信元 IP アドレスにスコアを割り当てるメールレピュテーションサービス
- ・ メッセージコンテンツを識別するトレンドマイクロのスパムメール対策エンジン



注意

InterScan MSS では、これらの種類のメールメッセージを検出しますが、スパムメールのタグは付けません。

管理者は、検出されたメールメッセージを処理するためのルールを条件を定義します。各グレーメールメッセージのルールには、メッセージフィルタをバイパスするアドレスオブジェクトを含む除外リストがあります。アドレスオブジェクトは、単一の IP アドレスまたはアドレス範囲 (IPv4 または IPv6)、または CIDR (Classless Inter-Domain Routing) ブロックのいずれかです。

管理者には、ネットワーク内のグレーメールメッセージトラフィックについて理解するためのいくつかのオプションが用意されています。レポートは、外部または内部の送信元からのグレーメールメッセージの最多送信者と最多受信者を示します。管理者は、詳細なログ情報のクエリを実行したり、メール隔離を表示して、許可するグレーメールメッセージとして識別されたメッセージを必要に応じて解除したりすることができます。

グレーメールメッセージの除外リストは、エクスポートおよびインポートできます。

**注意**

グレーメール検索で InterScan MSS が外部 DNS サーバをクエリできることを確認してください。DNS サーバの設定を変更する場合は、検索サーバを再起動して新しい設定をロードしてください。

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について

トレンドマイクロの C&C コンタクトアラートサービスでは、強化された検出およびアラート機能により、持続的標的型攻撃 (APT: Advanced Persistent Threats) や標的型攻撃によるダメージを軽減します。このサービスは、Trend Micro Smart Protection Network によってコンパイル、テスト、および評価されたグローバルインテリジェンスリストを使用してコールバックアドレスを検出します。

C&C コンタクトアラートサービスにより、InterScan MSS は、メッセージヘッダの送信者、受信者および返信先アドレスと、メッセージ本文に含まれる URL を調べて、いずれかが既知の C&C オブジェクトに一致しているかどうかを確認できます。管理者は、メッセージがフラグ付けされたら、該当するメッセージを隔離して通知を送信するように InterScan MSS を設定できます。検出されたすべてのメールは、C&C オブジェクトと、これらのメッセージに対して実行された処理とともにログに記録されます。これらのログは、クエリ目的で Control Manager に送信されます。

第 2 章

はじめに

この章では、Trend Micro InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) の管理コンソールへのログオン方法について説明します。また、InterScan MSS を稼働させるためにインストール後すぐに必要となる作業の手順も示します。

この章の内容は次のとおりです。

- ・ 48 ページの「InterScan MSS の管理コンソールを開く」
- ・ 49 ページの「管理コンソールのパスワードを変更する」
- ・ 50 ページの「スマートスキャンを使用する」
- ・ 50 ページの「プロキシを設定する」
- ・ 52 ページの「InterScan MSS サービス」
- ・ 53 ページの「エンドユーザメール隔離の管理コンソールを開く」

InterScan MSS の管理コンソールを開く

InterScan MSS の管理コンソールは、プログラムがインストールされているサーバから、またはネットワークを介してリモートで、Web ブラウザに表示できます。

手順

1. 次の URL を入力します。

`https://<ターゲットサーバの IP アドレス>:8445`



ヒント

IP アドレスを使用する代わりに、サーバの完全修飾ドメイン名 (FQDN) を使用することもできます。

2. 管理コンソールを開くには、ログオン情報を入力します。

初期設定のログオンアカウント情報は次のとおりです。

- ・ 管理者のユーザ名: `admin`
- ・ パスワード: `imss9.1`

3. [ログオン] をクリックします。



注意

Internet Explorer を使用して管理コンソールにアクセスする場合、Internet Explorer ではアクセスがブロックされ、別の Web アドレスから証明書が発行されたことを示すポップアップダイアログが表示されます。[信頼済みサイト] のリスト (Internet Explorer の [インターネット オプション] > [セキュリティ]) に管理コンソールの IP アドレスを追加するか、メッセージを無視して [このサイトの閲覧を続行する] をクリックし、処理を続行します。

次に進む前に

ポリシーが不正改ざんされないよう、配置が終了したら、ただちに新しいログオンパスワードを設定して、定期的にパスワードを変更することをお勧めします。

オンラインヘルプを使用する

InterScan MSS 管理コンソールには、ユーザインタフェースの各フィールドについて説明するオンラインヘルプが用意されています。

InterScan MSS 管理コンソールから特定のページのオンラインヘルプにアクセスするには、そのページの右上隅にあるヘルプアイコン (🔍) をクリックします。

オンラインヘルプの「目次」にアクセスするには、ページヘッダの右にある [ログオフ] ハイパーリンクの横のヘルプアイコン (🔍) をクリックします。

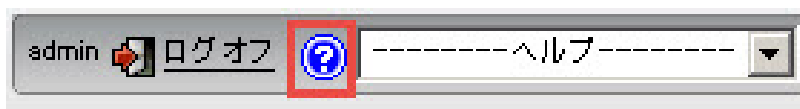


図 2-1. オンラインヘルプの目次にアクセスするためのアイコン

管理コンソールのパスワードを変更する

トレンドマイクロでは、管理コンソールへのアクセスに使用するパスワードを定期的に変更することをお勧めします。



警告!

管理者のパスワードは定期的に変更することを推奨します。

手順

1. [管理] > [パスワード] の順に選択します。
2. 現在のパスワードと新しいパスワードを指定し、新しいパスワードを確認します。



注意

使用できる文字は、英数字と、英数字以外の次の記号になります。`~!@#\$%^&*()[]{}+-.|:'<>?/.,=_

パスワードには、4～32 文字の英数字を使用してください。

3. [保存] をクリックします。
-

スマートスキャンを使用する

スマートスキャンのテキストフィールドに画面や機能の名前を入力すれば、管理コンソールの各画面へ簡単に移動できます。スマートスキャンのテキストボックスに画面や機能の名前を指定して、表示されるドロップダウンリストから目的のエントリを選択します。

プロキシを設定する

ネットワークでプロキシサーバが使用されている場合は、InterScan MSS でプロキシを設定します。プロキシ設定は、次の動作に影響を及ぼします。

- ・ コンポーネントのアップデート (パターンファイルと検索エンジン)
- ・ 製品ライセンスの登録
- ・ Web レピュテーションは Trend Micro Smart Protection Network にクエリを実行します。
- ・ クラウドプレフィルタサービスおよびスマートフィードバック

- ・ Trend Micro Email Encryption
- ・ 証明書の有効性の確認
- ・ Time-of-Click プロテクションサービス

手順

1. [管理] > [プロキシ] の順に選択します。

[プロキシ] 画面が表示されます。

プロキシ



☐ パターンファイル、エンジン、およびライセンスのアップデート、Webレピュテーションのクエリ、証明書の有効性の確認、さらにクラウドプレフィルタ、Trend Micro Email Encryption、および Time-of-Click プロテクションサービスとの通信にプロキシサーバを使用します。

プロキシ設定	
プロキシのタイプ:	HTTP
プロキシサーバ:	
ポート:	
ユーザ名:	
パスワード:	
保存 キャンセル	

2. [パターンファイル、エンジン、およびライセンスのアップデート、Webレピュテーションのクエリ、証明書の有効性の確認、さらにクラウドプレフィルタ、Trend Micro Email Encryption、および Time-of-Click プロテクションサービスとの通信にプロキシサーバを使用します。] をオンにします。
3. [HTTP]、[SOCKS4]、または [SOCKS5] のいずれかのプロキシプロトコルを指定します。



ヒント

クラウドプレフィルタを使用する場合は、[HTTP] または [SOCKS5] を使用することをお勧めします。

証明書の有効性の確認では、[HTTP] のみを使用します。

4. プロキシサーバのホスト名または IP アドレスを指定します。
 5. プロキシサーバがインターネットに接続するために使用するポートを指定します。
 6. プロキシサーバにアクセスするためのユーザ名を指定します。
 7. 上記に対応するパスワードを指定します。
 8. [保存] をクリックします。
-

InterScan MSS サービス

検索サービスおよびポリシーサービスは、InterScan MSS を使用してネットワークの保護を開始する際に必ず起動する必要があります。ただし、エンドユーザメール隔離管理コンソールは開始するかどうかを選択できます。

- ・ 検索サービス: SMTP/POP3 トラフィックの検索を実行します。
- ・ ポリシーサービス: 検索サービスのルールのリモートストアとして機能し、ルールの検索を強化します。
- ・ エンドユーザメール隔離管理コンソール: Web ベースの管理コンソールとして機能し、エンドユーザが受信したスパムメールを各自で表示、削除、および解除できるようにします。

これらのサービスの詳細については、「インストールガイド」を参照してください。

サービスを起動または停止する

InterScan MSS のインストールに成功し、各種の設定が終了したら、サービスを起動して、不正プログラムや他の脅威の検索を開始します。アップグレードまたはバックアップ機能を実行する際は、事前に InterScan MSS のサービスを停止する必要があります。

手順

1. [システムステータス] に移動します。
 2. サービスを開始または停止するには、[管理下のサービス] の下にある [開始] または [停止] ボタンをクリックします。
-

エンドユーザメール隔離の管理コンソールを開く

エンドユーザメール隔離管理コンソールにアクセスする前に、次の項目が実行済みであることを確認してください。

1. LDAP の設定。60 ページの「LDAP を設定する」を参照してください。
2. ユーザ隔離アクセスの有効化。445 ページの「エンドユーザアクセスを有効にする」を参照してください。

エンドユーザメール隔離管理コンソールは、InterScan MSS プログラムがインストールされているコンピュータから表示することも、ネットワークを介してブラウザからリモートで表示することもできます。

ネットワーク上の他のコンピュータからエンドユーザメール隔離管理コンソールを表示するには、インターネットブラウザに次の URL を入力します。

- ・ プライマリエンドユーザメール隔離サービス:

`https://<ターゲットサーバの IP アドレス>:8447`

- ・ セカンダリエンドユーザメール隔離サービス:

`https://<ターゲットサーバの IP アドレス>:8446`



警告!

セカンダリエンドユーザメール隔離サービスのすべての管理コンソールへ正常にアクセスするには、ネットワーク上にあるすべてのエンドユーザメール隔離サービスのシステム時間を同期化します。

IP アドレスを使用する代わりに、サーバの完全修飾ドメイン名 (FQDN) を使用することもできます。

ログオン名形式

エンドユーザメール隔離管理コンソールにアクセスするときに使用するログオン名の形式は、選択した認証タイプによって異なります。

表 2-1. エンドユーザメール隔離ログオン名の形式

認証タイプ	ログオン名形式
LDAP	ログオン名の形式は、LDAP を設定したときに選択した LDAP サーバの種類によって異なります。以下に有効なログオン名形式の例を示します。 ・ Domino: user1/domain ・ Microsoft Active Directory ・ Kerberos を使用しない場合: user1@domain.com (UPN) または domain\user1 ・ Kerberos を使用する場合: user1@domain.com ・ Microsoft Active Directory グローバルカタログ ・ Kerberos を使用しない場合: user1@domain.com (UPN) または domain\user1 ・ Kerberos を使用する場合: user1@domain.com ・ OpenLDAP: cn=manager, dc=test1, dc=com ・ Sun iPlanet Directory: uid=user1, ou=people, dc=domain, dc=com
SMTP	ログオン名として有効なメールアドレスを使用します。  注意 InterScan MSS では、auth login、auth plain、および starttls がサポートされます。

第 3 章

設定ウィザードの使用

この章では、設定ウィザードを使用して Trend Micro InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) を起動および実行する方法について説明します。

この章の内容は次のとおりです。

- ・ 56 ページの「設定ウィザードにより IMSS を設定する」
- ・ 56 ページの「通知を設定する」
- ・ 58 ページの「アップデート元を設定する」
- ・ 60 ページの「LDAP を設定する」
- ・ 64 ページの「内部アドレスを設定する」
- ・ 65 ページの「Control Manager サーバを設定する」
- ・ 67 ページの「製品をアクティベートする」
- ・ 68 ページの「設定を確認する」

設定ウィザードにより IMSS を設定する

このウィザードにアクセスするには、次のいずれかの方法を実行します。

手順

- 管理コンソールにログオンし、ログオン画面で [設定ウィザードを開く] がオンになっていることを確認して、ログオンします。

ウィザードが開きます。

- 管理コンソールにすでにログオンしている場合は、[管理] > [IMSS 設定] > [設定ウィザード] の順に選択します。

新しいウィンドウでウィザードが開きます。



通知を設定する

手順

- [次へ] をクリックします。

[通知設定] 画面が表示されます。

設定ウィザード
手順 7

通知設定 ログオフ 手順

初期設定のシステム通知について、メール通知およびSNMPトラップ 通知を設定します。

メール設定

受信者* root@localhost
複数のアドレスを指定する場合はセミコロン (,) で区切ってください。

送信者のメールアドレス* postmaster@localhost

SMTPサーバアドレス* 127.0.0.1

SMTPサーバポート番号* 10025

文字コード* UTF-8 (utf-8)

メッセージヘッダ:

メッセージフッタ:

SNMPトラップ

サーバ名 (IPまたはFQDN)

コミュニティ名 public

SNMPのバージョン: SNMPv1

< 戻る スキップ 次へ >

1. 通知設定
2. アップデート元
3. LDAP設定
4. 内部アドレス
5. Control Manager設定
6. 製品のアクティベーション
7. 設定の確認

2. [メール設定] で、次の項目を設定します。
 - ・ 受信者:受信者のメールアドレスを指定します。
 - ・ 送信者のメールアドレス:送信者として表示されるメールアドレスを指定します。
 - ・ SMTP サーバアドレス: ネットワーク上でメールを配信する SMTP サーバの完全修飾ドメイン名 (FQDN) または IP アドレス (IPv4 または IPv6) を指定します。
 - ・ SMTP ポート番号:InterScan MSS が SMTP サーバへの接続に使用するポート番号を指定します。
 - ・ 文字コード:InterScan MSS では、この設定を使用して、通知メッセージをエンコードします。
 - ・ メッセージヘッダ:通知の先頭に表示するテキストを指定します。
 - ・ メッセージフッタ:通知の末尾に表示するテキストを指定します。

3. [SNMP トラップ] で、次の項目を設定します。

**注意**

SNMP トラップは、管理上の注意が必要なイベントが発生したときに SNMP (Simple Network Management Protocol) サーバに送信される通知メッセージです。

- ・ サーバ名:SNMP サーバの完全修飾ドメイン名または IP アドレスを入力します。
- ・ コミュニティ名:SNMP サーバのコミュニティ名を入力します。
- ・ SNMP のバージョン: [SNMPv1] または [SNMPv2c] を選択します。

**注意**

コミュニティ名は、SNMP を実行するコンピュータおよび管理端末が属するグループです。すべての SNMP 管理端末に警告メッセージを送信するには、コミュニティ名として「public」を指定します。

アップデート元を設定する

手順

1. [次へ] をクリックします。

[アップデート元] 画面が表示されます。

設定ウィザード
手順 2/7

アップデート元 ログオフ ? 手順

アップデート元を選択し、プロキシを設定することで、MSSがコンポーネントのアップデート および アクティベートを行えるようにします。

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

☐ その他のインターネット上のサーバ

プロキシ設定

☐ [パターンファイル、エンジン、およびライセンスのアップデート、Webレピュテーションのクエリ、証明書の有効性の確認、さらにクラウドプレフィルタ、Trend Micro Email Encryption、およびTime-of-Clickプロテクションサービスとの通信にプロキシサーバを使用します。]

プロキシのタイプ*

プロキシサーバ*

ポート*

ユーザ名

パスワード

< 戻る スキップ 次へ >

手順

1. 通知設定
2. アップデート元
3. LDAP設定
4. 内部アドレス
5. Control Manager設定
6. 製品のアクティベーション
7. 設定の確認

2. アップデートに関する次のオプションを設定し、InterScan MSS がコンポーネントアップデートをどこから受け取り、InterScan MSS がどのプロキシ (使用する場合) を介してインターネットにアクセスするかを指定します。

オプション	説明
アップデート元	トレンドマイクロから直接アップデートを受け取る場合は、[トレンドマイクロのアップデートサーバ] をクリックします。または、[その他のインターネット上のサーバ] をクリックし、アップデート元の URL を入力します。アップデート元には、トレンドマイクロのアップデートサーバにアップデートがあるかどうかを確認するサーバを指定します。必要に応じて任意のアップデート元を指定できます。また、Control Manager サーバを使用できる場合は、その URL (http://<Control Manager サーバの IP アドレスまたは FQDN>/Tmcs Download/ActiveUpdate/) を入力することもできます。
プロキシ設定	[パターンファイル、エンジン、およびライセンスのアップデート、Webレピュテーションのクエリ、証明書の有効性の確認、さらにクラウドプ

オプション	説明
	レフィルタ、Trend Micro Email Encryption、および Time-of-Click プロテクションサービスとの通信にプロキシサーバを使用します。] チェックボックスをオンにして、プロキシのタイプ、プロキシサーバ、ポート、ユーザ名、パスワードを設定します。

LDAP を設定する



注意

LDAP 設定は、LDAP をユーザグループの定義、管理者権限、またはエンドユーザメール隔離の認証に使用する場合のみ指定します。

手順

1. [次へ] をクリックします。

[LDAP 設定] 画面が表示されます。

設定ウィザード
 手順 3/7

LDAP 設定

[ログアウト](#)
[手順](#)

LDAP 設定は、ユーザグループの定義、管理者権限、または Web 隔離機能に LDAP を使用する **場合にのみ** 入力します。Web 隔離機能を使用するには、LDAP を有効にする必要があります。複数の LDAP サーバを定義する必要がある場合は、次の画面を使用します。【管理】→【接続】→【LDAP】画面

LDAP の説明

説明*

LDAP 設定

LDAP サーバの種類*

☐ 有効 LDAP1

LDAP サーバ*

待機ポート番号*

☐ 有効 LDAP2

LDAP サーバ*

待機ポート番号*

例: example.com または 192.168.10.1

注意: LDAP サーバの種類が Microsoft Active Directory の場合は、グローバルカタログポート 3268 または 3269 (暗号化通信が有効な場合) を使用してください。

例: example.com または 192.168.10.1

注意: LDAP サーバの種類が Microsoft Active Directory の場合は、グローバルカタログポート 3268 または 3269 (暗号化通信が有効な場合) を使用してください。

1. 通知設定
2. アップデート元
3. LDAP 設定
4. 内部アドレス
5. Control Manager 設定
6. 製品のアクティベーション
7. 設定の確認

ポリシーサービスおよびEUGサービスのLDAPキャッシュ生存期限

キャッシュ生存期限 (分)*

LDAP管理者

LDAP管理者アカウント*

パスワード*

基本識別名* ⓘ

認証方法*
☒ 簡易 ⓘ
☐ 詳細: Active Directoryに対して Kerberos認証を使用する
 Kerberos認証の初期設定のレルム:
 初期設定のドメイン:
 鍵発行局 (KDC) および管理サーバ:
 鍵発行局 (KDC) ポート番号:

☐ IMSSとLDAP間の暗号化通信を有効にする
 CA証明書ファイル: ⓘ 参照...
 注意: IMSSとLDAP間の暗号化通信を有効にする場合は、636など、特定の暗号化通信 LDAP待機ポートを設定してください。

< 戻る スキップ 次へ >

2. 次の手順を実行して LDAP 設定を有効にします。
 - a. [LDAP サーバの種類] で、次のいずれかを選択します。
 - ・ Domino
 - ・ Microsoft Active Directory
 - ・ Microsoft Active Directory グローバルカタログ
 - ・ Open LDAP
 - ・ Sun iPlanet Directory
 - b. 片方または両方の LDAP サーバを有効にするには、[有効 LDAP1] または [有効 LDAP2] の横のチェックボックスをオンにします。

- c. LDAP サーバの名前と、これらのサーバの待機ポートの番号を指定します。
- d. [ポリシーサービスおよび EUQ サービスの LDAP キャッシュ生存期限] の [キャッシュ生存期限 (分)] に、生存期限の数値を指定します。
- e. [LDAP 管理者] では、管理者のアカウント、対応するパスワード、および基本識別名を指定します。LDAP サーバの種類と管理者アカウントの指定例を、次の表に示します。

表 3-1. LDAP サーバの種類

LDAP サーバ	LDAP 管理者アカウント (例)	基本識別名 (例)	認証方法
Active Directory™	Kerberos を使用しない場合: user1@domain.com (UPN) または domain¥user1 Kerberos を使用する場合: user1@domain.com	dc=domain, dc=com	簡易 詳細 (Kerberos 使用)
Active Directory グローバルカタログ	Kerberos を使用しない場合: user1@domain.com (UPN) または domain¥user1 Kerberos を使用する場合: user1@domain.com	dc=domain, dc=com dc=domain1,dc=com (一意のドメインが複数存在する場合)	簡易 詳細 (Kerberos 使用)
OpenLDAP	cn=manager, dc=test1, dc=com	dc=test1, dc=com	簡易
Lotus Domino™	user1/domain	該当なし	簡易

LDAP サーバ	LDAP 管理者アカウント (例)	基本識別名 (例)	認証方法
Sun iPlanet Directory	uid=user1, ou=people, dc=domain, dc=com	uid=user1, ou=people, dc=domain, dc=com	簡易

- f. [認証方法] では、[簡易] 認証または [詳細] 認証を選択します。Active Directory の [詳細] 認証を選択した場合は、Kerberos 認証の初期設定のレلم、初期設定のドメイン、KDC と管理サーバ、および KDC ポート番号を設定します。
- g. [InterScan MSS と LDAP 間の暗号化通信を有効にする] チェックボックスをオンにし、[参照] をクリックして CA 証明書ファイルをアップロードし、LDAP サーバで使用する証明書を確認します。

内部アドレスを設定する

InterScan MSS では、内部アドレスに登録された情報を使用して、ポリシーまたはイベントが受信用であるか、または送信用であるかを判断します。

- ・ 送信メッセージのルールを設定している場合、内部アドレスのリストは送信者に適用されます。
- ・ 受信メッセージのルールを設定している場合、内部アドレスのリストは受信者に適用されます。

手順

1. [次へ] をクリックします。

[内部アドレス] 画面が表示されます。

2. 内部ドメインおよびユーザグループを定義するには、次の手順を実行します。
 - ・ ドロップダウンリストから [ドメインの入力] を選択してテキストボックスでドメインを指定し、[>>] をクリックします。
 - ・ ドロップダウンリストから [LDAP グループの検索] を選択します。LDAP グループを選択する画面が表示されます。テキストボックスで検索対象の LDAP グループ名を指定して、[検索] をクリックします。検索結果がリストボックスに表示されます。[選択済み] リストに追加するには、[>>] をクリックします。
 - ・ [インポート] ボタンをクリックして、定義済みのドメインのリストが記載されたテキストファイルをインポートします。

Control Manager サーバを設定する

手順

1. [次へ] をクリックします。

[Control Manager サーバの設定] 画面が表示されます。

設定ウィザード
手順 5/7

Control Managerサーバの設定 ログオフ ? 手順

Trend Micro™ Control Manager™ (以下、Control Manager) は、IMSSデバイスや他のウイルス対策プログラムおよびコンテンツセキュリティプログラムを一元管理するためのソフトウェア管理ソリューションです。

Control Managerサーバの設定

IMSSをControl Managerで管理するには、Control Manager MCPエージェントを有効にして、すべてのControl Managerサーバの設定項目を入力してください。

☒ MCPエージェントを有効にする

サーバ*

通信プロトコル*
☒ HTTPポート:
☐ HTTPSポート:

Webサーバ認証
 ユーザ名*
 パスワード*

☒ プロキシを有効にする

プロキシのタイプ*

プロキシサーバ*

ポート*

ユーザ名*

パスワード*

< 戻る スキップ 次へ >

1. 通知設定
2. アップデート元
3. LDAP設定
4. 内部アドレス
5. Control Manager設定
6. 製品のアクティベーション
7. 設定の確認

2. Control Manager を使用して InterScan MSS を管理する場合は、次の操作を行います。
 - a. エージェントを有効にします (エージェントは、初期設定で InterScan MSS とともにインストールされています)。
 - b. [サーバ] に Control Manager の IP アドレス (IPv4 または IPv6) または完全修飾ドメイン名 (FQDN) を指定します。
 - c. [通信プロトコル] では [HTTP ポート] または [HTTPS ポート] を選択し、対応するポート番号を指定します。

HTTP アクセス用の初期設定ポート番号は 80 であり、HTTPS 用の初期設定ポート番号は 443 です。

- d. Web サーバで認証が必要な場合は、[Web サーバ認証] でユーザ名およびパスワードを指定します。
- e. InterScan MSS と Control Manager の間にプロキシサーバが配置されている場合は、[プロキシを有効にする] を選択します。
- f. プロキシのタイプ、プロキシサーバ、ポート、ユーザ名、およびパスワードを指定します。

製品をアクティベートする

手順

1. [次へ] をクリックします。

[製品のアクティベーション] 画面が表示されます。

設定ウィザード
手順 6/7

製品のアクティベーション

ログオフ 手順

1. 通知設定
2. アップデート元
3. LDAP設定
4. 内部アドレス
5. Control Manager設定
6. 製品のアクティベーション
7. 設定の確認

アクティベーションコードを取得していない場合は、レジストレーションキーを使用してオンライン登録を実行してください。

オンライン登録

アクティベート	設定
クラウドプレフィルタ	
ウイルス対策およびコンテンツフィルタ	
スパムメール対策 (コンテンツ検索)	
規制コンプライアンス	

< 戻る 次へ >

2. 適用可能なアクティベーションコードを取得したら、製品またはサービスごとにアクティベーションコードを指定してアクティベートします。

設定を確認する

手順

1. [次へ] をクリックします。

[設定の確認] 画面が表示されます。



2. 設定が正しい場合は、[完了] をクリックします。

指定された設定を変更するには、[戻る] をクリックして変更します。

第 4 章

コンポーネントのアップデート

この章では、Trend Micro InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) コンポーネントのアップデート方法について説明します。

この章の内容は次のとおりです。

- ・ 70 ページの「エンジンとパターンファイルをアップデートする」
- ・ 71 ページの「アップデート元を指定する」
- ・ 72 ページの「手動アップデートを実行する」
- ・ 74 ページの「コンポーネントのアップデートをロールバックする」
- ・ 74 ページの「予約コンポーネントをアップデートする」

エンジンとパターンファイルをアップデートする

最新の不正プログラムからネットワークを保護するには、InterScan MSS コンポーネントを定期的にアップデートするようにします。アップデートは、手動または予約による実行を選択できます。

以下の表に、InterScan MSS のすべてのコンポーネントの一覧を示します。

表 4-1. InterScan MSS のコンポーネント

コンポーネント	説明
ウイルス検索エンジン	インターネットワーム、マスメーリングソフト、トロイの木馬、フィッシングサイト、スパイウェア、ネットワークの脆弱性、およびメッセージや添付ファイルに含まれるウイルスを検出します。
高度な脅威検索エンジン	高度な脅威検索エンジン (以下、ATSE) では、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ることで使用することにより、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。
ウイルスパターンファイル	最新のウイルス/不正プログラムおよび複合型の攻撃を InterScan MSS で特定するための情報が含まれます。
スパイウェアパターンファイル	メッセージや添付ファイルに含まれるスパイウェア/グレーウェアを特定します。
IntelliTrap パターンファイル	IntelliTrap パターンファイルはリアルタイム圧縮された実行可能ファイル内の不正コードを検出します。
IntelliTrap 除外パターンファイル	IntelliTrap 除外パターンファイルには、「許可する」圧縮ファイルの一覧が含まれます。
スパムメール検索エンジン	スパムメールを検出します。
スパムメール対策パターンファイル	最新のスパムメールを特定するための情報が含まれます。
URL フィルタエンジン	URL フィルタエンジンにより、InterScan MSS とトレンドマイクロの URL フィルタサービス間の通信を容易にします。URL フィルタサービスによって URL が評価され、その評価情報が InterScan MSS に提供されます。

コンポーネント	説明
スマートスキャンエージェントパターンファイル	スマートスキャンモードで InterScan MSS が使用するパターン定義が含まれます。InterScan MSS は、その他のコンポーネントをダウンロードする場合と同じ方法で、このパターンファイルをアップデート元からダウンロードします。

アップデート元を指定する

InterScan MSS の検索エンジンおよびパターンファイルをアップデートする前に、アップデート元を指定します。初期設定では、最新コンポーネントのアップデート元であるトレンドマイクロのアップデートサーバからコンポーネントがダウンロードされます。ただし、Control Manager を使用して InterScan MSS を管理している場合は、Control Manager サーバからコンポーネントをアップデートできます。

InterScan MSS の設定時に設定ウィザードを使用してアップデート元を指定しなかった場合は、アップデート元またはプロキシ設定を入力してください。

手順

1. [管理] > [アップデート] > [コンポーネント] の順に選択します。
[コンポーネントのアップデート] 画面が表示されます。
2. [アップデート元] タブをクリックします。

コンポーネントのアップデート 

スケジュール **アップデート元**

コンポーネントをアップデートするにはアップデート元を選択します。IMSVAがネットワーク上のプロキシサーバにアクセスする必要がある場合は、プロキシの設定を行います。

☒ トレンドマイクロのアップデートサーバ
☐ その他のインターネット上のサーバ

保存 キャンセル

3. [アップデート元] で、次のいずれかを選択します。
 - ・ トrendマイクロのアップデートサーバ: 初期設定の最新コンポーネントのダウンロード元です。
 - ・ その他のインターネット上のサーバ: Control Manager サーバやその他のアップデート元の URL または IP アドレスを指定します。
 4. [保存] をクリックします。

設定ウィザードを使用している場合は、[次へ] をクリックします。
-

手動アップデートを実行する

次のような状況の場合は、InterScan MSS コンポーネントの手動アップデートを実行します。

- ・ InterScan MSS のインストール、配置、またはアップグレードの直後
- ・ ネットワークセキュリティが不正プログラムによる危険にさらされている恐れがあり、すぐにコンポーネントをアップデートしたい場合

手順

1. [システムステータス] 画面に移動します。

システムステータス



接続の有効化

☒ SMTP接続を許可する
☐ POP3接続を許可する
 保存

コンポーネント
前回の表示更新 2017/12/04 19:45:23 ↻ 表示更新

アップデート
ロールバック

☐ 名前	現在のバージョン	利用可能なバージョン	アップデートスケジュール
☐ ウイルス検索エンジン	9.950.1006	9.950.1006	
☐ 高度な脅威検索エンジン	9.867.1029	10.300.1010	
☐ ウイルスパターンファイル	12.439.00	13.821.00	
☐ スパイウェアパターンファイル	1.719.00	1.897.00	
☐ IntelliTrapパターンファイル IntelliTrap除外パターンファイル	0.227.00 1.279.00	0.235.00 1.457.00	
☐ スпамメール検索エンジン	8.100.1062	8.100.1062	
☐ スпамメール対策パターンファイル	22232.006	23508.006	
☐ URLフィルタエンジン	3.910.1008	3.910.1008	
☐ スマートスキャンエージェントパターンファイル	12.439.00	13.821.00	

管理下のサービス

ホスト名	接続	検索サービス	ポリマーサービス	EUQ管理コンソール
	✓	✓ 停止	✓ 停止	✓ 停止

2. [コンポーネント] で、InterScan MSS がネットワークを保護するために使用するウイルス対策、スパイウェア対策、およびスパムメール対策のコンポーネントのバージョン番号を確認します。
3. すべてのコンポーネントをアップデートするには、[名前] フィールドの隣にあるチェックボックスをオンにします。特定のコンポーネントをアップデートするには、必要なコンポーネントの横にあるチェックボックスをオンにします。
4. [アップデート] をクリックします。

コンポーネントのアップデートをロールバックする

InterScan MSS のコンポーネントをアップデートした後にシステムに障害が発生した場合、旧バージョンにロールバックできます。

手順

1. [システムステータス] 画面に移動します。
 2. すべてのコンポーネントを旧バージョンにロールバックするには、最初の列のヘッダにある ([名前] フィールドの隣にある) チェックボックスをオンにします。特定のコンポーネントをロールバックするには、必要なコンポーネントの横にあるチェックボックスをオンにします。
 3. [ロールバック] ボタンをクリックします。
-

予約コンポーネントをアップデートする

コンポーネントのアップデートは次の 2 段階の手順で実行されます。

1. 予約時間に、InterScan MSS 管理データベースにより、アップデート元へ新しい検索エンジンまたはパターンファイルの有無を最初にチェックします。
2. その後、InterScan MSS 検索サービスにより、コンポーネントのアップデートについて一定の間隔で管理データベースがチェックされます。初期設定の間隔は 3 分です。

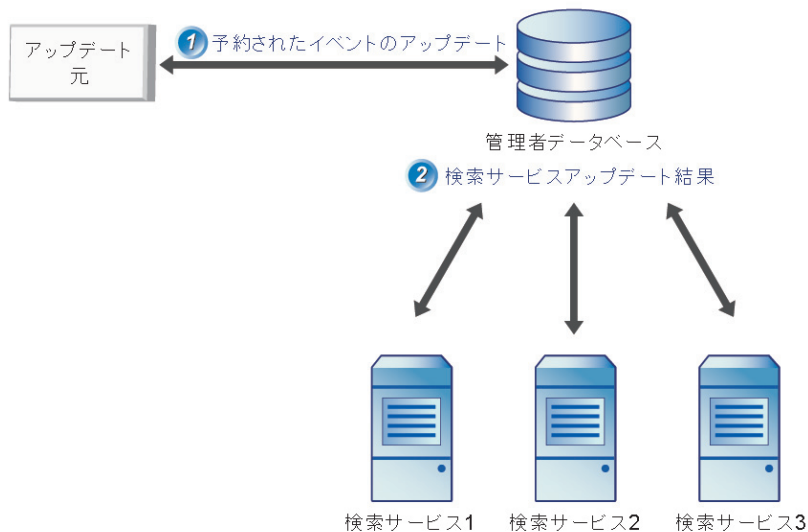


図 4-1. 検索エンジンおよびパターンファイルのアップデート

予約アップデートを設定する

ウイルス対策とスパムメール対策のコンポーネントを定期的にダウンロードできない場合、ネットワークはインターネット上の脅威に対して無防備になります。アップデートプロセスを自動化するには、予約アップデートを設定します。ネットワークで利用できるインターネット帯域幅が限られている場合は、予約アップデートを混雑していない時間に実行するように設定します。

手順

1. [管理] > [アップデート] > [コンポーネント] の順に選択します。

[コンポーネントのアップデート] 画面が表示され、初期設定では [スケジュール] タブが選択されます。

コンポーネントのアップデート



スケジュール
アップデート元

☒ 予約アップデートを有効にする

アップデートコンポーネント

☒ ウイルス検索エンジン
☒ 高度な脅威検索エンジン
☒ 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
☒ スпамメール検索エンジン
☒ スпамメール対策 パターンファイル
☒ 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

アップデートスケジュール

☒ 間隔 (分) 15
☐ (毎時) 00
☐ (毎日) 0 : 00
☐ (毎週) 日曜日 0 : 00

2. [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ます。
3. [アップデートコンポーネント] で、アップデートするコンポーネントを選択します。すべてのコンポーネントをアップデートすることをお勧めします。
4. [アップデートスケジュール] で、アップデートの頻度を選択します。
 - ・ 間隔 (分): 1 時間内に指定した間隔でアップデートを実行します。間隔 (分) を選択します。

たとえば、15 を選択すると、毎時 0 分、15 分、30 分、45 分にアップデートされます。30 を選択すると、毎時 0 分と 30 分にアップデートされます。

- ・ 毎時: 1 時間に 1 回アップデートを実行します。アップデートを実行する時刻 (分) を選択してください。

たとえば、15 を選択すると、毎時 15 分にアップデートされます。

- ・ 毎日: 1 日に 1 回アップデートを実行します。アップデートを実行する時刻 (時、分) を選択してください。
- ・ 毎週: 1 週間に 1 回アップデートを実行します。アップデートを実行する曜日と時刻 (時、分) を選択してください。

5. [保存] をクリックします。
-

第 5 章

クラウドプレフィルタの導入

この章では、主にクラウドプレフィルタについて、また InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) でクラウドプレフィルタを使用する方法について説明します。

この章の内容は次のとおりです。

- ・ 80 ページの「クラウドプレフィルタについて」
- ・ 83 ページの「クラウドプレフィルタアカウントを作成する」

クラウドプレフィルタについて

クラウドプレフィルタサービスは、トレンドマイクロの SaaS 型メールセキュリティソリューションと統合された管理下のメールセキュリティサービスです。このサービスを介して受信メッセージをルーティングすることにより、スパムメール、フィッシング、ウイルスなど、メッセージング関連の脅威がネットワークに到達するのを阻止し、これらの脅威からドメインを保護できます。

クラウドプレフィルタを使用したメールフローと使用しないメールフロー

クラウドプレフィルタを使用しない場合、ウイルス、スパムメール、およびその他の悪意のある脅威を含むメッセージがネットワークに直接到達します。これらの不正なメッセージは、ネットワーク帯域幅を消費し、その対応に必要なとなる管理作業のための人的リソースを浪費します。

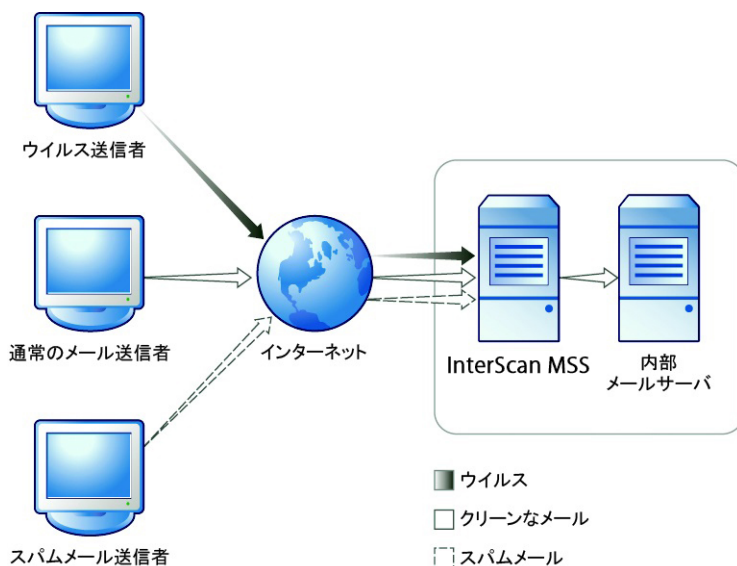


図 5-1. クラウドプレフィルタを使用しないメールフロー

クラウドプレフィルタを使用すると、ネットワーク外から送信される不正なメッセージに対してドメインを保護できます。クラウドプレフィルタは、不正なメッセージがネットワークに到達する前にそれをブロックします。

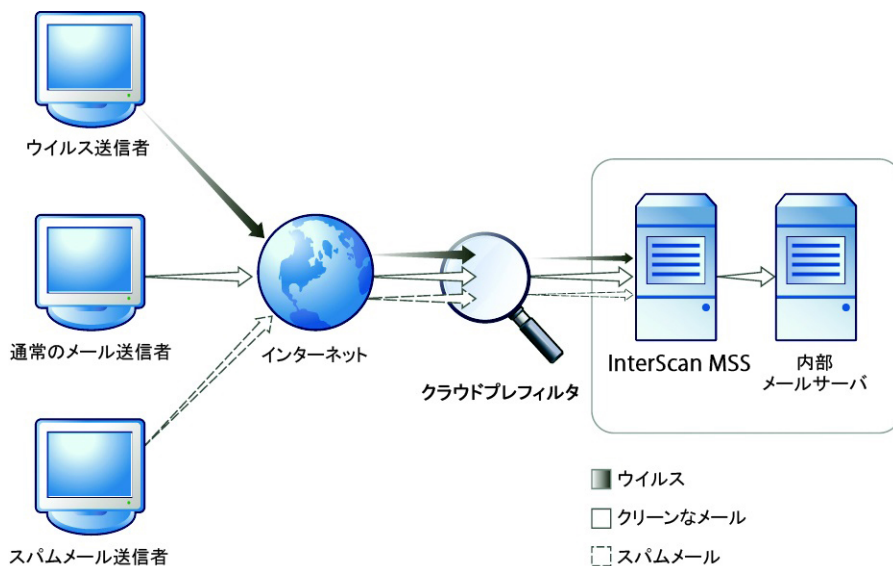


図 5-2. クラウドプレフィルタを使用したメールフロー

クラウドプレフィルタと InterScan MSS 間の通信

クラウドプレフィルタでは、SMTP プロトコルを使用してメッセージを InterScan MSS にルーティングします。

InterScan MSS は、HTTPS 接続を使用してクラウドプレフィルタと通信し、アカウントの作成、アカウントに関連したポリシーの管理、またはメッセージ追跡やレポートデータの取得といったコマンド要求を実行します。

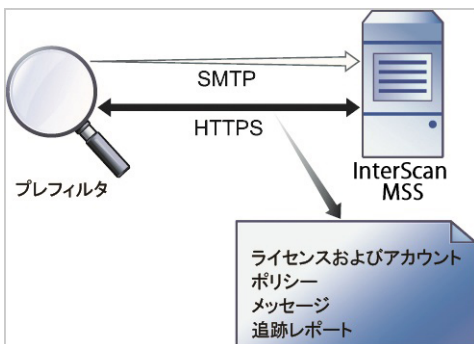


図 5-3. クラウドプレフィルタと InterScan MSS 間の通信

クラウドプレフィルタの用語

クラウドプレフィルタの説明には、次の用語が使用されます。

表 5-1. クラウドプレフィルタの用語

用語	説明
アカウント	クラウドプレフィルタアカウントは、クラウドプレフィルタポリシーを管理するために使用されます。クラウドプレフィルタサービスを使用する前に、1つのクラウドプレフィルタアカウントを作成する必要があります。 アカウントの作成後、InterScan MSS にアカウント情報がローカルで保存されます。InterScan MSS はこのアカウント情報を使用してクラウドプレフィルタと通信し、クラウドプレフィルタポリシーの管理、またはメッセージ追跡やレポートデータの取得といったコマンド要求を実行します。

用語	説明
ポリシー	クラウドプレフィルタポリシーはドメインに適用されます。1つのドメインにつき1つのポリシーのみを作成できます。あるドメインに対して送信されたメッセージがクラウドプレフィルタに到達すると、クラウドプレフィルタはそのドメインのポリシーを使用して、メッセージの検索方法やドメインにメッセージをルーティングする方法を決定します。 クラウドプレフィルタは、クラウドプレフィルタポリシーリストに存在しない、ドメインに対するすべてのメッセージを拒否します。 すべてのポリシーはクラウドプレフィルタサービスによってクラウド内に保存されます。
受信サーバ	クラウドプレフィルタの受信サーバは、受信メッセージを受け取るサーバです。ドメインを登録すると、クラウドプレフィルタは、MXレコードとして使用する、受信サーバのアドレスを提供します。

クラウドプレフィルタアカウントを作成する

クラウドプレフィルタを使用する前に、クラウドプレフィルタアカウントを作成する必要があります。

手順

1. [クラウドプレフィルタ] をクリックします。

[クラウドプレフィルタアカウントの作成/認証] 画面が表示されます。

クラウドプレフィルタアカウントの作成/認証



クラウドプレフィルタアカウントを最初に作成するとき、クラウドサーバによってそのアカウントのキーファイルが生成されます。クラウドサーバにプレフィルタサービスを登録するときには、アカウント名とキーファイルの両方が必要になります。

クラウドプレフィルタアカウントを作成済みですか。 ☐ はい ☒ いいえ

クラウドプレフィルタアカウントの作成

アカウント名*

アカウント名に使用できる文字: 「A～Z」、「a～z」、「0～9」、「-」。

メールアドレス*

メールアドレスに使用できる文字: 「A～Z」、「a～z」、「0～9」、「@」、「.」、「-」。

ユーザの場所*

North America

作成

2. [クラウドプレフィルタアカウントを作成済みですか。] のオプションで [いいえ] を選択します。
3. アカウントの名前とメールアドレスを指定します。
4. [ユーザの場所] リストから場所を指定します。この設定は、使用するトレンドマイクロのグローバルデータセンターを指定します。
5. [作成] をクリックします。

InterScan MSS で、クラウドプレフィルタアカウントのキーが生成されます。

クラウドプレフィルタアカウントの作成/認証



クラウドプレフィルタアカウントを最初に作成するとき、クラウドサーバによってそのアカウントのキーファイルが生成されます。クラウドサーバにプレフィルタサービスを登録するときには、アカウント名とキーファイルの両方が必要になります。



アカウントが正常に作成されました。キーファイルをエクスポートして安全な場所に保管してください。

キーファイルのエクスポート

クラウドプレフィルタサービスのロード

6. このキーを安全な場所に保存します。InterScan MSS では、このキーとユーザ名を使用してクラウドプレフィルタへの接続を認証します。



ヒント

キーファイルは保存することをお勧めします。キーファイルには、アカウントのパスワード、データセンター情報、およびその他の関連する設定が含まれます。

7. [クラウドプレフィルタサービスのロード] をクリックします。

[クラウドプレフィルタポリシーリスト] 画面が表示されます。

クラウドプレフィルタ

Powered by Trend Micro Email Security SaaS Solutions



クラウドプレフィルタポリシーリスト ?

[クラウドプレフィルタアカウントの情報](#)

[クラウドプレフィルタのサービス状況と定期メンテナンスのお知らせ](#)

☐ 追加 ☐ 削除	ドメイン ▲	メールレピュテーション	ウイルス対策	スパムメール対策
☐	imssjp.com 	詳細		

☐ 追加 ☐ 削除

1-1 / 1 |< < ページ 1 > > |

15件/ページ ▼

注意:クラウドプレフィルタのメリットを最大限引き出すために次の注意事項に従うことをお勧めします。

1. クラウドプレフィルタのMXレコードには、既存のMXレコードより高い優先度を設定 (より小さい数値を指定) してください。そうすることで、既存のMXレコードがクラウドプレフィルタのバックアップとして動作し、中断なくメール配信できます。

2. オンプレミスIMSSポリシーをミラーし、ただし、オンプレミスIMSSVAポリシーほど積極的でないクラウドプレフィルタポリシーを作成します。重複したポリシーを使用することで、万が一クラウドプレフィルタが使用不能になった場合でもビジネスを保護できます。

8. アカウント情報を表示するには、[クラウドプレフィルタポリシーリスト] 画面で [クラウドプレフィルタアカウントの情報] をクリックします。

クラウドプレフィルタアカウントの情報

アカウント名: andytest

キーファイル: [キーファイルのエクスポート](#)

メールアドレス:  andy01@trend02.com

メールアドレスの変更

メールアドレス: andy01@trend02.com

新規メールアドレス:

確認用メールアドレス:

[保存](#)

[キャンセル](#)

第 6 章

ATSE および仮想アナライザの導入

この章では、高度な脅威検索エンジン (ASTE) を有効にし、仮想アナライザを設定する方法について説明します。

この章の内容は次のとおりです。

- ・ 90 ページの「検索テクノロジー」
- ・ 90 ページの「高度な脅威検索エンジンについて」
- ・ 92 ページの「仮想アナライザについて」

検索テクノロジー

InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) では、検索エンジンを設定することで、会社のセキュリティポリシーに適した不正プログラム検出レベルを選択できます。

以下の表では、InterScan MSS で使用できる検索テクノロジーについて説明します。

表 6-1. 検索テクノロジー

検索テクノロジー	説明
ウイルス検索エンジン	ウイルス検索エンジンは、基本的な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ーを採用して脅威を特定します。
高度な脅威検索エンジン (ATSE)	ATSE では、強力な検索を実行して、ファイルにドキュメントエクспロイトなど従来とは異なる脅威が存在するかどうかをチェックします。ウイルス検索エンジンの機能を強化することで、ATSE では、潜在する高度な脅威を検出します。それらの脅威は、さらなる分析のために仮想アナライザに送信できます。  注意 InterScan MSS は仮想アナライザと統合されています。この隔離された仮想環境は、Deep Discovery Analyzer 内でサンプルを管理および分析するために使用されます。

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 (以下、ATSE) では、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ることで、標的型攻撃で使われるドキュメントエクспロイトやその他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

- ・ 埋め込まれた不正コードの検出
- ・ 既知の脆弱性の検出ルール
- ・ ファイルの損傷を処理する高度な解析機能

**重要**

ATSE は既知および未知の高度な脅威を識別するので、ATSE を有効化すると、正当なファイルが不正だとしてフラグ付けされる可能性が高まる場合があります。検出されたファイルは、さらに観察および分析するために、管理された仮想環境に送信することをお勧めします。

高度な脅威について

高度な脅威は、あまりなじみのない手段を使用してシステムを攻撃したり感染させたりします。ヒューリスティック検索は、高度な脅威を検出して企業システムへのダメージを軽減します。ATSE を使用すれば、標的型攻撃で 사용되는典型的な脅威に対するさらなる保護層をシステムに追加できます。

ATSE で検出される高度な脅威の種類のいくつかは、次のとおりです。

- ・ 攻撃コード: 攻撃コードとは、ソフトウェアの脆弱性を利用しようと、攻撃者が意図的に作成したコードの一部です。こうしたコードは一般的に、不正プログラムに組み込まれています。
- ・ 標的型攻撃: 標的型攻撃とは、攻撃者が、特定の標的を攻撃し、コンピュータへの不正アクセスを試みる侵入攻撃です。こうした攻撃では、攻撃者が標的のネットワーク内で機密情報を抜き取れるよう、ネットワーク内に継続的に留まろうとします。
- ・ ゼロデイ脅威: ゼロデイ脅威では、それまで知られていなかったソフトウェアの脆弱性を悪用します。

**ヒント**

ATSE を有効にすることをお勧めします。

高度な脅威検索エンジンを有効にする

手順

1. [ポリシー] > [検索エンジン] の順に選択します。
 2. [高度な脅威検索エンジンを有効にする] を選択します。
 3. [保存] をクリックします。
-

ATSE が有効になると、InterScan MSS のデーモンが自動的に再起動されます。

仮想アナライザについて

InterScan MSS は Deep Discovery Analyzer の仮想アナライザと統合されています。仮想アナライザはファイルや URL サンプルを必要に応じて分析するための製品で、別途ライセンスが必要になります。

InterScan MSS は、添付ファイルを含め、不審メッセージをさらに分析するために仮想アナライザに送信します。特定の添付ファイルのタイプに対して仮想アナライザの検索が有効になっている場合は、その添付ファイルを含むメッセージも仮想アナライザに送信されます。仮想アナライザは分離された仮想環境で内容のシミュレーションと分析を実行し、多くの種類の不正プログラムに一般に関連付けられている特性を識別します。

特に、仮想アナライザはメッセージに添付されたファイルに不正なコードが含まれているかどうかを確認します。多くのファイルには非実行可能データが含まれていますが、攻撃者はこうしたファイルを用いて、ファイルを実行するプログラムや OS の脆弱性を悪用する方法を見つけ出します。このため、攻撃者にとって、不正なファイルを対象ユーザに送信することが、システムを乗っ取る効果的な方法となっています。

詳細については、該当する製品の管理者ガイドを参照してください。

ATSE による検出と仮想アナライザ

InterScan MSS は、ATSE を利用して、仮想アナライザに送信するメッセージを決定します。ATSE を有効にすると、標的型攻撃で使用される文書の脆弱性やその他の脅威など、高度な脅威に対するさらなる保護層が実現されます。

ATSE の検出は、プレフィックス HEUR、EXPL、および AFI MACRO によって識別されます。検出名にいずれかのプレフィックスが含まれている場合、InterScan MSS では次のように処理します。

- ・ さらなる分析のため、添付ファイルを含むメッセージ全体を仮想アナライザに送信します。
- ・ 仮想アナライザからの分析結果に基づいて、追加の処理を決定します。

仮想アナライザでは、分析された各メッセージにリスクレベルを割り当てます。InterScan MSS では、メッセージを送信してから約 60 秒後に、仮想アナライザにリスクレベルを照会します。リスクレベルを受信した後、InterScan MSS は、このリスクレベルと、InterScan MSS 管理コンソールで選択されているセキュリティレベルに基づいて、メッセージが安全であるか、潜在的な脅威であるか、または分析済み脅威であるかを判断します。

仮想アナライザのリスクレベルと InterScan MSS のセキュリティレベルの設定

InterScan MSS は、仮想アナライザによって返されたリスクレベルと InterScan MSS 管理コンソールで選択したセキュリティレベルに基づいて、ATSE が検出したメッセージを処理します。考えられるシナリオは次のとおりです。

- ・ 返されたリスクレベルが選択したセキュリティレベルと一致しない場合、InterScan MSS は、メッセージが安全であると判断します。
- ・ リスクレベルが返されない場合、返されたリスクレベルが無効な場合、または仮想アナライザの分析の最長時間に達した場合は、仮想アナライザの検索の除外が開始され、検出結果が潜在的な脅威 (ATSE) としてログに記録されます。
- ・ 返されたリスクレベルが選択したセキュリティレベルと一致する場合は、指定した処理が実行され、検出結果が分析済み脅威 (ATSE) としてログに記録されます。

以下の表は、セキュリティレベル、それに対応する仮想アナライザのリスクレベル、および InterScan MSS が実行する処理を示しています。



ヒント

セキュリティレベルは [低] に設定することをお勧めします。

セキュリティレベル	説明	リスクレベル
高	不審な動作を示しているすべてのメッセージに処理を適用します。	・ 高リスク ・ 中リスク ・ 低リスク
中	不正である可能性が中程度から高度のメッセージに処理を適用します。	・ 高リスク ・ 中リスク
低	不正である可能性が高いメッセージにのみ処理を適用します。	・ 高リスク

仮想アナライザの設定

手順

1. [ポリシー] > [仮想アナライザ] の順に選択します。

[仮想アナライザの設定] タブが初期設定で表示されます。

仮想アナライザ
?

仮想アナライザの設定

サーバ管理

☐ メールメッセージを仮想アナライザに送信 !

セキュリティレベルの設定

仮想アナライザがメッセージのリスクレベルを評価した後、IMSVaが以下に設定されたセキュリティレベルに基づいて指定された処理をメッセージに対して実行します。

☒ 高
☐ 中
☐ 低

不審な動作を示しているすべてのメッセージに処理を適用する

不正プログラムである可能性が中程度から高いメッセージに処理を適用する

不正プログラムである可能性が高いメッセージにのみ処理を適用する (推奨)

タイミングの設定

分析の最長時間: 秒 (値の範囲: 300~1800)

データベース切断設定

IMSVaの管理データベースの接続が切断されると、次の処理が実行されます。

☒ 仮想アナライザへのメッセージ送信の停止
☐ 仮想アナライザの検索除外に指定された処理の実行

仮想アナライザのプロキシ設定

☐ プロキシを有効にする

プロキシのタイプ:

プロキシサーバ:

プロキシサーバポート:

ユーザ名:

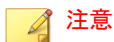
パスワード:

HTTP

保存

キャンセル

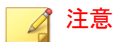
2. [メールメッセージを仮想アナライザに送信] を選択します。
3. 仮想アナライザで分析するメッセージの [セキュリティレベルの設定] を設定します。

**注意**

このセキュリティレベルにより、InterScan MSS で処理を実行する仮想アナライザのリスクレベルが決まります。詳細については、[93 ページの「仮想アナライザのリスクレベルと InterScan MSS のセキュリティレベルの設定」](#)を参照してください。

使用できるセキュリティレベル設定は、[高]、[中]、および [低] です。セキュリティレベルは [低] に設定することをお勧めします。

4. 仮想アナライザの分析の最長時間を設定します。
5. InterScan MSS 管理データベースの接続が切断されたときに実行する処理を、次のいずれかから選択します。
 - ・ 仮想アナライザへのメッセージ送信の停止
 - ・ 仮想アナライザの検索除外に指定された処理の実行
6. 仮想アナライザのプロキシサーバの設定を行います。
 - ・ プロキシサーバ
 - ・ プロキシサーバポート
 - ・ ユーザ名
 - ・ パスワード

**注意**

InterScan MSS では、HTTP プロキシのみをサポートします。

7. [保存] をクリックします。

**注意**

InterScan MSS では、仮想アナライザが有効または完全な分析結果を返せない場合に通知を送信することができます。通知の詳細については、[411 ページの通知](#)を参照してください。

仮想アナライザサーバを追加する

負荷分散とフェイルオーバー機能をさらに効率化するため、InterScan MSS では仮想アナライザに複数のサーバを追加できます。同じプリファレンスを持つサーバに対してはラウンドロビンアルゴリズムが使用されます。

仮想アナライザサーバは InterScan MSS 管理コンソールで有効化、無効化、および削除できます。

手順

1. [ポリシー] > [仮想アナライザ] の順に選択します。
[仮想アナライザの設定] タブが初期設定で表示されます。
2. [サーバ管理] タブをクリックします。
3. [追加] をクリックします。

仮想アナライザ

[サーバ管理] > [サーバの追加]

仮想アナライザサーバ

☐ 有効

サーバ: 例: server.us.trendnet.orgまたは10.1.1.1

ポート: 443

APIキー:

プリファレンス: 10

保存 キャンセル

4. [有効] チェックボックスをオンにします。
5. サーバの完全修飾ドメイン名または IP アドレス、ポート番号、API キー、およびプリファレンス値を指定します。



注意

プリファレンスは、仮想アナライザの優先度を表します。プリファレンス値が低いほど優先度は高くなります。

6. [保存] をクリックします。
-

第 7 章

Trend Micro Email Encryption の導入

この章では、主に Trend Micro Email Encryption について、また InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) で Trend Micro Email Encryption を使用する方法について説明します。

この章の内容は次のとおりです。

- ・ 100 ページの「Trend Micro Email Encryption について」
- ・ 101 ページの「Trend Micro Email Encryption を使用する」
- ・ 101 ページの「Trend Micro Email Encryption を登録する」
- ・ 102 ページの「ドメインを管理する」
- ・ 103 ページの「ドメインを登録する」

Trend Micro Email Encryption について

Trend Micro Email Encryption は、ID ベース暗号 (IBE) を使用してメッセージを暗号化します。たとえば、個人情報を含むメッセージを user1@a.com から user2@b.com に送信するとします。ドメイン a.com は、暗号化および復号化を行うために InterScan MSS に登録されています。ポリシールールにより個人情報を含む送信メッセージの暗号化が有効になっているため、InterScan MSS では、この user2@b.com 宛てのメッセージが暗号化されます。

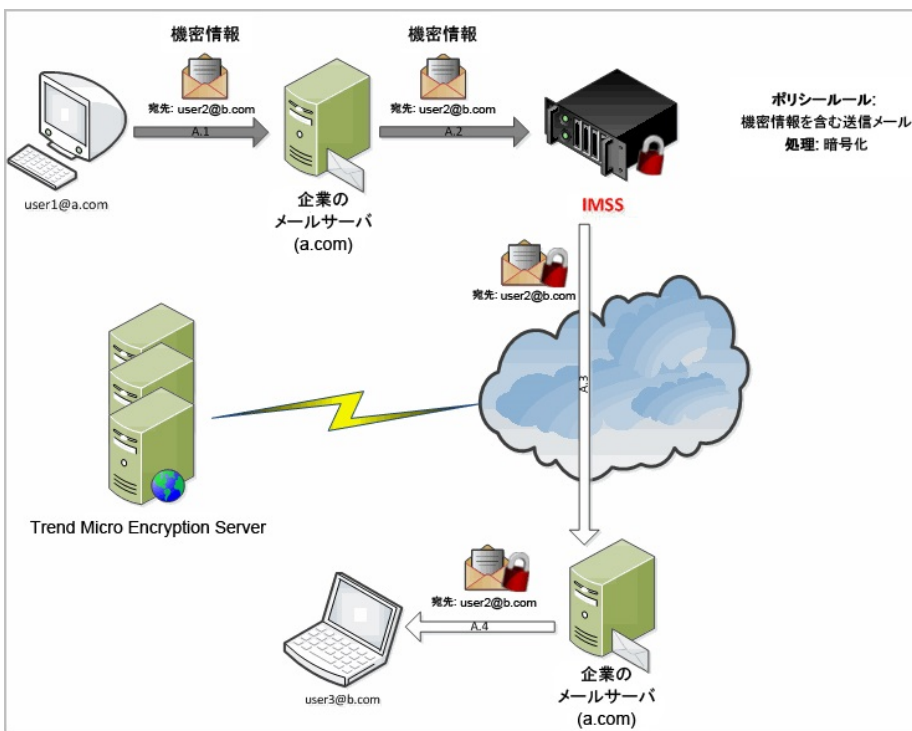


図 7-1. InterScan MSS でのメール暗号化



ヒント

Trend Micro Email Encryption を使用する前に、InterScan MSS で NTP サーバを使用することをお勧めします。これにより、InterScan MSS に対する標準的な日付と時刻のデータが確保されます。

Trend Micro Email Encryption を使用する

Trend Micro Email Encryption を使用するには、次の手順を実行する必要があります。

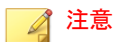
- ・ 手順 1: InterScan MSS を暗号化サービスに登録します (101 ページの「[Trend Micro Email Encryption を登録する](#)」を参照)。
- ・ 手順 2: ドメインを暗号化サービスに登録します (103 ページの「[ドメインを登録する](#)」を参照)。
- ・ 手順 3: メッセージを暗号化するためのポリシーを設定します (260 ページの「[ポリシーを追加する](#)」を参照)。

Trend Micro Email Encryption を登録する

Trend Micro Email Encryption テクノロジーでメッセージを暗号化するには、InterScan MSS を Trend Micro Email Encryption Server に登録する必要があります。

手順

1. [ポリシー] > [暗号化設定] の順に選択します。
[Trend Micro Email Encryption の登録] 画面が表示されます。
2. 連絡先情報を入力します。



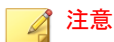
連絡先情報で入力するメールアドレスは、ドメインを Trend Micro Email Encryption Server へ登録するときに重要になります。指定したメールアドレスにキーファイルが送信されます。キーファイルをアップロードしてドメインの所有権処理を完了します。

Trend Micro Email Encryption Server チームは、このメールアドレスを使用して連絡を行います。このメールアドレスは、キーファイルと通知の送信のみに使用されます。この連絡先メールアドレスが、セールスの目的で使用されることはありません。

少なくとも 1 つのドメインを正常に登録している場合を除き、連絡先情報を変更することはできません。

3. [次へ] をクリックします。

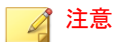
入力した連絡先情報が、Trend Micro Email Encryption Server に送信されます。



ドメインの所有権の検証が完了したことについて通知されるまで、1~2 営業日かかる場合があります。3 営業日以内にメッセージが送付されない場合は、販売代理店にお問い合わせください。

次に進む前に

連絡先情報を変更するには、[ゲートウェイ情報] タブで [変更] をクリックします。



少なくとも 1 つのドメインが正常に登録されるまで [変更] ボタンは有効になりません。

ドメインを管理する

管理者は、[ドメインの管理] タブで InterScan MSS のメール暗号化機能を使用する新しいドメインを登録できます。ドメインを暗号化サービスに登録する

と、そのドメインのメールアドレスに対する秘密鍵の入手が許可されます。たとえば、mycompany.org を登録するとします。暗号化サービスへの登録が承認され、完了すると、InterScan MSS は、user01@mycompany.org、user02@mycompany.org などに対するメールを復号化するための秘密鍵を入手できるようになります。InterScan MSS のドメイン登録を許可するセキュリティの処理およびチェックでは、ドメインの登録者に連絡する場合があるため、公開された情報もチェックされます。

**注意**

セキュリティ上の理由により、ドメインの登録済み所有者の名義人には、登録チームより InterScan MSS の登録を検証するために確認の連絡があります。したがって、ドメインを登録するには、そのドメイン名の所有者となるか、ドメイン名の所有者より許可を得ている必要があります。

ドメインは、ドメインの横の [削除] リンクを選択することで InterScan MSS から削除できます。これにより、暗号化サービスのデータベースから登録情報が削除され、このドメインのメールアドレス用の秘密鍵を入手できなくなります。

ドメインを登録する

Trend Micro Email Encryption Server にドメインを登録すると、ドメインの所有権を確認するために、次のメールアドレスにメッセージが送信されます。

- ・ postmaster@<ドメイン>
- ・ webmaster@<ドメイン>
- ・ ドメインの WHOIS 検索で返されるメールアドレス

**警告!**

ドメインを登録する前に、ドメインのメール管理者および Web 管理者のアカウントを作成して有効にしておく必要があります。

対象ドメインが存在すること、および postmaster@<ドメイン>と webmaster@<ドメイン>の両アカウントが存在して有効化されていることを確

認するメッセージが、トレンドマイクロから「連絡先情報」のメールアドレスに送信されます。

**警告!**

次のいずれかのメールアドレスから確認メッセージに返答する必要があります。

- ・ postmaster@<ドメイン>
- ・ webmaster@<ドメイン>
- ・ ドメインの WHOIS 検索で返されるメールアドレス

設計上の仕様により、ドメインの登録後、再登録することができません。ドメインが登録済みの場合、その後の再登録では「ドメインは既に登録済みです」というエラーが発生します。この制限はセキュリティ上の目的で設定されています。InterScan MSS を再インストールする必要がある場合は、再インストール前にデータベースをバックアップし、後から復元してください。これにより、再インストール後に InterScan MSS および同じドメインを再登録する必要がなくなります。

**注意**

ドメインを登録するには、その前に InterScan MSS を暗号化サービスに登録する必要があります。

ドメインの初期設定の送信者アドレスは、postmaster@<ドメイン>のようになります。初期設定の送信者アドレスは、[暗号化設定] 画面でカスタマイズできます。

初期設定の送信者アドレスが使用されるのは、InterScan MSS がメッセージを暗号化しようとしたとき、そのドメインがドメインリストにない場合です。InterScan MSS はこのメッセージを初期設定の送信者アドレスで署名します。

ドメインを暗号化サービスに登録する

手順

1. [ポリシー] > [暗号化設定] 画面に移動します。

2. [ドメイン] タブをクリックします。
3. [追加] をクリックします。
4. 保護するドメインをドメインリストに追加します。

ドメインは手動で入力するか、既存のドメインのリストから選択できます。ドメインは最大 10 エントリを一度に追加できます。

**注意**

ドメインとそのサブドメインは、個別のエントリとして処理されます。サブドメインは、ドメインリストに別途追加する必要があります。

サブドメインを含めるためにワイルドカードを使用することはできません。

LDAP グループ (「LDAP」で始まるエントリ) は、ドメインリストに追加できません。

5. [保存] をクリックします。

ドメイン情報が Trend Micro Email Encryption Server へ送信されているときに進行状況バーが表示されます。ドメイン情報が Trend Micro Encryption Server で受信されたかどうかを確認する画面が表示されます。

6. 認証キーファイルを受信したら、その後の手順についての指示を読みます。
7. [完了] をクリックします。

ドメインが、[ドメイン] タブの [ドメイン] リストと、[ドメイン] タブに関するメッセージに表示されます。

8. ドメインの登録済み所有者の場合は、Trend Micro Encryption Server からの確認メッセージに返信します。このメッセージは postmaster@<ドメイン> および webmaster@<ドメイン> に送信されます。ドメインが承認された場合は、ドメインの所有権の認証キーファイルが送付されます。確認メッセージに返信して、ドメインの所有者であることを証明する必要があります。



注意

ドメインを暗号化サービスに登録するためのキーファイルが送信されるまで、1～2 営業日かかる場合があります。キーファイルは、登録したドメインごとに送付されます。

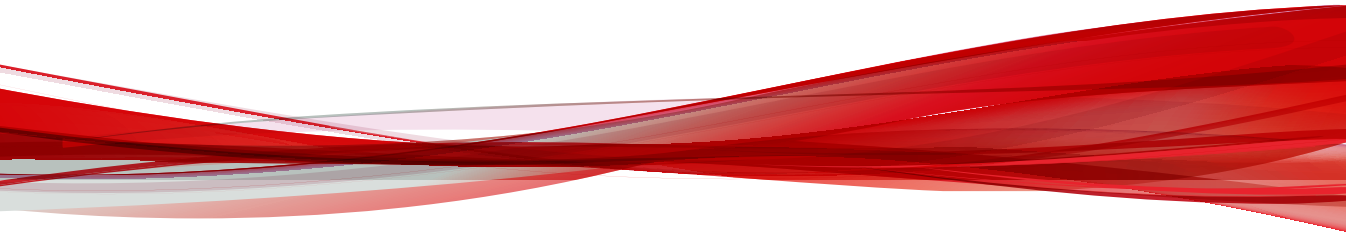
3 営業日以内にメッセージが送付されない場合は、販売代理店にお問い合わせください。

-
9. キーファイルが送付されたら、安全な場所に保存してください。
 10. [暗号化設定] 画面に移動します。
 11. [参照] をクリックして、キーを検索します。
 12. [アップロード] をクリックします。

登録が正常に完了すると確認メッセージが表示されます。

パート II

InterScan MSS の設定



第 8 章

クラウドプレフィルタの設定

この章では、クラウドプレフィルタを設定する方法について説明します。

この章の内容は次のとおりです。

- ・ 110 ページの「クラウドプレフィルタポリシーについて」
- ・ 112 ページの「クラウドプレフィルタポリシーを作成する」
- ・ 122 ページの「クラウドプレフィルタの動作を確認する」
- ・ 122 ページの「DNS の MX レコードを設定する」
- ・ 123 ページの「クラウドプレフィルタを使用する際に推奨される InterScan MSS の設定」
- ・ 125 ページの「クラウドプレフィルタを無効にする」

クラウドプレフィルタポリシーについて

クラウドプレフィルタサービスでは、メールセキュリティに対し、ポリシーベースの管理を提供します。ドメインにポリシーを適用することで、そのドメインに送信されるメッセージに対して各フィルタが適用される方法を定義します。

次の表に、各ポリシーを定義する情報を示します。

表 8-1. クラウドプレフィルタポリシー

セクション	説明
ドメイン	ポリシーの適用対象となるドメインです。適切なルーティング設定により、このドメインに対するすべてのメッセージがクラウドプレフィルタによって保護されます。 各ドメインは一意である必要があり、1つのドメインに対して1つのポリシーのみを適用できます。
有効な受信者	この設定は、LDAP サーバのユーザのリストと、クラウドプレフィルタのユーザのリストを比較することによって機能します。ユーザのクラウドプレフィルタリストは、LDAP サーバとの同期によって生成されます。 有効な受信者チェックを使用して、使用しているドメインに受信者がいないすべてのメッセージをブロックします。これにより、不正なメッセージやスパムメールがネットワークに到達するのを防ぐことができます。
フィルタ設定	次のクラウドプレフィルタのフィルタオプションを定義します。 ・ フィルタを有効化するかどうか ・ 各フィルタ条件がどのように適用されるか (選択できる場合) ・ どのフィルタ処理が実行されるか (選択できる場合)
送信先サーバ	送信先サーバとは、ドメインの受信メールサーバです。ドメイン宛てのメッセージは、クラウドプレフィルタサービスによって処理された後、これらのサーバで受信されます。

セクション	説明
承認済み送信者とブロックする送信者	- 承認済み送信者: 承認済み送信者からのメッセージは、メールレピュテーションサービスやスパムメール対策フィルタをバイパスします。 - ブロックする送信者: ブロックする送信者からのメッセージは即座にブロックされ、ネットワークには到達しません。

**注意**

クラウドプレフィルタのポリシーを作成する際には、ローカルの InterScan MSS の設定と同期をとりながらも、InterScan MSS より厳しくないポリシーを作成することを推奨します。重複したポリシーを使用することで、万が一クラウドプレフィルタが使用不能になった場合でもビジネスを保護できます。

考慮事項

- 各ポリシーは1つのドメインにのみ適用され、各ドメインに対して1つのポリシーのみ作成できます。
- 1つのポリシーは、ドメイン、フィルタ設定、承認済み送信者リストとブロックする送信者リスト、および送信先サーバによって構成されます。
- 各フィルタタイプを確認して、ポリシーを保存する前に、それをドメインに適用するかどうかを診断します。次のフィルタは初期設定で有効にされています。
 - メールレピュテーション
 - ウイルス対策
 - スパムメール対策

**ヒント**

ウイルス対策フィルタとスパムメール対策フィルタを有効にして、適切に設定することをお勧めします。これらのフィルタがないと、ドメインは大量のスパムメールや感染メッセージに対して非常に脆弱になります。

クラウドプレフィルタポリシーを作成する

ドメインにメールセキュリティサービスを提供するには、そのドメインに対してポリシーを作成します。



注意

ネットワークでプロキシサーバを使用する場合は、クラウドプレフィルタポリシーを作成する前に、[管理] > [プロキシ] でプロキシ設定が正しいことを確認してください。

クラウドプレフィルタポリシーを作成するには、次の手順を実行します。

- ・ 112 ページの「手順 1: ドメインを設定する」
- ・ 115 ページの「手順 2: 条件を設定する」
- ・ 119 ページの「手順 3: フィルタを設定する」

手順 1: ドメインを設定する

手順

1. [クラウドプレフィルタ] をクリックします。

[クラウドプレフィルタポリシーリスト] 画面が表示されます。

追加

削除

1-1 / 1

◀

 ページ 1

▶

☐ ドメイン ▲	メールレピュテーション	ウイルス対策	スパムメール対策
☐ example3.com	詳細		

追加

削除

1-1 / 1

◀

 ページ 1

▶

15件/ページ

▼

2. [追加] をクリックします。

[手順 1: ドメインと送信先サーバの指定] 画面が表示されます。

ポリシーの追加



[ポリシーリスト](#) > 新しいポリシー

▶ **手順1: ドメインと送信先サーバの指定** >>> 手順2 >>> 手順3

[戻る](#) [次へ>](#) [キャンセル](#)

ドメインの指定			
ドメイン名*:			
	例: example.com		
受信サーバのアドレス			
クラウドプレフィルタにポリシーが保存されると、このドメインのクラウドプレフィルタの受信サーバアドレスがここに表示されます。 このドメインのMXレコードを、クラウドプレフィルタの受信サーバアドレスに変更してください。MXレコードを変更すると、このドメインに送信されるすべてのメールメッセージがクラウドプレフィルタによって処理され、指定した送信先サーバに送信されるようになります。			
送信先サーバの指定			
追加	削除	インポート	エクスポート
☐	アドレスの種類	アドレス	ポート番号 優先度 ▲
戻る 次へ> キャンセル			

3. 保護するドメインの名前を指定します。



注意

ドメインまたはサブドメインを指定します。たとえば「example.com」や「*.example.com」のように入力します。トップレベルドメインは指定できません。サブドメインの一致は単一レベルのみサポートされます。

4. [送信先サーバの指定] で [追加] をクリックします。

[送信先サーバの追加] 画面が表示されます。

送信先サーバ 

新しいポリシー > 送信先サーバの追加

アドレスの種類: IPアドレス ▼

アドレス*:

ポート番号*:

優先度*: 

新しい送信先サーバの優先度を決定するときには、リスト内の既存サーバを確認してください。

アドレスの種類	アドレス	ポート番号	優先度 ▲
追加 キャンセル			

5. ポリシーの作成時に、実際の送信先サーバを指定して、クラウドプレフィルタが処理後にそれらのサーバにメッセージを配信できるようにします。
 - a. [アドレスの種類] ドロップダウンリストから、次のいずれかを選択します。
 - ・ IP アドレス: クラウドプレフィルタからメッセージを受信する MTA または InterScan MSS の IP アドレス
 - ・ A レコード: クラウドプレフィルタが DNS 検索に使用するホスト名
 - ・ MX レコード: クラウドプレフィルタが DNS 検索に使用する MX (Mail Exchange) レコード



注意

1 つのポリシーには、送信先サーバのアドレスの種類を 1 つのみ含めることができます。IP アドレスと A レコードは同じ種類であると見なされます。MX レコードは異なる種類であると見なされます。

- b. [アドレス] フィールドに InterScan MSS のアドレスを指定します。

- c. クラウドプレフィルタで処理されたメッセージを受信する InterScan MSS のポート番号を指定します。初期設定値はポート 25 です。
- d. 送信先サーバの [優先度] の値を指定します。

[優先度] オプションでは、送信先サーバのルーティングの優先度が指定されます。クラウドプレフィルタサービスは、より優先度の高いサーバに、最初にメッセージのルーティングを試行します。数値が低いほど優先度が高くなります。

[MX レコード] 送信先サーバに優先度を指定する必要はありません。MX レコードの優先度は自動的に解決されます。

6. [追加] をクリックします。

送信先サーバリストに InterScan MSS の詳細が記載された、[手順 1: ドメインと送信先サーバの指定] 画面が表示されます。

手順 2: 条件を設定する

承認済み送信者とブロックする送信者

承認済み送信者からのメッセージはメールレピュテーションサービスやスパムメール対策フィルタをバイパスできるのに対して、ブロックする送信者からのメッセージは受信者に到達できません。

IP アドレスを指定すると、その IP アドレスからのすべてのメッセージをブロックまたは承認できます。

承認済み送信者リストは、ブロックする送信者リスト、メールレピュテーションフィルタ、およびスパムメール対策フィルタより優先されます。承認済み送信者リスト内のアドレスに一致するアドレスからのすべてのメッセージは、これらのフィルタで処理されません。



注意

メールレピュテーション、IP プロファイラ、またはスパムメール判定ルールの承認済みリストを、クラウドプレフィルタの承認済みリストにインポートできます。

有効な受信者

この機能は、LDAP サーバのユーザのリストと、クラウドプレフィルタのユーザのリストを比較することによって機能します。ユーザのクラウドプレフィルタリストは、LDAP サーバとの同期によって生成されます。

有効な受信者チェックを使用して、使用しているドメインに受信者がいないすべてのメッセージをブロックします。これにより、不正なメッセージやスパムメールがネットワークに到達するのを防ぐことができます。



ヒント

すべての有効なメッセージがネットワークに確実に到達するように、予約同期を有効にすることをお勧めします。有効な受信者のチェックや予約同期を使用するには、事前に LDAP サーバを設定する必要があります。

手順

1. [次へ] をクリックします。

[手順 2: 送信者の条件の指定] 画面が表示されます。

ポリシーの追加



ポリシーリスト > 新しいポリシー

手順1 >>> **手順2: 送信者の条件の指定** >>> 手順3

[< 戻る](#) [次へ >](#) [キャンセル](#)

承認済み送信者リスト	
追加 削除 インポート エクスポート	0-0 / 0 0 < ページ 1 >
☐ アドレス	
承認済み送信者リストが空です	
追加 削除 インポート エクスポート	0-0 / 0 0 < ページ 1 >
15件/ページ	
ブロックする送信者リスト	
追加 削除 インポート エクスポート	0-0 / 0 0 < ページ 1 >
☐ アドレス	
ブロックする送信者リストが空です	
追加 削除 インポート エクスポート	0-0 / 0 0 < ページ 1 >
15件/ページ	
有効な受信者	
☐ 有効な受信者のチェックを有効にする	
定期メンテナンス:	☐ LDAPサーバとクラウドプレフィルタを毎日同期する ⓘ
手動メンテナンス:	今すぐ同期
受信者が有効であることを確認してください。	

[< 戻る](#) [次へ >](#) [キャンセル](#)

2. [追加] をクリックしてリストにエントリを追加します。

[承認済み送信者リストの追加] または [ブロックする送信者リストの追加] 画面が表示されます。

承認済み送信者リストの追加

ポリシーの追加 > 承認済み送信者リストの追加

☒ IPアドレス ☐ メールアドレス

メールアドレスまたはワイルドカードのユーザー名を格納します (例: username@domainname, *@domainname).

ブロックする送信者リストの追加

ポリシーの追加 > ブロックする送信者リストの追加

☒ IPアドレス ☐ メールアドレス

メールアドレスまたはワイルドカードのユーザー名を格納します (例: username@domainname, *@domainname).

3. メールアドレスまたは IP アドレスを指定します。
4. [IP アドレス] または [メールアドレス] フィールドの横の [追加] をクリックします。

リストにエントリが表示されます。



警告!

メールアドレスのローカル部 (ローカル部@domain.com) 内の任意の文字列の指定にワイルドカード文字 (*) を使用できます。ワイルドカード文字は、大量のメールアドレスからのメッセージを許可またはブロックする場合があるので、使用する場合は注意が必要です。

5. リストの下で [追加] をクリックします。
指定したリストにエントリが表示されます。
6. 承認済みまたはブロックする送信者リストにエントリをインポートします。

- ・ インポート機能を使用する際は、メールアドレスまたは IP アドレスが 1 行に 1 つのみ記載されたテキストファイルを使用します。
 - ・ 送信者のアドレスをインポートする際は、適切なマージオプションを選択してください。アドレスを置き換えるよう選択すると、リストから既存のアドレスがすべて削除されます。
7. 指定したリストに対して [インポート] をクリックします。
画面が表示されます。
 8. インポートするファイルを指定します。
 9. [インポート] をクリックします。
リストにインポートされたエントリが表示されます。
 10. [有効な受信者のチェックを有効にする] を選択します。
 11. [LDAP サーバとクラウドプレフィルタを毎日同期する] を選択します。

**注意**

すべての有効なメッセージがネットワークに確実に到達するように、予約同期を有効にすることをお勧めします。

アップグレード後はローカル LDAP キャッシュが空になるため、受信者のチェックと予約同期が正常に動作しません。受信者のチェックと予約同期は、LDAP 設定で [保存して同期] をクリックすれば手動で実行できます。

手順 3: フィルタを設定する

[手順 3: フィルタの選択] 画面には、次の 3 つのフィルタの設定が含まれます。

表 8-2. クラウドプレフィルタのフィルタ

フィルタ	説明
メールレピュテーション	メールレピュテーションを使用すると、継続的に更新される動的なメール送信元の評価システムを活用して、スパムメールやその他の不要なメッセージをブロックできます。メールレピュテーションは、現在の評価が良くない送信元 IP アドレスからのメッセージをブロックします。 「メールレピュテーション: 詳細」または「メールレピュテーション: 標準」のいずれかを選択できます。「メールレピュテーション: 標準」は、標準評価データベースに対してクエリを実行します。「メールレピュテーション: 詳細」では、標準評価データベースに加えて、リアルタイムでアップデートされる動的評価データベースに対してクエリを実行します。
ウイルス対策	ウイルス対策フィルタを有効にすると、既知および未知の不正プログラムコードを含むメッセージが (コードが添付ファイルに含まれているか、メッセージの本文に埋め込まれているかに関わりなく) ブロックされます。 不正プログラムコードが検出されたメッセージは、自動的に削除されます。
スパムメール対策	スパムメール対策フィルタを有効にすると、メッセージでスパムメールおよびフィッシングの特性がチェックされます。フィルタは、選択された検出率に基づいて、メッセージをスパムメールとして特定します。 スパムメール対策は、Web レピュテーションおよびスパムメール対策フィルタを使用して、スパムメールがネットワークに侵入するのを防止します。 スパムメール対策フィルタは、スパムメールの検出に次の 2 つの方法を使用します。 ・ スパムメール: この設定では、寛容な検索レベルで検出を行います。「スパムメール」として検出されるほぼすべてのメールは、実際に不要なメッセージです。この設定では、削除または隔離のどちらかの処理を実行します。 ・ スパムメールの可能性のあるメール: この設定では、より強力なセキュリティ設定が適用されます。ただし、「スパムメール」としてマークされるメッセージに、正当なメッセージが含まれている場合があります。この設定では、削除、隔離、または転送のいずれかの処理を実行します。

手順

1. [次へ] をクリックします。

[手順 3: フィルタの選択] 画面が表示されます。

ポリシーの追加



ポリシーリスト > 新しいポリシー

手順1 >>> 手順2 >>> **手順3: フィルタの選択**

[戻る](#) [完了](#) [キャンセル](#)

フィルタの選択		
フィルタの種類	ステータス	処理
メールレピュテーション	詳細	拒否
ウイルス対策	有効	削除
スパムメール対策	有効	削除 (スパムメール) 削除 (スパムメールの可能性のあるメール)

[戻る](#) [完了](#) [キャンセル](#)

2. フィルタのステータスを指定します。
3. フィルタの処理を指定します。

フィルタは次の処理を実行します。

- ・ 削除: 隔離せずにメッセージ全体を削除します。
- ・ 隔離: メッセージ全体のコピーを、ローカルの InterScan MSS 隔離領域に保存します。
管理者は、メッセージを評価した後に削除または配信できます。
- ・ 拒否: 隔離せずにメッセージを拒否します。
- ・ 転送: クラウドプレフィルタでは処理を実行せず、メッセージを直接 InterScan MSS に送信します。その後、InterScan MSS でメッセージが検索されます。

4. [完了] をクリックします。

ドメインの表示された、[クラウドプレフィルタポリシーリスト]が表示されます。フィルタのステータスがドメインとともに表示されます。

クラウドプレフィルタの動作を確認する

ポリシーをアクティベートする前に、ポリシーが正しく機能することを確認できます。

以下に例を示します。

example.com というドメインに対して作成したポリシーがメールトラフィックを正しく処理し、クラウドプレフィルタがメッセージを InterScan MSS にルーティングすることを確認します。

ポリシーが正しく機能することを確認するには、指定された送信者と受信者のアカウント (受信者のドメインは example.com に属している必要があります) を使用して、example.com のクラウドプレフィルタの受信サーバに直接メッセージを送信します。

このポリシーに対するサンプルのクラウドプレフィルタの受信サーバアドレスは、im.emailsecurity.trendmicro.com です。

受信サーバアドレスにテストメッセージを送信します。

メールメッセージの送信後、数分待ってから、メッセージ追跡ログの[クラウドプレフィルタと IMSS のデータ]を使用して、クエリを実行します。



注意

テストメッセージは、ドメインに対するクラウドプレフィルタの受信サーバに直接送信される必要があります。受信サーバのアドレスは、ポリシーの [ドメイン] タブに表示されます。

DNS の MX レコードを設定する

クラウドプレフィルタを設定し、メールトラフィックがクラウドプレフィルタから InterScan MSS に配信されることを確認したら、クラウドプレフィルタ

の [受信サーバのアドレス] を DNS サーバの MX レコードに追加します。クラウドプレフィルタのホストは、[ドメイン] タブの [受信サーバのアドレス] に表示されます。これが、クラウドプレフィルタを使用してメールトラフィックを検索する前に行う手順の最後です。

**警告!**

メールトラフィックをクラウドプレフィルタ経由でルーティングするように、メール配信 (MX) レコードを設定する必要があります。この手順を完了していない場合は、メッセージがローカルサーバに送信され、検索用のクラウドプレフィルタに送信されることはありません。

**ヒント**

クラウドプレフィルタに対する MX レコードは、既存の MX レコードよりも高い優先度 (より低い数値を指定) で設定することをお勧めします。これにより、既存の MX レコードがクラウドプレフィルタへのバックアップとして機能します。

クラウドプレフィルタを使用する際に推奨される InterScan MSS の設定

クラウドプレフィルタは、ポート 9000 を Web サービスの待機ポートとして使用します。InterScan MSS でクラウドプレフィルタに接続するには、ファイアウォールでこのポートが開かれている必要があります。

クラウドプレフィルタが InterScan MSS の配置に影響することはありませんが、InterScan MSS の設定方法には影響します。

表 8-3. クラウドプレフィルタを使用する際に推奨される InterScan MSS の設定

セキュリティサービス	推奨処理
送信者フィルタ (メールレピュテーションと IP プロファイラ)	クラウドプレフィルタですべてのドメインのメッセージをフィルタする場合: 送信者フィルタを無効にする、またはアクティベートしない クラウドプレフィルタでは、メールレピュテーションを使用して、メッセージがネットワークに到達する前にすべてのメッセージをフィルタします。このため、送信者フィルタ (メールレピュテーションと IP プロファイラ) の使用が冗長になります。 クラウドプレフィルタで一部のドメインのメッセージをフィルタする場合: 送信者フィルタ (メールレピュテーションと IP プロファイラ) を有効にして使用する クラウドプレフィルタでは、メールレピュテーションを使用して、メッセージがネットワークに到達する前にすべてのメッセージをフィルタしていません。クラウドプレフィルタ経由でルーティングされていないドメインからのメッセージは、依然として不正なメッセージである可能性があります。
スパムメール対策 (コンテンツ検索)	InterScan MSS では常にスパムメール対策を使用してください。つまり、スパムメール対策ポリシーを有効にして使用する必要があります。 クラウドプレフィルタでは、寛容な検索レベルでスパムメールの検出を行います。これは正当なメッセージがスパムメールとして誤検出されるリスクを下げるためです。 InterScan MSS でスパムメール対策ポリシーを使用することで、メール受信者に到達するスパムメールをさらに減らすことができます。

セキュリティサービス	推奨処理
トレンドマイクロのウイルス対策とコンテンツフィルタ	InterScan MSS では常にウイルス対策とコンテンツフィルタを使用してください。つまり、ウイルス対策ポリシーとコンテンツフィルタポリシーを有効にして使用する必要があります。 クラウドプレフィルタでは、メッセージのコンテンツフィルタをサポートしていません。コンテンツフィルタポリシーは、InterScan MSS で作成される必要があります。 また、クラウドプレフィルタでウイルスをフィルタする場合でも、ウイルス対策ポリシーを作成することをお勧めします。
DKIM	クラウドプレフィルタは、DKIM には影響を与えません。 ネットワークの必要に応じて、この機能を設定して使用してください。
Transport Layer Security (TLS)	クラウドプレフィルタは TLS をサポートしています。 クラウドプレフィルタにメッセージを送信する MTA で TLS をサポートしている場合、メッセージは TLS を使用して配信されます。 TLS を使用した受信サーバからのメッセージがクラウドプレフィルタに到達すると、クラウドプレフィルタは TLS を使用してそのメッセージを送信先サーバに配信します。送信先サーバが TLS をサポートしていない場合、メッセージは SMTP を介して配信されます。 TLS を使用しない受信サーバからのメッセージがクラウドプレフィルタに到達すると、クラウドプレフィルタは SMTP を介してそのメッセージを送信先サーバに配信します。

クラウドプレフィルタを無効にする

InterScan MSS の管理コンソールからクラウドプレフィルタを無効にすることはできません。クラウドプレフィルタを無効にする唯一の方法は、ドメインの DNS の MX レコードを変更して、InterScan MSS または MTA (その後 InterScan MSS) がポイントされるようにすることです。

第 9 章

送信者フィルタの設定

この章では、InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) を稼働させるために必要なさまざまな設定について説明します。

内容は次のとおりです。

- ・ 128 ページの「IP フィルタサービス」
- ・ 128 ページの「メールレピュテーション管理コンソールを使用する」
- ・ 130 ページの「送信者フィルタを設定する」
- ・ 143 ページの「不審 IP アドレスおよびドメインを表示する」

IP フィルタサービス

送信者フィルタサービスには、メールレピュテーションと IP プロファイラという、2つの独立したコンポーネントがあります。

- ・ メールレピュテーションは、SMTP セッションの確立時にスパムメール送信者からの接続をフィルタします。
- ・ IP プロファイラは、高度なプロファイル (SMTP IDS) を使用してメールサーバを攻撃から保護します。



ヒント

メッセージングインフラストラクチャの最前線の防御として、送信者フィルタのインストールをお勧めします。

メールシステムには、通常、既存の IP アドレスブロック機能、スパムメールフィルタ機能、ウイルスフィルタ機能などの多層構造が備わっていることがほとんどですが、他の IP アドレスブロック機能はメッセージング環境から削除することをお勧めします。送信者フィルタは、使用されるすべてのアプリケーションフィルタ機能よりも先行して動作する必要があります。



注意

送信者フィルタは、IPv4 ネットワークからのみ使用できます。IPv6 ネットワークからの受信メールメッセージは、メールレピュテーションや IP プロファイラではブロックされません。

メールレピュテーション管理コンソールを使用する

トレンドマイクロでは、既知のスパムメール送信者の IP アドレスリストを中央データベースで管理しています。メールレピュテーションは、このデータベース内に保存された IP アドレスをブロックすることでスパムメールをフィルタします。

メールレピュテーションサービスで使用するために MTA を準備する

契約されているメールレピュテーションの種類に適切な DNS クエリを実行するよう、MTA を設定します。

- ・ 標準: 標準評価データベースへ DNS クエリを実行するよう MTA を設定します。このデータベースへ登録されている IP アドレスから接続があった場合は、永続的に拒否する 550 エラー応答 (「Connection refused」) を返します。標準評価データベースには、既知のスパムメール送信者の IP アドレスが登録されています。
- ・ 詳細: 2 種類の DNS クエリを実行するよう MTA を設定します。MTA で、標準評価データベースへの最初のクエリから応答を受信しない場合、動的評価データベースへの 2 番目のクエリを実行します。このデータベースから応答が受信された場合、MTA は接続を一時的に拒否する 450 レベルエラーコード (「server temporarily unavailable, please retry」) を返します。

動的評価データベースには、一時的にスパムメールを送信する危険にさらされた正規のメールサーバが登録される可能性があります。接続要求が正規のメールサーバからのものである場合、それは再度キューに入り、後でメッセージの送信を試行します。この処理により、そのリストの期限が切れるまでメールの配信が少し遅れますが、そのメールがブロックされ続けることはありません。

一部のサーバでは、不審 IP 接続を処理する際に追加のオプションを設定できます。これらのオプションには、より詳細な検索のためにメッセージを絞り込んだり、ルーティングすることが含まれます。



注意

手順のテキスト例を置き換えるには、アクティベーションコードを挿入してください。ダッシュは含めないでください。

メールレピュテーション管理コンソールを使用する

<https://ers.trendmicro.com/> にアクセスしてメールレピュテーション管理コンソールにログオンし、グローバルスパムメール情報へのアクセス、レポート

の表示、メールレピュテーション設定の管理、および管理タスクを実行します。

詳細な手順については、メールレピュテーション管理コンソールのオンラインヘルプを参照してください。ヘルプ画面の右上隅にあるヘルプアイコンをクリックして、オンラインヘルプにアクセスします。

送信者フィルタを設定する

送信者フィルタを設定するには、次の手順を実行します。

1. [130 ページの「メールレピュテーションおよび IP プロファイラを有効にする」](#)
2. [131 ページの「承認済みリストのレコードを追加する」](#)
3. [132 ページの「ブロックリストのレコードを追加する」](#)
4. [133 ページの「送信者フィルタルールを有効にする」](#)
5. [141 ページの「メールレピュテーションを設定する」](#)

メールレピュテーションおよび IP プロファイラを有効にする

メールレピュテーションと IP プロファイラを有効にして、送信者フィルタ保護を開始します。これらの両方またはどちらかの保護を有効にできます。

手順

1. [送信者フィルタ] > [概要] の順に選択します。

[送信者フィルタの概要] 画面が表示されます。

送信者フィルタの概要


☐ メールレピュテーション
☐ IPプロファイラ
保存

ブロックされたドメイン/IPアドレス
更新
過去1日間 (過去24時間) ▼

DHA攻撃

ドメイン	IPアドレス	破棄された接続数
最近1日間にブロックされたドメインまたはIPアドレスはありません。		

バウンスメール

ドメイン	IPアドレス	破棄された接続数
最近1日間にブロックされたドメインまたはIPアドレスはありません。		

ウイルス

ドメイン	IPアドレス	破棄された接続数
最近1日間にブロックされたドメインまたはIPアドレスはありません。		

スパム

ドメイン	IPアドレス	破棄された接続数
最近1日間にブロックされたドメインまたはIPアドレスはありません。		

ユーザ指定

ドメイン	IPアドレス	破棄された接続数
最近1日間にブロックされたドメインまたはIPアドレスはありません。		

- 必要に応じて [メールレピュテーション] および [IP プロファイラ] チェックボックスをオンにします。
- [保存] をクリックします。

承認済みリストのレコードを追加する

InterScan MSS では、承認済みリストに表示されるホストをフィルタしません。

手順

1. [送信者フィルタ] > [承認済みリスト] の順に選択します。
[承認済みリスト] 画面が表示されます。
2. [追加] をクリックします。
[承認済みリストのレコードを追加] 画面が表示されます。
3. [有効にする] チェックボックスをオンにします。
4. 承認済みリストに追加するホストのドメイン、IP アドレス、またはサブネットアドレスとマスクを指定します。



注意

初期設定では [予約解決] チェックボックスがオンになっています。つまり、InterScan MSS はドメインに関連付けられた A レコードまたは MX レコードを定期的に解決します。

5. [保存] をクリックします。
ホストが [承認済みリスト] に表示されます。
-

ブロックリストのレコードを追加する

InterScan MSS では、ブロックリストに表示されているホストがブロックされます。

手順

1. [送信者フィルタ] > [ブロックリスト] の順に選択します。
[ブロックリスト] 画面が表示されます。
2. [追加] をクリックします。
[ブロックリストのレコードの追加] 画面が表示されます。

3. [有効にする] チェックボックスをオンにします。
 4. ブロックリストに追加するホストのドメイン、IP アドレス、またはサブネットアドレスとマスクを指定します。
 5. [一時的にブロック] または [常にブロック] を選択します。
 6. (オプション) [一時的にブロック] を選択する場合は、ブロック期間を指定します。
 7. [保存] をクリックします。
- ホストが [ブロックリスト] に表示されます。
-

送信者フィルタルールを有効にする

すべての送信者アドレスの動作を監視し、しきい値の設定に従ってブロックするルールが設定されます。ルールは次のように設定できます。

- ・ スпамメール
- ・ ウイルス
- ・ DHA 攻撃
- ・ バウンスメール



警告!

送信者フィルタのルールを有効にする前に、すべてのメールサーバの IP アドレス (InterScan MSS に送信メッセージを送信する) を送信者フィルタ承認済みリストに追加します。送信者フィルタ承認済みリストを設定するには、[131 ページの「承認済みリストのレコードを追加する」](#)を参照してください。

送信者フィルタスパム設定を指定する

手順

1. [送信者フィルタ] > [ルール] の順に選択します。

[ルール] 画面には、脅威の種類ごとに4つのタブがあります。

ルール: IPファイア設定 (IPの挙動監視)



すべてのIPアドレスの動作を監視し、しきい値の設定に従ってブロックするルールが設定されます。

スパムメール	ウイルス	DHA攻撃	バウンスメール
☐ 有効にする			
監視期間:	20	時間	
比率 (%):	80	%	
メッセージ総数:	1000		
処理:	一時的にブロック ▼		
ブロック期間:	30	分	
保存 キャンセル 既定値に戻す			

2. [スパムメール] タブをクリックします。
[スパムメール] 画面が表示されます。
3. スパムメールのブロックを有効にするには、[有効にする] チェックボックスをオンにします。
4. 次の項目に対する値を指定します。
 - ・ 監視期間: スパムメッセージの割合が設定するしきい値を超えていないかどうかについて、InterScan MSS がトラフィックを監視する時間数。
 - ・ 比率 (%): スパムメッセージについて許可する割合。
 - ・ メッセージ総数: しきい値の割合が算出されるスパムメッセージの総数。

次の例で考えます。

監視期間: 1 時間、比率: 20、メッセージ総数: 100。

スパムメールのブロックが有効に設定された 1 時間単位の期間で、受信したメッセージの 20%を超えるメッセージがスパムメールであり、かつメッセージの総数が 100 を超える場合に、InterScan MSS は配信元 (IP) アドレスによるブロックを開始します。

5. [処理] で次のいずれかを選択します。
 - ・ 一時的にブロック: その IP アドレスからのメッセージを一時的にブロックし、ブロック期間終了後にアップストリーム MTA からの再試行を許可します。
 - ・ 常にブロック: その IP アドレスからの今後のメッセージを永続的にブロックします。アップストリーム MTA は再試行を実行できません。
 6. (オプション) [一時的にブロック] を選択する場合は、ブロック期間を指定します。
 7. [保存] をクリックします。
-

送信者フィルタウイルス設定を指定する

手順

1. [送信者フィルタ] > [ルール] の順に選択します。

[ルール] 画面には、脅威の種類ごとに 4 つのタブがあります。

ルール: IPファイア設定 (IPの挙動監視)



すべてのIPアドレスの動作を監視し、しきい値の設定に従ってブロックするルールが設定されます。

スパムメール	ウイルス	DHA攻撃	バウンスメール
☐ 有効にする			
監視期間:		20	時間
比率 (%):		80	%
メッセージ総数:		1000	
処理:		一時的にブロック ▼	
ブロック期間:		30	分
保存 キャンセル 既定値に戻す			

- [ウイルス] タブをクリックします。
[ウイルス] 画面が表示されます。
- ウイルスのブロックを有効にするには、[有効にする] チェックボックスをオンにします。
- 次の項目を設定します。
 - 監視期間: ウイルスを含むメッセージの割合が設定するしきい値を超えていないかどうかについて、InterScan MSS がメールトラフィックを監視する時間数。
 - 比率 (%): ウイルスを含むメッセージについて許可する割合 (分子)。
 - メッセージ総数: しきい値の割合が算出される感染メッセージの総数 (分母)。

次の例で考えます。

監視期間: 1 時間、比率: 20、メッセージ総数: 100。

ウイルスのブロックが有効に設定された 1 時間単位の期間で、受信したメッセージの 20%を超えるメッセージにウイルスが含まれ、かつメッセージの総数が 100 を超える場合に、InterScan MSS は配信元 (IP) アドレスによるブロックを開始します。

5. [処理] で次のいずれかを選択します。
 - ・ 一時的にブロック: その IP アドレスからのメッセージを一時的にブロックし、ブロック期間終了後にアップストリーム MTA からの再試行を許可します。
 - ・ 常にブロック: その IP アドレスからの今後のメッセージを永続的にブロックします。アップストリーム MTA は再試行を実行できません。
 6. (オプション) [一時的にブロック] を選択する場合は、ブロック期間を指定します。
 7. [保存] をクリックします。
-

送信者フィルタディレクトリハーベスト攻撃 (DHA) 設定を指定する

手順

1. [送信者フィルタ] > [ルール] の順に選択します。
[ルール] 画面には、脅威の種類ごとに 4 つのタブがあります。
2. [DHA 攻撃] タブをクリックします。

[DHA 攻撃] 画面が表示されます。

ルール: IPプロファイラ設定 (IPの挙動監視)



すべてのIPアドレスの動作を監視し、しきい値の設定に従ってブロックするルールが設定されます。

スパムメール	ウイルス	DHA攻撃	バウンスメール
☐ 有効にする			
監視期間:		20	時間
比率 (%):		80	%
メッセージ総数:		1000	
送信先数の下限:		100	
存在しない受信者数:		0	(LDAPサービスが実行中の場合)
処理:		一時的にブロック ▼	
ブロック期間:		30	分

保存 キャンセル 既定値に戻す

- DHA 攻撃のブロックを有効にするには、[有効にする] チェックボックスをオンにします。
- 次の項目を設定します。
 - 監視期間: DHA 攻撃を示すメッセージの割合が設定するしきい値を超えていないかどうかについて、InterScan MSS がメールトラフィックを監視する時間数。
 - 比率 (%): DHA 脅威を含むメッセージについて許可する割合 (分子)。
 - メッセージ総数: しきい値の割合が算出される DHA メッセージの総数 (分母)。
 - 送信先数の下限: しきい値として可能な受信者の最大数。
 - 存在しない受信者数: しきい値として可能な存在しない受信者の最大数。DHA 攻撃には、受信者リスト内にランダムに生成されたメールアドレスが含まれることがあります。

**注意**

LDAP サービスは存在しない受信者を判断するために実行中であることが必要です。

次の例で考えます。

監視期間: 1 時間、比率: 20、メッセージ総数: 100、送信先数: 10 を超える、存在しない受信者数: 5 を超える

DHA のブロックが有効な間の 1 時間ごとに、11 人以上の受信者 (組織外の受信者 6 人以上を含む) に送信されたメッセージの 20% を超えるメッセージを受信し、かつメッセージの総数が 100 を超える場合に、InterScan MSS は配信元 IP アドレスによるブロックを開始します。

**ヒント**

技術的には、LDAP サーバは必須ではありません。InterScan MSS の DHA ルールは、Postfix から返された DHA の結果も入手できます。Postfix が次にこれらの結果を LDAP サーバ経由またはその他の手段で FoxProxy に渡します。FoxProxy は結果を分析して DHA 攻撃かどうか判断します。

LDAP サーバは、ユーザのメールボックスが存在するかどうかを Postfix が調べる手段の 1 つにすぎません。

5. [処理] で次のいずれかを選択します。
 - ・ 一時的にブロック: その IP アドレスからのメッセージを一時的にブロックし、ブロック期間終了後にアップストリーム MTA からの再試行を許可します。
 - ・ 常にブロック: その IP アドレスからの今後のメッセージを永続的にブロックします。アップストリーム MTA は再試行を実行できません。
6. [保存] をクリックします。

送信者フィルタバウンスメール設定を指定する

手順

1. [送信者フィルタ] > [ルール] の順に選択します。
[ルール] 画面には、脅威の種類ごとに 4 つのタブがあります。
2. [バウンスメール] タブをクリックします。
[バウンスメール] 画面が表示されます。

ルール: IPプロファイラ設定 (IPの挙動監視)



すべてのIPアドレスの動作を監視し、しきい値の設定に従ってブロックするルールが設定されます。

スパムメール	ウイルス	DHA攻撃	バウンスメール
☐ 有効にする			
監視期間:		20	時間
比率 (%):		80	%
メッセージ総数:		1000	
処理:		一時的にブロック ▼	
ブロック期間:		30	分
保存 キャンセル 既定値に戻す			

3. バウンスメールのブロックを有効にするには、[有効にする] チェックボックスをオンにします。
4. 次の項目を設定します。
 - ・ 監視期間: バウンスメールを示すメッセージの割合が設定するしきい値を超えていないかどうかについて、InterScan MSS がメールトラフィックを監視する時間数。
 - ・ 比率 (%): バウンスメールを示すメッセージについて許可する割合 (分子)。
 - ・ メッセージ総数: しきい値の割合が算出されるバウンスメッセージの総数 (分母)。

次の例で考えます。

監視期間: 1 時間、比率: 20、メッセージ総数: 100

バウンスメールのブロックが有効に設定された 1 時間単位の期間で、受信したメッセージの 20%を超えるメッセージがバウンスメッセージであり、かつメッセージの総数が 100 を超える場合に、InterScan MSS は配信元 (IP) アドレスによるブロックを開始します。

**注意**

バウンスメールをチェックするには、LDAP サービスが実行中である必要があります。

5. [処理] で次のいずれかを選択します。
 - ・ 一時的にブロック: その IP アドレスからのメッセージを一時的にブロックし、ブロック期間終了後にアップストリーム MTA からの再試行を許可します。
 - ・ 常にブロック: その IP アドレスからの今後のメッセージを永続的にブロックします。アップストリーム MTA は再試行を実行できません。
 6. (オプション) [一時的にブロック] を選択する場合は、ブロック期間を指定します。
 7. [保存] をクリックします。
-

メールレピュテーションを設定する

メールレピュテーションは、トレンドマイクロのメールレピュテーションデータベースを使用して、受信メッセージの IP アドレスを確認します。

手順

1. [送信者フィルタ] > [メールレピュテーション] の順に選択します。

[メールレピュテーション] 画面が表示されます。

メールレピュテーション



メールレピュテーションでは、新しいスパムメールやフィッシングメールの送信元を特定する動的評価データベースと共に、世界最大の、最も信頼されている評価データベースの一つを使用して、受信メールメッセージのIPアドレスを確認し、ゾンビやボットネットの最初の出現時にそれらが実行されるのを阻止します。

メールレピュテーションの設定	
☐	メールレピュテーションを有効にする
グローバルスパムメール情報およびレポートの表示、送信者IPアドレスの承認済みリストおよびブロックリストの作成または管理、管理タスクの実行、およびサービスの設定。 メールレピュテーションのポータル	
サービスレベルの設定	
☐	標準 標準評価データベースを使用して、既知のスパムメールの送信元から送られたメッセージをブロックします。
☒	初期設定の推奨処理 RBL+ Serviceのデータベースに一致するIPアドレスからの接続を常時拒否 (応答コード: 550)
☐	一致するすべての接続に対して適用する処理 SMTPエラーコード: 550 (範囲 400 ~ 599、初期設定値=550) SMTPエラー文字列: error message
☒	詳細 標準評価データベースと動的評価データベースの両方を使用して、既知のスパムメールの送信元および不審なスパムメールの送信元からのメッセージをブロックします。
☒	初期設定の推奨処理 RBL+ Serviceのデータベースに一致するIPアドレスからの接続を常時拒否 (応答コード: 550) Network Anti-Spam Service (QIL) のデータベースに一致するIPアドレスからの接続を一時拒否 (応答コード: 450)
☐	一致するすべての接続に対して適用する処理 SMTPエラーコード: 450 (範囲 400 ~ 599、初期設定値=450) SMTPエラー文字列: Service unavailable

- [メールレピュテーションを有効にする] チェックボックスをオンにします。
- サービスのレベルに応じて、次のいずれかの横にあるラジオボタンをクリックし、設定を実行します。

標準:

- 初期設定の推奨処理: メールレピュテーションにより、RBL+に一致する接続が常時拒否されます (応答コード: 550)。

- ・ 一致するすべての接続に対して適用する処理:
 - ・ SMTP エラーコード: 特定の SMTP コードを持つ接続をすべてブロックします。SMTP コードを指定します。
 - ・ SMTP エラー文字列: SMTP エラーコードに関連したメッセージを指定します。

詳細:

- ・ 初期設定の推奨処理: メールレピュテーションにより、RBL+に一致する接続が常時拒否 (応答コード: 550) され、QIL に一致する接続が一時的に拒否 (応答コード: 450) されます。
- ・ 一致するすべての接続に対して適用する処理:
 - ・ SMTP エラーコード: 特定の SMTP コードを持つ接続をすべてブロックします。SMTP コードを指定します。
 - ・ SMTP エラー文字列: SMTP エラーコードに関連したメッセージを指定します。



注意

上記の SMTP コードとエラー文字列は、アップストリーム MTA に送信され、エラーコードやエラー文字列をログファイルに記録するなど、事前に設定された必要な処理を実行します。

4. [保存] をクリックします。

不審 IP アドレスおよびドメインを表示する

メッセージの合計数が任意の期間に対して設定されたしきい値を超えていないため、検索条件に違反するメッセージを送信したにもかかわらずブロックされずにいる IP アドレスまたはドメインについて、InterScan MSS はログエントリを作成します。

手順

1. [送信者フィルタ] > [不審な IP] の順に選択します。
 2. 次のいずれかを設定します。
 - ・ [種類] で、IP フィルタで検出された脅威の種類の横にあるチェックボックスをオンにします。
 - ・ [期間] で、InterScan MSS によって送信者をブロックする日付と時間の範囲を選択します。
 - ・ 問い合わせる特定の IP アドレスがわかっている場合は、[IP アドレス] に指定します。
 - ・ その IP アドレスの対応するドメイン名を表示するには、[ドメイン名を表示] チェックボックスをオンにします。
 - ・ [ページごとの表示数] で、一度に画面に表示するログエントリの数を選択します。
 3. [ログ表示] をクリックします。
 4. 次のいずれかの処理を実行してください。
 - ・ その IP アドレスを一時的にブロックするには、リストの対応するチェックボックスをオンにしてから、[一時的にブロック] をクリックします。
 - ・ その IP アドレスを永続的にブロックするには、リストの対応するチェックボックスをオンにしてから、[常にブロック] をクリックします。
 - ・ リストで同時に表示される項目の数を変更するには、表の上部にあるドロップダウンボックスから新しい表示値を選択します。
 - ・ 表を並び替えるには、列のタイトルをクリックします。
-

第 10 章

SMTP を設定する

この章では、InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) を稼働させるために必要なさまざまな設定について説明します。

内容は次のとおりです。

- ・ 146 ページの「MTA (Message Transfer Agents)」
- ・ 146 ページの「SMTP 接続を有効にする」
- ・ 146 ページの「SMTP ルーティングを設定する」
- ・ 155 ページの「メッセージ配信について」

MTA (Message Transfer Agents)

InterScan MSS は、Postfix、Sendmail、および qmail という 3 種類の MTA (Message Transfer Agents) をサポートしています。

InterScan MSS で Postfix を使用していて、複数の検索サービスが配置されている場合は、検索サービスの SMTP ルーティング設定を一元管理できます。InterScan MSS 管理コンソールから、SMTP 設定を指定して同じ設定をすべての検索サービスに適用します。

sendmail または qmail を使用している場合、各 MTA 設定ファイルの SMTP 設定を手動で行う必要があります。詳細については、「InterScan MSS インストールガイド」の「MTA の準備」を参照してください。

SMTP 接続を有効にする

InterScan MSS がネットワーク上の受信トラフィックおよび送信トラフィックの検索を開始する前に、SMTP 接続を有効にします。

手順

1. メニューから [システムステータス] を選択します。
 2. [接続の有効化] で [SMTP 接続を許可する] チェックボックスをオンにします。
 3. [保存] をクリックします。
-

SMTP ルーティングを設定する

SMTP ルーティングを設定するには、次の手順を実行します。



注意

InterScan MSS 9.1 では、IPv6 ネットワークのアップストリームおよびダウンストリームのコンポーネントと通信できます。

1. 147 ページの「SMTP を設定する」
2. 148 ページの「接続を設定する」
3. 153 ページの「メッセージルールを指定する」
4. 156 ページの「メッセージ配信を設定する」

SMTP を設定する

[SMTP ルーティング] 画面を使用して、SMTP グリーティングメッセージを設定します。

手順

1. [管理] > [InterScan MSS の設定] > [SMTP ルーティング] の順に選択します。

[SMTP ルーティング] 画面が表示されます。

SMTPルーティング



☒ すべての検索サービスに適用

SMTP	接続	メッセージルール	メッセージ配信
グリーティングメッセージ SMTPサーバのグリーティングメッセージ ESMTP Postfix 			
メール処理キュー メール処理キューは、検索または配信前にメッセージを保存するために使用されます。 パス: /var/spool/postfix 例 /var/spool/postfix			
保存 キャンセル			

2. [すべての検索サービスに適用] チェックボックスをオンにします。

このオプションは、各タブで指定されたすべての設定を、同じ InterScan MSS 管理データベースに接続されたすべての検索サービスに適用します。

3. [SMTP サーバのグリーティングメッセージ] (セッションが確立された際に表示されるメッセージ) を指定します。
 4. [メール処理キュー] の [パス] を指定します。
 5. [保存] をクリックします。
-

接続を設定する

[接続] 画面で、MTA の SMTP 接続を設定します。

手順

1. [管理] > [InterScan MSS の設定] > [SMTP ルーティング] の順に選択します。
2. [接続] タブをクリックします。

[接続] 画面が表示されます。

SMTP 接続 メッセージルール メッセージ配信

SMTP インタフェース

IP アドレス:

ポート:

タイムアウト: 分 (非アクティブ状態の経過時間)

同時接続数: ☐ 無制限 ☒ 接続数 まで許可する

接続制御

コンピュータからサーバへの接続を許可または拒否できます。

☒ 次のリストに含まれているコンピュータを除くすべての接続を許可する

☒ コンピュータ別の指定

例: 123.123.123.123 または 2001:db8:10ff:ae:442

☐ グループ別の指定

IP のバージョン: >>

サブネットアドレス: <<

例: 10.123.123.123

サブネットマスク:

例: 255.255.255.0

☐ 次のリストに含まれているコンピュータを除くすべての接続を拒否する

Transport Layer Security 設定

☐ 受信 Transport Layer Security を有効にする

☐ TLS による SMTP 接続のみを許可する

OA 証明書:

秘密鍵:

SMTP サーバ証明書:

☐ 送信 Transport Layer Security を有効にする

3. [SMTP インタフェース] 設定を指定します。

- ・ IP アドレス: SMTP サーバに接続するインタフェースを選択します。

ループバックアドレス

SMTP サーバは、ローカルコンピュータ上の IP アドレスのみを待機します。

すべてのインタフェース

コンピュータ上に複数の IP アドレスがある場合、SMTP サーバは使用可能なすべての IP アドレスを待機します。

- ・ ポート: SMTP サーバの待機ポートを指定します。
 - ・ タイムアウト: { } 分 (非アクティブ状態の経過時間): タイムアウト値を指定します。
 - ・ 同時接続数: [無制限] を選択するか、[接続数 { } まで許可する] を選択して最大接続数を指定します。
4. [接続制御] 設定を指定します。
- a. [次のリストに含まれているコンピュータを除くすべての接続を許可する] を選択して拒否するリストを設定するか、または [次のリストに含まれているコンピュータを除くすべての接続を拒否する] を選択して許可するリストを設定します。
 - b. リストを設定します。
 - ・ コンピュータ別の指定: IP アドレスを指定してから、[>>] をクリックしてその IP アドレスをリストに追加します。
 - ・ グループ別の指定:
 - i. IP のバージョンを選択します。
 - ・ IPv4 アドレスには、サブネットアドレスとサブネットマスクを指定します。
 - ・ IPv6 アドレスには、サブネットアドレスを指定します。
 - ii. [>>] をクリックしてそのグループをリストに追加します。
 - ・ インポート: IP リストをファイルからインポートする場合にクリックします。IP リストのテキストファイルのサンプルの内容は、次のとおりです。


```
192.168.1.1
192.168.2.0:255.255.255.0
192.168.3.1:255.255.255.128
```

192.168.4.100

192.168.5.32:255.255.255.192

2001:db8:10ff::ae:44f2

2001:db8::/32

5. [Transport Layer Security 設定] を指定します。

- a. [受信 Transport Layer Security を有効にする] をオンにします。

このオプションによって、InterScan MSSSMTP サーバは TLS 接続を介してのみメッセージを受け入れるようになります。

- b. InterScan MSS で安全な接続要求のみ許可する場合は、[TLS による SMTP 接続のみを許可する] をオンにします。

このオプションによって、InterScan MSSSMTP サーバは TLS 接続を介してのみメッセージを受け入れるようになります。

- c. 次のいずれかの横にある [参照] ボタンをクリックします。

- CA 証明書: 通常、CA 証明書は SMTP クライアントの確認に使用されます。しかし、InterScan MSS では、クライアントは確認せず、CA 証明書を TLS 接続の有効化にのみ使用します。

このファイルは、公開鍵とともに提供されている場合に限りアップロードされます。それ以外の場合は、TLS 接続を有効化する際にこのファイルは必須とはなりません。

- 秘密鍵: SMTP クライアントで、InterScan MSS SMTP サーバの公開鍵と暗号化鍵を使用して乱数が暗号化され、セッション鍵が生成されます。

InterScan MSS SMTP サーバは、秘密鍵を使用してその乱数を復号化し、安全な接続を確立します。TLS 接続を有効にするためにこの鍵をアップロードする必要があります。

- SMTP サーバ証明書: InterScan MSS SMTP サーバの公開鍵は、SMTP クライアントがセッション鍵を生成するために公開されます。

TLS 接続を有効にするためにこの鍵をアップロードする必要があります。

- d. [アップロード] をクリックして、そのファイルを InterScan MSS サーバ上に保存します。
 - e. 送信メッセージを保護する必要があるときは、[送信 Transport Layer Security を有効にする] をオンにします。
6. [保存] をクリックします。
-

メッセージルールを設定する

InterScan MSS が処理できるメッセージの制限を設定して、メールリレーを制御するには、[メッセージルール] 画面ですべての項目を設定してください。

メールリレー

スパムメール送信者が InterScan MSS MTA をスパムメールの中継点として利用することを防ぐために、ネットワーク上のメールドメインを [受信メッセージ設定] リストに追加して、リレー制御を設定してください。InterScan MSS は、メッセージを受信すると、そのメッセージの最終宛先を確認してこのリストと比較します。次の場合は、メッセージが破棄されます。

- ・ 宛先ドメインがこのリストにない
- ・ 宛先ドメインの親ドメインがこのリストにない
- ・ ホストが [メッセージリレーの許可] リストにない

受信メッセージの設定は、メッセージ配信ドメインの設定とは異なります。詳細については、[155 ページの「メッセージ配信について」](#)を参照してください。

メッセージルールを指定する

手順

1. [管理] > [InterScan MSS の設定] > [SMTP ルーティング] の順に選択します。
2. [メッセージルール] タブをクリックします。
[メッセージルール] 画面が表示されます。

SMTP

接続

メッセージルール

メッセージ配信

メッセージの制限
 制限を設定しない場合は、「0」を入力してください。
 最大メッセージサイズ (1~無制限): MB
 最大受信者数: (1~99999)

受信メッセージ設定

受信メッセージ

指定されたドメイン内の受信者宛ての受信メッセージのみを配信します。

指定されたドメイン

受信者

ドメインを追加する

 例: example.com <<

注意: IMSS でメッセージを受信するには、ネットワークの内部ドメインをすべて追加することをお勧めします。

メッセージリレーの許可

次に指定したホストは、リレー制限の対象から除外され、すべてのドメインにメッセージをリレーすることができます。

☐ ホストのみ
☒ ホストと同じサブネット
☐ ホストと同じIPクラス
☐ 指定のIPアドレス:

- ☒ **コンピュータ別の指定**
 例: 123.123.123.123または
 2001:db8:10ff:ae:44f2
- ☐ **グループ別の指定**
 IPのバージョン: IPv4
 サブネットアドレス: >> <<
 例: 10.123.123.123
 サブネットマスク: << >>
 例: 255.255.255.0

3. [メッセージの制限] 設定を指定します。

- ・ 最大メッセージサイズ: メガバイト数を指定します。
- ・ 最大受信者数: 1～99999 の間で、受信者数を指定します。

4. [受信メッセージ設定] を指定します。

メッセージは、追加されているドメインにリレーされます。

ドメインリストのテキストファイルのサンプルの内容は、次のとおりです。

- ・ example.com: 指定したドメインがインポートされます。
- ・ *.example.com: すべてのサブドメインがインポートされます。
- ・ example.org: 指定したドメインがインポートされます。

5. [メッセージリレーの許可] を指定します。

- ・ ホストのみ

- ・ ホストと同じサブネット
 - ・ ホストと同じ IP クラス
 - ・ 指定の IP アドレス
6. [保存] をクリックします。



ヒント

セキュリティ上の理由から、メッセージルールを設定する際にオープンリレーを避けることをお勧めします。

メッセージ配信について

IMSS は、受信者のメールアドレスのドメイン名に基づいてルーティングテーブルを管理します。IMSS は、このルーティングテーブルを使用して、ドメインベースの配信を通して指定された SMTP サーバに、受信者メールアドレスが一致するメールメッセージを転送します。他のすべてのドメインに配信されるメールメッセージは、ドメインネームサーバ (DNS) のレコードに基づいて転送されます。

受信メッセージドメインとメッセージ配信ドメイン

受信メッセージ設定に使用するドメインは、メッセージ配信設定に使用するドメインとは異なります。

受信メッセージドメイン

IMSS は、受信メッセージドメイン宛てのメッセージだけを中継します。たとえば、受信メッセージドメインとして example.com だけが指定されている場合、IMSS は example.com ドメイン宛てに送信されたメッセージだけを中継します。

メッセージ配信ドメイン

IMSS は、メッセージ配信ドメインベースでメッセージを配信します。たとえば、送信先ドメインを example.com と指定し、SMTP サーバの IP アドレスを 10.10.10.10、ポートを 25 とした場合、example.com 宛て

に送信されたメールはすべてポート 25 経由で SMTP サーバ 10.10.10.10 に配信されます。

メッセージ配信を設定する

次の配信の設定に進みます。InterScan MSS により、受信者のメールアドレスが検索され、一致したドメインの SMTP ホストにメッセージが送信されます。

メッセージ配信リストをインポートする際は、リストは有効なファイルである必要があります。各エントリは次の要素で構成されます。

[ドメイン],[サーバ名または IP アドレス]:[ポート番号]

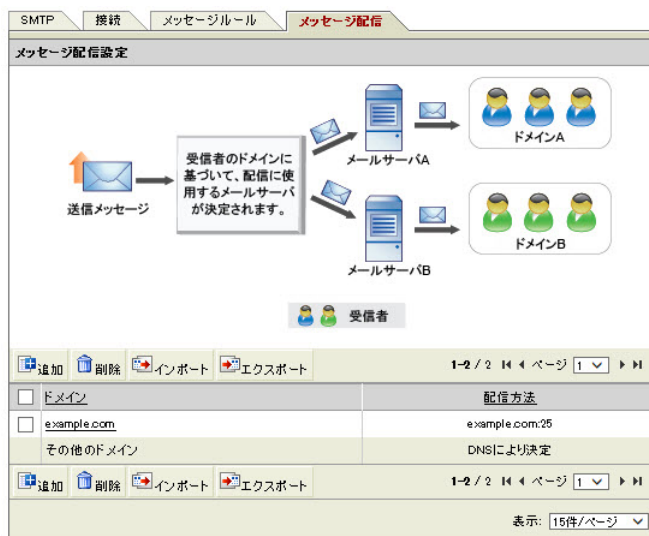
たとえば、次に示すエントリはすべて有効です。

- ・ domain1.com,192.168.1.1:2000
- ・ domain2.net,192.168.2.2:1029
- ・ domain3.com,smtp.domain3.com:25
- ・ domain4.com,mail.domain4.com:2000
- ・ domain5.com,[2001:db8:10ff::ae:44f2]:25

手順

1. [管理] > [InterScan MSS の設定] > [SMTP ルーティング] の順に選択します。
2. [メッセージ配信] タブをクリックします。

[メッセージ配信設定] 画面が表示されます。



3. [メッセージ配信設定] セクションで、[追加] をクリックします。
[送信先ドメイン] 画面が表示されます。

送信先ドメイン

名前:

配信方法

送信先ドメインに対して使用する配信方法を設定します。
次のSMTPサーバにメールを転送する:

サーバアドレス

ポート

OK

閉じる

4. [送信先ドメイン] と [配信方法] を指定します。
5. [OK] をクリックします。
[メッセージ配信設定] 表にドメインが追加されます。

6. [保存] をクリックします。
-

第 11 章

既知のホストの設定

この章では、既知のホストの概要と、既知のホストの追加、インポート、およびエクスポート方法について説明します。

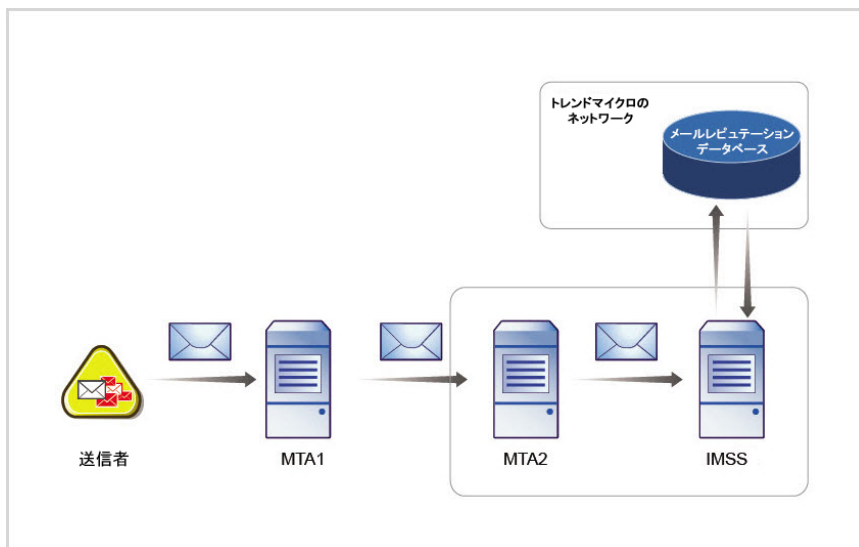
この章の内容は次のとおりです。

- ・ 160 ページの「既知のホストについて」
- ・ 161 ページの「既知のホストを追加する」
- ・ 162 ページの「既知のホストをインポートする」
- ・ 163 ページの「既知のホストをエクスポートする」

既知のホストについて

既知のホストには、信頼されるメール転送エージェント (MTA) と、ネットワーク上で InterScan MSS の外側に配置されたクラウドプレフィルタが含まれます。InterScan MSS がインターネットゲートウェイに配置されている場合、既知のホストを指定する必要はありません。既知のホストの設定は、次のいずれかの場合に使用します。

- ・ ネットワーク上で1つ以上の MTA が InterScan MSS のアップストリーム側に設定されている場合は、既知のホストの設定を有効にして、これらの MTA を既知のホストとして追加します。InterScan MSS は、既知のホストリストにない最も近いアップストリーム MTA を追跡し、その IP アドレスを、メールレピュテーションデータベースだけでなく、IP プロファイラの承認済みリストとブロックリストにクエリします。



たとえば、InterScan MSS のアップストリームに配置されたネットワーク上の MTA2 と、MTA2 のさらにアップストリームに配置されたネットワーク外の MTA1 がある場合は、既知のホストの設定を有効にして、MTA2 を既知のホストとして追加します。InterScan MSS は、MTA1 の IP アドレスを使用してクエリを実行します。

- ・ InterScan MSS がクラウドプレフィルタの後方に配置されている場合は、既知のホストの設定を有効にします。クラウドプレフィルタの IP アドレスは、初期設定で既知のホストリストに含まれます。

ネットワークでアップストリーム MTA またはクラウドプレフィルタが InterScan MSS の外側に配置されている場合は、次の理由があるため、既知のホストの設定を使用します。

- ・ InterScan MSS では、すべての外部メールメッセージをこれらの MTA またはクラウドプレフィルタから受信したものと見なし、その IP アドレスを使用してクエリを実行します。そのため、これらの IP アドレスを経由して転送されたすべてのメールトラフィックが安全だと見なされてしまいます。
- ・ メールフローでは、すべてのスパムメールがこれらのアドレスから送信されて InterScan MSS に到達するため、InterScan MSS ではこれらの IP アドレスをスパムメールの送信元と見なします。

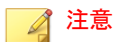
**注意**

InterScan MSS では、毎日午前 3 時にクラウドプレフィルタの IP アドレスを既知のホストリストに同期します。これらの既知のホストは、管理コンソールには表示されません。

既知のホストを追加する

手順

1. [管理] > [InterScan MSS の設定] > [既知のホスト] の順に選択します。
[既知のホスト] 画面が表示されます。
2. [既知のホストを有効にする] チェックボックスをオンにします。
3. IP アドレスと、追加するホストの説明を入力します。

**注意**

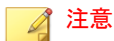
InterScan MSS は IPv4 および IPv6 の既知のホストのアドレスをサポートします。必要に応じて、単一の IP アドレスとサブネットアドレスを指定します。

4. [追加] をクリックします。
既知のホストリストに新しいホストが表示されます。
5. [保存] をクリックします。

既知のホストをインポートする

手順

1. [管理] > [InterScan MSS の設定] > [既知のホスト] の順に選択します。
[既知のホスト] 画面が表示されます。
2. [インポート] をクリックします。
[既知のホストのインポート] ダイアログボックスが表示されます。
3. [参照] をクリックして、インポートするファイルの場所を探します。
4. 次のいずれかを選択します。
 - ・ 現在のリストとマージ
 - ・ 現在のリストを上書き
5. [インポート] をクリックします。

**注意**

InterScan MSS では、ホストアドレスをインポートできるのは1つのテキストファイルからのみです。テキストファイルで、1行に1つの IP アドレスまたはサブネットアドレスのみが記載されていることを確認します。

既知のホストをエクスポートする

手順

1. [管理] > [InterScan MSS の設定] > [既知のホスト] の順に選択します。
[既知のホスト] 画面が表示されます。
2. エクスポートするホストを 1 つ以上選択します。
3. [エクスポート] をクリックします。



注意

InterScan MSS では、説明を含めずにホストアドレスのみをエクスポートします。

第 12 章

POP3 の設定をする

この章では、POP3 を設定する手順について説明します。

この章の内容は次のとおりです。

- ・ 166 ページの「POP3 メッセージを検索する」
- ・ 167 ページの「POP3 の検索を有効にする」
- ・ 168 ページの「POP3 の設定をする」
- ・ 169 ページの「POP3 検索サービスを設定する」

POP3 メッセージを検索する

InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) では、SMTP トラフィックを検索できるだけでなく、ネットワーク内のクライアントが POP3 メッセージを受信する際に、ゲートウェイでそれらのメッセージを検索することもできます。企業で POP3 メッセージが使用されていない場合でも、従業員がコンピュータ上にあるメールクライアントを使用して個人の POP3 メールアカウントにアクセスすることがあります。POP3 メールアカウントの例には、Gmail や Yahoo! などがあります。それらのアカウントからのメッセージを検索しなければ、ネットワーク上に脆弱ポイントが生じる場合があります。

POP3 メール検索を理解する

InterScan MSS の POP3 検索サービスは、メールクライアントと POP3 サーバとの間に配置されたプロキシサーバとして機能し、クライアントがメッセージを受信した際にメッセージを検索します。

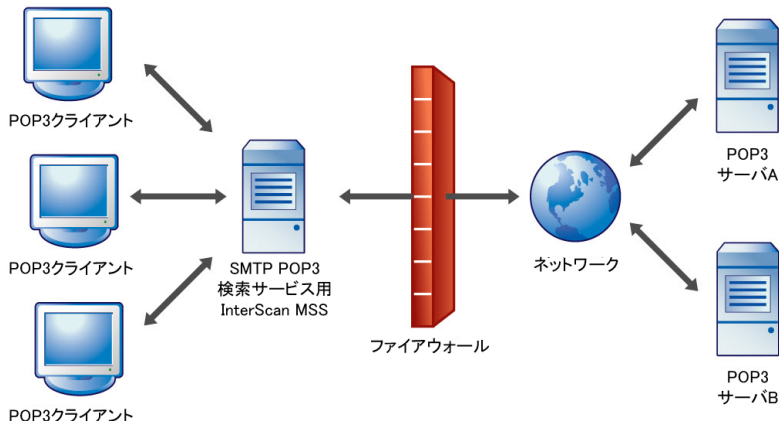


図 12-1. POP3 メッセージを検索する

POP3 トラフィックを検索するには、InterScan MSS サーバ POP3 プロキシに接続するようにメールクライアントを設定します。これにより、POP3 サーバに接続し、メッセージを受信して検索します。

設定可能な接続の種類は、次のとおりです。

- ・ 一般的な接続: 同じポートを使用して、異なる POP3 サーバにアクセスできます。ポートは通常 110 で、これは POP3 トラフィックの初期設定のポートです。
- ・ 専用の接続: 特定のポートを使用して、POP3 サーバにアクセスします。POP3 サーバで、APOP や NTLM などの安全なログオンを使用した認証が必要な場合は、これらの接続を使用します。

**注意**

InterScan MSS は、IPv6 POP3 サーバへの接続をサポートしています。

POP3 の要件

InterScan MSS で POP3 トラフィックが検索されるようにするためには、ファイアウォールがネットワークに配置され、ネットワーク上の InterScan MSS サーバを除くすべてのコンピュータからの POP3 要求をブロックするように設定されている必要があります。この設定により、すべての POP3 トラフィックがファイアウォールを通過して InterScan MSS に渡され、InterScan MSS で POP3 のデータフローが検索されます。

POP3 の検索を有効にする

InterScan MSS で POP3 トラフィックの検索が開始されるようにするには、POP3 検索を有効にして、POP3 の設定を実行します。

手順

1. [接続の有効化] で [POP3 接続を許可する] チェックボックスをオンにします。

2. [保存] をクリックします。

POP3 の設定をする

クライアントが使用する InterScan MSS サーバのポートを指定して、POP3 トラフィックを取り込むことができます。初期設定の POP3 ポートは「110」です。しかし、ユーザが認証済みの接続を介して POP3 サーバにアクセスする必要がある場合 (APOP コマンドや NTLM を使用する場合)、専用の接続を設定してカスタムポートを割り当てることもできます。

手順

1. [管理] > [InterScan MSS の設定] > [接続] の順に選択します。

初期設定で [コンポーネント] タブが表示されます。

2. [POP3] タブをクリックします。

接続 ?

コンポーネント LDAP **POP3** データベース Control Manager サーバ

一般的なPOP3接続

ユーザが要求した任意のPOP3サーバ

受信MSSポート:

専用のPOP3接続

受信POP3ポート	POP3サーバ	POP3サーバポート

メッセージテキスト

ユーザが受信しようとしているメッセージがフィルタされる場合、次のテキストがユーザに送信されます。通知は、[通知設定] 画面で選択した文字セットを使用して送信されます。

↑ ↓

3. 次のいずれかを実行します。

- ・ ユーザが初期設定のポート 110 と異なる POP3 サーバを要求した場合、それを許可するには、InterScan MSS 受信 POP3 ポート番号を指定します。
 - ・ 認証用に特定のポートを使用して POP3 サーバにアクセスするには、[追加] をクリックして新規の専用 POP3 接続を作成します。必要な情報を入力して、[OK] をクリックします。
4. [保存] をクリックします。
-

POP3 検索サービスを設定する

手順

1. POP3 接続を有効にします。
 - a. [システムステータス] に移動します。
 - b. [接続の有効化] で [POP3 接続を許可する] をクリックします。
 - c. [保存] をクリックします。
2. POP3 を設定します。

詳細については、[168 ページの「POP3 の設定をする」](#)を参照してください。
3. メールクライアントを設定します。
 - ・ POP3 サーバ: InterScan MSS の IP アドレス
 - ・ POP3 ポート番号: InterScan MSS で指定するポート
 - ・ POP3 ユーザアカウント
 - ・ 一般的な POP3 サーバを指定した場合: ユーザ名#リモートサーバ
 - ・ 専用の POP3 サーバを指定した場合: ユーザ名
 - ・ パスワード: リモートサーバ上のユーザのパスワード

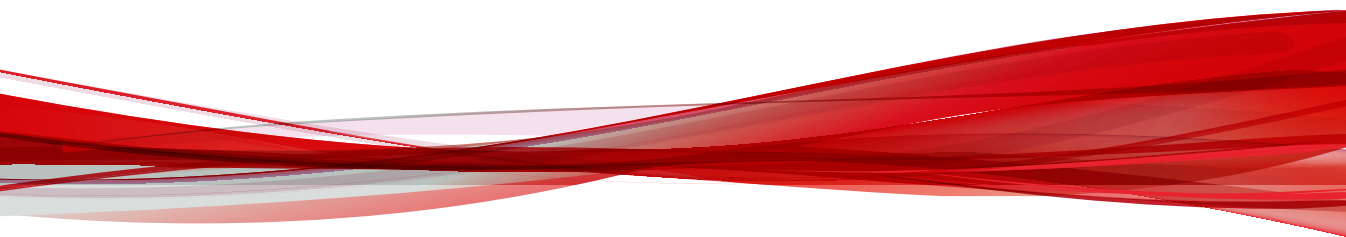


注意

一般的な POP3 サーバを指定して、POP3 ポートがリモート POP3 サーバで変更されている場合は、ユーザアカウントの形式を「**ユーザ名#リモートサーバ#リモート POP3 ポート**」に設定してください。

パート III

InterScan MSS ポリシー



第 13 章

ポリシーの管理

この章では、InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) ポリシーを作成、変更、および管理する手順について説明します。

この章の内容は次のとおりです。

- ・ 174 ページの「ポリシーについて」
- ・ 174 ページの「Policy Manager の仕組み」
- ・ 176 ページの「ポリシーリストに表示されるポリシーをフィルタする」

ポリシーについて

InterScan MSS ポリシーとは、SMTP および POP3 メッセージに適用されるルールのことです。ルールを作成して、組織のウイルス対策などのセキュリティを強化します。初期設定では、InterScan MSS には、ウイルスなどのインターネット上の脅威からネットワークを保護するためのグローバルウイルス対策ルールが組み込まれています。ウイルス対策ルールは、システムに害を与える可能性のある最も危険な種類のメッセージを対象としています。したがって、InterScan MSS でトラフィックにウイルスが含まれていないか最初に分析できるように、このルールを常にルールリストの一番上に配置しておく必要があります。

ウイルス対策ルールは、スパムメール対策に対応していません。適切にスパムメールに対処するには、検索条件にスパムメールを含むカスタムルールを設定して、送信者フィルタをアクティベートしてください。



注意

新しいポリシーを作成する前に、内部アドレスが定義されていることを確認します。詳細については、[240 ページの「内部アドレスを設定する」](#)を参照してください。

Policy Manager の仕組み

次の種類のポリシーに関する複数のルールを作成できます。ポリシーを使用することで、メッセージングシステムにおけるセキュリティ上の脅威を抑制し、生産性の低下を防ぎます。

- ・ ウイルス対策: メッセージ内のウイルスおよびその他の不正プログラム（スパイウェアやワームなど）を検索します。
- ・ その他: スパムメール/フィッシングメッセージ/ソーシャルエンジニアリング攻撃メッセージ、メッセージコンテンツ、およびその他の添付ファイルの条件を検索します。

InterScan MSS ポリシーには、次のコンポーネントが含まれます。

- ・ ルート: ポリシーが適用される、送信者および受信者のメールアドレスのセットまたはグループ、あるいは LDAP ユーザまたはグループ。アスタ

リスク(*)を使用してワイルドカード表現を作成し、ルートの設定を簡単にします。

- ・ フィルタ: 特定のルートに適用されるルールまたはルールセット。検索条件とも呼ばれます。InterScan MSS には、一般的なウイルスやその他の脅威に対処する定義済みのフィルタがあります。これらの定義済みフィルタを変更したり、専用のフィルタを定義できます。
- ・ 処理: フィルタの条件に一致した場合に、InterScan MSS により実行される処理。フィルタの結果に応じて、最終的にメッセージを処理する方法が決定されます。

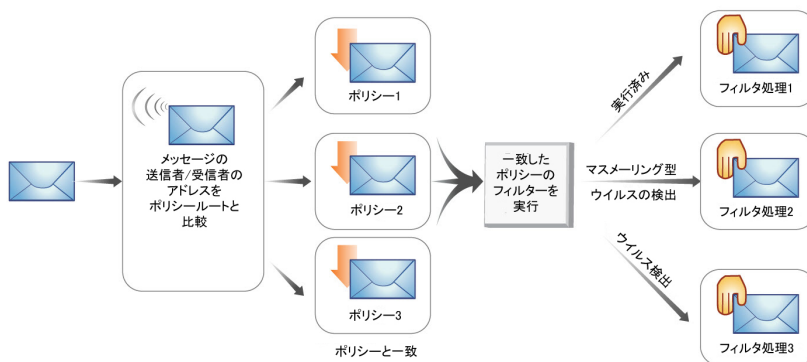


図 13-1. Policy Manager のプロセスフローの簡略図



注意

ポリシーの作成方法の詳細については、[259 ページのポリシーの設定](#)を参照してください。

ポリシーリストに表示されるポリシーをフィルタする

手順

1. [ポリシー] > [ポリシーリスト] の順に選択します。
[ポリシー] 画面が表示されます。
2. [フィルタ基準] オプションを設定します。
 - a. ルートを指定します。
 - ・ すべてのルート: すべてのポリシーを表示します。
 - ・ 受信: 受信メッセージのみを監視するポリシーを表示します。
 - ・ 送信: 送信メッセージのみを監視するポリシーを表示します。
 - ・ 両方向: 「受信」、「送信」、「受信および送信」メッセージを監視するポリシーを表示します。
 - ・ POP3: POP3 メッセージのみを監視するポリシーを表示します。
 - b. ポリシーで設定する保護の種類を指定します。
 - ・ すべての種類
 - ・ ウイルスと不正プログラム
 - ・ C&C メール
 - ・ スパムメール、フィッシングメール、およびソーシャルエンジニアリング攻撃メール
 - ・ グレーメール
 - ・ Web レピュテーション
 - ・ 添付ファイル
 - ・ 内容

- ・ コンプライアンス
 - ・ サイズ
 - ・ その他
- c. ポリシーの保護対象ユーザを指定します。
- ・ すべてのグループ
 - ・ [ユーザまたはグループの検索]
-

第 14 章

共通のポリシーオブジェクトの設定

この章では、アドレスグループ、キーワード、式、コンプライアンステンプレート、通知、スタンプなどの共通のポリシーオブジェクトを設定する手順について説明します。

この章の内容は次のとおりです。

- ・ 180 ページの「ポリシーオブジェクトの説明」
- ・ 181 ページの「アドレスグループ」
- ・ 192 ページの「キーワードリストを使用する」
- ・ 206 ページの「DLP コンプライアンステンプレート」
- ・ 226 ページの「ポリシー通知」
- ・ 231 ページの「スタンプ」
- ・ 234 ページの「DKIM 承認済みリスト」
- ・ 236 ページの「Web レピュテーション承認済みリスト」

ポリシーオブジェクトの説明

共通のポリシーオブジェクトを作成し、すべてのポリシーで共有できる設定を保存することで、ポリシー管理が簡単になります。

表 14-1. ポリシーオブジェクト

ポリシーオブジェクト	説明
アドレスグループ	複数のメールアドレスを 1 つのグループにまとめます。
キーワード	情報漏えいの防止、スパムメールのブロック、または中傷メッセージのネットワークへの侵入やネットワーク内での移動の阻止を目的としたキーワードを作成します。
コンプライアンステンプレート	コンプライアンステンプレートを作成して、機密データのネットワークからの流出を阻止します。
ポリシー通知	受信者またはメール管理者に、InterScan MSS がメッセージの添付ファイルに対して何らかの処理を実行したことや、メッセージが InterScan MSS ルールの検索条件に違反していることを通知するメッセージを作成します。
スタンプ	受信者に、InterScan MSS がメッセージの添付ファイルに対して何らかの処理を実行したことや、メッセージがルールの検索条件に違反していることを通知するスタンプを作成します。
DKIM 承認済みリスト	DKIM 署名が一致するドメインからのメッセージは、検索されたりスパムメールとしてマークされたりすることはありません。
Web レピュテーション承認済みリスト	Web レピュテーション承認済みリストに記載されているドメインは、Web レピュテーションフィルタによって検索もブロックもされません。ただし、これ以外のフィルタによって Web レピュテーション承認済みリストのメッセージがブロックされることはあります。

アドレスグループ

アドレスグループとは、ポリシーが適用されるメールアドレスのリストのことです。アドレスグループにより、複数のメールアドレスを1つのグループにまとめ、グループ内のすべてのアドレスに同じポリシーを適用できます。

たとえば、企業のメールシステムを使用して送信されないようにする3種類のコンテンツを識別し、これらのコンテンツを検出する3つのフィルタを定義しているとします(下記カッコ内はフィルタ名を示す)。

- ・ 企業の極秘財務データ (FINANCIAL)
- ・ 就職活動のメッセージ (JOBSEARCH)
- ・ VBS スクリプトウイルス (VBSCRIPT)

企業内に次のアドレスグループがあるとします。

- ・ すべての幹部
- ・ すべての人事部門
- ・ すべての IT 開発スタッフ

ポリシーで使用するフィルタは、次のようにこれらのグループに適用するとします。

アドレスグループ	FINANCIAL	JOBSEARCH	VBSCRIPT
すべての幹部	適用しない	適用する	適用する
すべての人事部門	適用する	適用しない	適用する
すべての IT 開発スタッフ	適用する	適用する	適用しない

幹部、人事スタッフ、および IT 開発者には、財務情報、就職活動関連の文書、および VBS ファイルを送信する正当な理由がそれぞれあるので、これらのグループには一部のフィルタを適用しません。

InterScan MSS では、メールアドレスによって組織のメンバーを識別し、メンバーに適用するポリシーを決定します。正確なアドレスグループを定義することで、適切なポリシーをグループ内の各メンバーに適用できます。

アドレスグループを作成する

アドレスグループとは、組織内の複数のユーザのメールアドレスの集合です。各メールアドレスにルールを個別に適用する代わりに、アドレスグループを作成して、複数のメールアドレスに一括してルールを適用できます。

アドレスグループは、ポリシー作成前、またはポリシー作成でルートを指定する際に作成できます。オプションで、既存のポリシーを変更する際に、アドレスグループを追加できます。アドレスグループは、手動で作成することも、1行につき1つのメールアドレスが含まれているテキストファイルからインポートすることもできます。



ヒント

アドレスグループは、ポリシー作成時にも作成できますが、ポリシー作成を開始する前に作成しておくことをお勧めします。

手順

1. [ポリシー] > [アドレスグループ] の順に選択します。
[アドレスグループ] 画面が表示されます。
2. [追加] をクリックします。
[アドレスグループの追加] 画面が表示されます。

アドレスグループの追加



アドレスグループ > アドレスグループの追加

アドレスグループには、メールアドレスまたはワイルドカードを使用したメイン (例: *@example.com、*@*.example.com) を含めることができます。

保存
キャンセル

アドレスグループ名:

アドレス:

追加

インポート

削除

エクスポート

保存
キャンセル

3. グループ名を指定します。
4. 次のいずれかを実行します。
 - ・ 個別にアドレスを追加する:
 - ・ メールアドレスを指定して [追加] をクリックします。オプションで、ワイルドカード文字を使用して、メールアドレスを指定できます。たとえば、「*@hr.com」のように入力します。
 - ・ アドレスのリストをインポートする:
 - a. [インポート] をクリックします。
アドレスグループのインポート画面が表示されます。
 - b. [参照] をクリックして、インポートするファイルの場所を探します。
 - c. 次のいずれかを選択します。

- ・ 現在のリストとマージ
 - ・ 現在のリストを上書き
- d. [インポート] をクリックします。

**注意**

InterScan MSS では、メールアドレスをインポートできるのは1つのテキストファイルからのみです。テキストファイルで、1行に1つのメールアドレスのみが記載されていることを確認します。オプションで、ワイルドカード文字を使用して、メールアドレスを指定できます。たとえば、「*@hr.com」のように入力します。

5. [保存] をクリックします。

[アドレスグループ] 画面が表示され、[アドレスグループ] テーブルに新しいアドレスグループが追加されています。

ポリシー作成時にアドレスグループを追加する

ポリシー作成でルートを指定する際に、アドレスグループを作成できます。そのためには、メールアドレスを個別に追加したり、テキストファイルからインポートします。

**注意**

InterScan MSS では、メールアドレスをインポートできるのは1つのテキストファイルからのみです。テキストファイルで、1行に1つのメールアドレスのみが記載されていることを確認します。オプションで、ワイルドカード文字を使用して、メールアドレスを指定できます。たとえば、「*@hr.com」のように入力します。

手順

1. [ポリシー] > [ポリシーリスト] の順に選択します。
2. [追加] ボタンをクリックします。

- ドロップダウンリストから [ウイルス対策] または [その他] を選択し、ウイルス対策ルールまたはその他の脅威に対するルールを作成します。

[手順 1: 受信者と送信者の選択] 画面が表示されます。

- [受信者] または [送信者] リンクをクリックします。

[アドレスの選択] 画面が表示されます。

ルールの追加



ポリシーリスト > 新規ルール

➤ 手順1: 受信者と送信者の選択 >>> 手順2 >>> 手順3 >>> 手順4

このルールの適用対象 受信メッセージ ▼

< 戻る

次へ >

キャンセル

宛先	受信者
差出人	送信者
除外設定	送信者から受信者

受信者と送信者

受信

宛先 すべてのユーザ

および

差出人 すべてのユーザ

< 戻る

次へ >

キャンセル

- ドロップダウンリストから [アドレスグループの選択] を選択します。

次の宛先への受信メッセージ



ルールの追加 > 次の宛先への受信メッセージ

保存 キャンセル

アドレスの選択

☐ すべてのユーザ
☒ 選択したアドレスのいずれか

アドレスグループの選択 ▼

追加 >

追加 編集 削除

選択済み

保存 キャンセル

6. [追加] をクリックします。
[アドレスグループの追加] 画面が表示されます。
7. グループ名を指定します。
8. 次のいずれかを実行します。
 - ・ 個々のアドレスの追加:
 - ・ メールアドレスを指定して、[追加] をクリックし個々にメールアドレスを追加します。オプションで、ワイルドカード文字を使用して、メールアドレスを指定できます。たとえば、「*@hr.com」のように入力します。
 - ・ アドレスのリストをインポートする:
 - a. [インポート] をクリックします。

アドレスグループのインポート画面が表示されます。

- b. [参照] をクリックして、インポートするファイルの場所を探します。
- c. 次のいずれかを選択します。
 - ・ 現在のリストとマージ
 - ・ 現在のリストを上書き
- d. [インポート] をクリックします。

**注意**

InterScan MSS では、メールアドレスをインポートできるのは1つのテキストファイルからのみです。テキストファイルで、1行に1つのメールアドレスのみが記載されていることを確認します。オプションで、ワイルドカード文字を使用して、メールアドレスを指定できます。たとえば、「*@hr.com」のように入力します。

9. [保存] をクリックします。

アドレスグループを編集または削除する

アドレスグループを編集または削除するには、[アドレスグループ] 画面を使用するか、既存のポリシーを編集します。

手順

1. [ポリシー] > [アドレスグループ] の順に選択します。
[アドレスグループ] 画面が表示されます。
2. 次のいずれかを実行します。
 - ・ アドレスグループの編集:
 - a. [アドレスグループ] テーブルで既存のアドレスグループをクリックします。
[アドレスグループ] 画面が表示されます。

b. 必要に応じてアドレスグループを編集します。

c. [保存] をクリックします。

[アドレスグループ] 画面が表示されます。

・ アドレスグループの削除:

a. アドレスグループの横のチェックボックスをオンにします。

b. [削除] をクリックします。

アドレスグループを既存のポリシーから編集または削除する

手順

1. [ポリシー] > [ポリシーリスト] の順に選択します。
2. 既存のポリシーのリンクをクリックします。
3. [受信者と送信者] リンクをクリックします。
4. [受信者] または [送信者] リンクをクリックします。

[アドレスの選択] 画面が表示されます。

次の宛先への受信メッセージ



初期設定のスパムメール対策ルール > 次の宛先への受信メッセージ

保存

キャンセル

アドレスの選択



すべてのユーザ



選択したアドレスのいずれか

メールアドレスの入力



追加 >

選択済み

@



test@imssrd.com



保存

キャンセル

5. ドロップダウンリストから [アドレスグループの選択] を選択します。

次の宛先への受信メッセージ



初期設定のスパムメール対策ルール > 次の宛先への受信メッセージ

保存 キャンセル

アドレスの選択

☐ すべてのユーザ
☒ 選択したアドレスのいずれか

アドレスグループの選択

test

追加 >

追加 編集 削除

保存 キャンセル

選択済み

@	
test@imssrd.com	

- 必要なアドレスグループを選択し、[編集] または [削除] ボタンを必要に応じてクリックします。

アドレスグループをエクスポートする

アドレスグループをエクスポートして、設定を他の InterScan MSS サーバにインポートします。アドレスグループのエクスポートは、既存のポリシーまたはアドレスグループリストから実行します。

手順

- [ポリシー] > [アドレスグループ] の順に選択します。

[アドレスグループ] 画面が表示されます。

2. エクスポートするアドレスグループをクリックします。
[アドレスグループ] 画面が表示されます。
 3. [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] 画面が表示されます。
 4. [保存] をクリックします。
[名前を付けて保存] ダイアログボックスが表示されます。
 5. 名前とアドレスグループをエクスポートする場所を指定します。
 6. [保存] をクリックします。
-

既存ポリシーからアドレスグループをエクスポートする

手順

1. [ポリシー] > [ポリシーリスト] の順に選択します。
2. 既存のポリシーのリンクをクリックします。
3. [受信者と送信者] リンクをクリックします。
4. [受信者] または [送信者] リンクをクリックします。
[アドレスの選択] 画面が表示されます。
5. ドロップダウンリストから [アドレスグループの選択] を選択します。
6. [編集] をクリックします。
[アドレスグループ] 画面が表示されます。
7. [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] 画面が表示されます。
8. [保存] をクリックします。
[名前を付けて保存] ダイアログボックスが表示されます。

9. 名前とアドレスグループをエクスポートする場所を指定します。
 10. [保存] をクリックします。
-

キーワードリストを使用する

キーワードは特別な単語またはフレーズです。特定のタイプ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。たとえば、診断書で使用されることのある「予後」、「血液型」、「予防接種」、「医師」などがキーワードとなります。診断書ファイルの送信を防ぐため、これらのキーワードが含まれるファイルをブロックするように InterScan MSS を設定します。

キーワードは特定の構造を備えたデータです。たとえば、クレジットカード番号は通常 16 桁の数字で構成され、「nnnn-nnnn-nnnn-nnnn」という形式で表示されるため、キーワードベースの検出に適しています。

InterScan MSS では、件名、本文、またはヘッダに基づいて、メールメッセージに対する処理を実行できます。コンテンツ別にメールメッセージをフィルタするには、キーワードリストのキーワードまたは正規表現を組み合わせます。

コンテンツの検索条件を選択する

手順

1. ウイルス対策ポリシーでない「その他」のポリシーを作成して変更します。
 - ・ 新しいルールを作成手順については、[259 ページのポリシーの設定](#)を参照してください。
 - ・ 既存ルールの変更手順については、[323 ページの既存のポリシーの設定](#)を参照してください。
2. [検索条件] 画面の [コンテンツ] で、コンテンツの条件を適用するメッセージ部分の横のチェックボックスをオンにします。

3. 内容の条件を設定するメッセージ部分のリンクをクリックします。

次の 2 つの列が表示されている [キーワードおよび式] 画面が表示されます。

- ・ 使用可能:キーワードは利用可能ですが、現在使用されていません。
- ・ 選択済み:キーワードは現在使用中です。

4. ヘッダにキーワードを設定する場合は、キーワードを適用するヘッダ項目の横のチェックボックスをオンにします。

5. [追加] をクリックします。

キーワード表現を管理する画面が表示されます。

6. キーワードを設定します。

7. [使用可能] リストで、有効にするキーワードリストをクリックします。

8. [➤] をクリックします。

キーワードが [選択済み] リストに表示されます。

キーワードリストを利用可能な状態にしておき、InterScan MSS で一時的に使用しないようにするには、選択されたリストでキーワードをクリックしてから [➤] をクリックします。

9. [保存] をクリックして、[検索条件] 画面を続行します。

キーワードを設定する

キーワードと正規表現を設定して、InterScan MSS でメッセージのコンテンツを検索できるようにします。キーワードは、[キーワード] 画面で、またはルールを作成時に作成します。



ヒント

キーワードは、ポリシー作成時にも作成できますが、ポリシー作成を開始する前に作成しておくことをお勧めします。

キーワードおよび式

キーワードは、[キーワード] 画面で、またはポリシー作成時に作成します。キーワードはポリシーを作成する前に作成することをお勧めします。

各キーワードリストには、コンテンツによる検出の実行の有無を決定する組み込みの条件が備わっています。キーワードリストは、InterScan MSS によるポリシーの適用に関係なく、指定した条件を満たす必要があります。

キーワードは強力な文字列マッチングツールです。キーワードを作成する前に、キーワードの構文を十分に理解しておく必要があります。粗雑に記述されたキーワードは、パフォーマンスに悪影響をもたらすことがあります。キーワードを作成する場合は、次の点を考慮してください。

- ・ InterScan MSS は Perl Compatible Regular Expressions (PCRE) で定義されたキーワード形式に準じていることに注意してください。PCRE の詳細については、<http://www.pcre.org/> を参照してください。
- ・ 有効なキーワードの定義方法のガイダンスについては、事前定義されたキーワードを参照してください。
- ・ シンプルなキーワードから開始します。誤ったアラームを引き起こす場合はキーワードを変更します。または、それらを調整して検出精度を向上します。
- ・ キーワードを作成する際の条件を指定します。キーワードは、InterScan MSS によるポリシーの適用に関係なく、指定した条件を満たす必要があります。

キーワードを作成する

手順

1. [ポリシー] > [キーワードおよび式] の順に選択します。

[キーワードおよび式] 画面が表示されます。

キーワードおよび式



追加 コピー 削除			
☐	キーワードおよび式名	条件	ポリシーで使用
☐	誹謗中傷	指定した任意のキーワード	0
☐	デマメール	指定した任意のキーワード	0
☐	チェーンメール	指定した任意のキーワード	0
☐	性差別	指定した任意のキーワード	0
☐	人種差別	指定した任意のキーワード	0
☐	HTML/スクリプトメッセージ	しきい値を超えています	0
☐	クレジットカード番号	指定した任意のキーワード	0
☐	社会保障番号	指定した任意のキーワード	0
☐	バウンスメール	指定した任意のキーワード	0

2. [追加] をクリックします。

[キーワードおよび式の追加] 画面が表示されます。

キーワードおよび式



キーワードおよび式 > キーワードおよび式の追加

リスト名:

一致:

指定した任意のキーワード

追加
 削除

☐	キーワード/正規表現	大文字/ 小文字 の区別	説明

3. [リスト名] に、わかりやすい名前を指定します。
4. [一致] の横で次のいずれかを選択し、InterScan MSS が処理を実行するタイミングを指定します。

- ・ 指定した任意のキーワード: メッセージのコンテンツがリスト内の任意のキーワードに一致するとき。
- ・ 指定したすべてのキーワード: メッセージのコンテンツがリスト内のすべてのキーワードに一致するとき。
- ・ 指定した以外のキーワード: メッセージのコンテンツがリスト内のどのキーワードにも一致しないとき。
- ・ 合計スコアがしきい値を超える場合のみ: メッセージのコンテンツがリスト内の 1 つ以上のキーワードを含むとき。キーワードが 1 つだけ検出された場合は、そのスコアがしきい値を超えている必要があります。複数のキーワードが検出された場合は、合計スコアがしきい値を超えている必要があります。

[処理が実行される総メッセージスコア] の横に、許容されるキーワードの最大スコアの数値を指定します。キーワードを追加するときに、その [スコア] の値を設定することができます。

5. 新しいキーワード表現を作成するには、次の手順を実行します。

- a. [追加] をクリックします。

[キーワードおよび式の追加] リストが表示されます。

キーワードおよび式の追加



キーワードおよび式 > キーワードおよび式の追加

保存

キャンセル

キーワードと正規表現の任意の組み合わせを使用してキーワードを定義できます。

キーワード:

、*、(、)、{、}、[、]、^、\$、%、+、または?という文字の直前には、「\」を入力してください。

☐ 大文字と小文字の区別

説明:

保存

キャンセル

- b. 次のパラメータを定義します。

キーワード

キーワードを指定します。部分一致の場合は、キーワードを指定してください。完全一致を指定するには、キーワードの前後に「\b」を使用します。

以下に例を示します。

- ・ 「keyword」は、「keywords」、「akeyword」と一致します。
- ・ 「\bkeyword\b」は、「keyword」とのみ一致します。

大文字/小文字の区別

キーワード表現で大文字と小文字を区別します。

説明

追加したキーワード表現について、わかりやすい説明を入力します。

- c. [保存] をクリックします。
6. [合計スコアがしきい値を超える場合のみ] を選択した場合:
 - a. [処理が実行される総メッセージスコア] フィールドでしきい値を指定します。
 - b. [スコア] ドロップダウンボックスから値を選択します。
7. [保存] をクリックします。

[キーワードおよび式] 画面のテーブルに新しいキーワードが表示されています。

ポリシーの作成時や変更時にキーワードを追加または編集する

手順

1. ウイルス対策ポリシーでない「その他」のポリシーを作成して変更します。
 - ・ 新しいルールを作成手順については、[259 ページのポリシーの設定](#)を参照してください。
 - ・ 既存ルールの変更手順については、[323 ページの既存のポリシーの設定](#)を参照してください。
2. [検索条件] 画面の [コンテンツ] で、内容の条件を設定するメッセージ部分のリンクをクリックします。

次の 2 つの列が表示されている [キーワードおよび式] 画面が表示されます。
3. [キーワードおよび式] 画面で [追加] または [編集] をクリックします。

キーワード表現リストの設定画面が表示されます。
4. [リスト名] に、わかりやすい名前を指定します。
5. [一致] の横で次のいずれかを選択し、InterScan MSS が処理を実行するタイミングを指定します。

- ・ 指定した任意のキーワード: メッセージのコンテンツがリスト内の任意のキーワードに一致するとき。
 - ・ 指定したすべてのキーワード: メッセージのコンテンツがリスト内のすべてのキーワードに一致するとき。
 - ・ 指定した以外のキーワード: メッセージのコンテンツがリスト内のどのキーワードにも一致しないとき。
 - ・ 合計スコアがしきい値を超える場合のみ: [処理が実行される総メッセージスコア] の横に、許容されるキーワードの最大スコアの数値を指定します。キーワードを追加するときに、その [スコア] の値を設定することができます。
6. キーワードを作成するには、[追加] をクリックします。
[キーワードおよび式の追加] リストが表示されます。
7. キーワードを指定します。部分一致の場合は、キーワードを指定してください。完全一致を指定するには、キーワードの前後に「\b」を使用します。
- 以下に例を示します。
- ・ 「keyword」は、「keywords」、「akeyword」と一致します。
 - ・ 「\bkeyword\b」は、「keyword」とのみ一致します。
8. キーワードの説明を指定します。
9. [合計スコアがしきい値を超える場合のみ] を選択した場合:
- a. [処理が実行される総メッセージスコア] フィールドでしきい値を指定します。
 - b. [スコア] ドロップダウンボックスから値を選択します。
10. [保存] をクリックします。
11. フィルタの使用時に、メッセージコンテンツの大文字/小文字が区別されるようにする場合は、[大文字と小文字の区別] のチェックボックスをオンにします。

12. [保存] をクリックして、ポリシーの変更または作成を続行します。

正規表現について

InterScan MSS はすべてのキーワードを正規表現として処理します。InterScan MSS でサポートしている正規表現は次のとおりです。



ヒント

キーワードは、ポリシー作成時にも作成できますが、ポリシー作成を開始する前に作成しておくことをお勧めします。

文字

正規表現	説明
.	(ドット) 改行文字以外の任意の文字 (バイト)
x	文字「x」
\\	文字「\」
\a	警告 (ベル) 文字 (ASCII 0x07)
\b	[b] や\b のように、このメタ記号が角カッコで囲まれているか単独で使用されている場合は、バックスペース文字 (ASCII 0x08) として扱われます。 - このメタ記号が正規表現の先頭 (または末尾) にある場合は、その正規表現に一致する文字列に対し、その一致文字列の左側 (または右側) が境界かどうかチェックする必要があることを意味します。以下に例を示します。 \bluck > 左側が境界でなければなりません。 - luck\b > 右側が境界でなければなりません。 \bluck\b > 両側が境界でなければなりません。 - このメタ記号が正規表現の内側で使用されている場合は構文エラーになります。

正規表現	説明
\f	改ページ文字 (ASCII 0x0C)
\n	改行文字 (ASCII 0x0A)
\r	復帰改行文字 (ASCII 0x0D)
\t	通常の (水平) タブ文字 (ASCII 0x09)
\v	垂直タブ文字 (ASCII 0x0B)
\n	8 進値 0n を持つ文字 (0 <= n <= 7)
\nn	8 進値 0nn を持つ文字 (0 <= n <= 7)
\mnn	8 進値 0nnn を持つ文字 (0 <= m <= 3、0 <= n <= 7)
\xhh	16 進値 0xhh を持つ文字。たとえば、\x20 は空白文字を意味します。

ブラケット表現と文字クラス

ブラケット表現とは、文字のリストや文字クラスを角カッコ [] で囲んだものです。ブラケット表現を使用することによって、リスト内の文字または文字範囲に対する一致を検索できます。リストの最初の文字が「^」の場合は、そのリスト以外の文字が検索されます。

以下に例を示します。

表現	一致する文字
[abc]	a、b、または c
[a-z]	a～z
[^abc]	a、b、c 以外の任意の文字
[[alpha:]]	任意の英字 (次の表を参照)

それぞれの文字クラスは、標準 C の対応する isXXX 関数と同等の文字セットを表します。たとえば、[alpha:] は、isalpha() で true が返される文字 (例: 任意の英字) を指定します。文字クラスはブラケット表現で囲む必要があります。

文字クラス	説明
[alpha:]	英字
[digit:]	数字
[alnum:]	英数字
[cntrl:]	制御文字
[blank:]	空白とタブ
[space:]	すべての空白文字
[graph:]	表示可能文字 (空白、制御文字、またはこれらと同種の文字以外のもの)
[print:]	[graph:] と同様、ただし空白文字を含む
[punct:]	句読点文字
[lower:]	アルファベット小文字
[upper:]	アルファベット大文字
[xdigit:]	16 進数 (0-9a-fA-F) で使用可能な数字

大文字と小文字が区別されない表現では、[lower:] と [upper:] は [alpha:] と同じになります。

境界一致

表現	説明
^	行の先頭
\$	行の末尾

量指定子

表現	説明
R?	1 つの R、または R なしと一致
R*	0 個以上の R と一致
R+	1 つ以上の R と一致
R{n}	厳密に n 個の R と一致
R{n,}	n 個以上の R と一致
R{n,m}	n 個以上かつ m 個以下の R と一致

R は任意の正規表現を表します。

正規表現では、「.*」は使用しないことをお勧めします。「.*」はあらゆる長さの文字と一致するため、一致が大量に検出されることによってメモリの使用率が上がり、パフォーマンスに影響する場合があります。

以下に例を示します。

正規表現「.*abc」を使用して 123456abc を検索した場合、一致結果は次のようになります。

- ・ 12345abc
- ・ 23455abc
- ・ 3456abc
- ・ 456abc
- ・ 56abc
- ・ 6abc
- ・ abc

この例では、「.*abc」の代わりに「abc」を使用することによってリソースの使用量を抑制できます。

論理演算子

表現	説明
RS	R と、それに続く S (連結)
R S	R または S のいずれか
R/S	後ろに S が続く 1 つの R
(R)	R のグループ化

R と S は正規表現を表します。

略記とメタ記号

コンテンツフィルタでは、複雑な正規表現を記述する代わりに次の略記法を使用できます。コンテンツフィルタは表現を前処理して略記を正規表現に変換します。

たとえば、{D}+は[0-9]+に変換されます。略記がブラケット ({} など) または二重引用符で囲まれている場合、InterScan MSS はその略記表現を正規表現に変換しません。

略記	説明
{D}	[0-9]
{L}	[A-Za-z]
{SP}	[(),;.\<>@[\]:]
{NUMBER}	[0-9]+
{WORD}	[A-Za-z]+
{CR}	\r
{LF}	\n
{LWSP}	[\t]

略記	説明
{CRLF}	(\r\n)
{WSP}	[\t\f]+
{ALLC}	.

コンテンツフィルタは次のメタ記号にも対応しています。略記とメタ記号との違いは、メタ記号はブラケット表現内に挿入できることです。

メタ記号	説明
\s	[[:space:]]
\S	[^[:space:]]
\d	[[:digit:]]
\D	[^[:digit:]]
\w	[[:alnum:]]
\W	[^[:alnum:]]

正規表現のリテラル文字列とエスケープ文字

正規表現で特別な意味を持つ文字(+など)を検索文字として使用する場合は、エスケープ文字\ (バックスラッシュ/円記号) を付加する必要があります。たとえば、C/C++という文字列を検索する場合は、C\ /C\+\+という表現を使用します。

場合によっては、C\ /C\+\+のようにエスケープ文字をいくつも表現に追加しなければならないこともあります。このようなときは文字列 C/C++を二重引用符で囲みます。たとえば、REG "C/C++" のようにします。この表現は元の表現と等しくなります。二重引用符で囲まれた文字 (エスケープ文字である \を除く) はリテラルとして解釈されます。次にいくつか例を示します。

表現	説明
"C/C++"	文字列 C/C++に一致 (二重引用符は含まない)

表現	説明
"Regular\x20Expression"	文字列 Regular Expression に一致 (二重引用符は含まない)。 <x20 td="" は空白文字を意味します。<=""></x20>
"[xyz]"foo"	リテラル文字列[xyz]"foo に一致

正規表現で次の表現を使用する場合は、左右の<空白>を「\x20」に変更します。

- ・ .AND.
- ・ .OR.
- ・ .NOT.
- ・ .WILD.

DLP コンプライアンステンプレート

DLP コンプライアンステンプレート (DLP) では、組織の機密データ (デジタル資産) を偶発的な開示や意図的な盗用から保護します。次のことが可能です。

- ・ 保護対象のデジタル資産の特定
- ・ 一般的なチャネル (メールや外部デバイスなど) を介したデジタル資産の転送を制限または防止するポリシーの作成
- ・ 確立された個人情報保護基準への準拠

DLP はポリシーに定義されたルールセットに照らし合わせてデータを評価します。ポリシーには、不正な転送から保護する必要のあるデータと、転送が検出された場合に実行する処理を指定します。

データ識別子の種類

デジタル資産とは、組織が不正な転送から保護する必要のあるファイルとデータを指します。デジタル資産は、次のデータ識別子を使用して定義します。

- ・ 式:特定の構造を持つデータ。詳細については、[207 ページの「式」](#)を参照してください。
- ・ ファイル属性:タイプやサイズなどのファイルのプロパティ。詳細については、[213 ページの「ファイル属性」](#)を参照してください。
- ・ キーワード:特殊な単語や語句のリスト。詳細については、[216 ページの「キーワード」](#)を参照してください。

**注意**

DLP 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。該当するテンプレートを削除してから、データ識別子を削除してください。

式

式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は通常 16 桁の数字で構成され、「nnnn-nnnn-nnnn-nnnn」という形式で表示されるため、式に基づく検出に適しています。

定義済みの式やカスタマイズされた式を使用できます。詳細については、[207 ページの「定義済みの式」](#)および[208 ページの「カスタマイズされた式」](#)を参照してください。

定義済みの式

InterScan MSS には、一連の定義済みの式が用意されています。これらの式を変更または削除することはできません。

InterScan MSS では、これらの式をパターンマッチングと数学的方程式を使用して検証します。InterScan MSS で潜在的な機密データと式が照合された後、そのデータに対して追加の検証が行われる場合もあります。

定義済みの式のリストについては、<http://esupport.trendmicro.com/solution/ja-JP/1107704.aspx> を参照してください。

定義済みの式の設定を表示する



注意

定義済みの式は変更または削除できません。

手順

1. [ポリシー] > [ポリシーオブジェクト] > [DLP データ識別子] の順に選択します。
2. [式] タブをクリックします。
3. 式の名前をクリックします。
4. 開いた画面に設定が表示されます。

カスタマイズされた式

どの定義済みの式も要件を満たさない場合は、カスタマイズされた式を作成します。

式は強力な文字列マッチングツールです。式を作成する前に、式の構文を十分に理解しておく必要があります。粗雑に記述された式は、パフォーマンスに大きな悪影響をもたらすことがあります。

式を作成する場合は、次の点を考慮してください。

- ・ 有効な式の定義方法のガイダンスについては、定義済みの式を参照してください。たとえば、日付を含む式を作成するには、「Date」プレフィックスを含む式を参照します。
- ・ InterScan MSS は Perl Compatible Regular Expressions (PCRE) で定義された式形式に準じています。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/>

- ・ シンプルな式から開始します。誤検出が発生する場合は式を変更し、さらに式を調整して検出精度を向上させます。

式を作成する際の条件を指定します。式は、InterScan MSS による情報漏えい対策ポリシーの適用に関係なく、指定した条件を満たす必要があります。さまざまな条件オプションの詳細については、[209 ページの「カスタマイズされた式の条件」](#)を参照してください。

カスタマイズされた式の条件

表 14-2. カスタマイズされた式の条件のオプション

条件	ルール	例
なし	なし	すべて - 米国国勢調査局の名前 式: <code>[^\\w]([A-Z][a-z]{1,12}(\\s? \\s?)\\s [A-Z]\\s)[A-Z][a-z]{1,12})[^\\w]</code>
特定の文字	式には、指定した文字が含まれている必要があります。 さらに、式の文字数は、最小および最大文字数以内である必要があります。	米国 - ABA 銀行ルーティング番号 式: <code>[^\\d]([0123678]\\d{8})[^\\d]</code> 文字: 0123456789 最小文字数: 9 (4~90) 最大文字数: 9 (4~90)  注意 最大文字数は最小文字数以上である必要があります。

条件	ルール	例
サフィックス	サフィックスは式の最終セグメントを意味します。サフィックスには、指定し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、式の文字数は、最小および最大文字数以内である必要があります。	すべて - 住所 式: \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 (3～90) 式の最小文字数: 25 (4～90) 式の最大文字数: 80 (4～90)  注意 式の文字数は、最小および最大文字数以内である必要があります。

条件	ルール	例
1 文字の区切り文字	式は 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。この文字は 1 バイト長にする必要があります。 さらに、区切り文字の左側の文字数は、最小および最大文字数以内である必要があります。区切り文字の右側の文字数は最大文字数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 式: <code>[^\\w.](\\w.){1,20}@[a-z0-9]{2,20}[\\.][a-z]{2,5}[a-z\\.]{0,10}[^\\w.]</code> 区切り文字: @ 左側の最小文字数: 3 (3~90) 左側の最大文字数: 15 (4~90) 右側の最大文字数: 30 (4~90)  注意 左側の最大文字数は、左側の最小文字数よりも大きくする必要があります。 右側の最大文字数は、左側の最大文字数よりも大きくする必要があります。

カスタマイズされた式を作成する

手順

1. [ポリシー] > [ポリシーオブジェクト] > [DLP データ識別子] の順に選択します。
2. [式] タブをクリックします。
3. [追加] をクリックします。
新しい画面が表示されます。
4. 式の名前を指定します。名前は 128 バイト以下で指定してください。
5. 説明を 255 バイト以下で指定します。
6. 式を指定して、大文字と小文字を区別するかどうかを設定します。

7. 表示するデータを指定します。

たとえば、ID 番号の式を作成している場合は、サンプル ID 番号を入力します。このデータは参照のみを目的として使用され、製品内の他の場所には表示されません。

8. 次のいずれかの条件を選択して、選択した条件の設定を行います (209 ページの「カスタマイズされた式の条件」参照)。

- ・ なし
- ・ 特定の文字
- ・ サフィックス
- ・ 1 文字の区切り文字

9. (オプション)式の検証ツールを選択します。

**注意**

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

10. 式を実際のデータと照合してテストします。

たとえば、国民 ID の式の場合は、有効な ID 番号を [テストデータ] テキストボックスに入力し、[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。

**注意**

テストに成功した場合のみ設定を保存します。データを検出できない式は、システムリソースを浪費し、パフォーマンスの低下を招く可能性があります。

**注意**

必要に応じて、定義済みの式をコピーして編集し、カスタマイズされた式を作成します。

カスタマイズされた式をインポートする

式を含む適切な形式の.xml ファイルがある場合は、このオプションを使用します。現在アクセスしている InterScan MSS サーバ、または別の InterScan MSS サーバから式をエクスポートすることによりファイルを生成します。

手順

1. [ポリシー] > [ポリシーオブジェクト] > [DLP データ識別子] の順に選択します。
2. [式] タブをクリックします。
3. [インポート] をクリックし、式が含まれる.xml ファイルを探します。
4. [インポート] をクリックします。

インポートの完了を示すメッセージが表示されます。

**注意**

カスタマイズされた式はそれぞれ、.xml ファイルの名前フィールドで識別します。この名前は一意の内部名で、管理コンソールには表示されません。

既存の式をカスタマイズした式がファイルに含まれる場合、InterScan MSS では既存の式が上書きされます。既存の式を保持するには、式ファイルをインポートする前に、既存の式の内部名を変更します。

ファイル属性

ファイル属性とは、ファイル固有のプロパティのことを指します。データ識別子を定義する際には、ファイルタイプとファイルサイズの2つの属性を使用します。たとえば、ソフトウェア開発会社でソフトウェアインストールパッケージの共有を、研究開発部門でソフトウェアの開発とテストを担当す

るメンバーのみに制限するとします。この場合、InterScan MSS の管理者は、10～40MB の実行可能ファイルを研究開発以外の部門に送信することをブロックするポリシーを作成できます。

ファイル属性を他の DLP データ識別子と組み合わせて、機密ファイルの検出をさらに絞り込むことをお勧めします。これは、ファイル属性自体は機密ファイルの識別子としては強力ではないためです。前述の例をそのまま採用すると、他の部門で共有されているサードパーティ製ソフトウェアのインストールパッケージはブロックされない可能性が高くなります。

サポート対象のすべてのファイルタイプのリストについては、<http://esupport.trendmicro.com/solution/ja-JP/1107704.aspx> を参照してください。

ファイル属性リストを作成する

手順

1. [ポリシー] > [ポリシーオブジェクト] > [DLP データ識別子] の順に選択します。
2. [ファイル属性] タブをクリックします。
3. [追加] をクリックします。
新しい画面が表示されます。
4. ファイル属性リストの名前を入力します。名前は 128 バイト以下で指定してください。
5. 説明を 255 バイト以下で指定します。
6. [除外フラグ] の横にある、次のいずれかを選択します。
 - ・ 除外: 選択したファイルタイプが除外されます。
 - ・ 除外なし: 選択したファイルタイプが含まれます。
7. 実際のファイルタイプを選択します。
8. 目的のファイルタイプがリストにない場合は、[ファイル拡張子] を選択して、ファイルタイプの拡張子を指定します。InterScan MSS は指定された拡張子を持つファイルを確認しますが、その実際のファイルタイプは確

認めません。ファイル拡張子を指定する際のガイドラインは次のとおりです。

- ・ 拡張子の先頭にはアスタリスク (*) を使用し、その後にピリオド (.) を指定してから拡張子を入力します。このアスタリスクはワイルドカードで、ファイルの実際の名前を表しています。たとえば、*.pol は 12345.pol と test.pol に一致します。
- ・ ワイルドカードは拡張子に含めることができます。疑問符 (?) は 1 文字、アスタリスク (*) は複数の文字を表します。次の例を参照してください。
 - *.m は ABC.dem、ABC.prm、および ABC.sdcm のファイルと一致します。
 - *.m*r は ABC.mgdr、ABC.mtp2r、および ABC.mdmr のファイルと一致します。
- ・ 拡張子の末尾にアスタリスクを追加する際は注意してください。ファイル名の一部や、無関係な拡張子と一致する可能性があります。たとえば、*.do* は abc.doctor_john.jpg や abc.donor12.pdf と一致します。
- ・ ファイル拡張子はセミコロン (;) で区切ります。セミコロンの後にスペースを追加する必要はありません。

9. 最小および最大ファイルサイズをバイト単位で指定します (1 バイト～2GB)。
10. [保存] をクリックします。



注意

必要に応じて、既存のファイル属性リストをコピーして編集し、別のファイル属性リストを作成します。

ファイル属性リストをインポートする

ファイル属性リストを含む適切な形式の .xml ファイルがある場合は、このオプションを使用します。現在アクセスしている InterScan MSS サーバ、または

別の InterScan MSS サーバからファイル属性リストをエクスポートすることによりファイルを生成します。

手順

1. [ポリシー] > [ポリシーオブジェクト] > [DLP データ識別子] の順に選択します。
2. [ファイル属性] タブをクリックします。
3. [インポート] をクリックし、ファイル属性リストが含まれる .xml ファイルを探します。
4. [インポート] をクリックします。

インポートの完了を示すメッセージが表示されます。



注意

ファイル属性リストはそれぞれ、.xml ファイルの名前フィールドで識別します。この名前は一意の内部名で、管理コンソールには表示されません。

すでに存在するファイル属性リストがファイルに含まれる場合、InterScan MSS では既存のファイル属性リストが上書きされます。既存のファイル属性リストを保持するには、ファイル属性ファイルをインポートする前に、既存のファイル属性リストの内部名を変更します。

キーワード

キーワードは特別な単語または語句です。特定のタイプ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。たとえば、診断書で使用されることのある「予後」、「血液型」、「予防接種」、「医師」などがキーワードとなります。診断書ファイルの送信を防ぐため、DLP ポリシーでこれらのキーワードを使用して、これらのキーワードが含まれるファイルをブロックするように InterScan MSS を設定できます。

一般的に使用される用語を組み合わせる意味のあるキーワードを作成します。たとえば、ソースコードに見られる「end」、「read」、「if」、「at」を組み合わせ、「END-IF」、「END-READ」、「AT END」などのキーワードを作成します。

定義済みのキーワードリストやカスタマイズされたキーワードリストを使用できます。詳細については、217 ページの「定義済みのキーワードリスト」および218 ページの「カスタマイズされたキーワードリスト」を参照してください。

定義済みのキーワードリスト

InterScan MSS には、一連の定義済みのキーワードリストが用意されています。これらのキーワードリストを変更または削除することはできません。各リストには、テンプレートでポリシー違反を実行するかどうかを決定する組み込みの条件が備わっています。

InterScan MSS の定義済みのキーワードリストの詳細については、<http://esupport.trendmicro.com/solution/ja-JP/1107704.aspx> を参照してください。

キーワードリストの使用方法

キーワード数の条件

キーワードリストにはそれぞれキーワード数に関する条件が含まれており、この条件に従ってドキュメント内に一定数のキーワードが存在すると、違反が発生したと見なされます。

キーワード数の条件には、次の値が含まれます。

- ・ すべて:リスト内のすべてのキーワードがドキュメントに含まれている必要があります。
- ・ 任意のキーワード:リスト内のいずれかのキーワードがドキュメントに含まれている必要があります。
- ・ (x)文字以内のキーワード:指定した数以上のキーワードがドキュメントに含まれている必要があります。指定した数よりドキュメント内のキーワードが多い場合は、違反が発生したことになります。

間隔の条件

一部のリストには、違反検出の条件に「間隔」が含まれます。「間隔」とは、あるキーワードの最初の文字と、別のキーワードの最初の文字との間の文字数を表します。次の例で考えます。

First Name:_John_ Last Name:_Smith_

[フォーム - 名、姓] リストには、50 文字の「間隔」条件があり、よく使用されるフォームフィールドである「名」と「姓」が含まれています。この例では、「名」の「F」と「姓」の「L」の間の文字数が 18 と等しいので、違反が発生したと見なされます。

違反が発生しないエントリの例については、次の例を考えます。

The first name of our new employee from Switzerland is John.His last name is Smith.

この例では、「名」の「f」と「姓」の「l」の間の文字数が 61 文字です。これは間隔のしきい値を超えるため、違反が発生したとは見なされません。

カスタマイズされたキーワードリスト

どの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、カスタマイズされたキーワードリストを作成します。

キーワードリストは、InterScan MSS による情報漏えい対策ポリシーの適用に関係なく、指定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いずれかの条件を選択します。

- ・ 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ているキーワード

条件のルールの詳細については、[218 ページの「カスタマイズされたキーワードリストの条件」](#)を参照してください。

カスタマイズされたキーワードリストの条件

表 14-3. キーワードリストの条件

条件	ルール
任意のキーワード	キーワードリストの 1 つ以上のキーワードがファイルに含まれる必要があります。

条件	ルール
すべてのキーワード	キーワードリストのすべてのキーワードがファイルに含まれる必要があります。
<x> 文字以内のすべてのキーワード	キーワードリストのすべてのキーワードがファイルに含まれる必要があります。さらに、最初のキーワードの先頭から最後のキーワードの先頭までの文字数が、<x> 文字以内である必要があります。 たとえば、3 つのキーワードが WEB、DISK、および USB で、指定した文字数が 20 であるとしめます。 すべてのキーワードが DISK、WEB、および USB の順に検出される場合、「D」(DISK の D) から「U」(USB の U) の間の文字数は 20 文字以内である必要があります。 次のデータは条件に一致します:DISK####WEB###USB 次のデータは条件に一致しません:DISK*****WEB****USB(「D」から「U」までが 21 文字) 文字数を決定する際は、通常、10 などの小さな数では検索速度が速くなりますが、対象範囲が比較的小さくなることに注意してください。これにより、特に大きなファイルでは、機密データの検出率が低下する可能性があります。数字が大きくなるほど対象範囲も広くなりますが、検索速度が低下することがあります。
合計スコアがしきい値を超えているキーワード	キーワードリストの 1 つ以上のキーワードがファイルに含まれる必要があります。キーワードが 1 つだけ検出された場合は、そのスコアがしきい値を超えている必要があります。キーワードが複数ある場合は、その合計スコアがしきい値を超えている必要があります。 各キーワードに 1～10 のスコアを割り当てます。人事部の「昇給」など、機密性の高い単語やフレーズには比較的高いスコアを指定する必要があります。単体では重要度がそれほど高くない単語や語句には、比較的低いスコアを指定できます。 しきい値を設定する際は、キーワードに割り当てたスコアを考慮します。たとえば、キーワードが 5 つあり、そのうち 3 つのキーワードの優先度が高い場合、しきい値は、優先度が高い 3 つのキーワードの合計スコア以下に設定できます。これは、これらの 3 つのキーワードが検出されることで、そのファイルは十分に機密であるといえるためです。

キーワードリストを作成する

手順

1. [ポリシー] > [ポリシーオブジェクト] > [DLP データ識別子] の順に選択します。
2. [キーワードリスト] タブをクリックします。
3. [追加] をクリックします。
新しい画面が表示されます。
4. キーワードリストの名前を指定します。名前は 128 バイト以下で指定してください。
5. 説明を 255 バイト以下で指定します。
6. 次のいずれかの条件を選択して、選択した条件の設定を行います。
 - ・ 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ているキーワード
7. キーワードを手動でリストに追加するには
 - a. 3~40 バイトのキーワードを指定して、大文字と小文字を区別するかどうかを設定します。
 - 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て [削除] をクリックします。
9. [保存] をクリックします。

**注意**

必要に応じて、定義済みのキーワードリストをコピーして編集し、カスタマイズされたキーワードリストを作成します。

キーワードリストをインポートする

キーワードリストを含む適切な形式の.xml ファイルがある場合は、このオプションを使用します。現在アクセスしている InterScan MSS サーバ、または別の InterScan MSS サーバからキーワードリストをエクスポートすることによりファイルを生成します。

手順

1. [ポリシー] > [ポリシーオブジェクト] > [DLP データ識別子] の順に選択します。
2. [キーワードリスト] タブをクリックします。
3. [インポート] をクリックし、キーワードリストが含まれる.xml ファイルを探します。
4. [インポート] をクリックします。

インポートの完了を示すメッセージが表示されます。

**注意**

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

既存のキーワードリストをカスタマイズしたキーワードリストがファイルに含まれる場合、InterScan MSS では既存のキーワードリストが上書きされます。既存のキーワードリストを保持するには、キーワードファイルをインポートする前に、既存のキーワードリストの内部名を変更します。

DLP コンプライアンステンプレート

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

たとえば、あるファイルが Microsoft Word ファイル (ファイル属性) であり、特定の法律用語 (キーワード) を含み、さらに「雇用契約」ポリシーの適用される特定の ID 番号 (式) を含む必要があるとします。このポリシーでは、人事部の職員が、従業員が署名できるようにファイルを印刷して渡すことができます。メールなど、それ以外のすべての伝達方法はブロックされます。

DLP データ識別子を設定している場合は、必要に応じて独自のテンプレートを作成します。定義済みのテンプレートを使用することもできます。詳細については、[222 ページの「カスタマイズされた DLP テンプレート」](#) および [222 ページの「定義済み DLP テンプレート」](#) を参照してください。



注意

DLP ポリシーで使用されているテンプレートを削除することはできません。テンプレートを削除するには、最初にポリシーから削除します。

定義済み DLP テンプレート

トレンドマイクロ製品には、さまざまな規制に合わせて使用できる一連の定義済みテンプレートが用意されています。これらのテンプレートを変更または削除することはできません。

すべての定義済みテンプレートの用途と、保護対象データの例については、<http://esupport.trendmicro.com/solution/ja-JP/1107704.aspx> を参照してください。

カスタマイズされた DLP テンプレート

データ識別子を設定している場合は、独自のテンプレートを作成します。テンプレートとは、データ識別子と論理演算子 (および、または、除外) を組み合わせて条件文を作成したものです。

条件文と論理演算子の使用方法の詳細および使用例については、[223 ページの「条件文と論理演算子」](#)を参照してください。

条件文と論理演算子

InterScan MSS では、条件文は左から右に向かって評価されます。条件文を設定する際は、論理演算子を慎重に使用してください。正しく使用しないと、条件文の誤りにより予期しない結果を招く場合があります。

次の表の例を参照してください。

表 14-4. 条件文の例

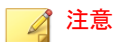
条件文	解釈と例
[データ識別子 1] And [データ識別子 2] Except [データ識別子 3]	ファイルは [データ識別子 1] と [データ識別子 2] に合致し、[データ識別子 3] には合致しない必要があります。 例: ファイルは [Adobe PDF ドキュメント] であり、[メールアドレス] を含みますが、[キーワードリストのすべてのキーワード] を含まないものである必要があります。
[データ識別子 1] Or [データ識別子 2]	ファイルは [データ識別子 1] または [データ識別子 2] に合致する必要があります。 例: ファイルは [Adobe PDF ドキュメント] または [Microsoft Word ドキュメント] である必要があります。
Except [データ識別子 1]	ファイルは [データ識別子 1] に合致しない必要があります。 例: ファイルは [マルチメディアファイル] でない必要があります。

表の最後の例で説明しているとおり、ファイルが条件文のすべてのデータ識別子と合致しない必要がある場合は、条件文の最初のデータ識別子に演算子「Except」を指定できます。多くの場合、最初のデータ識別子には演算子を指定しません。

テンプレートを作成する

手順

1. [ポリシー] > [ポリシーオブジェクト] > [DLP コンプライアンステンプレート] の順に選択します。
2. [追加] をクリックします。
新しい画面が表示されます。
3. テンプレートの名前を指定します。名前は 128 バイト以下で指定してください。
4. 説明を 255 バイト以下で指定します。
5. 次のいずれかを使用して、デジタル資産の定義を指定します。
 - ・ 式: [式] を選択し、式名を選択して、InterScan MSS でネットワークからメッセージが流出するのをブロックする前にその式が検出される回数を設定します。
 - ・ キーワード: [キーワード] を選択してキーワードリストを選択します。InterScan MSS では、選択したリスト内のキーワードがファイルに含まれる場合、そのファイルの送信を防ぎます。
6. エントリをさらに追加するには、[+] をクリックします。
7. 各エントリの論理演算子を選択します。



注意

条件文を設定する際は、論理演算子を慎重に使用してください。正しく使用しないと、条件文の誤りにより予期しない結果を招く場合があります。正しい使用例については、[223 ページの「条件文と論理演算子」](#)を参照してください。

8. [追加] をクリックします。
[コンプライアンステンプレートの定義] リストにデジタル資産の定義が表示されます。

9. 必要に応じて複数のデジタル資産の定義を追加します。

10. [保存] をクリックします。

コンプライアンステンプレートがコンプライアンステンプレートリストに表示されます。

テンプレートをインポートする

テンプレートを含む適切な形式の.xml ファイルがある場合は、このオプションを使用します。現在アクセスしている InterScan MSS サーバ、または別の InterScan MSS サーバからテンプレートをエクスポートすることによりファイルを生成します。

手順

1. [ポリシー] > [ポリシーオブジェクト] > [DLP コンプライアンステンプレート] の順に選択します。
2. [インポート] をクリックし、テンプレートが含まれる.xml ファイルを探します。
3. [インポート] をクリックします。

インポートの完了を示すメッセージが表示されます。



注意

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

既存テンプレートをカスタマイズしたテンプレートがファイルに含まれる場合、InterScan MSS では既存テンプレートが上書きされます。既存のテンプレートを保持するには、テンプレートファイルをインポートする前に、既存のテンプレートの内部名を変更します。

ポリシー通知

受信者またはメール管理者に、InterScan MSS がメッセージの添付ファイルに対して処理を実行したことや、メッセージが InterScan MSS ルールの検索条件に違反していることを通知するには、通知を送信します。

通知は、ポリシー作成時にも作成できますが、ポリシー作成を開始する前に作成しておくことをお勧めします。

ポリシー通知リストへの追加の詳細については、[227 ページの「ポリシー通知を追加または変更する」](#)を参照してください。

ポリシー通知を送信する

手順

1. ポリシーを作成または変更します。
 - ・ 新しいルールの作成手順については、[259 ページのポリシーの設定](#)を参照してください。
 - ・ 既存ルールの変更手順については、[323 ページの既存のポリシーの設定](#)を参照してください。
2. ポリシーの変更時または作成時に、[処理の選択] 画面の [監視] で [ポリシー通知の送信] をクリックします。

次の 2 つのリストボックスが表示されている [通知] 画面が開きます。

- ・ 使用可能: 通知メッセージは利用可能ですが、現在使用されていません。
 - ・ 選択済み: 通知メッセージは現在使用中です。
3. 通知を追加または変更します。
 4. [使用可能] リストで、有効にする通知をクリックします。
 5. [>>] をクリックします。
- 通知が [選択済み] リストに表示されます。

通知を利用可能な状態にしておき、InterScan MSS で一時的に使用しないようにするには、選択されたリストで通知をクリックしてから [<<] をクリックします。

6. [保存] をクリックして、ポリシーの作成または変更を続行します。

ポリシー通知を追加または変更する

ポリシー通知は、[ポリシー通知] 画面で、またはポリシーの作成時や変更時に作成します。

手順

1. [ポリシー] > [ポリシー通知] の順に選択します。

[ポリシー通知] 画面が表示されます。

ポリシー通知



ポリシー内で共通ポリシーオブジェクトとして使用する通知です。

追加 コピー 削除		
☐	ポリシー通知名:	ポリシーで使用
☐	セキュリティ設定通知	1
☐	検索の除外通知	1
☐	メッセージ復号化失敗通知	1

2. [追加] をクリックします。

[ポリシー通知の追加] 画面が表示されます。

ポリシー通知 

ポリシー通知 > ポリシー通知の追加

通知設定

ポリシー通知名:

差出人:

宛先:

☐ 元のメール送信者

☐ 元のメール受信者

メール

件名:

メッセージ: ☐ メッセージの添付 [変数リスト](#)

SNMPTラップ ☒ 禁止 ☐

メッセージ:

3. 次の項目を設定します。

- ・ 名前: 通知のわかりやすい名前を指定します。
- ・ 差出人: 送信者メールアドレスを指定します。
- ・ 宛先: 受信者メールアドレスを指定し、[元のメール送信者] と [元のメール受信者] の横にあるチェックボックスの両方、またはいずれかをオンにします。各アドレスはセミコロン (;) で区切ります。
- ・ 件名: 通知の件名を指定します。

- ・ メッセージ: 通知メッセージを指定します。
- 4. 元のメッセージを通知メッセージの添付ファイルとして送信するには、
[メッセージの添付] の横にあるチェックボックスをオンにします。
- 5. メッセージに挿入できる変数の種類を表示するには、[変数リスト] をクリックします。
- 6. SNMP トラップを送信するには、以下を設定します。
 - a. 次のいずれかをクリックします。
 - ・ 無効 (最初のラジオボタン): トラップ ID を送信しないようにします。
 - ・ 2 番目のラジオボタン: 初期設定の SNMP トラップのいずれかを選択します。
 - ・ 3 番目のラジオボタン: カスタムのトラップ ID を指定します。
 - b. メッセージ: 通知メッセージを指定します。
- 7. [保存] をクリックします。

ポリシーの作成時や変更時にポリシー通知を作成または変更する

手順

1. ポリシーを作成または変更します。
 - ・ 新しいルールを作成手順については、[259 ページのポリシーの設定](#)を参照してください。
 - ・ 既存ルールの変更手順については、[323 ページの既存のポリシーの設定](#)を参照してください。
2. [処理の選択] 画面の [監視] で [ポリシー通知の送信] をクリックします。
次の 2 つのリストボックスが表示されている [通知] 画面が開きます。

- ・ 使用可能: 通知メッセージは利用可能ですが、現在使用されていません。
 - ・ 選択済み: 通知メッセージは現在使用中です。
3. [追加] または [編集] をクリックします。
通知の設定画面が表示されます。
 4. メール通知を送信するには、以下を設定します。
 - ・ 名前: 通知のわかりやすい名前を指定します。
 - ・ 差出人: 送信者メールアドレスを指定します。
 - ・ 宛先: 受信者メールアドレスを指定し、[元のメール送信者] と [元のメール受信者] の横にあるチェックボックスの両方、またはいずれかをオンにします。各アドレスはセミicolon (;) で区切ります。
 - ・ 件名: 通知の件名を指定します。
 - ・ メッセージ: 通知メッセージを指定します。
 5. 元のメッセージを通知メッセージの添付ファイルとして送信するには、[メッセージの添付] の横にあるチェックボックスをオンにします。
 6. メッセージに挿入できる変数の種類を表示するには、[変数リスト] をクリックします。
 7. SNMP トラップを送信するには、以下を設定します。
 - a. 次のいずれかをクリックします。
 - ・ 無効 (最初のラジオボタン): トラップ ID を送信しないようにします。
 - ・ 2 番目のラジオボタン: 初期設定の SNMP トラップのいずれかを選択します。
 - ・ 3 番目のラジオボタン: カスタムのトラップ ID を指定します。
 - b. メッセージ: 通知メッセージを指定します。
 8. [保存] をクリックします。
-

スタンプ

受信者に、InterScan MSS がメッセージの添付ファイルに対して処理を実行したことや、メッセージがルールを検索条件に違反していることを通知するには、メッセージ本文の先頭または最後にスタンプを追加します。



ヒント

本来の受信者が最終的に受信するメッセージに対してのみスタンプを追加します。検索条件に違反するメッセージを削除するルールを設定している場合は、スタンプの追加は必要ありません。

ポリシーでスタンプを使用する

手順

1. ポリシーを作成または変更します。
 - ・ 新しいルールの作成手順については、[259 ページのポリシーの設定](#)を参照してください。
 - ・ 既存ルールの変更手順については、[323 ページの既存のポリシーの設定](#)を参照してください。
2. [処理の選択] 画面でポリシーを作成または変更する際に、[変更] にある [本文にスタンプを挿入] または [標準メッセージにスタンプを挿入] の横のチェックボックスをオンにします。

スタンプを作成する

スタンプは、[スタンプ] 画面で、またはポリシーの作成時や変更時に作成します。



注意

スタンプは、ポリシー作成時にも作成できますが、ポリシー作成を開始する前に作成しておくことをお勧めします。

手順

1. [ポリシー] > [スタンプ] の順に選択します。

[スタンプ] 画面が表示されます。

スタンプ



スタンプは処理ページのポリシー内で共通のポリシーオブジェクトとして使用されます。

追加 コピー 削除	
☐ スタンプ名	ポリシーで使用
☐ 検索不能な添付ファイル	1

2. [追加] をクリックするか、[スタンプ] リストから編集するスタンプを選択します。

スタンプの画面が表示されます。

スタンプ



スタンプ > 新しいスタンプ

名前:

挿入位置

☒ メッセージ本文の末尾
 ☐ メッセージ本文の先頭

テキスト: 変数リスト

☒ TNEFエンコードされたメッセージおよびデジタル署名されたメッセージにスタンプを挿入しない

3. [名前] の横に、スタンプの名前を指定します。
4. [挿入位置] の横で、[メッセージ本文の末尾] または [メッセージ本文の先頭] をクリックします。

5. [テキスト] にメッセージを指定します。メッセージに挿入できる変数の種類を表示するには、[変数リスト] をクリックします。
6. TNEF (Transport Neutral Encapsulation Format) でエンコードされたメッセージやデジタル署名されたメッセージを破損する危険性を回避するには、[TNEF エンコードされたメッセージおよびデジタル署名されたメッセージにスタンプを挿入しない] を選択します。
7. [保存] をクリックして、[スタンプ] 画面に戻ります。

ポリシーの作成時または変更時にスタンプを作成する

手順

1. ポリシーを作成または変更します。
 - ・ 新しいルールを作成手順については、[259 ページのポリシーの設定](#)を参照してください。
 - ・ 既存ルールの変更手順については、[323 ページの既存のポリシーの設定](#)を参照してください。
2. [処理の選択] 画面の [変更] で、[本文にスタンプを挿入] または [標準メッセージにスタンプを挿入] の横の [編集] をクリックします。

[スタンプ] 画面が開き、使用可能なスタンプが表示されます。
3. 新しいスタンプを追加するには、[追加] をクリックします。既存のスタンプを変更するには、リストボックスで対象のスタンプをクリックし、[編集] をクリックします。

編集画面が表示されます。
4. [名前] の横に、スタンプの名前を指定します。
5. [挿入位置] の横で、[メッセージ本文の末尾] または [メッセージ本文の先頭] をクリックします。
6. [テキスト] にメッセージを指定します。メッセージに挿入できる変数の種類を表示するには、[変数リスト] をクリックします。

7. TNEF でエンコードされたメッセージやデジタル署名されたメッセージを破損する危険性を回避するには、[TNEF エンコードされたメッセージおよびデジタル署名されたメッセージにスタンプを挿入しない] を選択します。
 8. [保存] をクリックして、[スタンプ] 画面に戻ります。
 9. [完了] をクリックします。
-

DKIM 承認済みリスト

DKIM (DomainKeys Identified Mail) は署名/暗号ベースのメール認証で、インターネット転送時にメッセージを検証するための方法を提供します。InterScan MSS は、メッセージが自称する送信元から送信されていることを検証することによって、ネットワークをスパムメールやフィッシングから保護します。検証されたメッセージは、スパムメールとしてマークされたり検索されたりすることはありません。これにより、安全であることが判明している送信元からのメッセージを検索する必要性が低減し、同時に誤検出も減少します。

DKIM 承認済みリストを有効にする

手順

1. [ポリシー] > [承認済みリスト] の順に選択します。
[DKIM 承認済みリスト] タブが表示されます。

2. [ポリシーで使用するために DKIM 承認済みリストを有効にする] チェックボックスをオンにします。
3. 安全であることが判明しているドメインをリストに入力します。

手動の場合

- a. ドメイン名を指定します。
- b. [追加] をクリックします。

リストをインポートする場合



注意

DKIM 承認済みリストにテキストファイルをインポートする場合は、1 行に 1 つずつドメインを記載します。

- a. [インポート] をクリックします。
[DKIM ホワイトリストのインポート] が表示されます。
- b. [参照] をクリックして、インポートするファイルの場所を探します。

- c. 次のいずれかを選択します。
 - ・ 現在のリストとマージ
 - ・ 現在のリストを上書き
 - d. [インポート] をクリックします。
4. [保存] をクリックします。
-

Web レピュテーション承認済みリスト

Web レピュテーションは、メッセージに埋め込まれた不正な URL からネットワークユーザを保護します。Web レピュテーションでは、メッセージ内の URL が検索され、トレンドマイクロの Web レピュテーションデータベースに保存されている既知の不正 URL と比較されます。Web レピュテーション承認済みリストを利用することで、管理者は、安全であることが判明している URL の検索とブロックを回避できます。

Web レピュテーション承認済みリストを有効にする

手順

1. ウイルス対策ポリシーでない「その他」のポリシーを作成して変更します。
 - ・ 新しいルールの作成手順については、[259 ページのポリシーの設定](#)を参照してください。
 - ・ 既存ルールの変更手順については、[323 ページの既存のポリシーの設定](#)を参照してください。
2. [検索条件の選択] 画面の [Web レピュテーション] で、[Web レピュテーション設定] をクリックします。

[Web レピュテーション設定] 画面が表示されます。
3. [Web レピュテーション承認済みリストの使用を有効にする] チェックボックスをオンにします。

4. [保存] をクリックします。
[手順 2: 検索条件の選択] 画面が表示されます。
5. ポリシーの設定を続行します。

Web レピュテーション承認済みリストに追加する

Web レピュテーション承認済みリストに追加されたドメインは、InterScan MSS の検索対象になりません。安全であることが判明しているドメインのみを追加してください。

手順

1. [ポリシー] > [承認済みリスト] の順に選択します。
2. [Web レピュテーション承認済みリスト] タブをクリックします。
[Web レピュテーション承認済みリスト] 画面が表示されます。

承認済みリスト



3. Web レピュテーション承認済みリストへの追加には、次のいずれかの方法を使用します。

手動の場合

- a. ドメインを指定します。例:*.trendmicro.com.
- b. [追加>>] をクリックします。

リストをインポートする場合

**注意**

Web レピュテーション承認済みリストにテキストファイルをインポートする場合は、1 行に 1 つずつドメインを記載します。

- a. [インポート] をクリックします。
[Web レピュテーション承認済みリストのインポート] が表示されます。
 - b. [参照] をクリックして、インポートするファイルの場所を探します。
 - c. 次のいずれかを選択します。
 - ・ 現在のリストとマージ
 - ・ 現在のリストを上書き
 - d. [インポート] をクリックします。
4. [保存] をクリックします。
-

第 15 章

内部アドレスの設定

この章では、内部アドレスを設定する手順について説明します。

この章の内容は次のとおりです。

- ・ 240 ページの「内部アドレスを設定する」
- ・ 243 ページの「ユーザまたはグループを検索する」
- ・ 244 ページの「LDAP ユーザまたはグループを検索する」

内部アドレスを設定する

InterScan MSS では、レポートとルールを作成する際に、どのポリシーとイベントが受信用であり、どれが送信用であるかを判断するために、内部アドレスが使用されます。

- ・ 受信メッセージの場合は、内部アドレスの範囲内にある、受信者のアドレスを指定します。以下に例を示します。内部アドレスが `example.com` の場合、有効な受信者のアドレスには `jim@example.com`、`bob@example.com` などがあります。
- ・ 送信メッセージの場合は、内部アドレスの範囲内にある、送信者のアドレスを指定します。以下に例を示します。内部アドレスが `example.com` の場合、有効な送信者のアドレスには `jim@example.com`、`bob@example.com` などがあります。
- ・ 受信メッセージと送信メッセージの両方の場合において、ルールは、メールアドレスに一致する受信者または送信者に適用されます。

内部アドレスを設定する

手順

1. [ポリシー] > [内部アドレス] の順に選択します。

[内部アドレス] 画面が表示されます。

内部アドレス



注意: 「既知の」一連のユーザまたはドメインを指定してください。これらには、レポートとルールを作成するための受信アドレスと送信アドレスも含める必要があります。

内部ドメインおよびユーザグループ

ドメインの入力
(例: example.com)

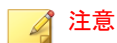
>>

選択済み

test.com	

2. [内部ドメインおよびユーザグループ] で、ドロップダウンボックスから次のいずれかを選択します。

- ・ ドメインの入力: メインを指定して [>>] をクリックします。「@」やメールアドレスのユーザ名の部分を使用しないでください。たとえば、example や example1.example2 は有効ですが、user@example は無効です。



注意

ドメイン名にはワイルドカードを使用できます。たとえば、*.example.com を指定すると、example.com のすべてのサブドメインが含まれます。ただし、ドメインに2つ以上のワイルドカードを使用することはできません。*.example.com や*.*は無効です。

- ・ LDAP グループの検索: LDAP グループを選択する画面が表示されます。個別の LDAP ユーザ名ではなく、LDAP グループ名をテキストボックスに指定して、[検索] をクリックします。検索結果がリスト

ボックスに表示されます。検索された LDAP グループを [選択済み] リストに追加するには、その LDAP グループをクリックしてから [>] をクリックします。

**注意**

内部アドレスに対して LDAP グループを検索する際、Microsoft Active Directory または Sun iPlanet Directory を LDAP サーバとして指定している場合は、LDAP グループの先頭または末尾、あるいはその両方にワイルドカードを使用できます。使用できるワイルドカードの例は、A*、*A、および*A*です。Domino を LDAP サーバとして選択している場合は、末尾にしかワイルドカードを使用できません。使用できないワイルドカードの例は、*A および*A*です。

3. ファイルからドメインをインポートするには、[インポート] をクリックして、ファイルを選択します。

**ヒント**

最適な結果が得られるようにするには、指定したドメインとそのすべてのサブドメインの両方をインポートします。

ドメインリストのテキストファイルのサンプルの内容は、次のとおりです。

- ・ example.com: 指定したドメインがインポートされます。
- ・ *.example.com: すべてのサブドメインがインポートされます。
- ・ example.org: 指定したドメインがインポートされます。

**注意**

インポートファイルは、1 行に 1 つのドメインが記載されたテキストファイルにする必要があります。ドメインの指定時は、ワイルドカードを使用できます。

4. [保存] をクリックします。

内部アドレスをエクスポートする

手順

1. [ポリシー] > [内部アドレス] の順に選択します。
[内部アドレス] 画面が表示されます。
 2. [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] ダイアログボックスが表示されます。
 3. [保存] をクリックします。
[名前を付けて保存] ダイアログボックスが表示されます。
 4. 場所とファイル名を指定します。
 5. [保存] をクリックします。
-

ユーザまたはグループを検索する

ユーザまたはグループ別にルールリストのフィルタを実行する際には、次のいずれかの項目を選択できます。

- ・ メールアドレス
- ・ LDAP グループ
- ・ アドレスグループ

手順

1. [ポリシー] > [ポリシーリスト] の順に選択します。
2. [フィルタ] の横の最後のドロップダウンリストから、[ユーザまたはグループの検索] を選択します。
[ユーザまたはグループのポリシーの検索] 画面が表示されます。

3. [送信者] および [受信者] のいずれかまたは両方のチェックボックスをオンにします。
 4. ドロップダウンボックスから、次のいずれかを選択します。
 - ・ メールアドレス
 - ・ LDAP ユーザまたはグループ
 - ・ アドレスグループ
 5. ボックスに、検索するキーワードを指定します。
 6. [選択] をクリックします。
-

LDAP ユーザまたはグループを検索する

ポリシーのルートを指定する際に、個々のメールアドレスまたはアドレスグループを入力せずに、LDAP ユーザまたはグループを検索することもできます。

InterScan MSS でサポートされる LDAP サーバの種類のシステム要件を確認します。

- ・ IBM Lotus Domino 6.0
- ・ Microsoft Active Directory 2000、2003、2008 R2、2012、および 2016
- ・ Sun iPlanet Directory 5.2
- ・ OpenLDAP 2.4

新規ポリシーを作成する際に LDAP ユーザまたはグループを追加するには、次の手順に従ってください。

手順

1. [ポリシー] > [ポリシーリスト] の順に選択します。
2. [追加] をクリックします。

- ドロップダウンリストから [ウイルス対策] または [その他] を選択し、ウイルス対策ルールまたはその他の脅威に対するルールを個別に作成します。
- [受信者] または [送信者] リンクをクリックします。
[アドレスの選択] 画面が表示されます。

次の宛先への受信メッセージ



ルールの追加 > 次の宛先への受信メッセージ

保存 キャンセル

アドレスの選択

☐ すべてのユーザ
 ☒ 選択したアドレスのいずれか

メールアドレスの入力

メールアドレスの入力
 10の宛先への追加またはグループの検索
 アドレスグループの選択

追加 >

選択済み

保存 キャンセル

- ドロップダウンリストから [LDAP ユーザまたはグループの検索] を選択します。

次の宛先への受信メッセージ



ルールの追加 > 次の宛先への受信メッセージ

保存 キャンセル

アドレスの選択

☐ すべてのユーザ
☒ 選択したアドレスのいずれか

LDAPユーザまたはグループの検索

追加 >

選択済み

保存 キャンセル

- 検索する LDAP ユーザまたはグループを指定します。

注意

- 検索する際には、アスタリスク (*) ワイルドカードを使用できます。
[337 ページの「アスタリスクワイルドカードを使用する」](#)を参照してください。
- 内部アドレスを追加する際には、LDAP グループも検索できます。
[240 ページの「内部アドレスを設定する」](#)を参照してください。

- [検索] をクリックします。
- InterScan MSS では、LDAP サーバ上に一致するレコードが存在する場合、LDAP ユーザまたはグループが表示されます。
- そのユーザまたはグループを選択して [追加] をクリックし、それを受信者または送信者のリストに追加します。

第 16 章

Trend Micro Smart Protection の使用

この章では、Trend Micro Smart Protection ソリューションの概要と、このソリューションに必要な環境の設定方法について説明します。

- ・ [42 ページの「トレンドマイクロの Smart Protection について」](#)
- ・ [251 ページの「Smart Protection ソース」](#)
- ・ [254 ページの「検索方法を選択する」](#)
- ・ [256 ページの「Web レピュテーションサービスを使用する」](#)

トレンドマイクロの Smart Protection について

トレンドマイクロは、Smart Protection サービスを介した次世代のコンテンツセキュリティを提供します。クラウド内で脅威情報を処理することにより、必要なシステムリソースを減らし、時間のかかる署名のダウンロードをなくします。

Smart Protection サービスには以下が含まれます。

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では、検索エンジンがローカルにあるパターンファイルではなく、Trend Micro Smart Protection Network にパターンファイルを照合してチェックします。パフォーマンスに優れたコンテンツ配信ネットワークにより、確認プロセスで発生する待ち時間が最小限に抑えられ、より迅速な保護が可能となります。

トレンドマイクロは、不正プログラムの検出率を高めるため、ファイルレピュテーションを継続的に強化しています。スマートフィードバックを採用することで、何百万ものユーザからファイルに関するフィードバックを集め、不正ファイルの可能性を判断するうえで役立つ情報を特定しています。

Web レピュテーションサービス

トレンドマイクロの Web レピュテーションでは、世界最大級のレピュテーションデータベースを使用して、Web サイトの存続期間や URL の変更、および不正プログラム挙動分析から検出される不審な活動の兆候といった要素を基に、ドメインの信頼性を判別します。精度を向上させると同時に誤検出を少なくするため、トレンドマイクロでは、サイト全体を分類するのではなく、特定のページにレピュテーションスコアを割り当てています。

Web レピュテーションテクノロジーは、次のことからユーザを守ります。

- ・ 感染サイトへのアクセス
- ・ サイバー犯罪に使用されている C&C サーバとの通信

新しいソリューションの必要性

従来の脅威処理方法では、不正プログラムのパターンファイル (または定義) が定期的にクライアントに配信され、ローカルに保存されます。保護を継続するためには、新しいアップデートを定期的に受信して、不正プログラム対策ソフトウェアに読み込む必要があります。

この方法が有効に機能する一方で、増加し続ける脅威は、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、さらに適切な保護を提供するまでにかかる全体的な時間に影響する可能性があります。急激な脅威の増加に対処するため、トレンドマイクロは、不正プログラム対策シグネチャをクラウドに格納するアプローチを他に先駆けて開発しました。このアプローチで使用されるテクノロジーとアーキテクチャにより、新たに出現する脅威からユーザを適切に保護できます。

Trend Micro Smart Protection Network

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は Trend Micro Smart Protection Network を介して InterScan MSS と連携します。

Trend Micro Smart Protection Network は、Web からの脅威やセキュリティリスクからユーザを保護する、次世代のクラウド-クライアント型コンテンツセキュリティインフラストラクチャです。このソリューションでは、軽量クライアントを使用し、独自のインターネットクラウドで提供されているメールレピュテーション、Web レピュテーション、ファイルレピュテーションの関連分析テクノロジーおよび脅威データベースにアクセスすることで、ローカルソリューションおよびホステッドソリューションの機能を強化して、企業ネットワーク内、自宅、または外出先にいる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、およびユーザが増えるとともに、お客さまのセキュリティ保護対策は自動的にアップデートおよび強化され、ユーザに対するリアルタイムのネイバーフッドウォッチ保護サービスが構築されています。

Smart Protection Network は、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。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、クライアントから Smart Protection Network に検索クエリが送信されます。

Smart Protection Network 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。クライアントから Smart Protection Network 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 サイトのレピュテーションが確認されます。クライアントは、Web サイトのレピュテーションを、コンピュータ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。

Smart Protection Network の詳細については、次のサイトを参照してください。

<http://www.trendmicro.co.jp/spn/>

スマートフィードバック

トレンドマイクロスマートフィードバックは、トレンドマイクロ製品と、弊社が所有する 24 時間体制の脅威に関する研究センターおよびテクノロジーとの間に、継続的な両方向の情報交換を実現します。個々の顧客の定期的なレピュテーションチェックで検出された新しい脅威により、トレンドマイクロの脅威データベースが自動的に更新され、顧客に特定の脅威が発生するのを防ぐことができます。

トレンドマイクロでは、顧客とパートナーの大規模なグローバルネットワークを通じて収集された脅威に関する情報を継続的に処理することにより、最新の脅威に対して自動的なリアルタイムの保護を提供し、住民を保護するために地域で行われる自動化された自警組織と同様に、「団結」することによるセキュリティの強化を実現しています。情報源のレピュテーションに基づいて脅威情報が収集されるため、顧客の個人情報やビジネス情報のプライバシーは常に保護されます。

トレンドマイクロに送信される情報のサンプルを次に示します。

- ・ ファイルのチェックサム
- ・ アクセスされた Web サイト
- ・ サイズやパスなどのファイル情報
- ・ 実行可能ファイルの名前

スマートフィードバック機能は、管理コンソールから無効化できます。



ヒント

ご使用のコンピュータを保護するためにスマートフィードバックに参加する必要はありません。参加は任意であり、いつでも参加の取り消しができます。トレンドマイクロのすべてのお客さまに対する全体的な保護の強化に役立つため、スマートフィードバックへの参加をお勧めします。

Trend Micro Smart Protection Network の詳細については、次のサイトを参照してください。

<http://www.trendmicro.co.jp/spn/?oss=1>

Smart Protection ソース

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は、InterScan MSS および Smart Protection ソースと連携します。

Smart Protection ソースは、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。残りの定義は InterScan MSS クライアントがホストします。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、クライアントから Smart Protection ソースに検索クエリが送信されます。Smart Protection ソースは識別情報を使用してリスクを判定します。

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。クライアントから 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 サイトのレピュテーションが確認されます。クライアントは、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。

クライアントの接続先となる Smart Protection ソースは、クライアントの場所によって異なります。クライアントは Trend Micro Smart Protection Network または Smart Protection Server のどちらかに接続できます。

Smart Protection ソースの比較

次の表に、Trend Micro Smart Protection Network と Smart Protection Server の違いを示します。

表 16-1. Smart Protection ソースの比較

比較の基準	SMART PROTECTION SERVER	TREND MICRO SMART PROTECTION NETWORK
目的	Smart Protection サービスを企業ネットワークに対してローカライズし、効率を最適化することを目的として設計されている	企業ネットワークにアクセスできないクライアントに Smart Protection サービスを提供する、グローバルに展開されたインターネットワークベースのインフラストラクチャ
管理	InterScan MSS 管理者がこれらの 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
パターンファイルのアップデート元	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
クライアント接続プロトコル	HTTP および HTTPS	HTTPS

Smart Protection Server を追加する

Smart Protection Server を使用すると、Smart Protection サービスを企業ネットワークに対してローカライズし、送信トラフィックを削減して、効率を最適化できます。

Smart Protection Server は InterScan MSS 管理コンソールで追加、削除、インポート、およびエクスポートできます。以下に示す手順では、Smart Protection Server を追加するプロセスについて説明します。

手順

1. [ポリシー] > [Smart Protection] の順に選択します。

[セキュリティリスク検索] タブが初期設定で表示されます。

2. [ローカルソース] タブをクリックします。
3. [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。
4. Smart Protection Server を設定します。
 - a. サーバの IP アドレスまたは完全修飾ドメイン名 (FQDN) を指定します。
 - b. ファイルレピュテーションサービスを使用するには、[ファイルレピュテーションポート] を選択してポート番号を指定します。
 - c. Web レピュテーションサービスを使用するには、[Web レピュテーションポート] を選択してポート番号を指定します。
 - d. プリファレンス値を指定します。

**注意**

プリファレンスは、Smart Protection Server の優先度を表します。プリファレンス値が低いほど優先度は高くなります。

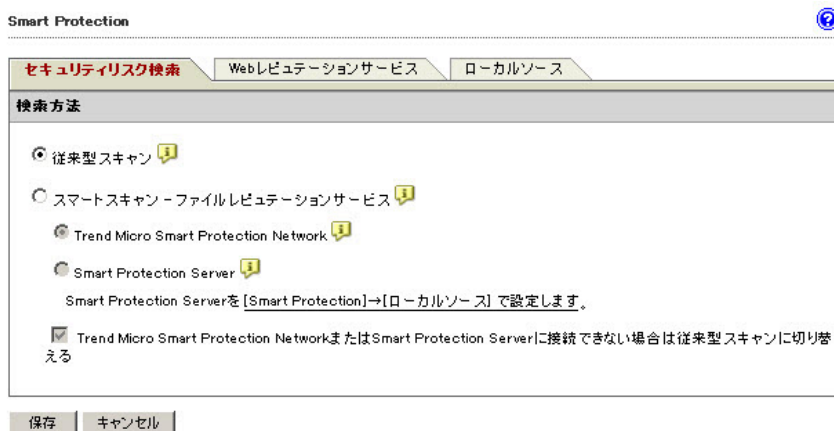
5. プロキシを設定します。
 - a. [有効にする] チェックボックスをオンにしてプロキシサーバを有効にします。
 - b. プロキシサーバの IP アドレスまたは完全修飾ドメイン名 (FQDN)、ポート番号、ユーザ名、およびパスワードを指定します。
 6. [接続テスト] をクリックして、Smart Protection Server の接続を確認します。
 7. [保存] をクリックします。
-

検索方法を選択する

InterScan MSS には、不正プログラムやその他のセキュリティ脅威を検出するための方法が 2 つあります。

手順

1. [ポリシー] > [Smart Protection] の順に選択します。
[セキュリティリスク検索] タブが初期設定で表示されます。



2. 次のいずれかの検索方法を選択します。
 - ・ 従来型スキャン: 従来型スキャンでは、ローカルに保存された不正プログラム対策コンポーネントとスパイウェア対策コンポーネントが使用されます。
ウイルスパターンファイルには、最新のウイルス/不正プログラムおよび複合型脅威の攻撃を特定するための情報が含まれています。トレンドマイクロでは、週に数回の割合で、特に破壊的なウイルス/不正プログラムが検出された後は常に、新たなバージョンのウイルスパターンファイルを作成し、リリースしています。
 - ・ スマートスキャン - ファイルレピュテーションサービス: スマートスキャンでは、クラウドに保存された脅威シグネチャが使用されます。

スマートスキャンモードの InterScan MSS は、スマートスキャンエージェントパターンファイルを使用してセキュリティリスクを確認します。スマートスキャンエージェントパターンファイルはトレンドマイクロによって毎日更新され、従来の不正プログラム対策やスパイウェア対策のパターンファイルと同様の保護を提供します。スマートスキャンエージェントパターンファイルでレピュテーションを判断できない場合、InterScan MSS は、Trend Micro Smart Protection Network にクエリを送信することで最新のセキュリティ対策を実現します。

**注意**

スマートスキャンが初期設定の検索方法です。

3. [スマートスキャン - ファイルレピュテーションサービス] を選択した場合、次の Smart Protection ソースのいずれかを選択します。
 - ・ Trend Micro Smart Protection Network: このオプションを選択した場合は、プロキシサーバ設定を指定します。
 - ・ Smart Protection Server: このオプションを選択した場合は、[ローカルソース] タブをクリックして Smart Protection Server を設定します。

**注意**

Trend Micro Smart Protection Network または Smart Protection Server に接続できない場合、InterScan MSS は従来型スキャンに切り替わります。[Trend Micro Smart Protection Network または Smart Protection Server に接続できない場合は従来型スキャンに切り替える] を選択している場合にのみ、従来型スキャンに切り替えることができます。

4. [保存] をクリックします。

**注意**

スマートスキャンが選択されている場合、[保存] をクリックすると、ただちに Trend Micro Smart Protection Network または Smart Protection Server への接続が試行されます。接続が確立されない場合、設定は保存されません。検索方法を選択しなおして、もう一度設定を保存します。

検索方法が変更されるたびに、自動的に検索サービスが再起動します。

従来型スキャンに戻る場合、検索サービスの接続タイムアウトのたびにシステムイベントログのクエリを実行できます。検索サービスが頻繁に接続タイムアウトになる場合は、ネットワーク設定を確認してください。システムイベントログのクエリの詳細については、[379 ページの「システムイベントログのクエリを実行する」](#)を参照してください。

検索方法の変更について通知を送信するように InterScan MSS を設定できません。通知の設定方法の詳細については、[415 ページの「イベント条件および通知メッセージを設定する」](#)を参照してください。

Web レピュテーションサービスを使用する

[セキュリティリスク検索] タブでスマートスキャンを設定すると、Smart Protection 環境が設定され、InterScan MSS でファイルレピュテーションサービスを使用できるようになります。InterScan MSS で Web レピュテーションサービスを使用するには、Web レピュテーションポリシーを設定します。

手順

1. [ポリシー] > [Smart Protection] の順に選択します。
[セキュリティリスク検索] タブが初期設定で表示されます。
2. [Web レピュテーションサービス] タブをクリックします。
3. 次の Smart Protection ソースのいずれかを選択します。
 - ・ Trend Micro Smart Protection Network: このオプションを選択した場合は、[管理] > [プロキシ] の順に選択してプロキシを設定します。
 - ・ Smart Protection Server: このオプションを選択した場合は、[ローカルソース] タブをクリックして Smart Protection Server を設定します。

**注意**

選択した Smart Protection Server に接続できない場合、InterScan MSS は Trend Micro Smart Protection Network に戻ります。[Smart Protection Server に接続できない場合は Trend Micro Smart Protection Network に切り替える] を選択している場合にのみ、Trend Micro Smart Protection Network に切り替えることができます。

[Smart Protection Network への外部クエリを実行しない] チェックボックスをオンにしている場合、InterScan MSS は Smart Protection Server にユーザ環境の外部でクエリを実行しないように要求します。

4. [保存] をクリックします。
-

第 17 章

ポリシーの設定

この章では、InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) ポリシーを作成、変更、および管理する手順について説明します。

この章の内容は次のとおりです。

- ・ 260 ページの「ポリシーを追加する」
- ・ 260 ページの「ルートを指定する」
- ・ 267 ページの「検索条件を指定する」
- ・ 297 ページの「処理を指定する」
- ・ 304 ページの「ポリシーを完成させる」

ポリシーを追加する

ポリシーを作成する前に、内部アドレスが設定されていることを確認します。詳細については、[240 ページの「内部アドレスを設定する」](#)を参照してください。

ポリシーを作成するには、次の手順を実行します。

- ・ 手順 1: [260 ページの「ルートを指定する」](#)
- ・ 手順 2: [267 ページの「検索条件を指定する」](#)
- ・ 手順 3: [297 ページの「処理を指定する」](#)
- ・ 手順 4: [304 ページの「ポリシーを完成させる」](#)



ヒント

ウイルスがまん延しないように、すべてのメッセージを確実に検索するために、「すべてのメッセージ」に適用するウイルス対策ルールを少なくとも 1 つ保持することをお勧めします。ウイルス対策ルールのルートを指定する際には、ドロップダウンリストから [すべてのメッセージ] を選択します。

ルートを指定する

ルートを追加するための最初の手順は、次の項目を設定することです。

ルート

受信者と送信者のメールアドレス、LDAP ユーザ、LDAP グループ、またはアドレスグループを含む特定の「宛先」と「差出人」の組み合わせ。ルートの除外を設定することもできます。

ルートの種類

SMTP トラフィック、POP3 トラフィック、またはすべてのトラフィックの方向です。

ルートを追加する

手順

1. [ポリシー] > [ポリシーリスト] の順に選択します。

[ポリシーリスト] 画面が表示されます。

2. [追加] をクリックし、次のいずれかを選択します。

- ・ ウイルス対策
- ・ その他

オプション	説明
ウイルス対策	ウイルス対策ルールにより、スパイウェア、ワームなどのウイルスおよびその他の不正プログラムについてメッセージが検索されます。
その他	その他のルールにより、スパムメールやフィッシングメッセージ、マーケティングメッセージ、メッセージの内容、暗号化されたメッセージ、規制コンプライアンス、およびその他の添付ファイルが検索されます。

[ルールの追加] 画面が表示されます。

3. [このルールの適用対象] の横にあるドロップダウンリストからポリシールートの種類を選択します。

- ・ 受信メッセージ
- ・ 送信メッセージ
- ・ 受信メッセージと送信メッセージの両方
- ・ POP3
- ・ すべてのメッセージ

4. 受信者と送信者を選択します。

- ・ 受信メッセージの場合は、内部アドレスの範囲内にある、受信者のアドレスを指定します。

たとえば、内部アドレスが example.com の場合、有効な受信者のアドレスには jim@example.com、bob@example.com があります。

- ・ 送信メッセージの場合は、内部アドレスの範囲内にある、送信者のアドレスを指定します。

たとえば、内部アドレスが example.com の場合、有効な送信者のアドレスには jim@example.com、bob@example.com があります。

- ・ 受信メッセージと送信メッセージの両方の場合において、ルールは、メールアドレスに一致する受信者または送信者に適用されます。



- メールアドレスを指定する際には、アスタリスク (*) ワイルドカードを使用できます。詳細については、[337 ページの「アスタリスクワイルドカードを使用する」](#)を参照してください。
- POP3 が選択されている場合、ルートを設定できません。ルールはすべての POP3 ルートに適用されます。
- ルールに対して [すべてのメッセージ] を選択した場合、そのルールは任意の送信者から任意の受信者へのメッセージにも適用されます。

5. [次へ] をクリックします。

[手順 2: 検索条件の選択] 画面が表示されます。

ルートを編集する

手順

1. [ポリシー] > [ポリシーリスト] の順に選択します。
[ポリシーリスト] 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。
ポリシーの [概要] 画面が表示されます。
3. [受信者と送信者] の [編集] をクリックします。
ポリシーの [受信者と送信者] 画面が表示されます。
4. [この規則の適用対象] の横にあるドロップダウンリストからポリシールートの種類を選択します。
 - ・ 受信メッセージ
 - ・ 送信メッセージ
 - ・ 受信メッセージと送信メッセージの両方
 - ・ POP3
 - ・ すべてのメッセージ



注意

グローバル DKIM 適用ルールでは、[この規則の適用対象] オプションを変更することはできません。

5. 受信者と送信者を選択します。
 - ・ 受信メッセージの場合は、内部アドレスの範囲内にある、受信者のアドレスを指定します。

以下に例を示します。内部アドレスが example.com の場合、有効な受信者のアドレスには jim@example.com、bob@example.com などがあります。

- ・ 送信メッセージの場合は、内部アドレスの範囲内にある、送信者のアドレスを指定します。

以下に例を示します。内部アドレスが example.com の場合、有効な送信者のアドレスには jim@example.com、bob@example.com があります。

- ・ 受信メッセージと送信メッセージの両方の場合において、ルールは、メールアドレスに一致する受信者または送信者に適用されます。

**注意**

- a. メールアドレスを指定する際には、アスタリスク (*) ワイルドカードを使用できます。詳細については、[337 ページの「アスタリスクワイルドカードを使用する」](#)を参照してください。
- b. POP3 が選択されている場合、ルートを設定できません。ルールはすべての POP3 ルートに適用されます。
- c. ルールに対して [すべてのメッセージ] を選択した場合、そのルールは任意の送信者 から任意の受信者へのメッセージにも適用されます。

6. [保存] をクリックします。

ルートの設定

ルートとは、受信者と送信者のメールアドレス、LDAP ユーザ、LDAP グループ、またはアドレスグループを含む特定の「宛先」と「差出人」の組み合わせのことです。ルートの除外を設定することもできます。

新規ルールの追加や既存ルールの変更時に、受信メッセージまたは送信メッセージを選択する場合、次のように送信者および受信者を [内部アドレス] リストに入れてください。

- ・ 送信メッセージを設定する場合は、[内部アドレス] リストは送信者に適用されます。
- ・ 受信メッセージを設定する場合は、[内部アドレス] リストは受信者に適用されます。

アスタリスク (*) ワイルドカードを使用して、特定範囲のメールアドレスを含めることができます。以下に例を示します。

- ・ user@example.com: 指定したアドレスだけが含まれます。
- ・ *@example.com: example.com ドメインのユーザすべてが含まれます。
- ・ *@*.company.com: example.com のすべてのサブドメインのユーザが含まれます。

たとえば、user1@accounting.example.com などが含まれます。

- ・ *@*: すべてのメールアドレスが含まれます。

ルートを設定する

手順

1. [受信者と送信者の選択] 画面で、次のいずれかをクリックします。
 - ・ 受信者または送信者: [受信メッセージ] または [送信メッセージ] を選択した場合に表示されます。
 - ・ ユーザ: [受信メッセージと送信メッセージの両方] を選択した場合に表示されます。
2. [アドレスの選択] で、次のいずれかを選択します。
 - ・ すべてのユーザ: このオプションを選択すると、受信者または送信者に関するすべての制限が解除されます。
 - ・ メールアドレスの入力: 追加するメールアドレスを指定します。
 - ・ LDAP ユーザまたはグループの検索: LDAP ユーザまたはグループ名を指定して [検索] をクリックします。結果がリストボックスに表示されます。
 - ・ アドレスグループの選択: すべての既存のアドレスグループがリストで表示されます。同一ルール内の複数のルートで個別に再利用する多数のメールアドレスがある場合は、[追加] をクリックしてアドレスグループを作成してください。

3. メールアドレスまたはメールアドレスグループを追加する場合は、[追加>] をクリックします。LDAP グループまたはアドレスグループを追加する場合は、そのグループをリストボックスでクリックし、[追加>] をクリックします。
4. [選択済み] リストからメールアドレスまたはメールアドレスグループを削除するには、ごみ箱のアイコンをクリックします。
5. [保存] をクリックします。



ヒント

受信者または送信者として LDAP グループを選択する際、Microsoft Active Directory または Sun iPlanet Directory を LDAP サーバとして指定している場合は、LDAP グループの先頭または末尾、あるいはその両方にワイルドカードを使用できます。

ウイルスの流出を防ぎ、すべてのメッセージが確実に検索されるようにするために、すべてのメッセージに常に適用されるウイルス対策ルールを少なくとも 1 つ保持することをお勧めします。

ルートの除外を設定する

[ルールの追加] 画面で、[除外設定] の横のリンクをクリックします。トラフィックの方向 (受信メッセージ、送信メッセージ、受信メッセージと送信メッセージの両方、またはすべてのメッセージ) に応じた [除外] 画面が表示されます。

手順

1. [ルールの追加] 画面で、[除外設定] の横のリンクをクリックします。
トラフィックの方向 (受信メッセージ、送信メッセージ、受信メッセージと送信メッセージの両方、またはすべてのメッセージ) に応じた [除外] 画面が表示されます。
2. [アドレスの選択] で、[差出人 (送信者)] および [宛先 (受信者)] の両方について次のいずれかを選択します。

- ・ メールアドレスの入力: 追加するメールアドレスを入力します。
 - ・ LDAP ユーザまたはグループの検索: LDAP ユーザまたはグループ名を指定して [検索] をクリックします。結果がリストボックスに表示されます。
 - ・ アドレスグループの選択: すべての既存のアドレスグループがリストで表示されます。同一ルール内の複数のルートで再利用する多数のメールアドレスがある場合は、[追加] をクリックしてアドレスグループを作成してください。
3. メールアドレスを追加する場合は、[追加>] をクリックします。LDAP グループまたはアドレスグループを追加する場合は、そのグループをリストボックスでクリックし、[追加>] をクリックします。
 4. 送信者と受信者のペアをリストから削除するには、ごみ箱のアイコンをクリックします。
 5. [保存] をクリックします。
-

検索条件を指定する

新しいルールの送信者と受信者を選択するか、既存のルールの送信者と受信者を変更した後で、いくつかの条件に基づいてメッセージトラフィックをフィルタするルールを設定します。

検索条件は、ウイルス対策ルールを作成しているか、その他のルールを作成しているかによって異なります。

手順

1. [手順 2: 検索条件の選択] 画面で、必要なチェックボックスをオンにします。ウイルス対策ルールおよびその他のルールに対する検索条件のカテゴリは、次のとおりです。
 - ・ ウイルス対策ルール

- a. ウイルス検索: ウイルスやその他の不正プログラムを含むメッセージと特定のファイルタイプを検索する初期設定の方法を設定します。

表 17-1. ウイルス検索

設定	説明
検索可能なすべてのファイル	すべてのファイルの検索を試行します。
トレンドマイクロの推奨設定: 実際のファイルタイプによる識別	トレンドマイクロの推奨設定を使用して、害のないファイル拡張子名で装った不正コードを特定します。
特定のファイルタイプ	検索対象とする以下の種類のファイル拡張子のいずれかの横にあるチェックボックスをオンにします。 ・ アプリケーションおよび実行可能ファイル: リンクをクリックして検索するサブタイプを選択します。 ・ 文書: リンクをクリックして検索するサブタイプを選択します。 ・ 圧縮ファイル: リンクをクリックして検索するサブタイプを選択します。 ・ 指定のファイル拡張子: テキストボックスに拡張子を指定します。拡張子の前にピリオド(.)を入力する必要はありません。拡張子にはアスタリスクワイルドカードを使用することもできます。

- b. IntelliTrap の設定: 圧縮ファイルのウイルス/不正プログラムを検索し、サンプルを調査のために TrendLabs (トレンドラボ) に送信します。
- ・ IntelliTrap を有効にする: メッセージに添付された自動実行型の圧縮ファイル (パッカー) を検索します。
 - ・ トレンドラボに IntelliTrap サンプルを送信する: InterScan MSS で、IntelliTrap で検出した添付ファイルを持つメッセージを自動的に送信できます。

- c. スパイウェア検索: スパイウェア、アドウェアなどのその他の種類の脅威を検索します。

- ・ その他のルール

- a. [次の場合にルールの処理を実行する] で次のいずれかを選択し、メッセージに対して処理を実行する条件を指定します。
 - ・ すべての条件に一致 (AND): メッセージが条件のすべてに一致するとき。
 - ・ いずれかの条件に一致 (OR): メッセージが条件のいずれかに一致するとき。
- b. スпамメール/フィッシングメール: スпамメールまたはフィッシングメッセージと特定されるメッセージを検索します。スパムメールとは、主に広告を目的とした迷惑メールのことです。一方、フィッシングメッセージは、信頼できる団体に見せかけた送信者から発信されます。
 - ・ スпамメール検出設定: リンクをクリックして、スパムメール検出レベルを選択し、承認済み送信者とブロックする送信者、およびテキスト除外のリストを設定します。
 - ・ フィッシングメール
- c. Web レピュテーション: メッセージ内の URL を検索して、フィッシング、およびその他の不正な Web サイトから保護します。
- d. マーケティングメッセージ: ERS スコアに照らしてメッセージを検索し、特定のマーケティングメッセージを許可します。
- e. 添付ファイル: 特定の拡張子が付いた添付ファイルや特定の実際のファイルタイプに属す添付ファイルなど、選択した条件に一致した添付ファイルを検索します。
 - ・ 名前または拡張子: リンクをクリックして、特定のファイル名または拡張子名のフィルタ設定を指定します。
 - ・ MIME コンテントタイプ: リンクをクリックして、MIME コンテントタイプのフィルタを設定します。

- ・ 実際のファイルタイプ: リンクをクリックして、一般的な実行可能ファイル、文書、画像、メディア、および圧縮ファイルのフィルタを設定します。
 - ・ サイズが {>, <, =} {} {MB, KB, B}: 特定のバイト数、キロバイト数、またはメガバイト数より大きい、小さい、または等しいサイズの添付ファイルをフィルタするために選択します。ファイルサイズを表す値を指定します。
 - ・ 添付ファイル数 {>, <, =} {}: 特定の数より大きい、小さい、または等しい添付ファイル数をフィルタするために選択します。各メッセージの添付ファイルの総数を表す値を指定します。
 - ・ パスワードで保護された zip ファイル (検索不能): InterScan MSS で検索できない、パスワードで保護された zip ファイルをフィルタするために選択します。
- f. サイズ: 指定されたメッセージサイズに一致するメッセージを検索します。
- ・ メッセージサイズが {>, <, =} {} {MB, KB}: 特定のキロバイト数、またはメガバイト数より大きい、小さい、または等しいサイズのメッセージをフィルタするために選択します。メッセージサイズを表す値を入力します。
- g. 内容: 件名、本文、ヘッダ、添付ファイルの内容のキーワード表現のリンク内で指定された表現と一致するキーワード表現を持つメッセージを検索します。
- ・ 件名のキーワード: リンクをクリックして、キーワードリストを管理します。
 - ・ 件名が空白: 件名のないメッセージのフィルタを選択します。スパムメールには件名が含まれていない場合があります。
 - ・ 本文のキーワード: リンクをクリックして、キーワードリストを管理します。
 - ・ ヘッダのキーワード: リンクをクリックして、キーワードリストを管理します。ヘッダには、件名、差出人、宛先、Cc、および指定可能な他のヘッダが含まれます。

- ・ 添付ファイルの内容のキーワード: リンクをクリックして、キーワードリストを管理します。添付ファイルには、添付ファイル名と添付ファイルのコンテンツが含まれます。
- h. その他: 指定された受信者数と一致するメッセージを検索します。また、指定された時間内に受信したメッセージを検索します。
 - ・ 受信者の数が {>, <, =} {}: 受信者数のフィルタを選択します。各メッセージの受信者の総数を表す値を指定します。
 - ・ 受信の時間帯: リンクをクリックして、メッセージの受信日と時間帯を選択します。
 - ・ 暗号化メッセージ: InterScan MSS で復号化できない、暗号化されたメッセージをフィルタするために選択します。

C&C メール承認済みリストを設定する

InterScan MSS では、このリストに含まれる送信者および受信者のメッセージは C&C メールとして検出されません。リストには最大 5,000 件のエントリを指定できます。



注意

InterScan MSS は、SMTP セッションではなく、メッセージヘッダで使用されているアドレスを識別します。

手順

1. [検索条件] 画面で、[C&C メール設定] を選択します。
2. [C&C メール設定] をクリックします。

[C&C メール設定] 画面が表示されます。

C&Cメール設定



[新規ルール > C&Cメール設定](#)

保存

キャンセル

C&Cメール承認済みリスト

☐ C&Cメール承認済みリストを有効にする

メールアドレス:

追加

删除

インポート

エクスポート

メールアドレスが誤って分類されている場合は、cnc_falsepositive@trendmicro.com にメッセージを送信してトレンドマイクロに通知してください。

保存

キャンセル

3. [C&C メール承認済みリストを有効にする] を選択します。
4. 次のいずれかの方法でメールアドレスを追加します。
 - a. ボックスにメールアドレスを入力して、[追加] をクリックします。
そのアドレスがリストに表示されます。



注意

アスタリスク文字を使用して複数のアドレスを追加できます。詳細については、[337 ページの「アスタリスクワイルドカードを使用する」](#)を参照してください。

- b. ローカルホストのテキストファイルからメールアドレスを InterScan MSS サーバにインポートします。

**注意**

ファイルの各行には、有効な形式に従ったメールアドレスを1つのみ記載します。不正な形式のメールアドレスはインポートされません。

リストにすでにメールアドレスが含まれている場合は、新しいエントリをマージするか既存のエントリを上書きするかを選択します。

5. (オプション) アドレスリストをテキストファイルとしてエクスポートします。
6. (オプション) メールアドレスが誤って分類されている場合は、cnc_falsepositive@trendmicro.com にメッセージを送信してトレンドマイクロに通知してください。

**注意**

詳細については、273 ページの「誤って分類されているメールアドレスをトレンドマイクロに送信する」を参照してください。

7. [保存] をクリックします。

誤って分類されているメールアドレスをトレンドマイクロに送信する

手順

1. 管理コンソール、エラーメッセージ、または InterScan MSS から受信した通知のスクリーンショットを撮ります。
2. 次の情報を記載して新しいメールメッセージを作成します。
 - ・ 件名:[InterScan MSS 9.1] 誤って分類されているメールアドレス
 - ・ メール本文:
 - ・ メールアドレス
 - ・ 誤って分類されていると判断できる理由

- ・ 添付ファイル:
 - ・ [273 ページの手順 1](#) で撮ったスクリーンショット
 - ・ 不正として識別されたメールメッセージ

**重要**

メッセージヘッダから必須の情報が削除されてしまうため、[転送] コマンドは使用しないでください。代わりに、添付ファイル (.msg または .eml) としてメッセージを送信してください。

3. cnc_falsepositive@trendmicro.com 宛てにメールメッセージを送信します。

スパムメールの検索条件を選択する

スパムメールの検索条件には、スパムメール検出レベルのしきい値の設定、承認済み送信者およびブロックする送信者やテキスト除外ルールの設定可能なリストが含まれます。

手順

1. その他のルールタイプの [検索条件の選択] 画面の [フィッシング/ソーシャルエンジニアリング攻撃/スパムメール] で、[スパムメール検出設定] の横にあるチェックボックスをオンにします。
2. [スパムメール検出設定] をクリックします。
[スパムメール検出設定] 画面が表示されます。
3. スパムメール検索を有効にするには、[スパムメールの検出レベルを指定する] チェックボックスをオンにします。

チェックボックスをオンにしなかった場合、InterScan MSS では、ルールに違反するメッセージがあってもスパムメールと見なされません。ただし、ブロックする送信者リストに指定した送信者に対しては処理が実行されます。

4. 次のスパムメールの検出レベルを 1 つ選択するか、検出のしきい値を指定します。

- ・ 高: より多くのスパムメールを検出します。クライアントに到達するスパムメールが多すぎる場合は高い検出率を選択します。
- ・ 中: 標準の設定です。
- ・ 低: より少ないスパムメールを検出します。InterScan MSS によってスパムメールと判定されるメッセージが多すぎる時に設定します。
- ・ 指定 {}: メッセージがスパムメールかどうか判断する基準を示す 3.0 から 10.0 までのしきい値を設定します。

**注意**

しきい値が高くなると、スパムメールの疑いが非常に高いメッセージでないかぎり InterScan MSS はスパムメールと見なしません。スパムメールの検出率は低くなりますが、また誤検出も少なくなります。InterScan MSS により多くの正規のメッセージがスパムメールと見なされる場合 (誤検出が多い場合) は、しきい値を高く設定してください。

しきい値が低くなると、少しでもスパムメールの疑いのあるメッセージでも InterScan MSS はスパムメールと見なします。スパムメールの検出率は高くなりますが、また誤検出も多くなります。多くのスパムメールが正規のメッセージとクライアントで認識される場合、しきい値を低く設定してください。

5. [DKIM 承認済みリスト] をクリックして、DKIM 承認済みリストの使用を有効または無効にします。DKIM 承認済みリストに記載されているドメインからのメッセージは、検索されたりスパムメールとしてマークされたりすることはありません。
6. 次の任意のリストの横にあるチェックボックスをオンにして、有効にします。
 - ・ 承認済み送信者リスト: このリストにある送信者からのメッセージは、スパムメールとして検出されません。
 - ・ ブロックする送信者リスト: このリストにある送信者からのメッセージは、スパムメールとして検出されます。
 - ・ テキスト除外ルール: このリストの任意のテキストを含むメッセージは、スパムメールとして検出されません。

**注意**

リストの設定方法については、276 ページの「承認済み送信者リストとブロックする送信者リストを設定する」を参照してください。

7. [保存] をクリックして、検索条件の選択を続行します。

承認済み送信者リストとブロックする送信者リストを設定する

スパムメールフィルタの検索条件にさらに柔軟性を与えるために、InterScan MSS には以下のリストが用意されています。

承認済み送信者リスト

このリストにある送信者からのメッセージは、スパムメールとして検出されません。

ブロックする送信者リスト

このリストにある送信者からのメッセージは、スパムメールとして検出されます。

スパムメールの検索条件を選択する際に、リストを設定します。

手順

1. [承認済み送信者リスト] または [ブロックする送信者リスト] の横にあるチェックボックスをオンにします。
2. アドレスを手動で追加するには、次の手順を実行します。
 - a. [メールアドレス] に、アドレスを指定します。複数のアドレスを追加するには、アスタリスク (*) ワイルドカードを使用します。
 - b. [追加] をクリックします。そのアドレスがリストに表示されます。
3. ローカルホスト上のファイルから InterScan MSS サーバにアドレスグループをインポートするには、次の手順を実行します。
 - a. [インポート] をクリックします。

- b. [参照] をクリックして、ファイルを検索します。画面が表示されます。
 - c. [開く] をクリックします。
 - d. リストに既存のアドレスがある場合は、インポートするリストとこれらのアドレスをマージするか、インポートするリストでこれらのアドレスを上書きするかを選択します。
 - e. [インポート] をクリックします。
 4. InterScan MSS サーバ上のファイルとしてアドレスグループをエクスポートするには、次の手順を実行します。
 - a. [エクスポート] をクリックします。[保存] ダイアログボックスが表示されます。
 - b. [保存] をクリックします。
 - c. ファイルの名前と保存場所を指定します。
 - d. [保存] をクリックします。ファイルがその場所に保存され、ダイアログボックスが表示されます。
 - e. [閉じる] をクリックします。
 5. [保存] をクリックします。

スパムメールテキスト除外ルールを設定する

InterScan MSS では、テキスト除外リスト内のテキストはスパムメールとして検出しません。必ず特定のキーワードを含むメッセージをユーザが受信するようにしたい場合は、このリストに関するルールを設定してください。

正規表現を使用して条件を定義します。以下の文字の前には、円記号 (バックスラッシュ) (\) を入力してください。

`\ | ( ) { } [ ] ^ $ * + . ?`

手順

1. スпамメールの検索条件を設定している場合は、[テキスト除外ルール] の [テキスト除外ルールに一致するメッセージを除外する] チェックボックスをオンにします。
2. 新しいテキスト除外ルールを追加するには、[追加] をクリックします。既存のルールを設定するには、リストボックスで設定するルールをクリックし、[編集] をクリックします。

[テキスト除外ルール] 画面が表示されます。

3. [名前] に、テキスト除外ルールのわかりやすい名前を指定します。
4. [検索領域] で、メッセージの一部を選択します。



注意

検索領域として [件名]、[差出人]、[宛先]、または [返信先] を選択し、[行の先頭] を使用してヘッダを検索する場合は、[行の先頭] に関するヘッダの内容だけを入力します。

例:

- a. 検索領域として [差出人] を選択します。
- b. [一致する文字列 (順に)] で、[行の先頭] にメッセージ文字列を入力します。たとえば、「test@trendmicro.com」のように入力します。

検索領域として [すべてのヘッダ] を選択して [行の先頭] を使用してヘッダを検索する場合は、同様にヘッダ名を入力する必要があります。

例:

- a. 検索領域として [すべてのヘッダ] を選択します。
- b. [一致する文字列 (順に)] で、[行の先頭] にヘッダ名とメッセージ文字列を入力します。たとえば、「From: test@trendmicro.com」のように入力します。

-
5. [大文字と小文字を区別する] のチェックボックスをオンにすると、テキストの大文字/小文字も区別します。
 6. [一致する文字列 (順に)] のテキストボックスにテキスト文字列を指定します。[本文の先頭] は行の最初で一致させる正規表現として、[行の末尾] は行の最後で一致させる正規表現として使用されます。

7. [保存] をクリックします。
-

グレイメール除外リストを設定する

除外リストとは、コンテンツのフィルタリングで無視する無害な IP アドレスのリストです。最大 5,000 件の IP アドレスを、個別に追加するか、複数のアドレスをテキストファイルからインポートして追加できます。ポリシーは、リスト内の順序で IP アドレスに影響を与えます。

手順

1. ウイルス対策ポリシーでない「その他」のポリシーを作成して変更します。
 - ・ 新しいルールを作成手順については、[259 ページのポリシーの設定](#)を参照してください。
 - ・ 既存ルールの変更手順については、[323 ページの既存のポリシーの設定](#)を参照してください。
2. [グレイメール] で [グレイメール検出設定] をクリックします。

[グレーメール検出設定] 画面が表示されます。

グレーメール検出設定



グレーメール > グレーメール検出設定

グレーメール検索カテゴリ

☒ マーケティングメッセージとニュースレター
 ☒ ソーシャルネットワークの通知
 ☒ その他のグレーメール

グレーメール除外リスト

除外リスト内のIPアドレスからのメッセージは検索またはブロックされません。

☐ 除外リストを有効にする

IPアドレス:

除外リストの各エントリの定義基準:

- IPv4アドレスまたはアドレスの範囲
例: 10.64.12.1, 10.64.12.1-10
- IPv4アドレス/サブネットマスク
例: 10.64.12.0/24
- IPv6アドレスまたはアドレスの範囲
例: 2001::10, 2001::10-64
- IPv6アドレス/プレフィックス長
例: 2001::10/64

3. [除外リストを有効にする] を選択します。
4. 次の方法で IP アドレスを追加します。
 - a. IP アドレスを指定して [追加>>] をクリックします。
その IP アドレスがリストに表示されます。

- b. ローカルホストのテキストファイルから IP アドレスを InterScan MSS サーバにインポートします。

詳細については、[281 ページの「グレーメール除外リストをインポートする」](#)を参照してください。

5. (オプション) IP アドレスリストをテキストファイルとしてエクスポートします。
6. [保存] をクリックします。

グレーメール除外リストをインポートする

始める前に

[279 ページの「グレーメール除外リストを設定する」](#)を完了してください。



注意

- ・ ファイルの各行には、有効な形式に従った IP アドレスを 1 つのみ記載します。不正な形式の IP アドレスはインポートされません。
- ・ ファイル内の IP アドレスがリストにすでに含まれている場合、その IP アドレスは無視されます。
- ・ ファイルに 5,000 件を超える IP アドレスが含まれている場合、最初の 5,000 件のみがインポートされます。

手順

1. [グレーメール除外リスト] 画面の右側のペインで [インポート] をクリックします。

[グレーメール除外リストのインポート] 画面が表示されます。

グレーメール除外リストのインポート

ファイル: 参照...

(形式: 1行あたり1つのIPアドレス)

マージオプション: ☒ 現在のリストとマージ

☐ 現在のリストを上書き

インポート キャンセル

2. [参照] をクリックして、ファイルを検索します。

次に有効な入力例を示します。

IPv4 アドレス

```
123.123.123.123  
62.36.52.1-255  
62.36.52.0/24
```

IPv6 アドレス

```
1050:0:0:0:5:600:300c:326b  
ff06::c3
```

3. 次のマージオプションのいずれかを選択します。
 - ・ [現在のリストとマージ] を選択すると、ファイル内の IP アドレスが既存の除外リストに追加されます。
 - ・ [現在のリストを上書き] を選択すると、既存のリストがファイル内の IP アドレスで置き換えられます。
4. [インポート] をクリックします。

Web レピュテーションを設定する



注意

日本語版ではこの機能は初期設定で有効になっています。

Web レピュテーションを有効にして設定すると、メッセージに埋め込まれた不正な URL からクライアントを保護できます。

Web レピュテーション設定を有効にする

手順

1. ウイルス対策ポリシーでない「その他」のポリシーを作成して変更します。
 - ・ 新しいルールを作成手順については、[259 ページのポリシーの設定](#)を参照してください。
 - ・ 既存ルールの変更手順については、[323 ページの既存のポリシーの設定](#)を参照してください。
 2. [検索条件] 画面の [Web レピュテーション] で、[Web レピュテーション設定] チェックボックスをオンにします。
 3. [次へ] をクリックしてポリシーの設定を続行します。
-

Web レピュテーションを設定する

手順

1. ウイルス対策ポリシーでない「その他」のポリシーを作成して変更します。
 - ・ 新しいルールを作成手順については、[259 ページのポリシーの設定](#)を参照してください。
 - ・ 既存ルールの変更手順については、[323 ページの既存のポリシーの設定](#)を参照してください。
2. [検索条件の選択] 画面の [Web レピュテーション] で、[Web レピュテーション設定] をオンにします。
3. [Web レピュテーション設定] をクリックします。
[Web レピュテーション設定] 画面が表示されます。
4. 次のセキュリティレベルのいずれかを選択します。

- ・ 高: メッセージに埋め込まれた、より多くの Web サイトをブロックしますが、誤検出のリスクも高くなります。ユーザーによる不正な Web サイトへのアクセスが多すぎる場合は、[高] を選択します。
 - ・ 中: 標準の設定です。誤検出数を低く抑えながら大半の Web 脅威をブロックするため、[中] が初期設定になります。
 - ・ 低: メッセージに埋め込まれた、比較的少数の Web サイトをブロックし、誤検出のリスクも低減します。InterScan MSS がブロックする正規の Web サイトが多すぎる場合は、[低] を選択します。
5. [Web レピュテーション承認済みリストの使用を有効にする] をオンにすると、Web レピュテーション承認済みリストに記載されたドメインの検索とブロックが回避されます。
 6. [保存] をクリックします。

Time-of-Click プロテクションを設定する

Time-of-Click プロテクションを有効にすると、InterScan MSS は、さらなる分析のためにメール内の URL を書き換えます。トレンドマイクロでは、これらの URL をクリック時に分析し、不正なものである場合はブロックします。

手順

1. [ポリシー] > [Time-of-Click プロテクション] の順に選択します。

[Time-of-Click プロテクション] 画面が表示されます。

Time-of-Clickプロテクション



Time-of-Clickプロテクションは、ユーザーがメール内の不正なURLをクリックした場合に保護を提供します。

Time-of-Clickプロテクションの設定	
処理:	
危険:	ブロック
極めて不審:	ブロック
不審:	許可
未評価:	許可
保存 キャンセル	

2. [処理] で、次の手順を実行します。

- ・ 危険:危険な URL に対して実行する処理 ([許可]、[警告]、または [ブロック]) を選択します。初期設定値は [ブロック] です。

危険な URL とは、不正、または脅威の既知の発信源であると確認されたページです。

- ・ 極めて不審:極めて不審な URL に対して実行する処理 ([許可]、[警告]、または [ブロック]) を選択します。初期設定値は [ブロック] です。

極めて不審な URL とは、不正、または脅威の発信源である可能性が疑われたページです。

- ・ 不審:不審 URL に対して実行する処理 ([許可]、[警告]、または [ブロック]) を選択します。初期設定値は [許可] です。

不審 URL とは、スパムメールに関連付けられている、または感染している可能性のあるページです。

- ・ 未評価:未評価の URL に対して実行する処理 ([許可]、[警告]、または [ブロック]) を選択します。初期設定値は [許可] です。

トレンドマイクロは積極的に URL の安全性をテストしていますが、ユーザが新しい Web サイトやあまり一般的でない Web サイトにアクセスすると、まだテストされていないページに遭遇することがあります。まだテストされていない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が妨げられることがあります。

3. [保存] をクリックします。

マーケティングメッセージ除外を設定する

除外リストとは、コンテンツのフィルタリングで無視する、無害なメールアドレスおよび IP アドレスのリストです。最大 5,000 件のアドレスを、個別に追加するか、複数のアドレスをテキストファイルからインポートして追加できます。ポリシーは、リスト内の順序でアドレスに影響を与えます。

手順

1. ウイルス対策ポリシーでない「その他」のポリシーを作成して変更します。
 - ・ 新しいルールを作成手順については、[259 ページのポリシーの設定](#)を参照してください。
 - ・ 既存ルールの変更手順については、[323 ページの既存のポリシーの設定](#)を参照してください。
2. [マーケティングメッセージ] の [マーケティングメッセージ設定] をクリックします。

[マーケティングメッセージ設定] 画面が表示されます。

The screenshot shows the 'Spam Mail Policy Rule' configuration window. The 'Spam Mail Search Category' section has three checked options: 'Marketing Messages and Newsletters', 'Social Network Notifications', and 'Other Spam Mail'. The 'Spam Mail Exclusion List' section has a checkbox for 'Enable Exclusion List' which is currently unchecked. Below this is an 'IP Address' input field and a 'Add >>' button. To the right of the input field are buttons for 'Delete', 'Import', and 'Export'. A large empty box is provided for entering exclusion list entries. At the bottom are 'Save' and 'Cancel' buttons.

グレーメール検出設定

初期設定のスパムメール対策ルール > グレーメール検出設定

グレーメール検索カテゴリ

- ☒ マーケティングメッセージとニュースレター
- ☒ ソーシャルネットワークの通知
- ☒ その他のグレーメール

グレーメール除外リスト

除外リスト内のIPアドレスからのメッセージは検索またはブロックされません。

☐ 除外リストを有効にする

IPアドレス

追加 >>

除外リストの各エントリの定義基準:

- IPv4アドレスまたはアドレスの範囲
例: 10.64.12.1, 10.64.12.1-10
- IPv4アドレス/サブネットマスク
例: 10.64.12.0/24
- IPv6アドレスまたはアドレスの範囲
例: 2001::10, 2001::10-64
- IPv6アドレス/プレフィックス長
例: 2001::10/64

削除 インポート エクスポート

保存 キャンセル

3. [除外リストを有効にする] を選択します。

4. 次の方法で、メールアドレスまたは IP アドレスを追加します。
 - a. メールアドレスまたは IP アドレスを指定して [追加>>] をクリックします。
そのアドレスがリストに表示されます。
 - b. ローカルホストのテキストファイルからメールアドレスを InterScan MSS サーバにインポートします。
詳細については、[287 ページの「マーケティングメール除外をインポートする」](#)を参照してください。
 5. (オプション) アドレスリストをテキストファイルとしてエクスポートします。
 6. [保存] をクリックします。
-

マーケティングメール除外をインポートする

始める前に

[285 ページの「マーケティングメッセージ除外を設定する」](#)を完了してください。



注意

- ・ ファイルの各行には、有効な形式に従ったメールアドレスまたは IP アドレスを 1 つのみ記載します。不正な形式のメールアドレスはインポートされません。
 - ・ ファイル内のメールアドレスまたは IP アドレスがリストにすでに含まれている場合、そのアドレスは無視されます。
 - ・ ファイルに 5,000 件を超えるアドレスが含まれている場合、最初の 5,000 件のみがインポートされます。
-

手順

1. [マーケティングメッセージ設定] ルール画面の右側のペインで [インポート] をクリックします。

[マーケティングメッセージ除外リストのインポート] 画面が表示されます。

グレーメール除外リストのインポート

ファイル: ファイルが選択されていません。
 (形式: 1行あたり1つのIPアドレス)

マージオプション: ☒ 現在のリストとマージ
☐ 現在のリストを上書き

2. [参照] をクリックして、インポートするファイルを選択します。
次に有効な入力例を示します。

メールアドレス

```
user@company.com
*/*.company.com
```

IPv4 アドレス

```
123.123.123.123
62.36.52.1-255
62.36.52.0/24
```

IPv6 アドレス

```
1050:0:0:0:5:600:300c:326b
ff06::c3
```

3. 次のマージオプションのいずれかを選択します。
 - ・ [現在のリストとマージ] を選択すると、ファイル内のアドレスが既存の除外リストに追加されます。
 - ・ [現在のリストを上書き] を選択すると、既存のリストがファイル内のアドレスで置き換えられます。

4. [インポート] をクリックします。
-

添付ファイルの検索条件を選択する

InterScan MSS では、メッセージに添付されているファイルに基づいて、メールトラフィックのフィルタを実行できます。

添付ファイル名または拡張子の検索条件を指定する

手順

1. [検索条件の選択] 画面の [添付ファイル] で、[名前または拡張子] の横にあるチェックボックスをオンにします。
2. [名前または拡張子] をクリックします。
[添付ファイルの名前または拡張子] 画面が表示されます。
3. [選択] で、次のいずれかを選択します。
 - ・ 選択された添付ファイル名: 選択した名前の添付ファイルが添付されているメッセージに対して処理を実行します。
 - ・ 選択された添付ファイル以外: 選択した名前以外の添付ファイルが添付されているメッセージに対して処理を実行します。
4. 検索対象または検索対象外の添付ファイルの横にあるチェックボックスをオンにします。
5. 独自の添付ファイル名を追加するには、次のようにします。
 - a. [指定のファイル名] の横にあるチェックボックスをオンにします。
 - b. [インポート] をクリックして既存のテキストファイルからインポートします。別の画面が表示されます。

または、テキストボックスに添付ファイル名を指定します。複数の値がある場合はセミコロン (;) で区切ります。拡張子にはアスタリスクワイルドカードを使用することもできます。

- c. [保存] をクリックします。
 6. [保存] をクリックして、検索条件の選択を続行します。
-

MIME コンテントタイプの検索条件を指定する

手順

1. [検索条件の選択] 画面の [添付ファイル] で、[MIME コンテントタイプ] の横にあるチェックボックスをオンにします。
 2. [MIME コンテントタイプ] をクリックします。
[MIME コンテントタイプ] 画面が表示されます。
 3. [選択] で、次のいずれかを選択します。
 - ・ 選択された添付ファイルタイプ: 選択したタイプの添付ファイルが添付されているメッセージに対して処理を実行します。
 - ・ 選択された添付ファイルタイプ以外: 選択したタイプ以外の添付ファイルが添付されているメッセージに対して処理を実行します。
 4. フィルタを実行する MIME コンテントタイプの横にあるチェックボックスをオンにします。
 5. 独自の MIME タイプを追加するには、テキストボックスにその MIME タイプを入力します。
複数の値がある場合はセミコロン (;) で区切ります。MIME タイプにはアスタリスクワイルドカードを使用することもできます。
 6. [保存] をクリックして、検索条件の選択を続行します。
-

実際のファイルタイプの検索条件を指定する

手順

1. [検索条件の選択] 画面の [添付ファイル] で、[実ファイルタイプ] の横にあるチェックボックスをオンにします。

2. [実ファイルタイプ] をクリックします。
[添付ファイルの実際のファイルタイプ] 画面が表示されます。
 3. [選択] で、次のいずれかを選択します。
 - ・ 選択された添付ファイルタイプ: 選択したタイプの添付ファイルが添付されているメッセージに対して処理を実行します。
 - ・ 選択された添付ファイルタイプ以外: 選択したタイプ以外の添付ファイルが添付されているメッセージに対して処理を実行します。
 4. フィルタを実行する実際のファイルタイプの横にあるチェックボックスをオンにします。
 5. [保存] をクリックして、検索条件の選択を続行します。
-

添付ファイルサイズの検索条件を指定する

手順

1. [検索条件の選択] 画面の [添付ファイル] で、[サイズが {>, <, =} {} {MB, KB, B}] の横にあるチェックボックスをオンにします。
 2. 比較記号 (>、<、=) を選択します。
 3. サイズを表す値を指定します。
 4. メガバイト、キロバイト、またはバイト (MB、KB、または B) のいずれかを選択します。
 5. 検索条件の選択を続行します。
-

添付ファイル数の検索条件を指定する

手順

1. [検索条件の選択] 画面の [添付ファイル] で、[添付ファイル数 {>, <, =} {}] の横にあるチェックボックスをオンにします。

2. 比較記号 (>、<、=) を選択します。
 3. 添付ファイルの数を表す値を指定します。
 4. 検索条件の選択を続行します。
-

パスワードで保護された zip ファイルをブロックする

手順

- ・ [手順 2: 検索条件の選択] 画面の [添付ファイル] で、[パスワードで保護された zip ファイル (検索不能)] の横にあるチェックボックスをオンにします。
-

メッセージサイズの検索条件を選択する

InterScan MSS では、すべての添付ファイルを含む合計サイズに基づいて、メッセージに対する処理を実行できます。

手順

1. [検索条件の選択] 画面の [サイズ] で、[メッセージサイズが {>, <, =} { } {MB, KB}] の横にあるチェックボックスをオンにします。
 2. 比較記号 (>、<、=) を選択します。
 3. メッセージのサイズを表す数値を指定します。
 4. メガバイトまたはキロバイト (MB または KB) のいずれかを選択します。
 5. 検索条件の選択を続行します。
-

メッセージ内容の検索条件を選択する

InterScan MSS では、メッセージの内容とその出現場所を基準にして、メッセージに対する処理を実行できます。フィルタする内容の指定方法については、[193 ページの「キーワードを設定する」](#)を参照してください。

手順

1. [ポリシー] > [ポリシーリスト] の順に選択します。
[ポリシー] 画面が表示されます。
 2. ウイルス対策ポリシーでない「その他」のポリシーを作成して変更します。
 3. [手順 2: 検索条件の選択] 画面の [内容] で、コンテンツの条件を適用するメッセージ部分の横のチェックボックスをオンにします。
 4. 内容の条件を設定するメッセージ部分のリンクをクリックします。次の 2 つの列が表示されている [キーワードおよび式] 画面が表示されます。
 - ・ 使用可能: キーワードは利用可能ですが、現在使用されていません。
 - ・ 選択済み: キーワードは現在使用中です。
 5. ヘッダにキーワードを設定する場合は、キーワードを適用するヘッダ項目の横のチェックボックスをオンにします。
 6. [追加] をクリックします。
キーワード表現を管理する画面が表示されます。
 7. キーワードを設定します。
 8. [使用可能] リストで、有効にするキーワードリストをクリックします。
 9. [>] をクリックします。
キーワードが [選択済み] リストに表示されます。

キーワードリストを利用可能な状態にしておき、InterScan MSS で一時的に使用しないようにするには、選択されたリストでキーワードをクリックしてから [<] をクリックします。
 10. [保存] をクリックして、[検索条件] 画面を続行します。
-

コンプライアンスの検索条件を指定する

コンプライアンステンプレートをポリシーで使用できるようにするためには、InterScan MSS の規制コンプライアンスを有効にする必要があります。

手順

1. [ポリシー] > [ポリシーリスト] の順に選択します。
[ポリシー] 画面が表示されます。
 2. ウイルス対策ポリシーでない「その他」のポリシーを作成して変更します。
 3. [情報漏えい対策] で、[DLP コンプライアンステンプレート] をクリックします。
[DLP コンプライアンステンプレート] 画面が表示されます。
 4. 必要な DLP コンプライアンステンプレートを [使用可能] リストから選択します。
 5. [保存] をクリックして、[検索条件] 画面を続行します。
-

「その他」の検索条件を指定する

InterScan MSS では、以下を基準にしてメールトラフィックをフィルタできます。

- ・ 受信者の数
- ・ メッセージの到着時間
- ・ メッセージコンテンツの暗号化

手順

1. [ポリシー] > [ポリシーリスト] の順に選択します。
[ポリシー] 画面が表示されます。

2. ウイルス対策ポリシーでない「その他」のポリシーを作成して変更します。
 - ・ 新しいルールを作成手順については、[259 ページのポリシーの設定](#)を参照してください。
 - ・ 既存ルールの変更手順については、[323 ページの既存のポリシーの設定](#)を参照してください。
3. [検索条件の選択] 画面の [その他] で、次のオプションの横にあるチェックボックスをオンにします。
 - ・ 受信者の数が {>, <, =} {}:受信者の数が指定された制限値より少ない、多い、または等しい場合にメッセージがブロックされます。
 - ・ 受信の時間帯:ネットワークへの着信が指定した時間範囲に該当する場合にメッセージがブロックされます。
 - ・ メッセージを暗号化できません: InterScan MSS で復号化できない、暗号化されたメッセージがブロックされます。

受信者数の検索条件を選択する

InterScan MSS では、メッセージが配信される受信者数に基づいて、メッセージに対する処理を実行できます。

手順

1. [検索条件の選択] 画面の [その他] で、[受信者の数が {>, <, =} {}] の横にあるチェックボックスをオンにします。
 2. 比較記号 (>、<、=) を選択します。
 3. 受信者の数を表す値を指定します。
 4. 検索条件の選択を続行します。
-

メッセージ受信時間の検索条件を設定する

InterScan MSS では、メッセージの到着時間に基づいて、メッセージに対する処理を実行できます。

手順

1. [検索条件の選択] 画面の [その他] で、[受信の時間帯] の横にあるチェックボックスをオンにします。
 2. [受信の時間帯] をクリックします。
[時間帯] 画面が表示されます。
 3. [選択] で、次のいずれかを選択します。
 - ・ 選択した範囲内の任意の時間
 - ・ 選択した範囲を除く任意の時間
 4. 日時のドロップダウンボックスから、曜日、時間の範囲を指定します。
 5. [追加] をクリックします。
 6. [保存] をクリックして、検索条件の選択を続行します。
-

スプーフィングされた内部メッセージの検索条件を設定する

InterScan MSS では、信頼された内部 IP アドレスリスト以外から発信されたすべてのメッセージがブロックされます。このフィルタは、送信者と受信者のドメインが同じであるメッセージに対してのみ起動されます。

手順

1. [検索条件の選択] 画面の [その他] で、[スプーフィングされた内部メッセージ] の横にあるチェックボックスをオンにします。
2. [スプーフィングされた内部メッセージ] をクリックします。
[スプーフィングされた内部メッセージ] 画面が表示されます。

**警告!**

この機能を有効にする場合、エッジ MTA の IP アドレスをすべてこのリストに追加する必要があります。IP アドレスを追加しないと、リストに追加されていないエッジ MTA からのメッセージがすべてブロックされます。

3. 信頼する内部 IP リストに IP アドレスを追加します。
4. [保存] をクリックします。

処理を指定する

ウイルス対策ルールとその他のルールの両方に対する基本処理は、同様の処理ですが、オプションが多少異なります。次のカテゴリから必要な処理を選択します。

インターセプト

メッセージをインターセプトして受信者に送信されないようにすることができます。インターセプトを選択すると、インターセプトされたメッセージに実行する処理を指定できます。

変更

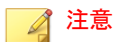
スタンプの挿入や件名へのタグ付けなど、メッセージや添付ファイルに対する変更を指示します。

監視

通知を送信したり、メッセージをさらに詳しく解析するためにアーカイブに保管または Bcc 送信したりするように指示します。

手順

1. [手順 2: 検索条件の選択] 画面で [次へ] をクリックします。
[手順 3: 処理の選択] 画面が表示されます。

**注意**

この手順で表示される画面は、作成しているルールの種類に応じて異なります。ウイルス対策ルールには2つのタブがあり、基本処理と特殊なウイルスに対する処理を設定できます。

「その他」のルールの処理を指定する

手順

1. [インターセプト] を設定します。

オプション	説明
メッセージをインターセプトしない	メッセージはインターセプトされません。他のルールが指定されている場合は、InterScan MSS によってメッセージが処理されます。指定されていない場合、InterScan MSS はネットワークにメッセージを渡します。
メッセージ全体を削除	メッセージとすべての添付ファイルを削除します。
次の場所に隔離	InterScan MSS は、メッセージとその添付ファイルを、ドロップダウンボックスから選択した隔離領域に格納します。
次の受信者に変更	メッセージを別の受信者に送信します。受信者のメールアドレスを指定し、複数の受信者がある場合はセミコロン (;) で区切ります。
中継	InterScan MSS では、メッセージを特定のメールサーバに転送します。ネットワーク上にメッセージを処理できる安全なメッセージサーバがある場合は、[中継] を選択します。次の項目を設定します。 ・ [ホスト] に、メールサーバの FQDN または IP アドレスを指定します。 ・ [ポート] に、メールサーバがメールトラフィックを受信するポート番号を指定します。

オプション	説明
	 注意 InterScan MSS では、中継後のメッセージを追跡することはできません。中継後のメッセージは、InterScan MSS で制御されなくなるため、追跡できなくなります。

2. [変更] を設定します。

オプション	説明
X-ヘッダの挿入	メッセージのヘッダにユーザ指定メッセージを挿入します。
添付ファイルを削除	InterScan MSS が実行する処理を選択します。 - 一致する添付ファイルを削除: 添付ファイルの検索条件に一致する添付ファイルのみを削除します。 - すべての添付ファイルを削除: すべての添付ファイルを削除します。
本文にスタンプを挿入	テキストをメッセージの先頭または末尾に挿入します。挿入するスタンプ名をドロップダウンボックスから選択するか、[編集] をクリックして [スタンプ] 画面に移動し、スタンプを管理します。
件名にタグを挿入	メッセージの件名にテキストを追加します。[件名にタグを挿入] をクリックしてタグを編集します。
配信を保留	指定した時刻まで配信を遅らせます。ドロップダウンボックスから、時間と分を選択します。

3. [監視] を設定します。

オプション	説明
ポリシー通知の送信	1 人または複数の受信者にメッセージを送信します。通知の種類を選択するには、[ポリシー通知の送信] をクリックします。通知の作成手順については、 226 ページの「ポリシー通知」 を参照してください。
変更済みメッセージの保存先	メッセージをアーカイブ領域にアーカイブします。

オプション	説明
Bcc	メッセージを別の受信者に Bcc で送信します。受信者のメールアドレスを指定し、複数のアドレスはセミコロン (;) で区切ります。[Bcc] オプションを選択すると、本来の受信者に知られることなく別の受信者にもメッセージを送信できます。

「ウイルス対策」ルールの基本処理を指定する

基本処理を使用して、メッセージが [手順 2: 検索条件の選択] で指定された検索条件と一致した場合の初期設定処理を指定できます。

手順

1. [インターセプト] を設定します。

オプション	説明
メッセージをインターセプトしない	メッセージはインターセプトされません。他のルールが指定されている場合は、InterScan MSS によってメッセージが処理されます。指定されていない場合、InterScan MSS はネットワークにメッセージを渡します。
メッセージ全体を削除	メッセージとすべての添付ファイルを削除します。
次の場所に隔離	InterScan MSS は、メッセージとその添付ファイルを、ドロップダウンボックスから選択した隔離領域に格納します。
次の受信者に変更	メッセージを別の受信者に送信します。受信者のメールアドレスを指定し、複数の受信者がある場合はセミコロン (;) で区切ります。
中継	InterScan MSS では、メッセージを特定のメールサーバに転送します。ネットワーク上にメッセージを処理できる安全なメッセージサーバがある場合は、[中継] を選択します。次の項目を設定します。 ・ [ホスト] に、メールサーバの FQDN または IP アドレスを指定します。 ・ [ポート] に、メールサーバがメールトラフィックを受信するポート番号を指定します。

オプション	説明
	 注意 InterScan MSS では、中継後のメッセージを追跡することはできません。中継後のメッセージは、InterScan MSS で制御されないため、それ以上追跡できません。

2. [変更] を設定します。



注意

[InterScan MSS でウイルスが検出された場合] のオプションは、ウイルス対策ルールに対してのみ使用することができます。

オプション	説明
InterScan MSS でウイルスが検出された場合	チェックボックスをオンにして、InterScan MSS がウイルスまたは他の不正プログラムを検出した場合の処理を有効にし、以下のいずれかをクリックします。 ・ トレンドマイクロの推奨処理: InterScan MSS が、特定の種類のウイルス/不正プログラムに対して事前設定された検索処理を自動的に使用できるようにします。 ・ ウイルス駆除不能な場合: InterScan MSS が添付ファイルを駆除できない場合に、実行する処理を選択します。 ・ 一致する添付ファイルを削除: ウイルス/不正プログラムが組み込まれた添付ファイルのみを削除します。 ・ すべての添付ファイルを削除: すべての添付ファイルを削除します。 ・ 添付ファイルを削除: InterScan MSS が実行する処理を選択します。 ・ 一致する添付ファイルを削除: ウイルス/不正プログラムが組み込まれた添付ファイルのみを削除します。 ・ すべての添付ファイルを削除: すべての添付ファイルを削除します。
X-ヘッダの挿入	メッセージのヘッダにユーザ指定メッセージを挿入します。

オプション	説明
	 注意 複数のルールで X-header の追加を設定していても、メッセージには X-header が 1 回のみ表示されます。X-header は、最後のルールの設定に従って表示されます。
本文にスタンプを挿入	テキストをメッセージの先頭または末尾に挿入します。挿入するスタンプ名をドロップダウンボックスから選択するか、[編集] をクリックして [スタンプ] 画面に移動し、スタンプを管理します。
本文に安全スタンプを挿入	クリーンなメッセージにテキストを挿入して、メッセージが安全であることを示します。挿入するスタンプ名をドロップダウンボックスから選択するか、[編集] をクリックして [スタンプ] 画面に移動し、スタンプを管理します。  注意 [標準メッセージにスタンプを挿入] オプションは、[特殊処理] タブでは使用できません。
件名にタグを挿入	メッセージの件名にテキストを追加します。[件名にタグを挿入] をクリックしてタグを編集します。
配信を保留	指定した時刻まで配信を遅らせます。ドロップダウンボックスから、時間と分を選択します。

3. [監視] を設定します。

オプション	説明
ポリシー通知の送信	1 人または複数の受信者に通知メッセージを送信します。通知の種類を選択するには、[ポリシー通知の送信] をクリックします。通知の作成手順については、 226 ページの「ポリシー通知」 を参照してください。
変更済みメッセージの保存先	メッセージをアーカイブ領域にアーカイブします。
Bcc	メッセージを別の受信者に Bcc で送信します。受信者のメールアドレスを指定し、複数のアドレスはセミコロン (;) で区切ります。[Bcc]

オプション	説明
	オプションを選択すると、本来の受信者に知られることなく別の受信者にもメッセージを送信できます。

「ウイルス対策」ルールの特殊処理を指定する

特殊処理設定を使用して、メッセージが次の基準のいずれかに一致した場合の処理を指定できます。この画面で指定する処理は、[基本処理] タブで指定した初期設定の処理に優先します。

ルールを追加

?

[ポリシーリスト](#) > 新規ルール

手順1 >>> 手順2 >>> 手順3: 処理の選択 >>> 手順4

< 戻る

次へ >

キャンセル

基本処理

特殊処理

☐ マスメーリング用処理を有効にする (他のすべての処理に優先されます) ▼

☐ スパイウェア対策用処理を有効にする (他のすべての処理に優先されます) ▼

☐ IntelliTrap用処理を有効にする (他のすべての処理に優先されます) ▼

< 戻る

次へ >

キャンセル

- ・ マスメーリング: マスメーリングメッセージが検出されると、このセクションで指定した処理が InterScan MSS により実行されます。
- ・ スパイウェア: [手順 2: 検索条件の選択] 画面で [スパイウェア検索] オプションのいずれかを選択している場合は、対応する処理を指定できます。スパイウェアが検出されると、ここで指定した処理が実行されます。



注意

処理が選択されていない場合、[スパイウェア検索] の条件に一致するメッセージに対して初期設定の処理が実行されます。

- ・ IntelliTrap を有効にする: [手順 2: 検索条件の選択] 画面で [IntelliTrap の設定] オプションが選択されている場合、対応する処理を指定できます。

**注意**

処理が選択されていない場合、[IntelliTrap の設定] の条件に一致するメッセージに対して初期設定の処理が実行されます。

件名タグを作成する

受信者に、InterScan MSS がメッセージの添付ファイルに対して処理を実行したことや、メッセージがルールを検索条件に違反していることを通知するには、件名の先頭に短いメッセージを追加します。本来の受信者が最終的に受信するメッセージに対してのみタグを追加します。検索条件に違反するメッセージを削除するルールを設定している場合は、タグの追加は必要ありません。

手順

1. 処理の選択時に、[変更] 処理の [件名にタグを挿入] をクリックします。
編集画面が表示されます。
2. [タグ] の横に、件名に挿入するテキストを指定します。
3. デジタル署名付きのメッセージを破損する危険性を回避するには、[デジタル署名されたメッセージにタグを挿入しない] を選択します。
4. [保存] をクリックして、処理の選択を続行します。
5. タグを使用するには、[変更] の [件名にタグを挿入] の横にあるチェックボックスをオンにします。

ポリシーを完成させる

ルールに対する処理を選択したら、そのルールに名前を付けて有効にします。また、ルールに検索する順序を示す番号も割り当てます。InterScan MSS では、将来参照する際に必要と思われるメモをそのルールに対して追加することもできます。既存のルールのこの情報を変更することもできます。

ルールを表示する場合は、次の点に注意してください。

- ・  緑のチェックマークボタンは、ルールが有効であることを示しています。
- ・  赤の X マークボタンは、ルールは保存されているが無効になっていることを示しています。
- ・  灰色の X マークボタンは、ルールと製品のアクティベーションコードがどちらも無効になっていることを示しています。

**注意**

ボタンをクリックして、ルールを有効または無効にできます。

ルールを完成させる

手順

1. 以下のいずれかの方法を使用して画面を開きます。
 - ・ 新しいポリシーを作成する場合は、[手順 3: 処理の選択] 画面で [次へ] をクリックします。[手順 4: 名前と順序] 画面が表示されます。

- 既存のポリシーを完成させる場合は、[ポリシー] > [ポリシーリスト] 画面のポリシーリストでポリシーの名前をクリックします。

ルールの追加 

ポリシーリスト > 新規ルール

手順1 >>> 手順2 >>> 手順3 >>> **手順4: 名前と順序**

[< 戻る](#) [完了](#) [キャンセル](#)

ルール **備考**

☒ 有効

ルール名:

順序番号:

順序	既存のルール	処理	変更日	ステータス
	グローバルDKIM適用ルール	隔離	2013/02/26	
1	グローバルウイルス対策ルール	トレンドマイクロの推奨処理	2013/03/06	
2	初期設定のスパムメール対策ルール	隔離	2013/03/06	
3	復号化できないメッセージの初期設定ルール	隔離...	2013/03/06	
4	パスワードで保護された添付ファイルの初期設定ルール	スタンプ	2013/03/06	
5	コンプライアンス - 医療情報	隔離...	2013/02/26	
6	コンプライアンス - 金融および銀行取引	隔離...	2013/02/26	
7	コンプライアンス - 個人識別番号	隔離...	2013/02/26	
8	コンプライアンス - クレジットカード名義人情報	隔離...	2013/02/26	

受信者と送信者

送信 宛先 すべてのユーザ および 差出人 *@trend02.com

検索条件 件名が空白

処理 メッセージを隔離

[< 戻る](#) [完了](#) [キャンセル](#)

- [有効] チェックボックスをオンにして、ルールを有効にします。
- [ルール名] フィールドにルールの名前を指定します。
- [順序番号] フィールドに、検索を実行する優先順位を指定します。指定した順位でメッセージにルールが適用されます。
- [備考] タブをクリックします。

[備考] 画面が表示されます。

ルールの追加

ポリシーリスト > 新規ルール

手順1 >>> 手順2 >>> 手順3 >>> 手順4: 名前と順序

< 戻る 完了 キャンセル

ルール 備考

作成日:
最終更新日:
備考:

Blocks outgoing email messages from test.com

< 戻る 完了 キャンセル

6. 備考を指定して、新しいルールを他のルールと区別します。
7. 新しいポリシーを作成している場合は、画面上の情報が正しいことを確認します。ルールに関する情報が間違っている場合は、[< 戻る] をクリックして修正します。
8. [完了] をクリックして新しいルールを完成させるか、[保存] をクリックして既存のルールを変更します。

第 18 章

暗号化の設定

この章では、InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) の暗号化を設定する手順について説明します。

この章の内容は次のとおりです。

- ・ 310 ページの「暗号化を設定する」
- ・ 311 ページの「メッセージトラフィックを暗号化する」
- ・ 311 ページの「暗号化ポリシーを設定する」

暗号化を設定する

Trend Micro Email Encryption が機能するには、ドメインを登録する必要があります。ドメインを登録すると、Trend Micro Email Encryption は登録および確定されたドメインに固有の暗号化キーを取得します。そのキーがないと、Trend Micro Email Encryption はメッセージを暗号化できません。



注意

ログインに加えて、このメールアドレスはその他の製品関連の目的 (パスワードのリセットや登録の通知など) にのみ使用されます。マーケティング目的で使用されたり、第三者に販売されることはありません。Email Encryption に登録することで、スパムメールを受信することはありません。

分散環境では、[暗号化設定] > [InterScan MSS] タブに表示される ID が、上位 InterScan MSS とすべての下位 InterScan MSS で共有されます。

暗号化の種類

[IBE 暗号化の除外] ルールと、[メッセージを復号化できません] ポリシールールには違いがあります。

表 18-1. 暗号化の種類

特長	説明
IBE 暗号化の除外	このルールは、InterScan MSS で ID ベース暗号 (IBE) アルゴリズムを使用してメッセージを復号化または暗号化できない場合に実行されます。
メッセージを復号化できません	このルールは、PGP (Pretty Good Privacy) 暗号化または S/MIME (Secure/Multipurpose Internet Mail Extensions) 暗号化を使用して暗号化されたメッセージを検出するために使用されます。 InterScan MSS では、IBE を使用して暗号化されたメッセージを復号化できます。ただし、事前にドメインを Trend Micro Email Encryption サーバに登録する必要があります。その後、InterScan MSS はメッセージをそのドメインから復号化できます。

メッセージトラフィックを暗号化する

メールの暗号化が機能するためには、Trend Micro Encryption Email サービスにドメインを登録している必要があります。詳細については、[104 ページの「ドメインを暗号化サービスに登録する」](#)を参照してください。

暗号化を設定したら、InterScan MSS でメッセージを復号化または暗号化してメッセージコンテンツを保護できるようになります。

暗号化されたメッセージトラフィックがネットワークに着信すると、InterScan MSS はメッセージを自動的に復号化して、指定したポリシールールに応じてメッセージを検索します。検索後に送信メッセージは再び暗号化され、メッセージコンテンツが保護されます。

暗号化ポリシーを設定する

ポリシーの検索処理として [メッセージを暗号化] を選択した場合、InterScan MSS でプレーンテキストメッセージコンテンツを暗号化できます。

受信メッセージを暗号化するルールを有効にした場合、privatepost.com からの登録およびサポートメッセージは暗号化されません。



注意

メッセージを暗号化することは最終的な処理です。この処理を実行すると、メッセージは目的の受信者に配信されます。

[メッセージを暗号化] を選択すると、[メッセージを配信] が自動的に選択され、次のオプションは利用できなくなります。[メッセージ全体を削除]、[次の受信者に変更]、および [配信を保留]。

第 19 章

検索除外の設定

この章では、InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) の検索の除外を設定する手順について説明します。

この章の内容は次のとおりです。

- ・ 314 ページの「検索除外を設定する」
- ・ 315 ページの「セキュリティ設定違反の除外を設定する」
- ・ 316 ページの「セキュリティ設定違反の検索処理を設定する」
- ・ 317 ページの「正しくない形式のメッセージの検索処理を設定する」
- ・ 319 ページの「暗号化されたメッセージの除外を設定する」
- ・ 320 ページの「暗号化されたメッセージの検索処理を設定する」
- ・ 321 ページの「仮想アナライザの検索の除外の検索処理を設定する」

検索除外を設定する

場合によっては、InterScan MSS による、DoS 攻撃の一環として送られてきた可能性のある特定種類のメッセージの検索を省略した方が望ましいことがあります。たとえば、非常にサイズの大きいファイルが添付されたメッセージを検索するには、InterScan MSS サーバの多大なリソースを要します。また、何百人もの受信者宛てに送信されたメッセージは、スパムメールか何らかの攻撃である可能性が非常に高いです。

検索除外を設定すると、InterScan MSS のリソースを消費してこれらのメッセージを検索する代わりに、これらのメッセージに対してただちに特定の処理を実行できます。



警告!

1. 検索除外で指定された処理を有効にするには、グローバルウイルス対策ルールが有効になっていることを確認してください。
2. 正しくない形式のメッセージに対して検索除外が実行されると、InterScan MSS では検索が停止し、対応する処理が実行されます。つまり、検索除外が実行されると InterScan MSS ではポリシールールが実行されません。

セキュリティ設定違反と IBE 暗号化の除外については、検索除外の処理が実行された後も InterScan MSS では検索が停止せず、他のポリシールールのチェックが続行されます。最終的な検索処理が発生すると、検索が停止します。

検索除外を設定する

手順

1. [ポリシー] > [検索の除外] の順に選択します。
2. いくつかの条件に基づいてメッセージの検索除外条件を設定するには、[除外設定] で [セキュリティ設定違反] リンクをクリックします。
[セキュリティ設定違反] 画面が表示されます。

3. 除外の種類に対して処理を設定するには、[処理] で対応するリンクをクリックします。
-

セキュリティ設定違反の除外を設定する

この画面で設定したセキュリティ設定違反の検索除外は、すべての送信者と受信者に適用されます。

手順

1. [検索の除外] 画面で、[除外] の [セキュリティ設定違反] をクリックします。
[セキュリティ設定違反] 画面が表示されます。
 2. InterScan MSS が検索できるメッセージの種類を制限するには、次の項目を設定します。
 - ・ メッセージの合計サイズが次の値を超える {} MB: 最大メガバイト数を指定します。
 - ・ 受信者の総数が次の値を超える {} 受信者: 最大受信者数を指定します。
 - ・ 圧縮ファイル内の埋め込み層の総数が次の値を超える {} 層: 最大階層数を選択します。
 - ・ いずれか1つのファイルの解凍後の合計サイズが次の値を超える {} MB: 最大メガバイト数を指定します。
 - ・ 圧縮ファイル内のファイルの総数が次の値を超える {} ファイル: 最大ファイル数を指定します。
 3. [保存] をクリックします。
[検索の除外] 画面が再表示されます。
-

セキュリティ設定違反の検索処理を設定する

この画面で設定したセキュリティ設定違反の検索処理は、すべての送信者と受信者に適用されます。

手順

1. [検索の除外] 画面で、[セキュリティ設定違反] の [処理] にある処理名のリンクをクリックします。

処理を設定する画面が表示されます。

2. [インターセプト] を設定します。

オプション	説明
メッセージをインターセプトしない	InterScan MSS では、メッセージに対して処理を実行しません。他のルールが存在する場合は、そのルールを使用してメッセージを処理します。
メッセージ全体を削除	メッセージとすべての添付ファイルを削除します。
次の場所に隔離	InterScan MSS は、メッセージとその添付ファイルを、ドロップダウンボックスから選択した隔離領域に格納します。新しい隔離領域の作成手順については、 390 ページの「隔離とアーカイブを設定する」 を参照してください。
中継	InterScan MSS では、メッセージを特定のメールサーバに転送します。ネットワーク上にメッセージを処理できる安全なメッセージサーバがある場合は、[中継] を選択します。次の項目を設定します。 ・ [ホスト] に、メールサーバの FQDN または IP アドレスを指定します。 ・ [ポート] に、メールサーバがメールトラフィックを受信するポート番号を指定します。  注意 InterScan MSS では、中継後のメッセージを追跡することはできません。中継後のメッセージは、InterScan MSS で制御されないため、それ以上追跡できません。

オプション	説明
	InterScan MSS では、IPv6 中継サーバアドレスをサポートしません。

3. [監視] を設定します。

オプション	説明
ポリシー通知の送信	1 人または複数の受信者に通知メッセージを送信します。通知の種類を選択するには、[ポリシー通知の送信] をクリックします。通知の作成手順については、 226 ページの「ポリシー通知」 を参照してください。
保存先	メッセージをアーカイブ領域にアーカイブします。新しいアーカイブ領域の作成手順については、 390 ページの「隔離とアーカイブを設定する」 を参照してください。
Bcc	メッセージを別の受信者に Bcc で送信します。受信者のメールアドレスを指定し、複数のアドレスはセミコロン (;) で区切ります。[Bcc] オプションを選択すると、本来の受信者に知られることなく別の受信者にもメッセージを送信できます。

4. [保存] をクリックします。

正しくない形式のメッセージの検索処理を設定する

この画面で設定した、正しくない形式のメッセージに関するセキュリティ設定違反の検索処理は、すべての送信者と受信者に適用されます。

手順

1. [検索の除外] 画面で、[正しくない形式のメッセージ] の [処理] にある処理名のリンクをクリックします。
処理を設定する画面が表示されます。
2. [インターセプト] を設定します。

オプション	説明
メッセージをインターセプトしない	InterScan MSS では、メッセージに対して処理を実行しません。他のルールが存在する場合は、そのルールを使用してメッセージを処理します。
メッセージ全体を削除	メッセージとすべての添付ファイルを削除します。
次の場所に隔離	InterScan MSS は、メッセージとその添付ファイルを、ドロップダウンボックスから選択した隔離領域に格納します。
中継	InterScan MSS では、メッセージを特定のメールサーバに転送します。ネットワーク上にメッセージを処理できる安全なメッセージサーバがある場合は、[中継] を選択します。次の項目を設定します。 ・ [ホスト] に、メールサーバの FQDN または IP アドレスを指定します。 ・ [ポート] に、メールサーバがメールトラフィックを受信するポート番号を指定します。  注意 InterScan MSS では、中継後のメッセージを追跡することはできません。中継後のメッセージは、InterScan MSS で制御されないため、それ以上追跡できません。 InterScan MSS では、IPv6 中継サーバアドレスをサポートしません。

3. [監視] を設定します。

オプション	説明
ポリシー通知の送信	1 人または複数の受信者に通知メッセージを送信します。通知の種類を選択するには、[ポリシー通知の送信] をクリックします。通知の作成手順については、 226 ページの「ポリシー通知」 を参照してください。
保存先	メッセージをアーカイブ領域にアーカイブします。
Bcc	メッセージを別の受信者に Bcc で送信します。受信者のメールアドレスを指定し、複数のアドレスはセミコロン (;) で区切ります。[Bcc] オプ

オプション	説明
	シヨンを選択すると、本来の受信者に知られることなく別の受信者にもメッセージを送信できます。

4. [保存] をクリックします。

暗号化されたメッセージの除外を設定する

この画面で指定された制限のいずれかを超えるメッセージは、InterScan MSS で復号化または暗号化されません。

手順

1. [ポリシー] > [検索の除外] > [IBE 暗号化の除外] の順に選択します。
2. InterScan MSS で処理する暗号化または復号化メッセージを制限するには、次の項目を設定します。
 - ・ 暗号化メッセージのサイズが次の値を超える {} MB: 最大メガバイト数を指定します。
 - ・ 復号化メッセージのサイズが次の値を超える {} MB: 最大メガバイト数を指定します。
 - ・ 受信者の総数が次の値を超える {} 受信者: 最大受信者数を指定します。
 - ・ 送信メッセージを暗号化できない時: InterScan MSS で暗号化できない送信メッセージに対して InterScan MSS で処理を実行するよう指定する場合は、このオプションをオンにします。
 - ・ 送信メッセージを復号化できない時: InterScan MSS で復号化できない送信メッセージに対して InterScan MSS で処理を実行するよう指定する場合は、このオプションをオンにします。
3. [保存] をクリックします。

[検索の除外] 画面が再表示されます。

暗号化されたメッセージの検索処理を設定する

手順

1. [ポリシー] > [検索の除外] の順に選択します。
2. [IBE 暗号化の除外] で [隔離および通知] リンクをクリックします。
処理を設定する画面が表示されます。
3. [インターセプト] で、次のいずれかのオプションを選択します。
 - ・ メッセージをインターセプトしない: InterScan MSS では、メッセージを処理しません。
 - ・ メッセージ全体を削除: メッセージとすべての添付ファイルを削除します。
 - ・ 次の場所に隔離: InterScan MSS は、メッセージとその添付ファイルを、ドロップダウンボックスから選択した隔離領域に格納します。
新しい隔離領域の作成手順については、[390 ページの「隔離とアーカイブを設定する」](#)を参照してください。
 - ・ 中継: InterScan MSS では、メッセージを特定のメールサーバに転送します。ネットワーク上にメッセージを処理できる安全なメッセージサーバがある場合は、[中継] を選択します。次の項目を設定します。
 - ・ [ホスト] に、メールサーバの FQDN または IP アドレスを指定します。
 - ・ [ポート] に、メールサーバがメールトラフィックを受信するポート番号を指定します。



注意

InterScan MSS では、中継後のメッセージを追跡することはできません。中継後のメッセージは、InterScan MSS で制御されないため、それ以上追跡できません。

4. [監視] で、次のいずれかのチェックボックスをオンにします。
 - ・ ポリシー通知の送信: 1 人または複数の受信者にメッセージを送信します。通知の種類を選択するには、[ポリシー通知の送信] をクリックします。通知の作成手順については、[226 ページの「ポリシー通知」](#)を参照してください。
 - ・ 保存先: メッセージをアーカイブ領域にアーカイブします。新しいアーカイブ領域の作成手順については、[390 ページの「隔離とアーカイブを設定する」](#)を参照してください。
 - ・ Bcc: メッセージを別の受信者に Bcc で送信します。受信者のメールアドレスを指定し、複数のアドレスはセミコロン (;) で区切ります。[Bcc] オプションを選択すると、本来の受信者に知られることなく別の受信者にもメッセージを送信できます。
 5. [保存] をクリックします。
-

仮想アナライザの検索の除外の検索処理を設定する

手順

1. [ポリシー] > [検索の除外] の順に選択します。
2. [仮想アナライザの検索の除外] で [隔離および通知] リンクをクリックします。

処理を設定する画面が表示されます。
3. [インターセプト] で、次のいずれかのオプションを選択します。
 - ・ メッセージをインターセプトしない: InterScan MSS では、メッセージを処理しません。
 - ・ メッセージ全体を削除: メッセージとすべての添付ファイルを削除します。

- ・ 次の場所に隔離: InterScan MSS は、メッセージとその添付ファイルを、ドロップダウンボックスから選択した隔離領域に格納します。新しい隔離領域の作成手順については、[390 ページの「隔離とアーカイブを設定する」](#)を参照してください。
- ・ 中継: InterScan MSS では、メッセージを特定のメールサーバに転送します。ネットワーク上にメッセージを処理できる安全なメッセージサーバがある場合は、[中継]を選択します。次の項目を設定します。
 - ・ [ホスト] に、メールサーバの FQDN または IP アドレスを指定します。
 - ・ [ポート] に、メールサーバがメールトラフィックを受信するポート番号を指定します。

**注意**

InterScan MSS では、中継後のメッセージを追跡することはできません。中継後のメッセージは、InterScan MSS で制御されないため、それ以上追跡できません。

4. [監視] で、次のいずれかのチェックボックスをオンにします。

- ・ ポリシー通知の送信: 1 人または複数の受信者にメッセージを送信します。通知の種類を選択するには、[ポリシー通知の送信] をクリックします。通知の作成手順については、[226 ページの「ポリシー通知」](#)を参照してください。
- ・ 保存先: メッセージをアーカイブ領域にアーカイブします。新しいアーカイブ領域の作成手順については、[390 ページの「隔離とアーカイブを設定する」](#)を参照してください。
- ・ BCC: メッセージを別の受信者に Bcc で送信します。受信者のメールアドレスを指定し、複数のアドレスはセミコロン (;) で区切ります。[Bcc] オプションを選択すると、本来の受信者に知られることなく別の受信者にもメッセージを送信できます。

5. [保存] をクリックします。

第 20 章

既存のポリシーの設定

この章では、InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) ポリシーを作成、変更、および管理する手順について説明します。

この章の内容は次のとおりです。

- ・ 324 ページの「既存ポリシーを変更する」
- ・ 327 ページの「ポリシーの例 1」
- ・ 332 ページの「ポリシーの例 2」
- ・ 337 ページの「アスタリスクワイルドカードを使用する」

既存ポリシーを変更する

ルールの変更手順には、作成時とは異なるプロセスを使用します。

手順

1. [ポリシー] > [ポリシーリスト] の順に選択します。
2. 編集するルールの名前をクリックします。
そのルールの [ルールの概要] 画面が表示されます。
3. [受信者と送信者] の [編集] をクリックします。
4. ルートを設定します。
詳細については、[260 ページの「ルートを指定する」](#)を参照してください。
5. 次のいずれかで [編集] をクリックします。
 - ・ 検索条件 (ウイルス対策ルールとその他のルール)
 - ・ DKIM 検証を行うドメイン (グローバル DKIM ルール)
6. 検索を設定します。詳細については、次を参照してください。
 - ・ ウイルス対策ルールとその他のルール:[267 ページの「検索条件を指定する」](#)
 - ・ グローバル DKIM 適用ルール:[325 ページの「グローバル DKIM 適用ルールでドメインリストを使用する」](#)
 - ・ [325 ページの「グローバル DKIM 適用ルールでドメインリストを使用する」](#)
7. [処理] で [編集] をクリックします。
8. 処理を設定します。
詳細については、[297 ページの「処理を指定する」](#)を参照してください。

9. [保存] をクリックします。
-

グローバル DKIM 適用ルールでドメインリストを使用する

InterScan MSS では、次に該当するドメインリストのドメインから受信したメッセージをスパムメールとしてマークします。

- ・ DKIM 検証に合格していない
- ・ DKIM 署名がない

グローバル DKIM 適用ルールのドメインリストにドメインを追加する

手順

1. [ポリシー] > [ポリシーリスト] の順に選択します。
[ポリシー] 画面が表示されます。
2. [グローバル DKIM 適用ルール] リンクをクリックします。
[ルールの概要] 画面が表示されます。
3. [DKIM 検証を行うドメイン] 行で [編集] をクリックします。
[検索条件] 画面が表示されます。
4. ドメインリストへの追加には、次のいずれかの方法を使用します。
 - ・ 手動の場合
 - a. ドメイン名を指定します。
 - b. [追加] をクリックします。
 - ・ リストをインポートする場合

**注意**

ドメインリストにテキストファイルをインポートする場合は、1 行に 1 つずつドメインを記載します。

- a. [インポート] をクリックします。[DKIM 適用リストのインポート] が表示されます。
 - b. ファイルのパスと名前を指定するか、[参照] をクリックしてファイルを探します。
 - c. 次のいずれかを選択します。
 - ・ 現在のリストとマージ
 - ・ 現在のリストを上書き
 - d. [インポート] をクリックします。
5. [保存] をクリックします。

既存のルールを受信者と送信者を変更する

手順

1. [ポリシー] > [ポリシーリスト] の順に選択します。
2. 編集するルールの名前をクリックします。
そのルールの [概要 (ポリシー名)] 画面が表示されます。
3. [受信者と送信者] の [編集] をクリックします。
4. [このルールの適用対象] の横にあるドロップダウンリストからポリシールートの種類を選択します。
 - ・ 受信メッセージ
 - ・ 送信メッセージ
 - ・ 受信メッセージと送信メッセージの両方

- ・ POP3
 - ・ すべてのメッセージ
5. 受信者と送信者を選択します。
- ・ 受信メッセージの場合は、内部アドレスの範囲内にある受信者のメールアドレスを指定します。たとえば、内部アドレスが `example.com` の場合、有効な受信者のアドレスには `jim@example.com`、`bob@example.com` などがあります。
 - ・ 送信メッセージの場合は、内部アドレスの範囲内にある送信者のアドレスを指定します。たとえば、内部アドレスが `example.com` の場合、有効な送信者のアドレスには `jim@example.com`、`bob@example.com` などがあります。
 - ・ 受信メッセージと送信メッセージの両方の場合において、ルールは、メールアドレスに一致する受信者または送信者に適用されます。
 - ・ POP3 が選択されている場合、ルートを設定できません。ルールはすべての POP3 ルートに適用されます。
 - ・ ルールに対して [すべてのメッセージ] を選択した場合、そのルールは任意の送信者から任意の受信者へのメッセージにも適用されます。
6. [保存] をクリックします。
-

ポリシーの例 1

特定のファイル名または拡張子を持つ添付ファイルを削除して、該当する受信メッセージに説明のスタンプを挿入して受信者に送信するルールを作成します。

- ・ [328 ページの「手順 1: ルートを指定する」](#)
- ・ [329 ページの「手順 2: 検索条件を指定する」](#)
- ・ [330 ページの「手順 3: 処理を指定する」](#)

332 ページの「手順 4: 優先順位を指定する」

手順 1: ルートを指定する

手順

1. [ポリシー] > [ポリシーリスト] の順に選択します。
 2. [追加] をクリックします。
 3. ドロップダウンリストから [その他] を選択します。
- [手順 1: 受信者と送信者の選択] 画面が表示されます。

ルールの追加



ポリシーリスト > 新規ルール

➤ 手順1: 受信者と送信者の選択 >>> 手順2 >>> 手順3 >>> 手順4

このルールの適用対象 受信メッセージ

< 戻る

次へ >

キャンセル

宛先	受信者
差出人	送信者
除外設定	送信者から受信者

受信者と送信者

受信

宛先 すべてのユーザ

および

差出人 すべてのユーザ

< 戻る

次へ >

キャンセル

4. [このルール適用対象] の横にあるドロップダウンリストから、[受信メッセージ] を選択します。
 5. [受信者] リンクをクリックします。
[アドレスの選択] 画面が表示されます。
 - ・ このルールを任意の受信者に適用するには、[すべてのユーザ] を選択します。
 - ・ このルールを特定の受信者に適用するには、[選択したアドレスのいずれか] を選択し、メールの宛先のアドレスまたはグループを指定します。
 6. [保存] をクリックします。
[手順 1: 受信者と送信者の選択] 画面が再表示されます。
-

手順 2: 検索条件を指定する

手順

1. [次へ] をクリックします。
[手順 2: 検索条件の選択] 画面が表示されます。
2. [次の場合にルール処理を実行する] の横にある [いずれかの条件に一致 (OR)] を選択します。
3. [名前または拡張子] 条件を有効にするには、その横のチェックボックスをオンにします。
4. [名前または拡張子] をクリックします。
[添付ファイルの名前または拡張子] 画面が表示されます。

添付ファイルの名前または拡張子 

新規ルール > 添付ファイルの名前または拡張子

選択: 選択された添付ファイル名 ▼

☐ 検索するファイル拡張子 (推奨) ▼

☐ 検索の検討が推奨されるファイル拡張子 ▼

☐ 指定のファイル名

完全なファイル名を使用し、各エントリをセミコロン (;) で区切って入力)

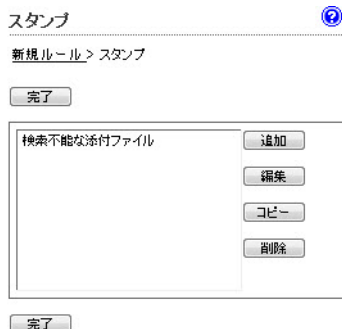
5. [検索するファイル拡張子 (推奨)] または [検索の検討が推奨されるファイル拡張子] を選択します。
 6. [保存] をクリックします。
- [手順 2: 検索条件の選択] 画面が再表示されます。

手順 3: 処理を指定する

手順

1. [次へ] をクリックします。
- [手順 3: 処理の選択] 画面が表示されます。
2. [変更] で [添付ファイルを削除] 処理を有効にするには、その横のチェックボックスをオンにします。
 3. [一致する添付ファイル] が選択されてない場合、ドロップダウンリストから選択します。
 4. [本文にスタンプを挿入] チェックボックスをオンにします。
 5. ドロップダウンリストに利用できる適切なスタンプがない場合、[編集] をクリックします。

[スタンプ] 画面が表示されます。



6. [追加] をクリックして、新しいスタンプを作成します。
[スタンプを追加] 画面が表示されます。



7. 必要な情報を指定します。
8. [保存] をクリックします。
[スタンプ] 画面が再表示されます。
9. [完了] をクリックします。
[処理の選択] 画面が再表示されます。
10. ドロップダウンリストから新しく作成したスタンプを選択します。

手順 4: 優先順位を指定する

手順

1. [次へ] をクリックします。
[手順 4: 名前と順序] 画面が表示されます。
 2. ルールの名前と順序の番号を指定します。
 3. [完了] をクリックします。
新しく作成したルールは、[ポリシーリスト] 画面で強調表示されます。
-

ポリシーの例 2

件名または本文に特定のキーワードを含むメッセージを隔離するルールを作成して、このルールを管理者を除くすべての受信者に適用します。

- ・ [332 ページの「手順 1: ルートを指定する」](#)
- ・ [334 ページの「手順 2: 検索条件を指定する」](#)
- ・ [337 ページの「手順 3: 処理を指定する」](#)
- ・ [337 ページの「手順 4: 優先順位を指定する」](#)

手順 1: ルートを指定する

手順

1. [ポリシー] > [ポリシーリスト] の順に選択します。
[ポリシーリスト] 画面が表示されます。
2. [追加] をクリックします。
3. ドロップダウンリストから [その他] を選択します。

[手順 1: 受信者と送信者の選択] 画面が表示されます。

4. [この規則の適用対象] の横にあるドロップダウンリストから、[受信メッセージ] を選択します。
5. [受信者] リンクをクリックします。
[アドレスの選択] 画面が表示されます。
6. [すべてのユーザ] を選択します。
7. [保存] をクリックします。

[手順 1: 受信者と送信者の選択] 画面が再表示されます。

8. [除外設定] の横の [送信者から受信者] リンクをクリックします。

[除外設定] 画面が表示されます。

次を除く受信メッセージ 

ルールの追加 > 次を除く受信メッセージ

アドレスの選択

差出人 (送信者)

宛先 (受信者)

メールアドレスの入力 

メールアドレスの入力 

差出人	宛先

9. [差出人 (送信者)] に、「*@*」と入力して任意の送信者を指定します。
10. [宛先 (受信者)] に管理者のメールアドレスを指定します。
11. [追加] をクリックします。
リストに送信者と受信者のペアが表示されます。
12. 他の管理者または受信者を追加するには、手順 9～11 を繰り返します。

- すべての必要な受信者を追加したら、[保存] をクリックします。

[手順 1: 受信者と送信者の選択] 画面が再表示されます。

手順 2: 検索条件を指定する

手順

- [次へ] をクリックします。
[手順 2: 検索条件の選択] 画面が表示されます。
- [次の場合にルール of の処理を実行する] の横にある [いずれかの条件に一致 (OR)] を選択します。
- [内容] で [件名のキーワード] 条件を有効にするには、その横のチェックボックスをオンにします。
- [件名のキーワード] をクリックします。
[キーワード] 画面が表示されます。

キーワードおよび式



追加 コピー 削除		
☐ キーワード名および式名	条件	ポリシーで使用
☐ 誹謗中傷	指定した任意のキーワード	0
☐ デマメール	指定した任意のキーワード	0
☐ チェーンメール	指定した任意のキーワード	0
☐ 性差別	指定した任意のキーワード	0
☐ 人種差別	指定した任意のキーワード	0
☐ HTML/スクリプトメッセージ	しきい値を超えています	0
☐ クレジットカード番号	指定した任意のキーワード	0
☐ 社会保障番号	指定した任意のキーワード	0
☐ バウンスメール	指定した任意のキーワード	0
☐ test	指定した任意のキーワード	0

- 既存のリストに必要なキーワードがない場合、[追加] をクリックして新しいキーワードリストを作成します。

[新規キーワード] 画面が表示されます。

キーワードおよび式 

新規ルール > キーワードおよび式 > 新規キーワード

保存 キャンセル

リスト名:

一致:

 追加  削除

☐	キーワード/正規表現	大文字/小文字の区別
☐	キーワード/正規表現	大文字/小文字の区別

保存 キャンセル

- 必要な情報を指定します。
- 個々のキーワードを追加するには、[追加] をクリックします。

[キーワードおよび式の追加] 画面が表示されます。

キーワードおよび式の追加 

新規ルール > キーワードおよび式 > キーワードおよび式の追加

保存 キャンセル

キーワードと正規表現の任意の組み合わせを使用してキーワードを定義できます。
 . * | () { } [] ^ \$ % + , または ? という文字の直前には、[] と入力してください。

保存 キャンセル

- 必要なキーワードを指定して、[保存] をクリックします。
 [新規キーワード] 画面が再表示されます。

9. 手順 7 と 8 を繰り返して、キーワードを追加します。
10. 必要なキーワードをすべて追加したら、新しいキーワードリストの [リスト名] を指定して [保存] をクリックします。
[新規キーワード] 画面が再表示されます。
11. 新しいリストを選択し、[>>] をクリックしてリストを [選択済み] ボックスに挿入します。
12. [保存] をクリックします。
[手順 2: 検索条件の選択] 画面が再表示されます。
13. [本文のキーワード] 条件を有効にするには、その横のチェックボックスをオンにします。
14. [本文のキーワード] をクリックします。
[キーワード] 画面が表示されます。
15. 新しいキーワードリストを選択し、[>>] をクリックしてリストを [選択済み] ボックスに挿入します。
16. [保存] をクリックします。
[手順 2: 検索条件の選択] 画面が再表示されます。
[件名のキーワード] と [本文のキーワード] の両方が選択されていることを確認します。

内容	
☐	件名のキーワード
☐	件名が空白
☐	本文のキーワード
☐	ヘッダのキーワード
☐	添付ファイルのキーワード

手順 3: 処理を指定する

手順

1. [次へ] をクリックします。
[手順 3: 処理の選択] 画面が表示されます。
 2. [インターセプト] で [次の場所に隔離] を選択します。
 3. 初期設定の隔離領域を使用するか、ドロップダウンリストをクリックして使用したい隔離領域を選択します。
-

手順 4: 優先順位を指定する

手順

1. [次へ] をクリックします。
[手順 4: 名前と順序] 画面が表示されます。
 2. ルールの名前と順序の番号を指定します。
 3. [完了] をクリックします。
新しく作成したルールは、[ポリシーリスト] 画面で強調表示されます。
-

アスタリスクワイルドカードを使用する

ルートを定義する際のメールアドレス、およびファイル名には、アスタリスク (*) をワイルドカードとして使用できます。

メールアドレスのワイルドカード

ワイルドカードは、メールアドレスの名前またはドメインの部分に使用できます。有効なワイルドカードの例は、次のとおりです。

- ・ `name@*`: 名前全体を表します。
- ・ `*@domain.tld`、`name@*.tld`: 前者は特定のドメイン名とトップレベルドメイン (TLD) を持つすべてのメールアドレスを表し、後者は特定のユーザ名と TLD を持つすべてのメールアドレスを表します。
- ・ `*@*.tld`: 特定の TLD を持つすべてのメールアドレスを表します。

ワイルドカードは、サブドメインやトップレベルドメインの部分には使用できません。ワイルドカードは、他の文字列と組み合わせることはできず、単独で使用する必要があります。無効なワイルドカードの例は、次のとおりです。

- ・ `name@domain*.tld`: ワイルドカードでサブドメインを表すことはできません。
- ・ `name@domain.*`: ワイルドカードで TLD を表すことはできません。
- ・ `*name@domain.tld`: ワイルドカードとユーザ名の一部を組み合わせることはできません。

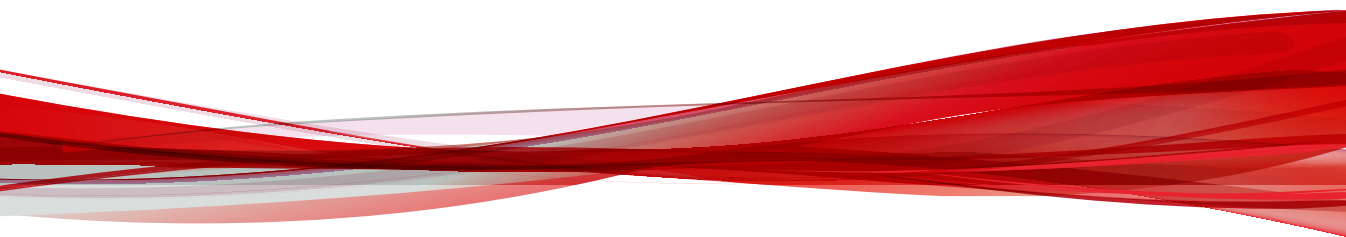
ファイル名のワイルドカード

ワイルドカードをメールアドレスと同様の方法でファイル名に使用できます。アスタリスクをファイル名の名前または拡張子の部分に使用します。ただし、名前や拡張子の一部として使用することはできません。有効なワイルドカードの例は、次のとおりです。

- ・ `*.*`: すべてのファイルを表します。
- ・ `*.拡張子`: 特定の拡張子のすべてのファイルを表します。
- ・ `名前.*`: 特定の名前を持つすべての拡張子のファイルを表します。
- ・ `*名前.*`: 名前の有効な表記方法です。
- ・ `名前.*拡張子`: 拡張子の有効な表記方法です。

パート IV

ネットワークの監視



第 21 章

ネットワークの監視

この章では、InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) の日常的な管理タスクの実行に必要な一般手順を説明します。

この章の内容は次のとおりです。

- ・ [342 ページの「ネットワークを監視する」](#)
- ・ [342 ページの「システムステータスを表示する」](#)

ネットワークを監視する

InterScan MSS には、ネットワークトラフィックを監視するためのツールセットが用意されています。InterScan MSS コンポーネントのパフォーマンスについての統計など、有用な情報を取得できます。また、さまざまな検索条件に一致するメッセージの詳細を表示するレポートも作成できます。

システムステータスを表示する

[システムステータス] 画面では、InterScan MSS のコンポーネントとサービスのステータスについての情報を一目で把握できます。

手順

1. [システムステータス] に移動します。
2. 設定を管理します。

オプション	説明
接続の有効化	現在有効になっている接続 (SMTP および POP3) を表示します。 接続を有効または無効にするには a. 接続項目の横にあるチェックボックスをオンまたはオフにします。 b. [保存] をクリックします。
コンポーネント	InterScan MSS がネットワークを保護するために使用するウイルス対策、スパイウェア対策、およびスパムメール対策のコンポーネントのバージョン番号を表示します。 コンポーネントを手動でアップデートするには a. アップデートするコンポーネントのチェックボックスをオンにします。 b. [アップデート] をクリックします。 コンポーネントの以前のバージョンにロールバックするには

オプション	説明
	a. ロールバックするコンポーネントのチェックボックスをオンにします。 b. [ロールバック] をクリックします。 ページを表示更新するには ・ [表示更新] をクリックしてアップデート元に接続すると、[利用可能なバージョン] 列にコンポーネントの最新バージョンが表示されます。
管理下のサービス	この InterScan MSS 管理データベースに登録されている他の InterScan MSS サービスを表示します。 管理下のサービスを開始または停止するには ・ 変更するサービスの [開始] または [停止] をクリックします。 管理下のサービスを登録解除するには ・ 管理下のサービスが非アクティブの場合 (InterScan MSS サーバから切断されている)、そのサービスの [接続] 列の横に [削除] ボタンが表示されます。管理下のサービスをこの InterScan MSS サーバから削除するには、[削除] をクリックします。  注意 管理下のサービスが切断される理由としては、次のことが考えられます。 ・ 検索サービスが削除されている。 ・ InterScan MSS マネージャサービスが停止している。 ・ 検索サーバが停止している。

第 22 章

ダッシュボードとウィジェット

この章では、InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) でダッシュボードとウィジェットを使用する際の一般的な手順を説明します。

この章の内容は次のとおりです。

- ・ [346 ページの「ダッシュボードを使用する」](#)
- ・ [346 ページの「タブについて」](#)
- ・ [351 ページの「ウィジェットについて」](#)

ダッシュボードを使用する

InterScan MSS ダッシュボードを使用すると、InterScan MSS ネットワークの情報を一目で把握できます。ダッシュボードは、次の 2 つのコンポーネントで構成されています。

- ・ タブ: 管理者はこれを使用して、1 つ以上のウィジェットを含む画面を作成できます。
- ・ ウィジェット: さまざまなセキュリティ関連のイベントについての特定の情報を提供します。

ユーザアカウントとダッシュボード

各ユーザアカウントには、独自のダッシュボードが表示されます。ユーザが InterScan MSS に初めてログオンすると、初期設定のタブと、それらのタブに含まれるウィジェットが、ダッシュボードに表示されます。

各ユーザアカウントで、そのアカウントの特定の必要に応じて、ダッシュボード、タブ、およびウィジェットをカスタマイズできます。あるユーザアカウントでダッシュボード、タブ、またはウィジェットをカスタマイズしても、別のユーザアカウントのダッシュボード、タブ、またはウィジェットには影響ありません。各ユーザアカウントのダッシュボード、タブ、およびウィジェットは、その他のアカウントのものとは独立しています。

タブについて

InterScan MSS ダッシュボードでは、タブを使用して管理者に柔軟性を提供します。タブはウィジェットのためのコンテナとして機能し、それによって管理者は独自のカスタマイズされたダッシュボードを作成できます。ダッシュボードでは、ユーザアカウントごとに最大 30 個のタブをサポートします。

ウィジェットをタブ上のさまざまな場所にドラッグ&ドロップして、タブ上のウィジェットを移動させることができます。タブのレイアウトにより、どこにウィジェットを移動できるかが決まります。

**注意**

あるユーザアカウントでダッシュボード、タブ、またはウィジェットをカスタマイズしても、別のユーザアカウントのダッシュボード、タブ、またはウィジェットには影響ありません。各ユーザアカウントのダッシュボード、タブ、およびウィジェットは、その他のアカウントのものとは独立しています。

初期設定のタブ

初期設定のタブは、以前のバージョンの InterScan MSS の [リアルタイム統計] 画面に代わるものです。以前のバージョンの InterScan MSS [リアルタイム統計] 画面で確認できたすべての情報は、初期設定のタブ上のウィジェットで表示できます。ダッシュボードには次の初期設定のタブが備わっています。

- ・ システムの概要
- ・ メッセージトラフィック
- ・ 送信者フィルタ
- ・ クラウドプレフィルタ

**注意**

初期設定のタブを削除すると、そのタブを削除したユーザアカウントの表示からタブが削除されます。削除したタブを復元する方法はありません。初期設定のタブを削除しても、その他のユーザアカウントのダッシュボードには影響はありません。

[システムの概要] タブ

[システムの概要] タブは、[リアルタイム統計] 画面の一部を置き換えます。[システムの概要] タブには、システムリソースの使用状況とキューのステータスの情報を表示するウィジェットが含まれます。

表 22-1. [システムの概要] タブのウィジェット

ウィジェット	説明
システムの使用状況	ネットワーク上の InterScan MSS が使用するシステムリソースが表示されます。
メールキュー	受信したばかりのメッセージ、配信可能なメッセージ、配信不能により遅延されたメッセージ、および後から手動で配信するために保留されているメッセージの数が表示されます。
InterScan MSS 隔離	隔離されているメッセージ数と、各隔離領域の空きディスク容量が表示されます。
InterScan MSS アーカイブ	アーカイブされているメッセージ数と、各アーカイブ領域の空きディスク容量が表示されます。

[メッセージトラフィック] タブ

[メッセージトラフィック] タブは、[リアルタイム統計] 画面の一部を置き換えます。[メッセージトラフィック] タブには、InterScan MSS により検出されたメッセージトラフィックの統計と違反を表示するウィジェットが含まれます。

表 22-2. [メッセージトラフィック] タブのウィジェット

ウィジェット	説明
InterScan MSS の検索パフォーマンス	一定期間に各タイプのフィルタを実行したメッセージの数を表示します。
検索条件	各タイプのフィルタを実行したメッセージの数および検出総数に対するこれらのメッセージの比率を表示します。
処理されたメッセージ	受信および送信メールトラフィックの数を表示します。

[送信者フィルタ] タブ

[送信者フィルタ] タブには、送信者フィルタコンポーネントによってブロックされたすべての不正なメッセージとすべてのスパムメールを表示するウィジェットが含まれます。

表 22-3. [送信者フィルタ] タブのウィジェット

ウィジェット	説明
送信者フィルタパフォーマンス	特定の送信者フィルタコンポーネントによってブロックされた不正なメッセージとスパムメールの数、およびブロックされた時間が表示されます。
送信者フィルタタイプ	特定の送信者フィルタコンポーネントによってブロックされた不正なメッセージとスパムメールの数が表示されます。

[クラウドプレフィルタ] タブ

[クラウドプレフィルタ] タブには、クラウドプレフィルタのメッセージトラフィックと脅威の検出を表示するウィジェットが含まれます。

表 22-4. [クラウドプレフィルタ] タブのウィジェット

ウィジェット	説明
クラウドプレフィルタのトラフィックの概要	クラウドプレフィルタによって処理されたメッセージの数を表示します。
クラウドプレフィルタの違反の種類	クラウドプレフィルタのメッセージ違反の数と種類を示します。

タブを追加する

タブをダッシュボードに追加して、InterScan MSS ネットワークのニーズに応じてカスタマイズされた情報マトリックスを実現できます。

手順

1. [ダッシュボード] 画面に移動します。

2. [新規タブ(+)] をクリックします。
[新規タブ] 画面が表示されます。
3. [タイトル] フィールドにタブの機能がわかるようなタイトルを指定します。
4. タブのレイアウトを選択します。

**注意**

1 つのタブに追加できるウィジェットの数は、タブのレイアウトによって決まります。タブに最大数のウィジェットがすでに含まれている場合、新しいウィジェットを追加するには、タブからウィジェットを 1 つ削除するか、そのウィジェット用に新しいタブを作成する必要があります。

5. [保存] をクリックします。
空のタブがダッシュボードに表示されます。
6. [ウィジェットの追加] をクリックして、タブにウィジェットを追加します。

タブを設定する

[タブ設定] 画面を使用して、タブの初期設定の名前を変更できます。

手順

1. [ダッシュボード] 画面に移動します。
2. [タブ設定] をクリックします。
[タブ設定] 画面が表示されます。
3. [タイトル] フィールドにタブの機能がわかるようなタイトルを指定します。
4. [保存] をクリックします。

ウィジェットについて

ウィジェットとは、ダッシュボードのコアとなるコンポーネントです。タブはレイアウトを提供するのに対し、ウィジェットはダッシュボードの実際のデータを提供します。



注意

あるユーザアカウントでダッシュボード、タブ、またはウィジェットをカスタマイズしても、別のユーザアカウントのダッシュボード、タブ、またはウィジェットには影響ありません。各ユーザアカウントのダッシュボード、タブ、およびウィジェットは、その他のアカウントのものとは独立しています。

一部のウィジェットでは、それぞれの検索条件に一致したメッセージの合計数は重複してカウントされます。たとえば、1件のメッセージが2つ以上の検索条件に一致した場合（例: スпамメールと添付ファイル）、このメッセージは2回カウントされます。つまり、スパムメールの合計数と添付ファイルの合計数にそれぞれ1回ずつカウントされます。

ウィジェットを使用する

各ウィジェットは、対象を設定した、セキュリティ関連の情報を提供します。ウィジェットには、次のいずれかの方法でこの情報を表示できます。

- ・ 棒グラフ
- ・ 円グラフ
- ・ 表

ウィジェットのヘルプアイコンをクリックして、次の種類の情報を表示できます。

表 22-5. ウィジェットのヘルプ

ウィジェットのトピック	説明
概要	ウィジェットの説明とウィジェットの使用方法を提供します。

ウィジェットのトピック	説明
ウィジェットデータ	ウィジェットの表に表示されるデータについての詳細情報です。
設定	ウィジェット上ですぐに表示可能な設定の説明です。
編集	編集アイコンをクリックして変更する必要がある設定についての説明です。

ウィジェットを設定する

ウィジェットを「設定する」とは、ウィジェット上ですぐに表示される、ウィジェットの設定を変更することを意味します。次の表に、ウィジェット設定管理者が変更できるいくつかの例を示します。

表 22-6. ウィジェットを設定する

設定	説明
範囲	表示されるデータの時間範囲を変更します。 ・ 1 時間以内 ・ 6 時間以内 ・ 12 時間以内 ・ 24 時間以内
データの集約	すべての InterScan MSS または単一の InterScan MSS を指定することによりデータの集約を変更します。
表示	データの表示方法を変更します。 ・ 棒グラフ ・ 円グラフ ・ 表

ウィジェットを編集する

ウィジェットを「編集する」とは、ウィジェット上ですぐに表示されない、ウィジェットの設定を変更することを意味します。編集アイコンをクリックして、これらの設定にアクセスします。次のような例があります。

表 22-7. ウィジェットを編集する

設定	説明
タイトル	ウィジェットに表示される名前を変更します。
その他	一部のウィジェットは、1つのウィジェットで表示するデータの量 (エントリの範囲) または表示するデータの種類 (セキュリティの脅威の種類やコンポーネントの種類と製品の種類) を変更するための設定を提供します

手順

1. [ダッシュボード] 画面に移動します。
2. ウィジェットの [編集] アイコンをクリックします。[編集] 画面が表示されます。
3. [タイトル] にウィジェットの機能がわかるようなタイトルを指定します。
4. [OK] をクリックします。
5. ウィジェットで利用可能なその他の設定についても値を指定します。



注意

[その他] の設定の詳細については、その特定のウィジェットのヘルプを参照してください。

6. [保存] をクリックします。

ウィジェットが新しい設定を適用して再読み込みされます。

ウィジェットを追加する

1つのタブに追加できるウィジェットの数は、タブのレイアウトによって決まります。タブに最大数のウィジェットがすでに含まれている場合、新しいウィジェットを追加するには、タブからウィジェットを1つ削除するか、そのウィジェット用に新しいタブを作成する必要があります。

手順

1. ダッシュボード上の任意のタブに移動します。
2. [ウィジェットの追加] をクリックします。
[ウィジェットの追加] 画面が表示されます。
3. 次のいずれかをクリックして、表示されるウィジェットをフィルタします。

カテゴリ	説明
すべてのウィジェット	利用可能なすべてのウィジェットが表示されます。
システム	システムウィジェットのみが表示されます。
メッセージトラフィック	メッセージトラフィックウィジェットのみが表示されます。
送信者フィルタ	送信者フィルタウィジェットのみが表示されます。
クラウドプレフィルタ	クラウドプレフィルタウィジェットのみが表示されます。

4. タブに追加する1つ以上のウィジェットを選択します。
 5. [追加] をクリックします。
-

第 23 章

レポート

この章では、1 回限りのレポートと予約レポートの作成方法について説明します。

この章の内容は次のとおりです。

- ・ 356 ページの「レポートを生成する」
- ・ 359 ページの「1 回限りのレポートを管理する」
- ・ 362 ページの「予約レポート」

レポートを生成する

必要に応じて、1 回限りのレポートの作成や指定した間隔で実行する予約レポートを選択できます。InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) にはレポートごとにコンテンツを指定して、結果を HTML または CSV 形式で表示または保存したり、レポートを特定の受信者にメールで送信したりする柔軟性に富んだ機能があります。

レポート内容の種類

レポートに記載する内容の種類を次の中から選択できます。

表 23-1. クラウドプレフィルタのレポート

レポート内容	説明
トラフィックと脅威の概要	受信メッセージの合計件数と合計サイズを表示します。また、特定の検索条件に一致したメッセージ数也表示します。

表 23-2. 概要レポート

レポート内容	説明
ポリシーとトラフィックの概要	受信メッセージと送信メッセージの合計件数と合計サイズ、特定の検索条件に一致したメッセージ数、および隔離イベントの概要を表示します。
ウイルスと不正プログラムコードの概要	処理ごとにウイルスメッセージ件数の概要を示します。
スパムメールの概要	スパムメール検索エンジン、メールレピュテーション、IP プロファイラおよび処理ごとにカウントされたスパムメール合計件数の概要を表示します。

レポート内容	説明
送信者 IP アドレスのブロックの概要	「IP プロファイラの概要」および「メールレピュテーションによる IP ブロックの概要」が含まれます。前者は、IP プロファイラに到達し、他の送信者フィルタルールによってブロックされた送信者接続合計数の概要を表示します。後者は、メールレピュテーションに到達し、メールレピュテーションによってブロックされた送信者接続の合計数を表示します。
仮想アナライザの分析の概要	リスクレベルによって分析済みの高度な脅威の合計件数を表示します。  注意 仮想アナライザは、次の場合にリスクレベルを返さないことがあります。 ・ サーバまたは接続にエラーが発生している ・ 添付ファイルのタイプがサポートされていない ・ 分析が完了しなかった
Time-of-Click プロテクションの概要	クリックの合計数、許可されたクリック数、ブロックされたクリック数、ユーザが警告を受けて中止したクリック数、およびユーザが警告を受けたもののアクセスを続行したクリック数を表示します。

表 23-3. トップ 10 レポート

レポート内容	説明
トラフィックのメールアドレス [トップ 10]	送信および受信メッセージ数でトップ 10 のメールアドレスを表示します。
感染ウイルス名 [トップ 10]	ウイルス検出数で、トップ 10 の感染ウイルス名を表示します。

レポート内容	説明
DHA 攻撃に対してブロックされた IP アドレス [トップ 10]	DHA 攻撃によるブロック数で、トップ 10 の IP アドレスを表示します。
バウンスメール攻撃によるブロック数で、トップ 10 の IP アドレスを表示します。	バウンスメール攻撃によるブロック数で、トップ 10 の IP アドレスを表示します。
ウイルス受信者と送信者 [トップ 10]	受信および送信ウイルスメッセージ合計件数で、トップ 10 のウイルス受信者および送信者を表示します。
最も頻繁に違反したルール [トップ 10]	ルールに一致したメール件数で、トップ 10 のルール名を表示します。
スパムメール受信者 [トップ 10]	受信スパムメールの合計件数で、トップ 10 のスパムメール受信者アドレスを表示します。
メールレピュテーションでブロックされた IP アドレス [トップ 10]	メールレピュテーションによって切断された接続数で、トップ 10 のブロックされた IP アドレスを表示します。
スパムメール送信元としてブロックされた IP アドレス [トップ 10]	スパムメール送信元としてブロックされた数で、トップ 10 の IP アドレスを表示します。
ウイルスまたは不正コードの送信元としてブロックされた IP アドレス [トップ 10]	ウイルスの送信元としてブロックされた数で、トップ 10 の IP アドレスを表示します。
不審な URL を使用したメッセージの送信者 [トップ 10]	不審 URL が含まれた受信メッセージの合計数で、トップ 10 の送信者アドレスを表示します。
Trend Micro Email Encryption の受信者と送信者 [トップ 10]	メール暗号化違反で、トップ 10 の受信者と送信者を表示します。
コンプライアンス受信者と送信者 [トップ 10]	規制コンプライアンス違反で、トップ 10 の受信者と送信者を表示します。
C&C メールを受信者と送信者 [トップ 10]	SMTP セッションで使用されたアドレスに基づいて、C&C メールのトップ 10 の受信者と送信者を表示します。

レポート内容	説明
マーケティンググレーメールの受信者と送信者 [トップ 10]	マーケティングニュースレターメールメッセージのトップ 10 の受信者と送信者を表示します。
ソーシャルネットワークグレーメールの受信者と送信者 [トップ 10]	ソーシャルネットワーク更新メールメッセージのトップ 10 の受信者と送信者を表示します。

**注意**

送信者「unknown@unknown」が表示されるレポートレコードがある場合、これは配達不能メッセージのバウンスメールなので無視してください。

1 回限りのレポートを管理する

1 回限りのレポートを生成すると、InterScan MSS の保護の概要を一目で把握できます。将来参照できるように、InterScan MSS はこの画面上の 1 回限りのレポートをすべて保持します。

InterScan MSS で、日次、週次、または月次のレポートの自動生成を有効にすることもできます。

以前に生成した 1 回限りのレポートのリストを表示するには、[レポート] > [1 回限りのレポート] の順に選択します。

手順

- ・ 表示内容を変更するには、次のいずれかの操作を実行します。
 - ・ 表を並び替えるには、下線付きの列見出しのいずれかをクリックします。
 - ・ リストに表示される項目が多すぎる場合は、リストの上部にある矢印ボタンをクリックして次のページに移動するか、表示するページの番号をドロップダウンボックスから選択します。
 - ・ リストで同時に表示される項目の数を変更するには、表の下部にあるドロップダウンボックスから新しい表示値を選択します。

- ・ レポートを生成するには、[追加] をクリックしてレポートの詳細を指定します。

レポートの生成中は、[出力] 列に「[処理中]」 と表示されます。

- ・ レポートを表示するには、[出力] で次の形式のいずれかをクリックします。
 - ・ HTML: 別のブラウザウィンドウでレポートを開きます。
 - ・ CSV: スプレッドシートアプリケーションで開くことができるカンマ区切り値ファイルとしてレポートを保存します。
- ・ レポートを削除するには、そのレポートの横にあるチェックボックスをオンにしてから [削除] をクリックします。
- ・ レポートをメールで送信するには、そのレポートの横にあるチェックボックスをオンにしてから [メール] をクリックします。



ERS レポートおよび IP プロファイラレポート内容は、これらの製品をアクティベートするまで出力できません。ERS および IP プロファイラをアクティベートする方法の詳細については、[476 ページの「製品ライセンスを管理する」](#)を参照してください。

1 回限りのレポートを追加する

必要に応じて 1 回限りのレポートを作成すると、ネットワークのトラフィックを監視するのに役立ちます。

手順

1. [レポート] > [1 回限りのレポート] の順に選択します。

1回限りのレポート



追加 削除		
☐ レポート名	日付▼	出力
10件/ページ▼		

2. [追加] をクリックします。

[1 回限りのレポートの追加] 画面が表示されます。利用可能なレポートのリストについては、[356 ページの「レポートを生成する」](#)を参照してください。

3. レポートを設定して、[保存] をクリックします。

オプション	説明
名前	内容を示す名前を入力します。
日付	レポートの対象となる期間を選択します。
レポート内容	レポートに記載する内容を選択します。
通知設定	レポートの通知設定を有効にする場合に選択します。
送信者	レポート送信者のメールアドレスを指定します。
受信者	レポートの受信者を指定します。

レポートの作成に数分かかります。レポートテーブルに、[実行中] というメッセージが表示されます。

1回限りのレポート



追加 削除 メール			1-1 / 1 ◀ ▶ ページ 1 ▶▶
☐ レポート名	日付▼	出力	
☐ トラフィックとポリシーの概要	2015/12/22 11:31:00	実行中	
15件/ページ▼			

レポートが生成されると、レポートテーブルに [HTML] および [CSV] のハイパーリンクが表示されます。

1回限りのレポート



追加 削除 メール 1-3 / 3 ページ 1		
☐ レポート名	日付	出力
☐ トラフィックと脅威の概要	2015/12/22 11:31:50	HTML CSV
☐ ウイルスと不正プログラムコードの概要	2015/12/22 11:31:21	HTML CSV
☐ トラフィックとポリシーの概要	2015/12/22 11:30:17	HTML CSV
		15件/ページ

4. [出力] の下で、レポートデータをエクスポートする出力形式を選択します。

レポートの作成は1回に5分程度かかります。レポート作成の所要時間は、レポートデータの収集や必要な計算を行ったうえにさらに5分程度かかる場合があります。

予約レポート

予約レポートを使用して、レポートの生成を自動化します。InterScan MSS には、日次、週次、および月次のレポートが用意されています。

予約レポートを設定する

予約レポートは、設定したスケジュールに従って自動的に作成されます。

手順

1. [レポート] > [設定] の順に選択します。

[予約レポートの設定] 画面が表示されます。

予約レポートの設定



レポートの種類	ステータス	予約	設定	保存する数
日次レポート	×	2:00	設定	60
週次レポート	×	日曜日 開始時刻 2:00	設定	20
月次レポート	×	1日目 開始時刻 2:00	設定	5

[保存](#) [キャンセル](#)

2. 次のいずれかのレポートの種類から [設定] リンクをクリックします。

- ・ 日次レポート
- ・ 週次レポート
- ・ 月次レポート

レポート設定画面が表示されます (例: [日次 (週次・月次) レポート設定])。

日次レポート設定



予約レポートの設定 > 日次レポート設定

☐ 日次レポートの作成

開始時刻: 2
時 (hh)

☐ レポート内容

クラウドプレフィルタのレポート

☐ トラフィックと脅威の概要

InterScan Messaging Security Virtual Applianceの概要レポート

☐ トラフィックとポリシーの概要

☐ ウィルスと不正プログラムコードの概要

☐ スпамメールの概要

☐ 送信者IPアドレスのブロックの概要

☐ Deep Discovery Advisorの分析の概要

暗号化レポート

☐ 復号化と暗号化の概要

InterScan Messaging Security Virtual Applianceのトップ10レポート

☐ トラフィックのメールアドレス [トップ10]

☐ 感染ウィルス名 [トップ10]

☐ DHA攻撃に対してブロックされたIPアドレス [トップ10]

☐ バウンスメール攻撃に対してブロックされたIPアドレス [トップ10]

☐ ウィルス受信者と送信者 [トップ10]

☐ 最も頻繁に違反したルール [トップ10]

☐ スпамメール受信者 [トップ10]

☐ メールレピュテーションでブロックされたIPアドレス [トップ10]

☐ スпамメール送信元としてブロックされたIPアドレス [トップ10]

☐ ウィルスまたは不正コードの送信元としてブロックされたIPアドレス [トップ10]

☐ 不審なURLを使用したメッセージの送信者 [トップ10]

☐ Trend Micro Email Encryptionの受信者と送信者 [トップ10]

☐ コンプライアンス受信者と送信者 [トップ10]

☐ O&Oメールの受信者と送信者 [トップ10]

3. レポートを設定します。

レポートのオプションについては、356 ページの「レポートを生成する」を参照してください。

**注意**

月次レポートを設定する際、レポートの作成日に 29 日、30 日、または 31 日を選択した場合、InterScan MSS では、月の日数に応じて月末にレポートが作成されます。たとえば、レポートの作成日を 31 日と選択した場合、InterScan MSS では、2 月には 28 日 (または 29 日)、4 月、6 月、9 月および 11 月には 30 日にレポートが作成されます。

4. [保存] をクリックします。
レポートのステータスが変更されます。
5. 保存する数をレポートの種類ごとに指定します。
6. [保存] をクリックします。
7. [レポート] > [予約レポート] の順に選択します。
[保存された予約レポート] 画面が表示されます。

**注意**

レポートはまだ作成されていません。

保存された予約レポート ?

毎日 毎週 毎月	
削除 メール 1-1 / 1 4 ページ 1	
☐ 保存されたレポート	出力
☐ 2015/12/21	HTML CSV 15件/ページ

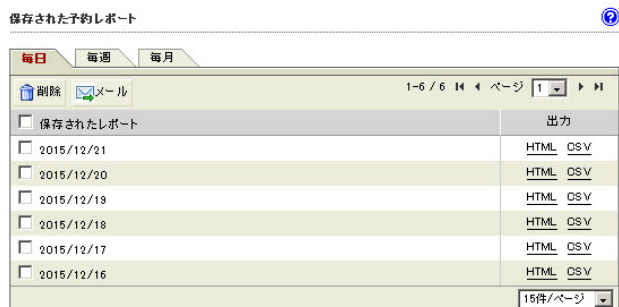
8. レポートの作成後、利用可能なレポートのオプションについては[365 ページの「予約レポートにアクセスする」](#)を参照してください。

予約レポートにアクセスする

手順

1. メニューから [レポート] > [予約レポート] の順に選択します。

[保存された予約レポート] 画面が表示されます。



2. 作成頻度に対応するタブを選択します。
 - ・ 毎日
 - ・ 毎週
 - ・ 毎月
3. 利用可能なレポートのオプションについては、[366 ページの「予約レポートを使用する」](#)を参照してください。

予約レポートを使用する

[レポート] > [予約レポート] の順に選択し、[日次]、[週次]、または [月次] タブのいずれかを開きます。

手順

- ・ レポートを表示するには、[出力] の下で次の形式のいずれかをクリックします。
 - ・ HTML:別のブラウザウィンドウでレポートを開きます。
 - ・ CSV:スプレッドシートアプリケーションで開くことができるカンマ区切り値ファイルとしてレポートを保存します。
- ・ 表示内容を変更するには、次のいずれかの操作を実行します。

- ・ リストに表示される項目が多すぎる場合は、リストの上部にある矢印ボタンをクリックして次のページに移動します。
 - ・ リストで同時に表示される項目の数を変更するには、表の下部にあるドロップダウンボックスから新しい表示値を選択します。
 - ・ レポートを削除するには、そのレポートの横にあるチェックボックスをオンにしてから [削除] をクリックします。
 - ・ レポートをメールで送信するには、そのレポートの横にあるチェックボックスをオンにしてから [メール] をクリックします。
-

第 24 章

ログ

この章では、ログを設定およびクエリする一般的な手順について説明します。

この章の内容は次のとおりです。

- ・ [370 ページの「ログについて」](#)
- ・ [370 ページの「ログを設定する」](#)
- ・ [372 ページの「ログのクエリを実行する」](#)

ログについて

ログによって、InterScan MSS 内のさまざまな種類のイベントや情報のフローを監視できます。また、トラブルシューティングの際の重要な情報源にもなります。

ログを有効にして情報を活用するには

- ・ 手順 1: [370 ページの「ログを設定する」](#)
- ・ 手順 2: [372 ページの「ログのクエリを実行する」](#)

ログを設定する

InterScan MSS のログに記録される内容の詳細レベルと、ログが保存される期間を設定できます。また、検索サービスがローカルログを InterScan MSS 管理データベースに記録する頻度をアップデート期間として設定することもできます。

手順

1. [ログ] > [設定] の順に選択します。

[ログの設定] 画面が表示されます。

ログの設定



データベースへのログのレポート	
データベースのアップデート間隔:	01 分
クエリ用にログを保存する日数:	30 日
ログファイル	
アプリケーションログの詳細レベル:	診断 ⓘ
☒ ログファイルを保存する日数:	90 日
☒ サービス別ログファイルの最大サイズ:	2000 MB
保存 キャンセル	

2. [データベースへのログのレポート] を設定します。

- ・ データベースのアップデート間隔: InterScan MSS は、ここで設定した間隔で定期的にログをアップデートします。間隔には、1~60 の数字を選択します。60 を選択すると、InterScan MSS は 1 時間ごとにログをアップデートします。
- ・ クエリ用にログを保存する日数: InterScan MSS 管理データベースにレポートログを保存する日数を 1~60 の数字で指定します。

3. [ログファイル] で、次の項目を設定します。

- ・ アプリケーションログの詳細レベル: ログの詳細レベルを設定します。次のいずれかを選択します。
 - ・ 標準: ログの詳細度は標準です。このレベルでは、管理者が毎日の監視と管理作業を実行するのに必要とする基本的な情報が提供されます。
 - ・ 詳細: ログの詳細度は高くなります。すべての InterScan MSS プロセスで、ログに詳細情報が書き込まれます。このレベルのログには、POP3 セッション情報、一致するポリシー、実行されたフィルタ、および実行された処理が含まれます。
 - ・ 診断: 各イベントまたは各処理に対する総合的な情報です。[診断] レベルのログには、[詳細] レベルのすべての情報に加えて、SMTP ルーティング情報、および適用するポリシーを決定したルート一致情報が含まれます。
 - ・ デバッグ: 最も詳細なレベルのログが出力されます。デバッグログは、トラブルシューティングの場合にのみ使用することをお勧めします。



注意

診断ログまたはデバッグログは、InterScan MSS リソースを多く消費してシステムパフォーマンスを低下させる可能性があります。

- ・ ログファイルを保存する日数: チェックボックスをオンにし、InterScan MSS でローカルログファイルが保存される日数を 1~150 の数字で指定します。InterScan MSS のログファイルが消去されないようにするには、このチェックボックスをオフにします。

- ・ サービス別ログファイルの最大サイズ: チェックボックスをオンにし、プロセスやサービスのタイプごとにローカルログファイルのサイズ (MB) を 100~99999 の数字で指定します。サイズ制限をすべて解除するには、チェックボックスをオフにします。

**注意**

InterScan MSS のログファイルは、初期設定で `/opt/trend/imss/log` フォルダに格納されます。

各種のイベントの日次ログファイルは午前 0 時に作成され、「<日付>.<カウント>」の接尾辞が付けられます。1 日に 2 つ以上のログファイルがある場合は、<カウント>接尾辞の数値が増えます。

ログファイルのサイズが各サービスのログファイルの最大サイズを超える場合、InterScan MSS では最も古いファイルから削除されます。

4. [保存] をクリックします。

ログのクエリを実行する

次の種類のイベントまたは情報のクエリを実行できます。

メッセージ追跡

送信者、受信者、メッセージサイズ、添付ファイル、および InterScan MSS によって実行された最終的な処理など、メッセージの詳細を記録します。起動されたポリシールールの名前と種類もクエリの結果に示されます。

システムイベント

検索エンジンやパターンファイルのアップデート、検索サービスのステータス変更、管理者による操作、および InterScan MSS で発生したエラーなど、システムイベントの詳細を記録します。

ポリシーイベント

起動されたポリシールールの詳細、実行された処理、およびメッセージの詳細を記録します。

URL クリックの追跡

メッセージの送信者、受信者、URL、メッセージ ID、および URL がブロック、警告、またはクリックスルーであるかどうかなど、URL クリックの詳細を記録します。

隔離イベント

たとえば、すべての隔離イベントにおける解除イベントの割合など、隔離イベントの詳細を示します。

MTA イベント

セントラルコントローラがインストールされているローカルコンピュータ上の Postfix の接続の詳細を記録します。

送信者フィルタ

InterScan MSS で、クエリ対象 IP アドレスまたは送信者アドレスからのメッセージのブロックを開始および停止した時間を記録します。

InterScan MSS では、大部分のログのクエリに対して、ワイルドカード (*) と完全一致をサポートしています (たとえば、名前に A または B を含むメール受信者を表示するには、受信者を「*A*;*B*」に設定します)。初期設定では、完全一致が使用されます。検索条件を空欄にしておくと、すべてのログが表示されます。複数条件のアイテムがある場合は、セミコロン (;) を使用して、受信者と添付ファイルのエントリを区切ります。

ログクエリの動作

InterScan MSS にクラウドプレフィルタが組み込まれたことによって、ユーザがログに対するクエリを実行する方法が変更されています。

メッセージ追跡機能の強化

InterScan MSS では、メッセージ追跡ログが次のように分割されています。

- ・ InterScan MSS のデータのみ: このメッセージ追跡ログには、InterScan MSS からのデータのみが記載されます。

使用可能なクエリ条件は [件名]、[メッセージ ID]、[送信者]、[受信者]、および [添付ファイル] で、すべてのクエリ条件を空白にできます。

- ・ クラウドプレフィルタと IMSS のデータ: このメッセージ追跡ログには、クラウドプレフィルタと InterScan MSS からデータが記載されます。

使用可能なクエリ条件は [送信者] と [受信者] で、[受信者] は必須です。

InterScan MSS によって、メッセージ追跡ログの隔離メッセージ、アーカイブメッセージおよび保留メッセージへのハイパーリンクが組み込まれます。これによって、これらのメッセージの詳細情報を確認できます。

クエリの動作

InterScan MSS では、ログクエリは次のように動作します。

表 24-1. 一般的なクエリ情報

クエリ	INTERSCAN MSS のみ	INTERSCAN MSS + クラウドプレフィルタ
a@a.com	完全一致のみが返されます。 結果: a@a.com	複数の受信者のものを含み、「a@a.com」の異形のすべてに送信されたすべてのメッセージが表示されます。 結果: ・ za@a.com ・ a@a.com.us ・ a@a.com、b@a.com ・ b@a.com、a@a.com ・ b@a.com、a@a.com、c@a.com
[件名] フィールドに*を指定 その他のすべてのクエリ条件が空白の場合	すべてのメッセージが返されます。	約 10,000 の検索結果が返されます。

クエリ	INTERSCAN MSS のみ	INTERSCAN MSS + クラウドプレフィルタ
[メッセージ ID] フィールドに*を指定 その他のすべてのクエリ条件が空白の場合	すべてのメッセージが返されます。	約 10,000 の検索結果が返されます。

表 24-2. 「送信者」のクエリ情報

クエリ	INTERSCAN MSS のみ	INTERSCAN MSS + クラウドプレフィルタ
5!#?	InterScan MSS で有効な [送信者] の値。ただし結果は返されません。	サポートされません。 ユーザは適切な形式でメールアドレス、またはメールアドレスの一部分を指定する必要があります。
test@example.com	InterScan MSS で有効な [送信者] の値。 戻り値: test@example.com で終わるすべての異形	サポートされません。[送信者] フィールドではワイルドカード文字「」がサポートされていません。
test@example.com	InterScan MSS で有効な [送信者] の値。 戻り値: test@example.com から送信されたメッセージのみ	InterScan MSS で有効な [送信者] の値。 戻り値: test@example.com から送信されたメッセージのみ

表 24-3. 「受信者」のクエリ情報

クエリ	INTERSCAN MSS のみ	INTERSCAN MSS + クラウドプレフィルタ
test@example.com	InterScan MSS で有効な [受信者] の値。 戻り値: test@example.com に送信されたメッセージのみ	InterScan MSS で有効な [受信者] の値。 戻り値: test@example.com のすべての異形に送信された約 10,000 の結果 (InterScan MSS のみのデータで「*test@example.com*」を使用した場合と同じ)
test@example.com	InterScan MSS で有効な [受信者] の値。 戻り値: test@example.com で終わるすべての異形	サポートされません。[受信者] フィールドではワイルドカード文字「」がサポートされていません。
test@example.com*	InterScan MSS で有効な [受信者] の値。 戻り値: 「test@example.com」で始まるすべての異形	サポートされません。[受信者] フィールドではワイルドカード文字「*」がサポートされていません。
test@example.com	InterScan MSS で有効な [受信者] の値。 戻り値: test@example.com のすべての異形	サポートされません。[受信者] フィールドではワイルドカード文字「*」がサポートされていません。  ヒント この代わりに test@example.com を使用します。

クエリ	INTERSCAN MSS のみ	INTERSCAN MSS + クラウドプレフィルタ
test@example.com; test2@example.com	InterScan MSS で有効な [受信者] の値。 結果: test@example.com と test2@example.com の検索 結果の結合。	サポートされません。  ヒント この代わりに 「test@example.com」 または 「test2@example.com」 を使用します。
%^\$&^	InterScan MSS で有効な [受信者] の値。ただし結果 は返されません。	サポートされません。 ユーザは適切な形式でメール アドレス、またはメール アドレスの一部分を指定する 必要があります。

**注意**

返されたクエリに含まれるデータ <サーバ名>[127.0.0.1] は、初期設定の DNS サーバを示します。

メッセージ追跡ログのクエリを実行する

手順

1. [ログ] > [クエリ] の順に選択します。

[ログクエリ] 画面が表示されます。

ログクエリ

基準	
種類	選択 選択 メッセージ追跡 システムイベント ポリシーイベント 隔離イベント URLクリックの追跡 MTAイベント 送信者フィルタ

2. [種類] の横で [メッセージ追跡] を選択します。
メッセージのイベントログの検索画面が表示されます。
3. [日付] の横で、日付と時間の範囲を選択します。
4. 次のいずれかの追加情報を指定してください。
 - ・ 件名
 - ・ メッセージ ID
 - ・ 送信者
 - ・ 受信者
 - ・ 添付ファイル



注意

いずれかのフィールドで部分検索をする場合はアスタリスク (*) ワイルドカードを使用します。

5. [ログ表示] をクリックします。
日時、送信者、受信者、件名、および最終処理が各イベントに対して表示されます。
6. [日時] リンクをクリックして、次の情報を表示します。

- ・ 日時
- ・ 送信者
- ・ 受信者
- ・ 件名
- ・ 元のサイズ
- ・ 添付ファイル
- ・ メッセージ ID
- ・ 内部 ID
- ・ 検索サービス
- ・ 最終処理
- ・ 処理の詳細

7. 次のいずれかの処理を実行してください。

- ・ リストで同時に表示される項目の数を変更するには、表の上部にあるドロップダウンボックスから新しい表示値を選択します。
- ・ 検索結果を印刷するには、[現在のページを印刷] をクリックします。
- ・ 検索結果をカンマ区切り値のファイルに保存するには、[CSV 形式にエクスポート] をクリックします。

システムイベントログのクエリを実行する

手順

1. [ログ] > [クエリ] の順に選択します。
2. [種類] の横の [システムイベント] を選択します。

システムイベントログの検索画面が表示されます。

3. [種類] の横にある 2 番目のドロップダウンボックスで、次のいずれかを選択します。
 - ・ すべてのイベント: すべてのシステムイベントの日時と説明が表示されます。
 - ・ アップデート: アップデートサーバから InterScan MSS 管理データベースへの検索エンジンとパターンファイルのアップデートが実行された日時が表示されます。
 - ・ サービスのステータス: 検索サービスが開始または停止された日時と説明が表示されます。
 - ・ 監査ログ: 指定された管理者アカウントにより実行された操作の日時と説明が表示されます。

**注意**

システムイベントのログカテゴリがさらに使いやすくなり、InterScan MSS 管理コンソールでは [管理者アクティビティ] が [監査ログ] になりました。監査ログでは、管理者のさまざまな操作を記録し、これにより指定された管理者アカウントのアクティビティのクエリを実行できます。

- ・ エラー: InterScan MSS で発生したすべてのエラーの日時と説明が表示されます。
4. [種類] の横にある 3 番目のドロップダウンボックスで、表示するサーバを選択します。
 5. [日付] の横で、日付と時間の範囲を選択します。
 6. [監査ログ] を選択する場合は、設定変更を検索する管理者アカウントを [管理者アカウント] に指定します。

**注意**

複数の管理者アカウントを指定する場合は、セミコロンで区切ってください。

7. [説明のキーワード] の横に、検索対象のキーワードを指定します。

8. [ログ表示] をクリックします。

日時、ホスト名、および説明が各イベントに対して表示されます。[監査ログ] を選択すると、各イベントの管理者の情報も表示されます。

9. 次のいずれかの処理を実行してください。
 - ・ リストで同時に表示される項目の数を変更するには、表の上部にあるドロップダウンボックスから新しい表示値を選択します。
 - ・ 表を並び替えるには、列のタイトルをクリックします。
 - ・ 検索結果を印刷するには、[現在のページを印刷] をクリックします。
 - ・ 検索結果をカンマ区切り値のファイルに保存するには、[CSV 形式にエクスポート] をクリックします。

ポリシーイベントログのクエリを実行する

手順

1. [ログ] > [クエリ] の順に選択します。
2. [種類] の横で [ポリシーイベント] を選択します。

ポリシーイベントログの検索画面が表示されます。
3. [種類] の横にある 2 番目のドロップダウンボックスで、次の項目からポリシーおよびそのポリシーに設定したルールに適合するものを選択します。
 - ・ すべて
 - ・ ウイルスまたは不正コード
 - ・ APT (標的型サイバー攻撃)
 - ・ スパイウェア/グレーウェア
 - ・ C&C メール
 - ・ スпамメール/フィッシング

- ・ グレーメール
- ・ Web レピュテーション

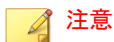
**注意**

[Web レピュテーション]を選択すると、Web サイトコンテンツのカテゴリを含む2つのドロップダウンリストが追加で表示されます。カテゴリ名を選択して、ログクエリを絞り込みます。

- ・ DKIM の適用
 - ・ 添付ファイル
 - ・ サイズ
 - ・ 内容
 - ・ コンプライアンス
 - ・ 検索の除外
 - ・ クラウドプレフィルタによってタグ付けされたスパムメール
 - ・ 不審オブジェクト
 - ・ その他
4. 次のいずれかの追加情報を指定してください。
- ・ 送信者
 - ・ 受信者
 - ・ ルール
 - ・ 件名
 - ・ 添付ファイル
 - ・ メッセージ ID

いずれかのテキストボックスを空白のままにすると、その項目に対するすべての結果が表示されます。

5. [ログ表示] をクリックします。日時、処理、ルール、およびメッセージ ID が各イベントに対して表示されます。
6. [日時] リンクをクリックして、次の情報を表示します。
 - ・ 日時
 - ・ 送信者
 - ・ 受信者
 - ・ 件名
 - ・ 元のサイズ
 - ・ 違反している添付ファイル
 - ・ ルールタイプ
 - ・ ルール
 - ・ 処理
 - ・ メッセージ ID
 - ・ 内部 ID
 - ・ 理由
 - ・ 検索サービス
7. 次のいずれかの処理を実行してください。
 - ・ リストで同時に表示される項目の数を変更するには、表の上部にあるドロップダウンボックスから新しい表示値を選択します。
 - ・ 表を並び替えるには、列のタイトルをクリックします。
 - ・ 検索結果を印刷するには、[現在のページを印刷] をクリックします。
 - ・ 検索結果をカンマ区切り値のファイルに保存するには、[CSV 形式にエクスポート] をクリックします。

**注意**

- ・ 「*A*;*B*」は、A または B が含まれる文字列を示します。
- ・ 「A*;*B」は、先頭が A である文字列、または末尾が B である文字列を示します。
- ・ 「;」は、OR 演算子を表します。

隔離イベントログのクエリを実行する

手順

1. [ログ] > [クエリ] の順に選択します。
2. [種類] の横で [隔離イベント] を選択します。
隔離イベントログの検索画面が表示されます。
3. [日付] の横で、日付と時間の範囲を選択します。
4. [ルール] の横に、検索対象のルール名のキーワードを指定します。
5. [ログ表示] をクリックします。

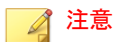
各ルールのルール名、隔離イベント数、解除イベント数、および解除の割合が表示されます。

6. 次のいずれかの処理を実行してください。
 - ・ リストで同時に表示される項目の数を変更するには、表の上部にあるドロップダウンボックスから新しい表示値を選択します。
 - ・ 表を並び替えるには、列のタイトルをクリックします。
 - ・ 検索結果を印刷するには、[現在のページを印刷] をクリックします。
 - ・ 検索結果をカンマ区切り値のファイルに保存するには、[CSV 形式にエクスポート] をクリックします。

URL クリックの追跡ログのクエリを実行する

手順

1. [ログ] > [クエリ] の順に選択します。
2. [種類] の横で [URL クリックの追跡] を選択します。
URL クリックの追跡ログの検索画面が表示されます。
3. [日付] の横で、日付と時間の範囲を選択します。
4. [URL] の横に、検索対象の URL を指定します。
5. 次のいずれかの追加情報を指定してください。
 - ・ 送信者
 - ・ 受信者
 - ・ メッセージ ID

**注意**

各 URL クリックの追跡ログはメールメッセージ情報と URL クリック情報で構成されます。[送信者]、[受信者]、および [メッセージ ID] を含むメールメッセージ情報は InterScan MSS によって生成され、[タイムスタンプ]、[URL]、[ブロック]、[警告]、および [クリックスルー] を含む URL クリック情報は Time-of-Click プロテクションサービスから取得されます。InterScan MSS はクエリ用のログを提供する前に、これら 2 つのソースからの情報を組み合わせます。

メールメッセージに関連するフィールドが検索結果で利用できないと表示される場合、次のような理由が考えられます。

- ・ InterScan MSS は、ログ設定で指定された一定期間のみのメールメッセージ情報を保存します。メールメッセージ情報の有効期限は切れているが URL クリック情報の有効期限は切れていないログを、フィールドを指定せずにクエリすると、これらのログは検索結果に表示されますが、メールメッセージに関連するフィールドは利用不可と見なされます。ただし、メールメッセージに関連するフィールドを指定してログをクエリした場合、指定されたフィールド値を InterScan MSS で照合できないため、これらのログは表示されません。
- ・ 各 InterScan MSS サーバにはログ用の独自のメールメッセージ情報がありますが、URL クリックの追跡ログはアクティベーションコードによって生成されます。複数の InterScan MSS サーバで 1 つのアクティベーションコードを共有している場合、1 つの InterScan MSS サーバが、他の InterScan MSS サーバに属するメールメッセージ情報を持つログを保持する場合があります。そのサーバ上でログのクエリを実行すると、期限切れのメールメッセージ情報を含むログの場合と類似した状況になります。

6. [ログ表示] をクリックします。

クリックのタイムスタンプ、メッセージの送信者、受信者、URL、メッセージ ID、および URL がブロック、警告、またはクリックスルーであるかどうかが各レコードに表示されます。

7. 次のいずれかの処理を実行してください。

- ・ リストで同時に表示される項目の数を変更するには、表の上部にあるドロップダウンボックスから新しい表示値を選択します。
- ・ 表を並び替えるには、列のタイトルをクリックします。

- ・ 検索結果を印刷するには、[現在のページを印刷] をクリックします。
 - ・ 検索結果をカンマ区切り値のファイルに保存するには、[CSV 形式にエクスポート] をクリックします。
-

MTA イベントログのクエリを実行する

手順

1. [ログ] > [クエリ] の順に選択します。
 2. [種類] の横で [MTA イベント] を選択します。
MTA イベントログの検索画面が表示されます。
 3. [日付] の横で、日付と時間の範囲を選択します。
 4. [ログ表示] をクリックします。
日時および説明が各イベントに対して表示されます。
 5. 次のいずれかの処理を実行してください。
 - ・ リストで同時に表示される項目の数を変更するには、表の上部にある [1 ページあたりの結果数] ドロップダウンボックスから新しい表示値を選択します。
 - ・ 検索結果を印刷するには、[現在のページを印刷] をクリックします。
 - ・ 検索結果をカンマ区切り値のファイルに保存するには、[CSV 形式にエクスポート] をクリックします。
-

送信者フィルタログのクエリを実行する

手順

1. [ログ] > [クエリ] の順に選択します。

2. [種類] の横で [送信者フィルタ] を選択します。
 3. [種類] の横にある 2 番目のドロップダウンボックスで、次の項目から送信者フィルタに適合するものを選択します。
 - ・ すべて
 - ・ ERS
 - ・ DHA 攻撃
 - ・ バウンスメール
 - ・ ウイルス
 - ・ スпамメール
 - ・ 手動: ブロックリストで手動で指定した IP アドレスを指します。
 4. [日付] の横で、日付と時間の範囲を選択します。
 5. [IP アドレス] の横に、検索対象の IP アドレスを入力します。
 6. [ログ表示] をクリックします。InterScan MSS が各 IP アドレスまたはドメインに対してブロックを開始した日時および停止した日時の情報が表示されます。
 7. 次のいずれかの処理を実行してください。
 - ・ リストで同時に表示される項目の数を変更するには、表の上部にあるドロップダウンボックスから新しい表示値を選択します。
 - ・ 検索結果を印刷するには、[現在のページを印刷] をクリックします。
 - ・ 検索結果をカンマ区切り値のファイルに保存するには、[CSV 形式にエクスポート] をクリックします。
-

第 25 章

メール領域とキュー

この章では、Trend Micro InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) のアーカイブ領域とメールキューについて説明します。

この章の内容は次のとおりです。

- ・ 390 ページの「メール領域とキューについて」
- ・ 390 ページの「隔離とアーカイブを設定する」
- ・ 392 ページの「隔離領域を管理する」
- ・ 395 ページの「アーカイブ領域を管理する」
- ・ 397 ページの「メッセージのクエリを実行する」
- ・ 404 ページの「隔離されたメッセージを表示する」
- ・ 406 ページの「アーカイブされたメッセージを表示する」
- ・ 407 ページの「保留されたメッセージを表示する」
- ・ 408 ページの「仮想アナライザのキューのメッセージを表示する」

メール領域とキューについて

InterScan MSS では、特定のポリシーールの処理で一致したメッセージが、次の領域およびキューに保存されます。

- ・ 隔離領域: 削除するか、目的の受信者に向けて送信するかを判断する前に分析する必要があるメッセージを保存します。
- ・ アーカイブ領域: 参照用に使用するメッセージを保存します。
- ・ 保留キュー: 指定された時刻に配信されるメッセージを保存します。
- ・ 仮想アナライザのキュー: InterScan MSS から仮想アナライザに送信したメッセージを、InterScan MSS でメッセージ解析結果を受信する前に保存します。

隔離とアーカイブを設定する

隔離とアーカイブを設定すると、隔離領域とアーカイブ領域を管理でき、検索サービス別に隔離メッセージおよびアーカイブメッセージを保存するディスク領域の容量を割り当てることができます。

手順

1. [隔離およびアーカイブ] > [設定] の順に選択します。

[隔離とアーカイブの設定] 画面が表示されます。

隔離とアーカイブの設定



隔離

アーカイブ

ディスク割り当て (検索サービスあたり)

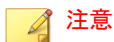
追加

削除

	領域	期限	サイズ	アイテム	EUQ
☐	初期設定の隔離	15 日	0 MB	0	
☐	コンプライアンスの隔離	15 日	0 MB	0	
☐	クラウドプレフィルタの隔離	15 日	0 MB	0	
☐	不審なオブジェクトの隔離	15 日	0 MB	0	

保存

2. [隔離] タブ (初期設定) または [アーカイブ] タブをクリックして、隔離領域かアーカイブ領域を設定します。
下の表に領域のリストが表示されます。
3. 各検索サービスのすべての隔離領域またはアーカイブ領域に割り当てられる合計ディスクサイズを変更するには、[ディスク割り当て (検索サービスあたり)] の横に領域のサイズを指定し、次にドロップダウンボックスから [MB] または [GB] を選択します。
4. 新しい隔離領域またはアーカイブ領域を追加するには、[追加] をクリックします。
5. [名前] の横に、わかりやすい名前を入力します。
6. [メッセージの保存日数が次の日数を超えた場合に削除する] の横に、日数を入力します。隔離またはアーカイブされたメッセージがこの日数を経過すると InterScan MSS から削除されます。この日数が経過するまでの間は削除されません。たとえば、15 と指定すると、隔離されたメッセージは 16 日目に InterScan MSS から削除されます。
7. [ウイルス対策ルール、フィッシング対策ルール、または Web レピュテーションルールに違反していないすべてのメールメッセージを EUQ データベースに同期させます (この領域でのみ)。] をオンにすると、自動的にメッセージがエンドユーザメール隔離データベースに保存されます。

**注意**

[ウイルス対策ルール、フィッシング対策ルール、または Web レピュテーションルールに違反していないすべてのメールメッセージを EUQ データベースに同期させます (この領域でのみ。)] をオンにすると、[隔離とアーカイブの設定] 画面のテーブルの [エンドユーザーメール隔離] 列にチェックマークが表示されます。

8. [保存] をクリックします。
[隔離とアーカイブの設定] 画面が再度表示されます。
9. 隔離領域またはアーカイブ領域を表示または変更するには、領域の名前をクリックし、上記の設定を実行します。
10. 隔離領域またはアーカイブ領域を削除するには、その領域の横にあるチェックボックスをオンにしてから [削除] をクリックします。
11. 設定を変更したら、[保存] をクリックします。

隔離領域を管理する

InterScan MSS では、サーバ上の次のディレクトリにメッセージを隔離できます。

```
$IMSS_HOME/queue/quarantine
```

**ヒント**

後で分析して本来の受信者に送信する可能性のあるメッセージは、隔離しておくことをお勧めします。スパムメール検索条件に違反するメッセージやメッセージコンテンツ条件に違反するメッセージなど、メッセージの種類ごとに異なる隔離領域を作成してください。

ポリシールールの [処理] 画面から隔離を管理する

ルールに対する処理を設定する場合は、次の手順を実行します。

手順

1. [インターセプト] 処理の [次の場所に隔離] の横にある [編集] をクリックします。

[隔離] 画面が開いて、使用可能な隔離領域が表示されます。

2. 次のいずれかを実行します。
 - ・ 新しい隔離領域を追加するには、[追加] をクリックします。
 - ・ 既存の隔離領域を変更するには、隔離領域名をクリックして、[編集] をクリックします。

編集画面が表示されます。

3. [名前] の横に、隔離領域の名前を指定します。
4. 特定の日数が経過した後に隔離されたメッセージを自動的に削除するには、[メッセージの保存日数が次の日数を超えた場合に削除する] の横に、1～60 の範囲で日数を指定します。

この日数の経過後に InterScan MSS によって隔離されたメッセージが削除されます。この日数が経過するまでの間は削除されません。たとえば、15 と指定すると、隔離されたメッセージは 16 日目に InterScan MSS から削除されます。

5. [次のルールに違反していないすべてのメッセージを EUQ データベースに同期させます (この領域でのみ)] をオンにすると、自動的にメッセージがエンドユーザメール隔離データベースに保存されます。



注意

[次のルールに違反していないすべてのメッセージを EUQ データベースに同期させます (この領域でのみ)] をオンにすると、[隔離とアーカイブの設定] 画面のテーブルの [エンドユーザメール隔離] 列にチェックマークが表示されます。

6. [保存] をクリックして、[隔離] 画面に戻ります。
7. [完了] をクリックして、処理の選択を続行します。

8. メッセージを隔離するには、[インターセプト]にある[次の場所に隔離]オプションを選択して、ドロップダウンボックスから目的の隔離領域を選択します。

隔離設定を管理する

手順

1. [メール領域とキュー]>[設定]の順に選択します。
[隔離およびアーカイブのクエリ]画面が開き、初期設定では[隔離]タブが表示されます。
2. [ディスク割り当て (検索サービスあたり)]の横で次の手順を実行します。
 - a. 領域の最大サイズを指定します。
 - b. [MB]または[GB]を選択します。



注意

隔離したメッセージの合計ディスクサイズが、検索サービスの割り当てを超えた場合、最も古い隔離されたメッセージから削除され、割り当てサイズ未満に保持されます。

3. 次のいずれかを実行します。
 - ・ 新しい隔離領域を追加するには、[追加]をクリックします。
 - ・ 既存の隔離領域を変更するには、隔離領域の名前をクリックします。
4. [名前]の横に、隔離領域の名前を指定します。
5. 特定の日数が経過した後に隔離されたメッセージを自動的に削除するには、[メッセージの保存日数が次の日数を超えた場合に削除する]の横に、1～60の範囲で日数を指定します。

この日数の経過後に InterScan MSS によって隔離されたメッセージが削除されます。この日数が経過するまでの間は削除されません。たとえば、15 と指定すると、隔離されたメッセージは 16 日目に InterScan MSS から削除されます。

6. [ウイルス対策ルール、フィッシング対策ルール、または Web レピュテーションルールに違反していないすべてのメールメッセージを EUQ データベースに同期させます (この領域でのみ)。] をオンにすると、自動的にメッセージがエンドユーザメール隔離データベースに保存されます。

**注意**

[ウイルス対策ルール、フィッシング対策ルール、または Web レピュテーションルールに違反していないすべてのメールメッセージを EUQ データベースに同期させます (この領域でのみ)。] をオンにすると、[隔離とアーカイブの設定] 画面のテーブルの [エンドユーザメール隔離] 列にチェックマークが表示されます。

7. [保存] をクリックして、[隔離およびアーカイブの設定] 画面に戻ります。
8. [保存] をクリックします。

アーカイブ領域を管理する

InterScan MSS では、サーバ上の次のディレクトリにメッセージをアーカイブできます。

```
$IMSS_HOME/queue/archive
```

ポリシールールの [処理] 画面からアーカイブを管理する

ルールに対する処理を設定する場合は、次の手順を実行します。

手順

1. [監視] 処理の [変更済みメッセージの保存先] の横にある [編集] をクリックします。
[アーカイブ] 画面が開いて、使用可能な隔離領域が表示されます。
2. 次のいずれかを実行します。

- ・ 新しいアーカイブ領域を追加するには、[追加] をクリックします。
- ・ 既存のアーカイブ領域を変更するには、アーカイブ領域名をクリックして、[編集] をクリックします。

編集画面が表示されます。

3. [名前] の横に、アーカイブ領域の名前を指定します。
4. 特定の日数が経過した後にアーカイブされたメッセージを自動的に削除するには、[メッセージの保存日数が次の日数を超えた場合に削除する] の横に、1～60 の範囲で日数を指定します。

この日数の経過後に InterScan MSS によってアーカイブされたメッセージが削除されます。この日数が経過するまでの間は削除されません。たとえば、15 と指定すると、アーカイブされたメッセージは 16 日目に InterScan MSS から削除されます。

5. [保存] をクリックして、[アーカイブ] 画面に戻ります。
6. [完了] をクリックして、処理の選択を続行します。
7. メッセージをアーカイブするには、[監視] にある [変更済みメッセージの保存先] オプションを選択して、ドロップダウンボックスから目的のアーカイブ領域を選択します。

アーカイブの設定を管理する

手順

1. [隔離およびアーカイブ] > [設定] の順に選択します。

[隔離とアーカイブの設定] 画面が開き、初期設定では [隔離] タブが表示されます。
2. [アーカイブ] タブをクリックします。
3. [ディスク割り当て (検索サービスあたり)] の横で次の手順を実行します。
 - a. 領域の最大サイズを指定します。

- b. [MB] または [GB] を選択します。

**注意**

アーカイブされたメッセージの合計ディスクサイズが、検索サービスの割り当てを超えた場合、最も古いアーカイブメッセージから削除され、割り当てサイズ未満に保持されます。

4. 次のいずれかを実行します。
- ・ 新しい隔離領域を追加するには、[追加] をクリックします。
 - ・ 既存の隔離領域を変更するには、隔離領域名をクリックして、[編集] をクリックします。
- 編集画面が表示されます。
5. [名前] の横に、アーカイブ領域の名前を指定します。
6. 特定の日数が経過した後にアーカイブされたメッセージを自動的に削除するには、[メッセージの保存日数が次の日数を超えた場合に削除する] の横に、1~60 の範囲で日数を指定します。
- この日数の経過後に InterScan MSS によってアーカイブされたメッセージが削除されます。この日数が経過するまでの間は削除されません。たとえば、15 と指定すると、アーカイブされたメッセージは 16 日目に InterScan MSS から削除されます。
7. [保存] をクリックして、[隔離およびアーカイブの設定] 画面に戻ります。
8. [保存] をクリックします。

メッセージのクエリを実行する

隔離およびアーカイブが行われたメッセージに関するクエリを実行してから、それらのメッセージに対する処理を決定できます。メッセージの詳細を確認した後で、InterScan MSS からアーカイブされたメッセージを送信するか、削除するかを選択できます。

**ヒント**

トレンドマイクロでは、ウイルス対策ルールに違反するメッセージや添付ファイルなど、ネットワークを危険にさらす可能性のあるアイテムは隔離することをお勧めします。隔離されたメッセージを再送信する前に、それがネットワークに脅威を与えないことを確認してください。

アーカイブの対象は後日の参照が必要になるアイテムに限定することをお勧めします。

隔離領域のクエリを実行する

手順

1. [隔離およびアーカイブ] > [クエリ] の順に選択します。

[隔離およびアーカイブのクエリ] 画面が表示されます。初期設定では [隔離] タブが表示されます。表示されない場合は、[隔離] をクリックします。

隔離とアーカイブの設定



隔離

アーカイブ

ディスク割り当て (検索サービスあたり) 10 GB

追加

削除

	領域	期限	サイズ	アイテム	EUQ
☐	初期設定の隔離	15 日	0 MB	0	
☐	コンプライアンスの隔離	15 日	0 MB	0	
☐	クラウドプレフィルタの隔離	15 日	0 MB	0	
☐	不審なオブジェクトの隔離	15 日	0 MB	0	

保存

2. [条件] で、次の項目を設定します。
 - ・ 検索: 隔離領域、メッセージが隔離された理由、およびメッセージを検索した検索サービスを選択します。
 - ・ 日付: 日付と時間の範囲を選択します。

3. 次の項目に対する値を指定します。

- ・ 送信者
- ・ 件名
- ・ 受信者
- ・ 添付ファイル
- ・ ルール
- ・ メッセージ ID



注意

複数の受信者または違反する添付ファイルを含むメッセージのクエリを実行する場合、「*文字列*」と入力します (ここで文字列は受信者または添付ファイルのいずれかの名前を指します)。

4. [ログ表示] をクリックします。結果が画面の下部に表示され、日時、送信者、受信者、件名、およびメッセージの隔離理由が示されます。
5. 表示内容を変更するには、次のいずれかの操作を実行します。
- ・ 表を並び替えるには、任意の列見出しをクリックします (理由を除く)。
 - ・ リストに表示される項目が多すぎる場合は、リストの上部にある矢印ボタンをクリックして次のページに移動するか、表示するページをドロップダウンリストから選択します。
 - ・ リストで同時に表示される項目の数を変更するには、表の下部にあるドロップダウンリストから新しい表示値を選択します。
6. 隔離されたメッセージの詳細を表示するには、そのアイテムの日時をクリックします。[隔離のクエリ] 画面が開いて、メッセージとそのすべての詳細情報が表示されます。
7. メッセージを再送信するには、検索結果表内のそのメッセージの横にあるチェックボックスをオンにしてから、次のいずれかのオプションをクリックします。

- ・ 配信: ウイルス検索ルール以外のすべてのルールを省略して検索し、メッセージを受信者に送信します。
- ・ 再処理: 隔離される原因となったルールでの検索を省略し、その他のルールによってメッセージを検索した後、受信者に送信します。このため、このメッセージはその他のフィルタによって再度隔離される場合があります。



ヒント

トレンドマイクロでは、ウイルス対策フィルタに違反するメッセージを再送信することをお勧めしません。再送信すると、ネットワークを危険にさらす可能性があります。

8. メッセージを削除するには、検索結果表内のそのメッセージの横にあるチェックボックスをオンにしてから [削除] をクリックします。



注意

検索条件として [添付ファイル] が指定されている場合のみ、InterScan MSS では違反する添付ファイルのファイル名を記録および表示します。ただし、ポリシーの検索条件で、メッセージ内の添付ファイル数が条件として指定され、その数を超過している場合、添付ファイル名は表示されません。

アーカイブ領域のクエリを実行する

手順

1. [隔離およびアーカイブ] > [クエリ] の順に選択します。
初期設定では [隔離] タブが表示されます。
2. [アーカイブ] タブをクリックします。
3. [条件] で、次の項目を設定します。
 - ・ 検索: アーカイブ領域、メッセージがアーカイブされた理由、およびメッセージを検索した検索サービスを選択します。

- ・ 日付: 時間の範囲を選択します。
4. 次の項目に対する値を指定します。

- ・ 送信者
- ・ 件名
- ・ 受信者
- ・ 添付ファイル
- ・ ルール
- ・ メッセージ ID

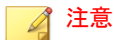
**注意**

複数の受信者または違反する添付ファイルを含むメッセージのクエリを実行する場合、「*文字列*」と入力します (ここで文字列は受信者または添付ファイルのいずれかの名前を指します)。

5. [ログ表示] をクリックします。結果が画面の下部に表示され、日時、送信者、受信者、件名、およびメッセージがアーカイブされた理由が表示されます。
6. 表示内容を変更するには、次のいずれかの操作を実行します。
- ・ 表を並び替えるには、任意の列見出しをクリックします (理由を除く)。
 - ・ リストに表示される項目が多すぎる場合は、リストの上部にある矢印ボタンをクリックして次のページに移動するか、表示するページをドロップダウンリストから選択します。
 - ・ リストで同時に表示される項目の数を変更するには、表の下部にあるドロップダウンリストから新しい表示値を選択します。
7. アーカイブされたメッセージの詳細を表示するには、そのアイテムの日時をクリックします。

[アーカイブのクエリ] 画面が開いて、メッセージとそのすべての詳細情報が表示されます。

- メッセージを削除するには、検索結果表内のそのメッセージの横にあるチェックボックスをオンにしてから [削除] をクリックします。

**注意**

検索条件として [添付ファイル] が指定されている場合のみ、InterScan MSS では違反する添付ファイルのファイル名を記録および表示します。ただし、ポリシーの検索条件で、メッセージ内の添付ファイル数が条件として指定され、その数を超過している場合、添付ファイル名は表示されません。

保留されたメッセージのクエリを実行する

手順

- [メール領域とキュー] > [クエリ] の順に選択します。
初期設定では [隔離] タブが表示されます。
- [保留] タブをクリックします。
- [条件] で、次の項目を設定します。
 - 検索:理由とデバイスを選択します。
 - 日付:日付と時間の範囲を選択します。
- 次の項目に対する値を指定します。
 - 送信者
 - 件名
 - 受信者
 - 違反する添付ファイル
 - ルール
 - 内部 ID
- [ログ表示] をクリックします。結果が画面の下部に表示され、日時、送信者、受信者、件名、およびこのメッセージを保留した理由が示されます。

6. 表示内容を変更するには、次のいずれかの操作を実行します。
 - ・ 表を並び替えるには、任意の列見出しをクリックします (理由を除く)。
 - ・ リストに表示される項目が多すぎる場合は、リストの上部にある矢印ボタンをクリックして次のページに移動するか、表示するページをドロップダウンリストから選択します。
 - ・ リストで同時に表示される項目の数を変更するには、表の下部にあるドロップダウンリストから新しい表示値を選択します。
 7. 保留されたメッセージの詳細を表示するには、その項目の [日時] をクリックします。メッセージとそのすべての詳細情報が表示されます。
 8. メッセージを再送信するには、検索結果表内のそのメッセージの横にあるチェックボックスをオンにしてから、[解除] をクリックします。
 9. メッセージを削除するには、検索結果表内のそのメッセージの横にあるチェックボックスをオンにしてから [削除] をクリックします。
-

仮想アナライザのキューでメッセージのクエリを実行する

手順

1. [メール領域とキュー] > [クエリ] の順に選択します。

初期設定では [隔離] タブが表示されます。
2. [仮想アナライザ] タブをクリックします。
3. [条件] で、次の項目を設定します。
 - ・ 検索: デバイスを選択します。
 - ・ 日付: 日付と時間の範囲を選択します。
4. 次の項目に対する値を指定します。
 - ・ 送信者

- ・ 受信者
 - ・ 件名
5. [ログ表示] をクリックします。
結果が画面の下部に表示されます。
 6. 表示内容を変更するには、次のいずれかの操作を実行します。
 - ・ 表を並び替えるには、任意の列見出しをクリックします (理由を除く)。
 - ・ リストに表示される項目が多すぎる場合は、リストの上部にある矢印ボタンをクリックして次のページに移動するか、表示するページをドロップダウンリストから選択します。
 - ・ リストで同時に表示される項目の数を変更するには、表の下部にあるドロップダウンリストから新しい表示値を選択します。
 7. 仮想アナライザのキューのメッセージの詳細を表示するには、その項目の [日時] をクリックします。メッセージとそのすべての詳細情報が表示されます。
 8. メッセージを仮想アナライザの検索対象から解除するには、検索結果表内のそのメッセージの横にあるチェックボックスをオンにしてから、[解除] をクリックします。

**注意**

不審メッセージを仮想アナライザの検索対象から解除することはお勧めしません。再送信すると、ネットワークを危険にさらす可能性があります。

隔離されたメッセージを表示する

InterScan MSS によって隔離されたすべてのメッセージは、クエリの実行および表示が可能です。

手順

1. 隔離されたメッセージのクエリ検索を実行した後で、検索結果表内のアイテムの日時をクリックします。次の情報とともに [隔離のクエリ] 画面が表示されます。
 - ・ 日時
 - ・ 送信者
 - ・ 理由
 - ・ 受信者
 - ・ ルール
 - ・ 件名
 - ・ 検索サービス
 - ・ 元のサイズ
 - ・ メッセージ ID
 - ・ 内部 ID
 - ・ 添付ファイル
2. [メッセージ表示] の横の [ヘッダ] または [メッセージ] をクリックします。
3. 次のボタンのいずれかをクリックします。
 - ・ リストに戻る: 検索画面に戻ります。
 - ・ 配信: メッセージを元の受信者に再送信します。
 - ・ 再処理: InterScan MSS によってメッセージが再度検索され、その結果に従って処理されます。
 - ・ 削除: メッセージを削除します。
 - ・ ダウンロード: メッセージをコンピュータに保存します。



ヒント

トレンドマイクロでは、ウイルス対策ルールに違反するメッセージまたは添付ファイルは保存しないことをお勧めします。

アーカイブされたメッセージを表示する

InterScan MSS によってアーカイブされたすべてのメッセージは、クエリの実行および表示が可能です。

手順

1. アーカイブされたメッセージのクエリ検索を実行した後で、検索結果表内のアイテムの日時をクリックします。次の情報とともに [アーカイブのクエリ] 画面が表示されます。
 - ・ 日時
 - ・ 送信者
 - ・ 理由
 - ・ 受信者
 - ・ ルール
 - ・ 件名
 - ・ 検索サービス
 - ・ 元のサイズ
 - ・ メッセージ ID
 - ・ 内部 ID
 - ・ 添付ファイル
2. [メッセージ表示] の横の [ヘッダ] または [メッセージ] をクリックします。

3. 次のボタンのいずれかをクリックします。
 - ・ リストに戻る: 検索画面に戻ります。
 - ・ 削除: メッセージを削除します。
 - ・ ダウンロード: メッセージをコンピュータに保存します。



ヒント

トレンドマイクロでは、ウイルス対策ルールに違反するメッセージまたは添付ファイルを保存することをお勧めしません。

保留されたメッセージを表示する

InterScan MSS によって保留されたすべてのメッセージは、クエリの実行および表示が可能です。

手順

1. 保留されたメッセージのクエリ検索を実行した後で、検索結果表内のアイテムの日時をクリックします。以下の情報とともに検索画面が表示されます。
 - ・ 日時
 - ・ 送信者
 - ・ 理由
 - ・ 受信者
 - ・ ルール
 - ・ 件名
 - ・ 検索サービス
 - ・ 元のサイズ

- ・ メッセージ ID
- ・ 内部 ID
- ・ 添付ファイル

ATSE が有効な場合、InterScan MSS では次の情報も表示されます。

- ・ 理由: 考えられる高度な脅威

ATSE と仮想アナライザの両方が有効な場合、InterScan MSS では次の情報も表示されます。

- ・ 理由: 考えられる高度な脅威または分析済みの高度な脅威
- ・ 仮想アナライザのステータス: 仮想アナライザの分析のステータス

2. [メッセージ表示] の横の [ヘッダ] または [メッセージ] をクリックします。
3. 次のボタンのいずれかをクリックします。

- ・ リストに戻る: 検索画面に戻ります。
- ・ 解除: メッセージを元の受信者に再送信します。
- ・ 削除: メッセージを削除します。
- ・ ダウンロード: メッセージをコンピュータに保存します。



ヒント

トレンドマイクロでは、ウイルス対策ルールに違反するメッセージまたは添付ファイルを保存することをお勧めしません。

仮想アナライザのキューのメッセージを表示する

InterScan MSS から仮想アナライザに送信するメールメッセージは、分析の保留中または分析の実行中、仮想アナライザのキューに保存されています。仮想アナライザのキューのメッセージはすべて、クエリおよび表示が可能です。

**注意**

InterScan MSS でメールメッセージの分析結果を受信すると、そのメッセージは仮想アナライザのキューから削除されます。

手順

1. 仮想アナライザのキューのメッセージのクエリ検索を実行した後で、検索結果表内のアイテムの日時をクリックします。以下の情報とともに検索画面が表示されます。
 - ・ 日時
 - ・ メッセージ ID
 - ・ 送信者
 - ・ 受信者
 - ・ ルール
 - ・ 添付ファイル
 - ・ 件名
 - ・ 検索サービス
 - ・ 元のサイズ
 - ・ 内部 ID
 - ・ 送信
 - ・ クエリ時間
 - ・ 回数
 - ・ 期限
2. [メッセージ表示] の横の [ヘッダ] または [メッセージ] をクリックします。
3. 次のボタンのいずれかをクリックします。
 - ・ リストに戻る:検索画面に戻ります。

- ・ 解除:メッセージを仮想アナライザの検索対象から解除します。他の検索条件に合致する場合は、このメッセージの検索が継続される場合があります。
-

第 26 章

通知

この章では、InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) の通知に関する一般的な手順について説明します。

この章の内容は次のとおりです。

- ・ 412 ページの「イベント通知」
- ・ 412 ページの「通知を設定する」
- ・ 415 ページの「イベント条件および通知メッセージを設定する」
- ・ 418 ページの「エンドユーザメール隔離通知」
- ・ 420 ページの「ログオン通知の設定」
- ・ 421 ページの「通知を編集する」

イベント通知

次のカテゴリのイベント発生時に、ユーザ自身または特定のユーザに、メールまたは SNMP 通知を送信するように InterScan MSS を設定することができます。

表 26-1. イベント通知

イベント	説明
システムステータス	特定の InterScan MSS のパフォーマンスが要求レベルを下回った場合に通知します。 たとえば、検索サービスの動作が停止した場合、または配信キュー内のメッセージ数が指定値を超えた場合です。
予約アップデートイベント	InterScan MSS で、アップデート元から管理データベースへの検索エンジンおよびパターンファイルの予約アップデートを実行できた場合、または実行できなかった場合に通知します。
検索サービスアップデート結果	InterScan MSS で、いずれかの検索サービスのエンジンまたはパターンファイルをアップデートできなかった場合に通知します。
仮想アナライザの設定	仮想アナライザの分析が不完全または無効である場合に通知します。
Smart Protection イベント	InterScan MSS が従来型スキャンに戻った場合、あるいは Smart Protection サービスまたはローカルソースを使用できない場合にアラートが送信されます。

通知を設定する

通知を設定すると、メールおよび SNMP トラップを設定して、システムおよびポリシーイベントの通知メッセージを配信できます。

**注意**

InterScan MSS 9.1 では、IPv6 サーバへの通知の送信をサポートしています。

手順

1. [管理] > [通知] の順に選択します。
初期設定で [イベント] タブが表示されます。
2. [通知設定] タブをクリックします。

通知

イベント	通知設定	EUQ通知	ログオン通知
メール設定			
受信者:	root@localhost 複数のアドレスを指定する場合はセミコロン (;) で区切ってください。		
送信者のメールアドレス	postmaster@localhost		
SMTPサーバアドレス	127.0.0.1		
SMTPサーバポート番号:	10026		
文字コード:	UTF-8 (utf-8)		
メッセージヘッダ:			
メッセージフッタ:			
SNMPトラップ			
サーバ名 (IPまたはFQDN)			
コミュニティ名:	public		
SNMPのバージョン:	SNMPv1		
保存 キャンセル			

3. [メール設定] で、次の項目を設定します。
 - ・ 受信者: 受信者のメールアドレスを指定します。
 - ・ 送信者のメールアドレス: 送信者として表示されるメールアドレスを指定します。

- ・ SMTP サーバアドレス: ネットワーク上でメールを配信する SMTP サーバの完全修飾ドメイン名 (FQDN) または IP アドレスを指定します。
 - ・ SMTP サーバポート番号: InterScan MSS が SMTP サーバへの接続に使用するポート番号を指定します。
 - ・ 文字コード: InterScan MSS ではこの設定を使用して、通知メッセージをエンコードします。
 - ・ メッセージヘッダ: 通知の先頭に表示するテキストを指定します。
 - ・ メッセージフッタ: 通知の末尾に表示するテキストを指定します。
4. [SNMP トラップ] で、次の項目を設定します。
- ・ サーバ名
 - ・ コミュニティ
 - ・ SNMP のバージョン

オプション	説明
サーバ名	SNMP サーバの完全修飾ドメイン名または IP アドレスを入力します。SNMP トラップは、管理上の注意が必要なイベントが発生したときに SNMP (Simple Network Management Protocol) サーバに送信される通知メッセージです。  注意 SNMP サーバは IPv6 形式のアドレスをサポートしません。
コミュニティ名	SNMP サーバのコミュニティ名を入力します。コミュニティは、SNMP を実行するコンピュータおよび管理端末が属するグループです。すべての SNMP 管理端末に警告メッセージを送信するには、コミュニティ名として「public」を指定します。
SNMP のバージョン	次のいずれかを選択します。 ・ SNMPv1 ・ SNMPv2c

オプション	説明
	詳細については、SNMP のドキュメントを参照してください。

5. [保存] をクリックします。
設定ウィザードを使用している場合は、[次へ] をクリックします。

イベント条件および通知メッセージを設定する

InterScan MSS により通知メッセージが送信される際の条件を設定したり、イベントごとにメッセージの内容をカスタマイズできます。

手順

1. [管理] > [通知] の順に選択します。

初期設定で [イベント] タブが表示されます。

通知 

イベント

通知設定

EUQ通知

ログオン通知

システムイベント通知		
システムステータス	メール	SNMP
次の間隔で通知 10 分		
検索サービスの停止時間が次の長さを超えている場合: 10 分	☒	☐
検索サービスで利用できる空きディスク容量が次の値を下回った場合: 10240 MB	☒	☐
次の値を超える件数のメッセージが配信キューにある場合: 20000 メッセージ	☒	☐
次の値を超える件数のメッセージが再試行キューにある場合: 10000 メッセージ	☒	☐
予約アップデートイベント	メール	SNMP
ウイルスパターンファイル、スプ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、およびスマートスキャンエージェントパターンファイルの予約アップデート:		
失敗	☒	☐
成功	☒	☐
高度な脅威検索エンジン、ウイルス検索エンジン、または URL フィルタエンジンの予約アップデート:		
失敗	☒	☐
成功	☒	☐
スパムメール検索エンジンまたはスパムメール対策パターンファイルの予約アップデート:		
失敗	☒	☐
成功	☒	☐
検索サービスアップデート結果	メール	SNMP
アップデートコンポーネントの適用に失敗した場合	☒	☐
仮想アナライザの設定	メール	SNMP
メッセージの分析が不完全または無効です	☒	☐
Smart Protection イベント	メール	SNMP
お使いのサーバーでは Smart Protection サービスが利用できません	☒	☐
従来型スキャンに切り替えました	☒	☐
Webレピューテーションのクエリにローカルソースを使用できません	☒	☐

保存

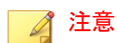
キャンセル

2. [システムステータス] で、次の項目を設定します。

- 次の間隔で通知 { } 分: すべてのパフォーマンス通知の通知間隔を指定します。

それぞれの通知を編集するには、次のリンクをクリックします。

- ・ 検索サービスの停止時間が次の長さを超えている場合: 時間を分単位で指定します。
- ・ 検索サービスで利用できる空きディスク容量が次の値を下回った場合: MB 単位の数値を指定します。
- ・ 次の値を超える件数のメッセージが配信キューにある場合: メッセージ数を指定します。
- ・ 次の値を超える件数のメッセージが再試行キューにある場合: メッセージ数を指定します。

**注意**

[次の値を超える件数のメッセージが配信キューにある場合]、および [次の値を超える件数のメッセージが再試行キューにある場合] の通知は、InterScan MSS が Postfix を使用している場合にのみ機能します。

3. [予約アップデートイベント] で、[失敗] と [成功] のリンクをクリックして、コンポーネントのアップデートに関する通知を編集します。

予約アップデートイベントとは、アップデート元から InterScan MSS 管理データベースに最新のエンジンおよびパターンファイルがアップデートされるイベントです。

4. [検索サービスアップデート結果] で、[アップデートコンポーネントの適用に失敗した場合] リンクをクリックして、通知を編集します。

検索サービスアップデート結果とは、InterScan MSS 管理データベースから検索サービスへの最新のエンジンおよびパターンファイルのアップデートの結果です。

5. [仮想アナライザの設定] で、[メッセージの分析が不完全または無効] リンクをクリックして、通知を編集します。

この通知は、InterScan MSS と仮想アナライザ間の通信の中断について説明します。InterScan MSS は、次の理由でこの通知を送信する場合があります。

- ・ ファイルまたはデータベース操作エラー
- ・ クライアント、サーバ、またはネットワーク通信エラー

- ・ 無効な分析レポート
6. [Smart Protection イベント] で、次のリンクをクリックして通知を編集します。
 - ・ お使いのサーバでは Smart Protection サービスが利用できません
 - ・ 従来型スキャンに切り替えました
 - ・ Web レピュテーションのクエリにローカルソースを使用できません
 7. 希望する通知の受信方法に従って、[メール]、[SNMP]、または両方のチェックボックスをオンにします。
 8. [保存] をクリックします。
-

エンドユーザメール隔離通知

エンドユーザメール隔離通知は、スパムメールとして処理され、一時的に [エンドユーザメール隔離] に保存されているメッセージについてユーザに知らせるために InterScan MSS から送信される通知です。



注意

InterScan MSS では、前回の通知以降に新しく隔離されたメッセージがある場合にのみ、エンドユーザメール隔離通知が送信されます。

配布リストアドレスにはエンドユーザメール隔離通知は送信されません。配布リストの隔離されたメッセージを管理するには、ユーザはエンドユーザメール隔離管理コンソールにログオンする必要があります。

エンドユーザメール隔離通知では、次の情報が提供されます。

- ・ スпамメールの総数: 前回の通知以降にエンドユーザメール隔離通知に新しく保存されたメッセージの数
- ・ メッセージリスト: スпамとして処理された新しいメッセージの概要
 - ・ 送信者: 送信者のメールアドレス

- ・ 件名: 件名行
- ・ サイズ: 添付ファイルを含むメッセージサイズ
- ・ 受信日時: メッセージを受信した日時
- ・ インライン処理リンク: 隔離されたメッセージに処理を適用、および、[承認済み送信者] リストに送信者を追加するためのリンク

**注意**

インライン処理リンクは、管理者がこの機能を有効にしている場合にのみ表示されます。

エンドユーザメール隔離通知を設定する

手順

1. [管理] > [通知] の順に選択します。
初期設定では [イベント] タブが表示されます。
2. [EUQ 通知] をクリックします。
3. [エンドユーザメール隔離 (EUQ) 通知を有効にする] の横にあるチェックボックスをオンにします。
4. [通知スケジュール] で、次のいずれかの頻度を選択します。
 - ・ 毎日: ドロップダウンボックスから時刻を選択します。
 - ・ 毎週: ドロップダウンボックスから曜日と時刻を選択します。
5. [通知メールテンプレート] に、件名と通知内容を指定します。
通知に挿入できる変数のリストを表示するには、[変数リスト] をクリックします。
6. エンドユーザメール隔離通知からユーザが処理を適用できるようにするには、[インライン処理を有効にする] を選択します。

7. [保存] をクリックします。
-

インライン処理リンク

InterScan MSS を使用すると、エンドユーザメール隔離通知内のリンクを介して隔離されたメッセージに処理を適用できます。ユーザは対応するリンクをクリックして、次の処理のいずれかを選択できます。

- ・ 削除: メッセージとすべての添付ファイルを削除します。
- ・ 解除: メッセージの隔離を解除します。InterScan MSS は再度メッセージを検索するか、またはそれを元の受信者に送信できます。



注意

[エンドユーザがメッセージを再処理するときに、承認済み送信者の動作を「自動追加」するかどうかを指定する] 機能を有効にしている場合、InterScan MSS は解除されたメッセージの送信者を自動的に [承認済み送信者] リストに追加します。

- ・ 送信者を承認済みリストに追加: InterScan MSS はこの送信者からのメッセージをスパムメールとして識別しません。

InterScan MSS は指定された一定の期間が経過すると自動的にメッセージを削除します。InterScan MSS 管理コンソールからメッセージを手動で削除したり、解除することもできます。ユーザは削除済みまたは解除済みのメッセージの処理を選択することはできません。



重要

トレンドマイクロでは、通知を転送することをお勧めしません。インライン処理リンクは、転送メッセージでも有効なままです。

ログオン通知の設定

ログオン通知は、ログオンページに表示される、管理者向けのカスタマイズ可能なメッセージです。

手順

1. [管理] > [通知] の順に選択します。
初期設定では [イベント] タブが表示されます。
2. [ログオン通知] をクリックします。

通知 

イベント 通知設定 ELUG通知 **ログオン通知**

ログオンページに表示する管理者向けのメッセージを指定してください。2,000文字まで指定できます。プレーンテキストのみサポートされます。エンドユーザーメール隔離のログオン通知を設定するには、「ユーザーメール隔離アクセス」ページを参照してください。

dsfs

保存 キャンセル

3. 管理者に表示されるログオン通知を指定します。
4. [保存] をクリックします。

通知を編集する

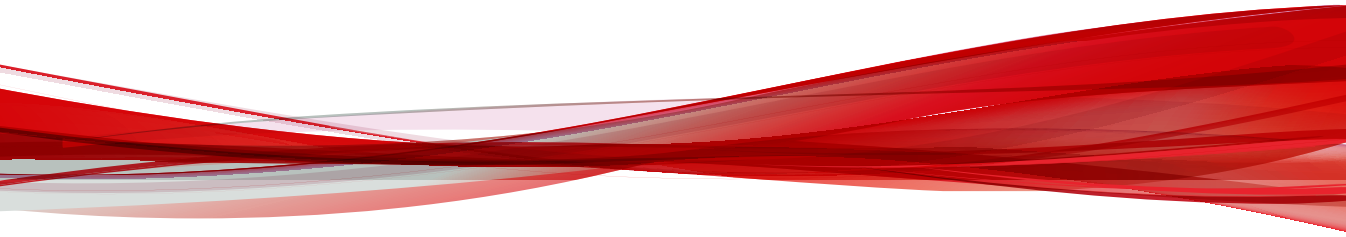
手順

1. [管理] > [通知] の順に選択します。
2. 編集する通知をクリックします。
その通知の編集画面が表示されます。

3. 件名とメッセージ、または SNMP メッセージを指定します。
通知に挿入できる変数のリストを表示するには、[変数リスト] をクリックします。
 4. [保存] をクリックします。
-

パート V

InterScan MSS の管理



第 27 章

設定のバックアップ、復元、および複製

この章では、InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) の設定をバックアップおよび復元する手順について説明します。複数の InterScan MSS 検索サービスが配置されており、Trend Micro Control Manager (以下、Control Manager) も使用している場合は、新しい検索サービスごとに設定を実行しなくても、InterScan MSS 設定を複製できます。

この章の内容は次のとおりです。

- ・ 426 ページの「設定のインポートとエクスポート」
- ・ 428 ページの「InterScan MSS をバックアップする」
- ・ 430 ページの「InterScan MSS を復元する」
- ・ 432 ページの「設定を複製する」
- ・ 434 ページの「デバッグログをエクスポートする」

設定のインポートとエクスポート

[インポート/エクスポート] 画面を使用して、InterScan MSS 設定のバックアップを作成します。バックアップを保存しておくと、設定を InterScan MSS 9.1 サーバに簡単に再適用できます。同じ設定ファイルを対象の InterScan MSS 9.1 サーバにインポートすることによって、複数のサーバ間で設定を複製することもできます。



重要

次の設定のみ InterScan MSS 9.1 Linux 版と互換性があります。その他の設定のインポートはサポートされていません。

- ・ InterScan MSS 7.0 Solaris 版 Service Pack 1 Patch 4
- ・ InterScan MSS 7.1 Linux 版 Service Pack 2 Patch 1
- ・ InterScan MSS 9.1 Linux 版



注意

InterScan MSS 9.1 では、IPv6 形式でインポートされたアドレスを認識し、IPv6 形式でアドレスをエクスポートできます。ただし、`imss.ini` 設定は手動でインポートまたはエクスポートする必要があります。

設定ファイルをエクスポートする

エクスポート中には次のことを行わないでください。

- ・ その他の管理コンソール画面にアクセスしたり、設定を変更したりする
- ・ データベースの操作を行う
- ・ InterScan MSS サービスを開始または停止する
- ・ EUQ データベースを InterScan MSS に登録する、または InterScan MSS から登録解除する
- ・ 他のエクスポートタスクまたはインポートタスクを開始する

手順

1. [管理] > [インポート/エクスポート] の順に選択します。
 2. [エクスポート] をクリックします。
 3. ダイアログボックスが表示されたら、[保存] をクリックしてコンピュータに保存します。
 4. [インポート/エクスポート] 画面に戻るには、[戻る] をクリックします。
-

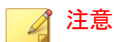
設定ファイルをインポートする

インポート中には次のことを行わないでください。

- ・ その他の管理コンソール画面にアクセスしたり、設定を変更したりする
- ・ データベースの操作を行う
- ・ InterScan MSS サービスを開始または停止する
- ・ EUQ データベースを InterScan MSS に登録する、または InterScan MSS から登録解除する
- ・ 他のエクスポートタスクまたはインポートタスクを開始する

手順

1. InterScan MSS 管理コンソールにログオンします。
2. [システムステータス] タブをクリックします。
3. 開始中または停止中のサービスがないことを確認します。開始中または停止中のサービスがある場合、その動作が終了するまで待機します。
4. [管理] > [インポート/エクスポート] の順に選択します。
5. [設定ファイルのインポート] で [参照] をクリックし、ファイルを検索します。

**注意**

InterScan MSS Linux 版の設定をインポートする際、インポートする設定ファイルは、現在のビルド番号以前の InterScan MSS Linux 版のビルド番号のものである必要があります。

6. [インポート] をクリックします。

ドメインベースの配信設定などの元の InterScan MSS 設定およびルールは削除され、インポートした設定およびルールと置き換えられます。

**注意**

移行後またはアップグレード後、エンドユーザメール隔離機能は無効になります。この機能を使用するには、設定ファイルのインポート後に手動で有効にします。詳細については、[439 ページの「エンドユーザメール隔離を有効にする」](#)を参照してください。

InterScan MSS をバックアップする

InterScan MSS をインストールして必要な設定を行った後、常に設定内容のバックアップを作成しておく、システム障害時にすばやく InterScan MSS を復元できます。

次のように、全体または最小限の InterScan MSS のバックアップを実行できます。

- ・ 全体 — /opt/trend に格納されたすべての InterScan MSS のローカル設定やバイナリファイル、および /var/imss に格納されたデータベース関連ファイルをバックアップします。
- ・ 最小限 — /opt/trend/imss/config に格納された InterScan MSS の設定のみをバックアップします。

**注意**

1. 本書で説明するバックアップおよび復元の手順は、InterScan MSS のオールインワン配置の場合を対象としています。分散配置の場合にバックアップが必要な内容は、次のとおりです。
 - a. データベースがインストールされたコンピュータ上のデータベースファイルまたはテーブル。
 - b. InterScan MSS コンポーネントがインストールされた各コンピュータ上のローカルのバイナリファイルおよび設定ファイル。
2. 最小限のバックアップを実行する際、InterScan MSS の復元後に、以前の HotFix、Patch、または Service Pack のインストールが必要になる場合があります。

全体のバックアップを実行する

手順

1. すべての InterScan MSS 関連プロセスを停止します。

```
/opt/trend/imss/script/imssstop.sh stop
```
2. Postfix を停止します。
3. /opt/trend/および/var/imss/フォルダのバックアップを作成します。
4. /etc/postfix にあるすべての Postfix 設定ファイルのバックアップを作成します。

main.cf、master.cf、allowAccessList、denyAccessList などです。
5. Postfix を起動します。
6. すべての InterScan MSS 関連プロセスを起動します。

```
/opt/trend/imss/script/imssstart.sh
```

最小限のバックアップを実行する

手順

1. すべての InterScan MSS 関連プロセスを停止します。
詳細については、[429 ページの「全体のバックアップを実行する」](#)を参照してください。
 2. Postfix を停止します。
 3. /opt/trend/imss/config フォルダのバックアップを作成します。
 4. /etc/postfix フォルダのバックアップを作成します。
 5. すべてのデータベーステーブルのバックアップを作成します。
 6. Postfix を起動します。
 7. すべての InterScan MSS 関連プロセスを起動します。
詳細については、[429 ページの「全体のバックアップを実行する」](#)を参照してください。
-

InterScan MSS を復元する

システム障害に備えて事前に作成した全体または最小限のバックアップに従って、InterScan MSS を復元できます。

全体の復元を実行する

手順

1. 1 台のコンピュータに InterScan MSS サーバを新規インストールし、IP アドレス、データベースユーザ名、およびパスワードは元のものと同じにします。

2. すべての InterScan MSS 関連プロセスを停止します。詳細については、[429 ページの「全体のバックアップを実行する」](#)を参照してください。
 3. Postfix を停止します。
 4. 以前のバックアップを使用して、/var/imss/フォルダおよび/opt/trend/フォルダを復元します。
 5. Postfix 設定ファイルを復元します。
 6. Postfix を起動します。
 7. すべての InterScan MSS 関連プロセスを起動します。詳細については、[429 ページの「全体のバックアップを実行する」](#)を参照してください。
-

最小限の復元を実行する

手順

1. 1 台のコンピュータに InterScan MSS サーバを新規インストールし、IP アドレス、データベースユーザ名、およびパスワードは元のものと同じにします。
 2. すべての InterScan MSS 関連プロセスを停止します。詳細については、[429 ページの「全体のバックアップを実行する」](#)を参照してください。
 3. Postfix を停止します。
 4. 以前のバックアップを使用して、/opt/trend/imss/config/フォルダを復元します。
 5. Postfix 設定ファイルを復元します。
 6. 以前のデータベーステーブルのバックアップを、新しいデータベースにインポートします。
 7. すべての InterScan MSS 関連プロセスを起動します。詳細については、[429 ページの「全体のバックアップを実行する」](#)を参照してください。
-

設定を複製する

同じ管理データベースを共有しない複数の InterScan MSS 検索サービスを配置した場合は、Control Manager を使用すると、各検索サービスを個別に設定しなくても、検索サービス全体に設定を複製できます。検索サービスが同じ管理データベースを共有している場合は、設定を複製する必要はありません。

Control Manager を使用して設定を複製する場合は、次の手順に従ってください。

- ・ 手順 1: InterScan MSS 設定のバックアップを作成します。
- ・ 手順 2: MCP エージェントを有効にします。
- ・ 手順 3: Control Manager 管理コンソールから設定を複製します。

MCP エージェントを有効にする

InterScan MSS のインストール時に Trend Micro Management Communication Protocol (MCP) エージェントが自動的にインストールされます。Control Manager と統合するには、管理コンソールから Control Manager サーバの情報を設定し、エージェントを有効にします。

手順

1. [管理] > [InterScan MSS の設定] > [接続] の順に選択します。
初期設定で [コンポーネント] タブが表示されます。
2. [Control Manager サーバ] タブをクリックします。

[Control Manager サーバの設定] 画面が表示されます。

3. 必要な情報を指定します。
4. [MCP エージェントを有効にする] チェックボックスをオンにします。
5. [保存] をクリックします。

Control Manager から設定を複製する

InterScan MSS 管理コンソールから MCP エージェントを有効にした後、Control Manager 管理コンソールにログオンして、InterScan MSS 設定の複製を開始します。

手順

1. Control Manager メニューから [製品] を選択します。

[製品ディレクトリ] 画面が表示されます。

2. [製品ディレクトリ] ツリーから、複製元の InterScan MSS 検索サービスを探します。
 3. [設定] にマウスを合わせます。
ドロップダウンリストが表示されます。
 4. ドロップダウンリストから [設定の複製] を選択します。
 5. 対象サーバの横のチェックボックスをオンにします。
 6. [複製] ボタンをクリックします。
-

デバッグログをエクスポートする

トラブルシューティングの目的でデバッグログを分析する必要がある場合は、上位デバイスと上位デバイスに登録されているすべてのデバイスのデバッグログを最大過去 2 日分エクスポートできます。



注意

デバッグログはパスワードで保護された Zip ファイル内にあります。このファイルの初期設定のパスワードは **trend** です。

手順

1. [管理] > [インポート/エクスポート] の順に選択します。
2. [デバッグログのエクスポート] タブをクリックします。
3. [検索サービス] でデバイスを選択します。
4. 何日分エクスポートするかを選択します。
5. [エクスポート] をクリックします。

ログファイルの合計サイズに応じて、このプロセスには 10 分から 1 時間以上かかることがあります。

**注意**

imss.ini ファイル内のデバッグログのパスを変更する場合は、新しいログのパスを /opt/sharon/imss/cdt/ExInterface の ExInterface_IMSS.ini ファイルにも追加してください。これにより、InterScan MSS で新しいパスからデバッグログを収集できるようになります。

第 28 章

エンドユーザメール隔離

この章では、エンドユーザメール隔離の使用方法について説明します。

この章の内容は次のとおりです。

- ・ 438 ページの「エンドユーザメール隔離について」
- ・ 438 ページの「EUQ 認証」
- ・ 439 ページの「エンドユーザメール隔離を設定する」
- ・ 450 ページの「配布リスト EUQ の管理」
- ・ 452 ページの「エンドユーザメール隔離を無効にする」
- ・ 453 ページの「EUQ データベースを管理する」

エンドユーザメール隔離について

InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) には、スパムメール管理を強化するための Web ベースのエンドユーザメール隔離が用意されています。Web ベースのエンドユーザメール隔離サービスを使用すると、エンドユーザは各自の個人アカウントのスパムメールの隔離方法を管理できます。スパムメールと判定されたメッセージは隔離されます。これらのメッセージは、エンドユーザメール隔離エージェントによってデータベース内でインデックスが付けられるため、エンドユーザはメッセージを再確認して、削除したり、配信を許可したりできるようになります。

メッセージを隔離状態に置く期間を指定できます。隔離を解除されないメッセージは、自動的に削除されます。削除されたメッセージは復元できません。

EUQ 認証

エンドユーザメール隔離を有効にするには、次の認証方法のいずれかが必要です。

- ・ LDAP 認証: エンドユーザメール隔離を有効にする前に、次のいずれかの方法を使用して LDAP を設定します。
 - ・ [管理] > [InterScan MSS の設定] > [接続] の順に選択し、[LDAP] タブをクリックします。
 - ・ [管理] > [InterScan MSS の設定] > [設定ウィザード] の順に選択します。詳細については、[60 ページの「LDAP を設定する」](#)を参照してください。
- ・ SMTP 認証: [エンドユーザメール隔離] 画面で「EUQ 認証に SMTP サーバを使用する」を有効化する際に、受信者ドメインとサーバアドレスを指定します。

エンドユーザメール隔離を設定する

InterScan MSS で誤ってスパムメールと検出された可能性のある隔離されたスパムメールアイテムに、エンドユーザがアクセスできるようにするには、次の手順を実行します。

1. [439 ページの「エンドユーザメール隔離を有効にする」](#)
2. [441 ページの「SMTP サーバを設定する」](#)
3. [443 ページの「エンドユーザメール隔離管理コンソールを開始または停止する」](#)
4. [445 ページの「エンドユーザアクセスを有効にする」](#)
5. [449 ページの「エンドユーザメール隔離の管理コンソールをリモートで開く」](#)

エンドユーザメール隔離を有効にする

エンドユーザメール隔離を有効にするには、次の認証方法のいずれかが必要です。

- ・ LDAP
- ・ SMTP

EUQ 認証の詳細については、[438 ページの「EUQ 認証」](#)を参照してください。

手順

1. [管理] > [エンドユーザメール隔離] の順に選択します。
[エンドユーザメール隔離管理] タブが表示されます。
2. [エンドユーザメール隔離を有効にする] を選択します。
3. 認証方法を選択します。

- ・ EUQ 認証に LDAP を使用する: LDAP が設定されていない場合、このオプションは無効になっています。LDAP が設定されている場合は、これが初期設定の認証方法となります。
- ・ EUQ 認証に SMTP サーバを使用する: 選択すると、SMTP の設定セクションが表示されます。受信者のドメインとサーバアドレスを指定してください。詳細については、[441 ページの「SMTP サーバを設定する」](#)を参照してください。

エンドユーザメール隔離



エンドユーザメール隔離管理

EUQ機能を有効にする

☒ エンドユーザメール隔離を有効にする
 保存

☒ EUQ認証にLDAPを使用する

☐ EUQ認証にSMTPサーバを使用する

EUQデータの削除

メッセージと承認済み送信者を含むすべてのデータをすべてのEUQサービスから削除します。
 削除

EUQデータの再配布

EUQデータをすべてのサーバに再配布して、パフォーマンスを高めます。

☐ 承認済み送信者リストのみを再配布

☒ すべて (承認済み送信者リストとスパムメール情報)を再配布
 再配布

(下位IMSVAデバイスでEUQサーバを起動または停止した後、あるいはEUQサーバに新しい下位IMSVAデバイスを追加した後に、EUQデータを再配布してください)。

注意: 複数の下位デバイスを追加したり、複数のEUQサーバを開始または停止したりする場合は、デバイスやEUQサーバごとに個別に[再配布]ボタンをクリックする必要はありません。追加をすべて終えてから、またはすべてのEUQサーバを開始/停止してから、[再配布]を一度だけクリックしてください。

4. [保存] をクリックします。

エンドユーザメール隔離サービスは自動的に開始します。



注意

設定は自動的に保存されません。情報が失われないよう、[保存] をクリックしてからページを移動してください。

エンドユーザメール隔離サービスは自動的に開始します。エンドユーザメール隔離管理コンソールを手動で起動する方法については、[443 ページの「エン](#)

「ドユーザメール隔離管理コンソールを開始または停止する」を参照してください。

SMTP サーバを設定する

手順

1. [管理] > [エンドユーザメール隔離] の順に選択します。
[エンドユーザメール隔離管理] タブが表示されます。
2. [EUQ 認証に SMTP サーバを使用する] を選択します。
SMTP の設定セクションが表示されます。

エンドユーザメール隔離

The screenshot shows the 'End User Mail Isolation Management' console. At the top, there's a tab labeled 'エンドユーザメール隔離管理'. Below it, a section titled 'EUQ機能を有効にする' (Enable EUQ function) contains a checked checkbox for 'エンドユーザメール隔離を有効にする' (Enable end user mail isolation) and a '保存' (Save) button. Two radio buttons are present: 'EUQ認証にLDAPを使用する' (Use LDAP for EUQ authentication) and 'EUQ認証にSMTPサーバを使用する' (Use SMTP server for EUQ authentication), with the latter being selected. Below the radio buttons, a text prompt says '受信者のドメインとSMTPサーバアドレスを指定してください。' (Please specify the recipient's domain and SMTP server address). A table with two columns, 'ドメイン' (Domain) and 'サーバ/ポート番号' (Server/Port number), is shown with a '追加' (Add) button and a '削除' (Delete) button. The table currently has 0 rows. A pagination bar at the bottom indicates '0-0 / 0' rows and 'ページ 1' (Page 1) with a '15件/ページ' (15 items per page) dropdown.

3. [追加] をクリックします。

[SMTP サーバの設定] 画面が表示されます。

メールドメイン

隔離管理で使用するドメインを指定してください。

ドメイン: ⓘ

サーバアドレスとポート番号

ドメインの認証で使用するSMTPサーバアドレスとポート番号を指定してください。

サーバアドレス ポート番号

:

OK 閉じる

4. 次の情報を指定します。

- ・ メールドメイン: エンドユーザメール隔離コンソールへのアクセスに使用するドメインを示します。InterScan MSS は、受信者のドメインを使用して、認証に使用される SMTP サーバを判別します。



注意

ドメインは次の形式で指定できます。

- ・ example.com
- ・ *.example.com: example.com の任意のサブドメイン
- ・ *: 任意のドメイン

リストできるドメインは1つだけです。一意のドメインのみがリストに追加されます。

- ・ サーバアドレスとポート番号: 宛先ドメインにサーバアドレスを割り当てるために使用するサーバアドレスとポートを示します。

**注意**

初期設定のポート 25 を使用するか、別のポートを指定します。

1 つのドメインに割り当てることができるのは 1 つの SMTP サーバのみです。ただし、複数のドメインを 1 つの SMTP サーバにマップすることは可能です。

5. [OK] をクリックします。

情報が SMTP の設定表に表示されます。

エンドユーザメール隔離管理コンソールを開始または停止する

エンドユーザメール隔離管理コンソールを手動で開始または停止できます。

手順

1. [システムステータス] に移動します。
[システムステータス] 画面が表示されます。

[管理下のサービス] テーブルで [EUQ 管理コンソール] に緑のチェックマークが表示され、エンドユーザメール隔離管理コンソールが有効であることが示されます。

システムステータス



接続の有効化

☒ SMTP接続を許可する
 ☐ POP3接続を許可する
 保存

コンポーネント

前回の表示更新: 表示更新

アップデート ロールバック

☐ 名前	現在のバージョン	利用可能なバージョン	アップデートスケジュール
☐ ウィルス検索エンジン	9.950.1006		15 分
☐ 高度な脅威検索エンジン	10.300.1010		15 分
☐ ウィルスパターンファイル	13.821.00		15 分
☐ スパイウェアパターンファイル	1.897.00		15 分
☐ IntelliTrapパターンファイル	0.235.00		15 分
☐ IntelliTrap除外パターンファイル	1.457.00		15 分
☐ スпамメール検索エンジン	8.100.1062		15 分
☐ スпамメール対策パターンファイル	23510.004		15 分
☐ URLフィルタエンジン	3.910.1008		15 分
☐ スマートスキャンエージェントパターンファイル	13.821.00		15 分

管理下のサービス

ホスト名	接続	検索サービス	ポリシーサービス	EUQ管理コンソール
localhost.localdomain	☒	☒ 停止	☒ 停止	☒ 停止

- [停止] をクリックします。
しばらくすると、エンドユーザメール隔離管理コンソールが停止します。
- [EUQ 管理コンソール] の [開始] をクリックします。
しばらくすると、エンドユーザメール隔離管理コンソールが開始します。

エンドユーザアクセスを有効にする

エンドユーザアクセスを有効にすると、InterScan MSS で誤ってスパムメールと判定されて隔離されたスパムメールアイテムにユーザがアクセスできます。クライアントは、LDAP 認証または SMTP 認証を使用して InterScan MSS のエンドユーザメール隔離サービスにアクセスします。



注意

ユーザがエンドユーザメール隔離管理コンソール上のメッセージを管理できるようにするには、ユーザの個々のメールアドレスおよび配布リストアドレスを LDAP サーバ上のユーザのリストに追加します。

SMTP 認証を使用している場合、LDAP を設定する必要はありません。

手順

1. [管理] > [エンドユーザメール隔離] の順に選択します。
[エンドユーザメール隔離管理] タブが表示されます。
2. [ユーザメール隔離アクセス] タブをクリックします。

[ユーザメール隔離アクセス] 画面が表示されます。表示される画面は、有効化プロセスで選択した認証方法によって異なります。

エンドユーザメール隔離



隔離されたスパムメールにアクセス可能なグループを指定します。これらのグループは、IMSS サーバに対してLDAP認証を使用します。

エンドユーザメール隔離管理

ユーザメール隔離アクセス

☒ エンドユーザアクセスを有効にする ⓘ
☐ 配布リストEUQの管理を有効にする ⓘ
☐ エンドユーザがEUQで隔離されたメールを直接配信することを許可する ⓘ
☒ エンドユーザがメッセージを再処理するときに、承認済み送信者の動作を「自動追加」するかどうかを指定する ⓘ

常に追加する ▼

隔離されたスパムメールの保存日数: 7日 ▼

シングルサインオン設定
☐ NTLMを有効にする ⓘ
☐ Kerberosを有効にする ⓘ
 keytab 参照... アップロード

承認済み送信者の最大数の設定
 エンドユーザ1人あたりの承認済み送信者の最大数: 50 ▼

ログオン通知の指定
 エンドユーザメール隔離のログオンページに表示するメッセージを指定してください。2,000文字まで指定できます。セキュリティ上の理由から、HTMLは使用しないことをお勧めします。管理者向けのログオン通知を設定するには、[ログオン通知] ページを参照してください。

↑

↓

アクセスを有効にするLDAPグループの選択
☒ すべて有効にする
 以下のLDAP検索でグループを選択します。

LDAPグループの検索 ▼

>>

<<

選択したグループ

図 28-1. LDAP 認証

446

3. [エンドユーザアクセスを有効にする] を選択します。
4. [配布リスト EUQ の管理を有効にする] をオンにすると、ユーザは自分が所属する配布リストの EUQ を管理できます。
5. [エンドユーザが EUQ で隔離されたメールを直接配信することを許可する] をオンにすると、隔離されたメッセージをエンドユーザが受信者に直接配信できます。このメッセージでは、ウイルス検索ルール以外のすべてのルールが省略されます。
6. [エンドユーザがメッセージを再処理するときに、承認済み送信者の動作を「自動追加」するかどうかを指定する] をオンにして、ドロップダウンリストから値を選択します。
7. [NTLM を有効にする] をオンにすると、エンドユーザは NTLM 認証プロトコルを使用してエンドユーザメール隔離管理コンソールにシングルサインオンでアクセスできます。
8. Kerberos シングルサインオンを有効にするには、次の手順を実行します。
 - a. [Kerberos を有効にする] をオンにすると、エンドユーザは Kerberos 認証プロトコルを使用してエンドユーザメール隔離管理コンソールにシングルサインオンでアクセスできます。
 - b. InterScan MSS がインストールされているホストのドメインに新しいユーザアカウントを作成します。
 - c. Active Directory ドメインコントローラで、次のコマンドを使用して InterScan MSS 用のキータブファイルを生成します。

```
C:\>ktpass.exe -out filename -princ HTTP/instance@REALM  
-mapuser account -ptype KRB5_NT_PRINCIPAL -pass password
```

各要素の説明は次のとおりです。

filename は、生成されるキータブファイルの保存場所を示します。たとえば、C:\test.keytab のように指定します。

instance は、InterScan MSS がインストールされているコンピュータのホスト名を示します。たとえば、imss.test.com のように指定します。

REALM は、認証に使用するレルムの大文字表記名で、一般に DNS サーバのドメイン名と同じになります。たとえば、TEST.COM のように指定します。

account は、InterScan MSS 用に作成されたアカウントを示します。たとえば、user@test.com のように指定します。

password は、アカウントのパスワードを示します。

- d. [参照] をクリックして、生成されたキータブファイルの場所を探します。
- e. [アップロード] をクリックして、キータブファイルを InterScan MSS にアップロードします。

ktpass.exe が見つからない場合は、Windows Server のインストール CD/DVD を使用してサポートツールをインストールするか、Microsoft の Web サイトからファイルをダウンロードできます。

Kerberos シングルサインオンが有効な場合、エンドユーザメール隔離管理コンソールにアクセスするには InterScan MSS のホスト名を使用します。

- 9. 隔離されたスパムメールを保存する日数を選択します。
- 10. エンドユーザごとの承認済み送信者の最大数を選択します。
- 11. ユーザが隔離されたメッセージへのアクセスを開始した際に、ユーザのブラウザに表示されるログオン画面メッセージを指定します。
- 12. 隔離されたスパムメールに LDAP グループのすべてのユーザがアクセスできるようにするには、[アクセスを有効にする LDAP グループの選択] で、[すべて有効にする] の横のチェックボックスをオンにします。
- 13. 個別の LDAP グループを追加するには、[すべて有効にする] チェックボックスをオフにして次のいずれかを実行します。
 - ・ グループを検索する場合
 - a. ドロップダウンリストから、[LDAP グループの検索] を選択します。
 - b. グループ名を指定します。

- c. [検索] をクリックします。下の表にグループが表示されます。
 - d. LDAP グループをクリックして追加します。
 - e. [>>] をクリックします。クリックしたグループが [選択したグループ] 表に表示されます。
 - ・ 既存のグループを参照する場合
 - a. ドロップダウンリストから、[LDAP グループの参照] を選択します。下の表にグループが表示されます。
 - b. LDAP グループをクリックして追加します。
 - c. [>>] をクリックします。クリックしたグループが [選択したグループ] 表に表示されます。
14. [保存] をクリックします。
-

エンドユーザメール隔離の管理コンソールをリモートで開く

ネットワークを経由したリモート操作で、またはプログラムが配置されているコンピュータから、エンドユーザメール隔離管理コンソールを表示できます。ブラウザで JavaScript が有効になっていることを確認してください。

プライマリエンドユーザメール隔離サービス

`https://<ターゲットサーバの IP アドレス>:8447`

IP アドレスを使用する代わりに、サーバの完全修飾ドメイン名 (FQDN) を使用することもできます。

ログオン名形式

エンドユーザメール隔離管理コンソールにアクセスするときに使用するログオン名の形式は、選択した認証タイプによって異なります。

表 28-1. エンドユーザメール隔離ログオン名の形式

認証タイプ	ログオン名形式
LDAP	ログオン名の形式は、LDAP を設定したときに選択した LDAP サーバの種類によって異なります。以下に有効なログオン名形式の例を示します。 ・ Domino: user1/domain ・ Microsoft Active Directory ・ Kerberos を使用しない場合: user1@domain.com (UPN) または domain\user1 ・ Kerberos を使用する場合: user1@domain.com ・ Microsoft Active Directory グローバルカタログ ・ Kerberos を使用しない場合: user1@domain.com (UPN) または domain\user1 ・ Kerberos を使用する場合: user1@domain.com ・ OpenLDAP: cn=manager, dc=test1, dc=com ・ Sun iPlanet Directory: uid=user1, ou=people, dc=domain, dc=com
SMTP	ログオン名として有効なメールアドレスを使用します。  注意 InterScan MSS では、auth login、auth plain、および starttls がサポートされます。

配布リスト EUQ の管理

InterScan MSS では、ユーザは自分が所属する配布リストの EUQ を管理できます。



注意

LDAP 認証を使用している場合のみ、配布リスト EUQ の管理を有効にできます。

この機能は次の LDAP サーバタイプをサポートします。

- ・ Domino
- ・ Microsoft Active Directory
- ・ Microsoft Active Directory グローバルカタログ

ユーザが管理権限を要求すると、配布リストアドレスに通知が送信されます。この通知には、次の情報が含まれます。

- ・ 要求したユーザのアドレス
- ・ 配布リストアドレス
- ・ 一意のワンタイム認証コード
- ・ 認証コードの有効期限



注意

初期設定では認証コードは 5 分後に期限切れになります。新しい有効期限を指定するには、`imss.ini` ファイルに次のセクションを追加します。

```
[EUQ]
expired_interval=5
```

一度に 1 人のユーザのみが EUQ を管理できます。別のユーザが次のことを実行する場合に、InterScan MSS は現在のユーザを強制的にログオフします。

- ・ 管理権限を要求する。
- ・ 現在のユーザを強制的にログオフするよう選択する。

配布リスト EUQ を管理する

配布リスト EUQ を利用するために、ユーザに次の手順を実施するよう指示します。

**注意**

[配布リスト EUQ の管理] リンクは、管理者がこの機能を有効にしている場合にのみ表示されます。

手順

1. 個人用のメール隔離にログオンします。
 2. [配布リスト EUQ の管理] をクリックします。
新しい画面が表示されます。
 3. 配布リストのメールアドレスを指定します。
 4. [次へ] をクリックします。
新しい画面が表示され、通知が配布リストへ送信されます。
 5. 通知に記載された認証コードを指定します。
認証コードの使用条件は次のとおりです。
 - ・ 要求したユーザのみ
 - ・ 1 回限り
 - ・ 指定された有効期限前のみ
 6. [ログオン] をクリックします。
-

エンドユーザメール隔離を無効にする

エンドユーザメール隔離を無効にする前に、隔離されたスパムメールを管理するようにユーザに通知します。

手順

1. [管理] > [エンドユーザメール隔離] の順に選択します。
[エンドユーザメール隔離管理] 画面が表示されます。

2. [エンドユーザメール隔離を有効にする] チェックボックスをオフにします。
3. (オプション) 各デバイスからすべてのエンドユーザメール隔離のデータを削除して、ディスク領域を節約します。データを削除するには、[エンドユーザメール隔離管理] タブで [削除] をクリックします。
4. [保存] をクリックします。

EUQ データベースを管理する

EUQ データベースは初期設定で InterScan MSS サーバ上にインストールされます。初期設定の EUQ データベース名は `imsseuq`、ユーザ名は `sa`、パスワードは `postgresql` です。

EUQ データベースは必要に応じて登録、アタッチ、無効化、およびデタッチすることができます。

手順

1. [管理] > [InterScan MSS の設定] > [接続] の順に選択します。
初期設定では [コンポーネント] タブが表示されます。
2. [データベース] タブをクリックします。

接続

コンポーネント LDAP POP3 **データベース** Control Manager サーバ NTP 設定 下位 IP アドレス

IMSVA データベース

データベースのタイプ:	PostgreSQL
サーバ:	127.0.0.1
ポート:	5432
ユーザ名:	sa
データベース名:	ims

EUQ データベース

登録 アタッチ デタッチ

☐	サーバ	データベース名	ユーザ名	ステータス
☐		imsseuq	sa	

注意: サーバのステータスを変更したり新しいデータベースを追加したりするなど EUQ データベースの設定を変更した場合は、変更後、EUQ データを再配布してください。

3. EUQ データベースを InterScan MSS に登録するには、[EUQ データベース] の下の [登録] をクリックします。EUQ データベースサーバの IP アドレス、ポート番号、管理者のユーザ名、パスワード、およびデータベース名を入力します。

**注意**

EUQ データベースの登録およびアタッチに使用する管理者アカウントには、スーパーユーザの役割が必要です。

4. EUQ データベースをアタッチするには、[アタッチ] をクリックします。EUQ データベースサーバの IP アドレス、ポート番号、管理者のユーザ名、パスワード、およびデータベース名を入力します。

**注意**

アタッチ機能を使用して、デタッチされたデータベースを復元できます。アタッチするデータベースに初期化されたスキーマがあることを確認してください。

5. EUQ データベースを InterScan MSS からデタッチするには、データベースを無効にし、データベースの横のチェックボックスをオンにして、[デタッチ] をクリックします。

**注意**

デタッチ機能により、EUQ データベースリストからデータベースが削除されます。これにより EUQ データベースが停止します。

データベースは必要に応じて再度アタッチできます。データベースをデタッチしても、実際のデータベースサーバが削除されたり何らかの影響を受けたりすることはありません。InterScan MSS でそのデータベースが使用されなくなるだけです。

6. EUQ データベースを無効にするには、[ステータス] 列でそのデータベースの緑のチェックマークをクリックします。

**注意**

無効化機能を使用して、EUQ データベースを一時的に停止できます。たとえば、特定の期間メンテナンスのために EUQ データベースを停止できます。

次に進む前に

グループ内の複数のエンドユーザメール隔離に対応したデバイスにデータを再配布すると、エンドユーザメール隔離のパフォーマンスが向上します。データは次のタイミングで再配布してください。

- ・ データベースを登録、アタッチ、または無効化した後
- ・ コマンドラインインタフェースを使用してエンドユーザメール隔離対応のデバイスを削除する前



ヒント

エンドユーザメール隔離データの再配布後は、以下を実行することをお勧めします。

- ・ 新たに追加した承認済み送信者が引き続き使用可能であることを確認します。
 - ・ 管理者が下位デバイスを追加したりエンドユーザメール隔離データを再配布している間は、承認済み送信者をリストに追加しないようにエンドユーザに指示します。
-

第 29 章

管理タスク

この章では、アカウントの管理、接続の設定、製品ライセンスの管理などの重要な管理タスクを実行する方法について説明します。

この章の内容は次のとおりです。

- ・ 458 ページの「管理者アカウントを管理する」
- ・ 462 ページの「接続を設定する」
- ・ 475 ページの「データベースのメンテナンススケジュールを設定する」
- ・ 476 ページの「製品ライセンスを管理する」
- ・ 480 ページの「製品のアクティベーションを実行する」
- ・ 482 ページの「Smart Protection Network を設定する」

管理者アカウントを管理する

InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) の管理上のボトルネックを軽減するために、新しい管理者アカウントを作成して、管理作業を他のスタッフに委任できます。委任管理者アカウントを作成したら、そのアカウントに管理コンソールのさまざまな領域への権限を割り当てます。初期設定の「admin」アカウントは、InterScan MSS のすべての機能にアクセスする権限を持ちます。

管理者アカウントを追加する

作成したアカウントには、InterScan MSS の機能に対して次の 3 つの権限を設定できます。

- ・ 表示/変更: メニュー項目に含まれるすべての機能と設定にアクセスできます。
- ・ 表示: メニュー項目に含まれる機能と設定を表示できますが、それらを変更することはできません。
- ・ 権限なし: メニュー項目が表示されないため、その設定を表示することも指定することもできません。

手順

1. [管理] > [管理者アカウント] の順に選択します。
[管理者アカウント] 画面が表示されます。
2. [追加] をクリックします。

[管理者のアカウントの追加] 画面が開き、[認証] タブが表示されます。

管理者のアカウントの追加



認証 権限

☒ アカウントを有効にする

認証:

☒ InterScan MSS認証

ユーザ名:

新しいパスワード:

パスワードの確認:

注意: パスワードには4~32文字を使用できます。

☐ LDAP認証

LDAPユーザ名:

保存 キャンセル

3. 認証の設定を次のように指定します。
 - a. [アカウントを有効にする] を選択します。
 - b. 次の認証タイプを選択します。
 - ・ InterScan MSS 認証: ユーザ名、新しいパスワードと確認のパスワードを指定します。
 - ・ LDAP 認証: LDAP のユーザ名を指定します。
4. [権限] タブをクリックします。

[権限] 画面が表示されます。

管理者のアカウントの追加



認証		権限		
アクセス領域	表示/変更	表示	権限なし	
ダッシュボードとシステムステータス	☐	☐	☒	
クラウドプレフィルタ	☐	☐	☒	
ポリシー	☐	☐	☒	
送信者フィルタ	☐	☐	☒	
レポート	☐	☐	☒	
ログ	☐	☐	☒	
メール領域とキュー	☐	☐	☒	
管理	☐	☐	☒	

5. 権限の設定を次のように指定します。
 - a. InterScan MSS 管理コンソールメニューに表示される次のアクセス領域のそれぞれに、[表示/変更]、[表示]、または [権限なし] のいずれかを選択します。
 - ・ ダッシュボードとシステムステータス
 - ・ クラウドプレフィルタ
 - ・ ポリシー
 - ・ 送信者フィルタ
 - ・ レポート
 - ・ ログ
 - ・ メール領域とキュー
 - ・ 管理
 - b. [保存] をクリックします。

**注意**

初期設定の InterScan MSS 管理者アカウントだけが、新しい管理者アカウントを追加できます。委任管理者アカウントでは、管理領域へのフル権限を割り当てられていても、新規管理者アカウントを追加できません。

フル権限を与えられた委任管理者アカウントでは、各自の InterScan MSS パスワードの変更のみが可能です。初期設定の管理者アカウントのパスワードを忘れた場合、トレンドマイクロのテクニカルサポートに連絡してパスワードのリセットを依頼してください。

管理者アカウントを編集する

ロールが変更になった場合やその他の組織変更があった場合は、委任管理者アカウントの権限を変更できます。

手順

1. [管理] > [管理者アカウント] の順に選択します。
[管理者アカウント] 画面が表示されます。
2. アカウント名のハイパーリンクをクリックします。
3. 必要な変更を実行します。
4. [保存] をクリックします。

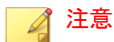
管理者アカウントを削除する

ロールが変更になった場合やその他の組織変更があった場合は、委任管理者アカウントの権限を削除できます。

手順

1. 削除するアカウントのチェックボックスをオンにします。
2. [削除] をクリックします。

3. 確認メッセージで、[OK] をクリックします。

**注意**

削除できるのは委任管理者アカウントのみで、初期設定の InterScan MSS 管理者アカウントは削除できません。

接続を設定する

検索サービスを有効にしてメッセージを受信し、ルールの検索の実行時にポリシーサービスのパフォーマンスを向上させるには、接続設定を実行してください。

手順

1. [管理] > [InterScan MSS の設定] > [接続] の順に選択します。

初期設定で [コンポーネント] タブが表示されます。

接続

コンポーネント		LDAP	POP3	データベース	Control Managerサーバ
すべての検索サービスの設定					
IMSS マネージャポート:		15506			
すべてのポリシーサービスの設定					
ポリシーサービスポート:		5060			
プロトコル:		HTTP ▼			
キープアライブ:		☐ 有効			
バックログされる要求数の上限:		100			
保存		キャンセル			

2. [すべての検索サービスの設定] で、InterScan MSS が検索サービスと通信するために使用するポート番号を指定します。

**注意**

ユーザがポート番号を設定していないか、ファイアウォールでこのポートを開けなかった場合、[システムステータス] ページで管理下のサーバは切断と表示されます。さらに、管理下のサービスに対して行った変更は有効になりません。

3. [すべてのポリシーサービスの設定] で、次の項目を設定します。
 - ・ ポリシーサービスポート: InterScan MSS がポリシーサービスとの通信に使用するポート番号を指定します。ポリシーサービスが InterScan MSS との通信に使用する初期設定のポート番号は 5060 です。
 - ・ プロトコル: 検索サービスがポリシーサービスとの通信に使用するプロトコルの種類として [HTTP] または [HTTPS] を選択します。
 - ・ キープアライブ: このチェックボックスをオンにすると、検索サービスとポリシーサービス間の常時アクティブな接続が維持されるためポリシー検索が強化されます。
 - ・ バックログされる要求数の上限: InterScan MSS が後で処理できるまで保持する要求の最大数を指定します。
4. [保存] をクリックします。

LDAP 設定について

ユーザグループ定義、管理者アカウント、またはエンドユーザメール隔離の認証に LDAP を使用する場合は、LDAP 情報を入力します。

[管理] > [接続] > [LDAP] 画面で LDAP 設定が指定されていない場合、次の LDAP 関連の項目は機能しません。

- ・ [ポリシー] > [内部アドレス] > (LDAP グループの検索)
- ・ [ポリシー] > (任意のルール) > [送信者から受信者] > (LDAP ユーザおよびグループの検索)
- ・ [管理] > [エンドユーザメール隔離] > [ユーザ隔離アクセス] > (アクセスを有効にする LDAP グループの選択)

- ・ [管理] > [管理者アカウント] > [追加] > (LDAP 認証)

LDAP サーバの種類

表 29-1. LDAP サーバの種類

LDAP サーバ	LDAP 管理者アカウント (例)	基本識別名 (例)	認証方法
Active Directory	Kerberos を使用しない場合: user1@domain.com (UPN) または domain\user1 Kerberos を使用する場合: user1@domain.com	dc=domain, dc=com	簡易 詳細 (Kerberos 使用)
Active Directory グローバルカタログ	Kerberos を使用しない場合: user1@domain.com (UPN) または domain\user1 Kerberos を使用する場合: user1@domain.com	dc=domain, dc=com dc=domain1, dc=com (一意のドメインが複数存在する場合)	簡易 詳細 (Kerberos 使用)
OpenLDAP	cn=manager, dc=test1, dc=com	dc=test1, dc=com	簡易
Lotus Domino	user1/domain	該当なし	簡易
Sun iPlanet Directory	uid=user1, ou=people, dc=domain, dc=com	dc=domain, dc=com	簡易

LDAP を設定する

手順

1. 次のいずれかを選択して、[LDAP] タブにアクセスします。
 - ・ [管理] > [InterScan MSS の設定] > [接続] | [LDAP]
 - ・ [管理] > [InterScan MSS の設定] > [設定ウィザード] | [手順 6: LDAP 設定]
2. [追加] をクリックします。
[LDAP 設定] 画面が表示されます。
3. LDAP サーバのわかりやすい説明を入力します。
4. [LDAP サーバの種類] で、ネットワーク上の LDAP サーバの種類として次のいずれかを選択します。
 - ・ Domino
 - ・ Microsoft Active Directory
 - ・ Microsoft Active Directory グローバルカタログ
 - ・ OpenLDAP
 - ・ Sun iPlanet Directory
5. [有効 LDAP1] のチェックボックスをオンにします。
6. [LDAP サーバ] に、サーバの名前または IP アドレスを指定します。
7. [待機ポート番号] に、LDAP サーバがアクセス要求の待機ポートとして使用するポート番号を指定します。
8. 必要に応じて [有効 LDAP2] の下の項目を設定します。
9. [ポリシーサービスおよび EUQ サービスの LDAP キャッシュ生存期限] で、[キャッシュ生存期限 (分)] を指定します。

キャッシュ生存期限: この値によって LDAP クエリの結果がキャッシュに保持される期間が決まります。長い期間を指定すると、ポリシー実行

中の LDAP クエリ機能が向上します。ただし、LDAP サーバにおける変更に対するポリシーサーバの対応は遅くなります。期間を短くすると、InterScan MSS が LDAP クエリをさらに頻繁に実行する必要があるため、パフォーマンスは低下します。

10. [LDAP 管理者] に、管理者アカウント、対応するパスワードおよび基本識別名を指定します。

詳細については、[464 ページの「LDAP サーバの種類」](#)を参照してください。

11. 次のいずれかの認証方法を選択します。

- ・ 簡易
- ・ 詳細: Active Directory に対して Kerberos 認証を使用します。次の項目を設定します。
 - ・ Kerberos 認証の初期設定のレルム: クライアントの初期設定のレルムを指定します。Windows のドメイン名を大文字で指定する必要があります (Kerberos 認証では大文字と小文字が区別されます)。
 - ・ 初期設定のドメイン: レルムに対応するインターネットドメイン名を指定します。
 - ・ 鍵発行局 (KDC) および管理サーバ: レルムの鍵発行局のホスト名または IP アドレスを指定します。通常はドメインコントローラの情報を指定します。
 - ・ 鍵発行局 (KDC) ポート番号: 発行局に関連付けられたポート番号を指定します。

12. [InterScan MSS と LDAP 間の暗号化通信を有効にする] チェックボックスをオンにし、[参照] をクリックして CA 証明書ファイルをアップロードし、LDAP サーバで使用する証明書を確認します。

13. [追加] をクリックします。

設定ウィザードを使用している場合は、[次へ] をクリックします。

**注意**

Kerberos 認証をサポートするのは、Active Directory と Active Directory グローバルカタログのみです。

14. [LDAP メールアドレス属性] で、InterScan MSS がユーザのメールアドレスを取得する LDAP 属性を選択します。
 - ・ mail: メールアドレスを保持している初期設定の LDAP 属性です。
 - ・ proxyAddresses: Microsoft Exchange Server を使用する場合に推奨される属性です。
 - ・ その他の属性: メールアドレスを保持している LDAP 属性を指定します。
15. [保存して同期] をクリックします。

LDAP サーバを有効/無効にする

ネットワーク要件に従って、LDAP サーバを有効または無効にできます。

手順

1. [管理] > [InterScan MSS の設定] > [接続] > [LDAP] の順に選択し、[LDAP] タブにアクセスします。
2. LDAP サーバ表で、有効または無効にするサーバをクリックします。
[LDAP 設定] 画面が表示されます。
3. [LDAP サーバの種類] で、[有効 LDAP1] と [有効 LDAP2] のチェックボックスをオンまたはオフにして、LDAP サーバを有効または無効にします。

**注意**

LDAP1 と LDAP2 は、互いのバックアップサーバを指します。選択するチェックボックスが 1 つのみの場合、LDAP サーバのステータスは有効ですが、そのバックアップサーバは有効でないことになります。

4. [保存] をクリックします。
-

POP3 の設定をする

SMTP トラフィックの他に、InterScan MSS では、クライアントがメッセージを受信する際に、ゲートウェイで POP3 メッセージも検索できます。



ヒント

POP3 メッセージフィルタを使用するには、[システムステータス] 画面の [POP3 接続を許可する] をオンにします。初期設定ではこのオプションは選択されていません。

手順

1. [管理] > [InterScan MSS の設定] > [接続] の順に選択します。
初期設定では [コンポーネント] タブが表示されます。
2. [POP3] タブをクリックします。
3. インターネット上の任意の POP3 サーバからの接続を設定するには、InterScan MSS が受信 POP3 接続用に使用するポート番号を [一般的な POP3 接続] に指定します。
4. 特定の POP3 サーバからの接続を設定するには、次の手順を実行します。
 - a. [専用の POP3 接続] の下の [追加] をクリックします。
[専用の POP3 接続] 画面が表示されます。
 - b. InterScan MSS が受信 POP3 接続用に使用するポート番号、POP3 サーバの IP アドレス、および POP3 サーバのポート番号を指定します。
 - c. [OK] をクリックします。
 - d. 既存の接続を変更するには、その接続名をクリックします。
5. [メッセージテキスト] で、ユーザが受信しようとしているメッセージがフィルタに一致して隔離または削除された場合に InterScan MSS からユーザに送信されるメッセージを編集します。

6. [保存] をクリックします。

**注意**

InterScan MSS のデーモンが正しく動作するためには、検索サービスの受信ポートが待機状態になっている必要があります。

一般的な POP3 サービスを設定する

一般的な POP3 サービスでは、POP3 クライアントは USER コマンドを使用してログオンし、値を区切るために UserServerSeparator 文字を使用して、ユーザ名、実際の POP3 サーバ、オプションのポート番号を指定します。

例 1: UserServerSeparator 文字「#」を使用して、ユーザ「User1」をサーバ「Server1」に接続する場合、クライアントは次の USER コマンドを発行します。

```
USER User1#Server1
```

例 2: Server1 上のポート 2000 に接続する場合は、次のコマンドが使用されます。

```
USER User1#Server1#2000
```

**注意**

ポート番号を指定しないと、InterScan MSS では初期設定値の 110 を使用します。

次の例では、Outlook で一般的な POP3 を設定する方法を示します。

手順

1. InterScan MSS 検索サービスの IP アドレス「192.168.11.147」で、POP3 サーバアドレスを指定します。
2. ユーザ名「test123#192.168.11.252」を入力します。
3. POP3 ポートを 110 に設定します。

POP3 専用サービスを設定する

専用の POP3 サービスでは、POP3 サービスは常に特定の POP3 サーバに接続されます。InterScan MSS では、このサービスを POP3 ログオン、および AUTH コマンドを使用したすべての種類のログオンに使用します。このサービスについては、クライアントの接続先となり得る特定の POP3 サーバごとに、プロキシ上で個別のポートを設定する必要があります。

次の例では、Microsoft Outlook で専用の POP3 を設定する方法を示します。

手順

1. InterScan MSS 検索サービスの IP アドレス「192.168.11.147」で、POP3 サーバアドレスを指定します。
 2. ユーザ名「test123」を指定します。
 3. POP3 ポートを 1100 に設定します。これは、InterScan MSS の専用の POP3 サービスが待機するポートです。
-

データベースを設定する

InterScan MSS がメッセージとデータを保存できるようにデータベース接続を設定します。

手順

1. [管理] > [InterScan MSS の設定] > [接続] の順に選択します。
初期設定では [コンポーネント] タブが表示されます。
2. [データベース] タブをクリックします。

表の上部に、InterScan MSS 管理データベースの種類、サーバの IP アドレス、ポート番号、ユーザ名、およびデータベース名が表示されます。

接続 ?

コンポーネント LDAP POP3 **データベース** Control Managerサーバ

IMSSデータベース

データベースのタイプ: PostgreSQL
 サーバ: 127.0.0.1
 ポート: 5432
 ユーザ名: sa
 データベース名: imss

EUQデータベース ⓘ

登録 アタッチ デタッチ

☐	サーバ	データベース名	ユーザ名	ステータス
☐	127.0.0.1	imsseq	sa	

注意: サーバのステータスを変更したり新しいデータベースを登録したりするなどEUQデータベースの設定を変更した場合は、変更後、EUQデータを再配布してください。

3. [EUQ データベース] で、必要に応じて EUQ データベースを管理するための操作を実行します。



注意

操作の詳細については、[453 ページの「EUQ データベースを管理する」](#)を参照してください。

Control Manager を設定する

Trend Micro Control Manager (以下、Control Manager) を使用して InterScan MSS を管理するには、InterScan MSS サーバの Control Manager/MCP エージェントを有効にし、Control Manager サーバを設定します。Control Manager サーバと InterScan MSS の間にプロキシサーバが配置されている場合は、プロキシを設定してください。Control Manager サーバと InterScan MSS の間にファイアウォールが配置されている場合は、ポート転送がファイアウォールのポート転送機能と連携するように設定してください。

**注意**

Control Manager の詳細については、Control Manager のドキュメントを参照してください。

手順

1. [管理] > [InterScan MSS の設定] > [接続] の順に選択します。
初期設定では [コンポーネント] タブが表示されます。
2. [Control Manager サーバ] タブをクリックします。
3. [Control Manager サーバの設定] で、次のパラメータを指定します。

オプション	説明
MCP エージェントを有効にする	チェックボックスをオンにしてエージェントを有効にします。
サーバ	Control Manager の IP アドレスまたは完全修飾ドメイン名 (FQDN) を指定します。
通信プロトコル	HTTP または HTTPS を選択し、対応するポート番号を指定します。HTTP アクセス用の初期設定ポート番号は 80 であり、HTTPS 用の初期設定ポート番号は 443 です。
Web サーバ認証	Control Manager Web サーバにアクセスするためのアクセスアカウント情報を指定します。

4. [プロキシ設定] で、次のパラメータを指定します。

オプション	説明
プロキシを有効にする	チェックボックスをオンにしてプロキシサーバを有効にします。
プロキシのタイプ	プロキシサーバが使用するプロトコルとして [HTTP]、[SOCKS4]、または [SOCKS5] を選択します。
プロキシサーバ	プロキシサーバの完全修飾ドメイン名または IP アドレス、ポート番号、およびユーザ名とパスワードを指定します。

オプション	説明
ポート	プロキシサーバのポートを指定します。
ユーザ名	プロキシサーバにアクセスするユーザ名を指定します。
パスワード	ユーザ名のパスワードを指定します。

5. [不審オブジェクトリストの設定] で、次の操作を行います。

- ・ InterScan MSS で不審ファイルを検出する場合は、[不審ファイルリスト] チェックボックスをオンにして、Control Manager から不審ファイルリストを同期する間隔を指定します。初期設定の同期間隔は 5 分、最小間隔は 1 分です。

不審オブジェクトリストの設定	
☒ 不審ファイルリスト 	
同期間隔:	5 分
前回の同期:	該当なし
☐ 不審URLリスト 	

- ・ InterScan MSS で不審 URL を検出する場合は、[不審 URL リスト] チェックボックスをオンにします。



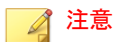
注意

Smart Protection Server を介して利用可能な Web レピュテーションサービスに基づいて不審 URL を検出します。Web レピュテーションと Smart Protection Server が正しく設定されていることを確認してください。

6. [保存] をクリックします。

設定ウィザードを使用している場合は、[次へ] をクリックします。

エージェントを有効にした場合、しばらくするとエージェントが Control Manager サーバに登録されます。エージェントを無効にした場合、InterScan MSS がただちに Control Manager サーバからログオフします。登録状況の変更については、Control Manager 管理コンソールで確認してください。

**注意**

また、Control Manager のバージョンが 6.0 Service Pack 3 Patch 3 HotFix 3611 以上であり、Smart Protection Server のバージョンが 3.0 Patch 1 以上であることを確認してください。

Control Manager で InterScan MSS のログオン資格情報を指定する

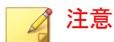
設定を有効にするには、Control Manager 管理コンソールで InterScan MSS の認証用のログオン資格情報を指定します。

手順

1. Control Manager の管理コンソールにログオンします。
2. [運用管理] > [管理下のサーバ] の順に選択します。
3. [サーバの種類] の横で、[InterScan Messaging Security Suite] を選択します。
4. 対象の InterScan MSS サーバを見つけて、[処理] 列にある [編集] アイコンをクリックします。

[サーバの編集] 画面が表示されます。

5. [認証] で、InterScan MSS のログオン資格情報を指定します。

**注意**

InterScan MSS の管理用に、Control Manager の初期設定の「admin」アカウントとは別の管理者アカウントを作成することをお勧めします。このアカウントは、Control Manager 管理コンソールでの認証に必要になります。

6. [保存] をクリックします。

Control Manager の登録を解除する

手順

1. [管理] > [InterScan MSS の設定] > [接続] の順に選択します。
初期設定では [コンポーネント] タブが表示されます。
2. [Control Manager サーバ] タブをクリックします。
3. [全エージェントを登録解除] ボタンをクリックします。

データベースのメンテナンススケジュールを設定する

クエリを実行したときにパフォーマンスが低下した場合、InterScan MSS データベースのインデックスを再作成した方が良い場合があります。インデックスの再作成は検索サービスのパフォーマンスに影響する可能性があるため、ピーク時以外に実行することをお勧めします。

手順

1. [管理] > [データベースの管理] の順に選択します。
[データベースの管理スケジュール] 画面が表示されます。

データベースの管理



データベースの管理スケジュール

☒ データベーステーブルのインデックス再作成

☒ 週次: 日曜日 4 : 00

☐ 月次: 1 日 4 : 00

保存

キャンセル

2. [データベーステーブルのインデックス再作成] チェックボックスをオンにします。
3. ドロップダウンボックスから週次スケジュールまたは月次スケジュールを選択します。
4. [保存] をクリックします。

製品ライセンスを管理する

InterScan MSS 製品は、管理コンソールからアクティベートできます。サポート契約の有効期限が切れている場合は、サポート契約を更新して新しいアクティベーションコードを入手し、管理コンソールからコードを指定する必要があります。製品がアクティベートされない場合は、その機能は無効になります。

コンポーネントの説明

InterScan MSS のコンポーネントには次のものがあります。

コンポーネント	説明
クラウドプレフィルタ	メッセージの承認済みリストやブロックリストを使用したフィルタ機能を提供し、メッセージがネットワークに到達する前に、スパムメール、ウイルス、およびその他の脅威を検索します。
トレンドマイクロのウイルス対策とコンテンツフィルタ	基本的なウイルス検索とフィルタ機能です。この製品は、InterScan MSS プログラムそのものです。
スパムメール対策 (コンテンツ検索)	オプションのスパムメールフィルタで、メールの内容からスパムメールを判定します。

コンポーネント	説明
IP プロファイラ	IP プロファイラにより、しきい値を設定して、以下の 4 つの潜在的なインターネットの脅威を検出したときの InterScan MSS の対処方法を決定できます。 ・ スパムメール: 不要な広告コンテンツが含まれるメッセージです。 ・ ウイルス: トロイの木馬プログラムなどの各種のウイルス脅威。 ・ DHA (ディレクトリハーベスト攻撃): ユーザのメールアドレスを収集し、スパムメール用のデータベースに追加するためにスパムメール送信者が使用する手法です。 ・ バウンスメール: 送信したメールが相手に届かずに、送達不能で送り返されたメッセージです。
Trend Micro Email Encryption	Trend Micro Email Encryption は、InterScan MSS と統合され、メッセージを暗号化および復号化したり、復号化できないメッセージをブロックしたりします。 Trend Micro Email Encryption は、InterScan MSS Linux 版ソリューションでは使用できません。
規制コンプライアンス	管理者は、規制コンプライアンスに対応するコンプライアンステンプレートを 사용할 수 있습니다. 利用可能なテンプレートのリストについては、http://esupport.trendmicro.com/solution/ja-JP/1107704.aspx を参照してください。

製品ライセンスを表示する

製品ライセンスは、[製品ライセンス情報] 画面で確認します。

手順

1. [管理] > [製品ライセンス] の順に選択します。

各ライセンスの簡単な概要が表示されます。

- ・ 製品
- ・ バージョン
 - ・ 製品版:ライセンスされた製品を購入していることを意味します。
 - ・ 体験版:無料でお試しいただける期限が設定された体験版にて使用していることを意味します。取得したアクティベーションコードによって体験期間が異なります。

体験期間の期限が切れる 14 日前から、管理コンソールに警告メッセージが表示されます。

体験期間後も InterScan MSS の使用を継続するには、InterScan MSS の製品版を購入して、新しいアクティベーションコードを入力する必要があります。

- ・ アクティベーションコード: xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx という形式の 31 文字の英数字から成るコードです。

製品をオンラインで登録すると、アクティベーションコードがメールで送信されてきます。このアクティベーションコードを [製品ライセンス] ページにコピーします。

- ・ ステータス: その製品の有効期限が切れているか、アクティベートされているかを示します。
 - ・ サポート契約の有効期限: トレンドマイクロのアップデートサーバから最新の検索エンジンとパターンファイルをダウンロードできなくなる日付です。最新の Web からの脅威に対してネットワークを保護するには、販売店に連絡してサポート契約を更新する必要があります。
2. 表示するライセンスについて、[詳細情報をオンラインで確認] をクリックします。

3. 最新のライセンスステータスを確認するには、[ステータス更新] をクリックします。
 4. ライセンスの概要の上部にある [無効なコンポーネントの通知を非表示] をクリックすると、無効なコンポーネントの通知が非表示になります。
-

ライセンスの更新またはアクティベーション

ライセンスの更新には 2 つの方法があります。

新しいアクティベーションコードを取得する

販売店に問い合わせて新しいアクティベーションコードを入手し、
[製品ライセンス情報] 画面でそのコードを入力します。

既存のアクティベーションコードの有効期限を延長する

販売店に問い合わせて、アクティベーションコードの有効期限を延長し、ライセンスのステータスを手動で更新するか、InterScan MSS
によって自動的に更新されるまで待ちます。

新しいアクティベーションコードを使用してライセンスを更新する

手順

1. [管理] > [製品ライセンス] の順に選択します。
各ライセンスの簡単な概要が表示されます。
2. [アクティベーションコード] の横にある [新規入力] をクリックします。
[アクティベーションコードの新規入力] 画面が表示されます。
3. [新しいコード] の横に、新しいコードを指定します。
4. [アクティベート] をクリックします。

管理コンソールからトレンドマイクロの Web サイトにアクセスし、ライセンスをアクティベートします。

トレンドマイクロの Web サイトにアクセスできない場合は、ネットワーク設定を確認し再試行してください。

既存のアクティベーションコードを使用してライセンスを更新する

手順

1. [管理] > [製品ライセンス] の順に選択します。
各ライセンスの簡単な概要が表示されます。
2. [詳細情報をオンラインで確認] をクリックすると、各ライセンスの詳細情報が表示されます。
3. [ステータス更新] をクリックします。管理コンソールからトレンドマイクロの Web サイトにアクセスし、ライセンスをアクティベートします。

トレンドマイクロの Web サイトにアクセスできない場合は、ネットワーク設定を確認し再試行してください。

現在のサポート契約の有効期限の 90 日前、60 日前、30 日前、0 日前と、現在のサポート契約の有効期限後の毎日、InterScan MSS によってライセンスのステータスがチェックされます。サポート契約が更新されると、InterScan MSS では保存されたライセンス情報が自動的に更新されます。



ヒント

ライセンスのステータスは InterScan MSS により自動的に更新されますが、アクティベーションコードの有効期限を延長後、すみやかに手動で更新することをお勧めします。

製品のアクティベーションを実行する

次の画面のいずれかを使用して製品をアクティベートします。

- ・ 設定ウィザードで、[アクティベート] 画面に進みます。
- ・ [管理] > [製品ライセンス] の順に選択します。

設定ウィザードからアクティベーションを実行する

手順

1. アクティベーションコードを指定して次のいずれかをアクティベートします。
 - ・ ウイルス対策およびコンテンツフィルタ
 - ・ スпамメール対策 (コンテンツ検索)
2. [次へ] をクリックします。



注意

アクティベーションコードは、xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx という形式です。

[製品ライセンス] からアクティベーションを実行する

手順

1. [管理] > [製品ライセンス] の順に選択します。
各ライセンスの簡単な概要が表示されます。
2. [アクティベーションコード] の横にある [新規入力] をクリックします。
[アクティベーションコードの新規入力] 画面が表示されます。
3. [新しいコード] の横に、新しいコードを指定します。
4. [アクティベート] をクリックします。

管理コンソールからトレンドマイクロの Web サイトにアクセスし、ライセンスをアクティベートします。トレンドマイクロの Web サイトにアクセスできない場合は、ネットワーク設定を確認し再試行してください。

Smart Protection Network を設定する

トレンドマイクロスマートフィードバックを有効にして、Trend Micro Smart Protection Network と脅威情報を共有するようにします。これにより、トレンドマイクロで新しい脅威を迅速に特定して対処することができるため、ネットワークの保護が強化されます。



注意

メールレピュテーション、ファイルレピュテーション、および Web レピュテーションは、すべて Smart Protection Network の一部です。

手順

1. [管理] > [Smart Protection Network] の順に選択します。
[Smart Protection Network] 画面が表示されます。
 2. [トレンドマイクロスマートフィードバックを有効にする (推奨)] を選択します。
 3. [保存] をクリックします。
-

第 30 章

システムとアプリケーションのアップデートと復旧

この章では、トレンドマイクロが Patch、Service Pack、およびその他のアップデートをリリースした際に、システムとアプリケーションファイルをアップデートおよび復旧する方法について説明します。

この章の内容は次のとおりです。

- ・ [484 ページの「システムとアプリケーションをアップデートする」](#)

システムとアプリケーションをアップデートする

新しい OS ファイルとアプリケーションファイルがトレンドマイクロから配布された場合、上位の InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) デバイスおよびそのすべての下位デバイスにファイルを配信します。初期設定では、下位デバイスは上位デバイスより先にアップデートされます。

内容は次のとおりです。

- ・ [484 ページの「システムとアプリケーションをアップデートする」](#)

新しいシステムファイルまたはアプリケーションファイルをアップロードする

手順

1. [管理] > [アップデート] > [システムとアプリケーション] の順に選択します。
2. [アップロード] で [参照] をクリックしファイルを検索します。
3. [アップロード] をクリックします。

ファイルのアップロードが終了したら、パッケージの種類、ビルド番号、およびタイトルが [最後にアップロードされたパッケージ] の下に表示されます。

システムファイルまたはアプリケーションファイルを配信する

手順

1. アップデートを配信するデバイスの横のチェックボックスをオンにします。
2. [アップデート] をクリックします。

3. 使用許諾契約書に同意できる場合は、該当するボタンをクリックします。
OS のアップデートまたはアップグレード後に InterScan MSS が再起動します。アプリケーションをアップグレードすると、InterScan MSS が自動的に再起動する場合があります。
4. InterScan MSS が再起動した場合、InterScan MSS が起動するまで待機して再度ログオンします。
5. [管理] > [アップデート] > [システムとアプリケーション] の順に選択して概要画面を表示します。

**注意**

- a. アップデート中は他の設定を変更しないでください。複数のデバイスをアップデートしている場合は、[キャンセル] をクリックして次のデバイスのアップデートを停止します。
- b. いくつかの Patch を下位デバイスに適用してから、そのデバイスの登録を上位デバイスから解除した場合、InterScan MSS では、システムファイルとアプリケーションファイルを自動的に復旧する処理が実行されます。そのため、ユーザが Patch を再適用する必要があります。

デバイスのチェックボックスがグレー表示されている場合、次の理由によりデバイスにファイルを配信できません。

- ・すでにアップデートされたファイルがある
- ・配信しようとしているファイルよりも新しいアップデートファイルがある
- ・デバイスが下位デバイスで、アップロードする Patch ファイルを上位デバイスに先に配信する必要がある、またはデバイスが上位デバイスで、アップロードする Patch ファイルを下位デバイスに先に配信する必要がある

すべてのデバイスのアップデート履歴を表示またはアップデートをロールバックする

手順

1. [ホスト名] で表示するデバイスの名前をクリックします。
[履歴] 画面にアップデートと関連するログの情報が表示されます。
 2. アップデートを削除するには、[ロールバック] をクリックします。
最新のアプリケーションのアップデートのみをロールバックできます。
 3. メイン画面に戻るには、[OK] をクリックします。
-

第 31 章

トラブルシューティングと FAQ

この章では、InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) の一般的な問題をトラブルシューティングする方法について説明します。

この章の内容は次のとおりです。

- ・ [488 ページの「トラブルシューティング」](#)
- ・ [505 ページの「FAQ」](#)
- ・ [524 ページの「クラウドプレフィルタのトラブルシューティング」](#)

トラブルシューティング

ここでは、InterScan MSS の設定または管理時に発生する可能性のある一般的な問題を解決する方法について説明します。この表を見ても問題が解決しない場合は、トレンドマイクロの製品 Q&A を確認してください。

InterScan MSS の配置に関するトラブルシューティングと FAQ 情報については、「*InterScan MSS インストールガイド*」を参照してください。

問題のトラブルシューティング

一般的な問題

管理コンソールまたはコンポーネントアクセスのトラブルシューティング

ターゲットポートがファイアウォールで許可されていません。ファイアウォールで、[502 ページの「InterScan MSS ポート」](#)に示されているポートを開きます。

管理コンソールにアクセスできない場合は、次の操作を行ってください。

手順

1. 管理コンソールの URL が Internet Explorer の信頼されたサイトでない場合は、その URL を信頼されたサイトに追加します。
2. セントラルコントローラプロセス S99ADMINUI を開始する前に、データベースプロセス dbctl.sh を開始します。
3. それでも管理コンソールにアクセスできない場合は、セントラルコントローラプロセス S99ADMINUI を再起動します。

詳細については、[535 ページの InterScan MSS スクリプト](#)を参照してください。

IMSSPS デーモンのトラブルシューティング

imssps デーモンが実行中の場合は、ポリシーサービスが機能しています。

手順

1. ポリシーサービスと検索サービス間の接続を確認します。
 2. LDAP 設定を確認します。
-

製品のアクティベーションまたはコンポーネントのアップデートのトラブルシューティング

この手順は、製品のアクティベーション (ウイルス対策/コンテンツフィルタ、スパムメール対策 (コンテンツ検索)、メールレピュテーション、送信者フィルタ) またはコンポーネントのアップデートに関する問題をトラブルシューティングする方法について説明します。メールレピュテーションを起動するには、InterScan MSS をトレンドマイクロに接続する必要があります。この処理には、有効な DNS 設定を指定した HTTP クエリが必要です。したがって、DNS サーバが使用できない場合や接続に問題がある場合は、起動に失敗します。

手順

- ・ 次のコマンドを使用して、DNS サーバの設定を確認します。

```
nslookup licenseupdate.trendmicro.com
```

このコマンドを実行すると、InterScan MSS サーバの IP アドレスが返されます。

インターネット接続にプロキシサーバが必要な場合は、プロキシ設定を確かめて、HTTP 要求が <http://licenseupdate.trendmicro.com> に到達することを確認してください。

- ・ 管理コンソールからプロキシ設定を確認します。
 - a. [管理] > [アップデート] の順に選択します。
初期設定では、[スケジュール] タブが表示されます。

- b. [アップデート元] タブをクリックします。
 - c. プロキシを設定します。
 - d. [保存] をクリックします。
-

メール通知のトラブルシューティング

通知メッセージに ASCII 以外の文字を使用している場合、通知メッセージの文字コードが正しく設定されていないと文字化けする場合があります。管理コンソールで、適切な文字コードを設定してください。

文字セットを変更するには

手順

1. [管理] > [通知] > [通知設定] の順に選択します。
 2. [文字コード] の横で、メッセージをエンコードする文字セットを選択します。
-

メッセージログクエリのトラブルシューティング

InterScan MSS 検索サービスでは、ログをローカル時刻で記録します。

手順

- ・ メッセージログをクエリするには、すべてのコンピュータの日時を InterScan MSS と同期させます。
-

[システムステータス] 画面のトラブルシューティング

管理下のサーバが切断される理由としては、次のことが考えられます。

- ・ 検索サービスがネットワークから削除された。
- ・ InterScan MSS マネージャサービスが停止している。

- ・ ネットワーク接続の問題が発生している。

手順

- ・ マネージャサービス待機ポートのファイアウォール設定を確認します。
-

添付ファイル情報のトラブルシューティング

隔離されたメッセージまたはアーカイブされたメッセージの詳細情報を表示する際、添付ファイル情報を利用できない

InterScan MSS は、添付ルールに一致したときにのみ添付情報を記録します。

手順

- ・ InterScan MSS がメッセージを隔離した理由を確認してください。
-

メールメッセージを受信しない場合のトラブルシューティング

手順

- ・ InterScan MSS 検索サービスと SMTP サービスが動作しているかどうか確認します。
 - ・ 別のアプリケーションが必要なポートを使用しているかどうか確認します。ポート 25 を開放します。
-

サービスが実行されない場合のトラブルシューティング

手順

1. InterScan MSS サービスを起動する前に、データベースを起動します。
 2. すべての InterScan MSS サービスを再起動します。
-

Web レピュテーションを有効にした場合の検索時間のトラブルシューティング

Web レピュテーションでは、トレンドマイクロの Web レピュテーションサーバに対してクエリを実行する必要があります。

手順

1. InterScan MSS の検索サービスから外部ネットワークへの HTTP 接続を確認します。
 2. Web レピュテーションの問題については、{インストールパス}\imss\log フォルダの wrsagent.* ファイルを確認してください。
-

エンドユーザメール隔離の問題

エンドユーザメール隔離へのアクセスのトラブルシューティング

ネットワーク上の他のコンピュータからコンソールを表示するには、次の URL にアクセスします。

手順

- ・ URL とポート番号が正しいことを確認します。

`https://<ターゲットサーバの IP アドレス>:8447`

エンドユーザメール隔離へのユーザアクセスのトラブルシューティング

手順

1. LDAP サーバ上で、ユーザアカウントのグループが正しいことを確認します。承認済みグループのユーザアカウントのみ、エンドユーザメール隔離にアクセスできます。

2. LDAP およびユーザメール隔離設定を InterScan MSS 管理コンソールで確認します。
 - a. [管理] > [InterScan MSS の設定] > [接続] > [LDAP] の順に選択します。
 - b. すべての設定、特に LDAP の種類とサーバ情報を確認します。
Kerberos 認証を使用している場合は、すべての InterScan MSS コンピュータと LDAP サーバの時刻が同期されていることを確認します。
 - c. [管理] > [エンドユーザメール隔離] の順に選択します。
 - d. [ユーザメール隔離アクセス]を選択します。
 - e. [選択したグループ] に正しい LDAP グループが表示され、ユーザアカウントが選択したグループに属していることを確認します。
3. ユーザのログオン名とパスワードが正しいことを確認します。
詳細については、[54 ページの「ログオン名形式」](#)を参照してください。
4. LDAP1 および LDAP2 サーバが同期していることを確認してください。
ユーザのアカウントが 1 つの LDAP サーバのみに存在する場合、ユーザはエンドユーザメール隔離管理コンソールに継続的にログオンできなくなります。InterScan MSS では、LDAP2 サーバを LDAP1 サーバのバックアップとして使用します。
5. 上記の設定の確認後も問題が継続する場合は、ログファイルをトレンドマイクロのテクニカルサポートに送信してください。

NTLM SSO を使用するエンドユーザメール隔離のトラブルシューティング

この手順は、NTLM シングルサインオン (SSO) を使用してエンドユーザメール隔離管理コンソールにログオンできないユーザのトラブルシューティング方法について説明しています。

**注意**

SSO を使用してエンドユーザメール隔離管理コンソールにログオンするには、NTLMv1 をサポートするように Active Directory の LMCapabilityLevel を設定する必要があります。

手順

1. LMCapabilityLevel を設定します。
 - a. [スタート] > [ファイル名を指定して実行] の順に選択し、**「secpol.msc」** と入力します。
 - b. [セキュリティの設定] > [ローカル ポリシー] > [セキュリティ オプション] > [ネットワーク セキュリティ: LAN Manager 認証レベル] > [ローカル セキュリティの設定] タブの順に選択します。
 - c. [LM と NTLM 応答を送信する] を選択して保存します。
2. LDAP1 または LDAP2 サーバのいずれかを有効にし、Active Directory で使用するよう指定します (IP/ドメイン名/FQDN)。
3. エンドポイントの OS で LMCapabilityLevel 設定の NTLMv1 がサポート (および有効化) されていることを確認します。
 - ・ Firefox を使用する場合: about:config リンクが NTLM 認証の信頼されるホストのリストを追加するように設定されている。
 - ・ Internet Explorer を使用する場合: エンドユーザメール隔離管理コンソールが内部サイトのリストに追加されている。
 - ・ Internet Explorer を使用する場合: Internet Explorer で統合 Windows 認証の設定が有効になっている。

エンドユーザメール隔離通知メッセージの表示のトラブルシューティング

適切な文字セットが選択されていないと、エンドユーザメール隔離通知で隔離されたメッセージ情報が正しく表示されない場合があります。

手順

1. [管理] > [通知] > [通知設定] の順に選択します。
2. [文字コード] の横で、言語を選択して、通知情報が正しく表示されるようにします。

エンドユーザメール隔離で表示されるメッセージのトラブルシューティング

エンドユーザメール隔離管理コンソールでは、管理者がアクセスを許可するようにエンドユーザメール隔離を設定しないと、ユーザは隔離されたメッセージを表示できません。

隔離領域がエンドユーザに表示されるようにするには

手順

1. [隔離およびアーカイブ] > [設定] の順に選択します。
2. エンドユーザメール隔離と同期させる隔離領域のリンクをクリックします。
3. [ウイルス対策ルール、フィッシング対策ルール、または Web レピュテーションルールに違反していないすべてのスパムメールおよびメールメッセージを EUQ データベースに同期させます (この領域でのみ)] の横にあるチェックボックスをオンにします。これにより、エンドユーザが、エンドユーザメール隔離コンソールからメッセージの表示と管理を行うことができます。

このオプションを有効にすると、この領域に隔離される不正でないすべてのメッセージ (ウイルス対策ルール、フィッシング対策条件、または Web レピュテーションに該当しないメッセージ) がエンドユーザメール隔離データベースと同期されます。これにより、エンドユーザが、エンドユーザメール隔離コンソールからメッセージの表示と管理を行うことができます。

エンドユーザは不正なメッセージにはアクセスできません。

Kerberos 認証における LDAP のトラブルシューティング

Kerberos プロトコルは、Kerberos サーバと InterScan MSS 間の時刻を同期する必要があります。

手順

1. InterScan MSS をインストールしたすべてのコンピュータの日付/時間を同期します。
 2. DNS サーバが正しく設定されていることを確認します。
-

エンドユーザメール隔離への Kerberos SSO のトラブルシューティング

SSO を使用してエンドユーザメール隔離管理コンソールにログオンするには、次の設定が必要です。

手順

1. LDAP1 または LDAP2 サーバのいずれかが有効であり、Active Directory で使用するよう指定されている (IP アドレス/ドメイン名/FQDN) ことを確認します。
2. InterScan MSS 用に設定されている DNS サーバに Kerberos サービスのレコードが含まれていることを確認します。
3. エンドポイントの OS で Kerberos 認証がサポート (および有効化) されていることを確認します。
 - ・ InterScan MSS と Kerberos 認証サービスとの間で時間が同期されている必要があります。
 - ・ Firefox を使用する場合:about:config リンクが、Negotiate 認証において信頼された URL リストを追加するように設定されている。
 - ・ Internet Explorer を使用する場合:エンドユーザメール隔離管理コンソールが内部サイトのリストに追加されている。

- ・ Internet Explorer で統合 Windows 認証の設定が有効になっている。
 - ・ Windows Vista 以上を使用する場合: キータブファイルの生成時にホスト名をインスタンスとして使用している。
4. 1 つのエンドユーザメール隔離管理コンソールインスタンスのみが 1 つのユーザアカウントにマップされていることを確認します。このインスタンスが複数のユーザにマップされている場合、SSO は機能しません。
 5. エンドユーザメール隔離が上位/下位の形態で配置されている場合は、上位デバイスの 8447 ポートを使用してエンドユーザメール隔離にアクセスしていることを確認します。下位デバイスのポートを使用すると、SSO は機能しません。
 6. [LDAP 設定] 画面で指定したアカウントに、認証用にすべてのアカウントを検索する権限があることを確認します。

送信者フィルタの問題

FoxyProxy の起動のトラブルシューティング

FoxyProxy が起動しない理由は、複数あります。理由を調べるには、IP プロファイラのログを表示します。

手順

1. IP プロファイラの設定ファイルがあるディレクトリに移動します (初期設定:/opt/trend/imss/config)。
2. foxproxy.ini を開きます。
3. log_level の値を 4 に変更します。
4. FoxyProxy を再起動するには、次のように入力します。

```
/opt/trend/imss/script/foxproxyd restart
```
5. ログファイルを開くには、次のように入力します。

```
/opt/trend/imss/log/foxproxy-general.****
```

FoxyProxy の接続性のトラブルシューティング

手順

1. FoxyProxy が稼働中で、設定されたポート (初期設定ではポート 25) にバインドしていることを確認します。
-

FoxyProxy のメッセージ処理速度のトラブルシューティング

FoxyProxy でメッセージが受信されると、FoxDNS で DNS クエリが実行されます。BIND サービスが稼働していない場合、FoxyProxy は DNS クエリがタイムアウトになるまで待機し続けます。

手順

- ・ 次の手順で、FoxDNS がインストールされているコンピュータで BIND サービスが稼働していることを確認します。
 - a. 次のコマンドを入力します。

```
ps -ef | grep named
```
 - b. サービスが稼働していない場合は、起動します。
-

FoxyProxy でブロックされた接続の表示のトラブルシューティング

ブロックされた接続に関する情報は、5 分ごとに FoxyProxy から InterScan MSS サーバに送信されます。

接続情報が表示されるまで、少なくとも 5 分間待機してください。

この時間の値を変更するには

手順

1. foxproxy.ini を開きます。
2. report_send_interval の値を変更します。
3. FoxProxy を再起動するには、次のように入力します。

```
/opt/trend/imss/script/foxproxyd restart
```

FoxDNS のトラブルシューティング

BIND サービスが稼働していることを確認します。

手順

1. 次のコマンドを指定します。

```
ps -ef | grep named
```

2. サービスが稼働していない場合は、起動します。
-

IP プロファイラのログのトラブルシューティング

次の IP プロファイラ関連ログファイルは、InterScan MSS 管理データベースにあります。

- ・ foxmsg.****
- ・ foxnullmsg.****
- ・ foxreport.****

この手順では、ログファイルが存在することを確認する方法について説明します。

手順

1. InterScan MSS がインストールされているコンピュータ上の log ディレクトリに移動します (初期設定:/opt/trend/imss/log/)。

2. ファイルが存在しない場合、次のコマンドを使用して、imssmgr が稼働しているかどうかを確認します。

```
ps -ef | grep imssmgr
```

3. 次のコマンドで、FoxProxy が稼働しているかどうかを確認します。

```
ps -ef | grep foxproxy
```

4. IP プロファイラが有効になっていることを確認します。
「t_foxhuntersetting」テーブル内で、次のように表示されている必要があります。

```
record: 'Type' = 1 and 'enable' = TRUE
```

管理コンソールを有効にした後のメールレピュテーションのトラブルシューティング

メールレピュテーションが機能しない理由として、次の可能性が考えられます。

- ・ メールレピュテーションがアクティベートされていない。
- ・ 検索サービスがインストールされているコンピュータからインターネットにアクセスできない。Mail Transfer Agent (以下、MTA) はアクティベーションコードの検証に関する DNS クエリの応答を取得できません。検索サービスをインストールしているコンピュータが、インターネットに接続されていることを確認してください。

手順

1. メールレピュテーションをアクティベートして、InterScan MSS からインターネットにアクセスできることを確認してください。

SMTP ルーティングと Postfix のトラブルシューティング

この手順では、管理コンソールの [SMTP ルーティング] 画面上の MTA 設定が Postfix 設定ファイルに書き込まれない問題のトラブルシューティングについて説明します。

初期設定では、[SMTP ルーティング] 画面の設定は、各検索サービスの Postfix に自動的に適用されません。

設定をすべての検索サービスに適用するには

手順

1. [管理] > [InterScan MSS の設定] > [SMTP ルーティング] の順に選択します。

[SMTP ルーティング] 画面が表示されます。

2. [すべての検索サービスに適用] チェックボックスをオンにします。
3. [保存] をクリックします。
4. 数分後に、各検索サービス上の InterScan MSS マネージャプロセスによって設定が Postfix に同期されます。InterScan MSS マネージャをただちに再起動するには、次のコマンドを使用します。

```
/opt/trend/imss/script/S99MANAGER restart
```

5. InterScan MSS マネージャプロセスによって同期されない場合は、ローカルの設定ファイル/opt/trend/imss/config/imss.ini で、enable_postset_thd キーが [yes] に設定されているか空白になっていることを確認します。
-

IP プロファイラのブロックリストのトラブルシューティング

変更が有効になるまで約 1 分かかります。

手順

1. 1 分待つてから、再度リストをチェックしてください。
-

[概要] ページでのブロックされた IP アドレスのトラブルシューティング

[概要] ページには、過去 24 時間の上位 10 のブロックされた IP アドレスが種類別に表示されます。たとえば、本日の 16:12 時点では、[概要] ページには、昨日の 16:00 から本日の 16:00 までのデータが表示されます。

手順

1. 1 時間後に [概要] ページを表示してください。

InterScan MSS ポート

次の表に、InterScan MSS で使用される初期設定のすべてのポートを示します。

表 31-1. InterScan MSS ポート

ポート番号	コンポーネントと役割	設定場所
25	MTA サービスポートです。メールサーバはこのポートで待機してからメッセージを受け入れます。ファイアウォールでこのポートを開いておかなければ、サーバはメールを受け入れることができません。	[管理] > [InterScan MSS の設定] > [SMTP ルーティング] > [接続] の順に選択します。
110	InterScan MSS 検索サービスの一般的な POP3 ポートです。検索サービスは、このポートを使用して POP3 要求の受け入れやすべての POP3 サーバに対する POP3 メールを検索を行います。	[管理] > [InterScan MSS の設定] > [接続] > [POP3] の順に選択します。
5060	ポリシーサーバの待機ポートです。検索サービスは、このポートに接続してすべてのメッセージで一致したルールを検索します。	[管理] > [InterScan MSS の設定] > [接続] > [コンポーネント] の順に選択します。

ポート番号	コンポーネントと役割	設定場所
8009	エンドユーザメール隔離管理コンソールの Tomcat AJP ポートです。このポートは、複数の Tomcat サーバと Apache HTTP サーバ間の負荷分散を行うために使用されます。	<code>{IMSS}%UI%euqUI%conf% server.xml: Server%Service %Connector (protocol=AJP %1.3)%port</code>
8445	管理コンソールの待機ポートです。Web ブラウザを使用して管理コンソールにログインするには、このポートを開く必要があります。	Apache 待機ポート: <code>{IMSS}%UI%php%conf%widget.conf: Listen%VirtualHost</code>
8446	エンドユーザメール隔離サービスの待機ポートです。	<code>{IMSS}%UI%euqUI%conf %server.xml:Server%Service %Connector%port</code>
8447	負荷分散を備えたエンドユーザメール隔離サービスの待機ポートです。	<code>{IMSS}%UI%euqUI%conf %EUQ.conf:Listen%VirtualHost %ServerName</code>
10024	InterScan MSS 検索サービスの再処理ポートです。管理データベースの中央隔離領域およびエンドユーザメール隔離データベースから発信されたメッセージは、このポートに送られて再処理されます。	<code>imss.ini%[Socket_3]%proxy_port</code>
10025	InterScan MSS 検索 SMTP サービスの待機ポートです。	<code>imss.ini%[socket_1]%proxy_port</code>

ポート番号	コンポーネントと役割	設定場所
10026	InterScan MSS で作成された通知メッセージの送信など内部で使用するための InterScan MSS 「パススルー」 SMTP ポートです。このポートに送信されたすべてのメッセージは、InterScan MSS によって検索されません。セキュリティ上の問題から、このポートは InterScan MSS サーバのループバックインタフェース (127.0.0.1) のみバインドされます。そのため、他のコンピュータからはアクセスできません。ファイアウォールでこのポートを開く必要はありません。	IMSS_HOME/postfix/etc/ postfix/master.cf
15505	InterScan MSS マネージャの待機ポートです。マネージャはこのポートを使用して、管理コンソールからサービスの開始や停止などの管理コマンドを受け入れます。また、このポートを経由して隔離/アーカイブのクエリ結果を、管理コンソールおよびエンドユーザーメール隔離管理コンソールに提供します。	InterScan MSS サーバでは設定できません。
関連するサービスを有効にしている場合、InterScan MSS によって次のポートに対する通信が行われます。		

ポート番号	コンポーネントと役割	設定場所
53	BIND サービスの待機ポートです。  警告! ポート番号は変更しないでください。	InterScan MSS サーバでは設定できません。

FAQ

この項では、よくある質問 (FAQ) に対する回答を提供します。

Postfix MTA 設定

Postfix に複数の検索サービスを配置した場合、これらの Postfix インスタンスを一元管理する方法はありますか。

管理コンソールからすべての Postfix コンピュータを制御するには、[すべての検索サービスに適用] オプションを有効にします。メニューから、[管理] > [SMTP ルーティング] > [SMTP] の順に選択します。

一部の Postfix インスタンスの設定を個別に例外とすることはできますか。

一部の Postfix 設定に例外を設けるには、`imss.ini` で「`detach_key_postfix`」キーを検索し、管理コンソールから適用しないキーを追加します。次に例を示します。

```
detach_key_postfix=smtpd_use_tls:smtpd_enforce_tls:queue_directory
```

上記のパラメータは、管理コンソールを介して実行された設定によって上書きされることはありません。`main.cf` を手動で変更します。

**注意**

"{Parameter1}:{Parameter2}::{Parameter n}"は、コロンを使用してパラメータを区切ることによって、1つ以上のパラメータを使用できることを意味します。

データベースのテーブル `tb_postfixconfig` で、`fieldname` 列の下にパラメータ名を見つけることができます。

**警告!**

設定ファイルを変更する際は、十分に注意してください。

InterScan MSS コンポーネント

どのようにデータベースを設定、管理できますか。

以下のコマンドを使用して、データベースを管理できます。

**注意**

`ex`、`psql`、`pgdump`、および `pgrestore` などの SQL コマンドを使用する前に、まず `source /IMSS_install_path/imss/script/pg.rc` コマンドを実行します。たとえば、`source /opt/trend/imss/script/pg.rc` のように実行します。

さらに、Red Hat Enterprise Linux 7 を実行するデータベースサーバに接続するには、コマンド行に `-h 127.0.0.1` を追加します。たとえば、`/opt/trend/imss/PostgreSQL/bin/psql -h 127.0.0.1 -U sa -d imss` のように実行します。

- ・ `pg_dump -d imss -U sa > YYMMDD.HHMMSS.backup` — データベースをバックアップします。
- ・ `psql -U sa -d imss < ./YYMMDD.HHMMSS.backup` — エラーが発生した場合に、最新のデータを取り出します。
- ・ `vacuum` — 頻繁にアクセスされるテーブルまたは大量のデータがあるテーブル上のデータベースをクリーンアップします。メールトラフィックが小さい、またはデバイスがネットワークに接続されていないときに、このコマンドを使用します。

- ・ `vacuumfull` — データベースの使用頻度が低い、またはデバイスがネットワークに接続されていないときに、データベース全体をクリーンアップします。
- ・ `redirect_stderr= and log_rotate_***=` — 古いデータベースログエントリをシステムログにリダイレクトする場合は、`postgresql.conf` でこれらのオプションを有効にします。ログファイルにダッシュ「-」で始まる名前を付けることができます。

メールレピュテーション

特定の IP アドレスまたはドメインをブロックしないようにするにはどのようにメールレピュテーションを設定すればいいですか？

次の手順で IP アドレスまたはドメインをメールレピュテーションの承認済みリストに追加します。



注意

ドメインが DNS サービスで解決されない場合、そのドメインは承認済みリストでは機能しません。

手順

1. 管理コンソールにログオンします。
2. [送信者フィルタ] > [承認済みリスト] の順に選択します。
3. ブロックしない IP アドレスまたはドメインを承認済みリストに追加します。

IP プロファイラ

FoxProxy ログを削除するにはどうしたらいいですか。

ログ削除プログラムが IP プロファイラのインストールディレクトリ内にあります (初期設定: `/opt/trend/imss/bin/TmFoxPurgeLog`)。

ログの削除機能に関する設定は設定ファイル `foxproxy.ini` に記載されています。キーは次のとおりです。

- `log_purge`
- `log_purge_unit`
- `log_purge_num`

FoxProxy のステータスを監視するのはどのプロセスですか。 FoxProxy の機能が停止したとき、復旧するのはどのプロセスですか。

FoxProxy は、マルチプロセスプログラムです。メインプロセスは、子プロセスのみを監視します。子プロセスの機能が停止した場合、メインプロセスが対応します。FoxProxy のメインプロセスは、`imssmgr` が監視します。メインプロセスが停止した場合には、`imssmgr` が対応します。

DNS クエリを実行するのはどのプロセス/コンポーネントですか。

DNS クエリは FoxProxy から直接実行されます。

ブロックリスト/承認済みリストに追加された IP アドレスのドメイン名が、いつも「該当なし」なのはなぜですか？

InterScan MSS では、ブロックリスト/承認済みリストに追加された IP アドレスのドメイン名を識別しません (InterScan MSS では、追加されたドメイン名の IP アドレスを解決しません)。

[送信者フィルタ] > [不審な IP] 画面でブロックする IP アドレスの接続情報も表示されるのはなぜですか？

[送信者フィルタ] > [不審な IP] 画面には、正常な接続の情報がすべて表示されます。したがって、IP アドレスがブロックするリストに含まれていても、当該 IP アドレスで以前ブロックされていなかった接続情報が表示されます。

IP プロファイラは既存の BIND サーバを使用できますか。

いいえ。InterScan MSS では新しい BIND サーバをインストールします。IP プロファイラで使用できるのは、この組み込みの BIND サーバのみです。

InterScan MSS 9.1 がメールメッセージを「Foxhunter_proxy@domain」に送信するのは、どのようなときですか。

InterScan MSS は、次の 3 つの状態になると、メールメッセージを「Foxhunter_proxy@domain」に送信します。

- ・ FoxProxy が「不完全な」メッセージを受信した場合。
- ・ FoxProxy が「Null」メッセージを受信した場合。
- ・ FoxProxy が接続を拒否した場合、5 分ごとに統計メールを送信します。
foxproxy.ini 内の report_send_interval (秒単位) 設定を変更して、時間間隔を設定できます。

受信トラフィックが DHA 攻撃であるかどうかの分析に LDAP サービスは必要ですか。

厳密には、LDAP サービスは必須ではありません。InterScan MSS の DHA ルールは、Postfix から返された結果に依存しています。その結果は、分析用の IP プロファイラのサブモジュールである FoxProxy に代わりに渡されます。LDAP サーバは、Postfix が受信者のメールボックスの存在をチェックするための方法の 1 つにすぎません。

メール領域とキュー

クエリの実行で特殊文字を使用できますか？

クエリの実行では次の特殊文字が使用できます。

- ・ アスタリスク (*) — ワイルドカード文字として文字の検索に使用されます。アスタリスク (*) を使用して、メールアドレスやファイル名を検索できます。

メールアドレスを検索するには、次の例を参照してください。

表 31-2. メールアドレスの検索

例	説明
*	すべてのメールアドレスを表します。
@domain.tld、 name@.tld	前者は特定のドメイン名とトップレベルドメイン (TLD) を持つすべてのメールアドレスを表し、後者は特定のユーザ名と TLD を持つすべてのメールアドレスを表します。
@.tld	特定の TLD を持つすべてのメールアドレスを表します。

ファイル名を検索するには、次の例を参照してください。

表 31-3. ファイル名の検索

例	説明
.	すべてのファイルを表します。
*.拡張子	特定の拡張子のすべてのファイルを表します。
名前.*	特定の名前を持つすべての拡張子のファイルを表します。

- ・ セミコロン (;): 複数の送信者や添付ファイルを検索する際の区切り文字として使用します。

ユーザがメッセージの詳細を表示するときに、メッセージ ID なしの隔離されたメッセージがあるのはなぜですか。

InterScan MSS は、セキュリティ上の理由で通知メールメッセージを再処理します。したがって、通知メールメッセージがポリシー違反によって隔離された場合、InterScan MSS によって作成されたこの通知メールメッセージにはメッセージ ID がありません。

InterScan MSS で通知メールメッセージを検索しないようにするには、次の手順を実行して通知メールメッセージの検索を無効にできます。

1. imss.ini の [general-notification] セクションで次の設定を変更します。

```
NotificationSkipScan=1
```

2. 次のコマンドを入力して InterScan MSS デーモンを再起動します。

```
net stop TmImssScan
```

```
net start TmImssScan
```

3. 次の手順に従って、InterScan MSS 検索サービスを再起動します。

- ・ [コントロールパネル] > [管理ツール] > [サービス] に移動します。
- ・ [InterScan MSS 検索サービス] を右クリックし、[再起動] を選択します。



注意

通知メールメッセージの検索は無効にしないことをお勧めします。

エンドユーザメール隔離

Kerberos を使用している場合、ユーザがエンドユーザメール隔離管理コンソールに「domain\user_name」の省略名でログオンできないのはなぜですか？

Kerberos サーバでは、Domain\user_name 形式のユーザ名を受け入れることができません。Kerberos では次の形式のユーザ名を使用する必要があります。

```
user_name@domain.xxx
```

Microsoft Exchange Server をインストールして、ユーザごとに複数のメールアドレスを設定している場合、1 人のユーザに対する複数のメールアドレスを確認するためには、エンドユーザメール隔離をどのように有効にすればいいですか？

1 つの Microsoft Exchange Server を Active Directory とともにインストールしている場合、次の操作を行うことができます。

手順

1. InterScan MSS 管理データベースで tb_global_setting テーブルを開き、LDAP-->mail_attr の値を「mail」から「proxyAddresses」に置き換えます。
 2. すべての InterScan MSS サービスを再起動します。
-

英語以外のエンドユーザメール隔離通知を送信するには、どうしたらいいですか。

次の手順を実行してください。

手順

1. 管理コンソールメニューから、[管理] > [通知] > [EUQ 通知] の順にクリックします。

[EUQ 通知] 画面が表示されます。

2. エンドユーザメール隔離通知の件名とコンテンツを英語以外の言語で入力します。

3. [管理] > [通知] > [通知設定] の順にクリックします。

[通知設定] 画面が表示されます。

4. 文字コードとして英語以外の言語を選択します。
-

LDAP サーバが Active Directory である場合、LDAP アクセスの速度を上げるにはどのようにしたらよいですか？

アクセスの速度を上げるには 2 つの方法があります。お使いのポート番号が、389 か 3268 によって方法が異なります。

Active Directory では、グローバルカタログでポート 3268 を使用します。グローバルカタログに送信される LDAP クエリは、別のドメインコントローラを参照することがないため、より早く処理されます。



注意

Active Directory に対する LDAP クエリではポート 3268 を使用することをお勧めします。

Active Directory では、LDAP クエリでポート 389 を使用します。1 つのアイテムが 1 つのドメインコントローラ内で照会できない場合、LDAP 参照メカニズムを使用して別のドメインでクエリを実行します。ドメインが 1 つしかない場合、またはポート 3268 が利用できない場合は、ポート 389 を使用します。

LDAP クエリでポート 3268 を使用する

手順

1. [管理] > [IMSS 設定] > [接続] の順にクリックします。
[接続] 画面が表示されます。
 2. [LDAP] タブをクリックします。
 3. 変更する LDAP サーバを選択します。
 4. LDAP 待機ポートの値を 3268 に設定します。
-

LDAP クエリでポート 389 を使用する

手順

1. [管理] > [InterScan MSS の設定] > [接続] の順にクリックします。
[接続] 画面が表示されます。
 2. [LDAP] タブをクリックします。
 3. 変更する LDAP サーバを選択します。
 4. LDAP 待機ポートの値を 389 に設定します。
 5. 次のキーを imss.ini ファイルに追加します。このファイルは
\$IMSS_HOME¥config に存在します。

[LDAP-Setting]

DisableAutoChaseReference=yes
 6. すべての InterScan MSS サービスを再起動します。
-

InterScan MSS では、Active Directory に対してどのような形式のユーザログオン名をサポートしていますか？

Active Directory では、次のようなログオン名形式がサポートされています。

- ・ 例 1: bob@imsstest.com



注意

ログオン名は (このような形で表示されますが) メールアドレスではありません。

- ・ 例 2 (Windows 2000 以前): IMSSTEST\bob



注意

Windows 2000 以前の形式は、Kerberos 認証ではサポートされていません。

一部のユーザが Kerberos SSO を使用できないのはなぜですか？

SPN (サービスプリンシパル名) にバインドされているユーザは Kerberos SSO を使用できません。

スパムメール対策サービス

スパムメールの検出率はどうに確定するのですか？

InterScan MSS がメッセージをスパムメールとして分類する際のしきい値を 3.0 ～10.0 で指定します。しきい値が高ければ、「スパムメールの可能性」が非常に高いメッセージがスパムメールとして分類されます (つまり、スパムメール検出率は低くなり、誤検出の可能性も減ります)。しきい値が低ければ、「スパムメールの可能性」が低くてもスパムメールとして分類されます (つまり、スパムメール検出率は高くなり、誤検出も増えます)。

アップデート

パターンファイルをどのようにロールバックするのですか？

[システムステータス] 画面で [ロールバック] ボタンをクリックしてください。

Control Manager

Control Manager での InterScan MSS の登録および登録解除の状況について確認する方法を教えてください。

確認方法には次の 3 つがあります。

- ・ Control Manager の管理コンソールを使用する
- ・ OS シェルを使用する
- ・ InterScan MSS の管理コンソールを使用する

Control Manager 管理コンソールから InterScan MSS の登録状況を確認する

手順

1. Control Manager の管理コンソールにログオンします。
 2. [製品] をクリックします。
[製品ディレクトリ] 画面が表示されます。
 3. 製品ディレクトリで InterScan MSS のローカルフォルダをチェックします。
-

OS シェルから InterScan MSS の登録状況を確認する

手順

1. OS シェルにログオンします。
2. 次のコマンドを入力します。

```
/opt/trend/imss/script/S99CMAGENT isregistered
```

InterScan MSS 管理コンソールから InterScan MSS の登録状況を確認する

手順

1. InterScan MSS 管理コンソールにログオンします。
 2. [管理] > [接続] > [Control Manager サーバ] の順に選択します。
 3. [接続ステータス] を確認します。
-

LDAP

正しい管理者アカウントを使用して LDAP サーバを追加できないのはなぜですか？

最初に、LDAP サーバから InterScan MSS に接続できることを確認します。次に、LDAP サーバの種類やログオン名の形式が正しく設定されていることを確認します。

Active Directory 2008 で Kerberos 認証を使用できないのはなぜですか？

最初に、DNS サーバが正しく設定されていることを確認します。次に、Active Directory 2008 Kerberos の ServicePrincipalName を確認します。

ServicePrincipalName が変更されている場合は、/opt/trend/imss/config/imss.ini の値を変更してください。

以下に例を示します。

```
[LDAP-Setting]
```

```
server-spn=ad2008@domain.com
```

LDAP サーバに Sun iPlanet を使用していますが、アカウントがクラウドプレフィルタと正しく同期されないのはなぜですか？

Sun iPlanet LDAP サーバに 2,000 を超えるアカウントを登録している場合は、Sun iPlanet LDAP サーバを一部変更する必要があります。[Directory Server] > [Directory] > [cn=config] > [Plugins] > [ldbm database] > [config] > [General Editor] 画面で、「nsslapd-lookthroughlimit」の値を増やします。

その他の FAQ

InterScan MSS または InterScan MSS コンポーネントの IP アドレスを変更できますか？

はい。

InterScan MSS (セントラルコントローラと検索サービス) の IP アドレスを変更する

手順

1. \$IMSS_Home/imss/script/imssstop.sh stop コマンドを実行してすべての InterScan MSS サービスを停止するか、サービスを個別に停止します。

InterScan MSS のスクリプトの詳細については、[535 ページの InterScan MSS スクリプト](#)を参照してください。

2. サーバの IP アドレスを変更します。
3. このサーバにデータベースサービスがインストールされている場合は、データベースサービスを開始します。InterScan MSS によってデータベースがインストールされている場合は、次のコマンドを使用します。

```
$IMSS_Home/imss/script/dbctl.sh start
```

4. odbc.ini ファイルおよび euqodbc.ini ファイルの IP アドレスを変更します。これらのファイルは、InterScan MSS 設定フォルダ (\$IMSS_Home/imss/config/) にあります。
5. 次のデータベースデータを変更します。

tb_component_list

コンピュータ名とすべての検索サービスの IP アドレスを指定します。

tb_euq_db_info

エンドユーザメール隔離データベースのコンピュータ設定を指定します。

tb_global_setting

[cmagent] name [ConfigUrl] セクションで、管理コンソールの URL を変更します。

6. 次のコマンドを使用して、すべての InterScan MSS サービスを起動します。

```
$IMSS_Home/imss/script/imssstart.sh
```

InterScan MSS では分割メッセージをどのように処理するのですか？

InterScan MSS での分割メッセージの処理方法は、InterScan MSS の設定ファイル imss.ini の BypassMessagePartial キーの設定によって異なります。

imss.ini ファイル内で BypassMessagePartial=no と設定されている場合、InterScan MSS では分割メッセージが正しくない形式のメッセージとして拒否されます。

キーが yes に設定されている場合 (初期設定)、InterScan MSS では分割メッセージが無視されます。

ポリシー設定の際に、InterScan MSS でインポートできるのはどのようなファイル形式ですか？

InterScan MSS では、1 行に 1 項目だけを含むテキストファイルのみをインポートできます。次は、管理コンソールからテキストファイルをインポートする方法の例です。

手順

1. 検索する添付ファイルを指定する場合
 - a. メニューから、[ポリシー] > [ポリシーリスト] の順にクリックします。
 - b. 既存のルールをクリックして、ルールを編集します。
 - c. [検索条件] リンクをクリックします。
 - d. [添付ファイル] セクションの下にある [名前または拡張子] リンクをクリックします。
 - e. [指定のファイル名] チェックボックスをオンにします。
 - f. [インポート] をクリックします。インポートされたファイルは、1 行に 1 つのファイル名または拡張子を含むテキストファイルでなければなりません。
2. スпамメール検出を設定する場合
 - a. メニューから、[ポリシー] > [ポリシーリスト] の順にクリックします。
 - b. 既存のルールをクリックして、ルールを編集します。
 - c. [検索条件] リンクをクリックします。
 - d. [スパムメール] リンクをクリックします。

- e. [承認済み送信者リスト] または [ブロックする送信者リスト] チェックボックスをオンにします。
- f. [インポート] をクリックします。インポートされたファイルは、1 行に 1 つのメールアドレスを含むテキストファイルでなければなりません。

新しく作成した管理者アカウントが [ユーザメール隔離アクセス]、[管理者アカウント]、または [製品ライセンス情報] ページにアクセスできないのはなぜですか？

初期設定の InterScan MSS 管理者アカウントだけが、[ユーザメール隔離アクセス]、[管理者アカウント]、または [製品ライセンス情報] ページにアクセスする権限を持っています。権限を委任された管理者のアカウントでは、これらのページにアクセスできません。

InterScan MSS 設定への変更がただちに適用されないのはなぜですか？

管理コンソールから設定を変更した時間と InterScan MSS サーバ上で変更内容が実際に更新される時間との間にわずかなずれがあります。

ポリシー設定は 3 分以内に再読み込みされます。この設定をより速く読み込むには、必要に応じて、InterScan MSS 管理データベースの `tb_global_setting` テーブルで `policy_server=>dbChangePollIntervalInSecs` 設定を変更します。

その他の一般的な設定については、管理コンソールから変更した新しい設定が、`imssmgr` により 1 分以内に再読み込みされます。



注意

トレンドマイクロでは、管理コンソールから設定を変更した直後に InterScan MSS ヘメールを送信しないことをお勧めします。

次の項目の最大数に制限はありますか？

- ・ 各ルールの送信者と受信者
- ・ 1つのアドレスグループ内のメールアドレス
- ・ スпамメール判定ルールの承認済み送信者とブロックする送信者

各ルールの合計サイズは最大 640KB です。合計サイズには、ルールルート (送信者と受信者)、ルールフィルタ (検索条件)、ルール処理などが含まれます。各メールアドレスまたは各 LDAP アカウントは 20 文字で構成されることが前提となっており、InterScan MSS では、ルールルートで少なくとも 10,000 の送信者と受信者をサポートできます。

1つのアドレスグループの最大メールアドレス数は、10,000 です。

スパムメール判定ルールの承認済み送信者とブロックする送信者の最大数は 5,000 です。

ログのパスを変更するにはどうしたらいいですか？

一部のログのパスを変更する場合は、必要に応じて、imss.ini の次のキーを検索して初期設定を変更してください。

```
[general]
sys_log_path=/opt/trend/imss/log
event_log_path=/opt/trend/imss/log
policy_evt_log_path=/opt/trend/imss/log
```

サードパーティのアップストリームサーバがインストールされていない場合、InterScan MSS 9.1 で InterScan MSS のリレーの制約を設定できますか？

いいえ。InterScan MSS 9.1 では InterScan MSS のリレーの制約は設定できません。これは、InterScan MSS が Linux プラットフォーム上の MTA を持たないためです。サードパーティの MTA を使用した場合のみ、リレーの制約を設定できます。

InterScan MSS 検索サービスのアクセス制御リスト (ACL) を変更するには、どうしたらいいですか？

imss.ini の次の設定を変更できます。

- ・ パラメータ smtp_allow_client_ip に対象となる IP アドレスを追加します。
- ・ または、open_to_all_connections=yes を設定して ACL チェックを無効にします。
- ・ 他のコンピュータが検索サービスに接続できることを確認するには、対象の IP アドレスをパラメータ proxy_smtp_server_ip に挿入します。

詳細については、imss.ini のコメントを参照してください。

特定の送信者からのメッセージが常に添付ファイルとして受信されるのはなぜですか？また、メッセージの本文がディスクリーマーやスタンプに置き換えられるのはなぜですか？

スタンプの文字コードがメッセージのコンテンツの文字コードと異なる場合、InterScan MSS では、メッセージの検索後にスタンプがメッセージの本文に挿入されるという問題が発生します。このような場合、InterScan MSS では、メッセージの本文にスタンプを挿入して、オリジナルのメッセージを添付ファイルにした新しいメッセージが作成されます。メールのコンテンツが変更されることはありません。

コンテンツフィルタのルールを作成する際に、「From」、「To」、または「Subject」などのフィールドが空の場合に一致させる、ヘッダのキーワード表現はどのように指定すればいいですか？

トレンドマイクロでは、空のヘッダを表すキーワードの正規表現として、「^(\\s)*\$」を使用することをお勧めします。「^(\\s)*\$」は、空のヘッダまたは空白文字を表します。

たとえば、メッセージの「From」ヘッダが空白であるかどうか確認する場合、ルールの検索条件を次のように編集します。

手順

1. [ポリシー] > [ポリシーリスト] の順に選択します。
 2. 既存のルールをクリックして、ルールを編集します。
 3. [検索条件] リンクをクリックします。
 4. [内容] セクションの下にある [ヘッダのキーワード] をクリックします。
 5. [追加] をクリックして新しいキーワード表現を作成します。
 6. 内容を「`^(\s)*$`」として追加します。
-

メッセージサイズの検索条件が暗号化されたメッセージに対して適用されないのはなぜですか？

InterScan MSS では、暗号化されたメッセージは特別な種類のメッセージとして処理されます。ほとんどの検索条件が適用されません。暗号化されたメッセージに対して検索または処理を実行するには、暗号化されたメッセージの検索条件を使用する必要があります。

クラウドプレフィルタのトラブルシューティング

クラウドプレフィルタに接続できない

クラウドプレフィルタに接続できない場合、次のことを試してください。

- ・ テストセグメントにファイアウォールがある場合は、ファイアウォールでポート 9000 を介したアクセスが許可されることを確認します。ポート 9000 は、クラウドプレフィルタがクラウドサービスに接続するために使用する初期設定のポートです。ファイアウォールでそのポートへの接続が許可されない場合は、ポート 9000 を開いてください。
- ・ クラウドプレフィルタへの接続にプロキシサーバを使用しない場合は、InterScan MSS から次のコマンドを使用して、InterScan MSS でクラウドプレフィルタに接続できることを確認してください。


```
telnet ws.emailsecurity.trendmicro.com 9000
```

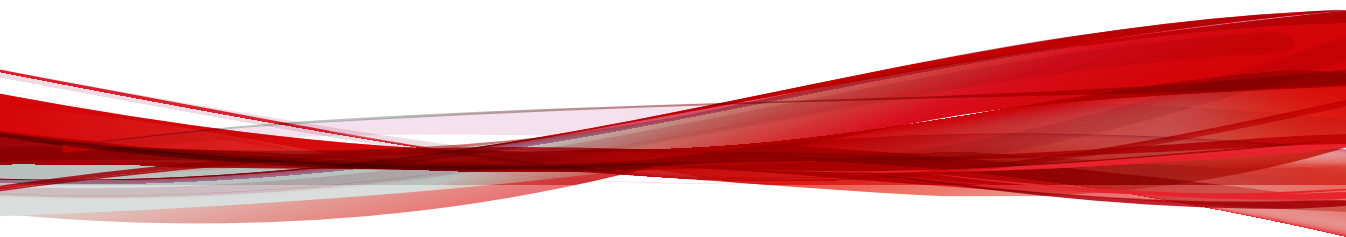
- ・ クラウドプレフィルタへの接続にプロキシサーバを使用する場合は、プロキシサーバでポート 9000 を介したアクセスが許可されることを確認してください。

クラウドプレフィルタからメッセージを受信できない

クラウドプレフィルタに接続はできるが、メッセージを受信できない場合、[クラウドプレフィルタポリシーリスト] 画面の [クラウドプレフィルタのサービス状況と定期メンテナンスのお知らせ] リンクをクリックして、クラウドプレフィルタのステータスを確認してください。

付録

付録



付録 A

テクニカルサポート

この付録では、トレンドマイクロの各種リソースとテクニカルサポートに関する情報について説明します。

この付録の内容は次のとおりです。

- ・ [530 ページの「トラブルシューティングのリソース」](#)
- ・ [531 ページの「製品サポート情報」](#)
- ・ [531 ページの「サポートサービスについて」](#)
- ・ [532 ページの「セキュリティニュース」](#)
- ・ [533 ページの「脅威解析・サポートセンター TrendLabs \(トレンドラボ\)」](#)

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/jp/technical-support>

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マニュー」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マニュー」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。

セキュリティニュース

トレンドマイクロ「セキュリティニュース」

トレンドマイクロでは、最新のセキュリティニュースをインターネットで公開しています。トレンドマイクロのセキュリティニュースでは、ウイルスやインターネットセキュリティに関する最新の情報を入手できます。セキュリティニュースは、次の URL からアクセスできます。

https://www.trendmicro.com/ja_jp/security-intelligence/breaking-news.html

- ・ ウイルス名やキーワードから検索できる脅威データベース
- ・ コンピュータウイルスの最新動向に関するニュース
- ・ 現在流行中のウイルスや不正プログラムの情報
- ・ デマウイルスまたは誤警告に関する情報
- ・ ウイルスやネットワークセキュリティの予備知識

セキュリティニュースに定期的にアクセスして、流行中のウイルス情報などを入手することをお勧めします。メールによる定期的なウイルス情報配信を希望する場合は、警告メール配信の登録フォームを利用してメールアドレスを登録してください。

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/jp/virus-and-threat-help>

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専門のスタッフが解析し、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。

脅威解析・サポートセンター TrendLabs (トレンドラボ)

TrendLabs (トレンドラボ) は、フィリピン・米国に本部を置き、日本・台湾・ドイツ・アイルランド・中国・フランス・イギリス・ブラジルの 10 カ国 12 か所の各国拠点と連携してソリューションを提供しています。

世界中から選び抜かれた 1,000 名以上のスタッフで 24 時間 365 日体制でインターネットの脅威動向を常時監視・分析しています。

付録 B

InterScan MSS スクリプト

この付録には、コマンドラインから実行する InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) スクリプトとそれに関連するパラメータの一覧が記載されています。

この付録の内容は次のとおりです。

- ・ [536 ページの「InterScan MSS スクリプトを使用する」](#)

InterScan MSS スクリプトを使用する

InterScan MSS スクリプトを使用することで、コマンドラインからも管理タスクを簡単に実行できます。

次の表に、InterScan MSS スクリプト、そのパラメータ、およびスクリプトが実行する機能の一覧を示します。



注意

表に記載されているすべてのスクリプトは、次の場所にあります。

`/$IMSS_Home/imss/script`

表 B-1. InterScan MSS スクリプト

スクリプト	パラメータ	説明
dbctl.sh	start / stop / status / reload / restart	Postgres データベースサービス
db_maintain.sh	{vacuum reindex analyze all} [vacuum] - 管理データベースとすべてのエンドユーザメール隔離データベースをクリーンアップします。 [reindex] - 管理データベースとすべてのエンドユーザメール隔離データベースのインデックスを再作成します。 [analyze] - 管理データベースとすべてのエンドユーザメール隔離データベースを解析します。 [all] - クリーンアップ、インデックスの再作成、および解析を実行します。	データベースをメンテナンスするために S99SCHEDULED によって使用されます。  注意 このスクリプトだけで実行しないでください。

スクリプト	パラメータ	説明
euqtrans	all / approved sender	エンドユーザメール隔離データベースのデータまたは承認済み送信者を転送します。
forceUpdate.sh	DBDSN ユーザ名パスワード	ポリシー設定を再読み込みするようにポリシーサーバに通知します。
foxproxyd	start / stop / restart	IP プロファイラサービス
ibe_server.sh	start / stop / restart	Trend Micro Email Encryption サービス
imssctl.sh	start / stop / stop_others / restart / restart_others / status	すべての InterScan MSS サービスを制御します。
imssstop.sh	stop	すべての InterScan MSS サービスを停止します。
imssstart.sh		すべての InterScan MSS サービスを開始します。
openldap.sh	start / stop / restart	OpenLDAP ローカルキャッシュサービス
postfixctl.sh	start / stop / reload / restart	Postfix デーモン
S99ADMINUI	start / stop / restart	セントラルコントローラ
S99CLEANEUQ		管理コンソールの [管理] > [ユーザメール隔離アクセス] での設定に従って、エンドユーザメール隔離データベースおよび管理データベースから期限切れの隔離データを削除します。
S99CLEANEXPIRE		管理コンソールの [隔離およびアーカイブ] > [設定] での設定に従って、エンドユーザメール隔離データベースおよび管理データベースから期限切れの隔離データおよびアーカイブされたデータを削除します。

スクリプト	パラメータ	説明
S99CMAGENT	start / stop / restart / unregister / isregistered	CMAgent サービス
S99DIGEST		エンドユーザメール隔離通知メッセージを送信します。
S99DTASAGENT	start / stop / restart	仮想アナライザエージェントサービス
S99EUQ	start / stop / restart	エンドユーザメール隔離サービス
S99FOXDNS	start / stop / restart	Foxdns サービス
S99IMSS	start / stop / restart	InterScan MSS 検索サービス
S99MANAGER	start / stop / restart	マネージャサービス
S99MONITOR	start / stop / restart	マネージャ監視サービス
S99POLICY	start / stop / restart	ポリシーサービス
S99REPORT	[option] start / stop / restart [option]: ・ -s: 一元化されたレポート機能を生成します (管理コンソールで設定された 1 回限りのレポートおよび予約レポートすべてを含みます)。 ・ -h: 1 時間ごとの個別のトラフィックデータを生成します。 ・ -t: 1 時間ごとのトラフィックデータを生成します。 ・ -d: データベースのログ管理を実行します。	関連するレポートを生成するために S99SCHEDULED によって使用されます。  注意 このスクリプトだけで実行しないでください。

スクリプト	パラメータ	説明
S99SCHEDULED	start / stop	予約タスクを開始します。
S99UPDATE	start / stop / restart	予約アップデートを実行するために S99SCHEDULED によって使用され ます。  注意 このスクリプトだけで実行しな いください。
S99WRSAGENT	start / stop / restart	Web レピュテーションサービスの エージェントサービス

付録 C

初期設定のディレクトリの場所

この付録では、InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) のメール処理で使用する初期設定のディレクトリの場所について説明します。

この付録の内容は次のとおりです。

- ・ 542 ページの「初期設定のメールキュー」
- ・ 543 ページの「コンテンツフィルタ、ウイルス、およびプログラムのログ」
- ・ 543 ページの「一時フォルダ」
- ・ 544 ページの「通知メールキュー」

初期設定のメールキュー

次の表は、InterScan MSS で管理するメールメッセージが保存されるさまざまなメールディレクトリを示しています。

表 C-1. 初期設定の InterScan MSS メール場所

通常のメールのキュー	大きいメールのキュー	説明
queue_malform= /opt/trend/imss/queue/ malform	該当なし	正しくない形式のメッセージを保存します。
queue_archive= /opt/trend/imss/queue/ archive	該当なし	アーカイブされたメッセージを保存します。
queue_quarantine = /opt/trend/imss/queue/ quarantine	該当なし	隔離されたメッセージを保存します。
queue_notify= /opt/trend/imss/queue/ notify	queue_notify_big= /opt/trend/imss/queue/ notifybig	通知メッセージを保存します。
queue_postpone= /opt/trend/imss/queue/ postpone	queue_postpone_big= /opt/trend/imss/queue/ postponebig	保留されたメッセージを保存します。
queue_deliver= /opt/trend/imss/queue/ deliver	queue_deliver_big= /opt/trend/imss/queue/ deliverbig	最終配信のメッセージを保存します。
queue_reprocess= /opt/trend/imss/queue/ reprocess	queue_reprocess_big= /opt/trend/imss/queue/ reprocessbig	再処理が保留中のメッセージを保存します。

通常のメールのキュー	大きいメールのキュー	説明
queue_handoff= /opt/trend/imss/queue/ handoff	queue_handoff_big= /opt/trend/imss/queue/ handoffbig	中継が保留中のメッセージを保存します。
queue_undeliverable= /opt/trend/imss/queue/ undeliverable	該当なし	配信できなかったメッセージを保存します。
queue_unnotify= /opt/trend/imss/queue/ unnotify	該当なし	配信できなかった通知メッセージを保存します。
/opt/trend/imss/queue/ dtas_upload	該当なし	分析を保留中、または仮想アナライザで分析中のメッセージを保存します。

コンテンツフィルタ、ウイルス、およびプログラムのログ

InterScan MSS の多くのモジュールでは、トラブルシューティングのためのログ情報が次のフォルダに書き込まれます。

- ・ /opt/trend/imss/log
- ・ /var/log

一時フォルダ

InterScan MSS では、アプリケーションによって生成されたすべての一時ファイルが次の一時フォルダに保存されます。

- ・ /opt/trend/imss/temp/
- ・ /tmp

**注意**

このディレクトリの設定は変更できません。

通知メールキュー

InterScan MSS では、次のフォルダにすべての通知メッセージが保存され、そこから選択されたメッセージが指定された SMTP 通知サーバに配信されます。

```
/opt/trend/imss/queue/notify/
```

および

```
/opt/trend/imss/queue/notifybig
```

SMTP 通知サーバを設定する

詳細については、[147 ページの「SMTP を設定する」](#)を参照してください。

手順

- ・ [管理] > [通知] > [通知設定] の順に選択します。

**注意**

queue_notify_big キューは大きいメールメッセージ用です。

索引

シンボル

1 回限りのレポート
管理, 359

アルファベット

APOP, 168

Control Manager

Trend Micro Control Manager 参照, 38

エージェントの有効化, 432

設定の複製, 433

Control Manager サーバの設定

設定, 66

Control Manager の設定

設定, 471

DHA 設定

設定, 137

DLP, 206

DLP コンプライアンステンプレート

(DLP), 206

Email Encryption

ドメインの管理, 102

ドメインの登録, 103

理解, 100

Email Encryption 用のドメインの管理,

102

Email Encryption 用のドメインの登録,

103

ERS

MTA 設定, 129

使用, 128

FAQ

ERS, 507

InterScan MSS コンポーネント, 506

IP プロファイラ, 508

Postfix, 505

エンドユーザメール隔離, 512

キュー, 510

メール領域, 510

IMSA

scripts, 536

InterScan MSS について, 22

InterScan MSS

scripts, 536

概要, 22

バックアップ, 428

復元, 430

IP プロファイラ

有効化, 130

LDAP 設定

設定, 60, 463

LDAP ユーザまたはグループ

検索, 244

MIME コンテントタイプ

検索条件, 290

MTA

メールレピュテーションサービス
で使用, 129

PCRE, 208

Perl Compatible Regular Expressions, 208

POP3 検索

有効化, 167

POP3 設定

設定, 168, 468

POP3 メッセージ

検索, 166

Smart Protection, 42, 248, 252

ソース, 252

比較, 252

プロトコル, 252

Smart Protection Network, 44, 249

SMTP

通知サーバ, 544

SMTP 設定

設定, 147

SMTP メッセージ

検索, 146

SMTP ルーティング, 147

設定, 146

Trend Micro Control Manager, 38

エージェント, 38

サーバ, 38

Web レピュテーションサービス, 43, 248

あ

アクティベート

製品, 480

ライセンス, 479

アスタリスクワイルドカード

使用, 337

アップデート

検索エンジン, 70

システムとアプリケーション, 484

自動, 75

手動, 72

パターンファイル, 70

アップデート元

指定, 71

設定, 58

アドウェア, 33

アドレスグループ

削除, 187

追加, 184

編集, 187

理解, 181

例, 181

暗号化の設定

設定, 310

アーカイブ

設定, 390

アーカイブされたメッセージ

表示, 406

アーカイブ領域

管理, 395

イベント条件

設定, 415

イベント条件の設定, 415

イベント通知, 412

インポートの注意, 426

ウィジェット

ウィジェットの設定, 352

ウィジェットの追加, 354

ウィジェットの編集, 353

ウィジェットを使用する, 351

理解, 351

ウイルス設定

設定, 135

ウイルス対策ルール, 267

エクスポートの注意, 426

エンドユーザアクセス

有効化, 445

エンドユーザメール隔離, 438

開始, 443

管理コンソール, 53, 449

コンソールを開く, 449

認証, 438

無効化, 452

有効, 439

エンドユーザメール隔離通知

設定, 418

か

開始

エンドユーザメール隔離, 443

- 隔離
 - 設定, 390
- 隔離されたメッセージ
 - 表示, 404
- 隔離とアーカイブ, 390
- 隔離領域
 - 管理, 392
- カスタマイズされたキーワード, 218
 - インポート, 221
 - 条件, 218, 219
- カスタマイズされた式, 208, 209, 213
 - インポート, 213
 - 条件, 209
- カスタマイズされたテンプレート, 222
 - インポート, 225
 - 作成, 224
- 仮想アナライザ, 92
- 仮想アナライザのキューのメッセージ
 - 表示, 408
- 管理
 - 1 回限りのレポート, 359
 - 管理者アカウント, 458
 - キーワードリスト, 192
 - 製品ライセンス, 476
 - 通知リスト, 226
- 管理コンソールのパスワード
 - 変更, 49
- 管理者アカウント
 - 管理, 458
 - 削除, 461
 - 追加, 458
 - 編集, 461
- 既知のホスト, 160
 - インポート, 162
 - エクスポート, 163
 - 追加, 161
- 許可された送信者, 154
- キーワード, 206, 216
 - カスタマイズ, 218, 219, 221
 - 設定, 193
 - 定義済み, 217
- キーワードリスト
 - 管理, 192
- クエリ
 - MTA イベントログ, 387
 - URL クリックの追跡ログ, 385
 - アーカイブ領域, 400
 - 隔離イベントログ, 384
 - 隔離領域, 398
 - 仮想アナライザのキューのメッセージ, 403
 - システムイベントログ, 379
 - 送信者フィルタログ, 387
 - ポリシーイベントログ, 381
 - 保留されたメッセージ, 402
 - メッセージ, 397
 - ログ, 372
- クラウドプレフィルタ
 - DNS の MX レコードの設定, 122
 - アカウントの作成, 83
 - 推奨される設定, 123
 - 動作の確認, 122
 - トラブルシューティング, 524
 - ポリシー, 110
 - ポリシーの作成, 112
 - 理解, 80
- [クラウドプレフィルタ] タブ, 349
- グレーメール, 45
- 検索
 - POP3 メッセージ, 166
 - SMTP メッセージ, 146
- 検索エンジン
 - アップデート, 70
- 検索条件, 290

- MIME コンテンツタイプ, 290
- 拡張子, 289
- 実際のファイルタイプ, 290
- 指定, 267
 - スパムメール, 274
- 添付ファイル, 289
- 添付ファイルサイズ, 291
- 添付ファイル数, 291
- 添付ファイル名, 289
- メッセージサイズ, 292
- 検索除外
 - 設定, 314
- 検索処理
 - 暗号化されたメッセージの設定, 320
 - 他の検索除外の設定, 317, 321
- 検索方法, 254
- 件名タグ
 - 追加, 304
- 更新
 - ライセンス, 479
- 高度な脅威検索エンジン, 90
- コマンド, 536
- 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, 46
- コンポーネントのアップデート, 74
- さ**
- 削除
 - アドレスグループ, 187
 - 管理者アカウント, 461
- サービス, 52
 - 送信者フィルタサービス, 128
- 式, 206, 207
 - カスタマイズ, 208, 213
 - 条件, 209
 - 定義済み, 207, 208
- [システムステータス] 画面, 342
- [システムの概要] タブ, 347
- 実際のファイルタイプ, 290
- 指定
 - アップデート元, 71
 - 検索条件, 267
 - 処理, 297
 - ルート, 260
- 従来型スキャン, 254
- 手動アップデート, 72
- 条件
 - カスタマイズされた式, 209
 - キーワード, 218, 219
- 条件文, 223
- 承認済み送信者リスト
 - 設定, 276
- 承認済みリスト
 - ホストの追加, 131
- 情報漏えい対策, 206
 - キーワード, 216-219, 221
 - 式, 207-209, 213
 - テンプレート, 222-225
 - データ識別子, 206
 - ファイル属性, 213, 215
- 初期設定のタブ, 347
- ジョークプログラム, 33
- 新機能, 14
- スパイウェア/グレーウェア, 33
 - アドウェア, 33
 - ジョークプログラム, 33
 - ダイヤラー, 33
 - ネットワークへの侵入, 33
 - パスワード解読アプリケーション, 33
 - ハッキングツール, 33
 - リスクと脅威, 34
 - リモートアクセスツール, 33

- スパムメール設定
 - 設定, 134
- スパムメールテキスト除外ルール
 - 設定, 277
- スマートスキャン, 254
- 生成
 - レポート, 356
- 製品サービス, 52
- 製品設定
 - 設定, 67
- 製品ライセンス
 - 管理, 476
 - 表示, 477
- セキュリティ設定違反
 - 検索処理の設定, 316
 - 除外設定, 315, 319
- セキュリティリスク
 - スパイウェア/グレーウェア, 33
- 接続設定
 - 設定, 148, 462
- 設定
 - Control Manager サーバの設定, 66
 - Control Manager の設定, 471
 - DHA 設定, 137
 - DNS の MX レコード, 122
 - LDAP 設定, 463
 - POP3 設定, 168, 468
 - SMTP 設定, 147
 - SMTP ルーティング, 146
 - アップデート元, 58
 - 暗号化されたメッセージの検索処理, 320
 - 暗号化の設定, 310
 - アーカイブ設定, 390
 - エンドユーザメール隔離通知の設定, 418
 - 隔離設定, 390
 - キーワード, 193
 - 検索除外, 314
 - 承認済み送信者リスト, 276
 - スパムメールテキスト除外ルール, 277
 - 製品設定, 67
 - セキュリティ設定違反除外, 315, 319
 - セキュリティ設定違反の検索処理, 316
 - 接続設定, 148, 462
 - 送信者フィルタ, 130
 - 送信者フィルタウイルス設定, 135
 - 送信者フィルタスパムメール設定, 134
 - 送信者フィルタバウンスメール設定, 140
 - 他の検索除外の検索処理, 317, 321
 - 通知設定, 56, 412
 - 通知メッセージ, 415
 - データベースのメンテナンススケジュール, 475
 - 内部アドレス, 64, 240
 - ブロックする送信者リスト, 276
 - メッセージ配信設定, 156
 - メッセージルールの設定, 152
 - メールレピュテーション, 141
 - 予約レポート, 362
 - ルート, 264
 - ログの設定, 370
- 設定ウィザード
 - アクセス, 56
- 設定の複製, 432
- 送信者フィルタ
 - DHA 設定の指定, 137
 - ウイルス設定の指定, 135
 - スパムメール設定の指定, 134
 - 設定, 130

バウンスメール設定の指定, 140
送信者フィルタサービス
 概要, 128
[送信者フィルタ] タブ, 349
その他のルール, 269

た

対象読者, 17
ダイヤラー, 33
ダッシュボード
 使用, 346
タブ
 クラウドプレフィルタ, 349
 システムの概要, 347
 初期設定のタブ, 347
 送信者フィルタ, 349
 タブの設定, 350
 タブを追加する, 349
 メッセージトラフィック, 348
 理解, 346

注意

インポート, 426
エクスポート, 426

追加

管理者アカウント, 458

通知

イベント, 412

通知設定

設定, 56, 412

通知メッセージ

設定, 415

通知リスト

管理, 226

定義済みテンプレート, 222

定義済みのキーワード

間隔, 217
キーワード数, 217

定義済みの式, 207

表示, 208

添付ファイルサイズ

検索条件, 291

テンプレート, 222-225

カスタマイズ, 222, 224, 225

条件文, 223

定義済み, 222

論理演算子, 223

データ識別子, 206

キーワード, 206

式, 206

ファイル属性, 206

データベース

メンテナンススケジュールの設定,
475

ドキュメント, 17

ドメイン

Email Encryption, 102, 103

表示, 143

トラブルシューティング, 488

imssps デーモン, 489

トランスポート層, 151

な

内部アドレス

設定, 64, 240

は

バウンスメール設定

設定, 140

パスワード

管理コンソール, 49

パスワード解読アプリケーション, 33

パターンファイル

アップデート, 70

ハッキングツール, 33

- バックアップ
 - InterScan MSS, 428
- 表現
 - 正規, 200
- 表示
 - アーカイブされたメッセージ, 406
 - 隔離されたメッセージ, 404
 - 仮想アナライザのキューのメッセージ, 408
 - 製品ライセンス, 477
 - ドメイン, 143
 - 不審な IP アドレス, 143
 - 保留されたメッセージ, 407
- ファイル属性, 206, 213, 215
 - インポート, 215
 - 作成, 215
 - ワイルドカード, 215
- ファイルレピュテーションサービス, 43, 248
- フィルタ
 - 例, 181
- フィルタ、機能, 28
- 復元
 - InterScan MSS, 430
- 不審な IP アドレス
 - 表示, 143
- ブロックする送信者リスト
 - 設定, 276
- ブロックリスト
 - レコードの追加, 132
- 変更
 - 管理コンソールのパスワード, 49
- 編集
 - アドレスグループ, 187
 - 管理者アカウント, 461
- ポリシー
 - 完成, 304
 - 追加, 260
 - 例 1, 327
- ポリシー管理
 - DLP, 206
- ポリシー通知
 - 追加, 227
 - 編集, 227
- 保留されたメッセージ
 - 表示, 407
- ま
- マスメーリング型ウイルス
 - パターン, 27
- メッセージサイズ
 - 検索条件, 292
- [メッセージトラフィック] タブ, 348
- メッセージの暗号化, 311
- メッセージ配信, 156
- メッセージ配信設定
 - 設定, 156
- メッセージルールの設定
 - 設定, 152
- メール脅威
 - スパム, 26
 - 非生産的メッセージ, 26
- メールリレー, 152
- メールレピュテーション
 - 概要, 35
 - 管理コンソール, 129
 - 種類, 35
 - 設定, 141
 - 有効化, 130
- や
- 有効
 - エンドユーザメール隔離, 439
 - 送信者フィルタルール, 133

- メールレピュテーション, 130
- 有効化
 - Control Manager エージェント, 432
 - IP プロファイラ, 130
 - POP3 検索, 167
 - エンドユーザアクセス, 445
- 予約アップデート, 75
- 予約レポート
 - アクセス, 362
 - 使用, 366
 - 設定, 362

ら

- ライセンス
 - アクティベート, 479
 - 更新, 479
- 理解
 - Email Encryption, 100
 - ウィジェット, 351
- リモートアクセスツール, 33
- ルート
 - 指定, 260
 - 設定, 264

- レポート
 - 1 回限りの管理, 359
 - 生成, 356
 - 内容, 356
 - 予約レポート, 362, 366

- ログ, 370
 - MTA イベントのクエリ実行, 387
 - URL クリックの追跡のクエリ, 385
 - 隔離イベントのクエリ, 384
 - クエリ, 372
 - システムイベントのクエリ実行, 379
 - 設定の指定, 370
 - 送信者フィルタのクエリ, 387

- ポリシーイベントのクエリ実行, 381
- メッセージ追跡のクエリ実行, 377
- 論理演算子, 223
- ロールバック
 - コンポーネント, 74

わ

- ワイルドカード, 215
- ファイル属性, 215