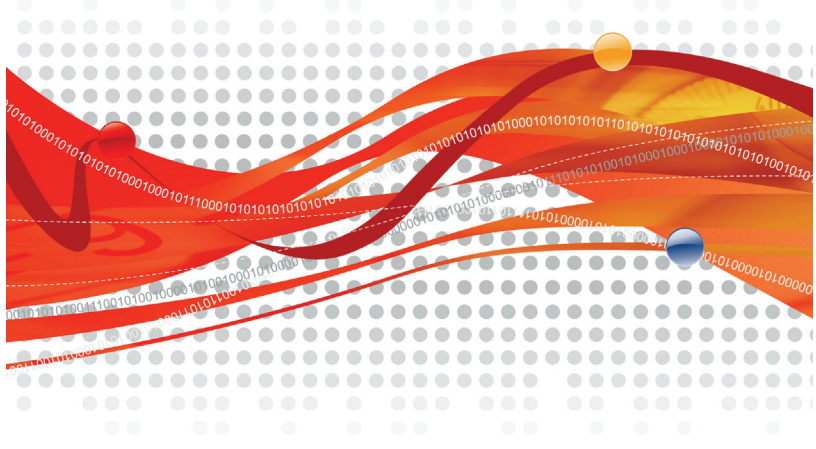
Trend Micro
InterScan Messaging Security Suite™



安心を、ひとつ上のステージへ。

TREND MICRO™

インストールガイド

※注意事項

トレンドマイクロへのお客様情報の送信について

- 「Webレピュテーションサービス」「フィッシング詐欺対策」「URLフィルタ」では、Webサイトの安全性の判定のために、お客様がアクセスしたURLの情報等(ドメイン、IPアドレス等を含む)を暗号化してトレンドマイクロのサーバに送信します。
  サーバに送信されたURL情報は、Webサイトの安全性の確認、および本機能の改良の目的にのみ利用されます。
  また、これらの機能を有効にしたうえで、コモンゲートウェイインタフェースアプリケーションを使用しているサーバで構築されているWebサイトにアクセスし、ID、パスワード等を入力した場合には、お客様がアクセスしたWebページのURLにお客様が入力したID、パスワード等が含まれた状態でトレンドマイクロのサーバに送信される場合があります。この場合、トレンドマイクロでは、お客様がアクセスするWebページの安全性の確認のため、これらのお客様より受領した情報にもとづき、お客様がアクセスするWebページのセキュリティチェックを実施します。
- 「ファイルレピュテーションサービス」では、ファイルの安全性の判定のために、ファイルのハッシュ値等の情報をトレンドマイクロのサーバに送信します。ファイルそのものや、ファイルの内容に関する情報は送信しません。
- 「ソフトウェア安全性評価サービス」では、プログラムの安全性の判定のために、プログラムの情報をトレンドマイクロのサーバに送信します。
- 「ウイルストラッキング/TrendCareプログラム」では、検出されたウイルス/脅威名、検出数、国/地域、感染元となったWebサイトのURLを、統計を取るためにトレンドマイクロのサーバに送信します。
- 「迷惑メール対策ツール」では、弊社製品の改良の目的および迷惑メールの判定精度の向上のため、トレンドマイクロのサーバに該当メールを送信します。また、迷惑メールの削減、迷惑メールによる被害の抑制を目指している政府関係機関に対して迷惑メール本体を開示する場合があります。
- 「E-mailレピュテーションサービス」では、スパムメールの判定のために、送信元のメールサーバの情報等をトレンドマイクロのサーバに送信します。
- 「スマートフィードバック」では、脅威に関する情報を収集、分析し保護を強化するために、ファイルのチェックサム、アクセスされたWebアドレス、サイズやパス等のファイル情報、実行ファイルの名前等の情報をトレンドマイクロのサーバに送信します。

輸出規制について

本製品は、外国為替及び外国貿易法、U.S. Export Administration Regulations、およびその他の国における輸出規制品目に該当している場合があります。したがって、本製品が輸出規制品目に該当する場合、適正な政府の許可なくして、禁輸国もしくは貿易制裁国の企業、居住者、国民、または、取引禁止者、取引禁止企業に対して、輸出もしくは再輸出できません。このような規制についての情報は以下のWebサイトから見つけることができます。

「http://www.treas.gov/ofac/」、および「http://www.bis.doc.gov/complianceandenforcement/ListsToCheck.htm」

2008年12月現在、米国により定められる禁輸国は、キューバ、イラン、北朝鮮、スーダン、シリアが含まれています。

あなたは本製品に関連した米国輸出管理法令の違法行為に対して責任があります。本契約の同意により、あなたは、あなたが米国により現時点で禁止されている国の居住者もしくは国民ではないこと、別途本製品を受け取ることが禁止されていないことを確認します。また、大量破壊を目的とした、核兵器、化学兵器、生物兵器、ミサイルの開発、設計、製造、生産を行うために使用しないことに同意します。

複数年契約について

- お客様が複数年契約（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://jp.trendmicro.com/jp/support/lifecycle/index.html

著作権について

本書に関する著作権は、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書面により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書またはその一部を複製することは禁じられています。本書の作成にあたっては細心の注意を払っていますが、本書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。本書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、ウイルスバスター、ウイルスバスター On-Line-Scan、PC-cillin、InterScan、INTERSCAN VIRUSWALL、ISVW、InterScanWebManager、ISWM、InterScan Message Security Suite、InterScan Web Security Suite、IWSS、TRENDMICRO SERVERPROTECT、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、トレンドマイクロ・プレミアム・サポート・プログラム、License for Enterprise Information Security、LEISec、Trend Park、Trend Labs、InterScan Gateway Security Appliance、Trend Micro Network VirusWall、Network VirusWall Enforcer、Trend Flex Security、LEAKPROOF、Trendプロテクト、Expert on Guard、InterScan Messaging Security Appliance、InterScan Web Security Appliance、InterScan Messaging Hosted Security、DataDNA、Trend Micro Threat Management Solution、Trend Micro Threat Management Services、Trend Micro Threat Management Agent、Trend Micro Threat Mitigator、Trend Micro Threat Discovery Appliance、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、Smart Protection Network、およびSPNは、トレンドマイクロ株式会社の登録商標です。

本書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 ©2002-2009 Trend Micro Incorporated. All rights reserved.

P/N: IMSSUX-AE0201_R1 (2009/10)

目次

はじめに 9

対象読者 10

InterScan MSS ドキュメント 10

ドキュメントの表記規則 11

第 1 章　InterScan MSS の概要 13

InterScan MSS の概要 14

新機能 14

InterScan MSS の主な機能と利点 15

スパイウェアと他の種類のグレーウェア 22

Web レピュテーションについて 23

Trend Micro Control Manager について 24

Control Manager との統合 25

第 2 章　コンポーネントの説明 29

InterScan MSS コンポーネントについて 30

InterScan MSS 管理データベース 30

セントラルコントローラ 30

検索サービス 30

ポリシーサービス 31

ポリシーの同期 31

エンドユーザメール隔離サービス 32

プライマリおよびセカンダリエンドユーザメール隔離サービス 32

エンドユーザメール隔離サーバコンポーネント 32

Apache および mod_jk 33

Tomcat 33

Struts フレームワーク 34
エンドユーザメール隔離アプリケーション 34
エンドユーザメール隔離データベース 34
IP フィルタ 35
Email Reputation Services 36
Email Reputation Services の種類 36
IP プロファイラの仕組み 37
Email Reputation Services の仕組み 38
ERS 管理コンソールを使用する 39
エンドユーザメール隔離について 42
一元化されたレポート機能について 42

第 3 章　配置計画 43

配置チェックリスト 44
コンポーネントおよびサブモジュールのインストール 47
InterScan MSS ポート 49
ネットワークトポロジに関する考慮事項 52
ファイアウォールを使用しないインストール 52
ファイアウォールの外側へのインストール 53
受信トラフィック 53
送信トラフィック 53
ファイアウォールの内側へのインストール 54
受信トラフィック 54
送信トラフィック 54
既存の SMTP ゲートウェイ上へのインストール 55
受信トラフィック 55
送信トラフィック 55
DMZ 内へのインストール 56
受信トラフィック 56

送信トラフィック 56
運用モデルについて 57
スタンドアロンモデル 57
サンドイッチモデル 58
インストールシナリオの理解 61
集中インストール 61
複数の検索サービスのインストール 63
複数のエンドユーザメール隔離サービスのインストール 65
エンドユーザメール隔離を配置する際のその他の検討事項 67
サーバ間の通信 68
複雑な分散インストール 68
WAN へのインストール 71
Trend Micro Control Manager 71
WAN のシナリオにおけるフォールトトレランスとフェイルオーバー 72
IP フィルタ 73
IP フィルタ機能を持つ InterScan MSS の配置 74
フェイルオーバーについて 74

第 4 章　InterScan MSS 7.1 のインストールおよびアンインストール 77

システム要件 78
MTA の準備 78
Postfix の準備 78
Sendmail の使用 79
Sendmail デーモン 79
Sendmail #1 の設定 80
Sendmail #2 の設定 81
Sendmail サービスの再起動 82
qmail の使用 83

qmail の設定 84
InterScan MSS コンポーネントとエンドユーザメール隔離のインストール 84
インストール手順 84
IP フィルタコンポーネントのインストール 87
Email Reputation Services と IP プロファイラのインストール 88
InterScan MSS の Sendmail および qmail との統合 91
FoxLib の Sendmail との統合 91
FoxLib の qmail との統合 92
インストールの確認 93
アンインストールの実行 94
InterScan MSS コンポーネントのアンインストール 94
Email Reputation Services と IP プロファイラのアンインストール 95
手動アンインストールの実行 95
InterScan MSS の手動アンインストール 95
データベースの手動アンインストール 96
Postfix の手動アンインストール 97
IP プロファイラの手動アンインストール 97

第 5 章　以前のバージョンからのアップグレード 99

体験版から移行する 100
InterScan MSS 7.0 から InterScan MSS 7.1 へアップグレードする 101
InterScan MSS 7.0 の設定を移行する 101
InterScan MSS 7.0 の設定をバックアップする 101
InterScan MSS 7.0 の単一サーバ配置をアップグレードする 103
InterScan MSS 7.0 の分散配置をアップグレードする 104
InterScan MSS 7.0 から InterScan MSS 7.1 へ移行する 106
InterScan MSS 7.0 の設定をエクスポートする 107
InterScan MSS 7.0 の設定を InterScan MSS 7.1 にインポートする 107
サポートされているサービスのアクティベーション 108

アップグレードをロールバックする 109
InterScan MSS 7.0 へロールバックする 109
InterScan MSS コンポーネントのアップグレード後にロールバックする 109
IP プロファイラのアップグレード後にロールバックする 110

第 6 章　トラブルシューティングとサポート情報 113
トラブルシューティング 114
よくある質問 (Q&A) 114
Postfix MTA 設定 114
インストールまたはアンインストール 115
製品サポート情報 116
サポートサービスについて 116
製品 Q&A のご案内 117
セキュリティ情報 117
セキュリティ情報の入手先 117
トレンドマイクロへのウイルス解析依頼 118
ウイルス解析サポートセンター「TrendLabs」 118

索引 121

はじめに

Trend Micro InterScan Messaging Security Suite 7.1 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、Trend Micro InterScan Messaging Security Suite7.1　(以下、InterScan MSS) の機能、システム要件、およびインストールとアップグレードの方法について説明しています。

InterScan MSS の設定方法については「Trend Micro InterScan Messaging Security Suite 7.1 管理者ガイド」を、またユーザインタフェースの詳細については管理コンソールから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。

- 10 ページの「対象読者」
- 10 ページの「InterScan MSS ドキュメント」
- 11 ページの「ドキュメントの表記規則」

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

本書は、読者の方に、ウイルス対策またはスパムメール対策技術についての知識があることを前提としていません。

InterScan MSS ドキュメント

InterScan MSS には、次のドキュメントが付属しています。

- **インストールガイド** — InterScan MSS の機能、システム要件、およびさまざまなネットワーク環境における InterScan MSS の配置およびアップグレード方法について説明しています。
- **管理者ガイド** — InterScan MSS のインストールと実行、およびインストール後の設定と管理方法について説明しています。
- **オンラインヘルプ** — 各フィールドの設定手順、およびユーザインタフェースを使用してすべての機能を設定する方法について説明します。オンラインヘルプにアクセスするには、管理コンソールを開いて、ヘルプアイコン ( ) をクリックしてください。
- **Readme ファイル** — 他のドキュメントには記載されていない可能性のある最新の製品情報を提供します。トピックには、機能の説明、インストールのヒント、既知の制限事項、および製品のリリースの履歴などが含まれます。

インストールガイド、管理者ガイド、および Readme ファイルは、

http://www.trendmicro.co.jp/download/ から入手できます。

ドキュメントの表記規則

このドキュメントでは、次の表記規則を使用しています。

表記	説明
注意：	設定上の注意
ヒント：	推奨事項
警告：	避けるべき操作や設定についての注意

表 1. 本書で使用している表記規則

第 1 章

InterScan MSS の概要

この章では、Trend Micro InterScan Messaging Security Suite 7.1 (以下、InterScan MSS) の機能、テクノロジ、およびスパムメール対策機能を強化するその他のトレンドマイクロ製品の概要について説明します。

この章の内容は次のとおりです。

- 14 ページの「InterScan MSS の概要」
- 14 ページの「新機能」
- 15 ページの「InterScan MSS の主な機能と利点」
- 22 ページの「スパイウェアと他の種類のグレーウェア」
- 23 ページの「Web レピュテーションについて」
- 24 ページの「Trend Micro Control Manager について」

InterScan MSS の概要

Trend Micro InterScan Messaging Security Suite 7.1 (以下、InterScan MSS) では、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メールを保護するコンテンツフィルタテクノロジが一元化されています。この柔軟性の高いソフトウェアソリューションには、高い評価を受けているウイルス対策機能およびゼロデイ保護機能が備わっており、既知のウイルスおよび潜在的なウイルスをブロックします。

スパムメール対策は多層構造となっており、IP プロファイラを介したカスタマイズ可能なトラフィック管理と Email Reputation Services による第 1 レベルの防御策と、さまざまな技術を組み合わせた強力な複合エンジンが統合されています。多言語スパムメール対策では、グローバルな企業に対して追加サポートが提供されます。高度なコンテンツフィルタ機能により、各種規格との適合および企業管理が達成され、機密情報が保護されます。InterScan MSS により、単一でスケーラビリティの高いプラットフォームで、管理が一元化され、ゲートウェイにおける総合的なメールセキュリティが実現します。

新機能

表 1-1 は、InterScan MSS で使用できる新機能の概要について説明しています。

表 1-1. InterScan MSS の新機能

新機能	説明
共通のポリシーオブジェクト	すべてのポリシーで使用できるいくつかの情報オブジェクトは、ポリシー作成から削除され、以下に示す独自の設定領域が確保されました。 ・ アドレスグループ ・ キーワードおよび式 ・ ポリシー通知 ・ スタンプ ・ DKIM 承認済みリスト ・ Web レピュテーション承認済みリスト
Web レピュテーション	メールメッセージに埋め込まれた不正なサイトに導く URL からクライアントを保護します。
NRS の用語の変更	Network Reputation Service (NRS) は、Email Reputation Services (ERS) に変更されました。

表 1-1. InterScan MSS の新機能 (続き)

新機能	説明
検出機能の強化	ポリシーで DKIM (DomainKeys Identified Mail) 承認済みリストや DKIM 適用ルールを使用することにより、該当ドメインに関する誤検出数を減少させて、フィッシングからの保護をサポートします。
X- ヘッダのサポート	メッセージの追跡や一覧化のため、X- ヘッダをメールメッセージに挿入します。
ファイル検索のサポートの拡大	Microsoft Office 2007 および Adobe Acrobat 8 ドキュメントの検索をサポートします。
新しい移行ツール	従来のバージョンの製品から円滑に移行するための新しいツールです。

InterScan MSS の主な機能と利点

次の表は、InterScan MSS によってネットワークにもたらされる主な機能と利点の概要について説明しています。

表 1-2. 主な機能と利点

機能	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。	InterScan MSS の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。

表 1-2.　主な機能と利点 (続き)

機能	説明	利点
IntelliTrap	ウイルス作成者は多くの場合、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 では、そのような圧縮ファイルをヒューリスティックに評価します。場合により、脅威ではないファイルにセキュリティ上のリスクがあると識別される可能性もあるため、IntelliTrap を有効にするときは、このカテゴリに分類された添付ファイルを隔離することをお勧めします。また、ユーザが圧縮ファイルを頻繁にやりとりする場合は、この機能を無効にすることができます。 初期設定では、IntelliTrap はウイルス対策ポリシーで検索条件の 1 つとして有効になっており、セキュリティ上のリスクとして分類された添付ファイルは隔離されるように設定されています。	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 では、ネットワーク内外に送信されるメールメッセージとその添付ファイルを分析して、適切なコンテンツかどうかをチェックします。	管理者が不適切だと判断したコンテンツ (個人的なやりとり、大容量の添付ファイルなど) は、InterScan MSS を使用してブロックしたり効果的に遅延することができます。
その他のメールの脅威に対する保護		
DoS 攻撃	巨大な添付ファイルでメールサーバをオーバーフローさせたり、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 を使用して、SMTP ゲートウェイで阻止したいメッセージの特徴を設定することができます。これにより、DoS 攻撃の発生を低減できます。

表 1-2.　主な機能と利点 (続き)

機能	説明	利点
不正なメールコンテンツ	多くのタイプの添付ファイル (実行可能プログラムや埋め込みマクロを含むドキュメントなど) は、ウイルスの隠れ蓑にな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、および ActiveX コンソールを含むメッセージも、有害な処理を実行する可能性があります。	InterScan MSS を使用して、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。
サービスの低下	多くの組織では、ビジネスに無関係のメールトラフィックが問題になっています。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、従業員の生産性にも影響します。また中には、会社のメッセージングシステムを使用して、就労時間中に個人的なメッセージを送信したり、大容量のマルチメディアファイルを転送したり、個人的なビジネスを行う従業員がいる場合があります。	多くの企業には、その組織のメッセージングシステムに最適な使用ポリシーがあります。InterScan MSS には、既存のポリシーを実行し、その遵守を確保するためのツールが用意されています。
法的責任とビジネスの完全性	メールを不正に使用することにより、会社が法的責任を負う状況に追い込まれることになる場合もあります。従業員が性的いやがらせや人種上のいやがらせ、または他の違法な活動に関与していることもあります。また、不誠実な従業員が会社のメッセージングシステムを使用して、機密情報を漏えいする可能性もあります。不適切なメッセージが会社のメールサーバから送信されると、メッセージに記された意見の内容がその会社のものでないとしても、会社の評判に傷がつきます。	InterScan MSS では、不適切な内容や機密資料を含むメッセージがゲートを通過するリスクを低減できる、コンテンツを監視およびブロックするためのツールを提供しています。

表 1-2.　主な機能と利点 (続き)

機能	説明	利点
マスメーリングウイルスの抑制	メールから発生したウイルスは、会社のメッセージングシステムを介して偽造のメッセージを自動的に拡散することがあります。それをクリーンナップするにはコストがかかり、そのウイルスによりユーザの間で混乱を引き起こす場合もあります。 InterScan MSS でマスメーリングウイルスを検出した場合、このウイルスに対する処理は他の種類のウイルスに対する処理と別にすることができます。 たとえば、重要な情報が記載された Microsoft Office ドキュメントの中でマクロウイルスが検出された場合、重要な情報が失われないように、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設定できます。しかし、マスメーリングウイルスが検出された場合は、メッセージ全体を自動的に削除するように設定できます。	マスメーリング型ウイルスが含まれたメッセージを自動的に削除すると、復元の価値がないメッセージやファイルの検索、隔離などにサーバリソースを消費しないようにできます。 既知のマスメーリングウイルスの識別情報は、マスメーリングパターンファイルに格納されます。このパターンファイルは TrendLabs （トレンドラボ) のアップデートサーバを使用してアップデートされます。この種類のウイルスおよびそのメールコンテナを自動的に削除することで、従業員からの問い合わせに対するヘルプデスクの対応が低減され、大規模感染後のクリーンナップ作業の手間が省けます。
スパイウェアと他の種類のグレーウェア		
スパイウェアと他の種類のグレーウェア	企業の顧客は、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、22 ページの「スパイウェアと他の種類のグレーウェア」を参照してください。	InterScan MSS が持つ、スパイウェアやその他の種類のグレーウェアからの保護機能により、セキュリティの上でも、機密性に関しても、法的な面でも、企業のリスクが大幅に軽減されます。

表 1-2.　主な機能と利点 (続き)

機能	説明	利点
スパムメール対策の統合		
スパムメール対策 (コンテンツ検索)	スパムメール対策 (コンテンツ検索) は、トレンドマイクロからライセンスされる製品であり、他のトレンドマイクロ製品に対してスパムメール検出サービスを提供します。スパムメール対策を使用するには、スパムメール対策のアクティベーションコードを取得します。詳細については、販売店に問い合わせてください。InterScan MSS のスパムメール対策機能は、組み込みのスパムメールフィルタを使用して機能します。このフィルタは、スパムメール対策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。 **注意：** IP プロファイラおよび ERS を設定する前に、スパムメール対策をアクティベートします。	スパムメール対策 (コンテンツ検索) で使用される検出テクノロジは、高度なコンテンツ処理および統計分析に基づいています。スパムメールを特定するための他の手法と異なり、コンテンツ分析はパフォーマンスが高く、スパムメール送信者がその技法を変えても、高度に適応できるリアルタイム検出を実現します。
IP プロファイラおよび ERS 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。ERS は、トレンドマイクロの中央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。	IP フィルタは、IP プロファイラと ERS で構成されます。IP フィルタを使用することにより、スパムメール送信者を IP レベルでブロックできます。

表 1-2.　主な機能と利点 (続き)

機能	説明	利点
その他		
LDAP およびドメインベースのポリシー	管理者権限およびユーザ / グループの定義に Lotus Domino や 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、LDAP を設定できます。 **注意：** エンドユーザメール隔離を使用するには、LDAP が必要です。	LDAP を使用すると、さまざまなルールを定義して、会社におけるメール使用のガイドラインを実行することができます。送信者または受信者のアドレスに基づいて、個人またはグループごとにルールを定義できます。
Web ベースの管理コンソール	Web ベースの管理コンソールを使用すると、InterScan MSS のポリシーと設定を効率的に指定することができます。	Web ベースのコンソールは SSL に対応しています。つまり、InterScan MSS へのアクセスに対するセキュリティが強化されています。
エンドユーザメール隔離	InterScan MSS では、スパムメールの管理効率を向上させるために、Web ベースのエンドユーザメール隔離機能を提供しています。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ことで、エンドユーザは独自のスパムメール隔離を管理できます。スパムメール対策 (コンテンツ検索) では、スパムメールと判断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。それにより、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。	Web ベースのエンドユーザメール隔離コンソールを使用して、エンドユーザは InterScan MSS によって隔離されるメッセージを管理できます。
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管理コンソールのセクションを選択できます。	管理者ロールを別の従業員に委任することで、管理職務の共有化を進めることができます。

表 1-2. 主な機能と利点 (続き)

機能	説明	利点
一元化されたレポート機能	一元化されたレポート機能により、(要求に応じた) 1 回限りのレポートや予約レポートを柔軟に生成できます。	InterScan MSS の実行内容を分析できます。 (要求に応じた) 1 回限りのレポートでは、必要に応じてレポートの内容の種類を指定できます。また、日次、週次、または月次で自動的にレポートを作成するように設定することもできます。
システム可用性の監視	組み込みのエージェントにより、InterScan MSS サーバの状況を監視し、障害状態によりメールフローが混乱する恐れがある場合、メールまたは SNMP トラップを使用して通知を配信します。	システム障害の検出時にメールおよび SNMP 通知を使用することより、直ちに修正作業を行い、停止時間を最小限に抑えることができます。
POP3 検索	管理コンソールから、POP3 メール検索を有効または無効にできます。	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 メッセージを検索することもできます。
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。

表 1-2.　主な機能と利点 (続き)

機能	説明	利点
Trend Micro 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、物理的な場所やプラットフォームにかかわりなく、中央から制御できる機能を提供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。 詳細については、24 ページの「Trend Micro Control Manager について」を参照してください。	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。トレンドマイクロ製品でメールから発生した新しいウイルスを検出した場合、TrendLabs （トレンドラボ) は InterScan MSS の詳細コンテンツフィルタを使用するポリシーを発行し、メッセージの疑わしい特徴を特定することでそのメッセージをブロックします。これらのルールにより、更新されたパターンファイルが使用可能になる前に感染が拡大する可能性を最小限に抑えることができます。

スパイウェアと他の種類のグレーウェア

企業ユーザは、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。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、企業に対して、深刻なセキュリティ上のリスクや機密保持のリスク、法的リスクをもたらします （表 1-3 を参照)。

表 1-3.　スパイウェア / グレーウェアの種類

スパイウェア / グレーウェアの種類	説明
スパイウェア / グレーウェア	アカウントユーザ名やパスワードなどのデータを収集し、サードパーティに送信します。
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 利用状況などのデータを収集します。
ダイヤラー	コンピュータのインターネット設定を変更し、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。

表 1-3.　スパイウェア / グレーウェアの種類 (続き)

スパイウェア / グレーウェアの種類	説明
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対して不正なアクセスをするためのツールです。
リモートアクセスツール	ハッカーがコンピュータに対してリモートにアクセスし、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。

Web レピュテーションについて

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「評判 (レピュテーション)」を割り当てることで、感染の連鎖を断ち切ることができます。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。

Trend Micro Control Manager について

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、物理的な場所やプラットフォームにかかわりなく、中央から制御できる機能を提供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 は、次のコンポーネントで構成されます。

- **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、このサーバからホストされます。

  注意： Control Manager 5.0 サーバ上で InterScan MSS と連携するには、Patch 3 以上をインストールする必要があります。

- **エージェント** — エージェントは、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、Control Manager による製品の管理を可能にします。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。

  注意： エージェントを個別にインストールする必要はありません。InterScan MSS をインストールすると、エージェントが自動的にインストールされます。

- **エンティティ** — エンティティは、Control Manager の製品ディレクトリ上の管理製品を表します。製品のディレクトリツリーには、各エンティティのアイコンが表示されます。Control Manager コンソールのディレクトリツリーには、すべての管理下のエンティティが表示されます。InterScan MSS もこれらのエンティティの 1 つです。

  InterScan MSS 検索サービスをインストールすると、Control Manager エージェントも自動的にインストールされます。エージェントが有効になると、検索サービスごとに Control Manager サーバに登録され、別々のエンティティとして表示されます。

注意： Control Manager を使用して InterScan MSS を管理する際は、Control Manager 5.0 サーバ (Patch 3 以上) を使用してください。最新のバージョンおよび最新の Patch とアップデートの詳細については、次のトレンドマイクロのアップデートセンターを参照してください。
http://www.trendmicro.co.jp/download/product.asp?productid=7

Control Manager との統合

表 1-4 に InterScan MSS でサポートされている Control Manager の機能のリストを表示します。

表 1-4. サポートされている Control Manager の機能

機能	説明	サポートの有無
双方向通信	双方向通信を使用して、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。
大規模感染予防ポリシー	TrendLabs (トレンドラボ) で開発された大規模感染予防ポリシー (OPP) は大規模感染に迅速に対応しており、InterScan MSS サーバまたはそのクライアントが感染する可能性を低くするために InterScan MSS が行うべき処理のリストが含まれています。 トレンドマイクロ アップデートサーバは、Control Manager を使用して InterScan MSS にこのポリシーを配信します。	あり
クエリ用のログのアップロード	検索の目的で 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 ERS 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 管理コンソールに先にログオンせずに、InterScan MSS を Control Manager から直接管理します。	なし。 Control Manager から InterScan MSS を管理するには、先に 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	既存の InterScan MSS サーバから新しい InterScan MSS サーバに Control Manager から設定を複製します。	あり
パターンファイルのアップデート	Control Manager から InterScan MSS が使用するパターンファイルをアップデートします。	あり
エンジンのアップデート	Control Manager から InterScan MSS が使用するエンジンをアップデートします。	あり

表 1-4.　サポートされている Control Manager の機能 (続き)

機能	説明	サポートの有無
製品コンポーネントのアップデート	HotFix や Patch などの InterScan MSS 製品コンポーネントを Control Manager からアップデートします。	なし。 製品コンポーネントをアップデートする手順については、特定の HotFix または Patch の Readme ファイル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 管理コンソール経由で InterScan MSS を設定します。	あり
製品登録の更新	InterScan MSS 製品ライセンスを Control Manager から更新します。	あり
Control Manager のメール関連レポート	次の InterScan MSS メール関連レポートを Control Manager から生成します。 • ウイルス検出ポイント [トップ 10] • すべてのエンティティのウイルス感染リスト • 感染メールの送信者 [トップ 10] レポート • セキュリティ違反 [トップ 10] レポート • ウイルス感染チャネル製品 - 関連レポート • 発生頻度別フィルタイベント • ポリシー別フィルタイベント • ゲートウェイメッセージスパムメール概要レポート • ゲートウェイメッセージスパムメール概要レポート (ドメイン用)	あり

表 1-4. サポートされている Control Manager の機能 (続き)

機能	説明	サポートの有無
Control Manager エージェントのインストールとアンインストール	InterScan MSS Control Manager エージェントを Control Manager から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 のインストール時に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手順を実行します。 1. メニューから [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、[Control Manager 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	InterScan MSS イベント通知を Control Manager から送信します。	あり
すべてのコマンドのコマンド追跡	Control Manager が InterScan MSS に発行するコマンドのステータスを追跡します。	あり

第 2 章

コンポーネントの説明

この章では、Trend Micro InterScan Messaging Security Suite 7.1 (以下、InterScan MSS) の管理に必要な要件、および InterScan MSS 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。

- 30 ページの「InterScan MSS コンポーネントについて」
- 35 ページの「IP フィルタ」
- 36 ページの「Email Reputation Services」
- 42 ページの「エンドユーザメール隔離について」

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、製品を個別のコンポーネントに切り分け、それぞれがメッセージ処理の特定のタスクを実行します。次の項では、各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、単一のコンピュータにも複数のコンピュータにもインストールできます。それぞれのコンポーネントが連携する仕組みは、61 ページの「インストールシナリオの理解」の図を参照してください。

InterScan MSS 管理データベース

InterScan MSS 管理データベースは、すべてのグローバル設定情報を保存します。データベースには、サーバ設定、ポリシー情報、ログ情報、およびコンポーネント間で共有されるその他の情報が格納されます。InterScan MSS をインストールする場合、他のコンポーネントをインストールする前に、データベースサーバをインストールして、適切なクエリを実行し、データベーステーブルを作成する必要があります。新しいデータベースをインストールすることも、既存の PostgreSQL データベースを使用することもできます。

セントラルコントローラ

セントラルコントローラには、Web サーバコンポーネントが含まれ、このコンポーネントにより、管理者が InterScan MSS を設定および制御するための管理コンソールを Web ブラウザで表示できるようになります。管理コンソールは、管理者と InterScan MSS データベースとの間のインタフェースとなり、さまざまなコンポーネントでそのデータベースを使用して、検索、ログ、およびその他のメッセージ処理を実行します。

検索サービス

検索サービスとして設定されたサーバは、次の処理を実行します。

- SMTP および POP3 メッセージトラフィックの受理
- ポリシーサービスへのポリシーのリクエスト
- 適切なポリシーに基づくメッセージの評価
- 評価結果に基づくメッセージに対する適切な処理の実行
- 隔離されたメッセージとアーカイブされたメッセージのローカルでの保存

- ポリシーおよびシステムの処理のローカルログへの記録、および指定した間隔での InterScan MSS データベースのログの自動更新。これを基にインデックスが作成され、隔離されたアイテムおよびログを検索できます。

検索サービスの設定は、管理コンソールを使用して検索サービスすべてにグローバルに適用されるため、同じハードウェア構成のサーバを指定して、検索サービスとして機能させます。使用している環境に同じハードウェア構成のコンピュータがない場合、最小のリソースを持つ検索サービスに保護を提供できるように、検索サービスの制限を設定します。たとえば、2 つの検索サービスがあり、1 つのコンピュータは 10GB のハードディスクを備え、もう 1 つは 80GB のハードディスクを備えているとします。この場合、最大ディスク使用量を 9GB に設定して、最小のリソースを持つコンピュータを保護します。

また、検索サービスのローカル設定ファイルを編集して、ローカルで制限を設定できます。この設定ファイルに設定された制限は、グローバル設定より優先されます。一度ローカルに設定された検索サービスは、管理コンソールからは設定できなくなります。また、インタフェースにローカル設定のすべての詳細が反映されなくなる場合があります。

注意： ローカル設定ファイル (.ini ファイル) を変更してカスタマイズする際は、十分に注意してください。必要に応じて、テクニカルサポートにお問い合わせください。

ポリシーサービス

パフォーマンスを向上させてルールの検索が効率的に実行されるように、InterScan MSS はポリシーサービスを使用して、メモリ内のキャッシュにメッセージルールを保存します。ポリシーサービスは検索サービスのルールのリモートストアとして機能し、ルールをキャッシュします。キャッシュにない場合はデータベース検索を行います (その場合、関連するネットワーク接続とディスク I/O のオーバーヘッドが発生します)。このメカニズムにより検索サービスの効率も向上し、ほとんどのメッセージ検索タスクは、ディスク処理を要することなく、検索サービスメモリ内で実行できます。

ポリシーの同期

InterScan MSS 管理データベーススキーマには、バージョン管理のメカニズムが組み込まれています。ポリシーサービスは、定期的にデータベースのバージョンをチェックします。データベースのバージョン番号がポリシーサービスにキャッシュされているバージョンと異なる場合、ポリシー

サービスはデータベースクエリを実行して、最新のバージョンを取得します。こうして、新規または変更されたエントリを調べるためにデータベース全体をチェックすることなく、データベースのキャッシュ版と実際のデータベースとの同期を維持します。

InterScan MSS の管理コンソールから変更を行うと、その変更は 3 分以内にポリシーサービスに反映されます。

エンドユーザメール隔離サービス

プライマリのエンドユーザメール隔離サービスには、InterScan MSS の管理コンソールと同様の Web ベースコンソールが生成されるため、ユーザは、処理されたスパムメールの表示、削除、または再送を行うことができます。

プライマリおよびセカンダリエンドユーザメール隔離サービス

負荷分散をサポートするために、追加のエンドユーザメール隔離サービス (セカンダリサービスと呼びます) をインストールできます。最初にインストールしたエンドユーザメール隔離サービス (プライマリサービスと呼びます) は、Apache を実行してセカンダリサービスと連携します。

エンドユーザメール隔離サーバコンポーネント

エンドユーザメール隔離サーバには、次のソフトウェアコンポーネントが含まれています。

- **Apache HTTP サーバ** — エンドユーザからの HTTP 要求を受け入れ、それをインストールされているエンドユーザメール隔離サーバすべてにわたって配信します。Apache は、プライマリエンドユーザメール隔離サーバにのみインストールされています。
- **Tomcat Application サーバ** — エンドユーザから HTTP 要求を受け入れ、それを Struts に渡します。
- **Struts フレームワーク** — エンドユーザに対するページ表示のフローを制御します。
- **エンドユーザメール隔離アプリケーション** — 他の InterScan MSS コンポーネントと通信して、エンドユーザメール隔離コンソールロジックを実装します。

Tomcat および Apache サーバは、{InterScan MSS}/UI ディレクトリにインストールされます。他のコンポーネントは、{InterScan MSS}/UI/euqUI ディレクトリにインストールされます。Apache および Tomcat はどちらも、{InterScan MSS}/script ディレクトリの S99EUQ スクリプトに制御され、停止、起動、および再起動のコマンドを受け入れます。

Apache および mod_jk

Apache HTTP サーバのバージョン 2.0.58 (http://httpd.apache.org/) は、プライマリエンドユーザメール隔離サーバにインストールされ、Apache Tomcat Connector mod_jk (http://tomcat.apache.org/connectors-doc/) ロードダブルモジュールを使用して、すべての要求をローカルでインストールされた Tomcat Application サーバへ転送します。

Apache は、標準の Apache ServerRoot 構造を持つ、{InterScan MSS}/UI/apache ディレクトリにインストールされます。Apache のメイン設定ファイル ({InterScan MSS}/UI/euqUI/conf ディレクトリ内の EUQ.conf) では、Apache によって転送される要求をすべて受信する Tomcat スレッドの名前と共に、Apache の受信接続の TCP ポート (8447)、サービス接続の最大数 (150) および mod_jk の設定が定義されています。

Tomcat

エンドユーザメール隔離サーバでは、Tomcat Application サーバを使用してエンドユーザからの要求が処理されます。また、プライマリエンドユーザメール隔離サーバにインストールされた Tomcat Application サーバも、Apache HTTP サーバからの要求を受け入れ、Apache JServ Protocol バージョン 1.3 プロトコル AJP13 (http://tomcat.apache.org/tomcat-3.3-doc/AJPv13.html を参照) とラウンドロビンアルゴリズムを使用して、インストールされたエンドユーザメール隔離サーバすべてにわたって負荷を分散します。

Tomcat 設定ファイル ({InterScan MSS}/UI/euqUI/conf ディレクトリ内の server.xml) では、TCP ポート (8446)、プロトコル (HTTPS)、SSL キーリングの場所 ({InterScan MSS}/UI/tomcat/sslkey/.keystore) など、さまざまな設定が定義されています。

{InterScan MSS}/UI/euqUI/conf ディレクトリ内の workers.properties 設定ファイル (http://tomcat.apache.org/tomcat-3.3-doc/Tomcat-Workers-HowTo.html) に、Tomcat worker スレッドの設定が記述されています。ここでは、loadbalancer と worker の 2 種類のスレッドが定義されています。loadbalancer スレッドは、インストールされたエンドユーザメール隔離サーバのすべてにわたって負荷を分配します。worker スレッドは、受信要求を処理し、エンドユーザメール隔離アプリケーションを実行します。この設定ファイルは Manager により自動的に管理され、tb_component_list データベーステーブルから使用できるすべてのエンドユーザメール隔離サーバに関する情報に基づいて再起動中にアップデートされます。

AJP13 プロトコルにより、Apache と Tomcat 間は常時接続され、この接続を使用して、オーバヘッドを増やさずに要求を Tomcat へ転送し、その要求の処理結果を受信します。

Struts フレームワーク

Struts は Model-View-Controller Java ベースのフレームワークで、これを使用して、HTTP 要求を処理する複雑な Java ベースのアプリケーションの開発と制御を容易にします (http://struts.apache.org/ を参照)。

Struts は受信 HTTP 要求、その要求を処理する Java プログラム (Servlet) およびこの処理の結果を表示するために使用される Java Server Page (JSP) の間の関係を制御します。

Struts 自体は、struts-config-common.xml および struts-config-enduser.xml という設定ファイルによって設定された struts.jar アーカイブファイル内でパッケージ化された一連の Java クラスです。

エンドユーザメール隔離アプリケーション

エンドユーザメール隔離アプリケーションは Java で記述され、エンドユーザの要求に基づいて、隔離されたメールメッセージを表示、隔離解除、または削除します。また、エンドユーザが承認済み送信者リストを管理できるようにします。

この機能を実装するために、エンドユーザメール隔離は管理データベースおよびエンドユーザメール隔離データベースにアクセスしてマネージャと通信します。

エンドユーザメール隔離アプリケーションは、{InterScan MSS}/UI/euqUI/ROOT/WEB-INF/classes ディレクトリ内に格納された com.trendmicro.imss.ui パッケージの一連の Java クラスと {InterScan MSS}/UI/euqUI/ROOT/jsp ディレクトリ内に格納された一連の Java Server Pages として実装されます。

エンドユーザメール隔離アプリケーションは、{InterScan MSS}/log/imssuieuq.< 日付 >.< カウント > ログファイルにログエントリを書き込みます。imss.ini ファイルの [general] / log_level 管理設定は、エンドユーザメール隔離アプリケーションによって書き込まれる情報量を制御します。ログに記録される情報量を増やすには、log_level を「debug」に設定し、S99EUQ スクリプト「S99EUQ restart」を使用して Tomcat を再起動します。

エンドユーザメール隔離データベース

エンドユーザメール隔離データベースは、隔離されたスパムメール情報およびエンドユーザが承認済みの送信者リストを保存します。エンドユーザメール隔離サービスをインストールする場合、エンドユーザメール隔離データベースもインストールする必要があります。スケーラビリティを高めるために、複数のデータベースをインストールすることもできます。また、既存の PostgreSQL データベースサーバを使用して、エンドユーザメール隔離データベースをインストールすることもできます。

次のいずれかのオプションで、imsseuq と呼ばれるエンドユーザメール隔離データベースをインストールできます。

- 管理データベースをホストするデータベースサーバにインストール
- ネットワーク内で使用可能な別のデータベースにインストール
- データベースサーバのソフトウェアと共にインストール

1 つの InterScan MSS インスタンスは、最大 8 つのエンドユーザメール隔離データベースに対応できます。エンドユーザメール隔離データは、すべてのエンドユーザメール隔離データベースに分散されます。あるデータベースが消失した場合、このデータベースに格納されたデータを持つユーザは隔離されたデータにアクセスできなくなります。

IP フィルタ

InterScan MSS には、IP フィルタがオプションで搭載されています。

- **IP プロファイラ** — メールトラフィックの分析に使用するしきい値の設定ができます。ある IP アドレスからのトラフィックがこの設定に違反した場合、IP プロファイラは送信者の IP アドレスをデータベースに追加し、その IP アドレスからの受信接続をブロックします。

  IP プロファイラは、次の 4 つのインターネットの脅威を検出します。

  - **スパムメール** — 不要な広告コンテンツが含まれるメール。
  - **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 攻撃** — 有効なドメイン名を持つ任意のメール名を組み合わせ、任意のメールアドレスを作成して有効なメールアドレスを収集するために、スパムメール発信者が使用する方法。メールは作成されたメールアドレスに送信されます。メールメッセージが配信されると、メールアドレスは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」フィールドに対象のメールドメインが記述されたメールメッセージを生成する攻撃。架空のアドレスでメールメッセージを送信し、それをエラーで返送しようとすると、対象のメールサーバはオーバーフローします。
- Email Reputation Services (ERS) — 既知のスパムメール送信者からのメールをネットワーク (IP) レベルでブロックします。

Email Reputation Services

Email Reputation Services (ERS) 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。

Email Reputation Services の種類

ERS は、標準と詳細の 2 種類のサービスを提供します。

Email Reputation Services 標準

このサービスでは、Trend Micro Smart Protection Network により強化された、トレンドマイクロのレピュテーションデータベースと照合して、要求された IP アドレスを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。

ERS 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した場合、指定されたメールサーバは標準レピュテーションデータベースサーバに対して DNS クエリを実行します。そのホストが標準レピュテーションデータベースに存在すれば、ERS 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。ERS からのスパムメールの識別情報を基に、そのメッセージに対して適切な処理を実行するように MTA を設定できます。

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は、受信せず、ブロックするように MTA を設定することをお勧めします。

Email Reputation Services 詳細

このサービスは、膨大な量のスパムメールの送信処理中に、メールソース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発信元が現れると、直ちに (通常はスパムメールの最初の兆候の数分以内) 動的レピュテーション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、動的レピュテーションデータベースもそれに応じて更新されます。

ERS 詳細は、ERS 標準と同様に DNS クエリベースのサービスですが、標準レピュテーションデータベースと動的レピュテーションデータベース (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 つの異なるデータベースに、2 つのクエリを実行できます。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発信元に素早く対応できる、非常に効果的で効率的なデータベースを維持できます。ERS 詳細サービスは、お客さまのネットワークで全受信接続の 80% 以上 (すべて不正接続) 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。

IP プロファイラの仕組み

IP プロファイラは、35 ページの「IP フィルタ」で記載された脅威が含まれるメールを送信するコンピュータの IP アドレスを能動的に特定します。InterScan MSS が IP アドレスに対して指定された処理を開始するタイミングを決める複数の条件をカスタマイズできます。条件は潜在的な脅威によって異なりますが、一般的には InterScan MSS が IP アドレスを監視する期間としきい値が含まれます。

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。

InterScan MSS が送信メールサーバから接続要求を受信すると、次の処理が発生します。

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

   IP アドレスがブロックリストに含まれていない場合、InterScan MSS は IP プロファイラで指定したしきい値条件に従ってメールトラフィックを分析します。
3. メールトラフィックが条件に違反する場合、InterScan MSS は送信者の IP アドレスをブロックリストに追加します。

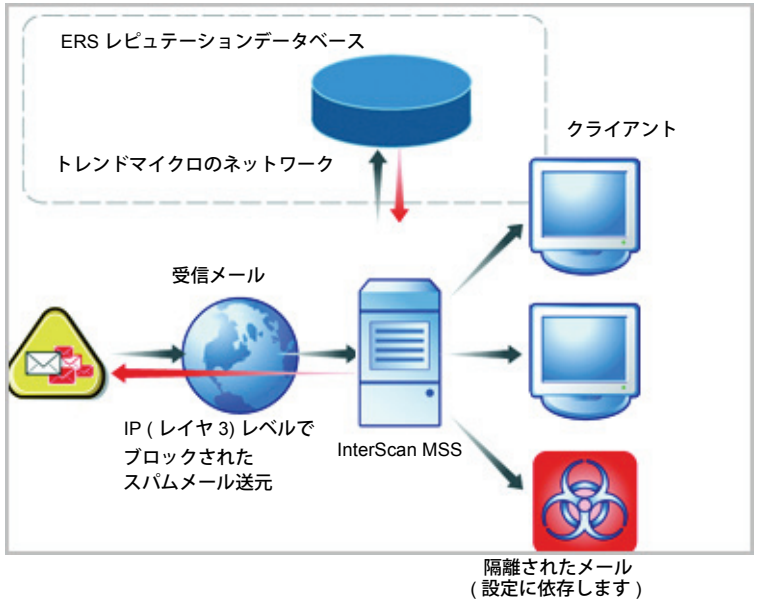
Email Reputation Services の仕組み

Email Reputation Services は、ドメインネームサービス (DNS) クエリベースのサービスです。InterScan MSS が送信メールサーバから接続要求を受信すると、次の処理が発生します。

1. InterScan MSS は、接続を要求するコンピュータの IP アドレスを記録します。
2. InterScan MSS は、その IP アドレスをトレンドマイクロの ERS DNS サーバに転送して、レピュテーションデータベースに問い合わせます。その IP アドレスがスパムメールの発信元としてレポートされている場合、その問い合わせの時点でデータベースにアドレスのレコードが存在しているはずです。
3. レコードが存在する場合、ERS は InterScan MSS に、接続要求を常にまたは一時的にブロックするよう指示します。要求をブロックする判断は、スパムメールの発信元の種類、履歴、現在の活動レベル、およびその他の観測パラメータにより異なります。

図 2-1. は、ERS の仕組みについて説明しています。

図 2-1. ERS の仕組み



Email Reputation Services の動作の詳細については、
http://jp.trendmicro.com/jp/products/enterprise/ers/ersa/index.html を参照してください。

ERS 管理コンソールを使用する

グローバルスパムメール情報へのアクセス、レポートの表示、ERS 設定の作成や管理などの管理作業を実行する場合は、ERS 管理コンソールにログオンします。

このセクションでは、ERS 管理コンソールを使用するための基本的な手順を説明します。各画面の設定に関する詳細な手順については、ERS 管理コンソールのオンラインヘルプを参照してください。ヘルプ画面の右上隅にあるヘルプアイコンをクリックして、オンラインヘルプにアクセスします。

ERS 管理コンソールを開くには

1. Web ブラウザを開き、次のアドレスを入力します。

   https://tmspn.securecloud.com/

2. Email Reputation Services のユーザ名とパスワードを使用してログオンします。Smart Protection Network ポータルが開き、[Email] タブが選択され、[一般] 画面が表示されます。
3. メニューから [グローバルスパムメール情報] を選択します。[グローバルスパムメール情報] 画面が表示されます。

   [グローバルスパムメール情報] 画面では、受信したスパムメールの量に基づいて、ISP のランクが付けられます。 [ISP 毎の送信量] リストには、特定の週内に上位 100 の ISP から送信されたスパムメールの総量が表示されます。一番多くのスパムメールを送信しているネットワークが上位にランク付けられます。ISP のランクは毎日変わります。 [ISP 毎の送信量] リストには次の項目が表示されます。

表 2-1.　ISP スパムメールリスト

列	説明
ランク　(今週)	今週のグローバルランクをスパムメールの総量に基づいて表示します。
ランク　(先週)	先週のグローバルランクをスパムメールの総量に基づいて表示します。
ASN	Autonomous System Number　(ASN) は、1 社以上の通信事業者が運営する、明確に定義された単一のルーティングポリシーを持つ IP ネットワークのグループに対するグローバル一意識別子です。
ISP 名	特定の ASN に対する登録名。一部の ISP では複数の ASN を保有していることがあります。この場合、テーブルに複数個登録されます。

表 2-1. ISP スパムメールリスト (続き)

列	説明
スパムメール量 (24 時間)	過去 24 時間内に送信されたスパムメールの推定総量。この総量は 1 時間ごと更新されます。
ボットネット活動	メールサーバに対するボットネットの活動状況の指標。ボットネットとは、中央からスパムメール送信元によって制御されている、ウイルスに感染したコンピュータのグループのことであり、現在インターネット上で最大のスパムメール送信元となっています。この数値は、1 時間前からのボット数におけるパーセント比率の変化を示します。ボットネットの活動を確認するには、[有効なメールサーバ] リストにメールサーバを追加する必要があります。

4. リリースアップデート をクリックします。リリースアップデート画面が表示されます。

   リリースアップデート画面には、新しいスパムメールに関する最新情報と、Email Reputation Services で使用可能な新機能が表示されます。次のタブをクリックすると情報が表示されます。

   - **スパムメール情報** 現在のスパムメールの手口に関する簡単な概要と説明、および組織に対する影響を示します。また、新しい手口がどのように配置されているか、この手口がどのようにトレンドマイクロシステムを通過するか、これらの新しい脅威に対してトレンドマイクロがどのように対応しているかについてを説明します。
   - **リリース情報** Email Reputation Services で使用可能な新機能の概要について説明します。

5. MTA と ERS データベースサーバ間の動作をまとめたレポートを表示するには、次の操作を実行します。

   a. メニューから [レポート] を選択します。サブメニューが表示されます。

   b. 次のいずれかをクリックします。

表 2-2. レポートの種類

レポート	説明
クエリの割合	このレポートは、IP アドレスの一致を返したクエリのパーセント比率を表示します。IP アドレスの一致は、メールサーバとの接続を確立しようとする送信者が、既知のスパムメール送信元であることを示します。レポートは、個々のスパムメールメッセージではなく、接続に基づいて作成されます。
1 時間あたりのクエリ数	このレポートは、メールサーバがレピュテーションデータベースにクエリを実行した回数を表示します。

表 2-2. レポートの種類 (続き)

レポート	説明
1 日あたりのクエリ数	このレポートは、メールサーバがレピュテーションデータベースにクエリを実行した 1 日あたりの回数を表示します。
ボットネットレポート	このレポートは、有効なメールサーバとして登録されているサーバを発信元とする、過去 7 日間のスパムメール活動の簡単な概要を示します。指定した IP アドレスのいずれかにおいて、過去 7 日間にスパムメール活動が見つかった場合には、赤いロボットアイコンが表示されます。

6. ERS 設定によって提供される保護を管理するには
   a. メニューから [ポリシー] を選択します。サブメニューが表示されます。
   b. 次のいずれかをクリックします。

表 2-3. ポリシー設定

ポリシー	説明
設定	承認済み送信者リストとブロックする送信者リストを設定します。 国別または ISP 別の個々の IP アドレスおよび CIDR ごとに、リストを定義できます。 ・ **承認済み送信者**: 承認済み送信者からのメッセージを許可して、IP レベルのフィルタを無視します。承認済み送信者リストは MTA に適用されませんが、追加の承認済み送信者リストまたはブロックする送信者リストを設定したり、MTA に対して追加のフィルタを実行することができます。 ・ **ブロックする送信者**: 特定の国、ISP、および IP アドレスからのメールメッセージを常にブロックするように ERS に指示します。
新規 ISP のリクエスト	トレンドマイクロでは、サービスに追加する他のインターネットサービスプロバイダ (ISP) に関する、お客さまからの助言をお待ちしています。 できる限り多くの ISP に関する情報を記入してください。この情報は、トレンドマイクロが ISP をサービスに追加するのに役立ちます。
Reputation 設定	ERS Standard と ERS Advanced の各設定を行います。 標準のお客さまには、[Standard 設定を有効にする] のみが表示されます。 詳細のお客さまには、[Dynamic 設定] セクションと [Standard 設定を有効にする] セクションの両方が表示されます。

7. パスワードまたはアクティベーションコードを変更する、または ERS にメールサーバを追加するには、メニューから [管理] を選択します。

エンドユーザメール隔離について

InterScan MSS では、スパムメールの管理効率を向上させるために、Web ベースのエンドユーザメール隔離機能を提供しています。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ことで、エンドユーザは独自のスパムメール隔離を管理できます。(InterScan MSS とは別のライセンスとなる) スパムメール対策 (コンテンツ検索) または管理者が作成したコンテンツフィルタでスパムメールと判断されたメッセージは、隔離領域に移動されます。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ます。これにより、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 の実行内容を分析するには、一元化されたレポート機能を使用します。(要求に応じた) 1 回限りのレポートまたは自動生成レポート (日次、週次、または月次) を設定することができます。

第 3 章

配置計画

本章では、InterScan MSS の配置を計画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。

- 44 ページの「配置チェックリスト」
- 47 ページの「コンポーネントおよびサブモジュールのインストール」
- 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に関する考慮事項」
- 57 ページの「運用モデルについて」
- 61 ページの「インストールシナリオの理解」
- 73 ページの「IP フィルタ」
- 74 ページの「フェイルオーバーについて」

配置チェックリスト

配置チェックリストでは、InterScan MSS を配置するためのインストール前とインストール後のタスクに関する手順を段階的に示します。

表 3-1.　配置チェックリスト

チェックマーク (完了時)	タスク	オプション	参照
	手順 1 — InterScan MSS の場所の特定		
	InterScan MSS をインストールするネットワーク上の場所を、次のいずれかから選択します。		
	・ ファイアウォールなし		52 ページの「ファイアウォールを使用しないインストール」
	・ ファイアウォールの外側		53 ページの「ファイアウォールの外側へのインストール」
	・ ファイアウォールの内側		54 ページの「ファイアウォールの内側へのインストール」
	・ 既存の SMTP ゲートウェイ上		55 ページの「既存の SMTP ゲートウェイ上へのインストール」
	・ DMZ 内		56 ページの「DMZ 内へのインストール」
	手順 2 — 範囲の計画		
	InterScan MSS をインストールするのは、単一のサーバか複数のサーバかを選択します。		
	・ 集中インストール		61 ページの「集中インストール」
	・ 複数の検索サービス		63 ページの「複数の検索サービスのインストール」

表 3-1.　配置チェックリスト (続き)

チェックマーク (完了時)	タスク	オプション	参照
	• 複数のエンドユーザメール隔離		65 ページの「複数のエンドユーザメール隔離サービスのインストール」
	• 複雑な分散インストール		68 ページの「複雑な分散インストール」
	• 広域ネットワーク		71 ページの「WAN へのインストール」
	• IP フィルタ ヒント： フェイルオーバーの方法を検討してから、範囲を決定することをお勧めします。		73 ページの「IP フィルタ」
	手順 3 — インストールまたはアップグレード		
	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		78 ページの「MTA の準備」
	• InterScan MSS コンポーネントのインストール		84 ページの「InterScan MSS コンポーネントとエンドユーザメール隔離のインストール」
	• IP フィルタのインストール	あり	87 ページの「IP フィルタコンポーネントのインストール」
	• 正常なインストールの確認		93 ページの「インストールの確認」
	手順 4 — InterScan MSS の基本設定		
	設定ウィザードに従って、セントラルコントローラの設定を手順 7 まで進めます。		

表 3-1.　配置チェックリスト (続き)

チェックマーク (完了時)	タスク	オプション	参照
	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」の項
	手順 5 — サービスの開始		
	さまざまな脅威からネットワークを保護する、InterScan MSS サービスを起動します。		
	• 検索サービス		管理者ガイドの「InterScan MSS サービス」の項
	• ポリシー		
	• エンドユーザメール隔離	あり	
	手順 5 — InterScan MSS のその他の設定		
	InterScan MSS のさまざまな設定を行い、InterScan MSS を起動します。		
	• IP フィルタのルール	あり	管理者ガイドの「IP フィルタサービス」の項
	• SMTP ルーティング		管理者ガイドの「SMTP メッセージの検索」の項
	• POP3 設定	あり	管理者ガイドの「POP3 メッセージの検索」の項
	• 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」の項
	• コンポーネントの手動アップデートの実行と予約アップデートの設定		管理者ガイドの「検索エンジンとパターンファイルのアップデート」の項
	• ログの設定		管理者ガイドの「ログの設定」の項
	手順 6 — InterScan MSS のバックアップ		
	システム障害時の予防措置として、InterScan MSS の全体または最小限のバックアップの作成を実行します。		

表 3-1.　配置チェックリスト (続き)

チェックマーク (完了時)	タスク	オプション	参照
	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」の項
	最小限のバックアップ		

コンポーネントおよびサブモジュールのインストール

InterScan MSS コンポーネントをインストールすると、その他のサブモジュールも自動的にインストールされます。表 3-2 は、各コンポーネントのサブモジュールを示しています。

表 3-2.　コンポーネントおよびサブモジュールのインストール

メインコンポーネント	インストールされるサブモジュール	サブモジュールの説明
InterScan MSS 管理データベース	管理データベース	すべてのグローバル設定を格納する、主要な InterScan MSS 管理データベース。
	データベースサーバ *	InterScan MSS 管理データベースが実行されるサーバ。
セントラルコントローラ	Apache Tomcat	InterScan MSS 管理コンソール用の Web サーバで、これを使用して設定を実行します。
	Named Server*	IP プロファイラ用の DNS サーバ。
	FoxDNS	IP プロファイラ用の IP アドレスのブロックリストおよび許可リストが含まれており、そのリストを DNS サーバに書き込みます。
	IMSSMGR	InterScan MSS 関連のプロセスを管理するモジュール。

表 3-2.　コンポーネントおよびサブモジュールのインストール (続き)

メイン コンポーネント	インストールされる サブモジュール	サブモジュールの説明
検索サービス	検索サービス	すべてのメールの検索処理を実行します。
	ポリシーサービス	検索サービスに対するルールのリモートストア。ルールがキャッシュされるため、データベース検索が不要になります。
	IMSSMGR	検索サービスプロセスを管理するモジュール。
エンドユーザメール隔離サービス	Apache Tomcat	エンドユーザメール隔離管理コンソール用の Web サーバ。これによって、ユーザはスパムメールとして隔離されたメールメッセージにアクセスできます。
	Apache サービス	複数のエンドユーザメール隔離サービスのインストールを選択した場合は、負荷分散のためにプライマリエンドユーザメール隔離サービスを備えたこのモジュールをインストールします。
	IMSSMGR	エンドユーザメール隔離プロセスを管理するモジュール。
エンドユーザメール隔離データベース	エンドユーザメール隔離データベース	スパムメールとして隔離されたすべてのメールメッセージを含むデータベース。
	データベースサーバ *	エンドユーザメール隔離データベースが実行されるサーバ。
IP プロファイラ	FoxProxy	FoxDNS でブロックリストをチェックして、InterScan MSS がメール要求を拒否するか許可するかを確認する IP フィルタモジュール。
	Foxlib	接続を要求するコンピュータの IP アドレスを取得し、その IP アドレスを Postfix に渡す IP フィルタモジュール。
ERS	メールログパーサ	ERS 関連のメールログを解析するモジュール。

注意： 表内のアスタリスク (*) の付いたサブモジュールは、メインコンポーネントをインストールする際にインストールを選択できるサブコンポーネントです。

InterScan MSS ポート

InterScan MSS で使用されるポートについては、表 3-3 を参照してください。アスタリスク (*) の付いた項目は InterScan MSS 管理コンソールから設定可能です。

表 3-3. InterScan MSS ポート

ポート番号	コンポーネントと役割	設定の保存先
25	Postfix のメールサービスポート。メールサーバは、このポートで待機してメッセージを受信します。ファイアウォールでは、このポートを開放する必要があります。開放されていないと、メールを受信できません。	master.cf
110	InterScan MSS 検索サービス用の一般 POP3 ポート。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	ポリシーサーバ待機ポート。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に対して一致するルールがないかどうか問い合わせます。	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 管理コマンドを処理する Admin Web サーバ (Tomcat) 管理ポート。	{InterScan MSS}/UI/adminUI/conf/server.xml: Server / port
8009	エンドユーザメール隔離コンソール Tomcat AJP ポート。このポートを使用して、複数の Tomcat サーバと Apache HTTP サーバ間の負荷分散を実行します。	{InterScan MSS}/UI/euqUI/conf/server.xml: Server / Service / Connector (protocol=AJP/1.3) / port
8015	Tomcat 管理コマンドを処理する Tomcat 管理ポート。	{InterScan MSS}/UI/euqUI/conf/server.xml: Server/port
8445	InterScan MSS 管理コンソール待機ポート。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 : {InterScan MSS}/UI/adminUI/conf/server.xml: Server / Service / Connector / port

表 3-3.　InterScan MSS ポート (続き)

ポート番号	コンポーネントと役割	設定の保存先
8446	エンドユーザメール隔離サービス待機ポート。	{InterScan MSS}/UI/euqUI/conf/server.xml: Server / Service / Connector / port
8447	負荷分散したエンドユーザメール隔離の待機ポート。	{InterScan MSS}/UI/euqUI/conf/EUQ.conf: Listen / VirtualHost / ServerName
10024	InterScan MSS 検索サービスの再処理ポート。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。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 によって生成された通知メッセージの配信など、内部使用向けの InterScan MSS「パススルー」SMTP ポート。 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。セキュリティを考慮しているため、このポートがバインドされているのは InterScan MSS サーバのループバックインタフェース (127.0.0.1) のみです。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は、このポートを開放する必要がありません。	master.cf

表 3-3. InterScan MSS ポート (続き)

ポート番号	コンポーネントと役割	設定の保存先
15505	InterScan MSS マネージャの待機ポート。InterScan MSS 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の管理コマンド (サービスの起動 / 停止など) を受け入れます。また、隔離 / アーカイブのクエリ結果も、このポートを使用して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送信されます。	管理コンソールのメニューから、[管理] → [InterScan MSS の設定] → [接続] → [コンポーネント] の順にクリックします。
関連するサービスが有効にされている場合、InterScan MSS によって次のポートが使用されます。		
389	LDAP サーバ待機ポート。	InterScan MSS サーバからは設定できません。
5432	PostgreSQL データベース待機ポート。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 待機ポート。Control Manager サーバが Microsoft IIS に依存している場合、Control Manager を使用して InterScan MSS を管理する際に、このポートが必要になります。	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 待機ポート。Control Manager サーバが Microsoft IIS に依存している場合、Control Manager を使用して InterScan MSS を管理する際に、このポートが必要になります。	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 レルム用 KDC ポート。	InterScan MSS サーバからは設定できません。
53	Bind サービス待機ポート。別のポート番号を割り当てないでください。	InterScan MSS サーバからは設定できません。

注意： アスタリスク (*) の付いた項目は InterScan MSS 管理コンソールから設定可能です。

ネットワークトポロジに関する考慮事項

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。

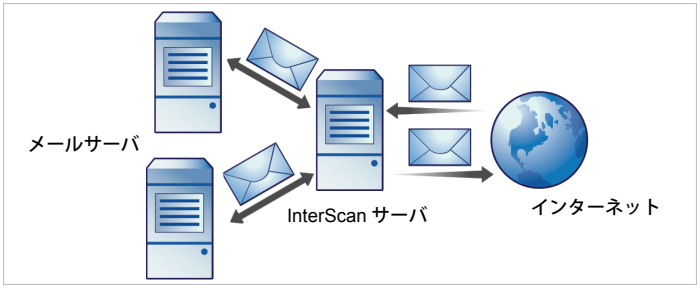
SMTP ゲートウェイの既存のメッセージング環境に InterScan MSS を配置します。この項では、さまざまなネットワークトポロジにおける InterScan MSS の配置について説明し、各シナリオの図と、その他のゲートウェイサービスを設定する一般的な手順について示します。

注意： 次の図は、InterScan MSS の集中インストールを前提としています。InterScan MSS は 1 つの論理単位として機能するため、同じトポロジが分散配置インストールにも適用されます。ただし InterScan MSS では検索サービス間のメッセージ配信が処理されないため、トラフィックを 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分散するには、サードパーティ製のソフトウェアまたはスイッチを使用する必要があります。

ファイアウォールを使用しないインストール

図 3-1. は、ネットワークでファイアウォールを使用しない場合の 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

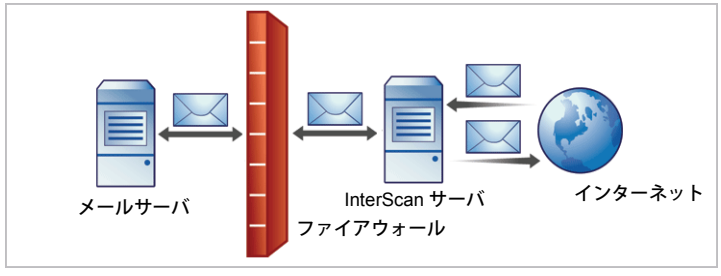


注意： トレンドマイクロでは、ファイアウォールを使用しない InterScan MSS のインストールはお勧めしません。InterScan MSS をホストするサーバをネットワークのエッジに配置すると、サーバがセキュリティ上の脅威にさらされる可能性があります。

ファイアウォールの外側へのインストール

図 3-2. は、InterScan MSS をファイアウォールの外側へインストールする場合のインストールトポロジを示しています。

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

- Postfix は最初に受信メッセージを受け取り、それを InterScan MSS に転送する必要があります。SMTP サーバを参照するように InterScan MSS を設定するか、InterScan MSS サーバからの受信トラフィックが許可されるようにファイアウォールを設定してください。
- ローカルドメインに対するリレーのみが許可されるようにリレー制御を設定します。

送信トラフィック

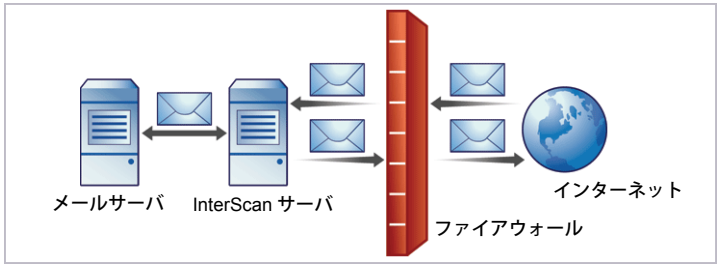
- すべての送信メッセージが InterScan MSS に転送されるように、ファイアウォール (プロキシベース) を設定します。これにより、メールのルーティングは次のようになります。
  - 送信 SMTP メールは Postfix 経由で InterScan MSS サーバに転送される。
  - 受信 SMTP メールは Postfix 経由でのみ InterScan MSS サーバに送信される。
- 内部 SMTP ゲートウェイで、すべてのドメインへの Postfix 経由のリレーが許可されるように InterScan MSS を設定します。

ヒント：　詳細については、管理者ガイドの「SMTP ルーティングの設定」の項を参照してください。

ファイアウォールの内側へのインストール

図 3-3. は、InterScan MSS および Postfix をファイアウォールの内側へ配置する方法を示しています。

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

- 次のようにプロキシベースのファイアウォールを設定します。
  - 送信 SMTP メールが Postfix 経由で InterScan MSS サーバか、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る。
  - 受信 SMTP メールが Postfix 経由で InterScan MSS に転送され、その後ドメイン内の SMTP サーバに転送される。
- 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。
  - InterScan MSS をホストしているサーバのアドレスを参照するように、現在 SMTP ゲートウェイを参照している DNS サーバの MX レコードを変更する。
  - 安全なサブネットを管理するように InterScan MSS またはファイアウォールを設定している場合は、MX レコードが InterScan MSS またはファイアウォールをポイントするように設定する。
- ローカルドメイン宛てのメールが SMTP ゲートウェイまたは内部メールサーバに転送されるように InterScan MSS を設定します。
- ローカルドメインに対するリレーのみが許可されるように、リレーの制約を設定します。

送信トラフィック

- 送信メールが Postfix 経由で InterScan MSS サーバに送信されるように、すべての内部 SMTP ゲートウェイを設定します。

- SMTP ゲートウェイを InterScan MSS と置き換える場合は、送信メールが Postfix 経由で InterScan MSS サーバへ送信されるように内部メールサーバを設定します。
- 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。
- InterScan MSS を使用したすべてのドメインへのリレーが内部 SMTP ゲートウェイで許可されるように InterScan MSS を設定します。

ヒント： 詳細については、管理者ガイドの「SMTP ルーティングの設定」の項を参照してください。

既存の SMTP ゲートウェイ上へのインストール

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

- 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 内へのインストール

InterScan MSS および Postfix を DMZ 内にインストールすることもできます。

受信トラフィック

- 受信および送信 SMTP メールが DMZ 経由でのみ内部メールサーバに送信されるように、プロキシベースのファイアウォールを設定します。
- パケットベースのファイアウォールを設定します。
- ローカルドメイン宛てのメールが SMTP ゲートウェイまたは内部メールサーバに転送されるように Postfix および InterScan MSS を設定します。

送信トラフィック

- ローカル以外のドメイン宛てのすべての送信メールをファイアウォールに転送するか、InterScan MSS を使用して直接配信するように、Postfix を設定します。
- 送信メールが Postfix 経由で InterScan MSS に転送されるように、すべての内部 SMTP ゲートウェイを設定します。
- 内部 SMTP ゲートウェイが、Postfix および InterScan MSS 経由ですべて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、管理者ガイドの「SMTP ルーティングの設定」の項を参照してください。

運用モデルについて

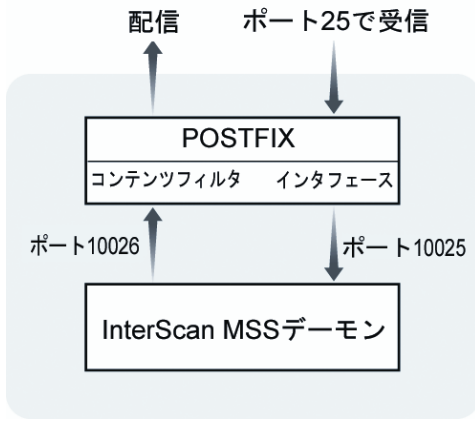
InterScan MSS は、InterScan MSS サーバが既存の MTA およびメールサーバとどのように対話するかに応じて、さまざまな方法で配置できます。運用モデルには、次の 3 つがあります。

- **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
```

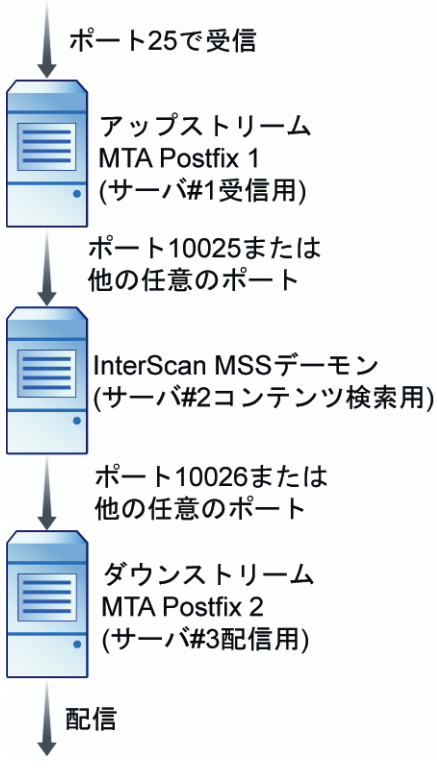
/etc/postfix/master.cf:

```
#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
#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
```

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、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。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。

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=smtp:[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
```

インストールシナリオの理解

InterScan MSS には、1 つのサーバに各コンポーネントの単一のインスタンスをインストールするツール (集中インストール) と、複数のサーバに InterScan MSS コンポーネントをインストールするツール (分散配置インストール) があります。次の情報を参照して、適切なシナリオを選択してください。

集中インストール

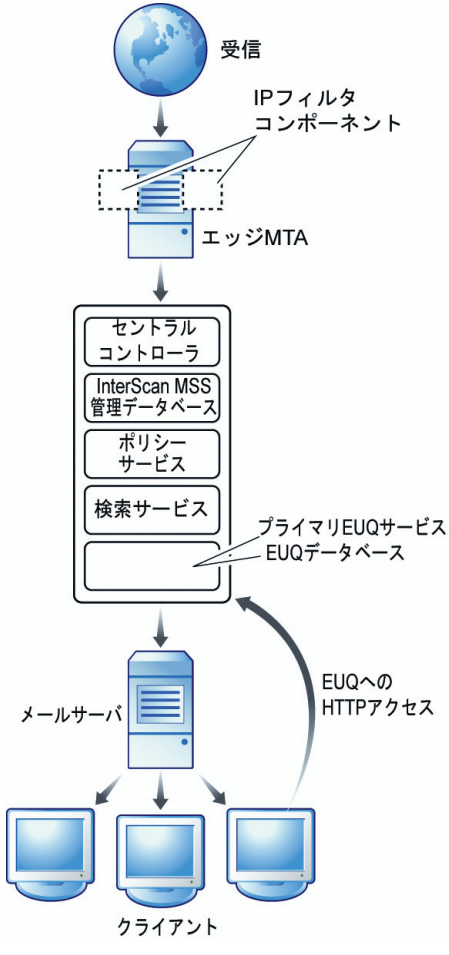
集中インストールでは、集中インストールの要件に合うサーバが必要になります。InterScan MSS の集中インストールでは、平均して、およそ 1,000 ユーザのメッセージトラフィックを処理できます。InterScan MSS を 1 つのサーバにインストールし、後からキャパシティを増やす必要がある場合は、コンポーネントをインストールプログラムから既存の InterScan MSS サーバに追加することで、簡単に検索サービスを追加できます。

1 つのサーバに、次を含むすべての InterScan MSS コンポーネントをインストールできます。

- セントラルコントローラ
- InterScan MSS 管理データベース
- ポリシーサービス
- 検索サービス
- プライマリエンドユーザメール隔離サービスおよびエンドユーザメール隔離データベース

図 3-6. は、InterScan MSS の集中インストールが標準のメッセージングネットワークトポロジにどのように適合するかを示しています。

図 3-6.　単一サーバ配置



集中インストールを実行するには

1. InterScan MSS およびエンドユーザメール隔離をインストールします (84 ページの「InterScan MSS コンポーネントとエンドユーザメール隔離のインストール」を参照)。
2. エッジ MTA サーバに、すべての IP フィルタコンポーネントをインストールします (87 ページの「IP フィルタコンポーネントのインストール」を参照)。

複数の検索サービスのインストール

大規模な組織の場合、単一サーバでは十分なメッセージ処理能力を確保できないことがあります。このような場合は、すべての InterScan MSS コンポーネントを 1 台のサーバにインストールしてから、追加のサーバに検索サービスコンポーネントをインストールできます。検索サービスは、InterScan MSS 管理データベースへのアクセスを共有します。また、隔離されたスパムメールアイテムをエンドユーザメール隔離で管理できるように、エンドユーザメール隔離管理コンソールをインストールすることもできます。

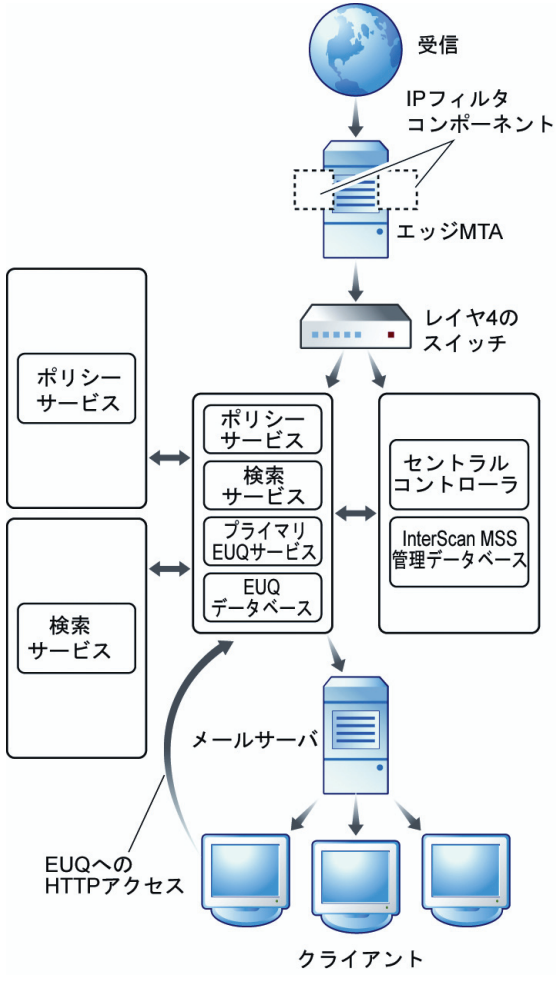
大量のメッセージングトラフィックを処理するために、次のように複数の InterScan MSS 検索サービスをインストールできます。

- 1 台目のサーバに 1 つの検索サービスをインストールします。
- インストールを追加して、2 台目のサーバにもう 1 つの検索サービスをインストールします。パフォーマンスを向上させるには、検索サービスまたはポリシーサービス / 検索サービスのペアをインストールに追加します。

図 3-7. は、2 つの検索サービスが追加された InterScan MSS の集中インストールが標準のメッセージングネットワークトポロジにどのように適合するかを示しています。

レイヤ 4 スイッチは、MTA と検索サービスの間に配置する必要があります。

図 3-7.　複数の検索サービスとポリシーサービスの配置



複数の検索サービスのインストールを実行するには

1. 1 台のコンピュータに、InterScan MSS およびエンドユーザメール隔離をインストールします (84 ページの「InterScan MSS コンポーネントとエンドユーザメール隔離のインストール」を参照)。
2. その他のコンピュータに、必要な検索サービスとポリシーサービスをインストールします。エッジ MTA サーバに、すべての IP フィルタコンポーネントをインストールします (87 ページ

の「IP フィルタコンポーネントのインストール」を参照)。

注意： ポリシーサービスは、必ず検索サービスとともにインストールされます。必要に応じて、任意のポリシーサービスを起動できます。

3. InterScan MSS 管理コンソールを開いて初期設定を実行したら (管理者ガイドの「設定ウィザードでの基本設定の実行」を参照)、[概要] → [システム] 画面に移動します。
4. 有効にする検索サービスまたはポリシーサービスで、[開始] をクリックします。

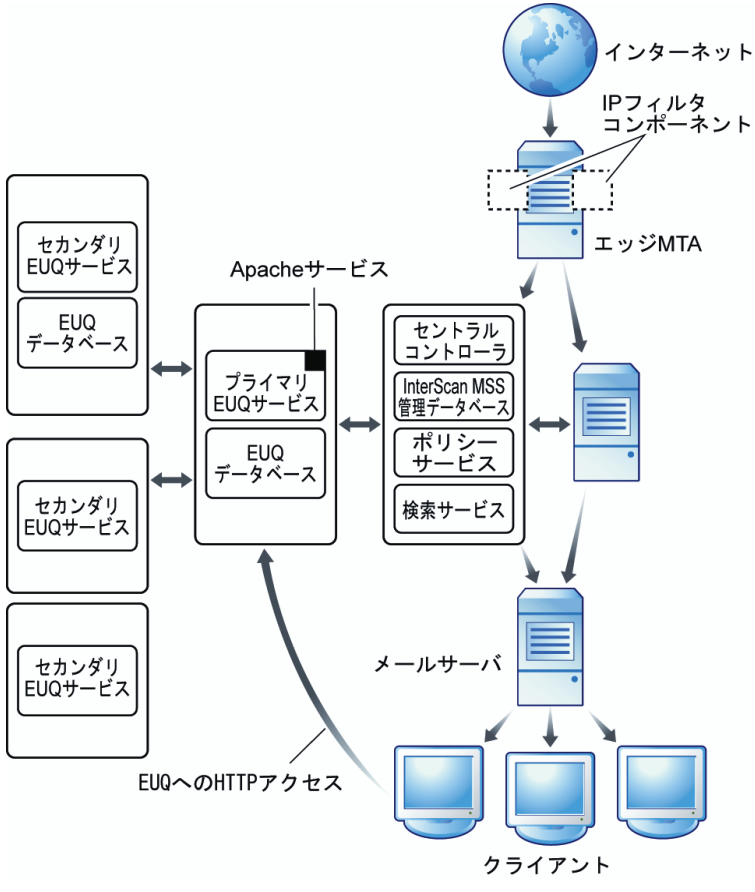
複数のエンドユーザメール隔離サービスのインストール

複数のエンドユーザメール隔離サービスをインストールすると、隔離されたスパムメールにアクセスしやすくなります。

企業が大量のスパムメールを受信し、ユーザがスパムメールにアクセスできるようにする場合は、複数のセカンダリエンドユーザメール隔離サービスをインストールします。

図 3-8. は、個々のプライマリエンドユーザメール隔離サービスと追加のセカンダリエンドユーザメール隔離サービス (負荷分散のための Apache サービスを含む)、および分散エンドユーザメール隔離データベースが追加された InterScan MSS の集中インストールが、標準のメッセージングネットワークトポロジにどのように適合するかを示しています。

図 3-8.　複数のエンドユーザメール隔離サービスの配置



複数のエンドユーザメール隔離サービスのインストールを実行するには

1. 1 台のコンピュータに、InterScan MSS をインストールします (84 ページの「InterScan MSS コンポーネントとエンドユーザメール隔離のインストール」を参照)。

注意： 同じコンピュータにエンドユーザメール隔離サービスをインストールするかどうかを選択できます。別のコンピュータに最初のエンドユーザメール隔離サービスをインストールする場合は、1 台目のコンピュータでエンドユーザメール隔離関連コンポーネントを選択しないでください。最初にインストールされたエンドユーザメール隔離サービスが、プライマリエンドユーザメール隔離サービスになります。負荷分散のた

めに、Apache サービスがプライマリエンドユーザメール隔離サービスとともにインストールされます。

2. プライマリエンドユーザメール隔離サービスと通信できるその他のコンピュータに、追加のエンドユーザメール隔離サービスをインストールします。エンドユーザメール隔離サービス用に、少なくとも 1 つのエンドユーザメール隔離データベースをインストールする必要があります。パフォーマンスを向上させるために、追加のエンドユーザメール隔離データベースをインストールすることもできます。

   注意： エンドユーザメール隔離データベースは、エンドユーザメール隔離サービスを実行しているコンピュータと同じコンピュータにも別のコンピュータにもインストールできます。ただしパフォーマンス上の理由から、InterScan MSS では、複数のエンドユーザメール隔離データベースを同じデータベースサーバへインストールできません。

3. エッジ MTA サーバに、すべての IP フィルタコンポーネントをインストールします (87 ページの「IP フィルタコンポーネントのインストール」を参照)。
4. InterScan MSS 管理コンソールを開いて初期設定を実行したら (管理者ガイドの「設定ウィザードでの基本設定の実行」と「InterScan MSS の設定」の項を参照)、[概要] → [システム] 画面に移動します。
5. 有効にするエンドユーザメール隔離サービスで、[開始] をクリックします。

   注意： 単一の InterScan MSS セントラルコントローラとデータベースでは、最大 8 つのエンドユーザメール隔離サービス / データベースを管理できます。

エンドユーザメール隔離を配置する際のその他の検討事項

社内のエンドユーザが Web ベースのエンドユーザメール隔離にアクセスするには、サーバへの HTTPS アクセスが必要です。また、エンドユーザメール隔離コンポーネントをホストするサーバは、InterScan MSS が隔離したアイテムの情報を格納するために使用する、エンドユーザメール隔離データベースに接続できる必要もあります。

つまり、エンドユーザメール隔離とネットワーク上のエンドユーザコンピュータの間に配置されるファイアウォールは、いずれも内部アドレスからの HTTPS 接続をブロックしないか、HTTPS トラフィックを許可するように設定されている必要があります。

Web ベースのエンドユーザ隔離とデータベースは、InterScan MSS とは別のサーバにインストールすることもできます。この場合は、InterScan MSS と他のサーバとの間に配置するファイアウォールを、これらの間のデータベース接続が許可されるように設定する必要があります。

詳細については、84 ページの「InterScan MSS コンポーネントとエンドユーザメール隔離のインストール」を参照してください。

サーバ間の通信

内部ファイアウォールを使用する場合は、InterScan MSS、エンドユーザメール隔離、およびデータベース間の通信が許可されるようにファイアウォールを設定します。たとえば、1 つのシステムにエンドユーザメール隔離を、もう 1 つのシステムにデータベースをインストールする場合は、2 つのシステム間にあるファイアウォールを、ポート 5432 上の通信が許可されるように設定する必要があります。このポートは、2 つのシステムがデータベースの接続に使用するポートです。

複雑な分散インストール

非常に規模の大きな企業では、分散配置インストールをお勧めします。分散配置インストールには、コンポーネントのインストール要件を満たすサーバが必要になります。このシナリオでは、InterScan MSS とエンドユーザメール隔離コンポーネントを異なるサーバにインストールします。1 台のサーバにデータベースを、もう 1 台のサーバにセントラルコントローラをインストールし、その他のサーバにポリシーサービスと検索サービスの両方をインストールできます。

また、隔離されたスパムメールアイテムをエンドユーザメール隔離で管理できるように、エンドユーザメール隔離管理コンソールの複数のインスタンスをインストールすることもできます。同様に、複数のエンドユーザメール隔離データベースをインストールして、エンドユーザメール隔離のパフォーマンスを向上させることができます。

高い処理能力が要求される環境では、個々のコンピュータに InterScan MSS コンポーネントをそれぞれインストールし、複数の検索サービス、エンドユーザメール隔離サービス、およびデータベースを配置できます。

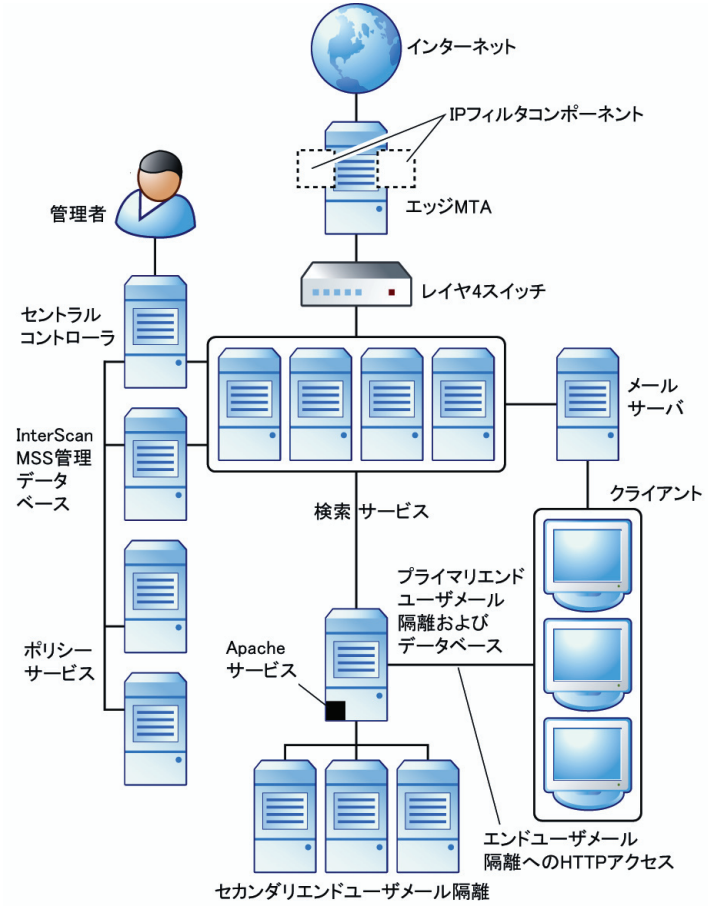
注意： エンドユーザメール隔離データベースを InterScan MSS 管理データベースと混同しないでください。一元化された InterScan MSS の配置には複数のエンドユーザメール隔離データベースをインストールできますが、InterScan MSS 管理データベースは 1 つしかインストールできません。

一元化された InterScan MSS の配置では、最大 8 つのエンドユーザメール隔離サービス / データベースを管理できます。

図 3-9. は、複数の検索サービス、ポリシーサービス、およびエンドユーザメール隔離サービス (負荷分散用 Apache サービスを含む) が追加された一元化された InterScan MSS インストールが、標準のメッセージングネットワークトポロジにどのように適合するかを示しています。

注意： ポリシーサービスは、必ず検索サービスとともにインストールされます。必要に応じて、任意のポリシーサービスを起動できます。

図 3-9.　複雑なアーキテクチャの配置



WAN へのインストール

広域ネットワーク (WAN) に複数のサイトがある場合、InterScan MSS コンポーネントを分散してインストールし、さまざまな方法で配置できます。

ヒント： コンポーネント間で適切な通信を行うためには、各サイトに 1 つ以上のセントラルコントローラコンポーネントと 1 つの InterScan MSS 管理データベースコンポーネントを配置することをお勧めします。そのためには、各サイトで InterScan MSS を新規にインストールし、複数の検索サービスまたはエンドユーザメール隔離サービスをインストールする場合には、インストール後にコンポーネントを追加します。

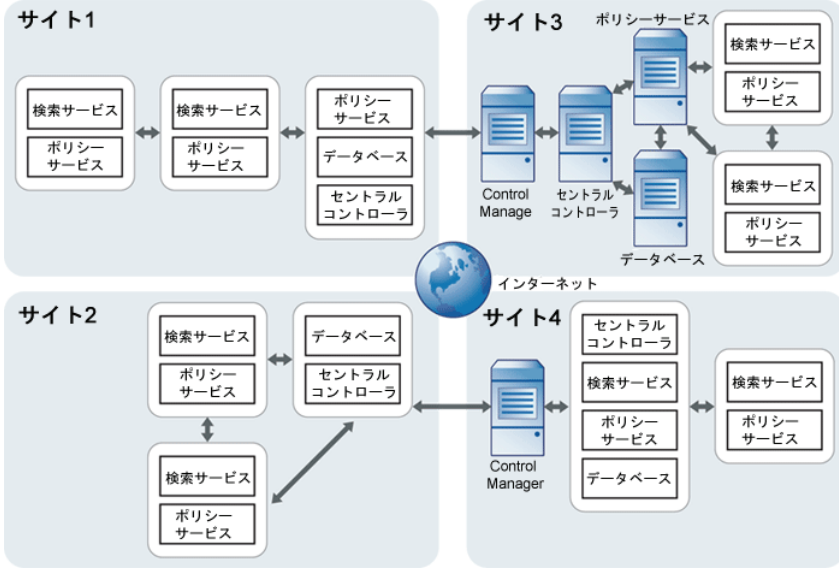
Trend Micro Control Manager

このシナリオには、すべてのサイトを管理する 2 つの Control Manager が含まれます。各 Control Manager サーバは、Control Manager に登録されている InterScan MSS 検索サービス間でデータベース情報を複製できます。

ヒント： セントラルコントローラがインストールされているすべての InterScan MSS サーバを簡単に管理するために、Trend Micro Control Manager サーバをインストールすることをお勧めします。

図 3-10. は、複数サイトの WAN での配置を示しています。

図 3-10. WAN での配置



このシナリオでの各サイトの違いは次のようになります。

- **サイト 1** — セントラルコントローラ、InterScan MSS 管理データベース、およびポリシーサービスを持つ InterScan MSS サーバ + ポリシーサービスが有効な 2 つの InterScan MSS 検索サービス。
- **サイト 2** — セントラルコントローラ、InterScan MSS 管理データベース、およびポリシーサービスを持つ InterScan MSS サーバ + ポリシーサービスが有効な 2 つの InterScan MSS 検索サービス (フォールトトレランス用)。
- **サイト 3** — InterScan MSS セントラルコントローラ + InterScan MSS 管理データベース + 単一のポリシーサービスのみ + ポリシーサービスが有効な 2 つの InterScan MSS 検索サービス (フォールトトレランス用)。
- **サイト 4** — セントラルコントローラ、InterScan MSS 管理データベースを持つ InterScan MSS サーバ + ポリシーサービスが有効な 1 つの InterScan MSS 検索サービス。

WAN のシナリオにおけるフォールトトレランスとフェイルオーバー

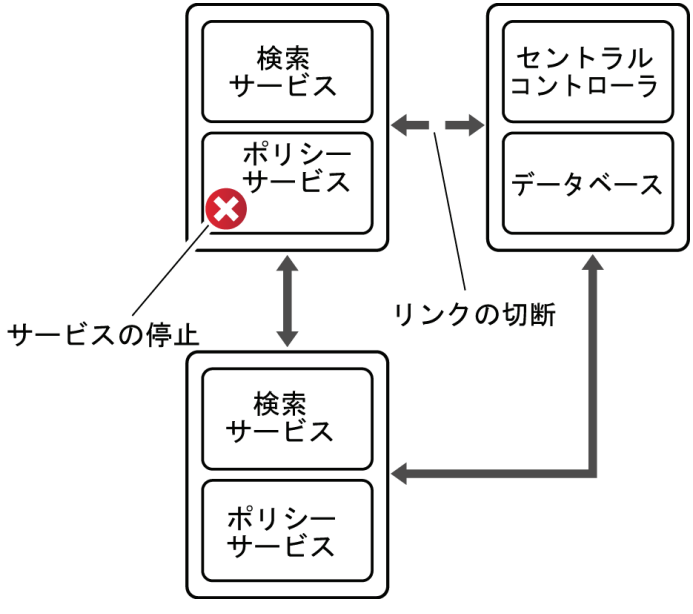
このシナリオでは、4 つのサイトのうち 3 つが、ポリシーサービスがインストールされた複数の検索サービスを使用します。ポリシーサービスは、キャッシュされた InterScan MSS 設定に InterScan MSS 管理データベースからアクセスできます。ポリシーサービスの機能が停止している検索サービスでは、別の有効なポリシーサービスを使用できます。したがって、1 つのポリシーサービスが停

止したり、セントラルデータベースとの通信が中断したりしても、検索サービスは InterScan MSS サーバに接続されている有効なポリシーサービスを使用して動作を続け、メールの処理を継続します。図 3-11 を参照してください。

各サイトには、独自のセントラルコントローラとデータベースサーバがあり、どちらも 2 つの Control Manager サーバにレポートを返します。Control Manager サーバは、Control Manager サーバに直接レポートする InterScan MSS 管理データベースを複製できます。InterScan MSS 管理データベースの 1 つが破損したり動作しなくなっても、複製されたデータベースを復元できます。

注意： Control Manager サーバは、サーバが Control Manager にレポートしていない場合、InterScan MSS 管理データベース情報を複製できません。

図 3-11. フェイルオーバー



IP フィルタ

IP フィルタ (IP プロファイルまたは ERS) を配置する場合は、ネットワークトポロジに関するその他の考慮事項に対処する必要があります。

IP フィルタ機能を持つ InterScan MSS の配置

IP フィルタ (IP プロファイラと ERS) 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。ERS 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。

注意： ネットワークのエッジから InterScan MSS 接続までの区間で、アドレス変更はできません。つまり、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、接続 IP アドレスを変更しないタイプのものであるか、変更しないように設定されている必要があります。

たとえば InterScan MSS がルータからの SMTP 接続を常に受け入れる場合は、IP フィルタは機能しません。これは、このアドレスがどの受信メッセージでも同じになり、IP フィルタソフトウェアが、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。

IP フィルタ機能を持つ InterScan MSS の配置の詳細については、本書の「IP フィルタのインストール」の項および管理者ガイドの「IP フィルタサービス」の項を参照してください。

フェイルオーバーについて

表 3-4 に、InterScan MSS コンポーネントの障害時に発生する問題点、および InterScan MSS の保護機能を維持したまま実行するフェイルオーバーの方法を示します。WAN での配置シナリオにおけるフェイルオーバーの詳細については、72 ページの「WAN のシナリオにおけるフォールトトレランスとフェイルオーバー」を参照してください。

表 3-4. フェイルオーバーシナリオ

障害のあるコンポーネント	予測される結果	推奨フェイルオーバー
検索サービスが起動しない、または切断される	1. InterScan MSS は検索サービスの再起動を試行します。 2. サービスが、指定した時間以内に起動できない場合には、イベント通知が送信されます。	負荷分散とフェイルオーバーのために、複数の検索サービスをインストールします。詳細については、63 ページの「複数の検索サービスのインストール」を参照してください。

表 3-4.　フェイルオーバーシナリオ (続き)

障害のあるコンポーネント	予測される結果	推奨フェイルオーバー
ポリシーサービスが起動しない、または InterScan MSS サーバとの通信に問題が発生する	1. 停止したポリシーサービスを使用している検索サービスは、有効なポリシーサービスがある場合、そのサービスへ切り替えます。 2. InterScan MSS はポリシーサービスの再起動を試行します。 3. サービスが、指定した時間以内に起動または再接続できない場合には、イベント通知が送信されます。	負荷分散とフェイルオーバーのために、複数の検索サービスをインストールします。詳細については、63 ページの「複数の検索サービスのインストール」を参照してください。
InterScan MSS 管理データベースが動作しない	1. InterScan MSS サーバは、動作を続行します。	管理データベースのバックアップを定期的に作成します。 バックアップと復元の詳細については、www.postgresql.org にアクセスしてください。
エンドユーザメール隔離データベースが動作しない	1. エンドユーザメール隔離管理コンソールにエラーメッセージが表示されます。	エンドユーザメール隔離データベースのバックアップを定期的に作成します。 バックアップと復元の詳細については、www.postgresql.org にアクセスしてください。

表 3-4.　フェイルオーバーシナリオ (続き)

障害のあるコンポーネント	予測される結果	推奨フェイルオーバー
LDAP サーバが動作しない	1. エンドユーザメール隔離にログオンする際、エンドユーザメール隔離管理コンソールにエラーメッセージが表示されます。 2. Foxhunter は LDAP 設定を使用しません。 3. LDAP が切断された場合、ポリシールートで LDAP グループが指定されていると、InterScan MSS はキャッシュ済みの LDAP エンティティ (使用可能な場合) をポリシー一致の実行時に使用して、正常に動作を続行します。また、切断に関するイベント通知も、指定されたアドレスへ自動的に送信されます。送信先のアドレスは、[管理] → [通知] → [通知設定] の順に選択して指定します。 **注意：** LDAP の切断の通知はバックエンドで自動的に送信されるので、この通知は管理コンソールで設定することはできません。	次の手順で、セカンダリ LDAP サーバを有効にします。 1. [管理] → [接続] の順に選択します。 2. [LDAP] タブをクリックします。 3. [有効 LDAP2] の横にあるチェックボックスをオンにし、必要な情報を入力します。 **ヒント：** LDAP サーバでフォールトトレランス機能を有効にすることをお勧めします。

第 4 章

InterScan MSS 7.1 のインストールおよびアンインストール

この章では、さまざまなシナリオで Trend Micro InterScan Messaging Security Suite 7.1 (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。

- 78 ページの「システム要件」
- 78 ページの「MTA の準備」
- 84 ページの「InterScan MSS コンポーネントとエンドユーザメール隔離のインストール」
- 87 ページの「IP フィルタコンポーネントのインストール」
- 93 ページの「インストールの確認」
- 94 ページの「アンインストールの実行」

システム要件

注意： 詳細は、弊社の「最新版ダウンロード」サイトにある最新の Readme を参照してください。

MTA の準備

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

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 と共に配布されている 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、www.postfix.org を参照してください。

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

```
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: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
#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
```

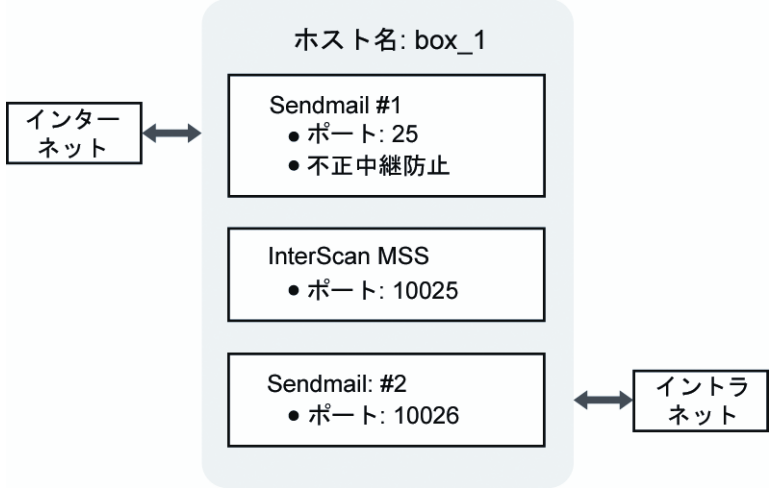
Sendmail の使用

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

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 ポートです)。

Sendmail #1 の設定

Sendmail #1 を設定するには

1. `Sendmail.cf.delivery` という名前の `Sendmail.cf` ファイルをコピーします。
2. `sendmail.cf` で、Msmtp、Mesmtp、Msmtp8、および Mrelay の「A」オプションを「`TCP $h`」から「`TCP localhost.your_domain_name 10025`」に変更します。ここで、10025 は box_1 の任意の使用されていないポートです。
3. `sendmail.cf` で、Msmtp、Mesmtp、Msmtp8、および Mrelay の「F」オプションに「k」フラッグを追加します。

   例として、Msmtp に加えた変更は次のようになります。
   変更前の Msmtp
   P= [IPC] , F=mDFMuX, S=11/31, R=21, E=¥r¥n, L=990,
   T=DNS/RFC822/SMTP,
   A=TCP $h
   変更後の Msmtp

P= [IPC] , F=kmDFMuX, S=11/31, R=21, E=¥r¥n, L=990,
T=DNS/RFC822/SMTP,
A=TCP localhost.your_domain_name 10025
マクロファイルを使用してこれらの変更を加える場合、次を使用します。

```
define ('SMTP_MAILER_FLAGS','k') dnl
define ('SMTP_MAILER_ARGS','TCP [127.0.0.1] 10025') dnl
```

4. `sendmail.cf` で、Mlocal のローカルメールソフトを [IPC] に置き換えます。
5. `sendmail.cf` で、Mlocal の「A」オプションを「`TCP localhost.your_domain_name 10025`」に変更します。
6. `sendmail.cf` で、Mlocal の「F」オプションに「k」フラッグを追加します。

Mlocal に加えた変更は次のようになります。
変更前の Mlocal
P=/usr/lib/mail.local, F=lsDFMAw5:/|@qfSmn9, S=10/30, R=20/40,
T=DNS/RFC822/X-Unix,
A=mail.local -d $u
変更後の Mlocal
P= [IPC] , F=klsDFMAw5:/|@qSmn9, S=10/30, R=20/40,
T=DNS/RFC822/X-Unix,
A=TCP localhost.your_domain_name 10025
マクロファイルに行われる対応する変更 (手順 4 ～ 6) は、次のとおりです。

```
define ('LOCAL_MAILER_PATH',' [IPC] ') dnl
define ('LOCAL_MAILER_FLAGS','k') dnl
define ('LOCAL_MAILER_ARGS','TCP [127.0.0.1] 10025') dnl
```

注意： Mlocal の「F」オプションに「f」フラッグおよび「z」フラッグが含まれていないことを確認してください。

Sendmail #2 の設定

Sendmail #2 を設定するには

1. `sendmail.cf.delivery` ファイルで、待機ポートを 10026 に変更します。

変更前

```
O DaemonPortOptions=Name=MTA-v4, Family=inet
O DaemonPortOptions=Name=MTA-v6, Family=inet6
O DaemonPortOptions=Port=587, Name=MSA, M=E
```

変更後

#O DaemonPortOptions=Name=MTA-v4, Family=inet

#O DaemonPortOptions=Name=MTA-v6, Family=inet6

#O DaemonPortOptions=Port=587, Name=MSA, M=E

O DaemonPortOptions=Port=10026

対応するマクロファイルの変更は、次のとおりです。

DAEMON_OPTIONS ('Port=10026') dnl

2. `sendmail.cf.delivery` で、メールキューを別のディレクトリに変更します。

   変更前

   O QueueDirectory=/var/spool/mqueue

   変更後

   O QueueDirectory=/var/spool/mqueue1

   対応するマクロファイルの変更は、次のとおりです。

   define ('QUEUE_DIR','/var/spool/mqueue1') dnl

3. ディレクトリ `/var/spool/mqueue1` を作成し、`/var/spool/mqueue` の元の所有権とアクセス権と同じものがこのディレクトリに設定されていることを確認します。

4. `sendmail.cf.delivery` で、Mlocal、Msmtp、Mesmtp、Msmtp8、および Mrelay の「F」オプションに「k」フラッグを追加します。

   マクロファイルの変更は、次のとおりです。

   define ('LOCAL_MAILER_FLAGS','k') dnl

   define ('SMTP_MAILER_FLAGS','k') dnl

   define ('ESMTP_MAILER_FLAGS','k') dnl

   define ('SMTP8_MAILER_FLAGS','k') dnl

   define ('RELAY_MAILER_FLAGS','k') dnl

Sendmail サービスの再起動

Sendmail の設定を完了するために、Sendmail サービスを再起動します。

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。

   ```
   /usr/lib/sendmail -bd -q1h
   ```

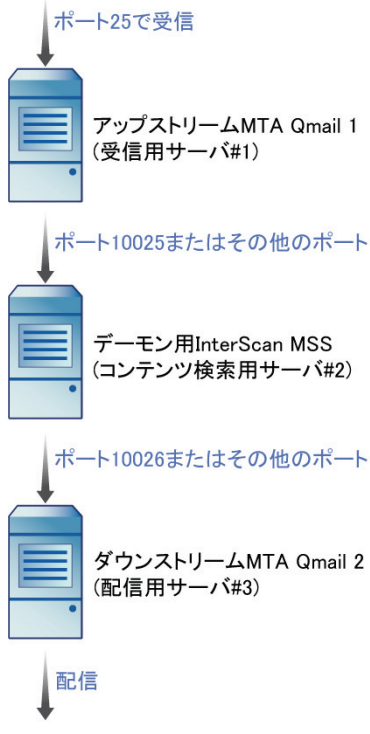
2. 次のコマンドを使用して、2 つ目の Sendmail デーモンを再起動し、InterScan MSS から SMTP トラフィックを受信します。

   ```
   /usr/lib/sendmail -bd -q1h -C/etc/mail/sendmail.cf.delivery
   ```

qmail の使用

次の図は、サンドイッチモデルをベースにした InterScan MSS による qmail の配置を示したものです。

図 4-2.　InterScan MSS による qmail の配置



qmail のインストールおよび設定の詳細については、

http://www.lifewithqmail.org/lwq.html にアクセスしてください。

qmail の設定

qmail を設定するには

qmail がインストールされたコンピュータで、InterScan MSS をホストするサーバの名前または IP アドレスを smtproutes ファイルに追加します。このとき、次のコマンドを使用します。

echo ": [< サーバ名 /IP>:< ポート >] " > /var/qmail/control/smtproutes

InterScan MSS コンポーネントとエンドユーザメール隔離のインストール

ここでは、InterScan MSS コンポーネントとエンドユーザメール隔離をインストールする方法について説明します。

InterScan MSS コンポーネントのインストール時に、管理データベースとエンドユーザメール隔離データベースの両方を InterScan MSS と同じ IP セグメントに配置する必要があります。同じ IP セグメントにないコンポーネントからは、これらのデータベースに接続できません。

この問題を解決するには

1. 次の行を追加して、管理データベースとエンドユーザメール隔離データベースの両方の「/var/imss/pgdata/pg_hba.conf」ファイルを変更します。

   host all all <InterScan MSS コンポーネントの IP アドレス > <InterScan MSS コンポーネントのネットマスク > password

2. 次のコマンドを使用して、データベースを再読み込みします。

   /opt/trend/imss/script/dbctl.sh reload

インストール手順

次に、InterScan MSS およびエンドユーザメール隔離のインストールの実行に必要な主な手順を示します。

1. スーパーユーザとしてログインし、インストールパッケージディレクトリに移動します。
2. 「**./isinst.sh**」と入力します。 [Main Menu] が表示され、各コンポーネントのステータスが示されます。InterScan MSS を初めてインストールする場合は、[Not Installed] と表示されます。

```
      Welcome to the InterScan Messaging Security Suite 7.1 Installation

------------------------------------------------------------------------------

                    -- Main Menu --

             Your Current System Configuration:

             Central Controller   -------- [ Not installed ]
             Scanner Service      -------- [ Not installed ]
             EUQ Service          -------- [ Not installed ]

     1.      Install components.
     2.      Uninstall components.
     3.      Exit.

Enter your choice (default is 1): [   ]
```

3. 「1」と入力してインストールを開始します。
4. 使用許諾契約書を読んで同意します。
5. [InterScan MSS Deployment Config Menu] で、新しい InterScan MSS サーバをインストールするか、またはコンポーネントを既存のインストールに追加するかを指定します。既存の InterScan MSS サーバに検索サービスまたはエンドユーザメール隔離を追加する場合は、これらのコンポーネントのデータベース情報が必要になります。

```
      Welcome to the InterScan Messaging Security Suite 7.1 Installation

------------------------------------------------------------------------------

                    -- IMSS Deployment Config Menu (1/2) --


     1.      Install a new IMSS server on the current computer.
     2.      Append components to an existing IMSS server.
     3.      Back to Main Menu.

             Enter your choice (default is 1): [ ]
```

6. 次のいずれかを実行します。
   - 新しい InterScan MSS サーバのインストールを選択した場合は、新しいデータベースサーバをインストールするか、または既存のデータベースサーバを使用するかを選択し、使用するデータベースサーバの情報を入力します。
   - 新しいデータベースサーバのインストールを選択した場合は、データベースの情報を入力します。

```
      Welcome to the InterScan Messaging Security Suite 7.1 Installation

------------------------------------------------------------------------------

                    -- IMSS Deployment Config Menu (2/2) --


    Specify how to install the database.

    1.      Install a new database server on the current computer.
    2.      Use an existing database server.
    3.      Back to previous menu.

            Enter your choice (default is 1): [ ]
```

[Install Components Menu] 画面が表示され、InterScan MSS コンポーネントのステータスが表示されます。インストーラによってインストールされるコンポーネントの横に [YES] と表示されます。初期設定では、Central Controller (セントラルコントローラ) および Scanner Service (検索サービス) がインストールされるようになっています。この 2 つは、InterScan MSS の使用に欠かせないコンポーネントです。

```
      Welcome to the InterScan Messaging Security Suite 7.1 Installation

------------------------------------------------------------------------------

                    -- Install Components Menu --

    InterScan Messaging Security Suite 7.1 Installation List

    Install Central Controller       -------- [ YES ]
    Install Scanner Service          -------- [ YES ]
    Install EUQ Service              -------- [ NO ]
    Install EUQ Database             -------- [ NO ]

    1.      Modify option for Central Controller.
    2.      Modify option for Scanner Service.
    3.      Modify option for EUQ Service.
    4.      Modify option for EUQ Database.
    5.      Modify option for Install path (current: /opt/trend).
    6.      Start installation.
    7.      Back to Main Menu.

Enter a choice (default is 6): [   ]
```

7. インストールするコンポーネントの選択を変更するには、コンポーネントに対応する番号を入力し、インストールするかどうかの質問に対して、「はい」の場合は「Y」または「y」、「いいえ」の場合は「N」または「n」を入力します。

   インストールディレクトリを変更することもできます。初期設定のインストールディレクトリは、`/opt/trend` です。

エンドユーザメール隔離サービスが存在しない場合、プライマリサービスがインストールされます。エンドユーザメール隔離サービスが存在する場合、エンドユーザメール隔離サービスはインストールされません。
エンドユーザメール隔離データベースをインストールする場合、新しいデータベースサーバをインストールするか、既存のデータベースサーバを使用して、データベースサーバの情報を入力します。

8. 「6」と入力して、続行します。

   コンピュータ上の使用可能な空きディスク領域、メモリ、スワップ領域、および BIND サーバがチェックされます。コンピュータが最小要件を満たしていない場合は、ここでインストールをキャンセルできます。
   インストールを続行する場合は、Postfix サーバに必要な設定事項が表示されます。これらの設定の概要については、78 ページの「Postfix の準備」を参照してください。

   注意： IP プロファイラでは、BIND サーバ 9.x 以上が必要です。既存の DNS サーバがこの要件を満たしていることを確認してください。満たしていない場合は、旧バージョンの BIND をアンインストールし、InterScan MSS インストールパッケージに付属の BIND 9.5.0 をインストールします。

9. <Enter> キーを押して、続行します。コンピュータ上の DNS サーバがアクティブかどうかに関する情報が表示されます。後でインストール可能な IP プロファイラを使用するには、DNS サーバがアクティブで正常に動作している必要があります。IP プロファイラのインストール手順については、87 ページの「IP フィルタコンポーネントのインストール」を参照してください。

   注意： DNS の設定を確認するには、次のコマンドを使用します。
   nslookup www.antivirus.com

   有効な IP アドレスが返されます。

10. <Enter> キーを押して、選択したコンポーネントのインストールを開始します。

IP フィルタコンポーネントのインストール

トレンドマイクロの IP フィルタは、次の 2 つのコンポーネントで構成されています。

- **IP プロファイラ** — InterScan MSS がスパムメール、ウイルス脅威、ディレクトリハーベスト攻撃、またはバウンスメール攻撃を検出したときに、メールメッセージに対する処理を実行します。
- Email Reputation Services (ERS) — 既知のスパムメール送信者をネットワーク (IP) レベルでブロックします。

Email Reputation Services と IP プロファイラのインストール

トレンドマイクロの Email Reputation Services (以下、ERS) は、変更された Postfix インストール上で動作します。ERS のインストールスクリプトによって Postfix 設定ファイルが変更され、IP フィルタをレポートできるようにログパーサがインストールされます。インストール時には、ERS のアクティベーションコードおよび InterScan MSS 管理データベースに関する情報の入力も求められます。Email Reputation Services と IP プロファイラをインストールする前に、管理データベースをインストールしてください。

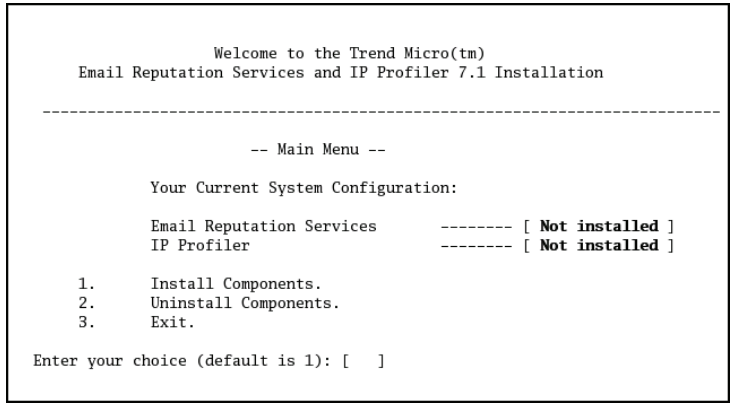
ERS のインストール先サーバには、Postfix のインスタンスがすでにインストールされている必要があります。また、ERS のインストール先サーバから InterScan MSS 管理データベースと、メッセージングを処理するサーバ (ほとんどの場合 InterScan MSS サーバ) に接続できる必要があります。トレンドマイクロでは、ERS と IP プロファイラをゲートウェイサーバまたはエッジサーバで実行することをお勧めします。

注意： ERS はインストール時にアクティベートする必要があります。後で管理コンソールからアクティベートすることはできません。

トレンドマイクロのスパムメール対策 (コンテンツ検索) のアクティベーションコードを持っている場合は、そのアクティベーションコードを使用して Email Reputation Services をアクティベートできます。

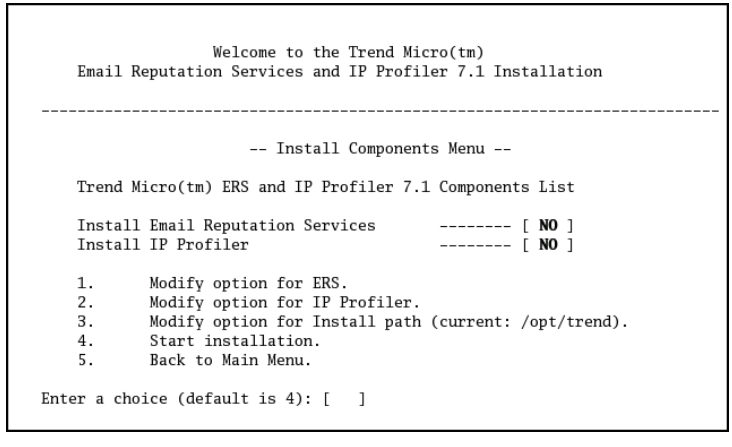
IP プロファイラおよび ERS をインストールするには

1. スーパーユーザとしてログインし、インストールパッケージディレクトリに移動します。
2. 「./ipfilterinst.sh」と入力します。 [Main Menu] が表示され、IP プロファイラおよび ERS のステータスが示されます。これらの製品を初めてインストールする場合は、[Not Installed] と表示されます。



3. 「1」と入力してインストールを開始します。
4. 使用許諾契約書を読んで同意します。

   [Installation List] 画面が表示され、これら 2 つの InterScan MSS コンポーネントのステータスが表示されます。インストーラによってインストールされるコンポーネントの横に [YES] と表示されます。初期設定では、IP プロファイラと ERS はインストールされないようになっています。



5. IP プロファイラまたは ERS のインストールを選択します。

   ERS をインストールするには

   a. 「1」と入力します。 [ERS Configuration] 画面が表示されます。
   b. ERS を現在のコンピュータにインストールするかどうかを指定します。

c. ERS のアクティベーションコードを入力します。Postfix サーバに加えられる変更についての情報が表示されます。

d. 変更を受け入れます。

e. 管理データベースを使用して ERS の設定を登録するために、インストーラでは、次の InterScan MSS の詳細を入力するようにプロンプトが表示されます。

   i. IP アドレス

   ii. データベース名

   iii. データベースのユーザ名

   iv. データベースのユーザパスワード

f. メールログへのパスを入力します。

インストールメニューが再表示され、[Install ERS] の横に [YES] と表示されます。

IP プロファイラをインストールするには

a. 「2」と入力します。 [IP Profiler Configuration] 画面が表示されます。

b. IP プロファイラを現在のコンピュータにインストールするかどうかを指定します。

c. IP プロファイラのポート番号を入力します (初期設定は 25)。

ポート 25 がすでに使用されている場合は、ポートに関する情報が表示されます。必要に応じてポート番号を変更するか、インストールの完了後に Postfix 待機ポートを 2500 に変更します。

d. <Enter> キーを押して、続行します。

e. セントラルコントローラをインストールした IP アドレスを入力します。これには、InterScan MSS の foxdns が含まれます。IP プロファイラは foxdns と通信する必要があります。

f. メールサーバのドメイン名を入力します。

g. <Enter> キーを押します。

h. 管理データベースを使用して IP プロファイラを登録するために、次の InterScan MSS Postgres データベースの詳細を入力するようにプロンプトが表示されます。

   i. IP アドレス

   ii. データベース名

   iii. データベースのユーザ名

   iv. データベースのユーザパスワード

要求された情報を入力します。インストールメニューが再表示され、[Install IP Profiler] の横に [YES] と表示されます。

6. インストールディレクトリを変更するには、「3」と入力してから、新しいディレクトリパスを入力します。初期設定のインストールディレクトリは、`opt/trend` です。
7. 「4」と入力してインストールを開始します。
8. <Enter> キーを押して、選択したコンポーネントのインストールを開始します。

InterScan MSS の Sendmail および qmail との統合

InterScan MSS では、Postfix の代わりに他の MTA を使用できます。ここでは、FoxProxy および ERS をサポートするように Sendmail および qmail を設定する手順について説明します。

FoxLib の Sendmail との統合

IP プロファイラを Sendmail MTA と共に使用する場合は、次の手順を実行して、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。

1. `sendmail.cf` ファイルで、待機ポートを 2500 に変更して、Sendmail を再起動します。

   変更前
   O DaemonPortOptions=Name=MTA-v4, Family=inet
   O DaemonPortOptions=Name=MTA-v6, Family=inet6
   O DaemonPortOptions=Port=587, Name=MSA, M=E
   変更後
   #O DaemonPortOptions=Name=MTA-v4, Family=inet
   #O DaemonPortOptions=Name=MTA-v6, Family=inet6
   #O DaemonPortOptions=Port=587, Name=MSA, M=E
   `O DaemonPortOptions=Port=2500`

2. Sendmail に関する情報を収集します。
   a. `which` コマンドを使用して、Sendmail プログラムファイルを検索します。

      # which sendmail
      /usr/sbin/sendmail

   b. `ls` コマンドを使用して、Sendmail で使用するユーザとグループを特定します。

      # ls – al /usr/sbin/sendmail
      -rwxr-sr-x 1 root root 732356 Sep 1 2004 /usr/sbin/sendmail
      (ユーザおよびグループ共に root)

c. Sendmail により使用されるユーザとグループのユーザ ID およびグループ ID を検索します。

```
# fgrep root /etc/passwd
root:x:0:0:root:/root:/bin/bash
# fgrep root /etc/group
root:x:0:root
```

(ユーザ ID およびグループ ID 共に 0)

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

a. TM_FOX_UID パラメータをユーザ ID に設定します。

```
TM_FOX_UID=0
```

b. TM_FOX_GID パラメータをグループ ID に設定します。

TM_FOX_GID=0

c. 「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/ipprofiler/config ディレクトリの foxproxy.ini 設定ファイルを変更します。

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

5. sendmail ではなく foxlibd スクリプトを使用して Sendmail を起動します。

/opt/trend/ipprofiler/script/foxlibd start/stop

6. FoxProxy を再起動します。

/opt/trend/ipprofiler/script/foxproxyd start/stop

FoxLib の qmail との統合

IP プロファイラを qmail MTA と共に使用する場合は、次の手順を実行して、qmail 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。

1. qmail 起動スクリプトを変更します。

a. qmail を起動するためのデーモンツールがインストールされている場合、smtpd 起動スクリプトは /service/qmail-smtpd/run にあります。

b. 実行ファイルを変更して、ファイル冒頭の #!/bin/sh が含まれる行の後ろに次の行を追加します。

```
TM_FOX_PROXY_LIST=/opt/trend/ipprofiler/config/foxproxy.list
LD_PRELOAD=/lib/libTmFoxSocketLib.so
TM_FOX_PROXY_CONNECT_PORT=2500
export TM_FOX_PROXY_CONNECT_PORT
export TM_FOX_PROXY_LIST
export LD_PRELOAD
```

2. qmail ユーザおよびグループを取得して、適切な `.so` ファイルをコピーします。
   a. 次のコマンドを実行して、ユーザおよびグループを確認します。

      ```
      #id qmaild
      uid=101  (qmaild) gid=100  (nofiles)
      ```

      SMTP ユーザが qmaild、グループが nofiles です。
   b. `.so` ファイルを適切なパスにコピーして、属性を変更し、次のコマンドを実行します。

      ```
      #cp /opt/trend/ipprofiler/lib/libTmFoxSocketLib.so /lib/libTmFoxSocketLib.so
      #chown qmaild /lib/libTmFoxSocketLib.so
      #chgrp nofiles /lib/libTmFoxSocketLib.so
      #chmod 550 /lib/libTmFoxSocketLib.so
      ```

3. 次のように、`/opt/trend/ipprofiler/config` ディレクトリの `foxproxy.ini` 設定ファイルを変更します。

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

4. 次のスクリプトを実行して foxproxyd を再起動します。

   ```
   #/opt/trend/ipprofiler/script/foxproxyd restart
   ```

5. 次のコマンドを入力して、qmail を起動します。

   ```
   #/command/svscanboot </dev/null >/var/log/svscan 2>&1 &
   ```

   または、qmail がすでに起動していて、システムのスタートアップスクリプトに追加されている場合は、システムを再起動します。

インストールの確認

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。

アンインストールの実行

ここでは、InterScan MSS コンポーネントを削除する方法について説明します。

InterScan MSS 7.1 をアンインストールした後、生成されたレポートデータが `/opt/trend/installlog/data` にバックアップされます。これは、InterScan MSS が `/opt/trend` にインストールされている場合にのみ実行されます。

InterScan MSS コンポーネントのアンインストール

セントラルコントローラ、検索サービス、およびエンドユーザメール隔離コンポーネントを個別にまたは同時にアンインストールできます。

1. スーパーユーザとしてログインし、インストールパッケージディレクトリに移動します。
2. 「**`./isinst.sh`**」と入力します。 [Main Menu] が表示され、各コンポーネントのステータスが示されます。これらの製品をすでにインストールしている場合は、[Installed] と表示されます。

```
        Welcome to the InterScan Messaging Security Suite 7.1 Installation

   ------------------------------------------------------------------------------

                       -- Main Menu --

                Your Current System Configuration:

                Central Controller    -------- [ Not installed ]
                Scanner Service       -------- [ Not installed ]
                EUQ Service           -------- [ Not installed ]

       1.       Install components.
       2.       Uninstall components.
       3.       Exit.

  Enter your choice (default is 1): [   ]
```

3. 「2」と入力します。

   アンインストールメニューが表示され、削除できるコンポーネントが示されます。初期設定では、各コンポーネントのアンインストールステータスは [NO] に設定されており、削除されないことを意味します。コンポーネントがインストールされていない場合は、[Not installed] と表示されます。
4. コンポーネントを削除するには、削除するコンポーネントに対応する番号を入力し、「Y」または「y」と入力して、アンインストールメニューのアンインストールステータスを [YES] に変更します。
5. アンインストールするコンポーネントのアンインストールステータスを [YES] に変更したら、「4」と入力します。

   コンポーネントがアンインストールされます。

注意： アンインストール中に、PostgreSQL プロセスを停止するかどうかを尋ねるメッセージが表示されます。他のアプリケーションで PostgreSQL プロセスを使用している場合は、停止しないことを選択できます。

Email Reputation Services と IP プロファイラのアンインストール

ERS および IP プロファイラをアンインストールするには

1. スーパーユーザとしてログインし、インストールパッケージディレクトリに移動します。
2. 「./ipfilterinst.sh」と入力します。[Main Menu] が表示され、IP プロファイラおよび ERS のステータスが示されます。これらの製品をすでにインストールしている場合は、[Installed] と表示されます。
3. 「2」と入力します。

   アンインストールメニューが表示され、削除できるコンポーネントが示されます。初期設定では、各コンポーネントのアンインストールステータスは [NO] に設定されており、削除されないことを意味します。コンポーネントがインストールされていない場合は、[Not installed] と表示されます。
4. コンポーネントを削除するには、削除するコンポーネントに対応する番号を入力し、「Y」または「y」と入力して、アンインストールメニューのアンインストールステータスを [YES] に変更します。
5. アンインストールするコンポーネントのアンインストールステータスを [YES] に変更したら、「3」と入力します。

   コンポーネントがアンインストールされます。

手動アンインストールの実行

InterScan MSS の手動アンインストール

自動化されたアンインストールで問題が発生した場合にのみ、InterScan MSS を手動でアンインストールします。

InterScan MSS を手動でアンインストールするには

1. 次のコマンドを使用して、InterScan MSS 関連のサービスをすべて停止します。

   $Home_IMSS/script/imssstop.sh

2. 次のコマンドを入力して、InterScan MSS パッケージを削除します。

   rpm -e imsscctrl-7.1-1
   rpm -e imss-7.1-1
   rpm -e imsseuq-7.1-1
   一部のコンポーネントがインストールされていない場合、このアンインストールのコマンドは機能しません。

3. /opt/trend/imss などの $Home_IMSS を削除します。

4. デーモン起動 / 停止スクリプトを削除します。

   - システムの再起動時に起動スクリプトが自動的に実行されます。/etc/rc2.d、/etc/rc3.d、および /etc/rc5.d から、次のスクリプトを削除します。

     S99IMSS、S98dbctl、S99CMAGENT、S99POLICY、S99bindctl、S99IMSSUI、99FOXDNS、S99SCHEDULED、S99MONITOR、S99MANAGER

   - 停止スクリプトにより、システムのシャットダウン時に自動的にサービスが停止されます。/etc/rc0.d および /etc/rc6.d から、次のスクリプトを削除します。

     K98dbctl、K97CMAGENT、K97IMSS、K97POLICY、K97EUQ、K97bindctl、K97IMSSUI、K97FOXDNS、K97SCHEDULED、K96MONITOR、K96MANAGER、K99IMSSSTOP

データベースの手動アンインストール

自動化されたアンインストールで問題が発生した場合にのみ、データベースを手動でアンインストールします。

データベースを手動でアンインストールするには

1. 次のコマンドを使用して、Postmaster のサービスを停止します。

   $Home_IMSS/script/dbctl.sh stop
   または
   次のコマンドを使用して、強制的にサービスを停止します。
   kill -9 pid

2. $Home_IMSS/PostgreSQL を削除します。

3. /var/imss を削除します。

4. 手順 1 で強制的にサービスを停止するように選択した場合、/tmp/.sPGSQL.5432 および /tmp/.s.PGSQL.5432.lock を削除します。

Postfix の手動アンインストール

Postfix を手動でアンインストールするには

1. コマンド `postfix stop` を使用して、Postfix 関連のサービスを停止します。
2. `/etc/postfix` を削除します。
3. `/usr/libexec/postfix` を削除します。
4. 次のような Postfix 関連のファイルを `/usr/sbin/post*` ディレクトリから削除します。
   - postalias
   - postcat
   - postconf
   - postdrop
   - postfix
   - postkick
   - postlock
   - postlog
   - postmap
   - postqueue
   - postsuper
5. `/var/spool/postfix` を削除します (オプション)。

IP プロファイラの手動アンインストール

IP プロファイラを手動でアンインストールするには

1. 次のコマンドを使用して、IP プロファイラ関連のサービスを停止します。

   /opt/trend/ipprofiler/script/foxproxyd stop
2. 次のコマンドを使用して、IP プロファイラパッケージおよび ERS パッケージを削除します。

   rpm -e ipprofiler-7.1-1
   rpm -e nrs-7.1-1
3. `/etc/postfix/ imss_rbl_reply` を削除します。
4. `main.cf` で設定を復元します。
5. `/etc/syslog.conf` のメールデバッグの設定を復元します。

第 5 章

以前のバージョンからのアップグレード

本章では、Trend Micro InterScan Messaging Security Suite 7.1 (以下、InterScan MSS) の以前のバージョンからのアップグレードの手順を説明します。

この章の内容は次のとおりです。

- 100 ページの「体験版から移行する」
- 101 ページの「InterScan MSS 7.0 から InterScan MSS 7.1 へアップグレードする」
- 106 ページの「InterScan MSS 7.0 から InterScan MSS 7.1 へ移行する」
- 108 ページの「サポートされているサービスのアクティベーション」
- 109 ページの「アップグレードをロールバックする」

体験版から移行する

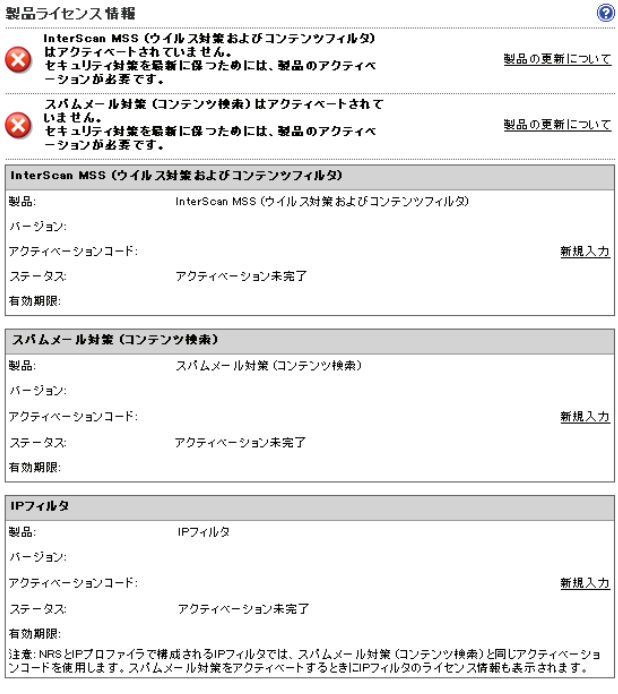
体験版アクティベーションコードを入力して InterScan MSS をアクティベートすると、製品のすべての機能を試すことができる体験版の使用期間が開始します。体験版の使用期間は、入力したアクティベーションコードの種類に応じて異なります。

体験版の有効期限が切れる 14 日前に、管理コンソールでは、有効期限が近づいていることを知らせる警告メッセージが表示されます。

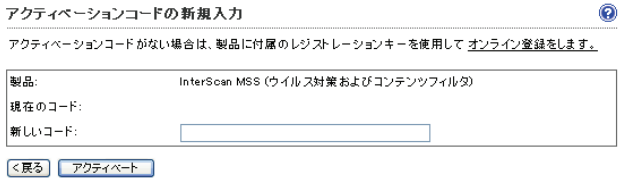
InterScan MSS を継続して使用するには、製品版を購入してください。その際に、新しいアクティベーションコードが提供されます。

体験版から移行するには

1. メニューから [管理] → [製品ライセンス] を選択します。



2. [InterScan MSS (ウイルス対策およびコンテンツフィルタ)] セクションまたは [スパムメール対策 (コンテンツ検索)] 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。



3. 表示される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： InterScan MSS 製品版を購入されると、新しいアクティベーションコードがメールで送信されます。

4. [アクティベート] をクリックします。

InterScan MSS 7.0 から InterScan MSS 7.1 へアップグレードする

サポート対象のプラットフォームにバージョン 7.0 の InterScan MSS が存在する場合、InterScan MSS のインストールプログラムは、これを自動的にアップグレードします。インストール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 設定のバックアップを作成します。
- InterScan MSS 7.1 をインストールします。
- 既存の設定を移行します。

InterScan MSS 7.0 から InterScan MSS 7.1 へのアップグレードは、InterScan MSS の配置によって異なります。単一サーバ配置と分散配置では、異なるアップグレード手順が必要です。

InterScan MSS 7.0 の設定を移行する

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。

InterScan MSS 7.0 の設定をバックアップする

InterScan MSS 7.1 インストーラでは、インストール時に全体のバイナリバックアップが作成されます。ただし、ユーザは、InterScan MSS 7.0 管理データベースおよび InterScan MSS 7.0 パッケージ情報の全体のバックアップを手動で作成する必要があります。

InterScan MSS 7.0 の設定をバックアップするには

1. 約 1 分間、InterScan MSS 7.0 のメールトラフィックを停止します。
2. 次のスクリプトを実行し、InterScan MSS 7.0 のすべてのプロセスを停止します。

   [停止方法]

   ```
   /opt/trend/imss/script/S99ADMINUI stop
   /opt/trend/imss /script/S99CMAGENT stop
   /opt/trend/imss /script/S99EUQ stop
   /opt/trend/imss /script/S99FOXDNS stop
   /opt/trend/ipprofiler/script/foxproxyd stop
   ```

3. 次のコマンドを使用して、Postfix を停止します。

   ```
   postfix stop
   ```

4. InterScan MSS 7.0 管理データベース (現在の検索サービスに InterScan MSS セントラルコントローラがインストールされている場合は必要) およびエンドユーザメール隔離データベース (現在の検索サービスに InterScan MSS エンドユーザメール隔離データベースがインストールされている場合は必要) のバックアップを作成します。
   a. InterScan MSS 7.0 にバンドルされている PostgreSQL を使用して、InterScan MSS 7.0 管理データベースまたはエンドユーザメール隔離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。
      i. 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
      ```

      ii. 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
      ```

   b. 独自の PostgreSQL サーバを使用して InterScan MSS エンドユーザメール隔離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。詳細な手順については、データベース管理システムのドキュメントを参照してください。
5. 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
   ```

6. 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
   ```

InterScan MSS 7.0 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には InterScan MSS 7.0 SP1 が必要です。

単一サーバ配置の InterScan MSS 7.0 をアップグレードするには

1. インストールの前に、InterScan MSS 7.0 のデータをバックアップします。詳細については、101 ページの「InterScan MSS 7.0 の設定をバックアップする」を参照してください。
2. スーパーユーザとしてログインし、インストールパッケージディレクトリに移動します。

   注意： 検索サービスごとに、最初に InterScan MSS コンポーネントをアップグレードして、次に IP プロファイラをアップグレードします。この順序を変更することはできません。

3. 次のコマンドを使用して、インストールを開始します。

   ```
   ./imss/isinst.sh
   ```

   [Main Menu] が表示され、InterScan MSS インストーラにより、InterScan MSS 7.0 が検出されたことが報告されます。
4. 「1」と入力して、バージョン 7.1 への設定の移行とアップグレードを選択します。これにより、現在の InterScan MSS 7.0 サーバが 7.1 にアップグレードされ、既存の設定が保持されます。

   [Install Components Menu] 画面が表示され、InterScan MSS コンポーネントのステータスが表示されます。インストーラによってインストールされるコンポーネントの横に [YES] と表示されます。
5. 「1」と入力してインストールを開始します。コンピュータ上の使用可能な空きディスク領域、メモリ、およびスワップ領域がチェックされます。コンピュータが最小要件を満たしていない場合は、ここでインストールをキャンセルできます。

   警告： これが、現在の InterScan MSS 7.0 インストールに損害を与えずにアップグレードプロセスを停止できる最後の機会です。アップグレードの準備ができていない場合は、<Ctrl>+<C> キーを押してインストールを停止します。準備ができている場合は <Enter> キーを押して続行します。

   インストーラにより、次の項目について制約の検証が実行されます。

   - InterScan MSS 7.0 管理データベースの接続確認。

- InterScan MSS 7.0 コンポーネントのステータス確認。インストーラにより、すべての検索サービス上のプロセス imssmgr のステータスがチェックされ、検索サービスがすべてシャットダウンされていることが確認されます。
- InterScan MSS 7.0 の分散アップグレードシーケンスの確認 (分散インストールのアップグレードの場合にのみ実行)。

制約の検証後に、インストーラにより次の項目が実行されます。

- 管理データベースのバックアップ (セントラルコントローラ上のみ)
- InterScan MSS バイナリパッケージの作成
- InterScan MSS 7.1 コンポーネントパッケージのインストール
- InterScan MSS 7.1 へのすべての設定の移行

注意： ハードウェアと配置によっては、このプロセスに最大 1 時間を要する場合があります。

6. コンポーネントのアップグレードが完了したら、次のコマンドを使用して IP プロファイラをアップグレードします。

```
./imss/ipfilterinst.sh
```

注意： IP プロファイラは、起動後に自動的にアップグレードされます。

InterScan MSS 7.0 の分散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には InterScan MSS 7.0 SP1 が必要です。

分散配置の InterScan MSS 7.0 をアップグレードするには

1. インストールの前に、InterScan MSS 7.0 のデータをバックアップします。詳細については、101 ページの「InterScan MSS 7.0 の設定をバックアップする」を参照してください。
2. グループ内のすべてのメールトラフィックを停止して、約 1 分間待ちます。
3. グループ内のすべての検索サービスのすべてのコンポーネントを停止します。
   a. 検索サービスごとに、次のコマンドを入力します。

```
/etc/rc.d/init.d/S99IMSSSTOP stop
```

b. InterScan MSS 7.0 にバンドルされている PostgreSQL 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 PostgreSQL を再起動します (S99IMSSSTOP コマンドによって停止されています)。

```
/etc/rc.d/init.d/S98dbctl start
```

4. スーパーユーザとしてログインし、インストールパッケージディレクトリに移動します。

注意： 検索サービスごとに、最初に InterScan MSS コンポーネントをアップグレードして、次に IP プロファイラをアップグレードします。この順序を変更することはできません。

---

5. 次のコマンドを使用して、インストールを開始します。

```
./imss/isinst.sh
```

[Main Menu] が表示され、InterScan MSS インストーラにより、InterScan MSS 7.0 が検出されたことが報告されます。

6. 「1」と入力して、バージョン 7.1 への設定の移行とアップグレードを選択します。これにより、現在の InterScan MSS 7.0 サーバが 7.1 にアップグレードされ、既存の設定が保持されます。

[Install Components Menu] 画面が表示され、InterScan MSS コンポーネントのステータスが表示されます。インストーラによってインストールされるコンポーネントの横に [YES] と表示されます。

7. 「1」と入力してインストールを開始します。コンピュータ上の使用可能な空きディスク領域、メモリ、およびスワップ領域がチェックされます。コンピュータが最小要件を満たしていない場合は、ここでインストールをキャンセルできます。

警告： これが、現在の InterScan MSS 7.0 インストールに損害を与えずにアップグレードプロセスを停止できる最後の機会です。アップグレードの準備ができていない場合は、<Ctrl>+<C> キーを押してインストールを停止します。準備ができている場合は <Enter> キーを押して続行します。

インストーラにより、次の項目について制約の検証が実行されます。

- InterScan MSS 7.0 管理データベースの接続確認。
- InterScan MSS 7.0 コンポーネントのステータス確認。インストーラにより、すべての検索サービス上のプロセス imssmgr のステータスがチェックされ、検索サービスがすべてシャットダウンされていることが確認されます。

- InterScan MSS 7.0 の分散アップグレードシーケンスの確認 (分散インストールのアップグレードの場合にのみ実行)。

制約の検証後に、インストーラにより次の項目が実行されます。

- 管理データベースのバックアップ (セントラルコントローラ上のみ)
- InterScan MSS バイナリパッケージの作成
- InterScan MSS 7.1 コンポーネントパッケージのインストール
- InterScan MSS 7.1 へのすべての設定の移行

注意： ハードウェアと配置によっては、このプロセスに最大 1 時間を要する場合があります。

8. コンポーネントのアップグレードが完了したら、次のコマンドを使用して IP プロファイラをアップグレードします。

```
./imss/ipfilterinst.sh
```

注意： IP プロファイラは、起動後に自動的にアップグレードされます。

9. 手順 4 ～ 9 に従ってすべての検索サービスをアップグレードします。2 つ目以降の検索サービスのアップグレード時に特別な順序は要求されません。
10. すべての検索サービスをアップグレードしたら、次のコマンドを使用して、すべての検索サービスの InterScan MSS サービスを起動します。

```
$IMSS_HOME/imss/script/imssstart.sh
```

InterScan MSS 7.0 から InterScan MSS 7.1 へ移行する

移行プロセスでは、次の手順を実行する必要があります。

手順 1 — InterScan MSS 7.0 の設定をエクスポートする

手順 2 — InterScan MSS 7.0 の設定を InterScan MSS 7.1 にインポートする

移行する前に、InterScan MSS 7.0 データベースのステータスと動作を確認します。

注意： アップグレードまたは移行には InterScan MSS 7.0 SP1 が必要です。

InterScan MSS 7.0 の設定をエクスポートする

InterScan MSS 7.0 エクスポートツールを使用して、InterScan MSS 7.0 から設定をエクスポートします。

InterScan MSS 7.0 の設定をエクスポートするには

1. InterScan MSS 7.0 サーバに migration_tool_70to71.tar.gz をコピーします。
2. 次のコマンドを使用して、エクスポートツールを抽出します。

   ```
   tar zxf migration_tool_70to71.tar.gz
   ```

3. 次のコマンドを使用して、エクスポートツールを実行します。

   ```
   ./export_tool_70.sh -e < ファイル名 >
   ```

注意： エクスポートツールのヘルプを表示するには、-h を使用します。

エクスポートツールにより、設定パッケージ imss_config_70.tar.gz が $PWD にエクスポートされます。

注意： エクスポートツールにより、詳細なエクスポートログ export_70.xxxxxxxx.log が現在のフォルダの下に作成されます。

InterScan MSS 7.0 の設定を InterScan MSS 7.1 にインポートする

移行後に、InterScan MSS 設定は上書きされ、すべてのサービスが再起動します。

警告： 移行中は、データベース操作を実行しないでください。

移行中は、グループ内のサービスを起動または停止しないでください。

ヒント： トレンドマイクロでは、新規インストールの InterScan MSS 7.1 で移行を実行することをお勧めします。

InterScan MSS 7.0 から InterScan MSS 7.1 に設定を移行するには

1. InterScan MSS 7.1 に移行パッケージ migration_tool_70to71.tar.gz をコピーします。
2. 次のコマンドを使用して、移行ツールを抽出します。

   ```
   tar zxf migration_tool_70to71.tar.gz
   ```

3. InterScan MSS 7.0 の設定パッケージを InterScan MSS 7.1 にコピーします。詳細については、107 ページの「InterScan MSS 7.0 の設定をエクスポートする」を参照してください。
4. 次のコマンドを使用して、移行ツールを起動します。

   ```
   ./migration_tool_70.sh
   ```

   注意： 続行する前に、移行ツールのスコープと制限事項をよくお読みください。

5. 表示される手順に従って、移行ツールを使用します。

   InterScan MSS 7.1 により、次の場所に詳細な移行レポートおよびログが作成されます。

   ```
   {InterScan MSS のインストールパス }/installlog/migration/MigrationReport
   and migration_70.yyyymmdd.log
   ```

6. 次の移行後タスクを実行して、移行の結果を確認します。
   c. 移行した項目の結果を確認します。
   d. すべてのサービス、特にポリシーサーバが起動可能であることを確認します。
   e. 管理サーバですべてのポリシーにアクセスできることを確認します。

サポートされているサービスのアクティベーション

アップグレード後に、InterScan MSS 7.1 では、InterScan MSS 7.0 からのアクティベーションコードが保持されます。アクティベーションコードの有効期限が切れている場合、次を使用して新しいアクティベーションコードを入力します。

- ウイルス対策およびコンテンツフィルタ
- スパムメール対策 (IP プロファイラを含む)

Email Reputation Services (以下、ERS) を使用するには、インストール時にアクティベーションコードを入力する必要があります。

アップグレードをロールバックする

バージョン 7.1 へのアップグレードで問題が発生した場合、前のバージョンにロールバックできます。InterScan MSS 7.0 インストールの詳細については、InterScan MSS 7.0 のドキュメントを参照してください。

InterScan MSS 7.0 へロールバックする

アップグレードプロセスでは、一定の段階までアップグレードが自動的にロールバックされます。ただし、次のように、元に戻せなくなる段階があります。

- InterScan MSS コンポーネントのアップグレード : 103 ページの「InterScan MSS 7.0 の単一サーバ配置をアップグレードする」プロセスの手順 6 または 104 ページの「InterScan MSS 7.0 の分散配置をアップグレードする」の手順 8 の後
- IP プロファイラのアップグレード

上記のプロセスでは、ロールバックを手動で実行する必要があります。

InterScan MSS コンポーネントのアップグレード後にロールバックする

アップグレードプロセスのこの段階では、インストーラにより InterScan MSS 7.0 パッケージが削除され、InterScan MSS 7.1 パッケージの管理データベースがインストールされ、データが新しい管理データベースに移行されます。

この段階でインストーラに問題が発生すると、ロールバックプロセスには次の手順が必要になります。

手順 1 — InterScan MSS 7.1 コンポーネントを削除する

手順 2 — InterScan MSS 7.0 へロールバックする

InterScan MSS 7.1 コンポーネントを削除するには

1. 次のコマンドを使用して、InterScan MSS 7.1 パッケージを削除します。

   ```
   rpm -e imss imsscctrl imsseuq
   ```

   注意： パッケージの不足に関して表示されるエラーメッセージは無視します。

2. アップグレード中に新しい PostgreSQL がインストールされていた場合は、次のコマンドを使用して PostgreSQL を削除します。

```
su - imss -c "/opt/trend/imss/PostgreSQL/bin/pg_ctl -D
'/var/imss/pgdata' -w -m fast stop"

rm -rf /var/imss
```

InterScan MSS 7.0 へのロールバックを完了するには

1. 次のコマンドを使用して、InterScan MSS 7.0 パッケージ情報にロールバックします。

   ```
   tar xvf rpm.tar -C /

   rpm -rebuilddb
   ```

   注意： この操作を実行すると、バックアップの作成後にインストールされたすべての RPM パッケージの情報が失われます。InterScan MSS 7.0 のアップグレード中に他の RPM パッケージをインストールしないでください。

2. 次のコマンドを使用して、InterScan MSS 7.0 バイナリにロールバックします。

   ```
   mv $IMSS_HOME/imss/queue $IMSS_HOME/installlog/binary

   rm -rf $IMSS_HOME/imss

   mv $IMSS_HOME/installlog/binary $IMSS_HOME/imss
   ```

3. 次のコマンドを使用して、InterScan MSS 7.0 エンドユーザメール隔離データベースにロールバックします。

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

4. 次のコマンドを使用して、Postfix 設定にロールバックします。

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

5. 次のコマンドを使用して、InterScan MSS 7.0 自動起動スクリプトを再作成します。

   ```
   ./imss/recreate_rclink_70.sh
   ```

   これで、InterScan MSS 7.0 環境は、アップグレード前と同じになります。

IP プロファイラのアップグレード後にロールバックする

アップグレードプロセスのこの段階では、インストーラにより InterScan MSS 7.0 パッケージが削除され、InterScan MSS 7.1 パッケージの管理データベースがインストールされ、データが新しい管理データベースに移行されます。IP プロファイラのインストールが試行されますが、問題が発生します。

この段階でインストーラに問題が発生すると、ロールバックプロセスには次の手順が必要になります。

手順 1 — InterScan MSS 7.1 コンポーネントを削除する

手順 2 — InterScan MSS 7.0 へロールバックする

InterScan MSS 7.1 コンポーネントを削除するには

1. 次のコマンドを使用して、InterScan MSS 7.1 パッケージを削除します。

   ```
   rpm -e imss imsscctrl imsseuq
   ```

   注意： パッケージの不足に関して表示されるエラーメッセージは無視します。

2. アップグレード中に新しい PostgreSQL がインストールされていた場合は、次のコマンドを使用して PostgreSQL を削除します。

   ```
   su - imss -c "/opt/trend/imss/PostgreSQL/bin/pg_ctl -D
   '/var/imss/pgdata' -w -m fast stop"
   ```

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

InterScan MSS 7.0 へのロールバックを完了するには

1. 次のコマンドを使用して、InterScan MSS 7.0 パッケージ情報にロールバックします。

   ```
   tar xvf rpm.tar -C /
   ```

   ```
   rpm -rebuilddb
   ```

   注意： この操作を実行すると、バックアップの作成後にインストールされたすべての RPM パッケージの情報が失われます。InterScan MSS 7.0 のアップグレード中に他の RPM パッケージをインストールしないでください。

2. 次のコマンドを使用して、InterScan MSS 7.0 バイナリにロールバックします。

   ```
   mv $IMSS_HOME/imss/queue $IMSS_HOME/installlog/binary
   ```

   ```
   rm -rf $IMSS_HOME/imss
   ```

   ```
   mv $IMSS_HOME/installlog/binary $IMSS_HOME/imss
   ```

3. 次のコマンドを使用して、InterScan MSS 7.0 エンドユーザメール隔離データベースにロールバックします。

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

4. 次のコマンドを使用して、Postfix 設定にロールバックします。

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

5. 次のコマンドを使用して、InterScan MSS 7.0 自動起動スクリプトを再作成します。

```
./imss/recreate_rclink_70.sh
```

これで、InterScan MSS 7.0 環境は、アップグレード前と同じになります。

6. 次のコマンドを使用して、IP プロファイラパッケージを削除します。

```
imss/remove_ipp.sh
```

7. InterScan MSS 7.0 へのロールバックを完了するには、次のコマンドを使用します。

```
imss/ipfilterinsh.sh #IMSS 7.0
```

注意： IP プロファイラの再インストール時には、ERS/IP プロファイラのアクティベーションコードを入力します。

第 6 章

トラブルシューティングとサポート情報

この章では、Trend Micro InterScan Messaging Security Suite 7.1 (以下、InterScan MSS) の一般的な問題のトラブルシューティング、トレンドマイクロの製品 Q&A の検索、およびトレンドマイクロサポートへの問い合わせの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。

- 114 ページの「トラブルシューティング」
- 114 ページの「よくある質問 (Q&A)」
- 116 ページの「製品サポート情報」
- 116 ページの「サポートサービスについて」
- 117 ページの「製品 Q&A のご案内」
- 117 ページの「セキュリティ情報」
- 118 ページの「トレンドマイクロへのウイルス解析依頼」
- 118 ページの「ウイルス解析サポートセンター「TrendLabs」」

トラブルシューティング

表 6-1 に、InterScan MSS のインストールで発生する可能性のある問題の一般的なトラブルシューティングの方法を示します。解決策についても、この表を参照してください。この表を見ても問題が解決しない場合は、トレンドマイクロの製品 Q&A を確認してください。

InterScan MSS の管理またはサポートに関するトラブルシューティングについては、「Trend Micro InterScan Messaging Security Suite 7.1 管理者ガイド」を参照してください。

表 6-1. インストールに関する問題のトラブルシューティング

問題	推奨される解決策
ERS のインストールで ERS アクティベーションコードの有効性が確認されない	アクティベーションコードの有効性を確認するために、ERS インストールスクリプトによりインターネットを経由してトレンドマイクロにアクセスします。 DNS サーバが正常に動作し、ERS をインストールするコンピュータからインターネットにアクセスできることを確認してください。

よくある質問 (Q&A)

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。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。

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 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。以下に例を示します。

```
detach_key_postfix=smtpd_use_tls:queue_directory:{Parameter1}:{Parameter2}:…::{Parameter n}
```

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

InterScan MSS 管理データベースを独立させてインストールできますか。

はい。InterScan MSS 管理データベースを独立させてインストールできます。インストールプログラムを実行し、他の InterScan MSS コンポーネントは選択せずに InterScan MSS データベースのみを設定します。

インストールできるエンドユーザメール隔離サービスおよびエンドユーザメール隔離データベースの数を教えてください。

最大 8 個のエンドユーザメール隔離サービスおよびエンドユーザメール隔離データベースをインストールできます。

エンドユーザメール隔離サービスごとに 1 つのエンドユーザメール隔離データベースをインストールする必要がありますか。

いいえ。複数のエンドユーザメール隔離サービスで 1 つのエンドユーザメール隔離データベースを共有できますが、エンドユーザメール隔離サービスには少なくとも 1 つのエンドユーザメール隔離データベースが必要です。

InterScan MSS エンドユーザメール隔離データベースは、アンインストール時に削除されますか。

いいえ。InterScan MSS エンドユーザメール隔離データベースは、InterScan MSS のアンインストール時には削除されません。

古い InterScan MSS データベースをインストール時に削除できないのはなぜですか。

インストールプログラムが古い InterScan MSS データベースを削除しようとするときに、一部のアプリケーションがこれらのデータベースに接続されている場合があります。古いデータベースへのすべての接続を切断して、再度実行してください。

外部 DNS サーバを使用するコンピュータに InterScan MSS 7.1 をインストールした場合、何か問題がありますか。

InterScan MSS 7.1 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 7.1 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。

製品サポート情報

InterScan MSS 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「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、FAX、メールなどをご利用ください。サポートセンターの連絡先は、「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、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。

製品 Q&A のご案内

トレンドマイクロの Web サイトでは、製品 Q&A の情報を提供しています。これは、トレンドマイクロの製品に関する技術的な質問と、それに対する回答を集めたものです。製品 Q&A には、次の URL からアクセスできます。

製品 Q&A

`http://esupport.trendmicro.co.jp/corporate/search.aspx`

製品 Q&A では、お使いの製品名およびキーワードを指定して、知りたい情報を検索できます。たとえば製品のマニュアル、ヘルプ、Readme ファイルなどに記載されていない情報が必要な場合に、製品 Q&A を利用してください。

トレンドマイクロでは製品 Q&A の内容を常に更新し、新しい情報を追加しています。

セキュリティ情報

セキュリティ情報の入手先

トレンドマイクロでは、最新のセキュリティ情報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情報 Web サイトでは、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。セキュリティ情報 Web サイトは、次の URL からアクセスできます。

`http://www.trendmicro.co.jp/vinfo/`

管理コンソールからセキュリティ情報サイトにアクセスすることもできます。セキュリティ情報サイトにアクセスするには、管理コンソールの画面の右上にあるリストボックスから [セキュリティ情報] リンクを選択します。

セキュリティ情報 Web サイトでは、次の情報を閲覧できます。

- ウイルス名やキーワードから検索できるウイルスデータベース
- 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

セキュリティ情報 Web サイト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ウイルスデータベース検索サイトにアクセスして、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。

```
http://www.trendmicro.co.jp/vinfo/virusencyclo/default.asp
```

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。

```
http://inet.trendmicro.co.jp/esolution/attach_agreement.asp
```

感染ファイルを送信する際には、感染症状について簡単に説明したメッセージを同時に送ってください。送信されたファイルがどのようなウイルスに感染しているかを、トレンドマイクロのウイルスエンジニアチームが解析し、回答をお送りします。

感染ファイルのウイルスを駆除するサービスではありません。ウイルスが検出された場合は、ご購入いただいた製品にてウイルス駆除を実行してください。

ウイルス解析サポートセンター「TrendLabs」

トレンドマイクロのウイルス解析サポートセンター「TrendLabs」(トレンドラボ) は、フィリピンセンターを本部として、米国、日本、台湾、ドイツ、アイルランド、中国、フランス、メキシコの各国センターで構成されています。24 時間体制でウイルスの活動を監視するウイルス解析エンジニアを含む 1000 名以上のスタッフが、セキュリティに関する最新の情報を収集し、高品質なサービスとソリューションを迅速かつ効果的に世界各国のトレンドマイクロのパートナーとお客さまに提供しています。

「TrendLabs」では、品質保証の ISO9001:2000 認定 (フィリピン)、国際規格 COPC-2000 規格 (フィリピン)、英国の国家規格 ITIL: BS15000 (ドイツ)、情報セキュリティマネージメントの英国規格 BS7799 (フィリピン) を取得しています。

索引

英数字

Apache 48
  Tomcat 47
Control Manager
  概要 24
Control Manager MCP エージェント、エージェント
  Control Manager MCP 24
ERS
  概要 36
  管理コンソール 39
  サービス 36
  仕組み 38
IMSSMGR 47
InterScan MSS
  概要 14
InterScan MSS コンポーネント
  インストール 47
  エンドユーザメール隔離データベース 34
  エンドユーザメール隔離プライマリおよびセカンダリサービス 32
  管理データベース 30
  検索サービス 30
  セントラルコントローラ 30
  ポリシーサービス 31
  ポリシーサービスの同期 31
IP フィルタ
  インストール 87
  概要 35
  削除 95
IP プロファイラ
  概要 35
  検出 35
  仕組み 37
MTA
  Postfix の準備 78
Named Server 47
Postfix の準備 78
Readme ファイル 10
Tomcat 47、48
TrendLabs 118
対象読者 10

あ

新しい機能 14
アップグレード
  InterScan MSS 7.0 101
アンインストール 94
  IP フィルタコンポーネント 95
移行
  InterScan MSS 7.0 から 106
  ロールバック 109
インストール
  Control Manager の使用 71
  DMZ 内 56
  IP フィルタ 87
  IP フィルタ、インストール
    エンドユーザメール隔離 73
  Postfix の準備 78

SMTP ゲートウェイ上 55
確認 93
クラスタ化 68
削除、InterScan MSS 94
シナリオ 61
手順 84
ファイアウォールなし 52
ファイアウォールの内側 54
ファイアウォールの外側 53
オンラインヘルプ 10

か

概要、InterScan MSS 14
確認、インストール 93
管理データベース 47
検索サービス 32
コンポーネントおよびサブモジュールのインストール 47

さ

最小要件 78
システム要件 78
新機能 14
スパイウェアとグレーウェア 22
セントラルコントローラ 31

た

データベース
セントラルコントローラ上 30
データベースサーバ 47
テクニカルサポート 116
ドキュメント
InterScan MSS 関連 10
トラブルシューティング 114
ERS 114

は

パターンマッチング 15
フィルタリング、仕組み 19
フェイルオーバー 74
ポリシー
ポリシーサービス 31

ま

マスメーリングウイルス
パターンファイル 18
メールの脅威
スパムメール 17
非生産的なメッセージ 17
メールログパーサ 48

や

要件 78
よくある質問
Postfix 114

ら

ロールバック
InterScan MSS 7.0 109
ロールバック、移行 109