InterScan Web Security Virtual Appliance™ 6.5 Service Pack 3

管理者ガイド

※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/jp/solution/000207383

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: IBEM67229/150925_JP_R5 (2023/02)

目次

はじめに

InterScan Web Security Virtual Appliance 6.5 SP3 (以下、IWSVA) 管理ガイドにようこそ。本書では、IWSVA の設定オプションについて詳しく説明します。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。

本章では、次の項目について説明します。

- IWSVA のドキュメント
- 対象読者
- ドキュメントの表記規則
- トレンドマイクロについて

IWSVA のドキュメント

IWSVA には、本書のほかに次のドキュメントが用意されています。

- **インストールガイド** — このガイドでは、IWSVA を紹介し、設置計画、実装、および設定の各作業を案内し、アップグレード後の主な設定作業について説明することで、IWSVA の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。
- **オンラインヘルプ** — オンラインヘルプの目的は、製品の主なタスクに関する操作手順、使用方法のアドバイス、および有効なパラメータの範囲、最適な値など、実際に使用する場面に固有の情報を提供することです。オンラインヘルプには、IWSVA の Web コンソールからアクセスできます。
- Readme — オンラインヘルプやマニュアルにない最新の製品情報や注意事項が記載されています。新機能、設置のヒント、既知の問題、およびリリース履歴が含まれています。

  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`

対象読者

この IWSVA 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、次のようなネットワークの概要に関する専門的な知識があることを前提としています。

- 企業で使用されている HTTP、HTTPS、FTP およびその他のインターネットプロトコル
- VMware ESX 上でインストールする場合は VMware ESX の管理経験、および Hyper-V 上でインストールする場合は Microsoft Hyper-V の管理経験

ただし、ウイルス対策または Web セキュリティの技術に精通していることを前提としていません。

注意： Silicom 社製バイパスカードは VMware で認識され、通常のネットワークカードとして使用できます。

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

トレンドマイクロについて

トレンドマイクロは、ネットワークウイルス対策およびインターネットコンテンツセキュリティのソフトウェアとサービスにおける世界的なリーダーです。1988 年に設立されたトレンドマイクロは、ウイルス監視機能のデスクトップからネットワークサーバおよびインターネットゲートウェイへの移行を牽引し、これまでにその先見の明と技術的な革新力について高い評価を得ています。

今日、トレンドマイクロは、一元管理されたサーバベースのウイルス監視機能とコンテンツフィルタを備えた製品とサービスを提供することで、情報への脅威の影響を管理できる包括的なセキュリティ戦略をお客さまに提供することに重点的に取り組んでいます。インターネットゲートウェイ、メールサーバ、およびファイルサーバを経由する情報を保護することで、世界中の企業やサービスプロバイダが一元管理している場所から、ウイルスやその他の不正コードがデスクトップに到達する前にそれらを阻止できるようにしてます。

詳細な情報またはトレンドマイクロ製品の評価版のダウンロードをご希望の場合は、当社の定評ある Web サイトをご覧ください。

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

第 1 章

製品の概要

本章では、InterScan Web Security Virtual Appliance（以下、IWSVA）の概要と、IWSVA を使用して企業のゲートウェイの安全性を確保する仕組みについて説明します。

本章で説明する内容には、次の項目が含まれます。

主な機能

インターネットゲートウェイの安全性を守るには、IWSVA の次の機能が役立ちます。

アプリケーション制御

アプリケーション制御機能では、人気の高いインターネットアプリケーションを自動的に検出し、管理者がポリシーを使用してそれらのアプリケーションを制御できるようにするセキュリティテクノロジを提供します。詳細については、130 ページの「アプリケーション制御の概要」を参照してください。

HTTP 検査

HTTP 検査により、管理者は動作を識別して、HTTP メソッド、URL、およびヘッダに基づいて Web トラフィックをフィルタできます。また、フィルタを作成するか、初期設定のフィルタを使用して Web トラフィックを識別したり、フィルタをインポートおよびエクスポートしたりすることもできます。トラフィックが識別されたら、IWSVA は、特定のトラフィックに対する適切な処理を決定するポリシー設定に従ってそのトラフィックを管理できます。たとえば、HTTP 検査ポリシーによって、ユーザにソーシャルネットワークや Web メールサイトのコンテンツの閲覧は許可するが、それらへのコンテンツの投稿は禁止することができます。詳細については、174 ページの「HTTP 検査の概要」を参照してください。

情報漏えい対策

便宜上、IWSVA にはコンテンツフィルタ情報漏えい対策 (DLP) ポリシーが初期設定として組み込まれています。地域ごとに 10 個の情報漏えい対策ポリシーが初期設定で設定されています。標準のコンテンツフィルタポリシーと異なり、情報漏えい対策ポリシーのキーワードは、実際のキーワードではなく正規表現の説明文字列です。

たとえば、IBAN は正規表現の説明では次のようになります。

[^\w] (([A-Z] {2}\d{2}\s?) ([A-Za-z0-9] {11,27}| ([A-Za-z0-9] {4}\s) {3,6} [A-Za-z0-9] {0,3}| ([A-Za-z0-9] {4}\s) {2} [A-Za-z0-9] {3,4})) [^\w]

「IBAN」という文字列を含むメッセージは、このポリシーをトリガしません。「BE68 5390 0754 7034」などの文字列は正規表現と一致し、このポリシーをトリガします。

情報漏えい対策では、カスタマイズ可能なデータ識別子、テンプレート、およびポリシーを使用して、企業固有の機密データを定義および監視し、不注意または意図的な喪失から保護します。

機密データを潜在的な喪失に対して監視する前に、次の質問に答える必要があります。

- どのデータを不正ユーザから保護する必要がありますか。
- 機密情報はどのようにネットワークを介して送信されますか。
- 機密データに対するアクセスまたは送信権限を持っているユーザは誰ですか。
- セキュリティ違反が発生した場合はどのように対処する必要がありますか。

この重要な監査には、通常、組織内の機密情報に通じた複数の部門および社員が関係します。

機密情報とセキュリティポリシーをすでに定義している場合は、情報漏えい対策システムでテンプレートと企業ポリシーの定義を開始できます。

データ識別子の種類

デジタル資産とは、組織が不正な転送から保護する必要のあるファイルとデータを指します。次のデータ識別子を使用して、デジタル資産を定義できます。

- **パターン**: 特定の構造を持つデータ。詳細については、29 ページの「パターン」を参照してください。
- **キーワードリスト**: 特殊な単語や語句のリスト。詳細については、30 ページの「キーワードリスト」を参照してください。

パターン

パターンは特定の構造を持つデータです。たとえば、クレジットカード番号は通常 16 桁の「nnnn-nnnn-nnnn-nnnn」の形式で表現されるため、パターンベースの検出に適しています。

事前定義されたパターン

IWSVA には、一連の事前定義されたパターンが用意されています。これらのパターンは変更または削除できません。

IWSVA は、これらのパターンをパターンマッチングと数学的方程式を使用して検証します。IWSVA で潜在的な機密データとパターンが照合された後、そのデータに対して追加の検証チェックが行われる場合もあります。

キーワードリスト

キーワードは特定の単語または語句です。関連するキーワードをキーワードリストに追加して、特定の種類のデータを識別できます。たとえば、診断書では「予後」、「血液型」、「予防接種」、「医師」などのキーワードが使用されると考えられます。診断書ファイルの転送を防ぎたい場合は、情報漏えい対策ポリシーでこれらのキーワードを指定し、これらのキーワードを含むファイルをブロックするように IWSVA を設定します。

一般に使用されている単語を組み合わせて、意味のあるキーワードを作成できます。たとえば、「end」、「read」、「if」、「at」を組み合わせて、ソースコード内で使用されている「END-IF」、「END-READ」、「AT END」などのキーワードを作成できます。

事前定義されたキーワードリスト

IWSVA には、一連の事前定義されたキーワードリストが用意されています。これらのキーワードリストは変更または削除できません。各リストには、テンプレートがポリシー違反の処理を実行するかどうかを判断する独自の条件が組み込まれています。

情報漏えい対策テンプレート

情報漏えい対策テンプレートを使用して、データ識別子の一連の組み合わせにより機密コンテンツをタグ付けおよび検出します。テンプレートでは、条件文内でデータ識別子と演算子 (And、Or) を組み合わせます。一連のデータが条件に一致したら、情報漏えい対策はポリシー処理をトリガします。たとえば、「すべて : 米国国勢調査局の名前」および「米国 : HICN (健康保険請求番号)」テンプレートに一致するデータを含むファイルには、HIPAA ポリシーをトリガします。

GLBA、PCI-DSS、SB-1386、US PII、および HIPAA などの規制準拠イニシアチブに対応するために、情報漏えい対策に初期設定で用意されたテンプレートを使用できます。企業は、独自のビジネス要件に合わせてカスタムテンプレートを作成することも、既存のテンプレートを変更することもできます。企業に既存のユーザ定義のテンプレートがある場合は、テンプレートをインポートおよびエクスポートして、組織全体でポリシーの一貫性を維持できます。

情報漏えい対策ポリシー

情報漏えい対策ポリシーを使用することで、企業はネットワーク上の機密情報の流れを監視できます。情報漏えい対策テンプレートを使用したポリシールールにより、ネットワーク全体の機密情報の配信を管理できます。管理者は、企業全体、グループ、または特定のエンドポイントに適用されるようにポリシーの適用範囲を変更できます。

ポリシーは、送信および受信メールトラフィックの両方に適用することも、監視する特定のメッセージの一部に適用することもできます。ポリシー設定により、特定のグループまたはユーザを検索から除外したり、特定のインシデントに対する応答処理を定義したりできます。

IWSVA では、情報漏えい対策ポリシーの管理を Trend Micro Control Manager（以下 Control Manager）または Trend Micro Apex Central（以下 Apex Central）と統合します。管理者は、企業の情報漏えい対策ポリシーを Control Manager または Apex Central コンソールから作成および管理し、Control Manager に登録されたすべての IWSVA サーバに設定を配信できます。

高度な脅威保護

APT（標的型サイバー攻撃）はあらかじめ対象が決められた標的型攻撃で、機密データを盗んだり、標的に被害をもたらしたりします。APT は通常単一のインシデントではなく、時間をかけて徐々に標的のネットワークの深くに入り込もうとする、失敗や成功を含む一連の試行で構成されます。

IWSVA は、HTTP トラフィックフローを検索してアップロードとダウンロード中のウイルスおよびその他のセキュリティ上の脅威を検出します。HTTP 検索は詳細に設定できます。たとえば HTTP ゲートウェイでブロック対象とするファイルの種類を設定できるほか、パフォーマンスに支障が生じたりブラウザがタイムアウトしないよう、IWSVA による圧縮ファイルと大容量ファイルの検索方法を設定できます。また、IWSVA では各種スパイウェアやその他の脅威も検索できます。

IWAVA は、ファイルおよび URL に不正なスクリプト、およびユーザのコンピュータ上で連続的なハッキング処理を引き起こす APT が含まれないかどうかもチェックします。

HTTPS 復号化

IWSVA は、暗号化されたコンテンツを復号化して検査することで HTTPS のセキュリティホールをふさぎます。ユーザは、選択した Web カテゴリの HTTPS トラフィックを復号化するためのポリシーを定義できます。復号化の際、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。

Web レピュテーション

Web レピュテーションは、新たに出現する Web の脅威からエンドユーザを保護します。Web レピュテーションにより、Web フィルタ機能が強化され、ネットサーフィンがさらに快適になります。Web レピュテーション検索は、URL フィルタモジュールを用いて URL カテゴリ情報を返すため、ローカル上に URL データベースを保持しません。

また、Web レピュテーションでは、レピュテーションスコアを URL に割り当てます。IWSVA は、URL にアクセスするたびに Web レピュテーションにレピュテーションスコアを問い合わせ、ユーザ定義のセキュリティレベルとスコアとの比較に基づき、必要な処理が実行されます。

IWSVA では、感染した URL についてフィードバックが提供可能なため、Web レピュテーションデータベースの精度を上げるのに役立ちます。このフィードバックには、製品名とバージョン、URL、ウイルス名が含まれます (フィードバックには、IP アドレス情報は含まれないため、フィードバックはすべて匿名であり、企業の情報が保護されます)。IWSVA では、既存の Web アクセスポリシーに影響を与えずに Web レピュテーションの有効性を監視することもできます。結果は、インターネットセキュリティログとダッシュボード ([上位の脅威検出数]) で確認できます。

Web レピュテーションの詳細については、212 ページの「Web レピュテーションルールの指定」および 214 ページの「Web レピュテーション設定」を参照してください。

高可用性

IWSVA は、サービスの冗長性を確保するために高可用性 (HA) をサポートしており、透過ブリッジモードでのアクティブ / パッシブフェイルオーバを提供することで要件の厳しいビジネス環境における継続性を保証します。IWSVA の HA は、配置ウィザードを通じて簡単に展開され、新しいクラスタ管理機能によって管理されます。詳細については、96 ページの「高可用性の概要」を参照してください。

FTP 検索

IWSVA では、FTP のアップロードとダウンロードを検索できるほか、FTP ゲートウェイで指定したファイルタイプをブロックすることもできます。パフォーマンスへの支障を避けるため、FTP 検索モジュールには圧縮ファイルと大容量ファイルに特別な設定が用意されています。このほか、スパイウェア検索もサポートされています。

IWSVA の FTP 検索は、別の FTP プロキシサーバと同じ環境に配置できます。また、IWSVA を FTP プロキシとして使用することも可能です。InterScan Web Security Virtual Appliance のセキュリティを強化するため、IWSVA とそのポートへのアクセスを制御する、多数のセキュリティに関する設定が用意されています。

URL フィルタ

IWSVA の URL フィルタオプションを使用して、「成人向け」、「ギャンブル」、「金融サービス」などの URL のカテゴリに基づいてポリシーを設定できます。ユーザが URL を要求すると、IWSVA はまずその URL のカテゴリを検索し、次に管理者が設定したポリシーに基づいてその URL へのアクセスの許可、拒否、または監視、警告の表示、パスワードのオーバーライド、あるいは時間割り当ての設定を実行します。承認する URL のリストを定義することもでき、これらの URL はフィルタ処理されません。

コンテンツキャッシュ

Web コンテンツキャッシュは Web オブジェクト (HTML ページ、画像など) のキャッシュであり、帯域幅使用率、サーバの負荷、認識される遅延を削減します。Web キャッシュは、通過するオブジェクトのコピーを格納します。一定の条件を満たせば、以降の複製要求はキャッシュで処理できます。IWSVA 経由で Web にアクセスするユーザは、コンテンツキャッシュ機能により、帯域幅を節約しながら操作をより速く実行できます。詳細については、217 ページの「コンテンツキャッシュの使用」を参照してください。

さまざまなユーザ識別方法

IWSVA では、アプリケーション制御、HTTPS 復号化、HTTP ウイルス検索、HTTP 検査、情報漏えい対策、URL フィルタ、およびアクセス割り当てに対するポリシーの設定をサポートしています。ポリシーの適用範囲は、クライアント IP アドレス、ホスト名、LDAP ユーザ名またはグループ名のいずれかを使用して設定できます。

Hyper-V のインストールのサポート

現在、IWSVA では、Windows Server 2008 R2 以上を実行する Microsoft Hyper-V へのインストールをサポートしています。Hyper-V プラットフォームの 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をサポートします。詳細については、「IWSVA インストールガイド」の付録 F を参照してください。

通知

IWSVA は、プログラムイベントやセキュリティイベントに関する各種通知を発行できます。管理者への通知は、メール経由で指定管理者の連絡先に送信されます。ユーザへの通知は、要求側クライアントのブラウザに表示されます。管理者への通知もユーザへの通知も、カスタマイズ可能です。

ネットワーク管理ツールと連携するために、IWSVA では SNMP トラップとして各種の通知も発行できます。IWSVA は、セキュリティの脅威の検出、セキュリティ違反、プログラムやパターンファイルのアップデート、サービス停止が発生するとトラップを送信します。

IntelliTrap での検出は一種のセキュリティリスクと見なされるため、高度な脅威保護と同じ通知が使用されます。

リアルタイム統計情報とアラート

IWSVA には動的な統計機能が備わっており、管理者は IWSVA システムの情報を「リアルタイム」で閲覧できます。リアルタイム統計情報は、[システムステータス] 画面にグラフや表で表示されます。次のような統計情報が含まれます。

- ハードディスクドライブ

  ハードディスクドライブの統計情報は静的であり、[システムステータス] 画面が開いたときにのみ更新されます。
- 同時接続数
- CPU 使用率
- 物理メモリ使用率

ログとレポート

IWSVA は、ゲートウェイのセキュリティ統計情報を示す多数のレポートを備えています。特定の期間にだけレポートを実行し、対象とするクライアントだけの情報を表示するようカスタマイズすることも可能です。レポートは次のように大別できます。

- インターネットアクセス
- インターネットセキュリティ
- 帯域幅
- ポリシー施行
- データセキュリティ

レポートは、データベース内のログ情報から生成されます。IWSVA はログ情報をテキストのみのログ、テキストログとデータベース、またはデータベースのみのログに出力します。

このレポートは即時に生成することも、毎日、毎週、毎月、あるいは将来のいずれかの時点など予約によって生成することも可能です。ログとレポートのデータは、さらに詳細に分析するためにカンマ区切り値（CSV) のファイルに出力できます。ログが必要以上にディスク空き容量を消費しないよう、古くなったログは予約タスクによってサーバから削除できます。

詳細については、323 ページの「レポート、ログおよび通知」を参照してください。

ログやレポートに加えて、ダッシュボード画面にはランタイムシステム情報が表示され、ネットワークまたは IWSVA が正常に機能しているかどうか、トラフィック量またはインターネットの使用状況に矛盾がないかどうか、およびネットワーク上で異常なウイルス活動が検出されていないかどうかが示されます。

詳細については、44 ページの「ダッシュボード」を参照してください。

syslog のサポート

IWSVA では、エンタープライズクラスのログ機能を提供するために、syslog プロトコル（初期設定は、UDP ポート 514) を使用して、構造化された形式で複数の外部の syslog サーバにログを送信できます。

Cisco WCCP との統合

IWSVA は、Cisco Systems 定義のプロトコルである Web Cache Communication Protocol（WCCP) バージョン 2 をサポートしています。このプロトコルの詳細については、Cisco 製品のドキュメントを参照してください。

IWSVA が WCCP をサポートした場合、次のような利点があります。

- エンドポイント設定の必要がない配信透過性
- 高可用性と複数の IWSVA システム間の負荷分散
- IWSVA アプライアンスの追加や削除における負荷分散の自動再設定
- Cisco 製ルータ、スイッチ、およびプロトコル用ファイアウォール実装のサポート

IWSVA の WCCP 実装は、Cisco 製ルータ、スイッチ、PIX ファイアウォール、および ASA セキュリティデバイスと互換性があります。

IWSVA で WCCP を設定する際は、次の Cisco IOS のバージョンを使用することをお勧めします。

- バージョン 12.2 (0) ～ 12.2 (22)。バージョン 12.2 ファミリで、リリース 23 以上は使用しないでください。
- バージョン 12.3 (10) 以上。バージョン 12.3 ファミリで、リリース 0 ～ 9 は使用しないでください。
- IOS 15.1 (1) T3 以上

Cisco PIX ファイアウォールにはバージョン 7.2 (3) 以上を使用し、バージョン 7.2 (2) を使用しないことをお勧めします。

Cisco 以外のデバイスで WCCP バージョン 2 をサポートするデバイスについては、トレンドマイクロで明示的なテストを実施しておりません。そのため、互換性については保証できません。

リバースプロキシのサポート

IWSVA は通常、インターネットのセキュリティ上の脅威からクライアントを保護するため、クライアントの近くに設置します。一方、Web サーバに不正プログラムがアップロードされないように、リバースプロキシとして設置して、Web サーバを保護することもできます。リバースプロキシとして、IWSVA は保護対象の Web サーバの近くにインストールされます。IWSVA はクライアントの要求を受け取り、コンテンツ全体を検索してから HTTP 要求を Web サーバにリダイレクトします。

詳細については、145 ページの「リバースプロキシ」を参照してください。

InterScan Web Security Virtual Appliance の複数設置のサポート

複数の IWSVA デバイスを 1 台のコンソールから管理する方法は、Control Manager または Apex Central を介して実行されます。Control Manager では、管理コンソールから複数のトレンドマイクロ製品を管理し、複数の IWSVA をアクティベートすることができます。

コマンドラインインタフェース

IWSVA で提供されるネイティブ型コマンドラインインタフェース (CLI) により、システムの監視機能、システムの管理機能、デバッグ機能、トラブルシューティング機能などが、セキュリティで保護されたシェルやコンソールの直接接続を介して実行されます。

IWSVA の CLI では、業界標準の構文が使用され、よく知られたインタフェースがアプライアンス設定に用意されています。IWSVA では、セキュリティを考慮して、管理者はコンソールまたは SSH 接続を通してのみ CLI にアクセスできます。この機能は、IWSVA Web コンソールで有効にできます。

新機能

InterScan Web Security Virtual Appliance 6.5 SP2 から SP3 への変更点については、Readme をご確認ください。

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。

ICAP 1.0 対応キャッシュサーバとの連携

キャッシュサーバは、Web トラフィック輻輳の緩和と帯域幅節約に役立ちます。キャッシュサーバには「1 回のウイルス検索で複数の要求に対応する」方法が採用されており、IWSVA を介するウイルス検索のようなサードパーティのアプリケーションと統合できます。オープンプロトコルの Internet Caching Acceleration Protocol (ICAP) を使用することで、キャッシュとウイルス監視機能をシームレスに連結できます。IWSVA は、ICAP 1.0 規格をサポートするキャッシュサーバと連携します。

X-Authenticated ICAP ヘッダのサポート

X-Authenticated ヘッダには、X-Authenticated-User と X-Authenticated-Groups の 2 つの形式があります。X-Authenticated ヘッダの利用メリットは、2 つあります。第一に、IWSVA 内で LDAP クエリのオーバーヘッドを減らすこと、第二に、ICAP クライアントが異なるスキーマの LDAP サーバで LDAP 検索ができるようになることです。

システムステータス

IWSVA コンソールの [ダッシュボード] 画面に、リアルタイムの動的なシステム情報が表示されます。その他の生成可能なレポートには、静的な情報が表示されます。[システムステータス] 画面から次の情報へアクセスできます。

- しきい値アラート設定の有効化
- 同時接続数の表示
- インタフェースステータス
- CPU 使用率の表示
- 物理メモリ使用率の表示
- ハードウェアステータス
- ハードディスクドライブの表示

しきい値アラート設定の有効化

次の項目が危険なレベルに達した場合に通知が送信されるように、しきい値アラートの値やアラートの頻度を指定できます。

- ウイルス
- スパイウェア
- データベース
- ハードディスクドライブ
- 帯域幅

IWSVA では、これらのアラートをメールまたは SNMP トラップ / 通知 (有効になっている場合)、または両方を使用して送信できます。339 ページの「通知先の設定」を参照してください。

注意 : メール通知のしきい値アラートを設定してください。しきい値アラート設定は、IWSVA が SNMP トラップを送信するタイミングに影響しません。

しきい値アラートを有効にするには

1. 管理コンソールから [システムステータス] を選択し、[しきい値アラート] をクリックします。
2. [しきい値] で必要なしきい値を指定し、初期設定を使用するか、または [しきい値] 列と [通知の送信間隔] 列に新たな値を指定します。

3. [通知メッセージ] で初期設定の通知メッセージを使用しない場合は、初期設定のテキストを選択して、任意のテキストを入力します。該当する場合は、339 ページの「通知の変数」で説明されているように、テキストに変数を挿入します。
4. [保存] をクリックします。

同時接続数の表示

HTTP/HTTPS の同時接続使用率は紫色で、FTP の同時接続使用率はオレンジ色で動的に表示されます。接続数と接続時間 (秒単位) が表示されます。

これには、FTP および HTTP/HTTPS に関する 2 つのグラフが含まれます。FTP については、コマンドとデータの両方のセッションの接続が測定されます。HTTP/HTTPS については、要求と応答の両方のセッションの接続が測定されます。初期設定の表示更新頻度は 30 秒です。X 軸と Y 軸のスケールはどちらも可変です。X 軸のスケールは設定した表示更新頻度によって決まり、Y 軸のスケールは特定時刻の同時接続数によって決まります。

インタフェースステータス

表 1-1 のアイコンは、インタフェースのステータスを表します。

表 1-1. インタフェースステータスのインジケータ

アイコン	説明
	リンクが検出されません。ポートが空であるか、ケーブルが外れているか壊れている、またはピアコンピュータがダウンしている可能性があります。
	リンクは正常です
	リンクエラー
	リンクが無効です
D	データインタフェース

表 1-1.　インタフェースステータスのインジケータ (続き)

アイコン	説明
M	管理インタフェース
H	高可用性インタフェース

ハードウェアステータス

ハードウェアステータス機能を使用すると、管理者は、Intelligent Platform Management Interface (IPMI) 対応デバイス上でファン、電圧、温度などのハードウェア情報を監視できます。

注意： IWSVA のハードウェア監視は、ベアメタルインストールされた Intelligent Platform Management Interface (IPMI) v2.0 がサポートされている Baseboard Management Controller (BMC) とのみ互換性があります。

管理者は、IWSVA Web コンソールまたは SNMP 要求を使用して、ハードウェアステータス情報を問い合わせることができます。SNMP トラップが有効になっている場合は、「温度のしきい値を超過した」、「電圧のしきい値を超過した」などのシステムイベントが検出されたときに、警告が送信されます。

警告は、管理者に問題を通知するときに送信できます。警告は次で設定されます。[通知] → [通知の設定] → [ハードウェア監視イベント] (チェックボックス)

以下では、[ハードウェアステータス] 画面で使用できるオプションを簡単に説明しています。

- **ハードウェアの種類**– 電圧、ファン、CPU、記憶装置、温度の統計を表示します。
- **ステータス**– ハードウェアの現在のステータスを表示します。通常の状態では「正常」と表示されますが、異常なイベントが発生した場合、イベントに応じて「重大」または「失敗」と表示されます。5 つのステータスを利用できます。
  - **正常**– コンポーネントのステータスは正常です。
  - **警告**– コンポーネントのステータスは危険にさらされています。
  - **重大**– コンポーネントのステータスは失敗になる危険があります。
  - **失敗**– コンポーネントは稼働していません。
  - **不明**– コンポーネント情報が利用できません。
- **センサー情報**– 監視されるハードウェアの種類のステータスに関する情報を表示します。

SNMP クエリとトラップ

管理者は、SNMP クエリを使用してハードウェアステータスをポーリングし、SNMP トラップを介してアラートを受信できます。これを実行するには、管理者は、ハードウェア監視 MIB ファイルを iReasoning MIB ブラウザなどの SNMP ツールにインポートする必要があります。

また、IWSVA は、ネットワークインタフェースカードの統計用の 2 つの標準 MIB ファイルをサポートしています。

- RFC1213-MIB
- HOST-RESOURCES-MIB

これらは以下から入手可能です。

`http://www.simpleweb.org/ietf/mibs/`

ハードウェアイベント監視用の 3 番目のトレンドマイクロ固有の MIB は、以下になります。
TM-HWMONITOR-MIB

これは、次のトレンドマイクロのダウンロードサイトにあります。

`http://www.trendmicro.com/ftp/documentation/guides/MIBs.zip`

IWSVA からトラップを受信するには、管理者が、[管理] → [ネットワーク設定] → [SNMP の設定] で SNMP トラップの宛先を設定する必要があります。

CPU 使用率の表示

これは、ローカルシステム上の CPU 使用状況を示す動的な表示機能です。複数の CPU がある場合、すべての CPU の IWSVA による平均的な使用率を表示します。すべての CPU 使用率を 1 つの線グラフで表します。IWSVA では、使用された CPU サイクル、IWSVA によって使用された CPU サイクル、バックエンドで使用された CPU サイクルの合計、CPU 監視 API を基に CPU 使用率を決定します。

初期設定では、IWSVA は毎秒の CPU 使用率を 2 分間サンプリングし、120 のデータポイントを作成します（1 データポイント / 秒 x 120 秒（2 分間) = 120 データポイント)。初期設定の表示更新頻度は、`/etc/iscan/intscan.ini` ファイルの `[metrics]` セクションにあるパラメータ `cpu_refresh` を編集することで変更できます。ファイルを変更したら、次のコマンドを使用して Tomcat サービスを再起動します。

```
/etc/iscan/S99IScanHttpd restart
```

[1 日間] ボタンまたは [30 日間] ボタンをクリックすると、ウィンドウが開き、それぞれ 1 日または 30 日間の CPU 使用率を表す静的グラフが表示されます。IWSVA ではこの情報をデータベースから取得します。データベースに十分なデータがない場合、この表示機能には利用可能なデータが表示されます。

注意： 30 日間表示するオプションでは、1 日分の CPU 使用率データが 1 つのポイントで示されます。1 日表示のオプションでは、画面に時間ごとの CPU 使用率が 1 つのポイントで示されます。IWSVA は利用可能な 2 つ以上のポイント分のデータがなければグラフデータとして処理できません。

物理メモリ使用率の表示

これは、ローカル IWSVA サーバが使用する物理メモリの容量を示す動的な表示機能です。

初期設定では、IWSVA は毎秒の物理メモリ使用率を 2 分間サンプリングし、120 のデータポイントを作成します（1 データポイント / 秒 x 120 秒（2 分間) = 120 データポイント)。初期設定の表示更新頻度は、`/etc/iscan/intscan.ini` ファイルの `[metrics]` セクションにあるパラメータ `memory_refresh` を編集することで変更できます。ファイルを変更したら、次のコマンドを使用して Tomcat サービスを再起動します。

```
/etc/iscan/S99IScanHttpd restart
```

[1 日間] ボタンまたは [30 日間] ボタンをクリックすると、ウィンドウが開き、それぞれ 1 日または 30 日間の物理メモリ使用率を表す静的グラフが表示されます。IWSVA ではこの情報をデータベースから取得します。データベースに十分なデータがない場合、この表示機能には利用可能なデータが表示されます。

注意： 30 日間表示するオプションでは、1 日分の物理メモリ使用率データが 1 つのポイントで示されます。1 日表示のオプションでは、画面に時間ごとの物理メモリ使用率が 1 つのポイントで示されます。IWSVA は利用可能な 2 つ以上のポイント分のデータがなければグラフデータとして処理できません。

詳細については、125 ページの「手動アップデート」を参照してください。

ハードディスクドライブの表示

IWSVA によって、システムファイル、隔離領域、一時領域、およびログに使用されるディスクのステータスを示す静的表示です。ハードディスクドライブの表示機能では、最大 12 のディスクを監視できます。

データベースがこれらのディレクトリと同じドライブに存在する場合、データベースディスクの使用率も表示されます。Y 軸の目盛りの範囲は 10 ～ 100% です。

しきい値アラートの値とアラートの頻度を指定して、ハードディスクのステータスが重大レベルに到達したときに通知を受け取ることができます。IWSVA では、これらのアラートをメールまたは SNMP トラップ / 通知（有効になっている場合)、または両方を使用して送信できます。設定されているしきい値に達すると SNMP トラップが送信されます。

その他の Web 脅威情報へのアクセス

[システムステータス] 画面の右上隅にある [脅威に関するリソース] リストで、トレンドマイクロの Web 脅威保護サイトへのリンクにアクセスすると、多様なことができます。最新の Web 脅威や多様な Web 脅威の発生元を調査したり、トレンドマイクロのセキュリティデータベース検索にアクセ

スしたり、Web とメール不正プログラムのリアルタイム統計情報を確認できます。[脅威に関するリソース] リストの表示については、233 ページの「高度な脅威保護のパフォーマンスに関する考慮事項」を参照してください。

図 1-1.　IWSVA でアクセス可能な Web 脅威保護テクノロジ

ダッシュボード

ダッシュボードには、ネットワークまたは IWSVA が正常に機能しているかどうか、トラフィック量またはインターネットの使用状況に矛盾がなく基準内であるかどうか、およびネットワーク上で異常なウイルス活動が検出されていないかどうかが示されます。IWSVA のダッシュボードには、過去 1 時間、12 時間、および 24 時間内に発生したデバイスグループのトランザクションと、過去 1 週間のトランザクションの増加の概要が表示されます。

IWSVA では、IWSVA サーバの「リアルタイム」な統計情報を動的に表示できます。

- **アクセスされた上位 URL カテゴリ** — このウィジェットには URL カテゴリに関連した違反が表示されます。過去 1 時間、1 日、1 週間、または 1 か月間の情報を表示できます。過去 1 時間、1 日、1 週間、または 1 か月間の情報を表示できます。ウィジェット右上にある [表示更新] アイコンをクリックすると、データの表示を手動で更新できます。初期設定の表示は棒グラフ形式ですが、表形式に切り替えることができます。表示するソースの数を設定するには、[表示更新] アイコンの横にある [編集] アイコンをクリックして、ポップアップウィンドウに必要な値を設定します。

- **インターネットセキュリティによってブロックされた上位ユーザ (初期設定)** — 指定期間内に最も多くブロックされたサイトにアクセスしたユーザを示し、インターネットセキュリティや許容される使用方法についてユーザに理解を促します。初期設定は上位 5 件、過去 1 日間です。
- **ブロックされた上位 URL カテゴリ (初期設定)** — 指定期間内に最も多くブロックされた URL カテゴリを示し、セキュリティ、帯域幅、および生産性の潜在的な問題について概要ビューを提供します。初期設定は上位 5 件、過去 1 日間です。
- **アプリケーション帯域幅 (初期設定)** — 指定期間のアプリケーションの使用状況における帯域幅 (kbps) のトラフィック傾向を示します。初期設定の期間は過去 1 日間です。
- **ブロックされた上位アプリケーション** — 指定期間内に最も多くブロックされたアプリケーションカテゴリを示し、セキュリティ、帯域幅、および生産性の潜在的な問題について概要ビューを提供します。初期設定は上位 5 件、過去 1 日間です。
- **ペイロード** — FTP および HTTP/HTTPS に関する 2 つのグラフを示す動的表示です。FTP については、コマンドとデータの両方のセッションの接続が測定されます。HTTP/HTTPS については、要求と応答の両方のセッションの接続が測定されます。初期設定は過去 1 日間です。
- **許可された上位アプリケーション** — 許可された上位アプリケーションへのアクセスインスタンスの指定期間内の合計数を示します。
- **上位の脅威検出数 (初期設定)** — 指定期間内に IWSVA によって検出された各種の脅威 (不正 URL、ウイルス、スパイウェア、ボットネット、セキュリティホール) の合計件数を示し、さまざまな脅威ベクトルのリスクレベルの概要ビューを提供します。初期設定は過去 1 日間です。
- **上位のポリシー施行 — アプリケーション制御** — 指定期間内に違反が発生したポリシーとその要求数を示すことで、ポリシーの実効性と変更の必要性を示します。初期設定は上位 5 件、過去 1 日間です。
- **上位のポリシー施行 — URL フィルタ** — 指定期間内に違反が発生したポリシーとその要求数を示すことで、ポリシーの実効性と変更の必要性を示します。初期設定は上位 5 件、過去 1 日間です。
- **上位のポリシー施行 — DLP** — 指定期間内に違反 (ブロック / 監視) が発生したポリシーとその要求数を示すことで、ポリシーの実効性と変更の必要性を示します。
- **C&C コールバック回数 (コマンド & コントロールコールバック回数)** — 指定期間内に検出された C&C コールバック試行回数を示します。

ウィジェット内の対象コンポーネントにマウスを合わせると、対応する数値データ値が表示されます。たとえば、「脅威検出合計件数」ウィジェットで不正 URL のバーにマウスを合わせると、対応するデータ値が表示されます。

ウィジェット内をクリックすると、現在のウィジェットの設定パラメータの詳細が表示されるログ分析画面に移動します。

Web トラフィックのセキュリティ上の脅威の概要

Web トラフィックにより、企業ネットワークは多数のセキュリティ上の脅威にさらされる可能性があります。ほとんどのコンピュータウイルスがメッセージングゲートウェイ経由で組織に侵入するとはいえ、Web トラフィックは新種のセキュリティリスクの媒介経路になっています。たとえば、複数のエントリポイントと脆弱性を突いた「複合型リスク」は、HTTP を介して蔓延します。

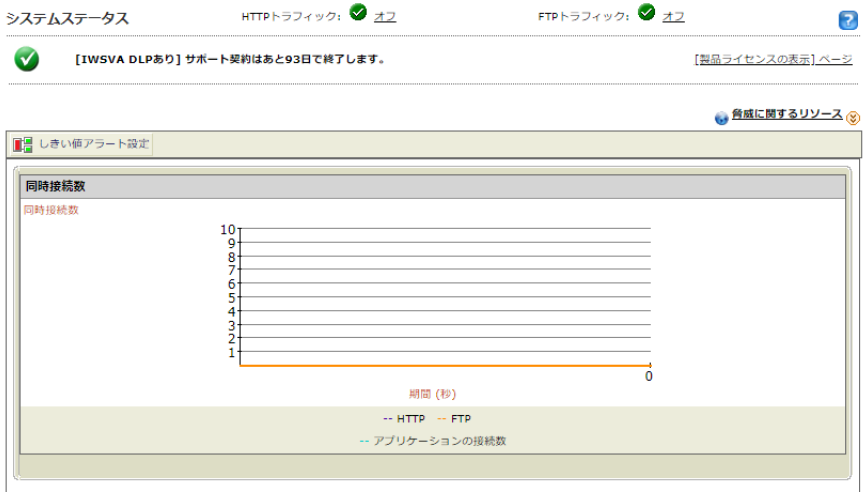


図 1-2. IWSVA の [システムステータス] 画面には、セキュリティリスクに関する情報が表示されます。

ウイルスの大規模感染によって必要となる診断、復旧、生産性損失に伴うコストは、事前に対策することによって大部分が回避可能です。IWSVA は、ウイルスやその他の脅威を特定し、企業ネットワークの HTTPS、HTTP、および FTP トラフィックを含む複数のインターネットプロトコルを保護する包括的なセキュリティ製品です。

コンテンツベースのウイルス対策検索はもちろん、IWSVA はその他のネットワークセキュリティ対策にも役立ちます。

- アプリケーション制御機能では、人気の高いインターネットアプリケーションを自動的に検出し、管理者がポリシーを使用してそれらのアプリケーションを制御できるようにするセキュリティテクノロジを提供します。
- 従業員によって悪用される可能性のある数百のインターネットアプリケーションを監視し、ブロック / 許可ポリシーを有効にします。

- Web レピュテーションでは、潜在的に危険な Web サイト、特に既知のフィッシングサイトまたはファーミングサイトにアクセスする前に URL を調べます。
- URL フィルタ機能を使用すると、企業で禁止されたコンテンツを含む Web サイトへのアクセスを許可、ブロック、オーバーライド付きブロック、警告した上での許可、または監視できます。
- HTTPS 復号化機能を使用すると、暗号化されたトラフィックは IWSVA 検索およびフィルタポリシーを「通常」の HTTP トラフィックとして通過することができ、HTTPS サーバからの証明書が検証されます。

第 2 章

配置ウィザード

この章の内容は、お使いのネットワークに応じて InterScan Web Security Virtual Appliance（以下、IWSVA) を設定する際に、展開プロセスの手順を理解する上で役立ちます。

本章で説明する内容には、次の項目が含まれます。

配置ウィザードの概要

配置ウィザードは初回ログイン時に自動的に表示され、配置プロセスの手順が順を追って示されます。また、設定を確認したり変更したりするために、いつでも [管理] → [配置ウィザード] から手動で起動できます。

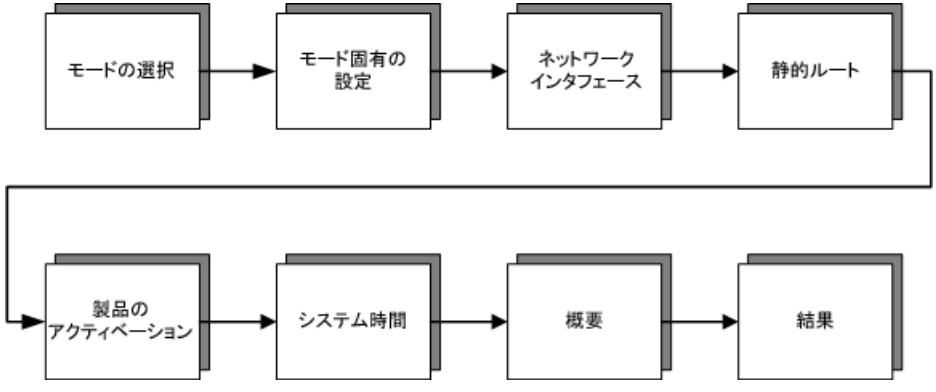


図 2-1.　配置ウィザードのフロー

モード選択

IWSVA は、ネットワークセキュリティのニーズに応じて、さまざまなモードで配信できます。選択するモードの詳細については、「IWSVA インストールガイド」の第 2 章の「配置について」を参照してください。

配置ウィザードを使用して、IWSVA を 7 つのモードのいずれかに設定できます。

- 51 ページの「透過ブリッジモード」
- 52 ページの「透過ブリッジモード - 高可用性」
- 56 ページの「プロキシ転送モード」
- 57 ページの「リバースプロキシモード」
- 58 ページの「ICAP モード」
- 60 ページの「通常の透過モード」
- 61 ページの「Web Cache Coordination Protocol（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、トラフィックが双方向で検索される最も容易な配信モードです。

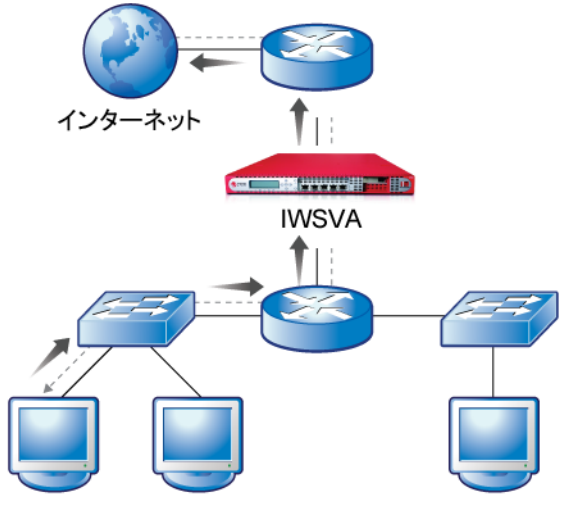


図 2-2.　透過ブリッジモード

透過ブリッジモードおよび透過ブリッジモード - 高可用性は、アプリケーション制御レポートおよびポリシーの機能に対応する唯一の配信モードです。これらの理由により、製品をこれらのモードのいずれかで配信してインターネットトラフィックの可視性と保護を最大限に実現することを強くお勧めします。

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。最大限の互換性を確保するには、次のネットワークカードの使用をお勧めします。

- Broadcom NetXtreme Series
- Intel Pro/1000 PT Dual Port Server Adapter
- Intel Pro/1000 MF Dual Port Fiber

注意： IWSVA を透過ブリッジモードで設定する方法の詳細については、147 ページの「ネットワーク設定および負荷の処理」を参照してください。

IWSVA を透過ブリッジモードで配信するには

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 [透過ブリッジモード] ラジオボタンをクリックします。
4. [次へ] をクリックします。
5. 72 ページの「ネットワークインタフェース」に移動して続行します。

注意： 単一ノードの透過ブリッジモードでは、モード固有の設定は必要ありません。IWSVA の設定方法の詳細については、147 ページの「ネットワーク設定および負荷の処理」を参照してください。

透過ブリッジモード - 高可用性

現在、IWSVA 高可用性 (HA) ソリューションでは、透過ブリッジモードを利用するアクティブ / パッシブペアがサポートされています。IPv4 アドレスの IWSVA クラスタを配置するには、IWSVA ユニットのそれぞれが別個の管理インタフェースを使用する必要があります。

透過ブリッジモード - 高可用性配置には、クラスタ配置ごとに少なくとも次の 4 つのネットワークインタフェースカード (NIC) が必要です。

- ブリッジデータインタフェース用に 2 つ
- HA インタフェース用に 1 つ
- 専用の管理インタフェース用に 1 つ

注意： 高可用性とクラスタ管理の詳細については、95 ページの「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。

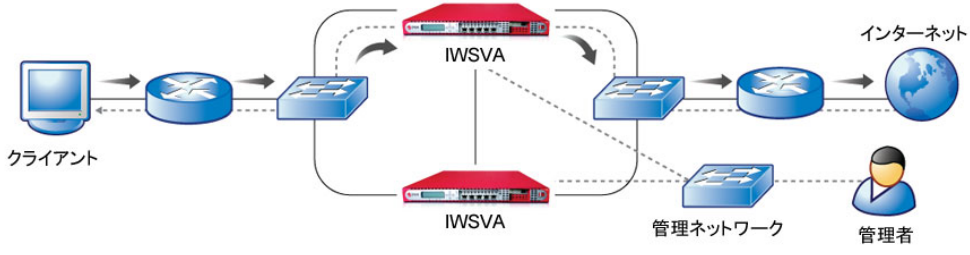


図 2-3. 透過ブリッジモード - 高可用性

注意： IWSVA が単一 HA クラスタ内でサポートする HA ノードは 2 つのみです。

配置ウィザードを使用して、次のいずれかを実行できます。

- 54 ページの「新規クラスタの作成」
- 55 ページの「既存クラスタの結合」

クラスタ IP アドレスについて

クラスタ IP アドレスとは、クラスタの管理ポートの浮動 IP アドレスを意味します。ユーザは Web コンソールまたは CLI からこの IP アドレスにアクセスして、クラスタを管理します。浮動 IP アドレスはクラスタ内で浮動します。スイッチオーバが発生すると、クラスタの浮動 IP アドレス（クラスタ IP アドレス) は常に上位デバイスを指します。

重み付けされた優先順位の選択について

重み付けされた優先順位の選択処理を有効にすると、最も重みが高いデバイスが常に上位メンバーとして選択されるようになります。重み付けされた優先順位の選択処理を無効にすると、より高い重みを持つ新しいクラスタメンバーがクラスタに追加された場合でも、現在の上位メンバーが上位メンバーとしてとどまることになります。

重みとは、クラスタ内のメンバーのユーザ定義による優先順位です。2 つのメンバーに同じ重みが割り当てられている場合でも、どちらかが上位でどちらかが下位になりますが、上位メンバーの選択は内部アルゴリズムに基づいて行われます。重み付けされた優先順位の選択を有効にしている場合、クラスタメンバーへの同じ重みの割り当ては禁止されます。

新規クラスタの作成

新しいクラスタを作成するには

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、[透過ブリッジモード - 高可用性] オプションをオンにします。
4. [新規クラスタ] オプションをオンにします。
5. [次へ] をクリックします。
6. 以下のようにクラスタを設定します。
   a. クラスタ名を入力します。
   b. クラスタの説明 (オプション) を入力します。
   c. クラスタの IP アドレスを入力します。詳細については、53 ページの「クラスタ IP アドレスについて」を参照してください。
   d. [重み付けされた優先順位の選択] ドロップダウンリストから、[有効にする] または [無効にする] を選択します。

      注意： 重み付けされた優先順位の選択の詳細については、53 ページの「重み付けされた優先順位の選択について」を参照してください。

      注意： クラスタ IP アドレスでは、IPv6 はサポートしていません。

      - 有効な場合、HA ペアは重みが最も大きいコンピュータを選択します。
      - 無効の場合、HA ペアは、現在アクティブな (プライマリ) コンピュータが使用できない場合にのみ選択を行います。

注意： HA モードはアクティブ / パッシブと表示されます。配信モードには「透過ブリッジモード - 高可用性」を示すブリッジが常に表示されます。

e. 「インタフェースステータス」セクションの情報を使用して、ドロップダウンリストから HA インタフェース (eth0、eth1、eth2、eth3 など) を選択します。

アクティブおよびパッシブ IWSVA は、HA または「接続ステータス」インタフェースを介して直接接続されます。インタフェースステータスのグラフィックに H と表示されたインタフェースには、次の 2 つの機能があります。

- アクティブおよびパッシブな仮想アプライアンスは、1 秒ごとに 1 パッケージを送信し、稼働中であることを互いに通知します。
- インタフェースは同期プロセスで使用されます。

インタフェースステータスのグラフィックを使用する方法の詳細については、74 ページの図および 74 ページの表 2-8 を参照してください。また、73 ページの「インタフェースステータスの判別」も参照してください。

f. 重みの値を入力します。(初期設定 128)

- 重みの高いメンバーは高い優先順位を持ち、上位メンバーになります。

7. [次へ] をクリックします。
8. 72 ページの「ネットワークインタフェース」をセットアップし、展開を続行します。

既存クラスタの結合

既存のクラスタを結合するには

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、[透過ブリッジモード - 高可用性] オプションをオンにします。
4. [クラスタの結合] オプションをオンにします。
5. [次へ] をクリックします。
6. 以下のようにクラスタを設定します。

a. 「インタフェースステータス」セクションの情報を使用して、ドロップダウンリストから HA インタフェース (eth0、eth1、eth2、eth3 など) を選択します。

アクティブおよびパッシブ IWSVA は、HA または「接続ステータス」インタフェースを介して直接接続されます。インタフェースステータスのグラフィックに H と表示されたインタフェースには、次の 2 つの機能があります。

- アクティブおよびパッシブな仮想アプライアンスは、1 秒ごとに 1 パッケージを送信し、稼働中であることを互いに通知します。
- インタフェースは同期プロセスで使用されます。

インタフェースステータスのグラフィックを使用する方法の詳細については、74 ページの図および 74 ページの表 2-8 を参照してください。また、73 ページの「インタフェースステータスの判別」も参照してください。

b. 重みの値を入力します。(初期設定 64)

7. [次へ] をクリックします。既存のクラスタへの接続の進行状況を示すバーが表示されます。
8. クラスタへの接続後に表示されるクラスタ情報画面を確認し、[次へ] をクリックします。
9. 72 ページの「ネットワークインタフェース」をセットアップし、展開を続行します。

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できます。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。コンテンツは、受信方向と送信方向の両方で検索されます。IWSVA は HTTP、HTTPS、および FTP プロトコルを認識するため、アプリケーション制御のレポートとポリシーもプロキシモードで機能します。

プロキシ転送モードは、次の機能も備えています。

- すべてのトラフィックを別の上位プロキシサーバに転送します。
- 別のプロキシサーバとのプロキシチェーン構成に参加し、X-Forwarded-For 機能をサポートします。
- ゲストユーザに専用のトラフィックチャネルを提供する場合は、ゲストポートを使用します。ゲストポートを通過するトラフィックにはゲストポリシーが適用されます。

注意： IWSVA をプロキシ転送モードで設定する方法の詳細については、147 ページの「ネットワーク設定および負荷の処理」を参照してください。

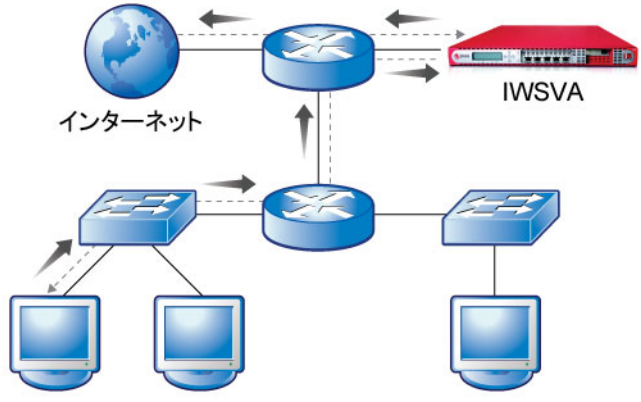


図 2-4.　プロキシ転送モード

IWSVA をプロキシ転送モードで配信するには

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 [プロキシ転送モード] ラジオボタンをクリックします。
4. [次へ] をクリックします。
5. 62 ページの「モード固有の設定」に移動して続行します。

リバースプロキシモード

この配信モードでは、IWSVA は Web サーバの前に配置されます。IWSVA は、Web サーバにアップロードされるクライアントの HTTP コンテンツと FTP コンテンツ、および 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。

警告： **このモードでは、DLP 機能は無効になります。**

注意： IWSVA をリバースプロキシモードで設定する方法の詳細については、147 ページの「ネットワーク設定および負荷の処理」を参照してください。

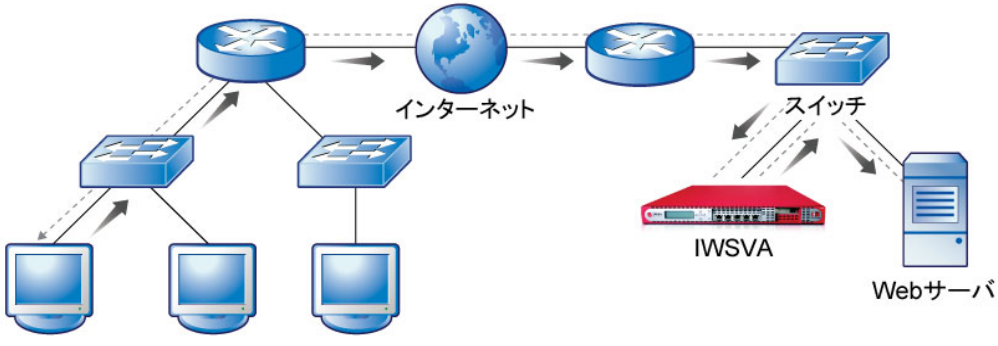


図 2-5.　リバースプロキシモード

IWSVA をリバースプロキシモードで配信するには

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] ラジオボタンをクリックします。
4. [次へ] をクリックします。
5. 62 ページの「モード固有の設定」に移動して続行します。

ICAP モード

現在、この配信モードは IPv6 をサポートしていません。この配信モードの IWSVA は、ICAP サーバとして機能し、(IWSVA のクライアントとして機能している) ICAP v1.0 対応キャッシュサーバからの ICAP 接続を受け入れます。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エンドユーザ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。

注意： ICAP モードの有効化と設定については、147 ページの「ネットワーク設定および負荷の処理」および 84 ページの「IWSVA ICAP の設定」を参照してください。

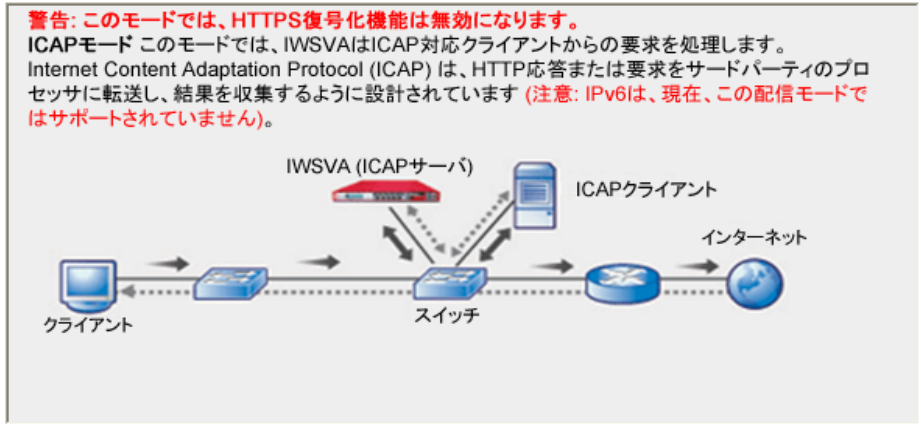


図 2-6. ICAP モード

配置ウィザードで IWSVA を ICAP モードで配信する

IWSVA を ICAP モードで配信するには

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 [ICAP モード] ラジオボタンをクリックします。
4. [次へ] をクリックします。
5. 62 ページの「モード固有の設定」に移動して続行します。

通常の透過モード

現在、この配信モードは IPv6 をサポートしていません。IWSVA の通常の透過モードは、一般的なレイヤ 4 負荷分散スイッチを使用して通常の透過モードをサポートし、クライアントのブラウザ設定を変更せずに HTTP 検索を実現します。このモードでは、HTTPS 復号化機能は無効になります。

注意： IWSVA を通常の透過モードで設定する方法の詳細については、147 ページの「ネットワーク設定および負荷の処理」を参照してください。

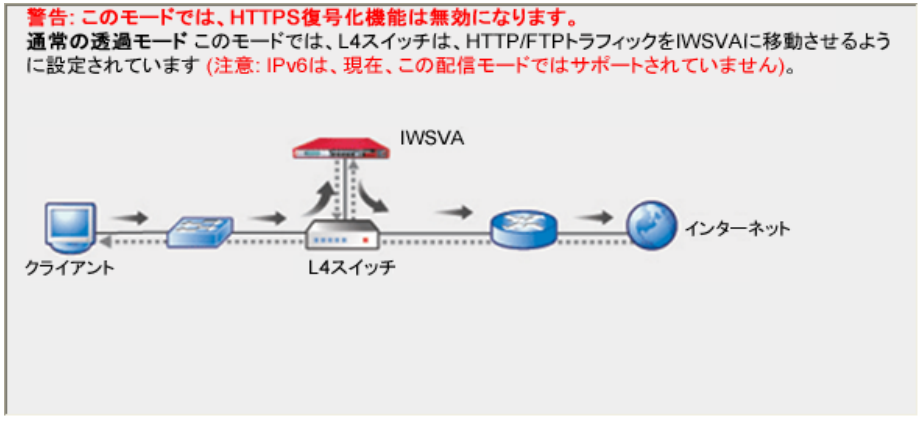


図 2-7.　通常の透過モード

IWSVA を通常の透過モードで配信するには

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 [通常の透過モード] ラジオボタンをクリックします。
4. [次へ] をクリックします。
5. 62 ページの「モード固有の設定」に移動して続行します。

Web Cache Coordination Protocol (WCCP) モード

この配信モードでは IPv6 がサポートされます。IWSVA は、Cisco の WCCP プロトコルと連携して、Web および FTP トラフィックのコンテンツ検索をクライアント設定を変更する必要なく実行し、また、ハードウェアを追加することなく、アーキテクチャの設計に冗長性と商品性を組み込むことができます。

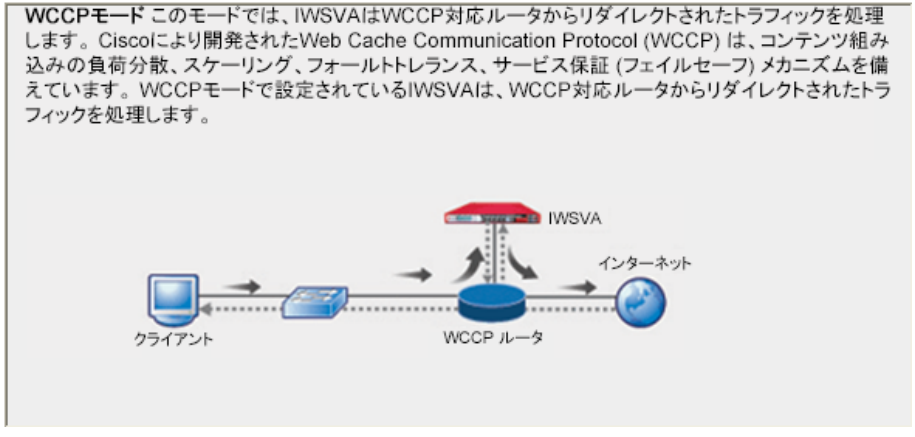


図 2-8. WCCP モード

注意： IWSVA と連携動作させるための WCCP サーバの設定方法の詳細については、147 ページの「ネットワーク設定および負荷の処理」および Cisco 製品ドキュメントを参照してください。

IWSVA を WCCP モードで配信するには

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 [WCCP モード] ラジオボタンをクリックします。
4. [次へ] をクリックします。
5. 62 ページの「モード固有の設定」に移動して続行します。

モード固有の設定

一部の配信モードには、モード固有の設定があります。配置ウィザードの 2 番目の手順では、モード固有の設定を行うことができます。透過ブリッジモードには、モード固有の設定はありません。

表 2-1.　モード固有の設定

モード	モード固有の設定	ページ
透過ブリッジモード	なし	該当なし
透過ブリッジモード - 高可用性	新規 : ・ クラスタの設定 ・ 重み付けされた優先順位の選択の有無 ・ HA インタフェース ・ 重み 既存 : ・ HA インタフェース ・ 重み	新規 : 54 既存 : 55
プロキシ転送モード	プロキシ設定	62
リバースプロキシモード	プロキシ設定	62
ICAP モード	ICAP 設定	65
通常の透過モード	透過設定	68
WCCP モード	WCCP 設定	69

プロキシ設定

以下のモードでインストールを実行している場合は、プロキシを設定する必要があります。

- プロキシ転送のスタンドアロンモード - 63 ページの「スタンドアロンプロキシモードの設定」を参照
- プロキシ転送の上位プロキシモード - 64 ページの「上位プロキシ (依存) モードの設定」を参照
- リバースプロキシモード - 64 ページの「リバースプロキシの設定」を参照

プロキシ転送モード

ネットワーク設定に応じて、次のいずれかを指定できます。

- 63 ページの「スタンドアロンプロキシモードの設定」
- 64 ページの「上位プロキシ (依存) モードの設定」

スタンドアロンプロキシモードの設定

スタンドアロンモードのプロキシを設定するには

1. [配信モード] 画面で [プロキシ転送モード] ラジオボタンを選択します。
   詳細については、56 ページの「プロキシ転送モード」を参照してください。
2. [次へ] をクリックします。
3. 表 2-2 の設定の推奨事項に従います。

表 2-2. プロキシ転送モードでのスタンドアロン設定

構成パラメータ	詳細	推奨値
HTTP 待機ポート番号	IWSVA が接続の受信を待機するポートです。	8080
上位プロキシを有効にする (チェックボックス)	上位プロキシを有効 / 無効にします。	IWSVA の別の上位プロキシデバイスを使用しない場合は、チェックボックスをオフのままにします。
ゲストユーザログインを有効にする	ゲストポートを有効 / 無効にします。	ゲストポートを使用しない場合はチェックボックスをオフのままにします。
ポート番号	ゲストポートのポート番号です。	8081

4. [次へ] をクリックします。
5. 72 ページの「ネットワークインタフェース」をセットアップし、展開を続行します。

上位プロキシ (依存) モードの設定

上位モードのプロキシを設定するには

1. [配信モード] 画面で [プロキシ転送モード] ラジオボタンを選択します。
   詳細については、56 ページの「プロキシ転送モード」を参照してください。
2. [次へ] をクリックします。
3. 表 2-3 の設定の推奨事項に従います。

表 2-3. プロキシ転送モードでの上位プロキシ (依存) の設定

構成パラメータ	詳細	推奨値
HTTP 待機ポート番号	IWSVA が接続の受信を待機するポートです。	8080
上位プロキシを有効にする (チェックボックス)	上位プロキシを有効 / 無効にします。	オン (有効) にします。
プロキシサーバ	上位プロキシサーバの IP アドレスです。	上位プロキシサーバの値を入力します。
ポート	上位プロキシサーバのポートです。	上位プロキシサーバのポート番号を入力します。
ゲストユーザログインを有効にする	ゲストポートを有効 / 無効にします。	ゲストポートを使用しない場合はチェックボックスをオフのままにします。
ポート番号	ゲストポートのポート番号です。	8081

4. [次へ] をクリックします。
5. 72 ページの「ネットワークインタフェース」をセットアップし、展開を続行します。

リバースプロキシの設定

リバースプロキシモードのプロキシを設定するには

1. [配信モード] 画面で [リバースプロキシモード] ラジオボタンを選択します。
   詳細については、57 ページの「リバースプロキシモード」を参照してください。

2. [次へ] をクリックします。
3. 表 2-4 の設定の推奨事項に従います。

表 2-4. リバースプロキシモードのプロキシの設定

構成パラメータ	詳細	推奨値
HTTP 待機ポート番号	IWSVA がリバースプロキシの接続の受信を待機するポートです。	80
保護対象サーバ	IWSVA が保護する Web サーバの IP アドレスです。	保護対象サーバの IP アドレスを入力します
ポート番号	IWSVA が保護する Web サーバのポートです。	保護対象サーバのポート番号を入力します。
SSL ポート番号	IWSVA が保護する Web サーバの SSL ポートです。	初期設定は 443 です。保護対象サーバの SSL ポート番号を入力します。
SSL ポートを有効にする (チェックボックス)	SSL を有効 / 無効にします。	不要な場合は、無効のままにします。有効にするには、オンにします。

4. [次へ] をクリックします。
5. 72 ページの「ネットワークインタフェース」をセットアップし、展開を続行します。

ICAP の設定

注意： SSL ハンドシェイクに SSLv2 または SSLv3 を使用している ICAP クライアントでは ICAPS は使用できません。セキュアな ICAP 通信には TLSv1、TLSv1.1、および TLSv1.2 のみがサポートされます。

ICAP モードでの配信には、追加の設定が必要です。

IWSVA は、ウイルスが検出されるたびに、またはユーザとグループに関する情報を提供するために、ICAP サーバから 4 つのオプションのヘッダを返すことができます。初期設定ではパフォーマンス上の理由から「X-Virus-ID」および「X-Infection-Found」は返されません。多くの ICAP クライアントはこれらのヘッダを使用しないためです。これらのヘッダを IWSVA Web コンソールで有効にする必要があります。

- X-Virus-ID: 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。たとえば、次のように記述します。

  ```
  X-Virus-ID:EICAR Test String
  ```

- X-Infection-Found: 感染の種類、解決策、およびリスクについての説明に対する数値コードを返します。

  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-Authenticated - User: 有効な場合、IWSVA は「X-Authenticated-User」ICAP ヘッダで送信されるユーザ名を要求します。ユーザの識別にユーザ / グループ名を使用するように IWSVA を設定している場合、IWSVA は、ICAP ヘッダから取得されたユーザ名を使用して、要求を発行したユーザを識別できます。
- X-Authenticated - Group: 有効な場合、ユーザの識別にユーザ / グループ名を使用するように IWSVA を設定していると、IWSVA は「X-Authenticated-Groups」ICAP ヘッダで送信されるグループメンバーシップ情報を要求します。無効な場合、IWSVA は、グループメンバーシップ情報について LDAP に問い合わせます。

注意： 一部の ICAP クライアントは、再帰的なグループメンバーシップの検索をサポートしていません。たとえば、ユーザがグループ A に所属し、グループ A がグループ B に所属している場合は、ICAP クライアントがヘッダで送信するのはグループ A の情報のみになります。再帰的なグループメンバーシップ情報が必要な場合は、「x_authenticated_groups」ヘッダを無効にすることをお勧めします。

ICAP を設定するには

1. 配置ウィザードの [配信モード] 画面で [ICAP モード] ラジオボタンを選択します。

   詳細については、58 ページの「ICAP モード」を参照してください。
2. [次へ] をクリックします。

3. 表 2-5 の設定の推奨事項に従います。

表 2-5.　ICAP モード固有の設定

構成パラメータ	詳細	推奨値
HTTP 待機ポート番号	IWSVA が ICAP の接続の受信を待機するポートです。	1344
ICAP over SSL を有効にする	セキュアな ICAP 通信を有効 / 無効にします。	無効にする
ICAPS ポート番号	IWSVA が ICAPS の接続の受信を待機するポートです。	11344
証明書	クライアントからの SSL で保護されたリクエストに対するサーバ証明書をインポートします。	
秘密鍵	SSL で保護された通信に対する秘密鍵をインポートします。	
パスフレーズ	秘密鍵のパスフレーズを入力します。	
パスフレーズの確認	確認のためにパスフレーズをもう一度入力します。	
「X-Virus-ID」ICAP ヘッダを有効にする (チェックボックス)	検出された感染の ICAP 短縮名の記録を有効 / 無効にします。	無効にする
「X-Infection-Found」ICAP ヘッダを有効にする (チェックボックス)	検出された不正プログラムに関する ICAP 詳細と、その ICAP デバイスへの詳細の転送を有効 / 無効にします。	無効にする
「X-Authenticated-User」ICAP ヘッダを有効にする	ユーザ名情報に関する ICAP 詳細を有効 / 無効にします。	有効にする
「X-Authenticated-Groups」ICAP ヘッダを有効にする	グループメンバーシップ情報に関する ICAP 詳細を有効 / 無効にします。	無効にする

4. [次へ] をクリックします。
5. 72 ページの「ネットワークインタフェース」をセットアップし、展開を続行します。

注意： ICAP モードで配信するには、配置ウィザードのすべての手順を完了します。配信が成功したというメッセージを受信したら、84 ページの「IWSVA ICAP の設定」で示すように、IWSVA ICAP のセットアップを実行します。

ICAP over SSL を有効にして IWSVA の証明書をインポートする場合は、ICAPS クライアントで ICAP サーバ証明書の検証機能を無効にすることをお勧めします。これにより、無効なサーバ証明書の確認による ICAPS クライアントの接続エラーを回避できます。Bluecoat ProxySG など ICAP クライアントの設定の詳細については、関連するドキュメントを参照してください。

通常の透過設定

通常の透過モードでは、モード固有の設定が必要です。

通常の透過モードのモード固有の設定を行うには

1. [配信モード] 画面で [通常の透過モード] ラジオボタンを選択します。
   詳細については、60 ページの「通常の透過モード」を参照してください。
2. [次へ] をクリックします。
3. [通常の透過設定] 画面で次の設定値を入力します。(表 2-6 を参照してください)。

表 2-6. 通常の透過モード固有の設定

構成パラメータ	説明	推奨値
HTTP 待機ポート番号	IWSVA が接続の受信を待機するポートです。	80
匿名 FTP over HTTP	FTP サイトに渡されるメールアドレスです。	適切なメールアドレスを入力します。

4. [次へ] をクリックします。
5. 72 ページの「ネットワークインタフェース」をセットアップし、展開を続行します。

WCCP の設定

WCCP モードでは、モード固有の設定が必要です。

WCCP モードのモード固有の設定を行うには

1. [配信モード] 画面で [Web Cache Coordination Protocol (WCCP) モード] ラジオボタンを選択します。

   詳細については、61 ページの「Web Cache Coordination Protocol (WCCP) モード」を参照してください。
2. [次へ] をクリックします。
3. [WCCP 設定] 画面で次の設定値を入力します。(表 2-7 を参照してください)。

表 2-7.　WCCP モード固有の設定

構成パラメータ	詳細	推奨値
HTTP 待機ポート番号	IWSVA が接続の受信を待機するポートです。	80
ルータの IP アドレス	WCCP 経由で通信するルータまたはスイッチの詳細です。	ルータまたはスイッチの IP アドレスを入力します。
パスワード	WCCP 認証のパスワードです。	WCCP 認証のパスワードを入力します。
オートネゴシエート	転送方法および割り当て方法のオートネゴシエーションを提供します。	[有効にする] (初期設定) を選択します。

表 2-7. WCCP **モード固有の設定 (続き)**

構成パラメータ	詳細	推奨値
注意 : [有効にする] を選択すると、転送方法パラメータと割り当て方法パラメータは自動的に設定されるため、グレーアウトします。配置ウィザードの終了後に、自動ネゴシエートされたパラメータの値を確認するには、次の順に選択します。[管理] → [ネットワーク設定] → [WCCP] — 1 つのルートが転送方法として L2/GRE をサポートしている場合、ルータと IWSVA が同じネットワークセグメントに配置されているときは、IWSVA は L2 を選択する必要があります (これによりパフォーマンスが考慮されます)。 — 1 つのルートが転送方法として L2/GRE をサポートしている場合、ルータと IWSVA が同じネットワークセグメントに配置されていないときは、IWSVA は GRE を選択する必要があります。 — 1 つのルートが割り当て方法として HASH/MASK をサポートしている場合、IWSVA は MASK を選択する必要があります (これによりパフォーマンスが考慮されます)。		
WCCP 転送方法	WCCP 転送方法では、インターセプトされたトラフィックを WCCP サーバ (IOS) から WCCP クライアントに送信する方法を決定します。	WCCP 転送方法として、Generic Routing Encapsulation (GRE) またはレイヤ 2 (L2) を選択します。
注意 : — 初期設定の転送方法である GRE 転送では、インターセプトされたパケットを、WCCP サーバ (IOS) の発信元 IP アドレスと対象 WCCP クライアントの送信先 IP アドレスとともに IP GRE ヘッダにカプセル化します。GRE 転送にはトンネル効果があり、WCCP サーバ (IOS) を、WCCP クライアントから離れた場所にある複数レイヤ 3 のホップにすることができます。 — L2 転送では、単純に、インターセプトされたパケットの宛先 MAC アドレスを書き直し、対象 WCCP クライアントの MAC アドレスと等しくします。L2 転送では、WCCP サーバ (IOS) は WCCP クライアントに隣接するレイヤ 2 である必要があります。		

表 2-7.　WCCP モード固有の設定 (続き)

構成パラメータ	詳細	推奨値
割り当て方法	WCCP では、2 つのアルゴリズム（ハッシュテーブルとマスク / 値セット) を使用してパケット配信を行います。	WCCP 割り当て方法として、ハッシュテーブルまたはマスク / 値セットを選択します。
ハッシュ割り当ての場合、ルータは、ハッシュ機能を使用してリダイレクトするパケットのヘッダ内の値を実行します。 マスク割り当ての場合、サービスグループ内の各ルータ / スイッチに、サービスグループ内のプロキシアプライアンス全体にトラフィックを配信するために使用するマスク / 値のテーブルが存在します。		
サービスグループ	標準または動的	• **標準** — 既知のサービス (静的サービスまたは標準サービスとも呼ばれる) には、IOS と WCCPv2 クライアント両方のデバイスに認識される特性の固定セットがあります。 • **動的** — 動的サービスは、最初はサービスグループ内の WCCPv2 クライアントのみに認識されます。
注意： たとえば、Web キャッシュと呼ばれる単一の既知の （標準) サービスには、サービス ID 0 があります。このサービスは、宛先ポートが 80 のすべての TCP トラフィックをリダイレクトします。 動的サービスの特性は、最初は、サービスグループ内の WCCPv2 クライアントにのみ認識されます。サービスグループを結合するために、サービスグループの特性が、1 番目の WCCPv2 クライアントデバイスから IOS デバイスに伝えられます。		
一意のサービス ID	サービスグループの特定 初期設定 : • 標準サービス = 0 • 動的サービス = 80	範囲 : • 標準 = 0-50 • 動的 = 51-255

表 2-7.　WCCP モード固有の設定 (続き)

構成パラメータ	詳細	推奨値
匿名 FTP over HTTP	FTP サイトに渡されるメールアドレスです。	適切なメールアドレスを入力します。

4. [次へ] をクリックします。
5. 72 ページの「ネットワークインタフェース」をセットアップし、展開を続行します。

ネットワークインタフェース

すべてのモードで、関連するネットワークインタフェースが設定されている必要があります。一部のモードは、他のモードと少し異なる情報が必要になります。次の手順では、必要なさまざまな設定を取り上げています。

ネットワークインタフェース設定には、次のものがあります。

- 72 ページの「ホスト情報」
- 76 ページの「データインタフェース」
- 78 ページの「専用の管理インタフェース」
- 79 ページの「その他の設定 (IPv4 および IPv6)」

ホスト情報

すべてのモードで、ホスト情報を入力する必要があります。この手順を開始する前に、以下を確認してください。

- 配信モードを選択していること
- モード固有の設定を行っていること

ホスト情報を入力するには

1. 配置ウィザードを使用して、適切な配信モードのラジオボタンを選択し、[次へ] をクリックします。
2. モード固有の設定を指定し、[次へ] をクリックします。
3. IWSVA ホストに適用できる完全修飾ドメイン名 (FQDN) を入力します。

注意： 完全修飾ホスト名が必要です。DNS サーバに IWSVA サーバのホスト名の DNS エントリを作成することをお勧めします。

4. 73 ページの「インタフェースステータス」についてのセクションに進みます。

注意： IWSVA が正常に機能するよう、DNS サーバを使用してホスト名を解決できることを確認してください。

インタフェースステータス

IWSVA では、ネットワークポートの設定をわかりやすくするため、IWSVA サーバ上の物理 Ethernet ポートのグラフィック表示を提供します。インタフェースステータスのグラフィックは、使用可能なインタフェースのステータスと機能を示します。

74 ページの図では、インタフェースステータスのセクションでの構成に使用される Ethernet ポートのステータスと機能について説明します。

インタフェースステータスの判別

IWSVA は、すべてのタイプのハードウェアにインストールできるソフトウェア仮想アプライアンスです。したがって、IWSVA の Web UI に表示されるネットワーク情報は、IWSVA を実行するサーバにインストールされた物理ネットワークインタフェースと直接関係しない場合があります。たとえば、サーバがマザーボードにインストールされた 2 つのネットワークインタフェースを備えており、さらに使用可能なネットワークインタフェースを増やすためにサーバに追加の 4 ポート Ethernet カードがインストールされた場合、1 番目のネットワークポートが実際には新しい Ethernet カードの物理ネットワークインタフェース Eth2 にマップされていても、IWSVA Web UI では Eth0 として表示されることがあります。

物理ネットワークインタフェースに対して IWSVA Web UI ネットワークインタフェースを確実に識別するために、IWSVA には、物理ネットワークインタフェースのリアルタイムのステータスを表示するためのコマンドラインインタフェース (CLI) と配置ウィザードのインタフェースステータスのグラフィックが用意されています。

IWSVA コンソールから `show network interfaces status` CLI コマンドを使用することで、すばやく物理インタフェースのリンクステータスを確認できます。以下の例では、Eth0 と Eth1 で物理リンク接続がアップしていることを確認できます。

```
enable# show network interfaces status

Network interface link status [press 'q' to quit]:
    eth0: up
    eth1: up
_
```

図 2-9.　「show network interfaces status」CLI コマンド

図 2-10.　インタフェースステータス

図 2-10 は、配置ウィザードのインタフェースステータス情報の表示を示しています。表 2-8 は、インタフェースステータスのグラフィックで使用されるアイコンを定義しています。

表 2-8.　インタフェースステータスアイコン

表記	意味
M	管理インタフェース
D	データインタフェース
H	HA（または接続ステータス）インタフェース

表 2-8.　インタフェースステータスアイコン (続き)

表記	意味
	リンクが検出されません。ポートが空であるか、ケーブルが外れているか壊れている、またはピアコンピュータがダウンしている可能性があります。
	リンクは正常です
	リンクエラー
	リンクが無効です

インタフェースマッピングについて

インタフェースを設定または変更する前に、インタフェースを物理インタフェースにマッピングすることをお勧めします。

IWSVA を再起動した後、未使用のインタフェースの番号付けは変更される可能性がありますが、使用中のインタフェース (データ、管理、または HA 用) が変更されることはありません。

クラスタを解除する前は、インタフェースは表 2-9 のようにマップされる可能性があります。

表 2-9.　元のインタフェースマッピング

物理インタフェース	A	B	C	D
相対インタフェース	eth1	eth2	eth0	eth3
目的	D (内部)	H	D (外部)	M

クラスタの解除、クラスタの結合、または再起動後は、インタフェースマッピングは表 2-10 のように変更される可能性があります。

表 2-10.　変更されたインタフェースマッピング

物理インタフェース	A	B	C	D
相対インタフェース	eth2	eth1	eth0	eth3
目的	(内部)	(未使用)	D (外部)	M

データインタフェース

データインタフェースでは、内部ネットワークへの、または内部ネットワークからのエンドユーザのインターネットトラフィックをサポートします。次の手順を使用して、データ（ブリッジ / プロキシ) インタフェースのホスト名と IP アドレスを設定します。IPv4 アドレスと IPv6 アドレスの両方を使用できます。

警告：　データインタフェースと管理インタフェースを同じネットワークサブネットに設定しないでください。同じネットワークセグメントに設定されると、IWSVA 内部ファイアウォールにより、HTTP および FTP トラフィックが適切に転送できなくなります。

この手順を開始する前に、以下を確認してください。

- 配信モードを選択していること
- モード固有の設定を行っていること
- IWSVA のホスト情報を設定していること

データインタフェースを設定するには

1. 配置ウィザードの [ネットワークインタフェース] ページから作業を続けます。
2. データインタフェースを設定します。
   a. **透過ブリッジモード以外のすべてのモード**: [Ethernet インタフェース] ドロップダウンリストから、データインタフェースに対応する適切な Ethernet ポートを選択します。

      動的なインタフェースステータスのグラフィック画面に、選択内容が表示されます。
   b. **透過ブリッジモードと透過ブリッジモード - 高可用性のみ**: ドロップダウンリストから、内部および外部インタフェースに対応する適切な Ethernet ポートを選択します。

      インタフェースステータスのグラフィック画面に、選択内容が表示されます。
   c. ドロップダウンリストから、IP アドレスの種類を選択します。
      - **静的 IP アドレス** — インタフェースの IP アドレスを手動で設定します。
      - **DHCP から取得する** — DHCP サーバによって自動的に IP アドレスをインタフェースに割り当てます。IPv6 アドレス、ゲートウェイ、および DNS は DHCPv6 から取得できます。
   d. IP アドレスとネットマスクを入力します。
   e. [PING を有効にする] チェックボックスをオンにして、ping ユーティリティを使用して接続を確認できるようにします。
   f. (オプション) **透過ブリッジモードと透過ブリッジモード - 高可用性のみ**: VLAN ID (1-4094) を有効にするには、チェックボックスをオンにします。

      注意: HA 上位ユニットと HA 下位ユニットは、個別で一意の VLAN ID 設定値を保持します。

   g. 次のいずれかを実行します。
      - IWSVA を初めてセットアップしている場合は、配信モードの設定を続行します。または、
      - 配信モードのセットアップが終了し、データインタフェースを変更するだけの場合は、[次へ] をクリックして残りの画面をクリックスルーします。

3. 必要に応じて、データインタフェースアクセス管理リストを設定します。148 ページの「インターネットアクセス管理の設定」を参照してください。
4. 78 ページの「専用の管理インタフェース」についてのセクションに進みます。

専用の管理インタフェース

専用の管理インタフェースでは、管理者は、Web コンソールまたは SSH のいずれかを介して IWSVA デバイスにログインするための独立したインタフェースを使用できます。

専用の管理インタフェースを有効化または無効化するには、配置ウィザードの [ネットワーク設定] 画面で値を設定し、その値を有効にします。IPv4 アドレスと IPv6 アドレスの両方を使用できます。

注意： 専用の管理インタフェースは高可用性環境に対応可能である必要があります。

この手順を開始する前に、以下を確認してください。

- 配信モードを選択していること
- モード固有の設定を行っていること
- IWSVA のホスト情報を設定していること
- データインタフェース情報を設定していること

専用の管理インタフェースを設定するには

1. 配置ウィザードの [ネットワークインタフェース] ページから作業を続けます。
2. [管理インタフェースを有効にする] チェックボックスをオンにします。
3. ドロップダウンリストから Ethernet インタフェースを選択します。
4. 管理インタフェースデバイスの静的な IP アドレスを入力します。
5. 管理インタフェースデバイスのネットマスクを入力します。
6. [PING を有効にする] チェックボックスをオンにして、ping ユーティリティを使用して接続を確認できるようにします。
7. 次のいずれかを実行します。
   - IWSVA を初めてセットアップしている場合は、配信モードの設定を続行します。または、
   - 配信モードのセットアップが終了し、専用の管理インタフェースを追加するだけの場合は、[次へ] をクリックして残りの画面をクリックスルーします。

その他の設定 (IPv4 および IPv6)

[その他の設定] (IPv4 および IPv6) では、DHCP から動的情報を取得したり、次の静的情報を入力したりすることができます。

- ゲートウェイの IP アドレス
- プライマリ DNS サーバの IP アドレス
- セカンダリ DNS サーバの IP アドレス

この手順を開始する前に、以下を確認してください。

- 配信モードを選択していること
- モード固有の設定を行っていること
- IWSVA のホスト情報を設定していること
- データおよび管理インタフェースの情報を設定していること

その他の設定を行うには

1. 配置ウィザードの [ネットワークインタフェース] ページから作業を続けます。
2. [その他の設定] までスクロールします。
3. 次のいずれかを実行します。
   - [DHCP から取得する] チェックボックスをオンにし、IWSVA が動的ゲートウェイ、プライマリ DNS、およびセカンダリ DNS の情報を取得するようにします。あるいは、
   - 静的なゲートウェイ、プライマリ DNS、およびセカンダリ DNS の場合は、その情報を入力します。

表 2-11. その他の設定の情報

パラメータ	説明
ゲートウェイ	ネットワークデバイスの静的な IP アドレス設定については、この IWSVA インストールでゲートウェイとして使用される適切な (IPv4 または IPv6 の) IP アドレスを入力します。
プライマリ DNS	ネットワークデバイスの静的な IP アドレス設定については、この IWSVA インストールでプライマリ DNS サーバとして使用される適切な IP アドレスを入力します。
セカンダリ DNS	ネットワークデバイスの静的な IP アドレス設定については、この IWSVA インストールでセカンダリ DNS サーバとして使用される適切な IP アドレスを入力します。

4. [次へ] をクリックします。
5. 80 ページの「静的ルート」についてのセクションに進みます。

静的ルート

IWSVA は、静的ルートを使用して、IWSVA が接続するルータのネクストホップの範囲外にあるネットワークセグメントとのトラフィックのルーティング問題を解決できます。静的ルートを使用すると、インターネットにトラフィックを送信したり、エンドユーザにトラフィックを戻したりするために使用されるルータ接続を手動で管理できます。

たとえば、IWSVA がさまざまなルータを介して内部のアップデート (AU) サーバでパターンを更新する場合、静的ルートを AU サーバに追加する必要があります。

注意： 静的ルートをインタフェースにバインドする場合、ルータポートはインタフェースと同じネットワークセグメントに配置されている必要があります。

この手順を開始する前に、以下を確認してください。

- 配信モードを選択していること
- モード固有の設定を行っていること
- ネットワークインタフェース情報を設定していること

静的ルートを設定するには

1. 配置ウィザードの [静的ルート] 画面から [設定] に移動し、以下を設定します。
   - ネットワーク ID
   - ネットマスク
   - ルータ
   - インタフェース

注意： これらの静的ルートに IPv6 ルートを追加することもできます。

---

2. [リストに追加] をクリックします。
   静的ルートが [静的ルート] リストに表示されます。
3. その他の静的ルートを追加します。
4. [次へ] をクリックします。

5. 81 ページの「製品のアクティベーション」に進みます。

製品のアクティベーション

配信中に実行される登録プロセスが完了したら、ソフトウェアをアクティベート (有効化) する必要があります。有効なアクティベーションコードが入力されていないと、トレンドマイクロ製品はトラフィック検索やポリシー設定の適用を行いません。

アクティベーションコードを受け取るには、トレンドマイクロ製品登録サーバでレジストレーションキーを入力する必要があります。

IWSVA をアクティベートするには

1. 配置ウィザードの [製品のアクティベーション] 画面に移動します。
2. IWSVA のアクティベーションコードを入力します。
3. [次へ] をクリックします。
4. 82 ページの「システム時間の設定」に進みます。

注意： サポート契約の更新については、トレンドマイクロの営業担当または販売代理店にお問い合わせください。[管理] → [製品ライセンス] で [ステータス更新] をクリックし、[製品ライセンス] 画面でサポート契約の有効期限を手動で更新します。

アクティベーションコードについて

検索と製品のアップデートを有効にするには、アクティベーションコードが必要です。インストール時に IWSVA のアクティベーションを実行しなかった場合は、インストール後に実行できます。インストール時に IWSVA を登録して、アクティベーションコードを受け取ります。

注意： IWSVA の登録後に、メールでアクティベーションコードを受け取ります。アクティベーションコードは 31 文字 (ハイフン含む) で次の形式です。

```
xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
```

この手順を開始する前に、以下を確認してください。

- 配信モードを選択していること

- モード固有の設定を行っていること
- ネットワークインタフェース情報を設定していること
- 静的ルートを設定していること

IWSVA をアクティベートするには

1. 配置ウィザードの [製品のアクティベーション] 画面に移動します。
2. IWSVA のアクティベーションコードを入力します。
3. [次へ] をクリックします。
4. 82 ページの「システム時間の設定」に進みます。

システム時間の設定

[システム時間] と [タイムゾーン] の設定では、以下を行うことができます。

- 現在のシステム時間を使用する
- NTP サーバと同期する
- 日付と時間を手動で入力する
- タイムゾーンを選択する

この手順を開始する前に、以下を確認してください。

- 配信モードを選択していること
- モード固有の設定を行っていること
- ネットワークインタフェース情報を設定していること
- 静的ルートを設定していること
- 製品のアクティベーション情報を入力していること

システム時間とタイムゾーンを設定するには

1. 配置ウィザードの [システム時間] 画面にアクセスします。
2. 次のオプションのいずれかを選択します。
   - 現在のシステム時間 — システムで設定済みの時間を維持します
   - NTP サーバと同期する (IPv4 サーバと IPv6 サーバの両方がサポートされます) -
   - 手動 - 時間と日付を手動で設定します
3. 適切なタイムゾーンを設定します。
   - ドロップダウンリストから、システムが配置されている地域を選択します。

- ドロップダウンリストから、システムが配置されている市 (または自分の所在地と同じ時間の近隣の市) を選択します。

4. [次へ] をクリックします。

結果

結果ページでは、設定が正しく入力されたかどうかや、IWSVA の配信が完了したことを確認できます。また、設定が受け入れられなかったかどうかもわかります。

配信設定は入力時にシステムによってチェックされ、ユーザはチェック後に配置ウィザードの次の画面に移動します。通常、設定は正しく入力されています。

配信ステータス

IWSVA の展開が成功すると、モード設定の配信状況を反映するステータスバーとともに次のメッセージが表示されます。

「おめでとうございます !IWSVA の設定と配信が完了しました。

間もなく、IWSVA の Web コンソールの IP アドレスにリダイレクトされます。新しい設定変更が適用されシステムの再起動後にログイン可能になるまで、数分かかる場合があります。」

注意： このメッセージが表示されたら、ただちに最新のソフトウェア /OS のアップデートを IWSVA に適用することをお勧めします。詳細については、第 4 章の 115 ページの「アップデート」を参照してください。

配信が成功した場合でも、Web コンソールへのアクセスエラーを示すメッセージが表示される場合があります。メッセージには、問題の修正方法に関する推奨事項が含まれています。次の例を参照してください。

「DHCP プロトコルを指定して IWSVA ネットワークインタフェースを設定したため、展開ウィザードは Web コンソールの IP アドレスを自動的に検出できません。IP アドレスとポート番号は、IWSVA サーバ表示から取得できます。」

配信後

配置ウィザードが正しく設定されると、IWSVA は自動的に再起動します。コンピュータの再起動時に、IPv6 アドレスが設定されている場合は、IPv4 と IPv6 の URL が含まれるすべてのアクセスアドレスが CLI シェルログインページに表示されます。

IWSVA で IPv6 アドレスを設定している場合は、インストールプロセスで設定された IP アドレス (IPv4 または IPv6 アドレス) を使用して Web コンソールにアクセスできます。IWSVA の再起動後は、可能なかぎり早く IWSVA をアップデートすることをお勧めします。詳細については、115 ページの「アップデート」を参照してください。

さらに、

- ICAP モードで配信した場合は、IWSVA と連携する ICAP 対応キャッシュサーバの設定の詳細について 84 ページの「IWSVA ICAP の設定」を参照してください。
- インストールを検証するための手順を追ったプロセスについては、401 ページの「IWSVA のテストと設定」を参照してください。

IWSVA ICAP の設定

ICAP ハンドラとともに IWSVA を実行する場合、次の設定手順に従います。

1. 84 ページの「ICAP 1.0 対応キャッシュサーバの設定」
2. 90 ページの「キャッシュされた既存のコンテンツをアプライアンスから消去」

注意： 次の ICAP の設定手順は、37 ページの「X-Authenticated ICAP ヘッダのサポート」で一覧表示されている ICAP バージョンに適用されます。これらは参考までに提供されているため、詳細については、本来のドキュメントを参照してください。

ICAP 1.0 対応キャッシュサーバの設定

ICAP サーバと通信するように ICAP クライアント (Network Appliance Blue Coat Port 80 Security Appliance キャッシュサーバ /Cisco ICAP サーバなど) を設定します。

使用する ICAP クライアントに対応するプロセスを参照してください。

- 85 ページの「Blue Coat Port 80 Security Appliance の ICAP を設定するには」
- 87 ページの「Cisco CE ICAP サーバを設定するには」

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 `https://{` **サーバ** `IP` **アドレス** `}:8082` と入力し、Web コンソールにログオンします。

注意： Blue Coat アプライアンスに ICAP を設定する手順は、製品のバージョンによって異なる場合があります。

---

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. 左のメニューから [ICAP] をクリックし、[ICAP Services] タブをクリックします。
4. [New] をクリックします。
   [Add ICAP Service] 画面が開きます。
5. [ICAP service name] に英数字で名前を入力します。[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 name] 画面が開きます。
7. 次の情報を入力または選択します。
   a. ICAP のバージョン番号 (つまり、1.0)
   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。初期設定の ICAP ポートは 1344 です。
      - 応答モード :

      `icap://{ICAP` **サーバの** `IP` **アドレス** `}:1344`
      - 要求モード :

      `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. 接続のタイムアウト。これは、Blue Coat Port 80 Security Appliance がウイルス検索サーバからの応答を待つ秒数です。範囲は、60 ～ 65,535 の間隔です。初期設定のタイムアウトは 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のゼロ (0) 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、[Apply] をクリックします。

注意： 設定した ICAP サービスを編集することができます。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。

9. 応答または要求モードポリシーを追加します。

   Visual Policy Manager には、Sun Microsystems 社の Java 2 Runtime Environment Standard Edition のバージョン 1.3.1 以降 (別称 : Java Runtime、JRE) が必要です。ワークステーションにすでに JRE がインストールされている場合、Security Gateway は別のブラウザウィンドウを開いて Visual Policy Manager を起動します。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 がインストールされていない場合、セキュリティの警告ウィンドウが開きます。作業を続行するには、[Yes] をクリックします。指示に従います。

応答モードポリシーを追加するには

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 [Policy] をクリックし、[Visual Policy Manager] タブをクリックします。
3. [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。
4. メニューバーで [Edit] → [Add Web Content Policy] の順に選択します。[Add New Policy Table] 画面が開きます。
5. [Select policy table name] にポリシー名を入力します。[OK] をクリックします。
6. [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] 画面が開きます。[New] をクリックし、[Use ICAP Response Service] を選択します。[Add ICAP Service Action] 画面が開きます。
7. [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、再度 [OK] をクリックします。
8. [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

1. 前の手順のステップ 1 〜ステップ 5 に従います。
2. [Action] 列で [Deny] を右クリックし、[Set] をクリックします。[Add Object] 画面が開きます。[New] をクリックし、[Use ICAP Request Service] を選択します。[Add ICAP Service Action] 画面が開きます。
3. [ICAP Service/Cluster Names] で ICAP サービス名を選択します。
4. [On communication error with ICAP service] で [Deny the request] を有効にします。
5. [OK] をクリックし、再度 [OK] をクリックします。
6. [Install Policies] をクリックします。
7. 要求 ICAP モードサービスと応答 ICAP モードサービスの両方を設定します。

   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。

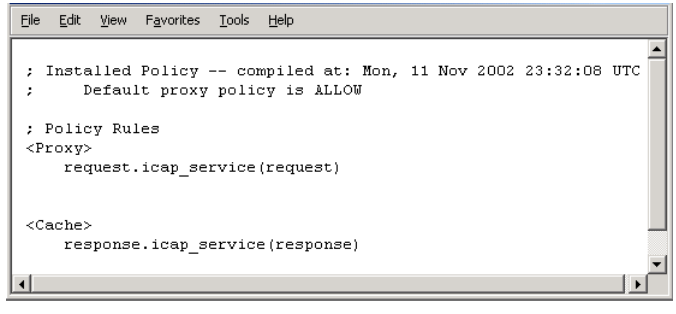


図 2-11. [Install Policies] **画面**

Cisco CE ICAP サーバを設定するには

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。

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 関連のすべてのコマンドのリストを表示するには、「**icap?**」と入力します。
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 RESPMOD SERVICE NAME
   ```

これにより ICAP サービス設定メニューに移動します。使用可能なすべてのコマンドのリストを表示するには、「**?**」と入力します。次のコマンドを入力します。

server icap://ICAP SERVER IP:1344/resp（サーバの種類を割り当てる）

vector-point respmod-precache（適切なベクタポイントの種類を割り当てる）

error-handling return-error（適切なエラー処理の種類を割り当てる）

enable（ICAP 複数サーバ設定を有効にする）

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 REQUESTMOD SERVICE NAME`

   このコマンドにより ICAP サービス設定メニューに移動します。利用できるすべてのコマンドのリストを表示するには、「**?**」と入力します。次のコマンドを発行します。

   server icap://ICAP SERVER IP:1344/REQ-Service（サーバの種類を割り当てる）

   vector-point reqmod-precache（適切なベクタポイントの種類を割り当てる）

   error-handling return-error（適切なエラー処理の種類を割り当てる）

   enable（ICAP 複数サーバ設定を有効にする）
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 サーバヘッダを有効にする）

   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 検索からストリーミングメディアを除外する）

   icap apply all（すべての設定を適用して ICAP の種類をアクティベートする）

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

ウイルス検索サーバクラスタの設定

複数のウイルス検索サーバと連携する Blue Coat Port 80 Security Appliance については、Security Gateway でクラスタを設定します（クラスタを追加してから、関連する ICAP サービスをクラスタに追加）。

Web コンソールで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] 画面が開きます。
4. [ICAP cluster name] に英数字で名前を入力し [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] 画面が開きます。
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] 画面が開きます。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のリストが含まれます。
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 name] 画面が開きます。
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、再度 [OK] をクリックしてから、[Apply] をクリックします。

クラスタの設定またはエントリの削除

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 ポリシーで使用されるクラスタは、ポリシーのルールがクラスタ名を使用する場合、削除しないでください。

Web コンソールでクラスタの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. 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] をクリックして確認します。

キャッシュされた既存のコンテンツをアプライアンスから消去

IWSVA ICAP が HTTP トラフィックの検索を開始する前に、Blue Coat Port 80 Security Appliance または Cisco ICAP サーバにキャッシュされたコンテンツから感染する危険性があります。この危険性に対処するには、IWSVA ICAP の設定後にすぐにキャッシュを消去することをお勧めします。Web コンテンツに対するすべての新しい要求はインターネットで対応され、キャッシュ前に IWSVA ICAP により検索されます。検索されたコンテンツは、Blue Coat Port 80 Security Appliance または Cisco ICAP サーバにキャッシュされます。Blue Coat Port 80 Security Appliance または Cisco ICAP サーバは、ネットワークユーザによる同じ Web コンテンツへの以降の要求に対応します。要求がインターネットに送信されないので、ダウンロードする時間は速くなります。

Blue Coat Port 80 Security Appliance 内のキャッシュを消去するには

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. [Maintenance] をクリックします。
3. [Tasks] タブをクリックし、[Clear] をクリックします。[OK] をクリックして確認します。

Cisco ICAP サーバのキャッシュを消去するには

1. Telnet で Cisco CE に接続します。
2. ルート CLI メニューで「cache clear」と入力します。
3. <Enter> キーを押します。

IWSVA が ICAP 要求を待機していることを確認する

IWSVA が正しいポートで待機していることを確認するには、PuTTY を使用して、admin ユーザとして SSH を介して IWSVA にアクセスします。

admin ユーザとしてログインしたら、CLI コマンド「show network connections all」を発行して、IWSVA を介したすべてのアクティブなネットワーク接続を表示します。これで、TCP ポートのアクセスがポート 1344 で有効になっていることを確認できます。

コマンドと出力の例 :

```
enable# show network connections all
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address             Foreign Address           State
tcp        0      0 0.0.0.0:9091                0.0.0.0:* LISTEN
tcp        0      0 127.0.0.1:8005              0.0.0.0:* LISTEN
tcp        0      0 0.0.0.0:1812                0.0.0.0:* LISTEN
```

```
tcp        0      0 0.0.0.0:22                  0.0.0.0:* LISTEN
tcp        0      0 0.0.0.0:5432                0.0.0.0:* LISTEN
tcp        0      0 10.204.170.156:22           10.204.170.158:2665 ESTABLISHED
udp        0      0 0.0.0.0:514                 0.0.0.0:*
udp        0      0 0.0.0.0:21273               0.0.0.0:*
udp        0      0 0.0.0.0:35739               0.0.0.0:*
udp        0      0 0.0.0.0:7068                0.0.0.0:*
udp        0      0 0.0.0.0:17437               0.0.0.0:*
udp        0      0 0.0.0.0:22688               0.0.0.0:*
udp        0      0 0.0.0.0:9911                0.0.0.0:*
udp        0      0 0.0.0.0:30138               0.0.0.0:*
udp        0      0 0.0.0.0:60733               0.0.0.0:*
udp        0      0 127.0.0.1:9925              127.0.0.1:9925
ESTABLISHED
udp        0      0 0.0.0.0:36946               0.0.0.0:*
udp        0      0 0.0.0.0:41560               0.0.0.0:*
udp        0      0 0.0.0.0:29294               0.0.0.0:*
udp        0      0 0.0.0.0:12655               0.0.0.0:*
udp        0      0 0.0.0.0:38390               0.0.0.0:*
udp        0      0 0.0.0.0:7036                0.0.0.0:*

Active UNIX domain sockets (servers and established)
Proto RefCnt Flags Type State    I-Node    Path
unix  2   [ ACC ] STREAM  LISTENING6643358 /tmp/ssh-ddgvf12499/agent.12499
unix  2   [ ACC ] STREAM LISTENING634599  /var/run/nscd/socket
unix  2   [ ACC ] STREAM LISTENING  7249  /var/run/dbus/system_bus_socket
unix  2   [ ACC ] STREAM LISTENING  7368  @/var/run/hald/dbus-uIGJbIMMam
unix  2[ ]        DGRAM             6421523 /tmp/tmsyslog
unix  2   [ ]     DGRAM             6421525 /tmp/log
unix  2   [ ACC ] STREAM LISTENING  3065236/tmp/.s.PGSQL.5432
unix  2   [ ]     DGRAM             1274  @/org/kernel/udev/udevd
unix  2   [ ]     DGRAM             7379 @/org/freedesktop/hal/udev_event
unix  2   [ ACC ] STREAM LISTENING  7369 @/var/run/hald/dbus-0oDgnh6zwa
unix  5   [ ]     DGRAM             6430159 /dev/log
unix  2   [ ]     DGRAM             6643350
unix  2   [ ]     DGRAM             6603791
unix  2   [ ]     DGRAM             6430163
unix  2   [ ]     DGRAM             065234
unix  3   [ ]     STREAM CONNECTED  8017 /var/run/dbus/system_bus_socket
unix  3   [ ]     STREAM CONNECTED  8016
unix  3   [ ]     STREAM CONNECTED  8003 @/var/run/hald/dbus-uIGJbIMMam
```

```
unix  3   [ ]     STREAM CONNECTED  8002
unix  3   [ ]     STREAM CONNECTED  7872 @/var/run/hald/dbus-uIGJbIMMam
unix  3   [ ]     STREAM CONNECTED  7870
unix  3   [ ]     STREAM CONNECTED  7835 @/var/run/hald/dbus-uIGJbIMMam
unix  3   [ ]     STREAM CONNECTED  7834
unix  3   [ ]     STREAM CONNECTED  7372 @/var/run/hald/dbus-0oDgnh6zwa
unix  3   [ ]     STREAM CONNECTED  7371
unix  3   [ ]     STREAM CONNECTED  7257
unix  3   [ ]     STREAM CONNECTED  7256
    enable#
```

要求モードと応答モードの違いについて

ICAP **要求モード** : 新しい要求を受信すると、有効なアクセス要求であることを確認するために、その要求が検索サーバに送信されます。

ICAP **応答モード** : 新しい要求が有効な場合、返されるコンテンツがすべて検索されます。

1 つの検索ベクトルのみを使用することもできますが、この場合、すべての適切なトラフィックを検索する機能が 50% 低下します。

要求モード処理をトリガする

次に示す手順は、特に IWSVA を介した要求モード処理のトリガに適用されます。

1. IWSVA にトラフィックを渡すクライアントにログインします。
2. Web ブラウザを開き、要求を行うサイトにアクセスします。

アウトバウンド URL は、InterScan Web Security Suite に渡されブロックされます。ダメージクリーンナップサービスが自動クリーンナップを実行するように設定されていると、ワークステーションでもこれに対して自動的に修正処理が実行されます。

応答モード処理をトリガする

次に示す手順は、特に IWSVA を介した応答モード処理のトリガに適用されます。

1. IWSVA にトラフィックを渡すクライアントにログインします。
2. Web ブラウザを開き、サイト www.eicar.org を開きます。
3. [AntiMalware Testfile] と表示されたボタンをクリックします。

4. ページの一番下までスクロールすると、[Download area using the standard protocol http] と書かれた場所にテストファイルが表示されています。
5. eicar.com.txt ファイルを選択してダウンロードします。

アウトバンド URL が有効なので、要求モードではこの URL は通過できます。トラフィックの応答 — 実際にダウンロードしようとすると InterScan Web Security でダウンロードの実行がブロックされます。

第 3 章

透過ブリッジモードの高可用性とクラスタ管理

本章では、高可用性が透過ブリッジモードでどのように機能するかと、クラスタ管理インタフェースの使用方法について説明します。

本章で説明する内容には、次の項目が含まれます。

高可用性の概要

IWSVA は、透過ブリッジモードで配信されるアクティブ / パッシブペアを使用したビジネスの継続性を確保するために、ネイティブの高可用性 (HA) を提供します。

注意： 現在、IWSVA 高可用性 (HA) ソリューションは、高可用性向け「透過ブリッジモード」のアクティブ / パッシブペアのみをサポートしています。1 つの HA クラスタ内で 2 つの HA のみがサポートされます。サポートされる別の配信モードで配信された複数の IWSVA 間の冗長性は、IWSVA に対して外部的に処理されます。特に、ロードバランサはプロキシモードのいずれにおいても冗長性をサポートします。Cisco WCCP デバイスは、WCCP モードの冗長化 IWSVA に対するトラフィックを管理できます。ICAP クライアントは、ICAP モードの冗長化 IWSVA に対するトラフィックを管理できます。

HA クラスタメンバーを説明する 4 つの用語を以下に示します。

- **アクティブメンバー** — リアルタイムのコンテンツ検索を提供する IWSVA です。
- **パッシブメンバー** — パッシブのスタンバイモードの IWSVA です。
- **上位メンバー** — すべての設定変更を受け入れ、ポリシーと設定を下位メンバーと同期する IWSVA です。
- **下位メンバー** — ポリシーと設定変更をバックグラウンドで受け取る IWSVA です。

HA スイッチオーバは自動 (フェイルオーバ) または手動のどちらでも実行できます。

フェイルオーバの場合

- IWSVA の HA サービスは、IWSVA アプリケーションの主要なサービスと基礎となる OS でエラーがないかどうかを監視します。アクティブユニット上で異常が発生すると、HA サービスはアクティブノードからパッシブノードに自動的に切り替えます。
- ノードの結合や上位ノードのシャットダウンなど、管理者が行う HA 管理操作の一部は、自動スイッチオーバをトリガできます。HA はこのタイプのスイッチオーバをグレースフルに、また自動的に処理します。

手動スイッチオーバの場合

- 管理者は上位ノードの Web コンソールを使用して、HA スイッチオーバを手動で強制できます。

注意： 1) HA では、STP （スパニングツリープロトコル) を有効にする必要があります。これにより、ネットワーク内でレイヤ 2 ループの発生を防止できます。
2) HA ソリューションで使用されるスイッチが RSTP (高速スパニングツリープロトコル) をサポートする場合、より高速の切り替えを可能にするために IWSVA 上で STP を無効にすることが必要になります。
3) STP/RSTP を有効にするには、両方のスイッチで PortFast ブリッジプロトコルデータユニット （BPDU) ガードを無効にする必要があります。これは、BPDU がスイッチ上のポートを無効にし、HA の動作を妨げるためです。

アクティブ / パッシブペアについて

アクティブ / パッシブペアは、直接接続することも、専用スイッチを介して接続することもできます。アクティブ / パッシブペアを適切に設定するには、2 つのプライベート IP アドレスとプライベートの予約されたサブネットが必要です。これらのプライベート IP アドレスは、HA 機能の内部使用のために予約され、HA 接続ステータス信号情報とデータ同期のために使用されます。このプライベートサブネット上でユーザデバイスの使用は許可されません。

IWSVA では、アクティブ / パッシブペアにクラスタ IP アドレスを使用します。これは HA クラスタを管理するために使用されます。このクラスタ管理 IP アドレスは 2 つの HA ユニット間を浮動し、常に HA ペアのアクティブなメンバーと関連付けられます。

アクティブノードは HTTP、HTTPS、および FTP トラフィックを検索します。パッシブノードはスタンバイデバイスとして機能し、通常の状態ではトラフィックを検索しません。次に挙げるような異常な事態が発生すると、パッシブノードはアクティブノードになります。

- データリンク障害
- OS カーネルパニック
- IWSVA アプリケーションの重要なサービスの失敗

IWSVA では、接続ステータス信号のダウン、アプリケーションのダウン、またはシステムのダウン状態によりアクティブなユニットがダウンすると、フェイルオーバがトリガされます。ダウンしたユニットがオンラインに戻ると、ユーザ定義の選択ポリシーによりどのユニットが次にアクティブなユニットとなるかが決定されます。管理者は、パッシブユニットがアクティブユニットとしてとどまるように選択ポリシーを設定するか （通常モード)、またはノードの重み付けによって選択ポリシーを設定して、特定の HA メンバーが常にアクティブユニットとして制御を再取得できるようにすることもできます。

HA エージェントがステータス変更を処理

初期設定では、クラスタに 1 番目のメンバーとして参加する IWSVA デバイスがアクティブな上位ノードになります。

[重み付けされた優先順位の選択] 機能が無効になっている場合、初期設定では、既存のクラスタに参加する 2 番目の IWSVA デバイスがパッシブな下位ノードになります。

[重み付けされた優先順位の選択] 機能が有効になっており、2 番目の IWSVA デバイスが、1 番目のクラスタメンバーより高い重みを持つ既存のクラスタに参加している場合は、その重み値が高い 2 番目のマシンがアクティブな上位メンバーとなり、元のメンバーはパッシブな下位メンバーになります。

フェイルオーバとスイッチオーバ

フェイルオーバは、アクティブノードがクラッシュするか、トラフィックを通常どおり処理できなくなった場合に生じます。IWSVA は自動的にクラスタ内のパッシブのスタンバイマシンに切り替え、その新しいマシンがアクティブメンバーになるよう選択します。

スイッチオーバは、上位の Web 管理インタフェースで手動による役割の変更が強制されたときに発生します。これにより、元の下位 / パッシブユニットが、新しい上位 / アクティブユニットになります。

HA エージェントとインタフェース

HA エージェントは、以下の管理機能を使用して設定できます。

- 98 ページの「配置ウィザードについて」
- 99 ページの「アプリケーションの状態監視について」
- 100 ページの「一元管理について」
- 104 ページの「クラスタ管理について」

配置ウィザードについて

配置ウィザードを使用して、次の操作にアクセスします。

- 99 ページの「クラスタの作成」
- 99 ページの「クラスタの結合」

注意： 配置ウィザードの使用の詳細については、第 2 章「配置ウィザード」を参照してください。

クラスタの作成

新しい HA クラスタは、配置ウィザードインタフェースで作成されます。新しい HA クラスタが作成されると、管理システムは望ましいポリシー設定で HA エージェントを構成し、上位メンバーに格納します。上位メンバーは、アクティブに構成できる唯一のユニットです。下位メンバーは、上位メンバーからアップデートを定期的に受信し、最新の構成情報およびポリシー情報との同期を維持します。クラスタを作成するには、54 ページの「新規クラスタの作成」のステップバイステップの手順を確認してください。

注意： HA クラスタの IP アドレスは IPv6 アドレスをサポートしません。

クラスタの結合

HA メンバーが HA クラスタに追加されると、配置ウィザードは各メンバーを取り込み、適切なネットワーク情報と重み付け情報を使用して各メンバーを設定し、上位メンバーと下位メンバーをセットアップします。

重みの高いメンバーは上位メンバーになります。これにより、主要なアクティブユニットになるコンピュータを手動で選択できます。

HA エージェントは、クラスタメンバー間の情報の同期と、フェールオーバーまたはスイッチオーバーの開始を担います。

55 ページの「既存クラスタの結合」のステップバイステップの手順を確認してください。

アプリケーションの状態監視について

アプリケーションの状態監視は、IWSVA アプリケーションと OS の状態を監視する別個のサービスです。このサービスはまた、HA エージェント間とすべての必要な情報をやり取りすることにより、アクティブメンバーとパッシブメンバー間でフェイルオーバが迅速に行われるようにします。

リンクロスの検出

上位ノードは、レイヤ 2 スイッチ接続でエラーがないかどうかを監視します。データポートでネットワーク接続が失われると、スイッチオーバが自動的に生成され、パッシブのスタンバイメンバーに迅速なフェイルオーバが行われます。

`linkloss_timeout` パラメータは、リンクロスの検出に使用されるダウンタイムの長さを制御します。linkloss_timeout パラメータに設定されたタイマーの値に到達すると、フェイルオーバプロセスが開始されます。

状態監視設定ファイルを使用して、`linkloss_timeout` 値を設定できます。初期設定は 2 秒です。この値は、状態監視設定ファイルの次の場所に見つかります。`/etc/iscan/intscan.ini`

```
[health-monitor]
linkloss_timeout=2
```

ファイルを変更したら、次のコマンドを使用して `svcmonitor` サービスを再起動します。

```
/etc/iscan/S99ISsvcmonitor restart
```

注意： IWSVA では、ベアメタル環境のリンクロスを検出できます。

一元管理について

一元管理機能は、2 つの HA ノードを単一のデバイスとして管理するために使用されます。これにより、上位ユニットで行われる設定変更が、下位ユニットで自動的に同期されるようになります。

注意： 一元管理はアクティブ / パッシブペアシナリオにのみ適用されます。単一のデバイスには使用できません。

一元管理では、上位メンバーと下位メンバー間で 5 分ごとに設定情報が自動的に同期されます。管理者は、上位ノードからアクセスできる IWSVA Web コンソールの [システムステータス] 画面のタイトルバーにある [同期] ボタンをクリックすることによって、手動で同期をトリガすることもできます。

IWSVA では、次の 2 つの同期メカニズムをサポートしています。

- **自動同期** — 上位ノードは 5 分ごとに予約タスクを実行して、ポリシーと設定を下位ノードに同期します。

- **手動同期** — ユーザは、上位ノードの Web コンソールの [管理] → [一般設定] → [クラスタ管理] 画面にある [同期] ボタンをクリックすることで同期を強制できます。

2 つのノード上の設定が同期されていない場合、ユーザは手動スイッチオーバを実行できません。設定が同期されていない場合にスイッチオーバを試行すると、2 つのメンバーをまず手動で同期するように指示する警告メッセージが表示されます。

自動フェイルオーバの場合、スイッチオーバは同期を強制することなく即座に実行されます。最後に完了した同期以降に加えられた設定変更は失われます。

ノードの手動同期

上位メンバーから下位メンバーへの同期は、5 分ごとに行われます。管理者は [クラスタ管理] 画面から、クラスタメンバー間の即座の同期を手動でトリガできます。

2 つのノードを手動で同期するには

1. 上位メンバーの Web コンソールで [システムステータス] 画面に移動します。
2. [システムステータス] 画面の上部にある [同期] をクリックします。
3. 上位メンバーから下位メンバーにポリシーと配信設定をただちに同期するには、確認画面で [OK] をクリックします。

一元管理される機能と分散管理される機能

クラスタレベル - 設定は一元管理され、上位ノードでのみ表示および指定可能で、上位ノードから下位ノードに同期されます。

インスタンスレベル - 設定は分散管理され、上位ノードと下位ノードで異なる場合があり、上位ノードまたは下位ノードに個別に指定できます。

機能には一元的に管理されるものがありますが、管理者が上位ノードまたは下位ノードの Web コンソールにログインする必要がある機能もあります。詳細については、表 3-1 を参照してください。

表 3-1. 一元管理される機能と分散管理される機能

上位ノードから一元管理される クラスタレベルの設定	上位ノードまたは下位ノードから 分散管理されるインスタンスレベルの設定
HTTP/HTTPS/FTP トラフィックの有効化 / 無効化	• ダッシュボード / ウイルス / 不正プログラム /URL/ スパイウェア / 概要レポート

表 3-1. 一元管理される機能と分散管理される機能 (続き)

上位ノードから一元管理される クラスタレベルの設定	上位ノードまたは下位ノードから 分散管理されるインスタンスレベルの設定
すべての HTTP/HTTPS ポリシーおよび設定 ([HTTP/HTTPS] セクション) ・ HTTPS 証明書を含む	レポート (機能とデータ) ・ レポートテンプレート ・ 手動レポートのデータ ・ 予約レポートのデータ
すべての FTP ポリシーおよび設定 ([FTP] セクション)	ログ (機能とデータ) ・ ログ分析
レポートの設定 ・ レポートテンプレート	アップデート (手動アップデート)
ログ設定 ・ Syslog 設定 ・ ログ設定	データベース接続のテスト機能 ([管理] → [一般設定] → [データベース接続])
アップデート設定 ・ 予約アップデートの設定 ・ 接続設定	データポートおよび管理ポートのインタフェース設定 ・ ホスト名 ・ IP アドレスとネットマスク ・ データインタフェースまたは管理インタフェースのポート
通知先の設定 ・ [通知] 画面 ・ [システムステータス] 画面の [しきい値アラート設定] ・ SMTP 設定 ・ [管理] → [ネットワーク設定] → [SNMP の設定] 下の SNMP 設定	Control Manager の登録
隔離管理 ([管理] → [一般設定] → [隔離管理])	システムパッチ
システム時間	OS のアップデート

表 3-1.　一元管理される機能と分散管理される機能 (続き)

上位ノードから一元管理される クラスタレベルの設定	上位ノードまたは下位ノードから 分散管理されるインスタンスレベルの設定
ネットワーク設定 (ホスト名、IP、ネットマスク、およびポートは除く) ・ 各インタフェースでの [PING を有効にする] ・ DNS ・ 初期設定ゲートウェイ ・ 静的ルート **注意：** DHCP は HA では解除されます。	サポート情報
Web コンソール設定 ([管理] → [ネットワーク設定] → [Web コンソール])	
リモート CLI 設定 ([管理] → [ネットワーク設定] → [リモート CLI])	
ユーザアカウント ([管理])	
設定のバックアップと復元	
製品ライセンス	
配置ウィザードの設定	
システム時間 配信モード 静的ルート データインタフェースと管理インタフェース ・ DNS ・ 初期設定ゲートウェイ ・ 静的ルータ ・ PING を有効にする	データインタフェースと管理インタフェース ・ ホスト名 ・ IP アドレスとネットマスク ・ ポート番号

クラスタ管理について

[クラスタ管理] 画面は、[管理] → [一般設定] → [クラスタ管理] からアクセスでき、HA クラスタを設定するために使用します。クラスタ設定はクラスタ設定ファイル内に保存され、一元管理機能と HA エージェントによって HA ポリシーとフェイルオーバの優先順位を作成するために使用されます。クラスタメンバーの重みの値を変更すると、手動で上位 / アクティブメンバーを選択できますが、スイッチオーバが発生する可能性もあります。詳細については、53 ページの「重み付けされた優先順位の選択について」を参照してください。

クラスタ設定

クラスタ設定とは、クラスタ全体に複製される設定で、各 HA メンバーは同じクラスタ設定情報を使用して設定されます。一元管理およびクラスタ管理コンポーネントは、クラスタ情報を使用して迅速なフェイルオーバを提供し、重要なポリシーおよび設定情報が失われることがないようにします。

クラスタ設定ファイル、`cluster.ini` は、`/etc/iscan` ディレクトリに格納され、HA クラスタ設定を保存するために使用されます。Web コンソールの [クラスタ管理] 画面から、クラスタの以下の要素を設定できます。

- **クラスタ名** — クラスタの名前です。
- **クラスタの説明** — クラスタの説明です。
- **クラスタの IP アドレス** — クラスタの浮動管理 IP アドレスは、常にアクティブノードと関連付けられます。IPv4 と IPv6 のアドレスがクラスタの上位および下位に対して設定されている場合、IWSVA は IPv4 と IPv6 両方のアドレスを表示できます (例 : 172.16.2.200/2001:10::101)。
- **重み付けされた優先順位の選択** — 有効または無効 (初期設定) にします。
- **クラスタメンバー** — 下位ノードへのログインアクセスが付与された、HA クラスタに属するノード (IPv4 または IPv6) のリストです。

注意 : このバージョンの IWSVA では、次の項目は設定不可です。
- クラスタ配置モード — 常に透過ブリッジモードになります。
- HA モード — 常にアクティブ / パッシブです。
- HA クラスタの IP アドレスは IPv6 アドレスをサポートしません。

ノード設定

ノード設定は、特定の HA メンバーに適用されるもので、クラスタ全体の設定ではありません。これらのノード固有の設定が、HA メンバー間で同期されることはありません。ノード固有の設定には次の項目が含まれます。

- **ホスト名** — ノードの名前です。
- **役割** — 上位または下位のどちらかです。
- IP **アドレス** — 接続ステータス信号ポートで使用される IP アドレスです。これが空の場合、クラスタメンバー間で新しい IP がネゴシエートされ、IP アドレスパラメータに書き込まれます。
- **重み** — ノードの重みです。有効な値は 1 ～ 255 です。重みが大きくなると、そのノードが上位ノードとしての役割を果たすよう選択される可能性が高くなります。
- **ステータス** — ノードのステータスです。緑色は稼働中、赤色は停止していることを意味します。
- **前回の同期** — 前回の成功した同期の日時を表示します。
- **同期ステータス** — 緑色は成功、赤色は失敗を意味します。失敗した場合は、ツールヒントに理由が表示されます。

クラスタログおよび通知

HA クラスタは、次のイベントのログを記録しレコードを作成します。

- クラスタの作成
- 既存のクラスタの解除または分解
- クラスタへのメンバーの追加
- クラスタの設定の変更
- クラスタからのメンバーの削除
- クラスタメンバーの役割の変更
- 手動同期の実行
- フェイルオーバ
- 異常の検出

次の場合に、クラスタ通知が発行されます。

- 異常が検出された
- フェイルオーバが発生した
- メンバーが復元された

- フェイルオーバまたはスイッチオーバを実行できなかった

クラスタへのアクセス

上位ノードにアクセスするには

管理者は、次の 2 つの IP アドレスのどちらかを使用して、上位メンバーの Web 管理インタフェースにアクセスできます。

- 上位メンバーの管理 IP アドレスとポート番号
- クラスタ IP アドレスとポート番号

例 :

`https://<` **上位メンバーの管理** `IP` **アドレス** `>:<` **ポート番号** `>`

`https://<` **クラスタ** `IP` **アドレス** `>:<` **ポート番号** `>`

下位ノードにアクセスするには

管理者は、下位ノードの Web 管理コンソールに次の 2 つの方法でログインできます。

- [クラスタ管理] 画面上のリンクを経由 ([管理] → [一般設定] → [クラスタ管理] →下位ノードの [ログイン] ボタン)
- 下位ノードの管理ポート IP アドレスを使用

例 :

`https://<` **下位ノードの** `IP` **アドレス** `>:<` **ポート番号** `>`

不注意による設定ミスから保護するために、すべてのクラスタレベルの機能は、下位メンバーの Web 管理インタフェースでは非表示またはブロックされています。(図 3-1 にある上位ノードの左のメニューと、図 3-2 にある下位ノードの左のメニューを比較します)。下位メンバーに対して特に

適用される、下位メンバーに適用可能な設定パラメータのみが、下位メンバーの Web 管理インタフェースで表示され、設定可能になっています。下位レベルの設定と機能の詳細なリストについては、表 3-1 を参照してください。

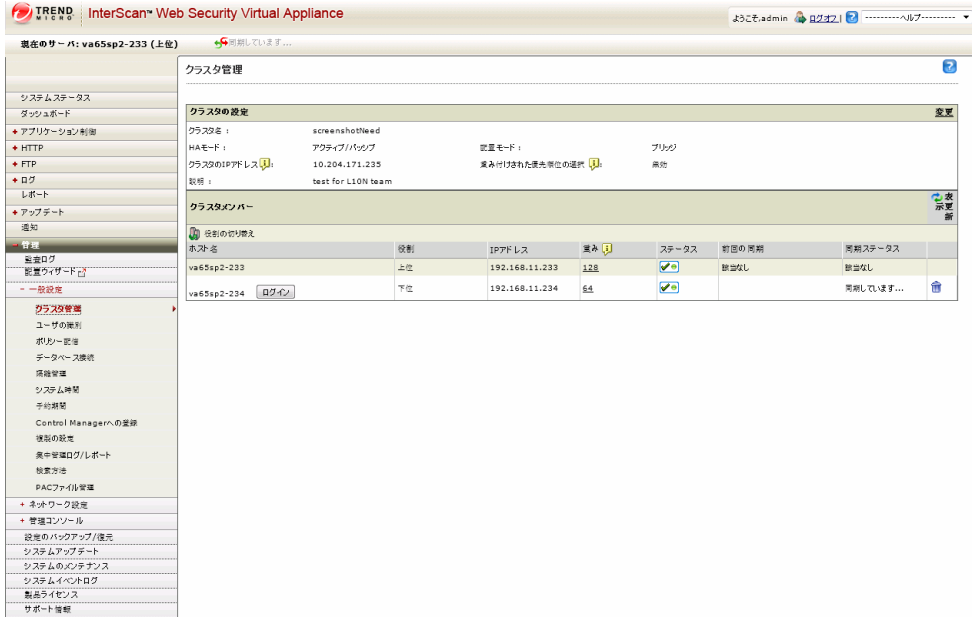


図 3-1.　下位ノードへのログインアクセスを備えた上位ノードのクラスタ管理画面

管理者が下位メンバーにログインしているときにクラスタレベルの設定を変更する必要が生じた場合は、[クラスタ管理] 画面で上位メンバーの横に表示される [ログイン] ボタンをクリックして上位メンバーにログインすることができます。

IWSVA HA は、シングルサインオン技術を使用してクラスタメンバー間で認証情報を渡すため、他のメンバーにアクセスするためにパスワードを入力する必要はありません。

図 3-2.　上位ノードにアクセスできる、子ノードのクラスタ管理画面

注意：　下位ノードでは、一元管理される機能に対応する CLI コマンドを使用できません。

クラスタ管理用の Web コンソール画面

管理者は、[管理] → [一般設定] → [クラスタ管理] の　[クラスタ管理] 画面で以下を設定できます。

- 108 ページの「クラスタからの下位メンバーの削除」
- 109 ページの「クラスタの解除」
- 109 ページの「手動スイッチオーバの実行」
- 101 ページの「ノードの手動同期」
- 110 ページの「クラスタの変更」

クラスタからの下位メンバーの削除

クラスタから下位ノードを削除すると、クラスタは唯一のメンバーである上位ノードとともに残ります。後から別のノードを下位ノードとして追加できます。

下位ノードを削除するには

1. 上位メンバーの Web コンソールで、[管理] → [一般設定] → [クラスタ管理] に移動します。
2. 画面の [クラスタメンバー] に移動します。
3. 下位行の削除アイコン（  ）をクリックし、下位メンバーを削除します。
4. [OK] をクリックして削除を確認します。進行状況を示すバーが表示されます。
5. 数秒後に削除が完了しなかった場合は、ブラウザの [表示更新] ボタンをクリックします。
   下位メンバーが [クラスタメンバー] リストに表示されなくなり、以前の下位ノードはプロキシ転送モードに戻ります。

クラスタの解除

HA クラスタの解除とは、HA クラスタが分解されることで、下位メンバーと上位メンバーが削除された後に起こります。HA クラスタを解除すると、アクティブな HA メンバーは透過ブリッジモードで動作するスタンドアロンの IWSVA デバイスに戻ります。

クラスタを解除するには

1. 上位メンバーの Web コンソールで、[管理] → [一般設定] → [クラスタ管理] に移動します。
2. 108 ページの「クラスタからの下位メンバーの削除」で示すように、クラスタの下位メンバーを削除します。
3. 画面の [クラスタメンバー] で、削除アイコン（  ）をクリックして上位メンバーを削除します。
4. [OK] をクリックして解除を確認します。進行状況を示すバーが表示されます。
   a. 5 分後に解除が完了しなかった場合は、ブラウザの [表示更新] ボタンをクリックします。
      上位メンバーが透過ブリッジモードでのスタンドアロン IWSVA になり、[クラスタ管理] 画面は表示されなくなります。

手動スイッチオーバの実行

管理者は HA クラスタ内の 2 つのメンバーの上位 / 下位の役割を手動で切り替えることができます。スイッチオーバが正常に完了すると、元の上位メンバーが下位メンバーとなり、パッシブモードになります。元の下位メンバーは上位メンバーとなり、アクティブモードに入ります。

注意： 重み付けされた優先順位の選択処理が無効にされている場合、管理者は手動スイッチオーバしか実行できません。重み付けされた優先順位の選択モードを有効にしてスイッチオーバを実行するには、管理者は各メンバーの重みを変更して HA スイッチオーバをトリガする必要があります。クラスタメンバーの重みを変更する方法については、110 ページの「クラスタの変更」を参照してください。

重み付けされた優先順位の選択モードを無効にして手動スイッチオーバを実行するには

注意： IWSVA が同期を実行している場合、それが手動であれ予約同期であれ、同期ステータスに「同期中 …」と表示され、手動スイッチオーバは実行されません。これは、重み付けされた優先順位の選択モードが無効になっている場合のスイッチオーバ（役割の切り替えによる）、または重み付けされた優先順位の選択モードを有効にした状態でノードの重み値を変更しようとした場合のスイッチオーバに適用されます。同期が進行中であっても自動フェイルオーバは発生し、最新の正常な同期の後に存在したポリシーと配信設定に戻ります。

1. 上位ノードの Web コンソールで、[管理] → [一般設定] → [クラスタ管理] に移動します。
2. [クラスタメンバー] セクションで、[役割の切り替え] をクリックします。
3. 役割の切り替えの確認画面で [OK] をクリックし、新しい上位ノードに再度ログインします。

クラスタの変更

[クラスタ管理] 画面では、管理者はクラスタ設定の表示、クラスタ設定の変更、および上位サーバと下位サーバ間での役割の切り替えを実行できます。

表 3-2 は、[クラスタ管理] 画面に表示されるクラスタの設定を示したものです。

表 3-2. クラスタの設定

値	説明
クラスタ名	これはクラスタが最初に配置ウィザードで作成されたときにクラスタに割り当てられた名前です（変更可能）。
HA モード	アクティブ / パッシブ（変更不可）
クラスタの IP アドレス	Web コンソールまたは CLI からクラスタにログインするために使用される浮動 IP アドレスです。この IP アドレスは、スイッチオーバが発生しても元のままになります（変更可能）。

表 3-2. クラスタの設定 (続き)

値	説明
説明	配置ウィザードを使用してクラスタを追加するときに入力された説明 (オプション) を表示します (変更可能)。
配信モード	IWSVA HA クラスタは透過ブリッジモードでのみサポートされるため、現時点ではこのパラメータには常に「ブリッジ」と表示されます (変更不可)。
重み付けされた優先順位の選択	有効または無効のどちらかが表示されます (変更可能)。
役割の切り替え	管理者が上位メンバーと下位メンバー間で役割を切り替えられるようにします。
表示更新	クラスタメンバーのステータスを更新します。

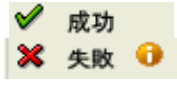
[クラスタ管理] 画面の [クラスタメンバー] セクションでは、クラスタメンバー (上位および下位メンバー) とステータスの詳細情報が表示され、下位ノードにログインアクセスすることができます。

表 3-3 は、上位ノードと下位ノード両方で表示されるパラメータを示したものです。

表 3-3. クラスタメンバーの設定

パラメータ	説明
ホスト名	サーバ名を表示します。
役割	「上位」または「下位」のどちらかが表示されます。
IP アドレス	デバイスの IP アドレスが表示されます。
重み	クラスタの設定時に入力された重みが表示されます。 (初期設定 : 上位 128/ 下位 64 - 変更可能。設定可能な値 : 1 ～ 255、大きい値 = 高い優先順位。)
ステータス	次のアイコンが表示されます。  稼働中のステータス  停止中のステータス

表 3-3. クラスタメンバーの設定 (続き)

パラメータ	説明
前回の同期	下位サーバが最後に上位サーバと同期された日時 (時間 : 分 : 秒) を表示します。
同期 ステータス	次を表示します。  成功 — 同期に成功しています。 失敗 — 同期に失敗しています。情報ツールヒントに同期が失敗した理由が表示されます。
解除	下位メンバーを削除するアイコン ( ) を表示します。下位メンバーが削除されている場合は、上位メンバーに関するアイコンのみが表示されます。上位メンバーを削除すると、クラスタ全体が解除されます。

クラスタ設定を変更するには

1. [管理] → [一般設定] → [クラスタ管理] に移動します。
2. [クラスタの設定] の横にある [変更] リンクをクリックします。
3. [クラスタの設定] 画面で、必要に応じて以下のパラメータを変更します。
   - **クラスタ名** — クラスタが最初に配置ウィザードで作成されたときにクラスタに割り当てられた名前を表示します (変更可能)。
   - **説明** — 配置ウィザードを使用してクラスタを追加するときに入力された説明 (オプション) を表示します (変更可能)。
   - **クラスタ IP アドレス** — Web コンソールまたは CLI からクラスタにログインするために使用される浮動管理 (またはクラスタ) IP アドレスを表示します。浮動 IP アドレスは、常にクラスタ内のアクティブノードと関連付けられます (変更可能)。
   - **重み付けされた優先順位の選択** — 有効または無効のどちらかを表示します。[重み付けされた優先順位の選択] の値が有効に設定されている場合、HA ペアでは、重みが最も大きいコンピュータを選択します。[重み付けされた優先順位の選択] の値が無効に設定されている場合、HA ペアでは、現在アクティブな (またはプライマリ) コンピュータが使用できない場合にのみ選択を行います (変更可能)。
   - HA **モード** — アクティブ / パッシブ (表示のみ)
   - **配信モード** — IWSVA HA クラスタは透過ブリッジモードでのみサポートされるため、現時点ではこのパラメータには常に「ブリッジ」と表示されます (表示のみ)。
4. [保存] をクリックします。

ノードの重みの値を変更するには

注意： 以下の手順を実行するには、[重み付けされた優先順位の選択] モードが有効にされている必要があります ([重み付けされた優先順位の選択] モードを有効にするには、112 ページの「クラスタ設定を変更するには」のステップ 3 を参照してください)。[重み付けされた優先順位の選択] が無効にされている場合は、役割は手動で切り替えることができます。詳細については、109 ページの「手動スイッチオーバの実行」を参照してください。

1. [管理] → [一般設定] → [クラスタ管理] に移動します。
2. [クラスタメンバー] セクションで、変更する重みの値をクリックします。
3. [重み] 画面で、重みの値を変更して適切な値が表示されるようにします (1 ～ 255、高い値 = 高い優先順位、2 つのノードに対して同じ値は保存できません)。
4. [保存] をクリックします。

   下位メンバーの重み値を上位メンバーの重み値よりも高くなるように変更し、[重み付けされた優先順位の選択] が有効にされている場合、その 2 つのメンバーの役割が切り替わります。

第 4 章

アップデート

不正なプログラムや悪質な Web サイトが日々開発され出現しています。このため、InterScan Web Security Virtual Appliance（以下、IWSVA) Web コンソールの［アップデート］→［手動］画面に表示されるパターンファイルと検索エンジンを常に最新に保つことが必要です。

本章で説明する内容には、次の項目が含まれます。

製品サポート

トレンドマイクロは随時、報告された既知の問題に対処する Patch、またはお使いの製品に適用するアップデートをリリースする場合があります。利用できる Patch の有無については、次の URL からご確認いただけます。

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

IWSVA のリンクをクリックすると、IWSVA のアップデート画面に移動します。

Patch には日付が付いています。適用していない Patch がある場合、Readme を開いて Patch を適用するかどうかを判断します。適用する場合、Readme 内のアップデートの指示に従ってください。

サポート契約の更新

トレンドマイクロまたは販売代理店では、すべての登録済みユーザに対して、テクニカルサポート、ウイルスパターンファイルのダウンロード、およびプログラムのアップデートを 1 年間提供します。この期間を過ぎると、サポート契約を更新する必要があります。

サポート契約の有効期限が切れても検索はできますが、ウイルスパターンファイルおよびプログラムのアップデートはできません。アップデート不能にならないように、できるだけ早くサポート契約を更新してください。

サポート契約を更新するには、製品をお買い上げいただいた購入元にお問い合わせください。契約期間を 1 年間延長したサポート契約は、登録プロファイルに表示される企業の担当者宛てに郵送されます。

企業の登録プロファイルを表示または変更するには、次のトレンドマイクロオンライン登録の Web サイトからアカウントにログインします。

https://clp.trendmicro.com/fullregistration

登録プロファイルを表示するには、最初にトレンドマイクロに製品を登録した際（新規登録）に作成したログオン ID およびパスワードを入力し、[ログイン] をクリックします。

アップデート機能について

アップデートは、多くのトレンドマイクロ製品に共通するサービスです。アップデート機能により、トレンドマイクロのアップデートサーバに接続し、最新のパターンファイルおよびエンジンをダウンロードします。

アップデートの実行後、コンピュータを再起動する必要はありません。アップデートは、予約しておいた間隔で自動で行うことも、必要に応じて手動で行うことも可能です。

IWSVA Web コンソールからアップデートする方法

トレンドマイクロ製品の集中管理に、Control Manager または Apex Central を使用しない場合、IWSVA からアップデートサーバに直接接続します。アップデートされたコンポーネントは、次のいずれかの間隔で IWSVA に配信できます。

- 次の間隔（15 分、30 分、45 分、60 分)

  これらの 15 分きざみのアップデートは、ウイルスパターンファイル、スパイウェアパターンファイル、ボットパターンファイル、IntelliTrap パターンファイル、IntelliTrap 除外パターンファイル、スマートスキャンエージェントパターンファイル、スクリプトアナライザパターンファイル、およびプロトコル情報抽出パターンファイルのみに対して適用されます。
- 毎時間
- 毎日
- 毎週
- 手動

注意： パターンファイルは毎時間、エンジンは毎日または毎週アップデートすることをお勧めします。すべてのアップデートには、ウイルスパターンファイル、スパイウェアパターンファイル、ボットパターンファイル、IntelliTrap パターンファイル、IntelliTrap 除外パターンファイル、スマートスキャンエージェントパターンファイル、スクリプトアナライザパターンファイル、およびプロトコル情報抽出パターンファイルが含まれています。

プロキシ設定 (アップデート用)

インターネットへのアクセスにプロキシサーバを使用する場合は、コンポーネントをアップデートする前に IWSVA Web コンソールでプロキシ情報を入力する必要があります。入力したプロキシ情報は、次の処理に使用されます。

- トレンドマイクロのアップデートサーバからのコンポーネントのアップデート
- 製品の登録およびライセンス確認
- Web レピュテーション検索

コンポーネントおよびライセンスのアップデート用にプロキシサーバを設定するには

1. IWSVA Web コンソールを開いて、[アップデート] → [接続設定] の順に選択します。
2. [コンポーネント、ライセンス、Web レピュテーションクエリのアップデートにプロキシサーバを使用する] を選択して、プロキシサーバまたはポートを指定します。IWSVA は、IPv4 と IPv6 の両方の AU サーバをサポートしています。アップデートプロキシでは、IPv6 プロキシまたは、ホスト名か IPv4/IPv6 アドレスによる IPv4 プロキシもサポートしています。
3. プロキシサーバで認証が必要な場合は、[ユーザ ID] と [パスワード] にそれぞれ入力します。

   認証を必要としないプロキシサーバの場合は、このフィールドを空欄のままにします。
4. 最新のパターンファイルにアップデートした後、[パターンファイル] に IWSVA デバイスに保存しておくパターンファイルの数を入力します（初期設定および推奨設定は 3 パターンファイル）。

   古いパターンファイルをサーバに保存しておけば、何度も誤警告を発したりするなど、環境に合わなかった場合でも元のパターンファイルに戻せます。サーバ上のパターンファイル数がこの設定値を超えた場合は、最も古いパターンファイルが自動的に削除されます。
5. [保存] をクリックします。

注意： 透過ブリッジモードでは、IWSVA には内部インタフェースと外部インタフェースがあります。アップデートが適切に機能するようにするには、アップデートプロキシおよびサーバの設定を、同じ側で行う必要があります。IWSVA を別のプロキシサーバで配信する場合、ネクストホップのアップデートプロキシおよびサーバに関するプロキシ設定は、同じ側のインタフェースの同じサーバとなっている必要があります。

アップデート可能なコンポーネント

最新のリスクに対する対策を最新に保つには、アップデート可能なコンポーネントがいくつかあります。

- **パターンファイルとシグネチャ** — パターンファイルには、ウイルスパターンファイル、スパイウェアパターンファイル、ボットパターンファイル、IntelliTrap パターンファイル、IntelliTrap 除外パターンファイル、スマートスキャンエージェントパターンファイル、スクリプトアナライザパターンファイル、およびプロトコル情報抽出パターンファイルがあります。これらのファイルは、既知のセキュリティ上の脅威のバイナリ「シグネチャ」やパターンを格

納しています。検索エンジンと同時に使用すると、それらがインターネットゲートウェイを通過する際に IWSVA によって脅威が検出されます。新しいウイルスパターンファイルは通常、週に数回提供されています。一方、スパイウェアパターンファイルはそれほど頻繁にはアップデートされません。

- **プロトコル情報抽出パターンファイル** — このファイルは、プロトコルのアップデートまたは新しいアプリケーションサポートの追加を目的としてアプリケーション制御モジュールで使用されます。

  プロトコル情報抽出パターンファイルは以下のディレクトリに保存されます。

  /etc/iscan/libtmprotocols.so.########

- **ウイルス検索エンジン** — 各ファイルのバイナリパターンを解析し、それをパターンファイル内のバイナリ情報と比較するモジュールです。一致した場合は、そのファイルを不正なものとして判断します。
- URL **フィルタエンジン** — IWSVA は、URL フィルタエンジンを使用して、クラウドベースの Smart Protection Network が提供する URL データに基づく URL の分類およびレピュテーションの評価を実行します。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。
- **高度な脅威検索エンジン** (ATSE) — ATSE はトレンドマイクロの新しい革新的な検索エンジンで、最新のヒューリスティックルールを使用して、広範囲に及ぶ従来とは異なるリスクを検出します。これには、ドキュメントの脆弱性を利用して標的を感染させるために攻撃者によって一般に使用されるドキュメントのセキュリティホールなどが含まれます。

ウイルスパターンファイル

トレンドマイクロの検索エンジンでは、ウイルスパターンファイルと呼ばれる外部データファイルを使用して、最新のウイルスおよびトロイの木馬、メール大量配信、ワーム、複合攻撃のようなその他のインターネット上の脅威情報を最新に保ちます。新たなウイルスパターンファイルは週に数回の割合で作成、リリースされ、特に致命的な危険が発見されたときは常に作成、リリースされます。

トレンドマイクロのウイルス対策プログラムでアップデート機能 (詳細については 116 ページの「アップデート機能について」を参照) を使用すると、新しいウイルスパターンファイルがサーバに用意されたことを検出できます。また、1 時間おき、1 日おき、1 週間おきなどに最新ファイルを取得するよう自動的にサーバにポーリングを予約しておくことも可能です。ウイルスパターンファイルの最新情報は、次の Web サイトで参照できます。

`https://appweb.trendmicro.com/ecs/Default.aspx`

ここには、ウイルスパターンファイルの最新バージョン、リリース日付、新ウイルス定義リストが用意されています。

ウイルスパターンファイルの仕組み

検索エンジンはウイルスパターンファイルと連携し、パターンマッチングと呼ばれる処理で一次レベルの検出を行います。それぞれのウイルスには、他のコードと識別できる固有のバイナリ「シグネチャ」または証拠となる文字列があるため、TrendLabs のウイルス専門エンジニアがこのコードのパターンの断片を取り込んでパターンファイルに格納します。これに対し、エンジンが検索対象ファイルごとに特定部分をウイルスパターンファイルのデータと比較して、一致する部分がないか検索します。

パターンファイル名は次のとおりです。

```
/etc/iscan/lpt$vpn.###
```

は、パターンファイル番号を表す 3 桁の数字です（例 : 400)。同じパターンファイル番号で別のビルド番号のパターンファイルを識別したり、999 より大きいパターンファイル番号にも対応する場合、これが IWSVA Web コンソールに表示されます。形式は次のとおりです。

ロール番号 . パターンファイル番号 . ビルド番号（形式 : xxxxx.###.xx)

- ロール番号 — パターンファイル番号が 999 を超えた回数を表します。桁数の最大は 5 桁です (0 ～ 21474)。
- パターンファイル番号 — /etc/iscan/lpt$vpn.### のパターン拡張子と同じで、3 桁です（100 ～ 999)。
- ビルド番号 — Patch またはリリースを表します。2 桁です（00 ～ 99)。

同じフォルダに複数のパターンファイルが存在する場合、通常は、最も数字の大きいファイルのみが使用されます。トレンドマイクロでは、新しいウイルスパターンファイルを随時提供しています (通常、週に数回更新しています)。[アップデート] → [スケジュール] 画面から毎時の自動アップデートを設定しておくことをお勧めします。アップデートは、有効なサポート契約をお持ちであればどなたでもご利用いただけます。

注意 : 古いパターンファイルを削除する必要はありません。また、新しいパターンファイルを「インストール」するのに特別な措置を講じる必要はありません。

スパイウェアパターンファイル

機密情報をひそかに収集する新型の隠しプログラム、グレーウェアが横行して見つかるようになったため、トレンドマイクロではそれらのシグネチャを収集し、スパイウェアパターンファイルに取り入れています。スパイウェアパターンファイルは初期設定で以下のディレクトリに保存されます。

`/etc/iscan/ssaptn.###`

は、パターンファイルの番号を表す 3 桁の数字です。同じパターンファイル番号で別のビルド番号のパターンファイルを識別します。また、999 より大きいパターンファイル番号にも対応しています。IWSVA Web コンソールには次の形式で表示されます。

ロール番号 . パターンファイル番号 . ビルド番号 (形式 : `xxxxx.###.xx`)

- ロール番号 — パターンファイル番号が 999 を超えた回数を表します。桁数の最大は 5 桁です (0 ～ 21474)。
- パターンファイル番号 — `/etc/iscan/ssaptn.###` のパターン拡張子と同じで、3 桁です (100 ～ 999)。
- ビルド番号 — Patch またはリリースを表します。2 桁です (00 ～ 99)。

ボットパターンファイル

ボットネットとは、一般的な C&C インフラストラクチャに基づいて、通常ワーム、トロイの木馬、あるいはバックドアと呼ばれるプログラムを実行する感染コンピュータで構成されるネットワークです。トレンドマイクロでは、ボットネットの URL を収集し、その情報をボットパターンファイルに組み込んでいます。ボットパターンファイルには既知のボットネット URL の暗号化されたリストが含まれています。ボットパターンファイルは初期設定で以下のディレクトリに保存されます。

`/etc/iscan/re###.ptn`

IntelliTrap パターンファイルおよび IntelliTrap 除外パターンファイル

IntelliTrap の検出では、IntelliTrap パターンファイル (不正プログラムが潜んでいる可能性のあるファイル検出用) および IntelliTrap 除外パターンファイル (許可リストとして使用) とともにトレンドマイクロのウイルス検索エンジンの検索オプションが使用されます。IWSVA では、IntelliTrap オプションおよびパターンファイルを使用して、圧縮ファイル内のボットなど、不正なプログラムが含まれる圧縮ファイルを検出します。ウイルス作成者は、複数のファイル圧縮スキームを使用して、

ウイルスフィルタを回避しようとします。IntelliTrap では、圧縮ファイルのヒューリスティック評価を提供することにより、ボットまたはその他の不正なプログラムを含む圧縮ファイルがネットワークに与えるリスクを軽減します。

IntelliTrap パターンファイル `tmblack.###` および IntelliTrap 除外パターンファイル `tmwhite.###` は、`/etc/iscan/` ディレクトリに保存されます。

スマートスキャンエージェントパターンファイル

スマートスキャンエージェントパターンファイルは、アクセスされるサンプルに対してローカルパターンマッチングを実行するためにスマートスキャンによって使用されます。サンプルがローカルパターンと一致すると、ローカルキャッシュまたはグローバルスマートスキャンサーバからのサンプルハッシュは照会されません。

スマートスキャンエージェントパターンファイルは初期設定で以下のディレクトリに保存されます。

`/etc/iscan/icrc$oth.###`

スクリプトアナライザ (SA) パターンファイル

SA パターンファイルは、不正スクリプトを分析するためにスクリプトアナライザモジュールによって使用されます。

パターンファイル名は次のとおりです。

`/etc/iscan/ssaptn.###`

プロトコル情報抽出パターンファイル

プロトコル情報抽出パターンファイルは、プロトコルを識別するためにアプリケーション制御で使用されます。

`/etc/iscan/libtmprotocols.so.###`

検索エンジン

トレンドマイクロのウイルス対策製品はすべて、独自に開発した検索エンジンを基盤としています。新種のウイルスに対抗すべく独自に改良を重ねてきた結果、現在では非常に高性能な検索エンジンとなっています。ウイルスはもとより、インターネットワーム、メール大量配信、トロイの木馬、セキュリティ上の弱点を突くツールなどの危険も検出できます。検索エンジンで検出できる脅威の種類は次のとおりです。

- 感染報告のあるウイルス。自ら蔓延するプログラム
- 出回っていないウイルスまたは制御されたウイルス。研究や脆弱性を実証するために利用および開発されるプログラム

トレンドマイクロの検索エンジンは度重なるテストの結果、単体ファイルのチェックでも、デスクトップコンピュータ上の 10 万ファイルの検索でも、インターネットゲートウェイにおけるメールトラフィックの検索でも、最速の部類に入ることが確認されています。ファイルごとバイトごとに検索を行うのではなく、検索エンジンとパターンファイルが連携してウイルスコードの文字列を識別し、ファイル内でウイルスが隠れていそうな場所を厳密に突き止めます。ウイルスが検出された場合は削除して、ファイルを正常な状態に修復することができます。

検索エンジンには、ディスク容量を空けるために、古いウイルスパターンファイル、スパイウェアパターンファイル、および IntelliTrap パターンファイルに対する自動クリーンナップルーチンが含まれています。また、帯域幅の使用を最小限に抑えるための差分パターンファイルのアップデートも含まれています。

検索エンジンはさらに、MIME や BinHex などの主要なインターネットエンコード形式をすべてデコードできます。このほか、Zip、Arj、Cab などの一般的な圧縮形式も認識して検索することができます。トレンドマイクロのほとんどの製品では、圧縮ファイル内にさらに圧縮ファイルが入っている場合、検索対象とする圧縮レイヤの数を最大 20 まで指定できます。

検索エンジンのアップデートについて

時間によって最も変動するウイルス情報をウイルスパターンファイル内に格納することにより、検索エンジンのアップデート回数をできるだけ減らすと同時に保護機能を最新に保つことができます。トレンドマイクロでは新バージョンの検索エンジンを定期的に公開しています。新しい検索エンジンは、たとえば次の時点で提供されます。

- ソフトウェアに新しい検索技術と新しい検出技術が採用されたとき
- 現在のエンジンでは対処できない新種で有害と思われるウイルスが検出されたとき
- 検索パフォーマンスが機能拡張されたとき
- 対応するファイル形式、スクリプト記述言語、エンコード、圧縮形式が新たに追加されたとき

検索エンジンの最新情報は、次の URL からご確認いただけます。

`https://success.trendmicro.com/jp/solution/000148744`

Web レピュテーションデータベース

Web レピュテーションデータベースは、他の Trend Smart Protection Network サーバとともにクラウド内に存在します。ある URL にユーザがアクセスしようとすると、IWSVA はこの URL についての情報を Web レピュテーションデータベースから取得し、ローカルキャッシュに保存します。Web レピュテーションデータベースをクラウド内に置き、データベース情報を使用してローカルキャッシュを作成することによって、IWSVA のオーバーヘッドを削減し、パフォーマンスを高めます。

要求された URL について Web レピュテーションデータベースが取得できる情報の種類は、次のとおりです。

- Web カテゴリ
- ファーミング / フィッシング検出で使用されるファーミングフラグとフィッシングフラグ
- 指定されたセキュリティレベルに基づき、URL アクセスのブロックに使用される Web レピュテーションスコア (212 ページの「Web レピュテーションルールの指定」を参照)

Web レピュテーションデータベースは、Web ページのカテゴリ分類が最新の状態でアップデートされます。

URL のレピュテーションが誤ったカテゴリに分類されていると思われる場合、または URL のレピュテーションを知りたい場合には、次のリンクをクリックして、トレンドマイクロまでお知らせください。

`https://global.sitesafety.trendmicro.com/`

パターンファイルおよびエンジンの差分アップデート

アップデートでは、最新のパターンファイルおよびエンジンファイルの差分アップデートがサポートされます。毎回ファイル全体をダウンロードするのではなく、ファイルの新しい部分のみをダウンロードして既存ファイルに付加できます。この効率的なアップデート方法により、ウイルス対策ソフトウェアのアップデート、およびお使いの環境へのパターンファイルおよびエンジンファイルの配信に必要な帯域幅を大幅に低減することができます。

コンポーネントのバージョン情報

実行中のパターンファイルや検索エンジンのバージョンを調べるには、管理コンソールで [アップデート] → [手動] の順に選択します。使用しているバージョンが [手動アップデート] 画面の [現在のバージョン] 列に表示されます。

手動アップデート

IWSVA の有効性は、最新のパターンファイルおよびエンジンファイルを使用するかどうかによって決まります。シグネチャベースのウイルス検索やスパイウェア / グレーウェア検索は、検索されたファイルのバイナリパターンをパターンファイル内の既知の脅威のバイナリパターンと比較することによって動作します。トレンドマイクロでは、新たに確認された脅威に対応して、新しいバージョンのウイルスパターンファイルとスパイウェアパターンファイルを頻繁にリリースします。同様に、新たなフィッシング URL が確認されると新しいバージョンのフィッシングパターンファイルがリリースされます。

新しいバージョンのトレンドマイクロの検索エンジンは、パフォーマンスが向上し、新しい脅威に対処する機能が追加される際にアップデートされます。

注意： ネットワーク上のインターネット接続がプロキシサーバを通過する場合、プロキシ情報を設定する必要があります。管理コンソールから [アップデート] → [接続設定] の順に選択し、プロキシサーバ情報を入力します。

エンジンおよびパターンファイルをアップデートするには

1. [アップデート] → [手動] をクリックします。
2. [手動アップデート] 画面の一覧にあるすべてのコンポーネントについて、次のいずれかをクリックします。
   - **すべてアップデート** — すべてのコンポーネントをアップデートします。
   - **アップデート** — 選択されたコンポーネントのみをアップデートします。

   IWSVA がすでに最新バージョンのコンポーネントを使用しており、更新されたアップデートがない場合、コンポーネントはアップデートされません。IWSVA デバイス上のコンポーネントが破損しているか、または使用できない場合を除いて、([アップデート] のクリックによる) アップデートの強制は不要です。

強制手動アップデート

IWSVA では、IWSVA がすでに最新のパターンファイルや検索エンジンを使用している場合であっても、パターンファイルと検索エンジンを強制的にアップデートするオプションが用意されています。通常は、アップデートの必要はないというメッセージが表示されます。パターンファイルまたは検索エンジンが破損していて、アップデートサーバからダウンロードし直す必要があるなど特殊な状況にも対応することができます。

コンポーネントを強制アップデートするには

1. 管理コンソールで [アップデート] → [手動] をクリックして、[手動アップデート] 画面を表示します。
2. 一覧に表示されているすべてのコンポーネントについて、[アップデート] をクリックして、選択されたコンポーネントのみをアップデートします。

   IWSVA がすでに最新のパターンファイルや検索エンジンを使用している場合は、メッセージボックスが表示されます。IWSVA がアップデートサーバよりも古いパターンファイルを使用している場合は、最新のパターンファイルがダウンロードされます。
3. 強制アップデートを開始するには、このメッセージボックスから [OK] をクリックします。

予約アップデート

IWSVA は次のパターンファイルについて予約アップデートを実行できます。

- ウイルス (トロイの木馬やワームのシグネチャを含む)
- スパイウェア
- ボット
- IntelliTrap
- IntelliTrap 除外
- スマートスキャンエージェント
- スクリプトアナライザ
- プロトコル情報抽出

また、IWSVA は検索エンジンおよび URL フィルタエンジンについても同様に予約アップデートを実行できます。

パターンファイルおよびエンジンの自動アップデートを予約するには

1. 管理コンソールから [アップデート] → [予約] の順に選択します。
2. アップデート対象のコンポーネントの種類ごとに、アップデート間隔を選択します。

   次のオプションが用意されています。

   - [次の間隔] (パターンファイルのみ。アップデートを何分おきに実行するか選択します。)
   - [毎時] (パターンファイルのみ)
   - [毎日]
   - [毎週] (ドロップダウンメニューから曜日を選択。最新のエンジンのアップデートにはこの設定をお勧めします。)

   注意： コンポーネントの予約アップデートを無効にするには、各コンポーネントのセクションで [予約アップデートを実行しない] を選択します。

3. コンポーネントごとに、予約アップデートを有効にする開始時刻を選択します。
4. [保存] をクリックします。

注意： ネットワーク設定にキャッシュサーバが含まれる場合、パターンファイルのアップデート後にキャッシュを消去してキャッシュサーバを再起動することをお勧めします。これにより、すべての URL 要求に対する検索が強制され、ネットワークがより強固に保護されます。キャッシュの消去とサーバの再起動の方法については、キャッシュサーバのドキュメントを参照してください。

アップデートの操作方法

アップデート通知

IWSVA では、パターンファイルまたはエンジンのアップデート状況を事前に管理者に知らせる通知を発行できます。アップデートに関する通知の設定方法については、354 ページの「パターンファイルのアップデート通知の有効化」および 359 ページの「URL フィルタエンジンおよび検索エンジンのアップデートの通知の有効化」を参照してください。

アップデートのロールバック

IWSVA では、プログラムのインストールフォルダを監視し、最新のパターンファイルまたは検索エンジンを使用して、インバウンドとアウトバウンドのトラフィックにウイルス検索を実行します。最新のパターンファイルは、ファイルの拡張子で判別されます。たとえば、lpt$vpn.401 は、lpt$vpn.400 より新しいファイルです。

新しいパターンファイルにより、感染していないファイルをウイルス感染と誤って検出する「誤警告」が発生する場合があります。このような場合、以前のパターンファイルや検索エンジンに戻すことができます。

注意： IWSVA では、URL フィルタエンジンのロールバックはサポートされていません。

パターンファイルまたは検索エンジンをロールバックするには

1. 管理コンソールから [アップデート] → [手動] の順に選択します。
2. ロールバック対象のコンポーネントを選択し、[ロールバック] をクリックします。

   ロールバックの進行状況を示すバーが表示され、ロールバック結果を示すメッセージ画面が表示されます。

パターンファイルの削除

パターンファイルのアップデート後も、IWSVA では、ロールバックに備えてウイルスパターンファイル、スパイウェアパターンファイル、ボットパターンファイル、IntelliTrap パターンファイル、IntelliTrap 除外パターンファイル、スマートスキャンエージェントパターンファイル、スクリプトアナライザパターンファイル、およびプロトコル情報抽出パターンファイルなど古いパターンファイルがサーバに保存されます。サーバに保存するパターンファイルの数は、[アップデート] → [設定] 画面の [保存するパターンファイルの数] で設定します。

パターンファイルを手動で削除する必要がある場合は、IWSVA の `/etc/iscan/` ディレクトリから検索してください。

第 5 章

アプリケーション制御

InterScan Web Security Virtual Appliance（以下、IWSVA) は、プロトコルによるアプリケーション使用率を管理する方法を提供し、アプリケーションの送受信トラフィックに関する有用なトラフィックの統計を表示します。

注意： アプリケーション制御機能を使用するには、IWSVA を透過ブリッジモード、透過ブリッジモード - 高可用性、またはプロキシ転送モードで配信する必要があります。詳細については、51 ページの「透過ブリッジモード」、52 ページの「透過ブリッジモード - 高可用性」、または 56 ページの「プロキシ転送モード」を参照してください。

本章で説明する内容には、次の項目が含まれます。

アプリケーション制御の概要

近年、インターネットベースのアプリケーションの人気は高まる一方で、単にブラウザを使用してネットサーフィンするだけにとどまりません。多くの企業では、企業の使用ポリシーがあっても、これらのアプリケーションの使用を防止または規制することができません。最近の調査では、75% ～ 80% の企業ユーザが、自社のコンピュータ使用ポリシーを無視していることがわかりました。深刻なリスクを回避するために、アプリケーション制御機能では、人気の高いインターネットアプリケーションを自動的に検出し、管理者がポリシーを使用してそれらのアプリケーションを管理できるようにするセキュリティテクノロジを提供します。

IWSVA は、カスタムクライアントを使用するアプリケーション (Skype、bitTorrent、P2P など) や、ブラウザ内で Web 2.0 テクノロジを活用するアプリケーション (SNS、Web メール、およびストリーミングメディアサイトなど) を含む、任意のポート上で実行される 1000 種類を超えるアプリケーションに対して可視性と管理を提供します。

注意： アプリケーション制御は、透過ブリッジモード、透過ブリッジモード - 高可用性、およびプロキシ転送モードで使用可能です。

アプリケーション制御を有効または無効にしても、すでに作成されたポリシーに影響はありません。それらのポリシーは HA ノード間で同期され、移行パッケージに含められます。

アプリケーション制御ポリシーおよび設定で処理を変更すると、それらは監査ログに記録されます。

アプリケーション制御ポリシーリスト

アプリケーション制御機能では、カテゴリ内のアプリケーションのすべての例で、単に許可またはブロックするオプション以上の処理が可能になります。この柔軟性が提供されているのは、多くの企業で、これらのアプリケーションの特定の機能がビジネスを行う上で役立つことがわかっているためです。アプリケーションを詳細に管理することで、Facebook などのアプリケーションを単にブロックしたり許可したりするだけでなく、アプリケーションを許可しながら新規投稿メッセージをブロックすることが可能になります。

管理者は、最もよく使用されるインスタントメッセージ 2 種を許可して、残りはブロックしたいと考えるかもしれません。P2P の場合、管理者は企業ネットワーク内の従業員同士でのファイルの転送は許可しますが、外部使用は禁止することを望むかもしれません。

アプリケーション制御ポリシーを作成すると、サポートされるインターネットベースのアプリケーションのカテゴリ内で、機能をきめ細かく管理することが可能になります。

アプリケーション制御ポリシーリストには、有効にされたものも無効にされたものも含め、システム上のすべてのポリシー (IPv4 および IPv6 アドレス用) が表示されます。[アプリケーション制御] → [ポリシー] に移動します。新規ポリシーを作成するには [追加] をクリックします。既存のポリシーを編集するにはそのポリシー名をクリックします。

- **アプリケーション制御を有効にする** — すべてのポリシーの有効ステータスをグローバルに制御します。個々のポリシーのステータスより優先されます。アプリケーション制御の有効化または無効化の後、[保存] をクリックします。アプリケーション制御を有効または無効にしても、すでに作成されたポリシーに影響はありません。それらのポリシーは HA ノード間で同期され、移行パッケージに含められます。
- **追加** — [ポリシーの追加] ウィザードを開きます。このウィザードでは、順を追って新規ポリシーを定義します。
- **優先順位** — 優先順位を設定します。2 つの競合するポリシーの範囲が重なる場合、優先順位が高い (1 に近い) ポリシーが適用され、他方のポリシーは無視されます。

注意： アプリケーション制御グローバルポリシーは、初期設定のポリシーです。すべてのユーザに自動的に適用されますが、優先順位は常に最も低くなります。より優先順位が高いポリシーがリストにある場合は、そちらが優先されます。

- **ポリシーの配信** — アプリケーション制御ポリシーの作成後または変更後、このボタンをクリックしてそのポリシーをただちに有効にします。これにより、ポリシー配信の時間間隔を待機する必要がなくなります。
- **アプリケーション検索** — 検索対象のアプリケーションプロトコル名を入力します。
- **詳細な処理検索** — アプリケーションの検索に適用する詳細な処理を 1 つ以上選択します。
- **処理** — 選択したアプリケーションに対して [許可]、[ブロック]、[次のポリシーに一致] のいずれかの処理を設定します。
- **スケジュール** — [スケジュールの選択] ドロップダウンリストをクリックして、現在のポリシーの予約期間を選択します。予約期間については、[管理] → [一般設定] → [予約期間] を参照してください。
- **カテゴリの折り畳みと展開** — 展開アイコン () を使用すると、すべてのアプリケーションカテゴリのコンテンツを表示できます。折り畳みアイコン () を使用すると、すべてのアプリケーションカテゴリを閉じることができます。
- **検索** — ポリシーの作成時に、検索フィールドを使用して、ポリシールールに追加したいアプリケーションを見つけることができます。

アプリケーション制御ポリシーを表示するには

1. [アプリケーション制御] → [ポリシー] に移動します。
2. 既存のポリシーの名前をクリックして、そのポリシーに関する詳細を表示します。

   アプリケーション制御グローバルポリシーは、初期設定のポリシーです。
3. ポリシーを追加するには、133 ページの「アプリケーション制御ポリシーの追加」を参照してください。

ポリシーの追加 : アカウントの選択

IWSVA には、HTTPS 復号化、高度な脅威保護、HTTP 検査、情報漏えい対策、および URL フィルタなどの動作について、初期設定のグローバルポリシーとゲストポリシーが用意されています。アプリケーション制御には、初期設定のグローバルポリシーのみがあります。

- **グローバルポリシー** — IWSVA を通してアクセスするクライアント用。
- **ゲストポリシー** — 特定のゲストアカウントを使用して、IWSVA 経由でプロキシ接続するクライアント、嘱託従業員、請負業者、および技術者用。

アプリケーション制御グローバルポリシーは、初期設定のポリシーです。

- **ポリシーを有効にする** — 個々のポリシーを有効または無効にします。ただし、アプリケーション制御のグローバル設定は、個々のポリシー設定より優先されます。
- IP **範囲** — このオプションは、アプリケーション制御ポリシーで影響を受ける IP アドレス (IPv4 および / または IPv6) の範囲を指定する場合に使用します。
- IP **アドレス** — アプリケーション制御ポリシーで影響を受ける IP アドレス (IPv4 または IPv6) を個別に指定する場合に使用します。
- IP **サブセット** — アプリケーション制御ポリシーで影響を受けるサブネット IP アドレスを指定する場合に使用します。
- **ユーザまたはグループ** (ユーザの識別が有効な場合) — アプリケーション制御ポリシーで影響を受けるユーザまたはグループを指定する場合に使用します。

注意 : この画面のオプションは、使用しているユーザの識別方法に応じて異なります。[IP アドレス] か、または LDAP 認証を有効にしている場合は [ユーザ / グループ名認証] のどちらかになります。ユーザの識別方法の設定とポリシー範囲の定義方法については、160 ページの「ユーザ識別方法の設定」と 170 ページの「ポリシーの範囲の設定」を参照してください。

- **追加** — アプリケーション制御ポリシーで影響を受ける IP アドレスのリストに、単一 IP アドレスまたは IP アドレスの範囲を追加する場合にクリックします。

アプリケーション制御ポリシーの追加

アプリケーション制御ポリシーを追加するには

1. [アプリケーション制御] → [ポリシー] に移動します。
2. ポリシーリストの上部にある [追加] リンクをクリックします。
3. わかりやすい [ポリシー名] を新しく入力します。これにより、ポリシーを覚えやすくなります。
4. また、[既存ポリシーからコピー] オプションをクリックして、ドロップダウンリストからポリシーを選択することで、既存のポリシーの設定に基づいて新規ポリシーを作成することもできます。
5. 単一の IP アドレス、IP アドレスの範囲、IP サブセット、またはユーザ / グループ名を入力して、影響を受けるユーザを示します。または、LDAP との統合がセットアップされている場合は、ユーザまたはグループの名前を選択します。
6. [追加] をクリックして、新規に作成した IP アドレス、IP アドレスの範囲、またはユーザ / グループ名を [種類] テーブルと [識別設定] テーブルに移動します。
7. 画面上部の [ポリシーを有効にする] チェックボックスをオンにして、作成したポリシーを有効にします。
8. 作業を続行するには、[次へ] をクリックします。
9. 指定したアカウントに適用するポリシーのルールをセットアップするには、134 ページの「アプリケーション制御ポリシールールの指定」を参照してください。

ポリシーの追加または編集 : アプリケーション制御ポリシーのルールの指定

次の 2 つの場所でポリシールールを追加または編集します。

- [アプリケーション制御] → [ポリシー] | [追加] → [アカウントの選択] → [ルールの指定]
- [アプリケーション制御] → [ポリシー] | [ポリシー名] | [ルール] (既存のポリシーを編集する場合)

アプリケーション制御ポリシーを追加するには、2 つの手順があります。まず、アカウントを作成して、ポリシーを適用するユーザを指定し、次にアプリケーション制御ルールをポリシーに割り当てます。

注意： ルール画面で特定のアプリケーションを見つけるには、検索フィールドを使用します。アプリケーションの詳細を表示するには、アプリケーション名をクリックします。そうすると、サポートされるアプリケーション、バージョン、その他の詳細の情報を含む別の画面が開きます。

アプリケーション制御ポリシールールの指定

アプリケーション制御ポリシーを編集するには、ポリシー名をクリックしてから [ルール] タブをクリックする必要があります。

- **ポリシーを有効にする** — 個々のポリシーを有効または無効にします。ただし、アプリケーション制御のグローバルポリシー設定は、個々のポリシー設定より優先されます。
- **アプリケーションカテゴリ** — アクセスを制限するプロトコルに対する処理を選択します。32 の論理グループに分けられた 420 以上のプロトコルがあります。特定のアプリケーション名を見つけるには、検索フィールドを使用します。
  - 「+」記号をクリックしてカテゴリを展開し、特定のプロトコルを選択します。
  - プロトコル名をクリックし、プロトコルの説明が表示される画面にアクセスします。

注意： ポリシーを作成するとき、現在の接続は新しいポリシーによってブロックされません。たとえば、ユーザが Skype にログオンしているときに管理者が Skype をブロックするポリシーを作成しても、ユーザは Skype を継続して使用できます。ただしユーザが一度ログオフすると、ポリシーが有効になるため、再び Skype にログオンすることができなくなります。

使用可能なフィルタ処理には次のものがあります。

- メールの送信を拒否
- ファイルのアップロードを拒否
- ファイルのダウンロードを拒否
- ファイルの転送を拒否
- メッセージの投稿を拒否
- ビデオ音声通話を拒否
- メディアの再生を拒否

「許可」、「ブロック」、「次のポリシーに一致」の処理はすべてのアプリケーションで選択でき、「ファイル転送」などその他の処理は一部のアプリケーションで使用できます。結果として、ポリシーの設定プロセスは次のようになります。

- **オプション** 1: アプリケーション検索のフィルタ
  - [アプリケーション検索] にアプリケーション名を入力して [検索] ボタンをクリックすると、アプリケーションがフィルタリングされます。
  - 処理を設定するアプリケーションを選択します。
  - [処理] に移動し、選択したアプリケーションに適用する処理を選択します。
- **オプション** 2: 詳細な処理検索のフィルタ
  - [詳細な処理検索] から処理を選択して [検索] ボタンをクリックすると、その処理を選択可能なアプリケーションがフィルタリングされます。
  - アプリケーション処理リストの [詳細オプション] で、処理を 1 つ以上選択して適用します。
- **許可** — ユーザアカウントはアプリケーションを通常どおり使用できます。管理者がこの設定を有効にしている場合、アプリケーション制御イベントが記録されます (詳細については、アプリケーション制御設定を参照してください)。
- **ブロック** — ユーザアカウントはこのアプリケーションを使用できません。このアプリケーションの一部として識別されるネットワークパケットは配信されません。この設定が有効にされている場合、アプリケーション制御イベントを記録できます。このイベントについてはログエントリも作成できます。
- **次のポリシーに一致** — 次のポリシー設定を使用します。この処理はグローバルポリシーおよびゲストポリシーには存在しません。
- **スケジュール** — 処理を適用するプロトコルの時間オブジェクトを選択します。制限する日数と時間は、[管理] → [一般設定] → [予約期間] で定義されます。(詳細については、377 ページの「予約期間」を参照してください)。選択したプロトコルにフィルタ処理を適用するには、[保存] をクリックします。

注意： 設定は HTTP サービスの再ロード後に適用されます。

- **備考** — ポリシーの目的や理由などの備考を入力します。この備考は簡単なメモとして、または今後この機能を管理する他のユーザへの連絡事項として使用できます。
- ルールリストの最後にある [保存] をクリックして、ポリシーリストに戻ります。
- ポリシーを配信する準備ができたら、ポリシーリストで [ポリシーの配信] をクリックします。

第 6 章

HTTP 設定

まず、HTTP トラフィックフローを制御する HTTP 設定を実行する必要があります。それから、InterScan Web Security Virtual Appliance（以下、IWSVA) を使用して、不正な HTTP/HTTPS ダウンロードの検索、URL のフィルタやブロック、アクセス割り当ての適用を実行します。IWSVA はネットワークに接続されている別のプロキシサーバと組み合わせて使用できます。また、IWSVA に搭載されているプロキシを使用するようにも設定できます。

注意： — WCCP の有効化と設定については、147 ページの「ネットワーク設定および負荷の処理」およびお使いの Cisco 製品のドキュメントを参照してください。
— 完全な透過性（透過ブリッジモード) の有効化と設定については、147 ページの「ネットワーク設定および負荷の処理」を参照してください。

本章で説明する内容には、次の項目が含まれます。

HTTP/HTTPS トラフィックフローの有効化

最初に、IWSVA 配置ウィザードによって配信モードが設定されます。設置後に配信モードを変更する場合には、[管理] → [配置ウィザード] 画面で変更します。

IWSVA を通じた HTTP/HTTPS トラフィックフローを有効 / 無効にするには

1. 管理コンソールから [システムステータス] を選択します。
2. 次のいずれかを選択します。
   - HTTP/HTTPS トラフィックがオフの場合は、[オン] のリンクをクリックすると有効になります。
   - HTTP/HTTPS トラフィックがオンの場合は、[オフ] のリンクをクリックすると無効になります。

HTTP/HTTPS トラフィックをオフにすると、クライアントは Web サイトや HTTP/HTTPS を経由するどのサービスにもアクセスできなくなります。

プロキシ設定および関連するその他の設定

設置後に配信モードを変更する場合には、[管理] → [配置ウィザード] 画面で変更します。

- **透過ブリッジモード** — IWSVA は、デバイス間に配置されたレイヤ 2 ブリッジとして動作し、クライアントと外部サービスとの間の HTTP、HTTPS、および FTP トラフィックを透過的に検索します。ネットワークデバイスへの設定の変更は不要です。透過ブリッジの設定は、HTTP トラフィックと FTP トラフィックの両方に適用されます。透過ブリッジが選択されると、FTP プロキシ設定は無効になります。初期設定では、SSL (HTTPS) トラフィックは IWSVA を通過しますが、検索は行われません。SSL で暗号化されたトラフィックを IWSVA で検索するには、検索する前にコンテンツを復号化するように HTTPS 復号化ポリシーを設定します。

  クライアントと IWSVA が同じセグメントにある場合、設定は不要です。同じセグメントでない場合、混合セグメントの設定について、次の考慮事項を参照してください。
  ネットワークデバイスと IWSVA デバイスが異なるネットワークセグメント上にある場合、IWSVA ルーティングテーブルを使用して IWSVA をデバイスにポイントします。2 つの NIC が必要です。
- **透過ブリッジモード - 高可用性** — NIC が 4 つ以上必要です。
- **プロキシ転送モード** — クライアントが不正な HTTP/HTTPS/FTP による脅威をサーバから受信しないように防ぐ設定です。最もよく使われる設定で、代表的な使用例はネットワークに接続する Web ユーザが不正なインターネットダウンロードを受信しないように防ぐ用法です。IWSVA と保護対象のクライアントは通常、同じ LAN 内にあります。

- **リバースプロキシモード** — 一般ユーザや個人ユーザが招いた攻撃や不正プログラムから Web サーバを保護するための設定です。
- **ICAP モード** — ICAP クライアントがネットワーク上にあり、検索のためトラフィックを IWSVA に通過させる場合、このトポロジを選択します。IWSVA は ICAP サーバとしての役割を果たします。
- **通常の透過モード** — L4 スイッチが HTTP/FTP トラフィックを IWSVA に移動させるように設定されています。このオプションでは IPv6 はサポートされていません。
- **WCCP モード** — WCCP を設定すると、ルータやスイッチの WCCP を有効にしてあるユーザが Web トラフィックや FTP トラフィックを IWSVA にリダイレクトして、高性能で拡張性のある冗長アーキテクチャを作成できるようになります。

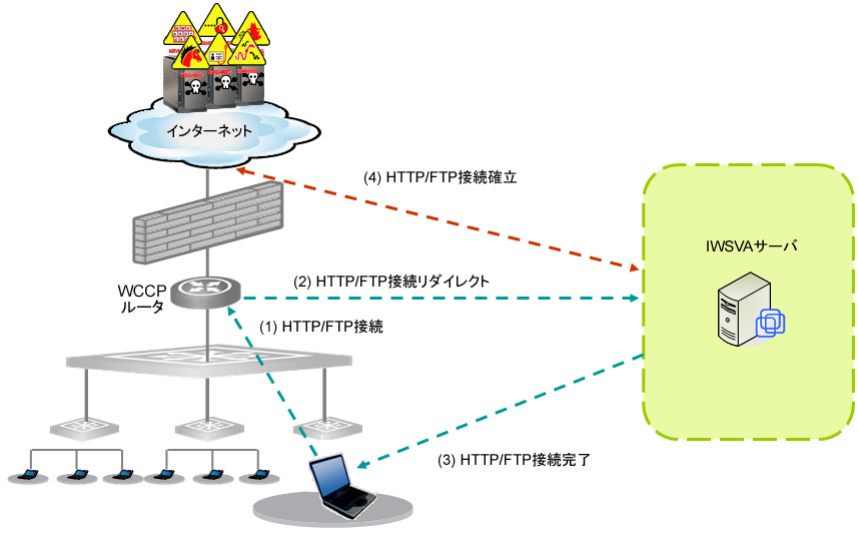


図 6-1.　WCCP 設定および Web トラフィックと FTP トラフィック

プロキシ設定

プロキシ設定には、次のような種類があります。

- 上位プロキシなし (スタンドアロンモード)
- 上位プロキシあり (依存モード)
- 通常の透過
- リバースプロキシ
- ICAP
- WCCP

上位プロキシなし (スタンドアロンモード)

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マイナス点は、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ユーザの協力が必要になります。

図 6-2.　上位プロキシなしのプロキシ転送

注意： IWSVA をスタンドアロンモードに設定する場合は、ネットワーク上の各クライアントで、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インターネット接続を設定する必要があります。

スタンドアロンの設置を設定するには

1. 管理コンソールから [管理] → [配置ウィザード] の順に選択します。

   配置ウィザードが表示されます。
2. [プロキシ転送モード] が選択されていることを確認します。[次へ] をクリックします。
3. [上位プロキシを有効にする] が選択されていないことを確認します。
4. [送信] ボタンが表示されるまで、[次へ] をクリックします。[送信] をクリックします。[閉じる] をクリックします。

上位プロキシあり (依存モード)

IWSVA は、ネットワーク上の別のプロキシサーバと組み合わせて動作するよう設定できます。この設定では、IWSVA がクライアントからの要求を別のプロキシサーバに渡し、その要求が要求側サーバに転送されます。

スタンドアロンモードと同様、依存モードのプロキシ設定でも、クライアントユーザがインターネット接続設定で IWSVA デバイスをプロキシサーバに設定する必要があります。上位プロキシを使用する利点は、上位プロキシサーバにコンテンツがキャッシュされるためパフォーマンスが向上することです。IWSVA は、プロキシ転送モード (有効な場合) でのみコンテンツのキャッシュを実行します。プロキシ転送モードが有効な場合、IWSVA はコンテンツのキャッシュを実行します。利用できる別のキャッシュサーバがあれば、そのキャッシュサーバをコンテンツキャッシュ用に設定できます。他のモードの場合や、プロキシ転送モードでコンテンツキャッシュが有効になっていない場合は、クライアントの要求ごとにインターネットサーバに問い合わせてコンテンツを取得する必要があります。上位プロキシを使用すると、プロキシサーバにキャッシュされた画面がすばやく表示されるようになります。

注意： 指定されたプロキシサーバを IWSVA が使用して、上位プロキシモードで動作するように設定する場合、そのプロキシサーバに対してアップデート用のプロキシ設定も設定することをお勧めします（117 ページの「プロキシ設定（アップデート用）」を参照）。特定の種類のアップデートイベントは、アップデートプロキシ設定を利用して重要な情報を取得します。プロキシ設定が正しく行われていないと、IWSVA はインターネットを介してそれらのサービスにアクセスできなくなります。

図 6-3.　上位プロキシを使用したプロキシ転送

注意： IWSVA が HTTP プロキシ転送モードで、上位プロキシが有効に設定されている場合、ファーミングサイトはブロックできません。

プロキシ転送モードで動作して上位プロキシを有効にするように IWSVA を設定する場合、サーバ IP アドレスの許可リストは有効になりません。サーバ IP アドレスの許可リストに設定したサーバのコンテンツは、検索もフィルタも実行されません。

上位プロキシと動作するよう IWSVA を設定するには

1. 管理コンソールから [管理] → [配置ウィザード] の順に選択します。

   配置ウィザードが表示されます。
2. [プロキシ転送モード] が選択されていることを確認します。[次へ] をクリックします。
3. [上位プロキシを有効にする] チェックボックスをオンにして、[プロキシサーバ] と [ポート番号] に上位プロキシの IP アドレス / ホスト名およびポート番号を入力します。
4. [送信] ボタンが表示されるまで、[次へ] をクリックします。[送信] をクリックします。[閉じる] をクリックします。

透過プロキシ

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多種多様な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。
- ホスト情報を格納しない HTTP 要求があった場合、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。
- IWSVA には不正なトラフィックの検索およびクリーンナップ対象となるクライアントの 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。

透過を有効にすると、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 要求を処理して検索できる利点があります。エンドユーザにとって便利な設定であるばかりでなく、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てしまうことを防ぐことができます。

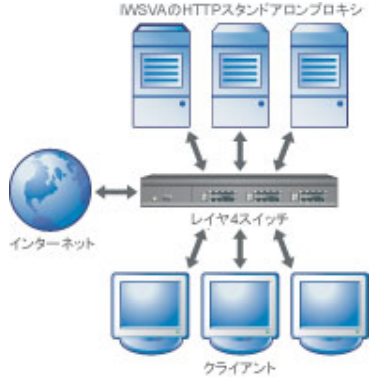


図 6-4.　透過を使用するプロキシ転送

注意： 通常の透過では、IWSVA が SSL (HTTPS) トラフィックを受け付けません。ポート 443 トラフィックを IWSVA にリダイレクトしないようルータを設定してください。

IWSVA を通常の透過モードで設定し、IWSVA サーバをレイヤ 4 スイッチに接続した場合、HTTP 待機ポートを 80 に設定してデータインタフェースで PING を有効にすると、ユーザは IWSVA を介してインターネットにアクセスできるようになります。

IWSVA では、通常の透過モードで HTTPS 復号化を使用することはできません。

この配信モードでは IPv6 はサポートされていません。

通常の透過を設定するには

1. 管理コンソールから [管理] → [配置ウィザード] の順に選択します。

   配置ウィザードが表示されます。
2. [通常の透過モード] を選択して、[次へ] をクリックします。
3. レイヤ 4 スイッチが使用するように設定されているポートと同じポートに [HTTP 待機ポート] 番号を変更します。

4. [送信] ボタンが表示されるまで、[次へ] をクリックします。[送信] をクリックします。[閉じる] をクリックします。

リバースプロキシ

IWSVA を使用して、クライアントから Web サーバにアップロードするコンテンツを検索することもできます。プロキシ転送検索設定またはリバースプロキシ検索設定のいずれかを使用して IWSVA を設置すると、アップロードとダウンロードの両方向のトラフィックが検索されます。

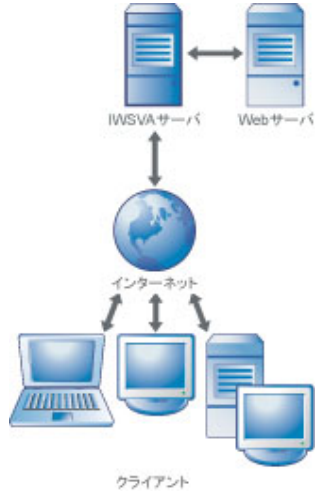


図 6-5. クライアントから Web サーバをリバースプロキシで保護

IWSVA をリバースプロキシとして設定するには

1. 管理コンソールから [管理] → [配置ウィザード] の順に選択します。

   配置ウィザードが表示されます。
2. [リバースプロキシモード] を選択して、[次へ] をクリックします。
3. HTTP 待機ポート番号、保護対象サーバの IP アドレスとポート番号を入力します。
4. 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。
5. [送信] ボタンが表示されるまで、[次へ] をクリックします。[送信] をクリックします。[閉じる] をクリックします。

注意： 配置ウィザードで [SSL ポートを有効にする] チェックボックスをオンにした場合、クライアントは SSL を使用して IWSVA と通信できますが、IWSVA と社内 Web サーバとの通信には SSL は使用されません。

注意： リバースプロキシモードでは HTTPS 復号化はサポートされていません。情報漏えい対策機能はこのモードではサポートされません。

プロキシに関する設定

プロキシ設定の種類を指定する以外に、以下のパラメータを設定することもできます。

- HTTP 待機ポート
- FTP over HTTP の匿名ログオンに使用するメールアドレス

HTTP 待機ポート

HTTP 検索を有効にする場合は、トラフィックが通過するよう HTTP ハンドラの待機するポート番号が正しく指定されていることを確認します。

注意： 透過ブリッジモードでは、HTTP 待機ポートを設定する必要はありません。

待機ポート番号を設定するには

1. IWSVA Web コンソールを開き、[管理] → [配置ウィザード] の順に選択します。
2. 必要なモードを選択して、[次へ] をクリックします。
3. [HTTP 待機ポート] 番号ボックスに、ポート番号を入力します（初期設定値は、ICAP が 1344、HTTP プロキシが 8080)。
4. [保存] をクリックします。

注意： IWSVA では、HTTPS 接続は HTTP 接続とは異なる形で処理されます。データが暗号化されているため、コンテンツを復号化するように HTTPS 復号化ポリシーを設定します。これにより、「通常」の HTTP トラフィックとしてフィルタポリシーおよび検索ポリシーを通過することができます。IWSVA では最初の CONNECT 要求を検証し、設定したパラメータと一致しない場合は拒否します。その例としては、対象となる URL がブロックリストにある場合、フィッシングパターンファイルに含まれている場合、使用ポート番号が許可されていない場合などがあります。

FTP over HTTP の匿名ログオンに使用するメールアドレス

FTP over HTTP を使用すると、ftp:// で始まる URL のハイパーリンクに Web 画面からアクセスできるようになります。また、ブラウザのアドレスバーに ftp:// で始まる URL を入力できるようになります。この種の URL にアクセスする際にユーザ名を省略すると、匿名ログオンとなり、ユーザのメールアドレスがパスワード文字列として通常使用され、FTP サーバに渡されます。

FTP over HTTP の匿名ログオンに使用するメールアドレスを設定するには

1. 管理コンソールから [管理] → [配置ウィザード] の順に選択します。
2. [通常の透過モード] を選択します。
3. 画面の指示に従って 配置ウィザードを実行し、プロキシ設定に進みます。[匿名 FTP over HTTP] の [使用するメールアドレス] を入力します。
4. [保存] をクリックします。

ネットワーク設定および負荷の処理

各 IWSVA インスタンスでサポートされるユーザの数は、多様な要因によって異なります。それらの要因には、IWSVA がインストールされたハードウェアの状況、ユーザごとに使用される同時セッションの平均数、各ユーザのセッションで使用される帯域幅、およびインターネットを同時に使用しているユーザの割合があります。通常、IWSVA サーバプラットフォームを強化すると、IWSVA の対応可能ユーザ数が増加します。

注意： 容量のサイズの詳細については、「IWSVA Sizing Guide」を参照してください。

次のモードでネットワーク上に IWSVA を設置できます。

- **透過ブリッジ** — 外部の（インターネットに接続されている) ネットワークデバイスから IWSVA の外部ポートへ、IWSVA の内部ポートから内部のネットワークデバイスへ、ケーブルを接続します。
- **プロキシ転送** — CLI で設定されたインタフェースから内部ネットワークデバイスへケーブルを接続します。
- ICAP — CLI で設定されたインタフェースを使用して、IWSVA を ICAP クライアントへ接続します。
- WCCP — IWSVA で WCCP を設定する際は、次の Cisco IOS のバージョンを使用することをお勧めします。
  - バージョン 12.2 (0) 〜 12.2 (22)。バージョン 12.2 ファミリで、リリース 23 以上は使用しないでください。
  - バージョン 12.3 (10) 以上。バージョン 12.3 ファミリで、リリース 0 〜 9 は使用しないでください。
  - IOS 12.4 (15) T3 以降を使用する必要があります。

IWSVA サーバの設定後に、IWSVA Web コンソールを開き、[管理] → [配置ウィザード] の順に選択して、該当する IWSVA 検索モードに設定します。

インターネットアクセス管理の設定

IWSVA には、クライアントの HTTP/HTTPS アクセスを管理できる設定がいくつか用意されています。この設定は、ユーザベースで設定できる検索ポリシーや URL フィルタポリシーとは別に設定できます。

- HTTP アクセスは、所定の IP/ ホスト名、IP 範囲、または IP サブセットを持つクライアントユーザに対して選択的に有効にできます。
- パフォーマンスを高めるため、クライアントユーザが「信頼する」サイトからコンテンツを要求した場合、指定した IP/ ホスト名を持つサーバ、または IP 範囲、IP サブセット内のサーバを検索から除外できます。
- IWSVA を通じてインターネットにアクセスするすべてのユーザに対し、ポートまたはポート範囲への HTTP および HTTPS 要求を選択的に許可または拒否できます。この機能は、特定の種類のインターネット転送を除外するのに便利な機能です。

クライアントとサーバの識別

クライアントの Web アクセスを管理したり信頼するサーバを設定するには、次の 3 種類の方法でクライアントとサーバを識別できます。

- IP/ ホスト名 — 単一の IP アドレスまたはホスト名。123.123.123.12 など。
- IP 範囲 — 一連の IP アドレス範囲に含まれるクライアント。123.123.123.12 ～ 123.123.123.15 など。
- IP サブセット — 指定したサブネット内の単一のクライアント。たとえば、IP に「192.168.1.0」、マスクに「255.255.255.0」と入力すると、192.168.1.x サブネット内のすべてのコンピュータが識別されます。このほか、マスクはビット数 (0 ～ 32) でも指定できます。

クライアント IP による設定

初期設定でネットワーク上のすべてのクライアントに IWSVA プロキシへのアクセスを許可できますが、明示的に指定したクライアントにだけ HTTP アクセスを許可するよう IWSVA を設定することもできます。社内でネットワークに接続している一部のユーザにインターネットアクセスを許可しない場合に、初期設定で HTTP アクセスをブロックするのに便利な方法です。

クライアントのアクセス管理では、IPv4 と IPv6 の両方のクライアントをサポートしています。ポリシーの選択時には、IPv4 と IPv6 の両方のポリシーが表示されます。クライアントのアクセス管理では、IPv4 でサポートされているものと同様に、単一の IPv6 アドレス、IPv6 アドレス範囲、または IPv6 マスクが受け入れられます。

HTTP アクセスをクライアント IP によって許可するには

1. 管理コンソールで [HTTP] → [設定] → [アクセス管理の設定] の順に選択します。

   透過ブリッジモードでは、宛先ポートおよび HTTPS ポートは利用できません。そのため、このモードのときには、[インターネットアクセス設定] 画面に [宛先ポート] タブおよび [HTTPS ポート] タブがありません。

2. [クライアント IP] タブがアクティブになっていることを確認します。
3. [クライアント IP に基づく HTTP アクセス管理を有効にする] チェックボックスをオンにします。
4. クライアントに HTTP アクセスを許可する方法を説明するオプションを [IP/ ホスト名]、[IP 範囲]、[IP サブセット] のいずれかから選択します。

注意： 単一の IP アドレスを指定してから単一の IP アドレスを含む IP アドレス範囲を指定する場合、ユーザが単一の IP アドレスの URL にアクセスを試みると IP アドレス範囲は無視されます。

クライアントの指定方法の詳細については、149 ページの「クライアントとサーバの識別」を参照してください。

クライアント IP または IP 範囲を削除するには、それに対応する隣の [削除] アイコンをクリックします。

5. [説明] フィールドにわかりやすい名前を入力します (40 文字以内)。
6. [追加] をクリックします。

   設定したクライアント IP アドレスが [クライアント IP] タブの下部にあるリストに追加されます。アクセス管理設定は、[クライアント IP] タブの下部にあるリストに表示された順序で評価されます。
7. [保存] をクリックします。

サーバ IP の除外リスト

ネットワークのパフォーマンスを高めるため、特定のサーバのコンテンツに対して検索とフィルタを省略するよう IWSVA を設定することができます。たとえば、イントラネットサーバをリバースプロキシ設定の IWSVA で保護している場合、コンテンツの安全性をほぼ確信でき、イントラネットサーバをサーバ IP アドレスの許可リストに追加することを検討することができます。

警告： **サーバ IP アドレスの許可リストに設定したサーバのコンテンツは、検索もフィルタも実行されません。緊密に管理しているコンテンツのサーバのみを追加することをお勧めします。**

ICAP モードでは、サーバ IP アドレスの許可リストは RESPMOD 要求にのみ適用されます。URL フィルタ、Web メールアップロードの検索、URL ブロックなどの REQMOD の動作には、ICAP 設置用のサーバ IP アドレスの許可リストは適用されません。

サーバのアクセス管理では、IPv4 と IPv6 の両方のクライアントをサポートしています。ポリシーの選択時には、IPv4 と IPv6 の両方のポリシーが表示されます。サーバのアクセス管理では、IPv4 でサポートされているものと同様に、単一の IPv6 アドレス、IPv6 アドレス範囲、または IPv6 マスクが受け入れられます。

サーバ IP アドレスの許可リストにサーバを追加するには

1. 管理コンソールで [HTTP] → [設定] → [アクセス管理の設定] の順に選択します。
2. [サーバ IP の除外リスト] タブがアクティブになっていることを確認します。
3. 信頼するサーバからコンテンツの検索やフィルタを除外する対象の指定方法を、[IP アドレス]、[IP 範囲]、[IP サブセット] のいずれかから選択します。

   クライアントの指定方法の詳細については、149 ページの「クライアントとサーバの識別」を参照してください。
4. [説明] フィールドにわかりやすい名前を入力します (40 文字以内)。
5. [追加] をクリックします。

   設定した信頼するサーバが [サーバ IP の除外リスト] タブの下部に表示されます。

   信頼するサーバ、サーバ範囲、または IP サブセットを削除するには、その横にある [削除] アイコンをクリックします。
6. アクセス管理の設定は、[サーバ IP の除外リスト] タブの下部にあるリストでの表示順序に従って評価されます。
7. [保存] をクリックします。

宛先ポートによる制限

IWSVA では、クライアントから接続できるサーバの宛先ポートを制限できます。拒否したポートへの HTTP 要求は転送されません。この方法を使用するとサーバを制約でき、ネットワークのセキュリティポリシーに違反したストリーミングメディアアプリケーションなどのサービスで使用するポートへのアクセスが拒否されます。

初期設定の設置後の設定では、ポート 80 (HTTP)、70 (Gopher)、210 (TCP)、21 (FTP)、443 (SSL)、563 (NNTPS)、および 1025 から 65535 までに対する要求を除き、すべての要求が拒否されます。

注意： Web ページで FTP リンクを開けるようクライアントに対して FTP over HTTP 接続を有効にするには、IWSVA からポート 21 の FTP サーバにコマンド接続を開く必要があります。これには、HTTP アクセス管理の設定でポート 21 へのアクセスを許可する必要があります。

各種アプリケーションおよびサービスで使用されるポートのリストについては、`http://www.iana.org/assignments/port-numbers` を参照してください。

クライアントから接続できる宛先ポートを制限するには

1. 管理コンソールで [HTTP] → [設定] → [アクセス管理の設定] の順に選択します。
2. [宛先ポート] タブがアクティブ化されていることを確認します。
3. 実行する [処理] を選択します。宛先サーバ上の特定ポートまたはポート範囲への接続を防止するには [拒否] を、許可するには [許可] を選択します。
4. [ポート] または [ポート範囲] を選択して、対応するポート番号を入力します。
5. [説明] フィールドにわかりやすい名前を入力します (40 文字以内)。
6. [追加] をクリックします。[宛先ポート] タブの最下部にあるリストに宛先ポートの制限が追加されます。

   アクセスを許可またはアクセスを拒否する宛先ポート番号または宛先ポート範囲を削除するには、その隣の [削除] アイコンをクリックします。
7. アクセス管理の設定は、[宛先ポート] タブの下部にあるリストでの表示順序に従って評価されます。

   リスト内に表示されるポートの順序を変更するには、[評価順] 列の上向き矢印または下向き矢印をクリックします。
8. [保存] をクリックします。

HTTPS ポートによる設定

IWSVA では、暗号化した HTTP トランザクションに使用するポートを制限できます。初期設定では、ポート 443 (初期設定の HTTPS ポート)、563 (暗号化されたニュースグループ用の初期設定ポート)、8443 (IWSVA セキュアコンソールの初期設定ポート)、および 1814 (Tomcat で使用されるキャプティブポータルページ用の初期設定ポート) での HTTPS 接続のみ許可されます。

注意： IWSVA 本体で接続しながら HTTPS 経由で Web コンソールにアクセスする必要がある場合は、IWSVA のセキュリティで保護されたコンソールポート番号 (初期設定では 8443) へのアクセスを許可します。

暗号化した HTTP トランザクションのトンネルに使用できるポートを制限するには

1. 管理コンソールで [HTTP] → [設定] → [アクセス管理の設定] の順に選択します。
2. [HTTPS ポート] タブをアクティブにします。
3. [HTTPS ポート] を [拒否] または [許可] のいずれかに選択します。
4. [ポート] または [ポート範囲] を選択して、対応するポート番号を入力します。

5. [説明] フィールドにわかりやすい名前を入力します (40 文字以内)。
6. [追加] をクリックします。宛先ポート制限が [HTTPS ポート] タブの下部にあるリストに表示されます。

   設定した HTTPS ポートアクセス制限を削除するには、削除するポート番号またはポート範囲の隣の [削除] アイコンをクリックします。
7. アクセス管理設定は、[HTTPS ポート] タブの下部のリストに表示された順序に評価されます。リスト内に表示されるポートの順序を変更するには、[評価順] 列の上向き矢印または下向き矢印をクリックします。
8. [保存] をクリックします。

第 7 章

ポリシーとユーザ識別方法

Trend Micro InterScan Web Security Virtual Appliance（以下、IWSVA）では、ネットワーク上の個人やグループごとに異なるアプリケーション制御、HTTPS 復号化、HTTP ウイルス検索、HTTP 検査、情報漏えい対策、URL フィルタ、およびアクセス割り当てのポリシーを適用できます。このように、潜在的な不正プログラムコードの処理方法、Web コンテンツの特定カテゴリの表示方法、または Web 閲覧で必要以上の帯域幅の使用しない方法について、ビジネスニーズに基づいてセキュリティポリシーをカスタマイズできます。

本章で説明する内容には、次の項目が含まれます。

ポリシーの仕組み

アクセスすべきファイル種類やインターネットリソースに応じて、ネットワーク上のユーザやグループごとに異なるセキュリティ設定を適用できます。IWSVA ポリシーは、HTTP/HTTPS 検索ポリシーや URL フィルタポリシーなどと同様に、IPv6 クライアントおよびサーバに適用できます。すべてのユーザ識別方法が、IPv6 環境（クライアント IP が IPv6) でも機能します。クライアントおよびサーバのアクセス管理では、IPv6 ホストをサポートする必要があります。次に、セキュリティポリシー種類別にいくつかの例を示します。

- **ウイルス検索 —** 組織の使用許可ポリシーを使用すると、クライアントによるオーディオ / ビデオのダウンロードを全体的に禁止できます。しかし、社内にはこの種のファイルを正規の業務目的で受信すべきグループもあります。各種のウイルス検索ポリシーを設定すれば、HTTP ウイルス検索ポリシーの異なるファイルブロックルールを社内のグループごとに適用できます。
- URL **フィルタ —** 社員に業務関連以外のネットサーフィンを行わせないよう、「ギャンブル」カテゴリ内の Web サイトへのアクセスをブロックするグローバルポリシーを設定できます。しかし、営業部門には、ゲーム業界の見込み客について調査できるよう、この種のサイトへのアクセスを許可するポリシーを別途設定すべき場合もあります。選択された事前定義のカテゴリに加えて、URL フィルタポリシーに適用する新しい Web カテゴリを作成することもできます。
- HTTPS **復号化 —** HTTPS 接続で暗号化されたコンテンツを検索するには、アクセス先のサイトの種類に基づいて HTTPS 復号化ポリシーを設定します。コンテンツが復号化されると、「通常の」HTTP トラフィックとして IWSVA 上のフィルタポリシーおよび検索ポリシーを通過することができます。HTTPS 復号化ポリシーにより、HTTPS トラフィックに埋め込まれているセキュリティ上の脅威を防ぎます。

  アカウントフィールドでは IPv6 アドレスがサポートされます。任意の IPv6 ホストに 1 つのルールを定義すると、クライアントが IWSVA を介して HTTPS サイトにアクセスしたときにこのポリシールールがトリガされます。

  - ポリシーの選択時には、IPv4 と IPv6 の両方のポリシーが表示されます。
  - [アカウント] で入力可能なアカウントエントリは、IPv4 でサポートされているものと同様に、単一の IPv6 アドレス、IPv6 アドレス範囲、または IPv6 マスクです。
- **アクセス割り当て —** IWSVA を使用すると、組織で使用する帯域幅を制御できるよう、クライアントが 1 日、1 週間、および 1 か月の間にダウンロードできるファイル容量を制限するアクセス割り当てポリシーを設定できます。正規の業務目的でインターネットを頻繁に閲覧しなくてはならない社員については、無制限にインターネットにアクセスできるポリシーを別途設定できます。

- **アプリケーション制御** — アプリケーション制御ポリシーでは、人気の高いインターネットベースのアプリケーションを自動的に検出するセキュリティテクノロジが使用され、管理者はそれらのアプリケーションの使用を管理できます。アプリケーション制御ポリシーでは、サポートされるインターネットベースのアプリケーションのカテゴリ内で、機能をきめ細かく管理することが可能になります。IWSVA では、単に許可またはブロックするオプション以上の処理が可能になります。なぜなら、多くの企業ではこれらのアプリケーションの特定の機能はビジネスを行う上で役立つことがわかっているからです。
- **HTTP 検査** — HTTP 検査により、管理者は動作を識別して、HTTP メソッド、URL、およびヘッダに基づいて Web トラフィックをフィルタできます。また、フィルタを作成するか、初期設定のフィルタを使用して Web トラフィックを識別したり、フィルタをインポートおよびエクスポートしたりすることもできます。トラフィックが識別されたら、IWSVA は、特定のトラフィックに対する適切な処理を決定するポリシー設定に従ってそのトラフィックを管理できます。
- **情報漏えい対策** — 情報漏えい対策では、デジタル資産と呼ばれる組織の機密データを不注意による開示や意図的な漏えいから守ります。IWSVA はファイルの内容を検索し、特定のデータについて送信トラフィックを確認します。
- IWSVA は、除外する URL またはファイル名のリストをポリシー別に設定および適用できる柔軟性を備えています。

特定のユーザに適用するカスタムポリシーを定義できるほか、IWSVA には基準レベルの HTTPS 復号化、HTTP ウイルス検索、HTTP 検査、情報漏えい対策、および URL フィルタを提供するグローバルポリシーとゲストポリシーの 2 つの初期設定ポリシーがあらかじめ用意されています。

注意： IWSVA では、キャプティブポータルおよび LDAP が有効になっているか、プロキシ転送モードでゲストユーザログインが有効になっている場合にのみゲストポリシーがサポートされます。

初期設定のグローバルポリシーとゲストポリシー

IWSVA には、HTTPS 復号化、高度な脅威保護、HTTP 検査、情報漏えい対策、アプレット /ActiveX 対策、および URL フィルタなどの動作について、初期設定のグローバルポリシーとゲストポリシーが用意されています。アプリケーション制御には、初期設定のグローバルポリシーのみがあります。

- **グローバルポリシー** — ゲストポリシーで制御されるクライアントを除く、IWSVA 経由でアクセスするすべてのクライアント用。

- **ゲストポリシー** — 特定の「ゲストアクセス」オプションを使用して、IWSVA 経由でプロキシ接続するクライアント、嘱託従業員、請負業者、および技術者用。

  ゲストアカウントは初期設定で無効になっています。ゲストアカウントを有効にするには、LDAP を無効にしてからのみ、[管理] → [一般設定] → [ユーザの識別] → [認証方法] → [キャプティブポータル] → [ゲストログインの許可] に移動します。159 ページの「ゲストアカウントの有効化」を参照してください。

注意： ゲストポリシー機能は、ユーザ識別方法として LDAP の「ユーザ / グループ名認証」機能を使用するよう管理者が IWSVA を設定しているか、プロキシ転送モードでゲストユーザログインが有効になっている場合に使用できます。請負社員や来社したベンダーなど、社内のディレクトリサーバ内にアカウントを持たないユーザでも Web にアクセスできるように、管理者は 1 つの「ゲストアクセス」ボタンを提供することができます。

ゲストポリシーについて

ゲストポリシーは、ゲストユーザに適用される唯一のポリシーです。

「ユーザ / グループ名認証」によるユーザ識別方法を有効にする方法については、162 ページの「ユーザ / グループ名認証」を参照してください。

ゲストポートの有効化

プロキシ転送モードで配置ウィザードを使用して、ゲストポートを有効化します。

ゲストポートを有効にするには

1. [配信モード] 画面で [プロキシ転送モード] ラジオボタンを選択します。

   詳細については、56 ページの「プロキシ転送モード」を参照してください。
2. [次へ] をクリックします。
3. [ゲストユーザログインを有効にする] を選択して、ポート番号 8081 (初期設定の値) を使用します。
4. [次へ] をクリックします。
5. その他の初期設定のプロキシ転送設定を変更せずに、[保存] をクリックします。

ゲストアカウントの有効化

LDAP ディレクトリにアカウントを持たないネットワークユーザにインターネット接続を許可してゲストポリシーを適用するには、[ユーザの識別] → [認証方法] で設定を有効にします。

ゲストアカウントを有効にするには

1. [ユーザの識別] 画面から、[キャプティブポータル（IWSVA によってブラウザに提供されるカスタム認証ページ)] オプションを選択して、[ゲストログインの許可] チェックボックスをオンにします。(認証されていないユーザには常に [キャプティブポータル] 画面が表示されます)。
2. [保存] をクリックします。

ポリシークエリ

新しいポリシーがクライアントに追加された場合に、管理者はそのポリシーが正しく機能していないことを検出することがあります。また、クライアントサーバ上でどのポリシーが現在機能しているか判断したい場合があります。ポリシークエリ機能は、クライアント上でいくつのポリシーが現在機能しているか判別できるように設計されています。

ポリシークエリを使用するのは、検索ボックスにクライアントの IP アドレスまたはユーザ名を入力して [検索] アイコンをクリックするのと同様に簡単です。

[検索] アイコンをクリックした後、IWSVA によって、ポリシータイプごとにグループ化され、順番に並べ替えられたクエリ結果が提供されます。この機能は、IWSVA で使用されているポリシーの概要または要約、および違反ログに書き込まれたポリシーのリストが必要な管理者に適しています。

ポリシーごとに [備考] フィールドがあり、管理者はそのフィールドを使用して、ポリシーに関する詳細情報を保存します。

ポリシーの配信

ポリシーの設定後、[保存] をクリックすると設定がデータベースに書き込まれます。[ポリシーの配信] をクリックすると、新しいポリシー設定がただちに適用されます。クリックしない場合は、[管理] → [一般設定] → [ポリシー配信] 画面の [ポリシー配信設定（分)] で指定した時間が経過後、IWSVA がデータベースから情報を読み取った時点で、ポリシーの変更内容が有効になります。

ユーザ識別方法の設定

アプリケーション制御、HTTPS 復号化、HTTP ウイルス検索、HTTP 検査、情報漏えい対策、URL フィルタ、およびアクセス割り当てポリシーの範囲を定義するには、IWSVA によるクライアントの識別方法を設定する必要があります。ユーザ識別方法を選択することで、ログファイルとレポート内の影響を受けたシステムに対するセキュリティイベントの追跡方法も決まります。

IWSVA には、クライアントを識別して適切なポリシーを適用するのに次の 3 種類のユーザ識別方法があります。

- IP アドレス (初期設定)
- ユーザ / グループ名認証 (LDAP)

次の表は、IWSVA でサポートされている、さまざまな配信モードでのユーザ識別方法を示しています。

表 7-1. さまざまな配信モードでサポートされているユーザ識別方法

	IP アドレス	**ユーザ / グループ名認証**
透過ブリッジモード	使用可	使用可
プロキシ転送モード (スタンドアロン / 依存)	使用可	使用可
WCCP モード	使用可	使用可
通常の透過モード	使用可 (ソース NAT が無効な場合)	使用不可 **注意** : 標準認証とキャプティブポータルは動作しますが、あるエンドユーザがユーザ名とパスワードを入力すると、その他のユーザが認証を通過し、同じユーザの同じ IWSVA レコードを使用します。キャプティブポータルおよび Cookie モードを有効にします。
リバースプロキシモード	使用可	使用不可

表 7-1. さまざまな配信モードでサポートされているユーザ識別方法 (続き)

	IP アドレス	ユーザ / グループ名認証
ICAP モード	使用可	使用可 **注意** : 標準認証のみがサポートされます。キャプティブポータルの認証はサポートされません。

IP アドレス

IP アドレスは初期設定の識別オプションで、以下の条件が必要です。

- DHCP では DHCP リースの有効期限が切れることによって IP アドレス識別が不正確になるため、クライアント IP アドレスを DHCP 経由で動的に割り当てていないこと。
- 影響を受けるシステムと IWSVA の間のネットワークパスでネットワークアドレス変換 (NAT) を実行していないこと。

ローカルネットワークがこの条件を満たしていれば、IP アドレスによるユーザ識別方法を使用するように IWSVA を設定できます。

IP アドレスで識別する場合、検索ポリシーの範囲は、ポリシーの追加または編集時に IP アドレス範囲または指定 IP アドレスを定義することで決まります。

IP アドレスによるユーザ識別方法を有効にするには

1. 管理コンソールから、[管理] → [一般設定] → [ユーザの識別] | [ユーザの識別] の順にクリックします。
2. [Active Directory の設定] で [なし] を選択します。
3. [保存] をクリックします。

クライアント登録ユーティリティ

[ホスト名 (変更された HTTP ヘッダ)] のユーザ識別オプションを使用するには、クライアントが IWSVA に接続してインターネットにアクセスする前に、トレンドマイクロが提供するプログラムを Windows クライアントごとに実行する必要があります。このプログラムファイルは `register_user_agent_header.exe` で、/usr/iwss/bin (IWSVA コンピュータ) に配置されています。このプログラムは、ローカル Windows ドメインにログオンスクリプトから呼び出すとクライアントに効果的に配信できます。

このプログラムは、次のレジストリエントリを修正することにより機能します。

32ビット版Windows [`HKLM \ Software \ Microsoft \ Windows \ CurrentVersion \ Internet Settings \User Agent \ Post Platform`]

64 ビット版 Windows [`HKLM \ Software \ Wow6432Node \ Microsoft \ Windows \ CurrentVersion \Internet Settings \ User Agent \ Post Platform`]

このレジストリエントリは、Internet Explorer の User-Agent HTTP ヘッダに含まれています。識別情報は、各種ログファイルの [User ID] 列に記録されます。これによって、クライアントの MAC アドレスと HTTP 要求を作成したコンピュータ名を含めるよう Windows 設定値が変更されます。MAC アドレスは固有かつ追跡可能な識別方法であり、コンピュータ名はもう 1 つの有用な識別子です。

`register_user_agent_header.exe` ユーティリティを実行すると、次のキーの下に新しいレジストリ値が作成されます。

32ビット版Windows [`HKLM \ Software \ Microsoft \ Windows \ CurrentVersion \ Internet Settings \User Agent \ Post Platform`]

64 ビット版 Windows [`HKLM \ Software \ Wow6432Node \ Microsoft \ Windows \ CurrentVersion \Internet Settings \ User Agent \ Post Platform`]

`IWSS31:<` **ホスト名** `>/<MAC` **アドレス** `>` という新しいレジストリ値は暗号化されます。ここで、**<ホスト名>** と **<MAC アドレス>** は、ユーティリティを実行したクライアントのホスト名と MAC アドレスです。

ユーザ / グループ名認証

IWSVA では、次の LDAP サーバと統合し、LDAP v2 プロトコルと LDAP v3 プロトコルの両方をサポートできます。

- Microsoft Active Directory for Windows Servers 2003、2008、および 2012
- Linux OpenLDAP Directory 2.2.16、2.3.39、または 2.4.11

LDAP 認証方法

[ユーザ / グループ名認証] 方法を有効にすると、インターネットにアクセスする前に、クライアントでネットワークのログオン認証情報を入力するよう求められます。

次の表は、サポートされている各 LDAP サーバで使用できる LDAP 認証情報をまとめたものです。

表 7-2.　サポートしている LDAP サーバで使用できる認証方法

	Kerberos	シンプル認証	NTLM
Microsoft Active Directory for Windows Servers 2003、2008、および 2012	使用可	使用不可	使用可
Linux OpenLDAP 2.2.16、2.3.39、2.4.11	使用可	使用可	使用不可

注意： サポートしている LDAP サーバの最新の情報は http://www.go-tm.jp/iwsva/req をご覧ください。

LDAP の通信フロー

クライアントからインターネットコンテンツを要求すると、ネットワーク認証情報の入力が求められます。詳細認証では、Kerberos サーバを安全なパスワードの集中保管場所として使用します。そのため、安全性が高まるという利点があります。Kerberos サーバでクライアント認証を実行すると、Kerberos サーバによって交付され、特別に暗号化された「チケット」が、IWSVA とインターネットのアクセスに使用されます。

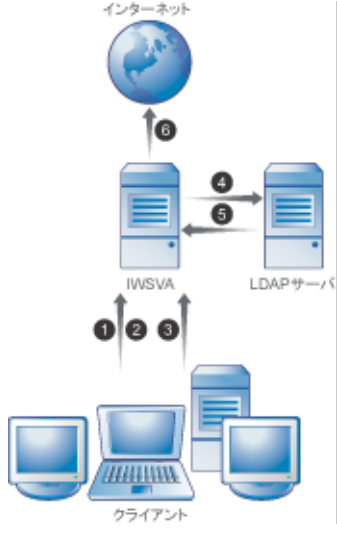


図 7-1.　Kerberos 認証による LDAP 通信フロー

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。

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 設定を行う必要があります。IE 7.0 以降では、初期設定で自動認証が有効になっています。

IWSVA では、次の認証方法での Internet Explorer の自動認証がサポートされます。

- 単一のドメイン (LAN または 802.11)

- 複数のドメイン環境で有効なグローバルカタログ（LAN または 802.11）

IE で自動認証を有効にするには

1. クライアントコンピュータで Internet Explorer を開き、[ツール] → [インターネット オプション] の順にクリックして、[セキュリティ] タブをクリックします。
2. [ローカル イントラネット] をクリックして、[レベルのカスタマイズ] をクリックします。
3. [イントラネット ゾーンでのみ自動的にログオンする] を選択して、[OK] をクリックします。
4. [サイト] をクリックして、[イントラネットのネットワークを自動的に検出する] を選択し、[詳細設定] をクリックします。
5. [ローカル イントラネット] 画面で、IWSVA ホスト名を入力して [追加] をクリックします。
6. 設定を保存します。

Firefox で自動認証を有効にするには

1. クライアントコンピュータで Firefox を開き、アドレスフィールドに「about:config」と入力します。
2. [検索] フィールドに「ntlm」と入力します。
3. [network.automatic-ntlm-auth.trusted-uris] をダブルクリックします。
4. ポップアップ画面が表示されます。IWSVA サーバのホスト名を入力して、[OK] をクリックします。

注意： その他のサポートされている Web ブラウザおよび上述されていない認証方法については、ユーザはポップアップ画面でログオン情報を入力する必要があります。

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。

- 透過ブリッジモードまたは透過 WCCP モードの設定時に、配置ウィザードで有効なホスト名を割り当てる必要があります。社内 DNS サーバにも同じホスト名が入力されている必要があります。

- 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。これは初期設定です。この設定は、透過モードでの認証を有効にする前に、有効にしておく必要があります。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。キャッシュタイムアウトの値を小さくするには、CLI で `configure module ldap ipuser_cache <interval>` コマンドを使用して、キャッシュの間隔を短く設定します。
- 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. ドメインコントローラまたは Windows クライアントのクエリを有効にします。これらのオプションのいずれかを有効にすると、IWSVA ではドメインコントローラまたはクライアントのクエリを通してユーザ名とドメイン名が取得されるため、認証は必要なくなります。
  b. 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。
  c. 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。
  d. 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 / 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 (IE) 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、Internet Explorer (IE) 設定を行う必要があります。IE では、初期設定で自動認証が有効になっています。

LDAP 設定

LDAP ユーザ / グループ名を認証およびポリシー設定に使用する場合、社内 LDAP サーバを使用するように IWSVA のユーザ識別機能を設定する必要があります。

注意： LDAP ディレクトリにアカウントを持たないネットワークユーザにゲストポリシーを適用するには、[認証方法] でゲストアカウントを有効にします。ゲストアカウントを有効にする方法の詳細については、159 ページの「ゲストアカウントの有効化」を参照してください。

ユーザ / グループ名認証方法を使用するよう IWSVA を設定するには

1. 管理コンソールから、[管理] → [一般設定] → [ユーザの識別] | [ユーザの識別] タブの順にクリックします。
2. LDAP サーバのドメイン名、サービスアカウント（AD UPN（ユーザプリンシパル名））、およびパスワードを入力し、[接続のテスト] をクリックして LDAP 接続を検証します。
3. [保存] をクリックして、設定を保存します。
4. 複数の LDAP ドメインまたは複数の LDAP サーバの種類が存在する場合は、[詳細（その他の / 複数の LDAP サーバ)] を選択します。
5. LDAP ドメイン名を入力します。
6. LDAP サーバが Microsoft Active Directory である場合は、ドメイン設定の検出と自動入力に「自動検出」を使用できます。認証情報として、少なくとも LDAP サーバに対する読み取り権限を持つ [管理者アカウント] と [パスワード] を入力します。ドメインが us.example.com の場合、次のようになります。
   - Microsoft Active Directory には、UserPrincipalName を管理者アカウントとして使用します。例 : NT_Logon_ID@us.example.com
   - OpenLDAP には、識別名 (DN) を管理者アカウントとして入力します。例 : `uid=LOGON_ID,ou=People,dc=us,dc=example,dc=com`
7. LDAP サーバが Microsoft Active Directory である場合は、LDAP 暗号化を設定します。
   - LDAP 暗号化を使用しない場合は、[LDAP 暗号化] で [なし] を選択します。
   - LDAP 暗号化を使用する場合は、[LDAP 暗号化] で [LDAPv3 StartTLS 拡張] または [LDAPS (LDAP over SSL)] を選択します。

> **注意：** StartTLS が LDAP 暗号化に選択されている場合、LDAP ポート番号は 389 または 3268 である必要があります。
> [LDAPS (LDAP over SSL)] が選択されている場合、使用される待機ポート番号は 636 または 3269 のどちらかになります。

8. 選択した LDAP サーバで使用する [待機ポート番号] を入力します (初期設定 = 389)。ネットワークに Active Directory サーバが複数あり、グローバルカタログ (GC) ポートを有効にしている場合は、待機ポートを 3268 に変更します。

> **注意：** Active Directory でグローバルカタログを有効にする場合は、ポート 3268 経由の通信を許可するようファイアウォールを設定する必要がある場合があります。

9. [LDAP サーバのホスト名] を完全修飾ドメイン名 (FQDN) で入力します。
10. [ベース識別名] を入力して、IWSVA で LDAP 検索を開始するディレクトリツリーのレベルを指定します。

    ベース識別名は、企業の DNS ドメインコンポーネントから取得されます。たとえば LDAP サーバが `us.example.com` の場合は、「DC=example, DC=com」と入力します。

    Active Directory サーバでグローバルカタログ (GC) ポートを有効にしている場合は、グローバルカタログを有効にした Active Directory のルートドメインを使用します。たとえば、dc=example,dc=com となります。
11. LDAP 認証方法に [シンプル]、[ダイジェスト - MD5]、[Kerberos] のいずれかを選択します。

    詳細認証を使用するには、さらに次のパラメータも設定します。

    - 初期設定のレルム
    - 初期設定のドメイン
    - **鍵発行局 (KDC) および管理サーバ** — Kerberos 鍵発行サーバのホスト名。Active Directory を使用している場合、通常は Active Directory サーバのホスト名と同じです。
    - **鍵発行局 (KDC) ポート番号** — 初期設定ポート = 88

      Internet Explorer を介した異なるフォレスト上の鍵発行局 (KDC) の認証に NTLM を使用している場合、または Active Directory でのリフェラル追跡に IWSVA を使用している場合は、[プロキシ接続で HTTP 1.1 を使用する] チェックボックスをオンにすることをお勧めします。この設定は、Internet Explorer で [ツール] → [インターネット オプション] → [詳細設定] の順に選択すると参照できます。この設定を有効にすると、キープアライブ接続が停止されるのを防ぎます。NTLM を使用できるのは、Microsoft Active Directory だけですので注意してください。

12. ホストを LDAP 認証プロセスから除外するように [認証の許可リスト] を設定します。

    たとえば、インターネットにアクセスするアプリケーションサーバがある場合、サーバによる認証を要求することなくアクセスを許可するには、LDAP 認証の許可リストにサーバの IP アドレスを追加します。
    IWSVA は IP アドレスベースのポリシー設定のみを適用し、ユーザ / グループ名のチェックを省略します。
    IWSVA は、IPv6 からの LDAP クエリを IPv4 の場合と同様にサポートします。LDAP クライアントの許可リストでは、IPv6 アドレスも IPv4 と同様にサポートします。[LDAP 承認リクエスト] ダイアログボックスでは、ポート 9090 の IPv4 および IPv6 をサポートします。IWSVA は、IWSVA の IPv4 アドレスまたは IPv6 アドレスの認証ダイアログボックスを、クライアントの IP アドレスバージョンに基づいて自動的にクライアントにリダイレクトできます。

    - クライアントが IPv4 アドレスを使用する場合、IWSVA は、リダイレクト要求を IWSVA の IPv4 アドレスとともに送信する必要があります。
    - クライアントが IPv6 アドレスを使用する場合、IWSVA は、リダイレクト要求を IWSVA の IPv6 アドレスとともに送信する必要があります。

13. 情報が正しく入力されたかどうか、および設定した LDAP サーバと IWSVA が通信できるかどうかを検証するには、[ユーザの識別設定] 画面で [LDAP 接続のテスト] をクリックします。

    LDAP サーバと正常に接続されたことを示すメッセージが表示されます。

14. [保存] をクリックします。

注意： LDAP サーバが正常に追加されると、[LDAP サーバと同期する] という新しいボタンが表示されます。このボタンをクリックすると、ユーザグループ情報の手動同期を実行できます。

クロスドメインの Active Directory オブジェクトクエリ

Microsoft Active Directory を使用する際にグローバルカタログポート (3268) を IWSVA の LDAP 通信ポートに使用することをお勧めします。ポート 3268 を使用すると、クロスドメイングループをネスティングしたオブジェクトクエリが有効になります。これは、あるドメインのオブジェクトの属性が、別のドメインにある他のオブジェクトを参照している場合に該当します (たとえば、同じフォレスト上の異なるドメインにいるクロスドメインユーザまたはグループメンバーシップなど)。

クロスドメイングループオブジェクトの属性を検索するには、同じ Active Directory フォレスト内のクロスドメイングループメンバーがグローバルカタログに含まれるよう、「ユニバーサル」グループ範囲でグループを作成する必要があります。ユニバーサルグループ範囲を使用したグループの作成では、クロスドメインクエリも実行できます。グローバルカタログが有効になっている場合は、グローバルグループポリシーを作成したり使用したりしないようにします。

注意： IWSVA がポート 3268 を待機に使用するよう設定するには、IWSVA が使用する Microsoft Active Directory サーバでグローバルカタログを有効に設定する必要があります。

メンバー属性はすべてのグループタイプのグローバルカタログに複製されるわけではありません。また、後方リンクのメンバー所属先属性の値は前方リンクのメンバー属性を参照して導き出されます。このため、グループメンバーの検索結果とメンバー所属先グループが一致しない場合があります。検索結果は、グローバルカタログ（ポート 3268）またはドメイン（ポート 389）のどちらを検索するのか、ユーザの所属先グループの種類（グローバルグループかドメインローカルグループか）、ユーザがローカルドメイン外のユニバーサルグループに所属しているかどうかによって異なります。

ポリシーの範囲の設定

アプリケーション制御、HTTPS 復号化、HTTP ウイルス検索、HTTP 検査、情報漏えい対策、URL フィルタ、およびアクセス割り当てポリシーの設定の最初の手順はすべて同じです。ポリシーを適用するクライアントユーザを識別することで、ポリシーの適用範囲を設定します。ここでは、IP アドレスとユーザ / グループ名認証によるユーザ識別方法を使用してアカウントを選択する方法について説明します。

この手順は次のとおりです。

- 170 ページの「IP アドレスを使用したポリシー設定」
- 171 ページの「LDAP を使用したポリシー設定」

注意： ユーザ / グループ名認証によるユーザ識別方法を IWSVA に設定した場合でも、IP アドレスまたは IP アドレス範囲を入力すれば、いつでもクライアントを指定できます。

ポリシーを追加してポリシー適用範囲を設定する前に、ユーザ識別方法を設定します。詳細については、160 ページの「ユーザ識別方法の設定」を参照してください。

IP アドレスを使用したポリシー設定

ユーザ識別方法の設定には関係なく、クライアントの IP アドレスを使用したポリシー設定が最も簡単な識別方法で、これは常に使用することができます。

IP アドレスでポリシー適用範囲を設定するには

1. 管理コンソールから [HTTP] をクリックし、作成するポリシーの種類 (HTTPS 復号化ポリシー、高度な脅威保護ポリシー、HTTP 検査ポリシー、情報漏えい対策ポリシー、URL フィルタポリシー、またはアクセス割り当てポリシー) を選択します。

   注意： アプリケーション制御ポリシーには、[アプリケーション制御] → [ポリシー] メニューからアクセスします。

2. 選択したポリシー種類の画面で [追加] をクリックします。
3. わかりやすい [ポリシー名] を新しく入力します。

   「エンジニア向けウイルスポリシー」や「研究者向け URL フィルタポリシー」など、ポリシーを適用するユーザやグループへの参照を含むポリシー名にすると、見分けやすくなります。
4. [開始] と [終了] に一連の IP アドレス範囲の開始アドレスと終了アドレスを入力して、このポリシーを適用するユーザを選択します。または、[IP アドレス] を 1 つだけ入力します。ポリシーのアドレスを追加するには、[追加] ボタンをクリックします。
5. 適用する IP アドレスを定義したら、[次へ] をクリックして残りのポリシー設定に進みます。

LDAP を使用したポリシー設定

LDAP サーバのユーザ名またはグループ名を使用してポリシーを設定する前に、ユーザ識別方法を設定し、使用する LDAP サーバの詳細を入力します。詳細については、167 ページの「LDAP 設定」を参照してください。

ユーザ / グループ名でポリシー範囲を設定するには

1. 管理コンソールから [HTTP] をクリックし、作成するポリシーの種類 (HTTPS 復号化ポリシー、高度な脅威保護ポリシー、HTTP 検査ポリシー、情報漏えい対策ポリシー、アプレット /ActiveX 対策ポリシー、URL フィルタポリシー、またはアクセス割り当てポリシー) を選択します。

   注意： アプリケーション制御ポリシーには、[アプリケーション制御] → [ポリシー] メニューからアクセスします。

2. 選択したポリシー種類の画面で [追加] をクリックします。
3. わかりやすい [ポリシー名] を新しく入力します。

4. ポリシーに追加するユーザまたはグループの LDAP ディレクトリを検索するには、次の手順に従ってください。
   a. [ユーザ] または [グループ] を選択します。
   b. [名前] にユーザ名またはグループ名の最初の一部分を入力し、[検索] をクリックします。
   c. リストボックスに、検索条件に一致したユーザまたはグループが表示されたら、ポリシーに追加するユーザまたはグループを選択して [追加] をクリックします。
5. ポリシー適用範囲が完成するまで、ユーザまたはグループを繰り返し追加します。
6. 新しいポリシーに名前を付け、適用するアカウントを定義したら、[次へ] をクリックして残りのポリシー設定に進みます。
7. 設定済みのディレクトリサーバ以外のサーバにユーザの認証情報が存在する場合は、複数のドメインを設定します。

第 8 章

HTTP 検索の設定

本章では、Trend Micro InterScan Web Security Virtual Appliance（以下、IWSVA）における HTTPS 復号化、HTTP ウイルス検索、HTTP 検査、および情報漏えい対策の設定方法について説明します。本章で説明する内容には、次の項目が含まれます。

HTTP 検査の概要

IWSVA の HTTP 検査機能は、HTTP メソッド、URL、および HTTP ヘッダに基づいたポリシー管理を提供します。

Web の動作はますます複雑さを増しています。IT 管理者は、ブラウザタイプのポリシーを実施したり、帯域幅を節約するために大きなサイズのファイル転送をブロックしたり、Web ファイルのアップロードや Web Distributed Authoring and Versioning (WebDAV) トラフィックをブロックするなど、さまざまな課題に直面しています。これらの処理は、企業データの喪失を防いだり、ビデオのアップロードをブロックしたり、ヘッダ内のキーワードをフィルタして処理を実行したり、ソーシャルネットワーキングサービス (SNS) サイトへのメッセージの投稿を防いだりするために使用されます。

HTTP 検査により、管理者は動作を識別して、HTTP メソッド、URL、およびヘッダに基づいて Web トラフィックをフィルタできるようになります。また、管理者はフィルタを作成するか、初期設定のフィルタを使用して Web トラフィックを識別することもできます。トラフィックが識別されたら、IWSVA はポリシー設定に従ってそれを管理し、管理者が特定のトラフィックに対して適切な処理を決定できるようにします。

注意： HTTP 検査フィルタでは、HTTP パケットのデータペイロードを検査できません。たとえば、Web メールや SNS サイト投稿のテキストまたはファイル内の一致パターンを検索することはできません。実行できるのは、定義された 1 つのサイトまたは一連のサイトに POST 処理が行われているかどうかを識別して、その POST を防止することだけです。

HTTP 検査についての情報は、対応するログとレポートに示されます。HTTP 検査通知を使用して、エンドユーザに対して Web 上の処理がブロックされた理由を知らせることもできます。

HTTP 検査ポリシー

[HTTP] → [HTTP 検査] → [ポリシー] にある [HTTP 検査ポリシー] リストには、システム上のすべての HTTP 検査 (IPv4 および IPv6) ポリシーが表示されます。有効なものも無効なものも表示されます。新規ポリシーを作成するには [追加] をクリックします。既存のポリシーを編集するにはそのポリシー名をクリックします。詳細については、下記を参照してください。

- 175 ページの「HTTP 検査 : アカウントの選択」
- 176 ページの「HTTP 検査 : ルールの指定」
- 179 ページの「HTTP 検査 : 除外リストの指定」

HTTP 検査ポリシーを編集するには、ポリシー名をクリックしてから [ルール] タブをクリックする必要があります。

HTTP 検査 : アカウントの選択

HTTP 検査ポリシーを追加するには、フィルタが必要です。初期設定のフィルタがいくつか用意されていますが、カスタムフィルタを使用するポリシーを作成するには、最初に [HTTP] → [HTTP 検査] → [フィルタ] でフィルタを作成する必要があります。条件を満たすアカウントには、IPv4 アカウントおよび / または IPv6 アカウント、ユーザ、またはグループ (ユーザの識別が有効な場合) の単一の IP アドレス、IP 範囲、または IP マスクが含まれています。

HTTPS 検査を有効にするには

1. メインメニューから [HTTP] → [HTTPS 復号化] → [ポリシー] の順にクリックします。
2. [HTTPS 検査を有効にする] をクリックします。
3. [保存] をクリックします。

HTTP 検査ポリシーに使用するアカウントを選択するには

1. [HTTP] → [HTTP 検査] → [ポリシー] に移動します。
2. [追加] をクリックします。
3. 次の情報を入力または指定します。
   - **ポリシーを有効にする** — 個々のポリシーを有効または無効にします。

注意 : グローバルレベルで ([HTTP] → [HTTP 検査] → [ポリシー] を選択して) HTTP 検査ポリシーを無効にしている場合、個々のポリシーの有効なステータスは無視されます。

- **新規ポリシーの作成** — ポリシールールの簡単でわかりやすい名前を入力します。名前は一意である必要があり、[HTTP] → [HTTP 検査] → [ポリシー] の順にクリックして表示されるポリシーリストに表示されます。
- **識別設定** — この画面のオプションは、使用しているユーザの識別方法に応じて異なります。[IP アドレス]、[ホスト名（変更された HTTP ヘッダ)]、または [ユーザ / グループ名認証] のいずれかになります。ユーザの識別方法の設定とポリシー適用範囲の設定の詳細については、160 ページの「ユーザ識別方法の設定」を参照してください。

注意： [ホスト名] を選択する前に、クライアントごとに下記のプログラムを実行して、LAN 上のすべてのクライアントを準備しておく必要があります。

```
/usr/iwss/bin/register_user_agent_header.exe
```

このプログラムを実行するには、Windows ドメインのログインスクリプトにこのプログラムを追加するか、またはこのプログラムを実行するためだけの専用スクリプトを作成します。

---

4. [次へ] をクリックして、新規ポリシーに指定するルールと除外があれば、それらを指定します。

HTTP 検査 : ルールの指定

[ルール] 画面では、HTTP トラフィックの検査フィルタを選択できます。HTTP 検査ポリシーの追加は、3 つの手順を実行します。最初に、アカウントを作成し、次に HTTP 検査フィルタルールを新しいアカウントに割り当て、最後に除外を指定します。

HTTP 検査ポリシーにルールを指定するには

1. 175 ページの「HTTP 検査ポリシーに使用するアカウントを選択するには」の手順を実行します。

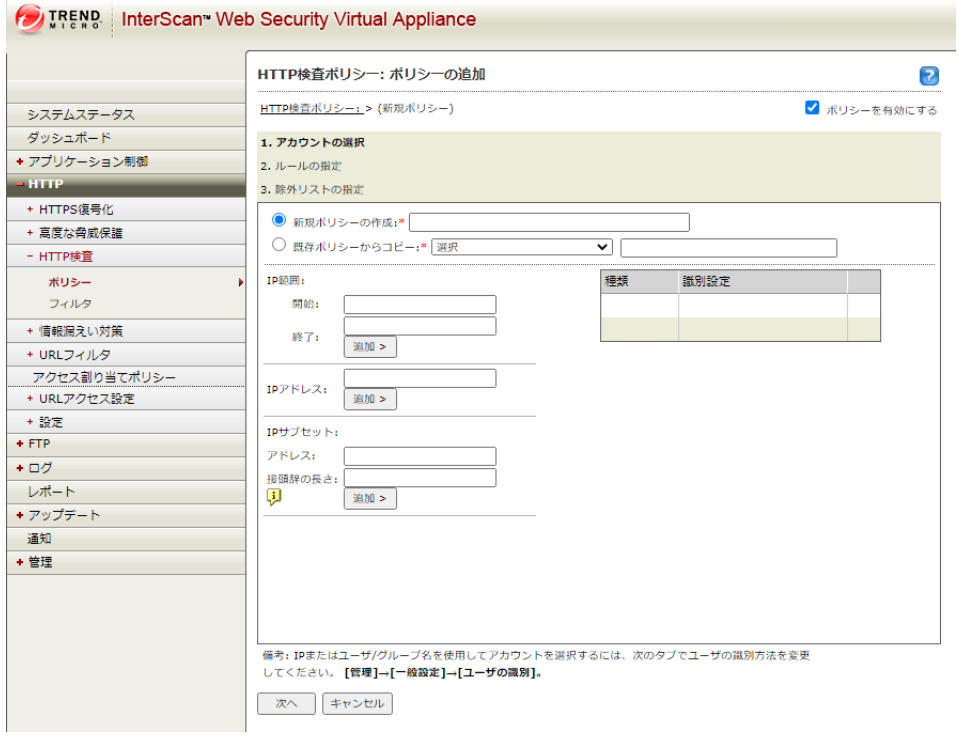


図 8-1. 指定したソーシャルネットワーキングサイトへのコンテンツ投稿をすべてブロックする HTTP 検査ポリシーの設定

2. 次の情報を入力または指定します。
   - **ポリシーを有効にする** — 個々のポリシーを有効または無効にします。ただし、HTTP 検査のグローバル設定は、個々のポリシー設定より優先されます。
   - **検査フィルタ** — 検査フィルタを選択し、ポリシーを適用するトラフィックの種類を指定します。利用できるフィルタの数は、初期設定のフィルタ数と作成されたカスタムフィルタ数の合計です。表 8-1 は初期設定のフィルタを示しています。

注意： カスタムフィルタは、[HTTP] → [HTTP 検査] → [フィルタ] → [追加] で作成できます。

   - 実行できるフィルタ処理は次のとおりです。
     - **許可 (検索)** — 対象サーバへの接続が許可され、ユーザはその Web サイトにアクセスできます。ただし、不正プログラムを検出するためにコンテンツが検索されます。
     - **許可 (検索なし)** — 対象サーバへの接続が許可され、ユーザはその Web サイトにアクセスできます。ただし、不正プログラムを検出するためのコンテンツの検索は行われません。
     - **ブロック** — 対象サーバへの接続が確立されず、ユーザはその Web サイトにアクセスできません。このイベントについてはログエントリも作成されます。
     - **監視** — 対象サーバへの接続が許可され、ユーザはその Web サイトにアクセスできます。このイベントについてはログエントリも作成されます。

注意： 次のセクションのために、制限する日数と時間は [管理] → [一般設定] → [予約期間] で定義されます。

   - **スケジュール** — [管理] → [一般設定] → [予約期間] に移動してスケジュールを設定します。初期設定は [常時] です。
   - **備考** — ポリシーの目的や理由などの備考を入力します。この備考は簡単なメモとして、または今後 HTTP 検査を管理する他のユーザへの連絡事項として使用できます。
3. 作業を続行するには、[次へ] をクリックします。

HTTP 検査 : 除外リストの指定

企業イントラネット、ビジネスパートナーサイト、および調査ツールサイトなどの一部の URL や Web サイトを、HTTP 検査フィルタの対象から除外したい場合があります。除外リスト内の URL は、ブロックも監視もされません。

除外リストは、[HTTP] → [設定] → [除外リスト] 画面で作成できます。

HTTP 検査ポリシーに除外を指定するには

1. アカウントとルールを設定します。
2. [HTTP 検査ポリシー : ポリシーの追加] 画面で、[承認する URL リスト] のドロップダウンリストから、HTTP 検査ルールから除外する URL 名を選択します。

   注意 : 除外リストは、[HTTP] → [設定] → [除外リスト] で設定されます。

3. [保存] をクリックします。[HTTP] → [HTTP 検査] → [ポリシー] を選択すると、新しいポリシーがポリシーのリストに表示されます。

HTTP 検査フィルタ

HTTP 検査フィルタには、Web トラフィックを特定する一般的な方法が用意されています。これにより、次のコンポーネントを使用してフィルタ条件を作成できます。

- URL ホスト
- URL パス
- URL クエリ
- HTTP メソッド
- HTTP ヘッダ

初期設定の HTTP 検査フィルタ

HTTP 検査の初期設定のフィルタでは、ソーシャルネットワーキングサービス (SNS) のアップロードのブロック、特定の種類のブラウザを介した Web アクセスの制限など、一般的なシナリオに対応するフィルタリングを実現します。

図 8-2. 指定したソーシャルネットワーキングサイトへの POST 処理を防止する HTTP 検査フィルタの設定

初期設定のフィルタ設定については、表 8-1 を参照してください。管理者は、初期設定または事前定義されたフィルタを微調整して、必要な管理機能を取得できます。

- **追加** — フィルタの追加ウィザードを開きます。このウィザードでは、順を追って新規フィルタを定義します。
- **削除** — フィルタを削除できます。
- **エクスポート** — 既存のフィルタをエクスポートできます。

- **インポート** — 別の場所で作成されたかサポートサービスによって作成されたカスタムフィルタ、またはエクスポートされたフィルタをインポートできます。

表 8-1. 初期設定の HTTP 検査フィルタのマトリックス

初期設定のフィルタ名	フィルタの種類	要求方法	URL ホスト	URL パス	URL クエリ	ヘッダ (名前 / 演算子 / 値)
ブラウザ種類	REQ	なし	なし	なし	なし	User-Agent / Contains/ MSIE || Firefox || Chrome || Opera
サイズの大きいデータのダウンロード	RESP	該当なし	なし	なし	なし	Content-length/ >/ 1048576
サイズの大きいデータのアップロード	REQ	なし	なし	なし	なし	Content-length/ >/ 1048576
クエリキーワード	REQ	なし	なし		< キーワード >	なし / なし / なし

表 8-1. 初期設定の HTTP 検査フィルタのマトリックス (続き)

初期設定のフィルタ名	フィルタの種類	要求方法	URL ホスト	URL パス	URL クエリ	ヘッダ (名前 / 演算子 / 値)

SNS サイト投稿	REQ	POST	(詳細ビューで追加)
			
			youtube_upload REQ {
			METHOD: POST
			HOST: upload\.youtube\.com }
			
			twitter_msg_post REQ {
			METHOD: POST
			HOST: twitter\.com
			PATH: status
			}
			facebook_upload REQ {
			METHOD: POST
			HOST: upload\.facebook\.com }
				なし	なし	なし / なし / なし

Web ファイルアップロード	REQ	POST	なし	なし	なし	Content-Type/ Contains/ multipart/form-data

表 8-1. 初期設定の HTTP 検査フィルタのマトリックス (続き)

初期設定のフィルタ名	フィルタの種類	要求方法	URL ホスト	URL パス	URL クエリ	ヘッダ (名前 / 演算子 / 値)
WebDAV	REQ	PROPFIND PROPMATCH MKCOL COPY MOVE	なし	なし	なし	なし / なし / なし

HTTP 検査フィルタの追加

HTTP 検査フィルタを追加するには、次の 2 つの方法があります。

- **基本ビュー** — フィルタの一般的なコンポーネントが提供され、フィルタの種類 (HTTP 要求または HTTP 応答)、URL ホスト、URL パス、URL クエリ、要求ヘッダ、応答ヘッダのオプションを使用できます。
- **詳細ビュー** — パターンを入力できます。

注意 : 新しいフィルタを追加する方法には、既存のフィルタの名前をクリックし、必要に応じて名前を変更して別の名前で保存する方法もあります。

基本ビューでのフィルタの追加

基本ビューで設定したフィルタでは、以下を定義します。

- **フィルタ名と説明** — ユーザが新しいフィルタに指定する名前と説明です。
- HTTP **要求または応答** — トラフィックの方向を示します。
- **フィルタスコープ** — HTTP メソッド (HTTP 要求のみ)、パス、クエリ、またはヘッダが含まれます。
- **キーワードマッチ** — HOST、PATH、QUERY、および METHOD オプションの場合、一致とは値に入力キーワードが含まれることです (単純な文字列比較を使用)。HEADER オプションの場合は、文字列一致と整数値比較の両方がサポートされます。

パケットの取り込みの使用

フィルタのコンポーネントの一部は、HTTP 要求または応答でのパケット取り込みの実行を利用して判別できます。取り込みの例（図 8-3）と説明（表 8-2）を参照してください。ネットワークパケットの取り込みツールの詳細については、398 ページの「ネットワークパケットの取り込み」を参照してください。

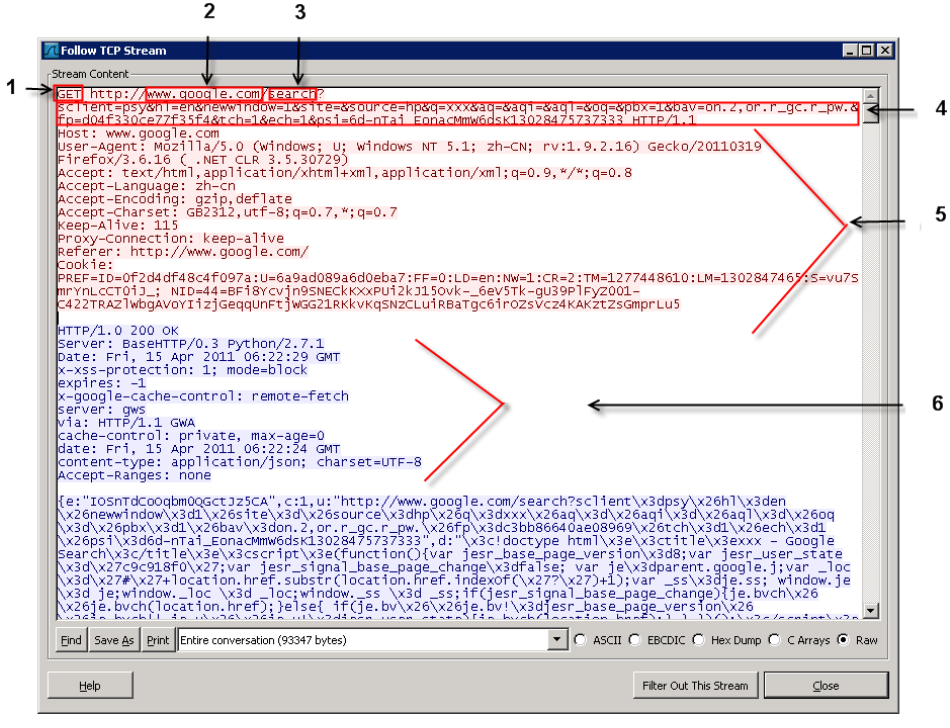


図 8-3. Google 検索の場合のパケットの取り込み

表 8-2.　パケットの取り込みで表示されるコンポーネント

番号	コンポーネント
1	要求方法
2	URL ホスト
3	URL パス
4	URL クエリ
5	要求ヘッダ
6	応答ヘッダ

基本ビューで新しい HTTP 検査フィルタを追加するには

1. [HTTP] → [HTTP 検査] → [フィルタ] に移動します。
2. [追加] をクリックします。
3. フィルタ名と説明を入力します。
4. [基本ビュー] ラジオボタンを選択します。図 8-2 を参照してください。
5. フィルタを作成する方向に応じて、フィルタの種類 (HTTP 要求または HTTP 応答) を選択します。
   - **HTTP 要求** — HTML ページを取得するためにクライアントが要求を Web サーバに送信するときに使用されるフィルタを作成します。要求フィルタには、次の範囲が含まれます。要求メソッド、URL ホスト、URL パス、URL クエリ、および HTTP ヘッダ。
   - **HTTP 応答** — Web サーバが応答メッセージをクライアントに返すときに使用されるフィルタを作成します。応答フィルタには、次の範囲が含まれます。URL ホスト *、URL パス *、URL クエリ *、および HTTP 応答ヘッダ。

注意： 上記のアスタリスク (*) が付いた項目の情報は、HTTP 要求から取得されます。応答には、この情報は含まれません。

6. 次のオプションの 1 つまたは複数を設定して、フィルタを定義する値を入力します。
   - (フィルタの種類が HTTP 要求の場合に限る) [要求方法] チェックボックスをオンにします。フィルタの範囲を制限するために、HTTP 要求のメソッドを指定します。値には、表 8-3 に示されているものか、その他の拡張メソッドの値を指定できます。

表 8-3.　HTTP 要求フィルタのメソッドの値

メソッド	説明
DELETE	指定されたリソースを削除します。
GET	指定されたリソースを要求します。
HEAD	GET リクエストと似ていますが、ヘッダ情報のみを要求します。これは、コンテンツ全体を送信することなく、応答ヘッダに書き込まれたメタ情報を取得するのに便利です。
OPTIONS	指定された URL でサーバがサポートする HTTP メソッドを返します。特定のリソースではなくアスタリスク (*) を指定すると、Web サーバの機能をチェックするために使用できます。
POST	処理対象のデータを (HTML フォームなどから) 特定されたリソースに送信します。データは要求の本体に含まれます。このメソッドにより、新しいリソースの作成や既存リソースのアップデートが実行される場合があります。
PUT	指定されたリソースをアップロードします。
TRACE	受信した要求をエコーバックします。これにより、クライアントは、中間サーバによってどのような変更または追加が行われたかを確認できます (変更、追加が行われた場合)。

注意： ユーザは、OR 関係を使用して複数のキーワードを定義できます。キーワードは「|」文字もしくは「||」文字で区切ります。また、URL クエリ、URL パス、ヘッダ、HTTP メソッドのオプション用の新しい行を定義することもできます。

- [URL ホスト] チェックボックスをオンにします。IPv4/IPv6 アドレスのホスト名 (ポート番号があれば含めます) を、URL の一部として入力します。
- [URL パス] チェックボックスをオンにします。(ある場合は) ホスト部分の末尾の「/」の直後からクエリの「?」の直前までの URL のパス部分を入力します。

- [URL クエリ] チェックボックスをオンにします。(ある場合は) 「?」の直後から URL 文字列の末尾までの URL のクエリ部分を、以下の変換ウィザードのフィールドに入力します。
  - UTF-8 文字列を変換する必要がある場合は、[変換処理が必要ですか？] チェックボックスをオンにします。

注意： キーワードクエリは、UTF-8 エンコードのみサポートします。マルチバイト文字を別の文字セットと照合するには、URL エンコードされた 16 進コードを使用します。

  - 変換する UTF-8 文字列を入力します。
  - 適切な文字セットを選択します。
    - 簡体字中国語 (GB2312)
    - 繁体字中国語 (Big5)
    - 日本語 (EUC)
    - 日本語 (Shift-JIS)
  - [変換] をクリックすると、変換された値が [変換された文字列] に表示されます。
- [ヘッダ] チェックボックスをオンにします。使用されるヘッダの名前と値を選択するには、最終列で「+」記号をクリックします。ここでは、文字列一致と整数値比較の両方がサポートされます。
  - **含む**｜**含まない** — 単純な文字列比較を使用し、値に入力キーワードが含まれていること / 含まれていないことを示します。
  - OR 関係を使用して、複数のキーワードを追加します。キーワードは「|」文字で区切ります。
  - =、≠、≥、≤ — 整数値比較を示します。
  - **存在する / 存在しない** — ヘッダに、定義済みのヘッダが含まれていること / 含まれていないことを示します。
  - Web トラフィックが 1 つのフィルタと照合されるのは、定義済みのすべての範囲が照合される場合に限ります。つまり、METHOD、HOST、PATH、QUERY、および複数の HEADER 内に AND 関係が存在します。
  - 使用される値を入力し、適切な演算子 (Contains、Not Contain、equals、does not equal、greater than、equal to、less than、equal to) をドロップダウンリストから選択します。

7. [保存] をクリックします。

   [HTTP] → [HTTP 検査] → [フィルタ] を選択すると、新しいフィルタ名がフィルタのリストに表示されます。

詳細ビューでのフィルタの追加

フィルタ定義を、定義済みの構文を使用してテキストモードで編集できます (HTTP BODY はサポートされていません)。正規表現がサポートされています。すべての正規表現が適用されます (http://www.pcre.org/pcre.txt を参照)。使用可能な PCRE (Perl 互換正規表現) フラグについては、表 8-4 を参照してください。

表 8-4. パターンの設定で使用可能な PCRE フラグ

正規表現	説明
PCRE_DOTALL	「.」(ピリオド) 文字は、行末文字 CR (\r) と LF (\n) を含むすべてのバイトと一致します。
PCRE_DOLLAR _ENDONLY	「$」(ドル記号) 文字は、完全な「ソースの終端」(データの終端) のみに一致し、行末文字には一致しません。
PCRE_EXTENDED	主に、次の文字 (リテラル) が正規表現の定義で無視されます。 空白、タブ、復帰改行、改行、改ページ、「#」 ただし、これらの文字のエスケープ形式は遵守されます。 「\ 」、「\t」、「\r」、「\n」、「\f」、「\#」 これが行われる主な理由は、(構造と分岐を目立たせる空白を使用して) よりわかりやすい方法で正規表現の定義を書式設定できるようにすることと、行の境界を越えて正規表現の定義を簡単に分割できるようにすることです。

注意： 注意 :PCRE_DOTALL と PCRE_EXTENDED は、表現にそれぞれ「(?-s)」および「(?-x)」を追加すると、無効になる場合があります。

その他のルールは次のとおりです。
— PCRE のランタイムフラグ PCRE_UTF8 (UTF-8 モード) は使用されません。つまり「.」文字は必ず 1 バイトのみに一致します。
— シグネチャ定義では、行の最後に「\」(バックスラッシュ) を使用すると行末がエスケープされます (UNIX シェルの場合)。バックスラッシュは PCRE の正規表現言語ではないため、念のために、行継続のバックスラッシュの前に 1 つ以上の空白を入れてください。複数行の正規表現をアセンブリして使用する場合、行が連結される前に、行末のバックスラッシュが削除され、先頭および末尾にあるすべての空白が各行から削除されます。

詳細ビューで新しい HTTP 検査フィルタを追加するには

1. [HTTP] → [HTTP 検査] → [フィルタ] に移動します。
2. [追加] をクリックします。
3. フィルタ名と説明を入力します。

4. [詳細ビュー] ラジオボタンを選択します。図 8-4 を参照してください。

図 8-4. 詳細ビューにおける要求モードの POST フィルタ例

5. 次のいずれかを実行します。

   - パターンマッチングを実行するには、[パターン] フィールドにパターンを入力します。次の構文を使用します。

     注意： [Filter Type] を、REQ（要求モードの場合）または RESP（応答モードの場合）に置換する必要があります。

```
[ScanSetName] [Filter Type] {
[TAG]:RegularEx
[HDR-TAG]:[HDR-NAME]:[HDR-OP]:RegularEx
[TAG]
METHOD, HOST, PATH, QUERY
[HDR-TAG]
REQ-HDR, RESP-HDR}
[HEADER_OP]:
-----------------------------------
```

```
EQ : =
NE : !=
GE : >=
LE : <=
M : Contain
NM : Not Contain
X  : Exist
NX : Not exist
```

i. 要求モードのパターン例を次に示します。

```
#
#        _SCAN_SET_1_ REQ {
#              METHOD: POST
#              HOST: ^www\.samplesite\.com:2345(?!\d)
#              PATH: test
#              QUERY: test
#               REQ-HDR:Content-Type:M:multipart/form-data
#              REQ-HDR:Content-Length:GE:1048576
#       }
#
```

ii. 応答モードのパターン例を次に示します。

```
#
#        _SCAN_SET_2_ RESP {
#             HOST: ^www\.samplesite\.com:2345(?!\d)
#             PATH: test
#             QUERY: test
#              RESP-HDR:Content-Type:M:multipart/form-data
#             RESP-HDR:Content-Length:GE:1048576
#       }
#
```

注意： その他の考慮事項

1. 整数値比較の場合は、IWSVA は文字列部分を変換します。文字列に「0x」プレフィックスが含まれる場合は、数字はベース 16 で読み込まれます。それ以外の場合、次の文字が「0」以外であれば 10 (10 進数) と解釈され、「0」であれば 8 (8 進数) と解釈されます。

2. 最初の空白以外の文字が記号または数字でない場合は、文字列は数字ではありません。

3. 要求ヘッダのチェックルールに、RESP-HDR を含めないでください。応答ヘッダにしか表示されないヘッダは、要求タイプのフィルタに追加できません。

4. 応答ヘッダのチェックルールに、METHOD と REQ-HDR を含めないでください。要求ヘッダにしか表示されないヘッダは、応答タイプのフィルタに追加できません。詳細ビューを使用して新しいフィルタを作成するときは、応答タイプのフィルタで METHOD を使用しないでください。

5.IWSVA は、フィルタが HTTP プロトコルに準拠しているかどうかは確認しません。不適切に作成されたフィルタは機能しません。

- HTTP ヘッダを変更するには、[パターン] フィールドにパターンを入力します。次の構文を使用します。
  - HTTP ヘッダを追加するには

```
EVENT: {
OP: HEADER_ADD
HEADER: X-GoogApps-Allowed-Domains
VALUE: unixlabs.net, unix.com
}
```

  - HTTP ヘッダを削除するには

```
EVENT: {
OP: HEADER_REMOVE
HEADER: X-GoogApps-Allowed-Domains
}
```

  - HTTP ヘッダの値を変更するには

```
EVENT: {
```

```
        OP: HEADER_MODIFY
        HEADER: cookie
        ORIGINAL_VALUE: [text1]
        FINAL_VALUE: [text2]
}
```

注意： この機能は、HTTP 検査フィルタの処理を [監視] または [許可 (検索)] に対してのみ有効にします。

6. [保存] をクリックします。

HTTP 検査フィルタの編集

既存のフィルタを変更したり、既存のフィルタを基準にして新しいフィルタを作成したりできます。

HTTP 検査フィルタを編集する場合は、以下を変更できます。

- フィルタ名
- フィルタの説明
- フィルタの手法 (基本ビュー)
- フィルタのパターン (詳細ビュー)

基本ビューまたは詳細ビューでフィルタを変更できます。

フィルタを変更するには

1. [HTTP] → [HTTP 検査] → [フィルタ] に移動します。
2. 変更するフィルタの名前をクリックします。
3. 次のようにパラメータを変更します。
   - 185 ページの「基本ビューで新しい HTTP 検査フィルタを追加するには」
   - 189 ページの「詳細ビューで新しい HTTP 検査フィルタを追加するには」
4. [保存] をクリックします。

HTTP 検査フィルタのインポート

次の 2 種類の HTTP 検査フィルタをインポートできます。

- ユーザが IWSVA を使用せずにテキストファイル形式で作成した新しいフィルタ
- トレンドマイクロのサポートサービスが作成したカスタムフィルタ

フィルタファイルは XML ファイルです。インポートされるフィルタファイルは、194 ページの「インポートするフィルタを作成するには」に示されている規定の基準に適合する必要があります。

インポートするフィルタを作成するには

1. インポートされるフィルタの XML ファイルは、いくつかの方法で作成できます。
   - IWSVA からエクスポートする
   - 新しいファイルとして作成する
2. 新しいファイルを作成する場合は、以下のサンプル形式を使用してください。

```
<?xml version="1.0" encoding="UTF-8"?>
<SDF>
    <Filter Mode="Basic" Name="Browser type filter" ID="1">
        <Note> FireFox ブラウザから送信された要求を
ユーザエージェントヘッダに従って特定します </Note>
        <Basic Type="REQ">
            <Headers Enable="true">
                <Header Value="Firefox" Op="M" Name="User-Agent"/>
            </Headers>
        </Basic>
    </Filter>
    <Filter Mode="Basic" Name="Large data upload filter" ID="3">
        <Note> サイズの大きいファイルのアップロードをコンテンツ長ヘッダに従って特定しま
す </Note>
        <Basic Type="REQ">
            <Headers Enable="true">
                <Header Value="1048576" Op="GE" Name="Content-Length"/>
            </Headers>
        </Basic>
    </Filter>
    <Filter Mode="Basic" Name="Query keyword filter" ID="4">
        <Note> 検索エンジン Web サイトなどのクエリキーワードを特定します </Note>
        <Basic Type="REQ">
            <Query Enable="true">
```

```
                <Value><![CDATA[[put query keywords here]]]></Value>
            </Query>
        </Basic>
    </Filter>
</SDF>
```

フィルタをインポートするには

1. [HTTP] → [HTTP 検査] → [フィルタ] に移動します。
2. [インポート] リンクをクリックします。
3. [参照] をクリックして、インポートするパスとフィルタを指定します。
4. [インポート] をクリックします。
5. フィルタ名のリストに、インポートされたフィルタの名前が表示されます。

HTTP 検査フィルタのエクスポート

次のようないくつかの理由で、既存のフィルタをエクスポートできます。

- フィルタは他の場所で使用可能である。
- トレンドマイクロのサポートサービスが作成したカスタムフィルタは、IWSVA 管理者によるエクスポート、お客さまへの送信、およびインポートが可能である。

注意： エクスポートされたフィルタファイルは手動で編集しないでください。変更すると、ファイルが正常にインポートされなくなる場合があります。

フィルタをエクスポートするには

1. [HTTP] → [HTTP 検査] → [フィルタ] に移動します。
2. エクスポート対象のファイルの名前のボックスをオンにします。
3. [エクスポート] リンクをクリックします（フィルタ名が選択されていない場合は、エラーメッセージが表示されます)。
4. [名前を付けて保存] ダイアログボックスで、ファイルを保存する場所を選択します。初期設定のファイル名を使用するか、変更します。
5. [保存] をクリックします。

情報漏えい対策

IWSVA に追加された情報漏えい対策 (DLP) は、ユーザに以下の機能を提供します。

- 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できます。
- 事前定義されたテンプレートを使用してポリシーを作成および変更することにより、個人情報をフィルタリングして世界各国のプライバシー規制要件をより確実に遵守できます。
- キーワードと正規表現を使用してカスタムポリシーを作成および変更することで、お客さまの定義する方法で知的財産をフィルタできます。
- どのユーザがどの DLP ポリシーを違反したかについてレポートを提供します。
- 管理者が製品の DLP ポリシーの有効性 (検出率と誤警告率) を評価するための監査機能を提供します。

ヒント : ベストプラクティスとして、できるだけ多く (「すべてのエンドポイント」または「すべてのユーザ」など) の対象 (ユーザまたはエンドポイント) に最も厳密なルールを課すポリシーを最初に作成して、その後「すべてのエンドポイント」または「すべてのユーザ」からの例外として少数のエンドポイントまたはユーザに対するポリシーを作成することを強くお勧めします。

ポリシー

[情報漏えい対策ポリシー] ページを使用して、組織のファイルが満たす必要のある、組織全体のルールおよび条件を作成します。

[情報漏えい対策ポリシー] ページでは、組織の情報漏えい対策ポリシーを追加、編集、削除、または保存できます。また、[DLP を有効にする] チェックボックスをオンまたはオフにすることで、この機能を有効にするかどうかを制御できます。IWSVA に含まれる DLP 検索の初期設定ポリシーは変更はできますが、削除することはできません。

[情報漏えい対策ポリシー] ページにアクセスするには

1. [HTTP] → [情報漏えい対策] → [ポリシー] に移動します。
   [情報漏えい対策ポリシー] ページが表示されます。
2. 編集または削除するポリシーを選択するか、または必要に応じて新規ポリシーを追加します。以下のセクションで必要な手順を説明します。

既存の DLP ポリシーを変更するには

1. [HTTP] → [情報漏えい対策] → [ポリシー] に移動し、変更するポリシーの名前をクリックします。

   [情報漏えい対策ポリシー : ポリシーの編集] ページが表示されます。
2. 各ポリシーテンプレートは、特定の地域または業界により分類され、[許可]、[ブロック]、または [監視] するよう選択できます。
3. 適用するルールテンプレートの左側にあるプラス記号のアイコンをクリックします。
4. ルールのチェックボックスをオンにしてプルダウンを使用することで必要に応じて変更を行い、希望する動作に変更して、[適用] をクリックします。

   処理アイコンが要求されたステータスに変わります。

新しい DLP ポリシーを追加するには

1. [HTTP] → [情報漏えい対策] → [ポリシー] に移動し、[追加] をクリックします。

   [情報漏えい対策ポリシー : (新規ポリシー)] ページが表示されます。
2. ポリシー名を入力します。
3. 保護または監視の対象を定義して有用なアカウント情報を入力します。このページでは、IP 範囲または特定の IP アドレスにより対象を選択できます。

注意 : これらのアカウントフィールドでは IPv6 アドレスがサポートされます。任意の IPv6 ホストに 1 つのルールを定義すると、クライアントが IWSVA を介して組織のセキュリティポリシーに違反するデータを送信したときにこのポリシールールがトリガされます。

---

4. 特定のユーザまたはユーザのグループ全体を対象として選択します。ユーザまたはグループの名前を入力して、[検索] をクリックします。
5. [次へ] をクリックします。

   [ルールの指定] ページが表示されます。
6. 既存のポリシーを編集する場合と同様に、定義済みの DLP テンプレートを使用するか、または特定の地域または業界で分類されたポリシーテンプレートを変更します。ポリシーテンプレートでは、特定のルールを許可、ブロック、または監視できるターゲットテンプレートを選択することで、コンテンツを検索できます。

   初期設定の検索トラフィックは HTTP/HTTPS に設定されています。
7. 適用するルールテンプレートの左側にあるプラス記号のアイコンをクリックします。
8. ルールのチェックボックスをオンにしてプルダウンを使用することで必要に応じて変更を行い、希望する動作に変更して、[適用] をクリックします。

9. 処理アイコンが要求されたステータスに変わります。
10. 残りのページ要素を入力します。
11. [次へ] をクリックします。

    [除外リストの指定] ページが表示されます。
12. 承認する URL リスト、除外ファイル名リストの設定を指定し、ファイルのサイズを制限する場合は、サイズ制限値を入力してチェックボックスをオンにします。
13. [保存] をクリックします。

テンプレート

[テンプレート] ページには、すべての初期設定のテンプレートと、管理者によってカスタマイズされたテンプレートが表示されます。これらのテンプレートは、関連付けられた業界または地域ごとに表示され、それぞれの説明が含まれます。このページからテンプレートを追加、コピー、削除、インポート、またはエクスポートできます。

新しい準拠テンプレートを追加するには

1. [HTTP] → [情報漏えい対策] → [テンプレート] に移動し、[追加] をクリックします。

   [テンプレートの追加] ページが表示されます。
2. 追加する準拠テンプレートの名前と説明を入力します。
3. 各デジタル資産を式またはキーワードとして定義します。
4. 新しい準拠テンプレートで、「デジタル資産の定義」として事前定義された式またはキーワード項目を、固定された出現回数または「および」/「または」の論理式と組み合わせて選択します。
5. デジタル資産を追加するには、ページの左側にあるプラス記号をクリックします。
6. [追加] をクリックして新しいデジタル資産を作成します。
7. [保存] をクリックして完了します。

iDLP

IWSVA 6.5 には Trend Micro Control Manager（以下、Control Manager）または Trend Micro Apex Central（以下、Apex Central）の情報漏えい対策ウィジェットが含まれており、企業の管理者は、このウィジェットを使用して Control Manager または Apex Central から IWSVA に情報漏えい対策ポ

リシー / テンプレートを配信できます。管理者は Control Manager または Apex Central を使用して、IWSVA 6.5 などトレンドマイクロ製品に対する組織全体の情報漏えい対策ポリシーを管理できます。

HTTPS のセキュリティ

HTTPS (Hypertext Transfer Protocol with Security) とは、HTTP とネットワークセキュリティプロトコル (SSL (Secured Sockets Layer) など) を組み合わせたものです。HTTPS 接続は、機密コンテンツを保護するための信頼性に優れた接続を必要とする、オンラインバンキングなどの Web アプリケーションで使用されています。従来のセキュリティデバイスではこの HTTPS コンテンツを復号化して検査できなかったため、HTTPS トラフィックに埋め込まれたウイルスや不正プログラムなどの脅威がセキュリティ防御機能を素通りしてエンタープライズネットワークに侵入していました。

IWSVA は、暗号化されたコンテンツを復号化して検査することで HTTPS のセキュリティホールをふさぎます。選択した Web カテゴリの HTTPS トラフィックを復号化するようにポリシーを定義できます。復号化の際、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。また、復号化されたデータは IWSVA サーバのメモリ内に保持されるため、セキュリティは保護されます。このデータは IWSVA サーバから送り出される前に暗号化されるため、クライアントのブラウザに安全に送信されます。

IWSVA は、次のモードで HTTPS の復号化および検索をサポートしています。

- プロキシ転送
- WCCP
- 透過ブリッジ
- リバースプロキシ

未確認の HTTPS コンテンツの危険性

次に、HTTPS 接続に関する主な問題点をいくつか示します。

- ウイルス検索ポリシーおよびコンテンツフィルタポリシーは、暗号化されたデータには適用できません。
- クライアントはデジタル証明書の失効リストをチェックすることがほとんどないため、デジタル証明書が偽造されたり、有効期限が切れたり、失効する可能性があります。
- 正規の証明書は悪意のある第三者によって容易に取得することができるため、提供された情報が安全であるとユーザが思い込んでしまう場合があります。

- Web ブラウザは証明書の挿入攻撃に対して脆弱であるため、悪意のある侵入者による社内イントラネットへのアクセスが可能になります。
- 証明書が信頼できるものかどうかを判断するのに必要な知識が、ユーザにない場合があります。
- URL パスやその他の情報が隠されているため、HTTPS トラフィックの監視が困難です。

SSL ハンドシェイクの概要

SSL プロトコルを使用して HTTPS 接続を確立するには、Web サーバで SSL 証明書をインストールする必要があります。証明書は認証機関 (CA) から提供され、Web サイトが信頼できるか、機密情報 (クレジットカード番号など) が暗号化されているか、送信データに改ざんやねつ造はないかなどを確認できます。

クライアントが「http://」ではなく「https://」から始まる URL を入力して SSL セッションを開始すると、SSL ハンドシェイクが実行され、識別情報が検証され (証明書の交換や妥当性など)、セッションに必要な暗号化方式の処理が行われます。IWSVA サーバは、クライアントと安全な Web サーバとの間の中継機として機能し、サーバ証明書を検証します。次に SSL ハンドシェイク処理の概要を示します。

1. クライアント Web ブラウザは、接続要求とその暗号化データを Web サーバに送信します。IWSVA はその要求を Web サーバに転送します。
2. Web サーバは、その SSL 情報 (サーバ証明書を含む) を返します。IWSVA はサーバ証明書を確認します。
3. サーバ証明書が検証テストに合格すると、その Web サーバとクライアント間で HTTPS 接続が許可されます。IWSVA は、HTTPS 復号化ポリシーを適用して、暗号化されたコンテンツを検索します。

   Web サーバがクライアント証明書を要求する場合、IWSVA は暗号化されたトラフィックをブロックまたはトンネルします。

IWSVA における HTTPS 復号化およびプロセスフロー

Web サーバとクライアント間で HTTPS 接続が許可されると、IWSVA は暗号化されたコンテンツを復号化して検査することで、HTTPS のセキュリティループホール（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化するようにポリシーを定義できます。復号化の際、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。

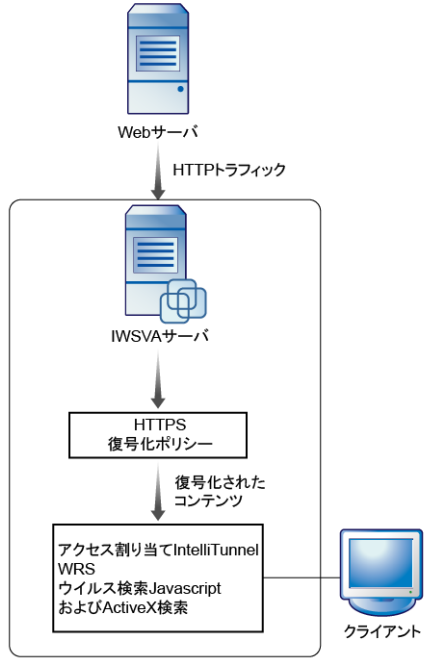


図 8-5.　IWSVA における復号化された HTTPS のトラフィックフロー

HTTPS 復号化機能には、次のような利点があります。

- ゲートウェイでの復号化 — IWSVA は HTTPS トラフィックを復号化して、既存のセキュリティポリシーを適用することができます。
- データのプライバシーの保護 — 復号化されたデータは IWSVA サーバのメモリに引き続き存在するので、まったく安全です。データは、IWSVA サーバから送信される前に暗号化されます。これにより、クライアントのブラウザまで安全に通過できるようになります。

- 証明書の一元的な処理 — IWSVA はリモートサーバで発行された証明書を検証して管理することで、クライアントを重要なタスクから解放します。

HTTPS 復号化ポリシーの設定

IWSVA で暗号化されたコンテンツに検索ポリシーおよびフィルタポリシーを適用するには、その前に、コンテンツを復号化するように HTTPS 復号化ポリシーを設定する必要があります。URL フィルタポリシーの設定と同様に、選択された Web カテゴリに基づいてコンテンツを復号化するように、HTTPS 暗号化ポリシーを設定します。たとえば、ビジネスカテゴリの Web サイトからの暗号化されたコンテンツを復号化するように、HTTPS 復号化ポリシーを設定することができます。

HTTPS 復号化ポリシーおよび URL フィルタポリシーでは、同じ Web カテゴリのグループと名前を使用します。会社またはユーザのニーズを満たすように、カスタムカテゴリを設定することもできます。

注意： カスタムカテゴリが複数選択されているか、まったく選択されていないかどうかに関係なく、IWSVA は最初のカスタムカテゴリのみを一致対象とします。

ブリッジモードで、プロキシサーバが IWSVA と Web サーバとの間に配置され、クライアントのブラウザがそのプロキシサーバを介してインターネットにアクセスするように設定されている場合、IWSVA はポリシー設定に従って、HTTPS 接続をトンネルするか、または復号化して検索します。

HTTPS 復号化の有効化

HTTPS 復号化を有効にするには

1. [HTTP] → [HTTPS 復号化] → [ポリシー] の順に選択します。
2. [HTTPS 復号化を有効にする] をクリックします。
3. [保存] をクリックします。
4. [ポリシーの配信] をクリックします。

新しい HTTPS 復号化ポリシーの作成

新しい HTTPS 復号化ポリシーを作成するには、次の 3 つの手順に従います。

- ポリシーを適用するアカウントを選択します。

- トラフィックを復号化する Web サイトカテゴリを指定します。
- 除外リストを選択します。

HTTPS 復号化を有効にするには

1. メインメニューから [HTTP] → [HTTPS 復号化] → [ポリシー] の順にクリックします。
2. [HTTPS 復号化を有効にする] をクリックします。
3. [保存] をクリックします。

新しい HTTPS 復号化ポリシーを作成するには

1. IWSVA Web コンソールを開き、管理コンソールから [HTTP] → [HTTPS 復号化] → [ポリシー] の順に選択します。

   [追加] をクリックします。[HTTPS 復号化ポリシー : ポリシーの追加] 画面が表示されます。
2. [新規ポリシーの作成] ボックスに、わかりやすいポリシー名を入力します。

   「Web メール用 HTTPS 復号化ポリシー」のように、適用対象となるユーザまたはグループへの参照が含まれるポリシー名は簡単に覚えられます。
3. ポリシーを適用するユーザを選択します。

   この画面のオプションは、使用しているユーザの識別方法に応じて異なります。[IP アドレス]、[ホスト名 (変更された HTTP ヘッダ)]、または [ユーザ / グループ名認証 (LDAP)] のいずれかになります。ユーザの識別方法の設定とポリシー適用範囲の設定の詳細については、160 ページの「ユーザ識別方法の設定」を参照してください。
4. [次へ] をクリックします。
5. [カテゴリの指定] 画面で、[ポリシーを有効にする] チェックボックスがオンになっていることを確認します。
6. 復号化する URL カテゴリを選択します。

   グループの全カテゴリを選択するには、対象グループで [すべて選択] をクリックします。グループ内のすべてのカテゴリを選択するのに、グループを展開する必要はありません。
7. 今後の参照のためにこのポリシーに関して役立つ情報を含めるには、オプションの [備考] を入力します。
8. [次へ] をクリックします。
9. 除外リストを適用する場合、[除外リストの指定] 画面で、ドロップダウンリストボックスから除外 HTTPS URL リスト名を選択します。IWSVA は、除外リスト内の URL から送信された HTTPS トラフィックをそのまま通過させます。つまり、この暗号化されたコンテンツは検査のために復号化されません。
10. [保存] をクリックします。

11. [HTTPS 復号化ポリシー] 画面で、[優先度] 列に表示されている上向きまたは下向きの矢印をクリックして、新しいポリシーの優先順位を設定します。

    2 つ以上のポリシーに属するアカウントがある場合、[優先度] の設定により、どのポリシーが適用されるかが決まります。

12. [保存] をクリックします。

13. ポリシーをただちに適用するには、[ポリシーの配信] をクリックします。すぐに適用しない場合、データベースキャッシュの有効期限が切れた後に、このポリシーが適用されます。

警告： **プロキシモードでは、IWSVA はクライアントのブラウザのドメインに基づいて HTTPS 復号化ポリシーを適用します。ただし透過モードでは、IWSVA はクライアントのドメイン情報を取得できないため、HTTPS 復号化ポリシーはサーバ証明書の CommonName に適用されます。**

HTTPS 復号化設定

[HTTP] → [HTTPS 復号化] → [設定] の順に選択して、次の項目を設定します。

- サーバ証明書の検証
- クライアント証明書の処理
- 認証機関

サーバ証明書の検証

[サーバ証明書の検証] 画面で、サーバ証明書の検証を有効にして、証明書失効リストの検索や証明書の正当性の確立などの証明書のテストを自動化するように検証設定を行います。

注意： 証明書の検証を無効にすると、クライアントはサーバ証明書の確認を行わずに任意の HTTPS Web サイトにアクセスできます。

証明書が証明書の検証テストに合格しなくても、クライアントは HTTPS 接続を介して Web サイトにアクセスすることを選択できます。クライアントのブラウザには警告画面が表示されます。

サーバ証明書の検証を設定をするには

1. 管理コンソールから [HTTP] → [HTTPS 復号化] → [設定] の順に選択します。[サーバ証明書の検証] 画面が表示されます。
2. [証明書検証を有効にする] を選択して、サーバ証明書を確認します。
3. 次のオプションの 1 つまたは複数を選択します。
   - CommonName **が** URL **に一致しない証明書を拒否する** — CommonName がアクセス先の URL と一致しない場合に証明書を拒否するには、このオプションを選択します。IWSVA はこの証明書を無効として扱います。
     - **ワイルドカード証明書を許可する** — このオプションを選択すると、CommonName がワイルドカードで表された証明書を許可および検証できます。このオプションを無効にすると、ワイルドカードを使用して表現された CommonName を含む証明書は拒否されます。
   - **有効期限の切れた証明書または不正な目的の証明書を拒否する** — このオプションを選択すると、有効期限が切れた証明書または意図した目的に使用できない証明書は拒否されます。
   - **証明書チェーン全体を検証する** — このオプションを選択すると、特定の証明書チェーン (提供された証明書からルート認証機関の証明書まで) が有効で信頼できることが確認されます。
   - CRL **による証明書失効確認** — 証明書取り消しリスト (CRL) を調べて証明書が失効している (無効になっている) かどうかを確認するには、このオプションを選択します。
4. [保存] をクリックします。

証明書の検証の除外

対象 Web サイトの証明書が検証に失敗した場合は、サーバ証明書の除外設定を追加して、IWSVA で特定の事前定義された処理を実行するようにできます。

除外項目には次の 2 つの種類があります。

- 証明書の種類 : 証明書の検証が HTTPS トラフィックで失敗した場合 (たとえば、Web サイトの証明書の有効期限が切れている場合など)、IWSVA では「警告」処理とともに、この証明書に対する証明書の種類の除外項目を自動的に追加します。

  この種類の除外項目の処理と説明は変更できます。
- URL の種類 : この画面で [追加] ボタンをクリックして、URL の種類の除外項目を追加できます。

クライアント証明書の処理

オンラインバンキングなどの多くのセキュリティの高いアプリケーションでは、Web サーバがクライアントを認証するためにクライアント証明書を要求する場合があります。IWSVA ではクライアント証明書を要求する Web サイトはサポートされないので、[クライアント証明書の処理] 画面で接続をトンネルまたはブロックするように選択できます。

- **トンネル** — HTTPS トラフィックをバイパスするには、このオプションを選択します。IWSVA は、コンテンツを検査するために復号化しません。
- **ブロック** — リモートサーバへのアクセスを拒否するには、このオプションを選択します。

認証機関

初期設定では、IWSVA はプライベートな認証機関 (CA) として動作し、動的にデジタル証明書を生成します。このデジタル証明書はクライアントのブラウザに送信され、HTTPS 接続の安全なセッションを確立します。ただし、初期設定の CA はインターネット上の信頼できる CA によって署名されていないため、ユーザが HTTPS Web サイトにアクセスするたびに、クライアントブラウザに証明書に関する警告が表示されます。ユーザはその警告を無視しても安全ですが、IWSVA には独自の証明書を使用することをお勧めします。

CA 証明書をインポートするには

1. 管理コンソールから [HTTP] → [HTTPS 復号化] → [設定 | 証明機関] の順に選択します。
2. [証明書ファイル] の横にある [参照] をクリックして、証明書ファイルを選択します。- IWSVA は、Base64 エンコードの証明書と、PEM ファイル形式の RSA ベースの暗号化された秘密鍵をサポートしています。
3. [秘密鍵] の横にある [参照] をクリックして、CA 証明書に関連付けられた秘密鍵を選択します。
4. 秘密鍵の [パスフレーズ] を入力します。
5. [パスフレーズの確認] フィールドに再度パスフレーズを入力します。
6. [CA のインポート] をクリックします。

注意： - IWSVA は、Base64 エンコードの証明書と、PEM ファイル形式の RSA ベースの暗号化された秘密鍵のみをサポートしています。

CA 証明書のインポート後に、エンドユーザが安全な Web サイトにアクセスしようとして、そのユーザのコンピュータに証明書に関する警告画面 (図 8-6) が表示される場合があります。これが表示されないようにするには、関連する証明書を適切な Web ブラウザの信頼す

るルート認証機関のリストに追加します。詳細については、図 8-7 を参照してください。

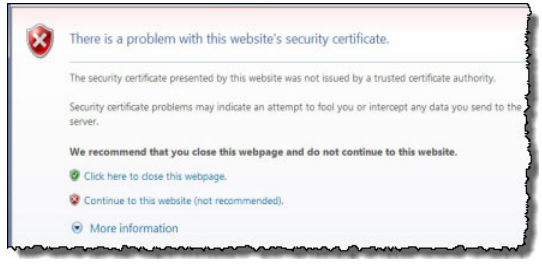


図 8-6.　証明書に関する警告画面

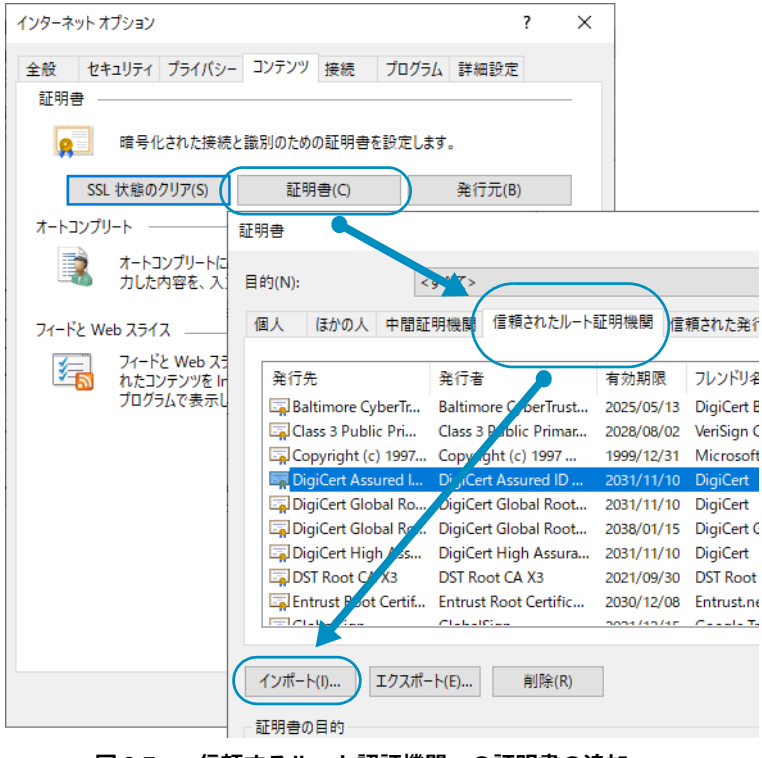


図 8-7.　信頼するルート認証機関への証明書の追加

CA 証明書 (公開鍵) をエクスポートするには

1. 管理コンソールから [HTTP] → [HTTPS 復号化] → [設定 | 証明機関] の順に選択します。
2. [CA 公開鍵の取得] をクリックします。
3. 画面上の指示に従って、証明書ファイルをコンピュータに保存します。

CA の秘密鍵をエクスポートするには

1. 管理コンソールから [HTTP] → [HTTPS 復号化] → [設定 | 証明機関] の順に選択します。
2. [CA 秘密鍵の取得] をクリックします。
3. 画面上の指示に従って、秘密鍵ファイルをコンピュータに保存します。

TLS/SSL プロトコル

TLS/SSL について

IWSVA では、TLS (Transport Layer Security) または SSL (Secure Sockets Layer) を使用して Web コンソールとサーバとの間の安全な通信を保証しています。

TLS とその前身である SSL は、データを暗号化して送受信するためのプロトコルです。これらのプロトコルを使用することで、Web コンソールとサーバは、長い非対称の公開鍵を使用して相互に認証を行い、安全にデータを送受信できるようになります。一度認証されると、Web コンソールとサーバで短い対称の秘密鍵が作成され、セッションの間、この秘密鍵を使用して通信データが暗号化されるようになります。公開鍵を使用して秘密鍵をリバースエンジニアリングすることはできません。

TLS および SSL プロトコルの認証では、X.509 証明書と非対称暗号化方式が使用されます。X.509 証明書を使用するには、認証局 (CA) と PKI (公開鍵インフラストラクチャ) を利用して、次のことを行う必要があります。

- 証明書の作成、署名、および認証
- 証明書とデータ送受信者との関係の確認

TLS/SSL 方式の指定

TLS/SSL 方式を指定するには

1. [HTTP] → [HTTPS 復号化] → [設定] → [SSL 方式] の順に選択します。
2. [クライアントの SSL 方式] および [サーバの SSL 方式] セクションでオプションを 1 つ以上選択します。

ドメイントンネリング

HTTPS トンネリングを使用すると、接続が制限されたネットワークの場所 (通常は NAT、ファイアウォール、またはプロキシサーバの内側) 間での通信が可能になります。接続の制限は通常、TCP/IP ポートのブロック、ネットワークの外部から開始されたトラフィックのブロック、またはほとんどのネットワークプロトコルのブロックによる結果で、これによりネットワークが内部および外部の脅威から保護されます。

グローバルな信頼リストと同様に、ドメイントンネルを使用すると、管理者は信頼されたサイトのリストを保持できます。

ドメイントンネルを設定するには

1. [HTTPS] → [HTTPS 復号化] → [トンネリング] に移動します。
2. 追加するドメイン名の一致を入力します。
3. 文字列 (完全な名前) に一致するするか、ドメイン全体に一致するかを選択します (ドメイン全体によるトンネルの横にはアスタリスクが表示されます)。
4. 承認されたエントリを含むファイルを以前に作成している場合は、[ファイルの選択] をクリックし、追加するファイルを選択して、[インポート] をクリックします。

   追加するトンネリングされたドメインが、[トンネリングされたドメイン] ボックスに表示されます。
5. [保存] をクリックします。

トンネリングされたドメイン

古くなったトンネルは、トンネリングされたドメインを選択して [削除] をクリックするか、[すべて削除] をクリックしてリスト全体をクリアすることで削除できます。[エクスポート] をクリックして安全な場所にリストを保存することで、トンネリングされたドメインのリストを保存することもできます。

トンネリングされたドメインの除外

除外もリストすることができます。除外リスト内のすべてのドメインが復号化されます。

HTTPS アクセスの失敗

HTTPS アクセスの試行の失敗は追跡および記録できます。管理者は、トンネルリストにトンネリングされたドメインを追加できます。ログは、時間、ユーザ名、およびドメインに基づいて検索できます。

[処理] 列には、ドメイン名をトンネリングリストに追加するためのボタンがあります。ドメインがすでにリストに含まれる場合は、列のスペースに「トンネリングあり」と表示されます。

HTTPS アクセスの試行の失敗を検索するには

1. [HTTPS] → [HTTPS 復号化] → [トンネリング] → [失敗した HTTPS アクセス] に移動します。
2. 自動トンネリングを開始する場合は、[致命的なエラーの場合に自動トンネリングを有効にする] オプションをオンにします。
3. レビューする HTTPS アクセスの失敗の数を、20、50、または 100 エントリから選択します。
4. 特定のユーザのアクセス試行を検索するには、[検索] ボックスにユーザのドメイン名に加えてユーザ名を入力します。

各エントリに対して、次の情報が表示されます。

- 日付
- ユーザ名 (ユーザまたは IP)
- ドメイン名
- 失敗した理由
- 処理

[処理] 列には、ドメイン名をトンネリングリストに追加するためのボタンがあります。ドメイン名がすでにリストに含まれる場合は、[処理] に「トンネリングあり」と表示されます。

高度な脅威保護ポリシーの作成と変更

初期設定のグローバルポリシーとゲストポリシーのほかに、組織の特別なメンバー用にカスタマイズした HTTP ウイルス検索ポリシーを作成できます。

新しいウイルス検索ポリシーを作成するには

1. 管理コンソールから [HTTP] → [高度な脅威保護] → [ポリシー] の順に選択します。
2. [ウイルス検索を有効にする] を選択してウイルス検索を有効にします。
3. [高度な脅威検索を有効にする] を選択して、高度な脅威検索エンジンを有効にします。

4. [Web レピュテーションを有効にする] を選択して Web レピュテーションを有効にします。

注意： Web レピュテーションは、ポリシーレベルで使用するため、グローバルレベルで有効にする必要があります。

5. [ボット検出を有効にする] を選択して、ボット検出を有効にします。
6. [追加] をクリックします。
7. [新規ポリシーの作成] に、わかりやすいポリシー名を入力します。

「エンジニア向けウイルスポリシー」や「研究者向け URL フィルタポリシー」など、ポリシーを適用するユーザやグループへの参照を含むポリシー名にすると、見分けやすくなります。
アカウントフィールドでは IPv6 アドレスがサポートされます。任意の IPv6 ホストに 1 つのルールを定義すると、クライアントが IWSVA を介して HTTP サイトにアクセスしたときにこのポリシールールがトリガされます。
使用可能なポリシーの選択時には、IPv4 と IPv6 の両方のポリシーが表示されます。[アカウント] フィールドで入力可能なアカウントエントリは、IPv4 でサポートされているものと同様に、単一の IPv6 アドレス、IPv6 アドレス範囲、または IPv6 マスクです。
IWSVA は、IPv6 で「配信前に検索」機能をサポートしており、IWSVA の IPv6 または IPv4 アドレスは、クライアントの IP アドレスのバージョンに基づいて、自動的にクライアントにリダイレクトされ処理が続行されます。

- クライアントが IPv4 アドレスを使用する場合、IWSVA は、リダイレクト要求を IWSVA の IPv4 アドレスとともに送信します。
- クライアントが IPv6 アドレスを使用する場合、IWSVA は、リダイレクト要求を IWSVA の IPv6 アドレスとともに送信します。

8. ポリシーを適用するユーザを選択します。

この画面のオプションは、使用しているユーザの識別方法に応じて異なります。[IP アドレス]、[ホスト名 (変更された HTTP ヘッダ)]、[IP サブセット]、または [ユーザ / グループ名認証] のいずれかになります。ユーザの識別方法の設定とポリシー適用範囲の設定の詳細については、160 ページの「ユーザ識別方法の設定」を参照してください。

注意： 設定したユーザの識別方法に関係なく、ポリシーを適用するクライアントの IP アドレスを入力できます。

9. 適用するアカウントを定義したら、[次へ] をクリックして HTTP ウイルス検索ルールの定義を続行します。

既存の高度な脅威保護ポリシーを変更するには

1. 管理コンソールから [HTTP] → [高度な脅威保護] → [ポリシー] の順に選択します。
2. 変更するポリシーの名前をクリックします。
3. Web レピュテーションルール、ウイルス検索ルール、ボット検出ルール、スパイウェア検索ルール、ポリシー除外、および検索処理を変更します。

   指定した検索処理がすべてのルールに適用されます。

既存の高度な脅威保護ポリシーでユーザを追加または削除するには

1. 管理コンソールから [HTTP] → [高度な脅威保護] → [ポリシー] の順に選択します。
2. 対象のウイルス検索ポリシーアカウントをクリックします。
3. [HTTP 検索ポリシー : 編集] 画面の [アカウント] タブで、ユーザを追加または削除します。
   - ユーザを追加するには、単一の IP アドレス、IP アドレス範囲、IP サブセット、またはユーザ / グループ名を指定して、影響を受けるユーザを示します。
   - ユーザを削除するには、ユーザの隣にあるごみ箱アイコンをクリックします。

HTTP ウイルス検索ポリシーを有効にするには

- グローバルレベルで HTTP 検索ポリシーを有効にするには
  [HTTP] → [HTTP 不正プログラム検索] → [ポリシー] の順にクリックして、[ウイルス検索を有効にする] を選択します。
- ポリシーレベルで HTTP 検索ポリシーを有効にするには
  [HTTP] → [HTTP 不正プログラム検索] → [ポリシー] の順にクリックし、追加したポリシーをクリックして、[ポリシーを有効にする] を選択します。

Web レピュテーションルールの指定

Web レピュテーションルールはポリシーレベルで作成されます。

Web レピュテーションルールを指定するには

1. Web レピュテーションがグローバルレベルで有効になっていることを確認します。

   Web レピュテーションは、ポリシーレベルで使用するため、グローバルレベルで有効にする必要があります ([HTTP] → [高度な脅威保護] → [ポリシー |Web レピュテーションを有効にする] チェックボックス)。
2. Web レピュテーションがポリシーレベルで有効になっていることを確認します。

   [HTTP] → [高度な脅威保護] → [ポリシー |Web レピュテーションルール] 画面の [追加] または [編集] オプションを使用して、[このポリシーで Web レピュテーションルールを使用する]

チェックボックスがオンになっていることを確認します。このチェックボックスは、初期設定でオンになっています。

3. URL ブロックのセキュリティレベルを指定します。

   Web レピュテーションスコアを受信すると、IWSVA はそのスコアがしきい値を下回っているか上回っているかを判断します。しきい値は、ユーザが設定したセキュリティレベルによって定義されます。初期設定のセキュリティレベルは中です。この設定は、誤検出を抑えながら、ほとんどの Web 脅威をブロックするため、お勧めします。

4. ファーミング / フィッシング /C&C コンタクト検出を許可または無効にします。

   初期設定では、すべての検出が有効になっています。213 ページの「フィッシング対策、ファーミング対策、および C&C コールバック試行検出」を参照してください。

フィッシング対策、ファーミング対策、および C&C コールバック試行検出

フィッシング攻撃とは、個人情報をだまし取ることを目的としたメールです。このメールには、ユーザを偽の Web サイトに誘導する URL が含まれており、そのサイトにアクセスすると、パスワード、クレジットカード番号、銀行口座番号などの個人情報を更新するように要求されます。

ファーミング攻撃とは、通常、金銭上の個人情報をだまし取る目的でユーザを偽の Web サイトにリダイレクトしようとする試みです。ファーミングは、偽の情報を与えて DNS サーバを改ざんすることによって、ユーザの要求を意図せぬ場所にリダイレクトします。困ったことに、Web ブラウザには正規の Web サイトに酷似したサイトが表示されます。

注意： フィッシング / ファーミング検出のソースは Web レピュテーションに基づいており、Web レピュテーションのポリシーのルールに含まれるため、Web レピュテーションがグローバルレベルで無効になっているとフィッシング対策 / ファーミング対策機能も無効になります。

ICAP モードでは、ファーミング対策はサポートされません。

コマンド & コントロールコールバック試行検出 (C&C コールバック) 攻撃は、トラフィックコンテンツで IRC コマンドを調べるか、またはハニーネットを設定することで、ボットネットの検出を試行するシステムです。

カスタム保護設定

IWSVA を Deep Discovery Inspector（DDI)、Control Manager または Apex Central、および Deep Discovery Analyzer（DDAN) サンドボックスと統合し、HTTP/HTTPS トラフィックを介した不正プログラムからのオフラインカスタム保護 APT 攻撃に対処できます。

ATSE エンジンを使用してウイルスや疑わしいファイルを検索できます。このエンジンは VSAPI エンジンよりも強力です。APT 検出を特定するようカスタム保護で設定可能な APT カスタム保護ルールを適用できます。カスタム保護設定は、Web コンソールの［HTTP] →［高度な脅威保護] →［カスタム保護] で指定できます。

カスタム保護を有効にする

DDI、Control Manager または Apex Central、および DDAN サーバとの IWSVA 統合を有効にするには、各製品のチェックボックスをオンにし、サーバアドレス、ポート番号、必要に応じて API キー情報を入力します。サーバとの接続が認識されない場合、IWSVA は設定を保存できません。

サンプル提出

DDAN に送信して検索する脅威またはファイルの種類を選択します。

リスクレベル設定

ブロックする不審オブジェクトのリスクレベルを選択します。変更を保存します。

処理

ブロックまたは監視する脅威のタイプに基づいて選択します。変更を保存します。

Web レピュテーション設定

Web レピュテーション設定では、次の項目を指定します。

- 感染した URL に関するフィードバックをトレンドマイクロに提出するかどうか
- URL がブロックされない監視のみのモードで Web レピュテーションを評価するかどうか

Web レピュテーションの有効化と無効化

IWSVA では、Web レピュテーションをグローバルレベルとポリシーレベルで有効 / 無効にすることができます。Web レピュテーションをグローバルレベルで無効にした場合は、自動的にポリシーレベルでも無効になります。

グローバルレベルで Web レピュテーションを有効 / 無効にするには

1. [HTTP] → [高度な脅威保護] → [ポリシー] → [ウイルス検索のグローバルポリシー] の順にクリックし、[Web レピュテーションルール] タブをクリックします。
2. [Web レピュテーションルール] 画面から、[このポリシーで Web レピュテーションルールを使用する] を選択して、Web レピュテーションを有効にします。Web レピュテーションを無効にするには、このチェックボックスをオフにします。

ポリシーレベルで Web レピュテーションを有効 / 無効にするには

1. [HTTP] → [高度な脅威保護] → [ポリシー] → [< ポリシー名 >] の順にクリックし、[Web レピュテーションルール] タブをクリックします。
2. [このポリシーで Web レピュテーションルールを使用する] チェックボックスをオンにしてこのポリシーで Web レピュテーションを有効にするか、チェックボックスをオフにして無効にします。

Web レピュテーション結果の管理

IWSVA には、Web レピュテーションの結果を管理するためのオプションが 2 つあります。

- **フィードバックオプション**: 感染した URL についてフィードバックが提供可能なため、Web レピュテーションデータベースの精度を上げるのに役立ちます。
- **監視のみのオプション**: 既存の Web アクセスポリシーに影響を与えずに Web レピュテーションの有効性を監視できます。

どちらか一方のオプションまたは両方のオプションを選択できます。

このオプションを設定するには、Web コンソールで [HTTP] → [高度な脅威保護] → [設定] の順にクリックします。

Web レピュテーションの管理を設定するには、Web コンソールで [HTTP] → [高度な脅威保護] → [設定] の順に移動します。

フィードバックオプション

現行の動的な URL ブロックリストに加えて、ウイルス検索結果を URL ローカルキャッシュと外部のバックエンド評価サーバにフィードバックできます。Trend Micro Feedback Engine（以下、TMFBE) では、IWSVA がウイルス検索結果をバックエンド評価サーバに送り返すためのフィードバックメカニズムが用意されています。このフィードバックオプションは初期設定で有効になっています。オプションを無効にするには、[HTTP] → [高度な脅威保護] → [設定] に移動し、[フィードバックオプション] で [感染した URL のフィードバックをトレンドマイクロに送信する] チェックボックスをオフにします。

注意： 上位プロキシモードを使用する場合、トレンドマイクロのサイト (www.trendmicro.co.jp) へのアクセスを IWSVA の IP アドレスに明示的に許可するように、プロキシサーバを設定する必要がある場合があります。

感染が検出された場合

トレンドマイクロのウイルス検索エンジンからの検索結果で感染が検出された場合、感染した URL は次の場所に送り返されます。

- 動的な URL ブロックリスト
- Web レピュテーションスコアを調整した URL ローカルキャッシュ
- VirusName と IntelliTrap フラグを含む TMFBE フィードバックバッファ。このバッファのエントリ数が 10 になるか、または、最後のフィードバックから 5 分が経過すると、これらの URL が順次バッチでバックエンド評価サーバに送信されます。

感染が検出されなかった場合

トレンドマイクロのウイルス検索エンジンからの検索結果で感染が検出されなかった場合、その URL は URL ローカルキャッシュに保存されます。これによって、トレンドマイクロのウイルス検索エンジンで同じ URL が再度検索されることがなくなります。

監視のみのオプション

監視のみのオプションでは、Web レピュテーション結果を評価する機会が与えられます。このオプションを選択した場合、URL ブロックログまたはセキュリティリスクレポートから Web レピュテーション結果を監視できます。この結果には、Web レピュテーション、フィッシング対策、およびファーミング対策によってフィルタにかけられた URL のみが含まれます。Web レピュテーション結果のみ監視するため、URL ブロックは発生せず、URL はクライアントに渡されます。

初期設定で、監視のみのオプションは無効になっています。

WRS/URL キャッシュのクリア

ユーザがある URL にアクセスしようとすると、IWSVA はこの URL についての情報をリモートデータベースの Web レピュテーションデータベースから取得し、ローカル WRS/URL キャッシュに保存します。リモートサーバ上に Web レピュテーションデータベースを配置して、そのデータベース情報を使用してローカル WRS/URL キャッシュを構築すると、IWSVA 上のオーバーヘッドを削減して、パフォーマンスを向上させることができます。

要求された URL に対して Web レピュテーションデータベースから WRS/URL キャッシュに保存される情報の種類は、次のとおりです。

- Web カテゴリ
- ファーミング / フィッシング検出で使用されるファーミングフラグとフィッシングフラグ
- URL をブロックするかどうかを判断するために使用される Web レピュテーション評価の結果 (212 ページの「Web レピュテーションルールの指定」を参照)

URL キャッシュには、頻繁にアクセスされる URL が保存され、すばやく検索できます。新しい URL の検索が必要な場合、または、キャッシュサイズがパフォーマンスに影響を及ぼす場合のみ、キャッシュをクリアします。

注意： キャッシュをクリアすると、HTTP 検索デーモンが停止し、再起動するため、IWSVA サービスが中断する場合があります。

WRS/URL キャッシュをクリアするには

1. 管理コンソールで [HTTP] → [設定] → [WRS/URL キャッシュ] の順に選択します。
2. [キャッシュをクリア] をクリックします。

コンテンツキャッシュの使用

注意： 設定の複製受信者のコンテンツキャッシュが無効になっている場合は、設定の複製受信者が設定の複製送信者からコンテンツキャッシュ設定を取得しても、コンテンツキャッシュ機能が反映されません。

Web コンテンツキャッシュは Web オブジェクト (HTML ページや画像など) のキャッシュであり、帯域幅使用率、サーバの負荷、認識される遅延を削減します。Web キャッシュは、通過するオブジェクトのコピーを格納します。一定の条件を満たせば、以降の複製要求はキャッシュで処理できます。キャッシュオブジェクトは、IWSVA により再検索されます。

IWSVA 経由で Web にアクセスするユーザは、コンテンツキャッシュ機能により、帯域幅を節約しながら操作をより速く実行できます。

注意： この機能は、プロキシ転送モードおよび WCCP モードで利用できます。コンテンツキャッシュ機能は、他のモードではグレーアウトし動作しなくなります。

管理者はコンテンツキャッシュ機能を使用して、IWSVA の受信トレイのキャッシュを有効または無効にしたり、Web コンソールを介してキャッシュを管理したりすることができます。

注意： コンテンツキャッシュ機能は、CLI から無効にすることはできません。

コンテンツキャッシュの有効化 / 無効化

コンテンツキャッシュ機能を有効 / 無効にするには

1. [HTTP] → [設定] → [コンテンツキャッシュ] に移動します。
2. コンテンツキャッシュ機能を有効にするには、画面上部の [コンテンツキャッシュを有効にする] チェックボックスをオンにします。図 8-8 を参照してください。
3. [保存] をクリックします。
4. コンテンツキャッシュ機能を無効にするには、[コンテンツキャッシュを有効にする] チェックボックスをオフにします。

5. [保存] をクリックします。

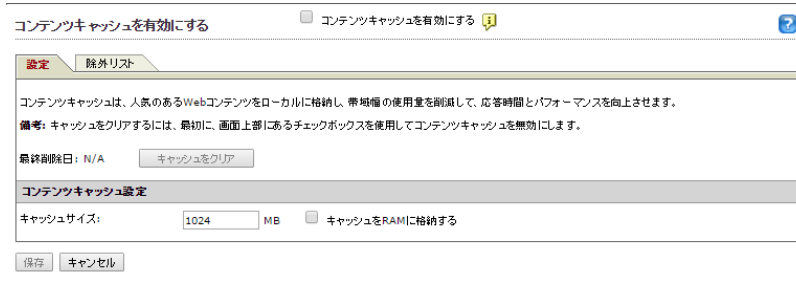


図 8-8.　コンテンツキャッシュ画面

コンテンツキャッシュのクリア

コンテンツキャッシュをクリアするには

1. [キャッシュをクリア] をクリックします。以下の警告が表示されます。

   「サイズの大きなキャッシュをクリアするには、長時間かかる可能性があります。キャッシュをクリアしますか ?」

2. [OK] をクリックします。キャッシュのクリア中に、進行状況を示すバーが表示されます。

   クリア処理が終了するまで、[キャッシュをクリア] ボタンと [コンテンツキャッシュを有効にする] チェックボックスはどちらも無効になります。キャッシュのクリアが終了したら、「最終削除日」が更新されます。

コンテンツキャッシュの管理

管理者は、次のコンテンツキャッシュ領域を設定できます。

- コンテンツキャッシュに対するハードディスク使用率
- コンテンツキャッシュに対する RAM 使用率

コンテンツキャッシュを管理するには

1. コンテンツキャッシュの [設定] タブの [コンテンツキャッシュに対するハードディスク使用率] に移動します。
2. [キャッシュサイズ] に容量を入力します。図 8-8 を参照してください。

   管理者は、キャッシュされたコンテンツの格納に使用するディスク容量または RAM を調整できます。キャッシュ容量が大きくなれば、より多くの Web オブジェクトをキャッシュできるようになります。キャッシュのパーティションが小さくなれば、キャッシュ可能なオブジェク

ト数が少なくなります。キャッシュ容量が非常に小さく、キャッシュ用のディスク容量が不足していると、IWSVA がリアルタイムコンテンツを取得する割合が増え、ローカルキャッシュ内のコンテンツを使用する割合が減るため、ヒット率が低下する可能性があります。
IWSVA の設定に基いて、利用可能なキャッシュサイズを指定してください。

3. [キャッシュを RAM に格納する] チェックボックスをオンにして、キャッシュを RAM に保存できるようにします。[キャッシュを RAM に格納する] チェックボックスがオフになっている場合、キャッシュは /var/cache/trafficserver/ に保管されます。
4. [保存] をクリックします。

コンテンツキャッシュの除外リスト

管理者が特定の URL をキャッシュしたくない場合、その URL をキャッシュの除外リストに追加できます。このリストでの動作は URL ブロックリストの場合と同じです。除外リストには Web サイト、URL キーワード、または文字列を追加できます。リストに一致する URL は、IWSVA によってキャッシュされません。

IWSVA では、特定の Web ページ、ドメイン、および URL をブロックして、コンテンツキャッシュに保存されないようにすることができます。コンテンツキャッシュからブロックされる URL は、ポリシーベースではありません。これは、組織内のすべてのユーザに影響を与えます。

注意： コンテンツキャッシュは、プロキシ転送モードおよび WCCP モードでサポートされます。

コンテンツキャッシュから URL をブロックすることで、サイズの大きな Web サイトがキャッシュされることを防いで、より一般的に使用される Web サイトのために効率的にキャッシュスペースを使用できるようになります。

- **コンテンツキャッシュを有効にする** — コンテンツキャッシュを有効または無効にします（コンテンツキャッシュを有効または無効にした後、[保存] をクリックします)。
- **一致** — 正確な Web サイト、キーワードか語句、または文字列を入力してから、一致を適用する方法を指定します。
- **前方一致** — URL を前方一致で照合します。このタイプのブロックは、Web サイト全体をキャッシュさせないようにする場合に特に役立ちます。URL には、http:// や https:// を含める必要はありません。入力しても、自動的に除去されます。
- 部分一致 — URL 内の任意の文字または数値から成る文字列を検索します。文字列が存在する場所に関係なく一致対象となります。たとえば「http://www.encyclopedia/content/sexton.htm」は、文字列「sex」の一致対象と見なされ、このページはブロックされます。

- **完全一致** — 文字列全体で照合します。たとえば、特定のサイト、ページ、ファイル、またはその他特定のアイテムを対象とします。
- **ブロックリスト / 除外リストのインポート** — コンテンツキャッシュからブロックまたは除外する URL の、既存のリストをインポートできます。たとえば、Trend Micro InterScan WebManager の URL リスト (整形が必要)、またはテキストエディタを使用して編集したリストをインポートできます。インポートされるリストは、規定の基準に適合する必要があります。

コンテンツキャッシュの除外リストの形式

コンテンツキャッシュの除外リストでは、除外リストのインポートに以下の形式が使用されます。

```
[no_cache]
@www.example1.com*
www.example2.com/c.jgp
*example3*
```

HTTP ウイルス検索ルール

IWSVA 管理者は、ブロックするファイルタイプと検索するファイルタイプ、および圧縮ファイルとサイズの大きいファイルの処理方法を設定できます。

[ウイルス / 不正プログラム検索ルール] タブで、[HTTP] → [高度な脅威保護] → [ポリシー] | [< ポリシー名 >] を参照してください。

高度な脅威検索

検索時に脅威を監視するかまたはブロックするかを選択します。

ブロックするファイルタイプの指定

セキュリティ、監視、またはパフォーマンス上の目的のためにブロックするファイルのタイプを識別できます。ブロックされたファイルは、要求元のクライアントによって受信されることも、検索されることもありません。ブロックされたファイルタイプの取得要求は実行されません。Microsoft Office 文書、画像、実行可能ファイル、オーディオ / ビデオファイル、Java クラスファイル、アーカイブ、または指定するその他のファイルタイプなどのファイルタイプをブロックするオプションが提供されています。

ブロックするファイルタイプを指定するには

1. ポリシーの追加または編集時に、[ウイルス / 不正プログラム検索ルール] → [ブロックするファイルタイプ] で、ブロックするファイルタイプのチェックボックスをオンにします。これによって、そのカテゴリのファイルがすべてブロックされるようになります。
2. 選択したカテゴリ内のファイルタイプをブロック解除するには、[詳細の表示] リンクをクリックします。
3. ブロックしないファイルのチェックボックスをオフにします。

検索するファイルタイプの指定

IWSVA には次の HTTP 検索機能があります。

- すべての検索可能ファイル
- トレンドマイクロの推奨設定
- 指定のファイル拡張子
- IntelliTrap

注意 : より高いレベルのセキュリティを実現するには、すべてのファイルを検索することをお勧めします。

トレンドマイクロの推奨設定について

現在、ほとんどのウイルス対策ソリューションは、潜在的な脅威に備えて検索するファイルを決定するにあたり、2 つのオプションを提供しています。最も安全なアプローチである、すべてのファイルを検索するオプションと、最も感染しやすいとされる特定の拡張子のファイルのみを検索するオプションです。ただし、最近ではファイルの拡張子を変更して「偽装した」ファイルが開発されているため、後者のオプションの効力が低下しています。トレンドマイクロの推奨設定は、ファイル名の拡張子に関係なく、ファイルの「実際のファイルタイプ」を識別するトレンドマイクロのテクノロジです。

注意 : トレンドマイクロの推奨設定では各ファイルのヘッダを検査し、一定の基準に基づいて、ウイルス感染を受けやすいと判定されるファイルのみを検索します。

実際のファイルタイプについて

トレンドマイクロの推奨設定を有効にすると、検索エンジンは、実際のファイルタイプを確認するために、ファイル名ではなくファイルヘッダを検査します。たとえば、検索エンジンがすべての実行可能ファイルを検索するように設定されていて、`family.gif` という名前のファイルが見つかった場合、そのファイルをグラフィックファイルとして受け入れて検索をスキップすることはしません。その代わりに、検索エンジンはファイルのヘッダを開き、ファイルが本当にグラフィックファイルかどうか、あるいは、検出されないように虚偽の命名がされている実行可能ファイルかどうかなどを判定するために、内部に登録されたデータタイプを検査します。

実際のファイルタイプ検索は、トレンドマイクロの推奨設定と連携して潜在的な脅威として知られているファイルタイプのみを検索します。これらのテクノロジによって検索エンジンが検査する必要のあるファイルの総数を最大で 3 分の 2 くらいまで削減できますが、その代償として潜在的なリスクが高まります。

たとえば、.gif ファイルと .jpg ファイルは Web トラフィックの大部分を占めています。悪意あるハッカーが、検索エンジンを回避してひそかにネットワークに侵入するために、有害なファイルに「安全な」ファイル名を付ける可能性があります。このような場合でも、トレンドマイクロの推奨設定では、実際のファイルタイプを確認してウイルス検索し、不正コードがネットワークに侵入するのを阻止します。

検索するファイルタイプを選択するには

IWSVA は、IWSVA を通過するすべてのファイル、または実際のファイルタイプチェック（トレンドマイクロの推奨設定) またはファイル拡張子によって決定されるファイルのサブセットのみを検索できます。さらに、圧縮ファイル内に含まれる個々のファイルも検索できます。

1. 検索するファイルを選択します。
   - ファイル名の拡張子に関係なく、すべてのファイルタイプを検索するには、[すべての検索可能ファイル] を選択します。IWSVA は、圧縮したファイルを開き、その中のすべてのファイルを検索します。これは、最も安全な推奨設定です。
   - 実際のファイルタイプによる識別を使用するには、[トレンドマイクロの推奨設定] を選択します。この設定では、ファイルの実際のファイルタイプを確認することで、ウイルスが潜伏していることがわかっているファイルタイプを検索します。実際のファイルタイプの確認は、ファイル名の拡張子とは無関係に行われるので、実際のファイルタイプを隠すために潜在的に有害なファイルの拡張子が変更されるのを防ぎます。
   - すべての HTTP トラフィックを検索する際に起こり得るパフォーマンスの問題を回避するために、拡張子に基づいて検索するファイル、または除外するファイルタイプを明示的に設定できます。ただし、ファイル拡張子はファイルの内容を判定するのに信頼できる方法ではないため、この設定はお勧めしません。

選択したファイルタイプのみを検索するには、[指定する拡張子] を選択してリストをクリックします (トレンドマイクロはこの設定をお勧めしません)。[拡張子による指定] 画面が開きます。初期設定の拡張子リストは、ウイルスが潜伏している可能性があると知られているすべてのファイルタイプを示しています。このリストは、ウイルスパターンファイルがリリースされるとアップデートされます。[拡張子による指定] 画面で、[その他の拡張子] と [除外する拡張子] に追加の拡張子を追加するかまたは除外します。

検索する、または検索から除外する拡張子をピリオドを入れずに入力します。通常は 3 文字です。拡張子の前にワイルドカード (*) 文字は付けないでください。また、複数のエントリはセミコロンで区切ります。

入力が完了したら [OK] をクリックします。画面が閉じます。

2. 特定の MIME コンテンツタイプを選択的に無視するように IWSVA を設定できます。RealAudio やその他のストリーミングコンテンツなどのファイルタイプは、ファイルの最初の一部がクライアントコンピュータに到着するとただちに再生されるため、結果的に遅延が発生して正しく動作しません。[ウイルス検索ルール] タブの [検索を省略する MIME コンテントタイプ] に適切な MIME タイプを追加することにより、IWSVA でこれらのファイルタイプを検索から除外できます。[検索を省略する MIME コンテントタイプ] に、無視する MIME コンテンツタイプを入力します。たとえば、image/、audio/、application/x-director video/、application/pdf です。詳細については、付録 B「ファイルタイプと MIME コンテンツタイプの対応」を参照してください。

   [MIME タイプの検証を有効にする] チェックボックスをオンにして、実際のファイルタイプの検索を有効にすることもできます。このオプションによって、MIME ストリームでの実際のファイルタイプのチェックが有効になります。ただし、すべての MIME タイプが正確に検出されるわけではありません。誤検出が発生する場合は、MIME タイプの検証を無効にして、代わりにコンテンツタイプを使用します。

注意： トレンドマイクロは、ウイルス感染の脅威を軽減するために、除外する MIME コンテンツタイプのリストを最小限に抑えることをお勧めします。さらに、トレンドマイクロは、MIME コンテンツタイプの偽造が可能なため、サイズの大きいファイルの処理が有効になっているときには、どの MIME コンテンツタイプも除外しないことをお勧めします。

図 8-9.　新しいパターンファイルごとにアップデートされる検索対象推奨拡張子

IntelliTrap について

IntelliTrap では、HTTP データとともに圧縮された実行可能ファイルを受信した場合、潜在的な不正コードをリアルタイムで検出します。ウイルス作成者は、複数のファイル圧縮スキームを使用して、ウイルスフィルタを回避しようとします。IntelliTrap では、圧縮ファイルのヒューリスティック評価を提供することにより、そうした方法で圧縮されたウイルスが Web を通してネットワークに侵入するリスクを軽減します。

IntelliTrap には次のようなオプションがあります。

- 検索ポリシーごとに [ウイルス検索ルール] タブで有効 / 無効にできるオプション (IntelliTrap は初期設定で有効)
- 不正な圧縮された実行可能ファイルに対して [処理] タブで指定された処理が実行されるオプション

IntelliTrap を有効 / 無効にするには

- [HTTP] → [高度な脅威保護] → [ポリシー] | [< ポリシー名 >] | [ウイルス / 不正プログラム検索ルール] タブの順に選択し、IntelliTrap セクションの [IntelliTrap を有効にする] チェックボックスをオンにします。

IntelliTrap の詳細については、121 ページの「IntelliTrap パターンファイルおよび IntelliTrap 除外パターンファイル」を参照してください。

ウイルス / 不正プログラム検索設定の優先順位

IWSVA は、次の優先順位で検索を実行します。

1. ブロックするファイルタイプ
2. 除外する MIME コンテンツタイプ
3. 検索するファイルタイプ

圧縮ファイルの検索制限の設定

圧縮ファイルの検索制限は、ポリシーごとに設定できます ([HTTP] → [高度な脅威保護] → [ポリシー] → [< ポリシー名 >] の順に選択して、[ウイルス検索ルール] タブをクリックします)。IWSVA は、HTTP ウイルス検索設定画面で指定した条件に従って、圧縮ファイルの内容を開いて検査します。また、IWSVA は、設定可能な制限 (圧縮アーカイブ内のファイル数、非圧縮時のファイルサイズ、圧縮レイヤ数、および圧縮率) に従ってファイルを解凍します。

圧縮ファイルの検索制限を設定するには

[圧縮ファイルの処理] で、次の設定を行います。

- **処理** — IWSVA が圧縮ファイルの違反を検出したときに実行する処理 ([放置]、[ブロック]、または [隔離]) を選択します。
- **適用先** — 次のオプションのいずれかを選択します。
  - **すべての圧縮ファイル** — 圧縮ファイルをダウンロードするすべての要求が一致対象となります。

- **圧縮ファイルが次の場合** — 設定された条件を超える圧縮ファイルをダウンロードする要求のみが一致対象となります。次のパラメータの値を入力します。
  - 解凍後のファイルが次の数を超える場合 (初期設定は 50000)
  - 解凍後のファイルが次のサイズを超える場合 (初期設定は 200MB)
  - 圧縮レイヤが次の数を超える場合 (範囲は 0 ～ 20、初期設定は 10)
    ※ 「0」を指定した場合は、本機能が無効になります。
  - 圧縮率が 99% を超える場合 (初期設定は無効)

IWSVA は、ゲートウェイで指定された条件を満たす圧縮ファイルに対して選択された処理を適用し、ファイルは検索されません。たとえば、図 8-10 に示されているように設定されているとします。

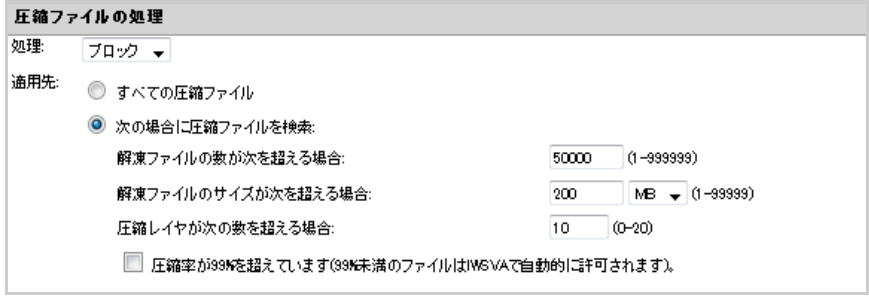


図 8-10. 「解凍の割合」を使用して IWSVA デバイスに対する DoS 攻撃を防ぐことができる

圧縮レベルが 10 を超える、または含まれるファイル数が 10,000 を超える圧縮ファイルは、ゲートウェイを通過しません。

サイズの大きいファイルの処理

サイズの大きいファイルの場合、ユーザの期待するパフォーマンスとセキュリティ維持の間でのトレードオフが必要となります。ウイルス検索の本質上、サイズの大きいファイルの場合、ファイル全体を IWSVA に転送してファイルを検索し、ファイル全体をクライアントに転送するために、ダウンロード時間が 2 倍かかります。環境によっては、2 倍かかるダウンロード時間を受け入れられない場合があります。ネットワークの速度やサーバの機能など、考慮する必要のある要素がほかにもあります。サイズの大きいファイルの処理を実行するほどサイズが十分に大きくない場合は、そのファイルは普通のファイルとして検索されます。

ユーザがファイルのダウンロードを試みているときにブラウザがタイムアウトする場合、サイズの大きいファイルの処理の設定を検討します。サイズの大きいファイルの検索には、次の 2 つのオプションがあります。

- 228 ページの「配信前に検索」
- 229 ページの「遅延検索」

配信前に検索

IWSVA が配信前に検索するオプションを使用するように設定されている場合、要求されたファイルは検索が終了するまでクライアントに渡されません。ブラウザのタイムアウトを防ぎ、検索が進行中であることをユーザに通知するために、進行ステータス画面が生成されます。

注意 : サイズの大きいファイルを処理する場合、IWSVA では進行ステータス画面においてダウンロードの進行ステータスを表示します。

進行ステータス画面が機能するには、外部に見えているどの IP アドレスにクライアントが接続するかを IWSVA が判別する必要があります。127.0.0.1 を使用すると問題が生じます。進行ステータス画面に関するメッセージが表示された場合、ホスト名による解決が 127.0.0.1 にならないように、コンピュータの IP アドレスを `iscan_web_server` に追加する (例 : `iscan_web_server=1.2.3.4:8443`) か、または `/etc/hosts` ファイルを変更します。

注意 : YouTube、Windows Update、ストリーミングなどのインターネットアプリケーションでは、特定の時間内に一定の量のデータをクライアント側で受信するようプログラミングされているものがあります (たとえば、90 秒以内に 20% のデータまたは 1MB のデータを受信するようプログラミングされているものなど)。配信前に検索するオプションを IWSVA が使用するように設定されている場合、要求されたファイルは検索が終了するまでクライアントに渡されません。この場合、インターネットアプリケーションでは、クライアント側が時間内に必要なデータを受信していないために転送エラーを検出する場合があります。そうなると、クライアント側ではビデオファイルやストリーミングファイルを処理できません。

遅延検索

IWSVA が遅延検索オプションを使用するように設定されている場合は、検索が続行されている間に、設定可能な割合の Web ページがクライアントに配信されます。ただし、ウイルス検索によって検索が中断された場合、Web ページ全体は配信されません。検索せずにクライアントに定期的に送信する受信データの割合の値を 100% に設定した場合、最後の 4KB は検索が完了するまでクライアントに送信されません。遅延検索オプションを使用する場合は、検索せずにクライアントに定期的に送信する受信データの割合を設定します。

ダウンロードするデータの割合 (%) には、20、40、60、80、または 100 を指定できます。初期設定の割合 (%) は 60 です。ブラウザに送信されたデータの実際の割合は、指定された値よりかなり少ない場合があります。

注意 : Blue Coat Port 80 Security Appliance を ICAP モードで使用する場合、サイズの大きいファイルを処理できません。さらに、ICAP モードで Blue Coat Security Appliance を使用している場合は、クライアントがサイズの大きいウイルス感染ファイルをダウンロードしたときに、クライアントブラウザにウイルスブロック通知画面が表示されないことがあります。代わりに、クライアントブラウザには、「Page cannot be displayed」と表示されます。ただし、IWSVA が Blue Coat Appliance に適した HTTP プロキシとして設定された場合、サイズの大きいファイルを処理できます。

IWSVA が受信した外部データは、検索が行われないまま、より小さいブロック単位でブラウザに送信されます。最後のブロックがブラウザに送信されると、データセット全体に対して検索が行われ、ダウンロードが完了します。ブロック送信によって、IWSVA と Web ブラウザ間の接続が維持されるだけでなく、ダウンロードの進行状況がエンドユーザに示されます。

サイズの大きいファイルの処理は、ポリシーごとに設定できます ([HTTP] → [高度な脅威保護] → [ポリシー] → [< ポリシー名 >] の順に選択して、[ウイルス / 不正プログラム検索ルール] タブをクリックします)。

図 8-11. サイズの大きいファイルに対する特殊処理の 2 つのオプション : (1) 配信前に検索と (2) 遅延検索

サイズが非常に大きいファイルのダウンロード時に生じるパフォーマンスの問題を軽減するには、[検索するファイルサイズの上限を設定する] オプションをオンにして、サイズの大きいファイルの検索を無効にします。これによって、整合性を制御できるようになります。

サイズの大きいファイルの検索を無効にするには

- [サイズの大きいファイルの処理] で [検索するファイルサイズの上限を設定する] チェックボックスをオンにして、検索するファイルサイズの上限を設定します。

  ネットワークにセキュリティの脆弱性が生じるため、サイズの大きいファイルであっても、検索は無効にしないことをお勧めします。

HTTP ウイルス検索でサイズの大きいファイルの処理を使用するには

1. [サイズの大きいファイルの処理] で [特殊処理を有効にする] チェックボックスをオンにして、サイズの大きいファイルと見なすファイルサイズ (KB または MB の単位) を入力します。
2. 使用するサイズの大きいファイル処理のタイプを選択します。
   - **配信前に検索** — 検索中の進行ステータスをクライアント上に表示し、その後ファイルを検索します (初期設定)。
   - **遅延検索** — 検索中にファイルの一部をクライアントに配信し、ウイルスが見つかると接続を停止します。

3. [保存] をクリックします。

サイズの大きいファイルの処理に関する重要な注意

- サイズの大きいファイルの処理に違反すると、要求元のクライアントのブラウザにユーザ通知が表示されます。
- サイズの大きいファイルの特殊処理は、HTTP 検索、FTP 検索、および HTTP プロキシを介した FTP over HTTP にのみ適用されます。ICAP トラフィックの FTP over HTTP には適用されません。FTP over HTTP を使用してサイズの大きいファイルをダウンロードしているとき、タイムアウトの問題が発生する場合があります。
- IWSVA では、「遅延検索」を使用している場合、最初に感染ファイルをダウンロードしたクライアントに対してはファイルが削除されず、配信されます。

隔離ファイルの処理

IWSVA が不正ファイルとして検出したファイルを隔離する場合、[隔離ファイルを暗号化する] チェックボックスをオンにすると、ファイルを暗号化してから隔離ディレクトリに移動できます。これにより、意図せずにファイルを実行してしまったり、開いたりしてしまう可能性がなくなります。暗号化されたファイルは、トレンドマイクロのサポートエンジニアによってのみ暗号を解除できることに注意してください。

[HTTP] → [高度な脅威保護] → [ポリシー] のポリシーの追加 / 編集画面で HTTP ウイルス検索ルールを設定したら、[次へ] をクリックしてスパイウェア検索ルールに移動します。

スパイウェア検索ルール

IWSVA が使用するパターンファイルには、コンピュータウイルスのほかに、多数の潜在的脅威に関する署名が含まれています。こういった脅威は、自己複製して拡散することはないので、ウイルスではありません。しかし、ユーザの知らないうちに個人情報を収集、転送したり、ポップアップウィンドウを表示したり、ブラウザのホームページを変更するなど、望ましくない処理や予測されない処理を実行することがあります。

IWSVA は、次の脅威を検索するように設定できます。

- **スパイウェア** — ユーザが知らないうちに、またはユーザの承諾なしに、ひそかに情報を収集および転送するソフトウェア
- **ダイヤラー** — ユーザのモデムを通じてひそかに課金式の電話番号や国際電話番号にダイヤルするソフトウェア
- **ハッキングツール** — 不正なハッキング目的に使用できるソフトウェア

- **パスワード解読アプリケーション** — コンピュータのパスワードおよびその他の認証スキームを無効にするために設計されたソフトウェア
- **アドウェア** — ユーザのブラウザまたはポップアップウィンドウにユーザを対象とする広告を表示するために、ユーザの Web 閲覧動作に関する情報を監視および収集するソフトウェア
- **ジョークプログラム** — ユーザを困らせたり不適切な警告を発したりするプログラム
- **リモートアクセスツール** — コンピュータへのアクセスが許可されるように設計されたソフトウェアで、多くの場合ユーザの承諾を得ていません。
- **その他** — 上記の分類に当てはまらないファイル。このうち一部は、不正な行動を取る可能性があるだけでなく、合法な目的を持つツールまたは商用ソフトウェアである場合があります。

スパイウェアおよびその他の不正プログラムを検索するには

1. [HTTP] → [高度な脅威保護] → [ポリシー] → [< ポリシー名 >] の順に選択して、[スパイウェア検索ルール] タブをクリックします。[その他の不正プログラムに対する検索] で、検出するその他の脅威の種類を選択します。

   パターンファイルにシグネチャがあるすべての脅威を検索するには、[すべて選択] をオンにします。

2. [次へ] をクリックして、セキュリティの脅威に対する処理を設定します。

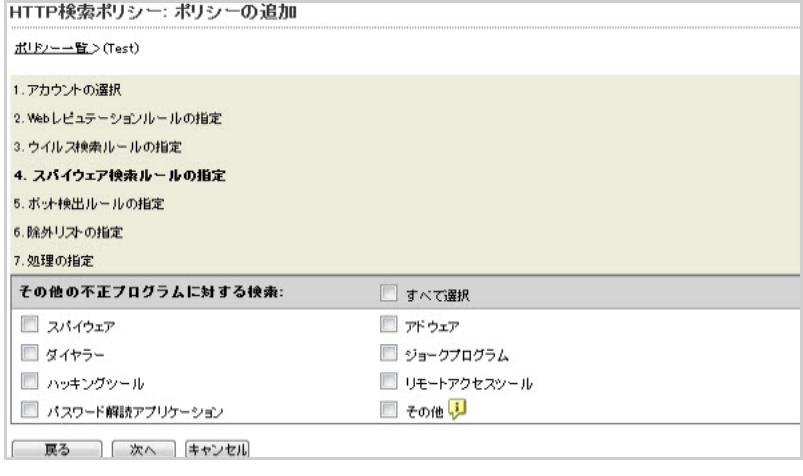


図 8-12. スパイウェアおよびその他の脅威の検索の設定

高度な脅威保護のパフォーマンスに関する考慮事項

不正コンテンツを見つけるために HTTP トラフィックを検索する際、パフォーマンスとセキュリティのトレードオフがあります。ユーザは、Web サイト上のリンクをクリックするとき、すばやい応答を期待します。ただし、ゲートウェイのウイルス対策ソフトウェアがウイルス検索を実行するので、応答までの時間が長くなる場合があります。要求されるファイルによってはサイズが大きく、安全かどうか判定するには、ユーザに送る前にそのファイル全体のダウンロードが必要になる場合もあります。また、コンテンツは、多数の小さいファイルで構成されていることもあります。この場合、ファイルの検索に必要な時間の合計がユーザの待機時間となります。

ユーザの操作性を向上させる方法の 1 つとして、サイズの大きいファイルやウイルスが潜伏している可能性の低いファイルを検索から除外する方法があります。たとえば、拡張子「.gif」を持つすべてのファイル、または MIME タイプのすべてのファイルを検索から除外します。

MIME コンテンツタイプによってファイルの検索を除外するように設定されている場合、IWSVA は、除外する前にそのファイルの実際のファイルタイプを判定し（この機能が有効になっているとき)、宣言された MIME タイプと照合します。ファイルの実際のファイルタイプが、トランザクションに添付されているコンテンツタイプヘッダに示されているのとは異なる MIME タイプにマップされている場合、そのファイルは検索対象になります。ただし、ファイルタイプと MIME タイプとの間に常に明確なマッピングがあるわけではありません。実際のファイルタイプのオプションが無効になっている場合、IWSVA では実際のファイルタイプが MIME タイプにマップされないため、設定されているコンテンツタイプヘッダに従って検索は省略されます。

ファイル拡張子に基づいてファイルを検索から除外できます。トレンドマイクロは、除外する MIME コンテンツタイプのリストを最小限に抑えることをお勧めします。一般的に、ファイルを検索するかどうかの判断を検索エンジンに任せた方が、検索を省略するファイルタイプを自分で選択するより安全です。1 つ目の理由として、HTTP ヘッダのコンテンツタイプが、ダウンロードするコンテンツの実際のタイプを正確に表していない場合があります。2 つ目の理由として、テキストファイルのように除外しても安全と思われるタイプが実際には安全でない場合があります。スクリプトはテキストファイルであり、不正なコードが含まれている可能性があります。その他に MIME コンテンツの除外を使用できるのは、セキュリティとパフォーマンスのトレードオフを意識的に行っている場合です。たとえば、Web トラフィックの多くはテキストであり、IWSVA 検索エンジンは、コンテンツにスクリプト、つまり潜在的に不正なコードが含まれている可能性があるため、すべてのトラフィックを検索します。ただし、Web スクリプトに悪用される可能性がない環境を閲覧していると確信できる場合、MIME コンテンツの除外リストに text/* を追加して、IWSVA が Web ページを検索しないように選択できます。

サイズの小さいファイル内にある不正プログラムは、ネットワーク全体に瞬時に広がる可能性があります。これに対し、サイズの大きいファイルに含まれる不正プログラムは転送に時間がかかるため、それほど速く広がりません。したがって、サイズの小さいファイルを効率的かつ完全に選別することが重要です。

X-Forwarded-For HTTP ヘッダ

X-Forwarded-For (XFF) HTTP ヘッダは、クライアントが HTTP プロキシまたはロードバランサ経由で Web サーバに接続する際に、クライアントの元の IP アドレスを識別するための事実上の業界標準となっています。X-Forwarded-For ヘッダは大部分のプロキシサーバでサポートされており、IWSVA では IPv6 X-Forward-For ヘッダがサポートされています。IPv4 アドレスの動作と同様に、ヘッダを構文解析してクライアントの IPv6 アドレスにアクセスできます。

IWSVA ではまた、IPv4 と同様に IPv6 アクセスのために 3 つの処理を実行します。これには、「X-Forwarded-For ヘッダの維持」および「X-Forwarded-For ヘッダの削除」機能が含まれます。

- IWSVA は XFF ヘッダを含む HTTP 要求を受け取ると、XFF ヘッダを構文解析して、クライアントの元の IP アドレスを取得し、その IP アドレスを使用してポリシーマッチングを実行します。
- IWSVA は HTTP 要求の転送時に、XFF HTTP ヘッダで管理者により設定された処理を実行します。表 8-5 を参照してください。

注意： IWSVA では、HTTPS トラフィックに対する XFF ヘッダの構文解析をサポートしません。

表 8-5. XFF HTTP ヘッダに利用可能な処理

処理	説明
X-Forwarded-For ヘッダの維持	IWSVA は XFF HTTP ヘッダを変更しません。
IWSVA が要求を受信する IP アドレスの追加	IWSVA は XFF HTTP ヘッダに最後のホップの IP アドレスを追加します。XFF HTTP ヘッダが存在しない場合、IWSVA は新規に作成します。
X-Forwarded-For ヘッダの削除	(初期設定) IWSVA は HTTP 要求から XFF HTTP ヘッダを削除することで、クライアントの個人情報がアップストリームへ漏えいしないようにします。

表 8-6 を参照して、配信シナリオが XFF HTTP ヘッダを使用して機能することを確認します。

表 8-6. X-Forwarded For HTTP ヘッダを使用した配信シナリオ

配信モード	XFF の構文解析	処理 : 維持	処理 : IP アドレスの追加	処理 : 削除	注意
プロキシ転送モード	使用可	使用可	使用可	使用可	
透過ブリッジモード	使用可	使用可	該当なし	使用可	このモードは透過的であるため、ヘッダに IP アドレスを追加する必要はありません。
WCCP モード	使用可	使用可	使用可	使用可	
通常の透過モード	使用可	使用可	使用可	使用可	
ICAP モード	該当なし	該当なし	該当なし	該当なし	IWSVA は ICAP サーバとしての役割を果たします。クライアントおよびサーバとの通信は行いません。IP アドレスは、X-Client-IP ヘッダを持つ ICAP クライアントにより提供されます。
リバースプロキシモード	該当なし	該当なし	該当なし	該当なし	XFF HTTP ヘッダはこのモードではサポートされません。

X-Forwarded-For HTTP ヘッダの設定

IWSVA では、主に次の 2 つの設定シナリオがあります。

- XFF HTTP ヘッダの構文解析を有効または無効にする
- XFF HTTP ヘッダで実行される処理を設定する

XFF HTTP ヘッダモジュールを設定するには

1. [HTTP] → [設定] → [X-Forwarded-For ヘッダ] に移動します。
2. XFF HTTP ヘッダの構文解析を有効または無効にします。
   - 有効にするには、ドロップダウンリストから [有効にする] を選択します。
   - 無効にするには、ドロップダウンリストから [無効にする] を選択します。
3. 処理を [X-Forwarded-For ヘッダの維持] (初期設定)、[IWSVA が要求を受信する IP アドレスの追加]、または [X-Forwarded-For ヘッダの削除] に設定します。表 8-5 を参照してください。
4. [保存] をクリックします。

ボットおよび C&C コンタクト検出ルールの指定

ネットワーク環境内で起こり得るボットの動作を監視および分析するために、ボット検出ルールに一致したときの処理を指定できます。[HTTP] → [高度な脅威保護] → [ポリシー] | [ポリシー] | [ボット検出ルール] タブに移動します。ボット /C&C 検出ルールの使用を有効または無効にするには、[このポリシーでボット /C&C 検出ルールを使用する] チェックボックスをオンまたはオフにします。ボット検出の処理も選択できます。

除外リストの指定

[HTTP] → [高度な脅威保護] → [ポリシー] | [< ポリシー名 >] | [除外設定] タブを参照してください。

除外リストに対してウイルス / スパイウェア検索および圧縮ファイルの処理を省略するように IWSVA を設定できます。そのため、この除外 Web サイトがハッキングされ、不正プログラムコードが埋め込まれることによって、セキュリティホールの原因になる可能性があります。IWSVA の場合は、初期設定でウイルス / スパイウェア検索機能が有効になっているため、この問題が回避されます。したがって、セキュリティポリシーで Web サイトが除外リストに含まれていることが判別されている場合でも、必ず Web ページの検索が実行されます。

除外リストは、[除外設定] 画面で適用できます。HTTP および FTP 検索ポリシーの場合、ファイル名除外リストも適用できます。[除外リスト] 画面で新しい除外リストを作成することができます (詳細については、237 ページの「除外リストの作成」を参照してください)。

次に、[除外設定] 画面のオプションについて説明します。

- **承認する URL リスト** — URL フィルタポリシー、HTTPS 復号化ポリシー、HTTP 検査ポリシー、情報漏えい対策ポリシー、または HTTP 検索ポリシーの WRS ルールおよびファイルタイプのブロックから除外することを承認された URL リストの名前を選択します。

- **除外ファイル名リスト** — ファイルタイプのブロックから除外するファイル名のリストを選択します。ファイル名除外リストは、HTTP 検索ポリシー、情報漏えい対策ポリシー、または FTP 検索ポリシーに適用できます。このオプションは、HTTPS 復号化ポリシー、HTTP 検査ポリシー、および URL フィルタポリシーには使用できません。
- **選択した除外リストの内容を検索しない** — 除外リスト内のファイルの内容をウイルス検索しない場合は、このオプションを選択します。このオプションが選択されている場合は、圧縮ファイルを処理できません。

図 8-13. ポリシー除外の設定

除外リストの作成

[除外リスト] 画面で新しい URL およびファイル名除外リストを作成できます。

URL 除外リストを設定するには

1. 管理コンソールから [HTTP] → [設定] → [除外リスト] の順に選択し、[URL リスト] タブをクリックします。
2. [追加] をクリックして、名前または一致対象のタイプを指定するか、URL 除外リストをインポートします。
   - **リスト名** — 除外リストの簡単でわかりやすい名前を入力します。

- **一致** — フィールドに、Web サイト、キーワードまたはフレーズ、あるいは文字列を入力します。このフィールドには、ワイルドカードとして「?」および「*」を使用できます。このフィールドに入力された内容は除外リストに 1 つずつ追加されます。

3. [一致] への入力内容に対応するオプションを選択します。
   - **前方一致** — 検索対象を文字列全体に制限します。この除外ルールを 1 つ以上のワイルドカードとともに使用すると、Web サイト全体へのアクセスを許可する場合に特に便利です。URL に「http://」や「https://」を入力する必要はありません（自動的に削除されます)。IWSVA では、Web ページの国際化ドメイン名を使用できます。Web サイトのドメイン名の前には「@」文字が追加されます。
   - **部分一致** — URL 内の任意の文字または数値から成る文字列を検索します。文字列が存在する場所に関係なく一致対象となります。たとえば「http://www.playboy.com/partner.htm」は、文字列「partner」の一致対象と見なされ、この URL は除外対象となります。このフィールドにワイルドカードを使用すると、誤検出や予期しない結果になる可能性が非常に高くなります。
   - **完全一致** — 検索対象を文字列全体に制限します。たとえば、特定のサイト、ページ、ファイル、その他の特定のアイテムを検索対象にします。

注意： — HTTPS 復号化ポリシーでは、照合する文字列は、IWSVA をプロキシモードまたは透過モードのどちらに設定しているかによって異なります。

— プロキシモードの場合、IWSVA は完全な URL ではなくドメイン名を照合します。したがって、ドメイン名のみを指定する必要があります。

— 透過モード (WCCP またはブリッジモード) の場合、受信したサーバ証明書の `CommonName` が一致対象となります。

— HTTPS 標準ポートの場合、`CommonName` が一致対象となります。

— HTTPS 標準以外のポートの場合、`CommonName:Port` が一致対象となります。

- **除外リストのインポート** — ウイルス検索や (URL フィルタモジュールで実行する) フィルタから除外する URL の既存のリストをインポートできます。たとえば、トレンドマイクロの WebManager から取得した URL のリストや、テキストエディタを使用して編集した URL のリストがある場合、それらの URL を 1 つ 1 つ入力する代わりに、そのリストをインポートすることができます。インポートリストは、規定の基準に適合する必要があります。239 ページの「除外リストの形式」を参照してください。

4. [保存] をクリックします。

ファイル名除外リストを設定するには

1. 管理コンソールから [HTTP] → [設定] → [除外リスト] の順に選択し、[ファイル名リスト] タブをクリックします。
2. [追加] または [編集] をクリックして一致対象のタイプを指定するか、URL 除外リストをインポートします。
   - **リスト名** — 除外リストの簡単でわかりやすい名前を入力します。
   - **一致** — ファイル拡張子付きのファイル名またはファイル拡張子をフィールドに入力します。このフィールドには、ワイルドカードとして「*」を使用できます。このフィールドに入力された内容は除外リストに 1 つずつ追加されます。
   - **除外リストのインポート** — ウイルス検索から除外するファイル名の既存のリストをインポートできます。たとえば、トレンドマイクロの Web サイトから取得したファイル名のリストや、テキストエディタを使用して編集したファイル名のリストがある場合、それらの URL を 1 つ 1 つ入力する代わりに、そのリストをインポートすることができます。インポートリストは、規定の基準に適合する必要があります。239 ページの「除外リストの形式」を参照してください。
3. [保存] をクリックします。

除外リストの形式

IWSVA では、2 種類の除外リスト (URL およびファイル名) がサポートされています。次に、それぞれのリスト形式について説明します。

> [approved] 形式を使用した除外リストはインポートできます。[blocked] 形式を使用したブロックリストと [allowed] 形式を使用した許可リストはインポートできます。

除外 URL リストの形式

除外 URL リストには、次のヘッダを含む任意の ASCII テキストファイルを指定できます。

[approved]

除外リストに含める URL の数に制限はありません。Web アドレス、URL、文字列は改行で区切ります。除外リストには、ワイルドカードとして「?」および「*」を使用できます。

サンプルファイル :

```
[approved]
www.good-job-habits.com/*
www.business-productivity.com/*
```

ファイル名リストの形式

除外ファイル名リストには、次のヘッダを含む任意の ASCII テキストファイルを指定できます。

[approved]

除外リストに含めるファイル名の数に制限はありません。ファイル名および文字列は改行で区切ります。除外リストには、ワイルドカードとして「*」を使用できます。

サンプルファイル :

```
[approved]
abcfile.doc
*.sc
```

ウイルス検出時の処理設定

HTTP ウイルス検索ルールを設定した後、感染したファイル、パスワードで保護されたファイル、またはマクロを含むファイルが検出された場合に IWSVA で実行する処理を設定します。

検索処理

[HTTP] → [高度な脅威保護] → [ポリシー] | [< ポリシー名 >] | [処理] タブには、ウイルス検索の結果に対して IWSVA が実行できる次の 4 つの処理があります。

- 感染ファイルを削除するには、[削除] を選択します。要求元クライアントはファイルを受信しません。この処理は、感染ファイル (1 次処理)、2 次処理、およびパスワードで保護されたファイルの検索イベントに適用できます。
- ファイルをクリーンナップせずに隔離ディレクトリに移動するには、[隔離] を選択します。

  `/var/iwss/quarantine`

  要求元クライアントはファイルを受信しません。この検索処理は、すべての 4 つの検索イベントに適用できます。オプションで、隔離ディレクトリに送る前にファイルを暗号化するように選択できます。詳細については、231 ページの「隔離ファイルの処理」を参照してください。
- IWSVA では、感染したファイルを自動的に駆除および処理するには、[駆除] を選択します。要求元のクライアントは、ファイルが駆除可能であれば駆除されたファイルを受信します。駆除できない場合は、2 次処理が実行されます。この処理は、感染ファイル (1 次処理) とマクロ検索イベントに適用できます。マクロ検索イベントで [駆除] を選択することにより、新しい脅威に対応するパターンファイルが公開されるまでの間、緊急の措置として、ファイルに含まれるすべてのマクロを削除できます。

- [放置] を選択すると、ファイルをそのまま要求元のユーザに配信します。この処理は、2 次処理、パスワードで保護されたファイル、およびマクロイベントに適用できます。マクロイベントについては、ウイルス大規模感染時にマクロを含むファイルをすべて削除するかまたは隔離しないかぎり、常に放置処理を実行することをお勧めします。

注意： 2 次処理で、検索処理として [放置] を選択することはお勧めしません。

検索イベント

検索の後、検索結果に合わせて 4 種類の処理を設定できます。

- **感染ファイル (1 次処理)** — ウイルスまたはその他の不正プログラムに感染していると判定されたファイルです。利用可能な処理には、[削除]、[隔離]、または [駆除] (推奨の処理で初期設定) があります。
- **2 次処理** — ファイルを感染させるウイルスまたは不正プログラムのタイプによって、検索エンジンは一部のファイルを駆除できない場合があります。利用可能な処理には、[削除] (推奨の処理で初期設定)、[隔離]、および [放置] があります。
- **パスワードで保護されたファイル** — パスワードで保護されているか暗号化されているため、検索できないファイルです。これらのタイプのファイルの感染状況を判定することはできません。利用可能な処理には、[削除]、[隔離]、および [放置] (推奨の処理で初期設定) があります。
- **検索の制限条件外のファイル** — 不明な理由によりウイルス検索エンジンで検索できないため、検索不可能なファイルです。利用可能な処理には、[削除]、[隔離]、および [放置] (推奨の処理で初期設定) があります。
- **マクロ** — マクロプログラムのコードを含む Microsoft Office のファイルです。亜種や新種が容易に作成できるのが特徴です。新しいウイルスパターンがパターンファイルに追加されて使用している環境に配信されるまで、すべてのファイルをブロックするため、ウイルス大規模感染の早い段階で、マクロを含むすべてのファイルを隔離できます。利用可能な処理には、[隔離]、[駆除]、および [放置] があります。アップデート済みのパターンファイルがリリースされる前のウイルス大規模感染時にマクロを隔離したり削除する必要がないかぎり、マクロに対する処理は常に [放置] に設定することをお勧めします。

図 8-14.　HTTP ウイルス検索ポリシー処理の設定

備考欄への入力

IWSVA で検出されたファイルに対する処理を設定した後、ポリシーに関する説明を記録するには、画面下部の [備考] を使用します。[HTTP] → [高度な脅威保護] → [ポリシー] | [< ポリシー名 >] | [処理] タブを参照してください。

ポリシーに適用する検索処理の設定が完了したら、[保存] をクリックします。ポリシーをただちに適用するには、[ポリシーの配信] をクリックします。すぐに適用しない場合、データベースキャッシュの有効期限が切れた後に、このポリシーが適用されます。

第 9 章

アクセス割り当てと URL アクセス設定

アクセス割り当ては、クライアントの帯域幅の使用を一定時間ごとに制限します。「URL の信頼」では、信頼する URL を検索とその他の InterScan Web Security Virtual Appliance（以下、IWSVA) の操作対象から除外することにより、閲覧パフォーマンスを改善できます。URL ブロックは、指定した URL、またはフィッシングパターンファイルに含まれているパターンを持つ URL への要求を拒否します。

本章で説明する内容には、次の項目が含まれます。

アクセス割り当てポリシーについて

IWSVA には、他のクライアントに対する定義可能なポリシーがあります（グローバルポリシーにアクセス割り当てはありません)。ポリシーに一致する接続がない場合、クライアントには無制限アクセスが許可されます。アクセス割り当てポリシーを変更し、データベースにポリシーを保存した後、複数サーバ構成環境の IWSVA サービスは、[ポリシー配信設定] 画面（[管理] → [一般設定] → [ポリシー配信]) で設定されたキャッシュ生存期限（TTL) 値に従ってポリシーをリロードします。

ダウンロード中に割り当てが超過しても、ダウンロードの続行は許可されます。ただし、アクセス割り当て間隔の有効期限が切れる前に行われた次のダウンロード / 閲覧要求は拒否されます。アクセス割り当て間隔の有効期限が切れた後、ユーザにはアクセスが再度許可されます。

注意： グループに対する割り当てポリシーの場合、割り当て量は、グループ内のクライアントに個々に適用されます。また、同一のポリシー内のクライアントに対する割り当て量はすべて同じです。

アクセス割り当てポリシーの管理

アクセス割り当てポリシーの範囲に含めるクライアント、帯域幅の割り当て、および割り当て期間の間隔を設定できます。アクセス割り当てポリシーは、IPv4 クライアントの場合と同様に IPv6 クライアントにも適用できます。アカウントフィールドでは IPv6 アドレスがサポートされます。任意の IPv6 ホストに 1 つのルールを定義すると、クライアントが IWSVA を介してインターネットにアクセスしたときにこのポリシールールがトリガされます。

使用可能なポリシーの選択時には、IPv4 と IPv6 の両方のポリシーが表示されます。[アカウント] フィールドで入力可能なアカウントエントリは、IPv4 でサポートされているものと同様に、単一の IPv6 アドレス、IPv6 アドレス範囲、または IPv6 ネットワークマスクです。

アクセス割り当てポリシーを追加するには

1. 管理コンソールから [HTTP] → [アクセス割り当てポリシー] の順に選択します。
2. [アクセス割り当てを有効にする] チェックボックスをオンにします。
3. ドロップダウンメニューから、[1 日]、[1 週間]、または [1 か月] のいずれかのアクセス割り当て間隔を選択します。

   アクセス割り当て間隔の値は、すべての既存のポリシーを含め、すべてのアクセス割り当てポリシーにグローバルに適用されます。
4. [保存] をクリックします。

5. [追加] をクリックします。
6. [ポリシーを有効にする] チェックボックスをオンにして、アクセス割り当てを入力します。
7. ポリシーを適用するユーザを選択します。

   この画面のオプションは、使用しているユーザの識別方法に応じて異なります。[IP アドレス]、[ホスト名（変更された HTTP ヘッダ)]、または [ユーザ / グループ名認証] のいずれかになります。これらの設定値は、[管理] → [一般設定] → [ユーザの識別] | [ユーザの識別] タブで設定されます。ユーザの識別方法の設定とポリシー適用範囲の設定の詳細については、160 ページの「ユーザ識別方法の設定」を参照してください。
   設定したユーザの識別方法に関係なく、ポリシーを適用するクライアントの IP アドレスを入力できます。
8. ポリシーに関する特別な情報がある場合は、必要に応じて備考を入力します。
9. [保存] をクリックします。
10. [アクセス割り当てポリシー] 画面に戻ったら、[ポリシーの配信] をクリックして、ただちにポリシーを適用します。すぐに適用しない場合、ポリシーはデータベースキャッシュの有効期限が切れた後に適用されます。

データベースから設定を削除せずに、一時的にポリシー設定を解除したい場合は、ポリシーを無効にすることができます。

ポリシーを無効にするには

1. 管理コンソールから [HTTP] → [アクセス割り当てポリシー] の順に選択します。
2. [アクセス割り当てポリシー] 画面から、[アカウント] 列または [アクセス割り当て] 列のいずれかにあるリンク項目をクリックして、[ポリシーの編集] 画面を表示します。
3. 画面の上部にある [ポリシーを有効にする] チェックボックスをオフにして、[保存] をクリックします。

   ポリシーを無効にしても、ポリシーキャッシュが更新されるか、または [ポリシーの配信] をクリックするまでポリシーは無効になりません。

クライアントを使用している従業員が組織を退職した場合など、ポリシーがまったく必要なくなった場合、ポリシー全体を削除するか、または IWSVA データベースからポリシーの範囲内のユーザを削除できます。

ポリシーを削除するには

1. 管理コンソールから [HTTP] → [アクセス割り当てポリシー] の順に選択します。
2. [アクセス割り当てポリシー] 画面からポリシーを選択して、[削除] をクリックします。

   ポリシーを削除しても、ポリシーキャッシュが更新されるか [ポリシーの配信] をクリックするまでポリシーは削除されません。

URL アクセス管理の概要

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、または両方の組み合わせに基づいて、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では、URL が属するカテゴリに基づき、Web アクセスが許可されたり、拒否されたりします。Web レピュテーションは、要求された URL が、ハッキングの可能性のあるフィッシング脅威かファーミング脅威か、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。URL フィルタモジュールも Web レピュテーションも、ポリシー内でユーザが設定することにより管理されます。[HTTP] → [URL アクセス設定] を参照してください。

ユーザが Web サイトにアクセスしようとすると、次のイベントが発生します。

- IWSVA が URL ブロックリストと信頼する URL リストに対して要求された URL を確認します (246 ページの「URL アクセス管理の概要」を参照)。

  URL が URL ブロックリストで見つかった場合、要求が拒否されます。URL が信頼する URL リストで見つかった場合、アクセスが許可され、アクセス制御は実行されません。
- URL がブロックリストでも信頼するリストでも見つからなかった場合、IWSVA が要求された URL を Web レピュテーションに送信して処理します。
- Web レピュテーションは、リモートデータベースから URL についての適切な URL 評価を取得します。

  この評価は、「高」、「中」、「低」のいずれかです。指定されたセキュリティレベルによって、IWSVA がその URL をブロックするかどうかが決定します (212 ページの「Web レピュテーションルールの指定」を参照)。
  URL が除外リストにある場合、IWSVA では、その URL に対するフィッシングおよびファーミング検出を省略します (236 ページの「除外リストの指定」を参照)。
- その後で、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を判断し、脅威が判明した場合、その URL にフラグを付けます (213 ページの「フィッシング対策、ファーミング対策、および C&C コールバック試行検出」を参照)。
- Web レピュテーションの最後のプロセスは、URL のカテゴリを決定することです (499 ページの「URL フィルタカテゴリのグループ」を参照)。

  カテゴリ情報は、後で、URL フィルタモジュールで使用されます。
- Web レピュテーションが、URL の評価、フィッシングフラグまたはファーミングフラグ、および URL カテゴリを IWSVA に返します。
- URL にフィッシングまたはファーミングのフラグが付いていた場合、IWSVA は Web サイトへのアクセスをブロックします。

- 次に、URL フィルタモジュールを使用している場合、このモジュールが、要求された URL についての Web カテゴリ情報を使用して、アクセスを許可するかどうかを判断します。

  URL が除外リストにある場合、カテゴリフィルタが無視され、URL アクセス管理の最終段階に進みます。
  要求された URL のカテゴリが URL フィルタポリシーで許可されている場合、URL の処理は最終段階に送られます。許可されていない場合、URL はブロックされます。
- 最後に、Web レピュテーションの URL 評価に基づいて、IWSVA では、要求された URL が検索ポリシーで指定されたセキュリティレベルより上か下かを判断します。

  URL が除外リストにある場合、IWSVA はその URL のセキュリティレベルチェックを省略します (236 ページの「除外リストの指定」を参照)。
  評価がセキュリティレベルを下回っていた場合、要求された URL はブロックされます。ただし、評価がセキュリティレベルを上回っていた場合、IWSVA ではその URL へのアクセスを許可します。

URL アクセス管理の設定

IWSVA では、低リスクサイトの閲覧パフォーマンスを改善するために、一部の信頼する URL を検索およびフィルタから除外できます。ユーザ設定のリストを使用することで、または、「フィッシング」スキームや悪質な行為に関連付けられているサイトを集めたフィッシングパターンファイルに要求されたサイトが含まれていないかを確認することで、サイトへのアクセスをブロックすることもできます。

信頼する URL の設定

IWSVA では、一部の URL を信頼してそれらを検索とフィルタから除外するように設定できます。この設定をすると、未確認のコンテンツがネットワークに入り、セキュリティリスクにさらされることになるので、「信頼する」URL は慎重に考慮する必要があります。信頼する URL は検索されないので、閲覧パフォーマンスが改善します。信頼する URL にふさわしいのは、頻繁にアクセスされる Web サイトで、自分の会社のイントラネットサイトのように、管理できるコンテンツが含まれているものです。

信頼する URL の情報は `/etc/iscan/TrustedURLs.ini` ファイルにあります。
`TrustedURL.ini` ファイルのパスは、`/etc/iscan/intscan.ini` 設定ファイルの `[URL-trusting]` セクションにある `normalLists` パラメータを使用して設定されます。

信頼する URL を設定する際、次のものを使用してサイトを指定できます。

- サブサイトを含む Web サイト
- 要求された URL 内の完全一致文字列

それ以外の場合には信頼する URL のリストの条件に一致するサイトが、通常どおり IWSVA で検索またはフィルタされるように、これらのサイトに除外設定を適用できます。

ユーザインタフェースを通じて信頼する URL のリストと除外を設定できるだけでなく、ファイルからこれらをインポートすることもできます。Web サイトや文字列のリストを含むファイルの一番上にコメントまたはタイトルを記述し、1 行ごとにルールを 1 つ記述します。コメントまたはタイトルは IWSVA では無視されます。次の例で示すように、[allow] の下に信頼するグループサイトを、[block] の下に信頼する URL リストから除外するグループサイトを記述します。

```
Trusted URLs Import File { このタイトルは無視されます }

[allow]
unwanted.com*
www.blockedsite.com*
urlkeyword
banned.com/file
banned.com/downloads/

[block]
www.blockedsite.com/file
www.unwanted.com/subsite/
```

注意： HTTPS 復号化ポリシーが適用されていない場合、一致対象の文字列は、IWSVA の設定がプロキシモードか透過モードかによって異なります。
— プロキシモードの場合、完全な URL ではなく、ドメイン名が一致対象となります。したがって、ドメイン名のみを指定する必要があります。
— 透過モード (WCCP またはブリッジモード) の場合、受信したサーバ証明書の CommonNames が一致対象となります。

信頼する URL と除外設定を管理するには

1. 管理コンソールから [HTTP] → [URL アクセス設定] → [グローバル URL の信頼] の順に選択します。
2. [URL の信頼] 画面で、[URL の信頼を有効にする] チェックボックスをオンにして、URL の信頼を有効にします。

警告： [URL の信頼を有効にする] オプションを選択すると、信頼する URL の内容に対してフィルタおよびウイルスの検索は行われなくなります。

3. 信頼する URL を指定する方法を選択します。
   - 前方一致 (すべてのサブサイトを含む)
   - 完全一致 (URL に文字列が含まれること)
4. [一致] に URL 文字列を入力して [信頼する] をクリックし、[信頼リスト] の下に表示されている信頼する URL リストに追加します。信頼する URL を除外するには、[信頼しない] をクリックして除外リストに追加します。
5. 信頼リストまたは除外リストから URL を削除するには、削除する項目を選択して [削除] をクリックします。[すべて削除] をクリックすると、すべて削除されます。
6. [保存] をクリックします。

信頼する URL リストとその除外設定をインポートするには

1. [HTTP] → [URL アクセス設定] → [グローバル URL の信頼] の順にクリックします。
2. 信頼する URL のリストとその除外設定を含むファイルの名前を参照するか、[信頼リスト / 除外リストのインポート] に入力します。
3. [インポート] をクリックします。インタフェース上の該当するフィールドに、ファイルからインポートされる信頼する URL とその除外設定が表示されます。
4. [保存] をクリックします。

URL のブロック

IWSVA は、グローバルブロック URL リストにある Web サイトと URL 文字列をブロックできます。

注意： ICAP プロキシハンドラをインストールしている場合、この機能を作動させるためには、事前キャッシュ (precache) 要求モードでファイルを検索するように ICAP クライアントを設定してください。

HTTPS Web サイトは FQDN を入力することでブロックできます。

URL のブロックを設定する際、次のキーワードを使用してサイトを指定できます。

- サブサイトを含む Web サイト
- 部分一致のキーワード
- 要求された URL 内の完全一致文字列

IWSVA で通常どおり要求が受け入れられるように、ブロックされた URL のリストに除外設定を適用できます。この機能を使用すると、任意のサイトをブロックしながら、そのサイトのサブサイトまたはファイルへのアクセスを許可できます。除外リストを含む URL ブロックリストは、`/etc/iscan/URLB.ini` ファイルに保持されます。`URLB.ini` ファイルのパスは、`/etc/iscan/intscan.ini` ファイルの [URL-blocking] セクションにある「normalLists」パラメータを使用して設定されます。

Web コンソールから URL を追加する以外に、テキストファイルから URL ブロックリストをインポートできます。

ローカルリストの使用

使用している環境用に保持しているブロックされたサイトと除外設定のリストに基づいて、URL へのアクセスをブロックするように IWSVA を設定できます。

URL を [ブロックリスト] および [除外リスト] に追加する場合、まず一方のリストにすべて追加して設定を保存してから、他方のリストへの追加操作を実行する方法をお勧めします。この方法により、同一の URL が両方のリストに存在するようにできます。URL を [ブロックリスト] に追加するか、または [除外リスト] に追加しようとするとき、その URL がすでに他のリストに存在している場合、IWSVA では追加操作を実行せず、他のリストに存在している旨の警告メッセージが表示されます。

ブロックする URL を設定するには

1. [HTTP] → [URL アクセス設定] → [グローバル URL ブロック] の順にクリックします。
2. [URL ブロックを有効にする] チェックボックスをオンにします。
3. [URL ブロック] 画面で、[キーワード] に Web アドレス全体、URL キーワード、完全一致文字列のいずれかを入力します。

   任意の Web サイトでフォルダまたはディレクトリを識別するには、最後の文字の後にスラッシュ (/) を使用します。たとえば、www.blockedsite.com をブロックしても、その charity ディレクトリへのアクセスを許可する場合は、次の手順に従ってください。

   a. [キーワード] に「www.blockedsite.com」と入力し、[ブロックする] をクリックします。
   b. [キーワード] に「www.blockedsite.com/charity/」と入力し、[ブロックしない] をクリックします。スラッシュなしで charity と記述すると、IWSVA は www.blockedsite.com/charity をファイルと見なします。

注意： HTTPS 復号化ポリシーが適用されていない場合、一致対象の文字列は、IWSVA の設定がプロキシモードか透過モードかによって異なります。
— プロキシモードの場合、完全な URL ではなく、ドメイン名が一致対象となります。したがって、ドメイン名のみを指定する必要があります。
— 透過モード (WCCP またはブリッジモード) の場合、CommonNames と URL の両方が一致対象となります。HTTPS サイトをブロックする場合、ブロックリストにこれらを含める必要があります。

---

4. リストからエントリを削除するには、削除する項目を選択して [削除] をクリックします。または、[すべて削除] をクリックしてすべてのエントリを削除します。
5. [保存] をクリックします。

ブロックする URL リストのインポート

IWSVA は、ブロックする URL のリストをファイルからインポートできます。Web サイト、URL キーワードまたは文字列のリストを含むファイルの 1 行目にわかりやすいタイトルまたはコメントを入力し、1 行ごとにルールを 1 つ記述します。例で示すように、[block] の下にブロックするグループサイトを、[allow] の下に除外するグループを記述します。たとえば、次のように記述します。

```
URL Blocking Import File { このタイトルは無視されます }

[block]
www.blockedsite.com*
unwanted.com*
```

```
urlkeyword
banned.com/file
banned.com/downloads/

[allow]
www.blockedsite.com/file
www.unwanted.com/subsite/
www.trendmicro.com*
```

IWSVA でワイルドカードと見なされないように、URL ブロックの文字列に「*」と「?」文字を含めるには、変数 %2a または %2A を使用して「*」を表示し、変数 %3f または %3F を使用して「?」を表示します。たとえば、www.example.com/*wildcard を文字どおり一致させるには、www.example.com/*wildcard ではなく、www.example.com/%2awildcard と指定します。

ファイルのインポートが成功しない場合、カスタマーセンターに連絡する前に、URL ブロックインポートファイル用に指定された形式に従っていることを確認します。次のことを確認します。

- [block] の下にブロックするエントリ、[allow] の下に除外するエントリを記述していること
- 本書またはオンラインヘルプで説明するとおりに、ワイルドカードを含むエントリの形式を設定していること

ブロックする URL のリストをインポートするには

1. 前述のように、ブロックする URL とすべての除外設定を含むテキストファイルの形式を設定します。
2. 管理コンソールから [HTTP] → [URL アクセス設定] → [グローバル URL ブロック] の順に選択します。
3. [参照] をクリックして、インポートするファイルの場所を [ブロックリスト / 除外リストのインポート] に指定し、[インポート] をクリックします。
4. [保存] をクリックします。

第 10 章

URL フィルタ

本章では、URL フィルタポリシーの作成と設定の手順を示しながら、InterScan Web Security Virtual Appliance（以下、IWSVA）の URL フィルタモジュールの概要および設定作業の流れについて説明します。

URL フィルタは、Web レピュテーションとともに IWSVA に搭載された、多層的かつ複合型の脅威に対する保護ソリューションです（246 ページの「URL アクセス管理の概要」を参照）。

本章で説明する内容には、次の項目が含まれます。

URL フィルタについて

IWSVA の URL フィルタモジュールの初期設定では、組織の主な関心が、有害なデータの表示に関連して発生する法的責任を回避し、従業員の業務に無関係な Web サイトの不正利用を防ぐことにあると想定しています。ただし例外が必要な場合もあるため、より広範なアクセスを必要とする業務に携わる従業員には、制限されたカテゴリグループへのアクセスが許可されるように追加のポリシーを作成できます。たとえば、組織で許容できるインターネット利用ポリシーの違反について調査するために、人事部門または IT 部門の従業員が無制限のインターネットアクセスを必要とする場合があります。

IWSVA では、検索エンジンのフィルタプロバイダ (Google や Yahoo など) によって提供される安全な検索機能がサポートされます。安全な検索は、検索結果からアダルトサイトやアダルトコンテンツをフィルタする際に使用され、子供にアダルトコンテンツを見せないようにします。

さらに IWSVA では、動的なフィルタを高度な Web レピュテーションデータベースと組み合わせることにより、フィルタ機能が向上しています。オンライン取り引き、ショッピング、オークション入札、出会い系、ギャンブル、およびその他の仕事に関係しない活動の Web サイトを業務時間中に閲覧することで従業員の生産性は低下し、正当な閲覧のために利用可能な帯域幅が減少します。IWSVA を使用すると、ユーザおよび作業チーム固有のニーズに応じてインターネットアクセスをカスタマイズできるため、インターネットの利用が最適化されます。

[HTTP] → [URL フィルタ] → [ポリシー] | [< ポリシー名 >] | [ルール] タブを参照してください。

IWSVA の URL フィルタポリシーには、インターネットアクセスを管理するための柔軟できめの細かいメカニズムが用意されています。各ポリシーには、次のような 3 つの基本的な要素があります。

- IWSVA では、「ギャンブル」、「ゲーム」、「出会い系」など 82 を超えるカテゴリに属する URL を格納する Web レピュテーションデータベースにアクセスできます。カテゴリは次の論理グループに含まれます。
  - カスタムカテゴリ
  - ネットワーク帯域幅
  - インターネットセキュリティ
  - コミュニケーション / メディア
  - アダルト
  - ビジネス
  - ライフスタイル
  - 一般

- 各カテゴリの Web サイトへのアクセスは、予約期間オブジェクトとして指定された期間中、許可、ブロック、または監視できます。
- 使用する環境で、ユーザごとに異なるポリシーを設定できます。

対象カテゴリにあるすべての識別された URL へのアクセスは、ポリシーに従って管理されます。各 URL は、データベースで 1 つ以上のカテゴリに関連付けられています。Web サイトを正確に定義するために、URL は複数の URL カテゴリに属することができます。たとえば、不正プログラムが存在するショッピングサイトは、「ショッピング」カテゴリと「不正プログラム流布」カテゴリに属することができます。URL を分類する URL カテゴリの数に応じて、URL フィルタポリシーによるアクセスの管理方法を変えることができます。組織でアクセスする必要のある URL が禁止されたカテゴリに関連付けられている場合、URL フィルタルールの除外設定を作成して、データベースの分類を変更できます。許可する URL リストで指定された文字列は、対象の URL と比較されるのであって、対象の URL が参照するドキュメントのコンテンツとは比較されません。IWSVA では、Web サイト、URL キーワード、および完全一致文字列により、URL フィルタの許可リストを設定するオプションが用意されています。

IWSVA の初期設定の URL 分類を省略するもう 1 つの方法は、カスタムカテゴリを作成して、ユーザのアクセスを許可するために必要なアクセス権限を割り当てることです。

URL フィルタ処理

次に、予約期間オブジェクトを使用して特定のポリシーに対して適用できるフィルタ処理を示します。

- **許可** — 対象サーバへの接続が許可され、ユーザはその Web サイトにアクセスできます。
- **ブロック** — 対象サーバへの接続が確立されず、ユーザはその Web サイトにアクセスできません。このイベントについてはログエントリも作成されます。
- **次のポリシーに一致** — 対象サーバへの接続は、次のレベルで設定されたポリシーに応じて異なります。
- **オーバーライド付きブロック** — ユーザがカテゴリブロックを無効にするための特定のパスワードを入力可能でないかぎり、対象のサービスへの接続は確立されません。

注意： 「オーバーライド付きブロック」処理をカテゴリに適用する場合、管理者は、ポリシー作成時にオーバーライド用に使用するパスワードを設定する必要があります。

- **監視** — 対象サーバへの接続が許可され、ユーザはその Web サイトにアクセスできます。このイベントについてはログエントリも作成されます。

- **時間制限** — 管理者によって設定された期間に、選択したカテゴリの URL へアクセスする対象サーバへの接続が許可されます。

注意： 1. カテゴリに対して「時間制限」処理を選択するには、管理者がカテゴリリストの下の [時間制限の設定] セクションで [時間割り当て] テキストボックスに値を入力する必要があります。

2. 初期設定の割り当て単位は、5 分です。[時間割り当て] の値は 5 の倍数にすることをお勧めします。それ以外の場合、IWSVA では 5 未満の端数は無視されます。たとえば、値を 4 分に設定すると、IWSVA はそれを 0 分と解釈します。値を 9 分に設定すると、5 分として解釈されます。

- **警告** — 対象サーバへの接続は許可されますが、会社のポリシーに違反するカテゴリに属する URL にアクセスしようとすると警告する通知が表示されます。ユーザは、ページへのアクセスを続行するか、前のページに戻るか選択できます。

URL フィルタの設定作業の流れ

URL フィルタを設定するには、対象の URL とユーザの ID (IP アドレス、IP アドレスの範囲、ユーザ名、グループ名、またはホスト名) を入力します。ユーザは、IWSVA で使用するように設定されているユーザの識別方法に従って特定されます (詳細については、160 ページの「ユーザ識別方法の設定」を参照)。

ユーザが要求した URL は、7 つの事前定義されたグループにまとめられている、82 を超えるカテゴリのうち 1 つ以上のカテゴリに分類できます。要求された URL は、IWSVA の URL フィルタエンジンに渡され、要求元のユーザに対するポリシーに従ってフィルタされます。要求された URL の分類先のカテゴリとポリシーの処理に基づいて、その URL は許可、ブロック、監視されるか、または警告が発行されます。

注意： URL フィルタエンジンに対する手動アップデートは、[手動アップデート] 画面で実行できます。

URL フィルタポリシーの管理

IWSVA は、初期設定されている次の 2 つの URL フィルタポリシーで事前設定されています。ネットワーク上のすべてのクライアントに適用されるグローバルポリシーと、ゲストアカウントで IWSVA にアクセスするクライアントに適用されるゲストポリシーです。

注意： ゲストポリシーは、IWSVA が次のように設定されている場合にのみサポートされます。
- ゲストアクセスを許可 (認証方法にキャプティブポータルを使用)
- 配置ウィザードでプロキシ転送モードを選択した後にゲストユーザログインポートを有効化

URL フィルタの有効化

URL フィルタモジュールが有効になっていることを確認してから、作業を開始してください。アカウントフィールドでは IPv6 アドレスがサポートされます。任意の IPv6 ホストに 1 つのルールを定義すると、クライアントが IWSVA を介して Web サイトにアクセスしたときにこのポリシールールがトリガされます。

ポリシーの選択時には、IPv4 と IPv6 の両方のポリシーが表示されます。[アカウント] フィールドで入力可能なアカウントエントリは、IPv4 でサポートされているものと同様に、単一の IPv6 アドレス、IPv6 アドレス範囲、または IPv6 マスクです。

IWSVA は、IPv6 で「URL 警告モード」機能をサポートしており、クライアントの IP アドレスのバージョンに基づいて、IWSVA の IPv6 または IPv4 アドレスへの警告メッセージが自動的にクライアントにリダイレクトされます。

- クライアントが IPv4 アドレスを使用する場合、IWSVA は、リダイレクト要求を IWSVA の IPv4 アドレスとともに送信します。
- クライアントが IPv6 アドレスを使用する場合、IWSVA は、リダイレクト要求を IWSVA の IPv6 アドレスとともに送信します。

URL フィルタを有効にするには

1. 管理コンソールから [HTTP] → [URL フィルタ] → [ポリシー] の順に選択します。
2. [URL フィルタを有効にする] チェックボックスをオンにします。
3. [保存] をクリックします。

動的な URL カテゴリ分類の有効化

IWSVA では、トレンドマイクロの URL フィルタエンジン (TMUFE) を使用して URL をフィルタします。アクセスされた URL が TMUFE データベースに存在しない場合、IWSVA は動的な URL カテゴリ分類テクノロジを使用して、Web サイトのコンテンツと HTTP URL に基づいて Web サイトのリアルタイムのカテゴリ分類を実行します。

動的な URL カテゴリ分類では、キーワード、ルール、および Web サイトを除外するその他の情報を含むパターンファイルを使用します。

動的な URL カテゴリ分類を有効にするには

1. メインメニューから [HTTP] → [URL フィルタ] → [ポリシー] の順にクリックします。
2. [動的な URL カテゴリ分類を有効にする] を選択します。
3. [保存] をクリックします。

新しいポリシーの作成

新しい URL フィルタポリシーを作成するには、次の 4 つの手順に従います。

- ポリシーを適用するアカウントを選択します。
- 予約期間オブジェクトで定義された期間に、許可、ブロック、監視、または警告する Web サイトのカテゴリを指定します。
- 安全な検索の設定を選択します。
- 除外リストを選択します。

新しいポリシーを作成するには

1. IWSVA Web コンソールを開き、管理コンソールから [HTTP] → [URL フィルタ] → [ポリシー] の順に選択します。
2. [追加] をクリックします。

   [URL フィルタポリシー : ポリシーの追加] 画面が表示されます。
3. わかりやすい [ポリシー名] を入力します。

   「研究者向け URL フィルタポリシー」のように、適用対象となるユーザまたはグループへの参照が含まれるポリシー名は簡単に覚えられます。
4. ポリシーを適用するユーザを選択します。

   この画面のオプションは、使用しているユーザの識別方法に応じて異なります。[IP アドレス]、[ホスト名 (変更された HTTP ヘッダ)]、または [ユーザ / グループ名認証] のいずれかになりま

す。ユーザの識別方法の設定とポリシー適用範囲の設定の詳細については、160 ページの「ユーザ識別方法の設定」を参照してください。

5. [次へ] をクリックします。
6. [ルールの指定] 画面で、[ポリシーを有効にする] チェックボックスがオンになっていることを確認します。
7. 各 URL カテゴリまたはサブカテゴリに対して、次のフィルタ処理のいずれかを選択します。
   - **許可** — 対象サーバへの接続が許可され、ユーザはその Web サイトにアクセスできます。
   - **ブロック** — 対象サーバへの接続が確立されず、ユーザはその Web サイトにアクセスできません。このイベントについてはログエントリも作成されます。
   - **次のポリシーに一致** — 対象サーバへの接続は、次のレベルで設定されたポリシーに応じて異なります。
   - **オーバーライド付きブロック** — ユーザがカテゴリブロックを無効にするための特定のパスワードを入力可能でないかぎり、対象のサービスへの接続は確立されません。
   - **監視** — 対象サーバへの接続が許可され、ユーザはその Web サイトにアクセスできます。
   - **時間制限** — 管理者によって設定された期間に、選択したカテゴリの URL へアクセスする対象サーバへの接続が許可されます。
   - **警告** — 対象サーバへの接続は許可されますが、会社のポリシーに違反するカテゴリに属する URL にアクセスしようとすると警告する通知が表示されます。ユーザは、ページへのアクセスを続行するか、前のページに戻るか選択できます。
8. 予約期間オブジェクトで定義された期間中フィルタ処理を適用するよう選択します。
   - **処理とスケジュール** — 適用するフィルタ処理を選択してから、予約を設定します。グループの全カテゴリを選択するには、グループのチェックボックスをクリックします。グループ内のすべてのカテゴリを選択するのに、グループを展開する必要はありません。アクセスを制限する期間は、[URL フィルタ設定] 画面 ([業務時間] タブ) で定義されます。詳細については、264 ページの「予約期間の設定」を参照してください。
9. 選択したカテゴリにフィルタ処理を適用するには、[適用] をクリックします。

注意： 同じグループのサブカテゴリに別のフィルタ処理を適用する場合は、手順 8 と 9 を繰り返します。

---

10. (オプション) [パスワードオーバーライドの設定] セクションで、ブロック処理を無効にするために使用されるパスワードを入力する必要があります。これは、URL フィルタカテゴリに対して「オーバーライド付きブロック」処理設定を使用するためのポリシーを設定する場合にのみ必要です。

注意： パスワードはポリシーごとに個別に設定できます。

11. 今後の参照のためにこのポリシーに関して役立つ情報を含めるには、オプションの [備考] を入力します。
12. [次へ] をクリックします。
13. 各検索エンジンに安全な検索の設定を選択し、[次へ] をクリックします。
    - **厳密** — すべての検索結果 (画像、ビデオ、Web 検索を含む) からアダルトコンテンツを排除します。
    - **適度** — Web 検索のみの結果 (イメージ検索を除く) からアダルトコンテンツを排除します。
    - **オフ** — 検索結果のフィルタを行いません。このオプションは初期設定です。
14. 除外リストを適用する場合、[除外リストの指定] 画面で、ドロップダウンリストボックスから除外 URL リスト名を選択します。除外リストにある URL は、URL フィルタ処理が省略されます。
15. [保存] をクリックします。
16. [URL フィルタポリシー] 画面で、[優先度] 列に表示されている上向きまたは下向きの矢印をクリックして、新しいポリシーの優先順位を設定します。

    2 つ以上のポリシーに属するアカウントがある場合、[優先度] の設定により、どのポリシーが適用されるかが決まります。複数のポリシーに属するアカウントに対しては、最初に一致したポリシーが実行されます。最初に一致したポリシーが実行された後は、そのアカウントを含むポリシーは省略されます。
17. [保存] をクリックします。
18. ポリシーをただちに適用するには、[ポリシーの配信] をクリックします。すぐに適用しない場合、データベースキャッシュの有効期限が切れた後に、このポリシーが適用されます。

ポリシーの変更と削除

IWSVA では、使用する環境により適合するように、任意で既存のポリシーを編集するオプションが用意されています。ポリシーから不要なアカウントを削除することもできます。

既存のポリシーを変更するには

1. 管理コンソールから [HTTP] → [URL フィルタ] → [ポリシー] の順に選択します。
2. 変更するポリシーの [アカウント名] リンクまたは [ポリシー名] リンクをクリックします。
3. [URL フィルタポリシー : ポリシーの編集] 画面が開きます。

- [アカウント] タブでクライアントを追加または削除することにより、ポリシーの範囲を変更します。
- [ルール] タブから、URL カテゴリのフィルタ処理を変更します。
- [安全な検索エンジン] タブから、検索エンジンごとに安全な検索モードを変更します。
- [除外設定] タブから、このポリシーに適用する除外リストを選択します。

4. [保存] をクリックします。
5. [HTTP] → [URL フィルタ] → [ポリシー] の順に選択し、矢印を使用してポリシーの優先順位を設定します。2 つ以上のポリシーに属するアカウントがある場合、[優先度] の設定により、どのポリシーが適用されるかが決まります。
6. [保存] をクリックします。
7. ポリシーをただちに適用するには、[ポリシーの配信] をクリックします。すぐに適用しない場合、データベースキャッシュの有効期限が切れた後に、このポリシーが適用されます。

URL フィルタの設定

URL フィルタに関連するいくつかの設定を変更して、実際の作業環境に反映させることができます。

- 7 つの論理グループに分けられた 82 を超える事前定義された Web サイトカテゴリ
- 独自のカスタムカテゴリの設定
- [予約期間] で定義された時間オブジェクトを選択します。

さらに、URL が不適切なカテゴリに分類されていると思われる場合は、URL の分類を見直すようにトレンドマイクロに依頼できます。不明な URL のカテゴリを検索することもできます。

カスタムカテゴリの作成

トレンドマイクロからあらかじめ提供されているカテゴリのほかに、新しい URL カテゴリを定義することができます。たとえば、競合企業の URL を格納する、「競合他社の Web サイト」というカテゴリを作成することができます。

[HTTP] → [設定] → [カスタムカテゴリ] 画面には、ユーザ定義カテゴリのリストが表示されます。[追加] をクリックして新しいカテゴリを作成するか、カテゴリ名をクリックして既存のカテゴリを編集します。

- **カテゴリ名** — 短くてわかりやすいカスタムカテゴリ名を入力します。名前は一意に指定する必要があります。

- **一致** — フィールドに、Web サイト、キーワードまたはフレーズ、あるいは文字列を入力してから、一致条件を適用する方法を指定します。このフィールドには、ワイルドカードとして「?」および「*」を使用できます。このフィールドに入力された内容はカスタムカテゴリに 1 つずつ追加されます。

  注意： HTTPS 復号化ポリシーが適用されていない場合、一致対象の文字列は、IWSVA の設定がプロキシモードか透過モードかによって異なります。
  — プロキシモードの場合、完全な URL ではなく、ドメイン名が一致対象となります。そのため、ドメイン名を指定するだけで済みます。
  — 透過モード (WCCP またはブリッジモード) の場合、受信したサーバ証明書の CommonNames が一致対象となります。

  - **前方一致** — 文字列全体が検索対象となるように制限します。この設定を 1 つ以上のワイルドカードとともに使用すると、設定した URL フィルタ処理を Web サイト全体に適用する場合に特に便利です。URL に「http://」や「https://」を入力する必要はありません (自動的に削除されます)。
  - **部分一致** — URL 内の任意の文字または数値から成る文字列を検索します。文字列が存在する場所に関係なく一致対象となります。たとえば「http://www.encyclopedia/content/sexton.htm」は、文字列「sex」の一致対象と見なされ、このページはブロックされます。このフィールドにワイルドカードを使用すると、誤検出や予期しない結果になる可能性が非常に高くなります。
  - **完全一致** — 文字列全体で照合します。たとえば、特定のサイト、ページ、ファイル、またはその他特定のアイテムを対象とします。

- **カスタムカテゴリリストのインポート** — カテゴリに追加する URL の既存のリストをインポートできます。たとえば、テキストエディタを使用して編集した競合他社の URL のリストがある場合、それらの URL を 1 つ 1 つ入力する代わりに、そのリストをインポートすることができます。インポートリストは、規定の基準に適合する必要があります (詳細については、オンラインヘルプを参照してください)。

URL カテゴリの見直しの依頼と URL 検索

IWSVA には、URL フィルタの基準レベルを提供する、7 つの論理グループに分けられた初期設定のカテゴリが含まれています。たとえば、ユーモアやジョークに関連する Web サイトは「インターネットセキュリティ」グループの「ジョークプログラム」カテゴリに属しています。

初期設定の URL 分類に同意できない場合は、トレンドマイクロにカテゴリの見直しを提案できます。除外リストやカスタムカテゴリを使用して、トレンドマイクロの URL フィルタデータベースで分類されたドメインおよび Web サイトの評価を省略することもできます。

URL フィルタポリシーを適用する前に、初期設定の分類が組織に対して適切かどうか確認することをお勧めします。たとえば、衣料販売業者は、正当な市場調査や競合他社の調査ができるように、「アダルト」グループに分類された「性的な服装 / 水着」カテゴリから水着の Web サイトを除外する必要がある場合があります。

URL のカテゴリを知りたい場合には、[HTTP] → [URL フィルタ] → [設定] | [URL の再分類と検索] タブで URL フィルタ設定を指定すると調べることができます。

未評価の URL および不明 URL

未評価の URL とは、認識されていながら、まだフィルタカテゴリに加えられていない Web サイトのことです。

不明 URL とは、次に該当する Web サイトのことです。

- トレンドマイクロが認識していない Web サイト
- Web レピュテーションデータベースに存在していない Web サイト
- サービスが機能していないか、URL を評価するリモート評価サーバにアクセスできない Web サイト

不明 URL の評価は「0」となり、ブロックできません。

URL カテゴリの見直し依頼

URL カテゴリの見直しを依頼するには

1. 管理コンソールから [HTTP] → [URL フィルタ] → [設定] の順に選択します。
2. [URL の再分類と検索] タブをクリックします。
3. Trend Micro Site Safety Center へのリンクをクリックします。

   [Trend Micro Online URL Query - Feedback System] 画面が表示されます。
4. フィールドに疑わしい URL を入力し、[今すぐ確認] をクリックします。

図 10-1 は、承認する URL からの結果を示しています。

図 10-1. [Trend Micro Online URL Query - Site Safety Center] **画面**

5. 変更を提案するには、[評価内容変更のリクエスト] をクリックして、必要な情報を入力します。

予約期間の設定

IWSVA では、異なる処理に対する日数と時間を設定できます。

URL フィルタのポリシーを作成する際に、特定の時間範囲に対して有効になるようポリシーを設定します。

注意： 同じクラスタ内にあるすべての IWSVA デバイスは、同じ時間帯にあると想定されます。

組織内で URL フィルタポリシーを実装する前に、予約期間に対して新しい時間オブジェクトを作成することをお勧めします。

URL フィルタポリシーのスケジュールを設定するには

1. IWSVA Web コンソールを開き、[管理] → [一般設定] → [予約期間] の順に選択します。
2. 時間オブジェクトの名前と説明を指定します。処理を適用する期間を選択します。
3. [保存] をクリックします。

URL アクセスの警告の TTL

URL アクセスの警告の有効期間 (TTL) 設定を使用すると、管理者は、ユーザが再表示を選択した場合に、初回の警告メッセージが表示されてから次の警告メッセージが表示されるまでの時間間隔を設定できます。

注意： 警告メッセージの反復表示は、初回の警告メッセージの表示後にユーザがその Web ページの続行を選択した場合にのみ実行されます。

[HTTP] → [URL フィルタ] → [設定] → [URL 警告の TTL] タブの順にクリックして、URL アクセスの警告の有効期間 (TTL) を変更できます。

初期設定値は、5 分です。これは、ユーザ別 / カテゴリ別に設定できます。

警告メッセージは、ポリシールールで選択された処理の値が [警告] に設定されている場合に表示されます。詳細については、258 ページの「新しいポリシーの作成」を参照してください。

通知の詳細については、355 ページの「URL アクセスの警告通知の設定」を参照してください。

URL フィルタの除外設定

IWSVA では、除外リストによって URL フィルタに例外を設定することができます (236 ページの「除外リストの指定」を参照)。除外リストにある URL は、ブロックや監視が行われません。URL フィルタによってブロックまたは監視されている Web サイトをクライアントで表示する正当な必要性がある場合、その URL を除外 URL リストに含めて、そのリストをポリシーに適用します。

注意： IWSVA は、安全な検索のフィルタを、除外 URL リストにある Web サイトに適用します。

除外 URL リストを URL フィルタポリシーに適用するには

1. IWSVA Web コンソールを開き、[HTTP] → [URL フィルタ] → [ポリシー] の順に選択して、ポリシー名をクリックしポリシーを編集します。
2. [除外設定] タブで、除外 URL リスト名を選択します。

   注意： 除外リストにある URL は、警告が省略されます。詳細については、355 ページの「URL アクセスの警告通知の設定」を参照してください。

3. [保存] をクリックします。

時間割り当てによる URL フィルタの延長

時間割り当ての延長は、「時間制限」処理が指定された URL フィルタポリシーに使用されます。IWSVA システム管理者が制限時間の経過後も特定の個人にインターネットの閲覧を許可する場合は、ここで時間を延長できます。割り当てられた時間に達すると、ユーザに通知が送信されます。各自の割り当てを使い果たしたユーザはログに記録されます。

このページには次の情報が表示されます。

- **ユーザ** — 名前または IP アドレスによってユーザが識別されます。管理者は、ユーザの検索や、ユーザ名を基準にした並べ替えも実行できます。
- **毎日の時間割り当て** — 閲覧に使用可能な時間量に関するポリシーで割り当てられた時間を表示します。
- **割り当てられた時間の延長** — すでに時間が延長されている場合にその時間を表示します。
- **毎日使用される時間割り当て** — 閲覧に使用された時間の合計を表示します。これには元来割り当てられていた時間と延長された時間、または、使用された時間延長部分を含めることができます。
- **割り当ての延長** — 延長を設定する場所で、次の指定が可能です。
  - **チェックボックス** — 時間を延長するにはオンにします。
  - **値** — 延長したい時間を指定します。
  - **単位** — 延張時間の単位で、分または時間を指定します。

注意： 時間は、URL フィルタポリシーでポリシールールの構成部分として「時間制限」処理が含まれている場合にのみ延長できます。

インターネット閲覧の割り当て時間を延長するには

1. [HTTP] → [アクセス割り当てポリシー] → [URL フィルタの割り当てた時間の延長] に移動します。
2. ユーザ列を並べ替えるか、検索フィールドを使用して該当するユーザを見つけます。
3. 該当するユーザの行の [割り当ての延長] 列に移動します。
4. 時間の延長を可能にするには、チェックボックスをオンにします。
5. 延長の範囲とする時間数を入力し、適切な単位 (時間または分) を選択します。
6. [保存] をクリックして、延長を適用します。

第 11 章

FTP 検索

本章では、InterScan Web Security Virtual Appliance（以下、IWSVA) の FTP ウイルス検索について説明します。また、お使いの環境に合わせて FTP 検索を導入し、設定するさまざまな方法についても説明します。

本章で説明する内容には、次の項目が含まれます。

FTP 検索について

IWSVA では、HTTP トラフィックを処理する場合と同様に、FTP トラフィックにおいてウイルスおよびその他の不正コードを検索できます。ただし、HTTP 検索とは異なり、1 つの設定がネットワーク上のすべてのクライアントに適用されます。FTP 検索では、ユーザまたはグループベースのポリシーはサポートされません。

IWSVA の FTP 検索は、スタンドアロンプロキシを使用するか、またはネットワーク上の別の FTP プロキシと連携して動作します。お使いの環境に FTP 検索を導入するには、最初にプロキシおよびデータ接続の種類 (パッシブ FTP またはアクティブ FTP。269 ページの「パッシブおよびアクティブ FTP」を参照) を制御する FTP 設定を実行します。次に、検索するトラフィックの方向、ブロックまたは検索するファイルのタイプ、圧縮ファイルおよびサイズの大きいファイルの処理方法、および不正コードの検出時に実行する処理を制御する検索ルールを設定します。

FTP 検索の設定が完了したら、オプションのセキュリティおよびパフォーマンス設定の変更について検討します。アクセス管理リストは、クライアントの IP アドレスに基づいて、クライアントの FTP アクセスを許可するように設定できます。コンテンツを直接管理できる FTP サイトに頻繁にアクセスする場合は、パフォーマンスを向上するために、特定の FTP サーバを許可リストに追加して、サイトからのダウンロードが検索されないようにできます。また、特定のポートへの FTP アクセスを許可または拒否して、さらに制限を設定できます。

注意： IWSVA では、WCCP モードでのアクティブ FTP 検索はサポートされません。

FTP 設定

IWSVA の FTP 検索設定には、IWSVA ネイティブ (スタンドアロン) のプロキシと別の FTP プロキシを使用するプロキシ設定のオプション、アクティブモードとパッシブモードを選択するデータコネクションのオプションが含まれています。

プロキシ設定

IWSVA の FTP 検索には、2 つのプロキシ設定オプションがあります。1 つはクライアントが IWSVA ネイティブのプロキシに接続し、IWSVA ネイティブのプロキシが FTP サーバに接続する「スタンドアロン」モード、もう 1 つは IWSVA が別の FTP プロキシ経由で要求を渡し、その FTP プロキシが FTP サーバに接続する「FTP プロキシ」モードです。

- スタンドアロンモードでは、クライアントは < **ユーザ名** >@<FTP **サーバ名** > を FTP ユーザ名として使用し、IWSVA の接続先となる FTP サーバを指定する必要があります。
- FTP プロキシモードでは、IWSVA は常に構成設定で指定された FTP プロキシおよびサーバに接続するため、サーバ名は必要ありません。

FTP プロキシモードは、FTP プロキシ設定で FTP サーバのホスト名または IP アドレスとポート番号を指定することによって、単一の FTP サーバを保護するために使用することもできます。この場合、IWSVA の FTP 検索モジュールは、HTTP 検索のリバースプロキシの場合と同様に、指定した FTP サーバ専用になります。

パッシブおよびアクティブ FTP

IWSVA では、ファイアウォール設定に応じて、データコネクションにアクティブ FTP またはパッシブ FTP のいずれかを使用します。FTP では、データポートとコマンドポートの 2 つのポートを使用します。アクティブ FTP では、サーバがクライアントに接続してデータコネクションを確立します。パッシブ FTP では、クライアントがサーバに接続します。

IWSVA の設定でパッシブ FTP が選択されると、IWSVA はクライアント側の「アクティブ」モードをサーバ側でパッシブモードに変換します。モードの変換は、IWSVA の設定がパッシブで、クライアントがアクティブモードを使用している場合にのみ実行されます。IWSVA の設定がアクティブの場合、変換は実行されないため、クライアントからのパッシブ要求はサーバ側でもパッシブ要求のままになります。

クライアント要求

FTP を設定するには、プロキシ設定とデータコネクションを指定する必要があります。

FTP プロキシでは、IPv4 FTP プロキシの場合と同様に IPv6 FTP プロキシがサポートされ、Web UI では IPv4 アドレスと IPv6 アドレスの両方が受け入れられます。

IWSVA は、FTP プロキシサーバの機能を実行できます。複数のサーバの FTP アップロードを保護するには、サーバごとに IWSVA FTP モジュールをインストールしてください。

FTP の設定を行うには

1. 管理コンソールから [FTP] → [設定] → [一般] の順に選択します。
2. [プロキシ設定] で、構成に基づいて適切な FTP 設定を選択します。ネイティブ IWSVA プロキシで FTP サイトに接続する場合は [スタンドアロンモードを使用] を選択します。FTP サービスと既存の FTP プロキシを組み合わせて使用する場合は、[FTP プロキシを使用] を選択し、[プロキシサーバ] にホスト名を入力して、[ポート番号] を指定します。

3. 使用するデータコネクションの種類を、[パッシブモード] または [アクティブモード] のいずれかから選択します。
4. [保存] をクリックします。

FTP 検索オプション

IWSVA では、事前定義されたポリシーに従って、IPv4 と IPv6 の両サーバの FTP トラフィックを検索できます。

プロキシ転送モードの場合、IWSVA は以下に説明する配信シナリオをサポートしており、IWSVA をデュアルスタックネットワーク環境に展開したときには、FTP、HTTP、HTTPS トラフィックについて IPv4 ネットワークと IPv6 ネットワーク間の自動切り替えを実行できます。このため、IPv4 クライアントから IPv4 クライアントへのアクセスや IPv6 クライアントから IPv4 サーバへのアクセスだけではなく、IWSVA プロキシによって IPv4 クライアントから IPv6 サーバ、または IPv6 クライアントから IPv4 サーバへのアクセスも可能になります。

表 11-1. サポートされているプロキシ転送モードの検索シナリオ

番号	クライアント	サーバ	サポートの有無
1	IPv4	IPv4	有
2	IPv6	IPv6	有
3	IPv4	IPv6	有
4	IPv6	IPv4	有

次の表に示すように、サポートされているその他の配信モードでは、IPv4 ネットワークと IPv6 ネットワーク間の切り替えは実行できません。

表 11-2. サポートされているその他の配信モードの検索シナリオ

番号	クライアント	サーバ	サポートの有無
1	IPv4	IPv4	有
2	IPv6	IPv6	有
3	IPv4	IPv6	無

表 11-2. サポートされているその他の配信モードの検索シナリオ (続き)

番号	クライアント	サーバ	サポートの有無
4	IPv6	IPv4	無

FTP 検索設定は HTTP 検索設定と似ていますが、次の 2 つの違いがあります。

- FTP 検索では、ユーザまたはグループベースのポリシーはサポートされません。そのため、1 つの設定が IWSVA 経由で FTP サイトにアクセスするすべてのクライアントに適用されます。
- 検索するトラフィックの方向を、アップロード、ダウンロード、またはその両方に設定できます。

FTP トラフィックおよび FTP 検索の有効化

クライアントが IWSVA 経由で FTP サイトにアクセスするには、FTP トラフィックを有効にする必要があります。

FTP 検索を有効にするには

1. IWSVA Web コンソールを開き、[FTP] → [検索ルール] の順に選択します。
2. [FTP 検索を有効にする] チェックボックスをオンにします。
3. [保存] をクリックします。

検索方向

IWSVA の FTP 検索をどのように使用するかに応じて、アップロード、ダウンロード、またはその両方を検索するように FTP 検索モジュールを設定できます。たとえば、組織内のすべてのワークステーションにウイルス対策ソフトウェアがインストールされている場合、ファイルはすでにクライアント上で検索されているはずなので、アップロードを無効にすることでパフォーマンスを向上できます。

ファイルのブロック

セキュリティ、監視、またはパフォーマンス上の目的のためにブロックするファイルのタイプを指定できます。ブロックできるのは、Java クラスファイル、Microsoft Office 文書、オーディオ / ビデオ、実行可能ファイル、画像、または手動で設定したその他のタイプのファイルです。組織のポリシーによって特定のタイプのファイルがネットワーク内で禁止されている場合、IWSVA の FTP ファイルブロックでは、該当するファイルを FTP ゲートウェイで阻止できます。

ファイル検索

検索するファイルのタイプを設定するときは、次の 3 つのオプションから選択できます。

- **すべての検索可能ファイル** — すべてのファイルが検索されます。最も安全なオプションです。
- **トレンドマイクロの推奨設定** — ウイルスが潜むことがわかっているファイルタイプのみが検索されます。ファイルタイプはファイルヘッダを確認することによって決定されます。詳細については、222 ページの「トレンドマイクロの推奨設定について」を参照してください。
- **指定のファイル拡張子** — 指定したファイル拡張子を持つファイルのみが検索されます。

パフォーマンス上の理由で他のオプションを選択する必要がある場合を除き、すべてのファイルを検索することをお勧めします。詳細については、274 ページの「FTP 検索の設定」を参照してください。

FTP 検索設定の優先順位

ウイルス検索ルールの設定が互いに競合する場合、プログラムでは次の優先順位に従って検索が実行されます。

1. ブロックするファイルタイプ
2. 検索するファイルタイプ (ブロックされなかった場合)

Intellitrap

HTTP データとともに圧縮された実行可能ファイルを受信した場合、潜在的な不正コードをリアルタイムで検出します。ウイルス作成者は、複数のファイル圧縮スキームを使用して、ウイルスフィルタを回避しようとします。IntelliTrap では、圧縮ファイルのヒューリスティック式評価機能が用意されており、その機能によって、圧縮スキームを使用して潜むウイルスが Web からネットワークに侵入するリスクを減らすことができます。圧縮ファイルに潜む不正な実行可能ファイルに対して、[処理] タブで指定された処理が適用されます。IntelliTrap は、初期設定で有効になっています。

圧縮ファイルの処理

圧縮ファイルは、解凍してからファイル内の個々のファイルを検索する必要があるため、ウイルス対策ソフトウェアのパフォーマンスに負担がかかることがあります。IWSVA には、すべての圧縮ファイルをゲートウェイでブロック、隔離、または放置するオプションが用意されています。

また、次の条件のいずれかを満たす圧縮ファイルに選択した処理を適用するように IWSVA を設定することもできます。

- 解凍後のファイル数が設定した最大値を超える場合
- 解凍後のファイルの累積サイズが設定した最大値を超える場合
- 多重圧縮されたファイルの圧縮レイヤ数が設定した最大値を超える場合

注意： IWSVA では、FTP 検索中も圧縮ファイル内の指定したファイルタイプをブロックできます。

サイズの大きいファイルの処理

サイズの大きいファイルのダウンロード時に遅延を発生させたくない場合、設定したしきい値より大きいファイルの検索を省略するように IWSVA を設定できます。さらに、FTP 検索モジュールでは、サイズの大きいファイルに対して「遅延検索」方法を使用して、クライアントの接続がタイムアウトになるのを防げます。詳細については、229 ページの「遅延検索」を参照してください。

注意： FTP 検索モジュールでは、サイズの大きいファイルを処理する方法として HTTP 検索モジュールで使用される「配信前に検索」はサポートされていません。

隔離ファイルの暗号化

IWSVA が検索処理としてファイルを隔離するように設定されている場合、誰かが隔離ディレクトリを参照中に誤ってファイルを実行しないように、オプションでファイルを暗号化できます。暗号化されたファイルは、トレンドマイクロのサポート部門の担当者以外は暗号化を解除できないため注意してください。

スパイウェアの検索

IWSVA では、ウイルス以外にも、スパイウェアパターンファイルに含まれている多くのリスクを検索できます。これらのリスクの概要については、231 ページの「スパイウェア検索ルール」を参照してください。

情報漏えい対策

IWSVA では、[HTTP] → [情報漏えい対策] → [ポリシー] で作成したポリシーを使用して情報漏えいを検索できます。[FTP] → [検索ルール] | [情報漏えい対策] タブで、DLP テンプレートの名前を選択し、適用する特定のフィルタを使用して許可、ブロック、または監視するかどうかに基づいて検索条件を変更します。

FTP 検索除外リスト

ファイルタイプブロックから除外するファイル名を、除外リストに含めることができます。さらに、除外リストにあるファイルに対してウイルス / スパイウェア検索および圧縮ファイルの処理を省略するように、IWSVA を設定することもできます。

詳細については、236 ページの「除外リストの指定」を参照してください。

FTP 検索の設定

FTP 検索の設定を行うには

1. 管理コンソールから [FTP] → [検索ルール] の順に選択します。
2. [FTP 検索を有効にする] チェックボックスをオンにします。
3. [アップロード]、[ダウンロード]、またはその両方から、検索する FTP 転送の種類を選択します。
4. [ブロックするファイルタイプ] で、ブロックするファイルタイプを選択します。
5. 検索するファイルを選択します。
   - 拡張子に関係なく、すべてのファイルタイプを検索するには、[すべての検索可能ファイル] を選択します。IWSVA は、圧縮したファイルを開き、その中のすべてのファイルを検索します。すべてのファイルを検索するのは最も安全な設定です。

- 実際のファイルタイプによる識別を使用するには、[トレンドマイクロの推奨設定] を選択します。トレンドマイクロの推奨設定では、実際の添付ファイルタイプの検索と正確な拡張子名の検索を組み合わせて使用します。実際の添付ファイルタイプの検索では、ファイルの拡張子が変更されていてもファイルタイプが認識されます。トレンドマイクロの推奨設定では、使用する検索方法が自動的に決定されます。
- 拡張子に基づいてファイルタイプを検索するには、[指定する拡張子] を選択します。これには、ウイルスが潜むことがわかっているファイルタイプのリストが含まれます。IWSVA は、[初期設定の拡張子] リストおよび [その他の拡張子] ボックスで明示的に指定されているファイルタイプのみを検索します。初期設定の拡張子のリストは、ウイルスパターンファイルから定期的にアップデートされます。

  このオプションは、たとえば IWSVA がチェックするファイルの総数を減らして、全体の検索時間を短縮する場合などに使用します。

注意： 指定できるファイルの数やタイプに制限はありません。拡張子の前にアスタリスク (*) を付けないでください。複数のエントリはセミコロン (;) で区切ってください。

6. [圧縮ファイルの処理] で、処理 (ブロック、隔離、放置) を選択して、処理を次のいずれかに適用することを選択します。
   - すべての圧縮ファイル
   - 次の場合に圧縮ファイルを検索

   「次の場合に圧縮ファイルを検索」を有効にする場合は、次のパラメータの値を入力します。
   - 解凍後のファイルが次の数を超える場合 (初期設定は 50000)
   - 解凍後のファイルが次のサイズを超える場合 (初期設定は 200MB)
   - 圧縮レイヤが次の数を超える場合 (0 ～ 20、初期設定は 10)
   - 圧縮率が 99% を超えている場合 (圧縮率 99% 未満のファイルは IWSVA で自動的に許可されます)。
7. [サイズの大きいファイルの処理] で、[検索するファイルサイズの上限を設定する] チェックボックスをオンにし、ファイルサイズを入力します。
8. サイズの大きいファイルをダウンロード中にブラウザがタイムアウトする問題を避けるには、[次のサイズを超えるファイルに対して遅延検索を有効にする] チェックボックスをオンにして、遅延検索が発生しない最大ファイルサイズを入力します。また、ドロップダウンリストから、検索されないクライアントに送信されるデータの割合を選択します。

警告： **検索実行前にファイルの一部を配信することで、ウイルス感染の可能性も生じます。そのため、パフォーマンスとセキュリティのバランスは管理者の判断にかかっています。このオプションは、現在タイムアウトの問題が発生している場合にのみ使用してください。**

9. 隔離ディレクトリに送信されるファイルを暗号化して、不注意で開かれたり実行されたりするのを防ぐには、[隔離ファイルを暗号化する] を選択します。
10. [保存] をクリックして、[スパイウェア検索ルール] タブに切り替えます。
11. 検索するその他のリスクの種類を選択して、[保存] をクリックします。
12. [情報漏えい対策] タブで、[HTTP] → [情報漏えい対策] → [ポリシー] で作成した DLP テンプレートを、DLP テンプレートリストから選択します。
13. フィルタルールを変更し、フィルタを使用して検索、ブロック、または監視するかどうかを決定します。[保存] をクリックします。
14. [除外設定] タブで、ドロップダウンリストから除外ファイル名リストを選択します。

    除外リストにあるファイルの内容についてウイルス検索をしないようにするには、[選択した除外リストの内容を検索しない] を選択します。この場合、圧縮ファイルの処理は適用されません。
15. [処理] タブに切り替え、検索に対して IWSVA で実行する処理を選択します。
16. [保存] をクリックします。

ウイルスに対する検索処理の設定

([FTP] → [検索ルール] → [処理] タブ) 感染ファイル（1 次処理) — 感染ファイルの検出時に FTP 検索で実行する処理を指定できます。推奨される処理設定は [駆除] です。

- 感染ファイルを駆除せずに隔離ディレクトリに移動するには、[隔離] を選択します。要求元クライアントはファイルを受信しません。
- 感染ファイルを削除するには、[削除] を選択します。要求元クライアントはファイルを受信しません。
- 感染ファイルを自動的に駆除して処理するには、[駆除] を選択します。ファイルが駆除可能な場合、要求元クライアントは駆除されたファイルを受信します。

2 次処理 — ワームやトロイの木馬などの駆除不能ファイルの検出時に FTP 検索で実行する処理を指定できます。推奨される処理設定は [削除] です。

- 駆除できないファイルを駆除せずにクライアントに送信するには、[放置] を選択します。感染ファイルがネットワークに侵入する可能性があるため、この設定はお勧めしません。
- 駆除できないファイルを駆除せずに隔離ディレクトリに移動するには、[隔離] を選択します。要求元クライアントはファイルを受信しません。
- 駆除不能なファイルを削除するには、[削除] を選択します。要求元クライアントはファイルを受信しません。

パスワードで保護されたファイル — パスワードで保護された圧縮ファイルに対して FTP 検索で実行する処理を指定できます。推奨される処理設定は [放置] です。

- パスワードで保護されたファイルを駆除せずにクライアントに送信するには、[放置] を選択します。
- パスワードで保護されたファイルを駆除せずに隔離ディレクトリに移動するには、[隔離] を選択します。要求元クライアントはファイルを受信しません。
- パスワードで保護されたファイルを削除するには、[削除] を選択します。要求元クライアントはファイルを受信しません。

マクロ — FTP 転送中にマクロ (マクロウイルスに限らず) を含むファイルが検出された場合は、次の処理を実行できます。推奨される処理設定は [放置] です。

- マクロを含むファイルを隔離ディレクトリに移動するには、[隔離] を選択します。
- ファイルの配信前にマクロを削除するには、[駆除] を選択します。
- マクロを含むファイルの特別な処理を無効にするには、[放置] を選択します。

FTP 一般設定

FTP を設定するには、プロキシ設定とデータコネクションを指定する必要があります。

FTP プロキシでは、IPv4 FTP プロキシの場合と同様に IPv6 FTP プロキシがサポートされ、Web UI では IPv4 アドレスと IPv6 アドレスの両方が受け入れられます。

IWSVA は、FTP プロキシサーバの機能を実行できます。複数のサーバの FTP アップロードを保護するには、サーバごとに IWSVA FTP モジュールをインストールしてください。

プロキシ設定

- **スタンドアロンモードを使用** — ネットワーク上の唯一の FTP プロキシとして IWSVA をインストールする場合は、このオプションを選択します。

- FTP **プロキシを使用** — ネットワーク上に既存の FTP プロキシとともに IWSVA をインストールする場合は、このオプションを選択します。IWSVA を FTP プロキシと同一のコンピュータにインストールするか異なるコンピュータにインストールするかによって、次のフィールドの入力値が異なります。
  - **プロキシサーバ** — IWSVA が FTP トラフィックを受信する FTP プロキシのホスト名または IP アドレスを指定します。IWSVA FTP 検索機能を FTP サーバと同じコンピュータにインストールする場合は、「localhost」を使用します。
  - **ポート** — FTP プロキシが IWSVA に FTP トラフィックを送信する際に使用するポート番号を示します。通常はポート 21 です。

データコネクション

ほとんどのファイアウォールは、LAN 外部からの無用なポート要求を拒否するように設定されているため、IWSVA ではアクティブ転送とパッシブ転送の両方をサポートしています。パッシブ転送が通常必要となるのは、LAN にファイアウォールがある場合、またはアクティブ FTP を設定する際にデータチャネルに障害が発生した場合です。

管理コンソールから [FTP] → [設定] → [一般] の順に選択します。

- **パッシブモード** — パッシブ FTP のみを許可するファイアウォール内で IWSVA を実行する場合は、このオプションを選択します。

  パッシブ FTP (PASV モード) では、FTP クライアントから FTP サーバに対して問い合わせが開始されます。FTP サーバがこのクライアントに対してデータ転送に使用する接続ポートを通知し、クライアントがこのポート上のサーバに対して別の接続を開きます。
- **アクティブモード** — スタンドアロンでインストールした IWSVA をアクティブ FTP を許可するファイアウォール内で実行する場合、またはファイアウォール外で実行するようにインストールした場合 (推奨しません)、このオプションを選択します。

  アクティブ FTP では、FTP クライアントから FTP サーバに対して問い合わせが開始され、次にお互いのデータ転送ポートを取り決めます。IWSVA では通常はポート 22020 が使用されます。取り決めたポートを使用して、サーバはクライアントに接続し直します。

注意： このポートに対してはファイアウォールを開き、FTP サーバがクライアントと通信できるようにする必要があります。または、ポートを手動で開く必要があります。

注意： 作成するクライアント要求およびワーカースレッドの最大数は、`/etc/iscan/intscan.ini` ファイルを編集することにより手動で設定できます。

FTP アクセス管理設定

IWSVA には、セキュリティおよびパフォーマンスをさらに調整するために、いくつかのアクセス管理設定が用意されています。

- クライアントの IP アドレスに基づいて FTP アクセスを有効にできます。
- コンテンツの厳しい管理が可能な信頼するサーバに頻繁にアクセスする場合、そのサーバを許可リストに追加できます。転送が検索されなくなるため、パフォーマンスが向上します。
- 設定したポートへのアクセスを拒否することによって、IWSVA の FTP サーバを制限できます。

クライアント IP による設定

初期設定では、FTP トラフィックが有効な場合、ネットワーク上のすべてのクライアントが IWSVA デバイス経由で FTP サイトにアクセスできます (271 ページの「FTP トラフィックおよび FTP 検索の有効化」を参照)

ポリシーの選択時には、IPv4 と IPv6 の両方のポリシーが表示されます。クライアントのアクセス管理では、IPv4 でサポートされているものと同様に、単一の IPv6 アドレス、IPv6 アドレス範囲、または IPv6 マスクが受け入れられます。

クライアントの IP アドレスに基づいて FTP アクセスを制限するには

1. 管理コンソールで [FTP] → [設定] → [アクセス管理の設定] の順に選択します。
2. [クライアント IP] タブに切り替えます。
3. [クライアント IP に基づく FTP アクセス管理を有効にする] チェックボックスをオンにします。
4. IWSVA 経由の FTP アクセスを許可するクライアントの IP アドレスを入力します。入力できるエントリは次のとおりです。
   - IP/**ホスト名** — 単一の IP アドレスまたはホスト名。たとえば、123.123.123.12 のようになります。
   - IP **範囲** — 連続する IP アドレスの範囲に含まれるクライアント。たとえば、123.123.123.12 ～ 123.123.123.15 のようになります。
   - IP **サブセット** — 指定したサブネット内の単一のクライアント。たとえば、IP に「192.168.1.0」、マスクに「255.255.255.0」と入力すると、192.168.1.x サブネット内のすべてのコンピュータが識別されます。または、マスクをビット数 (0 ～ 32) で指定することもできます。
5. [説明] フィールドにわかりやすい名前を入力します (40 文字以内)。

6. [追加] をクリックして、FTP サイトへのアクセスを許可する他のクライアントの入力を続けます。
7. [保存] をクリックします。

サーバ IP の除外リストによる設定

コンテンツの直接管理が可能な信頼する FTP サイトの場合、サイトへのアクセス時にパフォーマンスの問題が発生する可能性を少なくするために、一部の FTP サイトの IP アドレスを許可リストに追加して、これらのサイトを検索から除外できます。

注意： IP の許可リストによる検索の除外は、ファイルのダウンロードにのみ適用されます。アップロードされるファイルは検索されます。

ポリシーの選択時には、IPv4 と IPv6 の両方のポリシーが表示されます。サーバのアクセス管理では、IPv4 でサポートされているものと同様に、単一の IPv6 アドレス、IPv6 アドレス範囲、または IPv6 マスクが受け入れられます。

信頼するサーバを許可リストに追加するには

1. 管理コンソールで [FTP] → [設定] → [アクセス管理の設定] の順に選択します。
2. [サーバ IP の除外リスト] タブに切り替えます。
3. IWSVA の FTP ウイルス検索から除外する FTP サイトの IP アドレスを入力します。サーバの識別方法および例については、149 ページの「クライアントとサーバの識別」を参照してください。
4. [説明] フィールドにわかりやすい名前を入力します (40 文字以内)。
5. [追加] をクリックして、除外する他の FTP サイトの入力を続けます。
6. [保存] をクリックします。

宛先ポートによる設定

初期設定では、クライアントは IWSVA の FTP サーバのどのポートにもアクセスできます。セキュリティを強化するために、ポートへのアクセスを選択的に許可または拒否できます。

クライアントが接続できる IWSVA FTP ポートを設定するには

1. 管理コンソールで [FTP] → [設定] → [アクセス管理の設定] の順に選択します。
2. [宛先ポート] タブに切り替えます。

3. [拒否] または [許可] のいずれかから、ポートに適用する処理を選択します。
4. 処理を適用する [ポート番号] または [ポート範囲] を入力します。
5. [説明] フィールドにわかりやすい名前を入力します (40 文字以内)。
6. [追加] をクリックします。
7. 許可または拒否する他のポートの追加を続けます。
8. [保存] をクリックします。

注意 : [宛先ポート] タブのポートは、降順で一覧表示されます。宛先ポートによるアクセス管理は、FTP コマンド接続時にのみ適用されます。FTP データコネクションは影響を受けません。一般的な設定は、1.「すべてを拒否」および、ポート 21 へのアクセスのみが許可される 2.「21 を許可」です。

第 12 章

コマンドラインインタフェースのコマンド

本章では、InterScan Web Security Virtual Appliance（以下、IWSVA) 製品のコマンドラインインタフェース（CLI) のコマンドについて説明します。このコマンドは、監視、デバッグ、トラブルシューティング、設定の各タスクを実行する際に使用できます。

本章で説明する内容には、次の項目が含まれます。

SSH アクセス

IWSVA ターミナル (IWSVA サーバに直接接続されたキーボードとモニタ) を介して、または管理 IP アドレスへの SSH v2 接続を使用してリモートで IWSVA CLI インタフェースへアクセスできます。SSH を使用して CLI にアクセスする前に、まず Web コンソールで SSH アクセス管理を有効にする必要があります ([管理] → [ネットワーク設定] → [リモート CLI] の順に選択)。

SSH 経由のパスワードブルートフォースアタックを防止する

IWSVA では、ブルートフォースアタックからパスワードを保護できます。リモートターミナルから SSH を使用して間違ったパスワードで IWSVA にログオンが試行された場合、IWSVA は後続のログオン試行を拒否します。この機能は、CLI を使用して有効または無効にできます。

パスワードブルートフォースアタック対策機能を有効にするには

1. 「root」、「enable」、または「admin」アカウントを使用して IWSVA にログオンします。「root」および「admin」アカウントユーザは SSH を使用してログオンできますが、「enable」アカウントユーザは IWSVA ローカルマシンにしかログオンできません。
   - 「root」アカウントでログオンする場合は、**「clish」**および**「enable」**と入力して、clish 特権モードにアクセスします。
   - 「admin」アカウントでログオンする場合は、**「enable」**と入力して、clish 特権モードにアクセスします。
   - 「enable」アカウントでログオンする場合は、すでに clish 特権モードに入っています。
2. この機能を有効にするには、次のコマンドを入力します。**configure service pswd_protection enable**

パスワードブルートフォースアタック対策機能を無効にするには

1. 前の手順のステップ 1 を実行します。
2. この機能を無効にするには、次のコマンドを入力します。**configure service pswd_protection disable**

コマンドモード

コマンドラインインタフェースにアクセスするには、管理者アカウントとパスワードが必要になります。IWSVA の CLI コマンドは、非特権コマンドと特権コマンドの 2 つのカテゴリに分類されます。

非特権コマンドは基本的なコマンドです。これによって、管理者がセキュリティリスクの低い情報を取得したり、単純なタスクを実行できます。非特権コマンドプロンプトは、山括弧 (>) の入力で終了します。

リモート SSH から CLI にログイン — リモート SSH から IWSVA の CLI に管理者アカウントとパスワードでログインします (非特権コマンドのみサポート)。

ローカル SSH で CLI にログイン — ローカル SSH に `root` アカウントでログインし、コマンド `clish` を実行して CLI にログインします (非特権コマンドのみサポート)。

特権コマンドには、設定をフルに制御する機能、高度な監視機能、およびデバッグ機能が用意されています。

コマンドラインインタフェースのログイン方法 (ssh からのログイン) —

1. 管理コンソールから [管理] → [管理コンソール] → [アカウント管理] にて IWSVA のログインアカウントを作成します。
2. ssh にて IWSVA に接続し、IWSVA のログインアカウントを入力し、CLI にログインします。

コマンドラインインタフェースのログイン方法 (clish コマンドからのログイン) —

1. IWSVA に root でログインします。
2. clish コマンドで CLI にログインします。

   ```
   # clish
   ```

特権モードの移行方法 —

1. CLI にて enable コマンドを入力します。

   ```
   > enable
   ```

2. コマンドラインが以下のとおりに変更されたことを確認します。

   ```
   enable#
   ```

特権モードの終了方法 —

1. CLI の特権モードにて exit コマンドを入力します。

   ```
   enable# exit
   ```

コマンドラインインタフェースのログアウト方法 –

1. CLI の非特権モードにて exit コマンドを入力します。

```
> enable
```

注意： 一部の CLI コマンドは、HA クラスタの下位メンバーでは使用できません。これらのパラメータはクラスタの上位メンバーで設定する必要があるためです。下位サーバで使用できないコマンドは、`configure system date`、`configure module ntp`、`configure system password`、`configure service ssh`、および `configure system timezone` です。

コマンドのリスト

次の表は、使用可能なコマンドを示しています。

表 12-1. コマンドラインインタフェースのコマンド

コマンド	構文	説明
configure module database password	configure module database password	データベースのパスワードを設定します
configure module http bypass_non_http disable	configure module http bypass_non_http disable	HTTP 以外のトラフィックのバイパスを無効化します
configure module http bypass_non_http enable	configure module http bypass_non_http enable	HTTP パケットでないトラフィックのバイパスを有効化します
configure module http scan_before_deliver_port	configure module http scan_before_deliver_port < ポート > [管理インタフェース]	配信前の検索用のリダイレクトポートの IPv4 および IPv6 アドレスを設定します。IPv4 および IPv6 のリダイレクト要求は、クライアントに直接送信されます。

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
configure module http x-forwarded-for action add	configure module http x-forwarded-for action add	XFF HTTP ヘッダに最後のホップの IP アドレスを追加します
configure module http x-forwarded-for action keep	configure module http x-forwarded-for action keep	XFF HTTP ヘッダに変更を加えません
configure module http x-forwarded-for action remove	configure module http x-forwarded-for action remove	アップストリームのセキュリティを強化するため、HTTP 要求から XFF HTTP ヘッダを削除します
configure module http x-forwarded-for parse disable	configure module http x-forwarded-for parse disable	XFF HTTP ヘッダの構文解析を無効にします
configure module http x-forwarded-for parse enable	configure module http x-forwarded-for parse enable	XFF HTTP ヘッダの構文解析を有効にして、ポリシーマッチングに使用する元の IP アドレスを取得できるようにします
configure module https hardware_engine cavium	configure module https hardware_engine cavium	ハードウェアアクセラレータカードの「cavium」を使用します。この操作を実行するには、該当するハードウェアカードがコンピュータに挿入されている必要があります。
configure module https hardware_engine none	configure module https hardware_engine none	SSL ハードウェアアクセラレータカードを使用しないでください
configure module https logacccfullurl	configure module https logaccfullurl <enable （有効） /disable （無効） >	logaccfullurl を設定します
configure module identification mac_address <enable (有効)/disable (無効)>	configure module identification mac_address <enable (有効)/disable (無効)>	ホスト名の識別方法に MAC アドレスを含める、または除外します

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
configure module ldap groupcache interval	configure module ldap groupcache interval < 間隔 >	IWSVA LDAP ユーザグループメンバーシップ用キャッシュ間隔を設定します < 間隔 >: UINT 形式の間隔で、時間単位で指定します
configure module ldap ipuser_cache disable	configure module ldap ipuser_cache disable	IWSVA LDAP IP ユーザキャッシュを無効化します
configure module ldap ipuser_cache enable	configure module ldap ipuser_cache enable	IWSVA LDAP IP ユーザキャッシュを有効化します
configure module ldap ipuser_cache interval	configure module ldap ipuser_cache interval < 間隔 >	IWSVA LDAP IP ユーザキャッシュ間隔を設定します < 間隔 >: FLOAT 形式の間隔で、時間単位で指定します
configure module ldap www-auth port	configure module ldap www-auth port < ポート >	ユーザ / グループの認証ポートを透過モード (WCCP またはブリッジモード) で設定します
configure module log transaction disable	configure module log transaction disable	トランザクションログを無効化します
configure module log transaction enable	configure module log transaction enable	トランザクションログを有効化します
configure module log transaction filter disable	configure module log transaction filter disable	トランザクションログフィルタを無効化します。

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
configure module log transaction filter enable	configure module log transaction filter enable < 送信元 IP> < 送信先 IP>	トランザクションログフィルタを有効化します。 パラメータ名 :「送信元 IP」 AAA.BBB.CCC.DDD 形式の IP アドレス (各部分は 0 ～ 255 の範囲の値) パラメータ名 :「送信先 IP」 AAA.BBB.CCC.DDD 形式の IP アドレス (各部分は 0 ～ 255 の範囲の値)
configure module log verbose filter disable	configure module log verbose filter disable	デバッグログフィルタを無効化します
configure module log verbose filter enable	configure module log verbose filter enable < 送信元 IP> < 送信先 IP>	デバッグログフィルタを有効化します
configure module log verbose ftp disable	configure module log verbose ftp disable	デバッグ FTP ログを無効化します
configure module log verbose ftp enable	configure module log verbose ftp enable	デバッグ FTP ログを有効化します
configure module log verbose http disable	configure module log verbose http disable	デバッグ HTTP ログを無効化します
configure module log verbose http enable	configure module log verbose http enable	デバッグ HTTP ログを有効化します
configure module log verbose wccp disable	configure module log verbose wccp disable	デバッグ WCCP ログを無効化します
configure module log verbose wccp enable	configure module log verbose wccp enable	デバッグ WCCP ログを有効化します

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
configure module ntp schedule <enable （有効）/disable （無効）>	configure module ntp schedule <enable （有効）/disable （無効）>	予約 NTP 時刻の同期を有効化 / 無効化します
configure module ntp schedule	configure module ntp schedule < 間隔 > < プライマリサーバ > [セカンダリサーバ]	予約 NTP 時刻の同期を設定します < 間隔 >: 30 分、1 時間、2 時間、4 時間、6 時間、12 時間、1 日、2 日、3 日、1 週間、1 か月の単位で指定します < プライマリサーバ >: プライマリ NTP サーバを ADDRESS 形式で指定します < セカンダリサーバ >: セカンダリ NTP サーバを ADDRESS 形式で指定します
configure module ntp sync	configure module ntp sync < サーバ >	IPv4 および IPv6 NTP サーバの同期を設定します < サーバ >: NTP サーバを ADDRESS 形式で指定します
configure network bonding add	configure network bonding add < ボンディング名 > [インタフェース 1] [インタフェース 2] [インタフェース 3] [インタフェース 4]	リンク集合体のボンディングインタフェースを追加します < ボンディング名 > は、ボンディングインタフェースの名前です

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
configure network bonding options miimon	configure network bonding options miimon < 間隔 >	指定されたボンディングデバイスの miimon オプションを設定します < 間隔 > とは、設定される特定の miimon 間隔です。初期設定は 100 です。 **注意：** miimon の値は、ミリ秒単位で設定します。
configure network bonding options xmit_hash_policy	configure network bonding options xmit_hash_policy < ポリシー >	指定されたボンディングデバイスの xmit_hash_policy オプションを設定します < ポリシー > とは、設定される特定の xmit_hash_policy です 初期設定は 1 (3layer) です。0 (2layer) も使用できます。
configure network bonding remove	configure network bonding remove < ボンディング名 >	リンク集合体のボンディングインタフェースを削除します < ボンディング名 > は、ボンディングインタフェースの名前です
configure network bridge interface	configure network bridge interface [インタフェース 1] [インタフェース 2] [インタフェース 3] [インタフェース 4] [インタフェース 5] [インタフェース 6] [インタフェース 7] [インタフェース 8]	初期設定のブリッジインタフェースを変更します < 内部 > IFNAME インタフェース名またはリンク集合体のボンディング名です < 外部 > IFNAME インタフェース名またはリンク集合体のボンディング名です

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
configure network bridge redirect ftpports	configure network bridge redirect ftpports < ポート >	リダイレクション FTP ポートを設定します < ポート >: リダイレクトポートを < ポート 1; ポート 2;...> の MULTIPORTS 形式で指定します
configure network bridge redirect httpports	configure network bridge redirect httpports < ポート >	リダイレクション HTTP ポートを設定します < ポート >: リダイレクトポートを < ポート 1; ポート 2;...> の MULTIPORTS 形式で指定します
configure network bridge redirect httpsports	configure network bridge redirect httpsports < ポート >	リダイレクション HTTPS ポートを設定します < ポート >: リダイレクトポートを < ポート 1; ポート 2;...> の MULTIPORTS 形式で指定します
configure network bridge stp	configure network bridge stp	初期設定ブリッジの STP を設定します
configure network bridge stp disable	configure network bridge stp disable	IWSVA の STP を無効にします
configure network bridge stp enable	configure network bridge stp enable	IWSVA の STP を有効にします
configure network bridge stp priority	configure network bridge stp priority	IWSVA の STP の優先順位を設定します

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
configure network dns ipv4	configure network IPv4 dns <DNS1> [DNS2]	IPv4 の DNS を設定します <DNS1>: プライマリ IPv4 DNS サーバを IP_ADDR 形式で指定します <DNS2>: セカンダリ IPv4 DNS サーバを IP_ADDR 形式で指定します
configure network dns ipv6	configure network IPv6 dns <DNS1> [DNS2]	IPv6 の DNS を設定します <DNS1>: プライマリ IPv6 DNS サーバを IP_ADDR 形式で指定します <DNS2>: セカンダリ IPv6 DNS サーバを IP_ADDR 形式で指定します
configure network hostname	configure network hostname < ホスト名 >	ホスト名を設定します < ホスト名 >: HOSTNAME 形式のホスト名または FQDN です
configure network interface ipv4 dhcp < ネットワークインタフェース名 > [<VLAN>]	configure network interface ipv4 dhcp < ネットワークインタフェース名 > [<VLAN>]	DHCP を使用して IPv4 アドレスを取得するために、初期設定の Ethernet インタフェースを設定します。 VLAN: VLAN ID を 1 ～ 4094 の数字で指定します。初期設定では VLAN なしになります ([0])。
configure network interface ipv6 dhcp < ネットワークインタフェース名 > [<VLAN>]	configure network interface ipv6 dhcp < ネットワークインタフェース名 > [<VLAN>]	DHCP を使用して IPv6 アドレスを取得するために、初期設定の Ethernet インタフェースを設定します。 VLAN: VLAN ID を 1 ～ 4094 の数字で指定します。初期設定では VLAN なしになります ([0])。

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
configure network interface duplex	configure network interface duplex <Ethernet インタフェース名 > < 二重化 >	Ethernet インタフェースの二重化を設定します
configure network interface ping < インタフェース名 > < 処理 >	configure network interface ping < インタフェース名 > <enable (有効)/disable (無効)>	専用の管理インタフェースの ICMP 要求を受け入れ / 禁止します
configure network interface ipv4 static	静的 IPv4 を使用するためにネットワークインタフェースを設定します。< インタフェース名 > <IPv4 アドレス > < ネットワークマスク > [VLAN]	初期設定の Ethernet インタフェースで静的 IPv4 アドレスを使用するために設定します。
configure network interface ipv6 static	静的 IPv6 を使用するためにネットワークインタフェースを設定します。< インタフェース名 > <IPv6 アドレス > < ネットワークマスク > [VLAN]	初期設定の Ethernet インタフェースで静的 IPv6 アドレスを使用するために設定します。
configure network mgmt disable	configure network mgmt disable	別個の IWSVA 管理インタフェースを無効化します
configure network mgmt interface	configure network mgmt interface < インタフェース名 >	IWSVA 管理インタフェース名を設定します
configure network portgroup add	configure network portgroup add < ポートグループ名 > [インタフェース 1] [インタフェース 2] [インタフェース 3] [インタフェース 4] [インタフェース 5] [インタフェース 6] [インタフェース 7] [インタフェース 8]	ポートグループを追加します

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
configure network portgroup linkloss < ポートグループ名 >	configure network portgroup linkloss < ポートグループ名 >	ポートグループのリンクロスの転送を設定します
configure network portgroup remove < ポートグループ名 >	configure network portgroup remove < ポートグループ名 >	ポートグループを削除します
configure network portgroup vlan < ポートグループ名 >	configure network portgroup vlan < ポートグループ名 >	ポートグループの VLAN ID を設定します
configure network proxy interface	configure network proxy interface < プロキシ >	初期設定のプロキシインタフェースを設定します < プロキシ >: IFNAME インタフェース名です。
configure network route ipv4/ipv6 add <IP プレフィックスの長さ > < 経由 > < デバイス >	configure network route ipv4/ipv6 add <xxx.xxx.xxx.xxx/LL> < 経由 > < デバイス >	指定した NIC デバイスのルートを追加します
configure network route ipv4/ipv6 default < ゲートウェイ >	configure network route ipv4/ipv6 default < ゲートウェイ >	ネットワークルートの設定を実行することにより、初期設定のゲートウェイをリセットします <*.*.*.*>
configure network route ipv4/ipv6 del <IP プレフィックスの長さ > < 経由 > < デバイス >	configure network route ipv4/ipv6 del <xxx.xxx.xxx.xxx/LL> < 経由 > < デバイス >	指定した NIC デバイスのルートを削除します
configure service pswd_protection disable	configure service pswd_protection disable	SSH パスワード保護サービスを無効化します
configure service pswd_protection enable	configure service pswd_protection enable	SSH パスワード保護サービスを有効化します

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
configure service recycle time	configure service recycle time <hh:mm>	定時リサイクルを有効化します パラメータ名は「時刻」です 00:00 から 23:59 までの時刻を hh:mm の形式で指定します
configure service recycle disable time	configure service recycle disable time	定時リサイクルを無効化します
configure service recycle transaction	configure service recycle transaction < トランザクション数 >	トランザクション数ごとのリサイクルを有効化します パラメータ名は「トランザクション」です トランザクション数が 100000 ～ 99999999 に達すると、リサイクルが実行されます
configure service recycle disable transaction	configure service recycle disable transaction	トランザクション数ごとのリサイクルを無効化します
configure service ssh disable	configure service ssh disable	SSH デーモンを無効化します
configure service ssh enable	configure service ssh enable	SSH デーモンを有効化します
configure service ssh port	configure service ssh port < ポート >	SSH ポート番号を設定します < ポート >: SSH ポート番号を [1 ~ 65535] の PORT 形式で指定します
configure module socks_sftp_proxy enable	configure module socks_sftp_proxy enable	SOCKS 経由で SFTP を有効化します

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
configure module socks_sftp_proxy disable	configure module socks_sftp_proxy disable	SOCKS 経由で SFTP を無効化します
configure module socks_sftp_proxy port	configure module socks_sftp_proxy port < ポート >	初期設定のポート番号を変更します 範囲 : 1 ～ 65535
configure system date	configure system date < 日付 > < 時間 >	日付を設定して CMOS に保存します < 日付 >: DATE_FIELD [DATE_FIELD] < 時間 >: TIME_FIELD [TIME_FIELD]
configure system ha	configure system ha	高可用性の設定を行います
configure system ha remove	configure system ha remove	HA 設定を削除し、IWSVA を再起動します
configure system ha synchronization interval	configure system ha synchronization interval	HA 同期の間隔を設定します パラメータ名 :「間隔」 HA で設定が下位サーバに同期される間隔 (分単位)。 範囲 (分) : 5 ～ 60
configure system harddisk	configure system harddisk	新しいハードディスクを追加し、IWSVA のデータパーティション容量を拡張します **注意 :** IWSVA では、一度に 1 つのみの新しいハードディスクの追加をサポートし、IWSVA のデータパーティション容量を拡張します。

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
configure system hwmonitor	configure system hwmonitor	システムハードウェア監視情報を設定します。
configure system hwmonitor interval	configure system hwmonitor interval [1 ～ 60]	ハードウェアステータスのポーリング間隔を分単位で設定します。範囲は 1 ～ 60 分です。初期設定の長さは IPMI のポーリングサイクルによって決まります。
configure system keyboard	configure system keyboard	システムキーボードのレイアウトタイプを設定します
configure system keyboard us	configure system keyboard us	システムキーボードのレイアウトタイプを米国英語に設定します
configure system password	configure system password < ユーザ >	アカウントパスワードを設定します < ユーザ >: パスワードの変更対象となるユーザの名前を USER 形式で指定します。このユーザは、IWSVA の管理者グループの「enable」や「root」などのユーザに設定できます
configure system timezone Africa Cairo	configure system timezone Africa Cairo	タイムゾーンをアフリカのカイロ地域に設定する
configure system timezone Africa Harare	configure system timezone Africa Harare	タイムゾーンをアフリカのハラレ地域に設定する
configure system timezone Africa Nairobi	configure system timezone Africa Nairobi	タイムゾーンをアフリカのナイロビ地域に設定します
configure system timezone America Anchorage	configure system timezone America Anchorage	タイムゾーンを米国アンカレジ地域に設定します

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
configure system timezone America Bogota	configure system timezone America Bogota	タイムゾーンを南米のボゴタ地域に設定します
configure system timezone America Buenos_Aires	configure system timezone America Buenos_Aires	タイムゾーンを南米のブエノスアイレス地域に設定します
configure system timezone America Chicago	configure system timezone America Chicago	タイムゾーンを米国シカゴ地域に設定します
configure system timezone America Chihuahua	configure system timezone America Chihuahua	タイムゾーンを中央アメリカのチワワ地域に設定します
configure system timezone America Denver	configure system timezone America Denver	タイムゾーンを米国デンバー地域に設定します
configure system timezone America Godthab	configure system timezone America Godthab	タイムゾーンをアメリカのゴットホープ地域に設定します
configure system timezone America Lima	configure system timezone America Lima	タイムゾーンを南米のリマ地域に設定します
configure system timezone America Los_Angeles	configure system timezone America Los_Angeles	タイムゾーンを米国ロサンゼルス地域に設定します
configure system timezone America Mexico_City	configure system timezone America Mexico_City	タイムゾーンを中央アメリカのメキシコシティ地域に設定します
configure system timezone America New_York	configure system timezone America New_York	タイムゾーンを米国ニューヨーク地域に設定します
configure system timezone America Noronha	configure system timezone America Noronha	タイムゾーンを南米のノローニャ地域に設定します
configure system timezone America Phoenix	configure system timezone America Phoenix	タイムゾーンを米国フェニックス地域に設定します
configure system timezone America Santiago	configure system timezone America Santiago	タイムゾーンを南米のサンティアゴ地域に設定します

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
configure system timezone America St_Johns	configure system timezone America St_Johns	タイムゾーンを北米のセントジョンズ地域に設定します
configure system timezone America Tegucigalpa	configure system timezone America Tegucigalpa	タイムゾーンを中央アメリカのテグシガルパ地域に設定します
configure system timezone Asia Almaty	configure system system timezone Asia Almaty	タイムゾーンを中央アジアのアルマティ地域に設定します
configure system timezone Asia Baghdad	configure system timezone Asia Baghdad	タイムゾーンを中近東のバグダッド地域に設定します
configure system timezone Asia Baku	configure system timezone Asia Baku	タイムゾーンを中近東のバクー地域に設定します
configure system timezone Asia Bangkok	configure system timezone Asia Bangkok	タイムゾーンを東南アジアのバンコク地域に設定します
configure system timezone Asia Calcutta	configure system timezone Asia Calcutta	タイムゾーンを南アジアのカルカッタ地域に設定します
configure system timezone Asia Colombo	configure system timezone Asia Colombo	タイムゾーンを南アジアのコロンボ地域に設定します
configure system timezone Asia Dhaka	configure system timezone Asia Dhaka	タイムゾーンを南アジアのダッカ地域に設定します
configure system timezone Asia Hong_Kong	configure system timezone Asia Hong_Kong	タイムゾーンを極東の香港地域に設定します
configure system timezone Asia Irkutsk	configure system timezone Asia Irkutsk	タイムゾーンをアジアのイルクーツク地域に設定します
configure system timezone Asia Jerusalem	configure system timezone Asia Jerusalem	タイムゾーンを中近東のエルサレム地域に設定します
configure system timezone Asia Kabul	configure system timezone Asia Kabul	タイムゾーンを中近東のカブール地域に設定します

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
configure system timezone Asia Karachi	configure system timezone Asia Karachi	タイムゾーンをアジアのカラチ地域に設定します
configure system timezone Asia Katmandu	configure system timezone Asia Katmandu	タイムゾーンを中央アジアのカトマンズ地域に設定します
configure system timezone Asia Krasnoyarsk	configure system timezone Asia Krasnoyarsk	タイムゾーンをアジアのクラスノヤルスク地域に設定します
configure system timezone Asia Kuala_Lumpur	configure system timezone Asia Kuala_Lumpur	タイムゾーンを東南アジアのクアラルンプール地域に設定します
configure system timezone Asia Kuwait	configure system timezone Asia Kuwait	タイムゾーンを中近東のクウェート地域に設定します
configure system timezone Asia Magadan	configure system timezone Asia Magadan	タイムゾーンをアジアのマガダン地域に設定します
configure system timezone Asia Manila	configure system timezone Asia Manila	タイムゾーンを東南アジアのマニラ地域に設定します
configure system timezone Asia Muscat	configure system timezone Asia Muscat	タイムゾーンを中近東のマスカット地域に設定します
configure system timezone Asia Rangoon	configure system timezone Asia Rangoon	タイムゾーンをアジアのラングーン地域に設定します
configure system timezone Asia Seoul	configure system timezone Asia Seoul	タイムゾーンを極東のソウル地域に設定します
configure system timezone Asia Shanghai	configure system timezone Asia Shanghai	タイムゾーンを極東の上海地域に設定します
configure system timezone Asia Singapore	configure system timezone Asia Singapore	タイムゾーンを東南アジアのシンガポール地域に設定します

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
configure system timezone Asia Taipei	configure system timezone Asia Taipei	タイムゾーンを極東の台北地域に設定します
configure system timezone Asia Tehran	configure system timezone Asia Tehran	タイムゾーンを中近東のテヘラン地域に設定します
configure system timezone Asia Tokyo	configure system timezone Asia Tokyo	タイムゾーンを極東の東京地域に設定します
configure system timezone Asia Yakutsk	configure system timezone Asia Yakutsk	タイムゾーンをアジアのヤクーツク地域に設定します
configure system timezone Atlantic Azores	configure system timezone Atlantic Azores	タイムゾーンを大西洋のアゾレス地域に設定します
configure system timezone Australia Adelaide	configure system timezone Australia Adelaide	タイムゾーンをオーストラリアのアデレード地域に設定します
configure system timezone Australia Brisbane	configure system timezone Australia Brisbane	タイムゾーンをオーストラリアのブリズベーン地域に設定します
configure system timezone Australia Darwin	configure system timezone Australia Darwin	タイムゾーンをオーストラリアのダーウィン地域に設定します
configure system timezone Australia Hobart	configure system timezone Australia Hobart	タイムゾーンをオーストラリアのホーバート地域に設定します
configure system timezone Australia Melbourne	configure system timezone Australia Melbourne	タイムゾーンをオーストラリアのメルボルン地域に設定します
configure system timezone Australia Perth	configure system timezone Australia Perth	タイムゾーンをオーストラリアのパース地域に設定します

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
configure system timezone Europe Amsterdam	configure system timezone Europe Amsterdam	タイムゾーンをヨーロッパのアムステルダム地域に設定します
configure system timezone Europe Athens	configure system timezone Europe Athens	タイムゾーンをヨーロッパのアテネ地域に設定します
configure system timezone Europe Belgrade	configure system timezone Europe Belgrade	タイムゾーンをヨーロッパのベオグラード地域に設定します
configure system timezone Europe Berlin	configure system timezone Europe Berlin	タイムゾーンをヨーロッパのベルリン地域に設定します
configure system timezone Europe Brussels	configure system timezone Europe Brussels	タイムゾーンをヨーロッパのブリュッセル地域に設定します
configure system timezone Europe Bucharest	configure system timezone Europe Bucharest	タイムゾーンをヨーロッパのブカレスト地域に設定します
configure system timezone Europe Dublin	configure system timezone Europe Dublin	タイムゾーンをヨーロッパのダブリン地域に設定します
configure system timezone Europe Moscow	configure system timezone Europe Moscow	タイムゾーンをヨーロッパのモスクワ地域に設定します
configure system timezone Europe Paris	configure system timezone Europe Paris	タイムゾーンをヨーロッパのパリ地域に設定します
configure system timezone Pacific Auckland	configure system timezone Pacific Auckland	タイムゾーンを太平洋オークランド地域に設定します
configure system timezone Pacific Fiji	configure system timezone Pacific Fiji	タイムゾーンを太平洋フィジー地域に設定します
configure system timezone Pacific Guam	configure system timezone Pacific Guam	タイムゾーンを太平洋グアム地域に設定します

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
configure system timezone Pacific Honolulu	configure system timezone Pacific Honolulu	タイムゾーンを太平洋ホノルル地域に設定します
configure system timezone Pacific Kwajalein	configure system timezone Pacific Kwajalein	タイムゾーンを太平洋クウェジェリン環礁地域に設定します
configure system timezone Pacific Midway	configure system timezone Pacific Midway	タイムゾーンを太平洋ミッドウェー地域に設定します
configure system timezone US Alaska	configure system timezone US Alaska	タイムゾーンを米国アラスカ地域に設定します
configure system timezone US Arizona	configure system timezone US Arizona	タイムゾーンを米国アリゾナ地域に設定します
configure system timezone US Central	configure system timezone US Central	タイムゾーンを米国中部地域に設定します
configure system timezone US East-Indiana	configure system timezone US East-Indiana	タイムゾーンを米国東インディアナ地域に設定します
configure system timezone US Eastern	configure system timezone US Eastern	タイムゾーンを米国東部地域に設定します
configure system timezone US Hawaii	configure system timezone US Hawaii	タイムゾーンを米国ハワイ地域に設定します
configure system timezone US Mountain	configure system timezone US Mountain	タイムゾーンを米国山岳地域に設定します
configure system timezone US Pacific	configure system timezone US Pacific	タイムゾーンを米国太平洋岸地域に設定します
enable	enable	管理者コマンドを有効化します
exit	exit	セッションを終了します

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
ftpput	ftpput <URL> < ファイル名 > [--< アクティブモード >]	FTP プロトコルを介してファイルをアップロードします <URL>: 「ftp://< ユーザ名 >:< パスワード >@< ホスト名 >/< パス >」形式の STRING です < ファイル名 >: アップロード対象ファイルの名前とアップロード先のパスを FILENAME 形式で指定します < アクティブモード >: ACTIVETYPE の FTP アクティブモードです
help	help	CLI 構文の概要を表示します
history	history [制限]	現在のセッションのコマンドライン履歴を表示します
ping	ping [-c < エコーリクエスト数 >] [-i < 間隔 >] < 送信先 >	-c < エコーリクエスト数 >: 送信するエコーリクエスト (Echo Request) の数を UINT 形式で指定します ([5]) -i < 間隔 >: 各パケットの送信間隔を秒単位の UINT 形式で指定します < 送信先 >: ホスト名または IP アドレスを ADDRESS 形式で指定します
ping6	ping6 <IPv6 アドレス >	IPv6 ホストの ping に使用するコマンドです。

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
reboot	reboot [時間]	このコンピュータを再起動します (指定時間の経過後か即座に実行) < 時間 >: このコンピュータを再起動するまでの待ち時間を分単位の UINT 形式で指定します ([0])
resolve	resolve < 対象ホスト >	ネットワークの IP アドレスを解決します < 対象ホスト >: 解決対象のリモート IP アドレスを ADDRESS 形式で指定します
resolve6	resolve6 <IPv6 対象ホスト >	ネットワークの IPv6 IP アドレスを解決します < 対象ホスト >: 解決対象のリモート IPv6 アドレスを ADDRESS 形式で指定します
restart service database	restart service database	データベースデーモンを再起動します
restart service ftpd	restart service ftpd	FTP トラフィック検索デーモンを再起動します
restart service httpd	restart service httpd	HTTP トラフィック検索デーモンを再起動します
restart service iwss_daemons	restart service iwss_daemons	IWSVA サービスをすべて再起動します
restart service logtodb	restart service logtodb	ログをデータベースに保存するデーモンを再起動します
restart service maild	restart service maild	メール通知デーモンを再起動します

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
restart service metric_mgmt	restart service metric_mgmt	測定管理デーモンを再起動します
restart service ssh	restart service ssh	SSH デーモンを再起動します
restart service svcmonitor	restart service svcmonitor	監視デーモンを再起動します
restart service tmcmagent	restart service tmcmagent	Control Manager エージェントを再起動します
restart service tmsyslog	restart service tmsyslog	syslog デーモンを再起動します
restart service wccpd	restart service wccpd	WCCP デーモンを再起動します
restart service webui	restart service webui	tomcat デーモンを再起動します
show kernel iostat	show kernel iostat	デバイス、パーティション、NFS (ネットワークファイルシステム) の入出力統計、および CPU (中央処理装置) の統計を表示します
show kernel messages	show kernel messages	カーネルメッセージを表示します
show kernel modules	show kernel modules	カーネルにロードされたモジュールを表示します
show kernel parameters	show kernel parameters	実行中のカーネルのパラメータを表示します
show memory statistics	show memory statistics	メモリ統計を表示します
show module config all	show module config all	すべての設定ファイルを表示します

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
show module config database	show module config database	データベース設定ファイルを表示します
show module config file intscan	show module config file intscan	intscan 設定ファイルを表示します
show module config file IWSSPIJavascan	show module config file IWSSPIJavascan	IWSSPIJavascan 設定ファイルを表示します
show module config file IWSSPIProtocolFtp	show module config file IWSSPIProtocolFtp	IWSSPIProtocolFtp 設定ファイルを表示します
show module config file IWSSPIProtocolHttpProxy	show module config file IWSSPIProtocolHttpProxy	IWSSPIProtocolHttpProxy 設定ファイルを表示します
show module config file IWSSPIProtocolIcap	show module config file IWSSPIProtocolIcap	IWSSPIProtocolIcap 設定ファイルを表示します
show module config file IWSSPIScanVsapi	show module config file IWSSPIScanVsapi	IWSSPIScanVsapi 設定ファイルを表示します
show module config file IWSSPISigScan	show module config file IWSSPISigScan	IWSSPISigScan 設定ファイルを表示します
show module config file IWSSPIUrlFilter	show module config file IWSSPIUrlFilter	IWSSPIUrlFilter 設定ファイルを表示します
show module database backup	show module database backup	データベースのバックアップリストを表示します
show module database password	show module database password	データベースのパスワードを表示します
show module database settings	show module database settings	データベースの設定を表示します
show module database size	show module database size	IWSVA データベースのサイズを表示します

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
show module http x-forwarded-for	show module http x-forwarded-for	XFF HTTP ヘッダモジュールの設定を表示します
show module ldap groupcache interval	show module ldap groupcache interval	IWSVA LDAP ユーザグループメンバーシップ用キャッシュ間隔を表示します
show module ldap ipuser_cache	show module ldap ipuser_cache	IWSVA LDAP IP ユーザキャッシュの設定を表示します。クライアント IP 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。その期間中、IWSVA が認識するクライアント IP アドレスはユーザごとに一意でなければなりません。したがって、クライアントと IWSVA の間にプロキシサーバやソース NAT が存在する環境や DHCP が頻繁にクライアント IP アドレスを再び割り当てる環境では、このキャッシュは使用できません。
show module ldap ipuser_cache interval	show module ldap ipuser_cache interval	IWSVA LDAP IP ユーザ用キャッシュ間隔を表示します
show module ldap www-auth port	show module ldap www-auth port	認証ポートを表示します

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
show module log admin	show module log admin［ログ接尾辞]	管理ログファイルを表示します [ログ接尾辞] は「date.revision」の形式で入力します。 例 : 20120518.0001 管理ログを表示する場合の入力方法 show module log admin 20120518.0001
show module log ftp	show module log ftp ［ログ接尾辞]	FTP ログファイルを表示します [ログ接尾辞] は「date.revision」の形式で入力します 例 : 20120518.0001 FTP ログを表示する場合の入力方法 show module log ftp 20120518.0001
show module log http	show module log http［ログ接尾辞]	HTTP ログファイルを表示します [ログ接尾辞] は「date.revision」の形式で入力します 例 : 20120518.0001 FTP ログを表示する場合の入力方法 show module log ftp 20120518.0001

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
show module log mail	show module log mail [ログ接尾辞]	メールログファイルを表示します [ログ接尾辞] は「date.revision」の形式で入力します 例 : 20120518.0001 メールログを表示する場合の入力方法 show module log mail 20120518.0001
show module log postgres	show module log postgres	postgres ログを表示します
show module log tmudump	show module log tmudump	tmudump ログファイルを表示します
show module log update	show module log update [ログ接尾辞]	アップデートログファイルを表示します < ログ接尾辞 >:「[< ログ接尾辞 >]」の LOGSUFFIX 形式で指定します
show module metrics ftp	show module metrics ftp	IWSVA FTP パフォーマンス測定値を表示します
show module metrics http	show module metrics http	IWSVA HTTP パフォーマンス測定値を表示します
show module ntp schedule	show module ntp schedule	予約 NTP サーバ設定を表示します
show module webui port	show module webui port	Web サーバのポート設定を表示します

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
show network neighbour	show network neighbour [対象ホスト]	システム ARP テーブルを表示します < 対象ホスト >: ARP 先のリモート IP アドレスを ADDRESS 形式で指定します
show network bonding < ボンディング名 >	show network bonding < ボンディング名 >	ボンディング設定を表示します < ボンディング名 > がない場合、すべてのボンディング設定が表示されます。 < ボンディング名 > が指定されている場合、指定されたボンディング設定が表示されます。
show network bridge redirect ftpports	show network bridge redirect ftpports	FTP リダイレクションポート番号を表示します
show network bridge redirect httpports	show network bridge redirect httpports	HTTP リダイレクションポート番号を表示します
show network bridge redirect httpsports	show network bridge redirect httpsports	HTTPS リダイレクションポート番号を表示します
show network bridge stp	show network bridge stp	ブリッジの STP 設定を表示します
show network capture	show network capture [ファイル名]	取り込パケットを表示します < ファイル名 >: STRING 形式のファイル名です
show network connections <all (すべて) /listening (待機中) > <all (すべて) /tcp/udp>	show network connections <all (すべて) /listening (待機中) > <all (すべて) /tcp/udp>	システム接続またはデーモンを表示します。 たとえば、「show network connections listing」を実行すると実行中のデーモンが表示されます

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
show network conntrack	show network conntrack	状態が追跡されている接続を表示します
show network conntrack expect	show network conntrack expect	接続の状態を表示します
show network data interface	show network data interface インタフェース :eth0 IPv4 アドレス / マスク : 10.168.10.78/255.255.255.0 IPv6 アドレス / 接頭辞 : 2001:20::1/64 種類 : 静的	ネットワークアドレスを表示します
show network dns	show network dns	ネットワーク DNS サーバを表示します
show network ethernet	show network ethernet <Ethernet インタフェース名 >	Ethernet カード設定を表示します <Ethernet インタフェース名 >: IFNAME インタフェース名です
show network firewall filter	show firewall filter IPv4 ファイアウォールルールに IPv6 ファイアウォールルールが追加されました。	ファイアウォールフィルタを表示します
show network firewall nat	show firewall nat	ファイアウォール NAT を表示します
show network gateway ipv4/ipv6	show network gateway IPv4 ゲートウェイ : 10.168.10.254 IPv6 ゲートウェイ : 2001:10::1	IPv4 または IPv6 のネットワークゲートウェイを表示します

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
show network hostname	show network hostname	ネットワークホスト名を表示します
show network interfaces	show network interfaces	ネットワークインタフェース情報を表示します
show network interfaces status	show network interfaces status	ネットワークカードのリンクステータスを表示します
show network interfaces status once	show network interfaces status once	ネットワークカードのリンクステータスを 1 回表示します
show network interfaces statistic	show network interfaces statistic	ネットワークカードのリンクステータスを表示します
show network mgmt interface	show network mgmt interface 管理インタフェース : enable インタフェース :eth1 IPv4 アドレス / マスク : 10.168.20.78/255.255.255.0 IPv6 アドレス / 接頭辞 : 2001:10::1/64 種類 : 静的	ステータスおよびアドレスの情報を表示します
show network ping	show network ping	データおよび管理のステータスを表示します
show network portgroup	show network portgroup	現在のポートグループ設定を表示します

表 12-1. コマンドラインインタフェースのコマンド (続き)

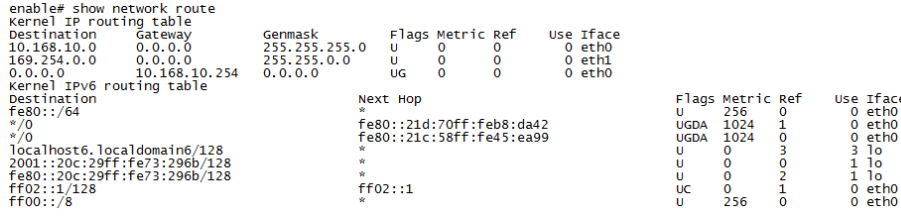
コマンド	構文	説明
show network route ipv4/ipv6	show network route ipv4/ipv6 (ルートは次のように表示されます) :	IPv4 または IPv6 のネットワークルーティングテーブルを表示します
		
show network sockets	show network sockets	オープンしているネットワークソケットに関する統計を表示します
show process library	show process library <pid>	ライブラリコール用トレーサです <pid>: pid を UINT 形式で指定します
show process stack	show process stack <pid>	実行プロセスのスタックトレースを表示します <pid>: pid を UINT 形式で指定します
show process [< 対象プロセス >]	show process [対象プロセス]	プロセス情報を表示します < 対象プロセス >:「[< オプションの名前または ID でワイルドカードが使用可能 >]」の STRING 形式で指定します
show process top	show process top	実行中のプロセスに関する情報を表示します

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
show process trace	show process trace <pid>	システムコールとシグナルをトレースします <pid>: pid を UINT 形式で指定します
show service ssh	show service ssh	SSH サービスのステータスを表示します
show storage partition	show storage partition [パーティション]	ファイルシステムの使用状況を読み取り可能な形式のみでレポートします < パーティション >:「[< オプションのパーティション >]」の STRING 形式で指定します
show storage space	show disk space [対象ディスク]	ファイル容量の使用状況を読み取り可能な形式のみでレポートします < 象ディスク >:「[< オプションのディレクトリまたはファイル名 >]」の STRING 形式で指定します
show storage statistic	show storage statistic	ディスク統計を表示します
show system configuration	show system configuration	IPv4 および IPv6 の実行設定の概要情報を表示します
show system configuration [-verbose]	show system configuration [-verbose]	実行設定の詳細な情報を表示します
show system date 以前のコマンド構文 : show date	show system date	現在の日時を表示します

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
show system ha	show system ha	クラスタ名、説明、HA モード、配信モード、クラスタ IP アドレス (IPv4/IPv6) などの HA 情報を表示します。「172.16.2.200/2001:10::1」のように設定する必要があります。例 : 重み付けされた優先順位の選択、メンバーリスト、役割、ローカルホスト、ホスト名、 IP アドレス、重み
show system hwmonitor	show system hwmonitor	ハードウェア監視情報を表示します。
show system hwmonitor interval	show system hwmonitor interval	現在のポーリング間隔の値を表示します
show system hwmonitor sel	show system hwmonitor sel	ハードウェアイベントログ情報を SNMP トラップ送信のベースとして表示します。
show system hwmonitor sensor	show system hwmonitor sensor	センサーで収集したすべての情報を表示します。
show system keyboard	show system keyboard	初期設定のキーボードテーブルを表示します
show system openfiles	show system openfiles [対象ファイル]	オープンしているファイルを表示します < 対象ファイル >:「[< オプションのディレクトリまたはファイル名 >]」の STRING 形式で指定します
show system timezone	show timezone	IWSVA のタイムゾーンを表示します

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
show system uptime	show system uptime	システムがこれまでに実行された時間の長さを表示します
show system version	show system version	IWSVA のバージョンを表示します
shutdown	shutdown [時間]	このコンピュータをシャットダウンします (指定時間の経過後か即座に実行) < 時間 >: このコンピュータをシャットダウンするまでの待ち時間を分単位の UINT 形式で指定します ([0])
start service database	start service database	データベースデーモンを起動します
start service ftpd	start service ftpd	FTP トラフィック検索デーモンを起動します
start service httpd	start service httpd	HTTP トラフィック検索デーモンを起動します
start service logtodb	start service logtodb	ログをデータベースに保存するデーモンを起動します
start service maild	start service maild start	メール通知デーモンを起動します
start service metric_mgmt	start service metric_mgmt	測定管理デーモンを起動します
start service ssh	start service ssh	sshd デーモンを有効化します
start service svcmonitor	start service svcmonitor	監視デーモンを起動します
start service tmcmagent	start service tmcmagent	Control Manager エージェントを起動します
start service tmsyslog	start service tmsyslog	syslog デーモンを起動します

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
start service wccpd	start service wccpd	WCCP デーモンを起動します
start service webui	start service webui	tomcat デーモンを起動します
start shell	start shell	管理者シェルにアクセスします
start task database backup	start task database backup	データベースをバックアップします
start task database reindex	start task database reindex	IWSVA データベースの索引を再作成します
start task database restore	start task database restore [ファイル名]	バックアップからデータベースを復元します
start task database truncate	start task database truncate <DATE_FIELD>	不要な IWSVA データベースを切り捨てます
start task database vacuum	start task database vacuum	不要な IWSVA データベースをクリアします
注意： 不要なデータベースが完全にクリアされなかった場合は、`/var/iwss/postgres/pgdata/` にある設定ファイル `postgresql.conf` の「max_fsm_pages」パラメータを調整します。		
start task capture interface	start task capture interface < インタフェース > [-h < ホスト >] [-p < ポート >]	ネットワークインタフェースのトラフィックを取り込みます < インタフェース >: パケット取り込み対象のインタフェースです -h: IP アドレスによるホスト IP_ADDR フィルタです -p: ポート番号によるポート UINT フィルタです

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
start task monitor ftp	start task monitor ftp	FTP ログを監視します
start task monitor http	start task monitor http	HTTP ログを監視します
stop process	stop process <pid>	実行中のプロセスを停止します <pid>: pid を UINT 形式で指定します
stop process core	stop process core <pid>	実行中のプロセスを停止しコアファイルを生成します <pid>: pid を UINT 形式で指定します
stop service database	stop service database	データベースデーモンを停止します
stop service ftpd	stop service ftpd	FTP トラフィックデーモンを停止します
stop service httpd	stop service httpd	HTTP トラフィックデーモンを停止します
stop service logtodb	stop service logtodb	ログをデータベースに保存するデーモンを停止します
stop service maild	stop service maild	メール通知デーモンを停止します
stop service metric_mgmt	stop service metric_mgmt	測定管理デーモンを停止します
stop service ssh	stop service ssh	sshd デーモンを無効化します
stop service svcmonitor	stop service svcmonitor	監視デーモンを停止します
stop service tmcmagent	service stop tmcmagent	Control Manager エージェントを停止します
stop service tmsyslog	stop service tmsyslog	syslog デーモンを停止します

表 12-1. コマンドラインインタフェースのコマンド (続き)

コマンド	構文	説明
stop service wccpd	stop service wccpd	WCCP デーモンを停止します
stop service webui	stop service webui	tomcat デーモンを停止します
traceroute	traceroute [-h < ホップ数 >] < 対象ホスト > [-n]	TraceRoute -h < ホップ数 >: 最大ホップ数を UINT 形式で指定します < 対象ホスト >: トレース対象のリモートシステムを ADDRESS 形式で指定します -n: ホスト名を解決しない場合に DASHN 形式で指定します
traceroute6	traceroute6 <IPv6 アドレス >	TraceRoute6 -h < ホップ数 >: 最大ホップ数を UINT 形式で指定します < 対象ホスト >: トレース対象のリモート IPv6 ホストを ADDRESS 形式で指定します -n: ホスト名を解決しない場合に DASHN 形式で指定します
wget	wget <URL> < パス >	HTTP/FTP プロトコルを介してファイルをダウンロードします <URL>: 「http://< ユーザ名 >:< パスワード >@< ホスト名 >/< パス >」形式の STRING で指定します < パス >: ファイルのダウンロード先となるローカルパスを FILENAME 形式で指定します

第 13 章

レポート、ログおよび通知

本章では、管理者が Trend Micro InterScan Web Security Virtual Appliance（以下、IWSVA）のレポート、ログ、および通知により、ゲートウェイのセキュリティに関する情報をタイムリーに取得する方法について説明します。

本章で説明する内容には、次の項目が含まれます。

レポートについて

IWSVA では、ウイルスおよび不正コードの検出、ブロックされたファイル、およびアクセスされた URL に関するレポートを生成できます。IWSVA のプログラムイベントに関するこの情報を使用して、プログラムの設定を最適化し、組織のセキュリティポリシーを微調整できます。

レポートは設定およびカスタマイズできます。たとえば、IWSVA では、すべてまたは特定のユーザ、ユーザグループ、またはデバイスグループに対するレポートを必要に応じてリアルタイムに、またはスケジュールに従って生成できます。

選択したレポート情報を必要とする人と共有できるように、IWSVA では、生成されたレポートをメールに添付して送信できます。

IWSVA ユーザアカウントでは、アカウントに関連付けられた役割に基づいてレポートを生成できます。つまり、役割で IP アドレス範囲に関連するデータへのアクセスが許可されている場合、そのユーザアカウントでは、その IP アドレスのみに関するレポートを生成できます。

レポート情報

目的のレポート名と、そのレポートの短い説明を入力します。[使用可] または [使用不可] のいずれかを選択して、レポートを有効にします。

レポート設定

レポートテンプレートを生成する際は、次の情報を指定する必要があります。

- 特定のスケジュールに基づいてレポートを生成するかどうか
- 特定の期間に基づいてレポートを生成するかどうか
- レポートを生成する時間 (業務時間、業務時間外、またはカスタマイズした期間フィルタ)
- レポートを生成するデバイスグループ
- 出力の種類 (PDF、HTML、または CSV ファイル)
- 保存して保持するレポート数

注意 : [レポートの設定] では、時間は次のように指定されます。
過去 1 日間 : その日の 00:00 から前に 1 日間

このレポートをメールで送信

すべてのレポートで、

[このレポートをメールで送信] を選択し、次の設定を行います。

- 「送信者」のメールアドレスを入力します。
- 「受信者」のメールアドレスを入力して、レポートの生成後、特定の個人またはメール配信リストにそのレポートのコピーを送信します。
- 目的のメッセージを入力します。
- レポートを添付ファイルとして送信することを「有効」にします。
- メッセージ配信に失敗した場合の通知の選択内容を示します。

作成対象 (ユーザおよびグループ)

レポートを生成する対象のユーザを選択します。次のオプションがあります。

- **すべてのユーザ** : IWSVA 経由でインターネットにアクセスしているすべてのユーザ
- **指定するユーザ** : 特定の IP アドレス、ホスト名、または LDAP ディレクトリエントリを持つクライアント
- **すべてのグループ** : LDAP ディレクトリ内のすべてのグループ。IP アドレスまたはホスト名を指定する場合は、すべてのグループは、すべてのユーザと同等です。
- **指定するグループ** : 特定の LDAP グループまたは IP アドレスの範囲のいずれか

特定のユーザまたはグループに対してレポートを生成する場合、ユーザの選択方法は [管理] → [一般設定] → [ユーザの識別 | ユーザの識別] で設定した方法によって決まります。ユーザの識別の詳細については、160 ページの「ユーザ識別方法の設定」を参照してください。

レポートの種類

IWSVA では、次のカテゴリのレポートを示す棒グラフまたは表を生成できます。

- インターネットセキュリティ — 次のインターネットセキュリティの検出上位 n 件を示したレポートが生成されます。
  - 不正プログラム / スパイウェア検出
  - ボットネット検出
  - ドキュメントセキュリティホール APT 検出
  - カスタム保護 APT ブロック

  - C&C コンタクトアラート件数 (日付別)
  - C&C アドレス
  - C&C コンタクトアラートで検出されたユーザ / ホスト
  - C&C コンタクトアラートで検出されたグループ
  - 最もブロックの多い不正サイト
  - 最もブロックの多いユーザ (不正プログラム / スパイウェア別)
  - 最もブロックの多いユーザ (不正サイト別)
  - 最もブロックの多いグループ (不正プログラム / スパイウェア別)
  - 最もブロックの多いグループ (不正サイト別)
  - ユーザ (ボットネット検出別)
  - HTTP 不正プログラム検索ポリシーに対する最も多い違反
  - ブロックされた不正サイト (日付別)
  - 不正プログラム / スパイウェア検出 (日付別)
  - 不正プログラム / スパイウェア検出傾向
- インターネットアクセス — 次のインターネットアクセスの検出上位 n 件を示したレポートが生成されます。
  - 最もアクセスの多いアプリケーション
  - 最もアクセスの多い URL カテゴリ
  - 最もアクセスの多いサイト
  - ユーザ (要求別)
  - グループ (要求別)
  - URL カテゴリ (参照時間別)
  - アクセスサイト (参照時間別)
  - ユーザ (参照時間別)
  - アクセス数 (時間別)
- 帯域幅 — 次の帯域幅の検出上位 n 件を示したレポートが生成されます。
  - URL カテゴリ (帯域幅別)
  - アプリケーション (帯域幅別)
  - ユーザ (帯域幅別)
  - グループ (帯域幅別)
  - サイト (帯域幅別)

    - 合計トラフィック (日付別)
- ポリシー施行 — 次のポリシー施行の検出上位 n 件を示したレポートが生成されます。
    - 最もブロックの多い URL カテゴリ
    - 最もブロックの多いアプリケーション
    - 最も施行の多いユーザ
    - 最も施行の多いグループ
    - 最もブロックの多いサイト
    - ユーザ (HTTP 検査別)
    - URL フィルタポリシーに対する最も多い違反
    - アプリケーション制御ポリシーに対する最も多い違反
    - アクセス割り当て管理ポリシーに対する最も多い違反
    - アプレット /ActiveX 対策ポリシーに対する最も多い違反
    - HTTP 検査ポリシーに対する最も多い違反
- データセキュリティ — 次のデータセキュリティの検出上位 n 件を示したレポートが生成されます。
    - 最もブロックの多い DLP テンプレート (要求別)
    - 最もブロックの多いユーザ
    - 最もブロックの多いグループ
    - 情報漏えい対策ポリシーに対する最も多い違反
- カスタムレポート — レポート対象の定義済みの [お気に入りログ] が含まれます。詳細については、329 ページの「レポートの種類」を参照してください。

レポートの生成

IPv4 の動作と同様に、特定の IPv6 ユーザまたは IPv6 ユーザグループ別にレポートを生成できます。選択したユーザまたはユーザグループのページは、IPv6 アドレスまたは IPv6 アドレス範囲もサポートします。

レポートは、IPv4 ユーザと IPv6 ユーザのどちらの場合も、レイアウト問題が生じることなく、CSV 形式、PDF 形式、または HTML 形式で生成できます。IPv4 の動作と同様に、ユーザ関連のレポートを生成するとき、レポート内ですべての IPv6 ユーザを使用できます。

レポートの設定

IWSVA では、インターネットにアクセスしているすべてまたは一部のクライアントに対してレポートを生成できます。生成したレポートは、PDF 形式、HTML 形式、または CSV 形式で保存できます。

レポートを設定するには

1. 管理コンソールで [レポート] をクリックします。
2. 新しいレポートテンプレートを追加するには、[追加] をクリックします。
3. レポートテンプレートの名前と説明を入力します。テンプレートを有効にする準備ができたら、[はい] をクリックして有効にします。
4. [レポートの設定] でレポートのスケジュールを選択し ([今回のみ]、[今後 1 回のみ]、[毎日]、[毎週]、または [毎月] のいずれか)、次に [レポート期間] を選択します。特定の時間帯にレポートを生成するには [カスタム時間帯] をクリックし、[開始] および [終了] の日付を選択します。
5. 予約期間フィルタ ([常時]、[業務時間]、[業務時間外]、または [管理] → [一般設定] → [予約期間] でカスタマイズした期間フィルタ) を選択します。
6. デバイスグループを選択します。

注意： デバイスグループを追加するには、[管理] → [一般設定] → [集中管理ログ / レポート] を選択し、[デバイスグループ管理] の下で [追加] をクリックします。初期設定では、すべてのデバイスが同じグループに追加されます。

---

7. レポートの出力を選択します。
8. メールの受信者、件名、およびメッセージをオプションとともに設定します。
9. [作成対象] で、レポートを生成する対象として [すべてのユーザ]、[特定のユーザ / グループ] のいずれかを選択します。[指定するユーザ]、[すべてのグループ]、または [指定するグループ] の選択時には IPv6 アドレスも定義できます。指定するユーザまたはグループに対するレポートの詳細については、「特定のユーザまたはグループを選択するには」を参照してください。
10. [レポートの種類] でレポートの種類を選択し、目的のレポートのレコード番号を入力します。

注意： IWSVA では複数のレポートパラメータを 1 つのレポートにまとめ、レポートパラメータごとに記載があります。

---

11. メニューから、グラフの種類 (棒グラフ、表グラフ、または両方) を選択します。
12. [レポートの保存] をクリックします。

次の表は、レポートを構成するパラメータの情報を示しています。

表 13-1. レポートタイプによって異なる使用可能なレポートパラメータ

作成対象	含まれるレポートパラメータ
すべてのユーザ	リストに含まれる「個別ユーザレポート」以外のすべてのレポートパラメータを含みます。
特定のユーザ / グループ	「ユーザ別レポート」のパラメータのみを含みます。
* Web レピュテーションの場合（ファーミング対策、フィッシング対策など)、ブロックされたサイトはこれらのレポートに表示されます。ただし、ブロックされたサイトを検索する場合、情報が記載されているのは「最もブロックの多い不正サイト上位 N 件」のみです。	

特定のユーザまたはグループを選択するには

1. 管理コンソールで [レポート] をクリックします。
2. [作成対象] で [特定のユーザ / グループ] を選択し、[選択] をクリックします。
   [管理] → [一般設定] → [ユーザの識別｜ユーザの識別] で設定したユーザの識別方法に従って、[ユーザの選択] または [グループの選択] ポップアップ画面が表示されます。
3. IP ホスト名またはアドレス範囲を入力するか、「ユーザ / グループ名認証」による識別方法を使用している場合は LDAP ディレクトリでグループ名を検索します。
4. 特定のユーザまたはグループを入力して、[検索] をクリックします。
5. [追加] をクリックします。
6. レポートに含めるグループを追加したら、[保存] をクリックします。

レポートの種類

それぞれのレポートパラメータについて、レポートに出力するレコード数を指定できます。それぞれのレポートの種類について、初期設定には、上位のユーザ、URL、カテゴリなどのレコードが含まれています。99 などの大きな数値を指定すると、レポートサイズと作成時間が影響を受けます。

[上位カテゴリ (重み付け)] というレポートパラメータは、ブロックまたは監視された URL カテゴリも含めて、URL カテゴリに関する情報を提供します。URL カテゴリおよびアクセスされた URL ごとの要求数も示します。この情報は、各種のインターネットグループに対して、どの URL カテゴリをブロックまたは監視する必要があるかを判断する上で参考になります。

レポートパラメータには、次の条件が当てはまります。

- ユーザはアドレス、ユーザ名、またはホスト名です。
- HTTP については、URL アドレスは、トップレベルドメインのみでなく、アドレス全体です。HTTPS については、URL アドレスは、トップレベルドメインのみです。
- 内容は、ユーザ指定の最も頻繁にアクセスされた URL ごとにリストされ、アクセス回数順に表示されます。

管理者はこのアクセスを確認して、要求を許可するかどうかを決定できます。

カスタムレポートでは、カスタマイズしたレポートに保存済みのログまたは「お気に入り」のログを含めることができます。カスタムレポートには、レポートテンプレートの時間範囲および指定されたユーザが使用されます。その他の設定は、お気に入りログの設定と同じです。

レポートの予約

予約レポートを今回のみ、今後 1 回のみ、毎日、毎週、または毎月生成するように IWSVA を設定できます。

予約レポートを設定するには

1. 管理コンソールの [レポート] で新しいレポートを作成します。
2. [追加] をクリックするか、レポート名をクリックして編集します。
3. 新しいレポートの名前を入力します。[レポートの設定] で、予約レポートを生成する時間および日付を設定します。
4. [メール] および添付ファイルの形式を選択して、IWSVA が生成したレポートを添付ファイルとして送信する先のメールアドレスを入力します。また、[送信者] フィールドと [件名] フィールドにも入力する必要があります。複数のメールアドレスはカンマ (,) で区切ります。

注意： SMTP サーバに関する設定は、[通知] → [通知先の設定 ...] で行います。

5. [保存] をクリックします。

作成された予約レポートを削除するには

1. 管理コンソールで [レポート] をクリックします。
2. 削除するレポートテンプレートを選択して [削除] をクリックします。

保存されている予約レポート

予約レポートが生成されると、IWSVA は指定されている受信者にレポートを送信し、コピーをデータベースに保存します。保存したレポートを表示またはダウンロードするには、[レポート] の [保存されているレポート] タブをクリックします。IWSVA がデータベースに保存する、保存されているレポートの数を設定できます。

ログについて

注意 : [ログ分析] では、時間は次のように指定されます。
過去 1 時間 : 現在の時刻から、その時刻の 0 分まで
過去 1 日間 : 現在の時刻から、その時刻の 0 分から前に 23 時間

ログはログのタイプによってカテゴリ分類され、次のようにマップおよびグループ化されます。

- アプリケーション帯域幅
- ポリシー施行
- インターネットアクセス
- インターネットセキュリティ
- データセキュリティ
- アクセス管理

アプリケーション帯域幅

それぞれのログの表示で次のいずれかのフィルタを利用できます。

- 受信トラフィック
- 送信トラフィック
- すべてのトラフィック
- ユーザ名
- デバイスグループ
- クライアント IP
- アプリ ID
- ポリシー名

時間範囲のフィルタを使用してソートを続行します。[今日]、[過去 1 時間]、[過去 12 時間]、[過去 1 日間]、[過去 7 日間]、または指定した時間範囲を選択できます。表示するインスタンス数を上位 5 件～ 20 件の範囲で設定します。結果の出力形式を棒グラフ、線グラフ、円グラフなどから選択します。

ポリシー施行

それぞれのログの表示で次のいずれかのフィルタを利用できます。

- 処理
- メッセージの種類
- デバイスグループ
- クライアント IP
- チャネル
- アプリ ID
- ポリシー名
- ユーザ名
- ルール名
- URL カテゴリ

時間範囲のフィルタを使用してソートを続行します。[今日]、[過去 1 時間]、[過去 12 時間]、[過去 1 日間]、[過去 7 日間]、または指定した時間範囲を選択できます。表示するインスタンス数を上位 5 件～ 20 件の範囲で設定します。結果の出力形式を棒グラフ、線グラフ、円グラフなどから選択します。

インターネットアクセス

それぞれのログの表示で次のいずれかのフィルタを利用できます。

- ドメイン
- デバイスグループ
- クライアント IP
- ユーザ名
- URL カテゴリ

時間範囲のフィルタを使用してソートを続行します。[今日]、[過去 1 時間]、[過去 12 時間]、[過去 1 日間]、[過去 7 日間]、または指定した時間範囲を選択できます。表示するインスタンス数を上位 5 件～ 20 件の範囲で設定します。結果の出力形式を棒グラフ、線グラフ、円グラフなどから選択します。

インターネットセキュリティ

それぞれのログの表示で次のいずれかのフィルタを利用できます。

- 処理
- メッセージの種類
- 不正プログラム名
- デバイスグループ
- クライアント IP
- チャネル
- ポリシー名
- ユーザ名

時間範囲のフィルタを使用してソートを続行します。[今日]、[過去 1 時間]、[過去 12 時間]、[過去 1 日間]、[過去 7 日間]、または指定した時間範囲を選択できます。表示するインスタンス数を上位 5 件～ 20 件の範囲で設定します。結果の出力形式を棒グラフ、線グラフ、円グラフなどから選択します。

データセキュリティ

それぞれのログの表示で次のいずれかのフィルタを利用できます。

- 処理
- デバイスグループ
- クライアント IP
- チャネル
- ポリシー名
- ユーザ名
- ルール名

時間範囲のフィルタを使用してソートを続行します。[今日]、[過去 1 時間]、[過去 12 時間]、[過去 1 日間]、[過去 7 日間]、または指定した時間範囲を選択できます。表示するインスタンス数を上位 5 件～ 20 件の範囲で設定します。結果の出力形式を棒グラフ、線グラフ、円グラフなどから選択します。

アクセス管理

それぞれのログの表示で次のいずれかのフィルタを利用できます。

- 処理
- メッセージの種類
- デバイスグループ
- クライアント IP
- チャネル
- ポリシー名
- ユーザ名

時間範囲のフィルタを使用してソートを続行します。[今日]、[過去 1 時間]、[過去 12 時間]、[過去 1 日間]、[過去 7 日間]、または指定した時間範囲を選択できます。表示するインスタンス数を上位 5 件～ 20 件の範囲で設定します。結果の出力形式を棒グラフ、線グラフ、円グラフなどから選択します。

詳細なログ設定

ログ設定の詳細は、IWSVA Web コンソールの [ログ] → [ログ設定] で確認できます (詳細については、335 ページの「ログの設定」を参照)。

ログのクエリおよび表示

IWSVA Web コンソールには、ログファイルにクエリを実行するためのツールが用意されています。

- **ログ検索** — IWSVA には個々のファセットの検索ボックスが用意されています。これには、検索用語を強調表示して、可能性のある結果を表示する「オートコンプリート」機能も含まれます。
- **タイムゾーン** — すべてのログは、クライアントに元々設定されている同じタイムゾーンで表示されます。

- **円グラフ** — 円グラフに「その他」のカテゴリが含まれるようになりました。たとえば、上位 5 件の不正プログラムインスタンスを表示する場合、各不正プログラムにはグラフのくさび状の部分が 1 つずつ割り当てられ、上位 5 件以外のすべての不正プログラムはまとめて「その他」のくさびに表示されます。不正プログラムインスタンスが 5 件のみの場合、「その他」のくさびは表示されません。
- **お気に入りとして保存** — よく使用するログ設定を [お気に入りのログ分析] に保存できます。「お気に入り」のログは、[ログ] → [お気に入り] にあります。

注意： 折れ線グラフと円グラフにはいずれも「ドリルダウン」機能があり、グラフ内で詳細を知りたいと思う箇所をクリックすると、その詳細情報が表示されます。

ログの設定

[ログ設定] 画面から、次の内容を設定できます。

- ログの保存期間や保存する最大ログサイズなどのグローバルログ設定。
- ポリシー施行、インターネットアクセス、インターネットセキュリティ、データセキュリティ、およびアクセス管理フィルタを使用するユーザ名とドメインの両方を基準としたグローバルログフィルタ、および帯域幅フィルタを使用するユーザ名を基準としたグローバルログフィルタ。
- 匿名ログを有効または無効にできるかどうか。
- ログのタイプと優先度に基づいて追加のログストレージに使用する Syslog サーバ。
- ローカルまたは外部の場所のマウント、以前のログ (少なくとも過去 45 日間のログ) のマウントされた場所へのアンロード、およびその場所からのログのインポート。

グローバルログを設定するには

1. [ログ] → [ログ設定] に移動します。
   [ログ設定] 画面が表示されます。
2. [グローバルログ設定] で以下を設定します。
   a. **次のログを保存**: 削除するまでログを保持する日数を入力します。

      注意： この値を 62 日より大きく設定すると、蓄積されたデータが大きくなりすぎてパフォーマンスに影響を及ぼす可能性があります。

b. **最大ログディスクサイズ**: 保存するログデータの最大ファイルサイズを設定します。ログデータが指定されたサイズを超えると、最も古いログが最初に削除されます。

c. **マウントデバイス**: ログを保存するローカルまたは外部の場所のパスを入力して、[マウント] をクリックします。

d. **ログのアンロード**: マウントされた場所にログを保存する場合は、このオプションをオンにします。

e. **ログのインポート**: マウントされた場所に保存されている履歴ログを分析のためにインポートして使用する場合は、このオプションをオンにします。

f. [保存] をクリックします。

3. [グローバルログフィルタ] で以下を設定します。

a. ドロップダウンリストからポリシーとユーザを選択して、表示されるテキストフィールドにフィルタ名を入力します。

b. + アイコンをクリックします。

c. [保存] をクリックします。

4. すべてのログを Syslog サーバに転送する場合は、[Syslog サーバ] で次の手順を実行します。

a. [追加] をクリックします。

[Syslog 設定] の [サーバの追加] 画面が表示されます。

b. [Syslog を有効にする] を選択します。

c. Syslog の転送先のサーバの IP アドレスとポート番号を入力します。

d. 保存するログのタイプまたは Syslog 優先度レベルを選択します。

e. [保存] をクリックして設定を保存し、[ログ設定] 画面に戻ります。

f. Syslog サーバを選択します。

5. [保存] をクリックします。

グローバルログフィルタ

ログから特定のデータを省略したい場合、グローバルログフィルタを使用します。たとえば、John Smith というユーザのインターネットアクセスログや、www.google.com にアクセスしたユーザの帯域幅使用率をログに記録する必要がない場合は、このフィルタを使用します。

匿名ログ

欧州の一部の国では、ユーザ名をログに記録することを禁じる法律があります。この機能を有効にすると、ログ内のユーザ名は、実際のユーザ名の代わりに MD5 値で記録されます。

ログのアンロードと取得

IWSVA にはログストレージ制限があります。古いログを削除したくない場合は、それらのログをデバイスにアンロードして永続的に保存できます。将来ログを分析する場合は、これらのログをデバイスから取得して IWSVA で復元できます。

ログおよびレポートデータの CSV ファイルへのエクスポート

IWSVA では、ログまたはリアルタイムレポートを表示したときに、CSV 形式でファイルにデータを出力できます。出力した CSV 形式のファイルは、他のアプリケーションで表示および分析できます。表のアイコンをクリックし、[CSV ファイルのエクスポート] をクリックして、IWSVA サーバからファイルをダウンロードします。

PDF 形式でのレポートデータの出力

CSV 出力機能に加えて、IWSVA ではレポートデータ（最大 1000 行までのログ) を PDF 形式で出力することもできます。PDF 形式のデータは PDF リーダーアプリケーションを使用してあらゆるプラットフォームで表示できます。IWSVA サーバからファイルをダウンロードするには、[PDF] をクリックして、画面上のプロンプトに従ってください。

syslog 設定

IWSVA は syslog サーバをサポートしているため、外部の syslog サーバにログを送信できます。syslog サーバは最大 4 つまで設定でき、ログの種類や優先度を指定して、各 syslog サーバに送信できます。

syslog サーバを設定するには

1. 管理コンソールから [ログ] → [ログ設定] → [Syslog サーバ] の順に選択します。
2. [追加] をクリックします。
3. [Syslog サーバの設定] で次の設定を行います。

a. [Syslog を有効にする] を選択して、IWSVA でこの syslog サーバにログを送信できるようにします。

b. [サーバ名 /IP アドレス] を指定します。IWSVA は、IPv4 と IPv6 の両方のホストへの Syslog メッセージの送信をサポートしています。Web UI は、IPv4 と同様に、IPv6 のホスト名とアドレスの両方を受け入れることができます。

c. [UDP ポート番号] を指定します (初期設定は 514)。

4. [次のログを保存する] で、送信するログを指定します。ログの種類別または syslog 優先度別に、syslog サーバにイベントを送信するように選択できます。
   - [ログタイプ別] をクリックしてログの種類を選択します。または、
   - [Syslog 優先度別] をクリックしてレベルを選択します。
5. [保存] をクリックします。

通知について

通知は、検索、ブロック、アラート、およびプログラムアップデートイベントに対して発行できます。通知には、管理者への通知とユーザへの通知の 2 種類があります。通知は、次に示すように、メインメニューの [通知] で設定できます。

- **管理者への通知**により、多様な情報が提供されます。それらの情報には、HTTP/HTTPS 検索、HTTP/HTTPS のファイルタイプによるブロック、FTP のファイルタイプによるブロック、FTP 検索、しきい値アラート、制限されたトンネルトラフィック、高可用性イベント、パターンファイルや検索エンジンのアップデートなどがあります。IWSVA は、管理者への通知を [通知先の設定 ...] 画面で設定したアドレスにメールで送信します。
- **ユーザへの通知**では、HTTPS アクセスエラー、HTTPS 証明書に関する警告、HTTP/HTTPS 検索、HTTP/HTTPS ファイルブロック、FTP 検索、URL ブロック、FTP ファイルタイプによるブロック、および高可用性イベントに関する情報が提供されます。IWSVA は、クライアントが閲覧またはダウンロードしようとしている禁止 Web ページやファイルの代わりに、ユーザへの通知をクライアントのブラウザまたは FTP クライアントに表示します。

管理者への通知およびユーザへの通知の両方に表示されるメッセージは設定可能です。「トークン」または変数を含めて、イベント情報に関する通知メッセージをカスタマイズできます。さらに、ユーザへの通知では HTML タグがサポートされているため、メッセージの外観をカスタマイズしたり、イントラネット上でホストされているセキュリティポリシードキュメントなど、他のリソースへのリンクを提供したりできます。

注意： IPv4 と同様に、次を含むすべてのトークンを IPv6 アクセスに適用できます。
%N — ユーザ名
%c —「Error! Hyperlink reference not valid」の後ろの IP アドレス : ポート（HTTPS 復号化用）。IPv6 の場合は、https:// [IPv6 アドレス] : ポートになります。IPv4 は、https://IPv4 アドレス : ポートを維持します。

通知先の設定

IWSVA は、管理者への通知を指定されたメールアドレスに送信します。管理者は IWSVA をインストールしてセットアッププログラムを実行する際にメールの設定を入力します。ただし、メールの設定はインストール後に Web コンソールの [通知] → [通知先の設定 ...] 画面でも変更できます。

管理者への通知用のメール設定を行うには

1. 管理コンソールで [通知] をクリックします。
2. [通知] 画面で、[通知先の設定 ...] をクリックします。
3. 通知の送信先メールアドレス、送信者のメールアドレス、DLP 通知の送信先アドレス、SMTP サーバ、SMTP サーバポート、およびメールキューを確認する間隔を入力します。IWSVA は、IPv4 ホストと IPv6 ホストへの通知の送信をサポートしています。Web UI は、IPv4 と同様に、ホスト名と IPv6 アドレスの両方を受け入れることができます。
4. メールサーバで ESMTP が必要な場合は、IWSVA で EHLO コマンドを使用して SMTP セッションを初期化できるように、[EHLO（Extended Hello) コマンドを使用する] チェックボックスをオンにします。
5. [保存] をクリックします。

通知の変数

より意味のある通知にするために、IWSVA では通知内で情報のプレースホルダとして変数を使用できます。イベントが発生すると、IWSVA は変数を特定の情報と動的に置き換え、その特定のイベントに関する詳細な情報を提供します。

たとえば、次のような一般的な通知を作成できます。

HTTP トラフィックでウイルスが検出されました。

この通知では、問題が発生していることはわかりますが、詳細は提供されません。代わりに、変数を使用して次のような通知を設定できます。

%Y に、IWSVA がファイル %F でセキュリティリスク %v を検出しました。%N が %U からファイルをダウンロードしようとしました。

この通知は、たとえば次のようになります。

5/28/08 6:31:56 PM に、IWSVA がファイル EXT_JS.JS でセキュリティリスク JS_TEST_VIRUS を検出しました。10.2.203.130 が http://10.2.203.130/TESTDATA/virus/NonCleanable/EXT_JS.JS からファイルをダウンロードしようとしました。

この情報があれば、管理者はクライアントに連絡して、さらに多くのセキュリティ情報を提供できます。この例の通知では、%Y、%v、%F、%N、および %U の 5 つの変数が使用されています。

次の表は、通知メッセージおよび画面で使用できる変数のリストを示しています。

表 13-2. 変数の説明

変数	変数の意味	変数の使用方法
HTTPS アクセス拒否および HTTPS 証明書エラー		
%o	IWSVA ホスト名	イベントが発生した IWSVA ホスト名
%u	URL/URI	
%c	「https://」の後の IP アドレス : ポート	%c の使用例については、初期設定のメッセージを参照してください
$$DETAILS	証明書エラーの理由 / アクセス拒否の理由の詳細	
FTP 検索および HTTP/HTTPS 検索		
%A	実行された処理	IWSVA によって実行された処理
%F	ファイル名	anti_virus_test_file.htm など、リスクが検出されたファイルの名前
%H	IWSVA ホスト名	イベントが発生した IWSVA ホスト名
%L	ファイル名および理由の詳細	
%M	移動先	ファイルが移動された隔離ディレクトリの場所
%N	ユーザ名	
%R	転送方向	
%U	URL/URI	

表 13-2. 変数の説明 (続き)

変数	変数の意味	変数の使用方法
%V	不正プログラム名 (ウイルス、トロイの木馬、またはボット名)	検出されたリスクの名前
%X	理由 / ブロックタイプ	
%Y	日付と時刻	イベントが発生した日時
アプリケーション制御による HTTP/HTTPS アクセス拒否		
%N	ユーザ名	
%A	処理	
%P	パスおよびファイル名	
%C	カテゴリ	
%Z	ポリシー名	
%Y	日付と時刻	
%H	IWSVA ホスト名	
情報漏えい対策		
%T	テンプレート名	
%U	URL/URI	
%Y	日付と時刻	イベントが発生した日時
%A	実行された処理	
%N	ユーザ名	
%Z	ポリシー名	
%H	IWSVA ホスト名	
C&C コールバック試行検出		
%Z	ポリシー名	
%N	ユーザ名	
%U	URL/URI	
%A	処理	
%K	リスクレベル	
FTP ファイルタイプブロックおよび HTTP/HTTPS ファイルタイプブロック		

表 13-2. 変数の説明 (続き)

変数	変数の意味	変数の使用方法
%U	URL/URI	
次の変数は、管理者へのメッセージまたはユーザへの通知メッセージにのみ使用されます。		
%F	ファイル名	
%A	実行された処理	
%H	IWSVA ホスト名	
%R	転送方向	
%X	理由 / ブロックタイプ	
%Y	日付と時刻	
%N	ユーザ名	
%V	ウイルス、トロイの木馬、またはボット名	
アプレット /ActiveX 検索		
%D	検索されるプロトコル	
%H	IWSVA ホスト名	
%N	ユーザ名	
%U	URL/URI	
%W	新しい証明書の情報	
%X	[理由 / ブロックタイプ]	
%Y	日付と時刻	
%Z	ポリシー名	
HA イベント		
%H	ホスト名	
%P	ピア名	
%R	理由	
時間割り当てによる URL フィルタ		
%U	URL/URI	
%C	カテゴリ	

表 13-2. 変数の説明 (続き)

変数	変数の意味	変数の使用方法
%H	IWSVA ホスト名	
%N	ユーザ名	
%Q	時間数	
%Y	日付と時刻	
アクセス管理による URL ブロック		
%H	IWSVA ホスト名 (ヘッダフィールドでのみ機能)	
%N	ユーザ名	
%U	URL/URI (本文でのみ機能)	
%Y	日付と時刻	
%X	理由 (本文でのみ機能)	
HTTP 検査による URL ブロック		
%H	IWSVA ホスト名	
%I	フィルタ名	
%N	ユーザ名	
%U	URL/URI	
%Y	日付と時刻	
URL フィルタによる URL ブロック		
%C	カテゴリ	
%H	IWSVA ホスト名 (ヘッダフィールドでのみ機能)	
%N	ユーザ名	
%U	URL/URI	
%Y	日付と時刻	
URL アクセスの警告		
%A	処理	
%B	警告と続行	

表 13-2. 変数の説明 (続き)

変数	変数の意味	変数の使用方法
%C	カテゴリ	
%H	IWSVA ホスト名 (ヘッダフィールドでのみ機能)	
%N	ユーザ名	
%U	URL/URI (本文でのみ機能)	
%Y	日付と時刻	
URL アクセスの警告通知をカスタマイズするには、メッセージテンプレートに次のフォームを含め、[続行する] オプションを表示する必要があります。 `<form id="warncontinue" method="post" action="%B$$$IWSX_URL_ACTION$$$"> <INPUT type=hidden value="%A" name=data> </form>` カスタマイズした通知では、ユーザが続行できるようにフォームを送信するためのボタンまたはハイパーリンクを定義する必要があります。例 : `<input name="button2" type="button" value="Continue at your own risk" style="width:195px" onclick="document.getElementById('warncontinue').submit(); return false;"></input>`		
URL アクセスのオーバーライド		
%A	処理	
%B	URL/URI を続行	
%C	カテゴリ	
%E	ポリシーの初期設定の時間制限	
%H	IWSVA ホスト名	
%J	ポリシーの最大時間制限	
%N	ユーザ名	
%U	URL/URI (本文でのみ機能)	
%Y	日付と時刻	
%Z	ポリシー名	

表 13-2. 変数の説明 (続き)

変数	変数の意味	変数の使用方法

URL アクセスのオーバーライドの通知をカスタマイズする場合は、メッセージテンプレートにパスワードを base64 コードで暗号化する Java スクリプトコードを組み込む必要があります。パスワード、時間制限、および ttl_type などの要素を組み込みます。このようにしないと、カスタマイズした通知ページが機能しません。
`<form id="overridecontinue" method="post" action="%B[Warn and Continue URL/URI]/$$$IWSX_URL_ACTION$$$">`
`<INPUT type=hidden value="%A[Action]" name=data>`
 	
カスタマイズした通知では、ユーザが続行できるようにフォームを送信するためのボタンまたはハイパーリンクを定義する必要があります。例 :
`<input type="button" name="Button22"`
`value="Submit" class="style3"`
`onclick="doSubmit();" />`		

しきい値アラート		
%m	基準	
%t	しきい値	

通知の設定

通知を設定するには、通知を発行するイベントの種類を選択し、メールまたはブラウザ通知メッセージを編集します。

ユーザへの通知での HTML タグの使用

ユーザへの通知メッセージは、HTML を使用して書式を設定できます。HTML ファイルには外部の画像またはスタイルへの参照リンクを含めることができますが、IWSVA でサポートされるのは HTML ファイルのアップロードだけです。その他のファイルは個別に Web サーバにアップロードする必要があります。リンクの破損を防ぐために絶対リンクを使用することをお勧めします。

C&C コンタクトコールバック通知の設定

IWSVA は、セキュリティポリシーに違反する C&C コンタクトオブジェクトのダウンロードを検出すると、管理者への通知をメールで送信し、ユーザへの通知メッセージを要求元クライアントのブラウザに表示します。

C&C コンタクトコールバック通知を設定するには

1. 管理コンソールで [通知] をクリックし、[C&C コールバック試行通知] をクリックします。
2. [管理者への通知] で、[C&C コールバック施行が検出された場合に通知を送信する] をオンにします。
3. 各インシデントごとに、または特定のリスクレベル (低、中、または高) を超えた場合にルート受信者にメッセージを送信するように選択します。
4. 初期設定の通知メッセージを使用しない場合は、初期設定のテキストを選択して、任意のテキストを入力します。該当する場合は、339 ページの「通知の変数」で説明されているように、テキストに変数を挿入します。
5. [ユーザへの通知] は、次のように設定します。
   a. 初期設定の警告メッセージを表示するには、[初期設定] チェックボックスをオンにします。
   b. 独自のメッセージを表示するには [カスタマイズ] チェックボックスをオンにし、カスタマイズしたメッセージの内容を入力するか、[インポート] を使用してインポートします。
      - 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSVA に [インポート] できます。
      - IWSVA 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。
6. [保存] をクリックします。

情報漏えい対策通知の設定

IWSVA は、セキュリティポリシーに違反するデータ漏えいを検出すると、管理者への通知をメールで送信し、ユーザへの通知メッセージを要求元クライアントのブラウザに表示します。

情報漏えい対策通知を設定するには

1. 管理コンソールで [通知] をクリックし、[情報漏えい対策] をクリックします。
2. [管理者への通知] で、[データ漏えいが検出された場合に通知を送信する] をオンにします。

3. 初期設定の通知メッセージを使用しない場合は、初期設定のテキストを選択して、任意のテキストを入力します。該当する場合は、339 ページの「通知の変数」で説明されているように、テキストに変数を挿入します。
4. [ユーザへの通知] は、次のように設定します。
   a. 初期設定の警告メッセージを表示するには、[初期設定] チェックボックスをオンにします。
   b. 独自のメッセージを表示するには [カスタマイズ] チェックボックスをオンにし、カスタマイズしたメッセージの内容を入力するか、[インポート] を使用してインポートします。
      - 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSVA に [インポート] できます。
      - IWSVA 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。
5. [保存] をクリックします。

FTP 情報漏えい対策通知の設定

IWSVA は、セキュリティポリシーに違反する FTP データ漏えいを検出すると、管理者への通知をメールで送信し、ユーザへの通知メッセージを要求元クライアントのブラウザに表示します。

FTP 情報漏えい対策通知を設定するには

1. 管理コンソールで [通知] をクリックし、[FTP 情報漏えい対策] をクリックします。
2. [管理者への通知] で、[データ漏えいが検出された場合に通知を送信する] をオンにします。
3. 初期設定の通知メッセージを使用しない場合は、初期設定のテキストを選択して、任意のテキストを入力します。該当する場合は、339 ページの「通知の変数」で説明されているように、テキストに変数を挿入します。
4. [ユーザへの通知] は、次のように設定します。
   a. 初期設定の警告メッセージを表示するには、[初期設定] チェックボックスをオンにします。
   b. 独自のメッセージを表示するには [カスタマイズ] チェックボックスをオンにし、カスタマイズしたメッセージの内容を入力するか、[インポート] を使用してインポートします。
      - 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSVA に [インポート] できます。

- IWSVA 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。

5. [保存] をクリックします。

FTP ファイルタイプによるブロック通知の設定

IWSVA では、FTP でのアップロードおよびダウンロードの検索に加えて、FTP のゲートウェイでファイルタイプによるブロックも実行できます。パフォーマンスの問題を避けるため、FTP の検索モジュールには圧縮ファイルおよびサイズの大きいファイルについての特別な設定が用意されています。スパイウェア検索もサポートされています。

IWSVA の FTP 検索は、他の FTP プロキシサーバと連係する環境または IWSVA が自身の FTP プロキシとして動作する環境に配置できます。IWSVA サーバのセキュリティを確保するために、IWSVA サーバとそのポートへのアクセスを制御する複数のセキュリティ関連の設定が用意されています。

FTP ファイルタイプによるブロック通知を設定するには

1. 管理コンソールから [通知] を選択し、[FTP ファイルタイプブロック] をクリックします。
2. [管理者への通知] で、[FTP でブロックするファイルタイプがアクセスされた場合に通知を送信する] チェックボックスをオンにします。

   IWSVA のブロック対象の設定によっては、このオプションによって初期設定の受信者に大量の通知メッセージが送信される場合があります。個別の通知の代わりに、ブロックされたファイルはログに記録されるので、それを IWSVA が生成するレポートの 1 つに含めることも可能です。
3. 初期設定の通知メッセージを使用しない場合は、初期設定のテキストを選択して、任意のテキストを入力します。該当する場合は、339 ページの「通知の変数」で説明されているように、テキストに変数を挿入します。
4. [ユーザへの通知] は、次のように設定します。
   a. 初期設定の警告メッセージを表示するには、[初期設定] チェックボックスをオンにします。
   b. 独自のメッセージを表示するには [カスタマイズ] チェックボックスをオンにして、カスタマイズした内容を入力します。
      - 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSVA に [インポート] できます。
      - IWSVA 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。

5. [保存] をクリックします。

FTP 検索通知の設定

IWSVA では、ユーザの FTP 転送に不正コードが検出されると、カスタマイズした管理者への通知を指定されたメールアドレスに自動的に送信したり、要求元 FTP クライアントのプログラムに通知を表示したりすることができます。

FTP 検索通知を設定するには

1. 管理コンソールから [通知] を選択し、[FTP 検索] をクリックします。
2. [管理者への通知] で、通知の対象とする検出イベントのチェックボックスをオンにします ([ウイルス]、[トロイの木馬]、[その他の不正プログラム] のいずれかまたはすべて)。
3. 初期設定の通知メッセージを使用しない場合は、初期設定のテキストを選択して、任意のテキストを入力します。該当する場合は、339 ページの「通知の変数」で説明されているように、テキストに変数を挿入します。
4. [ユーザへの通知] は、次のように設定します。
   a. 初期設定の警告メッセージを表示するには、[初期設定] チェックボックスをオンにします。
   b. 独自のメッセージを表示するには [カスタマイズ] チェックボックスをオンにして、カスタマイズした内容を入力します。
      - 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSVA に [インポート] できます。
      - IWSVA 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。
5. [保存] をクリックします。

HTTP/HTTPS ファイルタイプによるブロック通知の設定

IWSVA は、ファイルをブロックすると、管理者への通知をメールで送信します。ユーザへの通知メッセージは要求元クライアントのブラウザに表示されます。

HTTP/HTTPS ファイルタイプによるブロック通知を設定するには

1. [通知] をクリックし、[HTTP/HTTPS ファイルタイプブロック] をクリックします。
2. [管理者への通知] で、[HTTP/HTTPS でブロックするファイルタイプがアクセスされた場合に通知を送信する] チェックボックスをオンにします。

3. 初期設定の通知メッセージを使用しない場合は、初期設定のテキストを選択して、任意のテキストを入力します。該当する場合は、339 ページの「通知の変数」で説明されているように、テキストに変数を挿入します。
4. ブラウザに表示する [タイトル] を入力します。

   初期設定のタイトルは、「Trend Micro InterScan Web Security イベント」です。タイトルは、ウイルス感染メッセージ、ファイルタイプブロック、および URL ブロックメッセージで共通です。
5. [ユーザへの通知] は、次のように設定します。
   a. 初期設定の警告メッセージを表示するには、[初期設定] チェックボックスをオンにします。
   b. 独自のメッセージを表示するには [カスタマイズ] チェックボックスをオンにし、メッセージの内容を入力するか、HTML ファイルからインポートします。
      - 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSVA に [インポート] できます。
      - IWSVA 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。
6. [プレビュー] をクリックして、通知が正しく表示されることを確認します。
7. [保存] をクリックします。

HTTP/HTTPS 検索通知の設定

クライアントが要求したファイル中に不正コードを検出すると、IWSVA は管理者への通知をメールで発行し、ユーザへの通知を要求元クライアントのブラウザに送信します。

IntelliTrap は一種のセキュリティの脅威と見なされるため、HTTP/HTTPS 検索と同じ通知が使用されます。

HTTP/HTTPS 検索通知を設定するには

1. [通知] → [HTTP/HTTPS 検索] の順に選択します。
2. [管理者への通知] で、通知の対象とする検出イベントのチェックボックスをオンにします ([ウイルス]、[トロイの木馬]、[その他のインターネット上の脅威]、[ボット] のいずれかまたはすべて)。

注意： IntelliTrap 通知は、[その他のインターネット上の脅威] に関連付けられています。したがって、IntelliTrap 通知は [その他のインターネット上の脅威] を選択すると有効になります。

3. 初期設定の通知メッセージを使用しない場合は、初期設定のテキストを選択して、任意のテキストを入力します。該当する場合は、339 ページの「通知の変数」で説明されているように、メッセージに変数を挿入します。
4. ブラウザに表示する [タイトル] を入力します。

   初期設定のタイトルは、「Trend Micro InterScan Web Security イベント」です。タイトルは、ウイルス感染メッセージ、ファイルタイプブロック、および URL ブロックメッセージで共通です。
5. [ダウンロードファイルに対するメッセージ] および [アップロードファイルに対するメッセージ] のユーザ通知メッセージは、次のように設定します。
   a. 初期設定の警告メッセージを表示するには、[初期設定] チェックボックスをオンにします。
   b. 独自のメッセージを表示するには [カスタマイズ] チェックボックスをオンにし、カスタマイズしたメッセージの内容を入力するか、HTML ファイルからインポートします。
      - 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSVA に [インポート] できます。
      - IWSVA 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。
   c. [プレビュー] をクリックして、通知が正しく表示されることを確認します。
6. [保存] をクリックします。

HTTPS アクセス拒否通知の設定

HTTPS 接続を介した Web サイトへのアクセスが拒否されたユーザには、要求が拒否されたことを示す HTML ページが表示されます。

HTTPS アクセス拒否通知を設定するには

1. [通知] → [HTTPS アクセス拒否] の順に選択します。
2. ブラウザに表示する [タイトル] を入力します。

初期設定のタイトルは、「Trend Micro InterScan Web Security イベント」です。タイトルは、ウイルス感染メッセージ、ファイルタイプブロック、および URL ブロックメッセージで共通です。

3. [ユーザへの通知] は、次のように設定します。
   a. 初期設定の警告メッセージを表示するには、[初期設定] チェックボックスをオンにします。
   b. 独自のメッセージを表示するには [カスタマイズ] チェックボックスをオンにし、メッセージの内容を入力するか、HTML ファイルからインポートします。
      - 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSVA に [インポート] できます。
      - IWSVA 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。
4. [プレビュー] をクリックして、通知が正しく表示されることを確認します。
5. [保存] をクリックします。

HTTPS 証明書エラー通知の設定

証明書が検証テストに合格していない Web サイトへのアクセスが拒否されたユーザには、警告メッセージを示す HTML 画面が表示されます。ユーザは、HTTPS トラフィックを復号化およびチェックせずに、Web サイトへのアクセスを継続することもできます。

HTTPS 証明書エラー通知を設定するには

1. [通知] → [HTTPS 証明書エラー] の順に選択します。
2. ブラウザに表示する [タイトル] を入力します。

   初期設定のタイトルは、「Trend Micro InterScan Web Security イベント」です。タイトルは、ウイルス感染メッセージ、ファイルタイプブロック、および URL ブロックメッセージで共通です。
3. [ユーザへの通知] は、次のように設定します。
   a. 初期設定の警告メッセージを表示するには、[初期設定] チェックボックスをオンにします。
   b. 独自のメッセージを表示するには [カスタマイズ] チェックボックスをオンにし、メッセージの内容を入力するか、HTML ファイルからインポートします。

- 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSVA に [インポート] できます。
- IWSVA 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。

4. [プレビュー] をクリックして、通知が正しく表示されることを確認します。
5. [保存] をクリックします。

アプリケーション制御通知による HTTP/HTTPS アクセス拒否の設定

検証テストに合格しない証明書を持つ HTTP/HTTPS Web サイトへのアクセスをユーザが拒否されるたびに、警告メッセージが示された HTML 画面が表示されます。ユーザは、HTTP/HTTPS トラフィックを復号化およびチェックせずに、HTTP/HTTPS Web サイトへのアクセスを継続することもできます。

HTTPS 証明書エラー通知を設定するには

1. [通知] → [アプリケーション制御による HTTP/HTTPS アクセス拒否] の順に選択します。
2. ブラウザに表示する [タイトル] を入力します。

   初期設定のタイトルは、「Trend Micro InterScan Web Security イベント」です。タイトルは、ウイルス感染メッセージ、ファイルタイプブロック、および URL ブロックメッセージで共通です。
3. [ユーザへの通知] は、次のように設定します。
   a. 初期設定の警告メッセージを表示するには、[初期設定] チェックボックスをオンにします。
   b. 独自のメッセージを表示するには [カスタマイズ] チェックボックスをオンにし、メッセージの内容を入力するか、HTML ファイルからインポートします。
      - 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSVA に [インポート] できます。
      - IWSVA 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。
4. [プレビュー] をクリックして、通知が正しく表示されることを確認します。
5. [保存] をクリックします。

パターンファイルのアップデート通知の有効化

IWSVA では、パターンファイルの予約アップデートに基づいた検索エンジンまたはパターンファイルのアップデート試行の際に通知を送信できます。

注意： IWSVA では、手動によるパターンファイルアップデートの通知は送信されません。

パターンファイルのアップデート通知を有効にするには

1. 管理コンソールから [通知] を選択し、[パターンファイルのアップデート] をクリックします。
2. パターンファイルのアップデート試行は、次のように設定します。
   a. 通知の対象とするアップデートイベントを選択します。[成功]、[失敗]、または [アップデート不要] のアップデート試行に対して通知を設定できます。
   b. 通知メッセージの [件名] を入力します。初期設定は、「IWSVA パターンファイルのアップデート結果」です。
3. [保存] をクリックします。

しきい値アラートの設定

IWSVA では、設定したしきい値を超えた場合に通知を送信できます。

しきい値アラートの通知を有効にするには

1. 管理コンソールから [通知] を選択し、[しきい値アラート] をクリックします。
2. しきい値アラートについて、次の設定を行います。
   a. 通知メッセージのしきい値アラートの種類、値、および頻度の制限を有効にします。
   b. 通知先を変更するには、管理コンソールの [通知] をクリックして、画面右上の [通知先の設定 ...] をクリックします。
   c. 初期設定のメッセージを使用するか、[通知メッセージ] で独自のメッセージを作成します。
3. [保存] をクリックします。

URL アクセスの警告通知の設定

URL フィルタルール処理が「警告」に設定されている場合に、会社ポリシーによって禁止されているカテゴリに属する URL にアクセスしようとすると、URL アクセスの警告モードにより通知が送信されます (詳細については、258 ページの「新しいポリシーの作成」を参照してください)。該当の Web ページの表示前に、ユーザに警告が送信されます。

必要に応じて警告メッセージの次のリンクのいずれかを選択できます。

- 安全に前の Web ページに戻る
- 自己責任で続行する (非推奨)

URL アクセスの警告通知を設定するには

1. 管理コンソールから [通知] を選択し、[URL アクセスの警告] をクリックします。
2. ブラウザに表示する [タイトル] を入力します。

   初期設定のタイトルは、「Trend Micro InterScan Web Security イベント」です。タイトルは、ウイルス感染メッセージ、ファイルタイプブロック、および URL ブロックメッセージで共通です。
3. [ユーザへの通知] は、次のように設定します。
   a. 初期設定の警告メッセージを表示するには、[初期設定] チェックボックスをオンにします。
   b. 独自のメッセージを表示するには [カスタマイズ] チェックボックスをオンにし、メッセージの内容を入力するか、HTML ファイルからインポートします。
      - 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSVA に [インポート] できます。
      - IWSVA 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。
      - 通知には、エンドユーザが続行を選択する場合に必要な情報を IWSVA に送信するためのフォームを含める必要があります。このフォーマットは、次のとおりです。

```
<form id="warncontinue" method="post" action="%B$$$IWSX_URL_ACTION$$$">
<INPUT type=hidden value="%A" name=data>
</form>
```

      - カスタマイズした通知では、ユーザが続行を求めてフォームを送信するためのボタンまたはハイパーリンクを定義する必要があります。例:

```
<a href="javascript:void(0)"
onclick="document.getElementById('warncontinue').submit();
return false;">Continue to this website (not recommended)</a>
```

4. [プレビュー] をクリックして、通知が正しく表示されることを確認します。
5. [保存] をクリックします。

URL アクセスのオーバーライドの通知の設定

会社ポリシーによって「オーバーライド付きブロック」処理が設定されたカテゴリ内の URL にアクセスしようとすると、ユーザに URL アクセスのオーバーライドモード通知が送信されます。オーバーライドの警告が表示され、続行するにはパスワードの入力が必要です。この通知では、閲覧が許容される残り時間量が表示されます。正しいパスワードを入力した後に、要求する Web ページを続行できます。

必要に応じて警告メッセージの次のリンクのいずれかを選択できます。

- パスワードが不明の場合、ページの参照を中止
- パスワードを入力して、指定された期間内で閲覧を続行

管理者は、あらかじめポリシーでカテゴリ処理を「オーバーライド付きブロック」の処理に設定しておく必要があります。詳細については、258 ページの「新しいポリシーの作成」を参照してください。

URL アクセスのオーバーライドのユーザ通知メッセージを設定するには

1. 管理コンソールから [通知] を選択し、[URL アクセスのオーバーライド] をクリックします。
2. [ユーザへの通知 URL アクセスのオーバーライド用] で、次の操作を実行します。
   a. ブラウザに表示する [タイトル] を入力します。

      初期設定のタイトルは、「Trend Micro InterScan Web Security イベント」です。タイトルは、ウイルス感染メッセージ、ファイルタイプブロック、および URL ブロックメッセージで共通です。
   b. 初期設定の警告メッセージを表示するには [初期設定] チェックボックスをオンにします。
   c. 独自の警告メッセージを表示するには [カスタマイズ] チェックボックスをオンにします。メッセージをテキストボックスに入力するか、ローカルコンピュータの HTML ファイルからメッセージをインポートします。
      - 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSVA に [インポート] できます。

- IWSVA 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。

d. URL アクセスのオーバーライドの通知をカスタマイズする場合は、メッセージテンプレートにパスワードを base64 コードで暗号化する Java スクリプトコードを組み込む必要があります。パスワード、時間制限、および ttl_type などの要素を組み込みます。このようにしないと、カスタマイズした通知ページが機能しません。

例 :

```
<form id="overridecontinue" method="post" action="%B[Warn and Continue
URL/URI]$$$IWSX_URL_ACTION$$$">
<INPUT type=hidden value="%A[Action]" name=data>
..
</form>
```

e. カスタマイズした通知では、ユーザが続行を求めてフォームを送信するためのボタンまたはハイパーリンクを定義する必要があります。

例 :

```
<input type="button" name="Button22"
value="Submit" class="style3"
onclick="doSubmit();" />
```

3. [プレビュー] をクリックして、通知が正しく表示されることを確認します。
4. [保存] をクリックします。

アクセス管理通知による URL ブロックの設定

IWSVA で、ローカル IWSVA リストからフィッシングパターンファイルにある URL または禁止 URL へのアクセスが検出されると、IWSVA は要求元クライアントのブラウザに、URL がブロックされたことを示す警告画面を表示します。

アクセス管理による URL ブロックのユーザ通知メッセージを設定するには

1. 管理コンソールから [通知] を選択し、[アクセス管理による URL ブロック] をクリックします。
2. [制限された URL やブロックされた URL のユーザ通知メッセージ] で、次の操作を実行します。

a. ブラウザに表示する [タイトル] を入力します。

初期設定のタイトルは、「Trend Micro InterScan Web Security イベント」です。タイトルは、ウイルス感染メッセージ、ファイルタイプブロック、および URL ブロックメッセージで共通です。

b. 初期設定の警告メッセージを表示するには [初期設定] チェックボックスをオンにします。

c. 独自の警告メッセージを表示するには [カスタマイズ] チェックボックスをオンにします。メッセージをテキストボックスに入力するか、ローカルコンピュータの HTML ファイルからメッセージをインポートします。

- 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSVA に [インポート] できます。
- IWSVA 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。

3. [プレビュー] をクリックして、通知が正しく表示されることを確認します。
4. [保存] をクリックします。

HTTP 検査通知による URL ブロックの設定

IWSVA で、ブロック処理により、HTTP 検査ポリシーに違反している URL へのアクセスが検出されると、IWSVA は要求元クライアントのブラウザに、URL がブロックされたことを示す警告画面を表示します。

HTTP 検査のユーザ通知メッセージを設定するには

1. 管理コンソールから [通知] を選択し、[HTTP 検査による URL ブロック] をクリックします。
2. [制限された URL やブロックされた URL のユーザ通知メッセージ] で、次の操作を実行します。

a. ブラウザに表示する [タイトル] を入力します。

初期設定のタイトルは、「Trend Micro InterScan Web Security イベント」です。タイトルは、ウイルス感染メッセージ、ファイルタイプブロック、および URL ブロックメッセージで共通です。

b. 初期設定の警告メッセージを表示するには [初期設定] チェックボックスをオンにします。

c. 独自の警告メッセージを表示するには [カスタマイズ] チェックボックスをオンにします。メッセージをテキストボックスに入力するか、ローカルコンピュータの HTML ファイルからメッセージをインポートします。

- 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSVA に [インポート] できます。
- IWSVA 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。

3. [プレビュー] をクリックして、通知が正しく表示されることを確認します。

URL フィルタ通知による URL ブロックの設定

IWSVA で、ローカル IWSVA リストからフィッシングパターンファイルにある URL または禁止 URL へのアクセスが検出されると、IWSVA は要求元クライアントのブラウザに、URL がブロックされたことを示す警告画面を表示します。

URL フィルタによる URL ブロックのユーザ通知メッセージを設定するには

1. 管理コンソールから [通知] を選択し、[URL フィルタによる URL ブロック] をクリックします。
2. [制限された URL やブロックされた URL のユーザ通知メッセージ] で、次の操作を実行します。
   a. ブラウザに表示する [タイトル] を入力します。

      初期設定のタイトルは、「Trend Micro InterScan Web Security イベント」です。タイトルは、ウイルス感染、ファイルタイプによるブロック、および URL ブロックのメッセージで共通です。
   b. 初期設定の警告メッセージを表示するには [初期設定] チェックボックスをオンにします。
   c. 独自の警告メッセージを表示するには [カスタマイズ] チェックボックスをオンにします。メッセージをテキストボックスに入力するか、ローカルコンピュータの HTML ファイルからメッセージをインポートします。
      - 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSVA に [インポート] できます。
      - IWSVA 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。
3. [プレビュー] をクリックして、通知が正しく表示されることを確認します。
4. [保存] をクリックします。

URL フィルタエンジンおよび検索エンジンのアップデートの通知の有効化

パターンファイルのアップデートほど頻繁ではありませんが、トレンドマイクロでは、ウイルスおよび不正コードの検出方法の進化を反映するために、定期的に新しいバージョンの検索エンジンをリリースします。IWSVA では、検索エンジンの予約アップデートに応じて、管理者への通知を発行できます。

注意： IWSVA では、手動によるエンジンのアップデートの通知は送信されません。

URL フィルタおよび検索エンジンのアップデート通知を有効にするには

1. 管理コンソールから [通知] を選択し、[URL フィルタエンジンおよび検索エンジンのアップデート] をクリックします。
2. 検索エンジンまたは URL フィルタエンジンについて、通知の対象とするアップデートイベントを選択します。

   [成功]、[失敗]、または [アップデート不要] のアップデート試行に対して通知を設定できます。
3. 検索エンジンまたは URL フィルタエンジンについて、通知メールメッセージの [件名] を入力します。
4. [保存] をクリックします。

時間割り当て通知による URL フィルタの設定

URL フィルタポリシーのルールで時間制限の処理が設定されている場合は、ユーザに時間割り当て通知による URL フィルタを送信できます。[URL フィルタ] → [ポリシー] | [ルール] タブで、ポリシーに [時間制限] 処理が設定されている場合は、常にエンドユーザの Web ブラウザに表示されます。詳細については、258 ページの「新しいポリシーの作成」を参照してください。

このオプションが有効化されている場合、IWSVA で時間制限処理が設定されているページをダウンロードしようとした場合、および制限時間が経過した場合は、必ず要求が拒否されたことを示す HTML ページが表示されます。詳細については、266 ページの「時間割り当てによる URL フィルタの延長」を参照してください。

時間割り当て通知による URL フィルタを設定するには

1. 管理コンソールから [通知] を選択し、[時間割り当てによる URL フィルタ] をクリックします。
2. 初期設定の通知メッセージを使用しない場合は、[カスタマイズ] チェックボックスをオンにして、任意のテキストを入力します。該当する場合は、339 ページの「通知の変数」で説明されているように、テキストに変数を挿入します。
3. [保存] をクリックします。

スマートスキャンイベント通知の設定

IWSVA では、グローバル Smart Protection Server が利用できない場合に通知メールを送信し、従来型の検索に切り替えることができます。

「Smart Protection Server 使用不可」通知を有効にするには

1. メインメニューから [通知] を選択し、[スマートスキャンイベント] をクリックします。
2. [Smart Protection Server が使用不可の場合に通知を送信する] チェックボックスをオンにします。
3. [保存] をクリックします。

注意： IWSVA では、Smart Protection Server にアクセスできず、従来型の検索に切り替える場合のみメール通知を送信します。ユーザが手動でスマートスキャンから従来型の検索に切り替えた場合は通知を送信しません。

注意： スマートスキャンイベント通知では変数を使用しません。

SNMP トラップ通知の有効化

IWSVA では、セキュリティ、アップデート、またはプログラムイベントに対する SNMP トラップの送信がサポートされています。

注意： SNMP が有効でなければ、[通知] 画面に SNMP 設定は表示されません。SNMP トラップを送信するには、[管理] → [ネットワーク設定] → [SNMP 設定] で SNMP を設定して、この機能を有効にする必要があります。

SNMP 通知の送信を有効にするには

1. 管理コンソールから [通知] を選択し、画面の下部に表示される [SNMP 通知の設定] で [通知の設定 ...] をクリックします。
2. SNMP 通知を実行するイベントの種類を選択します。イベントには次のような種類があります。
   - **ウイルスまたはインターネット上の脅威の検出** — ウイルスまたは不正コードの検出に関連するイベントです。
   - **セキュリティ違反** — ウイルス検出以外の、IWSVA ポリシーで禁止されている活動に関連するイベントです（アクセス割り当てポリシー、URL ブロック設定など）。
   - **パターンファイル** /URL **フィルタデータベース / 検索エンジンのアップデート** — IWSVA のアップデートに関連するイベントです。

- IWSVA **サービスの予期しない停止** — IWSVA サービスが異常停止したときのイベントです。
- **システムパフォーマンス測定** — 次のパフォーマンスデータを記載した SNMP トラップを定期的に送信するイベントです。
  - CPU 使用率
  - メモリ使用率
  - ディスク使用率
  - 同時接続 (ICAP 要求および応答モードおよびプロキシモード)
  - 送受信スループット (バイト / 秒)
- **高可用性イベント** — HA が使用されている場合は、HA 機能が異常停止したときのイベントです。
- **ハードウェア監視イベント** — 監視される次のハードウェアコンポーネントに関するイベントです。
  - 電圧
  - ファン
  - CPU
  - 記憶装置
  - 温度

3. [保存] をクリックします。

第 14 章

管理

本章では、InterScan Web Security Virtual Appliance（以下、IWSVA）で使用可能な管理機能について説明します。

本章で説明する内容には、次の項目が含まれます。

概要

[管理] メニューには、次のオプションが含まれます。

- 365 ページの「監査ログ」
- 365 ページの「一般設定」
  - 366 ページの「ユーザの識別」
  - 375 ページの「ポリシー配信」
  - 375 ページの「データベース接続」
  - 376 ページの「隔離管理」
  - 377 ページの「システム時間」
  - 377 ページの「予約期間」
  - 378 ページの「Control Manager への登録」
  - 378 ページの「設定の複製」
  - 379 ページの「集中管理ログ / レポート」
  - 380 ページの「検索方法」
  - 381 ページの「PAC ファイル管理」
  - 381 ページの「ネットワーク設定」
  - 381 ページの「ネットワークインタフェース」
  - 381 ページの「Web コンソール」
  - 382 ページの「リモート CLI」
  - 383 ページの「SNMP の設定」
  - 384 ページの「静的ルート」
- 385 ページの「管理コンソール」
  - 385 ページの「役割ベースの管理」
  - 386 ページの「役割の管理」
  - 389 ページの「アカウント管理」
  - 392 ページの「アクセス管理の設定」
- 393 ページの「Syslog サーバ」
- 393 ページの「設定のバックアップと復元」
- 394 ページの「システムアップデート」
- 395 ページの「システムのメンテナンス」

- 395 ページの「システムイベントログ」
- 396 ページの「製品ライセンス」
- 398 ページの「サポート情報」

監査ログ

監査ログには、ユーザが変更したアプリケーションの設定を説明する情報が記載されています。たとえば、ユーザが移行またはロールバックの手順を実施した場合、移行活動を記録するエントリが監査ログに作成されます。

注意： IPv4 監査ログの場合と同様に、IPv6 関連の設定変更はすべてログに記録されます。

監査ログを表示するには

1. 管理コンソールから [管理] → [監査ログ] の順に選択します。
2. [期間] で、レポートを生成する時間を選択します。
   任意の期間のウイルスログを表示するには、[範囲] をクリックし、開始と終了の日付を選択します。
3. [ユーザ] で、ログエントリを表示するユーザを選択します。[追加] をクリックします。リストにあるすべてのユーザを追加する場合は、[すべて追加] をクリックします。ユーザを右側のリストボックスから削除するには、[削除] をクリックします。リストにあるすべてのユーザを削除する場合は、[すべて削除] をクリックします。
4. [並べ替え基準] で、ログの並べ替えの基準とするオプションを選択します。オプションは、[ユーザ] および [日付] です。
5. [ログ表示] をクリックします。[監査ログ] 画面が開きます。
6. 画面を更新するには、[表示更新] をクリックします。

一般設定

[一般設定] には、次の項目が含まれます。

- 366 ページの「ユーザの識別」
- 373 ページの「ポリシー確認画面」
- 374 ページの「認証の許可リスト」

- 375 ページの「ポリシー配信」
- 375 ページの「データベース接続」
- 376 ページの「隔離管理」
- 377 ページの「システム時間」
- 377 ページの「予約期間」
- 378 ページの「Control Manager への登録」
- 378 ページの「設定の複製」
- 379 ページの「集中管理ログ / レポート」
- 380 ページの「検索方法」
- 381 ページの「PAC ファイル管理」

ユーザの識別

IWSVA では、次の複数のユーザ識別方法がサポートされます。

- IP アドレス
- ホスト名
- ユーザ / グループ名

注意： ユーザの識別方法を変更すると、ログやレポートのほか、今まで作成した既存ポリシーに影響を及ぼすことがあります。

IWSVA でユーザ / グループベースのポリシーを使用する必要があり、ネットワーク上に LDAP サーバがある場合は、[ユーザ / グループ認証の設定] を選択し、各種の属性設定に関する情報について LDAP 管理者に問い合わせてください。

レポート、ログ、通知メッセージ、および検索ポリシーの作成に任意のユーザの識別方法を選択します。

ユーザ / グループ認証の設定

基本 (単一の Active Directory サーバ)

IWSVA では LDAP 機能が強化され、Microsoft の Active Directory のいくつかの設定が自動的に検出できるようになりました。これにより、設定作業が簡素化されます。Microsoft Active Directory は多くのユーザに使用されているので、これは、あまり複雑な設定を必要としないユーザにとって最適なオプションとなります。

基本（単一の Active Directory サーバ) を使用するには、[ユーザの識別] 画面で [管理] → [一般設定] → [ユーザの識別] の順に選択して、[基本（単一の Active Directory サーバ)] チェックボックスをオンにします。
[基本（単一の Active Directory サーバ)] ビューでは、次の設定のみが必要になります。

- ドメイン名
- サービスアカウント
- パスワード

自動検出機能を正しく機能させるには、LDAP ベンダーで Microsoft Active Directory を使用する必要があります。IWSVA によって特定のドメインに対して使用可能なすべてのサーバが自動的に検出され、ユーザの設定に最適なサーバが、他の重要な設定とともに選択されます。
IWSVA では、次のように自動検出が実行されます。

- DNS クエリによって LDAP サーバのリストを取得します。
- 接続していないサーバを排除します。
- LDAP サーバの中に複数の GC または DC が配置されている場合は、レスポンス速度が速い GC または DC がプライマリ LDAP サーバとして選択されます。
- ドメイン名が BDN に変換されます。
- Kerberos 情報が生成され、認証されます。

詳細 (その他の / 複数の LDAP サーバ)

このオプションは、詳細または複雑な LDAP 設定を使用する場合に選択します。[詳細（その他の / 複数の LDAP サーバ)] ビューでは、Active Directory 以外にも、その他の LDAP サーバと複数ドメインフォレスト、および冗長 LDAP サーバがサポートされます。ユーザ / グループ認証用に複数のドメインを追加できます。IWSVA は、これらのドメインに対するクエリを順次実行して、ユーザを識別し、ポリシーを適用します。

Web コンソールで [詳細（その他の / 複数の LDAP サーバ)] を使用するには、[管理] → [一般設定] → [ユーザの識別] の順にクリックし、[ユーザの識別] で [詳細 （その他の / 複数の LDAP サーバ)] チェックボックスをオンにします。

[詳細（その他の / 複数の LDAP サーバ)] ビューでドメインの設定を追加、削除、または編集し、設定されているすべてのドメインが記載されるリストを作成できます。ドメイン名をクリックするか、下向き矢印ボタンをクリックすると、そのドメインの詳細が表示されます。

注意： IWSVA では、ドメインがサブドメインであるかどうかを確認できません。一方が他方のサブドメインである 2 つのドメインを指定しても、IWSVA では両方とも独立したドメインとして処理されます。

新規 LDAP の設定画面で設定するには

1. [詳細 （その他の / 複数の LDAP サーバ)] を有効にして、[新規ドメインの追加] をクリックするか、既存の LDAP ドメイン名をクリックして詳細を表示します。
2. 次の情報を入力または編集します。
   - **ドメイン名**
   - **サーバの種類**
   - **サービスアカウント**
   - **パスワード**
   - LDAP **サーバのホスト名**
   - **待機ポート番号**
   - LDAP **ポート番号**
   - LDAP **暗号化**
   - **基本識別名** (BDN)

注意： 初期設定の暗号化方式は [なし] です。LDAP サーバで LDAPv3 StartTLS 拡張または LDAPS（LDAP over SSL) がサポートされる場合は、対応する暗号化方式を選択します。

3. [認証方法] で、必要なものを 1 つ選択し、Kerberos ドメインまたはレルム、Kerberos サーバ、および Kerberos ポートを入力します。
4. [認証の高可用性] では、[同じドメインで追加の LDAP サーバを有効にする] を選択することによって、同じドメインに対して追加するサーバの関係を有効にできます。サーバの関係 （ラウ

ンドロビンまたはフェイルオーバ) を設定し、追加するバックアップ LDAP サーバの名前を入力します。

ドメインの設定作業は、かなりの量になります。単純な設定を実行するには、基本ビューの自動検出ボタンを使用します。これで、フォームに自動入力されます。自動検出設定の出力をベースとしてドメインの設定を変更できます。このボタンは、Microsoft Active Directory ユーザが基本ビューでのみ使用できます。

認証方法の設定はある程度 LDAP ベンダーに依存します。一部の認証方法は、特定のベンダーでのみ有効です。次の表は、この関係を示しています。

表 14-1. LDAP ベンダーと認証方法の関係

	Active Directory	OpenLDAP
簡易	使用不可	使用可能
Kerberos	使用可能	使用可能
ダイジェスト - MD5	使用不可	使用可能

IWSVA では LDAP 認証の高可用性をサポートしています。プライマリサーバと同じ設定を共有するバックアップの LDAP サーバを 1 つ指定できます。ただし、次の 2 つの高可用性モードがサポートされています。

- ラウンドロビン : IWSVA の初期設定では、すべての LDAP サーバで交互にユーザの認証が実行されます。
- フェイルオーバ : プライマリサーバがダウンした場合、IWSVA は他のサーバを参照してユーザを認証します。

注意 : ドメインのそれぞれで設定可能な BDN と LDAP サーバのタイプは 1 つのみです。BDN はドメイン間で一意である必要があります。

複数のドメインがサポートされる場合は、任意のドメインに属するアカウントを使用してログインできます。IWSVA はまずドメイン名を確認し、次に一致したドメイン名サーバに対するユーザの認証を実行します。ドメイン名が入力されていない場合は、最初のドメインが初期設定のログインドメイン名として使用されます。

---

5. 設定の準備が完了したら、[保存] をクリックします。最初からやり直す場合は、[キャンセル] をクリックします。設定が正常に保存されたら、LDAP サーバのリストに戻ります。

次に該当する場合は保存できません。対応するエラーメッセージが表示されます。

- LDAP サーバが存在しない
- BDN がリストされていない
- 管理者アカウントまたはパスワードが入力されていない
- 詳細認証モードの選択時に認証情報が入力されていない
- LDAP 接続テストに失敗した

グローバルな認証キャッシュの設定

固定 TTL — Client IP to User ID 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 — Client IP to User ID キャッシュにレコードを追加する際、そのレコードに 360 秒など事前設定された生存期間が設定されます。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 360 秒になります。生存期間内にヒットしなければレコードは削除されます。

前回アクティブな TTL は初期設定で有効になっています。

標準認証方法

標準認証は、Web コンソールの [管理] → [一般設定] → [ユーザの識別] 画面で [標準認証 (OS またはブラウザが実行)] オプションを選択することによって設定できます。

標準認証の認証は、OS またはブラウザによって提供される認証機能を介して実装されます。

ドメインに参加するクライアントが NTLM 認証をサポートするブラウザを介して Web にアクセスする場合、認証情報はブラウザから自動的に送信されるため、認証情報の入力を求めるポップアップ画面は表示されません。

クライアントがドメインに参加していない、ブラウザが NTLM 認証をサポートしていない、またはブラウザで自動認証が無効になっている場合は、自動認証が実装されないため、認証情報の入力を求めるポップアップ画面が表示されます。

キャプティブポータル

キャプティブポータルを設定するには、Web コンソールの [管理] → [一般設定] → [ユーザの識別] 画面で [キャプティブポータル (IWSVA によってブラウザに提供されるカスタム認証ページ)] オプションを選択します。

キャプティブポータルが設定されていると、カスタム認証ページが表示され、ドメインに参加しているクライアントが Web に初めてアクセスする際に認証情報の入力を求められます (自動認証は透過的には実装されません)。

ログインインタフェース画面はカスタマイズできます。この画面は、制限されたネットワークにユーザが初めてアクセスする際、またはユーザが IWSVA で認識されない場合に表示されます。

IWSVA には、カスタムのキャプティブポータルを作成するための詳細モードも用意されています。詳細モードでは、独自の HTML を作成できます。ただし、少なくとも次の JavaScript をカスタムのキャプティブポータルの最初に挿入する必要があります。

```
<SCRIPT LANGUAGE="JavaScript">function accesspolicy(){var str1 =
window.location.href;//alert(str1);var
s=str1.indexOf("?forward=");//alert(s);var
d=str1.indexOf("&IP");//alert(d);var
uri=str1.substring(s+9,d)+"/$$$GUEST_POLICY$$$";//alert(uri);return
uri;}</SCRIPT><form name="loginForm" method="POST"
action="com.trend.iwss.gui.servlet.captiveportal"><tr><td>User name:
</td><td><input name="username" type="text" class="button" size="24"
/></td><td> </td></tr><tr><td>Password:</td><td><input
name="password" type="password" class="button" size="24" /></td><td><input
name="Submit" type="submit"></td></tr></form><div class="accessmsg"
[Display GuestPolicy Message...]>If you are a guest, please select the
Guest Access option to access the Internet</div><input name="Access"
type="button" onclick="window.location.href=accesspolicy();" [Display
GuestPolicy...]/>
```

認証フォームにゲストアクセスボタンとイベントハンドラを表示するには、この Java スクリプトが必要です。このスクリプトがないと、ユーザは認証を通過できません。

注意： キャプティブポータルは、ICAP モードではサポートされません。

ゲストログインの許可

ゲストアクセスは、[ゲストログインの許可] ボックスがオンの場合に有効になります。有効である場合は、[ゲスト] と表示されたボタンが追加表示されます。ゲストはこのボタンを選択することでインターネットにアクセスできますが、その操作はゲストポリシーによって管理されます。ゲストポリシーは、ポリシーリストでゲストアクセスが有効である場合に自動的に表示されます。これ以外の場合には表示されません。

ゲストアクセスを許可するには

1. [認証方法] セクションで、[キャプティブポータル（IWSVA によってブラウザに提供されるカスタム認証ページ)] オプションを選択します。
2. [ゲストログインの許可] チェックボックスをオンにします。
3. [キャプティブポータル] 画面の外観をあらかじめ設計して、HTML 形式で保存することができます。色、ロゴ、およびテキストを使用して、企業のブランドイメージに合わせます。カスタマイズした HTML コードをコピーして空白のボックスに貼り付けます。ログイン認証方法とゲストアクセスボタンを表示するには、<%T%> タグを使用します。
4. [ログインのプレビュー画面] をクリックして、設定結果を表示します。
5. [保存] をクリックして、設定を保存します。

Cookie モード

Cookie モードは、NAT およびターミナルサーバ環境におけるユーザの識別に使用されます。Cookie モードを使用するには、クライアントコンピュータに Adobe Flash Player がインストールされ、ブラウザの Cookie が有効であることを確認します。

Cookie モードは、ユーザ / グループ認証が有効でキャプティブポータルが選択されている場合にのみ使用できます。

[キャプティブポータル] ログイン画面の [サインインを保持する] オプションを使用すると、Cookie の「有効期間」を最大で 1 年間、有効にできます。[サインインを保持する] オプションが選択されていない場合、Cookie の「有効期間」は 1 日です。

なし

(推奨しません) ログイベントおよびレポートに出力されるユーザが匿名になり、URL フィルタとその他のポリシーが IP アドレスに基づいて作成されます。

注意： 1. ホスト名の識別は、Microsoft Windows プラットフォームの Internet Explorer で閲覧するエンドユーザに対してのみサポートされています。
2.IWSVA は、HTTPS コンテンツを復号化する前にホスト名情報を取得できないため、ブリッジモードや WCCP モードでは HTTPS 復号化ポリシーに対するホスト名識別をサポートしていません。
3.CLI で「`configure module identification mac_address enable`」コマンドを使用して、クライアントコンピュータのマシンアドレス (MAC) をイベントログ、レポート、および通知に挿入できます。各クライアント上で `register_user_agent_header.exe` ファイルを実行する必要があります。

警告： **[ホスト名] を選択する前に、クライアントごとに `register_user_agent_header.exe` ファイルを実行して、LAN 上のすべてのクライアントを準備しておく必要があります。このファイルはインストールパッケージの付属品です。Windows ドメインのログインスクリプトにこれを追加しておくか、この目的のためにスクリプトを作成しておくとファイルの実行に便利です。**

ポリシー確認画面

[ポリシー確認] 画面タブは、企業のネットワークユーザにインターネット使用ポリシーを知らせます。

基本モード

[ポリシー確認] 画面 (PAS) が有効であると、会社のインターネットアクセスポリシーのコピーがユーザに表示されます。ただし、[ポリシー確認] 画面を使用可能にするには、事前に LDAP 認証を有効にしておく必要があります。

PAS は、Web コンソールの [管理] → [一般設定] → [ユーザの識別] タブの [ポリシー確認画面] タブを使用してカスタマイズできます。この場所で、[ポリシー確認] 画面の有効と無効を切り替えることもできます。

ポリシー確認画面をカスタマイズする

1. ポリシー確認画面の表示 — このボックスをオンにすると、IWSVA がユーザを透過的に認証できるかどうかにかかわりなく、すべてのユーザが PAS に転送されます。IWSVA でユーザを透過的に認証できなかった場合は、キャプティブポータルで、続行する前にユーザ名とパスワードを入力するよう求められます。IWSVA がユーザを透過的に認証した場合は、[OK] と表示されたボタンをクリックすると続行できます。いずれの場合も、PAS が表示されて会社のインターネットアクセスの使用ポリシーが示されます。PAS は、ユーザが初めてインターネットにアクセスする際にのみ表示されます。その後は、キャッシュの有効期限が切れるまで表示されません。

基本設定でポリシー確認画面をカスタマイズする

1. ようこそメッセージを入力します。
2. Trend Micro、Google など、自社名を入力します。
3. 会社のロゴをアップロードします。画像サイズは 1MB 未満にする必要があります。
4. 外部 HTTP リンクを入力します。
5. ポリシーメッセージを入力します。
6. [保存] をクリックします。

ポリシー確認画面を表示する

1. [管理] → [一般設定] → [ユーザの識別] | [ポリシー確認画面] の画面オプションにアクセスします。
2. [ポリシー確認画面の表示] のチェックボックスをオンにします。24 時間サイクルでユーザがインターネットにアクセスするたびに適切な使用ポリシーメッセージが、別画面で示されます。
3. この画面は、次に説明するように、基本モードまたは詳細モードのいずれかの方法で設定します。

認証の許可リスト

LDAP 認証を有効にした後は、会社の認証の許可リストに IP アドレスが登録されているユーザを除き、すべてのユーザがユーザ名とパスワードを提供する必要があります。このリストには、特定の IP/ ホスト名、IP 範囲、または IP サブセットを定義できます。会社の許可リストを作成または編集するには、[管理] → [一般設定] → [ユーザの識別] → [認証の許可リスト] の順に選択します。

ポリシー配信

作成または変更したポリシーは、[ポリシーの配信] ボタンをクリックすることによって、ただちに IWSVA ポリシーデータベースに配信できます。または、何も実行しなくても、[管理] → [ポリシー配信] 画面で設定されている生存期限 (TTL) 間隔に従って、ポリシーは自動的に配信されます。

初期設定では、IWSVA から 30 分ごとに次の最新ポリシーが自動的に配信されます。

- ウイルス検索ポリシー
- HTTPS ポリシー
- HTTP 検査ポリシー
- URL フィルタポリシー
- アクセス割り当てポリシー
- アプリケーション制御ポリシー
- DLP ポリシー

データベース接続

IWSVA は既存の PostgreSQL データベースを使用するか、独自の PostgreSQL データベースをインストールします。データベースにはポリシー設定とログデータが格納されていますデータベース接続は、Web コンソールの [管理] → [一般設定] → [データベース接続] タブで確認できます。データベースの設定は `/etc/iscan/intscan.ini` ファイルに保存されます。これらのフィールドはセットアップ時に選択されたものなので、Linux の ODBC データソースと関係なく変更しないでください。

データベース接続設定

- ODBC **データソース名** — セットアップ時に選択した ODBC 名を表示します。
- **ユーザ名** — セットアップ時に決定した ODBC データソースのユーザ名を表示します。初期設定は「sa」です。
- **パスワード** — セットアップ時に選択した暗号化された ODBC パスワードを表示します。
- **データベース接続のテスト** — ポリシーデータベースおよびログデータベースの接続が正しいか、接続が機能しているかを確認するには、これをクリックします。応答メッセージが ODBC データソースから生成されます。

隔離管理

スパイウェア、トロイの木馬、ワームなどのインターネット上の脅威のほとんどは、ファイルに感染しないため「駆除」の対象になりません。IWSVA の検出対象に設定しておいたワーム (膨大な数になる可能性があるため) は削除し、スパイウェア、トロイの木馬、その他の不要なプログラムは隔離または削除することをお勧めします。

隔離ディレクトリ

隔離先のディレクトリ — [HTTP 検索] または [FTP 検索] の [処理] を [隔離] に設定している場合は、ファイルはここで指定したディレクトリに移動されます。初期設定のディレクトリは、次のとおりです。

```
/var/iwss/quarantine
```

注意： 376 ページの「隔離ファイルの暗号化」で説明しているように、隔離ファイルはすべて暗号化することをお勧めします。

隔離ファイルの暗号化

隔離ファイルは危険です。隔離ファイルを暗号化すれば、不注意による再感染および他の種類の悪意のあるコードから保護できます。

疑わしいファイルを削除せずに隔離する場合は、隔離ディレクトリに保存する前にファイルを暗号化することをお勧めします。

注意： 隔離ファイルを復号化する手順については、IWSVA オンラインヘルプの「操作方法」セクションを参照してください。

HTTP 隔離ファイルを暗号化するには

1. [HTTP] → [高度な脅威保護] → [ポリシー] の順に選択し、リストから既存のポリシーを選択するか、または [追加] をクリックして新しいポリシーを作成します。
2. [ウイルス / 不正プログラム検索ルール] タブを開きます。画面の下部で、[隔離ファイルを暗号化する] チェックボックスをオンにします。

FTP 隔離ファイルを暗号化するには

1. [FTP] → [検索ルール] をクリックします。
2. [ウイルス検索ルール] タブを開きます。画面の下部で、[隔離ファイルを暗号化する] チェックボックスをオンにします。

システム時間

IWSVA Web コンソールの [システム時間] 画面では、日時を手動で設定できます。IWSVA は NTP サーバもサポートしており、指定されたスケジュールに基づいて日時情報を同期します。

システム時間の設定

NTP サーバと日時を同期する — 指定された NTP サーバから日時情報を取得するには、このオプションを選択します。IWSVA は、IPv4 と IPv6 の両方の NTP サーバをサポートしています。リストから選択したスケジュールに基づいて、自動的に日時を同期することもできます。[同期] をクリックすると、NTP サーバに接続してシステムの日時を更新します。これにより、NTP サーバが使用可能かどうかをテストすることもできます。

システム時間を手動で設定 — このオプションを選択した場合は、システムの日時を該当するフィールドに入力します。

タイムゾーン

システムが配置されている大陸および最も近い都市を、表示されるリストから選択します。

予約期間

URL フィルタまたはアプリケーション制御のポリシーを設定する場合、複数の予約期間で IWSVA に異なる動作をさせることができます。たとえば、業務時間外にレクリエーション目的の Web アクセスやインスタントメッセージの使用を許可することができます。URL フィルタのポリシーは、この業務時間の設定に基づいて実行でき、異なる個人またはグループに異なる設定を適用できます。

Control Manager への登録

注意： IWSVA は、Trend Micro Control Manager または Apex Central への IPv4 アドレスでの接続のみをサポートします。

[管理] → [一般設定] → [Control Manager への登録] 画面を使用して、管理通信プロトコル（MCP）エージェントと Control Manager または Apex Central サーバとの間の通信を設定します。

- **接続設定** — エンティティ名（特定のコンピュータ上の IWSVA インスタンス）を指定します。エンティティ名が Control Manager または Apex Central の製品ツリーに表示されるので、製品の識別に役立ちます。
- Control Manager **サーバ設定** — Control Manager または Apex Central サーバの完全修飾ドメイン名（FQDN）または IP アドレスを指定します。Web サーバの認証ユーザ名は、Internet Information Services（IIS）サーバで認証に使用されます。この情報は Control Manager または Apex Central では使用されません。
- MCP **プロキシ設定** — このセクションでは、Control Manager または Apex Central サーバとの通信に使用するプロキシサーバを指定します。
- **双方向通信ポート転送** — 双方向通信にすると、Control Manager または Apex Central サーバから IWSVA にリアルタイムでコマンドを送信できます。この情報を指定しない場合、エージェントの初期設定は一方向通信になるため、IWSVA は、コマンドを受信するために所定の間隔で Control Manager または Apex Central サーバをポーリングします。

設定の複製

IWSVA 複製元インスタンスから IWSVA 複製先インスタンスへの、IWSVA デバイスの登録および設定の複製を提供します。1 つの IWSVA デバイスから 1 つ以上の IWSVA 複製先に、手動または定期的な間隔でポリシーと設定ファイルをコピーしたい場合は [設定の複製] を使用します。ポリシーを設定して、複製の頻度を設定し、root アカウントを選択して、設定ファイルを複製元からエクスポートできます。

設定の複製ポリシーを設定するには

1. IWSVA Web コンソールを開き、[管理] → [一般設定] → [複製の設定] の順にクリックします。
2. スタンドアロン（初期設定）、複製元、または複製先のいずれかのサーバの役割を選択します。

   複製元を選択する場合は、[設定の複製元] チェックボックスをオンにして、[保存] をクリックします。複製元が正常に確立されたことを確認するポップアップメッセージが表示されますの

で、[OK] をクリックします。
複製先の場合は、次の手順を実行します。

3. [設定の受信者] チェックボックスをオンにして、複製元の管理 IP アドレス、ポート、およびセキュリティプロトコルを入力します。

   複製元から設定ファイルをエクスポートするために使用する複製元の管理者アカウント (admin) の名前とパスワードを指定します。ポリシーと設定の複製は、初期設定では 1 時間ごとに行われます。

4. [保存] をクリックします。

注意： 手動で同期できるのは「マスター管理者」のみです。

集中管理ログ / レポート

IWSVA では、ログ送信元リストと、サーバから利用可能なステータスを使用します。集中管理ログ / レポート機能は複数の IWSVA サーバでサポートされます。IWSVA サーバの 1 つを選択して、ログ / レポートコンソール (ログサーバ) として使用できます。IWSVA はログをこのサーバに送信します。ログサーバ上のログ / レポートは、デバイスグループを使用して管理できます。

集中管理ログ / レポートを設定するには

1. IWSVA メニューから、[管理] → [一般設定] → [集中管理ログ / レポート] の順にクリックします。
2. 初期設定のサーバの役割はスタンドアロンです。ログサーバまたはログ送信元のどちらかのサーバの役割を選択します。
   - **ログサーバ**
     i. ログを受信するサーバとして使用する場合は、[ログサーバ] チェックボックスをオンにして [保存] をクリックします。
     ii. 表示されるポップアップ画面で [OK] をクリックします。
     iii. IWSVA Web コンソールを開き、[管理] → [一般設定] → [集中管理ログ / レポート] の順にクリックして、[デバイスグループ管理] でデバイスグループを選択します。
     iv. 新規グループを追加するには、[追加] をクリックし、グループ名と説明を指定し、IP アドレスを選択して、[保存] をクリックします。

- **ログ送信元**
  i. ログ送信元サーバとして使用する場合は、[ログ送信元] チェックボックスをオンにして、ログを受信するサーバの管理 IP、管理ポート、および管理者アカウントのパスワードを指定します。
  ii. [保存] をクリックします。

既存のすべてのデバイスグループが [デバイスグループ管理] に表示されます。デバイスグループは [ログ]、[レポート]、[ダッシュボード] 画面にも表示され、これらの画面でログとレポートのクエリを実行できます。

検索方法

この画面を使用して、データおよび Web サイトの検索方法を設定できます。IWSVA には次の 3 種類の検索方法があります。

- グローバル Smart Protection Server (SPS) を使用したスマートスキャン — Trend Micro Smart Protection Network を使用して Web サイトやデータを検索します。クラウドに保存された脅威のシグネチャを利用して最新の保護を提供します。
- ローカル Smart Protection Server (SPS) を使用したスマートスキャン — クラウド検索における遅延を回避するため、検索リクエストをローカルの Smart Protection Server に送信します。ローカル Smart Protection Server を使用することで、プライバシーがより強化され、処理速度も向上します。ネットワークにアクセスする製品、サービス、およびユーザが増えるにつれて、セキュリティ保護は自動的に更新および強化され、ユーザに対するリアルタイムのネイバーフッドウォッチ (近隣監視活動) 保護サービスが形成されます。
- 従来型の検索 — 従来型の検索では、ローカルに保存された不正プログラム対策コンポーネントやスパイウェア対策コンポーネントを使用します。

注意： スマートスキャンを使用するには、IWSVA で Smart Protection Network に継続的に接続できる必要があります。3 回連続して Smart Protection Network に接続できなかった場合、IWSVA は自動的に従来型の検索に切り替え、継続して保護を提供できるようにします。自動的に従来型の検索に切り替わった場合は、[管理] → [一般設定] → [検索方法] から [スマートスキャン] を選択する必要があります。

PAC ファイル管理

この画面を使用して、PAC (Proxy Auto-configuration) ファイルの追加、編集、コピー、および削除を含む、PAC ファイルの管理を実行できます。

各 PAC ファイルに対して、ファイルの名前、説明、および内容を指定できます。IWSVA では、PAC ファイルの内容については確認しません。

サンプルの PAC ファイルが用意されています。サンプルファイルを使用するには、IWSVA-HOSTNAME を実際の IWSVA ホスト名で置き換えます。サンプル PAC ファイルは編集のみ可能で、削除することはできません。

ネットワーク設定

[ネットワーク設定] には、次の項目が含まれます。

- 381 ページの「ネットワークインタフェース」
- 381 ページの「Web コンソール」
- 382 ページの「リモート CLI」
- 383 ページの「SNMP の設定」
- 384 ページの「静的ルート」

ネットワークインタフェース

IWSVA では、プロキシ転送モードで HTTP トラフィックを処理する複数のネットワークインタフェースをサポートしています。サーバハードウェアには通常、複数のネットワークインタフェースがあり、IWSVA は、プロキシ転送の配信で複数のネットワークインタフェースを使用するように設定できます。

Web コンソール

初期設定で、IWSVA 管理コンソールへのアクセスは、ポート 8443 上の HTTP 接続を介して行われます。セキュリティを高めるため、セキュアソケットレイヤ接続 (HTTPS) の使用をお勧めします。Web コンソールへの接続は、Web コンソールの [管理] → [ネットワーク設定] → [Web コンソール] 画面で設定できます。

注意： Web コンソールの初期設定の秘密鍵に対する初期設定のパスワードは「adminIWSS85」です。
Web コンソールを非 SSL モードから SSL モードに変更する場合、証明書と秘密鍵のインポートは不要です。初期設定のパスワードを入力して処理を続行できます。

ブリッジモードでは、IWSVA は次のように指定されたポートを使用します。

- **非 SSL モード** — たとえば、セキュリティで保護されていない以下のような URL を使用して、IWSVA 管理コンソールにアクセスします。

  `http://<IWSVA サーバ IP アドレス：ポート>`

  - **ポート番号** — 初期設定は 1812 です。ファイアウォールで認識されている未使用のポートに変更することができます。
- SSL **モード** — 初期設定の推奨モードです。セキュリティで保護された、IWSVA 管理コンソールへの接続を有効にするには、このオプションを選択します。
  - SSL **証明書** — IWSVA で SSL をサポートするには、公開鍵と証明書が必要です。使用する証明書を指定し、IWSVA サーバにアップロードします。
  - SSL **パスワード** — SSL 証明書に関連付けられたパスワードがあれば入力します。
  - **ポート番号** — 初期設定は 8443 です。IWSVA 管理コンソールを開くために使用するポートを次のように入力します。

    `https://<IWSVA サーバ IP アドレス：ポート>`

リモート CLI

SSH（セキュアシェル）は、2 台のネットワークデバイスがセキュリティで保護された接続を介してデータを送受信することを可能にするネットワークプロトコルです。SSH は、パスワードなどのデータを平文で送信する Telnet に代わるものとして使用されています。IWSVA では、管理者は SSH を介してのみ遠隔地から CLI にアクセスできます。

[管理] → [ネットワーク設定] → [リモート CLI] 画面を使用して、リモート CLI アクセスのために IWSVA 上で SSH を設定します。

- SSH: コマンドラインアクセス — リモート CLI アクセスのための SSH 接続を有効にするには、このオプションを選択します。SSH サービスを無効にするには、このチェックボックスをオフにします。
- **ポート番号** — SSH のサービスポート番号を入力します。初期設定では、ポート番号は 22 です。

SNMP の設定

SNMP 通知は、IWSVA サービスの状況を監視するのに特に役立ちます。サービスが予期せず停止した場合、IWSVA が SNMP 通知を送信します。IWSVA は、IPv4 または IPv6 のいずれかのアドレスを使用して、トラップの宛先ネットワークの管理システムをサポートします。IWSVA では、以下のイベントに関する SNMP エージェントの通知をサポートしています。

- HTTP、FTP、および ICAP でのサービス停止
- ウイルスパターンファイル、IntelliTunnel パターンファイル、検索エンジン、および URL フィルタエンジンの各アップデート
- セキュリティイベント
- HA イベント

注意： IWSVA は、HTTP または FTP 検索サービスの停止を検出した場合、サービスの再開を 2 回試みます。それでもサービスを再開できない場合は、サービスが再開されるまで、指定しておいた宛先に 30 分ごとに SNMP 通知が発行されます。

注意： IWSVA は、SNMP バージョン 3 の SNMP 通知をサポートします。

システム情報の設定

必要なシステム情報はすべて、[管理] → [ネットワーク設定] → [SNMP の設定] 画面の [システム情報] で指定します。

[コミュニティ名] および [初期設定のコミュニティ] に指定するコミュニティは、SNMP オブジェクトが属するコミュニティを識別します。SNMP では、すべての管理対象オブジェクトがコミュニティに属します。これにより、コミュニティを指定して通信可能な SNMP エージェントを定義できるようになるため、最低限のセキュリティが確保されます。

アクセス管理設定

必要なアクセス管理情報はすべて、[管理] → [ネットワーク設定] → [SNMP の設定] 画面の [アクセス管理の設定] で指定します。

IWSVA が簡単なステータスメッセージやアラートメッセージを送信するため、このセクションのフィールドは読み取り専用です。[読み取り専用オブジェクト ID (OID)] のオブジェクト ID (OID) は、特定のメッセージ、アラート、またはアラームのコードです。「オブジェクト」とは、実際のメッセージ、アラート、またはアラームです。

静的ルート

[管理] → [ネットワーク設定] → [静的ルート] では静的ルートを設定および配信します。IPv4 と IPv6 の両方のアドレスルートがサポートされています。Web UI は、IPv4 と IPv6 の両方のアドレス形式を同様に受け入れます。

> **注意：** 静的ルートは、配信中に追加したり、[管理] → [配置ウィザード] を使用して変更したりすることができます。

以下では、この画面上のオプションを簡単に説明しています。

追加 — [静的ルートの追加] 画面を開きます。この画面では、新しい静的ルートを作成できます。最大で 50 の静的ルートを追加できます。

- 静的ルートをインタフェースにバインドする場合、ルータ設定がインタフェースと同じネットワークセグメントにある必要があります。
- 静的ルートをポートにバインドする場合、ルータ設定がポートと同じネットワークセグメントにある必要があります。

削除 — 静的ルートをリストから削除します。

ネットワーク ID — 設定を編集するにはネットワーク ID をクリックします。

ネットマスク — このルート用のルータのサブネットマスクを表示します。

ルータ — このルート用のルータの IP アドレスを表示します。

インタフェース — このルートにバインドするインタフェースを表示します。

配信ステータス — 静的ルートが正常に配信されたかどうかを表示します。

必要な設定をすべて指定してから、[配信] をクリックします。

静的ルートを設定する

静的ルートを設定するには

次の項目を指定します。

- **ネットワーク ID** — 宛先のネットワーク ID またはホスト ID を入力します。
- **ネットマスク** — サブネットマスクを入力します。
- **ルータ** — このルートのルータ (次のホップ) の IP アドレスを入力します。
- **インタフェース** — このルートにバインドするインタフェースを選択します。ルータ設定は、バインド元インタフェースと同じネットワークセグメント内にある必要があります。

管理コンソール

[管理コンソール] 画面では、admin アカウントがログインアカウントを追加または削除できます。ログインアカウントは、Web コンソールの [管理] → [管理コンソール] → [アカウント管理] 画面で設定できます。

管理コンソールには、次のオプションが用意されています。

- 385 ページの「役割ベースの管理」
- 386 ページの「役割の管理」
- 389 ページの「アカウント管理」
- 392 ページの「アクセス管理の設定」

役割ベースの管理

IWSVA Web コンソールへのアクセスを許可および制御するには、役割ベースの管理を使用します。組織内に IWSVA 管理者が複数いる場合は、この機能を使用して Web コンソールの権限を管理者に個別に割り当て、特定のタスクの実行に必要なツールと権限のみを付与できます。1 つ以上のドメインを管理対象として割り当てることにより、エージェントツリーへのアクセスを制御することもできます。さらに、Web コンソールへの「閲覧のみ」のアクセス権を管理者以外のユーザに付与できます。

各ユーザ (管理者または非管理者) に特定の役割が割り当てられます。役割とは、Web コンソールへのアクセスレベルを定義するものです。ユーザは、カスタムユーザアカウントまたは Active Directory アカウントを使用して Web コンソールにログオンします。

役割ベースの管理には、次のタスクがあります。

1. ユーザの役割を定義します。詳細については、386 ページの「役割の管理」を参照してください。
   - ユーザアカウントを設定し、各ユーザアカウントに特定の役割を割り当てます。詳細については、389 ページの「アカウント管理」を参照してください。

役割の管理

役割の管理により、必要に応じて役割を追加または削除できます。これらの役割には次のものがあります。

- **管理者** — システムへの制限のない完全なアクセスが許可されます。コンソールからアクセスして、ユーザアカウントの作成、削除、変更を含む設定の読み取り、変更が可能です。管理者権限を持つユーザは、SSH 接続を介して IWSVA にログインできます。これは新規ユーザの初期設定アクセスレベルです。
- **監査担当者** — 設定の変更はできませんが、設定、ログ、およびレポートの表示と、自身のパスワードの変更はできます。
- **レポート専用** — システムステータスと予約レポートの閲覧のみ可能です。ログ、およびリアルタイムのレポートクエリを生成できます。また、自分のパスワードを変更できます。
- **カスタムの役割** — 一部あるいはすべての管理ドメインに対する完全なアクセス、読み取り専用、またはアクセスなしで、手動で追加されます。ユーザは、自身の役割に割り当てられたアクセス権に基づいてさまざまなページを変更または表示できます。

詳細については、385 ページの「役割ベースの管理」を参照してください。

メニュー項目の権限

ユーザの役割により、ユーザがアクセス可能な Web コンソールのメニュー項目が決まります。役割には各メニュー項目の権限が割り当てられています。

権限は各メニュー項目へのアクセスレベルを決定します。メニュー項目の権限は次のいずれかに設定できます。

- **フルアクセス**: メニュー項目への完全なアクセスが許可されます。ユーザはメニュー項目ですべての設定およびタスクを実行し、データを表示することができます。
- **読み取り専用**: メニュー項目の設定、タスク、およびデータを表示することのみが許可されます。
- **アクセスなし**: メニュー項目を非表示にします。

管理メニュー項目のアクセス

次の表に、管理者が利用できるメニュー項目のリストを示します。

表 14-2. 管理メニュー項目

管理ドメイン	メニュー項目
ステータス監視	• システムステータス • ダッシュボード
ポリシー管理	• アプリケーション制御 • HTTP • FTP
ログ	• ログ分析 • お気に入りログ • 設定
レポート	• 選択されたユーザ / グループのレポート
システム管理	• アップデート • 通知 • 管理 **注意：** 組み込みの管理者アカウント (Admin) を使用するユーザのみが、ユーザアカウントおよびユーザの役割にアクセスできます。

組み込みのユーザの役割

IWSVA には一連の組み込みのユーザの役割が用意されており、これらを変更または削除することはできません。組み込みの役割は次のとおりです。

表 14-3. 管理メニュー項目

管理ドメイン	説明
管理者	ユーザには、システムへの制限のないアクセスが許可されます。コンソールからアクセスして、ユーザアカウントの作成、削除、変更を含む、設定の読み取り、変更が可能です。管理者は、このアカウントとパスワードを使用して CLI にログインできます。これは新規ユーザの初期設定アクセスレベルです。
監査担当者	設定変更はできませんが、設定、ログ、レポートの閲覧が可能です。自分のパスワードを変更することもできます。
レポート専用	ダッシュボードと予約レポートの閲覧のみ可能です。ログやリアルタイムのレポートクエリを生成します。

注意： 管理者権限を持っているアカウントは、SSH 経由でターミナルコンソールにログインして CLI を使用できます。また、CLI からシェルに root でログインすることもできます。

カスタムの役割

要件を満たす組み込みの役割がない場合、カスタムの役割を作成できます。組み込みの管理者の役割を持つユーザのみが、カスタムのユーザの役割を作成して、その役割をユーザアカウントに割り当てることができます。

カスタムの役割の追加

カスタムの役割を追加するには

1. メインメニューから、[管理] → [管理コンソール] → [役割の管理] の順にクリックします。
2. [追加] をクリックします。
   新しい画面が表示されます。
3. 役割の名前およびオプションで説明を入力します。

4. [役割の権限] で各管理ドメインのアクセス権を選択します。アクセスの詳細については、387 ページの「管理メニュー項目のアクセス」を参照を参照してください。
5. [保存] をクリックします。

新しい役割が役割リストに表示されます。

カスタムの役割の変更

カスタムの役割を変更するには

1. メインメニューから、[管理] → [管理コンソール] → [役割の管理] の順にクリックします。
2. 役割の名前をクリックします。
   新しい画面が表示されます。
3. 次のいずれかを変更します。
   - 役割の名前
   - 役割の説明 (任意)
   - 役割の権限 : 各管理ドメインのアクセス権を変更します。
4. [保存] をクリックします。

カスタムの役割の削除

カスタムの役割を削除するには

1. メインメニューから、[管理] → [管理コンソール] → [役割の管理] の順にクリックします。
2. 削除する役割を選択します。
3. [削除] をクリックします。
   確認メッセージが表示されます。
4. [OK] をクリックします。

アカウント管理

アカウント管理を使用して、アカウントの追加および削除を実行できます。アカウント管理では、既存のすべてのアカウントをユーザ名と説明とともに表示し、役割を割り当てます。

ログインアカウント

[ログインアカウント] 画面では、ログインアカウントの情報がすべて表示されます。

- 新規ログインアカウントを作成するには [追加] をクリックします。既存のアカウントを編集するにはユーザ名をクリックします。
- ログインアカウントを削除するには、ログインアカウントと関連のあるチェックボックスをオンにしてから、[削除] をクリックします。
- **ユーザ名** — ログインアカウントに割り当てられたユーザの名前。
- **パスワード** — 安全なパスワードを入力して確認します。
- **説明** — ログインアカウントの簡単な説明。
- **役割** — ユーザアカウントに割り当てられた役割。386 ページの「役割の管理」を参照してください。

ログインアカウントは、Web コンソールの [管理] → [管理コンソール] → [アカウント管理] 画面で設定できます。

割り当てられたアクセス権を使用して、最大 128 のユーザが IWSVA にアクセスできます。アプリケーション内で、ユーザは設定変更を行うことができ、その変更は監視ログに記録されます (365 ページの「監査ログ」を参照)。

各セキュリティ管理者の責任範囲が異なる場合、各々に異なる権限を付与できることは組織にとって有用です。IWSVA の管理では、このようにさまざまなユーザが、権限が異なるさまざまなログオン認証情報を持つことができます。

アクセス権により、IWSVA で加えられている変更内容を監査することができます。特定の政府機関の標準に準拠する必要がある場合、この機能は重要になります。

ログインアカウントを追加する

ログインアカウントを追加するには

1. メインメニューから [管理] → [管理コンソール] → [アカウント管理] の順に選択します。
2. [アカウント管理] 画面で、[追加] をクリックします。
3. [ログインアカウント] 画面で、必要な情報を入力します。
   - [**ローカルアカウント**] **または** [LDAP **アカウント**] — アカウントの種類を選択します。

注意： IWSVA Web コンソールで LDAP が設定されていない場合、[LDAP アカウント] オプションは無効になります。

[LDAP アカウント] を選択すると、[ユーザ名] と [パスワード] が無効になり、代わりに LDAP アカウント情報が使用されます。

- **ユーザ名** — ログインアカウントに割り当てられたユーザの名前。
- **パスワード** — 4 ～ 32 文字の英数字で指定する必要があります。辞書に掲載されている語句、名前、日付は避けます。
- **説明** — ログインアカウントの簡単な説明。
- **役割** — ドロップダウンリストから役割を選択します。388 ページの「組み込みのユーザの役割」を参照してください。

4. [保存] をクリックします。

   [アカウント管理] 画面に、新しいログインアカウントが表示されます。

ログインアカウントを変更する

ログインアカウントを変更するには

1. メインメニューから [管理] → [管理コンソール] → [アカウント管理] の順に選択します。
2. 対象のユーザ名をクリックします。
3. [ログインアカウント] 画面で、必要な情報を変更します。
   - **パスワード** — 4 ～ 32 文字の英数字で指定する必要があります。辞書に掲載されている語句、名前、日付は避けます。
   - **説明** — ログインアカウントの簡単な説明。
   - **役割** — ドロップダウンリストから役割を選択します。388 ページの「組み込みのユーザの役割」を参照してください。
4. [保存] をクリックします。

   [ログインアカウント] 画面に、変更されたログインアカウントが表示されます。

注意： 管理者アカウントが SSH 経由でターミナルコンソールにログインしてセッションを閉じていない場合は、管理者が直接そのアカウントを「監査者」または「レポート閲覧のみ」に変更することはできません。警告メッセージが表示されます。

アクセス管理の設定

管理者は、アクセスコントロールリスト (ACL) を設定して、管理コンソール (Web コンソール、CLI、PING 要求など) や特定の IP アドレス、IP アドレス範囲へのアクセスを制限できます。

ACL は、IPv4 と IPv6 の両方のアドレスをサポートしています。単一のアドレス、アドレス範囲、またはネットワークマスクを使用して、ルールを設定できます。

管理 ACL (初期設定では無効) を使用すると、ユーザは IWSVA 管理コンソールにアクセスできます。管理者は、1 つ以上の IP アドレスを管理 ACL に追加できます。管理 ACL に追加された IP アドレスは、個々に削除することもできます。リストが有効な場合、管理者は、許可された IP アドレスのリストに表示される IP アドレスからのみ IWSVA 管理コンソールに接続できます。

注意： IWSVA で登録されている中心的なマネージャ (Trend Micro Control Manager など) の IP アドレスをアクセスリストに追加し、その IP アドレスが適切に機能し、IWSVA の必要なデータにアクセスできるようにします。

管理コンソールのアクセス管理リストを有効にして設定するには

1. [管理] → [管理コンソール] → [アクセス管理の設定] の順に選択します。
2. 次のオプションのいずれかを選択します。
   - IP **アドレス** — 単一の IP アドレスを管理 ACL に追加します
   - IP **範囲** — IP アドレスの範囲を管理 ACL に追加します
   - IP **マスク** — ネットワークセグメントのすべての IP アドレスを管理 ACL に追加します

   注意： 20 を超えるエントリは管理 ACL に追加できません。
3. [追加] をクリックし、エントリを許可リストに追加します。
4. [クライアント IP に基づく管理者アクセスを有効にする] チェックボックスをオンにします。

   注意： この機能を有効にする前に、1 つ以上の IP アドレスを管理 ACL に追加する必要があります。許可された IP アドレスのリスト内のユーザのみが、管理コンソールにアクセスできます。
5. [保存] をクリックします。
6. エントリを削除するには、削除するエントリの行の [削除] アイコンをクリックし、[保存] をクリックして削除を確認します。

Syslog サーバ

Syslog サーバが設定されている場合、Syslog サーバにログをリダイレクトできます。Syslog サーバは IWSVA から追加、編集、または削除できます。

Syslog サーバを設定するには

1. [ログ] → [ログ設定] の順に選択します。
2. Syslog サーバで [追加] をクリックします。既存の Syslog サーバを編集するには、[Syslog サーバ名] をクリックします。
3. [Syslog を有効にする] をクリックします。
4. サーバ名または IP アドレスを指定します。
5. UDP ポートを指定します。
6. ログの種類または優先度を示します。
7. [保存] をクリックします。

設定のバックアップと復元

[設定のバックアップ / 復元] 画面では、バックアップ用の IWSVA 設定ファイルを生成できます。また、この画面から、次のトレンドマイクロ製品の設定情報とポリシー情報を IWSVA 6.5 SP3 に移行できます。

- IWSVA 6.5 SP2
- IWSVA 6.5 SP3

IWSVA は、完全な移行と部分的な移行の両方をサポートしています。完全な移行を実行すると、システムやアプリケーションの設定を復元したり、現在の設定を交換用の IWSVA コンピュータに適用したりできます。部分的な移行を実行すると、ポリシーレベルやアプリケーションレベルの設定を置き換えることができます。移行されない情報の詳細については、「インストールガイド」の「移行されない情報」を参照してください。

注意： 1. 完全な移行を実行するには、配信モード、IP アドレス、およびネットワークカードが 2 台の IWSVA コンピュータ上で同じである必要があります。
2. 完全な移行や部分的な移行を実行しても、OS 設定、システムパッチ情報、およびパターンファイルはアップデートされません。
3. 高可用性モードの IWSVA では、部分的な移行のみがサポートされます。

システムアップデート

IWSVA はシステムのアップデートをサポートしていませんが、次のトレンドマイクロの最新版ダウンロードサイトからシステムアップデートを入手できます。
https://www.trendmicro.com/ja_jp/business/products/downloads.html

システムアップデートには以下の 2 種類があります。

- アプリケーションパッチ
- OS のアップデート

どちらも同じ方法で扱うことができ、[管理] → [システムアップデート] 画面の [履歴] に表示できます。このユーティリティでは、正しくフォーマットされ、暗号化されたトレンドマイクロのアップデートのみアップロードできます。

システムアップデートをインストールするには

1. 次のトレンドマイクロの最新版ダウンロードサイトから最新のアップデートを入手します。
   `https://www.trendmicro.com/ja_jp/business/products/downloads.html`
2. [管理] → [システムアップデート] に移動します。
3. [参照] をクリックして、ダウンロードしたファイルを選択します。
4. [アップロード] をクリックします。
5. [概要] 画面で、[インストール] をクリックします。
6. 正常にインストールされたことを示すメッセージを受け取ったら、別の画面に移動できます。

注意： アプリケーションパッチを削除する手順については、418 ページの「アプリケーションパッチの適用またはアプリケーションパッチの削除」を参照してください。

警告： **他のソースからのアップデートファイルは、IWSVA サーバに適用しないでください。**

注意： アップデート後に、IWSVA サーバは再起動することがあります。

システムのメンテナンス

メンテナンスを目的としてシステムをシャットダウンまたは再起動するには、[管理] → [システムのメンテナンス] の順に選択します。実行した操作は、監査ログとシステムイベントログに記録されます。

終了 — IWSVA アプライアンスをオフにしてサービスを停止するには、このオプションを選択します。

再起動 — IWSVA サービスまたはシステムを再起動するには、このオプションを選択します。システムの再起動中は IWSVA サービスを使用できません。

コメント — 実行しようとしている操作の理由を入力します。このフィールドを空白のままにすることはできません。このフィールドに入力した情報はログに記録されます。

システムイベントログ

システムイベントログには、システムで発生する状態の変化やエラーに関する情報が含まれます。次のような種類のイベントが記録されます。

- アップデート
- 製品の登録
- 製品のメンテナンス

システムイベントログを表示するには

1. 管理コンソールから [管理] → [システムイベントログ] の順に選択します。
2. [期間] で期間を選択します ([すべて]、[今日]、[過去 7 日間]、[過去 30 日間])。

   任意の期間を選択するには、[範囲] をクリックし、開始と終了の日付を選択します。
3. [レベル] で、ログエントリを表示するイベントレベルを選択します。[追加] をクリックします。リストにあるすべてのスパイウェアを追加する場合は、[すべて追加] をクリックします。

   イベントレベルを右側のリストボックスから削除するには、[削除] をクリックします。リストにあるすべてのレベルを削除する場合は、[すべて削除] をクリックします。
4. [並べ替え基準] で、ログの並べ替えの基準とする項目を選択します。[サーバ]、[日付]、[レベル]、[送信元] のオプションがあります。
5. [ログ表示] をクリックします。[システムイベントログ] 画面が開きます。
6. 表示を更新するには、[表示更新] をクリックします。

製品ライセンス

製品ライセンス機能を使用して、IWSVA の登録およびライセンス確認を実行できます。IWSVA の完全なアクティベーションプロセスは、2 つの手順で構成されます。まず、トレンドマイクロに IWSVA を登録する必要があります。登録後、製品の使用を許可する有効な IWSVA アクティベーションコード (AC) が提供されます。

トレンドマイクロ製品に対するライセンスには通常、購入日から 1 年間のみ、製品のアップデート、パターンファイルのアップデート、および基本的なテクニカルサポート (「サポート契約」) を得る権利が含まれます。

IWSVA をアクティベートするには、まず、製品の登録時に取得するレジストレーションキーが必要です。これを使用してアクティベーションコードを取得できます。配置ウィザードを使用して、または後で IWSVA 管理コンソールを使用して、IWSVA をアクティベートできます。

ライセンス期限切れの警告

通常、サポート契約の有効期限が切れる 90 日前から、期限切れが近付いていることを警告するメール通知を受信し始めます。サポート契約の更新については、販売代理店またはトレンドマイクロの営業担当にお問い合わせください。以下のトレンドマイクロオンライン登録の URL からも更新できます。

https://clp.trendmicro.com/fullregistration

注意： サポート契約の更新については、トレンドマイクロの営業担当または販売代理店にお問い合わせください。[管理] → [製品ライセンス] で [ステータス更新] をクリックし、[製品ライセンス] 画面でサポート契約の有効期限を手動で更新します。

レジストレーションキーの取得

レジストレーションキーは、以下の場所にあります。

- Trend Micro Enterprise Solution DVD
- ライセンス証明書 (製品の購入後に取得)

次の機能をご利用いただくために、お客さまのレジストレーションキーを登録およびアクティベートしていただく必要があります。

- IWSVA パターンファイルおよび検索エンジンのアップデート

- テクニカルサポート
- ライセンスの有効期限の更新、登録、および詳細情報の表示

レジストレーションキーは 31 文字であり、以下のようになります。

```
xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
```

アクティベーションコードの取得と入力

[製品ライセンス] 画面では、製品ライセンスの更新手順やステータスを確認できます。

IWSVA をアクティベートするには、アクティベーションコードが必要です。

アクティベーションコードは 31 文字であり、以下のようになります。

```
xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
```

ライセンスの更新

Web から最新のライセンスを取得するには、[管理] → [製品ライセンス] に移動して、[ステータス更新] をクリックします。

更新の詳細については、次を参照してください。
https://www.trendmicro.com/ja_jp/buy/renewal.html

サポート契約の更新

トレンドマイクロまたは販売代理店では、すべての登録済みユーザに対して、テクニカルサポート、ウイルスパターンファイルのダウンロード、およびプログラムのアップデートを 1 年間提供します。この期間を過ぎると、サポート契約を更新する必要があります。

サポート契約の有効期限が切れても検索はできますが、ウイルスパターンファイルおよびプログラムのアップデートはできません。アップデート不能にならないように、できるだけ早くサポート契約を更新してください。

- サポート契約を更新するには、製品をお買い上げいただいた購入元にお問い合わせください。契約期間を 1 年間延長したサポート契約は、登録プロファイルに表示される企業の担当者宛てに郵送されます。
- 企業の登録プロファイルを表示または変更するには、次のトレンドマイクロオンライン登録の Web サイトからアカウントにログインします。

  https://clp.trendmicro.com/fullregistration

サポート情報

IWSVA では、ケース診断ツール (CDT) を使用して、プロセスが異常終了したときのメモリ内のシステムデータを含むコアおよびシステム情報ファイルを収集します。[システム情報ファイルの生成] ボタンはこの機能を拡張したもので、クリックすると現在のコンピュータの「状態」をパッケージ化することができます。

IWSVA によって収集されるコアおよびシステム情報ファイルには次の情報が含まれます。

- **IWSVA 情報** — IWSVA 製品バージョン、検索エンジンのバージョン、ビルド番号、および IWSVA HotFix と Service Pack の情報。製品設定および統合設定もこの情報に含まれます。
- **IWSVA/ システムログ** — IWSVA ログとデバッグログ、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の場合)、およびコアダンプファイル。
- **システム / ネットワーク情報** — ハードウェア設定、OS、ビルド、システムリソースのステータス、他のインストール済みアプリケーション、およびネットワーク情報。
- **CDT 対応設定 / プラグイン情報** — Contorl Manager または MCP エージェントなどの新しいコンポーネントを IWSVA に追加したことによる、CDT への変更に関する情報。
- **デバッグログ** — IP フィルタを使用して作成されたデバッグログ。

ネットワークパケットの取り込み

ネットワークパケットの取り込みウィザードは、[管理] → [サポート情報] | [ネットワークパケットの取り込み] タブにあります。取り込まれたネットワークパケットを使用して、管理者またはサポートチームは、トラフィックのデバッグまたは分析を実行できます。

この機能を使用すると、管理者は単一のネットワークインタフェースからネットワークパケットを取り込むか、または複数のネットワークインタフェースから同時にネットワークパケットを取り込むかを選択できます。取り込みが始まると、経過した時間が表示されます。管理者が [取り込みの停止] をクリックするか、または (初期設定の) 最大ファイルサイズである 10GB に達すると、取り込み操作は停止します。

各インタフェースのパケットの取り込みは、「capture-{interface}-{date:time}.pcap」の命名規則を使用して個別のファイルに保存されます。たとえば、2011 年 11 月 1 日に実行された eth0 ネットワークインタフェース上のパケットの取り込みの名前は、「capture-eth0-20111101:31:31;01.pcap」となります。

ネットワークパケットの取り込みが完了すると、すべてのパケットの取り込みファイルは「capture-{date}.tgz」という名前の 1 つの圧縮パッケージファイルに保存されます。このファイルはダウンロード可能なリストの形で表示されます。管理者は圧縮ファイルをダウンロードすることも、削除することもできます。

ネットワークパケットの取り込みの使用

管理者は、選択したインタフェースまたは単一インタフェースのパケットの取り込みを可能にするこの機能を使用してトラフィックを分析できます。

ネットワークパケットを取り込むには

1. [管理] → [サポート情報] 画面に移動して、[ネットワークパケットの取り込み] タブをクリックします。
2. [使用可能] 列から適切なインタフェースを選択します。
3. [追加] または [すべて追加] をクリックして、選択したインタフェースを [選択済み] 列に移動します。
4. 必要に応じて、[削除] または [すべて削除] をクリックして、[選択済み] 列からインタフェースを削除します。
5. [取り込みの開始] をクリックします。経過時間が表示されます。最大ファイルサイズの 10GB に達すると、取り込みは停止します。
6. 必要に応じて、[取り込みの停止] をクリックして、最大ファイルサイズに達する前にパケットの取り込みを停止できます。
7. 取り込みが終了したら、適切な生成ファイルを選択するか、すべてを選択します。
8. 処理を選択します。
   - [ダウンロード] をクリックして参照し、取り込みファイルをディレクトリに保存します。
   - [削除] をクリックして、生成されたファイルを削除して、[OK] をクリックします。

デバッグログ

デバッグログでは、ローカルコンピュータおよびそのコンピュータにログオンしているユーザに、グループポリシーやその拡張子を使用して適用されたすべての変更と設定を追跡します。デバッグログを有効にすると、デバッグログにレジストリキーが追加されます。

デバッグログを有効にするには

1. デバッグログで追跡する IP アドレスまたは IP 範囲を入力します。
2. [選択済み] ボックスにエントリを追加します。

3. [取り込みの開始] をクリックします。
4. ダウンロード対象の生成済みデバッグログの種類を 1 つ選択します。
5. ログを削除するか、今後の評価のためにコンピュータにダウンロードするかを選択します。

配信診断

トレンドマイクロのサポートサービスを利用して配信の問題の原因を診断する場合は、配信診断ファイルを使用します。

IWSVA でシステムファイルの生成中に、すべての診断情報の収集の妨げになる状況がアプリケーションで発生することがあります。この場合、IWSVA では、利用可能な情報を収集し、発生したエラーを包括的なメッセージとともにログファイルに記録します。このメッセージは、削除することも、今後評価するためにコンピュータにダウンロードすることもできます。

第 15 章

IWSVA のテストと設定

Trend Micro InterScan Web Security Virtual Appliance（以下、IWSVA）コンソールを開いてから、次のテストを実施してプログラムが正しく動作していることを確認します。この章で説明するテストは次のとおりです。

EICAR テストファイル

European Institute for Computer Antivirus Research (EICAR) は、ウイルス対策アプライアンスをテストするためのテストウイルスを開発しました。このスクリプトは、不活性のテキストファイルです。ほとんどのウイルス対策ベンダーから提供されるウイルスパターンファイルには、バイナリパターンが含まれています。このテストウイルスは、ウイルスではないため、プログラムコードは含まれていません。

警告： インターネットの安全性をテストするために実際のウイルスは使用しないでください。

EICAR テストウイルスは、次の URL からダウンロードできます。

https://secure.eicar.org/eicar.com

または、テキストファイルに次の内容を入力またはコピーして、そのファイルに「eicar.com」という名前を付けることによって、独自の EICAR テストウイルスを作成できます。

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

注意： テストの前に、URL キャッシュ ([HTTP] → [設定] → [WRS/URL キャッシュ])、コンテンツキャッシュ ([HTTP] → [設定] → [コンテンツキャッシュ])、およびローカルブラウザを消去します。いずれかのキャッシュにテストウイルスのコピーが保存されていると、ファイルをダウンロードしようとする際インターネットからではなくキャッシュからファイルを読み込もうとして、IWSVA によりファイルが検出されない場合があります。

Web レピュテーションのテスト

IWSVA の Web レピュテーション機能をテストするには、Web ブラウザを開いて、アドレスフィールドに次のように入力します。

```
http://wrs21.winshipway.com
```

テストが正常に実行されると、「この URL には、企業ポリシーに基づいてアクセスを禁止する Web セキュリティレーティングが設定されています。」という IWSVA セキュリティイベントが表示されます。

アップロード検索のテスト

ウイルスのアップロードをテストするには、次の手順に従います。

1. IWSVA コンソールの管理コンソールで [HTTP] → [高度な脅威保護] → [ポリシー] の順に選択します。[ウイルス検索を有効にする] をオフにしてから [保存] をクリックします。
2. 次の Web サイトからテストウイルス (eicar.com) をダウンロードします。

   `http://www.eicar.org/download/eicar.com.txt`
3. ダウンロードしたテストウイルスをローカルコンピュータに保存します。
4. IWSVA コンソールをもう一度開き、管理コンソールで [HTTP] → [高度な脅威保護] → [ポリシー] の順に選択します。[ウイルス検索を有効にする] チェックボックスをオンにして、[保存] をクリックします。
5. テストウイルスを Web サイトにアップロードします。図 15-1 に示すようなメッセージがブラウザに表示されます。

図 15-1. EICAR テストウイルスを検出したことを示す警告画面

HTTPS 復号化検索のテスト

この項では、スタンドアロンモードの IWSVA で HTTPS 復号化をテストする手順について説明します。

復号化された HTTPS トラフィックのウイルス検索をテストするには

1. Web クライアントの HTTP プロキシが IWSVA を使用するように設定します。たとえば、Internet Explorer を開き、[ツール] → [インターネット オプション] → [接続] → [LAN の設定] → [LAN にプロキシ サーバーを使用する] の順に選択します。
2. IWSVA Web コンソールを開いて、[HTTP] → [HTTPS 復号化] → [設定] の [サーバ証明書の検証] で、すべてのオプションがオンになっていることを確認します。
3. [HTTP] → [HTTPS 復号化] → [ポリシー] の順に選択し、[HTTPS 復号化を有効にする] をオンにします。
4. [追加] をクリックして、新しい HTTPS 復号化ポリシーを作成します。[カテゴリの指定] で、[一般] の [コンピュータ / インターネット] を選択します。
5. クライアントコンピュータから、次の URL を使用してテストウイルスファイルにアクセスします。

   ```
   https://secure.eicar.org/eicar.com
   ```

6. セキュリティ警告画面が表示されます。警告メッセージは、URL フィルタも有効か無効かによって異なります。

図 15-2. URL フィルタが無効な場合のセキュリティ警告画面

図 15-3.　URL フィルタも有効な場合のセキュリティ警告画面

管理コンソールの [ログ] → [ログ分析] → [インターネットセキュリティ] にて URL フィルタによるブロック情報を確認できます。

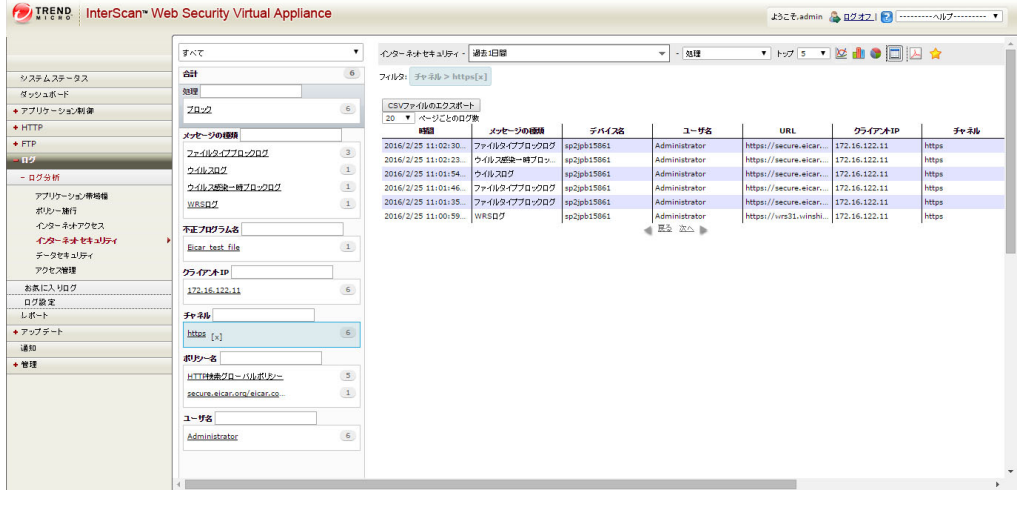


図 15-4.　インターネットセキュリティログ画面の HTTPS 復号化テストのログ (URL フィルタが無効な場合)

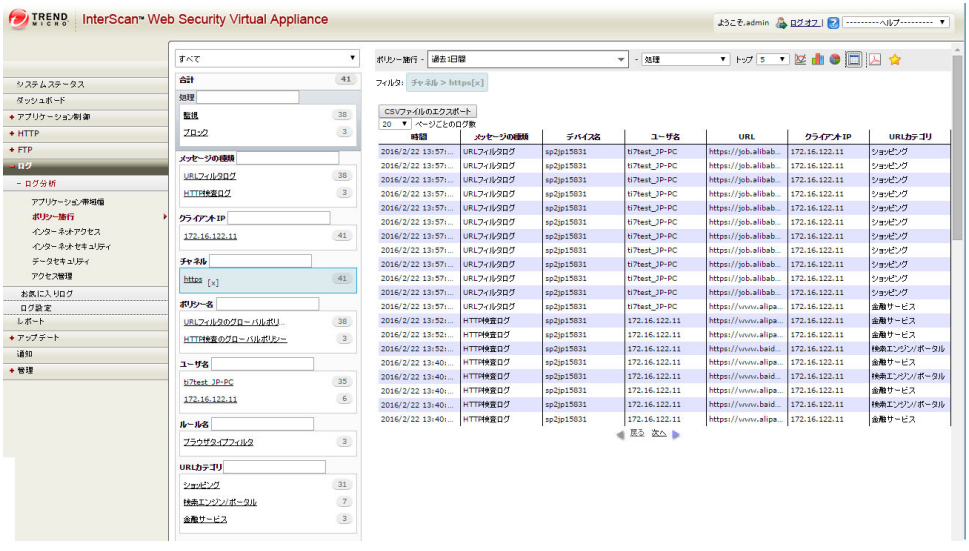


図 15-5. ポリシー施行ログ画面の HTTPS 復号化テストのログ (URL フィルタが有効な場合)

FTP 検索のテスト

スタンドアロンモードで FTP ウイルス検索機能をテストするには、次の手順に従います。

FTP トラフィックのウイルス検索をテストするには

1. 次のページからテストウイルスをダウンロードします。

   http://www.eicar.org/download/eicar.com.txt

2. FTP プロキシとして動作する IWSVA を介して FTP サーバにアクセスします。

   たとえば、IWSVAFTP プロキシサーバの IP アドレスが 10.2.203.126、FTP サーバの IP アドレスが 10.2.202.168 であるとします。
   コマンドラインプロンプトを開き、次のように入力します。

   ```
   ftp 10.2.203.126
   ```

3. user@host としてログオンします。たとえば、FTP アカウント名が anonymous で FTP サーバの IP アドレスが 10.2.202.168 の場合は、anonymous@10.2.202.168 としてログオンします。

4. 次のコマンドを入力して、テストウイルス (例 : eicar_com.zip) をアップロードします。

   ```
   put eicar_com.zip
   ```

5. IWSVA の FTP プロキシモード設定が完了したら、図 15-6 に示すようなメッセージが表示されます。

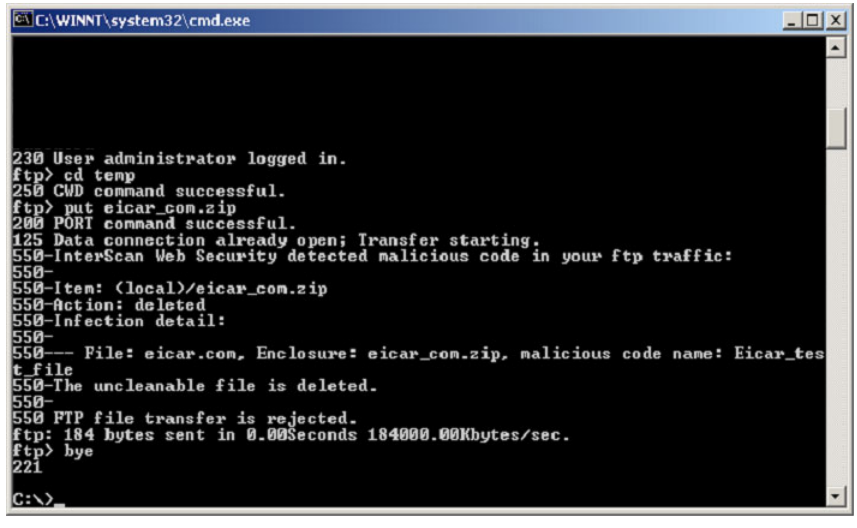


図 15-6. eicar_com.zip **でウイルスが検出されたことを示す警告メッセージ**

アプリケーション制御のテスト

アプリケーション制御機能を使用するには、IWSVA をプロキシ転送モード、透過ブリッジモード、または透過ブリッジモード - 高可用性で配信する必要があります。

次の手順を使用すると、アプリケーション制御グローバルポリシーを変更して、エンドユーザによる Google Web サイトへのアクセスをブロックできます。

アプリケーション制御をテストするには

1. IWSVA コンソールを開き、[アプリケーション制御] → [ポリシー] に移動します。
2. [アプリケーション制御を有効にする] チェックボックスをオンにして、[保存] をクリックします。
3. [アプリケーション制御グローバルポリシー] 名をクリックして変更します。
4. 次の 2 つの方法のいずれかを使用して、Google プロトコルを検索します。

a. [アプリケーション検索] フィールドに「Google」と入力して、[検索] ボタンをクリックします。

   検索結果で、Web カテゴリに「Google」とリストされます。

b. Web カテゴリを下にスクロールして、カテゴリを展開し、エントリから Google を探します。

5. Web サイトのカテゴリ名の右側の列で、処理のドロップダウンメニューから、[ブロック] の処理を選択します。
6. [スケジュール] で予約期間のいずれかのオブジェクトを選択します。
7. [適用] をクリックします。
8. [保存] をクリックして、[アプリケーション制御ポリシー] 画面に戻ります。
9. [ポリシーの配信] をクリックして、更新後のポリシーを配信します。
10. ブラウザを開き、http://www.google.com へのアクセスを試行します。

    ブラウザに、アプリケーション制御ポリシー侵害を確認する通知メッセージが表示されます。

HTTP 検査のテスト

この手順を使用して、HTTP 検査ブラウザタイプフィルタをテストします。このフィルタは一致する FireFox ブラウザから送信される要求を識別します。

HTTP 検査をテストするには

1. IWSVA コンソールを開き、[HTTP] → [HTTP 検査] → [ポリシー] の順に選択します。
2. [HTTP 検査を有効にする] チェックボックスをオンにして、[保存] をクリックします。
3. [HTTP 検査のグローバルポリシー] 名をクリックして、変更するポリシーにアクセスします。
4. HTTP 検査フィルタのリストの上にある処理のドロップダウンメニューから、[ブロック] の処理を選択します。
5. [スケジュール] で予約期間のいずれかのオブジェクトを選択します。
6. [適用] をクリックします。
7. [保存] をクリックして、[HTTP 検査ポリシー] 画面に戻ります。
8. [ポリシーの配信] をクリックして、更新後のポリシーを配信します。
9. FireFox ブラウザを使用して、http://www.google.com などの http:// URL にアクセスしてみます。図 15-7 に示すような通知メッセージがブラウザに表示されます。

図 15-7. HTTP **検査のポリシー侵害通知**

URL 監視のテスト

URL フィルタの監視機能をテストする前に、Web クライアントの HTTP プロキシが IWSVA を使用するように設定する必要があります。

URL フィルタをテストするには

1. IWSVA Web コンソールを開き、[HTTP] → [設定] → [カスタムカテゴリ] の順に選択し、次の URL 用の新しいカテゴリ「monitor」を作成します。

   ```
   http://www.download.com
   ```

2. [HTTP] → [URL フィルタ] → [ポリシー] の順にクリックし、[URL フィルタを有効にする] をオンにし、[URL フィルタのグローバルポリシー] 名をクリックしてポリシーにアクセスし、編集します。

3. [カスタムカテゴリ] の [monitor] と、[コミュニケーション / メディア] の [検索エンジン / ポータル] のチェックボックスをオンにし、[監視] を選択して [適用] をクリックします。

図 15-8.　URL 監視のテストのための [ルール] 画面の設定

4. このポリシーを保存して配信します。

5. クライアントコンピュータから次の Web サイトにアクセスします。

   ```
   http://www.download.com
   ```

```
http://www.google.com
http://www.yahoo.com
```

これで、警告メッセージが表示されずに Web サイトにアクセスできるようになるはずです。URL フィルタログをクエリおよび表示するには、IWSVA Web コンソールにアクセスして [ログ] → [ログ分析] → [ポリシー施行] の順にクリックします。

ダウンロード検索のテスト

HTTP または FTP over HTTP を使用したダウンロード時のウイルス検索をテストするには、次の Web サイトからテストウイルスをダウンロードします。

http://www.eicar.org/download/eicar.com.txt

図 15-9. システムが正しくセットアップされている場合に表示されるウイルス警告画面

クライアントが感染ファイルをダウンロードしようとすると、IWSVA は初期設定で、そのサイトへの他のユーザのアクセスを 4 時間ブロックします。その後も、他のクライアントがウイルスを含む同じ URL にアクセスしようとすると、ウイルス警告メッセージではなく、URL ブロックメッセージが表示されます。

初期設定のブロック期間 (時間単位) を設定するには、`/etc/iscan/intscan.ini` ファイルの `[Scan-configuration]` セクションにあるパラメータ `infected_url_block_length` を変更して、`/etc/iscan/S99ISproxy stop` および `/etc/iscan/S99ISproxy start` を実行します。

自動 URL ブロックを無効にするには、/etc/iscan/intscan.ini ファイルの [Scan-configuration] セクションにあるパラメータ disable_infected_url_block を変更して、/etc/iscan/S99ISproxy stop および /etc/iscan/S99ISproxy start を実行します。

disable_infected_url_block パラメータについて

no: 自動 URL ブロックを有効にする

yes: 自動 URL ブロックを無効にする

注意： セキュリティレベルが低下するため、この機能は無効にしないことをお勧めします。

URL フィルタのテスト

URL フィルタをテストする場合は、初期設定を使用することをお勧めします。

URL フィルタをテストするには

1. 管理コンソールから [HTTP] → [URL フィルタ] → [ポリシー] の順に選択します。
2. [URL フィルタを有効にする] をオンにしてから [保存] をクリックします。
3. [URL フィルタのグローバルポリシー] をクリックして、ブロックするカテゴリに適用するブロック処理を選択します。

   [安全な検索エンジン] および [除外] タブの初期設定をそのまま受け入れます。
4. [保存] をクリックして変更内容を保存します。[ポリシーの配信] をクリックして、ポリシーをただちに有効にします。
5. ブラウザを開いて、ブロックするように指定したサイトにアクセスします。IWSVA は、ブロックされるように設定されているカテゴリに属する URL へのアクセスをブロックします。

スパイウェア検索のテスト

スパイウェア検索をテストするには

1. [HTTP] → [高度な脅威保護] → [ポリシー] の順にクリックします。
2. [ウイルス検索のグローバルポリシー] をクリックします。

3. [スパイウェア検索ルール] タブをクリックし、検索対象のスパイウェア / 不正プログラムの種類を選択します。
4. [保存] をクリックします。
5. [ウイルス検索のグローバルポリシー] をクリックします。
6. [処理] タブをクリックします。
7. [2 次処理] フィールドで、削除、隔離、放置から処理設定を選択します。
8. [保存] をクリックします。
9. [ポリシーの配信] をクリックして、ポリシーをただちに有効にします。

   スパイウェアの検出が正常に機能していれば、例に示すようなメッセージが表示されます。

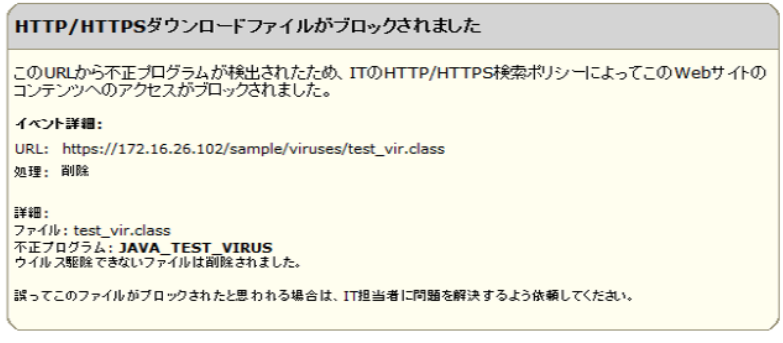


図 15-10. 設定の「削除」処理を伴うスパイウェアを検出後のメッセージ例

その他の IWSVA の設定

本項では、IWSVA の一般的な設定タスクについて簡単に説明します。

専用の管理インタフェースの設定

多くの大企業や安全なネットワーク環境では、別個のネットワークセグメント (管理ネットワークとも呼ばれる) を使用して各種のネットワークデバイスを管理することができます。セキュリティ上の理由で、この管理ネットワークはインターネットに接続されず、通常のユーザがアクセスを許可されない別個のネットワークとなります。

IWSVA サーバでは、会社の管理ネットワークに接続する専用の管理インタフェースを有効にできます。別個のネットワークインタフェースは、専用管理インタフェースとして IWSVA サーバで使用できるようにする必要があります。管理インタフェースが IWSVA でアクティブ化され、設定されると、専用の管理インタフェースを介して IWSVA の Web コンソールまたは CLI にアクセスできます。次の図は、ネットワークトポロジの例を示しています。

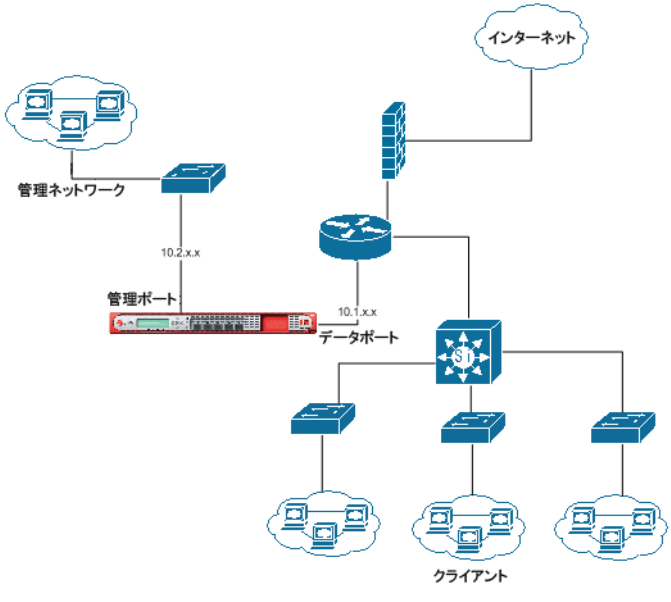


図 15-11. ネットワーク内での IWSVA 管理インタフェースの配置

この例では、IWSVA の管理インタフェースは、会社の管理ネットワークに接続されています。クライアントは、データ（ブリッジまたはプロキシ）インタフェースを介してインターネットにアクセスします。

警告： データ (ブリッジ / プロキシ) インタフェースと管理インタフェースを同じネットワーク環境に設定しないでください。

専用の管理インタフェースを設定するには

1. メインメニューから、[管理] → [ネットワーク設定] → [ネットワークインタフェース] の順にクリックし、[管理インタフェースを有効にする] チェックボックスをオンにします。
2. [イーサネットインタフェース] ドロップダウンリストから、管理インタフェースの対象となるインタフェースを選択します。
3. IP アドレスを設定します。
4. このインタフェースで IWSVA が PING 要求に応答するようにする場合は、[PING を有効にする] を選択します。
5. [保存] をクリックします。専用の管理インタフェースにアクセスして、Web コンソールにログインし、IWSVA を管理できます。

ヒント： IWSVA コンピュータが管理ネットワークのルータ / スイッチの背後にある場合は、Web コンソールまたは SSH を介して IWSVA にアクセスするように管理インタフェース上で静的ルートを設定してください。

専用の管理インタフェースをテストするには

1. まず、データ（ブリッジまたはプロキシ）インタフェースを介した Web コンソールへのログオンを試みます。IWSVA にログオンし、管理できるはずです。
2. 次に、専用の管理インタフェースで Web コンソールへのアクセスを試みます。IWSVA にログオンし、管理できるはずです。

リモート CLI のアクティブ化

リモート CLI 機能を有効にすると、IWSVA サーバに接続して CLI コマンドを使用して設定することができます。リモート接続は、SSH v2（Secure SHell）を介して保護されます。SSH とは、2 つのネットワークデバイスを安全に接続してデータを交換するためのネットワークプロトコルです。SSH はデータ（パスワードを含む）を暗号化せずに送信する Telnet に置き換わるものです。

IWSVA サーバでリモート CLI を有効にするには

1. 管理コンソールで、[管理] → [ネットワーク設定] → [リモート CLI] の順にクリックし、[SSH: コマンドラインアクセス] を選択して、IWSVA の SSH を使用したリモート CLI アクセスを有効にします。
2. SSH v2 に対するサービスポート番号を入力します。初期設定では、ポート番号は 22 です。
3. [保存] をクリックします。

高度な脅威保護検索の指定

高度な脅威保護検索は、初期設定で有効になっています。クライアントが Web を閲覧したり、その他の HTTP 処理を実行するための HTTP トラフィックフローを有効 / 無効にすることができます (138 ページの「HTTP/HTTPS トラフィックフローの有効化」を参照)。

ユーザの識別方法の指定

IWSVA では、ポリシーの範囲を設定するときにクライアントを識別する方法を複数サポートしています (160 ページの「ユーザ識別方法の設定」を参照)。初期設定の識別方法は、クライアントの IP アドレスを経由する方法です。また、IWSVA では、ホスト名や MAC アドレスを経由してクライアントを識別することも、LDAP ディレクトリを経由してクライアントを識別することもできます。

ゲストアカウントの有効化 (LDAP のみ)

ユーザ / グループ名認証による識別方法を使用する場合、HTTPS 復号化、HTTP ウイルス検索、HTTP 検査、情報漏えい対策、URL フィルタ、およびアクセス割り当てのポリシーで、一時的にネットワークにアクセスするユーザ向けのポリシー設定がサポートされます。ゲストアカウントは、初期設定で無効になっています。ゲストアカウントのインターネットへのアクセスを許可する場合はこのアカウントを有効にします。ゲストアカウントを有効にするには、IWSVA をユーザ / グループ名認証 (LDAP) 対応として設定する必要があります。

ゲストアカウントを有効にするには

1. ゲストアカウントを有効にするには、[管理] → [一般設定] → [ユーザの識別] タブの順に選択します。
2. [認証方法] で、[キャプティブポータル] を選択し、[ゲストログインの許可] をオンにして [保存] をクリックします。

検索ポリシーとフィルタポリシーの見直し

IWSVA は、基本的なゲートウェイセキュリティを提供するように事前設定されています。HTTP ウイルス検索のグローバルポリシーとゲストポリシーの設定を見直して、組織のセキュリティポリシーを反映しているかどうか確認することをお勧めします。

また、URL フィルタモジュール、および FTP 検索モジュールを実行している場合、これらの設定を見直して必要に応じて変更してください。

アクセス割り当てポリシーの有効化

帯域幅の使用を制限するには、アクセスの割り当て管理を有効にして、クライアントが指定された期間内に取得またはダウンロードできるデータ量の上限を設定します。

アクセス割り当て管理を有効にするには

1. 管理コンソールから [HTTP] → [アクセス割り当てポリシー] の順に選択します。
2. [アクセス割り当てを有効にする] チェックボックスをオンにします。
3. ネットワークのゲストユーザに対するアクセス割り当て管理を設定するには、[アクセス割り当てポリシー] をクリックして設定値を指定します。その他のネットワークユーザに対してアクセス割り当て制御を設定するには、[追加] をクリックして新しいポリシーを設定します。
4. [保存] をクリックします。

   新しいポリシーをただちに有効にするために、[HTTP] → [アクセス割り当てポリシー] 画面で [ポリシーの配信] をクリックします。

インターネットアクセス管理の設定

IWSVA の初期設定では、ゲストクライアント以外のクライアントはインターネットアクセスが許可されます。一部のクライアントに対してインターネットアクセスを許可するには、[アクセス管理設定] 画面で対象のクライアントの IP アドレスを設定します。

また、信頼するサイトへのアクセス時の閲覧パフォーマンスを高めるために、IWSVA では、一部のサーバを検索から除外するように設定できます。たとえば、イントラネットサイトの IP アドレス範囲をサーバ IP の除外リストに追加して、頻繁にアクセスされるサイトを検索とフィルタから除外することを検討します。

インターネットアクセスを許可するクライアントを設定するには

1. 管理コンソールで [HTTP] → [設定] → [アクセス管理の設定] の順に選択します。
2. [クライアント IP] タブで [クライアント IP に基づく HTTP アクセス管理を有効にする] を選択して、インターネットアクセスを許可する IP アドレス / ホスト名を入力します。
3. 簡単な説明を入力します。
4. [追加] をクリックします。
5. [保存] をクリックします。

フィルタと検索から除外するサーバを設定するには

1. 管理コンソールから [HTTP] → [設定] → [アクセス管理の設定] の順に選択します。
2. [サーバ IP の除外リスト] タブをクリックし、HTTP 検索、URL フィルタ、および URL ブロックから除外するサーバの IP アドレスを設定します。
3. 簡単な説明を入力します。
4. [追加] をクリックします。
5. [保存] をクリックします。

アプリケーションパッチの適用またはアプリケーションパッチの削除

トレンドマイクロのダウンロードサイトで、アップデートを入手できます。最新のアップデートをダウンロードサイトからデスクトップまたはその他のコンピュータにダウンロードしたら、それを IWSVA デバイスにアップロードすれば自動的にインストールされます。

アプリケーションパッチを適用するには

1. https://www.trendmicro.com/ja_jp/business/products/downloads.html から最新のアップデートをダウンロードします。
2. 管理コンソールで [管理] → [システムアップデート] の順に選択してから、[参照] ボタンをクリックします。
3. トレンドマイクロのダウンロードサイトからダウンロードしたアップデートを検索します。
4. [アップロード] をクリックすると、IWSVA がアップデートを IWSVA デバイスにコピーし、インストールを開始します。

   このユーティリティでは、正しくフォーマットされ暗号化されたトレンドマイクロの Patch のみアップロードできます。

アプリケーションパッチを削除するには

1. 管理コンソールから [管理] → [システムアップデート] の順に選択します。
2. [履歴] で [アプリケーションのパッチ] タブをクリックします。
3. アプリケーションパッチ番号の横にある [アンインストール] リンクをクリックします。
4. 表示されたプレビュー画面で、アンインストールするパッチのバージョンを確認します。

   インストール済みの最も新しいアプリケーションパッチはいつでもアンインストールできます。
5. [アンインストール] をクリックします。進行ステータス画面が表示されます。パッチがアンインストールされると、ウィンドウが閉じ、IWSVA コンソールのメイン画面に戻ります。

HotFix、Patch、および Service Pack について

トレンドマイクロでは、公式の製品リリース後に、問題を解決したり、製品のパフォーマンスを向上させたり、新しい機能を追加するために、HotFix、Patch、および Servie Pack を提供することがあります。

トレンドマイクロによりリリースされるアイテムを次に示します。

- HotFix: お客さまから報告された単独の問題に対する次善策または解決策。HotFix は、問題固有であるため、すべてのお客さまにリリースされるわけではありません。Windows の HotFix には、セットアッププログラムが含まれています。
- Critical Patch / Security Patch: 至急対策の必要がある問題のみを修正する目的で一般公開されるプログラムです。特定の問題を修正するプログラムであるため、基本的に、他の修正は含まれませんが、同時期に発見された問題に対する複数の修正が含まれる場合があります。一般公開時期に応じて、後述の Patch に統合されます。
- Patch: 複数のプログラム上の問題を解決する HotFix と Security Patch のグループ。トレンドマイクロでは定期的に Patch を提供しています。
- Service Pack: HotFix、Patch、および機能強化を組み合わせたもので、製品のアップグレードに相当します。

  Patch や Service Pack は、次のトレンドマイクロの Web サイトを定期的にチェックしてダウンロードしてください。

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

  すべてのリリースには、対象製品のインストール、展開、および設定に必要な情報を含む Readme ファイルが付属しています。HotFix、Patch、または Service Pack ファイルをインストールする前に、Readme ファイルを読んでください。

データベース接続の確認

データベース接続設定を確認するには

1. [管理] → [一般設定] → [データベース接続] の順に選択します。
2. [ポリシーデータベースの接続設定] でデータベース設定を確認します。
3. [データベース接続のテスト] をクリックします。

ポリシーの設定は、データベースに格納され、IWSVA によって設定がメモリキャッシュにコピーされます。IWSVA では、[ポリシー配信設定（分)] オプションの間隔指定に従ってデータベースからメモリに設定がリロードされます。

[ポリシー配信設定 (分)] を設定するには

1. IWSVA Web コンソールを開き、[管理] → [一般設定] → [ポリシー配信] の順にクリックします。
2. [ポリシー配信設定（分)] で、次のパラメータの値を入力します。
   - ウイルス検索ポリシー
   - HTTPS ポリシー
   - HTTP 検査ポリシー
   - URL フィルタポリシー
   - アクセス割り当てポリシー
   - アプリケーション制御ポリシー
   - DLP ポリシー
3. [保存] をクリックします。

管理コンソールパスワードの変更

Web コンソールパスワードは、IWSVA デバイスを不正な変更から守るための基本的な手段です。環境のセキュリティをより高めるには、コンソールパスワードを定期的に変更し、推測が困難なパスワードを使用するようにしてください。

管理者パスワードは、Web コンソールインタフェースを使用して変更できます。CLI では、Enable、Root、およびすべての Administrator アカウントのパスワードを変更できます。それらの変更を実行する場合、CLI コマンドでは「configure password」コマンドが使用されます。

Web コンソールパスワードを CLI で変更するには

1. CLI コンソールにログインし、特権モードに移ります。
2. 次のコマンドを入力します。

   configure system password

安全なパスワードの作成には、次のヒントを参考にしてください。

- パスワードに文字列と数字の両方を含めます。
- どんな言語であっても、辞書に掲載された単語は避けます。
- 意図的に単語のスペルを間違えます。
- 成句を使用したり、単語を組み合わせます。
- 大文字と小文字を混在させます。

Web コンソールパスワードを変更するには

1. IWSVA コンソールを開いて、管理コンソールで [管理] → [管理コンソール] → [アカウント管理] の順に選択します。
2. パスワードを変更するユーザアカウントをクリックします。
3. [ログインアカウント] 画面で、[パスワード] に新しいパスワードを入力してから、[パスワードの確認入力] にもう一度同じパスワードを入力します。
4. [保存] をクリックします。

Web コンソールの待機ポート変更後の設定

ユーザが [管理] → [ネットワーク設定] → [Web コンソール] 画面にアクセスして、SSL モード用のポート番号を他のアプリケーションで使用されていないポート (8443 など) に設定することで HTTPS Web コンソールの管理モードを有効にする場合、[HTTP] → [設定] → [アクセス管理の設定] 画面でもこの SSL 管理ポート番号を指定する必要があります。

[アクセス管理設定] 画面でこのポート番号が指定されていないと、HTTPS Web コンソールを使用する際、IWSVA によって IWSVA 進行ステータス画面が自動的にブロックされます。つまり、クライアントが URL にアクセスしようすると、IWSVA によってブロックされた進行ステータスバーが表示されます。

URL フィルタ設定の確認

URL フィルタモジュールを実行している場合、設置後のタスクを見直して IWSVA を環境に合わせて調整します。

IWSVA では、「ギャンブル」、「ゲーム」、「出会い系」など 80 を超えるカテゴリに属する URL を格納する Web レピュテーションデータベースにアクセスできます。これらのカテゴリは論理グループに含まれます。

トレンドマイクロでは、URL フィルタ設定を見直すことをお勧めします。それにより、社内で禁止サイトと見なすカテゴリが、組織の価値を反映しており、従業員が業務で使用する Web 閲覧に支障がないか確認してください。URL フィルタポリシーを適用する前に、初期設定の分類が組織に対して適切かどうか確認することをお勧めします。たとえば、衣料販売業者は、正当な市場調査や競合他社の調査ができるように、「アダルト」グループに分類された「性的な服装 / 水着」カテゴリから水着の Web サイトを除外する必要がある場合があります。

また、除外 URL を設定して、本来はブロックすべき特定のサイトへの従業員のアクセスを有効にしたり、「業務時間」の定義を見直して、職場のスケジュールを反映したりする必要がある場合もあります。

URL フィルタ設定を見直すには

1. 管理コンソールから [HTTP] → [URL フィルタ] → [ポリシー] → [ポリシー] → [除外設定] の順に選択します。
2. URL フィルタから除外する Web サイトを含む除外 URL リストをドロップダウンリストから選択して、これらの Web サイトにクライアントから常にアクセスができるようにします。
3. [保存] をクリックします。
4. 管理コンソールで、[管理] → [一般設定] → [予約期間] をクリックします。

注意： 「業務時間」の初期設定は、月曜から金曜の 8:00 ～ 12:00 および 13:00 ～ 17:00 までになっています。

---

5. 職場の従業員のスケジュールに応じてこれらの時間設定を変更します。
6. 管理コンソールで [HTTP] → [URL フィルタ] → [ポリシー] の順に選択して、URL フィルタのゲストポリシーとグローバルポリシーのカテゴリ設定を見直します。

IWSVA パフォーマンスの調整

閲覧パフォーマンスが遅くて困る場合は、本項で説明する変更内容を検討してください。

LDAP パフォーマンスの調整

ユーザ / グループ名認証による識別方法 (LDAP) を使用する IWSVA を実行する場合、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に依存します。最悪の場合、HTTP 要求ごとに、ユーザ認証を求める LDAP クエリや、対象ユーザのグループメンバーシップ情報の取得を求める別の LDAP クエリが必要になります。こうしたクエリによって、IWSVA と LDAP サーバ間の送受信に遅延が発生し、LDAP サーバ自体の負荷が増大します。

LDAP の内部キャッシュ

必要な LDAP クエリ量を減らすために、IWSVA は複数の内部キャッシュを提供しています。

- **ユーザグループメンバーシップキャッシュ** — ユーザグループメンバーシップ用キャッシュには、数百人のユーザのグループメンバーシップ情報を格納できます。このキャッシュ内のエントリの同期間隔は、`/etc/iscan/commonldap/LdapSetting.ini` ファイルの `LDAP_Setting` にあるパラメータ `SyncInterval` で設定できます。初期設定値は 1440 (24 時間) です。0 を設定すると同期は無効になります。
- **クライアント IP アドレスとユーザ ID 間のキャッシュ** — クライアント IP 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。その期間中、IWSVA が認識するクライアント IP アドレスはユーザごとに一意でなければなりません。したがって、このキャッシュは、クライアントと IWSVA の間にプロキシサーバやソース NAT が存在する環境や DHCP が頻繁にクライアント IP アドレスを再割り当てする環境では使用できません。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。
- **ユーザ認証キャッシュ** — このキャッシュは、接続中に発行された複数の HTTP 要求の再認証を回避します。接続中にユーザの認証情報が確認されると、IWSVA はユーザ認証キャッシュにエントリ (1 つのキャッシュエントリ内の 2 つの重要な鍵はクライアントの IP アドレスとユーザ名) を追加して、接続中に次の要求が来ても再認証しないようにします。クライアントの IP アドレスとユーザ名は、それぞれ「クライアント IP アドレスとユーザ ID 間のキャッシュ」と「ユーザグループメンバーシップキャッシュ」に対する前方参照またはリンクとしての役割を果たします。つまり、IWSVA はユーザの接続情報を IP アドレスとユーザ ID のキャッシュおよ

びユーザグループキャッシュの両方から取得できます。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。このキャッシュの生存期限 (TTL) を変更するには、`/etc/iscan/commonldap/LdapCache.ini` 設定ファイルの `expire_interval` を変更します (秒単位)。初期設定値は 7200 (2 時間) です。

IWSVA を LDAP と連携して展開する場合、HTTP 要求の認証により LDAP ディレクトリサーバに課せられる追加の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 間の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 が有効な場合の冗長ログの無効化

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。製品展開では、通常、冗長ログは必要ありません。

冗長ログと LDAP がともに有効になっている場合は、IWSVA が、ユーザ認証情報とグループメンバーシップ情報を Log フォルダ内の HTTP ログに記録します。ログには、ユーザごとに何百行もの情報が含まれるため、内部トラフィック量やユーザが属しているグループ数によっては、大量のハードディスク容量が必要になる場合があります。冗長ログは、OS に対して I/O 処理を要求することによって、サービスをビジー状態にします。これにより、サービスが HTTP 要求にタイムリーに応答できなくなり、その結果、遅延が発生する場合があります。極端に HTTP トラフィックが集中する環境では、IWSVA を冗長モードで起動した場合に大きな遅延が発生します。

付録 A

サポート情報

本付録では、InterScan Web Security Virtual Appliance（以下、IWSVA) のパフォーマンスを最適化し、技術的な問題に関するさらなる支援を受けるための情報を提供します。

本付録で説明する内容には、次の項目が含まれます。

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/jp/technical-support`

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/jp/virus-and-threat-help`

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 B

ファイルタイプと MIME コンテンツタイプの対応

次の表は、対応する MIME コンテンツタイプの検索を省略するために、HTTP ウイルス検索ポリシーの [検索を省略する MIME コンテントタイプ] フィールドに入力できるファイルタイプを示しています。

概要

MIME 名は表 B-1 に限定されているわけではありません。つまり、IWSVA UI 除外リストには任意の名前を入力できます (詳細については、223 ページの「検索するファイルタイプを選択するには」を参照してください)。ただし、次の依存関係がある場合には、検索を省略できるのは MIME タイプのみです。

IWSVA はファイルを受信すると、次の点を判別します。

- MIME 名が UI で検索を省略するように設定されているか
- ファイルタイプ (MIME 名ではなく) がマッピングテーブルにリストされているか
- MIME 名がマッピングテーブルにリストされている場合、MIME 名は UI 除外リストに含まれているか

IWSVA は一致を見つけると、検索を省略します。IWSVA で一致を見つけることができなかった場合、検索は省略されません。

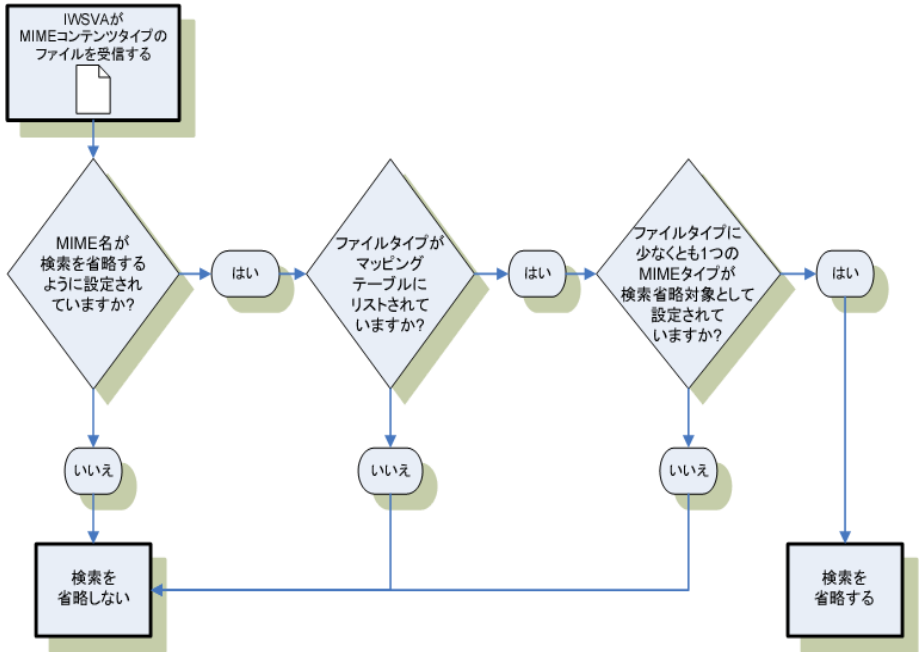


図 B-1.　検索が省略されるファイルの MIME コンテンツタイプのフロー

管理者が MIME 名を入力し、IWSVA にとってそのファイルタイプが不明の場合、そのファイルの検索は省略されます。MIME タイプが IWSVA で検索を省略するように設定されており、ファイルタイプ -MIME テーブルに存在しない場合は、検索は省略されます。これは、ファイルタイプ -MIME テーブルで、すべての可能なファイルタイプについてすべての可能な MIME タイプをリストすることができないからです。

1 つのファイルタイプに対して少なくとも 1 つの MIME タイプが検索省略対象として設定されている場合も、検索は省略されます。MIME 名が標準というわけではないからです。ファイルタイプ -MIME テーブルで、既知のファイルタイプに対するすべての MIME タイプをリストすることはできません。

たとえば、ファイルタイプ -MIME テーブルには FLV ファイルのマッピングとして video/flv と video/x-flv が含まれていますが、「application/flv」は含まれていません。ただし、一部の Web サイトは「application/flv」を使用しています。IWSVA は該当するマッピングエントリを見つけることはできませんが、ファイルタイプのチェックを実行して、これが FLV ファイルであることを認識します。このファイルの検索は省略されます。

管理者が「video/flv」と「application/flv」を除外リストに入力している場合は、次のチェックが実行されます。

- MIME 名が検索を省略するように設定されている （MIME タイプ : application/flv) > はい >
- ファイルタイプがマッピングテーブルにリストされているかどうかチェックする （ファイルタイプ : flv) > ある >
- ファイルタイプに少なくとも 1 つの MIME タイプが検索省略対象として設定されている > はい > 検索を省略する

MIME コンテンツファイルのファイルタイプマッピングテーブル

表 B-1.　MIME コンテンツファイルのファイルタイプマッピングテーブル

ファイルタイプ	MIME コンテンツタイプ
ACE 圧縮ファイル	application/x-ace
ACE 圧縮ファイル	application/x-compressed
Apple サウンド	audio/aiff
Apple サウンド	audio/x-aiff
Apple/SGI の Audio InterChange File Format (以下、AIFF)	audio/aiff
Apple/SGI の AIFF	audio/x-aiff
Apple/SGI の AIFF	sound/aiff
Apple/SGI の AIFF	audio/rmf
Apple/SGI の AIFF	audio/x-rmf
Apple/SGI の AIFF	audio/x-pn-aiff
Apple/SGI の AIFF	audio/x-gsm
Apple/SGI の AIFF	audio/x-midi
Apple/SGI の AIFF	audio/vnd.qcelp
ARJ	application/arj
ARJ	application/x-arj
ARJ	application/x-compress
ARJ	application/x-compressed
ARJ	zz-application/zz-winassoc-arj
Advanced Systems Format （以下、ASF)	video/x-ms-asf

表 B-1.　MIME コンテンツファイルのファイルタイプマッピングテーブル（続き）

ファイルタイプ	MIME コンテンツタイプ
ASF	video/x-ms-asf-plugin
ASF	video/x-ms-wm
ASF	video/x-ms-wmx
ASF	audio/asf
ASF	application/asx
ASF	application/x-mplayer2
ASF	application/vnd.ms-as"
Nullsoft AVS	video/avs-video
Mime Base 64	application/base64
Macintosh MacBinary アーカイブ	application/mac-binary
Macintosh MacBinary アーカイブ	application/macbinary
Macintosh MacBinary アーカイブ	application/octet-stream
Macintosh MacBinary アーカイブ	application/x-binary
Macintosh MacBinary アーカイブ	application/x-macbinary
BINHEX	application/binhex
BINHEX	application/binhex4
BINHEX	application/mac-binhex
BINHEX	application/mac-binhex40
BINHEX	application/x-binhex40
Windows BMP	image/bmp
Windows BMP	image/x-bmp

表 B-1.　MIME コンテンツファイルのファイルタイプマッピングテーブル（続き）

ファイルタイプ	MIME コンテンツタイプ
Windows BMP	image/x-bitmap
Windows BMP	image/x-xbitmap
Windows BMP	image/x-win-bitmap
Windows BMP	image/x-windows-bmp
Windows BMP	image/ms-bmp
Windows BMP	image/x-ms-bmp
SGI イメージ	image/x-sgi-bw
GNU BZIP2	application/x-bzip2
GNU BZIP3	application/bzip2
GNU BZIP4	application/x-bz2
GNU BZIP5	application/x-compressed
Computer Graphics Metafiles	image/cgm
COM	application/octet-stream
COM	application/x-msdos-program
COM	application/x-msdownload
UNIX cpio アーカイブ	application/x-cpio
Adobe Director Shockwave Movie	application/x-director
WordPerfect	application/wordperfect
AutoCAD DWG	application/acad
AutoCAD DWG	application/x-acad
AutoCAD DWG	drawing/x-dwg

表 B-1.　MIME コンテンツファイルのファイルタイプマッピングテーブル（続き）

ファイルタイプ	MIME コンテンツタイプ
AutoCAD DWG	image/vnd.dwg
AutoCAD DWG	image/x-dwg
Encapsulated Postscript （以下、EPS)	application/postscript
EPS	image/x-eps
EPS	image/eps
EPS	application/x-eps
EPS	application/eps
EXE	application/octet-stream
EXE	application/exe
EXE	application/x-msdownload
EXE	application/x-exe
EXE	application/dos-exe
EXE	vms/exe
EXE	application/x-winexe
EXE	application/msdos-windows
FreeHand ドキュメント	image/x-freehand
AutoDesk Animator （FLI または FLC)	video/x-fli
AutoDesk Animator （FLI または FLC)	video/flc
AutoDesk Animator （FLI または FLC)	video/fli
AutoDesk Animator （FLI または FLC)	video/x-acad-anim
Adobe Flash FLV ビデオ	video/flv

表 B-1.　MIME コンテンツファイルのファイルタイプマッピングテーブル（続き）

ファイルタイプ	MIME コンテンツタイプ
Adobe Flash FLV ビデオ	video/x-flv
Adobe Flash FLV ビデオ	flv-application/octet-stream
Frame Maker	application/vnd.framemaker
GIF	image/gif
GNU ZIP	application/gzip
GNU ZIP	application/x-gzip
GNU ZIP	application/x-gunzip
GNU ZIP	application/gzipped
GNU ZIP	application/gzip-compressed
GNU ZIP	application/x-compressed
GNU ZIP	application/x-compress
GNU ZIP	gzip/document
GNU ZIP	encoding/x-gzip
Windows アイコン	image/ico
Windows アイコン	image/x-icon
Windows アイコン	application/ico
Windows アイコン	application/x-ico
Windows アイコン	application/x-win-bitmap
Windows アイコン	image/x-win-bitmap
Amiga 8SVX Audio Interchange File Format (以下、AIFF)	audio/x-aiff

表 B-1.　MIME コンテンツファイルのファイルタイプマッピングテーブル（続き）

ファイルタイプ	MIME コンテンツタイプ
Amiga 9SVX AIFF	image/iff
Amiga 10SVX AIFF	image/x-iff
Amiga 11SVX AIFF	application/iff
JAVA アプレット	text/x-java-source
JAVA アプレット	application/java-class
JAVA アプレット	application/x-java-applet
JAVA アプレット	application/x-java-vm
JPEG	image/jpeg
JPEG	image/jpg
JPEG	image/jp_
JPEG	image/pipeg
JPEG	image/pjpeg
LHA	application/x-lha
LHA	application/lha
LHA	application/x-compress
LHA	application/x-compressed
LHA	application/maclha
Compiled LISP	application/x-lisp
NT/95 ショートカット　(*.lnk)	application/x-ms-shortcut
LightWave 3D オブジェクト	image/x-lwo
MAUD Sample Format	audio/x-maud

表 B-1.　MIME コンテンツファイルのファイルタイプマッピングテーブル（続き）

ファイルタイプ	MIME コンテンツタイプ
Microsoft Document Imaging	image/vnd.ms-modi
MIDI	audio/midi
Magick Image File Format (MIFF)	application/x-mif
Multi-image Network Graphics	video/x-mng
Multi-image Network Graphics	video/mng
MP3	audio/mpeg
MP3	audio/mpeg3
MP3	audio/x-mpeg-3
MPEG	video/mpeg
MPEG	video/mpg
MPEG	video/x-mpg
MPEG	video/mpeg2
MPEG	video/x-mpeg
MPEG	video/x-mpeg2a
Microsoft Cabinet	application/x-cainet-win32-x86
Windows Word	application/msword
Windows Word	application/doc
Windows Word	application/vnd.msword
Windows Word	application/vnd.ms-word
Windows Word	application/x-msw6
Windows Word	application/x-msword

表 B-1.　MIME コンテンツファイルのファイルタイプマッピングテーブル（続き）

ファイルタイプ	MIME コンテンツタイプ
Windows Excel	application/excel
Windows Excel	application/x-msexcel
Windows Excel	application/x-ms-excel
Windows Excel	application/x-excel
Windows Excel	application/vnd.ms-excel
Windows Excel	application/xls
Windows Excel	application/x-xls
Windows Installer	application/x-ole-storage
Microsoft Access (MDB)	application/x-msaccess
Microsoft Access (MDB)	application/msaccess
Microsoft Access (MDB)	application/vnd.msaccess
Microsoft Access (MDB)	application/vnd.ms-access
Microsoft Access (MDB)	application/mdb
Microsoft Access (MDB)	application/x-mdb
Microsoft Access (MDB)	zz-application/zz-winassoc-mdb
Microsoft Office 12	application/vnd.ms-word.document.macroEnabled.12
Microsoft Office 12	application/vnd.openxmlformats-officedocument.wordprocessingml.document
Microsoft Office 12	application/vnd.ms-word.template.macroEnabled.12
Microsoft Office 12	application/vnd.openxmlformats-officedocument.wordprocessingml.template

表 B-1.　MIME コンテンツファイルのファイルタイプマッピングテーブル（続き）

ファイルタイプ	MIME コンテンツタイプ
Microsoft Office 12	application/vnd.ms-powerpoint.template.macroEnabled.12
Microsoft Office 12	application/vnd.openxmlformats-officedocument.presentationml.template
Microsoft Office 12	application/vnd.ms-powerpoint.addin.macroEnabled.12
Microsoft Office 12	application/vnd.ms-powerpoint.slideshow.macroEnabled.12
Microsoft Office 12	application/vnd.openxmlformats-officedocument.presentationml.slideshow
Microsoft Office 12	application/vnd.ms-powerpoint.presentation.macroEnabled.12
Microsoft Office 12	application/vnd.openxmlformats-officedocument.presentationml.presentation
Microsoft Office 12	application/vnd.ms-excel.addin.macroEnabled.12
Microsoft Office 12	application/vnd.ms-excel.sheet.binary.macroEnabled.12
Microsoft Office 12	application/vnd.ms-excel.sheet.macroEnabled.12
Microsoft Office 12	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
Microsoft Office 12	application/vnd.ms-excel.template.macroEnabled.12
Microsoft Office 12	application/vnd.openxmlformats-officedocument.spreadsheetml.template
Microsoft Office 12	application/vnd.openxmlformats

表 B-1.　MIME コンテンツファイルのファイルタイプマッピングテーブル（続き）

ファイルタイプ	MIME コンテンツタイプ
Windows PowerPoint	application/mspowerpoint
Windows PowerPoint	application/powerpoint
Windows PowerPoint	application/vnd.ms-powerpoint
Windows PowerPoint	application/ms-powerpoint
Windows PowerPoint	application/mspowerpnt
Windows PowerPoint	application/vnd-mspowerpoint
Windows PowerPoint	application/x-powerpoint
Windows PowerPoint	application/x-mspowerpoint
Windows Project	application/vnd.ms-project
Windows Project	application/x-msproject
Windows Project	application/x-project
Windows Project	application/msproj
Windows Project	application/msproject
Windows Project	application/x-ms-project
Windows Project	application/x-dos_ms_project
Windows Project	application/mpp
Windows Project	zz-application/zz-winassoc-mpp
Windows Write	application/mswrite
Windows Write	application/x-mswrite
Windows Write	application/wri
Windows Write	application/x-wri

表 B-1.　MIME コンテンツファイルのファイルタイプマッピングテーブル（続き）

ファイルタイプ	MIME コンテンツタイプ
Windows Write	application/msword
Windows Write	application/microsoft_word
Windows Write	zz-application/zz-winassoc-wri
OpenDocument	application/vnd.oasis.opendocument.text
OpenDocument	application/vnd.oasis.opendocument.text-template
OpenDocument	application/vnd.oasis.opendocument.graphics
OpenDocument	application/vnd.oasis.opendocument.graphics-template
OpenDocument	application/vnd.oasis.opendocument.presentation
OpenDocument	application/vnd.oasis.opendocument.presentation-template
OpenDocument	application/vnd.oasis.opendocument.spreadsheet
OpenDocument	application/vnd.oasis.opendocument.spreadsheet-template
OpenDocument	application/vnd.oasis.opendocument.chart
OpenDocument	application/vnd.oasis.opendocument.chart-template
OpenDocument	application/vnd.oasis.opendocument.image
OpenDocument	application/vnd.oasis.opendocument.image-template
OpenDocument	application/vnd.oasis.opendocument.formula

表 B-1.　MIME コンテンツファイルのファイルタイプマッピングテーブル（続き）

ファイルタイプ	MIME コンテンツタイプ
OpenDocument	application/vnd.oasis.opendocument.formula-template
OpenDocument	application/vnd.oasis.opendocument.text-master
OpenDocument	application/vnd.oasis.opendocument.text-web
Gravis Patch ファイル	audio/pat
Gravis Patch ファイル	audio/x-pat
Microsoft Paint v1.x	image/x-pcx
Microsoft Paint v1.x	image/pcx
Microsoft Paint v1.x	image/x-pc-paintbrush
Microsoft Paint v1.x	application/x-pcx
Microsoft Paint v1.x	application/pcx
Microsoft Paint v1.x	zz-application/zz-winassoc-pcx
Microsoft Paint v2.x	image/x-pcx
Microsoft Paint v2.x	image/pcx
Microsoft Paint v2.x	image/x-pc-paintbrush
Microsoft Paint v2.x	application/x-pcx
Microsoft Paint v2.x	application/pcx
Microsoft Paint v2.x	zz-application/zz-winassoc-pcx
PCX	image/x-pcx
PCX	image/pcx
PCX	image/x-pc-paintbrush

表 B-1.　MIME コンテンツファイルのファイルタイプマッピングテーブル（続き）

ファイルタイプ	MIME コンテンツタイプ
PCX	application/x-pcx
PCX	application/pcx
PCX	zz-application/zz-winassoc-pcx
Palm Pilot Image	application/x-pilot-pdb
Adobe Portable Document Format　(PDF)	application/pdf
Adobe PDF	application/x-pdf
Adobe フォントファイル	application/x-font
Macintosh ビットマップ	image/pict
Macintosh ビットマップ	image/x-pict
Portable Network Graphics	image/png
PPM Image	image/x-portable-pixmap
PPM Image	image/x-p
PPM Image	image/x-ppm
PPM Image	application/ppm
PPM Image	application/x-ppm
Postscript	application/postscript
Adobe Photoshop　(PSD)	application/octet-stream
Paint Shop Pro	image/bmp
Quick Time Media	video/quicktime
Quick Time Media	video/x-quicktime
Quick Time Media	image/mov

表 B-1.　MIME コンテンツファイルのファイルタイプマッピングテーブル（続き）

ファイルタイプ	MIME コンテンツタイプ
Quick Time Media	audio/aiff
Quick Time Media	audio/x-midi
QuarkXPress Document (QXD)	application/quarkxpress
QuarkXPress Document (QXD)	application/x-quark-express
Real Audio	audio/vnd.rn-realaudio
Real Audio	audio/x-pn-realaudio
Real Audio	audio/x-realaudio
Real Audio	audio/x-pm-realaudio-plugin
Real Audio	video/x-pn-realvideo
RAR	application/rar
Sun Raster (RAS)	image/x-cmu-raster
Sun Raster (RAS)	image/cmu-raster
Real Media	application/vnd.rn-realmedia
Microsoft RTF	application/rtf
Microsoft RTF	application/x-rtf
Microsoft RTF	text/richtext
Lotus ScreenCam ムービー	application/vnd.lotus-screencam
Lotus ScreenCam ムービー	application/x-lotusscreencam
Lotus ScreenCam ムービー	application/x-screencam
Lotus ScreenCam ムービー	video/x-scm
Lotus ScreenCam ムービー	video/x-screencam

表 B-1.　MIME コンテンツファイルのファイルタイプマッピングテーブル（続き）

ファイルタイプ	MIME コンテンツタイプ
IRCAM サウンドファイル	audio/x-sf
Sonic Foundry ファイル	audio/sfr
Adobe Flash	application/x-shockwave-flash
TAR	application/x-tar
TAR	application/tar
TAR	application/x-gtar
TAR	multipart/x-tar
TAR	application/x-compress
TAR	application/x-compressed
Targa Image	image/tga
Targa Image	image/x-tga
Targa Image	image/targa
Targa Image	image/x-targa
TIFF	image/tiff
TNEF ファイル	application/ms-tnef
TNEF ファイル	application/vnd.ms-tne
ASCII テキスト	text/plain
ASCII テキスト	application/txt
ASCII テキスト	text/html
ASCII テキスト	text/css
UUENCODE	text/x-uuencode

表 B-1.　MIME コンテンツファイルのファイルタイプマッピングテーブル（続き）

ファイルタイプ	MIME コンテンツタイプ
VBScript	text/vbscript
VBScript	text/vbs
VBScript	application/x-vbs
Creative Voice Format （VOC)	audio/voc
Creative Voice Format （VOC)	audio/x-voc
Microsoft RIFF	audio/wav
Microsoft RIFF	application/x-cdf
Microsoft RIFF	application/x-cmx
Microsoft RIFF	image/x-cmx
Microsoft RIFF	drawing/cmx
Microsoft RIFF	application/cmx
Webshots Picture Collection	application/x-webshots
Webshots Picture Collection	application/wbc
Windows Metafile	application/x-msmetafile
Windows Metafile	application/wmf
Windows Metafile	application/x-wmf
Windows Metafile	image/x-wmf
Windows Metafile	zz-application/zz-winassoc-wmf
PKZIP	application/zip
PKZIP	application/x-zip
PKZIP	application/x-zip-compressed

表 B-1.　MIME コンテンツファイルのファイルタイプマッピングテーブル（続き）

ファイルタイプ	MIME コンテンツタイプ
PKZIP	multipart/x-zip
PKZIP	application/x-compress
PKZIP	application/x-compressed
ACE 圧縮ファイル	application/x-ace
ACE 圧縮ファイル	application/x-compressed
Apple サウンド	audio/aiff
Apple サウンド	audio/x-aiff
Apple/SGI の AIFF	audio/aiff
Apple/SGI の AIFF	audio/x-aiff
Apple/SGI の AIFF	sound/aiff
Apple/SGI の AIFF	audio/rmf
Apple/SGI の AIFF	audio/x-rmf
Apple/SGI の AIFF	audio/x-pn-aiff
Apple/SGI の AIFF	audio/x-gsm
Apple/SGI の AIFF	audio/x-midi
Apple/SGI の AIFF	audio/vnd.qcelp
ARJ	application/arj
ARJ	application/x-arj
ARJ	application/x-compress
ARJ	application/x-compressed
ARJ	zz-application/zz-winassoc-arj

表 B-1.　MIME コンテンツファイルのファイルタイプマッピングテーブル（続き）

ファイルタイプ	MIME コンテンツタイプ
Advanced Systems Format （以下、ASF)	video/x-ms-asf
ASF	video/x-ms-asf-plugin
ASF	video/x-ms-wm
ASF	video/x-ms-wmx
ASF	audio/asf
ASF	application/asx
ASF	application/x-mplayer2

付録 C

アーキテクチャと設定ファイル

本付録で説明する内容には、次の項目が含まれます。

モジュールの構成

InterScan Web Security Virtual Appliance（以下、IWSVA) は次のモジュールで構成されます。

- **メインプログラム** — Web コンソールと、IWSVA に必要な基本ライブラリファイルが含まれます。
- **高度な脅威保護** — ICAP 検索または HTTP 検索のいずれかの HTTP 検索と、URL ブロックに必要なサービスが含まれます。
- **アプリケーション制御** — 人気の高いインターネットアプリケーションを自動的に検出し、管理者がポリシーを使用してそれらのアプリケーションを管理できるようにするセキュリティテクノロジを提供します。
- HTTP **検査** — 管理者は動作を識別して、HTTP メソッド、URL、およびヘッダに基づいて Web トラフィックをフィルタできます。
- **情報漏えい対策** — 有効 / 無効に関係なく、システム上のすべての DLP ポリシーが表示されます。
- FTP **検索** : — FTP 検索に必要なサービスが含まれます。
- URL **フィルタ** — Web セキュリティ強化フィルタオプションの機能が含まれます。
- SNMP **通知** — SNMP 対応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が含まれます。
- IWSVA **用** Control Manager **エージェント** — Trend Micro Control Manager（以下、Control Manager) からの監視および設定を可能にする Control Manager エージェントに必要なファイルが含まれます。

サービス

ここで示すサービスを開始または停止するには、ローカルターミナルまたは SSH を使用して、`root` として IWSVA にログオンする必要があります。IWSVA CLI から停止または開始できるのは、HTTP サービスおよび FTP サービスのみです（138 ページの「HTTP/HTTPS トラフィックフローの有効化」および 271 ページの「FTP トラフィックおよび FTP 検索の有効化」を参照)。それ以外のサービスは IWSVA から停止または開始できません。

IWSVA で実行されるサービスは次のとおりです。

- Trend Micro IWSVA Console (java) — Web コンソールをホストする Web サーバです。
- Trend Micro IWSVA for FTP (isftpd) — FTP トラフィックフローと FTP ウイルス検索を使用可能にするサービスです。

- Trend Micro IWSVA for HTTP (iwssd) — FTP over HTTP を含む、HTTP トラフィックフローと HTTP 検索を使用可能にするサービスです。アプレット /ActiveX 対策処理も行います。

  注意： FTP over HTTP は、透過ブリッジモードではサポートされていません。

- Trend Micro IWSVA Log Import (logtodb) — テキストファイルからデータベースにログを出力するサービスです。
- Trend Micro IWSVA Notification Delivery Service (isdelvd) — メールによる管理者への通知と、ブラウザによるユーザへの通知を処理するサービスです。
- Trend Micro SNMP Service (snmpd) — SNMP トラップ通知を SNMP 対応ネットワーク監視デバイスに送信するサービスです。
- Trend Micro Service Monitor (svcmonitor) — HTTP、FTP、アプリケーション制御、Tomcat、および WMI のデーモンの状態を確認するサービスです。
- Trend Micro Database Service (postgres、postmaster) — IWSVA のローカル PostgreSQL データベースを管理するサービスです。このデータベースには、ポリシー設定、レポートログ、および [概要] 画面の統計データが保存されます。
- Trend Micro Authentication Service (AuthDaemon) — iwssd デーモンまたは appd デーモンから認証要求を受け取り、認証結果を返すサービスです。
- Trend Micro Syslog Service (tmsyslogd) — 企業クラスのログ機能を提供し、Syslog イベントを複数の異なるサーバに送信するサービスです。
- Trend Micro Control Manager Service (En_Main) — Control Manager を使用している場合、Control Manager からの IWSVA の設定とステータスレポートを許可するサービスです。
- Trend Micro IWSVA for Dashboard (ismetricmgmtd) — リアルタイムダッシュボードの表示で使用されるシステムリソースデータを収集するサービスです。

予約タスク

IWSVA を設置すると、セットアッププログラムによって予約タスクがいくつか作成されます。

- purgefile — 毎日午前 2 時に実行され、ログの保持期間の設定に従って古くなったテキストログファイルを削除します。
- schedulereport — 1 時間ごとに実行され、予約レポートが起動するよう設定されているかどうかを確認します。
- schedulepr_update — 1 日に 1 回実行され、製品ライセンスのステータスを確認します。

- schedule_au — 15 分ごとに実行され、パターンファイルまたはその他のプログラムコンポーネントのアップデート時期かどうかを確認します。
- cleanfile — 1 時間ごとに実行され、検索または大容量ファイルの検索に伴ってダウンロードした一時ファイルを削除します。
- DbOldDataCleanup.sh — 毎日午前 2 時 5 分に実行され、データベース内で古くなったレポーティングログのデータおよびアクセス割り当てカウンタをクリーンナップします。
- svc_snmpmonitor.sh — 5 分ごとに実行され、logtodb、mail、postgres、および metric の各デーモンが動作していることを確認します。これらのデーモンが動作していない場合は、それらを再起動します。
- db_reindex.sh — 毎日、1 時間おきの 28 分に実行され、無効なデータが含まれる破損したデータベースインデックスを復元します。これにより、最適なデータベースのパフォーマンスを維持します。
- db_vacuum.sh — 毎日、午前 3 時 58 分に実行され、最適なデータベースのパフォーマンスを維持するために、ガーベージコレクションを実行して、未使用スペースをデータベーステーブルから使えるようにします。
- S99ISSnmpd restart — 毎日、午前 1 時 48 分に実行され、SNMP デーモンを再起動します。
- tomcatchecker.sh — 毎日、午前 1 時 18 分、午前 4 時 18 分、午前 6 時 18 分、午後 10 時 18 分に実行され、Tomcat サービスを再起動する必要がないかどうかを確認します。
- schedule_crl_update.sh — 毎日、午前 2 時に実行され、証明書の失効リスト (CRL) をアップデートします。
- IniRecover.sh — 毎日、午前 3 時 55 分に実行され、`/etc/iscan/intscan.ini` ファイルを回復する必要がないかどうかを確認します。
- log_purge.py — 毎日、午前 1 時 30 分に実行され、古くなったテキストログファイルを削除します。
- clear_tmpfs.py — 毎日、午前 3 時に実行され、tmpfs をクリアします。
- month_table.sh — 毎日、午前 4 時に実行され、ログやレポート機能で利用される月次のテーブル作成のスケジュールを設定します。
- logpurge.sh — 毎日、午前 1 時 20 分に実行され、***report_log.**** をクリアします。このファイルは `/etc/iscan/log` ディレクトリにあります。
- archive_debug_log.py — 1 分ごとに実行され、デバッグログのアーカイブ時期かどうかを確認します。
- bifconnect.sh — 毎週土曜日、午前 1 時 15 分に実行され、製品情報を Control Manager に送信します。

- logbackup.sh — 毎日、午前 0 時 20 分に実行され、バックアップログのスケジュールを設定します。

設定ファイルについて

設定ファイルにアクセスするには、ローカルターミナルまたは SSH を使用して、root としてアプライアンスにログオンする必要があります。

設定ファイルには、メイン、プロトコルモジュール、検索モジュール用の 3 種類があります。すべての設定ファイルは {IWSS root} ディレクトリにあります。{IWSS root} の初期設定は /etc/iscan/ です。メインの設定ファイルは、/etc/iscan/intscan.ini です。

- ウイルス検索固有の設定は、次のファイルにあります。

  `{IWSS root}/IWSSPIScanVsapi.dsc`

- ICAP プロトコル固有の設定は、次のファイルにあります。

  `{IWSS root}/IWSSPIProtocolIcap.pni`

- スタンドアロンプロキシ固有の設定は、次のファイルにあります。

  `{IWSS root}/IWSSPIProtocolHttpProxy.pni`

- URL フィルタ検索モジュールの設定は、次のファイルにあります。

  `{IWSS root}/IWSSPIUrlFilter.dsc`

- レポート固有の設定は、次のファイルにあります。

  `{IWSS root}/report.ini`

- ボットネット検索固有の設定は、次のファイルにあります。

  `{IWSS root}/IWSSPINcieScan.dsc`

- DLP 検索の設定は、次のファイルにあります。

  `{IWSS root}/IWSSPIDlpFilter.dsc`

- HTTP 検査固有の設定は、次のファイルにあります。

  `{IWSS root}/IWSSPISigScan.dsc`

- FTP 検索固有の設定は、次のファイルにあります。

  `{IWSS root}/IWSSPIProtocolFtp.pni`

- アプリケーション制御固有の設定は、次のファイルにあります。

  `{IWSS root}/appcMapping.ini`

- URL 分類データベースの設定は、次のファイルにあります。

  `{IWSS root}/urlfxIFX.ini`

- 初期設定の URL カテゴリと、そのマッピング情報の設定は、次のファイルにあります。

  `{IWSS root}/urlfcMapping.ini`

- IP アドレスと、IWSVA デバイスにアクセスできるすべてのコンピュータの IP アドレスおよび IP の範囲のリストの設定は、次のファイルにあります。

  `{IWSS root}/ClientACL_http.ini (HTTP` **の場合** `)`

  `{IWSS root}/ClientACL_ftp.ini (FTP` **の場合** `)`

- IWSVA で HTTP 要求を転送するポートを定義するルールの設定は、次のファイルにあります。

  `{IWSS root}/HttpPortPermission_http.ini (HTTP` **の場合** `)`

  `{IWSS root}/HttpPortPermission_ftp.ini (FTP` **の場合** `)`

- IWSVA で HTTPS トンネリングを許可するポートを定義するルールの設定は、次のファイルにあります。

  `{IWSS root}/HttpsConectACL_http.ini`

- 信頼されるサーバの IP アドレスと IP の範囲のリストの設定は、次のファイルにあります。

  `{IWSS root}/ServerIPWhiteList_http.ini (HTTP` **の場合** `)`

  `{IWSS root}/ServerIPWhiteList_ftp.ini (FTP` **の場合** `)`

IWSVA Web コンソールは、使用されているモジュールによって異なります。これまで旧バージョンの IWSVA を使用していた場合は、IWSVA には新しい .ini ファイルエントリを必要とする多数の新機能が用意されています。

プロトコルハンドラ

一般に普及している通信プロトコルでメッセージを解釈および処理する関数は、プロトコルハンドラと呼ばれるダイナミックライブラリに含まれています。IWSVA では、IWSVA が ICAP サーバとして動作できるようにする ICAP プロトコルハンドラ、または IWSVA が HTTP プロキシサーバとして動作する HTTP プロキシハンドラを選択できます。HTTP プロトコルハンドラはブリッジモードでも使用されます。アプリケーションバイナリは、プロトコルハンドラから独立しており、設定を変更すれば同じアプリケーションで別のプロトコルをサポートできます。

プロトコルのアクティブな設定ファイルの完全なパスを、`/etc/iscan/intscan.ini`ファイルの [main] セクションにある「protocol_config_path」パラメータに入力します。

プロトコルハンドラには、固有の設定ファイルが必要です。このファイルには、そのプロトコルのみに関連するエントリが含まれます。これらのプロトコル設定ファイルは、ファイル名の `.pni` という拡張子で示されます。

検索モジュール

トラフィックの検索機能は、検索モジュールとして知られるダイナミックライブラリを使用して提供されます。IWSVA で使用できる最初の検索モジュールは、検索エンジンを使用するコンテンツ検索を提供します。

各検索モジュールには、拡張子 `.dsc` を持つ設定ファイルがあります。IWSVA アプリケーションは、`/etc/iscan/intscan.ini` ファイルの [scan] セクションにある「plugin_dir」パラメータに示されるディレクトリで `.dsc` ファイルを探すことにより、使用可能な検索モジュールを検出します。

付録 D

IWSVA のベストプラクティス

本付録では、InterScan Web Security Virtual Appliance（以下、IWSVA) を使用するためのベストプラクティスについて説明します。

内容は次のとおりです。

共有パーソナルコンピュータで複数のユーザを認証する (標準認証方法)

認証に Microsoft Active Directory サーバを使用して 1 つの共有パーソナルコンピュータ (PC) で複数のユーザをサポートすることが、IT マネージャとユーザにとっての課題になることがあります。IWSVA は、ブラウザの機能に基づく認証機能を提供し、Microsoft Internet Explorer を初期設定のブラウザとして使用することで、共有 PC における複数ユーザの認証をサポートします。

ベストプラクティスの提案

Microsoft ShellRunas ユーティリティの利用

- 共有 PC では、Microsoft ShellRunas ユーティリティを利用して、Microsoft Internet Explorer が開始されるたびにユーザ認証を強制することができます。ユーザの認証には AD 認証情報が使用されます。Internet Explorer はその認証情報を使用して、HTTP ヘッダにユーザ ID 情報を自動的に入力するため、IWSVA は、ログ記録、レポート作成、およびポリシー適用の目的でユーザを識別できるようになります。
- 次のサイトから MS ShellRunas ユーティリティをダウンロードします。

  http://technet.microsoft.com/ja-jp/sysinternals/cc300361.aspx
- コンピュータの使用が終了したら、ユーザは、必ず IE ブラウザセッションをシャットダウンする必要があります。これにより、Microsoft Internet Explorer は次のユーザに認証情報の入力を促すことができます。このツールが正常に機能するためには、ユーザがこのことを認識していることが重要です。
- 認証されたユーザキャッシュのキャッシュ間隔を延長または短縮するように IP ユーザキャッシュパラメータを変更して、ユーザに認証情報の入力を促すタイミングを微調整することもできます。IWSVA の初期設定のユーザキャッシュ値は 2 時間 (120 分) です。詳細については、「`configure module ldap ipuser_cache interval <` **間隔** `>`」CLI コマンドを参照してください。

検索に関する考慮事項

IWSVA の不正プログラム検索アーキテクチャはハイブリッドソリューションで、トレンドマイクロの Smart Protection Network (SPN) などのクラウドベースの不正プログラム検出方法、ローカルなオンボックス検索テクノロジ、およびシグネチャファイルを使用します。

Smart Protection Network — クラウドベースのサービス

IWSVA の Smart Protection Network（SPN) は、業界最高のパフォーマンスを備えたクラウドベースの不正プログラム対策サービスです。Smart Protection Network には、以下のような不正プログラム検出コンポーネントがあります。

- Web **レピュテーションサービス** (WRS) は、既知の不正な Web サイト、ドメイン、ファイル、オブジェクト、およびメール関連項目の事前検出とブロック機能（ファーミング / フィッシング検出など) を提供する相関性のあるいくつかのサービスから構成されています。
  - ドメインレピュテーション
  - ページレピュテーション
  - メールレピュテーション
  - ファイルレピュテーション
- URL **フィルタサービス**では、URL データベースをクラウドに格納してデータベースの迅速な更新を実現し、トレンドマイクロのグローバルなユーザベースを保護します。このとき、IWSVA サーバで URL データベースファイルのダウンロードや更新を行う必要はありません。これにより最新の URL 情報がすべてのお客さまに提供されます。また事前保護機能の迅速化が図られ、不正サイトが発見されてから不正サイトが URL データベースに追加されるまでの時間が短縮されることで、すべてお客さまが保護されます。
- **フィードバックループ**は、すべてのトレンドマイクロ製品からのリアルタイムの情報を提供し、SPN のクラウドベースのコンポーネントと URL フィルタデータベースを更新します。顧客端末で発見された不正プログラムは、クラウドアーキテクチャにフィードバックされ、情報をリアルタイムに微調整するために使用されます。これにより、トレンドマイクロのグローバルなユーザベースで、誤警告の少ない迅速な事前防止機能が実現します。

ベストプラクティスの提案

Smart Protection Network（SPN) は、クラウドベースのサービスを使用し、検索に DNS クエリを利用します。迅速な応答と最小限の待ち時間を実現するために、IWSVA デバイスはプライマリおよびセカンダリ DNS サーバで構成されている必要があります。

DNS サーバは、IWSVA による多くの DNS 要求をサポートできる必要があります。通常、IWSVA によってローカルな DNS キャッシュが作成されるまでは、アクセスされる URL ごとに 2 つの DNS 要求が作成されます。DNS サーバが、必要以上の DNS を処理できるだけのリソースとパフォーマンスを備えたサーバに設置されていることを確認します。

待ち時間を少なくするには、DNS サーバが高速なネットワークカードを保有し、高速なネットワークスイッチに取り付けられている必要があります。

トレンドマイクロは、現地 DNS サーバと、企業ネットワーク外に設置された ISP 提供の DNS サーバを使用することをお勧めします。通常、IPS DNS サーバは待ち時間が長く、単一の IP アドレスからの多量の DNS クエリはサポートしません。多くの IPS DNS サーバは、1 秒あたりの DNS 要求数を制限する調整メカニズムを備え、IWSVA の Web レピュテーションサービス (WRS) のパフォーマンスに影響を与える可能性があります。

ネットワーク応答時間とパフォーマンスを向上させるには、DNS サーバを IWSVA のできるだけ近くに設置し、デバイス間の不要なネットワークホップを削減するようにしてください。

WRS と URL フィルタ要求は、HTTP ポート 80 を介して作成されます。ファイアウォール上のこれらのポートでは、IWSVA の管理 IP アドレスをブロックしないでください。

ローカルな IWSVA 検索エンジン

IWSVA は、ローカルなオンボックス検索機能を備え、インターネットからダウンロードされたコンテンツに対して不正プログラムの検索が実行されるようにします。Smart Protection Network の Web レピュテーションサービスと URL フィルタサービスでは、既知の不正サイトとコンテンツおよび新たに発見された不正サイトとコンテンツの大部分をフィルタできますが、ローカルなファイル検索では、受信したファイルとオブジェクトにウイルス、ワームや、トロイの木馬などの不正プログラムが埋め込まれていないことを確認します。

IWSVA には、以下のローカル検索エンジンがあります。

- **ファイルタイプブロック**では、60 を超えるさまざまなファイルの MIME タイプを識別してブロックすることができます。このファイルには、Java アプレット、実行可能ファイル、Microsoft Office ドキュメントなどの一般的なファイルが含まれます。サポートされているファイルタイプの詳細については、429 ページの「ファイルタイプと MIME コンテンツタイプの対応」を参照してください。
- **ウイルス検索** (VSAPI) では、シグネチャベースのウイルス検索と不正プログラム検索を実行します。
- **トレンドマイクロの推奨設定**では、実際のファイルタイプに基づいてファイルの特定と検索を実行するため、ファイル拡張子を変更したり他の形式のファイル操作を使用したりして、ユーザが検索エンジンをバイパスするのを防ぐことができます。
- IntelliTrap はヒューリスティックな検索機能を提供し、ネットワーク内を移動するときに状態を変える不正プログラムを特定して防御します。
- **圧縮ファイルの検索**は、何度も圧縮された高度な圧縮ファイルに潜む不正プログラムを防御します。不正プログラムの作成者たちは、この一般的な配信方法を使用して、従来のウイルス対策検索ソフトウェアから逃れようとします。

- **スパイウェア検索**は、スパイウェア、ダイヤラー、ハッキングツール、パスワード解読アプリケーション、アドウェア、ジョークプログラム、リモートアクセスツール、およびその他のグレーウェアを防御します。このローカル検索エンジンは、スパイウェアシグネチャに基づく防御機能を提供し、URL フィルタ機能にあるスパイウェア URL カテゴリの補完に使用されます。ローカルなスパイウェア検索エンジンは、スパイウェアやグレーウェアに感染している可能性のある、インターネットからダウンロードされたファイルまたはインターネットにアップロードされたファイルの検索に使用されます。一方、URL フィルタのスパイウェアカテゴリは、スパイウェアに関連するファイルとオブジェクトを含んでいることがわかっているサイトへのアクセスを事前にブロックするために使用されます。
- **サイズの大きいファイルの検索**を使用すると、管理者は、多くのシステムリソースを消費する可能性のあるサイズの大きいファイルの検索をバイパスすることができます。従来、不正プログラムの作成者たちは、多くの注意をファイルに向かせることなく不正プログラムをすばやく拡散させたいため、サイズの大きいファイルにウイルスを埋め込みません。

ベストプラクティスの提案

- IWSVA のローカル検索サービスは、不必要な検索を減らすために、特定の順番で動作します。IWSVA でのインターネットトラフィックの検索は、Smart Protection Network のクラウドベースの予防的サービスから始まって、次の順序で行われます。
  - Web レピュテーションサービス (WRS)
  - URL フィルタサービス
  - ファイルタイプブロック
  - ウイルス検索
  - IntelliTrap ヒューリスティック
  - MacroTrap
  - トレンドマイクロの推奨設定の実際のファイルタイプ
- ウイルス検索 (VSAPI) の検索エンジンは、多くのリソースを消費します。Web レピュテーションサービス (WRS) を有効にし、URL フィルタサービスに加入し、そのコンピュータ / 危険カテゴリを有効にすると、従来の VSAPI ベースのウイルス検索を実行する必要性を大幅に低減することができます。このような変更を行うと、サーバリソースを削減し、使用環境に新たな拡張性をもたらすことができます。
- 高い整合性評価を持つ、許可リストにある信頼されたサイトとファイルについては、不正プログラム検索を無効にすると、パフォーマンスを向上させサーバリソースの使用を軽減することができます。[除外設定] タブの [グローバル URL の信頼]、[承認する URL]、および [除外ファイル] の許可リストを使用して、信頼するサイトとファイルの検索をバイパスします。

- 特定のサイズを超えるファイルの検索を省略するように、サイズの大きいファイルの検索を設定できます。これにより、大きなファイルの不要な検索を減らし、リソース使用率を下げて、能力とパフォーマンスを向上させることができます。
- 大きなファイルのダウンロードに対するユーザ応答時間を向上させるには、[サイズの大きいファイルの処理] 機能の [遅延検索] オプションを有効にし、要求元ホストに検索されたファイルの一部を少しずつ配信するようにします。これにより、ブラウザのファイル転送状態のインジケータが維持され、ファイルの検索中の進行状況がユーザに表示されます。少量ずつ配信されているファイルの中で不正プログラムが見つかると、IWSVA はファイルの残りをブロックします。その結果、実行できない不完全なファイルが生成されます。マルチメディアファイルや、YouTube コンテンツなどの HTTP ポート 80 を使用するストリーミングコンテンツの場合は、[遅延検索] を有効にし、メディアの一部が流れるようにする必要があります。[配信前に検索] オプションを選択すると、ストリーミングコンテンツは完全に検索されるまでブロックされるため、ユーザの操作性が悪くなります。
- ユーザに配信する前にファイル全体を検索する必要のあるお客さまの場合は、[サイズの大きいファイルの処理] 機能の [配信前に検索] オプションを選択してください。これにより、IWSVA はファイルをバッファに格納し、ファイルをユーザに配信する前に検索を完了します。この方法は、エンドユーザのパフォーマンスの認識の点では若干遅くなりますが、感染ファイルは一部たりとも侵入できません。
- [除外設定] タブには、HTTP/FTP 検索ポリシーにある許可リストの項目を検索するオプションがあります。

付録 E

WCCP の配信およびトラブルシューティング

本付録では、Cisco 社の Web Cache Communication Protocol（WCCP) を使用する InterScan Web Security Virtual Appliance（以下、IWSVA) の設備の配置およびトラブルシューティングについて説明します。

内容は次のとおりです。

WCCP について

Web Cache Communication Protocol（WCCP）をサポートしている Cisco 社製ルータおよびスイッチは、1 台以上の透過プロキシ Web キャッシュサーバにトラフィックをリダイレクトできます。Web キャッシュにより、エンドユーザは以前にアクセスしたことのある Web ページを、Web サーバからではなくメモリバッファまたは「キャッシュ」から取得できるので、ネットワークの遅延が減少します。

Cisco 社では、適応型セキュリティアプライアンス（ASA）と外部 Web キャッシュデバイスのやり取りを制御するために WCCP を作成しました。WCCP は Web キャッシュデバイスの負荷を軽減するだけでなく、負荷分散機能や、複数のルータおよびプロトコルをサポートする機能も提供します。WCCP はエンドユーザには意識されず、エンドポイントデバイスで設定を変更する必要はありません。

IWSVA および WCCP の概要

本付録では、IWSVA を WCCP モードで実行するための設定方法や、n 階層環境で Cisco WCCP が有効化されているデバイスとの通信方法について説明します。IWSVA を WCCP モードで実行し、Cisco WCCP デバイスと統合すると、特にキャッシュされたコンテンツを処理するわけではなくても、「Web キャッシュ」となります。代わりに、ASA の「キャッシュエンジン」となり、Web コンテンツのフィルタおよび検索のための Web ゲートウェイ機能を実行します。

本書で示す例では、IWSVA および Cisco WCCP 対応デバイスで必要な設定手順を説明しています。トレンドマイクロでは、WCCP をサポートするすべての Cisco 製デバイスをテストおよび検証することはできませんが、WCCP を使用する IWSVA の各バージョンでテストを実行しています。

注意： IWSVA の WCCP 実装の初期設定では、WCCP サービス 80 および動的 WCCP サービスタイプとなっており、ほとんどの WCCP v2 実装と互換性があります。ただし、Cisco 製デバイスが 80 以外の別の WCCP サービス番号または標準 WCCP サービスメソッドを使用している場合は、それに合わせて IWSVA の WCCP パラメータを変更する必要があります。IWSVA の WCCP サービスパラメータの変更方法の詳細については、478 ページの「IWSVA に関するその他のヒント」を参照してください。

本書で示す例は、IWSVA および以下の Cisco 製品を使用して作成されています。

- IOS バージョン 12.4（13r）T を実行する Cisco 2821 ルータ
- IOS バージョン 12.2（40）SE を実行する Cisco 3750 スイッチ
- バージョン 8.4（35）k8 を実行する Cisco ASA 5510

Cisco 2821 ルータに WCCP を配信する

Cisco 製ルータの既知の問題および配信要件は、次のとおりです。

1. Cisco IOS バージョン 12.2 (23) ～ 12.3 (9) では、WCCP の接続性の問題が知られています。これらのバージョンは、IWSVA との統合を避けてください。
2. 自動的に選択されるルータ ID は、Cisco 製ルータで設定される最上位の IP アドレスです。この IP アドレスをサポートするインタフェースに IWSVA デバイスが直接アクセスできない場合は、WCCP L2 のリダイレクションメソッドが機能しません。この場合、ルータ ID を使用して設定されたインタフェースと IWSVA が通信できるように、適切なルートエントリが設定され、ルータおよびスイッチで有効化されていることを確認する必要があります。

配信例

この例では、IOS 12.4 (13r) T を実行する Cisco 2821 ルータを 2 つのネットワークセグメント (プライベートネットワークおよび外部ネットワークに接続された DMZ ネットワーク) で使用しています。

- **プライベートネットワーク** — 192.168.1.0/24 — 192.168.1.1 をゲートウェイアドレスとして使用する、Cisco 製 Gigiabit Ethernet 0/0 インタフェースでサポートされます。
- DMZ **ネットワーク** — 172.16.1.0/24 — 172.16.1.5 をゲートウェイアドレスとして使用する、Cisco 製 Gigiabit Ethernet 0/1 インタフェースでサポートされます。
- IWSVA **デバイス** — 172.16.1.101 — WCCP キャッシュデバイスとして動作し、コンテンツの検索およびフィルタを実行します。

プライベートネットワークは企業のクライアントコンピュータをホストし、DMZ ネットワークには外部ネットワークに接続されたサーバ (Web、FTP など) および IWSVA が置かれます。IWSVA は、図 E-1 に示すように、企業のファイアウォールを通じてインターネットにアクセスできます。

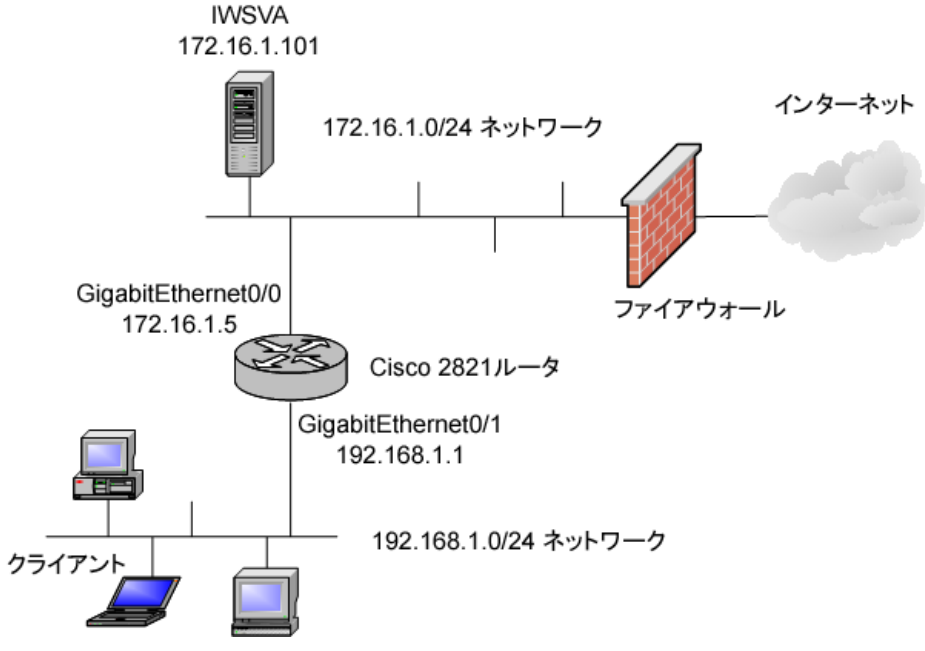


図 E-1.　Cisco 2821 ルータを実装するトポロジ例

Cisco 2821 ルータを設定する

Cisco 製のルータに管理者権限でログインし、次の設定手順を実行します。

Cisco 2821 ルータを設定するには

1. Cisco 製ルータのターミナル設定モードに入ります。

   ```
   Hostname#conf t
   Hostname(config)#
   ```

2. クライアントプロトコルを含むリダイレクトリストを、IWSVA にリダイレクトされるように設定します。この例では、HTTP、WWW、および FTP プロトコルがリダイレクトされ、検索さ

れます。この例で使用されるアクセスリスト番号は 101 です。ただしこの番号は、お使いの環境とは異なる可能性があります。

```
Hostname (config)# access-list 101 permit tcp 192.168.1.0 0.0.0.255 any eq www
```

```
Hostname (config)# access-list 101 permit tcp 192.168.1.0 0.0.0.255 any eq ftp
```

3. WCCP サーバのすべてのメンバーが含まれるグループリストを設定します。この例では、IWSVA メンバーでグループリストを設定しました。WCCP は、前の手順で選択したプロトコルを、このグループリストで指定された IWSVA に転送します。この例で使用されるアクセスリスト番号は 22 です。この番号は、お使いの環境とは異なる可能性があります。

   ```
   Hostname (config)# access-list 22 permit 172.16.1.101 0.0.0.1
   ```

4. Cisco 製ルータで WCCP を有効にします。この例で使用される WCCP サービス番号は 80 です。初期設定では、IWSVA は動的 WCCP サービスでサービス番号 80 を常に使用します。Cisco IOS 12.2 または 12.3 を使用している場合、WCCP のバージョンは初期設定で 2 となっています。こうした場合は、WCCP のバージョンを設定する必要はありません。お使いの Cisco 製デバイスが同じ値に設定されていることを確認してください。この例で使用されるパスワードは「novirus」に設定されており、IWSVA の WCCP 設定で指定されたパスワードと一致する必要があります。

   ```
   Hostname (config)# ip wccp 80 redirect-list 101 group-list 22 password novirus
   ```

5. トラフィックをインターネットに到達させるインタフェースで、WCCP アウトバウンドリダイレクションを有効化します。このインタフェースは、キャッシュデバイスをインストールしたインタフェース（この例では IWSVA）である必要はありません。この例では、インターネットに直接接続するインタフェースは 0/0 であり、このルータインタフェースでの WCCP リダイレクションは OUT で有効化されています。

   ```
   Hostname (config)# interface GigabitEthernet0/0
   ```

   ```
   Hostname (config-if)# ip wccp 80 redirect out
   ```

6. クライアントデバイスからトラフィックを受信するインタフェースで、WCCP インバウンドリダイレクションを有効化します。この例では、クライアントに直接接続するインタフェースは 0/1 であり、このルータインタフェースでの WCCP リダイレクションは IN で有効化します。

   ```
   Hostname (config)# interface GigabitEthernet0/1
   ```

   ```
   Hostname (config-if)# ip wccp 80 redirect in
   ```

   Cisco 2821 ルータは、ハッシュおよびマスクの割り当て方法のほかに、GRE および L2 の転送方法をサポートできます。上記の例では、パフォーマンス強化のため、転送方法は L2、割り当て方法はマスクが選択されています。

Cisco 3750 スイッチに WCCP を配信する

Cisco 製スイッチの既知の問題および配信要件は、次のとおりです。

1. Cisco IOS バージョン 12.2 (23) ～ 12.3 (9) では、WCCP の接続性の問題が知られています。これらのバージョンは、IWSVA との統合を避けてください。
2. WCCP エントリおよび PBR エントリは、同じ TCAM 領域を使用します。WCCP は、PBR をサポートするテンプレート（アクセス、ルーティング、およびデュアル IPv4/v6 ルーティング) のみでサポートされます。その結果、WCCP をサポートするスイッチ（3750、3560 シリーズなど) では、SDM テンプレートを変更して「初期設定」とは別の設定にする必要があります。TCAM エントリで WCCP エントリを追加できない場合は、パケットはリダイレクトされず、標準ルーティングテーブルを使用して転送されます。
3. IWSVA は WCCP が有効なスイッチに直接接続する必要があります。それらは同じサブネットワークに存在する必要があります。
4. Web クライアント、IWSVA、および Web サーバにレイヤ 3 インタフェース（ルートされるポートおよびスイッチ仮想インタフェース [SVI]) として接続されているスイッチインタフェースを設定します。WCCP のパケットリダイレクションが機能するためには、サーバ、IWSVA、およびクライアントが別々のサブネットにある必要があります。
5. スイッチでサポートされる転送と割り当ての方法を確認し、これら 2 つが IWSVA で正しく設定されていることを確認します。たとえば、3560 シリーズおよび 3750 シリーズは、転送方法は L2、割り当て方法はマスクのみをサポートしています。
6. WCCP および VPN ルーティング / 転送（VRF) を同一のスイッチインタフェースで設定することはできません。
7. WCCP および PBR を同一のスイッチインタフェースで設定することはできません。
8. WCCP およびプライベート VLAN (PVLAN) を同一のスイッチインタフェースで設定することはできません。

配信例

この例では、IOS 12.2 (40) SE を実行する Cisco 3750 スイッチを、2 つの VLAN ネットワークセグメント（VLAN 30 および VLAN 160) で使用しています。

- **VLAN 30 ネットワーク** — 10.168.30.0/24 — 企業ネットワークのクライアントをサポートしています。この VLAN では、ゲートウェイアドレスを 10.168.30.254 に設定しています。
- **VLAN 160 ネットワーク** — 10.168.160.0/24 — IWSVA およびその他のサーバをサポートし、企業ファイアウォールを介してインターネットに接続できます。この VLAN では、ゲートウェイアドレスを 10.168.160.254 に設定しています。

- **IWSVA デバイス** — 10.168.160.54 — WCCP キャッシュデバイスとして動作し、コンテンツの検索およびフィルタを実行します。

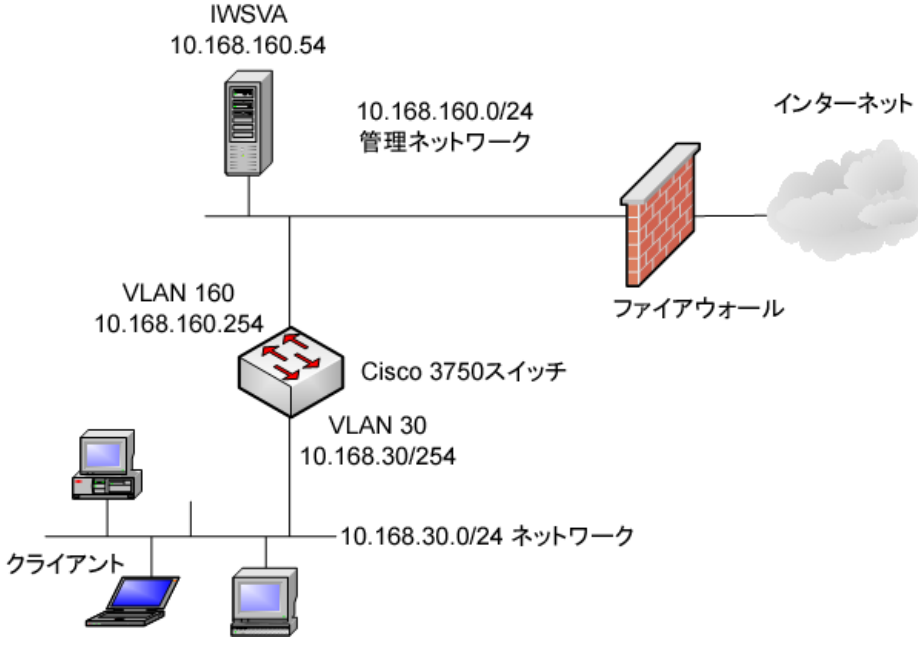


図 E-2. Cisco 3750 **スイッチを実装するトポロジ例**

Cisco 3750 スイッチを設定する

Cisco 3750 スイッチに管理者権限でログインし、次の設定手順を実行します。

Cisco 3750 スイッチを設定するには

1. Cisco 製スイッチのターミナル設定モードに入ります。

   ```
   Switch #conf t
   Switch(config)#
   ```

2. クライアント VLAN を含むアクセスリストを、IWSVA にリダイレクトされるように設定します。この例では、10.168.30.0/24 クライアントサブネットをリダイレクトします。使用されているアクセスリストは標準のリストで、WCCP80 はこの ACL の識別子です。この識別子は、お使いの環境の命名規則に合わせて変更できます。

```
Switch (config)# ip access-list standard wccp80 permit 10.168.30.0
0.0.0.255
```

3. WCCP キャッシュのすべてのメンバーが含まれるグループリストを設定します。この例では、グループリストは IWSVA デバイスの 10.168.160.54 の IP アドレスで設定されます。前の手順で選択したトラフィックが WCCP により転送される場合は、IWSVA デバイスがインバウンドリダイレクションを処理します。group80 はこの ACL の識別子で、お使いの環境の命名規則に合わせて変更できます。

   ```
   Switch (config)# ip access-list standard  group80 permit  host
   10.168.160.54
   ```

4. Cisco 製スイッチで WCCP を有効にします。この例で使用される WCCP サービス番号は 80 です。初期設定では、IWSVA は動的サービスタイプでサービス番号 80 を使用します。お使いの Cisco 製デバイスが同じ値に設定されていることを確認してください。この例で使用されるパスワードは「novirus」に設定されており、IWSVA の WCCP 設定で指定されたパスワードと一致する必要があります。

   ```
   Switch (config)# ip wccp 80 redirect-list wccp80 group-list group80
   password novirus
   ```

5. クライアントに接続する VLAN インタフェースで、WCCP インバウンドリダイレクションを有効化します。クライアント側のインタフェースは、IWSVA および Web サーバの VLAN とは異なる VLAN（サブネット）に存在する必要があります。そうでない場合、適切な WCCP リダイレクションが失敗します。この例では、クライアント側のサブネットが VLAN30、IWSVA サーバ側のサブネットが VLAN160 となっています。

   ```
   Switch (config)# interface vlan 30

   Switch (config-if)# ip wccp 80 redirect in
   ```

6. WCCP を設定するための IWSVA デバイスの Web UI で、転送方法に L2、割り当て方法にマスクが選択されていることを確認してください。Cisco 3750 スイッチでは、これら 2 つのパラメータに対して上記の設定のみがサポートされます。

Cisco ASA デバイスに WCCP を配信する

Cisco ASA デバイスの既知の問題および配信要件は、次のとおりです。

1. Cisco ASA は、WCCP をサポートするためにバージョン 7.2.1 以上を実行する必要があります。バージョン 7.2 (2) と IWSVA には互換性の問題があることが知られているので、バージョン 7.2 (2) の使用は避けてください。
2. Cisco ASA は、クライアントと IWSVA デバイスが ASA デバイスの同じ内部インタフェースに接しているトポロジのみをサポートします。これにより IWSVA は、ASA デバイスを介することなくクライアントホストと直接通信できます。
3. 自動的に選択されるルータ ID は、Cisco ASA で設定される最上位の IP アドレスです。ルータ ID が、DMZ インタフェースや外部インターネットに直接接続するインタフェースなど、IWSVA デバイスの外部のインタフェースに設定された場合、必要なすべてのルーティングデバイスおよびスイッチングデバイスで適切なルートを定義して、IWSVA がルータ ID の IP アドレスにアクセスできるようにする必要があります。

配信例

この例では、ソフトウェアバージョン 8.4 (35) k8 を実行する Cisco ASA 5510 を 2 つのネットワークセグメント (内部ネットワークおよび外部ネットワーク) で使用します。

- **内部ネットワーク** — 192.168.1.0/24 — クライアントが存在する内部ネットワークをサポートします。この内部ネットワークには、IWSVA デバイスも存在します。192.168.1.1 は、ASA の 0/1 インタフェースで定義されるゲートウェイアドレスです。
- **外部ネットワーク** — 172.16.12.0/24 — 外部ネットワークおよびインターネットへのパスをサポートします。172.16.12.1 は、ASA の 0/0 インタフェースで定義されるゲートウェイアドレスです。

- IWSVA **デバイス** — 192.168.6.10 — WCCP キャッシュデバイスとして動作し、コンテンツの検索およびフィルタを実行します。

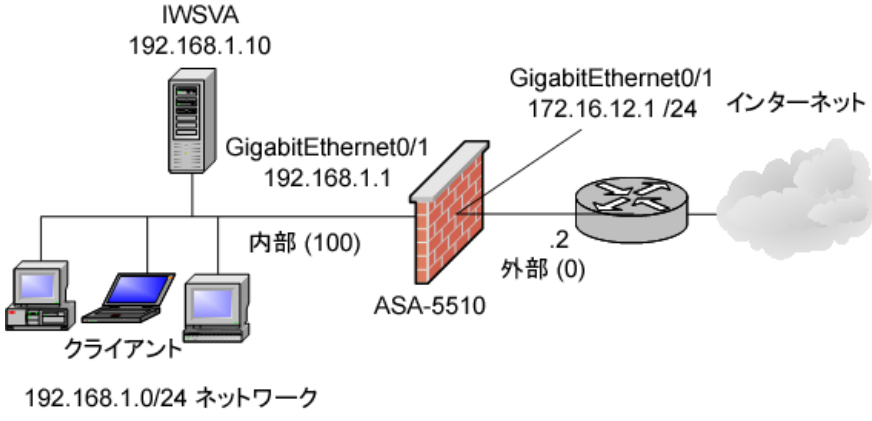


図 E-3. Cisco ASA **を実装するトポロジ例**

Cisco ASA を設定する

Cisco ASA に管理者権限でログインし、次の設定手順を実行します。

Cisco ASA を設定するには

1. Cisco ASA のターミナル設定モードに入ります。

   ```
   ASA #conf t
   ASA(config)#
   ```

2. WCCP サーバメンバーが含まれるアクセスリストを設定します。この例では、IWSVA デバイスとなる WCCP サーバは 1 台のみです。

   ```
   ASA (config)# access-list wccp-servers permit ip host 192.168.1.10 any
   ```

3. アクセスリストを作成して、ASA がトラフィックをキャッシュサーバにリダイレクトできるようにします。この例では、192.168.1.0/24 のサブネットは、キャッシュサーバとして動作する IWSVA にリダイレクトされます。

   ```
   ASA (config)# access-list wccp-traffic permit ip 192.168.1.0
   255.255.255.0 any
   ```

4. 「wccp-traffic」フィルタから「wccp-servers」デバイスへトラフィックをリダイレクトするように WCCP を設定します。この例で使用されるパスワードは「novirus」に設定されており、IWSVA の WCCP 設定で指定されたパスワードと一致する必要があります。

   ```
   ASA (config)# wccp web-cache group-list wccp-servers redirect-list
   wccp-traffic password novirus
   ```

5. 内部クライアントインタフェースで WCCP インバウンドリダイレクションを有効化します。この例では、内部クライアントインタフェースは「inside」と呼ばれます。標準サービスは「web-cache」(サービスグループ ID 0) で、TCP ポート 80 (HTTP) のトラフィックをインターセプトしてキャッシュサーバにリダイレクトします。

   ```
   ASA (config)# wccp interface inside web-cache redirect in
   ```

   この例では、IWSVA デバイスの WCCP 設定の Web UI 画面で、転送方法は GRE、割り当て方法はハッシュが選択されています。

WCCP 配信モードで IWSVA を設定する

WCCP は、IWSVA のすべてのバージョンでサポートされています。設定手順は IWSVA の各バージョンで非常に類似しているため、本書では特に IWSVA のインストール手順について説明します。

IWSS と IWSVA WCCP の配信の細かい相違点は次のとおりです。

- **転送方法** — IWSVA 製品は、GRE と L2 の転送方法をどちらもサポートします。一般的に、L2 の転送方法は GRE よりもパフォーマンスが高くなりますが、ネットワークトポロジおよび Cisco 製デバイスに応じてパフォーマンスは異なります。たとえば、WCCP バージョン 1 をサポートする Cisco 製ルータは、L2 の転送方法を使用できません。
- **ルータ IP アドレス** — WCCP サービスグループのルータ ID が、トポロジ設計に影響を与える可能性があります。ルータ ID は IPv4 アドレスとして扱われますが、WCCP で生成された任意の GRE フレームの送信元アドレスとしても使用できます。GRE の転送方法を設定すると、IWSVA ではルータ ID を GRE パケットの送信元 IP アドレスとして使用します。

  ほとんどの Cisco 製ルータでは、ルータ ID を再設定できません。Cisco 製ルータは、ルータで定義された最も到達可能性が高い IPv4 アドレスを利用して、ルータ ID を自動的に選択します。ただし、この IP アドレスは、WCCP ルータ ID に関しては最善の選択とならない場合があり、お客さまはルータ ID の IP アドレスと IWSVA デバイスが通信できるようにネットワークデバイスのルートテーブルを必ずアップデートする必要があります。
- **割り当て方法** — WCCP では、ハッシュまたはマスクの割り当て方法を使用できます。マスクの割り当て方法は、WCCP バージョン 2 に対応する IOS バージョンでのみサポートされます。IWSS 製品はハッシュの割り当て方法のみをサポートしますが、IWSVA 製品はハッシュとマスクの両方の割り当て方法をサポートできます。

IWSVA デバイスで WCCP を設定する

使用する IWSVA のバージョンに応じて、WCCP の設定は配置ウィザードまたはプロキシ配信の HTTP 設定 (旧バージョンの場合) で実行します。この説明の例では、IWSVA を使用して WCCP の設定手順を説明します。

図 4 は WCCP のパラメータを示し、初期設定の WCCP サービス 80 および動的サービスタイプでの基本的な WCCP v2 配信に必要な WCCP の各パラメータについて説明しています。

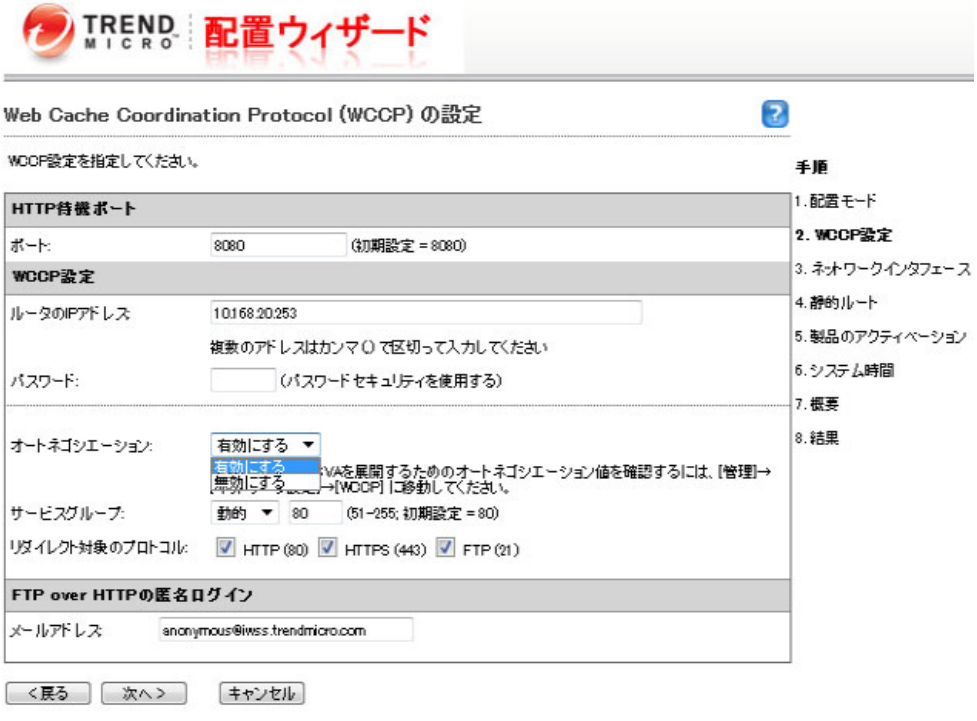


図 E-4.　IWSVA の配置ウィザードの [WCCP 設定] 画面

WCCP の設定および説明については、表 E-1 を参照してください。

表 E-1.　WCCP 設定

パラメータ	説明
ルータの IP アドレス	Cisco 製デバイスで、検索および URL フィルタのために IWSVA デバイスにトラフィックをリダイレクトするインタフェースの IP アドレスを入力します。Cisco 製デバイスの IP アドレスを複数入力する場合は、カンマで区切ります。
パスワード	Cisco 製ルータを WCCP のセキュリティパスワードで設定した場合に使用します。パスワードは、IWSVA と Cisco 製デバイスとで一致している必要があります。
転送方法	WCCP でサポートされている転送方法は、GRE およびレイヤ 2 (L2) です。この設定は、Cisco 製デバイスで指定された転送タイプと一致している必要があります。一般的には L2 転送の方がパフォーマンスが多少高くなりますが、ルーティングが不可能で、クライアントおよび IWSVA を同一のサブネット /VLAN に置く必要があります。
割り当て方法	WCCP プロトコルで使用される、マスクの割り当て方法です。ハッシュテーブルとマスク値のセットがサポートされており、選択された割り当て方法が Cisco 製デバイスの機能と一致する必要があります。サポートされる割り当て方法の詳細については、Cisco 製デバイスの IOS バージョンを確認してください。
サービスグループ	サービスグループは、標準または動的に設定でき、初期設定のサービスグループ ID は 80 です。この値を、Cisco 製デバイスのサービスグループ設定に合わせて変更します。
リダイレクト対象のプロトコル	コンテンツ検索のために、Cisco 製デバイスから IWSVA へリダイレクトされるプロトコルです。HTTP (80)、HTTPS (443)、および FTP (21) のオプションがあります。

IWSVA に関するその他のヒント

Cisco の WCCP は、Cisco 製ルータおよびスイッチ固有の仕様非公開のリダイレクション技術です。そのため、その実装に関しては、異なるデバイスで実行される IOS のバージョン間で多少違う可能性があり、IWSVA デバイスでさらに微調整が必要となる場合があります。ここでは、完全な互換性を実現するために追加の微調整が必要な場合がある、いくつかの例を説明します。

IWSVA の WCCP 設定ファイル

IWSVA は、WCCP 設定ファイルを「/var/iwss」ディレクトリの「IWSSPIProtocolHttpProxy.pni」ファイルに保存し、WCCP デーモンに使用されます。IWSVA WCCP の Web UI 設定画面に表示されない WCCP パラメータを変更する必要がある場合、これが変更対象の設定ファイルになります。トレンドマイクロでは、通常の状況では WCCP の機能は IWSVA の Web UI で設定することをお勧めします。どうしても必要な場合のみ、「IWSSPIProtocolHttpProxy.pni」ファイルを手作業で変更してください。

トレンドマイクロでは、変更の前にファイルのコピーを作成することを強くお勧めします。ファイルをバックアップするには、次のようにコピーコマンド「cp」を使用できます。

```
cp IWSSPIProtocolHttpProxy.pni IWSSPIProtocolHttProxy.pni_backup
```

このファイルは、「vi」などのエディタで開いて変更できます。vi エディタになじみがない場合は、次の Web サイトでコマンドの詳細情報を取得できます。

https://www.cs.colostate.edu/helpdocs/vi.html

変更を加えた場合は必ず、ファイルを保存し、WCCP デーモンを再起動して新しく変更した内容を有効化します。次のコマンドで、WCCP サーバデーモンを再起動します。

```
/usr/iwss/S99ISWCCPd stop
/usr/iwss/S99ISWCCPd start
```

次の WCCP パラメータは、「IWSSPIProtocolHttpProxy.pni」設定ファイルで手作業で変更できます。

```
# Name: wccp_router
# Type: address
# Default:
# Description
# IWSx を登録する Cisco 製ルータの１～８の IP アドレスを
# 入力します。
```

```
# 例: wccp_router=192.168.1.254,192.168.2.254
wccp_router=

# Name: wccp_address
# Type: address
# Default:
# Description
# このオプションは、WCCP で特定のインタフェースアドレスを使用する必要がある場合に使用します。
# 初期設定の動作では、特定のアドレスはバインドされません。
# 例 : wccp_address=192.168.1.1
wccp_address=

# NAME: wccp_forwarding_method
# TYPE: int
# DEFAULT: 1
# Description:
# WCCP2 では、ルータ / スイッチとキャッシュとの間の転送メソッドの設定を
# 使用できます。有効な値は次のとおりです。
# 1 - GRE カプセル化 (GRE/WCCP トンネルでパケットを転送します)
# 2 - L2 リダイレクト (レイヤ 2/MAC の書き直しを使用してパケットを転送します)
wccp_forwarding_method=1

# NAME: wccp_return_method
# TYPE: int
# DEFAULT: 1
# Description:
# このフィールドは将来のために予約されています。この値を変更しても、効果は
# ありません。
wccp_return_method=1

# NAME: wccp_assignment_method
# TYPE: int
# DEFAULT: 2
# Description:
# Cisco の割り当て方法。1 はハッシュ、2 はマスクです。
wccp_assignment_method=2

#wccp_std_service=standard 0
#wccp_dynamic_service=dynamic 80

# NAME: wccp_service
# TYPE: wccp_service
```

```
# DEFAULT:
# Description:
# 動的 WCCPv2 サービスでは、方向を変えたいトラフィックを定義するには、
# さらに詳細な情報が必要です。
# フォーマットは、次のとおりです。
#
#       wccp_service <ID> protocol=< プロトコル > flags=< フラグ >,< フラグ >..
#           priority=< 優先順位 > ports=< ポート >,< ポート >..
#
#       関連する WCCPv2 フラグは、次のとおりです。
#       + src_ip_hash、dst_ip_hash
#       + source_port_hash、dest_port_hash
#       + src_ip_alt_hash、dst_ip_alt_hash
#       + src_port_alt_hash、dst_port_alt_hash
#       + ports_source、ports_defined
#
#       ポートリストには、1 ～ 8 のエントリを含めることができます。
wccp_service=dynamic 80 protocol=tcp flags=src_ip_hash priority=120
ports=80,21,443

# NAME: wccp_service_info
# TYPE: wccp_service_info
# DEFAULT:
# Description:
# 動的 WCCPv2 サービスでは、方向を変えたいトラフィックを定義するには、
# さらに詳細な情報が必要です。
# フォーマットは、次のとおりです。
#
#  wccp_service_info <ID> protocol=< プロトコル > flags=< フラグ >,< フラグ >..
#           priority=< 優先順位 > ports=< ポート >,< ポート >..
#
#       関連する WCCPv2 フラグは、次のとおりです。
#       + src_ip_hash、dst_ip_hash
#       + source_port_hash、dest_port_hash
#       + src_ip_alt_hash、dst_ip_alt_hash
#       + src_port_alt_hash、dst_port_alt_hash
#       + ports_source、ports_defined
#
#       ポートリストには、1 ～ 8 のエントリを含めることができます。

# wccp_service_info=80 protocol=tcp flags=source_port_hash,
src_port_alt_hash priority=120 ports=80,21,443
```

```
# NAME: wccp_password
# TYPE: cyphered text
# DEFAULT:
# Description:
# MD5 サービス認証は、
# wccp_password=< 暗号化されたパスワード > を設定することで有効化できます。
# このフィールドは、ユーザが手作業で変更すべきでないことに注意してください。# ユーザが
WebUI でパスワードを設定すると、UI では
# パスワードを MD5 で暗号化し、設定ファイルに保存します。
wccp_password=

wccp_logging=0
#       0 ― オフ。WCCP ログなし。エラーのみ
#       1 ― オン (初期設定)、WCCP ログを「http.log」ファイルに書き込みます。
```

初期設定の WCCP サービスを変更する

初期設定では、IWSVA は WCCP サービス 80 と動的サービスタイプを使用するように設定されています。これは、多くの WCCP v2 環境で適切に動作しますが、これらの値が Cisco 製デバイスで変更されている場合は、変更が必要な場合があります。

初期設定の WCCP サービス値から変更するには

1. 完全な管理者権限を持つ「root」レベルのユーザを使用して、IWSVA のコンソールにログインします。
2. `cd /etc/iscan` コマンドを使用して、「`/etc/iscan`」ディレクトリに移動します。
3. 「`intscan.ini`」を開いて編集します。たとえば、`vi intscan.ini` コマンドを使用できます。
4. 「`/wccp_service`」と入力して <Enter> キーを押し、「`wccp_service`」パラメータを検索します。おおむね以下のような WCCP 設定が表示されます。初期設定のサービスタイプおよび番号は「dynamic 80」であることに注意してください。

```
wccp_service=dynamic 80 protocol=tcp flags=src_ip_hash priority=120
        ports=80,21,443,8080
```

5. 「`wccp_std=dynamic 80`」を、Cisco 製デバイスでサポートされる値に変更します。たとえば、次の例に示すように「Dynamic 80」を「Standard 0」に変更します。変更の操作の前に、「`i`」で vi エディタを挿入モードにする必要があります。

```
wccp_std_service=standard 0 protocol=tcp flags=src_ip_hash priority=120
ports=80
```

6. <Esc> キーを押して挿入モードを終了します。「:wq」と入力し、上書きして終了します。
7. 次のコマンドで、WCCP サーバデーモンを再起動します。

```
/usr/iwss/S99ISWCCPd stop
/usr/iwss/S99ISWCCPd start
```

注意： Standard 0 サービスを使用する場合、Cisco 製デバイスは HTTP ポート 80 トラフィックのみを IWSVA デバイスにリダイレクトできます。動的サービスを使用する場合、Cisco 製デバイスはポート 80 に加えてその他のポートもリダイレクトできます。たとえば、動的サービスではポート 80、21、443、および 8080 をサポートできます。

高度な概念：冗長性およびフォールトトレランスのために WCCP を配置する

IWSVA を WCCP モードで配置する方法は数多くあります。拡張性や冗長性が求められる比較的大規模な環境では、負荷分散およびフォールトトレランス用に WCCP バージョン 2 の複数の Cisco 製ルータを使用して、複数の IWSVA を配置できます。

図 5 は、複数の IWSVA デバイスと複数の WCCP バージョン 2 対応ルータを使用した冗長アーキテクチャの例を示しています。

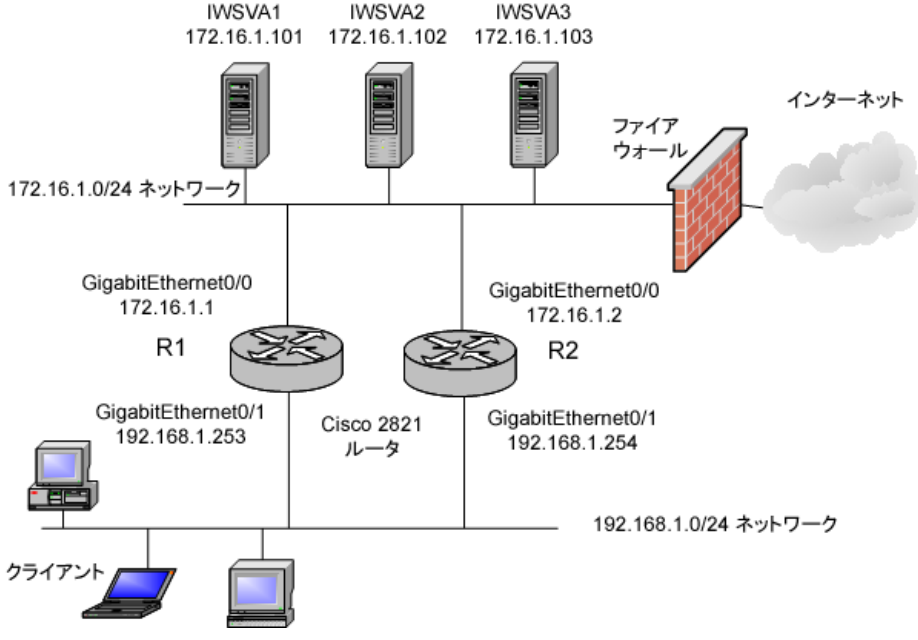


図 E-5.　高可用性設定で配置された IWSVA および Cisco 製ルータ

この例では、IOS 12.4 (13r) T を実行する 2 台の Cisco 2821 ルータを使用して、3 台の IWSVA デバイスにトラフィックをリダイレクトし、URL フィルタおよびコンテンツ検索を実行します。このお客さまは、3 台すべての IWSVA デバイス間で負荷分散を行い、いずれかの IWSVA がダウンした場合にはフォールトトレランスを行うことを望んでいます。この設計では、残った IWSVA デバイスを使用して追加の負荷を検出できるので、トラフィック処理が中断されません。Cisco 製ルータのいずれかがオフラインになっても、残りのルータが自動的に負荷を検出し、IWSVA デバイス間でのトラフィックの振り分けを続行します。

Cisco 製ルータを設定する

この設定の手順およびコマンドは、Cisco 2821 ルータの例と類似しています。以下に示すのは、参照用のルータ設定の完成例です。

Cisco 製ルータ 1

次の設定は、Cisco 製ルータ 1 での WCCP の設定および有効化の方法を示しています。この例では、転送方法は L2、割り当て方法はマスクを使用し、ルータの IOS は WCCP バージョン 2 をサポートするバージョンとなっています。

```
!
ip access-list standard wccp80
permit 192.168.1.0 0.0.0.255
!
ip access-list standard wccp-servers
 permit 172.16.1.101
 permit 172.16.1.102
 permit 172.16.1.103
!
ip wccp 80 redirect-list wccp80 group-list wccp-servers
!
interface GigabitEthernet0/1
ip wccp 80 redirect in
!
```

Cisco 製ルータ 2

次の設定は、Cisco 製ルータ 2 での WCCP の設定および有効化の方法を示しています。この例では、転送方法は L2、割り当て方法はマスクを使用し、ルータの IOS は WCCP バージョン 2 をサポートするバージョンとなっています。

```
!
ip access-list standard wccp80
permit 192.168.1.0 0.0.0.255
!
ip access-list standard wccp-servers
 permit 172.16.1.101
 permit 172.16.1.102
 permit 172.16.1.103
```

```
!
ip wccp 80 redirect-list wccp80 group-list wccp-servers
!
interface GigabitEthernet0/1
ip wccp 80 redirect in
!
```

IWSVA デバイスを設定する

この例では、3 台の IWSVA デバイスの設定が同じ WCCP 設定になっています。図 E-6 は、WCCP 設定の設定値を示しています。

図 E-6.　IWSVA の [WCCP 設定] 画面

この例では、2 台の Cisco 製ルータの IP アドレスが [ルータ IP アドレス] にカンマで区切って入力されています。転送方法は L2、割り当て方法はマスクが選択されています。

Cisco WCCP および IWSVA のトラブルシューティング

お使いの WCCP 環境で適切なトラブルシューティングを行うためには、IWSVA デバイスおよび Cisco 製デバイスで、WCCP イベント情報の冗長ログ（デバッグモード）を記録する必要があります。初期設定では、冗長ログは無効になっています。本書を使用しても解決できない問題に遭遇した場合は、トレンドマイクロのテクニカルサポートチームにお問い合わせください。テクニカルサポートチームでは、IWSVA デバイスおよび Cisco 製デバイスの冗長 / デバッグログを有効化して、トラブルシューティングに必要な情報を収集することをお願いする場合があります。

注意： IWSVA デバイスおよび Cisco 製デバイスをデバッグまたは冗長ログモードで実行すると、デバッグ目的で大量のデータを取得することが必要になる場合があるため、遅延が発生することがあります。こうした冗長ログモードは、トレンドマイクロのテクニカルサポート担当者の要請があったときのみ有効化してください。

IWSVA の WCCP イベントログを有効化する

IWSVA の WCCP ログ機能を有効化するには

1. IWSVA 管理コンソールに「root」ユーザでログインします。
2. 「`cd /var/iwss`」と入力して、「`/var/iwss`」ディレクトリに移動します。
3. vi などのエディタで「`IWSSPIProtocolHttProxy.pni`」ファイルを開きます。vi では、「`vi IWSSPIProtocolHttProxy.pni`」と入力します。
4. 「`/wccp_logging`」と入力して、ファイル内の「wccp_logging」パラメータを検索します。
5. 「`i`」と入力して、vi エディタを挿入モードにし、値を「0」から「1」に変更します。これにより、IWSVA の WCCP ログ機能が有効になります。

   ```
   wccp_logging=1
   #    0 ― オフ。WCCP ログなし。エラーのみ
   #    1 ― オン（初期設定)、WCCP ログを「http.log」ファイルに書き込みます。
   ```

6. <Esc> キーを押して挿入モードを終了し、「`:wq`」と入力して、ファイルに上書きして vi エディタを終了します。

   WCCP イベントは、IWSVA デバイスの「`/etc/iscan/log`」ディレクトリの HTTP ログファイルに保存されます。このログファイルは、`http.log.20110325.0001` のように、ファイル作成日時を示す形式で保存されます。

このディレクトリに移動し、vi などのエディタを使用して、このファイルを開いて表示することができます。

Cisco 製デバイスの WCCP イベントログを有効化する

お使いの Cisco 製デバイスによっては、WCCP イベントログを有効化する手順が、本書に示すものと異なる場合があります。ここでは、Cisco ASA ルータの例を示しています。お使いの Cisco 製ルータまたはスイッチの管理ガイドを参照してください。

Cisco 製デバイスで WCCP イベントログを有効化するには

1. Cisco 製デバイスのコンソールに、設定の権限を持つ管理アカウントを使用してログインします。
2. 「config」モードに入り、コマンドを入力して WCCP イベントデバッグ機能を有効化します。

```
Router (config) # debug wccp event
```

トラブルシューティングプロセスを開始する

WCCP が有効なデバイスで、検索するトラフィックが IWSVA デバイスに転送されない場合、まず確認することは、Cisco 製デバイスと IWSVA デバイス間の通信です。ここでは、キャッシュデバイスとして機能する IWSVA と Cisco 製デバイスとの間の通信のトラブルシューティングに使用するさまざまなコマンドについて説明します。

次のように、Cisco 製デバイスでは、Cisco 製デバイスの設定の確認に役立つコマンドがいくつか用意されています。

- `show ip wccp <サービス ID>`
- `show ip wccp <サービス ID> view`
- `debug ip wccp event`
- `debug ip wccp packet`

注意： このトラブルシューティング項に示すコマンドは、Cisco 製デバイスの種類によって多少異なる場合があります。この項に示すコマンドは、本書を通して使用されている Cisco 製ルーティングおよびスイッチングデバイスに対応するものです。Cisco ASA デバイスについては、コマンドが多少異なります。トラブルシューティングコマンドの詳細については、お使いの Cisco 製品の管理ガイドを参照してください。

IWSVA の設定を確認する

IWSVA デバイスで次の設定パラメータを確認して、IWSVA デバイスで通信が正常に実行されていることを確かめます。

IWSVA の設定を確認するには

1. IWSVA WCCP のパスワードパラメータに設定されたパスワードが、WCCP デバイスのパスワードと一致することを確認します。パスワードが同じでない場合、デバイス間で通信が行われません。
2. パスワードが一致する場合、IWSVA 検索デーモン (サービス) が正常に機能していることを確認します。
   a. IWSVA 管理コンソールに「root」ユーザでログインします。
   b. 「`lsof -iTCP -n -P`」コマンドを使用してデーモンのリストを表示し、`iwssd` デーモンおよび `isftpd` デーモンを探して、どちらも「LISTEN」モードになっていることを確認します。

```
-bash-3.2# lsof -iTCP -n -P
COMMAND     PID  USER   FD   TYPE DEVICE SIZE NODE NAME
sshd       3823  root    3u  IPv4   8554       TCP *:22 (LISTEN)
postmaste  4079 iscan    3u  IPv4  10299       TCP *:5432 (LISTEN)
java       4503 iscan   10u  IPv4  11379       TCP *:1812 (LISTEN)
java       4503 iscan   24u  IPv4  11426       TCP 127.0.0.1:8005 (LISTEN)
microdasy 22870   mds    6u  IPv4 389050       TCP *:8070 (LISTEN)
microdasy 22871   mds    4u  IPv4 388582       TCP *:8071 (LISTEN)
microdasy 22872   mds    6u  IPv4 389053       TCP *:8090 (LISTEN)
iwssd     22901 iscan    9u  IPv4 387267       TCP *:8080 (LISTEN)
iwssd     22901 iscan   10u  IPv4 387268       TCP *:443 (LISTEN)
iwssd     22901 iscan   11u  IPv4 387269       TCP *:8100 (LISTEN)
iwssd     22901 iscan   12u  IPv4 387270       TCP *:9090 (LISTEN)
java      22906 iscan    6u  IPv4 387474       TCP 127.0.0.1:5963 (LISTEN)
…
isftpd    23244 iscan    9u  IPv4 388281       TCP *:21 (LISTEN)
isftpd    23662 iscan    9u  IPv4 388281       TCP *:21 (LISTEN)
…
```

図 E-7.　iwssd および isftpd が表示されているデーモンリスト

3. IWSVA の WCCP 管理接続が正常に実行されていることを確認します。
   a. IWSVA 管理コンソールに「root」ユーザでログインします。
   b. 「/etc/iscan/wccp_status」ファイルでステータス値を確認します。ステータスが「2」に設定され、WCCP サーバデーモンが実行中の場合、管理接続は良好です。「cat」コマンドを使用すると、ファイルを開いて表示できます。

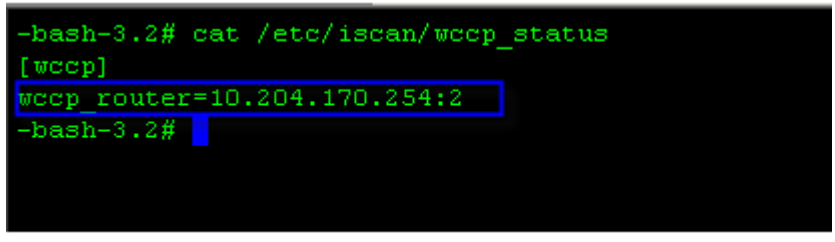


図 E-8.　WCCP 管理接続の確認

4. IWSVA と Cisco 製デバイスとの間の通信を確認します。
   a. IWSVA で、WCCP サーバデーモンのデバッグレベルのログを有効化します。
      i. 「/var/iwss」ディレクトリの「IWSSPIProtocolHttpProxy.pni」ファイルで「wccp_logging=1」と設定します。
      ii. 次のコマンドで、WCCP サーバデーモンを再起動します。

```
/usr/iwss/S99ISWCCPd stop
/usr/iwss/S99ISWCCPd start
```

   b. IWSVA の「/etc/iscan/log」ディレクトリの「http.log.current_date_time.nnnn」ファイルで、次のログエントリを確認します。「vi」などのエディタを使用してログファイルを開いて表示するか、「cat filename |more」コマンドを使用します。

```
… <6887> WCCP: Sending WCCPv2 HERE_I_AM for service ID 80
… <6887> WCCP: Received WCCPv2 I_SEE_YOU from 10.13.9.185
… <6887> WCCP: Good Received WCCPv2 I_SEE_YOU
```

   最初のログエントリに「Here I Am」メッセージが入っていない場合は、WCCP の透過モードが設定されていないか、WCCP サーバデーモンが実行されていません。
   2 番目のログエントリに「I See You」メッセージが入っていない場合は、ネットワークデバイスが応答していません。IWSVA とネットワークデバイスの設定または接続性を確認してください。

3 番目のログエントリに確認の「I See You」が入っていない場合は、ネットワークデバイスからのメッセージが解析できていません。これは、サポート対象外のネットワークデバイスを使用している場合に発生する可能性があります。

5. Cisco 製ルータまたはスイッチの管理接続を確認します。Cisco 製デバイスのコンソールに管理ユーザとしてログインし、次の診断手順を実行します。

   a. 「`show ip wccp <サービス ID> view`」コマンドを実行して、すべてのルータおよび IWSVA システムのリストを取得します。

   ```
   Router# show ip wccp 80 view
   WCCP Routers Informed of:
   10.13.10.17
   WCCP Cache Engines Visible:
   10.13.9.189
   WCCP Cache Engines NOT Visible:
   -none-
   ```

   「Cache Engines Visible」に「-none-」が含まれている場合、管理接続では通信が行われていません。

   b. 「`show ip wccp <サービス ID>`」コマンドを実行して、すべてのルータおよび IWSVA システムのリストを取得します。別のサービス値が選択されていないかぎり、初期設定のサービス ID は 80 にする必要があります。

   ```
   Router# show ip wccp 80
   Global WCCP information:
       Router information:
           Router Identifier:          10.13.10.17
           Protocol Version:           2.0
       Service Identifier: web-cache
           Number of Cache Engines:    1
           Number of routers:          1
           Total Packets Redirected:   0
           Redirect access-list:       -none-
           Total Packets Denied Redirect: 0
           Total Packets Unassigned:   0
           Group access-list:          -none-
           Total Messages Denied to Group:     0
           Total Authentication failures:      0
   ```

   ルータ識別子は、IWSVA が認識する Cisco 製ルータの IP アドレスです。このアドレスは、リダイレクトされたトラフィックがキャッシュに到達するために使用するルータインタ

フェースでなくても構いませんが、表示される IP アドレスは IWSVA から到達可能なものである必要があります。
「Total Packets Unassigned」の値は、IWSVA デバイスへの割り当てが不足したためにリダイレクトされなかったパケット数です。リダイレクションの失敗は、IWSVA デバイスの最初の検出時、またはメンテナンスやサービスの再起動による IWSVA のダウンなど、IWSVA が短時間使用できない場合に発生する可能性があります。

WCCP 登録アクティビティを確認する

Cisco 製デバイスで次の手順を実行して、WCCP 登録アクティビティを確認します。

WCCP 登録アクティビティを確認するには

1. 「`show ip wccp 80 view`」コマンドを実行して、ルータおよび IWSVA システムのリストを取得します。この例では、サービス ID は初期設定値の 80 のままとしています。
2. Cisco 製デバイスが IWSVA と「パートナーを組めない」場合、デバッグ機能を有効化して、Cisco 製デバイスの WCCP アクティビティを表示して確認する必要があります。WCCP イベントおよびパケットを有効化するデバッグコマンドは次のとおりです。

   ```
   debug ip wccp events
   debug ip wccp packets
   ```

   IWSVA デバイスおよび WCCP を使用する Cisco 製デバイスの設定後、以下に示す例のようにデバッグコマンドを有効化する必要があります。デバッグにより、2 台のデバイス間の WCCP 通信セッションが表示されます。
3. Cisco 製デバイスのコンソールに管理ユーザとしてログインし、次の手順を実行します。
   a. Router# `debug ip wccp event`

      WCCP イベントのデバッグはオンです。
   b. Router# debug ip wccp packet

      WCCP パケット情報のデバッグはオンです。
      Cisco 製デバイスにより、パケットデバッグの結果が次のように表示されます。

```
Router#
2d18h: WCCP-EVNT:S00: Built new router view: 0 routers, 0 usable web caches, change
 # 00000001
2d18h: %SYS-5-CONFIG_I: Configured from console by console
2d18h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2 w/ rcv_id 00000001
2d18h: WCCP-EVNT:S00: Redirect_Assignment packet from 192.168.15.2 fails source check
2d18h: %WCCP-5-SERVICEFOUND: Service web-cache acquired on Web Cache 192.168.15.2
2d18h: WCCP-PKT:S00: Received valid Here_I_Am packet from 192.168.15.2 w/rcv_id 00000001
```

```
2d18h: WCCP-EVNT:S00: Built new router view: 1 routers, 1 usable web caches, change
 # 00000002
2d18h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2 w/ rcv_id 00000002
2d18h: WCCP-EVNT:S00: Built new router view: 1 routers, 1 usable web caches, change
 # 00000002
2d18h: WCCP-PKT:S00: Received valid Redirect_Assignment packet from 192.168.15.2 w/rcv_id
 00000002
2d18h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2 w/ rcv_id 00000003
2d18h: WCCP-EVNT:S00: Built new router view: 1 routers, 1 usable web caches, change
 # 00000002
2d18h: WCCP-PKT:S00: Received valid Redirect_Assignment packet from 192.168.15.2 w/rcv_id
 00000003
2d18h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2 w/ rcv_id 00000004
2d18h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2 w/ rcv_id 00000005
2d18h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2 w/ rcv_id 00000006
2d18h: WCCP-EVNT:S00: Built new router view: 1 routers, 1 usable web caches, change
 # 00000002
2d18h: WCCP-PKT:S00: Received valid Redirect_Assignment packet from 192.168.15.2 w/rcv_id
 00000006
```

パケットデバッグで着目すべき点

Cisco 製デバイスがキャッシュ (IWSVA) から「Here I Am」パケットを受信するたびに、その Cisco 製デバイスは「I See You」パケットを返しています。IWSVA が Cisco 製デバイスと正常に通信している場合は、前述の例に示すような応答内容となるはずです。

本番環境では、無関係なメッセージが多数あって、デバッグの解読が困難になる場合があります。トラブルシューティングを早めるためにデバッグトラフィックをフィルタし、適切な IP アドレスを見つけやすくするため、ACL を使用して、デバッグの取得を IWSVA の IP アドレスが送信元アドレスとなるパケットのみに制限します。

以下の例では、ACL を使用して IWSVA の IP アドレスに的を絞る方法を示します。

1. 次に示す 2 つのコマンドを実行して、IWSVA の IP アドレスの ACL を設定し、デバッグ処理を有効化します。

   ```
   Router(config)# access-list 130 permit ip host 192.168.15.2  host
   192.168.15.1
   ```

   ```
   Router# debug ip packet 130
   ```

   次の例は、IWSVA の IP アドレスを使用してフィルタされたデバッグパケットのトレースを示しています。

```
IP packet debugging is on for access list 130
```

```
2d19h: WCCP-EVNT:S00: Built new router view: 1 routers, 1 usable web caches, change
 # 00000002
2d19h: WCCP-PKT:S00: Received valid Redirect_Assignment packet from 192.168.15.2
 w/rcv_id 0000001B
2d19h: datagramsize=174, IP 18390: s=192.168.15.2 (Vlan300), d=192.168.15.1 (Vlan300),
 totlen 160, fragment 0, fo 0, rcvd 3
2d19h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2 w/ rcv_id 0000001C
2d19h: datagramsize=174, IP 18392: s=192.168.15.2 (Vlan300), d=192.168.15.1 (Vlan300),
 totlen 160, fragment 0, fo 0, rcvd 3
2d19h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2 w/ rcv_id 0000001D
2d19h: datagramsize=174, IP 18394: s=192.168.15.2 (Vlan300), d=192.168.15.1 (Vlan300),
 totlen 160, fragment 0, fo 0, rcvd 3
2d19h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2 w/ rcv_id 0000001E
2d19h: datagramsize=378, IP 18398: s=192.168.15.2 (Vlan300), d=192.168.15.1 (Vlan300),
 totlen 364, fragment 0, fo 0, rcvd 3
2d19h: WCCP-EVNT:S00: Built new router view: 1 routers, 1 usable web caches, change
 # 00000002
2d19h: WCCP-PKT:S00: Received valid Redirect_Assignment packet from 192.168.15.2
 w/rcv_id 0000001E
2d19h: datagramsize=174, IP 18402: s=192.168.15.2 (Vlan300), d=192.168.15.1 (Vlan300),
 totlen 160, fragment 0, fo 0, rcvd 3
2d19h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2 w/ rcv_id 0000001F
2d19h: datagramsize=174, IP 18404: s=192.168.15.2 (Vlan300), d=192.168.15.1 (Vlan300),
 totlen 160, fragment 0, fo 0, rcvd 3
2d19h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2 w/ rcv_id 00000020
2d19h: datagramsize=174, IP 18406: s=192.168.15.2 (Vlan300), d=192.168.15.1 (Vlan300),
 totlen 160, fragment 0, fo 0, rcvd 3
2d19h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2 w/ rcv_id 00000021
2d19h: datagramsize=378, IP 18410: s=192.168.15.2 (Vlan300), d=192.168.15.1 (Vlan300),
 totlen 364, fragment 0, fo 0, rcvd 3
2d19h: WCCP-EVNT:S00: Built new router view: 1 routers, 1 usable web caches, change
 # 00000002
2d19h: WCCP-PKT:S00: Received valid Redirect_Assignment packet from 192.168.15.2
 w/rcv_id 00000021
2d19h: datagramsize=174, IP 18414: s=192.168.15.2 (Vlan300), d=192.168.15.1 (Vlan300),
 totlen 160, fragment 0, fo 0, rcvd 3
2d19h: WCCP-PKT:S00: Sending I_See_You packet to 192.168.15.2 w/ rcv_id 00000022
2d19h: datagramsize=174, IP 18416: s=192.168.15.2 (Vlan300), d=192.168.15.1 (Vlan300),
 totlen 160, fragment 0, fo 0, rcvd 3
```

パケットデバッグで着目すべき点

IWSVA または WCCP のアクティビティをルータから認識できない場合、2 台のデバイス間の基本的な接続性を確認します。ルータから IWSVA へ、または IWSVA デバイスからルータへ ping してみます。ping が通る場合、ルータの設定が正しいことを確認します。

キャッシュの取得が行われているが、パケットのリダイレクションがない場合、トラフィックが実際にルータに到達していることを確認します。また、トラフィックが正しい Cisco 製デバイスインタフェースに転送されていることも確認します。これは、前述の例のトラフィックリダイレクションの手順で設定されています。インターセプトおよびリダイレクトされたトラフィックは、TCP ポート 80 に送られることに注意してください。

キャッシュの取得が発生し、パケットのリダイレクションを認識できるが、クライアントがインターネットを閲覧できない場合は、IWSVA デバイスのインターネットおよびクライアントへの接続性を確認します。IWSVA のコンソール管理画面で、インターネット上のいくつかの IP アドレスや、内部ネットワークのいくつかのクライアントに ping を実行してみます。

パケットのリダイレクションを確認する

Cisco 製デバイスで次の手順を実行して、パケットリダイレクションのアクティビティを検証し、パケットが正常に転送されていることを確認します。

パケットリダイレクションアクティビティを確認するには

1. Cisco 製デバイスの管理コンソールに管理ユーザとしてログインします。
2. 「`show ip wccp 80 detail`」コマンドを実行して、リダイレクションの統計を Cisco 製デバイスから取得します。この例では、サービス ID は初期設定の 80 に設定されています。

```
Router# show ip wccp 80 detail
WCCP Cache-Engine information:
Web Cache ID: 10.13.9.189
Protocol Version: 2.0
State: Usable
Redirection:        GRE
Initial Hash Info: 00000000000000000000000000000000
00000000000000000000000000000000
Assigned Hash Info: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
Hash Allotment: 256 (100.00%)
Packets Redirected: 736
Connect Time: 00:07:45
```

「Redirection」パラメータは、Cisco 製デバイスとキャッシュ（IWSVA）との間で使用されるパケットリダイレクションプロトコルを示しています。リダイレクションプロトコルは、Generic Routing Encapsulation（GRE）またはレイヤ 2（L2）に設定できます。GRE は通信をトンネル化し、ポイントツーポイント接続を作成して、IP ネットワークを介してデバイス間で通信できるようにします。一

方、L2 リダイレクションは、パケットを最初にカプセル化せず、直接キャッシュ (IWSVA) に送信します。ただしこれには、Cisco 製デバイスおよび IWSVA が同じレイヤ 2 ネットワーク上にある必要があります。

「Hash Allotment」は、IWSVA に割り当てられているハッシュバケットの数です。16 進数の値は、「Hash Allotment」と、「Initial Hash Info」および「Assigned Hash Info」の値を示しています。ハッシュアルゴリズムを使用すると、割り当てられたバケット数以内で、到達先となる可能性があるインターネットアドレスすべてを収集し、分類できます。定義されたサービスグループの各 IWSVA デバイスは、あらかじめ設定されたバケットの割合を受信します。WCCP は、負荷およびその他のあらかじめ設定された条件に従って、これらのリソースを動的に管理します。定義されたキャッシュデバイスが IWSVA のみの場合、WCCP はすべてのバケットリソースを IWSVA に割り当てます。

Cisco 製デバイスがキャッシュエンジン (IWSVA) へのパケットのリダイレクションを開始すると、「Packets Redirected」の値が上昇するのがわかるはずです。

IWSVA でのパケットフローを確認する

転送方法が GRE に設定され、パケットが Cisco 製デバイスからリダイレクトされるが、IWSVA 検索デーモンに受信されない場合 (「`/etc/iscan/log`」ディレクトリの「http.log」ファイルに基づいて) は、次の IWSVA 設定を確認します。

注意： 転送方法が L2 の配信では、手順 2 に進み、手順 3 へと続けてください。

IWSVA でのパケットフローを確認するには

1. IWSVA コンソールに「root」ユーザでログインします。
2. 転送方法が GRE の配信では、「`ifconfig`」コマンドを使用して、「gre1」デバイスが正常に動作していることを確認します。

- bash - 3.2# ifconfig

```
/ # ifconfig
…
gre1      Link encap:UNSPEC  HWaddr 0A-0D-09-BD-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.13.9.189  P-t-P:10.13.9.189  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP  MTU:1476  Metric:1
          RX packets:50 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:5110 (4.9 KiB)  TX bytes:0 (0.0 b)
…
/ #
```

図 E-9. 「ifconfig」コマンドを使用して、「gre1」デバイスが正常に動作していることを確認

3. 「iptunnel」コマンドを使用して、ルータから IWSVA への IP トンネルが設定されていることを確認します。

   -bash-3.2# iptunnel

```
-bash-3.2# iptunnel
gre0: gre/ip  remote any  local any  ttl inherit  nopmtudisc
gre1: gre/ip  remote 10.204.170.254  local 10.204.170.97  dev eth0  ttl inherit
-bash-3.2#
```

図 E-10. 「iptunnel」コマンドを使用して、IP トンネルが設定されていることを確認

4. 「iptables」コマンドを使用して、IWSVA ファイアウォールがパケットを検索デーモンにリダイレクトしていることを確認します。

```
-bash-3.2# iptables -t nat  -vL
```

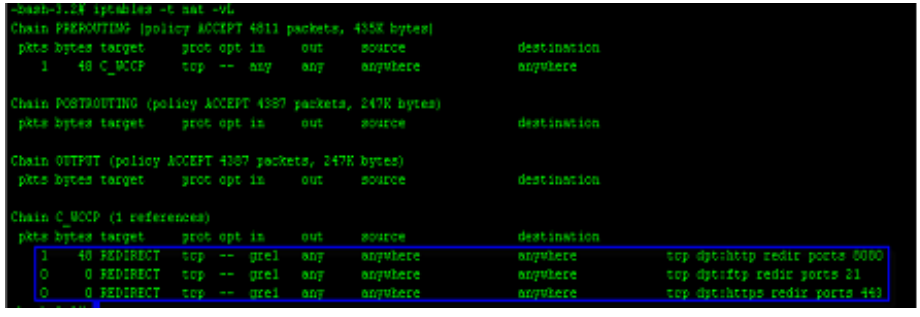


図 E-11. 「iptables」コマンドを使用して、IWSVA ファイアウォールがパケットをリダイレクトしていることを確認

5. (オプション)「高度な」トラブルシューティング手順として、「tcpdump」コマンドを使用して IWSVA ファイアウォールからのパケットを取り込むことができます。これにより、IWSVA でパケットを正常に処理していることが確認できます。

   a. パケット取り込みコマンド「tcpdump」で取り込むデータの量を制限するには、ACL を使用して Cisco 製ルータを設定し、WCCP のリダイレクションを 1 つのクライアントに制限します。これにより、範囲を狭めて、1 つのクライアントに集中できます。

      次の例では、WCCP のリダイレクションを 1 つのクライアント (10.10.10.152) に制限し、WCCP のリダイレクション処理を開始する方法を示しています。

      ```
      Router(config)# access-list 50 permit 10.10.10.152
      Router(config)# ip wccp web-cache redirect-list 50
      ```

   b. 「tcpdump」コマンドを使用して、IWSVA でのパケットの取り込みを有効化します。これは IWSVA の管理コンソールから実行し、「root」ユーザでコンソールにアクセスする必要があります。

      ```
      -bash-3.2# tcpdump -s0 -w wccp.cap
      ```

   c. 十分な量のパケットを取り込んだら、パケットの取り込みを停止し、「wccp.cap」ファイルをローカルホストにコピーします。

   d. Wireshark などのパケット解析ツールを使用して「wccp.cap」ファイルを開き、パケットの取り込みを分析します。

   e. パケットの取り込みを分析して、Cisco 製デバイスと IWSVA デバイスとの間の通信が正常に行われていることを確認します。

注意： 「tcpdump」パケット取り込みユーティリティを使用するのは高度な概念であり、Cisco 製デバイスと IWSVA デバイスの間の通信を解読するのは容易ではない可能性があります。ここまでの手順のトラブルシューティングを実行しても WCCP の問題を解決できない場合は、トレンドマイクロのカスタマーセンターにお問い合わせください。

付録 F

URL フィルタカテゴリのグループ

URL カテゴリは、表 F-1 に示される URL フィルタグループに分類されます。

表 F-1.　URL カテゴリのグループ定義

カテゴリのグループ	説明
アダルト	子どもが閲覧するのに不適切だと広く一般に思われている Web サイトです。
ビジネス	ビジネス、雇用、または経済に関する Web サイトです。
コミュニケーション / メディア	オンライン上のコミュニケーションや検索に関するツール / サービスを提供する Web サイトです。
一般	他のカテゴリに属さない Web サイトです。
インターネットのセキュリティ	不正プログラムをダウンロードする可能性などがある、潜在的に危険な Web サイトです。
ライフスタイル	日常生活に関する情報を提供する Web サイトです。
ネットワーク	お使いのネットワークの帯域幅に大きな影響を与える可能性のあるサービスを提供する Web サイトです。
カスタムカテゴリ	カスタマイズした特定のカテゴリに対して管理者が定義した Web サイトです。

注意： URL フィルタが適切に動作するには、IWSVA はトレンドマイクロサービスに HTTP 要求を送信できる必要があります。HTTP プロキシが必要な場合は、[管理] → [配置ウィザード] の順に選択してプロキシを設定します。

URL フィルタのカテゴリ

表 F-2 は、URL フィルタのカテゴリの定義と、割り当てられるグループを示しています。

表 F-2.　URL フィルタカテゴリの定義

カテゴリのグループ	カテゴリのタイプ	カテゴリの定義
アダルト	アダルト / 成人向け	子どもが閲覧するのに不適切だと広く一般に思われている、性的に露骨なコンテンツを表示する成人向けコンテンツのある Web サイトです。
アダルト	ポルノ	性的に露骨なコンテンツを表示する成人向けコンテンツのある Web サイトです。
アダルト	性教育	性教育 (セーフセックス、避妊法)、人工中絶、性に関する Web サイトです。
アダルト	下着 / 水着	水着、下着などのイメージを扱った Web サイトです。販売商品の 1 つとして水着や下着が扱われている Web サイトは含まれません。
アダルト	ヌード	人体の裸体描写や半裸描写を扱った Web サイトです (ヌーディストサイトも含まれます)。
アダルト	酒 / タバコ	アルコールやタバコの製造、販売促進に関する Web サイトです。飲酒や喫煙を勧める Web サイトも含まれます。販売商品の 1 つとしてアルコールやタバコが扱われている Web サイトは含まれません。

表 F-2.　URL フィルタカテゴリの定義 (続き)

カテゴリのグループ	カテゴリのタイプ	カテゴリの定義
アダルト	違法と思われる行為	違法行為 (強盗、窃盗、法の適用の回避、詐欺、盗作など) に関連すると思われる Web サイトです。違法行為を擁護する Web サイト、アドバイスする Web サイト、レポートを販売する Web サイトが含まれます。
アダルト	低俗	一般的に不適切と思われる表現や画像などを含む Web サイトです。
アダルト	ギャンブル	ギャンブルに関する情報を提供する Web サイトです。ギャンブルを勧める Web サイト、オンラインカジノの Web サイトも含まれます。ギャンブル関連の製品や機械を販売する Web サイトは含まれません。
アダルト	暴力 / 差別	暴力や差別に関する記述や描写がある Web サイトです。暴力や差別を助長する Web サイト、援護する Web サイトも含まれます。
アダルト	武器	武器、兵器などに関する Web サイトです。軍事関連組織や、ハンティング、射撃に関する Web サイトは含まれません。
アダルト	妊娠中絶	人工中絶 (手順の説明、サポート、影響など) に関する Web サイトです。
コミュニケーション / メディア	ダイナミック DNS	ダイナミック DNS サービスを利用して、ドメイン名を動的 IP アドレスに割り当てている Web サイトです。
ライフスタイル	レジャー / 趣味	ガーデニング、アウトドア、コレクション、ゲーム (テレビゲームを除く)、手工芸などのレジャーや趣味に関する Web サイトです。ペットやレジャー関連施設 / 団体の Web サイトも含まれます。
ライフスタイル	アート	絵画、彫刻などの視覚芸術に関する Web サイトです。

表 F-2. URL フィルタカテゴリの定義 (続き)

カテゴリのグループ	カテゴリのタイプ	カテゴリの定義
ライフスタイル	エンターテインメント	映画、音楽、ラジオ番組やテレビ番組 (ニュースを除く)、書籍や雑誌などに関する情報を提供する Web サイトです。
ビジネス	ビジネス / 経済	起業、マーケティングなどのビジネスや経済に関する Web サイトです。他のカテゴリに当てはまらない企業 Web サイトも含まれます。
ライフスタイル	特定の宗教 / オカルト	特定の宗教や信仰に関する表記、信念、科学的に証明できない呪文、魔術、超常現象に関する情報を提供する Web サイトです。
ネットワーク	インターネットラジオ / テレビ	ストリーミングラジオやテレビを主に配信する Web サイトです。
コミュニケーション / メディア	インターネット電話	インターネット電話に関する Web サイトです。
アダルト	違法と思われる薬物	違法と思われる薬物の宣伝、販売および、処方薬などの不適切な使用や方法に関する Web サイトです。
アダルト	マリファナ	マリファナの栽培、使用、調合方法に関する Web サイトです。関連器材に関する Web サイトも含まれます。
一般	教育	学校、通信教育などの教育に関する Web サイトです。
インターネットのセキュリティ	安全でない IoT 機器の接続	IoT デバイスにダメージを与えたり、感染させたり、または悪用したりする潜在的な可能性のある、安全でないインターネット接続です。
ライフスタイル	文化団体	図書館、美術館、博物館などの文化遺産保護を目的とした団体が運営する Web サイトです。ボーイスカウト、ガールスカウト、国際ロータリークラブなどの組織が管理する Web サイトも含まれます。

表 F-2.　URL フィルタカテゴリの定義 (続き)

カテゴリのグループ	カテゴリのタイプ	カテゴリの定義
ライフスタイル	一般団体	公共政策、世論、社会的慣習、経済活動などに関する意見を提言する Web サイトです。サービス団体、慈善団体、専門家集団、労働団体が運営する Web サイトも含まれます。
ビジネス	金融サービス	金融サービス全般の情報やサービスを提供する Web サイトです。金融業界の企業が運営する Web サイトも含まれます。
ビジネス	貿易 / 仲介	株式や債券への投資に関する Web サイトです。オンライントレードや自動車保険に関する Web サイトも含まれます。
ライフスタイル	ゲーム	テレビゲーム、コンピュータゲーム、ボードゲームの Web サイトです。賞金や賞品をプレゼントする Web サイト、競技やダウンロードに関する Web サイトは含まれません。
一般	政府 / 法律	法律や政治など、政府に関する Web サイトです。軍隊、医療に関する Web サイトは含まれません。
一般	軍隊	軍隊に関する Web サイトです。武器や軍装備品の情報提供や販売を行う Web サイトは含まれません。
一般	政治	政党、政党後援組織、その他政治的団体に関する Web サイトです。政治に関連する話題の Web サイトも含まれます。政治に関連のない団体 / 集団による Web サイトは含まれません。
一般	健康	健康、フィットネス、美容 / 健康促進に関する Web サイトです
一般	コンピュータ / インターネット	コンピュータ、インターネット、その他の関連技術に関する Web サイトです。電子機器の販売や評価を行う Web サイトも含まれます。

表 F-2. URL フィルタカテゴリの定義 (続き)

カテゴリのグループ	カテゴリのタイプ	カテゴリの定義
コミュニケーション / メディア	プロキシ回避システム / 匿名化ソフトウェア	プロキシサーバや Web フィルタリングシステムの回避に使用される可能性がある、またはインターネットを匿名や追跡されない状態で使用することを可能にする Web サイトです。これらを目的としたツールを提供する Web サイトも含まれます。
コミュニケーション / メディア	検索エンジン / ポータル	Web 上の情報検索システムを提供する検索エンジンサイトやポータルです。
コミュニケーション / メディア	インターネット インフラストラクチャ	データやデータ分析の収集、処理、提示に使用されるコンテンツサーバ、イメージサーバ、または Web サイトです。Web の分析ツールやネットワーク監視を行う Web サイトも含まれます。
コミュニケーション / メディア	ブログ / 掲示板 / コミュニケーション	ブログ、掲示板など、Web ベースのコミュニケーションを行う Web サイトです。
ネットワーク	画像検索	画像を検索する Web サイトです。
ライフスタイル	その他出版物	タブロイド誌や時事の話題などに関する出版物の Web サイトです。
ビジネス	就職 / 転職	就職や雇用サービスに関する Web サイトです。
一般	ニュース / メディア	ニュース、時事問題、天気に関する Web サイトです。他のカテゴリに当てはまらないオンラインマガジンも含まれます。
ライフスタイル	出会い	恋愛、デート、交際などの目的で人と出会うための Web サイトです。
一般	翻訳 / キャッシュページ	オンライン翻訳や検索エンジンにおけるキャッシュされた Web ページです。プロキシサーバや Web フィルタリングシステムの回避に使用される可能性があります。

表 F-2.　URL フィルタカテゴリの定義 (続き)

カテゴリのグループ	カテゴリのタイプ	カテゴリの定義
一般	レファレンス / 参照情報	地図、百科事典、辞書、天気、実用書、数値の換算など、一般的または専門的な情報を照会するための Web サイトです。
コミュニケーション / メディア	ソーシャルネットワーキング	人と人とのつながりを促進 / サポートする、コミュニティ型の Web サイトです。
コミュニケーション / メディア	チャット / メッセンジャー	チャットやインスタントメッセンジャーの Web サイトです。インスタントメッセンジャーのソフトウェアを提供する Web サイトも含まれます。
コミュニケーション / メディア	メール	Web メール、グリーティングカード、メーリングリストなど、Web ベースのメールサービスの Web サイトです。
コミュニケーション / メディア	ニュースグループ / フォーラム	ニュースグループ、フォーラム、または BBS に関する Web サイトです。
ライフスタイル	宗教	一般的な宗教、信仰、宗教建築物に関する Web サイトです。
ライフスタイル	個人 Web サイト	個人が開設した趣味などに関する Web サイトです。ソーシャルネットワーキング、ブログサイトなどのサービスに登録されている個人ページは含まれません。
ネットワーク	ファイル共有サービス	ファイルやデータを共有できる Web サイトです。
ネットワーク	ピアツーピア	ピアツーピア (P2P) ネットワーク内でファイルを共有 / 転送するための情報やソフトウェアを提供する Web サイトです。
ビジネス	ショッピング	ショッピング関係の Web サイトです。
ビジネス	オークション	オークション関係の Web サイトです。
ビジネス	不動産	不動産に関する Web サイトです。物件の販売、購入、賃貸に関するサービスを提供する Web サイトも含まれます。

表 F-2. URL フィルタカテゴリの定義 (続き)

カテゴリのグループ	カテゴリのタイプ	カテゴリの定義
ライフスタイル	生活 / ライフスタイル	日常生活に関する情報を提供する Web サイトです。化粧品やファッションに関する Web サイトも含まれます。エンターテインメント、趣味、性、スポーツに関する Web サイトは含まれません。
ライフスタイル	ガンクラブ / ハンティング	ガンクラブなどの団体に関する Web サイトです。ハンティング、射撃、サバイバルゲーム、ペイントボールの施設に関する Web サイトも含まれます。
ライフスタイル	レストラン / フード	食品、ケータリング、ダイニングサービス、料理、レシピに関する宣伝、説明、評価などを行う Web サイトです。
ライフスタイル	スポーツ	スポーツや各種競技に関する Web サイトです。ファンサイト、スポーツ用品を販売する Web サイトも含まれます。
ライフスタイル	旅行	旅行や観光地に関する Web サイトです。旅行の予約や計画を行う Web サイトも含まれます。
一般	乗り物	乗り物に関する Web サイトです。車両本体や部品のカスタマイズ、購入、修理サービスなども含まれます。軍用車両に関する Web サイトは含まれません。
ライフスタイル	ユーモア	ユーモアに関する Web サイトです。
ネットワーク	ストリーミングメディア /MP3	ラジオ番組やテレビ番組以外のストリーミング映像や音声を提供する Web サイトです。MP3、AVI ファイル形式などの音楽や動画のダウンロードを行う Web サイトも含まれます。
ネットワーク	着信メロディ / 携帯電話向け ダウンロードサービス	携帯電話向けに着信メロディ、ゲーム、動画などを配信する Web サイトです。

表 F-2.　URL フィルタカテゴリの定義 (続き)

カテゴリのグループ	カテゴリのタイプ	カテゴリの定義
ネットワーク	ソフトウェア ダウンロード	ソフトウェアのダウンロードに関する Web サイトです。
ネットワーク	懸賞 / サイドビジネス	Web サイト、メール、オンライン広告などの閲覧、リンクのクリック、アンケートの回答などに対して報酬を得る Web サイトです。
インターネットのセキュリティ	不正と思われるプログラム (グレーウェア)	コンピュータに害を与える可能性のある Web サイトです。
インターネットのセキュリティ	スパイウェア	ユーザに無断でデータを収集し転送するソフトウェアをダウンロードする可能性がある Web サイトです。
インターネットのセキュリティ	スパム	スパムメールを配信している疑いのある Web サイトです。
インターネットのセキュリティ	アドウェア	広告などの宣伝用コンテンツを表示するソフトウェアをダウンロードする可能性のある Web サイトです。ブラウザヘルパーオブジェクト (BHO) をインストールする Web サイトも含まれます。
インターネットのセキュリティ	不正プログラムによる外部アクセス	不正プログラムによって利用される、不正プログラムのアップデートや盗み取った情報の格納に使用される Web サイトです。
インターネットのセキュリティ	不正プログラム配信	有害なプログラムやソースコードの配布を直接的または間接的に促す Web サイトです。
コミュニケーション / メディア	コインマイナー	スクリプトまたは実行ファイルで、コインマイニングなどの仮想通貨に関する処理を実行します。
インターネットのセキュリティ	MFA (MadeforAdSense) サイト	独自のコンテンツを持たずに、GoogleAdSense 広告を表示するために開設された Web サイトです。

表 F-2.　URL フィルタカテゴリの定義 (続き)

カテゴリのグループ	カテゴリのタイプ	カテゴリの定義
ライフスタイル	子ども向け	子どもを対象として提供されている Web サイトです。
インターネットのセキュリティ	Web 広告	広告の表示を主に行う Web サイトです。バナー広告、ポップアップ広告の表示に使用される Web サイトも含まれます。
コミュニケーション / メディア	Web ホスティング	トップレベルドメインや Web ホスティングサービスを提供する組織の Web サイトです。
一般	未評価	カテゴリが未分類の Web サイトです。
インターネットのセキュリティ	新たに確認されたドメイン	最近アクティブになった、もしくは新たに確認されたドメインで、トレンドマイクロによる分類がまだ行われていないドメインです。使い捨てドメインなど、以前からドメイン登録されていたものも含みます。
インターネットのセキュリティ	詐欺サイト	個人または団体から信用を得た上で金銭などをだまし取ろうとする Web サイトです。多くの場合、人間誰もが持つような欲望や同情などにつけ込む巧みな手口が使われます。
インターネットのセキュリティ	ランサムウェア	ランサムウェア（身代金要求型不正プログラム) を広めるため、直接的または間接的に利用される Web サイトです。
一般	その他	他のカテゴリに分類できない評価済みの Web サイトです。

用語集

この用語集では、本書またはオンラインヘルプで使用される用語を説明しています。

用語	説明
ActiveX (アクティブ エックス)	OLE (Object Linking and Embedding) を実装するオープンソフトウェアアーキテクチャのタイプ。Web ページのダウンロードなどの一部の標準インタフェースを有効にします。
ActiveX 不正コード	ActiveX コントロールは Web ページに埋め込まれたコンポーネントオブジェクトで、ページが表示されると自動的に実行されます。ActiveX コントロールを使用することにより、Web 開発者は、たとえばトレンドマイクロの無料オンライン検索であるウイルスバスターオンラインスキャンなど、幅広い機能を使用して、インタラクティブで動的な Web ページを作成できます。 ハッカー、ウイルス作成者、および悪質ないたずらを目的とするその他の人間は、システムを攻撃するための媒体として ActiveX 不正コードを使用することがあります。多くの場合、Web ブラウザのセキュリティ設定を「高」に変更することで、こうした ActiveX コントロールを実行しないように設定できます。
Audio/Video ファイル	音楽などの音声やビデオ映像を含むファイルです。
cookie	インターネットユーザについての情報、たとえば名前、好み、興味などを保持するメカニズムで、後で使用するために Web ブラウザに保存されます。次回、ブラウザが cookie を保存している Web サイトにアクセスすると、ブラウザは Web サーバに cookie を送信します。Web サーバはその cookie を使用して、カスタマイズされた Web ページを表示できます。たとえば、名前を表示して開始する Web サイトなどです。

用語	説明
DNS	ドメインネームシステム (Domain Name System) ― ホスト名を IP アドレスに変換するために主にインターネット上で使用されている汎用的なデータクエリサービスです。
DNS 名前解決	DNS クライアントが DNS サーバにホスト名とアドレスデータを要求するときのプロセス。基本的な DNS 設定では、サーバが初期設定された名前解決プロセスを実行します。たとえば、リモートサーバは、現在のゾーンにあるコンピュータ上のデータについて別のサーバに問い合わせます。リモートサーバ上のクライアントソフトウェアはリゾルバに問い合わせます。リゾルバは、データベースファイルからの要求に応答します。
DOS ウイルス	「COM」および「EXE」ファイル感染型ウイルスとも呼ばれます。DOS ウイルスは、拡張子 *.COM または *.EXE が付く、DOS の実行可能プログラムファイルに感染します。元のプログラムのコードの一部を上書きしたり不注意により破壊するほか、ほとんどの DOS ウイルスは、他のホストプログラムに感染することで増殖および伝染を図ります。
ELF	Executable and Linkable Format の略。UNIX および Linux プラットフォーム用の実行可能ファイル形式です。
Ethernet	Xerox Corporation と Palo Alto Research Center が考案したローカルエリアネットワーク (LAN) 技術です。Ethernet は、ベストエフォート型通信システムで、CSMA/CD 技術を使用しています。Ethernet は、太い同軸ケーブル、細い同軸ケーブル、ツイストペアケーブル、および光ファイバーケーブルなど、さまざまなケーブルスキームで使用できます。Ethernet は、コンピュータをローカルエリアネットワークに接続するための規格です。
EXE ファイル感染型ウイルス	ファイル拡張子が .exe の実行可能プログラムです。「DOS ウイルス」も参照してください。
FAQ	Frequently Asked Questions の略。特定のトピックに関する質問とその回答のリストです。

用語	説明
FTP	あるコンピュータのユーザが別のコンピュータとの間で TCP/IP ネットワークを介してファイルを双方向に転送できるクライアント / サーバのプロトコル。また、ユーザがファイルを転送するために実行するクライアントプログラムのことも表します。
GUI	グラフィカルユーザインタフェース (Graphical User Interface) — プログラムの入出力を表すために言葉のみではなく絵を使用すること。これは、やり取りをテキストの文字列で行うコマンドラインインタフェースと対比されます。
HTTP	ハイパーテキスト転送プロトコル (Hypertext Transfer Protocol) — HTML 文書の交換のために WWW (World Wide Web) 上で使用されるクライアント / サーバの TCP/IP プロトコル。通常はポート 80 を使用します。
HTTPS	ハイパーテキスト転送プロトコルセキュリティ (Hypertext Transfer Protocol Secure) — セキュリティで保護されたトランザクションの処理に使用される HTTP の強化版。
ICSA	ICSA Labs は、TruSecure Corporation の独立した部門です。10 年以上にわたり、製品テストの調査、情報収集、および認定に関する、セキュリティ業界の中心的な権威として存在しています。ICSA Labs は情報セキュリティ製品の基準を設定し、現在、インストールベースで世界の 90% 以上のウイルス対策、ファイアウォール、IPSec、暗号技術、およびコンピュータファイアウォール製品を認定しています。
IP	Internet Protocol の略。「IP アドレス」を参照してください。
IP アドレス	ネットワーク上のデバイス用のインターネットアドレスです。通常、123.123.123.123 のようにピリオドで区切る IPv4 アドレスの表記方法や、コロンで区切る IPv6 アドレスの表記方法で表されます。
IP ゲートウェイ	ゲートウェイは、最終的な送信先に到達するまで、あるネットワークから別のネットワークへと IP データグラムを転送するプログラム、または特殊な目的のデバイスです。
IT	情報技術のことで、ハードウェア、ソフトウェア、ネットワーク、電気通信、およびユーザサポートを含みます。

用語	説明
JavaScript ウイルス	JavaScript は、Netscape が開発した簡単なプログラミング言語です。これを使用することにより、Web 開発者は、ブラウザに表示される HTML ページに、スクリプトを使用して動的なコンテンツを追加できます。Javascript は、Sun Microsystems の Java プログラミング言語の一部の機能を共有していますが、独立して開発されました。 JavaScript ウイルスは、HTML コードのこれらの JavaScript を標的にするウイルスです。これにより Web ページにウイルスを潜ませ、ユーザのブラウザを使用してウイルスをユーザのデスクトップにダウンロードできます。 「VBscript ウイルス」も参照してください。
Java アプレット	HTML ページに埋め込まれた小さくポータブルな Java プログラムで、ページが表示されるときに自動的に実行できます。Java アプレットを使用することで、Web 開発者は、幅広い機能を使用して、インタラクティブで動的な Web ページを作成できます。 Java アプレットは、不正コードの作成者たちによる攻撃媒体として使用されてきました。しかし多くの場合、Web ブラウザのセキュリティ設定を「高」に変更することなどにより、簡単に、こうしたアプレットを実行しないように設定できます。
Java ファイル	Java は、Sun Microsystems が開発した汎用プログラミング言語です。Java ファイルには、Java コードが含まれます。Java は、プラットフォームに依存しない Java「アプレット」の形式で、インターネット用のプログラミングをサポートしています（アプレットとは、HTML ページに含めることができる、Java プログラミング言語で記述されたプログラムです。Java 技術が有効になっているブラウザを使用して、アプレットを含むページを表示すると、そのアプレットのコードがシステムに転送され、ブラウザの Java Virtual Machine により実行されます)。
Java 不正コード	Java で記述された、または埋め込まれたウイルスコードです。「Java ファイル」も参照してください。
KB	キロバイト (Kilobyte) — 1024 バイトのデータです。

用語	説明
LAN (Local Area Network)	地理的に制限されたデータ通信ネットワークです。これを使用することにより、同じ建物内のコンピュータを簡単に相互接続できます。
LDAP (Lightweight Directory Access Protocol)	メールプログラムが、サーバから連絡先情報を取得するために使用するインターネットプロトコルです。
MAC (Media Access Control) アドレス	Ethernet アダプタなどのネットワークインタフェースカードを一意に識別するアドレスのことをいいます。Ethernet では、MAC アドレスは IEEE により割り当てられる 6 オクテットのアドレスです。LAN またはその他のネットワークでは、MAC アドレスはコンピュータの一意のハードウェア番号です (Ethernet LAN では、Ethernet アドレスと同じです)。コンピュータからインターネットに接続すると (または、インターネットプロトコルでのホスト)、対応テーブルでその IP アドレスが LAN 上のコンピュータの物理的 (MAC) アドレスに関連付けられます。MAC アドレスは、電気通信プロトコルのデータリンク層のメディアアクセス制御の副層で使用されます。各物理的装置タイプに対して、MAC 副層が異なります。
MacroTrap	トレンドマイクロのユーティリティです。文書に関連して保存されるすべてのマクロコードに対してルールベースの検査を実行します。マクロウイルスのコードは通常、多くの文書とともに運ばれる、非表示のテンプレートの一部に含まれます (たとえば、Microsoft Word 文書では .dot)。MacroTrap は、テンプレートをチェックし、ウイルスのような行動をする主な命令を探して、マクロウイルスの兆候があるかどうかを確認します。命令とは、テンプレートの一部を別のテンプレートにコピー (複製) する命令や、潜在的に有害なコマンド (破壊) を実行する命令などです。
MB	メガバイト (Megabyte) — 1024 キロバイトのデータ
Mbps	100 万ビット毎秒。データ通信の帯域幅の単位です。
Microsoft Office ファイル	Excel や Word など、Microsoft Office ツールで作成されたファイルです。

用語	説明
NAT (Network Address Translation)	セキュア IP アドレスを、アドレスプールにある一時的な外部の登録 IP アドレスに変換するための規格です。これにより、信頼するネットワークに非公開の IP アドレスを割り当てて、インターネットにアクセスさせることができます。これは、ネットワーク内のすべてのコンピュータについて登録済みの IP アドレスを取得する必要がないことも意味します。
Network Content Inspection Engine (NCIE)	ボットや Web ロボットを検出できるトレンドマイクロのエンジンです。
OS	周辺機器のインタフェース、タスクのスケジュール管理、および記憶装置の割り当てなどのタスクを処理するソフトウェアです。このドキュメントでは、ウィンドウシステムおよびグラフィカルユーザインタフェースを提供するソフトウェアも指します。
SMTP	Simple Mail Transfer Protocol の略。通常は Ethernet を介して、コンピュータ間で電子メールを送受信するために使用するプロトコルです。サーバ対サーバのプロトコルであるため、メッセージのアクセスには別のプロトコルを使用します。
SMTP サーバ	メールメッセージを送信先にリレーするサーバです。
SNMP	Simple Network Management Protocol の略。管理上注意するべき状態について、ネットワークに接続されたデバイスの監視をサポートするプロトコルです。
SNMP トラップ	トラップとは、コンピュータプログラムのエラーまたはその他の問題を処理するプログラミングメカニズムです。SNMP トラップは、ネットワークデバイスの監視に関するエラーを処理します。 「SNMP」を参照してください。
SSL (Secure Socket Layer)	SSL (Secure Socket Layer) は、アプリケーションプロトコル (HTTP、Telnet、FTP など) と TCP/IP の間に層をなすデータセキュリティを提供するために Netscape が設計したプロトコルです。このセキュリティプロトコルは、データの暗号化、サーバの認証、メッセージの完全性、およびオプションで TCP/IP 接続のクライアント認証を提供します。

用語	説明
TCP	Transmission Control Protocol の略。TCP は、IP (Internet Protocol) と組み合わせて最も一般的に使用されるネットワークプロトコルで、コンピュータシステムからインターネットへの接続を管理します。
TCP/IP (Transmission Control Protocol/Internet Protocol)	ローカルおよび広域ネットワークの両方で、ピアツーピア接続機能をサポートする通信プロトコルのセットです。この通信プロトコルは、異なる OS を使用するコンピュータ間の通信を可能にします。インターネット上のコンピュータ間でデータを伝達する方法を制御します。
Telnet	TCP/IP (Transmission Control Protocol/Internet Protocol) の上で実行されるリモートログインのインターネット標準プロトコルです。リモートログインセッションのターミナルエミュレータとして動作するネットワークソフトウェアを指すこともあります。
URL	Uniform Resource Locator の略。インターネット上のオブジェクト、通常は Web ページの場所を指定する標準的な方法です。たとえば、「www.trendmicro.com」のようになります。URL は、DNS を使用して IP アドレスに変換されます。
VBscript ウイルス	VBscript (Microsoft Visual Basic スクリプト言語) は簡単なプログラム言語で、これを使用することにより、Web 開発者は、ブラウザに表示される HTML ページにインタラクティブな機能を追加できます。たとえば VBscript を使用して、Web ページに「詳細についてはここをクリックしてください」というボタンを追加できます。 VBscript ウイルスは、HTML コードのこれらの VBscript を標的にするウイルスです。これにより Web ページにウイルスを潜ませ、ユーザのブラウザを使用してウイルスをユーザのデスクトップにダウンロードできます。 「JavaScript ウイルス」も参照してください。
VLAN (Virtual Local Area Network)	デバイスの (物理的でなく) 論理的なグループで、単一のブロードキャストドメインを構成します。VLAN のメンバーは、物理的なサブネットワーク上の場所ではなく、送信データのフレームヘッダにあるタグの使用によって識別されます。VLAN は、IEEE 802.1Q 規格で記述されます。

用語	説明
VPN (Virtual Private Network)	VPN は、在宅勤務者およびモバイルプロフェッショナルが、企業のネットワークまたは別のインターネットサービスプロバイダ (ISP) に市内通話のダイヤルアップでアクセスできるようにする、簡単で費用効果が高く、安全な方法です。インターネットを介する安全なプライベート接続は、専用プライベート回線よりも費用効果が高くなります。VPN は、トンネリングや暗号化などの技術と規格によって可能になりました。
Web	World Wide Web のことで、Web またはインターネットとも呼ばれます。
Web コンソール	トレンドマイクロ製品のユーザインタフェースです。
Web サーバ	Web サイトで実行されるサーバプロセスで、リモートブラウザからの HTTP 要求に応えて Web ページを送信します。
アーカイブ	1 つのファイル、または通常は複数の個別ファイルと情報を含む単一のファイルです。.zip ファイルなどがあります。適切なプログラムを使用して解凍 (分離) できます。
アクセス	コンピュータやサーバなどの記憶装置との間で、データの読み取りまたは書き込みを行うことをいいます。
アクセス権	データの読み取りまたは書き込みを行う権限です。ほとんどの OS では、仕事に対する責任に応じて、異なるレベルのアクセス権を定義できます。
アクティブ FTP	FTP プロトコルの設定です。クライアントにコマンドセッションの「ハンドシェイク」信号の開始を許可しますが、ホストではデータセッションが開始されます。
アクティベーション	アクティベーションコードを入力して製品をアクティベートすることをいいます。製品の機能は、アクティベートが完了するまで使用できません。アクティベーションは、インストール時またはインストール後に Web コンソールの [製品ライセンス] 画面で行います。
アクティベーションコード	ハイフンを含む 37 文字のコードで、トレンドマイクロ製品のアクティベーションに使用します。アクティベーションコードの例 : SM-9UE7-HG5B3-8577B-TD5P4-Q2XT5-48PG4 「レジストレーションキー」も参照してください。

用語	説明
圧縮ファイル	1 つまたは複数の個別ファイルと情報を含む単一のファイルです。WinZip などの適切なプログラムを使用して解凍できます。
圧縮ファイル	1 つまたは複数の個別ファイルと情報を含む単一のファイルです。WinZip などの適切なプログラムを使用して解凍できます。
アップデート	アップデート機能は、多くのトレンドマイクロ製品に共通の機能です。トレンドマイクロのアップデートサーバに接続し、インターネットを介して最新のウイルスパターンファイル、検索エンジン、およびプログラムファイルをダウンロードできます。
アドウェア	広告を目的としたソフトウェアで、プログラムの実行中に広告バナーを表示します。「バックドア」をインストールし、ユーザが知らない間にユーザのコンピュータのメカニズムを追跡するアドウェアを「スパイウェア」と呼びます。
アドレス	ネットワークアドレス (「IP アドレス」を参照) またはメールアドレスを指します。メールアドレスは、メールメッセージの発信元または送信先を指定する文字列です。
暗号化	データを目的の受信者のみが読み取れる形式に変更する処理を指します。メッセージを解読するには、暗号化されたデータの受信者は、適切な解読キーを持っている必要があります。従来の暗号化スキームでは、送信者と受信者が同じキーを使用してデータを暗号化および解読します。公開鍵暗号化スキームでは 2 つの鍵を使用します。公開鍵は誰でも使用でき、対応する秘密鍵は作成者のみが所有します。この方法では、所有者の公開鍵を使用して誰もがメッセージを暗号化して送信できますが、解読に必要な秘密鍵は所有者のみが持っています。
インスタンスレベルの設定	個々のインスタンスにのみ適用される IWSVA のポリシーと設定です。
インストールスクリプト	トレンドマイクロ製品の UNIX バージョンのインストールに使用されるインストールプロシージャです。

用語	説明
インターネット	クライアントサーバ間のハイパーテキスト情報取得システムで、ルータにより接続された一連のネットワークを基礎としています。インターネットは現代の情報システムで、大学やその他多くの研究ネットワークだけでなく、広告、オンライン販売、およびサービスの媒体も幅広く受け入れています。World Wide Web は、インターネットで最も多く使用されているアプリケーションです。
インターネットプロトコル（IP）	インターネットの標準プロトコルで、データグラムと呼ばれる、データの基本単位を定義します。データグラムは、コネクションレス型で、ベストエフォート型の配信システムで使用されます。インターネットプロトコルは、インターネット上のシステム間で情報を伝達する方法を定義します。
インターネットボット	Web ロボットまたは単にボットは、DDoS 攻撃などの特定の標的に対する攻撃を開始するためによく使用されるソフトウェアアプリケーションです。これらは一般に、企業ネットワーク、個人、およびインターネットに対する脅威となり、増加の一途をたどっています。ボットが企業環境に存在すると、かなりの量のネットワーク帯域幅と処理能力が消費される可能性があります。またボットは、企業に法的責任を負わせる可能性があります。
イントラネット	外部のインターネットで提供されるものと似たサービスを組織内で提供するネットワークを指します。必ずしもインターネットには接続されていません。
ウイルス	コンピュータウイルスは、感染するという独特な能力を持つプログラム、つまり 1 つの実行可能コードです。生物学上のウイルスと同様に、コンピュータウイルスは急速に広がり、多くの場合、撲滅が困難です。 増殖することに加え、一部のコンピュータウイルスには別の共通点があります。それは、ウイルスのペイロードを配信するダメージルーチンです。ペイロードはメッセージや画像を表示するだけかもしれませんが、ファイルの破壊、ハードディスクドライブの再フォーマット、またはその他の被害を引き起こす可能性もあります。ウイルスにダメージルーチンが含まれていない場合でも、記憶領域およびメモリを消費し、コンピュータの全体的なパフォーマンスを低下させることにより、問題を引き起こすことがあります。

用語	説明
ウイルスキット	ウイルスの構築および実行のためのソースコードのテンプレートで、インターネットで入手できます。
ウイルス作成者	コンピュータハッカーとも呼ばれる、ウイルスコードを記述する人のことを指します。
ウイルスシグネチャ	ウイルスシグネチャとは、特定のウイルスを識別するビットの一意の列です。ウイルスシグネチャは、トレンドマイクロのウイルスパターンファイルに保存されています。トレンドマイクロの検索エンジンは、メールメッセージの本文や HTTP ダウンロードの内容など、ファイル内のコードをパターンファイル内のシグネチャと比較します。一致が検出されると、ウイルスが検出され、セキュリティポリシーに従って処理が実行されます (駆除、削除、または隔離など)。
ウイルス対策	コンピュータウイルスを検出および駆除するために設計されたコンピュータプログラムです。
ウイルストラップ	ウイルスコードのサンプルを分析用に捕獲するために使用するソフトウェアです。
オープンソース	一般ユーザが、ライセンスによる制限を受けずに無料で使用または変更できるプログラミングコードです。
オンラインヘルプ	IWSVA の Web コンソールから参照できるヘルプです。
隔離	メールメッセージ、感染した添付ファイル、感染した HTTP ダウンロード、または感染した FTP ファイルなど、感染したデータをサーバの隔離されたディレクトリ (隔離ディレクトリ) に置くことをいいます。
仮想 IP アドレス (VIP アドレス)	VIP アドレスは、ある IP アドレスで受信したトラフィックを、パケットヘッダの送信先のポート番号に基づいて、別のアドレスに割り当てます。
画像ファイル	2 次元で表されるデータ、つまり画像を含むファイルです。画像は、たとえばデジタルカメラを使用して現実の世界から取り込まれたり、グラフィックソフトウェアを使用してコンピュータで作成されます。
完全性のチェック	「チェックサム」を参照してください。

用語	説明
感染報告のあるウイルス	活発に移動する既知のウイルスを指します。「出回っていないウイルス」も参照してください。
管理者	「システム管理者」を指します。システム管理者とは、組織の一員で、新しいハードウェアおよびソフトウェアの設定、ユーザ名およびパスワードの割り当て、ディスク容量やその他の IT リソースの監視、バックアップの実施、およびネットワークセキュリティの管理について責任を持ちます。
管理者アカウント	管理者レベルの権限を持つ、ユーザ名およびパスワードです。
管理者メールアドレス	トレンドマイクロ製品の管理者が、通知および警告の管理に使用するアドレスです。
管理ドメイン	共通のデータベースおよびセキュリティポリシーを共有するコンピュータのグループです。
キーロガー	キーロガーは、キーボードのすべての動きを捕捉して保存するプログラムです。企業が従業員を監視したり、親が子供を監視するために使用する、合法的なキーロギングプログラムもあります。しかし、犯罪者によってキーストロークのログが使用され、ログオン認証情報やクレジットカード番号などの重要な情報が利用されることもあります。
キャッシュ	最近アクセスしたデータを保持する、小さく高速なメモリ。同じデータに続けてアクセスする際の速度を上げるように設計されています。この用語は、プロセッサとメモリの間のアクセスに適用される場合が最も多いのですが、ネットワークを介してアクセス可能なデータのローカルコピーなどにも適用されます。
キュー	メールが処理可能な速度よりも速く受信される場合に、1 つのリソースに対する複数の要求を一定の順序で配列するために使用するデータ構造です。FIFO（一番新しく格納されたものを一番最後に処理する) アプローチを使用して、メッセージはキューの末尾に追加され、キューの先頭にあるメッセージから処理されます。
共有ドライブ	複数のユーザが使用するコンピュータ周辺デバイスです。そのため、ウイルスにさらされる危険性が高まります。

用語	説明
駆除	ファイルまたはメッセージからウイルスコードを削除することをいいます。
クライアント	ある種のプロトコルを使用し、別のコンピュータシステムまたはプロセス (「サーバ」) のサービスを要求してサーバの応答を受け取る、コンピュータシステムまたはプロセスです。クライアントは、クライアントサーバソフトウェアアーキテクチャの一部です。
クライアント / サーバ環境	分散型システムの一般的な形式で、ソフトウェアがサーバのタスクとクライアントのタスクに分離されます。クライアントは、一定のプロトコルに従い、情報または処理を求めてサーバに要求を送信し、その要求にサーバが応答します。
グレーウェア	正規なプログラムではあるが、望ましくない、または不正な可能性のあるソフトウェアのカテゴリです。ウイルス、ワーム、およびトロイの木馬などの脅威とは異なり、感染、増殖、またはデータの破壊は行いませんが、プライバシーを侵害する可能性があります。グレーウェアの例には、スパイウェア、アドウェア、およびリモートアクセスツールなどがあります。
警告	システムのユーザまたは管理者に、システムの稼働状態の変化や、ある種のエラー状態について知らせることを目的としたメッセージです。
ゲートウェイ	情報源と Web サーバとの間のインタフェースです。
原因	URL ブロックやファイルブロックなど、保護処理が開始された理由です。この情報は、ログファイルに表示されます。
検索	ファイル内のアイテムを順番に調べて、特定の条件に一致するアイテムを探すことをいいます。
検索エンジン	ウイルス対策検索を実行したり、統合されているホスト製品の検出を実行するモジュールです。

用語	説明
公開鍵暗号方式	暗号化のスキームで、各ユーザは公開鍵と秘密鍵と呼ばれる一対の「鍵」を取得します。各ユーザの公開鍵は公開されていますが、秘密鍵は秘密にされています。メッセージは、目的の受信者の公開鍵を使用して暗号化され、受信者の秘密鍵を使用してのみ解読されます。「認証」および「デジタル署名」も参照してください。
サーバ	あるサービスを他の (クライアント) プログラムに提供するプログラムです。クライアントとサーバの間の接続は、通常、メッセージの伝達により実行されます。多くの場合ネットワークを介し、特定のプロトコルを使用してクライアントの要求とサーバの応答をエンコードします。サーバは、要求の到着を待って継続的に (デーモンとして) 稼働するか、または、いくつかの特定のサーバを制御するより高いレベルのプロセスによって呼び出されます。
サブネットマスク	比較的大規模なネットワークでは、サブネットマスクを使用してサブネットワークを定義できます。たとえば、クラス B のネットワークがある場合、サブネットマスク 255.255.255.0 は、ピリオドで区切られた最初の 2 つの部分がネットワーク番号、3 番目の部分がサブネット番号を指定します。4 番目の部分はホスト番号です。クラス B のネットワークでサブネットを使用しない場合は、サブネットマスク 255.255.0.0 を使用します。 1 つのネットワークは、メインネットワークのサブセットを形成する、1 つ以上の物理ネットワークにサブネット化できます。サブネットマスクは IP アドレスの一部であり、ネットワーク内のサブネットワークを表すのに使用します。サブネットマスクを使用して、通常は使用できないネットワークアドレスの領域を使用できるようにしたり、意図しないかぎりネットワークトラフィックがネットワーク全体に送信されないようにします。サブネットマスクは複雑な機能であり、使用する際には細心の注意を払う必要があります。「IP アドレス」も参照してください。
シート	1 人のユーザがトレンドマイクロ製品を使用するためのライセンスのことです。
シグネチャ	「ウイルスシグネチャ」を参照してください。

用語	説明
実行可能ファイル	機械語のプログラムを含む、すぐに実行可能なバイナリファイルです。
実際のファイルタイプ	ウイルス検索技術で、ファイル名拡張子に関係なく (だまされる場合があります)、ファイルヘッダを調べることによってファイル内の情報の種類を特定します。
受信	お使いのネットワークに送信されてくる、メールメッセージまたはその他のデータです。
受信者	メールメッセージの宛先となるユーザまたはエンティティです。
使用許諾契約書 (EULA)	使用許諾契約書は、ソフトウェア公開者とソフトウェアユーザとの間の法的契約です。通常はユーザ側の規定について述べられています。ユーザはインストールの際に「同意します」をクリックしなければ、その契約を拒否できます。もちろん「同意しません」をクリックすると、ソフトウェア製品のインストールは終了します。 多くのユーザは、ある種のフリーソフトウェアのインストールの際に表示される使用許諾契約書の同意を求める画面で「同意します」をクリックして、スパイウェアやアドウェアのコンピュータへのインストールに不注意で同意してしまいます。
ジョークプログラム	ユーザを困らせたり不適切な警告を発したりする実行可能プログラムです。ウイルスとは異なり自己増殖しないので、システムから簡単に削除できます。
初期設定	Web コンソールのインタフェースで、あらかじめ入力されている値のことを指します。初期設定値は論理的な選択を表し、便宜上入力されています。初期設定値はそのまま使用することも、変更することもできます。
スクリプト	呼び出して一緒に実行できる、プログラミングコマンドのセットです。「スクリプト」と同義で使用される他の用語には、「マクロ」や「バッチファイル」があります。
スパイウェア	広告を目的としたソフトウェアで、通常はシステムに追跡ソフトウェアをインストールします。追跡ソフトウェアは、個人に関する情報を第三者に送信できます。スパイウェアの脅威は、収集されるデータやその使用目的をユーザが管理できないことにあります。

用語	説明
スパムメール	製品またはサービスの宣伝販売を目的として、無差別に送信されるメールメッセージです。
セキュリティホール	ソフトウェアの脆弱性などを利用するコードです。セキュリティホールは、脆弱なコンピュータの間で広まり、複雑なルーチンを実行できます。
セクタ	ディスクを物理的に分割した部分です(「パーティション」も参照してください。パーティションは、ディスクを論理的に分割した部分です)。
設定	トレンドマイクロ製品をどのように機能させるかについてオプションを選択することをいいます。たとえば、ウイルスに感染したメールメッセージを隔離するか削除するかを選択します。
増殖	ウイルスやワームが自己複製することをいいます。
送信	お使いのネットワークからインターネットに送信される、メールメッセージまたはその他のデータです。
ゾーン	ゾーンには、セキュリティ基準が適用されるネットワークスペースのセグメント (セキュリティゾーン)、VPN トンネルインタフェースがバインドされる論理セグメント (トンネルゾーン)、または、特定の機能を実行する物理的または論理的エンティティ (機能ゾーン) があります。
待機ポート	データ交換についてクライアント接続要求に使用するポートです。
対象 (「処理」および「通知」も参照)	メールメッセージで検出されるウイルスなど、イベントの違反について監視する活動の範囲を指します。たとえば、ウイルス検索について、ネットワークを通過するすべてのファイルを対象にしたり、特定のファイル名拡張子を含むファイルのみを対象にできます。
ダイヤラー	トロイの木馬の一種で、実行されると、ユーザのシステムをペイパーコールの通話先に接続します。疑いを持たないユーザは、知らない間に、その通話に対して請求されます。

用語	説明
ダウンロード	あるコンピュータから別のコンピュータへ、データまたはコードを転送することをいいます。ダウンロードとは、多くの場合、より大きな「ホスト」システム (特にサーバまたはメインフレーム) から、より小さな「クライアント」システムに転送することをいいます。
ダメージルーチン	ウイルスコードの破壊的な部分のことで、ペイロードとも呼ばれます。
通知 (「処理」および「対象」も参照)	次のいずれかまたは複数の宛先に送信されるメッセージです。 — システム管理者 — メッセージの送信者 — メッセージ、ファイルのダウンロード、またはファイル転送の受信者 通知の目的は、HTTP でのファイルダウンロードを試みた際に検出されたウイルスなど、禁止された処理が発生した、または試みられたことを知らせることです。
ディスクレーマー	メールの先頭または最後尾に挿入されるメッセージで、メールの内容に関する法律厳守や守秘義務の条項を表します。
ディレクトリ	階層型のコンピュータファイルシステム構造の一部であるノードを指します。ディレクトリには、通常、別のノード、フォルダ、またはファイルが含まれます。たとえば、C:\Windows は、C ドライブの Windows ディレクトリです。
ディレクトリパス	ディレクトリ内の続いている層で、その先にファイルなどが存在します。
デーモン	明示的には実行されませんが、ある条件が発生するのを待って休止しているプログラムです。
デジタル署名	メッセージに付加される追加データです。公開鍵暗号方式という技術を使用して、メールの送信者とメッセージデータを識別し、認証します。「公開鍵暗号方式」および「認証」も参照してください。
出回っていないウイルス	現在ウイルス対策製品で制御されている、既知のウイルスを指します。「感染報告のあるウイルス」も参照してください。

用語	説明
添付ファイル	メールメッセージに添付されて一緒に送信されるファイルです。
登録	[ユーザ登録] 画面で製品のレジストレーションキーを使用して、お客さまをトレンドマイクロのユーザとして認識する処理です。 https://clp.trendmicro.com/fullregistration
トータル ソリューション CD/DVD	最新製品バージョンとすべてのパッチが格納されている CD または DVD です。それらのパッチは、前の期間において適用されているものです。トータルソリューション CD または DVD は、トレンドマイクロ プレミアム サポートを受けるすべてのお客さまで利用できます。
トップレベルドメイン	インターネットの完全修飾ドメイン名の最後にある最も重要な構成要素で、最後の「.」の後の部分です。たとえば、ホスト「trendmicro.co.jp」のトップレベルドメインは「jp」です。
ドメイン名	システムの完全な名前で、ローカルホスト名とドメイン名で構成されます。たとえば、texample.com などです。ドメイン名は、インターネット上のすべてのホストに一意のインターネットアドレスを定めるのに十分なものである必要があります。この処理は「名前解決」と呼ばれ、Domain Name System (DNS) を使用します。
トラフィック	インターネットとお使いのネットワークの間を流れる送受信データです。
トリガ	活動の発生を引き起こすイベントです。たとえば、トレンドマイクロ製品がメールメッセージでウイルスを検出したとします。この「トリガ」により、メッセージが隔離ディレクトリに置かれ、システム管理者、メッセージの送信者、およびメッセージの受信者に通知が送信されます。
トレンドマイクロの推奨設定	トレンドマイクロの検索技術です。実際のファイルタイプによる認識を使用してファイルヘッダを調べ、潜在的に不正コードが潜んでいる可能性があると知られているファイルタイプのみを検索することにより、パフォーマンスを最適化します。実際のファイルタイプによる認識は、無害な拡張子名で偽装している可能性のある不正コードの識別に役立ちます。

用語	説明
トロイの木馬	害のないプログラムを装う不正プログラムです。トロイの木馬は実行可能プログラムです。増殖はせず、代わりにシステムに常駐して、侵入者に対してポートを開くなどの不正な行為を実行します。
ドロッパ	ウイルス、トロイの木馬、またはワームをシステムに運ぶ送信メカニズムとして機能するプログラムです。
トンネリング	あるネットワークが別のネットワークの接続を介してデータを送信できる、データの送信方法です。トンネリングは、インターネットでサポートされないプロトコルを使用する管理ドメイン間のデータを、そのドメイン間でやり取りするために使用されます。 VPN トンネリングでは、モバイルプロフェッショナルは企業のネットワークに直接ダイヤルするのではなく、市内のインターネットサービスプロバイダのアクセスポイントにダイヤルします。これは、モバイルプロフェッショナルがどこにいても、VPN トンネリング技術をサポートする市内のインターネットサービスプロバイダにダイヤルして、市内通話の電話料金のみで企業のネットワークにアクセスできることを意味します。 リモートユーザが、VPN トンネリングをサポートするインターネットサービスプロバイダを使用して企業のネットワークにダイヤルすると、組織だけでなく、リモートユーザもその接続が安全であるとわかります。すべてのリモートダイヤルインユーザは、インターネットサービスプロバイダのサイトの認証サーバで認証されてから、企業のネットワークにある別の認証サーバで再度認証されます。これは、許可されたリモートユーザのみが企業のネットワークにアクセスでき、そのユーザによる使用が許可されたホストのみにアクセスできることを意味します。

用語	説明
トンネル インタフェース	トンネルインタフェースとは、トラフィックが VPN トンネルを通過するための通路または戸口を指します。トンネルインタフェースには、番号を付ける（つまり、IP アドレスを割り当てる) ことも、付けないこともできます。番号の付いたトンネルインタフェースは、トンネルゾーンまたはセキュリティゾーンのいずれかに配置できます。番号の付いていないトンネルインタフェースは、少なくとも 1 つのセキュリティゾーンインタフェースを含むセキュリティゾーンにのみ配置できます。番号の付いていないトンネルインタフェースは、セキュリティゾーンインタフェースから IP アドレスを借用します。「VPN（Virtual Private Network)」も参照してください。
トンネルゾーン	1 つ以上のトンネルインタフェースをホストする論理セグメントです。トンネルゾーンは、キャリアとして動作するセキュリティゾーンに関連付けられます。
認証	人またはプロセスの同一性の確認を行います。認証を使用することで、デジタルデータ伝送が、目的の受信者に対して確実に行われます。受信者側では、メッセージとその送信元（どこの誰から送られてきたか) が改変されていないことが保証されます。 認証の最も単純な形式では、特定のアカウントにアクセスするために、ユーザ名とパスワードが必要です。認証プロトコルは、秘密鍵暗号方式や、デジタル署名を使用する公開鍵システムを基にすることもできます。 「公開鍵暗号方式」および「デジタル署名」も参照してください。
ネットワークウイルス	TCP、FTP、UDP、HTTP、およびメールプロトコルなどのネットワークプロトコルを使用して増殖するタイプのウイルスです。ネットワークウイルスは、多くの場合、システムファイルの改ざんやハードディスクのブートセクタの変更は行いません。代わりにクライアントコンピュータのメモリに感染し、そのコンピュータを使用してネットワークのトラフィックをあふれさせて、ネットワークの速度低下や完全な機能不全さえも引き起こす可能性があります。
パージ	ログで古いエントリを削除することによりすべて削除することを指します。

用語	説明
パーティション	ディスクを論理的に分割した部分です (「セクタ」も参照してください。セクタは、ディスクを物理的に分割した部分です)。
ハードディスク (またはハードディスクドライブ)	中央の軸を中心に回転する、1 つまたは複数の固定された磁気ディスクです。ハードディスクまたはフロッピーディスクの読み書きやデータの保存に使用される、読み書き用のヘッドと電子機器を備えています。ほとんどのハードディスクはドライブ (固定されたディスク) に常時接続されていますが、取り外し可能なディスクもあります。
配置ウィザード	Web コンソールベースのウィザードで、配信を容易にするために使用されます。配信関連の設定は、製品インストールからこのウィザードに移動されました。
バイナリ	数字の 0 と 1 で構成されるデータで、デジタル電子工学およびブール代数を使用した実装が容易なため、事実上すべてのコンピュータで使用されます。
パスワード解析アプリケーション	失効した、または忘れてしまったパスワードを取り戻すために使用するアプリケーションプログラムです。こうしたアプリケーションは、侵入者がコンピュータまたはネットワークリソースに権限を持たずにアクセスするために使用されることもあります。
パターンファイル (またはオフィシャルパターンリリース)	パターンファイルはオフィシャルパターンリリース (OPR) とも呼ばれ、確認済みのウイルスパターンを編集した最新版です。最新のウイルスの脅威から確実に保護されるよう、いくつもの厳しいテストを通過したことが保証されています。このパターンファイルは、最新の検索エンジンと併用すると最も効果的です。
ハッキングツール	不当に使用される恐れのあるセキュリティの脆弱性を発見する目的で、コンピュータシステムまたはネットワークへの侵入テストを実行できるようにする、ハードウェアおよびソフトウェアなどのツールです。
パッシブ FTP	FTP プロトコルの設定です。ローカルエリアネットワーク内のクライアントに、ランダムな上位ポート番号 (1024 以上) を使用したファイル転送の開始を許可します。
パラメータ	値の範囲 (1 ～ 10 の数) などの変数です。

用語	説明
非武装地帯 (DMZ)	元は軍事用語で、敵同士の間で戦闘が行われていない領域のことを指します。DMZ Ethernet は、異なる組織によって制御されているネットワークおよびコンピュータを接続します。これらの組織は外部または内部の可能性があります。外部 DMZ Ethernet は、ルータで地域のネットワークにリンクします。
ヒューリスティック ルールベースの検索	プロパティの論理分析を使用したネットワークトラフィックの検索で、ソリューションの検索を減らすまたは制限します。
ファイアウォール	特殊なセキュリティ対策を施したゲートウェイコンピュータで、外部ネットワーク (特にインターネット) の接続およびダイヤルイン回線に使用されます。
ファイル	データの要素で、メールメッセージや HTTP ダウンロードなどを指します。
ファイル感染型 ウイルス	ファイル感染型ウイルスは、実行可能プログラム (一般的には、.com または .exe の拡張子を持つファイル) に感染します。こうしたウイルスのほとんどは、他のホストのプログラムに感染して増殖し、拡散しようとしますが、ウイルスによっては、感染したプログラムのオリジナルコードの一部を上書きして不注意により破壊するものもあります。こうした少数のウイルスは非常に破壊的で、あらかじめ設定された時刻にハードディスクドライブをフォーマットしようとしたり、その他の不正な処理を実行しようとしたりします。 多くの場合、ファイル感染型ウイルスは、感染ファイルから正常に削除できます。ただし、ウイルスがプログラムコードの一部を上書きした場合、オリジナルファイルは元に戻せません。
ファイルタイプ	ファイルに保存されるデータの種類です。ほとんどの OS では、ファイル名拡張子を使用してファイルタイプを特定します。ファイルタイプにより、そのファイルを表すユーザインタフェース上の適切なアイコンと、ファイルの表示、編集、実行、または印刷に使用する適切なアプリケーションが選択されます。

用語	説明
ファイルタイプグループ	共通のテーマを持つファイルの種類です。たとえば、次のものがあります。 — オーディオ / ビデオ — 圧縮 — 実行可能 — 画像 — Java — Microsoft Office
ファイル名拡張子	「.dll」や「.xml」など、ファイル名の一部分で、ファイルに保存されているデータの種類を表します。ファイル名拡張子は、ファイル内の情報の種類を示すだけでなく、通常、ファイルの実行時に起動するプログラムを識別するのに使用されます。
不快なコンテンツ	冒涜、セクシュアルハラスメント、人種に関する嫌がらせ、または中傷など、他人にとって不快と見なされるメッセージの語句または添付ファイルです。
負荷分散	負荷分散とは、同時に発生するコンピュータ処理の効率を高める目的で、複数のプロセッサに仕事を割り当てる (再割り当てする) ことをいいます。
複合的な脅威による攻撃	企業ネットワークの複数の侵入ポイントおよび脆弱性を利用する複合的な攻撃で、「Nimda」や「Code Red」などの脅威があります。
不正プログラム(不正ソフトウェア)	ウイルス、ワーム、およびトロイの木馬など、危害を与えることを目的として開発されるプログラムまたはファイルです。
ブラウザ	人間がハイパーテキストを読めるようにするプログラムで、Internet Explorer などがあります。ブラウザを使用することにより、ノード (または「ページ」) の内容を表示したり、ノード間の移動が可能になります。ブラウザは、リモート Web サーバに対してはクライアントとして動作します。
プロキシサーバ	特殊な接頭辞が付いた URL を受け入れる Web サーバです。ローカルキャッシュまたはリモートサーバのいずれかから文書を取得して、その URL を要求者に返すために使用されます。

用語	説明
プログラム ディレクトリ	メインのアプリケーションファイルを保存する、インストール先のディレクトリです。たとえば、C:\Program Files\Trend Micro\IWSVA などです。
ブロック	ネットワークへの侵入を防ぐことをいいます。
ヘッダ (ネットワーク定義)	ファイルまたは伝送に関する暗号化されていない情報を含む、データパケットの一部です。
ポート	通信システムの論理チャンネルまたはチャンネルの終点で、同じコンピュータの同じネットワークインタフェースにおいて、異なる論理チャンネルを区別するために使用されます。
保護された ネットワーク	IWSVA (InterScan Web Security Virtual Appliance) によって保護されたネットワークです。
ホスト	ネットワークに接続されたコンピュータ。
ポリシー	ポリシーは、ファイアウォールに対して最初の保護メカニズムを提供します。これを使用することにより、IP セッションの詳細に基づいて、どのトラフィックを通過させるかを決めることができます。ポリシーは、信頼するサーバの検索など、外部の攻撃から信頼するネットワークを保護します。ポリシーにより、ファイアウォールを通過しようとするトラフィックを監視するセキュリティポリシーを設定した環境を作成できます。
マクロ	アプリケーション内で特定の機能を自動的に実行するために使用されるコマンドです。
マクロウイルス	マクロウイルスは多くの場合、アプリケーションのマクロとしてコード化され、文書に含まれています。他のウイルスタイプと異なり、マクロウイルスは OS 特有のものではなく、メールの添付ファイル、Web ダウンロード、ファイル転送、および連携アプリケーションを介して広がる可能性があります。
マスメーリング型 ウイルス	大量のネットワークトラフィックを発生させるため大きな損害を与える可能性が高い、不正プログラムです。
ライセンス	トレンドマイクロ製品を使用するための法的な許可です。

用語	説明
ライセンス証明書	トレンドマイクロ製品の認定ユーザであることを証明する文書です。
リムーバブルドライブ	コンピュータの取り外し可能なハードウェアコンポーネントまたは周辺デバイスです。
リモートアクセスツール (RAT)	正当なシステム管理者がネットワークをリモートで管理できるようにする、ハードウェアおよびソフトウェアです。ただし、このようなツールは、侵入者がシステムのセキュリティを突破するために使用される可能性もあります。
リレー	さまざまな他のポイントを通過して伝送することをいいます。
リンク (ハイパーリンクとも呼ばれます)	あるハイパーテキスト文書内のポイントから、別の文書または同じ文書内の別のポイントへの参照です。リンクは通常、下線を引いた青いテキストなど、異なる色またはテキストスタイルで区別されます。たとえばマウスでリンクをクリックするなど、リンクをアクティブにすると、ブラウザにリンク先が表示されます。
ルータ	このハードウェア装置は、ローカルエリアネットワーク (LAN) から長距離回線にデータを発送します。
レジストレーションキー	ハイフンを含む 22 文字のコードで、トレンドマイクロの顧客データベースでの登録時に使用されます。レジストレーションキーの例 : SM-27RT-UY4Z-39HB-MNW8 「アクティベーションコード」も参照してください。
ローカルエリアネットワーク (LAN)	Ethernet など、通常は高速でオフィス環境内のリソースを相互接続するネットワーク技術です。ローカルエリアネットワークは短距離のネットワークで、同じ建物内のコンピュータグループを互いに接続するために使用します。
ログ保存ディレクトリ	ログファイルを保存する、サーバ上のディレクトリです。
論理爆弾	アプリケーションまたは OS に不正に挿入されたコードで、指定された条件に一致するたびに、破壊的な、またはセキュリティを危険にさらす活動を実行します。

用語	説明
ワークステーション (またはクライアント)	一度に 1 人のユーザが使用するように設計された汎用コンピュータで、特に画像、処理能力、および複数のタスクを同時に実行する能力において、通常はパーソナルコンピュータよりも高いパフォーマンスを提供します。
ワーム	他のプログラムに寄生しないプログラム（またはプログラムセット) で、自身の機能のコピーを広めたり、セグメントを別のコンピュータシステムに送信します。
ワイルドカード	コンテンツフィルタの参照に関する用語で、アスタリスク (*) が任意の文字を表します。たとえば、*ber という表現は、barber、number、plumber、timber などを表すことができます。この用語は、トランプのゲームに由来します。トランプのゲームでは、特定のカードが「ワイルドカード」として識別されます。ワイルドカードは、ゲームで任意の数や組に使用できます。
割り込み	通常の処理を中断し、「割り込みハンドラ」ルーチンを通じて制御の流れを一時的に変える、非同期のイベントです。

索引

英数字

あ

か

さ

た

な

は

わ