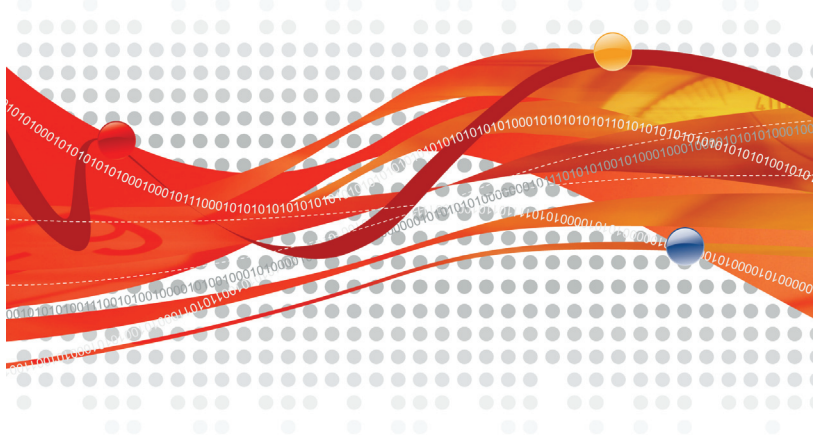
Trend Micro
InterScan Messaging Security Suite™



インストールガイド

安心を、ひとつ上のステージへ。

TREND MICRO™

※注意事項

トレンドマイクロへのお客様情報の送信について

- 「Webレピュテーションサービス」「フィッシング詐欺対策」「有害サイト規制/URLフィルタリング」では、Webサイトの安全性の判定のために、お客様がアクセスしたURLの情報等(ドメイン、IPアドレス等を含む)を暗号化してトレンドマイクロのサーバに送信します。
  サーバに送信されたURL情報は、Webサイトの安全性の確認、および本機能の改良の目的にのみ利用されます。
  また、これらの機能を有効にしたうえで、Webページにアクセスした場合、以下の事象がおこることがあります。
  (a)お客様がアクセスしたWebページのWebサーバ側の仕様が、お客様が入力した情報等をURLのオプション情報として付加しWebサーバへ送信する仕様の場合、URLのオプション情報にお客様の入力した情報（ID、パスワード等）などを含んだURLがトレンドマイクロのサーバに送信される。この場合、トレンドマイクロでは、お客様がアクセスするWebページの安全性の確認のため、これらのお客様より受領した情報にもとづき、お客様がアクセスするWebページのセキュリティチェックを実施します。
- 「ファイルレピュテーションサービス」では、ファイルの安全性の判定のために、ファイルのハッシュ値等の情報をトレンドマイクロのサーバに送信します。ファイルそのものや、ファイルの内容に関する情報は送信しません。
- 「ソフトウェア安全性評価サービス/脅威情報の送信」では、プログラムの安全性の判定のために、プログラムまたはプログラムの情報をトレンドマイクロのサーバに送信します。
- 「ウイルストラッキング/TrendCareプログラム」では、検出されたウイルス/脅威名、検出数、国/地域、感染元となったWebサイトのURLを、統計を取るためにトレンドマイクロのサーバに送信します。
- 「迷惑メール対策ツール」では、弊社製品の改良の目的および迷惑メールの判定精度の向上のため、トレンドマイクロのサーバに該当メールを送信します。また、迷惑メールの削減、迷惑メールによる被害の抑制を目指している政府関係機関に対して迷惑メール本体を開示する場合があります。
- 「E-mailレピュテーションサービス」では、スパムメールの判定のために、送信元のメールサーバの情報等をトレンドマイクロのサーバに送信します。
- 「スマートフィードバック」では、脅威に関する情報を収集、分析し保護を強化するために、不正な動きをする可能性があるとトレンドマイクロが判断したファイル、ファイルのチェックサム、アクセスされたWebアドレス、サイズやパス等のファイル情報、実行ファイルの名前等の情報をトレンドマイクロのサーバに送信します。送信されたファイルはプログラムの安全性の判定のために利用されます。またファイルにお客さまの個人情報や機密情報等が意図せず含まれる可能性がありますが、トレンドマイクロがファイルに含まれる個人情報や機密情報自体を収集または利用することはありません。お客さまから収集された情報の取り扱いについての詳細は、<http://jp.trendmicro.com/jp/about/privacy/spn/index.html >をご覧ください。

輸出規制について

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

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

2009年7月現在、米国により定められる禁輸国は、キューバ、イラン、北朝鮮、スーダン、シリアが含まれています。

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

複数年契約について

- お客様が複数年契約（複数年分のサポート費用前払い）された場合でも、各製品のサポート期間については、当該契約期間によらず、製品ごとに設定されたサポート提供期間が適用されます。
- 複数年契約は、当該契約期間中の製品のサポート提供を保証するものではなく、また製品のサポート提供期間が終了した場合のバージョンアップを保証するものではありませんのでご注意ください。
- 各製品のサポート提供期間は以下のWebサイトからご確認いただけます。
  http://jp.trendmicro.com/jp/support/lifecycle/index.html

著作権について

商標について

P/N: IMSSFF-AE0105 (2010/01)

目次

はじめに

はじめに

Trend Micro InterScan Messaging Security Suite 7.1 (以下、InterScan MSS) インストールガイドをお読みいただきありがとうございます。本書では、InterScan MSS の機能、システム要件、およびインストールとアップグレードの手順について説明しています。

InterScan MSS の設定方法については「Trend Micro InterScan Messaging Security Suite 7.1 管理者ガイド」を、またユーザインタフェースの詳細については管理コンソールからオンラインヘルプを参照してください。

この章の内容は次のとおりです。

対象読者

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

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

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

InterScan MSS ドキュメント

InterScan MSS には、次のドキュメントが付属しています。

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

インストールガイド、管理者ガイド、および Readme ファイルは、以下から入手できます。

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

ドキュメントの表記規則

このドキュメントでは、次の表記規則を使用しています。

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

表 1. 本書で使用している表記規則

第 1 章

InterScan MSS の概要

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

この章の内容は次のとおりです。

InterScan MSS の概要

InterScan MSS では、ウイルス対策機能、スパムメール対策機能、フィッシング対策機能、およびコンテンツフィルタテクノロジが一元化されているため、メールを包括的に保護できます。この柔軟性の高いソフトウェアソリューションには、高い評価を受けているウイルス対策機能およびゼロデイ保護機能が備わっており、既知のウイルスおよび潜在的なウイルスをブロックします。

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

新機能

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

表 1-1. InterScan MSS の新機能

新機能	説明
共通のポリシーオブジェクト	ポリシーで使用できるいくつかの情報オブジェクトは、ポリシー作成から削除され、以下に示す独自の設定領域が確保されました。 ・ アドレスグループ ・ BATV キー ・ キーワードおよび式 ・ ポリシー通知 ・ スタンプ ・ DKIM 承認済みリスト ・ Web レピュテーション承認済みリスト
Web レピュテーション	メールメッセージに埋め込まれた不正なサイトに導く URL からクライアントを保護します。
BATV のサポート	BATV (バウンスアドレスタグ検証) は、クライアントをバウンスメールメッセージ攻撃から保護します。

表 1-1. InterScan MSS の新機能 (続き)

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

InterScan MSS の主な機能と利点

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

表 1-2.　主な機能と利点

機能	説明	利点
ウイルス対策による保護	InterScan MSS では、トレンドマイクロの検索エンジンおよびパターンマッチングというテクノロジを使用して、ウイルスの検出を実行します。検索エンジンは、ゲートウェイを通過するファイル内のコードと、パターンファイルに記述された既知のウイルスのバイナリパターンを比較します。パターンの一致を検出すると、検索エンジンはポリシールールの設定に応じて、処理を実行します。	InterScan MSS の機能強化されたウイルス / コンテンツ検索サービスにより、メッセージングシステムは最適な状態で稼働し続けることができます。
IntelliTrap	ウイルス作成者は多くの場合、さまざまなファイル圧縮スキームを使用して、ウイルスフィルタを回避しようとします。IntelliTrap では、そのような圧縮ファイルをヒューリスティックに評価します。場合により、脅威ではないファイルにセキュリティ上のリスクがあると識別される可能性もあるため、IntelliTrap を有効にするときは、このカテゴリに分類された添付ファイルを隔離することをお勧めします。また、ユーザが圧縮ファイルを頻繁にやりとりする場合は、この機能を無効にすることができます。 初期設定では、IntelliTrap はウイルス対策ポリシーで検索条件の 1 つとして有効になっており、セキュリティ上のリスクとして分類された添付ファイルは隔離されるように設定されています。	IntelliTrap を使用すると、さまざまなファイル圧縮スキームを使用して圧縮されたウイルスがメールを介してネットワークに侵入するリスクを低減できます。
コンテンツ管理	InterScan MSS では、ネットワーク内外に送信されるメールメッセージとその添付ファイルを分析して、適切なコンテンツかどうかをチェックします。	管理者が不適切だと判断したコンテンツ（個人的なやりとり、大容量の添付ファイルなど）は、InterScan MSS を使用してブロックしたり効果的に遅延することができます。

表 1-2. 主な機能と利点（続き）

機能	説明	利点
その他のメールの脅威に対する保護		
DoS 攻撃	巨大な添付ファイルでメールサーバをオーバーフローさせたり、複数のウイルスや多重圧縮ファイルが含まれるメッセージを送信したりすることで、悪意のあるユーザがメール処理を妨害することがあります。	InterScan MSS を使用して、SMTP ゲートウェイで阻止したいメッセージの特徴を設定することができます。これにより、DoS 攻撃の発生を低減できます。
不正なメールコンテンツ	多くのタイプの添付ファイル (実行可能プログラムや埋め込みマクロを含むドキュメントなど) は、ウイルスの隠れ蓑になる可能性があります。HTML スクリプトファイル、HTML リンク、Java アプレット、および ActiveX コンソールを含むメッセージも、有害な処理を実行する可能性があります。	InterScan MSS を使用して、SMTP ゲートウェイの通過を許可するメッセージの種類を設定できます。
サービスの低下	多くの組織では、ビジネスに無関係のメールトラフィックが問題になっています。スパムメールメッセージはネットワーク帯域幅を消費し、従業員の生産性にも影響します。また中には、会社のメッセージングシステムを使用して、就労時間中に個人的なメッセージを送信したり、大容量のマルチメディアファイルを転送したり、個人的なビジネスを行う従業員がいる場合があります。	多くの企業には、その組織のメッセージングシステムに最適な使用ポリシーがあります。InterScan MSS には、既存のポリシーを実行し、その遵守を確保するためのツールが用意されています。
法的責任とビジネスの保全	メールを不正に使用することにより、会社が法的責任を負う状況に追い込まれることになる場合もあります。従業員が性的いやがらせや人種上のいやがらせ、または他の違法な活動に関与していることもあります。また、不誠実な従業員が会社のメッセージングシステムを使用して、機密情報を漏えいする可能性もあります。不適切なメッセージが会社のメールサーバから送信されると、メッセージに記された意見の内容がその会社のものでないとしても、会社の評判に傷がつきます。	InterScan MSS では、不適切な内容や機密資料を含むメッセージがゲートを通過するリスクを低減できる、コンテンツを監視およびブロックするためのツールを提供しています。

表 1-2.　主な機能と利点（続き）

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

表 1-2.　主な機能と利点（続き）

機能	説明	利点
スパムメール対策の統合		
スパムメール対策 (コンテンツ検索)	スパムメール対策 (コンテンツ検索) は、トレンドマイクロからライセンスされる製品であり、他のトレンドマイクロ製品に対してスパムメール検出サービスを提供します。スパムメール対策を使用するには、スパムメール対策のアクティベーションコードを取得します。詳細については、販売店に問い合わせてください。InterScan MSS のスパムメール対策機能は、組み込みのスパムメールフィルタを使用して機能します。このフィルタは、スパムメール対策用のアクティベーションコードを入力してアクティベーションを完了した時点で有効になります。 **注意：** IP プロファイラおよびメールレピュテーションを設定する前に、スパムメール対策をアクティベートします。	スパムメール対策 (コンテンツ検索) で使用される検出テクノロジは、高度なコンテンツ処理および統計分析に基づいています。スパムメールを特定するための他の手法と異なり、コンテンツ分析はパフォーマンスが高く、スパムメール送信者がその技法を変えても、高度に適応できるリアルタイム検出を実現します。
IP プロファイラおよびメールレピュテーションによるスパムメールフィルタ	IP プロファイラは、自己学習能力と十分なカスタマイズ性を備えており、スパムメールや他の潜在的な脅威を送信するコンピュータの IP アドレスを能動的にブロックします。メールレピュテーションは、トレンドマイクロの中央データベースで管理される既知のスパムメール送信者の IP アドレスをブロックします。	IP フィルタは、IP プロファイラとメールレピュテーションで構成されます。IP フィルタを使用することにより、スパムメール送信者を IP レベルでブロックできます。

表 1-2.　主な機能と利点（続き）

機能	説明	利点
その他		
LDAP およびドメインベースのポリシー	管理者権限およびユーザ / グループの定義に Lotus Domino や Microsoft Active Directory などの LDAP ディレクトリサービスを使用している場合、LDAP を設定できます。 **注意：** エンドユーザメール隔離を使用するには、LDAP が必要です。	LDAP を使用すると、さまざまなルールを定義して、会社におけるメール使用のガイドラインを実行することができます。送信者または受信者のアドレスに基づいて、個人またはグループごとにルールを定義できます。
Web ベースの管理コンソール	Web ベースの管理コンソールを使用すると、InterScan MSS のポリシーと設定を効率的に指定することができます。	Web ベースのコンソールは SSL に対応しています。つまり、InterScan MSS へのアクセスに対するセキュリティが強化されています。
エンドユーザメール隔離	InterScan MSS では、スパムメールの管理効率を向上させるために、Web ベースのエンドユーザメール隔離機能を提供しています。Web ベースのエンドユーザメール隔離サービスを使用することで、エンドユーザは独自のスパムメール隔離を管理できます。スパムメール対策（コンテンツ検索）では、スパムメールと判断されたメッセージを隔離します。これらのメッセージは、エンドユーザメール隔離によってデータベース内でインデックスが付けられます。それにより、エンドユーザはメッセージを再確認して、削除したり配信を許可したりできるようになります。	Web ベースのエンドユーザメール隔離コンソールを使用して、エンドユーザは InterScan MSS によって隔離されるメッセージを管理できます。
管理タスクの委任	InterScan MSS には、管理コンソールにさまざまなアクセス権限を作成する機能が用意されています。管理者のログオンアカウントごとに、アクセスを許可する管理コンソールのセクションを選択できます。	管理者ロールを別の従業員に委任することで、管理職務の共有化を進めることができます。

表 1-2. 主な機能と利点（続き）

機能	説明	利点
一元化されたレポート機能	一元化されたレポート機能により、(要求に応じた) 1 回限りのレポートや予約レポートを柔軟に生成できます。	InterScan MSS の実行内容を分析できます。 (要求に応じた) 1 回限りのレポートでは、必要に応じてレポートの内容の種類を指定できます。また、日次、週次、または月次で自動的にレポートを作成するように設定することもできます。
システム可用性の監視	組み込みのエージェントにより、InterScan MSS サーバの状況を監視し、障害状態によりメールフローが混乱する恐れがある場合、メールまたは SNMP トラップを使用して通知を配信します。	システム障害の検出時にメールおよび SNMP 通知を使用することより、直ちに修正作業を行い、停止時間を最小限に抑えることができます。
POP3 検索	管理コンソールから、POP3 メール検索を有効または無効にできます。	SMTP トラフィックの他に、InterScan MSS では、ネットワーク内のメッセージングクライアントがメッセージを受信する際に、ゲートウェイで POP3 メッセージを検索することもできます。
クラスタ化アーキテクチャ	本バージョンの InterScan MSS は、分散配置が可能になるように設計されています。	各種の InterScan MSS コンポーネントをさまざまなコンピュータ上にインストールできます。一部のコンポーネントは複数のコンピュータに配置できます。たとえば、メッセージの量に応じて、追加サーバ上に追加の InterScan MSS 検索サービスコンポーネントをインストールして、すべてのサーバで同じポリシーサービスを使用することができます。

表 1-2.　主な機能と利点（続き）

機能	説明	利点
Trend Micro Control Manager との統合	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、物理的な場所やプラットフォームにかかわりなく、中央から制御できる機能を提供するソフトウェア管理ソリューションです。このアプリケーションは、企業のウイルスおよびコンテンツセキュリティポリシーの管理を簡略化します。 詳細については、24 ページの「Trend Micro Control Manager について」を参照してください。	Control Manager から配信される大規模感染予防サービスにより、大規模感染のリスクを低減できます。トレンドマイクロ製品でメールから発生した新しいウイルスを検出した場合、TrendLabs （トレンドラボ) は InterScan MSS の高度なコンテンツフィルタを使用するポリシーを発行し、メッセージの疑わしい特徴を特定することでそのメッセージをブロックします。これらのルールにより、更新されたパターンファイルが使用可能になる前に感染が拡大する可能性を最小限に抑えることができます。

スパイウェアと他の種類のグレーウェア

企業ユーザは、ウイルス以外の潜在的な脅威のリスクにもさらされています。グレーウェアは、ネットワーク上のコンピュータのパフォーマンスに悪影響を与え、企業に対して、深刻なセキュリティ上のリスクや機密保持のリスク、法的リスクをもたらします （表 1-3 を参照)。

表 1-3.　スパイウェア / グレーウェアの種類

スパイウェア / グレーウェアの種類	説明
スパイウェア / グレーウェア	アカウントユーザ名やパスワードなどのデータを収集し、サードパーティに送信します。
アドウェア	広告を表示したり、Web ブラウザを通じて、ユーザの Web 利用状況などのデータを収集します。
ダイヤラー	コンピュータのインターネット設定を変更し、あらかじめ設定された電話番号に、コンピュータがモデムを通じて自動的にダイヤルするようにします。
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。

表 1-3.　スパイウェア / グレーウェアの種類（続き）

スパイウェア / グレーウェアの種類	説明
ハッキングツール	ハッカーがコンピュータに対して不正なアクセスをするためのツールです。
リモートアクセスツール	ハッカーがコンピュータに対してリモートにアクセスし、制御するためのツールです。
パスワード解読アプリケーション	ハッカーがアカウントユーザ名とパスワードを解読するためのツールです。
その他	上記以外の種類。

Web レピュテーションについて

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

Trend Micro Control Manager について

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、物理的な場所やプラットフォームにかかわりなく、中央から制御できる機能を提供するソフトウェア管理ソリューションです。このアプリケーションは、企業のウイルスおよびコンテンツセキュリティポリシーの管理を簡略化します。

Control Manager は、次のコンポーネントで構成されます。

- **Control Manager サーバ** — Control Manager サーバは、Control Manager アプリケーションがインストールされるコンピュータです。Control Manager の Web ベースの管理コンソールは、このサーバからホストされます。

  注意： Control Manager 5.0 サーバを InterScan MSS と連携させるには、このサーバに Patch 3 以上をインストールする必要があります。

- **エージェント** — エージェントは、管理下の製品にインストールされるアプリケーションで、Control Manager による製品の管理を可能にします。エージェントは Control Manager サーバからコマンドを受信して、管理下の製品に適用します。また、製品からログを収集して、Control Manager に送信します。

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

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

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

注意： Control Manager を使用して InterScan MSS を管理する際は、Control Manager5.0 サーバ (Patch 3 以上) を使用してください。最新のバージョンおよび最新の Patch とアップデートの詳細については、次の Web サイトを参照してください。
http://www.trendmicro.co.jp/download/

Control Manager との統合

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

表 1-4. サポートされている Control Manager の機能

機能	説明	サポートの有無
双方向通信	双方向通信を使用して、InterScan MSS と Control Manager のいずれも通信プロセスを開始できます。	なし。 InterScan MSS のみが Control Manager との通信プロセスを開始できます。
大規模感染予防ポリシー	TrendLabs (トレンドラボ) で開発された大規模感染予防ポリシー (OPP) は大規模感染に迅速に対応しており、InterScan MSS サーバまたはそのクライアントが感染する可能性を低くするために InterScan MSS が行うべき処理のリストが含まれています。 トレンドマイクロのアップデートサーバは、Control Manager を使用して InterScan MSS にこのポリシーを配信します。	あり
クエリ用のログのアップロード	検索の目的で InterScan MSS のウイルスログ、コンテンツセキュリティログ、およびメールレピュテーションログを Control Manager にアップロードします。	あり
シングルサインオン	InterScan MSS 管理コンソールに先にログオンせずに、InterScan MSS を Control Manager から直接管理します。	なし。 Control Manager から InterScan MSS を管理するには、先に InterScan MSS 管理コンソールにログオンする必要があります。
設定の複製	既存の InterScan MSS サーバから新しい InterScan MSS サーバに Control Manager から設定を複製します。	あり
パターンファイルのアップデート	Control Manager から InterScan MSS が使用するパターンファイルをアップデートします。	あり
エンジンのアップデート	Control Manager から InterScan MSS が使用するエンジンをアップデートします。	あり

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

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

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

機能	説明	サポートの有無
Control Manager エージェントのインストールとアンインストール	InterScan MSS Control Manager エージェントを Control Manager からインストールまたはアンインストールします。	なし。 InterScan MSS Control Manager エージェントは、InterScan MSS のインストール時に自動的にインストールされます。エージェントを有効または無効にするには、InterScan MSS 管理コンソールから次の手順を実行します。 1. メニューから [管理] → [接続] の順に選択します。 2. [Control Managerサーバ] タブをクリックします。 3. エージェントを有効または無効にするには、[Control Manager エージェントを有効にする] の横にあるチェックボックスをオンまたはオフにします。
イベント通知	InterScan MSS イベント通知を Control Manager から送信します。	あり
すべてのコマンドのコマンド追跡	Control Manager が InterScan MSS に発行するコマンドのステータスを追跡します。	あり

第 2 章

コンポーネントの説明

この章では、Trend Micro InterScan Messaging Security Suite 7.1 (以下、InterScan MSS) の管理に必要な要件、および InterScan MSS が機能するために必要なさまざまなソフトウェアコンポーネントについて説明します。

この章の内容は次のとおりです。

InterScan MSS コンポーネントについて

InterScan MSS の新しいアーキテクチャでは、製品を個別のコンポーネントに切り分け、それぞれがメッセージ処理の特定のタスクを実行します。次の項では、各コンポーネントの概要について説明します。

InterScan MSS コンポーネントは、単一のコンピュータにも複数のコンピュータにもインストールできます。それぞれのコンポーネントが連携する仕組みは、56 ページの「インストールシナリオについて」の図を参照してください。

InterScan MSS 管理データベース

InterScan MSS 管理データベースには、すべてのグローバル設定情報が保存されます。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情報が格納されます。InterScan MSS をインストールする場合、他のコンポーネントをインストールする前に、データベースサーバをインストールして、適切なクエリを実行し、データベーステーブルを作成する必要があります。新しい SQL Server Express データベースをインストールすることも、既存の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含まれている Web サーバコンポーネントによって管理コンソールのインタフェース画面がブラウザに表示され、管理者は InterScan MSS 管理コンソールを使用して InterScan MSS を設定および制御できるようになります。管理コンソールは、管理者と InterScan MSS データベースとの間のインタフェースとなり、さまざまなコンポーネントでそのデータベースを使用して、検索、ログ、およびその他のメッセージ処理を実行します。

検索サービス

検索サービスとして設定されたサーバは、次の処理を実行します。

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

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

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

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

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

ポリシーサービス

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

ポリシーの同期

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

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

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

エンドユーザメール隔離サービス

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

プライマリおよびセカンダリエンドユーザメール隔離サービス

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

エンドユーザメール隔離サーバコンポーネント

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

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

Apache Web サーバおよび mod_jk

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

Apache Web サーバは、標準の Apache ServerRoot 構造を持つ、{InterScan MSS}¥UI¥apache ディレクトリにインストールされます。Apache のメイン設定ファイル （{InterScan MSS}¥UI¥euqUI¥conf ディレクトリ内の EUQ.conf) では、Apache Web サーバによって転送されるすべての要求を受信する Tomcat スレッドの名前と共に、Apache が受信接続を受け付ける TCP ポート （8447)、処理可能な最大接続数 （150)、および mod_jk の設定が定義されています。

Tomcat

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

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

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

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

Struts フレームワーク

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

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

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

エンドユーザメール隔離アプリケーション

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

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

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

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

エンドユーザメール隔離データベース

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

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

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

- データベースサーバのソフトウェアと共にインストール

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

IP フィルタ

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

これは、IP プロファイラと Email Reputation Services の 2 つの機能で構成されています。

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

  IP プロファイラは、次の 4 つのインターネットの脅威を検出します。

  - **スパムメール** — 不要な広告コンテンツが含まれるメール。
  - **ウイルス** — トロイの木馬プログラムなどの各種のウイルス脅威。
  - **DHA 攻撃** — 有効なドメイン名を持つ任意のメール名を組み合わせ、任意のメールアドレスを作成して有効なメールアドレスを収集するために、スパムメール発信者が使用する方法。メールは作成されたメールアドレスに送信されます。メールメッセージが配信されると、メールアドレスは本物であると判断され、スパムメールデータベースに追加されます。
  - **バウンスメール** — メールサーバを使用して、「差出人」フィールドに対象のメールドメインが記述されたメールメッセージを生成する攻撃。架空のアドレスでメールメッセージを送信し、それをエラーで返送しようとすると、対象のメールサーバはオーバーフローします。
- **メールレピュテーション** — 既知のスパムメール送信者からのメールをネットワーク (IP) レベルでブロックします。

IP プロファイラの仕組み

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

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

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

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

メールレピュテーション

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

メールレピュテーションの種類

メールレピュテーションには、Standard と Advanced の 2 種類があります。

メールレピュテーション： Standard

このサービスでは、要求された IP アドレスを、Trend Micro Threat Protection Network によって管理されているトレンドマイクロのレピュテーションデータベースと照合して検証することにより、スパムメールをブロックします。この拡張を続けるデータベースには、現在 10 億を超える IP アドレスが、スパムメールの活動に基づく評価とともに格納されています。トレンドマイクロのスパムメール調査担当者は、これらの評価の見直しと更新を継続的に行い、その精度を高めています。

「メールレピュテーション : Standard」サービスは、DNS 単一クエリベースのサービスです。未知のホストからメールメッセージを受信した場合、指定されたメールサーバは Standard レピュテーションデータベースサーバに対して DNS クエリを実行します。そのホストが Standard レピュテーションデータベースに存在すれば、メールレピュテーションはそのメールメッセージをスパムメールとしてレポートします。メールレピュテーションからのスパムメールの識別情報を基に、そのメッセージに対して適切な処理を実行するように MTA を設定できます。

ヒント： Standard レピュテーションデータベースのデータに合致した IP アドレスからのメールは、受信せず、ブロックするように MTA を設定することをお勧めします。

メールレピュテーション： Advanced

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

これは、動的でリアルタイムなスパムメール対策ソリューションです。このサービスを提供するために、トレンドマイクロは、継続的にネットワークおよびトラフィックパターンを監視し、新しいスパムメールの発信元が現れると、直ちに (通常はスパムメールの最初の兆候の数分以内) 動的レピュテーションデータベースを更新します。スパムメールの活動の形跡がなくなると、動的レピュテーションデータベースもそれに応じて更新されます。

「メールレピュテーション : Advanced」は「メールレピュテーション : Standard」と同様に DNS クエリベースのサービスですが、Standard レピュテーションデータベースと動的レピュテーションデータベース (動的にリアルタイムに更新されるデータベース) という 2 種類のデータベースに対して 2 つのクエリを発行できます。この 2 つのデータベースには個別のエントリが格納されます (IP アドレスは重複しません)。そのため、トレンドマイクロは極めて動的なスパムメールの発信元に素早く対応できる、非常に効果的で効率的なデータベースを維持できます。「メールレピュテーション : Advanced」サービスは、お客さまのネットワークでこれまで全受信接続 (すべて不正接続) の 80% 以上をブロックしています。この結果は、受信メールストリームに占めるスパムメールの量により異なります。受信するスパムメールが多いほど、ブロックされる接続の割合は高くなります。

メールレピュテーションテクノロジの仕組み

トレンドマイクロのメールレピュテーションテクノロジは、ドメインネームサービス (DNS) クエリベースのサービスです。InterScan MSS が送信メールサーバから接続要求を受信すると、次の処理が発生します。

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

図 2-1 は、メールレピュテーションの仕組みを示しています。

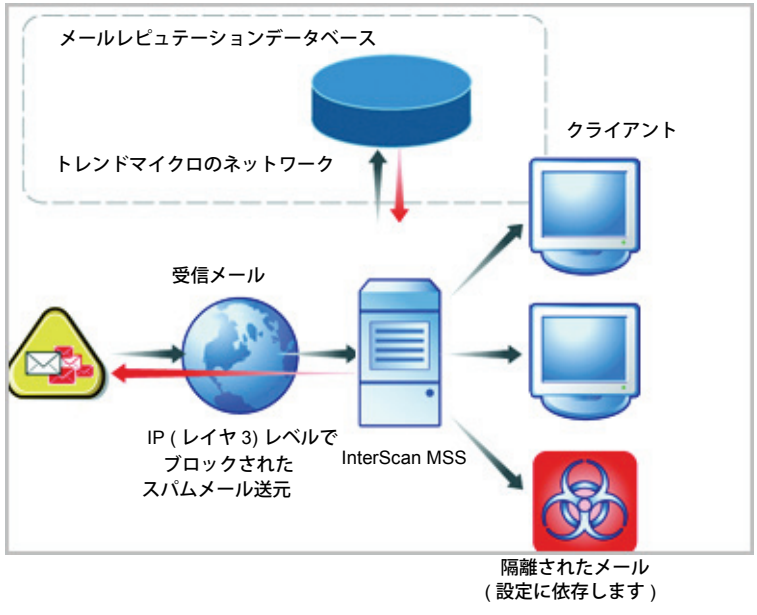


図 2-1.　メールレピュテーションの仕組み

メールレピュテーションの動作の詳細については、
http://jp.trendmicro.com/jp/products/enterprise/ers/ersa/index.html を参照してください。

メールレピュテーション管理コンソールを使用する

メールレピュテーション管理コンソールにログオンすると、グローバルスパムメール情報へのアクセス、レポートの表示、メールレピュテーション設定の作成や管理、および管理作業を実行できます。

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

メールレピュテーション管理コンソールを開くには

1. Web ブラウザを開き、次のアドレスを入力します。

   https://tmspn.securecloud.com/

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

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

表 2-1. ISP 毎の送信量

列	説明
ランク (今週)	今週のグローバルランクをスパムメールの総量に基づいて表示します。
ランク (先週)	先週のグローバルランクをスパムメールの総量に基づいて表示します。
ASN	Autonomous System Number (ASN) は、1 社以上の通信事業者が運営する、明確に定義された単一のルーティングポリシーを持つ IP ネットワークのグループに対するグローバル一意識別子です。
ISP 名	特定の ASN に対する登録名。一部の ISP では複数の ASN を保有していることがあります。この場合、テーブルに複数個登録されます。
スパムメール量 (24 時間)	過去 24 時間内に送信されたスパムメールの推定総量。この総量は 1 時間ごと更新されます。
ボットネット活動	メールサーバに対するボットネットの活動状況の指標。ボットネットとは、中央からスパムメール送信元によって制御されている、ウイルスに感染したコンピュータのグループのことであり、現在インターネット上で最大のスパムメール送信元となっています。この数値は、1 時間前からのボット数におけるパーセント比率の変化を示します。ボットネットの活動を確認するには、[有効なメールサーバ] リストにメールサーバを追加する必要があります。

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

[リリースアップデート] 画面には、新しいスパムメールに関する最新情報と、メールレピュテーションで使用可能な新機能が表示されます。次のタブをクリックすると情報が表示されます。

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

5. MTA とメールレピュテーションデータベースサーバ間の動作をまとめたレポートを表示するには、次の操作を実行します。
   a. メニューから [レポート] を選択します。サブメニューが表示されます。
   b. 次のいずれかをクリックします。

表 2-2. レポートの種類

レポート	説明
クエリの割合	このレポートは、IP アドレスの一致を返したクエリのパーセント比率を表示します。IP アドレスの一致は、メールサーバとの接続を確立しようとする送信者が、既知のスパムメール送信元であることを示します。レポートは、個々のスパムメールメッセージではなく、接続に基づいて作成されます。
1 時間あたりのクエリ数	このレポートは、メールサーバがレピュテーションデータベースにクエリを実行した回数を表示します。
1 日あたりのクエリ数	このレポートは、メールサーバがレピュテーションデータベースにクエリを実行した 1 日あたりの回数を表示します。
ボットネットレポート	このレポートは、有効なメールサーバとして登録されているサーバを発信元とする、過去 7 日間のスパムメール活動の簡単な概要を示します。指定した IP アドレスのいずれかにおいて、過去 7 日間にスパムメール活動が見つかった場合には、赤いロボットアイコンが表示されます。

6. メールレピュテーション設定によって提供される保護を管理するには
   a. メニューから [ポリシー] を選択します。サブメニューが表示されます。

b. 次のいずれかをクリックします。

表 2-3. ポリシー設定

ポリシー	説明
設定	承認済み送信者リストとブロックする送信者リストを設定します。国別または ISP 別の個々の IP アドレスおよび CIDR ごとに、リストを定義できます。 • **承認済み送信者 (許可タブ)**: 特定の国、ISP、および IP アドレスからのメールメッセージを常に許可するように ERS に指定します。 • **ブロックする送信者 (ブロックタブ)**: 特定の国、ISP、および IP アドレスからのメールメッセージを常にブロックするように ERS に指定します。
新規 ISP のリクエスト	トレンドマイクロでは、サービスに追加する他のインターネットサービスプロバイダ (ISP) に関する、お客さまからの助言をお待ちしています。 できる限り多くの ISP に関する情報を記入してください。この情報を参考にして、トレンドマイクロが ISP をサービスに追加します。
Reputation 設定	メールレピュテーションの Standard 設定および Advanced 設定を行います。 Standard のお客さまには、[Standard 設定を有効にする] のみが表示されます。 Advanced のお客さまには、[Dynamic 設定] セクションと [Standard 設定を有効にする] セクションの両方が表示されます。

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

エンドユーザメール隔離について

InterScan MSS では、スパムメールの管理効率を向上させるために、Web ベースのエンドユーザメール隔離機能を提供しています。Web ベースのエンドユーザメール隔離サービスを使用することで、エンドユーザは独自のスパムメール隔離を管理できます。(InterScan MSS とは別のライセンスとなる) スパムメール対策 (コンテンツ検索) または管理者が作成したコンテンツフィルタでスパム

メールと判断されたメッセージは、隔離領域に移動されます。これらのメッセージは、エンドユーザメール隔離エージェントによってデータベース内でインデックスが付けられます。これにより、エンドユーザはメッセージを再確認して、削除したり配信を許可したりできるようになります。

一元化されたレポート機能について

InterScan MSS の実行内容を分析するには、一元化されたレポート機能を使用します。(要求に応じた) 1 回限りのレポートまたは自動生成レポート (日次、週次、または月次) を設定することができます。

第 3 章

配置計画

本章では、InterScan MSS の配置を計画する方法について説明します。

この章の内容は次のとおりです。

配置チェックリスト

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

表 3-1.　配置チェックリスト

チェックマーク (完了時)	タスク	オプション	参照
	手順 1 — InterScan MSS の場所の特定		
	InterScan MSS をインストールするネットワーク上の場所を、次のいずれかから選択します。		
	・ ファイアウォールなし		52 ページの「ファイアウォールを使用しないインストール」
	・ ファイアウォールの外側		52 ページの「ファイアウォールの外側へのインストール」
	・ ファイアウォールの内側		53 ページの「ファイアウォールの内側へのインストール」
	・ 既存の SMTP ゲートウェイ上		54 ページの「既存の SMTP ゲートウェイ上へのインストール」
	・ DMZ 内		55 ページの「DMZ 内へのインストール」
	手順 2 — 範囲の計画		
	InterScan MSS をインストールするのは、単一のサーバか複数のサーバかを選択します。		
	・ 集中インストール		56 ページの「集中インストール」
	・ 複数の検索サービス		58 ページの「複数の検索サービスのインストール」
	・ 複数のエンドユーザメール隔離		60 ページの「複数のエンドユーザメール隔離サービスのインストール」

表 3-1.　配置チェックリスト（続き）

チェックマーク ☑（完了時）	タスク	オプション	参照
	• 複雑な分散インストール		63 ページの「複雑な分散インストール」
	• 広域ネットワーク		65 ページの「WAN へのインストール」
	• IP フィルタ ヒント：フェイルオーバーの方法を検討してから、範囲を決定することをお勧めします。		68 ページの「IP フィルタ」
	手順 3 — インストールまたはアップグレード		
	InterScan MSS の新規インストールまたは以前のバージョンからのアップグレードを実行します。		
	• InterScan MSS コンポーネントのインストール		86 ページの「複数の検索サービスとエンドユーザメール隔離サービス / データベースのインストール」
	手順 4 — InterScan MSS の基本設定		
	設定ウィザードに従って、セントラルコントローラの設定を手順 8 まで進めます。		
	設定ウィザードを使用した設定		管理者ガイドの「設定ウィザードでの基本設定の実行」の項
	手順 5 — サービスの開始		
	さまざまな脅威からネットワークを保護する、InterScan MSS サービスを起動します。		

表 3-1.　配置チェックリスト（続き）

チェックマーク ☑（完了時）	タスク	オプション	参照
	• 検索サービス		管理者ガイドの「InterScan MSS サービス」の項
	• ポリシー		
	• エンドユーザメール隔離	あり	
	手順 6 — InterScan MSS のその他の設定		
	InterScan MSS のさまざまな設定を行い、InterScan MSS を起動します。		
	• IP フィルタのルール	あり	管理者ガイドの「IP フィルタ サービス」の項
	• SMTP ルーティング		管理者ガイドの「SMTP メッセージの検索」の項
	• POP3 設定	あり	管理者ガイドの「POP3 メッセージの検索」の項
	• ポリシーおよび検索の除外		管理者ガイドの「ポリシーの管理」の項
	• コンポーネントの手動アップデートの実行と予約アップデートの設定		管理者ガイドの「検索エンジンとパターンファイルのアップデート」の項
	• ログの設定		管理者ガイドの「ログの設定」の項
	手順 7 — InterScan MSS のバックアップ		
	システム障害時の予防措置として、InterScan MSS のバックアップを実行します。		
	InterScan MSS 管理データベースのバックアップを作成します。		管理者ガイドの「InterScan MSS のバックアップ」の項

コンポーネントおよびサブモジュールのインストール

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

表 3-2.　コンポーネントおよびサブモジュールのインストール

メインコンポーネント	インストールされるサブモジュール	サブモジュールの説明
InterScan MSS 管理データベース	管理データベース	すべてのグローバル設定を格納するメインの InterScan MSS 管理データベース。
	データベースサーバ *	InterScan MSS 管理データベースが実行されるサーバ。
セントラルコントローラ	Apache Tomcat	InterScan MSS 管理コンソール用の Web サーバで、これを使用して設定を実行します。
	Named Server	IP プロファイラ用の DNS サーバ。
	FoxDNS	IP プロファイラ用の IP アドレスのブロックリストおよび許可リストが含まれており、そのリストを DNS サーバに書き込みます。
	IMSSMGR	InterScan MSS 関連のプロセスを管理するモジュール。
検索サービス	検索サービス	すべてのメールの検索処理を実行します。
	ポリシーサービス	検索サービスに対するルールのリモートストア。ルールがキャッシュされるため、データベース検索が不要になります。
	IMSSMGR	検索サービスプロセスを管理するモジュール。
	SMTP サービス	Trend Micro MTA/MDA
	IP プロファイラ	Trend Micro MTA の一部
	メールレピュテーション	Trend Micro MTA の一部
エンドユーザメール隔離サービス	Apache Tomcat	エンドユーザメール隔離管理コンソール用の Web サーバ。これによって、ユーザはスパムメールとして隔離されたメールメッセージにアクセスできます。
	Apache サービス	複数のエンドユーザメール隔離サービスのインストールを選択した場合は、負荷分散のためにプライマリエンドユーザメール隔離サービスを備えたこのモジュールをインストールします。
	IMSSMGR	エンドユーザメール隔離プロセスを管理するモジュール。

表 3-2.　コンポーネントおよびサブモジュールのインストール（続き）

メインコンポーネント	インストールされるサブモジュール	サブモジュールの説明
エンドユーザメール隔離データベース	エンドユーザメール隔離データベース	スパムメールとして隔離されたすべてのメールメッセージを含むデータベース。
	データベースサーバ *	エンドユーザメール隔離データベースが実行されるサーバ。

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

InterScan MSS ポート

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

表 3-3.　InterScan MSS ポート

ポート番号	コンポーネントと役割	設定の保存先
25	MTA のサービスポート。メールサーバは、このポートで待機してメッセージを受信します。ファイアウォールでは、このポートを開放する必要があります。開放されていないと、メールを受信できません。	管理コンソールのメニューから、[管理] → [InterScan MSS の設定] → [SMTP ルーティング] → [接続] の順にクリックします。
110	InterScan MSS 検索サービス用の一般 POP3 ポート。検索サービスはこのポートを使用して、POP3 要求を受け入れ、POP3 メールを検索します。	管理コンソールのメニューから、[管理] → [InterScan MSS の設定] → [接続] → [POP3] の順にクリックします。
5060	ポリシーサーバ待機ポート。検索サービスはこのポートに接続して、すべてのメッセージに対して一致するルールがないかどうか問い合わせます。	管理コンソールのメニューから、[管理] → [InterScan MSS の設定] → [接続] → [コンポーネント] の順にクリックします。

表 3-3. InterScan MSS ポート（続き）

ポート番号	コンポーネントと役割	設定の保存先
8005	Tomcat 管理コマンドを処理する Admin Web サーバ (Tomcat) 管理ポート。	{InterScan MSS}/UI/adminUI/conf/server.xml: Server / port
8009	エンドユーザメール隔離コンソール Tomcat AJP ポート。このポートを使用して、複数の Tomcat サーバと Apache HTTP サーバ間の負荷分散を実行します。	{InterScan MSS}/UI/euqUI/conf/server.xml: Server / Service / Connector (protocol=AJP/1.3) / port
8015	Tomcat 管理コマンドを処理する Tomcat 管理ポート。	{InterScan MSS}/UI/euqUI/conf/server.xml: Server/port
8445	InterScan MSS 管理コンソール待機ポート。Web ブラウザを使用して管理コンソールにログオンするには、このポートを開放します。	Tomcat 待機ポート : {InterScan MSS}/UI/adminUI/conf/server.xml: Server / Service / Connector / port
8446	エンドユーザメール隔離サービス待機ポート。	{InterScan MSS}/UI/euqUI/conf/server.xml: Server / Service / Connector / port
8447	負荷分散したエンドユーザメール隔離の待機ポート。	{InterScan MSS}/UI/euqUI/conf/EUQ.conf: Listen / VirtualHost / ServerName
10024	InterScan MSS 検索サービスの再処理ポート。管理データベースの中央隔離領域やエンドユーザメール隔離データベースから隔離解除されたメッセージは、このポートを通して送信され再処理されます。	imss.ini / [socket_2] / proxy_port

表 3-3. InterScan MSS ポート（続き）

ポート番号	コンポーネントと役割	設定の保存先
10026	InterScan MSS によって生成された通知メッセージの配信など、内部使用向けの InterScan MSS「パススルー」SMTP ポート。 このポートを通して送信されたすべてのメッセージは、InterScan MSS によって検索されません。セキュリティを考慮しているため、このポートがバインドされているのはInterScan MSS サーバのループバックインタフェース (127.0.0.1) のみです。そのため、他のコンピュータからはアクセスできません。ファイアウォールでは、このポートを開放する必要がありません。	tsmtpd.ini
15505	InterScan MSS マネージャの待機ポート。InterScan MSS マネージャは、このポートを使用して管理コンソールからの管理コマンド (サービスの起動 / 停止など) を受け入れます。また、隔離 / アーカイブのクエリ結果も、このポートを使用して管理コンソールおよびエンドユーザメール隔離管理コンソールに送信されます。	管理コンソールのメニューから、[管理] → [InterScan MSS の設定] → [接続] → [コンポーネント] の順にクリックします。
関連するサービスを有効にしている場合、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 管理コンソールのメニューから、[管理] → [InterScan MSS の設定] → [接続] → [LDAP] の順にクリックします。

表 3-3.　InterScan MSS ポート（続き）

ポート番号	コンポーネントと役割	設定の保存先
80	Microsoft IIS HTTP 待機ポート。Control Manager サーバが Microsoft IIS に依存している場合、Control Manager を使用して InterScan MSS を管理する際に、このポートが必要になります。	管理コンソールのメニューから、[管理] → [InterScan MSS の設定] → [接続] → [Control Manager サーバ] の順にクリックします。
443	Microsoft IIS HTTPS 待機ポート。Control Manager サーバが Microsoft IIS に依存している場合、Control Manager を使用して InterScan MSS を管理する際に、このポートが必要になります。	管理コンソールのメニューから、[管理] → [InterScan MSS の設定] → [接続] → [Control Manager サーバ] の順にクリックします。
88	Kerberos レルム用 KDC ポート。	InterScan MSS サーバからは設定できません。
53	Bind サービス待機ポート。別のポート番号を割り当てないでください。	InterScan MSS サーバからは設定できません。

ネットワークトポロジに関する考慮事項

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

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

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

ファイアウォールを使用しないインストール

図 3-1. は、ネットワークでファイアウォールを使用しない場合の InterScan MSS の配置方法を示しています。

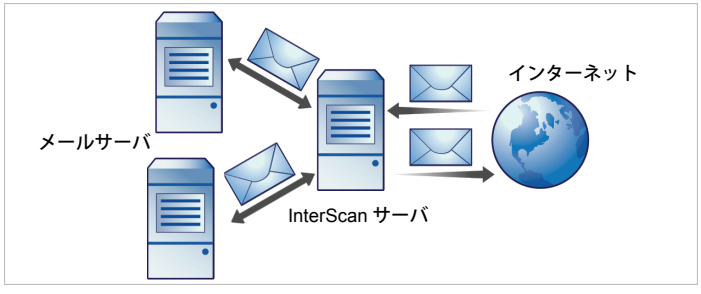


図 3-1.　インストールトポロジ : ファイアウォールなし

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

ファイアウォールの外側へのインストール

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

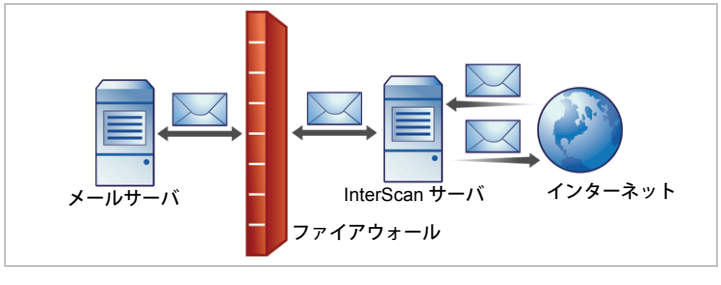


図 3-2.　インストールトポロジ : ファイアウォールの外側

受信トラフィック

- DNS サーバ上の MX レコードを、現在の SMTP ゲートウェイまたはファイアウォールから、InterScan MSS サーバのアドレスまたは検索サービス間の負荷分散を実行するスイッチのアドレスを参照するように変更します。
- ローカルドメインに対するリレーのみが許可されるようにリレー制御を設定します。

送信トラフィック

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

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

ファイアウォールの内側へのインストール

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

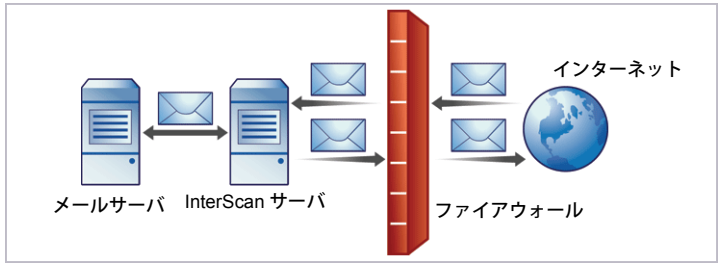


図 3-3.　インストールシナリオ：ファイアウォールの内側

受信トラフィック

- 次のようにプロキシベースのファイアウォールを設定します。
  - 送信 SMTP メールが InterScan MSS サーバか、検索サービス間の負荷分散を実行するスイッチに転送される。
  - 受信 SMTP メールは InterScan MSS サーバ経由でのみ送信される。
- 次のようにパケットベースのファイアウォールを設定します。
  - InterScan MSS をホストしているサーバのアドレスを参照するように、現在 SMTP ゲートウェイを参照している DNS サーバの MX レコードを変更する。
  - 安全なサブネットを管理するように InterScan MSS またはファイアウォールを設定している場合は、MX レコードが InterScan MSS またはファイアウォールをポイントするように設定する。
- ローカルドメイン宛てのメールが SMTP ゲートウェイまたは内部メールサーバに転送されるように InterScan MSS を設定します。
- ローカルドメインに対するリレーのみが許可されるように、リレーの制約を設定します。

送信トラフィック

- 送信メールが InterScan MSS サーバに送信されるように、すべての内部 SMTP ゲートウェイを設定します。
- SMTP ゲートウェイを InterScan MSS と置き換える場合は、送信メールが InterScan MSS サーバに転送されるように内部メールサーバを設定します。
- ローカル以外のドメイン宛てのすべての送信メールをファイアウォールに転送するか、外部 DNS サーバを使用して直接配信するように、InterScan MSS を設定します。
- InterScan MSS を使用したすべてのドメインへのリレーが内部 SMTP ゲートウェイで許可されるように InterScan MSS を設定します。

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

既存の SMTP ゲートウェイ上へのインストール

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

SMTP ゲートウェイ上で

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

受信トラフィック

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

送信トラフィック

- 送信メールが InterScan MSS のポート 25 に転送されるように、SMTP ゲートウェイを設定します。
- ローカル以外のドメイン宛てのすべての送信メールをファイアウォールに転送するか、外部 DNS サーバを使用して直接配信するように、InterScan MSS を設定します。

DMZ 内へのインストール

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

受信トラフィック

- 受信および送信 SMTP メールが DMZ 経由でのみ内部メールサーバに送信されるように、プロキシベースのファイアウォールを設定します。
- 現在 SMTP ゲートウェイを参照している DNS サーバ上のメール交換 (MX) レコードが、InterScan MSS をホストしているサーバのアドレス、または検索サービス間の負荷分散を実行しているスイッチのアドレスを参照するように、パケットベースのファイアウォールを再設定します。
- ローカルドメイン宛てのメールが SMTP ゲートウェイまたは内部メールサーバに転送されるように InterScan MSS を設定します。

送信トラフィック

- ローカル以外のドメイン宛てのすべての送信メールをファイアウォールに転送するか、外部 DNS サーバを使用して直接配信するように、InterScan MSS を設定します。
- 送信メールが InterScan MSS に転送されるように、すべての内部 SMTP ゲートウェイを設定します。
- 内部 SMTP ゲートウェイで、すべてのドメインへの InterScan MSS 経由のリレーが許可されるように InterScan MSS を設定します。

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

インストールシナリオについて

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

集中インストール

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

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

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

- IP フィルタサービス

注意： IP フィルタサービスを使用するには、InterScan MSS をエッジ MTA として配置する必要があります。

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。

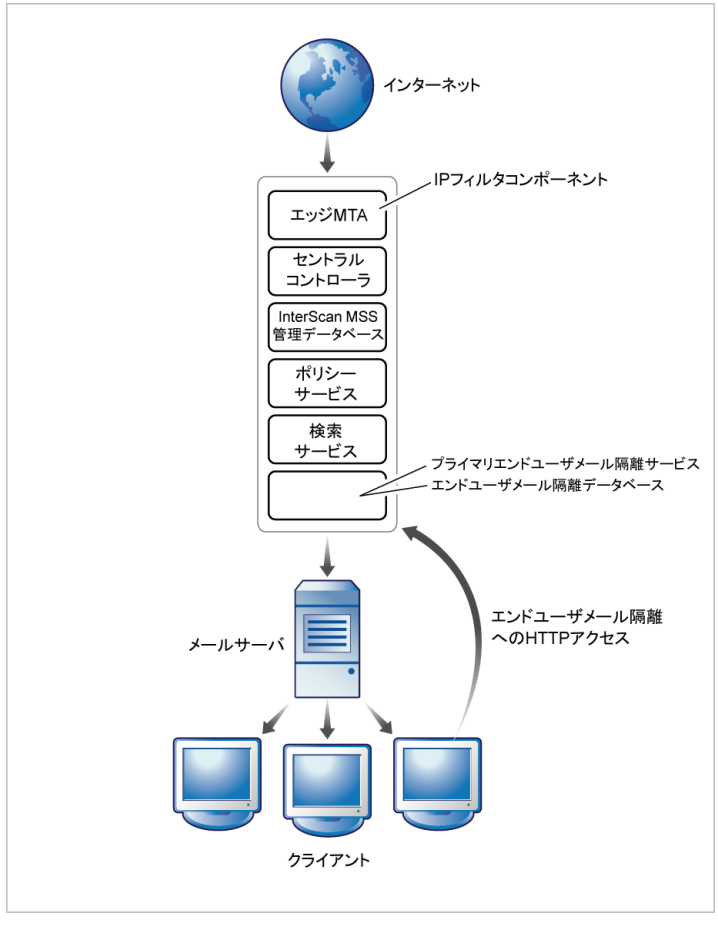


図 3-4.　単一サーバ配置

集中インストールを実行するには

1. InterScan MSS およびエンドユーザメール隔離をインストールします (72 ページの「集中インストール」を参照)。

複数の検索サービスのインストール

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

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

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

図 3-5. は、2 つの検索サービスが追加された InterScan MSS の集中インストールが標準のメッセージングネットワークトポロジにどのように適合するかを示しています。

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

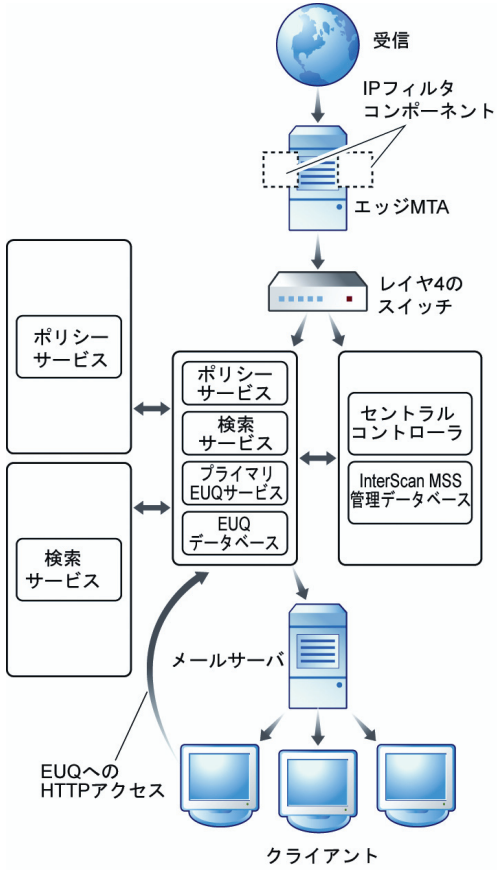


図 3-5.　複数の検索サービスとポリシーサービスの配置

複数の検索サービスのインストールを実行するには

1. 1 台のコンピュータに、InterScan MSS およびエンドユーザメール隔離をインストールします (97 ページの「複雑な分散インストール」を参照)。
2. その他のコンピュータに、必要な検索サービスとポリシーサービスをインストールします。

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

---

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

複数のエンドユーザメール隔離サービスのインストール

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

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

注意： 最大 8 つのエンドユーザメール隔離サーバおよびエンドユーザメール隔離データベースをインストールできます。

図 3-6. は、個々のプライマリエンドユーザメール隔離サービスと追加のセカンダリエンドユーザメール隔離サービス (負荷分散のための Apache サービスを含む)、および分散エンドユーザメール隔離データベースが追加された InterScan MSS の集中インストールが、標準のメッセージングネットワークトポロジにどのように適合するかを示しています。

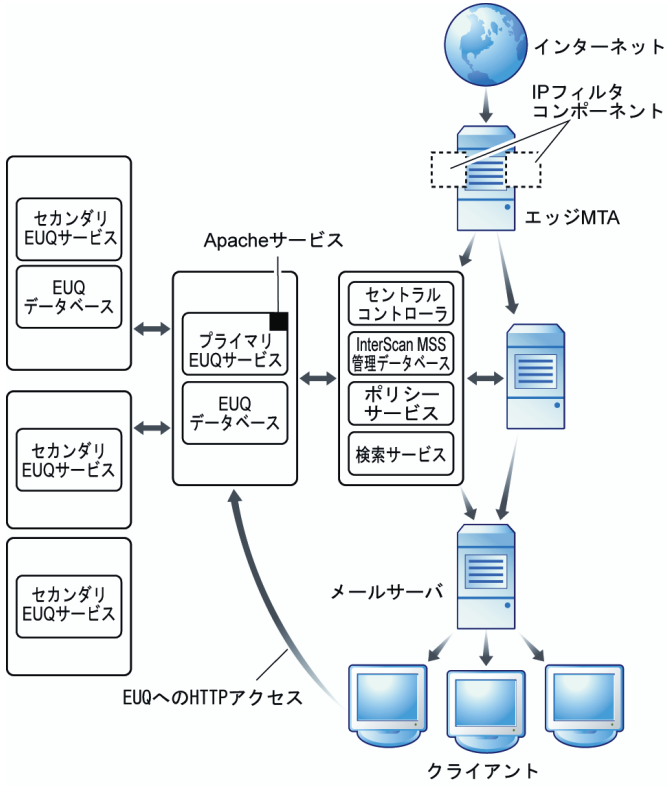


図 3-6.　複数のエンドユーザメール隔離サービスの配置

複数のエンドユーザメール隔離サービスのインストールを実行するには

1. 1 台のコンピュータに、InterScan MSS をインストールします (72 ページの「集中インストール」または 97 ページの「複雑な分散インストール」を参照)。
2. 別のコンピュータに、単一インスタンス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。これが、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。
3. プライマリエンドユーザメール隔離サービスと通信できるその他のコンピュータに、追加のエンドユーザメール隔離サービスをインストールします。エンドユーザメール隔離サービス用に、少なくとも 1 つのエンドユーザメール隔離データベースをインストールする必要があります。パフォーマンスを向上させるために、追加のエンドユーザメール隔離データベースをインストールすることもできます。

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

4. InterScan MSS 管理コンソールを開いて初期設定を実行したら（管理者ガイドの「設定ウィザードでの基本設定の実行」と「InterScan MSS の設定」の項を参照）、[概要] → [システム] 画面に移動します。
5. 有効にするエンドユーザメール隔離サービスで、[開始] をクリックします。

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

エンドユーザメール隔離を配置する際のその他の検討事項

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

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

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

詳細については、72 ページの「集中インストール」または 97 ページの「複雑な分散インストール」を参照してください。

サーバ間の通信

内部ファイアウォールを使用する場合は、InterScan MSS、エンドユーザメール隔離、およびデータベース間の通信が許可されるようにファイアウォールを設定します。たとえば、1 つのサーバにエンドユーザメール隔離サービスを、もう 1 つのサーバにデータベースをインストールする場合は、2 つのサーバ間にあるファイアウォールを、データベース接続用のポート上の通信が許可されるように設定します。

複雑な分散インストール

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

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

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

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

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

図 3-7. は、複数の検索サービス、ポリシーサービス、およびエンドユーザメール隔離サービス (負荷分散用 Apache サービスを含む) が追加された一元化された InterScan MSS インストールが、標準のメッセージングネットワークトポロジにどのように適合するかを示しています。

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

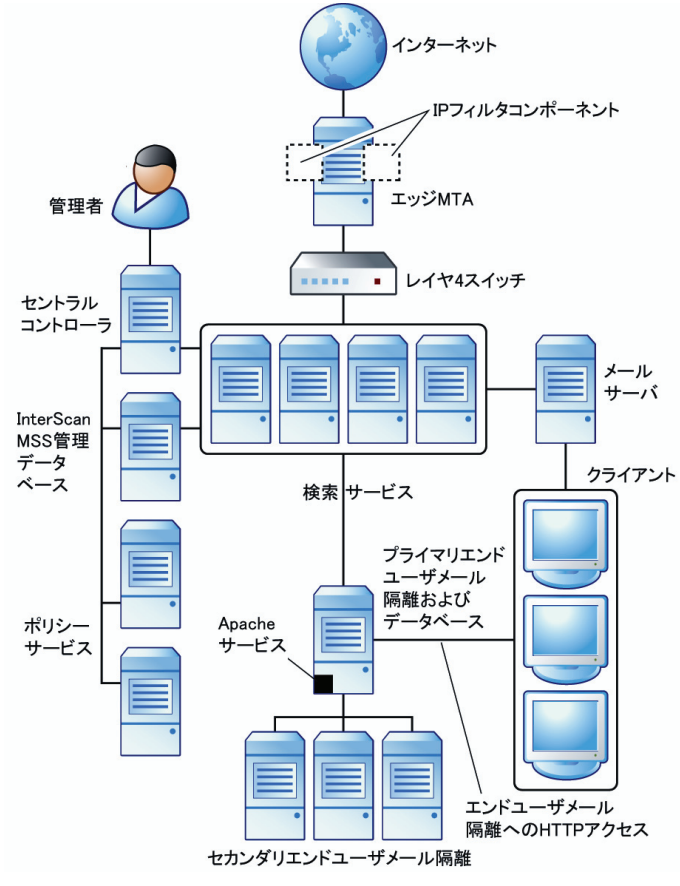


図 3-7.　複雑なアーキテクチャの配置

WAN へのインストール

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

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

Control Manager

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

ヒント： セントラルコントローラがインストールされているすべての InterScan MSS サーバを簡単に管理するために、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。

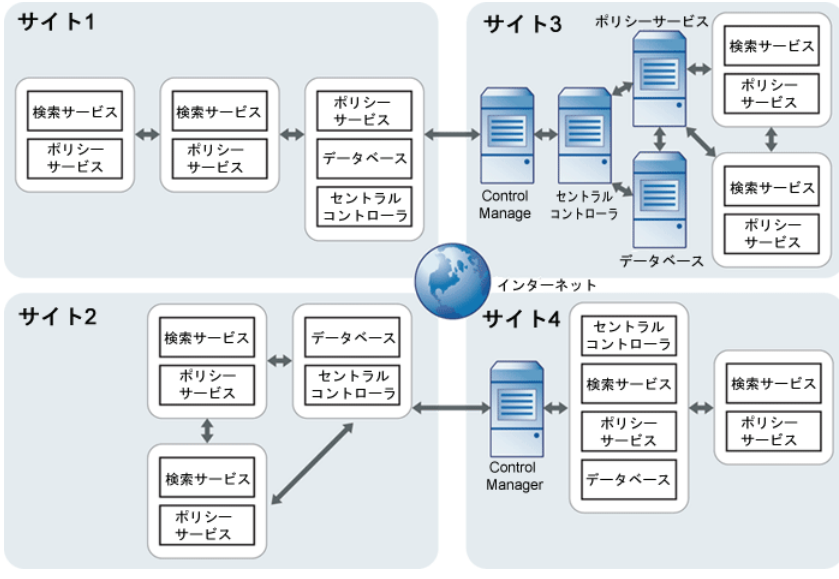


図 3-8.　WAN での配置

このシナリオでの各サイトの違いは次のようになります。

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

WAN のシナリオにおけるフォールトトレランスとフェイルオーバー

このシナリオでは、4 つのサイトのうち 3 つが、ポリシーサービスがインストールされた複数の検索サービスを使用します。ポリシーサービスは、キャッシュされた InterScan MSS 設定に InterScan MSS 管理データベースからアクセスできます。ポリシーサービスの機能が停止している検索サービスでは、別の有効なポリシーサービスを使用できます。したがって、1 つのポリシーサービスが停止したり、セントラルデータベースとの通信が中断したりしても、検索サービスは InterScan MSS サーバに接続されている有効なポリシーサービスを使用して動作を続け、メールの処理を継続します。図 3-9 を参照してください。

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

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

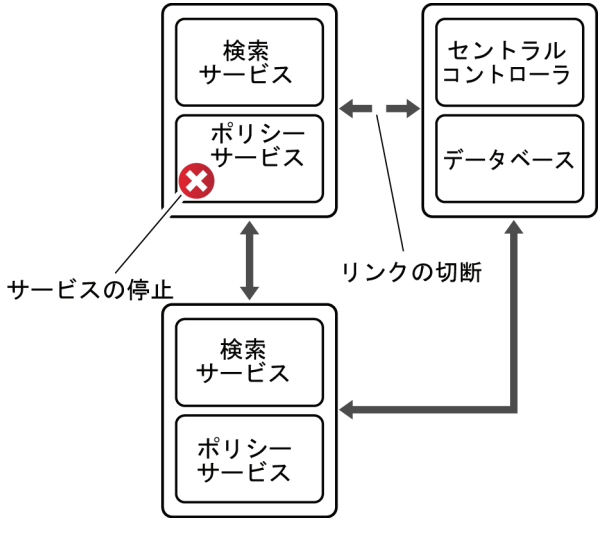


図 3-9.　フェイルオーバー

IP フィルタ

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

IP フィルタ機能を持つ InterScan MSS の配置

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

注意： ネットワークのエッジから InterScan MSS 接続までの区間で、アドレス変更はできません。つまり、InterScan MSS とネットワークエッジの間に配置されるファイアウォールは、接続 IP アドレスを変更しないタイプのものであるか、変更しないように設定されている必要があります。

たとえば InterScan MSS がルータからの SMTP 接続を常に受け入れる場合は、IP フィルタは機能しません。これは、このアドレスがどの受信メッセージでも同じになり、IP フィルタソフトウェアが、SMTP セッションの開始者が既知のスパムメール送信者であるかどうかを判断できなくなるためです。

フェイルオーバーについて

表 3-4 に、InterScan MSS コンポーネントの障害時に発生する問題点、および InterScan MSS の保護機能を維持したまま実行するフェイルオーバーの方法を示します。WAN での配置シナリオにおけるフェイルオーバーの詳細については、67 ページの「WAN のシナリオにおけるフォールトトレランスとフェイルオーバー」を参照してください。

表 3-4. フェイルオーバーシナリオ

障害のあるコンポーネント	予測される結果	推奨フェイルオーバー
検索サービスが起動しない、または切断される	1. InterScan MSS は検索サービスの再起動を試行します。 2. サービスが、指定した時間以内に起動できない場合には、イベント通知が送信されます。	負荷分散とフェイルオーバーのために、複数の検索サービスをインストールします。詳細については、58 ページの「複数の検索サービスのインストール」を参照してください。
ポリシーサービスが起動しない、または InterScan MSS サーバとの通信に問題が発生する	1. 停止したポリシーサービスを使用している検索サービスは、有効なポリシーサービスがある場合、そのサービスへ切り替えます。 2. InterScan MSS はポリシーサービスの再起動を試行します。 3. サービスが、指定した時間以内に起動または再接続できない場合には、イベント通知が送信されます。	負荷分散とフェイルオーバーのために、複数の検索サービスをインストールします。詳細については、58 ページの「複数の検索サービスのインストール」を参照してください。
InterScan MSS 管理データベースが動作しない	1. InterScan MSS サーバは、動作を続行します。	管理データベースのバックアップを定期的に作成します。 http://www.microsoft.com/japan/sqlserver/2005/editions/express/default.mspx
エンドユーザメール隔離データベースが動作しない	1. エンドユーザメール隔離管理コンソールにエラーメッセージが表示されます。	エンドユーザメール隔離データベースのバックアップを定期的に作成します。 http://www.microsoft.com/japan/sqlserver/2005/editions/express/default.mspx

表 3-4.　フェイルオーバーシナリオ（続き）

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

第 4 章

InterScan MSS 7.1 のインストールおよびアンインストール

この章では、さまざまなシナリオで Trend Micro InterScan Messaging Security Suite 7.1　(以下、InterScan MSS) をインストールする方法について説明します。

この章の内容は次のとおりです。

システム要件

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

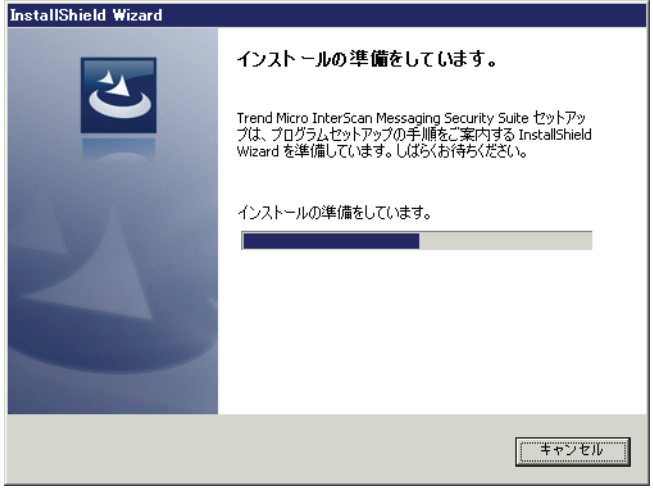
集中インストール

集中インストールとは、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することです。

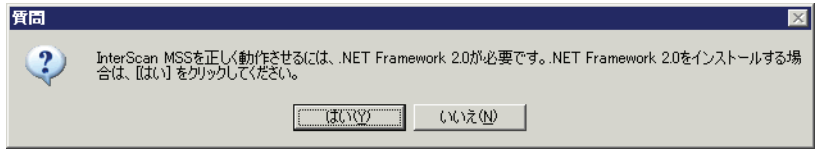
インストールが停止して、上書きできないファイルについてのメッセージが表示された場合は、インストール先フォルダ内のすべてのファイルを手動で削除してから、インストールをやり直してください。場合によっては、インストール先フォルダ下のすべての実行中のアプリケーションを停止する必要があります。たとえば、端末サービスインスタンスによって statmon.exe が実行されている可能性があります。

基本インストールを実行するには

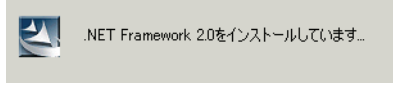
1. Setup.exe をダブルクリックします。[インストールの準備をしています。] 画面が表示されます。

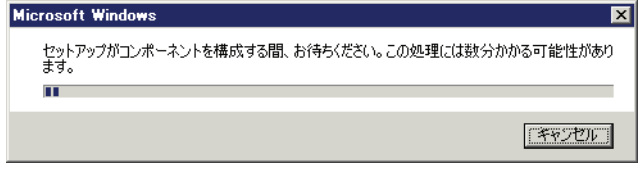


サーバに Microsoft .NET Framework 2.0 がインストールされていない場合は、次のようなダイアログボックスが表示されることがあります。



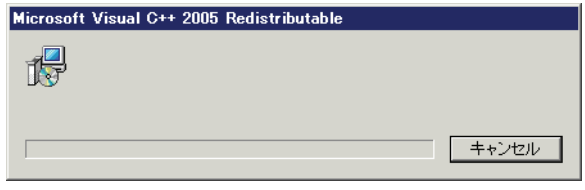
2. [はい] をクリックします。Microsoft .NET Framework 2.0 ランタイムライブラリのインストールが開始されます。



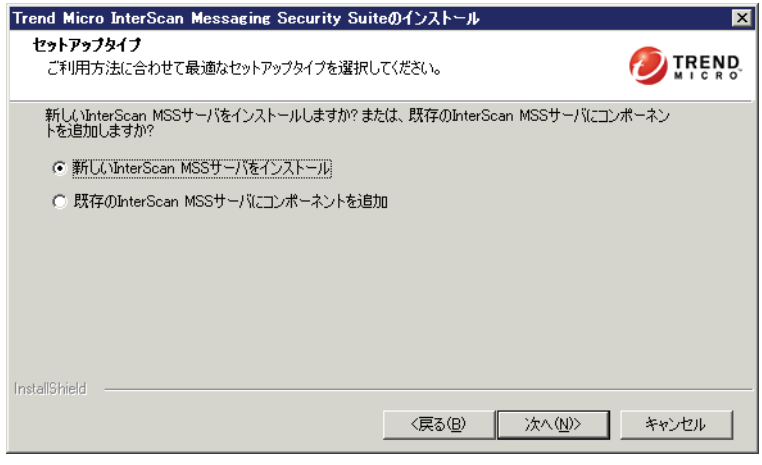


Microsoft Visual C 2005 ランタイムライブラリがインストールされていない場合は、ダイアログボックスが表示されます。

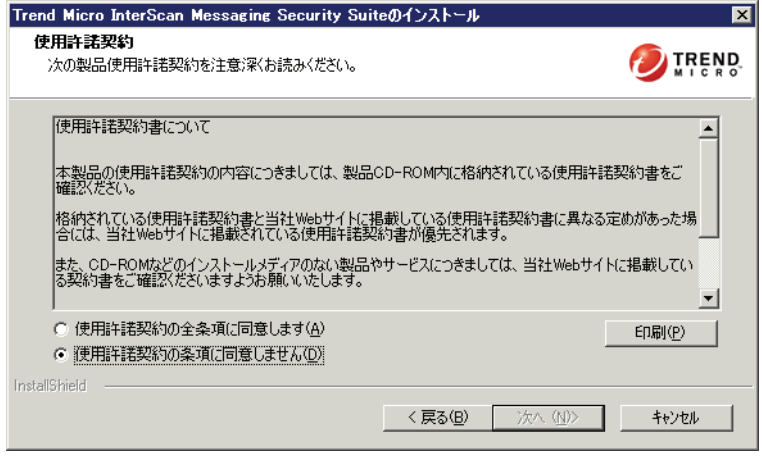
3. [はい] をクリックします。Microsoft Visual C++ 2005 ランタイムライブラリのインストールが開始されます。



4. [次へ] をクリックします。[セットアップタイプ] 画面が表示されます。

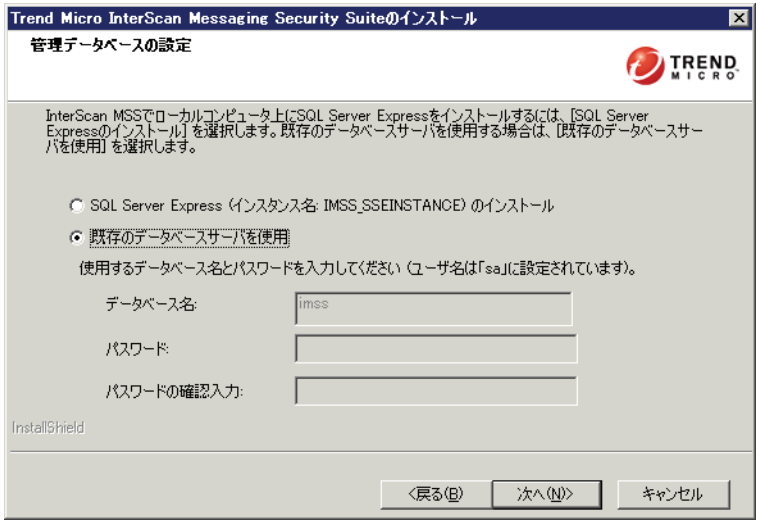


5. [新しい InterScan MSS サーバをインストール] を選択します。
6. [次へ] をクリックします。[使用許諾契約] 画面が表示されます。



7. 使用許諾契約書の内容をよく読んでから、[使用許諾契約の全条項に同意します] を選択します。

8. [次へ] をクリックします。[管理データベースの設定] 画面が表示されます。



既存のデータベースサーバを使用する場合

外部データベースを指定する場合は、外部 SQL Server のリモート接続を有効にします。

リモート接続を有効にしたら、SQL Server Browser サービスを開始します。初期設定の SQL Server は専用ポートで待機しているため、外部プログラムは、SQL Server Browser サービスと通信して、SQL Server の新しい待機ポートを見つける必要があります。このポートが特定のプログラムによってすでに使用されている場合、SQL Server は別のポートを選択します。

外部データベースを選択する際は、そのデータベースが配置されているサーバの DNS レコードが DNS サーバ内に存在する必要があります。そのサーバの IP アドレスまたはホスト名を指定できます。InterScan MSS のセットアッププログラムが、外部データベースが配置されているサーバの DNS レコードに対するクエリを実行できない場合、InterScan MSS は外部データベースに接続できません。

注意： InterScan MSS は、「Windows 認証モード」を使用するデータベースをサポートしていません。

a. [既存のデータベースサーバを使用] を選択します。

b. [次へ] をクリックします。既存のデータベースサーバの必要な情報を入力します。

パスワードには、英数字と記号 (`、~、!、@、#、$、%、^、&、*、(、)、[、]、{、}、+、-、|、:、'、<、>、?、/、,、.、=、_) を使用できます。

注意： ターゲットコンピュータ上に複数のデータベースインスタンスがある場合は、IP アドレスまたはホスト名とインスタンス名の組み合わせを入力します。

ターゲットコンピュータ上に 1 つのデータベースサーバしかない場合でも、そのインスタンス名が初期設定の名前でない場合は、IP アドレスまたはホスト名の後ろにインスタンス名を追加してください。

このサーバに SQL Server Express データベースをインストールする場合

SQL Server Express のインストールをキャンセルした場合、手動クリーンナップを実行する必要があります。次のコンポーネントは自動的に削除されません。

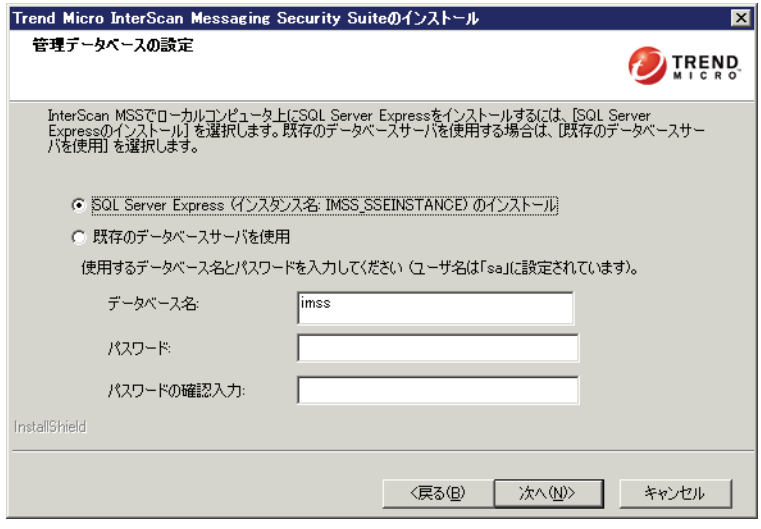
- Microsoft SQL Server Native Client
- Microsoft SQL Server セットアップサポートファイル
- Microsoft SQL Server VSS Writer

SQL Server Express をインストールすると、データベースの初期設定はローカル接続向けになります。データベースへの外部接続が必要な場合は、SQL Server のリモート接続を有効にしてください。

a. [SQL Server Express (インスタンス名 : IMSS_SSEINSTANCE) のインストール] を選択します。

b. 「sa」ユーザアカウントの [データベース名] と [パスワード] を入力します。

パスワードには、英数字と記号 (`、~、!、@、#、$、%、^、&、*、(、)、[、]、{、}、+、-、|、:、'、<、>、?、/、,、.、=、_) を使用できます。



インストールされるデータベースのインスタンスは、IMSS_SSEINSTANCE です。この InterScan MSS インストールに検索サービスを付加する際は、次のように指定します。

< ホスト名 （IP アドレス ）>¥IMSS_SSEINSTANCE

9. [次へ] をクリックします。[インストール先の選択] 画面が表示されます。

10. インストール先ディレクトリを変更するには、[参照] をクリックして目的のディレクトリを指定します。

    Windows Server 2003 x64 プラットフォームでは、InterScan MSS を次のディレクトリにインストールすることはできません。

    `C:¥Program Files¥Trend Micro¥imss`

    Windows Server 2003 x64 プラットフォーム上のこのディレクトリに配置できるのは、x64 プログラムのみです。

    Windows Server 2003 x64 プラットフォームでは、InterScan MSS を次のディレクトリにインストールします。

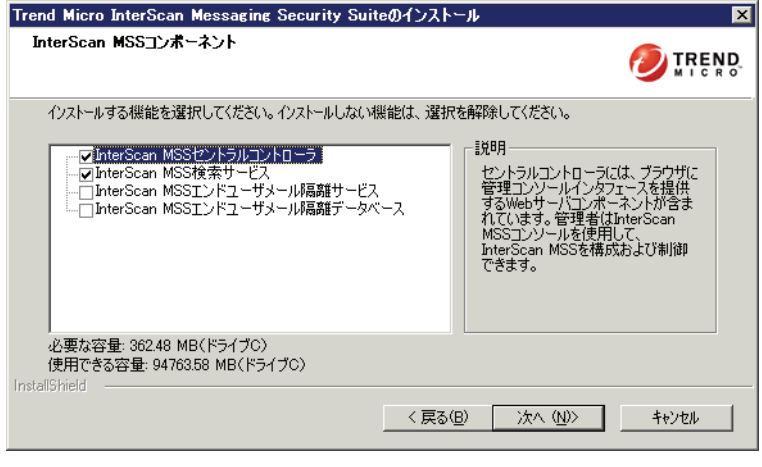
    `C:¥Program Files(x86)¥Trend Micro¥imss`

警告： InterScan MSS は、名前に全角文字を使用しているディレクトリにインストールしないでください。InterScan MSS は、全角文字が使用されたディレクトリの下にインストールすると正しく機能しません。

InterScan MSS は、[内容を暗号化してデータをセキュリティで保護する] という機能が有効化されたディレクトリにはインストールしないでください。InterScan MSS は、この機能が有効化されたディレクトリの下にインストールすると正しく機能しません。

---

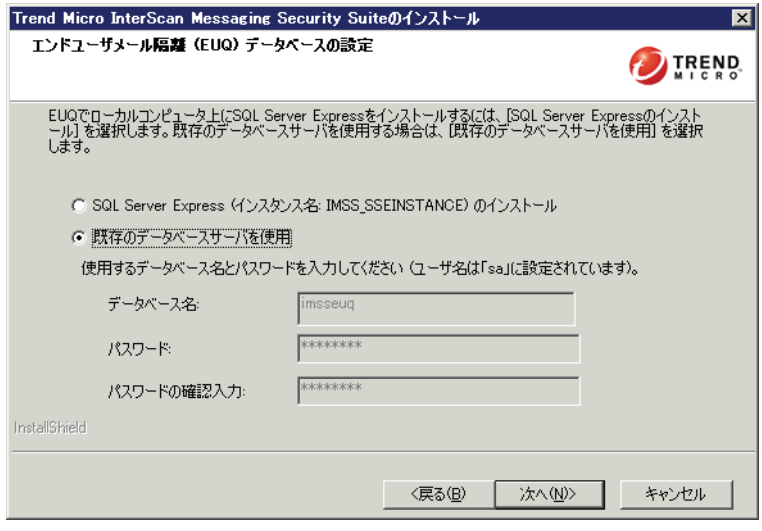
11. [次へ] をクリックします。[InterScan MSS コンポーネント] 画面が表示されます。



12. 必要なコンポーネントを選択します。

    - **InterScan MSS セントラルコントローラ** — セントラルコントローラに含まれている Web サーバコンポーネントにより、管理コンソールを Web ブラウザで表示できるようになります。管理者はこの Web ベースの管理コンソールを使用して、InterScan MSS を設定および制御できます。
    - **InterScan MSS 検索サービス** — 検索サービスは、SMTP と POP3 のメッセージトラフィックを受け入れ、ポリシーサーバに対してポリシーを要求し、適用可能なポリシーに基づいてメッセージを評価して、評価結果に基づいてメッセージに対して適切な処理を実行します。
    - **InterScan MSS 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バには、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。
    - **InterScan MSS エンドユーザメール隔離データベース** — エンドユーザメール隔離データベースは、隔離されたスパムメール情報およびエンドユーザが承認済みの送信者リストを保存します。エンドユーザメール隔離をインストールする場合、エンドユーザメール隔離データベースもインストールする必要があります。スケーラビリティを高めるために、複数のデータベースをインストールすることもできます。

13. [次へ] をクリックします。[InterScan MSS エンドユーザメール隔離データベース] オプションを選択した場合は、[エンドユーザメール隔離　(EUQ) データベースの設定] 画面が表示されます。



既存のデータベースサーバを使用する場合

外部データベースを指定する場合は、外部 SQL Server のリモート接続を有効にします。

リモート接続を有効にしたら、SQL Server Browser サービスを開始します。初期設定の SQL Server は専用ポートで待機しているため、外部プログラムは、SQL Server Browser サービスと通信して、SQL Server の新しい待機ポートを見つける必要があります。このポートが特定のプログラムによってすでに使用されている場合、SQL Server は別のポートを選択します。

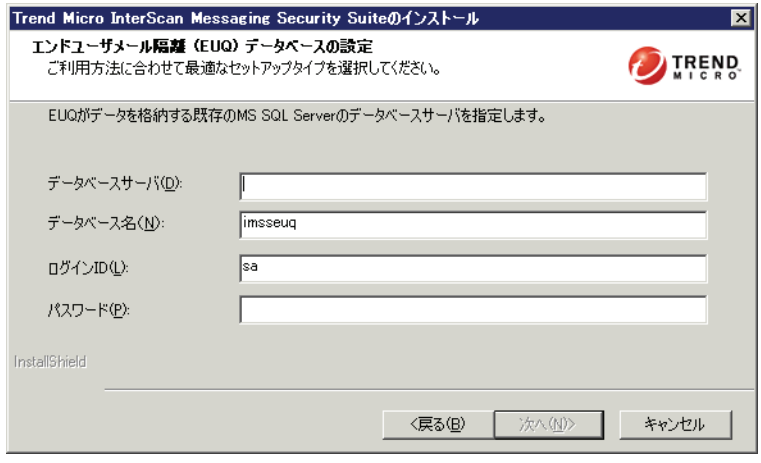
注意： InterScan MSS は、「Windows 認証モード」を使用するデータベースをサポートしていません。

---

a. [既存のデータベースサーバを使用] を選択します。

b. [次へ] をクリックします。既存のデータベースサーバの情報を入力します。

パスワードには、英数字と記号 (`、~、!、@、#、$、%、^、&、*、(、)、[、]、{、}、+、-、|、:、'、<、>、?、/、,、.、=、_) を使用できます。



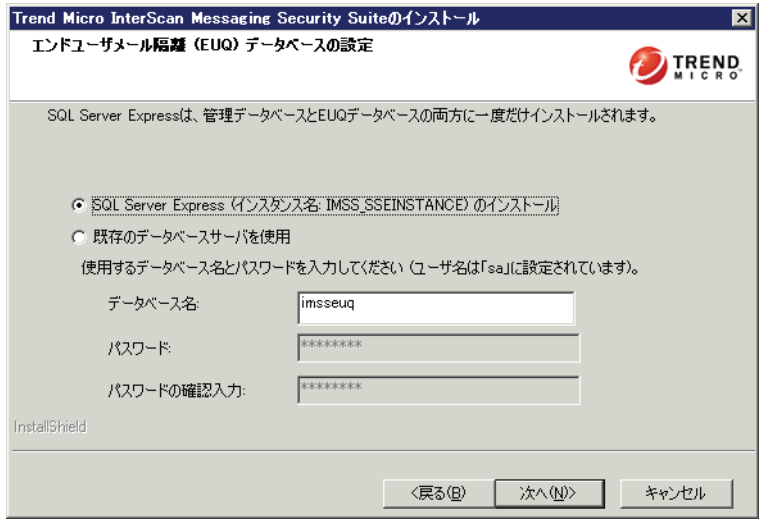
このサーバに SQL Server Express データベースをインストールする場合

SQL Server Express のインストールをキャンセルした場合、手動クリーンナップを実行する必要があります。一部のコンポーネントは自動的に削除されません。

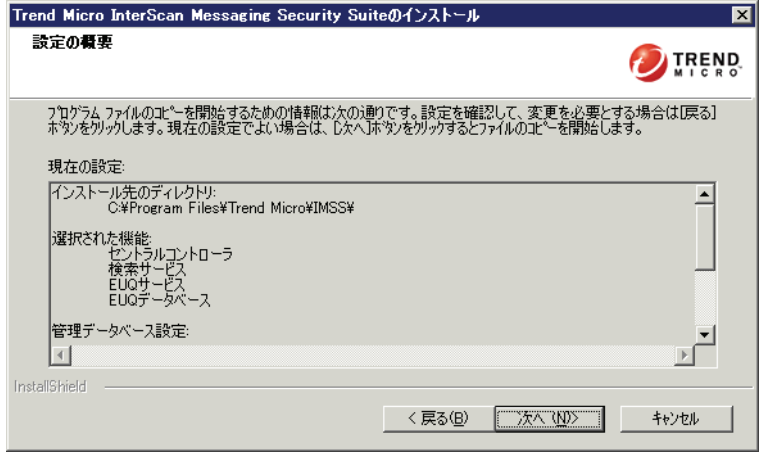
a. [Install SQL Server Express] を選択します。

b. SQL Server Express の「sa」ユーザアカウントの [データベース名] と [パスワード] を入力します。

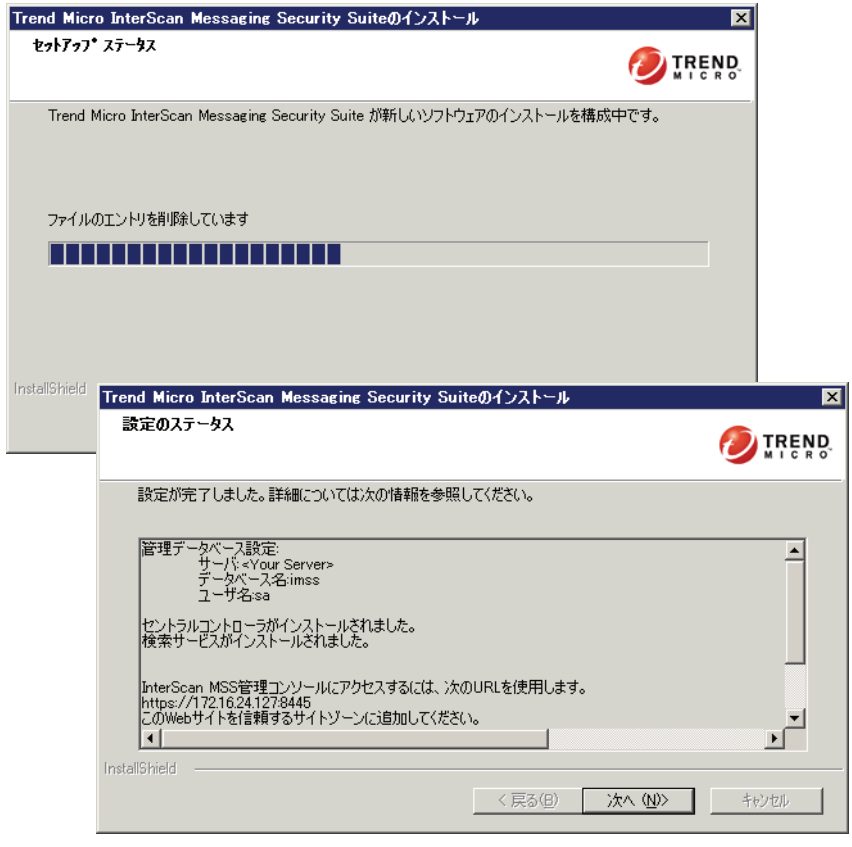
   パスワードには、英数字と記号（`、~、!、@、#、$、%、^、&、*、(、)、[、]、{、}、+、-、|、:、'、<、>、?、/、,、.、=、_）を使用できます。



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。選択したコンポーネントと設定内容が正しいことを確認します。



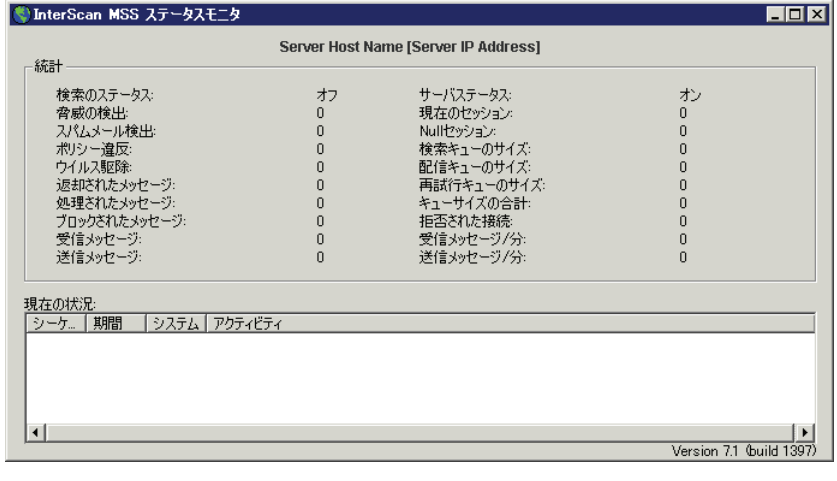
15. [次へ] をクリックします。[設定の概要] 画面が表示され、インストールが開始されます。



16. [次へ] をクリックします。[InstallShield Wizard の完了] 画面が表示されます。

17. [完了] をクリックします。InterScan MSS モニタが表示されます。

注意： InterScan MSS は 32 ビットプログラムです。64 ビット OS にインストールした後は、「perfmon.msc -32」または「mmc /32 perfmon.msc」というコマンドを使用して InterScan MSS モニタを起動してください。



複数の検索サービスとエンドユーザメール隔離サービス / データベースのインストール

ここでは、複数の検索サービスとエンドユーザメール隔離サービスをインストールする方法について説明します。また、InterScan MSS のコンポーネントがすでに存在しているコンピュータに追加のコンポーネントを付加する場合と、InterScan MSS のコンポーネントが存在していないコンピュータに新しいコンポーネントをインストールする場合の違いについても説明します。

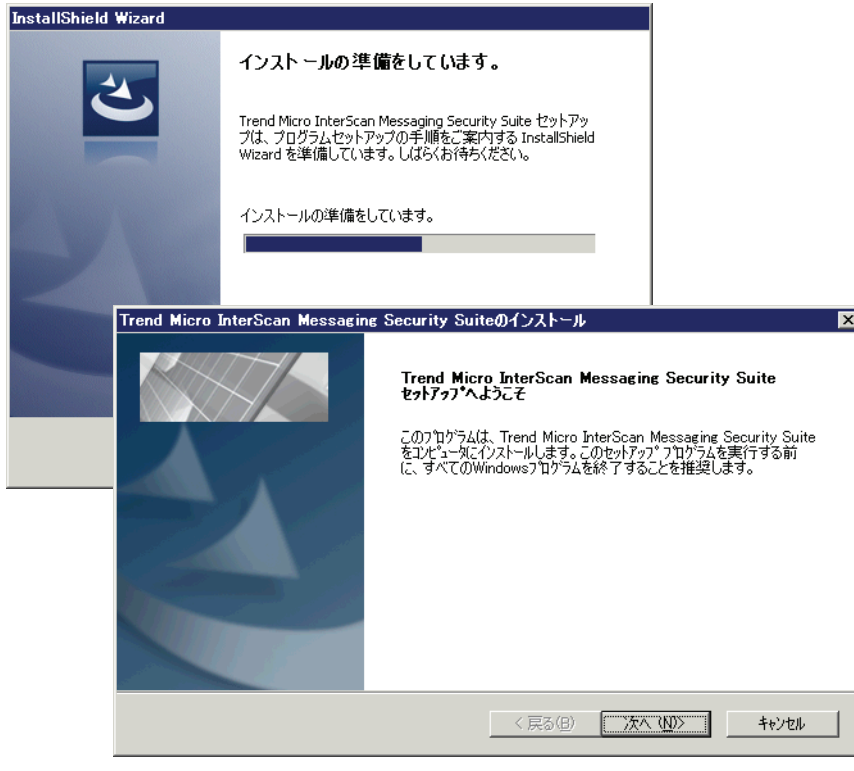
インストールが停止して、上書きできないファイルについてのメッセージが表示された場合は、インストール先フォルダ下のすべてのファイルを手動で削除してから、インストールをやり直してください。場合によっては、インストール先フォルダ下のすべての実行中のアプリケーションを停止する必要があります。たとえば、端末サービスインスタンスによって statmon.exe が実行されている可能性があります。

以前にインストールされたコンポーネントがない場合にコンポーネントを追加する

InterScan MSS のコンポーネントが配置されていないサーバに、InterScan MSS のコンポーネントを追加します。

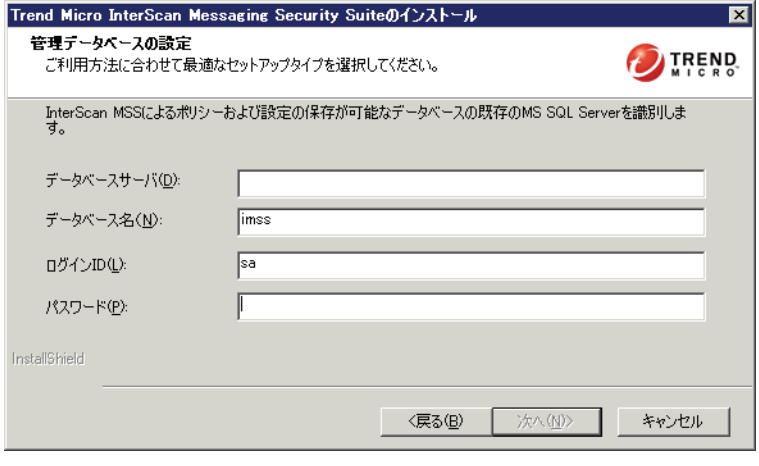
以前にインストールされたコンポーネントがないコンピュータに、検索サービスまたはエンドユーザメール隔離サービス / データベースを追加するには

1. Setup.exe をダブルクリックします。[インストールの準備をしています。] 画面が表示されます。



2. [次へ] をクリックします。[セットアップタイプ] 画面が表示されます。

3. [既存の InterScan MSS サーバにコンポーネントを追加] を選択します。
4. [次へ] をクリックします。[管理データベースの設定] 画面が表示されます。

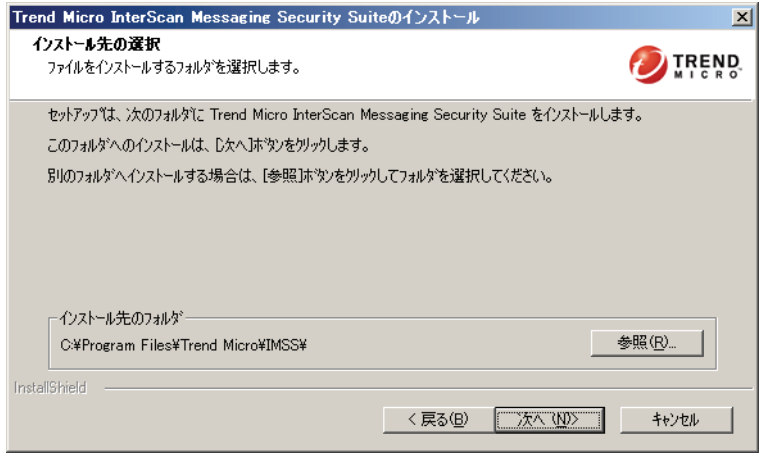


5. 管理データベースの必要な情報を入力します。

   パスワードには、英数字と記号 (`、~、!、@、#、$、%、^、&、*、(、)、[、]、{、}、+、-、|、:、'、<、>、?、/、,、.、=、_) を使用できます。

この InterScan MSS インストールに検索サービスを追加する際に、データベースが InterScan MSS のインストールパッケージからインストールされた場合は、データベースサーバに対して「< ホスト名 （IP アドレス)>¥IMSS_SSEINSTANCE」と指定します。

6. [次へ] をクリックします。[インストール先の選択] 画面が表示されます。



7. インストール先のパスを指定します。

InterScan MSS は、Windows 2003 x64 プラットフォームの次のディレクトリにインストールすることはできません。

```
C:¥program Files¥Trend Micro¥imss
```

Windows 2003 x64 プラットフォームのこのディレクトリに配置できるのは、x64 プログラムのみです。

InterScan MSS を x64 プラットフォームにインストールするには、次のディレクトリを使用します。

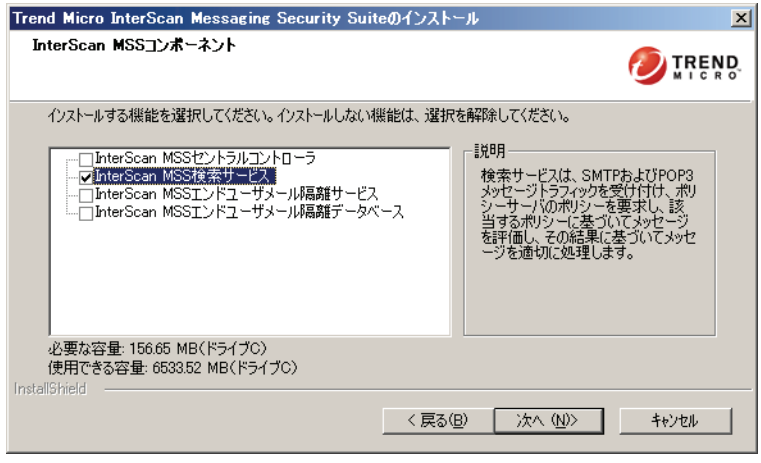
```
C:¥program Files(x86)¥Trend Micro¥imss
```

警告： InterScan MSS は、名前に全角文字を使用しているディレクトリにインストールしないでください。InterScan MSS は、全角文字が使用されたディレクトリの下にインストールすると正しく機能しません。

InterScan MSS は、[内容を暗号化してデータをセキュリティで保護する] という機能が有効化されたディレクトリにはインストールしないでください。InterScan MSS は、この機能が有効化されたディレクトリの下にインストールすると正しく機能しません。

---

8. [次へ] をクリックします。[InterScan MSS コンポーネント] 画面が表示されます。

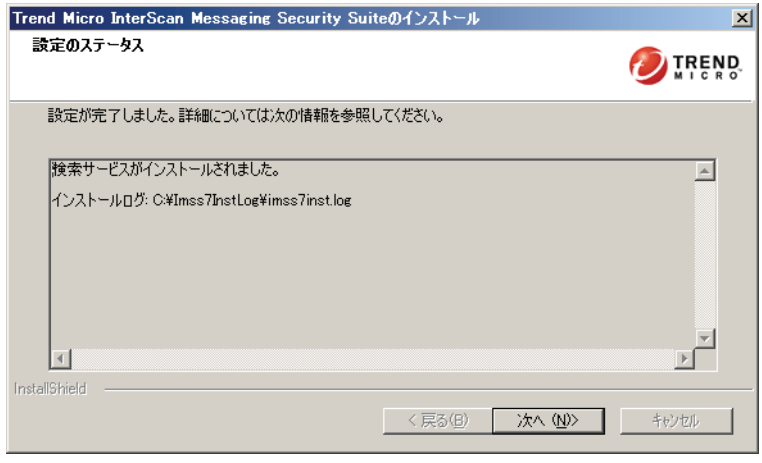


追加の InterScan MSS 検索サービスをインストールするには

a. [InterScan MSS 検索サービス] コンポーネントを選択します。

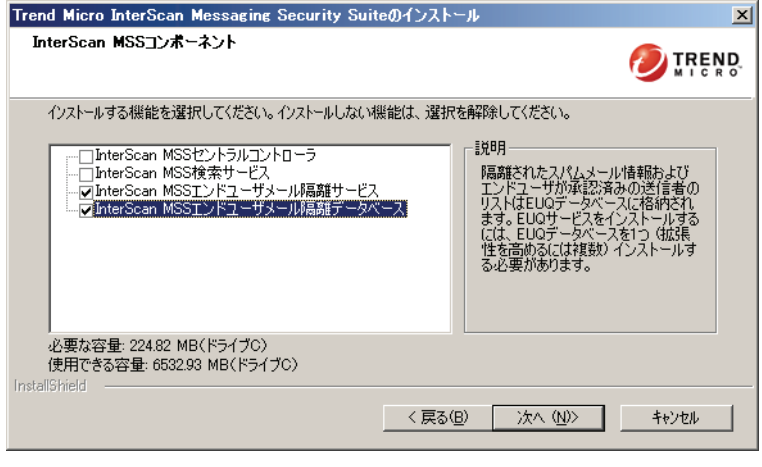
b. [次へ] をクリックします。[設定の概要] 画面が表示されます。

c. 設定を確認して、[次へ] をクリックします。[設定の概要] 画面が表示されます。



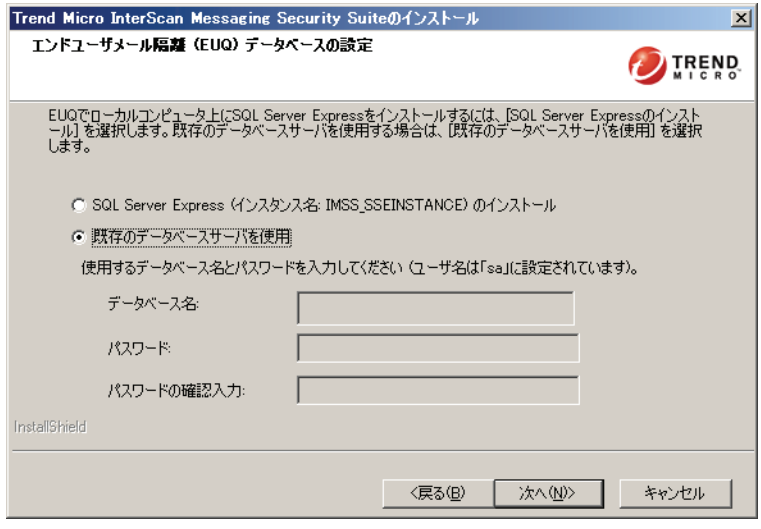
d. [次へ] をクリックします。ファイルがインストールされます。

追加のエンドユーザメール隔離サービスまたは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には



a. [InterScan MSS エンドユーザメール隔離サービス] または [InterScan MSS エンドユーザメール隔離データベース] を選択します。

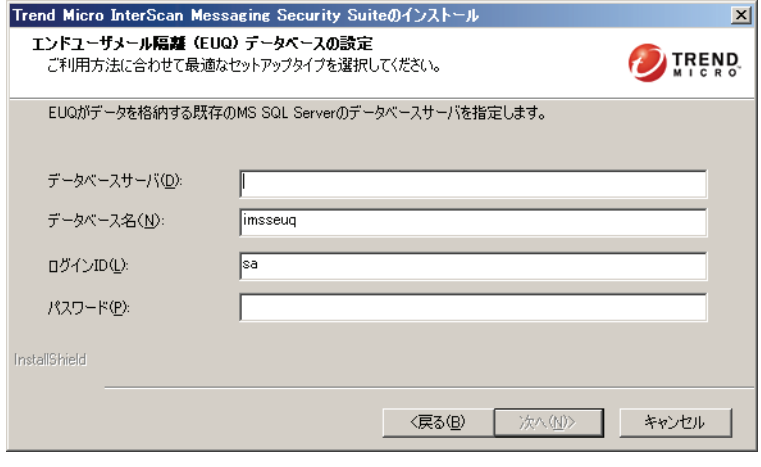
b. [次へ] をクリックします。[エンドユーザメール隔離 (EUQ) データベースの設定] 画面が表示されます。



エンドユーザメール隔離データベースを既存のデータベースサーバにインストールするには

i. [既存のデータベースサーバを使用] を選択します。

ii. [次へ] をクリックします。[エンドユーザメール隔離 (EUQ) データベースの設定] 画面が表示されます。



iii. 既存のデータベースサーバの情報を入力します。

パスワードには、英数字と記号（`、~、!、@、#、$、%、^、&、*、(、)、[、]、{、}、+、-、|、:、'、<、>、?、/、,、.、=、_）を使用できます。

このサーバに SQL Server Express データベースをインストールするには

i. [Install SQL Server Express] を選択します。

ii. 「sa」ユーザアカウントの [データベース名] と [パスワード] を入力します。

パスワードには、英数字と記号（`、~、!、@、#、$、%、^、&、*、(、)、[、]、{、}、+、-、|、:、'、<、>、?、/、,、.、=、_）を使用できます。

c. [次へ] をクリックします。[設定の概要] 画面が表示されます。

d. 選択したコンポーネントと設定内容を確認します。

e. [次へ] をクリックします。[設定の概要] 画面が表示されます。

9. [次へ] をクリックします。[InstallShield Wizard の完了] 画面が表示されます。

10. [完了] をクリックします。

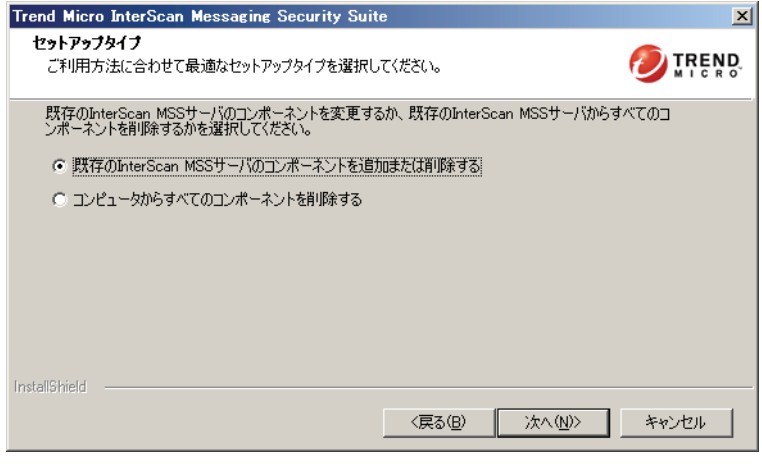
注意： 追加のエンドユーザメール隔離データベースをインストールすることを選択した場合は、セントラルコントローラの `$IMSS_HOME\bin\` ディレクトリに移動して、コマンドラインで `euqtrans.bat` を実行し、元のエンドユーザメール隔離データベース内のデータをすべてのデータベースに配布します。

以前にインストールされたコンポーネントがある場合にコンポーネントを追加する

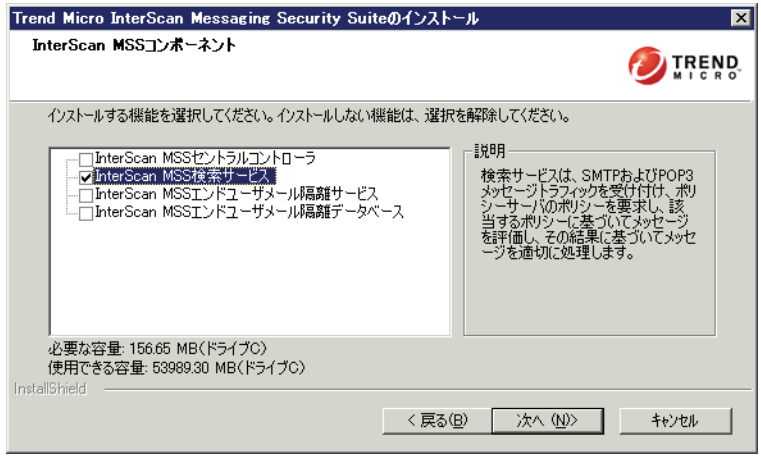
InterScan MSS のコンポーネントがすでに配置されているサーバに、InterScan MSS のコンポーネントを追加します。

InterScan MSS コンポーネントがすでに存在するコンピュータに、検索サービスまたはエンドユーザメール隔離サービス / データベースを追加するには

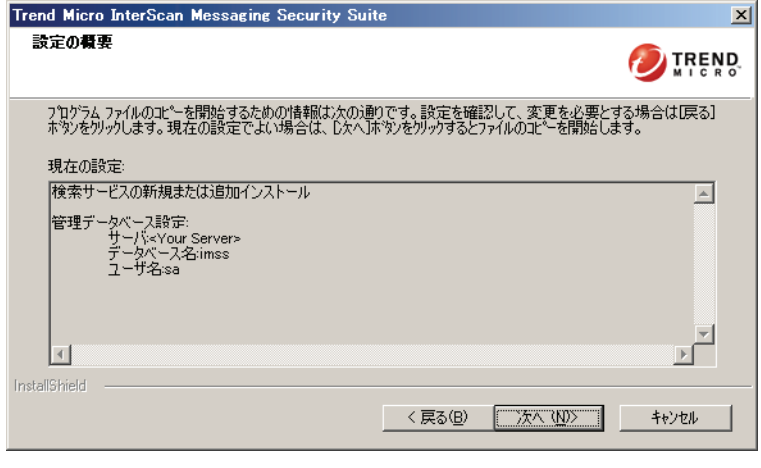
1. Setup.exe をダブルクリックします。[インストールの準備をしています。] 画面が表示され、続けて [ようこそ] 画面が表示されます。
2. [次へ] をクリックします。[セットアップタイプ] 画面が表示されます。



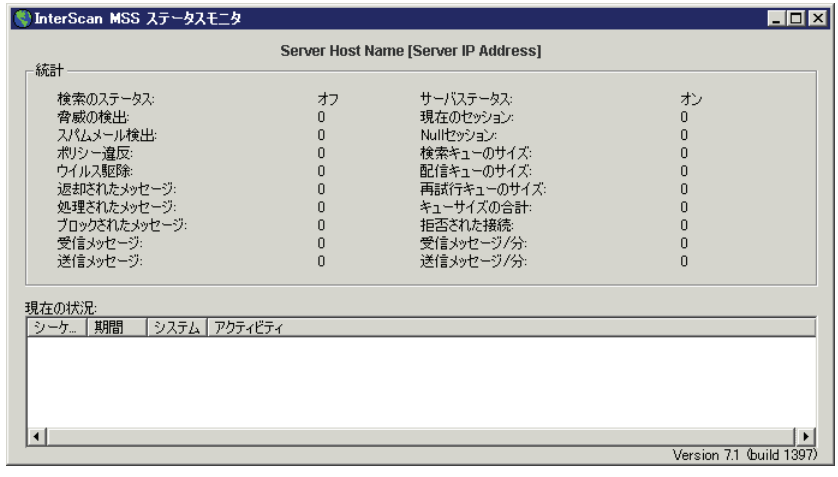
3. [既存の InterScan MSS サーバのコンポーネントと追加または削除する] を選択します。
4. [次へ] をクリックします。[機能の選択] 画面が表示されます。



5. 追加するコンポーネントを選択します。
6. [次へ] をクリックします。[設定の概要] 画面が表示されます。追加のエンドユーザメール隔離サービスまたはデータベースをインストールすることを選択した場合は、[設定の概要] 画面が表示される前に、エンドユーザメール隔離データベースの情報の入力を求められます。



7. [次へ] をクリックします。[設定の概要] 画面が表示されます。
   インストール後に、InterScan MSS モニタが表示されます。



複雑な分散インストール

インストールが停止して、上書きできないファイルについてのメッセージが表示された場合は、インストール先フォルダ内のすべてのファイルを手動で削除してから、インストールをやり直してください。場合によっては、インストール先フォルダ内のすべての実行中のアプリケーションを停止する必要があります。たとえば、端末サービスインスタンスによって `statmon.exe` が実行されている可能性があります。

複雑な分散インストールを実行するには、次の手順を実行します。

1. 1 台のサーバに InterScan MSS をインストールします (72 ページの「集中インストール」を参照)。
2. 必要に応じて、追加の InterScan MSS 検索サービス、エンドユーザメール隔離サービス、またはエンドユーザメール隔離データベースを付加します (86 ページの「複数の検索サービスとエンドユーザメール隔離サービス / データベースのインストール」を参照)。

サイレントインストール

サイレントインストールを実行すると、他のコンピュータで Setup.exe を実行するたびに手動で再設定を行うことなく、同じ設定の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。

サイレントインストールを実行するには、インストール手順をスクリプトに記録してから、このスクリプトを実行して追加の InterScan MSS コンポーネントを後からインストールします。同様に、アンインストール手順をスクリプトに記録してから、この記録されたスクリプトを実行してサイレントアンインストールを実行することもできます。

サイレントインストールは次の 2 つの主な手順からなります。

手順 1 — インストール手順を記録する

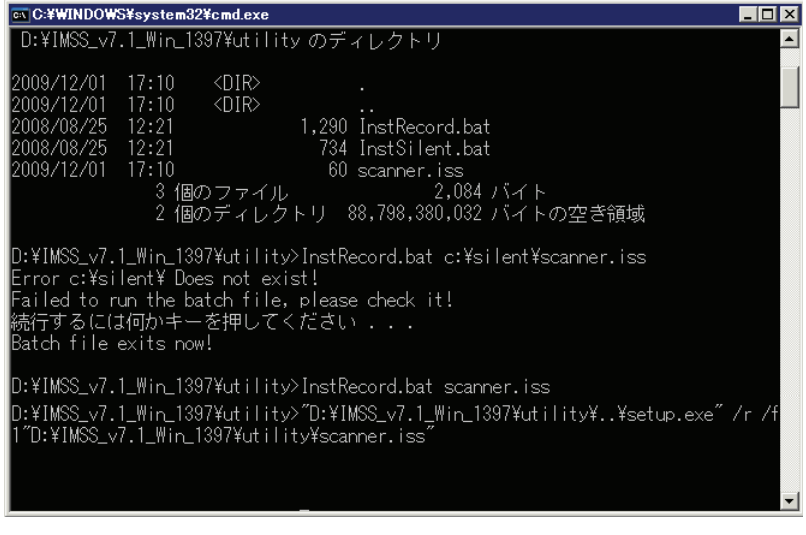
手順 2 — スクリプトを実行して追加のコンポーネントをインストールする

インストール手順を記録する

サイレントインストールでは、インストール時に指定された構成設定が記録されます。

インストール手順を記録するには

1. コマンドウィンドウを開いて、セットアッププログラムが格納されているフォルダに移動します。



2. `utility` というサブフォルダに移動します。
3. `InstRecord.bat` ファイルを実行して、インストール手順を指定したスクリプトに記録します。次に例を示します。

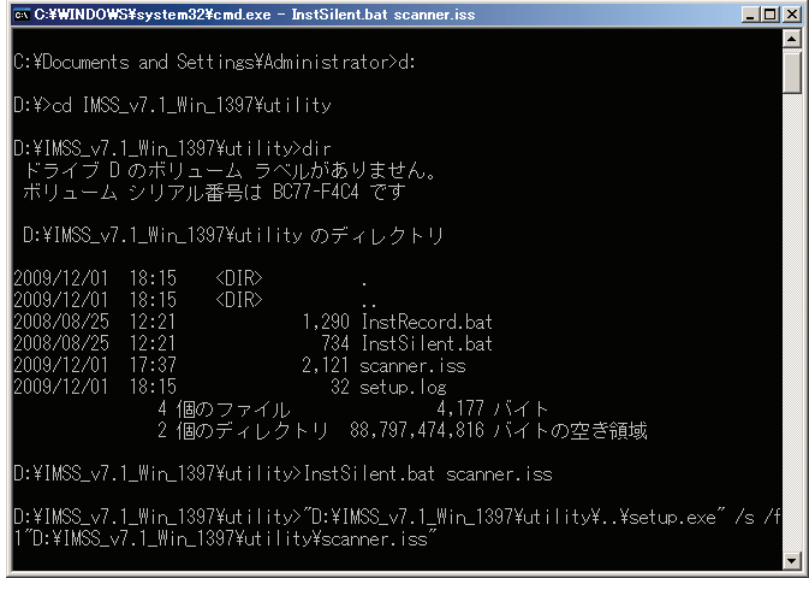
   ```
   InstRecord.bat scanner.iss
   ```

注意： 1. スクリプトを保存するパスを指定できます。ただし、このパスは `InstRecord.bat` を実行する前にすでに存在している必要があります。
2. スクリプトファイルの拡張子は `.iss` である必要があります。
3. パスを指定しない場合は、スクリプトは現在のフォルダの下に作成されます。

サイレントインストールスクリプトを実行する

サイレントインストールスクリプトを使用して追加のコンポーネントをインストールするには

1. コマンドウィンドウを開いて、セットアッププログラムが格納されているフォルダに移動します。



2. `utility` というサブフォルダに移動します。
3. `InstSilent.bat` ファイルを実行し、前に作成したサイレントインストールスクリプトを使用してコンポーネントをインストールします。98 ページの「インストール手順を記録する」を参照してください。次に例を示します。

   ```
   InstSilent.bat scanner.iss
   ```

   インストールは、ポップアップインストールページなどを表示せずに、バックグラウンドで進行します。
4. インストールが正常に完了したことを確認するには、管理コンソールで [概要] → [システム] の順にクリックして、[管理下のサーバ設定] を確認します。

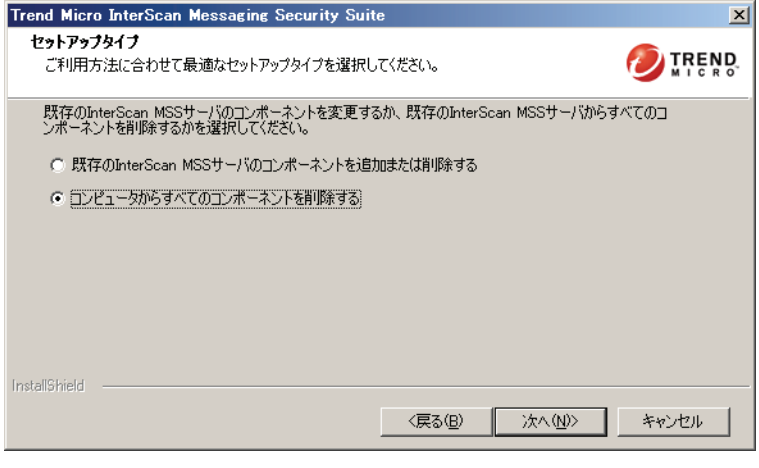
アンインストールの実行

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

InterScan MSS コンポーネントをアンインストールする

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

1. Setup.exe をクリックします。[セットアップタイプ] 画面が表示されます。

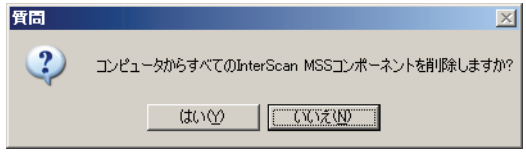


2. 削除するコンポーネントを選択します。

すべての InterScan MSS コンポーネントをコンピュータから削除するには

a. [コンピュータからすべてのコンポーネントを削除する] を選択します。

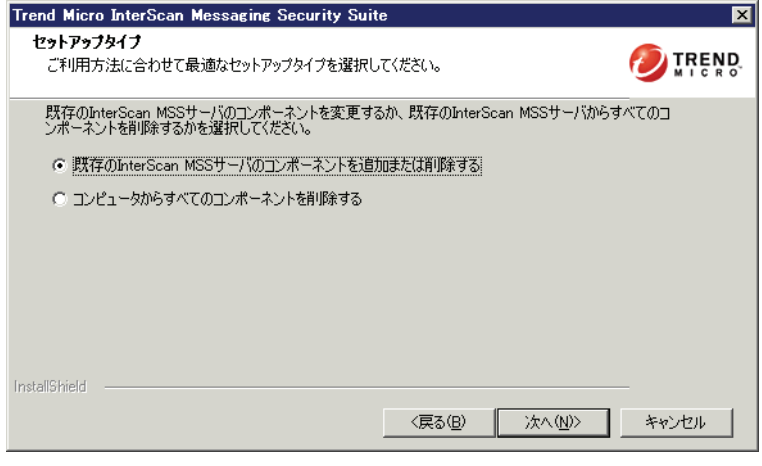
b. [次へ] をクリックします。確認画面が表示されます。



c. [はい] をクリックして操作を確定します。

選択した InterScan MSS コンポーネントを削除するには

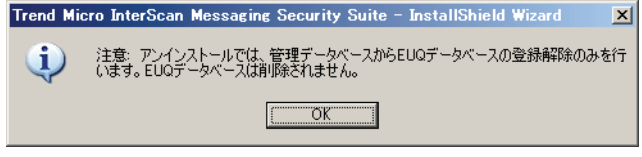
a. 選択したコンポーネントを個別にアンインストールするには、[既存の InterScan MSS サーバのコンポーネントと追加または削除する] を選択します。



b. [次へ] をクリックします。[機能の選択] 画面が表示されます。

c. アンインストールするコンポーネントのチェックボックスをオフにします。

d. [次へ] をクリックします。エンドユーザメール隔離データベースをアンインストールすることを選択した場合は、次のメッセージが表示されます。

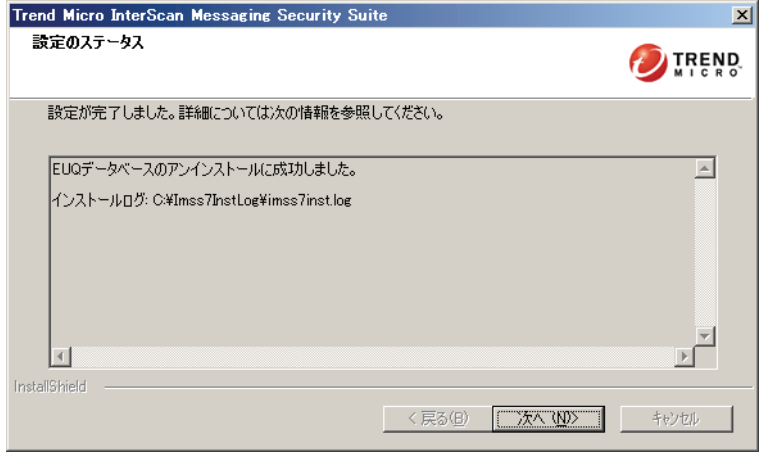


e. [OK] をクリックします。

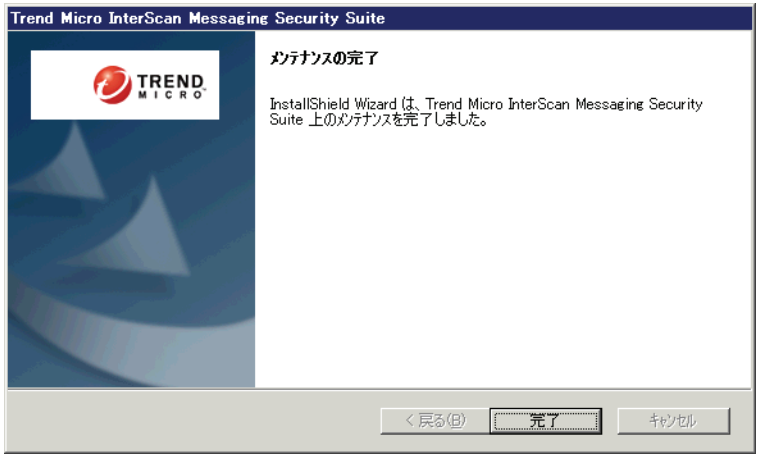
注意： エンドユーザメール隔離データベースのアンインストールを選択しても、このデータベースが管理データベースから登録解除されるだけです。他のすべてのコンポーネントを削除した後に、エンドユーザメール隔離データベースを手動で削除してください。

3. [次へ] をクリックします。[設定の概要] 画面が表示されます。

4. [次へ] をクリックします。コンポーネントがアンインストールされます。[設定の概要] 画面が表示されます。



5. [次へ] をクリックします。[メンテナンスの完了] 画面が表示されます。



6. [完了] をクリックします。

サイレントアンインストール

サイレントアンインストールの手順は、98 ページの「サイレントインストール」の手順と似ています。

注意： サイレントアンインストールは、サイレントインストールスクリプトを記録したコンピュータと類似する環境のコンピュータ上で実行してください。
サイレントインストールスクリプトの記録時やサイレントインストールの実行時には、すべての Microsoft 管理コンソール画面を閉じてください。

第 5 章

以前のバージョンからのアップグレード

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

この章の内容は次のとおりです。

体験版から移行する

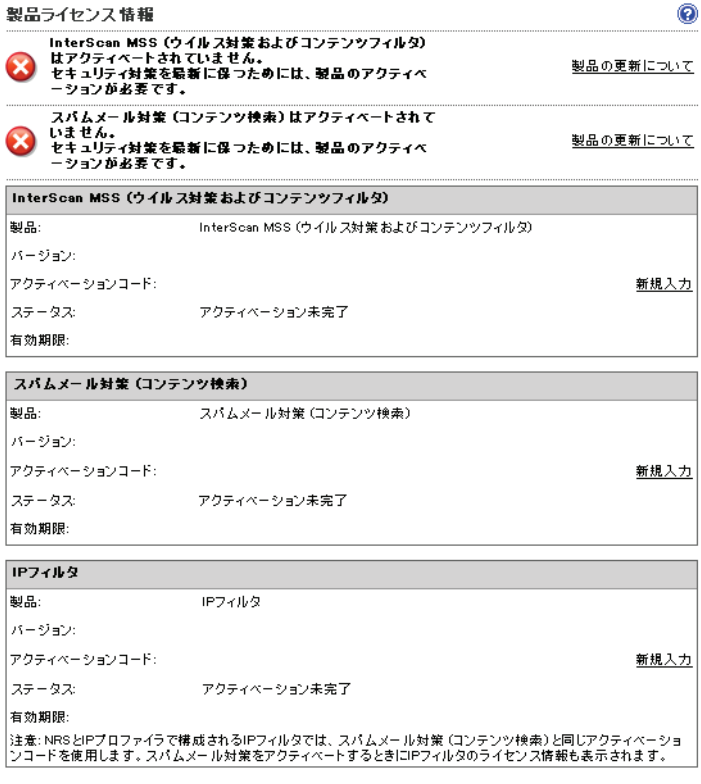
体験版アクティベーションコードを入力して InterScan MSS をアクティベートすると、製品のすべての機能を試すことができる体験版の使用期間が開始します。体験版の使用期間は、入力したアクティベーションコードの種類に応じて異なります。

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

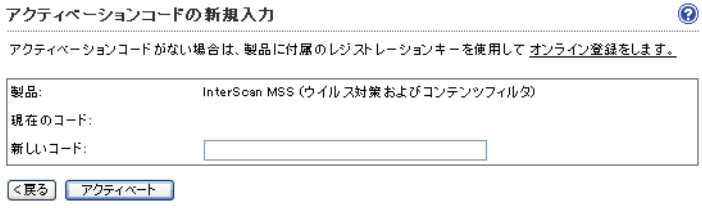
InterScan MSS を継続して使用するには、製品版を購入してください。そうすることで、新しいアクティベーションコードを取得できます。

体験版から移行するには

1. メニューから [管理] → [製品ライセンス] を選択します。



2. [InterScan MSS (ウイルス対策およびコンテンツフィルタ)] セクションまたは [スパムメール対策 (コンテンツ検索)] セクションにある [新規入力] ハイパーリンクをクリックします。



3. 表示されるボックスに新しいアクティベーションコードを入力します。

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

4. [アクティベート] をクリックします。

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

サポート対象のプラットフォームにバージョン 7.0 の InterScan MSS がインストールされている場合、InterScan MSS のセットアッププログラムは、このバージョンを自動的にアップグレードできます。セットアッププログラムでこのバージョンが検出されると、インストールプログラムでは次の処理を実行できます。

- 旧バージョンの InterScan MSS 設定のバックアップを作成します。
- InterScan MSS 7.1 をインストールします。
- 既存の設定を移行します。

セットアッププログラムは、現在の InterScan MSS サーバを Control Manager から登録解除しません。そのため、旧サーバ内のすべてのログについて、Control Manager から引き続きクエリを実行できます。

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

移行または InterScan MSS 7.0 に上書きインストールする

移行または InterScan MSS 7.0 に上書きインストールする前に、次のことを確認してください。

- 上書きインストールでは、InterScan MSS 7.0 のすべてのデータが保持されます。
- 上書きインストールでは、InterScan MSS 7.0 の非表示キー設定が imss.ini ファイルに保持されます。
- 上書きインストールでは、InterScan MSS 7.0 のすべてのレポートが保持されます。
- 上書きインストールでは、InterScan MSS 7.0 のすべての Control Manager 設定が保持されます。
- 分散配置の環境 に上書きインストールする場合、この配置が保持されます。
- InterScan MSS 7.0 に上書きインストールするには、InterScan MSS 7.0 が配置されているサーバへのメッセージトラフィックを停止する必要があります。InterScan MSS 7.1 サーバへ移行する場合は、ネットワーク上のメッセージトラフィックは影響を受けません。

InterScan MSS 7.0 の設定を移行する

アップグレードまたは移行後は、すべての検索サービスのデータと設定が保持されます。

InterScan MSS 7.0 の設定をバックアップする

製品をバックアップするには、その製品のデータとログファイルをバックアップフォルダにコピーします。アップグレード時にエラーが発生した場合は、新しいデータベースを削除できます。その後で、バックアップしたデータとログファイルを元の製品データベースに取り込むと、元のデータベースが完全に復元されます。

設定をバックアップする

InterScan MSS 7.1 を既存の InterScan MSS 7.0 に上書きインストールすると、InterScan MSS 7.1 のセットアッププログラムによって InterScan MSS 7.0 の設定ファイルが自動的にバックアップされます。設定ファイルのバックアップは、インストールの過程で、管理データベースのアップグレードの直前に実行されます。

`C:¥Program Files¥Trend Micro¥IMSS¥config` フォルダの内容を手動でバックアップすることもできます。

InterScan MSS 7.0 データベースをバックアップする

InterScan MSS 7.1 のセットアッププログラムは、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バックアップを実施しません。

既存の InterScan MSS 7.0 に InterScan MSS 7.1 を上書きインストールする場合は、次のことが当てはまります。

1. InterScan MSS 7.1 のセットアッププログラムは、MSDE が InterScan MSS 7.0 によってインストールされたことを検出した場合、この MSDE を SQL Server Express 2005 にアップグレードします。メッセージが表示され、MSDE サーバのデータベースリストが示されます。
2. InterScan MSS 7.1 のセントラルコントローラがインストールされている場合、InterScan MSS 7.1 のセットアッププログラムは管理データベースをアップグレードする必要があります。

ヒント： インストール時にエラーが発生した場合のデータ損失を防止するために、次のデータベースの全体バックアップを手動で実行することをお勧めします。

- 管理データベース (セントラルコントローラをアップグレードする前)

- MSDE サーバ内のすべてのデータベース (MSDE が InterScan MSS 7.0 とともにインストールされている場合)

データベースのデータとログファイルをコピーする前に、次のことを確認してください。

- そのデータベースが現在使用されていないこと
- そのデータベースに対して現在リモート接続されていないこと

データベースのデータとログをコピーできない場合は、上記を確認した後に、Microsoft 管理コンソールからデータベースサービスを停止して、やり直してください。

osql.exe または sqlcmd.exe を使用してデータベースのデータとログファイルの場所を確認するには

`osql.exe` および `sqlcmd.exe` は、SQL Server のインストールパスの `Tools¥bin` フォルダにあります。

1. コマンドラインインタフェースを開いて、`osql.exe` または `sqlcmd.exe` が格納されているディレクトリに移動します。
2. 次のコマンドを使用してデータベースサーバに接続します。
   - `osql.exe` の場合：

     `osql -S <データベースサーバ> -U <ユーザ名> -P <パスワード>`
   - `sqlcmd.exe` の場合：

     `sqlcmd -S <データベースサーバ> -U <ユーザ名> -P <パスワード>`
3. データベースサーバに正常に接続されると、SQL コマンドラインコンソールが表示されます。

4. SQL コマンドラインコンソールで、次の SQL コマンドを入力します。

   `SELECT filename FROM <データベース名>.dbo.sysfiles`

5. <Enter> キーを押して、「GO」と入力し、コマンドを実行します。このクエリが完了するのを待ちます。

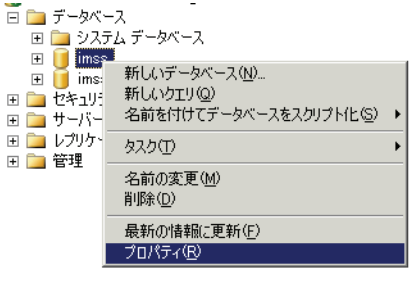
   このクエリは次のような結果を返します。

   - データファイル：`C:¥Program Files¥Microsoft SQL Server¥MSSQL.1¥MSSQL¥Data¥imss.mdf`
   - ログファイル：`C:¥Program Files¥Microsoft SQL Server¥MSSQL.1¥MSSQL¥Data¥imss_log.ldf`

6. これらのファイルを、InterScan MSS データベースをバックアップするために指定したディレクトリにコピーします。

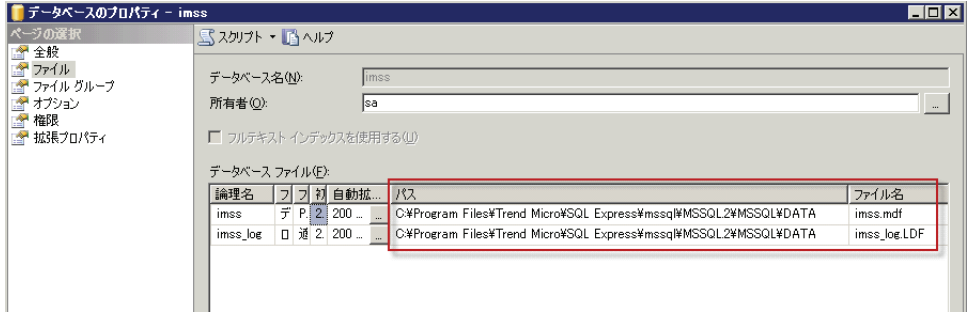
SQL Server Management Studio Express を使用してデータベースのデータとログファイルの場所を確認するには

1. データベースサーバにログオンします。
2. データベースのリストからデータベースを選択します。
3. 選択したデータベースを右クリックします。ポップアップメニューが表示されます。



4. ポップアップメニューから [プロパティ] を選択します。ダイアログボックスが表示されます。

5. [ページの選択] リストから [ファイル] をクリックします。右側のペインが変化して表が表示されます。



6. 水平バーを移動して、[パス] 列を表示します。
7. これらのファイルを、InterScan MSS データベースをバックアップするために指定したディレクトリにコピーします。

InterScan MSS 7.0 の単一サーバ配置をアップグレードする

単一サーバ配置のアップグレードは、分散配置のアップグレードとよく似ています。インストール済みの旧バージョンに上書きインストールするか、または InterScan MSS 7.1 を新規インストールしてからすべての設定を移行します。

注意： アップグレードまたは移行を行うには、InterScan MSS 7.0 SP1 Patch 2 以上を適用した環境で行う必要があります。

InterScan MSS 7.0 の分散配置をアップグレードする

分散配置のアップグレードは、単一サーバ配置のアップグレードとよく似ています。旧バージョンのインストール済みセントラルコントローラに上書きインストールするか、または InterScan MSS 7.1 のセントラルコントローラを新規インストールしてからすべての設定を移行します。

注意： アップグレードまたは移行を行うには、InterScan MSS 7.0 SP1 Patch 2 以上を適用した環境で行う必要があります。

InterScan MSS 7.0 から InterScan MSS 7.1 へ移行する

移行プロセスでは、次の作業を実行する必要があります。

手順 1 — InterScan MSS 7.0 の設定をエクスポートする

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

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

注意： アップグレードまたは移行を行うには、InterScan MSS 7.0 SP1 Patch 2 以上を適用した環境で行う必要があります。

InterScan MSS 7.0 の設定をエクスポートする

InterScan MSS 7.0 エクスポートツールを使用して、InterScan MSS 7.0 から設定をエクスポートします。InterScan MSS 7.0 エクスポートツールは、InterScan MSS 7.1 のインストールフォルダに配置されています。

InterScan MSS 7.0 の設定をエクスポートするには

1. `migration_tool_70to71.zip` を InterScan MSS 7.0 サーバにコピーします。
2. エクスポートツールを解凍します。
3. このツールの解凍先となるディレクトリの名前を次のように変更します。

   `migration_tool_70to71`
4. `export_tool_70.bat` スクリプトを実行して、InterScan MSS 7.0 から設定をエクスポートします。移行パッケージ imss_config_70.tar.gz が現在のフォルダの下に作成されます。

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

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

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

警告： 移行中は、データベース操作を実行しないでください。

移行中は、グループ内のサービスを起動または停止しないでください。

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

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

1. InterScan MSS 7.1 をサーバにインストールします。詳細については、72 ページの「集中インストール」または 97 ページの「複雑な分散インストール」を参照してください。
2. 分散配置の場合は、設定を移行する前に、すべての InterScan MSS サービスを手動で停止します。
3. InterScan MSS 7.1 セントラルコントローラがインストールされているサーバに、`migration_tool_70to71.zip` を解凍します。
4. このツールの解凍先となるディレクトリの名前を次のように変更します。

   `migration_tool_70to71`
5. InterScan MSS 7.0 移行パッケージ (imss_config_70.tar.gz) を、InterScan MSS 7.0 サーバ上の `migration_tool_70to71` ディレクトリから取得します。
6. この移行パッケージを、InterScan MSS 7.1 セントラルコントローラがインストールされているサーバ上の次のディレクトリに配置します。

   `migration_tool_70to71`
7. migration_tool_70.bat スクリプトを実行して、移行ツールを開始します。

   注意： 続行する前に、移行ツールのスコープと制限事項をよくお読みください。
8. 表示される手順に従って、移行ツールを使用します。

   InterScan MSS 7.1 により、次の場所に詳細な移行レポートおよびログが作成されます。`C:¥Imss7InstLog¥migration¥MigrationReport` および `C:¥Imss7InstLog¥migration` (ログには `migration_70.yyyymmdd.log` という形式で名前が付けられます)
9. 次の移行後タスクを実行して、移行の結果を確認します。
   a. 移行した項目の結果を確認します。

b. すべてのサービス、特にポリシーサーバが起動可能であることを確認します。

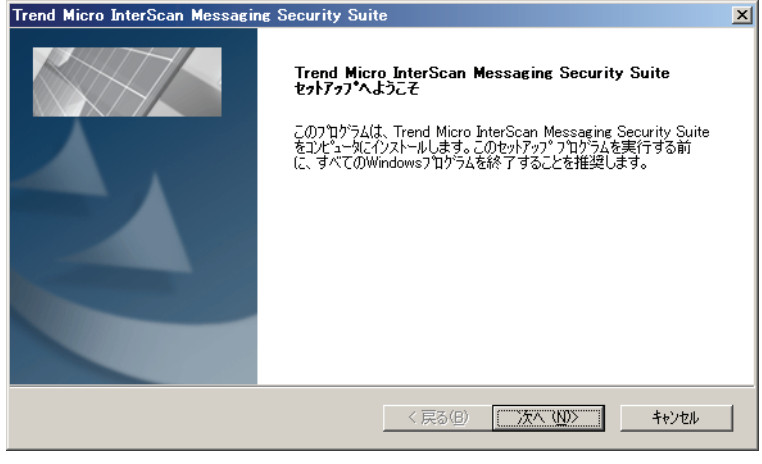
c. 管理コンソールですべてのポリシーにアクセスできることを確認します。

InterScan MSS 7.1 を InterScan MSS 7.0 に上書きインストールする

注意： アップグレードまたは移行を行うには、InterScan MSS 7.0 SP1 Patch 2 以上を適用した環境で行う必要があります。

InterScan MSS 7.1 を InterScan MSS 7.0 に上書きインストールするには

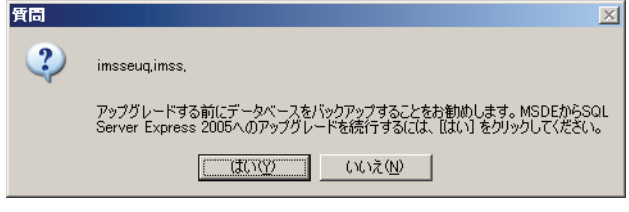
1. Setup.exe をダブルクリックします。[ようこそ] 画面が表示されます。



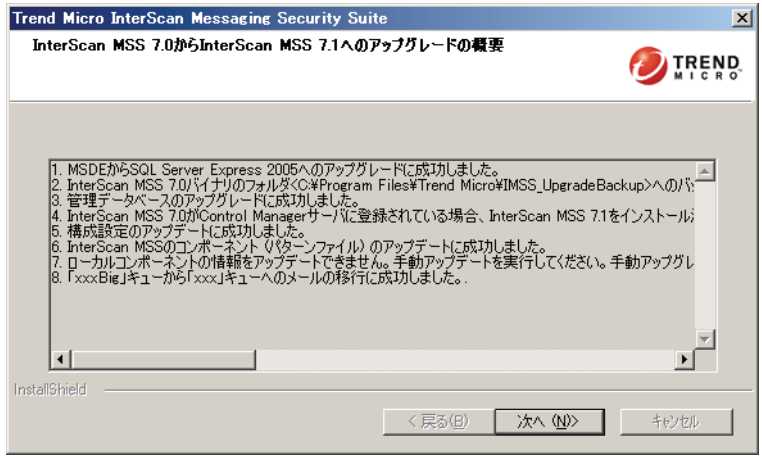
2. [次へ] をクリックします。

3. 使用許諾契約書の内容をよく読んでから、[使用許諾契約の全条項に同意します] を選択します。
4. [次へ] をクリックします。

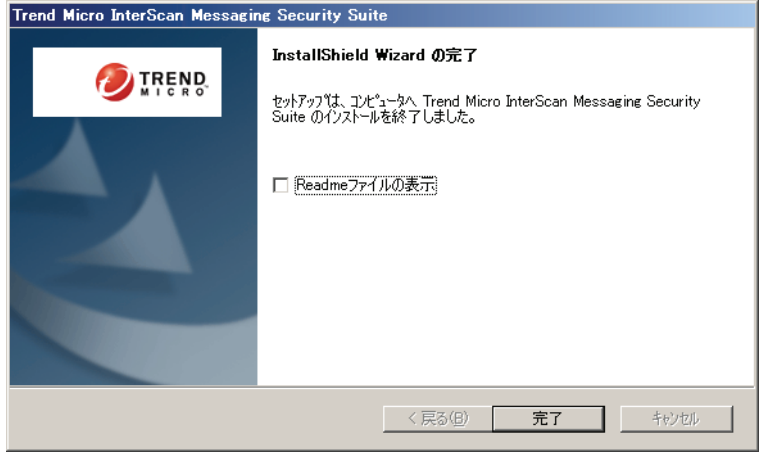
5. [はい] をクリックして、InterScan MSS 7.1 を InterScan MSS 7.0 に上書きインストールします。



6. [はい] をクリックして、MSDE を SQL Server Express 2005 にアップグレードします。アップグレードの概要が表示されます。



7. [次へ] をクリックします。[インストールの完了] 画面が表示されます。



8. [完了] をクリックしてアップグレードを完了します。

サポートされているサービスのアクティベーション

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

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

メールレピュテーションを使用するには、インストールの完了後に管理コンソールからアクティベーションコードを入力します。

アップグレードをロールバックする

バージョン 7.1 への移行で問題が発生した場合、以前のバージョンにロールバックできます。InterScan MSS 7.0 のインストールに関する問題点の詳細については、InterScan MSS 7.0 のドキュメントを参照してください。

第 6 章

トラブルシューティングとサポート情報

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

この章の内容は次のとおりです。

トラブルシューティング

表 6-1 は、InterScan MSS をインストールする際に発生する可能性のある一般的な問題を示しています。この表を見ても問題が解決しない場合は、トレンドマイクロの製品 Q&A を確認してください。

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

表 6-1. インストールに関する問題のトラブルシューティング

問題	推奨される解決策
インストールが停止して、上書きできないファイルについてのメッセージが表示される	インストール先フォルダ内のすべてのファイルを手動で削除してから、インストールを再試行してください。 **注意：** 場合によっては、インストール先フォルダ内のすべての実行中のアプリケーションを停止する必要があります。たとえば、端末サービスインスタンスによって statmon.exe が実行されている可能性があります。
データベース情報が適切でないため、コンポーネントを既存のインストールに追加できない	InterScan MSS インストールに検索サービスを追加する際、データベースサーバ (サーバで初期設定のインスタンス名を使用していない場合) に対して次のように指定してください。 < ホスト名 (IP アドレス) >¥IMSS_SSEINSTANCE

よくある質問 (Q&A)

MTA

管理コンソールを使用しないで MTA 設定を変更するにはどうしたらいいですか。

ローカルの MTA コンポーネントの再起動後にコンポーネントに適用される MTA 設定ファイルを変更できます。

1. 次の MTA 設定ファイルを開いて編集します。

```
%IMSS_HOME%¥config¥tsmtpd.ini
```

2. コマンドラインインタフェースを使用して、検索サービスと MTA コンポーネントを再起動することで、変更を適用します。

   ```
   net stop TmImssScan
   net stop TmImssMTA
   net start TmImssMTA
   net start TmImssScan
   ```

3. MTA コンポーネントに適用される設定を確認します。

InterScan MSS では分割メールをどのように処理するのですか。

`imss.ini` ファイルで `BypassMessagePartial=no` に設定されている場合 (初期設定)、InterScan MSS は分割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。

キーが `yes` に設定されている場合、InterScan MSS は分割メールに特別な処理を行わないでメールが配信されます。トレンドマイクロでは `BypassMessagePartial` 項目を `yes` に変更することはお勧めしません。この変更によって、ウイルスがまん延する危険性があるためです。

自己署名 MTA SSL 証明書を置換するには、どうしたらいいですか。

次の手順を実行してください。

1. 設定ファイルを記述します。詳細については、http://www.openssl.org/docs/apps/req.html を参照してください。
2. 次のコマンドを実行します。

   ```
   openssl req -new -x509 -days 1460 -nodes -config
   tsmtpd.cfg -out tsmtpd.pem -keyout tsmtpd.pem
   ```

3. `tsmtpd.pem` を管理コンソールからアップロードします。
4. OpenSSL ユーティリティコマンドラインの詳細については、次の Web サイトを参照してください。

   http://www.openssl.org/docs/apps/req.html

「ドメインベースリレー」と「初期設定リレー」用に SMTP AUTH 機能はサポートされていますか。サポートされている場合、どの認証方法が InterScan MSS でサポートされていますか。

InterScan MSS では、「ドメインベースリレー」と「初期設定リレー」用に CRAM-MD5、PLAIN、および LOGIN SMTP AUTH の認証方法がサポートされています。ただし、管理コンソールでは設定できません。この設定を実行するには、`<auth>=1` に設定して AUTH 機能を使用し、`tsmtpd.ini` を次に示すように手動で編集します。

構文:

```
[SmtpClient]
# for Domain-based delivery
RelayHostCount=1
RelayHost0=trend.com:guid0
[D_guid0]
UseMethod=1
SmartHostCount=1
SmartHost0=<hostname_or_ip>:<port>:<auth>:<username>:<password>

# for Default delivery
[DefaultRelay]
UseMethod=1
SmartHostCount=1
SmartHost0=<hostname_or_ip>:<port>:<auth>:<username>:<password>
```

例:

```
[SmtpClient]
# for Domain-based delivery
RelayHostCount=1
RelayHost0=trend.com:guid0
[D_guid0]
UseMethod=1
SmartHostCount=1
```

```
SmartHost0=192.168.1.1:25:1:user1:@trend.com:!CRYPT!66AE674C2079B2CD00
CAB0D02E765970

# for Default delivery

[DefaultRelay]

UseMethod=1

SmartHostCount=1

SmartHost0=192.168.1.2:25:1:user2@trend.com:
!CRYPT!66AE674C2079B2CD00CAB0D02E765970
```

注意： <password> については、次のコマンドを入力してパスワードを暗号化してから、tsmtpd.ini に追加します。

C:¥Program Files¥Trend Micro¥IMSS¥bin¥password.exe < パスワードテキスト >

SMTP の設定

初期設定では InterScan MSS はオープンリレーメールサーバですか。

いいえ。初期設定では InterScan MSS はオープンリレーメールサーバではありません。ただし、一部の管理ツールでは、InterScan MSS を誤ってオープンリレーメールサーバとして報告する場合があります。InterScan MSS では、パーセント記号 (%) や感嘆符 (!) などの特殊記号をメールアドレスで使用できるためです。旧式の UNIX メールサーバの実装の中には、メールアドレスに埋め込まれたこのような特殊文字を、不正なソースルーティングとして処理するものがあるため、一部のサードパーティ製管理ツールでは、InterScan MSS を誤ってオープンリレーとして認識することがあります。InterScan MSS が誤ってオープンリレーメールサーバとして認識されないようにするには、次のいずれかを実行します。

- 中央データベースの下にあるすべての InterScan MSS サーバに設定を適用します。

  InterScan MSS を分散環境に配置している場合、次の SQL ステートメントを実行して、新しい設定を中央データベースの tb_mta_config テーブルに追加します。

  ```
  insert into tb_mta_config (section, name, value, inifile) values (
  'SmtpServer', ' RestrictInDomain', '1', 'tsmtpd.ini');

  insert into tb_mta_config (section, name, value, inifile) values (
  'SmtpServer', ' RestrictInDomainMeta', ' !#$%', 'tsmtpd.ini');
  ```

- 設定を InterScan MSS サーバに適用します。

IMSS_INSTALL_ROOT¥config¥ にある tsmtpd.ini を編集して、次のキーのコメントを削除します。

```
RestrictInDomain=1
RestrictInDomainMeta=!#$%
```

インストールまたはアンインストール

InterScan MSS 管理データベースを別個にインストールできますか。

はい。次の 2 つの方法で InterScan MSS 管理データベースを別個にインストールできます。

- セットアッププログラムを実行して、InterScan MSS データベースを設定します。その他の InterScan MSS コンポーネントを選択しないでください。
- ターゲットコンピュータ上に既存のデータベースサーバがある場合は、セットアッププログラムをコマンドインタフェースで実行します。
  - セットアップフォルダに移動します。
  - 次のコマンドを使用して、セットアッププログラムを実行します。

    ```
    setup.exe /zOnlyInstDB
    ```
  - インストール画面に従って、InterScan MSS 管理データベースをインストールします。

注意： InterScan MSS 管理データベースをインストールしたら、セットアッププログラムを実行し、アカウントが作成されたデータベースを使用して他のコンポーネントをインストールしてから、InterScan MSS データベースに接続します。

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

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

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

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

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

いいえ。アンインストール時には、InterScan MSS エンドユーザメール隔離データベースが管理データベースから登録解除されるだけです。管理コンソールを使用して InterScan MSS エンドユーザメール隔離データベースを再登録できます。

インストール時に、古い InterScan MSS データベースを削除することはできますか。

いいえ。セットアッププログラムがデータベースを削除しようとする際、アプリケーションがデータベースに接続しているからです。古いデータベースへのすべての接続を切断し、データベースを削除してから、データベースを新規作成してください。

InterScan MSS は初期設定のパスでインストールする必要がありますか。

いいえ。64 ビット OS での `X:\Program Files` を除いて、任意のインストールパスを指定できます。ここで、X はシステムディスクです。このフォルダは、64 ビットプログラムのために予約されています。

ターゲットコンピュータで管理コンソールのショートカットが機能しないのはなぜですか。

ターゲットコンピュータで Windows Server 2003 を実行している場合、ショートカットのアドレスをブラウザの信頼済みゾーンに追加してください。

データベースプロセスが以下の場合

- **稼働していない場合**: データベースサービスを開始してから、InterScan MSS 管理コンソールのサービスを再起動してください。
- **稼働している場合**: 管理コンソールがデータベースよりも先に起動している場合、InterScan MSS 管理コンソールのサービスを再起動してください。

InterScan MSS ではドメインアカウントを使用して、データベースにアクセスできますか。

いいえ。InterScan MSS は、Windows 認証をサポートしていません。

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。「ホスト名 ¥ インスタンス」または「IP アドレス ¥ インスタンス」の形式で指定して、データベースサーバを参照できます。

InterScan MSS または InterScan MSS コンポーネントの IP アドレスを変更できますか。

はい。

InterScan MSS (セントラルコントローラと検索サービス) の IP アドレスを変更するには

1. 次に示すようにすべての InterScan MSS サービスを停止します。

   Windows の [コントロール パネル] → [管理ツール] → [サービス] を開きます。次のサービスを順番に停止します。

   InterScan MSS 管理コンソール

   InterScan MSS IP プロファイラ

   InterScan MSS タスクサービス

   InterScan MSS CMAgent サービス

   InterScan MSS ポリシーサービス

   InterScan MSS 検索サービス

   InterScan MSS SMTP サービス

   InterScan MSS マネージャ
2. サーバの IP アドレスを変更します。
3. InterScan MSS 設定フォルダにある ODBC.ini および EUQ.ini で IP アドレスを変更します。
4. %IMSS_HOME\ui%adminUI\webapps\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。
5. 次のデータベースデータを変更します。
   - tb_component_list: コンピュータ名とすべての検索サービスの IP アドレスを指定します。
   - tb_euq_db_info: エンドユーザメール隔離データベースのコンピュータ設定を指定します。
   - tb_global_setting: [cmagent] name [ConfigUrl] セクションで、管理コンソールの URL を変更します。
6. SQL Server の IP 設定を変更してから、Microsoft SQL Server サービスを再起動します。
7. 次に示すようにすべての InterScan MSS サービスを再起動します。

   Windows の [コントロール パネル] → [管理ツール] → [サービス] を開きます。次のサービスを順番に再起動します。

   InterScan MSS マネージャ

InterScan MSS SMTP サービス

InterScan MSS 検索サービス

InterScan MSS ポリシーサービス

InterScan MSS CMAgent サービス

InterScan MSS タスクサービス

InterScan MSS IP プロファイラ

InterScan MSS 管理コンソール

検索サービスの IP アドレスを変更するには

InterScan MSS の TmImssManager サービスを再起動すると、検索サービスの新しい IP アドレスは、このサービスによって tb_component_list 内で自動的にアップデートされます。検索サービスの IP アドレスをアップデートするには、TmImssManager サービスを再起動します。

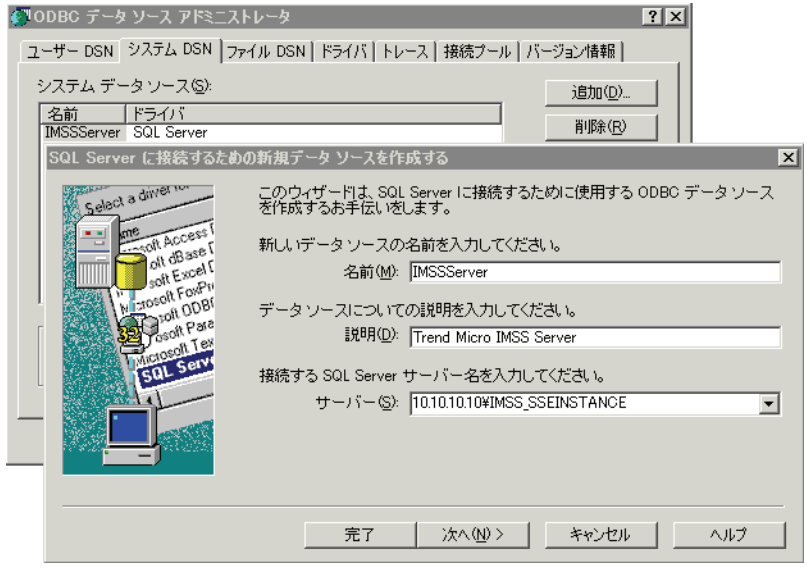
セントラルコントローラの IP アドレスを変更するには

1. InterScan MSS の TmImssManager サービスを再起動します。
2. tb_global_setting テーブル内の [cmagent]/ConfigUrl パラメータで、セントラルコントローラの新しい IP アドレスを指定します。
3. IP プロファイラがインストールされている場合は、次の手順を実行します。
   - セントラルコントローラで BIND サービス (ISC BIND) を再起動します。
   - 検索サービスごとに tsmtpd.ini ファイル内の [SmtpServer]/IPProfilerDNSServerIP パラメータの IP アドレスをアップデートします。
4. 検索サービスごとに SMTP サービスを再起動して、IP プロファイラの DNS サーバの新しい IP アドレスを使用します。
5. 管理コンソールにアクセスするには、adminui ファイルで IP アドレスを新しい IP アドレスに変更します。このファイルは、InterScan MSS のインストールディレクトリにあります。

管理データベースの IP アドレスを変更するには

1. すべての InterScan MSS コンポーネントを停止します。
2. すべての検索サービスとエンドユーザメール隔離サーバにおいて、ODBC システム DSN 設定でサーバパラメータをデータベースサーバの新しい IP アドレスに設定します。

   [ODBC データ ソース アドミニストレータ] ダイアログボックス ([スタート] → [管理ツール] → [データ ソース (ODBC)]) で設定を変更します。



注意： 64 ビットプラットフォームでは、`%systemdrive%¥Windows¥SysWOW64¥Odbcad32.exe` を実行して、InterScan MSS の DSN 設定を変更します。

3. すべての検索サービスとエンドユーザメール隔離サーバにおいて、`IMSS¥config¥` にある `odbc.ini` ファイルで、ServerName パラメータをデータベースサーバの新しい IP アドレスに設定します。
4. セントラルコントローラにおいて、`IMSS¥ui¥adminUI¥webapps¥ROOT¥WEB-INF¥` にある `struts-config-common.xml` ファイルで、データベース URL をデータベースサーバの新しい IP アドレスに設定します。設定を変更するには、次に示すような文字列を探してから、IP アドレスを変更します。

```
<set-property
property="url"
value="jdbc:sqlserver://10.100.10.31;DatabaseName=imss" />
```

5. すべてのサーバで、すべての InterScan MSS コンポーネントを起動します。

プライマリエンドユーザメール隔離サーバの IP アドレスを変更するには

1. /opt/trend/imss/UI/euqUI/conf/ にある EUQ.conf ファイルで、「ServerName」を新しい IP アドレスに変更します。
2. 次のファイルで IP アドレスを新しい IP アドレスに変更します。
   - euqbalance
   - euqui

   両方のファイルは、InterScan MSS インストールディレクトリにあります。
3. プライマリエンドユーザメール隔離サーバに対する tb_global_setting の admin_cmd パラメータを 12288 に設定します。
4. プライマリエンドユーザメール隔離サーバで InterScan MSS マネージャサービスを再起動します。これにより、tb_component_list で IP アドレスが新しい IP アドレスに変更され、負荷分散設定がアップデートされ、TmImssEuqLoadBalancer サービスが再起動します。
5. プライマリエンドユーザメール隔離サーバでプライマリエンドユーザメール隔離サービスを再起動します。

セカンダリエンドユーザメール隔離サーバの IP アドレスを変更するには

1. euqui ファイルで IP アドレスを新しい IP アドレスに変更します。このファイルは、InterScan MSS のインストールディレクトリにあります。
2. セカンダリエンドユーザメール隔離サーバで InterScan MSS マネージャサービスを再起動します。これにより、tb_component_list で IP アドレスが新しい IP アドレスに変更されます。
3. プライマリエンドユーザメール隔離サーバに対する tb_global_setting の admin_cmd パラメータを 12288 に設定します。
4. プライマリエンドユーザメール隔離サーバで InterScan MSS マネージャサービスを再起動して、worker.properties 設定ファイルをアップデートします。

InterScan MSS グループに対してエンドユーザメール隔離サーバの削除や追加を実行するには

セットアッププログラムは、プライマリエンドユーザメール隔離サーバ上の InterScan MSS マネージャサービスに対して、Apache Web サーバ用の負荷分散設定をアップデートするように指示します。プライマリエンドユーザメール隔離サーバ上の InterScan MSS マネージャサービスは、admin_cmd コマンドを検出して workers.properties 設定ファイルをアップデートし、Apache Web サーバで使用されるエンドユーザメール隔離サーバのプール内のエンドユーザメール隔離サーバを追加または削除して、エンドユーザ要求を分散させます。

エンドユーザメール隔離データベースを追加するには

InterScan MSS 管理コンソールまたはセットアッププログラムを使用して、新しいエンドユーザメール隔離データベースを追加します。インストールが完了したら、セントラルコントローラの <IMSS>¥bin ディレクトリで、euqtrans.bat スクリプトを使用して、エンドユーザメール隔離データベースの負荷分散を再び実行します。

エンドユーザメール隔離データベースを削除するには

1. InterScan MSS 管理コンソールを使用して、エンドユーザメール隔離データベースの登録を解除します (削除はしません)。
2. euqtrans.bat スクリプトを実行して、承認済み送信者リストと隔離済みメールメッセージ情報を別のデータベースに移動してから、新しい配置に基づいて、データベースの負荷分散を再び実行します。

エンドユーザメール隔離データベースの IP アドレスを変更するには

1. euq.ini ファイルで IP アドレスを新しい IP アドレスに変更します。このファイルは、<IMSS>¥config¥ にあります。
2. InterScan MSS 管理コンソールを使用して、エンドユーザメール隔離データベースの IP アドレスをこのデータベースの新しい IP アドレスに変更します。

   エンドユーザメール隔離データベースを設定したら、InterScan MSS からすべてのサービスに対して再起動するように自動的に指示されます。再起動時に、サービスでは自動的に、アップデートされたエンドユーザメール隔離データベース接続設定を tb_euq_db_info テーブルで確認し、Windows レジストリでローカルの ODBC ユーザ DSN 設定をアップデートします。

SNMP 通知用の MIB ファイルはどこにありますか。

IMSS_win.mib ファイルは、解凍した InterScan MSS インストールパッケージの最上位レベルのフォルダにあります。

製品サポート情報

InterScan MSS のユーザ登録により、さまざまなサポートサービスを受けることができます。

トレンドマイクロの Web サイトでは、ネットワークを脅かすウイルスやセキュリティに関する最新の情報を公開しています。ウイルスが検出された場合や、最新のウイルス情報を知りたい場合などにご利用ください。

サポートサービスについて

サポートサービス内容の詳細については、製品パッケージに同梱されている「スタンダードサポート サービスメニュー」をご覧ください。

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

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

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

製品 Q&A のご案内

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

製品 Q&A

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

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

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

セキュリティ情報

セキュリティ情報の入手先

トレンドマイクロでは、最新のセキュリティ情報をインターネットで公開しています。トレンドマイクロのセキュリティ情報 Web サイトでは、ウイルスやインターネットセキュリティに関する最新の情報を入手できます。セキュリティ情報 Web サイトは、次の URL からアクセスできます。

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

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

セキュリティ情報 Web サイトでは、次の情報を閲覧できます。

- ウイルス名やキーワードから検索できるウイルスデータベース
- コンピュータウイルスの最新動向に関するニュース
- 現在流行中のウイルスや不正プログラムの情報
- デマウイルスまたは誤警告に関する情報
- ウイルスやネットワークセキュリティの予備知識

セキュリティ情報 Web サイトに定期的にアクセスして、流行中のウイルス情報などを入手することをお勧めします。メールによる定期的なウイルス情報配信を希望する場合は、警告メール配信の登録フォームを利用してメールアドレスを登録してください。

トレンドマイクロへのウイルス解析依頼

ウイルス感染の疑いのあるファイルがあるのに、最新の検索エンジンおよびパターンファイルを使用してもウイルスを検出 / 駆除できない場合などに、感染の疑いのあるファイルをトレンドマイクロのサポートセンターへ送信していただくことができます。

ファイルを送信いただく前に、トレンドマイクロのウイルスデータベース検索サイトにアクセスして、ウイルスを特定できる情報がないかどうか確認してください。

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

ファイルを送信いただく場合は、次の URL にアクセスして、サポートセンターの受付フォームからファイルを送信してください。

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

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

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

ウイルス解析サポートセンター「TrendLabs」

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

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

索引

英数字

あ