InterScan Messaging Security Virtual Appliance™ 9.1 Service Pack 1

インストールガイド

※注意事項

複数年契約について

・お客さまが複数年契約（複数年分のサポート費用前払い）された場合でも、各製品のサポート期間については、当該契約期間によらず、製品ごとに設定されたサポート提供期間が適用されます。

・複数年契約は、当該契約期間中の製品のサポート提供を保証するものではなく、また製品のサポート提供期間が終了した場合のバージョンアップを保証するものではありませんのでご注意ください。

・各製品のサポート提供期間は以下の Web サイトからご確認いただけます。

https://success.trendmicro.com/dcx/s/solution/000207383?language=ja

法人向け製品のサポートについて

・法人向け製品のサポートの一部または全部の内容、範囲または条件は、トレンドマイクロの裁量により随時変更される場合があります。

・法人向け製品のサポートの提供におけるトレンドマイクロの義務は、法人向け製品サポートに関する合理的な努力を行うことに限られるものとします。

商標について

TRENDMICRO、TREND MICRO、ウイルスバスター、InterScan、INTERSCAN VIRUSWALL、InterScanWebManager、InterScan Web Security Suite、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、Trend Park、Trend Labs、Network VirusWall Enforcer、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、SPN、SMARTSCAN、Trend Micro Kids Safety、Trend Micro Web Security、Trend Micro Portable Security、Trend Micro Standard Web Security、Trend Micro Hosted Email Security、Trend Micro Deep Security、ウイルスバスタークラウド、スマートスキャン、Trend Micro Enterprise Security for Gateways、Enterprise Security for Gateways、Smart Protection Server、Deep Security、ウイルスバスター ビジネスセキュリティサービス、SafeSync、Trend Micro NAS Security、Trend Micro Data Loss Prevention、Trend Micro オンラインスキャン、Trend Micro Deep Security Anti Virus for VDI、Trend Micro Deep Security Virtual Patch、SECURE CLOUD、Trend Micro VDI オプション、おまかせ不正請求クリーンナップサービス、Deep Discovery、TCSE、おまかせインストール・バージョンアップ、Trend Micro Safe Lock、Deep Discovery Inspector、Trend Micro Mobile App Reputation、Jewelry Box、InterScan Messaging Security Suite Plus、おもいでバックアップサービス、おまかせ！スマホお探しサポート、保険&デジタルライフサポート、おまかせ！迷惑ソフトクリーンナップサービス、InterScan Web Security as a Service、Client/Server Suite Premium、Cloud Edge、Trend Micro Remote Manager、Threat Defense Expert、Next Generation Threat Defense、Trend Micro Smart Home Network、Retro Scan、is702、デジタルライフサポート プレミアム、Air サポート、Connected Threat Defense、ライトクリーナー、Trend Micro Policy Manager、フォルダシールド、トレンドマイクロ認定プロフェッショナルトレーニング、Trend Micro Certified Professional、TMCP、XGen、InterScan Messaging Security、InterScan Web Security、Trend Micro Policy-based Security Orchestration、Writing Style DNA、Securing Your Connected World、Apex One、Apex Central、MSPL、TMOL、TSSL、ZERO DAY INITIATIVE、Edge Fire、Smart Check、Trend Micro XDR、Trend Micro Managed XDR、OT Defense Console、Edge IPS、スマスキャ、Cloud One、Cloud One - Workload Security、Cloud One - Conformity、ウイルスバスター チェック！、Trend Micro Security Master、Worry-Free XDR、Worry-Free Managed XDR、Network One、Trend Micro Network One、らくらくサポート、Service One、超早得、

P/N: MSEM99651/221214_JP (2023/09)

プライバシーと個人データの収集に関する規定

トレンドマイクロ製品の一部の機能は、お客さまの製品の利用状況や検出にかかわる情報を収集してトレンドマイクロに送信します。この情報は一定の管轄区域内および特定の法令等において個人データとみなされることがあります。トレンドマイクロによるこのデータの収集を停止するには、お客さまが関連機能を無効にする必要があります。

InterScan Messaging Security Virtual Appliance により収集されるデータの種類と各機能によるデータの収集を無効にする手順については、次の Web サイトを参照してください。

https://www.go-tm.jp/data-collection-disclosure

重要

データ収集の無効化やデータの削除により、製品、サービス、または機能の利用に影響が発生する場合があります。InterScan Messaging Security Virtual Appliance における無効化の影響をご確認の上、無効化はお客さまの責任で行っていただくようお願いいたします。

トレンドマイクロは、次の Web サイトに規定されたトレンドマイクロのプライバシーポリシー (Global Privacy Notice) に従って、お客さまのデータを取り扱います。

https://www.trendmicro.com/ja_jp/about/legal/privacy-policy-product.html

目次

本書について

第 1 章：InterScan Messaging Security Virtual Appliance の概要

第 2 章：コンポーネントの説明

第 3 章：配置計画

第 4 章：IMSVA9.1 SP1 のインストール

第 5 章：以前のバージョンからのアップグレード

第 6 章：トラブルシューティング

付録 A：テクニカルサポート

付録 B：VMware ESX for IMSVA での新しい仮想マシンの作成

付録 C：Microsoft Hyper-V for IMSVA での新しい仮想マシンの作成

索引

本書について

IMSVA のインストールガイドをお読みいただきありがとうございます。本書では、IMSVA の特徴、システム要件、および IMSVA の設定のインストールおよびアップグレード手順について説明しています。

IMSVA の設定手順については、*IMSVA9.1 SP1* 管理者ガイドを参照してください。また、ユーザインタフェースの各フィールドの詳細については、管理コンソールのオンラインヘルプを参照してください。

この章の内容は次のとおりです。

- viii ページの「新機能」
- xii ページの「対象読者」
- xii ページの「InterScan Messaging Security Virtual Appliance ドキュメント」
- xiii ページの「ドキュメントの表記規則」

新機能

表 1. IMSVA 9.1 SP1 の新機能

新機能	説明
Trend Vision One との統合	Trend Vision One との統合により、IMSVA がログを Trend Vision One に転送して、相関検出やその他の高度な分析を行うことができます。
OS のアップグレード	IMSVA では、標準の CentOS Linux OS を使用する自己完結型のインストールを実行できます。このサービスパックでは、IMSVA の自己完結型インストールの OS を直接アップグレードします。

表 2. IMSVA 9.1 Patch 3 の新機能

新機能	説明
URL の分析	メールメッセージに含まれる不審ファイルに加えて、不審 URL も仮想アナライザで詳細に分析できるようになります。 不正な URL から保護するため、IMSVA ではまず、メールメッセージ内の URL を Web レピュテーションデータベースに登録されている既知の不正な URL と比較し、さらにこれらの URL をクリック時にも分析します。ただし、未評価の URL はこれらの分析を通過する可能性があります。IMSVA では、仮想アナライザで使用可能なサンドボックス機能を利用して URL のシミュレーションと分析を実行することで、保護を強化しています。

表 3. IMSVA 9.1 Patch 2 の新機能

新機能	説明
Domain-based Message Authentication, Reporting and Conformance (DMARC)	メールのスプーフィングを検出して阻止するメール検証システムです。正規の組織から送信されたようにメールメッセージの送信者アドレスを偽装するなど、フィッシングメールやスパムメールで利用される技術に対処することを目的としています。 IMSVA の既存のメール認証プロセスに適合するように設計されており、ユーザは、DMARC 検証に失敗したメールメッセージに実行する処理を指定するなど、DMARC 設定を定義できます。

表 4. IMSVA 9.1 の新機能

新機能	説明
Syslog の統合	法人向けのログ機能を提供するため、IMSVA では、Syslog プロトコルを使用して複数の外部 Syslog サーバに構造化された形式でログを送信できます。Syslog サーバは IMSVA 管理コンソールで追加、削除、インポート、およびエクスポートできます。

新機能	説明
複数の仮想アナライザサーバのサポート	負荷分散とフェイルオーバー機能をさらに効率化するため、IMSVA では仮想アナライザに複数のサーバを追加できます。仮想アナライザサーバは IMSVA 管理コンソールで有効化、無効化、および削除できます。
SMTP トラフィックスロットリング	SMTP トラフィックスロットリングは、接続数またはメッセージ数が指定した最大数に達した場合に、単一の IP アドレスまたは送信者からのメッセージを一定期間ブロックします。
監査ログのサポート	システムイベントのログカテゴリがさらに使いやすくなり、IMSVA 管理コンソールでは [管理者アクティビティ] が [監査ログ] になりました。監査ログでは、管理者のさまざまな操作を記録し、これにより指定された管理者アカウントのアクティビティのクエリを実行できます。
キュー管理の強化	IMSVA では、受信したばかりのメッセージ、次のメール転送エージェント (MTA) に配信可能なメッセージ、配信不能により遅延されたメッセージ、および後から手動で配信するために保留されているメッセージを MTA キューに保存します。MTA キュー内のメッセージには特定の処理を実行できます。
Smart Protection の強化	IMSVA では、Smart Protection ソースに Trend Micro Smart Protection Network と Smart Protection Server の両方を使用できます。Smart Protection Server を使用すると、Smart Protection サービスを企業ネットワークに対してローカライズし、送信トラフィックを削減して、効率を最適化できます。
外部データベースのサポート	IMSVA では、内部 PostgreSQL データベースに加えて、外部 PostgreSQL データベースを管理データベースまたは EUQ データベースに使用できます。
Time-of-Click プロテクション	メールメッセージ内の不正 URL に対して Time-of-Click プロテクションが提供されます。Time-of-Click プロテクションを有効にすると、IMSVA は、さらなる分析のためにメール内の URL を書き換えます。トレンドマイクロでは、これらの URL をクリック時に分析し、不正なものである場合はブロックします。

新機能	説明
Connected Threat Defense(CTD)	Trend Micro Control Manager (以下、Control Manager) サーバの不審オブジェクトリストを利用するように IMSVA を設定します。Control Manager コンソールを使用すると、不審オブジェクトリストを基に検出されたオブジェクトに対する処理を指定して、トレンドマイクロ製品により保護されているエンドポイントで特定された脅威に対して環境固有のポリシーを提供できます。 Control Manager は、不審オブジェクトを利用して標的型攻撃や高度な脅威を調査します。これにより、システムに危険やデータ損失をもたらす可能性のあるファイルまたは URL が検出されます。
DKIM (DomainKeys Identified Mail) 署名のサポート	送信メールメッセージへの DKIM 署名の追加がサポートされます。IMSVA 管理コンソールでは、DKIM 署名の追加または削除、および DKIM 署名ファイルのインポートまたはエクスポートを実行できます。
メールでのレポート配信	IMSVA では、新しく生成されたレポートや保存されたレポートをメールで送信できます。レポートの詳細情報が含まれます。
キーワードのログクエリへの表示	本文や件名等のエンティティ名 (キーワードが検出されたメッセージ内の項目) および一致したキーワードが [ログクエリの詳細] 画面に表示され、フィルタの実行に使用されたキーワードをより簡単に確認できるようになります。また、キーワードリストで設定したキーワード/正規表現の意味を分かりやすくするために、各キーワードの説明を記載する項目が追加されました。
メッセージ追跡ログでの添付ファイル名のサポート	メッセージ追跡ログに、新しい属性として添付ファイル名が含まれます。メッセージ追跡ログのクエリには、複数の添付ファイル名を指定できます。
ログオン通知のサポート	管理者ログオンページとエンドユーザメール隔離ログオンページの両方で、ログオン通知をカスタマイズできます。
隔離イベントの概要	すべての隔離イベントにおける解除イベントの割合など、詳細情報を含む隔離イベントのログとレポートが提供されます。

新機能	説明
LDAPS のサポート	LDAP over SSL (LDAPS) がサポートされるため、安全で暗号化されたチャネルを使用して LDAP サーバと通信できます。
ランサムウェアの検出	ランサムウェアの検出をよりわかりやすく視覚化する機能が提供されます。ユーザは、ログをクエリするかダッシュボードに専用のウィジェットを追加することでランサムウェアの検出を確認できます。
仮想アナライザとの統合の改善	添付ファイルの名前や拡張子に基づいてメールメッセージを分析用に仮想アナライザに送信するルールを定義できます。

対象読者

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

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

InterScan Messaging Security Virtual Appliance ドキュメント

本製品には、次のドキュメントが付属しています。

- Readme — 基本的なインストール方法と既知の制限事項に関する説明
- オンラインヘルプ — 各種作業を実行するための詳細な手順の説明

- インストールガイド — 製品の概要、インストール計画、インストール、設定、起動方法に関する説明
- 管理者ガイド — 製品の概要、インストール計画、インストール、設定、および製品環境を管理するために必要な詳細情報の説明

注意

最新の情報については弊社の「最新版ダウンロード」サイトをご参照ください。

https://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

---

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 5. ドキュメントの表記規則

表記	説明
注意	設定上の注意
ヒント	推奨事項
重要	必須または初期設定および製品の制限事項に関する情報
警告!	重要な処理と設定オプション

第 1 章

InterScan Messaging Security Virtual Appliance の概要

この章では、InterScan Messaging Security Virtual Appliance 9.1 Service Pack 1 (以下、IMSVA) の特徴、機能、およびテクノロジについて説明します。また、スパムメール対策機能を強化する他のトレンドマイクロ製品の基本情報も示します。

この章の内容は次のとおりです。

IMSVA について

IMSVA では、実績の高いウイルス対策およびスパイウェア対策と、複数層のスパムメール対策およびフィッシング対策が一元化されています。コンテンツフィルタにより、コンプライアンスに対応し、情報漏えいを防止します。IMSVA は、スケーラビリティの高いプラットフォームに簡単に配置でき、集中管理機能の搭載により管理が容易になります。IMSVA は、高度なパフォーマンスと継続的なセキュリティに向けて最適化され、ゲートウェイにおける総合的なメールセキュリティを提供します。

IMSVA の主な特長と利点

次の表に、ネットワークにおける IMSVA の特長と利点について説明します。

表 1-1. 主な特長と利点

特長	説明	利点
データおよびシステムの保護		
クラウドベースのメッセージのプレフィルタ	クラウドプレフィルタは、IMSVA と統合され、メールトラフィックがネットワークに到達する前にすべてのトラフィックを検索します。	クラウドプレフィルタは、スパムメールや不正なメッセージがネットワークに到達しないように、これらの大量のメッセージをブロックできます (全メッセージトラフィックの最大 90%)。
メール暗号化	Trend Micro Email Encryption は、IMSVA と統合され、ネットワークで送受信されるすべてのメールトラフィックを暗号化または復号化します。	Trend Micro Email Encryption によって、IMSVA では、ネットワークから送信されるすべてのメールメッセージを暗号化できます。ネットワークから送信されるすべてのメールメッセージを暗号化することで、ネットワーク管理者は、機密データの漏えいを防ぐことができます。

特長	説明	利点
高度な不正プログラム対策保護	高度な脅威検索エンジン (以下、ATSE) では、パターンベースの検索と強力なヒューリスティック検索を組み合わせて使用することにより、標的型攻撃で使用されるドキュメントエクスプロイトやその他の脅威を検出します。	ATSE では、既知および未知の高度な脅威を識別し、パターンにまだ追加されていない新型の脅威からシステムを保護します。
コマンド&コントロール (C&C) コンタクトアラートサービス	C&C コンタクトアラートサービスにより、IMSVA は、メッセージヘッダの送信者、受信者および返信先アドレスと、メッセージ本文に含まれる URL を調べて、いずれかが既知の C&C オブジェクトに一致しているかどうかを確認できます。	C&C コンタクトアラートサービスでは、強化された検出およびアラート機能により、持続的標的型攻撃 (APT: Advanced Persistent Threats) や標的型攻撃によるダメージを軽減します。
グレーメールの管理	グレーメールとは、スパムメールではなく、ユーザ自身が過去に受信設定を行ったメールです。IMSVA では、マーケティングメッセージ、ニュースレター、およびソーシャルネットワークの通知をグレーメールとして検出します。	IMSVA では、管理者が識別できるように、一般のスパムメールとは区別してグレーメールを管理します。グレーメール除外リストに指定された IP アドレスは検索対象外となります。
規制コンプライアンス	管理者は、新しい初期設定のポリシー検索条件である *[コンプライアンステンプレート]* を使用して、行政機関の規制要件に適合させることができます。	管理者は、規制コンプライアンスに対応するコンプライアンステンプレートを使用できます。利用可能なテンプレートのリストについては、https://success.trendmicro.com/dcx/s/solution/1107704?language=ja を参照してください。

特長	説明	利点
スマートスキャン	スマートスキャンでは、以前 IMSVA サーバに格納されていた脅威のシグネチャをクラウドに格納することで負荷を軽減し、より効率的に検索を実行できるようになります。	スマートスキャンは、Trend Micro Smart Protection Network を利用して次のことを実現します。 • クラウド内での高速かつリアルタイムなセキュリティステータス検索機能の提供 • 新たな脅威に対する保護に必要な時間の短縮 • サーバのメモリ消費量の低減
IntelliTrap	ウイルス作成者は、通常、さまざまなファイル圧縮スキームを使用して、ウイルスフィルタを回避しようとします。IntelliTrap は、これらの圧縮ファイルのヒューリスティック評価を行います。 IntelliTrap が脅威のないファイルをセキュリティリスクとして識別する可能性があるため、IntelliTrap が有効な場合は、このカテゴリに分類されるメッセージの添付ファイルを隔離することをお勧めします。また、ユーザが定期的に圧縮ファイルを交換する場合は、この機能を無効にしなければならないこともあります。 初期設定では、IntelliTrap は、ウイルス対策ポリシーに対する検索条件の 1 つとして有効になっており、セキュリティリスクとして分類される可能性のあるメッセージの添付ファイルを隔離するように設定されています。	IntelliTrap を使用すると、さまざまなファイル圧縮スキームを使用して圧縮されたウイルスがメールを介してネットワークに侵入するリスクを低減できます。
コンテンツ管理	IMSVA は、ネットワークを通じてやりとりされるメールメッセージと添付ファイルの内容が適切かどうかを分析します。	IMSVA では、業務に不要なやりとりや巨大な添付ファイルなど、不適切と思われる内容を効果的にブロックまたは保留できます。

特長	説明	利点
リアルタイムの統計情報と監視	管理者は、管理コンソールでグループ内のすべての IMSVA デバイスの検索パフォーマンスと送信者フィルタパフォーマンスを監視できます。	IMSVA では、管理者がメール処理に関する問題の兆候をすぐに把握できるように、システムの概要を提供します。管理者は、詳細ログを参照して、問題が大きくなる前に対処できます。
その他のメール脅威からの保護		
DoS 攻撃	巨大な添付ファイルでメールサーバを氾濫させたり、複数のウイルスや多重圧縮ファイルが含まれるメッセージを送信したりすることで、悪意のあるユーザがメール処理を妨害することがあります。	IMSVA を使用すると、どのような特性を持つメッセージを SMTP ゲートウェイで阻止するかを設定できるため、DoS 攻撃のリスクを低減できます。
不正なメールコンテンツ	実行可能プログラムや、マクロが埋め込まれたドキュメントなど、ウイルスはさまざまな種類の添付ファイルに潜んでいる可能性があります。HTML スクリプトファイル、HTML リンク、Java アプレット、ActiveX コントロールが含まれるメッセージも、有害な処理を実行する可能性があります。	IMSVA では、SMTP ゲートウェイの通過を許可するメッセージの種類を設定できます。
生産性の低下	ビジネスに関係のないメールトラフィックは、多くの企業で問題となっています。スパムメールメッセージはネットワーク帯域幅を消費し、従業員の生産性に影響します。従業員の中には、会社のメッセージングシステムから個人的なメッセージを送信したり、巨大なマルチメディアファイルを転送したり、業務時間内に個人的なビジネスを行ったりする人もいます。	ほとんどの企業では、メッセージングシステムの使用許容範囲を示すポリシーを制定しています。IMSVA は、企業の既存のポリシーを適用し、準拠させることのできるツールを提供します。

特長	説明	利点
法的責任とビジネスの信頼性	メールが不正に使用されると、企業の法的責任が問われる場合があります。従業員が性的または人種的嫌がらせを行っていたり、他の違法活動に携わっていたりするかもしれません。また、従業員の不正行為により、社内のメッセージングシステムから機密情報が漏えいする可能性もあります。企業のメールサーバから配信される不適切なメッセージは、そのメッセージの内容が企業の持論と異なるものであったとしても、企業の評判を損ねることになります。	IMSVA には、コンテンツを監視してブロックするツールが装備されているため、不適切な内容や機密事項が含まれるメッセージがゲートウェイを通過するリスクを低減できます。
マスメーリング型ウイルスの封じ込め	メール送信型ウイルスにより、社内のメッセージングシステムを介して偽装メッセージが自動的に広がることがあります。そのため、クリーンナップに費用がかかったり、ユーザの間でパニックが発生したりする可能性があります。 IMSVA がマスメーリング型ウイルスを検出した場合、このウイルスに対する処理を、他の種類のウイルスに対する処理とは異なったものにすることが可能です。 たとえば、IMSVA が重要な情報を含む Microsoft Office ドキュメントにマクロウイルスを検出した場合、重要な情報を失わないようにするために、メッセージ全体を削除するのではなくメッセージを隔離するようにプログラムを設定できます。一方で、マスメーリング型ウイルスを検出した場合は、メッセージ全体を自動的に削除するようにプログラムを設定できます。	マスメーリング型ウイルスを含むメッセージを自動的に削除することにより維持する価値のないメッセージやファイルを検出、隔離、または処理するためにサーバのリソースを削減できます。 既知のマスメーリング型ウイルス ID は、TrendLabs℠ (トレンドラボ) アップデートサーバを使用してアップデートされるマスメーリングパターンファイル内にあります。この種類のウイルスとそのメールの自動削除を有効にすることにより、リソースの節約、関連部署へのヘルプデスクコールの回避、および大規模感染後のクリーンナップ作業の排除を実現できます。
スパイウェアと他の種類のグレーウェアからの保護		

特長	説明	利点
スパイウェアと他の種類のグレーウェア	クライアントは、スパイウェア、アドウェア、ダイヤラーなど、ウイルス以外の潜在的な脅威のリスクにもさらされています。詳細については、13 ページの「スパイウェアと他の種類のグレーウェアについて」を参照してください。	IMSVA を使用すると、スパイウェアや他の種類のグレーウェアから環境を保護できるため、企業のセキュリティ、機密性、法的責任に関わるリスクを大幅に軽減できます。
統合されたスパムメール対策機能		
スパムメール対策 (コンテンツ検索)	IMSVA では、オプションでスパムメール対策 (コンテンツ検索) 機能を追加できます。この機能を使用するには、別途アクティベーションコードが必要になります。詳細については、販売店にお問い合わせください。 なお、スパムメール対策機能は、アクティベーションコードを入力してアクティベーションを完了した時点で有効になります。	スパムメール対策 (コンテンツ検索) では、高度なコンテンツ処理と統計分析に基づく検索テクノロジが使用されています。他の手法によるスパムメールの識別とは異なり、コンテンツ分析機能を採用したことで、パフォーマンスの高いリアルタイムの検出が可能です。スパムメールの送信者が手法を変更した場合でも、容易に対応できます。

特長	説明	利点
IP プロファイラ、メールレピュテーション、および SMTP トラフィックスロットリングによるスパムメールフィルタ	IP プロファイラは、自己学習能力と十分なカスタマイズ性を備えており、スパムメールや他の潜在的な脅威を送信するコンピュータの IP アドレスを能動的にブロックします。メールレピュテーションは、トレンドマイクロのデータベースで管理される既知のスパムメール送信者の IP アドレスをブロックします。SMTP トラフィックスロットリングは、接続数またはメッセージ数が指定した最大数に達した場合に、単一の IP アドレスまたは送信者からのメッセージを一定期間ブロックします。 注意 IP プロファイラとメールレピュテーションを設定する前にスパムメール対策 (コンテンツ検索) をアクティベートしてください。	IP プロファイラ、メールレピュテーション、および SMTP トラフィックスロットリングからなる送信者フィルタ機能を統合することで、IMSVA は IP レベルでスパムメール送信者をブロックできます。
ソーシャルエンジニアリング攻撃からの保護	ソーシャルエンジニアリング攻撃からの保護機能により、メールに含まれるソーシャルエンジニアリング攻撃を行う可能性のある不審な動作を検出できます。	本機能が有効な場合、スパムメール検索エンジンは、送信メール内のメールヘッダ、件名、本文、添付ファイル、SMTP プロトコル情報などに対して不審な動作を検索します。スパムメール検索エンジンは、ソーシャルエンジニアリング攻撃に関連する動作を検出するとメッセージの詳細を IMSVA に返し、IMSVA は、追加の処理を実行するか、ポリシーを適用するか、またはレポートを作成します。
管理と統合		

特長	説明	利点
LDAP およびドメインベースのポリシー	ユーザグループの定義および管理者権限に Lotus Domino™、Microsoft™ Active Directory™などの LDAP ディレクトリサービスを使用している場合は、LDAP を設定できます。	LDAP を使用すると、さまざまなルールを定義して、企業のメールの使用ガイドラインを適用することができます。送信者および受信者のアドレスに基づいて、個人またはグループ用のルールを定義できます。
Web ベースの管理コンソール	管理コンソールを使用すると、IMSVA のポリシーおよび設定を簡単に変更できます。	管理コンソールは SSL に準拠しています。SSL に準拠することで、より安全に IMSVA にアクセスできます。
エンドユーザメール隔離	IMSVA には、スパムメール管理を強化するための Web ベースのエンドユーザメール隔離が用意されています。Web ベースのエンドユーザメール隔離サービスを使用すると、エンドユーザは各自の個人アカウントおよび、自分が所属する配布リストのスパムメールの隔離方法を管理できます。IMSVA では、スパムメールと判定されたメッセージを隔離します。これらのメッセージは、エンドユーザメール隔離によってデータベース内でインデックスが付けられます。エンドユーザはメッセージを再確認したり、削除したり、または配信を許可したりできます。	Web ベースのエンドユーザメール隔離管理コンソールを使用すると、エンドユーザは IMSVA によって隔離されたメッセージを管理できます。 IMSVA ではさらに、エンドユーザメール隔離通知内のリンクを介して隔離されたメッセージに処理を適用でき、送信者を承認済み送信者リストに追加できます。
管理タスクの委任	IMSVA には、管理コンソールにさまざまなアクセス権限を作成する機能が用意されています。管理者のログオンアカウントごとに、アクセスを許可するコンソールのセクションを選択できます。	管理ロールをさまざまな従業員に委任することで、管理職務の共有を促進できます。

特長	説明	利点
レポート機能の一元化	一元化されたレポート機能により、レポートを必要に応じてそのつど作成することも、予約して作成することもできます。	IMSVA の稼働状況を解析できます。 必要に応じてそのつど作成するレポートでは、レポートのコンテンツを必要に応じて指定できます。また、レポートを日次、週次、および月次ベースで自動生成するように設定することもできます。 IMSVA では、1 回限りのレポートと予約レポートをメールで送信できます。
システムの可用性の監視	組み込みエージェントが IMSVA サーバの状態を監視し、メールフローを妨害する可能性のある違反状況が発生した場合に、メールまたは SNMP トラップを通じて通知を配信します。	システム障害の検出をメールや SNMP で通知することにより、迅速に修正措置を実行し、停止時間を最小限に抑えられるようにします。
POP3 検索	管理コンソールからの POP3 検索は、任意で有効または無効に設定できます。	SMTP トラフィックの他に、IMSVA では、ネットワーク内のメッセージングクライアントがメッセージを受信する際に、ゲートウェイで POP3 メッセージも検索できます。
クラスタ化アーキテクチャ	本バージョンの IMSVA 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 IMSVA 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 IMSVA 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。

特長	説明	利点
仮想アナライザとの統合	IMSVA は仮想アナライザと統合されています。この隔離された仮想環境は、Deep Discovery Advisor と Deep Discovery Analyzer 内でサンプルを管理および分析するために使用されます。	IMSVA では、不審なファイルや URL を仮想アナライザのサンドボックス環境に送信してシミュレーションを実行します。仮想アナライザでは、パスワードで保護されたアーカイブやドキュメントなどのファイルを開き、URL にアクセスして、不正なコード、C&C とボットネット接続、その他の不審な動作や特性についてテストします。
Control Manager との統合	Control Manager は、ウイルス対策プログラムとコンテンツセキュリティプログラムを、その物理的な位置やプラットフォームに関係なく中央から制御できるようにするソフトウェア管理ソリューションです。このアプリケーションは、企業のウイルスおよびコンテンツセキュリティポリシーの管理を簡略化します。	Control Manager から配信される大規模感染予防サービスにより、大規模感染のリスクを低減できます。トレンドマイクロの製品で新種のメール送信型ウイルスが検出されると、トレンドラボから詳細なコンテンツフィルタを使用するポリシーが発行されるため、IMSVA でメッセージ内の不審な特性を識別して、メッセージをブロックすることができます。これらのルールは、最新のパターンファイルが提供されるまでの期間、感染の機会を最小限に抑えるのに役立ちます。
Syslog サーバとの統合	IMSVA は、Syslog プロトコルを使用してログメッセージを受信する Syslog サーバと統合されています。Syslog プロトコルは幅広いネットワークデバイスでサポートされるネットワークログ記録の標準プロトコルであり、Syslog サーバにはネットワークのイベントやエラーに関する情報が格納されます。	Syslog サーバを統合することで、複数の IMSVA サーバを管理してログの収集を一元化し、ネットワーク全体のログデータを単一の集中リポジトリに統合できます。Syslog メッセージの収集と分析は、ネットワークの安定性の維持とネットワークセキュリティの監査に欠かせません。

特長	説明	利点
Time-of-Click プロテクション	メールメッセージ内の不正 URL に対して Time-of-Click プロテクションが提供されます。	Time-of-Click プロテクションを有効にすると、IMSVA は、さらなる分析のためにメール内の URL を書き換えます。トレンドマイクロでは、これらの URL をクリック時に分析し、不正なものである場合はブロックします。

クラウドプレフィルタについて

クラウドプレフィルタは、IMSVA と統合され、クラウドでの予防的なプライバシーの保護と、ローカルの仮想アプライアンスの制御を可能にするクラウドセキュリティソリューションです。

クラウドプレフィルタは、ネットワークの外側でスパムメールや不正プログラムをブロックすることにより、最大 90%まで受信メールメッセージの量を削減します。クラウドプレフィルタは、ゲートウェイの位置で IMSVA と統合され、機密情報の柔軟な制御を可能にします。さらに、メールメッセージはローカルへ隔離されるため、メールメッセージの機密性が維持されます。メールメッセージがクラウド内に保存されることはありません。クラウドプレフィルタを使用することで、複雑さが緩和され、管理工数が削減されるため、大幅な経費の節約が可能です。

Trend Micro Email Encryption の概要

Trend Micro Email Encryption によって、IMSVA では、メールメッセージの暗号化および復号化を実行できます。Trend Micro Email Encryption を使用することで、メールクライアントやプラットフォームがどの場所にあっても、IMSVA ではメールメッセージの暗号化および復号化が可能になります。Trend Micro Email Encryption でのメールメッセージの暗号化および復号化は Policy Manager で制御します。管理者は、Policy Manager で送信者や受信者のメールアドレス、キーワード、またはメールメッセージ (添付ファイルを含む) に含まれているクレジットカード番号の場所などのパラメータを基にポリシーを設定できます。Trend Micro Email Encryption 自体は、SMTP (Simple Mail Transfer Protocol) インタフェースとして提供され、メールメッセージは SMTP を介して、設定済みの送信メール転送エージェント (MTA) へ配信されます。これにより、コンテンツ検索サービス、メールサーバ、アー

カイブソリューションなど、他のメールサーバベース製品と簡単に統合できます。

スパイウェアと他の種類のグレーウェアについて

企業ユーザは、ウイルスや不正プログラム以外の潜在的な脅威のリスクにもさらされています。グレーウェアは、ネットワーク上のコンピュータのパフォーマンスに悪影響を与え、セキュリティ上、機密性、および法的責任において、企業に深刻なリスクをもたらします。

表 1-2. グレーウェアの種類

種類	説明
スパイウェア	アカウント ID やパスワードなどの情報を収集し、外部へ送信します。
アドウェア	広告を表示したり、Web ブラウザを通じてユーザの Web 閲覧の好みなどの情報を収集したりして、ユーザに対する広告の的を絞ります。
ダイヤラー	コンピュータのインターネット設定を変更し、あらかじめ設定された電話番号に、コンピュータがモデムを通じて自動的にダイヤルするようにします。
ジョークプログラム	CD-ROM トレイを開閉したり、大量のメッセージボックスを表示したりするなど、コンピュータの異常動作を引き起こします。
ハッキングツール	ハッカーがコンピュータに侵入するのを手助けします。
リモートアクセスツール	ハッカーがコンピュータへリモートアクセスして制御するためのツールです。
パスワード解読アプリケーション	ハッカーがアカウントユーザ名とパスワードを解読するためのツールです。
その他	上記以外の種類

スパイウェア/グレーウェアがネットワークに侵入する方法

スパイウェア/グレーウェアは、ユーザが正規のソフトウェアをダウンロードした場合でも、そのソフトウェアのインストールパッケージにグレーウェアアプリケーションが含まれていて、企業ネットワークに侵入することがあります。

大部分のソフトウェアプログラムには、ダウンロードする前にユーザが同意しなければならない使用許諾契約書 (EULA) が含まれています。多くの場合、使用許諾契約書にはアプリケーションと個人データ収集の使用目的に関する情報が記載されていますが、ユーザはこうした情報を見過ごしたり、法律用語を理解できないことがあります。

潜在的なリスクと脅威

ネットワーク上にスパイウェアやグレーウェアが存在すると、以下の事態が発生する可能性があります。

表 1-3. リスクの種類

種類	説明
コンピュータのパフォーマンスの低下	スパイウェア/グレーウェアアプリケーションがタスクを実行するには、CPU とシステムメモリのリソースを大量に必要とします。
Web ブラウザ関連のクラッシュの増加	アドウェアなど特定の種類のグレーウェアは、ポップアップウィンドウを作成したり、ブラウザフレーム内やウィンドウ内に情報を表示するように設計されているものがあります。こうしたアプリケーションのコードがシステム処理に与える影響の程度によって、グレーウェアはブラウザをクラッシュまたはフリーズさせたりする場合があり、システムの再起動が必要になることもあります。
ユーザ効率の低下	頻繁に表示されるポップアップ広告を閉じて、ジョークプログラムの弊害に対処しなければならないため、ユーザは本来の作業に集中できない場合があります。
ネットワーク帯域幅の効率低下	スパイウェア/グレーウェアアプリケーションは、収集したデータをネットワーク上で実行されている他のアプリケーションやネットワークの外部に定期的に送信することがあります。
個人情報や企業情報の漏えい	スパイウェア/グレーウェアが収集するデータは、ユーザがアクセスする Web サイトの一覧のような無害な情報ばかりではありません。スパイウェア/グレーウェアは、銀行口座などの個人アカウントや、ネットワーク上のリソースに接続している企業アカウントへのアクセス時に入力したユーザ名やパスワードも収集できます。

種類	説明
法的責任におけるリスクの増大	ネットワーク上のコンピュータリソースにハッカーが侵入した場合、ハッカーはクライアントコンピュータを利用して攻撃を開始したり、ネットワーク外のコンピュータにスパイウェア/グレーウェアをインストールしたりできます。このような活動に社内のネットワークリソースが関与すると、他の組織が被った損害に対して法律上の責任を問われる場合があります。

Web レピュテーションサービスについて

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

メールレピュテーションについて

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

メールレピュテーションの種類

メールレピュテーションには、「15 ページの標準」と「16 ページの詳細」の 2 種類があります。

メールレピュテーション: 標準

このサービスでは、要求された IP アドレスを、Trend Micro Smart Protection Network によって管理されているトレンドマイクロの評価データベースと照合して検証することにより、スパムメールをブロックします。この拡張を続けるデータベースには、現在 10 億を超える IP アドレスが、スパムメールの活動に基づく評価とともに格納されています。トレンドマイクロのスパムメ

ール調査担当者は、これらの評価の見直しと更新を継続的に行い、その精度を高めています。

「メールレピュテーション: 標準」サービスは、DNS 単一クエリベースのサービスです。未知のホストからメールメッセージを受信するたびに、指定されたメールサーバは、標準評価データベースサーバに対して DNS クエリを実行します。そのホストが標準評価データベースに存在すれば、メールレピュテーションはそのメールメッセージをスパムメールとしてレポートします。

ヒント

標準レピュテーションデータベースのデータに合致した IP アドレスからのメールメッセージは、受信せずブロックするように IMSVA を設定することをお勧めします。

メールレピュテーション: 詳細

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

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

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

メールレピュテーションテクノロジの仕組み

トレンドマイクロのメールレピュテーションテクノロジは、ドメインネームサービス (DNS) のクエリベースのサービスです。次のプロセスは、IMSVA が、送信側メールサーバから接続要求を受信した後に実行されます。

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

下記の図は、メールレピュテーションの仕組みを示します。

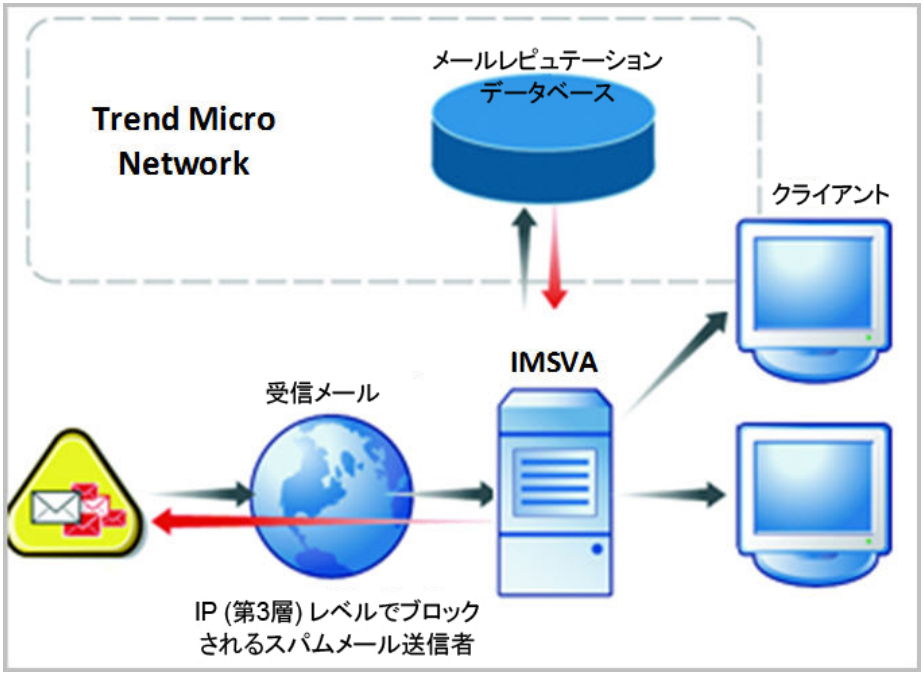


図 1-1. メールレピュテーションの仕組み

メールレピュテーションの動作の詳細については、https://servicecentral.trendmicro.com/ja-jp/ers/を参照してください。

Trend Micro Control Manager について

Trend Micro Control Manager (以下、Control Manager) は、ウイルス対策プログラムとコンテンツセキュリティプログラムを、その物理的な位置やプラットフォームに関係なく中央から制御できるようにするソフトウェア管理ソリューションです。このアプリケーションは、企業のウイルス/不正プログラムおよびコンテンツセキュリティポリシーの管理を簡略化します。

- Control Manager サーバ: Control Manager サーバは、Control Manager アプリケーションがインストールされるコンピュータです。Control

Manager の Web ベースの管理コンソールは、このサーバでホストされます。

- エージェント: エージェントは、Control Manager が製品を管理できるように、管理下の製品にインストールされるアプリケーションです。エージェントは Control Manager サーバからコマンドを受信して、管理下の製品に適用します。また、製品からログを収集して、Control Manager に送信します。
- エンティティ: エンティティは、製品ディレクトリ上の管理下の製品を表します。各エンティティは、ディレクトリツリーにアイコンで表示されます。このディレクトリには、Control Manager コンソールにある、管理下のすべてのエンティティが表示されます。

Control Manager サポート

次の表では、IMSVA でサポートされている Control Manager の機能を示しています。

表 1-4. サポートされる Control Manager の機能

特長	説明	サポートの有無
双方向通信	双方向通信では、IMSVA と Control Manager のいずれも通信プロセスを開始できます。	なし IMSVA 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	大規模感染予防ポリシー (OPP) は、トレンドラボによって開発され、大規模感染に迅速に対応します。このポリシーには、IMSVA サーバまたはそのクライアントの感染確率を減らすために、IMSVA で実行する必要のある処理が一覧表示されます。 トレンドマイクロのアップデートサーバは、このポリシーを Control Manager 経由で IMSVA に配信します。	あり

特長	説明	サポートの有無
クエリ用のログのアップロード	クエリの目的で IMSVA 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	IMSVA 管理コンソールに最初にログオンせずに、Control Manager から IMSVA を直接管理します。	なし Control Manager から IMSVA を管理するには、まず IMSVA 管理コンソールにログオンする必要があります。
設定の複製	Control Manager で既存の IMSVA サーバから新規の IMSVA サーバに設定を複製します。	あり
パターンファイルのアップデート	Control Manager から IMSVA によって使用されるパターンファイルをアップデートします。	あり
エンジンのアップデート	Control Manager から IMSVA によって使用されるエンジンをアップデートします。	あり
製品コンポーネントのアップデート	Control Manager から Patch や HotFix などの IMSVA 製品コンポーネントをアップデートします。	なし 製品コンポーネントのアップデート方法については、Patch または HotFix の Readme を参照してください。
ユーザインタフェースリダイレクトによる設定	Control Manager からアクセス可能な IMSVA 管理コンソールを使用して IMSVA を設定します。	あり
製品登録の更新	Control Manager から IMSVA ライセンスを更新します。	あり

特長	説明	サポートの有無
Control Manager のカスタムレポート	Control Manager には、メール関連データについてカスタムレポートを生成したりログクエリを実行したりする機能が用意されています。	あり
Control Manager エージェントのインストール/アンインストール	Control Manager から IMSVA Control Manager エージェントをインストールまたはアンインストールします。	なし IMSVA Control Manager エージェントは、IMSVA をインストールすると自動的にインストールされます。エージェントを有効または無効にするには、IMSVA 管理コンソールから次の操作を行います。 1. [管理] > [接続] の順に選択します。 2. [Control Manager サーバ] タブをクリックします。 3. エージェントを有効または無効にするには、[MCP エージェントを有効にする] の横にあるチェックボックスをオンまたはオフにします。
イベント通知	Control Manager から IMSVA イベント通知を送信します。	あり
すべてのコマンドに対するコマンド追跡	Control Manager が IMSVA に対して発行するコマンドのステータスを追跡します。	あり

グレーメールの検索について

グレーメールとは、スパムメールではなく、ユーザ自身が過去に要請した大量のメールメッセージのことを指します。IMSVA では、マーケティングメッセージ、ニュースレター、およびソーシャルネットワークの通知をグレーメールとして検出します。IMSVA では、次の 2 つの方法でグレーメールメッセージを識別します。

- 送信元 IP アドレスにスコアを割り当てるメールレピュテーションサービス
- メッセージコンテンツを識別するトレンドマイクロのスパムメール対策エンジン

注意

IMSVA では、これらの種類のメールメッセージを検出しますが、スパムメールのタグは付けません。

管理者は、検出されたメールメッセージを処理するためのルールの条件を定義します。各グレーメールメッセージのルールには、メッセージフィルタをバイパスするアドレスオブジェクトを含む除外リストがあります。アドレスオブジェクトは、単一の IP アドレスまたはアドレス範囲 (IPv4 または IPv6)、または CIDR (Classless Inter-Domain Routing) ブロックのいずれかです。

管理者には、ネットワーク内のグレーメールメッセージトラフィックについて理解するためのいくつかのオプションが用意されています。レポートは、外部または内部の送信元からのグレーメールメッセージの最多送信者と最多受信者を示します。管理者は、詳細なログ情報のクエリを実行したり、メール隔離を表示して、許可するグレーメールメッセージとして識別されたメッセージを必要に応じて解除したりすることができます。

グレーメールメッセージの除外リストは、エクスポートおよびインポートできます。

注意

グレーメール検索で IMSVA が外部 DNS サーバをクエリできることを確認してください。DNS サーバの設定を変更する場合は、検索サーバを再起動して新しい設定をロードしてください。

コマンド&コントロール (C&C) コンタクトアラートサービスについて

トレンドマイクロの C&C コンタクトアラートサービスでは、強化された検出およびアラート機能により、持続的標的型攻撃 (APT: Advanced Persistent Threats) や標的型攻撃によるダメージを軽減します。このサービスは、Trend

Micro Smart Protection Network によってコンパイル、テスト、および評価されたグローバルインテリジェンスリストを使用してコールバックアドレスを検出します。

C&C コンタクトアラートサービスにより、IMSVA は、メッセージヘッダの送信者、受信者および返信先アドレスと、メッセージ本文に含まれる URL を調べて、いずれかが既知の C&C オブジェクトに一致しているかどうかを確認できます。管理者は、メッセージがフラグ付けされたら、該当するメッセージを隔離して通知を送信するように IMSVA を設定できます。検出されたすべてのメールは、C&C オブジェクトと、これらのメッセージに対して実行された処理とともにログに記録されます。これらのログは、クエリ目的で Control Manager に送信されます。

第 2 章

コンポーネントの説明

この章では、IMSVA の管理に必要な要件と使用される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。

IMSVA コンポーネントについて

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

クラウドプレフィルタサービスの概要

クラウドプレフィルタサービスは、トレンドマイクロのメールセキュリティプラットフォームと統合された管理下のメールセキュリティサービスです。このサービスを介して受信メッセージをルーティングすることにより、スパムメール、フィッシング、不正プログラムなど、メッセージング関連の脅威がネットワークに到達するのを阻止し、これらの脅威からドメインを保護できます。

送信者フィルタ

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

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

レピュテーションベースの送信元のフィルタ

トレンドマイクロのメールレピュテーションにより、クラウドプレフィルタサービスは、メールの送信元を動的な自己更新型のレピュテーションデータベースに対して検証することで、スパムメール/フィッシング詐欺メールの送信者や不正プログラムの配布元によって制御された IP アドレスからのメッセージ、および最新のボットネットからのメッセージをブロックします。

ウイルスおよびスパムメールからの保護

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

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

スパムメール対策 (コンテンツ検索) について

IMSVA では、オプションでスパムメール対策 (コンテンツ検索) 機能をインストールすることもできます。この機能を使用するには、別途アクティベーションコードが必要になります。詳細については、販売店にお問い合わせください。

スパムメール対策 (コンテンツ検索) テクノロジ

スパムメール対策 (コンテンツ検索) では、最新のコンテンツ処理および統計分析に基づく検出テクノロジが使用されています。スパムメール識別の他の手法とは異なり、コンテンツ分析機能を採用したことで、パフォーマンスの高いリアルタイムの検出が可能となっています。スパムメールの送信者が手法を変更した場合でも、容易に対応できます。

スパムメール対策 (コンテンツ検索) の使用

スパムメール対策 (コンテンツ検索) は、組み込みのスパムメールフィルタを通じて機能します。このフィルタは、スパムメール対策 (コンテンツ検索) 用のアクティベーションコードを入力してアクティベーションを完了した時点で有効になります。

送信者フィルタについて

IMSVA には、オプションの送信者フィルタも搭載されています。これは、次の 3 つの機能で構成されます。

IP プロファイラ

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

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

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

メールレピュテーション
既知のスパムメール送信者からのメールを IP レベルでブロックします。

SMTP トラフィックスロットリング
接続数またはメッセージ数が指定した最大数に達した場合に、単一の IP アドレスまたは送信者からのメッセージを一定期間ブロックします。

IP プロファイラの機能

IP プロファイラは、27 ページの「送信者フィルタについて」の項で説明した脅威を含むメールメッセージを送信したコンピュータの IP アドレスを能動的に特定します。IMSVA でいつ IP アドレスに対して指定の処理を開始するかは、いくつかの条件をカスタマイズすることで指定できます。条件は潜在的な脅威に応じて異なりますが、IMSVA が IP アドレスとしきい値を監視する期間はいずれも共通です。

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

1. FoxProxy が IP プロファイラの DNS サーバに問い合わせを行い、ブロックリストにその IP アドレスが含まれているかどうかを確認します。

2. ブロックリストに IP アドレスが含まれている場合は、IMSVA が接続要求を拒否します。

   ブロックリストに IP アドレスが含まれていない場合、IMSVA が、IP プロファイラに指定されたしきい値の条件に従ってメールトラフィックを解析します。

3. メールトラフィックが条件に違反している場合、IMSVA はその送信者の IP アドレスをブロックリストに追加します。

SMTP トラフィックスロットリングの機能

SMTP トラフィックスロットリングは、接続要求やメールメッセージを頻繁に配信する IP アドレスまたは送信者アドレスを特定し、それらのアドレスが特定のルールに該当する場合にブロックします。すべての IP アドレスと送信者の動作を監視し、必要に応じて処理を実行するように、IP ベースまたは送信者ベースのスロットリングルールをカスタマイズできます。ルールの条件には、監視期間、許可される接続またはメッセージの最大数、およびブロック期間が含まれます。送信者ベースのスロットリングでは接続の最大数を指定できないのに対し、IP ベースのスロットリングでは指定できる点が異なります。

次のプロセスは、SMTP トラフィックスロットリングが、送信側メールサーバまたは送信者から接続要求を受信した後に実行されます。

1. 指定した監視期間に対象の IP アドレスから受信した接続数が記録されます。
2. 指定した監視期間に対象の IP アドレスから受信したメールメッセージ数が記録されます。
3. 指定した監視期間に対象の送信者から受信したメールメッセージ数が記録されます。
4. 対象の IP アドレスから受信した接続またはメッセージの数が設定したしきい値に達した場合、この IP アドレスがブロックリストに追加され、この IP アドレスからの後続の接続またはメッセージを一時的にブロックします。
5. 対象の送信者から受信した接続またはメッセージの数が設定したしきい値に達した場合、この送信者がブロックリストに追加され、この送信者からの後続の接続またはメッセージを一時的にブロックします。

エンドユーザメール隔離について

IMSVA には、スパムメール管理を強化するための Web ベースのエンドユーザメール隔離が用意されています。Web ベースのエンドユーザメール隔離サービスを使用すると、エンドユーザは各自のスパムメールの隔離方法を管理できます。スパムメール対策 (コンテンツ検索)、または管理者が作成したコンテンツフィルタによってスパムメールと判定されたメッセージは隔離されます。これらのメッセージは、エンドユーザメール隔離エージェントによってデータベース内でインデックスが付けられるため、エンドユーザはメッセージを再確認して、削除したり、配信を許可したりできます。

一元化されたレポート機能について

IMSVA の稼働状況を解析するために、一元化されたレポート機能を使用できます。レポートは、必要に応じてそのつど作成するように設定することも、日次、週次、および月次ベースで自動生成するように設定することもできます。IMSVA では、1 回限りのレポートと予約レポートをメールで送信できます。

第 3 章

配置計画

この章では、IMSVA の配置計画の手順について説明します。初期設定を実行する手順については、「管理者ガイド」を参照してください。

この章の内容は次のとおりです。

配置タスクのチェックリスト

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

1. クラウドプレフィルタを使用して IMSVA を配置する

完了したらチェックマークを記入	タスク	オプションかどうか	参照先
	クラウドプレフィルタを使用する配置	オプション	35 ページの「クラウドプレフィルタを使用して IMSVA を配置する」

2. IMSVA の配置場所の決定

完了したらチェックマークを記入	タスク	オプションかどうか	参照先
	IMSVA をネットワーク上のどの位置に配置するかを、次の中から選択します。		
	ゲートウェイ		36 ページの「ゲートウェイまたはゲートウェイの内側へ配置する」
	ゲートウェイの内側		36 ページの「ゲートウェイまたはゲートウェイの内側へ配置する」
	ファイアウォールなし		
	ファイアウォールの外側		
	ファイアウォールの内側		
	DMZ (非武装地帯) 内		

3. 範囲の計画

完了したらチェックマークを記入	タスク	オプションかどうか	参照先
	単一の IMSVA デバイスをインストールするか、複数の IMSVA デバイスをインストールするかを選択します。		
	1 つのデバイスのインストール		42 ページの「デバイスの役割について」
	複数の IMSVA デバイス		42 ページの「デバイスの役割について」

4. 配置またはアップグレード

完了したらチェックマークを記入	タスク	オプションかどうか	参照先
	新しい IMSVA デバイスを配置するか、以前のバージョンからアップグレードします。		
	以前のバージョンからのアップグレード		89 ページの以前のバージョンからのアップグレード

5. サービスの開始

完了したらチェックマークを記入	タスク	オプションかどうか	参照先
	IMSVA の各サービスを有効にし、さまざまな脅威に対するネットワークの保護を開始します。		
	検索サービス		「管理者ガイド」の IMSVA サービスに関する項
	ポリシー		

完了したらチェックマークを記入	タスク	オプションかどうか	参照先
	エンドユーザメール隔離	オプション	

6. その他の IMSVA の設定

完了したらチェックマークを記入	タスク	オプションかどうか	参照先
	IMSVA の起動および実行に必要な各種項目を設定します。		
	送信者フィルタルール	オプション	「管理者ガイド」の送信者フィルタサービスに関する項
	SMTP ルーティング		「管理者ガイド」の SMTP メッセージの検索に関する項
	POP3 設定	オプション	「管理者ガイド」の POP3 メッセージの検索に関する項
	ポリシーおよび検索の除外		「管理者ガイド」のポリシーの管理に関する項
	コンポーネントの手動アップデートの実行および予約アップデートの設定		「管理者ガイド」の検索エンジンおよびパターンファイルのアップデートに関する項
	ログ設定		「管理者ガイド」のログの設定に関する項

7. IMSVA のバックアップ

完了したらチェックマークを記入	タスク	オプションかどうか	参照先
	システムの障害時に備えて IMSVA のバックアップを実行します。		

完了したらチェックマークを記入	タスク	オプションかどうか	参照先
	IMSVA 設定をバックアップする		「管理者ガイド」の IMSVA のバックアップに関する項

ネットワークトポロジの考慮事項

既存のメールおよびネットワークトポロジでの IMSVA の使用方法を決定します。この項では、SMTP トラフィックを処理する際の一般的なシナリオを示します。

クラウドプレフィルタを使用して IMSVA を配置する

クラウドプレフィルタが IMSVA の配置方法に影響することはありません。

注意

クラウドプレフィルタは、ポート 9000 を Web サービスの待機ポートとして使用します。IMSVA でクラウドプレフィルタに接続するには、ファイアウォールでこのポートが開かれている必要があります。

ただし、クラウドプレフィルタのポリシーを追加する際は、MX レコードの変更が必要です。ポリシーで指定されたドメインの MX レコードを、クラウドプレフィルタの受信アドレスの MX レコードに変更します。このアドレスは、[クラウドプレフィルタポリシーリスト] 画面の下部に表示されます。IMSVA 管理コンソールの [クラウドプレフィルタ] をクリックして、[クラウドプレフィルタポリシーリスト] 画面を表示します。

ヒント

IMSVA のアドレスをドメインの MX レコードに追加して、IMSVA の優先度をクラウドプレフィルタよりも低くすることをお勧めします。これにより、クラウドプレフィルタのバックアップとして、IMSVA でメールサービスの継続性を確保できます。

ゲートウェイまたはゲートウェイの内側へ配置する

表 3-1. SMTP トラフィックを処理する際の一般的なシナリオ

	1 つのデバイス	複数のデバイス
ゲートウェイ	このデバイスに送信者フィルタを使用する場合にのみこのセットアップを実行します。IMSVA は、ウイルス対策、コンテンツフィルタ、スパムメール対策、および IP フィルタサービスを提供するゲートウェイに配置されます。送信者フィルタサービスには、Trend Micro Network Reputation Services (以下、NRS) と IP プロファイラがあります。37 ページの図 3-1：ゲートウェイに 1 つの IMSVA デバイスを配置する場合を参照してください。	1 つ以上のデバイス上で送信者フィルタを使用する場合にのみ用いるセットアップです。それぞれのデバイスでサービスを有効または無効にできます。次の項目を参照してください。 • 38 ページの図 3-3：ゲートウェイに IMSVA グループを配置する場合 • 43 ページの「サービスの選択」
ゲートウェイの内側	最も一般的なセットアップです。IMSVA は、ウイルス対策、コンテンツフィルタ、およびスパムメール対策サービスを提供する、アップストリーム MTA とダウンストリーム MTA の間に配置されます。37 ページの図 3-2：ゲートウェイの内側に 1 つの IMSVA デバイスを配置する場合を参照してください。	最も一般的なグループセットアップです。IMSVA デバイスは、ウイルス対策、コンテンツフィルタ、およびスパムメール対策サービスを提供する、アップストリーム MTA とダウンストリーム MTA の間に配置されます。それぞれのデバイスでサービスを有効または無効にできます。次の項目を参照してください。 • 38 ページの図 3-4：ゲートウェイの内側に IMSVA グループを配置する場合 • 43 ページの「サービスの選択」
Trend Micro Control Manager シナリオ		

	1 つのデバイス	複数のデバイス
複数のグループを使用する場合は、Trend Micro Control Manager (以下、Control Manager) を使用してデバイスを管理できます。		

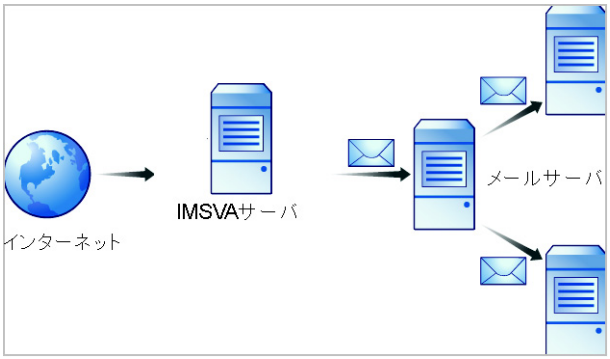


図 3-1. ゲートウェイに 1 つの IMSVA デバイスを配置する場合

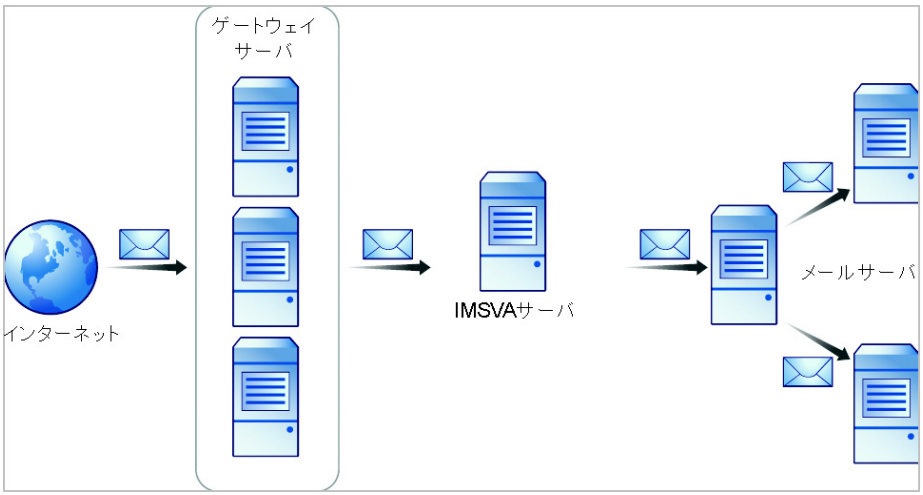


図 3-2. ゲートウェイの内側に 1 つの IMSVA デバイスを配置する場合

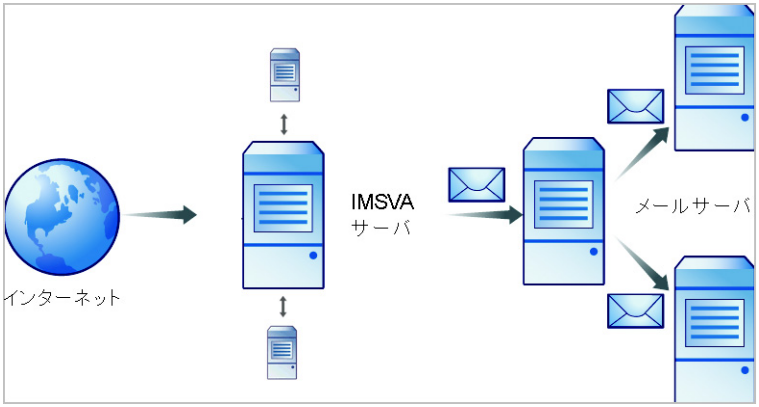


図 3-3. ゲートウェイに IMSVA グループを配置する場合

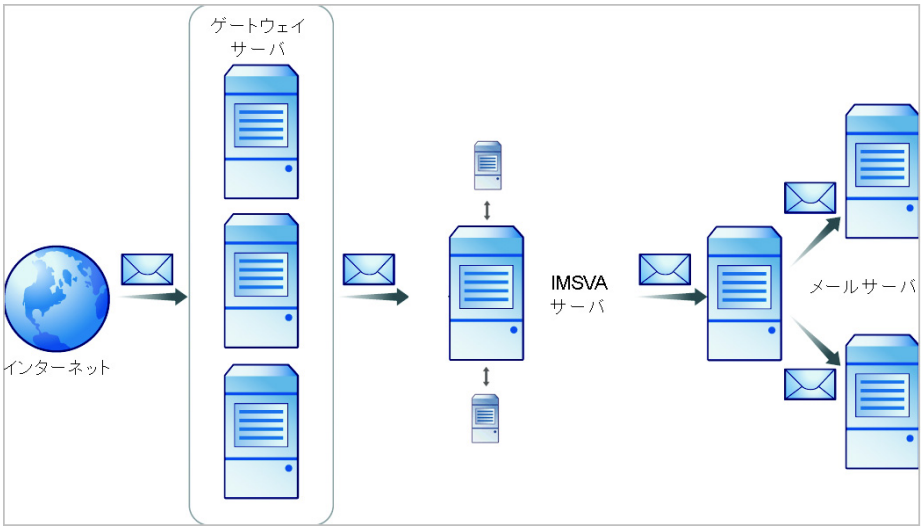


図 3-4. ゲートウェイの内側に IMSVA グループを配置する場合

ファイアウォールなしで配置する

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

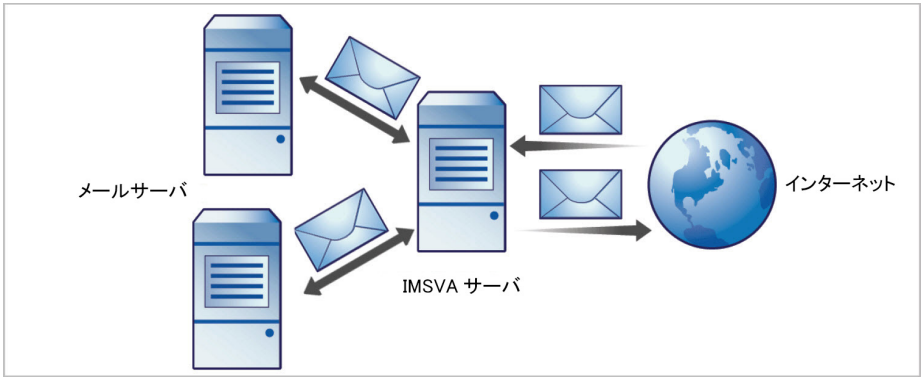


図 3-5. インストールトポロジ: ファイアウォールなし

注意

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

ファイアウォールの外側にインストールする

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

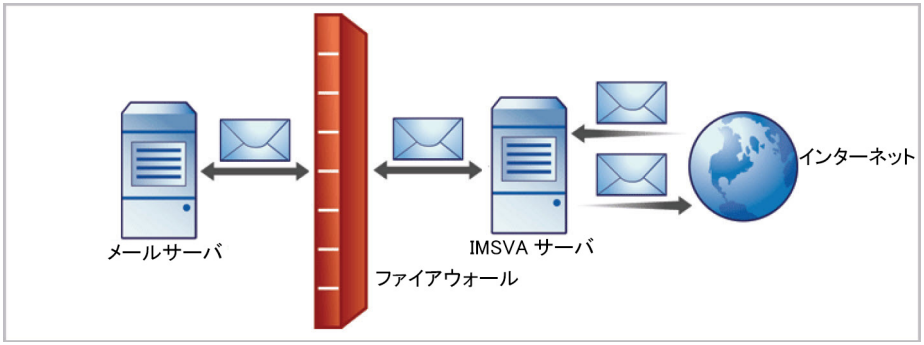


図 3-6. インストールトポロジ: ファイアウォールの外側

受信トラフィック

- SMTP サーバを参照するように IMSVA を設定し、IMSVA サーバからの受信トラフィックを許可するようにファイアウォールを設定します。
- ローカルドメインへのリレーのみを許可するように、[リレー管理] を設定します。

送信トラフィック

- すべての送信メッセージが IMSVA にルーティングされるようにファイアウォール (プロキシベース) を設定します。
- 内部の SMTP ゲートウェイが IMSVA を使用して任意のドメインにリレーできるように、IMSVA を設定します。

ヒント

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

ファイアウォールの内側へインストールする

次の図は、ファイアウォールの内側への IMSVA の配置方法を示します。

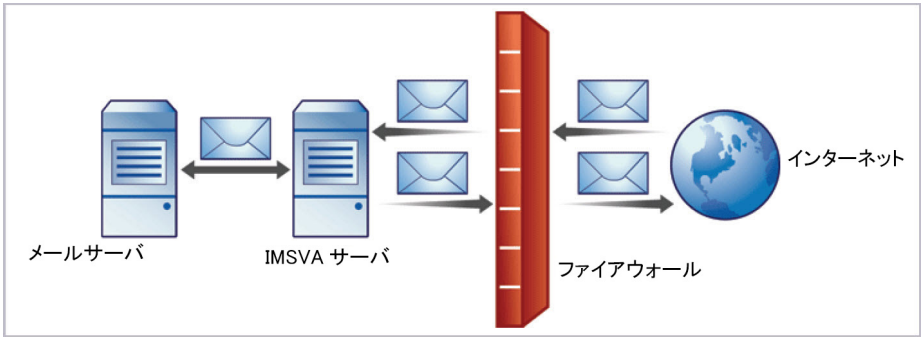


図 3-7. インストールシナリオ: ファイアウォールの内側

受信トラフィック

- プロキシベースのファイアウォールを設定して、SMTP メールが次のように転送されるようにします。
  - 受信 SMTP メッセージは IMSVA に送られ、次にドメイン内の SMTP サーバに転送されます。
- ローカルドメイン向けのメッセージが SMTP ゲートウェイまたは内部のメールサーバにルーティングされるように IMSVA を設定します。
- ローカルドメインへのリレーのみが許可されるようにリレー制限を設定します。

送信トラフィック

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

- 内部の SMTP ゲートウェイが IMSVA を使用して任意のドメインにリレーできるように、IMSVA を設定します。

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

DMZ (非武装地帯) 内へインストールする

IMSVA は DMZ (非武装地帯) にインストールすることもできます。

受信トラフィック

- パケットベースのファイアウォールを設定します。
- ローカルドメイン向けのメールメッセージが SMTP ゲートウェイまたは内部のメールサーバにルーティングされるように IMSVA を設定します。

送信トラフィック

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

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

デバイスの役割について

IMSVA は、上位デバイスまたは下位デバイスとして機能させることができます。単一の上位デバイスと複数の下位デバイスが、1 つのグループを構成しま

す。このグループでは、上位デバイスに登録された下位デバイスに対して、上位デバイスが中央管理サービスを提供します。

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

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

デバイスサービスについて

IMSVA デバイスでは、さまざまな種類のサービスを有効にできます。

上位のみのサービス:

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

上位および下位のサービス:

- ポリシーサービス: 設定するルールを管理します。
- 検索サービス: メールトラフィックを検索します。
- エンドユーザメール隔離サービス: エンドユーザメール隔離を管理します。これによって、IMSVA がスパムメールと判定したメールメッセージを表示することができます。
- コマンドラインインタフェース (CLI) サービス: CLI 機能へのアクセスを提供します。

下位デバイスは、上位デバイスに登録されている場合にのみ機能します。

サービスの選択

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

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

上記の SMTP 検索シナリオ以外に、IMSVA で POP3 トラフィックを検索する場合もあります。詳細については、45 ページの「POP3 メール検索を理解する」を参照してください。

送信者フィルタを使用して配置する

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

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

内部通信ポートについて

IMSVA では、複数のネットワークインタフェースをサポートします。つまり、1 つの IMSVA デバイスに複数の IP アドレスがある場合もあります。この場合、デバイスが一意の IP アドレスを使用して通信しようとすると問題が発生します。IMSVA では、内部通信ポートと組み合わせて使用することにより、この問題を解決します。

- インストール時に、IMSVA デバイスを識別するために、1 つのネットワークインタフェースカード (NIC) を内部通信ポートとして指定する必要があります。
- インストール後も、設定ウィザードまたはコマンドラインインタフェース (CLI) を使用して、IMSVA の管理コンソール上で内部通信ポートを変更することができます。

- グループシナリオの場合、上位デバイスと下位デバイスが相互通信するには、それぞれの内部通信ポートを使用する必要があります。下位デバイスを上位デバイスに登録する際、上位デバイスの内部通信ポートの IP アドレスを指定する必要があります。

ヒント

上位と下位の通信に内部通信ポートが使用されるように、グループの各 IMSVA デバイスにホストルートエントリを設定することをお勧めします。

- IMSVA デバイスでは、内部通信ポートの IP アドレスを使用して、Control Manager サーバに登録します。Control Manager 管理コンソールから IMSVA デバイスを設定する場合は、内部通信ポート上の管理コンソールサービスを有効にする必要があります。初期設定では、管理コンソールサービスは全ポート上で有効になっています。

POP3 メール検索を理解する

SMTP トラフィックの他に、IMSVA では、クライアントがメッセージを受信する際に、ゲートウェイで POP3 メッセージも検索できます。会社で POP3 メールを使用していない場合でも、従業員が、個人的な Web ベースの POP3 メールアカウントにアクセスする場合があります。これらのアカウントからのメッセージが検索されない場合、これが、ネットワーク上の脆弱なポイントになる可能性があります。

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

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

POP3 トラフィックを検索するには、IMSVA サーバ POP3 プロキシに接続するようにメールクライアントを設定します。これにより、POP3 サーバに接続し、メッセージを受信して検索します。

POP3 検索の要件

IMSVA で POP3 トラフィックを検索するには、ネットワーク上にファイアウォールをインストールして、IMSVA を除くすべてのコンピュータからの POP3 要求をブロックするように設定する必要があります。このように設定すると、すべての POP3 トラフィックがファイアウォールを通過して IMSVA に到達し、IMSVA のみで POP3 トラフィックが検索されるようになります。

注意

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

IMSVA を経由してメールを受信する POP3 クライアントを設定する

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

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

  例: user#10.18.125.168

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

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

  例: user

IMSVA の管理コンソールを開く

IMSVA の管理コンソールは、プログラムが配信されているサーバから、またはネットワークを介してリモートで、Web ブラウザに表示できます。

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

https://{IMSS}:8445

{IMSS} は、IP アドレスまたは完全修飾ドメイン名です。

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

IP アドレスを使用する代わりに、サーバの完全修飾ドメイン名 (FQDN) を使用することもできます。SSL を使用して管理コンソールを表示するには、ドメイン名の前に「https://」を付け、その後にポート番号を付けます。

初期設定のログオンアカウント情報は次のとおりです。

- 管理者のユーザ名: admin
- パスワード: imss9.1

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

警告!

ポリシーが不正改ざんされないよう、配置が終了したら、ただちに新しいログオンパスワードを設定して、定期的にパスワードを変更することをお勧めします。

注意

Internet Explorer (IE) を使用して管理コンソールにアクセスする場合、IE ではアクセスがブロックされ、別の Web アドレスから証明書が発行されたことを示すポップアップダイアログが表示されます。このメッセージは無視して、[このサイトの閲覧を続行する] をクリックし、作業を続けてください。

第 4 章

IMSVA9.1 SP1 のインストール

この章では、さまざまな条件の下で IMSVA 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

システム要件については、次の Web サイトを参照してください。

https://success.trendmicro.com/dcx/s/solution/000296766?language=ja

IMSVA をインストールする

IMSVA 9.1 では、IMSVA 9.0 からのアップグレードのみをサポートし、アップグレード時に既存の設定とポリシーが移行されます。

IMSVA のインストール処理では、既存のシステムがフォーマットされ、IMSVA がインストールされます。インストールの手順は、基本的にはベアメタルと VMware ESX 仮想マシンプラットフォームで同一です。ベアメタルのインストールでは、IMSVA インストール DVD を起動するとインストール手順が開始します。VMware のインストールでは、仮想マシンを作成してからインストールする必要があります。

警告!

インストール処理の間、既存のデータやパーティションは削除されます。システムで既存のデータが存在する場合は、バックアップしてから IMSVA をインストールしてください。

手順

1. IMSVA のインストールを開始します。

   システム要件については、50 ページの「システム要件」を参照してください。

   - ベアメタルサーバの場合

     a. ベアメタルサーバが CentOS 6.4 x86_64 をサポートしていることを確認します。

     b. IMSVA インストール DVD を目的のサーバの DVD ドライブに挿入します。

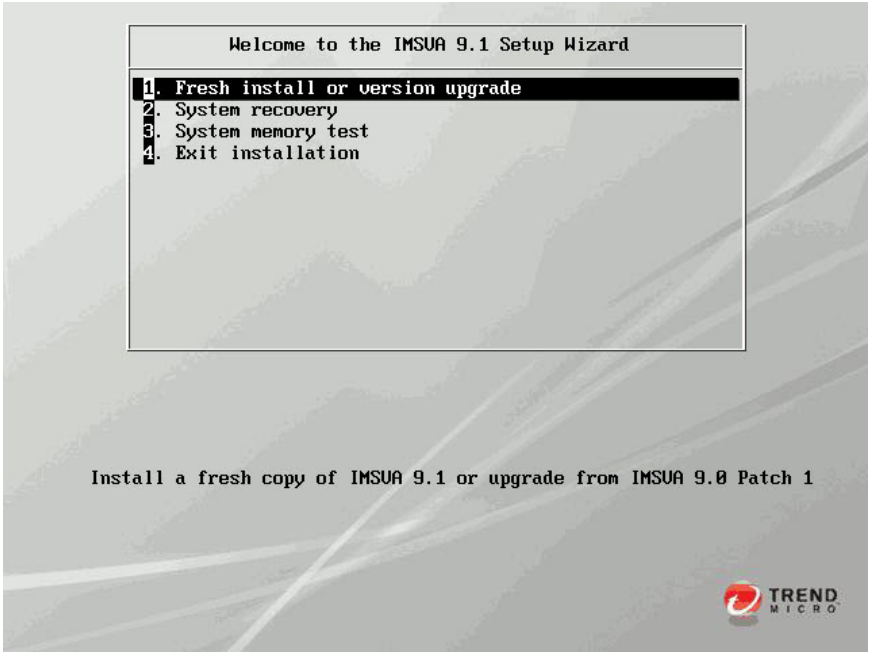
     c. ベアメタルサーバの電源をオンにします。

- VMware ESX 仮想マシンの場合
  a. VMware ESX サーバ上に仮想マシンを作成します。
  b. 仮想マシンを起動します。
  c. IMSVA インストール DVD を、次のいずれかの方法で仮想 DVD ドライブに挿入します。
     - IMSVA インストール DVD を ESX サーバの物理 DVD ドライブに挿入します。そして、仮想マシンの仮想 DVD ドライブを物理 DVD ドライブに接続します。
     - 仮想マシンの仮想 DVD ドライブを `IMSVA-9.1-xxxx-x86_64.iso` ファイルに接続します。`IMSVA-9.1-xxxx-x86_64.iso` ファイルは、次の場所で入手できます。

       http://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp
  d. VMware 管理コンソールで [仮想マシン] > [Ctrl+Alt+Del の送信] の順にクリックして、仮想マシンを再起動します。

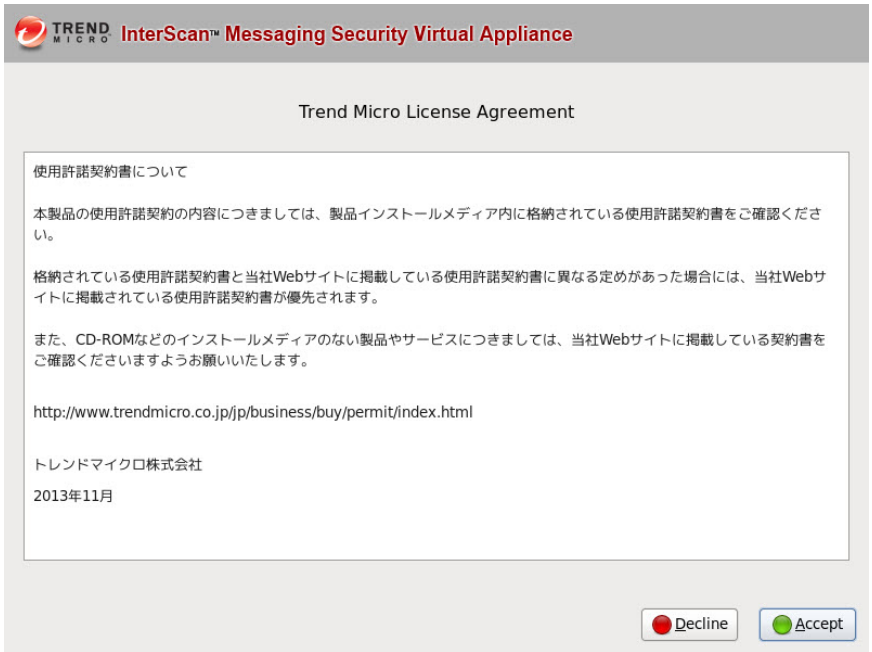
画面には次のオプションのある [IMSVA 9.1 Setup Wizard] が表示されます。

- Fresh install or version upgrade: 新しいハードウェアまたは仮想マシンに IMSVA をインストールする場合、あるいは既存の IMSVA をアップグレードする場合、このオプションを選択します。
- System recovery: OS エラーを修復して管理パスワードを復旧する場合、このオプションを選択します。
- System memory test: メモリ診断テストを実行する場合、このオプションを選択します。
- Exit installation: インストール処理を終了してローカルディスクから起動する場合、このオプションを選択します。



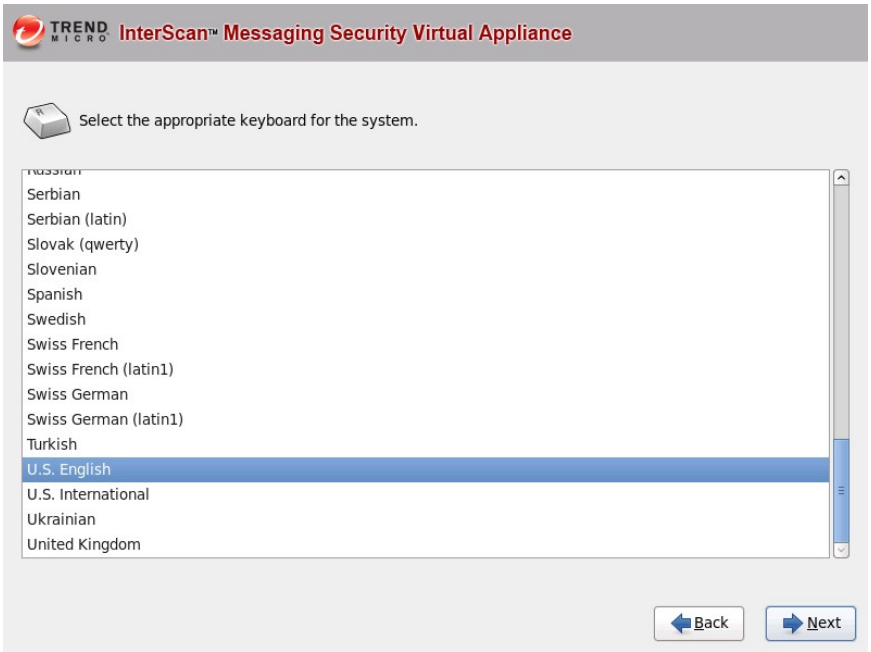
2. [Fresh install or version upgrade] を選択します。

使用許諾契約書の同意に関する画面が表示されます。



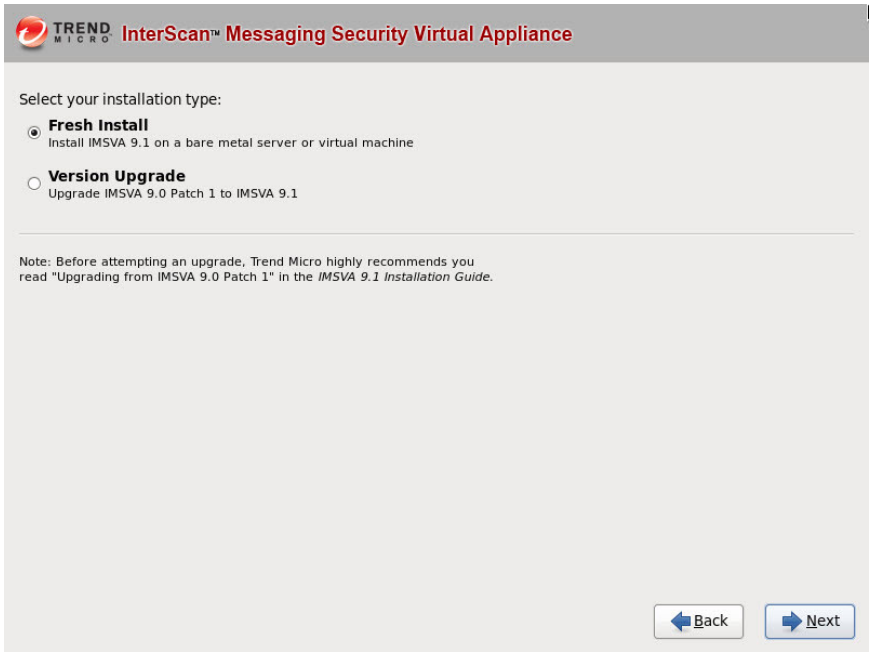
3. 使用許諾契約書の内容に同意できる場合は [Accept] をクリックして続行します。

キーボードの言語を選択する画面が表示されます。



4. システムのキーボード言語を選択して、[Next] をクリックします。

インストールのタイプを選択する画面が表示されます。



5. [Fresh Install] を選択して、[Next] をクリックします。

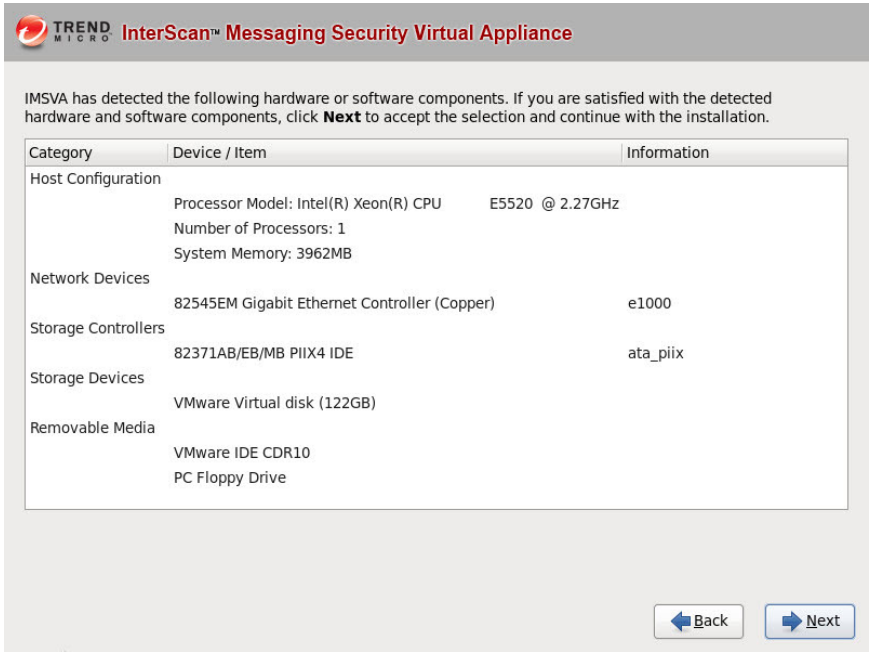
インストールに使用するドライブを選択するための画面が表示されます。

6. ドライブを選択して、[Next] をクリックします。

   警告画面が表示されます。

7. 確認して [Yes] をクリックします。

   IMSVA インストールプログラムがハードウェアとソフトウェアを検索し、最小要件が満たされているかどうかを調べて結果を表示します。最小要件に適合しないコンポーネントがハードウェアまたはソフトウェアに存在する場合、適合しないコンポーネントがインストールプログラムにより強調表示され、インストールは停止します。



8. ハードウェアおよびソフトウェアの情報が正しいことを確認して、[Next] をクリックします。

ネットワークデバイスの設定画面が表示されます。

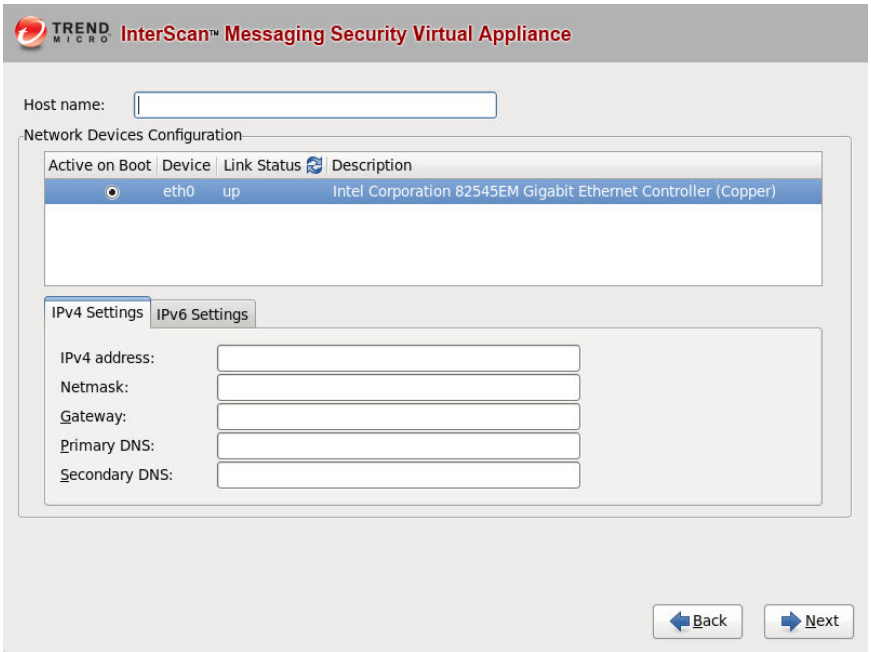


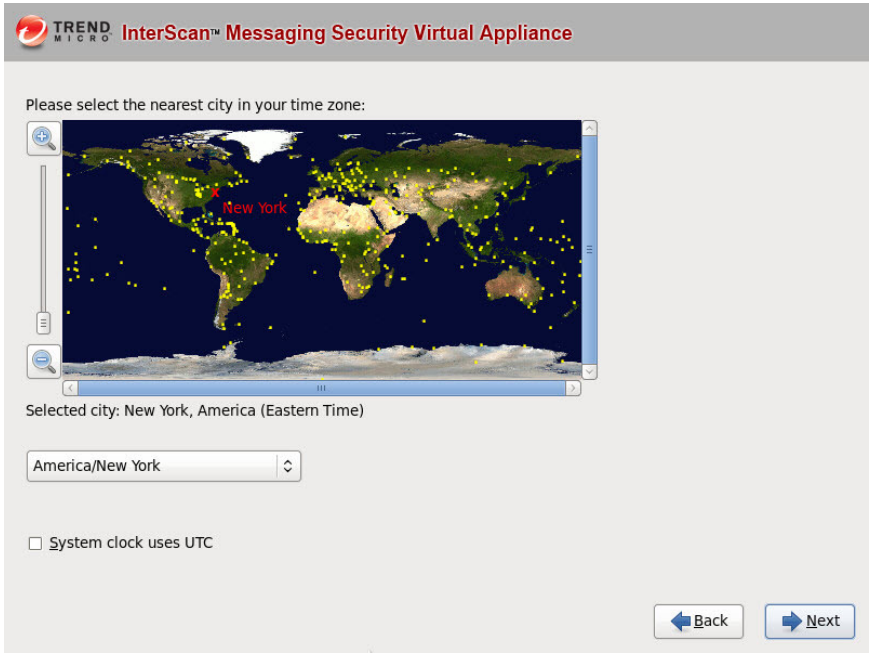
表 4-1. ネットワークデバイスの設定

設定パラメータ	説明
Host name	この IMSVA ホストで適切な FQDN を入力します。
IPv4 address	IMSVA 管理インタフェースの IP アドレスを入力します。
Netmask	指定した IPv4 アドレスのサブネットマスクを入力します。
Gateway	適切な IP アドレスを入力して、この IMSVA のインストールに対するゲートウェイとして使用します。

設定パラメータ	説明
Primary DNS	適切な IP アドレスを入力して、この IMSVA のインストールに対するプライマリ DNS サーバとして使用します。
Secondary DNS	適切な IP アドレスを入力して、この IMSVA のインストールに対するセカンダリ DNS サーバとして使用します。

9. IMSVA をインストールするのに必要なすべての情報を入力して [Next] をクリックします。

   タイムゾーンの設定画面が表示されます。



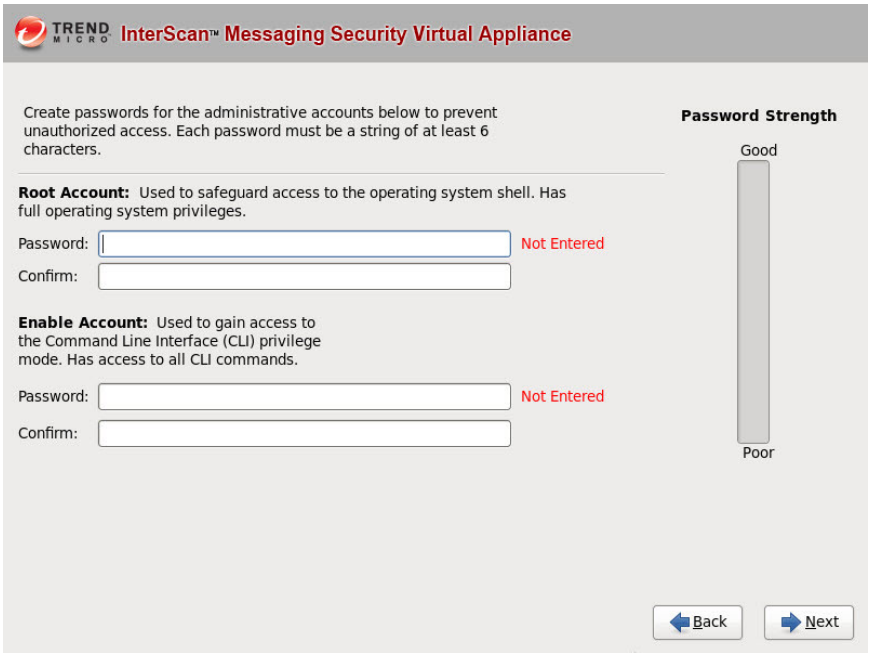
10. IMSVA サーバの時間帯と時刻を指定します。

    a. IMSVA サーバの配置場所を選択します。

b. [System clock uses UTC] チェックボックスをオンまたはオフにして、サーバのシステムクロックで UTC を使用するかどうかを指定します。

11. [Next] をクリックします。

アカウントの設定画面が表示されます。



12. [Root Account] および [Enable Account] のパスワードを指定します。

IMSVA では 2 つの異なるレベルの管理者アカウントを使用して、システムの安全を確保します。

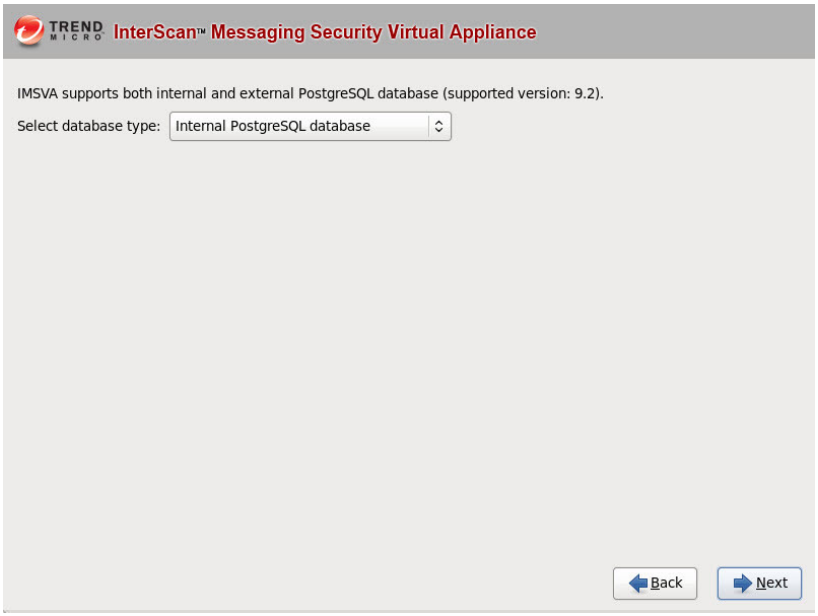
パスワードの文字数は、6～32 文字にしてください。

ヒント

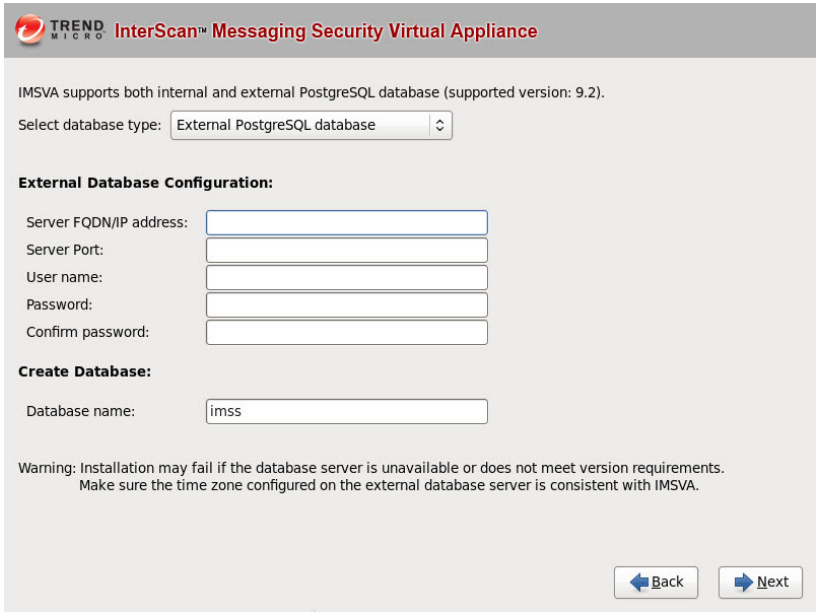
セキュリティを最大限にするために、他人には知られないように一意性の高いパスワードにしてください。英字の大文字と小文字、数字、およびキーボード上にある任意の特殊文字を使用して、パスワードを作成できます。

- Root Account: OS のシェルにアクセスする際に使用され、サーバに対するすべての権限を持っています。これは、システム上で最も強力なユーザです。
- Enable Account: コマンドラインインタフェースの特権モードにアクセスする際に使用します。このアカウントには、任意の CLI コマンドを実行するためのすべての権限があります。

13. 次のいずれかのデータベースを選択します。
    - Internal PostgreSQL database: 初期設定で使用されるデータベースです。



- External PostgreSQL database: このオプションを選択した場合は、必要に応じて外部データベース情報を提供します。



注意

外部データベースを使用するには、次の手順を実行します。

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

b. データベース接続の最大数を 600 に変更します。

```
vi /var/lib/pgsql/9.2/data/postgresql.conf
```

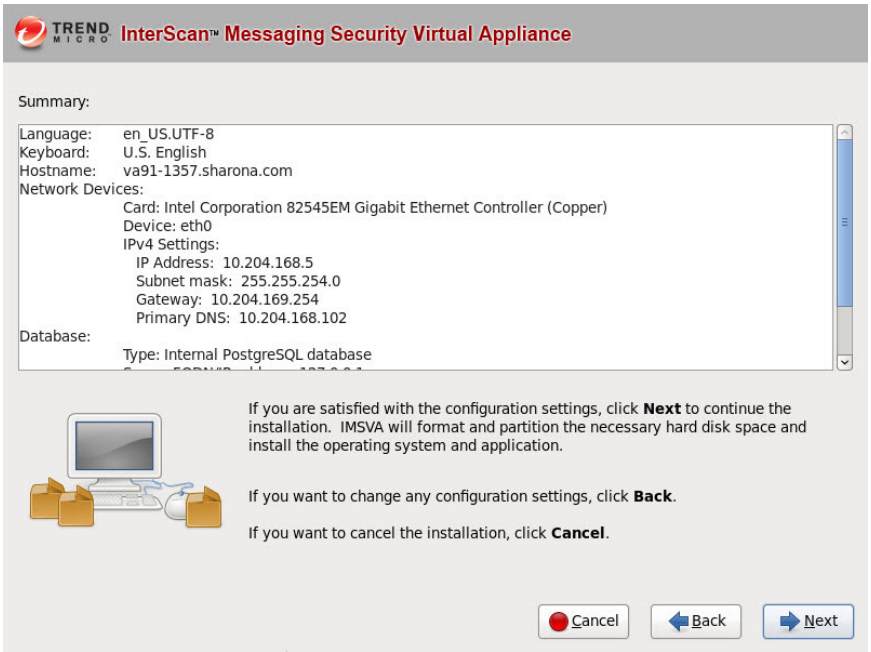
`max_connection = 600` (初期設定では `100` です)

`restart DB service` (コマンドは「`service postgresql-9.2 restart`」または「`systemctl restart postgresql`」です)

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

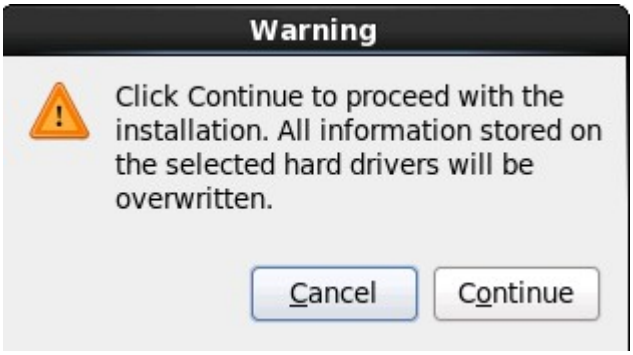
14. [Next] をクリックします。

設定の確認画面が表示されます。



15. 設定を確認して [Next] をクリックします。

    インストールの開始が確認されます。



重要

[Continue] を選択すると、ハードディスクパーティションのデータがすべて消去され、ハードディスクがフォーマットされます。保存対象データがハードディスクにある場合、インストールをキャンセルします。そしてその情報のバックアップを作成してから次に進みます。

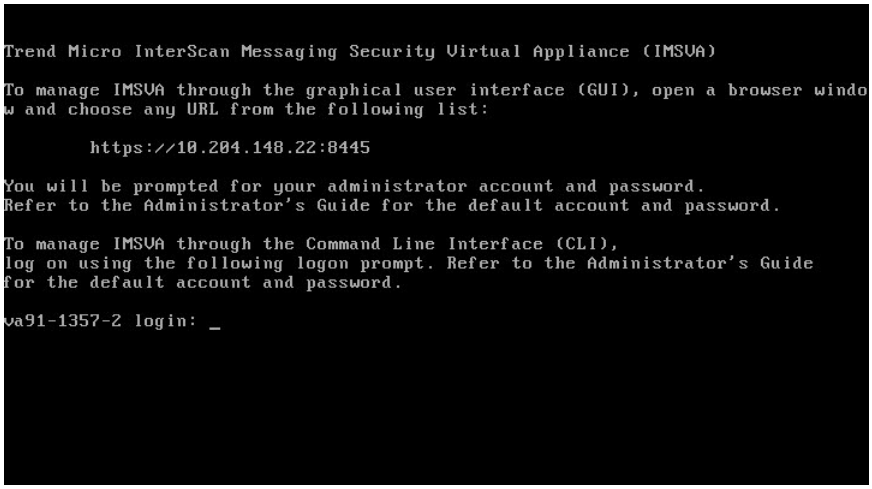
16. [Continue] をクリックします。

IMSVA のインストール先ローカルドライブのフォーマット進行状況を示す画面が表示されます。フォーマットが完了すると、IMSVA のインストールが開始されます。

インストールが完了すると、概要画面が表示されます。インストールログは、参照用に`/var/app_data/installlog` ファイルに保存されます。

17. [Restart] をクリックしてシステムを再起動します。
    - IMSVA がインストールされたら、DVD-ROM デバイスの接続を仮想マシンから切断しておくことをお勧めします。

IMSVA が再起動されると、CLI の初期ログオン画面が表示されます。



18. CLI または IMSVA 管理コンソールのいずれかにログオンし、IMSVA を起動します。

ヒント

追加の設定、トラブルシューティング、または管理作業を実行する場合は、CLI シェルにログオンします。

単一の上位デバイスを設定する

IMSVA には、IMSVA の起動と実行に必要なすべての項目を簡単に設定できる、設定ウィザードが用意されています。

手順

1. 管理コンピュータで、インストール時に設定した IMSVA の IP アドレスに ping を実行できるようにしておきます。
2. 管理コンピュータで Internet Explorer、Firefox、または Microsoft Edge を開きます。

3. 次の URL を入力します (必要に応じて、セキュリティ証明書を受け入れます)。

   `https://<IP アドレス>:8445`

   ログオン画面が表示されます。

4. [設定ウィザードを開く] チェックボックスをオンにします。

5. 次に示す初期設定のユーザ名とパスワードを入力します。

   - ユーザ名: admin
   - パスワード: imsva

   [設定ウィザード] 画面が表示されます。

図 4-1. [設定ウィザード] 画面

6. [設定ウィザード] 画面に従って、次の項目を設定します。

手順 1: システムを設定する

手順

1. 最初の画面の内容を読んでから、[次へ] をクリックします。[ローカルシステム設定] 画面が表示されます。

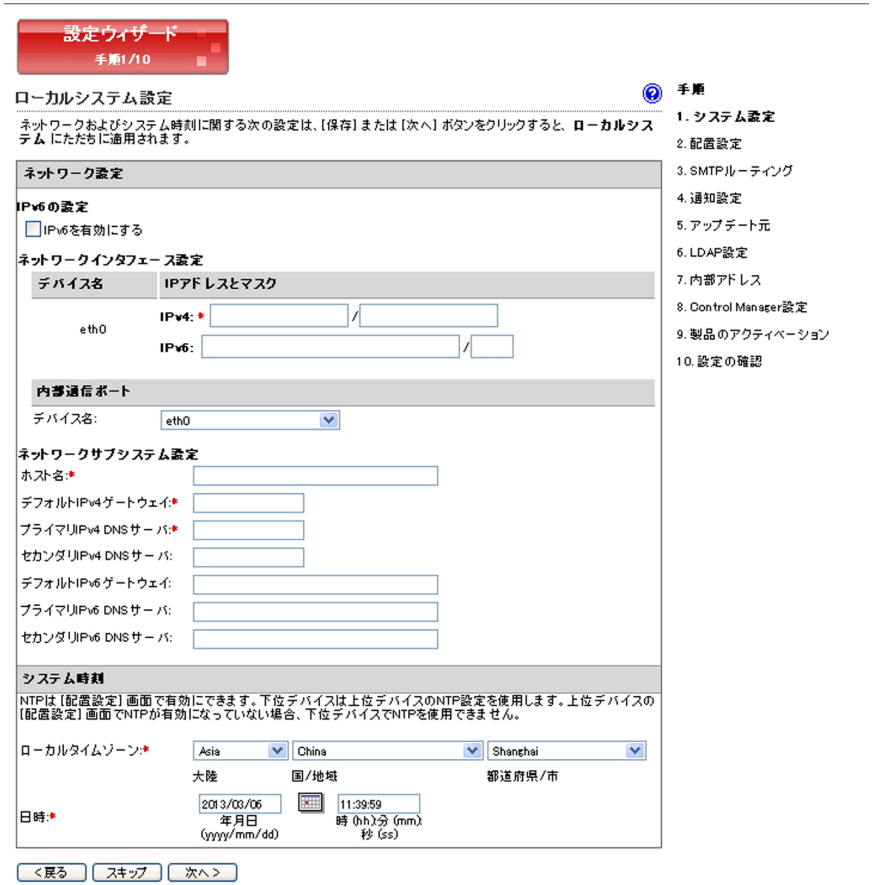


図 4-2. ローカルシステム設定

2. デバイス名、IP アドレス、およびネットマスクを必要に応じて変更します。また、ネットワークの設定およびデバイスシステム時刻の設定を行います。

注意

[次へ] ボタンをクリックすると、ただちにローカルシステム設定が有効になります。IP アドレスや時刻設定を変更した場合は、IMSVA が再起動します。IMSVA がオンライン状態になるまで待ってから、再度ログオンします。

手順 2: 配置を設定する

手順

1. [次へ] をクリックします。

   [配置設定] 画面が表示されます。

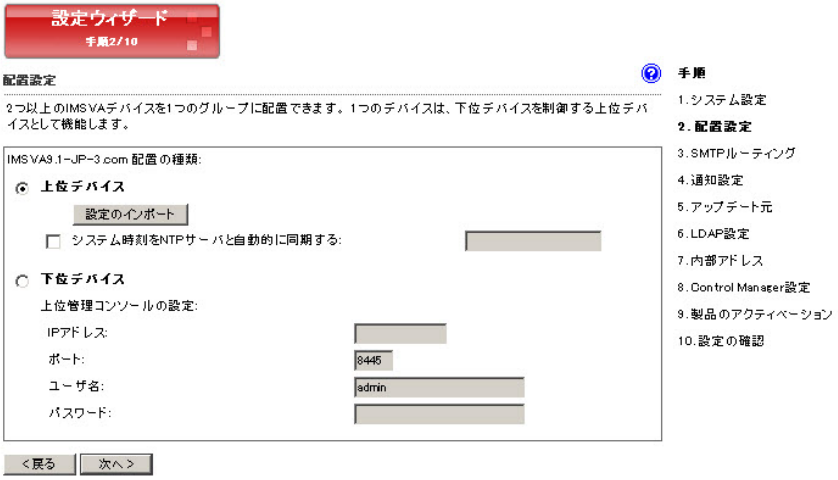


図 4-3. 配置設定

2. [上位デバイス] または [下位デバイス] を選択します。

   - [上位デバイス]: このデバイスが、設定する最初のデバイスである場合は、上位デバイスを選択します。追加する下位デバイスは、後で

設定できます。また、NTP サービスを使用するかどうかを決定します。

- [下位デバイス]: このオプションを選択する場合は、上位管理コンソールの設定を指定します。ここで使用するユーザアカウントに、フル管理者権限があることを確認してください。

手順 3: SMTP ルーティングを設定する

手順

1. [次へ] をクリックします。

[SMTP ルーティング設定] 画面が表示されます。

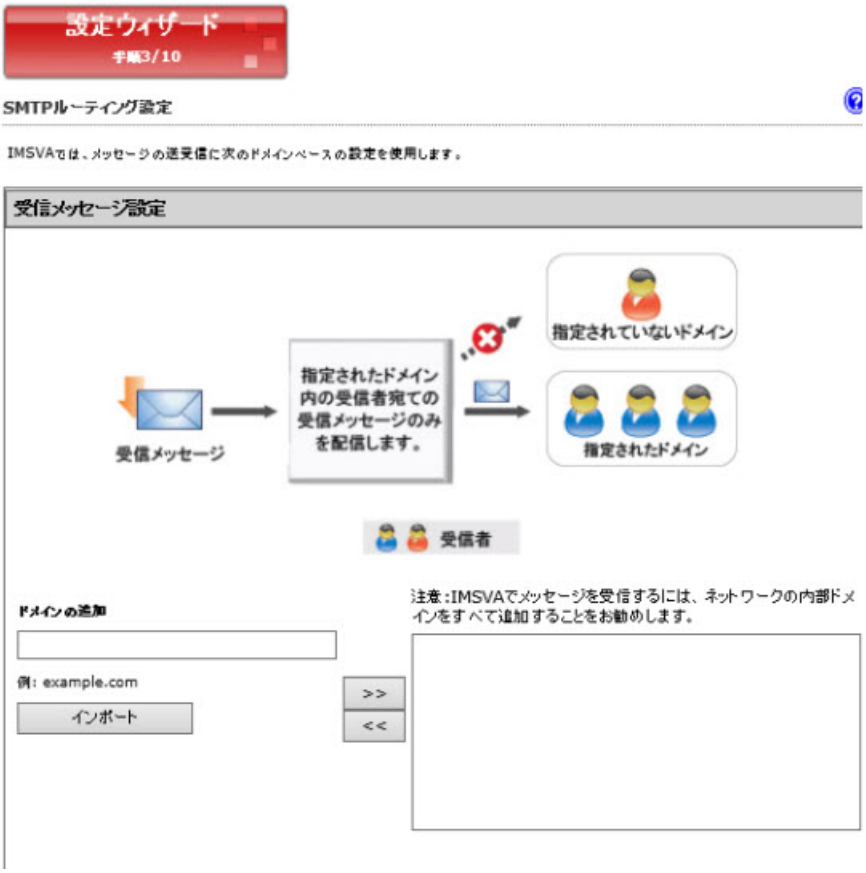
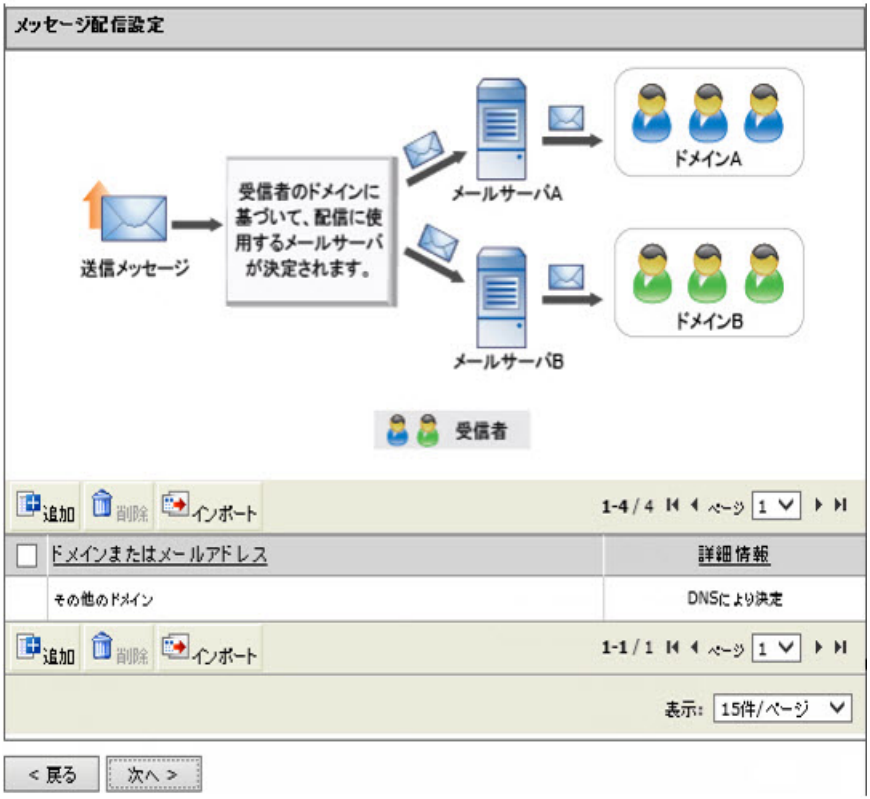


図 4-4. SMTP ルーティング設定



2. 受信メッセージ設定を指定します。
3. メッセージ配信設定を指定します。

手順 4: 通知を設定する

手順

1. [次へ] をクリックします。

[通知設定] 画面が表示されます。

図 4-5. 通知設定

2. システムおよびポリシーイベントに関する通知を受信する場合は、[メール設定] または [SNMP トラップ] の通知を設定します。

手順 5: アップデート元を設定する

手順

1. [次へ] をクリックします。

[アップデート元] 画面が表示されます。

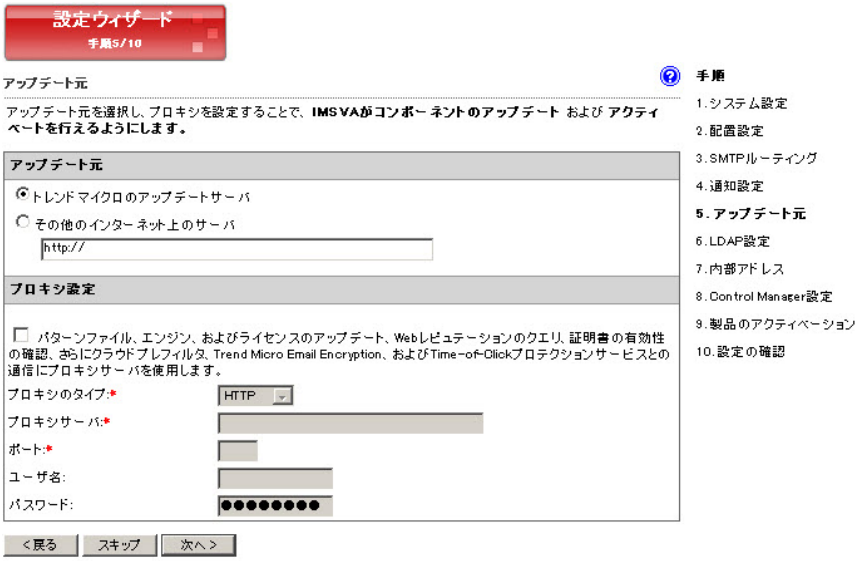


図 4-6. アップデート元

2. アップデートに関する次のオプションを設定し、IMSVA がコンポーネントアップデートをどこから受け取り、IMSVA がどのプロキシ (使用する場合) を介してインターネットにアクセスするかを指定します。

   - アップデート元: トレンドマイクロから直接アップデートを受け取る場合は、[トレンドマイクロのアップデートサーバ] をクリックします。または、[その他のインターネット上のサーバ] をクリックし、アップデート元の URL を入力します。アップデート元には、トレンドマイクロのアップデートサーバにアップデートがあるかどうか確認するサーバを指定します。必要に応じて任意のアップデート元を指定できます。また、Control Manager サーバを使用できる場合は、その URL (`http://<Control Manager サーバのアドレス>/TvcsDownload/ActiveUpdate/`) を入力することもできます。

   - プロキシ設定: [プロキシサーバは、パターンファイル、エンジン、およびライセンスのアップデート、Web レピュテーションのクエリ、クラウドプレフィルタ、さらに Trend Micro Email Encryption に使

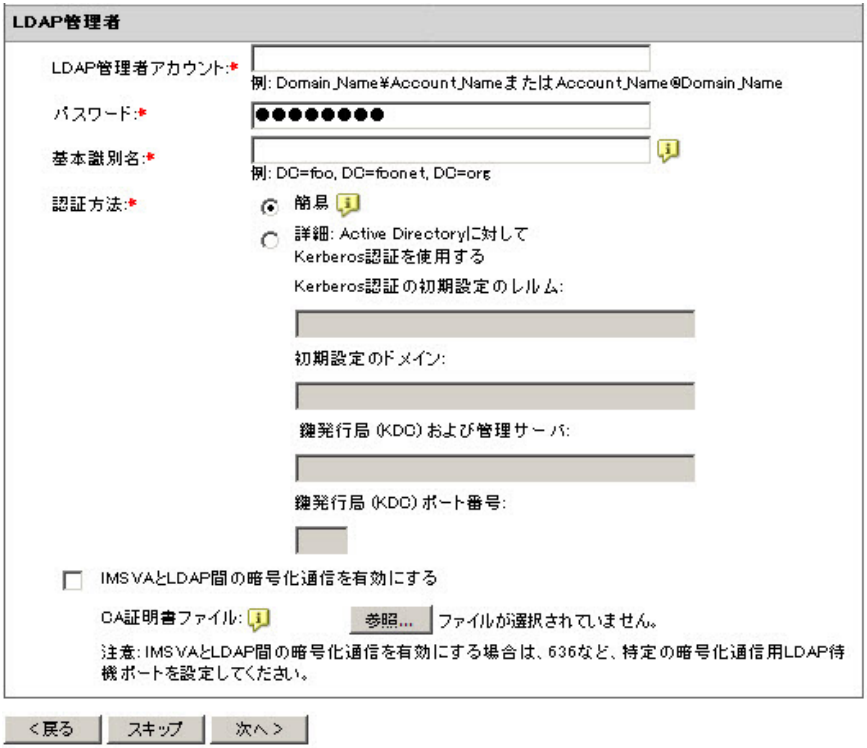
用できます。] チェックボックスをオンにして、プロキシの種類、サーバ名、ポート、ユーザ名、パスワードを設定します。

手順 6: LDAP を設定する

手順

1. [次へ] をクリックします。

   [LDAP 設定] 画面が表示されます。



2. LDAP サーバのわかりやすい説明を入力します。
3. 次の手順を実行して LDAP 設定を有効にします。
   a. [LDAP サーバの種類] で、次のいずれかを選択します。
      - Domino
      - Microsoft Active Directory
      - Microsoft Active Directory グローバルカタログ
      - OpenLDAP
      - Sun iPlanet Directory
   b. 片方または両方の LDAP サーバを有効にするには、[有効 LDAP1] または [有効 LDAP2] の横のチェックボックスをオンにします。

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

d. [ポリシーサービスおよび EUQ サービスの LDAP キャッシュ生存期限] の [キャッシュ生存期限 (分)] に、生存期限の数値を入力します。

e. [LDAP 管理者] では、管理者のアカウント、対応するパスワード、および基本識別名を入力します。LDAP サーバの種類と管理者アカウントの指定例を、次の表に示します。

表 4-2. LDAP 管理設定

LDAP サーバ	LDAP 管理者アカウント (例)	基本識別名 (例)	認証方法
Active Directory	Kerberos を使用しない場合: user1@domain.com (UPN) または domain\user1 Kerberos を使用する場合: user1@domain.com	dc=domain, dc=com	簡易 詳細 (Kerberos 使用)
Active Directory グローバルカタログ	Kerberos を使用しない場合: user1@domain.com (UPN) または domain\user1 Kerberos を使用する場合: user1@domain.com	dc=domain, dc=com dc=domain1,dc=com (一意のドメインが複数存在する場合)	簡易 詳細 (Kerberos 使用)
Lotus Domino	cn=manager, dc=test1, dc=com	dc=test1, dc=com	簡易
Lotus Domino	user1/domain	該当なし	簡易
Sun iPlanet Directory	uid=user1, ou=people, dc=domain, dc=com	dc=domain, dc=com	簡易
Open LDAP	cn=manager, dc=test1, dc=com	dc=test1, dc=com	簡易

f. [認証方法] では、[簡易] 認証または [詳細] 認証を選択します。Active Directory の [詳細] 認証を選択した場合は、Kerberos 認証の初期設定のレルム、初期設定のドメイン、KDC と管理サーバ、および KDC ポート番号を設定します。

注意

LDAP 設定は、LDAP をユーザグループの定義、管理者権限、またはエンドユーザメール隔離の認証に使用する場合のみ指定します。

g. [IMSVA と LDAP 間の暗号化通信を有効にする] チェックボックスをオンにし、[参照] をクリックして CA 証明書ファイルをアップロードします。

手順 7: 内部アドレスを設定する

手順

1. [次へ] をクリックします。

[内部アドレス] 画面が表示されます。

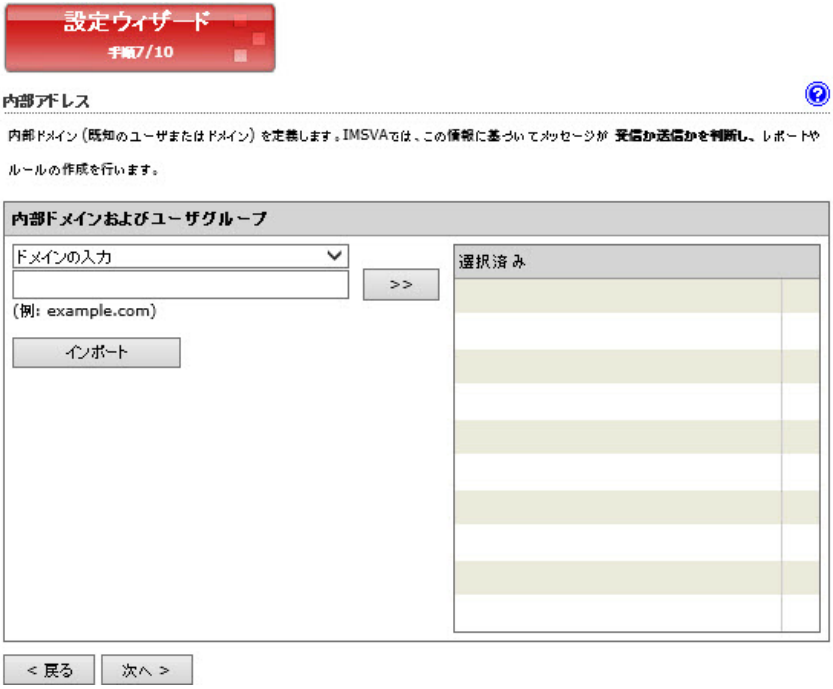


図 4-7. 内部アドレス

2. IMSVA では、内部アドレスに登録された情報を使用して、ポリシーまたはイベントが受信用であるか、または送信用であるかを判断します。

   - 送信メッセージのルールを設定している場合、内部アドレスのリストは送信者に適用されます。
   - 受信メッセージのルールを設定している場合、内部アドレスのリストは受信者に適用されます。

   内部ドメインおよびユーザグループを定義するには、次の手順を実行します。

   - ドロップダウンリストから [ドメインの入力] を選択してテキストボックスにドメインを入力し、[>>] をクリックします。

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

手順 8: Control Manager サーバを設定する

手順

1. [次へ] をクリックします。

[Control Manager サーバの設定] 画面が表示されます。

図 4-8. Control Manager サーバの設定

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

   a. [MCP エージェントを有効にする] を選択します (MCP エージェントは、初期設定で IMSVA に含まれています)。

   b. [サーバ] に Control Manager の IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。

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

d. Web サーバで認証が必要な場合は、[Web サーバ認証] でユーザ名およびパスワードを入力します。

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

f. プロキシサーバのポート番号、ユーザ名、およびパスワードを入力します。

手順 9: 製品をアクティベートする

手順

1. [次へ] をクリックします。

   [製品のアクティベーション] 画面が表示されます。

図 4-9. 製品のアクティベーション

2. 製品またはサービスのアクティベーションコードを入力します。

手順 10: 設定を確認する

手順

1. [次へ] をクリックします。

   [設定の確認] 画面が表示されます。

図 4-10. 設定の確認

2. 設定が正しい場合は、[完了] をクリックします。

   設定の変更が必要な場合は、[戻る] をクリックして該当する手順まで戻り、設定を完了します。[完了] をクリックしてウィザードを終了した後、IMSVA が使用可能になります。

下位デバイスを設定する

この項では、下位デバイスを設定して、上位デバイスに登録する方法について説明します。

手順

1. 下位デバイスの IP アドレスを決定します。
2. 上位デバイス上で次のことを実行します。
   a. 上位デバイスを設定したら (67 ページの「単一の上位デバイスを設定する」を参照)、その上位デバイスが使用可能であることを確認します。
   b. 管理コンソールにログオンします。上位デバイスの管理コンソールにログオンしていることを確認します。
   c. [管理] > [IMSVA 設定] > [接続] > [下位 IP アドレス] の順に選択します。
   d. [IP アドレスの追加] で、下位デバイスの内部通信ポート用の IP アドレスを追加します。
3. 下位デバイス上で次のことを実行します。
   a. 上位デバイスの場合と同様の手順で管理コンソールにログオンします。すべての IMSVA デバイスに、同一の初期設定の管理コンソールログオンアカウント情報を設定します。
   b. 設定ウィザードで、ローカルシステム設定を行い、[次へ] をクリックします。
   c. [配置設定] 画面で、[下位デバイス] を選択し、上位デバイスの管理コンソールの IP アドレス、ポート、ログオンユーザ名、およびパスワードを指定します。

注意

指定するログオンユーザアカウントにはフル管理者権限が必要です。

下位デバイスと上位デバイスが同じサブネットに属していないとインストールは失敗します。上位デバイスの PostgreSQL 設定ファイル (`/var/imss/pgdata/pg_hba.conf`) を変更して、下位デバイスから上位デバイスのデータベースに接続できるようにします。

d. [完了] をクリックします。

4. 上位デバイス上で次のことを実行します。

   a. [システムステータス] に移動します。

   b. [管理下のサービス] に下位デバイスが表示され、[接続] の下に緑のチェックマークが表示されていることを確認します。検索サービス、ポリシーサービス、またはエンドユーザメール隔離サービスを、開始または停止できます。

   注意

   エンドユーザメール隔離を上位で有効にした場合、下位でも有効になります。

5. 下位デバイスでエンドユーザメール隔離を使用する場合は、エンドユーザメール隔離データベース全体にデータを再配布します。

   a. 上位デバイスで、[管理] > [エンドユーザメール隔離] の順に選択します。

      [エンドユーザメール隔離管理] タブが初期設定で表示されます。

   b. [すべて (承認済み送信者リストとスパムメール情報) を再配布] または [承認済み送信者リストのみを再配布] を選択します。[すべて (承認済み送信者リストとスパムメール情報) に再配布] を選択することをお勧めします。

   c. [再配布] をクリックします。

注意

エンドユーザメール隔離が有効な下位デバイスをその上位デバイスに登録し、承認済み送信者リストに送信者を追加してから、エンドユーザメール隔離データを再配布すると、新規に追加した承認済み送信者の一部が表示されない場合があります。

次の方法で対処することをお勧めします。

- エンドユーザメール隔離を再配布した後、管理者は、新規に追加された承認済みの送信者が引き続き使用可能であることを確認するように、すべてのエンドユーザに通知します。
- 管理者は、下位デバイスを追加して、エンドユーザメール隔離を再配布したときに、エンドユーザメール隔離の承認済み送信者リストを追加しないように、すべてのエンドユーザに通知します。

配置の成功を確認する

IMSVA デバイスのセットアップが完了したら、サービスが自動的に開始されます。

手順

1. [システムステータス] に移動します。
2. [管理下のサービス] で、検索およびポリシーサービスが有効になっていることを確認します。有効でない場合は、[開始] ボタンをクリックして、それらのサービスを有効にします。

注意

エンドユーザメール隔離サービスは、任意で有効または無効に設定できます。

第 5 章

以前のバージョンからのアップグレード

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

この章の内容は次のとおりです。

体験版からアップグレードする

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

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

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

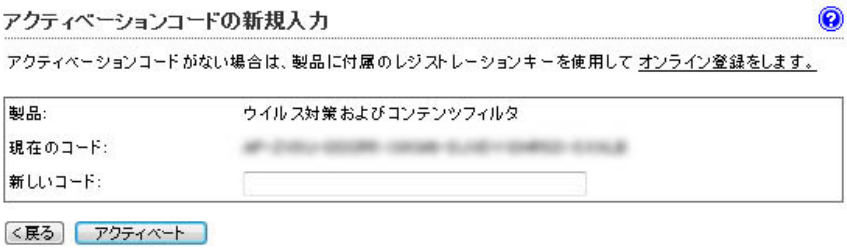
手順

1. [管理] > [製品ライセンス] の順に選択します。

[製品ライセンス] 画面が表示されます。

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

[アクティベーションコードの新規入力] 画面が表示されます。



3. 表示されたボックスに新しいアクティベーションコードを入力します。

注意

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

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

IMSVA 9.0 の Patch からアップグレードする

このアップグレードプロセスは、IMSVA 9.0 Patch 1 と Patch 2 の両方に適用されます。

以下の各項では、IMSVA を 9.1 にアップグレードする方法を説明する例として IMSVA 9.0 Patch 1 を使用しています。IMSVA 9.0 Patch 2 を 9.1 にアップグレードする場合も、以下の各項を参照してください。

IMSVA 9.0 Patch 1 または Patch 2 を単一デバイスとしてアップグレードするか、分散環境全体をアップグレードします。

注意

アップグレードプロセスが完了するまで、IMSVA は再起動しないでください。

アップグレード時は、ホスト、ネットワーク、およびゲートウェイの設定を除くカスタマイズされたシステム設定は移行されません。元の設定を保持するには、次の手順を実行します。

1. 元のルートパーティションを、アップグレードされたサーバのパスにマウントします。たとえば、`/root/original_root` の場合は次のように指定します。

   ```
   mount /dev/mapper/IMSVA-Root1 /root/original_root
   ```

2. マウントされたパスで元の設定を見つけます。
3. 元の設定をアップグレードされたサーバに追加します。

IMSVA 9.0 Patch 1 をバックアップする

IMSVA 9.0 Patch 1 は、設定をバックアップし、アップグレードに成功しなかった場合には自動的にロールバックを実行します。ただし、IMSVA 9.1 へのアップグレードを開始する前に、IMSVA 9.0 Patch 1 をバックアップしておくことをお勧めします。

手順

1. 次のいずれかのタスクを実行して、IMSVA 9.0 Patch 1 をバックアップします。
   - IMSVA 9.0 Patch 1 がインストールされているコンピュータ全体をゴースト化します。
   - 仮想マシンに IMSVA 9.0 Patch 1 がインストールされている場合はスナップショットを取ります。
   - IMSVA 9.0 Patch 1 app_data パーティションをバックアップします。
     a. OS のシェルコンソールを開いて、次のコマンドを実行します。

     ```
     /opt/trend/imss/script/imssctl.sh stop
     service crond stop
     ```

b. 外部ディスクを/var/udisk にマウントします。

c. すべてのファイルをディスクにコピーします。

```
cp -rf --preserve /var/app_data/* /var/udisk/
app_data_backup/
```

2. バックアップ後、すべての IMSVA サービスを起動します。

単一の IMSVA をアップグレードする

この手順では、単一の IMSVA をバージョン 9.1 にアップグレードします。

手順

1. IMSVA 9.0 Patch 1 をバックアップします。

   注意

   詳細については、93 ページの「IMSVA 9.0 Patch 1 をバックアップする」を参照してください。

2. CLI コンソールで次のコマンドを使用して、Postfix キューにメッセージがないことを確認します。

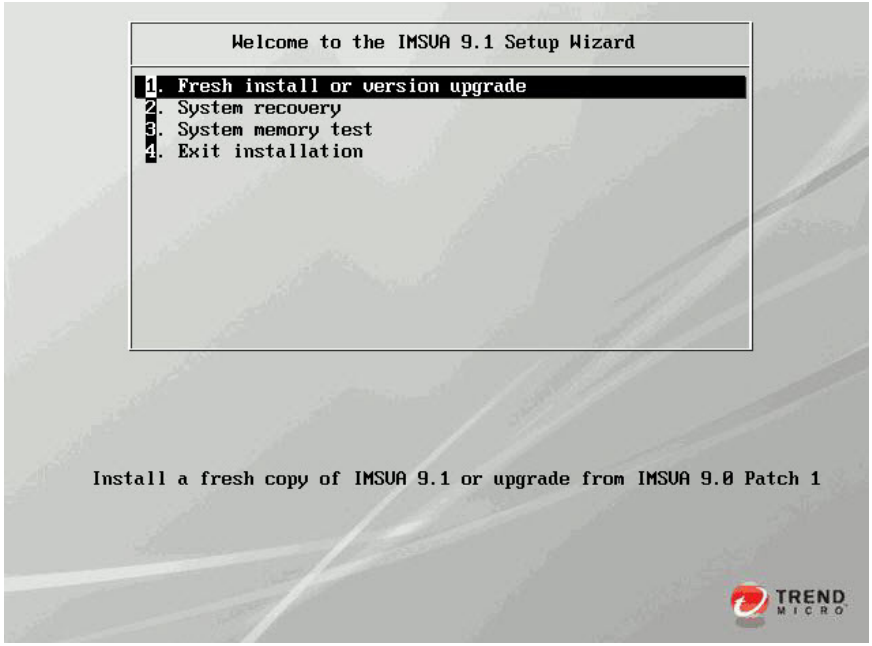
   ```
   postqueue -p
   ```

3. IMSVA インストール DVD を使用してアップグレードするサーバを再起動します。

   注意

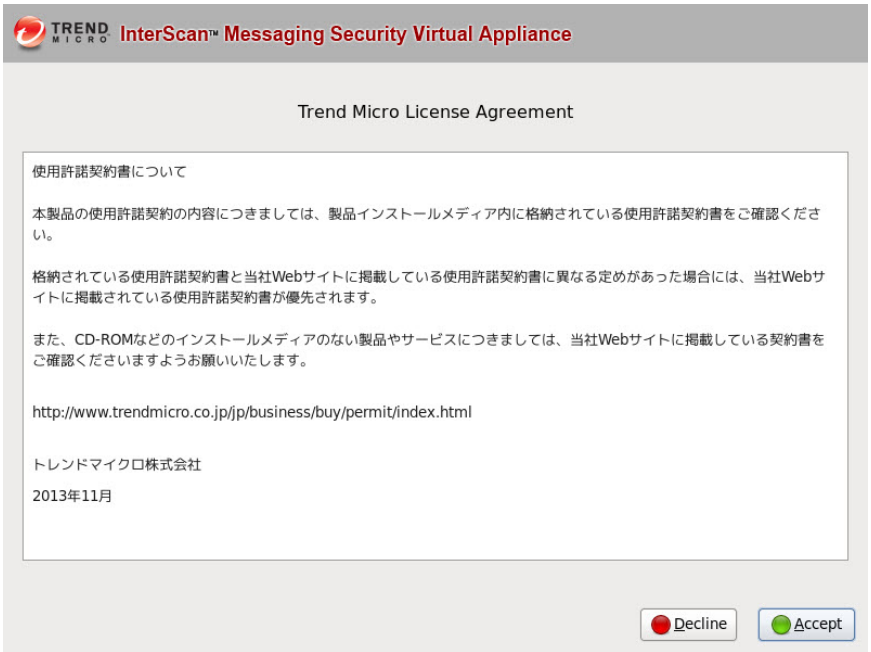
   詳細については、50 ページの「IMSVA をインストールする」の手順 1 を参照してください。

[IMSVA 9.1 Setup Wizard] 画面が表示されます。



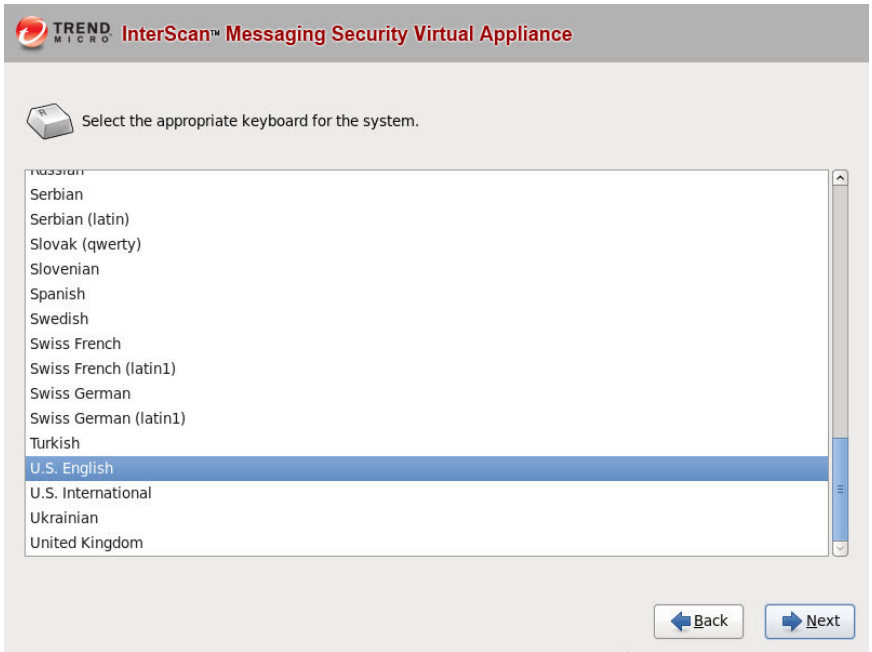
4. [Fresh install or version upgrade] を選択します。

使用許諾契約書の同意に関する画面が表示されます。



5. 使用許諾契約書の内容に同意できる場合は [Accept] をクリックして続行します。

キーボードの言語を選択する画面が表示されます。

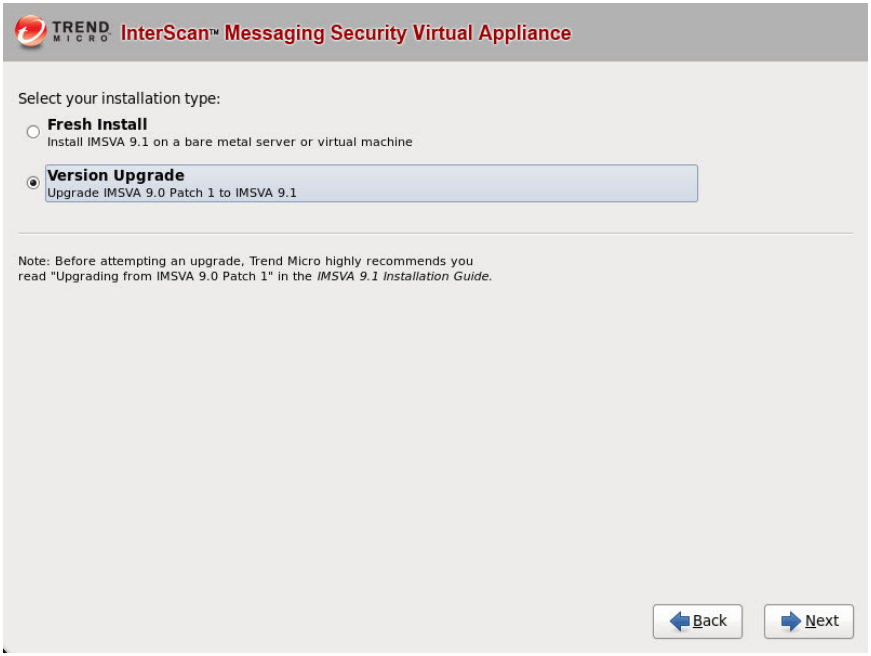


6. システムのキーボード言語を選択して、[Next] をクリックします。

   インストールのタイプを選択する画面が表示されます。

注意

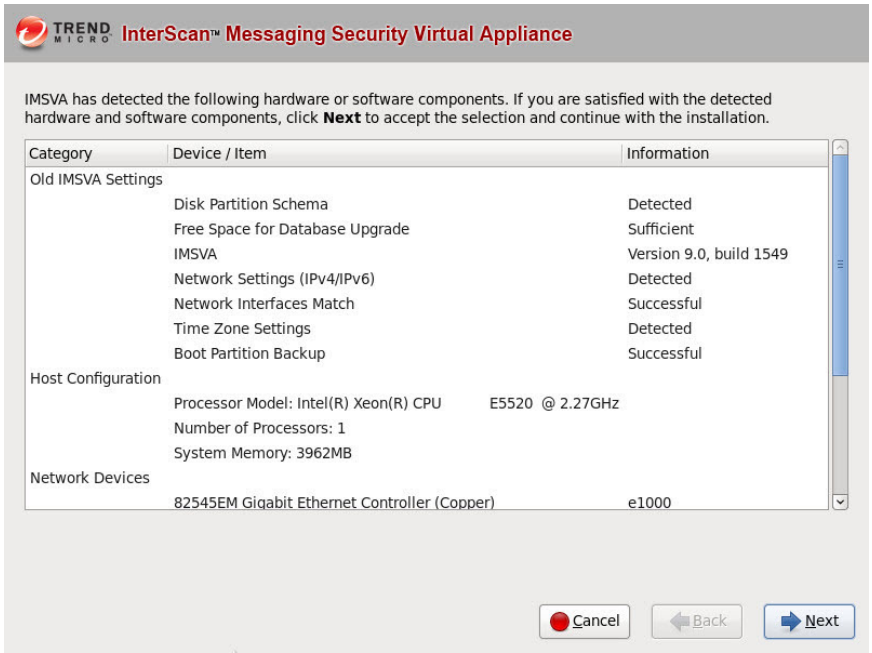
IMSVA 9.0 Patch 2 のアップグレード時に「Upgrade IMSVA 9.0 Patch 1 to IMSVA 9.1」というメッセージが表示されても無視してください。セットアップウィザードは 9.0 Patch 2 に対して正常に機能します。



7. [Version Upgrade] を選択して、[Next] をクリックします。

   IMSVA アップグレードプログラムがハードウェアとソフトウェアを検索し、最小要件が満たされているかどうかを調べて結果を表示します。最小要件に適合しないコンポーネントがハードウェアまたはソフトウェア

に存在する場合、適合しないコンポーネントがアップグレードプログラムにより強調表示され、アップグレードは停止します。

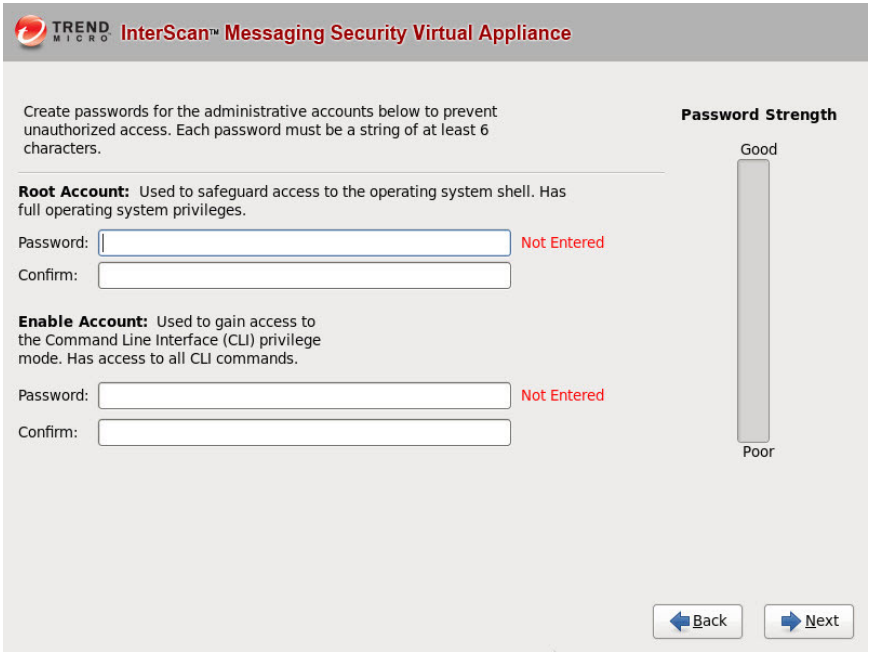


注意

データベースをアップグレードするための十分な空き容量がない場合は、`/var/app_data/imss/log` から古いログファイルを削除して、再度実行してください。`/var/app_data` のディスク空き容量が`/var/imss` のディスク容量の 1.25 倍以上あることを確認してください。

8. ハードウェアおよびソフトウェアの情報が正しいことを確認して、[Next] をクリックします。

アカウント設定の画面が表示されます。



9. [Root Account] および [Enable Account] のパスワードを指定します。

   IMSVA では 2 つの異なるレベルの管理者タイプを使用して、システムの安全を確保します。

   パスワードの文字数は、6～32 文字にしてください。

ヒント

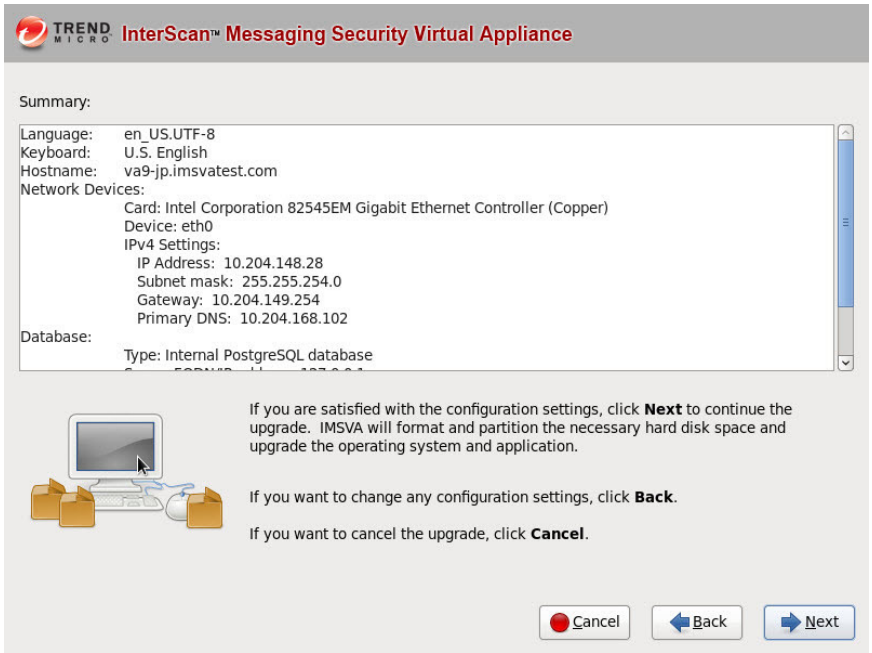
セキュリティを最大限にするために、他人には知られないように一意性の高いパスワードにしてください。英字の大文字と小文字、数字、および任意の特殊文字を使用して、パスワードを作成できます。

- Root Account: OS のシェルにアクセスする際に使用され、サーバに対するすべての権限を持っています。これは、システム上で最も強力なユーザです。

- Enable Account: コマンドラインインタフェースの特権モードにアクセスする際に使用します。このアカウントには、任意の CLI コマンドを実行するためのすべての権限があります。

10. [Next] をクリックします。

    設定の確認画面が表示されます。



11. 設定を確認して [Next] をクリックします。

IMSVA のアップグレード先ローカルドライブのフォーマット進行状況を示す画面が表示されます。

フォーマットが完了すると、概要画面が表示されます。

12. [Restart] をクリックしてシステムを再起動します。

システムの再起動後にアップグレードが続行されます。次の情報が表示されたら、アップグレードは完了です。

```
Generating SSH1 RSA host key:                              [  OK  ]
Generating SSH2 DSA host key:                              [  OK  ]
Starting sshd:                                             [  OK  ]
Starting crond:                                            [  OK  ]
Applying firewall rules...                                 [  OK  ]
Starting upgrade...
Exporting configuration settings from the database...
Export of configuration settings from the database is complete.
Starting database backup...
This may take several minutes.
Database backup is complete.
Starting pre-installation check...
Starting the upgrade process.
Installing the RPM "imsva-9.1-1.i386.rpm"...
The RPM "rpm/imsva-9.1-1.i386.rpm" has been installed successfully.
Installing database...
The database has been installed successfully.
Starting database restore...
Database restore is complete.
Updating the database...
It may take a few hours if your database size is large.
Refer to the Installation Guide for information on how to start 2 hours' dry run
 period for InterScan Messaging Security Virtual Appliance.
Press any key to enter the operating system shell command line interface.
_
```

注意

予期しないエラーを回避するため、次のいずれの手順でもコンピュータを再起動しないでください。

13. 任意のキーを押して、システムシェルコマンドラインインタフェースに切り替えます。
14. 次のコマンドを使用してアップグレードを確認します。

    ```
    # tail -1 /var/app_data/installlog
    ```

15. IMSVA のアップグレードが完了したら、CLI コンソールで次のコマンドを使用して IMSVA サービスを再起動します。

    ```
    /mnt/backup/dry_run.sh
    ```

16. アップグレード後に IMSVA が正常に機能していることを確認します。
17. IMSVA 9.0 Patch 1 にロールバックするには、次のコマンドを使用します。

    ```
    /mnt/backup/confirm.sh
    ```

“no”

18. IMSVA がアップグレード後に正常に機能している場合は、次のコマンドを使用してアップグレードを完了します。

    ```
    /mnt/backup/confirm.sh
    ```

    “yes”

    2 時間以内に IMSVA 9.0 Patch 1 へロールバックしない場合は、IMSVA のすべてのサービスが自動的に停止します。次のコマンドを使用して、IMSVA 9.0 Patch 1 へロールバックするか、アップグレードを完了するかを決定する必要があります。

    ```
    /mnt/backup/confirm.sh
    ```

    アップグレードを完了するには「yes」、ロールバックするには「no」と入力します。

分散環境をアップグレードする

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

手順

1. アップグレードの準備をします。

   a. IMSVA 9.0 Patch 1 をバックアップします。

   注意
   詳細については、93 ページの「IMSVA 9.0 Patch 1 をバックアップする」を参照してください。

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

   ```
   postqueue -p
   ```

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

[システムステータス] 画面で、[管理下のサービス] のすべてのサービスがアクティブになっています。

d. 次のコマンドを使用して、下位デバイスのすべてのサービスを停止します。

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

注意

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

警告!

次の手順を実行するとメールトラフィックが中断されます。トラフィックの中断を回避する場合は、108 ページの「一括アップグレード」または116 ページの「オフラインアップグレード」を実行します。

---

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

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

2. 上位デバイスと下位デバイスをアップグレードします。

a. 上位デバイスをアップグレードします。94 ページの「単一の IMSVA をアップグレードする」の手順 3〜13 を参照してください。

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

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

次のような情報が表示されます。

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

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

警告!

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

すべてのデバイスのアップグレードが完了するまでは、上位デバイスまたは下位デバイスのどちらであっても `/mnt/backup/dry_run.sh` または `/mnt/backup/confirm.sh` を実行しないでください。

アップグレード中に下位デバイスのいずれかで問題が発生した場合は、CLI を使用してその下位デバイスを登録解除します。

3. アップグレードが正常に完了したことを確認します。

a. 次のコマンドを使用して、インストールログファイルを開きます。

```
# tail -1 /var/app_data/installlog
```

b. インストールログファイルで、アップグレードの成功を示す情報を確認します。

4. アップグレードを完了します。

   a. すべてのデバイスをアップグレードしたら、次のコマンドを使用して、上位デバイス、下位デバイスの順に IMSVA サービスを再起動します。

      ```
      /mnt/backup/dry_run.sh
      ```

   b. アップグレード後に IMSVA が正常に機能していることを確認します。

   c. IMSVA 9.0 Patch 1 にロールバックするには、次のコマンドを使用して最初にすべての下位デバイスをロールバックし、次に上位デバイスをロールバックします。

      ```
      /mnt/backup/confirm.sh
      ```

      “no”

   d. IMSVA がアップグレード後に正常に機能している場合は、次のコマンドを使用してアップグレードを完了します。

      ```
      /mnt/backup/confirm.sh
      ```

      “yes”

      2 時間以内に IMSVA 9.0 Patch 1 へロールバックしない場合は、IMSVA のすべてのサービスが自動的に停止します。次のコマンドを使用して、IMSVA 9.0 Patch 1 へロールバックするか、アップグレードを完了するかを決定する必要があります。

      ```
      /mnt/backup/confirm.sh
      ```

      アップグレードを完了するには「`yes`」、ロールバックするには「`no`」と入力します。

一括アップグレード

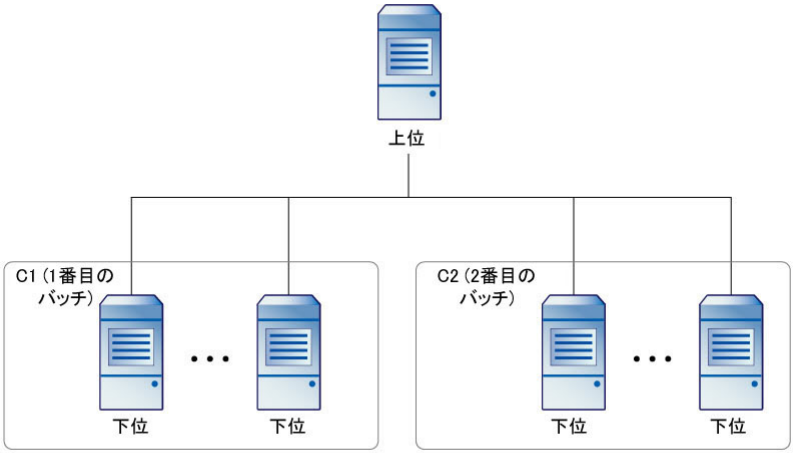
一括アップグレードでは、複数の上位デバイスと下位デバイスをアップグレードできます。アップグレード処理の間、情報はログに記録され、ダウンタイムが発生することはありません。

ヒント

一括アップグレードは、メールトラフィックが最小の時間帯に実行することをお勧めします。最初のバッチ以外のアップグレード対象の IMSVA デバイスで、アップグレード処理時の総メールトラフィック量に対応できるかどうかを評価します。

一括アップグレードに最も適した時間帯は 22:00～4:00 の間です。下位デバイスのデーモンサービスが推奨される時間帯以外に再起動されることがあり、これによって下位デバイスから上位デバイスへの接続が阻止されることがあります。

一括アップグレードの概要は次のとおりです。



1. アップグレードする下位デバイスの最初のバッチを選択します。
2. 手順 1 で選択したデバイスを除き、上位デバイスと下位デバイス間の接続をブロックします (IP テーブルまたはファイアウォールを使用)。

注意

この段階では、下位デバイスは上位デバイスに接続できませんが、上位デバイスはアップグレード前のチェックを実行するために下位デバイスに接続できるよう構成します。

3. 上位デバイスと、手順 1 で選択した下位デバイスのオフラインアップグレードを実行します。
4. アップグレードしたデバイスを実稼働環境に配置します。
5. その他の下位デバイスでオフラインアップグレードを実行します。
6. アップグレードした上位デバイスと下位デバイス間の接続を復元します。
7. アップグレードしたデバイスを実稼働環境に配置します。
8. 上位デバイスと下位デバイスがすべてアップグレードされるまで手順を繰り返します。

注意

一括アップグレード処理の間は、上位デバイスと下位デバイス間の接続をブロックすることが重要です。

上位デバイスと下位デバイスのファイアウォールを設定して、下位デバイスのアップグレードの 2 番目のバッチをブロックします。下位デバイスは、接続がブロックされないかぎり再起動できません。

手順 1: 上位デバイスと下位デバイス間の接続をブロックする

注意

この手順では、C1 はアップグレードする下位デバイスの最初のバッチを表し、C2 は下位デバイスの 2 番目のバッチを表しています。

手順

1. アップグレードするデバイスの最初のバッチ (以下、C1) を選択します。

a. 上位デバイスを選択します。

b. 下位デバイスを選択します。

c. DNS レコードを変更し、選択したデバイスへのメッセージの送信を停止します。

2. 2 番目のバッチ (以下、C2)の下位デバイスにログオンし、IP テーブルを変更します。

a. IP テーブルを変更します。

`/init.d/rcFirewall` を開きます。

```
# vi /etc/init.d/rcFirewall
```

"`start()`" セクションの終わり ("echo" 行と "}" 行の間) に以下のルールを追加します。

```
iptables -I INPUT -s [parent's IP] -j REJECT

iptables -I INPUT -s [C1's IP] -j REJECT

iptables -I INPUT -s [parent's IP] -p tcp --sport 5432
-j ACCEPT

iptables -I INPUT -s [parent's IP] -p tcp --dport 5432
-j ACCEPT

iptables -I OUTPUT -d [C1's IP] -j REJECT

iptables -I OUTPUT -d [parent's IP] -p tcp --sport 5432
-j ACCEPT
```

b. 追加したルールを適用します。

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

3. 上位デバイスの IP テーブルを変更します。

a. 上位デバイスにログオンし/etc/init.d/rcFirewall を開きます。

```
# vi /etc/init.d/rcFirewall
```

"start()" セクションの最後（"}"行の前）に，以下のルールを追加します。

```
iptables -I INPUT -s [C2's IP] -p tcp --sport 5432 -j
ACCEPT
```

b. 追加したルールを適用します。

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

手順 2: インラインアップグレードを実行する

注意

この手順では、C1 はアップグレードする下位デバイスの最初のバッチを表し、C2 は下位デバイスの 2 番目のバッチを表しています。

手順

1. 上位デバイスと C1 デバイスの両方の Postfix キューにメッセージがないことを確認します。

   a. CLI コンソールで、Postfix キューを確認します。

   ```
   # postqueue -p
   ```

   アップグレードは、Postfix キューが空の場合のみ実行します。それ以外の場合は、Postfix キューのメッセージが失われることがあります。

2. 次のコマンドを使用して、C1 デバイス上のデータベースを除くすべての IMSVA サービスを停止します。

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

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

3. IMSVA 9.1 へのインラインアップグレードを実行します。

   注意

   アップグレード手順の詳細については、94 ページの「単一の IMSVA をアップグレードする」を参照してください。

4. IMSVA 9.1 のテスト配置を実行します。

   a. C1 デバイスのアップグレード後、上位デバイスの IP テーブルを変更して任意のリモートサーバとの接続を確立できるようにします。このリモートサーバから上位デバイスのデータベースデータをアップデートできます。

   ```
   # iptables -I INPUT -s [Remote server's IP] -p tcp --
   sport 5432 -j ACCEPT
   ```

   ```
   # iptables -I INPUT -s [Remote server's IP] -p tcp --
   dport 5432 -j ACCEPT
   ```

   b. SQL 接続ツールなどを使用して、上位デバイスの SQL データベースにログオンし、テーブルをアップデートします。

   ```
   # select * from tb_component_list;
   ```

   ```
   # update tb_component_list set app_ver='9.1.0.xxxx'
   where ip_addr='[C2's IP]';
   ```

   注意

   この手順により、IMSVA では、dry_run の前に実行されるチェックが回避されます。

   114 ページの「手順 3: その他の下位デバイスでインラインアップグレードを実行する」(手順 4-b) の参考用に、C2 デバイスの元の IMSVA バージョン (`app_ver`) を記録しておきます。その後、`9.1.0.xxxx` を、イントール予定の IMSVA 9.1 のビルド番号で置き換えます。

   c. CLI コンソールで、すべての IMSVA サービスを再起動します。

   ```
   # /mnt/backup/dry_run.sh
   ```

   注意

   最初に上位デバイスを再起動し、次にすべての下位デバイスを再起動します。

5. ビルド番号を確認します。

a. [管理] > [アップデート] > [システムとアプリケーション] の順に選択します。

b. [現在のステータス] の下で、アプリケーションのバージョンが 9.1.0.xxxx であることを確認します。

6. インラインアップグレードを完了します。

a. 上位デバイスと C1 デバイスのすべてでアップグレードを完了するには、次のコマンドを実行します。最初に上位デバイスで実行し、次に C1 デバイスで実行してください。

```
# /mnt/backup/confirm.sh
```

“yes”

b. IMSVA 9.0 にロールバックするには、最初にすべての下位デバイスをロールバックしてから、上位デバイスをロールバックします。

```
# /mnt/backup/confirm.sh
```

“no”

c. DNS レコードを変更して、アップグレードされた上位デバイスと C1 デバイスへのメッセージの送信を開始し、C2 デバイスへのメッセージの送信を停止します。

手順 3: その他の下位デバイスでインラインアップグレードを実行する

注意

下位デバイスを個々に、または一括してアップグレードします。

この手順では、C1 はアップグレードする下位デバイスの最初のバッチを表し、C2 は下位デバイスの 2 番目のバッチを表しています。

手順

1. 下位デバイスを選択します。

2. DNS レコードを変更し、選択したデバイスへのメッセージの送信を停止します。
3. Postfix キューにメッセージがないことを確認します。
   a. CLI コンソールで、Postfix キューを確認します。

      # `postqueue -p`
4. C2 デバイスの設定を変更します。
   a. インラインアップグレードのチェックを回避するため、C2 デバイスの IP テーブルを変更します。以下のコマンドを実行してください。

      ```
      # iptables -I OUTPUT -d [parent's IP] -p tcp --dport
      5432 -j ACCEPT
      ```
   b. 上位デバイスのデータベースで C2 デバイスの IMSVA バージョンを変更します。

      ```
      # /opt/trend/imss/PostgreSQL/bin/psql imss sa
      ```

      ```
      # select * from tb_component_list;
      ```

      ```
      # update tb_component_list set app_ver='9.0.0.1549'
      where ip_addr='[C2's IP]';
      ```

      注意

      IMSVA バージョン (`app_ver`) には、112 ページの「手順 2: インラインアップグレードを実行する」(手順 4-b) で記録したバージョンを指定します。
5. IMSVA 9.1 へのインラインアップグレードを実行します。

   注意

   アップグレード手順の詳細については、94 ページの「単一の IMSVA をアップグレードする」を参照してください。
6. IMSVA 9.1 のテスト配置を実行します。
   a. CLI コンソールで、すべての IMSVA サービスを再起動します。

```
# /mnt/backup/dry_run.sh
```

7. ビルド番号を確認します。
   a. [管理] > [アップデート] > [システムとアプリケーション] の順に選択します。
   b. [現在のステータス] の下で、アプリケーションのバージョンが 9.1.0.xxxx であることを確認します。
8. インラインアップグレードを完了します。
   a. すべてのデバイスのアップグレードを完了するには、次のコマンドを実行します。

      ```
      # /mnt/backup/confirm.sh
      ```

      “yes”
   b. IMSVA 9.0 にロールバックするには、次のコマンドを実行します。

      ```
      # /mnt/backup/confirm.sh
      ```

      “no”
9. C2 デバイスを復元します。
   a. DNS レコードを変更し、C2 デバイスへのメッセージの送信を開始します。
   b. バッチのアップグレード処理が完了するまで、他の下位デバイスのアップグレードを続けます。

オフラインアップグレード

オフラインアップグレードでは、一時 IMSVA デバイスを使用してメールトラフィックを処理します。アップグレード処理の間、すべての情報は IMSVA ログに記録され、ダウンタイムが発生することはありません。

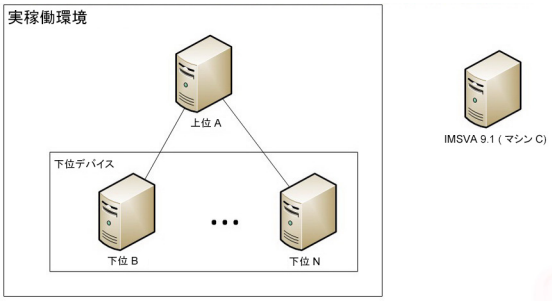
ヒント

オフラインアップグレードは、メールトラフィックが最小の時間帯に実行することをお勧めします。一時 IMSVA デバイスが、アップグレード処理時の総メールトラフィック量に対応できるかどうかを評価します。

オフラインアップグレードを実施する場合は、次の点に注意してください。

1. IMSVA を仮想マシンに配置する前にファイルをバックアップします。
2. NTP サーバを使用して、実稼働 IMSVA デバイスと一時 IMSVA デバイスが同じシステム時間を使用するようにします。

オフラインアップグレードの概要は次のとおりです。



1. IMSVA 9.1 を一時デバイスにインストールします。
2. 実稼働 IMSVA デバイスから設定をインポートします。
3. DNS MX レコードを変更して、メールトラフィックを一時デバイスにリダイレクトします。
4. 実稼働デバイスをネットワークから切断します。
5. デバイスをアップグレードします。
6. メールトラフィックを実稼働デバイスにリダイレクトしなおします。
7. 一時デバイスから実稼働下位デバイスのいずれかにログとキューフォルダをコピーします。

注意

下位デバイスにデータを復元した後、データに差異が生じることがあります。仮想アナライザの通知が有効な場合は、データの復元後に仮想アナライザの通知メールを受け取ることがあります。

手順 1: IMSVA 9.1 を一時デバイスにインストールする

手順

1. ISO ファイルを使用して IMSVA 9.1 を一時デバイスにインストールします。
2. 一時 IMSVA 9.1 デバイスの初期設定をバックアップします。
   a. 上位デバイスの管理コンソールにログオンします。
   b. [管理] > [インポート/エクスポート] の順に選択します。
   c. [エクスポート] をクリックして、エクスポートされたファイルを保存します。
3. 既存の上位デバイスと下位デバイスの設定をエクスポートします。
   a. 上位デバイスの管理コンソールにログオンします。
   b. [管理] > [インポート/エクスポート] の順に選択します。
   c. [エクスポート] をクリックして、エクスポートされたファイルを保存します。
4. 上位デバイスの設定を一時デバイスにインポートします。
   a. 一時デバイスの管理コンソールにログオンします。
   b. [管理] > [インポート/エクスポート] の順に選択します。
   c. [インポート] をクリックします。

注意

インポート処理で問題が発生した場合は、手順 2 で作成したバックアップファイルを使用して、IMSVA 9.1 の初期設定を復元します。

手順 2: メールトラフィックを一時 IMSVA デバイスにリダイレクトする

実稼働サーバはメールトラフィックが最小の時間帯にアップグレードすることをお勧めします。

手順

1. DNS MX レコードを変更して、メールトラフィックを一時 IMSVA デバイスにリダイレクトします。
2. 上位デバイスと下位デバイスへのメッセージの送信を停止します。

手順 3: オフラインアップグレードを実行する

手順

1. オフラインの状態で上位デバイスと下位デバイスをアップグレードします。詳細については、105 ページの「分散環境をアップグレードする」を参照してください。
2. DNS MX レコードを変更して、メールトラフィックを上位デバイスと、1 つを除くすべての下位デバイスにリダイレクトします。
3. アップグレード処理で失われたカスタマイズ設定を指定します。
4. 一時 IMSVA デバイスへのメッセージの送信を停止します。

手順 4: IMSVA 9.1 のログおよびキューフォルダを下位デバイスにコピーする

手順

1. 下位デバイス (マシン B) の監視サービス、マネージャサービス、およびメッセージ追跡サービスを停止します。

```
[root@machine B ~]# S99MONITOR stop
```

```
[root@machine B ~]# S99MANAGER stop
```

```
[root@machine B ~]# S99CMAGENT stop
```

```
[root@machine B ~]# S99MSGTRACING stop
```

2. 一時デバイスで仮想アナライザを有効にしている場合は、仮想アナライザのアップロードフォルダにメッセージがないことを確認します。

```
[root@machine C ~]# ls -l /var/app_data/imss/dtas_upload/
```

注意

ログのインポート後に通知を受信しないよう、一時 IMSVA デバイスの仮想アナライザは無効にすることをお勧めします。仮想アナライザを有効のままにする場合は、通知を無視します。

3. 一時 IMSVA デバイスから下位 B デバイスにキューフォルダをコピーしてマージします。

```
[root@machine C ~]# scp -r /opt/trend/imss/queue
root@machine B:/opt/trend/imss/
```

```
[root@machine B ~]# chown -R imss:imss /opt/trend/imss/queue
```

4. 一時 IMSVA デバイスのポリシーイベントログをコピーして、最新の下位 B デバイスのポリシーイベントログの末尾に追加します。

以下に例を示します。

```
[root@machine C ~]# scp /opt/trend/imss/log/
polevt.imss.20130325.0001 root@machine B:/root/
```

```
[root@machine B ~]# cat /root/polevt.imss.20130325.0001 >>
```

```
/opt/trend/imss/log/polevt.imss.20130325.0001
```

5. 一時 IMSVA デバイスのメールログをコピーして、下位 B デバイスのメールログの末尾に追加します。

```
[root@machine C ~]# scp /var/log/maillog root@machine B:/
root/

[root@machine B ~]# cat /root/maillog >> /var/log/maillog
```

6. 一時 IMSVA デバイスの fox*ログをコピーして、最新の下位 B デバイスの fox*ログの末尾に追加します。

   以下に例を示します。

```
[root@machine C ~]# scp /opt/trend/imss/log/
foxmsg.20130325.0001 root@machine B:/root/

[root@machine B ~]# cat /root/foxmsg.20130325.0001 >>

/opt/trend/imss/log/foxmsg.20130325.0001
```

7. 下位 B デバイスで、監視サービス、マネージャサービス、およびメッセージ追跡サービスを開始します。まもなく、追加したログがデータベースにインポートされます。

```
[root@machine B ~]# S99MANAGER start

[root@machine B ~]# S99MONITOR start

[root@machine B ~]# S99CMAGENT start

[root@machine B ~]# S99MSGTRACING start
```

8. 追加したログがデータベースにインポートされた後、DNS MX レコードを変更して、下位 B デバイスの設定を復元します。

アップグレードをロールバックする

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

手順

1. ゴーストイメージを作成している場合や、元の IMSVA の仮想マシンイメージがある場合は、アップグレードしたイメージを元のイメージで上書きします。
2. 次のコマンドを使用して、cron サービスを停止します。

   ```
   service crond stop
   ```

3. cron 設定バックアップファイル`/var/spool/cron/root.bakForUpgrade` を確認します。ファイルを見つけたら、次のコマンドを使用して cron 設定を復元します。

   ```
   rm -rf /var/spool/cron/root && /bin/mv -f /var/spool/cron/root.bakForUpgrade /var/spool/cron/root
   ```

4. ログバックアップファイル`/var/app_data/imss/log.bakForUpgrade` を確認します。バックアップファイルを見つけたら、次のコマンドを使用してログファイルを復元します。

   ```
   rm -rf /var/app_data/imss/log/ && /bin/mv -f /var/app_data/imss/log.bakForUpgrade /var/app_data/imss/log/
   ```

5. 次のコマンドを使用して、データベースサービスを停止します。

   ```
   killall postgres
   ```

6. 上位デバイスで、データベースバックアップファイル`/var/app_data/imss/pgdata.bakForUpgrade` を確認します。ファイルを見つけたら、次のコマンドを使用してデータベースファイルを復元します。

   ```
   rm -rf /var/app_data/imss/db/pgdata && /bin/mv -f /var/app_data/imss/pgdata.bakForUpgrade /var/app_data/imss/db/pgdata
   ```

7. IMSVA 9.0 Patch 1 のルートパーティションがマウントされていない場合は、次のコマンドを使用してマウントします。

   ```
   mkdir -p /var/tmp/orig_root
   ```

   ```
   mount -t ext3 /dev/mapper/IMSVA-Root1 /var/tmp/orig_root
   ```

8. 次のコマンドを使用して、/boot フォルダを復元します。

```
/bin/cp -af /var/tmp/orig_root/boot-imsva-9.0-back-
up-for-9.1/* /boot
```

9. ブートパーティションの UUID をアップデートします。
   a. `/etc/fstab` から 9.1 のブートパーティションの UUID を取得します。
   b. `/var/tmp/orig_root/etc/fstab` にある 9.0 Patch 1 のブートパーティションの UUID を、9.1 のブートパーティションの UUID で上書きします。
10. コンピュータを再起動します。

以前のバージョンから移行する

IMSVA9.1 SP1 は、以前のバージョンの IMSVA からの移行をサポートしています。

以下の表は、IMSVA9.1 SP1 への移行をサポートするバージョンを示しています。

表 5-1. サポートされる移行プラットフォームおよびバージョン

プラットフォーム	バージョン
InterScan MSS Solaris 版	7.0 Service Pack 1 Patch 4
InterScan MSS Linux 版	7.1 Service Pack 2 Patch 1
InterScan MSS Windows 版	7.1 Patch 3
InterScan MSS Windows 版	7.5 Patch 1
IMSVA	8.0 Patch 2
IMSVA	8.2 Service Pack 2 Patch 1
IMSVA	8.5 Service Pack 1 Patch 1
IMSVA	9.0 Patch 2
IMSVA	9.1

移行プロセス

移行プロセスで必要な作業は次のとおりです。

- 手順 1: 以前のバージョンの InterScan MSS または IMSVA から設定をエクスポートする
- 手順 2: IMSVA 9.1 SP1 に設定をインポートする

以前のバージョンの InterScan MSS または IMSVA から設定をエクスポートする

次の設定は移行されません。

表 5-2. 移行できない設定

MTA 設定	移行されない設定
MTA 設定	SMTP インタフェースの IP アドレス
設定	データベース設定 (内部ファイルのパスなど)
	管理コンソールのパスワード
	Control Manager 設定
	アクティベーションコード 注意 IMSVA の以前のすべてのバージョンで、クラウドプレフィルタのアクティベーションコードが IMSVA9.1 SP1 に移行されます。

重要

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

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

下位デバイスの証明書の使用状況はエクスポートできません。

手順

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

   [インポート/エクスポート] 画面が表示されます。

2. [エクスポート] をクリックします。

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

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

手順

1. 移行ツールのパッケージ (`export_tool_sol_70.tar.gz`) を InterScan MSS 7.0 Solaris 版サーバにコピーします。

2. 次のコマンドを使用して、エクスポートツールを解凍します。

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

   ```
   tar xf export_tool_sol_70.tar
   ```

   注意

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

3. 次のコマンドを使用して、現在の作業ディレクトリを変更します。

   ```
   cd export70sol
   ```

4. 次のコマンドを実行します。

   ```
   ./export_tool_70.sh
   ```

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

IMSVA 9.1 に設定をインポートする

手順

1. IMSVA 9.1 の新規インストールを実行します。

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

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

   [インポート/エクスポート] 画面が表示されます。

4. 設定パッケージをインポートします。

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

InterScan MSS Windows 版から移行する

InterScan MSS Windows 版から IMSVA9.1 SP1 に移行するには、124 ページの「移行プロセス」を参照してください。

変更される InterScan MSS Windows 版の設定

次の InterScan MSS Windows 版の設定は移行時に変更されます。

- 移行時は、カスタマイズされたすべての処理が IMSVA9.1 SP1 によって [初期設定の推奨処理] に変更されます。ただし、カスタマイズされた処理が [接続の拒否] の場合は例外で、設定が変更されずに保持されます。
- [初期設定の配信] が [スマートホスト] に設定されている場合は、[*] に変更されます。
- ドメインに複数の [スマートホスト] が設定されていた場合は、リスト内のすべてのスマートホストが IMSVA9.1 SP1 に移行され、配信方法が静的ルーティングに設定されます。
- 1 接続あたりのデータサイズ上限および最大メッセージ件数の設定が減少します。
- IMSVA9.1 SP1 では、[検索サービスで使用できる空きディスク容量が次の値を下回った場合] が [いずれかのホストでデータパーティションの空き容量が次の値を下回った場合] に変更されます。

移行されない Windows 版 InterScan MSS 7.1 Patch 3 の設定

次を除くすべての Windows 版 InterScan MSS 7.1 Patch 3 の設定が IMSVA9.1 SP1 に移行されます。

- Control Manager エージェントのすべての設定
- 管理者アカウントのユーザ名とパスワード
- パターンファイルとエンジン
- SMTP インタフェースとポート番号
- システムパフォーマンスに影響する内部設定
- Transport Layer Security 設定
- アクティベーションコード (IMSVA では Windows 版 InterScan MSS 7.1 のアクティベーションコードを使用できないため)
- [管理] > [接続] > [コンポーネント] の次の内部ポートは移行されません。
  - InterScan MSS マネージャポート
  - ポリシーサービスポート
- BATV ルールおよび関連するすべての設定は移行されません。

移行されない InterScan MSS 7.5 Windows 版の設定

次を除くすべての InterScan MSS 7.5 Windows 版の設定が IMSVA9.1 SP1 に移行されます。

- Control Manager エージェントのすべての設定
- 管理者アカウントのユーザ名とパスワード
- パターンファイルとエンジン
- SMTP インタフェースとポート番号
- システムパフォーマンスに影響する内部設定
- 仮想アナライザの設定
- Transport Layer Security 設定
- アクティベーションコード (IMSVA では InterScan MSS 7.5 Windows 版のアクティベーションコードを使用できないため)
- [管理] > [接続] > [コンポーネント] の次の内部ポートは移行されません。
  - InterScan MSS マネージャポート
  - ポリシーサービスポート
- BATV ルールおよび関連するすべての設定は移行されません。

InterScan MSS Linux 版から移行する

InterScan MSS Linux 版から IMSVA9.1 SP1 に移行するには、124 ページの「移行プロセス」を参照してください。

変更される InterScan MSS Linux 版の設定

次の InterScan MSS Linux 版の設定は移行時に変更されます。

- [管理] > [通知] > [イベント]通知:

  IMSVA9.1 SP1 では、[検索サービスで使用できる空きディスク容量が次の値を下回った場合] が [いずれかのホストでデータパーティションの空き容量が次の値を下回った場合] に変更されます。

移行されない InterScan MSS 7.1 Linux 版 SP2 の設定

次を除くすべての InterScan MSS 7.1 Linux 版 SP2 の設定が IMSVA9.1 SP1 に移行されます。

- Control Manager エージェントのすべての設定
- 管理者アカウントのユーザ名とパスワード
- パターンファイルとエンジン
- SMTP インタフェースとポート番号
- システムパフォーマンスに影響する内部設定
- Transport Layer Security 設定
- アクティベーションコード (IMSVA では InterScan MSS 7.1 Linux 版のアクティベーションコードを使用できないため)
- マーケティングメッセージ除外リストのメールアドレス

InterScan MSS Solaris 版から移行する

InterScan MSS Solaris 版から IMSVA9.1 SP1 に移行するには、124 ページの「移行プロセス」を参照してください。

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

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

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

IMSVA 8.0 Patch 2、IMSVA 8.2 SP2 Patch 1、IMSVA 8.5 SP1 Patch 1、または IMSVA 9.0 Patch 2 から移行する

旧バージョンの IMSVA から IMSVA9.1 SP1 に移行するには、124 ページの「移行プロセス」を参照してください。

移行されない IMSVA 8.0 Patch 2 の設定

次を除くすべての IMSVA 8.0 Patch 2 の設定が IMSVA9.1 SP1 に移行されます。

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

移行されない IMSVA 8.2 SP2 Patch 1 の設定

次を除くすべての IMSVA 8.2 SP2 Patch 1 の設定が IMSVA9.1 SP1 に移行されます。

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

移行されない IMSVA 8.5 SP1 Patch 1 の設定

次を除くすべての IMSVA 8.5 SP1 Patch 1 の設定が IMSVA9.1 SP1 に移行されます。

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

移行されない IMSVA 9.0 Patch 2 の設定

次を除くすべての IMSVA 9.0 Patch 2 の設定が IMSVA9.1 SP1 に移行されます。

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

デバッグログをエクスポートする

トラブルシューティングの目的でデバッグログを分析する必要がある場合は、上位デバイスと上位デバイスに登録されているすべてのデバイスのデバッグログを最大過去 2 日分エクスポートできます。

注意

デバッグログはパスワードで保護された Zip ファイル内にあります。このファイルの初期設定のパスワードは `trend` です。

手順

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

   ログファイルの合計サイズに応じて、このプロセスには 10 分から 1 時間以上かかることがあります。

第 6 章

トラブルシューティング

ここでは、IMSVA のインストール、設定、または管理時に発生する可能性のある一般的な問題を解決する方法について説明します。その他の問題については、トレンドマイクロの製品 QA を確認してください。

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のユーティリティ

次のトラブルシューティングに関連するユーティリティおよびコマンドは、慎重に使用してください。サポート担当者に連絡してから、IMSVA 内部のファイルを修正することをお勧めします。

- 管理データベース

  `/opt/trend/imss/config/odbc.ini` を開いて主要データベースの値を確認します。

- EUQ データベース

  `/opt/trend/imss/config/euqodbc.ini` を開いて主要データベースの値を確認します。

注意

内部データベースを使用する場合、データベースの初期設定のパスワードは postgreSQL になります。

- ファイアウォール設定の確認:

  ```
  iptables -nvxL
  ```

- PostgreSQL コマンドラインツール:

  ```
  /opt/trend/imss/PostgreSQL/bin/psql -U sa -d imss
  ```

注意

imss は`/opt/trend/imss/config/odbc.ini` から取得する管理データベース名を指します。

- cdt (パスワード: 「trend」) — 次の情報を収集:
  - 設定情報
  - ログ
  - コアダンプ
- その他のユーティリティ:

- pstack: すべてのスレッドを含む、プロセスのコールスタックを表示
- ipcs: 現行システムのすべての IPC を一覧表示
- gdb: デバッガ
- tcpdump: ネットワークパッケージを監視
- netstat: 現在のネットワーク接続を表示

グループ内のデバイス間通信のトラブルシューティング

グループ内に複数の IMSVA デバイスが配置されている場合、デバイス間で通信する必要があります。

手順

1. 次のポートがすべてのデバイスでアクセス可能になっているか確認してください。
   - 5060: ポリシーサービス
   - 15505: IMSVA 制御サービス
   - 53 UDP/TCP: IP プロファイラ
   - 5432: データベースサービス
   - 8009: エンドユーザメール隔離の内部サービス
   - 389: LDAP ローカルキャッシュサービス
   - 998/999: TLS 設定サービス
   - 10030: メッセージ配信設定サービス
   - 10040: SMTP トラフィックスロットリングサービス
   - 8891: DKIM 設定サービス
2. 次の項目を確認してください。
   - 「iptables」内の現在のファイアウォールの設定

- `/etc/conf/fw.rules` 内のファイアウォール設定ファイル
- データベース内のテーブル「tb_trusted_ip_list」に、正しいデバイスの IP アドレスがある。一方のデバイスから他のデバイスのアクセスしようとする IP アドレスがこのリスト内に存在する。

3. すべての必要なポートが、関連サービスにアクセス可能であることを確認してください。

下位デバイスの登録のトラブルシューティング

手順

1. 上位デバイスの管理コンソールを開き、[管理] > [IMSVA 設定] > [接続] > [下位 IP アドレス] の順に選択します。
2. 下位デバイスの IP アドレスが下位デバイスの IP アドレスリストに含まれているかどうか確認します。
3. 設定ウィザードで、[下位デバイス] がデバイスロールとして選択されていることを確認してください。
4. 管理データベースへのアクセスが可能であることを確認してください。
5. MCP エージェントが有効になっている場合、エージェントの登録を解除します。
6. 上位デバイスに登録されている他の下位デバイスの IP アドレスが、登録しようとしているデバイスと異なることを確認します。
7. すべてのログと隔離されたメッセージを削除します。
8. 設定を変更して、サービスを再起動します。
9. 設定ウィザードで、上位デバイスの管理コンソールから、最初の要求を実行します。

下位デバイスの登録解除のトラブルシューティング

手順

1. コマンドラインインタフェースで下位デバイスに接続します。
2. 管理データベースへのアクセスが可能であるかどうかを確認してください。アクセスが可能であれば、上位デバイスの管理コンソールで、下位デバイスを下位デバイス IP リストから削除して、信頼する下位デバイスリストを更新します。
3. デバイスを復旧することにより、下位デバイスを上位デバイスから強制的に登録解除します。
4. Patch をアップデートします。
5. 下位デバイスが上位デバイスから登録解除されたことを確認するには、次のいずれかを実行します。
   - 下位デバイスで管理コンソールにアクセスしてみます。コンソールにアクセスできれば、デバイスは正常に登録解除されています。
   - 次のコマンドを実行します。

     ```
     /opt/trend/imss/script/cfgtool.sh dereg
     ```

ハードウェア認識エラーのトラブルシューティング

IMSVA でストレージやネットワークデバイスなどのハードウェアを認識できない場合は、IMSVA を再インストールする前に、ドライバディスクを読み込んでください。

ハードウェアメーカーに問い合わせて、CentOS 6.4 (x86_64) に適合するハードウェアドライバを取得します。ドライバのインストールガイドを参照して、ドライバディスクを読み込みます。

次に、ドライバディスクの読み込み例を示します。

手順

1. USB などのリムーバブルディスクを用意します。リムーバブルディスクのファイルシステムが使用可能であることを確認します。
2. ドライバイメージを USB にコピーします。

   ```
   cp dd.iso /mnt/usb
   ```

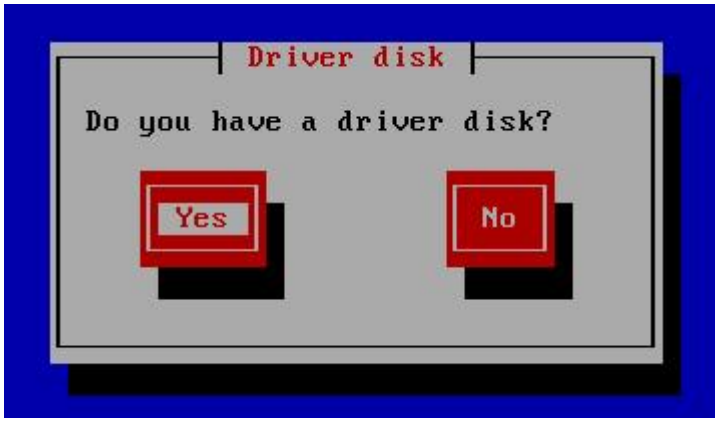
3. IMSVA のインストール DVD を DVD ドライブに挿入し、IMSVA のインストールを開始します。

   セットアップウィザードの画面が表示されます。

4. [Fresh install or version upgrade] を選択し、Tab キーを押して編集モードにします。
5. セットアップウィザード画面の下部に表示される情報に「`dd`」を追加します。

6. Enter キーを押します。

[Driver disk] 画面が表示されます。

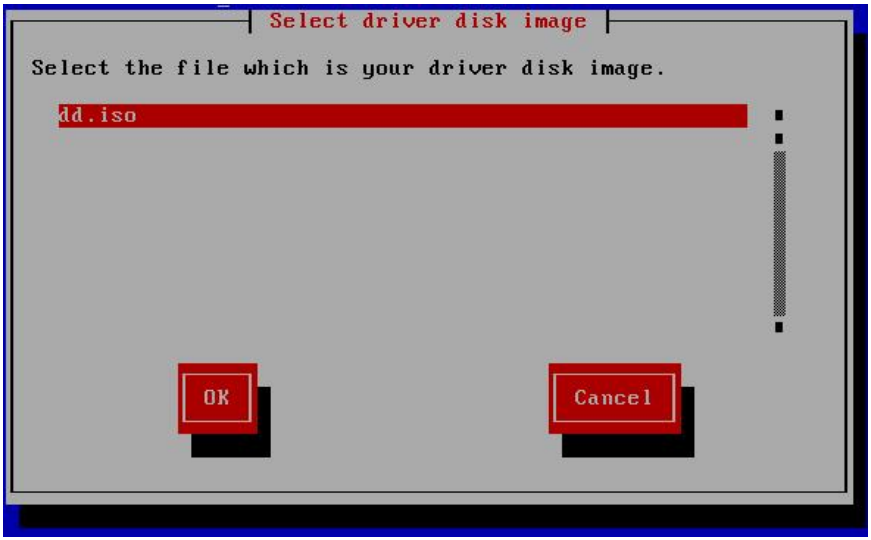


7. USB を挿入し、[はい] を選択します。

   [Driver Disk Source] 画面が表示されます。

8. USB (例: sdb) を選択し、[OK] を選択します。

[Select driver disk image] 画面が表示されます。



9. ドライバディスクイメージを選択します。

   [More Driver Disks] 画面が表示されます。

10. USB を取り外し、[いいえ] をクリックして IMSVA のインストールを続行します。

ネットワーク接続のトラブルシューティング

仮想マシンでネットワーク接続に問題が発生した場合は、ご使用の NIC カードに割り当てられている MAC アドレスが変更されていないかどうか確認してください。

仮想マシンに自動的に割り当てられた MAC アドレスは動的に変更されることがあります。しかし、インタフェースの設定ファイルや udev の永続的なネットワークルールファイルに記録されている MAC アドレスは変更されません。結果として NIC カードが使用できなくなることがあります。

トレンドマイクロでは、静的な MAC アドレスを使用することをお勧めします。MAC アドレスが変更されている場合は、次の手順を実行して、NIC カードが適切に機能することを確認してください。

手順

1. 次のコマンドを使用して、udev ルールファイルを削除します。

```
rm -rf /etc/udev/rules.d/70-persistent-net.rules
```

2. `/etc/sysconfig/network-scripts/ifcfg-eth<x>`ファイルから次の行を削除します。

```
HWADDR=<MAC>

UUID=<UUID>
```

> **注意**
> インタフェースの設定ファイル名は`/etc/sysconfig/network-scripts/ifcfg-eth<x>`のようになっています。`<x>`は特定のカードに対応する一意の番号です。

3. `/lib/udev/rules.d/75-persistent-net-generator.rules` ファイルで、次の情報が含まれる行を検索します。

```
ATTR{addr_assign_type}=="0"
```

4. この行の前に次の情報を追加します。

```
# ignore VMWare virtual interfaces

ENV{MATCHADDR}=="00:0c:29:*|00:50:56:*",
GOTO="persistent_net_generator_end"

# ignore Hyper-V virtual interfaces

ENV{MATCHADDR}=="00:15:5d:*",
GOTO="persistent_net_generator_end"
```

5. 仮想マシンを再起動してネットワーク接続を確認します。

付録 A

テクニカルサポート

ここでは、次の項目について説明します。

トラブルシューティングのリソース

トレンドマイクロでは以下のオンラインリソースを提供しています。テクニカルサポートに問い合わせる前に、こちらのサイトも参考にしてください。

サポートポータルの利用

サポートポータルでは、よく寄せられるお問い合わせや、障害発生時の参考となる情報、リリース後に更新された製品情報などを提供しています。

https://success.trendmicro.com/dcx/s/?language=ja

脅威データベース

現在、不正プログラムの多くは、コンピュータのセキュリティプロトコルを回避するために、2 つ以上の技術を組み合わせた複合型脅威で構成されています。トレンドマイクロは、カスタマイズされた防御戦略を策定した製品で、この複雑な不正プログラムに対抗します。脅威データベースは、既知の不正プログラム、スパム、悪意のある URL、および既知の脆弱性など、さまざまな混合型脅威の名前や兆候を包括的に提供します。

詳細については、https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/ をご覧ください。

- 現在アクティブまたは「in the Wild」と呼ばれている生きた不正プログラムと悪意のあるモバイルコード
- これまでの Web 攻撃の記録を記載した、相関性のある脅威の情報ページ
- 対象となる攻撃やセキュリティの脅威に関するオンライン勧告
- Web 攻撃およびオンラインのトレンド情報
- 不正プログラムの週次レポート

製品サポート情報

製品のユーザ登録により、さまざまなサポートサービスを受けることができます。

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

サポートサービスについて

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

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

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

注意

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

トレンドマイクロへのウイルス解析依頼

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

ファイルを送信いただく前に、トレンドマイクロの不正プログラム情報検索サイト「脅威データベース」にアクセスして、ウイルスを特定できる情報がないかどうか確認してください。

https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/

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

https://success.trendmicro.com/dcx/s/threat?language=ja

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。

メールレピュテーションについて

スパムメールやフィッシングメールなどの送信元を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

ファイルレピュテーションについて

不正プログラムなどのファイル情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

Web レピュテーションについて

不正な Web サイトや URL などの情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

その他のリソース

製品やサービスについてのその他の情報として、次のようなものがあります。

最新版ダウンロード

製品やドキュメントの最新版は、次の Web ページからダウンロードできます。

https://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

---

注意

サービス製品、販売代理店経由での販売製品、または異なる提供形態をとる製品など、一部対象外の製品があります。

付録 B

VMware ESX for IMSVA での新しい仮想マシンの作成

この付録では、IMSVA 用の新しい仮想マシンを作成する方法について説明します。

この付録の内容は次のとおりです。

新しい仮想マシンを作成する

本書では、ESX の実際のインストールについては説明しません。この製品のインストールについては、VMware 製品のドキュメントを参照してください。

以下に記載された手順では、IMSVA をインストールするために VMware ESX で新しい仮想マシンを作成するプロセスを説明します。次の手順に従って、ご使用の環境に仮想マシンを作成してください。選択した CPU、NIC の数、メモリおよびハードディスク容量は、配置要件を考慮する必要があります。この手順で入力する値は、説明用です。

手順

1. メニューバーから [ファイル] > [新規] > [仮想マシン] を選択します。

[仮想マシンの新規作成ウィザード] が表示されます。

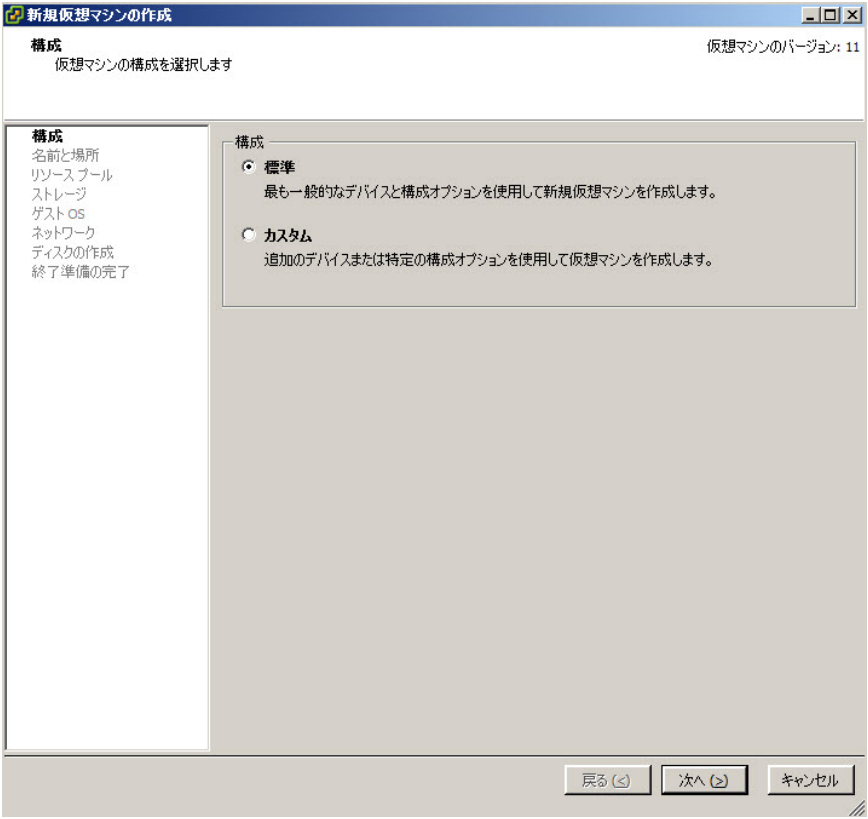


図 B-1. 仮想マシンの設定

2. 仮想マシンの構成方法で、[標準] のラジオボタンが選択された状態にします。
3. [次へ] をクリックします。

[名前と場所] 画面が表示されます。

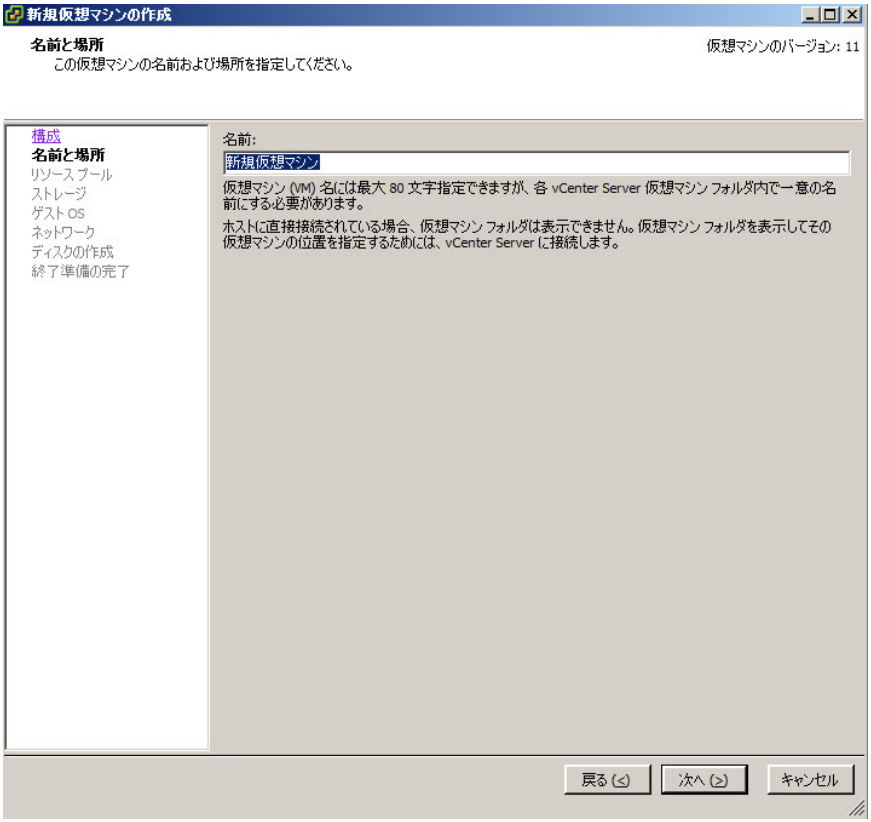


図 B-2. 仮想マシンの名前および場所の指定

4. [名前] フィールドに適切なマシン名を入力し、[次へ] をクリックします。

[ストレージ] 画面が表示されます。

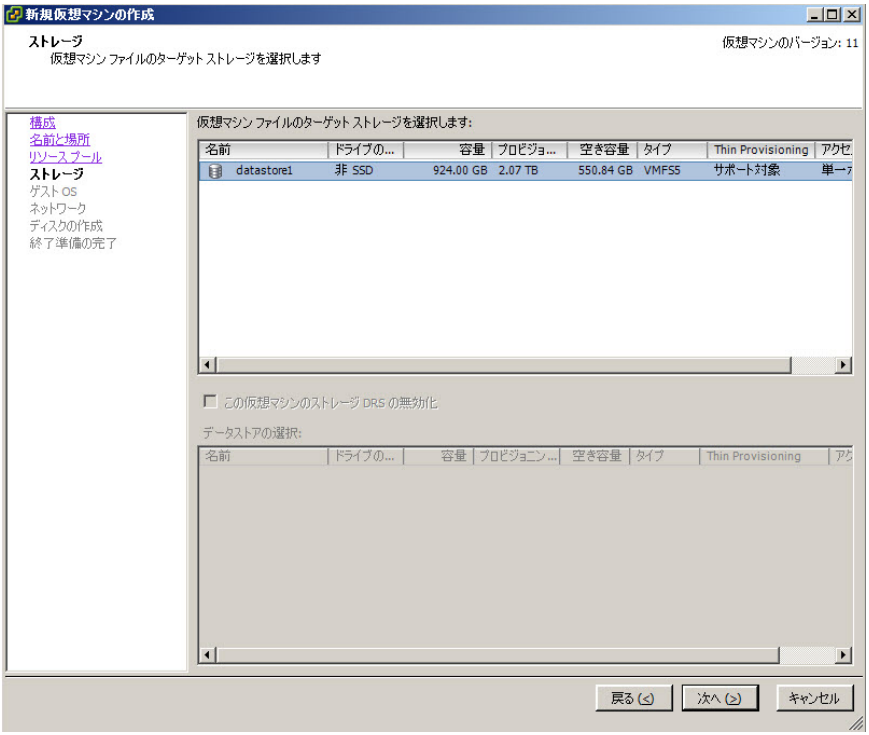


図 B-3. 仮想マシンのストレージ

5. 仮想マシンを置くデータストアを選択します。
6. [次へ] をクリックします。

[ゲスト OS] 画面が表示されます。

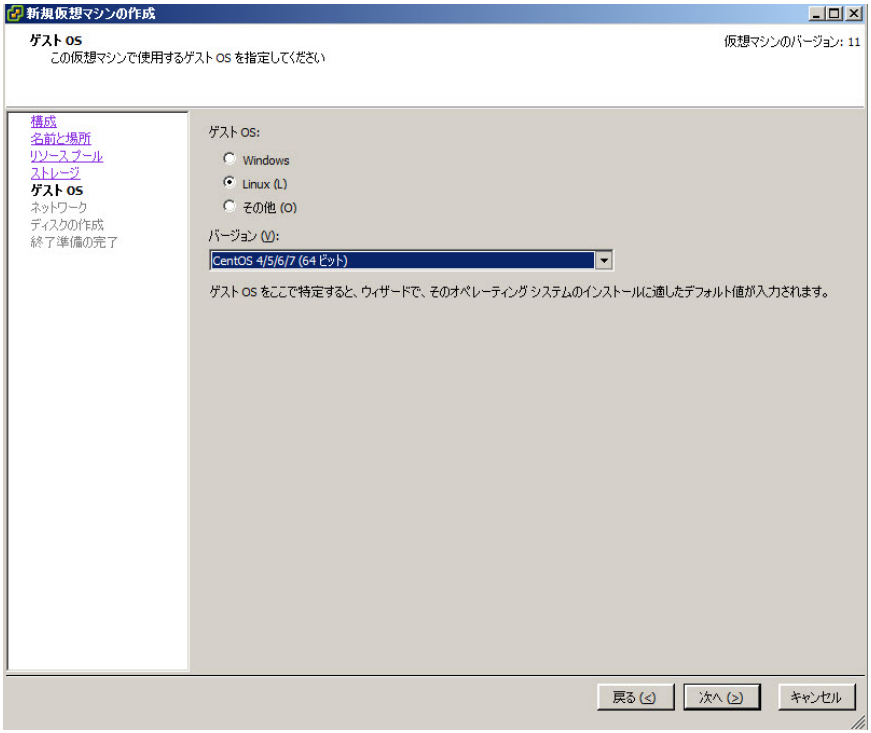


図 B-4. 仮想マシンのゲスト OS

7. ゲスト OS については、[Linux]→[その他の Linux (64 ビット)] または [CentOS 4/5/6/7 (64 ビット)] の順に選択します。
8. [次へ] をクリックします。

[ネットワーク] 画面が表示されます。

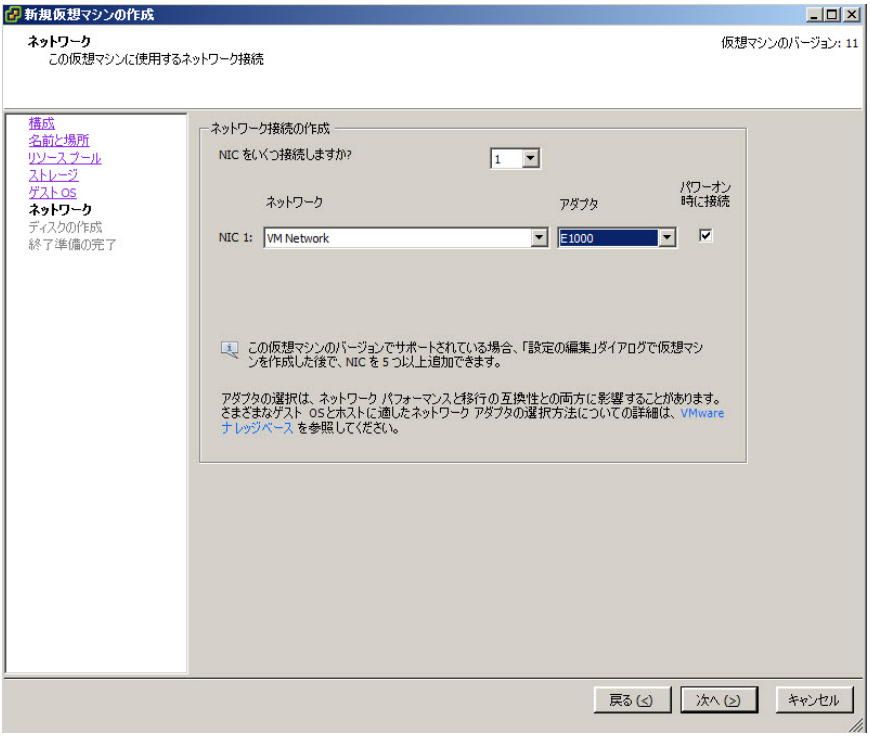


図 B-5. 仮想マシンのネットワーク

9. 初期設定のネットワーク設定を受け入れます。
10. [次へ] をクリックします。

[ディスクの作成] 画面が表示されます。

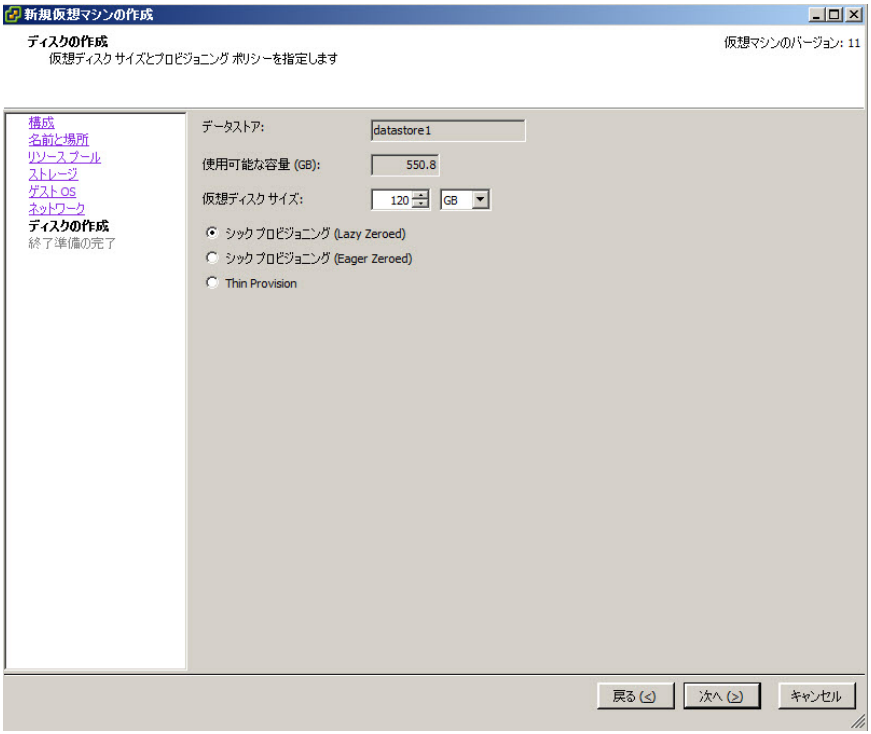


図 B-6. 仮想ディスク容量

11. 120GB 以上のディスク領域を指定します。IMSVA には、120GB 以上のディスク領域が必要です。ディスク領域の割り当てに関する詳細については、弊社の「最新版ダウンロード」サイトにある最新の Readme をご参照ください。

ヒント

メッセージの隔離およびログの記録用に、ディスク領域を 250GB 以上にすることをお勧めします。

---

12. [次へ] をクリックします。

[終了準備の完了] 画面が表示されます。

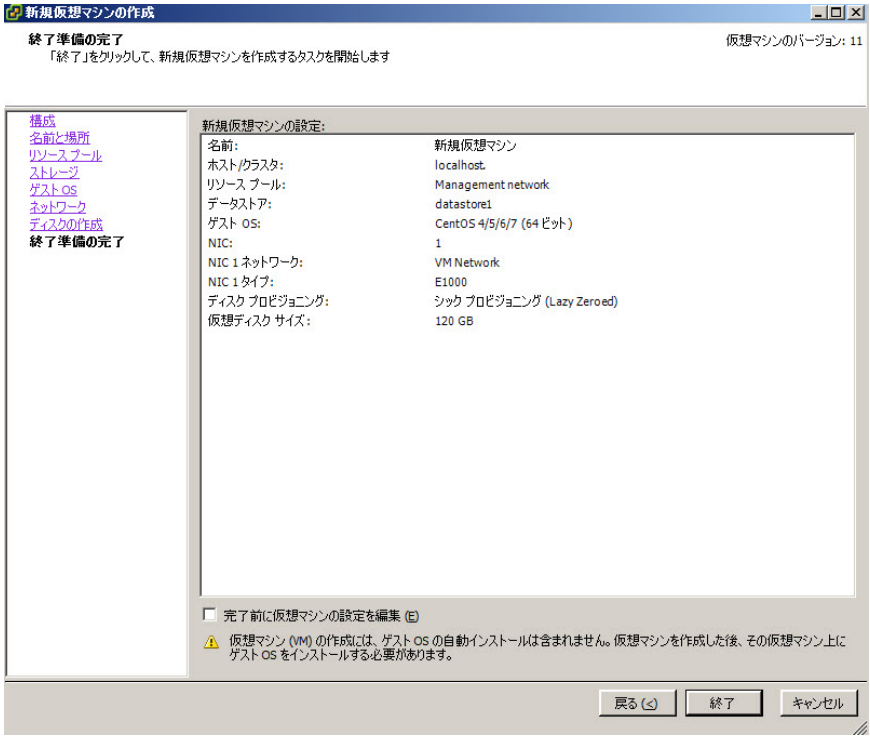


図 B-7. 完了確認

13. [完了] をクリックします。

    システムコンポーネントの設定を修正する場合は、[完了前に仮想マシンの設定を編集] チェックボックスをオンにして [終了] をクリックします。

14. 設定を確認して [終了] をクリックします。

    新しい仮想マシンの準備が完了し、電源がオンになってインストール処理が開始するように設定されました。

付録 C

Microsoft Hyper-V for IMSVA での新しい仮想マシンの作成

この付録では、IMSVA 用の新しい仮想マシンを Microsoft Hyper-V で作成する方法について説明します。

この付録の内容は次のとおりです。

Hyper-V のインストールについて

IMSVA では、Microsoft Hyper-V ベースの仮想プラットフォームでのインストールがサポートされています。この付録では、IMSVA を Hyper-V ベースの仮想マシンにインストールする手順について説明します。本書では、Hyper-V の実際のインストールについては説明しません。Hyper-V のインストールについては、Microsoft 製品のドキュメントを参照してください。この付録に記載されている手順は、IMSVA を Windows Server 2012 R2 Hyper-V サーバにインストールする方法を示しています。

IMSVA での Hyper-V のサポート

IMSVA では、次のプラットフォームで Hyper-V をサポートします。

- Windows Server 2008 R2 SP1
- Windows Server 2012
- Windows Server 2012 R2
- Microsoft Hyper-V Server 2008 R2 SP1
- Microsoft Hyper-V Server 2012 R2

IMSVA を Hyper-V 仮想マシンにインストールする

次の手順に従って、ご使用の環境に仮想マシンを作成してください。CPU や NIC の数、メモリ、およびハードディスク容量を選択する際は、各マシンのデプロイ要件を考慮する必要があります。この手順で入力している値は、説明を目的としたものです。

仮想ネットワーク割り当てを作成する

手順

1. Hyper-V の [サーバー マネージャー] メニューで、[Hyper-V マネージャー] を右クリックします。

メニューが表示されます。

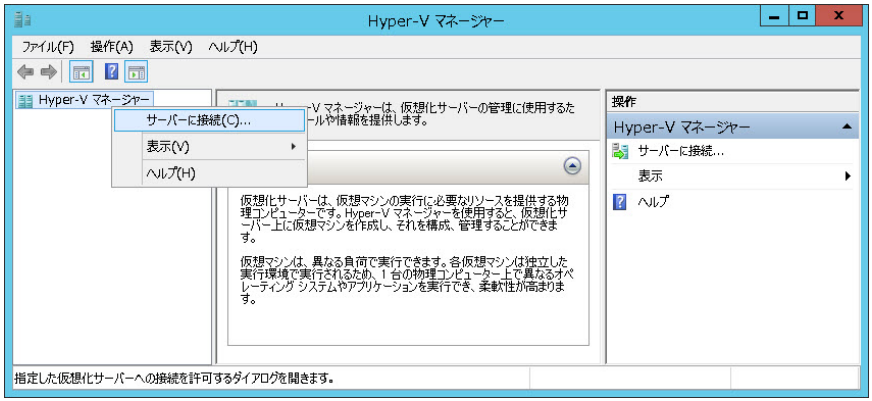


図 C-1. サーバへの接続

2. [サーバーに接続] を選択します。

   接続先の仮想化サーバの場所を選択するダイアログボックスが表示されます。

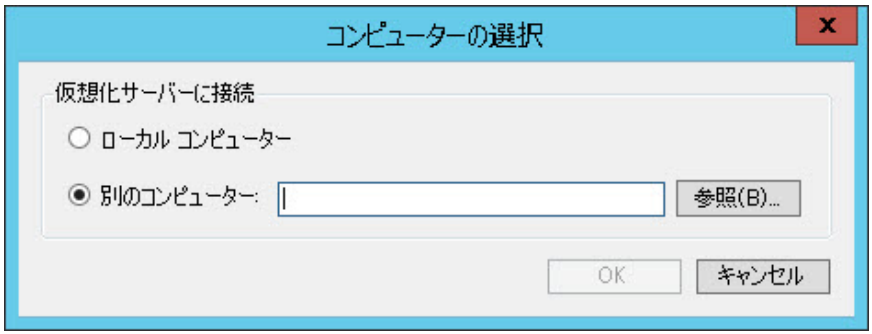


図 C-2. 仮想化サーバの場所

3. 仮想化サーバの場所を指定して、[OK] をクリックします。

4. Windows Server 2012 R2 サーバを右クリックして、[仮想スイッチ マネージャー] を選択します。

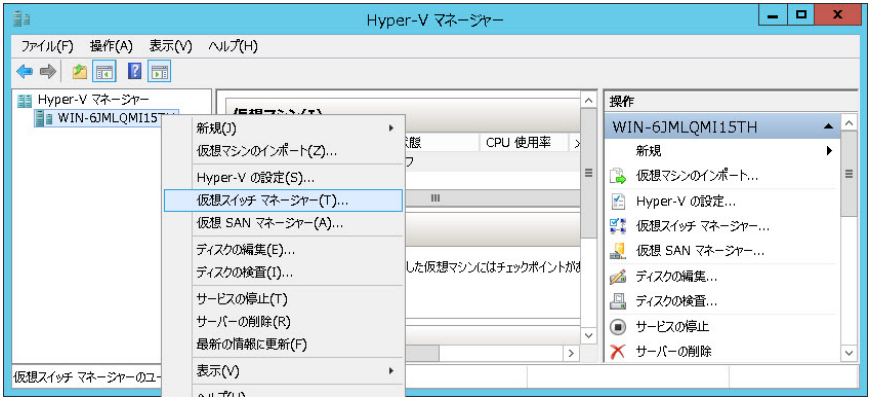


図 C-3. [仮想ネットワーク マネージャー] の選択

5. オプションのリストから [外部] を選択し、[追加] をクリックして新しい仮想ネットワークを作成します。

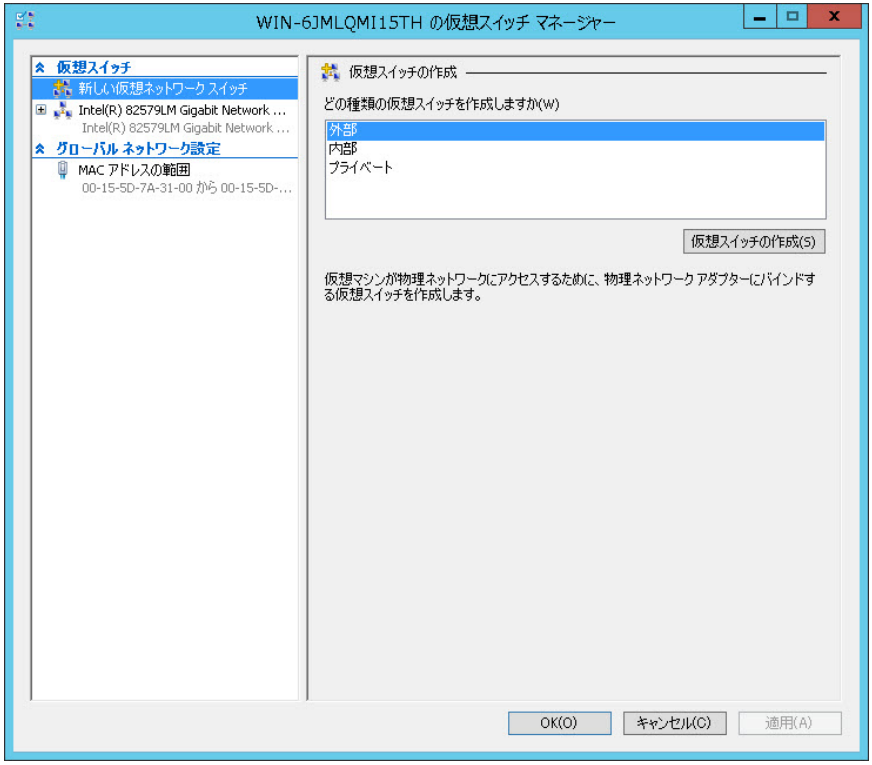


図 C-4. 「外部」仮想ネットワークの追加

6. [外部] ドロップダウンメニューから、接続先の物理ネットワークアダプタを選択します。

注意

この物理アダプタは、ネットワークに接続されており、企業ネットワークやインターネットにアクセスできる必要があります。

Microsoft Windows Server 2012 または Windows Server 2012 R2 で実行する Hyper-V を、Broadcom NetXtreme 1 ギガビットネットワークアダプタ (NetXtreme II ネットワークではない) と併用すると、次の現象が発生することがあります。

- 仮想マシンとネットワークの接続が不規則に切断されることがある。ネットワークアダプタは仮想マシン内で動作しているように見えますが、仮想マシンからネットワークリソースに ping を実行したりアクセスしたりできません。仮想マシンを再起動しても問題は解決されません。
- リモートコンピュータから仮想マシンに ping を実行したり接続したりできない。

これは既知の問題です。詳細については、https://support.microsoft.com/ja-jp/kb/2986895 を参照してください。

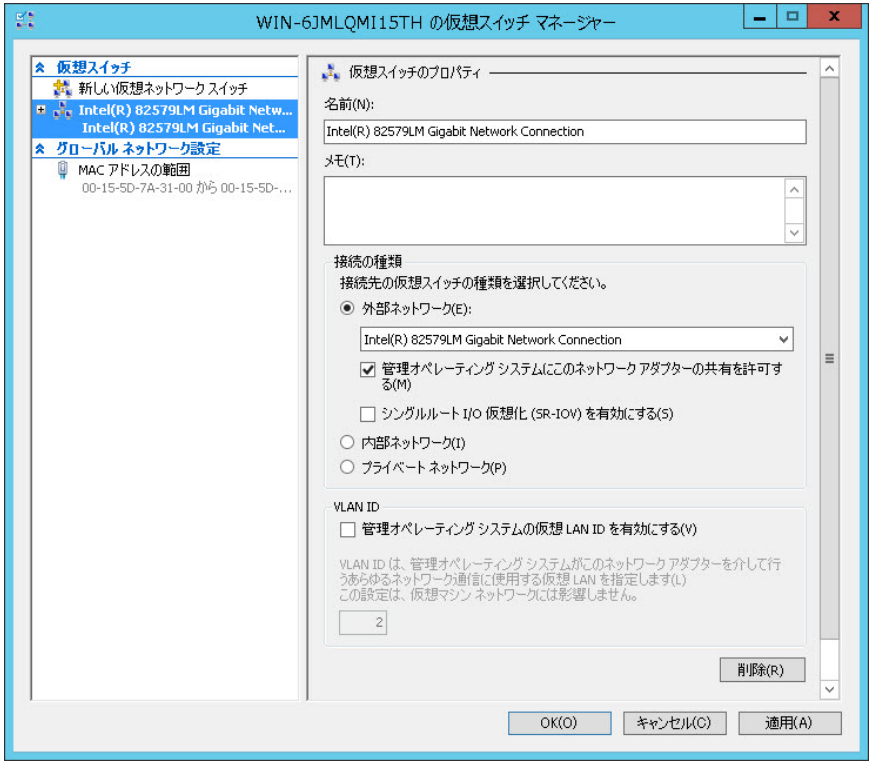


図 C-5. 物理ネットワークアダプタの選択

新しい仮想マシンを作成する

手順

1. Hyper-V の [サーバ マネージャ] メニューで、Windows Server 2012 R2 サーバを右クリックし、[新規] > [仮想マシン] の順に選択します。

[仮想マシンの新規作成ウィザード] が表示されます。

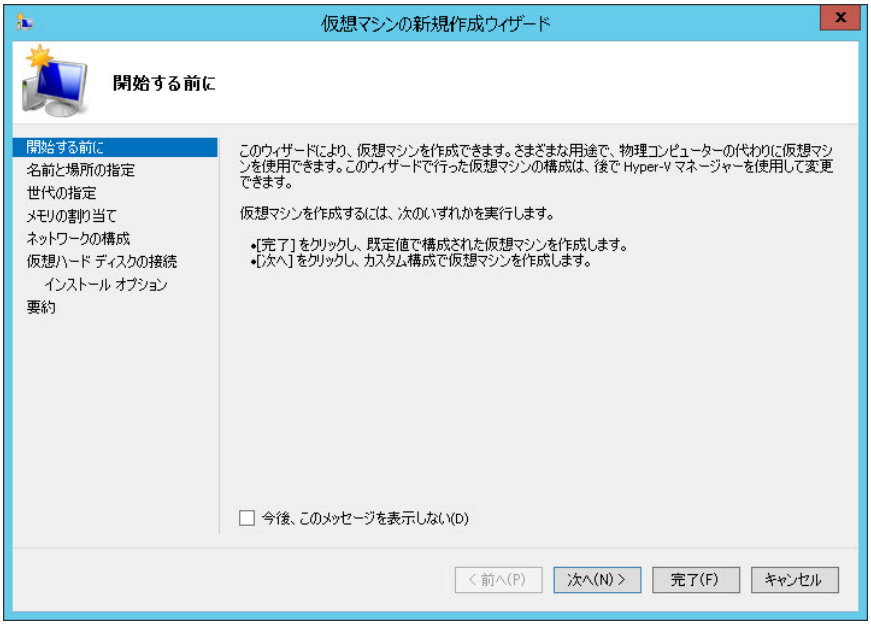


図 C-6. 仮想マシンの新規作成ウィザード

2. [次へ] をクリックします。

[名前と場所の指定] 画面が表示されます。

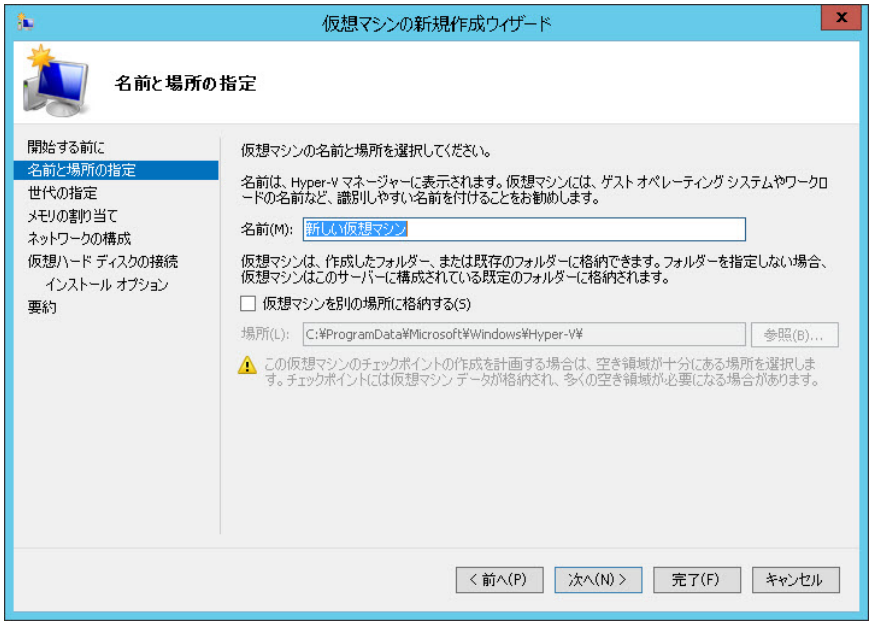


図 C-7. 名前と場所の指定

3. [名前] フィールドに、このコンピュータを識別するための名前を入力します。仮想マシンを別のフォルダに格納する場合は、[仮想マシンを別の場所に格納する] を選択し、正しい場所を指定します。

4. [次へ] をクリックします。

[世代の指定] 画面が表示されます。

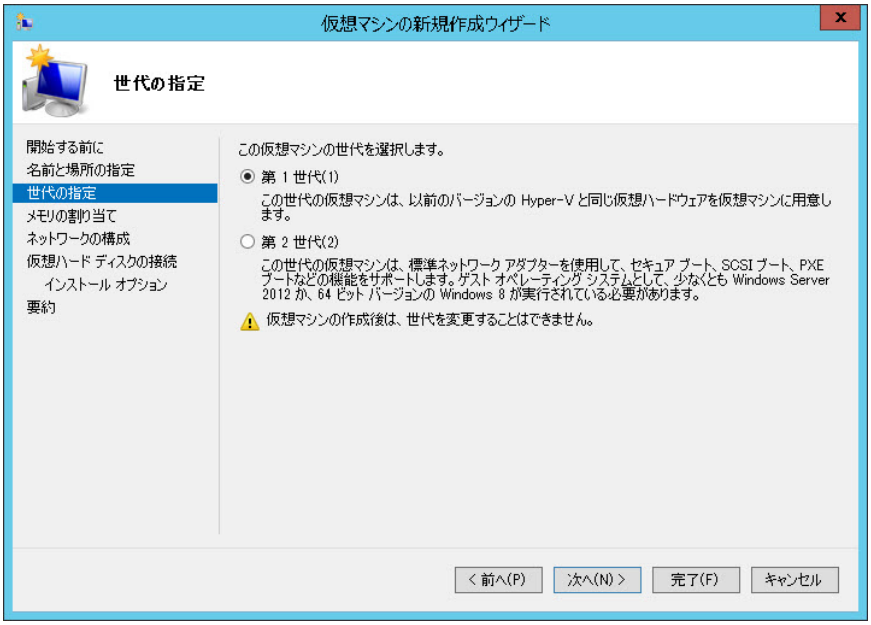


図 C-8. 世代の指定

5. [第 1 世代] を選択し、[次へ] をクリックします。

[メモリの割り当て] 画面が表示されます。

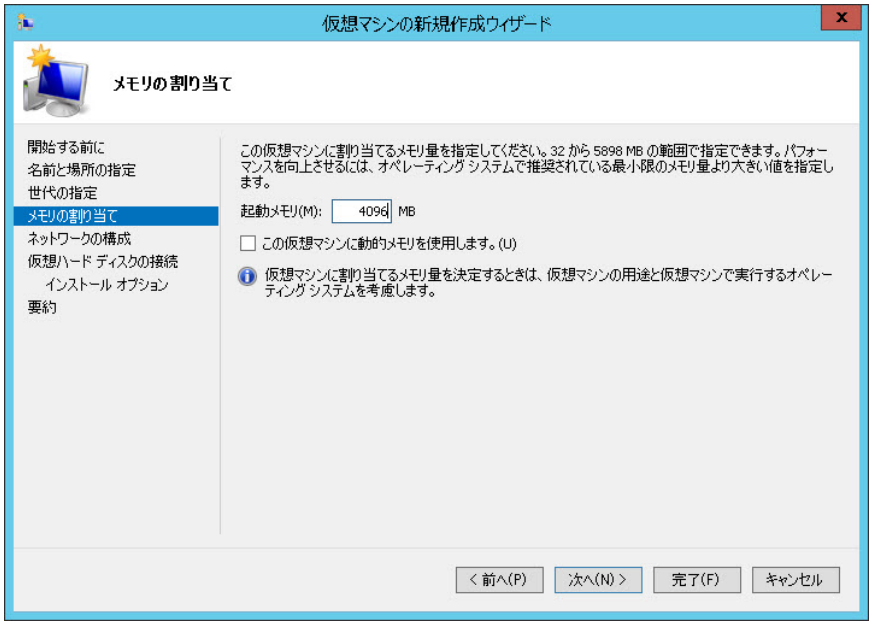


図 C-9. メモリの割り当て

6. IMSVA 用に 4,096MB 以上のメモリを割り当てます。

ヒント

RAM には 8,192MB を割り当てることをお勧めします。

Windows 2008 R2 Hyper-V で使用できる仮想プロセッサの最大数は 4 です。4 を超えるコア CPU および 4,096MB を超えるメモリを追加するには、Hyper-V および IMSVA で `numa=off` に設定します。

---

7. [次へ] をクリックします。

[ネットワークの構成] 画面が表示されます。

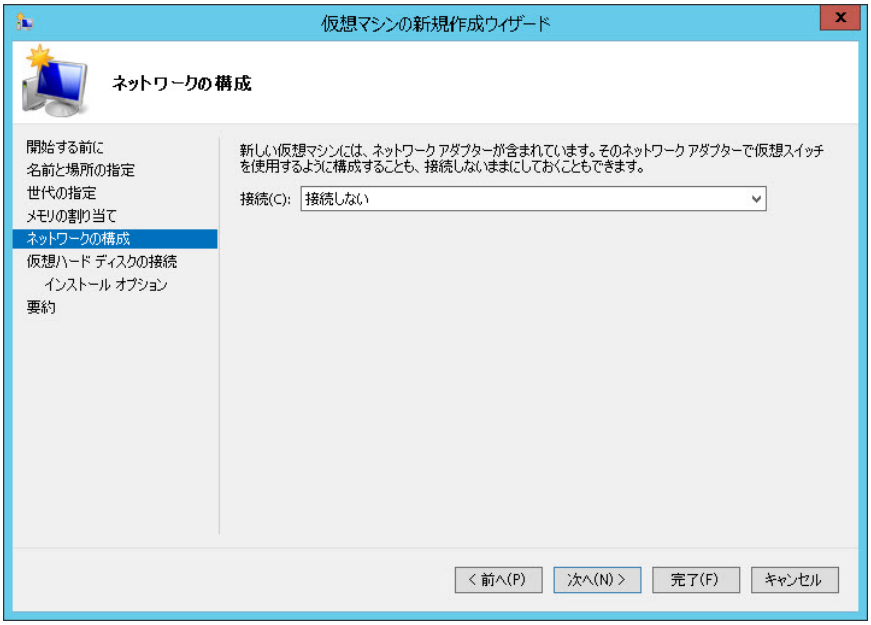


図 C-10. ネットワークの構成

8. 160 ページの「仮想ネットワーク割り当てを作成する」で作成した仮想ネットワークを選択します。

9. [次へ] をクリックします。

[仮想ハードディスクの接続] 画面が表示されます。

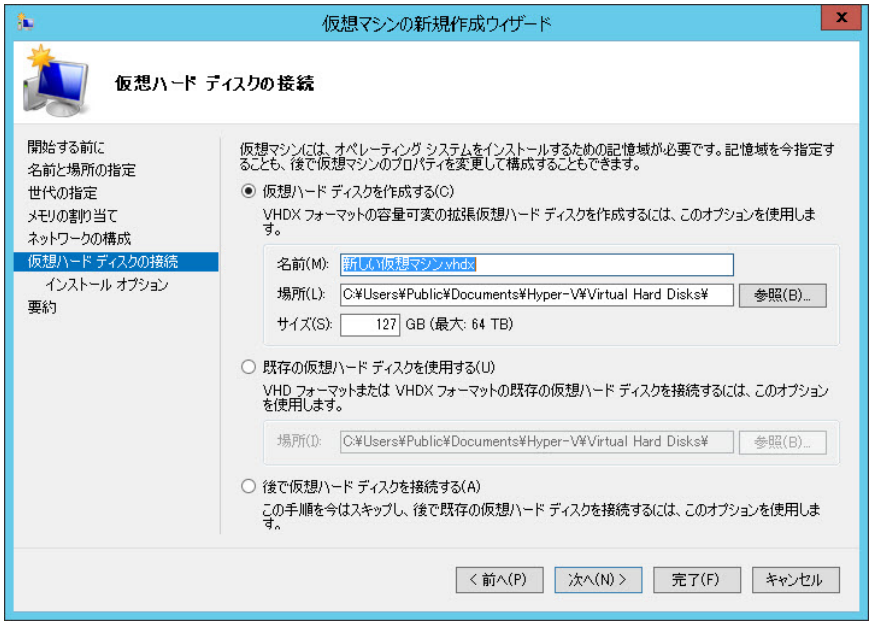


図 C-11. 仮想ハードディスクの接続

10. IMSVA 用に 120GB 以上のディスク領域を指定します。

ヒント

メッセージの隔離およびログの記録用に、ディスク領域を 250GB 以上にすることをお勧めします。

---

11. 仮想ハードディスクを格納する場所を指定して、[次へ] をクリックします。

[インストール オプション] 画面が表示されます。

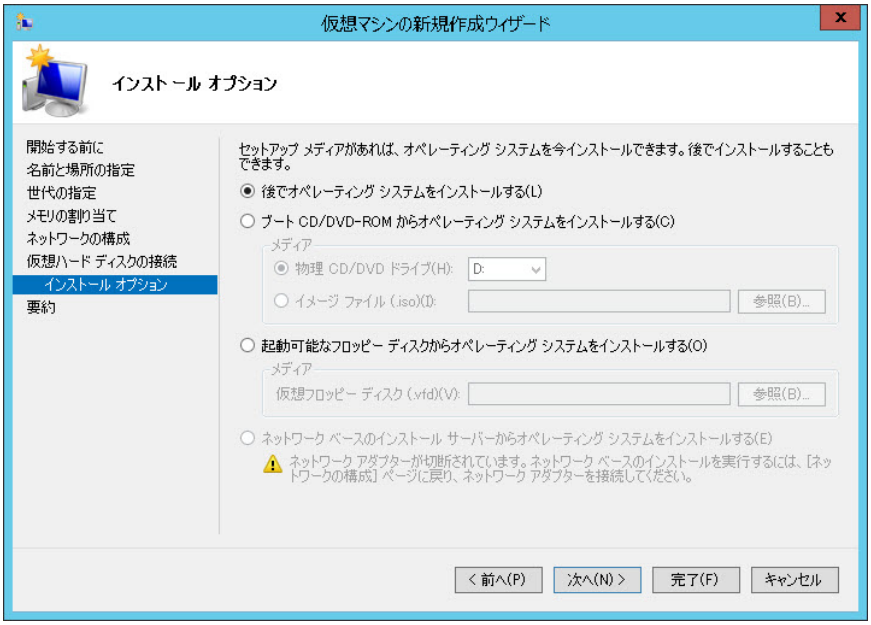


図 C-12. インストールオプション

12. [ブート CD/DVD-ROM からオペレーティングシステムをインストールする] をクリックし、IMSVA 用のインストール ISO ファイルを指定して、[次へ] をクリックします。

[仮想マシンの新規作成ウィザードの完了] 画面が表示されます。

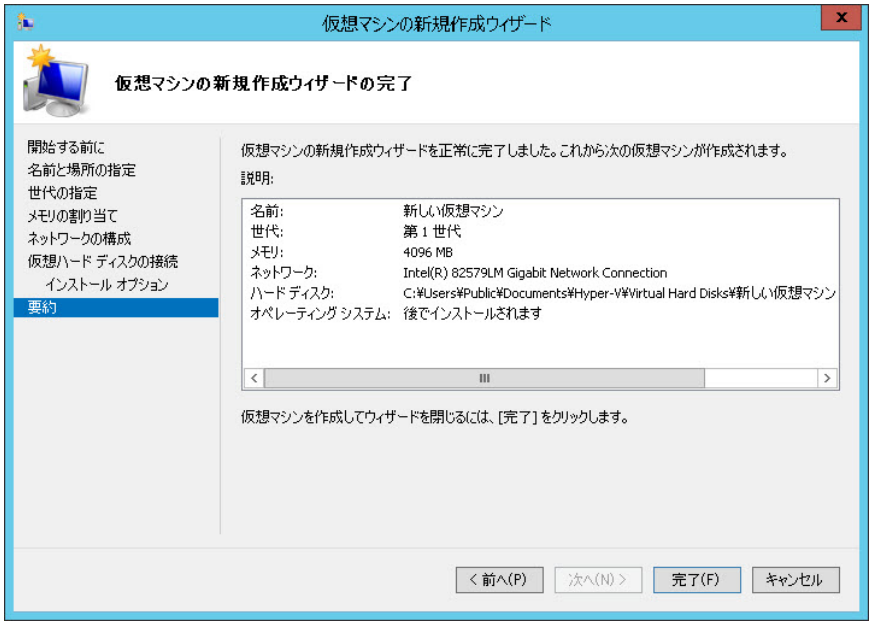


図 C-13. 仮想マシンの新規作成ウィザードの完了

13. 設定を確認して [完了] をクリックします。

    これで、仮想マシンの電源をオンにしてインストール処理を開始する準備が完了しました。

索引

アルファベット

あ

か

さ

た

は

ま

や

ら