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

トレンドマイクロへのお客様情報の送信について

「フィッシング詐欺対策」「URL フィルタ」では、Webサイトが安全かどうかの判定のために、お客さまがアクセスしたURLの情報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。

「ソフトウェア安全性評価サービス」では、プログラムが安全かどうかの判定のために、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、弊社製品の改良目的および迷惑メールの撲滅のため、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。

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ウェブ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ウェブ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。本ドキュメントの作成にあたっては細心の注意を払っていますが、本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。

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、Trend Micro Policy Server、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、Trend Micro Enterprise Protection Strategy、InterScan Gateway Security Appliance、Trend Micro Network VirusWall、Network VirusWall Enforcer、Trend Flex Security、EPS、Trend Micro EPS、LEAKPROOF、Trendプロテクト、Expert on Guard、InterScan Messaging Security Appliance、InterScan Web Security Appliance、InterScan Messaging Hosted Security、およびDataDNA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 © 2007-2009 Trend Micro Incorporated. All rights reserved.

P/N: IMSSUX-AE0105_R2 (2009/01)

目次

はじめに 9

ドキュメント 10

対象読者 10

ドキュメントの表記規則 11

第 1 章　製品の概要 13

InterScan MSS 7.0 について 14

新機能 14

InterScan MSS の主な特長と利点 17

スパイウェアと他の種類のグレーウェア 24

Trend Micro Control Manager について 26

Trend Micro Control Manager との統合 27

第 2 章　システム要件とコンポーネント 31

システム要件 32

InterScan MSS コンポーネントについて 36

InterScan MSS 管理データベース 36

セントラルコントローラ 36

検索サービス 37

ポリシーサービス 38

ポリシーの同期 38

エンドユーザメール隔離サービス 38

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 39
エンドユーザメール隔離サーバコンポーネント 39
Apache および mod_jk 40
Tomcat 40
Struts フレームワーク 41
エンドユーザメール隔離アプリケーション 41
エンドユーザメール隔離のデータベース 42
IP フィルタ 42
Trend Micro Network Reputation Services 43
Trend Micro Network Reputation Services の種類 43
IP プロファイラの機能 44
Trend Micro Network Reputation Service の機能 45

第 3 章 配置計画 47

配置チェックリスト 48
コンポーネントおよびサブモジュールのインストール 52
InterScan MSS で使用されるポート 55
ネットワークトポロジの検討 58
ファイアウォールを使用しないインストール 58
ファイアウォールの外側へのインストール 59
受信トラフィック 59
送信トラフィック 59
ファイアウォールの内側へのインストール 60
受信トラフィック 60
送信トラフィック 61
既存の SMTP ゲートウェイ上へのインストール 61
受信トラフィック 62
送信トラフィック 62

DMZ 内へのインストール 62
受信トラフィック 62
送信トラフィック 62
運用モデルについて 64
スタンドアロンモデル 65
サンドイッチモデル 67
プロキシモデル 69
インストールシナリオの理解 70
集中インストール 70
複数の検索サービスのインストール 72
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 74
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 77
サーバ間の通信 77
複雑な分散インストール 78
WAN へのインストール 80
Trend Micro Control Manager 80
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 82
IP フィルタ 84
IP フィルタ機能を付加した InterScan MSS の配置 84
フェイルオーバーについて 85

第 4 章 インストールとアップグレード 87

MTA の準備 88
Postfix の準備 88
InterScan MSS 7.0 Solaris での Postfix のインストール 88
sendmail の使用 93
sendmail のデーモン 94
sendmail #1 の設定 94

sendmail #2 の設定 96
sendmail サービスの再起動 97
Qmail の使用 98
Qmail の設定 99
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 100
Solaris システムファイルの設定 100
インストール手順 101
IP フィルタのインストール 106
IP プロファイラと NRS のインストール 106
sendmail および qmail と InterScan MSS の統合 109
FoxLib と sendmail の統合 109
FoxLib と qmail の統合 111
体験版からの移行 113
バージョン 5.1x からバージョン 7.0 への移行 116
複数の検索サービス配置のアップグレードオプション 116
単一の管理データベース 116
複数の管理データサービス 118
設定のバックアップ 119
移行の手順 120
アクティベート 124
移行できない設定 125
移行レポートの使用 126
移行のロールバック 126
アンインストールの実行 128
InterScan MSS のアンインストール 128
IP プロファイラと NRS のアンインストール 129
手動アンインストールの実行 130
InterScan MSS の手動アンインストール 130

データベースの手動アンインストール 131
Postfix の手動アンインストール 131
IP プロファイラの手動アンインストール 132

第 5 章 トラブルシューティングとサポート情報 135
トラブルシューティング 136
よくある質問 (Q&A) 137
Postfix MTA 設定 137
インストールとアンインストール 138
アップグレード 139
その他 141
製品サポート情報 142
サポートサービスについて 142
製品 Q&A のご案内 143
セキュリティ情報 143
セキュリティ情報の入手先 143
トレンドマイクロへのウイルス解析依頼 144
トレンドマイクロへのスパムメールの報告 145
ウイルス解析サポートセンター「TrendLabs」 145

索引 147

はじめに

Trend Micro InterScan Messaging Security Suite 7.0 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 Suite (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 7.0 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「ドキュメント」
- 10 ページの「対象読者」
- 11 ページの「ドキュメントの表記規則」

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** — 各フィールドの詳細や、ユーザインタフェースを使用してあらゆる機能の設定方法について説明しています。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、既知の問題、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。

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 などの Message Transfer Agent (MTA)
- LDAP
- データベース管理

ドキュメントの表記規則

情報を簡単に検索し、理解できるように、InterScan MSS 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

第 1 章

製品の概要

この章では、TrendMicro InterScan Messaging Security Suite (以下、InterScan MSS) の特長、機能、およびテクノロジについて説明します。また、既存のスパムメール対策機能を強化することのできる他のトレンドマイクロ製品の基本情報も示します。

この章の内容は次のとおりです。

- 14 ページの「InterScan MSS 7.0 について」
- 14 ページの「新機能」
- 17 ページの「InterScan MSS の主な特長と利点」
- 24 ページの「スパイウェアと他の種類のグレーウェア」
- 26 ページの「Trend Micro Control Manager について」

InterScan MSS 7.0 について

InterScan Messaging Security Suite 7.0 (以下、InterScan MSS) では、メールを完全に保護するために、ウイルス対策、スパムメール対策、フィッシング対策、およびコンテンツフィルタの機能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攻撃対策機能が備わっており、既知のウイルスおよび変種 / 亜種のウイルスをブロックします。

InterScan MSS のスパムメール対策は、Trend Micro Network Reputation Services (以下、NRS) と IP プロファイラによるカスタマイズ可能なトラフィック管理機能による第 1 防御レベルと、やさまざまな技術を取り入れた強力なエンジンによる多層構造になっています。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 の保護機能により、単一でスケーラビリティの高いプラットフォームで、一元化管理が容易になり、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 に、バージョン 7.0 の新機能の概要を示します。

新機能	説明
さまざまなウイルス対策および不正プログラムのポリシー	さまざまな InterScan MSS ポリシーと LDAP のサポートにより、さまざまな条件に基づいて、特定の送信者および受信者に適用するフィルタを設定できます。
ポリシーの一元化	一元化された InterScan MSS ポリシーと LDAP のサポートにより、さまざまな条件に基づいて、特定の送信者および受信者に適用するフィルタを設定できます。

表 1-1. 新機能

新機能	説明
ログおよびレポート機能の一元化	一元管理される詳細なレポート機能により、ポリシーに一致した送受信者の上位を示す統計データや、トラフィックデータを作成できます。 ログ機能も一元化されているため、管理者はメッセージに関連する活動をすばやく監査できます。
アーカイブおよび隔離領域管理の一元化	InterScan MSS の複数のメッセージ隔離領域とアーカイブ領域を簡単に検索できます。
スケーラブルなエンドユーザメール隔離	複数のエンドユーザメール隔離サービスは、スパムメールとして検出、隔離されたメールメッセージの表示機能を提供します。 InterScan MSS でエンドユーザメール隔離の通知機能を使用することで、ヘルプデスクの管理作業にかかるコストを低減できます。
さまざまなスパムメール対策テクノロジ	次の 3 層にわたるスパムメール対策が用意されています。 ・接続層でスパムメール送信者をフィルタする NRS ・高度なプロファイル (SMTP IDS) を使用してメールサーバを攻撃から保護する IP プロファイラ ・スパムメールを的確に検出し、削除するスパムメール検索エンジン
IntelliTrap	IntelliTrap は、さまざまな圧縮スキームで圧縮されたウイルスがメールを通じてネットワークに侵入するリスクを軽減できるよう、圧縮ファイルのヒューリスティック評価機能を提供します。
管理タスクの委任	LDAP が統合されたアカウント管理により、ユーザは設定タスクごとに管理権限を割り当てることができます。
設定ウィザードによる簡単配置	InterScan MSS をすぐに起動して実行できるように、使いやすい設定ウィザードが用意されています。
高度な MTA 機能	TLS や、ドメインベースの配信などの MTA 機能により、InterScan MSS は安全な方法で効果的にメールを処理します。

表 1-1. 新機能

新機能	説明
移行	アップグレード手順が簡単なため、セットアップ時は最小限の操作で設定内容を移行できます。
メールの監査とトラッキング	すべてのメッセージが詳細にログされるため、メッセージフローに関する問題をトラックして特定できます。
Trend Micro Control Manager (以下、Control Manager) との統合	さまざまな対応機能に加え、Control Manager から NRS のログクエリを実行します。

表 1-1. 新機能

InterScan MSS の主な特長と利点

特長	説明	利点
ウイルス対策	InterScan MSS は、トレンドマイクロの検索エンジンとパターンマッチングと呼ばれるテクノロジを使用して、ウイルスを検出します。検索エンジンは、ゲートウェイを介して受信したファイルに含まれるコードを、パターンファイルに格納されている既知のウイルスのバイナリパターンと比較します。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、そのウイルスコードの削除、メッセージの隔離などの処理を実行することによりファイル内のウイルス駆除を試みます。	InterScan MSS では、ウイルス検索およびコンテンツ検索機能が強化されているため、メッセージングシステムの動作効率を最適な状態で維持できます。
IntelliTrap	ウイルス作成者は通常、さまざまなファイル圧縮スキームを使用してウイルスフィルタを回避しようとします。IntelliTrap は、これらの圧縮ファイルのヒューリスティック評価機能します。 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誤って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、ユーザが日常的に圧縮ファイルをやり取りしている場合は、この機能を無効にした方がよい場合もあります。 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誤っ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で圧縮されたウイルスがメールを通じてネットワークに侵入するリスクを軽減できるようにします。

表 1-2.　主な特長と利点

特長	説明	利点
コンテンツ管理	InterScan MSS は、ネットワーク経由で送受信されるメールのメッセージと添付ファイルを解析し、適切な内容かどうかをチェックします。	個人的なメールのやり取りや巨大な添付ファイルなど、企業が不適切と見なす内容は、InterScan MSS を使用して効果的にブロックしたり、受信を遅延したりできます。
その他のメール脅威からの保護		
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 を使用すると、どのような特性を持つメッセージを SMTP ゲートウェイで阻止するかを設定できるため、DoS 攻撃のリスクを低減できます。
不正なメールコンテンツ	実行可能プログラムや、マクロが埋め込まれたドキュメントなど、ウイルスはさまざまな種類の添付ファイルに潜んでいる可能性があります。HTML スクリプトファイル、HTML リンク、Java アプレット、ActiveX コントロールが含まれるメッセージも、有害な処理を実行する可能性があります。	InterScan MSS では、SMTP ゲートウェイの通過を許可するメッセージの種類を設定できます。
生産性の劣化	ビジネスに関係のないメールトラフィックは、多くの企業で問題となっています。スパムメールメッセージはネットワーク帯域幅を消費し、従業員の生産性に影響します。従業員の中には、会社のメッセージングシステムから個人的なメッセージを送信したり、巨大なマルチメディアファイルを転送したり、業務時間内に個人的なビジネスを行ったりする人もいます。	ほとんどの企業では、メッセージングシステムの使用許容範囲を示すポリシーを制定しています。InterScan MSS は、企業の既存のポリシーを強化し、確実に準拠させることのできるツールを提供します。

表 1-2.　主な特長と利点

特長	説明	利点
法的責任とビジネスの信頼性	メールが不正に使用されると、企業の法的責任が問われる場合があります。従業員が性的または人種的嫌がらせを行っていたり、他の違法活動に携わっていたりするかもしれません。また、従業員の不正行為により、社内のメッセージングシステムから機密情報が漏えいする可能性もあります。企業のメールサーバから不適切なメッセージが配信されれば、そのメッセージの内容が企業の持論と異なるものであったとしても、企業の評判を損ねることになります。	InterScan MSS には、コンテンツを監視してブロックするツールが装備されているため、不適切な内容や機密事項が含まれるメッセージがゲートウェイを通過するリスクを低減できます。
マスメーリング型ウイルスの抑制	企業のメッセージングシステムを介して偽造メッセージを自動的に広めるメール送信型ウイルスは、クリーンナップに費用がかかり、ユーザ間にパニックを引き起こす可能性があります。 InterScan MSS では、マスメーリング型ウイルスを検出したときに、他の種類のウイルスとは異なる処置を講じます。 たとえば、重要な情報が含まれる Microsoft Office ドキュメントに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代わりにメッセージを隔離するようプログラムを設定できます。また一方で、マスメーリング型ウイルスが検出されたときに、プログラムでメッセージ全体を自動的に削除することも可能です。	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型ウイルスの識別情報は、マスメーリング型パターンファイルに含まれています。このパターンは、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。これらの種類のウイルスとそのメールコンテナを自動的に削除するように指定すれば、リソースを節約すると共に、従業員からのヘルプデスクへの問い合わせを回避し、大規模感染後のクリーンナップ作業も排除することができます。

表 1-2.　主な特長と利点

特長	説明	利点
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	クライアントは、ウイルス以外のスパイウェア、アドウェア、ダイヤラーなど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、24 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。
総合的なスパムメール対策		
スパムメール対策 (コンテンツ検索)	InterScan MSS では、オプションでスパムメール対策 (コンテンツ検索) 機能をインストールすることもできます。この機能を使用するには、別途アクティベーションコードが必要になります。詳細については、販売店にお問い合わせください。 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** : InterScan MSS のスパムメール対策機能は、IP プロファイラと NRS を設定する前にアクティベートしてください。	InterScan MSS のスパムメール対策機能では、最新のコンテンツ処理および統計分析に基づく検出テクノロジが使用されています。コンテンツ分析機能を採用したことで、パフォーマンスの高いリアルタイムの検出が可能となっています。スパムメールの送信者が手法を変更した場合でも、容易に対応できます。

表 1-2. 主な特長と利点

特長	説明	利点
IP プロファイラと NRS 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。NRS 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。 詳細については、以下を参照してください。 ・42 ページの「IP フィルタ」 ・43 ページの「Trend Micro Network Reputation Services」 ・44 ページの「IP プロファイラの機能」 ・45 ページの「Trend Micro Network Reputation Service の機能」	IP プロファイラおよび NRS から成る IP フィルタ機能を統合することで、InterScan MSS は IP レベルでスパムメール送信者をブロックできます。
その他		
LDAP およびドメインベースのポリシー	Lotus Domino、Microsoft Active Directory などの LDAP ディレクトリサービスをユーザグループの定義および管理者権限に使用している場合、LDAP を設定できます。Web 隔離ツールを使用するには、LDAP を有効にする必要があります。	LDAP を使用すると、さまざまなルールを定義して、企業のメールの使用ガイドラインを適用することができます。送信者および受信者のアドレスに基づいて、個人またはグループ用のルールを定義できます。
Web ベースの管理コンソール	Web ベースの管理コンソールを使用すると、InterScan MSS のポリシーや設定を、Web 上で必要に応じて設定できます。	Web ベースのコンソールは、SSL に準拠しているので、高い安全性が確保されます。

表 1-2.　主な特長と利点

特長	説明	利点
エンドユーザメール隔離	InterScan MSS には、スパムメール管理を強化するための Web ベースのエンドユーザメール隔離が用意されています。Web ベースのエンドユーザメール隔離を使用すると、エンドユーザは各自のスパムメールの処理方法を管理できます。InterScan MSS のスパムメール対策機能によって、スパムメールが隔離されます。これらのメッセージは、エンドユーザメール隔離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。	別々の従業員に管理役割を委任して、人材のバックアップ体制を構築し、管理業務全般の共有を促進できます。
一元化されたレポート機能	一元化されたレポート機能では、必要に応じてそのつどレポートを作成することも、指定されたときにレポートを作成することも可能です。	InterScan MSS の稼動状況を解析できます。 必要なときにそのつどレポートを作成する場合、レポート内容の種類を必要に応じて指定できます。また、日次、週次、および月次ベースで自動生成するように InterScan MSS を設定することもできます。
システムの可用性の監視	組み込みエージェントが InterScan MSS サーバの状態を監視し、メールフローを妨害する可能性のある違反状況が発生した場合に、メールまたは SNMP トラップを通じて通知を配信します。	システム障害の検出をメールで通知するので、ただちに適切な処置を講じて、ダウンタイムを最小限にすることができます。

表 1-2.　主な特長と利点

特長	説明	利点
POP3 メール検索	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 トラフィックのほかに、InterScan MSS では、ネットワーク内のメッセージングクライアントがメッセージを受信する際に、ゲートウェイで POP3 メッセージも検索できます。
クラスタアーキテクチャ	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。	さまざまな InterScan MSS コンポーネントを個別のコンピュータにインストールすることも、いくつかの同じコンポーネントを複数のコンピュータにインストールすることもできます。たとえば、メッセージングのボリュームに応じて、InterScan MSS の追加の検索サービスコンポーネントを別のサーバにインストールし、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.　主な特長と利点

特長	説明	利点
Control Manager との統合	Control Manager は、ウイルス対策プログラムとコンテンツセキュリティプログラムを、その物理的な位置やプラットフォームに関係なく中央から制御できるようにするソフトウェア管理ソリューションです。このアプリケーションは、企業のウイルスおよびコンテンツセキュリティポリシーの管理を簡略化します。 詳細については、26 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。新種のメール送信型ウイルスが検出されると、トレンドラボから詳細なコンテンツフィルタを使用するポリシーが発行されるため、InterScan MSS では、メッセージ内の疑わしい特性を識別して、メッセージをブロックすることができます。これらのルールは、最新のパターンファイルが提供されるまでの期間、感染の機会を最小限に抑えるのに役立ちます。

表 1-2.　主な特長と利点

スパイウェアと他の種類のグレーウェア

クライアントは、ウイルス以外の脅威のリスクにもさらされています。グレーウェアは、ネットワーク上のコンピュータのパフォーマンスに悪影響を与え、セキュリティの上でも、機密性に関しても、法的な面でも、企業に深刻なリスクをもたらします (表 1-3 を参照)。

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 ブラウザを通じてそのユーザをさまざまな広告のターゲットとするために、ユーザの Web サーフィンの好みなどのデータを収集したりします。

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
ダイヤラー	コンピュータのインターネット設定を変更し、あらかじめ設定された電話番号に、コンピュータがモデムを通じて自動的にダイヤルするようにします。
ジョークプログラム	CD-ROM トレイを開閉したり、大量のメッセージボックスを表示したりするなど、コンピュータの異常動作を引き起こします。
ハッキングツール	ハッカーがコンピュータに侵入するために使用するツールです。
リモートアクセスツール	ハッカーがコンピュータをリモートにアクセスして制御するためのツールです。
パスワード解読アプリケーション	ハッカーがアカウントユーザ名とパスワードを解読するためのツールです。
その他	上記以外の種類。

表 1-3. スパイウェア / グレーウェアの種類

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、その物理的な位置やプラットフォームに関係なく中央から制御できるようにするソフトウェア管理ソリューションです。このアプリケーションは、企業のウイルスおよびコンテンツセキュリティポリシーの管理を簡略化します。

Control Manager 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、このサーバに生成されます。

  注意： InterScan MSS 7.0 Solaris を Control Manager で管理する場合、Control Manager 3.5 Patch 3 以降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、Control Manager が製品を管理できるように、製品サーバ上にインストールされるアプリケーションです。エージェントは Control Manager サーバからコマンドを受信して、管理対象製品に適用します。また、製品からログを収集して、Control Manager に送信します。

  注意： エージェントは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、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。ディレクトリツリーは、Control Manager に登録されたすべての管理下のエンティティの組織図です。InterScan MSS は、Control Manager 管理コンソールの 1 つのエンティティといえます。

検索サービスをインストールする際に、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、検索サービスはそれぞれ Control Manager サーバに登録され、個別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 を管理する場合は、Control Manager サーバのバージョン 3.5 以降を使用します。Control Manager の詳細およびアップデートプログラムについては、トレンドマイクロの最新版ダウンロードサイトを参照してください。
http://www.trendmicro.co.jp/download/product.asp?productid=7

Trend Micro Control Manager との統合

表 1-4 は、InterScan MSS でサポートされている Control Manager の機能を示しています。

機能	説明	サポートの有無
双方向の通信	双方向の通信では、InterScan MSS または Control Manager のいずれかが通信処理を開始できます。	サポートなし。 Control Manager との通信処理を開始できるのは、InterScan MSS のみです。
大規模感染予防ポリシー	大規模感染予防ポリシーは、トレンドラボで開発された、大規模感染に素早く対応するポリシーです。これには、InterScan MSS サーバやクライアントが感染する可能性を低減するために InterScan MSS で実行される、一連の処理が含まれています。 トレンドマイクロアップデートサーバは、Control Manager を通してこのポリシーを InterScan MSS に配置します。	サポートあり

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
クエリに対するログのアップロード	InterScan MSS ウイルスログ、コンテンツセキュリティログ、NRS ログを、クエリの目的で Control Manager にアップロードします。	サポートあり
シングルサインオン	InterScan MSS Web 管理コンソールにログオンせずに、Control Manager から InterScan MSS を直接管理します。	サポートなし。 Control Manager から InterScan MSS を管理するには、まず、InterScan MSS Web 管理コンソールにログオンする必要があります。
設定の複製	Control Manager から、既存の InterScan MSS サーバの設定を新しい InterScan MSS サーバへ複製します。	サポートあり
パターンファイルのアップデート	Control Manager から、ウイルス / 不正プログラムのパターンファイルをアップデートします。	サポートあり
検索エンジンのアップデート	Control Manager から検索エンジンをアップデートします。	サポートあり
製品コンポーネントのアップデート	Control Manager から、Patch や HotFix などの InterScan MSS 製品コンポーネントをアップデートします。	サポートなし。 製品コンポーネントのアップデートの方法については、特定の Patch または HotFix の Readme ファイルを参照してください。

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
ユーザインタフェースリダイレクトによる設定	Control Manager 内からアクセスできる InterScan MSS Web 管理コンソール使用して、InterScan MSS を設定します。	サポートあり
製品登録の更新	Control Manager から InterScan MSS 製品ライセンスを更新します。	サポートあり
Control Manager 上のメール関連のレポート	Control Manager から次の InterScan MSS メール関連のレポートを生成します。 ・上位 10 位のウイルス検出ポイント ・すべてのエンティティのウイルス感染リスト ・上位 10 位の感染メール送信者のレポート ・上位 10 位のセキュリティ違反のレポート ・ウイルス感染チャネル - 製品の関係のレポート ・頻度別のイベントのフィルタ処理 ・ポリシー別のイベントのフィルタ処理 ・ゲートウェイメッセージングスパムメールの概要レポート ・ゲートウェイメッセージングスパムメールの概要レポート (ドメイン用)	サポートあり

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
Control Manager エージェントのインストール / アンインストール	Control Manager から、InterScan MSS Control Manager エージェントをインストール / アンインストールします。	サポートなし。 InterScan MSS Control Manager エージェントは、InterScan MSS をインストールした時点で自動的にインストールされます。エージェントを有効 / 無効にするには、InterScan MSS Web 管理コンソールから次の操作を実行します。 1. メニューから [管理] → [接続] を選択します。 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 / 無効にするには、[Control Manager エージェントを有効にする] の横のチェックボックスを、それぞれオン / オフにします。
イベント通知	Control Manager から InterScan MSS イベント通知を送信します。	サポートあり
すべてのコマンドに対するコマンド追跡	Control Manager から InterScan MSS に発行されるコマンドのステータスをトラックします。	サポートあり

表 1-4. サポートされている Control Manager の機能

第 2 章

システム要件とコンポーネント

この章では、Trend Micro InterScan Messaging Security Suite (以下、InterScan MSS) を管理するために必要な要件、および InterScan MSS が機能するうえで必要な各種の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。

- 32 ページの「システム要件」
- 36 ページの「InterScan MSS コンポーネントについて」

システム要件

表 2-1 に、InterScan MSS を実行するうえで推奨されるシステムの最小要件を示します。

OS	Linux: ・Red Hat Enterprise Linux AS 3 Update 3 以降 ・Red Hat Enterprise Linux AS 4 Update 3 以降 ・Red Hat Enterprise Linux ES 3 Update 3 以降 ・Red Hat Enterprise Linux ES 4 Update 3 以降 ・SUSE Linux Enterprise Server 9 SP3 以降 ・SUSE Linux Enterprise Server 10 SP1 Solaris: Solaris SPARC 8、9、10
推奨 CPU	Linux: デュアル構成の Xeon 3GHz 以上 Solaris: UltraSPARC IIIi 1.0 GHz 以上
最小 CPU	Linux: Intel Pentium 4 2.4GHz Solaris: Ultra SPARC II 650MHz
推奨メモリ	2GB の RAM
最小メモリ	1GB の RAM
推奨ハードディスク領域	・メール保存用に 10GB ・管理データベース用に 50GB 以上 ・エンドユーザメール隔離データベース用に 20GB 以上 ・作業隔離フォルダ用に 40GB 以上 **注意**: これらの要件は、1 日あたり 500,000 件のメールメッセージ、50% の隔離率で、1ヵ月あたりに保存されるログ数に基づいています。

表 2-1.　システム要件

最小ハードディスク領域	・メール保存用に 1GB ・管理データベース用に 20GB ・エンドユーザメール隔離データベース用に 10GB ・作業隔離フォルダ用に 10GB **注意** : 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初期設定の場所は、/var/imss です。作業隔離フォルダの初期設定の場所は、/opt/trend/imss/queue/ です。
推奨スワップ領域	スワップ領域には、物理メモリの 4 倍のサイズをお勧めします。 **注意** : 各 InterScan MSS の下位プロセスには、120MB のメモリを消費します。したがって、優れたパフォーマンスを得るには、十分な物理メモリおよび仮想メモリを割り当ててピーク時のトラフィックを処理する必要があります。たとえば、2GB の物理メモリと 8GB のスワップ領域を持つコンピュータでは 75 件の下位プロセスを作成できます。必要なスワップ領域は、他のアプリケーションのメモリ消費量に応じて異なります。InterScan MSS は、アップストリーム MTA からの 75 件の接続要求を同時に処理できます。
最小スワップ領域	Linux: 2GB Solaris: 4GB
ブラウザ	・Internet Explorer 6 SP1 または Internet Explorer 7 ・Firefox 1.5
PostgreSQL	バージョン 7.4.8 以上 **注意** : InterScan MSS 7.0 Linux には、PostgreSQL 8.1.3 がバンドルされています。 InterScan MSS 7.0 Solaris には、PostgreSQL 8.1.5 がバンドルされています。
LDAP サーバ	・Microsoft Active Directory 2000 または 2003 ・IBM Lotus Domino 6.0 以上 ・Sun One LDAP 5.2 以上 ・OpenLDAP 2.2 以上

表 2-1.　システム要件

MTA	・Postfix (InterScan MSS 専用の場合) : 2.0 以上 ・Postfix (IP プロファイルを使用する場合) : 2.1 以上 ・Sendmail: 8.2 以上 ・qmail: 1.0.3 以上 **注意** : InterScan MSS 7.0 Solaris には、Postfix 2.3.8 がバンドルされています。
Linux Libraries (全プラットフォーム用)	・glibc-2.2.5 ・libstdc++-libc6.2-2.so.3 (PostgreSQL 用) ・libreadline.so.4
Solaris パッチ	Solaris 10 にパッチ 119689 をインストールしている場合、パッチ 118833-36 が必要になります。パッチ 118833-36 には、次のパッチも必要です。 ・118918-13 ・119042-09 ・119254-36 ・119578-30 ・120900-04 ・121133-02

表 2-1. システム要件

Solaris パッケージ	InterScan MSS をインストールする前に、次のものをインストールしてください。 Solaris 8 および Solaris 9 用 SUNWlibC IP プロファイラをインストールする場合には、次のものをインストールしてください。 ・ Bash Shell ・ BIND バージョン 9.x 以上 **注意** : InterScan MSS 7.0 Linux には、BIND 9.3.2 がバンドルされています。 InterScan MSS 7.0 Solaris には、BIND 9.4.0 がバンドルされています。 Trend Micro Network Reputation Services (以下、NRS) をインストールする場合には、次のものをインストールしてください。 ・ Solaris 8 および Solaris 9 に SUNWcsu ・ Solaris 10 に SUNWbind PostgreSQL をインストールする場合には、次のものをインストールしてください。 ・ Solaris 8 および Solaris 9 に SUNWzlib Trend Micro Control Manager (以下、Control Manager) エージェントを使用する場合には、次のものをインストールしてください。 ・ Solaris 8 および Solaris 9 に SUNWcsl または SUNWcslx ・ Solaris 10 に SUNWcsl または SUNWcslr ・ Control Manager サーバに Patch 3 以降

表 2-1. システム要件

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は、メッセージ処理で実行されるタスクごとに、この製品を個別のコンポーネントに分類しています。以下の項では、各コンポーネントの概要を示します。

InterScan MSS のコンポーネントは、単一のコンピュータまはた複数のコンピュータにインストールできます。コンポーネントの連携方法の図解については、70 ページの「インストールシナリオの理解」を参照してください。

InterScan MSS 管理データベース

InterScan MSS 管理データベースには、グローバル設定情報がすべて保存されます。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データが保持されます。InterScan MSS をインストールする際は、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、データベーステーブルを作成するための適切なクエリを実行する必要があります。データベースは、新しく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。この管理コンソールは、各種のコンポーネントによって検索やログなどのメッセージ処理タスクの実行に使用される InterScan MSS データベースと管理者間のインタフェースとして機能します。

検索サービス

検索サービスとして設定されたサーバでは、次の操作が実行されます。

- SMTP および POP3 メッセージングトラフィックの受け入れ
- ポリシーサービスからのポリシーの要求
- 適用可能なポリシーに基づいたメッセージの評価
- 評価結果に基づいたメッセージへの適切な処理
- 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
- ポリシーとシステムの動作のローカルログへの記録、および指定された間隔での InterScan MSS データベースのログの一部の自動更新。その際、隔離されたアイテムとログを検索できるよう、インデックスが作成されます。

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。同じハードウェア構成のコンピュータが環境内にない場合は、最小限のリソースで検索サービスを保護できるよう、検索サービスの上限を設定する必要があります。たとえば、2 つの検索サービスがあり、1 つのハードディスクが 10GB、もう 1 つのハードディスクが 80GB の場合は、ディスク使用量の上限を 9GB に設定して、最小限のリソースでコンピュータを保護する必要があります。

別の方法として、検索サービスのローカルの設定ファイルを編集し、上限値をローカルに設定することもできます。設定ファイルに設定した上限値は、グローバル設定に優先されます。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： .ini ファイルを変更してカスタマイズする際は、注意してください。必要に応じて、サポート担当者にお問い合わせください。

ポリシーサービス

パフォーマンスを高め、ルールの検索を効率的に実行するために、InterScan MSS はポリシーサービスのメモリ内キャッシュを使用して、メッセージングルールを格納します。ポリシーサービスは、ルールをキャッシュに格納することで、検索サービスに対するルールのリモートストアとして機能します。これにより、データベースを検索する必要もなくなり、関連するネットワークやディスク I/O のオーバーヘッドも排除できます。また、このメカニズムによって検索サービスの効率もアップするため、ほとんどのメッセージ検索タスクを、ディスクを使用せずに検索サービスのメモリで実行することができます。

ポリシーの同期

InterScan MSS 管理データベースのスキーマには、バージョニングメカニズムが含まれています。ポリシーサービスは、データベースのバージョンを定期的にチェックします。データベース内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。これにより、キャッシュ内のデータベースのバージョンとデータベースとの同期がとれ、データベース全体に対して新規のエントリまたは変更されたエントリをチェックする必要がなくなります。

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

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

負荷分散を支援するために、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することができます。これを「セカンダリサービス」と呼びます。インストールした 1 台目のエンドユーザメール隔離サービスは、「プライマリサービス」と呼ばれ、Apache を実行してセカンダリサービスと連動します。

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 HTTPS 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 HTTPS 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 ソフトウェアは、{IMSS}/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、{IMSS}/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、{IMSS}/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、{IMSS}/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 ({IMSS}/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 ({IMSS}/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 ({IMSS}/UI/tomcat/sslkey/.keystore) など、さまざまな設定が定義されています。

{IMSS}/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)。

つまり、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アプリケーションは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、{IMSS}/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 {IMSS}/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、{IMSS}/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「デバッグ」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のデータベース

エンドユーザメール隔離データベースには、隔離されたスパムメールの情報、およびエンドユーザの承認済み送信者リストが格納されます。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は、エンドユーザメール隔離データベース (拡張性を求める場合は複数のデータベース) もインストールする必要があります。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、オプションの IP フィルタも搭載されています。これは、次の 2 つの機能で構成されます。

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

IP プロファイラは、次の 4 つの潜在的なインターネット脅威をすべて検出します。

- スパムメール - 不要な広告的な内容が含まれるメール。
- 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。
- ディレクトリハーベスト攻撃 (DHA) - 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。
- バウンスメール - メールサーバを使用して、差出人フィールドにターゲットのメールドメインを挿入したメールメッセージを生成する攻撃。生成されたメールメッセージは偽アドレスに送信された後、ターゲットのメールサーバに戻されます。これにより、メールサーバを氾濫させます。

- NRS - 既知のスパムメール送信者からのメールを IP レベルでブロックします。

Trend Micro Network Reputation Services

NRS は、接続要求のあったインターネットプロトコル (IP) アドレスを Trend Micro Threat Protection Network にルーティングして、大規模な評価データベースで検証することで、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ように設計されています。

Trend Micro Network Reputation Services の種類

NRS では、次の 2 種類のサービスが用意されています。

- Trend Micro RBL+ Service - IP アドレスを企業の最も総合的で信頼できる評価データベースで検証して、スパムメールをメールソースでブロックします。メールメッセージを不明なホストから受信した場合には必ず、指定したメールサーバから RBL+ データベースサーバに対して DNS クエリが実行されます。そのホストが RBL+ データベースにリストされている場合、接続を拒否してその送信者からのスパムメールをブロックできます。

- Trend Micro Network Anti-Spam Service - 膨大な量のスパムメールの送信が処理されている際に、メールソースを特定して送信プロセスを停止する、動的なリアルタイムソリューションです。Network Anti-Spam Service は、RBL+ サービス同様、DNS クエリベースのサービスです。このサービスの中心になるのが、RBL+ データベースと、動的リアルタイムデータベースである QIL データベースです。これら 2 つのデータベースには個別のエントリがあり、IP アドレスの重複はありません。これにより、ゾンビ、BGP 攻撃など、スパムメールの高度な動的ソースに素早く対応できる、効率の高いデータベースを保持できます。

IP プロファイラの機能

IP プロファイラは、42 ページの「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 でいつ IP アドレスに指定の処理を開始するかは、いくつかの条件をカスタマイズすることで指定できます。条件は潜在的な脅威に応じて異なりますが、InterScan MSS が IP アドレスとしきい値を監視する期間はいずれも共通です。

この機能を果たすために、IP プロファイラは複数のコンポーネントを利用します。最も重要なコンポーネントは、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、Foxproxy です。

次のプロセスは、InterScan MSS が、送信側メールサーバから接続要求を受信した後に実行されます。

1. Foxproxy が IP プロファイラの DNS サーバに問い合わせを行い、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、接続要求は拒否されます。

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

Trend Micro Network Reputation Service の機能

NRS は、ドメインネームサービス (DNS) のクエリベースのサービスです。次のプロセスは、InterScan MSS が、送信側メールサーバから接続要求を受信した後に実行されます。

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

図 2-1. は、NRS の機能を図示しています。

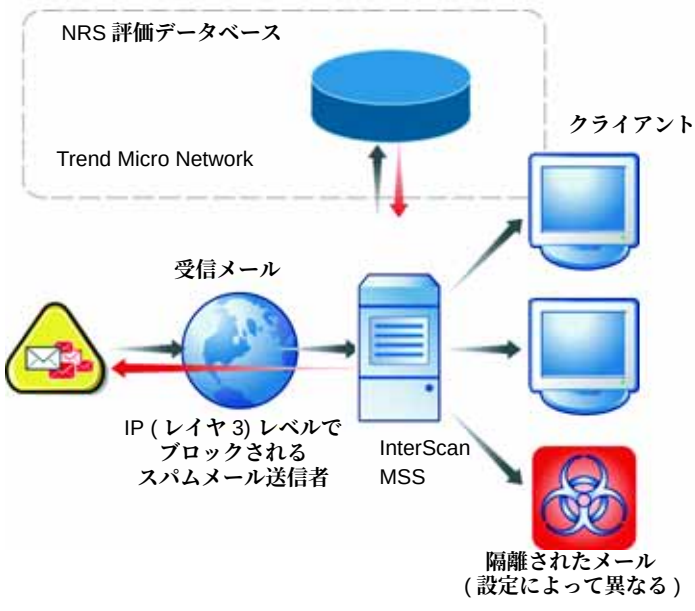


図 2-1. NRS の機能

NRS の操作の詳細については、次のサイトを参照してください。

http://jp.trendmicro.com/jp/products/enterprise/ers/ersa/index.html

第 3 章

配置計画

この章では、Trend Micro InterScan Messaging Security Suite (以下、InterScan MSS) の配置計画の手順について説明します。

この章の内容は次のとおりです。

- 48 ページの「配置チェックリスト」
- 52 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」
- 55 ページの「InterScan MSS で使用されるポート」
- 58 ページの「ネットワークトポロジの検討」
- 64 ページの「運用モデルについて」
- 70 ページの「インストールシナリオの理解」
- 85 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 配置のためのインストールの前後のタスクに関する手順を段階的に示します。

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		58 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		59 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		60 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		61 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		62 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		70 ページの「集中インストール」

チェックマーク （完了時）	タスク	オプション	参照
	・複数の検索サービス		72 ページの「複数の検索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		74 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		78 ページの「複雑な分散インストール」
	・広域ネットワーク		80 ページの「WAN へのインストール」
	注意：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。		84 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前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		88 ページの「MTA の準備」
	・InterScan MSS コンポーネントのインストール		101 ページの「インストール手順」
	・IP フィルタのインストール	あり	106 ページの「IP フィルタのインストール」
	・前バージョンからのアップグレード		113 ページの「体験版からの移行」
	・正常なインストールの確認		

チェックマーク (完了時)	タスク	オプション	参照
	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。		
	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 6 — 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「InterScan MSS 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

チェックマーク （完了時）	タスク	オプション	参照
	・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 7 — 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。		
	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、追加のサブモジュールも自動的にインストールされます。表 3-1 には、各コンポーネントのサブモジュールが示されています。

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な設定が保存されたメインの InterScan MSS 管理データベース。
	データベースサーバ *	InterScan MSS 管理データベースを実行するサーバ。
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 3-1. 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
検索サービス	検索サービス	すべてのメール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です。ルールをキャッシュに格納するので、データベースを検索する必要もなくなります。
	Control Manager エージェント	Trend Micro Control Manager (以下、Control Manager) が InterScan MSS を管理するのに必要なソフトウェアコンポーネント。
	IMSSMGR	検索サービスの処理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の Web サーバです。これによって、ユーザはスパムメールとして InterScan MSS が隔離し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に、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使用して、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の処理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	InterScan MSS がスパムメールとして隔離し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を実行するサーバ。

表 3-1. 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
IP プロファイラ	FoxProxy	FoxDNS でブロックリストをチェックして、メール要求を拒否するかまたは承認するかを確認する 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 アドレスを取得して、その IP アドレスを Postfix へ渡す IP フィルタモジュール。
Trend Micro Network Reputation Services (以下、NRS)	メールログパーサ	NRS 関連のメールログを解析するモジュール。
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。		

表 3-1. 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 で使用されるポート

InterScan MSS で使用されるポートについては、表 3-2 を参照してください。

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、すべての POP3 サーバに対して 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 UI Web サーバ (Tomcat) 管理ポート。	{IMSS}/UI/adminUI/conf/server.xml: Server / port
8009	エンドユーザメール隔離コンソール 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。	{IMSS}/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。	{IMSS}/UI/euqUI/conf/server.xml: Server/port

表 3-2.　IMSS ポート

ポート番号	コンポーネントと役割	設定の保存先
8445	Admin UI 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、このポートを開放する必要があります。	Tomcat listen port: {IMSS}/UI/adminUI/conf/server.xml: Server / Service / Connector / port
8446	EUQ service listening port.	{IMSS}/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。	{IMSS}/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、このポートに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。このポートに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。 このポートに送信されたすべてのメッセージは、InterScan MSS によって検索されません。セキュリティ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 3-2.　IMSS ポート

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。このポートを変更しないでください。	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。このポートを変更しないでください。	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。		

表 3-2. IMSS ポート

ネットワークトポロジの検討

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を図で示します。

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。

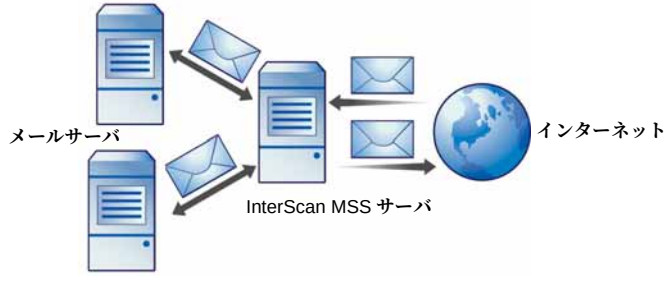


図 3-1. インストールトポロジ : ファイアウォールなし

ファイアウォールの外側へのインストール

図 3-2. は、ファイアウォールの外側に InterScan MSS を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。

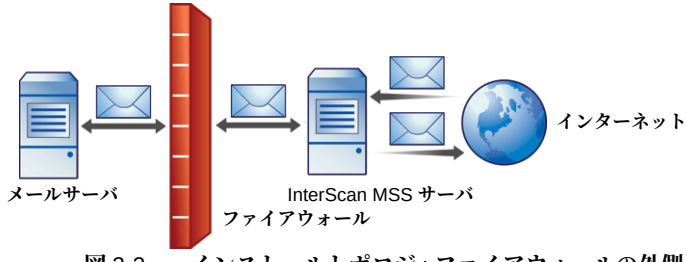


図 3-2. インストールトポロジ : ファイアウォールの外側

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。したがって、SMTP サーバが参照されるように InterScan MSS を設定するか、または 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ます。
- ローカルドメインのリレーのみが許可されるようにリレードメインを設定します

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 に転送される。
  - 受信 SMTP メールは Postfix 経由でのみ InterScan MSS 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、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、ファイアウォールの内側に InterScan MSS および Postfix を配置する方法を示しています。

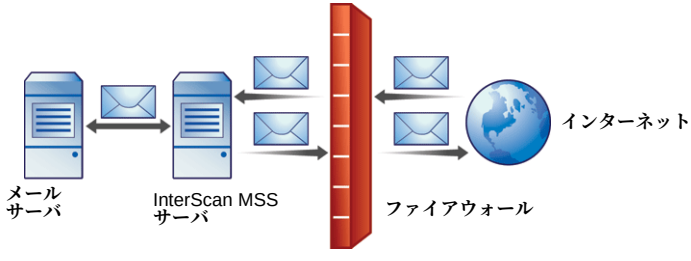


図 3-3. インストールシナリオ : ファイアウォールの内側

受信トラフィック

- 次のルーティングが可能になるように、プロキシベースのファイアウォールを設定します。
  - 送信 SMTP メールが Postfix 経由で InterScan MSS に転送される。
  - 受信 SMTP メールが Postfix 経由で InterScan MSS に転送され、そこからドメイン内の SMTP サーバに転送される。
- 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、InterScan MSS を設定します。
- ローカルドメインへのリレーのみが許可されるよう、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 に送信されるよう、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 に送信されるよう、内部メールサーバを設定します。
- すべての送信メール (ローカル以外のドメイン宛てのもの) がファイアウォールに転送されるか、または直接配信されるよう、Postfix および InterScan MSS を設定します。
- 内部 SMTP ゲートウェイで InterScan MSS を使用したすべてのドメインへのリレーが許可されるよう、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

これまで SMTP ゲートウェイをホストしていたサーバと同じサーバに、InterScan MSS および Postfix もインストールできます。

SMTP ゲートウェイ

- 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。これには、他のサービスで使用されていないポートを割り当てる必要があります。
- 新しく割り当てたポートがバインドされるように 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、InterScan MSS を設定します。

送信トラフィック

- 送信メールが InterScan MSS サーバのポート 25 に転送されるよう、SMTP ゲートウェイを設定します。
- すべての送信メール (ローカル以外のドメイン宛てのメッセージ) がファイアウォールに転送されるか、または直接配信されるよう、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 にインストールすることもできます。

受信トラフィック

- プロキシベースのファイアウォールを設定して、受信および送信 SMTP メールが 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、Postfix および InterScan MSS を設定します。

送信トラフィック

- すべての送信メール (ローカルドメイン以外に宛てられたもの) がファイアウォールに転送されるか、または InterScan MSS を使用して直接配信されるよう、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、すべての内部 SMTP ゲートウェイを設定します。

- 内部 SMTP ゲートウェイですべてのドメインへの Postfix および InterScan MSS 経由のリレーが許可されるよう、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。
- **プロキシモデル** — InterScan MSS を、アップストリームメールサーバとダウンストリームメールサーバの間に配置します。

注意： プロキシモデルでは、InterScan MSS を連携する MTA が配置されていないイントラネットのエッジに配置します。このモデルでは、IP フィルタ機能 (IP プロファイラと NRS) はサポートされません。

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。

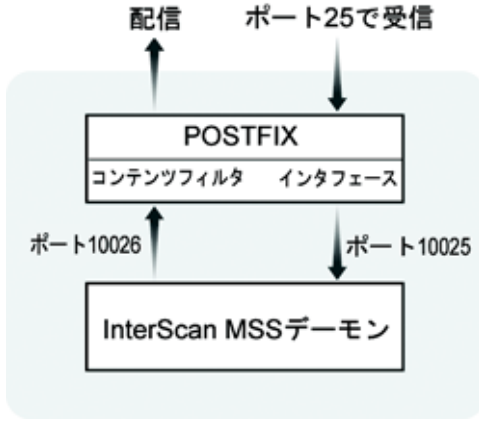


図 3-4. スタンドアロンモデル

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.imss70

-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。

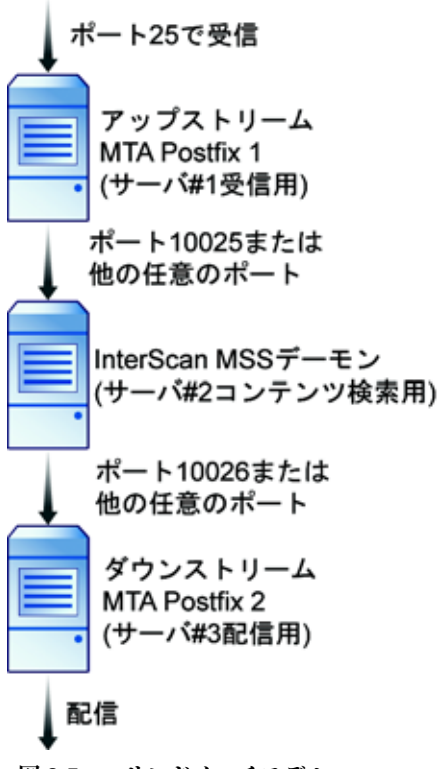


図 3-5.　サンドイッチモデル

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。ただし、このタイプの構成を使用すると、ネットワーク負荷が増加します。

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

ここでは、Postfix を MTA として使用する場合の設定を示します。

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

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

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

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

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

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

プロキシモデル

このモデルでは、InterScan MSS がアップストリームメールサーバとダウンストリームメールサーバの間に位置し、MTA はネットワーク上の別の場所に配置されます。

図 3-6.　プロキシモデル

このモデルの最大の利点は、他のモデルより高いパフォーマンスとスループットです。ただし、このモデルでは、IP プロファイラや NRS は使用できません。これらの機能を使用するには、受信 IP アドレスが InterScan MSS に到達するまでの区間で変更されないようにする必要があるからです。

インストールシナリオの理解

InterScan MSS は、1 つのサーバにすべてのコンポーネントをインストールする集中インストール、または複数のサーバに分けてコンポーネントをインストールする分散インストールのいずれにも対応します。次の情報を参照し、適切なシナリオを選択してください。

集中インストール

集中インストールには、集中インストールの要件を満たす 1 台のサーバが必要です。InterScan MSS の集中インストールの場合、平均約 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。

単一サーバ上に、次に示す InterScan MSS コンポーネントをすべて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 3-7. 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。

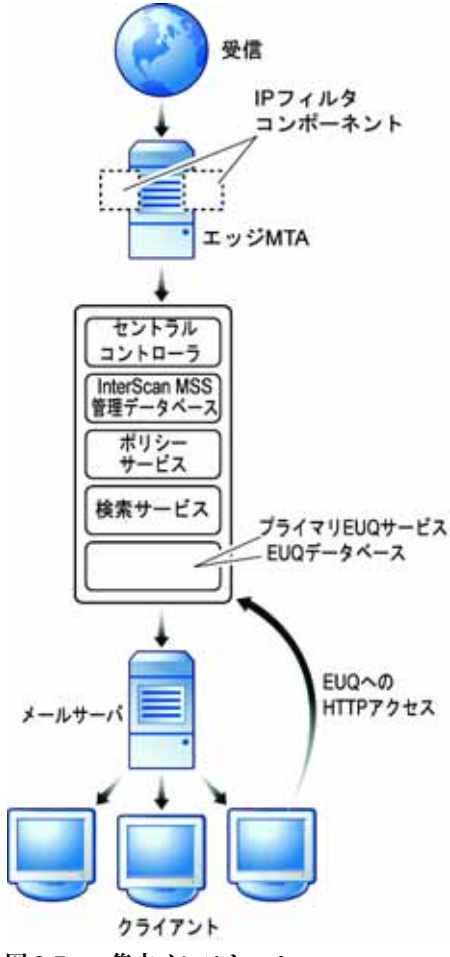


図 3-7.　集中インストール

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サービスをインストールします (100 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 (106 ページの「IP フィルタのインストール」を参照)。

複数の検索サービスのインストール

大規模企業の場合、単一サーバでは十分なメッセージスループット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することができます。検索サービスは、InterScan MSS 管理データベースを共有します。また、スパムメールの隔離アイテムをエンドユーザメール隔離で管理できるよう、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可能です。

複数の InterScan MSS 検索サービスをインストールすると、大量のメッセージングトラフィックを処理できます。

- 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と検索サービスの組み合わせをインストール後に追加します。

図 3-8. は、InterScan MSS の単一サーバのインストールに、複数の検索サービスを追加した構成が、標準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される必要があります。

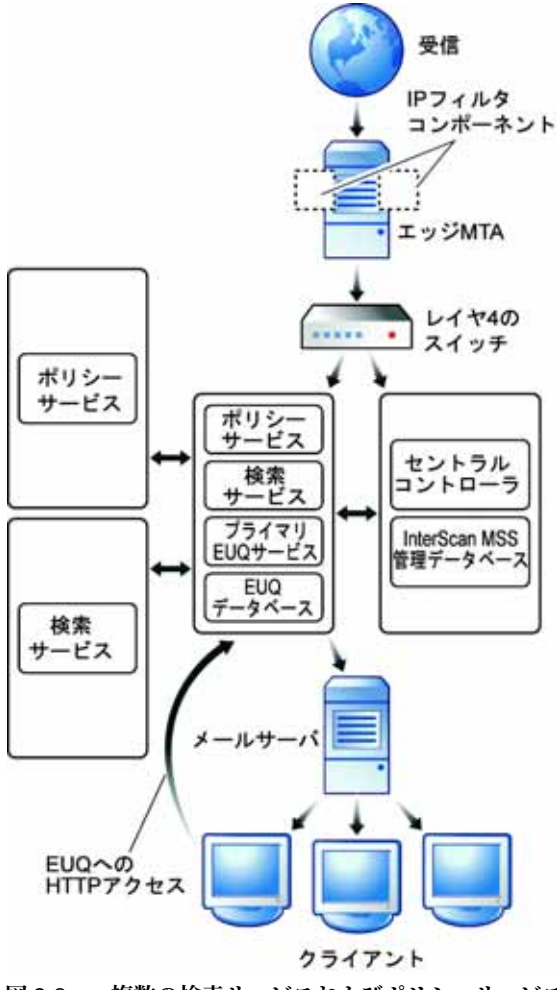


図 3-8.　複数の検索サービスおよびポリシーサービスのインストール

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 (100 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は、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 (106 ページの「IP フィルタのインストール」を参照)。

   注意： ポリシーサービスは、常に、検索サービスと共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の起動を選択できます。

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へ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 3-9. は、InterScan MSS の集中インストールに、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サービスを追加した構成が、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。

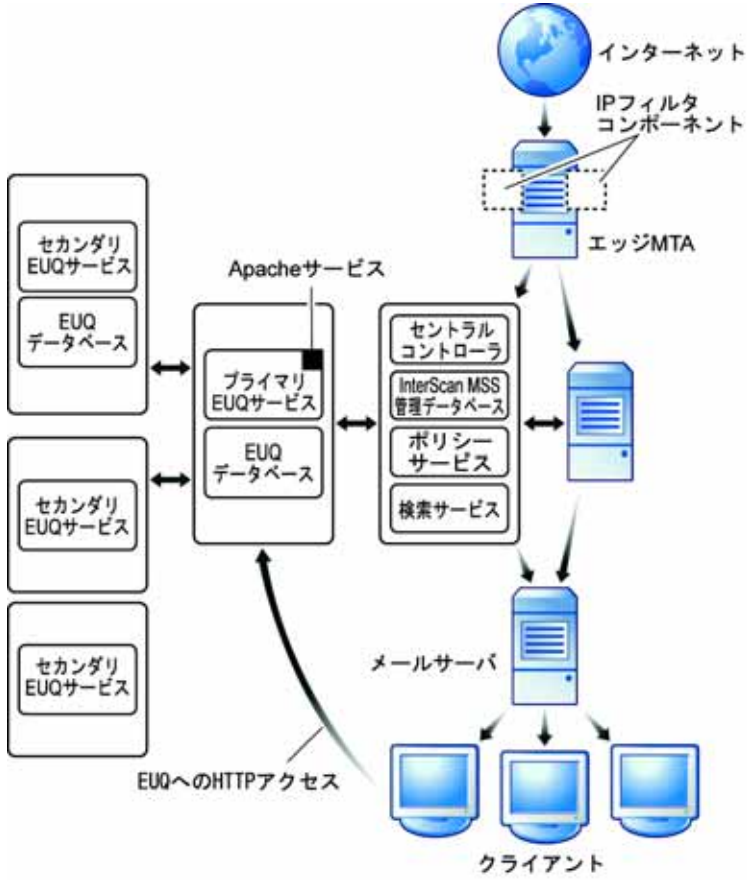


図 3-9.　複数のエンドユーザメール隔離サービスのインストール

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 (100 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： この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。もう 1 台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、このコンピュータでエンドユーザメール隔離関係のコンポーネントを選択しないでください。最初の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、プライマリエンドユーザメール隔離サービスに Apache サービスが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。さらにパフォーマンスを向上させるため、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できます。

   注意： エンドユーザメール隔離データベースを、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、同一のデータベースサーバ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することは許可されていません。

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 (106 ページの「IP フィルタのインストール」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」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およびデータベースは、最高 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の格納に使用する、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 HTTP 接続をブロックしない種類であるか、HTTP 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、100 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、分散インストールを選択することをお勧めします。このシナリオでは、コンポーネントごとにインストール要件を満たすサーバが必要です。分散インストールでは、InterScan MSS とエンドユーザメール隔離の各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、他の複数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、スパムメールの隔離アイテムをエンドユーザメール隔離で管理できるよう、複数の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可能です。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パフォーマンスを強化することもできます。

高スループットが求められる環境では、各 InterScan MSS コンポーネントを個別のコンピュータにインストールし、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 の管理データベースと混同しないようにしてください。一元化された InterScan MSS の配置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することはできますが、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 3-10. は、InterScan MSS と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 サービス付き) を一元化したインストールが、標準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、常に、検索サービスと共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の起動を選択できます。

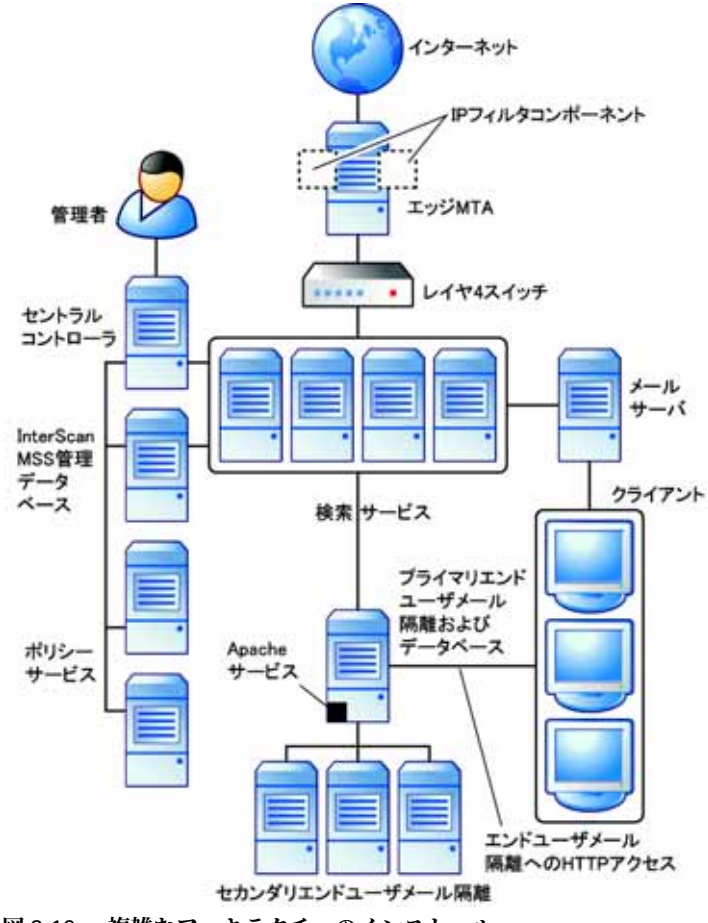


図 3-10. 複雑なアーキテクチャのインストール

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確保するために、各サイトには少なくとも 1 つ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ようお勧めします。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

次のシナリオには 2 つの Control Manager サーバがあり、それらはすべてのサイトを管理します。各 Control Manager サーバは、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することができます。

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

図 3-11. は、複数サイトの WAN での配置を示しています。

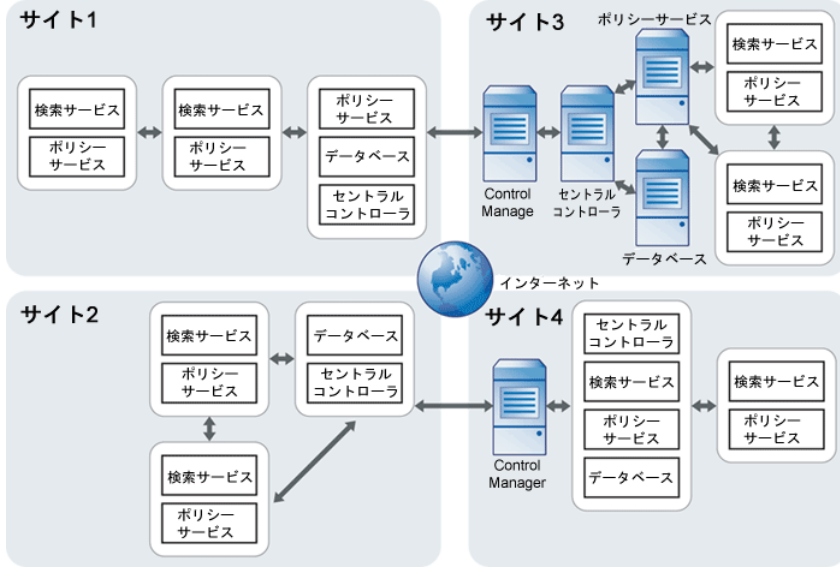


図 3-11.　WAN での配置

この配置の場合、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になっている 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になっている 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 + ポリシーサービスが有効になっている 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と 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になっている 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 つはポリシーサービスをインストールし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。検索サービスはポリシーサービスが機能停止になっても、別の有効なポリシーサービスを使用することができます。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切断されたりしても、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メールの処理を続行します。図 3-12 を参照してください。

各サイトには、専用セントラルコントローラとデータベースサーバがあり、それらはすべて 2 つの Contol Manager サーバにレポートを返しています。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。1 つの InterScan MSS 管理データベースが壊れて動作しなくなっても、複製を使用して復元できます。Control Manager サーバは、サーバ間で InterScan MSS 管理データベース情報を複製できません。

注意： Control Manager サーバは、サーバ間で InterScan MSS 管理データベース情報を複製できません。

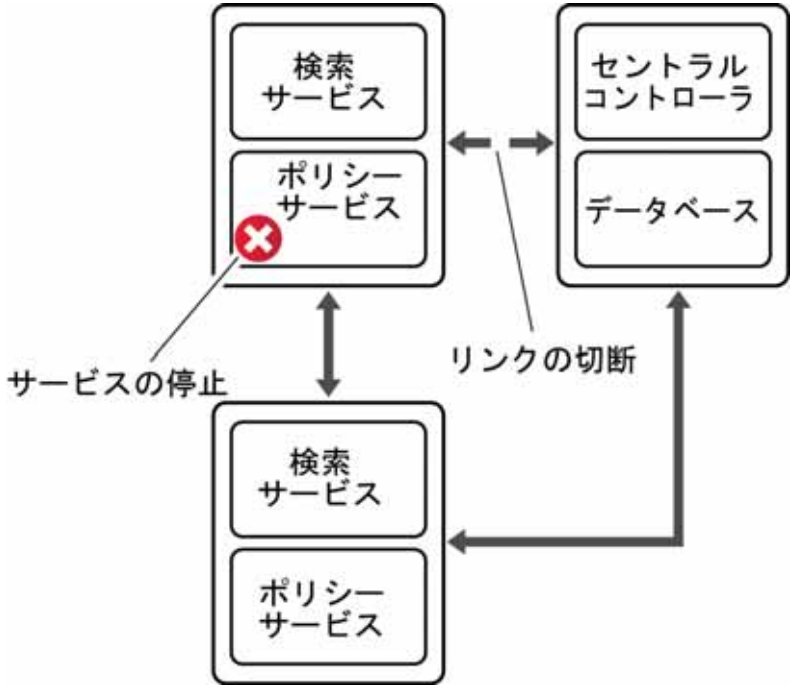


図 3-12.　フェイルオーバー

IP フィルタ

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。

IP フィルタ機能を付加した InterScan MSS の配置

IP フィルタ、すなわち IP プロファイラと NRS は、どちらも 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。NRS 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定します。

注意： ネットワークエッジから InterScan MSS 接続までの区間でアドレスが変更されない必要があります。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、または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、このアドレスがすべての受信メッセージのアドレスと同じになり、IP フィルタが、SMTP セッションの開始者が既知のスパムメール送信者であるかどうかを判断できなくなるためです。

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」および管理者ガイドの「IP フィルタサービス」を参照してください。

フェイルオーバーについて

表 3-1 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 InterScanMSS 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 配置のフェイルオーバーに関する詳細については、82 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。

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、72 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。
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、72 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。 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。	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。

表 3-3.　フェイルオーバーのシナリオ

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
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。 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。	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。
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インする際、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 エントリ (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] を選択します。 2. [LDAP] タブをクリックします。 3. [有効]、[LDAP2] 横のチェックボックスをオンにし、必要な情報を入力します。 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もお勧めします。

表 3-3. フェイルオーバーのシナリオ

第 4 章

インストールとアップグレード

この章では、さまざまな状況で Trend Micro InterScan Messaging Security Suite (以下、InterScan MSS) のインストールを行う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。

- 88 ページの「MTA の準備」
- 100 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」
- 106 ページの「IP フィルタのインストール」
- 113 ページの「体験版からの移行」
- 116 ページの「バージョン 5.1x からバージョン 7.0 への移行」
- 126 ページの「移行のロールバック」
- 128 ページの「アンインストールの実行」

MTA の準備

InterScan MSS は、Postfix、sendmail、および qmail の 3 種類の MTA をサポートしています。この項では、InterScan MSS コンポーネントをインストールする前に、InterScan MSS と共に使用できるように MTA を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、この項の説明に従って Postfix を設定してください。この手順は、Linux および Solaris の両プラットフォームに適用できます。

注意： 1. InterScan MSS 7.0 Linux: InterScan MSS サーバのインストールでは、MTA はインストールされません。あらかじめ MTA をインストールし、運用可能な状態にしておく必要があります。InterScan MSS をインストールするコンピュータに Postfix がインストールされている場合は、Postfix の設定が正しいことを確認してください。
トレンドマイクロでは、Linux バージョンで配布されている Postfix をインストールして使用することを強くお勧めしています。詳細については、www.postfix.org を参照してください。

2. InterScan MSS 7.0 Solaris: インストール先コンピュータに MTA が存在しない場合、インストーラは、InterScan MSS サーバのインストール中に Postfix をインストールすることができます。既に MTA がインストールされ、動作可能になっている場合は、MTA の設定が正しいことを確認してください。

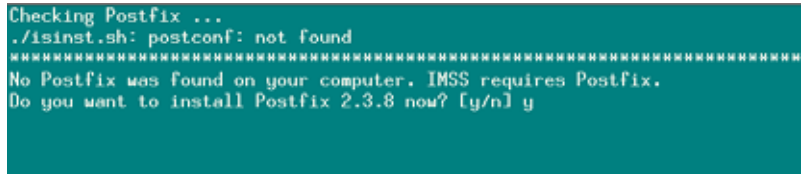
InterScan MSS 7.0 Solaris での Postfix のインストール

次の手順は、インストール先コンピュータに既存の Postfix が存在しない場合に、InterScan MSS サーバのインストール中に Postfix をインストールする方法を示しています。

1. 「**./isinst.sh**」と入力して、InterScan MSS をインストールします。InterScan MSS コンポーネントのインストールの詳細については、101 ページの「インストール手順」を参照してください。

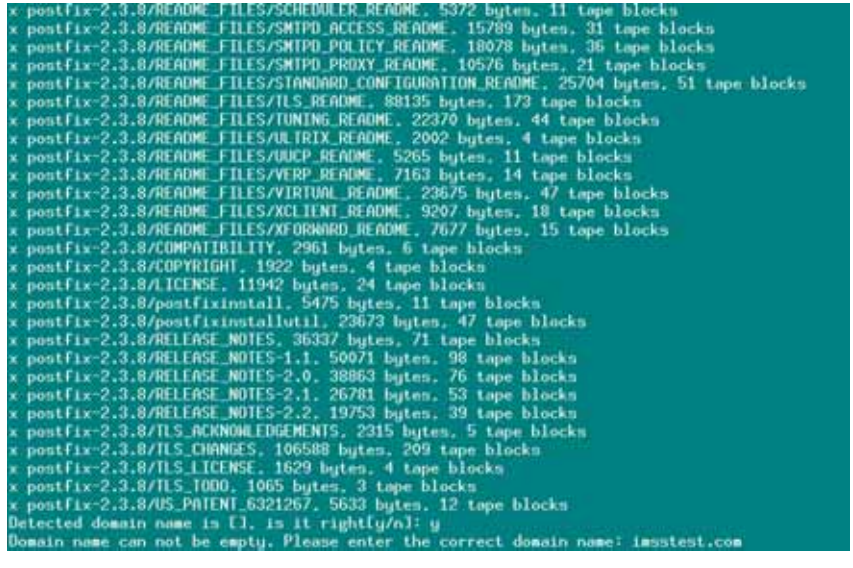
   インストールの開始に必要なオプションの選択後、インストーラにより、使用可能な空きディスク領域、メモリ、スワップ領域、および BIND サーバがチェックされます。インストール先コンピュータで Postfix が検出されなかった場合、Postfix をインストールするかどうかをたずねるメッセージが表示されます。

2. 「**Y**」と入力して、Postfix 2.3.8 をインストールします。



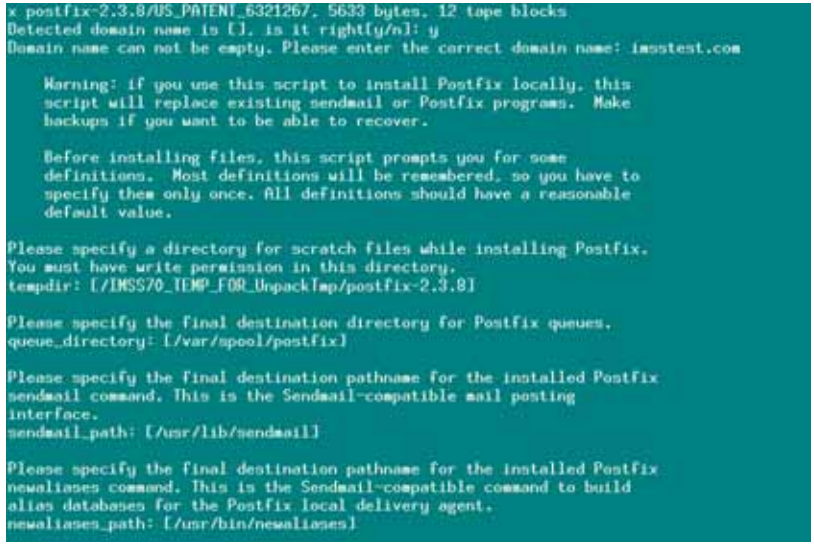
3. インストール先コンピュータで既存のドメイン名がチェックされます。検出されたドメイン名が Null であった場合、正しいドメイン名の入力を求めるプロンプトが表示されます。

   有効なドメイン名を入力し、**<Enter>** キーを押します。

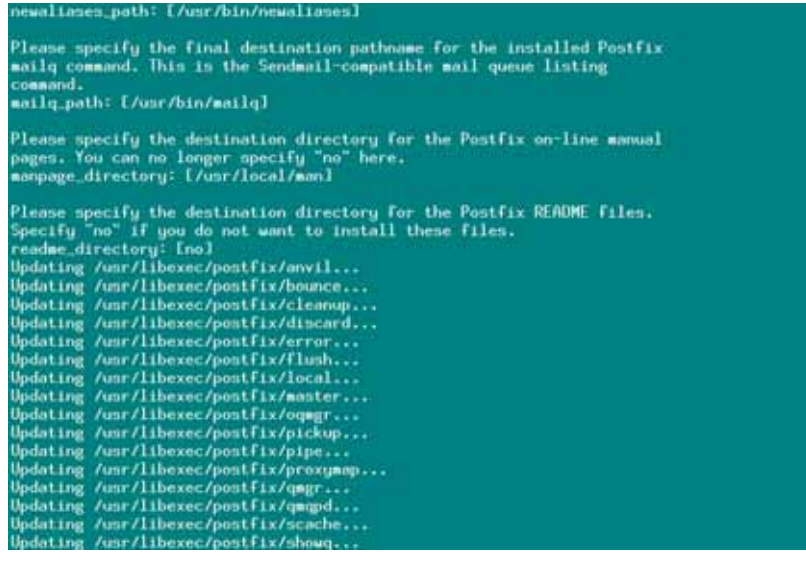


4. Postfix ファイルのインストール前に、定義の入力を求めるプロンプトが表示されます。必要に応じて、各種ファイルへのパスを入力します。

ヒント： トレンドマイクロでは、初期設定されているパスをそのまま使用することをお勧めします。

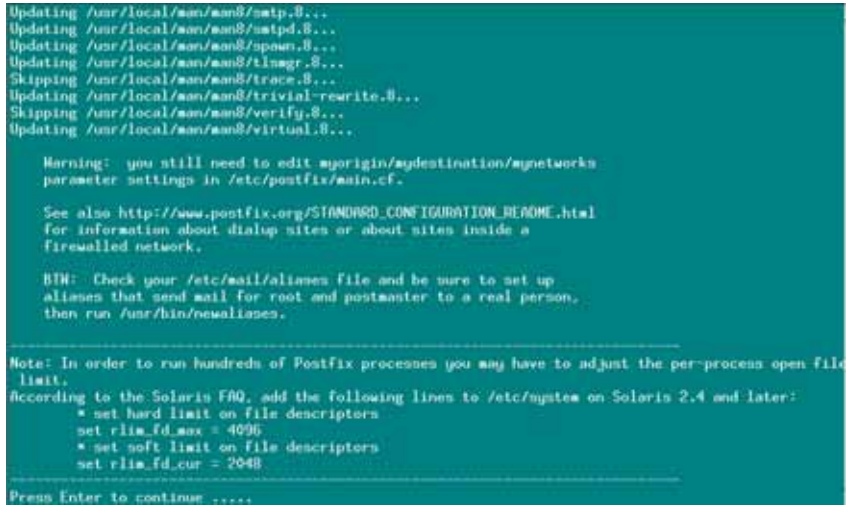


5. 必要なパスの指定後、Postfix のインストールが開始されます。



6. Postfix のインストール後、あとで Postfix を設定するよう伝えるメッセージが表示されます。Postfix の設定方法の詳細については、92 ページの「/etc/postfix/main.cf で次の設定を挿入または変更」および 93 ページの「/etc/postfix/master.cf で次の設定を挿入」を参照してください。

   <Enter> キーを押して、InterScan MSS コンポーネントのインストールを続けます。



/etc/postfix/main.cf で次の設定を挿入または変更

```
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=20
```

/etc/postfix/master.cf で次の設定を挿入

```
#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.imss70
  -o smtpd_client_restrictions=
```

sendmail の使用

このセクションでは、InterScan MSS と共に sendmail を使用するための設定方法について説明します。

sendmail のデーモン

次の図は、同じサーバ上で InterScan MSS と 2 つの sendmail デーモンが動作している場合を示したものです。

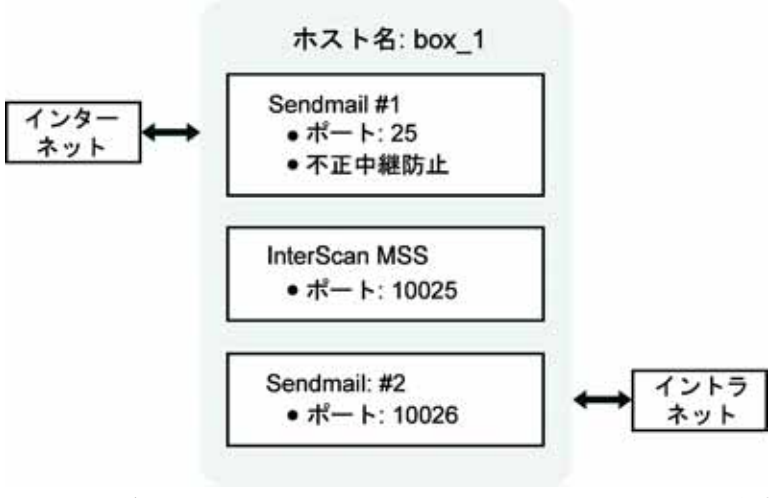


図 4-1.　1 台のサーバに InterScan MSS と 2 つの sendmail デーモンを設定

ポート 10025 と 10026 は、任意のポート番号です。次に示す設定を実行する場合は、10025 および 10026 を任意の空きポート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 と呼ばれる sendmail.cf ファイルをコピーします。
2. sendmail.cf 内の 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。この 10025 は、box_1 の任意の空きポートです。

3. sendmail.cf 内の Msmtp、Mesmtp、Msmtp8、および Mrelay の「F」オプションに「k」フラグを追加します。

   この例のとおりに実行すると、Msmtp 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. ローカルのメールソフトを、sendmail.cf 内の Mlocal の[IPC]で置き換えます。

5. sendmail.cf 内の A オプションを Mlocal の「TCP localhost.your_domain_name 10025」に変更します。

6. sendmail.cf 内の Mlocal の「F」オプションに「k」フラグを追加します。

   Mlocal に対する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

#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 内で、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、元の /var/spool/mqueue と同じ所有者および権限が設定されていることを確認します。

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

   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 1 つ目の sendmail デーモンを再起動し、ポート 25 上の SMTP トラフィックを処理します。

   ```
   /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、InterScanMSS 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。

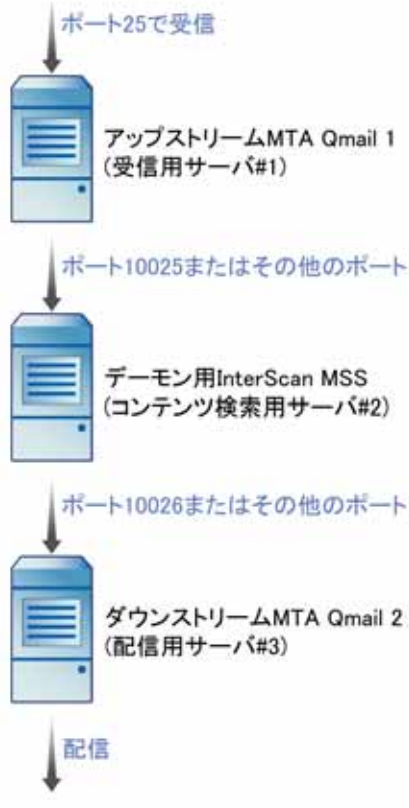


図 4-2.　InterScan MSS による Qmail の配置

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。

注意： Qmail を MTA として使用する場合、InterScan MSS を配置できるのはサンドイッチモデルまたはプロキシモデルを使用した場合のみです。

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に、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 ":[server name/IP:port]" > /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

この項では、Solaris システムファイルの設定方法、および 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手順について説明します。

Solaris システムファイルの設定

InterScan MSS 7.0 Solaris では、Solaris バージョン 8 および 9 へのインストール前にシステム IPC チェックが実行されます。Solaris の IPC の設定値が小さすぎる場合、プロンプトが表示されます。メモリの問題が発生した場合は、システムファイルで次の IPC 値を設定し、システムを再起動してから、インストールを続けます。

/etc/system で次の設定を挿入

```
set shmsys:shminfo_shmmax=0x2000000
set shmsys:shminfo_shmmin=1
set shmsys:shminfo_shmmni=256
set shmsys:shminfo_shmseg=256

set semsys:seminfo_semmap=256
set semsys:seminfo_semmni=512
set semsys:seminfo_semmns=512
set semsys:seminfo_semmsl=50
set semsys:seminfo_semopm=30
set semsys:seminfo_semmnu=100
```

注意： Solaris 8 および Solaris 9 でのみ、Solaris システムファイルに上記の変更を行う必要があります。Solaris 10 では必要ありません。

インストール手順

ここでは、InterScan MSS およびエンドユーザメール隔離のインストールに必要な主な手順を説明します。

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] に、各コンポーネントのステータスが表示されます。はじめて InterScan MSS をインストールする場合は、[Not Installed] と表示されます。

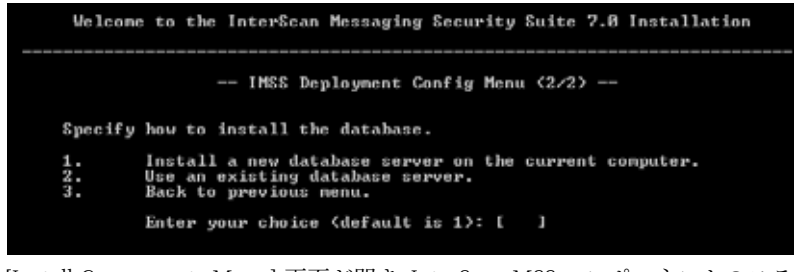
3. 「1」を入力してインストールを開始します。

4. 使用許諾契約書を読み、同意します。

5. [IMSS Deployment Config Menu] で、新しい InterScan MSS サーバをインストールするか、または既存のインストールにコンポーネントを追加するかを選択します。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。

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。
- インストールの追加を選択した場合は、データベース情報を入力します。



[Install Components Menu] 画面が開き、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は [YES] と表示されます。初期設定では、セントラルコントローラおよび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。

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も変更できます。初期設定は /opt/trend です。

   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は、現在のコンピュータにエンドユーザメール隔離サービスが存在しているかどうか、また、存在している場合は、それがプライマリサービスかセカンダリサービスかが確認されます。エンドユーザメール隔離サービスが存在していない場合、または既存のサービスがセカンダリサービスの場合は、プライマリサービスがインストールされます。プライマリサービスの負荷分散はセカンダリサービスによって補助されます。

   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は、新しいデータベースサーバをインストールすることも、既存のデータベースサーバを使用することもできます。どちらかを選択し、使用するデータベースサーバの情報を入力します。

8. 「6」と入力して処理を続行します。

   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した場合は、Postfix サーバの必要な設定が表示されます。これらの設定の概要については、88 ページの「Postfix の準備」を参照してください。

注意： 1. インストール先コンピュータに Postfix が存在しない場合、インストーラは、Postfix をインストールすることができます。ただし、インストール後に Postfix を設定する必要があります。88 ページの「Postfix の準備」を参照してください。

2. 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 9.4.0 をインストールします。

---

9. <Enter> キーを押して処理を続行します。コンピュータで DNS サーバが起動されているかどうかを示す注意書きが表示されます。IP プロファイラを使用する場合は、DNS サーバが起動し、正しく実行されている必要があります。なお、IP プロファイラは後からインストールできます。IP プロファイラのインストール手順については、106 ページの「IP フィルタのインストール」を参照してください。

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 フィルタのインストール

IP フィルタは、次の 2 つのコンポーネントで構成されます。

- 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。
- Trend Micro Network Reputation Services (以下、NRS) - ネットワーク (IP) レベルで既知のスパムメール送信元メールサーバからメールをブロックします。

IP プロファイラと NRS のインストール

NRS は、変更された Postfix 上で動作します。NRS インストールスクリプトを実行すると、Postfix の設定ファイルが変更され、IP フィルタレポート機能を実行するためのログパーサがインストールされます。このインストールでは、NRS のアクティベーションコードと、InterScan MSS の管理データベースに関する情報を入力するよう要求されます。NRS および IP プロファイラをインストールするには、事前にデータベースをインストールしておく必要があります。

NRS をインストールするサーバには、Postfix がインストールされている必要があります。また、NRS をインストールするサーバは、InterScan MSS 管理データベース、およびメッセージングを処理するサーバ (通常は InterScan MSS サーバ) に接続できる必要があります。NRS および IP プロファイラは、ゲートウェイまたはエッジサーバ上で実行することをお勧めします。

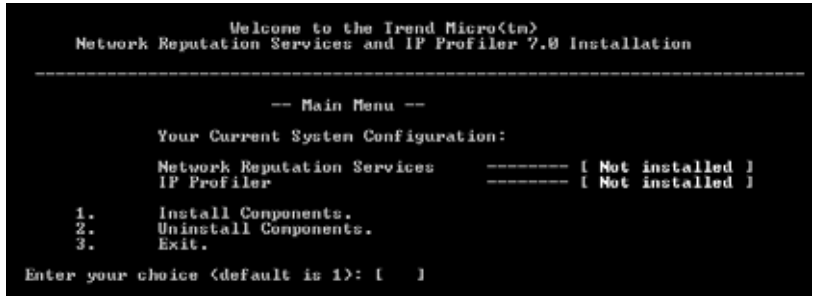
注意： NRS はインストール時にアクティベートする必要があります。後から管理コンソールでアクティベートすることはできません。

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取得している場合は、同じアクティベーションコードを使用して NRS をアクティベートできます。

IP プロファイラおよび NRS 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。

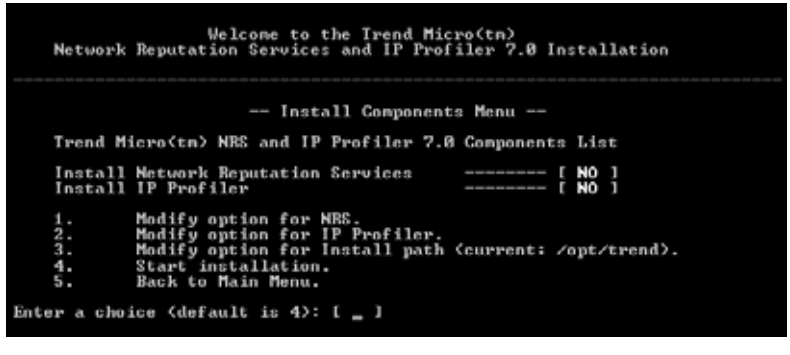
2. 「**./ipfilterinst.sh**」と入力します。[Main Menu] に、IP プロファイラおよび NRS のステータスが表示されます。はじめてこれらの製品をインストールする場合は、[Not Installed] と表示されます。



3. 「1」を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み、同意します。

   [Installation List] 画面が開き、この 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は [YES] と表示されます。初期設定では、IP プロファイラと NRS 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 NRS のインストールを指定します。

   NRS をインストールするには

a. 「1」と入力します。[NRS Config Menu] 画面が表示されます。

b. NRS を現在のコンピュータにインストールするかどうかを決定します。

c. NRS のアクティベーションコードを入力します。インストールを実行することによって Postfix サーバがどのように変更されるかを示す注意書きが表示されます。

d. 変更を受け入れます。

e. メールログのパスを入力します。

インストールメニューが再び開き、[Install NRS] 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決定します。

c. IP プロファイラに使用するポートを入力します (初期設定は 25)。

ポート 25 が既に使用されている場合は、ポートに関する注意が表示されます。必要に応じてポート番号を変更するか、インストールが完了した後に Postfix の待機ポートを 2500 に変更します。

d. <Enter> キーを押して処理を続行します。

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、インストーラでは、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び開き、[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」を入力し、新しいディレクトリパスを入力します。初期設定は /opt/trend です。

7. 「4」を入力してインストールを開始します。

sendmail および qmail と InterScan MSS の統合

InterScan MSS では、Postfix を他の MTA で置き換えることができます。この項では、FoxProxy および NRS をサポートするように sendmail と qmail を設定する手順を説明します。

FoxLib と sendmail の統合

IP プロファイラを sendmail MTA と共に使用する場合は、以下の手順を実行して、sendmail で FoxLib が確実に使用されるようにして、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。

- 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

- sendmail に関する情報を収集します。
  - 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
  - ls コマンドを使用して、sendmail により使用されるユーザとグループを明らかにします。

    # ls -al /usr/sbin/sendmail

    -rwxr-sr-x 1 root root 732356 Sep 1 2004 /usr/sbin/sendmail

    (ユーザ、グループ共に root です)
  - 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、グループ ID 共に 0 です)
- /opt/trend/ipprofiler/script ディレクトリ内の foxlibd スクリプトを次のように変更します。
  - TM_FOX_UID パラメータにユーザ ID を設定します。

    TM_FOX_UID=0
  - TM_FOX_GID パラメータにグループ ID を設定します。

    TM_FOX_GID=0
  - 「export LD_LIBRARY_PATH」を含む行の後に、次の 2 行を追加します。

    TM_FOX_PROXY_CONNECT_PORT=2500

    export TM_FOX_PROXY_CONNECT_PORT

- /opt/trend/ipprofiler/config ディレクトリ内の foxproxy.ini 設定ファイルを次のように変更します。
    - has_foxlib_installed パラメータの値を「0」から「1」に変更します。
- sendmail を起動するため、sendmail スクリプトの代わりに foxlibd を使用します。

  /opt/trend/ipprofiler/script/foxlibd start/stop
- FoxProxy を再起動します。

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

FoxLib と qmail の統合

IP プロファイラを qmail MTA と共に使用する場合は、以下の手順を実行して、qmail で FoxLib が確実に使用されるようにして、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。

- qmail の起動スクリプトを変更します。
    - qmail を起動するためにデーモンツールをインストールした場合は、smtpd 起動スクリプトを /service/qmail-smtpd/run に保存しておく必要があります。
    - 実行ファイルを変更して、#!/bin/sh を含む行の後のファイルの先頭に、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
- qmail ユーザおよびグループを取得して、正しい .so ファイルをコピーします。
    - 次のコマンドを実行して、ユーザとグループをチェックします。

      #id qmaild

uid=101(qmaild) gid=100(nofiles)

- smtp ユーザは qmaild、グループは nofiles であることがわかります。
- .so ファイルを正しいパスにコピーして、属性を変更してから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

- /opt/trend/ipprofiler/config ディレクトリ内の foxproxy.ini 設定ファイルを次のように変更します。

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

- 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

- 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 &

  以前、qmail を起動したことがあり、システムの起動スクリプトに qmail が追加されている場合は、代わりにシステムをリブートします。

体験版からの移行

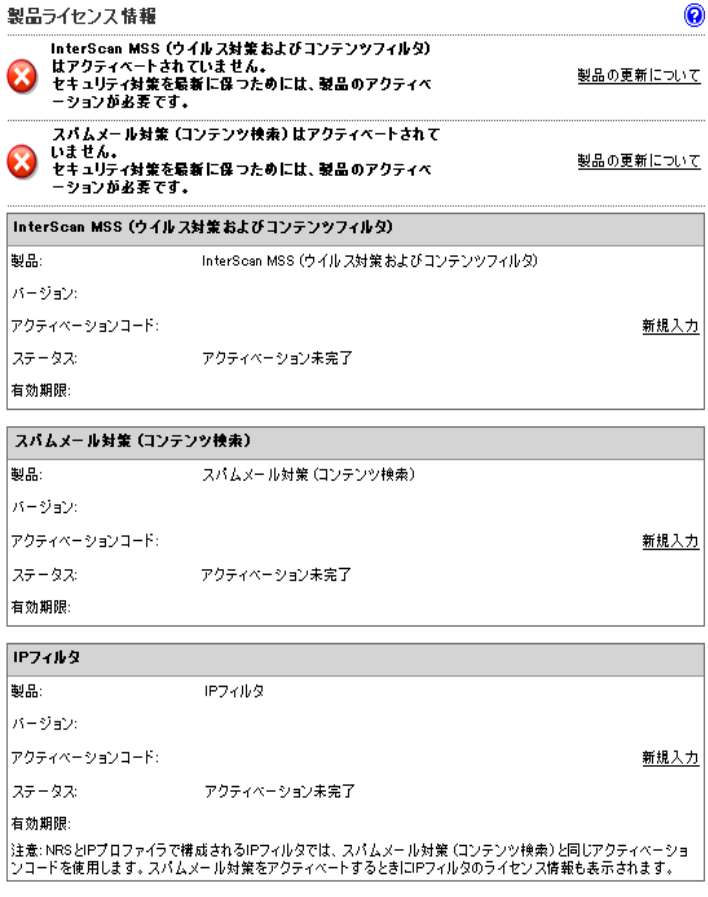
体験版アクティベーションコードを入力して InterScan MSS をアクティベートすると、製品のすべての機能を試すことができる体験版の使用期間が開始します。体験版の使用期間は、入力したアクティベーションコードの種類に応じて異なります。

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。

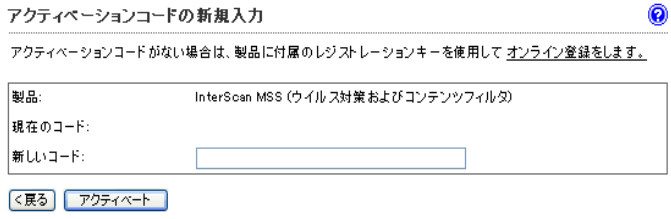
InterScan MSS を継続して使用するには、製品版を購入してください。その際に、新しいアクティベーションコードが提供されます。

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] の順に選択します。



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。
4. [アクティベート] をクリックします。

バージョン 5.1x からバージョン 7.0 への移行

InterScan MSS のインストールプログラムは、サポート対象プラットフォームにバージョン 5.1x の InterScan MSS が存在する場合、これを自動的にアップグレードします。このバージョンが検出されると、次の処理が実行されます。

- 前バージョンの InterScan MSS のアンインストール
- InterScan MSS 7.0 のインストール
- 既存の設定の移行

ヒント： 1. インストールプログラムにより、旧バージョンの InterScan MSS の設定がバックアップされますが、バージョン 5.1x の設定を手動でバックアップしてから移行を実行することをお勧めします (119 ページの「設定のバックアップ」を参照)。移行中に問題が発生した場合、バージョン 5.1x にロールバックできます (126 ページの「移行のロールバック」を参照)。

2. 旧バージョンの InterScan MSS 設定を移行しない場合は、既存の InterScan MSS に InterScan MSS 7.0 を上書きインストールするのではなく、InterScan MSS 5.1x を完全にアンインストールしてから新規インストールを実行することをお勧めします。

複数の検索サービス配置のアップグレードオプション

InterScan MSS 5.1x に複数の検索サービスをインストールしている場合、すべての検索サービスが共有する単一の管理データベースをインストールするか、InterScan MSS 7.0 の検索サービスごとに管理データベースをインストールするかによって、異なるアップグレードを実行する必要があります。

単一の管理データベース

すべての InterScan 検索サービスを InterScan MSS 7.0 内の単一の管理データベースにアクセスさせる場合、次の手順を実行して InterScan MSS 5.1x から移行します。

1. 最初の検索サービスの場合、InterScan MSS 7.0 インストーラを起動して移行インストールを実行します。
2. 以降の検索サービスの場合、InterScan MSS 5.1x インストーラを起動して既存の InterScan MSS をアンインストールしてから、InterScan MSS 7.0 インストーラを起動して追加インストールを選択します。

注意： 単一の管理データベースのアップグレードオプションには、次のような特性があります。
1. InterScan MSS は 1 つしかありません。
2. すべての検索サービスを一元的に制御できます。
3. すべての検索サービスで同一の設定を共有する場合のみ、このアップグレードオプションを選択します。
4. 検索サービスごとに異なる設定を行った場合、このアップグレードオプションを選択しても、InterScan MSS では最初の検索サービスの設定のみ保持されます。

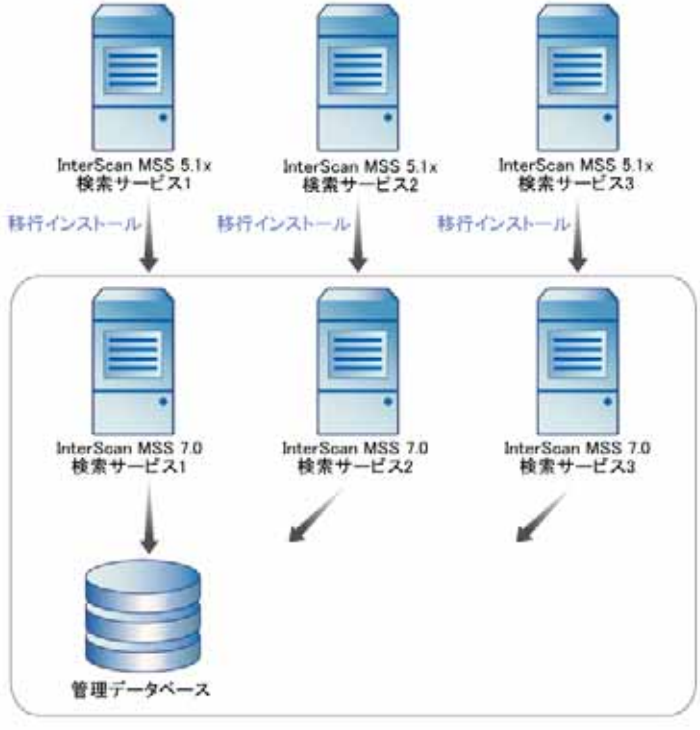


図 4-3.　単一の管理データベース

複数の管理データサービス

InterScan MSS 検索サービスごとに異なる管理データベースにアクセスするには、各検索サービスに対して下図のような移行インストールを実行します。

注意： 複数の管理データベースのアップグレードオプションには、次のような特性があります。

1. InterScan MSS が複数のサイトでインストールされています。
2. 検索サービスごとに異なる設定を行う場合、このオプションを選択します。
3. Control Manager を使用して、検索サービスを一元的に制御できます。

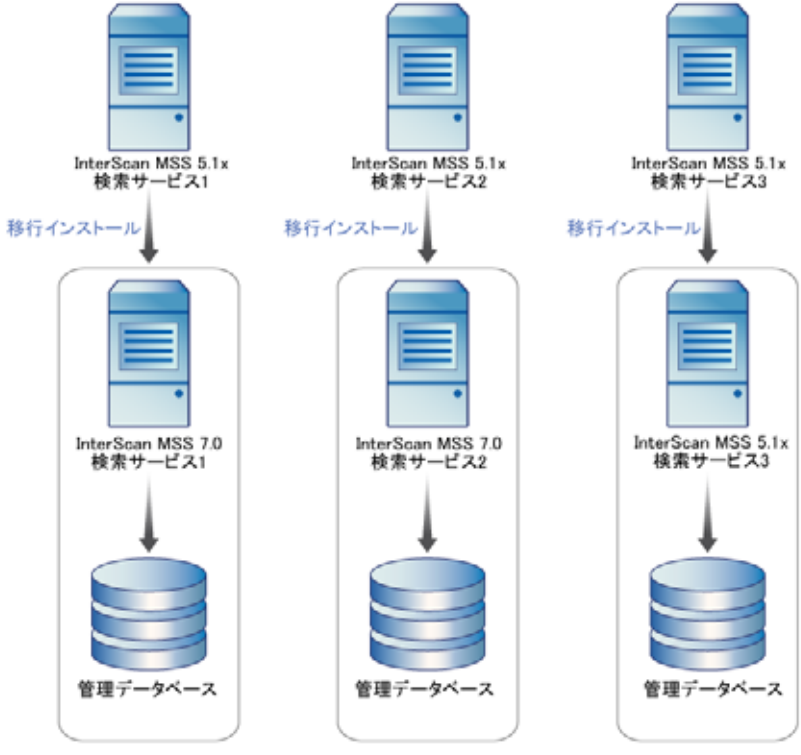


図 4-4.　複数の管理データサービス

設定のバックアップ

移行を実行する前に、まず InterScan MSS 5.1x のデータをバックアップします。

InterScan MSS 5.1x のデータをバックアップするには

1. 以下のコマンドを入力して、すべての InterScan MSS 5.1x のプロセスを停止します。

```
# $IMSS_HOME/imss/script/S99ISIMSS stop
```

2. 下のコマンドを入力して、Postfix を停止します。

```
# postfix stop
```

3. 以下のコマンドを入力して、InterScan MSS 5.1x のホームフォルダをバックアップします。

```
# tar cvf imss51.tar /$IMSS_HOME/imss
```

4. 以下のコマンドを入力して、Postfix 設定ファイルをバックアップします。

```
# tar cvf  postfix_config.tar /etc /postfix/main.cf
/etc/postfix/master.cf
```

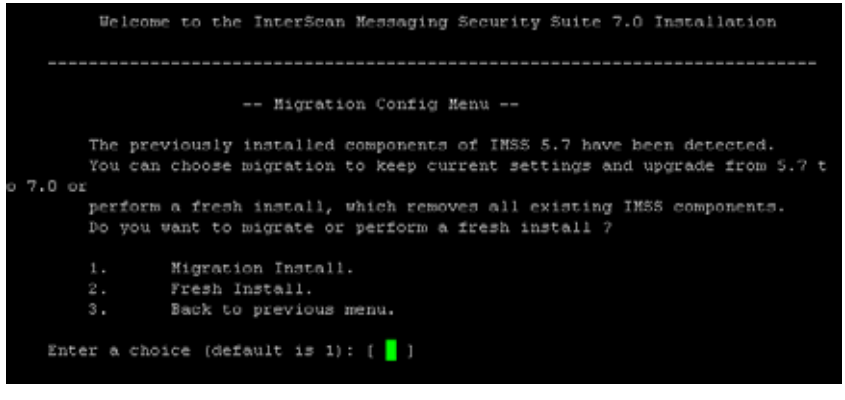
移行の手順

InterScan MSS バージョン 7.0 に移行するには

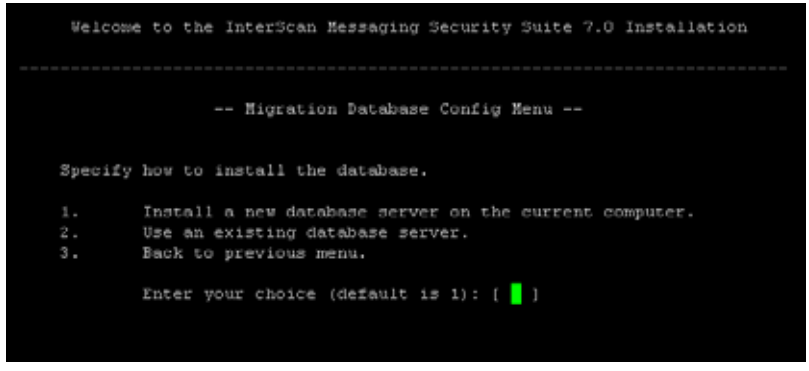
1. バージョン 5.1x がインストールされているコンピュータにスーパーユーザとしてログインし、インストールパッケージディレクトリに移動します。

2. 「./isinst.sh」と入力します。[Main Menu] が表示されます。

3. 「1」と入力して、バージョン 7.0 への設定の移行とアップグレードを選択します。[Migration Config Menu] が表示され、InterScan MSS 5.1x の旧コンポーネントが検出されたことを示します。

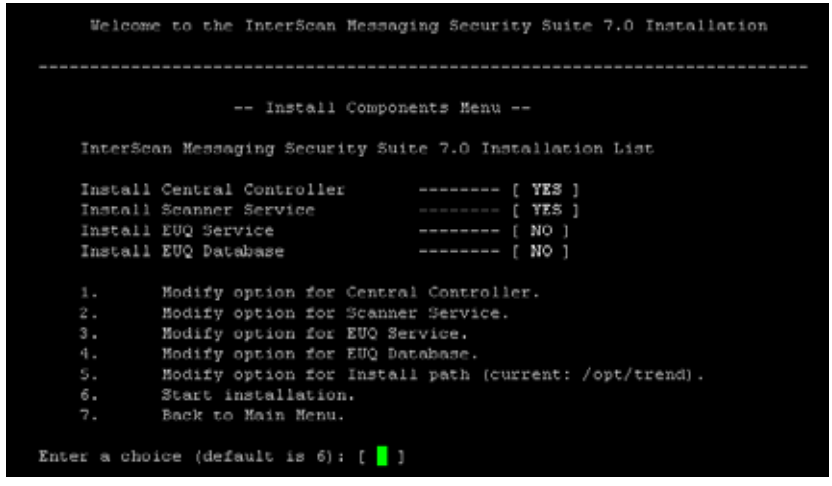


4. 「1」と入力して、移行インストールを実行します。[Migration Database Config Menu] が表示されます。インストーラは旧バージョンの InterScan MSS の設定をバックアップしてから、InterScan MSS 5.1x をアンインストールし、InterScan MSS 7.0 をインストールします。



5. 新規の InterScan MSS 管理データベースサーバをインストールするか、既存のサーバを使用するかを選択します。データベースサーバの詳細を入力します。既存サーバの使用を選択した場合、インストーラはサーバに接続します。

6. [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 (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。



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。

注意： 初期設定では、旧バージョンのインストールパスが使用されます。移行インストールを選択した場合、インストールパスを変更できません。

- エンドユーザメール隔離をインストールするには、最初にインストールされたエンドユーザメール隔離がプライマリサービスになることに留意してください。セカンダリサービスは、プライマリサービスの負荷分散を補助します。
- 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」を入力してインストールを開始します。次のように、後続の手順が開始されます。

   a. 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。

b. インストールを続行する場合、コンピュータ上の既存の DNS が確認され、後で IP プロファイラをインストールする場合には、BIND をインストールするようプロンプトが表示されます。

注意： InterScan MSS 7.0 Linux には、BIND 9.3.2 がバンドルされています。InterScan MSS 7.0 Solaris には、BIND 9.4.0 がバンドルされています。

c. 次に、移行できない設定のリストが表示されます。

d. インストーラは旧バージョンの InterScan MSS の設定をバックアップし、InterScan MSS 5.1x をアンインストールしてから、InterScan MSS 7.0 をインストールします。

注意： 1. バージョン 5.1x のポリシーおよびサブポリシーでのフィルタは、バージョン 7.0 のルールとして表示されます。インストーラでは、ポリシーが自動的に検出され、ルールに移行されます。InterScan MSS 7.0 のルールの詳細については、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。

2. 特別なルートが設定された InterScan MSS 5.1x の旧ポリシーは、移行できない場合があります。その場合、[Policy Migration Menu] が表示され、次のいずれかのポリシーの方向を選択する必要があります。
[1]-incoming
[2]-outgoing

アクティベート

移行後、InterScan MSS 5.1x のアクティベーションコードは、有効期限が切れていなければそのまま保持されます。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する必要があります。

- InterScan MSS (ウイルス対策およびコンテンツフィルタ)
- スパムメール対策 (コンテンツ検索) - オプション

NRS を使用するには、NRS の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。

移行できない設定

次の設定は移行できません。

レポート設定

- Perl レポート

管理設定

- 隔離領域およびアーカイブフォルダのパス
- キューフォルダ内のメールメッセージ

注意： InterScan MSS 5.1x のキューフォルダの名前が、移行の際に、「queue_backup_yy-mm-dd-HH-MM-SS」と変更されます。移行後、手動でバックアップされたメッセージを処理する必要があります。

- ログのパス
- 時間あたりの通知数の制限
- 管理コンソールのパスワード
- 製品のシリアル番号

ポリシー設定

- 検索制限 : 駆除の試行回数、ウイルスレポート数、メッセージのサイズ制限の基準
- ユーザ定義のサブポリシーのウイルスフィルタ
- ウイルスフィルタに設定された、ウイルスが検出されなかった場合のカスタム処理
- ウイルス検索における除外する拡張子の設定
- グローバルスパムメール検索モード
- 疑わしいメールへの処理設定

- 詳細コンテンツフィルタに設定された、添付ファイルまたはファイルタイプに一致するキーワードのリスト
- オリジナルメッセージのアーカイブに関する設定
- オリジナルメッセージを添付した通知に関する設定
- オリジナルメッセージを添付した転送に関する設定

NRS 設定

NRS の設定は移行されません。

移行レポートの使用

次の 2 種類の移行レポートを $IMSS_Home/installlog/MigrationReport で確認できます。

- GeneralReport.txt - 移行されなかったすべての項目を表示します。
- DetailReport.txt - 移行する設定と移行しない設定について、InterScan MSS 5.1x と InterScan MSS 7.0 間の関係を表示します。

移行のロールバック

バージョン 7.0 への移行で問題が発生した場合、バージョン 5.1x にロールバックできます。バージョン 5.1x の詳細については、InterScan MSS 5.1x のドキュメントを参照してください。この項では、どのようにロールバックを実行するかを説明します。

バージョン 5.1x にロールバックするには

1. インストールしたバージョン 7.0 をアンインストールします (128 ページの「アンインストールの実行」を参照)。
2. InterScan MSS 5.1x を再インストールします (InterScan MSS 5.1x のドキュメントを参照)。

3. 実行中のすべての InterScan MSS 5.1x のプロセスを停止させるために、次のように入力します。

```
# $IMSS_HOME/imss/script/S99ISIMSS stop
```

4. Postfix を停止させるために、次のように入力します。

```
# postfix stop
```

5. InterScan MSS 5.1x ホームフォルダを復元するために、ルートディレクトリ下の imss51.tar ファイルを解凍します。これを実行するには、次のように入力します。

```
# tar vxf imss51.tar
```

6. Postfix の設定を復元するために、ルートディレクトリ下の postfix_config.tar ファイルを解凍します。これを Postfix の設定ファイルと置換します。これを実行するには、次のように入力します。

```
# tar vxf postfix_config.tar
```

7. InterScan MSS 5.1x のすべての処理を起動するために、次のコマンドを入力します。

```
# $IMSS_HOME/imss/script/S99ISIMSS start
```

8. Postfix を起動させるために、次のコマンドを入力します。

```
# postfix start
```

アンインストールの実行

InterScan MSS 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は、個別にも、同時にもアンインストールできます。

注意： Solaris のコアインストールを実行した場合は、InterScan MSS をアンインストールする前に、以下のインストールを行います。
- SUNWipc
- SUNWipx

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] に、コンポーネントのステータスが表示されます。これらの製品がインストール済みの場合は、[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開き、削除できるコンポーネントが表示されます。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]、すなわち削除されないように設定されています。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、その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。
6. 指定した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、PostgreSQL プロセスを停止するかどうかを確認するメッセージが表示されます。別のアプリケーションにより、そのプロセスがまだ使用されている場合は、プロセスを停止しないことを選択できます。

IP プロファイラと NRS のアンインストール

IP プロファイラおよび NRS 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] に、IP プロファイラおよび NRS のステータスが表示されます。これらの製品がインストール済みの場合は、[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開き、削除できるコンポーネントが表示されます。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]、すなわち削除されないように設定されています。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、その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。

   指定したコンポーネントがアンインストールされます。

6. NRS をアンインストールする場合は、メールログファイルも削除するかどうかを選択します。このファイルを削除しない場合、Postfix のメールログは引き続きこのファイルに書き込まれます。

   データベースが実行されている場合は、InterScan MSS 管理データベースから IP プロファイラと NRS の登録が削除されます。

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

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 stop

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

   $Home_IMSS/script/dbctl.sh stop

3. 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 imss-7.0-1
   rpm -e imsseuq-7.0-1
   rpm -e imsscctrl-7.0-1
   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。

4. 「$Home_IMSS, such as /opt/trend/imss」を削除します。

5. デーモン起動 / 停止スクリプトを削除します。

   - 起動スクリプトにより、自動的にシステムが再起動されます。「/etc/rc2.d/ /etc/rc3.d　/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を停止します。「/etc/rc0.d　/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

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.s.PGSQL.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「directory /usr/sbin/post*」から削除します。
   - postalias
   - postcat
   - postconf
   - postdrop
   - postfix
   - postkick
   - postlock
   - postlog
   - postmap
   - postqueue
   - postsuper
5. 「/var/spool/postfix」(オプション) を削除します。

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 NRS パッケージを削除します。

   ```
   rpm -e ipprofiler-7.0-1
   rpm -e nrs-7.0-1
   ```
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

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 (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。

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

トラブルシューティング

表 5-1 に、InterScan MSS インストール時に発生する可能性がある一般的なトラブルシューティングの問題を示します。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 の管理および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 管理者ガイド」を参照してください。

問題	推奨される解決策
NRS のインストール時、NRS アクティベーションコードが認証されない	アクティベーションコードを認証するために、NRS インストールスクリプトはインターネットでトレンドマイクロにアクセスします。 DNS サーバが正しく動作しており、NRS をインストールしているコンピュータがインターネットへアクセスできることを確認してください。
NRS をインストールすると、次のエラーメッセージが表示される「Applying change to Postfix failed」	Postfix が稼動していません。NRS インストールスクリプトが設定情報を Postfix 設定ファイルに書き込みます。 Postfix が稼働していることを確認してから、NRS インストールを再び実行してください。

表 5-1. 問題のトラブルシューティング

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場合は、[すべての検索サービスに適用] オプションを有効にする必要があります。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場合は、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できます。
例 :

detach_key_postfix=smtpd_use_tls:smtpd_enforce_tls:queue_directory

管理コンソールを使用せずに、どのように MTA 設定を変更できますか。

次の手順に従い、InterScan MSS 設定ファイルを変更して、キーを追加します。

1. imss.ini を開きます。
2. 次のように変更を加えます。

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

上記のパラメータは、管理コンソールで設定した設定内容によって上書きされません。main.cf を手動で変更できます。

警告 : 設定ファイルを変更する際は、細心の注意を払ってください。

インストールとアンインストール

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。

検索サービスは、いくつインストールできますか。

検索サービスはいくつでも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とエンドユーザメール隔離データベースは、いくつインストールできますか。

最大 8 つのエンドユーザメール隔離サービスとエンドユーザ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はありますか。

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中に削除されますか。

いいえ。InterScan MSS エンドユーザメール隔離データベースはアンインストール中に削除されません。

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

それは、インストールプログラムが古い InterScan MSS データベース削除しようとするときに、一部のアプリケーションがそのデータベースに接続していることがあるからです。古いデータベースへの接続をすべて切断してから再試行してください。

外部 DNS サーバを持つコンピュータに InterScan MSS 7.0 をインストールした場合、何か問題がありますか。

基本的には、InterScan MSS 7.0 を DNS サーバと統合しても機能的な問題はありません。同じコンピュータ上で InterScan MSS 7.0 を外部 DNS サーバと統合しても機能的には問題ありませんが、パフォーマンスの理由からお勧めしません。

既存の Apache サーバを持つコンピュータに InterScan MSS 7.0 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/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。

アップグレード

移行で、InterScan MSS 5.11 の設定はすべて維持されますか。

いいえ。InterScan MSS 7.0 ではアーキテクチャ上の変更のため、一部の設定は維持されません。移行の際に、InterScan MSS 7.0 インストーラによってこれらの設定の新しい値の設定を求められます。これらの設定は標準の移行レポートでも確認できます。

$IMSS_Home/installlog/MigrationReport/

GeneralReport.txt

InterScan MSS 5.11 の複数の検索サービスはどのように移行するのですか。

複数の InterScan MSS 5.11 検索サービスを移行するには

- 移行に最も適した設定を使用している検索サービスから移行します。
- その他の検索サービスはアンインストールします。
- 複数の検索サービスを追加します。

詳細については、116 ページの「複数の検索サービス配置のアップグレードオプション」を参照してください。

移行後、InterScan MSS 5.11 へのスムーズなロールバックは可能ですか。

はい。ロールバックの詳細な手順については、126 ページの「移行のロールバック」を参照してください。

移行中、内部アドレスの送信元はどのようになりますか。

InterScan MSS 5.11 の内部ドメインを維持するため、InterScan MSS 7.0 は次のフィールドからすべてのドメインを抽出します。

- 受信ポリシールートの「To」フィールドのドメイン
- 送信ポリシールートの「From」フィールドのドメイン

注意： 上記の 2 つのフィールドにアドレスグループがある場合は、アドレスグループ内のすべてのドメインが抽出されます。

移行時、フィルタとポリシーはどのようにマッピングされるのですか。

InterScan MSS 5.11 のアーキテクチャと InterScan MSS 7.0 のアーキテクチャは異なります。したがって、移行モジュールでは、次のような方法で、InterScan MSS 5.11 のすべてのフィルタを、InterScan MSS 7.0 内の関連するルールにマップします。

- ウイルスフィルタ : 移行後、ウイルス対策ルールは (InterScan MSS 5.11 でのウイルスフィルタの数に関係なく) すべてのメッセージに対して 1 つだけです。
    - InterScan MSS 5.11 でウイルスフィルタが 1 つでも「アクティブ」になっていると、ウイルスルールの状態は「有効」になります。
    - それ以外の場合、ウイルスルールの状態は移行後に「無効」になります。
- スパムメール対策フィルタ : 移行モジュールは、移行後、各スパムメール対策フィルタを 1 つまたは複数のスパムメール対策ルールにマッピングします。
- コンテンツフィルタ
    - コンテンツフィルタが、InterScan MSS 5.11 で SMTP と POP3 トラフィックの両方について「アクティブ」の場合、移行後は、1 つのコンテンツフィルタに対するルールは 2 つになります。

- コンテンツフィルタが、InterScan MSS 5.11 で SMTP と POP3 トラフィックの両方について「非アクティブ」の場合、移行後は、1 つのコンテンツフィルタに対するルールは 1 つだけになります。ルールの方向は、「受信と送信の両方向」になります。InterScan MSS 7.0 では、必要に応じて、POP3 の方向に対する関連ルールを追加できます。

各ポリシーの詳細なマッピング関係については、$IMSS_Home/installlog/MigrationReport/DetailReport.txt を確認してください。

その他

サンドイッチモデルとプロキシモデルの違いは何ですか。

サンドイッチモデルでは、アップストリーム MTA、InterScan MSS、およびダウンストリーム MTA をイントラネット内の異なるコンピュータにインストールします。インターネットからの外部メッセージは、まずアップストリーム MTA に到達し、そこから InterScan MSS に渡されます。しかし、プロキシモデルでは外部メッセージを中継するアップストリーム MTA がないため、メッセージは InterScan MSS に直接送信されます。

プロキシモデルが配置されていない場合、ポート 25 は待機しますか。

プロキシモデルにはメッセージを InterScan MSS に中継するアップストリーム MTA がないため、初期設定の InterScan MSS 待機ポートはポート 25 に設定され、インターネットから直接メッセージを受信できるようにします。

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。

中小 / 中堅企業のお客さま

http://esupport.trendmicro.co.jp/supportjp/smb/search.do

大企業のお客さま

http://esupport.trendmicro.co.jp/supportjp/enterprise/search.do

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。

トレンドマイクロへのスパムメールの報告

トレンドマイクロでは、できるだけ最新のスパムメールデータベースを提供できるように、スパムメールが検出されずに受信された場合、そのメールをトレンドマイクロの次のメールアドレスに転送するようにお願いしています。

jp-spam@support.trendmicro.com

また、通常のメールがスパムメールとして検出（誤検出）された場合は、そのメールを次のメールアドレスに転送してください。

jp-false@support.trendmicro.com

注意： お客さまから転送されたメールはスパムメールの検出精度向上のための用途にのみ使用します。お客さまからのメールに含まれる個人情報は、スパムメール検出精度向上のための作業後、すみやかに削除します。

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 800 名以上 (2006 年 1 月現在) 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 53
  Tomcat 52
Control Manaager エージェント、エージェント
  Control Manager 26
Control Manager
  概要、Control Manager
    概要 26
CPU の要件 32
Firefox 33
IMSSMGR 52
Internet Explorer 33
InterScan MSS 14
InterScan MSS 5.1x 116
InterScan MSS コンポーネント
  インストール 52
  エンドユーザメール隔離データベース 42
  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 39
  管理データベース 36
  検索サービス 37
  セントラルコントローラ 36
  ポリシーサービス 38
  ポリシーサービスの同期 38
InterScan MSS について 14
IP フィルタ
  インストール 106
  概要 42
  削除 129
IP プロファイラ 15
  概要 42
  機能 44
  検出 43
LDAP サーバの要件 33
MTA
  Postfix の準備 88
MTA 機能、便宜的な TLS 15
MTA の要件 34
Named Server 52
NRS 15
  概要 43
  機能 45
  サービス 43
Postfix の準備 88
Postgre の要件 33
Readme ファイル 10
Tomcat 52、53
TrendLabs 145
Web エンドユーザメール隔離 15

あ

アーカイブ 15
アーカイブおよび隔離領域の一元化 15
新しい機能 14
アップグレード 113
アンインストール 128
  IP フィルタコンポーネント 129

移行
ロールバック 126
移行のロールバック 126
インストール 31
Control Manager の使用 80
DMZ 内 62
InterScan MSS の削除 128
IP フィルタ 106
IP フィルタ、インストール
エンドユーザメール隔離 84
Postfix の準備 88
SMTP ゲートウェイ 61
クラスタ化 78
シナリオ 70
手順 100
ファイアウォールなし 58
ファイアウォールの内側 60
ファイアウォールの外側 59
エンドユーザメール隔離 15
オンラインヘルプ 10

か

隔離 15
管理データベース 52
検索サービス 38
コンポーネントおよびサブモジュールのインストール 52

さ

最小要件 32
システム要件 32
新機能 14
スパイウェアとグレーウェア 24
スパムメール対策 15
スワップ領域の要件 33
設定
移行 125
設定ウィザード 15
設定の移行 125
セントラルコントローラ 38

た

対象読者 10
ディスク領域の要件 32
データベース
セントラルコントローラ 36
データベースサーバ 52
テクニカルサポート 142
ドキュメント 10
トラブルシューティング 136
NRS 136

は

バージョン 5.1x 116
はじめに 9
パターンマッチング 17
フィルタ、機能 20
ブラウザ要件 33
ポリシー 14
ポリシーサービス 38
ポリシーの一元化 14

ま

マスメーリング型ウイルス
パターン 19
メール脅威
スパムメール 18
非生産的メッセージ 18
メールログパーサ 54
メモリの要件 32

や

要件 32
よくある質問
postfix 137

ら

レポート 15
ログ 15
ログ機能の一元化 15