Trend Micro
InterScan Web Security Suite™

Linux版

インストールガイド

安心を、ひとつ上のステージへ。

TREND MICRO™

P/N: IWSSLX-AE0103 (2008/5)

目次

はじめに

Trend Micro InterScan Web Security Suite 3.1 (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。

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。本書では、読者が、次の項目に関する詳しい内容を含め、ネットワークスキームに関する知識が豊富であることを前提としています。

- HTTP および FTP プロトコル
- データベース設定

ただし、ウイルス対策またはスパムメール対策の技術に精通していることを前提としていません。

ドキュメント

Trend Micro InterScan Web Security Suite 3.1 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** — ユーザインターフェースを使用してあらゆる機能を設定するのに役立ちます。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。

  オンラインヘルプの目的は、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固有の情報を提供することです。固有の情報としては、有効なパラメータ範囲や最適値などがあります。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/

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、また次の 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

情報を簡単に検索し、理解できるように、IWSS 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

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。

サーバ要件

OS

- Red Hat Enterprise Linux 4.0 Update 5

  必要なインストールパッケージクラスタ : 最小システム

- Red Hat Enterprise Linux 5.0 以降

  必要なインストールパッケージクラスタ : 最小システム

- SUSE Linux Enterprise Server 10 (SP1)

追加で必要なフォント :

- Japanese TrueType fonts (Red Hat OS)
- Sazanami-fonts (SUSE OS)

ヒント : 上記のフォントは、以下のようなパッケージファイルに含まれています。
- Red Hat Enterprise Linux: ttfonts-ja-1.2 〜 .rpm
- SUSE Enterprise Server: sazanami-fonts. 〜 .rpm
(〜の部分はリリースバージョンを指します。リリースバージョンは、ディストリビューションによって異なります。

ハードウェア要件

- Intel Pentium 4 2.4GHz プロセッサまたは同等
- 2GB の RAM:
  - モバイルコードセキュリティオプションを使用する場合は、128MB の RAM を追加

- ハードディスクドライブの空き容量 :
  - 150MB
  - 物理メモリの 4 倍のスワップパーティション
  - PostgreSQL のインストール用に 125MB のディスク空き容量
- 解像度 800 x 600 をサポートするモニタ、256 色以上

Web ブラウザ

HTTP 対応の Web コンソールにアクセスするには、表 1-1 に記載されたブラウザを使用してください。

表 1-1. サポートされている Web ブラウザ

ブラウザ	Windows			Apple
	2003	XP SP2	Vista	
Internet Explorer 6.0	X	X		
Internet Explorer 7.0		X	X	
Firefox 1.5		X		
Firefox 2.0		X	X	
Safari 2.0				X

その他

- データベース要件 :
  - PostgreSQL v7.4.16 (同梱されています)
  - サーバファーム設定で複数の IWSS サーバを使用する場合、PostgreSQL 用に別のサーバ (可能であればクラスタサーバ) を使用することをお勧めします。
  - ログファイル管理のために、1 日 300 万件の HTTP リクエスト毎に 1.7GB のディスクの空き容量 (アクセスログが有効になっている場合)
  - アクセスログが有効な場合、256MB の RAM (アクセスログが無効な場合、64MB)
- IWSS では、Internet Content Adaptation Protocol (ICAP) 1.0 をサポートします。
- ディレクトリサーバ :

  LDAP (Lightweight Directory Access Protocol) のユーザ / グループに基づいてポリシーを設定する場合、IWSS と次の LDAP ディレクトリとの連携が可能です。
  - Microsoft Active Directory 2000 および 2003
  - Linux OpenLDAP Directory 2.2.17
  - Sun Java System Directory Server 5.2 (旧名称 : Sun ONE Directory Server)
- トレンドマイクロ ダメージクリーンナップサービスおよび Trend Micro Control Manager (オプション製品)
  - 不正プログラムのクリーンナップ用に DCS 3.2
  - 集中管理用に Trend Micro Control Manager 3.5 Patch 2 以降

注意 : IWSS 3.1 Linux 版をインストールしたサーバに、Trend Micro InterScan Messaging Security Suite をインストールすることはサポートされていません。

注意： IWSS 3.1 Linux 版をインストールしたサーバに、他のプロキシサーバ製品をインストールした場合、十分なパフォーマンスを得られる可能性が低いため推奨しません。
同一のサーバにインストールする場合には、事前に十分な検証を行ったうえでご利用ください。

追加の要件

- サーバコンピュータに対する root 権限が必要です。
- IWSS サーバおよび IWSS クライアントでは、ICMP エコー応答シーケンスを実行できる必要があります。ICMP エコー応答シーケンスでは、インストール時に選択したサーバに応じて、DNS 名または IP アドレスのいずれかを使用します。

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。最新のシステム要件については、弊社 Web サイトやサポート窓口にご確認ください。

IWSS のインストールに必要な情報

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

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

IWSS インストール後に管理者は HTTP 検索方法を変更できます。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、26 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

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リスク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。ただし、透過を有効にした場合を除きます。しかし、透過を有効にすると、ユーザ識別方法が IP アドレスまたはホスト名 (またはその両方) に制限されます。これによって、一部の FTP にアクセスできなくなる可能性があります。

別の設定シナリオとして、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、26 ページの「HTTP フローを計画する」および 42 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。Control Manager サーバには IWSS をインストールしないでください。

データベースの種類と場所

IWSS では、レポートのログ、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。既存のインスタンスがない場合は、PostgreSQL インスタンスをインストールします。

IWSS では、多くのセキュリティリスクの検出、ポリシー違反、またはプログラムイベントに応答して通知を送信します。

SNMP 通知

SNMP 通知の使用を予定している場合、管理コンソールの [管理] → [IWSS 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 SNMP 通知を使用できます。

SNMP の設定画面では、コミュニティ名、ホスト名、オブジェクト識別子 (OID)、場所、担当者など、いくつかの SNMP 設定入力が必要です。また、ホスト、コミュニティ名、ポート番号、SNMP トラップを受け取るホストの初期設定のトラップコミュニティの入力も要求されます。

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、インストール時に設定されるパスワードによって制限されます。

インターネットアップデート用のプロキシ

IWSS とインターネットの間にプロキシがある場合は、プロキシサーバのホスト名または IP アドレス、ポート番号、およびアカウントを入力します。

アクティベーションコード

IWSS を構成する 3 つのモジュールである、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、個別のアクティベーションコードが必要です。

新規インストールまたは移行

IWSS を新規インストールする場合、または IWSS のバージョン 2.x またはバージョン 3.0 から本バージョンに移行する場合は、./install_iwss.sh スクリプトを実行します。第 3 章「インストール」または第 4 章「旧バージョンからの移行」を参照してください。

リモートインストールまたはローカルインストール

IWSS は、ローカルサーバまたはリモートサーバのいずれかにインストールできます。UNIX システム上でリモートインストールを実行するには、NFS を介してそのシステムに接続し、そのシステムのコンソールから IWSS インストーラを実行する必要があります。

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。

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

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。この設定を使用すると、FTP over HTTP トラフィックは確実に 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 プロキシモードへ変更する必要があります。

pni ファイルの [http] セクションに、次のパラメータを設定します。

- transparency= no　　透過モードを無効にします。
- self_proxy= (yes|no)　　トラフィックの配信要件に応じて yes または no を指定します。

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 1-2.　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。

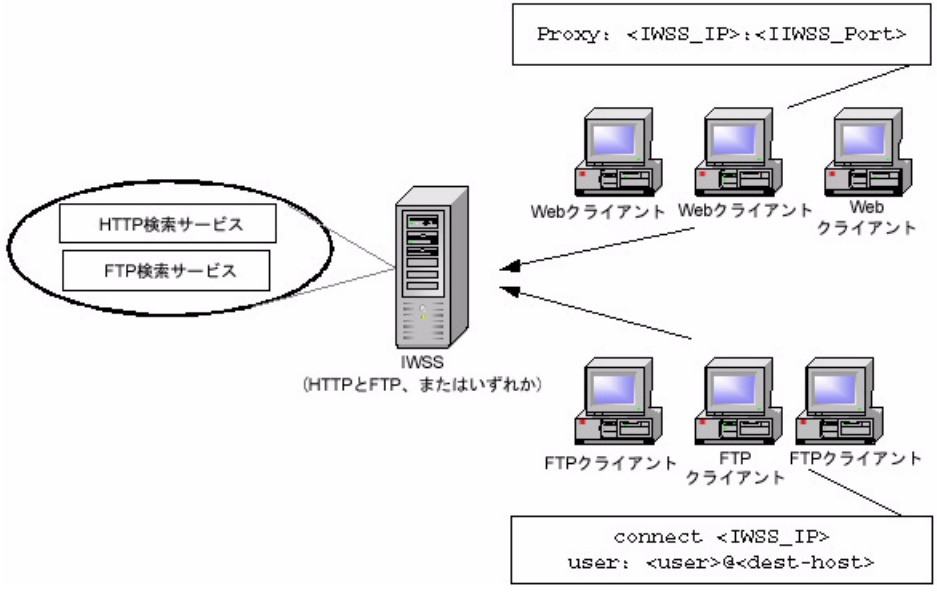

図 1-1.　クライアントを再設定する場合

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。HTTP 検索サービスで、透過を有効にする設定変更が必要です。

pni ファイルの [http] セクションに、次のパラメータを設定します。

- transparency=simple　通常の透過モードが有効になります。
- self_proxy yes|no　トラフィックの配信要件に応じて yes または no を指定します。

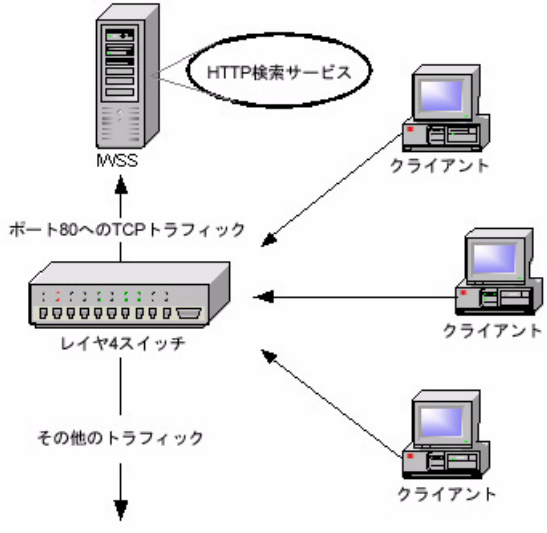

図 1-2.　レイヤ 4 スイッチを使用する場合

表 1-3.　レイヤ 4 スイッチを使用する場合

利点	制限
クライアントにとって透過的です。	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。
容易に確立できます。	FTP トラフィックにスイッチベースのリダイレクトを使用できません。
	LDAP がサポートされません。

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 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。

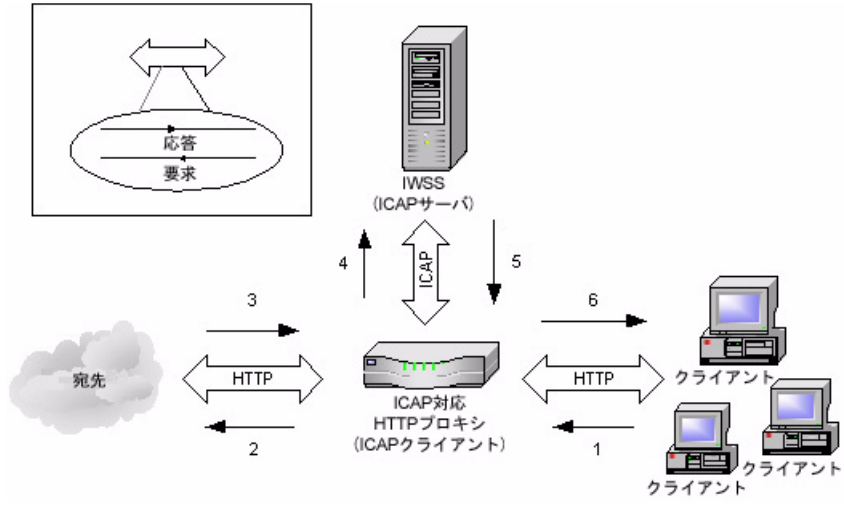

図 1-3.　ICAP 対応のプロキシを使用する場合

表 1-4.　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。	管理が必要です。

利点	制限
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。	管理が必要です。

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について決定します。
- サービスに使用するポートを決定します。たとえば、初期設定では、HTTP サービスにはポート 8080、FTP サービスにはポート 21 が使用されますが、他のアプリケーションまたはサービスでポート 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の要求を直接 Web サイトに送信するのか、上位 HTTP プロキシに送信するのかなどについて決定します。
- サービス固有の考慮事項があれば追加します。たとえば、HTTP サービスフローには ICAP デバイスを含めても、FTP サービスフローには含めないなどについて検討します。

以上の情報を収集したうえで、管理者は、考えられるフローを基に IWSS の設定を変更します。

HTTP フローを計画する

IWSS に使用する HTTP フローを計画する際は、最初の手順として、ハンドラの種類を選択します。

- HTTP プロキシ
- ICAP デバイス

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
- **透過プロキシモード** — このフローは、クライアントコンピュータが IWSS サーバを初期設定のゲートウェイとして使用するように設定されていないにもかかわらず、IWSS 経由でインターネットに接続する必要がある場合に使用します。

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、このフローを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使用し、複雑な Web サイトを持つ組織では、中央でアクセスを制御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、次の順序でやり取りされます。

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完了します。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 1-5. 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。

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。

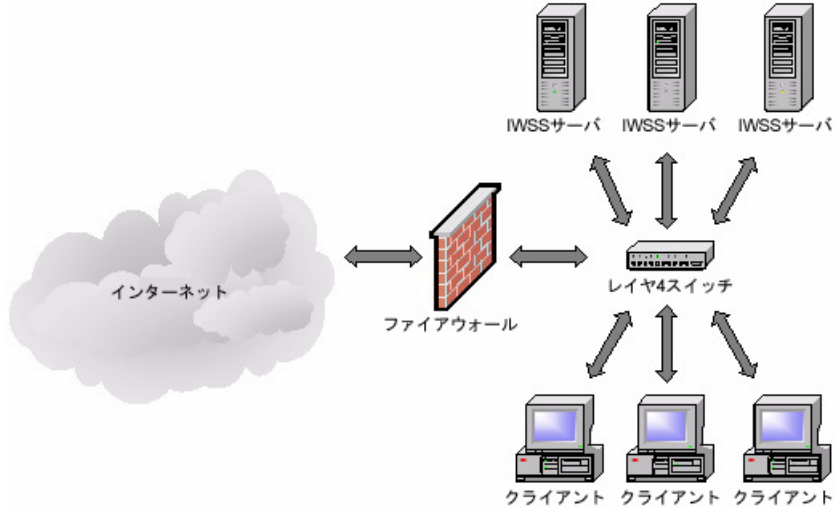

図 1-4. レイヤ 4 スイッチを使用し、複数の HTTP スタンドアロンサーバに対して IWSS サーバ間で負荷を分散する構成

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、次の順序でやり取りされます。

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完了します。
   - 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 (理想的には 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。

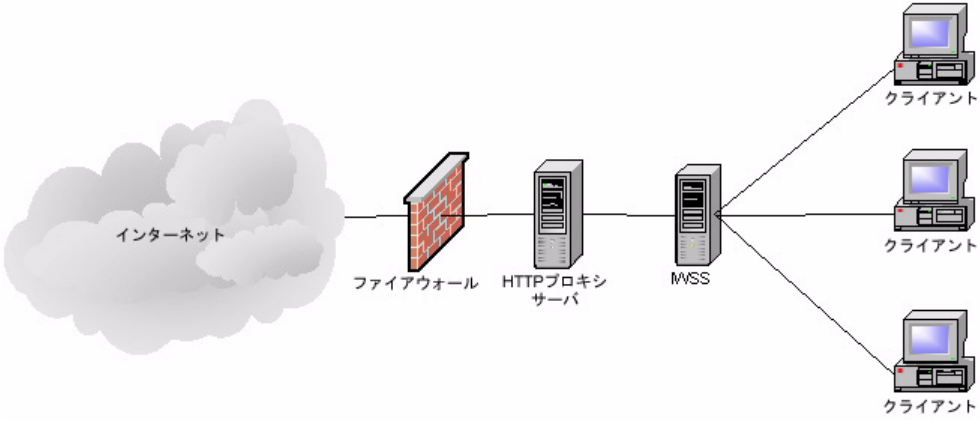

図 1-5.　依存モードの HTTP プロキシ (プロキシを外側に配置する場合)

表 1-6.　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 つのリスクも含んでいます。
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、次の順序でやり取りされます。

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完了します。
   - 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。

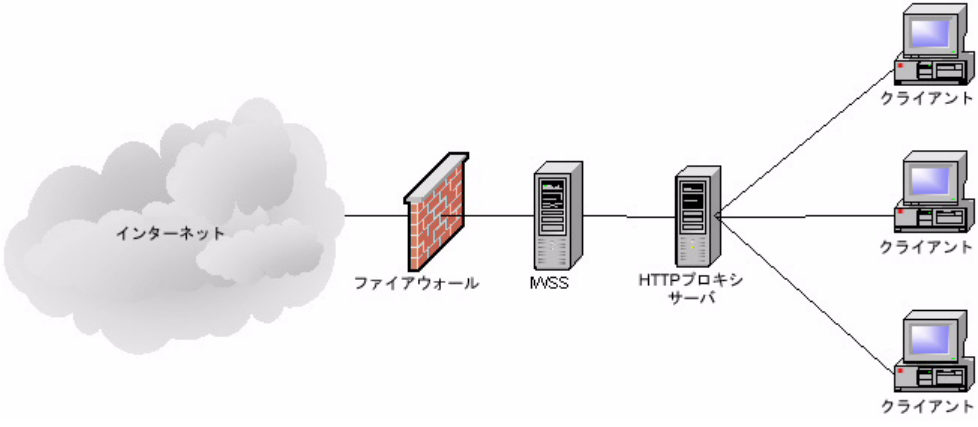

図 1-6. 依存モードの HTTP プロキシ (プロキシを内側に配置する場合)

表 1-7. 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 の設定変更がキャッシュされているオブジェクトに反映されます。
キャッシュされているオブジェクトがプロキシサーバからクライアントに直接ダウンロードされるため、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、次の順序でやり取りされます。

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完了します。
   - 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。

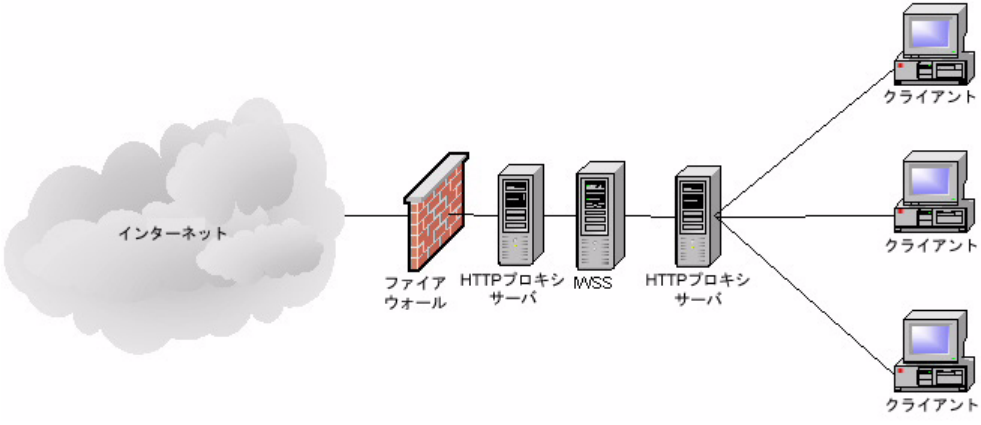

図 1-7.　依存モードの HTTP 二重プロキシ

表 1-8.　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。
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。	
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。

- 通常の透過を使用すると、ポリシーを定義するのに使用できるユーザの識別方法が IP アドレスとホスト名に限られます。LDAP ではポリシーを設定できなくなります。
- FTP over HTTP は使用できません。このため、FTP 接続を許可しないファイアウォール設定では、ftp:// で始まる URL へのリンクは機能しません。または ftp:// で始まる URL に接続できても、ファイルが検索されません。
- HTTP 要求にホスト情報が格納されていない場合、旧バージョンの Web ブラウザの中には通常の透過に対応できないものがあります。
- HTTP の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ないことになります。
- 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。
- トレンドマイクロ ダメージクリーンナップサービス (DCS) がクリーンナップを行うために IP アドレスからクライアントコンピュータ名を解決できる環境が必要です。

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、次の順序でやり取りされます。

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。

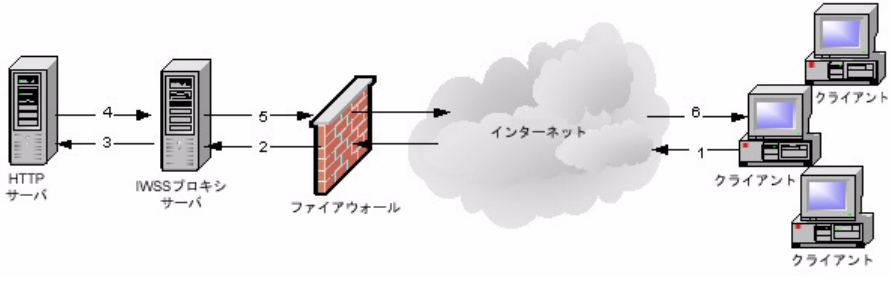

図 1-8. 依存モードの HTTP リバースプロキシ

表 1-9. 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 つの手順のみ実行すればよく、8 つの手順を実行する必要はありません。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、次の順序でやり取りされます。

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完了します。
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。

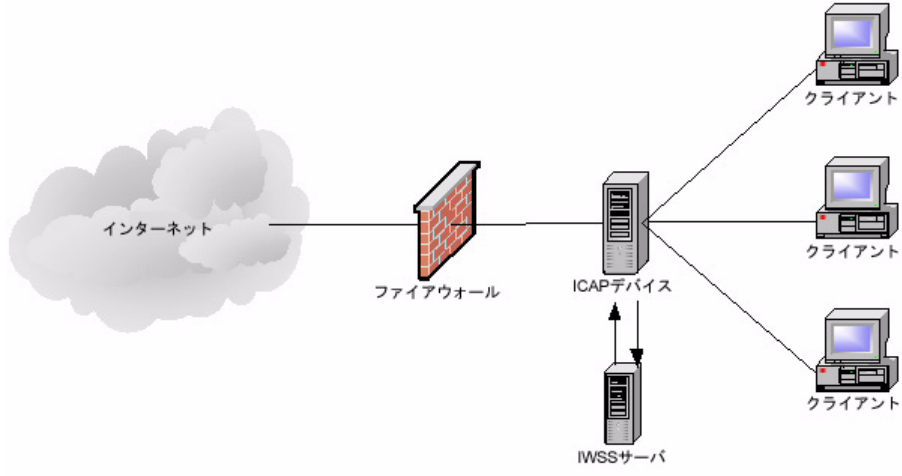

図 1-9. ICAP モードの HTTP プロキシ (1 台の IWSS サーバを配置する場合)

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 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。

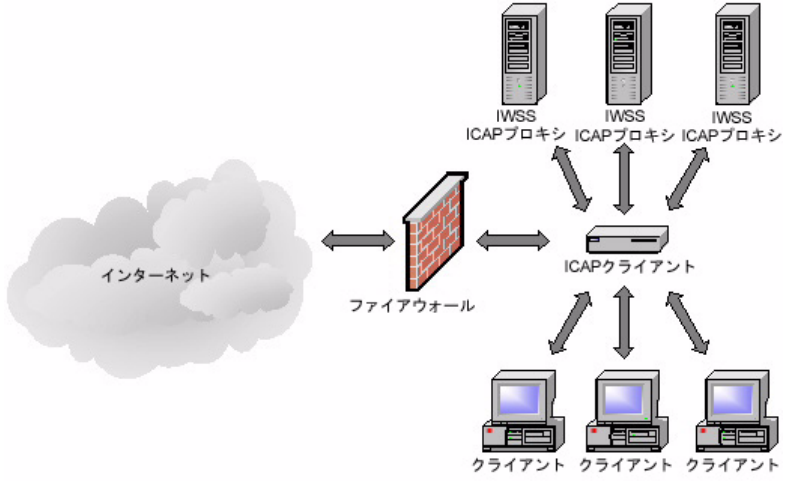

図 1-10.　ICAP モードの HTTP プロキシ (複数の IWSS サーバを配置する場合)

表 1-10.　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。	IWSS 上でユーザ識別がサポートされないため、セキュリティが制限されます。
キャッシュされているオブジェクトが、プロキシサーバからクライアントに直接ダウンロードされます。このため、遅延を最小限に抑え、パフォーマンスを強化できます。	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。
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、スタンドアロンと依存の 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** — 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** — 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。これによって、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、ターゲットの 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、次の順序でやり取りされます。

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。

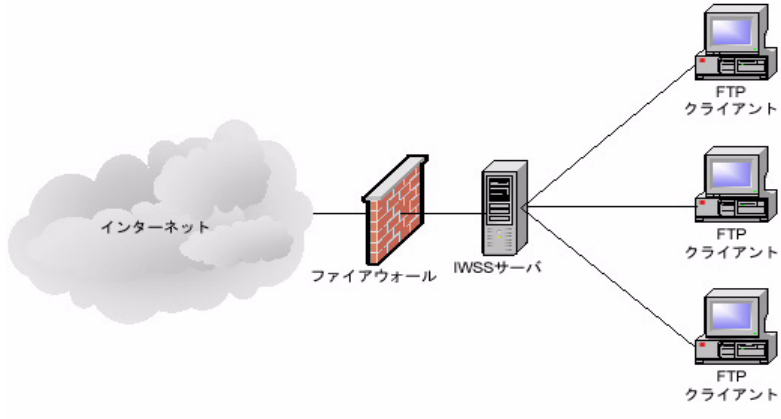

図 1-11.　スタンドアロンモードの FTP プロキシ

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 プロキシサーバが蓄積交換技法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、次の順序でやり取りされます。

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。

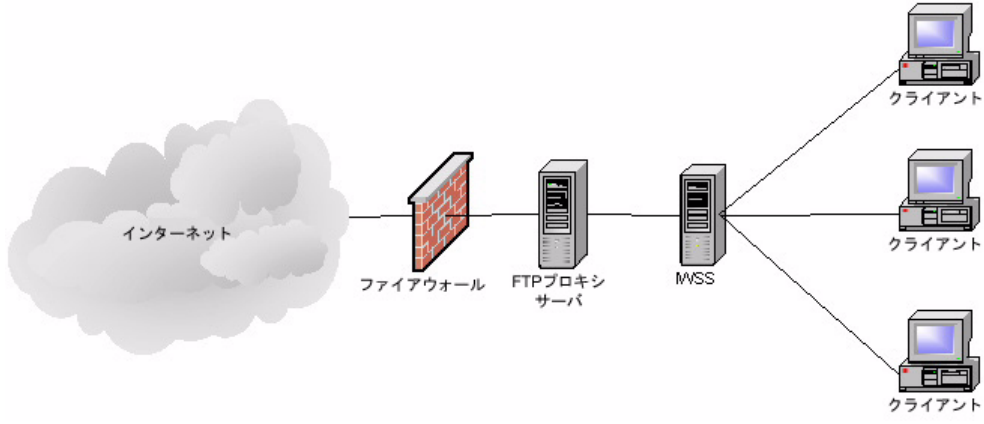

図 1-12.　依存モードの FTP プロキシ

第 2 章

導入

本章で説明する内容には、次の項目が含まれます。

オペレーティングモード

以前のバージョンと異なり、Trend Micro InterScan Web Security Suite (以下、IWSS) 3.1 では 1 つのオペレーティングモードである TPC (Threads per Connection) モードが使用されます。このモードでは、4 つのプロセスが実行されますが、各プロセスでは 500 個のスレッドが実行されます。IWSS では合計 2000 個のスレッドを処理できます。プロセスの数とプロセスごとのスレッドの数は、ハードウェアとネットワークの環境に応じて設定することができます。詳細については、95 ページの「適切なプロセス / スレッド値を設定する」を参照してください。

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既存のサーバを確認します。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。

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

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。

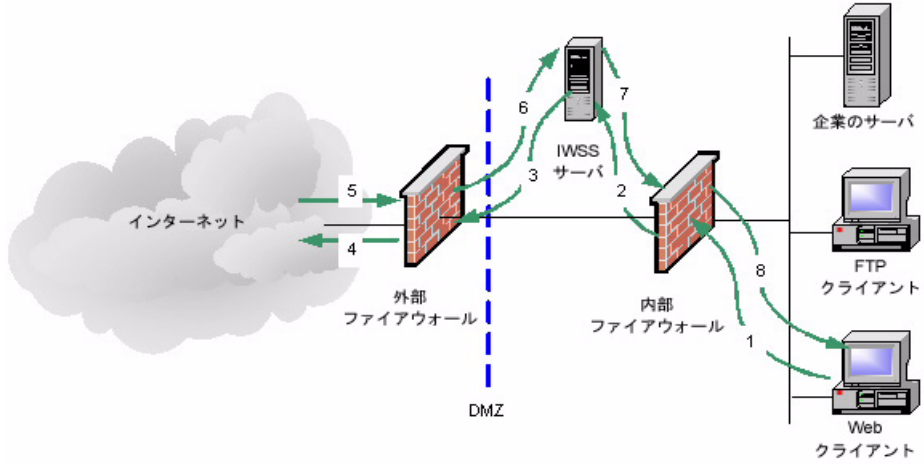

図 2-1.　DMZ を備えた 2 つのファイアウォール

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。

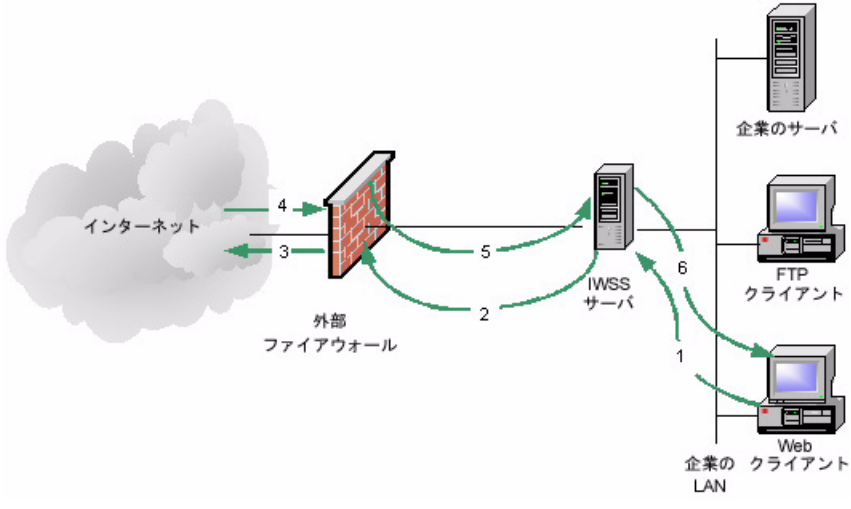

図 2-2.　DMZ を備えていない 1 つのファイアウォール

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。

- クライアントの再設定
- レイヤ 4 スイッチの使用
- ICAP 対応プロキシの使用

詳細については、付録 A の 81 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について決定します。
- サービスに使用するポートを決定します。たとえば、初期設定では、HTTP サービスにはポート 8080、FTP サービスにはポート 21 が使用されますが、他のアプリケーションまたはサービスでポート 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の要求を直接 Web サイトに送信するのか、上位 HTTP プロキシに送信するのかなどについて決定します。

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

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。

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、Trend Micro 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。
- **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。
- **IntelliTunnel セキュリティ** — 特定のインスタントメッセージプロトコルおよび認証接続プロトコルによる通信をブロックするサービスです。
- **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。

注意： URL フィルタ機能およびアプレット /ActiveX 対策機能を使用するには、個別のアクティベーションコードが必要です。

インストール前に関する注意

次のいずれかの操作を実行して、DNS サーバで IWSS ホスト名を IP アドレスに解決できることを確認してください。

- IWSS サーバ用のレコードを DNS サーバに追加します。
- 適切なエントリを /etc/hosts ファイルに追加します。

  エントリは次のような形式になります。

  {IP アドレス} { ホスト名 }

  たとえば、次のように記述します。

  10.1.1.1 iwsssrv

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。

注意： 検索機能や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 (「管理者ガイド」を参照)。

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。

3. 表示されるプロンプトに応答します。<Enter> キーを押して初期設定を受け入れるか、または選択する情報を入力してから <Enter> キーを押します。

   入力した内容に応じてインストール操作についての説明が表示されます。

体験版をダウンロードするには

1. 次の Web サイトを参照してください。

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

2. [製品・サービス一覧] にあるドロップダウンリストから [InterScan Web Security Suite] を選択します。

3. [InterScan Web Security Suite] 画面で、[体験版ダウンロード] リンクをクリックします。

4. [体験版ダウンロード] 画面で、インストール対象 OS 用のプログラムの [メールアドレス登録フォームへ] をクリックします。

5. 表示される画面で必要な情報を入力し、使用許諾書をよくお読みいただき、同意していただける場合に [個人情報の取り扱いに同意し、確認画面へ] をクリックします。

6. IWSS を実行するサーバ上の一時ディレクトリに製品をダウンロードしてから、ファイルを解凍します。

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。

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、保護対象サーバポート番号と同様に 80 のみをサポートしています。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 待機ポート番号] と、保護対象サーバの [ポート番号] にそれぞれ指定してください。リバースプロキシ用の IWSS 待機ポート番号は、80 に固定化されています。

第 4 章

旧バージョンからの移行

本章で説明する内容には、次の項目が含まれます。

移行について

Web コンソールを使用して、Trend Micro InterScan Web Security Suite (以下、IWSS) のバージョン 3.0 をバージョン 3.1 に移行できます。

注意： バージョン 3.1 へのアップグレードは、バージョン 3.0 からのみ可能です。バージョン 1.02 からアップグレードしたい場合は、まずバージョン 3.0 にアップグレードし、そこからもう一度バージョン 3.1 にアップグレードする必要があります。

Red Hat Enterprise Linux (RHEL) に関する注意

IWSS では、Red Hat Enterprise Linux 3.0 (RHEL 3) はサポートされていません。IWSS を RHEL 3 でインストールする場合、移行前に OS を RHEL 4 または RHEL 5 へアップグレードしてください。

RHEL 5 では、RHEL 3 や RHEL 4 とは異なる POSIX 標準が採用されています。これによって、IWSS 3.0 は IWSS 3.1 への移行を続行するためのシステム Patch ファイルをアップロードできません。IWSS 3.0 を RHEL 3 または RHEL 4 上で実行している環境において、IWSS 3.1 への移行前に RHEL 5 以降にアップグレードする場合、次の手順に従う必要があります。

1. IWSS サーバの OS を RHEL 5 以降にアップグレードします。
2. change_tail_semantics.sh スクリプトを IWSS サーバにコピーします。

   注意： change_tail_semantics.sh スクリプトは、IWSS 3.1 パッケージに収録されています。

3. change_tail_semantics.sh スクリプトを実行します。
4. 63 ページの「旧バージョンから移行する」の手順で続行します。

ログの移行に関する注意

IWSS は、自動的に IWSS 3.0 がコンピュータにインストールされていることを検出して、設定内容を保存します。しかし、カスタマイズされたディレクトリは移行時に保存されますが、ディレクトリの内容は保存されません。

次のディレクトリの内容は移行されません。

- セキュリティログおよびシステムログ
- 隔離ログ

オペレーティングモードの移行に関する注意

以前のバージョンでは、IWSS は異なるオペレーティングモードであるスレッドモードとプロセスモードで実行されていました。しかし、現在のバージョンの IWSS では 1 つのオペレーティングモードである TPC (Threads per Connection) モードが使用されます。移行時において、バージョン 3.0 のオペレーティングモード (スレッドモードとプロセスモードのどちらか) は、自動的に TPC モードに変更されます。TPC モードは、ユーザインタフェースを介して設定することはできません。

要件

IWSS ソフトウェア要件は次のとおりです。

- **Web ブラウザ** : Internet Explorer (バージョン 6.0 または 7.0) または Mozilla Firefox (バージョン 1.5 または 2.0)
- **ファイル** :
  - **バージョン 3.0 拡張用 Patch**: iwss_30_patch_enhancement_ja_patch.tgz
  - **バージョン 3.1 のパッケージ** : iwss_30_to_31_ja_patch.tgz

注意 : バージョン 3.1 のパッケージをアップロードする前に、必要な Patch をバージョン 3.0 にアップロードしてください。

移行に必要なファイルは、次のサイトにあります。

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

旧バージョンから移行する

旧バージョンから移行するには

1. IWSS 3.0 の Web コンソールを開きます。

   http://< 管理コンソールの IP アドレス >:1812

2. [管理] → [システムパッチ] の順に選択します。
3. [参照] をクリックします。
4. 次のファイルを探します。

   iwss_30_patch_enhancement_ja_patch.tgz

5. [アップロード] をクリックし、次の画面で [インストール] をクリックします。
6. 手順 1 ～ 4 を繰り返しますが、アップロードするパッケージは次のパッケージです。

   iwss_30_to_31_ja_patch.tgz

   アップロードが完了したら、必要に応じて Web コンソールに再度ログインすると、[システムパッチのインストール] 画面が表示されます。画面には初期設定で [IWSS 3.1 へのアップグレード] タブが表示されます。
7. リモート共有データベース設定で移行する場合は、次の手順に従ってください。

   a. [IWSS サーバファーム] タブを選択します。
   b. [IWSS サーバファーム配信に使用できるようにデータベースの移行を有効にする] チェックボックスをオンにします。
   c. [マスター] または [スレーブ] のオプションを選択します。
   d. データベースを別のサーバに移行するには、[既存のデータベースを次のサーバに移行] チェックボックスをオンにして、サーバの詳細を設定します。

8. [IWSS 3.1 へのアップグレード] タブで [インストール] をクリックし、インストールが完了するまで待機します。

注意： 移行によって、IWSS の Web コンソールへの接続が切断される場合があります。この場合は、Web コンソールをブラウザでリロードします。これによって、IWSS ログイン画面にリダイレクトされます。

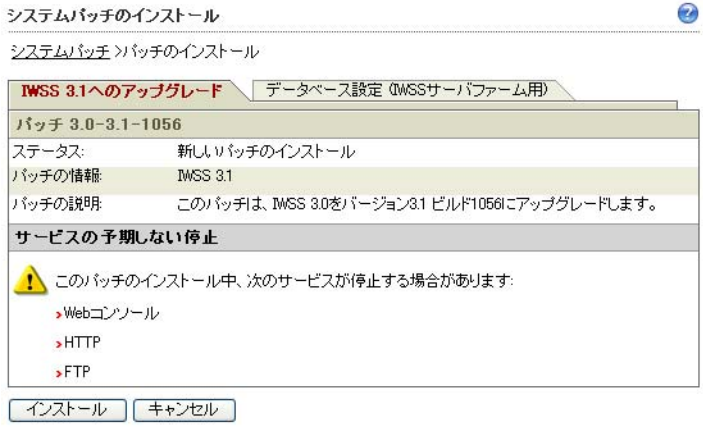

図 4-1. 移行インストール

9. 移行用パッケージがインストールされていることを [管理] → [システムパッチ] 画面で確認します。

移行されたパッケージが表形式で表示されます。

バージョン 3.0 にロールバックする

Web コンソールを使用して、以前のバージョンの IWSS にロールバックすることができます。ロールバック手順は、アップグレード手順と同じです。ただし、ロールバックでは以前のバージョンの IWSS のプログラムファイルが必要です。

ポリシーのみロールバックできます。ウイルス感染情報はロールバックできません。

以前のバージョンにロールバックするには

1. Web コンソールで、[管理] → [システムパッチ] の順に選択します。

図 4-2. [システムパッチ] 画面

2. IWSS 3.1 の移行元の Patch を選択して、[アンインストール] をクリックします。
3. [システムパッチのアンインストール] 画面で、[アンインストール] をクリックします。
4. ロールバックが終了したら、処理を完了するために IWSS の再起動を待機します。
5. ロールバックが正常に実行されたことを確認するには、Web コンソールを開き、[管理] → [システムパッチ] の順に選択します。そこで、バージョン 3.1 の Patch が存在しないことを確認します。

第 5 章

ICAP の設定

本章で説明する内容には、次の項目が含まれます。

IWSS ICAP のインストール後の設定

インストールした Trend Micro 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。

1. 68 ページの「ICAP 1.0 準拠のキャッシュサーバを設定する」
2. 77 ページの「「X-Virus-ID」ヘッダと「X-Infection-Found」ヘッダを有効化する」

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。

- 68 ページの「NetCache アプライアンスについて ICAP を設定するには」
- 71 ページの「Blue Coat Port 80 Security Appliance について ICAP を設定するには」
- 74 ページの「Cisco CE ICAP servers について ICAP を設定するには」

NetCache アプライアンスについて ICAP を設定する

NetCache アプライアンスについて ICAP を設定するには

1. ブラウザで http://{ **キャッシュサーバの IP アドレス** }:3132 を開いて、NetCache コンソールにログオンします。
2. [Setup] タブをクリックし、左側のメニューで [ICAP] → [ICAP 1.0] の順に選択します。
3. [General] タブを選択し、[Enable ICAP Version 1.0] を選択します。[Commit Changes] をクリックします。

注意： NetCache に必要な ICAP ライセンスキーを指定しなかった場合は、エラーメッセージ「icap: This service is not licensed.」が表示されます。

4. ICAP ライセンスキーを入力します。

   a. [Setup] タブを選択し、左側のメニューで [System] → [Licenses] の順に選択します。[System Licenses] 画面が表示されます。

   b. [ICAP License] に「IWFLPWA」と入力します。

   c. [Commit Changes] をクリックします。

5. [ICAP 1.0] 画面で [Service Farms] タブを選択し、[New Service Farm] ボタンをクリックして ICAP サーバを追加します。[Service Farm Name] フィールドにサービスファーム名を入力します。

   - 応答モードの場合は、[Vectoring Point] フィールドで [RESPMOD_PRECACHE] を選択します。
   - 要求モードの場合は、[Vectoring Point] フィールドで [REQMOD_PRECACHE] を選択します。

   [Service Farm Enable] チェックボックスをオンにします。

6. サービスファームに複数の ICAP サーバがある場合は、負荷分散に使用する適切なアルゴリズムを [Load Balancing] フィールドで選択します。[Bypass on Failure] チェックボックスをオフにします。

   注意： ネットワーク内でのウイルスの繁殖阻止を最優先する場合は、[Bypass on Failure] を無効にします。それ以外の場合は、[Bypass on Failure] を有効にして、インターネット接続がブロックされないようにします。

7. [Consistency] フィールドで、ドロップダウンメニューから [strong] を選択し、[lbw Threshold] フィールドを空白のままにします。

8. 応答モードの場合は、[Services] ボックスに次のように入力します。
icap://{ICAP サーバの IP アドレス }:1344/resp on
ICAP サーバの IP アドレスは、応答モードの IP アドレスです。

要求モードの場合は、[Services] ボックスに次のように入力します。
icap://{ICAP サーバの IP アドレス }:1344/REQ-Service on
ICAP サーバの IP アドレスは、要求モードの IP アドレスです。
複数の IWSS ICAP サーバがある場合は、複数のエントリを入力します。
たとえば、応答モードでは次にように入力します。

- icap://{ICAP サーバ 1 の IP アドレス }:1344/resp on
- icap://{ICAP サーバ 2 の IP アドレス }:1344/resp on

[Commit Changes] をクリックします。
要求モードでは次のように入力します。

- icap://{ICAP サーバ 1 の IP アドレス }:1344/REQ-Service on
- icap://{ICAP サーバ 2 の IP アドレス }:1344/REQ-Service on

[Commit Changes] をクリックします。

注意： サービスファームに複数の ICAP サーバを配置しており、[Consistency] で [strong] を選択した場合は、それらすべての ICAP サーバで、同一の intscan.ini、その他の設定ファイル、およびウイルスパターンファイルが使用されていることを確認してください。ICAP サーバの設定が互いに異なっていると、サービスファームは正常に動作しません。

---

9. [Access Control Lists] タブを選択し、[Enable Access Control Lists] チェックボックスをオンにします。[HTTP ACL] に「icap (ICAP サーバのサービスファーム名) any」と入力します。[Commit Changes] をクリックします。

FTP over HTTP トラフィックの検索を設定するには、[FTP] → [Configuration] → [Access Control Lists] に移動し、[FTP ACL] フィールドに「icap (サービスファーム名) any」を追加します。

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。[はい] 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。[警告 - セキュリティ] 画面が表示された場合は、[はい] をクリックします。

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

e. [Select policy table name] フィールドにポリシー名を入力します。[OK] 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] フィールドのリストから 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] ボタンをクリックします。

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。[警告 - セキュリティ] 画面が表示された場合は、[はい] をクリックします。

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

e. [Select policy table name] フィールドにポリシー名を入力します。[OK] 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] ボタンをクリックし、[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] フィールドのリストから 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。

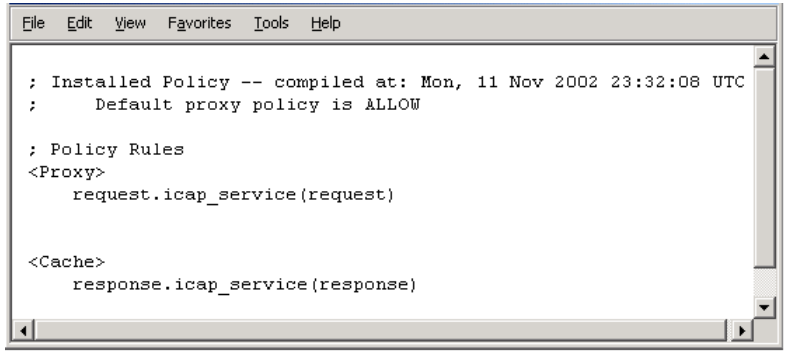

図 5-1. 要求モードと応答モードの ICAP サービスを設定します。現在のポリシーを確認するには、[Policy] 画面に移動し、[Policy Files] タブをクリックし、[Current Policy] をクリックします。

Cisco CE ICAP Servers について ICAP を設定する

Cisco CE ICAP servers について ICAP を設定するには

IWSS は、Cisco ICAP servers (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動させるには、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] フィールドに、クラスタ名を英数字で入力します。[OK] をクリックします。
5. 新しい ICAP クラスタ名を選択し、[Edit] をクリックします。[Edit ICAP Cluster name] 画面が表示されます。
6. [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 の範囲でウエイトを割り当てます。[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。[削除] 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-file
  ```

- 「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.i-cap.org/spec/draft-stecher-icap-subid-00.txt

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 [HTTP] → [設定] → [プロキシ検索] の順に選択します。
2. [プロキシ検索設定] 画面で、["X-Virus-ID" ICAP ヘッダを有効にする] または ["X-Infection-Found" ICAP ヘッダを有効にする] (またはその両方) を選択します。

ダメージクリーンナップサービスで SSL を使用する

HTTPS 対応の Web 管理コンソールを使用している場合、クライアントをトレンドマイクロ ダメージクリーンナップサービス (以下、DCS) にリダイレクトして不正なコードをクリーンナップするには、IWSS で使用している安全なポート (通常は 8443) へのアクセスを有効にする必要があります。これを有効にしないと、リダイレクト要求がブロックされるため、クライアントを DCS にリダイレクトできません。

安全なポート 8443 へのアクセスを許可するには

1. IWSS 管理コンソールのメインメニューから [HTTP] → [設定] → [アクセス管理] の順に選択し、[宛先ポート] タブを選択します。
2. [処理] ボックスのリストで [許可] を選択します。
3. [ポート番号] オプションを選択します。
4. [ポート番号] ボックスに、HTTPS トラフィックで使用するポート番号を入力します (通常は 8443)。

5. [追加] をクリックし、[保存] をクリックします。

図 5-2. DCS と HTTPS 管理コンソールを使用して、安全なポート (通常は 8443) へのアクセスを許可する

また、HTTPS を使用するように IWSS を設定する場合は、intscan.ini ファイルの [http] セクションで、次の 2 つのパラメータを変更する必要があります。

```
iscan_web_server=[ ユーザ定義の HTTPS ポート （例： 8443)]
iscan_web_protocol=https
```

導入の統合

この付録では、次の項目について説明します。

分散環境における IWSS

Trend Micro InterScan Web Security Suite (以下、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
データベースサーバ	タイプ : TCP データ量 : ・ 少 — アクセスログが無効になっている場合 ・ 中 — アクセスログが有効になっている場合	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。
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 ～ 50 MB/ 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。
Rating Service サーバ (設定されている場合)	タイプ : HTTP データ量 : 個別のアクセスによって異なります。	要求されたリソースが適切に分類されません。ポリシー設定でアクセスが禁じられている URL にアクセスできます。
トレンドマイクロダメージクリーンナップサービス (以下、DCS) サーバ (設定されている場合)	タイプ : HTTP データ量 : 感染したコンピュータの数によって異なります。	感染したコンピュータの駆除処理は実行されません。

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 サーバによるリフェラル追跡をサポートする

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 Web コンソールの [HTTP] → [設定] → [ユーザの識別] 画面で指定したメイン LDAP サーバがクライアントの認証情報を特定できない場合、参照サーバを構成して「リフェラル追跡」を有効にしておけば、指定したプライマリ参照サーバで、要求されたユーザ / グループオブジェクトが検索されます。プライマリ参照サーバで目的のオブジェクトが見つからない場合は、さらに、指定したセカンダリ参照サーバに対してクエリが実行されます。このような処理を行うには、すべての LDAP サーバについて、それぞれの管理アカウントに割り当てられている認証情報を intscan.ini ファイルの [LDAP-Setting] セクションに追加する必要があります。

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、グローバルグループや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 [HTTP] → [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 / 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。IWSS でグローバルカタログポートを使用できるのは、IWSS リフェラル追跡サーバの一部としてではなく、メイン LDAP サーバとして設定されている場合のみです。

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。

ゲストアカウント

LDAP のサポートが有効になっている場合、IWSS は認証されたプロキシモードで動作します。つまり、すべてのクライアントについて認証が必要になります。ゲストコンピュータやモバイルコンピュータのユーザはローカル LDAP サーバに登録されていないので、このルールを適用すると問題が発生する場合があります。

この問題を解決するため、HTTP プロキシモードの HTTP 検索サービスでは、ゲストコンピュータ用のプロキシサーバとして別の待機ポイントを使用できます。

次の設定パラメータでこの動作を制御します。

- intscan.ini/[http]/guest_user_login　ゲストポートを有効にする
- IWSSPIProtocolHttpProxy.pni/[main]/guestport　待機ポート番号を指定する

このポートを経由してアクセスしてきたコンピュータに対しては、LDAP のユーザ識別情報ではなく、特別な (ゲスト) ポリシーが適用されます。

ダメージクリーンナップサービスとの連携

IWSS は、HTTP および FTP ゲートウェイでワームやスパイウェアを検出し、ブロックできますが、DCS と連携して動作し、感染したクライアントをクリーンナップすることもできます。DCS は、システムのダメージの診断およびクリーンナップを行うことができる包括的なサービスです。ネットワーク内のクライアントコンピュータ上にソフトウェアをインストールする必要はありません。DCS は次の処理を実行します。

- ワームまたはトロイの木馬によって作成されたレジストリエントリを削除する
- メモリ内に残っているワーム、トロイの木馬、スパイウェアを削除する
- 不正プログラムによって改ざんされたシステムファイル設定を修正する

DCS サーバに IWSS を登録しておくと、次のいずれかの実行条件が検出された場合に、IWSS からクリーンナップ要求が発行されます。

- クライアントコンピュータが、フィッシングパターンファイルで「スパイウェア」、「不正サイト」、または「ウイルス流布サイト」に分類されている URL にアクセスしようとした場合
- クライアントコンピュータが、ワームとして分類されているウイルスをアップロードした場合

注意： 不正プログラムが、HTTP 以外のプロトコルを使用してリモートサーバにアクセスを試みた場合、IWSS では検出されないため、クリーンナップは実行されません。

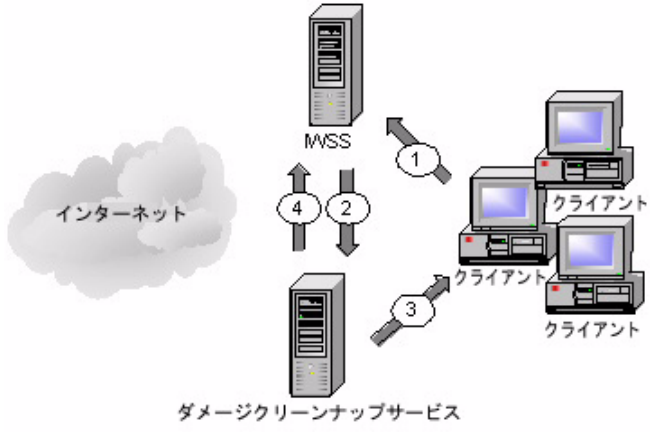

図 A-1. IWSS が DCS にクライアントのクリーンナップを要求する仕組み

IWSS を DCS サーバに登録すると、感染したクライアントのクリーンナップは次のように処理されます。

1. IWSS が、フィッシングパターンファイルに登録されている URL へアクセスしようとしているクライアント、またはワームをアップロードしようとしているクライアントを検出します。
2. IWSS が、感染したクライアントのクリーンナップを DCS サーバに要求します。
3. DCS は、感染したクライアントに接続し、そのクライアントをリモートからクリーンナップします。
4. クリーンナップの実行結果が DCS から IWSS へ報告され、ログに記録されます。

IWSS からクリーンナップ要求を受け取った DCS は、感染したクライアントに接続して、システムダメージの修復を試みます。その後、クリーンナップに成功したかどうかを IWSS サーバに報告します。この情報はログに記録されます。正常にクリーンナップできなかった場合、そのクライアントは、DCS サーバが管理している Web ページにリダイレクトされます。さらに、感染したコンピュータのユーザの許可を得たうえで、ActiveX コントロールがそのコンピュータのクリーンナップを再試行します。

注意： HTTPS 対応の IWSS 管理コンソールと DCS を併用する場合は、セキュリティで保護されたポート (通常は 8443) へアクセスできるように IWSS を設定する必要があります。セキュリティで保護されたポートへのアクセスがブロックされると、IWSS はクリーンナップ要求のためにクライアントを DCS にリダイレクトできません。詳細については、78 ページの「ダメージクリーンナップサービスで SSL を使用する」を参照してください。

Cisco 製ルータとの連携

クライアントコンピュータのブラウザ設定を変更しなくても、Cisco 製ルータをゲートウェイとして使用しているネットワークで IWSS を使用できます。

そのためには、Cisco 製ルータでポリシーベースルーティング (PBR) を設定し、透過プロキシ設定を使用して IWSS をネットワークに組み込みます。適用するポリシーは以下のとおりです。

ポリシー1 条件 :

- パケットが IWSS サーバから送信された場合
- パケットの宛先がポート 80/tcp またはポート 443/tcp である場合

処理 : パケットをインターネットにルーティングする

ポリシー2 条件 :

- パケットがローカルエリアネットワークから送信された場合 (IWSS サーバ以外)
- パケットの宛先がポート 80/tcp またはポート 443/tcp である場合
- IWSS サーバから送信されたパケットでない場合

処理 : パケットを IWSS プロキシポートへ転送する

ポリシーベースルーティングの詳細については、『Cisco Online Configuration Guide』を参照してください。

注意 : IWSS では、このセットアップを実装する際に、IWSS を透過プロキシに設定します。詳細については、24 ページの「ICAP 対応のプロキシを使用する」を参照してください。

HTTP サーバまたは FTP サーバを保護する

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

- /etc/iscan/ にある IWSSPIProtocolHttpProxy.pni ファイル内の [http] セクションの次のパラメータを変更します。
  - self_proxy=reverse — 動作モードを指定します。
  - reverse_server — 保護する HTTP サーバの IP アドレスを指定します。
  - reverse_server_port — 保護する HTTP サーバの TCP ポートを指定します。

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、[main]/secondaryport 設定パラメータで指定されているポートで外部からの (HTTPS) 接続を受け付けます。さらに、このトラフィックに対してはウイルスチェックを行わず、保護サーバのポート 443 へ直接転送します。

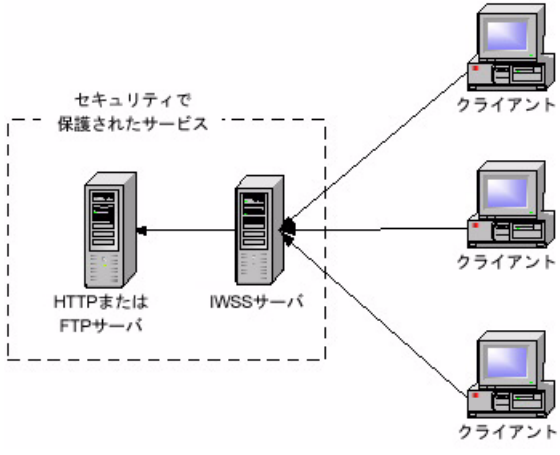

図 A-2.　専用サーバの保護

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

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

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。

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

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 4 章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、IWSS には以下のような内部キャッシュが備わっています。

- 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、数百人のユーザのグループメンバーシップ情報を保存できます。初期設定では、このキャッシュのエントリは、48 時間またはキャッシュが一杯になるまで (最も古いエントリから置き換えが始まる時点まで) 有効です。このキャッシュ内のエントリの生存期限 (TTL) は、intscan.ini 設定ファイルの [user-identification] セクションにある「user_groups_central_cache_interval」パラメータで設定できます。
- クライアント IP アドレスとユーザ ID の関連付けキャッシュ — このキャッシュでは、クライアントの IP アドレスは、その IP アドレスで最近認証されたユーザに関連付けられます。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 (初期設定で HTTP の場合は 15 分、ICAP の場合は 90 分) 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 IP アドレスとユーザとを IWSS が 1 対 1 で特定できることが条件となります。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または無効にするには、intscan.ini の [user-identification] セクションにある「enable_ip_user_cache」パラメータを変更します。このキャッシュの TTL を変更するには、「ip_user_central_cache_interval」パラメータを時間単位で設定します。たとえば、30 分の TTL を作成するには「0.5」と入力します。
- ユーザ認証キャッシュ — このキャッシュを使用すれば、Keep-Alive 接続にて複数の HTTP 要求が渡されたとき、2 回目以降は再認証する必要がなくなります。ユーザから持続接続を介して認証情報を渡されたとき、IWSS は、そのエントリ (クライアントの IP アドレスとクライアントのユーザ名) をユーザ認証キャッシュに追加します。したがって、それ以降、同じ接続を経由して渡された要求は再認証されません。クライアント IP アドレスとクライアントのユーザ名は、それぞれ、「クライアント IP とユーザ ID の関連付けキャッシュ」および「ユーザグループメンバーシップキャッシュ」に対応しています。したがって、IWSS は、これら両方のキャッシュから対象ユーザの接続情報を取得できます。

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 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 認証が有効な時は冗長ログを無効にする

サーバのパフォーマンスを向上するため、LDAP が有効になっているときは、intscan.ini ファイルの [http] セクションで冗長ログ (「verbose」パラメータ) 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。

TCP/IP スタックの調整

ネットワークトラフィック負荷の大きい環境で IWSS を効率的に実行するには、/etc/sysctl.conf ファイルで以下の値を変更して、TCP/IP スタックを調整します。

- net.ipv4.netfilter.ip_conntrack_max = 1048576

  注意： 上記のパラメータを調整するのは、「ip_conntrack」カーネルモジュールを使用している場合のみです。現在使用しているすべてのカーネルモジュールを確認するには、「lsmod」コマンドを実行します。

- net.ipv4.tcp_max_tw_buckets=360000

- net.ipv4.tcp_tw_recycle=1
- net.ipv4.tcp_tw_reuse=1

これらの変更を確認するには、sysctl -p コマンドを実行します。

適切なプロセス / スレッド値を設定する

それぞれの環境に合わせて IWSS http デーモンを調整し、パフォーマンスを向上することができます。このハイブリッドモードデーモンは、スレッドとプロセスの組み合わせに基づいて作業負荷を分散します。デーモンを調整するには、各環境におけるピーク時の同時接続数を把握しておくことが重要です。

デーモンが実行する合計スレッド数 (max_tpc_proc * max_threads_per_proc) は、IWSS インスタンスが処理すると予想されるピーク時接続数より大きい値でなければなりません。たとえば、ピーク時の平均的な同時セッション数が 2,000 であるとすると、これに合わせて、初期設定の max_tpc_proc 値を大きくする必要があります (max_tpc_proc = 5, max_threads_per_proc = 500)。

スレッド数とプロセス数について

- プロセスあたりのスレッド数 (max_threads_per_proc) が 500 以下の場合に、最適な IWSS パフォーマンスを得られます。
- 環境内のメモリに制約がなければ、max_tpc_proc の値を大きくし、max_threads_per_proc には、できるだけ 250 に近い値を指定することをお勧めします。
- スレッド数を 1 つ増やすごとに、必要なメモリが約 160 ～ 500KB 増大します。

注意： max_tpc_proc または max_threads_per_proc を変更した場合は、すべての IWSS デーモンプロセスを再起動して変更を適用する必要があります。

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] → [IWSS 設定] → [データベース] の [データベース設定] で、データベース設定が適切であることを確認してください。問題が解決されない場合は、etc/iscan/odbc.ini ファイルに指定されている権限が正しいことを確認してください。

テクニカルサポートに問い合わせる前に

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

インストールに関する問題

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

1. 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 UNIX 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。
- **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。
- **CDT 準拠設定 / プラグイン情報** — Trend Micro Control Manager エージェントや MCP エージェントなど、新しいコンポーネントを追加した結果として、CDT に加えられた変更に関する情報。

2. まず、以下の 1 番目のディレクトリにコアファイルが作成され、その後、2 番目のディレクトリに移動されます。

   - /etc/iscan/iwss/
   - /etc/iscan/iwss/UserDumps

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

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)。
   - **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。
   - **intscan.ini** ファイルの [ftp] セクションおよび [http] セクションで、「**log_trans=yes**」と設定します。

4. Web コンソールで [概要] → [検索] 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。

追加テスト

この付録では、次の項目について説明します。

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。

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. Trend Micro InterScan Web Security Suite (以下、IWSS) 管理コンソールのメインメニューから [HTTP] → [ウイルス検索ポリシー] 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/anti_virus_test_file.htm

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、メインメニューから [HTTP] → [HTTP 検索] → [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。

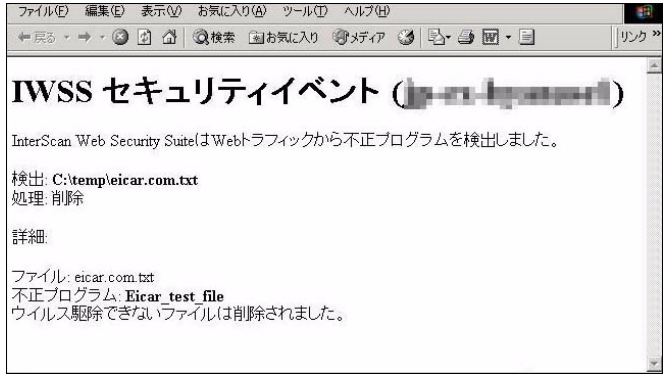

図 C-1.　EICAR テストウイルスを検出したことを示す警告画面

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/anti_virus_test_file.htm
   ```

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。

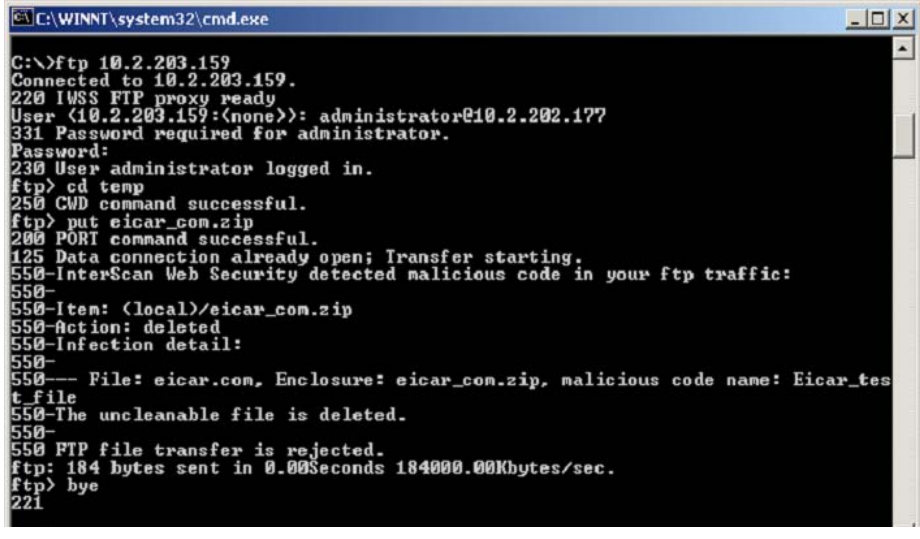

図 C-2. eicar_com.zip でウイルスが検出されたことを示す警告メッセージ

URL ブロックをテストする

URL ブロックをテストする前に、Web クライアントの HTTP プロキシが 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 [HTTP] → [設定] → [プロキシ検索] の順に選択し、依存モードを有効にします。プロキシアドレスとポート番号を入力します。

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] → [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] フィール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。

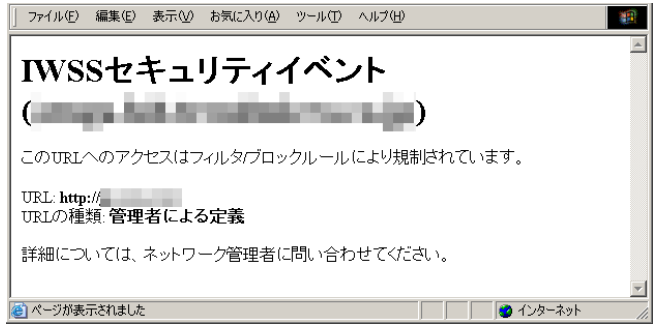

図 C-3. URL ブロックの警告メッセージ例

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

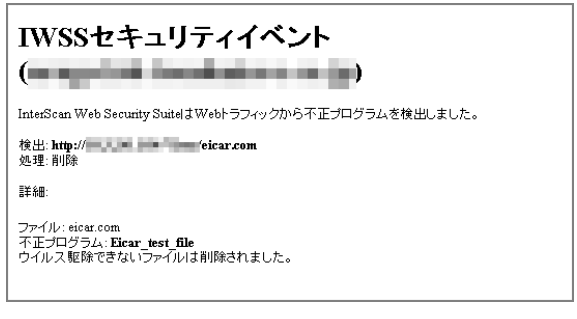

図 C-4. ウイルス検出の警告メッセージ例

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) を変更するには、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。

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. [HTTP] → [URL フィルタ] → [設定] の順に選択します。
2. [承認する URL リスト] 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。

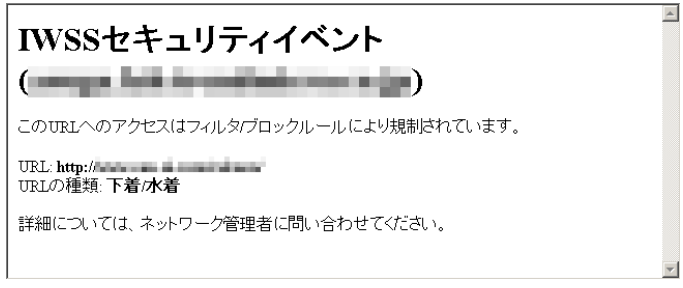

図 C-5. URL フィルタが適切に設定されている場合に表示されるメッセージ

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、[概要] をクリックします。
2. [検索] タブをクリックします。
3. [HTTP 検索] チェックボックスをオンにして、スパイウェアカテゴリの検索を有効にします。
4. [HTTP] → [ウイルス検索ポリシー] の順に選択します。
5. [スパイウェア] 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。
6. [処理] タブをクリックします。
7. [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。
8. [保存] をクリックします。

9. 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。

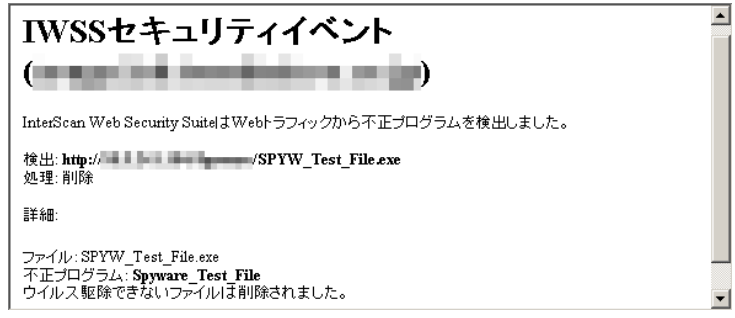

図 C-6. [削除] 処理を指定した場合のスパイウェア検出メッセージ例

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] → [URL アクセス設定] → [URL ブロック] の順に選択します。
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. [パターンファイルによる規制 (フィッシング対策)] タブをクリックします。
4. [ブロックするフィッシング URL カテゴリ] で、4 つのカテゴリ ([フィッシング]、[スパイウェア]、[ウイルス流布]、[不正サイト]) をすべて選択します。
5. [保存] をクリックします。

6. 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。

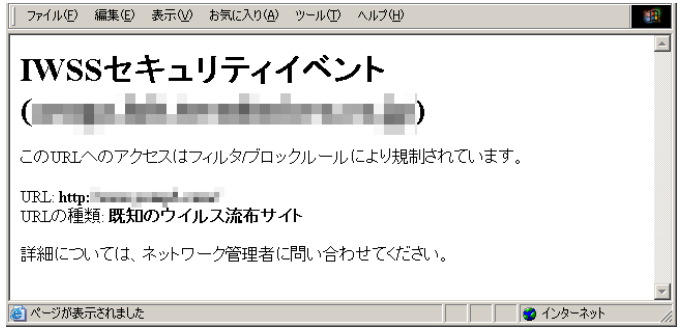

図 C-7. フィッシングサイトの検出を知らせるメッセージの例

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. 必要に応じて、[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。

IntelliTunnel をテストする

IntelliTunnel をテストするには

1. 最新の Windows Live メッセンジャーを http://get.live.com/messenger/overview からダウンロードします。
2. Windows Live メッセンジャーをインストールします。
3. IntelliTunnel を設定します。
   a. [HTTP] → [IntelliTunnel] の順にクリックします。
   b. 新しいポリシーを作成するか、既存のポリシーを開きます。
   c. [MSN Messenger] を選択します。
   d. [保存] をクリックします。
   e. ポリシー一覧画面に戻り、IntelliTunnel が有効になっていることを確認して、[ポリシーの配信] をクリックします。
4. 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] の順にクリックします。

c. [接続] タブをクリックします。

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] フィールドに、IWSS の IP アドレスを入力します。

g. [ポート番号] フィールドに、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 [HTTP] → [設定] → [プロキシ検索設定] → [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。

i. Internet Explorer を閉じます。

5. Windows Live メッセンジャーにログインします。

   現時点では Windows Live メッセンジャーにサインインできなかったことを知らせるエラーメッセージが表示されます。

6. IntelliTunnel を無効にします。

   a. [HTTP] → [IntelliTunnel] の順にクリックします。

   b. ポリシーを開きます。

   c. [MSN Messenger] を選択解除します。

   d. [保存] をクリックします。

   e. 該当するポリシーを選択して、[ポリシーの配信] をクリックします。

7. Windows Live メッセンジャーにログインします。

   Windows Live メッセンジャーが動作する事を確認します。

注意： Windows Live メッセンジャーでは Internet Explorer のプロキシ設定が使用されるので、ファイアウォールやネットワークなどを変更しなくても、このテストを実行できます。他のインスタントメッセージングアプリケーションでは、Internet Explorer のプロキシ設定が適用されない可能性があります。その場合、標準ポートがブロックされたときはポート 80 に戻すだけです。

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。

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。

インストール時に、ハードディスクをパーティションで区切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。

- サービス拒否 (DoS) 攻撃に備えて、ログファイル専用のパーティションを作成します。

注意： Trend Micro InterScan Web Security Suite の初期設定では、/etc/iscan ディレクトリにログファイルが保存されます。インストールが完了したら、ログファイルの場所を移動する必要があります。

- 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。
- インストールプロセスでは、パスワードを入力する必要があります。一般的な注意事項に従って、パスワードを設定してください。たとえば、数字、特殊文字、および大文字で構成されたパスワードを設定します。
- 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 Security Patch をダウンロードできます。

   - Red Hat Linux: http://www.redhat.com/security/
   - SuSE: http://www.suse.com/us/support/download/updates/index.html

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、Solaris では init s 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。

UNIX セキュリティの脆弱性トップ 10

以下は、UNIX のセキュリティで最も問題になる脆弱性トップ 10 です。Linux でもほぼ同様です。

1. Remote Procedure Calls (RPC)
2. Apache Web サーバ
3. セキュアシェル (SSH)
4. Simple Network Management Protocol (SNMP)
5. File Transfer Protocol (FTP)
6. R-Services -- Trust Relationships
7. Line Printer Daemon (LPD)
8. Sendmail
9. BIND/DNS
10. 一般的な UNIX 認証 - パスワードのないアカウント、脆弱なパスワードのアカウント[1]

1. 出典 : SANS Institute (www.sans.org) 2002 年 12 月

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。

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/

上記の URL にアクセスすると、[最新版ダウンロード] 画面が表示されます。

Trend Micro InterScan Web Security Suite のリンクをクリックして、IWSS の [最新版ダウンロード] ページを開きます。スクロールダウンして利用可能な 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

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

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

サポートサービスについて

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

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

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、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。

中小 / 中堅企業のお客さま

http://esupport.trendmicro.co.jp/supportjp/smb/search.do

大企業のお客さま

http://esupport.trendmicro.co.jp/supportjp/enterprise/search.do

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

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

セキュリティ情報

セキュリティ情報の入手先

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

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

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

セキュリティ情報 Web サイトでは、次の情報を閲覧できます。

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

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

トレンドマイクロへのウイルス解析依頼

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

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

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

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

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

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

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

ウイルス解析サポートセンター「TrendLabs」

トレンドマイクロのウイルス解析サポートセンター「TrendLabs」(トレンドラボ) は、フィリピンセンターを本部として、米国、日本、台湾、ドイツ、アイルランド、中国の各国センターで構成されています。24 時間体制でウイルスの活動を監視するウイルス解析エンジニアを含む 800 名以上 (2006 年 1 月現在) のスタッフが、セキュリティに関する最新の情報を収集し、高品質なサービスとソリューションを迅速かつ効果的に世界各国のトレンドマイクロのパートナーとお客さまに提供しています。

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

よくある質問

Flash を使用した Web ページが表示されない場合の回避方法

A. 「配信前に検索」機能を有効にしている場合

IWSS の HTTP 検索において、「サイズの大きいファイルの処理」機能の「配信前に検索」を有効している場合、ブラウザのタイムアウトを防止するため、クライアントにダウンロードの進行状況を表すページ (プログレスページ) が渡されます。Flash の場合このプログレスページがブラウザの Flash プラグインへ渡されますが、プラグインでは解釈できないため、本現象が発生します。

解決方法

設定ファイル intscan.ini の [http] セクションにある skip_type_intermediate パラメータに以下のように記述してください。

```
[http]

skip_type_intermediate=application/x-shockwave-flash text/html
text/plain
```

上記パラメータで設定した値が、レスポンスヘッダに含まれる Content-Type と一致した場合、クライアントへのダウンロード時にプログレスページが表示されなくなります。

Flash コンテンツの場合に付加される主な Content-Type は以下のようなものがあります。

- application/x-shockwave-flash
- text/html
- text/plain
- flv-application/octet-stream
- application/octet-stream

> **注意：** application/octet-stream については、汎用的に使用されるため推奨はしません。

注意： 上記の設定をした場合、プログレスページが表示されないため、大きな容量のファイルをダウンロードする際にタイムアウトが生じる可能性があります。

B. コンテンツの容量が大きく、タイムアウトが発生している場合

IWSS を介して大きな容量の Flash コンテンツをダウンロードした場合、タイムアウトが発生し、ページが正しく表示されない可能性があります。

解決方法

設定ファイル intscan.ini の [http] セクションの client_skip_content のパラメータに以下のように記述ください。

```
[http]

client_skip_content= x-flash-version: 9,x-flash-version:
8,x-flash-version: 7
```

上記のパラメータは、クライアントが付加するリクエストヘッダに特定の文字列が含まれる場合に、要求したデータを検索除外する設定となります。

上記の場合、リクエストヘッダに「x-flash-version: 9」または「x-flash-version: 8」、「x-flash-version: 7」が含まれる際の応答データは検索除外され、正常に Flash ストリーミングのデータを表示できるようになります。

注意： x-flash-version は、クライアントブラウザの flash プラグインのバージョンに応じて設定を変更してください。

HTTPS サイトへのログオンや検索処理に失敗してしまう場合の回避方法

HTTPS を使用する通信の場合ウイルス検索は行いませんが、リクエストやデータの中継は行われます。そのため、Web サーバ側での処理に時間がかる場合、タイムアウトが発生し HTTPS サイトが表示できない場合があります。

解決方法

タイムアウト値の初期設定値は 30 秒となっており、この値を増やすことにより回避できます。

intscan.ini ファイルの [main] セクションにある「timeout」パラメータを変更します。

```
[main]
timeout=30
```

* 単位は秒です。

タイムアウト値の設定は、お客さまの環境と Web サーバ側の相互の環境に依存しますので、環境に合わせてタイムアウト値を調整してください。

Windows Update や Adobe 社ソフトのアップデートに失敗する問題について

この問題は、タイムアウト防止機能の「配信前に検索」を設定している場合にタイムアウトを防止するために使用するプログレスページがブラウザのプラグインなどに送信された場合、プラグインがプログレスページを解釈することができずにダウンロードに失敗する場合があります。

解決方法

このような現象が発生した場合には、該当の URL のホスト名を検索除外として設定してください。以下に、お問い合わせの多い "Adobe Download Manager" と "WindowsUpdate" について、検索除外を設定する方法を紹介します。

1. 設定ファイル intscan.ini をテキストエディタで開き、[http] セクションの client_skip_content パラメータに以下値を設定します。

   - WindowsUpdate の場合は以下を追加

   ```
   Host: c.microsoft.com,Host: crl.microsoft.com,Host:
   download.windowsupdate.com,Host:
   office.microsoft.com,Host: update.microsoft.com,Host:
   v4.windowsupdate.microsoft.com,Host:
   v5.windowsupdate.microsoft.com,Host:
   v5stats.windowsupdate.microsoft.com,Host:
   W2KSP4.microsoft.com,Host:
   w2ksp5.windowsupdate.microsoft.com,Host:
   windowsupdate.com,Host: windowsupdate.microsoft.com,Host:
   wustat.windows.com,Host: www.download.windowsupdate.com,
   ```

   - Adobe Download Manager の場合は以下を追加

   ```
   Host: ardownload.adobe.com,Host: download.adobe.com
   ```

2. 変更した intscan.ini を保存します。
3. HTTP 検索デーモンまたはサービスを再起動します。

設定ファイル intscan.ini について

intscan.ini は、UNIX/LINUX の場合 /etc/iscan/intscan.ini に、Windows の場合 C:¥Program Files¥Trend Micro¥IWSS¥intscan.ini に保存されています。作業前には、設定ファイルのバックアップをお願いします。また、設定ファイルの編集後、設定を有効にするためには、HTTP/FTP 検索のデーモンやサービスを再起動する必要があります。

アクティベーションコードについて

アクティベーションコードには、体験版および製品版の 2 種類があります。体験版のアクティベーションコードにはあらかじめ使用期間の情報が設定されており、使用期限を過ぎると製品を使用できなくなります。製品版のアクティベーションコードをお使いの場合、製品ライセンス契約の情報をインターネット経由で取得し、ライセンス契約期間内であれば製品をご利用いただけます。

インターネットに常時接続されている環境の場合、有効期限は自動的に更新されますか。

回答 : はい。有効期限情報は自動的に更新されます。InterScan WSS はインターネットを経由して定期的にトレンドマイクロのライセンス認証サーバより有効期限情報の取得を行います。

アクティベーションコードの有効期限が近づいています。有効期限経過後に発生する機能制限について教えてください。

回答 : アクティベートせずにこの期間を経過した場合、パターンファイル / 検索エンジンのアップデート (Trend Micro Control Manager からの配信含む) 機能が無効になります。体験版の場合、有効期限が切れるとアップデートと検索機能の両方が無効になります。

アクティベート後、ハードウェア構成の変更 /IP アドレスの変更を行いました。再びアクティベートを行う必要はありますか。

回答 : 一度アクティベート処理が完了した場合、有効期限が経過するまで再アクティベートを行う必要はありません。ハードウェア構成の変更、IP アドレスの変更を行った場合においても再アクティベートの必要はありません。

索引

英数字

あ

か

ま

や

ら