Trend Micro
InterScan Web Security Suite™

Linux 版

安心を、ひとつ上のステージへ。

TREND MICRO™

管理者ガイド

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。本ドキュメント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。

TRENDMICRO、ウイルスバスター、ウイルスバスター On-Line-Scan、PC-cillin、InterScan、INTERSCAN VIRUSWALL、ISVW、InterScanWebManager、ISWM、InterScan Message Security Suite、InterScan Web Security Suite、IWSS、TRENDMICRO SERVERPROTECT、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、GateLock、VSAPI、eDoctor、eManager、Trend Micro Policy Server、トレンドマイクロ・プレミアム・サポート・プログラム、Certified Rescue Partner、License for Enterprise Information Security、LEISec、Trend Park、Trend Labs、Trend Micro Enterprise Protection Strategy、RBL+、Phish Checker、InterScan Gateway Security Appliance、Trend Micro Network VirusWall、Network VirusWall Enforcer、Trend Flex Security、EPS、Trend Micro EPS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 © 1998-2008 Trend Micro Incorporated. All rights reserved.

P/N: IWSSLX-AE0300 (2008/5)

目次

はじめに 13
ドキュメント 14
対象読者 15
ドキュメントの表記規則 15

第 1 章　本製品について 17
新機能 18
Web レピュテーション 18
サポート診断用のシステム情報の容易な収集 19
圧縮ファイル内での実際のファイルタイプによるブロック 19
IntelliTunnel 19
URL フィルタカテゴリの直接選択 20
リアルタイム統計情報とアラート 20
設定可能なしきい値警告 21
SNMP トラップとイベント通知 21
リバースプロキシのサポート 21
ログとレポート 21
その他のレポート情報 22
HTTP と FTP のセキュリティ上の脅威の概要 23
主な利点 23
総合的な Web セキュリティ 24
集中管理と連携 24
拡張性と柔軟性 24
スパイウェア対策 25

ICAP 1.0 対応キャッシュサーバとの連携 26
最新のウイルス予防 26
主な機能 27
HTTP ウイルス検索 27
アプレット /ActiveX 対策 27
URL フィルタ 27
アクセス割り当てポリシー 28
URL アクセス管理 28
さまざまなユーザ識別方法 28
サーバとポートのアクセス管理制限 28
FTP 検索 29
レポートとログ 29
通知 29
IWSS の複数インストールのサポート 30
IWSS のテクノロジ 31
アップデート可能なコンポーネント 31
アップデート 32
ウイルスパターンファイル 32
フィッシングパターンファイル 34
スパイウェアパターンファイル 34
検索エンジン 36
コンポーネントのバージョン情報 37
トレンドマイクロの推奨設定について 38
ダメージクリーンナップサービスについて 39
ダメージクリーンナップ要求の発行 40
IWSS アーキテクチャ 41
IWSS のモジュール 41

サービス 41
予約タスク 42

第 2 章 使用開始 45

使用開始時のチェックリスト 46
IWSS Web コンソールを開く 48
Web コンソールへのログイン 48
インストール後の初期設定 49
プロキシ検索の設定 53
IWSS のアップデート 54
HTTP トラフィックフローの有効化の確認 54
EICAR テストウイルスによる IWSS のテスト 55

第 3 章 アップデート 57

プロキシ設定 (アップデート用) 58
手動アップデート 59
強制手動アップデート 59
予約アップデート 60
アップデートの操作方法 61
アップデート成否の確認 61
アップデート通知 61
アップデートのロールバック 61
パターンファイルの削除 62

第 4 章 ポリシーについて 63

ポリシーの仕組み 64
初期設定のグローバルポリシーとゲストポリシー 66

ゲストポリシーについて 66
ポリシーの配信 67
ユーザの識別方法について 67
「識別なし」の使用 68
IP アドレス 68
ホスト名 68
グループユーザまたはグループ名の使用 70
HTTP 検索に関する注意 81
Java アプレット /ActiveX 対策に関する注意 83
アプレット /ActiveX 対策の仕組み 84
URL フィルタに関する注意 87
URL フィルタの仕組み 88
圧縮ファイルの処理 89
サイズの大きいファイルの処理 89
隔離ファイルの暗号化 89
スパイウェアの検索 90
IntelliTunnel に関する注意 90
インスタントメッセンジャプロトコルについて 90
認証接続プロトコルについて 91
アクセス割り当てポリシーに関する注意 92
URL アクセス管理に関する注意 93
FTP 検索に関する注意 95
FTP 設定 96

第 5 章 ユーザ識別方法とゲスト用ポートの設定 99

ユーザ識別方法の設定 100
IP アドレス 100

ホスト名 100
ユーザ / グループ名 (LDAP) 102
ゲストポリシーのゲスト用ポートの有効化 107

第 6 章 HTTP 検索の設定 109
HTTP 検索の有効化の確認 110
HTTP 検索ポリシーの作成 110
Web レピュテーションルールの指定 111
Web レピュテーション設定 111
URL キャッシュのクリア 114
HTTP ウイルス検索ルール 115
スパイウェア検索ルール 122
ウイルス検出時の処理設定 123

第 7 章 アプレット /ActiveX 対策の設定 125
アプレット /ActiveX 対策の有効化 126
アプレット /ActiveX 検索ポリシーの追加と変更 126
アプレット /ActiveX 対策の設定 132
アプレットの署名の妥当性を検査するための証明書の追加 133
アプレットの再署名 135
ActiveX の署名の妥当性検査 136
アプレット処理のためのデジタル証明書の管理 137
クライアント側アプレットのセキュリティ通知 140

第 8 章 URL フィルタおよび IntelliTunnel ポリシー 143
URL フィルタポリシーの管理 144
URL フィルタの有効化 144

新しいポリシーの作成 145
URL フィルタの設定 147
URL カテゴリの見直しの依頼と URL 検索 147
URL フィルタの除外設定 149
業務時間および業務時間外の設定 151
新しい IntelliTunnel ポリシーの作成 153

第 9 章 アクセス割り当てと URL アクセス設定 155
アクセス割り当てポリシーの管理 156
URL アクセス管理の設定 157
信頼する URL の設定 157
URL のブロック 159

第 10 章 FTP 検索 167
FTP 設定 168
FTP 検索オプション 168
FTP トラフィックおよび FTP 検索の有効化 169
FTP 検索の設定 170
ウイルスに対する検索処理の設定 172
FTP アクセス管理設定 172
クライアント IP による設定 173
許可されたサーバ IP のリスト 173
宛先ポートによる設定 174

第 11 章 プロキシ検索設定 177
プロキシ設定および関連するその他の設定 178
プロキシ設定 178

プロキシに関する設定 181
ネットワーク設定および負荷の処理 183
ゲストアカウントの有効化 (LDAP のみ) 183
ICAP プロキシの設定 184

第 12 章 管理タスク 185
隔離ディレクトリの設定 186
データベース接続の確認 186
Web コンソールパスワードを変更する 188
ブラウザコンソール通信の暗号化 (HTTPS) 189
IWSS およびオプション機能のアクティベーション 192
ログインアカウントの管理 193
アクセス権について 193
ログインアカウントを追加する 193
監査ログファイル 194
IWSS サーバファームの設定 194
Trend Micro Control Manager エージェントの登録 195

第 13 章 通知 197
通知について 198
受信者設定 199
通知の変数 / パラメータ 199
通知の設定 202

第 14 章 レポートおよびログ 211
レポートについて 212
レポートの種類 212

ブロックイベントレポート 213
個別 / ユーザ別レポート 213
トラフィックレポート 214
スパイウェアレポート 214
クリーンナップレポート 214
レポート設定 215
レポートの作成対象 215
レポートの種類 215
オプション 215
その他のレポート設定 216
レポートの生成 216
リアルタイムレポート 216
予約レポート 219
レポートのカスタマイズ 220
ログについて 222
データ記録のオプション 223
ログのクエリおよび表示 224
ログの削除 232
ログの設定 232
ログファイルの命名規則 234
CSV 形式でのログおよびレポートデータの出力 236

付録 A　ファイルタイプと MIME コンテントタイプの対応..... 237

付録 B　設定ファイル..... 241
プロトコルハンドラ 243
検索モジュール 243

付録 C　OpenLDAP 245
OpenLDAP サーバ側の設定 246
ソフトウェアパッケージの従属関係 246
設定ファイル 246
ツール 252
カスタマイズされた属性の等価テーブル設定 255
LDIF 形式のサンプルエントリ 257
設定のサンプル 258

索引 261

はじめに

Trend Micro InterScan Web Security Suite (以下、IWSS) 3.1 Linux 版管理者ガイドへようこそ。本書では、IWSS の設定オプションについて詳しく説明します。ソフトウェアをアップデートして最新のリスクから保護する方法、セキュリティ上の目標を達成するためのポリシーの設定および使用方法、ログとレポートの使用方法に関する項目が含まれています。

本章では、次の項目について説明します。

- 14 ページの「ドキュメント」
- 15 ページの「対象読者」
- 15 ページの「ドキュメントの表記規則」

ドキュメント

IWSS には、本書のほかに次のドキュメントが用意されています。

- **インストールガイド** (導入に関する情報を含む) — 本書では、IWSS を紹介し、インストール計画、実装、および設定の各作業を案内し、インストール後の主な設定作業について説明することで、IWSS の導入と運用を支援します。また、害のないテストウイルスを使用した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。
- **オンラインヘルプ** — オンラインヘルプの目的は、製品の主なタスクに関する操作手順、使用方法のアドバイス、および有効なパラメータの範囲、最適な値など、実際に使用する場面に固有の情報を提供することです。オンラインヘルプには、IWSS の管理コンソールからアクセスできます。
- **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や注意事項が記載されています。新機能、設置のヒント、既知の問題、およびリリース履歴が含まれています。

  各種ドキュメントの最新版は、次の Web サイトから入手できます。

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

- **製品 Q&A Web サイト** — 製品 Q&A Web サイトでは、問題解決およびトラブルシューティング情報に関するオンラインのデータベースを提供します。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

対象読者

IWSS のドキュメントは、大企業および中規模企業の IT 責任者およびメール管理者を対象としています。また、次の技術を含めて、メールメッセージングネットワークに精通していることを前提としています。

- SMTP プロトコルおよび POP3 プトロコル
- Message Transfer Agent (MTA)

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

本製品について

本章で説明する内容には、次の項目が含まれます。

- 18 ページの「新機能」
- 23 ページの「HTTP と FTP のセキュリティ上の脅威の概要」
- 23 ページの「主な利点」
- 27 ページの「主な機能」
- 31 ページの「IWSS のテクノロジ」
- 38 ページの「トレンドマイクロの推奨設定について」
- 41 ページの「IWSS アーキテクチャ」

新機能

この項では、Trend Micro InterScan Web Security Suite (以下、IWSS) 3.1 Linux 版の新機能について説明します。

Web レピュテーション

Web レピュテーションは、新たに出現する Web の脅威からエンドユーザを保護します。Web レピュテーションにより、Web フィルタ機能が強化され、ネットサーフィンがさらに快適になります。IWSS の Web レピュテーション検索では、オプションの URL フィルタモジュールが使用する URL カテゴリ情報を返すため、ローカルに格納された URL データベースは使用されません。

また、Web レピュテーションでは、レピュテーションスコアを URL に割り当てます。IWSS は、URL にアクセスするたびに Web レピュテーションにレピュテーションスコアを問い合わせ、スコアとユーザの定義した感度レベルとの比較に基づき、必要な処理を行います。

IWSS では、感染した URL についてフィードバックが提供可能なため、Web レピュテーションデータベースの精度を上げるのに役立ちます。このフィードバックには、製品名とバージョン、URL、ウイルス名が含まれます (フィードバックには、IP アドレス情報は含まれません。フィードバックはすべて匿名で扱われ、企業の情報は保護されます)。IWSS では、既存の Web アクセスポリシーに影響を与えずに Web レピュテーションの有効性を監視することもできます。結果は、URL ブロックログ、および [概要] 画面の [概要レポート] タブで確認できます。

Web レピュテーションの詳細については、111 ページの「Web レピュテーションルールの指定」および 111 ページの「Web レピュテーション設定」を参照してください。

Web レピュテーションに基づくファーミング対策およびフィッシング対策

IWSS では、Web レピュテーションを通じてファーミング対策とフィッシング対策が提供されます。初期設定では、いずれの機能も有効です。

- フィッシング対策を使用すると、個人情報を騙し取ろうとするフィッシングサイトへの Web アクセスをブロックします。
- ファーミング対策を使用すると、通常、金銭上の個人情報を騙し取る目的の Web サイトにリダイレクトしようとする試みをブロックします。

サポート診断用のシステム情報の容易な収集

トレンドマイクロのサポートに問い合わせる際、迅速に情報を送信できるように、ログ情報やシステム設定情報を容易に収集できるようになりました。[管理] → [サポート情報] → [サポート情報] 画面の [システム情報ファイルの生成] ボタンをクリックすると、IWSS のシステム情報のスナップショットを撮ることができます。詳細については、オンラインヘルプを参照してください。

圧縮ファイル内での実際のファイルタイプによるブロック

IWSS では、zip ファイルなど圧縮ファイルの内容に対して、ファイルタイプによるブロックを適用します。したがって、実行可能ファイルをブロックするポリシーによって、実行可能ファイルを含む zip ファイルもブロックされます。

IntelliTunnel

IWSS では IntelliTunnel 技術を使用して、ポート 80 を使用する不要なインスタントメッセージ (IM) のプロトコルや認証接続プロトコルをブロックします。動的にアップデート可能なパターンファイルを使用して、通常のブラウザトラフィックとポート 80 を経由した他の通信プロトコルを区別します。

詳細については、90 ページの「IntelliTunnel に関する注意」を参照してください。

URL フィルタカテゴリの直接選択

IWSS では、Web レピュテーションデータベースから「ギャンブル」、「ゲーム」、「出会い系」など 60 以上のカテゴリの URL にアクセスできます。

カテゴリは次の論理グループに含まれます。

- コンピュータ / 帯域幅
- コンピュータ / 危険
- コンピュータ / 通信
- アダルト
- ビジネス
- 社会
- 一般

特定のグループのカテゴリをすべて選択するか、またはグループを構成するカテゴリを表示して特定のカテゴリだけを選択することもできます。詳細については、147 ページの「URL フィルタの設定」を参照してください。

リアルタイム統計情報とアラート

IWSS には動的な統計機能が備わっており、管理者は IWSS システムの情報を「リアルタイム」で閲覧できます。リアルタイム統計情報は、[概要] 画面の [システムダッシュボード] タブにグラフや表で表示されます。次のような統計情報が含まれます。

- ハードディスクドライブ (静的な統計情報で、画面を開いたときにアップデートされる)
- 帯域幅
- 同時接続数
- CPU 使用率
- 物理メモリ使用率

設定可能なしきい値警告

ウイルスおよびスパイウェアのトラフィック、データベースおよびハードディスクドライブの大きさ、または帯域幅の使用率が指定したしきい値を超えた場合に発する警告を設定できます。詳細については、208 ページの「しきい値アラートの通知の有効化」を参照してください。

SNMP トラップとイベント通知

サードパーティのネットワーク監視ツールと連携できるよう、IWSS では SNMP トラップとして各種の通知をサポートしています。IWSS は、セキュリティの脅威の検出、セキュリティ違反、プログラムやパターンファイルのアップデート、サービス停止が発生するとトラップを送信します。詳細については、209 ページの「SNMP トラップ通知の有効化」を参照してください。

IntelliTrap で検出されたファイルは一種のセキュリティの脅威と見なされるので、HTTP 検索と同じ通知が使用されます。

リバースプロキシのサポート

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。

詳細については、180 ページの「リバースプロキシ」を参照してください。

ログとレポート

IWSS は、ゲートウェイのセキュリティ統計情報を示す多数のレポートを備えています。特定の期間にだけレポートを実行し、対象とするクライアントだけの情報を表示するようカスタマイズすることも可能です。レポートは次の 4 つに大別できます。

- ブロックイベントレポート
- トラフィックレポート
- スパイウェアレポート
- クリーンナップレポート

レポートは、データベース内の情報から生成されます。IWSS はログ情報をテキストのみのログ、テキストログとデータベース、またはデータベースのみのログに出力します。不要なログ情報がディスク空き容量を消費しないよう、古くなったログは即時または予定に従って定期的に削除できます。

その他のレポート情報

IWSS では、Web レピュテーション、ファーミング対策、およびフィッシング対策のレポートが [概要] 画面および URL ブロックレポートで表示されます。

- **[概要] 画面**: **[概要レポート] タブ**: 1 週間、および 28 日間に検出されたファーミングサイトの合計数は、他の Web の脅威同様にセキュリティリスクレポートで表示することができます。
- **レポート (リアルタイムおよび予約)**: レポート生成に使用される URL ブロックログに情報が記録されるので、ブロックされたファーミングサイトが次のレポートに表示されます。
  - 最もブロックの多い URL
  - 曜日別 URL ブロック数
  - 時間別 URL ブロック数

IWSS では、IntelliTrap アクティビティが次の領域にレポートされます。

- **[概要] 画面**: **[概要レポート] タブ**: IntelliTrap によって検出されたファイルは、レポート内で個別のリスクとして数えられます。
- **[概要] 画面**: **[検索] タブ**: IntelliTrap によって検出されたファイルは、頻度とともに「検索結果」リストに表示されます。
- **リアルタイムレポート**

HTTP と FTP のセキュリティ上の脅威の概要

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

ウイルスの大規模感染によって必要となる診断、復旧、生産性損失に伴うコストは、事前に対策することによって大部分が回避可能です。IWSS は、企業ネットワークの HTTP および FTP トラフィックをウイルスとその他の脅威から守る総合的なセキュリティ製品です。

ウイルス対策はもちろん、IWSS はその他のネットワークセキュリティ対策にも役立ちます。

- Web レピュテーションでは、潜在的に危険な Web サイト、特に既知のフィッシングサイトまたはファーミングサイトにアクセスする前に URL を調べます。
- オプションの URL フィルタ機能を使用すると、企業で禁止されたコンテンツを含む Web サイトへのアクセスをブロックします。
- オプションのアプレット /ActiveX 対策モジュールを使用すると、HTTP ゲートウェイにおけるデジタル署名をチェックし、禁止されている操作をクライアントで実行しようとするアプレットを監視して、不正なモバイルコードの脅威を回避します。

主な利点

IWSS は、組織の HTTP と FTP ゲートウェイトラフィックを強力に保護します。

総合的な Web セキュリティ

IWSS は、ウイルス、トロイの木馬、ワーム、フィッシング攻撃、スパイウェアなどのインターネット上の脅威をブロックするよう設計されています。これらの脅威は、不正プログラムを忍び込ませた Web ベースのメールと Web ページを通して企業ネットワークを攻撃します。IWSS は、攻撃を受ける媒体になりやすい HTTP と FTP トラフィックを検索し、これらの脅威を回避します。この HTTP/FTP に特化したソリューションがセキュリティの向上とスループットの高速化を実現します。これによって、Web の閲覧がいっそう改善されるようになります。

集中管理と連携

IT 管理者は、集中管理コンソールの Trend Micro Control Manager (以下、Control Manager) から IWSS とその他のトレンドマイクロ製品を簡単に操作できます。Control Manager を使用すれば、企業内にインストールされたトレンドマイクロのソフトウェアを 1 つのコンソールから管理できます。アクティビティを集中的に監視でき、ポリシーをすべてのセキュリティ層に同時に適用できます。リアルタイムのレポートと予約しておいたレポートを高度なグラフと表で表示することも可能です。このようにして、新しい脅威の発生時にも迅速な対策を講じることが可能です。

拡張性と柔軟性

IWSS はスタンドアロンによる設定をサポートするため、プロキシサーバの役割を果たすだけでなく、既存のプロキシサーバおよび Cisco 製 Network Appliance などの ICAP 対応のキャッシュサーバと連携できます。また、IWSS は複数の LDAP ディレクトリをサポートするため、IT 責任者が 1 台のパソコンからグループまでポリシーとルールを設定できるようになります。ウイルスパターンファイルと URL フィルタエンジンのアップデートのような日常的なタスクは、予約しておいて自動化できます。

スパイウェア対策

トレンドマイクロのスパイウェア対策技術は、スパイウェアとアドウェアのほか、ネットワークに支障を与えるハッキングツールやリモートアクセスツールをブロックするように設計されています。この新しい対策により、侵入者が個人情報や企業情報、パスワード、メールアドレスなどのデータを騙し取るのを防ぎます。それと同時にシステムリソースと使用可能な帯域幅を解放し、ネットワークのパフォーマンスを向上してスパイウェアによるシステム障害を軽減します (35 ページの「スパイウェアについて」を参照)。

フィッシング対策とファーミング対策

フィッシングでは、個人情報を騙し取ることを目的としたメールを発行します。このメールには、ユーザを偽の Web サイトに誘導する URL が含まれており、そのサイトにアクセスすると、パスワード、クレジットカード番号、銀行口座番号などの個人情報を更新するように要求されます。

ファーミングは、通常、金銭上の個人情報を騙し取る目的でユーザを偽の Web サイトにリダイレクトしようとします。ファーミングは、偽の情報を与えて DNS サーバを改ざんすることによって、ユーザの要求を意図せぬ場所にリダイレクトします。困ったことに、Web ブラウザには正規の Web サイトに酷似したサイトが表示されます。

注意 : フィッシング / ファーミング検出のソースは、脅威対策処理機能の中の Web レピュテーションおよびフィッシング対策 / ファーミング対策機能に基づくため、Web レピュテーションのポリシーのルールに含まれています。また、Web レピュテーションはグローバルレベルで有効になっていないと、ポリシーレベルで機能しないため、Web レピュテーションがグローバルレベルで無効になっていると、フィッシング対策 / ファーミング対策機能も無効になります。

ICAP 1.0 対応キャッシュサーバとの連携

キャッシュサーバには「1 回のウイルス検索で複数の要求に対応する」方法が採用されており、Web トラフィック輻輳の緩和と帯域幅節約に役立ちます。オープンプロトコルの、Internet Caching Acceleration Protocol (ICAP) を使用することで、キャッシュとウイルス監視機能をシームレスに連結できます。

最新のウイルス予防

IWSS はトレンドマイクロのウイルス対策技術に基づいて構築されており、ウイルス解析センター「TrendLabs」(トレンドラボ) に常駐する上級エンジニアチームの手によって 24 時間常時見守られています。これらのエンジニアがウイルスの活動状態を監視し、大規模感染予防ポリシーや最新のパターンファイルを提供することで、企業は大規模感染によって生じる損失と復旧コストを最小限に抑えることができます。

主な機能

HTTP と FTP ゲートウェイの安全性を守るには、IWSS の次の機能が役立ちます。

HTTP ウイルス検索

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

アプレット /ActiveX 対策

IWSS では、Java アプレット /ActiveX コントロールをブロックしたり許可したりして、インターネットからのモバイルコードのダウンロードにおけるセキュリティ脅威の問題に対応できます。IWSS には、Java アプレットの署名に使用する、信頼されるフラグ付きの証明書を管理する独自の証明局が含まれています。

さらに IWSS では、Java アプレットを計測処理し、クライアントのブラウザで実行中の Java アプレット動作を監視します。禁止する動作が実行された場合は、クライアントにこれを通知し、その動作を許可または拒否します。

URL フィルタ

IWSS の URL フィルタオプションを使用すると、「成人向け」、「ギャンブル」、「金融サービス」など、URL のカテゴリに基づいてポリシーを設定できます。ユーザが URL を要求すると、IWSS はまずその URL のカテゴリを検索し、設定されたポリシーに基づき URL へのアクセスを許可または拒否します。承認する URL のリストを定義することもでき、これらの URL はフィルタ処理されません。

アクセス割り当てポリシー

クライアントの Web アクセス量に上限を設定するため、IWSS ではアクセス割り当てポリシーを使用できます。ポリシー設定に応じて、クライアント側では 1 日あたり、1 週間あたり、または 1ヵ月あたりのアクセス量の上限に達するまでインターネットを閲覧できます。割り当てを超えると、設定期間内はアクセスがブロックされるようになります。

URL アクセス管理

IWSS では、信頼する URL を検索対象から除外することで、サーバの検索負荷を軽減できます。同様に、従業員に閲覧させたくないコンテンツの検索にサーバのリソースを使用しないように、URL をブロックすることもできます (URL ブロック)。

さまざまなユーザ識別方法

IWSS では、HTTP ウイルス検索、アプレット /ActiveX 対策、URL フィルタ、IntelliTunnel、アクセス割り当てに設定ポリシーを使用できます。ポリシーの適用範囲は、クライアント IP アドレス、ホスト名、LDAP ユーザ名またはグループ名のいずれかを使用して設定できます。

サーバとポートのアクセス管理制限

IWSS のセキュリティを強化するため、アクセス管理設定によって指定クライアントからのサーバアクセスに制限を設けます。同じように、不正目的のアクセスを軽減するために、ポートアクセスもブロックできます。

FTP 検索

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

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

レポートとログ

HTTP と FTP ゲートウェイのセキュリティに関する最新情報を提供するため、IWSS 各種のブロックイベントレポート、トラフィックレポート、スパイウェアレポート、クリーンナップレポートを生成するように設定されています。このレポートは即時に生成することも、毎日、毎週、毎月など予約によって生成することも可能です。ログとレポートのデータは、更に詳細に分析するためにカンマ区切り値 (CSV) のファイルに出力できます。ログが必要以上にディスク空き容量を消費しないよう、古くなったログは予約タスクによってサーバから削除できます。

通知

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

また、ネットワーク管理ツールで使用できるよう、IWSS から SNMP トラップとして通知を発行できます。

IWSS の複数インストールのサポート

複数の IWSS サーバを 1 台のコンソールから本格的に管理する方法は、Control Manager を介して実行されます。ただし、複数の IWSS サーバが同一のデータベースサーバにアクセスするように設定されている場合は、ポリシー (URL、アプレット /ActiveX、IntelliTunnel、アクセス割り当てポリシーなど) はすべてのサーバ間で共有されます。

管理コンソールの [IWSS サーバファーム] ページで「マスター」/「スレーブ」を指定する場合のみ、動的データ (一時的にブロックする URL のリストやスパイウェアに感染している疑われるクライアント IP アドレスのリスト) を複数の IWSS サーバ間で共有する方法を設定できます。

レポートとログは、ネットワーク上のすべての IWSS サーバを合わせた形で表示されます。

IWSS のテクノロジ

この項では、IWSS のテクノロジと、そのテクノロジを使用したネットワークの保護方法について説明します。

アップデート可能なコンポーネント

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

- **IntelliTunnel パターンファイル** — このファイルには、HTTP や SSL 認証要求を介してインスタントメッセージングプロトコルをトンネルするなど、ユーザが制御できる特定の HTTP 対話の「署名」が含まれています。新しい署名定義ファイルは、対象プロトコルに変更があるたびに、または新しいタイプの HTTP 対話が追加されるたびにリリースされ、通常、1 年に数回リリースされます。153 ページの「新しい IntelliTunnel ポリシーの作成」を参照してください。

  注意： IntelliTunnel の機能は、検索エンジンとは関係なく、独自の検索エンジンを使用するため、動的なアップデートはできません。

- **パターンファイル** — パターンファイルには、ウイルスパターンファイル、フィッシングパターンファイル、スパイウェアパターンファイル、IntelliTrap パターンファイル、および IntelliTrap 除外パターンファイルがあります。これらのファイルは、バイナリ「シグネチャ」や既知のセキュリティ上の脅威のパターンを格納しています。検索エンジンと同時に使用すると、それらがインターネットゲートウェイを通過する際に IWSS によって脅威が検出されます。新しいウイルスパターンファイルは週に数回提供されています。一方、フィッシングパターンファイルとスパイウェアパターンファイルはそれほど頻繁にはアップデートされません。

- **検索エンジン** — 各ファイルのバイナリパターンを解析し、それをパターンファイル内のバイナリ情報と比較するモジュールです。一致した場合は、そのファイルを不正なものとして判断します。

- **URL フィルタエンジン** － IWSS は、URL フィルタエンジンを使用して、トレンドマイクロ Web レピュテーション機能が提供するデータに基づく URL の分類およびレピュテーションの評価を実行します。初期設定の毎週のアップデートにより、URL フィルタエンジンを最新の状態にすることをお勧めします。

アップデート

アップデートは、多くのトレンドマイクロ製品に共通するサービスです。アップデート機能により、各製品はトレンドマイクロのアップデートサーバに接続し、パターンファイル、検索エンジン、URL フィルタエンジンなどのコンポーネントをダウンロードします。

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

ウイルスパターンファイル

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

トレンドマイクロのウイルス対策プログラムでアップデート機能 (詳細については 32 ページの「アップデート」を参照) を使用すると、新しいウイルスパターンファイルがサーバに用意されたことを検出できます。また、1 時間おき、1 日おき、1 週間おきなどに最新ファイルを取得するよう自動的にサーバにポーリングを予約しておくことも可能です。

検索の仕組み

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

パターンファイル名は次のとおりです。

```
lpt$vpn.###
```

は、パターンファイル番号を表す 3 桁の数字です (例 : 400)。同じパターンファイル番号で別のビルド番号のパターンファイルを識別します。また、999 より大きいパターンファイル番号にも対応しています。IWSS 管理コンソールには次の形式で表示されます。

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

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

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

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

ウイルスパターンファイルの差分アップデート

IWSS のアップデート機能は、ウイルスパターンファイルの差分アップデートに対応しています。毎回パターンファイル全体をダウンロードするのではなく、ファイルの新しい部分のみをダウンロードして既存ファイルに付加することができます。この効率的なアップデート方法により、ウイルス対策ソフトウェアのアップデート、およびお使いの環境へのパターンファイルの配信に必要な帯域幅を大幅に低減することができます。

フィッシングパターンファイル

正規の Web サイトを偽造して個人情報を騙し取ろうとするフィッシング詐欺が近年増加しているため、トレンドマイクロでは関連する URL を収集してフィッシングパターンファイルにその情報を取り入れています。フィッシングパターンファイルは、初期設定で /etc/iscan/phishB.ini に保存されます。フィッシングパターンファイルには、既知のフィッシング URL のリストが暗号化された形で格納されています。

スパイウェアパターンファイル

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

/etc/iscan/ssaptn.###

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

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

- **ロール番号** — パターンファイル番号が 999 を超えた回数を表します。桁数の最大は 5 桁です (0 ～ 21474)。
- **パターンファイル番号** — ssaptn.### のパターン拡張子と同じで、3 桁です (100 ～ 999)。

- **ビルド番号** — Patch またはリリースを表します。2 桁です (00 ～ 99)。

スパイウェアについて

IWSS が使用するパターンファイルには、コンピュータウイルスのほかに、多数の潜在的脅威に関する署名が含まれています。こういった脅威は、自己複製して拡散することはないので、ウイルスではありません。しかし、ユーザの知らないうちに個人情報を収集、転送したり、ポップアップウィンドウを表示したり、ブラウザのホームページを変更するなど、望ましくない処理や予測されない処理を実行することがあります。

IWSS は、次の脅威を検索するように設定できます。

- **スパイウェア** — ユーザが知らないうちに、またはユーザの承諾なしに、ひそかに情報を収集および転送するソフトウェア
- **ダイヤラー** — ユーザのモデムを通じて密かに課金式の電話番号や国際電話番号にダイヤルするソフトウェア
- **ハッキングツール** — 不正なハッキング目的に使用できるソフトウェア
- **パスワード解読アプリケーション** — コンピュータのパスワードおよびその他の認証スキームを無効にするために設計されたソフトウェア
- **アドウェア** — ユーザのブラウザまたはポップアップウィンドウにユーザを対象とする広告を表示するために、ユーザの Web 閲覧動作に関する情報を監視および収集するソフトウェア
- **ジョークプログラム** — ユーザを困らせたり不適切な警告を発したりするプログラム
- **リモートアクセスツール** — コンピュータへのアクセスが許可されるように設計されたソフトウェアで、多くの場合ユーザの承諾を得ていません。
- **その他** — 上記の分類に当てはまらないファイルこのうち一部は、不正な行動をとる可能性があるだけでなく、合法な目的を持つツールまたは商用ソフトウェアである場合があります。

検索エンジン

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

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

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

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

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

最新のリスクに対処するため、検索エンジンを最新に保つことが重要です。検索エンジンを最新に保つには、次の 2 つの方法があります。

1. ウイルスパターンファイルと呼ばれる検索エンジンのデータファイルの頻繁なアップデート。このファイルは、エンジンのコード自体を変更しなくてもエンジンによってダウンロードされ、読み込むことができます。

2. SQL Slammer のような複合的脅威の発生など、ウイルスの脅威の性質の変化に対処するエンジンソフトウェアの技術上のアップグレード

いずれの場合にも、アップデートは自動的に予約することも、手動で開始することもできます。

トレンドマイクロの検索エンジンは、International Computer Security Association (ICSA) などの国際的なコンピュータセキュリティ機関によって毎年認定されています。

検索エンジンのアップデートについて

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

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

検索エンジンの最新情報は、次の URL からご確認いただけます。

http://www.trendmicro.co.jp/download/engine.asp#prod_34

コンポーネントのバージョン情報

実行中のパターンファイル、検索エンジン、URL フィルタエンジン、プログラムビルドのバージョン情報を調べるには、メインメニューから [概要] をクリックします。使用しているバージョン情報が [検索] タブの [現在のバージョン] 列に表示されます。

トレンドマイクロの推奨設定について

現在、ほとんどのウイルス対策ソリューションは、潜在的な脅威に備えて検索するファイルを決定するにあたり、2 つのオプションを提供しています。最も安全なアプローチである、すべてのファイルを検索するオプションと、最も感染しやすいとされる特定の拡張子のファイルのみを検索するオプションです。しかし、最近ではファイルの拡張子を変更して「偽装した」ファイルが開発されているため、後者のオプションの効力が低下しています。トレンドマイクロの推奨設定は、ファイル名の拡張子に関係なく、ファイルの「実際のファイルタイプ」を識別するトレンドマイクロのテクノロジです。

注意： トレンドマイクロの推奨設定では各ファイルのヘッダを検査し、一定の基準に基づいて、ウイルス感染を受けやすいと判定されるファイルのみを検索します。

実際のファイルタイプ

トレンドマイクロの推奨設定を有効にすると、検索エンジンは、実際のファイルタイプを確認するために、ファイル名ではなくファイルヘッダを検査します。たとえば、検索エンジンがすべての実行可能ファイルを検索するように設定されており、family.gif という名前のファイルが見つかった場合、そのファイルをグラフィックファイルとは見なさず、検索対象とします。その代わりに、検索エンジンはファイルのヘッダを開き、ファイルが本当にグラフィックファイルかどうか、あるいは、検出されないように虚偽の命名がされている実行可能ファイルかどうかなどを判定するために、内部に登録されたデータタイプを検査します。

実際のファイルタイプ検索は、トレンドマイクロの推奨設定と連携して潜在的な脅威として知られているファイルタイプのみを検索します。これらのテクノロジによって検索エンジンが検索する必要のあるファイルの総数を最大で 3 分の 2 くらいまで削減できますが、その代償として潜在的なリスクが高まります。

たとえば、.gif ファイルと .jpg ファイルは Web トラフィックの大部分を占めています。これらのファイルは、ウイルスを潜伏させたり、実行可能コードを起動したり、既知のまたは理論的な攻撃を実行したりできません。しかし、これらのファイルが安全というわけではありません。悪意あるハッカーが、検索エンジンを回避してひそかにネットワークに侵入するために、有害なファイルに「安全な」ファイル名を付ける可能性があります。このような場合でも、トレンドマイクロの推奨設定では、実際のファイルタイプを確認してウイルス検索し、不正コードがネットワークに侵入するのを阻止します。

注意： より高いレベルのセキュリティを実現するには、すべてのファイルを検索することをお勧めします。

ダメージクリーンナップサービスについて

IWSS はトレンドマイクロ ダメージクリーンナップサービス (以下、DCS) に対応しています。DCS は、トレンドマイクロが提供する、IWSS と連携可能な別製品で、これによりスパイウェア、フィッシング、およびその他のインターネット上の脅威の検出時にクライアントシステムのクリーンナップと修復を自動化できます。

IWSS と DCS の連携が特に重要となるのは、ノートパソコンなどの「外部」コンピュータがアクセス可能なネットワークや、リアルタイムのウイルス対策ソリューションを持たないデスクトップがあるネットワークです。IWSS では、HTTP の送受信トラフィックを監視しますが、既知のフィッシング、スパイウェア、およびトロイの木馬を宛先とする送信トラフィックを検出し、それらをブロックできます。ただし、影響を受けたシステムのクリーンナップと修復を自動的に実行できるのは DCS です。

通常、DCS によって実行される修復作業には、トロイの木馬がクライアントシステムに落とした攻撃プログラムの削除、Windows レジストリのクリーンナップ、メモリやブートセクタからの不正コードの除去などがあります。

DCS が影響を受けたシステムと連携できない場合または修復できない場合は、DCS のレポートを IWSS に送信させることができます。これにより、ActiveX DCS の手動クリーンナップページにクライアントのブラウザをリダイレクトして、インターネットアクセスを制限できます。

注意： Firefox を使用して Web サイトにアクセスし、DCS の手動クリーンナップページにリダイレクトされた場合、ページのロードが中止され、ロード中であることを示すメッセージが表示されます。この問題が発生するのは、DCS の手動クリーンナップエージェントが ActiveX プラグインで、Internet Explorer にのみ対応しているためです。

ダメージクリーンナップ要求の発行

IWSS が DCS サーバに登録されていると、次の場合に DCS 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によってスパイウェア、不正サイト、またはウイルス流布サイトとして分類される URL にアクセスを試みたとき
- クライアントコンピュータが「ワーム」として分類されるウイルスをアップロードしたとき
- DCS は、感染したファイルを駆除するためにクライアントに接続します。

IWSS アーキテクチャ

IWSS には、使用する機能によって必須モジュールとオプションモジュールがいくつか用意されています。次に、主要なモジュールとサービスを簡単に説明します。多くの予約タスクは、インストール時に設定されます。

IWSS のモジュール

IWSS は次のモジュールで構成されます。

- **メインプログラム** — 管理コンソールと、IWSS に必要な基本ライブラリファイルが含まれます。
- **HTTP 検索** — ICAP 検索または HTTP 検索のいずれかの HTTP 検索と、URL ブロックに必要なサービスが含まれます。
- **FTP 検索** — FTP 検索に必要なサービスが含まれます。
- **URL フィルタ** — Web セキュリティ強化フィルタオプションの機能が含まれます。この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。
- **アプレット /ActiveX 検索** — モバイルコードセキュリティオプションの機能が含まれます。この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。
- **SNMP 通知** — SNMP 対応ネットワーク管理ソフトウェアに SNMP トラップを送信するサービスが含まれます。
- **IWSS 用 Control Manager エージェント** — Control Manager からの監視および設定を可能にする Control Manager エージェントに必要なファイルが含まれます。

サービス

IWSS では、次のサービスが使用されます。

- Trend Micro InterScan Web Security Suite Console (java) — Web 管理コンソールをホストする Web サーバです。

- Trend Micro InterScan Web Security Suite for FTP (isftpd) — FTP トラフィックフローと FTP ウイルス検索を使用可能にするサービスです。
- Trend Micro InterScan Web Security Suite for HTTP (iwssd) — FTP over HTTP を含む、HTTP トラフィックフローと HTTP 検索を使用可能にするサービスです。アプレット /ActiveX 対策処理も行います。
- Trend Micro IWSS Log Import (logtodb) — テキストファイルからデータベースにログを出力するサービスです。
- Trend Micro IWSS Notification Delivery Service (isdelvd) — メールによる管理者への通知と、ブラウザによるユーザへの通知を処理するサービスです。
- Trend Micro SNMP Service (svcmonitor) — SNMP トラップ通知を SNMP 対応ネットワーク監視デバイスに送信するサービスです。
- Trend Micro Control Manager Service (En_Main) — Control Manager を使用している場合、Control Manager からの IWSS の設定とステータスレポートを許可するサービスです。
- Trend Micro InterScan Web Security Suite for Dashboard (ismetricmgmtd) — リアルタイムダッシュボードの表示で使用されるシステムリソースデータを収集するサービスです。

予約タスク

IWSS を設置すると、セットアッププログラムによって予約タスクがいくつか作成されます。

- purgefile — 毎日午前 2 時に実行され、ログの保持期間の設定に従って古くなったテキストログファイルを削除します。
- schedulereport — 1 時間ごとに実行され、予約レポートが起動するよう設定されているかどうかを確認します。
- schedulepr_update — 1 日に 1 回実行され、製品ライセンスのステータスを確認します。
- schedule_au — 15 分ごとに実行され、パターンファイルまたはその他のプログラムコンポーネントのアップデート時期かどうかを確認します。

- cleanfile — 1 時間ごとに実行され、検索または大容量ファイルの検索に伴ってダウンロードした一時ファイルを削除します。
- DbOldDataCleanup.sh — 毎日午前 2 時 5 分に実行され、データベース内で古くなったセキュリティログのデータおよびアクセス割り当てカウンタをクリーンナップします。
- svc_snmpmonitor.sh — 5 分毎に実行され、監視 /SNMP デーモンが動作しているかどうか確認します。
- db_reindex.sh — 毎日、1 時間おきの 28 分に実行され、無効なデータが含まれる破損したデータベースインデックスを復元します。これにより、最適なデータベースのパフォーマンスを維持します。
- db_vacuum.sh — 毎日、午前 3 時 58 分に実行され、最適なデータベースのパフォーマンスを維持するために、ガーベージコレクションを実行して、未使用スペースをデータベーステーブルから使えるようにします。

第 2 章

使用開始

本章で説明する内容には、次の項目が含まれます。

- 46 ページの「使用開始時のチェックリスト」
- 48 ページの「IWSS Web コンソールを開く」
- 49 ページの「インストール後の初期設定」
- 53 ページの「プロキシ検索の設定」
- 54 ページの「IWSS のアップデート」
- 54 ページの「HTTP トラフィックフローの有効化の確認」
- 55 ページの「EICAR テストウイルスによる IWSS のテスト」

使用開始時のチェックリスト

Trend Micro InterScan Web Security Suite (以下、IWSS) の要件については、IWSS 3.1 のインストールガイドを参照してください。

表 2-1 に、IWSS のインストール後に実行するタスクのチェックリストを示します。

表 2-1. 使用開始時のチェックリスト

タスク	参照先
基本の理解	
Web コンソールの使用方法を理解する	48 ページの「IWSS Web コンソールを開く」
初期設定を理解する	49 ページの「インストール後の初期設定」
ポリシーの動作を理解する	63 ページの「ポリシーについて」
起動と実行	
プロキシ検索の設定が正しいことを確認する	53 ページの「プロキシ検索の設定」
アップデート関連のプロキシを設定する	58 ページの「プロキシ設定 (アップデート用)」
IWSS コンポーネントをアップデートし保護機能を最新に保つ	54 ページの「IWSS のアップデート」
HTTP トラフィックフローの有効化を確認する	54 ページの「HTTP トラフィックフローの有効化の確認」
EICAR テストウイルスを使用して IWSS をテストする	55 ページの「EICAR テストウイルスによる IWSS のテスト」
ネットワークの保護	
IWSS が各ポリシーの適用対象を特定する際に使用するユーザ識別方法を設定する	第 5 章

タスク	参照先
次のポリシーを設定する ・HTTP 検索 ・アプレット /ActiveX ・URL フィルタ ・IntelliTunnel ・アクセス管理ポリシー	第 6 章 から 第 10 章
FTP 検索を設定する	第 10 章
使用開始時のタスク以外に実行可能なタスク レポートとログを使用する ・隔離ディレクトリの変更やデータベース設定の変更など IWSS の管理タスクを実行する ・製品ライセンスを表示する	第 12 章

IWSS Web コンソールを開く

IWSS の管理には、IWSS Web コンソールを使用します。

ローカルコンピュータ上の IWSS Web コンソールを開くには

Web ブラウザを開き、[アドレス] フィールドに次の URL を入力します。

http://localhost:1812

リモートの IWSS Web コンソールを開くには

Web ブラウザを開き、[アドレス] フィールドに次の URL のいずれかを入力します。

- http://< ドメイン名 >:1812/index.jsp
- http://< コンピュータ名 >:1812/index.jsp
- http://<IP アドレス >:1812/index.jsp

HTTPS を使用して IWSS コンソールにアクセスする方法については、190 ページの「HTTPS 経由での IWSS コンソールへのアクセス」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。

インストール後の初期設定

次の表に、インストール後の IWSS の初期設定を要約します。

表 2-2. インストール後の IWSS の初期設定

機能	インストール後の初期設定
全般的な設定	・HTTP トラフィックはオンになっています。 ・FTP トラフィックはオンになっています。 ・HTTP および FTP ウイルス検索、Java アプレット /ActiveX 対策、URL ブロック、URL フィルタはすべて有効になっています。 ・ゲストアカウントは無効 (したがって、すべてのゲストポリシーが無効) になっています。 ・IP アドレスによる識別方法は有効になっています。 ・隔離フォルダは /etc/iscan/quarantine に設定されています。
HTTP ウイルス検索	グローバルポリシーとゲストポリシーの初期設定 ・ファイルは一切ブロックされません。 ・すべてのファイルが検索されます。 圧縮ファイルの検索の設定 次の圧縮ファイルはブロックされます。 ・ファイル数が 50,000 を超える ・解凍後のファイルサイズが 200MB を超える ・圧縮レベルが 10 を超える ・解凍後のファイルサイズが圧縮時のサイズの 100 倍を超える 大容量ファイルの検索 ・2048MB を超えるサイズのファイルは検索されません。 ・512KB を超えるサイズのファイルは遅延検索を使用して検索されます。 ウイルス検索の処理 ・感染ファイルはクリーンナップされます。 ・クリーンナップできないファイルは削除されます。 ・パスワードで保護されたファイルは通過します。 ・マクロを含むファイルに対する特別な処理は実行されません。 その他の設定 ・隔離ファイルは暗号化されます。 ・スパイウェアに対する特別な検索は実行されません。

表 2-2.　インストール後の IWSS の初期設定

機能	インストール後の初期設定
Java アプレットの対策ルールと設定	署名の妥当性検査 ・有効な署名と信頼された証明書を持つ — アプレットは放置されます。 ・有効な署名と拒否リストに含まれる証明書を持つ — アプレットはブロックされます。 ・未署名 — アプレットは計測処理されます。 ・無効な署名 — アプレットはブロックされます。 ・アプレットの署名は署名証明書の有効期限を確認することにより検証されます。 ・信頼性が検証できない証明書はその署名が削除されています。 アプレットに許可する操作 ・送信元サーバへの接続 アプレットに禁止する操作 ・破壊的および非破壊的な操作 ・ローカルディスクに対するデータの読み書き ・ローカルポートへのバインド その他 ・アプレットは新規のスレッドグループを作成できません。 ・アプレットはアクティブスレッドを作成できます (最大 8)。 ・アプレットはアクティブウィンドウを作成できます (最大 5)。 ・計測処理後のアプレットには署名がありません。
ActiveX の対策ルールと設定	・*.cab ファイル、PE ファイル (*.exe, *.ocx) — 署名を検証し、拒否リストに含まれるか処理不可能な署名を持つ cab ファイルと、処理不可能な PE ファイルをブロックします。 ・署名証明書の有効期限が確認されます。
URL フィルタポリシー	・URL フィルタは有効になっています。 ・グローバルポリシーおよびゲストポリシーにより、業務時間および業務時間外に、「アダルト」(違法薬物、暴力、人種差別、および成人向けの内容に関連するサイト) および「コンピュータ / 危険」カテゴリのサイトがブロックされます。 ・業務時間の定義は、月曜から金曜までの午前 8 時から 11 時 50 分までと午後 13 時から 17 時までです。

表 2-2.　インストール後の IWSS の初期設定

機能	インストール後の初期設定
アクセス割り当てポリシー	・なし
URL ブロック	・URL ブロックは有効になっています。 ・フィッシングパターンに該当するすべての URL (フィッシング、スパイウェア、ウイルス流布、および不正サイト) がブロックされます。
FTP 検索	・FTP 検索は有効になっています (アップロード検索とダウンロード検索の両方に対して)。 ・どのファイルタイプもブロックされません。 ・すべてのファイルが検索されます。 圧縮ファイルの検索の設定 次の圧縮ファイルはブロックされます。 ・ファイル数が 50,000 を超える ・解凍後のファイルサイズが 200MB を超える ・圧縮レベルが 10 を超える ・解凍後のファイルサイズが圧縮時のサイズの 100 倍を超える 大容量ファイルの検索 ・1,024MB を超えるサイズのファイルは検索されません。 ・512KB を超えるサイズのファイルに対する遅延検索が有効になっています。 その他 ・隔離ファイルは暗号化されます。 ・スパイウェアに対する検索は実行されません。 ・感染ファイルは、駆除できる場合は駆除され、それ以外の場合は削除されます。 ・パスワードで保護されたファイルは放置されます。 ・マクロを含むファイルに対する特別な処理は実行されません。

表 2-2.　インストール後の IWSS の初期設定

機能	インストール後の初期設定
レポートとログ	・すべてのユーザに対して、日次、週次、月次の総合レポートが有効になっています。 ・セキュリティログはデータベースとログファイルに記録され、30 日間保持されます。 ・セキュリティログにはパフォーマンスデータが含まれます。 ・システムログは /etc/iscan/log フォルダに記録され、5 日間保持されます。
アップデート	・ウイルスパターンファイル、スパイウェアパターンファイル、およびフィッシングパターンファイルのアップデートの有無は毎週チェックされます。 ・検索エンジンのアップデートの有無は毎週チェックされます。 ・URL フィルタエンジンのアップデートの有無は毎週チェックされます。
通知	有効になっているメール通知 ・HTTP のファイルタイプによるブロックイベント ・URL ブロックイベント ・ウイルスパターンファイル、フィッシングパターンファイル、およびスパイウェアパターンファイルのアップデートと URL フィルタエンジンのアップデート (成功と失敗の両方) 無効になっているメール通知 ・HTTP 検索イベント ・Java アプレット /ActiveX に関する各種イベント ・FTP 通知の初期設定はオン ・しきい値アラートの初期設定はオフ ・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) は有効 (ただし、DCS サーバの IP アドレスとポートの設定が必要)
ダメージクリーンナップサービス	・ファイルの駆除に失敗した場合、クライアントブラウザは DCS にリダイレクトされます。

注意： サイズの大きいファイルを処理する場合、IWSS は進行ステータス画面を使用します。進行ステータス画面は、JavaScript とポップアップウィンドウを使用して、ダウンロードの進行ステータスを表示します。デスクトップのセキュリティポリシーでポップアップブロック機能が有効になっている場合、または JavaScript が無効になっている場合、進行ステータス画面は機能せずに、検索は実行されません。

進行ステータス画面が機能するには、外部に見えているどの IP アドレスにクライアントが接続するかを IWSS が認識する必要があります。127.0.0.1 を使用すると問題が生じます。進行ステータス画面に関するメッセージが表示された場合、コンピュータの IP アドレスを iscan_web_server (例 : iscan_web_server=1.2.3.4:1812) に追加するか、またはホスト名による解決が 127.0.0.1. にならないように、/etc/hosts ファイルを変更します。

プロキシ検索の設定

IWSS は初期設定でフォワードプロキシ (スタンドアロン) モードになっています。プロキシのタイプは、IWSS コンソールで変更できます。FTP over HTTP の匿名ログオン用のメールアドレス、スレッド数、IWSS サーバへの同時接続数などのプロキシ関連のその他の設定も変更できます。

プロキシの設定を変更するには

1. メインメニューで [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、既存の設定を確認し、必要に応じて変更します。

IWSS のアップデート

IWSS がインターネットに接続されたら、ネットワークを最新の脅威から保護するためにコンポーネントをアップデートする必要があります。

手動でアップデートするには

1. メインメニューで [概要] をクリックします。
2. [概要] 画面の [検索] タブで、アップデートするコンポーネントを選択して、[アップデート] をクリックします。アップデートの進行状況を示すバーが表示され、アップデート結果を示すメッセージ画面が表示されます。

HTTP トラフィックフローの有効化の確認

IWSS のインストール後、HTTP サービスは初期設定で有効になっています。クライアントが Web を閲覧したり、その他の HTTP 処理を実行するための HTTP トラフィックフローをオン / オフにすることができます。

HTTP トラフィックフローの有効化を確認するには

1. メインメニューから [概要] をクリックします。
   [オフ] リンクが表示されている場合は、クリックする必要はありません。
2. HTTP トラフィックがオフになっている場合は、[オン] をクリックします。

EICAR テストウイルスによる IWSS のテスト

European Institute for Computer Antivirus Research (EICAR) は、ウイルス対策ソフトウェアをテストするためのテストウイルスを開発しました。このスクリプトは、不活性のテキストファイルです。ほとんどのウイルス対策ベンダーから提供されるウイルスパターンファイルには、バイナリパターンが含まれています。このテストウイルスは、ウイルスではないため、プログラムコードは含まれていません。

警告： ウイルス対策のソフトウェアをテストする目的で実際のウイルスを使用しないでください。

EICAR テストファイルの取得

EICAR テストウイルスは、次の URL からダウンロードできます。

http://www.trendmicro.co.jp/download/test-virus.asp

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

または、テキストファイルに次の内容を入力またはコピーして、そのファイルに「eicar.com」という名前を付けることによって、独自の EICAR テストウイルスを作成できます。

X5O!P%@AP[4¥PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

注意： テストを行う前に、キャッシュサーバとローカルブラウザのキャッシュを消去してください。いずれかのキャッシュにテストウイルスのコピーが保存されていると、ファイルをダウンロードしようとする際にインターネットからではなくキャッシュからファイルを読み込もうとして、IWSS によりファイルが検出されない場合があります。

IWSS をさらにテストするには、付録 C「OpenLDAP」を参照してください。

第 3 章

アップデート

本章で説明する内容には、次の項目が含まれます。

- 58 ページの「プロキシ設定 (アップデート用)」
- 59 ページの「手動アップデート」
- 60 ページの「予約アップデート」
- 61 ページの「アップデートの操作方法」

プロキシ設定 (アップデート用)

インターネットへのアクセスにプロキシサーバを使用する場合は、コンポーネントをアップデートする前に Trend Micro InterScan Web Security Suite (以下、IWSS) 管理コンソールでプロキシ情報を入力する必要があります。入力したプロキシ情報は、トレンドマイクロのアップデートサーバからのコンポーネントのアップデートと、製品登録およびライセンス確認の両方に使用されます。

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

1. IWSS 管理コンソールを開いて、[アップデート] → [設定] の順に選択します。
2. [コンポーネントとライセンスのアップデートにプロキシサーバを使用する] を選択して、プロキシサーバまたはポートを指定します。
3. プロキシサーバで認証が必要な場合は、[ユーザ ID] と [パスワード] フィールドにそれぞれ入力します。

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

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

手動アップデート

手動でアップデートするには

1. メインメニューで [概要] をクリックします。
2. [概要] 画面の [検索] タブで、アップデートするコンポーネントを選択して、[アップデート] をクリックします。アップデートの進行状況を示すバーが表示され、アップデート結果を示すメッセージ画面が表示されます。

強制手動アップデート

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

コンポーネントを強制アップデートするには

1. メインメニューで [概要] をクリックします。
2. アップデート対象のコンポーネントを選択し、[アップデート] をクリックします。IWSS サーバがすでに最新のパターンファイルや検索エンジンを使用している場合は、メッセージボックスが表示されます。IWSS サーバがアップデートサーバよりも古いパターンファイルを使用している場合は、最新のパターンファイルがダウンロードされます。
3. 強制アップデートを開始するには、このメッセージボックスから [OK] をクリックします。

予約アップデート

パターンファイル、検索エンジン、URL フィルタエンジンの自動アップデートを予約するには

1. メインメニューから [アップデート] → [スケジュール] の順に選択します。
2. アップデート対象のコンポーネントの種類ごとに、アップデート間隔を選択します。次のオプションが用意されています。
   - [次の間隔] (パターンファイルのみ。アップデートを何分おきに実行するか選択します。)
   - [毎時] (パターンファイルのみ)
   - [毎日]
   - [毎週] (ドロップダウンメニューから曜日を選択。検索エンジンおよび URL フィルタエンジンのアップデートにはこの設定をお勧めします。)

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

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

注意： 最新バージョンのウイルスパターンファイルを確認するには、IWSS 管理コンソールの [概要] 画面を使用します。ウイルスパターンファイルをアップデートした後は、NetCache アプライアンスおよび Blue Coat Port 80 Security Appliance のキャッシュを消去して再起動することで、ウイルスがキャッシュされないようにすることをお勧めします。NetCache アプライアンスおよび Blue Coat Security Appliance のキャッシュの消去方法と再起動方法は、それぞれの機器に付属のドキュメントを参照してください。

アップデートの操作方法

アップデート成否の確認

使用しているコンポーネントのバージョンと最後のアップデート日時は、IWSS 管理コンソールの [概要] 画面の [検索] タブで確認できます。手動アップデートまたは予約アップデートが正常に完了しているかどうかを確認するには、[概要] 画面を調べます。

アップデート通知

IWSS では、パターンファイル、URL フィルタエンジン、または検索エンジンのアップデート状況を事前に管理者に知らせる通知を発行できます (197 ページの「通知」を参照)。

アップデートのロールバック

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

新しいパターンファイルが、感染していないファイルをウイルス感染と誤って検出してしまう「誤警告」を発してしまうことがあります。このような場合、以前のパターンファイルや検索エンジンに戻すことができます。

パターンファイルまたは検索エンジンをロールバックするには

1. メインメニューで [概要] をクリックします。初期設定では [システムダッシュボード] タブが表示されます。
2. [検索] タブをクリックします。

3. ロールバック対象のコンポーネントを選択し、[ロールバック] をクリックします。ロールバックの進行状況を示すバーが表示され、ロールバック結果を示すメッセージ画面が表示されます。ロールバックが完了すると、[概要] 画面の [検索] タブに現在のバージョンと最後のアップデート日付が表示されます。

注意： IWSS は URL フィルタエンジンのロールバックには対応していません。

パターンファイルの削除

パターンファイルのアップデート後も、IWSS では、ロールバックに備えてウイルスパターンファイルやスパイウェアパターンファイルなど古いパターンファイルがサーバに保存されます。サーバに保存するパターンファイルの数は、[アップデート] → [接続の設定] 画面の [保存するパターンファイルの数 :] で設定します。

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

第 4 章

ポリシーについて

本章で説明する内容には、次の項目が含まれます。

- 64 ページの「ポリシーの仕組み」
- 67 ページの「ポリシーの配信」
- 66 ページの「初期設定のグローバルポリシーとゲストポリシー」
- 67 ページの「ユーザの識別方法について」
- 81 ページの「HTTP 検索に関する注意」
- 83 ページの「Java アプレット /ActiveX 対策に関する注意」
- 87 ページの「URL フィルタに関する注意」
- 89 ページの「圧縮ファイルの処理」
- 89 ページの「サイズの大きいファイルの処理」
- 89 ページの「隔離ファイルの暗号化」
- 90 ページの「スパイウェアの検索」
- 90 ページの「IntelliTunnel に関する注意」
- 92 ページの「アクセス割り当てポリシーに関する注意」
- 93 ページの「URL アクセス管理に関する注意」
- 95 ページの「FTP 検索に関する注意」

ポリシーの仕組み

アクセスすべきファイル種類やインターネットリソースに応じて、ネットワーク上のユーザやグループごとに異なるセキュリティ設定を適用できます。

注意： ポリシーを作成する前に、ユーザ識別方法、つまり Trend Micro InterScan Web Security Suite (以下、IWSS) がネットワーク上でクライアントを識別する方法を正しく設定していることを確認します。手順については、67 ページの「ユーザの識別方法について」を参照してください。

ポリシーは次のように分類されます。

- **ウイルスとスパイウェアに対する HTTP 検索** — 組織の使用許可ポリシーを使用すると、クライアントによるオーディオ / ビデオのダウンロードを全体的に禁止できます。しかし、社内にはこの種のファイルを正規の業務目的で受信すべきグループもあります。各種のウイルス検索ポリシーを設定すれば、HTTP ウイルス検索ポリシーの異なるファイルブロックルールを社内のグループごとに適用できます。

  詳細については、81 ページの「HTTP 検索に関する注意」を参照してください。

- **Java アプレット /ActiveX 対策** — 機密情報を傍受してインターネット経由で転送可能なアプレットをクライアントが実行しないようにするために、アプレットが起点サーバに接続できないようにするポリシーを社内の大部分に設定することができます。ただし、Java アプレットの株式相場表示機能によって相場を調べるなど、社内にこの種のアプレットを正規の業務目的で実行すべきグループがある場合は、別のポリシーを設定してクライアントベースのサブセットに適用できます。

  詳細については、83 ページの「Java アプレット /ActiveX 対策に関する注意」を参照してください。

- **URL フィルタ** — 社員に業務関連以外のネットサーフィンを行わせないよう、「ギャンブル」カテゴリ内の Web サイトへのアクセスをブロックするグローバルポリシーを設定できます。しかし、営業部門には、ゲーム業界の見込み客について調査できるよう、この種のサイトへのアクセスを許可するポリシーを別途設定すべき場合もあります。

  詳細については、87 ページの「URL フィルタに関する注意」を参照してください。

- IntelliTunnel — IWSS では、特定のインスタントメッセージ (IM) プロトコルや認証接続プロトコルによる通信をブロックできます。

  詳細については、90 ページの「IntelliTunnel に関する注意」を参照してください。

- **アクセス割り当て** — IWSS を使用すると、組織で使用する帯域幅を制御できるよう、クライアントが 1 ヵ月の間にダウンロードできるファイル容量を制限するアクセス割り当てポリシーを設定できます。正規の業務目的でインターネットを頻繁に閲覧しなくてはならない社員については、無制限にインターネットにアクセスできるポリシーを別途設定できます。

  詳細については、155 ページの「アクセス割り当てと URL アクセス設定」を参照してください。

初期設定のグローバルポリシーとゲストポリシー

IWSS では、すべてのポリシー種類に対して次の初期設定ポリシーがあります。

- **グローバルポリシー** — 待機ポート (初期設定ポート = 8080) を経由して IWSS にアクセスするすべてのクライアントです。
- **ゲストポリシー** — 特定のゲスト用ポート (初期設定ポート = 8081) 経由で IWSS にアクセスするクライアント (通常は嘱託従業員、請負業者、技術者など) です。

注意： 初期設定では、初期設定の待機ポートを通じて IWSS にアクセスするクライアントに対し、アクセス割り当てが用意されていません。したがって、事前に設定されているグローバルアクセス割り当てポリシーはありません。

メインメニューで [HTTP] → [設定] → [プロキシ検索] の順に選択して、両方のポリシーを設定します。

ゲストポリシーについて

ゲスト用ポート機能は、ユーザ識別方法として LDAP のユーザ / グループ名を使用し、IWSS を HTTP プロキシモードで実行できるように設定すると使用できます。請負社員や来社したベンダーなど、ディレクトリサーバ内にアカウントを持っていないユーザでも Web にアクセスできるよう 2 次待機ポートを使用できます。ディレクトリ内のユーザ用には 8080 が、ゲスト用には 8081 が初期設定のポート値として設定されています。ゲストポリシーは、ゲストに適用される唯一のポリシーです。

「ユーザ / グループ名」によるユーザ識別方法を有効にする方法については、70 ページの「グループユーザまたはグループ名の使用」を参照してください。

ポリシーの配信

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

注意： キャッシュ生存期限を経過したとき、または [ポリシーの配信] をクリックしてポリシーを適用している間は、HTTP 接続および FTP 接続が少しの間 (10 秒程度) 中断されます。

注意： IWSS の初期設定では、LDAP キャッシュは IWSS で 1.5 時間ごとに更新されます。このため、あるユーザを別のグループに移動するなど、ディレクトリを変更すると、IWSS 内ですぐに表示が更新されない場合があります。

ユーザの識別方法について

HTTP ウイルス検索、URL フィルタ、アプレット /ActiveX 対策、IntelliTunnel 対策、アクセス割り当てポリシーの範囲を定義するには、IWSS によるクライアントの識別方法を設定します。ユーザ識別方法を選択することで、ログファイルとレポート内の影響を受けたシステムに対するセキュリティイベントの追跡方法も決まります。

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

- 識別なし (HTTP 要求に対してクライアントコンピュータを識別しません)
- IP アドレス (初期設定)
- ホスト名 (変更された HTTP ヘッダ)
- ユーザ / グループ名 (LDAP)

「識別なし」の使用

HTTP 経由のトラフィックについて、管理者がクライアントコンピュータ名の確認を望まない場合は、[識別なし] オプションを使用します。このオプションを選択した場合、さまざまなログの [ユーザ ID] の値として「不明」が表示されます。

IP アドレス

IP アドレスは初期設定の識別オプションで、以下の条件が必要です。

- クライアント IP アドレスを DHCP 経由で動的に割り当てていないこと。
- 影響を受けるシステムと IWSS の間のネットワークパスでネットワークアドレス変換 (NAT) を実行していないこと。

次の条件をすべて満たす場合は、ユーザの識別に IP アドレスを使用します。

- 組織内の全員に各自のクライアントコンピュータが割り当てられていること。
- 各クライアントコンピュータに専用の静的 IP アドレスが割り当てられていること。
- 各クライアントコンピュータが他者による使用から保護されていること。

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

ホスト名

ホスト名によるユーザの識別には、IWSS で追加手順を実行する必要があります。IWSS は、各 HTTP プロキシ要求のソース IP アドレス上でホスト名検索を実行します。

[ホスト名 (変更された HTTP ヘッダ)] オプションでは、影響を受けるコンピュータの MAC アドレスと Windows コンピュータ名をウイルスログ、URL ブロックログ、インターネットアクセスログに記録します。Windows 上の Internet Explorer からアクセスする場合は、このオプションを選択します。このオプションを使用するには、トレンドマイクロが提供するプログラムを Windows クライアントごとに実行する必要があります。

ローカル Windows ドメインに対してログオンスクリプトから呼び出すと効果的に導入できます。このプログラムは、Internet Explorer が User-Agent HTTP ヘッダに含めるレジストリのエントリ (HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Internet Settings¥User Agent¥Post Platform) を修正することにより機能します。識別情報は、各種ログファイルの [User ID] 列に記録されます。これによって、クライアントの MAC アドレスと HTTP 要求を作成したコンピュータ名を含めるよう Windows 設定値が変更されます。MAC アドレスは固有かつ追跡可能な ID であるため、MAC アドレスの使用をお勧めします。コンピュータ名はもう 1 つの有用な識別子です。

追加の作業を行うことで、このメカニズムは IP アドレスを使用する場合より時間がかかる場合があります。このメカニズムは IP アドレスに基づいているため、次の要件と選択肢があります。

- クライアントが Windows プラットフォーム上で Internet Explorer を使用していること。
- IP アドレスのみを使用する場合の条件をすべて満たしていること。
    - 組織内の全員に各自のクライアントコンピュータが割り当てられていること。
    - 各クライアントコンピュータに専用の静的 IP アドレスが割り当てられていること。
    - 各クライアントコンピュータが他者による使用から保護されていること。
- 管理者は、< インストールディレクトリ >¥HTTP にあるユーティリティプログラム register_user_agent_header.exe を使用して、MAC アドレスとコンピュータ名を含む拡張された HTTP 要求ヘッダを使用するように各クライアントコンピュータ (Windows ベースの OS のみ) を設定する必要があります。このプログラムは、Internet Explorer が使用するレジストリのエントリ を変更します。管理者は、Windows ドメインログオンスクリプトからユーティリティを呼び出してこのタスクを簡単に実行できます。
- 管理者は、個別のホスト名に基づいてポリシーを設定できます。

グループユーザまたはグループ名の使用

ユーザ / グループ名によるユーザ識別方法は、LDAP データベースにのみ依存します。このメカニズムを使用する場合、管理者は次を実行する必要があります。

- ネットワーク上でサポートされている LDAP サーバを設定します。
- IWSS 経由でプロキシ要求を行う各ユーザに対してユーザアカウントまたはレコードを LDAP サーバ上で作成します。

注意： IWSS は、Windows 200X サーバ上の Active Directory サービス、Linux OpenLDAP サーバ、または Sun の iPlanet Directory Server の一部である LDAP データベースの使用をサポートします。

このメカニズムを使用する場合、管理者は次を実行する必要があります。

- ネットワーク上でサポートされている LDAP サーバを設定します。
- IWSS 経由でプロキシ要求を行う各ユーザに対してユーザアカウントまたはレコードを LDAP サーバ上で作成します。

このメカニズムを使用してユーザを識別する場合、管理者は次を使用してポリシーを作成できます。

- 個別の IP アドレス (IP アドレスメカニズムと同様)
- IP アドレスの範囲 (IP アドレスメカニズムと同様)
- LDAP 認証ユーザまたはグループ

管理者がユーザ識別メカニズムとして LDAP を設定する場合、ブラウザが最初に IWSS HTTP サービスに最初に接続された際に、ユーザは有効なユーザ名とパスワードを入力する必要があります。いったん認証されたら、ブラウザのセッション中、ユーザの認証は維持されます。

ユーザ / グループ名による識別方法では、ユーザの認証情報を確認し、グループ情報を取得します。ディレクトリサービスは、ネットワーク上のユーザが物理的に接続している方法と場所を知らずにどんなリソースにもアクセスできるように、物理的なネットワークトポロジとプロトコルを透過的にします。LDAP は、ディレクトリ内の情報にアクセスしてアップデートする標準的な方法を定義します。プロキシ認証中にユーザ確認 / グループ取得のために必要な情報は、次のとおりです。

- LDAP サーバのホスト名
- 待機ポート番号
- LDAP 管理者アカウント
- パスワード
- 基本識別名 (LDAP 検索操作の開始点として使用)
- 認証方法 (ディレクトリサーバのベンダーに応じて、管理者パスワードを平文として渡す場合は [シンプル]、Kerberos/Digest-MD5 認証を使用する場合は [詳細])

IWSS とディレクトリサーバ間の認証動作は、クライアントブラウザと IWSS 間で使用する認証方法とは異なります。クライアントブラウザと IWSS 間の認証方法については、73 ページの表 4-1 で説明しています。IWSS とディレクトリサーバ間でやり取りされるユーザ認証情報にシンプル認証を選択しても、ユーザのログオン認証の安全は維持されます。このオプションは、LDAP 設定ページで設定する LDAP 管理アカウント認証情報に平文を使用します。この認証情報は、初回 LDAP 認証または接続テストの目的でのみ IWSS とディレクトリサーバ間でやり取りされます。ユーザログオン時、ユーザの認証情報を IWSS とディレクトリサーバ間で送信する場合は、IWSS は詳細認証方法を使用します (ユーザのパスワードは公開しません)。後者のための安全な認証は、ディレクトリサーバのベンダー、Kerberos か Digest-MD5 かによって異なります。

ユーザ / グループ名によるポリシー設定に関する注意

ユーザ / グループ名による識別方法は、他の識別方法での制限の一部を解決します。

- **IP アドレス** — 複数のユーザが同じコンピュータを共有している場合や、要求の発信元のコンピュータが IP アドレスによって的確に特定されない場合、要求を行った人物を特定できません。

- **ホスト名 (変更された HTTP ヘッダ)** — ユーザ / グループ名による識別方法は、複数の OS が使用されている環境で設定できます。一方、ホスト名による識別方法は Web 閲覧に Internet Explorer を使用している Windows でしか機能しません。

ユーザ / グループ名による識別方法は次のような環境で有効に機能します。

- 複数のプラットフォームまたはアプリケーションが使用されている環境
- 社員がコンピュータを共有している環境
- IP アドレスによってソースコンピュータを特定できない環境

ユーザ / グループ名による識別方法を有効にすると、IP アドレス /IP アドレス範囲とコンピュータ名ではなく、ユーザ名とグループに基づいてポリシーを定義できます。

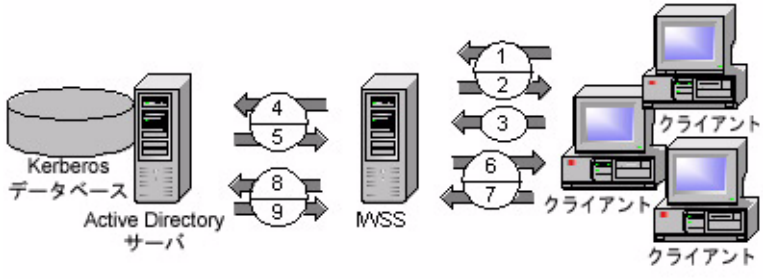


図 4-1.　LDAP サーバ認証の流れ (Active Directory の場合)

次の手順は、図 4-1. に示されている Active Directory (AD) の認証の流れを説明しています。他のディレクトリサーバの認証の流れも同様です。

1. クライアントが URL を要求します。
2. IWSS がプロキシ認証要求をクライアントに送信します。
3. クライアントが URL を再度要求し、ハンドシェイク情報を送信します。
4. IWSS がハンドシェイク情報を Active Directory サーバに送信します。
5. Active Directory サーバがハンドシェイク情報を IWSS に送信します。
6. IWSS がハンドシェイク情報をクライアントに送信します。

7. クライアントがプロキシ認証情報を入力します。
8. IWSS がユーザ認証情報を LDAP サーバに転送します。
9. Active Directory サーバがユーザを認証します。

クライアントの認証後、IWSS はクライアント要求を Web サーバに転送します。

ただし、プロキシ認証にも考慮する必要のあるマイナス点がいくつかあります。一番大きなマイナス点は、エンドユーザが使いにくいことです。IWSS では、認証のためにクライアントがユーザ名とパスワードを入力することが求められます。これらの認証情報が確認されると、閲覧が可能になります。アプリケーションの多くは、アプリケーションが開いている限りこの情報を保存し、各要求に認証情報を添付します。しかし、この情報は、他のアプリケーションや、同じアプリケーションの別のインスタンスと共有されません。結果として、クライアントは自分の認証情報を何度も入力しなければならない場合があります。

さらに、ポート 80 を使用する一部のアプリケーションは、「チャレンジ」の際にポップアップ ウィンドウを表示せず、ユーザが事前に構成設定で自分のプロキシ認証情報を設定することを必要とします。または、プロキシが認証を必要とする場合に単に機能しなくなります。

もう 1 つの問題は、セキュリティです。IWSS は HTTP プロキシモードでインストールされている場合、BASIC および NT LAN Manager (NTLM) 認証技術をサポートしますが、ICAP モードでインストールされている場合は、BASIC しかサポートしません。次の点を考慮してください。

表 4-1. BASIC および NTLM 認証方法の動作

動作	BASIC 認証	NTLM 認証
ユーザ名 / パスワード	ブラウザと IWSS 間で暗号化せずに送受信されます。	ブラウザと IWSS 間でユーザの認証情報を送受信する場合にハッシュのみを使用します。

表 4-1.　BASIC および NTLM 認証方法の動作 (続き)

動作	BASIC 認証	NTLM 認証
Kerberos による Active Directory 認証 (ブラウザ > IWSS > Active Directory サーバ)	ブラウザと IWSS 間のやり取りの間、ユーザの認証情報は攻撃を受けやすいので、認証情報は IWSS と Active Directory サーバ間では Kerberos によって暗号化されます。	ブラウザと IWSS 間、および IWSS と Active Directory サーバ間のやり取りで、ユーザの認証情報は安全です。
Microsoft アプリケーション	新しいアプリケーションはユーザに認証情報を入力するよう求めます。アプリケーションの認証後、同じアプリケーションの別のインスタンスは通常、認証情報を「記憶」し、その後の要求に対しても引き続き提供します。	Internet Explorer などの一部のアプリケーションは、ユーザの認証情報にポップアップウインドウなしでアクセスできます。Mozilla、ストリーミングメディアプレイヤー、Java ニュースティッカーなどその他のアプリケーションでは、引き続きポップアップウインドウが表示されます。注意 : NTLM は ICAP インストールで使用できません。
NTLM アプリケーションサポート	IWSS は Internet Explorer と 1.4.1 以上のバージョンの Mozilla にのみ NTLM チャレンジを発行します。	

要求の発信元のコンピュータを IP アドレスによって的確に特定できるネットワーク環境では、IWSS は以前に入力された認証情報を一定期間維持するキャッシュを使用できます。このキャッシュ内のエントリの初期設定の生存期限 (TTL) は、HTTP モードと ICAP モードの両方で 90 分です。

注意 : (1) ICAP モードは、NTLM やシングルサインオンをサポートしませんが、BASIC および IP ベースの認証情報のキャッシュはサポートします。
(2) HTTP モードまたは依存モードは、NTLM、BASIC、シングルサインオン、および IP ベースの認証情報のキャッシュをサポートします。

IWSS と LDAP

IWSS では、次の LDAP サーバと統合し、LDAP2 プロトコルと LDAP3 プロトコルの両方をサポートできます。

- Microsoft Active Directory 2000 および 2003
- Linux OpenLDAP Directory 2.2.17
- Sun Java System Directory Server 5.2 (旧 Sun ONE Directory Server)

LDAP 認証方法

[ユーザ / グループ名] 方法を有効にすると、インターネットにアクセスする前に、クライアントでネットワークのログオン認証情報を入力するよう求められます。次の表は、サポートされている各 LDAP サーバで使用できる LDAP 認証情報をまとめたものです。

	Kerberos	シンプル認証	NTLM
Microsoft Active Directory 2000 および 2003	使用可	使用可	使用可
Linux OpenLDAP Directory 2.2.17	使用可	使用不可	使用不可
Sun Java System Directory Server 5.2 (旧 Sun ONE Directory Server)	使用不可	使用可	使用不可

表 4-2. サポートしている LDAP サーバで使用できる認証方法

LDAP の通信フロー

クライアントからインターネットコンテンツを要求すると、ネットワーク認証情報の入力が求められます。シンプル認証では、ネットワーク認証情報は暗号化せずに送信されます。詳細認証では、Kerberos サーバを安全なパスワードの集中保管場所として使用するため、安全性が高まるという利点があります。Kerberos でクライアント認証を行うと、Kerberos サーバによって交付された「チケット」が IWSS とインターネットのアクセスに使用されます。

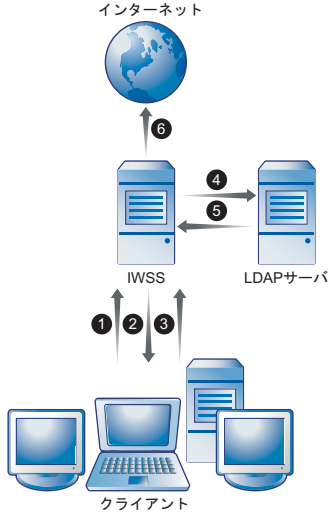


図 4-2. Kerberos 認証による LDAP 通信フロー

次の手順は、図 4-2 に示されている Active Directory (AD) の認証の流れを説明しています。他のディレクトリサーバの認証の流れも同様です。

1. クライアントが URL を要求します。
2. IWSS がプロキシ認証要求をクライアントに送信します。
3. クライアントが URL を再度要求し、ハンドシェイク情報を送信します。

4. IWSS がハンドシェイク情報を Active Directory サーバに送信します。
5. Active Directory サーバがハンドシェイク情報を IWSS に送信します。
6. IWSS がハンドシェイク情報をクライアントに送信します。
7. クライアントがプロキシ認証情報を入力します。
8. IWSS がユーザ認証情報を LDAP サーバに転送します。
9. Active Directory サーバがユーザを認証します。

クライアントの認証後、IWSS はクライアント要求を Web サーバに転送します。

ただし、プロキシ認証にも考慮する必要のあるマイナス点がいくつかあります。一番大きなマイナス点は、エンドユーザが使いにくいことです。IWSS では、認証のためにクライアントがユーザ名とパスワードを入力することが求められます。これらの認証情報が確認されると、閲覧が可能になります。アプリケーションの多くは、アプリケーションが開いている限りこの情報を保存し、各要求に認証情報を添付します。しかし、この情報は、他のアプリケーションや、同じアプリケーションの別のインスタンスと共有されません。結果として、クライアントは自分の認証情報を何度も入力しなければならない場合があります。

さらに、ポート 80 を使用する一部のアプリケーションは、「チャレンジ」の際にポップアップ ウィンドウを表示せず、ユーザが事前に構成設定で自分のプロキシ認証情報を設定することを必要とします。または、プロキシが認証を必要とする場合に単に機能しなくなります。

もう 1 つの問題は、セキュリティです。IWSS は HTTP プロキシモードでインストールされている場合、BASIC および NT LAN Manager (NTLM) 認証技術をサポートしますが、ICAP モードでインストールされている場合は、BASIC しかサポートしません。次の点を考慮してください。

表 4-3. BASIC および NTLM 認証方法の動作

動作	BASIC 認証	NTLM 認証
ユーザ名 / パスワード	ブラウザと IWSS 間で暗号化せずに送受信されます。	ブラウザと IWSS 間でユーザの認証情報を送受信する場合にハッシュのみを使用します。

表 4-3.　BASIC および NTLM 認証方法の動作 (続き)

動作	BASIC 認証	NTLM 認証
Kerberos による Active Directory 認証 (ブラウザ > IWSS > Active Directory サーバ)	ブラウザと IWSS 間のやり取りの間、ユーザの認証情報は攻撃を受けやすいので、認証情報は IWSS と Active Directory サーバ間では Kerberos によって暗号化されます。	ブラウザと IWSS 間、および IWSS と Active Directory サーバ間のやり取りで、ユーザの認証情報は安全です。
Microsoft アプリケーション	新しいアプリケーションはユーザに認証情報を入力するよう求めます。アプリケーションの認証後、同じアプリケーションの別のインスタンスは通常、認証情報を「記憶」し、その後の要求に対しても引き続き提供します。	Internet Explorer などの一部のアプリケーションは、ユーザの認証情報にポップアップ ウインドウなしでアクセスできます。Mozilla、ストリーミング メディア プレイヤー、Java ニュースティッカーなどその他のアプリケーションでは、引き続きポップアップ ウインドウが表示されます。 注意 : NTLM は ICAP インストールで使用できません。
NTLM アプリケーション サポート	IWSS は Internet Explorer と 1.4.1 以上のバージョンの Mozilla にのみ NTLM チャレンジを発行します。	

要求の発信元のコンピュータを IP アドレスによって的確に特定できるネットワーク環境では、IWSS は以前に入力された認証情報を一定期間維持するキャッシュを使用できます。このキャッシュ内のエントリの初期設定の生存期限 (TTL) は、HTTP モードと ICAP モードの両方で 90 分です。

注意： (1) ICAP モードは、NTLM やシングルサインオンをサポートしませんが、BASIC および IP ベースの認証情報のキャッシュはサポートします。
(2) HTTP モードまたは依存モードは、NTLM、BASIC、シングルサインオン、および IP ベースの認証情報のキャッシュをサポートします。

メインサーバと参照サーバに対する LDAP クエリマッチング

[ユーザ / グループ名] 識別方法でポリシーの範囲にユーザまたはグループを追加すると、IWSS はメイン LDAP サーバ内を最初に検索します。一致するエントリがない場合は、プライマリ参照サーバとセカンダリ参照サーバを検索します。ただし、メイン LDAP サーバに検索文字列と一致するエントリが見つかった場合、クエリはプライマリ参照サーバとセカンダリ参照サーバに一致結果を返しません。

たとえば、次のような状況を想定します。

- メイン LDAP サーバに「John Smith」と「John Jones」というエントリがあります。
- プライマリ参照サーバに「John Watson」というエントリがあります。
- セカンダリ参照サーバに「John Carter Rubin」というエントリがあります。

「John」に対するクエリでは、メイン LDAP サーバに一致するエントリがあるため「John Smith」と「John Jones」のみが返され、参照サーバまでは検索されません。しかし「John Carter」に対するクエリでは、メインサーバにもプライマリ参照サーバにも一致するエントリがないため、セカンダリ参照サーバまで検索されて「John Carter Rubin」が返されます。

クロスドメインの Active Directory オブジェクトクエリ

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

クロスドメイングループオブジェクトの属性を検索するには、同じ Active Directory フォレスト内のクロスドメイングループメンバーがグローバルカタログに含まれるよう、「ユニバーサル」グループ範囲でグループを作成することをお勧めします。

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

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

詳細については、http://www.microsoft.com で「How the Global Catalog Works」という記事を検索してください。

HTTP 検索に関する注意

不正コンテンツを見つけるために HTTP トラフィックを検索する際、パフォーマンスとセキュリティのトレードオフがあります。ユーザは、Web サイト上のリンクをクリックするとき、素早い応答を期待します。ただし、ゲートウェイのウイルス対策ソフトウェアがウイルス検索を実行するので、応答までの時間が長くなる場合があります。要求されるファイルによってはサイズが大きく、安全かどうか判定するには、ユーザに送る前にそのファイル全体のダウンロードが必要になる場合もあります。また、コンテンツは、多数の小さいファイルで構成されていることもあります。この場合、ファイルの検索に必要な時間の合計がユーザの待機時間となります。

ユーザの操作性を向上させる方法の 1 つとして、サイズの大きいファイルやウイルスが潜伏している可能性の低いファイルを検索から除外する方法があります。たとえば、拡張子「.gif」を持つすべてのファイル、または MIME タイプのすべてのファイルを検索から除外します。

MIME コンテントタイプによってファイルの検索を除外するように設定されている場合、IWSS は除外する前に、そのファイルの実際のファイルタイプを判定し、宣言された MIME タイプと照合します。ファイルの実際のファイルタイプが、トランザクションに添付されているコンテントタイプヘッダに示されているのとは異なる MIME タイプにマップされている場合、そのファイルは検索対象になります。ただし、ファイルタイプと MIME タイプとの間に常に明確なマッピングがあるわけではありません。IWSS で実際のファイルタイプを MIME タイプにマップできない場合、設定どおりに、コンテントタイプヘッダに従って検索が除外されます。

拡張子に基づいてファイルを検索から除外できます。トレンドマイクロは、除外する MIME コンテントタイプのリストを最小限に抑えることをお勧めします。一般的に、ファイルを検索するかどうかの判断を検索エンジンに任せた方が、検索を省略するファイルタイプを自分で選択するより安全です。1 つ目の理由として、HTTP ヘッダのコンテントタイプが、ダウンロードするコンテンツの実際のタイプを正確に表していない場合があります。2 つ目の理由として、テキストファイルのように除外しても安全と思われるタイプが実際には安全でない場合があります。スクリプトはテキストファイルであり、不正なコードが含まれている可能性があります。その他に MIME コンテントの除外を使用できるのは、セキュリティとパフォーマンスのトレードオフを意識的に行っている場合です。たとえば、Web トラフィックの多くはテキストであり、IWSS 検索エンジンは、コンテンツにスクリプト、つまり潜在的に不正なコードが含まれている可能性があるため、すべてのトラフィックを検索します。ただし、Web スクリプトに悪用される可能性がない環境を閲覧していると確信できる場合、MIME コンテントの除外リストに text/* を追加して、IWSS が Web ページを検索しないように選択できます。

サイズの小さいファイル内にある不正プログラムは、ネットワーク全体に瞬時に広がる可能性があります。これに対し、サイズの大きいファイルに含まれる不正プログラムは転送に時間がかかるため、それほど速く広がりません。したがって、サイズの小さいファイルを効率的かつ徹底的に選別することが重要です。

注意： ActiveX 検索のメインポリシーにより、ActiveX コントロールがサブタイプの COM オブジェクトだけでなく、すべての PE (Windows 実行可能) ファイルを検索するよう指示する場合、またはすべての未署名 PE ファイルをブロックする場合は、パフォーマンスが低下することがあります。パフォーマンスへの影響は、これらのファイルにポリシーを実施する Javascan デーモンがより頻繁に起動されるため発生します。

Java アプレット /ActiveX 対策に関する注意

IWSS のアプレット /ActiveX 検索は、不正な Java アプレットと安全でない ActiveX コントロールをインターネットゲートウェイでブロックし、これらがネットワークに侵入してクライアントワークステーションに対して不正な行為をするのを防ぎます。

IWSS では、インターネットゲートウェイサーバおよびデスクトップの両方で動作する階層型の技術アプローチを取り入れています。

- IWSS は、サーバ上で、デジタル署名がされているかどうか、署名の正当性、および署名に使用する証明書のステータスに基づいて、Java アプレットと ActiveX コントロールを事前にフィルタします。
- クライアントワークステーション上で、Java アプレットに挿入された IWSS コードが、リアルタイムでアプレットの動作を監視し、事前設定された対策ポリシーに従ってその動作が不正であるかどうか判定します。

図 4-3. は、IWSS が不正なアプレットと ActiveX オブジェクトを検索およびブロックする方法を示しています。

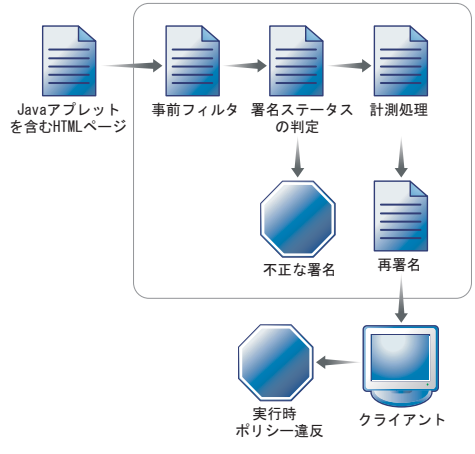


図 4-3.　Java アプレット対策の仕組み

アプレット /ActiveX 対策の仕組み

アプレットと ActiveX オブジェクトがゲートウェイを通過するとき、そのデジタル署名の正当性が確認されます。さらに、IWSS は、クライアントワークステーション上でリアルタイムにアプレットを監視し、禁止された操作が試みられると警告を発行します。

手順 1: サーバ上でのアプレット /ActiveX のフィルタ

Java アプレットと ActiveX コントロールがプロキシサーバにダウンロードされるとき、IWSS は次の条件に従ってこれらをフィルタします。

ActiveX オブジェクトの場合

ActiveX 対策を有効にすると、IWSS は、デジタル署名済みの CAB ファイルおよび実行可能な COM オブジェクト (ActiveX コントロール型) の署名をチェックします。その後で、署名に含まれているデジタル証明書を検査し、IWSS 固有の証明書データベースにある証明書と比較します。署名されていない、署名が無効である、または未知のルート認証機関 (CA) を使用して署名されている ActiveX オブジェクトはブロックされます。代わりに、システムは警告メッセージを含む新しい HTML ページを作成します。この新しいページは、クライアントワークステーションに配信されます。

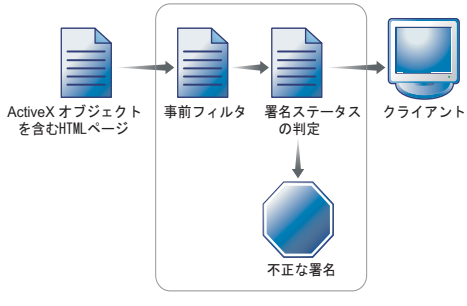


図 4-4.　ActiveX 対策の仕組み

Java アプレットの場合

IWSS は、デジタル署名がされているかどうか、署名の正当性、および署名に使用する証明書のステータスに基づいて、Java アプレットをフィルタします。

署名確認が有効になっている場合、IWSS はデジタル署名されたアプレットの署名を確認します。署名されていない、未知のまたは非アクティブなルート認証機関 (CA) を使用して署名されている、フラグ付きの証明書を使用して署名されている、または署名が無効であるものはブロックできます。これらは、警告メッセージを表示する新しいアプレットに置き換えられます。証明書の確認が無効になっている場合、システムはアプレットに含まれている証明書に関係なく、すべての Java アプレットを受け付けます。

IWSS は、承認された証明書のデータベースを保持しており、これをフィルタ処理で使用します。このデータベースは、システムで使用されるすべての承認されていない証明書を取り込んで、自動的にアップデートされます。[HTTP] → [アプレット /ActiveX 対策] → [デジタル証明書] 画面では、データベースからエントリを削除することも、エントリを有効 / 無効にすることもできます。

Java アプレットの場合、IWSS は、クライアントにアプレットを送信する前に、次の手順 2 と手順 3 を実行します。

手順 2: Java アプレットの計測処理

IWSS は、アプレットのコードを分析して、実行される可能性のある潜在的に危険な処理を特定します。次に、これらの処理を監視および制御するために計測処理コード、すなわち特定のプログラミング操作についてユーザに通知する指示を追加します。

計測処理中に、IWSS は、疑わしい命令の周囲に監視コードを挿入し、対象受信者に割り当てられた対策ポリシーを添付します。この対策ポリシーは、IWSS の設定方法によって、クライアントの属しているドメインまたは IP アドレスごとに異なる場合があります。IWSS では、ネットワーク内の複数のユーザグループにマップできるように複数のポリシーを作成することができます。IWSS は、挿入された監視コードと添付された対策ポリシーを使用して、アプレットの動作をリアルタイムで監視し、その動作が不正かどうかを判断します。

注意： 署名されたアプレットに対する計測処理により、署名は無効となります。したがって、署名は削除され、未署名になります。クライアントブラウザで要求される場合、IWSS は、オプションでアプレットに再署名することができます。

手順 3: 計測処理されたアプレットへの再署名

再署名するよう設定されている場合、IWSS は、クライアントワークステーションに送信する前に、インポートされた「秘密鍵」を使用して、計測処理されたアプレットに再署名します。計測処理プロセス中は元のコードに変更が加えられるため、アプレットは元の署名を失います。この再署名機能を使用することで、クライアントの Web ブラウザは、計測処理されたアプレットの実行に必要なアクセス許可を使用して確実に正しく実行できるようになります。

IWSS は、再署名プロセスで使用するために、「秘密鍵」と、これに対応する「公開鍵」が含まれる関連証明書のインポートをサポートします。このキーは、認証機関 (CA) から入手できます。使用の際に設定できる再署名キーは、1 回に 1 つのみです。

注意： 再署名は、有効な署名があるアプレットにのみ適用されます。署名のないアプレットを受け付けるようにシステムが設定されている場合、これらのアプレットでは再署名が省略され、アプレットは計測処理後、ただちにクライアントワークステーションに配信されます。

手順 4: 計測処理されたアプレットの動作の監視

ブラウザ内でアプレットが実行されるときは、潜在的に危険な操作が実行される前に、計測処理が自動的に起動されます。計測処理は、添付された対策ポリシーとの比較に基づき処理を許可するかどうか判定します。処理が許可された場合は、IWSS により、その処理が実行に移されます。許可されない場合は、IWSS は設定された処理を行います。これは、次のいずれかです。

- アプレットを停止してメッセージを表示します。
- 警告画面によってユーザに通知し、アプレットの動作を許可するか、終了するか、またはアプレットを停止するかを選択するオプションを提供します。

URL フィルタに関する注意

IWSS の URL フィルタモジュールの初期設定では、組織の主な関心が、有害なデータの表示に関連して発生する法的責任を回避することにあると想定しています。ただし例外が必要な場合もあるため、より広範なアクセスを必要とする職務に携わる従業員には、制限されたカテゴリグループへのアクセスが許可されるように追加のポリシーを作成できます。たとえば、組織で許容できるインターネット利用ポリシーの違反について調査するために、人事部門または IT 部門の従業員が無制限のインターネットアクセスを必要とする場合があります。

さらに IWSS では、動的フィルタと高度なデータベースを組み合わせることにより、機能が向上しています。オンライン取引、ショッピング、オークション入札、出会い系、ギャンブル、およびその他の仕事に関係しないトピックの Web サイトを業務時間中に閲覧することで従業員の生産性は低下し、正当な閲覧のために利用可能な帯域幅が減少します。IWSS を使用すると、ユーザおよび作業チーム固有のニーズに応じてインターネットアクセスをカスタマイズできるため、インターネットの利用が最適化されます。

IWSS を使用することで、URL フィルタポリシーを非常に柔軟に応用できます。カスタマイズには、次の 3 つの基本的なメカニズムがあります。

- IWSS では、「ギャンブル」、「ゲーム」、「出会い系」など 60 以上のカテゴリの URL を含むデータベースが備わっています。

  カテゴリは次の論理グループに含まれます。

  - コンピュータ / 帯域幅
  - コンピュータ / 危険
  - コンピュータ / 通信
  - アダルト
  - ビジネス
  - 社会
  - 一般

- 各カテゴリは、業務時間中または業務時間外として指定された時間中、ブロックすることも、ブロックしないこともできます。
- 使用する環境で、ユーザごとに異なるポリシーを設定できます。

対象カテゴリ内のすべての識別された URL へのアクセスは、ポリシーに従って管理されます。各 URL は、データベースで 1 つ以上のカテゴリに関連付けられています。組織でアクセスする必要のある URL が禁止されたカテゴリに関連付けられている場合、URL フィルタの除外設定を使用して、データベースの分類を無効にできます。承認する URL リストで指定されるパターンは、URL に対する一致であり、URL が参照するドキュメントのコンテンツに対する一致ではありません。IWSS では、前方一致、部分一致、および完全一致により、URL フィルタの除外リストを設定するオプションが用意されています。

任意の時間帯に任意のポリシーに対して適用できる 2 つのルールは次のとおりです。

- 業務時間中に、設定したサイトカテゴリへのアクセスをブロックする
- 業務時間外に、設定したサイトカテゴリへのアクセスをブロックする

URL フィルタの仕組み

URL フィルタを設定するには、対象の URL とユーザの ID (IP アドレス、IP アドレスの範囲、ユーザ名、グループ名、またはホスト名) を入力します。ユーザは、IWSS で使用するように設定されているユーザの識別方法に従って特定されます (詳細については、100 ページの「ユーザ識別方法の設定」を参照)。

ユーザが要求した URL は、7 つのグループにまとめられている、60 を超えるカテゴリのうち 1 つ以上のカテゴリに分類できます。要求する URL を入力すると、Web レピュテーションデータベースに対する検索が実行されます。要求した URL へのアクセスの可否が検索の結果となります。

注意： URL フィルタエンジンへの手動アップデートは、[概要] 画面の [検索] タブで実行できます。

圧縮ファイルの処理

圧縮ファイルは、解凍してからファイル内の個々のファイルを検索する必要があるため、ウイルス対策ソフトウェアのパフォーマンスに負担がかかることがあります。IWSS には、すべての圧縮ファイルをゲートウェイでブロックするオプションが用意されています。また、通常はゲートウェイで圧縮ファイルを受け入れ、次のいずれかを指定してブロックすることもできます。

- 解凍後のファイル数が設定した最大値を超える場合
- 解凍後のファイルの累積サイズが設定した最大値を超える場合
- 多重圧縮されたファイルの圧縮レイヤ数が設定した最大値を超える場合
- 圧縮率が 99% を超える場合 (圧縮率が 99% 未満のファイルは IWSS によって自動的に許可されます)

サイズの大きいファイルの処理

サイズの大きいファイルのダウンロード時に遅延を発生させたくない場合、設定したしきい値より大きいファイルの検索を省略するように IWSS を設定できます。さらに、FTP 検索モジュールでは、サイズの大きいファイルに対して「遅延検索」方法を使用して、クライアントの接続がタイムアウトになるのを防げます。詳細については、121 ページの「遅延検索」を参照してください。FTP 検索モジュールでは、サイズの大きいファイルを処理する方法として、HTTP 検索モジュールで使用される「配信前に検索」はサポートされていません。

隔離ファイルの暗号化

IWSS が検索処理としてファイルを隔離するように設定されている場合、誰かが隔離フォルダを参照中に誤ってファイルを実行しないように、オプションでファイルを暗号化できます。暗号化されたファイルは、トレンドマイクロのサポート部門の担当者以外は暗号化を解除できないため注意してください。

スパイウェアの検索

IWSS では、ウイルス以外にも、スパイウェアパターンファイルに含まれている多くのリスクを検索できます。これらのリスクの概要については、122 ページの「スパイウェア検索ルール」を参照してください。

IntelliTunnel に関する注意

IWSS では、IM プロトコルおよび認証接続プロトコルについて HTTP トラフィックをフィルタし、指定されたポリシーに基づいて、特定のコンテンツが LAN に侵入するのをブロックします。複数のポリシーを作成し、IWSS で異なるフィルタ基準を組織内の異なるユーザグループに適用できます。

注意： IM/ 認証接続ポリシーは、IM/ 認証接続クライアントが HTTP トンネリングを使用するように設定されている場合にのみ実施できます。これには、サイトが HTTP を介した外部ネットワーク接続のみを許可するように設定されていることが必要です。つまり、内部クライアントは、どの形式およびポートでも外部サーバへ直接接続できないということです。これは、ファイアウォール設定の一部であり、IWSS の設定ではありません。

インスタントメッセンジャプロトコルについて

IWSS では、一般的なインスタントメッセージングプロトコルを使用する AOL、MSN Messenger、Yahoo! メッセンジャーのサービスをブロックできます。

認証接続プロトコルについて

IWSS では、次の技術を使用する認証接続通信をブロックできます。

- **Google トーク** — VoIP を含むオープン Jabber プロトコルに基づく、本格的なインスタントメッセージングクライアント。VoIP は、ユーザが電話の通信媒体としてインターネットを使用できる、ハードウェアやソフトウェアのひとつのカテゴリです。この技術では、従来の公衆電話交換回線網 (PSTN) の通話機能ではなくインターネットプロトコル (IP) を使用して、音声データをパケットで送信します。
- **Jabber IM** (jabber.org) — インターネット上で、2 地点間のリアルタイムのメッセージやプレゼンス交換機能で使用するオープン XML プロトコル。Jabber の非同期インスタントメッセージングのプラットフォームは、AIM、ICQ および MSN などのインスタントメッセージングシステムに似ていますが、これはオープンソースで、XML の使用により伸張性があり、どこでも Jabber サーバを実行できるため分散的です。また、Jabber サーバは、セキュリティを高めるために一般の Jabber ネットワークから切り離すこともできます。

注意： IntelliTunnel は、ICAP モードでは Google トークや Jabber IM をブロックしません。

Google のユーザ認証方式により、Gmail アプリケーションは Google Talk 製品と同じ認証を使用します。つまり、Google Talk をブロックすると Gmail もブロックされます。

アクセス割り当てポリシーに関する注意

IWSS アクセス割り当てゲストポリシーは、IWSS ゲストポートを介してインターネットにアクセスするクライアントによって使用される HTTP 帯域幅を制限します。その他のクライアントに対するポリシーも定義できます。アクセス割り当てグローバルポリシーはありません。ポリシーに一致する接続がない場合、クライアントには無制限アクセスが許可されます。アクセス割り当てポリシーを変更し、データベースにポリシーを保存した後、複数サーバ構成環境の IWSS サービスは、[HTTP 設定] 画面で設定されたキャッシュ生存期限 (TTL) 値に従ってポリシーをリロードします。

ダウンロード中に割り当てが超過しても、ダウンロードの続行は許可されます。ただし、アクセス割り当て間隔の有効期限が切れる前に行われた次のダウンロード / 閲覧要求は拒否されます。アクセス割り当て間隔の有効期限が切れた後、ユーザにはアクセスが再度許可されます。

グループに対する割り当てポリシーの場合、割り当て量は、グループ内のクライアントに個々に適用されます。また、同一のポリシー内のクライアントに対する割り当て量はすべて同じです。

URL アクセス管理に関する注意

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、または両方の組み合わせに基づいて、URL アクセスを制御できます。Web レピュテーションと URL フィルタモジュールの組み合わせは、複合型脅威に対する保護策で、IWSS によって提供されます。

オプションの URL フィルタモジュールは、URL が属してい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も Web レピュテーションも、ポリシー内でユーザが設定することにより管理されます。

ユーザが Web サイトにアクセスしようとすると、次のイベントが発生します。

- IWSS が URL ブロックリストと信頼する URL リストに対して要求された URL を確認します。
  URL が URL ブロックリストで見つかった場合、要求が拒否されます。URL が信頼する URL リストで見つかった場合、アクセスが許可され、アクセス制御は実行されません。
- URL がブロックリストでも信頼するリストでも見つからなかった場合、IWSS が要求された URL を Web レピュテーションに送信して処理します。
- Web レピュテーションは、リモートデータベースから URL についての適切な URL 評価を取得します。
  この評価は、「高」、「中」、「低」のいずれかです。指定された感度レベルによって、IWSS がその URL をブロックするかどうかが決定します (111 ページの「Web レピュテーションルールの指定」を参照)。
  URL が Web レピュテーションの除外リストにある場合、IWSS では、その URL に対するフィッシングおよびファーミング検出を省略します (112 ページの「Web レピュテーション除外の指定」を参照)。
- その後で、Web レピュテーションは、要求された URL がフィッシング脅威かファーミング脅威かを判断し、脅威が判明した場合、その URL にフラグを付けます。

- Web レピュテーションの最後のプロセスは、URL のカテゴリを決定することです。このカテゴリ情報は、後でオプションの URL フィルタモジュールによって使用されます。
- Web レピュテーションが、URL の評価、フィッシングフラグまたはファーミングフラグ、および URL カテゴリを IWSS に返します。
- URL にフィッシングまたはファーミングのフラグが付いていた場合、IWSS は Web サイトへのアクセスをブロックします。
- 次に、オプションの URL フィルタモジュールを使用している場合、このモジュールが、要求された URL についての Web カテゴリ情報を使用して、アクセスを許可するかどうかを判断します。
  URL が URL フィルタモジュールの除外リストで見つかった場合、カテゴリフィルタが無視され、URL アクセス管理の最終段階に進みます (149 ページの「URL フィルタの除外設定」を参照)。
  要求された URL のカテゴリが URL フィルタポリシーで許可されている場合、URL の処理は最終段階に送られます。許可されていない場合、URL はブロックされます。
- 最後に、Web レピュテーションの URL 評価に基づいて、IWSS では、要求された URL が検索ポリシーで指定された感度レベルより上か下かを判断します。
  URL が Web レピュテーションの除外リストで見つかった場合、IWSS はその URL の感度レベルチェックを省略します (112 ページの「Web レピュテーション除外の指定」を参照)。
  評価が感度レベルを下回っていた場合、要求された URL はブロックされます。ただし、評価が感度レベルを上回っていた場合、IWSS ではその URL へのアクセスを許可します。

FTP 検索に関する注意

IWSS では、HTTP トラフィックを処理する場合と同様に、FTP トラフィックにおいてウイルスおよびその他の不正コードを検索できます。ただし、HTTP 検索とは異なり、1 つの設定がネットワーク上のすべてのクライアントに適用されます。FTP 検索では、ユーザまたはグループベースのポリシーはサポートされません。

IWSS の FTP 検索は、スタンドアロンプロキシを使用するか、またはネットワーク上の別の FTP プロキシと連携して動作します。お使いの環境に FTP 検索を導入するには、最初にプロキシおよびデータ接続の種類 (パッシブ FTP またはアクティブ FTP。97 ページの「パッシブおよびアクティブ FTP」を参照) を制御する FTP 設定を実行します。次に、検索するトラフィックの方向、ブロックまたは検索するファイルのタイプ、圧縮ファイルおよびサイズの大きいファイルの処理方法、および不正コードの検出時に実行する処理を制御する検索ルールを設定します。

FTP 検索の設定が完了したら、オプションのセキュリティおよびパフォーマンス設定の変更について検討します。アクセス管理リストは、クライアントの IP アドレスに基づいて、クライアントの FTP アクセスを選択的に許可するように設定できます。コンテンツを直接管理できる FTP サイトに頻繁にアクセスする場合は、パフォーマンスを向上するために、特定の FTP サーバを許可リストに追加して、サイトからのダウンロードが検索されないようにできます。また、特定のポートへの FTP アクセスを許可または拒否して、さらに制限を設定できます。

FTP 設定

IWSS の FTP 検索設定には、IWSS ネイティブ (スタンドアロン) のプロキシと別の FTP プロキシのいずれかを使用するオプション、データ接続方法の 2 つのオプション (アクティブ FTP とパッシブ FTP)、および同時クライアント接続と処理スレッドの最大数を制御するパフォーマンス関連の設定が含まれています。

プロキシ設定

IWSS の FTP 検索には、2 つのプロキシオプションがあります。1 つはクライアントが IWSS ネイティブのプロキシに接続し、IWSS ネイティブのプロキシが FTP サーバに接続する「スタンドアロン」モード、もう 1 つは IWSS が別の FTP プロキシ経由で要求を渡し、その FTP プロキシが FTP サーバに接続する「FTP プロキシ」モードです。

- スタンドアロンモードでは、クライアントは < **ユーザ名** >@<FTP **サーバ名** > を FTP ユーザ名として使用し、IWSS の接続先となる FTP サーバを指定する必要があります。
- FTP プロキシモードでは、IWSS は常に構成設定で指定された FTP プロキシおよびサーバに接続するため、サーバ名は必要ありません。

FTP プロキシモードは、FTP プロキシ構成で FTP サーバのホスト名または IP アドレスとポート番号を指定することによって、単一の FTP サーバを保護するために使用することもできます。この場合、IWSS の FTP 検索モジュールは、HTTP 検索のリバースプロキシの場合と同様に、指定した FTP サーバ専用になります。IWSS の FTP プロキシオプションの詳細については、「IWSS インストールガイド」を参照してください。

パッシブおよびアクティブ FTP

IWSS では、ファイアウォール設定に応じて、データ接続にアクティブ FTP またはパッシブ FTP のいずれかを使用します。FTP では、データポートとコマンドポートの 2 つのポートを使用します。アクティブ FTP では、サーバがクライアントに接続してデータ接続を確立します。パッシブ FTP では、クライアントがサーバに接続します。

IWSS の設定でパッシブ FTP が選択されると、IWSS はクライアント側の「アクティブ」モードをサーバ側でパッシブモードに変換します。モードの変換は、IWSS の設定がパッシブで、クライアントがアクティブモードを使用している場合にのみ実行されます。IWSS の設定がアクティブの場合、変換は実行されないため、クライアントからのパッシブ要求はサーバ側でもパッシブ要求のままになります。

FTP 検索方向

IWSS の FTP 検索をどのように使用するかに応じて、アップロード、ダウンロード、またはその両方を検索するように FTP 検索モジュールを設定できます。たとえば、組織内のすべてのワークステーションにウイルス対策ソフトウェアがインストールされている場合、ファイルはすでにクライアント上で検索されているはずなので、アップロードを無効にすることでパフォーマンスを向上できます。

ファイルのブロック

セキュリティ、監視、またはパフォーマンス上の目的のためにブロックするファイルのタイプを識別できます。ブロックできるのは、Java クラスファイル、Microsoft Office 文書、オーディオ / ビデオ、実行可能ファイル、画像、または手動で設定したその他のタイプのファイルです。組織のポリシーによって特定のタイプのファイルがネットワーク内で禁止されている場合、IWSS の FTP ファイルブロックでは、該当するファイルを FTP ゲートウェイで阻止できます。

ファイル検索

検索するファイルのタイプを設定するときは、次の 3 つのオプションから選択できます。

- 検索可能なすべてのファイル — すべてのファイルが検索されます。最も安全なオプションです。
- トレンドマイクロの推奨設定 — ウイルスが潜むことがわかっているファイルタイプのみが検索されます。ファイルタイプはファイルヘッダを確認することによって決定されます。詳細については、38 ページの「トレンドマイクロの推奨設定について」を参照してください。
- 指定のファイル拡張子 — 指定したファイル拡張子を持つファイルのみが検索されます。

パフォーマンス上の理由で他のオプションを選択する必要がある場合を除き、すべてのファイルを検索することをお勧めします。

第 5 章

ユーザ識別方法とゲスト用ポートの設定

本章で説明する内容には、次の項目が含まれます。

- 100 ページの「ユーザ識別方法の設定」
- 107 ページの「ゲストポリシーのゲスト用ポートの有効化」

ユーザ識別方法の設定

Trend Micro InterScan Web Security Suite (以下、IWSS) がクライアントを識別する方法を設定します。

- IP アドレス (初期設定)
- ホスト名 (変更された HTTP ヘッダ)
- ユーザ / グループ名 (LDAP)

IP アドレス

IP アドレスによるユーザ識別方法を有効にするには

1. メインメニューから [HTTP] → [設定] → [ユーザの識別] の順に選択します。
2. [ユーザの識別方法] で、[IP アドレス] を選択します。
3. [保存] をクリックします。

ホスト名

ホスト名の識別方法を使用するには、クライアントが Windows プラットフォーム上で Internet Explorer を使用している必要があります。[ホスト名 (変更された HTTP ヘッダ)] によるユーザの識別オプションでは、ポリシーの適用先アカウントを定義する際にユーザのホスト名を指定してポリシーの範囲を定義するほか、MAC アドレスと Windows コンピュータ名をセキュリティイベントログに記録します。

注意： 初期設定では、ホスト名と MAC アドレスの組み合わせのうち、ホスト名の部分のみが IWSS のログに保存され、ポリシーのマッチングに使用されます。

ユーザ識別でホスト名と MAC アドレスの両方を使用する場合は、intscan.ini を編集して、[user-identification] セクションで use_mac_address=no を use_mac_address=yes に変更します。

注意： アプレットフィルタメッセージには、ホスト名の代わりにクライアント IP アドレスが表示されます。これは、Internet Explorer を使用している場合でも、HTTP 要求がブラウザではなく Java プラグインを介して送信されるため、ブラウザで要求に特別なヘッダを付加できないためです。

ホスト名で識別する方法を有効にするには

1. メインメニューから [HTTP] → [設定] → [ユーザの識別] の順に選択します。
2. [ホスト名 (変更された HTTP ヘッダ)] を選択します。
3. [保存] をクリックします。

注意： ユーザがインターネットにアクセスできるようになる前に、また、IWSS がポリシーを適用する前に、クライアント登録ユーティリティを実行しておいてください。

クライアント登録ユーティリティ

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

このプログラムは、Internet Explorer が User-Agent HTTP ヘッダに含めるレジストリのエントリ (HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Internet Settings¥User Agent¥Post Platform) を修正することにより機能します。識別情報は、各種ログファイルの [User ID] 列に記録されます。これによって、クライアントの MAC アドレスと HTTP 要求を作成したコンピュータ名を含めるよう Windows 設定値が変更されます。MAC アドレスは固有かつ追跡可能な識別方法であり、コンピュータ名はもう 1 つの有用な識別子です。

register_user_agent_header.exe ユーティリティを実行すると、HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Internet Settings¥User Agent¥Post Platform キーに「IWSS:< ホスト名 >/<MAC アドレス >」という新しいレジストリ値が作成されます。< ホスト名 > と <MAC アドレス > は、ユーティリティを実行したクライアントのホスト名と MAC アドレスです。これらの情報は、暗号化されています。

ユーザ / グループ名 (LDAP)

IWSS では、次の LDAP サーバと統合し、LDAP2 プロトコルと LDAP3 プロトコルの両方をサポートできます。

- Microsoft Active Directory 2000 および 2003
- Linux OpenLDAP Directory 2.2.17
- Sun Java System Directory Server 5.2 (旧 Sun ONE Directory Server)

LDAP 認証方法

[ユーザ / グループ名] 方法を有効にすると、インターネットにアクセスする前に、クライアントでネットワークのログオン認証情報を入力するよう求められます。次の表は、サポートされている各 LDAP サーバで使用できる LDAP 認証情報をまとめたものです。

	Kerberos	シンプル認証	NTLM
Microsoft Active Directory 2000 および 2003	使用可	使用可	使用可
Linux OpenLDAP Directory 2.2.17	使用可	使用不可	使用不可
Sun Java System Directory Server 5.2 (旧 Sun ONE Directory Server)	使用不可	使用可	使用不可

表 5-1. サポートしている LDAP サーバで使用できる認証方法

注意： Sun Java System Directory Server 5.2 で Digest-MD5 認証方法を使用するには、すべてのパスワードを暗号化せずに LDAP ディレクトリに保存してください。

[ユーザの識別] 画面 ([HTTP] → [設定] → [ユーザの識別]) の [LDAP 認証方法] で [シンプル] を選択し、管理アカウントで使用されるユーザの認証情報を、初回の LDAP 接続時のみ平文で送信します。

セキュリティ保護を強化するため、以降の IWSS から LDAP サーバへのユーザログオン認証ではすべて、Kerberos または Digest-MD5 の高度な認証方法を使用します。

LDAP 設定

[ユーザ / グループ名] の識別方法でネットワークの LDAP サーバにリンクされたポリシーを設定するには、まず LDAP 設定を設定します。

ユーザをユーザ / グループ名で識別するよう IWSS を設定するには

1. メインメニューから [HTTP] → [設定] → [ユーザの識別] の順に選択します。
2. [ユーザの識別方法] で、[ユーザ / グループ名] を選択します。
3. [選択] リンクをクリックします。
4. 次のブラウザウィンドウで、サポートされている LDAP サーバの一覧から使用している [LDAP ベンダー] を選択します。

   注意： Microsoft Active Directory の今後のバージョンでスキームが変更された場合に備え、IWSS ではユーザの識別名を構成する属性名を変更できるようにしています。Microsoft Active Directory 2000 または 2003 を使用している場合は、[初期設定] オプションを選択してください。

5. [LDAP 接続の設定] 画面で、[保存] をクリックして LDAP ベンダーの設定を確認します。
6. [ユーザの識別設定] 画面の [LDAP サーバのホスト名] に FQDN (完全修飾ドメイン名) で入力します。

   注意： [LDAP サーバのホスト名] には IP アドレスも入力できますが、IP アドレスを使用すると識別側 LDAP サーバと Kerberos サーバの間で不一致が生じる場合があるため、完全修飾ドメイン名で入力することをお勧めします。

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

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

8. 認証情報として、少なくとも LDAP サーバに対する読み取り権限を持つ [アカウント] と [パスワード] を入力します。ドメインが us.example.com の場合、次のようになります。

   - Microsoft Active Directory には、UserPrincipalName を管理者アカウントとして使用します。例 : NT_Logon_ID@us.example.com
   - OpenLDAP および Sun Java System Directory Server 5.2 には、識別名 (DN) を管理者アカウントとして入力します。例 : uid=LOGON_ID,ou=People,dc=us,dc=example,dc=com

9. [基本識別名] を入力して、IWSS で LDAP 検索を開始するディレクトリツリーのレベルを指定します。

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

注意： Active Directory サーバでグローバルカタログ (GC) ポートを有効にしている場合は、グローバルカタログを有効にした Active Directory のルートドメインを使用します。たとえば、dc=us,dc=example,dc=com ではなく dc=example,dc=com となります。

10. LDAP 認証方法に [シンプル] または [詳細] のいずれかを選択します。[詳細] 認証を選択した場合は、次の認証方法を使用します。

- Microsoft Active Directory および OpenLDAP の場合 — Kerberos
- Sun Java System Directory Server 5.2 (旧 Sun ONE Directory Server) の場合 — Digest-MD5

詳細認証を使用するには、さらに次のパラメータも設定します。

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

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

11. クライアントが指定の LDAP サーバまたは Kerberos サーバで認証できない場合は、ネットワーク上の他の LDAP サーバまたは Kerberos サーバを確認するように IWSS を設定できます。[リフェラル追跡を有効にする] チェックボックスをオンにして、[プライマリ参照サーバ ...] と [セカンダリ参照サーバ ...] リンクをクリックします。他の LDAP サーバの情報を入力します。

注意： Active Directory を使用してグローバルカタログポート (初期設定 = 3268) を有効にしている場合は、IWSS のリフェラル追跡はサポートされません。グローバルカタログポートが有効になっている場合、IWSS は異なるメカニズムで Active Directory サーバに問い合わせるため、参照サーバを設定すると重複してしまいます。

12. 情報が正しく入力されたかどうか、および設定した LDAP サーバと IWSS が通信できるかどうかを検証するには、[ユーザの識別] 画面で [LDAP 接続のテスト] をクリックします。LDAP サーバと正常に接続されたことを示すメッセージボックスが表示されます。

13. [保存] をクリックします。

注意 : LDAP ディレクトリにアカウントを持たないネットワークユーザにゲストポリシーを適用するには、ゲストアカウントを有効にして IWSS サーバ上の要求を受信するゲスト用ポートを設定します (初期設定 = 8081)。ゲストアカウントの有効化とゲスト用ポートの設定方法については、107 ページの「ゲストポリシーのゲスト用ポートの有効化」を参照してください。ゲスト用ポートが有効でない場合、インターネットを閲覧できるのは LDAP ディレクトリ内のユーザだけとなります。

ゲストポリシーのゲスト用ポートの有効化

LDAP ディレクトリにアカウントを持たないネットワークユーザにインターネット接続を許可してゲストポリシーを適用するには、IWSS と通信するクライアントに対してゲスト用ポートを開きます。

ゲスト用ポートを有効にするには

1. メインメニューから [HTTP] → [設定] → [ユーザの識別] の順に選択します。
2. [ユーザの識別設定] 画面で、[ユーザ / グループ名] を選択し、指定するディレクトリサーバを入力します。
3. [保存] をクリックします。
4. 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。
5. [プロキシ検索設定] 画面で、[ゲストアカウントを有効にする] チェックボックスをオンにします。
6. [保存] をクリックします。

第 6 章

HTTP 検索の設定

本章で説明する内容には、次の項目が含まれます。

- 110 ページの「HTTP 検索の有効化の確認」
- 110 ページの「HTTP 検索ポリシーの作成」

HTTP 検索の有効化の確認

HTTP 検索の有効化を確認するには

1. メインメニューから [概要] をクリックします。
2. [HTTP トラフィック] の横のリンクが [オン] になっている場合は、リンクをクリックします。[オフ] の場合は、リンクをクリックする必要はありません。

HTTP 検索ポリシーの作成

初期設定のグローバルポリシーとゲストポリシーのほかに、組織の特別なメンバー用にカスタマイズした HTTP ウイルス検索ポリシーを作成できます。

新しい HTTP 検索ポリシーを作成するには

1. 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。
2. [ウイルス検索を有効にする] を選択して、ポリシーをオンにします。
3. [追加] をクリックします。
4. 分かりやすい [ポリシー名] を入力します。「エンジニア向けウイルスポリシー」や「研究者向け URL フィルタポリシー」など、ポリシーを適用するユーザやグループへの参照を含むポリシー名にすると、見分けやすくなります。
5. このポリシーを適用するユーザを選択します。この画面のオプションは、使用しているユーザの識別方法に応じて異なります。[IP アドレス]、[ホスト名 (変更された HTTP ヘッダ)]、または [ユーザ / グループ名] のいずれかになります。ユーザの識別方法の設定とポリシー適用範囲の定義の詳細については、100 ページの「ユーザ識別方法の設定」を参照してください。

注意 : 設定したユーザの識別方法に関係なく、クライアントの IP アドレスによってポリシーを適用できます。

6. 適用するアカウントを定義したら、[次へ] をクリックして HTTP ウイルス検索ルールの定義を続行します。

Web レピュテーションルールの指定

Web レピュテーションルールはポリシーレベルで作成されます。

Web レピュテーションルールを指定するには

1. Web レピュテーションがグローバルレベルで有効になっていることを確認します。

   Web レピュテーションは、ポリシーレベルで使用するため、グローバルレベルで有効にする必要があります ([HTTP] → [HTTP 検索] → [ポリシー |Web レピュテーションを有効にする] チェックボックス)。

2. Web レピュテーションがポリシーレベルで有効になっていることを確認します。

   [HTTP] → [HTTP 検索] → [Policies | Web Reputation Rule] 画面の [追加] または [Edit] オプションを使用して、[このポリシーで Web レピュテーションルールを使用する] チェックボックスがオンになっていることを確認します。このチェックボックスは、初期設定でオンになっています。

3. URL ブロックの感度レベルを指定します。

   Web レピュテーションスコアを受信すると、Trend Micro InterScan Web Security Suite (以下、IWSS) はそのスコアがしきい値を下回っているか上回っているかを判断します。しきい値は、ユーザが設定した感度レベルによって定義されます。初期設定の感度レベルは中です。この設定は、誤検出を抑えながら、ほとんどの Web 脅威をブロックするため、お勧めします。

4. ファーミング / フィッシング検出を許可または無効にします。

   初期設定では、ファーミング / フィッシング検出は有効になっています。

Web レピュテーション設定

Web レピュテーション設定では、次の項目を指定します。

- 検索方法
- URL 除外リスト

- 感染した URL に関するフィードバックをトレンドマイクロに提出するかどうか
- URL がブロックされない評価モードで Web レピュテーションを評価するかどうか

Web レピュテーションの有効化と無効化

IWSS では、Web レピュテーションをグローバルレベルとポリシーレベルで有効 / 無効にすることができます。Web レピュテーションをグローバルレベルで無効にした場合は、自動的にポリシーレベルでも無効になります。

Web レピュテーションを有効 / 無効にするには

1. メインメニューで [HTTP] → [HTTP 検索] → [ポリシー] の順に選択します。
2. [検索ポリシー] 画面で、[Web レピュテーションを有効にする] チェックボックスをオンまたはオフにして、Web レピュテーションを有効または無効にします。

Web レピュテーション除外の指定

Web レピュテーション除外は、Web サイトの URL 全体、URL のキーワード、または URL の一部を入力するか、または既存の URL の除外リストをインポートすることにより定義できます。

Web レピュテーション除外を指定するには

1. メインメニューで [HTTP] → [HTTP 検索] → [設定 |Web レピュテーション除外リスト] タブの順に選択します。
2. 一致した種類を指定するか、URL 除外リストをインポートします。

   初期設定のオプションは、[前方一致] (Web サイトの URL 全体) です。
3. [保存] をクリックします。

   Web レピュテーションに対する除外として特定の URL を指定してから、承認するリスト内の URL を選択して [削除] をクリックすると、その URL を Web レピュテーションに含めることもできます。承認するリスト内のすべての URL を Web レピュテーションに含めるには、[すべて削除] をクリックします。

Web レピュテーション結果の管理

IWSS には、Web レピュテーションの結果を管理するためのオプションが 2 つあります。(1) 感染した URL に関するフィードバックを提出して Web レピュテーションデータベースを改善するオプションと、(2) 既存の Web アクセスポリシーに影響を与えずに Web レピュテーションの有効性を監視するオプションです。どちらか一方または両方のオプションを選択できます。

フィードバックオプション

現行の動的な URL ブロックリストに加えて、検索エンジン検索結果を URL ローカルキャッシュと外部のバックエンド評価サーバにフィードバックできます。Trend Micro Feedback Engine (以下、TMFBE) では、IWSS が検索エンジン検索結果をバックエンド評価サーバに送り返すためのフィードバックメカニズムが用意されています。このフィードバックオプションは初期設定で有効になっています。

注意 : 上位プロキシモードを使用する場合、IWSS の IP アドレスがトレンドマイクロのサイト (trendmicro.com) にアクセスできるように明示的にプロキシサーバを設定する必要がある場合があります。

感染が検出されなかった場合

検索エンジンからの検索結果で感染が検出されなかった場合、その URL は URL ローカルキャッシュに保存されます。これによって、検索エンジンで同じ URL が再度検索されることがなくなります。

感染が検出された場合

検索エンジンからの検索結果で感染が検出された場合、感染した URL は次の場所に送り返されます。

- 動的な URL ブロックリスト
- Web レピュテーションスコアを調整した URL ローカルキャッシュ

- VirusName と IntelliTrap フラグを含む TMFBE フィードバックバッファ。このバッファのエントリ数が 10 になるか、または、最後のフィードバックから 5 分が経過すると、これらの URL が順次バッチでバックエンド評価サーバに送信されます。

監視のみのオプション

監視のみのオプションでは、Web レピュテーション結果を評価する機会が与えられます。このオプションを選択した場合、URL ブロックログまたはセキュリティリスクレポートから Web レピュテーション結果を監視できます。この結果には、Web レピュテーション、フィッシング対策、およびファーミング対策によってフィルタにかけられた URL のみが含まれます。Web レピュテーション結果のみ監視するため、URL ブロックは発生せず、URL はクライアントに渡されます。

初期設定で、監視のみのオプションは無効になっています。

URL キャッシュのクリア

ユーザがある URL にアクセスしようとすると、IWSS はこの URL についての情報をリモートデータベースの Web レピュテーションデータベースから取得し、ローカル URL キャッシュに保存します。リモートサーバ上に Web レピュテーションデータベースを配置して、そのデータベース情報を使用してローカル URL キャッシュを構築すると、IWSS 上のオーバーヘッドを削減して、パフォーマンスを向上させることができます。

要求された URL に対して Web レピュテーションデータベースから URL キャッシュに保存される情報の種類は、次のとおりです。

- Web カテゴリ
- ファーミング / フィッシング検出で使用されるファーミングフラグとフィッシングフラグ
- URL をブロックするかどうかを判断するために使用される Web レピュテーション評価の結果 (111 ページの「Web レピュテーションルールの指定」を参照)

検索をすばやくするため、URL キャッシュには、頻繁にアクセスされる URL が保存されます。新しい URL の検索が必要な場合、または、キャッシュサイズがパフォーマンスに影響を及ぼす場合のみ、キャッシュをクリアします。

注意： キャッシュをクリアすると、HTTP 検索デーモンが停止して再起動されます。これによって、IWSS サービスが中断する場合があります。

URL キャッシュをクリアするには

1. メインメニューで [HTTP] → [設定] → [URL キャッシュ] の順に選択します。
2. [キャッシュをクリア] をクリックします。

HTTP ウイルス検索ルール

管理者は、ブロックするファイルタイプと検索するファイルタイプ、および圧縮ファイルとサイズの大きいファイルの処理方法を設定できます。

ブロックするファイルタイプの指定

セキュリティ、監視、またはパフォーマンス上の目的のためにブロックするファイルのタイプを識別できます。ブロックされたファイルは、要求先のクライアントによって受信されることも、検索されることもありません。ブロックされたファイルの取得要求は実行されません。Java クラスファイル、実行可能ファイル、Microsoft Office 文書、オーディオ / ビデオファイル、画像、または設定するその他のファイルタイプなどのファイルタイプをブロックするオプションが提供されています。

ブロックするファイルタイプを指定するには

1. ポリシーの追加または変更時に、[ブロックするファイルタイプ] でブロックするファイルタイプを選択します。
2. ブロックするその他のファイルタイプを [その他] フィールドに入力します。複数のエントリを区切るにはスペースを使用します。ブロック可能なその他のファイルタイプを、対応する MIME コンテントタイプとともに入力する方法については、237 ページの「ファイルタイプと MIME コンテントタイプの対応」を参照してください。

検索するファイルタイプの指定

トレンドマイクロの推奨設定と実際のファイルタイプの詳細は、38 ページの「トレンドマイクロの推奨設定について」および 38 ページの「実際のファイルタイプ」を参照してください。

検索するファイルタイプを選択するには

IWSS は、IWSS を通過するすべてのファイル、または実際のファイルタイプチェック (トレンドマイクロの推奨設定) またはファイル拡張子によって決定されるファイルのサブセットのみを検索できます。さらに、圧縮ファイル内に含まれる個々のファイルも検索できます。

1. 検索するファイルを選択します。

   - ファイル名の拡張子に関係なく、すべてのファイルタイプを検索するには、[検索可能なすべてのファイル] を選択します。IWSS は、圧縮ファイルを開いてその中のすべてのファイルを検索します。これは、最も安全な推奨設定です。
   - 実際のファイルタイプによる識別を使用するには、[トレンドマイクロの推奨設定] を選択します。この設定では、ファイルの実際のファイルタイプを確認することで、ウイルスが潜伏していることが分かっているファイルタイプを検索します。実際のファイルタイプの確認は、ファイル名の拡張子とは無関係に行われるので、実際のファイルタイプを隠すために潜在的に有害なファイルの拡張子が変更されるのを防ぎます。
   - すべての HTTP トラフィックを検索する際に起こりうるパフォーマンスの問題を回避するために、拡張子に基づいて検索するファイル、または除外するファイルタイプを明示的に設定できます。ただし、ファイル拡張子はファイルの内容を判定するのに信頼できる方法ではないため、この設定はお勧めしません。

     トレンドマイクロはこの設定をお勧めしませんが、選択したファイルタイプのみを検索するには、[指定のファイル拡張子] を選択してリストをクリックします。[拡張子による指定] 画面が開きます。初期設定の拡張子リストは、ウイルスが潜伏している可能性があると知られているすべてのファイルタイプを示しています。このリストは、ウイルスパターンファイルがリリー

スされるとアップデートされます。[拡張子による指定] 画面で、[その他の拡張子] フィールドに追加の拡張子を追加するかまたは除外します。入力が完了したら [OK] をクリックします。画面が閉じます。

注意： 検索する、または検索から除外する拡張子をピリオドを入れずに入力します。通常は 3 文字です。拡張子の前にワイルドカード (*) 文字は付けないでください。また、複数のエントリはセミコロンで区切ります。

2. 特定の MIME コンテントタイプを選択的に無視するように IWSS を設定できます。RealAudio やその他のストリーミングコンテンツなどのファイルタイプは、ファイルの最初の一部がクライアントコンピュータに到着するとただちに再生されるため、結果的に遅延が発生して正しく動作しません。[ウイルス検索ルール] タブの [検索を省略する MIME コンテントタイプ] に適切な MIME タイプを追加することにより、IWSS でこれらのファイルタイプを検索から除外できます。[検索を省略する MIME コンテントタイプ] フィールドに、無視する MIME コンテントタイプを入力します。たとえば、image/、audio/、application/x-director video/、application/pdf です。

注意： トレンドマイクロは、ウイルス感染の脅威を軽減するために、除外する MIME コンテントタイプのリストを最小限に抑えることをお勧めします。さらに、MIME コンテントタイプの偽造が可能なため、サイズの大きいファイルの処理が有効になっているときには、どの MIME コンテントタイプも除外しないことをお勧めします。

HTTP 検索設定の優先順位

IWSS 検索は、次の優先順位に従って実行されます。

1. 除外する MIME コンテントタイプ
2. ブロックするファイルタイプ
3. 検索するファイルタイプ

圧縮ファイルの検索制限の設定

圧縮ファイルの検索制限は、[HTTP] → [HTTP 検索] → [ポリシー] → [検索ポリシー] 画面の [追加] または [編集] オプションを使用して設定できます。IWSS は、HTTP ウイルス検索設定画面で指定された条件に従って、圧縮ファイルの内容を検査します。また、IWSS は、設定可能な制限 (圧縮アーカイブ内のファイル数、圧縮ファイルのサイズ、圧縮レベル、および圧縮率) に従ってファイルを解凍します。

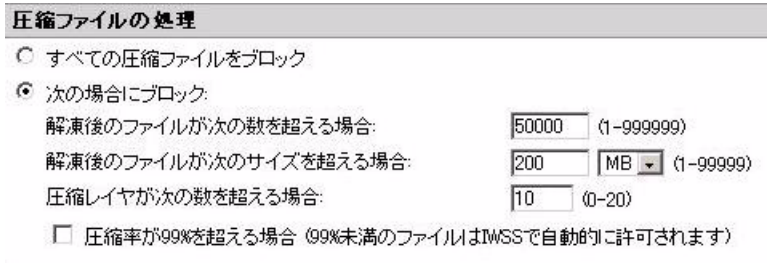


図 6-1. 「解凍の割合」を使用して IWSS サーバに対する DoS 攻撃を防ぐことができる

圧縮ファイルの検索制限を設定するには

[圧縮ファイルの処理] で、次の 2 つのオプションから選択します。

- **[すべての圧縮ファイルをブロック]** — 圧縮ファイルをダウンロードする要求はすべて実行されません。
- **[次の場合にブロック]** — 設定された条件を超える圧縮ファイルをダウンロードする要求は実行されません。次のパラメータの値を入力します。
    - 解凍後のファイルが次の数を超える場合 (初期設定は 50000)
    - 解凍後のファイルが次のサイズを超える場合 (初期設定は 200MB)
    - 圧縮レイヤが次の数を超える場合 (0 ～ 20、初期設定は 10)
    - 圧縮率が 99% を超える場合 (圧縮率が 99% 未満のファイルは IWSS によって自動的に許可されます)

条件のいずれかを満たす圧縮ファイルはゲートウェイでブロックされます。

サイズの大きいファイルの処理

サイズの大きいファイルの処理は、[HTTP] → [HTTP 検索] → [ポリシー] → [検索ポリシー] 画面の [追加] または [編集] オプションを使用して設定できます。

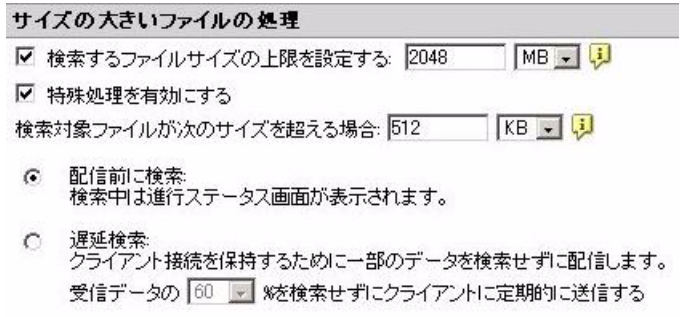


図 6-2.　サイズの大きいファイルの処理

IWSS には、サイズの大きいファイルが見つかったときに備えて、ブラウザがタイムアウトしない方法で検索する設定が用意されています。非常にサイズの大きいファイルをダウンロードする際に、そのファイルが安全であると想定できるときは、パフォーマンスの問題を軽減する [検索するファイルサイズの上限を設定する] チェックボックスをオンにすると、サイズの大きいファイルの検索を無効にできます。

サイズの大きいファイルの検索を無効にするには

- [サイズの大きいファイルの処理] で [検索するファイルサイズの上限を設定する] チェックボックスをオンにして、検索するファイルの上限を設定します。初期設定は、2,048MB です。

ネットワークにセキュリティの脆弱性が生じるため、サイズの大きいファイルであっても、検索は無効にしないことをお勧めします。

HTTP ウイルス検索でサイズの大きいファイルの処理を使用するには

1. [サイズの大きいファイルの処理] で [特殊処理を有効にする] チェックボックスをオンにして、サイズの大きいファイルと見なすファイルサイズ (KB または MB) を入力します。初期設定値は、512KB です。
2. 使用するサイズの大きいファイル処理のタイプを選択します (120 ページの「配信前に検索」および 121 ページの「遅延検索」を参照)。
   - **遅延検索** — ファイルの一部を検索せずに配信し、残りを後で検索します (クライアント接続は有効なまま保持されます)。ウイルスが見つかると接続を停止します。
   - **配信前に検索** — 検索中の進行ステータスをクライアント上に表示し、その後ファイルを配信します。これは初期設定の動作です。
   - **受信データの xx % を検索せずにクライアントに定期的に送信する** — 割合 (%) を選択します。

   注意： Blue Coat Port 80 Security Appliance を ICAP モードで使用する場合、サイズの大きいファイルを処理できません。ただし、IWSS が Blue Coat Appliance に適した HTTP プロキシとして設定された場合、サイズの大きいファイルを処理できます。
3. [保存] をクリックします。

ユーザがファイルのダウンロードを試みているときにブラウザがタイムアウトする場合は、サイズの大きいファイルの処理の設定を検討します。サイズの大きいファイルの検索には、次の 2 つのオプションがあります。

配信前に検索

IWSS が配信前に検索するオプションを使用するように設定されている場合、要求されたファイルは検索が終了するまでクライアントに渡されません。ブラウザのタイムアウトを防ぎ、ユーザが接続に問題があると思わないように、進行ステータス画面が生成されます。これによって、検索が進行中であることをユーザに通知します。

遅延検索

IWSS が遅延検索オプションを使用するように設定されている場合は、検索が続行されている間に、設定可能な割合の Web ページがクライアントに配信されます。検索せずにクライアントに定期的に送信する受信データの割合の値を 100% に設定した場合、最後の 4KB は検索が完了するまでクライアントに送信されません。

遅延検索オプションを使用する場合は、検索せずにクライアントに定期的に送信する受信データの割合を設定します。

サイズの大きいファイルの処理に関する重要な注意

- サイズの大きいファイルの特殊処理は、HTTP 検索、FTP 検索、および HTTP プロキシを介した FTP over HTTP にのみ適用されます。一部の ICAP トラフィックには適用されません。この機能に未対応の ICAP クライアントを介してサイズの大きなファイルをダウンロードすると、タイムアウトの問題が発生する場合があります。

サイズの大きいファイルの処理に違反すると、要求元のクライアントのブラウザにユーザ通知が表示されます。

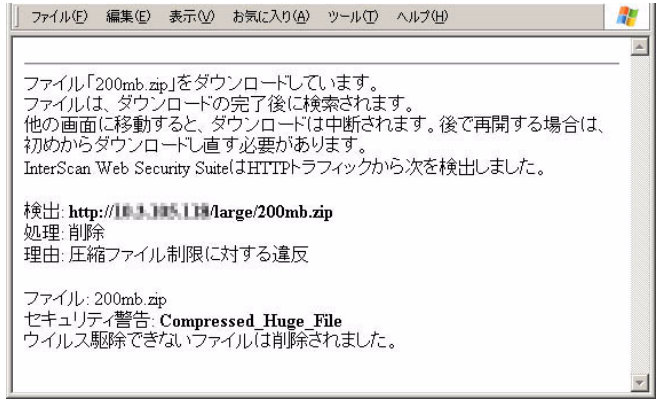


図 6-3.　検索の完了およびファイルのダウンロード後の通知

隔離ファイルの処理

IWSS で不正であるとして検出されたファイルを隔離する場合、[隔離ファイルを暗号化する] をオンにすると、ファイルを暗号化してから隔離フォルダに隔離することができます。これにより、意図せずにファイルを実行してしまったり、開いたりしてしまう可能性がなくなります。暗号化されたファイルは、トレンドマイクロのサポートエンジニアによってのみ暗号を解除できることに注意してください。

[HTTP] のポリシーの追加 / 編集画面で HTTP ウイルス検索ルールの設定が完了していれば、[次へ] をクリックしてスパイウェア検索ルールに移動します。

スパイウェア検索ルール

スパイウェアおよびその他の不正プログラムを検索するには

1. [HTTP] → [ポリシー] のポリシー編集画面、または [FTP] → [検索ルール] → [FTP 検索] 画面の [スパイウェア検索ルール] タブで、削除するその他の脅威のタイプを選択します。パターンファイルに署名があるすべての脅威を検索するには、[すべて選択] をオンにします。
2. [次へ] をクリックして、セキュリティの脅威に対する処理を設定します。

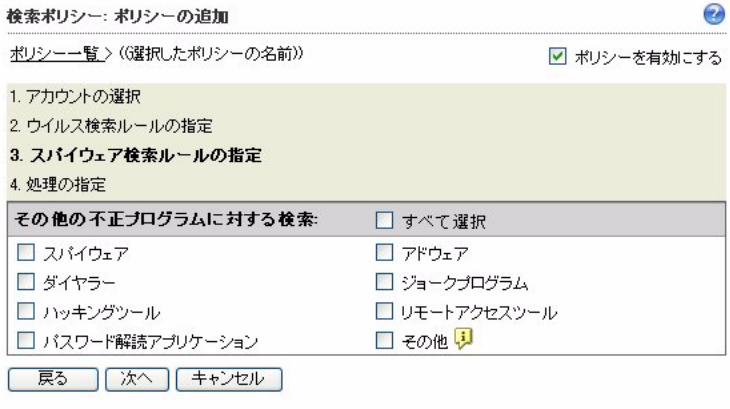


図 6-4. スパイウェアおよびその他の脅威の検索の設定

ウイルス検出時の処理設定

HTTP ウイルス検索ルールを設定した後、感染したファイル、パスワードで保護されたファイル、またはマクロを含むファイルが検出された場合に IWSS で実行する処理を設定します。

検索処理

ウイルス検索の結果に対応して IWSS が実行できる処理には、次の 4 つがあります。

- 感染ファイルをサーバで削除するには、[削除] を選択します。要求元クライアントはファイルを受信しません。この処理は、1 次処理、2 次処理、およびパスワードで保護されたファイルの検索イベントに適用できます。
- ファイルをクリーンナップせずに隔離ディレクトリに隔離するには、[隔離] を選択します。隔離ディレクトリの初期設定は次のとおりです。

  /etc/iscan/quarantine

  要求元クライアントはファイルを受信しません。この検索処理は、すべての 4 つの検索イベントに適用できます。オプションで、隔離ディレクトリに送る前にファイルを暗号化するように選択できます。詳細については、122 ページの「隔離ファイルの処理」を参照してください。
- IWSS では、感染したファイルを自動的に駆除および処理するには、[駆除] を選択します。要求元のクライアントは、ファイルが駆除可能であれば駆除されたファイルを受信します。駆除できない場合は、2 次処理が実行されます。この処理は、1 次処理とマクロ検索イベントに適用できます。マクロ検索イベントで [駆除] を選択することにより、新しい脅威に対応するパターンファイルが公開されるまでの間、緊急の措置として、ファイルに含まれるすべてのマクロを削除することができます。
- [放置] を選択すると、ファイルをそのまま要求元のユーザに配信します。この処理は、2 次処理、パスワードで保護されたファイル、およびマクロイベントに適用できます。マクロイベントについては、ウイルス大規模感染時にマクロを含むファイルをすべて削除するかまたは隔離しない限り、常に放置処理を実行することをお勧めします。

注意： 2 次処理で、検索処理として [放置] を選択することはお勧めしません。

検索イベント

検索の後、検索結果に合わせて 4 種類の処理を設定できます。

- **1 次処理** — ウイルスまたはその他の不正プログラムに感染していると判定されたファイルです。利用可能な処理には、[削除]、[隔離]、または [駆除] (推奨の処理で初期設定) があります。
- **2 次処理** — ファイルを感染させるウイルスまたは不正プログラムのタイプによって、検索エンジンは一部のファイルを駆除できない場合があります。利用可能な処理には、[削除] (推奨の処理で初期設定)、[隔離]、および [放置] があります。
- **パスワードで保護されたファイル** — パスワードで保護されているか暗号化されているため、検索できないファイルです。これらのタイプのファイルの感染状況を判定することはできません。利用可能な処理には、[削除]、[隔離] (推奨の処理で初期設定)、および [放置] があります。
- **マクロ** — マクロプログラムのコードを含む Microsoft Office のファイルです。亜種や新種が容易に作成できるのが特徴です。新しいウイルスパターンがパターンファイルに追加されて使用している環境に配信されるまで、すべてのファイルをブロックするため、ウイルス大規模感染の早い段階で、マクロを含むすべてのファイルを隔離できます。利用可能な処理には、[隔離]、[駆除]、および [放置] があります。アップデート済みのパターンファイルがリリースされる前のウイルス大規模感染時にマクロを隔離するか削除する必要がない限り、マクロに対する処理は常に放置に設定することをお勧めします。

備考欄への入力

IWSS で検出されたファイルに対する処理を設定した後、ポリシーに関する説明を記録するには、画面下部の [備考] フィールドを使用します。

- ポリシーに適用する検索処理の設定が完了したら、[保存] をクリックします。[ポリシーの配信] をクリックして、ポリシーをただちに適用します。そうしない場合、ポリシーはデータベースキャッシュの有効期限が切れた後に適用されます。

第 7 章

アプレット /ActiveX 対策の設定

本章で説明する内容には、次の項目が含まれます。

- 126 ページの「アプレット /ActiveX 対策の有効化」
- 132 ページの「アプレット /ActiveX 対策の設定」

アプレット /ActiveX 対策の有効化

不正なアプレットと ActiveX オブジェクト対策のために HTTP トラフィックの検索を開始するには、[アプレット /ActiveX 対策ポリシー] 画面または [概要] → [検索] 画面で検索を有効にする必要があります。

HTTP トラフィックでの不正なアプレット /ActiveX の検索を有効にするには

1. メインメニューから [HTTP] → [アプレット /ActiveX 対策] → [ポリシー] の順に選択します。または、メインメニューから [概要] をクリックします。
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ます。
3. [保存] をクリックします。

アプレット /ActiveX 検索ポリシーの追加と変更

新しいポリシーを設定するには、まず、ポリシーを適用するクライアントアカウントを設定します。

すべての設定可能なポリシーは [アプレット /ActiveX 対策ポリシー] 画面上に一覧表示されています。この画面は、[HTTP] → [アプレット /ActiveX 対策] → [ポリシー] から使用できます。

ポリシーの範囲を変更するには

1. メインメニューから [HTTP] → [アプレット /ActiveX 対策] → [ポリシー] の順に選択し、[アプレット /ActiveX 対策ポリシー] 画面を開きます。

2. 次のいずれかを実行します。

   - ポリシーの範囲からアカウントを削除するには、ユーザを選択して [削除] をクリックしてから、[保存] をクリックします。
   - ポリシーの範囲にアカウントを追加するには、[ポリシー名] をクリックして [アカウント] タブに切り替え、ポリシーを適用するアカウントを追加または削除し、[保存] をクリックします。

3. [ポリシーの配信] をクリックします。変更されたポリシーが配信されるまでポリシーの範囲への変更は有効になりません。

ポリシーの範囲を設定したら、アプレットと ActiveX の検索ルールを設定します。

Java アプレット対策ルールの設定

[HTTP] → [アプレット /ActiveX 対策] → [ポリシー] 画面で、新しいポリシーを追加するかまたは、既存のポリシーを選択します。[Java アプレット対策ルール] タブでは、すべてのアプレットをブロックするか、またはセキュリティ設定で指定してアプレットを受け入れて処理するように、Trend Micro InterScan Web Security Suite (以下、IWSS) を設定できます。

署名ステータス

デジタル署名は、アプレットの本物の発行元を確認する方法です。また、デジタル署名により、アプレットが改ざんされていないこと、または発行以来変更されていないことを確認できます。アプレットの署名を分析した後、IWSS は次のいずれかの判定をします。

- 有効な署名
- 署名なし ― アプレットが未署名
- 無効な署名 ― アプレットの署名が壊れているか、信頼するルート証明書が見つからないなどの理由で確認できない。

アプレットの署名の確認は、2 段階で実行します。まず、署名内のデータに対するアプレットの整合性を確認します。次に、証明書の整合性、つまり署名を作成するために使用される「証明書チェーン」を確認します。署名が有効と見なされるには、IWSS で信頼されていると分かっている証明書で証明書チェーンの確認が終了している必要があります。管理コンソールで [HTTP] → [アプレット /ActiveX 対策] → [デジタル証明書] → [アクティブな証明書] を開くと、これらの証明書のセットを表示および管理できます。

証明書のステータス

Java アプレット対策ルールは、証明書のステータスに基づいて、有効な署名のあるアプレットに対し、異なる処理を適用できます。

初期設定で、IWSS はそのアクティブな証明書を信用します。ただし、証明書チェーンで証明書を持つアプレットを信用しない場合は、アクティブな証明書に「フラグを付ける」ことができます。フラグ付きの証明書は、フラグ付きのステータスが表示されますが、引き続きアクティブな証明書としてリストされます。

計測処理と再署名

計測処理は、IWSS が監視コードおよび制御コードをアプレットに追加するプロセスです。計測処理ではアプレットの署名が削除されるので、必要な場合は、計測処理の後に再署名するように設定することもできます。このように設定すれば、計測処理されたアプレットがブラウザ内で確実に実行され、期待どおりに操作が実行されるようになります。

アプレットの計測処理設定

アプレットの計測処理の目的は、クライアントコンピュータ上で禁止された操作が実行されないようにすることです。初期設定では、IWSS により処理される Java アプレットの次のタイプの操作が許可されていません。

- **破壊的な操作** — ファイルの削除と名前変更
- **非破壊的な操作** — ディレクトリ内のファイルの一覧表示やファイルの属性情報の取得
- **書き込み** — 新しいファイルの書き込みまたは既存のファイルの変更
- **読み取り** — ファイルの内容の読み取り

除外設定

選択的に許可または禁止できる各タイプの操作に、対策ポリシーを適用しないファイルまたはフォルダを設定できます。

- ファイルのサブセットによって実行される場合を除き、任意のタイプのファイル操作を許可するには、ファイル操作の隣の [許可] ボタンをオンにします。[除外設定] リンクをクリックします。[ファイル操作の除外設定] 画面が表示されます。操作を許可しないファイルとフォルダを設定します。
- ファイルのサブセットによって実行される場合を除き、全般的に任意のタイプのファイル操作を禁止するには、ファイル操作の隣の [禁止] ボタンをオンにします。[除外設定] リンクをクリックして、操作を許可するファイルとフォルダを設定します。

Java アプレットの処理を設定するには

1. ポリシーの範囲を設定した後、次のいずれかを実行します。
   - IWSS で署名と証明書のステータスに基づいてアプレットを放置、ブロック、または計測処理するには、[次の設定を使用してアプレットを処理] を選択します。
   - IWSS で、すべてのアプレットがクライアントに渡されないようにするには、[すべてのアプレットをブロック] を選択します。この設定を選択した場合は、手順ステップ 3 に進みます。
2. 次の署名と証明書のステータスについて、使用する処理を選択します (* は、初期設定のトレンドマイクロ推奨の設定を示します)。
   - **有効な署名と信頼された証明書を持つ** — 放置 *、アプレットの計測処理 (再署名)、アプレットの計測処理 (署名の削除)、ブロック
   - **有効な署名とフラグ付きの証明書を持つ** — 放置、アプレットの計測処理 (再署名)、アプレットの計測処理 (署名の削除)、ブロック *
   - **未署名** — 放置、アプレットの計測処理 *、ブロック
   - **無効な署名を持つ** — 放置、アプレットの計測処理 (署名の削除)、ブロック *

3. 選択的に有効または無効にできる 4 つの操作 (破壊的な操作、非破壊的な操作、書き込み、読み取り) について、[許可] または [禁止] ボタンをクリックして、対策ポリシーを設定します。

4. [除外設定] ボタンをクリックし、対策ポリシーから除外されるファイルまたはフォルダを設定します。

   a. 設定した対策ポリシーを適用しないファイルのパスを [ディレクトリ / ファイル] に入力します。

      - 特定のファイルパスを設定するには、[ファイル名 (絶対パス)] をオンにします。
      - 対策ルールからフォルダ全体のコンテンツを除外するには、[このディレクトリ内のすべてのファイルを対象にする] をオンにします。
      - 対策ルールからフォルダとサブディレクトリ内のファイルをすべて除外するには、[このディレクトリとそのすべてのサブディレクトリ内のファイルを対象にする] をオンにします。

   注意 : すべてのファイルパスは、アプレットが実行されるクライアントコンピュータ上のパスです。ファイルパスの形式は、クライアント上で実行されている OS で要求される形式にする必要があります。

   b. [追加] ボタンをクリックして、任意の対策ポリシーに除外設定を追加します。

   c. アプレットのセキュリティ設定から除外するその他のファイルまたはディレクトリを設定します。

   d. ファイルとフォルダの除外設定が完了したら、[保存] をクリックします。

5. クライアントワークステーションのポートにアプレットのバインドを許可するには、[Java アプレット対策ルール] タブに戻り、[ローカルポートのバインド] を選択します。

6. アプレットの発信元サーバへの接続を許可するには、[リモートホストへの接続] を選択します。

7. ホスト接続を設定アプレット発信元以外のホストへの接続を許可するには、[ホスト接続] の隣にある [許可] または [禁止] をオンにして、対策ポリシーの除外設定を行います。

   a. 設定した対策ポリシーを適用しないホスト名を [ホスト] に入力します。

   b. [追加] ボタンをクリックして、任意の対策ポリシーに除外設定を追加します。

   c. 対策ポリシーを適用しないその他のホストを入力します。

   d. ポリシーの対策ルールから除外するホストの設定が完了したら、[保存] をクリックします。

8. アプレットに新しいスレッドグループの作成を許可するには、[新しいスレッドグループの作成] チェックボックスをオンにします。この操作を禁止するには、このチェックボックスをオフにします。

9. アプレットから LAN 上のクライアントへダウンロードされたスレッドの動作を IWSS が無視するように設定するには、[アクティブなスレッドの作成 (無制限)] チェックボックスをオンにします。アプレットが一度に作成できるスレッドの数を制限するには、このチェックボックスをオフにし、上限を指定します。

10. [アクティブなウィンドウの作成 (無制限)] を選択して、アプレットが開けるアクティブなトップレベルのウィンドウの数を制限します。提供されたテキストボックスに、許容できるウィンドウの数を入力します。このオプションをオフにすると、一部の不正な Java アプレットがユーザを邪魔するときのように、アプレットが無制限にウィンドウを開けるようになります。

11. このポリシーに関する今後の参照のために、オプションで [備考] を入力します。

12. 新しいアプレット /ActiveX ポリシーを設定している場合は、[次へ] をクリックして、ActiveX 対策ルールの設定を継続します。既存のポリシーを変更する場合は、[保存] をクリックします。

13. [ポリシーの配信] をクリックして、ポリシーをただちに適用します。そうしない場合、ポリシーはデータベースキャッシュの有効期限が切れた後に適用されます。

このポリシーに関する適切な情報を保存するための備考を入力し、[保存] をクリックします。

ActiveX 対策ルールの設定

ActiveX 対策ルールは、2 つの異なるタイプの ActiveX コントロールに適用できます。

- **実行可能キャビネットファイル (*.cab)** — Windows ネイティブ圧縮アーカイブ形式を使用して配信された ActiveX コントロール
- **ポータブル実行可能 (PE) ファイル (*.exe や *.ocx など)** — Windows の 32 ビット版と 64 ビット版のすべてにわたって「移植性」のある実行可能なファイル形式

これらの 2 つのファイルタイプごとに、次の対策ポリシーを設定できます。

- そのタイプのすべての ActiveX コントロールをブロックします。
- そのタイプのすべての ActiveX コントロールを許可します。
- 署名を確認し、場合によっては、無効な署名または未署名をブロックします。

このポリシーに関する備考を入力し、[保存] をクリックします。

アプレット /ActiveX 対策の設定

アプレット /ActiveX 対策ポリシーは、[アプレット /ActiveX 対策の設定] 画面で設定されたとおりに、証明書と署名のステータスを決定します。たとえば、IWSS は、署名の妥当性を検査するか、署名を削除してすべてのアプレットを未署名として処理するか、証明書の失効ステータスを確認することができます。さらに、IWSS は、計測処理後にアプレットに再署名できます。

ActiveX コントロールの署名の妥当性を検査するため、IWSS は、署名する証明書の有効期限を確認したり、署名する証明書を除く署名チェーン内すべての証明書を確認したり、証明書の失効情報源が利用可能であれば証明書の失効ステータスを確認したりできます。

Java アプレットおよび ActiveX の署名の妥当性を検査する方法を設定するには

1. メインメニューから [HTTP] → [アプレット /ActiveX 対策] → [設定] の順に選択します。

2. [Java アプレット] タブと [ActiveX 実行可能ファイル] タブの設定を完了します。
3. [保存] をクリックします。

アプレットの署名の妥当性を検査するための証明書の追加

Java アプレットの署名は、インストールされているルート証明書を使用して検査されます。ルート証明書のリストを表示するには、メインメニューで [HTTP] → [アプレット /ActiveX 対策] → [デジタル証明書] の順に選択します。ActiveX の署名は、IWSS サーバの Windows 証明書ストア内のルート証明書に対して検証が行われます。

IWSS とともにインストールされなかったルート証明書を使用して署名されたアプレットを実行する必要がある場合、その証明書を IWSS のデジタル証明書ストアに追加します。

証明書を IWSS の証明書ストアに追加するには

1. メインメニューで [HTTP] → [アプレット /ActiveX 対策] → [デジタル証明書] の順に選択します。
2. [アクティブな証明書] タブで、[追加] をクリックし、証明書を選択してから、[追加] をクリックします。
3. [アクティブな証明書] 画面に戻り、追加した証明書がリストに表示されていることを確認します。

証明書の有効期限

IWSS は、次のように設定できます。

- アプレットの署名に使用されている証明書の有効期限が切れていないかどうか確認します。
- チェーン内の証明書がすべて有効かどうかを確認します。

信頼されない署名ステータス

証明書パスにより、IWSS が証明書を信頼してよいかどうか判定できない場合は、アプレットの署名ステータスを次のように設定できます。

- 未署名、つまり、署名が削除されている
- 無効

証明書失効リスト (CRL)

デジタル証明書はその発行者によって取り消すことができます。IWSS は、ステータス確認元が利用可能な場合、証明書が失効しているかどうか確認できます。

IWSS が定義されたステータス確認元にアクセスできない場合、IWSS で、その証明書のステータスを有効、未署名 (削除された署名)、または無効と設定することができます。

アプレットの再署名

IWSS は、クライアントワークステーションに送信される前に、会社「固有の」秘密鍵で、計測処理したアプレットに再署名できます。アプレットは計測処理中に元の証明書を失うため、アプレットに再署名すると、クライアントの Web ブラウザが常時無制限にアプレットを受け入れるようになります。

再署名機能を使用するには、2 つの鍵が必要です。1) IWSS にインポートする必要のある「秘密鍵」と、2) クライアントの Web ブラウザにインポートする必要のある、「秘密鍵」に対応する「公開鍵」を含む証明書です。証明書により、ブラウザは計測処理されたアプレットに付いた署名を認識できます。この証明書がない場合、これらのアプレットは未署名アプレットとして取り扱われ、ブラウザによってブロックされるか、またはシステムリソースへのアクセスが制限されます。

IWSS は、PKCS12 鍵形式をサポートしています。まだ鍵がない場合は、既知の認証機関 (CA) から入手できます。

計測処理後にアプレットに再署名するには

1. [HTTP] → [アプレット /ActiveX 対策] → [設定] の順に選択して、[アプレット /ActiveX 対策の設定] 画面の [Java アプレット] タブで、[次の証明書を使用してアプレットに再署名する] をオンにします。
2. 再署名に使用する証明書へのパスを入力するか、[参照] をクリックしてその証明書に移動します。
3. 証明書の [パスワード] を入力します。
4. [追加] をクリックします。
5. [保存] をクリックします。

ActiveX の署名の妥当性検査

ActiveX コントロールの署名が有効かどうかを検証するには、Cab ファイルおよび PE ファイルについて複数の方法で ActiveX コントロールの証明書を確認できます。この妥当性検査には、署名する証明書や署名チェーンのすべての証明書の有効期限を確認したり、ステータス確認元が定義されている場合は証明書の失効テータスを確認する方法があります。

ActiveX コントロールの署名ステータスの確認方法を設定するには

1. メインメニューから [HTTP] → [アプレット /ActiveX 対策] → [設定] の順に選択し、[ActiveX 実行可能ファイル] タブをクリックします。
2. ActiveX コントロールの署名の確認方法を設定します。有効にする確認方法に対応するチェックボックスをオンにします。
   - 署名する証明書の有効期限を確認します。
   - 証明するパス内のすべての証明書の有効期限を確認します。
   - 証明書の失効ステータスを確認します。
   - 署名のタイムスタンプを確認します。このオプションを選択すると、失効した証明書に有効なタイムスタンプ直列署名がある場合、その証明書の署名は有効とみなされます。

   IWSS が証明書の発行者にアクセスできない場合、その署名のステータスを [有効] または [無効] のいずれかに設定できます。
3. [保存] をクリックします。

アプレット処理のためのデジタル証明書の管理

IWSS がアプレットの署名が信頼できると判断するには、署名のベースになっているルート認証機関 (CA) を IWSS の証明書ストアに追加する必要があります。

デジタル署名の作成には、次の 3 つのタイプのデジタル証明書が使用されます。

- 実際のアプレットの署名を検証するための公開鍵を含む、「エンド」証明書または「署名」証明書
- チェーン内の署名証明書または別の中間証明書を検証するための公開鍵を含む、1 つ以上の「中間」証明機関 (CA) 証明書
- チェーン内の最初の中間 CA 証明書、または、稀に直接署名証明書を検証するための公開鍵を含む、「ルート」CA 証明書。その他の有効な署名は、その署名のルート CA 証明書が IWSS によって認識され、アクティブで、フラグがついていなければ、信頼されます。

IWSS がアプレットの署名の処理中に未知の証明書を検出した場合、署名を含むアプレットの URL と一緒に証明書を「非アクティブ」リストに保存します。すべてのタイプの証明書は、この方法 (エンド、中間、およびルート) で収集されます。後で必要な場合、この方法で収集されたルート CA 証明書は、依存しているアプレットの署名が有効なものとして処理されるように、「アクティブ化」して IWSS に信頼させます。中間 CA とエンド証明書はアクティブ化できますが、そのルート証明書もアクティブ化されている場合にのみ有効となります。すなわち、中間 CA またはエンド証明書のアクティブ化によって、証明書を信頼させることはできません。ルート CA 証明書のみ信頼させることができます。ただし、どの証明書にもフラグを付けることができます。

IWSS の証明書ストア内の証明書に対して、次の操作を実行できます。

- **削除** — 証明書ストアから選択された証明書を削除します。
- **非アクティブ化** — IWSS の証明書ストアに証明書を保持しますが、その証明書パス内で使用する証明書は信頼しません。
- **アクティブ化** — ルート CA 証明書を信頼させます。
- **フラグ付け** — 証明書パス内の証明書を使用するすべての署名にフラグを付けます。
- **フラグの消去** — その証明書パス内の証明書を使用する証明書が信頼されるように、過去にフラグが付けられた証明書の信頼ステータスを復元します。

既存の証明書を表示するには

1. メインメニューから [HTTP] → [アプレット /ActiveX 対策] → [デジタル証明書] の順に選択します。
2. [アクティブな証明書] タブと [非アクティブな証明書] タブを切り替えて、どの証明書が IWSS で認識されているかを確認します。

信用する証明書を追加するには

1. メインメニューから [HTTP] → [アプレット /ActiveX 対策] → [デジタル証明書] の順に選択します。
2. [アクティブな証明書] タブがアクティブになっていることを確認します。
3. [追加] をクリックします。

   [証明書の追加] 画面が開きます。
4. 追加する証明書へのパスを入力するか、または [参照] をクリックしてその証明書に移動して、[追加] をクリックします。

注意： 証明書は通常、拡張子が .cer、.der、.crt のファイルに含まれています。前述のように、アクティブなルート CA 証明書のみが信用されるとみなされますが、すべてのアクティブな証明書にフラグを付けられることに注意してください。

画面が [アクティブな証明書] タブに戻ります。追加した証明書が、証明書のタイプとその有効期限とともに表示されます。

証明書を削除するには

1. メインメニューから [HTTP] → [アプレット /ActiveX 対策] → [デジタル証明書] の順に選択します。
2. 削除する証明書を選択します。
3. [削除] をクリックします。

信頼する証明書を非アクティブ化するには

1. メインメニューから [HTTP] → [アプレット /ActiveX 対策] → [デジタル証明書] の順に選択します。
2. [アクティブな証明書] タブがアクティブになっていることを確認します。
3. 非アクティブ化する証明書を選択します。
4. [非アクティブ化] をクリックします。
5. 選択した証明書が [非アクティブな証明書] タブに移動します。

証明書をアクティブ化するには

1. メインメニューから [HTTP] → [アプレット /ActiveX 対策] → [デジタル証明書] の順に選択します。
2. [非アクティブな証明] タブがアクティブになっていることを確認します。
3. アクティブ化する証明書を選択します。
4. [アクティブ化] をクリックします。
5. 選択した証明書は、[アクティブな証明書] タブに移動します。

証明書にフラグを付けるには

1. メインメニューから [HTTP] → [アプレット /ActiveX 対策] → [デジタル証明書] の順に選択します。
2. [アクティブな証明書] タブがアクティブになっていることを確認します。
3. フラグを付ける証明書を選択します。
4. [証明書にフラグを付ける] をクリックします。
5. フラグ付き証明書は、[アクティブな証明書] タブに残りますが、ステータス列に赤いフラグが表示されます。

証明書からフラグを削除するには

1. メインメニューから [HTTP] → [アプレット /ActiveX 対策] → [デジタル証明書] の順に選択します。
2. [アクティブな証明書] タブがアクティブになっていることを確認します。
3. フラグを消去する証明書を選択します (フラグ付きステータスの証明書には、ステータス列に赤いフラグが表示されます)。
4. [証明書のフラグを消去] をクリックします。
5. フラグ付き証明書は、[アクティブな証明書] タブに残りますが、ステータス列に赤いフラグが表示されません。

クライアント側アプレットのセキュリティ通知

IWSS の Java アプレット対策ポリシーに対応して、クライアントのブラウザに表示される警告メッセージがいくつかあります。

署名または証明書ステータスのためにアプレットがブロックされている場合、要求元のクライアントには、アプレットをブロックしたポリシーとその理由を示すメッセージが表示されます。

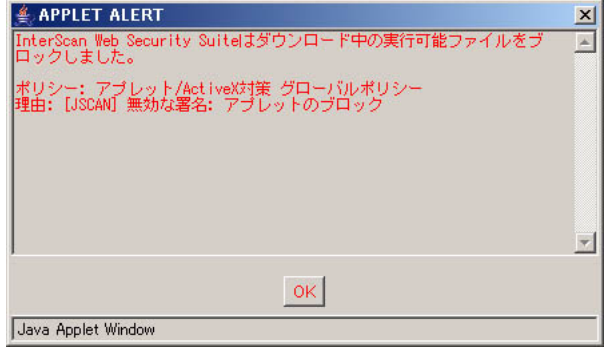


図 7-1. ブロックされたアプレットの通知

計測処理されたアプレットがポリシー設定で許可されていない操作を実行しようとすると、拒否された操作の通知が表示され、ユーザに操作の選択を求めます。利用可能なオプションは次のとおりです。

- **許可** — 計測処理されたアプレットは、ポリシーで許可されていない操作を含め、引き続き実行されます。
- **禁止** — アプレット対策ポリシーの対象となっている操作は停止されますが、計測処理されたアプレットは引き続き実行されます。
- **アプレットの停止** — 計測処理されたアプレットが終了します。

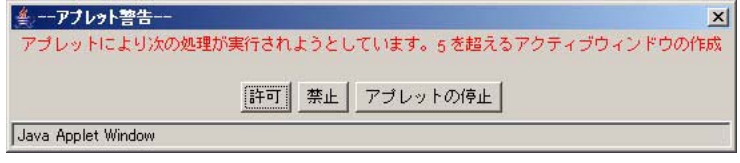


図 7-2.　アプレット対策違反通知

クライアントが [アプレットの停止] を選択した場合、アプレットが終了したことを示す別の通知が表示されます。

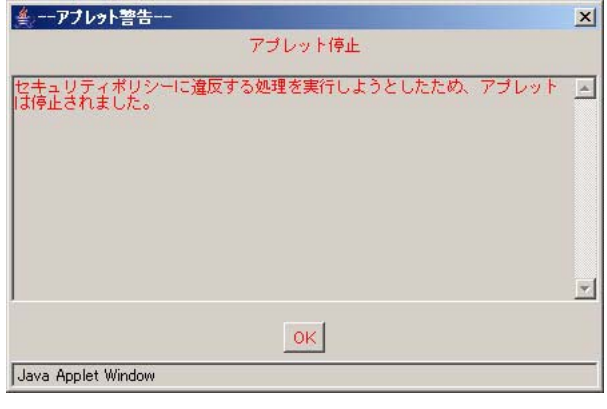


図 7-3.　アプレット実行終了通知

第 8 章

URL フィルタおよび IntelliTunnel ポリシー

本章で説明する内容には、次の項目が含まれます。

- 144 ページの「URL フィルタポリシーの管理」
- 145 ページの「新しいポリシーの作成」
- 147 ページの「URL フィルタの設定」
- 153 ページの「新しい IntelliTunnel ポリシーの作成」

URL フィルタポリシーの管理

Trend Micro InterScan Web Security Suite (以下、IWSS) は、初期設定されている次の 2 つの URL フィルタポリシーで事前設定されています。ネットワーク上のすべてのクライアントに適用されるグローバルポリシーと、ゲストポートを介して IWSS にアクセスするクライアントに適用されるゲストポリシーです。

注意 : ゲストポリシーは、IWSS が LDAP 対応の HTTP プロキシ転送モードで実行している場合にのみサポートされます

URL フィルタの有効化

URL フィルタモジュールが有効になっていることを確認してから、作業を開始してください。

URL フィルタを有効にするには

1. メインメニューから [HTTP] → [URL フィルタ] → [ポリシー] の順に選択します。
2. [URL フィルタを有効にする] チェックボックスをオンにします。
3. [保存] をクリックします。

新しいポリシーの作成

新しい URL フィルタポリシーを作成するには、次の 2 つの手順に従います。

- ポリシーを適用するアカウントを選択します。
- 業務時間および業務時間外にブロックする Web サイトのカテゴリを指定します。

新しいポリシーを作成するには

1. IWSS Web コンソールを開き、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。
2. [追加] をクリックします。

   [URL フィルタポリシー : ポリシーの追加] 画面が表示されます。
3. わかりやすい [ポリシー名] を入力します。

   「研究者向け URL フィルタポリシー」のように、適用対象となるユーザまたはグループへの参照が含まれるポリシー名は簡単に覚えられます。
4. ポリシーを適用するユーザを選択します。

   この画面のオプションは、使用しているユーザの識別方法に応じて異なり、[IP アドレス]、[ホスト名 (変更された HTTP ヘッダ)]、または [ユーザ / グループ名] (LDAP) のいずれかになります。ユーザの識別方法の設定とポリシー適用範囲の定義の詳細については、100 ページの「ユーザ識別方法の設定」を参照してください。
5. [次へ] をクリックします。
6. [ルールの指定] 画面で、[ポリシーを有効にする] チェックボックスがオンになっていることを確認します。

7. アクセスを制限する URL のカテゴリを選択します。

   - 業務時間中にブロックするカテゴリのチェックボックスをオンにします。グループの全カテゴリを選択するには、対象グループで [すべて選択] をクリックします。グループ内のすべてのカテゴリを選択するのに、グループを展開する必要はありません。アクセスを制限する期間は、[URL フィルタ設定] 画面 ([業務時間] タブ) で定義されます。
   - 業務時間外にブロックするカテゴリのチェックボックスをオンにします。グループの全カテゴリを選択するには、対象グループで [すべて選択] をクリックします。グループ内のすべてのカテゴリを選択するのに、グループを展開する必要はありません。指定されていない時間帯は、「業務時間外」とみなされます。

   グループ内のリストは変更できません。

8. 今後の参照のためにこのポリシーに関して役立つ情報を含めるには、オプションの [備考] を入力します。

9. [保存] をクリックします。

10. [URL フィルタポリシー] 画面で、[優先度] 列に表示されている上向きまたは下向きの矢印をクリックして、新しいポリシーの優先順位を設定します。

    2 つ以上のポリシーに属するアカウントがある場合、[優先度] の設定により、どのポリシーが適用されるかが決まります。

11. [保存] をクリックします。

12. ポリシーをただちに適用するには、[ポリシーの配信] をクリックします。そうしない場合、ポリシーはデータベースキャッシュの有効期限が切れた後に適用されます。

URL フィルタの設定

URL フィルタに関連するいくつかの設定を変更して、実際の作業環境を反映させることができます。

- 7 つの論理グループに分けられた 60 を超える Web サイトカテゴリ
- URL フィルタルールによってブロックされている特定の Web サイトへのアクセスを許可する、除外の設定
- 「業務時間中」と「業務時間外」のスケジュールの設定

さらに、URL が不適切なカテゴリに分類されていると思われる場合は、URL の分類を見直すようにトレンドマイクロに依頼できます。不明な URL のカテゴリを検索することもできます。

URL カテゴリの見直しの依頼と URL 検索

IWSS には、URL フィルタの基準レベルを提供する、7 つの論理グループに分けられた初期設定のカテゴリが含まれています。たとえば、ユーモアやジョークに関連する Web サイトは「Computers/Bandwidth」グループの「Joke Programs」カテゴリに属しています。

初期設定の URL 分類に同意できない場合は、トレンドマイクロにカテゴリの見直しを提案できます。

URL フィルタポリシーを適用する前に、初期設定の分類が組織に対して適切かどうか確認することをお勧めします。たとえば、衣服の小売業者は、正当な市場分析および競合他社の調査を許可するために、「成人向け」グループの「下着 / 水着」カテゴリから水着の Web サイトを削除する必要があるかもしれません。

URL のカテゴリを知りたい場合には、[URL フィルタ設定] 画面の [URL カテゴリの見直し依頼と検索] タブで URL フィルタ設定を指定する際に検索できます。

未評価の URL および不明 URL

未評価の URL とは、認識されていながら、まだフィルタカテゴリに加えられていない Web サイトのことです。

不明 URL とは、次に該当する Web サイトのことです。

- トレンドマイクロが認識していない Web サイト
- Web レピュテーションデータベースに存在していない Web サイト
- デーモンが機能していないか、URL を評価するリモート評価サーバにアクセスできない Web サイト

不明 URL の評価は「0」となり、ブロックできません。

URL カテゴリの見直し依頼

URL カテゴリの見直しを依頼するには

1. メインメニューから [HTTP] → [URL フィルタ] → [設定] の順に選択します。
2. [URL カテゴリの見直し依頼と検索] タブをクリックします。
3. URL をクリックします。

   [Trend Micro Online URL Query - Feedback System] 画面が開きます。
4. 必要な情報をすべて入力し、[Submit feedback] をクリックします。

URL フィルタの除外設定

IWSS では、URL フィルタポリシーの除外設定および Web レピュテーションデータベースによる URL フィルタの除外設定を行うオプションが用意されています (112 ページの「Web レピュテーション除外の指定」を参照)。URL 除外設定により、ブロックするように設定された Web サイトへのアクセスが許可されます。URL フィルタによってブロックされている Web サイトをクライアントで表示する正当な必要性がある場合、そのサイトを URL フィルタの除外対象として入力します。URL 以外にも次の項目のいずれかを入力できます。

- URL 内に部分一致する特定の文字列
- ブロックするように設定されたサイトに含まれる特定のファイルへのアクセスを許可するための、完全一致する文字列

URL フィルタポリシーの除外設定リストは、
/etc/iscan/ URLFilteringExceptions.ini ファイルに保存されています。
URLFilteringExceptions.ini ファイルへのパスは、
/etc/iscan/ IWSSPIUrlFilter.dsc ファイルの [url-filtering] セクションにある
filtering_exception_list パラメータを使用して設定します。

URL フィルタの許可リストを設定するには

1. IWSS Web コンソールを開き、[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、[キーワード] フィールドに、Web アドレス、URL キーワード、または完全一致する文字列を入力します。次の 3 つのオプションのいずれかを選択することにより、入力した値が識別されます。
   - Web サイト
   - URL キーワード
   - 文字列

3. [追加] をクリックして、入力した値を [承認する URL リスト] に追加します。

   リストからエントリを削除するには、削除する項目を選択して [削除] をクリックします。または、[すべて削除] をクリックしてすべてのエントリを削除します。

   URL フィルタ除外設定のリストをファイルからインポートするには、[除外リストのインポート] フィールドにパスを入力するか [参照] をクリックして、ファイルの場所へ移動し、[インポート] をクリックします。

注意： URL フィルタの除外設定テキストファイルを次の形式で記述します。

1 行目 = URL Filtering Import File
2 行目 = [approved]
3 行目以降 :
* 情報 * の形式で記述された Web サイト、URL キーワード、および文字列
たとえば、次のように記述します。

```
URL Filtering Import File
[approved]
*www.trendmicro.com*
*www.antivirus.com*
```

IWSS でワイルドカードとみなされないようにキーワードに「*」と「?」文字を含めるには、変数 %2a または %2A を使用して「*」を表示し、変数 %3f または %3F を使用して「?」を表示します。たとえば、サイト www.example.com/*wildcard を文字どおりフィルタするには、フィルタルールを www.example.com/*wildcard. ではなく、www.example.com/%2awildcard と指定します。

---

4. [保存] をクリックします。

業務時間および業務時間外の設定

IWSS では、業務時間 1 と業務時間 2 の 2 セットの業務時間を指定できます。どちらの業務時間も 24 時間制で指定します。

URL フィルタのポリシーを作成する際に、業務時間 1 と業務時間 2 の両方、または「業務時間外」に対して、あるいは、業務時間 1、業務時間 2、および「業務時間外」すべてに対して有効に設定できます。業務時間 1 にポリシーを設定すると、実際には業務時間 2 にも有効となります。

IWSS ポリシーを使用すると、業務時間および業務時間外に URL カテゴリへのアクセスを許可またはブロックできます。IWSS では、初期設定で次の業務時間設定が使用されます。

- 曜日 : 月曜日～金曜日まで
- 時間 : 8:00 ～ 11:59 (業務時間 1) および 13:00 ～ 17:00 (業務時間 2)

業務時間として定義されていない時間帯はすべて「業務時間外」として扱われます。

注意 : 同じクラスタ内にあるすべての IWSS サーバは、同じ時間帯にあると想定しています。

組織で URL フィルタポリシーを適用する前に、業務時間と業務時間外の設定が使用する環境に対して適切かどうか確認することをお勧めします。

URL フィルタポリシーのスケジュールを設定するには

1. IWSS Web コンソールを開き、[HTTP] → [URL フィルタ] → [設定] → [業務時間] の順に選択します。
2. [業務時間の設定] に表示されるフィールドで、曜日と時間を選択します。

   [業務時間 1] および [業務時間 2] の両方、あるいはいずれかの箇所で、選択した URL カテゴリへのアクセスを制限する時間帯を指定します。
3. [保存] をクリックします。

業務時間なしまたはすべてを業務時間に指定するには

- 業務時間の設定を使用しない場合は、曜日のチェックボックスをすべてオフにします。すべての時間が業務時間外となります。
- すべての時間を業務時間にする場合は、曜日のチェックボックスをすべてオンにして、次のように指定します。
    - 業務時間 1 には、[開始] リストから [0:00] を選択し、[終了] リストから [11:59] を選択します。
    - 業務時間 2 には、[開始] リストから [12:00] を選択し、[終了] リストから [23:59] を選択します。

新しい IntelliTunnel ポリシーの作成

IntelliTunnel の詳細については、90 ページの「IntelliTunnel に関する注意」を参照してください。

新しい IntelliTunnel ポリシーを作成するには

1. メインメニューで [HTTP] → [IntelliTunnel] の順に選択します。
2. 画面の上部にある [IntelliTunnel を有効にする] チェックボックスをオンにします。
3. [IntelliTunnel] 画面で、[追加] リンクをクリックします。
4. [IntelliTunnel: ポリシーの追加] 画面の「1. アカウントの選択」で、ポリシー名を指定します。
5. IP 範囲と IP アドレスのいずれかまたは両方を指定して、[追加] をクリックします。

   IWSS では、インスタントメッセージおよび認証接続ルールを、指定された任意の IP 範囲および IP アドレスに適用します。LDAP を使用している場合、ユーザ名など、より詳細な情報が [追加] テーブルに表示されます。
6. [次へ] をクリックします。
7. [IntelliTunnel: ポリシーの追加] 画面の「2. IntelliTunnel ルールの指定」で、目的のオプションを選択します。

   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の詳細な説明については、IWSS のオンラインヘルプを参照してください。
8. [保存] をクリックします。

第 9 章

アクセス割り当てと URL アクセス設定

本章で説明する内容には、次の項目が含まれます。

- 156 ページの「アクセス割り当てポリシーの管理」
- 157 ページの「URL アクセス管理の設定」

アクセス割り当てポリシーの管理

アクセス割り当てポリシーの詳細については、92 ページの「アクセス割り当てポリシーに関する注意」を参照してください。

アクセス割り当てポリシーの範囲に含めるクライアント、帯域幅の割り当て、および割り当て期間の間隔を設定できます。

アクセス割り当てポリシーを追加するには

1. メインメニューから [HTTP] → [アクセス割り当てポリシー] の順に選択します。
2. [アクセス割り当てを有効にする] チェックボックスをオンにします。
3. ドロップダウンメニューから、[1 日]、[1 週]、または [1ヶ月] のいずれかのアクセス割り当て間隔を選択します。

   アクセス割り当て間隔の値は、すべての既存のポリシーを含め、すべてのアクセス割り当てポリシーにグローバルに適用されます。
4. [保存] をクリックします。
5. [追加] をクリックします。
6. [ポリシーを有効にする] チェックボックスをオンにして、アクセス割り当てを入力します。
7. ポリシーを適用するユーザを選択します。この画面のオプションは、使用しているユーザの識別方法に応じて異なります。[IP アドレス]、[ホスト名 (変更された HTTP ヘッダ)]、または [ユーザ / グループ名] のいずれかになります。これらの設定は、[HTTP] → [設定] → [ユーザの識別] 画面で行います。ユーザの識別方法の設定とポリシー適用範囲の定義の詳細については、100 ページの「ユーザ識別方法の設定」を参照してください。

   設定したユーザの識別方法に関係なく、ポリシーを適用するクライアントの IP アドレスを入力できます。
8. ポリシーに関する特別な情報がある場合は、必要に応じて備考を入力します。
9. [保存] をクリックします。

10. [アクセス割り当てポリシー] 画面に戻ったら、[ポリシーの配信] をクリックして、ただちにポリシーを適用します。すぐに適用しない場合、ポリシーはデータベースキャッシュの有効期限が切れた後に適用されます。

URL アクセス管理の設定

Trend Micro InterScan Web Security Suite (以下、IWSS) は、低リスクサイトの閲覧パフォーマンスを改善するために、オプションで「信頼する」URL を検索およびフィルタから除外できます。ユーザ設定のリストを使用して、または、「フィッシング」スキームまたは悪質な行為に関連付けられているサイトを編集したフィッシングパターンファイルに要求されたサイトが含まれていないかどうかを確認することにより、サイトへのアクセスをブロックすることもできます。

アクセス割り当てポリシーの詳細については、93 ページの「URL アクセス管理に関する注意」を参照してください。

信頼する URL の設定

IWSS では、一部の URL を信頼してそれらを検索とフィルタから除外するように設定できます。この設定をすると、未確認のコンテンツがネットワークに入り、セキュリティリスクにさらされることになるので、「信頼する」URL は慎重に考慮する必要があります。信頼する URL は検索されないので、閲覧パフォーマンスが改善します。信頼する URL にふさわしいのは、頻繁にアクセスされる Web サイトで、自分の会社のイントラネットサイトのように、管理できるコンテンツが含まれているものです。

HTTP スタンドアロンプロキシハンドラをインストールすると、信頼する URL はすべての IWSS 検索から除外されます。ICAP プロキシハンドラをインストールしている場合、URL フィルタ、Web メールアップロード検索、URL ブロックなどの REQMOD の動作で信頼する URL リストを無視することはできません。

信頼する URL 情報は、intscan.ini 設定ファイルの [URL-trusting], normalLists セクションにあります。

信頼する URL を設定する際、次のものを使用してサイトを指定できます。

- サブサイトを含む Web サイト
- 要求された URL 内の完全一致文字列

それ以外の場合には信頼する URL のリストの条件に一致するサイトが、通常どおり IWSS で検索またはフィルタされるように、これらのサイトに除外設定を適用できます。

ユーザインタフェースを通じて信頼する URL のリストと除外を設定できるだけでなく、ファイルからこれらをインポートすることもできます。Web サイト、URL キーワードまたは文字列のリストを含むファイルの一番上にコメントまたはタイトルを記述し、1 行ごとにルールを 1 つ記述します。コメントまたはタイトルは、IWSS では無視されます。次の例で示すように、[block] の下にブロックするグループサイトを、[allow] の下に除外するグループサイトを記述します。

```
URL Blocking Import File { このタイトルは無視されます }

[block]
www.blockedsite.com*
unwanted.com*
urlkeyword
banned.com/file
banned.com/downloads/

[allow]
www.blockedsite.com/file
www.unwanted.com/subsite/
www.trendmicro.com*
```

信頼する URL と除外設定を管理するには

1. メインメニューから [HTTP] → [URL アクセス設定] → [URL の信頼] の順に選択します。
2. [URL の信頼] 画面で、[URL の信頼を有効にする] チェックボックスをオンにします。
3. 信頼する URL を指定する方法を選択します。
   - 前方一致 (すべてのサブサイトを含む)
   - 完全一致 (URL に文字列が含まれること)

4. [キーワード] に URL 文字列を入力して [信頼する] をクリックし、[信頼リスト] セクションの下に表示されている信頼する URL リストに追加します。信頼する URL を除外するには、[信頼しない] をクリックして除外リストに追加します。
5. 信頼リストまたは除外リストから URL を削除するには、削除する項目を選択して [削除] をクリックします。[すべて削除] をクリックすると、すべて削除されます。
6. [保存] をクリックします。

信頼する URL リストとその除外設定をインポートするには

1. メインメニューから [HTTP] → [URL アクセス設定] → [URL の信頼] の順に選択します。
2. 信頼する URL のリストとその除外設定を含むファイルの名前を参照するか、または [信頼リスト / 除外リストのインポート] フィールドに入力します。
3. [インポート] をクリックします。インタフェース上の該当するフィールドに、ファイルからインポートされる信頼する URL とその除外設定が表示されます。
4. [保存] をクリックします。

URL のブロック

IWSS は、ICAP と HTTP プロキシモードの両方で、Web サイトと URL 文字列をブロックできます。

注意： ICAP プロキシハンドラをインストールしている場合、この機能を作動させるためには、事前キャッシュ (precache) 要求モードでファイルを検索するように ICAP クライアントを設定してください。スタンドアロンプロキシでは、追加の設定は必要ありません。

URL のブロックを設定する際、次のキーワードを使用してサイトを指定できます。

- 前方一致

- 部分一致
- 完全一致

IWSS で通常どおり要求が受け入れられるように、ブロックされた URL のリストに除外設定を適用できます。この機能を使用すると、任意のサイトをブロックしながら、そのサイトのサブサイトまたはファイルへのアクセスを許可できます。除外リストを含む URL ブロックリストは、**/< インストールフォルダ >/data/URLB.ini** ファイルに保持されます。URLB.ini ファイルのパスは、intscan.ini ファイルの [URL-blocking] セクションにある「normalLists」パラメータを使用して設定されます。

また、フィッシングパターンファイルを使用したパターンマッチングに基づいて URL をブロックすることもできます。フィッシングパターンファイルは、フィッシングまたは関連スキームに関連付けられた Web サイトのパターンが格納されているデータベースです。

Web コンソールから URL を追加する以外に、テキストファイルから URL ブロックリストをインポートできます。

ローカルリストの使用

使用している環境用に保持しているブロックされたサイトと除外設定のリストに基づいて、URL へのアクセスをブロックするように IWSS を設定できます。

URL を [ブロックリスト] と [除外リスト] の両方に追加する場合、まず一方のリストにすべて追加して設定を保存してから、他方のリストへの追加操作を実行する方法をお勧めします。この方法により、同一の URL が両方のリストに存在するようにできます。URL を [ブロックリスト] に追加するか、または [除外リスト] に追加しようとする時、その URL がすでに他のリストに存在している場合、IWSS では追加操作を実行せず、他のリストに存在している旨の警告メッセージが表示されます。

ブロックする URL を設定するには

1. [HTTP] → [URL アクセス設定] → [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. [ローカルリストによる規制] タブで、[キーワード] に前方一致、部分一致、完全一致文字列のいずれかを入力します。

   任意の Web サイトでフォルダまたはディレクトリを識別するには、最後の文字の後にスラッシュ (/) を使用します。たとえば、www.blockedsite.com をブロックしても、その charity ディレクトリへのアクセスを許可する場合は、次の手順に従ってください。

   a. [キーワード] フィールドに「www.blockedsite.com」と入力し、[ブロック] をクリックします。

   b. [キーワード] フィールドに「www.blockedsite.com/charity/」と入力し、[ブロックしない] をクリックします。スラッシュなしで「charity」と記述すると、IWSS は www.blockedsite.com/charity をファイルとみなします。

4. リストからエントリを削除するには、削除する項目を選択して [削除] をクリックします。または [すべて削除] をクリックしてすべてのエントリを削除します。

5. [保存] をクリックします。

ブロックする URL リストのインポート

IWSS は、ブロックする URL のリストをファイルからインポートできます。Web サイト、URL キーワードまたは文字列のリストを含むファイルの 1 行目にコメントまたはタイトルを記述し、1 行ごとにルールを 1 つ記述します。例で示すように、[block] の下にブロックするグループサイトを、[allow] の下に除外するグループを記述します。たとえば、次のように記述します。

```
URL Blocking Import File { このタイトルは無視されます }

[block]
www.blockedsite.com*
unwanted.com*
urlkeyword
banned.com/file
banned.com/downloads/

[allow]
www.blockedsite.com/file
www.unwanted.com/subsite/
www.trendmicro.com*
```

IWSS でワイルドカードとみなされないように、URL ブロックの文字列に「*」と「?」文字を含めるには、変数 %2a または %2A を使用して「*」を表示し、変数 %3f または %3F を使用して「?」を表示します。たとえば、www.example.com/*wildcard を文字どおり一致させるには、www.example.com/*wildcard ではなく、www.example.com/%2awildcard と指定します。

ファイルのインポートが成功しない場合、カスタマーセンターに連絡する前に、URL ブロックインポートファイル用に指定された形式に従っていることを確認します。次のことを確認します。

- [block] の下にブロックするエントリ、[allow] の下に除外するエントリを記述していること
- 本書またはオンラインヘルプで説明するとおりに、ワイルドカードを含むエントリの形式を設定していること

ブロックする URL のリストをインポートするには

1. 前述のように、ブロックする URL とすべての除外設定を含むテキストファイルを作成します。
2. メインメニューから [HTTP] → [URL アクセス設定] → [URL ブロック] の順に選択します。
3. [参照] をクリックして、インポートするファイルの場所を [ブロックリスト / 除外リストのインポート] フィールドに指定し、[インポート] をクリックします。
4. [保存] をクリックします。

フィッシングパターンファイルの使用

「フィッシング」とは、急速に広まっているコンピュータ詐欺の一種です。たとえば、ユーザがアカウントを持っている会社からの連絡を装ったメールで偽の Web サイトにアクセスを促し、クレジットカード番号などの個人情報を入力するように求めます。送られてくるメールは本物のように見えるため、騙されて詐欺の被害に遭うユーザもいます。

フィッシング対策は、トレンドマイクロの次の技術に基づいています。

- 特定の URL へのアウトバウンドアクセスをブロックする IWSS の機能
- 顧客からの情報に基づいて収集、分析された、既知の有害な URL 情報を含むトレンドマイクロのフィッシングパターンファイル

フィッシング対策により、プライベートな機密情報がクライアントから外部へ送出される被害を最小限に抑えることができます。また、既知のフィッシング URL へのアクセスを防ぎます。

故意にユーザ情報を収集しようとしている URL は、フィッシングパターンファイルに追加されます。フィッシングパターンファイルは、IWSS でブロックされる URL のリストです。IWSS は、トレンドマイクロのアップデートサーバを介してアップデートされたフィッシングパターンファイルを定期的に取得します。

IWSS を使用して、疑わしいフィッシング URL を診断するために TrendLabs (トレンドラボ) に送信できます。トレンドラボでは、送信された URL が悪質かどうかを判定するために Web サイトを診断します。次に列挙するカテゴリのいずれかの条件を満たす場合、URL は悪質であると見なされます。

- **フィッシング** － 機密情報を不正に収集することです。正当な会社からの通知に見せかけたメールメッセージ、または Web サイトが提供され、個人情報の盗用目的で情報が要求されます。
- **スパイウェア** － ひそかに機密情報を収集する、プログラムです。スパイウェアは、ユーザのコンピュータ利用習慣や個人情報を監視し、この情報をユーザの承諾なく第三者に送信します。
- **ウイルス流布** － 既知の不正コードの動作によって引き起こされるアウトバウンドの HTTP 要求です。不正コードが情報を送信したり、特定の URL から不正なコンポーネントをダウンロードします。これらは、スパイウェアまたはトロイの木馬に感染した現象です。
- **不正サイト** － 不正な目的のために存在する Web サイトのことです。

フィッシングパターンファイルを使用した URL のブロック

フィッシング URL をブロックするには

1. IWSS Web コンソールを開き、[HTTP] → [URL アクセス設定] → [URL ブロック] → [パターンファイルによる規制 (フィッシング対策)] の順に選択します。
2. [URL ブロックを有効にする] チェックボックスがオンになっていることを確認します。
3. ブロックするフィッシング URL カテゴリを有効にします。
4. [保存] をクリックします。

疑わしいフィッシング URL をトレンドラボに報告するには

疑わしいフィッシング URL をトレンドマイクロに報告するには、[URL ブロック] 画面の送信フォームを使用します。送信された URL は調査され、悪質な動作に関連している場合、その URL はフィッシングパターンファイルの今後のリリースに追加されます。

1. IWSS Web コンソールを開き、[HTTP] → [URL アクセス設定] → [URL ブロック] → [パターンファイルによる規制 (フィッシング対策)] の順に選択します。
2. トレンドマイクロに調査を依頼したい URL を [URL] フィールドに入力します。
3. URL が関連していると思われるカテゴリ (「フィッシング」、「スパイウェア」、「ウイルス流布」、「不正サイト」、「その他」のいずれか) を [カテゴリ] のドロップダウンメニューから選択します。
4. 必要に応じて、連絡可能なメールアドレスを入力します。
5. [説明] フィールドに任意の報告を入力します。
6. [送信] をクリックします。

第 10 章

FTP 検索

本章で説明する内容には、次の項目が含まれます。

- 168 ページの「FTP 設定」
- 168 ページの「FTP 検索オプション」
- 170 ページの「FTP 検索の設定」
- 172 ページの「ウイルスに対する検索処理の設定」
- 172 ページの「FTP アクセス管理設定」

FTP 設定

FTP を設定するには、プロキシ設定とデータ接続を指定する必要があります。

FTP の設定を行うには

1. メインメニューから [FTP] → [設定] → [一般] の順に選択します。
2. [プロキシ設定] で、構成に基づいて適切な FTP 設定を選択します。ネイティブ Trend Micro InterScan Web Security Suite (以下、IWSS) プロキシで FTP サイトに接続する場合は [スタンドアロンモードを使用] を選択します。FTP サービスと既存の FTP プロキシを組み合わせて使用する場合は、[FTP プロキシを使用] を選択し、[プロキシサーバ] にホスト名を入力して、[ポート] を指定します。
3. 使用するデータ接続の種類を、[パッシブモード] または [アクティブモード] のいずれかから選択します。
4. [保存] をクリックします。

FTP 検索オプション

FTP ウイルス検索設定は HTTP 検索設定と似ていますが、次の 2 つの違いがあります。

- FTP 検索では、ユーザまたはグループベースのポリシーはサポートされません。そのため、1 つの設定が IWSS 経由で FTP サイトにアクセスするすべてのクライアントに適用されます。
- 検索するトラフィックの方向を、アップロード、ダウンロード、またはその両方に設定できます。

FTP トラフィックおよび FTP 検索の有効化

クライアントが IWSS 経由で FTP サイトにアクセスするには、FTP トラフィックを有効にする必要があります。

FTP トラフィックをオンにするには

1. メインメニューで [概要] をクリックします。
2. 画面の上部で [オン] または [オフ] をクリックし、FTP トラフィックフローを開始または停止します。
   [オフ] にすると、IWSS サーバ上の FTP サービスがシャットダウンされるため、クライアントは IWSS の FTP プロキシ経由で FTP サーバに接続できなくなります。初期設定は [オン] です。
   FTP トラフィックが有効になっても、FTP 検索をオンにしないと、ウイルス検索されません。

FTP 検索を有効にするには

1. IWSS Web コンソールを開き、[FTP] → [検索ルール] の順に選択します。
2. [FTP 検索を有効にする] チェックボックスをオンにします。
3. [保存] をクリックします。

FTP 検索設定の優先順位

ウイルス検索ルールの設定が互いに競合する場合、プログラムでは次の優先順位に従って検索が実行されます。

1. ブロックするファイルタイプ
2. 検索するファイルタイプ (ブロックされなかった場合)

FTP 検索の設定

FTP 検索の設定を行うには

1. メインメニューから [FTP] → [検索ルール] の順に選択します。
2. [FTP 検索を有効にする] チェックボックスをオンにします。
3. [アップロード]、[ダウンロード]、またはその両方から、検索する FTP 転送の種類を選択します。
4. [ブロックするファイルタイプ] で、ブロックするファイルタイプを選択します。[その他] フィールドに、ブロックするその他のファイルタイプを入力します。複数のエントリはスペースで区切ります。ブロックできるその他のファイルタイプのリストは、付録 A「ファイルタイプと MIME コンテントタイプの対応」を参照してください。
5. 検索するファイルを選択します。
   - 拡張子に関係なく、すべてのファイルを検索するには、[検索可能なすべてのファイル] を選択します。IWSS は、圧縮したファイルを開き、その中のすべてのファイルを検索します。すべてのファイルを検索するのは最も安全な設定です。
   - 実際のファイルタイプによる識別を使用するには、[トレンドマイクロの推奨設定] を選択します。トレンドマイクロの推奨設定では、実際のファイルタイプの検索と正確な拡張子名の検索を組み合わせて使用します。実際のファイルタイプの検索では、ファイルの拡張子が変更されていてもファイルタイプが認識されます。トレンドマイクロの推奨設定では、使用する検索方法が自動的に決定されます。
   - 拡張子に基づいてファイルタイプを検索するには、[指定する拡張子] を選択します。これには、ウイルスが潜むことがわかっているファイルタイプのリストが含まれます。IWSS は、[初期設定の拡張子] リストおよび [その他の拡張子] テキストボックスで明示的に指定されているファイルタイプのみを検索します。初期設定の拡張子のリストは、ウイルスパターンファイルから定期的にアップデートされます。

このオプションは、たとえば IWSS がチェックするファイルの総数を減らして、全体の検索時間を短縮する場合などに使用します。

注意： 指定できるファイルの数やタイプに制限はありません。拡張子の前にアスタリスク (*) を付けないでください。複数のエントリはセミコロンで区切ってください。

6. [圧縮ファイルの処理] で、次の 2 つのオプションのいずれかを選択します。
   - すべての圧縮ファイルをブロック
   - 次の場合にブロック

「次の場合にブロック」を有効にする場合は、次のパラメータの値を入力します。

- 解凍後のファイルが次の数を超える場合 (初期設定は 50000)
- 解凍後のファイルが次のサイズを超える場合 (初期設定は 200MB)
- 圧縮レイヤが次の数を超える場合 (0 ～ 20、初期設定は 10)
- 圧縮率が 99% を超える場合 (圧縮率が 99% 未満のファイルは IWSS によって自動的に許可されます)

7. [サイズの大きいファイルの処理] で、[検索するファイルサイズの上限を設定する] チェックボックスをオンにし、ファイルサイズを入力します。

8. サイズの大きいファイルをダウンロード中にタイムアウトする問題を避けるには、[次のサイズを超えるファイルに対して遅延検索を有効にする] チェックボックスをオンにして、遅延検索が発生しない最大ファイルサイズを入力します。また、ドロップダウンリストから、検索されないクライアントに送信されるデータの割合を選択します。

警告： ファイルの部分配信により、ウイルス感染の可能性も生じます。そのため、パフォーマンスとセキュリティのバランスは管理者の判断にかかっています。このオプションは、現在タイムアウトの問題が発生している場合にのみ使用してください。

9. 隔離ディレクトリに送信されるファイルを暗号化して、不注意で開かれたり実行されたりするのを防ぐには、[隔離ファイルを暗号化する] を選択します。

10. [保存] をクリックして、[スパイウェア検索ルール] タブに切り替えます。
11. 検索するその他のリスクの種類を選択して、[保存] をクリックします。
12. [処理] タブに切り替え、検索結果に対して IWSS で実行する処理を選択します。
13. [保存] をクリックします。

ウイルスに対する検索処理の設定

ファイルに対して FTP 検索で実行する処理を指定できます。

- ファイルを駆除せずにクライアントに送信するには、[放置] を選択します。感染ファイルがネットワークに侵入する可能性があるため、この設定はお勧めしません。
- ファイルを駆除せずに隔離ディレクトリに隔離するには、[隔離] を選択します。要求元クライアントはファイルを受信しません。
- ファイルを IWSS で削除するには、[削除] を選択します。要求元クライアントはファイルを受信しません。
- ファイルを自動的に駆除して処理するには、[駆除] を選択します。ファイルが駆除可能な場合、要求元クライアントは駆除されたファイルを受信します。

FTP アクセス管理設定

IWSS には、セキュリティおよびパフォーマンスをさらに調整するために、いくつかのアクセス管理設定が用意されています。

- クライアントの IP アドレスに基づいて FTP アクセスを有効にできます。
- コンテンツの厳しく管理している信頼できるサーバに頻繁にアクセスする場合、そのサーバを許可リストに追加できます。FTP アクセスが検索されなくなるため、パフォーマンスが向上します。
- 指定した宛先ポートへのアクセスを拒否することによって、IWSS FTP サーバの接続を制限できます。

クライアント IP による設定

初期設定では、FTP トラフィックが有効な場合、ネットワーク上のすべてのクライアントが IWSS 経由で FTP サイトにアクセスできます (169 ページの「FTP トラフィックおよび FTP 検索の有効化」を参照)

クライアントの IP アドレスに基づいて FTP アクセスを制限するには

1. メインメニューから [FTP] → [設定] → [アクセス管理] の順に選択します。
2. [クライアント IP] タブに切り替えます。
3. [クライアント IP に基づく FTP アクセス管理を有効にする] チェックボックスをオンにします。
4. IWSS 経由の FTP アクセスを許可するクライアントの IP アドレスを入力します。入力できるエントリは次のとおりです。
   - **IP アドレス** － 単一の IP アドレス。たとえば、123.123.123.12 のようになります。
   - **IP 範囲** － 連続する IP アドレスの範囲に含まれるクライアント。たとえば、123.123.123.12 ～ 123.123.123.15 のようになります。
   - **IP マスク** － 指定したサブネット内の単一のクライアント。たとえば、IP に「192.168.1.0」、マスクに「255.255.255.0」と入力すると、192.168.1.x サブネット内のすべてのコンピュータが識別されます。または、マスクをビット数 (0 ～ 32) で指定することもできます。
5. [追加] をクリックして、FTP サイトへのアクセスを許可する他のクライアントの入力を続けます。
6. [保存] をクリックします。

許可されたサーバ IP のリスト

コンテンツの直接管理が可能な信頼する FTP サイトの場合、サイトへのアクセス時にパフォーマンスの問題が発生する可能性を少なくするために、FTP サイトの IP アドレスを許可リストに追加して、これらのサイトを検索から除外できます。

注意： IP の許可リストによる検索の除外は、ファイルのダウンロードにのみ適用されます。アップロードされるファイルは検索されます。

信頼するサーバを許可リストに追加するには

1. メインメニューから [FTP] → [設定] → [アクセス管理] の順に選択します。
2. [サーバ IP の除外リスト] タブに切り替えます。
3. IWSS の FTP ウイルス検索から除外する FTP サイトの IP アドレスを入力します。
4. [追加] をクリックして、除外する他の FTP サイトの入力を続けます。
5. [保存] をクリックします。

宛先ポートによる設定

初期設定では、クライアントは IWSS FTP サーバのどのポートにもアクセスできます。セキュリティを強化するために、ポートへのアクセスを選択的に許可または拒否できます。

クライアントが接続できる IWSS FTP ポートを設定するには

1. メインメニューから [FTP] → [設定] → [アクセス管理] の順に選択します。
2. [宛先ポート] タブに切り替えます。
3. [拒否] または [許可] のいずれかから、ポートに適用する処理を選択します。
4. 処理を適用する [ポート] または [ポート範囲] を入力し、[追加] をクリックします。
5. 許可または拒否する他のポートの追加を続けます。
6. [保存] をクリックします。

注意： [宛先ポート] タブのポートは、評価順 (降順) で一覧表示されます。宛先ポートによるアクセス管理は、FTP コマンド接続時にのみ適用されます。FTP データ接続は影響を受けません。一般的な設定は、1.「すべてを拒否」および 2.「21 を許可」です。これにより、ポート 21 へのアクセスのみが許可されます。

第 11 章

プロキシ検索設定

本章で説明する内容には、次の項目が含まれます。

- 178 ページの「プロキシ設定および関連するその他の設定」
- 183 ページの「ネットワーク設定および負荷の処理」
- 183 ページの「ゲストアカウントの有効化 (LDAP のみ)」
- 184 ページの「ICAP プロキシの設定」

プロキシ設定および関連するその他の設定

Trend Micro InterScan Web Security Suite (以下、IWSS) がネットワーク上でどのように配置されているかによって、検索モードを選択します。

- **HTTP プロキシ** — クライアントが不正な HTTP による脅威をサーバから受信しないように防ぐ設定です。最もよく使われる設定で、代表的な使用例はネットワークに接続する Web ユーザが不正なインターネットダウンロードを受信しないよう防ぐ用法です。IWSS と保護対象のクライアントは通常、同じ LAN 内にあります。
- **ICAP モード** — ICAP クライアントがネットワーク上にあり、検索のためトラフィックを IWSS に通過させる場合、このトポロジを選択します。IWSS は ICAP サーバとしての役割を果たします (184 ページの「ICAP プロキシの設定」を参照)。

プロキシ設定

注意 : プロキシ設定および計画の詳細については、「IWSS インストールガイド」を参照してください。

プロキシ設定には、次のような種類があります。

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

上位プロキシなし (スタンドアロンモード)

スタンドアロンの設置を設定するには

1. 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. [プロキシ転送] チェックボックスをオンにして、[上位プロキシを有効にする] および [透過を有効にする] チェックボックスをオフにします。

3. [保存] をクリックします。

上位プロキシあり (依存モード)

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

スタンドアロンモードと同様、依存モードのプロキシ設定でも、クライアントユーザがインターネット接続設定で IWSS サーバをプロキシサーバに設定する必要があります。上位プロキシを使用する利点は、上位プロキシサーバにコンテンツがキャッシュされるためパフォーマンスが向上することです。IWSS ではコンテンツのキャッシュを一切行わないため、クライアントの要求ごとにインターネットサーバに問い合わせてコンテンツを取得する必要があります。上位プロキシを使用すると、プロキシサーバにキャッシュされた画面が素早く表示されるようになります。

注意 : IWSS が指定されたプロキシサーバを使用して、上位プロキシモードで実行するように設定する場合、アップデート用のプロキシ設定も指定されたプロキシサーバが WAN アクセスできるように設定することをお勧めします (58 ページの「プロキシ設定 (アップデート用)」を参照)。特定の種類のアップデートイベントは、アップデートプロキシ設定を利用して重要な情報を取得します。

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

上位プロキシと動作するよう IWSS を設定するには

1. 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. [プロキシ転送] を選択します。

3. [上位プロキシを有効にする] チェックボックスをオンにして、[プロキシサーバ] と [ポート] に上位プロキシの IP アドレス / ホスト名およびポート番号を入力します。
4. [保存] をクリックします。

透過プロキシ

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

通常の透過を設定するには

1. 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. [プロキシ転送] を選択します。
3. [透過を有効にする] を選択します。
4. [クライアント要求] セクションで、レイヤ 4 スイッチが使用するように設定されているポートと同じポートに [待機ポート番号] を変更します。
5. [保存] をクリックします。

リバースプロキシ

IWSS をリバースプロキシとして設定するには

1. 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. [リバースプロキシ] チェックボックスをオンにし、リバースプロキシが保護する [保護対象サーバ] の IP アドレスまたはホスト名を入力します。
3. [ポート] に入力します (初期設定 = 80)。
4. HTTPS アクセスを有効にするには、[SSL 接続を有効にする] チェックボックスをオンにして [ポート番号] を入力します。

5. [保存] をクリックします。

注意 : 社内 Web サーバとの通信を SSL 経由で行っている場合は、HTTPS ポートを必ず設定してください。

リバースプロキシ設定を完成するには、リバースプロキシが保護する Web サーバのホスト名として IWSS サーバの IP アドレスを DNS に登録してください。このようにすることで、クライアントから保護する間は、IWSS サーバが Web サーバとして表示されます。

プロキシに関する設定

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

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

HTTP 待機ポート

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

待機ポート番号を設定するには

1. IWSS Web コンソールを開き、[HTTP] → [設定] → [プロキシ検索] の順に選択します。
2. [HTTP 待機ポート番号] テキストボックスに、ポート番号を入力します (初期設定値は、ICAP が 1344、HTTP プロキシが 8080)。
3. [保存] をクリックします。

注意： IWSS では、HTTPS 接続は HTTP 接続とは異なる形で処理されます。データが暗号化されているため、HTTPS 経由でダウンロードしたコンテンツは IWSS では検索できません。IWSS では最初の CONNECT 要求を検証し、対象となる URL がブロックリストにある、またはフィッシングパターンファイルに含まれている、または使用ポート番号が HttpsConnectACL.ini ファイルで定義されていない場合など、設定したパラメータと一致しない場合には拒否します。

FTP over HTTP の匿名ログオンに使用するメールアドレス

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

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

1. 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. [FTP over HTTP の匿名ログインで使用するメールアドレス] を入力します。
3. [保存] をクリックします。

ハイブリッド検索

ハイブリッド検索では、それぞれ 500 のスレッドを持つプロセスを 4 つ確立します。ハイブリッド検索は、マルチプロセスアーキテクチャとマルチスレッドアーキテクチャを組み合わせたものです。マルチスレッドアーキテクチャによってより多くの接続を確立でき、マルチプロセスアーキテクチャではデッドプロセスが原因ですべての接続が切断するというリスクが軽減されます。

ハイブリッド検索は、複数の同種のプロセスが同じセットの待機ソケットへのアクセスを共有し、各プロセスが TPC を使用して複数のセッションを処理する、プロキシフレームワークを提供します。

注意： 4 つのプロセスのうち 1 つが停止すると、HTTP 接続が切断する可能性があります。ただし、プロセスが停止しても、切断するのは全接続の 25% のみで、HTTP トラフィックとしては低いです。

同時接続数

IWSS が受け付ける同時接続の最大数は 4,000 です。この数を超えると、IWSS は HTTP 要求を拒否します。同時接続数が 1,200 の場合、平均的ユーザがインターネットの Web ページの閲覧時に、約 2 秒間の待ち時間があります。同時接続数が 1,200 ～ 4,000 の場合、待ち時間は Web サイトの複雑さに応じて増加します。[概要] 画面で表示する同時接続数を監視することで、システムの接続負荷によるユーザの閲覧への影響を監視できます。

ネットワーク設定および負荷の処理

同時接続数が 1,200 の場合、各 IWSS サーバでは、平均 3,000 ユーザのコミュニティのトラフィックを処理できます。この数は、どの時点においても、そのユーザの 20% がインターネット要求を行っていると想定しています。ユーザの数が多いコミュニティ、またはアクセス数が多いユーザコミュニティをサポートするには、サーバファームで連携する追加の IWSS サーバを設定する必要があります。

ゲストアカウントの有効化 (LDAP のみ)

ユーザ / グループ名による識別方法を使用する場合、ウイルス検索、Java アプレット /ActiveX 対策、URL フィルタ、およびアクセス割り当てのポリシーで、一時的にネットワークへアクセスするユーザ向けのポリシー設定がサポートされます。これらのゲストポリシーは、ゲスト用ポートを経由して IWSS に接続しているクライアントに適用されます。ゲストアカウントは、インストール後の初期設定で無効になっています。ゲストのインターネットアクセスを許可する場合はこのアカウントを有効にします。

ゲストアカウントを有効にしてゲスト用ポートを設定するには

1. メインメニューで [HTTP] → [設定] → [プロキシ検索] の順に選択します。
2. [ゲストアカウントを有効にする] チェックボックスをオンにします。
3. 初期設定の [ゲスト用ポート番号] は 8081 になっていますが、このポートが使用中でなければ変更する必要はありません。
4. [保存] をクリックします。

ICAP プロキシの設定

ICAP プロキシの設定を行うには

1. [HTTP] → [設定] → [プロキシ検索] の順で選択した画面で、[ICAP] を選択します。
2. ["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] のいずれかを選択します。

第 12 章

管理タスク

本章で説明する内容には、次の項目が含まれます。

- 186 ページの「隔離ディレクトリの設定」
- 186 ページの「データベース接続の確認」
- 188 ページの「Web コンソールパスワードを変更する」
- 189 ページの「ブラウザコンソール通信の暗号化 (HTTPS)」
- 192 ページの「IWSS およびオプション機能のアクティベーション」
- 193 ページの「ログインアカウントの管理」
- 194 ページの「IWSS サーバファームの設定」
- 195 ページの「Trend Micro Control Manager エージェントの登録」

隔離ディレクトリの設定

インストール時に、Trend Micro InterScan Web Security Suite (以下、IWSS) は隔離ディレクトリを作成してセキュリティイベントに関するファイルをコピーします。初期設定の保存先は /etc/iscan/quarantine です。

隔離ディレクトリを変更するには

1. メインメニューから [管理] → [IWSS 設定] → [一般] の順に選択します。
2. [隔離先のディレクトリ] に隔離フォルダの保存先を入力して [保存] をクリックします。

注意： 指定したフォルダは IWSS サーバ上に存在する必要があります。リモートサーバに格納する場合、隔離フォルダを設定する前にネットワークドライブを割り当てておく必要があります。UNC パスはサポートされません。

データベース接続の確認

[管理] → [IWSS 設定] → [データベース] の [データベース接続設定] セクションで、データベースを適切に設定していることを確認します。1 つのデータベースを複数の IWSS サーバ設定に対してセットアップする場合は、すべての IWSS サーバに対して同じデータベースを指定します。テーブル定義やストアドプロシージャなど、IWSS で使用されるスキームはインストール時に初期化されます。

データベース接続を設定するには

1. IWSS 管理コンソールを開いて、[管理] → [IWSS 設定] → [データベース] の順に選択します。

2. [データベース設定] に次のパラメータの値を入力します。
   - ODBC データソース名
   - ユーザ名
   - パスワード
3. [保存] をクリックします。

ポリシー設定がデータベースに保存され、IWSS がその設定をメモリキャッシュにコピーします。IWSS は、そのキャッシュ生存期限 (TTL) に従って設定をデータベースからメモリにリロードします。

分単位でキャッシュ生存期限を設定するには

1. IWSS 管理コンソールを開いて、[管理] → [IWSS 設定] → [データベース] の順に選択します。
2. [ポリシー配信設定 (分)] で、次のパラメータの値を入力します。
   - ウイルス検索ポリシー
   - アプレット /ActiveX 対策ポリシー
   - IntelliTunnel ポリシー
   - URL フィルタポリシー
   - アクセス割り当てポリシー
3. [保存] をクリックします。

Web コンソールパスワードを変更する

Web コンソールパスワードは、IWSS サーバを不正な変更から守るための基本的な手段です。環境のセキュリティをより高めるには、コンソールパスワードを定期的に変更し、推測が困難なパスワードを使用するようにしてください。

管理者レベルのユーザのみがパスワードを変更できます。

安全なパスワードの作成には、次のヒントを参考にしてください。

- パスワードに文字列と数字の両方を含めます。
- どんな言語であっても、辞書に掲載された単語は避けます。
- 意図的に単語のスペルを間違えます。
- 成句を使用したり、単語を組み合わせます。
- 大文字と小文字を混在させます。

コンソールパスワードを変更するには

1. admin ユーザとして IWSS コンソールにログインします。
2. IWSS コンソールを開いて、メインメニューで [管理] → [ログインアカウント] の順に選択します。
3. リスト内のアカウント名をクリックします。
4. [パスワード] に新しいパスワードを入力してから、[パスワードの確認入力] に新しいパスワードをもう一度入力して確認します。
5. 説明を入力します。
6. [保存] をクリックします。

ブラウザコンソール通信の暗号化 (HTTPS)

設定データが管理コンソールからサーバへ送信される際にインターセプトされないように、IWSS では保護された HTTPS プロトコルを使用することができます。Tomcat は JKS 形式のキーストアでのみ動作します。このキーストアは、Java の標準形式「Java KeyStore」のことで、keytool コマンドラインユーティリティによって作成された形式です。実行可能な keytool は次のディレクトリに用意されています。

[Install_directory]/IWSS/AdminUI/jre/bin (**初期設定のインストールディレクトリは** /opt/trend/)

1 つの自己署名証明書を含む新しいキーストアを作成するには

1. ターミナルコマンドラインから以下を実行します。

   ```
   ./keytool  -genkey -alias tomcat -keyalg RSA -keystore
   ./mykeystore
   ```

2. 画面上の手順に従います。パスワードの入力が求められたら一意のパスワードを指定します。

   mykeystore ファイルが現在のプログラムディレクトリに生成されます。

3. mykeystore ファイルを Tomcat のベースディレクトリにコピーし、ファイル名を keystore.tmp に変更します。

   cp /etc/iscan/AdminUI/jre/bin/mykeystore to
   /etc/iscan/AdminUI/tomcat/keystore.tmp

4. [管理] 画面で、mykeystore ファイルを作成するために使用される SSL パスワードを入力します。

5. SSL 接続で使用するポート番号を入力し、この情報を保存します。

6. IWSS Web コンソールによって、ユーザが適切なポート番号にリダイレクトされ、Web コンソールにログイン画面が表示されます。

   Web コンソールがユーザを適切なポート番号にリダイレクトしない場合は、次の手順を実行します。

7. URL https://<iwss server>:port にアクセスし、適切なポートを指定します。

HTTPS 経由での IWSS コンソールへのアクセス

Web ベースのコンソールからサーバに渡す設定データを暗号化するには、URL を変更して HTTPS プロトコルを使用し、ポート 1812 の代わりにポート 8443 を指定する必要があります。次の形式で暗号化通信 (HTTPS) 用の URL を入力します。

```
https://{SERVER-IP}:8443/index.jsp
https://123.123.123.12:8443/index.jsp
```

ここで SERVER-IP はサーバの IP アドレスです。比較できるように、非暗号化通信 (HTTP) の URL を次に示します。

```
http://{SERVER-IP}:1812/index.jsp
http://123.123.123.12:1812/index.jsp
```

非 HTTPS アクセスの無効化

HTTPS を有効にしてブラウザコンソール通信を暗号化すると、非 HTTPS アクセスを無効にして設定データのインターセプトを阻止できます。

非 HTTPS アクセスを無効にするには

1. Tomcat の HTTP 設定ファイル /etc/iscan/AdminUI/tomcat/conf/server.xml を編集します。
2. 次のノードを削除します。

```
<Connector
className="org.apache.coyote.tomcat4.CoyoteConnecto"

port="1812"
minProcessors="5"
maxProcessors="75"
enableLookups="true"
redirectPort="8443"
acceptCount="100"
debug="0"
connectionTimeout="2"000"
useURIValidationHack="false" disableUploadTimeout="true" />
```

3. IWSS サーバの /etc/rcX.d (X = インストールされたホストの実行レベル番号) に移動し、S99IScanHttpd を手動で再起動します。

```
./S99IScanHttpd stop
./S99IScanHttpd start
```

これらを変更すると、IWSS Web コンソールは以下を経由する場合のみアクセス可能になります。

```
https://<IWSS_server_IP>:8443/index.jsp
```

コンソールの待機ポート変更後の設定

管理コンソールの待機ポートが変更され、HTTP アクセスが無効になった場合、検索進行ステータス画面の使用を続行するには、intscan.ini ファイル内の 2 つの設定パラメータを変更する必要があります。

新しいポートおよびプロトコルまたはそのいずれかに対応するために、intscan.ini ファイルの [HTTP] セクションで、次の初期設定パラメータを変更します。

```
[http]
iscan_web_server=1812
iscan_web_protocol=http
```

たとえば、管理コンソールへの HTTPS アクセスを有効にした後で HTTP を無効にした場合、設定パラメータを次のように変更します。

```
[http]
iscan_web_server=8443
iscan_web_protocol=https
```

IWSS およびオプション機能のアクティベーション

IWSS のアクティベーションは、インストール時、またはインストール後に IWSS コンソールを使用して実行できます。ただし、オプションの URL フィルタおよびアプレット/ActiveX 対策のアクティベーションは、IWSS コンソールを使用して実行します。IWSS およびオプション機能のアクティベーションには、個別のアクティベーションコードが必要です。

アクティベーションコードの取得

- トレンドマイクロの Web サイトから IWSS をダウンロードした場合、体験版のアクティベーションコードを自動的に受け取ります。
- 製品版を購入された場合は、アクティベーションコードがパッケージに同梱されています。

ログインアカウントの管理

割り当てられたアクセス権を使用して、最大 128 のユーザが IWSS にアクセスできます。IWSS にログインしている間、ユーザは [ログインアカウント] ページに設定されているアクセス権に応じて設定を変更することができます。

アクセス権について

責任範囲が部門ごとで、また場合によってはヘルプデスク権限を有するセキュリティ管理者のチームがある場合、アクセス権の割り当ては組織にとって好都合です。IWSS の管理では、このようにユーザが異なる権限でログインできます。

アクセス権により、IWSS 内で加えられている変更内容を監査することができます。特定の機関の標準に準拠する必要がある場合、この機能は重要になります。

アクセスレベルには次の 3 種類があります。

- 管理者 — システムへのまったく制限のないアクセスが許可されます。コンソールからアクセスして、ユーザアカウントの作成、削除、変更を含む、設定の読み取り、変更が可能です。
- 閲覧のみ — 設定変更はできませんが、設定、ログ、レポートの閲覧のみ可能です。自分のパスワードを変更できます。
- レポート閲覧のみ — 概要ページと予約レポートの閲覧のみ可能です。ログやリアルタイムのレポートクエリを生成します。これは新規ユーザの初期設定アクセスレベルです。

ログインアカウントを追加する

ログインアカウントを追加するには

1. メインメニューから [管理] → [ログインアカウント] の順に選択します。
2. [ログインアカウント] 画面で、[追加] をクリックします。

3. [アカウントの追加] 画面で、必要な情報を入力します。

   - **ユーザ名** — ログインアカウントに割り当てられたユーザの名前。
   - **パスワード** — 4 ～ 32 文字の英数字を組み合わせて使用します。辞書に掲載されている語句、名前、日付は避けます。
   - **説明** — ログインアカウントに関する説明を入力するフィールド。
   - **アクセス権** — 193 ページの「アクセス権について」を参照してください。

4. [保存] をクリックします。[ログインアカウント] 画面に、新しいログインアカウントが表示されます。

監査ログファイル

監査ログファイルとは、ユーザが IWSS に対して実行した設定変更を保存するファイルです。ログファイルには、ログを整理するために使用できるプレフィックスが含まれます。

ログのプレフィックスは、自動生成されますが、コマンドラインインタフェース (CLI) で変更できます。ログのプレフィックスを変更するには、ユーザに root 権限があることが必要で、CLI から設定ファイル (/iscan/intscan.ini) を開いて、必要な変更を加えます。最後に、変更内容を有効にするため IWSS を再起動します。

IWSS サーバファームの設定

トラフィックおよび検索の負荷を分散するために、複数の IWSS サーバを使用できます。複数サーバ構成では、1 つのサーバが「マスター」として指定され、ファーム内の他のサーバが「スレーブ」として指定されます。スレーブサーバはマスターから設定を取得し、セキュリティおよびプログラムイベント情報をマスターに報告するので、管理者はネットワーク上のすべての IWSS サーバからの総合レポートを表示できます。

注意： 1 つの IWSS サーバファームには、1 つのマスターサーバのみ必要です。

サーバの指定を設定するには

1. IWSS Web コンソールを開き、[管理] → [IWSS 設定] → [IWSS サーバファーム] の順に選択します。
2. [IWSS サーバファームを有効にする] を選択します。
3. マスターの待機ポート番号の値を入力します (初期設定では 1444)。
4. [サーバの役割] で、次の 2 つのオプションのうち 1 つをクリックします。
   - マスターサーバ
   - スレーブサーバ

     スレーブサーバロールについて、マスターの IP アドレスを表示されるフィールドに入力します。
5. [保存] をクリックします。

Trend Micro Control Manager エージェントの登録

Trend Micro Control Manager (以下、Control Manager) エージェントを使用できるようにする前に、このエージェントを Control Manager に登録する必要があります。

Control Manager エージェントを登録するには

1. IWSS Web コンソールで [管理] → [IWSS 設定] → [Control Manager 設定] 画面に進みます。
2. [Control Manager 設定] 画面で、適切な情報を入力します。
3. [登録] をクリックします。

   登録が正常に完了した場合、[接続ステータス] に 「登録済み Control Manager サーバ: 接続されました」と表示され、[登録] ボタンが [アップデート設定] ボタンになります。
   登録に失敗した場合、[接続ステータス] に 「登録済み Control Manager サーバ: 接続されていません」と表示されます。

MCP プロキシの設定または双方向通信ポート転送情報をアップデートするには

注意： Control Manager サーバ設定をアップデートできません。

1. [MCP プロキシの設定] および [双方向通信ポート転送] またはそのいずれかで必要な変更を行います。
2. [登録] をクリックします。
3. エージェントが新しい設定にアップデートされるまで 20 ～ 30 秒待ち、[Control Manager 設定] 画面に戻ります。

Control Manager エージェントをアップデートするには

1. [登録解除] をクリックしてエージェントの登録を解除します。エージェントを Control Manager から登録解除するまで 20 ～ 30 秒待ちます。
2. 必要な変更を行い、[登録] をクリックします。
3. エージェントが新しい設定にアップデートされるまで 20 ～ 30 秒待ち、[Control Manager 設定] 画面に戻ります。

   エージェントは新しい Control Manager サーバ設定で Control Manager に登録されます。

第 13 章

通知

本章で説明する内容には、次の項目が含まれます。

- 198 ページの「通知について」
- 199 ページの「受信者設定」

通知について

通知は、検索、ブロック、アラート、およびプログラムアップデートイベントに対して発行できます。通知には、管理者への通知とユーザへの通知の 2 種類あります。

- 管理者への通知では、HTTP 検索、HTTP のファイルタイプによるブロック、FTP のファイルタイプによるブロック、FTP 検索、しきい値アラート、制限されたトンネルトラフィック、アップレット /ActiveX 対策イベント、またパターンファイルや検索エンジンのアップデートに関する情報が提供されます。Trend Micro InterScan Web Security Suite (以下、IWSS) は、管理者への通知を [メール設定] 画面で設定したアドレスに送信します。
- ユーザへの通知では、HTTP 検索、HTTP のファイルタイプによるブロック、FTP 検索、URL ブロック、FTP のファイルタイプによるブロック、およびアプレット /ActiveX 検索イベントに関する情報が提供されます。IWSS は、クライアントが閲覧またはダウンロードしようとしている禁止 Web ページやファイルの代わりに、ユーザへの通知をクライアントのブラウザまたは FTP クライアントに表示します。

管理者への通知およびユーザへの通知の両方に表示されるメッセージは設定可能です。「トークン」または変数を含めて、イベント情報に関する通知メッセージをカスタマイズできます。さらに、ユーザへの通知では HTML タグがサポートされているため、メッセージの外観をカスタマイズしたり、イントラネット上でホストされているセキュリティポリシードキュメントなど、他のリソースへのリンクを提供したりできます。

受信者設定

IWSS は、管理者への通知を指定されたメールアドレスに送信します。管理者は IWSS をインストールしてセットアッププログラムを実行する際にメールの設定を入力します。ただし、メールの設定はインストール後に Web コンソールの [メール設定] 画面で変更することもできます。

管理者への通知用のメール設定を行うには

1. メインメニューから [通知] をクリックします。
2. [通知] 画面の上部で、[通知先の設定 ...] をクリックします。
3. 通知の送信先メールアドレス、送信者のメールアドレス、SMTP サーバ、SMTP サーバポート、およびメールキューを確認する間隔を入力します。
4. メールサーバで ESMTP が必要な場合は、IWSS で EHLO コマンドを使用して SMTP セッションを開始できるように、[EHLO (Extended Hello) コマンドを使用する] チェックボックスをオンにします。
5. [保存] をクリックします。

通知の変数 / パラメータ

より意味のある通知にするために、IWSS では通知内で情報のプレースホルダとして変数を使用できます。イベントが発生すると、IWSS は変数を特定の情報と動的に置き換え、その特定のイベントに関する詳細な情報を提供します。

たとえば、次のような一般的な通知を作成できます。

HTTP トラフィックでウイルスが検出されました。

この通知では、問題が発生していることはわかりますが、詳細は提供されません。代わりに、変数を使用して次のような通知を設定できます。

%Y に、IWSS がファイル %F でセキュリティリスク %V を検出しました。%N が %U からファイルをダウンロードしようとしました。

この通知は、たとえば次のようになります。

07/01/23 8:36 AM に、IWSS がファイル eicar.com でセキュリティリスク Eicar_test_file を検出しました。123.123.123.12 が http://www.eicar.org/download/eicar.com からファイルをダウンロードしようとしました。

この情報があれば、管理者はクライアントに連絡して、さらに多くのセキュリティ情報を提供できます。この例の通知では、5 つの変数が使用されています。%Y、%V、%F、%N、および %U です。

次の表は、通知メッセージおよび画面で使用できる変数のリストを示しています。

表 13-1. 変数の説明

変数	変数の意味	変数の使用方法
HTTP および FTP 検索		
%Y	日付と時刻	イベントが発生した日時
%F	ファイル名	anti_virus_test_file.htm など、リスクが検出されたファイルの名前
%V	不正プログラム名 (ウイルス、トロイの木馬など)	検出されたリスクの名前
%	文字「%」自体	パーセント文字を通知メッセージまたはページに挿入するために使用
%f	送信元	感染またはブロックされたファイル、またはフィルタされた URL を発信したサーバ。この変数は、通知 (メールまたは SNMP) には使用できません。
%A	実行された処理	IWSS によって実行された処理
%m	方法	イベントを発生させた処理方法。この変数は、通知 (メールまたは SNMP) には使用できません。
%M	移動先	ファイルが移動された隔離フォルダの場所
%H	IWSS ホスト名	イベントが発生した IWSS ホスト名
%N	ユーザ名	

変数	変数の意味	変数の使用方法
%R	転送方向	
%U	URL/URI	
%X	理由 / ブロックタイプ	
HTTP/FTP ファイルタイプのブロック		
%U	URL/URI	
次の変数は、管理者へのメッセージまたはユーザへの通知メッセージにのみ使用されます。		
%F	ファイル名	
%A	実行された処理	
%H	IWSS ホスト名	
%R	転送方向	
%X	理由 / ブロックタイプ	
%Y	日付と時刻	
%N	ユーザ名	
%V	ウイルスまたはトロイの木馬	
アプレットおよび ActiveX 対策		
%D	検索されるプロトコル	
%H	IWSS ホスト名	
%N	ユーザ名	
%U	URL/URI	
%W	独自のメールの送信	
%X	理由	
%Y	日付と時刻	
%Z	ポリシー名	
インスタントメッセージ (IM) および IntelliTunnel セキュリティ		
%D	検索されるプロトコル (HTTP または FTP)	
%H	IWSS ホスト名	
%N	ユーザ名	

変数	変数の意味	変数の使用方法
%U	URL/URI	
%X	理由 (ブロックされたプロトコルのローカライズ名)	
%Y	日付と時刻	
%Z	ポリシー名	
URL ブロック		
%H	IWSS ホスト名 (ヘッダフィールドでのみ機能)	
%U	URL/URI (本文でのみ機能)	
%X	理由 (本文でのみ機能)	
URL フィルタ		
%U	URL/URI	
%X	理由	
しきい値の通知		
%m	基準	
%t	しきい値	

通知の設定

通知を設定するには、通知を発行するイベントの種類を選択し、メールまたはブラウザ通知メッセージを編集します。

ユーザへの通知での HTML タグの使用

ユーザへの通知メッセージは、HTML を使用して書式を設定できます。HTML ファイルには外部の画像またはスタイルへの参照リンクを含めることができますが、IWSS でサポートされるのは HTML ファイルのアップロードだけです。その他のファイルは個別に Web サーバにアップロードする必要があります。リンクの破損を防ぐために絶対リンクを使用することをお勧めします。

HTTP 検索通知の設定

クライアントが要求したファイル中に不正コードを検出すると、IWSS は管理者への通知をメールで発行し、ユーザへの通知を要求元クライアントのブラウザに送信します。

IntelliTrap で検出されたファイルは一種のセキュリティの脅威と見なされるので、HTTP 検索と同じ通知が使用されます。

HTTP 検索通知を設定するには

1. [通知] → [HTTP 検索] の順に選択します。
2. [管理者への通知] で、通知の対象とする検出イベントのチェックボックスをオンにします ([ウイルス]、[トロイの木馬]、[その他のインターネット上の脅威] のいずれかまたはすべて)。

   注意： IntelliTrap 通知は、[その他のインターネット上の脅威] に関連付けられています。したがって、IntelliTrap 通知は [その他のインターネット上の脅威] を選択すると有効になります。

3. 初期設定の通知メッセージを使用しない場合は、初期設定のテキストを選択して、任意のテキストを入力します。該当する場合は、199 ページの「通知の変数 / パラメータ」で説明されているように、メッセージに変数を挿入します。
4. ブラウザに表示する [タイトル] を入力します。初期設定は「IWSS セキュリティイベント (サーバ名)」です。タイトルは、ウイルス感染メッセージ、ファイルタイプブロック、および URL ブロックメッセージで共通です。
5. [ダウンロードファイルに対するメッセージ] および [アップロードファイルに対するメッセージ] は、次のように設定します。

   a. 初期設定の警告メッセージを表示するには、[初期設定] チェックボックスをオンにします。

   b. 独自のメッセージを表示するには [カスタマイズ] チェックボックスをオンにし、カスタマイズしたメッセージの内容を入力するか、または HTML ファイルからインポートします。

c. [プレビュー] をクリックして、通知が正しく表示されることを確認します。

6. [保存] をクリックします。

URL ブロックのユーザへの通知の設定

IWSS で、ローカル IWSS リストからフィッシングパターンファイルにある URL または禁止 URL へのアクセスが検出されると、IWSS は要求元クライアントのブラウザに、URL がブロックされたことを示す警告画面が表示されます。

URL ブロック通知を設定するには

1. メインメニューから [通知] を選択し、[URL ブロック] をクリックします。
2. [規制された URL にアクセスしたユーザへの通知] で、次の操作を実行します。

   a. 初期設定の警告メッセージを表示するには [初期設定] チェックボックスをオンにします。

   b. 独自の警告メッセージを表示するには [カスタマイズ] チェックボックスをオンにします。メッセージをテキストボックスに入力するか、ローカルコンピュータの HTML ファイルからメッセージをインポートします。

3. [プレビュー] をクリックして、通知が正しく表示されることを確認します。
4. [保存] をクリックします。

FTP 検索通知の設定

IWSS では、ユーザの FTP 転送に不正コードが検出されると、カスタマイズした管理者への通知を指定されたメールアドレスに自動的に送信したり、要求元 FTP クライアントのプログラムに通知を表示したりできます。

FTP 検索通知を設定するには

1. メインメニューから [通知] を選択し、[FTP 検索] をクリックします。
2. [管理者への通知] で、通知の対象とする検出イベントのチェックボックスをオンにします ([ウイルス]、[トロイの木馬]、[その他の不正プログラム] のいずれかまたはすべて)。
3. 初期設定の通知メッセージを使用しない場合は、初期設定のテキストを選択して、任意のテキストを入力します。該当する場合は、199 ページの「通知の変数 / パラメータ」で説明されているように、テキストに変数を挿入します。
4. ユーザへの通知の [メッセージ] は、次のように設定します。
   a. 初期設定の警告メッセージを表示するには、[初期設定] チェックボックスをオンにします。
   b. 独自のメッセージを表示するには [カスタマイズ] チェックボックスをオンにして、カスタマイズした内容を入力します。
5. [保存] をクリックします。

IntelliTunnel セキュリティ通知の設定

IWSS はポート 80 で規制されたトンネルトラフィックを検出すると、このトラフィックをブロックして、[IntelliTunnel の通知] 画面で指定されたアドレスに通知をメールで送信します。90 ページの「IntelliTunnel に関する注意」を参照してください。

IntelliTunnel セキュリティの通知を設定するには

1. メインメニューから [通知] をクリックし、[IntelliTunnel] をクリックします。

2. [管理者への通知] で、[規制されたトンネルトラフィックが検出された場合に通知を送信する] チェックボックスをオンにします。
3. 初期設定の通知メッセージを使用しない場合は、初期設定のテキストを選択して、任意のテキストを入力します。該当する場合は、199 ページの「通知の変数 / パラメータ」で説明されているように、テキストに変数を挿入します。
4. [保存] をクリックします。

アプレットおよび ActiveX 対策通知の設定

IWSS は、セキュリティポリシーに違反する Java アプレットまたは ActiveX オブジェクトのダウンロードを検出すると、管理者への通知をメールで送信し、ユーザへの通知メッセージを要求元クライアントのブラウザに表示します。

アプレットおよび ActiveX 対策通知を設定するには

1. メインメニューから [通知] をクリックし、[アプレット /ActiveX 検索] をクリックします。
2. [管理者への通知] で、[不正なアプレット /ActiveX の動作が検出された場合に通知を送信する] チェックボックスをオンにします。
3. 初期設定の通知メッセージを使用しない場合は、初期設定のテキストを選択して、任意のテキストを入力します。該当する場合は、199 ページの「通知の変数 / パラメータ」で説明されているように、テキストに変数を挿入します。
4. [ユーザへの通知] は、次のように設定します。
   a. 初期設定の警告メッセージを表示するには、[初期設定] チェックボックスをオンにします。
   b. 独自のメッセージを表示するには [カスタマイズ] チェックボックスをオンにし、カスタマイズしたメッセージの内容を入力するか、[インポート] を使用してインポートします。
5. [保存] をクリックします。

パターンファイルのアップデート通知の有効化

IWSS では、検索エンジンまたはパターンファイルのアップデート試行の際に通知を送信できます。

パターンファイルのアップデート通知を有効にするには

1. メインメニューから [通知] を選択し、[パターンファイルのアップデート] をクリックします。
2. パターンファイルのアップデート試行は、次のように設定します。
   a. 通知の対象とするアップデートイベントを選択します。[成功]、[失敗]、または [アップデート不要] のアップデート試行に対して通知を設定できます。
   b. 通知メッセージの [件名] を入力します。
3. [保存] をクリックします。

URL フィルタおよび検索エンジンのアップデート通知の有効化

パターンファイルのアップデートほど頻繁ではありませんが、トレンドマイクロでは、ウイルスおよび不正コードの検出方法の進化を反映するために、定期的に新しいバージョンの検索エンジンをリリースします。IWSS では、検索エンジンのアップデートに応じて、管理者への通知を発行できます。

URL フィルタおよび検索エンジンのアップデート通知を有効にするには

1. メインメニューから [通知] を選択し、[URL フィルタエンジンおよび検索エンジンのアップデート] をクリックします。
2. 検索エンジンまたは URL フィルタエンジンについて、通知の対象とするアップデートイベントを選択します。

[成功]、[失敗]、または [アップデート不要] のアップデート試行に対して通知を設定できます。

3. 検索エンジンまたは URL フィルタエンジンについて、通知メールメッセージの [件名] を入力します。

4. [保存] をクリックします。

しきい値アラートの通知の有効化

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

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

IWSS では、これらのアラートをメールまたは SNMP トラップ / 通知 (有効になっている場合)、または両方を使用して送信できます。

しきい値アラートの通知を有効にするには

1. メインメニューから [通知] を選択し、[しきい値アラート] をクリックします。

2. [しきい値] で必要なしきい値を指定し、初期設定を使用するか、または [しきい値] 列と [通知の送信間隔] 列に新たな値を指定します。

3. [通知メッセージ] で初期設定の通知メッセージを使用しない場合は、初期設定のテキストを選択して、任意のテキストを入力します。該当する場合は、199 ページの「通知の変数 / パラメータ」で説明されているように、テキストに変数を挿入します。

4. [保存] をクリックします。

SNMP トラップ通知の有効化

IWSS では、セキュリティ、アップデート、またはプログラムイベントに対する SNMP トラップの送信がサポートされています。

SNMP 通知を送信するには、まず SNMP を設定してから、この機能を有効にする必要があります。そのためには、[管理] → [IWSS 設定] → [SNMP 設定] の順に選択します。

SNMP トラップの送信を有効にするには

1. メインメニューから [通知] をクリックし、[SNMP 通知] → [通知の設定 ...] をクリックします。
2. SNMP 通知を実行するイベントの種類を選択します。イベントには次のような種類があります。
   - **ウイルスまたはインターネット上の脅威の検出** — ウイルスまたは不正コードの検出に関連するイベントです。
   - **セキュリティ違反** — ウイルス検出以外の、IWSS ポリシーで禁止されている活動に関連するイベントです (アクセス割り当てポリシー、URL ブロック設定など)。
   - **パターンファイル /URL フィルタデータベース / 検索エンジンのアップデート** — IWSS のアップデートに関連するイベントです。
   - **IWSS サービスの予期しない停止** — IWSS サービスが異常停止したときのイベントです。
   - **システムパフォーマンス測定** — 次のパフォーマンスデータを記載した SNMP トラップを定期的に送信するイベントです。
     - CPU 使用率
     - メモリ使用率
     - ディスク使用率
     - 同時接続 (ICAP 要求および応答モードおよびプロキシモード)
     - 送受信スループット (バイト / 秒)
3. [保存] をクリックします。

第 14 章

レポートおよびログ

本章で説明する内容には、次の項目が含まれます。

- 212 ページの「レポートについて」
- 212 ページの「レポートの種類」
- 215 ページの「レポート設定」
- 216 ページの「レポートの生成」
- 222 ページの「ログについて」

レポートについて

Trend Micro InterScan Web Security Suite (以下、IWSS) では、ウイルスおよび不正コードの検出、ブロックされたファイル、アクセスされた URL、およびトレンドマイクロ ダメージクリーンナップサービス (以下、DCS) によるクリーンナップに関するレポートを生成できます。IWSS のプログラムイベントに関するこの情報を使用して、プログラムの設定を最適化し、組織のセキュリティポリシーを微調整できます。

レポートは設定およびカスタマイズできます。たとえば、IWSS では、すべてのユーザまたは特定のユーザに対するレポートを必要に応じてリアルタイムに、またはスケジュールに従って生成できます。最新の情報を必要とする人と共有できるように、IWSS では、予約レポートを表示する準備ができた際にメールで通知を送信できます。

レポートの種類

IWSS では、以下のカテゴリのレポートを作成できます。

- **ブロックイベントレポート** — ウイルス検出、ポリシー違反、およびブロックされた URL に関するレポートです。
- **トラフィックレポート** — Web 閲覧活動や最もアクセスの多い Web サイトとダウンロードに関するレポート、およびその他の Web 閲覧活動の詳細に関するレポートです。
- **スパイウェアレポート** — スパイウェアの検出に関するレポートです。
- **クリーンナップレポート** — IWSS によって要求された DCS のクリーンナップ試行に関するレポートです。
- **個別 / ユーザ別レポート**

次のリストは、生成可能なすべてのレポートを示しています。

ブロックイベントレポート

リアルタイムのレポートには IntelliTrap が使用され、HTTP データとともに圧縮された実行可能ファイルを受信した場合、潜在的な不正コードをリアルタイムで検出します。IntelliTrap によって不正な実行可能ファイルが検出されると、検出結果がブロックイベントレポートに表示されます。

- 最もウイルス検出の多い URL
- 最も不正 URL へのアクセス要求の多いユーザ
- 最も違反の多いユーザ
- 最も違反の多いグループ
- 最もブロックの多い URL カテゴリ *
- 最もブロックの多いアプレット /ActiveX オブジェクト *
- 最もブロックの多い URL
- 曜日別 URL ブロック数
- 時間別 URL ブロック数
- IntelliTunnel レポート

* 個別ライセンスが必要

個別 / ユーザ別レポート

- 概要レポート
- 最もユーザアクセスの多いサイト
- 最もブロックの多い URL
- 最もブロックの多い URL カテゴリ *
- ユーザによる URL アクセス

* 個別ライセンスが必要

トラフィックレポート

トラフィックレポートでは、[ログ] → [設定] で [HTTP/FTP アクセスイベントの記録] を有効にする必要があります。

トラフィックレポートは生成に時間がかかる場合があります。アクセスログの多い大きなサイトの場合は数時間かかることもあります。

- 最もアクセス数の多いユーザ
- 最もアクセスの多い URL
- 最もアクセスの多いダウンロード対象
- 最もアクセスの多い検索サイト
- 日次トラフィック量
- 上位カテゴリ (重み付け)*
- 曜日別アクセス数
- 時間別アクセス数

* 上位カテゴリレポートにアクセスするには、URL フィルタアクティベーションコードを取得する必要があります。

スパイウェアレポート

- 最もクリーンナップの多いスパイウェアの種類
- 最も検出の多いスパイウェア
- 最もスパイウェアの感染回数が多いユーザ

クリーンナップレポート

- 最もクリーンナップの多い不正プログラムの種類 *
- 最もクリーンナップの多い不正プログラム *
- 最も感染の多い IP アドレス *

* 個別ライセンスが必要

レポート設定

リアルタイムレポートの生成時または予約レポートの設定時に、次の情報を指定する必要があります。

レポートの作成対象

レポートを生成する対象のユーザを選択します。次のオプションがあります。

- **すべてのユーザ** — IWSS 経由でインターネットにアクセスしているすべてのユーザ
- **指定するユーザ** — 特定の IP アドレス、ホスト名、または LDAP ディレクトリエントリを持つクライアント
- **すべてのグループ** — LDAP ディレクトリ内のすべてのグループ。IP アドレスまたはホスト名を指定する場合は、すべてのグループは、すべてのユーザと同等です。
- **指定するグループ** — LDAP グループまたは IP アドレスの指定

特定のユーザまたはグループに対してレポートを生成する場合、ユーザの選択方法は [HTTP] → [設定] → [ユーザの識別] で設定した方法によって決まります。ユーザの識別の詳細については、100 ページの「ユーザ識別方法の設定」を参照してください。

レポートの種類

IWSS では、予約レポートで、可能なレポートをすべて含む総合レポートを生成します。予約レポートでもリアルタイムレポートでも、個別レポートを指定して生成できます。生成可能なレポートのリストは、212 ページの「レポートの種類」を参照してください。

オプション

IWSS では、プログラム情報を棒グラフ、積み重ね棒グラフ、または線グラフで表示できます。IWSS でブロックされた URL またはダウンロードと成功した要求では、グラフで色分けすることもできます。

その他のレポート設定

リアルタイムレポートでは、レポートの対象となる期間を指定します。

予約レポートを設定する際は、次のような設定項目もあります。

- レポートの生成時に送信する通知メールの設定
- 作成日および作成時刻の設定
- 予約レポートの有効 / 無効の設定

レポートの生成

リアルタイムレポート

IWSS では、インターネットにアクセスしているすべてまたは一部のクライアントに対して、リアルタイムでレポートを生成できます。

リアルタイムレポートを設定するには

1. メインメニューから [レポート] → [リアルタイムレポート] の順に選択します。
2. [期間] で、レポートの対象期間を選択します ([すべて]、[今日]、[過去 7 日間]、[過去 30 日間] のいずれか)。
3. 任意の期間でレポートを生成するには [指定] をクリックし、[開始] と [終了] の日付と時間を選択します。
4. [作成対象] で、レポートを生成する対象として [すべてのユーザ]、[指定するユーザ]、[すべてのグループ]、または [指定するグループ] を選択します。指定するユーザに対するレポートの詳細については、「特定のグループを選択するには」および 218 ページの「特定のユーザを選択するには」を参照してください。

5. [レポートの種類] で、必要なレポートのパラメータを選択します。

注意： IWSS では複数のレポートパラメータを 1 つのレポートにまとめ、レポートパラメータごとに記載があります。

6. [オプション] で、グラフの種類をメニューから選択します。ブロックされたトラフィックとブロックされていないトラフィックを異なる色で示すには、[ブロックトラフィックと通過トラフィックの区別] チェックボックスをオンにします。

7. [レポートの生成] をクリックします。

フォームを初期設定値にリセットするには、[リセット] をクリックします。

次の表は、レポートを構成するパラメータの情報を示しています。

作成対象	レポートを構成するパラメータ
すべてのユーザ	リストに含まれる「ユーザ別レポート」以外のすべてのレポートパラメータを含みます。
指定するユーザ	「ユーザ別レポート」パラメータのみを含みます。
すべてのグループまたは指定するグループ	有効になっているレポートは次のとおりです。 - 最も違反の多いグループ * - 最もブロックの多い URL カテゴリ * - 最もブロックの多いアプレット /ActiveX オブジェクト - 最もブロックの多い URL* - 曜日別 URL ブロック数 * - 時間別 URL ブロック数 *
* Web レピュテーションの場合 (ファーミング対策、フィッシング対策など)、ブロックされたサイトはこれらのレポートに表示されます。ただし、ブロックされたサイトを検索する場合、情報が記載されているのは「最もブロックの多い URL」のみです。	

表 14-1. レポートタイプによって異なる使用可能なレポートパラメータ

特定のグループを選択するには

1. メインメニューから [レポート] → [リアルタイムレポート] の順に選択します。
2. [作成対象] で [指定するグループ] を選択し、[選択] をクリックします。[指定するグループ] ([レポート] → [リアルタイムレポート] → [作成対象]) で [選択] をクリックすると、[HTTP] → [設定] → [ユーザの識別] で設定したユーザの識別方法に従って、[グループの選択] 画面が表示されます。.
3. IP アドレス範囲を入力するか、「ユーザ / グループ名」による識別方法を使用している場合は LDAP ディレクトリでグループ名を検索します。
4. [追加] をクリックします。
5. レポートの含めるグループを追加したら、[保存] をクリックします。

特定のユーザを選択するには

1. メインメニューから [レポート] → [リアルタイムレポート] の順に選択します。
2. [作成対象] で [指定するユーザ] を選択し、[選択] をクリックします。

   [指定するユーザ] ([レポート] → [リアルタイムレポート] → [作成対象]) で [選択] をクリックすると、[HTTP] → [設定] → [ユーザの識別] で設定したユーザの識別方法に従って、[ユーザの選択] ポップアップ画面が表示されます。
3. [IP アドレス] または [ホスト名] に入力するか、「ユーザ / グループ名」による識別方法を使用している場合は LDAP ディレクトリでユーザ名を検索します
4. [追加] をクリックします。
5. レポートに含めるユーザを追加したら、[保存] をクリックします。

予約レポート

予約レポートを日、週、または月ベースで生成するように IWSS を設定できます。生成される大量のレポートを管理するために、IWSS では指定したレポートのみを生成し、不要な予約レポートを保存先ディレクトリから削除できます。

予約レポートを設定するには

1. メインメニューから [レポート] → [予約レポート] の順に選択します。
2. 予約レポートを作成する頻度に応じて、[日]、[週]、または [月] のいずれかのタブをクリックします。
3. [{ 頻度 } レポートを有効にする] チェックボックスをオンにします。
4. [{ 頻度 } レポート設定] リンクをクリックします。
5. 予約レポートを生成する時間および日付を設定します。
6. [作成対象] で、レポートの対象を選択します。
   - すべてのユーザ
   - 指定するユーザ
   - すべてのグループ
   - 指定するグループ

   注意： 指定するユーザに対するレポートの詳細については、218 ページの「特定のグループを選択するには」および 218 ページの「特定のユーザを選択するには」を参照してください。
7. [レポートの種類] で、生成するレポートの種類を選択します。
   - 総合レポート
   - 個別レポート 個別レポートを選択した場合には、含めるレポートの種類を選択します。

8. [オプション] で、メニューから [棒グラフ]、[積み重ね棒グラフ]、または [線グラフ] のいずれかのグラフの種類を選択します。

   ブロックされたトラフィックとブロックされていないトラフィックを異なる色で示すには、[ブロックトラフィックと通過トラフィックの区別する] チェックボックスをオンにします。

9. [通知] の [レポート通知の送信先] フィールドに、新しく生成されたレポートを表示する準備ができたら IWSS で通知を送信するメールアドレスを入力します。複数のメールアドレスはカンマ (,) で区切ります。

10. [保存] をクリックします。

作成された予約レポートを削除するには

1. メインメニューから [レポート] → [予約レポート] の順に選択します。

2. 削除するレポートに応じて、[日]、[週]、または [月] のいずれかのタブをクリックします。

3. 削除するレポートを選択して [削除] をクリックします。

レポートのカスタマイズ

IWSS では、各種レポートに表示するレコード数をカスタマイズできます。たとえば、Web トラフィックレポートの「最もアクセスの多いユーザ」に表示するユーザ数を設定できます。初期設定のレコード数は、すべてのレポートで 10 です。

IWSS は、予約レポートを保存するように設定できます。初期設定の保存先は /etc/iscan/report ですが、これは変更できます。初期設定では、60 個の日次レポート、20 個の週次レポート、4 個の月次レポートを、サーバから削除せずに保存するよう設定されています。ただし、保存する予約レポートの数は設定できます。

レポートのデータ管理設定をカスタマイズするには

1. メインメニューから [レポート] → [カスタマイズ] の順に選択します。

2. [表示する件数] で、各レポートに含めるレコード数を入力します。

3. [レポートの保存] で、各フィールドに次の情報を入力します。

   a. レポートを保存する [保存先ディレクトリ] (初期設定は /etc/iscan/report)

   注意 : [保存先ディレクトリ] を変更する場合、フォルダを [レポートのカスタマイズ] 画面に入力する前に、そのフォルダが IWSS サーバ上に存在する必要があります。すでに生成されたレポートを表示するには、新しいフォルダにレポートをコピーします。

   b. 保存する予約レポートの数

   - [日次レポート] (初期設定は 60)
   - [週次レポート] (初期設定は 20)
   - [月次レポート] (初期設定は 4)

4. [保存] をクリックします。

ログについて

IWSS で使用できるログは 2 種類あります。セキュリティログとシステムログです。

セキュリティログには、プログラムイベントに関する情報が含まれます。セキュリティログは、IWSS Web コンソールを使用してクエリまたは表示できます。このログに含まれるものは次のとおりです。

- ウイルス
- URL ブロック
- パフォーマンス
- URL アクセス

システムログには、ソフトウェアの状態の変化やエラーに関する非構造化メッセージが含まれています。これは、ログファイルを表示した場合にのみ見ることができ、Web コンソールには表示されません。このログに含まれるものは次のとおりです。

- HTTP 検索
- FTP 検索
- メール配信
- 管理、アップデートおよび監査

すべてのセキュリティログデータはデータベースに保存されます。ログデータはテキストログファイルに保存することもできます。テキストログファイルは、旧バージョンの IWSS と互換性があり、カスタムスクリプトを使用したデータの追加分析が許可されます。テキストログファイルにログデータを保存した場合、データベースが適切にアップデートされていることを確認する冗長性が備わります。しかし、テキストログファイルによりディスク領域を圧迫する可能性があるのでデータベースをログデータの唯一の保存場所として使用することをお勧めします。

データ記録のオプション

IWSS では、セキュリティログのデータを使用してレポートを生成します。IWSS は、セキュリティログのデータをデータベースとテキストログの両方、データベースのみ、またはテキストログのみに書き込むように設定できます。テキストのみのオプションを選択した場合、IWSS ユーザインタフェース内からレポートもログも表示できません。この場合、作成されたテキストファイルを直接開いて、ログのみを表示できます。

セキュリティログのオプションは、IWSS Web コンソールの [ログ] → [設定] で設定します (詳細については、232 ページの「ログの設定」を参照)。テキストログは、旧バージョンの IWSS との下位互換性を提供し、カスタムスクリプトまたはその他のサードパーティアプリケーションでログデータを詳しく分析するために使用できます。また、データベースに記録されたログの完全性と正確さを確認するために、テキストログを使用することもできます。

アクセスログを有効にすると、パフォーマンスが低下します。そのため、[HTTP/FTP アクセスイベントの記録] は、初期設定では無効になっています。アクセスログを有効にしない場合、ユーザの活動に関する多くのレポートが使用できなくなります。さらに、IWSS が上位プロキシとして設定されている場合、ユーザの活動に関する重要なデータが使用できなくなる可能性があります。IWSS ですべての Web 関連活動の要約を作成する場合は、[ログ] → [設定] → [セキュリティログ] → [オプション] でアクセスログを有効にします。

注意 : アクセスログを有効にすると、IWSS サービスが再起動されます。再起動時に、ルータで再度 IWSS が認識されるまでに最大 30 秒程度かかる可能性があります。この間、ルータではパケットがリダイレクトされません。

ログのクエリおよび表示

IWSS Web コンソールには、ログファイルにクエリを実行するためのツールが用意されています。

監査ログ

監査ログには、ユーザが変更したアプリケーションの設定を説明する情報が記載されています。たとえば、ユーザが移行またはロールバックの手順をアクティブ化した場合、移行活動を記録するエントリが監査ログに作成されます。

監査ログを表示するには

1. メインメニューから [ログ] → [監査ログ] の順に選択します
2. [期間] で、レポートを生成する時間を選択します。

   任意の期間のウイルスログを表示するには、[指定] をクリックし、開始と終了の日付と時間を選択します。
3. [ユーザ] で、ログエントリを表示するユーザを選択します。[追加] をクリックします。リストにあるすべてのユーザを追加する場合は、[すべて追加] をクリックします。ユーザを右側のリストボックスから削除するには、[削除] をクリックします。リストにあるすべてのユーザを削除する場合は、[すべて削除] をクリックします。
4. [並べ替え基準] で、ログの並べ替えの基準とするオプションを選択します。
5. [ログ表示] をクリックします。

   [監査ログ] 画面が開きます。
6. 画面を更新するには、[表示更新] をクリックします。

ウイルスログ

ウイルスログには、IWSS が検出したウイルスに関する情報が含まれます。

ウイルスログを表示するには

1. メインメニューから [ログ] → [ウイルスログ] の順に選択します。
2. [期間] で、レポートを生成する時間を選択します。

   任意の期間のウイルスログを表示するには、[指定] をクリックし、開始と終了の日付と時間を選択します。
3. [ウイルス] で、ログエントリを表示するウイルスを選択します。[追加] をクリックします。リストにあるすべてのウイルスを追加する場合は、[すべて追加] をクリックします。ウイルスを右側のリストボックスから削除するには、[削除] をクリックします。リストにあるすべてのウイルスを削除する場合は、[すべて削除] をクリックします。
4. [並べ替え基準] で、ログの並べ替えの基準とするオプションを選択します。
5. [ログ表示] をクリックします。

   [ウイルスログ] 画面が開きます。
6. 画面を更新するには、[表示更新] をクリックします。

スパイウェアログ

スパイウェアログには、スパイウェアの名前、検出日、処理、カテゴリ、検索の種類、感染したファイル名、関わったクライアントのユーザ ID など、IWSS で検出されたスパイウェアに関する情報が含まれます。

スパイウェアログを表示するには

1. メインメニューから [ログ] → [スパイウェアログ] の順に選択します。

2. [期間] で期間を選択します ([すべて]、[今日]、[過去 7 日間]、[過去 30 日間])。

   任意の期間を選択するには、[指定] をクリックし、開始と終了の日付と時間を選択します。

3. [スパイウェア] で、ログエントリを表示するスパイウェアを選択します。[追加] をクリックします。リストにあるすべてのスパイウェアを追加する場合は、[すべて追加] をクリックします。

   スパイウェアを右側のリストボックスから削除するには、[削除] をクリックします。リストにあるすべてのウイルスを削除する場合は、[すべて削除] をクリックします。

4. [並べ替え基準] で、ログの並べ替えの基準とする項目を選択します。[スパイウェア]、[日付]、[処理]、[カテゴリ]、[検索の種類]、[ファイル名]、[ユーザ ID] のオプションがあります。

5. [ログ表示] をクリックします。[スパイウェアログ] 画面が開きます。

6. 表示を更新するには、[表示更新] をクリックします。

URL ブロックログ

URL ブロックログには、ブロックの日時、カテゴリ、適用されたブロックルール、ユーザ ID、該当する場合は大規模感染予防ポリシー (OPP)、検索の種類など、ブロックされた URL に関する情報が含まれます。

URL ブロックログを表示するには

1. メインメニューから [ログ] → [URL ブロックログ] の順に選択します。

2. [期間] を選択します ([すべて]、[今日]、[過去 7 日間]、[過去 30 日間])。

   任意の期間を選択するには、[指定] をクリックし、開始と終了の日付と時間を選択します。

3. [ブロックされた URL] で、左側のリストボックスにある URL を右側のリストボックスに追加できます。

   追加する URL を選択し、[追加] をクリックします。リストにある URL をすべて追加する場合は、[すべて追加] をクリックします。URL のリストを右側のリストボックスから削除するには、[削除] をクリックします。リストにあるすべての URL を削除する場合は、[すべて削除] をクリックします。

4. [並べ替え基準] で、ログの並べ替えの基準とする項目を選択します。次のオプションがあります。

   - URL — ブロックされた URL
   - **日付** — URL がブロックされた日時
   - **カテゴリ** — URL フィルタ、アクセス割り当て、ファイルブロック、および URL ブロックポリシーでユーザによって定義されたルール
   - **ルール** — URL がブロックされた方法
     - IWSS **定義ルール (ウイルスを含む URL をブロック)** — ブロックされた URL を表示します。
     - URL **ブロックルール** — ブロックリストにある URL を表示します。
     - URL **フィルタルール** — ポリシー名を表示します。
     - **大規模感染予防ポリシー (OPP) 定義ルール** — OPP ルールを表示します。
     - **ファイルタイプ定義ルール** — ブロックされたファイルタイプを表示します。
     - **フィッシング定義ルール** — フィッシング違反ルールを表示します。
     - **アクセス割り当てポリシー** — アクセス割り当て違反ルールを表示します。
   - **ユーザ** ID — URL を要求したクライアントに関連付けられている IP アドレス、ホスト名、または LDAP ユーザ名
   - OPP ID — 大規模感染予防ポリシー (OPP) の ID 番号
   - **検索の種類** — アクセス割り当て、ファイルタイプ、URL メモリブロックリスト、コンテンツフィルタ、またはフィッシング対策のいずれか

5. [ログ表示] をクリックします。[URL ブロックログ] 画面が開きます。
6. 画面を更新するには、[表示更新] をクリックします。

注意： FTP プロキシがタイプ別にファイルをブロックする場合も、[URL ブロックログ] にエントリが表示されます。

URL アクセスログ

URL アクセスログには、URL アクセスの情報が含まれます。IWSS は、[ログ] → [設定] → [セキュリティログ] で [HTTP/FTP アクセスイベントの記録] が有効になっている場合にのみ、URL アクセスログに書き込みます。初期設定では、[HTTP/FTP アクセスイベントの記録] は無効になっています。URL アクセスログの各レコードには、次の情報が含まれています。

- アクセスされた日時
- サイトにアクセスしたユーザ
- アクセスを処理した IWSS サーバ
- アクセスを要求したクライアントの IP アドレス

注意： ネットワークアドレス変換によってこのデータが無意味になったり、またはすべてのアクセスが単一クライアントから発生するように見えることがあります。また、アクセスログを有効にすると、IWSS サービスが再起動されます。再起動時に、ルータで再度 IWSS が認識されるまでに最大 30 秒程度かかる可能性があります。この間、ルータではパケットがリダイレクトされません。

- アクセスされたドメイン
- URL のパスの部分 (HTTP サービスの場合は、URL のフルパスが表示されます)
- データの取得元サーバの IP アドレス
- アクセスイベントごとの URL カテゴリ

URL アクセスログを表示するには

1. IWSS Web コンソールを開き、メインメニューから [ログ] → [URL アクセスログ] の順に選択します。
2. ドロップダウンメニューから [期間] を選択します ([すべて]、[今日]、[過去 7 日間]、[過去 30 日間])。

   任意の期間を選択するには、[指定] をクリックし、開始と終了の日付と時間を選択します。
3. [並べ替え基準] で、ログの並べ替えの基準とする項目を選択します。
4. [ログ表示] をクリックします。[URL アクセスログ] 画面が開きます。
5. URL アクセスログを更新するには、[表示更新] をクリックします。

パフォーマンスログ

パフォーマンスログには、サーバのパフォーマンスに関する情報が含まれます。パフォーマンスログの各レコードには、次の情報が含まれています。

- 基準が記録された日時
- 基準を記録した IWSS サーバ
- 基準名 (HTTP Requests Processed、HTTP Responses Processed、Number of HTTP threads、HTTP CPU Utilization のいずれか)
- 基準の値

パフォーマンスログを表示するには

1. IWSS Web コンソールを開き、メインメニューから [ログ] → [パフォーマンスログ] の順に選択します。
2. ドロップダウンメニューから [期間] を選択します ([すべて]、[今日]、[過去 7 日間]、[過去 30 日間])。

   任意の期間を選択するには、[指定] をクリックし、開始と終了の日付と時間を選択します。

3. [並べ替え基準] で、ログの並べ替えの基準とする項目を選択します。
4. [ログ表示] をクリックします。[パフォーマンスログ] 画面が開きます。
5. 画面を更新するには、[表示更新] をクリックします。

FTP Get ログ

FTP Get ログには、ユーザ ID、日付、FTP 転送元、ファイル名など、FTP Get トランザクションのすべての情報が含まれます。

FTP Get ログを表示するには

1. メインメニューから [ログ] → [FTP Get ログ] の順に選択します。
2. [期間] を選択します ([すべて]、[今日]、[過去 7 日間]、[過去 30 日間])。

   任意の期間を選択するには、[指定] をクリックし、開始と終了の日付と時間を選択します。
3. [並べ替え基準] で、ログの並べ替えの基準とする項目を選択します。
4. [ログ表示] をクリックします。[FTP Get ログ] 画面が開きます。
5. 画面を更新するには、[表示更新] をクリックします。

FTP Put ログ

FTP Put ログには、ユーザ ID、日付、送信者情報、ファイル名など、FTP Put トランザクションのすべての情報が含まれます。

FTP Put ログを表示するには

1. メインメニューから [ログ] → [FTP Put ログ] の順に選択します。
2. [期間] を選択します ([すべて]、[今日]、[過去 7 日間]、[過去 30 日間])。

   任意の期間を選択するには、[指定] をクリックし、開始と終了の日付と時間を選択します。
3. [並べ替え基準] で、ログの並べ替えの基準とする項目を選択します。

4. [ログ表示] をクリックします。[FTP Put ログ] 画面が開きます。
5. 画面を更新するには、[表示更新] をクリックします。

クリーンナップログ

クリーンナップログには、DCS がクライアントコンピュータのクリーンナップを実行した後に返した情報が含まれます。DCS サーバから応答がない場合には、そのクリーンナップ要求に対するエントリはありません。

クリーンナップログを表示するには

1. メインメニューから [ログ] → [クリーンナップログ] の順に選択します。
2. [期間] を選択します ([すべて]、[今日]、[過去 7 日間]、[過去 30 日間])。

   任意の期間を選択するには、[指定] をクリックし、開始と終了の日付と時間を選択します。
3. [検出名] で、不正プログラム名を選択します。

   追加する名前を選択し、[追加] をクリックします。リストにあるウイルスをすべて追加する場合は、[すべて追加] をクリックします。不正プログラム名を右側のリストボックスから削除するには、[削除] をクリックします。リストにあるすべてのウイルスを削除する場合は、[すべて削除] をクリックします。
   状況によっては、IWSS がクリーンナップ要求を送信したときに、DCS がクライアントコンピュータに接続できないことがあります。この場合、不正プログラムはクリーンナップされないため、不正プログラム名でクリーンナップログにクエリを実行しても、情報は何も表示されません。DCS がクライアントコンピュータに正常に接続できなかった場合のクリーンナップ試行に関するログを表示するには、[接続失敗イベントを表示する] チェックボックスをオンにします。
4. [並べ替え基準] で、ログの並べ替えの基準とする項目を選択します。[不正プログラム名]、[日付]、[IP アドレス]、[クリーンナップ結果]、[種類]、[サブタイプ] のオプションがあります。
5. [ログ表示] をクリックします。[クリーンナップログ] 画面が開きます。
6. 画面を更新するには、[表示更新] をクリックします。

ログの削除

テキストログファイルを参照する必要がなくなった場合は、ディレクトリからファイルを削除できます。

注意： 次の手順で、テキストログファイルを削除します。データベース内のログは、手動で削除できません。[ログ] → [設定] 画面で、データベースログの削除の予約を設定します

1 つまたは複数のログを削除するには

1. メインメニューから [ログ] → [削除] の順に選択します。
2. [ウイルスログ]、[URL ブロックログ]、[URL アクセスログ]、および [パフォーマンスログ] の 4 つのタブそれぞれで、削除するログを選択します。
3. [削除] をクリックし、次の画面で [OK] をクリックして削除を確定します。

ログの設定

[ログの設定] 画面から、次の内容を設定できます。

- セキュリティログおよびシステムログのディレクトリ (テキストログファイルのみ)
- システムログを保存する日数
- パフォーマンスデータまたは HTTP/FTP アクセスイベントを収集するかどうか、およびそれぞれのログの間隔
- ログデータベースにログを保存する日数、およびログデータベースのアップデート間隔
- ログをデータベースまたはテキストへのみ書き込むか、またはデータベースとログファイルに書き込むか

注意： セキュリティログのテキストログファイルは自動的には削除できません。[ログ] → [削除] 画面から手動で削除できます。データベースログは手動では削除できません。[ログ] → [設定] 画面で削除スケジュールを設定できます。

ログファイルのフォルダの場所

セキュリティログおよびシステムログ用のフォルダを設定できます。初期設定は、/etc/iscan/log です。ログファイルの保存先としてフォルダを設定するには、フォルダがすでに IWSS サーバ上に存在し、アクセス許可があることが必要です。フォルダのパスを入力すると IWSS でチェックされ、フォルダにアクセスできない場合はエラーメッセージが表示されます。

セキュリティログのディレクトリを設定するには

1. メインメニューから [ログ] → [設定] → [セキュリティログ] の順に選択します。
2. 該当するテキストボックスに、ログファイルの保存先フォルダの場所を入力します。
3. [保存] をクリックします。

システムログのディレクトリを設定するには

1. [ログ] → [設定] → [システムログ] の順に選択します。
2. 該当するテキストボックスに、ログファイルの保存先フォルダの場所を入力します。
3. [保存] をクリックします。

ログのその他のオプション

IWSS でイベントをログに記録する方法を制御する設定は、他にもいくつかあります。これらは [ログの設定] 画面で設定できます。

システムログ

[システムログ] タブで、システムログを自動的に削除するまで保存する日数を設定します。初期設定は 5 日間です。

セキュリティログ

[セキュリティログ] タブで、パフォーマンスデータを収集し、HTTP/FTP アクセスイベントのログを記録するように IWSS を設定できます。これらの設定を有効にする場合は、ログの間隔を設定します。

データベースにログが記録される期間は、初期設定では 30 日間です。実際の環境のニーズに合わせてカスタマイズします。さらに、データベースが新しいログでアップデートされる間隔も設定します。初期設定は 30 秒間です。

ログファイルの命名規則

初期設定では、ログファイルは /etc/iscan/log ディレクトリに書き込まれます。IWSS には、ログファイルに名前を付ける際の標準的な命名規則があります。たとえば、ウイルスログは次のような名前で作成されます。

virus.log.2007.01.09

これは、2007 年 1 月 9 日に作成されたウイルスログという意味です。

各ログの命名規則は次のとおりです。

表 14-2. ログファイルの命名規則

ウイルスログ	virus.log.yyyy.mm.dd
URL ブロック	url_blocking.log.yyyy.mm.dd.0001

表 14-2. ログファイルの命名規則

パフォーマンスログ	perf.log.yyyy.mm.dd
URL アクセスログ	access.log.yyyy.mm.dd.0001
FTP ログ	ftp.log.yyyymmdd.0001
HTTP ログ	http.log.yyyymmdd.0001
メール配信ログ	mail.log.yyyymmdd.0001
アップデートログ	update.log.yyyymmdd.0001
予約アップデートログ	admin.log.yyyymmdd.0001
一時 Control Manager ログ	CM.yyyymmdd.0001
Java アプレット検索ログ	jscan.log.yyyymmdd.0001
監査ログ	audit.trail.log
データベースインポートツールログ	log_to_db.log.yyyymmdd.0001
ワールドウイルストラッキングセンターログ	logtowvts.log.yyyymmdd.0001

注意： ログを削除しても、該当するデータが IWSS Web コンソールに表示されなくなるわけではありません。IWSS でデータが表示されないようにするには、該当するデータを対応データベーステーブルから削除する必要があります。

表 14-3. IWSS のログ / レポートの主なデータベーステーブル

テーブル名	列の例
tb_url_usage	username、url、path
tb_report_by	period、category、entity_type、entity_name
tb_violation	username、url、file_name、action、blocked_by、category
tb_performance_value	server、date_field、metric_value、metric_id

CSV 形式でのログおよびレポートデータの出力

IWSS では、ログまたはリアルタイムレポートを表示したときに、CSV 形式でファイルにデータを出力できます。出力した CSV 形式のファイルは、他のアプリケーションで表示および分析できます。ログまたはリアルタイムレポートの画面上で [CSV 形式で出力] をクリックすると、IWSS サーバからデータが CSV 形式でダウンロードされます。

IWSS でデータを CSV ファイルで出力する際の文字エンコード形式は、intscan.ini ファイルの [Common] にある csvcharformat パラメータで設定できます。初期設定は Shift JIS です。

ファイルタイプと MIME コンテントタイプの対応

次の表は、対応する MIME コンテントタイプをブロックするために、HTTP および FTP のウイルス検索ポリシーの [その他] フィールドに入力できるファイルタイプを示しています。たとえば、afc と入力すると、audio/aiff と audio/x-aiff の両方の MIME コンテントタイプがブロックされます。

ファイルタイプ	MIME コンテントタイプ	ファイルタイプ	MIME コンテントタイプ	ファイルタイプ	MIME コンテントタイプ
afc	audio/aiff	avs	video/avs-video	bin	application/x-binary
afc	audio/x-aiff	audiovideo	video/	binhex	application/binhex
ani	application/octet-stream	base64	application/base64	binhex	application/binhex4
arc	application/octet-stream	bin	application/mac-binary	binhex	application/mac-binhex
arj	application/octet-stream	bin	application/macbinary	binhex	application/mac-binhex40
asf	video/x-ms-asf	bin	application/octet-stream	binhex	application/x-binhex40
bin	application/x-macbinary	bmp	image/bmp	bmp	image/x-windows-bmp
bw	image/x-sgi-bw	bzip2	application/x-bzi2	cgm	image/cgm

ファイルタイプ	MIMEコンテントタイプ	ファイルタイプ	MIMEコンテントタイプ	ファイルタイプ	MIMEコンテントタイプ
cmx	application/x-cmx	cmx	image/x-cmx	com	application/octet-stream
core	application/octet-stream	cpio	application/x-cpio	dcr	application/x-director
doc	application/wordperfect	dwg	application/acad	dwg	application/x-acad
dwg	drawing/x-dwg	dwg	image/vnd.dwg	dwg	image/x-dwg
eps	application/postscript	eps	image/x-eps	exec	application/octet-stream
exec	application/x-msdownload	exe	application/octet-stream	fh9	image/x-freehand
fli	video/x-fli	fm	application/vnd.framemaker	gif	image/gif
gzip	application/x-gzip	gzip	encoding/x-gzip	hpexe	application/octet-stream
iff	audio/x-aiff	java	text/x-java-source	java	application/java-class
java	application/x-java-applet	java	application/x-java-vm	java	text/x-java-source
java	application/java-class	java	application/x-java-applet	java	application/x-java-vm
jpeg	image/jpeg	jpeg	image/pjpeg	lha	application/x-lha
lisp	application/x-lisp	maud	audio/x-maud	midi	audio/midi
mif	application/x-mif	mng	video/x-mng	mp3	audio/mpeg
mp3	audio/mpeg3	mp3	audio/x-mpeg-3	mp3	video/mpeg

ファイル タイプ	MIME コンテント タイプ	ファイル タイプ	MIME コンテント タイプ	ファイル タイプ	MIME コンテント タイプ
mp3	video/x-mpeg	mpeg	video/mpeg	mscab	application/ x-cainet-win32-x86
msdoc	application/ msword	msexl	application/ excel	msexl	application/ x-msexcel
msexl	application/ x-excel	msexl	application/ vnd.ms-excel	msmdb	application/ x-msaccess
msppt	application/ mspowerpoint	msppt	application/ powerpoint	msppt	application/ vnd.ms-powerpoint
msproj	application/ vnd.ms-project	msproj	application/ x-msproject	msproj	application/ x-project
mswri	application/ mswrite	pcx	image/x-pcx	pdb	application/ x-pilot-pdb
pdf	application/ pdf	pdf	application/ x-pdf	pfb	application/ x-font
pict	image/pict	pict	image/x-pict	picture	image/
png	image/png	ppm	image/ x-portable-pixmap	ps	application/ postscript
psd	application/ octet-stream	qtm	video/quicktime	ra	audio/ vnd.rn-realaudio
ra	audio/ x-pn-realaudio	ra	audio/ x-realaudio	rar	application/ rar
ras	image/ x-cmu-raster	ras	image/ cmu-raster	risc	application/ octet-stream
rmf	application/ vnd.rn-realmedia, g_audiovideo	rtf	application/rtf	rtf	application/ x-rtf

ファイルタイプ	MIMEコンテントタイプ	ファイルタイプ	MIMEコンテントタイプ	ファイルタイプ	MIMEコンテントタイプ
rtf	text/richtext	scm	application/vnd.lotus-screencam	scm	application/x-lotusscreencam
scm	application/x-screencam	scm	video/x-scm	sf	audio/x-sf
swf	application/x-shockwave-flash	tar	application/x-tar	tga	image/tga
tiff	image/tiff	tnef	application/ms-tnef	tnef	application/vnd.mstnef
txt	text/plain	uuencode	text/x-uuencode	zip	application/zip
voc	audio/voc	voc	audio/x-voc	wav	audio/wav
wbc	application/x-webshots	wmf	application/x-msmetafile	wmf	image/x-wmf

設定ファイル

設定ファイルには、メイン、プロトコルモジュール、検索モジュール用の 3 種類があります。すべての設定ファイルは {IWSS root} ディレクトリにあります。{IWSS root} の初期設定は /etc/iscan/ です。メインの設定ファイルは、intscan.ini です。

- ウイルス検索固有の設定は、次のファイルにあります。

  {IWSS root}/IWSSPIScanVsapi.dsc

- ICAP プロトコル固有の設定は、次のファイルにあります。

  {IWSS root}/IWSSPIProtocolIcap.pni

- スタンドアロンプロキシ固有の設定は、次のファイルにあります。

  {IWSS root}/IWSSPIProtocolHttpProxy.pni

- URL フィルタ検索モジュールの設定は、次のファイルにあります。

  {IWSS root}/IWSSPIUrlFilter.dsc

- レポート固有の設定は、次のファイルにあります。

  {IWSS root}/report.ini

- URL 分類データベースの設定は、次のファイルにあります。

  {IWSS root}/urlfcIFX.ini

- 初期設定の URL カテゴリと、そのマッピング情報の設定は、次のファイルにあります。

  {IWSS root}/urlfcMapping.ini

- IP アドレスと、Trend Micro InterScan Web Security Suite (以下、IWSS) サーバにアクセスできるすべてのコンピュータの IP アドレスおよび IP の範囲のリストの設定は、次のファイルにあります。

  {IWSS root}/ClientACL_http.ini および {IWSS root}/ClientACL_ftp.ini

- IWSS で HTTP および FTP 要求を転送するポートを定義するルールの設定は、次のファイルにあります。

  {IWSS root}/HttpPortPermission_http.ini および {IWSS root}/HttpPortPermission_ftp.ini

- IWSS で HTTPS トンネリングを許可するポートを定義するルールの設定は、次のファイルにあります。

  {IWSS root}/HttpsConnectACL_http.ini

- 信頼されるサーバの IP アドレスと IP の範囲のリストの設定は、次のファイルにあります。

  {IWSS root}/ServerIPWhiteList_http.ini および {IWSS root}/ServerIPWhiteList_ftp.ini

IWSS 管理コンソールは、インストールされているモジュールによって異なります。これまで旧バージョンの IWSS を使用していた場合は、IWSS には新しい .ini ファイルエントリを必要とする多数の新機能が用意されています。

プロトコルハンドラ

承認されたいくつかの伝送プロトコルでメッセージの解釈および処理を担う機能は、プロトコルハンドラと呼ばれるダイナミックライブラリでカプセル化されます。IWSS では、ICAP プロトコルハンドラか、HTTP プロキシハンドラのどちらかを選択できます。ICAP プロトコルハンドラは、IWSS を ICAP サーバとして動作させることができ、HTTP プロキシハンドラでは、IWSS が直接 HTTP プロキシサーバのように動作します。アプリケーションバイナリは、プロトコルハンドラから独立しており、設定を変更すれば同じアプリケーションで別のプロトコルをサポートできます。

プロトコルのアクティブな設定ファイルの完全なパスを、intscan.ini ファイルの [main] セクションにある「protocol_config_path」パラメータに入力します。

プロトコルハンドラには、固有の設定ファイルが必要です。このファイルには、そのプロトコルのみに関連するエントリが含まれます。これらのプロトコル設定ファイルは、ファイル名の「.pni」という拡張子で示されます。

検索モジュール

トラフィックの検索機能は、検索モジュールとして知られるダイナミックライブラリを使用して提供されます。IWSS で使用できる最初の検索モジュールは、検索エンジンを使用するコンテンツ検索を提供します。

各検索モジュールには、拡張子 .dsc を持つ設定ファイルがあります。IWSS アプリケーションは、intscan.ini ファイルの [scan] セクションにある「plugin_dir」パラメータに示されるディレクトリで .dsc ファイルを探すことにより、使用可能な検索モジュールを検出します。

OpenLDAP

OpenLDAP は Kerberos 認証をサポートしますが、Kerberos 認証のサポートを有効にするパッケージは初期設定ではインストールされません。IWSS で OpenLDAP を使用する場合、Kerberos 認証を有効にする必要があります。本付録では、OpenLDAP での Kerberos サポートのインストールおよび設定方法について説明します。さらに本付録では、ユーザ / グループ認証方法を使用する際に、Trend Micro InterScan Web Security Suite (以下、IWSS) が OpenLDAP ディレクトリを照会できるように OpenLDAP ディレクトリをセットアップする方法についても説明します。

本章で説明する内容には、次の項目が含まれます。

- IWSS で OpenLDAP を使用する際に Kerberos 認証を有効にするための、テストされたソフトウェアパッケージ
- OpenLDAP 設定ファイルの変更
- LDIF 形式でのユーザおよびグループのサンプルエントリ

OpenLDAP サーバ側の設定

ソフトウェアパッケージの従属関係

次のソフトウェアパッケージは、IWSS 3.1 と互換性があります。

- cyrus-sasl-2.1.19
- db-4.2.52.NC
- heimdal-0.6.2
- openldap-2.2.17
- openssl-0.9.7d

設定ファイル

OpenLDAP を IWSS で使用するには、次の設定ファイルを変更する必要があります。

/etc/openldap/ldap.conf

/etc/openldap/slapd.conf

ldap.conf のサンプル

```
#
# System-wide ldap configuration files. See ldap.conf(5) for
# details
# This file should be world readable but not world writable.



# OpenLDAP supports the ldap.conf file. You could use this file to
# specify a number of defaults for OpenLDAP clients. Normally this
# file can be found under /etc/openldap based on /etc/init.d/ldap
# start script's setting

# Set host IP address or fully qualified domain name

HOST example.peter.com
#HOST 10.2.1.1

# Set the default BASE DN where LDAP search will start off

BASE dc=peter,dc=com

# Set the default URI

URI   ldap://example.peter.com

# SASL options
# specify the sasl mechanism to use. This is a user-only option.
# SASL_MECH <mechanism>
# specify the realm. This is a user-only option
# SASL_REALM <realm>
# specify the authentication identity.
# SASL_AUTHCID <authcid>
```

slapd.conf のサンプル

```
#
# See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
#
# Enforce all changes to follow the defined schemas loaded via
# include statements in the conf file


# NOTE 1
# All the OpenLDAP config files and backend databases are accessed
# and created by "ldap", so if you touch these config files by
# "root", "a Permission Denied" error will occur. Please modify
# ownership accordingly.

# NOTE 2
# krb5-kdc.schema fails to work with current OpenLDAP 2.2.x distro
# krb5ValidStart, krb5ValidEnd, krb5PasswordEnd need to have
# "EQUALITY generalizedTimeMatch" inserted before the ORDERING
# statement.
# www.openldap.org/lists/openldap-bugs/200309/msg00029.html

# Enforce all changes to follow the defined schemas loaded via
# include statements in the conf file

schemacheck on

# Included schemas

include /usr/local/etc/openldap/schema/core.schema
include /usr/local/etc/openldap/schema/krb5-kdc.schema
include /usr/local/etc/openldap/schema/cosine.schema
include /usr/local/etc/openldap/schema/inetorgperson.schema
include /usr/local/etc/openldap/schema/nis.schema
include /usr/local/etc/openldap/schema/java.schema

# Do not enable referrals since IWSS 2.5 has its own implementation
# referral ldap://root.openldap.org

# Directives say where to write out slapd's PID and arguments
# started with

pidfile /usr/local/var/run/slapd.pid
argsfile /usr/local/var/run/slapd.args

# Load dynamic backend modules:
# modulepath/usr/local/libexec/openldap
# moduleloadback_bdb.la
```

```
# moduleloadback_ldap.la
# moduleloadback_ldbm.la
# moduleloadback_passwd.la
# moduleloadback_shell.la

# Sample security restrictions
#Require integrity protection (prevent hijacking)
#Require 112-bit (3DES or better) encryption for updates
#Require 63-bit encryption for simple bind
# security ssf=1 update_ssf=112 simple_bind=64

# Sample access control policy:
#Root DSE: allow anyone to read it
#Subschema (sub)entry DSE:allow anyone to read it
#Other DSEs:
#Allow self write access
#Allow authenticated users read access
#Allow anonymous users to authenticate
#Directives needed to implement policy:
# access to dn.base="" by * read
# access to dn.base="cn=Subschema" by * read
# access to *
#by self write
#by users read
#by anonymous auth
#
# if no access controls are present, the default policy
# allows anyone and everyone to read anything but restricts
# updates to rootdn.(e.g., "access to * by * read")
#
# rootdn can always read and write EVERYTHING!
access to dn.base="" by * read
access to dn.base="cn=Subschema" by * read
access to *
by self write
by users read
by anonymous auth
by * none

# We have found this gives a useful amount of information about
# directory

loglevel 256

#Specify the number of threads used in slapd, default = 16
#Increasing or decreasing the number of threads used can
#drastically affect performance, we found 20 threads to be optimal
#for our setup, but it can be different under other operating
#systems

threads 20
```

```
#Tell slapd to close connections that have been idle for 30 seconds
#or more

idletimeout 30

# Enable LDAPv2 support. This option is disabled by default.

allow bind_v2

# Disable anonymous bind

disallow bind_anon

# Comment this section to enable simple bind

#disallow bind_simple

# NOTE 3
# SASL Configuration
# Caution: make sure you use the canonical name of the machine
# in sasl-host. Otherwise, OpenLDAP wont be able to offer GSSAPI
# authentication

# Set the SASL realm and canonical name of the host
sasl_hostexample.peter.com
sasl_realmPETER.COM

# Allow proxy authentication if it's configured

sasl-authz-policyboth

# NOTE 4
# Mapping of SASL authentication identities to LDAP entries
# The sasl-regexp line are particularly critical. They are what
# rewrite incoming connections who have SASL formatted DNs to the
# DNs that are in the directory DB. It's important to remember that
# they are processed in order, so you want to write them from most
# specific to most general

# NOTE 5
# We set the cn=.* since we are going to adopt different security
# mechanisms. If Kerberos v5 is the only one used, change wildcard
# to cn=GSSAPI,cn=auth

#sasl-regexp uid=(.*),cn=GSSAPI,cn=auth
#uid=$1,ou=people,dc=peter,dc=com

sasl-regexp uid=(.*),cn=.*,cn=auth
```

```
uid=$1,ou=people,dc=peter,dc=com

# ldbm database definitions

# NOTE 6
# Correctly configuring the backend Berkeley DB is very critical
# follow the guideline at
# http://www.openldap.org/faq/data/cache/1073.html

# Cleartext passwords, especially for the rootdn, should
# be avoided. See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.

databasebdb

# These options specify a DN and passwd that can be used to
# authenticate as the super-user entry of the database. The DN and
# password specified here will always work, regardless of whether
# the entry named actually exists or has the password given.
# This solves the chicken-and-egg problem of how to authenticate and
# add entries before any entries yet exist

suffix"dc=peter,dc=com"
rootdn"cn=admin,dc=peter,dc=com"
rootpwadmin

# NOTE 7
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd/tools. Mode 700
# recommended.

directory/usr/local/var/openldap-data

#Tell the slapd to store the 10000 most accessed entries in memory
#Having a properly configured cache size can drastically affect
#performance

cachesize 10000

# Indices to maintain
# Some versions of OpenLDAP don't support the index of uniqueMember
# "pres" indexing allows you to see a filter that asks if the
# attribute is present in an entry
# "eq" indexing allows to ask if an attribute has an exact value
# "apporx" indexing allows to ask if an attribute value sounds like
# something
#  This option is tied to --enable-phonetic compile option in
# OpenLDAP
# "sub" indexing allows to do substring search on an attribute's
```

```
# values

index default eq,pres
index objectclass   eq,pres
index cn,sn,givenname,mail   eq,pres,approx,sub
index uideq,pres
index uidNumber,gidNumber,memberUid   eq,pres
```

ツール

- 既存の LDIF ファイルをインポートすることにより、サーバデータベースおよび付随するインデックスを作成します。

名前

slapadd — SLAPD データベースにエントリを追加します。

概要

```
/usr/sbin/slapadd  [-v]  [-c]  [-d  level] [-b suffix] [-n dbnum]
[-f slapd.conf] [-l ldif-file]
```

説明

LDAP Directory Interchange Format (LDIF) で指定されたエントリを slapd データベースに追加します。

- サーバデータベースを LDIF ファイルに出力します。現在のデータベースについて、参照しやすい形式でのバックアップを作成する際に役立ちます。

名前

slapcat — SLAPD データベースからの LDIF ユーティリティ。

概要

```
/usr/sbin/slapcat  [-v]  [-c]  [-d  level] [-b suffix] [-n dbnum]
[-f slapd.conf] [-l ldif-file]
```

説明

slapd データベースの内容を基に、LDAP Directory Interchange Format (LDIF) 出力を生成します。

- 現在のデータベースの内容を基に、すべてのインデックスを再構築します。

名前

slapindex — SLAPD インデックスからの LDIF ユーティリティ。

概要

```
/usr/sbin/slapcat [-v] [-c] [-d level] [-b suffix] [-n dbnum]
[-f slapd.conf]
```

説明

データベースの現在の内容を基に、slapd インデックスを再生成します。

- slapd.conf の設定を確認します。

名前

Slaptest — slapd.conf ファイルの適合性を確認します。

概要

```
/usr/sbin/slaptest [-v] [-d level] [-f slapd.conf]
```

説明

slapd.conf 設定ファイルの適合性を確認します。slapd.conf 設定ファイルを開き、ファイルの内容を一般的なルールおよびバックエンド固有のルールに従って解析して、適合性を確認します。

- LDAP クエリユーティリティ

名前

ldapsearch — LDAP の検索ツール。

概要

```
ldapsearch [-D binddn] [-W] [-w bindpasswd] [-H ldapuri] [-h
ldaphost] [-p ldap- port] [-b searchbase] [-s base|one|sub] [-x]
[-Y mech] [-Z[Z]] filter [attrs...]
```

説明

LDAP サーバへの接続を開き、バインドを実行して、指定されたパラメータを使用して検索を実行します。

例

次のコマンドは、「uid=petery」と一致するエントリに対し、単純な平文認証を使用してクエリを実行し、一致したエントリのメール属性を LDAP サーバが返すように要求します。

```
ldapsearch -x -D "cn=admin,dc=peter,dc=com" -w admin -b
"dc=peter,dc=com" -s sub "uid=petery" mail
```

詳細については、OpenLDAP のドキュメントを参照してください。

SASL/OpenLDAP/Kerberos v5 の認証を確認するには

```
1. KRB5_CONFIG="/etc/heimdal/krb5.conf" ./ldapsearch -v -x ¥

-D "cn=admin,dc=peter,dc=com" -W -b "" -s base -LLL ¥

-H ldap://example.peter.com/ supportedSASLMechanisms

2. KRB5_CONFIG="/etc/heimdal/krb5.conf" ./ldapsearch -b
"dc=peter,dc=com" ¥

-H ldap://example.peter.com/

3. KRB5_CONFIG="/etc/heimdal/krb5.conf" ./ldapwhoami -H
ldap://example.peter.com
```

カスタマイズされた属性の等価テーブル設定

IWSS で OpenLDAP または Sun Java System Directory Server 5.2 (旧 Sun ONE Directory Server) のディレクトリを使用するよう設定する場合は、ユーザグループの関連付けをいくつか設定できます。

図 C-1.　OpenLDAP の属性マッピング設定画面

[組織グループ] には、LDAP グループオブジェクトを検索する際に LDAP 検索フィルタの一部として使用するオブジェクトクラスを指定します。[組織ユーザ] には、ユーザオブジェクトの検索フィルタの一部として使用するオブジェクトクラスを示します。LDAP ではエントリがグループ固有のものであるかユーザ固有のものであるかを区別できないため、IWSS でクエリを実行するためにはこの「タグ」が必要です。

[組織メンバー所属先] には、エントリ、ユーザ、またはグループのグループメンバーシップを定義します。一方、ユーザは最も小さいエンティティであり、メンバーを含めることができないため、[組織メンバー] にはグループエントリのメンバーを指定します。属性名はこの等価テーブルの最初の列にあり、関連する情報を含む属性を示します。初期設定の属性は、標準 OpenLDAP スキーマの「ou」および「uniquemember」です。

属性の構文は等価テーブルの 2 番目の列にあり、IWSS で LDAP サーバのグループまたはメンバーのエントリを関連付けたり検索するための属性を定義します。IWSS には、この設定、すなわち {[一般名 (CN)]、[識別名 (DN)]、[カスタム属性]} を設定するオプションが 3 つあります。

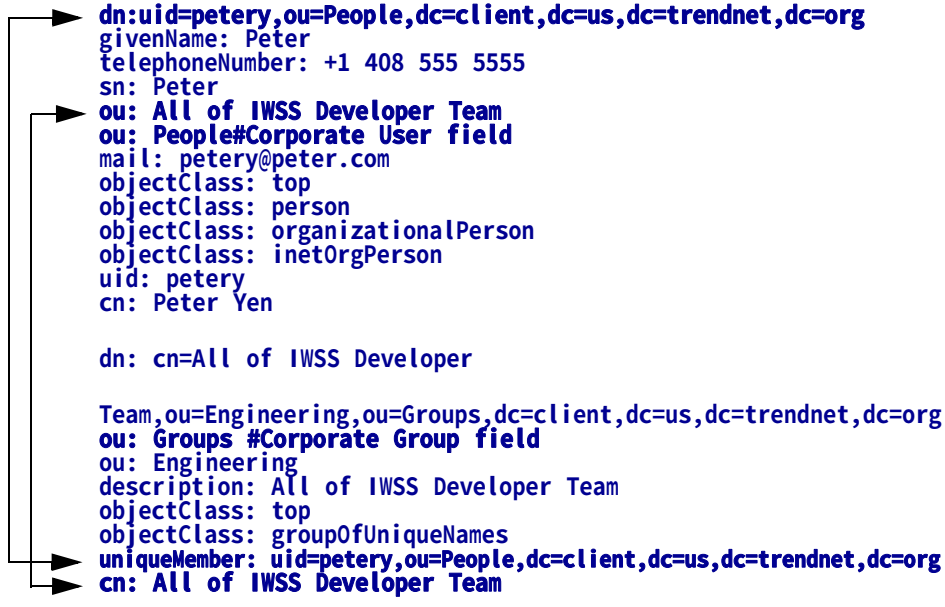
例として、次の単純な LDIF ファイルを考えます。以下のことに留意してください。

- LDIF は、LDAP ディレクトリのデータを人間が読み取り可能な形式で表す方法です。
- 例を分かりやすくするため、一部のエントリを削除してあります。
- OpenLDAP サーバの LDIF ファイルを出力するには、slapcat を実行します。slapcat は通常、OpenLDAP のインストールパスまたは /usr/local/sbin にあります。

```
slapcat l [output_file_name]
```

LDIF 形式のサンプルエントリ

次の例は、LDIF 形式でのユーザおよびグループのエントリを単純化したものです。



```
dn:uid=petery,ou=People,dc=client,dc=us,dc=trendnet,dc=org
givenName: Peter
telephoneNumber: +1 408 555 5555
sn: Peter
ou: All of IWSS Developer Team
ou: People#Corporate User field
mail: petery@peter.com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: petery
cn: Peter Yen

dn: cn=All of IWSS Developer

Team,ou=Engineering,ou=Groups,dc=client,dc=us,dc=trendnet,dc=org
ou: Groups #Corporate Group field
ou: Engineering
description: All of IWSS Developer Team
objectClass: top
objectClass: groupOfUniqueNames
uniqueMember: uid=petery,ou=People,dc=client,dc=us,dc=trendnet,dc=org
cn: All of IWSS Developer Team
```

次のことに注意してください。

- グループエントリの uniqueMember 属性で組織メンバー (ユーザエントリ) の [識別名 (DN)] を関連付けます。
- ユーザエントリの [組織メンバー所属先] 属性で組織メンバー所属先 (グループエントリ) の [一般名 (CN)] を関連付けます。

設定のサンプル

次の LDAP 属性マッピングを考えます。

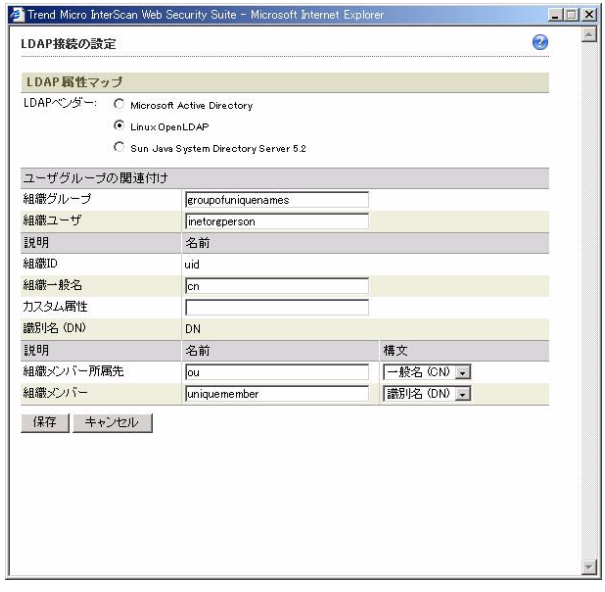
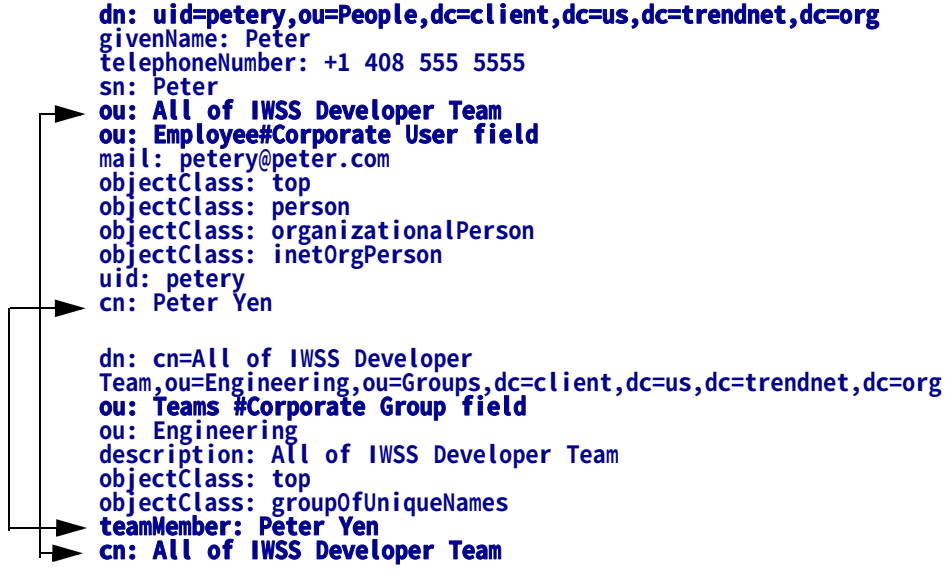


図 C-2.　OpenLDAP の属性マッピング設定画面



次のことに注意してください。

1. グループエントリの uniqueMember 属性で組織メンバー (ユーザエントリ) の [識別名 (DN)] を関連付けます。
2. ユーザエントリの [組織メンバー所属先] 属性で組織メンバー所属先 (グループエントリ) の [一般名 (CN)] を関連付けます。

索引

英数字

ActiveX オブジェクト
署名確認 84、136
対策ルール 132
Control Manager 24、195
CSV 29
cyrus-sasl-2.1.19 246
DCS 39、40
EICAR テストファイル 55
ESMTP 199
FTP
サービスのオン / オフ 168
セキュリティ上の脅威 23
匿名 182
プロキシ 96
ポート制限 174
FTP Get ログ 230
FTP get ログ 230
FTP Put ログ 230
FTP put ログ 230
FTP アクセス管理
設定 172
FTP 検索 29
圧縮ファイル 89、171
オプション 168
隔離 89
許可されたサーバ IP のリスト 173
検索するファイル 98
検索方向 97、169
サイズの大きいファイル 89
設定 168、169、170
注意 95
通知 205
ファイルのブロック 97
プロキシ設定 96
有効化 169
優先順位 169
FTP 設定 168
heimdal-0.6.2 246
HTTP
検索するファイルタイプ 116
サービスのオン / オフ 178
セキュリティ脅威 18、46
プロキシ設定 53
ブロックするファイルタイプ 115
HTTPS
Web コンソール 189、190
検索 182
HTTP 検索 81
圧縮ファイル 118
イントラネットサイト 157
隔離 122
検索イベント 124
検索処理 123
検索するファイル 116
サイズの大きいファイル 119
進行ステータス画面 53
信頼する URL 157
セキュリティ設定 118

遅延検索 120、121
通知 203
配信前に検索 120
パフォーマンス 110
ファイルの除外 81
ファイルのブロック 115
ポリシーの作成 / 変更 110
優先順位 117
HTTP トラフィックフロー
オン / オフ 54
ICAP 26
設置後の作業 194
ICAP プロキシの設定 184
ICSA 認定 37
IntelliTunnel 19
ポリシーの作成 153
Internet Caching Acceleration Protocol ICAP を参照
iscan_web_protocol 191
iscan_web_server 191
IWSS
ウイルスを検出する仕組み 23
主な機能 27
機能 27
コンポーネント 41
サービス 41
テスト 55、191
モジュール 41
予約タスク 42
利点 23
IWSSPIUrlFilter.dsc 149
Java アプレット
計測処理 85
計測処理設定 128
署名確認 85
署名ステータス 127
対策ルール 127
リアルタイムの監視 86
Kerberos 245
LDAP 24
AD Global カタログ 80
サポートしているディレクトリ 75、102
参照サーバ 106
参照サーバに対するマッチング 79
接続のテスト 107
設定 104
属性名 104
通信フロー 76
認証 71、73、75、77、103
ldapsearch 253
LDIF ファイル 256
lpt$vpn.xyz 61
MIME タイプ 81、117、237
ODBC 187
OpenLDAP 245
ldap.conf のサンプル 247
slapd.conf のサンプル 248
属性の等価 255
ソフトウェアの互換性 246
openldap-2.2.17 246
openssl-0.9.7d 246
Readme 14
RealAudio 117

register_user_agent_header.exe 102
slapadd 252
slapcat 252
slapd.conf 248
slapindex 253
slaptest 253
SNMP 21、29、209
SolutionBank - 製品 Q&A Web サイトを参照 14
Tomcat 189
  HTTP 190
Trend Micro Control Manager 195
TrendLabs 26
uniquemember 255
URL
  検索エンジンのバージョン 37
  製品 Q&A 14
URLFilteringExceptions.ini 149
URL アクセス 28、157
  ログ 228
URL アクセス管理 157
  注意 93
URL アクセスログ 228
URL の信頼 28
URL フィルタ 27
  URL カテゴリの見直し 148
  概要 144
  カスタマイズ 87
  カテゴリ 20
  カテゴリの管理 147
  時間設定 151
  仕組み 88
  除外設定 149
  除外設定のインポート 150
  スケジュール 151
  設定 147
  注意 87
  ポリシーの概要 144
  ポリシーの管理 144
  ポリシーの作成 145
  有効化 144
  ルール 227
URL フィルタログ 226
URL ブロック 28、159
  インポート 162
  通知 204
  パターンファイルによる規制 163
  フィッシング対策 164
  リストのインポート 163
  ルール 227
  ワイルドカード 162
Web コンソール 48
  パスワード 188
Web レピュテーション 18

あ

アーキテクチャ 41
あいさつの受信 172
アクセス管理
  FTP 172
アクセスログ 223
  上位プロキシ 223
アクセス割り当て 28

概要 92
管理 156
ゲストポリシー 92
ダウンロード中の超過 92
追加 156
アクセス割り当てポリシー 156
アクティブ FTP 97
圧縮ファイル 171
処理 118
セキュリティ設定 118
圧縮ファイルの処理 89
アップデート 32、54
強制 59
コンポーネント 31、37
差分 34
差分アップデート 34
手動 59
成否の確認 61
操作方法 61
通知 61、207
プロキシ設定 58
予約 60
予約アップデートの無効化 60
ロールバック 61
宛先ポート (FTP) 175
アプレット /ActiveX
ポリシー設定 132
アプレット /ActiveX 対策 23、27
仕組み 84
スレッドグループ 131
設定 132
注意 83
通知 140
デジタル証明書 137
ポリシーの追加、変更 126
有効化 126
アプレットおよび ActiveX 対策
通知 206
暗号化 189
依存モード 179
ウイルス
感染報告のあるウイルス 36
処理 123
通知 150
出回っていないウイルス 36
パターンファイルの提供 33
ウイルス検索 27
処理 172
設定 178
ウイルスシグネチャ
ウイルスパターンファイルを参照
ウイルスパターンファイル 32
ウイルス流布サイト 164
ウイルスログ 225
オンラインヘルプ 14

か

隔離ディレクトリ 186
隔離ファイル
暗号化 89
監査ログ 224
カンマ区切り値 (CSV) 29

キャッシュ
  生存期限 187
  ポリシー設定 187
キャッシュサーバ 26
  Cisco 24
  Network Appliance 24
  消去 60
キャッシュ生存期限 92
キャッシュ生存期限 (TTL) 74、78、92、187
脅威 23
強制アップデート 61
業務時間 88
クリーンナップログ 231
グローバルポリシー 66
計測処理 85
ゲストアカウント 183
ゲストポリシー 66
  概要 66
ゲスト用ポート
  有効化 107
検索
  ファイルタイプの選択 116
  モジュール 243
検索エンジン 31、36
  ICSA 認定 37
  アップデート 36、37
  アップデートを開始するイベント 37
  最新バージョンを確認するための URL 37
誤警告 61

さ

サーバファーム 194
サイズの大きいファイルの処理
  HTTP 119
  重要な注意 121
  遅延検索 120
差分パターンファイルアップデート 34
システム
  ログディレクトリの設定 233
実際のファイルタイプ 38
使用開始 46
初期設定 49
署名ステータス
  証明書失効リスト (CRL) 134
  信頼されない 134
進行ステータス画面 120
信頼する URL 157
  インポート 158
  管理 158
スパイウェア 25、164
  検索ルール 122
  定義 35
  レポート 29
スパイウェア対策 25
スパイウェアログ 225
製品 Q&A 14
  URL 14
セキュリティ上の脅威の概要 23
設定ファイル 241
その他の脅威
  定義 35

た

待機ポート 181、191
大規模感染予防ポリシー (OPP) 226
ID 227
定義ルール 227
対象読者 15
通知 29、172
ESMTP のサポート 199
HTML タグの使用 202
SNMP 209
概要 198
管理者とユーザ 198
設定 202
変数 199
変数の使用 199
通知の変数 199
データベース
接続設定 186
接続の設定 186
接続のテスト 187
ログファイル 223
デジタル証明書
管理 137
透過 180
同時接続数 183
ドキュメント 14
匿名 FTP 182
トレンドマイクロ ダメージクリーンナップサービス (DCS) 39、40
トレンドマイクロの推奨設定 38

は

はじめに 13
パスワード 188
作成のヒント 188
パターンファイル 31
サーバ上に複数 33
削除 62
手動で削除 62
スパイウェア 34
番号 33、34
パターンマッチング 33
パッシブ FTP 97
パフォーマンスログ 229
ファイルタイプ 38
指定 (FTP) 98
ブロック 115
フィッシング 163、164
URL 165
フィッシング対策 34
URL の送信 165
概要 164
カテゴリ 164
定義ルール 227
取り込み条件 163
ブロック 164
利点 163
負荷の処理 183
複合型脅威 23
複数インストール 30
複数サーバ 194
不正サイト 164

フラグ付きの証明書 128
プロキシ
キャッシュ 179
上位プロキシあり (依存モード) 179
スタンドアロンモード 178
設定 58、178、181
待機ポート 181
リバース 21、180
プロキシ設定 178
プロトコルハンドラ 243
変数 199
通知での使用 200
ポリシー
仕組み 64
実用例 64
初期設定 66
配信 67

ま

マクロ検索 124
処理 123

や

ユーザ / グループ名による識別 (LDAP) 183
ユーザ ID 227
ユーザ識別方法 28、99
IP アドレス 68、100
クライアント登録ユーティリティ 102
種類 67
設定 67、100
ホスト名 68、100
ユーザ / グループ名 70、102
予約タスク 42

ら

利点 23
リバースプロキシ 180
DNS の変更 181
設定 180
ルート証明書 133
レジストレーションキー 192
レポート 21、29
概要 212
カスタマイズ 220
グラフの種類 215
種類 212
使用可能 217
設定 215、216
総合と個別 215
トラフィック 214
日次 219
範囲の設定 215
ブロックイベント 213
保存 220
予約 219
予約の削除 220
リアルタイム 216
ログの設定 233
ロールバック 61
ログ 21、29
CSV ファイルとしてエクスポート 236
FTP get 230

FTP put 230
URL アクセス 228
URL フィルタ 226
ウイルス 225
概要 222
監査 224
クエリ / 表示 224
クリーンナップ 231
削除 231、232
システム 222
スパイウェア 225
設定 232
パフォーマンス 229
ファイルの命名規則 234
フォルダ 233
レポート 222
ログとレポート 21
ログファイル
FTP Get ログ 230
FTP Put ログ 230
URL ブロックログ 225
ウイルスログ 235
命名規則 234

わ

ワイルドカード 162