TREND MICRO

InterScan Messaging Security Suite™ 9.1

インストールガイド

Messaging Security

※注意事項

複数年契約について

- お客さまが複数年契約（複数年分のサポート費用前払い）された場合でも、各製品のサポート期間については、当該契約期間によらず、製品ごとに設定されたサポート提供期間が適用されます。
- 複数年契約は、当該契約期間中の製品のサポート提供を保証するものではなく、また製品のサポート提供期間が終了した場合のバージョンアップを保証するものではありませんのでご注意ください。
- 各製品のサポート提供期間は以下のWebサイトからご確認いただけます。
  http://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ナップサービス、Deep Discovery、TCSE、おまかせインストール・バージョンアップ、Trend Micro Safe Lock、Deep Discovery Inspector、Trend Micro Mobile App Reputation、Jewelry Box、InterScan Messaging Security Suite Plus、おもいでバックアップサービス、おまかせ！スマホお探しサポート、保険&デジタルライフサポート、おまかせ！迷惑ソフトクリーンナップサービス、InterScan Web Security as a Service、Client/Server Suite Premium、Cloud Edge、Trend Micro Remote Manager、Threat Defense Expert、Next Generation Threat Defense、Trend Micro Smart Home Network、Retro Scan、is702、デジタルライフサポート プレミアム、Airサポート、Connected Threat Defense、ライトクリーナー、Trend Micro Policy Manager、フォルダシールド、トレンドマイクロ認定プロフェッショナルトレーニング、Trend Micro Certified Professional、TMCP、XGen、InterScan Messaging Security、InterScan Web Security、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: MSEM77874_170627_JP_R2 (2019/01)

目次

本書について

本書について 7
新機能 8
対象読者 11
InterScan Messaging Security Suite ドキュメント 11
ドキュメントの表記規則 12

第 1 章：InterScan Messaging Security Suite の概要

InterScan MSS について 14
InterScan MSS の主な特長と利点 14
クラウドプレフィルタについて 24
スパイウェアと他の種類のグレーウェアについて 25
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 25
潜在的なリスクと脅威 26
Web レピュテーションサービスについて 27
メールレピュテーションについて 27
メールレピュテーションの種類 27
メールレピュテーションテクノロジの仕組み 29
Trend Micro Control Manager について 30
Control Manager のサポート 31
トレンドマイクロの Smart Protection について 34
新しいソリューションの必要性 35
Trend Micro Smart Protection Network 36
グレーメールの検索について 37
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 38

第 2 章：コンポーネントの説明

InterScan MSS コンポーネントについて 40
クラウドプレフィルタサービスの概要 40
送信者のフィルタ 40
レピュテーションベースの送信元のフィルタ 40
ウイルスおよびスパムメールからの保護 41
スパムメール対策 (コンテンツ検索) について 41
スパムメール対策 (コンテンツ検索) テクノロジ 41
スパムメール対策 (コンテンツ検索) の使用 41
送信者フィルタについて 42
IP プロファイラの機能 42
エンドユーザメール隔離について 43
一元化されたレポート機能について 44

第 3 章：配置計画

配置タスクのチェックリスト 46
InterScan MSS ポート 49
ネットワークトポロジの考慮事項 52
ファイアウォールなしで配置する 53
ファイアウォールの外側にインストールする 54
ファイアウォールの内側へインストールする 55
既存の SMTP ゲートウェイ上にインストールする 56
DMZ (非武装地帯) 内へインストールする 57
デバイスの役割について 58
デバイスサービスについて 59
サービスの選択 59
送信者フィルタを使用して配置する 60
POP3 メール検索を理解する 60
POP3 検索の要件 61
InterScan MSS を経由してメールを受信する POP3 クライアントを設定する 61
InterScan MSS の管理コンソールを開く 62

運用モデルについて 63
スタンドアロンモデル 63
サンドイッチモデル 66

第 4 章：インストールおよびアンインストール

システム要件 72

MTA を準備する 72
Postfix を準備する 72
Sendmail について 74

InterScan MSS をインストールする 81

送信者フィルタを Sendmail とともに使用する 83
Red Hat 6 で FoxLib を Sendmail と統合する 83
Red Hat 7 で FoxLib を Sendmail と統合する 86

インストールを確認する 88

IPv6 サポートについて 89
サーバを IPv6 対応に設定する 90
InterScan MSS を IPv6 対応に設定する 91

InterScan MSS をアンインストールする 94

第 5 章：以前のバージョンからのアップグレード

体験版からアップグレードする 98

InterScan MSS Linux 9.1 にアップグレードする 100
データ転送の注意事項 100
InterScan MSS 7.1 Linux 版 SP2 Patch 1 から InterScan MSS 9.1 Linux 版にアップグレードする 101

以前のバージョンから移行する 115
InterScan MSS Linux 9.1 に移行する 116
デバッグログをエクスポートする 119

第 6 章：FAQ

Postfix MTA 設定 122
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。 122

インストールまたはアンインストール 122
外部 DNS サーバを使用するコンピュータに InterScan MSS 9.1 をインストールした場合、何か問題がありますか。 123
既存の Apache サーバを使用するコンピュータに InterScan MSS 9.1 をインストールした場合、何か問題がありますか。 123

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 126
サポートポータルの利用 126
脅威データベース 126
製品サポート情報 127
サポートサービスについて 127
セキュリティニュース 128
脅威解析・サポートセンター TrendLabs (トレンドラボ) 129

索引

索引 131

はじめに

本書について

Trend Micro InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) のインストール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、さらに InterScan MSS のインストールおよび設定のアップグレード手順について説明します。

InterScan MSS の設定手順については、*InterScan MSS 9.1 管理者ガイド*を参照してください。また、ユーザインタフェースの各フィールドの詳細については、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。

この章の内容は次のとおりです。

- 8 ページの「新機能」
- 11 ページの「対象読者」
- 11 ページの「InterScan Messaging Security Suite ドキュメント」
- 12 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。

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 — 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

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。

- 14 ページの「InterScan MSS について」
- 14 ページの「InterScan MSS の主な特長と利点」
- 24 ページの「クラウドプレフィルタについて」
- 25 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」
- 27 ページの「Web レピュテーションサービスについて」
- 27 ページの「メールレピュテーションについて」
- 30 ページの「Trend Micro Control Manager について」
- 34 ページの「トレンドマイクロの Smart Protection について」
- 37 ページの「グレーメールの検索について」
- 38 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ルールの設定に応じて、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。	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ことがあります。そのため、クリーンナ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、TrendLabs℠ (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ナ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、25 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、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、27 ページの「標準」と28 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、

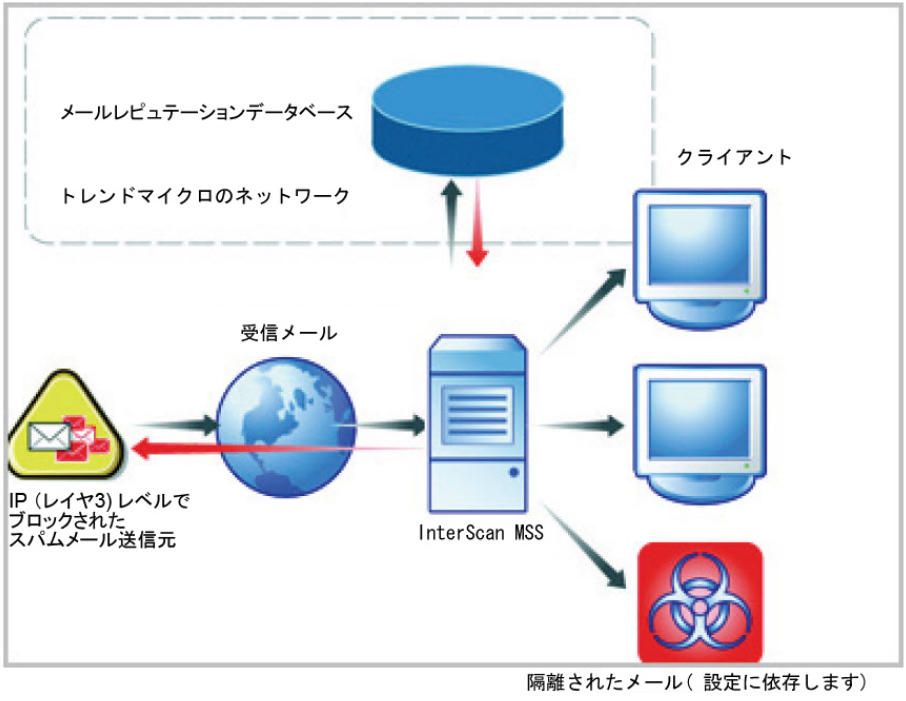
受信メールストリームに占めるスパムメールの量により異なります。受信するスパムメールが多いほど、ブロックされる接続の割合は高くなります。

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相関分析テクノロジおよび脅威データベースにアクセスすることで、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きます。

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の条件を定義します。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

コンポーネントの説明

この章では、製品の管理に必要な要件、および製品が機能するために必要なさまざまなソフトウェアコンポーネントについて説明します。

この章の内容は次のとおりです。

- 40 ページの「InterScan MSS コンポーネントについて」
- 40 ページの「クラウドプレフィルタサービスの概要」
- 41 ページの「スパムメール対策 (コンテンツ検索) について」
- 42 ページの「送信者フィルタについて」
- 43 ページの「エンドユーザメール隔離について」
- 44 ページの「一元化されたレポート機能について」

InterScan MSS コンポーネントについて

InterScan MSS の新しいアーキテクチャでは、メッセージ処理で実行される特定のタスクごとに、この製品を個別のコンポーネントに分類しています。次の項では、それぞれのコンポーネントの概要について説明します。

InterScan MSS コンポーネントは、1 台または複数のコンピュータにインストールできます。

クラウドプレフィルタサービスの概要

クラウドプレフィルタサービスは、トレンドマイクロのメールセキュリティプラットフォーム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、不正プログラムなど、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。

送信者のフィルタ

クラウドプレフィルタサービスの契約者は、送信者を承認することによって、信頼されたメールサーバやメールアドレスからのメッセージを自動的に許可できます。承認された送信者からのメッセージでは、スパムメールまたは送信元のレピュテーションがチェックされることはありません。承認された送信者からのメッセージは、ウイルスについて検索されます。

送信者をブロックすることにより、契約者は信頼されない送信元からのメッセージを自動的にブロックできます。

レピュテーションベースの送信元のフィルタ

トレンドマイクロのメールレピュテーションにより、クラウドプレフィルタサービスは、メールの送信元を動的な自己更新型のレピュテーションデータベースに対して検証することで、スパムメール/フィッシング詐欺メールの送

信者や不正プログラムの配布元によって制御された IP アドレスからのメッセージ、および最新のボットネットからのメッセージをブロックします。

ウイルスおよびスパムメールからの保護

トレンドマイクロのウイルス対策テクノロジにより、クラウドプレフィルタサービスは、マスメーリングワームによる感染メッセージ、またはトロイの木馬やスパイウェアなどの不正プログラムコードを含む手動で作成されたメッセージからユーザを保護します。

クラウドプレフィルタサービスは、メッセージ内のスパムメールの特性をチェックして、迷惑メールの数を効果的に減らします。

スパムメール対策 (コンテンツ検索) について

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) 機能をインストールすることもできます。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。

スパムメール対策 (コンテンツ検索) テクノロジ

スパムメール対策 (コンテンツ検索) では、最新のコンテンツ処理および統計分析に基づく検出テクノロジが使用されています。スパムメール識別の他の手法とは異なり、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となっています。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。

スパムメール対策 (コンテンツ検索) の使用

スパムメール対策 (コンテンツ検索) は、組み込みのスパムメールフィルタを通じて機能します。このフィルタは、スパムメール対策 (コンテンツ検索) 用の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。

送信者フィルタについて

InterScan MSS には、オプションの送信者フィルタも搭載されています。これは、次の 2 つの機能で構成されます。

IP プロファイラ

メールトラフィックの解析に使用するしきい値を設定できます。ある IP アドレスから送信されたトラフィックがこの設定に違反している場合、IP プロファイラはその送信者の IP アドレスを自身のデータベースに追加して、同じ IP アドレスからの接続要求をブロックします。

IP プロファイラは、次の 4 つの潜在的なインターネット脅威のいずれかを検出します。

- スパムメール: 不要な広告コンテンツが含まれるメールメッセージです。
- 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): 有効なドメイン名とランダムなメール名の組み合わせを使用してランダムなメールアドレスを生成することによって、有効なメールアドレスを収集するためにスパムメール送信者が使用する手段。生成されたメールアドレスにメールが送信されます。メールメッセージが配信されると、そのメールアドレスが本物であると判断され、スパムメールデータベースに追加されます。
- バウンスメール: メールサーバを使用して、差出人フィールドにターゲットのメールドメインを挿入したメールメッセージを生成する攻撃。偽アドレスにメールメッセージが送信され、それらが戻されます。これにより、メールサーバを氾濫させます。

メールレピュテーション

既知のスパムメール送信者からのメールを IP レベルでブロックします。

IP プロファイラの機能

IP プロファイラは、42 ページの「送信者フィルタについて」の項で説明した脅威を含むメールメッセージを送信したコンピュータの IP アドレスを能動

的に特定します。InterScan MSS でいつ IP アドレスに対して指定の処理を開始するかは、いくつかの条件をカスタマイズすることで指定できます。条件は潜在的な脅威に応じて異なりますが、InterScan MSS が IP アドレスとしきい値を監視する期間はいずれも共通です。

これを実行するために、IP プロファイラはいくつかのコンポーネントを使用します。その中で最も重要なのは、Foxproxy です。これは、メールトラフィックに関する情報を InterScan MSS に中継するサーバです。

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. FoxProxy が IP プロファイラの DNS サーバに問い合わせを行い、ブロックするリストに IP アドレスが含まれているかどうかを確認します。
2. ブロックリストに IP アドレスが含まれている場合は、InterScan MSS が接続要求を拒否します。

   ブロックリストに IP アドレスが含まれていない場合、InterScan MSS が、IP プロファイラに指定されたしきい値の条件に従ってメールトラフィックを解析します。
3. メールトラフィックが条件に違反している場合、InterScan MSS はその送信者の IP アドレスをブロックリストに追加します。

エンドユーザメール隔離について

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スパムメールの隔離方法を管理できます。スパムメール対策 (コンテンツ対策)、または管理者が作成したコンテンツフィルタによって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。

一元化されたレポート機能について

InterScan MSS の稼働状況を解析するために、一元化されたレポート機能を使用できます。レポートは、必要に応じてそのつど作成するように設定することも、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。

第 3 章

配置計画

この章では、InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) の配置計画の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。

- 46 ページの「配置タスクのチェックリスト」
- 49 ページの「InterScan MSS ポート」
- 52 ページの「ネットワークトポロジの考慮事項」
- 58 ページの「デバイスの役割について」
- 59 ページの「デバイスサービスについて」
- 60 ページの「POP3 メール検索を理解する」
- 62 ページの「InterScan MSS の管理コンソールを開く」
- 63 ページの「運用モデルについて」

配置タスクのチェックリスト

配置タスクのチェックリストには、InterScan MSS の配置について、インストール前とインストール後の段階的な手順が示されています。

1. InterScan MSS の配置場所の決定

完了したらチェックマークを記入	タスク	オプションかどうか	参照先
	InterScan MSS をネットワーク上のどの位置に配置するかを、次の中から選択します。		
	ファイアウォールなし		53 ページの「ファイアウォールなしで配置する」
	ファイアウォールの外側		54 ページの「ファイアウォールの外側にインストールする」
	ファイアウォールの内側		55 ページの「ファイアウォールの内側へインストールする」
	既存の SMTP ゲートウェイ上		56 ページの「既存の SMTP ゲートウェイ上にインストールする」
	DMZ (非武装地帯) 内		57 ページの「DMZ (非武装地帯) 内へインストールする」

2. インストールまたはアップグレード

完了したらチェックマークを記入	タスク	オプションかどうか	参照先
	InterScan MSS の新規インストールまたは以前のバージョンからのアップグレードを実行します。		
	MTA の準備		72 ページの「MTA を準備する」
	InterScan MSS コンポーネントのインストール		81 ページの「InterScan MSS をインストールする」
	以前のバージョンからのアップグレード		97 ページの以前のバージョンからのアップグレード
	正常なインストールの確認		88 ページの「インストールを確認する」

3. InterScan MSS の基本設定

完了したらチェックマークを記入	タスク	オプションかどうか	参照先
	設定ウィザードを使用してセントラルコントローラを設定します。		
	設定ウィザードを使用した設定		「管理者ガイド」の設定ウィザードでの基本設定の実行に関する項

4. サービスの開始

完了したらチェックマークを記入	タスク	オプションかどうか	参照先
	InterScan MSS の各サービスを有効にし、さまざまな脅威に対するネットワークの保護を開始します。		

完了したらチェックマークを記入	タスク	オプションかどうか	参照先
	検索サービス		「管理者ガイド」の InterScan MSS サービスに関する項
	ポリシー		
	エンドユーザメール隔離	オプション	

5. その他の InterScan MSS の設定

完了したらチェックマークを記入	タスク	オプションかどうか	参照先
	InterScan MSS の起動および実行に必要な各種項目を設定します。		
	送信者フィルタルール	オプション	「管理者ガイド」の送信者フィルタサービスに関する項
	SMTP ルーティング		「管理者ガイド」の SMTP メッセージの検索に関する項
	POP3 設定	オプション	「管理者ガイド」の POP3 メッセージの検索に関する項
	ポリシーおよび検索の除外		「管理者ガイド」のポリシーの管理に関する項 **注意** グレーメールメッセージを検索する場合は、DNS 設定と DNS クエリが正しいことを確認してください。
	コンポーネントの手動アップデートの実行および予約アップデートの設定		「管理者ガイド」の検索エンジンおよびパターンファイルのアップデートに関する項

完了したらチェックマークを記入	タスク	オプションかどうか	参照先
	ログ設定		「管理者ガイド」のログの設定に関する項

6. InterScan MSS のバックアップ

完了したらチェックマークを記入	タスク	オプションかどうか	参照先
	システムの障害時に備えて InterScan MSS の全体または最小限のバックアップを実行します。		
	全体のバックアップ		「管理者ガイド」の InterScan MSS のバックアップに関する項
	最小限のバックアップ		

InterScan MSS ポート

InterScan MSS が使用するポートについては次の表を参照してください。

表 3-1. 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	Postfix のメール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。	master.cf

ポート番号	コンポーネントと役割	設定場所
953	IP フィルタのサービスポートです。	InterScan MSS サーバでは設定できません。
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 要求を受け入れ、POP3 メールを検索します。	`imss.ini / [Socket_2]/ proxy_port`
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。	管理コンソールのメニューから、[管理] > [InterScan MSS の設定] > [接続] > [コンポーネント] の順にクリックします。
8005	Tomcat の管理コマンドを操作できる Admin Web サーバ (Tomcat) の管理ポートです。	`{IMSS}/UI/adminUI/conf/ server.xml:Server / port`
8009	エンドユーザメール隔離コンソールの 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。	`{IMSS}/UI/euqUI/conf/ server.xml:Server / Service / Connector (protocol=AJP/1.3) / port`
8015	Tomcat の管理コマンドを操作できる Tomcat の管理ポートです。	`{IMSS}/UI/euqUI/conf/ server.xml:Server/port`
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オンするには、このポートを開放します。	Tomcat 待機ポート: `{IMSS}/UI/adminUI/conf/ server.xml:Server / Service / Connector / port`
8446	エンドユーザメール隔離サービスの待機ポートです。	`{IMSS}/UI/euqUI/conf/ server.xml:Server / Service / Connector / port`
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。	`{IMSS}/UI/euqUI/conf/ EUQ.conf:Listen / VirtualHost / ServerName`

ポート番号	コンポーネントと役割	設定場所
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やエンドユーザメール隔離データベースから隔離解除されたメッセージは、このポートを通して送信され再処理されます。	`imss.ini / [Socket_3]/ proxy_port`
10025	InterScan MSS 検索サービスの検索ポートです。このポートを通して送信されたすべてのメッセージは、検索サービスによって検索されます。	`imss.ini / [Socket_1]/ proxy_port`
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。 このポートを通して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) で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。	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メール隔離管理コンソールに提供します。	管理コンソールのメニューから、[管理] > [InterScan MSS の設定] > [接続] > [コンポーネント] の順にクリックします。

ポート番号	コンポーネントと役割	設定場所
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。		
389	LDAP サーバの待機ポートです。	InterScan MSS サーバでは設定できません。
5432	PostgreSQL データベースの待機ポートです。別のポート番号を割り当てないでください。	このポートは変更できません。
80	Microsoft IIS HTTP の待機ポートです。Control Manager を使用して InterScan MSS を管理する際に、InterScan MSS からこのポートに対する通信が行われます。	管理コンソールのメニューから、[管理] > [InterScan MSS の設定] > [接続] > [Control Manager サーバ] の順にクリックします。
443	Microsoft IIS HTTPS の待機ポートです。Control Manager を使用して InterScan MSS を管理する際に、InterScan MSS からこのポートに対する通信が行われます。	管理コンソールのメニューから、[管理] > [InterScan MSS の設定] > [接続] > [Control Manager サーバ] の順にクリックします。
88	Kerberos レルムの鍵発行局 (KDC) ポートです。	InterScan MSS サーバでは設定できません。
53	BIND サービスの待機ポートです。別のポート番号を割り当てないでください。	InterScan MSS サーバでは設定できません。

ネットワークトポロジの考慮事項

この項では、ネットワーク上のファイアウォールの位置に基づいて InterScan MSS を配置する、さまざまな方法について説明します。

既存のメッセージング環境の SMTP ゲートウェイに InterScan MSS を配置します。この項では、さまざまなネットワークトポロジにおける InterScan MSS の適切な配置場所について、各シナリオの図および他のゲートウェイサービスの一般的な設定方法を交えて説明します。

注意

以下の図は、InterScan MSS を 1 台のサーバにインストールしたと仮定しています。インストールした InterScan MSS はいずれも 1 つの論理的単位として機能するので、分散配置されてインストールされた場合にも同じトポロジが適用されます。ただし、InterScan MSS では検索サービス間でのメッセージの配布は取り扱われないので、サードパーティ製ソフトウェアを使用するか、InterScan MSS 検索サービスコンポーネントの複数のインスタンス間でトラフィックのバランスを取るスイッチを使用する必要があります。

ファイアウォールなしで配置する

次の図は、ネットワークにファイアウォールがない場合の InterScan MSS および Postfix の配置方法を示しています。

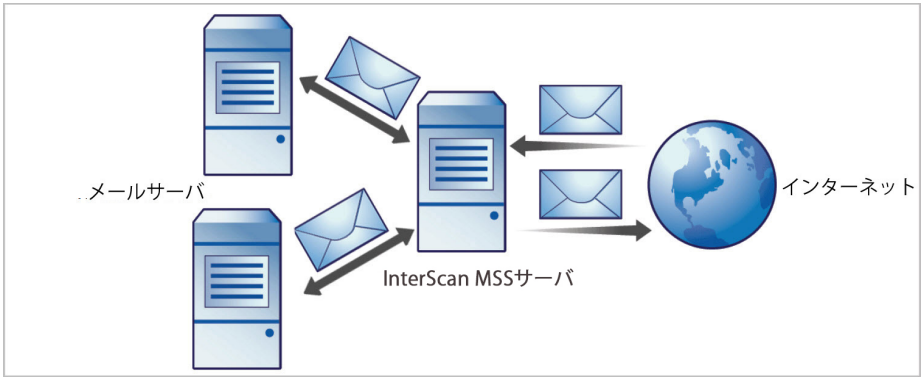


図 3-1. インストールトポロジ: ファイアウォールなし

注意

トレンドマイクロでは、ファイアウォールなしの InterScan MSS のインストールを推奨していません。InterScan MSS をインストールするサーバをネットワークエッジに配置すると、サーバをセキュリティの脅威にさらす可能性があります。

ファイアウォールの外側にインストールする

次の図は、ファイアウォールの外側に InterScan MSS をインストールするときのインストールトポロジを示します。

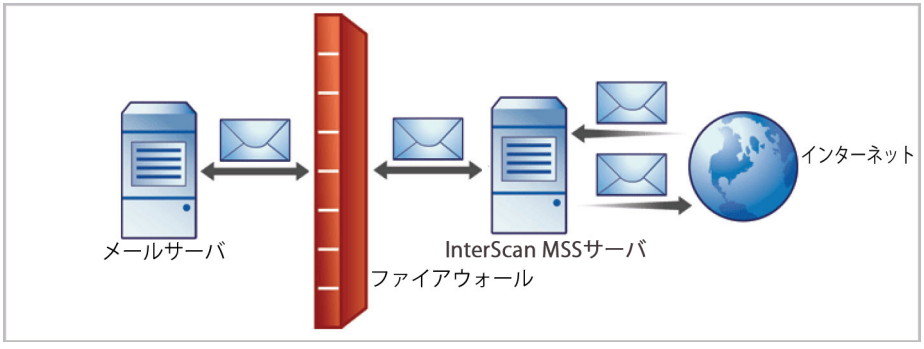


図 3-2. インストールトポロジ: ファイアウォールの外側

受信トラフィック

- 受信メッセージは最初に Postfix が受け取り、その後に InterScan MSS に転送されるようにします。SMTP サーバを参照するように InterScan MSS を設定し、InterScan MSS サーバからの受信トラフィックを許可するようにファイアウォールを設定します。
- ローカルドメインへのリレーのみを許可するように、[リレー管理] を設定します。

送信トラフィック

- すべての送信メッセージが InterScan MSS にルーティングされるようにファイアウォール (プロキシベース) を設定して、SMTP メッセージが次のように転送されるようにします。
  - 送信の SMTP メッセージは、まず Postfix にのみ転送でき、その後 InterScan MSS サーバへ転送されます。
  - 受信の SMTP メッセージは、InterScan MSS サーバからのみ転送できます。

- 内部の SMTP ゲートウェイが Postfix 経由で、InterScan MSS を介して任意のドメインにリレーできるように InterScan MSS を設定します。

ヒント

詳細については、「InterScan MSS 管理者ガイド」の *SMTP ルーティングの設定*に関する項を参照してください。

ファイアウォールの内側へインストールする

次の図は、ファイアウォールの内側への InterScan MSS の配置方法を示します。

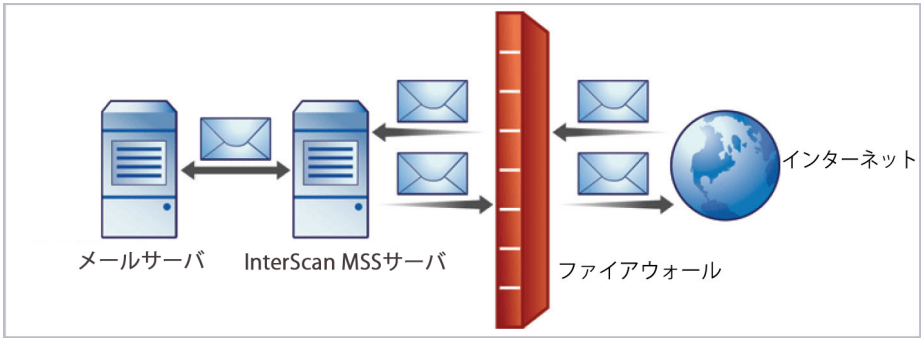


図 3-3. インストールシナリオ: ファイアウォールの内側

受信トラフィック

- プロキシベースのファイアウォールを設定して、SMTP メールが次のように転送されるようにします。
  - 送信の SMTP メッセージは、最初に Postfix、次に InterScan MSS サーバ、または検索サービス間の負荷分散を実行するスイッチに転送されます。
  - 受信の SMTP メッセージは最初に Postfix、次に InterScan MSS に転送され、それからドメイン内の SMTP サーバに転送されます。
- 次のように、パケットベースのファイアウォールを設定します。

  - 使用中の SMTP ゲートウェイを現在参照している DNS サーバの MX レコードを、InterScan MSS をホストするサーバのアドレスを参照するように変更します。
  - セキュアサブネットを管理するように設定している場合は、MX レコードを InterScan MSS またはファイアウォールにポイントします。
- ローカルドメイン向けのメッセージが SMTP ゲートウェイまたは内部のメールサーバにルーティングされるように InterScan MSS を設定します。
- ローカルドメインへのリレーのみが許可されるようにリレー制限を設定します。

送信トラフィック

- 送信メッセージが Postfix、次に InterScan MSS サーバに送信されるように、内部のすべての SMTP ゲートウェイを設定します。
- SMTP ゲートウェイを InterScan MSS で置き換える場合は、送信メッセージが Postfix、次に InterScan MSS サーバに送信されるように、内部のメールサーバを設定します。
- すべての送信メッセージ (ローカル以外のドメイン向け) がファイアウォールにルーティングされるか、またはそのメッセージが配信されるように、Postfix および InterScan MSS を設定します。
- 内部の SMTP ゲートウェイが InterScan MSS を使用して任意のドメインにリレーできるように、InterScan MSS を設定します。

ヒント

詳細については、「InterScan MSS 管理者ガイド」の SMTP ルーティングの設定に関する項を参照してください。

既存の SMTP ゲートウェイ上にインストールする

以前 SMTP ゲートウェイをホストしていた同じサーバに、InterScan MSS および Postfix をインストールすることもできます。

SMTP ゲートウェイ上で次の手順を実行します。

- SMTP メールを InterScan MSS に転送するための新しい TCP/IP ポートを割り当てます。ポートが他のサービスで使用されていないことを確認します。
- 新しく割り当てられたポートにバインドするように InterScan MSS を設定し、ポート 25 を開放します。

注意

既存の SMTP ゲートウェイがポート 25 にバインドされます。

受信トラフィック

受信メールメッセージが SMTP ゲートウェイと新しく割り当てたポートに転送されるように、InterScan MSS を設定します。

送信トラフィック

- 送信メールメッセージが InterScan MSS のポート 25 に転送されるように、SMTP ゲートウェイを設定します。
- ローカル以外のドメイン宛てのすべての送信メールメッセージをファイアウォールに転送するか直接配信するように、Postfix および InterScan MSS を設定します。

DMZ (非武装地帯) 内へインストールする

InterScan MSS および Postfix は DMZ (非武装地帯) にインストールすることもできます。

受信トラフィック

- プロキシベースのファイアウォールを設定して、受信および送信 SMTP メッセージが非武装地帯からのみ内部メールサーバへ送られるようにします。
- パケットベースのファイアウォールを設定します。

- ローカルドメイン向けのメッセージが SMTP ゲートウェイまたは内部のメールサーバにルーティングされるように Postfix および InterScan MSS を設定します。

送信トラフィック

- すべての送信メッセージ (ローカル以外のドメイン向け) がファイアウォールにルーティングされるか、または InterScan MSS を使用して配信されるように、Postfix を設定します。
- 送信メールが Postfix、InterScan MSS の順に転送されるように、内部のすべての SMTP ゲートウェイを設定します。
- 内部の SMTP ゲートウェイが Postfix および InterScan MSS 経由で任意のドメインにリレーされるように InterScan MSS を設定します。

ヒント

詳細については、「InterScan MSS 管理者ガイド」の SMTP ルーティングの設定に関する項を参照してください。

デバイスの役割について

InterScan MSS は、上位デバイスまたは下位デバイスとして機能させることができます。単一の上位デバイスと複数の下位デバイスが、1 つのグループを構成します。このグループでは、上位デバイスに登録された下位デバイスに対して、上位デバイスが中央管理サービスを提供します。

- 上位: 下位デバイスを管理します。1 つの InterScan MSS デバイスを配置する場合は、セットアップ時にすべての InterScan MSS コンポーネントが配置されるように、[上位モード] を選択します。
- 下位:1 つの上位デバイスによって管理され、すべてのグローバル設定を使用します。グローバル設定は、上位デバイスの管理コンソールを通して設定します。

グループとは、1 つの上位デバイスと、それに登録された 1 つ以上の下位デバイスの組み合わせです。

デバイスサービスについて

InterScan MSS デバイスでは、さまざまな種類のサービスを有効にできます。

上位のみのサービス:

- 管理ユーザインタフェースサービス (管理コンソール): グローバル設定を管理します。

上位および下位のサービス:

- ポリシーサービス: 設定するルールを管理します。
- 検索サービス: メールトラフィックを検索します。
- エンドユーザメール隔離サービス: エンドユーザメール隔離を管理します。これによって、InterScan MSS がスパムメールと判定したメールメッセージを表示することができます。

下位デバイスは、上位デバイスに登録されている場合にのみ機能します。

サービスの選択

上位デバイスおよび下位デバイスでは、さまざまな種類のサービスを有効にできます。たとえば、スループットを増やすために、下位デバイスを追加してそのすべてのサービスを有効にし、下位デバイスでトラフィックを検索したり、エンドユーザメール隔離サービスを提供したりすることができます。

いずれの配置構成でも、1 つの上位/下位グループに複数の InterScan MSS デバイスを配置することができます。ただし、上位デバイスおよび下位デバイスで検索サービスを有効にする場合は、1 つのグループ内ですべてのデバイスに同じ種類の配置を使用する必要があります。ゲートウェイに一部の下位デバイスを配置して、ゲートウェイの内側にそれ以外の下位デバイスを配置することはできません。

上記の SMTP 検索シナリオ以外に、InterScan MSS で POP3 トラフィックを検索する場合もあります。詳細については、60 ページの「POP3 メール検索を理解する」を参照してください。

送信者フィルタを使用して配置する

IP プロファイラ、メールレピュテーション、および SMTP トラフィックスロットリングで構成される送信者フィルタは、IP レベルで接続をブロックします。

送信者フィルタを使用する場合、InterScan MSS とネットワークエッジの間に配置されるファイアウォールは、いずれも接続 IP アドレスを変更してはいけません。これは、送信者フィルタが、Network Address Translation (NAT) を使用するネットワークと互換性がないためです。たとえば、InterScan MSS が同じ送信元 IP アドレスからの SMTP 接続を受け入れる場合は、送信者フィルタは機能しません。これは、このアドレスがすべての受信メッセージのアドレスと同じになり、送信者フィルタが、SMTP セッションの開始者が既知のスパムメール送信者であるかどうかを判断できなくなるためです。

POP3 メール検索を理解する

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。会社で POP3 メールを使用していない場合でも、従業員が、個人的な Web ベースの POP3 メールアカウントにアクセスする場合があります。これらのアカウントからのメッセージが検索されない場合、これが、ネットワーク上の脆弱なポイントになる可能性があります。

最も一般的なメール検索配置では、InterScan MSS を使用して、SMTP トラフィックを検索します。初期設定では、このように設定されています。ただし、企業がインターネット経由で POP3 サーバから受信する POP3 トラフィックを検索する場合は、POP3 検索を有効にします。

POP3 検索を有効にすると、InterScan MSS は、メールクライアントと POP3 サーバ間に配置されたプロキシとして機能し、クライアントがメッセージを受信する際にそのメッセージを検索します。

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。

POP3 検索の要件

InterScan MSS で POP3 トラフィックを検索するには、ネットワーク上にファイアウォールをインストールして、InterScan MSS 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する必要があります。このように設定すると、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 に到達し、InterScan MSS のみで POP3 トラフィックが検索されるようになります。

注意

POP3 検索を無効にした場合、クライアントは POP3 メールを受信できません。

InterScan MSS を経由してメールを受信する POP3 クライアントを設定する

一般的な POP3 接続を使用して POP3 クライアントを設定するには、次の項目を設定します。

- IP アドレスまたはドメイン名: InterScan MSS の IP アドレスまたはドメイン名
- ポート: InterScan MSS の一般的な POP3 ポート
- アカウント:<アカウント名>#<POP3 サーバドメイン名>

  例:user#10.18.125.168

専用の POP3 接続を使用して POP3 クライアントを設定するには、次の項目を設定します。

- IP アドレス: InterScan MSS の IP アドレス
- ポート: InterScan MSS の専用の POP3 ポート
- アカウント:<アカウント名>

  例:user

InterScan MSS の管理コンソールを開く

InterScan MSS の管理コンソールは、プログラムが配信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。

Web ブラウザで管理コンソールを表示するには、次の URL にアクセスします。

https://{IMSS}:8445

{IMSS} は、IP アドレスまたは完全修飾ドメイン名です。

以下に例を示します。`https://196.168.10.1:8445` または `https://IMSS1:8445`

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。SSL を使用して管理コンソールを表示するには、ドメイン名の前に「https://」を付け、その後にポート番号を付けます。

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

初めてコンソールを開いたら、ログオンアカウント情報を入力し、[ログオン] をクリックします。

警告!

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。

注意

Internet Explorer (IE) を使用して管理コンソールにアクセスする場合、IE 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。このメッセージは無視して、[このサイトの閲覧を続行する] をクリックし、作業を続けてください。

運用モデルについて

InterScan MSS は、InterScan MSS サーバが既存の MTA およびメールサーバとどのようにやりとりするかに応じて、さまざまな方法で配置できます。運用モデルには、次の 2 つがあります。

スタンドアロンモデル

InterScan MSS を、Postfix などの MTA と同じコンピュータに配置します。

サンドイッチモデル

InterScan MSS を、アップストリーム MTA とダウンストリーム MTA の間に配置します。

スタンドアロンモデル

スタンドアロンモデルでは、1 台のコンピュータに、MTA として機能する 1 つの Postfix インスタンスと、1 つの InterScan MSS デーモンが配置されます。

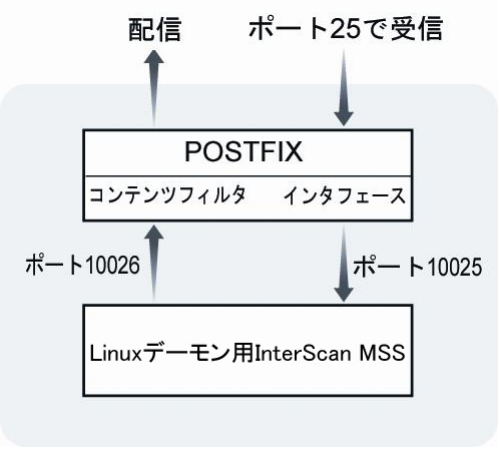


図 3-4. スタンドアロンモデル

この構成は、小規模から中規模企業のほとんどのニーズを満たすことができます。また、すべてのプロセスが同じサーバ上で実行されるため、ネットワー

クへの影響もあまりありません。ただし、同じリソースを共有するため、Postfix と InterScan MSS デーモンをホストするのに十分耐えうるサーバが要求されます。

両サイドの初期設定の設定パラメータは、次のとおりです。

/etc/postfix/main.cf:

```
mydomain = your.domain.name
myhostname = your.hostname.domainname
mydestination = $myhostname, localhost.$mydomain,
$mydomain
default_process_limit=200
imss_timeout=10m
imss_connect_timeout=1s
content_filter = imss:localhost:10025
imss_destination_recipient_limit=200
imss_destination_concurrency_limit=200
```

/etc/postfix/master.cf:

```
#IMSS: content filter smtp transport imss for IMSS
imss unix - - n - - smtp
  -o disable_dns_lookups=yes
  -o smtp_connect_timeout=$imss_connect_timeout
  -o smtp_data_done_timeout=$imss_timeout
  -o smtpd_tls_security_level=none
#IMSS: content filter loop back smtpd
localhost:10026 inet n - n - 200 smtpd
  -o content_filter=
  -o smtpd_timeout=$imss_timeout
  -o local_recipient_maps=
  -o myhostname=postfix.imss71
  -o smtpd_client_restrictions=
  -o smtpd_enforce_tls=no
  -o smtpd_tls_security_level=none
```

注意

上記の設定をコピーして貼り付ける場合は、すべての行のインデントをそれぞれ修正してください。

IPv6 環境でのスタンドアロンモデル

IPv6 をサポートする場合、/etc/postfix/main.cf に次の変更を加えます。

```
mydomain = your.domain.name
myhostname = your.hostname.domainname
mydestination = $myhostname, localhost.$mydomain,
$mydomain
default_process_limit=200
imss_timeout=10m
imss_connect_timeout=1s
content_filter = imss:[::1]:10025
imss_destination_recipient_limit=200
imss_destination_concurrency_limit=200
```

IPv6 をサポートする場合、/etc/postfix/master.cf に次の変更を加えます。

```
#IMSS: content filter smtp transport imss for IMSS
imss unix - - n - - smtp
  -o disable_dns_lookups=yes
  -o smtp_connect_timeout=$imss_connect_timeout
  -o smtp_data_done_timeout=$imss_timeout
  -o smtpd_tls_security_level=none
#IMSS: content filter loop back smtpd
[::1]:10026 inet n - n - 200 smtpd
  -o content_filter=
  -o smtpd_timeout=$imss_timeout
  -o local_recipient_maps=
  -o myhostname=postfix.imss71
  -o smtpd_client_restrictions=
  -o smtpd_enforce_tls=no
  -o smtpd_tls_security_level=none
```

注意

上記の設定をコピーして貼り付ける場合は、すべての行のインデントをそれぞれ修正してください。

`/opt/trend/imss/config/imss.ini` で、接続制限を開き、ダウンストリームサーバの IP を IPv6 localhost に指定します。

```
[socket]
proxy_smtp_server_ip=all
[smtp]
smtp_allow_client_ip=127.0.0.1, ::1
downstream_smtp_server_addr=::1
```

サンドイッチモデル

この構成では、1 台目のサーバに受信用のアップストリーム MTA として機能する Postfix が配置され (Server #1)、2 台目のサーバに配信用のダウンストリーム MTA として機能する Postfix が配置されます (Server #3)。3 台目のサーバに

は InterScan MSS デーモンが配置されます。このサーバは、2 台の Postfix サーバの間に検索プロキシとして配置されます (Server #2)。

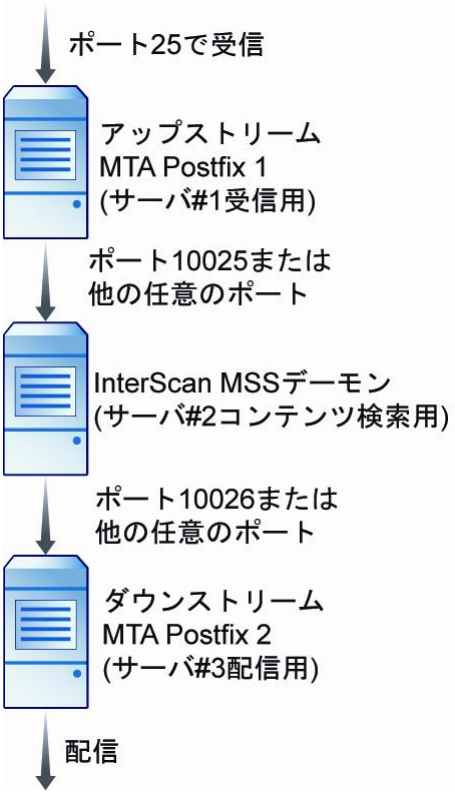


図 3-5. サンドイッチモデル

この構成は、大容量の SMTP トラフィックを処理する大規模企業に適しています。サーバごとに固有の用途とタスクを割り当てるため、サーバ間で影響しあうことはありません。このタイプの構成を使用すると、ネットワーク負荷が増加します。

この構成は柔軟性が高いため、Postfix の代わりに任意の SMTP MTA を使用できます。ただし、接続の制御とドメインのリレーに関する設定を各自で行う必要があります。

ここでは、Postfix を MTA として使用する場合の設定を示します。

- サーバ#1 の/etc/postfix/main.cf に次のパラメータを追加して、メールをサーバ#2 にリレーするようにします。

```
relayhost=[ip_of_server2]:10025
default_destination_recipient_limit=100
default_destination_concurrency_limit=50
```

- /opt/trend/imss/config/imss.ini で、接続制限を開き、ダウンストリームサーバの IP をサーバ#3 に指定します。

```
imss socket binding address
[socket]
proxy_smtp_server_ip=all
[smtp]
smtp_allow_client_ip=127.0.0.1, ip_of_server1
downstream_smtp_server_addr=ip_of_server3
```

- サーバ#3 の/etc/postfix/master.cf で、smtpd 設定を変更し、ポート 10026 でメールを受信するようにします。

```
10026 inet n - n - - smtpd
```

IPv6 環境でのサンドイッチモデル

ここでは、Postfix を MTA として使用する場合の設定を示します。

サーバ#1 の/etc/postfix/main.cf に次のパラメータを追加して、メールをサーバ#2 にリレーするようにします。

```
relayhost=[ipv6_address_of_server2]:10025
default_destination_recipient_limit=100
default_destination_concurrency_limit=50
```

/opt/trend/imss/config/imss.ini で、接続制限を開き、ダウンストリームサーバの IP をサーバ#3 に指定します。

```
[socket]
proxy_smtp_server_ip=all
```

```
[smtp]
smtp_allow_client_ip=127.0.0.1, ipv6_address_of_server1
downstream_smtp_server_addr=ipv6_address_of_server3
```

サーバ#3 の/etc/postfix/master.cf で、smtpd 設定を変更し、ポート 10026 でメールを受信するようにします。

```
10026 inet n - n - - smtpd
```

第 4 章

インストールおよびアンインストール

この章では、さまざまな条件の下で Trend Micro InterScan Messaging Security Suite 9.1 (以下、InterScan MSS) をインストール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。

- 72 ページの「システム要件」
- 72 ページの「MTA を準備する」
- 81 ページの「InterScan MSS をインストールする」
- 83 ページの「送信者フィルタを Sendmail とともに使用する」
- 88 ページの「インストールを確認する」
- 89 ページの「IPv6 サポートについて」
- 94 ページの「InterScan MSS をアンインストールする」

システム要件

最新の情報については弊社の「最新版ダウンロード」サイトにある最新の Readme をご参照ください。

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

MTA を準備する

InterScan MSS は、Postfix と Sendmail の 2 種類の MTA (Message Transfer Agents) をサポートしています。ここでは、InterScan MSS コンポーネントをインストールする前に、これらの MTA を InterScan MSS とともに使用できるように準備する方法について説明します。

Postfix を準備する

Postfix がインストールされているコンピュータに InterScan MSS をインストールする場合は、Postfix を次のように設定します。

注意

InterScan MSS サーバのインストール時にインストーラによって MTA がインストールされることはありません。すでに MTA がインストールされていて、動作可能である必要があります。InterScan MSS をインストールするコンピュータに Postfix をインストールする場合は、Postfix の設定が適切であることを確認してください。トレンドマイクロでは、お使いのバージョンの Linux とともに配布されている Postfix をインストールして使用することを強くお勧めします。詳細については、http://www.postfix.org を参照してください。

手順

- 次の設定を/etc/postfix/main.cf に挿入するか変更します。

```
mydomain = your.domain.name (use the server FQDN here)
myhostname = your.hostname.domainname
mydestination = $myhostname, localhost.$mydomain, $mydomain
```

```
default_process_limit=200
imss_timeout=10m
imss_connect_timeout=1s
content_filter = imss:localhost:10025
imss_destination_recipient_limit=200
imss_destination_concurrency_limit=200
```

- 次の設定を/etc/postfix/master.cf に挿入します。

```
#IMSS: content filter smtp transport imss for IMSS
imss unix - - n - - smtp
  -o disable_dns_lookups=yes
  -o smtp_connect_timeout=$imss_connect_timeout
  -o smtp_data_done_timeout=$imss_timeout
  -o smtpd_tls_security_level=none

#IMSS: content filter loop back smtpd
localhost:10026 inet n - n - 200 smtpd
  -o content_filter=
  -o smtpd_timeout=$imss_timeout
  -o smtpd_tls_security_level=none
  -o local_recipient_maps=
  -o myhostname=postfix.imss91
  -o smtpd_client_restrictions=
  -o smtpd_enforce_tls=no
```

注意

上記の設定をコピーして貼り付ける場合は、すべての行のインデントをそれぞれ修正してください。

Postfix の IPv6 サポートを有効にする

次の手順は、Postfix を IPv6 対応に設定する方法を示しています。Postfix 2.2 の IPv6 プロトコルのサポートの詳細については、次の URL を参照してください。

http://www.postfix.org/IPV6_README.html

手順

1. `/etc/postfix/main.cf` を開きます。
2. `inet_protocols = all` と設定します。
3. Postfix サービスを再起動します。

Sendmail について

ここでは、Sendmail を設定して InterScan MSS とともに使用する方法について説明します。

注意

Sendmail は v8.10 から IPv6 をサポートしています。詳細については、次の URL から入手可能なサポートドキュメントを参照してください。

http://www.sendmail.org/~gshapiro/8.10.Training/IPv6.html

Sendmail デーモン

次の図は、2 つの Sendmail デーモンと InterScan MSS を同一サーバ上で実行している様子を示しています。

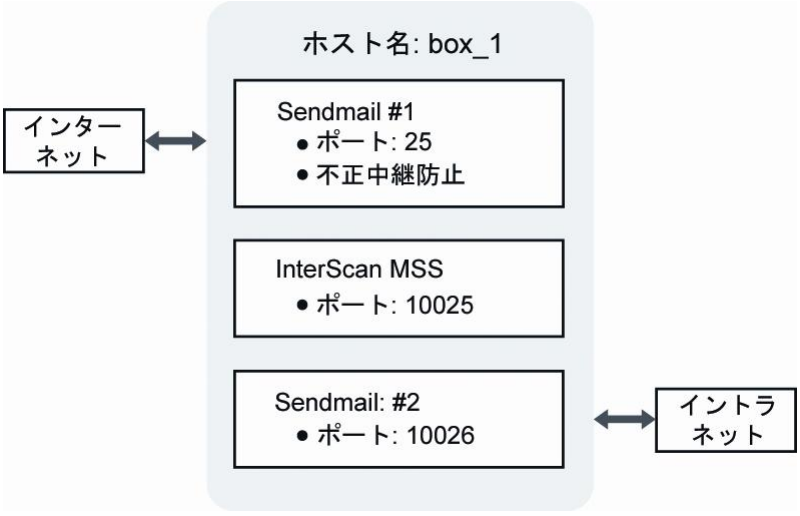


図 4-1. 1 つのサーバ上にある複数の Sendmail デーモン

ポート 10025 と 10026 は任意のポート番号なので、次の設定を完了する際には、10025 と 10026 を使用されていないポート番号に置き換えてください (ポート 25 は標準の SMTP ポート)。

Sendmail #1 を設定する

手順

1. `sendmail.mc` ファイルをコピーして、名前を `sendmail.d.mc` に変更します。

   ```
   # cp -p /etc/mail/sendmail.mc /etc/mail/sendmail.d.mc
   ```

2. `sendmail.mc` ファイルに次の文を追加して、すべてのメールメッセージを InterScan MSS にリレーします。

```
define(`SMTP_MAILER_ARGS',`TCP [127.0.0.1] 10025')dnl
MODIFY_MAILER_FLAGS(`SMTP', `+k') dnl
define(`ESMTP_MAILER_ARGS',`TCP [127.0.0.1] 10025')dnl
MODIFY_MAILER_FLAGS(`ESMTP', `+k') dnl
define(`SMTP8_MAILER_ARGS',`TCP [127.0.0.1] 10025')dnl
MODIFY_MAILER_FLAGS(`SMTP8', `+k') dnl
define(`RELAY_MAILER_ARGS',`TCP [127.0.0.1] 10025')dnl
MODIFY_MAILER_FLAGS(`RELAY', `+k') dnl
MODIFY_MAILER_FLAGS(`LOCAL', `+k') dnl
define(`LOCAL_MAILER_PATH',`[IPC]')dnl
define(`LOCAL_MAILER_ARGS',`TCP [127.0.0.1] 10025')dnl
```

3. sendmail.mc ファイルの既存の DAEMON_OPTIONS の設定を次のように変更して、すべてのホストから SMTP 要求を受信します。

   ```
   DAEMON_OPTIONS(`Port=smtp, Addr=0.0.0.0, Name=MTA')dnl
   ```

   次の DAEMON_OPTIONS の設定を必要に応じて追加し、IPv6 のサポートを有効にします。

   ```
   DAEMON_OPTIONS(`Port=smtp, Addr=<IPv6_address>,
   Name=MTA_IPv6, Family=inet6')dnl
   ```

4. sendmail.cf ファイルに次のコマンドを実行して、有効にします。

   ```
   # m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
   ```

Sendmail #2 を設定する

手順

1. /var/spool/mqueue キューディレクトリをコピーして、Sendmail #2 用に名前を/var/spool/mqueue1 に変更します。

   ```
   # cp -pr /var/spool/mqueue /var/spool/mqueue1
   ```

2. sendmail.d.mc ファイルに次の文を追加します。

```
define(`QUEUE_DIRECTORY', `/var/spool/mqueue1')dnl
define(`confPID_FILE', `/var/run/sendmail_delivery.pid')dnl
```

3. sendmail.d.mc ファイルの既存の DAEMON_OPTIONS の設定を次のように変更して、InterScan MSS から SMTP 要求を受信します。

   ```
   DAEMON_OPTIONS(`Port=10026, Addr=127.0.0.1,
   Name=MTA_DELIVERY')dnl
   ```

4. sendmail.cf.delivery ファイルに次のコマンドを実行して、有効にします。

   ```
   # m4 /etc/mail/sendmail.d.mc > /etc/mail/
   sendmail.cf.delivery
   ```

Sendmail サービスのセットアップを完了して再起動する

手順

1. 次のコマンドを使用して、最初の Sendmail デーモンを再起動し、ポート 25 で SMTP トラフィックを受信します。

   - Red Hat Enterprise Linux 6

     ```
     # /etc/init.d/sendmail restart
     ```

   - Red Hat Enterprise Linux 7

     ```
     # systemctl sendmail restart
     ```

2. 2 つ目の Sendmail デーモン用に、次の新しいファイルを作成します。

   - Red Hat Enterprise Linux 6

     sendmail_delivery ファイルを作成します。

     ```
     vi /etc/init.d/sendmail_delivery
     ```

     ```
     #!/bin/bash
     #
     # sendmail_delivery  This shell script takes care of
     ```

```
#                   starting and stopping
#                   sendmail_delivery
#
# chkconfig: 2345 80 30
#

PROG=sendmail_delivery
CONFFILE=/etc/mail/sendmail.cf.delivery
PIDFILE=/var/run/sendmail_delivery.pid

# Source function library.
. /etc/rc.d/init.d/functions

# Source networking configuration.
[ -f /etc/sysconfig/network ] && \
. /etc/sysconfig/network

# Source sendmail configureation.
if [ -f /etc/sysconfig/sendmail ]; then
    . /etc/sysconfig/sendmail
else
    DAEMON=no
    QUEUE=1h
fi

# Check that we're a privileged user
[ `id -u` = 0 ] || exit 4

# Check that networking is up.
[ "${NETWORKING}" = "no" ] && exit 1

[ -x /usr/sbin/sendmail ] || exit 5


start() {
    ret=0
    echo -n $"Starting $PROG: "
    daemon --pidfile $PIDFILE /usr/sbin/sendmail \
        $([ "x$DAEMON" = xyes ] && echo -bd) \
    $([ -n "$QUEUE" ] && echo -q$QUEUE) \
        $SENDMAIL_OPTARG -C $CONFFILE
    RETVAL=$?
```

```
    echo
    [ $RETVAL -eq 0 ] && touch /var/lock/subsys/$PROG
    let ret+=$RETVAL

    [ $ret -eq 0 ] && return 0 || return 1
}

stop() {
    echo -n $"Shutting down $PROG: "
    killproc $PROG
    RETVAL=$?
    echo
    [ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/$PROG
    return $RETVAL
}

status -p $PIDFILE >/dev/null
running=$?

case "$1" in
    start)
    [ $running -eq 0 ] && exit 0
    start
    RETVAL=$?
    ;;
    stop)
    [ $running -eq 0 ] || exit 0
    stop
    RETVAL=$?
    ;;
    restart)
    stop
    start
    RETVAL=$?
    ;;
    status)
    echo -n $PROG ; status -p $PIDFILE -l $PROG
    RETVAL=$?
    ;;
    *)
    echo $"Usage: $0 {start|stop|restart|status}"
    RETVAL=2
```

```
esac

exit $RETVAL
```

- Red Hat Enterprise Linux 7

  a. sendmail_delivery.service ファイルを作成します。

  ```
  vi /usr/lib/systemd/system/sendmail_delivery.service
  ```

  ```
  [Unit]
   Description=Sendmail Mail Transport Agent
   for Delivery
   After=syslog.target network.target
   Conflicts=postfix.service exim.service

   [Service]
   Type=forking
   StartLimitInterval=0
   PIDFile=/var/run/sendmail_delivery.pid
   Environment=SENDMAIL_OPTS="-q1h"
   EnvironmentFile=-/etc/sysconfig/sendmail
   ExecStartPre=-/etc/mail/make
   ExecStartPre=-/etc/mail/make aliases
   ExecStart=/usr/sbin/sendmail -bd $SENDMAIL_OPTS
   $SENDMAIL_OPTARG -C /etc/mail/sendmail.cf.delivery

   [Install]
   WantedBy=multi-user.target
  ```

  b. sendmail_delivery.service ファイルへのソフトリンクを作成します。

  ```
  ln -s /usr/lib/systemd/system/
  sendmail_delivery.service /etc/systemd/system/multi-
  user.target.wants/sendmail_delivery
  ```

3. 次のコマンドを使用して、2 つ目の Sendmail デーモンを再起動し、IMSS から SMTP トラフィックを受信します。

   - Red Hat Enterprise Linux 6

   ```
   # /etc/init.d/sendmail_delivery restart
   ```

- Red Hat Enterprise Linux 7

  ```
  # systemctl sendmail_delivery restart
  ```

InterScan MSS をインストールする

次に、InterScan MSS のインストールの実行に必要な主な手順を示します。

注意

インストール前に画面のフォントサイズが 24 未満であることを確認してください。24 以上の場合は、インストールに失敗することがあります。

手順

1. `/IMSSPackagePath/imss/install.sh` ファイルを実行して、InterScan MSS のインストールウィザードを開始します。
2. <F12> キーを押してインストールを続行します。
3. <F12> キーを押して使用許諾契約書に同意します。
4. インストールの種類を選択します。
   - 新規インストール
   - Append install

     このオプションを選択する場合は、[下位デバイス] を選択し、上位デバイスの管理コンソールの IP アドレス、ログオンユーザ名、およびパスワードを指定します。

注意

次のことに注意してください。

- 指定するログオンユーザアカウントにはフル管理者権限が必要です。
- 下位デバイスと上位デバイスが同じサブネットに属していないと [Append install] は失敗します。この場合、`/var/imss/pgdata` にある上位デバイスの設定ファイル `pg_hba.conf` を変更して、下位デバイスから上位デバイスのデータベースに接続できるようにします。

5. ローカルデータベースまたはリモートデータベースのインストールを選択します。

- Internal PostgreSQL database: 初期設定で使用されるデータベースです。
- External PostgreSQL database: このオプションを選択した場合は、必要に応じて外部データベース情報を提供します。

注意

外部データベースを使用するには、次の手順を実行します。

a. InterScan MSS 管理データベースのインストールに使用するアカウントにスーパーユーザの役割があることを確認します。

b. データベース接続の最大数を 600 に変更します。

```
vi /var/lib/pgsql/9.6/data/postgresql.conf

max_connection = 600 (初期設定では 100 です)

restart DB service (コマンドは「service postgresql-9.6 restart」または「systemctl restart postgresql」です)
```

c. InterScan MSS と外部データベースサーバで同じタイムゾーンと時刻設定が使用されていることを確認します。そうでないと、予期しない問題が発生することがあります。

d. `postgresql.conf` の max_locks_per_transaction が 256 に設定されていることを確認して、データベースサービスを再起動します。

6. InterScan MSS のインストール先フォルダを指定します。
7. 送信者フィルタサービスのコンポーネントを選択して有効にします。
   - メールレピュテーションを有効にする
   - Enable IP Profiler
8. 使用環境が最小システム要件をすべて満たしていることを確認します。
9. 進行状況バーが 100%になるまで待ちます。

   インストールが完了したことを示すメッセージが表示されます。

送信者フィルタを Sendmail とともに使用する

送信者フィルタ (IP プロファイラとメールレピュテーション) は、IP レベルで接続をブロックします。IP プロファイラは、カスタム設定を使用して、各種の攻撃を示すメールメッセージに対応します。メールレピュテーションは、Trend Micro Threat Reputation Network の情報を使用して、SMTP 接続を開始しようとしているコンピュータが既知のスパムメール送信者かどうかを判断します。

送信者フィルタ (IP プロファイラまたはメールレピュテーション) を Sendmail MTA とともに使用する場合は、追加の設定を実行して、Sendmail で FoxLib が確実に使用されるようにし、SMTP クライアントと通信する FoxProxy の実際の IP アドレスを取得する必要があります。

この項では、Red Hat 6 および 7 で、Sendmail と送信者フィルタをサポートするように FoxLib を設定する手順について説明します。

Red Hat 6 で FoxLib を Sendmail と統合する

手順

1. FoxProxy からのみ SMTP トラフィックを受信するように最初の Sendmail を変更します。

a. sendmail.mc ファイルの DAEMON_OPTIONS の設定を次のように変更します。

```
DAEMON_OPTIONS(`Port=2500, Addr=127.0.0.1, Name=MTA')dnl
```

b. sendmail.cf ファイルに次のコマンドを実行して、有効にします。

```
# m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
```

2. Sendmail のプロパティを変更します。

a. プロパティのリストを表示します。

```
ll /usr/sbin/sendmail.sendmail
```

```
-rwxr-sr-x 1 root smmsp 746328 Jan 22 2007 /usr/sbin/
sendmail.sendmail
```

b. SGID ビットを削除します。

```
chmod g-s /usr/sbin/sendmail.sendmail
```

c. Sendmail で使用するグループを変更します。

```
chgrp root /usr/sbin/sendmail.sendmail
```

d. プロパティを確認します。

```
ll /usr/sbin/sendmail.sendmail
```

```
-rwxr-xr-x 1 root root 746328 Jan 22 2007 /usr/sbin/
sendmail.sendmail
```

3. /opt/trend/imss/script ディレクトリの foxlibd スクリプトを変更します。

a. TM_FOX_UID パラメータを、Sendmail で使用するユーザの ID に設定します。

```
TM_FOX_UID=0
```

b. TM_FOX_GID パラメータを、Sendmail で使用するグループの ID に設定します。

```
TM_FOX_GID=0
```

c. (オプション) Red Hat (64 ビット) を使用している場合は、LD_PRELOAD パラメータを次のように設定します。

```
LD_PRELOAD=/opt/trend/imss/lib64/libTmFoxSocketLib.so
```

d. 「export LD_LIBRARY_PATH」が含まれる行の後ろに、次の 2 行を追加します。

```
TM_FOX_PROXY_CONNECT_PORT=2500

export TM_FOX_PROXY_CONNECT_PORT
```

4. `/opt/trend/imss/config` ディレクトリの `foxproxy.ini` 設定ファイルを変更します。

a. has_foxlib_installed パラメータの値を「`0`」から「`1`」に変更します。

```
has_foxlib_installed=1
```

5. `foxlibd` スクリプトを使用して、Sendmail と FoxProxy を再起動します。

a. アップストリーム MTA を停止します。

```
/opt/trend/imss/script/foxlibd stop
```

次のエラーメッセージが表示された場合は無視します。

```
"ERROR: ld.so: object '/opt/trend/imss/lib
/libTmFoxSocketLib.so' from LD_PRELOAD cannot be
      preloaded: ignored."
```

b. Sendmail を開始します。

```
/opt/trend/imss/script/foxlibd start
```

前の手順で説明したエラーメッセージが表示された場合は無視します。

c. FoxProxy を再起動します。

```
/opt/trend/imss/script/foxproxyd stop

/opt/trend/imss/script/foxproxyd start
```

6. テストサーバを使用してインストールを確認します。

a. InterScan MSS サーバへの接続をテストします。

```
telnet <InterScan MSS サーバのアドレス> 25

ehlo imss
```

> **注意**
> InterScan MSS サーバとテストサーバのアドレスは、同じサブネットに属している必要があります。

b. 応答にテストサーバのアドレスが含まれているかどうか確認します。

応答に「127.0.0.1」の文字列が含まれている場合、インストールは失敗しています。

Red Hat 7 で FoxLib を Sendmail と統合する

手順

1. FoxProxy からのみ SMTP トラフィックを受信するように最初の Sendmail を変更します。

   a. `sendmail.mc` ファイルの DAEMON_OPTIONS の設定を次のように変更します。

   ```
   DAEMON_OPTIONS(`Port=2500, Addr=127.0.0.1, Name=MTA')dnl
   ```

   b. `sendmail.cf` ファイルに次のコマンドを実行して、有効にします。

   ```
   # m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
   ```

2. Sendmail のプロパティを変更します。

   a. プロパティのリストを表示します。

   ```
   ll /usr/sbin/sendmail.sendmail

   -rwxr-sr-x 1 root smmsp 746328 Jan 22 2007 /usr/sbin/
   sendmail.sendmail
   ```

b. SGID ビットを削除します。

```
chmod g-s /usr/sbin/sendmail.sendmail
```

c. Sendmail で使用するグループを変更します。

```
chgrp root /usr/sbin/sendmail.sendmail
```

d. プロパティを確認します。

```
ll /usr/sbin/sendmail.sendmail
```

```
-rwxr-xr-x 1 root root 746328 Jan 22 2007 /usr/sbin/
sendmail.sendmail
```

3. Sendmail の環境を変更します。

a. 次のコマンドを実行します。

```
# systemctl edit sendmail
```

b. 次の行を追加して、変更を保存します。

```
[Service]
Environment="LD_PRELOAD=/opt/trend/imss/lib64
/libTmFoxSocketLib.so"
Environment="TM_FOX_PROXY_CONNECT_PORT=2500"
Environment="TM_FOX_PROXY_LIST=
/opt/trend/imss/config/foxproxy.list"
```

注意

InterScan MSS を初期設定のパス (`/opt/trend`) にインストールしていない場合は、それに応じて前の行のパスを変更します。

4. `/opt/trend/imss/config` ディレクトリの `foxproxy.ini` 設定ファイルを変更します。

a. has_foxlib_installed パラメータの値を「`0`」から「`1`」に変更します。

```
has_foxlib_installed=1
```

5. Sendmail と FoxProxy を再起動します。

a. アップストリーム MTA を再起動します。

```
systemctl restart sendmail
```

b. FoxProxy を再起動します。

```
/opt/trend/imss/script/foxproxyd stop
```

```
/opt/trend/imss/script/foxproxyd start
```

6. テストサーバを使用してインストールを確認します。

a. InterScan MSS サーバへの接続をテストします。

```
telnet <InterScan MSS サーバのアドレス> 25
```

```
ehlo imss
```

> **注意**
>
> InterScan MSS サーバとテストサーバのアドレスは、同じサブネットに属している必要があります。

b. 応答にテストサーバのアドレスが含まれているかどうか確認します。

応答に「127.0.0.1」の文字列が含まれている場合、インストールは失敗しています。

インストールを確認する

インストールの完了後にデーモンのリストを確認するには、コマンドプロンプトに次のコマンドを入力します。

```
# ps -ef | grep imss
```

ポート 25 に Telnet を実行して、InterScan MSS または Postfix が応答することを確認します。

IPv6 サポートについて

InterScan MSS のインストール後、IPv6 サポートを設定します。InterScan MSS では、IPv6 ネットワークおよび IPv6 ネットワーク内のプロキシで次の IPv6 機能がサポートされます。

SMTP ルーティング

InterScan MSS 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。

POP3 接続

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

トレンドマイクロサービス

InterScan MSS は IPv6 を使用した次のサービスとの通信をサポートしています。

- Web レピュテーションサービス
- 製品登録
- アップデート
- スマートフィードバック

メールの保護

InterScan MSS は、マーケティングメッセージを含め、IPv6 ネットワークからの受信メッセージの検索をサポートしています。

通知

InterScan MSS は、IPv6 通知サーバへの通知の送信をサポートしています。

Trend Micro Control Manager

InterScan MSS は、IPv6 ネットワーク内に配置された Control Manager サーバに接続できます。Control Manager が IPv6 をサポートするように設定されていることを確認してください。

IP アドレスのインポートおよびエクスポート

InterScan MSS 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。

サーバを IPv6 対応に設定する

IPv6 サポートを設定するには、IPv6 ネットワークを有効にしてから、サーバで IPv6 アドレスを設定します。

手順

1. IPv6 ネットワークを有効にします。
   a. シェルにログオンし、次のコマンドを使用して/etc/sysconfig/network を編集します。

      ```
      # vi /etc/sysconfig/network
      ```

   b. 次の行が存在しない場合は、それを追加します。

      ```
      NETWORKING_IPV6=yes
      ```

2. IPv6 アドレスを設定します。
   a. インタフェース用の設定ファイルを編集します。

      例:`# vi /etc/sysconfig/network-scripts/ifcfg-eth0`

   b. 次の行を追加します。

      ```
      IPV6INIT=yes

      IPV6_AUTOCONF=no

      IPV6ADDR=<エンドポイントの IPv6 アドレス> (例:
      2001:db8:10ff::ae:44f2/64)
      ```

   c. ネットワークサービスを再起動します。

      ```
      # service network restart
      ```

IPv6 設定を確認する

次の手順は、IPv6 サポートが機能していることを確認する方法を示しています。

手順

1. サーバを使用して他のエンドポイントへ ping を実行します。

   ```
   # ping6 ::1
   ```

   ```
   # ping6 <別のエンドポイントの IPv6 アドレス>
   ```

2. 別のエンドポイントを使用してサーバへ ping を実行します。

   ```
   # ping6 <このサーバの IPv6 アドレス>
   ```

InterScan MSS を IPv6 対応に設定する

サーバ OS を IPv6 対応に設定したら、InterScan MSS で IPv6 サポートを設定します。これは<InterScan MSS のインストール先>/imss/config/imss.ini で設定します。

IPv6 サポート対応のプロキシ設定

proxy_smtp_server_ip および proxy_pop3_server_ip を変更して、InterScan MSS デーモンのバインド先の IP アドレスを設定します。

- proxy_smtp_server_ip が指定されていない場合は、SMTP プロキシサービスによって IP アドレスが 127.0.0.1 に設定されます。
- proxy_pop3_server_ip が指定されていない場合は、プロキシサービスによって IP アドレスが 0.0.0.0 に設定されます。
- proxy_smtp_server_ip および proxy_pop3_server_ip が all として指定されている場合、プロキシサービスは IPv4 クライアントまたは IPv6 クライアントを含むすべてのインタフェースからパケットを受信します。
- proxy_smtp_server_ip および proxy_pop3_server_ip が 0.0.0.0 として指定されている場合、プロキシサービスは IPv4 クライアントのみに限定されたすべてのインタフェースからパケットを受信します。

次の変更は、IPv4 と IPv6 の両方のネットワークを待機するようにデーモンを設定します。

```
proxy_smtp_server_ip=all
proxy_pop3_server_ip=all
```

IPv6 クライアントを許可するように設定する

smtp_allow_client_ip を変更して、InterScan MSS デーモンの SMTP ストリームポートに接続できるクライアント IP アドレス (カンマまたはスペース区切り) を指定します。

- smtp_allow_client_ip が指定されていない場合、初期設定値は 127.0.0.1 です。
- smtp_allow_client_ip は、次の IP 形式で IPv4 アドレスと IPv6 アドレスをサポートしています。

  127.0.0.1

  ::1

  123.123.123.123

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

  123.123.123.123/24

  2001:db8:10ff::ae:44f2/64

  123.123.123.123-223

  2001:db8:10ff::ae:44f2-45ff

たとえば、localhost (IPv4 と IPv6 のいずれか) と IPv6 アドレス 2001:db8:10ff::ae:44f3 のみにデーモンへの接続を許可する場合は、次の設定を使用します。

```
smtp_allow_client_ip=127.0.0.1, ::1, 2001:db8:10ff::ae:44f3
```

ダウンストリーム IPv6 サーバを設定する

downstream_smtp_server_addr および downstream_smtp_server_port を変更して、ダウンストリーム MTA サーバまたはバックエンド MTA サーバの IP アドレスまたはホスト名およびポートを指定します。

注意

ホストの解決時に発生するセキュリティの問題を回避するため、IP アドレスを使用することをお勧めします。

- `downstream_smtp_server_addr` および `downstream_smtp_server_port` が指定されていない場合、初期設定値はそれぞれ `127.0.0.1` と 10026 です。
- `downstream_smtp_server_addr` は、次の IP 形式で IPv4 アドレスと IPv6 アドレスをサポートしています。

  127.0.0.1

  ::1

  123.123.123.123

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

  Domain.com

たとえば、ダウンストリーム IP アドレスが `2001:db8:10ff::ae:44f2` でポートが 25 の場合は、次の設定を使用します。

```
downstream_smtp_server_addr=2001:db8:10ff::ae:44f2
downstream_smtp_server_port=25
```

IPv6 設定を確認する

始める前に

次のパラメータを設定します。

- `proxy_smtp_server_ip`
- `proxy_pop3_server_ip`
- `smtp_allow_client_ip`
- `downstream_smtp_server_addr`

- downstream_smtp_server_port

パラメータを設定したら、次の手順を実行して設定を確認します。

手順

1. 次のコマンドを使用して InterScan MSS デーモンを再起動します。

   <InterScan MSS のインストール先>/imss/script/S99IMSS restart

2. 次のコマンドを使用してデーモンサービスの待機ポートを確認します。

   ```
   # netstat -ltpn|grep 10025
   #netstat -ltpn|grep 110
   ```

3. smtp_allow_client_ip リスト内の IP アドレスからデーモン IPv4/IPv6 SMTP ポートにメールメッセージを送信します。

   メールメッセージは正常に送信されます。

4. smtp_allow_client_ip リストにない IP アドレスからデーモン IPv4/IPv6 SMTP ポートにメールメッセージを送信します。

   メールメッセージは拒否されます。

5. デーモン IPv4/IPv6 POP3 ポートからのメールメッセージを受信します。

   メールメッセージは受信されます。

以上の手順で、InterScan MSS 9.1 の IPv6 サポートは正しく設定されます。

InterScan MSS をアンインストールする

次に、InterScan MSS のアンインストールの実行に必要な主な手順を示します。

手順

1. /$IMSS_HOME/imss/backup/uninstall.sh スクリプトファイルを実行して、InterScan MSS のアンインストールウィザードを開始します。

注意

上位/下位の配置では、下位デバイスをアンインストールしてから上位デバイスをアンインストールします。

2. <F12> キーを押してアンインストールを続行します。
3. 設定、ログ、キュー、およびデータベースデータの削除を確認します。
4. 進行状況バーが 100%になるまで待ちます。

   アンインストールが完了したことを示すメッセージが表示されます。

第 5 章

以前のバージョンからのアップグレード

この章では、以前のバージョンの InterScan Messaging Security Suite (以下、InterScan MSS) からのアップグレードについて説明します。

この章の内容は次のとおりです。

- 98 ページの「体験版からアップグレードする」
- 100 ページの「InterScan MSS Linux 9.1 にアップグレードする」
- 115 ページの「以前のバージョンから移行する」

体験版からアップグレードする

体験版のアクティベーションコードを入力して InterScan MSS をアクティベートされた場合、その日から始まる一定の試用期間の間、製品のすべての機能をご利用いただけます。この試用期間は、使用されているアクティベーションコードの種類により異なります。

試用期間の期限が切れる 14 日前になると、試用期間がまもなく終了することを知らせるメッセージが InterScan MSS の管理コンソールに表示されます。

引き続き InterScan MSS を使用するには、製品版ライセンスの購入が必要となります。購入後に、製品版の新しいアクティベーションコードが発行されます。

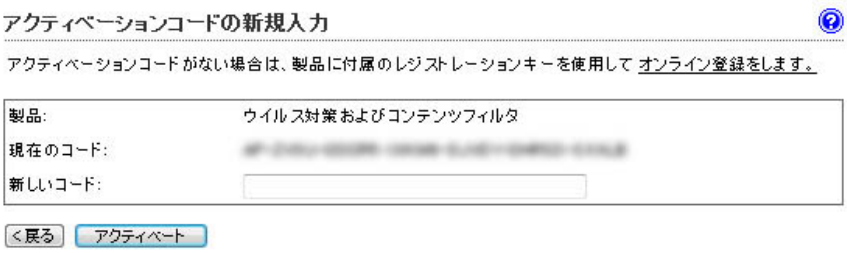
手順

1. [管理] > [製品ライセンス] の順に選択します。

[製品ライセンス] 画面が表示されます。

2. アクティベートする製品またはサービスのセクションにある [新規入力] ハイパーリンクをクリックします。

[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. 表示されたボックスに新しいアクティベーションコードを入力します。

注意

製品版の InterScan MSS を購入されると、メールで新しいアクティベーションコードが発行されます。アクティベーションコード (xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx 形式) の入力時にコードの入力ミスを防止するには、メールからアクティベーションコードをコピーしてボックスに貼り付けます。

4. [アクティベート] をクリックします。
5. アクティベートするすべての製品またはサービスに対して 2～5 の手順を繰り返します。

InterScan MSS Linux 9.1 にアップグレードする

データ転送の注意事項

InterScan MSS 7.1 と 9.1 では、ポリシーイベントログ、隔離されたメッセージ、およびアーカイブされたメッセージに使用するデータベーススキーマが異なります。そのため、データ転送はアップグレード中およびアップグレード後に実行されます。InterScan MSS 9.1 では、24 時間以内に生成されたデータはアップグレード中、24 時間を経過しているデータはアップグレード後に転送されます。

データ転送のステータスは、[ダッシュボード] 画面の通知領域に表示されます。通常、データ転送が完了するまでには、InterScan MSS 7.1 のデータベースのサイズに応じて最短でも 2.5 時間かかります。

注意

アップグレード前にメールトラフィックを停止して、ポリシーイベントログをデータベースにインポートしてください。インポートしないログはアップグレード中に失われます。ログのインポートが完了すると、`/INSTALLPATH/imss/bin/policy_event_bookmark` に記録された `polevt.imss.latesttime` ファイルのサイズが、`/INSTLLPATH/imss/log` の実際のファイルのサイズと同じになります。

InterScan MSS 7.1 Linux 版 SP2 Patch 1 から InterScan MSS 9.1 Linux 版にアップグレードする

InterScan MSS のセットアッププログラムを使用すれば、サポート対象プラットフォームの InterScan MSS 7.1 SP2 Patch 1 を自動的にアップグレードできます。セットアッププログラムでこのバージョンが検出されると、インストールプログラムでは次の処理を実行できます。

- 旧バージョンの InterScan MSS の設定をバックアップします。
- InterScan MSS をインストールします。
- 既存の設定を移行します。

セットアッププログラムでは、現在の InterScan MSS サーバの登録が Control Manager から解除されません。そのため、旧サーバ内のすべてのログについて、Control Manager から引き続きクエリを実行できます。

InterScan MSS を移行、または InterScan MSS に上書きインストールする

InterScan MSS 7.1 SP2 Patch 1 から移行、または InterScan MSS 7.1 SP2 Patch 1 に上書きインストールを実行する前に、次のことを確認してください。

- InterScan MSS 9.1 では、InterScan MSS 7.1 SP2 Patch 1 のすべてのデータが保持されます。

- InterScan MSS 9.1 では、InterScan MSS 7.1 SP2 Patch 1 の非表示キー設定がファイルに保持されます。
- InterScan MSS 9.1 では、InterScan MSS 7.1 SP2 Patch 1 のすべてのレポートが保持されます。
- InterScan MSS 9.1 では、InterScan MSS 7.1 SP2 Patch 1 の Control Manager のすべての設定が保持されます。
- 管理者は、InterScan MSS 7.1 SP2 Patch 1 が配置されているサーバへのメッセージトラフィックを停止する必要があります。

注意

アップグレード後または移行後、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場合は手動で有効にします。詳細については、「InterScan MSS 管理者ガイド」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 9.1 Linux 版に移行できない設定

アップグレードまたは移行後は、すべての検索サービスのデータと設定が保持されます。移行できない設定はありません。

InterScan MSS の設定をバックアップする

手動バックアップやロールバックの実行中は、RPM パッケージに対して操作を実行しないでください。操作を実行すると RPM パッケージが失われます。

手順

1. InterScan MSS 7.1 SP2 Patch 1 のコンポーネントがサーバにインストールされていることを確認します。

   次の表は、コンポーネント名とホームフォルダのマッピング関係を示しています。

コンポーネント名	ホームフォルダ
imss-7.1	`$IMSS_HOME`
imsscctrl	`$IMSS_HOME` **注意** **このホームフォルダは上位サーバにのみ存在します。**
imsseuq	`$IMSS_HOME`
nrs	`$NRS_HOME`
ipprofiler	`$IPP_HOME`

注意

ホームフォルダがわからない場合は、次のコマンドを実行します。

```
rpm -ql Components Name|tee 2|head -1
```

2. cron サービスを停止して、InterScan MSS 7.1 の設定をバックアップします。

   - OS が Red Hat 7 以上の場合は、次のコマンドを実行します。

     ```
     systemctl stop crond.service
     ```

     ```
     crontab -l >cronlist.bak
     ```

   - OS が Red Hat 7 未満の場合は、次のコマンドを実行します。

     ```
     service crond stop
     ```

     ```
     crontab -l >cronlist.bak
     ```

3. InterScan MSS 7.1 のメッセージトラフィックを約 5 分間停止します。

4. 次のコマンドを使用して、InterScan MSS 7.1 のすべてのプロセスを停止します。

   ```
   $IMSS_HOME/imss/script/imssstop.sh stop
   ```

```
$NRS_HOME/nrs/imssstop.sh

$IPP_HOME/ipprofiler/script/imssstop.sh
```

5. 次のコマンドを使用して、Postfix 設定ファイルをバックアップします。

```
tar cvf postfix_config.tar /etc/postfix
```

6. インストールされているすべての InterScan MSS 7.1 コンポーネントのホームフォルダをバックアップします。

```
tar cvf imss71.tar /$IMSS_HOME/imss

tar cvf nrs.tar /$NRS_HOME/nrs

tar cvf ipprofiler.tar /$IPP_HOME/ipprofiler
```

7. InterScan MSS 7.1 を初期設定のパスにインストールしておらず、内部データベースを使用している場合は、次のコマンドを使用してデータベースをバックアップします。

```
tar cvf default_path_folder.tar /opt/trend/imss
```

8. 次のコマンドを使用して、RPM データベース関連データをバックアップします。

```
tar cvf rpm.tar /var/lib/rpm
```

9. InterScan MSS 7.1 データベースをバックアップします。

   - InterScan MSS 7.1 にバンドルされている PostgreSQL を使用してデータベースを管理している場合は、次の操作を実行します。

     a. 次のコマンドを使用して、PostgreSQL サーバを停止します。

     ```
     $IMSS_HOME/imss/script/dbctl.sh stop
     ```

     b. 次のコマンドを使用して、PostgreSQL データをバックアップします。

     ```
     tar cvf imssdb.tar /var/imss
     ```

- 独自の PostgreSQL サーバを使用して InterScan MSS 7.1 データベースを管理している場合は、コールド物理バックアップとホット論理バックアップのいずれかを実行します。

InterScan MSS の単一サーバ配置をアップグレードする

注意

アップグレードまたは移行の際には、InterScan MSS 7.1 SP2 Patch 1 以上が必要です。

手順

1. 管理コンソールで、すべての InterScan MSS サービスが正常に稼働していることを確認します。

   [概要] 画面で、[管理下のサーバ設定] のすべてのサービスがアクティブになっています。

2. インストールパッケージのパスで InterScan MSS のアップグレードウィザードを開始します (`/imss/upgrade.sh`)。

3. <F12> キーを押してアップグレードを続行します。

4. <F12> キーを押して使用許諾契約書に同意します。

5. インストールされたコンポーネントとデータベースを確認し、<F12> キーを押して続行します。

6. 使用環境が最小システム要件をすべて満たしていることを確認し、<F12> キーを押して続行します。

7. 管理データベースの設定を確認し、<F12> キーを押して続行します。

   - 内部データベースを使用している場合は、ウィザードによってデータが PostgreSQL 9.6 の内部データベースに移行されます。
   - 外部データベースを使用している場合は、データをダンプして、PostgreSQL 9.6 データベースサーバに転送します。リモートデータベースの設定を完了します。

詳細については、108 ページの「外部の管理データベースをアップグレードする」を参照してください。

8. 進行状況バーが 100%になるまで待ちます。

   アップグレードが完了したことを示すメッセージが表示されます。

注意

送信者フィルタを Sendmail MTA とともに使用する場合は、追加の設定を実行して、Sendmail で FoxLib が確実に使用されるようにし、SMTP クライアントと通信する FoxProxy の実際の IP アドレスを取得する必要があります。詳細については、83 ページの「送信者フィルタを Sendmail とともに使用する」を参照してください。

InterScan MSS の分散配置をアップグレードする

InterScan MSS では、分散環境全体のアップグレードがサポートされるようになりました。たとえば、InterScan MSS が、上位と下位の配置で使用されているネットワークなどが該当します。

注意

アップグレードまたは移行の際には、InterScan MSS 7.1 SP2 Patch 1 以上が必要です。

IP プロファイラがエッジサーバに配置されており、検索サービスを別のダウンストリームサーバで実行する場合は、次の推奨タスクを実行してください。

1. IP プロファイラがインストールされている InterScan MSS 7.1 サーバをアンインストールします。
2. 残りの InterScan MSS 7.1 サーバを 9.1 にアップグレードします。
3. 既知のホスト設定と IP プロファイラを有効にします。

手順

1. アップグレードの準備をします。

a. InterScan MSS 設定のバックアップを作成します。

> **注意**
>
> 詳細については、102 ページの「InterScan MSS の設定をバックアップする」を参照してください。

b. 次のコマンドを使用して、Postfix キューにメッセージがないことを確認します。

```
postqueue -p
```

c. 管理コンソールで、すべての InterScan MSS サービスが正常に稼働していることを確認します。

[概要] 画面で、[管理下のサーバ設定] のすべてのサービスがアクティブになっています。

d. 次のコマンドを使用して、下位デバイスのすべてのサービスを停止します。

```
# /opt/trend/imss/script/imssstop.sh stop
```

> **注意**
>
> 分散配置では、上位デバイスを下位デバイスより先にアップグレードする必要があります。

e. 次のコマンドを使用して、下位デバイスのデータベースサービスを開始します。

```
#/opt/trend/imss/script/dbctl.sh start
```

2. 上位デバイスと下位デバイスをアップグレードします。

a. 上位デバイスをアップグレードします。

詳細については、105 ページの「InterScan MSS の単一サーバ配置をアップグレードする」を参照してください。

b. 次のコマンドを使用して、上位デバイスでデータベースが正常に動作していることを確認します。

```
# ps -ef |grep imss
```

次のような情報が表示されます。

```
imss 5602 0.0 0.2 63412 3376 ? S Oct14 1:09 /opt/trend/
imss/PostgreSQL/bin/postgres -D /var/imss/pgdata -i
```

c. 下位デバイスを 1 つずつアップグレードするか、いくつかまたはすべてを一度にアップグレードします。

警告!

すべてのデバイスのアップグレードが完了するまで、InterScan MSS サービスを再起動しないでください。

3. [アップグレードが必要なコンポーネント] の情報を見て、すべてのサーバがアップグレードされていることを確認します。

注意

送信者フィルタを Sendmail MTA とともに使用する場合は、追加の設定を実行して、Sendmail で FoxLib が確実に使用されるようにし、SMTP クライアントと通信する FoxProxy の実際の IP アドレスを取得する必要があります。詳細については、83 ページの「送信者フィルタを Sendmail とともに使用する」を参照してください。

各デバイスで設定を完了させます。

外部の管理データベースをアップグレードする

InterScan MSS 7.1 が外部の管理データベースとともにインストールされている場合は、InterScan MSS をアップグレードする前に PostgreSQL サーバをアップグレードします。さらに、105 ページの「InterScan MSS の単一サーバ配置をアップグレードする」で新しい PostgreSQL の情報を提供します。

PostgreSQL サーバをアップグレードするには、次の手順を実行します。

手順

1. アップグレード元の PostgreSQL サーバからデータベースをダンプします。

a. InterScan MSS のインストールパッケージをアップグレード元の PostgreSQL サーバにコピーして、パッケージを解凍します。

b. 環境変数を設定します。

```
export LD_LIBRARY_PATH=IMSSPackagePath/imss/imssbase/lib
```

c. 次のコマンドを実行して、データベースをダンプします。

```
IMSSPackagePath/imss/database/pg_dump -U DBUSERNAME -v -
Fc IMSSDBNAME > backupfile.tar
```

```
ex: pg_dump -U sa -v -Fc imss > backup_admin.tar
```

2. PostgreSQL サーバをバージョン 9.6 にアップグレードするか、新しい PostgreSQL 9.6 サーバを準備します。

a. InterScan MSS 7.1 の管理データベースアカウント (手順 1 で説明した「DBUSERNAME」) と同じデータベースアカウントを作成します。スーパーユーザの役割があることを確認します。

b. データベース接続の最大数を 600 に変更します。

```
vi /var/lib/pgsql/9.6/data/postgresql.conf
```

```
max_connection = 600 （初期設定では 100 です）
```

c. PostgreSQL サービスを再起動します。

d. InterScan MSS と外部のデータベースサーバが同じタイムゾーンと時刻設定を使用していることを確認します。

3. データベースを PostgreSQL 9.6 サーバに復元します。

a. `backupfile.tar` をアップグレード元の PostgreSQL サーバからアップグレード先の PostgreSQL サーバにコピーします。

b. InterScan MSS のインストールパッケージを新しい PostgreSQL サーバにコピーして、パッケージを解凍します。

c. ローカル認証方法を `pg_hba.conf` のパスワードに変更します。

```
change "local all all peer"
```

```
TO "local all all password"
```

d. PostgreSQL サービスを再起動します。

e. glibc.i686 ライブラリをインストールします。

f. 環境変数を設定します。

```
export LD_LIBRARY_PATH=IMSSPackagePath/imss/imssbase/lib
```

g. 次のコマンドを実行して、データベースを復元します。

```
IMSSPackagePath/imss/database/pg_restore -U DBUSERNAME -
d postgres -C -v -e < backupfile.tar

ex: pg_restore -U sa -d postgres -C -v -e <
backup_admin.tar
```

注意

pgrestore コマンドを実行すると、次のエラーメッセージが表示される場合があります。

```
pg_restore: connecting to database for restorePassword:
pg_restore: creating DATABASE xxxx
pg_restore: connecting to new database "xxxx"
pg_restore: connecting to database "xxxx" as user "xx"
pg_restore: creating SCHEMA public
pg_restore: creating COMMENT SCHEMA public
pg_restore: creating PROCEDURAL LANGUAGE plpgsql
pg_restore: [archiver (db)] Error while PROCESSING TOC:
pg_restore: [archiver (db)] Error from TOC entry 10536;
2612 94235 PROCEDURAL LANGUAGE plpgsql imss
pg_restore: [archiver (db)] could not execute query:
ERROR:  role "XXXX" does not exist
Command was: ALTER PROCEDURAL LANGUAGE plpgsql OWNER TO imss;
```

その場合は、エラーメッセージで要求されるデータベースの役割を追加します。このエラーが表示されてもデータベースは復元されます。データベースの役割を作成したら、復元されたデータベースを削除して、pgrestore コマンドを再度実行します。

4. pg_hba.conf のローカル認証方法を復元します。

5. PostgreSQL サービスを再起動します。

外部のエンドユーザメール隔離データベースをアップグレードする

InterScan MSS 7.1 サーバがエンドユーザメール隔離データベースのみとともにインストールされている場合、そのデータベースは外部のエンドユーザメール隔離データベースサーバと見なされます。このサーバで InterScan MSS 9.1 へのアップグレードを実行することはできません。エンドユーザメール隔離データベースの手動アップグレードが必要となります。

手順

1. アップグレード元の PostgreSQL サーバからエンドユーザメール隔離データベースをダンプします。

   詳細については、108 ページの「外部の管理データベースをアップグレードする」の手順 1 を参照してください。

2. PostgreSQL サーバをバージョン 9.6 にアップグレードするか、新しい PostgreSQL 9.6 サーバを準備します。

   詳細については、108 ページの「外部の管理データベースをアップグレードする」の手順 2 を参照してください。

3. エンドユーザメール隔離データベースを PostgreSQL 9.6 サーバに復元します。

   詳細については、108 ページの「外部の管理データベースをアップグレードする」の手順 3 を参照してください。

4. エンドユーザメール隔離データベースのスキーマをアップデートします。

```
CREATE TABLE
       tb_dl_entry_keys(  id serial NOT
       NULL ,
       distribution_list varchar(256),  submitter
       varchar(256),
       authentication_code varchar(8),  created_time
       timestamptz,  expired_time
       timestamptz,  heartbeat_time
       timestamptz,  is_logined int4
```

```
        DEFAULT 0
);
```

5. 元のエンドユーザメール隔離データベースをデタッチします。

   a. InterScan MSS 管理コンソールにログオンします。

   b. [管理] > [IMSS 設定] > [接続] の順に選択します。

   c. [データベース] タブをクリックします。

   d. データベースを無効にし、データベースの横にある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。

6. 新しいエンドユーザメール隔離データベースをアタッチします。

   エンドユーザメール隔離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。新しいエンドユーザメール隔離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。

アップグレードをロールバックする

アップグレード処理の間に問題が発生した場合は、InterScan MSS が自動的にロールバックを行います。ただし、自動ロールバックで問題が発生した場合には、手動ロールバックを実行する必要があります。

手順

1. cronjob サービスを停止して、cronjob を InterScan MSS 7.1 のインストール時の状態にロールバックします。

   - OS が Red Hat 7 以上の場合は、次のコマンドを実行します。

     ```
     systemctl stop crond.service

     crontab ./cronlist.bak
     ```

   - OS が Red Hat 7 未満の場合は、次のコマンドを実行します。

     ```
     service crond stop
     ```

```
crontab ./cronlist.bak
```

2. 次のコマンドを使用して、InterScan MSS 9.1 をアンインストールし、$IMSS_HOME フォルダを削除します。

```
$IMSS_HOME/imss/backup/uninstall.sh

rm -rf $IMSS_HOME
```

3. 次のコマンドを使用して、データフォルダを削除します。

```
rm -rf /var/imss/pgdata
```

4. パッケージ情報を InterScan MSS 7.1 のインストール時の状態にロールバックします。

```
tar xvf rpm.tar -C /

rpm --rebuilddb
```

5. 次のコマンドを使用して、InterScan MSS コンポーネントをロールバックします。

```
tar xvf imss71.tar -C /

tar xvf nrs.tar -C /

tar xvf ipprofiler.tar -C /
```

6. 内部データベースを使用しており、InterScan MSS コンポーネントが初期設定のパスにインストールされていない場合は、次のコマンドを実行します。

```
tar xvf default_path_folder.tar -C /
```

7. 次のコマンドを使用して、InterScan MSS 7.1 データベースにロールバックします。

```
tar xvf imssdb.tar -C /
```

8. 次のコマンドを使用して、Postfix 設定ファイルをロールバックします。

```
tar xvf postfix_config.tar -C /
```

9. InterScan MSS の自動起動スクリプトを再作成します。

- OS が Red Hat 7 未満の場合は、次の手順を実行します。

  a. $IMSS_HOME を実際のフォルダ名に置き換えて次のスクリプト情報をファイルに保存し、そのファイルを実行します。

```
work_directory=$IMSS_HOME/imss
RC_D="/etc/rc.d"
RCDIR0="/etc/rc.d/rc0.d"
RCDIR1="/etc/rc.d/rc1.d"
RCDIR2="/etc/rc.d/rc2.d"
RCDIR3="/etc/rc.d/rc3.d"
RCDIR4="/etc/rc.d/rc4.d"
RCDIR5="/etc/rc.d/rc5.d"
RCDIR6="/etc/rc.d/rc6.d"
RCDIR=$RCDIR3
RCINITDIR="$RC_D/init.d"

CreateLink()
{
    test -f $1 && (rm -rf $2 ; ln -s $1 $2)
}

CreateRCLinkLinux()
{
    if test -f $1 ; then
        if test ! -f $RCINITDIR/$2 ; then
            cp $1 $RCINITDIR/$2
            chmod +x $RCINITDIR/$2
        fi
        CreateLink $RCINITDIR/$2 $RCDIR2/$2
        CreateLink $RCINITDIR/$2 $RCDIR3/$2
        CreateLink $RCINITDIR/$2 $RCDIR5/$2
    fi
}

CreateRCKLinkLinux()
{
    if test -f $1 ; then
        if test ! -f $RCINITDIR/$2 ; then
            cp $1 $RCINITDIR/$2
            chmod +x $RCINITDIR/$2
        fi

        CreateLink $RCINITDIR/$2  $RCDIR0/$3
        CreateLink $RCINITDIR/$2  $RCDIR6/$3
    fi
}


CreateRCLinkLinux $work_directory/script/S99MONITOR S99MONITOR
CreateRCKLinkLinux $work_directory/script/S99MONITOR S99MONITOR K01MONITOR

CreateLink $work_directory/script/imssstop.sh $RCINITDIR/imssstop
CreateLink $RCINITDIR/imssstop  $RCDIR0/K00IMSSSTOP
CreateLink $RCINITDIR/imssstop  $RCDIR6/K00IMSSSTOP
CreateRCLinkLinux $work_directory/script/S99CMAGENT S99CMAGENT
CreateRCKLinkLinux $work_directory/script/S99CMAGENT S99CMAGENT K97CMAGENT
CreateRCLinkLinux $work_directory/bind/bindctl.sh S99bindctl
CreateRCKLinkLinux $work_directory/bind/bindctl.sh S99bindctl K03bindctl
CreateRCLinkLinux $work_directory/UI/adminUI/bin/Tomcat.sh S99IMSSUI
CreateRCKLinkLinux $work_directory/UI/adminUI/bin/Tomcat.sh S99IMSSUI K97IMSSUI
```

```
CreateRCLinkLinux $work_directory/script/S99FOXDNS S99FOXDNS
CreateRCKLinkLinux $work_directory/script/S99FOXDNS S99FOXDNS K02FOXDNS
CreateRCLinkLinux $work_directory/script/S99SCHEDULED S99SCHEDULED
CreateRCKLinkLinux $work_directory/script/S99SCHEDULED S99SCHEDULED K02SCHEDULED
CreateRCLinkLinux $work_directory/script/dbctl.sh S98dbctl
CreateRCKLinkLinux $work_directory/script/dbctl.sh S98dbctl K98dbctl
if [ -f $RCINITDIR/S99dbctl ];then
    DeleteRCLinkLinux S99dbctl K99dbctl
    DeleteRCLinkLinux S99dbctl K03dbctl
    CreateRCLinkLinux $work_directory/script/dbctl.sh S98dbctl
    CreateRCKLinkLinux $work_directory/script/dbctl.sh S98dbctl K03dbctl
fi
```

b. 次のコマンドを実行して、InterScan MSS サービスを自動的に開始します。

```
chkconfig --add S98dbctl
```

- OS が Red Hat 7 以上の場合は、次の手順を実行します。

a. `imss.service` ファイルを`/usr/lib/systemd/system` に作成します。

b. `$IMSS_HOME` を実際のフォルダ名に置き換えて次のスクリプト情報を `imss.service` ファイルに保存します。

```
[Unit]
Description=InterScan Messaging Security Suite
After=network.target remote-fs.target nss-lookup.target

[Service]
Type=simple
RemainAfterExit=yes
ExecStart=$IMSS_HOME/imss/script/imssstart.sh start
ExecStop=$IMSS_HOME/imss/script/imssstop.sh stop
PrivateTmp=true

[Install]
WantedBy=multi-user.target
```

c. 次のコマンドを使用して、InterScan MSS サービスを開始します。

```
systemctl enable imss.service
```

以前のバージョンから移行する

InterScan MSS 9.1 は、以前のバージョンの InterScan MSS からの移行をサポートしています。

以下の表は、InterScan MSS 9.1 への移行をサポートするバージョンを示しています。

表 5-1. サポートされる移行プラットフォームおよびバージョン

プラットフォーム	バージョン
InterScan MSS Solaris 版	7.0 Service Pack 1 Patch 4
InterScan MSS Linux 版	7.1 SP2 Patch 1

InterScan MSS Linux 9.1 に移行する

移行プロセスで必要な作業は次のとおりです。

- 手順 1: 以前のバージョンの InterScan MSS から設定をエクスポートする
- 手順 2: InterScan MSS 9.1 に設定をインポートする

InterScan MSS 7.1 SP2 Patch 1 から設定をエクスポートする

次の設定は移行されません。

表 5-2. 移行できない設定

MTA 設定	移行されない設定
MTA 設定	SMTP インタフェースの IP アドレスとポート
設定	データベース設定 (内部ファイルのパスなど)
	管理コンソールのパスワード
	Control Manager 設定

重要

設定をエクスポートする際は、InterScan MSS サーバが次の状態であることを確認します。

- データベース関連のタスクを実行していない。
- 停止または開始されていない。

下位デバイスの証明書の使用状況はエクスポートできません。

手順

1. 移行元の InterScan MSS サーバで、[管理] > [インポート/エクスポート] の順に選択します。

   [インポート/エクスポート] 画面が表示されます。

2. [エクスポート] をクリックします。

   InterScan MSS にインポート可能なパッケージに設定がエクスポートされます。

InterScan MSS 7.0 Service Pack 1 Patch 4 Solaris 版から設定をエクスポートする

手順

1. 移行ツールのパッケージ (`export_tool_sol_70.tar.gz`) を IMSS 7.0 Solaris 版サーバにコピーします。
2. 次のコマンドを使用して、エクスポートツールを解凍します。

```
gzip -d export_tool_sol_70.tar.gz
tar xf export_tool_sol_70.tar
```

注意

このツールは、暗号化されたパッケージに設定をエクスポートします。このパッケージは、他の InterScan Messaging Security 製品の同様の設定の複製にも使用できます。

3. 次のコマンドを使用して、現在の作業ディレクトリを変更します。

   ```
   cd export70sol
   ```

4. 次のコマンドを実行します。

   ```
   ./export_tool_70.sh
   ```

   このツールにより、エクスポート済みの設定パッケージ (`imss_config_70.tar.gz`) と詳細ログファイル (`export_70.<xxxxxxxx>.log`) が現在のディレクトリに作成されます。

移行されない InterScan MSS 7.0 Solaris 版 SP1 Patch 4 の設定

次を除くすべての InterScan MSS 7.0 Solaris 版 SP1 Patch 4 の設定が InterScan MSS 9.1 に移行されます。

- Control Manager エージェントのすべての設定
- 管理者アカウントのユーザ名とパスワード
- パターンファイルとエンジン
- SMTP インタフェースとポート番号
- システムパフォーマンスに影響する内部設定
- TLS 設定

InterScan MSS 9.1 に設定をインポートする

手順

1. InterScan MSS 9.1 の新規インストールを実行します。

   ヒント

   インポートする設定によって既存のすべての設定が上書きされるため、設定パッケージは InterScan MSS 9.1 の新規インストールにインポートすることをお勧めします。

2. 移行する設定が含まれているパッケージを取得します。
3. InterScan MSS 9.1 の管理コンソールで、[管理] > [インポート/エクスポート] の順に選択します。

   [インポート/エクスポート] 画面が表示されます。
4. 設定パッケージをインポートします。

注意

初期設定では、移行後はすべての下位デバイスが上位デバイスの証明書を使用します。上位デバイスの証明書を使用しない場合は、別の証明書を下位デバイスに割り当てます。

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] > [デバッグログのエクスポート] の順に選択します。
2. [検索サービス] でデバイスを選択します。
3. 何日分エクスポートするかを選択します。
4. [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。

第 6 章

FAQ

この章では、InterScan MSS のインストールに関するよくある質問 (FAQ) について回答を提供します。

この章の内容は次のとおりです。

- 122 ページの「Postfix MTA 設定」
- 122 ページの「インストールまたはアンインストール」

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。

インストールまたはアンインストール

外部 DNS サーバを使用するコンピュータに InterScan MSS 9.1 をインストールした場合、何か問題がありますか。

InterScan MSS 9.1 と DNS サーバを統合しても機能上の問題はありません。機能的には、同じコンピュータ上で InterScan MSS を外部 DNS サーバと統合できますが、パフォーマンスの理由からお勧めはしません。

既存の Apache サーバを使用するコンピュータに InterScan MSS 9.1 をインストールした場合、何か問題がありますか。

InterScan MSS では、エンドユーザメール隔離サーバの負荷分散の目的で、Apache サーバを`$IMSS_HOME/imss/UI/apache` ディレクトリにインストールします。ポートの競合がない場合は、既存の Apache サーバとの競合は発生しません。InterScan MSS Apache のポートは 8447 です。

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。

- 126 ページの「トラブルシューティングのリソース」
- 127 ページの「製品サポート情報」
- 127 ページの「サポートサービスについて」
- 128 ページの「セキュリティニュース」
- 129 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メニュー」をご覧ください。

サポートサービス内容は、予告なく変更される場合があります。また、製品に関するお問い合わせについては、サポートセンターまでご相談ください。トレンドマイクロのサポートセンターへの連絡には、電話またはお問い合わせ Web フォームをご利用ください。サポートセンターの連絡先は、「製品サポートガイド」または「スタンダードサポートサービスメニュー」に記載されています。

サポート契約の有効期限は、ユーザ登録完了から 1 年間です (ライセンス形態によって異なる場合があります)。契約を更新しないと、パターンファイルや検索エンジンの更新などのサポートサービスが受けられなくなりますので、サポートサービス継続を希望される場合は契約満了前に必ず更新してください。更新手続きの詳細は、トレンドマイクロの営業部、または販売代理店までお問い合わせください。

注意

サポートセンターへの問い合わせ時に発生する通信料金は、お客さまの負担とさせていただきます。

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。

索引

アルファベット

Control Manager
    Trend Micro Control Manager 参照, 30
FAQ
    Postfix, 122
imss.ini, 94
InterScan MSS について, 14
InterScan MSS
    概要, 14
IPv6, 89, 91
    確認, 94
    クライアントの許可, 92
    ダウンストリーム, 92
IP プロファイラ
    概要, 42
    機能, 42
    検出, 42
POP3
    配置計画, 60
Smart Protection, 34
Smart Protection Network, 36
Trend Micro Control Manager, 30
    エージェント, 30
    サーバ, 30
Web レピュテーションサービス, 35

あ

アップグレード
    InterScan MSS 7.1 SP2 Patch 1, 101
アドウェア, 25
一元化されたレポート機能, 44
インストール
    SMTP ゲートウェイ上, 56
    確認, 88
    手順, 81
    非武装地帯内, 57
    ファイアウォールなし, 53
    ファイアウォールの内側, 55
    ファイアウォールの外側, 54
インストールの確認, 88
エンドユーザメール隔離, 43

か

グレーメール, 37
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, 38

さ

準備
    IPv6 の確認, 90
    IPv6 の設定, 90
ジョークプログラム, 25
新機能, 8
スパイウェア/グレーウェア, 25
    アドウェア, 25
    ジョークプログラム, 25
    ダイヤラー, 25
    ネットワークへの侵入, 25
    パスワード解読アプリケーション, 25
    ハッキングツール, 25
    リスクと脅威, 26
    リモートアクセスツール, 25
セキュリティリスク
    スパイウェア/グレーウェア, 25
送信者フィルタ
    概要, 42

た

対象読者, 11

ダイヤラー, 25
ドキュメント, 11

な
ネットワークトポロジ, 52

は
パスワード解読アプリケーション, 25
ハッキングツール, 25
ファイルレピュテーションサービス, 35
フィルタ、機能, 20
プレフィルタサービス, 40

ま
マスメーリング型ウイルス
　パターン, 19
メール脅威
　スパム, 18
　非生産的メッセージ, 18
メールレピュテーション
　概要, 27
　種類, 27

ら
リモートアクセスツール, 25