InterScan Web Security Suite™ 6.5 Linux版

インストールガイド

Web Security

※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。
  http://esupport.trendmicro.com/ja-jp/support-lifecycle/default.aspx

著作権について

本書に関する著作権は、トレンドマイクロ株式会社へ独占的に帰属します。トレンドマイクロ株式会社が事前に承諾している場合を除き、形態および手段を問わず、本書またはその一部を複製することは禁じられています。本書の作成にあたっては細心の注意を払っていますが、本書の記述に誤りや欠落があってもトレンドマイクロ株式会社はいかなる責任も負わないものとします。本書およびその記述内容は予告なしに変更される場合があります。

商標について

TRENDMICRO、TREND MICRO、ウイルスバスター、ウイルスバスター On‐Line Scan、PC-cillin、InterScan、INTERSCAN VIRUSWALL、InterScanWebManager、
InterScan Web Security Suite、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、トレンドマイクロ・プレミアム・サポート・プログラム、Trend Park、
Trend Labs、Trend Micro Network VirusWall、Network VirusWall Enforcer、LEAKPROOF、Trend Micro Threat Management Solution、Trend Micro Threat Management Services、
Trend Micro Threat Mitigator、Trend Micro Threat Discovery Appliance、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、
Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、SPN、SMARTSCAN、Trend Micro Kids Safety、Trend Micro Web Security、
Trend Micro Collaboration Security、Trend Micro Portable Security、Trend Micro Standard Web Security、Trend Micro Hosted Email Security、Trend Micro Deep Security、
ウイルスバスタークラウド、Smart Surfing、スマートスキャン、Trend Micro Instant Security、Trend Micro Enterprise Security for Gateways、Enterprise Security for Gateways、
Trend Micro Email Security Platform、Trend Micro Vulnerability Management Services、Trend Micro PCI Scanning Service、Trend Micro Titanium AntiVirus Plus、Smart Protection Server、
Deep Security、ウイルスバスター ビジネスセキュリティサービス、SafeSync、Trend Micro InterScan WebManager SCC、Trend Micro NAS Security、Trend Micro Data Loss Prevention、
Securing Your Journey to the Cloud、Trend Micro オンラインスキャン、Trend Micro Deep Security Anti Virus for VDI、Trend Micro Deep Security Virtual Patch、
Trend Micro Threat Discovery Software Appliance、SECURE CLOUD、Trend Micro VDIオプション、おまかせ不正請求クリーンナップサービス、
Trend Micro Deep Security あんしんパック、こどもーど、Deep Discovery、TCSE、おまかせインストール・バージョンアップ、Trend Micro Safe Lock、Deep Discovery Advisor、
Deep Discovery Inspector、Trend Micro Mobile App Reputation、あんしんブラウザ、Jewelry Box、カスタム ディフェンス、InterScan Messaging Security Suite Plus、
おもいでバックアップサービス、おまかせ！スマホお探しサポート、保険&デジタルライフサポート、おまかせ！迷惑ソフトクリーンナップサービス、
Smart Protection Integration Framework、InterScan Web Security as a Service、Client/Server Suite Premium、Cloud Edge、Trend Micro Remote Manager、Threat Defense Expert、
スマートプロテクションプラットフォーム、Next Generation Threat Defense、セキュリティアットホーム、セキュリティエプリウェア、セキュリティコンシェルジュ、
Trend Micro Smart Home Network、Dr.Booster、Trend Micro Retro Scan、is702、デジタルライフサポート プレミアム、Airサポート、Connected Threat Defense、および
ライトクリーナーは、トレンドマイクロ株式会社の登録商標です。

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

Copyright © 2016 Trend Micro Incorporated. All rights reserved.

P/N: IHEM67228/150924_JP_R2 (2016/09)

目次

はじめに 7
対象 8
ドキュメント 8
ドキュメントの表記規則 9

第 1 章　インストール計画 11
システム要件 12
その他の要件 12
IWSS のインストールに必要な情報 12
HTTP ハンドラの種類 13
プロキシ設定の種類 13
Trend Micro Control Manager サーバ情報 13
データベースの種類と場所 13
SNMP 通知 14
Web コンソールのパスワード 14
IWSS とインターネット間のプロキシ 14
アクティベーションコード 14
新規インストール 14
ネットワークトラフィック保護を計画する 15
クライアントを再設定する 15
レイヤ 4 スイッチを使用する 17
ICAP 対応のプロキシを使用する 18
不特定のクライアントから特定の HTTP サーバまたは FTP サーバを保護する 19
HTTP および FTP のサービスフローを計画する 19
HTTP フローを計画する 20
依存モードの HTTP リバースプロキシ 28

FTP フローを計画する 33

第 2 章　配置について 37

オペレーティングモード 38

サーバの設置場所を確認する 38

DMZ を備えた 2 つのファイアウォール 38

DMZ を備えていない 1 つのファイアウォール 39

ネットワーク保護および HTTP/FTP サービスフローを計画する 40

第 3 章　インストール 43

インストール対象コンポーネント 44

インストール前に関する注意 45

ユーザプロセスと開くファイルの最大数を設定する 45

SELinux の無効化 46

IWSS をインストールする 46

インストール後に関する注意 47

付録 A　導入の統合 49

ICAP デバイスとの連携 50

IWSS ICAP のインストール後の設定 50

「X-Virus-ID」ヘッダと「X-Infection-Found」ヘッダを有効化する 55

分散環境における IWSS 56

接続の要件と特性 56

LDAP との連携 57

複数の LDAP サーバによるマルチドメインのサポート 57

HTTP サーバを保護する 59

FTP サーバを保護する 60

付録 B　調整とトラブルシューティング 61

パフォーマンスの調整 62
URL フィルタ 62
LDAP パフォーマンスの調整 62
OS の調整 64
トラブルシューティング 65
トラブルシューティングのヒント 65
テクニカルサポートに問い合わせる前に 66
インストールに関する問題 66
一般的な機能に関する問題 66

付録 C 追加テスト 69
アップロード検索をテストする 70
FTP 検索をテストする 71
URL ブロックをテストする 72
ダウンロード検索をテストする 73
URL フィルタをテストする 74
スパイウェア検索をテストする 75
フィッシング対策をテストする 76
Java アプレット /ActiveX 対策をテストする 77
情報漏えい対策をテストする 78

付録 D インストール後のタスクと参考情報 81
OS のセキュリティ強化 82
セキュリティ強化に必要な OS インストール前の手順 82
セキュリティ強化に必要な OS インストールの手順 82
OS インストール後のその他の手順 83

付録 E テクニカルサポート 85
アップデートプログラムについて 86

製品サポート情報 86
サポートサービスについて 86
製品 Q&A のご案内 87
セキュリティ情報 87
トレンドマイクロ「セキュリティ情報」..... 87
トレンドマイクロへのウイルス解析依頼 88
脅威解析・サポートセンター TrendLabs (トレンドラボ) 88

索引 89

はじめに

はじめに

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

本章では、次の項目について説明します。

- 8 ページの「対象」
- 8 ページの「ドキュメント」
- 9 ページの「ドキュメントの表記規則」

対象

この IWSS ドキュメントは、中小企業および大企業のシステム管理者を対象として書かれています。本書は、次の項目に関する詳しい内容とネットワークに関する知識を持った方を対象としています。

- HTTP および FTP プロトコル
- データベース設定

ドキュメント

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

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

  各種ドキュメントの最新版は、次の Web サイトから入手できます。

  `http://www.trendmicro.co.jp/download/`
- **オンラインヘルプ** — ユーザインタフェースを使用して IWSS を設定する方法を確認できます。Web コンソールを開いて、ヘルプアイコンをクリックすると、オンラインヘルプにアクセスできます。オンラインヘルプは、製品の主なタスクの操作手順、利用方法のアドバイス、および実際に使用する場面にさまざまな情報を提供します。オンラインヘルプの情報には、有効なパラメータ範囲や最適値などが存在します。オンラインヘルプには、IWSS の管理コンソールからアクセスできます。
- **製品 Q&A** — 製品 Q&A は、問題解決およびトラブルシューティング情報のオンラインデータベースを提供しています。製品の既知の問題に関する最新情報も参照できます。次の製品 Q&A Web サイトをご利用ください。

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

管理者ガイドと Readme ファイルは、IWSS 付属の CD-ROM に収録されており、Web サイト (`http://www.trendmicro.co.jp/download/`) からも入手できます。

ドキュメントの表記規則

このドキュメントでは、次の表記規則を使用しています。

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

表 1.　本書で使用している表記規則

第 1 章

インストール計画

本章で説明する内容には、次の項目が含まれます。

- 12 ページの「システム要件」
- 12 ページの「IWSS のインストールに必要な情報」
- 15 ページの「ネットワークトラフィック保護を計画する」
- 19 ページの「HTTP および FTP のサービスフローを計画する」

システム要件

最新の情報については、次の Web サイトを参照してください。

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

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

その他の要件

- ネットワーク上のクライアントは、配置ウィザードで IWSS サーバ用に選択した HTTP プロキシポートにアクセスできる必要があります。
- InterScan Web Security Suite 6.5 (以下、IWSS) サーバとクライアントは、社内ネットワーク経由で相互に通信できる必要があります。

注意： システム要件に記載されているオペレーティングシステムの種類やハードディスク容量などは、本ドキュメント作成時点の情報です。システム要件は、オペレーティングシステムのサポート終了や、弊社製品の改良、検索エンジンやパターンファイルのバージョンアップなどに伴い、変更、追加、または削除される場合があります。また、製品の運用環境によっては、ログファイルの保存、他のソフトウェアとの共存などにより、必要となるメモリサイズやハードディスク容量も異なりますので、ご注意ください。最新の情報については、http://www.go-tm.jp/iwsva/req を参照してください。

IWSS のインストールに必要な情報

IWSS を購入するか、IWSS の体験版を使用できます。体験版では IWSS の機能がすべて提供されます。試用期間が終了すると、セキュリティアップデートと検索の両方の機能が無効になります。

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

HTTP ハンドラの種類

プロキシ転送を指定した場合、IWSS はネットワークの HTTP プロキシとして動作するか、または別の HTTP プロキシを上位プロキシとして設定し連携して動作することもできます。また、ICAP サーバとして動作するように設定することもできます。詳細については、20 ページの「HTTP フローを計画する」を参照してください。

プロキシ設定の種類

IWSS は、複数の配信モードをサポートします。

- クライアントが直接 IWSS に接続するプロキシ転送
- 既存の内部プロキシサーバへの上位プロキシ
- 既存の ICAP 1.0 準拠キャッシュコントローラへの ICAP サーバ
- Web サーバを保護するためのリバースプロキシ
- 通常の透過モード

最も一般的なプロキシ設定では、IWSS をフォワードプロキシとして設定し、インターネットからのダウンロードに伴う脅威からクライアントを保護します。

IWSS サーバをクライアントのプロキシとして使用するには、クライアントのインターネット接続設定を変更する必要があります (透過を有効にした場合を除く)。

別の設定方法として、IWSS をリバースプロキシとして構成し、Web サーバに不正なコンテンツがアップロードされないようにすることもできます。詳細については、20 ページの「HTTP フローを計画する」および 33 ページの「FTP フローを計画する」を参照してください。

Trend Micro Control Manager サーバ情報

IWSS をネットワーク上の既存の Trend Micro Control Manager (以下、Control Manager) に登録する場合は、Control Manager サーバのホスト名または IP アドレスとユーザ ID が必要です。

データベースの種類と場所

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

SNMP 通知

SNMP 通知は、管理コンソールの [管理] → [一般設定] → [SNMP の設定] で表示される画面で情報を入力することにより使用できます。

Web コンソールのパスワード

IWSS Web コンソールへのアクセスは、管理者アカウントによって制限されます。

Web コンソールへのログイン

IWSS Web コンソールを開くには、次の初期情報が必要です。この情報は大文字と小文字が区別されます。

- ユーザ名 — admin
- パスワード — adminIWSS85

ヒント： パスワードは定期的に変更してください。

IWSS とインターネット間のプロキシ

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

アクティベーションコード

メインプログラム、Web セキュリティ強化フィルタオプション (URL フィルタ)、およびモバイルコードセキュリティオプション (アプレット /Active X 対策) 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。

新規インストール

IWSS を新規インストールする場合は、`./install_iwss.sh` スクリプトを実行します。第 3 章「インストール」を参照してください。

ネットワークトラフィック保護を計画する

IWSS を使用してネットワークトラフィック保護を実施するには、別のソリューション (ハードウェア、ソフトウェア、または設定) を導入して、HTTP または FTP トラフィックを IWSS にリダイレクトする必要があります。この項では、次のソリューションについて説明します。

- 15 ページの「クライアントを再設定する」参照
- 17 ページの「レイヤ 4 スイッチを使用する」参照
- 18 ページの「ICAP 対応のプロキシを使用する」参照

クライアントを再設定する

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

FTP クライアントは、宛先サーバの代わりに IWSS と通信して、変更されたハンドシェイクを使って FTP サーバアドレスを提供する必要があります。このトラフィックを処理するには、FTP 検索サービスをスタンドアロンモードへ変更する必要があります。

表 1-1.　クライアントを再設定する場合

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

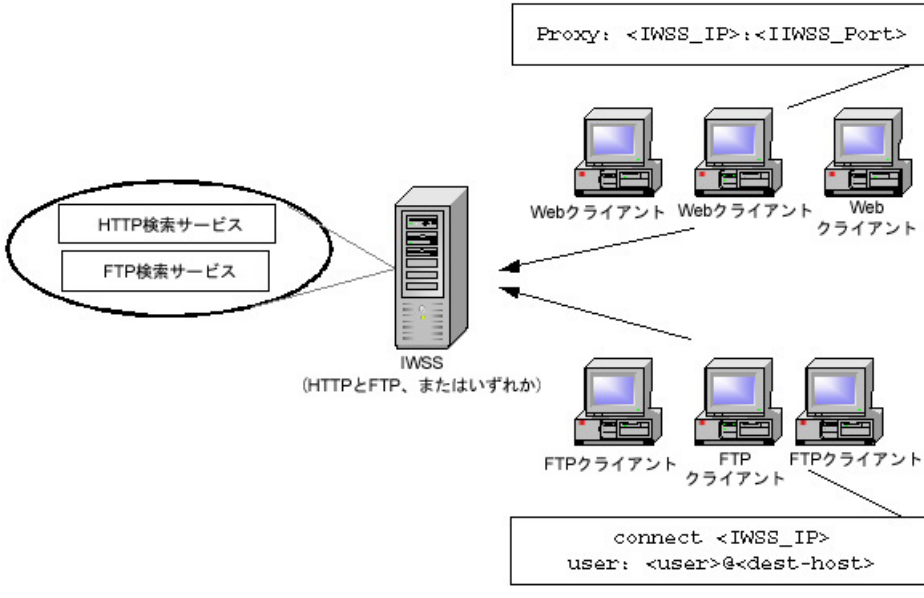

図 1-1.　クライアントを再設定する場合

レイヤ 4 スイッチを使用する

HTTP トラフィックを IWSS にリダイレクトするには、レイヤ 4 スイッチを使用できます。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。IWSS は通常の透過モードで配置する必要があります。

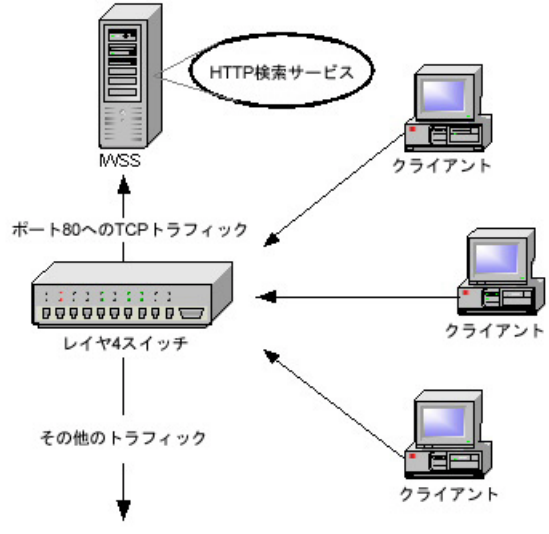

図 1-2.　レイヤ 4 スイッチを使用する場合

表 1-2.　レイヤ 4 スイッチを使用する場合

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

ICAP 対応のプロキシを使用する

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

IWSS 管理コンソールの [管理] → [配置ウィザード] から、「ICAP モード」を設定します。

IWSS を ICAP モードで設定すると、ICAP 準拠のクライアントから送信される要求を処理できます。

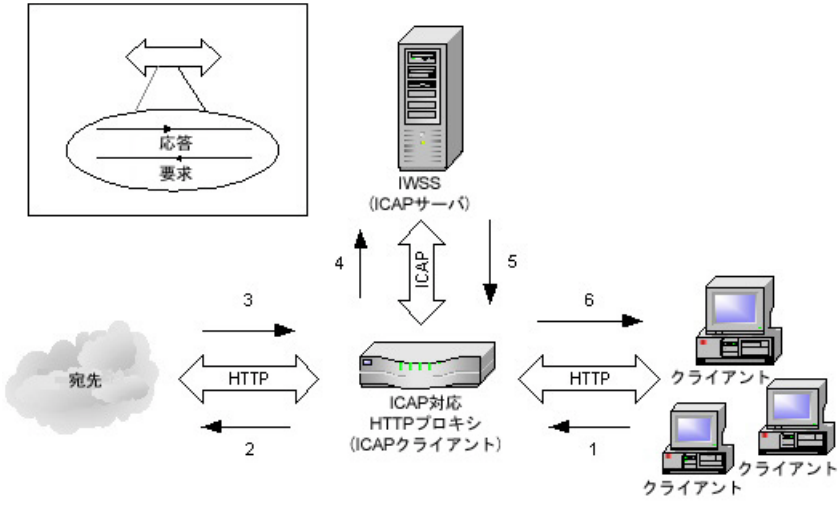

図 1-3.　ICAP 対応のプロキシを使用する場合

表 1-3.　ICAP 対応のプロキシを使用する場合

利点	制限
ICAP により、新規コンテンツおよび必要なコンテンツのみの検索が可能になります。	ICAP リソースのコストが発生します。
検索量が少なく、選択的に実行されるため、パフォーマンスが向上します。	ICAP 管理が必要です。
リソース効率の上昇により、必要な IWSS サーバハードウェア数を削減できます。	ICAP 管理が必要です。

不特定のクライアントから特定の HTTP サーバまたは FTP サーバを保護する

IWSS 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。この場合、IWSS 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。

IWSS 管理コンソールの [管理] - [配置ウィザード] から、「リバースプロキシモード」を設定します。

HTTP 待機ポート

ポート番号 : 保護する HTTP サーバの TCP ポートを指定します。

リバースプロキシモード

保護対象サーバ : 保護する HTTP サーバの IP アドレスを指定します。ポート番号 : 保護する HTTP サーバの TCP ポートを指定します。

HTTP および FTP のサービスフローを計画する

HTTP と FTP の設定はそれぞれ、IWSS の設定、ネットワークの設定、およびネットワークセキュリティに影響します。

HTTP および FTP サービスのフロー計画を作成するには、次のことが必要です。

- 各 IWSS サービスの目的と機能を理解します。
- 各サービスの有効なデータ送信元を決定します。たとえば、HTTP サービスが HTTP ブラウザから要求を直接受信するのか、ICAP プロキシデバイス経由で間接的に受信するのかなどを決定します。
- 各サービスの有効なポートを決定します。たとえば、初期設定では、HTTP サービスにはポート 8080、FTP サービスにはポート 21 が使用されます。ただし、他のアプリケーションやサービスでポート 8080 が使用されている場合は、別のポートを使用するように HTTP サービスを設定する必要があります。
- 各サービスの有効なデータ送信先を決定します。たとえば、HTTP サービスが検証済み要求を直接 Web サイトに送信するのか、上位 HTTP プロキシに送信するのかなどを決定します。

- サービス固有の考慮事項があれば追加します。たとえば、HTTP サービスフローには ICAP デバイスを含めても、FTP サービスフローには含めないなどを検討します。

以上の情報を考慮したうえで、管理者は、想定されるフローを基に IWSS の設定を変更します。

HTTP フローを計画する

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

- HTTP プロキシ
- ICAP デバイス
- 通常の透過
- リバースプロキシ

ICAP デバイスを使用するフローは、ICAP デバイスを使用しないフローと大きく異なります。

使用できるフローは、主に次の 5 つです。

フォワードプロキシ設定の場合 :

- **スタンドアロンモード** — ICAP デバイスを使用せずに IWSS をインターネットに直接接続する場合に、このフローを使用します。初期設定ではこのフローを使用しています。
- **依存モード** — ICAP デバイスを使用せずに IWSS を別の HTTP プロキシ経由でインターネットに接続する必要がある (直接接続できないため) 場合に、このフローを使用します。これは、次の 3 通りの方法で実現できます。
  - プロキシを IWSS の外側に配置するモード
  - プロキシを IWSS の内側に配置するモード (非推奨)
  - 二重プロキシモード
- **通常の透過モード** — このモードは、L4 (負荷分散) スイッチを使用している場合に使用します。

リバースプロキシ設定の場合 :

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

ICAP プロキシ設定の場合 :

- **ICAP プロトコルモード** — ICAP プロトコルフローは、IWSS とともに ICAP デバイスを使用する場合に使用します。

それぞれの設定は、IWSS の設定、ネットワークの設定、およびネットワークセキュリティに影響します。

スタンドアロンモードの HTTP プロキシ

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

注意： IWSS 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は、インターネット接続を設定する必要があります。接続設定では、IWSS デバイスとポート (初期設定では 8080) をプロキシサーバとして使用するようにします。

Web ページ要求は、次の順序で処理されます。

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

表 1-4.　スタンドアロンモードの HTTP プロキシ

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

複数のサーバを使用するスタンドアロンモード

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

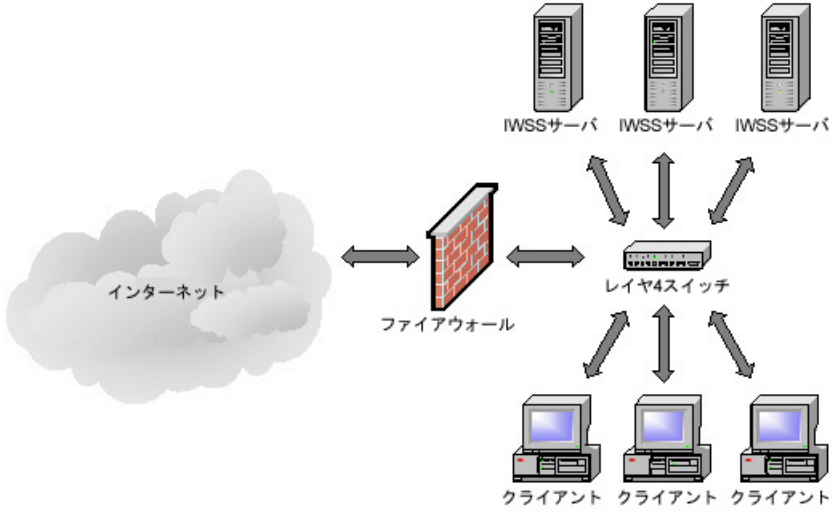

図 1-4.　レイヤ 4 スイッチを使用し、複数の HTTP スタンドアロンサーバに対して IWSS サーバ間で負荷を分散する構成

依存モードの HTTP プロキシ (プロキシを外側に配置する場合)

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

Web ページ要求は、次の順序で処理されます。

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

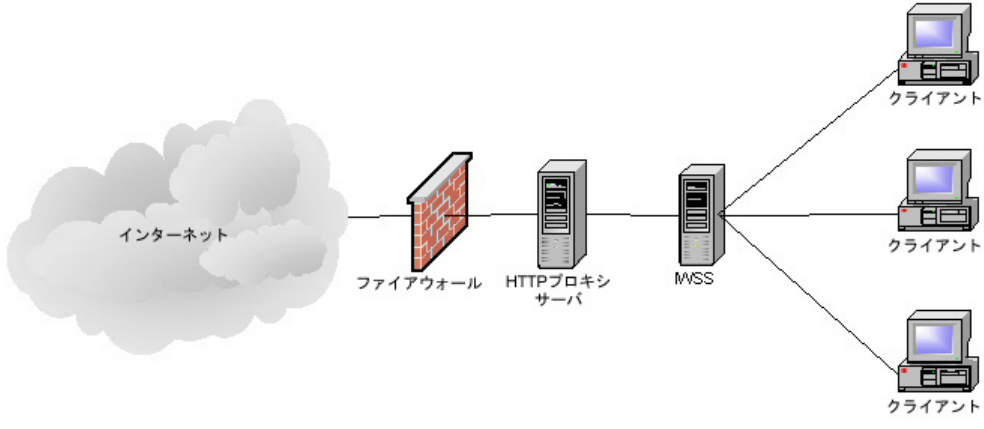

図 1-5. 依存モードの HTTP プロキシ (プロキシを外側に配置する場合)

表 1-5.　依存モードの HTTP プロキシ (プロキシを外側に配置する場合)

利点	制限
プロキシサーバによってタイミングとコンテンツの可用性動作が制御されます。	キャッシュされている応答を含め、すべての応答を IWSS で検索する必要があります。
安全性が高くなります。キャッシュされているオブジェクトに設定変更が反映されます。	
キャッシュ済みオブジェクトのダウンロードを IWSS で待機する必要がありません。	

依存モードの HTTP プロキシ (プロキシを内側に配置する場合)

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

警告：　このフローは、パフォーマンスの向上を期待できる一方で、次の 2 つのリスクがあります。
1. ウイルス感染したデータがキャッシュ内に存在する場合、そのデータがキャッシュで検索されたときにパターンファイルが存在しないと、IWSS HTTP サービスはウイルスの繁殖に対して無防備な状態になります。
2. 同様に、有効なコンテンツに関するポリシーが変更された場合や、キャッシュ内の承認済みユーザ関連データを未承認ユーザが要求した場合、HTTP サービスはそのデータへの後続の不正アクセスに対して無防備になります。

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

Web ページ要求は、次の順序で処理されます。

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

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

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

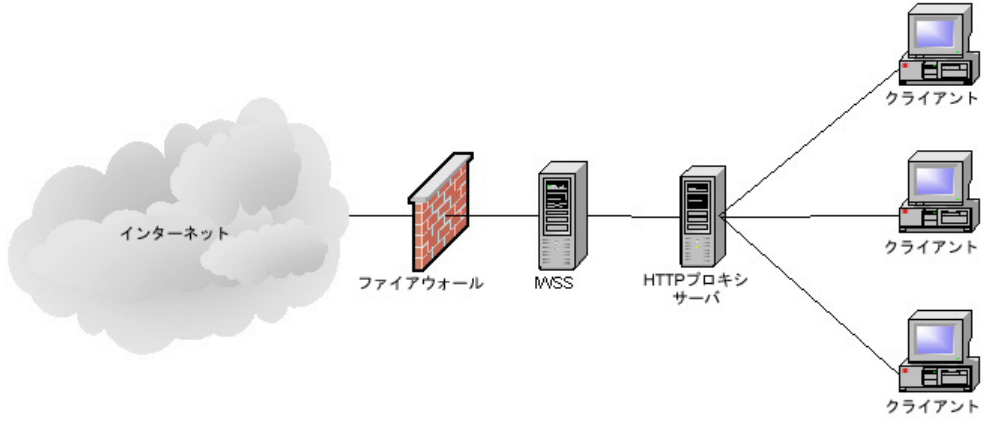

図 1-6. 依存モードの HTTP プロキシ (プロキシを内側に配置する場合)

表 1-6. 依存モードの HTTP プロキシ (プロキシを内側に配置する場合)

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

依存モードの HTTP 二重プロキシ

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

Web ページ要求は、次の順序で処理されます。

1. Web クライアントが 1 つ目のプロキシサーバに要求を送信します。
2. 1 つ目のプロキシサーバが要求を IWSS に転送します。
3. IWSS が URL フィルタおよびブロック機能を使用して要求を検証します。
   - URL が無効な場合、またはブロックされている場合、HTTP サービスは適切な通知を HTTP クライアントに送信し、トランザクションを終了します。
   - URL が有効な場合、HTTP サービスは要求を 2 つ目のプロキシサーバに転送します。
4. 2 つ目のプロキシサーバが処理を実行し、要求をインターネット上の Web サーバに転送します。
5. 接続された Web サーバが、応答 (理想的には Web ページ) を 2 つ目のプロキシサーバに返します。
6. 2 つ目のプロキシサーバがデータをキャッシュし (キャッシュ可能な場合)、応答またはデータを IWSS に配信します。
7. IWSS が、返されたデータ (ウイルス、スパイウェア、ActiveX 対策) に対する処理を実行し、適切な応答またはデータを 1 つ目のプロキシサーバに転送します。
8. 1 つ目のプロキシサーバがデータをキャッシュし (キャッシュ可能な場合)、応答またはデータを HTTP クライアントに配信します。

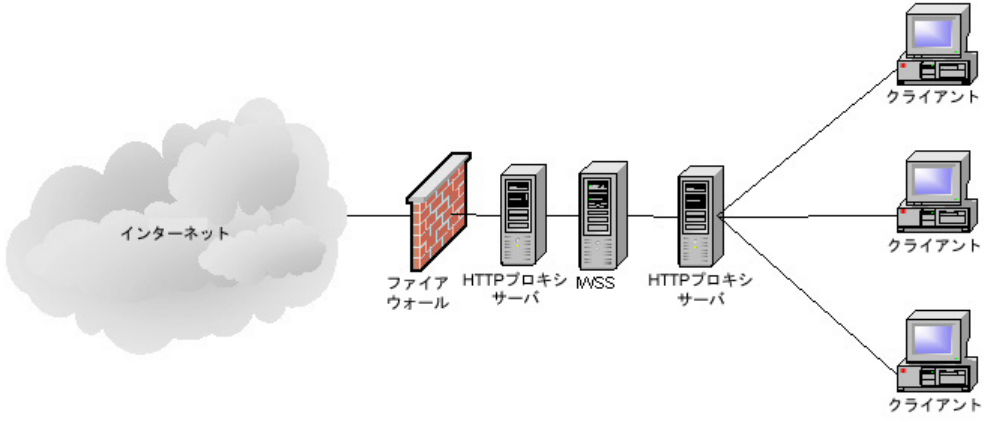

図 1-7.　依存モードの HTTP 二重プロキシ

表 1-7.　依存モードの HTTP 二重プロキシ

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

透過モードの HTTP プロキシ

透過とは、IWSS 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。

IWSS 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。

- FTP over HTTP は使用できません。そのため、FTP 接続を許可しないファイアウォール設定では、ftp:// で始まる URL へのリンクは機能しません。または、ftp:// で始まる URL に接続できても、ファイルが検索されません。
- HTTP 要求にホスト情報が格納されていない場合、旧バージョンの Web ブラウザの中には通常の透過に対応できないものがあります。
- HTTP の初期設定ポートである 80 以外のポートを経由する HTTP 要求が IWSS にリダイレクトされます。SSL (HTTPS) 要求については、通常受け付けられますがコンテンツは検索されません。
- IWSS にはクリーンナップ対象のクライアントの IP アドレスが必要なため、IWSS 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 IWSS 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。これはエンドユーザにとって便利な設定です。また、インターネット接続設定を変更しただけでクライアントがセキュリティポリシーから除外されることが防止されます。

依存モードの HTTP リバースプロキシ

リバースプロキシモードでは、IWSS はプロキシサーバを使用して Web サーバを保護します。HTTP プロキシは、インターネットと Web サーバの間に配置されます。この設定は、Web サーバでクライアントからのファイルのアップロードを受け入れる場合や、複数の Web サーバ間の負荷を分散させることで各 Web サーバの負荷を軽減する場合に有用です。ASP および ISP では、IWSS を HTTP プロキシとして使用して、ウイルスからアップロードトラフィックを保護します。また、複雑な Web サイトを持つ企業では、IWSS を中央アクセス制御点として使用します。

このフローは特に、e コマーストランザクションに使用される Web サイト、インターネット上でデータをやり取りする分散アプリケーション、またはクライアントが遠隔地から Web サーバにファイルをアップロードするような状況に適しています。

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

注意： 管理者は、次の点に注意する必要があります。

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

Web ページ要求は、次の順序で処理されます。

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

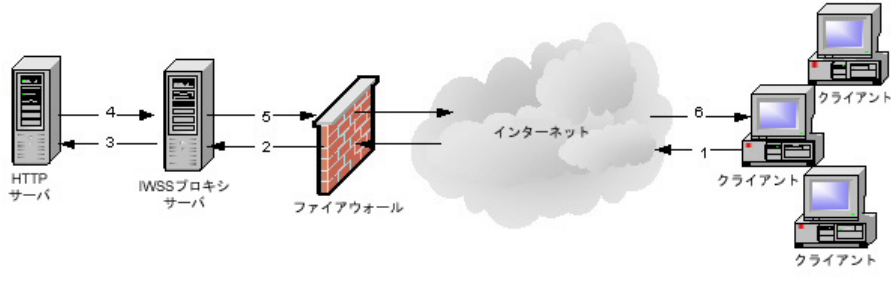

図 1-8.　依存モードの HTTP リバースプロキシ

表 1-8.　依存モードの HTTP リバースプロキシ

利点	制限
IWSS では、すべてのオブジェクトをキャッシュ前に一度検索するだけで済みます。	新しいエンジン、パターン、および設定が、キャッシュされているオブジェクトに反映されません。
	IWSS のアクセスログ機能の効果は低下します。

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

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

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

- **クリーンなデータのキャッシュ** — データがクリーンな場合は、ICAP デバイスでデータをキャッシュします。後続の要求には 4 つの手順のみを実行します。ただし、ICAP は、後続の要求を作成したユーザがデータを閲覧できるかどうか、ユーザが割り当てを超過していないかどうかなどを検証するために、ポリシーをチェックするよう IWSS に依頼する必要があります。
- **IWSS サーバのクラスタ化** — 複数の IWSS サーバを使用する場合は、ICAP デバイスでサーバ間の要求を負荷分散します。これは、受信するページの検索要求を 1 台の IWSS サーバで処理しきれない企業環境にとっては不可欠です。ICAP を使用すると、ICAP デバイスで負荷分散が行われるため、使用可能な IWSS サーバのパフォーマンスを最大限に引き出すことができます。

注意 :　ICAP を使用しない環境でも、複数の IWSS サーバを使用することで、同様の利点を得ることができます。ただし、管理者は、使用可能な IWSS サーバを介してプロキシするように個々のユーザを設定し、各ユーザに割り当てるクライアントとその数を見積もる必要があります。

IWSS を ICAP モードで設定すると、ICAP 準拠のクライアントから送信される要求を処理できます。

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

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

Web ページ要求は、次の順序で処理されます。

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

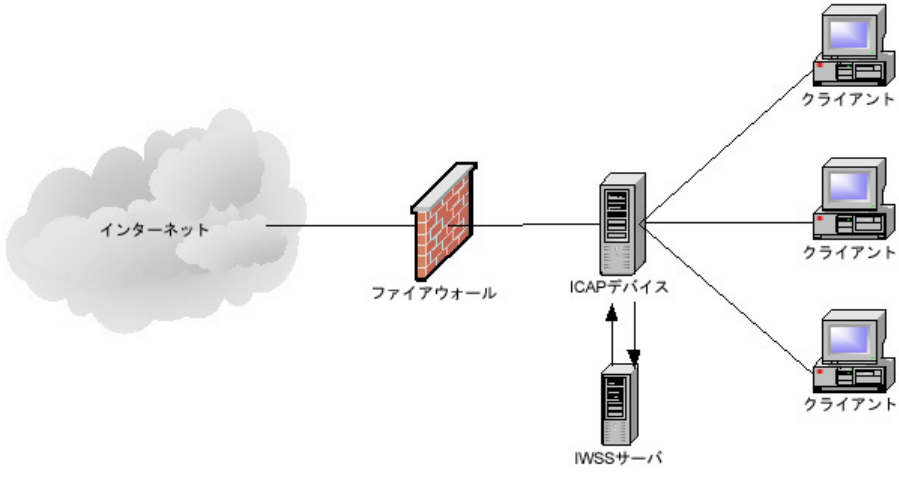

図 1-9. ICAP モードの HTTP プロキシ (1 台の IWSS サーバを配置する場合)

複数のサーバを使用する ICAP モードの IWSS

ネットワーク上にすでにコンテンツキャッシュサーバが存在する場合は、ICAP HTTP ハンドラをインストールすることをお勧めします。次の図は、複数のサーバがある環境で IWSS を ICAP モードでインストールした構成を示しています。ICAP モードでインストールした複数の IWSS サーバが適切に動作するには、対応するパターンファイル、検索エンジンのバージョン、および `/etc/iscan/intscan.ini` ファイルが同一である必要があります。また、すべてのサーバが同じデータベースを使用していることが必要です。

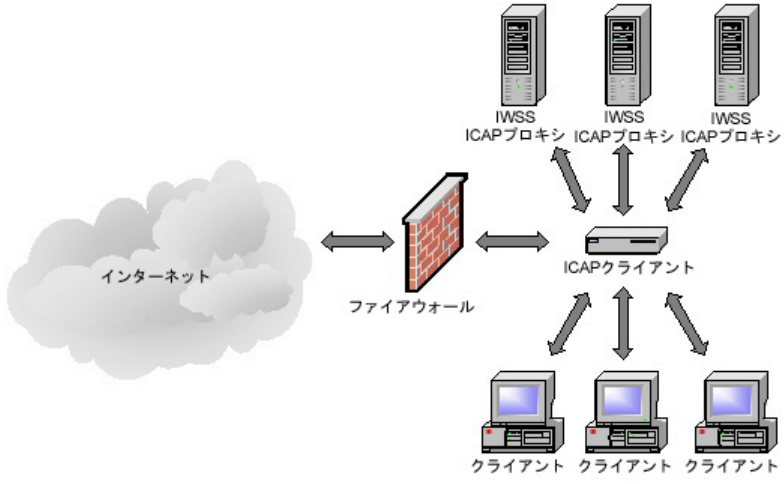

図 1-10. ICAP モードの HTTP プロキシ (複数の IWSS サーバを配置する場合)

表 1-9. ICAP モードの HTTP プロキシ

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

FTP フローを計画する

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

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

スタンドアロンモードの FTP プロキシ

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

FTP スタンドアロンフローの考慮事項は、次のとおりです。

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

このフローを使用するように FTP クライアントを設定するには

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

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

FTP 要求は、次の順序で処理されます。

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

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

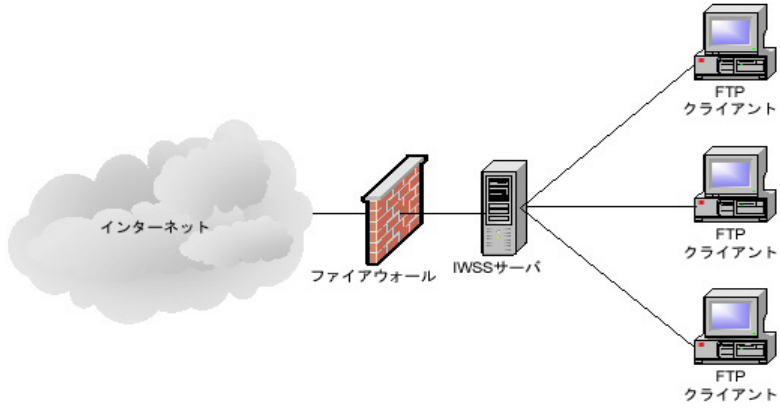

図 1-11.　スタンドアロンモードの FTP プロキシ

依存モードの FTP プロキシ

IWSS FTP は、上位プロキシと要求元クライアントの間に設置した専用コンピュータにもインストールできます。この設定は、アクセスブロック、ログ、フィルタなどの他の FTP 機能を追加して既存の FTP プロキシを補完する場合に使用します。

IWSS の FTP プロキシモードは、図 1-12 に示すように、HTTP サービスの依存モードに類似しています。このモードにすると、他の FTP プロキシサーバによって、余分なホップや余分な処理といったパフォーマンス上の不利な条件が発生します。このため、このモードを使用するのは、組織の方針によりインターネットへの直接接続が IWSS サーバで禁止されている場合のみにしてください。

他の FTP プロキシサーバがストアアンドフォワードを使用している場合、ファイルはそれらのプロキシサーバでいったんダウンロードされてから IWSS FTP サービスに転送されるため、大きなファイルについては、パフォーマンスが劣化する可能性がさらに大きくなります。また、他の FTP プロキシには、進行中のすべての転送を保持するのに十分な空き領域を確保する必要があります。

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

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

FTP 要求は、次の順序で処理されます。

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

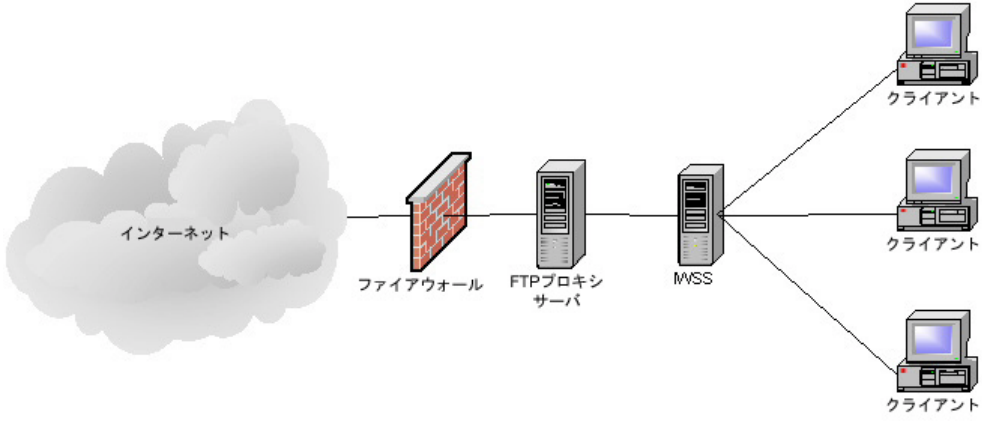

図 1-12.　依存モードの FTP プロキシ

第 2 章

配置について

本章で説明する内容には、次の項目が含まれます。

- 38 ページの「オペレーティングモード」
- 38 ページの「サーバの設置場所を確認する」
- 40 ページの「ネットワーク保護および HTTP/FTP サービスフローを計画する」

オペレーティングモード

InterScan Web Security Suite (以下、IWSS) 6.5 では、プロセス数はハードウェア環境で使われている CPU 数およびメモリサイズに応じて動的に変わります。

各子プロセスは複数のスレッドを生成して、受信した接続を処理します。

サーバの設置場所を確認する

まず、IWSS サーバをインストールする場所を確認します。次に、既存の配置オプションを確認して、要件に適合しないものを除きます。

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

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

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

DMZ を備えた 2 つのファイアウォール

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

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

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

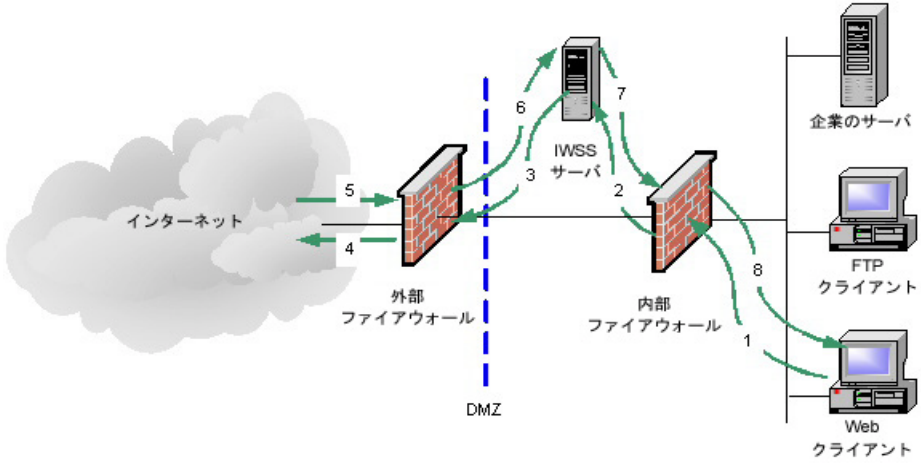

図 2-1. DMZ を備えた 2 つのファイアウォール

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

DMZ を備えていない 1 つのファイアウォール

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

- IWSS サーバは企業の LAN から切り離されていないので、外部のコンピュータと企業の LAN 上のコンピュータとの間のホップは DMZ がある場合より 1 つ少なくなります。この場合、図のように、要求の処理には発信 1 つと着信 1 つの 2 ステップが少なくなります。

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

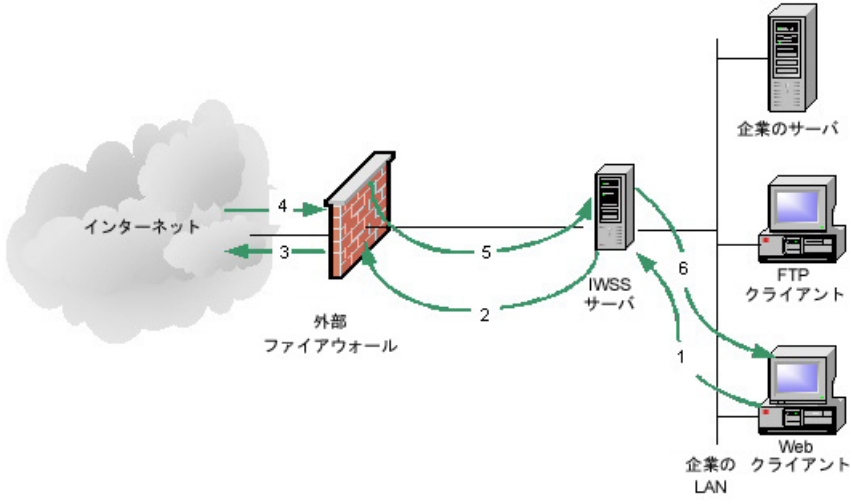

図 2-2. DMZ を備えていない 1 つのファイアウォール

ネットワーク保護および HTTP/FTP サービスフローを計画する

ネットワークトラフィック

IWSS を使用してネットワークトラフィック保護を実施するには、別のソリューション (ハードウェア、ソフトウェア、または設定) を導入して、HTTP または FTP トラフィックを IWSS にリダイレクトする必要があります。このソリューションには、次の事項が含まれます。

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

詳細については、付録 A の 49 ページの「導入の統合」を参照してください。

HTTP および FTP のサービスフロー

HTTP と FTP の設定はそれぞれ、IWSS の設定、ネットワークの設定、およびネットワークセキュリティに影響します。

HTTP および FTP サービスのフロー計画を作成するには、次のことが必要です。

- 各 IWSS サービスの目的と機能を理解します。
- 各サービスの有効なデータ送信元を決定します。たとえば、HTTP サービスが HTTP ブラウザから要求を直接受信するのか、ICAP プロキシデバイス経由で間接的に受信するのかなどを決定します。
- 各サービスの有効なポートを決定します。たとえば、初期設定では、HTTP サービスにはポート 8080、FTP サービスにはポート 21 が使用されます。ただし、他のアプリケーションやサービスでポート 8080 が使用されている場合は、別のポートを使用するように HTTP サービスを設定する必要があります。
- 各サービスの有効なデータ送信先を決定します。たとえば、HTTP サービスが検証済み要求を直接 Web サイトに送信するのか、上位 HTTP プロキシに送信するのかなどを決定します。
- サービス固有の考慮事項があれば追加します。たとえば、HTTP サービスフローには ICAP デバイスを含めても、FTP サービスフローには含めないなどを検討します。

以上の情報を収集したうえで、管理者は、考えられるフローの中からインストールに使用できるものを決定します。

第 3 章

インストール

本章で説明する内容には、次の項目が含まれます。

- 44 ページの「インストール対象コンポーネント」
- 45 ページの「インストール前に関する注意」
- 46 ページの「IWSS をインストールする」
- 47 ページの「インストール後に関する注意」

インストール対象コンポーネント

注意： トレンドマイクロでは、InterScan Web Security Suite (以下、IWSS) を専用のサーバにインストールすることをお勧めします。

インストール時、次のコンポーネントは自動的にインストールされます。

- **メインプログラム** — 管理コンソールおよび IWSS に必要な基本的なライブラリファイルです。
- **HTTP 検索** — ICAP または HTTP プロキシによる HTTP 検索および URL ブロックに必要なサービスです。
- **FTP 検索** — FTP 検索に必要なサービスです。
- **URL フィルタ** — URL フィルタに必要なサービスです (初期設定では有効)。
- **アプレット /ActiveX 対策** — Java アプレットおよび ActiveX コントロールを検索するのに必要なサービスです (初期設定では無効)。
- **情報漏えい対策** — 組織の機密データを含むコンテンツの送信トラフィックを検索するサービスです。
- **SNMP 通知** — SNMP 準拠のネットワーク管理ソフトウェアに SNMP トラップを送信するサービスです。
- **IWSS 用 Trend Micro Control Manager エージェント** — Trend Micro Control Manager (以下、Control Manager) への登録に必要なコンポーネントです。Control Manager (トレンドマイクロの集中管理コンソール) を使用する場合は、このエージェントをインストールする必要があります。
- **IWSS 用 dtas エージェント** — Deep Discovery Analyzer エージェント (初期設定では無効) に必要なファイルです。

インストール前に関する注意

お使いの DNS サーバで IWSS ホスト名を IP アドレスに解決できる必要があります。

これを行うには、次のいずれかの操作を実行します。

- IWSS サーバの A レコードを DNS サーバに追加する
- 適切なエントリを `/etc/hosts` ファイルに追加する

  たとえば、次のエントリを追加します。

  ```
  10.1.1.1  iwsssrv
  ```

ユーザプロセスと開くファイルの最大数を設定する

Red Hat Enterprise Linux 環境によっては、`root` または `iscan` ユーザが実行できるプロセスの最大数と、各プロセスで開くことのできるファイルの最大数が、どちらも `1024` に設定されている場合があります。IWSS が適切に動作するためには、以下の手順で、プロセスの最大数 (`nproc`) と開くことのできるファイルの最大数 (`nofile`) を変更します。

※`iscan` ユーザの設定値は、IWSS インストール時に自動的に追加されます。

1. SSH 接続経由で IWSS サーバに接続します。
2. 次のコマンドを使用して、`/etc/security/limits.conf` ファイルを開きます。

   ```
   vi /etc/security/limits.conf
   ```

3. 次の情報をファイルに追加します。

   ```
   iscan            soft     nproc           11000
   iscan            hard     nproc           11000
   iscan            soft     nofile          4096
   iscan            hard     nofile          4096
   root             soft     nproc           11000
   root             hard     nproc           11000
   root             soft     nofile          4096
   root             hard     nofile          4096
   ```

4. IWSS サーバを再起動します。

SELinux の無効化

1. /etc/selinux/config ファイルに移動して、次の記述を入力します。

   ```
   SELINUX=disabled
   ```

2. 次のコマンドを実行します。

   ```
   # setenforce 0
   ```

注意： IWSS では SELinux をサポートしていません。

IWSS をインストールする

トレンドマイクロでは、IWSS を専用のサーバにインストールすることをお勧めします。IWSS をインストールするには、root 権限で対象サーバにログオンする必要があります。

IWSS のインストールは、製品 CD-ROM から実行するか、または Web サイトからインストールファイルをダウンロードして行います。

製品 CD-ROM からインストールするには

1. IWSS をインストールするサーバの CD-ROM ドライブに CD-ROM を挿入します。
2. 製品 CD-ROM にある製品フォルダからインストールスクリプト「./install_iwss.sh」を実行し、<Enter> キーを押します。

IWSS 6.5 スクリプトをダウンロードして実行するには

1. トレンドマイクロのダウンロードセンターからインストール用のパッケージをダウンロードします。
2. 次を実行して、インストーラのコンポーネントを解凍します。

   ```
   tar xvzf iwss-linux-6.5-XXXX.tgz
   ```

3. IWSS 依存関係チェックスクリプトを含むディレクトリで、「`./check_env.sh`」と入力して <Enter> キーを押します。

   何も出力されない場合は、すべての依存関係パッケージがインストールされています。それ以外の場合は、依存関係パッケージをインストールする必要があります。

4. IWSS インストールファイルを含むディレクトリで、「`./install_iwss.sh`」と入力して <Enter> キーを押します。

5. 表示されるプロンプトを確認します。<Enter> キーを押して選択を受け入れます。

   画面に表示される指示に従ってインストール処理を完了します。

注意： アプリケーション制御のトラフィック統計は、カーネルパッチが適用され、[アプリケーション制御] → [ポリシー] でアプリケーション制御機能が有効になっている場合にのみ表示されます。
カーネルパッチを適用するには
1.「`cd /usr/iwss/bin/`」と入力してパッチディレクトリに移動します。
2. このディレクトリで「`./build_nfq_ko.sh`」と入力します。
3. コマンド「`/etc/iscan/S99ISappd start`」を実行して、すべてのアプリケーション帯域幅統計の監視とレポートを許可します。

インストール後に関する注意

インストール終了後、IWSS Web コンソールを開き、管理者パスワードを変更して、ご使用のシステムのセキュリティが確保されるようにします。詳細については、「管理者ガイド」を参照してください。

Web コンソールへのログイン

IWSS Web コンソールを開くには、次の初期情報が必要です。この情報は大文字と小文字が区別されます。

- ユーザ名 — admin
- パスワード — adminIWSS85

ヒント： パスワードは定期的に変更してください。

次のことにも注意してください。

- トレンドマイクロでは、製品のインストール、登録、およびアクティベートの実行直後に、検索エンジンとウイルスパターンファイルをアップデートすることをお勧めします。
- トレンドマイクロでは、リバースプロキシモードの IWSS 用待機ポート番号は、保護対象サーバのポート番号と同様に 80 を使用することをお勧めします。IWSS をリバースプロキシとして設定する場合は、ポート番号 80 を [HTTP 待機ポート] に指定してください。

付録 A

導入の統合

この付録では、次の項目について説明します。

- 50 ページの「ICAP デバイスとの連携」
  - 50 ページの「IWSS ICAP のインストール後の設定」
  - 55 ページの「「X-Virus-ID」ヘッダと「X-Infection-Found」ヘッダを有効化する」
- 56 ページの「分散環境における IWSS」
- 57 ページの「LDAP との連携」
- 59 ページの「HTTP サーバを保護する」
- 60 ページの「FTP サーバを保護する」

ICAP デバイスとの連携

IWSS ICAP のインストール後の設定

インストールした InterScan Web Security Suite (以下、IWSS) を ICAP 環境で使用したい場合、以下のインストール後設定の手順を実行します。

ICAP 1.0 準拠のキャッシュサーバを設定する

ICAP サーバと通信できるように ICAP クライアントを設定します。

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

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

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

Web ブラウザのアドレスバーに「http://{ キャッシュサーバの IP アドレス }:8081」と入力して管理コンソールにログオンします。ここでは、初期設定の管理ポートとして 8081 を指定します。たとえば、最初のインストール時に設定した IP アドレスが「123.123.123.12」の場合は、Web ブラウザに URL「http://123.123.123.12:8081」を入力します。

1. [Management] を選択します。入力画面が表示されたら、ログオンユーザ名とパスワードを入力します。
2. 左側のメニューで [ICAP] を選択し、[ICAP Services] タブを選択します。
3. [New] をクリックします。[Add ICAP Service] 画面が表示されます。
4. [ICAP service name] フィールドに、サービス名を英数字で入力します。[OK] をクリックします。
5. 新しく追加した ICAP サービス名を選択し、[Edit] をクリックします。[Edit ICAP Service { サービス名 }] 画面が表示されます。
6. 次の情報を入力または選択します。
   a. ICAP バージョン番号。ここでは [1.0] を選択します。
   b. ウイルス検索サーバのホスト名または IP アドレスを含むサービス URL、および ICAP ポート番号。初期設定では、ICAP ポート番号は 1344 です。
      - 応答モードの場合

`icap://{ICAP サーバの IP アドレス }:1344`

- 要求モードの場合

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

c. 最大接続数 (1 ～ 65,535 の範囲)。初期設定値は「5」です。

d. 接続タイムアウト。Blue Coat Port 80 Security Appliance がウイルス検索サーバからの応答を待つ最大秒数です。60 ～ 65,535 の値を指定できます。初期設定値は 70 秒です。

e. サポートされた方法の種類を選択します (応答モードまたは要求モード)。

f. 初期設定のプレビューサイズ (0 バイト) を使用します。

g. ICAP サーバから設定を取得するには、[Sense settings] をクリックします (推奨)。

h. 状態チェックの対象として ICAP サービスを登録する場合は、[Health Check Options] の [Register] ボタンをクリックします。

7. [OK] をクリックし、次に [Apply] をクリックします。

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

---

8. 応答モードまたは要求モードのポリシーを追加します。

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

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

応答モードのポリシーを追加するには

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

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

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

d. メニューバーで [Edit] → [Add Web Content Policy] の順に選択します。[Add New Policy Table] 画面が表示されます。

e. [Select policy table name] にポリシー名を入力します。[OK] ボタンをクリックします。

f. [Action] 列で [Bypass ICAP Response Service] を右クリックし、[Set] をクリックします。[Add Object] 画面が表示されます。[New] をクリックし、[Use ICAP Response Service] を選択します。[Add ICAP Service Action] 画面が表示されます。

g. [ICAP Service/Cluster Names] のリストから ICAP サービス名を選択します。[On communication error with ICAP service] で [Deny the request] オプションを選択します。[OK] をクリックし、もう一度 [OK] をクリックします。

h. [Install Policies] をクリックします。

要求モードのポリシーを追加するには

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

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

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

d. メニューバーで、[Edit] → [Add Web Access Policy] の順に選択します。[Add New Policy Table] 画面が表示されます。

e. [Select policy table name] にポリシー名を入力します。[OK] ボタンをクリックします。

f. [Action] 列で [Deny] を右クリックし、[Set] をクリックします。[Add Object] 画面が表示されます。[New] をクリックし、[Use ICAP Request Service] を選択します。[Add ICAP Service Action] 画面が表示されます。

g. [ICAP Service/Cluster Names] のリストから ICAP サービス名を選択します。[On communication error with ICAP service] で [Deny the request] オプションを選択します。[OK] をクリックし、もう一度 [OK] をクリックします。

h. [Install Policies] をクリックします。

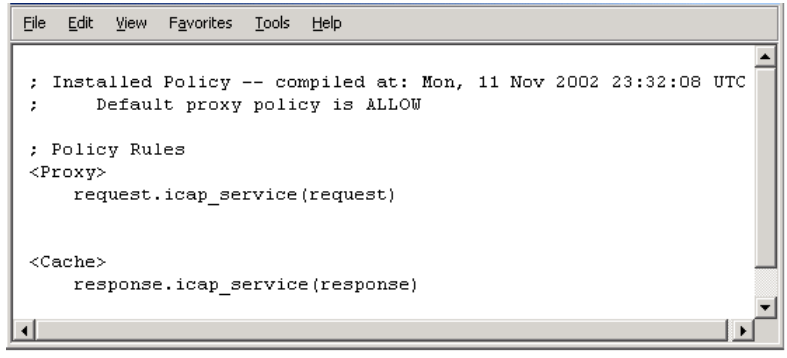

図 A-1. 要求モードと応答モードの ICAP サービスを設定します。現在のポリシーを確認するには、[Policy] 画面に移動し、[Policy Files] タブをクリックして、[Current Policy] をクリックします。

Cisco CE ICAP サーバについて ICAP を設定する

Cisco CE ICAP サーバについて ICAP を設定するには

IWSS は、Cisco ICAP サーバ (CDN) 5.1.3, b15 に対応しています。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. 「`config`」と入力して、設定モードに切り替えます。
3. 「`ICAP`」と入力します。ICAP 関連のすべてのコマンドが一覧表示されます。
4. 次のように入力して応答変更サービスを作成します。

   `icap service { 応答モードサービス名 }`

   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が一覧表示されます。次のコマンドを入力します。

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

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

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

   `enable` (ICAP 複数サーバ設定の有効化)
5. 「`exit`」と入力します。
6. 次のように入力して、要求変更サービスを作成します。

```
icap service { 要求モードサービス名 }
```

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

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

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

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

`enable` (ICAP 複数サーバ設定の有効化)

7. 「`exit`」と入力します。
8. その他の設定の手順として、次のように入力します。

   `icap append-x-headers x-client-ip` (レポートの X クライアントヘッダの有効化)

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

   `icap rescan-cache ISTag-change` (アップデートの ISTAG 再検索の有効化)

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

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

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

ウイルス検索サーバクラスタを設定する

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

管理コンソールを使用してクラスタを設定するには

1. [Management] を選択します。入力画面が表示されたら、ログオンユーザ名とパスワードを入力します。
2. 左側のメニューで [ICAP] を選択し、[ICAP Clusters] タブを選択します。
3. [New] をクリックします。[Add ICAP Cluster] 画面が表示されます。
4. [ICAP cluster name] に、クラスタ名を英数字で入力します。[OK] をクリックします。
5. 新しい ICAP クラスタ名を選択し、[Edit] をクリックします。[Edit ICAP Cluster name] 画面が表示されます。
6. [New] をクリックして、ICAP サービスをクラスタに追加します。[Add ICAP Cluster Entry] 画面が表示されます。選択リストには、クラスタに追加できるすべてのサービスが一覧表示されます。サービスを選択して、[OK] をクリックします。

7. 新しく追加した ICAP クラスタエントリを選択して、[Edit] をクリックします。[Edit ICAP Cluster Entry { エントリ名 }] 画面が表示されます。[ICAP cluster entry weight] フィールドで 0 ～ 255 の範囲で重み付けを割り当てます。[OK] をクリックし、もう一度 [OK] をクリックしてから [Apply] をクリックします。

クラスタ設定またはエントリを削除する

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

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

管理コンソールを使用してクラスタ設定を削除するには

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

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

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

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

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

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

パラメータ値の詳細については、次を参照してください。

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

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

1. IWSS 管理コンソールのメインメニューから [管理] → [配置ウィザード] → [ICAP モード] の順に選択します。
2. [ICAP 設定] 画面で、次のいずれかを選択します。
   - 「X-Virus-ID」ICAP ヘッダを有効にする
   - 「X-Infection-Found」ICAP ヘッダを有効にする

分散環境における IWSS

IWSS は、分散システムを構成する一部として設計されており、設定によってさまざまなネットワーク接続を確立できます。

管理者は、次の点を確認する必要があります。

- 必要なチャネルがブロックされていないこと
- すべてのチャネルに十分なスループットがあること
- サーバが使用するソフトウェアは、サポートしているバージョンであること
- サーバのパフォーマンスが十分であること

接続の要件と特性

以下の表 A-1 に、必要な接続とその特性を示します。

表 A-1. 必要な接続と特性

接続するコンポーネント	トラフィック : タイプおよびデータ量	接続が切断された場合
クライアント	実際のネットワークで測定する必要があります。	保護なし
LDAP サーバ (設定されている場合)	**タイプ** : LDAP **データ量** : 中	すでに開始されているサービスでは、キャッシュ内のデータが使用されます。 新しいサービスは開始されません。

表 A-1.　必要な接続と特性 (続き)

接続するコンポーネント	トラフィック : タイプおよびデータ量	接続が切断された場合
トレンドマイクロのアップデートサーバ	**タイプ** : HTTP および HTTPS **データ量** : 10 ～ 50MB/ 日	IWSS コンポーネントは時間内にアップデートできません。
Web レピュテーション	**タイプ** : HTTP **データ量** : 個別のアクセスによって異なります。	すでに開始されているサービスでは、キャッシュ内のデータが使用されます。 サービスは開始されません。ユーザは要求した URL にアクセスできます。

スループットと可用性の要件

管理者は、IWSS の可用性の要件を決定する必要があります。

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

LDAP との連携

複数の LDAP サーバによるマルチドメインのサポート

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

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

IWSS Web コンソールで LDAP 機能を設定するには

1. [管理] → [一般設定] → [ユーザの識別] の順に選択します。
2. LDAP 接続に関する必要な情報を入力します。

3. [接続のテスト] をクリックし、LDAP の設定と接続を確認します。テストが成功すると、成功を示すメッセージが表示されます。
4. [保存] をクリックして、設定を保存します。

詳細については、「管理者ガイド」の第 6 章「ポリシーとユーザ識別方法」を参照してください。

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

標準認証では、ユーザアカウントとパスワードを指定するための標準の 401 認証ダイアログボックスを提供します。クライアントコンピュータが Microsoft Active Directory 内の Windows デスクトップである場合は、透過的な認証が適用されます。キャプティブポータルは、ユーザを識別するための Web ベースの認証ページを表示します。キャプティブポータル認証にはゲストポリシーを適用できます。キャプティブポータルでのみ使用可能な NAT およびターミナルサーバ環境でユーザ識別を実現するために、Cookie モードが存在します。

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

この機能を使用するには、Web コンソールの [管理] → [一般設定] → [ユーザの識別] 画面で、IWSS が使用するメイン LDAP サーバを指定する必要があります。その際、指定したグローバルカタログ対応 Active Directory サーバが、初期設定の LDAP 通信ポート 389 ではなく、ポート 3268 で通信できるように設定します。

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

ヒント： グローバルカタログを有効にしたルート Active Directory サーバを検索できるように設定し、ポリシーの適用時には、ユニバーサルグループを使用してグループをネストすることをお勧めします。この設定はグローバルカタログで確認できます。また、Active Directory にも表示されます。詳細については、Microsoft サポート (http://support.microsoft.com/kb/231273) を参照してください。

HTTP サーバを保護する

HTTP サーバを保護している場合は、配置ウィザードを使用して、リバースプロキシモードで IWSS を配置します。

IWSS をリバースプロキシモードで配置するには

1. [管理] → [配置ウィザード] に移動します。

   配置ウィザードが表示されます。

   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. [リバースプロキシモード] → [次へ] の順にクリックします。
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. [SSL ポートを有効にする] を選択します。必要に応じて [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] をクリックしていきます。
6. [送信] ボタンをクリックします。

   注意： HTTP/HTTPS 環境でのリバースプロキシ設定を単純化するため、IWSS は、配信ウィザードの設定で指定されているポートで外部からの (HTTPS) 接続を待機し、このトラフィックを保護対象サーバの HTTP ポートに転送します。

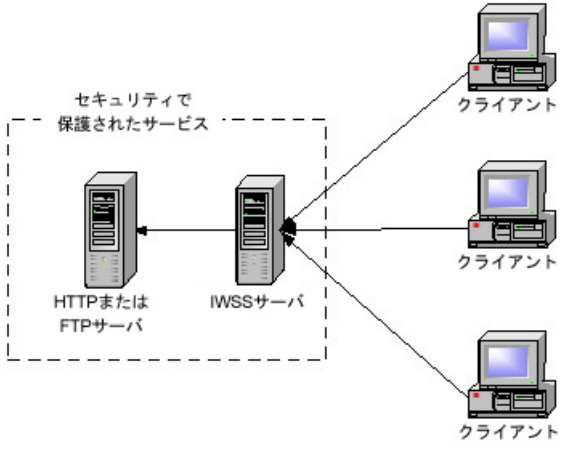

図 A-2.　専用サーバの保護

FTP サーバを保護する

FTP サーバを保護している場合は、FTP プロキシを使用するように IWSS を設定します。

リバースプロキシモードで FTP 検索を設定するには

1. IWSS 管理コンソールを開いて、[FTP] → [設定] → [一般] の順にクリックします。
2. [プロキシ設定] で [FTP プロキシを使用] をクリックし、FTP サーバの IP アドレスまたはホスト名とポート番号を入力します。
3. [保存] をクリックします。

付録 B

調整とトラブルシューティング

この付録では、次の項目について説明します。

- 62 ページの「パフォーマンスの調整」
  - 62 ページの「URL フィルタ」
  - 62 ページの「LDAP パフォーマンスの調整」
  - 64 ページの「OS の調整」
- 65 ページの「トラブルシューティング」
  - 65 ページの「トラブルシューティングのヒント」
  - 66 ページの「テクニカルサポートに問い合わせる前に」
  - 66 ページの「インストールに関する問題」
  - 66 ページの「一般的な機能に関する問題」

パフォーマンスの調整

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

URL フィルタ

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

IWSS では、Web レピュテーションのフィードバック、オプションの URL フィルタモジュール、またはこれら両方を使用して URL アクセスを制御できます。Web レピュテーションと URL フィルタモジュールの組み合わせは、複合型脅威に対する IWSS の保護ソリューションです。

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

詳細については、「管理者ガイド」の第 7 章「HTTP 検索の設定」を参照してください。

LDAP パフォーマンスの調整

IWSS でユーザ / グループ名の識別方法 (LDAP) を使用する場合、HTTP プロキシのパフォーマンスは、LDAP ディレクトリサーバの応答性に依存します。場合によっては、HTTP 要求が発生するたびに、LDAP クエリを実行して対象ユーザの本人性を確認し、さらに別の LDAP クエリを実行して、そのユーザのグループメンバーシップ情報を取得しなければなりません。このため、IWSS と LDAP サーバ間のクエリが増加し、LDAP サーバ自体の負荷が増大します。

LDAP 内部キャッシュ

必要な LDAP クエリ量を減らすために、IWSS 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 — このキャッシュには、グループメンバーシップ情報を格納できます。ローカルサーバと LDAP サーバの初期設定の同期間隔は 24 時間です。

クライアント IP アドレスとユーザ ID 間のキャッシュ — このキャッシュは、クライアント IP アドレスと同じ IP アドレスで最近認証されたユーザを関連付けます。過去に認証された要求と同じ IP アドレスから発行された要求は、新しい要求が前回の認証から設定可能な期間内に発行された場合であれば、同じユーザのものであると見なされます。ただし、この期間内は、クライアントの IP アドレスとユーザを IWSS が 1 対 1 で特定できることが必要な条件となります。したがって、クライアントと IWSS 間にプロキシサーバや NAT がある環境や、DHCP によってクライアント IP が頻繁に割り当て直される環境では、このキャッシュを使用できません。

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。

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

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

クライアント IP アドレスとユーザ ID の関連付けキャッシュの期限を設定するには、次の手順を実行します。

1. IWSS 管理コンソールを開きます。
2. [管理] → [一般設定] → [ユーザの識別] の順にクリックします。
3. [グローバルな認証キャッシュの設定] で [固定の TTL] または [前回アクティブな TTL] を選択します。テキストボックスに期限を入力します。

- 固定の TTL

  レコードは、[expire_interval] パラメータで設定されている期限まで利用されます。その生存期間が期限に達した場合に削除されます。レコードの期限は次のように計算されます。
  期限 = レコード生成時刻 + 固定の TTL

- 前回のアクティブな TTL

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

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

LDAP 認証が有効なときは冗長ログを無効にする

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

冗長ログと LDAP を両方とも有効にすると、ユーザ認証情報とグループメンバーシップ情報がログフォルダ内の HTTP ログに記録されます。内部トラフィック量やユーザが属しているグループの数によっては、1 人のユーザにつき数百行のログが書き込まれるので、ディスク領域が大量に消費されます。冗長ログを使用すると、頻繁に OS から I/O 操作が発行され、その間はサービスがビジー状態になりやすくなります。これにより、サービスが HTTP 要求に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。HTTP トラフィックが過度に集中する環境では、IWSS を冗長モードで起動したとき、大きな遅延が発生する可能性があります。

OS の調整

ネットワークトラフィック負荷の高い環境で IWSS を効率的に実行するため、IWSS のインストールプロセスによって次のシステムカーネルパラメータに自動的に上書き処理されます。

キー	OS の初期設定値	IWSS インストール後
net.ipv4.tcp_tw_recycle	0	1
net.ipv4.tcp_tw_reuse	0	1
net.ipv4.tcp_max_tw_buckets	262144	720000
net.ipv4.tcp_fin_timeout	60	30
net.ipv4.tcp_timestamps	1	0
net.ipv4.tcp_sack	1	1
net.ipv4.tcp_dsack	1	0
net.ipv4.tcp_fack	1	0
net.ipv4.tcp_window_scaling	1	0
net.ipv4.tcp_syn_retries	5	3
net.ipv4.tcp_synack_retries	5	3
net.ipv4.tcp_rfc1337	0	1
net.ipv4.tcp_ecn	2	0

net.ipv4.tcp_max_syn_backlog	2048	4096
net.ipv4.ip_local_port_range	32768 61000	1024 65535
net.ipv4.tcp_rmem	4096 87380 4194304	4096 262144 4194304
net.ipv4.tcp_wmem	4096 16384 4194304	4096 262144 4194304
net.ipv4.tcp_mem	275232 366976 550464	8388608 8388608 8388608
kernel.sysrq	0	1
kernel.panic	0	1

パフォーマンスを高めるため、さらに IWSS インストールスクリプトによって、`/etc/security/limits.conf` ファイルで、iscan ユーザが実行できるプロセスの最大数が `11000`、開くことのできるファイルの最大数が `4096` に変更されます。

注意： commonlog モジュールは `/proc/sys/net/core/somaxconn` のカーネルパラメータに大きく依存しています。commonlog 関連のサービスが正しく機能するように、IWSS インストールスクリプトによって、このパラメータの値が初期設定の 128 から 1024 に調整されます。

トラブルシューティング

トラブルシューティングのヒント

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

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

  解決策：

  - ODBC 接続とデータベースサーバを確認して、再試行してください。

- **問題**：IWSS 管理コンソールに次のような認証エラーメッセージが表示される。

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

解決策:

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

テクニカルサポートに問い合わせる前に

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

インストールに関する問題

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

1. IWSS のバージョン番号とビルド番号
2. インストール中に発生したエラーのスクリーンショット
3. 問題が発生したインストールまたはアンインストールの段階
4. `/tmp/install.log` インストールログファイル

一般的な機能に関する問題

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

1. IWSS の現在の状態を示すシステムファイル。

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

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

   `Info_YYYYMMDD_999999.tar.gz`

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

システムファイルには次の情報が保存されます。

- **IWSS 情報** — IWSS の製品バージョン、エンジンバージョン、ビルド番号、現在のパターンファイル (入手可能な場合)、IWSS HotFix、および Service Pack 情報。製品設定および他製品との連携設定もこの情報に含まれます。
- **IWSS/ システムログ** — IWSS ログ、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な場合)、コアダンプファイル `/etc/iscan/CDT_Config.ini` ([SystemLog] セクションに「CoreDump=1」が設定されている)。
- **システム / ネットワーク情報** — ハードウェア構成、OS、ビルド、システムリソースの状態、インストールされているその他のアプリケーション、ネットワーク情報。
- **設定ファイル** — Trend Micro Control Manager エージェントや MCP エージェントなど調査に必要な設定情報

2. コアファイル

   `/etc/iscan/intscan.ini` で「`only_stacktrace_on_fault=yes`」が設定されている場合、まず、以下の 1 番目のディレクトリにバックトレースファイルが作成され、その後、2 番目のディレクトリに移動されます。

   `/etc/iscan/coredumps`

   `/etc/iscan/UserDumps`

   `/etc/iscan/intscan.ini` で「`only_stacktrace_on_fault=no`」が設定されている場合は、以下のディレクトリにフルコアダンプファイルが作成されます。

   `/etc/iscan/`

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

3. 問題が発生した日のログファイル。
   - 問題が発生した日のすべてのログファイル (初期設定では、ログは `/etc/iscan/log` に保存されます)。
   - `/etc/iscan/intscan.ini` ファイルの `[ftp]` セクション、`[http]` セクション、および `[notification]` セクションで、「`verbose=1`」と設定します。

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

HTTP デーモン：

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

FTP デーモン：

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

通知：

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

4. Web コンソールで [管理] → [システムアップデート] タブの順に選択し、この画面のスクリーンショットを撮ります。
5. IWSS のバージョン番号を記録します。
6. URL サンプル (必要な場合) または、アクセス時に問題が発生する URL のアドレスを取得します。
7. 可能であれば、ethereal や wireshark または tcpdump を使用して、失敗したトランザクションのパケットをキャプチャします。

付録 C

追加テスト

この付録では、次の項目について説明します。

- 70 ページの「アップロード検索をテストする」
- 71 ページの「FTP 検索をテストする」
- 72 ページの「URL ブロックをテストする」
- 73 ページの「ダウンロード検索をテストする」
- 74 ページの「URL フィルタをテストする」
- 75 ページの「スパイウェア検索をテストする」
- 76 ページの「フィッシング対策をテストする」
- 77 ページの「Java アプレット /ActiveX 対策をテストする」
- 78 ページの「情報漏えい対策をテストする」

動作テストの前に、Web クライアントの HTTP プロキシが InterScan Web Security Suite (以下、IWSS) を経由するように設定する必要があります。

- スタンドアロンモードの場合、Web クライアントの HTTP プロキシが IWSS をポイント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。
- 上位プロキシを有効にしている場合、Web クライアントの HTTP プロキシが IWSS をポイント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。IWSS コンソールを開き、左側のメニューから [管理] → [配置ウィザード] を選択して、[上位プロキシを有効にする] を有効にします。プロキシアドレスとポート番号を入力します。

アップロード検索をテストする

Web ベースメールの添付ファイルに対するウイルス検索をテストすることをお勧めします。

注意： Web ベースメールが HTTPS を使用している場合には、HTTPS 復号化機能が有効な場合にのみウイルス検索が行われます。

Web ベースメールの添付ファイルに対するウイルス検索をテストするには

1. IWSS 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] チェックボックスをオフにして、[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をダウンロードします。

   `http://www.eicar.org/85-0-Download.html`
3. 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. IWSS 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. インターネットメールサービスなどを使用し、ダウンロードしたテストウイルスをメールに添付して送信します。以下のようなメッセージがブラウザに表示されます。

図 C-1. EICAR テストウイルスを検出したことを示す警告画面

FTP 検索をテストする

スタンドアロンモードで FTP ウイルス検索をテストするには、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 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/85-0-Download.html`

2. FTP プロキシとして動作する IWSS を介して FTP サーバにアクセスします。
   たとえば、次のような IP アドレスを想定します。IWSS FTP プロキシサーバ (`10.2.10.2`)、FTP サーバ (`10.2.10.10`)
   コマンドラインプロンプトを開いて、次のように入力します。

   ```
   ftp 10.2.10.2
   ```

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`」、FTP サーバの IP アドレスが「`10.2.10.10`」の場合は、「`anonymous@10.2.10.10`」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. IWSS FTP プロキシの設定が適切であれば、IWSS により次のようなメッセージが表示されます。

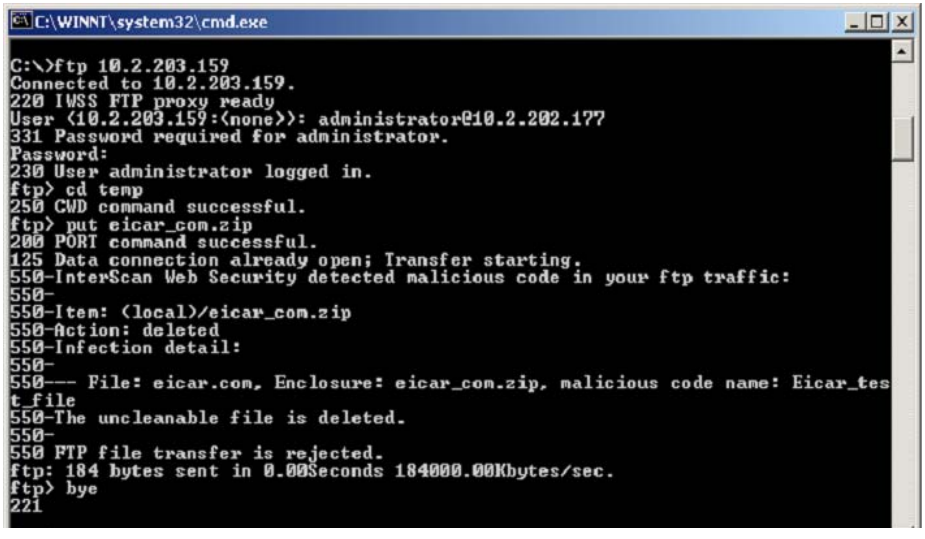

図 C-2. eicar_com.zip でウイルスが検出されたことを示す警告メッセージ

URL ブロックをテストする

URL ブロックをテストするには

1. IWSS コンソールを開き、メインメニューから [HTTP] → [URL アクセス設定] → [グローバル URL ブロック] の順に選択して、[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。
2. [キーワード] にキーワード文字列を入力し、[前方一致]、[部分一致]、[完全一致] のいずれかのオプションを選択します。
3. [ブロックする] をクリックし、[保存] をクリックします。

4. Web ブラウザを開き、ブロックした Web サイト、キーワードを含む URL、または完全一致文字列へのアクセスを試みます。以下のようなメッセージがブラウザに表示されます。

Trend Micro InterScan Web Securityイベント

URLがブロックされました

このWebサイトへのアクセスは、ITのURLアクセス管理ポリシーによってブロックされました。

イベント詳細:
URL: http://example.com/
理由: 管理者による定義

誤ってこのURLがブロックされたと思われる場合は、IT担当者に問題を解決するよう依頼してください。

図 C-3. URL ブロックの警告メッセージ例

ダウンロード検索をテストする

HTTP または FTP over HTTP を使用してダウンロードする場合に、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のダウンロードを試みます。

`http://www.eicar.org/anti_virus_test_file.htm`

Trend Micro InterScan Web Securityイベント

HTTP/HTTPSダウンロードファイルがブロックされました

このURLから不正プログラムが検出されたため、ITのHTTP/HTTPS検索ポリシーによってこのWebサイトのコンテンツへのアクセスがブロックされました。

イベント詳細:
URL: http://www.eicar.org/download/eicar_com.zip
処理: 削除

詳細:
ファイル: eicar.com
エンクロージャ: eicar_com.zip
不正プログラム: **Eicar_test_file**
ウイルス駆除できないファイルは削除されました。

誤ってこのファイルがブロックされたと思われる場合は、IT担当者に問題を解決するよう依頼してください。

図 C-4. ウイルス検出の警告メッセージ例

あるクライアントが感染ファイルをダウンロードしようとした場合、IWSS の初期設定では、他のクライアントがそのサイトにアクセスしようとしても、4 時間はブロックされます。他のクライアントがそのウイルスを含む同一 URL に続いてアクセスしようとすると、ユーザには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 (単位は時間) 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 `infected_url_block_length` パラメータを編集します。

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

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

URL フィルタをテストする

URL フィルタのテストに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. IWSS コンソールを開き、[HTTP] → [URL フィルタ] → [ポリシー] をクリックします。
2. [URL フィルタのグローバルポリシー] をクリックし、[除外設定] タブで、「承認する URL リスト」として分類されている Web サイトカテゴリを確認します。
3. メインメニューから [HTTP] → [URL フィルタ] → [ポリシー] の順に選択します。
4. [URL フィルタを有効にする] 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. [URL フィルタのグローバルポリシー] をクリックし、業務時間中と業務時間外に適切なカテゴリがブロックされていることを確認します。
6. ブラウザを開き、禁止カテゴリに指定されている任意のサイトにアクセスします。

図 C-5. URL フィルタが適切に設定されている場合に表示されるメッセージ

スパイウェア検索をテストする

スパイウェア検索をテストするには、次の手順を実行します。

スパイウェア検索をテストするには

1. IWSS コンソールを開き、[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] の順に選択します。
2. [スパイウェア検索ルール] タブをクリックし、検索するスパイウェアの種類を選択します。
3. [処理] タブをクリックします。
4. [2 次処理] フィールドで、実行する処理 ([削除]、[隔離]、または [放置]) を選択します。
5. [保存] をクリックします。

6. スパイウェアを正常に検出すると、次のようなメッセージが表示されます。

図 C-6. [削除] 処理を指定した場合のスパイウェア検出メッセージ例

フィッシング対策をテストする

フィッシング対策をテストするには、次の手順を実行します。

フィッシング対策をテストするには

1. IWSS コンソールを開き、[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] の順に選択します。
2. [Web レピュテーションルール] タブで [フィッシング検索を含める] を選択します。
3. [保存] をクリックします。

4. フィッシングサイトを正常に検出すると、次のようなメッセージが表示されます。

図 C-7. フィッシングサイトの検出を知らせるメッセージの例

Java アプレット /ActiveX 対策をテストする

Java アプレットと ActiveX コントロールは、多くの Web ページでインタラクティブなコンテンツやアプリケーションを表示するために使用されています。インストール状態をテストする 1 つの方法は、すべてのアプレットと ActiveX コントロールをブロックするグローバルポリシーを一時的に設定し、それらを使用している Web サイトを開くことです。これにより、アプレットやオブジェクトがブロックされることを確認できます。

Java アプレット /ActiveX 対策をテストするには

1. メインメニューで [HTTP] → [アプレット /ActiveX 対策] → [ポリシー] の順に選択します。
2. [アプレット /ActiveX 対策を有効にする] 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. [アプレット /ActiveX 対策のグローバルポリシー] をクリックします。
4. [Java アプレット対策ルール] タブで、[すべてのアプレットをブロック] を選択し、[保存] をクリックします。
5. [ActiveX 対策ルール] タブで、[すべてのキャビネットファイルをブロック] と [すべての PE 形式ファイルをブロック] を選択し、[保存] をクリックします。
6. Web ブラウザを開き、株式情報やゲームなど、Java アプレットと ActiveX コントロールを使用している Web サイトにアクセスします。IWSS により、モバイルコードのダウンロードおよびブラウザでの実行がブロックされます。

注意： すべての Java アプレットと ActiveX コントロールをブロックすると、安全な Web サイトの多くも正しく動作しなくなるので、実際の運用環境にとっては制限が厳しすぎる場合があります。このテストが終了したら、[アプレット /ActiveX ポリシー : グローバルポリシーの編集] 画面に戻り、設定を初期設定に戻すか、または制約の少ない独自の設定に戻すことをお勧めします。

情報漏えい対策をテストする

情報漏えい対策 (DLP) をテストするには

1. 機密データを含むサンプルファイル、たとえば、`test@example.com` などのメールアドレスを含むファイルを用意します。
2. IWSS で DLP を有効にします。
   a. [HTTP] → [情報漏えい対策] → [テンプレート] の順に選択します。
   b. テンプレートを追加して、すべてのメールアドレスを機密データとして指定します。
   c. [HTTP] → [情報漏えい対策] → [ポリシー] → [DLP 検索のグローバルポリシー] の順に選択します。
   d. 新しいテンプレートを選択して、[処理] を [ブロック] に設定します。
   e. [保存] をクリックします。
   f. [DLP 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。
   g. ポリシーを選択して、[ポリシーの配信] をクリックします。
3. Internet Explorer でプロキシを設定します。
   a. Internet Explorer を開きます。
   b. [ツール] → [インターネット オプション] の順に選択します。
   c. [接続] タブを選択します。
   d. [LAN の設定] をクリックします。
   e. [LAN にプロキシ サーバーを使用する] チェックボックスをオンにします。これらの設定は、ダイヤルアップ接続や VPN 接続には適用されません。
   f. [アドレス] に、IWSS の IP アドレスを入力します。
   g. [ポート番号] に、IWSS の HTTP 待機ポート番号を入力します。ここには、IWSS 管理コンソールの [管理] → [配置ウィザード] → [プロキシ設定] → [HTTP 待機ポート番号] と同じ値を指定する必要があります。

h. [OK] をクリックし、もう一度 [OK] をクリックします。

4. Internet Explorer を使用してサンプルファイルをアップロードします。IWSS により、送信時にファイルがブロックされます。

図 C-8. 情報漏えい対策のメッセージの例

5. IWSS で DLP を無効にします。
   a. [HTTP] → [情報漏えい対策] → [ポリシー] → [DLP 検索のグローバルポリシー] の順に選択します。
   b. [DLP 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。
   c. ポリシーを選択して、[ポリシーの配信] をクリックします。
6. サンプルファイルをアップロードします。IWSS は、送信時にファイルをブロックしません。

付録 D

インストール後のタスクと参考情報

この付録では、次の項目について説明します。

- 82 ページの「OS のセキュリティ強化」
- 83 ページの「OS インストール後のその他の手順」

OS のセキュリティ強化

OS のインストール前とインストール後に、セキュリティを強化するための作業を行います。

注意： 本書に記載する推奨設定は、すべてのユーザのニーズを満たすものではありません。推奨設定を実装する前に、ご使用の環境や状態を慎重に検討してください。

セキュリティ強化に必要な OS インストール前の手順

UNIX または Linux システムをインストールする前に独自のポリシーを作成します。次の考慮事項を参考にしてポリシーを作成してください。

- サーバの主な利用目的
- 頻繁に利用するサービスと外部アクセスポート
- アカウントおよびサーバへのアクセスを必要とするユーザ
- 必要なローカルアプリケーション

トレンドマイクロでは次の手順を推奨します。

- ネットワークに接続せずにインストールプロセスを開始します。ネットワークに接続していなければ、インストール中にシステムが攻撃を受ける危険性を軽減できます。
- サポートされている最新バージョンの OS をインストールします。
- 必要なサーバ保護対策をすべて行った後で、ネットワークに再接続します。

セキュリティ強化に必要な OS インストールの手順

ほとんどの OS にはカスタマイズされたインストールオプションが備わっていますが、必要なパッケージのみをインストールし、不要なパッケージは無効にすることをお勧めします。

パーティションのサイズに関する要件はありません。適切なサイズは、ご使用の環境によっても、サーバの計画によっても異なります。次の説明を参考にして、パーティションを作成してください。

- サーバにメールホストをインストールする場合は、メールボックス専用のパーティションを作成します。
- RAM の約 2 倍の容量のスワップパーティションを作成します。
- ほとんどの UNIX システムは、階層型ファイルシステム (FHS[2]) に移行しています。パーティションサイズがこの規格に対応していることを確認してください。

- 初期設定ログインで使用するために、特権のないユーザアカウントを作成します。

OS インストール後のその他の手順

インストールプロセスが終了したら、次のインストール後の作業を実行することをお勧めします。

1. インストールしたすべてのパッケージの推奨アップデートと Security Patch を使用して、システムのセキュリティを強化します。

   次の Web サイトから Red Hat Linux の Security Patch をダウンロードできます。
   http://www.redhat.com/security/

2. 実行中のプロセスとアップグレードするパッケージ間で競合が発生するリスクを軽減するため、システムをシングルユーザモードに変更してから Patch をインストールします。シングルユーザモードに変更するには、Linux では init 1 を使用します。

3. さらに、http://www.rpmfind.net から Linux パッケージを検索できます。パッケージが配布者によるオリジナルパッケージであることを確認するために、ファイルのシグネチャを確認します。リモート管理用に SSH をインストールすることをお勧めします。次のコマンドを使用して、インストールされたパッケージや Patch を表示します。

   ```
   # rpm –qa
   ```

   さらに詳しい情報を表示するには、上記のコマンドと more コマンドまたは grep コマンドを組み合わせます。以下に例を示します。

   ```
   # rpm –qa |grep package-name
   ```

4. `/etc/passwd` (`/etc/shadow`) およびグループファイルから、割り当てられていないすべてのユーザを削除します。

付録 E

テクニカルサポート

この付録では、次の項目について説明します。

- 86 ページの「アップデートプログラムについて」
- 86 ページの「製品サポート情報」
- 86 ページの「サポートサービスについて」
- 87 ページの「製品 Q&A のご案内」
- 87 ページの「セキュリティ情報」
- 88 ページの「脅威解析・サポートセンター TrendLabs (トレンドラボ)」

アップデートプログラムについて

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。以下の URL で最新の Patch をご確認いただけます。

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

InterScan Web Security Suite (以下、IWSS) のリンクをクリックして、IWSS の [ダウンロード] ページを開きます。[Patch] タブをクリックして、使用可能な Patch を確認してください。

Patch には日付が付いています。まだ適用していない Patch については Readme ドキュメントを参照し、適用するかどうかを判断します。Patch を適用する場合は、Readme の説明に従ってインストールします。

製品サポート情報

製品のユーザ登録により、さまざまなサポートサービスを受けることができます。

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

サポートサービスについて

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

サポートサービス内容は、予告なく変更される場合があります。また、製品に関するお問い合わせについては、サポートセンターまでご相談ください。トレンドマイクロのサポートセンターへの連絡には、電話、FAX、メールなどをご利用ください。サポートセンターの連絡先は、「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、サポートサービスの継続をご希望される場合は、契約満了前に更新されることをお勧めします。更新手続きの詳細は、トレンドマイクロの営業部、または販売代理店までお問い合わせください。

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

製品 Q&A のご案内

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

製品 Q&A

`http://esupport.trendmicro.com/ja-jp/enterprise/default.aspx`

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

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

セキュリティ情報

トレンドマイクロ「セキュリティ情報」

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

`http://www.trendmicro.co.jp/jp/security-intelligence/index.html`

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

セキュリティ情報 Web サイトでは、次の情報を閲覧できます。

- ウイルス名やキーワードから検索できるウイルスデータベース
- コンピュータウイルスの最新動向に関するニュース
- 現在流行中のウイルスや不正プログラムの情報

- デマウイルスまたは誤警告に関する情報
- ウイルスやネットワークセキュリティの予備知識

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

トレンドマイクロへのウイルス解析依頼

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

ファイルを送信いただく前に、トレンドマイクロの不正プログラム情報検索サイト「セキュリティデータベース」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。

`http://about-threats.trendmicro.com/ThreatEncyclopedia.aspx?language=jp`

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

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

感染ファイルを送信する際には、感染症状について簡単に説明したメッセージを同時に送ってください。送信されたファイルがどのようなウイルスに感染しているかを、トレンドマイクロの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 箇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。

索引

英数字

availability requirements 57
Blue Coat Port 80 Security Gateway、設定 50
Cisco CE ICAP サーバ、設定 53
components
installation 44
Control Manager
コンポーネント 44
Control Manager、Trend Micro Control Manager 13
enable_ip_user_cache 63
FTP
検索コンポーネント 44
サービス 19
上位プロキシ 34
フロー 33
FTP over HTTP 28
HTTP
検索コンポーネント 44
サービス 19
ハンドラ 13
HTTP/FTP
サーバの保護 59、19
HTTP および FTP のサービスフロー 41
ICAP
Blue Coat アプライアンスについて 50
Cisco CE サーバ 53
準拠のキャッシュサーバ、設定 50
ICAP モード
HTTP プロキシ 30
複数のサーバ 32
IWSS
コンポーネント 44
テスト 69
IWSS サーバ
DMZ を備えた 2 つのファイアウォールの設置場所 38
DMZ を備えていない 1 つのファイアウォールの設置場所 39
ネットワーク上の設置場所 38
Java Runtime 51
LDAP
連携 57
OS
強化 82
その他のインストール手順 83
Patch 86
PostgreSQL データベース 13
Readme 8、86
removing 43
SNMP 14
SNMP 通知コンポーネント 44
SolutionBank、製品 Q&A を参照 8
Trend Micro Control Manager
コンポーネント 44
TrendLabs 88
URL フィルタコンポーネント 44
Visual Policy Manager 51
Web コンソールのパスワード 14
X-Infection-Found 55

X-Virus-ID 55
対象 8

あ

アクティベーションコード 14
アップデートプログラム 86
アプレット /ActiveX 対策コンポーネント 44
依存モード
FTP プロキシ 35
HTTP 二重プロキシ 26
HTTP プロキシを内側に配置 24
HTTP プロキシを外側に配置 23
HTTP リバースプロキシ 28
二重プロキシ 25
インストール 11、43、44
Blue Coat Port 80 Security Appliance 50、53
CD-ROM 46
IWSS 37
既存の FTP プロキシ 34
必要な情報 12
インストール後 47
インストール前 45
ウイルス
検索サーバクラスタ、設定 54
ウイルス検索サーバクラスタ
サーバクラスタ 54
オンラインヘルプ 8

か

可用性の要件 57
クライアント設定 15
クラスタ設定またはエントリ、削除 55

さ

削除 11
サポート 86
冗長ログ 64
スタンドアロンモード 21
FTP プロキシ 34
HTTP プロキシ 21
複数のサーバ 22
スループットの要件 57
製品 Q&A 8
製品のアップデート 86
接続の要件 56

た

データベース 13
トラブルシューティング 65
データベースの種類と場所 13
ディレクトリ (LDAP) サーバ
パフォーマンス 62
テクニカルサポート 86
テスト
FTP 検索 71
URL フィルタ 74
URL ブロック 70、72
アップロード検索 70
スパイウェア検索 75
ダウンロード検索 73
透過モード
HTTP プロキシ 27

ドキュメント 8

な

ネットワークトラフィック 15
ネットワーク保護 40

は

はじめに 7
パフォーマンスの調整 62
複数のサーバ 32
プロキシ
  ICAP 対応 18
  アップデート 14
  設定 13
分散環境 56
ポリシーの追加
  応答モード 51
  要求モード 52

ま

メインプログラム 44

や

ユーザ認証キャッシュ 63
要件 12

ら

リバースプロキシ 13
レイヤ 4 スイッチ 17