InterScan Web Security Virtual Appliance™ 6.5 Service Pack 3

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。

著作権について

商標について

P/N: IBEM67230/150925_JP_R6（2023/11）

目次

はじめに

はじめに

InterScan Web Security Virtual Appliance 6.5 SP3（以下、IWSVA）へようこそ。本書では、IWSVA を紹介し、配置、インストール、移行（必要に応じて）、初期設定、トラブルシューティング、パフォーマンス調整、およびインストール後の主な設定の各作業について説明することで、導入と運用を支援します。また、害のないテストウイルスを使用した設置のテスト、トラブルシューティング、サポートへの問い合わせについても説明しています。

本章では、次の項目について説明します。

対象読者

このドキュメントは、企業の IT 管理者およびシステム管理者を対象として書かれています。本書は、次の項目に関する詳しい内容とネットワークの知識を持つユーザを対象としています。

- HTTP、HTTPS、FTP および企業で使用されているその他のプロトコル
- VMware ESX にインストールする場合は VMware ESX の管理経験、および Hyper-V 仮想プラットフォームにインストールする場合は Microsoft Hyper-V の使用経験

本書の使用方法

本書には、IWSVA を理解して使用するために必要な情報が記載されています。

上級ユーザの方は、第 3 章「InterScan Web Security Virtual Appliance のインストール」を直接参照できます。VMware ESX に IWSVA をインストールする場合は、付録 E「VMware ESX 下での IWSVA 用の新しい仮想マシンの作成」を参照してください。Microsoft Hyper-V に IWSVA をインストールする場合は、付録 F「Microsoft Hyper-V 下での IWSVA 用の新しい仮想マシンの作成」を参照してください。

第 1 章「インストール計画」	この章では、IWSVA のインストール前に実行が必要な作業について説明します。これには、ネットワークトラフィック、HTTP サービスフロー、および FTP サービスフローの計画と、サーバが特定の要件を満たしていることの確認が含まれます。
第 2 章「配置について」	この章では、IWSVA をインストールして、HTTP サービスフローと FTP サービスフローに伴うサーバ配置とネットワーク保護の計画に役立つ多様なトポロジの概要が記載されています。
第 3 章「InterScan Web Security Virtual Appliance のインストール」	この章では、IWSVA の体験版と製品版の入手方法とアプリケーションのインストール方法について説明します。
第 4 章「InterScan Web Security Virtual Appliance への移行」	この章では、多様な移行シナリオと IWSVA への移行方法について説明します。
付録 A「導入の統合」	この付録では、多様な技術に関連して、IWSVA の配置シナリオについて説明します。多様な技術の例には、LDAP、WCCP 対応の Cisco 製ルータ、ICAP、透過ブリッジなどがあります。

付録 B「調整とトラブルシューティング」	この付録では、URL フィルタと LDAP に関するパフォーマンス調整について説明します。また、一般的なトラブルシューティングのヒント、およびインストールや機能に関して発生する場合がある問題についても説明します。
付録 C「IWSVA のインストールと配置のベストプラクティス」	この付録では、IWSVA において推奨されるインストールと配置のベストプラクティスについて説明します。
付録 D「テクニカルサポート」	この付録では、保守契約とトレンドマイクロのサポートセンターの役割について説明します。
付録 E「VMware ESX 下での IWSVA 用の新しい仮想マシンの作成」	この付録では、VMware ESX 下での IWSVA 用の新しい仮想マシンの作成方法について説明します。
付録 F「Microsoft Hyper-V 下での IWSVA 用の新しい仮想マシンの作成」	この付録では、Microsoft Hyper-V 下での IWSVA 用の新しい仮想マシンの作成方法について説明します。

IWSVA のドキュメント

IWSVA 6.5 SP3 インストールガイドのほかに、次のドキュメントがあります。

- **管理者ガイド** — IWSVA の設定オプションについて詳細な情報が記載されています。ソフトウェアをアップデートして最新のリスクから保護する方法、セキュリティ上の目標を達成するためのポリシーの設定および使用方法、ログとレポートの使用方法に関する項目が含まれています。
- Readme **ファイル** — オンラインヘルプやマニュアルには存在しない最新の製品情報が記載されています。新機能、使用上の注意点、既知の問題などの説明が含まれています。

  各種ドキュメントの最新版は、次の Web サイトから入手できます。

  https://www.trendmicro.com/ja_jp/business/products/downloads.html

  オンラインヘルプ — ユーザインタフェースを使用して IWSVA を設定する方法を確認できます。Web 管理コンソールを開いて、ヘルプアイコンをクリックすると、オンラインヘルプにアクセスできます。オンラインヘルプは、製品の主なタスクの操作手順、利用方法のアドバイス、および実際に使用する場面にさまざまな情報を提供します。オンラインヘルプの情報には、有効なパラメータ範囲や最適値などが存在します。オンラインヘルプには、IWSVA の管理コンソールからアクセスできます。

ドキュメントの表記規則

このドキュメントでは、次の表記規則を使用しています。

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

表 1. **本書で使用している表記規則**

第 1 章

インストール計画

本章で説明する内容には、次の項目が含まれます。

- 14 ページの「システム要件」
- 15 ページの「IWSVA のインストールに必要な情報」
- 17 ページの「ネットワークトラフィック保護を計画する」

システム要件

最新の情報については、次の Web サイトを参照してください。

http://www.go-tm.jp/iwsva/req

注意： システム要件に記載されている OS の種類やハードディスク容量などは、OS のサポート終了、弊社製品の改良などの理由により、予告なく変更される場合があります。

インストール対象コンポーネント

インストール時、次のコンポーネントは自動的にインストールされます。

- **メインプログラム** — 管理コンソールと、IWSVA に必要な基本ライブラリファイルです。
- **アプリケーション制御** — プロトコルによるアプリケーション使用率を管理するためのサービスです。
- **高度な脅威保護** — ICAP または HTTP プロキシによる HTTP 検索および URL ブロックに必要なサービスです。
- **FTP 検索** — FTP 検索に必要なサービスです。
- **URL フィルタ** — URL フィルタに必要なサービスです（初期設定で有効)。
- **SNMP 通知** — SNMP 準拠のネットワーク管理ソフトウェアに SNMP トラップを送信するサービスです。
- **IWSVA 用 Trend Micro Control Manager エージェント** — Trend Micro Control Manager（以下、Control Manager) または Trend Micro Apex Central（以下、Apex Central) への登録に必要なコンポーネントです。Control Manager または Apex Central（トレンドマイクロの集中管理コンソール) を使用する場合は、このエージェントが必要です。
- **情報漏えい対策** — 組織の機密データを含むコンテンツの送信トラフィックを検索するサービスです。
- **コマンドラインインタフェース** — TTY または SSH を使用してコマンドラインから IWSVA を管理するためのカスタム CLI シェルです。

インストール中に次のアプリケーションがインストールされますが、初期設定で有効にはなりません。

- Apache Traffic Server（ATS)

IWSVA のインストールに必要な情報

IWSVA を購入するか、または 30 日間体験版をダウンロードできます。30 日間体験版では、IWSVA の機能がすべて提供されています。

IWSVA のセットアッププログラムでは、インストール時に選択したオプションに応じて、必要な情報の入力を求められます。

はじめに、実行するインストールのタイプを決定します。

- 新たにインストールする新規のお客さまの場合は、製品配置のアドバイスが記載された第 2 章 21 ページの「配置について」と、第 3 章 55 ページの「InterScan Web Security Virtual Appliance のインストール」を参照してください。
- IWSVA6.5 SP2 または他の IWSVA 6.5 SP3 から移行する場合は、データの移行について第 4 章 65 ページの「InterScan Web Security Virtual Appliance への移行」を参照してください。

新規インストール

IWSVA 6.5 SP3 では、新規インストールがサポートされます。新規インストールプロセスでは、IWSVA をインストールするように既存のシステムが初期化されます (56 ページの「IWSVA のインストール」を参照)。

移行

IWSVA 6.5 SP3 では、次のトレンドマイクロ製品からの既存の設定とポリシーデータの移行がサポートされています。

- InterScan Web Security Virtual Appliance 6.5 SP2 (同じ言語バージョン)

移行の詳細については、第 4 章「InterScan Web Security Virtual Appliance への移行」を参照してください。

注意： InterScan Web Security Suite からの移行はサポートされておりません。

プロキシ設定の種類

IWSVA は、複数の配信モードをサポートします。

- クライアントが直接 IWSVA に接続するプロキシ転送

- 既存の内部プロキシサーバへの上位プロキシ
- 既存の ICAP 1.0 準拠キャッシュコントローラへの ICAP サーバ
- ファイアウォールの設定済み WCCP 対応ルータへの WCCP クライアント
- 透過ブリッジモード
- Web サーバを保護するためのリバースプロキシ
- 通常の透過

配置は、IWSVA のインストール後に設定され、Web 管理コンソールの配置ウィザードを使用して変更できます。IWSVA によってサポートされている透過ブリッジセグメントごとに 2 枚ずつのネットワークインタフェースカードが必要です。25 ページの「HTTP フローを計画する」および 27 ページの「FTP フローを計画する」を参照してください。

Trend Micro Control Manager サーバ情報

Control Manager または Apex Central の登録は、IWSVA のインストール完了後に IWSVA Web 管理コンソール経由で行います。

データベースの種類と場所

IWSVA では、ポリシー、ルール、各種設定で、PostgreSQL データベースを使用します。ローカル PostgreSQL インストールが、IWSVA のインストール中に実行されます。

SNMP 通知

SNMP 通知の使用を予定している場合は、IWSVA のセットアッププログラムによって適切な SNMP ライブラリがインストールされます。

Web 管理コンソールのパスワード

IWSVA Web 管理コンソール (https://<IWSVA 6.5 の IP アドレス >:8443) へのアクセスは、初期設定のユーザ名「admin」で管理されます。初期パスワードは「adminIWSS85」です。

ヒント： セキュリティ上の理由から、Web 管理コンソールへの初回ログイン後に、admin パスワードを変更することをお勧めします。

ヒント： OS アカウント「root」、CLI アカウント「enable」、および IWSVA アカウント「admin」のパスワードは、いずれも初期設定で「adminIWSS85」です。IWSVA 管理者が、それぞれ異なるパスワードに変更できます。詳細については、「管理者ガイド」の「管理コンソールパスワードの変更」を参照してください。

コマンドラインによるアクセス

IWSVA ではコマンドラインインタフェース (CLI) が用意されています。このため、業界標準の CLI 構文を使用してアプライアンスの設定ができます。CLI では、IWSVA の管理、保守を実行するためのコマンドや機能があります。CLI には、ローカルコンソールのキーボードとモニタを使用してアクセスできます。また、SSHv2 経由でリモートでもアクセスできます。

IWSVA とインターネット間のプロキシ

IWSVA とインターネットとの間にプロキシを配置する場合、トレンドマイクロからのアップデートを受信するように IWSVA のプロキシ設定が必要です。メニューから、[アップデート] → [接続設定] の順に選択して、上位プロキシ設定を実行します。詳細については、「管理者ガイド」の「プロキシ設定 (アップデート用)」を参照してください。

アクティベーションコード

IWSVA を構成するモジュールである、メインプログラム (URL フィルタを含む)、情報漏えい対策 (DLP) をアクティベーションするには、個別のアクティベーションコードが必要です。

ネットワークトラフィック保護を計画する

IWSVA は、ネットワークの保護に役立つ多様なモードで配置ができます (第 2 章「配置について」を参照)。IWSVA では、次の配置トポロジがサポートされています。

- 18 ページの「透過ブリッジモード」
- 18 ページの「プロキシ転送モード」
- 19 ページの「リバースプロキシモード」
- 19 ページの「ICAP モード」
- 19 ページの「通常の透過モード」

- 19 ページの「WCCP モード」

透過ブリッジモード

IWSVA は、ルータやスイッチなどのネットワークデバイス間のブリッジとして機能します。IWSVA は、通過する HTTP および FTP トラフィックを検索し、その際に使用ブラウザ、またはネットワークの設定を変更する必要はありません。これは、両方向のトラフィックを検索する最も簡単な配信モードです。

この配信モードでは、追加要件として IWSVA で保護される透過ブリッジセグメントごとに 2 枚のネットワークインタフェースカードが必要です。この配信モードでは、最大限の互換性を確保するために、次のネットワークカードの使用をお勧めします。

- Broadcom NetXtreme シリーズ
- Intel Pro/1000 PT Dual Port Server Adapter
- Intel Pro/1000 MF Dual Port Fiber

IWSVA 6.5 SP3 には、オプションの高可用性 (HA) 配信モードが搭載されています。このモードでは、2 つの IWSVA 6.5 SP3 ノードが 1 つの HA クラスタとして設定されます。この設定では、一方のノードが上位、つまりアクティブノードとして指定され、「接続ステータス」リンクを介して、下位、つまりパッシブノードに接続されます。

HA 配信モードでは、上位ノードがすべてのトラフィックを処理し、下位ノードはパッシブ状態になっています。上位ノードでエラーが検出されると、下位ノードがアクティブノードになり、上位ノードはオフラインになります。

HA 配信モードは、透過ブリッジモードでのみサポートされます。

透過ブリッジモードの詳細については、51 ページの「透過ブリッジモードで配置する」を参照してください。

プロキシ転送モード

IWSVA は、ネットワーククライアントの上位プロキシとして機能します。トラフィックを IWSVA にリダイレクトするように、クライアントのブラウザを設定する必要があります。IWSVA は HTTP トラフィックと FTP トラフィックを検索するため、別の専用プロキシサーバを用意する必要がありません。入出力方向の両方でコンテンツの検索が実行されます。

また、プロキシ転送モードはすべてのトラフィックを別の上位プロキシサーバへ転送することも可能です。

プロキシ転送モードの詳細については、30 ページの「プロキシ転送モードで配置する」を参照してください。

リバースプロキシモード

IWSVA が Web サーバの直前に配置されます。IWSVA は、Web サーバにアップロードされるクライアントの HTTP、HTTPS、および FTP コンテンツと、Web サーバからクライアントにダウンロードされるコンテンツを検索し、Web サーバの安全性を確保します。

リバースプロキシモードの詳細については、48 ページの「リバースプロキシモードで配置する」を参照してください。

ICAP モード

IWSVA は、ICAP プロキシとして機能します。これによって、ICAP v1.0 準拠のキャッシュサーバからの ICAP 接続を受信します。キャッシュサーバは、キャッシュされたコンテンツをローカルに処理するため、全体的な帯域幅要件を削減し、待ち時間を短縮するのに役立ちます。IWSVA は、キャッシュサーバおよびクライアントに返されるすべてのコンテンツを検索し、安全性を確保します。

ICAP モードの詳細については、42 ページの「ICAP モードで配置する」を参照してください。

通常の透過モード

IWSVA のプロキシ転送モードは、一般的なレイヤ 4 負荷分散スイッチを使用した通常の透過をサポートしており、クライアントのブラウザ設定を変更することなく HTTP 検索を実行できます。

通常の透過モードの詳細については、36 ページの「通常の透過モードの HTTP プロキシ」を参照してください。

WCCP モード

IWSVA は、Cisco の WCCP プロトコルを使用して、クライアントの設定を変更することなく、Web トラフィックと FTP トラックのコンテンツ検索を実行できます。これにより、ハードウェアを追加することなくアーキテクチャの冗長性と商品性を高めることができます。

WCCP モードの詳細については、41 ページの「WCCP モードで配置する」を参照してください。

第 2 章

配置について

本章で説明する内容には、次の項目が含まれます。

サーバの設置場所を確認する

InterScan Web Security Virtual Appliance 6.5（以下、IWSVA）をインストールする前に、IWSVA の配信モードを確認し、IWSVA をネットワーク環境にインストールしてニーズを満たす最良の方法を決定する必要があります。これには、ネットワーク上の IWSVA サーバの配置場所と、ネットワークに最適な配信モードの特定が含まれます。

今日の企業向けネットワークトポロジは、通常、次の 2 つのカテゴリのいずれかに該当します。

- DMZ を備えた 2 つのファイアウォールのトポロジ
- DMZ を備えていない 1 つのファイアウォールのトポロジ

IWSVA サーバの理想的な配置場所は、使用しているトポロジによって異なります。

DMZ を備えた 2 つのファイアウォールのトポロジ

今日のセキュリティ上の問題を考慮して、多くの組織では 2 つのファイアウォール（外部用と内部用）で構成されたトポロジが実装されています。この 2 つのファイアウォールによって、ネットワークは 2 つの主要領域に分割されます。

- DMZ — DMZ は外部ファイアウォールと内部ファイアウォールの間に配置されます。この領域に常駐するホストは、外部から組織のネットワークへの接続を受け入れます。外部ファイアウォールの設定によって、外部コンピュータからのパケットは DMZ 内のサーバにのみ到達します。

- **企業 LAN** — これらのセグメントは、内部ファイアウォールの内側に配置されます。内部ファイアウォールの設定により、DMZ 内のコンピュータから発信されているトラフィックのみ、企業 LAN のコンピュータに渡されます。

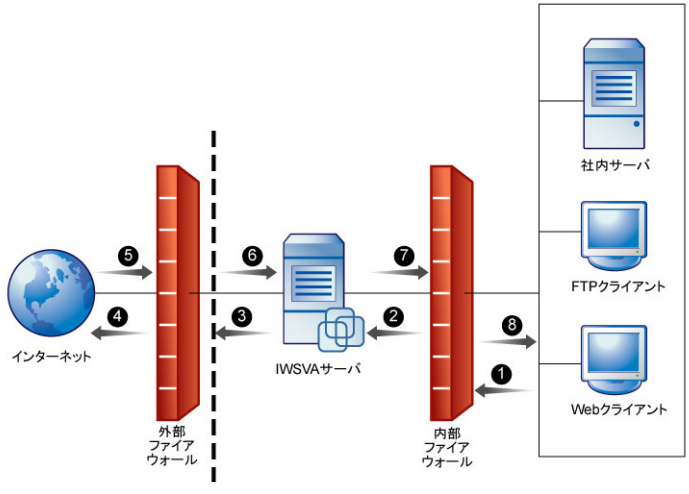


図 2-1.　DMZ を備えた 2 つのファイアウォールのトポロジ

このトポロジでは、インターネット上にあるサーバなどの外部サーバから発信されたデータはすべて、DMZ 内のサーバを介して渡される必要があります。特定の種類のデータ (HTTP や FTP のパケットなど) が内部セグメントから発信される場合にも、DMZ 内のサーバを経由して接続される必要があります。このため、IWSVA などのプロキシが強制的に使用されます。

DMZ を備えていない 1 つのファイアウォールのトポロジ

組織のファイアウォールには、DMZ を備えていないものもあります。「DMZ なし」トポロジを使用する際には、IWSVA サーバをファイアウォールの内側に配置します。

- IWSVA サーバは企業の LAN から切り離されていません。このため、外部のコンピュータと企業の LAN 上のコンピュータとの間におけるホップの数は、DMZ がある場合より 1 つ少なくなります。この場合、図のように、要求の処理には発信 1 つと着信 1 つの 2 ステップが少なくなります。

- このファイアウォールの設定によって、企業の LAN 上のコンピュータへの接続が許可されます。セキュリティのために、LAN 上のコンピュータに到達できるデータの種類をファイアウォールで制限する必要があります。たとえば、インターネットからの HTTP データが IWSVA サーバにのみ到達できるようにファイアウォールを設定します。

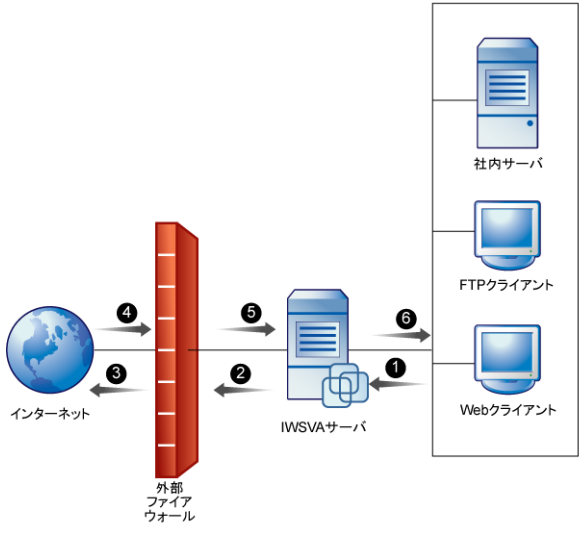


図 2-2.　DMZ を備えていない 1 つのファイアウォールのトポロジ

ネットワークトラフィックフローを計画する

保護するために、ネットワークトラフィックを IWSVA 経由で送信する方法は、次を含め数通りあります。

- プロキシとして IWSVA をポイントするようにクライアントを再設定する
- レイヤ 4 スイッチを使用する
- ICAP 対応のプロキシを使用して選択したトラフィックを検索対象としてリダイレクトする
- WCCP を使用して選択したトラフィックを検索対象として送信する
- 別のプロキシおよびキャッシングデバイス、またはどちらか一方からのトラフィックを転送する

詳細については、付録 A の 71 ページの「導入の統合」を参照してください。

それぞれのネットワークトラフィックフロー設定は、IWSVA の設定、ネットワークの設定、およびネットワークセキュリティに影響します。

ネットワークトラフィックのフロー計画を作成するには、次のことが必要です。

- 各 IWSVA サービスの目的と機能を理解します。
- 各サービスの有効なデータ送信元を決定します。たとえば、HTTP サービスが HTTP ブラウザから要求を直接受信するのか、ICAP プロキシデバイス経由で間接的に受信するのかなどについて決定します。
- サービスに使用するポートを決定します。たとえば、初期設定では、HTTP プロキシサービスにはポート 8080、FTP サービスにはポート 21 が使用されます。ただし、他のアプリケーションやサービスでポート 8080 が使用される場合、別のポートを使用するように HTTP サービスを設定する必要があります。
- 各サービスの有効なデータ送信先を決定します。たとえば、HTTP プロキシサービスが検証済み要求を直接 Web サイトに送信するのか、上位 HTTP プロキシに送信するのかなどについて決定します。
- サービス固有の考慮事項があれば追加します。たとえば、HTTP サービスフローには ICAP デバイスを含めても、FTP サービスフローには含めないなどについて検討します。
- IWSVA を使用してすべてのポートのトラフィックを監視する場合は、透過ブリッジモードの間、IWSVA の上位スイッチのすべてのトラフィックが、必ず、IWSVA を経由するようにします。

前述の情報を収集すると、管理者はインストールに使用可能な中で最適なフローを決定できます。

HTTP フローを計画する

IWSVA の用途が HTTP トラフィックのフィルタリングに限定される場合は、次の配信モードオプションを検討してください。

- HTTP プロキシ
- ICAP デバイス
- WCCP デバイス
- 透過ブリッジ
- 通常の透過
- リバースプロキシ

ICAP デバイスや WCCP デバイスを使用するフローは、使用しない場合と比較してフローが大きく異なります。

使用可能な配信モードは 7 種類あります。

透過ブリッジ設定

- **透過ブリッジモード** — 透過ブリッジモードは、クライアントのコンピュータがプロキシとして IWSVA サーバを使用するように設定されていないが、IWSVA 経由でインターネットに接続する必要がある場合に使用します。このモードでは、HTTP/HTTPS および FTP を含むすべてのネットワークトラフィックを IWSVA が認識できます。
- **透過ブリッジ高可用性 (HA) モード**– このモードは、2 つの IWSVA デバイスをクラスタとして設定し、IWSVA クラスタメンバーの一方にエラーが生じても継続したサービスを提供できるようにする場合に使用します。

プロキシ転送設定の場合 :

- **スタンドアロンモード** — ICAP デバイスを使用せず、IWSVA を直接インターネットに接続する場合、このフローを使用します。
- **依存モード** — ICAP デバイスを使用せず、IWSVA を別の HTTP プロキシ経由でインターネットに接続する必要がある (直接接続できないため) 場合、このフローを使用します。これは、次の 3 通りのいずれかで実現できます。
  - プロキシを IWSVA の外側に配置するモード
  - プロキシを IWSVA の内側に配置するモード (非推奨)
  - 二重プロキシモード
- **通常の透過モード** — このモードは、L4 (負荷分散) スイッチを使用している場合に使用します。
- WCCP **モード** — WCCP プロトコルを使用して WCCP 対応デバイスと IWSVA を連動させます。

リバースプロキシ設定の場合 :

- **リバースプロキシモード** — このフローは、HTTP プロキシをインターネットと Web サーバの間に配置して、プロキシサーバで Web サーバを保護する場合に使用します。ISP や ASP では、アップロードトラフィックをウイルスから保護するためにこのフローを使用します。また、複雑な Web サイトを持つ組織では、アクセスを管理するために使用します。

ICAP プロキシ設定の場合 :

- ICAP **モード** — ICAP モードは、IWSVA と ICAP デバイスを併用する場合に使用します。

HTTPS 復号

IWSVA は、不正プログラムや URL アクセスポリシー違反がないかどうか、暗号化されたコンテンツを復号して検査することで、HTTPS のセキュリティホール（セキュリティの抜け穴）をふさぎます。選択した Web カテゴリの HTTPS トラフィックを復号するようにポリシーを定義できます。復号の際、データは HTTP トラフィックと同じ方法で扱われ、URL フィルタおよび検索のルールを適用可能です。

IWSVA では、次のモードで HTTPS 復号および検索がサポートされています。

- 透過ブリッジ
- WCCP
- プロキシ転送
- リバースプロキシ

FTP フローを計画する

FTP に使用できるフローには、スタンドアロンモードと依存モードの 2 種類があります。これらは HTTP サービスのスタンドアロンモードと依存モードのフローに類似しています。それぞれ必要な設定が異なり、固有の考慮事項があります。

- **スタンドアロンモード** — IWSVA サーバは、要求元クライアントとリモートサイト間の FTP プロキシサーバとして機能し、すべてのトランザクションを仲介します。
- **依存モード** — IWSVA は、LAN 内で別の FTP プロキシサーバと連携して動作します。

スタンドアロンモードの FTP プロキシ

LAN 内外からの FTP トラフィックをすべて検索するには、すべての接続を「仲介」するように FTP クライアントを設定します。この場合、クライアントは IWSVA サーバに FTP 接続を実行し、目的のサイトにログオン認証情報を渡します。これによって、IWSVA FTP サーバが目的のサイトに接続できるようになります。リモートサイトはファイルを IWSVA FTP に転送します。ファイルを要求元クライアントに配信する前に、IWSVA FTP サーバはファイルを検索し、ウイルスなどのセキュリティリスクがないことを確認します。

FTP スタンドアロンフローの考慮事項は、次のとおりです。

- IWSVA は、対象の FTP サーバにアクセスできる必要があります。
- FTP 依存モードに比べ、このフローの手順は 1 つ少なくなります。

このフローを使用するように FTP クライアントを設定するには

- IWSVA サーバを FTP プロキシとして設定します。
- ユーザ名を、通常のユーザ名ではなく、`username@targetftp-server` の形式で設定します。

注意： IWSVA FTP は通常、FTP プロキシ用ポートを開くようにファイアウォールを変更するだけで、大半のファイアウォールで動作します。

FTP 要求は、次の順序でやり取りされます。

1. FTP クライアントが IWSVA FTP サービスに要求を送信します。
2. IWSVA FTP サービスが要求を検証し、ファイルタイプがブロックされていないかどうかなどを確認します。要求が有効な場合、IWSVA FTP サービスは、インターネット上の適切な FTP サーバへの接続を試みます。接続に成功すると、IWSVA FTP サービスは要求を対象の FTP サーバに送信します。
3. インターネット上の FTP サーバが要求に応答します。理想的には、要求されたファイルを使用して応答します。
4. IWSVA FTP サービスが、返されたデータを検索して不要なコンテンツがないかを確認します。不要なコンテンツが検出された場合は、適切なメッセージを FTP クライアントに返します。不要なコンテンツが検出されなかった場合は、要求されたデータを FTP クライアントに返します。

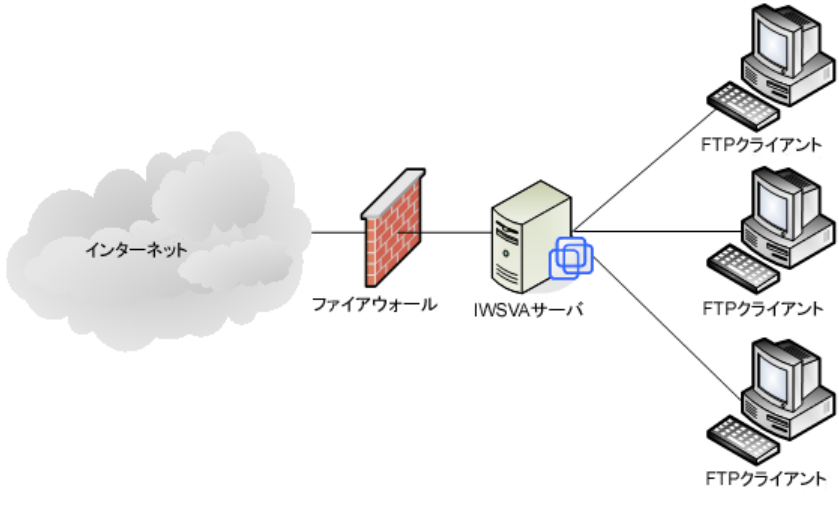


図 2-3.　スタンドアロンモードの FTP プロキシ

依存モードの FTP プロキシ

IWSVA FTP は、上位プロキシと要求元クライアントの間に設置した専用コンピュータにもインストールできます。この設定を使用すると、アクセスブロック、ログ、フィルタなどの他の FTP 機能が追加されて、既存の FTP プロキシが補完されます。

IWSVA の FTP 依存モードは、図 2-4 に示すように、HTTP サービスの依存モードに類似しています。このモードにすると、他の FTP プロキシサーバによって、余分なホップや余分な処理といったパフォーマンス上の不利な条件が発生します。このため、このモードを使用するのは、組織の方針によりインターネットへの直接接続が IWSVA サーバで禁止されている場合のみにしてください。

他の FTP プロキシサーバがストアアンドフォワードを使用している場合、サイズの大きいファイルではパフォーマンスがさらに低下します。その理由は、ファイルはそれらのプロキシサーバで一度ダウンロードしてから IWSVA FTP サービスに転送されるためです。また、他の FTP プロキシには、進行中のすべての転送を保持するのに十分な空き領域を確保する必要があります。

要求をキャッシュできるという利点がある HTTP 依存モードサービスと異なり、FTP プロキシサーバは、ほとんどの場合、要求をキャッシュしません。

FTP 依存モードも、アップロードおよびダウンロードの脅威から FTP サーバを保護します。

FTP 要求は、次の順序でやり取りされます。

1. FTP クライアントが IWSVA FTP サービスに要求を送信します。
2. IWSVA FTP サービスが要求を検証し、ファイルタイプがブロックされていないかどうかなどを確認します。要求が有効な場合、IWSVA FTP サービスはその要求を他の FTP プロキシ、または IWSVA で保護されている FTP サーバにリレーします。
3. インターネット上の FTP サーバが要求に応答します。理想的には、要求されたファイルを使用して応答します。
4. IWSVA FTP サービスが、返されたデータを検索して不要なコンテンツがないかを確認します。不要なコンテンツが検出された場合は、適切なメッセージを FTP クライアントに返します。不

要なコンテンツが検出されなかった場合は、要求されたデータを FTP クライアントに返します。

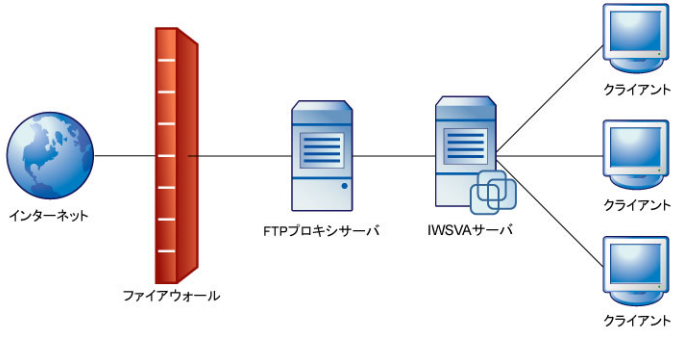


図 2-4.　依存モードの FTP プロキシ

プロキシ転送モードで配置する

プロキシ転送モードの概要

透過と非透過の 2 種類のプロキシ転送があります。透過プロキシは、レイヤ 4 スイッチ（通常の透過）または WCCP 対応スイッチ（WCCP モード）によって実現できます。

プロキシ転送モードに設定された IWSVA では、次の設定オプションを使用してクライアントを保護できます。

- 31 ページの「クライアントを再設定する」
- 32 ページの「レイヤ 4 スイッチを使用する」
- 34 ページの「WCCP 対応のスイッチまたはルータを使用する」

また、IWSVA がこのモードに設定されている場合、必要に応じて、すべてのトラフィックを上位プロキシサーバに送信するようにも設定できます。

以下の表に示す設定オプションに関する説明により、使用する配置設定を決定します。

この設定をサポートするためには、IWSVA のインストール中に IWSVA をプロキシ転送モードでインストールすることを選択します。

クライアントを再設定する

HTTP クライアント（ブラウザまたはプロキシサーバ）は、プロキシとして IWSVA と通信するように設定できます。この設定変更によって、クライアントの Web トラフィックが IWSVA に転送されるようになります。このトラフィックを処理するには、HTTP 検索サービスを HTTP プロキシモードで使用可能にする必要があります。

FTP クライアントは、宛先サーバではなく IWSVA と通信するため、IWSVA へログイン時に FTP サーバアドレスを渡す必要があります。このトラフィックを処理するには、FTP 検索モジュールをスタンドアロンモードへ設定を変更する必要があります。

表 2-1.　クライアントを再設定する場合

利点	制限
ハードウェアの追加は不要です。	管理者がすべてのコンピュータの設定を制御する必要があり、ゲストコンピュータの場合には困難な場合があります。

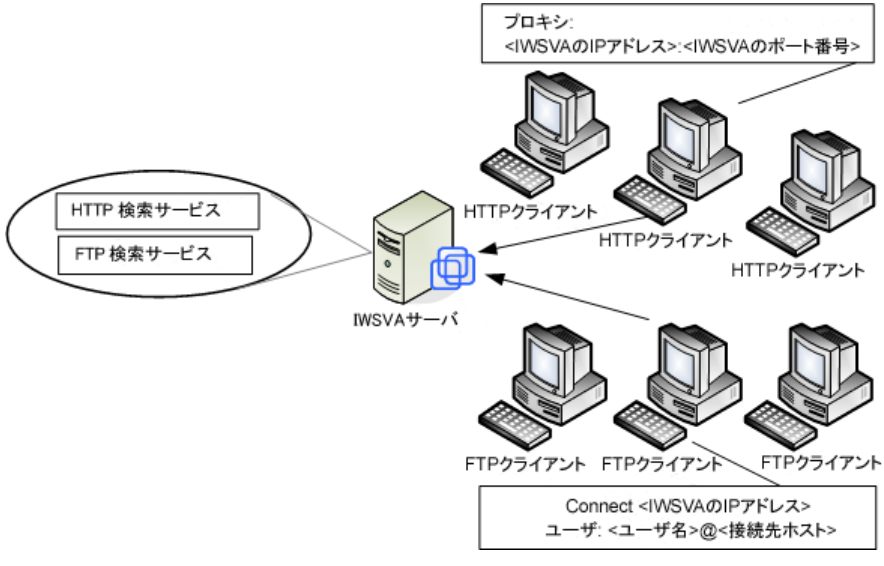


図 2-5.　クライアントを再設定する場合

レイヤ 4 スイッチを使用する

透過とは、IWSVA を組み合わせて使用するのにクライアントユーザがインターネット接続のプロキシ設定を変更しなくても済む機能です。透過は、レイヤ 4 スイッチが HTTP パケットをプロキシサーバにリダイレクトし、そのパケットが要求側サーバに転送されることによって実現されます。

IWSVA では、「通常」の透過をサポートしています。通常の透過は、ほとんどのレイヤ 4 スイッチでサポートされています。さまざまなベンダー製の各種ネットワークハードウェアに対応していますが、通常の透過の設定には次のような制約事項があります。

- 通常の透過を使用すると、ポリシーを定義するのに使用できるユーザの識別方法が IP アドレスとホスト名に限られます。LDAP ではポリシーを設定できなくなります。
- FTP over HTTP は使用できません。このため、FTP 接続を許可しないファイアウォール設定では、ftp:// で始まる URL へのリンクは機能しません。または ftp:// で始まる URL に接続できても、ファイルが検索されません。
- HTTP 要求にホスト情報が格納されていない場合、旧バージョンの Web ブラウザの中には通常の透過に対応できないものがあります。
- HTTP のウェルノウンポートである 80 以外のポートを経由する HTTP 要求が IWSVA にリダイレクトされます。SSL (HTTPS) 要求については、通常受け付けられますがコンテンツは検索されません。
- IWSVA にはクリーンナップ対象のクライアントの IP アドレスが必要なため、IWSVA の下位で NAT (IP マスカレード) を使用しないでください。
- DNS サーバが必要です。

HTTP トラフィックを IWSVA にリダイレクトするには、レイヤ 4 スイッチを使用できます。HTTP 検索サービスを HTTP プロキシモードで使用可能にする必要があります。

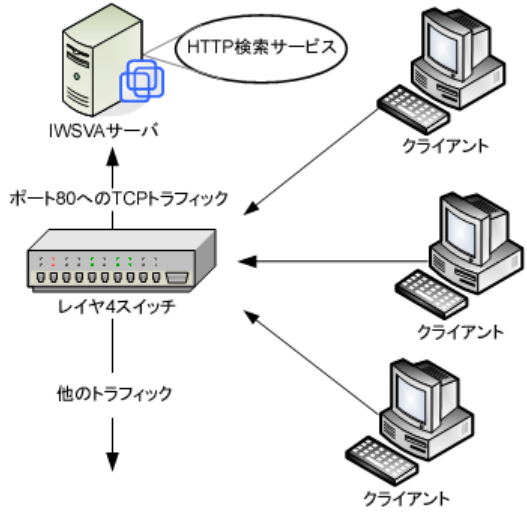


図 2-6.　レイヤ 4 スイッチを使用する場合

インストール中に、透過でこの配信モードをサポートできるようにするチェックボックスをオンにする必要があります。

表 2-2.　レイヤ 4 スイッチを使用する場合

利点	制限
クライアントは透過的に HTTP サービスを利用できます。	トラフィックは、1 ポートごとにプロトコルベースでなくポートベースで傍受する必要があります。HTTP に標準以外のポートを使用する場合、スイッチが経由されません。
容易にコネクションが確立できます。	FTP トラフィックにスイッチベースのリダイレクトを使用できません。
	LDAP がサポートされません。

WCCP 対応のスイッチまたはルータを使用する

IWSVA では、WCCP v2.0 と、GRE および L2 （レイヤ 2) に基づいた転送方法がサポートされます。

WCCP 透過を使用している場合、FTP ダウンロードも検索されます。IWSVA では、WCCP v2.0 がサポートされています。これによって、IWSVA デバイスのクラスタに参加して、負荷分散 WCCP Web セキュリティプラットフォームが実現されます。

WCCP を使用する場合の利点 :

- クライアント側の透過
- スケーラブル

WCCP を使用する場合の制限 :

- Cisco 社独自プロトコル

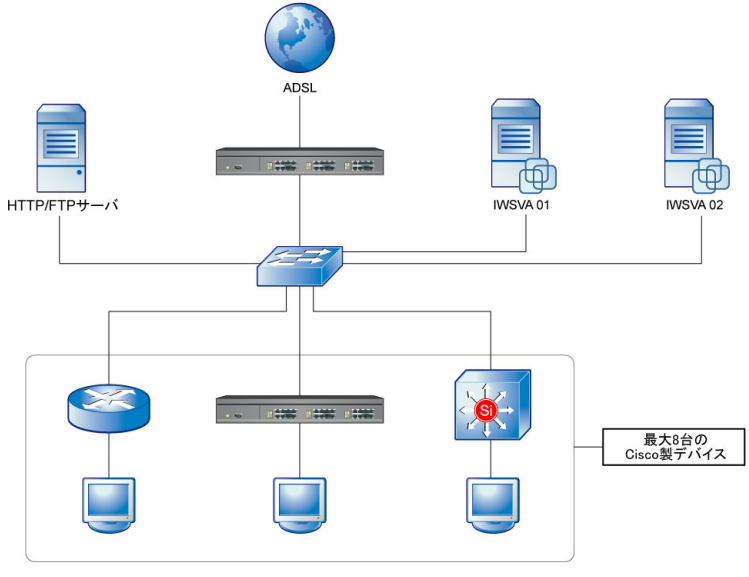


図 2-7. WCCP 環境における IWSVA の配置

プロキシ転送モードにより HTTP フローを計画する

スタンドアロンモードの HTTP プロキシ

最も簡単な設定は、上位プロキシを使用しないスタンドアロンモードで IWSVA を設置することです。この場合、IWSVA がクライアントのプロキシサーバの役割を果たします。この設定の利点は、比較的に導入が簡単なことと、プロキシサーバを個別に用意する必要がないことです。プロキシ転送をスタンドアロンモードにする欠点は、各クライアントがブラウザのインターネット接続設定から IWSVA デバイスをプロキシサーバに設定しなくてはならない点です。これにはネットワークを利用するユーザの協力が必要であり、インターネット接続設定を変更すると、組織のセキュリティポリシーから除外されるユーザが発生する可能性があります。

注意： IWSVA をスタンドアロンモードに設定する場合、ネットワーク上の各クライアントでは、インターネット接続を設定する必要があります。接続設定では、IWSVA デバイスとポート (初期設定では 8080) をプロキシサーバとして使用するようにします。

Web ページ要求は、次の順序で処理されます。

1. Web クライアントが HTTP サービスに要求を送信します。
2. HTTP サービスが要求を検証し、URL がブロックされていないかどうかを確認します。URL が無効な場合、またはブロックされている場合、HTTP サービスは適切な通知を HTTP クライアントに送信し、トランザクションを終了します。URL が有効な場合、HTTP サービスは適切な Web サーバとの接続を試みます。
3. 接続された Web サイトが、Web サーバからの応答を HTTP サービスに返します。
4. HTTP サービスがコンテンツを検索して不要なデータが含まれていないかどうかを確認し、適切な応答をクライアントに返します。

表 2-3. スタンドアロンモードの HTTP プロキシ

利点	制限
インストールと配置が容易にできます。	接続に時間がかかると許容接続時間の上限に達する可能性があります。
	ネットワーク上の各クライアントがプロキシサーバを設定する必要があります。

通常の透過モードの HTTP プロキシ

複数の IWSVA サーバをインストールして、ネットワークのトラフィックおよび検索の負荷を分散できます。次のインストール例では、レイヤ 4 スイッチがクライアント要求を受け取り、IWSVA サーバに転送します。

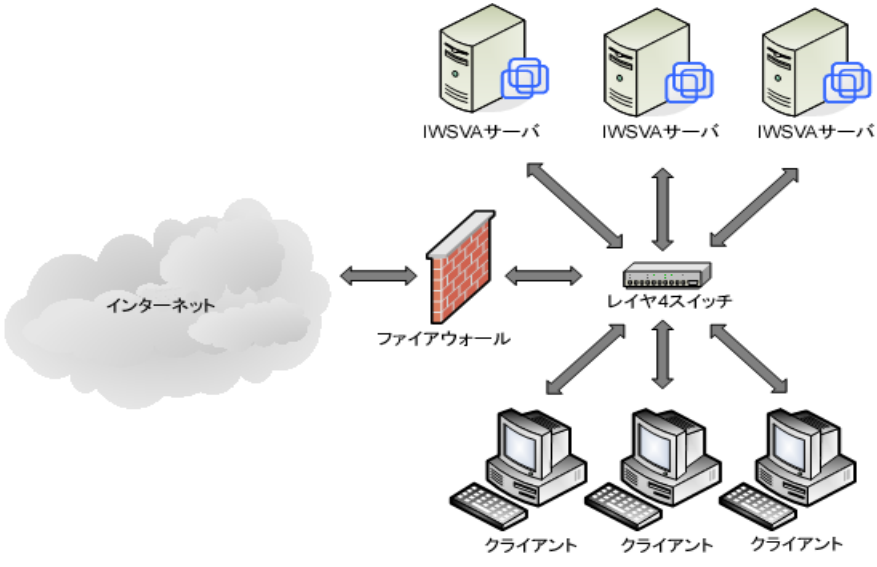
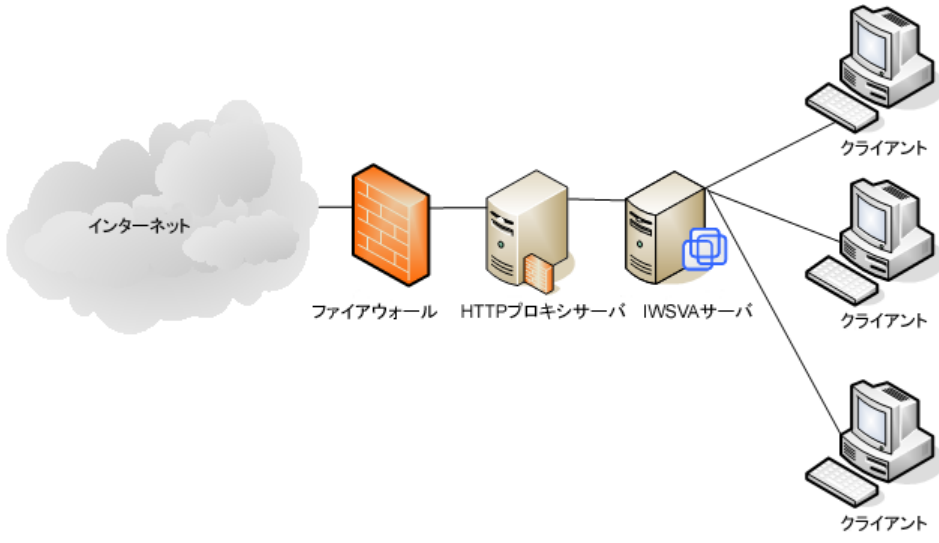


図 2-8. レイヤ 4 スイッチを使用し、通常の透過モードで IWSVA サーバ間で負荷を分散する構成

依存モードの HTTP プロキシ (プロキシを外側に配置する場合)

このフローを使用する HTTP ブラウザでは、IWSVA サーバを介してプロキシするようにブラウザを設定します。初期設定のポートは 8080 です。



依存モードの HTTP プロキシ (プロキシを外側に配置する場合)

Web ページ要求は、次の順序で処理されます。

1. Web クライアントが HTTP サービスに要求を送信します。
2. HTTP サービスが要求を検証します。
   - URL が無効な場合、またはブロックされている場合、HTTP サービスは適切な通知を HTTP クライアントに送信し、トランザクションを終了します。
   - URL が有効な場合、HTTP サービスは要求を上位 HTTP プロキシサーバに転送します。
3. 上位プロキシサーバが処理を実行し、要求をインターネット上の Web サイトに転送します。
4. 接続された Web サイトが、応答 (Web ページ) を HTTP プロキシサーバに返します。
5. HTTP プロキシサーバが処理を実行し、応答データを IWSVA HTTP サービスに転送します。
6. HTTP サービスがコンテンツを検索して不要なデータが含まれていないかどうかを確認し、適切な応答を HTTP クライアントに返します。

表 2-4. 依存モードの HTTP プロキシ (プロキシを外側に配置する場合)

利点	制限
プロキシサーバによってタイミングとコンテンツの可用性動作が制御されます。	キャッシュされている応答を含め、すべての応答を IWSVA で検索する必要があります。

表 2-4. 依存モードの HTTP プロキシ (プロキシを外側に配置する場合) (続き)

利点	制限
安全性が高くなります。キャッシュされているオブジェクトに設定変更が反映されます。	
キャッシュ済みオブジェクトのダウンロードを IWSVA で待機する必要がありません。	

依存モードの HTTP プロキシ (プロキシを内側に配置する場合)

プロキシを内側に配置するフローは、HTTP クライアントと IWSVA サーバの間に配置されたキャッシュプロキシで構成されます。ICAP は使用しません。企業では通常、このフローを使用して ICAP の場合と同様にパフォーマンスを強化します。

警告： このフローは、パフォーマンスの向上を期待できる一方で、次の 2 つのリスクがあります。

1. **ウイルスに感染したデータがキャッシュ内に存在する場合、そのデータがキャッシュで検索された際にパターンファイルが存在しないと、IWSVA HTTP サービスはウイルスの繁殖を防止できません。**

2. **同様に、有効なコンテンツに関するポリシーが変更された場合や、キャッシュ内の承認済みユーザ関連データを未承認ユーザが要求した場合、HTTP サービスはそのデータへの後続不正アクセスを防止できません。**

プロキシを内側に配置するフローを使用する代わりに、ICAP キャッシュデバイスを使用することをお勧めします。このソリューションではキャッシュのパフォーマンスを強化できます。また、プロキシを内側に配置するトポロジにおけるセキュリティ問題がありません。

Web ページ要求は、次の順序で処理されます。

1. Web クライアントが HTTP プロキシサーバに要求を送信します。
2. プロキシサーバが要求を IWSVA に転送します。
3. IWSVA が URL フィルタおよび URL アクセス設定を使用して要求を検証します。
   - URL が無効な場合、またはブロックされている場合、HTTP サービスは適切な通知を HTTP クライアントに送信し、トランザクションを終了します。

- URL が有効な場合、HTTP サービスは要求をインターネット上の Web サーバに転送します。

4. 接続された Web サーバが、応答 (Web ページ) を IWSVA に返します。
5. IWSVA が、返されたデータに対する処理 (ウイルス検索、スパイウェア検索、ActiveX 対策) を実行し、適切な応答やデータをプロキシサーバに転送します。
6. プロキシサーバがデータをキャッシュし (キャッシュ可能な場合)、応答またはデータを HTTP クライアントに配信します。

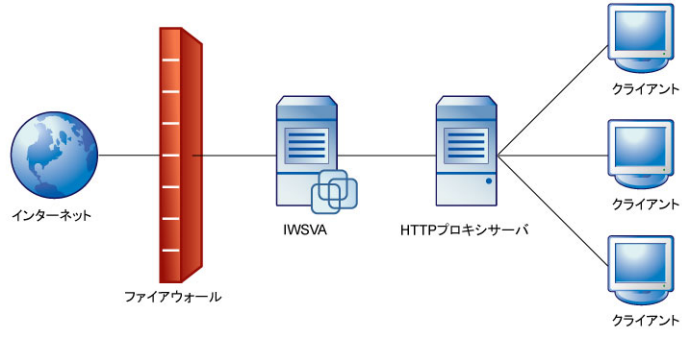


図 2-9. 依存モードの HTTP プロキシ (プロキシを内側に配置する場合)

表 2-5. 依存モードの HTTP プロキシ (プロキシを内側に配置する場合)

利点	制限
クライアントの設定変更が不要です。	IWSVA 上の設定変更やパターンファイルのアップデートは、キャッシュされたオブジェクトに影響しません。
キャッシュされているオブジェクトがプロキシサーバからクライアントに直接ダウンロードされるため、遅延を最小限に抑えられます。	

依存モードの HTTP 二重プロキシ

二重プロキシ設定には、2 つのキャッシュプロキシが必要です。1 つ目のプロキシを HTTP クライアントと IWSVA サーバの間に配置し、もう 1 つのプロキシを IWSVA サーバとインターネットの間に配置します。この設定は通常、プロキシを IWSVA の外側に配置する場合と内側に配置する場合の 2 つの依存モードの利点を両方活かす場合に使用されます。

Web ページ要求は、次の順序で処理されます。

1. Web クライアントが 1 つ目のプロキシサーバに要求を送信します。
2. 1 つ目のプロキシサーバが要求を IWSVA に転送します。
3. IWSVA が URL フィルタおよび URL アクセス設定を使用して要求を検証します。
   - URL が無効な場合、またはブロックされている場合、HTTP サービスは適切な通知を HTTP クライアントに送信し、トランザクションを終了します。
   - URL が有効な場合、HTTP サービスは要求を 2 つ目のプロキシサーバに転送します。
4. 2 つ目のプロキシサーバが処理を実行し、要求をインターネット上の Web サーバに転送します。
5. 接続された Web サーバが、応答 (理想的には Web ページ) を 2 つ目のプロキシサーバに返します。
6. 2 つ目のプロキシサーバがデータをキャッシュし (キャッシュ可能な場合)、応答またはデータを IWSVA に配信します。
7. IWSVA が、返されたデータに対する処理 (ウイルス検索、スパイウェア検索、ActiveX 対策) を実行し、適切な応答またはデータを 1 つ目のプロキシサーバに転送します。

8. 1 つ目のプロキシサーバがデータをキャッシュし (キャッシュ可能な場合)、応答またはデータを HTTP クライアントに配信します。

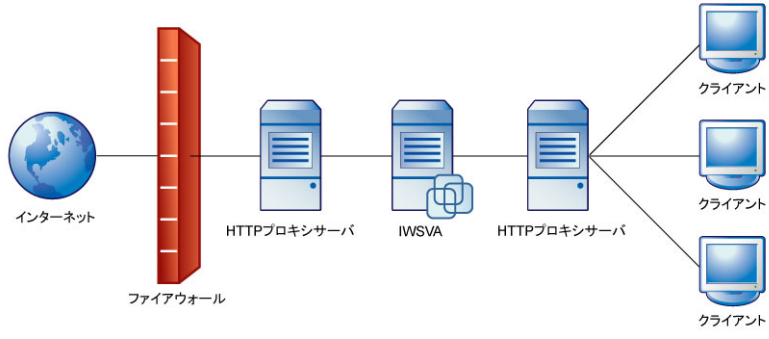


図 2-10. 依存モードの HTTP 二重プロキシ

表 2-6. 依存モードの HTTP 二重プロキシ

利点	制限
プロキシサーバによってタイミングとコンテンツの可用性動作が制御されます。	追加のプロキシサーバが必要なため、コストが高くなります。
キャッシュ済みオブジェクトのダウンロードを IWSVA で待機する必要がありません。	
クライアントの設定変更が不要です。	

WCCP モードで配置する

注意： WCCP モードでの配置方法の詳細については、IWSVA 6.5 SP3「管理者ガイド」の「付録 E: WCCP の配信およびトラブルシューティング」を参照してください。

WCCP モードの HTTP プロキシ (1 台または複数の IWSVA サーバを配置する場合)

WCCP モードに設定された IWSVA は、次の順序で Web ページ要求を処理します。

1. Web クライアントが Web サーバに要求を送信します。
2. ルータが要求を受信してから、その要求を IWSVA に転送します。
3. IWSVA が Web クライアントとの接続を確立します。
4. IWSVA がクライアント要求を Web サーバに転送し、Web サーバとの接続を確立します。
5. IWSVA が Web クライアントと Web サーバ間のデータ送信を開始します。
6. データがウイルスに感染していなければ、IWSVA がそのデータを Web クライアントに送信します。
7. データがウイルスに感染していれば、IWSVA が、ブロックされたページを Web クライアントに送信します。

ICAP モードで配置する

ICAP モードの概要

ICAP（Internet Content Adaptation Protocol) は、HTTP 応答と要求をサードパーティのプロセッサに転送し、結果を収集するよう設計されています。ICAP 要求を送信するコンポーネントを、ICAP クライアントと呼びます。要求を処理するコンポーネントを、ICAP サーバと呼びます。

IWSVA を ICAP モードで設定すると、ICAP 準拠のクライアントから送信される要求を処理できます。サポートされている実装については、Readme を参照してください。

IWSVA 6.5 SP3 では、ICAP over SSL 機能を持つ ICAP 準拠のクライアントとのセキュアな ICAP 通信がサポートされます。セキュアな ICAP 通信を有効にするには、IWSVA で配置ウィザードを使用してサーバ証明書をインポートし、関連する設定を行います。

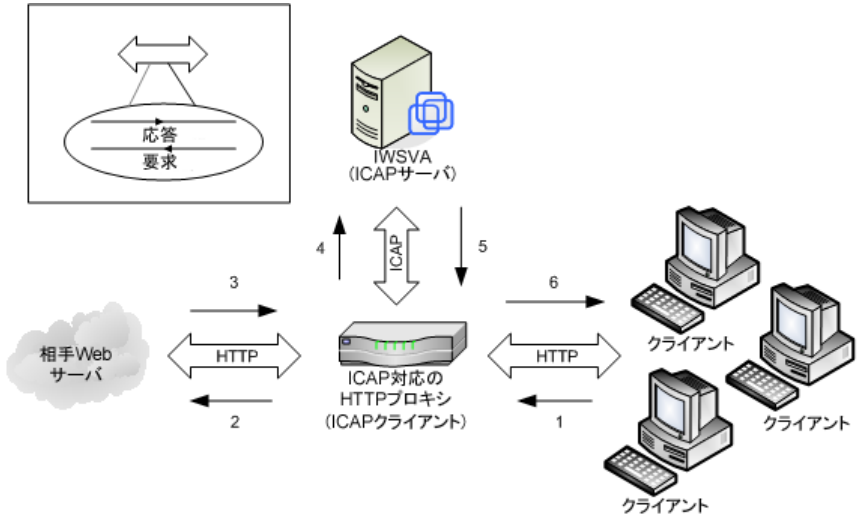


図 2-11.　ICAP 対応のプロキシを使用する場合

表 2-7.　ICAP 対応のプロキシ

利点	制限
ICAP により、新規コンテンツおよび必要なコンテンツのみの検索が可能になります。	ICAP 装置のコストが発生します。
検索量が少なく、選択的に実行されるため、パフォーマンスが向上します。	IWSVA のインストール時に追加の手順が必要です。
リソース効率が改善され、必要な IWSVA サーバハードウェアの台数が削減されます。	ICAP 管理が必要です。

ICAP モードにより HTTP フローを計画する

ICAP モードの HTTP プロキシ (1 台または複数の IWSVA サーバを配置する場合)

この項では、ICAP デバイスと IWSVA サーバの両方を使用した場合の一般的な HTTP GET 要求のフローについて説明します。以下のフローでは、IWSVA は ICAP のルールに応じて ICAP デバイスと通信します。これは、他のフロー、すなわち IWSVA が HTTP クライアントからの URL 要求を受信するフローとは大きく異なります。以下のフローを HTTP ブラウザで使用するには、ICAP デバイスを HTTP プロキシとして使用するようにブラウザを設定します。

ICAP デバイスを使用すると、次の 2 通りの方法でパフォーマンスを強化できます。

- **クリーンなデータのキャッシュ** — データがクリーンな場合は、ICAP デバイスでデータをキャッシュします。ただし、後続の要求を作成したユーザのデータ閲覧可否や、ユーザが割り当てを超過していないことなどを検証するために、ICAP ではポリシーをチェックするよう IWSVA に依頼する必要があります。
- **IWSVA サーバのクラスタ化** — 複数の IWSVA サーバを使用する場合は、ICAP デバイスでサーバ間の要求を負荷分散します。これは、受信ページの検索要求を 1 台の IWSVA サーバで処理しきれない企業環境にとっては不可欠です。ICAP を使用すると、ICAP デバイスで負荷分散が実行されます。このため、使用可能な IWSVA サーバのパフォーマンスを最大限にできます。

注意 : ICAP を使用しない環境でも、複数の IWSVA サーバを使用することで、同様の利点を享受できます。ただし、管理者は別の負荷分散技術を利用する必要があります。

IWSVA を ICAP モードで設定すると、ICAP 準拠のクライアントから送信される要求を処理できます。IWSVA では、ICAP v1.0 準拠のキャッシュサーバをサポートしています。

- Blue Coat
- Cisco Content Engines (CE)
- Oracle ZFS Storage Appliance
- Dell NAS FluidFS
- EMC Isilon NAS OneFS
- Squid

IWSVA では、不要なコンテンツを検出するために他のフローと同じ URL フィルタ処理とデータ検索が実行されます。しかし、まったく異なる通信プロトコルが必要であるという点で、ICAP モードのフローは他のフローと大幅に異なります。管理者は、インストール後の設定で、使用するプロトコル (ICAP または非 ICAP) を指定します。

次の図は、1 台以上の IWSVA サーバを使用した場合の HTTP フローを示しています。どちらの図も、要求されたデータが ICAP デバイスのキャッシュに存在しないことを前提としています。複数のサーバを使用する環境では、要求を受信する IWSVA サーバが ICAP サービスによって選択されます。

ICAP モードに設定された IWSVA は、次の順序で Web ページ要求を処理します。

1. HTTP クライアントが URL の要求を作成し、ICAP キャッシュプロキシデバイスに送信します。
2. ICAP デバイスが、自身の設定に基づいて、要求を IWSVA サーバに転送する必要があることを判断します。複数のサーバが使用可能な場合は、ラウンドロビン方式で順番にサーバを選択し、負荷分散を行います。
3. IWSVA サーバが URL を検証します。
   - URL がブロックされていない場合、IWSVA は応答を ICAP デバイスに送信します。
   - URL が無効な場合、またはブロックされている場合、IWSVA は HTTP クライアントへ適切な応答を送信するよう ICAP デバイスに指示し、トランザクションを終了します。
4. URL が有効な場合、ICAP サーバはインターネット上の Web サイトにページを要求します。
5. インターネット上の Web サイトが、要求されたページまたは他の適切な応答を返します。
6. ページが返された場合、ICAP デバイスが自身の設定に基づいて、IWSVA サーバでデータを検索する必要があることを判断します。複数のサーバが使用可能な場合は、ラウンドロビン方式で順番にサーバを選択し、負荷分散を行います。
7. IWSVA サーバが結果を検索し、データがクリーンか、あるいは不要なコンテンツが含まれているかに応じて、適切な応答を ICAP デバイスに返します。
8. データがクリーンな場合、ICAP デバイスがそのデータを HTTP クライアントに返し、後続の要求に備えてデータのコピーを自身に維持します。データに不要なコンテンツが含まれる場合、

ICAP デバイスは、IWSVA から指示された適切なエラーメッセージを HTTP クライアントに返します。後続の要求に備えてデータのコピーを維持することはありません。

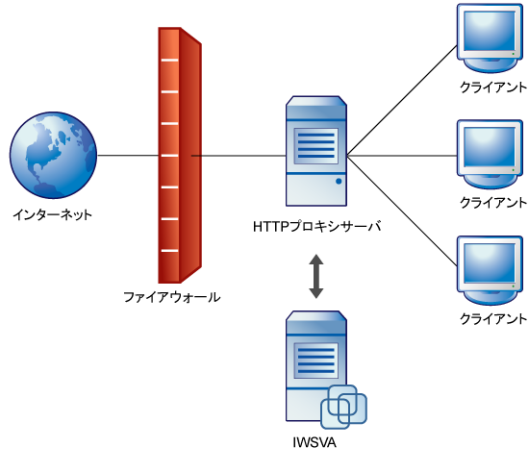


図 2-12. ICAP **モードの** HTTP **プロキシ** (1 **台の** IWSVA **サーバを配置する場合**)

複数のサーバを使用する ICAP モードの IWSVA

ネットワーク上にすでにコンテンツキャッシュサーバが存在する場合は、ICAP HTTP ハンドラをインストールすることをお勧めします。次の図は、複数のサーバがある環境で IWSVA を ICAP モードでインストールした構成を示しています。複数の IWSVA ICAP サーバを正常に動作させるためには、対応するパターンファイル、検索エンジンのバージョン、および設定ファイル (`/etc/iscan/intscan.ini`) を同じにする必要があります。

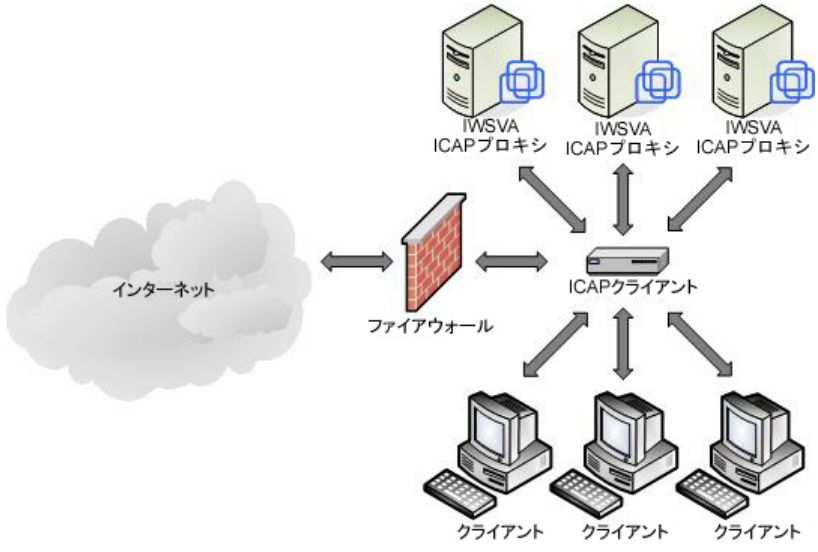


図 2-13. ICAP **モードの** HTTP **プロキシ (複数の** IWSVA **サーバを配置する場合)**

表 2-8. ICAP **モードの** HTTP **プロキシ**

利点	制限
クライアントの設定変更が不要です。	IWSVA の設定変更がキャッシュされているオブジェクトに反映されます。
キャッシュされているオブジェクトが、プロキシサーバからクライアントに直接ダウンロードされます。このため、遅延を最小限に抑え、パフォーマンスを強化できます。	
ICAP クライアントの設定後に負荷分散が可能です。	

リバースプロキシモードで配置する

リバースプロキシモードの概要

通常 IWSVA はクライアントの近くにインストールされ、インターネット上のセキュリティリスクからクライアントを保護します。ただし、IWSVA をリバースプロキシとしてインストールし、不正プログラムのアップロードから Web サーバを保護することもできます。リバースプロキシモードでは、保護対象の Web サーバの近くに IWSVA がインストールされます。このモードでは、IWSVA はプロキシサーバとして Web サーバを保護します。HTTP プロキシは、インターネットと Web サーバの間に配置されます。この設定は、Web サーバでクライアントからのファイルのアップロードを受け入れる場合や、複数の Web サーバ間の負荷を分散させることで各 Web サーバの負荷を軽減する場合に有用です。IWSVA を使用して負荷分散によって複数の Web サーバを保護する場合、クライアントと Web サーバの間の通信は HTTP で行われます。ASP や ISP は IWSVA を HTTP プロキシとして使用し、アップロードトラフィックをウイルスから保護できます。また、複雑な Web サイトを持つ企業では中央のアクセス管理点としても使用できます。

IWSVA は、クライアント要求を受信し、すべてのコンテンツを検索してから、その HTTP 要求を実際の Web サーバにリダイレクトします。このフローは特に、e コマーストランザクションに使用される Web サイト、インターネット上でデータをやり取りする分散アプリケーション、またはクライアントが遠隔地から Web サーバにファイルをアップロードするような状況に適しています。

リバースプロキシモードでは、SSL ポートで受信要求を待機するように IWSVA を設定できます。この機能を有効にするには、IWSVA Web コンソールで配置ウィザードを使用してサーバ証明書をインポートし、関連する設定を行います。

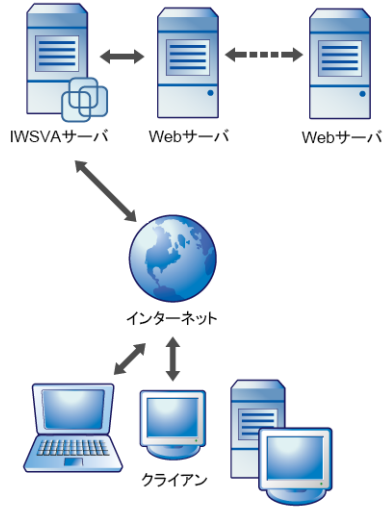


図 2-14.　クライアントから Web サーバを保護するリバースプロキシ

リバースプロキシモードにより HTTP フローを計画する

依存モードの HTTP リバースプロキシ

リバースプロキシモードでは、HTTP プロキシはクライアントシステムに対する Web サーバとして機能します。要求はすべてプロキシで受信されてから、実際の Web サーバに転送されます。したがって、すべての HTTP トラフィックが HTTP プロキシを経由することになるため、プロキシでコンテンツを検索し、感染したトランザクションをブロックすることが可能になります。

注意： 管理者は、次の点に注意する必要があります。
- この設定では URL フィルタは機能しません。ウイルス検索機能のみが有用です。
- リバースプロキシモードでは、Web サーバのアクセスログは無意味です。Web サイトの接続を解析するには、IWSVA のアクセスログを使用する必要があります。
- 理想としては、リバースプロキシサーバをファイアウォールの内側に配置することをお勧めしますが、多くの場合、プロキシはインターネットに直接接続されるため、直接的な攻撃を受けやすくなります。ファイアウォールを使用せずにリバースプロキシを設定する場合、IWSVA をホストする OS を保護するために、適切な予防措置をすべて講じる必要があります。

リバースプロキシモードに設定された IWSVA は、次の順序で Web ページ要求を処理します。

1. クライアントが Web 要求を開始します。
2. 要求が InterScan Web Security Virtual Appliance で受信され、ポート 80 または 443 で待機するように設定されます。
3. InterScan Web Security Virtual Appliance がコンテンツを検索し、実際の Web サーバに転送します。
4. 要求されたページを Web サーバが IWSVA に返します。
5. InterScan Web Security Virtual Appliance がページのヘッダをリライトし、要求に基づいて送信します。
6. 変更されたページが要求元に返されます。

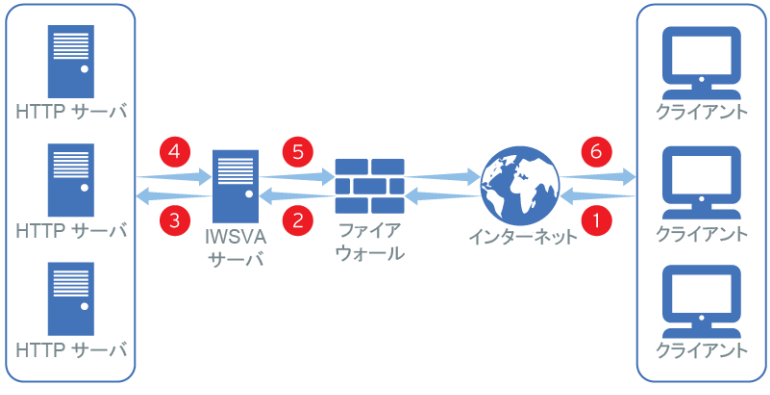


図 2-15. 依存モードの HTTP リバースプロキシ

表 2-9. 依存モードの HTTP リバースプロキシの詳細

利点	制限
オブジェクトがキャッシュされる前に、IWSVA がすべてのオブジェクトを検索します。	新しいエンジン、パターンファイル、および設定が、キャッシュされているオブジェクトに反映されません。
	IWSVA のアクセスログ機能の効果は低下します。

透過ブリッジモードで配置する

透過ブリッジモードの概要

透過ブリッジモードでは、IWSVA が 2 台のネットワークデバイス（スイッチ、ルータ、またはファイアウォール) 間のブリッジとして機能して、HTTP/HTTPS トラフィックや FTP トラフィックを透過的に検索します。透過ブリッジモードは、IWSVA を既存のネットワークトポロジに配置する最も簡単な方法です。また、クライアント、ルータ、またはスイッチの設定を変更する必要がありません。IWSVA は、「Bump In The Wire」機能として動作し、不正プログラムを検索します。IWSVA を透過ブリッジモードに設定するには、2 枚のネットワークカードが必要です。

透過ブリッジモードでは、クライアント側の設定を変更しなくても、IWSVA でクライアントの HTTP/HTTPS 要求を処理して検索できる利点があります。これはエンドユーザにとって便利な設定です。また、インターネット接続設定を変更しただけでクライアントがセキュリティポリシーから除外されることが防止されます。

この配信モードのもう 1 つの重要な利点は、IWSVA がすべてのポートのすべてのトラフィックを認識する点です。これにより、IWSVA のアプリケーション制御機能を使用して、HTTP/HTTPS および FTP だけでなく、420 種類を超えるその他のアプリケーションとプロトコルを監視し制御できます。

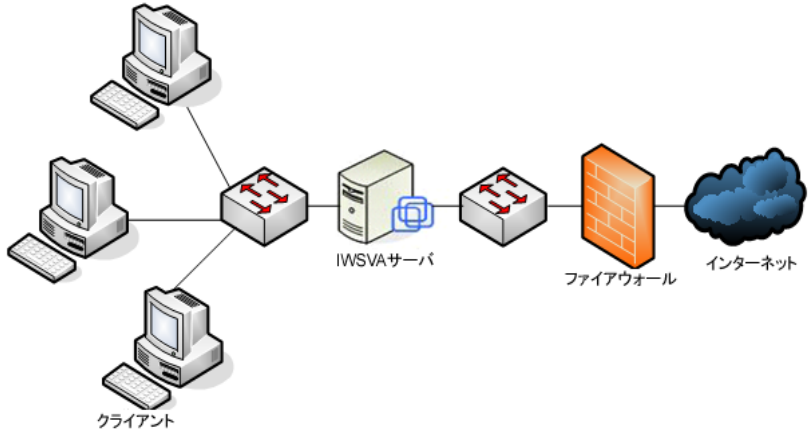


図 2-16.　一般的なブリッジモードの配置

透過ブリッジモードにより HTTP フローを計画する

透過ブリッジモードに設定された IWSVA は、次の順序で Web ページ要求を処理します。

1. Web クライアントが Web サーバに要求を送信します。
2. IWSVA がクライアントからの接続を受信し、Web サーバに要求を送信します。
3. IWSVA が Web クライアントとの接続を確立します。
4. IWSVA が Web サーバとの接続を確立して、Web サーバからデータを取得します。
5. データがウイルスに感染していなければ、IWSVA がそのデータを Web クライアントに送信します。
6. データがウイルスに感染していれば、IWSVA が、ブロックされたページを Web クライアントに送信します。

高可用性配信モード

IWSVA 6.5 SP3 透過ブリッジモードは、高可用性 (HA) モードでの配置をサポートしています。HA モードでは、2 つの IWSVA 6.5 SP3 ノードが 1 つの HA クラスタとして設定されます。この設定では、一方のノードが上位、つまりアクティブノードとして指定され、「接続ステータス」リンクを介して、下位、つまりパッシブノードに接続されます。

HA モードの配置では、各 IWSVA 6.5 SP3 HA クラスタメンバーで Bare Metal インストールを実行することをお勧めします。これにより、両方の HA クラスタメンバーが 1 つの仮想サーバにインストールされ、仮想サーバが動作不能になる状況が回避されます。この状況では、HS クラスタの両方のメンバーも操作不能になります。

注意： HA 配信モードは、透過ブリッジモードでのみサポートされます。その他のサポートされる配信モードで配置された複数の IWSVA 間の高可用性は、IWSVA インスタンスの外部で処理されます。特に、ロードバランサはどのプロキシモードでも冗長性をサポートします。Cisco WCCP デバイスは、WCCP モードの冗長な IWSVA へのトラフィックを管理できます。また、ICAP プロキシクライアントは、ICAP モードの冗長な IWSVA へのトラフィックを管理できます。

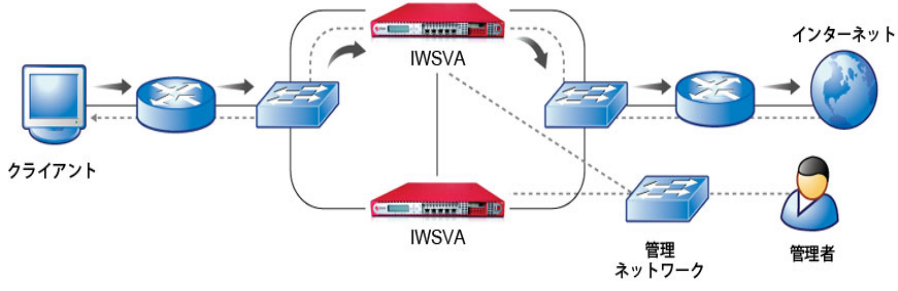


図 2-17.　高可用性配信モード

HA 配信モードでのインストールのガイドライン

IWSVA の初回インストール時に、HA クラスタを構成する各 IWSVA ユニットの選択されたネットワークインタフェースに静的 IP アドレスが割り当てられます。

HA 機能を正常に構成するには、インストール時にどのネットワークカード（eth0、eth1 など）に IP アドレスが割り当てられたかと、サーバ上でネットワークインタフェースがどのように設定されているかを把握している必要があります。IWSVA には、この情報の収集を簡素化するための CLI コマンドがあります。IWSVA の初回インストール後にこの CLI コマンドを実行することで、Web コンソールで必要な情報を収集および記録して、インストールを完了することができます。

CLI コマンドを使用して必要な情報を収集した後に、ブラウザを介して Web コンソールに接続できます。新規インストールの場合は、配置ウィザードが自動的に起動され、配信モードの手順が順を追って表示されます。

ネットワークループの作成を避けるために、必ず最初に、各 IWSVA ユニットをプロキシ転送デバイスとして設定してください。すべてのネットワーク情報が設定されると、配置ウィザードを使用して HA クラスタを作成できます。

警告： **透過ブリッジモードで、誤って両方の IWSVA デバイスを上位デバイスつまりアクティブデバイスとして設定した場合、ネットワークループが作成されることがあります。この可能性を回避するために、HA 機能を設定する前に、各 IWSVA をプロキシ転送デバイスとして設定してください。**

IWSVA HA クラスタを設定するには

1. 2 つの IWSVA デバイスをプロキシ転送モードでインストールします。一方が上位アクティブデバイスになり、もう一方が下位パッシブデバイスになります。
2. IWSVA デバイスは汎用サーバハードウェアにインストールされる場合があるため、HA クラスタをセットアップする前に、ネットワークカードとネットワークの情報を確認する必要があります。HA クラスタ設定を完了するための Web UI 設定手順で使用されるネットワークカード情報を収集します。これを行うには、IWSVA の CLI コンソールにログインして、次の CLI コマンドを実行します。

   ```
   show network interface status
   ```
3. 両方の IWSVA デバイスが、前の手順で識別されたアクティブネットワークカードを使用してネットワークに接続されていることを確認します。両方の IWSVA ユニットは互いに通信可能であり、さらに HA クラスタを設定するために使用される管理ホストとも通信可能である必要があります。
4. 管理ホストからブラウザを使用して、上位つまりアクティブメンバーとして動作する IWSVA デバイスに接続します。初回インストール後に IWSVA の Web コンソールへ初めてアクセスした場合は、配置ウィザードが自動的に起動します。配置ウィザードには、[管理] → [配置ウィザード] メニューオプションからアクセスすることもできます。
5. 配置ウィザードの画面上の指示に従って、最初の HA クラスタメンバーを設定します。これが上位つまりアクティブユニットになります。
6. 下位メンバーになる IWSVA デバイスに対して手順 4 と 5 を繰り返します。下位メンバーが上位メンバーと結合すると HA クラスタが完了します。

   HA クラスタの作成方法の詳細については、「IWSVA 管理者ガイド」の第 3 章「透過ブリッジモードの高可用性とクラスタ管理」を参照してください。

第 3 章

InterScan Web Security Virtual Appliance のインストール

本章で説明する内容には、次の項目が含まれます。

IWSVA を入手する

ダウンロードサイト (https://www.trendmicro.com/ja_jp/business/products/downloads.html) からインストール ISO イメージをダウンロードできます。

IWSVA のサーバ要件の詳細については、14 ページの「システム要件」を参照してください。

ご使用の環境にどのインストール方法が適しているかを検証することをお勧めします。

IWSVA のインストール

IWSVA では、新規のインストールまたは特定のバージョンからの移行のみがサポートされています。

IWSVA では、IWSVA 6.5 SP2 製品から既存の設定およびポリシーデータを移行することがサポートされています (15 ページの「移行」を参照してください)。

このインストールプロセスでは、IWSVA をインストールするために、既存のシステムを初期化します。VMware および Hyper-V のインストールでは、インストールの前に仮想マシンを作成する必要があります。その他の VMware 仮想マシン設定については、付録 E の 105 ページの「VMware ESX 下での IWSVA 用の新しい仮想マシンの作成」を参照してください。その他の Hyper-V 仮想マシン設定については、付録 F の 121 ページの「Microsoft Hyper-V 下での IWSVA 用の新しい仮想マシンの作成」を参照してください。

警告： インストールプロセス中に既存のデータやパーティションはすべて削除されます。システム上のデータが存在する場合は、IWSVA をインストールする前にバックアップをしてください。

オープンソース型コンテンツキャッシング用アプリケーションの Apache Traffic Server (ATS) もインストールされます。このアプリケーションは初期設定で無効です。IWSVA 管理 Web コンソール [HTTP] > [設定] > [コンテンツキャッシュ] にて [コンテンツキャッシュを有効にする] にチェックをつけることで、このユーティリティを有効にできます。トレンドマイクロでは、インストールを簡単にするために使用の有無にかかわらず、便宜上 ATS を提供しています。ATS のサポートは、ATS オープンソースコミュニティから提供されています。

トレンドマイクロディスクレーマー： IWSVA は Apache Traffic Server (ATS) を標準装備し、基本的な設計レポートと統計レポートを提供しています。これによって、ATS をインストールして IWSVA と連動するように設定する作業が簡略化されます。ATS は初期設定で無効になります。このため、インストールの完了後に IWSVA Web コンソール経由で有効にする必要があります。ATS のサポートはオープンソースチャネルにより提供されます。ATS の利点と機能に精通してから有効にしてください。

ATS アプリケーションに関するその他の情報、ドキュメント、およびサポートについては、公式の ATS Web プロキシキャッシュ Web サイト (`trafficserver.apache.org`) を参照してください。

トレンドマイクロでは、ATS の機能に対するサポートは提供しません。

IWSVA をインストールするには

1. IWSVA のインストールを開始します。

Microsoft Hyper-V 仮想マシンにインストールする

a. Microsoft Hyper-V サーバ上に仮想マシンを作成します。

   付録 F の「Microsoft Hyper-V 下での IWSVA 用の新しい仮想マシンの作成」(121 ページ) を参照してください。

b. 作成した仮想マシンの電源をオンにして、IWSVA インストール ISO から起動します。

VMware ESX 仮想マシン上でインストールする

a. VMware ESX サーバ上で仮想マシンを作成します。

付録 E の 105 ページの「VMware ESX 下での IWSVA 用の新しい仮想マシンの作成」を参照してください。

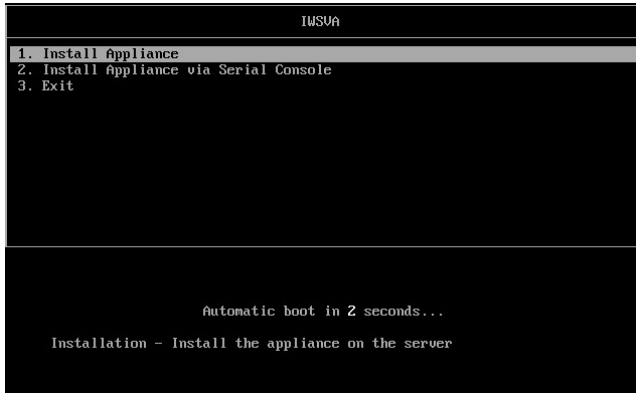
b. 作成した仮想マシンの電源をオンにして、IWSVA インストール ISO から起動します。

注意： コンピュータが ISO イメージ (ISOLINUX など) から起動された場合、ブートローダのプロンプトで <Enter> キーを押して IWSVA インストールプロセスを続行する必要があります。

Microsoft Hyper-V 仮想マシンと VMware ESX 仮想マシンの両方に共通するインストール手順

注意： IWSVA は、インストール時にはネットワーク接続は不要ですが、インストールの完了後に配置ウィザードを使用する際にインターネットに接続する必要があります。

2. 仮想マシンの起動後、[Install Appliance] 画面に IWSVA のインストールメニューと次のオプションが表示されます。[Install Appliance] を選択します。
   - Install Appliance
   - Install Appliance via Serial Console
   - Exit

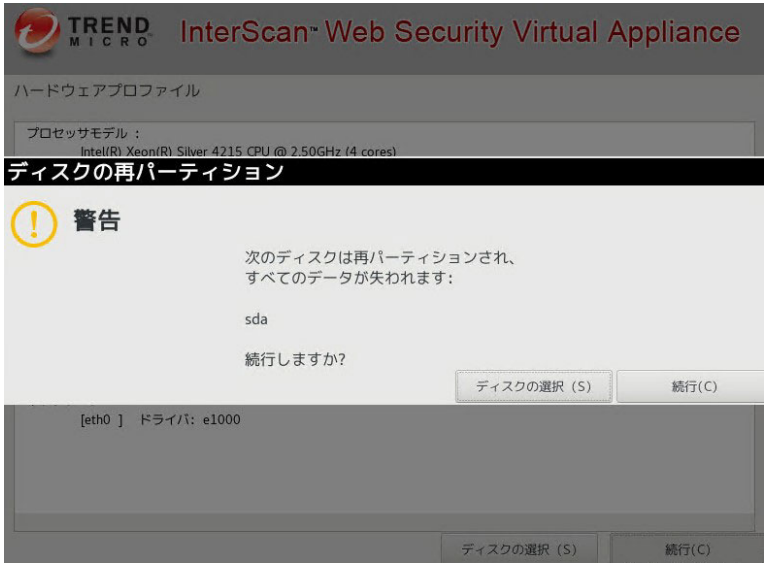


3. 使用許諾画面が表示されます。[同意する] をクリックして続行します。

4. インストールに使用するディスクを選択するように求められます。選択されているディスクに問題なければ [続行] をクリックします。

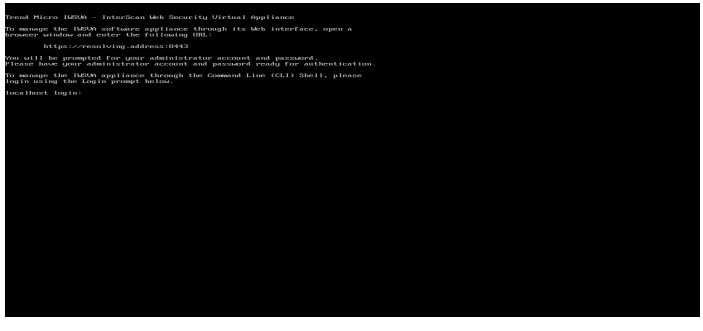
5. ハードウェアプロファイル画面が表示されます。問題なければ [続行] をクリックします。

6. ディスクが再パーティション化され、すべてのデータが失われることを通知する警告画面が表示されます。続行して問題なければ [続行] をクリックします。



7. インストールの進捗状況を示す画面が表示されます。

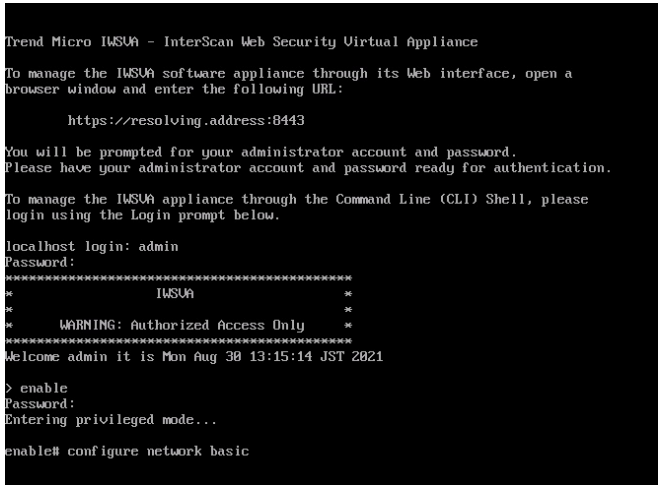
8. インストールの完了後、システムが自動的に再起動され、IWSVA の CLI シェル画面が表示されます。



9. 初期設定のシステムアカウント「admin」とパスワード「adminIWSS85」でログインします。
10. プロンプトに「enable」と入力して実行し、特権モードに入ります。パスワードを求められるので、初期パスワード「adminIWSS85」を入力します。

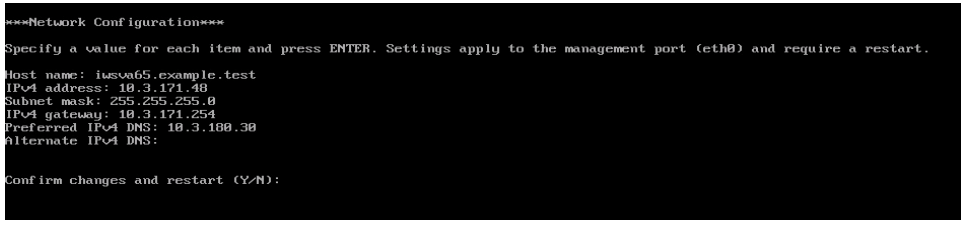
11. 以下のコマンドを実行し、ネットワーク設定を行います。

    ```
    configure network basic
    ```



12. ガイドに従って、次のネットワーク関連の設定を行います。
    - ホスト名
    - IPv4 アドレス
    - サブネットマスク
    - IPv4 ゲートウェイ
    - 優先 IPv4 DNS
    - 代替 IPv4 DNS（オプション設定、省略可）

    設定入力後、「Confirm changes and restart」と聞かれるので、問題なければ「Y」と入力してシステムを再起動します。



13. 再起動完了後、「exit」と入力して実行し、特権モードを終了します。その後、更に「exit」と入力して実行し、CLI を終了します。
14. IWSVA Web 管理コンソールにログインし、63 ページの「インストール後の注意事項」に記載の作業を実施します。Web 管理コンソールへのログインについては、63 ページの「初めて IWSVA にログインする」を参照してください。

初めて IWSVA にログインする

IWSVA が再起動したら、CLI インタフェースまたは Web 管理コンソールを通してアプライアンスにログインできます。

- CLI インタフェースの場合は、コンソールのログインプロンプトで管理者のユーザ名とパスワードを入力します。

  注意： 初めて Web 管理コンソールにログインする前に、ブラウザのポップアップブロッカを無効にしてください。ポップアップブロッカは、[Change Password] ダイアログと配置ウィザードをブロックします。

- Web 管理コンソールの場合は、ワークステーション (IWSVA 以外) 上で新しい Web ブラウザを開いて、初期 CLI バナーに指定された URL (`https://<IWSVA 6.5 SP3 の IP アドレス>:8443`) を入力します。ログインするには、IWSVA 管理者アカウントとパスワードが必要です。管理者アカウント名は「admin」で、初期パスワードは「adminIWSS85」です。

インストール後の注意事項

初期 CLI が使用可能になった後 :

- Web 管理コンソールの初回ログイン時には配置ウィザードが起動します。配置ウィザードを使用して、インストールを完了できます (「管理者ガイド」の第 2 章を参照)。
- 製品の登録とアクティベートの直後に検索エンジンとウイルスパターンファイルのアップデートをお勧めします (「管理者ガイド」の第 4 章を参照)。

第 4 章

InterScan Web Security Virtual Appliance への移行

本章で説明する内容には、次の項目が含まれます。

移行について

InterScan Web Security Virtual Appliance 6.5 SP3（以下、IWSVA) では、全面的および部分的な移行の両方がサポートされています。システムおよびアプリケーション設定を復元する場合や、現在の設定を IWSVA の置換コンピュータに適用する場合は、完全な移行をします。ポリシーおよびアプリケーションレベルの設定を置き換える場合は、部分的な移行をします。

警告： **IWSVA 6.5 SP3 では、IWSVA の同じ言語バージョンからの移行のみサポートしてます。**

完全な移行を実行する場合は、その前に、移行元と移行先の両方の IWSVA 6.5 SP3 コンピュータで、ハードウェア構成と配信モードが同じであることを確認してください。

完全な移行の後で予期しない動作が発生することを回避するために、移行先の IWSVA 6.5 SP3 コンピュータを、バックアップ設定ファイル (移行元の IWSVA 6.5 SP3 コンピュータから出力されたファイル) で指定されているものと同じ IP アドレスを使用するように設定することをお勧めします。

両方の IWSVA 6.5 SP3 コンピュータを同時にネットワークに接続しないでください。一度に接続する IWSVA 6.5 SP3 コンピュータは 1 つだけにする必要があります。

次の IWSVA 製品に関する設定情報とポリシー情報は、IWSVA に移行できます。

- IWSVA 6.5 SP2

重要な注意事項

- IWSVA の設定をバックアップファイルに出力できます。出力情報には、システムレベルとアプリケーションレベルの両方の設定が含まれます。
- Web 管理コンソールの [設定のバックアップ / 復元] 画面を使用して、IWSVA 6.5 SP3 の設定を含むバックアップファイルをインポートします。完全な移行と部分的な移行のいずれかを選択するように促す画面が表示されます。
- 設定バックアップファイル内のパスワード情報は、クリアテキストでは表示されません。
- IWSVA は、監査ログに設定のインポートまたは出力処理を記録します。

移行されない情報

次に示す項目は移行されません。

全面的に移行する場合

- データベースに格納されているログ、レポート、メッセージ、および隔離ファイル
- パターンファイルと検索エンジンファイル、および設定ファイル内の関連バージョン情報
- データベースのパスワード
- 製品のアクティベーションコード
- OS およびアプリケーションのパッチ
- 次の設定を除く、Web 管理コンソールの [管理] メニューの下にあるすべての設定
  - ユーザの識別
  - ポリシー配信
  - 隔離管理 (移行元サーバと同じディレクトリ内にある場合)
  - システム時間
  - 予約期間
  - PAC ファイル管理
  - ネットワーク設定
  - 検索方法

部分的に移行する場合

- データベースに格納されているログ、レポート、メッセージ、および隔離ファイル
- パターンファイルと検索エンジンファイル、および設定ファイル内の関連バージョン情報
- データベースのパスワードと設定
- 製品のアクティベーションコード
- 配信モードの設定
- IP アドレス、ホスト名など、システムレベルの設定
- OS およびアプリケーションのパッチ
- 次の設定を除く、Web 管理コンソールの [管理] メニューの下にあるすべての設定
  - ユーザの識別
  - ポリシー配信
  - 予約期間

移行プロセスの概要

移行の主な手順は、次のとおりです。

手順：

1. 前の IWSVA 設定をバックアップします。
2. IWSVA 6.5 SP3 をインストールします。
3. 新しい IWSVA コンピュータに、すでにバックアップ済みの設定ファイルをインポートします。移行元と移行先が IWSVA 6.5 SP3 で、両方のデバイスがスタンドアロンモードに設定されている場合は、全面的または部分的のどちらの移行を実行するかを選択できます。
4. Web 管理コンソールにアクセスして、IWSVA 6.5 SP3 を設定できます。

注意： 移行プロセスが完了すると、IWSVA 6.5 SP3 の機能に対してインポートされた初期設定が適用されます。

移行されない設定の一覧については、67 ページの「移行されない情報」を参照してください。

IWSVA 6.5 SP2 または IWSVA 6.5 SP3 から別の IWSVA 6.5 SP3 に移行する

注意： IWSVA 6.5 SP3 では、別の言語バージョンからの移行はサポートされていません。

IWSVA 6.5 SP3 デバイスから別の IWSVA 6.5 SP3 デバイスへの完全な移行は、両方のデバイスがスタンドアロンモードに設定されている場合のみサポートされます。

完全な移行を実行するには、両方の IWSVA コンピュータでハードウェア構成と配信モードが同じであることを確認してください。さらに、完全な移行の後で予期しない動作が発生することを回避するために、両方のコンピュータを、同じ IP アドレスを使用するように設定することをお勧めします。

バックアップファイルの IP アドレス情報が、ファイルのインポート先の IWSVA コンピュータの IP アドレスと異なっていると、移行の結果の画面が表示されません。この場合、[監査ログ] 画面で移行の結果を表示できます。

完全な移行の後、移行元の IWSVA コンピュータで別の管理インタフェースが有効になっている場合は、移行元の IWSVA コンピュータの管理 IP アドレスを使用して、移行先の IWSVA 6.5 SP3 コンピュータ上の Web 管理コンソールにアクセスする必要があります。

手順 :

1. 移行元の IWSVA 6.5 SP2 または IWSVA 6.5 SP3 コンピュータの Web 管理コンソールを開いて、[管理] → [設定のバックアップ / 復元] の順に選択します。[エクスポート] をクリックして、設定をバックアップします。

   画面に進行状況を示すバーが表示されます。出力プロセスが終了すると、結果画面にステータスが表示されます。設定の出力プロセスが成功した場合は、IWSVA のダイアログボックスが開いて、ローカルディスクに設定ファイルを保存するように促されます。コンピュータのローカルドライブにファイルを保存します。

2. 移行先の IWSVA 6.5 SP3 コンピュータの Web 管理コンソールを開いて、メインメニューで [管理] → [設定のバックアップ / 復元] の順にクリックします。

3. [参照] をクリックして手順 1 で保存したバックアップファイルを選択し、[インポート] をクリックします。

   注意 : 移行元が IWSVA 6.5 SP3 で移行先が IWSVA 6.5 SP3 で、両方のデバイスがスタンドアロンモードに設定されている場合は、全面的または部分的のどちらの移行を実行するかを選択できます。それ以外の場合、部分的な移行のみが実行されます。

4. いずれかのオプションを選択し、[OK] をクリックして続行します。

付録 A

導入の統合

この付録では、次の項目について説明します。

分散環境での IWSVA

InterScan Web Security Virtual Appliance 6.5（以下、IWSVA) は、分散システムを構成する一部として設計されています。また、設定によって多様なネットワーク接続を確立できます。

管理者は、次の点を確認する必要があります。

- 必要なチャネルがブロックされていないこと
- すべてのチャネルに十分なスループットがあること
- サーバが使用するソフトウェアは、サポートしているバージョンであること
- サーバは、高負荷のトラフィックを処理できること

接続の要件と特性

表 A-1 に、必要な接続とその特性を示します。

表 A-1.　必要な接続と特性

接続するコンポーネント	**トラフィック**： **タイプおよびデータ量**	**接続が切断された場合**
クライアント	実際のネットワークで測定する必要があります。	保護なし
LDAP サーバ (設定されている場合)	**タイプ**：LDAP **データ量**：中	すでに開始されているサービスでは、キャッシュ内のデータが使用されます。 新しいサービスは開始されません。
トレンドマイクロの アップデートサーバ	**タイプ**：HTTP および HTTPS **データ量**：10 ～ 50MB/ 日	IWSVA コンポーネントは時間内にアップデートできません。
Web レピュテーション	**タイプ**：HTTP **データ量**：個別のアクセスによって異なります。	すでに開始されているサービスでは、キャッシュ内のデータが使用されます。 サービスは開始されません。ユーザは要求した URL にアクセスできます。

スループットと可用性の要件

管理者は、IWSVA の可用性の要件を決定する必要があります。

- IWSVA のダウンタイムを許容できるかどうか
- 許容できる場合は、IWSVA のダウン時にどのような措置をとるか (迂回または停止)
- 複数の IWSVA インスタンスをフェイルオーバー構成にしている場合、LDAP サーバとデータベースサーバに同レベルのフェイルオーバーを適用するかどうか

LDAP との連携

複数の LDAP サーバによるマルチドメインのサポート

IWSVA には、複数の LDAP サーバと通信し、マルチドメインツリーやフォレストと同様の環境を構成できる LDAP モジュールが備わっています。

IWSVA LDAP 統合は、マルチドメインと複数の LDAP サーバをサポートします。

IWSVA Web 管理コンソールで LDAP 機能を設定するには

1. [管理] → [一般設定] → [ユーザの識別] → [ユーザの識別] タブに移動します。
2. LDAP 接続に関する必要な情報を入力します。
3. [接続のテスト] をクリックし、LDAP の設定と接続を確認します。テストが成功すると、成功を示すメッセージが表示されます。
4. [保存] をクリックして、設定を保存します。

注意： 詳細については、管理者ガイドの「ポリシーとユーザ識別方法」を参照してください。

注意： LDAP を設定する前に、LDAP ドメイン名が名前解決可能であることを確認します。

ユーザ認証用に 2 通りの認証方法があります。標準認証では、ユーザアカウントとパスワードを指定するための標準の 401 または 407 認証ダイアログボックスを提供します。クライアントコンピュータが Microsoft Active Directory 内の Windows デスクトップである場合は、透過的な認証が適用されます。キャプティブポータルは、ユーザを識別するための Web ベースの認証ページを表示

します。キャプティブポータル認証にはゲストポリシーを適用できます。キャプティブポータルでのみ使用可能な NAT およびターミナルサーバ環境でユーザ識別を実現するために、Cookie モードが存在します。

クエリ対象の AD サーバおよびリモート AD サーバで Windows Active Directory（AD) グローバルカタログが有効になっている場合、IWSVA などの LDAP クライアントは、対象ドメインに属しているオブジェクトだけでなく、その他のリモートドメインに属しているオブジェクトも一括して検索できます。グローバルカタログサーバは、ポート 3268 で LDAP 要求を受け取ります。これにより、フォレスト内のすべてのドメインを対象にユニバーサルグループのユーザ認証情報、フルネーム、およびメンバーシップを検索できます。リモートドメインに属するユーザやグループメンバーで親グループが構成されており、それらのリモートドメインが多様なサブドメインレベルにある場合、グローバルカタログを使用して IWSVA LDAP ポリシーを作成すると便利です。

この機能を使用するには、Web 管理コンソールの [管理] → [設定] → [ユーザの識別] 画面で、IWSVA が使用するメイン LDAP サーバを指定する必要があります。その際、指定したグローバルカタログ対応 Active Directory サーバが、初期設定の LDAP 通信ポート 389 ではなく、ポート 3268 で通信できるように設定します。

注意： グローバルカタログは Microsoft Active Directory のみで使用できます。グローバルカタログポートを使用することで、LDAP オブジェクト検索のパフォーマンスが向上し、Active Directory ツリーの多数のサブレベル（4 つ以上) に属するオブジェクトを検索できます。ただし、IWSVA でグローバルカタログを利用するには、オブジェクトの要求先 AD、および要求されたユーザオブジェクトまたはグループオブジェクトが存在する AD で、グローバルカタログが有効になっている必要があります。

ヒント： グローバルカタログを有効にしたルート Active Directory サーバを検索できるように設定することをお勧めします。また、ポリシーの適用時には、ユニバーサルグループを使用してグループをネストすることもお勧めします。この設定はグローバルカタログで確認できます。また、Active Directory にも表示されます。詳細については、Microsoft サポートを参照してください。

透過モードでの LDAP 認証

透過モード（ブリッジモードおよび WCCP モード) で配置されている IWSVA 上で LDAP 認証を設定するには、その前に、次の基準をよく読んで、各項目が完全に満たされていることを確認してください。

- IWSVA には、Web 管理コンソールの [管理] → [ネットワーク設定] → [ネットワークインタフェース] 画面で有効なホスト名が割り当てられている必要があります。社内 DNS サーバにそのホスト名が入力されていることも確認してください。
- ユーザ ID キャッシュが有効であることを確認してください。ユーザ ID キャッシュは初期設定で有効になっています。何らかの理由により無効になっている場合は、透過モードの認証を有効にする前に、ユーザ ID キャッシュを再度有効にする必要があります。CLI で「`configure module ldap ipuser_cache enable`」コマンドを使用して、ユーザ ID キャッシュを有効にできます。
- 初期設定では、IWSVA は、ユーザ ID キャッシュ情報を最長で 2 時間保持します。キャッシュのタイムアウトの値をこれより低くする必要がある場合は、CLI の「`configure module ldap ipuser_cache interval`」コマンドを使用して、もっと短いキャッシュ間隔を設定します。
- 認証が有効になると、IWSVA は、インターネットにアクセスしようとしているすべての非ブラウザアプリケーションをブロックします。たとえば、MSN アプリケーションは、ユーザが IWSVA サーバにログインできるようになる前に、インターネットにアクセスしようとする可能性があります。この場合、ユーザが IWSVA に対して正常に認証されないと、アプリケーションはブロックされます。次のいずれかの処理を実行できます。
  a. アプリケーションがアクセスする URL を「グローバル URL の信頼」に追加することで、そのアプリケーションに対する LDAP 認証を実行しないようにします。このリスト内の URL については、認証もコンテンツ検索も実行されません。
  b. ユーザに対して、各自の Web ブラウザを開き、インターネットへのアクセスを必要とするアプリケーションを起動する前に認証を受けるよう指示します。
  c. クライアントコンピュータの IP アドレスを「LDAP 認証の許可リスト」に追加します。このリスト内の IP アドレスについては、LDAP 認証は実行されません。
- ユーザ認証またはグループ認証が、Active Directory を使用したプロキシ転送モードか透過モードのいずれかで有効になっている場合、Internet Explorer Web ブラウザの自動認証機能を利用することができます。自動認証を使用すると、ドメインネットワークにすでにログオンしているクライアントは、ユーザ名やパスワードなどのログオン情報の入力を求められることなく、ローカルのイントラネットにアクセスできます。つまり、パスワード入力のポップアップ画面は表示されません。

注意： 各クライアントコンピュータ上で自動認証を有効にするように、IE を設定してください。

詳細については、「管理者ガイド」を参照してください。

WCCP を使用した Cisco 製ルータと統合する

クライアントコンピュータのブラウザ設定を変更しなくても、Cisco 製ルータをゲートウェイとして使用しているネットワークで IWSVA を使用できます。これは、Cisco の WCCP プロトコルを利用して実現されます。

注意： WCCP モードでの配置方法の詳細については、IWSVA 6.5 SP3「管理者ガイド」の「付録 E: WCCP の配信およびトラブルシューティング」を参照してください。

リバースプロキシを使用して HTTP サーバまたは FTP サーバを保護する

HTTP サーバを保護している場合は、HTTP 検索サービスをリバースプロキシモードで使用するように設定します。

リバースプロキシモードを使用するには

1. [管理] → [配置ウィザード] に移動します。

   注意： 配置ウィザードは、管理者が初めてログインしたときに自動的に起動します。

2. [ようこそ] 画面で [開始] をクリックします。
3. [配信モード] 画面で [リバースプロキシモード] を選択します。
4. [次へ] をクリックします。
5. [HTTP 待機ポート]、[保護対象サーバ]、および [ポート番号] に情報を入力します。
6. 必要に応じて [SSL ポートを有効にする] チェックボックスをオンにして [SSL ポート番号] を入力し、証明書と秘密鍵をアップロードしてから、一致するパスフレーズを入力します。
7. [次へ] をクリックします。

8. [ネットワークインタフェース]、[静的ルート]、[製品のアクティベーション]、および [システム時間] 画面に必要な設定情報を入力します。
9. [概要] 画面ですべての設定を確認して、[送信] をクリックします。
10. 配置が正常に実行されると、IWSVA がリバースプロキシモードに変更されます。

注意： HTTP/HTTPS 環境でのリバースプロキシ設定を単純にするため、IWSVA では、配置ウィザードで設定されているポート (初期設定値は 433) で外部からの (HTTPS) 接続を待機し、データを複合および検索して、そのデータを保護対象サーバのポート 80 に HTTP プロトコルを使用して転送できます。

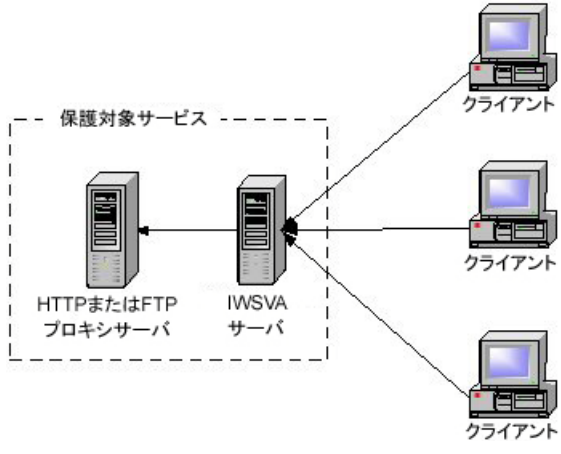


図 A-1. 専用サーバを保護する

FTP サーバを保護している場合は、FTP 検索サービスを FTP プロキシを使用するように設定します。

- `/etc/iscan/IWSSPIProtocolFtp.pni` ファイル内の [ftp] セクションの次のパラメータを変更します。
  - `proxy_mode=dedicated` 動作モードを指定します。
  - `ftp_server` 保護する FTP サーバの IP アドレスを指定します。

- `ftp_server_port` 保護するサーバの TCP ポートを指定します。

  設定が完了したら、次のコマンドを実行して FTP 検索デーモンを再起動します。

  ```
  /etc/iscan/S99ISftp restart
  ```

ICAP デバイスと統合する

ICAP 1.0 準拠のキャッシュサーバを利用しているネットワーク上に IWSVA を導入できます。

ICAP 1.0 対応キャッシュサーバの設定

ICAP サーバと通信できるように ICAP クライアントを設定します。

- 78 ページの「Blue Coat Port 80 Security Appliance の ICAP を設定するには」
- 81 ページの「Cisco CE ICAP サーバについて ICAP を設定するには」

Blue Coat Port 80 Security Appliance について ICAP を設定する

Blue Coat Port 80 Security Appliance の ICAP を設定するには

1. Web ブラウザのアドレスバーに「`http://{` **キャッシュサーバの** `IP` **アドレス** `}:8081`」と入力して管理コンソールにログオンします。ここでは、初期設定の管理ポートとして 8081 を指定します。

   たとえば、最初のインストール時に設定した IP アドレスが「123.123.123.12」の場合は、Web ブラウザに URL「http://123.123.123.12:8081」を入力します。

2. [Management] を選択します。入力画面が表示されたら、ログオンユーザ名とパスワードを入力します。
3. 左側のメニューで [ICAP] を選択し、[ICAP Services] を選択します。
4. [New] をクリックします。[Add ICAP Service] 画面が表示されます。
5. [ICAP service name] フィールドに、サービス名を英数字で入力します。[OK] をクリックします。
6. 新しい ICAP サービス名を選択し、[Edit] をクリックします。

   [Edit ICAP Service { サービス名 }] 画面が表示されます。

7. 次の情報を入力または選択します。
   a. ICAP バージョン番号。ここでは [1.0] を選択します。
   b. ウイルス検索サーバのホスト名または IP アドレスを含むサービス URL、および ICAP ポート番号。初期設定では、ICAP ポート番号は 1344 です。
      - 応答モードの場合

      `icap://{ICAP サーバの IP アドレス }:1344`

      - 要求モードの場合

      `icap://{ICAP サーバの IP アドレス }:1344/REQ-Service`
      ICAP サーバの IP アドレスは、IWSVA ICAP の IP アドレスです。
   c. 最大接続数 (1 ～ 65,535 の範囲)。初期設定値は「5」です。
   d. 接続タイムアウト。Blue Coat Port 80 Security Appliance がウイルス検索サーバからの応答を待つ最大秒数です。60 ～ 65,535 の値を指定できます。初期設定値は 70 秒です。
   e. サポートされた方法の種類を選択します (応答モードまたは要求モード)。
   f. 初期設定のプレビューサイズ (0 バイト) を使用します。
   g. ICAP サーバから設定を取得するには、[Sense settings] をクリックします (推奨)。
   h. ICAP サービスを検診のために登録するには、[Health Check Options] の [Register] をクリックします。
8. [OK] をクリックし、次に [Apply] をクリックします。

注意： すでに設定されている ICAP サービスを編集できます。サーバの設定を再度編集するには、サービスを選択して [Edit] をクリックします。Blue Coat を対象とする ICAP の設定では、例としてバージョン 2.1.07 を使用しています。これらの設定は、使用している Blue Coat のバージョンによって異なる場合があります。

---

9. 応答モードまたは要求モードのポリシーを追加します。

   Visual Policy Manager を実行するには、Sun Microsystems, Inc. の Java 2 Runtime Environment Standard Edition (別名 Java Runtime または JRE) の v.1.3.1 以降が必要です。使用しているワークステーションに JRE がすでにインストールされている場合は、Security Gateway により別のブラウザが開き、Visual Policy Manager が起動します。ポリシーエディタを最初に起動すると、空のポリシーが表示されます。

   ワークステーションに JRE をインストールしていない場合は、セキュリティ警告画面が表示されます。作業を続行するには、[Yes] をクリックします。指示に従って JRE をインストールします。

応答モードポリシーを追加するには

a. [Management] を選択します。入力画面が表示されたら、ログオンユーザ名とパスワードを入力します。

b. 左側のメニューで [Policy] を選択し、[Visual Policy Manager] を選択します。

c. [Start] をクリックします。

[Java Plug-in Security Warning] 画面が表示された場合、[Grant this session] をクリックします。

d. メニューバーで [Edit] → [Add Web Content Policy] の順に選択します。

[Add New Policy Table] 画面が表示されます。

e. [Select policy table name] フィールドにポリシー名を入力します。[OK] をクリックします。

f. [Action] 列で [Bypass ICAP Response Service] を右クリックし、[Set] をクリックします。

[Add Object] 画面が表示されます。

g. [New] をクリックし、[Use ICAP Response Service] を選択します。

[Add ICAP Service Action] 画面が表示されます。

h. [ICAP Service/Cluster Names] で ICAP サービス名を選択します。[On communication error with ICAP service] で [Deny the request] を有効にします。[OK] をクリックし、もう一度 [OK] をクリックします。

i. [Install Policies] をクリックします。

要求モードポリシーを追加するには

a. [Management] を選択します。入力画面が表示されたら、ログオンユーザ名とパスワードを入力します。

b. 左側のメニューで [Policy] を選択し、[Visual Policy Manager] タブを選択します。

c. [Start] をクリックします。[Java Plug-in Security Warning] 画面が表示された場合、[Grant this session] をクリックします。

d. メニューバーで、[Edit] → [Add Web Access Policy] の順に選択します。

[Add New Policy Table] 画面が表示されます。

e. [Select policy table name] フィールドにポリシー名を入力します。[OK] をクリックします。

f. [Action] 列で [Deny] を右クリックし、[Set] をクリックします。

[Add Object] 画面が表示されます。

g. [New] をクリックし、[Use ICAP Request Service] を選択します。[Add ICAP Service Action] 画面が表示されます。

h. [ICAP Service/Cluster Names] で ICAP サービス名を選択します。

i. [On communication error with ICAP service] で [Deny the request] を有効にします。

j. [OK] をクリックし、もう一度 [OK] をクリックします。

k. [Install Policies] をクリックします。

10. 現在のポリシーを確認するには、[Install Policies] 画面に移動し、[Policy Files] タブをクリックし、[Current Policy] をクリックします。

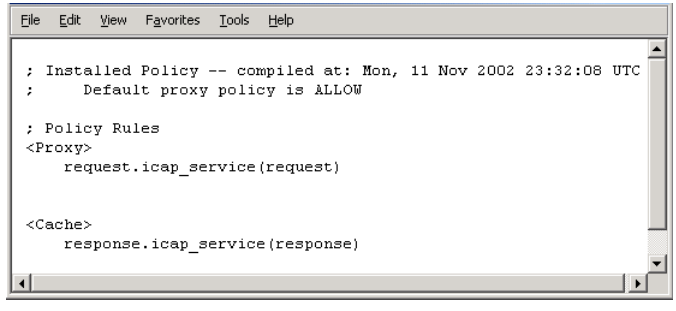


図 A-2. 現在設定されているポリシー

Cisco CE ICAP Servers について ICAP を設定する

IWSVA では、Cisco ICAP サーバ (CE バージョン 5.1.3, b15) がサポートされています。ICAP 設定はすべてコマンドラインインタフェース (CLI) を通じて実行されます。Cisco ICAP の実装に関連付けられたユーザインタフェースはありません。

Cisco CE ICAP サーバについて ICAP を設定するには

1. Cisco CE コンソールを開きます。
2. 設定モードを入力するには、「`config`」と入力します。
3. 「`ICAP`」と入力します。ICAP 関連のすべてのコマンドが一覧表示されます。
4. 次のように入力して応答変更サービスを作成します。

   `icap service {` **応答モードサービス名** `}`

   ICAP サービスの設定メニューが開きます。使用可能なすべてのコマンドが一覧表示されます。次のコマンドを入力します。

   `server icap://{ICAP` **サーバの** `IP` **アドレス** `}:1344/resp` (サーバタイプの割り当て)

   `vector-point respmod-precache` (適切なベクタポイントタイプの割り当て)

   `error-handling return-error` (適切なエラー処理タイプの割り当て)

`enable` (ICAP 複数サーバ設定の有効化)

5. 「`exit`」と入力します。
6. 次のように入力して、要求変更サービスを作成します。

   `icap service {` **要求モードサービス名** `}`

   このコマンドを実行すると ICAP サービス設定メニューに切り替わり、使用可能なすべてのコマンドが一覧表示されます。次のコマンドを発行します。

   `server icap://{ICAP` **サーバの** `IP` **アドレス** `}:1344/REQ-Service` (サーバタイプの割り当て)

   `vector-point reqmod-precache` (適切なベクタポイントタイプの割り当て)

   `error-handling return-error` (適切なエラー処理タイプの割り当て)

   `enable` (ICAP 複数サーバ設定の有効化)
7. 「`exit`」と入力します。
8. その他の設定の手順として、次のように入力します。

   `icap append-x-headers x-client-ip` (レポートの X クライアントヘッダを有効にする)

   `icap append-x-headers x-server-ip` (レポートの X サーバヘッダの有効化)

   `icap rescan-cache ISTag-change` (アップデートの ISTAG 再検索をオンにする)

   `icap bypass streaming-media` (ICAP 検索からのストリーミングメディアの除外)

   `icap apply all` (すべての設定を適用し、ICAP タイプをアクティベート)

   `show icap` (現在の ICAP 設定をルート CLI メニューに表示)

ウイルス検索サーバクラスタを設定する

Blue Coat Port 80 Security Appliance を複数のウイルス検索サーバで稼働させるには、Security Gateway にクラスタを設定する必要があります。このためには、クラスタを追加し、対応する ICAP サービスをそのクラスタに追加します。

管理コンソールを使用してクラスタを設定するには

1. [Management] を選択します。

   入力画面が表示されたら、ログオンユーザ名とパスワードを入力します。
2. 左のメニューから [ICAP] をクリックし、[ICAP Clusters] タブをクリックします。
3. [New] をクリックします。

   [Add ICAP Cluster] 画面が表示されます。

4. [ICAP cluster name] フィールドに、クラスタ名を英数字で入力します。[OK] をクリックします。
5. 新しい ICAP クラスタ名を選択し、[Edit] をクリックします。

   [Edit ICAP Cluster name] 画面が表示されます。
6. クラスタに ICAP サービスを追加するには、[New] をクリックします。

   [Add ICAP Cluster Entry] 画面が表示されます。選択リストには、クラスタに追加できるすべてのサービスが一覧表示されます。
7. サービスを選択して、[OK] をクリックします。
8. ICAP クラスタエントリを選択し、[Edit] をクリックします。

   [Edit ICAP Cluster Entry { エントリ名 }] 画面が表示されます。
9. [ICAP cluster entry weight] で 0 ～ 255 から重み付けを割り当てます。
10. [OK] をクリックし、もう一度 [OK] をクリックしてから [Apply] をクリックします。

クラスタ設定またはエントリを削除する

ウイルス検索サーバクラスタ全体の設定を削除することも、個別のエントリをクラスタから削除することもできます。

注意： Blue Coat Port 80 Security Appliance ポリシーのポリシールールでクラスタ名を使用している場合は、そのクラスタを削除しないでください。

管理コンソールを使用してクラスタ設定を削除するには

1. [Management] を選択します。入力画面が表示されたら、ログオンユーザ名とパスワードを入力します。
2. 左側のメニューで [ICAP] を選択し、[ICAP Clusters] タブを選択します。
3. 削除するクラスタをクリックします。
4. [Delete] をクリックし、[OK] をクリックして削除を確定します。

「X-Virus-ID」ヘッダと「X-Infection-Found」ヘッダを有効化する

IWSVA では、ウイルスが検出されるたびに、ICAP サーバから 2 つのオプションヘッダ「X-Virus-ID」と「X-Infection-Found」を返すことができます。ICAP クライアントの多くはこれらのヘッダを使用しないため、初期設定では、パフォーマンスを確保する目的からこれらのヘッダは返されません。これらのヘッダは、IWSVA 管理コンソールで有効にする必要があります。

- 「X-Virus-ID」には、検出したウイルスや脅威の名前を記述した US-ASCII テキスト 1 行が含まれます。以下に例を示します。

  `X-Virus-ID: EICAR` **テスト文字列**

- 「X-Infection-Found」には、感染の種類を示す数値コード、解決策、およびリスクについての説明が表示されます。

パラメータ値の詳細については、次を参照してください。

`http://www.icap-forum.org/`

X-Virus-ID ヘッダおよび X-Infection-Found ヘッダを有効にするには

1. IWSVA 管理コンソールのメインメニューから [管理] → [ネットワーク設定] → [配信モード] の順に選択します。
2. [配信モード] 画面で、[「X-Virus-ID」ICAP ヘッダを有効にする] または [「X-Infection-Found」ICAP ヘッダを有効にする] (あるいはその両方) を選択します。

付録 B

調整とトラブルシューティング

この付録では、次の項目について説明します。

- 86 ページの「IWSVA パフォーマンスの調整」
- 89 ページの「トラブルシューティング」

IWSVA パフォーマンスの調整

画面表示が遅くなるなどの問題が発生した場合は、以下の調整手順を参照してください。

URL フィルタ

InterScan Web Security Virtual Appliance 6.5（以下、IWSVA）は、トレンドマイクロの URL フィルタエンジンを使用し、Web レピュテーション機能が提供するデータに基づいて URL の分類とレピュテーション評価を行います。初期設定の毎週のアップデートにより、URL フィルタエンジンを最新の状態にすることをお勧めします。

IWSVA では、Web レピュテーションのフィードバック、URL フィルタモジュール、またはこれら両方を使用して URL アクセスを制御できます。Web レピュテーションと URL フィルタモジュールの組み合わせは、複合型脅威に対する保護策で、IWSVA によって提供されます。

URL フィルタモジュールは、URL が属するカテゴリに基づいて、Web アクセスを許可または拒否します。Web レピュテーションは、要求された URL が、フィッシング脅威かファーミング脅威か、ハッキングの可能性はないか、または信頼できないレピュテーションスコアでないかという判断に基づいて、Web アクセスを許可または拒否します。オプションの URL フィルタモジュールと Web レピュテーションは、ユーザが指定するポリシー内容によって制御されます。

詳細については、「管理者ガイド」の第 10 章を参照してください。

LDAP パフォーマンスの調整

IWSVA でユーザ / グループ名の認証識別方法（LDAP）を使用する場合、HTTP プロキシのパフォーマンスは、LDAP ディレクトリサーバの応答性によって異なります。場合によっては、HTTP 要求が発生するたびに、LDAP クエリを実行して対象ユーザの本人性を確認しなければなりません。このため、IWSVA と LDAP サーバ間のクエリが増加し、LDAP サーバ自体の負荷が増大します。

LDAP 内部キャッシュ

必要な LDAP クエリ量を減らすために、IWSVA はクライアント IP アドレスとユーザ ID 間のキャッシュを提供しています。

このキャッシュは、クライアント IP アドレスと、同じ IP アドレスで最近認証されたユーザを関連付けます。過去に認証された要求と同じ IP アドレスから発行された要求は、新しい要求が設定可能な期間内に認証から発行された場合であれば、同じユーザのものであると見なされます。ただし、IWSVA で参照されるクライアント IP アドレスは、その時間内においてユーザに対して一意にする

必要があります。したがって、クライアントと IWSVA との間においてプロキシサーバやソース NAT のある環境では、このキャッシュは有用ではありません。DHCP で頻繁にクライアント IP アドレスの割り当てを変更する環境でも、同様に有用ではありません。

このキャッシュを有効 / 無効にするには、`/etc/iscan/intscan.ini` 設定ファイルの `[user-identification]` セクションにある `enable_ip_user_cache` 設定を変更します。

パラメータを設定したら、次のコマンドを使用して IWSVA デーモンを再起動します。

```
/etc/iscan/S99ISproxy stop
```

```
/etc/iscan/S99ISproxy start
```

クライアント IP アドレスとユーザ ID 間のキャッシュの生存期間を設定するには、[管理] → [一般設定] → [ユーザの識別] → [ユーザの識別] タブにて次のオプションを選択します。

- 0: 固定 TTL
  1: 前回アクティブな TTL

固定 TTL

クライアント IP アドレスとユーザ ID 間のキャッシュに含まれるレコードの生存期間はそれぞれ異なります。レコードの生存期間が終了すると、そのレコードは削除されます。レコードの生存期間は次のように計算されます。

生存期間 = レコードの生成時間 + 固定 TTL

前回アクティブな TTL

クライアント IP アドレスとユーザ ID 間のキャッシュにレコードを追加する際、そのレコードに 120 分など事前設定された生存期間が設定されます。例えば、生存期間が終了する前にレコードがヒットすると、その生存期間が更新されて再度 120 分になります。

IWSVA と LDAP を連携させる場合は、HTTP 要求の認証によって LDAP ディレクトリサーバに課せられる負荷を考慮する必要があります。クライアント IP アドレスとユーザ ID の関連付けキャッシュを効果的に使用できない環境では、IWSVA が HTTP 要求を受信する速度と同じ速度でディレクトリサーバがクエリを処理できる必要があります。

LDAP 認証が有効なときは冗長ログを無効にする

LDAP が有効になっている場合、サーバのパフォーマンスを考慮して、`/etc/iscan/intscan.ini` ファイルの [http] セクションにある「verbose」パラメータで冗長ログをオフにすることをお勧めします。本来、冗長ログは、ソフトウェア開発者が、異常なアプリケーション動作の特定やトラブルシューティングに使用します。実運用環境では、通常、冗長ログは必要ありません。

冗長ログと LDAP を両方とも有効にすると、ユーザ認証情報とグループメンバーシップ情報がログフォルダ内の HTTP ログに記録されます。内部トラフィック量やユーザの所属先グループの数に応じて、各ユーザにつき数百行のログが出力されます。このため、大容量のディスク領域が使用されます。冗長ログを使用すると、頻繁に OS から I/O 操作が発行され、その間はサービスがビジー状態になりやすくなります。これにより、サービスが HTTP 要求に即座に応答できないことがあります。その結果、遅延が発生する場合があります。HTTP トラフィックが過度に集中する環境では、IWSVA を冗長モードで起動したとき、大きな遅延が発生する可能性があります。

透過モードでの LDAP 認証

透過モードで配置されている IWSVA 上で LDAP 認証を設定するには、その前に、次の基準をよく読んで、各項目が完全に満たされていることを確認してください。

- IWSVA に有効なホスト名が割り当てられている必要があります ([管理] → [配置ウィザード] をクリックし、その後 [ネットワークインタフェース] 画面でホスト名を更新)。社内 DNS サーバにそのホスト名が入力されていることも確認してください。
- ユーザ ID キャッシュが有効であることを確認してください。ユーザ ID キャッシュは初期設定で有効になっています。何らかの理由により無効になっている場合は、透過モードの認証を有効にする前に、ユーザ ID キャッシュを再度有効にする必要があります。CLI で `configure module ldap ipuser_cache enable` コマンドを使用して、ユーザ ID キャッシュを有効にできます。
- 初期設定では、IWSVA は、ユーザ ID キャッシュ情報を最長で 2 時間保持します。キャッシュのタイムアウトの値をこれより低くする必要がある場合は、CLI の「`configure module ldap ipuser_cache interval`」コマンドを使用して、もっと短いキャッシュ間隔を設定します。
- 認証が有効になると、IWSVA は、インターネットにアクセスしようとしているすべての非ブラウザアプリケーションをブロックします。たとえば、MSN アプリケーションは、ユーザが IWSVA サーバにログインできるようになる前に、インターネットにアクセスしようとする可能性があります。この場合、ユーザが IWSVA に対して正常に認証されないと、アプリケーションはブロックされます。次のいずれかの処理を実行できます。
  a. アプリケーションがアクセスする URL を「グローバル URL の信頼」に追加することで、そのアプリケーションに対する LDAP 認証を実行しないようにします。このリスト内の URL については、認証もコンテンツ検索も実行されません。
  b. ユーザに対して、各自の Web ブラウザを開き、インターネットへのアクセスを必要とするアプリケーションを起動する前に認証を受けるよう指示します。
  c. クライアントコンピュータの IP アドレスを「LDAP 認証の許可リスト」に追加します。このリスト内の IP アドレスについては、LDAP 認証は実行されません。

注意： ユーザ / グループ認証が、Active Directory を使用したプロキシ転送モードか透過モードのいずれかで有効になっている場合、Internet Explorer Web ブラウザの自動認証機能を利用することができます。自動認証を使用すると、ドメインネットワークにすでにログオンしているクライアントは、ユーザ名やパスワードなどのログオン情報の入力を求められることなく、ローカルのイントラネットにアクセスできます。つまり、パスワード入力のポップアップ画面は表示されません。

設定手順の詳細については、「IWSVA 管理者ガイド」を参照してください。

トラブルシューティング

トラブルシューティングのヒント

- **問題**：[データベース設定] 画面で指定したデータベースに IWSVA から接続できない。IWSVA 管理コンソールに次のようなエラーメッセージが表示されます。

  ```
  JDBC-ODBC BRIDGE: [UNIXODBC] Could not connect to the server; Could not connect to remote socket.
  ```

  解決策：

  - ODBC 接続またはデータベースサーバを確認して、再試行してください。
- **問題**：IWSVA 管理コンソールに次のような認証エラーメッセージが表示される。

  ```
  JDBC-ODBC BRIDGE: [UNIXODBC]FATAL: Password authentication failed for user.
  ```

  解決策：

  - PostgreSQL Server の認証情報を確認してください。さらに、[管理] → [一般設定] → [データベースの接続設定] で、データベース設定が適切であることを確認してください。問題が解決されない場合は、`/etc/iscan/odbc.ini` ファイルに指定されている権限が正しいことを確認してください。

テクニカルサポートに問い合わせる前に

問題が発生してテクニカルサポートに問い合わせる場合、詳細な情報が提供されることにより、効率よく処理できます。

インストールに関する問題

インストールに関する問題をすみやかに解決するため、トレンドマイクロのテクニカルサポートへ問い合わせる前に、次の情報を収集してください。

1. IWSVA のバージョン番号とビルド番号
2. インストール中に発生したエラーのスクリーンショット
3. 問題の発生したインストールの段階

一般的な機能に関する問題

IWSVA の機能に問題がある場合は、次の情報を収集してテクニカルサポートに提示してください。

- IWSVA の現在の状態を示すシステムファイル。

  これらのファイルを生成するには、Web 管理コンソールで [管理] → [サポート情報] の順に選択し、[システム情報ファイルの生成] ボタンをクリックします。このボタンは、ケース診断ツール（CDT) の拡張機能です。このボタンをクリックするだけで、IWSVA と OS の現在の「状態」を収集できます。

  [システム情報ファイルの生成] ボタンをクリックして生成したシステムファイルは、以下の形式の 1 つのファイルにまとめられます。

  `info_YYYYMMDD_hhmmss_999999.tar.gz`

  `YYYY`、`MM`、`DD` は、パッケージファイルが生成された年月日です。`999999` は Linux タイムコードです。

  システムファイルには次の情報が保存されます。

  - IWSVA **情報** — IWSVA の製品バージョン、エンジンバージョン、ビルド番号、現在のパターンファイル（入手可能な場合)、IWSVA HotFix、および Service Pack 情報。製品設定および他製品との連携設定もこの情報に含まれます。
  - IWSVA **システムログ** — IWSVA ログ、デバッグログ、および syslogd デーモンによって生成されたログ（システムログが有効な場合)。
  - **システム / ネットワーク情報** — ハードウェア構成、OS、ビルド、システムリソースの状態、インストールされているその他のアプリケーション、およびネットワーク情報。
  - **設定ファイル** — Control Manager エージェントや MCP エージェントなど、調査に必要な設定情報。
- まず、以下の 1 番目のディレクトリにコアファイルが作成され、その後、2 番目のディレクトリに移動されます。

  - `/etc/iscan/coredumps`
  - `/etc/iscan/UserDumps`

  問題の原因をすみやかに診断できるよう、トレンドマイクロのテクニカルサポートに連絡するときは、これらのファイルを使用します。これらのファイルを自分で表示するには、GDB (GNU プロジェクトデバッガ) などのプログラムを使用します。

- 問題が発生した日のログファイル。
  - 問題が発生した日のすべてのログファイル (初期設定では、ログは `/etc/iscan/log` に保存されます)。
  - `/etc/iscan/intscan.ini` ファイルの [ftp] セクション、[http] セクション、および [notification] セクションで、「`verbose=1`」と設定します。
- 設定したら、対応するデーモンを再起動します。
  - http デーモンを再起動するには、次のコマンドを入力します。
    ```
    /etc/iscan/S99ISproxy stop
    /etc/iscan/S99ISproxy start
    ```
  - ftp デーモンを再起動するには、次のコマンドを入力します。
    ```
    /etc/iscan/S99ISftp restart
    ```
  - 通知デーモンを再起動するには、次のコマンドを入力します。
    ```
    /etc/iscan/S99ISsvcmonitor restart
    ```
- Web 管理コンソールで [システムステータス] 画面のスクリーンショットを撮ります。
- IWSVA のバージョン番号を記録します。
- URL サンプル (必要な場合) または、アクセス時に問題が発生する URL のアドレスを取得します。
- CLI から capture コマンドを使用して、失敗したトランザクションのパケットをキャプチャします (たとえば、enable モードで「`start task capture interface eth0`」と入力します)。

付録 C

IWSVA のインストールと配置のベストプラクティス

この付録では、次の項目について説明します。

IWSVA のインストールの概要

このインストールの概要では、InterScan Web Security Virtual Appliance 6.5（以下、IWSVA) をインストールおよび設定して、コア検索、ログ、レポートといった機能を動作させる主な手順をとりまとめて説明します。「IWSVA 管理者ガイド」のベストプラクティスに関する付録の詳細を示すセクションに、必要な資料をダウンロードするための URL が記載されています。IWSVA のインストール手順の詳細については、次の章を参照してください。

- 55 ページの「InterScan Web Security Virtual Appliance のインストール」
- 65 ページの「InterScan Web Security Virtual Appliance への移行」

機能とコマンドの詳細な手順については、「IWSVA 管理者ガイド」を参照してください。

IWSVA をインストールおよび設定するには

1. 最新の IWSVA ソフトウェアとドキュメントセットをトレンドマイクロのダウンロードセンターから入手します。IWSVA 製品とアップデートは次の URL からダウンロードできます。

   https://www.trendmicro.com/ja_jp/business/products/downloads.html

2. 製品を登録してアクティベーションコードを入手します。これらは、IWSVA とそのコアモジュールをアクティブ化するために必要となります。製品は次の URL で登録できます。

   https://clp.trendmicro.com/fullregistration

3. 「IWSVA インストールガイド」を参照して、お使いの環境をサポートするための配置トポロジと IWSVA ユニットの数を決定します。
4. IWSVA アプリケーションとステップ 2 から取得したアクティベーションキーをインストールします。このタスクを実行するには、[管理] → [製品ライセンス] 機能を使用します。
5. インストールした IWSVA 製品に適用可能なサービスパックとクリティカルパッチをダウンロードします。サービスパックとクリティカルパッチはバージョン固有であり、累積的です。最新のサービスパックにはそれ以前のサービスパックの HotFix とクリティカルパッチが含まれます。ベストプラクティスは、IWSVA バージョンの最新のサービスパックと最新のクリティカルパッチをダウンロードしてインストールし、IWSVA ユニットを最新にすることです。

   IWSVA では、アプリケーションサービスパックとは別個にオペレーションシステムのアップデートが提供されます。アプリケーションサービスパックとともに、最新のオペレーティングシステムパッチもダウンロードされ適用されていることを確認してください。システムをアップグレードする前に、必ずパッチの ReadMe ファイルを読み、インストール手順を十分に理解してください。
   これらのタスクを実行するには、[管理] → [システムアップデート] 機能を使用します。
6. システムの設定を行います。これには、システム日時の設定、オプションのネットワーク構成の設定（リモートアクセス用の SSH の有効化、PING、オプションの静的ルートなど)、オプショ

ンの上位プロキシサーバの定義、SNMP の有効化などが含まれます。これらのタスクを実行するには、[管理] 機能を使用します。

7. LDAP ユーザおよび LDAP グループまたはどちらか一方に基づいて、ポリシーの適用、イベントの記録、インターネットアクティビティのレポートを行う必要がある場合は、IWSVA を企業 LDAP サーバに設定します。この機能を実行するには、[管理] → [一般設定] → [ユーザの識別] タブを使用します。
8. パターンファイルと検索エンジンの自動アップデート間隔の初期設定を確認します。必要に応じて要件を満たすように変更します。また、新たにインストールした IWSVA システムの手動アップデートを実行して、署名ファイルと検索エンジンを更新します。これらのタスクを実行するには、[アップデート] 機能を使用します。
9. ログの設定値と外部 syslog サーバについて、ログの詳細レベルとサードパーティのログサポートを設定します。システムログ保持オプションの初期設定を確認し、必要に応じて要件を満たすように変更します。これらのタスクを実行するには、[ログ] 機能を使用します。
10. インターネットトラフィックを監視し制御するためのポリシーを作成します。ポリシーは、次のプロトコルとトラフィックタイプに対して定義できます。アプリケーション制御、HTTPS、HTTP、URL フィルタ、アクセス割り当て、および FTP です。これらのタスクを実行するには、[アプリケーション制御]、[HTTP]、[FTP] 機能を使用します。
11. レポートのテンプレートと予約レポートを定義します。日次、週次、月次レポートに関して保存する予約レポート数の初期設定を確認します。必要に応じて要件を満たすように変更します。これらのタスクを実行するには、[レポート] 機能を使用します。
12. 管理者アカウントをバックアップしたり、他のユーザに管理機能とレポート機能へのアクセス権を付与したりするために追加の管理者アカウント、監査担当者アカウント、またはレポータアカウントを作成します。このタスクを完了するには、[管理] → [管理コンソール] → [アカウント管理] 機能を使用します。
13. IWSVA 設定のバックアップを取り、新たに作成した設定のコピーを保持します。このタスクを完了するには、[管理] → [設定のバックアップ / 復元] 機能を使用します。
14. オプションのインストール手順には、次のものがあります。
    - 通知メッセージのカスタマイズ
    - IWSVA の Trend Micro Control Manager または Trend Micro Apex Central 集中管理システムへの登録

環境の適切なサイジング

IWSVA をネットワークにインストールする前に、最初に、会社のユーザ総数とインターネットアクティビティをサポートするために必要な IWSVA サーバの数を決定する必要があります。

環境を適切にサイジングする際の考慮事項 :

- 会社内でインターネットにアクセスする総ユーザ数
- インターネットに同時にアクセスするユーザ数
- 各アクティブユーザが使用する同時セッションの平均数
- ユーザ総数とインターネット使用の成長
- 使用されているサーバハードウェアのタイプ
- IWSVA が検索する必要がある帯域幅量
- 冗長性とフェイルオーバー

ベストプラクティスの提案

- 常に成長を見越して環境のサイズを決定します。インターネットの使用は常に増大しているため、現在の最大ピーク負荷に基づいて展開のサイズを決定することはお勧めしません。
- IWSVA アーキテクチャには冗長性を組み込み、障害の単一点の発生を阻止し、デバイスで障害が生じた際のロールオーバーを可能にします。
- バックアップユニットやセカンダリへのフェイルオーバー時に最大ユーザ数をサポートできるように、冗長なアーキテクチャを設計する必要があります。そうでないと、ユニットで障害が発生したとき、パフォーマンスと応答時間が期待値を下回ることになります。

配置方法と冗長性の選択

IWSVA は、配置オプションに関して最も柔軟な Web ゲートウェイセキュリティ製品です。IWSVA は次のトポロジで配置できます。

- プロキシ転送モード
- 透過ブリッジモード
- 高可用性向け透過ブリッジ
- WCCP モード
- ICAP モード
- リバースプロキシモード

- 通常の透過モード

配信モードはそれぞれ利点があり、特定のニーズを満たします。IWSVA 製品をネットワークにインストールする方法を決定する前に、各配信モードの利点と欠点を把握する必要があります。各配置方法と、それぞれが備える主な利点の詳細については、21 ページの「配置について」を参照してください。

冗長アーキテクチャを検討している場合は、以下の点を確認し検討する必要があります。

WCCP - Cisco WCCP プロトコルをサポートし、IWSVA アーキテクチャに負荷分散、冗長性、および拡張性をもたらします。ルータまたはスイッチもしくは両方が Cisco WCCP をサポートしている場合、これは、高可用性機能を追加するための最も経済的な方法の 1 つです。WCCP の欠点の 1 つは、一般的なインターネットプロトコルしか検索デバイスに効率的にリダイレクトできないことです。サポートされる WCCP のバージョンについては、IWSVA ReadMe ドキュメントを参照してください。

ICAP - ICAP v1.0 デバイスをサポートし、一般的なキャッシュサーバからコンテンツを検索できます。また、ICAP を使用すると、単一のキャッシュサーバに接続された複数の IWSVA サーバから成る 1 対多構成でスケーラブルなアーキテクチャを作成できます。これは、Web コンテンツをキャッシュして、帯域幅消費量を削減するとともにインターネットの遅延を低減する必要のあるお客さまに適したオプションです。

Apache Traffic Server (ATS) - Apache Traffic Server（ATS) と呼ばれる人気のあるオープンソースキャッシュプログラムをバンドルし、追加のライセンス料を支払うことなく Web コンテンツをキャッシュする経済的な方法をお客さまに提供します。IWSVA 6.5 SP2 以降では、基本的な ATS の設定および有効化機能が IWSVA 6.5 SP2 Web 管理コンソールに統合されています。ATS は IWSVA 6.5 SP2 以降で上位プロキシモードでサポートされます。ATS のサポートはオープンソースコミュニティを通じて提供されます。トレンドマイクロでは、便宜上、Web ゲートウェイ製品に関するサポートを提供します。

プロキシ Pac ファイル - プロキシ転送モードで配置している場合は、プロキシ pac ファイルを通じて簡易な負荷分散を実現できます。送信元 IP アドレスまたは送信元ネットワークに基づいてトラフィックを特定の IWSVA デバイスにルーティングするプロキシ pac ファイルを作成することで、多くのお客さまが優れた結果を得ています。これによって、手動でネットワークを拡張でき、コストやネットワークの複雑さを増やすことなく、多数の IWSVA サーバ間でユーザを負荷分散できます。

また、複数のプロキシサーバに返るようにプロキシ pac ファイルを設定することで、簡易な冗長性ソリューションを確立できます。すべてのブラウザが複数のプロキシサーバの応答を解釈できるわけではない点に注意してください。ブラウザが複数のプロキシサーバの応答を解釈できない場合は、冗長性は確立できません。

レイヤ 4 負荷分散スイッチ - IWSVA は、「通常の透過」機能を使用して、プロキシ転送モードで外部負荷分散スイッチをサポートできます。外部負荷分散スイッチを配置するとコストと設定の複雑さが高まりますが、冗長性と負荷分散に関して最高のパフォーマンスと柔軟性が実現されます。トレンドマイクロのお客さまが採用し成功した商用のロードバランサには、Foundry Networks/Brocade、F5、Citrix NetScaler などがあります。コストが懸案事項となる場合は、Red Hat Enterprise などの代替のオープンソースソフトウェアベースのロードバランサも、優れた拡張性および冗長性オプションを提供できます。

- VMware 上にインストールする場合は、VMware の冗長性および耐障害性機能を使用して強固でスケーラブルなソリューションを作成することを検討してください。このような機能には次のものが含まれます。
  - VMotion
  - vSphere 耐障害性サービス

本書の執筆時点では、vSphere の耐障害性サービスは 1 つの仮想 CPU にしか対応していません。これにより完全な冗長性ソリューションを開発できますが、単一の CPU に制限されるためパフォーマンスは低くなります。vSphere FT の設定の詳細については、VMware Web サイトの「Best Practices Guide for Utilizing VMware Fault Tolerance for High Availability」を参照してください。

ベストプラクティスの提案

- IWSVA では、クラウドベースの検索とオンボックス検索エンジンから成るハイブリッド不正プログラム検索アーキテクチャを採用しています。このソリューションは、業界最高の検出率と防御率を実現します。クラウドベースの検索エンジンは、レピュテーションサービスに基づきプロアクティブな検出およびブロックサービスを提供します。低遅延の高速パフォーマンスを確保するには、IWSVA が高速で強固な DNS アーキテクチャにアクセスする必要があります。ISP が提供する DNS サーバは使用しないでください。IWSVA デバイスが頻繁に作成する DNS 要求を十分にサポートできず、ISP の DNS サーバが圧倒される可能性があるからです。
- IWSVA の内部クロック設定をセキュリティアーキテクチャ内の他のサーバやデバイスと同期する必要があります。これには、LDAP サーバ、syslog サーバ、および上位 SIEM デバイスが含まれます。日時が一致しないと、重要なイベントが不適切に記録されたりレポートされたりすることがあります。最適な結果を得るには、同一の NTP サーバのセットを使用し、すべてのデバイスの日時を同期します。
- 冗長性と拡張性を実現するには、IWSVA の複数のインスタンスをインストールし、このセクションで述べた拡張オプションのいずれかを使用して障害の単一点をなくし、システムのアップタイムを改善することを検討してください。代替として、2 つの IWSVA デバイスを高可用性配信モードでクラスタペアとしてインストールすることもできます。

- 上位プロキシとともにインストールする場合は、IWSVA の上位プロキシのプロキシ転送設定と [アップデート] → [接続設定] を適切に設定し、適切なインターネットアクセスを確保する必要があります。
- IWSVA を使用して、お客さまがアクセス可能な外部に公開された Web サーバを保護する予定の場合は、IWSVA の個別のインスタンスをリバースプロキシモードでインストールし、これらの Web サーバを保護することを検討してください。外部に公開された Web サーバを通常のユーザが使用する企業 IWSVA サーバの内側に配置しないでください。そのように配置すると、お客さま向けのポリシーと通常の企業ユーザ向けポリシーの両方を適用する能力に影響することがあります。
- VMWare ESX または Hyper-V 上で透過ブリッジモードでインストールする場合は、IWSVA の外部インタフェースが物理ネットワークアダプタにバインドされた仮想スイッチに接続されます。他の仮想マシンはこの仮想スイッチに接続せず、仮想マシンを IWSVA の使用専用にしておくことをお勧めします。
- IWSVA のインストール後は、追加のクリティカルパッチやサービスパックがないかどうか常にトレンドマイクロのダウンロードサイトを確認し、最新のパッチがインストールされている状態を保持してください。IWSVA ダウンロードサイトのパッチのリストは発生順です。常に、最新のアプリケーションと OS パッチを特定のバージョンに適用してください。IWSVA サービスパックは、下位互換性を備えています。つまり、最新のサービスパックには常に、そのサービスパックのリリース日以前に発行された HotFix とパッチがすべて含まれています。製品の最新の適用可能なサービスパックの前に、以前のパッチをインストールする必要はありません。

付録 D

テクニカルサポート

この付録では、次の項目について説明します。

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。

製品 Q&A のご案内

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

製品 Q&A

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

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

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

セキュリティニュース

トレンドマイクロ「セキュリティニュース」

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

`https://www.trendmicro.com/ja_jp/security-intelligence/breaking-news.html`

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

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

トレンドマイクロへのウイルス解析依頼

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

ファイルを送信いただく前に、トレンドマイクロの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専門のスタッフが解析し、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。

脅威解析・サポートセンター TrendLabs (トレンドラボ)

TrendLabs （トレンドラボ) は、フィリピン・米国に本部を置き、日本・台湾・ドイツ・アイルランド・中国・フランス・イギリス・ブラジルの 10 カ国 12 か所の各国拠点と連携してソリューションを提供しています。

世界中から選び抜かれた 1,000 名以上のスタッフで 24 時間 365 日体制でインターネットの脅威動向を常時監視・分析しています。

付録 E

VMware ESX 下での IWSVA 用の新しい仮想マシンの作成

この付録では、InterScan Web Security Virtual Appliance 6.5（以下、IWSVA) 用の新しい仮想マシンの作成方法について説明します。

概要

本書では、ESX のインストール方法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 の製品マニュアルを参照してください。

以下のセクションの手順では、VMware ESX 下で新しい仮想マシンを作成して IWSVA をインストールするプロセスについて詳しく説明します。

新しい仮想マシンを作成する

以下の手順は、ご使用の環境に適した仮想マシンを作成するためのガイドラインとしてご利用ください。選択した CPU の数、NIC カードの枚数、メモリ容量、およびハードディスク容量は、配置要件を反映したものにする必要があります。ここで入力する値はあくまでも参考用です。

新しい仮想マシンを作成するには

1. VMware Virtual Infrastructure クライアントを開いて、[Configuration] タブをクリックします。
2. [Hardware] 領域で [Storage] をクリックします。

3. [Storage] 領域で、IWSVA ISO のアップロードに十分な容量のストレージ領域をダブルクリックします。

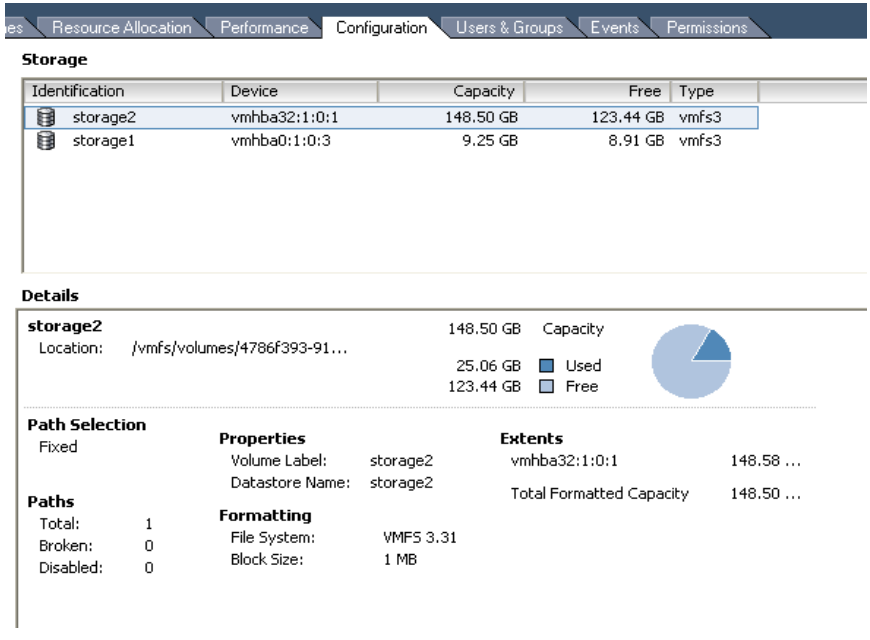


図 E-1. [Configuration] **タブ**

[Datastore Browser] 画面が開きます。

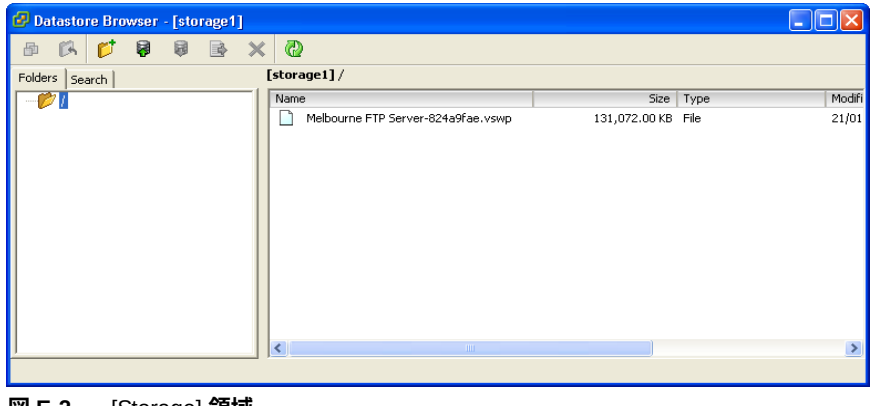
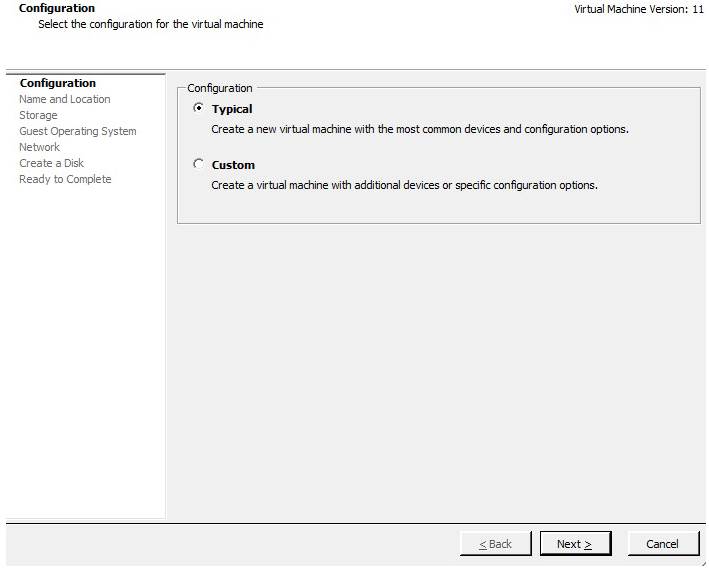


図 E-2. [Storage] **領域**

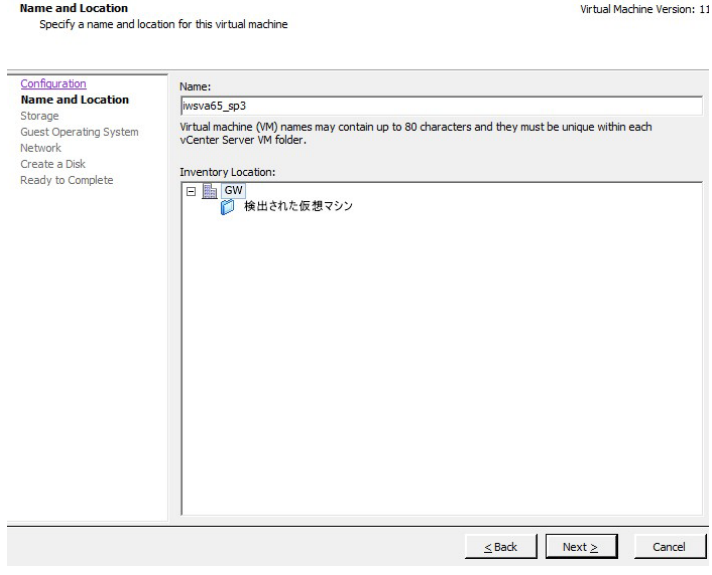
4. ボタンバーで、アップロードボタン (上矢印付きのデータベースアイコン) をクリックして、IWSVA ISO をこのデータストアにアップロードします。
5. アップロードが完了したらデータストアを閉じます。

仮想マシンを作成するには

6. メニューバーで、[File] → [New] → [Virtual Machine] の順に選択します。
   [Create New Virtual Machine] ウィザードが表示されます。
7. [Configuration] で [Typical] を選択し、[Next] をクリックします。

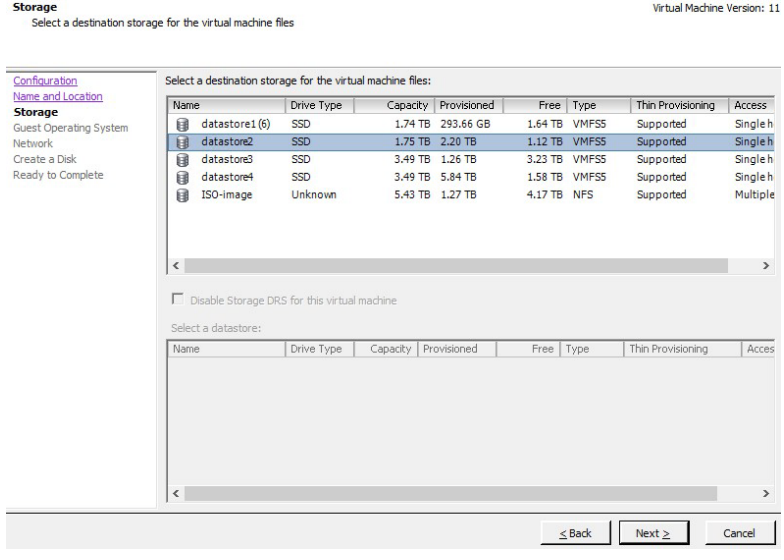


8. [Name and Location] に移動します。[Name] に適切な仮想マシン名を入力して、[Next] をクリックします。

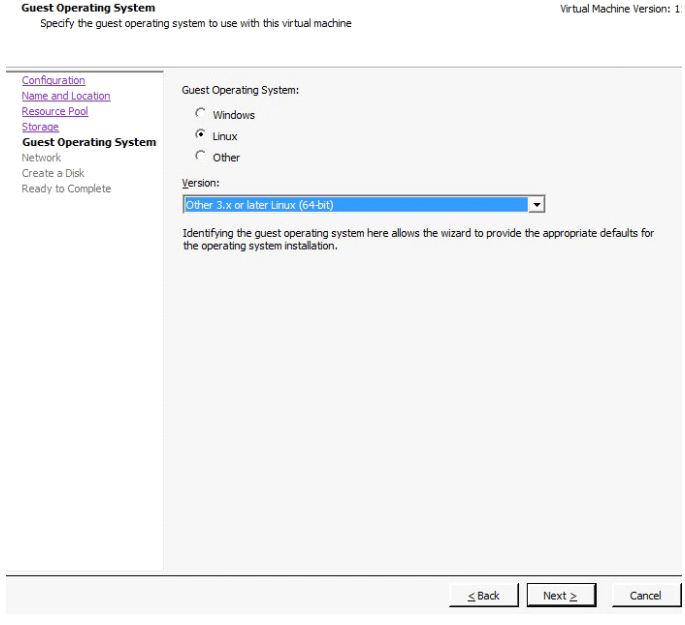


9. [Storage] に移動します。仮想マシンを配置するデータストアを選択し、[Next] をクリックします。

   なお、IWSVA ISO のアップロードに使用したデータストアと同じにする必要はありません。

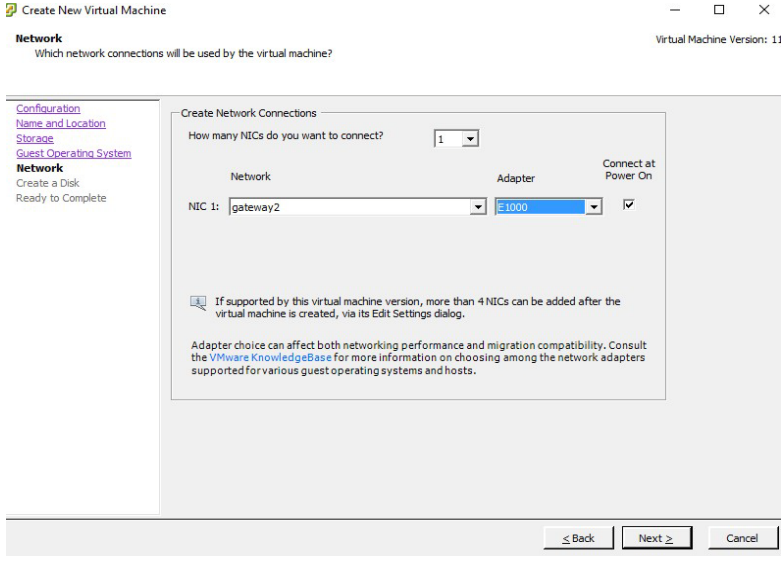


10. [Guest Operating System] に移動します。[Guest Operating System] として [Linux] を、[Version] として [Other 3.x or later Linux (64-bit)] ([その他の Linux 3.x 以降 (64 ビット)]) をそれぞれ選択し、[Next] をクリックします。

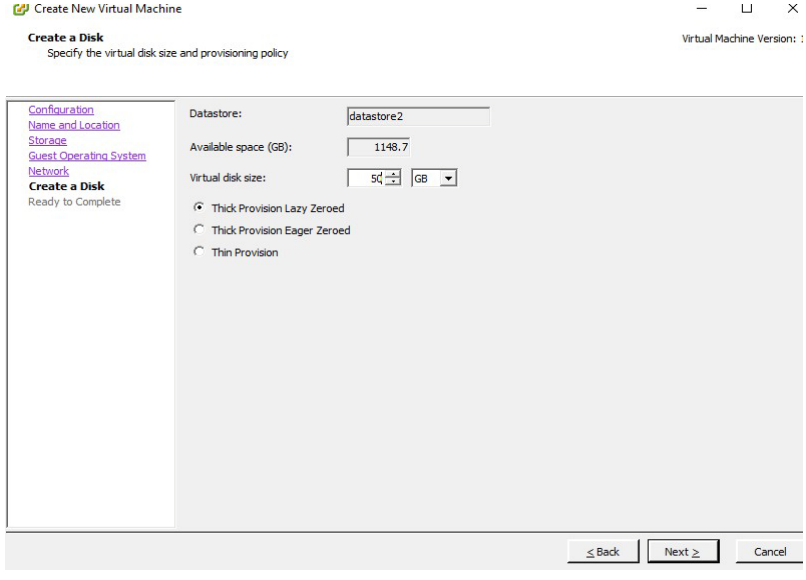


注意： [Guest Operating System] として [Linux] を、[Version] として [Other 3.x or later Linux (64-bit)] ([その他の Linux 3.x 以降 (64 ビット)]) をそれぞれ選択する必要があります。

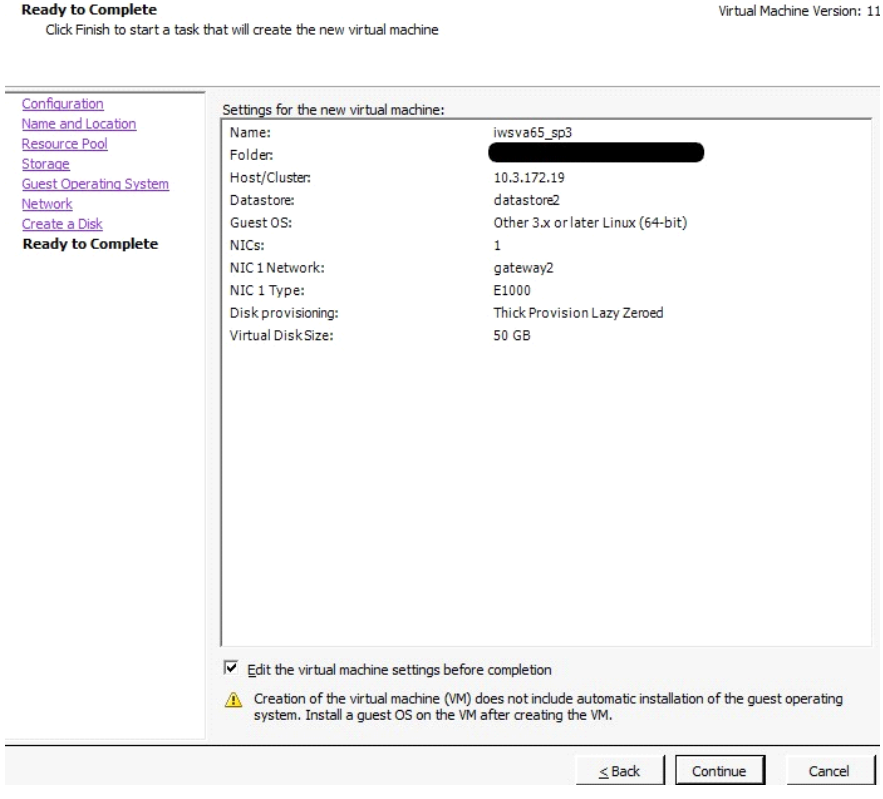
11. [Network] に移動します。仮想マシンで使用する NIC の数と、使用する NIC に対するネットワークとアダプタのタイプを設定し、[Next] をクリックします。



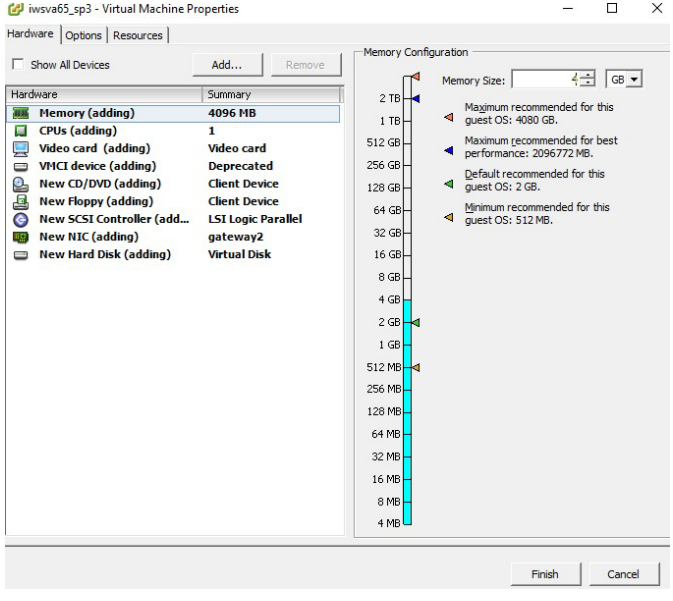
12. [Create a Disk] に移動します。仮想マシンのディスク容量を設定し、[Next] をクリックします。ディスク容量の要件については、14 ページの「システム要件」を参照してください。



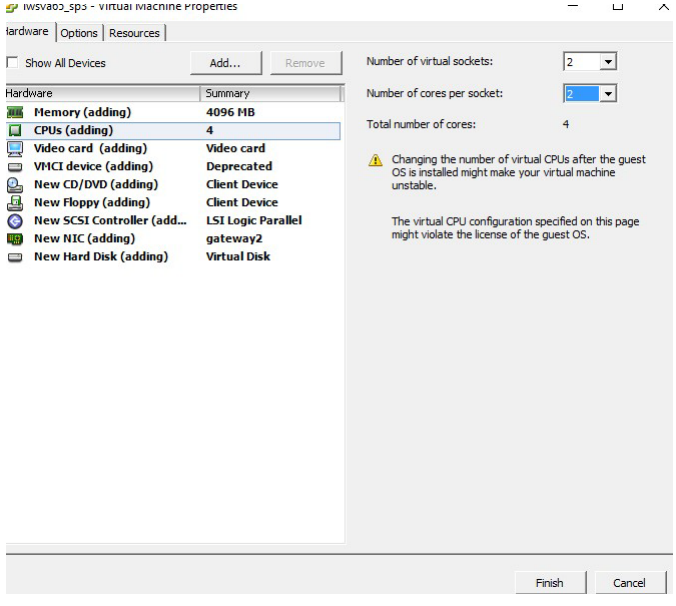
13. [Ready to Complete] に移動します。設定内容を確認し、問題なければ [Edit the virtual machine settings before completion] チェックボックスをオンにして [Continue] をクリックします。



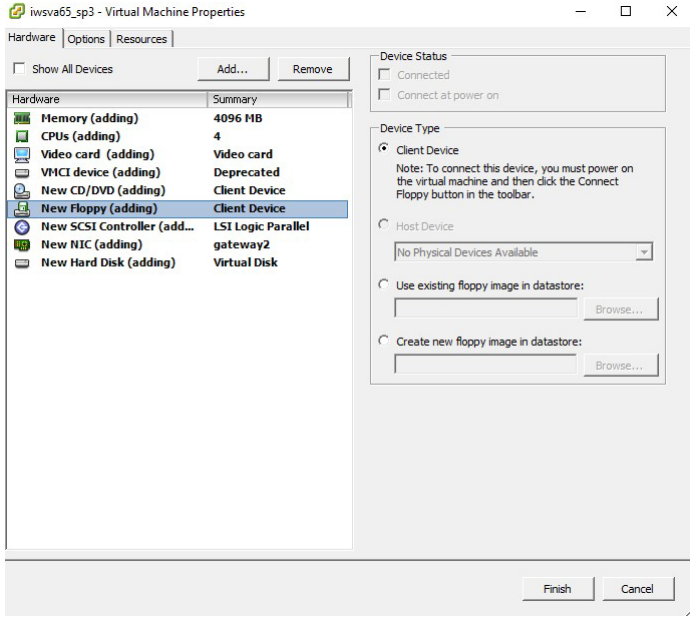
14. [Virtual Machine Properties] に移動します。[Memory (adding)] をクリックし、使用するメモリ容量を設定します。メモリ容量の要件については、14 ページの「システム要件」を参照してください。



15. [CPUs (adding)] をクリックし、使用する仮想 CPU のソケット数とソケット毎のコア数を設定します。CPU の要件については、14 ページの「システム要件」を参照してください。

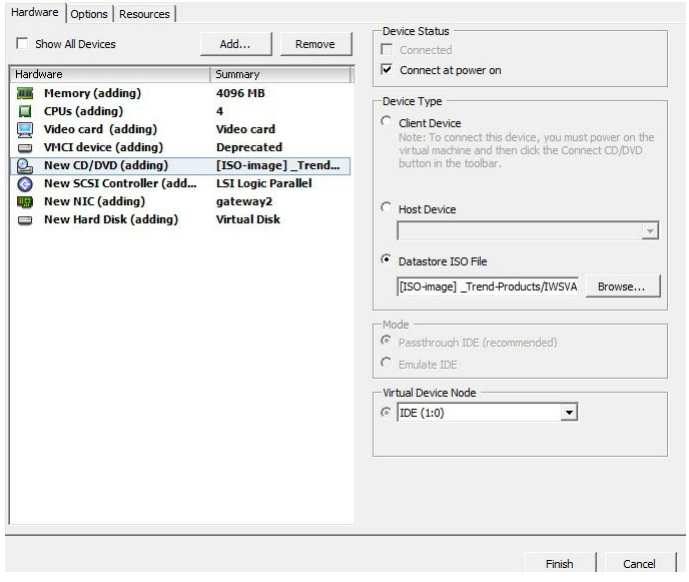


16. [New Floppy (adding)] をクリックし、[Remove] をクリックしてフロッピードライブを削除します。



17. [New CD/DVD (adding)] をクリックし、[Connect at power on] チェックボックスをオンにします。次に、右側の [Datastore ISO file] ラジオボタンを選択し、[Browse...] をクリックして、手順 4 でアップロードした IWSVA インストール ISO を選択します。

    インストール ISO を VMware サーバのハードディスクにコピーしなかった場合は、インストーラのロード先となる [Host Device] または [Client Device] を選択できます。[Client Device] では、リモートワークステーションの CD/DVD ROM ドライブを使用してインストールが実行されます。また、[Host Device] では、VMware サーバの CD/DVD ROM ドライブを使用してインストールが実行されます。

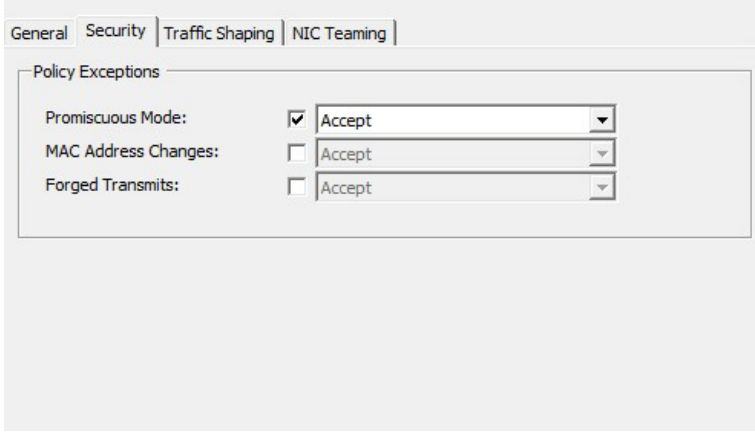


18. [Resources] タブをクリックして、IWSVA 仮想マシンの CPU とメモリのリソースの予約を行います。

警告： **この手順を省略した場合、他の仮想マシンによって IWSVA に割り当てられるリソースが不足し、パフォーマンスの低下を招く恐れがあります。パフォーマンスの低下が発生した場合は、リソースの予約状況を見直してください。**

19. [Finish] をクリックします。これで、新しい IWSVA 6.5 SP3 仮想マシンの準備が完了し、電源をオンにすればインストールプロセスが開始されるように設定されました。

注意： IWSVA を VMware ESX サーバにインストールして透過ブリッジモードに設定した場合は、データインタフェースとして使用する 2 つのネットワークインタフェースの仮想スイッチに対し、設定 [Promiscuous Mode] を [Accept] とする必要があります。
また、IWSVA を透過ブリッジモードで配置する場合は、同じスイッチに 2 つのデータインタフェースを接続しないでください。同じスイッチに 2 つのデータインタフェースを接続すると、ネットワーク内にループが発生します。



IWSVA 仮想マシンの電源投入とインストールの完了

以下の手順は、インストールを完了して仮想マシンに電源を投入するためのガイドラインとしてご利用ください。

新しい仮想マシンに電源を投入するには

1. VMware Virtual Infrastructure クライアントコンソールから、作成した仮想マシンの名前を選択します。
2. 名前を右クリックして [Power] を選択し、[Power On] を選択します。仮想マシンに電源が投入されます。
3. IWSVA 仮想マシンのコンソールに接続します。

IWSVA 仮想マシンのコンソールに接続するには

1. VMware Virtual Infrastructure クライアントコンソールで、作成した仮想マシンの名前をクリックします。
2. 右側のフレームから、[Console] タブを選択します。

   IWSVA 仮想マシンログオンプロンプトが表示されます。
3. ユーザ名として「enable」と入力します。
4. パスワードを入力します。初期パスワードは「adminIWSS85」です。

付録 F

Microsoft Hyper-V 下での IWSVA 用の新しい仮想マシンの作成

この付録では、Microsoft Hyper-V 下での InterScan Web Security Virtual Appliance 6.5 (以下、IWSVA) 用の新しい仮想マシンの作成方法について説明します。

概要

IWSVA では、Microsoft Hyper-V ベースの仮想プラットフォームがサポートされています。本書では、Hyper-V ベースの仮想マシンに IWSVA 6.5 SP3 をインストールするための手順を、順を追って説明します。

本書では、Hyper-V のインストール方法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、Microsoft の製品マニュアルを参照してください。

ここで取り上げる手順では、Windows 2016 Server Hyper-V サーバに IWSVA 6.5 SP3 をインストールする方法を説明しています。事前に、Hyper-V をサポートする適切な Microsoft Windows 2012 Server R2 がインストールされている必要があります。

IWSVA における Hyper-V のサポート

IWSVA 6.5 SP3 は、Windows Server 2008 R2 SP1 Hyper-V、Windows Server 2012 Hyper-V、Windows Server 2012 R2 Hyper-V、Windows Server 2016 Hyper-V、Windows Server 2019 Hyper-V をサポートしています。Hyper-V プラットフォームへの IWSVA のインストールでは、プロキシ転送モード、WCCP モード、ICAP モード、リバースプロキシモード、および透過ブリッジモードがサポートされます。

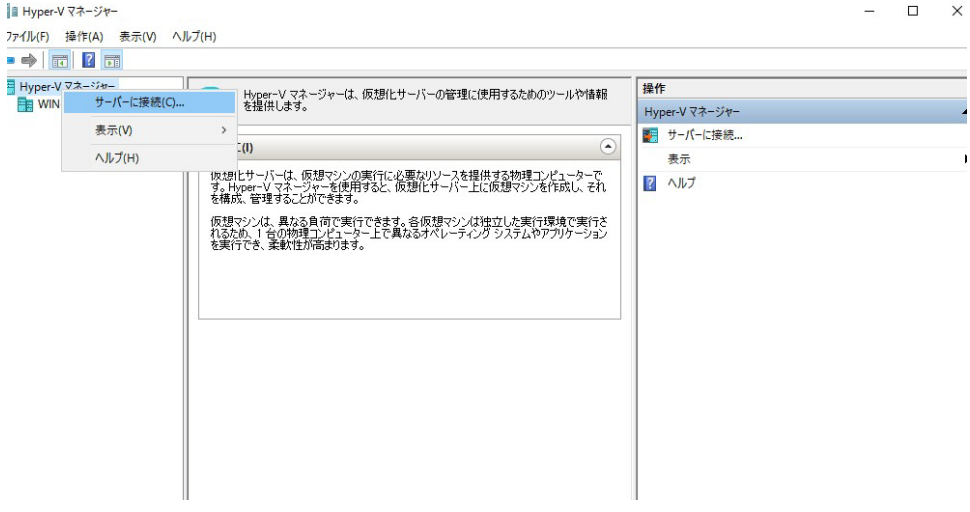
Microsoft Hyper-V 上での IWSVA 6.5 SP3 のインストール

以下の手順は、ご使用の環境に適した仮想マシンを作成するためのガイドラインとしてご利用ください。選択した CPU の数、NIC カードの枚数、メモリ容量、およびハードディスク容量は、配置要件を反映したものにする必要があります。ここで入力する値はあくまでも参考用です。

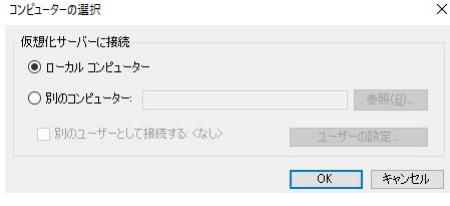
仮想スイッチを作成するには

1. Hyper-V の [サーバー マネージャー] メニューで [ツール] → [Hyper-V マネージャー] を選択し、Hyper-V マネージャーを開きます。

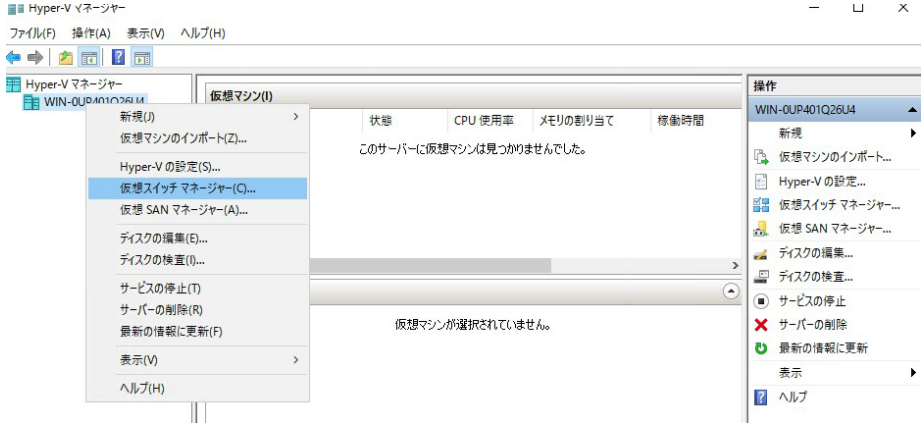
2. Hyper-V マネージャーを右クリックし、[サーバーに接続] を選択します。



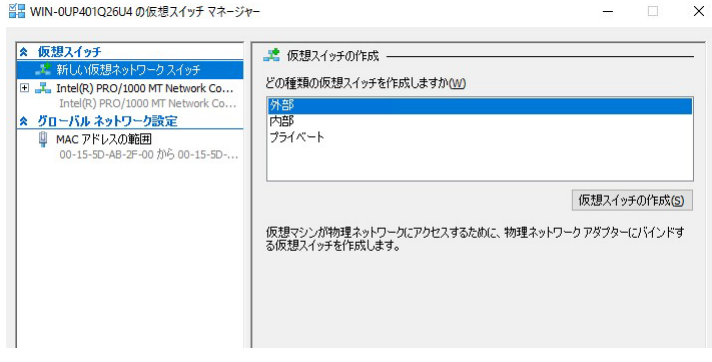
3. 接続先の仮想化サーバの場所を選択するように求めるダイアログボックスが表示されます。仮想化サーバの場所を選択し、[OK] をクリックします。



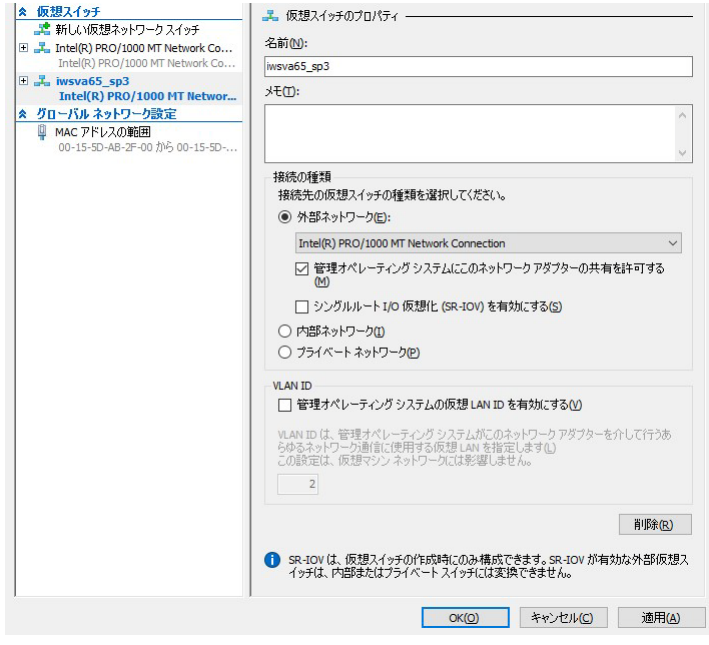
4. 接続した Hyper-V サーバを右クリックし、[仮想スイッチ マネージャー] を選択します。



5. オプションリストから [外部] を選択し [仮想スイッチの作成] をクリックすることで、新しい仮想スイッチを作成します。



6. [名前] に適切な仮想スイッチ名を設定します。[接続の種類] で [外部ネットワーク] を選択し、仮想スイッチに接続する物理ネットワークアダプタを選択します。その後、[OK] をクリックすると仮想スイッチが作成されます。

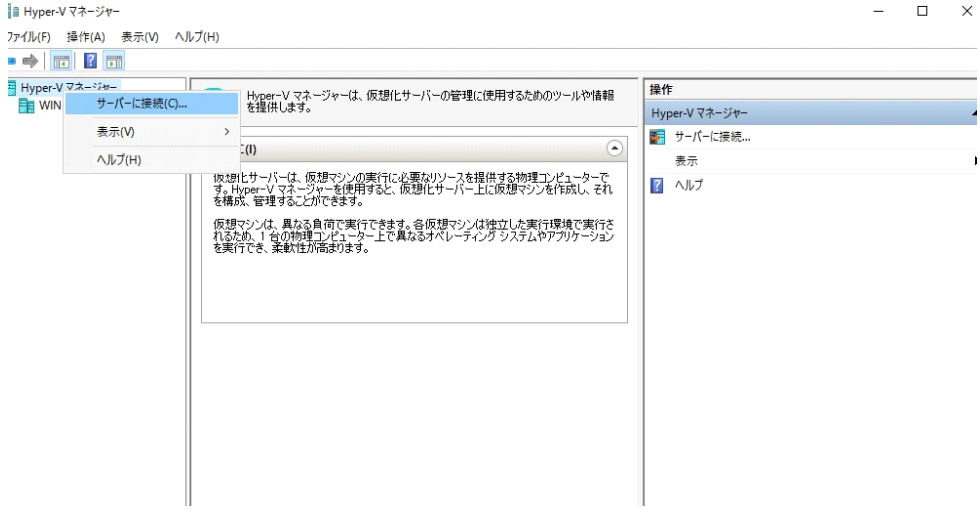


注意： 物理アダプタは、ネットワークに接続され、企業ネットワークとパブリックインターネットへのアクセス権を保持している必要があります。

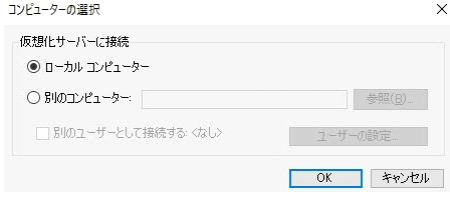
新しい仮想マシンを作成する

新しい仮想マシンを作成するには

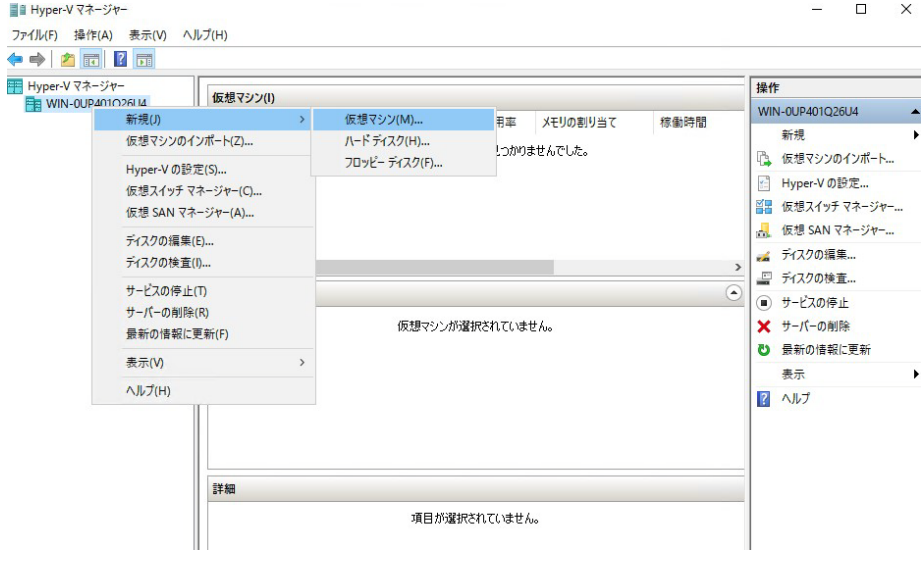
1. Hyper-V の [サーバー マネージャー] メニューで [ツール] -> [Hyper-V マネージャー] を選択し、Hyper-V マネージャーを開きます。
2. Hyper-V マネージャーを右クリックし、[サーバーに接続] を選択します。



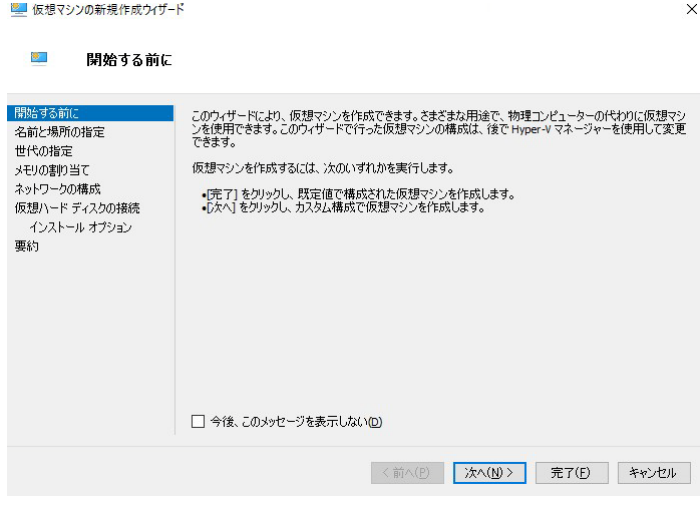
3. 接続先の仮想化サーバの場所を選択するように求めるダイアログボックスが表示されます。仮想化サーバの場所を選択し、[OK] をクリックします。



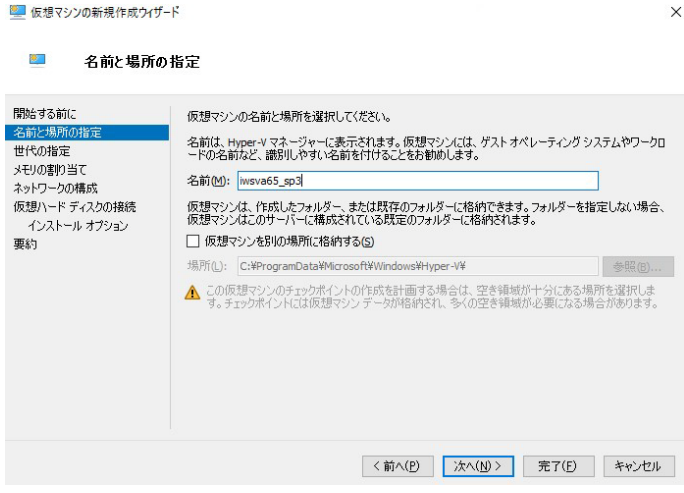
4. 接続した Hyper-V サーバを右クリックし、[新規] → [仮想マシン] を選択します。



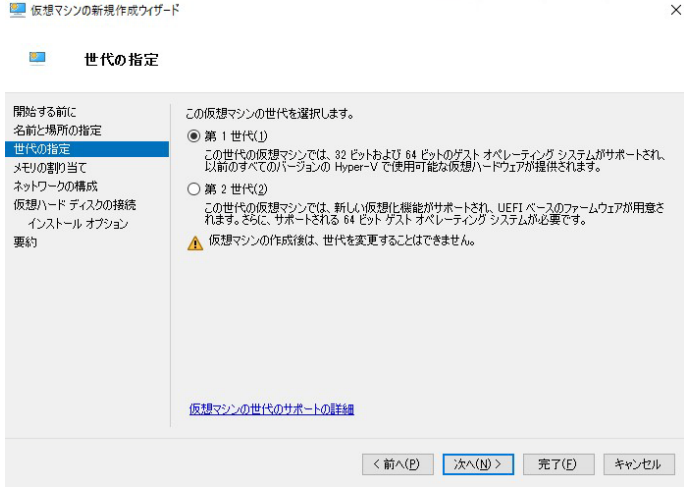
5. [仮想マシンの新規作成ウィザード] が表示されます。[開始する前に] で [次へ] をクリックします。



6. [名前と場所の指定] へ移動します。適切な仮想マシン名と仮想マシンの格納場所を設定し、[次へ] をクリックします。

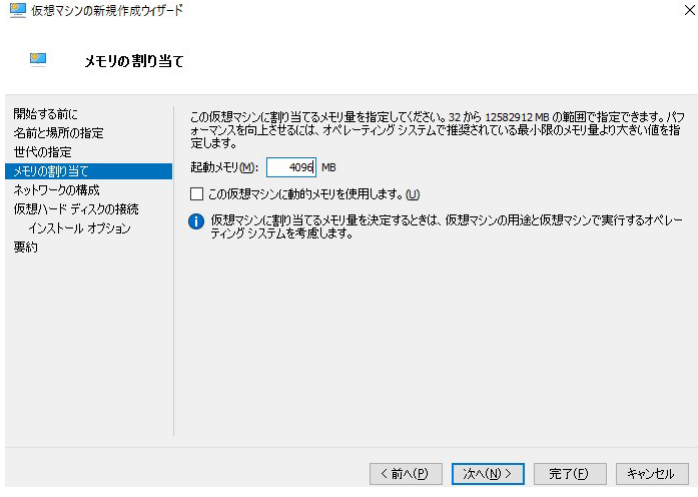


7. [世代の指定] に移動します。[第 1 世代] を選択し、[次へ] をクリックします。

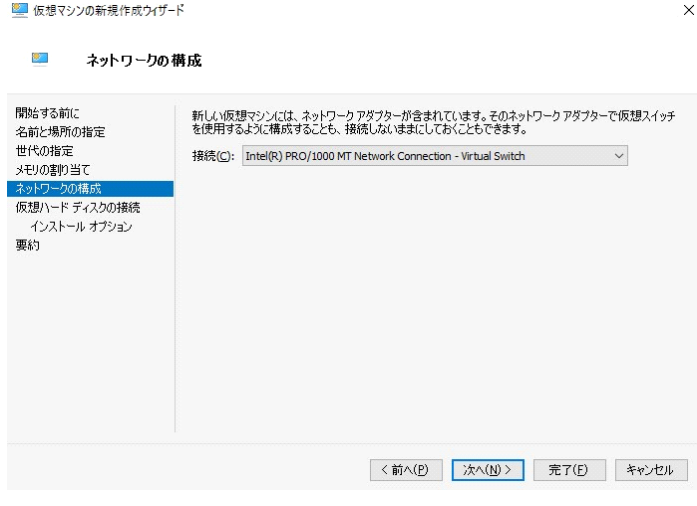


注意： IWSVA 6.5 SP3 は第 2 世代の仮想マシンをサポートしておりません。

8. [メモリの割り当て] に移動します。[起動メモリ] で使用するメモリ容量を設定し、[次へ] をクリックします。メモリ容量の要件については、14 ページの「システム要件」を参照してください。

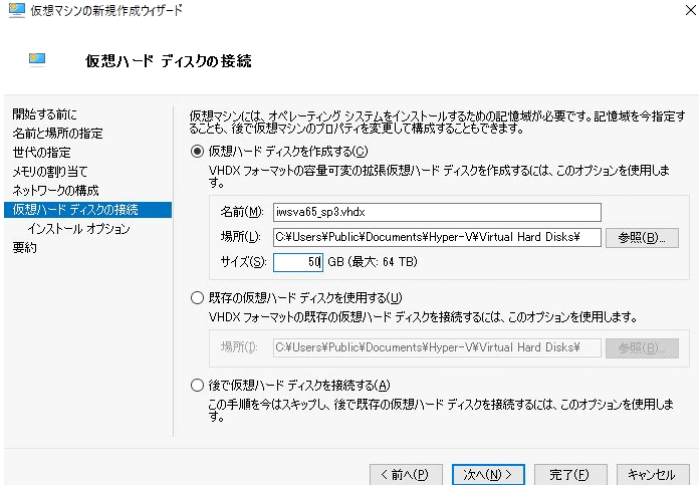


9. [ネットワークの構成] に移動します。IWSVA 用の仮想スイッチを選択し、[次へ] をクリックします。仮想スイッチの作成方法については、122 ページの「仮想スイッチを作成するには」を参照してください。

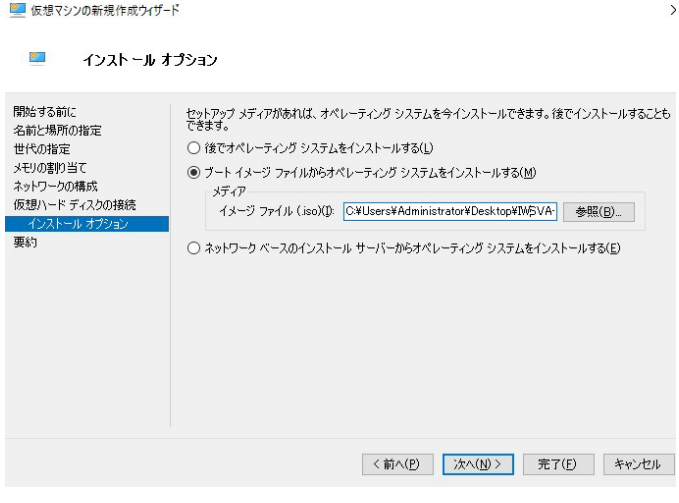


10. [仮想ハード ディスクの接続] に移動します。[仮想ハード ディスクを作成する] を選択し、[サイズ] に仮想マシンのディスク容量を設定して、[次へ] をクリックします。

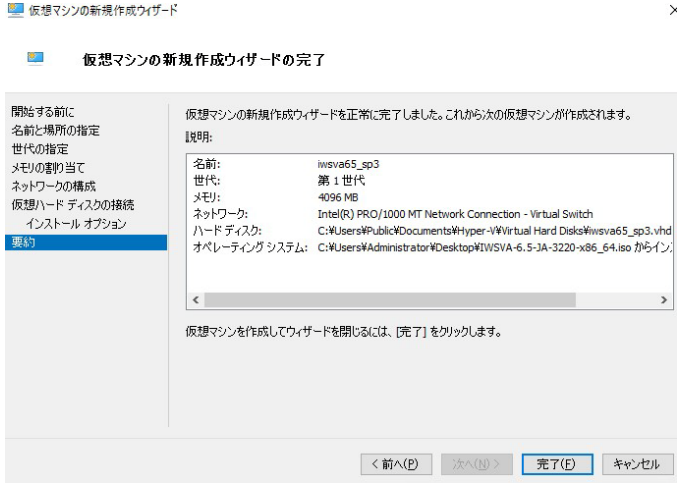
    ディスク容量の要件については、14 ページの「システム要件」を参照してください。



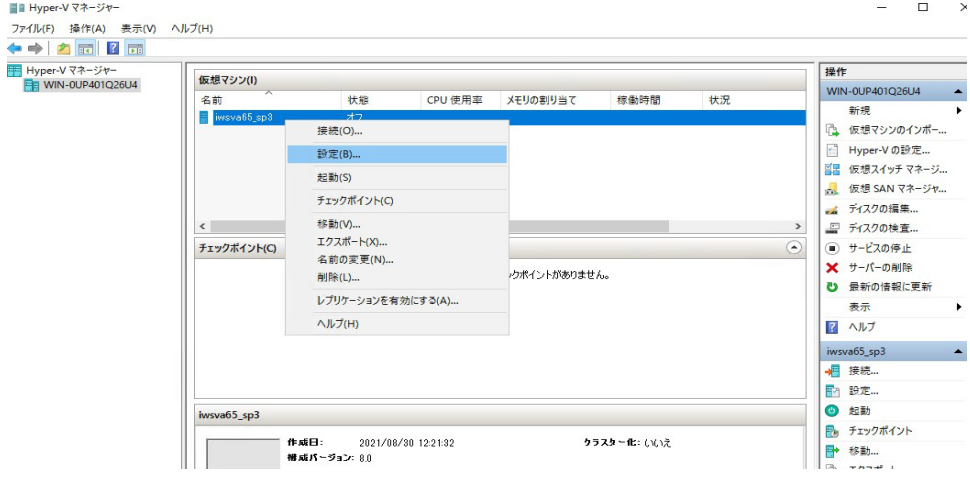
11. [インストール オプション] に移動します。[ブート イメージ ファイルからオペレーティング システムをインストールする] を選択し、[イメージ ファイル] で IWSVA インストール ISO を設定して、[次へ] をクリックします。



12. [仮想マシンの新規作成ウィザードの完了] に移動します。表示の内容に問題がなければ、[完了] をクリックします。

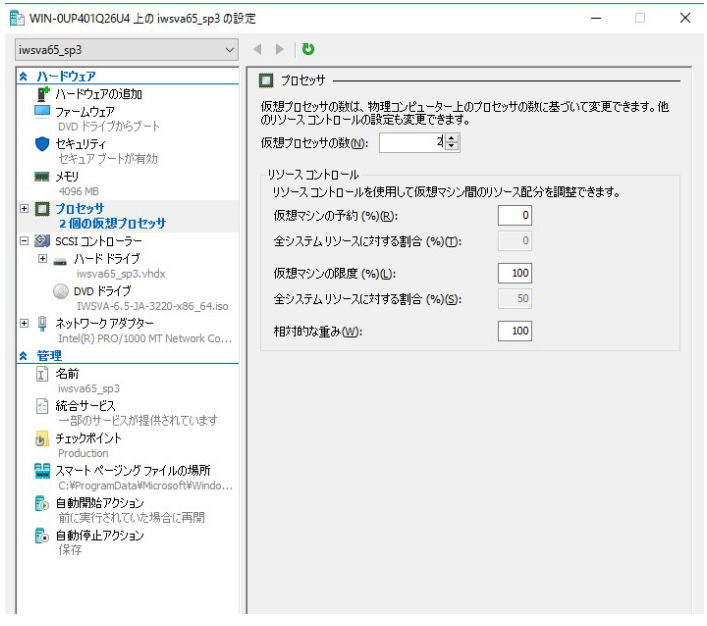


13. 新規作成された仮想マシンを右クリックし、[設定] を選択します。



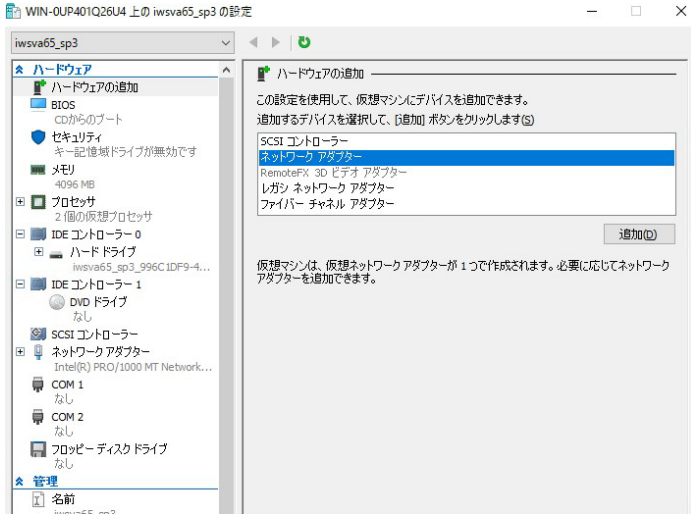
14. [プロセッサ] を選択し、[仮想プロセッサの数] で使用する CPU 数を設定します。CPU の要件については、14 ページの「システム要件」を参照してください。

    次に、[リソースコントロール] の [仮想マシンの予約] でリソースの予約を行います。

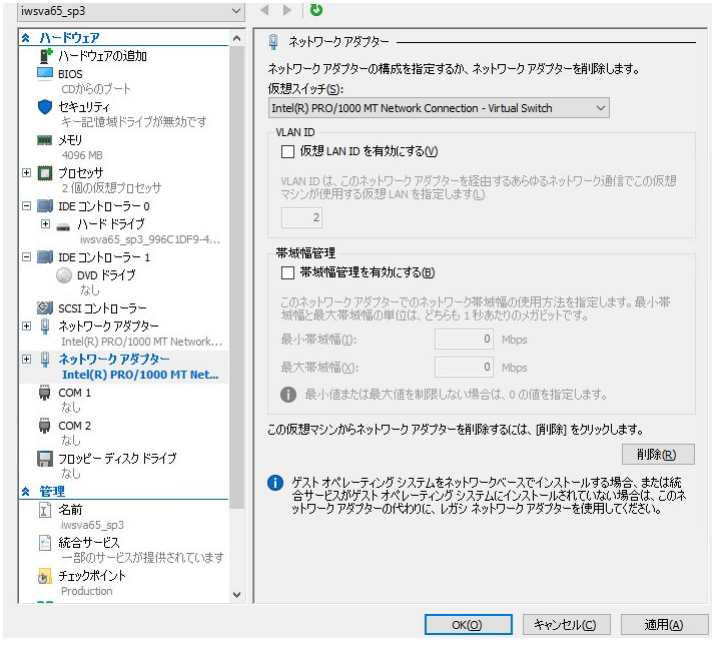


警告： **リソースの予約を省略した場合、他の仮想マシンによって IWSVA に割り当てられるリソースが不足し、パフォーマンスの低下を招く恐れがあります。パフォーマンスの低下が発生した場合は、リソースの予約状況を見直してください。**

15. 追加でネットワークインタフェースが必要な場合は、[ハードウェアの追加] を選択し、[ネットワーク アダプター] を選択して、[追加] をクリックします。



そして、追加されたネットワークアダプタの [仮想スイッチ] で、IWSVA 用の仮想スイッチを選択し、[OK] をクリックします。仮想スイッチの作成方法については、122 ページの「仮想スイッチを作成するには」を参照してください。



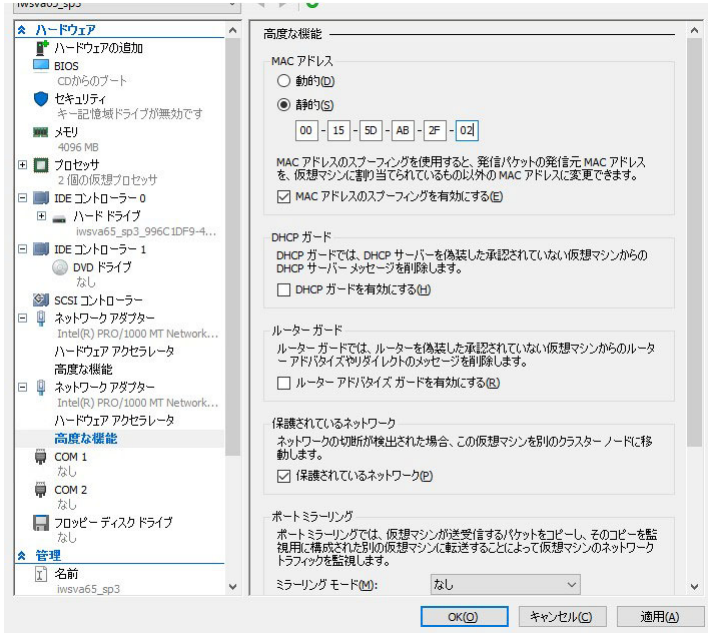
16. これで、新しい IWSVA 6.5 SP3 仮想マシンの準備が完了し、電源をオンにすればインストールプロセスが開始されるように設定されました。

注意： IWSVA を Hyper-V サーバにインストールして透過ブリッジモードに設定した場合は、データインタフェースとして使用する 2 つのネットワークアダプタに対して、[高度な設定] の [MAC アドレス] で以下を設定する必要があります。

・ [静的] を選択します。

・ [MAC アドレスのスプーフィングを有効にする] をオンにします。

また、IWSVA を透過ブリッジモードで配置する場合は、同じスイッチに 2 つのデータインタフェースを接続しないでください。同じスイッチに 2 つのデータインタフェースを接続すると、ネットワーク内にループが発生します。



IWSVA 仮想マシンの電源投入とインストールの完了

以下の手順は、インストールを完了して仮想マシンに電源を投入するためのガイドラインとしてご利用ください。

新しい仮想マシンに電源を投入するには

1. [Hyper-V マネージャー] で、作成した仮想マシンの名前を右クリックします。
2. メニューから [起動] を選択します。これで仮想マシンに電源が投入されます。

IWSVA 仮想マシンのコンソールに接続するには

1. [Hyper-V マネージャー] で、作成した仮想マシンの名前を右クリックします。
2. メニューから [接続 ...] を選択します。IWSVA 仮想マシンログオンプロンプトが表示されます。
3. ユーザ名として「enable」と入力します。
4. パスワードを入力します。初期パスワードは「adminIWSS85」です。

索引

英数字

あ

か

さ

た

な

は

ま

や

ら