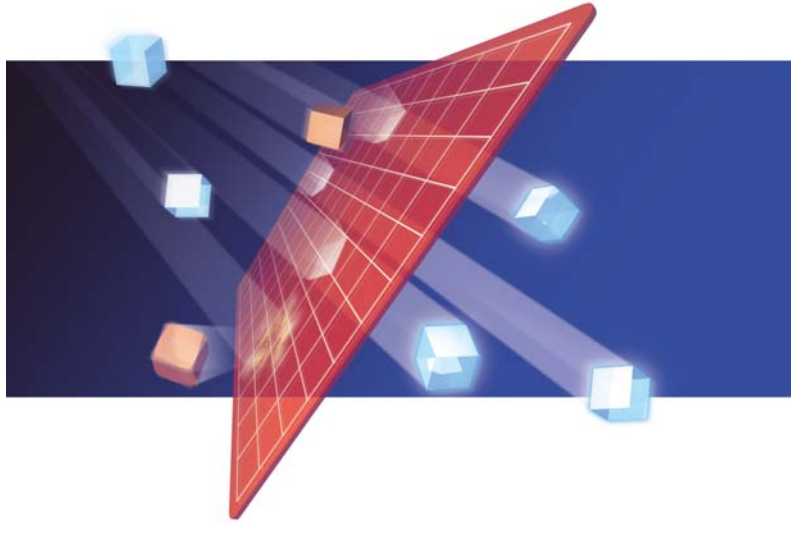
Trend Micro InterScan Messaging Security Suite™

UNIX版



クイックスタートガイド

TREND MICRO™

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、GateLock、VSAPI、eDoctor、eManager、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、Certified Rescue Partner、License for Enterprise Information Security、LEISec、Trend Park、Trend Labs、Trend Micro Enterprise Protection Strategy、RBL+、Phish Checker、スパイバスター、InterScan Gateway Security Appliance、Trend Micro Network VirusWall、Network VirusWall Enforcer、Trend Flex Security、EPS、Trend Micro EPSは、トレンドマイクロ株式会社の登録商標です。

本書に記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。

Copyright ©2002-2007 Trend Micro Incorporated. All rights reserved.

P/N: IMSSUX-AE0104 (2007/09)

目次

はじめに 11

ドキュメント 12

対象読者 12

ドキュメントの表記規則 13

第 1 章　製品の概要 15

InterScan MSS 7.0 について 16

新機能 16

InterScan MSS の主な特長と利点 18

スパイウェアと他の種類のグレーウェア 27

Trend Micro Control Manager について 29

Control Manager との統合 30

第 2 章　システム要件とコンポーネント 35

システム要件 36

InterScan MSS で使用されるポート 40

InterScan MSS コンポーネントについて 43

InterScan MSS 管理データベース 43

セントラルコントローラ 43

検索サービス 44

ポリシーサービス 45

ポリシーの同期 45

エンドユーザメール隔離サービス 45

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 46

エンドユーザメール隔離のデータベース 46
IP フィルタ 46
Trend Micro Network Reputation Services 47
Trend Micro Network Reputation Services の種類 47
IP プロファイラの機能 48
Trend Micro Network Reputation Service の機能 49

第 3 章 配置計画 51
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
ネットワークトポロジの検討 55
ファイアウォールを使用しないインストール 55
ファイアウォールの外側へのインストール 56
受信トラフィック 56
送信トラフィック 56
ファイアウォールの内側へのインストール 57
受信トラフィック 57
送信トラフィック 57
既存の SMTP ゲートウェイ上へのインストール 58
受信トラフィック 58
送信トラフィック 58
DMZ 内 59
受信トラフィック 59
送信トラフィック 59
インストールシナリオの理解 60
集中インストール 60
複数の検索サービスのインストール 62
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 64
複雑な分散インストール 67

WAN へのインストール 69
Trend Micro Control Manager 69
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 71
フェイルオーバーについて 73
運用モデルについて 75
スタンドアロンモデル 76
サンドイッチモデル 78
プロキシモデル 80
IP フィルタとエンドユーザメール隔離 81
IP フィルタ機能を付加した InterScan MSS の配置 81
エンドユーザメール隔離を付加した InterScan MSS の配置 81
サーバ間の通信 82

第 4 章 インストールとアップグレード 83

MTA の準備 84
Postfix の準備 84
InterScan MSS 7.0 Solaris での Postfix のインストール 84
sendmail の使用 89
sendmail のデーモン 90
sendmail #1 の設定 90
sendmail #2 の設定 92
sendmail サービスの再起動 92
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 94
Solaris システムファイルの設定 94
インストール手順 95
IP フィルタのインストール 100
IP プロファイラと NRS のインストール 100

sendmail および qmail と InterScan MSS の統合 102
FoxLib と sendmail の統合 102
FoxLib と qmail の統合 104
前バージョンからのアップグレード 106
設定のバックアップ 106
単一サーバ配置での InterScan MSS 5.1x データのバックアップ 106
分散配置での InterScan MSS 5.1x データのバックアップ 108
アクティベート 112
移行できない設定 112
移行レポートの使用 113
バージョン 5.1x からバージョン 7.0 への移行 113
移行のロールバック 123
単一サーバ配置でのロールバック 124
分散配置でのロールバック 124
アンインストールの実行 126
InterScan MSS のアンインストール 126
IP プロファイラと NRS のアンインストール 127

第 5 章 使用開始 129

InterScan MSS の管理コンソールを開く 130
SSL を使用した管理コンソールの表示 131
設定ウィザードでの基本設定の実行 132
Trend Micro Network Reputation Services の使用 141
スパムメール対策のアクティベーションコードの使用 141
NRS の設定 141
NRS で使用するための MTA の準備 142
NRS 管理コンソールの使用 143

エンドユーザメール隔離の管理コンソールを開く 145

第 6 章 設定 147

IP フィルタの設定 148

IP フィルタのログのクエリ 154

SMTP ルーティングの設定 155

SMTP ルーティングの SMTP の設定 155

SMTP ルーティングの接続の設定 156

SMTP ルーティングのメッセージルールの設定 158

SMTP ルーティングのドメインベース配信の設定 159

メッセージ追跡 160

ポリシーの追加 161

既存のポリシーの表示 162

内部アドレスの設定 164

ルートの指定 165

検索条件の指定 167

処理の指定 168

優先順位の指定 169

ポリシーイベントのログのクエリ 170

隔離およびアーカイブの管理 172

エンドユーザメール隔離データベースの追加 / 削除 174

エンドユーザメール隔離データベースの追加 174

エンドユーザメール隔離データベースの削除 175

euqtrans ツールのコマンドラインオプション 175

第 7 章 ログとレポート 177

InterScan MSS のログのクエリ 178

1 回限りのレポートの作成 180
予約レポートの設定 183

第 8 章　トラブルシューティングとサポート情報 187

トラブルシューティング 188
よくある質問 (Q&A) 197
Postfix MTA 設定 197
インストールとアンインストール 197
アップグレード 198
InterScan MSS コンポーネント 200
NRS 201
IP プロファイラ 202
隔離とアーカイブ 206
エンドユーザメール隔離 207
スパムメール対策サービス 209
アップデート 210
その他 210
製品サポート情報 215
サポートサービスについて 215
製品 Q&A のご案内 216
セキュリティ情報 217
セキュリティ情報の入手先 217
トレンドマイクロへのウイルス解析依頼 217
トレンドマイクロへのスパムメールの報告 218
ウイルス解析サポートセンター「TrendLabs」..... 219

付録 A　その他の設定..... 221

その他のタスクの実行 222

索引 225

はじめに

本書では、Trend Micro InterScan Messaging Security Suite (以下、InterScan MSS) の起動および実行方法について説明しています。すべての機能の詳細な設定情報については、オンラインヘルプを参照してください。オンラインヘルプには管理コンソールからアクセスできます。

この章の内容は、次のとおりです。

- 12 ページの「ドキュメント」
- 12 ページの「対象読者」
- 13 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。

- **クイックスタートガイド** - InterScan MSS のインストールおよび実行について説明しています。
- **オンラインヘルプ** - ユーザインタフェースを使用して、すべての機能を設定する方法について説明しています。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。

クイックスタートガイドおよび 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 管理者およびメール管理者を対象に書かれています。本書は、読者の方に、次の知識を含め、メールメッセージングネットワークの専門的な知識があることを前提としています。

- SMTP および POP3 プロトコル
- Postfix 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。

- 16 ページの「InterScan MSS 7.0 について」
- 16 ページの「新機能」
- 18 ページの「InterScan MSS の主な特長と利点」
- 27 ページの「スパイウェアと他の種類のグレーウェア」
- 29 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 P 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
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。
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。

表 1-1. 新機能

新機能	説明
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。
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。

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、検索エンジンはそのウイルスコードを削除することにより、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。

表 1-2.　主な特長と利点

特長	説明	利点
IntelliTrap	ウイルス作成者は通常、さまざまなファイル圧縮スキームを使用してウイルスフィルタを回避しようとします。IntelliTrap は、これらの圧縮ファイルのヒューリスティック評価機能します。 場合により、誤って脅威ではないファイルが危険なファイルとして識別される可能性もあるため、IntelliTrap 機能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。この機能は、初期設定では有効になっており、このカテゴリに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。
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。

表 1-2.　主な特長と利点

特長	説明	利点
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。

表 1-2.　主な特長と利点

特長	説明	利点
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、Trend Labs (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。
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、27 ページの「スパイウェアと他の種類のグレーウェア」を参照してください。	InterScan MSS が持つ、スパイウェアやその他の種類のグレーウェアからの保護機能により、セキュリティの上でも、機密性に関しても、法的な面でも、企業のリスクが大幅に軽減されます。

表 1-2. 主な特長と利点

特長	説明	利点
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通じて機能します。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。 ・ 46 ページの「IP フィルタ」 ・ 47 ページの「Trend Micro Network Reputation Services」 ・ 48 ページの「IP プロファイラの機能」 ・ 49 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、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管理コンソールを使用して、エンドユーザは InterScan MSS によって隔離またはアーカイブ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。管理者のログイ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。

表 1-2.　主な特長と利点

特長	説明	利点
システムの可用性の監視	組み込みエージェントが InterScan MSS サーバの状態を監視し、メールフローを妨害する可能性のある違反状況が発生した場合に、メールまたは SNMP トラップを通じて通知を配信します。	システム障害の検出をメールで通知するので、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。
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、分散配置を考慮して設計されています。	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
Trend Micro Control Manager との統合	Trend Micro Control Manager (以下、Control Manager) は、ウイルス対策プログラムとコンテンツセキュリティプログラムを、その物理的な位置やプラットフォームに関係なく中央から制御できるようにするソフトウェア管理ソリューションです。このアプリケーションは、企業のウイルス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、29 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、ウイルス以外の潜在的な脅威のリスクにもさらされています。グレーウェアは、ネットワーク上のコンピュータのパフォーマンスに悪影響を与え、セキュリティの上でも、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

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 ウイルスログとコンテンツフィルタログを、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 管理コンソールのユーザインタフェースを使用して、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 ・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。

- 36 ページの「システム要件」
- 40 ページの「InterScan MSS で使用されるポート」
- 43 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 6 以降 ・Red Hat Enterprise Linux AS 4 Update 2 以降 ・SUSE Linux Enterprise Server 8 および SP1 以降 ・SUSE Linux Enterprise Server 9 SP3 以降 Solaris: Solaris SPARC 8、9、10
推奨 CPU	Linux: デュアル構成の Pentium 4 3GHz 以上 Solaris: UltraSPARC IIIi 1.0 GHz 以上
最小 CPU	Linux: Intel Pentium 4 2.4GHz Solaris: Ultra SPARC II 650Hz
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 1GB **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	Linux: 4GB Solaris: スワップ領域には、物理メモリの 4 倍のサイズが必要です。 **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。これは、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 Solaris は PostgreSQL 8.1.5 に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

表 2-1.　システム要件

MTA	・InterScan MSS 専用 Postfix: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-2.3.4 ・libstdc++-libc6.2-2.so.3
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 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 ・ Solaris 10 に SUNWcstu 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 で使用されるポート

InterScan MSS で使用されるポートを表 2-2 に示します。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。

ポート番号	コンポーネントと役割	設定の保存先
25	* 外部接続を受け付ける Postfix SMTP デーモン	master.cf
110	* 検索デーモンの POP3 エンドポイント	imss.ini / [Socket_2]/ proxy_port
5060	* ポリシーサービス	管理コンソールのメニューで、[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	InterScan MSS 管理コンソールの Tomcat シャットダウンポート	{IMSS}/UI/adminUI/conf/server.xml: Server / port
8009	エンドユーザメール隔離管理コンソールの Tomcat AJP (負荷均衡) ポート	{IMSS}/UI/euqUI/conf/server.xml: Server / Service / Connector (protocol=AJP/1.3) / port
8015	エンドユーザメール隔離管理コンソール Tomcat シャットダウンポート	{IMSS}/UI/euqUI/conf/server.xml: Server/port
8445	InterScan MSS 管理コンソール Tomcat 待機ポート	Tomcat 待機ポート :{IMSS}/UI/adminUI/conf/server.xml: Server / Service / Connector / port
8446	エンドユーザメール隔離管理コンソール Tomcat 待機ポート	{IMSS}/UI/euqUI/conf/server.xml: Server / Service / Connector / port

表 2-2.　InterScan MSS で使用されるポート

ポート番号	コンポーネントと役割	設定の保存先
8447	プライマリエンドユーザメール隔離サーバ Apache Web サーバ待機ポート	{IMSS}/UI/euqUI/conf/EUQ.conf: Listen / VirtualHost / ServerName
10024	検索デーモンの SMTP 再処理エンドポイント	imss.ini / [Socket_3]/ proxy_port
10025	検索デーモンの SMTP エンドポイント	imss.ini / [Socket_1]/ proxy_port
10026	検索デーモンからの接続を受け付ける Postfix SMTP デーモン	master.cf
15505	* InterScan MSS マネージャ (IMSSMGR) ポート	管理コンソールのメニューで、[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 からは設定できません。
5432	PostgreSQL サーバポート	このポートは変更できません。
80	* Control Manager サーバ HTTP ポート	管理コンソールのメニューで、[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	* Control Manager サーバ HTTPS ポート	管理コンソールのメニューで、[管理]→[InterScan MSS の設定]→[接続]→[Control Manager サーバ] の順にクリックします。

表 2-2. InterScan MSS で使用されるポート

ポート番号	コンポーネントと役割	設定の保存先
88	Kerberos レルム用 KDC ポート	InterScan MSS からは設定できません。
53	Bind ポート	InterScan MSS 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		

表 2-2.　InterScan MSS で使用されるポート

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、81 ページの「IP フィルタとエンドユーザメール隔離」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 InterScan MSS インストール内の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、InterScan MSS 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プッシュされます。

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。

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。
- Directory Harvest Attack (DHA) - ユーザのメールアドレスをスパムメールのデータベースに追加する可能性のあるプログラム。
- 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メッセージ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、46 ページの「IP フィルタ」で挙げた潜在的な脅威が含まれるメールを検出すると、その送信元コンピュータの IP アドレスを能動的に学習します。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。

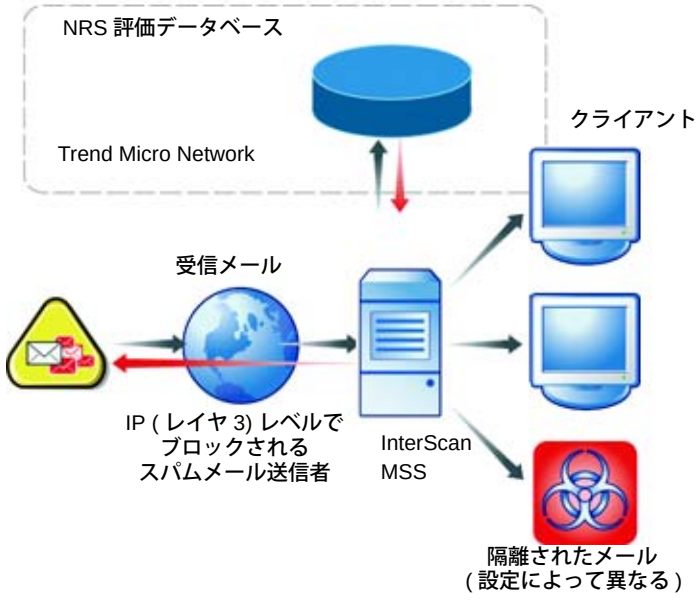


図 2-1. NRS の機能

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://www.trendmicro.com/jp/products/nrs/overview.htm

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。

- 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「ネットワークトポロジの検討」
- 60 ページの「インストールシナリオの理解」
- 73 ページの「フェイルオーバーについて」
- 75 ページの「運用モデルについて」
- 81 ページの「IP フィルタとエンドユーザメール隔離」

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	Fox Proxy	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

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。

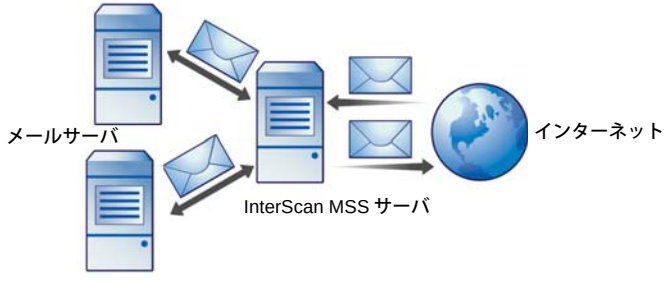


図 3-1. インストールトポロジ : ファイアウォールなし

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。

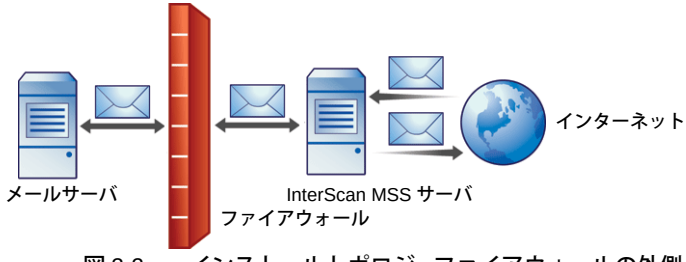


図 3-2. インストールトポロジ : ファイアウォールの外側

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

- ファイアウォールを使用しない場合は、すべての送信メールが Postfix 経由でインターネットに送信されるよう SMTP サーバを設定します。
- ファイアウォールを使用する場合は、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。

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。

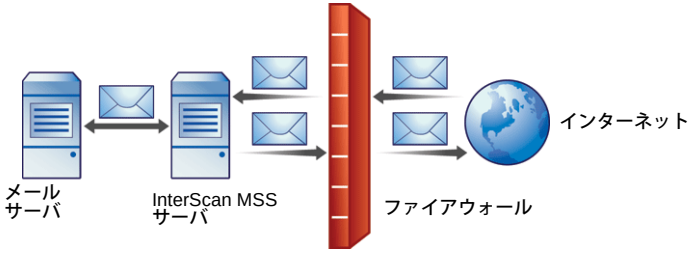


図 3-3. インストールシナリオ : ファイアウォールの内側

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。

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

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。

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。このシナリオでは、1 つのサーバにすべての InterScan MSS コンポーネント、すなわち、InterScan MSS 管理データベース、セントラルコントローラ、ポリシーサービス、検索サービスコンポーネント、エンドユーザメール隔離サース、およびエンドユーザメール隔離データベースをインストールします。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、次の項に示すように、複数の検索サービスをインストール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 3-4. 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。

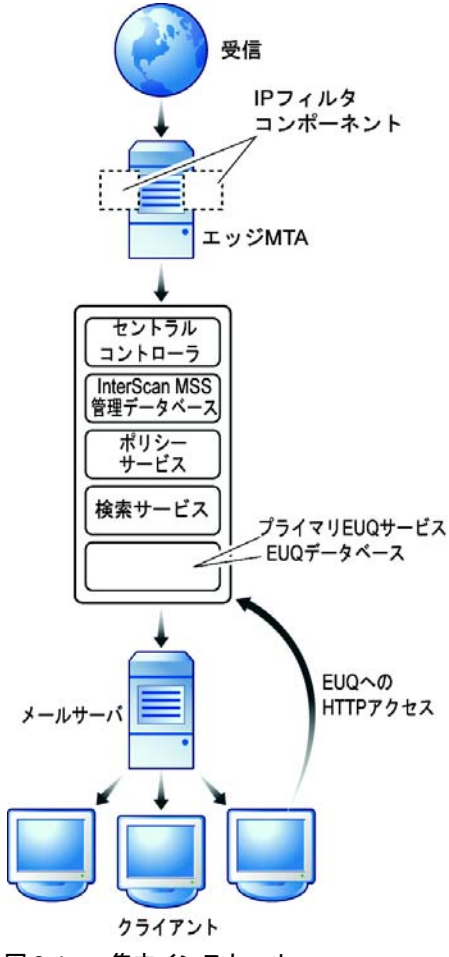


図 3-4.　集中インストール

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 (94 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 (100 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。このインストールシナリオを使用すると、効率の高いメッセージスループットを実現できます。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、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てから、インストールの追加を選択し、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 3-5. 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。

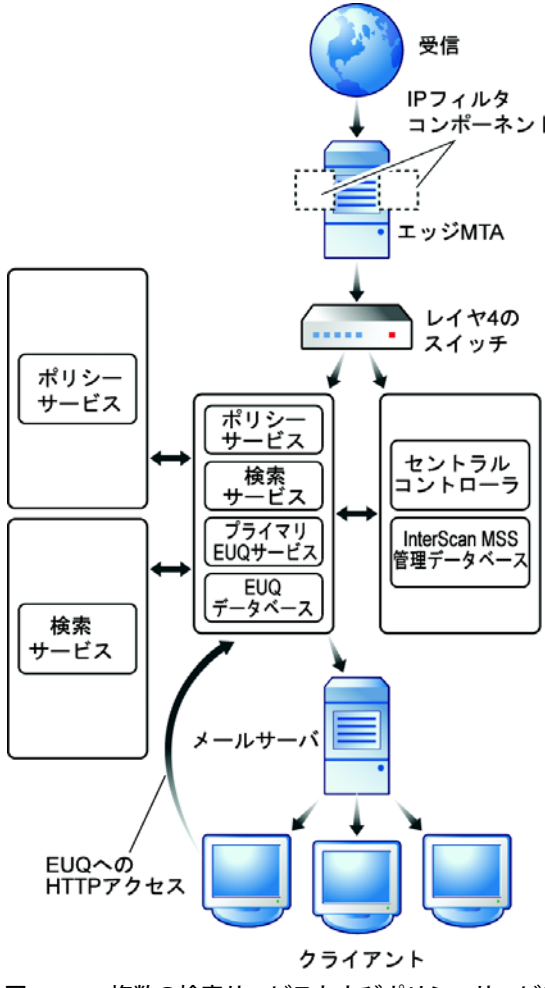


図 3-5.　複数の検索サービスおよびポリシーサービスのインストール

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 (94 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 (100 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 (129 ページの「使用開始」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 3-6. 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。

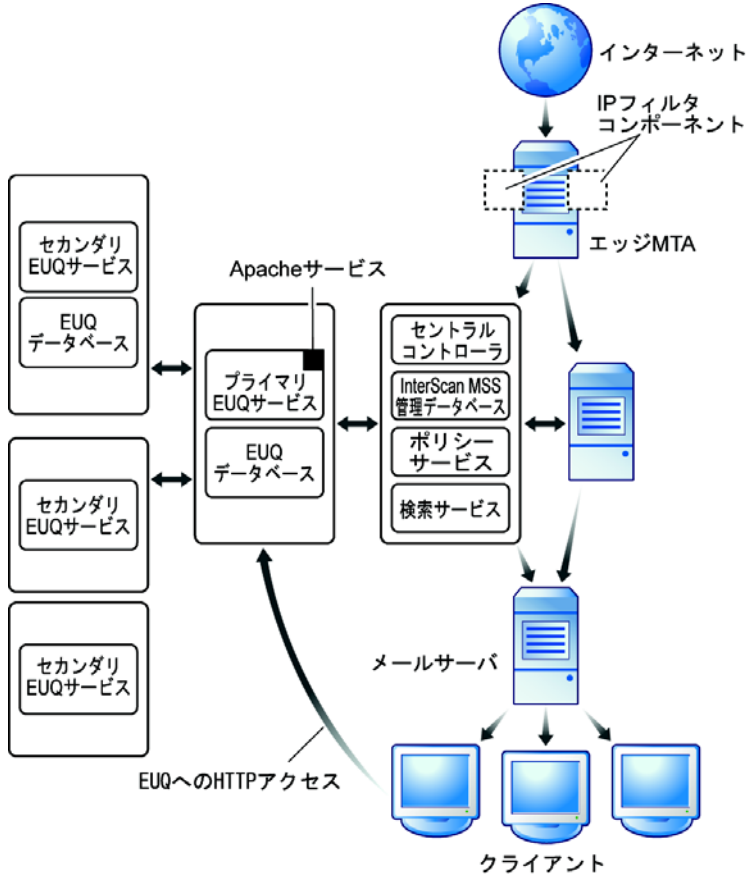


図 3-6.　複数のエンドユーザメール隔離サービスのインストール

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 (94 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 (100 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 (129 ページの「使用開始」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。

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 3-7. 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。

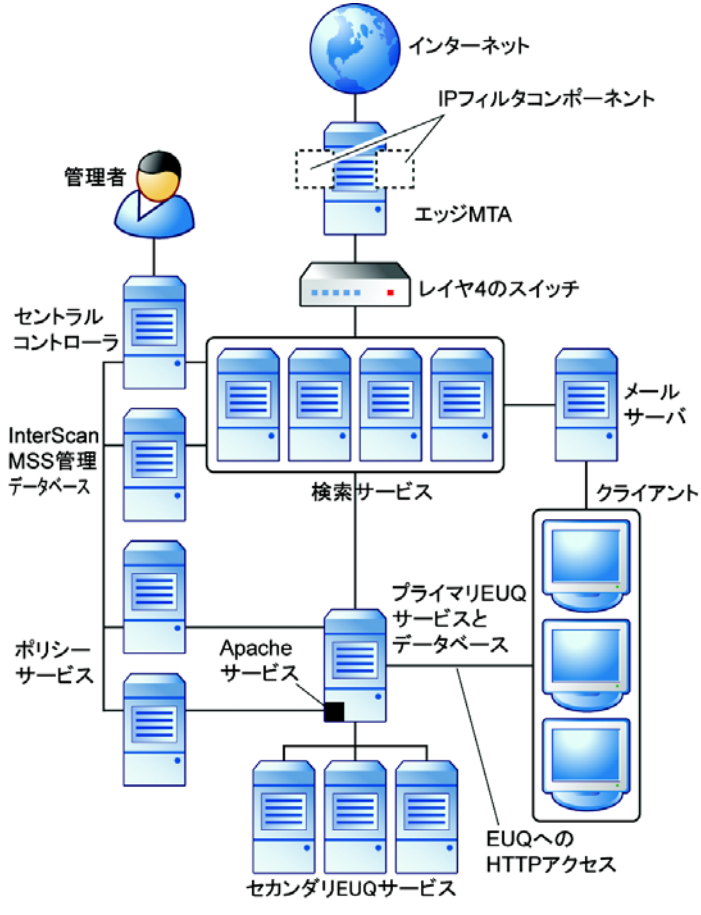


図 3-7.　複雑なアーキテクチャのインストール

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、コンポーネントを分散してインストールできますが、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が必要です。

WAN に複数のサイトがある場合、InterScan MSS コンポーネントを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。

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 3-8. は、複数サイトの WAN での配置を示しています。

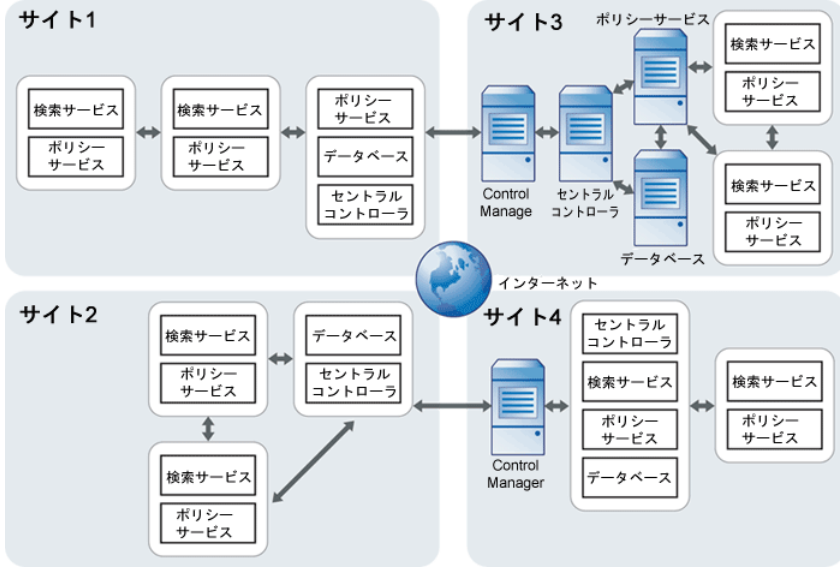


図 3-8. WAN での配置

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 3-9 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。

フェイルオーバーの詳細については、71 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。

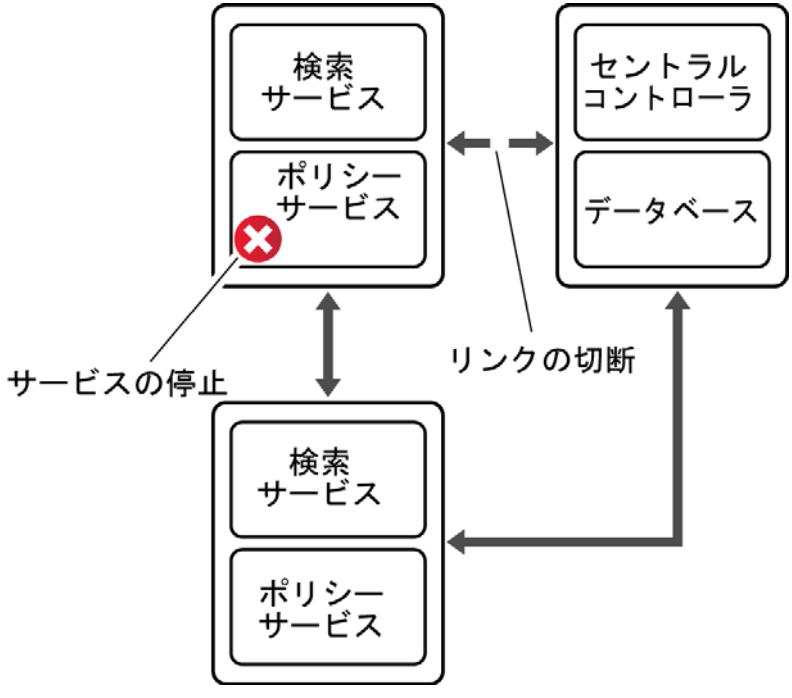


図 3-9.　フェイルオーバー

フェイルオーバーについて

表 3-2 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、71 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
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。 3. その検索サービスへのメールトラフィックは、すべて停止されます。
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。
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。
エンドユーザメール隔離サービス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。

障害のあるコンポーネント	予測される結果
LDAP サーバが動作しない	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. Foxhunter は LDAP 設定を使用しません。 3. LDAP が有効な場合、InterScan MSS は正常に動作を続行し、指定した時間以内にサービスが起動されない場合には、イベント通知が送信されます。

表 3-2.　フェイルオーバーのシナリオ

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： 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。

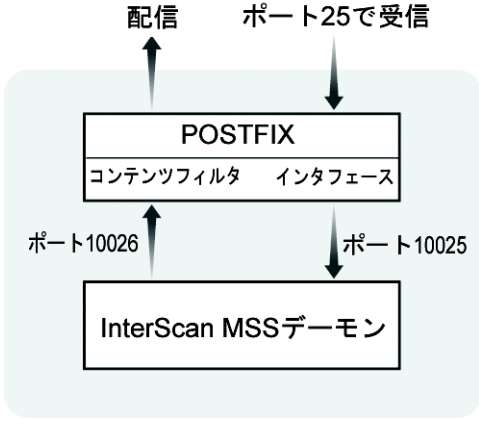


図 3-10.　スタンドアロンモデル

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=20

/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 - 20 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。

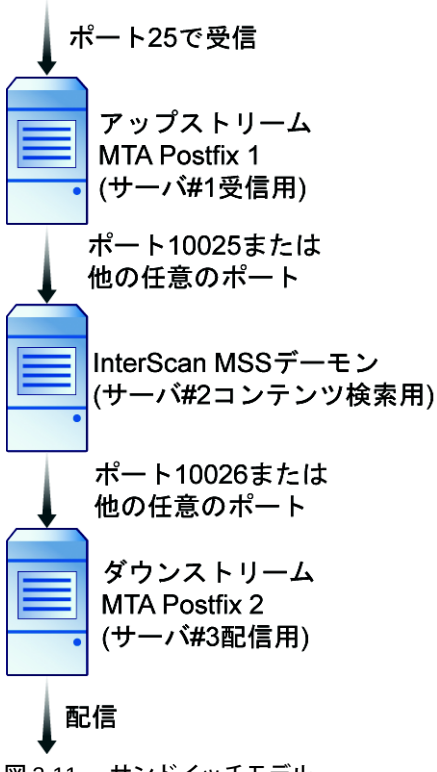


図 3-11.　サンドイッチモデル

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

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

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

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

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

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 3-12.　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。

IP フィルタとエンドユーザメール隔離

IP フィルタ (IP プロファイラおよび NRS)、またはエンドユーザメール隔離を配置する場合は、ネットワークトポロジに関してさらに考慮する点があります。

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。

エンドユーザメール隔離を付加した InterScan MSS の配置

Web ベースのエンドユーザメール隔離を使用すると、ユーザは、InterScan MSS がスパムメールとして隔離したメッセージにアクセスできます。Web ベースのエンドユーザメール隔離は、InterScan MSS と同じサーバに配置することも、別のサーバに配置することもできます。

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 HTTPS 接続をブロックしない種類であるか、HTTPS トラフィックを許可するように設定されている必要があります。

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

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サービス、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サービスを、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。

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。

- 84 ページの「MTA の準備」
- 94 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」
- 100 ページの「IP フィルタのインストール」
- 102 ページの「sendmail および qmail と InterScan MSS の統合」
- 106 ページの「前バージョンからのアップグレード」
- 113 ページの「バージョン 5.1x からバージョン 7.0 への移行」
- 123 ページの「移行のロールバック」
- 126 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、95 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。

```
Checking Postfix ...
./isinst.sh: postconf: not found
*******************************************************************************
No Postfix was found on your computer. IMSS requires Postfix.
Do you want to install Postfix 2.3.8 now? [y/n] y
```

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。

```
x postfix-2.3.8/README_FILES/SCHEDULER_README, 5372 bytes, 11 tape blocks
x postfix-2.3.8/README_FILES/SMTPD_ACCESS_README, 15789 bytes, 31 tape blocks
x postfix-2.3.8/README_FILES/SMTPD_POLICY_README, 18078 bytes, 36 tape blocks
x postfix-2.3.8/README_FILES/SMTPD_PROXY_README, 10576 bytes, 21 tape blocks
x postfix-2.3.8/README_FILES/STANDARD_CONFIGURATION_README, 25704 bytes, 51 tape blocks
x postfix-2.3.8/README_FILES/TLS_README, 88135 bytes, 173 tape blocks
x postfix-2.3.8/README_FILES/TUNING_README, 22370 bytes, 44 tape blocks
x postfix-2.3.8/README_FILES/ULTRIX_README, 2002 bytes, 4 tape blocks
x postfix-2.3.8/README_FILES/UUCP_README, 5265 bytes, 11 tape blocks
x postfix-2.3.8/README_FILES/VERP_README, 7163 bytes, 14 tape blocks
x postfix-2.3.8/README_FILES/VIRTUAL_README, 23675 bytes, 47 tape blocks
x postfix-2.3.8/README_FILES/XCLIENT_README, 9207 bytes, 18 tape blocks
x postfix-2.3.8/README_FILES/XFORWARD_README, 7677 bytes, 15 tape blocks
x postfix-2.3.8/COMPATIBILITY, 2961 bytes, 6 tape blocks
x postfix-2.3.8/COPYRIGHT, 1922 bytes, 4 tape blocks
x postfix-2.3.8/LICENSE, 11942 bytes, 24 tape blocks
x postfix-2.3.8/postfixinstall, 5475 bytes, 11 tape blocks
x postfix-2.3.8/postfixinstallutil, 23673 bytes, 47 tape blocks
x postfix-2.3.8/RELEASE_NOTES, 36337 bytes, 71 tape blocks
x postfix-2.3.8/RELEASE_NOTES-1.1, 50071 bytes, 98 tape blocks
x postfix-2.3.8/RELEASE_NOTES-2.0, 38863 bytes, 76 tape blocks
x postfix-2.3.8/RELEASE_NOTES-2.1, 26781 bytes, 53 tape blocks
x postfix-2.3.8/RELEASE_NOTES-2.2, 19753 bytes, 39 tape blocks
x postfix-2.3.8/TLS_ACKNOWLEDGEMENTS, 2315 bytes, 5 tape blocks
x postfix-2.3.8/TLS_CHANGES, 106588 bytes, 209 tape blocks
x postfix-2.3.8/TLS_LICENSE, 1629 bytes, 4 tape blocks
x postfix-2.3.8/TLS_TODO, 1065 bytes, 3 tape blocks
x postfix-2.3.8/US_PATENT_6321267, 5633 bytes, 12 tape blocks
Detected domain name is [], is it right[y/n]: y
Domain name can not be empty. Please enter the correct domain name: imsstest.com
```

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。

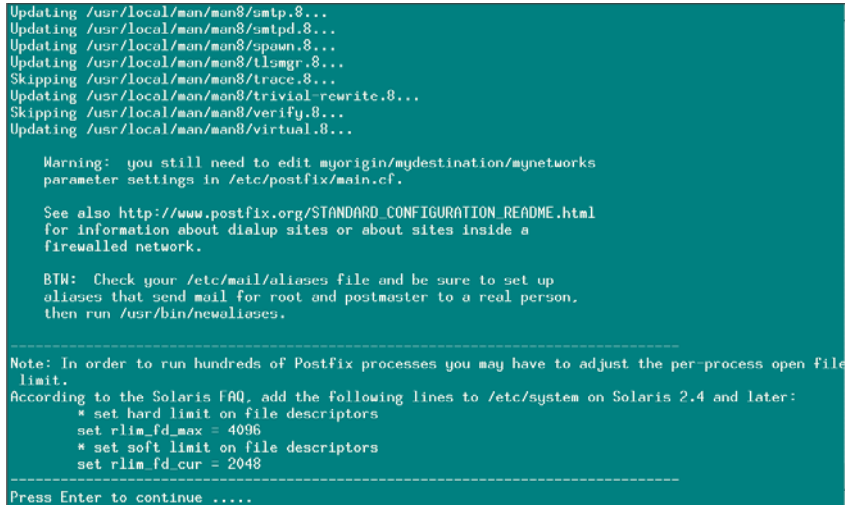
```
x postfix-2.3.8/US_PATENT_6321267, 5633 bytes, 12 tape blocks
Detected domain name is [], is it right[y/n]: y
Domain name can not be empty. Please enter the correct domain name: imsstest.com

    Warning: if you use this script to install Postfix locally, this
    script will replace existing sendmail or Postfix programs.  Make
    backups if you want to be able to recover.

    Before installing files, this script prompts you for some
    definitions.  Most definitions will be remembered, so you have to
    specify them only once. All definitions should have a reasonable
    default value.

Please specify a directory for scratch files while installing Postfix.
You must have write permission in this directory.
tempdir: [/IMSS70_TEMP_FOR_UnpackTmp/postfix-2.3.8]

Please specify the final destination directory for Postfix queues.
queue_directory: [/var/spool/postfix]

Please specify the final destination pathname for the installed Postfix
sendmail command. This is the Sendmail-compatible mail posting
interface.
sendmail_path: [/usr/lib/sendmail]

Please specify the final destination pathname for the installed Postfix
newaliases command. This is the Sendmail-compatible command to build
alias databases for the Postfix local delivery agent.
newaliases_path: [/usr/bin/newaliases]
```

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。

```
newaliases_path: [/usr/bin/newaliases]

Please specify the final destination pathname for the installed Postfix
mailq command. This is the Sendmail-compatible mail queue listing
command.
mailq_path: [/usr/bin/mailq]

Please specify the destination directory for the Postfix on-line manual
pages. You can no longer specify "no" here.
manpage_directory: [/usr/local/man]

Please specify the destination directory for the Postfix README files.
Specify "no" if you do not want to install these files.
readme_directory: [no]
Updating /usr/libexec/postfix/anvil...
Updating /usr/libexec/postfix/bounce...
Updating /usr/libexec/postfix/cleanup...
Updating /usr/libexec/postfix/discard...
Updating /usr/libexec/postfix/error...
Updating /usr/libexec/postfix/flush...
Updating /usr/libexec/postfix/local...
Updating /usr/libexec/postfix/master...
Updating /usr/libexec/postfix/oqmgr...
Updating /usr/libexec/postfix/pickup...
Updating /usr/libexec/postfix/pipe...
Updating /usr/libexec/postfix/proxymap...
Updating /usr/libexec/postfix/qmgr...
Updating /usr/libexec/postfix/qmqpd...
Updating /usr/libexec/postfix/scache...
Updating /usr/libexec/postfix/showq...
```

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、88 ページの「/etc/postfix/main.cf で次の設定を挿入または変更」および 89 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  20 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。

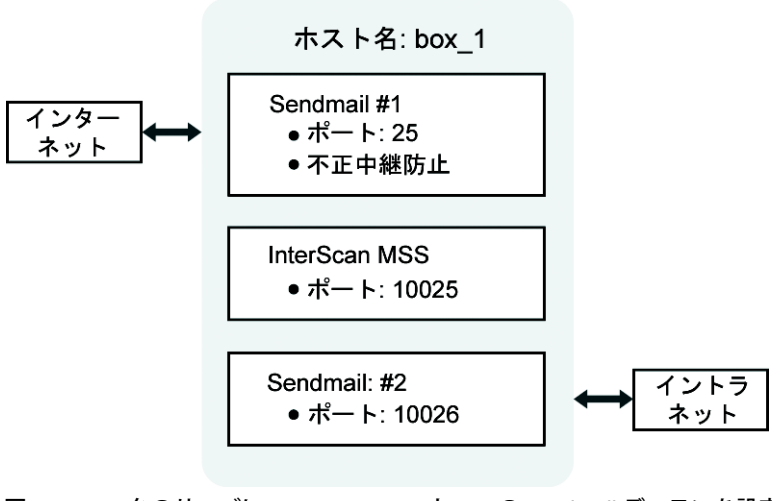


図 4-1. 1 台のサーバに InterScan MSS と 2 つの sendmail デーモンを設定

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

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

注意： Mlocal の「F」オプションに「f」フラグが設定さ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、待機するポートを 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

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

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。

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
   ```

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 では、インストールの前にメモリチェックが行われます。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。

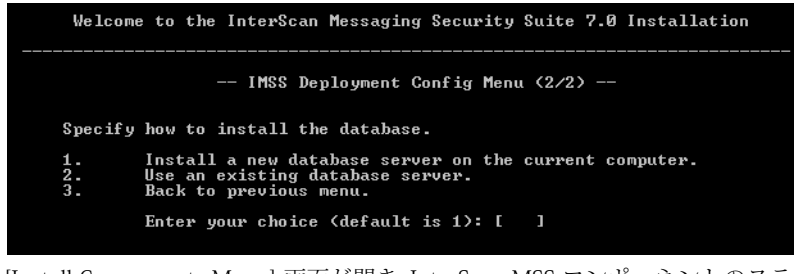
3. 「1」を入力してインストールを開始します。

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のインストールを追加する場合は、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。

- 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。
- 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。



[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、84 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。84 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、前バージョンの 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、100 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。

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、待機するポートを 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。

前バージョンからのアップグレード

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 のインストール
- 既存の設定の移行

ヒント：前バージョンの InterScan MSS の設定を移行しない場合は、既存のインストールに InterScan MSS 7.0 をインストールするのではなく、InterScan MSS を完全にアンインストールしてからインストールを実行することをお勧めします。

設定のバックアップ

以下のセクションを参照してください。

- 106 ページの「単一サーバ配置での InterScan MSS 5.1x データのバックアップ」
- 108 ページの「分散配置での InterScan MSS 5.1x データのバックアップ」

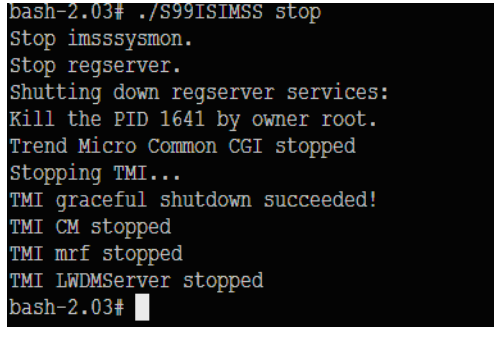
単一サーバ配置での InterScan MSS 5.1x データのバックアップ

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 のサービスを停止します。

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



2. 以下のコマンド入力して、データベースサーバ上の InterScan MSS をバックアップします。

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

imssdb.tar を安全な場所にバックアップします。

```
bash-2.03#
bash-2.03# tar -cvf imssdb.tar /var/imss
a /var/imss/ 0K
a /var/imss/pgdata/ 0K
a /var/imss/pgdata/global/ 0K
a /var/imss/pgdata/global/pg_control 8K
a /var/imss/pgdata/global/1262 8K
a /var/imss/pgdata/global/1213 8K
a /var/imss/pgdata/global/1136 8K
a /var/imss/pgdata/global/1260 8K
a /var/imss/pgdata/global/1261 0K
a /var/imss/pgdata/global/1214 1032K
a /var/imss/pgdata/global/2676 16K
a /var/imss/pgdata/global/2677 16K
a /var/imss/pgdata/global/2694 8K
a /var/imss/pgdata/global/2695 8K
a /var/imss/pgdata/global/2671 16K
a /var/imss/pgdata/global/2672 16K
a /var/imss/pgdata/global/1137 16K
a /var/imss/pgdata/global/1232 896K
a /var/imss/pgdata/global/1233 488K
a /var/imss/pgdata/global/2697 16K
a /var/imss/pgdata/global/2698 16K
a /var/imss/pgdata/global/10290 0K
a /var/imss/pgdata/global/pg_database 1K
```

3. 以下のコマンドを入力して、InterScan MSS のインストールフォルダをバックアップします。

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

imss.tar を安全な場所にバックアップします。

分散配置での InterScan MSS 5.1x データのバックアップ

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。このシナリオでは、次の 3 種類のサーバを想定しています。

- サーバ 1 - InterScan MSS 5.1x の検索サービスを実行
- サーバ 2 - InterScan MSS 5.1x データベースを実行
- サーバ 3 - InterScan 5.1x EUQ および中央レポートを実行

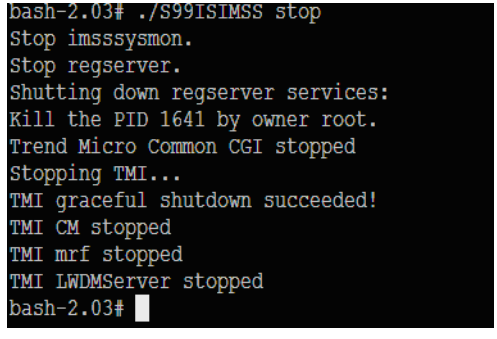
この環境では、単一サーバ配置の場合とはロールバック方法が多少異なります。

InterScan MSS 5.1x のデータをバックアップするには

サーバ 1:

1. 以下のコマンドを入力して、すべての InterScan MSS 5.1x のサービスを停止します。

   # $IMSS_HOME/script/S99ISIMSS stop



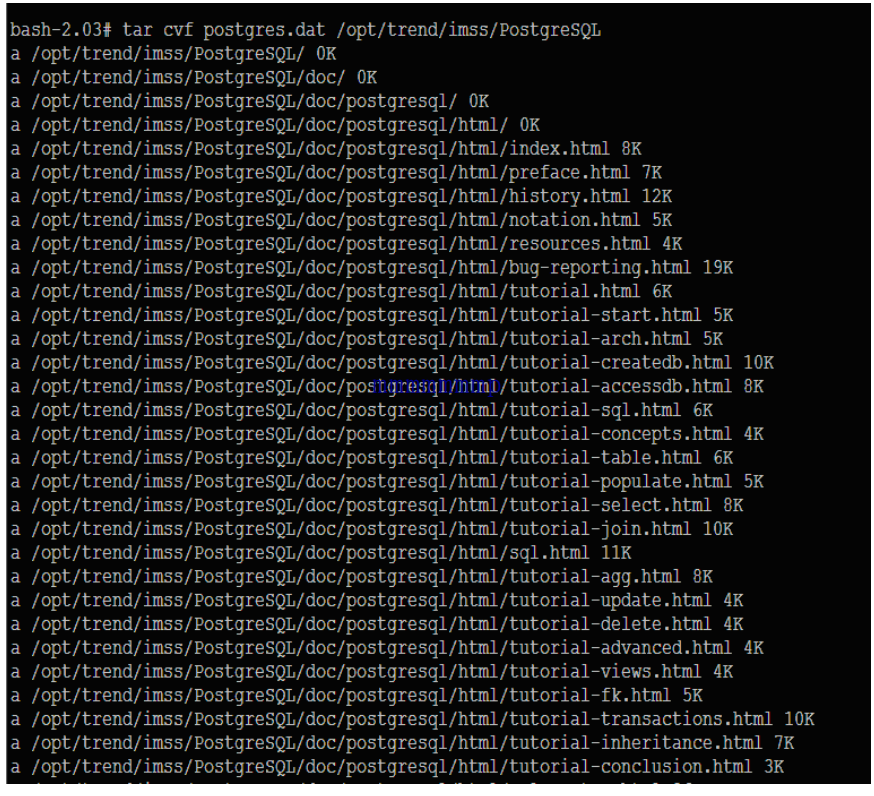
2. 以下のコマンドを入力して、InterScan MSS 5.1x のホームフォルダをバックアップします。

   # tar cvf imss.tar /opt/trend/imss
   imss.tar をバックアップします。

サーバ 2:

1. 以下のコマンドを入力して、データベースサーバ上の InterScan MSS のデータベースバイナリファイルをバックアップします。

   # tar cvf postgres.dat /opt/trend/imss/PostgreSQL



2. 以下のコマンドを入力して、InterScan MSS データベースデータをバックアップします。

   # tar cvf imssdb.tar /var/imss

```
bash-2.03#
bash-2.03# tar -cvf imssdb.tar /var/imss
a /var/imss/ 0K
a /var/imss/pgdata/ 0K
a /var/imss/pgdata/global/ 0K
a /var/imss/pgdata/global/pg_control 8K
a /var/imss/pgdata/global/1262 8K
a /var/imss/pgdata/global/1213 8K
a /var/imss/pgdata/global/1136 8K
a /var/imss/pgdata/global/1260 8K
a /var/imss/pgdata/global/1261 0K
a /var/imss/pgdata/global/1214 1032K
a /var/imss/pgdata/global/2676 16K
a /var/imss/pgdata/global/2677 16K
a /var/imss/pgdata/global/2694 8K
a /var/imss/pgdata/global/2695 8K
a /var/imss/pgdata/global/2671 16K
a /var/imss/pgdata/global/2672 16K
a /var/imss/pgdata/global/1137 16K
a /var/imss/pgdata/global/1232 896K
a /var/imss/pgdata/global/1233 488K
a /var/imss/pgdata/global/2697 16K
a /var/imss/pgdata/global/2698 16K
a /var/imss/pgdata/global/10290 0K
a /var/imss/pgdata/global/pg_database 1K
```

サーバ 3:

1. 以下のコマンドを入力して、すべての InterScan MSS 5.1x のサービスを停止します。

   $IMSS_HOME/script/S99ISIMSS stop

```
bash-2.03# ./S99ISIMSS stop
Stop imsssysmon.
Stop regserver.
Shutting down regserver services:
Kill the PID 1641 by owner root.
Trend Micro Common CGI stopped
Stopping TMI...
TMI graceful shutdown succeeded!
TMI CM stopped
TMI mrf stopped
TMI LWDMServer stopped
bash-2.03#
```

2. 以下のコマンドを入力して、InterScan MSS のインストールフォルダをバックアップします。

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

アクティベート

アップグレードが終了したら、次のアクティベーションコードを入力して製品をアクティベートします。

- 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
- アーカイブフォルダ内のメールメッセージ
- 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。

バージョン 5.1x からバージョン 7.0 への移行

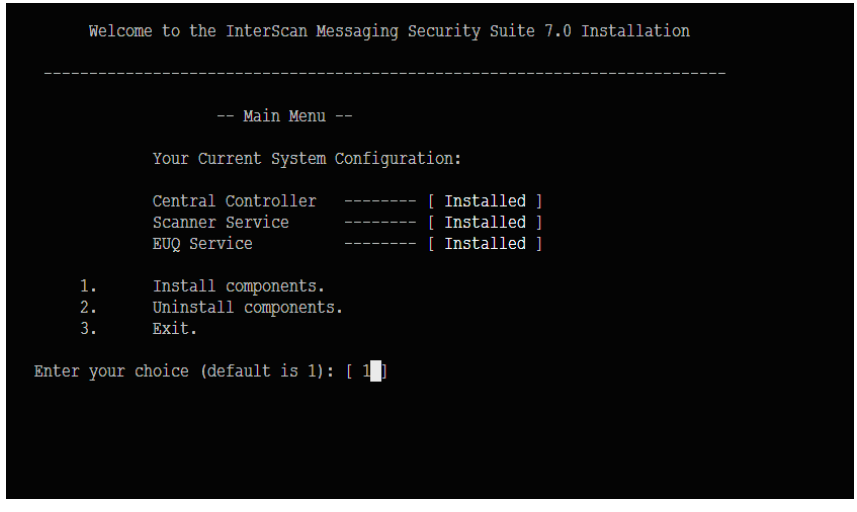
このセクションでは、InterScan MSS バージョン 5.1x からバージョン 7.0 への移行手順を説明します。

注意： 移行を実行する前に、バージョン 5.1x の設定をバックアップします。移行中に問題が発生した場合は、バージョン 5.1x にロールバックできます (123 ページの「移行のロールバック」を参照)。

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。

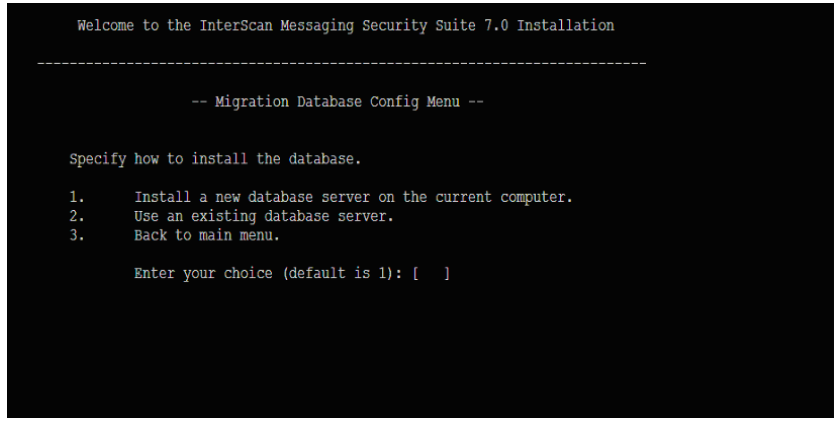
2. 「./isinst.sh」と入力します。[Main Menu] が表示されます。



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。[Database Migration Config] 画面が表示され、インストール済みのコンポーネントが検出されたことを知らせるメッセージが表示されます。

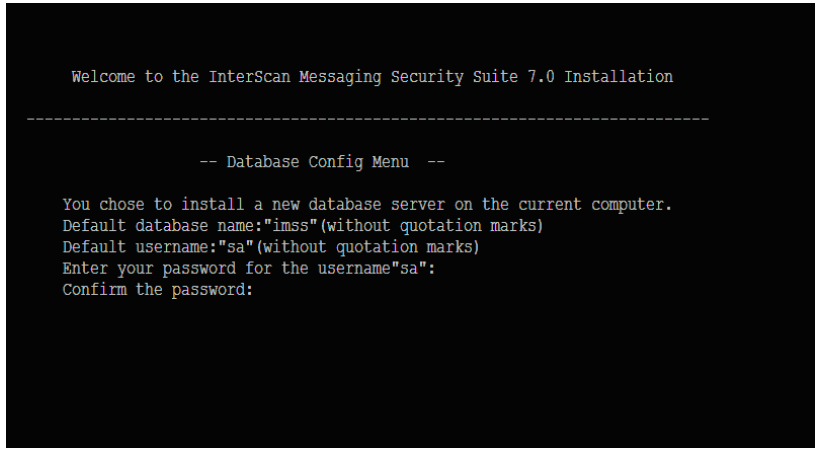
4. 「1」を入力して、「Migration Install」を選択します。[Migration Database Config menu] 画面が表示されます。

注意： 新規インストールを選択した場合、バージョン 7.0 をインストールする前に、バージョン 5.1x がアンインストールされます。

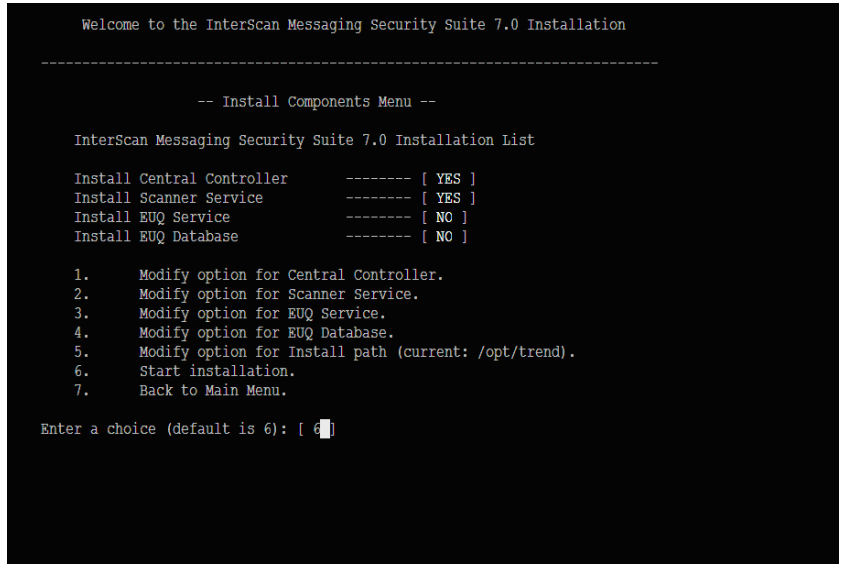


5. 「1」を入力して、新しいデータベースサーバをインストールするか、「2」を入力して、既存のデータベースサーバを使用します。

6. 「1」を入力して、新しいデータベースサーバのインストールを選択した場合、[Database Config menu] 画面が表示されます。



7. データベースユーザのパスワードを入力し、同じパスワードを確認のために再入力します。[Install Components Menu] 画面が表示され、InterScan MSS コンポーネントのステータスが表示されます。インストーラによってインストールされるコンポーネントの横には [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。



注意： バージョン 7.0 の管理データベースまたは EUQ データベースのインストールに既存のバージョン 5.1x のデータベースを使用する場合、PostgreSQL のアクセス制御を以下のように変更する必要があります。

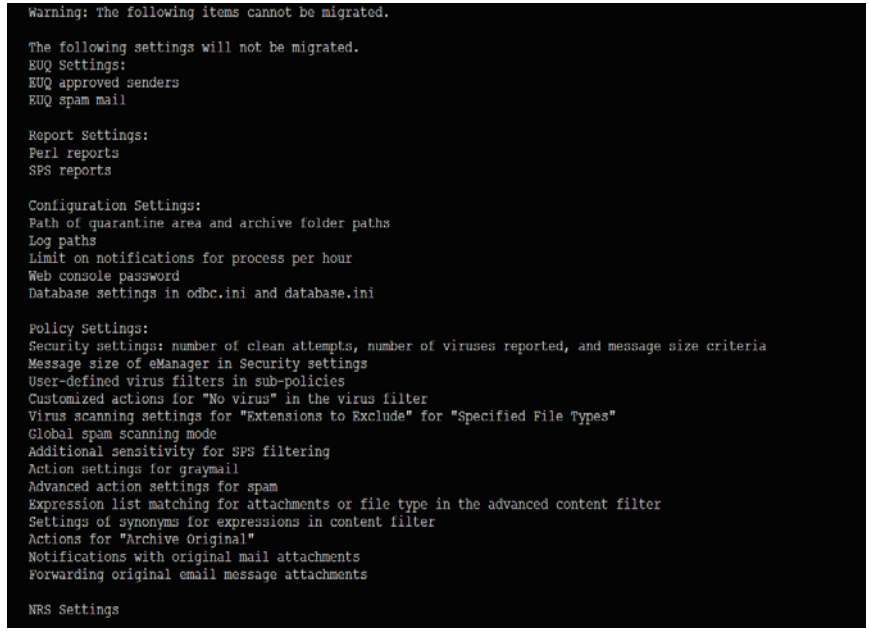
1. vi /var/imss/pgdata/pg_hba.conf
2. 60 行目の「255.255.255.255」を「255.255.255.0」に変更します。
3. 63 行目の「ffffff00」を「255.255.255.0」に変更します。
4. 変更を保存します。
5. /opt/trend/imss/script/dbctl.sh stop
6. /opt/trend/imss/script/dbctl.sh start

8. 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。インストールパスを変更できます。

EUQ サービスをインストールするには、最初にインストールされた EUQ サービス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。
EUQ 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、データベースサーバの情報を入力します。

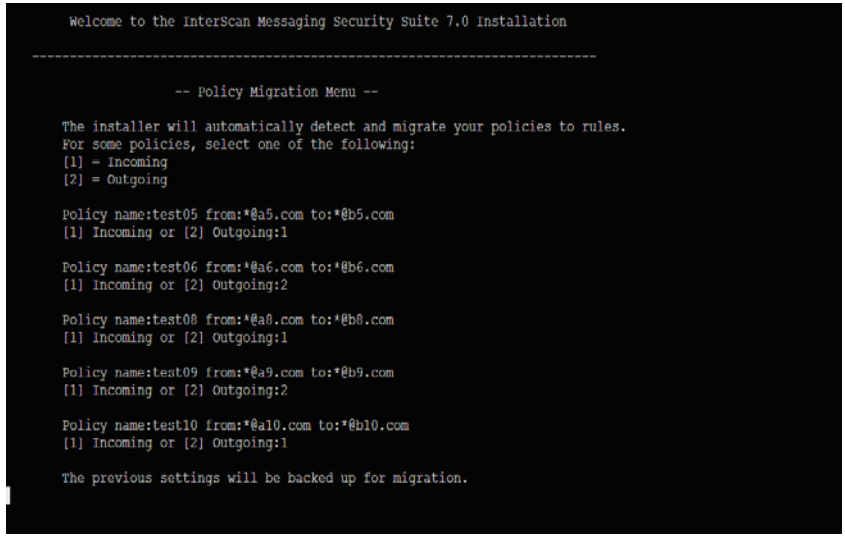
9. 「6」と入力して続行します。[Migration Information] 画面が表示されます。



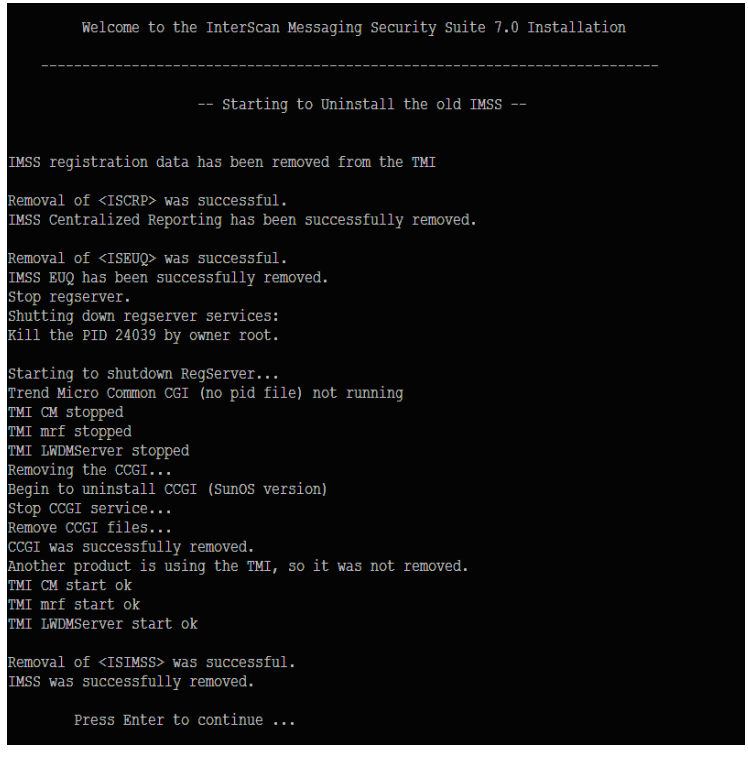
注意： 移行されない設定はこの画面で、または以下のフォルダの「GeneralReport.txt」で確認できます。
/opt/trend/installlog/MigrationReport

10. 特別なルートが設定された前バージョンの InterScan MSS 5.1x のポリシーは移行できない場合があります。このような場合は、次のいずれかを選択します。

- [1] - incoming
- [2] - outgoing



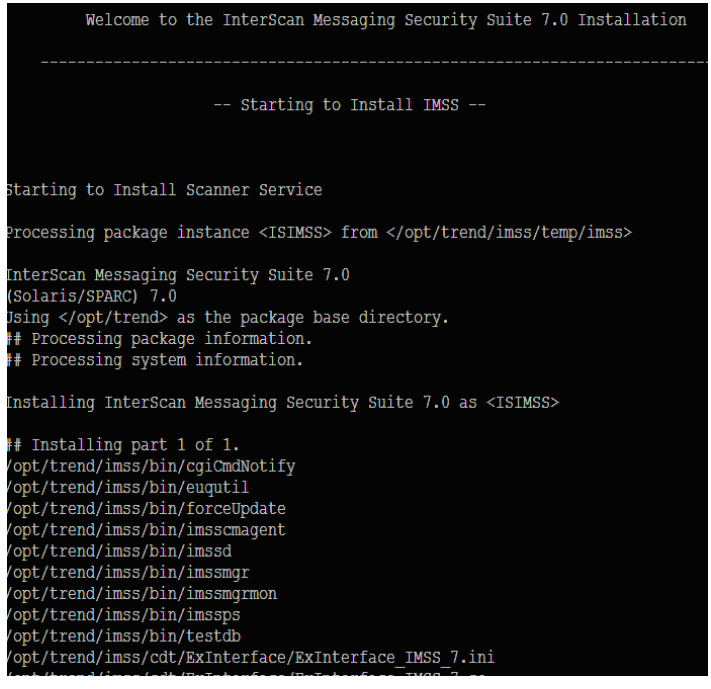
前のバージョンの InterScan MSS のアンインストール画面が表示されます。



11. <Enter> キーを押して続行します。InterScan MSS では、Postfix 設定ファイルをバックアップする前に、既存の Postfix の確認を開始します。画面の指示に従って、main.cf と master.cf の Postfix 設定を変更してください。

```
Checking Postfix ...

*************************************************************************
IMSS has backed up the Postfix configuration file in /opt/trend/installlog
Postfix 2.3.8 has been found on your computer.
Please manually change the Postfix configuration to enable the content filter interface to the IMSS scanning daemon in
 fashion:

Insert or modify the following settings to /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=20

Insert the following settings to /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 - 20 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

This information has also been stored in the installation log: /opt/trend/installlog/ImssInstall.log.
*************************************************************************
```

12. 次に、InterScan MSS のインストール画面が次のように表示されます。



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。

- 単一サーバ配置 - 移行前にバージョン 5.1x のすべてのコンポーネントが単一サーバにインストールされていた場合 (124 ページの「単一サーバ配置でのロールバック」を参照)
- 分散配置 - バージョン 5.1x のそれぞれのコンポーネントが別々のサーバにインストールされていた場合 (124 ページの「分散配置でのロールバック」を参照)

単一サーバ配置でのロールバック

バージョン 5.1x を単一サーバ配置でインストールしていた場合、次の手順に従ってください。

単一サーバ配置でバージョン 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 (126 ページの「アンインストールの実行」を参照)。
2. 以下のコマンドを入力して、InterScan MSS 5.1x のインストールフォルダを復元します。

   ```
   # tar xvf imss.tar
   ```

3. 以下のコマンドを入力して、InterScan MSS 5.1x のデータベースデータを復元します。

   ```
   # tar xvf imssdb.tar
   ```

4. 以下のコマンドを入力して、InterScan MSS 5.1x のすべてのサービスを開始します。

   ```
   # $IMSS_HOME/script/S99ISIMSS start
   # $IMSS_HOME/script/dbctl.sh start
   ```

分散配置でのロールバック

バージョン 5.1x のコンポーネントを複数のコンピュータに分散配置していた場合、次の手順に従ってください。

このシナリオでは、次の 3 種類のサーバを想定しています。

- サーバ 1 - InterScan MSS 5.1x の検索サービスとセントラルコントローラを実行
- サーバ 2 - InterScan MSS 5.1x データベースを実行
- サーバ 3 - InterScan 5.1x EUQ および中央レポートを実行

分散配置でバージョン 5.1x にロールバックするには

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 (126 ページの「アンインストールの実行」を参照)。

サーバ 1 とサーバ 3:

1. 以下のコマンドを入力して、InterScan MSS 5.1x 関連データを復元します。

   ```
   # tar xvf imss.tar
   ```

2. 以下のコマンドを入力して、すべての InterScan MSS 関連サービスを開始します。

   ```
   # /opt/trend/imss/script/S99ISIMSS start
   ```

サーバ 2:

1. pg_restore ツールを使用して、InterScan MSS 5.1x データベースデータを復元します。
2. postgres sql バイナリファイルを復元します。

   # tar xvf postgres.dat
3. データベースデータを復元します。

   # tar xvf imssdb.tar
4. postgres sql データベースを開始します。

   # /opt/trend/imss/script/dbctl.sh 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。

第 5 章

使用開始

この章では、Trend Micro InterScan Messaging Security Suite (以下、InterScan MSS) の管理コンソールへのアクセス方法について説明します。また、インストール後にすぐに実行する作業についてのヒントも示します。

この章の内容は次のとおりです。

- 130 ページの「InterScan MSS の管理コンソールを開く」
- 131 ページの「SSL を使用した管理コンソールの表示」
- 132 ページの「設定ウィザードでの基本設定の実行」
- 141 ページの「Trend Micro Network Reputation Services の使用」
- 143 ページの「NRS 管理コンソールの使用」
- 145 ページの「エンドユーザメール隔離の管理コンソールを開く」

InterScan MSS の管理コンソールを開く

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

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

- https://< サーバ IP アドレス >:8445

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

初期設定のログインアカウント情報は次のとおりです。

- ユーザ名 :admin
- パスワード :imss7.0

はじめて管理コンソールを開いたら、ログオンアカウント情報を入力し、[ログオン] ボタンをクリックします。

注意： Internet Explorer (IE) 7.0 を使用して管理コンソールにアクセスする場合、IE はアクセスをブロックし、別の Web アドレスから証明書が発行されたことを示すポップアップダイアログが表示されます。このメッセージを無視し、[このサイトの閲覧を続行する] をクリックして操作を続行します。

ヒント： ポリシーの不正改ざんを防ぐために、パスワードは定期的に変更してください。

SSL を使用した管理コンソールの表示

InterScan MSS の管理コンソールは、SSL を使用する暗号化通信をサポートしています。InterScan MSS のインストールには既定の証明書が含まれているため、インストールが終了した後は SSL 通信が実行できるようになっています。ただし、セキュリティを強化するために、独自の証明書を作成することをお勧めします。

独自の証明書を使用する場合は、次のファイルを置き換えてください。

$IMSS_HOME/UI/tomcat/sslkey/.keystore

設定ウィザードでの基本設定の実行

InterScan MSS には、InterScan MSS を実行するために必要なすべての設定項目を簡単に設定できる、設定ウィザードが用意されています。

設定ウィザードを使用するには

1. 次のいずれかの方法でウィザードにアクセスします。

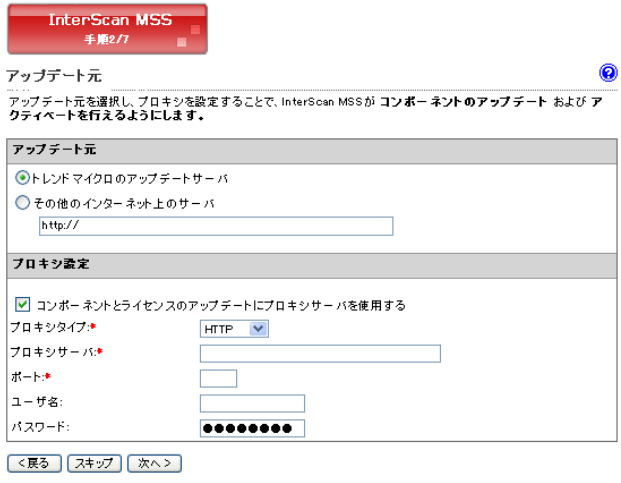
   - 管理コンソールのログオン画面で [設定ウィザードを開く] チェックボックスがオンになっていることを確認します。この状態でログオンすると、ウィザードが開きます。
   - 管理コンソールに既にログオンしている場合は、[管理]→[InterScan MSS の設定]→[設定ウィザード] の順に選択します。新しいウィンドウにウィザードが表示されます。

2. 最初の画面の内容を読んだら、[次へ] をクリックします。[通知設定] 画面が表示されます。

3. 次の通知関連の設定を行います。これらの設定は、InterScan MSS ですべての初期設定のシステム通知およびポリシーイベント通知に使用されます。

- メール設定 - 送信者および受信者のアドレス、InterScan MSS がメールの配信に使用するサーバの名前、SMTP サーバポート、文字コード、メッセージに追加するヘッダまたはフッタを入力します。
- SNMP トラップ - ネットワークに SNMP サーバが配置されている場合は、そのサーバの名前とコミュニティ名を入力します。

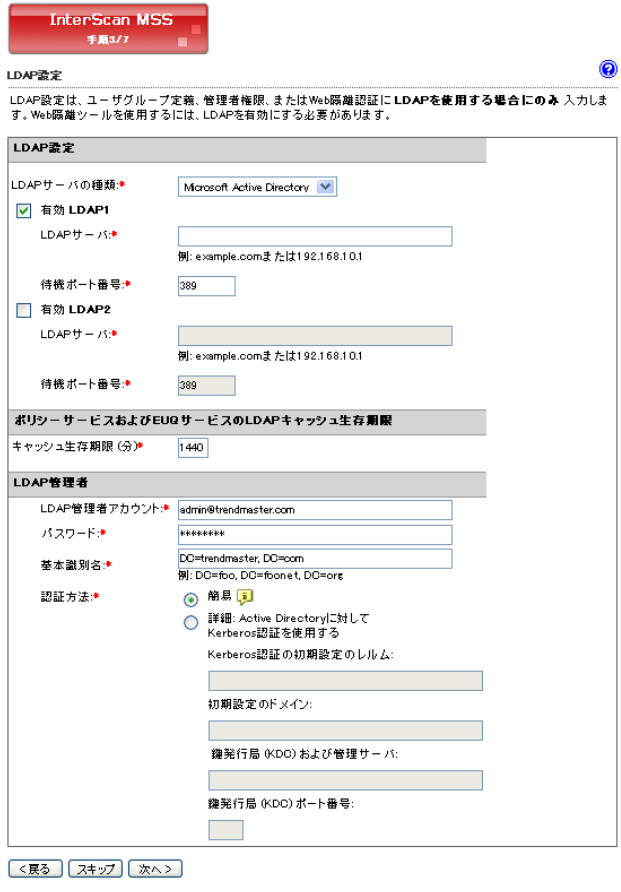
4. [次へ] をクリックします。[アップデート元] 画面が表示されます。



5. 次のアップデート設定を行います。これらの設定は、どのプロキシ (使用する場合) を介してインターネットにアクセスし、InterScan MSS が最新のコンポーネントをどこから受け取るかを定義します。

- アップデート元 - トレンドマイクロから直接アップデートを受け取る場合は、[トレンドマイクロのアップデートサーバ] をクリックします。それ以外の場合は、[その他のインターネット上のサーバ] をクリックして、Trend Micro Control Manager (以下、Control Manager) などのアップデート元の名前を入力します。
- プロキシ設定 - [コンポーネントとライセンスのアップデートにプロキシサーバを使用する] チェックボックスをオンにして、プロキシの種類、サーバ名、ポート、ユーザ名、パスワードを設定します。

6. [次へ] をクリックします。[LDAP 設定] 画面が表示されます。



7. 次の操作を行って、LDAP 設定を有効にします。

   a. [LDAP サーバの種類] の横にある次のいずれかを選択します。

      - Microsoft Active Directory
      - Domino
      - Sun iPlanet Directory

b. 片方または両方の LDAP サーバを有効にするには、[有効 LDAP1] または [有効 LDAP2] の横のチェックボックスをオンにします。

c. LDAP サーバの名前と、これらのサーバの待機ポートの番号を入力します。

d. [ポリシーサービスおよび EUQ サービスの LDAP キャッシュ生存期限] の下の [キャッシュ生存期限(分)] の横に、有効時間を表す数値を入力します。

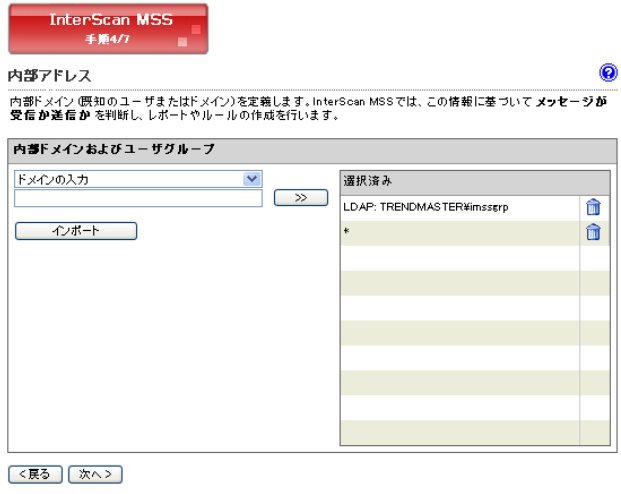
e. [LDAP 管理者] の下に、管理者アカウントとパスワード、および基本識別名を入力します。

f. [認証方法] の横にある認証方法から、[簡易]、または Active Directory の Kerberos 認証を使用する [詳細] をクリックします。[詳細] 認証を選択した場合は、Kerberos 認証の初期設定のレルム、初期設定のドメイン、KDC と管理サーバ、および KDC ポート番号を設定します。

注意： LDAP 設定は、LDAP をユーザグループの定義、管理者権限、またはエンドユーザメール隔離の認証に使用する場合のみ指定します。エンドユーザメール隔離を使用するには、LDAP を有効にする必要があります。

---

8. [次へ] をクリックします。[内部アドレス] 画面が表示されます。



9. 内部ドメイン (既知のユーザまたはドメイン) を定義します。これは、InterScan MSS がレポートとルールを作成する際に、受信および送信用のポリシーとイベントを判断するのに使用されます。ドメインを定義するには、次のいずれかを行います。

   - ドロップダウンボックスから [ドメインの入力] を選択し、テキストボックスにドメインを入力して [>>] をクリックします。
   - ドロップダウンボックスから [LDAP グループの検索] を選択します。LDAP グループを選択する画面が表示されます。検索する LDAP グループ名をテキストボックスに入力し、[検索] をクリックします。検索結果がリストボックスに表示されます。その LDAP グループ名を [選択済み] リストに追加するには、[>>] をクリックします。

10. [次へ] をクリックします。[Control Manager サーバの設定] 画面が表示されます。

11. Control Manager を使用して InterScan MSS を管理する場合は、次の操作を行います。

    a. [Control Manager エージェントを有効にする] を選択します (Control Manager エージェントは、InterScan MSS と共に既にインストールされています)。

    b. [サーバ] の横に、Control Manager の IP アドレスまたは完全修飾ドメイン名を入力します。

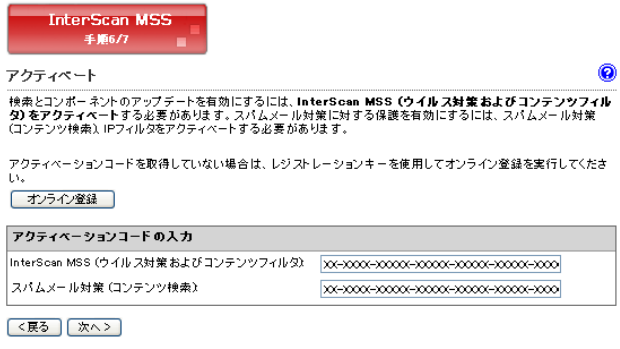
    c. [通信プロトコル] の横から [HTTP ポート番号] または [HTTPS ポート番号] を選択し、対応するポート番号を入力します。HTTP アクセス用の初期設定ポート番号は 80 で、HTTPS 用の初期設定ポート番号は 443 です。

    d. Web サーバの認証が必要な場合は、[Web サーバ認証] に Web サーバのユーザ名とパスワードを入力します。

e. InterScan MSS と Control Manager の間にプロキシサーバが配置されている場合は、[プロキシを有効にする] を選択します。

f. プロキシサーバのポート番号、ユーザ名、およびパスワードを入力します。

12. [次へ] をクリックします。[アクティベート] 画面が表示されます。検索およびアップデート機能を有効にするには、「InterScan MSS (ウイルス対策およびコンテンツフィルタ)」をアクティベートする必要があります。



13. 製品のアクティベーションコードを入力します。

14. [次へ] をクリックします。[設定の概要] 画面が表示されます。

15. 設定が正しい場合は、[完了] をクリックします。

    設定を変更する場合は、[戻る] をクリックしながら画面を移動して、設定を変更してください。

Trend Micro Network Reputation Services の使用

Trend Micro Network Reputation Services (以下、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。

ヒント： メッセージングインフラストラクチャの最前線の防御として、NRS のインストールをお勧めします。

ほとんどのメールメッセージングシステムには、通常、既存の DNS ブロック機能、スパムメールフィルタ機能、ウイルスフィルタ機能などの多層構造が備わっていますが、他の DNS ブロック機能はメッセージング環境から完全に削除することをお勧めします。NRS は、使用されるすべてのアプリケーションフィルタ機能よりも先行して動作する必要があります。

スパムメール対策のアクティベーションコードの使用

スパムメール対策 (コンテンツ検索) の製品版を購入すると、アクティベーションコードが発行されます。このアクティベーションコードを使用して、NRS をアクティベートすることができます。

NRS の設定

NRS のアクティベートは、NRS のインストール時に実行します (100 ページの「IP フィルタのインストール」を参照)。

NRS を使用するには

1. メニューから [IP フィルタ]→[NRS] の順に選択します。
2. [有効にする] チェックボックスをオンにします。

3. 次のいずれかの横にあるラジオボタンをクリックします。

   - 初期設定の推奨処理 - NRS は、RBL+Service との一致に対しては接続を永続的に拒否 (応答コード : 550) し、Network Anti-Spam Service (QIL) のデータベースに一致する接続に対しては一時的拒否（応答コード : 450）をします。
   - 一致するすべての接続に対して適用する処理
     - SMTP エラーコード - 特定の SMTP コードの接続をすべて拒否します。SMTP コードを入力します。

4. [保存] をクリックします。

NRS で使用するための MTA の準備

MTA を準備して NRS で使用するには

- Trend Micro RBL+ Service - 550 レベルエラーコード (Connection refused) で接続を拒否するように MTA を設定します。このエラーコードは、肯定応答を RBL+ データベースから受信したことを示しています。RBL+ データベースには、スパムメール送信者またはメール送信をすべきでない送信元のリストが含まれます。このリストに含まれる送信者からのメールの標準的な処理方法は、接続を全面的に拒否することです。

  詳細については、次の URL を参照してください。

  http://www.trendmicro.com/jp/products/nrs/rbl/evaluate/overview.htm

- Trend Micro Network Anti-Spam Service - 2 つの DNS クエリを実行するように MTA を設定します。QIL データベースが肯定応答を受信しない場合、MTA は 2 番目のクエリを RBL+ データベースに行う必要があります。

  MTA は、450 レベルのエラーコード (server temporarily unavailable, please retry) で接続を一時的に拒否します。その際、肯定応答をこのデータベースから受信します。このデータベースのリストには、正規のメールサーバが存在することがあります。そのメールサーバには背後に信用できないホストが存在し、一時的にスパムメールを送信することがあります。接続要求が正規のメールサーバからのものである場合、それは再度キューに入り、後でメッセージの送信を試行します。これによ

り、そのリストの期限が切れるまでメールの配信が少し遅れますが、そのメールが永遠にブロックされることはありません。

詳細については、次の URL を参照してください。

http://www.trendmicro.com/jp/products/nrs/nas/evaluate/overview.htm

NRS 管理コンソールの使用

グローバルスパムメール情報へのアクセス、レポートの表示、承認済み送信者 IP リストおよびブロックする送信者 IP リストの作成または管理、管理作業の実行を行う場合は、NRS 管理コンソールにログオンします。

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

NRS 管理コンソールを使用するには

1. Web ブラウザを開き、次のアドレスにアクセスします。

   https://nrs.nssg.trendmicro.com/

2. メニューから [グローバルスパムメール情報] を選択します。
3. 次のいずれかのタブをクリックします。

   - スパムメールアラート : 現在のスパムメールの手口に関する簡単な概要と説明、および企業に対する影響を示します。新しい手口がどのように配置されているか、この手口がどのようにトレンドマイクロシステムを通過するように設計されたかを説明し、さらにこの新しい手口に対してトレンドマイクロがどのように対応しているかについても説明します。
   - ISP スパム TOP.x: 特定の週内に上位 100 の ISP から送信されたスパムメールの総量。一番多くのスパムメールを送信しているネットワークが上位にランク付けられます。ISP のランクは毎日変わります。

4. MTA と NRS データベースサーバ間のクエリの動作をまとめたレポートを表示するには、以下を実行します。

   a. メニューから [レポート] を選択します。

   b. [クエリの割合]、[1 時間あたりのクエリ数]、または [1 日あたりのクエリ数] をクリックします。

5. 承認済み送信者 IP リストおよびブロックする送信者 IP リストを作成または管理するには、メニューから [ポリシー] を選択します。国別または ISP 別の個々の IP アドレスおよび CIDR ごとに、承認済み送信者を定義できます。

6. ISP をリストに追加するには、メニューから [新規 ISP のリクエスト] を選択します。

パスワードまたはアクティベーションコードを変更するには、メニューから [管理] を選択します。

エンドユーザメール隔離の管理コンソールを開く

エンドユーザメール隔離の管理コンソールは、プログラムがインストールされたコンピュータから、またはネットワークを介してリモートで表示できます。

ネットワーク上の他のコンピュータから管理コンソールを表示するには、次の URL にアクセスします。

- プライマリエンドユーザメール隔離サービス - https://< サーバ IP アドレス >:8447
- セカンダリエンドユーザメール隔離サービス - https://< サーバ IP アドレス >:8446

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

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

ログインアカウント情報は次のとおりです。

- ユーザ名 :{ ユーザ名 @ ドメイン名 }
- パスワード

第 6 章

設定

この章では、Trend Micro InterScan Messaging Security Suite (以下、InterScan MSS) の設定について説明します。

- 148 ページの「IP フィルタの設定」
- 155 ページの「SMTP ルーティングの設定」
- 161 ページの「ポリシーの追加」
- 172 ページの「隔離およびアーカイブの管理」

IP フィルタの設定

IP フィルタサービスには、Network Reputation Service (以下、NRS) と IP プロファイラという、2 つのコンポーネントがあります。

- NRS は、接続層でスパムメール送信者をフィルタします。
- IP プロファイラは、高度なプロファイル (SMTP IDS) を使用してメールサーバを攻撃から保護します。

スパムメール対策 (コンテンツ検索) の製品版を購入すると、アクティベーションコードが発行されます。このアクティベーションコードを使用して、NRS をアクティベートすることができます。

ヒント： メッセージングインフラストラクチャの最前線の防御として、IP フィルタのインストールをお勧めします。たいていのメールメッセージングシステムには、通常、既存の DNS ブロック機能、スパムメールフィルタ機能、ウイルスフィルタ機能などの多層構造が備わっていますが、他の DNS ブロック機能はメッセージング環境から完全に削除することをお勧めします。IP フィルタは、使用されるすべてのアプリケーションフィルタ機能よりも先行して動作する必要があります。

IP フィルタを完全に設定するには、次の手順を実行します。

手順 1:NRS および IP プロファイラの有効化
手順 2:IP プロファイラのルールの有効化
手順 3:NRS の設定
手順 4:IP アドレスの承認済みリストへの追加
手順 5:IP アドレスのブロックリストへの追加

手順 1: NRS および IP プロファイラの有効化

NRS および IP プロファイラを有効化するには

1. メニューから、[IP フィルタ]→[概要] の順に選択します。[IP フィルタの概要] 画面が表示されます。

2. [IP フィルタを有効にする] チェックボックスをオンにします。同時に、[NRS] および [IP プロファイラ] がオンになります。
3. 必要がなければ、[NRS] または [IP プロファイラ] チェックボックスをオフにします。
4. [保存] をクリックします。

手順 2: IP プロファイラのルールの有効化

IP プロファイラは、4 種類の攻撃を防御できます。

IP プロファイラのルールを有効化するには

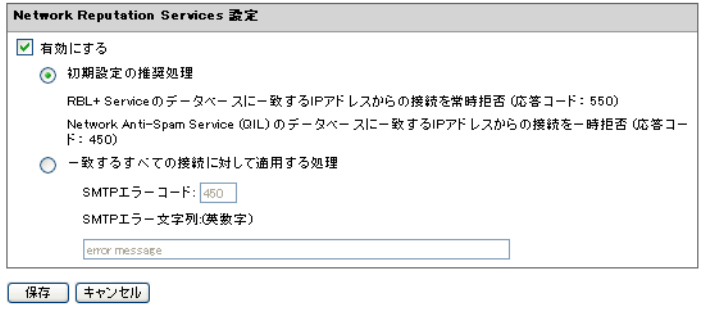
1. メニューから、[IP フィルタ]→[ルール] の順に選択します。[ルール] 画面が表示されます。

2. 防御の対象となる脅威のタブを選択します。
3. [有効にする] チェックボックスをオンにします。
4. 必要なパラメータを指定します (詳細については、オンラインヘルプを参照してください)。
5. [保存] をクリックします。

手順 3: NRS の設定

NRS を設定するには

1. メニューから、[IP フィルタ]→[NRS] の順に選択します。[NRS] 画面が表示されます。



2. [有効にする] チェックボックスをオンにします。
3. 必要な設定を行います (詳細については、オンラインヘルプを参照してください)。
4. [保存] をクリックします。

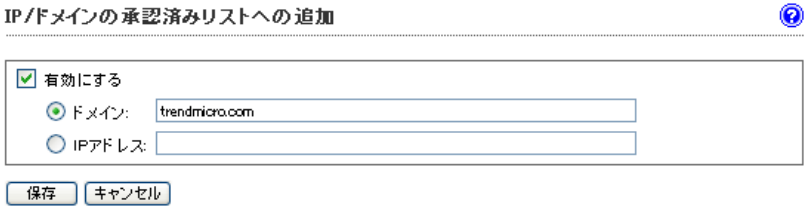
手順 4: IP アドレスの承認済みリストへの追加

InterScan MSS では、承認済みリストに表示されている IP アドレスやドメインはフィルタされません。

承認済みリストに IP アドレスを追加するには

1. メニューから、[IP フィルタ]→[承認済みリスト] の順に選択します。[承認済みリスト] 画面が表示されます。

2. [追加] をクリックします。[IP/ ドメインの承認済みリストへの追加] 画面が表示されます。



3. [有効にする] チェックボックスをオンにします。
4. 承認済みリストに追加するドメインまたは IP アドレスを入力します。
5. [保存] をクリックします。承認済みリストに指定したドメインが表示されます。

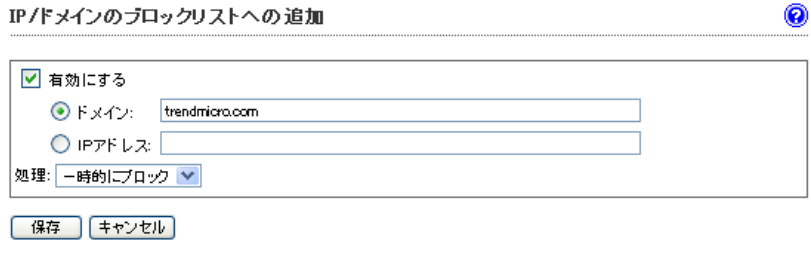
手順 5: IP アドレスのブロックリストへの追加

InterScan MSS では、ブロックリストに表示される IP アドレスがブロックされます。

ブロックリストに IP アドレスを追加するには

1. メニューから、[IP フィルタ]→[ブロックリスト] の順に選択します。[ブロックリスト] 画面が表示されます。

2. [追加] をクリックします。[IP/ ドメインのブロックリストへの追加] 画面が表示されます。



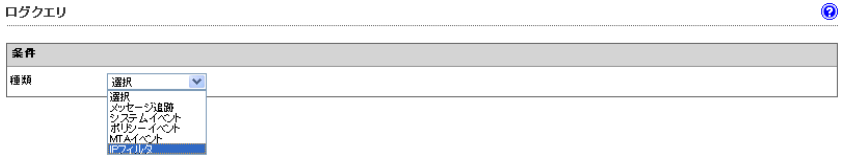
3. [有効にする] チェックボックスをオンにします。
4. ドメインまたは IP アドレスを入力します。
5. [一時的にブロック] または [常にブロック] を選択します。
6. [保存] をクリックします。ドメインがブロックリストに追加されます。

IP フィルタのログのクエリ

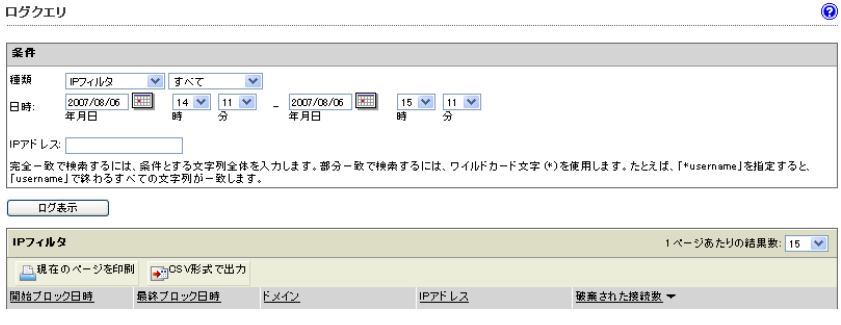
IP フィルタでは、ネットワークでイベントが発生したときに、これらのイベントをログに記録します。IP フィルタの処理履歴をクエリできます。

IP フィルタをクエリするには

1. メニューから、[ログ]→[クエリ] の順に選択します。[ログクエリ] 画面が表示されます。
2. [種類] として、[IP フィルタ] を選択します。



3. 検索データを指定します (すべてのデータを表示するには、空欄のままにしておきます)。初期設定では、完全一致で検索されます。複数の異なる条件を指定する場合は「; (セミコロン)」で区切ります。
4. [ログ表示] をクリックして、結果を確認します。



SMTP ルーティングの設定

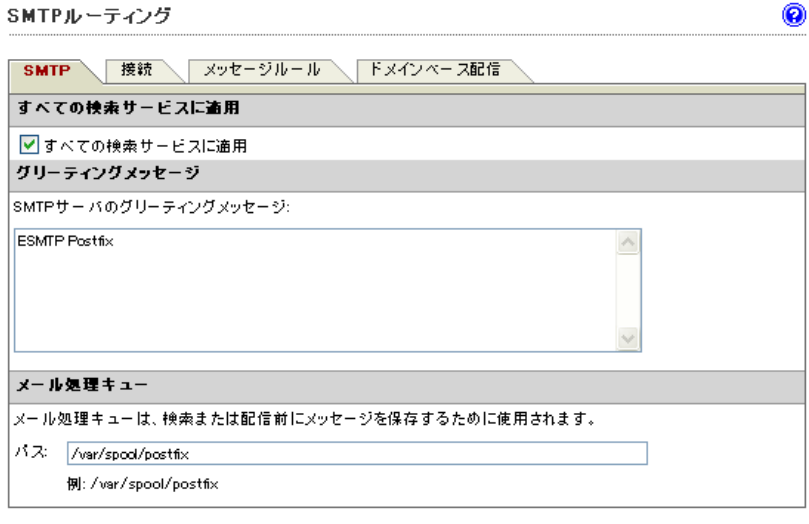
IP フィルタを完全に設定するには、次の手順を実行します。

手順 1:[SMTP] タブの設定
手順 2:[接続] タブの設定
手順 3:[メッセージルール] タブの設定
手順 4:[ドメインベース配信] タブの設定

SMTP ルーティングの SMTP の設定

SMTP の設定を指定するには

1. メニューから、[管理]→[InterScan MSS の設定]→[SMTP ルーティング] を選択します。[[SMTP ルーティング] 画面が表示されます。



2. [すべての検索サービスに適用] チェックボックスをオンにします。
3. [SMTP サーバのグリーティングメッセージ] (セッションの作成時に表示されるもの) を指定します。

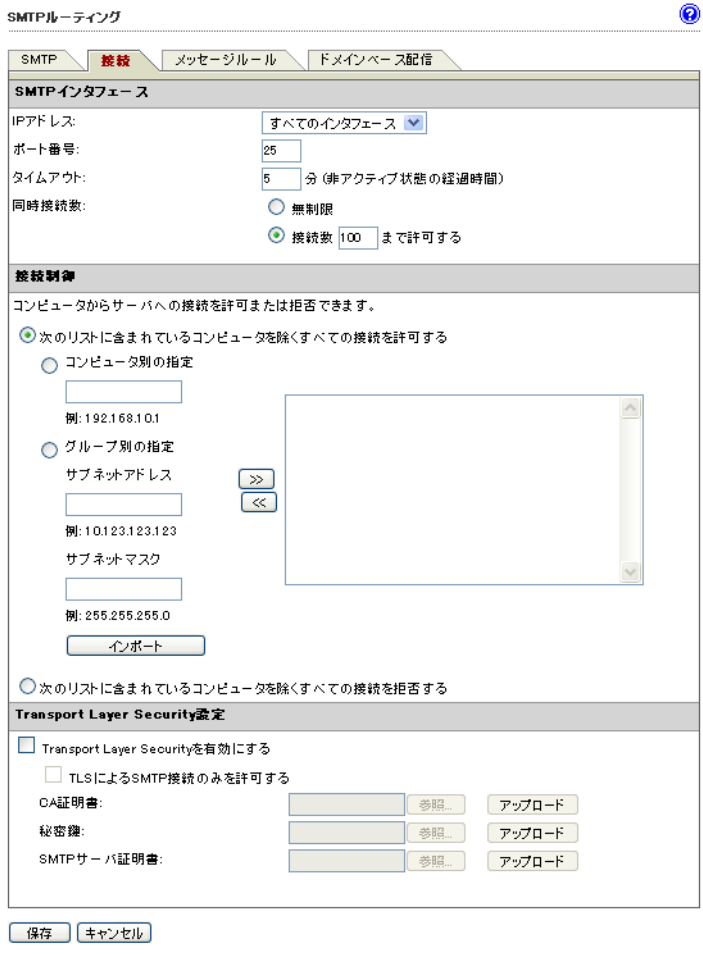
4. [メール処理キュー] の [パス] を指定します。
5. [保存] をクリックします。

SMTP ルーティングの接続の設定

接続の設定を指定するには

1. メニューから、[管理]→[InterScan MSS の設定]→[SMTP ルーティング] を選択します。

2. [接続] タブをクリックします。[接続] 画面が表示されます。



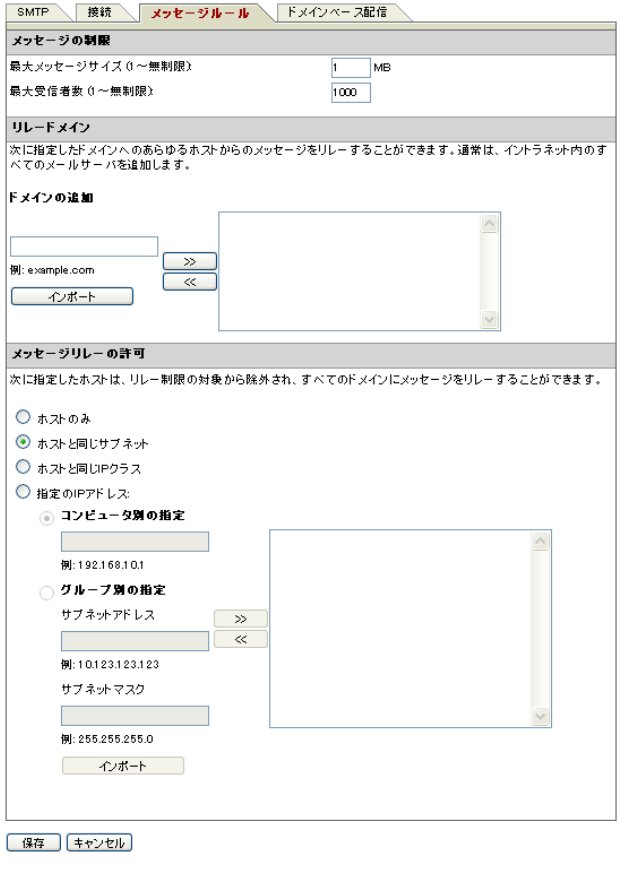
3. [SMTP インタフェース] および [接続制御] のパラメータを指定します。
4. [Transport Layer Security 設定] のパラメータを指定します。
5. [保存] をクリックします。

SMTP ルーティングのメッセージルールの設定

メッセージルールを指定するには

1. メニューから、[管理]→[InterScan MSS の設定]→[SMTP ルーティング] を選択します。

2. [メッセージルール] タブをクリックします。[メッセージルール] 画面が表示されます。



3. [メッセージの制限] のパラメータを指定します。

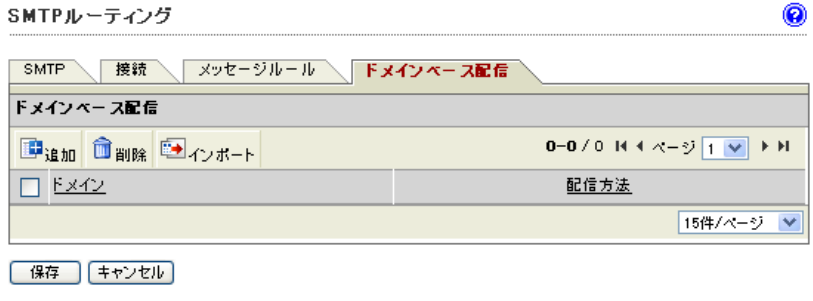
4. [リレードメイン] を指定します。InterScan MSS は、リストされている IP からリストされているドメインにメッセージをリレーします。
5. [メッセージリレーの許可] を指定します。
6. [保存] をクリックします。

SMTP ルーティングのドメインベース配信の設定

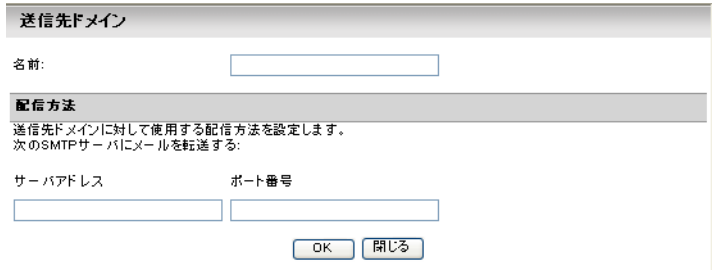
配信の次の段階に関する設定を行います。InterScan MSS は、受信者のメールドメインを検索して、一致したドメインの次の SMTP ホストにメールを送信します。

ドメインベースの配信を指定するには

1. メニューから、[管理]→[InterScan MSS の設定]→[SMTP ルーティング] を選択します。
2. [ドメインベース配信] タブをクリックします。[ドメインベース配信] 画面が表示されます。



3. [追加] をクリックします。[送信先ドメイン] 画面が表示されます。



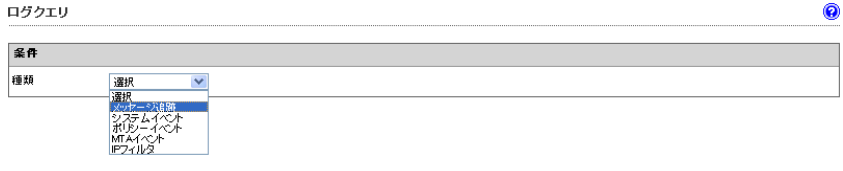
4. [送信先ドメイン] および [配信方法] を指定します。
5. [OK] をクリックします。
6. [保存] をクリックします。

メッセージ追跡

InterScan MSS は、すべてのメッセージアクティビティを追跡します。メッセージアクティビティはすべて、メッセージ追跡のログからクエリできます。

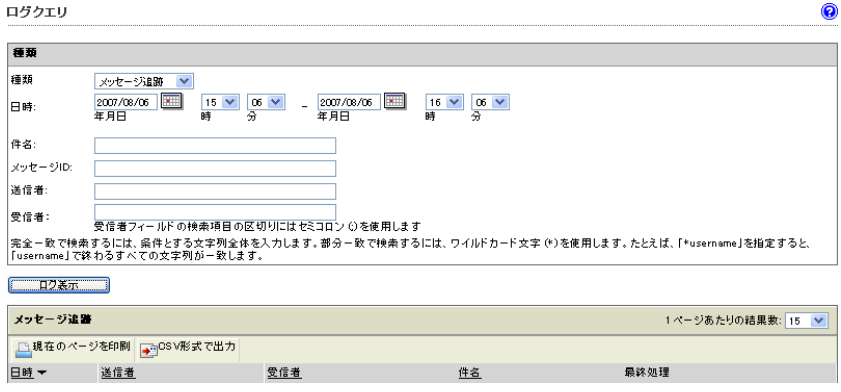
メッセージ追跡のログを表示するには

1. メニューから、[ログ]→[クエリ] の順に選択します。[ログクエリ] 画面が表示されます。
2. [種類] リストから [メッセージ追跡] を選択します。



3. 必要なパラメータを入力します。

4. [ログ表示] をクリックします。



ポリシーの追加

このセクションでは、ポリシーの作成、編集、および表示方法について説明します。

ポリシーを作成するには、次の 4 つの手順が必要です。

手順 1:ルートの指定
手順 2:検索条件の指定
手順 3:処理の指定
手順 4:優先順位の指定

既存のポリシーの表示

既存のポリシーを表示するには

1. メニューから、[ポリシー]→[ポリシーリスト] の順に選択します。[ポリシー] 画面が表示されます。

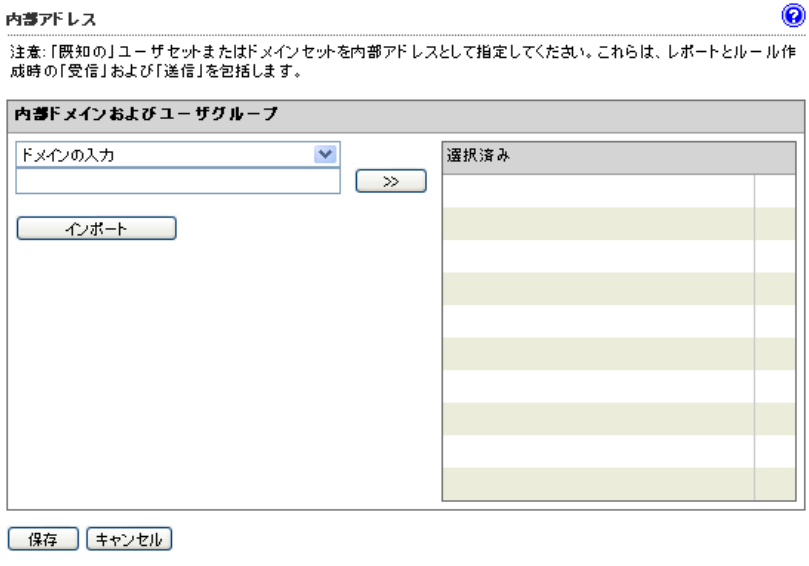
2. [グローバルウイルス対策ルール] をクリックして、既に設定されているウイルス対策ポリシーを表示します。

内部アドレスの設定

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

内部アドレスを設定するには

1. メニューから、[ポリシー]→[内部アドレス] の順に選択します。[内部アドレス] 画面が表示されます。

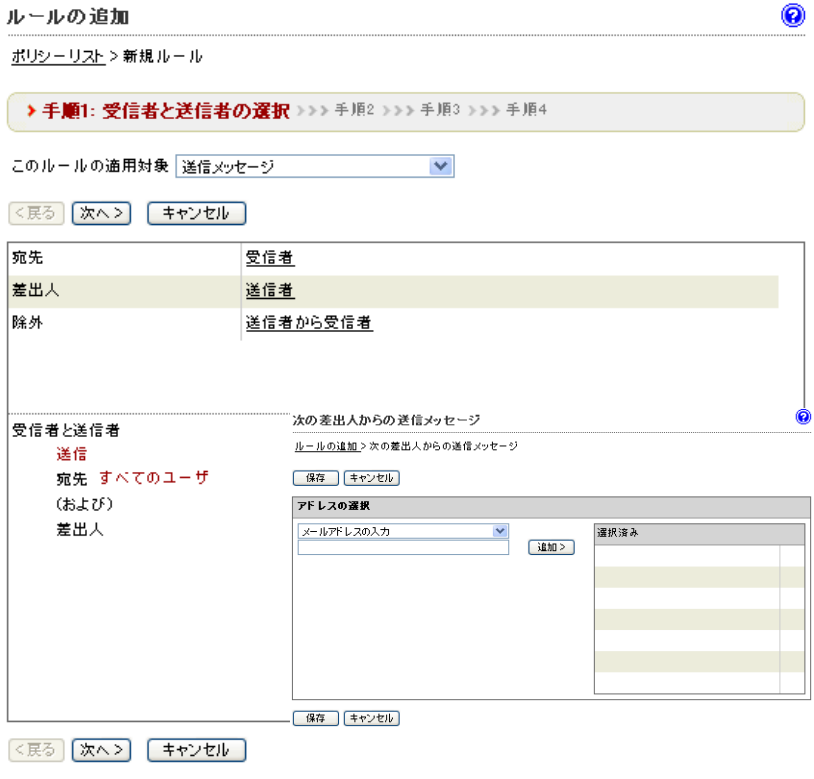


2. 内部アドレスとして扱うアドレスを追加します。
3. [保存] をクリックします。

ルートの指定

新しいポリシーを追加するには

1. メニューから、[ポリシー]→[ポリシーリスト] の順に選択します。[ポリシーリスト] 画面が表示されます。
2. [追加] をクリックします。[ルールの追加] 画面が表示されます。



3. ポリシーのルートの種類を選択します。

4. 受信者と送信者を選択します。

   - 受信メッセージの場合は、内部アドレスの範囲内にある、受信者のアドレスを指定します(例 : 内部アドレスは「*@example.com」で、有効な受信者は「jim@example.com」、「bob@example.com」などです)。
   - 送信メッセージの場合は、内部アドレスの範囲内にある、送信者のアドレスを指定します(例 : 内部アドレスは「*@example.com」で、有効な送信者は「jim@example.com」、「bob@example.com」などです)。
   - 受信メッセージと送信メッセージの両方の場合において、ルールは、メールアドレスに一致する受信者または送信者に適用されます。

検索条件の指定

検索条件を指定するには

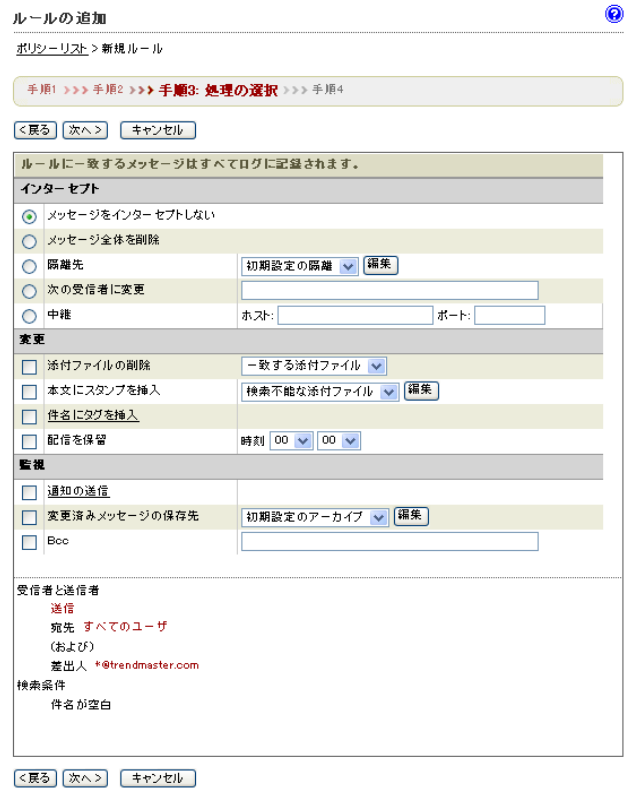
1. [次へ] をクリックします。[手順 2: 検索条件の選択] 画面が表示されます。

2. 使用する検索ルールを指定します。

処理の指定

メッセージに対する処理を設定します。これにより、InterScan MSS のルールが起動します。

1. [次へ] をクリックします。[手順 3: 処理の選択] 画面が表示されます。



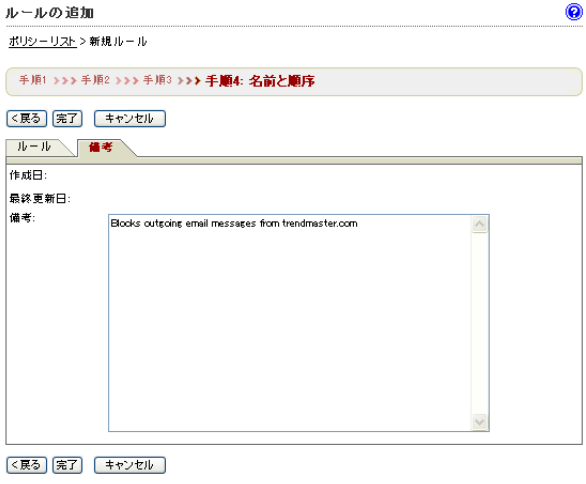
2. メッセージに対して実行する処理を指定します。

優先順位の指定

1. [次へ] をクリックします。[手順 4: 名前と順序] 画面が表示されます。

2. [有効] チェックボックスをオンにして、ルールを有効にします。
3. [ルール名] フィールドにルールの名前を入力します。
4. [順序番号] フィールドに、検索を実行する優先順位を指定します。指定した順番でメッセージにルールが適用されます。

5. [備考] タブをクリックします。[備考] 画面が表示されます。

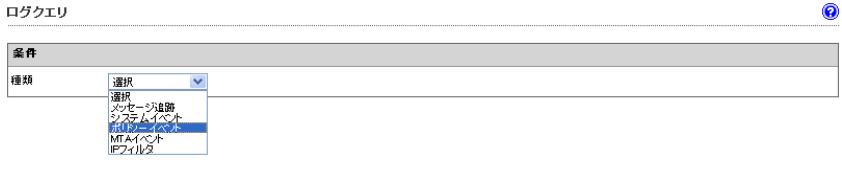


6. 新しいルールに対する備考を追加します。
7. [完了] をクリックします。

ポリシーイベントのログのクエリ

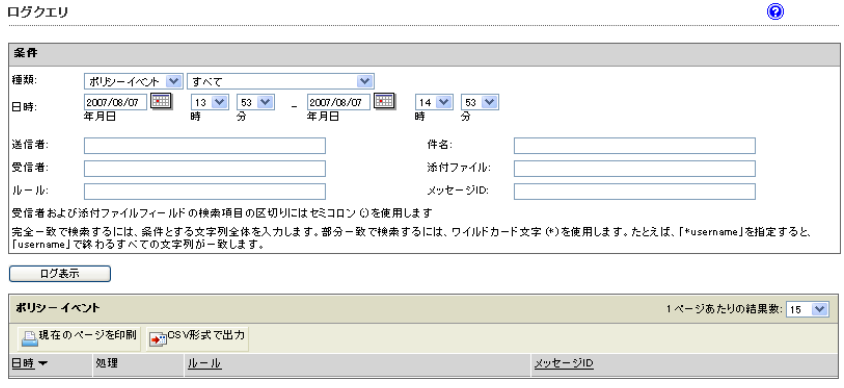
ポリシーイベントのログをクエリするには

1. メニューから、[ログ]→[クエリ] の順に選択します。
2. [種類] として、[ポリシーイベント] を選択します。



3. 必要なパラメータを入力します。

4. [ログ表示] をクリックします。

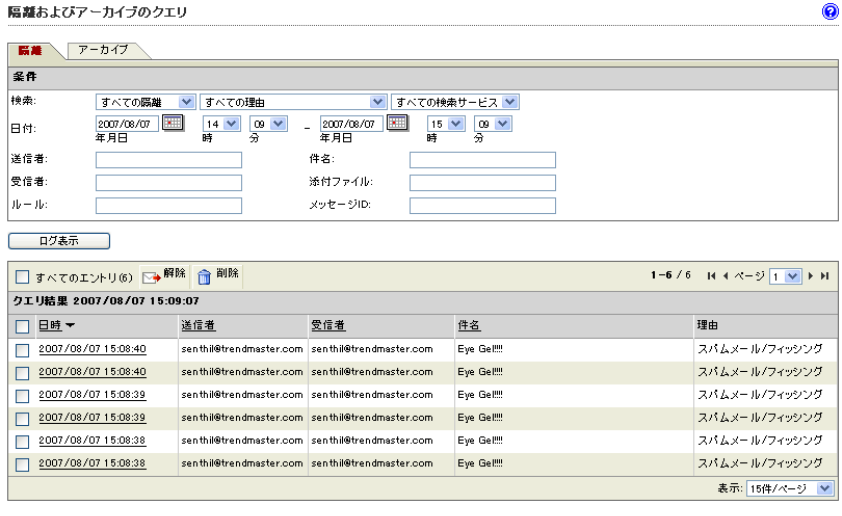


隔離およびアーカイブの管理

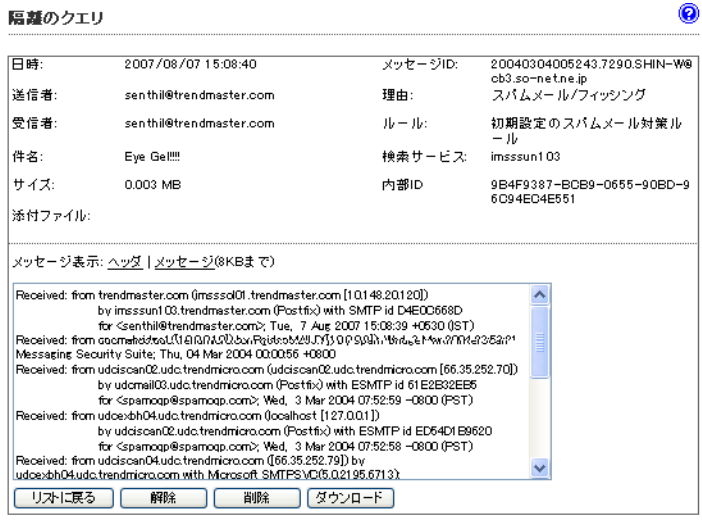
隔離されたメッセージを、InterScan MSS から解除または削除することができます。アーカイブされたメッセージを、InterScan MSS から削除することも可能です。

隔離されたメールを管理するには

1. メニューから、[隔離およびアーカイブ]→[クエリ] の順に選択します。[隔離およびアーカイブのクエリ] 画面が表示されます。
2. [隔離] タブで、検索条件を指定します。
3. [ログ表示] をクリックします。



4. 結果アイテムをクリックします。アイテムの詳細が [隔離のクエリ] 画面に表示されます。



5. [解除] をクリックすると、アイテムが隔離から解除されます。

エンドユーザメール隔離データベースの追加 / 削除

既存のエンドユーザメール隔離データベースがある場合、またはさらに多くのエンドユーザがこのデータベースにアクセスできるようにする必要がある場合は、新しいエンドユーザメール隔離データベースを追加して、負荷を分散することができます。また、エンドユーザメール隔離データベースの数を減らすことも可能です。

エンドユーザメール隔離データベースの追加

エンドユーザメール隔離データベースを追加するには、次の手順を実行します。

手順 1:エンドユーザメール隔離データベースの設定
手順 2:エンドユーザデータの再構築

手順 1: エンドユーザメール隔離データベースの設定

エンドユーザメール隔離データベースは既にインストールされているがまだ登録されていないという場合は、管理コンソールからこのデータベースを登録できます。それ以外の場合は、InterScan MSS のインストールプログラムを実行して、新しいエンドユーザメール隔離データベースをシステムに追加してください。

手順 2: エンドユーザデータの再構築

元のエンドユーザのデータをそのまま保持するには、セントラルコントローラの $IMSS_HOME/script ディレクトリから、euqtrans スクリプトを実行し、エンドユーザメール隔離データベースの負荷を再分散します。このスクリプトは以下の操作を実行します。

- 承認済みリストの転送

- 隔離されたメールに関する情報の転送

注意： 新しいエンドユーザメール隔離データベースの追加後、euqtrans スクリプトを実行しない場合、エンドユーザは、以前隔離したメールメッセージの一部にアクセスできない可能性があります。

エンドユーザメール隔離データベースの削除

エンドユーザメール隔離データベースを削除するには、次の手順を実行します。

手順 1:エンドユーザメール隔離データベースの削除
手順 2:エンドユーザデータの再構築

手順 1: エンドユーザメール隔離データベースの削除

管理コンソールを使用して、システムからエンドユーザメール隔離データベースの登録を解除することはできますが、削除することはできません。データベースの登録を解除するということは、データベースはそのまま残りますが、InterScan MSS により使用されることはなくなるということを意味します。

手順 2: エンドユーザデータの再構築

セントラルコントローラの $IMSS_HOME/script ディレクトリから、euqtrans スクリプトを実行して、承認済み送信者リストと、隔離されたメールメッセージに関する情報をこのデータベースから別のデータベースに移動し、移動先のデータベースの負荷を再分散します。

euqtrans ツールのコマンドラインオプション

euqtrans スクリプトには、以下のコマンドラインオプションがあります。

all — 個々の承認済み送信者リストと、隔離されたメールメッセージに関する情報を、更新後のテーブルおよびデータベースマッピングに基づいて、削除されたデータベースから新しい場所 (データベース) に転送します。

approvedsender — 個々の承認済み送信者リストを、新しいマッピングに基づいて、削除されたデータベースから新しい場所 (データベース) に転送します。

第 7 章

ログとレポート

この章では、ログへのアクセス、および Trend Micro InterScan Messaging Security Suite (以下、InterScan MSS) でネットワークに関して提供されるデータを使用したレポートの作成について説明します。この章の内容は、次のとおりです。

- 178 ページの「InterScan MSS のログのクエリ」
- 180 ページの「1 回限りのレポートの作成」
- 183 ページの「予約レポートの設定」

InterScan MSS のログのクエリ

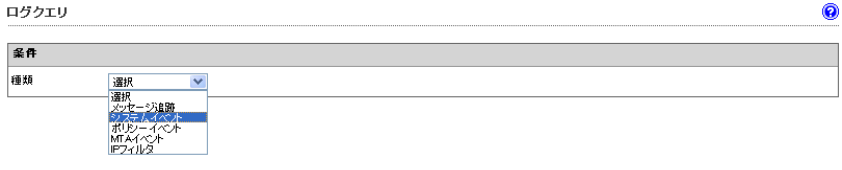
InterScan MSS では、クエリを実行するために次の 5 種類のログが用意されています。

- メッセージ追跡
- システムイベント
- ポリシーイベント
- MTA ログ
- IP フィルタ

InterScan MSS では、大部分のログのクエリに対して、ワイルドカード (*) と完全一致をサポートしています (たとえば、名前に A または B を含むメール受信者を表示するには、受信者を「*A*;*B*」に設定します)。初期設定では、完全一致が使用されます。検索条件を空欄にしておくと、すべてのログが表示されます。複数条件のアイテムがある場合は、セミコロン (;) を使用して、受信者と添付ファイルのエントリを区切ります。

ログをクエリするには

1. メニューから、[ログ]→[クエリ] の順に選択します。[ログクエリ] 画面が表示されます。
2. [種類] ドロップダウンリストで、クエリするログの種類を選択します。



3. クエリの詳細を指定します。

4. [ログ表示] をクリックします。

1 回限りのレポートの作成

1 回限りのレポートを作成すると、ネットワークのトラフィックを監視するのに役立ちます。

1 回限りのレポートを作成するには

1. メニューから、[レポート]→[1 回限りのレポート] の順に選択します。

2. [追加] をクリックします。

3. 必要な情報を指定します。

4. [保存] をクリックします。レポートの作成に数分かかります。レポートテーブルに、「処理中」というメッセージが表示されます。

レポート作成後に、ハイパーリンク [HTML] および [CSV] がレポートテーブルに表示されます。

5. レポートを HTML 形式で表示するには、[HTML] をクリックします。

6. データを csv ファイルにエクスポートするには、[CSV] をクリックします。

予約レポートの設定

指定した設定に従って予約レポートが自動的に作成されます。

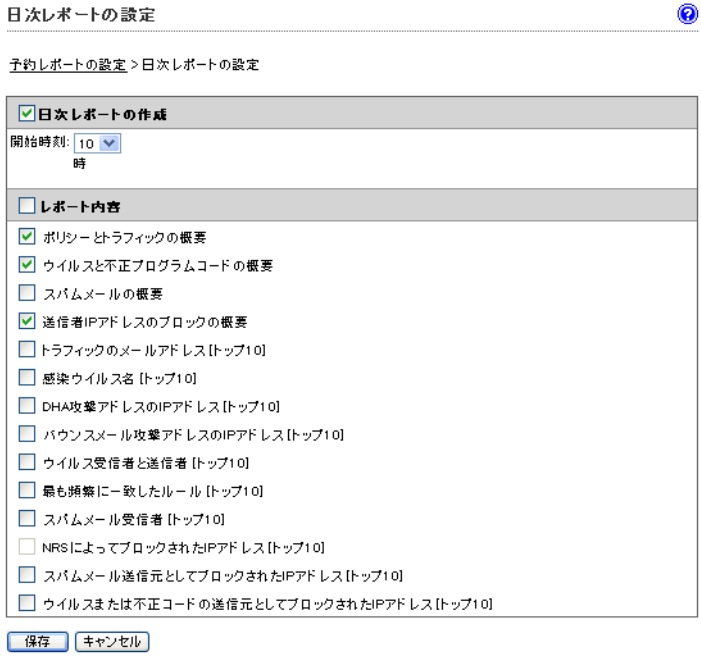
予約レポートを作成するには

1. メニューから、[レポート]→[設定] の順に選択します。[予約レポートの設定] 画面が表示されます。

2. 次のいずれかから [設定] リンクをクリックします。

   - 日次レポート
   - 週次レポート
   - 月次レポート

   [レポート設定] 画面が表示されます。



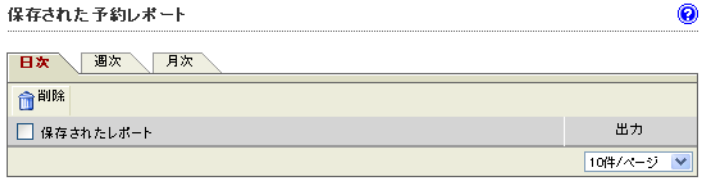
3. レポートの設定を指定します。

4. [保存] をクリックします。レポートのステータスが変更されます。

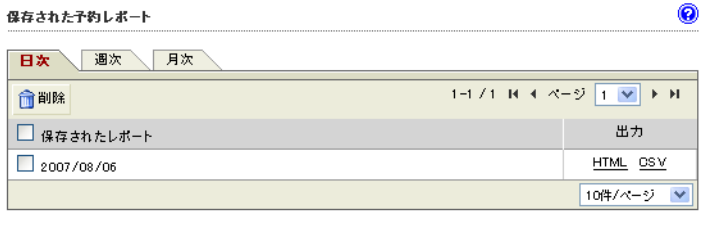
5. [保存] をクリックします。

6. メニューから、[レポート]→[予約レポート] の順に選択します。[予約レポート] 画面が表示されます。

注意： レポートはまだ作成されていません。



7. レポート作成後に、[HTML] または [CSV] をクリックするとレポートを表示できます。



第 8 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。

- 188 ページの「トラブルシューティング」
- 197 ページの「よくある質問 (Q&A)」
- 215 ページの「製品サポート情報」
- 215 ページの「サポートサービスについて」
- 216 ページの「製品 Q&A のご案内」
- 217 ページの「セキュリティ情報」
- 219 ページの「ウイルス解析サポートセンター「TrendLabs」」

トラブルシューティング

表 8-1 に、InterScan MSS で発生する可能性のある問題の一般的なトラブルシューティングの方法を示します。解決策についても、この表を参照してください。この表を見ても問題が解決しない場合は、トレンドマイクロの製品 Q&A を確認してください。

問題	推奨される解決策
一般的な問題	
管理コンソールまたはその他のコンポーネントにアクセスできない	ターゲットポートがファイアウォール承認済みリストに存在していません。ファイアウォールで 196 ページの表 8-2 に示されるポートを開きます。
管理コンソールへのアクセスが行われない	管理コンソールの URL が、Internet Explorer で信頼されたサイトではありません。URL を信頼されたサイトに追加します。
imssps デーモンは実行中だが、接続を拒否する	imssps デーモンが実行中の場合、ポリシーサービスが機能しています。ポリシーサービスと検索サービス間の接続を確認して、LDAP 設定を確認してください。

表 8-1. 問題のトラブルシューティング

問題	推奨される解決策
製品 (InterScan MSS、スパムメール対策、IP フィルタ) を起動できない、またはコンポーネントをアップデートできない	ネットワークにプロキシサーバが使用されている場合は、プロキシ設定を確認してください。 Trend Micro Network Reputation Services (以下、NRS) を起動するには、InterScan MSS をトレンドマイクロに接続する必要があります。この処理には、DNS クエリが必要です。したがって、DNS サーバが使用できなかったり、接続に問題がある場合は、起動に失敗します。 DNS サーバの設定を確認してください。 **管理コンソールから DNS の設定を確認するには** **1.** メニューから [管理] → [アップデート] の順に選択します。初期設定では [スケジュール] タブが表示されます。 **2.** [アップデート元] タブをクリックします。 **3.** プロキシを設定します。 **4.** [保存] をクリックします。
メール通知が正しく表示されない	通知メッセージに ASCII 以外の文字を使用している場合、通知メッセージの文字コードが正しく設定されていないと文字化けする場合があります。管理コンソールで、適切な文字コードを設定してください。 **文字セットを変更するには** **1.** 管理コンソールメニューから、[管理] → [通知] → [通知設定] の順に選択します。 **2.** [文字コード] の横から、メッセージをエンコードする際の言語を選択します。
InterScan MSS でメッセージログをクエリできない	InterScan MSS 検索サービスでは、ログをローカル時刻で記録します。メッセージログをクエリするには、すべてのコンピュータの日時を InterScan MSS と同期させます。

表 8-1. 問題のトラブルシューティング

問題	推奨される解決策
[概要] 画面でサーバが切断されていると表示される	管理対象サーバは、次のいずれかの理由で切断される場合があります。 ・ 検索サービスがネットワークから削除されていた。 ・ InterScan MSS マネージャサービスが停止していた。 ・ ネットワーク接続の問題。 マネージャサービス待機ポートのファイアウォール設定を確認します。[管理]→[InterScan MSS の設定]→[接続]→[コンポーネント]→[InterScan MSS マネージャポート] の順にクリックします。
隔離されたメールまたはアーカイブされたメールの詳細な情報を表示する場合は、添付ファイルの情報を利用できないことがある	起動されたルールが添付ファイルに関するものであった場合にのみ、InterScan MSS では添付ファイル情報が記録されます。InterScan MSS でメールが隔離された理由を確認してください。
InterScan MSS でメールが受信されない	別のアプリケーションが、必要なポートを使用しています。ポート 25 を解放します。
サービスが通常通り実行されない	データベースが起動していないか、または管理者サービスが起動した後でデータベースが起動しました。すべての InterScan MSS サービスを再起動します。

表 8-1. 問題のトラブルシューティング

問題	推奨される解決策
エンドユーザメール隔離の問題	
エンドユーザメール隔離管理コンソールにアクセスできない	次の項目を実行してください。 **1.** 正しいURLとポート番号を使用していることを確認します。ネットワーク上の他のコンピュータからエンドユーザメール隔離管理コンソールを表示するには、次の URL にアクセスします。 ・ プライマリエンドユーザメール隔離サービス - https://<**サーバ IP アドレス**>:8447 ・ セカンダリエンドユーザメール隔離サービス - https://<**サーバ IP アドレス**>:8446 **2.** ネットワーク上の各エンドユーザメール隔離サービスのシステム時間が同期されていることを確認します。
ユーザがエンドユーザメール隔離管理コンソールにログインできない	次の項目を実行してください。 **1.** LDAP サーバで、ユーザアカウントが適切なグループにあることを確認してください。承認済みグループのユーザアカウントのみが、エンドユーザメール隔離にアクセスできます。 **2.** LDAP とユーザメール隔離アクセスの設定を InterScan MSS 管理コンソールで確認してください。 **a.** [管理] → [InterScan MSS の設定] → [接続] → [LDAP] の順に選択します。 **b.** すべての設定内容、特に LDAP の種類とサーバ情報を確認してください。 **c.** [管理] → [ユーザ隔離アクセス] の順に選択します。 **d.** [ユーザ隔離アクセス] を有効にします。 **e.** 適切な LDAP グループが [選択したグループ] の下に表示されていることを確認します。 **3.** ユーザが適切なログイン名とパスワードを使用していることを確認します。
エンドユーザメール隔離通知が隔離されたメールの情報を正しく表示しない	文字セットが適切であることを確認してください。 **1.** [管理] → [通知] → [設定] の順に選択します。 **2.** [文字コード] の横から、通知情報を適切に表示する文字セットを選択します。

表 8-1. 問題のトラブルシューティング

問題	推奨される解決策
隔離されたメールメッセージの一部がエンドユーザメール隔離管理コンソールに表示されない	エンドユーザメール隔離管理コンソールからアクセスできるのは、InterScan MSS がスパムメールまたはフィッシングメールと判定したメールのみです。 エンドユーザメール隔離管理コンソールでは、ウイルス対策ルールなどルールに違反した隔離メールを表示できません。
Kerberos 認証で LDAP を有効にできない	Kerberos プロトコルでは、Kerberos サーバと InterScan MSS の間で時間を同期させる必要があります。 すべてのコンピュータの日時を InterScan MSS と同期させます。
IP フィルタの問題	
Foxproxy が起動しない	Foxproxy が起動しない理由は、複数あります。理由を調べるには、IP プロファイラのログを表示します。 **IP プロファイラのログを表示するには** **1.** IP プロファイラの設定ファイルがあるディレクトリに移動します (初期設定 : /opt/trend/ipprofiler/config)。 **2.** foxproxy.ini を開きます。 **3.** log_level の値を 4 に変更します。 **4.** Foxproxy を再起動するには、次のように入力します。 /opt/trend/ipprofiler/script/foxproxyd restart **5.** ログファイルを開くには、次のように入力します。 /opt/trend/ipprofiler/logs/foxproxy-general.****
Foxproxy に接続できない	Foxproxy が稼働中で、ポート 25 にバインドしていることを確認します。
Foxproxy のメールメッセージの処理が遅い	Foxproxy がメールを受信すると、FoxDNS で DNS クエリを実行します。BIND サービスが稼働していない場合、Foxproxy は DNS クエリがタイムアウトになるまで待機し続けます。 **FoxDNS がインストールされているコンピュータで BIND サービスが稼働していることを確認** **1.** 次のコマンドを入力します。 ps -ef | grep named **2.** サービスが稼働していない場合は、起動します。

表 8-1.　問題のトラブルシューティング

問題	推奨される解決策
Foxproxy がブロックしている接続を表示できない	5 分ごとに、Foxproxy はブロックされた接続に関する情報を InterScan MSS サーバに送信します。 接続情報が表示されるまで、少なくとも 5 分間待機してください。 **この時間の値を変更するには** **1.** foxproxy.ini を開きます。 **2.** report_send_interval の値を変更します。
FoxDNS が機能しない	**BIND サービスが稼動していることを確認** **1.** 次のコマンドを入力します。 ps -ef | grep named **2.** サービスが稼働していない場合は、起動します。
IP プロファイラのログ情報がまったくない	次の IP プロファイラ関連のログファイルは、InterScan MSS 管理データベースにあります。 ・ foxmsg.**** ・ foxnullmsg.**** ・ foxreport.**** **次の手順で、ログファイルが存在することを確認** **1.** InterScan MSSがインストールされているディレクトリに移動します (初期設定 : /opt/trend/imss/log/)。 **2.** ファイルが存在しない場合、次のコマンドを使用して、InterScan マネージャが稼働しているかどうかを確認します。 ps -ef | grep imssmgr **3.** 次のコマンドで、Foxproxy が稼働しているかどうかを確認します。 ps -ef |grep foxproxy **4.** IP プロファイラが有効になっていることを確認します。InterScan MSS データベースの「t_foxhuntersetting」テーブル内で、次のように表示されている必要があります。 record: `Type' = 1 and 'enable' = TRUE

表 8-1.　問題のトラブルシューティング

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。
管理コンソールから NRS を有効にした後で、NRS が機能しない	NRS が機能しない理由として、次の可能性が考えられます。 ・ スパムメール対策が有効になっていません。NRS はスパムメール対策と同じアクティベーションコードを共有しています。スパムメール対策が有効になっていない場合は、スパムメール対策を有効にしてから NRS を有効にします。 ・ 検索サービスがインストールされているコンピュータは、インターネットにアクセスできません。MTA はアクティベーションコードの検証に関する DNS クエリの応答を取得できません。検索サービスをインストールしているコンピュータが、インターネットへアクセスできることを確認してください。 スパムメール対策を有効にして、スパムメール対策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 8-1.　問題のトラブルシューティング

問題	推奨される解決策
管理コンソールの [SMTP ルーティング] 画面上の MTA 設定が Postfix 設定ファイルに書き込まれない	初期設定では、[SMTP ルーティング] 画面の設定では Postfix に書き込まれません。次の手順に従って、この機能を有効にします。 InterScan MSS 設定ディレクトリに移動します (初期設定 : /opt/trend/imss/config)。 InterScan MSS 設定ファイル imss.ini を開きます。 enable_postset_thd の値を [yes] に変更するか、空欄のままにします。 次のコマンドを使用して、InterScan MSS Manager を再起動します。 /opt/trend/imss/script/S99MANAGER restart
IP プロファイラがブロックリストの IP アドレスをブロックしない	変更が有効になるまで 1 分ほどかかります。 1 分お待ちください。
ブロックされた IP アドレスが [概要] ページに表示されない	[概要] ページには、過去 24 時間の上位 10 のブロックされた IP アドレスが種類別に表示されます。たとえば、本日の 16:12 時点では、[概要] ページには、昨日の 16:00 から本日の 16:00 までのデータが表示されます。 1 時間後に [概要] ページを表示してください。

表 8-1.　問題のトラブルシューティング

モジュール	ポート	説明
Admin UI	8445	Tomcat 待機ポート (HTTPS)
Bind	53	ネームドメインサーバ
EUQ UI	8009	Tomcat AJP (負荷分散) ポート
EUQ UI	8446	Tomcat 待機ポート
EUQ UI	8447	負荷分散用
マネージャ	15505	SOAP サーバ
MTA	25	SMTP
MTA	465	SSMTP (SSL)
ポリシーサーバ	5060	SOAP 待機ポート
検索サービス	110	POP3 待機ポート

表 8-2.　コンポーネントで使用されるポート

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 を一元管理する方法はありますか。一部の Postfix 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

インストールとアンインストール

InterScan MSS 管理データベースは個別にインストールできますか。

はい。InterScan MSS 管理データベースは個別に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 のポリシーと InterScan MSS 7.0 のルールの間のマッピング関係はどのようになっていますか。

マッピング関係については、次の詳細な移行レポートに記載されています。

$IMSS_Home/installlog/MigrationReport/DetailReport.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。

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、123 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。

InterScan MSS コンポーネント

セントラルコントローラをあるコンピュータから別のコンピュータへ移動できますか。

はい。まず、InterScan MSS インストールスクリプトを実行して、セントラルコントローラをコンピュータからアンインストールします。次に、InterScan MSS インストールスクリプトを実行して、セントラルコントローラを別のコンピュータにインストールします。

どのようにデータベースを設定、管理できますか？

以下のコマンドを使用して、データベースを管理できます。

- pg_dump imss > YYMMDD.HHMMSS.backup : データベースをバックアップします。
- psql imss < YYMMDD.HHMMSS.backup : エラーが発生した場合に、最新のデータを取り出します。
- vacuum : 頻繁にアクセスされるテーブルまたは大量のデータがあるテーブル上のデータベースをクリーンナップします。メールトラフィックが小さい、またはデバイスがネットワークに接続されていないときに使用します。
- vacuumfull : データベースの使用頻度が高くない、またはデバイスがネットワークに接続されていないときに、データベース全体をクリーンナップします。
- redirect_stderr= and log_rotate_***= : 古いデータベースログエントリをシステムログにリダイレクトする場合は、postgresql.conf でこれらのオプションを有効にします。ログファイルにダッシュ「-」で始まる名前を付けることができます。

IP フィルタやその他のログデータは SQL を使用して削除することもできます。また、管理コンソールの [ログ]→[設定] 画面でログの保存期間を設定できます。

NRS

特定の IP アドレスまたはドメインをブロックしないようにするには、NRS をどのように設定するのですか。

IP アドレスまたはドメインを NRS の承認済みリストに追加します。追加の手順は、次のとおりです。

- 管理コンソールにログオンします。
- [IP フィルタ]→[承認済みリスト] の順にクリックします。
- ブロックされない IP アドレスまたはドメインを承認済みリストに追加します。

IP プロファイラ

Foxproxy ログを削除するにはどうしたらいいですか。

ログ削除プログラムが IP プロファイラのインストールディレクトリ内にあります (初期設定 : /opt/trend/ipprofiler/script/foxpurgelog)。
ログの削除機能に関する設定は設定ファイル foxproxy.ini に記載されています。キーは次のとおりです。

- log_purge
- log_purge_unit
- log_purge_num

Foxproxy の機能が停止したとき、どのように復旧されますか。

Foxproxy は、マルチプロセスプログラムです。メインプロセスは、子プロセスのみを監視します。子プロセスの機能が停止した場合、メインプロセスが対応します。ただし、メインプロセスの機能が停止している場合には、子プロセスには復旧措置が取られません。
Foxproxy で問題が発生した場合には、メインプロセスが実行中であることを確認してください。

DNS クエリはどのように実行されますか？

DNS クエリは、検索サービスから直接実行されます。

DNS サーバは、セントラルコントローラのインストール時に一緒にインストールされます。IP プロファイラをインストールすると、DNS サーバがセントラルコントローラにあることを、インストールスクリプトが IP プロファイラに通知します。

ブロックリストまたは承認済みリストに追加された IP アドレスのドメイン名が常に表示されていないのはなぜですか。

InterScan MSS では、ブロックリストまたは承認済みリストに追加された IP アドレスのドメイン名は解決されません (追加されたドメイン名の IP アドレスは InterScan MSS によって解決されます)。

[IP フィルタ] の [疑わしい IP] 画面にも、ブロックされる IP アドレスの接続情報が表示されるのはなぜですか。

[IP フィルタ]→[疑わしい IP] 画面には、正常な接続の情報がすべて表示されます。したがって、IP アドレスがブロックリストに現在は含まれている場合でも、この IP アドレスのブロックされていなかった以前の接続が表示されます。

InterScan MSS はメールをどのように処理するのですか。

IP フィルタによって、送信元の IP アドレスが安全な IP アドレスかどうか判断します。InterScan MSS 検索サービスによって、InterScan MSS ポリシーサービスに一致したポリシーがないかどうか確認されます。要求された順序で、メールにポリシーが適用されます。メールの隔離、削除、または配信をポリシーが指定する場合は、処理が実行され、残りのポリシーは適用されません。

IP プロファイラは既存の BIND サーバを使用できますか。

はい。IP プロファイラには BIND サーバが必要です。ユーザが InterScan MSS をインストールするとき、コンピュータ上に既に BIND サーバが存在する場合は、IP プロファイラはこの BIND サーバを使用します。BIND サーバが存在しない場合は、InterScan MSS によって新しい BIND サーバがインストールされます。

IP プロファイラが正常に機能することを確認するには、BIND 9.x をどのように設定すればいいですか。

インストールまたは移行時に BIND 9.x をインストールしなかったが、後で IP プロファイラを使用する場合は、次の操作を行ってください。

a. 古い BIND サーバが存在する場合は、9.x より前のバージョンであれば、対象のコンピュータでその BIND サーバをアンインストールします。

b. コマンド tar -xvf imss.tar を実行して、bind.tar ファイルを取得します。

c. bind.tar を指定のフォルダにコピーします。

d. コマンド tar -xvf bind.tar を実行してファイルを抽出します。

e. cd コマンドを入力して bind フォルダにディレクトリ変更します。フォルダの外部では、次の項目を表示できます。

```
bash-2.03# pwd
/export/home/bob
bash-2.03# ls
bind bind.tar
```

f. 次のコマンドを実行します。

```
chgrp -R imss bind
chown -R imss bind
chmod -R 555 bind

cp -f bind/named.conf /etc
cp -f bind/rndc.key /etc

mkdir -p /var/named
chmod 770 /var/named
```

g. 名前付きグループまたはユーザが存在しない場合は、次のコマンドを実行します。

```
groupadd named
useradd -g named -s /bin/false -d /var/named named
```

h. 次のコマンドを実行して BIND サーバを設定します。

```
chown named:named /var/named
mkdir -p /var/run/named
chmod 770 /var/run/named
chown named:named  /var/run/named

chown named:named  /etc/named.conf
chown named:named  /etc/rndc.key
chmod 555 /etc/named.conf
chmod 555 /etc/rndc.key
```

i. 次のように foxdns.ini を変更します。

```
vi $IMSS_HOME/config/foxdns.ini
#$IMSS_HOME is /opt/trend/imss/ by default.
#modify the following item:
# /export/home/bob/bind is the folder for bind
dig_path=/export/home/bob/bind/dig
rndc_path=/export/home/bob/bind/rndc
named_pid_path=/var/run/named/named.pid
named_db_path=/var/named/ipprofiler
```

j. 「bash-2.03# /export/home/bob/bind/named」を入力して BIND サーバを実行します。

k. $IMSS_HOME/script で S99FOXDNS を再起動します。

InterScan MSS 7.0 がメールを「Foxhunter_proxy@domain」に送信するのは、どのようなときですか。

InterScan MSS は、次の 3 つの状態になると、メールを「Foxhunter_proxy@domain」に送信します。

- FoxProxy が「不完全な」メッセージを受信した場合。
- FoxProxy が「Null」メッセージを受信した場合。
- FoxProxy が接続を拒否した場合、5 分ごとに統計メールを送信します。foxproxy.ini 内の report_send_interval (秒単位) 設定を変更して、時間間隔を設定できます。

隔離とアーカイブ

検索にはどのような特殊文字を使用できますか。

ワイルドカードとしてアスタリスク (*) を使用します。また、受信者や添付ファイル名を区切るにはセミコロン (;) を使用します。

ユーザがメッセージの詳細を表示するときに、メッセージ ID なしの隔離されたメッセージがあるのはなぜですか。

InterScan MSS は、セキュリティ上の理由で通知メールを再処理します。したがって、通知メールがポリシー設定によって隔離された場合、InterScan MSS によって作成されたこの通知メールにはメッセージ ID がありません。

InterScan MSS で通知メールを検索しない場合は、次のように通知メールの検索を無効にできます。

a. imss.ini の [general-notification] セクションで次の設定を変更します。

NotificationSkipScan=1

b. コマンド $IMSS_Home/script/S99IMSS restart を入力して InterScan MSS デーモンを再起動します。

警告： ポリシー設定に起因するセキュリティ漏えいのリスクが存在するため、トレンドマイクロでは通知メールの検索を無効にすることはお勧めしません。

エンドユーザメール隔離

Kerberos を使用している場合、ユーザがエンドユーザメール隔離コンソールに「domain¥user_name」の省略名でログインできないのはなぜですか？

Kerberos サーバでは domain¥user_name 形式のユーザ名を受け入れることができません。Kerberos では user_name@domain.xxx という形式のユーザ名を使用する必要があります。

Exchange Server をインストールして、ユーザごとに複数のメールアドレスを設定している場合、1 人のユーザに対する複数のメールアドレスを確認するためには、エンドユーザメール隔離をどのように有効化すればいいですか。

1 つの Exchange Server を Active Directory と共にインストールしている場合、次の操作を実行できます。

a. InterScan MSS 管理データベースで tb_global_setting テーブルを開き、LDAP-->mail_attr の値を「mail」から「proxyAddresses」に置き換えます。

b. すべての InterScan MSS サービスを再開します。

日本語のエンドユーザメール隔離の通知はどのように送信するのですか。

次の項目を実行してください。

a. 管理コンソールメニューから、[管理]→[通知]→[EUQ 通知] の順にクリックします。

[EUQ 通知] 画面が表示されます。エンドユーザメール隔離の件名または内容を日本語で入力します。

b. [管理]→[通知]→[通知設定] の順にクリックします。

[通知設定] 画面が表示されます。文字コードとして日本語を選択します。

LDAP サーバが Active Directory の場合、LDAP アクセスの速度を速くするにはどうすればいいですか。

アクセス速度を速くするには 2 とおりの方法があります。どちらの方法を使用するかは、使用するポート番号が 389 か、3268 かによって決まります。

Active Directory は、グローバルカタログに 3268 を使用します。グローバルカタログに対する LDAP クエリは、別のドメインコントローラへの参照を使用しないため、アクセス速度が速くなります。

ヒント： トレンドマイクロでは、LDAP クエリにはポート 3268 を使用することをお勧めします。

Active Directory は、LDAP クエリに 389 を使用します。あるドメインコントローラで、アイテムのクエリが実行できない場合は、LDAP 参照メカニズムを使用して、別のドメインコントローラでクエリを実行します。社内のドメイン数が 1 つだけの場合またはポート 3268 を利用できない場合は、ポート 389 を使用してください。

LDAP クエリにポート 3268 を使用するには

a. [管理]→[InterScan MSS の設定]→[接続] の順にクリックします。[接続] 画面が表示されます。

b. [LDAP] タブをクリックします。

c. LDAP 待機ポートを 3268 に設定します。

LDAP クエリにポート 389 を使用するには

a. [管理]→[InterScan MSS の設定]→[接続] の順にクリックします。[接続] 画面が表示されます。

b. [LDAP] タブをクリックします。

c. LDAP 待機ポートを 389 に設定します。

d. $IMSS_HOME¥config にある imss.ini ファイルに次のキーを追加します。

```
[LDAP-Setting]
DisableAutoChaseReference=yes
```

e. すべての InterScan MSS サービスを再開します。

InterScan MSS では、Active Directory に対してどのような形式のユーザログオン名をサポートしていますか。

Active Directory では、次のようなログオン名形式がサポートされています。

- 例 1: bob@example.com

注意： ログオン名は (このような形で表示されますが) メールアドレスではありません。

- 例 2 (Windows 2000 以前): example¥bob

注意： Windows 2000 以前の形式は、Kerberos 認証ではサポートされていません。

スパムメール対策サービス

スパムメールの検出レベルはどのように決められるのですか。

InterScan MSS のメッセージをスパムメールとして分類するしきい値 (3.0 ～ 10.0 の間) を指定します。しきい値が高いと、スパムメールの疑いが強い場合でなければメッセージはスパムメールとして分類されません (これによりスパムメール検出レベルは低下しますが、誤検出は少なくなります)。しきい値が低いと、スパムメールの疑いがそれほど強くない場合でもメッセージをスパムメールとして分類します (これによりスパムメール検出レベルは向上しますが、誤検出は多くなります)。

アップデート

パターンファイルはどのようにロールバックするのですか。

[概要] ページで [ロールバック] ボタンをクリックしてください。

その他

TLS (Transport Layer Security) を使用するには、何をすればいいですか？

[管理]→[InterScan MSS の設定]→[SMTP ルーティング] 画面で TLS の証明書をアップロードし、設定を有効にします。

InterScan MSS 7.0 では、Postfix TLS 機能を使用します。すべての設定は、設定ファイル main.cf に書き込まれます。詳細については、以下を参照してください。

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

データベースサーバをホスト名で参照することはできますか。

はい。「IP¥Instance」や「Hostname¥Instance」のように指定できます。

サーバの IP アドレスを変更できますか。

はい。

サーバの IP アドレスを変更するには

a. すべての InterScan MSS サービスを停止します。

b. サーバの IP アドレスを変更します。

c. InterScan MSS 設定フォルダの ODBC.ini および EUQ.ini の IP アドレスを変更します。

d. $IMSS_HOME/UI/adminUI/ROOT/WEB-INF/struts-config-common.xml でデータベース URL およびユーザ名 / パスワードを変更します。

e. 次のデータベースデータを変更します。

- Tb_component_list: コンピュータ名とすべての検索サービスの IP アドレスを指定します。

- Tb_euq_db_info: エンドユーザメール隔離データベースのコンピュータ設定を指定します。
- Tb_global_setting: [cmagent] name [ConfigUrl] セクションで、管理コンソールの URL を変更します。

f. すべての InterScan MSS サービスを再開します。

InterScan MSS では部分メールをどのように処理するのですか。

InterScan MSS では、imss.ini ファイル内で BypassMessagePartial=no と設定されている場合、部分メールを正しくない形式のメッセージとして拒否します。

InterScan MSS でインポートできるのはどのようなファイル形式ですか。

InterScan MSS でインポートできるのは、テキスト形式ファイルのみです。次は、管理コンソールからテキストファイルをインポートする方法の例です。

a. 検索する添付ファイルを指定する場合

- メニューから、[ポリシー]→[ポリシーリスト] の順にクリックします。
- 既存のルールのリンクをクリックして、ルールを編集します。
- [検索条件] リンクをクリックします。
- [添付ファイル] セクションの下にある [名前または拡張子] リンクをクリックします。
- [指定のファイル名] の横のチェックボックスをオンにします。
- [インポート] をクリックします。インポートされたファイルはテキストファイルである必要があります。

b. スパムメール検出を設定する場合

- メニューから、[ポリシー]→[ポリシーリスト] の順にクリックします。
- 既存のルールのリンクをクリックして、ルールを編集します。
- [検索条件] リンクをクリックします。

- [スパムメール] リンクをクリックします。
- [承認済み送信者リスト] または [ブロックする送信者リスト] の横のチェックボックスをオンにします。
- [インポート] をクリックします。インポートされたファイルはテキストファイルである必要があります。

新しく作成した管理者アカウントが [ユーザ隔離アクセス]、[管理者アカウント]、または [製品ライセンス情報] ページにアクセスできないのはなぜですか。

初期設定の InterScan MSS 管理者アカウントだけが、[ユーザ隔離アクセス]、[管理者アカウント]、または [製品ライセンス情報] ページにアクセスする権限を持っています。委任された管理者のアカウントでは、これらのページにアクセスできません。

InterScan MSS 設定への変更は、なぜ直ちに有効にならないのですか。

管理コンソールから設定を変更した時間と InterScan MSS サーバ上で変更が実際に更新される時間との間にわずかなずれがあります。

ポリシー設定は 3 分以内に再読み込みされます。この設定をより速く読み込むには、必要に応じて、InterScan MSS 管理データベースの tb_global_setting テーブルで policy_server=>dbChangePollIntervalInSecs 設定を変更してください。

その他の一般的な設定については、imssmgr により、1 分以内に管理コンソールから変更した新しい設定が再度読み込まれます。

トレンドマイクロでは、管理コンソールから設定を変更した直後に InterScan MSS へメールを送信しないことをお勧めします。

次の項目の最大数に制限がありますか。

- 各ルールの送信者と受信者
- 1 つのアドレスグループ内のメールアドレス
- スパムメール対策ルールの承認済み送信者とブロックする送信者

技術的に、各ルールの合計サイズに 640KB という 1 つの制限があります。合計サイズには、ルールルート (送信者と受信者)、ルールフィルタ (検索条件)、ルール処理などが含まれます。各メールアドレスまたは各 LDAP アカウントは 20 文字で構成されることを前提としており、InterScan MSS では、ルールルートで少なくとも 10,000 の送信者と受信者をサポートできます。

1 つのアドレスグループのメールアドレス最大数は 10,000 です。

スパムメール対策ルールの承認済み送信者とブロックする送信者の最大数は 5,000 です。

ログのパスを変更するにはどうしたらいいですか。

一部のログのパスを変更する場合は、必要に応じて、imss.ini の次のキーを検索して初期設定を変更してください。

[general]

sys_log_path=/opt/trend/imss/log

event_log_path=/opt/trend/imss/log

policy_evt_log_path = /opt/trend/imss/log

[policy_server]

log_path = /opt/trend/imss/log

[logs]

log_path=/opt/trend/ipprofiler/logs

SSL 証明書を作成するにはどうしたらいいですか。

次の操作を実行してください。

a. 次のように Tomcat SSL 証明書を作成します。

keytool -genkey -alias tomcat -keyalg RSA -keystore /opt/trend/imss/UI/tomcat/sslkey/.keystore

Tomcat における SSL 設定の詳細については、次のサイトにアクセスしてください。

http://tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html

b. 次のように Apache SSL 証明書を作成します。

i. 秘密鍵および Certificate Signing Request (CSR) を作成します。

openssl req -new > new.cert.csr

ii. 鍵からパスフレーズを削除します。

openssl rsa -in privkey.pem -out new.cert.key

iii. 自己署名証明書を作成します。

openssl x509 -in new.cert.csr -out new.cert.cert -req -signkey new.cert.key -days 1825

iv. 証明書と鍵を Apache のパスにコピーします。

cp new.cert.cert $IMSS_HOME/UI/apache/conf/ssl.crt/server.crt

cp new.cert.key $IMSS_HOME/UI/apache/conf/ssl.key/server.key

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、契約期間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 (トラブルシューティング) 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。

http://esupport.trendmicro.co.jp/supportjp/supportcentral/supportcentral_adv_ja.do

図 8-1.　製品 Q&A の Web サイト

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/supform.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、フィリピンを本拠地に、欧州、日本、中国、台湾にわたる 800 名以上 (2006 年 1 月現在) のエンジニアから構成されています。ウイルス情報の収集、調査、解析やサポートを年中無休 24 時間の体制で行っています。

「TrendLabs」の本拠地、フィリピンのマニラ近くにあるラボは、高度な技術水準と最新設備を備えており、管理とサービス提供の手続きにおいて品質保証の国際基準を満たす ISO9001:2000 認定を取得しています。

その他の設定

この付録では、Trend Micro InterScan Messaging Security Suite (以下、InterScan MSS) をネットワーク環境で稼動させるために役立つ設定情報を提供します。設定は、インストール先の環境や、MTA、メールサーバがどのように構成されているかに大きく依存します。

この付録の内容は次のとおりです。

- 222 ページの「その他のタスクの実行」

その他のタスクの実行

次の表は、InterScan MSS を使用するうえで必要になる可能性のあるタスクと、そのためのコマンドをまとめたものです。これらのコマンドは、特に指定のない限り、Linux および Solaris の両方のプラットフォームに当てはまります。

タスク	コマンド
既存の sendmail のアンインストール	rpm -qa | grep sendmail /etc/rc.d/init.d/sendmail stop rpm -e --nodeps sendmail
postfix のインストール	rpm -Uvh postfix-2.2.11-1.rhel4.i386.rpm (Solaris には適用されない)
Bind のインストールの確認	bind-9.2.4-16.EL4 (Linux)、bind -9.4.0 (Solaris) binutils-2.15.92.0.2-21 bind-libs-9.2.4-16.EL4 ypbind-1.17.2-8 bind-chroot-9.2.4-16.EL4 bind-utils-9.2.4-16.EL4
Bind サーバの確認と自動起動の設定	service named status service named start chkconfig --list named chkconfig named on
SMTP ポートの 2500 への変更	master.cf の次の行で「smtp」を「2500」に変更します。 smtp inet n - n - - smtpd 変更後 : 2500 inet n - n - - smtpd
transport_maps パラメータが設定済みかどうかの確認	postconf transport_maps
transport_maps の再設定	postconf -e 'transport_maps=$default_database_type:$config_directory/transportList'

表 A-1. その他のタスクのコマンド

タスク	コマンド
transport ファイルの名前変更と表示	cat /etc/postfix/transport >> /etc/postfix/transportList
transportList.db のコンパイル	postmap -v hash:/etc/postfix/transportList
main.cf の変更	mydomain = tests-mexico.trendmicro.com myhostname = correo.tests-mexico.trendmicro.com mydestination = $myhostname, localhost.$mydomain, $mydomain default_process_limit=200 imss_timeout=10m imss_connect_timeout=1s content_filter = imss:localhost:10025 imss_destination_recipient_limit=200 imss_destination_concurrency_limit=20
master.cf の変更	#InterScan MSS:content filter smtp transport imss for InterScan MSS imss unix - - n - - smtp -o disable_dns_lookups=yes -o smtp_connect_timeout=$imss_connect_timeout -o smtp_data_done_timeout=$imss_timeout #InterScan MSS:content filter loop back smtpd localhost:10026 inet n - n - 20 smtpd -o content_filter= -o smtpd_timeout=$imss_timeout -o local_recipient_maps= -o myhostname=postfix.imss70 -o smtpd_client_restrictions=
main.cf の変更	local_recipient_maps=
imss.ini の変更	smtp_allow_client_ip=127.0.0.1 または open_to_all_connections = yes

表 A-1.　その他のタスクのコマンド

索引

英数字

AJP 196
Apache 53
  Tomcat 52
Control Manaager エージェント、エージェント
  Control Manager 29
Control Manager
  概要、Control Manager
    概要 29
CPU の要件 36
Firefox 37
IMSSMGR 52
Internet Explorer 37
InterScan MSS 16
InterScan MSS 5.1x 106
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 46
  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 46
  管理データベース 43
  検索サービス 44
  セントラルコントローラ 43
  ポリシーサービス 45
  ポリシーサービスの同期 45
InterScan MSS について 16
IP フィルタ
  インストール 100
  概要 46
  削除 127
IP プロファイラ 17
  概要 46
  機能 48
  検出 47
LDAP サーバの要件 37
MTA
  NRS での使用 142
  Postfix の準備 84
MTA 機能、便宜的な TLS 17
MTA の要件 38
Named Server 52
NRS 17
  MTA 設定 142
  アクティベーションコード 141
  概要 47
  管理コンソール 143
  機能 49
  サービス 47
  使用 141
  設定 141
POP3 待機ポート 196
Postfix の準備 84
Postgre の要件 37
Readme ファイル 12
SMTP ルーティング 155
SOAP サーバ 196
SSL 証明書 131
Tomcat 52、53
TrendLabs 219

Web エンドユーザメール隔離 17

あ

アーカイブ 17
アーカイブおよび隔離領域の一元化 17
新しい機能 16
アップグレード 106
アンインストール 126
  IP フィルタコンポーネント 127
移行
  5.1x から 7.0 113
  ロールバック 123
移行のロールバック 123
インストール 35、129、147、177
  Control Manager の使用 69
  DMZ 内 59
  InterScan MSS の削除 126
  IP フィルタ 100
  IP フィルタ、インストール
    エンドユーザメール隔離 81
  Postfix の準備 84
  SMTP ゲートウェイ 58
  SSL の使用 131
  クラスタ化 67
  シナリオ 60
  手順 94
  ファイアウォールなし 55
  ファイアウォールの内側 57
  ファイアウォールの外側 56
ウィザード 132
エンドユーザメール隔離 17
  管理コンソール 145
オンラインヘルプ 12

か

隔離 17
管理コンソール 130
管理データベース 52
基本設定 132
許可された送信者 159
検索サービス 45
検索条件 167
コマンド 222
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 36
システム要件 36
新機能 16
スパイウェアとグレーウェア 27
スパムメール対策 17
  アクティベーションコード 141
スワップ領域の要件 37
接続 156
設定
  移行 112
  バックアップ 106
設定ウィザード 17、132
設定の移行 112
設定のバックアップ 106
セントラルコントローラ 45

た

対象読者 12
ディスク領域の要件 36
データベース
セントラルコントローラ 43
データベースサーバ 52
テクニカルサポート 215
ドキュメント 12
ドメインベースの配信 159
トラブルシューティング 188
imssps デーモン 188
IP フィルタ 192
NRS 194
エンドユーザメール隔離管理コンソールへのアクセス 191
エンドユーザメール隔離通知 191
エンドユーザメール隔離の隔離されたメッセージ 192
製品の起動 189
メール通知 189
トランスポート層 157

は

バージョン 5.1x 106
はじめに 11
パスワード
InterScan MSS 管理コンソール初期設定 130
エンドユーザメール隔離管理コンソール初期設定 145
パターンマッチング 18
フィルタ、機能 23
フェイルオーバー 73
ブラウザ要件 37
ポリシー 16
ポリシーサービス 45
ポリシーの一元化 16

ま

マスメーリング型ウイルス
パターン 22
メール脅威
スパムメール 20
非生産的メッセージ 20
メールログパーサ 54
メッセージ追跡 160
メモリの要件 36

や

ユーザ名
InterScan MSS 管理コンソール初期設定 130
エンドユーザメール隔離管理コンソール初期設定 145
要件 36
よくある質問
InterScan MSS コンポーネント 200
IP プロファイラ 202
postfix 197
TLS 210
エンドユーザメール隔離 207

ら

レポート 16

ログ 16
ログ機能の一元化 16