



InterScan Web Security Suite™ 6.5 Linux版 Patch 3

管理者ガイド

注意事項

複数年契約について

- お客さまが複数年契約（複数年分のサポート費用前払い）された場合でも、各製品のサポート期間については、当該契約期間によらず、製品ごとに設定されたサポート提供期間が適用されます。
- 複数年契約は、当該契約期間中の製品のサポート提供を保证するものではなく、また製品のサポート提供期間が終了した場合のバージョンアップを保证するものではありませんのでご注意ください。
- 各製品のサポート提供期間は以下のWebサイトからご確認ください。
<https://success.trendmicro.com/doc/s/solution/000207383?language=ja>

法人向け製品のサポートについて

- 法人向け製品のサポートの一部または全部の内容、範囲または条件は、トレンドマイクロの裁量により随時変更される場合があります。
- 法人向け製品のサポートの提供におけるトレンドマイクロの義務は、法人向け製品サポートに関する合理的な努力を行うことに限られるものとします。

著作権について

本ドキュメントに関する著作権は、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、本ドキュメント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、本ドキュメント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。本ドキュメントおよびその記述内容は予告なしに変更される場合があります。

商標について

TRENDMICRO、TREND MICRO、ウイルスバスター、InterScan、INTERSCAN VIRUSWALL、InterScanWebManager、InterScan Web Security Suite、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、Trend Park、Trend Labs、Network VirusWall Enforcer、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、SPN、SMARTSCAN、Trend Micro Kids Safety、Trend Micro Web Security、Trend Micro Portable Security、Trend Micro Standard Web Security、Trend Micro Hosted Email Security、Trend Micro Deep Security、ウイルスバスタークラウド、スマートスキャン、Trend Micro Enterprise Security for Gateways、Enterprise Security for Gateways、Smart Protection Server、Deep Security、ウイルスバスター ビジネスセキュリティサービス、SafeSync、Trend Micro NAS Security、Trend Micro Data Loss Prevention、Trend Micro オンラインスキャン、Trend Micro Deep Security Anti Virus for VDI、Trend Micro Deep Security Virtual Patch、SECURE CLOUD、Trend Micro VDIオプション、おまかせ不正請求クリーンアップサービス、Deep Discovery、TCSE、おまかせインストール・バージョンアップ、Trend Micro Safe Lock、Deep Discovery Inspector、Trend Micro Mobile App Reputation、Jewelry Box、InterScan Messaging Security Suite Plus、おもいでバックアップサービス、おまかせ！スマホお探しサポート、保険&デジタルライフサポート、おまかせ！迷惑ソフトクリーンアップサービス、InterScan Web Security as a Service、Client/Server Suite Premium、Cloud Edge、Trend Micro Remote Manager、Threat Defense Expert、Next Generation Threat Defense、Trend Micro Smart Home Network、Retro Scan、is702、デジタルライフサポート プレミアム、Airサポート、Connected Threat Defense、ライトクリーナー、Trend Micro Policy Manager、フォルダシールド、トレンドマイクロ認定プロフェッショナルトレーニング、Trend Micro Certified Professional、TMCP、XGen、InterScan Messaging Security、InterScan Web Security、Trend Micro Policy-based Security Orchestration、Writing Style DNA、Securing Your Connected World、Apex One、Apex Central、MSPL、TMOL、TSSL、ZERO DAY INITIATIVE、Edge Fire、Smart Check、Trend Micro XDR、Trend Micro Managed XDR、OT Defense Console、Edge IPS、Trend Micro Cloud One、スマスキャ、Cloud One、Cloud One - Workload Security、Cloud One - Conformity、ウイルスバスター チェック！、Trend Micro Security Master、Trend Micro Service One、Worry-Free XDR、Worry-Free Managed XDR、Network One、Trend Micro Network One、らくらくサポート、Service One、超早得、先得、Trend Micro One、Workforce One、Security Go、Dock 365、およびTrendConnectは、トレンドマイクロ株式会社の登録商標です。

本ドキュメント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 © 2023 Trend Micro Incorporated. All rights reserved.

P/N: IHEM67227/150924_JP_R6 (2023/11)

目次

はじめに	19
IWSS のドキュメント	20
対象読者	20
ドキュメントの表記規則	21
トレンドマイクロについて	21
第 1 章 製品の概要	23
主な機能	24
アプリケーション制御	24
HTTP 検査	24
情報漏えい対策	24
データ識別子の種類	25
パターン	25
事前定義されたパターン	25
キーワードリスト	26
事前定義されたキーワードリスト	26
情報漏えい対策テンプレート	26
情報漏えい対策ポリシー	26
高度な脅威保護	27
HTTPS 復号化	27
Web レピュテーション	27
FTP 検索	28
URL フィルタ	28
さまざまなユーザ識別方法	29
通知	29
リアルタイム統計情報とアラート	29

ログとレポート	30
syslog のサポート	30
リバースプロキシのサポート	31
IWSS の複数設置のサポート	31
新機能	31
新機能	31
システム要件	31
ICAP 1.0 対応キャッシュサーバとの連携	32
X-Authenticated ICAP ヘッダのサポート	32
システムステータス	32
しきい値アラート設定の有効化	32
同時接続数の表示	33
CPU 使用率の表示	34
物理メモリ使用率の表示	34
ハードディスクドライブの表示	35
その他の Web 脅威情報へのアクセス	36
ダッシュボード	37
Web トラフィックのセキュリティ上の脅威の概要	39
第 2 章 配置ウィザード	41
配置ウィザードの概要	42
モード選択	42
プロキシ転送モード	43
リバースプロキシモード	44
ICAP モード	45
配置ウィザードで IWSS を ICAP モードで配信する	45
通常の透過モード	46
モード固有の設定	47
プロキシ設定	47

プロキシ転送モード	47
リバースプロキシの設定	49
ICAP の設定	50
通常の透過設定	53
製品のアクティベーション	53
アクティベーションコードについて	54
結果	54
配信ステータス	55
配信後	55
IWSS ICAP の設定	55
ICAP 1.0 対応キャッシュサーバの設定	56
ウイルス検索サーバクラスタの設定	59
クラスタの設定またはエントリの削除	60
キャッシュされた既存のコンテンツをアプライアンスから消去	61
IWSS が ICAP 要求を待機していることを確認する	61
リクエストモードとレスポンスモードの違いについて	62
リクエストモード処理をトリガする	62
レスポンスモード処理をトリガする	63
第 3 章 アップデート	65
製品サポート	66
サポート契約の更新	66
アップデート機能について	66
IWSS 管理コンソールからアップデートする方法	67
プロキシ設定 (アップデート用)	67
アップデート可能なコンポーネント	68
ウイルスパターンファイル	69
ウイルスパターンファイルの仕組み	69
スパイウェアパターンファイル	70

ポットパターンファイル	71
IntelliTrap パターンファイルおよび IntelliTrap 除外パターンファイル	71
スマートスキャンエージェントパターンファイル	71
スクリプトアナライザ (SA) パターンファイル	72
プロトコル情報抽出パターンファイル	72
検索エンジン	72
検索エンジンのアップデートについて	73
Web レピュテーションデータベース	73
パターンファイルおよびエンジンの差分アップデート	74
コンポーネントのバージョン情報	74
手動アップデート	74
強制手動アップデート	75
予約アップデート	76
アップデートの操作方法	77
アップデート通知	77
アップデートのロールバック	77
パターンファイルの削除	78
第 4 章 アプリケーション制御	79
アプリケーション制御の概要	80
アプリケーション制御ポリシーリスト	80
ポリシーの追加：アカウントの選択	82
アプリケーション制御ポリシーの追加	83
ポリシーの追加または編集：アプリケーション制御ポリシーのルールの 指定	83
アプリケーション制御ポリシールールの指定	84
第 5 章 HTTP 設定	87
HTTP/HTTPS トラフィックフローの有効化	88

プロキシ設定および関連するその他の設定	88
プロキシ設定	89
上位プロキシなし (スタンドアロンモード)	89
上位プロキシあり (依存モード)	90
通常の透過 (透過プロキシモード)	92
リバースプロキシ	94
プロキシに関する設定	95
HTTP 待機ポート	95
FTP over HTTP の匿名ログオンに使用するメールアドレス	96
ネットワーク設定および負荷の処理	96
インターネットアクセス管理の設定	97
クライアントとサーバの識別	97
クライアント IP による設定	97
サーバ IP の除外リスト	98
宛先ポートによる制限	100
HTTPS ポートによる設定	101
第 6 章 ポリシーとユーザ識別方法	103
ポリシーの仕組み	104
初期設定のグローバルポリシーとゲストポリシー	105
ゲストポリシーについて	106
ゲストポートの有効化	106
ゲストアカウントの有効化	107
ポリシークエリ	107
ポリシーの配信	107
ユーザ識別方法の設定	108
IP アドレス	109
クライアント登録ユーティリティ	109
ユーザ / グループ名認証	110

LDAP 認証方法	110
LDAP の通信フロー	111
LDAP 設定	113
クロスドメインの Active Directory オブジェクトクエリ	115
ポリシーの範囲の設定	116
IP アドレスを使用したポリシー設定	117
LDAP を使用したポリシー設定	117
第 7 章 HTTP 検索の設定	119
HTTP 検査の概要	120
HTTP 検査ポリシー	121
HTTP 検査: アカウントの選択	121
HTTP 検査: ルールの指定	122
HTTP 検査: 除外リストの指定	125
HTTP 検査フィルタ	125
初期設定の HTTP 検査フィルタ	126
HTTP 検査フィルタの追加	129
HTTP 検査フィルタの編集	138
HTTP 検査フィルタのインポート	138
HTTP 検査フィルタのエクスポート	140
情報漏えい対策	141
ポリシー	141
テンプレート	143
情報漏えい対策オプション (iDLP)	144
HTTPS のセキュリティ	144
未確認の HTTPS コンテンツの危険性	144
SSL ハンドシェイクの概要	145
IWSS における HTTPS 復号化およびプロセスフロー	146
HTTPS 復号化ポリシーの設定	147

HTTPS 復号化の有効化	147
新しい HTTPS 復号化ポリシーの作成	147
HTTPS 復号化設定	149
サーバ証明書の検証	149
証明書の検証の除外	150
クライアント証明書の処理	150
認証機関	151
SSL 方式	153
ドメイントンネリング	154
トンネリングされたドメイン	154
トンネリングされたドメインの除外	154
HTTPS アクセスの失敗	155
高度な脅威保護ポリシーの作成と変更	155
Web レピュテーションルールの指定	157
フィッシング対策、ファームウェア対策、および C&C コールバック 試行検出	158
カスタム保護設定	159
カスタム保護を有効にする	159
サンプル提出	159
リスクレベル設定	159
処理	159
Web レピュテーション設定	159
Web レピュテーションの有効化と無効化	160
Web レピュテーション結果の管理	160
WRS/URL キャッシュのクリア	162
HTTP ウイルス検索ルール	162
高度な脅威検索	162
ブロックするファイルタイプの指定	163
検索するファイルタイプの指定	163
ウイルス / 不正プログラム検索設定の優先順位	167

圧縮ファイルの検索制限の設定	167
サイズの大きいファイルの処理	168
隔離ファイルの処理	173
スパイウェア検索ルール	173
高度な脅威保護のパフォーマンスに関する注意事項	174
X-Forwarded-For HTTP ヘッダ	175
X-Forwarded-For HTTP ヘッダの設定	177
ポットおよび C&C コンタクト検出ルールの指定	178
除外リストの指定	178
除外リストの作成	179
ウイルス検出時の処理設定	182
検索処理	182
検索イベント	183
備考欄への入力	184
第 8 章 アクセス割り当てと URL アクセス設定	185
アクセス割り当てポリシーについて	186
アクセス割り当てポリシーの管理	186
URL アクセス管理の概要	188
URL アクセス管理の設定	189
信頼する URL の設定	189
URL のブロック	191
ローカルリストの使用	192
第 9 章 URL フィルタ	195
URL フィルタについて	196
URL フィルタ処理	197
URL フィルタの設定作業の流れ	198
URL フィルタポリシーの管理	199

URL フィルタの有効化	199
動的な URL カテゴリ分類の有効化	200
新しいポリシーの作成	200
ポリシーの変更と削除	202
URL フィルタの設定	203
カスタムカテゴリの作成	203
URL カテゴリの見直しの依頼と URL 検索	204
未評価の URL および不明 URL	205
URL カテゴリの見直し依頼	205
予約期間の設定	206
URL 警告の TTL	207
URL フィルタの除外設定	207
URL フィルタの割り当てた時間の延長	208
第 10 章 FTP 検索	211
FTP 検索について	212
FTP 設定	212
プロキシ設定	212
パッシブおよびアクティブモード	213
クライアント要求	213
FTP 検索オプション	214
FTP トラフィックおよび FTP 検索の有効化	214
検索対象	215
ブロックするファイルタイプ	215
検索するファイルタイプ	215
FTP 検索設定の優先順位	216
圧縮ファイルの処理	216
サイズの大きいファイルの処理	216
隔離ファイルの暗号化	217

スパイウェアの検索	217
情報漏えい対策	217
FTP 検索除外リスト	217
FTP 検索の設定	217
ウイルスに対する検索処理の設定	219
FTP 一般設定	220
プロキシ設定	221
データコネクション	221
FTP アクセス管理設定	222
クライアント IP による設定	222
サーバ IP の除外リストによる設定	223
宛先ポートによる設定	223
第 11 章 レポート、ログおよび通知	225
レポートについて	226
レポート情報	226
レポート設定	226
このレポートをメールで送信	227
作成対象 (ユーザおよびグループ)	227
レポートの種類	227
レポートの生成	229
レポートの設定	230
レポートの種類	231
レポートの予約	232
保存されている予約レポート	233
ログについて	233
アプリケーション帯域幅	233
ポリシー施行	234
インターネットアクセス	234

インターネットセキュリティ	235
データセキュリティ	235
アクセス管理	236
データ記録のオプション	236
ログのクエリおよび表示	236
ログの設定	237
グローバルログフィルタ	239
匿名ログ	239
ログのアンロードと取得	239
ログおよびレポートデータの CSV ファイルへのエクスポート	239
PDF 形式でのレポートデータの出力	239
syslog 設定	240
通知について	240
通知先の設定	241
通知の変数	242
通知の設定	247
ユーザへの通知での HTML タグの使用	247
C&C コンタクトコールバック通知の設定	248
情報漏えい対策通知の設定	248
FTP 情報漏えい対策通知の設定	249
FTP ファイルタイプによるブロック通知の設定	250
FTP 検索通知の設定	251
HTTP/HTTPS ファイルタイプによるブロック通知の設定	251
HTTP/HTTPS 検索通知の設定	252
HTTPS アクセス拒否通知の設定	253
HTTPS 証明書エラー通知の設定	254
アプリケーション制御通知による HTTP/HTTPS アクセス拒否の設定	255
パターンファイルのアップデート通知の有効化	256
しきい値アラートの設定	256
URL アクセスの警告通知の設定	257

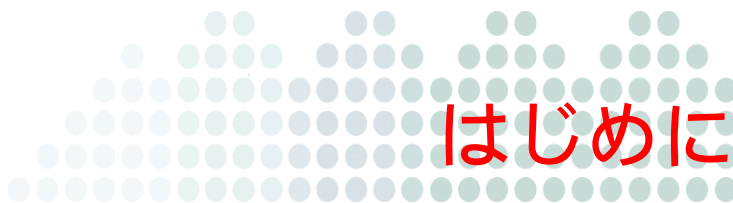
URL アクセスのオーバーライドの通知の設定	258
アクセス管理通知による URL ブロックの設定	259
HTTP 検査通知による URL ブロックの設定	260
URL フィルタ通知による URL ブロックの設定	261
URL フィルタエンジンおよび検索エンジンのアップデートの通知の有効化	261
時間割り当て通知による URL フィルタの設定	262
スマートスキャンイベント通知の設定	262
SNMP トラップ通知の有効化	263
第 12 章 管理	265
概要	266
監査ログ	267
一般設定	268
ユーザの識別	268
ユーザ / グループ認証の設定	269
グローバルな認証キャッシュの設定	272
標準認証	272
キャプティブポータル	273
なし	274
ポリシー確認画面	275
基本モード	275
認証の許可リスト	276
ポリシー配信	276
データベース接続	277
隔離管理	277
隔離ディレクトリ	277
隔離ファイルの暗号化	278
予約期間	278
Control Manager への登録	279

複製の設定	279
集中管理ログ/レポート	280
検索方法	281
PAC ファイル管理	281
管理コンソール	282
アカウント管理	282
ログインアカウントを追加する	282
ログインアカウントを変更する	283
役割ベースの管理	283
役割の管理	284
メニュー項目の権限	284
管理メニュー項目のアクセス	285
組み込みのユーザの役割	286
カスタムの役割	286
カスタムの役割の追加	286
カスタムの役割の変更	287
カスタムの役割の削除	287
設定のバックアップと復元	287
システムアップデート	288
システムイベントログ	289
製品ライセンス	289
ライセンス期限切れの警告	290
レジストレーションキーの取得	290
アクティベーションコードの取得と入力	291
ライセンスの更新	291
サポート契約の更新	291
SNMP の設定	292
システム情報の設定	292
アクセス管理設定	292
Web コンソール	293

サポート情報	293
デバッグログ	294
配信診断	294
第 13 章 製品のテストと設定	295
EICAR テストファイル	296
Web レピュテーションのテスト	296
アップロード検索のテスト	297
HTTPS 復号化検索のテスト	298
FTP 検索のテスト	301
アプリケーション制御のテスト	302
HTTP 検査のテスト	303
URL 監視のテスト	304
ダウンロード検索のテスト	306
URL フィルタのテスト	307
スパイウェア検索のテスト	308
その他の IWSS の設定	309
高度な脅威保護検索の指定	309
ユーザの識別方法の指定	309
ゲストアカウントの有効化 (LDAP のみ)	309
検索ポリシーとフィルタポリシーの見直し	310
アクセス割り当てポリシーの有効化	310
インターネットアクセス管理の設定	310
アプリケーションパッチの適用またはアプリケーションパッチの削除	311
HotFix、Patch、および Service Pack について	312
データベース接続の確認	313
管理コンソールパスワードの変更	313
管理コンソールの待機ポート変更後の設定	314
URL フィルタ設定の確認	314

IWSS パフォーマンスの調整	315
LDAP パフォーマンスの調整	315
LDAP の内部キャッシュ	315
LDAP が有効な場合の冗長ログの無効化	316
付録 A サポート情報	317
トラブルシューティングのリソース	318
サポートポータルの利用	318
脅威データベース	318
製品サポート情報	319
サポートサービスについて	319
セキュリティニュース	320
トレンドマイクロ「セキュリティニュース」	320
トレンドマイクロへのウイルス解析依頼	320
メールレピュテーションについて	321
ファイルレピュテーションについて	321
Web レピュテーションについて	321
その他のリソース	321
最新版ダウンロード	321
脅威解析・サポートセンター TrendLabs (トレンドラボ)	322
付録 B ファイルタイプと MIME コンテンツタイプの対応	323
概要	324
MIME コンテンツファイルのファイルタイプマッピングテーブル	326
付録 C アーキテクチャと設定ファイル	345
モジュールの構成	346
サービス	346
予約タスク	348

設定ファイルについて	350
プロトコルハンドラ	351
検索モジュール	352
付録 D IWSS のベストプラクティス	353
共有パーソナルコンピュータで複数のユーザを認証する (標準認証)	354
ベストプラクティスの提案	354
Microsoft ShellRunas ユーティリティの利用	354
検索に関する考慮事項	355
Smart Protection Network — クラウドベースのサービス	355
ベストプラクティスの提案	356
ローカルな IWSS 検索エンジン	356
ベストプラクティスの提案	357
付録 E URL フィルタカテゴリのグループ	359
URL フィルタのカテゴリ	360



はじめに

InterScan Web Security Suite 6.5 Patch 3 (以下、IWSS) 管理者ガイドによろこそ。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。

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

IWSS のドキュメント

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** このガイドでは、IWSS を紹介し、設置計画、実装、および設定の各作業を案内し、アップグレード後の主な設定作業について説明することで、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設置のテスト、トラブルシューティング、サポートへの問い合わせについても説明しています。
- ・ **オンラインヘルプ** オンラインヘルプの目的は、製品の主なタスクに関する操作手順、使用方法のアドバイス、および有効なパラメータの範囲、最適な値など、実際に使用する場面に固有の情報を提供することです。オンラインヘルプには、IWSS の Web コンソールからアクセスできます。
- ・ **Readme** オンラインヘルプやマニュアルにない最新の製品情報や注意事項が記載されています。新機能、設置のヒント、既知の問題、およびリリース履歴が含まれています。各種ドキュメントの最新版は、次の Web サイトから入手できます。

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

- ・ **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。

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

対象読者

この IWSS ドキュメントは、企業の IT 管理者およびシステム管理者を対象として書かれています。本書は、次のようなネットワークの概要に関する専門的な知識があることを前提としています。

- ・ HTTP
- ・ HTTPS
- ・ FTP
- ・ 一部の企業で使用されるその他のインターネットプロトコル

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

ドキュメントの表記規則

このドキュメントでは、次の表記規則を使用しています。

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

表 1. 本書で使用している表記規則

トレンドマイクロについて

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

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

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

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



第1章

製品の概要

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

本章で説明する内容には、次の項目が含まれます。

- ・ 24 ページの「主な機能」
- ・ 31 ページの「新機能」
- ・ 31 ページの「システム要件」
- ・ 32 ページの「システムステータス」
- ・ 37 ページの「ダッシュボード」
- ・ 39 ページの「Web トラフィックのセキュリティ上の脅威の概要」

主な機能

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

アプリケーション制御

アプリケーション制御機能では、人気の高いインターネットアプリケーションを自動的に検出し、管理者がポリシーを使用してそれらのアプリケーションを制御できるようにするセキュリティテクノロジーを提供します。詳細については、80 ページの「アプリケーション制御の概要」を参照してください。

HTTP 検査

HTTP 検査により、管理者は動作を識別して、HTTP メソッド、URL、およびヘッダに基づいて Web トラフィックをフィルタできます。また、フィルタを作成するか、初期設定のフィルタを使用して Web トラフィックを識別したり、フィルタをインポートおよびエクスポートしたりすることもできます。トラフィックが識別されたら、IWSS は、特定のトラフィックに対する適切な処理を決定するポリシー設定に従ってそのトラフィックを管理できます。たとえば、HTTP 検査ポリシーによって、ユーザにソーシャルネットワーキングや Web メールサイトのコンテンツの閲覧は許可しますが、それらへのコンテンツの投稿は禁止することができます。詳細については、120 ページの「HTTP 検査の概要」を参照してください。

情報漏えい対策

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

たとえば、IBAN は正規表現の説明では次のようになります。

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

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

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

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

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

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

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

データ識別子の種類

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

- ・ パターン：特定の構造を持つデータ。詳細については、25 ページの「パターン」を参照してください。
- ・ キーワードリスト：特殊な単語や語句のリスト。詳細については、26 ページの「キーワードリスト」を参照してください。

パターン

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

事前定義されたパターン

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

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

キーワードリスト

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

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

事前定義されたキーワードリスト

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

情報漏えい対策テンプレート

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

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

情報漏えい対策ポリシー

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

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

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

高度な脅威保護

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

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。

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

HTTPS 復号化

IWSS は、暗号化されたコンテンツを復号化して検査することで HTTPS のセキュリティホールをふさぎます。選択した Web カテゴリの HTTPS トラフィックを復号化するようにポリシーを定義できます。復号化の際、データは HTTP トラフィックと同じ方法で扱われ、URL フィルタおよび検索のルールを適用可能です。

Web レピュテーション

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

また、Web レピュテーションでは、レピュテーションスコアを URL に割り当てます。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、ユーザ定義のセキュリティレベルとスコアとの比較に基づき、必要な処理が実行されます。

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、インターネットセキュリティログとダッシュボード ([上位の脅威検出数]) で確認できます。

Web レピュテーションの詳細については、157 ページの「Web レピュテーションルールの指定」および 159 ページの「Web レピュテーション設定」を参照してください。

FTP 検索

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

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。

URL フィルタ

IWSS の URL フィルタオプションを使用して、「成人向け」、「ギャンブル」、「金融サービス」などの URL のカテゴリに基づいてポリシーを設定できます。ユーザが URL を要求すると、IWSS はまずその URL のカテゴリを検索し、次に管理者が設定したポリシーに基づいてその URL へのアクセスの許可、拒否、または監視を行って、ブロック、警告、オーバーライド付きブロック、または時間制限の通知を表示します。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。

さまざまなユーザ識別方法

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

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または FTP 接続コンソールに表示されます。管理者への通知もユーザへの通知も、カスタマイズ可能です。

ネットワーク管理ツールと連携するために、IWSS では SNMP トラップとして各種の通知も発行できます。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。

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

リアルタイム統計情報とアラート

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、[システムステータス] 画面にグラフや表で表示されます。次のような統計情報が含まれます。

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

ログとレポート

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。レポートは次のように大別できます。

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

レポートは、データベース内の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。

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

詳細については、225 ページの「レポート、ログおよび通知」を参照してください。

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

詳細については、37 ページの「ダッシュボード」を参照してください。

syslog のサポート

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

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。リバースプロキシとして、IWSS は保護対象の Web サーバの近くにインストールされます。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、94 ページの「リバースプロキシ」を参照してください。

IWSS の複数設置のサポート

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

新機能

新機能

InterScan Web Security Suite 6.5 Linux 版 Patch 2 から Patch 3 への変更点については、Readme をご確認ください。

システム要件

最新の情報については、次の Web サイトを参照してください。

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

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

ICAP 1.0 対応キャッシュサーバとの連携

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

X-Authenticated ICAP ヘッダのサポート

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

システムステータス

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

- ・ しきい値アラート設定の有効化
- ・ 同時接続数の表示
- ・ CPU 使用率の表示
- ・ 物理メモリ使用率の表示
- ・ ハードディスクドライブの表示

しきい値アラート設定の有効化

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

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

- ・ 帯域幅

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。241 ページの「通知先の設定」を参照してください。

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

しきい値アラートを有効にするには

1. 管理コンソールから [システムステータス] を選択し、[しきい値アラート] をクリックします。
2. [しきい値] で必要なしきい値を指定し、初期設定を使用するか、または [しきい値] 列と [通知の送信間隔] 列に新たな値を指定します。
3. [通知メッセージ] で初期設定の通知メッセージを使用しない場合は、初期設定のテキストを選択して、任意のテキストを入力します。該当する場合は、242 ページの「通知の変数」で説明されているように、テキストに変数を挿入します。
4. [保存] をクリックします。

同時接続数の表示

HTTP/HTTPS の同時接続使用率は紫色で、FTP の同時接続使用率はオレンジ色で、アプリケーション接続の同時接続使用率は緑色で動的に表示されます。接続数と接続時間（秒単位）が表示されません。

ここには次のグラフが表示されます。

- ・ FTP: コマンドとデータの両方のセッションの接続が測定されます。
- ・ HTTP(S): 要求と応答の両方のセッションの接続が測定されます。
- ・ アプリケーションの接続数: アプリケーションの送受信トラフィックのセッションが測定されます。

初期設定の表示更新頻度は 30 秒です。X 軸と Y 軸のスケールはどちらも可変です。X 軸のスケールは設定した表示更新頻度によって決まり、Y 軸のスケールは特定時刻の同時接続数によって決まります。

CPU 使用率の表示

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

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

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

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

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

物理メモリ使用率の表示

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

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

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

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

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

詳細については、74 ページの「手動アップデート」を参照してください。

ハードディスクドライブの表示

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

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

しきい値アラートの値とアラートの頻度を指定して、ハードディスクのステータスが重大レベルに到達したときに通知を受け取ることができます。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。

その他の Web 脅威情報へのアクセス

[システムステータス] 画面の右上隅にある [脅威に関するリソース] リストで、トレンドマイクロの Web 評価サイトへのリンクにアクセスすると、多様なことができます。最新の Web 脅威や多様な Web 脅威の発生元を調査したり、トレンドマイクロのセキュリティデータベース検索にアクセスしたり、Web とメール不正プログラムのリアルタイム統計情報を確認できます。[脅威に関するリソース] リストの表示については、174 ページの「高度な脅威保護のパフォーマンスに関する注意事項」を参照してください。

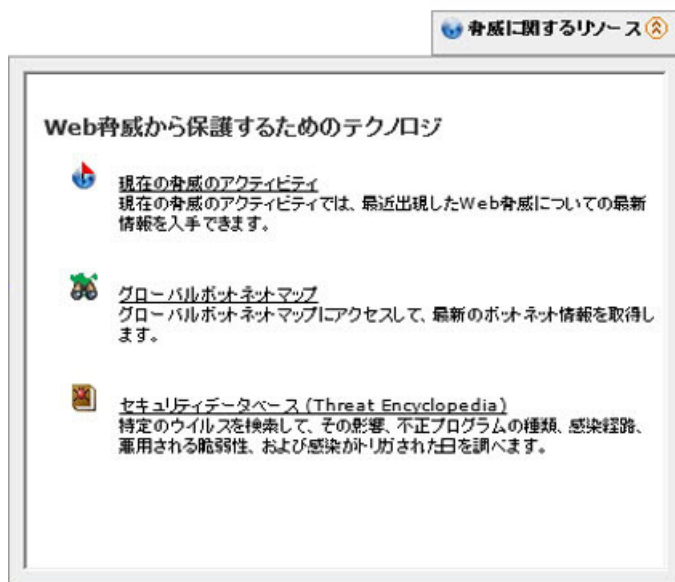


図 1-1. IWSS でアクセス可能な Web 評価テクノロジー

ダッシュボード

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

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

- ・ **アクセスされた上位 URL カテゴリ** このウィジェットには URL カテゴリに関連した違反が表示されます。今日、過去 1 時間、過去 12 時間、または過去 7 日間の情報を表示できます。初期設定は棒グラフですが、円グラフに切り替えることができます。表示するソースの数は、ウィジェット上部にあるドロップダウンリストから選択します。
- ・ **インターネットセキュリティによってブロックされた上位ユーザ (初期設定)** 指定期間内に最も多くブロックされたサイトにアクセスしたユーザを示し、インターネットセキュリティや許容される使用方法についてユーザに理解を促します。初期設定は上位 5 件、過去 1 日間です。
- ・ **ブロックされた上位 URL カテゴリ (初期設定)** 指定期間内に最も多くブロックされた URL カテゴリを示し、セキュリティ、帯域幅、および生産性の潜在的な問題について概要ビューを提供します。初期設定は上位 5 件、過去 1 日間です。
- ・ **アプリケーション帯域幅 (初期設定)** 指定期間のアプリケーションの使用状況における帯域幅 (kbps) のトラフィック傾向を示します。初期設定の期間は過去 1 日間です。

注意： ダッシュボードでのアプリケーション帯域幅のデータ統計には Linux カーネルのサポートが必要です。サポートを有効にするには、
`/usr/iwss/bin/build_nfq_ko.sh` スクリプトを実行して `nfq_redirect.ko` をコンパイルし、`/etc/iscan/S99ISappd start` を実行して `appd` デーモンを起動します。

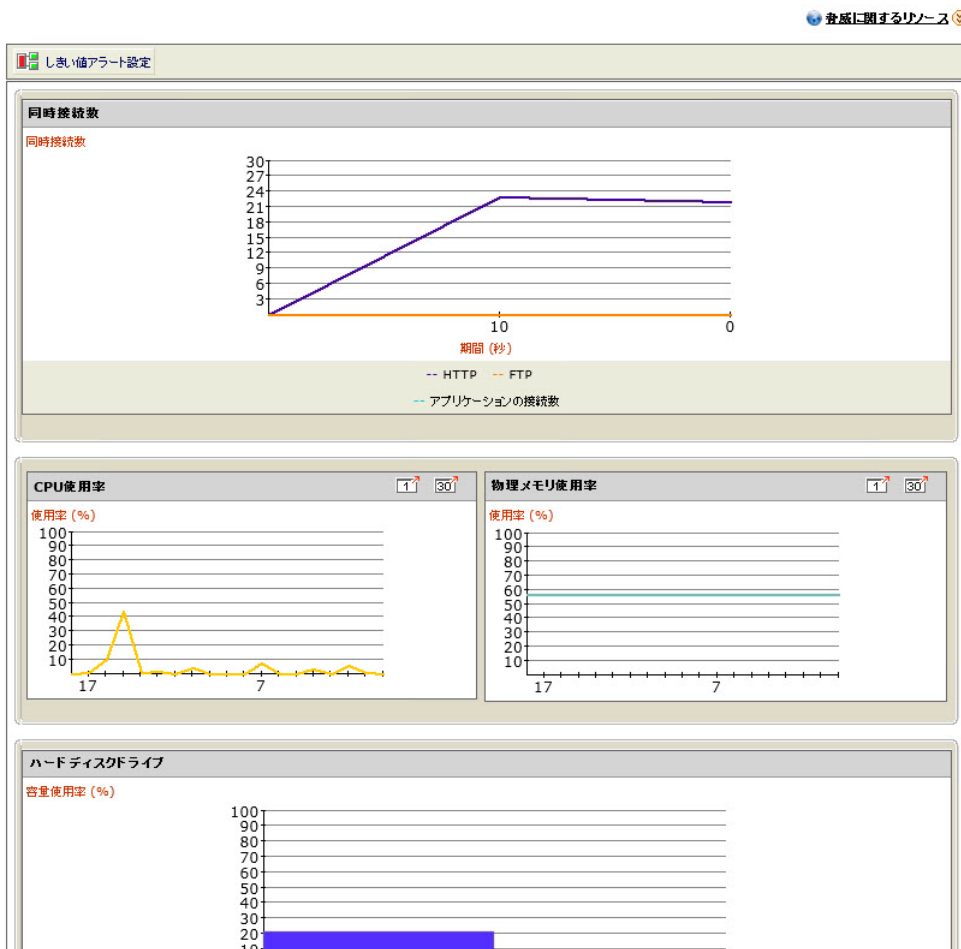
- ・ **ブロックされた上位アプリケーション** 指定期間内に最も多くブロックされたアプリケーションカテゴリを示し、セキュリティ、帯域幅、および生産性の潜在的な問題について概要ビューを提供します。初期設定は上位 20 件、過去 7 日間です。
- ・ **ペイロード** FTP および HTTP/HTTPS に関する 2 つのグラフを示す動的表示です。FTP については、コマンドとデータの両方のセッションの接続が測定されます。HTTP/HTTPS については、要求と応答の両方のセッションの接続が測定されます。初期設定は過去 12 時間です。
- ・ **許可された上位アプリケーション** 許可された上位アプリケーションへのアクセスインスタンスの指定期間内の合計数を示します。
- ・ **上位の脅威検出数 (初期設定)** 指定期間内に IWSS によって検出された各種の脅威 (不正 URL、ウイルス、スパイウェア、ボットネット、攻撃コード) の合計件数を示し、さまざまな脅威ベクトルのリスクレベルの概要ビューを提供します。初期設定は上位 20 件、過去 1 日間です。
- ・ **上位のポリシー施行 アプリケーション制御** 指定期間内に違反が発生したポリシーとその要求数を示すことで、ポリシーの実効性と変更の必要性を示します。初期設定は上位 5 件、過去 1 日間です。
- ・ **上位のポリシー施行 URL フィルタ** 指定期間内に違反が発生したポリシーとその要求数を示すことで、ポリシーの実効性と変更の必要性を示します。初期設定は上位 5 件、過去 1 日間です。
- ・ **上位のポリシー施行 DLP** 指定期間内に違反 (ブロック / 監視) が発生したポリシーとその要求数を示すことで、ポリシーの実効性と変更の必要性を示します。初期設定は上位 5 件、過去 1 日間です。
- ・ **C&C コールバック回数 (コマンド & コントロールコールバック回数)** 指定期間内に検出された C&C コールバック試行回数を示します。初期設定は過去 1 日間です。

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

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

Web トラフィックのセキュリティ上の脅威の概要

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



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、ウイルスやその他の脅威を特定し、企業ネットワークの HTTPS、HTTP、および FTP トラフィックを含む複数のインターネットプロトコルを保護する包括的なセキュリティ製品です。

コンテンツベースのウイルス検索はもちろん、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。

- ・ アプリケーション制御機能では、人気の高いインターネットアプリケーションを自動的に検出し、管理者がポリシーを使用してそれらのアプリケーションを制御できるようにするセキュリティテクノロジーを提供します。
- ・ 従業員によって悪用される可能性のある数百のインターネットアプリケーションを監視し、ブロック / 許可ポリシーを有効にします。
- ・ Web レピュテーションでは、潜在的に危険な Web サイト、特に既知のフィッシングサイトまたはファームングサイトにアクセスする前に URL を調べます。
- ・ URL フィルタ機能を使用すると、企業で禁止されたコンテンツを含む Web サイトへのアクセスを許可、ブロック、オーバーライド付きブロック、警告した上での許可、時間制限、または監視できます。
- ・ HTTPS 復号化機能を使用すると、暗号化されたトラフィックは IWSS 検索およびフィルタポリシーを「通常」の HTTP トラフィックとして通過することができ、HTTPS サーバからの証明書が検証されます。



第2章

配置ウィザード

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

本章で説明する内容には、次の項目が含まれます。

- ・ 42 ページの「配置ウィザードの概要」
- ・ 42 ページの「モード選択」
- ・ 47 ページの「モード固有の設定」
- ・ 53 ページの「製品のアクティベーション」
- ・ 54 ページの「結果」
- ・ 55 ページの「配信後」

配置ウィザードの概要

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

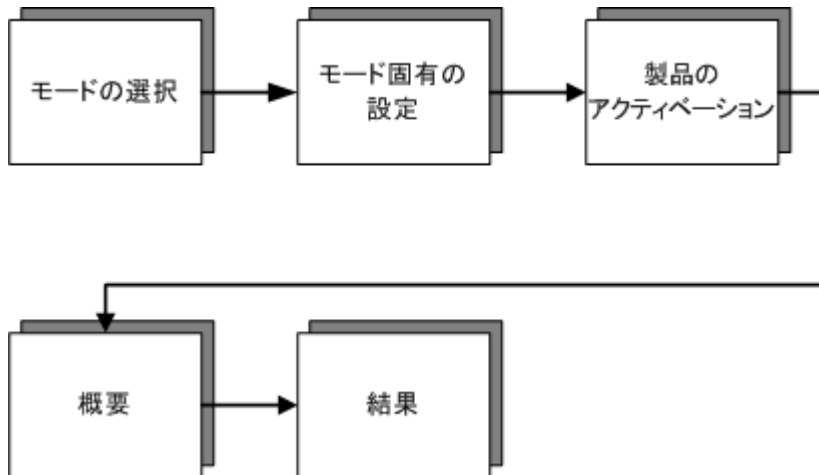


図 2-1. 配置ウィザードのフロー

モード選択

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

配置ウィザードを使用して、IWSS を次のモードのいずれかに設定できます。

- ・ 43 ページの「プロキシ転送モード」
- ・ 44 ページの「リバースプロキシモード」
- ・ 45 ページの「ICAP モード」
- ・ 46 ページの「通常の透過モード」

プロキシ転送モード

IWSS は、ネットワーククライアントの上位プロキシとして機能できます。トラフィックを IWSS にリダイレクトするように、クライアントのブラウザを設定する必要があります。IWSS は HTTP トラフィックと FTP トラフィックを検索するため、別の専用プロキシサーバを用意する必要があります。コンテンツは、受信方向と送信方向の両方で検索されます。IWSS は HTTP および HTTPS プロトコルを検出するため、アプリケーション制御のレポートとポリシーもプロキシモードで機能します。

プロキシ転送モードは、次の機能も備えています。

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

注意： IWSS をプロキシ転送モードで設定する方法の詳細については、96 ページの「ネットワーク設定および負荷の処理」を参照してください。

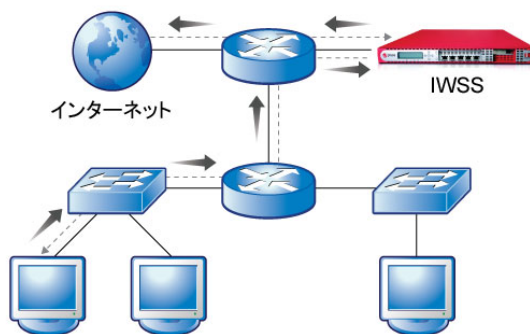


図 2-2. プロキシ転送モード

IWSS をプロキシ転送モードで配信するには

1. [管理] [配置ウィザード] に移動します。

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

2. [ようこそ] 画面で [開始] をクリックします。
3. [配信モード] 画面で [プロキシ転送モード] オプションを選択します。
4. [次へ] をクリックします。
5. 47 ページの「モード固有の設定」に移動して続行します。

リバースプロキシモード

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

警告： このモードでは、DLP 機能は無効になります。

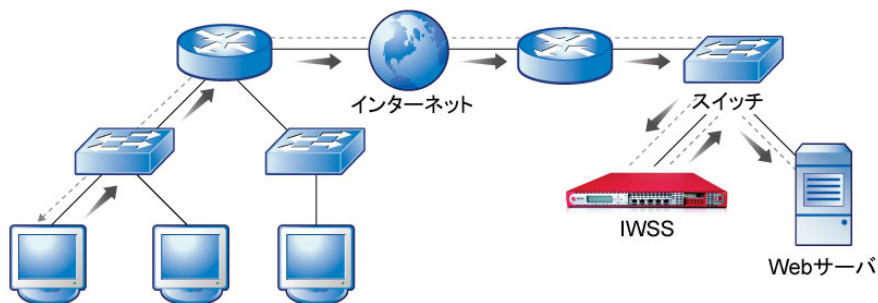


図 2-3. リバースプロキシモード

IWSS をリバースプロキシモードで配信するには

1. [管理] [配置ウィザード] に移動します。

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

2. [ようこそ] 画面で [開始] をクリックします。
3. [配信モード] 画面で [リバースプロキシモード] オプションを選択します。
4. [次へ] をクリックします。
5. 47 ページの「モード固有の設定」に移動して続行します。

ICAP モード

現在、この配信モードは IPv6 をサポートしていません。この配信モードの IWSS は、ICAP サーバとして機能し、(IWSS のクライアントとして機能している) ICAP v1.0 対応キャッシュサーバからの ICAP 接続を受け入れます。キャッシュサーバは、キャッシュされたコンテンツをローカルに処理するため、全体的な帯域幅要件を削減し、待ち時間を短縮するのに役立ちます。IWSS は、キャッシュサーバおよびエンドユーザクライアントに返されるすべてのコンテンツを検索し、安全性を確保します。

注意： ICAP モードの有効化と設定については、96 ページの「ネットワーク設定および負荷の処理」および 55 ページの「IWSS ICAP の設定」を参照してください。

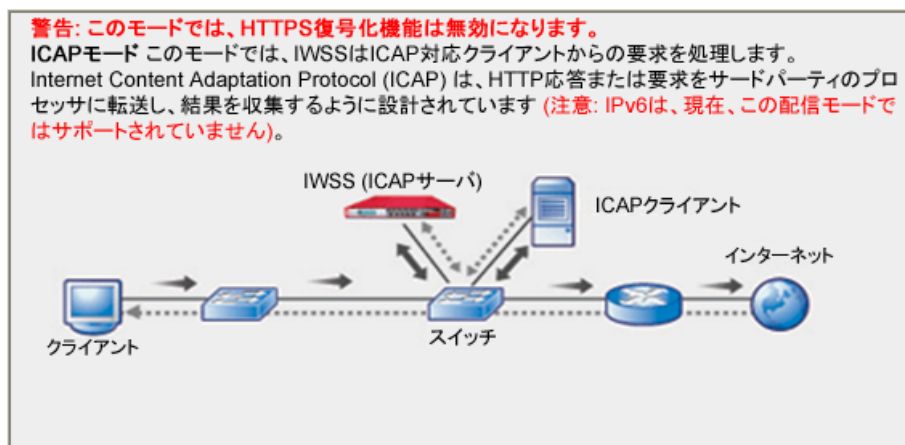


図 2-4. ICAP モード

配置ウィザードで IWSS を ICAP モードで配信する

IWSS を ICAP モードで配信するには

1. [管理] [配置ウィザード] に移動します。

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

2. [ようこそ] 画面で [開始] をクリックします。
3. [配信モード] 画面で [ICAP モード] オプションを選択します。

4. [次へ] をクリックします。
5. 47 ページの「モード固有の設定」に移動して続行します。

通常の透過モード

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

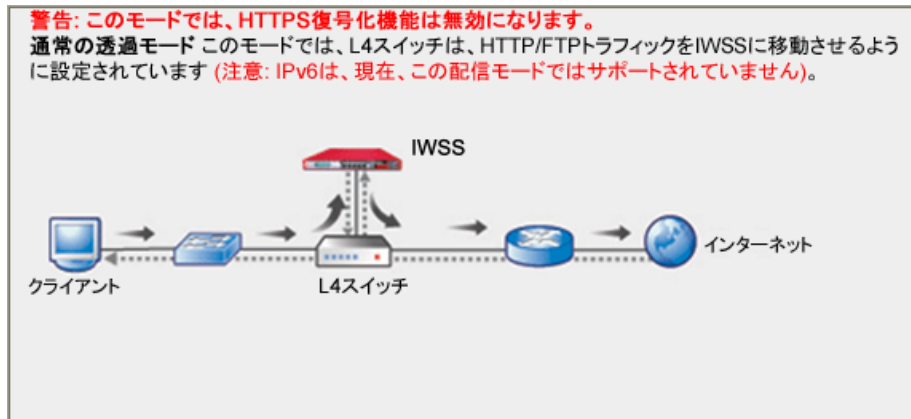


図 2-5. 通常の透過モード

IWSS を通常の透過モードで配信するには

1. [管理] [配置ウィザード] に移動します。

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

2. [ようこそ] 画面で [開始] をクリックします。
3. [配信モード] 画面で [通常の透過モード] オプションを選択します。
4. [次へ] をクリックします。
5. 47 ページの「モード固有の設定」に移動して続行します。

モード固有の設定

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

表 2-1. モード固有の設定

モード	モード固有の設定	ページ
プロキシ転送モード	プロキシ設定	47
リバースプロキシモード	リバースプロキシの設定	47
ICAP モード	ICAP 設定	50
通常の透過モード	透過設定	53

プロキシ設定

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

- ・ プロキシ転送のスタンドアロンモード - 47 ページの「スタンドアロンプロキシモードの設定」を参照
- ・ プロキシ転送の上位プロキシモード - 48 ページの「上位プロキシ (依存) モードの設定」を参照
- ・ リバースプロキシモード - 49 ページの「リバースプロキシの設定」を参照

プロキシ転送モード

ネットワーク設定に応じて、次のいずれかを指定できます。

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

スタンドアロンプロキシモードの設定

スタンドアロンモードのプロキシを設定するには

1. [配信モード] 画面で [プロキシ転送モード] オプションを選択します。
詳細については、43 ページの「プロキシ転送モード」参照。
2. [次へ] をクリックします。

3. 表 2-2 の設定の推奨事項に従います。

表 2-2. プロキシ転送モードでのスタンドアロン設定

構成パラメータ	詳細	推奨値
HTTP 待機ポート番号	IWSS が接続の受信を待機するポートです。	8080

4. [次へ] をクリックします。

上位プロキシ (依存) モードの設定

上位モードのプロキシを設定するには

1. [配信モード] 画面で [プロキシ転送モード] オプションを選択します。
詳細については、43 ページの「プロキシ転送モード」参照。
2. [次へ] をクリックします。
3. 表 2-3 の設定の推奨事項に従います。

表 2-3. プロキシ転送モードでの上位プロキシ (依存) の設定

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

4. [次へ] をクリックします。

リバースプロキシの設定

リバースプロキシモードのプロキシを設定するには

1. [配信モード] 画面で [リバースプロキシモード] オプションを選択します。
詳細については、44 ページの「リバースプロキシモード」参照。
2. [次へ] をクリックします。
3. 表 2-4 の設定の推奨事項に従います。

表 2-4. リバースプロキシモードのプロキシの設定

構成パラメータ	詳細	推奨値
HTTP 待機ポート番号	IWSS がリバースプロキシの接続の受信を待機するポートです。	80
SSL ポートを有効にする (チェックボックス)	SSL を有効 / 無効にします。	不要な場合は、無効のままにします。有効にするには、オンにします。
SSL ポート番号	IWSS がリバースプロキシの HTTPS 接続の受信を待機するポートです。	初期設定は 443 です。
証明書	インポートが必要な HTTPS の証明書ファイルです。	Base64 エンコードを使用する証明書ファイルをインポートします。
秘密鍵	インポートが必要な HTTPS 証明書の秘密鍵ファイルです。	証明書に関連付けられた秘密鍵をインポートします。
パスフレーズ	インポートが必要な HTTPS 証明書のパスフレーズです。	秘密鍵のパスフレーズを入力します。
保護対象サーバ	IWSS が保護する Web サーバの IP アドレスです。	保護対象サーバの IP アドレスを入力します。
保護対象サーバのポート番号	IWSS が保護する Web サーバのポートです。	保護対象サーバのポート番号を入力します。

4. [次へ] をクリックします。

ICAP の設定

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

ICAP モードでの配信には、追加の設定が必要です。

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

- X-Virus-ID: 検出したウイルスや脅威の名前を記述した US-ASCII テキスト 1 行が含まれます。たとえば、次のように記述します。

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

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

パラメータ値の詳細については、次を参照してください。

<http://www.icap-forum.org/>

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

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

ICAP を設定するには

1. 配置ウィザードの [配信モード] 画面で [ICAP モード] オプションを選択します。
詳細については、45 ページの「ICAP モード」を参照してください。
2. [次へ] をクリックします。
3. 表 2-5 の設定の推奨事項に従います。

表 2-5. ICAP モード固有の設定

構成パラメータ	詳細	推奨値
HTTP 待機ポート番号	IWSS が ICAP の接続の受信を待機するポートです。	1344
ICAP over SSL を有効にする	セキュアな ICAP 通信を有効または無効にします。	無効にする
ICAPS ポート番号	IWSS が ICAPS の接続の受信を待機するポートです。	11344
証明書	クライアントからの SSL で保護されたリクエストに対するサーバ証明書をインポートします。	
秘密鍵	SSL で保護された通信に対する秘密鍵をインポートします。	
パスフレーズ	秘密鍵のパスフレーズを入力します。	
パスフレーズの確認	確認のためにパスフレーズをもう一度入力します。	

表 2-5. ICAP モード固有の設定 (続き)

構成パラメータ	詳細	推奨値
「X-Virus-ID」ICAP ヘッダを有効にする (チェックボックス)	検出された感染の ICAP 短縮名の記録を有効または無効にします。	有効にする
「X-Infection-Found」ICAP ヘッダを有効にする (チェックボックス)	検出された不正プログラムに関する ICAP 詳細と、その ICAP デバイスへの詳細の転送を有効または無効にします。	有効にする
「X-Authenticated-User」ICAP ヘッダを有効にする	ユーザ名情報に関する ICAP 詳細を有効 / 無効にします。	有効にする
「X-Authenticated-Groups」ICAP ヘッダを有効にする	グループメンバーシップ情報に関する ICAP 詳細を有効 / 無効にします。	無効にする

4. [次へ] をクリックします。

注意: ICAP モードで配信するには、配置ウィザードのすべての手順を完了します。配信が成功したというメッセージを受信したら、55 ページの「IWSS ICAP の設定」で示すように、IWSS ICAP のセットアップを実行します。

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

通常の透過設定

通常の透過モードでは、モード固有の設定が必要です。

通常の透過モードのモード固有の設定を行うには

1. [配信モード] 画面で [通常の透過モード] オプションを選択します。
詳細については、46 ページの「通常の透過モード」を参照してください。
2. [次へ] をクリックします。
3. [通常の透過設定] 画面で次の設定値を入力します。(表 2-6 を参照してください)。

表 2-6. 通常の透過モード固有の設定

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

4. [次へ] をクリックします。

製品のアクティベーション

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

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

IWSS をアクティベートするには

1. 配置ウィザードの [製品のアクティベーション] 画面に移動します。
2. IWSS のアクティベーションコードを入力します。
3. [次へ] をクリックします。

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

アクティベーションコードについて

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

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

xx-xxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx

この手順を開始する前に、以下を確認してください。

- 配信モードを選択していること
- モード固有の設定を行っていること

IWSS をアクティベートするには

1. 配置ウィザードの [製品のアクティベーション] 画面に移動します。
2. IWSS のアクティベーションコードを入力します。
3. [次へ] をクリックします。

結果

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

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

配信ステータス

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

「おめでとうございます!!IWSS の設定と配信が完了しました。

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

注意： このメッセージが表示されたら、ただちに IWSS の最新のソフトウェアアップデートを適用することをお勧めします。詳細については、第 3 章 (65 ページの「アップデート」) を参照してください。

配信後

配置ウィザードが正しく設定されると、IWSS によってデーモンが自動的に再起動されます。

- ・ 再起動後は、できるだけ早く IWSS をアップデートしてください。65 ページの「アップデート」を参照してください。
- ・ ICAP モードで配信した場合は、IWSS と連携する ICAP 対応キャッシュサーバを設定します。55 ページの「IWSS ICAP の設定」を参照してください。
- ・ インストールを検証します。295 ページの「製品のテストと設定」参照

IWSS ICAP の設定

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

1. 56 ページの「ICAP 1.0 対応キャッシュサーバの設定」
2. 61 ページの「キャッシュされた既存のコンテンツをアプライアンスから消去」

注意： 次の ICAP の設定手順は、32 ページの「X-Authenticated ICAP ヘッダのサポート」で一覧表示されている ICAP バージョンに適用されます。これらは参考までに提供されているため、詳細については、本来のドキュメントを参照してください。

ICAP 1.0 対応キャッシュサーバの設定

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

使用する ICAP クライアントに対応するプロセスを参照してください。

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

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

1. Web ブラウザのアドレスバーに `https://{サーバ IP アドレス}:8082` と入力し、Web コンソールにログオンします。

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

2. [Management] を選択します。
入力画面が表示されたら、ログオンユーザ名とパスワードを入力します。
3. 左のメニューから [ICAP] をクリックし、[ICAP Services] タブをクリックします。
4. [New] をクリックします。
[Add ICAP Service] 画面が開きます。
5. [ICAP service name] に英数字で名前を入力します。[OK] をクリックします。
6. 新しい ICAP サービス名を選択し、[Edit] をクリックします。
[Edit ICAP Service name] 画面が開きます。
7. 次の情報を入力または選択します。
 - a. ICAP のバージョン番号 (つまり、1.0)
 - b. ウイルス検索サーバのホスト名または IP アドレスを含むサービス URL、および ICAP ポート。初期設定の ICAP ポートは 1344 です。
 - ・ レスポンスモード：
`icap://{ICAP サーバの IP アドレス}:1344`
 - ・ リクエストモード：
`icap://{ICAP サーバの IP アドレス}:1344/REQ-Service`
ICAP サーバの IP アドレスは、IWSS ICAP の IP アドレスです。
 - c. 最大接続数 (1 ~ 65,535 の範囲)。初期設定値は、5 です。

- d. 接続のタイムアウト。これは、Blue Coat Port 80 Security Appliance がウイルス検索サーバからの応答を待つ秒数です。範囲は、60 ~ 65,535 の間隔です。初期設定のタイムアウトは 70 秒です。
 - e. サポートされた方法の種類を選択します (レスポンスモードまたはリクエストモード)。
 - f. 初期設定のプレビューサイズのゼロ (0) を使用します。
 - g. ICAP サーバから設定を取得するには、[Sense settings] をクリックします (推奨)。
 - h. ICAP サービスを検診のために登録するには、[Health Check Options] の [Register] をクリックします。
8. [OK] をクリックし、[Apply] をクリックします。

注意： 設定した ICAP サービスを編集することができます。サーバの設定を再度編集するには、サービスを選択して [Edit] をクリックします。

9. 応答またはリクエストモードポリシーを追加します。
- Visual Policy Manager には、Oracle 社の Java 2 Runtime Environment Standard Edition のバージョン 1.3.1 以降 (別称: Java Runtime、JRE) が必要です。ワークステーションにすでに JRE がインストールされている場合、Security Gateway は別のブラウザウィンドウを開いて Visual Policy Manager を起動します。ポリシーエディタを最初に起動すると、空のポリシーが表示されます。
- ワークステーションに JRE がインストールされていない場合、セキュリティの警告ウィンドウが開きます。作業を続行するには、[Yes] をクリックします。指示に従います。

レスポンスモードポリシーを追加するには

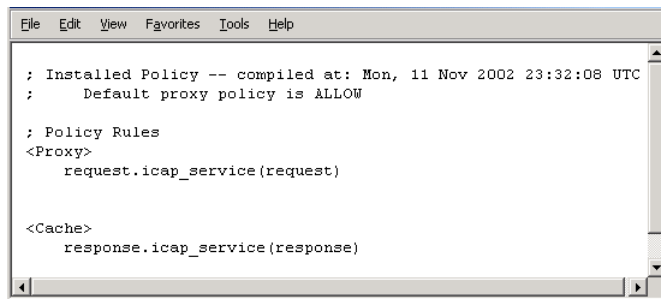
1. [Management] を選択します。
入力画面が表示されたら、ログオンユーザ名とパスワードを入力します。
2. 左のメニューから [Policy] をクリックし、[Visual Policy Manager] タブをクリックします。
3. [Start] をクリックします。[Java Plug-in Security Warning] 画面が表示された場合、[Grant this session] をクリックします。
4. メニューバーで [Edit] [Add Web Content Policy] の順に選択します。[Add New Policy Table] 画面が開きます。
5. [Select policy table name] にポリシー名を入力します。[OK] をクリックします。
6. [Action] 列で [Bypass ICAP Response Service] を右クリックし、[Set] をクリックします。[Add Object] 画面が開きます。[New] をクリックし、[Use ICAP Response Service] を選択します。[Add ICAP Service Action] 画面が開きます。

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

リクエストモードポリシーを追加するには

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

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

A screenshot of a web browser window titled "[Install Policies]". The window has a menu bar with "File", "Edit", "View", "Favorites", "Tools", and "Help". The main content area displays a configuration script for a proxy policy. The script includes comments about the installation date and default proxy policy, followed by policy rules for proxy and cache actions.

```
File Edit View Favorites Tools Help

; Installed Policy -- compiled at: Mon, 11 Nov 2002 23:32:08 UTC
;   Default proxy policy is ALLOW

; Policy Rules
<Proxy>
  request.icap_service(request)

<Cache>
  response.icap_service(response)
```

図 2-6. [Install Policies] 画面

Cisco CE ICAP サーバを設定するには

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

1. Cisco CE コンソールを開きます。
2. 設定モードに切り替えるには、「**config**」と入力します。

3. ICAP 関連のすべてのコマンドのリストを表示するには、「**icap?**」と入力します。
4. 次のように入力して応答変更サービスを作成します。

```
icap service RESPMOD SERVICE NAME
```

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

```
server icap://ICAP SERVER IP:1344/resp (サーバの種類を割り当てる)
vector-point respmod-precache (適切なベクタポイントの種類を割り当てる)
error-handling return-error (適切なエラー処理の種類を割り当てる)
enable (ICAP 複数サーバ設定を有効にする)
```

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

```
icap service REQUESTMOD SERVICE NAME
```

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

```
server icap://ICAP SERVER IP:1344/REQ-Service (サーバの種類を割り当てる)
vector-point reqmod-precache (適切なベクタポイントの種類を割り当てる)
error-handling return-error (適切なエラー処理の種類を割り当てる)
enable (ICAP 複数サーバ設定を有効にする)
```

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

```
icap append-x-headers x-client-ip (レポートの X クライアントヘッダを有効にする)
icap append-x-headers x-server-ip (レポートの X サーバヘッダを有効にする)
icap rescan-cache IStag-change (アップデートの IStag 再検索をオンにする)
icap bypass streaming-media (ICAP 検索からストリーミングメディアを除外する)
icap apply all (すべての設定を適用して ICAP の種類をアクティベートする)
show icap (現在の ICAP 設定をルート CLI メニューに表示する)
```

ウイルス検索サーバクラスタの設定

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

Web コンソールでクラスタを設定するには

1. [Management] を選択します。
入力画面が表示されたら、ログオンユーザ名とパスワードを入力します。
2. 左のメニューから [ICAP] をクリックし、[ICAP Clusters] タブをクリックします。
3. [New] をクリックします。
[Add ICAP Cluster] 画面が開きます。
4. [ICAP cluster name] に英数字で名前を入力し [OK] をクリックします。
5. 新しい ICAP クラスタ名を選択し、[Edit] をクリックします。
[Edit ICAP Cluster name] 画面が開きます。
6. クラスタに ICAP サービスを追加するには、[New] をクリックします。
[Add ICAP Cluster Entry] 画面が開きます。選択リストには、クラスタに追加できるすべてのサービスのリストが含まれます。
7. サービスを選択して [OK] をクリックします。
8. ICAP クラスタエントリを選択し、[Edit] をクリックします。
[Edit ICAP Cluster Entry name] 画面が開きます。
9. [ICAP cluster entry weight] で 0 ~ 255 から重み付けを割り当てます。
10. [OK] をクリックし、再度 [OK] をクリックしてから [Apply] をクリックします。

クラスタの設定またはエントリの削除

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

注意： Blue Coat Port 80 Security Appliance ポリシーで使用されるクラスタは、ポリシーのルールがクラスタ名を使用する場合、削除しないでください。

Web コンソールでクラスタの設定を削除するには

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

キャッシュされた既存のコンテンツをアプライアンスから消去

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

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

1. [Management] を選択します。
入力画面が表示されたら、ログオンユーザ名とパスワードを入力します。
2. [Maintenance] をクリックします。
3. [Tasks] タブをクリックし、[Clear] をクリックします。[OK] をクリックして確認します。

Cisco ICAP サーバのキャッシュを消去するには

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

IWSS が ICAP 要求を待機していることを確認する

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

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

コマンドと出力の例は次のとおりです。

```
[root@iwss65-40 ~]# netstat -nat |grep 1344
tcp 0 0 0.0.0.0:1344 0.0.0.0:*
LISTEN
tcp 0 0 127.0.0.1:12983 127.0.0.1:1344
```

```
TIME_WAIT
tcp 0 0 10.204.151.40:1344 10.204.151.52:37708
ESTABLISHED
tcp 0 0 10.204.151.40:1344 10.204.151.52:37707
ESTABLISHED
tcp 0 0 127.0.0.1:12987 127.0.0.1:1344
TIME_WAIT
tcp 0 0 127.0.0.1:12991 127.0.0.1:1344
TIME_WAIT
tcp 0 0 127.0.0.1:12979 127.0.0.1:1344
TIME_WAIT
tcp 0 0 127.0.0.1:12975 127.0.0.1:1344
TIME_WAIT
```

リクエストモードとレスポンスモードの違いについて

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

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

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

リクエストモード処理をトリガする

次に示す手順は、特に IWSS を介したリクエストモード処理のトリガに適用されます。

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

アウトバウンド URL は、IWSS に渡されブロックされます。

レスポンスモード処理をトリガする

次に示す手順は、特に IWSS を介したレスポンスモード処理のトリガに適用されます。

1. IWSS にトラフィックを渡すクライアントにログインします。
2. Web ブラウザを開き、サイト www.eicar.org を開きます。
3. [AntiMalware Testfile] と表示されたボタンをクリックします。
4. ページの一番下までスクロールすると、[Download area using the standard protocol http] と書かれた場所にテストファイルが表示されています。
5. `ecar.com.txt` ファイルを選択してダウンロードします。

アウトバンド URL が有効なので、リクエストモードではこの URL は通過できます。トラフィックの応答 実際にはダウンロードしようとする IWSS でダウンロードの実行がブロックされます。

アップデート

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

本章で説明する内容には、次の項目が含まれます。

- ・ 66 ページの「製品サポート」
- ・ 66 ページの「アップデート機能について」
- ・ 67 ページの「プロキシ設定 (アップデート用)」
- ・ 68 ページの「アップデート可能なコンポーネント」
- ・ 74 ページの「手動アップデート」
- ・ 76 ページの「予約アップデート」
- ・ 77 ページの「アップデートの操作方法」

製品サポート

トレンドマイクロは、報告された既知の問題に対処する Patch を不定期にリリースしています。最新 Patch の有無については、以下 URL からご確認いただけます。

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

サポート契約の更新

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

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

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

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

<https://clp.trendmicro.com/fullregistration>

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

アップデート機能について

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

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

IWSS 管理コンソールからアップデートする方法

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

- ・ 次の間隔 (15 分、30 分、45 分、60 分)

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

- ・ 毎時
- ・ 毎日
- ・ 毎週
- ・ 手動

注意： パターンファイルを毎時、エンジンを毎日または毎週アップデートすることをお勧めします。

すべてのアップデートには、ウイルスパターンファイル、スパイウェアパターンファイル、ボットパターンファイル、IntelliTrap パターンファイル、IntelliTrap 除外パターンファイル、スマートスキャンエージェントパターンファイル、スクリプトアナライザパターンファイル、およびプロトコル情報抽出パターンファイルが含まれています。

すべてのアップデートには、ウイルス検索エンジン、高度な脅威検索エンジン、および URL フィルタエンジンが含まれています。

プロキシ設定 (アップデート用)

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

- ・ トレンドマイクロのアップデートサーバからのコンポーネントのアップデート
- ・ 製品の登録およびライセンス確認

- Web レピュテーション検索
- 証明書失効リスト (CRL) のアップデート
- Trend Micro Global Smart Protection Server (SPS) へのスマートスキャンクエリ

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 Web コンソールを開いて、[アップデート] [接続設定] の順に選択します。
2. [コンポーネント、ライセンス、Web レピュテーションクエリのアップデートにプロキシサーバを使用する] を選択して、プロキシサーバまたはポートを指定します。IWSS は、IPv4 と IPv6 の両方の ActiveUpdate サーバをサポートしています。アップデートプロキシでは、IPv6 プロキシまたは、ホスト名が IPv4/IPv6 アドレスによる IPv4 プロキシもサポートしています。
3. プロキシサーバで認証が必要な場合は、[ユーザ ID] と [パスワード] にそれぞれ入力します。認証を必要としないプロキシサーバの場合は、このフィールドを空欄のままにします。
4. 最新のパターンファイルにアップデートした後、[パターンファイル] に IWSS デバイスに保存しておくパターンファイルの数を入力します (初期設定および推奨設定は 3 パターンファイル)。

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

5. [保存] をクリックします。

アップデート可能なコンポーネント

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

- パターンファイル—パターンファイルには、ウイルスパターンファイル、スパイウェアパターンファイル、ポットパターンファイル、IntelliTrap パターンファイル、IntelliTrap 除外パターンファイル、スマートスキャンエージェントパターンファイル、スクリプトアナライザパターンファイル、およびプロトコル情報抽出パターンファイルが含まれています。これらのファイルは、既知のセキュリティ上の脅威のバイナリ「シグネチャ」やパターンを格納しています。検索エンジンと同時に使用すると、それらがインターネットゲートウェイを通過する際に 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通常、週に数回提供されています。一方、スパイウェアパターンファイルはそれほど頻繁にはアップデートされません。

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

ウイルスパターンファイル

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

トレンドマイクロのウイルス対策プログラムでアップデート機能（詳細については 66 ページの「アップデート機能について」を参照）を使用すると、新しいウイルスパターンファイルがサーバに用意されたことを検出できます。また、1 時間おき、1 日おき、1 週間おきなどに最新ファイルを取得するよう自動的にサーバにポーリングを予約しておくことも可能です。ウイルスパターンファイルの最新情報は、次の Web サイトで参照できます。

<https://appweb.trendmicro.com/ecs/Default.aspx>

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

ウイルスパターンファイルの仕組み

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

パターンファイル名は次のとおりです。

`lpt$vpn.###`

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

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

- ・ ルール番号 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、新しいウイルスパターンファイルを随時提供しています (通常、週に数回更新しています)。[アップデート] [予約] 画面から毎時の自動アップデートを設定しておくことをお勧めします。アップデートは、有効なサポート契約をお持ちであればどなたでもご利用いただけます。

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

スパイウェアパターンファイル

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

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

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

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

- ・ ルール番号 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)。

ボットパターンファイル

ボットネットとは、共通のコマンドと制御インフラストラクチャの下で、通常、ワーム、トロイの木馬、またはバックドアなどと呼ばれるプログラムを実行する感染コンピュータの集合を指します。トレンドマイクロではボットネット URL を収集し、それらをボットパターンファイルに取り入れています。ボットパターンファイルには既知のボットネット URL の暗号化されたリストが含まれています。ボットパターンファイルは初期設定で以下のディレクトリに保存されます。

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

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

IntelliTrap の検出では、IntelliTrap パターンファイル (不正プログラムが潜んでいる可能性のあるファイル検出用) および IntelliTrap 除外パターンファイル (許可リストとして使用) とともにトレンドマイクロのウイルス検索エンジンの検索オプションが使用されます。IWSS では、IntelliTrap オプションおよびパターンファイルを使用して、圧縮ファイル内のボットなど、不正なプログラムが含まれる圧縮ファイルを検出します。ウイルス作成者は、複数のファイル圧縮スキームを使用して、ウイルスフィルタを回避しようとしています。IntelliTrap では、圧縮ファイルのヒューリスティック評価を提供することにより、ボットまたはその他の不正なプログラムを含む圧縮ファイルがネットワークに与えるリスクを軽減します。

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

スマートスキャンエージェントパターンファイル

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

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

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

スクリプトアナライザ (SA) パターンファイル

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

パターンファイル名は次のとおりです。

```
tmsa.ptn.#####
```

プロトコル情報抽出パターンファイル

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

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

検索エンジン

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

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

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

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

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

検索エンジンのアップデートについて

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

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

Web レピュテーションデータベース

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

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

- ・ Web カテゴリ
- ・ ファーミング、フィッシング、および C&C コールバック試行の検出で使用するファーミング、フィッシング、および CCCA フラグ
- ・ 指定されたセキュリティレベルに基づき、URL アクセスのブロックに使用される Web レピュテーションスコア (157 ページの「Web レピュテーションルールの指定」を参照)

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

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

<https://global.sitesafety.trendmicro.com/>

パターンファイルおよびエンジンの差分アップデート

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

コンポーネントのバージョン情報

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

手動アップデート

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

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

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

エンジンおよびパターンファイルをアップデートするには

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

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

強制手動アップデート

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

IWSS 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 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

IWSS は次のパターンファイルについて予約アップデートを実行できます。

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

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

パターンファイルおよびエンジンの自動アップデートを予約するには

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

次のオプションが用意されています。

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

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

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

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

アップデートの操作方法

アップデート通知

IWSS では、パターンファイルまたはエンジンのアップデート状況を事前に管理者に知らせる通知を発行できます。アップデートに関する通知の設定方法については、256 ページの「パターンファイルのアップデート通知の有効化」および 261 ページの「URL フィルタエンジンおよび検索エンジンのアップデートの通知の有効化」を参照してください。

アップデートのロールバック

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を使用して、インバウンドとアウトバウンドのトラフィックにウイルス検索を実行します。最新のパターンファイルは、ファイルの拡張子で判別されます。たとえば、lpt\$vpn.401 は、lpt\$vpn.400 より新しいファイルです。

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

注意： 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。

パターンファイルまたは検索エンジンをロールバックするには

1. 管理コンソールから [アップデート] [手動] の順に選択します。
2. ロールバック対象のコンポーネントを選択し、[ロールバック] をクリックします。
ロールバックの進行状況を示すバーが表示され、ロールバック結果を示すメッセージ画面が表示されます。

パターンファイルの削除

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

アプリケーション制御

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

本章で説明する内容には、次の項目が含まれます。

- ・ 80 ページの「アプリケーション制御の概要」
- ・ 80 ページの「アプリケーション制御ポリシーリスト」

アプリケーション制御の概要

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

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

注意： アプリケーション制御はプロキシ転送モードでのみ使用可能です。

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

アプリケーション制御ポリシーリスト

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

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



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

アプリケーション制御ポリシーリストには、有効にされたものも無効にされたものも含め、システム上のすべてのポリシー (IPv4 および IPv6 アドレス用) が表示されます。[アプリケーション制御]

[ポリシー] に移動します。新規ポリシーを作成するには [追加] をクリックします。既存のポリシーを編集するにはそのポリシー名をクリックします。

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

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

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

アプリケーション制御ポリシーを表示するには

1. [アプリケーション制御] [ポリシー] に移動します。
2. 既存のポリシーの名前をクリックして、そのポリシーに関する詳細を表示します。
アプリケーション制御グローバルポリシーは、初期設定のポリシーです。

3. ポリシーを追加するには、83 ページの「アプリケーション制御ポリシーの追加」を参照してください。

ポリシーの追加 : アカウントの選択

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

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

アプリケーション制御グローバルポリシーは、初期設定のポリシーです。

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

注意： この画面のオプションは、使用しているユーザの識別方法に応じて異なります。[IP アドレス]、[ホスト名 (変更された HTTP ヘッダ)]、または [ユーザ / グループ名認証] (LDAP) のいずれかになります。ユーザの識別方法の設定とポリシー範囲の定義方法については、108 ページの「ユーザ識別方法の設定」と 116 ページの「ポリシーの範囲の設定」を参照してください。

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

アプリケーション制御ポリシーの追加

アプリケーション制御ポリシーを追加するには

1. [アプリケーション制御] [ポリシー] に移動します。
2. ポリシーリストの上部にある [追加] リンクをクリックします。
3. わかりやすい [ポリシー名] を新しく入力します。これにより、ポリシーを覚えやすくなります。
4. また、[既存ポリシーからコピー] オプションをクリックして、ドロップダウンリストからポリシーを選択することで、既存のポリシーの設定に基づいて新規ポリシーを作成することもできます。
5. 単一の IP アドレス、IP アドレス範囲、IP サブセット、またはユーザ / グループ名を入力して、影響を受けるユーザを示します。
6. [追加] をクリックして、新規に作成した IP アドレス、IP アドレスの範囲、またはユーザ / グループ名を [種類] テーブルと [識別設定] テーブルに移動します。
7. 画面上部の [ポリシーを有効にする] チェックボックスをオンにして、作成したポリシーを有効にします。
8. 作業を続行するには、[次へ] をクリックします。
9. 指定したアカウントに適用するポリシーのルールをセットアップするには、84 ページの「アプリケーション制御ポリシールールの指定」を参照してください。

ポリシーの追加または編集：アプリケーション制御ポリシーのルールの指定

次の 2 つのメニューでポリシールールを追加または編集します。

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

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

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

アプリケーション制御ポリシーの指定

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

- ・ ポリシーを有効にする 個々のポリシーを有効または無効にします。ただし、アプリケーション制御のグローバルポリシー設定は、個々のポリシー設定より優先されます。
- ・ アプリケーションカテゴリ アクセスを制限するプロトコルに対する処理を選択します。25の論理グループに分けられた 1000 以上のプロトコルがあります。特定のアプリケーション名を見つけるには、検索フィールドを使用します。
 - ・ 「+」記号をクリックしてカテゴリを展開し、特定のプロトコルを選択します。
 - ・ プロトコル名をクリックし、プロトコルの説明が表示される画面にアクセスします。

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

使用可能なフィルタ処理には次のものがあります。

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

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

- ・ オプション 1: アプリケーション検索のフィルタ
 - ・ [アプリケーション検索] にアプリケーション名を入力して [検索] ボタンをクリックすると、アプリケーションがフィルタリングされます。
 - ・ 処理を設定するアプリケーションを選択します。
 - ・ [処理] に移動し、選択したアプリケーションに適用する処理を選択します。
- ・ オプション 2: 詳細な処理検索のフィルタ
 - ・ [詳細な処理検索] から処理を選択して [検索] ボタンをクリックすると、その処理を選択可能なアプリケーションがフィルタリングされます。
 - ・ アプリケーション処理リストの [詳細オプション] で、処理を 1 つ以上選択して適用します。
- ・ 許可 ユーザアカウントはアプリケーションを通常どおり使用できます。管理者がこの設定を有効にしている場合、アプリケーション制御イベントが記録されます。
- ・ ブロック ユーザアカウントはこのアプリケーションを使用できません。このアプリケーションの一部として識別されるネットワークパケットは配信されません。このイベントについてはログエントリも作成できます。
- ・ 次のポリシーに一致 次のポリシー設定を使用します。この処理はグローバルポリシーおよびゲストポリシーには存在しません。
- ・ スケジュール 処理を適用するプロトコルの時間オブジェクトを選択します。制限する日数と時間は、[管理] [一般設定] [予約期間] で定義されます。(詳細については、278 ページの「予約期間」を参照してください)。選択したプロトコルにフィルタ処理を適用するには、[保存] をクリックします。

注意： 設定は HTTP サービスの再ロード後に適用されます。

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

HTTP 設定

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

本章で説明する内容には、次の項目が含まれます。

- ・ 88 ページの「HTTP/HTTPS トラフィックフローの有効化」
- ・ 88 ページの「プロキシ設定および関連するその他の設定」
- ・ 96 ページの「ネットワーク設定および負荷の処理」
- ・ 97 ページの「インターネットアクセス管理の設定」

HTTP/HTTPS トラフィックフローの有効化

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

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

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

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

プロキシ設定および関連するその他の設定

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

- ・ **プロキシ転送モード** クライアントが不正な HTTP/HTTPS/FTP による脅威をサーバから受信しないように防ぐ設定です。最もよく使われる設定で、代表的な使用例はネットワークに接続する Web ユーザが不正なインターネットダウンロードを受信しないように防ぐ用法です。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。
- ・ **リバースプロキシモード** 一般ユーザや個人ユーザが招いた攻撃や不正プログラムから Web サーバを保護するための設定です。
- ・ **ICAP モード** ICAP クライアントがネットワーク上にあり、検索のためトラフィックを 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。
- ・ **通常の透過モード** L4 スイッチが HTTP トラフィックを IWSS に移動させるように設定されています。このオプションでは IPv6 はサポートされていません。

プロキシ設定

プロキシ設定には、次のような種類があります。

- ・ 上位プロキシなし (スタンドアロンモード)
- ・ 上位プロキシあり (依存モード)
- ・ 通常の透過 (透過プロキシモード)
- ・ 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)

最も簡単な設定は、上位プロキシを使用しないスタンドアロンモードで IWSS を設置することです。この場合、IWSS がクライアントのプロキシサーバの役割を果たします。この設定の利点は、比較的簡単なことと、プロキシサーバを個別に用意する必要がないことです。プロキシ転送をスタンドアロンモードにするマイナス点は、各クライアントがブラウザのインターネット接続設定から IWSS デバイスをプロキシサーバに設定しなくてはならない点です。これにはネットワークユーザの協力が必要になります。



図 5-1. 上位プロキシなしのプロキシ転送

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

スタンドアロンの設置を設定するには

1. 管理コンソールから [管理] [配置ウィザード] の順に選択します。
配置ウィザードが表示されます。
2. [プロキシ転送モード] が選択されていることを確認します。[次へ] をクリックします。
3. [上位プロキシを有効にする] チェックボックスがオフであることを確認します。
4. [送信] ボタンが表示されるまで、[次へ] をクリックします。[送信] をクリックします。[閉じる] をクリックします。

上位プロキシあり (依存モード)

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、その要求が要求側サーバに転送されます。

スタンドアロンモードと同様、依存モードのプロキシ設定でも、クライアントユーザがインターネット接続設定で IWSS デバイスをプロキシサーバに設定する必要があります。上位プロキシを使用する利点は、上位プロキシサーバにコンテンツがキャッシュされるためパフォーマンスが向上することです。上位プロキシを使用すると、プロキシサーバにキャッシュされた画面がすばやく表示されるようになります。

注意： 指定されたプロキシサーバを IWSS が使用して、上位プロキシモードで動作するように設定する場合、そのプロキシサーバに対してアップデート用のプロキシ設定も設定することをお勧めします（67 ページの「プロキシ設定（アップデート用）」を参照）。特定の種類のアップデートイベントは、アップデートプロキシ設定を利用して重要な情報を取得します。プロキシ設定が正しく行われていないと、IWSS はインターネットを介してそれらのサービスにアクセスできなくなります。



図 5-2. 上位プロキシを使用したプロキシ転送

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、ファームウェアはブロックできません。

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

上位プロキシと動作するよう **IWSS** を設定するには

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

通常の透過 (透過プロキシモード)

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

IWSS では、「通常」の透過をサポートしています。通常の透過 (透過プロキシモード) は、ほとんどのレイヤ 4 スイッチでサポートされています。さまざまなベンダー製の多種多様なネットワークハードウェアに対応していますが、通常の透過の設定には次のような制約事項があります。

- FTP over HTTP は使用できません。このため、FTP 接続を許可しないファイアウォール設定では、ftp:// で始まる URL へのリンクは機能しません。または ftp:// で始まる URL に接続できても、ファイルが検索されません。
- ホスト情報を格納しない HTTP 要求があった場合、旧バージョンの Web ブラウザの中には通常の透過に対応できないものがあります。
- IWSS には不正なトラフィックの検索およびクリーンアップ対象となるクライアントの IP アドレスが必要なため、IWSS の下位で NAT (IP マスカレード) を使用しないでください。

透過を有効にすると、クライアント側の設定を変更しなくても IWSS でクライアントの HTTP 要求を処理して検索できる利点があります。エンドユーザにとって便利な設定であるばかりでなく、インターネット接続設定を変更しただけでクライアントがセキュリティポリシーから除外されてしまうことを防ぐことができます。

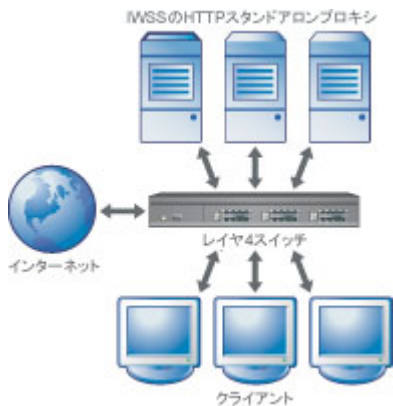


図 5-3. 透過を使用するプロキシ転送

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。

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

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

この配信モードでは IPv6 はサポートされていません。

通常の透過を設定するには

1. 管理コンソールから [管理] [配置ウィザード] の順に選択します。
配置ウィザードが表示されます。
2. [通常の透過モード] を選択して、[次へ] をクリックします。

3. レイヤ 4 スイッチが使用するように設定されているポートと同じポートに [HTTP 待機ポート番号] を変更します。
4. [送信] ボタンが表示されるまで、[次へ] をクリックします。[送信] をクリックします。[閉じる] をクリックします。

リバースプロキシ

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

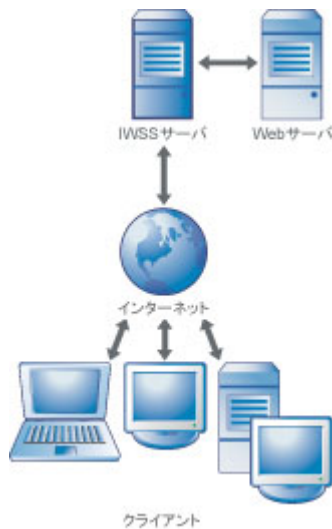


図 5-4. クライアントから Web サーバをリバースプロキシで保護

IWSS をリバースプロキシとして設定するには

1. 管理コンソールから [管理] [配置ウィザード] の順に選択します。配置ウィザードが表示されます。
2. [リバースプロキシモード] を選択して、[次へ] をクリックします。
3. HTTP 待機ポート番号、保護対象サーバの IP アドレスとポート番号を入力します。
4. 必要に応じて [SSL ポート を有効にする] チェックボックスをオンにして [SSL ポート番号] を入力し、証明書と秘密鍵をアップロードしてから、一致するパスフレーズを入力します。

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

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

このモードでは、DLP 機能は無効になります。

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

プロキシに関する設定

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

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

HTTP 待機ポート

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

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

注意： 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、コンテンツを復号化するように HTTPS 復号化ポリシーを設定します。これにより、「通常」の HTTP トラフィックとしてフィルタポリシーおよび検索ポリシーを通過することができます。IWSS では最初の CONNECT 要求を検証し、設定したパラメータと一致しない場合は拒否します。その例としては、対象となる URL がブロックリストにある場合や、使用ポート番号が許可されていない場合があります。

FTP over HTTP の匿名ログオンに使用するメールアドレス

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

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

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

ネットワーク設定および負荷の処理

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

次のモードでネットワーク上に IWSS を設置できます。

- プロキシ転送 Linux で設定されたインターフェースから内部ネットワークデバイスへケーブルを接続します。
- ICAP Linux で設定されたインターフェースを使用して、IWSS を ICAP クライアントへ接続します。

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

インターネットアクセス管理の設定

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

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

クライアントとサーバの識別

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

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

クライアント IP による設定

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

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

HTTP アクセスをクライアント IP によって許可するには

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

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

クライアントの指定方法の詳細については、97 ページの「クライアントとサーバの識別」を参照してください。

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

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

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

7. [保存] をクリックします。

サーバ IP の除外リスト

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

信頼するサーバの IP アドレスまたは IP 範囲を設定すると、その設定内容は `/etc/iscan/ServerIPWhiteList_http.ini` 設定ファイルに保存されます。

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

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

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

サーバ IP アドレスの許可リストにサーバを追加するには

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

クライアントの指定方法の詳細については、97 ページの「クライアントとサーバの識別」を参照してください。

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

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

信頼するサーバ、サーバ範囲、または IP サブセットを削除するには、その横にある [削除] アイコンをクリックします。

6. アクセス管理の設定は、[サーバ IP の除外リスト] タブの下部にあるリストでの表示順序に従って評価されます。
7. [保存] をクリックします。

宛先ポートによる制限

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

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

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

各種アプリケーションおよびサービスで使用するポートの一覧については、
<http://www.iana.org/assignments/port-numbers> を参照してください。

クライアントから接続できる宛先ポートを制限するには

1. 管理コンソールで [HTTP] [設定] [アクセス管理の設定] の順に選択します。
2. [宛先ポート] タブがアクティブになっていることを確認します。
3. 実行する [処理] を選択します。宛先サーバの特定のポート番号またはポート範囲に接続できないようにするには [拒否] を、特定のポート番号またはポート範囲に接続できるようにするには [許可] を選択します。
4. [ポート] または [ポート範囲] を選択して、対応するポート番号を入力します。
5. [説明] にわかりやすい名前を入力します (40 文字以内)。
6. [追加] をクリックします。宛先ポート制限が、[宛先ポート] タブの下部にあるリストに追加されます。

アクセスを許可またはアクセスを拒否する宛先ポート番号または宛先ポート範囲を削除するには、その隣の [削除] アイコンをクリックします。

7. アクセス管理の設定は、[宛先ポート] タブの下部にあるリストでの表示順序に従って評価されます。

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

8. [保存] をクリックします。

HTTPS ポートによる設定

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

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

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

1. 管理コンソールで [HTTP] [設定] [アクセス管理の設定] の順に選択します。
2. [HTTPS ポート] タブをアクティブにします。
3. [HTTPS ポート] を [拒否] または [許可] のいずれかに選択します。
4. [ポート] または [ポート範囲] を選択して、対応するポート番号を入力します。
5. [説明] にわかりやすい名前を入力します (40 文字以内)。
6. [追加] をクリックします。宛先ポート制限が [HTTPS ポート] タブの下部にあるリストに表示されます。
設定した HTTPS ポートアクセス制限を削除するには、削除するポート番号またはポート範囲の隣の [削除] アイコンをクリックします。
7. アクセス管理設定は、[HTTPS ポート] タブの下部のリストに表示された順序で評価されます。リスト内に表示されるポートの順序を変更するには、[評価順] 列の上向き矢印または下向き矢印をクリックします。
8. [保存] をクリックします。

ポリシーとユーザ識別方法

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

本章で説明する内容には、次の項目が含まれます。

- ・ 104 ページの「ポリシーの仕組み」
- ・ 105 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」
- ・ 107 ページの「ポリシーの配信」
- ・ 108 ページの「ユーザ識別方法の設定」
- ・ 117 ページの「LDAP を使用したポリシー設定」

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。IWSS ポリシーは、HTTP/HTTPS 検索ポリシーや URL フィルタポリシーなどと同様に、IPv6 クライアントおよびサーバに適用できます。すべてのユーザ識別方法が、IPv6 環境（クライアント IP が IPv6）でも機能します。クライアントおよびサーバのアクセス管理では、IPv6 ホストをサポートする必要があります。次に、セキュリティポリシー種類別にいくつかの例を示します。

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

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

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

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

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

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

初期設定のグローバルポリシーとゲストポリシー

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

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

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

ゲストアカウントは初期設定で無効になっています。ゲストアカウントを有効にするには、LDAP を有効にしてからのみ、[管理] [一般設定] [ユーザの識別] [認証方法] [キャプティブポータル] [ゲストログインの許可] に移動します。107 ページの「ゲストアカウントの有効化」を参照してください。

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

ゲストポリシーについて

ゲストポリシーは、ゲストユーザに適用される唯一のポリシーです。

「ユーザ / グループ名認証」によるユーザ識別方法を有効にする方法については、110 ページの「ユーザ / グループ名認証」を参照してください。

ゲストポートの有効化

プロキシ転送モードで配置ウィザードを使用して、ゲストポートを有効化します。

ゲストポートを有効にするには

1. [配信モード] 画面で [プロキシ転送モード] オプションを選択します。
詳細については、43 ページの「プロキシ転送モード」を参照してください。
2. [次へ] をクリックします。
3. [ゲストユーザログインを有効にする] を選択して、ポート番号 8081 (初期設定の値) を使用します。
4. [次へ] をクリックします。
5. その他の初期設定のプロキシ転送設定を変更せずに、[保存] をクリックします。

ゲストアカウントの有効化

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

ゲストアカウントを有効にするには

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

ポリシークエリ

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

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

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

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

ポリシーの配信

ポリシーの設定後、[保存] をクリックすると設定がデータベースに書き込まれます。[ポリシーの配信] をクリックすると、新しいポリシー設定がただちに適用されます。クリックしない場合は、[管理] [一般設定] [ポリシー配信] 画面の [ポリシー配信設定 (分)] で指定した時間が経過後、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。

ユーザ識別方法の設定

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

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。

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

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

表 6-1. さまざまな配信モードでサポートされているユーザ識別方法

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

IP アドレス

IP アドレスは初期設定の識別オプションで、以下の条件が必要です。

- ・ DHCP では DHCP リースの有効期限が切れることによって IP アドレス識別が不正確になるため、クライアント IP アドレスを DHCP 経由で動的に割り当てていないこと。
- ・ 影響を受けるシステムと 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。

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

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

IP アドレスによるユーザ識別方法を有効にするには

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

クライアント登録ユーティリティ

ホスト名 (変更された HTTP ヘッダ) のユーザ識別オプションを使用するには、クライアントが 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、`/usr/iwss/bin` (IWSS コンピュータ) に配置されています。このプログラムは、ローカル Windows ドメインにログオンスクリプトから呼び出すとクライアントに効果的に配信できます。

このプログラムは、次のレジストリエントリを修正することにより機能します。

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

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

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

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

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

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

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

ユーザ/グループ名認証

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

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

LDAP 認証方法

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

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

表 6.2. サポートしている LDAP サーバで使用できる認証方法

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

表 6-2. サポートしている LDAP サーバで使用できる認証方法 (続き)

	Kerberos	シンプル認証	NTLM
Linux OpenLDAP 2.2.16、2.3.39、2.4.11	使用可	使用可	使用不可

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

LDAP の通信フロー

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

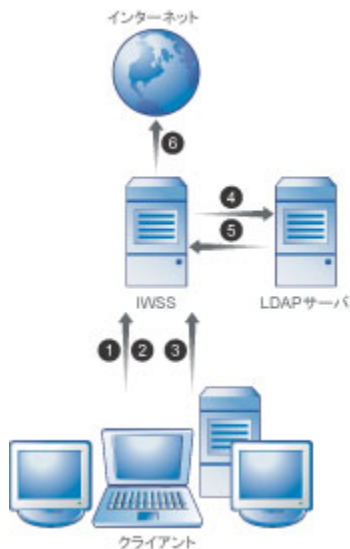


図 6-1. Kerberos 認証による LDAP 通信フロー

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

注意： 各クライアントコンピュータ上で自動認証を有効にするように、IE 設定を行う必要があります。IE 7.0 以降では、初期設定で自動認証が有効になっています。

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

- ・ 単一のドメイン (LAN または 802.11)
- ・ 複数のドメイン環境で有効なグローバルカタログ (LAN または 802.11)

IE で自動認証を有効にするには

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

Firefox で自動認証を有効にするには

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

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

LDAP 設定

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

注意： LDAP ディレクトリにアカウントを持たないネットワークユーザにゲストポリシーを適用するには、[認証方法] でゲストアカウントを有効にします。ゲストアカウントを有効にする方法の詳細については、107 ページの「ゲストアカウントの有効化」を参照してください。

ユーザ / グループ名認証方法を使用するよう **IWSS** を設定するには

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

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

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

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

9. [LDAP サーバのホスト名] を完全修飾ドメイン名 (FQDN) で入力します。
10. [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=example, DC=com」と入力します。

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

11. LDAP 認証方法に [シンプル]、[ダイジェスト - MD5]、[Kerberos] のいずれかを選択します。

詳細認証を使用するには、さらに次のパラメータも設定します。

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

Internet Explorer を介した異なるフォレスト上の鍵発行局 (KDC) の認証に NTLM を使用している場合、または Active Directory でのリフェラル追跡に 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] タブ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、キーブアライブ接続が停止されるのを防ぎます。NTLM を使用できるのは、Microsoft Active Directory だけです。注意してください。

12. ホストを LDAP 認証プロセスから除外するように [認証の許可リスト] を設定します。
たとえば、インターネットにアクセスするアプリケーションサーバがある場合、サーバによる認証を要求することなくアクセスを許可するには、LDAP 認証の許可リストにサーバの IP アドレスを追加します。
IWSS は IP アドレスベースのポリシー設定のみを適用し、ユーザ / グループ名のチェックを省略します。
IWSS は、IPv6 からの LDAP クエリを IPv4 の場合と同様にサポートします。LDAP クライアントの許可リストでは、IPv6 アドレスも IPv4 と同様にサポートします。
13. 情報が正しく入力されたかどうか、および設定した LDAP サーバと IWSS が通信できるかどうかを検証するには、[ユーザの識別設定] 画面で [LDAP 接続のテスト] をクリックします。
LDAP サーバと正常に接続されたことを示すメッセージが表示されます。
14. [保存] をクリックします。

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

クロスドメインの Active Directory オブジェクトクエリ

Microsoft Active Directory を使用する際にグローバルカタログポート (3268) を 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必要があります。ユニバーサルグループ範囲を使用したグループの作成では、クロスドメインクエリも実行できます。グローバルカタログが有効になっている場合は、グローバルグループポリシーを作成したり使用したりしないようにします。

注意： 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。

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

ポリシーの範囲の設定

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

この手順は次のとおりです。

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

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

ポリシーを追加してポリシー適用範囲を設定する前に、ユーザ識別方法を設定します。詳細については、108 ページの「ユーザ識別方法の設定」を参照してください。

IP アドレスを使用したポリシー設定

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

IP アドレスでポリシー適用範囲を設定するには

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

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

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

LDAP を使用したポリシー設定

LDAP サーバのユーザ名またはグループ名を使用してポリシーを設定する前に、ユーザ識別方法を設定し、使用する LDAP サーバの詳細を入力します。詳細については、113 ページの「LDAP 設定」を参照してください。

ユーザ / グループ名でポリシー範囲を設定するには

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

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

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

HTTP 検索の設定

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

- ・ 120 ページの「HTTP 検査の概要」
- ・ 141 ページの「情報漏えい対策」
- ・ 144 ページの「HTTPS のセキュリティ」
- ・ 155 ページの「高度な脅威保護ポリシーの作成と変更」
- ・ 174 ページの「高度な脅威保護のパフォーマンスに関する注意事項」
- ・ 175 ページの「X-Forwarded-For HTTP ヘッダ」

HTTP 検査の概要

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

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

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

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

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

HTTP 検査ポリシー

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

- ・ 121 ページの「HTTP 検査: アカウントの選択」
- ・ 122 ページの「HTTP 検査: ルールの指定」
- ・ 125 ページの「HTTP 検査: 除外リストの指定」

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

HTTP 検査: アカウントの選択

HTTP 検査ポリシーを追加するには、フィルタが必要です。初期設定のフィルタがいくつか用意されていますが、カスタムフィルタを使用するポリシーを作成するには、最初に [HTTP] [HTTP 検査] [フィルタ] でフィルタを作成する必要があります。条件を満たすアカウントには、IPv4 アカウントまたは IPv6 アカウント、あるいはその両方の単一の IP アドレス、IP アドレス範囲、または IP サブセットと、ホスト名、ユーザ名、またはユーザ識別が有効な場合はグループ名が含まれています。

HTTPS 検査を有効にするには

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

HTTP 検査ポリシーに使用するアカウントを選択するには

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

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

- ・ 新規ポリシーの作成 ポリシールールを簡単でわかりやすい名前を入力します。名前は一意である必要があり、[HTTP] [HTTP 検査] [ポリシー] の順に選択して表示されるポリシーリストに表示されます。
- ・ 識別設定 この画面のオプションは、使用しているユーザの識別方法に応じて異なります。[IP アドレス]、[ホスト名 (変更された HTTP ヘッダ)]、または [ユーザ / グループ名認証 (LDAP)] のいずれかになります。ユーザの識別方法の設定とポリシー適用範囲の設定の詳細については、108 ページの「ユーザ識別方法の設定」を参照してください。

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

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

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

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

HTTP 検査：ルールの指定

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

HTTP 検査ポリシーにルールを指定するには

1. 121 ページの「HTTP 検査ポリシーに使用するアカウントを選択するには」の手順を実行します。

TREND MICRO InterScan™ Web Security Suite

システムステータス
ダッシュボード
+ アプリケーション制御
- HTTP
+ HTTPS復号化
+ 高度な脅威保護
- HTTP検査
ポリシー
フィルタ
+ 情報漏えい対策
+ URLフィルタ
アクセス割り当てポリシー
+ URLアクセス設定
+ 設定
+ FTP
+ ログ
レポート
+ アップデート
通知
+ 管理

HTTP検査ポリシー: ポリシーの追加

HTTP検査ポリシー > (新規ポリシー) ポリシーを有効にする

1. アカウントの選択
2. ルールの指定
3. 除外リストの指定

新規ポリシーの作成: *
 既存ポリシーからコピー: * 選択

IP範囲:
開始:
終了:

種類	識別設定

IPアドレス:

IPサブセット:
アドレス:
接頭辞の長さ:

備考: IPまたはユーザ/グループ名を使用してアカウントを選択するには、次のタブでユーザの識別方法を変更してください。【管理】→【一般設定】→【ユーザの識別】。

図 7-1. 指定したソーシャルネットワーキングサイトへのコンテンツ投稿をすべてブロックする HTTP 検査ポリシーの設定

2. 次の情報を入力または指定します。

- ・ **ポリシーを有効にする** 個々のポリシーを有効または無効にします。ただし、HTTP 検査のグローバル設定は、個々のポリシー設定より優先されます。
- ・ **検査フィルタ** 検査フィルタを選択し、ポリシーを適用するトラフィックの種類を指定します。利用できるフィルタの数は、初期設定のフィルタ数と作成されたカスタムフィルタ数の合計です。表 7-1 は初期設定のフィルタを示しています。

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

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

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

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

HTTP 検査：除外リストの指定

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

除外リストは、[HTTP] [設定] [除外リスト] [URL リスト] タブで作成できます。

HTTP 検査ポリシーに除外を指定するには

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

注意： 除外リストは、[HTTP] [設定] [URL リスト] タブで作成できます。

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

HTTP 検査フィルタ

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

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

初期設定の HTTP 検査フィルタ

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



図 7-2. 指定したソーシャルネットワーキングサイトへの POST 処理を防止する HTTP 検査フィルタの設定

初期設定のフィルタ設定については、表 7-1 を参照してください。管理者は、初期設定または事前定義されたフィルタを微調整して、必要な管理機能を取得できます。

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

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

表 7-1. 初期設定の HTTP 検査フィルタのマトリックス

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

表 7-1. 初期設定の HTTP 検査フィルタのマトリックス (続き)

初期設定の フィルタ名	フィルタの 種類	要求方法	URL ホスト	URL パス	URL クエリ	ヘッダ (名前/ 演算子/ 値)
SNS サイト 投稿	REQ	POST	(詳細ビューで追加) youtube_upload REQ { METHOD:POST HOST: upload\.youtube \.com }	なし	なし	なし/ なし/ なし
Web ファイル アップロード	REQ	POST	なし	なし	なし	Content -Type/ Contains/ multipart/f orm- data

表 7-1. 初期設定の HTTP 検査フィルタのマトリックス (続き)

初期設定の フィルタ名	フィルタの 種類	要求方法	URL ホスト	URL パス	URL クエリ	ヘッダ (名前/ 演算子/ 値)
WebDAV トラフィック	REQ	PROPFIND PROPMAT CH MKCOL COPY MOVE	なし	なし	なし	なし/ なし/ なし

HTTP 検査フィルタの追加

HTTP 検査フィルタを追加するには、次の 2 つの方法があります。

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

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

基本ビューでのフィルタの追加

基本ビューで設定したフィルタでは、以下を定義します。

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

パケットの取り込みの使用

フィルタのコンポーネントの一部は、HTTP 要求または応答でのパケット取り込みの実行を利用して判別できます。取り込みの例（図 7-3）と説明（表 7-2）を参照してください。

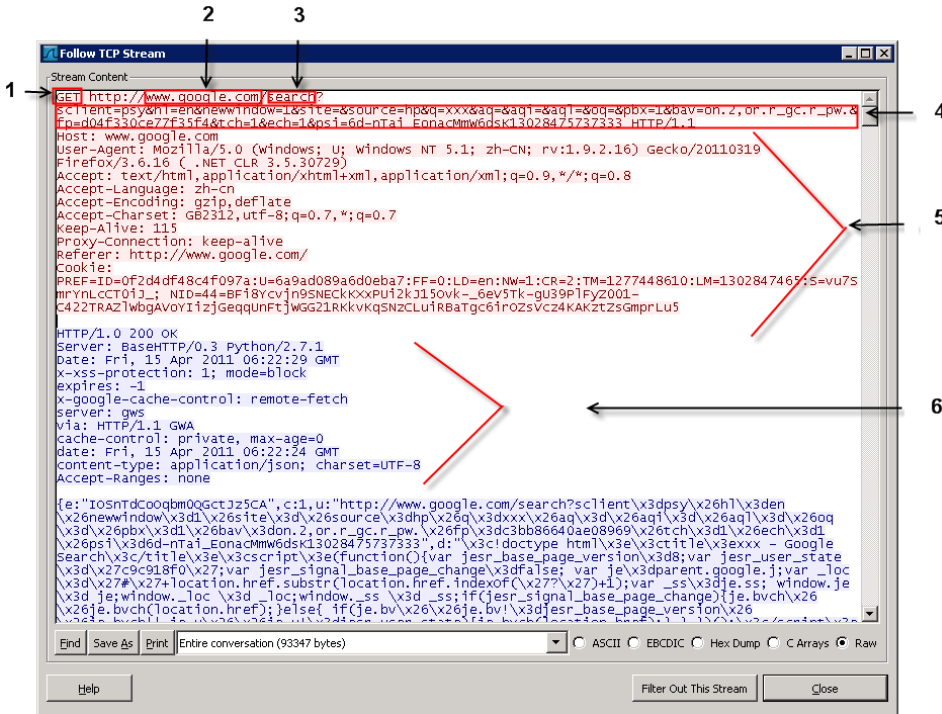


図 7-3. Google 検索の場合のパケットの取り込み

表 7-2. パケットの取り込みで表示されるコンポーネント

番号	コンポーネント
1	要求方法
2	URL ホスト
3	URL パス

表 7-2. パケットの取り込みで表示されるコンポーネント (続き)

番号	コンポーネント
4	URL クエリ
5	要求ヘッダ
6	応答ヘッダ

基本ビューで新しい HTTP 検査フィルタを追加するには

1. [HTTP] [HTTP 検査] [フィルタ] に移動します。
2. [追加] をクリックします。
3. フィルタ名と説明を入力します。
4. [基本ビュー] オプションを選択します。図 7-2 を参照してください。
5. フィルタを作成する方向に応じて、フィルタの種類 (HTTP 要求または HTTP 応答) を選択します。
 - ・ HTTP 要求 HTML ページを取得するためにクライアントが要求を Web サーバに送信するときに使用されるフィルタを作成します。要求フィルタには、次の範囲が含まれます。要求メソッド、URL ホスト、URL パス、URL クエリ、および HTTP ヘッダ。
 - ・ HTTP 応答 Web サーバが応答メッセージをクライアントに返すときに使用されるフィルタを作成します。応答フィルタには、次の範囲が含まれます。URL ホスト*、URL パス*、URL クエリ*、および HTTP 応答ヘッダ。

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

6. 次のオプションの 1 つまたは複数を設定して、フィルタを定義する値を入力します。
 - ・ (フィルタの種類が HTTP 要求の場合に限る) [要求方法] チェックボックスをオンにします。フィルタの範囲を制限するために、HTTP 要求のメソッドを指定します。値には、表 7-3 に示されているものか、その他の拡張メソッドの値を指定できます。

表 7-3. HTTP 要求フィルタのメソッドの値

メソッド	説明
DELETE	指定されたリソースを削除します。

表 7-3. HTTP 要求フィルタのメソッドの値 (続き)

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

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

- [URL ホスト] チェックボックスをオンにします。IPv4/IPv6 アドレスのホスト名 (ポート番号があれば含めます) を、URL の一部として入力します。
- [URL パス] チェックボックスをオンにします。(ある場合は) ホスト部分の末尾の「/」の直後からクエリの「?」の直前までの URL のパス部分を入力します。
- [URL クエリ] チェックボックスをオンにします。(ある場合は) 「?」の直後から URL 文字列の末尾までの URL のクエリ部分を、以下の変換ウィザードのフィールドに入力します。
 - UTF-8 文字列を変換する必要がある場合は、[変換処理が必要ですか?] チェックボックスをオンにします。

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

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

詳細ビューでのフィルタの追加

フィルタ定義を、定義済みの構文を使用してテキストモードで編集できます (HTTP BODY はサポートされていません)。正規表現がサポートされています。すべての正規表現が適用されます (<http://www.pcre.org/pcre.txt> を参照)。使用可能な PCRE (Perl 互換正規表現) フラグについては、表 7-4 を参照してください。

表 7-4. パターンの設定で使用可能な PCRE フラグ

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

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

その他のルールは次のとおりです。

PCRE のランタイムフラグ PCRE_UTF8 (UTF-8 モード) は使用されません。つまり、「.」文字は常に 1 バイトのみに一致します。

シグネチャ定義では、行の最後に「/」(バックスラッシュ) を使用すると行末がエスケープされます (UNIX シェルの場合)。バックスラッシュは PCRE の正規表現言語ではないため、念のために、行継続のバックスラッシュの前に 1 つ以上の空白を入れてください。複数行の正規表現をアセンブリして使用する場合、行が連結される前に、行末のバックスラッシュが削除され、先頭および末尾にあるすべての空白が各行から削除されます。

詳細ビューで新しいHTTP 検索フィルタを追加するには

1. [HTTP] [HTTP 検査] [フィルタ] に移動します。
2. [追加] をクリックします。
3. フィルタ名と説明を入力します。
4. [詳細ビュー] オプションを選択します。図 7-4 を参照してください。



図 7-4. 詳細ビューにおけるリクエストモードの POST フィルタ例

5. 次のいずれかを実行します。

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

注意： [Filter Type] を、REQ (リクエストモードの場合) または RESP (レスポンスモードの場合) に置換する必要があります。

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

```
[HDR-TAG]
REQ-HDR, RESP-HDR}
[HEADER_OP]:
```

```
-----
EQ :=
```

```
NE :=
```

```
GE :=
```

```
LE :=
```

```
M :Contain
```

```
NM :Not Contain
```

```
X :Exist
```

```
NX :Not exist
```

i. リクエストモードのパターン例を次に示します。

```
#
#     _SCAN_SET_1_ REQ {
#         METHOD:POST
#         HOST:^www\.example\.com:2345(?!\d)
#         PATH: test
#         QUERY: test
#         REQ-HDR:Content-Type:M:multipart/form-data
#         REQ-HDR:Content-Length:GE:1048576
#     }
```

ii. レスponseモードのパターン例を次に示します。

```
#
#     _SCAN_SET_2_ RESP {
#         HOST:^www\.example\.com:2345(?!\d)
#         PATH: test
#         QUERY: test
#         RESP-HDR:Content-Type:M:multipart/form-data
#         RESP-HDR:Content-Length:GE:1048576
#     }
```

注意： その他の考慮事項：

1. 整数値比較の場合、IWSS は文字列部分を変換します。文字列に「0x」プレフィックスが含まれる場合は、数字はベース 16 で読み込まれます。それ以外の場合、次の文字が「0」以外であれば 10 (10 進数) と解釈され、「0」であれば 8 (8 進数) と解釈されます。
 2. 最初の空白以外の文字が記号または数字でない場合は、文字列は数字ではありません。
 3. 要求ヘッダのチェックルールに、RESP-HDR を含めないでください。応答ヘッダにしか表示されないヘッダは、要求タイプのフィルタに追加できません。
 4. 応答ヘッダのチェックルールに、METHOD および REQ-HDR を含めないでください。要求ヘッダにしか表示されないヘッダは、応答タイプのフィルタに追加できません。詳細ビューを使用して新しいフィルタを作成するときは、応答タイプのフィルタで METHOD を使用しないでください。
 5. IWSS は、フィルタが HTTP プロトコルに準拠しているかどうかは確認しません。不適切に作成されたフィルタは機能しません。
-

- HTTP ヘッダを変更するには、[パターン] フィールドにパターンを入力します。次の構文を使用します。
 - HTTP ヘッダを追加するには

```
EVENT: {
OP: HEADER_ADD
HEADER: X-GoogApps-Allowed-Domains
VALUE: unixlabs.net, unix.com
}
```
 - HTTP ヘッダを削除するには

```
EVENT: {
OP: HEADER_REMOVE
HEADER: X-GoogApps-Allowed-Domains
}
```
 - HTTP ヘッダの値を変更するには

```
EVENT: {
```

```
OP:HEADER_MODIFY
HEADER: cookie
ORIGINAL_VALUE:[text1]
FINAL_VALUE:[text2]
}
```

注意: この機能は、HTTP 検査フィルタの処理を [監視] または [許可 (検索)] に対してのみ有効にします。

6. [保存] をクリックします。

HTTP 検査フィルタの編集

既存のフィルタを変更したり、既存のフィルタを基準にして新しいフィルタを作成したりできます。

HTTP 検査フィルタを編集する場合は、以下を変更できます。

- ・ フィルタ名
- ・ フィルタの説明
- ・ フィルタの手法 (基本ビュー)
- ・ フィルタのパターン (詳細ビュー)

基本ビューまたは詳細ビューでフィルタを変更できます。

フィルタを変更するには

1. [HTTP] [HTTP 検査] [フィルタ] に移動します。
2. 変更するフィルタの名前をクリックします。
3. 次のようにパラメータを変更します。
 - ・ 131 ページの「基本ビューで新しい HTTP 検査フィルタを追加するには」
 - ・ 135 ページの「詳細ビューで新しい HTTP 検査フィルタを追加するには」
4. [保存] をクリックします。

HTTP 検査フィルタのインポート

次の 2 種類の HTTP 検査フィルタをインポートできます。

- ・ ユーザが IWSS を使用せずにテキストファイル形式で作成した新しいフィルタ
- ・ トレンドマイクロのサポートサービスが作成したカスタムフィルタ

フィルタファイルはXMLファイルです。インポートされるフィルタファイルは、139ページの「インポートするフィルタを作成するには」に示されている規定の基準に適合する必要があります。

インポートするフィルタを作成するには

1. インポートされるフィルタのXMLファイルは、いくつかの方法で作成できます。
 - ・ IWSS からエクスポートする
 - ・ 新しいファイルとして作成する
2. 新しいファイルを作成する場合は、以下のサンプル形式を使用してください。

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<SDF>
```

```
  <Filter Mode="Basic" Name="Browser type filter" ID="1">
```

```
    <Note>Firefox ブラウザから送信された要求を
```

```
    ユーザーエージェントヘッダに従って特定します </Note>
```

```
    <Basic Type="REQ">
```

```
      <Headers Enable="true">
```

```
        <Header Value="Firefox" Op="M" Name="User-Agent"/>
```

```
      </Headers>
```

```
    </Basic>
```

```
  </Filter>
```

```
  <Filter Mode="Basic" Name="Large data upload filter" ID="3">
```

```
    <Note> サイズの大きいファイルのアップロードをコンテンツ長ヘッダに従って特定しま  
す </Note>
```

```
    <Basic Type="REQ">
```

```
      <Headers Enable="true">
```

```
        <Header Value="1048576" Op="GE" Name="Content-Length"/>
```

```
      </Headers>
```

```
    </Basic>
```

```
  </Filter>
```

```
  <Filter Mode="Basic" Name="Query keyword filter" ID="4">
```

```
    <Note> 検索エンジン Web サイトなどのクエリキーワードを特定します </Note>
```

```
    <Basic Type="REQ">
```

```
      <Query Enable="true">
```

```
<Value><![CDATA[[put query keywords here]]]></Value>
</Query>
</Basic>
</Filter>
</SDF>
```

フィルタをインポートするには

1. [HTTP] [HTTP 検査] [フィルタ] に移動します。
2. [インポート] リンクをクリックします。
3. [参照] をクリックして、インポートするパスとフィルタを指定します。
4. [インポート] をクリックします。
5. フィルタ名のリストに、インポートされたフィルタの名前が表示されます。

HTTP 検査フィルタのエクスポート

次のようないくつかの理由で、既存のフィルタをエクスポートできます。

- ・ フィルタは他の場所で使用可能である。
- ・ トレンドマイクロのサポートサービスが作成したカスタムフィルタは、IWSS 管理者によるエクスポート、お客さまへの送信、およびインポートが可能である。

注意： エクスポートされたフィルタファイルは手動で編集しないでください。変更すると、ファイルが正常にインポートされなくなる場合があります。

フィルタをエクスポートするには

1. [HTTP] [HTTP 検査] [フィルタ] に移動します。
2. エクスポート対象のファイルの名前のボックスをオンにします。
3. [エクスポート] リンクをクリックします (フィルタ名が選択されていない場合は、エラーメッセージが表示されます)。
4. [名前を付けて保存] ダイアログボックスで、ファイルを保存する場所を選択します。初期設定のファイル名を使用するか、変更します。
5. [保存] をクリックします。

情報漏えい対策

IWSS に追加された情報漏えい対策 (DLP) は、ユーザに以下の機能を提供します。

- ・ 組織の機密データを含むコンテンツの送信トラフィックを検索できます。
- ・ 事前定義されたテンプレートを使用してポリシーを作成および変更することにより、個人情報データをフィルタリングして世界各国のプライバシー規制要件をより確実に遵守できます。
- ・ キーワードと正規表現を使用してカスタムポリシーを作成および変更することで、お客さまの定義する方法で知的財産をフィルタできます。
- ・ どのユーザがどの DLP ポリシーを違反したかについてレポートを提供します。
- ・ 管理者が製品の DLP ポリシーの有効性 (検出率と誤警告率) を評価するための監査機能を提供します。

ヒント: ベストプラクティスとして、できるだけ多く (「すべてのエンドポイント」または「すべてのユーザ」など) の対象 (ユーザまたはエンドポイント) に最も厳密なルールを課すポリシーを最初に作成して、その後「すべてのエンドポイント」または「すべてのユーザ」からの例外として少数のエンドポイントまたはユーザに対するポリシーを作成することを強くお勧めします。

ポリシー

[情報漏えい対策ポリシー] ページを使用して、組織のファイルが満たす必要のある、組織全体のルールおよび条件を作成します。

[情報漏えい対策ポリシー] ページでは、組織の情報漏えい対策ポリシーを追加、編集、削除、または保存できます。また、[DLP を有効にする] チェックボックスをオンまたはオフにすることで、この機能を有効にするかどうかを制御できます。IWSS に含まれる DLP 検索の初期設定ポリシーは変更はできません。

[情報漏えい対策ポリシー] ページにアクセスするには

1. [HTTP] [情報漏えい対策] [ポリシー] に移動します。
[情報漏えい対策ポリシー] ページが表示されます。
2. 編集または削除するポリシーを選択するか、または必要に応じて新規ポリシーを追加します。
以下のセクションで必要な手順を説明します。

既存の情報漏えい対策ポリシーを変更するには

1. [HTTP] [情報漏えい対策] [ポリシー] に移動し、変更するポリシーの名前をクリックします。
DLP ポリシー： [情報漏えい対策ポリシー] ページが表示されます。
2. 各ポリシーテンプレートは、特定の地域または業界により分類され、[許可]、[ブロック]、または [監視] するよう選択できます。
3. 適用するルールテンプレートの左側にあるプラス記号のアイコンをクリックします。
4. ルールのチェックボックスをオンにしてプルダウンを使用することで必要に応じて変更を行い、希望する動作に変更して、[適用] をクリックします。
処理アイコンが要求されたステータスに変わります。

新しい情報漏えい対策ポリシーを追加するには

1. [HTTP] [情報漏えい対策] [ポリシー] に移動し、[追加] をクリックします。
[情報漏えい対策ポリシー： (新規ポリシー)] ページが表示されます。
2. ポリシー名を入力します。
3. 保護または監視の対象を定義して有効なアカウント情報を入力します。このページでは、IP 範囲または特定の IP アドレス、ホスト名により対象を選択できます。

注意： これらのアカウントフィールドでは IPv6 アドレスがサポートされます。任意の IPv6 ホストに 1 つのルールを定義すると、クライアントが IWSS を介して組織のセキュリティポリシーに違反するデータを送信したときにこのポリシールールがトリガされます。

4. 特定のユーザまたはユーザのグループ全体を対象として選択します。ユーザまたはグループの名前を入力して、[検索] をクリックします。
5. [次へ] をクリックします。
[ルールの指定] ページが表示されます。
6. 既存のポリシーを編集する場合と同様に、定義済みの DLP テンプレートを使用するか、または特定の地域または業界で分類されたポリシーテンプレートを変更します。ポリシーテンプレートでは、特定のルールを許可、ブロック、または監視できるターゲットテンプレートを選択することで、コンテンツを検索できます。
初期設定の検索トラフィックは HTTP/HTTPS に設定されています。
7. 適用するルールテンプレートの左側にあるプラス記号のアイコンをクリックします。
8. ルールのチェックボックスをオンにしてプルダウンを使用することで必要に応じて変更を行い、希望する動作に変更して、[適用] をクリックします。

9. 処理アイコンが要求されたステータスに変わります。
10. 残りのページ要素を入力します。
11. [次へ] をクリックします。
[除外リストの指定] ページが表示されます。
12. 承認する URL リスト、除外ファイル名リストの設定を指定し、ファイルのサイズを制限する場合は、サイズ制限値を入力してチェックボックスをオンにします。
13. [保存] をクリックします。

テンプレート

[テンプレート] ページには、すべての初期設定のテンプレートと、管理者によってカスタマイズされたテンプレートが表示されます。これらのテンプレートは、関連付けられた業界または地域ごとに表示され、それぞれの説明が含まれます。このページからテンプレートを追加、コピー、削除、インポート、またはエクスポートできます。

新しい準拠テンプレートを追加するには

1. [HTTP] [情報漏えい対策] [テンプレート] に移動し、[追加] をクリックします。
[テンプレートの追加] ページが表示されます。
2. 追加する準拠テンプレートの名前と説明を入力します。
3. 各デジタル資産を式またはキーワードとして定義します。
4. 新しい準拠テンプレートで、「デジタル資産の定義」として事前定義された式またはキーワード項目を、固定された出現回数または「および」/「または」の論理式と組み合わせて選択します。
5. デジタル資産を追加するには、ページの左側にあるプラス記号をクリックします。
6. [追加] をクリックして新しいデジタル資産を作成します。
7. [保存] をクリックして完了します。

DLP モジュールでは、カスタマイズされた DLP テンプレートや事前定義された DLP テンプレートを含め、DLP ポリシーのすべての DLP テンプレートが照合されます。DLP テンプレートが一致すると、DLP テンプレートごとに設定された処理に基づいて HTTP トランザクションが許可、ブロック、または監視されます。送信トラフィックのコンテンツが複数のテンプレートに一致する場合は、ブロック、監視、許可の優先順位で処理が適用されます。

情報漏えい対策オプション (iDLP)

IWSS 6.5 には Trend Micro Control Manager (以下、Control Manager) または Trend Micro Apex Central (以下、Apex Central) の情報漏えい対策ウィジェットが含まれており、企業の管理者は、このウィジェットを使用して Control Manager または Apex Central から IWSS に情報漏えい対策のポリシーやテンプレートを配信できます。管理者は Control Manager または Apex Central を使用して、IWSS 6.5 などトレンドマイクロ製品に対する組織全体の情報漏えい対策ポリシーを管理できます。

HTTPS のセキュリティ

HTTPS (Hypertext Transfer Protocol with Security) とは、HTTP とネットワークセキュリティプロトコル (SSL (Secured Sockets Layer) など) を組み合わせたものです。HTTPS 接続は、機密コンテンツを保護するための信頼性に優れた接続を必要とする、オンラインバンキングなどの Web アプリケーションで使用されています。従来のセキュリティデバイスではこの HTTPS コンテンツを復号化して検査できなかったため、HTTPS トラフィックに埋め込まれたウイルスや不正プログラムなどの脅威がセキュリティ防御機能を素通りしてエンタープライズネットワークに侵入していました。

IWSS は、暗号化されたコンテンツを復号化して検査することで HTTPS のセキュリティホールをふさぎます。選択した Web カテゴリの HTTPS トラフィックを復号化するようにポリシーを定義できます。復号化の際、データは HTTP トラフィックと同じ方法で扱われ、URL フィルタおよび検索のルールを適用可能です。また、復号化されたデータは IWSS サーバのメモリ内に保持されるため、セキュリティは保護されます。このデータは IWSS サーバから送り出される前に暗号化されるため、クライアントのブラウザに安全に送信されます。

IWSS は、プロキシ転送モードでの HTTPS の復号化および検索をサポートしています。

未確認の HTTPS コンテンツの危険性

次に、HTTPS 接続に関する主な問題点をいくつか示します。

- ・ ウイルス検索ポリシーおよびコンテンツフィルタポリシーは、暗号化されたデータには適用できません。
- ・ クライアントはデジタル証明書の失効リストをチェックすることがほとんどないため、デジタル証明書が偽造されたり、有効期限が切れたり、失効する可能性があります。
- ・ 正規の証明書は悪意のある第三者によって容易に取得することができるため、提供された情報が安全であるとユーザが思い込んでしまう場合があります。

- Web ブラウザは証明書の挿入攻撃に対して脆弱であるため、悪意のある侵入者による社内イントラネットへのアクセスが可能になります。
- 証明書が信頼できるものかどうかを判断するのに必要な知識が、ユーザにない場合があります。
- URL パスやその他の情報が隠されているため、HTTPS トラフィックの監視が困難です。

SSL ハンドシェイクの概要

SSL プロトコルを使用して HTTPS 接続を確立するには、Web サーバで SSL 証明書をインストールする必要があります。証明書は認証機関 (CA) から提供され、Web サイトが信頼できるか、機密情報 (クレジットカード番号など) が暗号化されているか、送信データに改ざんやねつ造はないかなどを確認できます。

クライアントが「http://」ではなく「https://」から始まる URL を入力して SSL セッションを開始すると、SSL ハンドシェイクが実行され、識別情報が検証され (証明書の交換や妥当性など)、セッションに必要な暗号化方式の処理が行われます。IWSS サーバは、クライアントと安全な Web サーバとの間の中継機として機能し、サーバ証明書を検証します。次に SSL ハンドシェイク処理の概要を示します。

1. クライアント Web ブラウザは、接続要求とその暗号化データを Web サーバに送信します。IWSS はその要求を Web サーバに転送します。
2. Web サーバは、その SSL 情報 (サーバ証明書を含む) を返します。IWSS はサーバ証明書を確認します。
3. サーバ証明書が検証テストに合格すると、その Web サーバとクライアント間で HTTPS 接続が許可されます。IWSS は、HTTPS 復号化ポリシーを適用して、暗号化されたコンテンツを検索します。

Web サーバがクライアント証明書を要求する場合、IWSS は暗号化されたトラフィックをブロックまたはトンネルします。

IWSS における HTTPS 復号化およびプロセスフロー

Web サーバとクライアント間で HTTPS 接続が許可されると、IWSS は暗号化されたコンテンツを復号化して検査することで、HTTPS のセキュリティループホール（セキュリティの抜け穴）をふさぎます。選択した Web カテゴリの HTTPS トラフィックを復号化するようにポリシーを定義できます。復号化の際、データは HTTP トラフィックと同じ方法で扱われ、URL フィルタおよび検索のルールを適用可能です。

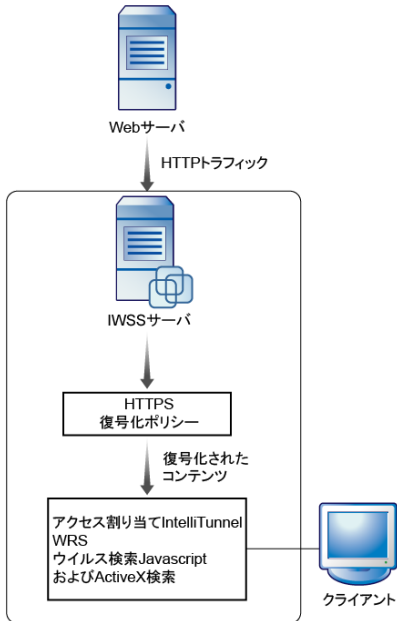


図 7-5. IWSS における復号化された HTTPS のトラフィックフロー

HTTPS 復号化機能には、次のような利点があります。

- ・ ゲートウェイでの復号化 IWSS は HTTPS トラフィックを復号化して、既存のセキュリティポリシーを適用することができます。
- ・ データのプライバシーの保護 復号化されたデータは IWSS サーバのメモリに引き続き存在するので、まったく安全です。データは、IWSS サーバから送信される前に暗号化されます。これにより、クライアントのブラウザまで安全に通過できるようになります。

- ・ 証明書の一元的な処理 IWSS はリモートサーバで発行された証明書を検証して管理することで、クライアントを重要なタスクから解放します。

HTTPS 復号化ポリシーの設定

IWSS で暗号化されたコンテンツに検索ポリシーおよびフィルタポリシーを適用するには、その前に、コンテンツを復号化するように HTTPS 復号化ポリシーを設定する必要があります。URL フィルタポリシーの設定と同様に、選択された Web カテゴリに基づいてコンテンツを復号化するように、HTTPS 暗号化ポリシーを設定します。たとえば、ビジネスカテゴリの Web サイトからの暗号化されたコンテンツを復号化するように、HTTPS 復号化ポリシーを設定することができます。

HTTPS 復号化ポリシーおよび URL フィルタポリシーでは、同じ Web カテゴリのグループと名前を使用します。会社またはユーザのニーズを満たすように、カスタムカテゴリを設定することもできます。

注意： カスタムカテゴリが複数選択されているか、まったく選択されていないかどうかに関係なく、IWSS は最初のカスタムカテゴリのみを一致対象とします。

HTTPS 復号化の有効化

HTTPS 復号化を有効にするには

1. メインメニューから [HTTP] [HTTPS 復号化] [ポリシー] の順に選択します。
2. [HTTPS 復号化を有効にする] をクリックします。
 - ・ ポリシーを適用するアカウントを選択します。
 - ・ トラフィックを復号化する Web サイトカテゴリを指定します。
 - ・ 除外リストを選択します。
3. [保存] をクリックします。

新しい HTTPS 復号化ポリシーの作成

新しい HTTPS 復号化ポリシーを作成するには、次の 3 つの手順に従います。

- ・ ポリシーを適用するアカウントを選択します。
- ・ トラフィックを復号化する Web サイトカテゴリを指定します。
- ・ 除外リストを選択します。

新しい HTTPS 復号化ポリシーを作成するには

1. IWSS Web コンソールを開き、管理コンソールから [HTTP] [HTTPS 復号化] [ポリシー] の順に選択します。
[追加] をクリックします。[HTTPS 復号化ポリシー: ポリシーの追加] 画面が表示されます。
2. [新規ポリシーの作成] ボックスに、わかりやすいポリシー名を入力します。
「Web メール用 HTTPS 復号化ポリシー」のように、適用対象となるユーザまたはグループへの参照が含まれるポリシー名は簡単に覚えられます。
3. ポリシーを適用するユーザを選択します。
この画面のオプションは、使用しているユーザの識別方法に応じて異なります。[IP アドレス]、[ホスト名 (変更された HTTP ヘッダ)]、または [ユーザ / グループ名認証] (LDAP) のいずれかになります。ユーザの識別方法の設定とポリシー適用範囲の設定の詳細については、108 ページの「ユーザ識別方法の設定」を参照してください。
4. [次へ] をクリックします。
5. [カテゴリの指定] 画面で、[ポリシーを有効にする] チェックボックスがオンになっていることを確認します。
6. 復号化する URL カテゴリを選択します。
グループの全カテゴリを選択するには、対象グループで [すべて選択] をクリックします。グループ内のすべてのカテゴリを選択するのに、グループを展開する必要はありません。
7. 今後の参照のためにこのポリシーに関して役立つ情報を含めるには、オプションの [備考] を入力します。
8. [次へ] をクリックします。
9. 除外リストを適用する場合、[除外リストの指定] 画面で、ドロップダウンリストボックスから除外 HTTPS URL リスト名を選択します。IWSS は、除外リストにある URL からの HTTPS トラフィックをトンネルします。つまり、暗号化されたコンテンツは復号化されて検査されることはありません。
10. [保存] をクリックします。
11. [HTTPS 復号化ポリシー] 画面で、[優先度] 列に表示されている上向きまたは下向きの矢印をクリックして、新しいポリシーの優先順位を設定します。
2 つ以上のポリシーに属するアカウントがある場合、[優先度] の設定により、どのポリシーが適用されるかが決まります。
12. [保存] をクリックします。
13. ポリシーをただちに適用するには、[ポリシーの配信] をクリックします。すぐに適用しない場合、データベースキャッシュの有効期限が切れた後に、このポリシーが適用されます。

警告： プロキシモードでは、IWSS はクライアントのブラウザのドメインに基づいて HTTPS 復号化ポリシーを適用します。

HTTPS 復号化設定

[HTTP] [HTTPS 復号化] [設定] の順に選択して、次の項目を設定します。

- ・ サーバ証明書の検証
- ・ クライアント証明書の処理
- ・ 認証機関
- ・ SSL 方式

サーバ証明書の検証

[サーバ証明書の検証] 画面で、サーバ証明書の検証を有効にして、証明書失効リストの検索や証明書の正当性の確立などの証明書のテストを自動化するように検証設定を行います。

注意： 証明書の検証を無効にすると、クライアントはサーバ証明書の確認を行わずに任意の HTTPS Web サイトにアクセスできます。

証明書が証明書の検証テストに合格しなくても、クライアントは HTTPS 接続を介して Web サイトにアクセスすることを選択できます。クライアントのブラウザには警告画面が表示されます。

サーバ証明書の検証を設定するには

1. 管理コンソールから [HTTP] [HTTPS 復号化] [設定] の順に選択します。[サーバ証明書の検証] 画面が表示されます。
2. [証明書検証を有効にする] を選択して、サーバ証明書を確認します。
3. 次のオプションの 1 つまたは複数を選択します。
 - ・ 一般名が URL に一致しない証明書を拒否する このオプションを選択すると、CommonName がアクセス先の URL と一致しない場合、証明書は拒否されます。IWSS はその証明書を無効として処理します。

- ・ ワイルドカード証明書を許可する このオプションを選択すると、CommonName がワイルドカードで表された証明書を許可および検証できます。このオプションを無効にすると、ワイルドカードを使用して表現された CommonName を含む証明書は拒否されます。
 - ・ 有効期限の切れた証明書または不正な目的の証明書を拒否する このオプションを選択すると、有効期限が切れた証明書または意図した目的に使用できない証明書は拒否されます。
 - ・ 証明書チェーン全体を検証する このオプションを選択すると、特定の証明書チェーン (提供された証明書からルート認証機関の証明書まで) が有効で信頼できることが確認されます。
 - ・ CRL による証明書失効確認 証明書取り消しリスト (CRL) を調べて証明書が失効している (無効になっている) かどうかを確認するには、このオプションを選択します。
4. [保存] をクリックします。

証明書の検証の除外

対象 Web サイトの証明書が検証に失敗した場合は、サーバ証明書の除外設定を追加して、IWSS で特定の事前定義された処理を実行するようにできます。

除外項目には次の 2 つの種類があります。

- ・ 証明書の種類: 証明書の検証が HTTPS トラフィックで失敗した場合 (たとえば、Web サイトの証明書の有効期限が切れている場合など)、IWSS では「警告」処理とともに、この証明書に対する証明書の種類の除外項目を自動的に追加します。
この種類の除外項目の処理と説明は変更できます。
- ・ URL の種類: この画面で [追加] ボタンをクリックして、URL の種類の除外項目を追加できます。

クライアント証明書の処理

オンラインバンキングなどの多くのセキュリティの高いアプリケーションでは、Web サーバがクライアントを認証するためにクライアント証明書を要求する場合があります。IWSS ではクライアント証明書を要求する Web サイトはサポートされないで、[クライアント証明書の処理] 画面で接続をトンネルまたはブロックするように選択できます。

- ・ トンネル このオプションを選択すると、HTTPS トラフィックがバイパスされます。IWSS でコンテンツを復号化して検査することはありません。
- ・ ブロック このオプションを選択すると、リモートサーバへのアクセスが拒否されます。

認証機関

初期設定では、IWSS はプライベートな認証機関 (CA) として動作し、動的にデジタル証明書を作成します。このデジタル証明書はクライアントのブラウザに送信され、HTTPS 接続の安全なセッションを確立します。ただし、初期設定の CA はインターネット上の信頼できる CA によって署名されていないため、ユーザが HTTPS Web サイトにアクセスするたびに、クライアントブラウザに証明書に関する警告が表示されます。ユーザはその警告を無視しても安全ですが、IWSS には独自の証明書を使用することをお勧めします。

CA 証明書をインポートするには

1. 管理コンソールから [HTTP] [HTTPS 復号化] [設定 | 証明機関] の順に選択します。
2. [証明書ファイル] の横にある [参照] をクリックして、証明書ファイルを選択します。- IWSS は、Base64 エンコードの証明書と、PEM ファイル形式の RSA ベースの暗号化された秘密鍵をサポートしています。
3. [秘密鍵] の横にある [参照] をクリックして、CA 証明書に関連付けられた秘密鍵を選択します。
4. 秘密鍵の [パスフレーズ] を入力します。
5. [パスフレーズの確認] フィールドに再度パスフレーズを入力します。
6. [CA のインポート] をクリックします。

注意： IWSS は、Base64 エンコードの証明書と、PEM ファイル形式の RSA ベースの暗号化された秘密鍵のみをサポートしています。

CA 証明書のインポート後に、エンドユーザが安全な Web サイトにアクセスしようとして、そのユーザのコンピュータに証明書に関する警告画面 (図 7-6) が表示される場合があります。これが表示されないようにするには、関連する証明書を Web ブラウザの信頼するルート認証機関のリストに追加します。詳細については、図 7-7 を参照してください。

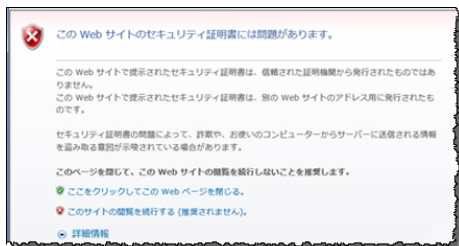


図 7-6. 証明書に関する警告画面

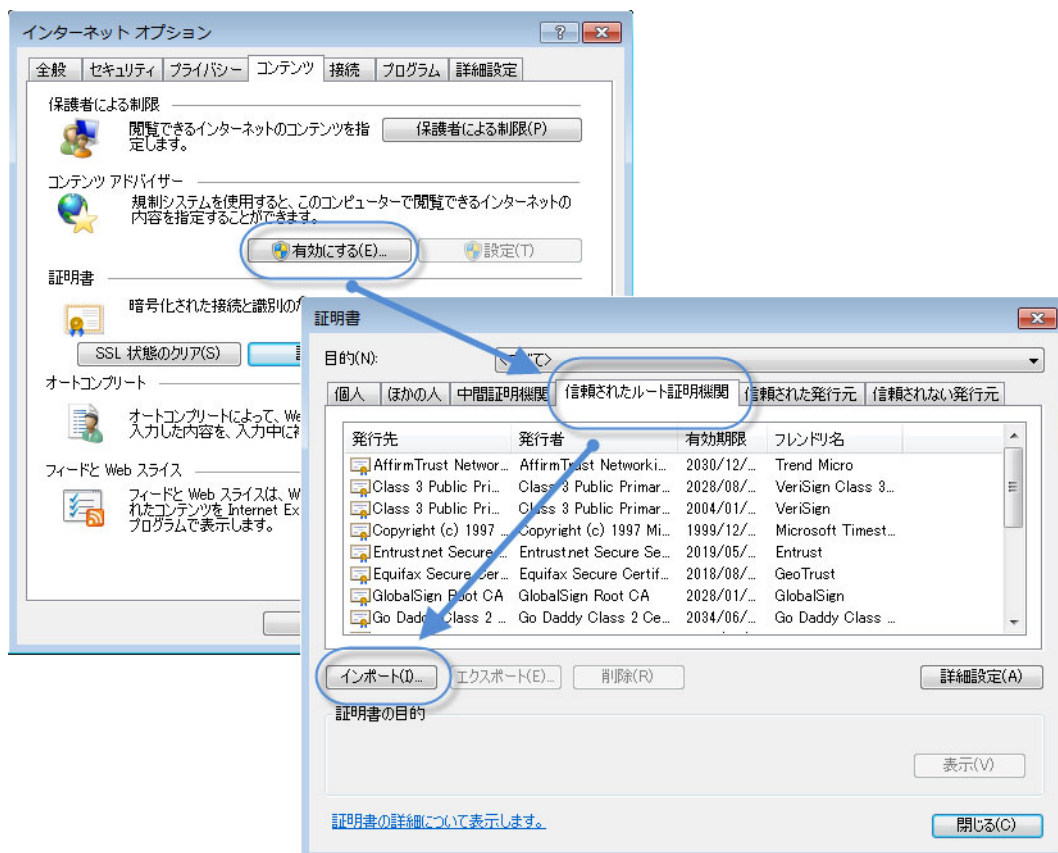


図 7-7. 信頼するルート認証機関への証明書の追加

CA 証明書 (公開鍵) をエクスポートするには

1. 管理コンソールから [HTTP] [HTTPS 復号化] [設定 | 証明機関] の順に選択します。
2. [CA 公開鍵の取得] をクリックします。
3. 画面上の指示に従って、証明書ファイルをコンピュータに保存します。

CA の秘密鍵をエクスポートするには

1. 管理コンソールから [HTTP] [HTTPS 復号化] [設定 | 証明機関] の順に選択します。
2. [CA 秘密鍵の取得] をクリックします。
3. 画面上の指示に従って、秘密鍵ファイルをコンピュータに保存します。

SSL 方式

SSL 方式について

IWSS では、TLS (Transport Layer Security) または SSL (Secure Sockets Layer) を使用して Web コンソールとサーバとの間の安全な通信を保証しています。

TLS とその前身である SSL は、データを暗号化して送受信するためのプロトコルです。これらのプロトコルを使用することで、Web コンソールとサーバは、長い非対称の公開鍵を使用して相互に認証を行い、安全にデータを送受信できるようになります。一度認証されると、Web コンソールとサーバで短い対称の秘密鍵が作成され、セッションの間、この秘密鍵を使用して通信データが暗号化されるようになります。公開鍵を使用して秘密鍵をリバースエンジニアリングすることはできません。

TLS および SSL プロトコルの認証では、X.509 証明書と非対称暗号化方式が使用されます。X.509 証明書を使用するには、認証局 (CA) と PKI (公開鍵インフラストラクチャ) を利用して、次のことを行う必要があります。

- ・ 証明書の作成、署名、および認証
- ・ 証明書とデータ送受信者との関係の確認

SSL 方式の指定

SSL 方式を指定するには

1. [HTTP] [HTTPS 復号化] [設定] [SSL 方式] の順に選択します。
2. [クライアントの SSL 方式] および [サーバの SSL 方式] セクションでオプションを 1 つ以上選択します。

ドメイントンネリング

HTTPS トンネリングを使用すると、接続が制限されたネットワークの場所（通常は NAT、ファイアウォール、またはプロキシサーバの内側）間での通信が可能になります。接続の制限は通常、TCP/IP ポートのブロック、ネットワークの外部から開始されたトラフィックのブロック、またはほとんどのネットワークプロトコルのブロックによる結果で、これによりネットワークが内部および外部の脅威から保護されます。

グローバルな信頼リストと同様に、ドメイントンネルを使用すると、管理者は信頼されたサイトのリストを保持できます。

ドメイントンネルを設定するには

1. [HTTPS] [HTTPS 復号化] [トンネリング] に移動します。
2. 追加するドメイン名の一致を入力します。
3. 文字列（完全な名前）に一致するするか、ドメイン全体に一致するかを選択します（ドメイン全体によるトンネルの横にはアスタリスクが表示されます）。
4. 承認されたエントリを含むファイルを以前に作成している場合は、[ファイルの選択] をクリックし、追加するファイルを選択して、[インポート] をクリックします。
追加するトンネリングされたドメインが、[トンネリングされたドメイン] ボックスに表示されます。
5. [保存] をクリックします。

トンネリングされたドメイン

古くなったトンネルは、トンネリングされたドメインを選択して [削除] をクリックするか、[すべて削除] をクリックしてリスト全体をクリアすることで削除できます。[エクスポート] をクリックして安全な場所にリストを保存することで、トンネリングされたドメインのリストを保存することもできます。

トンネリングされたドメインの除外

除外もリストすることができます。除外リスト内のすべてのドメインが復号化されます。

HTTPS アクセスの失敗

HTTPS アクセスの試行の失敗は追跡および記録できます。管理者は、トンネルリストにトンネリングされたドメインを追加できます。ログは、時間、ユーザ名、およびドメインに基づいて検索できます。

[処理] 列には、ドメイン名をトンネリングリストに追加するためのボタンがあります。ドメインがすでにリストに含まれる場合は、列のスペースに「トンネリングあり」と表示されます。

HTTPS アクセスの試行の失敗を検索するには

1. [HTTP] [HTTPS 復号化] [トンネリング] [失敗した HTTPS アクセス] に移動します。
2. 自動トンネリングを開始する場合は、[致命的なエラーの場合に自動トンネリングを有効にする] オプションをオンにします。
3. レビューする HTTPS アクセスの失敗の数を、20、50、または 100 エントリから選択します。
4. 特定のユーザのアクセス試行を検索するには、[検索] ボックスにユーザのドメイン名に加えてユーザ名を入力します。

各エントリに対して、次の情報が表示されます。

- ・ 日付
- ・ ユーザ名 (ユーザまたは IP)
- ・ ドメイン名
- ・ 失敗した理由
- ・ 処理

[処理] 列には、ドメイン名をトンネリングリストに追加するためのボタンがあります。ドメイン名がすでにリストに含まれる場合は、[処理] に「トンネリングあり」と表示されます。

高度な脅威保護ポリシーの作成と変更

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

新しいウイルス検索ポリシーを作成するには

1. 管理コンソールから [HTTP] [高度な脅威保護] [ポリシー] の順に選択します。
2. [ウイルス検索を有効にする] を選択してウイルス検索を有効にします。
3. [高度な脅威検索を有効にする] を選択して、高度な脅威検索エンジンを有効にします。

4. [Web レピュテーションを有効にする] を選択して Web レピュテーションを有効にします。

注意： Web レピュテーションは、ポリシーレベルで使用するため、グローバルレベルで有効にする必要があります。

5. [ポット検出を有効にする] を選択して、ポット検出を有効にします。
6. [追加] をクリックします。
7. [新規ポリシーの作成] に、わかりやすいポリシー名を入力します。

「エンジニア向けウイルスポリシー」や「研究者向け URL フィルタポリシー」など、ポリシーを適用するユーザやグループへの参照を含むポリシー名にすると、見分けやすくなります。アカウントフィールドでは IPv6 アドレスがサポートされます。任意の IPv6 ホストに 1 つのルールを定義すると、クライアントが IWSS を介して HTTP サイトにアクセスしたときにこのポリシールールがトリガされます。

使用可能なポリシーの選択時には、IPv4 と IPv6 の両方のポリシーが表示されます。[アカウント] フィールドで入力可能なアカウントエントリは、IPv4 でサポートされているものと同様に、単一の IPv6 アドレス、IPv6 アドレス範囲、または IPv6 マスクです。

IWSS は、IPv6 で「配信前に検索」機能をサポートしており、IWSS の IPv6 または IPv4 アドレスは、クライアントの IP アドレスのバージョンに基づいて、自動的にクライアントにリダイレクトされ処理が続行されます。

- ・ クライアントが IPv4 アドレスを使用する場合、IWSS は、リダイレクト要求を IWSS の IPv4 アドレスとともに送信します。
 - ・ クライアントが IPv6 アドレスを使用する場合、IWSS は、リダイレクト要求を IWSS の IPv6 アドレスとともに送信します。
8. ポリシーを適用するユーザを選択します。

この画面のオプションは、使用しているユーザの識別方法に応じて異なります。[IP アドレス]、[ホスト名 (変更された HTTP ヘッダ)]、または [ユーザ / グループ名認証] (LDAP) のいずれかになります。ユーザの識別方法の設定とポリシー適用範囲の設定の詳細については、108 ページの「ユーザ識別方法の設定」を参照してください。

注意： 設定したユーザの識別方法に関係なく、ポリシーを適用するクライアントの IP アドレスを入力できます。

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

既存の高度な脅威保護ポリシーを変更するには

1. 管理コンソールから [HTTP] [高度な脅威保護] [ポリシー] の順に選択します。
2. 変更するポリシーの名前をクリックします。
3. Web レピュテーションルール、ウイルス検索ルール、ポット検出ルール、スパイウェア検索ルール、ポリシー除外、および検索処理を変更します。
指定した検索処理がすべてのルールに適用されます。

既存の高度な脅威保護ポリシーでユーザを追加または削除するには

1. 管理コンソールから [HTTP] [高度な脅威保護] [ポリシー] の順に選択します。
2. 対象のウイルス検索ポリシーアカウントをクリックします。
3. [HTTP 検索ポリシー : 編集] 画面の [アカウント] タブで、ユーザを追加または削除します。
 - ・ ユーザを追加するには、単一の IP アドレス、IP アドレス範囲、IP サブセット、またはユーザ / グループ名を指定して、影響を受けるユーザを示します。
 - ・ ユーザを削除するには、ユーザの隣にあるごみ箱アイコンをクリックします。

HTTP ウイルス検索ポリシーを有効にするには

- ・ グローバルレベルで HTTP 検索ポリシーを有効にするには [HTTP] [HTTP 不正プログラム検索] [ポリシー] の順に選択して、[ウイルス検索を有効にする] をクリックします。
- ・ ポリシーレベルで HTTP 検索ポリシーを有効にするには [HTTP] [HTTP 不正プログラム検索] [ポリシー] の順に選択し、追加したポリシーをクリックして、[ポリシーを有効にする] を選択します。

Web レピュテーションルールの指定

Web レピュテーションルールはポリシーレベルで作成されます。

Web レピュテーションルールを指定するには

1. Web レピュテーションがグローバルレベルで有効になっていることを確認します。
Web レピュテーションは、ポリシーレベルで使用するため、グローバルレベルで有効にする必要があります ([HTTP] [高度な脅威保護] [ポリシー | Web レピュテーションを有効にする] チェックボックス)。
2. Web レピュテーションがポリシーレベルで有効になっていることを確認します。
[HTTP] [高度な脅威保護] [ポリシー | Web レピュテーションルール] 画面の [追加] または [編集] オプションを使用して、[このポリシーで Web レピュテーションルールを使用する]

チェックボックスがオンになっていることを確認します。このチェックボックスは、初期設定でオンになっています。

3. URL ブロックのセキュリティレベルを指定します。

Web レピュテーションスコアを受信すると、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、ユーザが設定したセキュリティレベルによって定義されます。初期設定のセキュリティレベルは中です。この設定は、誤検出を抑えながら、Web 脅威をブロックするため、お勧めします。

4. 下記を許可、または無効にします。

- ・ [ファームング検索を含める] / [フィッシング検索を含める] / [C&C コールバック試行の検出を含める]

初期設定では、すべての検出が有効になっています。158 ページの「フィッシング対策、ファームング対策、および C&C コールバック試行検出」参照を参照してください。

フィッシング対策、ファームング対策、および C&C コールバック試行検出

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

ファームング攻撃とは、通常、金銭上の個人情報をだまし取る目的でユーザを偽の Web サイトにリダイレクトしようとする試みです。ファームングは、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 / ファームング検出のソースは Web レピュテーションに基づいており、Web レピュテーションのポリシーのルールに含まれるため、Web レピュテーションがグローバルレベルで無効になっているとフィッシング対策 / ファームング対策機能も無効になります。

ICAP モードでは、ファームング対策はサポートされません。

コマンド & コントロールコールバック試行検出 (C&C コールバック) 攻撃は、トラフィックコンテンツで IRC コマンドを調べるか、またはハニーネットを設定することで、ポットネットの検出を試行するシステムです。

カスタム保護設定

IWSS を Deep Discovery Inspector (DDI)、Control Manager または Apex Central、および Deep Discovery Analyzer (DDAN) サンドボックスと統合し、HTTP/HTTPS トラフィックを介した不正プログラムからのオフラインカスタム保護 APT 攻撃に対処できます。

ATSE エンジンを使用してウイルスや疑わしいファイルを検索できます。このエンジンはウイルス検索エンジン (VSAPI) よりも強力です。APT 検出を特定するようカスタム保護で設定可能な APT カスタム保護ルールを適用できます。カスタム保護は、Web コンソールの [HTTP] [高度な脅威保護] [カスタム保護] で設定できます。

カスタム保護を有効にする

DDI、Control Manager または Apex Central、および DDAN サーバとの IWSS 統合を有効にするには、各製品のチェックボックスをオンにし、サーバアドレス、ポート番号、必要に応じて API キー情報を入力します。サーバとの接続が認識されない場合、IWSS は設定を保存できません。

サンプル提出

DDAN に送信して検索する脅威またはファイルの種類を選択します。

リスクレベル設定

ブロックする不審オブジェクトのリスクレベルを選択します。変更を保存します。

処理

ブロックまたは監視する脅威のタイプに基づいて選択し、変更を保存します。

Web レピュテーション設定

Web レピュテーション設定では、次の項目を指定します。

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

Web レピュテーションの有効化と無効化

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。

グローバルレベルで **Web** レピュテーションを有効 / 無効にするには

1. [HTTP] [高度な脅威保護] [ポリシー] の順に選択します。
2. [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にすると、グローバルレベルで Web レピュテーションが有効になります。

ポリシーレベルで **Web** レピュテーションを有効 / 無効にするには

1. [HTTP] [高度な脅威保護] [ポリシー] [< ポリシー名 >] の順に選択し、[Web レピュテーションルール] タブをクリックします。
2. [このポリシーで Web レピュテーションルールを使用する] チェックボックスをオンにしてこのポリシーで Web レピュテーションを有効にするか、チェックボックスをオフにして無効にします。

Web レピュテーション結果の管理

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。

- ・ フィードバックオプション: 感染した URL についてフィードバックが提供可能なため、Web レピュテーションデータベースの精度を上げるのに役立ちます。
- ・ 監視のみのオプション: 既存の Web アクセスポリシーに影響を与えずに Web レピュテーションの有効性を監視できます。

どちらか一方のオプションまたは両方のオプションを選択できます。

このオプションを設定するには、Web コンソールで [HTTP] [高度な脅威保護] [設定] の順に選択します。

Web レピュテーションの管理を設定するには、Web コンソールで [HTTP] [高度な脅威保護] [設定] の順に移動します。

フィードバックオプション

現行の動的な URL ブロックリストに加えて、ウイルス検索結果を URL ローカルキャッシュと外部のバックエンド評価サーバにフィードバックできます。スマートフィードバックエンジン (以下、TMFBE) では、IWSS がウイルス検索結果をバックエンド評価サーバに送り返すためのフィードバッ

クメカニズムが用意されています。オプションを無効にするには、[HTTP] [高度な脅威保護] [設定] に移動し、[フィードバックオプション] で [感染した URL のフィードバックをトレンドマイクロに送信する] チェックボックスをオフにします。

注意： 上位プロキシモードを使用する場合、トレンドマイクロのサイト (www.trendmicro.co.jp) へのアクセスを IWSS の IP アドレスに明示的に許可するように、プロキシサーバを設定する必要がある場合があります。

感染が検出された場合

トレンドマイクロのウイルス検索エンジンからの検索結果で感染が検出された場合、感染した URL は次の場所に送り返されます。

- ・ 動的な URL ブロックリスト
- ・ Web レピュテーションスコアを調整した URL ローカルキャッシュ
- ・ VirusName と IntelliTrap フラグを含む TMFBE フィードバックバッファ。このバッファのエントリ数が 10 になるか、または、最後のフィードバックから 5 分が経過すると、これらの URL が順次バッチでバックエンド評価サーバに送信されます。

感染が検出されなかった場合

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

監視のみのオプション

監視のみのオプションでは、Web レピュテーション結果を評価する機会が与えられます。このオプションを選択した場合、インターネットセキュリティログから 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、ファームウェア対策、および C&C コールバック試行検出によってフィルタにかけられた URL のみが含まれます。Web レピュテーション結果のみ監視するため、URL ブロックは発生せず、URL はクライアントに渡されます。

初期設定で、監視のみのオプションは無効になっています。

WRS/URL キャッシュのクリア

ユーザがある URL にアクセスしようとする、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 WRS/URL キャッシュに保存します。リモートサーバ上に Web レピュテーションデータベースを配置して、そのデータベース情報を使用してローカル WRS/URL キャッシュを構築すると、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 WRS/URL キャッシュに保存される情報の種類は、次のとおりです。

- Web カテゴリ
- ファーミング / フィッシング検出で使用するファーム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 (157 ページの「Web レピュテーションルールの指定」を参照)

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

注意： キャッシュをクリアすると、HTTP 検索デーモンが停止し、再起動するため、IWSS サービスが中断する場合があります。

WRS/URL キャッシュをクリアするには

1. 管理コンソールで [HTTP] [設定] [WRS/URL キャッシュ] の順に選択します。
2. [キャッシュをクリア] をクリックします。

HTTP ウイルス検索ルール

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

[ウイルス / 不正プログラム検索ルール] タブで、[HTTP] [高度な脅威保護] [ポリシー] | [<ポリシー名>] を参照してください。

高度な脅威検索

検索時に脅威を監視するかまたはブロックするかを選択します。

ブロックするファイルタイプの指定

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

ブロックするファイルタイプを指定するには

1. ポリシーの追加または編集時に、[ウイルス / 不正プログラム検索ルール] [ブロックするファイルタイプ] で、ブロックするファイルタイプのチェックボックスをオンにします。これによって、そのカテゴリのファイルがすべてブロックされるようになります。
2. 選択したカテゴリ内のファイルタイプをブロック解除するには、[詳細の表示] リンクをクリックします。
3. ブロックしないファイルのチェックボックスをオフにします。

検索するファイルタイプの指定

IWSS には次の HTTP 検索機能があります。

- すべての検索可能ファイル
- トレンドマイクロの推奨設定
- 指定のファイル拡張子
- IntelliTrap

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

トレンドマイクロの推奨設定について

現在、ほとんどのウイルス対策ソリューションは、潜在的な脅威に備えて検索するファイルを決定するにあたり、2つのオプションを提供しています。最も安全なアプローチである、すべてのファイルを検索するオプションと、最も感染しやすいとされる特定の拡張子のファイルのみを検索するオプションです。ただし、最近ではファイルの拡張子を変更して「偽装した」ファイルが開発され

ているため、後者のオプションの効力が低下しています。トレンドマイクロの推奨設定は、ファイル名の拡張子に関係なく、ファイルの「実際のファイルタイプ」を識別するトレンドマイクロのテクノロジーです。

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

実際のファイルタイプについて

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

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

たとえば、.gif ファイルと .jpg ファイルは Web トラフィックの大部分を占めています。悪意あるハッカーが、検索エンジンを回避してひそかにネットワークに侵入するために、有害なファイルに「安全な」ファイル名を付ける可能性があります。このような場合でも、トレンドマイクロの推奨設定では、実際のファイルタイプを確認してウイルス検索し、不正コードがネットワークに侵入するのを阻止します。

検索するファイルタイプを選択するには

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、[すべての検索可能ファイル] 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わかっているファイルタイプを検索します。実際のファイルタイプの確認は、ファイル名の拡張子とは無関係に行われるので、実際のファイルタイプを隠すために潜在的に有害なファイルの拡張子の変更されるのを防ぎます。
- すべての HTTP トラフィックを検索する際に起こり得るパフォーマンスの問題を回避するために、拡張子に基づいて検索するファイル、または除外するファイルタイプを明示的に設定できます。ただし、ファイル拡張子はファイルの内容を判定するのに信頼できる方法ではないため、この設定はお勧めしません。

選択したファイルタイプのみを検索するには、[指定する拡張子] を選択してリストをクリックします (トレンドマイクロはこの設定をお勧めしません)。[拡張子による指定] 画面が開きます。初期設定の拡張子リストは、ウイルスが潜伏している可能性があるとして知られているすべてのファイルタイプを示しています。このリストは、ウイルスパターンファイルがリリースされるとアップデートされます。[拡張子による指定] 画面で、[その他の拡張子] と [除外する拡張子] に追加の拡張子を追加するかまたは除外します。

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

入力が完了したら [OK] をクリックします。画面が閉じます。

2. 特定の MIME コンテンツタイプを選択的に無視するように 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 コンテンツタイプ] 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 コンテンツタイプ] に、無視する MIME コンテンツタイプを入力します。たとえば、image/、audio/、application/x-director video/、application/pdf です。詳細については、付録 B「ファイルタイプと MIME コンテンツタイプの対応」を参照してください。

[MIME タイプの検証を有効にする] チェックボックスをオンにして、実際のファイルタイプの検索を有効にすることもできます。このオプションによって、MIME ストリームでの実際のファイルタイプのチェックが有効になります。ただし、すべての MIME タイプが正確に検出されるわけではありません。誤検出が発生する場合は、MIME タイプの検証を無効にして、代わりにコンテンツタイプを使用します。

IntelliTrap には次のようなオプションがあります。

- ・ 検索ポリシーごとに [ウイルス検索ルール] タブで有効 / 無効にできるオプション (IntelliTrap は初期設定で有効)
- ・ 不正な圧縮された実行可能ファイルに対して [処理] タブで指定された処理が実行されるオプション

IntelliTrap を有効 / 無効にするには

- ・ [HTTP] [高度な脅威保護] [ポリシー] | [<ポリシー名>] | [ウイルス / 不正プログラム検索ルール] タブの順に選択し、IntelliTrap セクションの [IntelliTrap を有効にする] チェックボックスをオンにします。

IntelliTrap の詳細については、71 ページの「IntelliTrap パターンファイルおよび IntelliTrap 除外パターンファイル」を参照してください。

ウイルス / 不正プログラム検索設定の優先順位

IWSS は、次の優先順位で検索を実行します。

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

圧縮ファイルの検索制限の設定

圧縮ファイルの検索制限は、ポリシーごとに設定できます ([HTTP] [高度な脅威保護] [ポリシー] [<ポリシー名>] の順に選択して、[ウイルス検索ルール] タブをクリックします)。IWSS は、HTTP ウイルス検索設定画面で指定した条件に従って、圧縮ファイルの内容を開いて検査します。また、IWSS は、設定可能な制限 (圧縮アーカイブ内のファイル数、非圧縮時のファイルサイズ、圧縮レイヤ数、および圧縮率) に従ってファイルを解凍します。

圧縮ファイルの検索制限を設定するには

[圧縮ファイルの処理] で、次の設定を行います。

- ・ 処理: IWSS が圧縮ファイルの違反を検出したときに実行する処理 ([放置]、[ブロック]、または [隔離]) を選択します。
- ・ 適用先: 次のオプションのいずれかを選択します。
 - ・ すべての圧縮ファイル: 圧縮ファイルをダウンロードするすべての要求が一致対象となります。

- ・ 圧縮ファイルが次の場合：設定された条件を超える圧縮ファイルをダウンロードする要求のみが一致対象となります。次のパラメータの値を入力します。
 - ・ 解凍ファイルの数が次を超える場合（初期設定は 50000）
 - ・ 解凍ファイルのサイズが次を超える場合（初期設定は 200MB）
 - ・ 圧縮レイヤが次の数を超える場合（範囲は 0 ~ 20、初期設定は 10）
 - 「0」を指定した場合は、本機能が無効になります。
 - ・ 圧縮率が 99% を超える場合（初期設定は無効）

IWSS は、指定された条件を満たす圧縮ファイルに対して検索をスキップします。たとえば、図 7-9 に示されているように設定されているとします。

圧縮ファイルの処理

処理: ブロック ▼

適用先:

- すべての圧縮ファイル
- 圧縮ファイルが次の場合:
 - 解凍ファイルの数が次を超える場合: (1-999999)
 - 解凍ファイルのサイズが次を超える場合: MB ▼ (1-99999)
 - 圧縮レイヤが次の数を超える場合: (0-20)
- 圧縮率が99%を超えています(99%未満のファイルはIWSSで自動的に許可されます)。

図 7-9. 「解凍の割合」を使用して IWSS デバイスに対する DoS 攻撃を防ぐことができる

圧縮レベルが 10 を超える、または含まれるファイル数が 10,000 を超える圧縮ファイルは、ゲートウェイ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場合、ユーザの期待するパフォーマンスとセキュリティ維持の間でのトレードオフが必要となります。ウイルス検索の本質上、サイズの大きいファイルの場合、ファイル全体を IWSS に転送してファイルを検索し、ファイル全体をクライアントに転送するために、ダウンロード時間が 2 倍かかります。環境によっては、2 倍かかるダウンロード時間を受け入れられない場合があります。ネットワークの速度やサーバの機能など、考慮する必要のある要素がほかにもあります。サイズの大きいファイルの処理を実行するほどサイズが十分に大きくない場合は、そのファイルは普通のファイルとして検索されます。

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

- ・ 169 ページの「配信前に検索」
- ・ 170 ページの「遅延検索」

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、検索が進行中であることをユーザに通知するために、進行ステータス画面が生成されます。

注意： サイズの大きいファイルを処理する場合、IWSS では進行ステータス画面においてダウンロードの進行ステータスを表示します。

進行ステータス画面が機能するには、外部に見えているどの IP アドレスにクライアントが接続するかを IWSS が判別する必要があります。127.0.0.1 を使用すると問題が生じます。進行ステータス画面に関するメッセージが表示された場合、ホスト名による解決が 127.0.0.1 にならないように、コンピュータの IP アドレスを `iscan_web_server` に追加する (例: `iscan_web_server=1.2.3.4:8443`) か、または `/etc/hosts` ファイルを変更します。

注意： YouTube、Windows Update、ストリーミングなどのインターネットアプリケーションでは、特定の時間内に一定量のデータをクライアント側で受信するようプログラミングされているものがあります (たとえば、90 秒以内に 20% のデータまたは 1MB のデータを受信するようプログラミングされているものなど)。配信前に検索するオプションを IWSS が使用するよう設定されている場合、要求されたファイルは検索が終了するまでクライアントに渡されません。この場合、インターネットアプリケーションでは、クライアント側が時間内に必要なデータを受信していないために転送エラーを検出する場合があります。そうなると、クライアント側ではビデオファイルやストリーミングファイルを処理できません。

遅延検索

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、検索が実行されている間に、設定可能な割合の Web ページがクライアントに配信されます。ただし、ウイルス検索によって検索が中断された場合、Web ページ全体は配信されません。検索せずにクライアントに定期的に送信する受信データの割合の値を 100% に設定した場合、最後の 4KB は検索が完了するまでクライアントに送信されません。遅延検索オプションを使用する場合は、検索せずにクライアントに定期的に送信する受信データの割合を設定します。

ダウンロードするデータの割合 (%) には、20、40、60、80 (初期設定)、または 100 を指定できます。ブラウザに送信されたデータの実際の割合は、指定された値よりかなり少ない場合があります。

注意： Blue Coat Port 80 Security Appliance を ICAP モードで使用する場合、サイズの大きいファイルを処理できません。さらに、ICAP モードで Blue Coat Security Appliance を使用している場合は、クライアントがサイズの大きいウイルス感染ファイルをダウンロードしたときに、クライアントブラウザにウイルスブロック通知画面が表示されないことがあります。代わりに、クライアントブラウザには、「Page cannot be displayed」と表示されます。ただし、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。

IWSS が受信した外部データは、検索が行われないうまま、より小さいブロック単位でブラウザに送信されます。最後のブロックがブラウザに送信されると、データセット全体に対して検索が行われ、ダウンロードが完了します。ブロック送信によって、IWSS と Web ブラウザ間の接続が維持されるだけでなく、ダウンロードの進行状況がエンドユーザに示されます。

サイズの大きいファイルの処理は、ポリシーごとに設定できます ([HTTP] [高度な脅威保護] [ポリシー] [<ポリシー名>] の順に選択して、[ウイルス / 不正プログラム検索ルール] タブをクリックします)。



図 7-10. サイズの大きいファイルに対する特殊処理の 2 つのオプション: (1) 配信前に検索と (2) 遅延検索

サイズが非常に大きいファイルのダウンロード時に生じるパフォーマンスの問題を軽減するには、[検索するファイルサイズの上限] オプションをオンにして、サイズの大きいファイルの検索を無効にします。これによって、整合性を制御できるようになります。

サイズの大きいファイルの検索を無効にするには

- ・ [サイズの大きいファイルの処理] で [検索するファイルサイズの上限] チェックボックスをオンにして、検索するファイルサイズの上限を設定します。
- ネットワークにセキュリティの脆弱性が生じるため、サイズの大きいファイルであっても、検索は無効にしないことをお勧めします。

HTTP ウィルス検索でサイズの大きいファイルの処理を使用するには

1. [サイズの大きいファイルの処理] で [特殊処理を有効にする] チェックボックスをオンにして、サイズの大きいファイルと見なすファイルサイズ (KB または MB の単位) を入力します。
2. 使用するサイズの大きいファイル処理のタイプを選択します。

- ・ 配信前に検索 検索中の進行ステータスをクライアント上に表示し、その後ファイルを
検索します。
 - ・ 遅延検索 検索中にファイルの一部をクライアントに配信し、ウイルスが見つかったと接
続を停止します (初期設定)。
3. [保存] をクリックします。

サイズの大きいファイルの処理に関する重要な注意

- ・ サイズの大きいファイルの処理に違反すると、要求元のクライアントのブラウザにユーザ通知
が表示されます。図 7-11 の例を参照してください。

Trend Micro InterScan Web Security イベント

HTTP/HTTPSダウンロードファイルがブロックされました

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

イベント詳細:

URL: http://10.204.170.87/TESTDATA/virus/NonCleanable/p1_100M.zip

処理: 削除

詳細:

-- ファイル: aa.aa、添付ファイル: p1_100M.zip、不正プログラム: **Exceed_File_Count_Limit**
ファイルが削除されました。

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

Trend Micro InterScan Web Security Suite: rhel60x64-56

図 7-11. 検索の完了およびファイルのダウンロード後の通知

- ・ サイズの大きいファイルの特殊処理は、HTTP 検索、FTP 検索、および HTTP プロキシを介した FTP over HTTP にのみ適用されます。ICAP トラフィックの FTP over HTTP には適用されません。FTP over HTTP を使用してサイズの大きいファイルをダウンロードしているとき、タイムアウトの問題が発生する場合があります。
- ・ IWSS では、「遅延検索」を使用している場合、最初に感染ファイルをダウンロードしたクライアントに対してはファイルが削除されず、配信されます。

隔離ファイルの処理

IWSS が不正ファイルとして検出したファイルを隔離する場合、[隔離ファイルを暗号化する] チェックボックスをオンにすると、ファイルを暗号化してから隔離ディレクトリに移動できます。これにより、意図せずにファイルを実行してしまったり、開いたりしてしまう可能性がなくなります。暗号化されたファイルは、トレンドマイクロのサポートエンジニアによってのみ暗号を解除できることに注意してください。

[HTTP] [高度な脅威保護] [ポリシー] のポリシーの追加 / 編集画面で HTTP ウィルス検索ルールを設定したら、[次へ] をクリックしてスパイウェア検索ルールに移動します。

スパイウェア検索ルール

IWSS が使用するパターンファイルには、コンピュータウィルスのほかに、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、ウィ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
- ・ ダイアラー ユーザのモデムを通じてひそかに課金式の電話番号や国際電話番号にダイヤルするソフトウェア
- ・ ハッキングツール 不正なハッキング目的に使用できるソフトウェア
- ・ パスワードクラックソフト コンピュータのパスワードおよびその他の認証スキームを無効にするために設計されたソフトウェア
- ・ アドウェア ユーザのブラウザまたはポップアップウィンドウにユーザを対象とする広告を表示するために、ユーザの Web 閲覧動作に関する情報を監視および収集するソフトウェア
- ・ ジョークプログラム ユーザを困らせたり不適切な警告を発したりするプログラム
- ・ リモートアクセスツール コンピュータへのアクセスが許可されるように設計されたソフトウェアで、多くの場合ユーザの承諾を得ていません
- ・ その他 上記の分類に当てはまらないファイル。このうち一部は、不正な行動を取る可能性があるだけでなく、合法的な目的を持つツールまたは商用ソフトウェアである場合があります。

スパイウェアおよびその他の不正プログラムを検索するには

1. [HTTP] [高度な脅威保護] [ポリシー] [<ポリシー名>] の順に選択して、[スパイウェア検索ルール] タブをクリックします。[その他の不正プログラムに対する検索] で、検出するその他の脅威の種類を選択します。

パターンファイルにシグネチャがあるすべての脅威を検索するには、[すべて選択] をオンにします。

2. [次へ] をクリックして、セキュリティの脅威に対する処理を設定します。

HTTP検索ポリシー: ポリシーの追加

ポリシー名: (Test)

1. アカウントの選択

2. Webレピュテーションルールの指定

3. ウイルス検索ルールの指定

4. **スパイウェア検索ルールの指定**

5. ポスト検出ルールの指定

6. 除外リストの指定

7. 処理の指定

その他の不正プログラムに対する検索:

すべて選択

スパイウェア

アドウェア

ダイヤラー

ジョークプログラム

ハッキングツール

リモートアクセスツール

パスワード解読アプリケーション

その他 ⓘ

戻る 次へ キャンセル

図 7-12. スパイウェアおよびその他の脅威の検索の設定

高度な脅威保護のパフォーマンスに関する注意事項

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

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

MIME コンテンツタイプによってファイルの検索を除外するように設定されている場合、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（この機能が有効になっているとき）、宣言された MIME タイプと照合します。ファイルの実際のファイルタイプが、トランザクションに添付されているコンテンツタイプヘッダに示されているのとは異なる MIME タイプにマップされている場合、そのファイルは検索対象になります。ただし、ファイルタイプと MIME タイプとの間に常に明確なマッピングがあるわけではありません。実際のファイルタイプのオプションが無効になっている場合、IWSS では実際のファイルタイプが MIME タイプにマップされないため、設定されているコンテンツタイプヘッダに従って検索は省略されます。

ファイル拡張子に基づいてファイルを検索から除外できます。トレンドマイクロは、除外する MIME コンテンツタイプのリストを最小限に抑えることをお勧めします。一般的に、ファイルを検索するかどうかの判断を検索エンジンに任せの方が、検索を省略するファイルタイプを自分で選択するより安全です。1 つ目の理由として、HTTP ヘッダのコンテンツタイプが、ダウンロードするコンテンツの実際のタイプを正確に表していない場合があります。2 つ目の理由として、テキストファイルのように除外しても安全と思われるタイプが実際には安全でない場合があります。スクリプトはテキストファイルであり、不正なコードが含まれている可能性があります。その他に MIME コンテンツの除外を使用できるのは、セキュリティとパフォーマンスのトレードオフを意識的に行っている場合です。たとえば、Web トラフィックの多くはテキストであり、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 コンテンツの除外リストに `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完全に選別することが重要です。

X-Forwarded-For HTTP ヘッダ

X-Forwarded-For (XFF) HTTP ヘッダは、クライアントが HTTP プロキシまたはロードバランサ経由で Web サーバに接続する際に、クライアントの元の IP アドレスを識別するための事実上の業界標準となっています。X-Forwarded-For ヘッダは大部分のプロキシサーバでサポートされており、IWSS では IPv6 X-Forward-For ヘッダがサポートされています。IPv4 アドレスの動作と同様に、ヘッダを構文解析してクライアントの IPv6 アドレスにアクセスできます。

IWSS ではまた、IPv4 と同様に IPv6 アクセスのために 3 つの処理を実行します。これには、「X-Forwarded-For ヘッダの維持」および「X-Forwarded-For ヘッダの削除」機能が含まれます。

- ・ IWSS は XFF ヘッダを含む HTTP 要求を受け取ると、XFF ヘッダを構文解析して、クライアントの元の IP アドレスを取得し、その IP アドレスを使用してポリシーマッチングを実行します。
- ・ IWSS は HTTP 要求の転送時に、XFF HTTP ヘッダで管理者により設定された処理を実行します。表 7-5 を参照してください。

注意： IWSS では、HTTPS トラフィックに対する XFF ヘッダの構文解析をサポートしません。

表 7-5. XFF HTTP ヘッダに利用可能な処理

処理	説明
X-Forwarded-For ヘッダの維持	IWSS は XFF HTTP ヘッダを変更しません。
IWSS が要求を受信する IP アドレスの追加	IWSS は XFF HTTP ヘッダに最後のホップの IP アドレスを追加します。XFF HTTP ヘッダが存在しない場合、IWSS は新規に作成します。
X-Forwarded-For ヘッダの削除	(初期設定) IWSS は HTTP 要求から XFF HTTP ヘッダを削除することで、クライアントの個人情報がアップストリームへ漏えいしないようにします。

表 7-6 を参照して、配信シナリオが XFF HTTP ヘッダを使用して機能することを確認します。

表 7-6. X-Forwarded For HTTP ヘッダを使用した配信シナリオ

配信モード	XFF の構文解析	処理：維持	処理：IP アドレスの追加	処理：削除	注意
プロキシ転送モード	使用可	使用可	使用可	使用可	
通常の透過モード	使用可	使用可	使用可	使用可	

表 7-6. X-Forwarded For HTTP ヘッダを使用した配信シナリオ (続き)

配信モード	XFF の構文解析	処理：維持	処理：IP アドレスの追加	処理：削除	注意
ICAP モード	該当なし	該当なし	該当なし	該当なし	IWSS は ICAP サーバとしての役割を果たします。クライアントおよびサーバとの通信は行いません。IP アドレスは、X-Client-IP ヘッダを持つ ICAP クライアントにより提供されます。
リバースプロキシモード	該当なし	該当なし	該当なし	該当なし	XFF HTTP ヘッダはこのモードではサポートされません。

X-Forwarded-For HTTP ヘッダの設定

IWSS では、主に次の 2 つの設定シナリオがあります。

- ・ XFF HTTP ヘッダの構文解析を有効または無効にする
- ・ XFF HTTP ヘッダで実行される処理を設定する

XFF HTTP ヘッダモジュールを設定するには

1. [HTTP] [設定] [X-Forwarded-For ヘッダ] に移動します。
2. XFF HTTP ヘッダの構文解析を有効または無効にします。
 - ・ 有効にするには、ドロップダウンリストから [有効にする] を選択します。
 - ・ 無効にするには、ドロップダウンリストから [無効にする] を選択します。
3. 処理を [X-Forwarded-For ヘッダの維持] (初期設定)、[IWSS が要求を受信する IP アドレスの追加]、または [X-Forwarded-For ヘッダの削除] (初期設定) に設定します。(表 7-5 を参照)。
4. [保存] をクリックします。

ボットおよび C&C コンタクト検出ルールの指定

ネットワーク環境内で起こり得るボットの動作を監視および分析するために、ボット検出ルールに一致したときの処理を指定できます。[HTTP] [高度な脅威保護] [ポリシー] | [ポリシー] | [ボット検出ルール] タブに移動します。ボット /C&C 検出ルールの使用を有効または無効にするには、[このポリシーでボット /C&C 検出ルールを使用する] チェックボックスをオンまたはオフにします。ボット検出の処理も選択できます。

除外リストの指定

[HTTP] [高度な脅威保護] [ポリシー] | [<ポリシー名>] | [除外設定] タブを参照してください。

除外リストに対してウイルス / スパイウェア検索および圧縮ファイルの処理を省略するように IWSS を設定できます。そのため、この除外 Web サイトがハッキングされ、不正プログラムコードが埋め込まれることによって、セキュリティホールの原因になる可能性があります。IWSS の場合は、初期設定でウイルス / スパイウェア検索機能が有効になっているため、この問題が回避されます。したがって、セキュリティポリシーで Web サイトが除外リストに含まれていることが判別されている場合でも、必ず Web ページの検索が実行されます。

除外リストは、[除外設定] 画面で適用できます。HTTP および FTP 検索ポリシーの場合、ファイル名除外リストも適用できます。[除外リスト] 画面で新しい除外リストを作成することができます (詳細については、179 ページの「除外リストの作成」を参照してください)。

次に、[除外設定] 画面のオプションについて説明します。

- ・ 承認する URL リスト URL フィルタポリシー、HTTPS 復号化ポリシー、HTTP 検査ポリシー、情報漏えい対策ポリシー、または HTTP 検索ポリシーの WRS ルールおよびファイルタイプのブロックから除外することを承認された URL リストの名前を選択します。
- ・ 除外ファイル名リスト ファイルタイプのブロックから除外するファイル名のリストを選択します。ファイル名除外リストは、HTTP 検索ポリシー、情報漏えい対策ポリシー、または FTP 検索ポリシーに適用できます。このオプションは、HTTPS 復号化ポリシー、HTTP 検査ポリシー、および URL フィルタポリシーには使用できません。

- ・ 選択した除外リストの内容を検索しない 除外リストにある URL またはファイルの内容についてウイルス検索をしないようにする場合、このオプションを選択します。このオプションが選択されている場合は、圧縮ファイルを処理できません。

HTTP検索ポリシー: ポリシーの追加

ポリシー一覧 > (ポリシー) ☑ ポリシーを有効にする

1. アカウントの選択
2. Webレビュテーションルールの指定
3. ウイルス検索ルールの指定
4. スパイウェア検索ルールの指定
5. ボット検出ルールの指定
6. 除外リストの指定
7. 処理の指定

ポリシー除外

承認するURLリスト:

除外ファイル名リスト:

選択した除外リストの内容を検索しない ⓘ

備考: 除外リストは、[HTTP]→[設定]→[除外リスト] で定義します。

戻る 次へ キャンセル

図 7-13. ポリシー除外の設定

除外リストの作成

[除外リスト] 画面で新しい URL およびファイル名除外リストを作成できます。

URL 除外リストを設定するには

1. 管理コンソールから [HTTP] [設定] [除外リスト] の順に選択し、[URL リスト] タブをクリックします。
2. [追加] をクリックして、名前または一致対象のタイプを指定するか、URL 除外リストをインポートします。
 - ・ リスト名 除外リストの簡単でわかりやすい名前を入力します。
 - ・ 一致 フィールドに、Web サイト、キーワードまたはフレーズ、あるいは文字列を入力します。このフィールドには、ワイルドカードとして「?」および「*」を使用できます。このフィールドに入力された内容は除外リストに 1 つずつ追加されます。

3. [一致] への入力内容に対応するオプションを選択します。

- ・ 前方一致 検索対象を文字列全体に制限します。この除外ルールを1つ以上のワイルドカードとともに使用すると、Web サイト全体へのアクセスを許可する場合に特に便利です。URL に「http://」や「https://」を入力する必要はありません（自動的に削除されます）。IWSS では、Web ページの国際化ドメイン名を使用できます。Web サイトのドメイン名の前には「@」文字が追加されます。
- ・ 部分一致 URL 内の任意の文字または数値から成る文字列を検索します。文字列が存在する場所に関係なく一致対象となります。たとえば「http://www.playboy.com/partner.htm」は、文字列「partner」の一致対象と見なされ、この URL は除外対象となります。このフィールドにワイルドカードを使用すると、誤検出や予期しない結果になる可能性が非常に高くなります。
- ・ 完全一致 検索対象を文字列全体に制限します。たとえば、特定のサイト、ページ、ファイル、その他の特定のアイテムを検索対象にします。

注意： プロキシモードの場合、IWSS は完全な URL ではなくドメイン名を照合します。したがって、ドメイン名のみを指定する必要があります。

- ・ 除外リストのインポート ウイルス検索や (URL フィルタモジュールで実行する) フィルタから除外する URL の既存のリストをインポートできます。たとえば、トレンドマイクロの WebManager から取得した URL のリストや、テキストエディタを使用して編集した URL のリストがある場合、それらの URL を1つ1つ入力する代わりに、そのリストをインポートすることができます。インポートリストは、規定の基準に適合する必要があります。181 ページの「除外リストの形式」を参照してください。

4. [保存] をクリックします。

ファイル名除外リストを設定するには

1. 管理コンソールから [HTTP] [設定] [除外リスト] の順に選択し、[ファイル名リスト] タブをクリックします。
2. [追加] または [編集] をクリックして一致対象のタイプを指定するか、URL 除外リストをインポートします。
 - ・ リスト名 除外リストの簡単でわかりやすい名前を入力します。
 - ・ 一致 ファイル拡張子付きのファイル名またはファイル拡張子をフィールドに入力します。このフィールドには、ワイルドカードとして「*」を使用できます。このフィールドに入力された内容は除外リストに1つずつ追加されます。

- ・ 除外リストのインポート ウイルス検索から除外するファイル名の既存のリストをインポートできます。たとえば、トレンドマイクロの Web サイトから取得したファイル名のリストや、テキストエディタを使用して編集したファイル名のリストがある場合、それらの URL を 1 つ 1 つ入力する代わりに、そのリストをインポートすることができます。インポートリストは、規定の基準に適合する必要があります。181 ページの「除外リストの形式」を参照してください。

3. [保存] をクリックします。

除外リストの形式

IWSS では、2 種類の除外リスト (URL およびファイル名) がサポートされています。次に、それぞれのリスト形式について説明します。

[approved] 形式を使用した除外リストはインポートできます。[blocked] 形式を使用したブロックリストと [allowed] 形式を使用した許可リストはインポートできません。

除外 URL リストの形式

除外 URL リストには、次のヘッダを含む任意の ASCII テキストファイルを指定できます。

[approved]

除外リストに含める URL の数に制限はありません。Web アドレス、URL、文字列は改行で区切ります。除外リストには、ワイルドカードとして「?」および「*」を使用できます。

サンプルファイル:

[approved]

www.good-job-habits.com/*

www.business-productivity.com/*

ファイル名リストの形式

除外ファイル名リストには、次のヘッダを含む任意の ASCII テキストファイルを指定できます。

[approved]

除外リストに含めるファイル名の数に制限はありません。ファイル名および文字列は改行で区切ります。除外リストには、ワイルドカードとして「*」を使用できます。

サンプルファイル:

[approved]

abcfile.doc

*.sc

ウイルス検出時の処理設定

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

検索処理

[HTTP] [高度な脅威保護] [ポリシー] | [<ポリシー名>] | [処理] タブには、ウイルス検索の結果に対して IWSS が実行できる次の 4 つの処理があります。

- ・ 感染ファイルを削除するには、[削除] を選択します。要求元クライアントはファイルを受信しません。この処理は、感染ファイル (1 次処理)、2 次処理、パスワードで保護されたファイル、および検索の制限条件外のファイルの検索イベントに適用できます。
- ・ ファイルをクリーンナップせずに隔離ディレクトリに移動するには、[隔離] を選択します。

```
/var/iwss/quarantine
```

要求元クライアントはファイルを受信しません。この検索処理は、すべての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、173 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、検索の制限条件外のファイル、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次の処理を設定できます。

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



図 7-14. HTTP ウイルス検索ポリシー処理の設定

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] を使用します。[HTTP] [高度な脅威保護] [ポリシー] | [<ポリシー名>] | [処理] タブを参照してください。

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



第8章

アクセス割り当てと URL アクセス設定

アクセス割り当ては、クライアントの帯域幅の使用を一定時間ごとに制限します。「URL の信頼」では、信頼する URL を検索とその他の Trend Micro InterScan Web Security Suite (以下、IWSS) の操作対象から除外することにより、閲覧パフォーマンスを改善できます。URL ブロックでは、指定した URL への要求を拒否します。

本章で説明する内容には、次の項目が含まれます。

- ・ 186 ページの「アクセス割り当てポリシーについて」
- ・ 188 ページの「URL アクセス管理の概要」
- ・ 189 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について

IWSS には、他のクライアントに対する定義可能なポリシーがあります（グローバルポリシーにアクセス割り当てではありません）。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、[ポリシー配信設定] 画面（[管理] [一般設定] [ポリシー配信]）で設定されたキャッシュ生存期限（TTL）値に従ってポリシーをリロードします。

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

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

アクセス割り当てポリシーの管理

アクセス割り当てポリシーの範囲に含めるクライアント、帯域幅の割り当て、および割り当て期間の間隔を設定できます。アクセス割り当てポリシーは、IPv4 クライアントの場合と同様に IPv6 クライアントにも適用できます。アカウントフィールドでは IPv6 アドレスがサポートされます。任意の IPv6 ホストに 1 つのルールを定義すると、クライアントが IWSS を介してインターネットにアクセスしたときにこのポリシールールがトリガされます。

使用可能なポリシーの選択時には、IPv4 と IPv6 の両方のポリシーが表示されます。[アカウント] フィールドで入力可能なアカウントエントリは、IPv4 でサポートされているものと同様に、単一の IPv6 アドレス、IPv6 アドレス範囲、または IPv6 ネットワークマスクです。

アクセス割り当てポリシーを追加するには

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

アクセス割り当て間隔の値は、すべての既存のポリシーを含め、すべてのアクセス割り当てポリシーにグローバルに適用されます。

4. [保存] をクリックします。

5. [追加] をクリックします。
6. [ポリシーを有効にする] チェックボックスをオンにして、アクセス割り当てを入力します。
7. ポリシーを適用するユーザを選択します。

この画面のオプションは、使用しているユーザの識別方法に応じて異なります。[IP アドレス]、[ホスト名 (変更された HTTP ヘッダ)]、または [ユーザ / グループ名認証] (LDAP) のいずれかになります。これらの設定値は、[管理] [一般設定] [ユーザの識別] | [ユーザの識別] タブで設定されます。ユーザの識別方法の設定とポリシー適用範囲の設定の詳細については、108 ページの「ユーザ識別方法の設定」を参照してください。

設定したユーザの識別方法に関係なく、ポリシーを適用するクライアントの IP アドレスを入力できます。

8. ポリシーに関する特別な情報がある場合は、必要に応じて備考を入力します。
9. [保存] をクリックします。
10. [アクセス割り当てポリシー] 画面に戻ったら、[ポリシーの配信] をクリックして、ただちにポリシーを適用します。すぐに適用しない場合、ポリシーはデータベースキャッシュの有効期限が切れた後に適用されます。

データベースから設定を削除せずに、一時的にポリシー設定を解除したい場合は、ポリシーを無効にすることができます。

ポリシーを無効にするには

1. 管理コンソールから [HTTP] [アクセス割り当てポリシー] の順に選択します。
2. [アクセス割り当てポリシー] 画面から、[アカウント] 列または [アクセス割り当て] 列のいずれかにあるリンク項目をクリックして、[ポリシーの編集] 画面を表示します。
3. 画面の上部にある [ポリシーを有効にする] チェックボックスをオフにして、[保存] をクリックします。

ポリシーを無効にしても、ポリシーキャッシュが更新されるか、または [ポリシーの配信] をクリックするまでポリシーは無効になりません。

クライアントを使用している従業員が組織を退職した場合など、ポリシーがまったく必要なくなった場合、ポリシー全体を削除するか、または IWSS データベースからポリシーの範囲内のユーザを削除できます。

ポリシーを削除するには

1. 管理コンソールから [HTTP] [アクセス割り当てポリシー] の順に選択します。
2. [アクセス割り当てポリシー] 画面からポリシーを選択して、[削除] をクリックします。

ポリシーを削除しても、ポリシーキャッシュが更新されるか [ポリシーの配信] をクリックするまでポリシーは削除されません。

URL アクセス管理の概要

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

URL フィルタモジュールでは、URL が属するカテゴリに基づき、Web アクセスが許可されたり、拒否されたりします。Web レピュテーションは、要求された URL が、ハッキングの可能性のあるフィッシング脅威かファームিং脅威か、または信頼できないレピュテーションスコアでないかという判断に基づいて、Web アクセスを許可または拒否します。URL フィルタモジュールも Web レピュテーションも、ポリシー内でユーザが設定することにより管理されます。[HTTP] [URL アクセス設定] を参照してください。

ユーザが Web サイトにアクセスしようとする、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 (188 ページの「URL アクセス管理の概要」を参照)。URL が URL ブロックリストで見つかった場合、要求が拒否されます。URL が信頼する URL リストで見つかった場合、アクセスが許可され、アクセス制御は実行されません。
- URL がブロックリストでも信頼するリストでも見つからなかった場合、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。指定されたセキュリティレベルによって、IWSS がその URL をブロックするかどうかが決まります (157 ページの「Web レピュテーションルールの指定」を参照)。URL が除外リストにある場合、IWSS では、その URL に対するフィッシングおよびファームিং検出を省略します (178 ページの「除外リストの指定」を参照)。
- その後で、Web レピュテーションは、要求された URL がフィッシング脅威かファームিং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 (158 ページの「フィッシング対策、ファームিং対策、および C&C コールバック試行検出」を参照)。
- Web レピュテーションの最後のプロセスは、URL のカテゴリを決定することです。カテゴリ情報は、後で、URL フィルタモジュールで使用されます。
- Web レピュテーションが、URL の評価、フィッシングフラグまたはファームングフラグ、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ム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、URL フィルタモジュールを使用している場合、このモジュールが、要求された URL についての Web カテゴリ情報を使用して、アクセスを許可するかどうかを判断します。
URL が除外リストにある場合、カテゴリフィルタが無視され、URL アクセス管理の最終段階に進みます。
要求された URL のカテゴリが URL フィルタポリシーで許可されている場合、URL の処理は最終段階に送られます。許可されていない場合、URL はブロックされます。
- ・ 最後に、Web レピュテーションの URL 評価に基づいて、IWSS では、要求された URL が検索ポリシーで指定されたセキュリティレベルより上か下かを判断します。
URL が除外リストにある場合、IWSS はその URL のセキュリティレベルチェックを省略します (178 ページの「除外リストの指定」を参照)。
評価がセキュリティレベルを下回っていた場合、要求された URL はブロックされます。ただし、評価がセキュリティレベルを上回っていた場合、IWSS ではその URL へのアクセスを許可します。

URL アクセス管理の設定

IWSS では、低リスクサイトの閲覧パフォーマンスを改善するために、一部の信頼する URL を検索およびフィルタから除外できます。ユーザ設定のリストを使用して、サイトへのアクセスをブロックすることもできます。

信頼する URL の設定

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 は検索されないため、閲覧パフォーマンスが改善します。信頼する URL にふさわしいのは、頻繁にアクセスされる Web サイトで、自分の会社のイントラネットサイトのように、管理できるコンテンツが含まれているものです。

信頼する URL の情報は `/etc/iscan/TrustedURLs.ini` ファイルにあります。
`TrustedURL.ini` ファイルのパスは、`/etc/iscan/intscan.ini` 設定ファイルの `[URL-trusting]` セクションにある `normalLists` パラメータを使用して設定されます。

信頼する URL を設定する際、次のものを使用してサイトを指定できます。

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

それ以外の場合には信頼する URL のリストの条件に一致するサイトが、通常どおり 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 サイトや文字列のリストを含むファイルの一番上にコメントまたはタイトルを記述し、1 行ごとにルールを 1 つ記述します。コメントまたはタイトルは IWSS では無視されます。次の例で示すように、[allow] の下に信頼するグループサイトを、[block] の下に信頼する URL リストで除外するグループサイトを記述します。

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

```
[allow]
```

```
unwanted.com*
```

```
www.blockedsite.com*
```

```
urlkeyword
```

```
banned.com/file
```

```
banned.com/downloads/
```

```
[block]
```

```
www.blockedsite.com/file
```

```
www.unwanted.com/subsite/
```

注意： HTTPS 復号化ポリシーの場合、一致対象の文字列は、IWSS の設定がプロキシモードかどうかによって異なります。プロキシモードの場合、完全な URL ではなく、ドメイン名が一致対象となります。そのため、ドメイン名を指定するだけで済みます。

信頼する URL と除外設定を管理するには

1. 管理コンソールから [HTTP] [URL アクセス設定] [グローバル URL の信頼] の順に選択します。
2. [URL の信頼] 画面で、[URL の信頼を有効にする] チェックボックスをオンにして、URL の信頼を有効にします。

警告： [URL の信頼を有効にする] オプションを選択すると、信頼する URL の内容に対してフィルタおよびウイルスの検索は行われなくなります。

3. 信頼する URL を指定する方法を選択します。
 - ・ 前方一致 (すべてのサブサイトを含む)
 - ・ 完全一致 (URL に文字列が含まれること)
4. [一致] に URL 文字列を入力して [信頼する] をクリックし、[信頼リスト] の下に表示されている信頼する URL リストに追加します。信頼する URL を除外するには、[信頼しない] をクリックして除外リストに追加します。
5. 信頼リストまたは除外リストから URL を削除するには、削除する項目を選択して [削除] をクリックします。[すべて削除] をクリックすると、すべて削除されます。
6. [保存] をクリックします。

信頼する URL リストとその除外設定をインポートするには

1. [HTTP] [URL アクセス設定] [グローバル URL の信頼] の順に選択します。
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、[信頼リスト / 除外リストのインポート] に入力します。
3. [インポート] をクリックします。インター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、グローバルブロック URL リストにある Web サイトと URL 文字列をブロックできます。

注意： ICAP プロキシハンドラをインストールしている場合、この機能を作動させるためには、事前キャッシュ (precache) リクエストモードでファイルを検索するように ICAP クライアントを設定してください。

HTTPS Web サイトは、スタンドアロン / 依存プロキシモードで FQDN を入力することでブロックできます。

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

- ・ サブサイトを含む Web サイト
- ・ 部分一致のキーワード
- ・ 要求された URL 内の完全一致文字列

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、`/etc/iscan/URLB.ini` ファイルに保持されます。URLB.ini ファイルのパスは、`/etc/iscan/intscan.ini` ファイルの [URL-blocking] セクションにある「normalLists」パラメータを使用して設定されます。

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

ローカルリストの使用

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

URL を [ブロックリスト] および [除外リスト] に追加する場合、まず一方のリストにすべて追加して設定を保存してから、他方のリストへの追加操作を実行する方法をお勧めします。この方法により、同一の URL が両方のリストに存在するようにできます。URL を [ブロックリスト] に追加するか、または [除外リスト] に追加しようとするとき、その URL がすでに他のリストに存在している場合、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] [グローバル 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. [URL ブロック] 画面で、[キーワード] に Web アドレス全体、URL キーワード、完全一致文字列のいずれかを入力します。

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

- a. [キーワード] に「`www.blockedsite.com`」と入力し、[ブロックする] をクリックします。
- b. [キーワード] に「`www.blockedsite.com/charity/`」と入力し、[ブロックしない] をクリックします。スラッシュなしで `charity` と記述すると、IWSS は `www.blockedsite.com/charity` をファイルと見なします。

注意： HTTPS 復号化ポリシーの場合、一致対象の文字列は、IWSS の設定がプロキシモードかどうかによって異なります。プロキシモードの場合、完全な URL ではなく、ドメイン名が一致対象となります。そのため、ドメイン名を指定するだけで済みます。

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 行目にわかりやすいタイトルまたはコメントを入力し、1 行ごとにルールを 1 つ記述します。例で示すように、[block] の下にブロックするグループサイトを、[allow] の下に除外するグループを記述します。たとえば、次のように記述します。

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

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

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

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

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

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

ブロックする URL のリストをインポートするには

1. 前述のように、ブロックする URL とすべての除外設定を含むテキストファイルの形式を設定します。
2. 管理コンソールから [HTTP] [URL アクセス設定] [グローバル URL ブロック] の順に選択します。

3. [参照] をクリックして、インポートするファイルの場所を [ブロックリスト / 除外リストのインポート] に指定し、[インポート] をクリックします。
4. [保存] をクリックします。

URL フィルタ

本章では、URL フィルタポリシーの作成と設定の手順を示しながら、InterScan Web Security Suite (以下、IWSS) の URL フィルタモジュールの概要および設定作業の流れについて説明します。

URL フィルタは、Web レピュテーションとともに IWSS に搭載された、多層かつ複合型の脅威に対する保護ソリューションです (188 ページの「URL アクセス管理の概要」を参照)。

本章で説明する内容には、次の項目が含まれます。

- ・ 196 ページの「URL フィルタについて」
- ・ 199 ページの「URL フィルタポリシーの管理」
- ・ 203 ページの「URL フィルタの設定」
- ・ 208 ページの「URL フィルタの割り当てた時間の延長」

URL フィルタについて

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し、従業員の業務に無関係な Web サイトの不正利用を防ぐことにあると想定しています。ただし例外が必要な場合もあるため、より広範なアクセスを必要とする業務に携わる従業員には、制限されたカテゴリグループへのアクセスが許可されるように追加のポリシーを作成できます。たとえば、組織で許容できるインターネット利用ポリシーの違反について調査するために、人事部門または IT 部門の従業員が無制限のインターネットアクセスを必要とする場合があります。

IWSS では、検索エンジンのフィルタプロバイダ (Google や Yahoo など) によって提供される安全な検索機能がサポートされます。安全な検索は、検索結果からアダルトサイトやアダルトコンテンツをフィルタする際に使用され、子供にアダルトコンテンツを見せないようにします。

さらに IWSS では、動的なフィルタを高度な Web レピュテーションデータベースと組み合わせることにより、フィルタ機能が向上しています。オンライン取り引き、ショッピング、オークション入札、出会い系、ギャンブル、およびその他の仕事に関係しない活動の Web サイトを業務時間中に閲覧することで従業員の生産性は低下し、正当な閲覧のために利用可能な帯域幅が減少します。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。

[HTTP] [URL フィルタ] [ポリシー] | [<ポリシー名>] | [ルール] タブを参照してください。

IWSS の URL フィルタポリシーには、インターネットアクセスを管理するための柔軟できめの細かいメカニズムが用意されています。各ポリシーには、次のような 3 つの基本的な要素があります。

- IWSS では、「ギャンブル」、「ゲーム」、「出会い系」など 82 を超えるカテゴリに属する URL を格納する Web レピュテーションデータベースにアクセスできます。カテゴリは次の論理グループに含まれます。
 - カスタムカテゴリ
 - ネットワーク帯域幅
 - インターネットセキュリティ
 - コミュニケーション / メディア
 - アダルト
 - ビジネス
 - ライフスタイル
 - 一般
- 各カテゴリの Web サイトへのアクセスは、予約期間オブジェクトとして指定された期間中、許可、ブロック、または監視できます。

- ・ 使用する環境で、ユーザごとに異なるポリシーを設定できます。

対象カテゴリにあるすべての識別された URL へのアクセスは、ポリシーに従って管理されます。各 URL は、データベースで 1 つ以上のカテゴリに関連付けられています。Web サイトを正確に定義するために、URL は複数の URL カテゴリに属することができます。たとえば、不正プログラムが存在するショッピングサイトは、「ショッピング」カテゴリと「不正プログラム流布」カテゴリに属することができます。URL を分類する URL カテゴリの数に応じて、URL フィルタポリシーによるアクセスの管理方法を変えることができます。組織でアクセスする必要のある URL が禁止されたカテゴリに関連付けられている場合、URL フィルタルールの除外設定を作成して、データベースの分類を変更できます。許可する URL リストで指定された文字列は、対象の URL と比較されるのであって、対象の URL が参照するドキュメントのコンテンツとは比較されません。IWSS では、Web サイト、URL キーワード、および完全一致文字列により、URL フィルタの許可リストを設定するオプションが用意されています。

IWSS の初期設定の URL 分類を省略するもう 1 つの方法は、カスタムカテゴリを作成して、ユーザのアクセスを許可するために必要なアクセス権限を割り当てることです。

URL フィルタ処理

次に、予約期間オブジェクトを使用して特定のポリシーに対して適用できるフィルタ処理を示します。

- ・ 許可 対象サーバへの接続が許可され、ユーザはその Web サイトにアクセスできます。
- ・ ブロック 対象サーバへの接続が確立されず、ユーザはその Web サイトにアクセスできません。このイベントについてはログエントリも作成されます。
- ・ 次のポリシーに一致 対象サーバへの接続は、次のレベルで設定されたポリシーに応じて異なります。
- ・ オーバーライド付きブロック ユーザがカテゴリブロックを無効にするための特定のパスワードを入力可能でない限り、対象のサービスへの接続は確立されません。

注意：「オーバーライド付きブロック」処理をカテゴリに適用する場合、管理者は、ポリシー作成時にオーバーライド用に使用するパスワードを設定する必要があります。

- ・ 監視 対象サーバへの接続が許可され、ユーザはその Web サイトにアクセスできます。このイベントについてはログエントリも作成されます。
- ・ 時間制限 管理者によって設定された期間に、選択したカテゴリの URL へアクセスする対象サーバへの接続が許可されます。

注意： カテゴリに対して「時間制限」処理を選択するには、管理者がカテゴリリストの下の [時間制限の設定] で [時間割り当て] テキストボックスに値を入力する必要があります。

時間割り当ての値には5の倍数を指定する必要があります。これは時間割り当ての実装方法に起因するものです。初期設定の割り当て単位は5分です。[時間割り当て] の値は5の倍数にすることをお勧めします。それ以外の場合、IWSSでは5未満の端数は無視されます。たとえば、値を4分に設定すると、IWSSはそれを0分と解釈します。値を9分に設定すると、5分として解釈されます。

時間割り当ての設定はシステム時間に依存します。たとえば、現在10時3分で、時間割り当ての値が5の場合、エンドユーザのアクセス時間は2分のみになる場合があります。これは、時間割り当てが5分ずつに区切られている (10:00 ~ 10:05、10:05 ~ 10:10 など) ことによるものです。5分ごとに新しい区切りが始まります。

- ・ **警告** 対象サーバへの接続は許可されますが、会社のポリシーに違反するカテゴリに属するURLにアクセスしようとするすると警告する通知が表示されます。ユーザは、ページへのアクセスを続行するか、前のページに戻るか選択できます。

URL フィルタの設定作業の流れ

URL フィルタを設定するには、対象の URL とユーザの ID (IP アドレス、IP アドレスの範囲、IP サブセット、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、108 ページの「ユーザ識別方法の設定」を参照)。

ユーザが要求した URL は、7つの事前定義されたグループにまとめられている、82を超えるカテゴリのうち1つ以上のカテゴリに分類できます。要求された URL は、IWSS の URL フィルタエンジンに渡され、要求元のユーザに対するポリシーに従ってフィルタされます。要求された URL の分類先のカテゴリとポリシーの処理に基づいて、その URL は許可、ブロック、監視されるか、または警告が発行されます。

注意： URL フィルタエンジンに対する手動アップデートは、[手動アップデート] 画面で実行できます。

URL フィルタポリシーの管理

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、ゲストアカウントで 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 が次のように設定されている場合にのみサポートされます。

- ゲストアクセスを許可（認証方法にキャプティブポータルを使用）
- 配置ウィザードでプロキシ転送モードを選択した後にゲストユーザログインポートを有効化

URL フィルタの有効化

URL フィルタモジュールが有効になっていることを確認してから、作業を開始してください。アカウントフィールドでは IPv6 アドレスがサポートされます。任意の IPv6 ホストに 1 つのルールを定義すると、クライアントが IWSS を介して Web サイトにアクセスしたときにこのポリシールールがトリガされます。

ポリシーの選択時には、IPv4 と IPv6 の両方のポリシーが表示されます。[アカウント] フィールドで入力可能なアカウントエントリは、IPv4 でサポートされているものと同様に、単一の IPv6 アドレス、IPv6 アドレス範囲、または IPv6 マスクです。

IWSS は、IPv6 で「URL 警告モード」機能をサポートしており、クライアントの IP アドレスのバージョンに基づいて、IWSS の IPv6 または IPv4 アドレスへの警告メッセージが自動的にクライアントにリダイレクトされます。

- ・ クライアントが IPv4 アドレスを使用する場合、IWSS は、リダイレクト要求を IWSS の IPv4 アドレスとともに送信します。
- ・ クライアントが IPv6 アドレスを使用する場合、IWSS は、リダイレクト要求を IWSS の IPv6 アドレスとともに送信します。

URL フィルタを有効にするには

1. 管理コンソールから [HTTP] [URL フィルタ] [ポリシー] の順に選択します。
2. [URL フィルタを有効にする] チェックボックスをオンにします。
3. [保存] をクリックします。

動的な URL カテゴリ分類の有効化

IWSS では、トレンドマイクロの URL フィルタリングエンジン (TMUFE) を使用して URL をフィルタします。アクセスされた URL が TMUFE データベースに存在しない場合、IWSS は動的な URL カテゴリ分類テクノロジーを使用して、Web サイトのコンテンツと HTTP URL に基づいて Web サイトのリアルタイムのカテゴリ分類を実行します。

動的な URL カテゴリ分類では、キーワード、ルール、および Web サイトを除外するその他の情報を含むパターンファイルを使用します。

動的な URL カテゴリ分類を有効にするには

1. 管理コンソールから [HTTP] [URL フィルタ] [ポリシー] の順に選択します。
2. [動的な URL カテゴリ分類を有効にする] を選択します。
3. [保存] をクリックします。

新しいポリシーの作成

新しい URL フィルタポリシーを作成するには、次の 4 つの手順に従います。

- ポリシーを適用するアカウントを選択します。
- 予約期間オブジェクトで定義された期間に、許可、ブロック、監視、または警告する Web サイトのカテゴリを指定します。
- 安全な検索の設定を選択します。
- 除外リストを選択します。

新しいポリシーを作成するには

1. IWSS Web コンソールを開き、管理コンソールから [HTTP] [URL フィルタ] [ポリシー] の順に選択します。
2. [追加] をクリックします。
[URL フィルタポリシー: ポリシーの追加] 画面が表示されます。
3. わかりやすい [ポリシー名] を入力します。
「研究者向け URL フィルタポリシー」のように、適用対象となるユーザまたはグループへの参照が含まれるポリシー名は簡単に覚えられます。
4. ポリシーを適用するユーザを選択します。
この画面のオプションは、使用しているユーザの識別方法に応じて異なります。[IP アドレス]、[ホスト名 (変更された HTTP ヘッダ)]、または [ユーザ / グループ名認証] (LDAP) のいずれかに

なります。ユーザの識別方法の設定とポリシー適用範囲の設定の詳細については、108 ページの「ユーザ識別方法の設定」を参照してください。

5. [次へ] をクリックします。
6. [ルールの指定] 画面で、[ポリシーを有効にする] チェックボックスがオンになっていることを確認します。
7. 各 URL カテゴリまたはサブカテゴリに対して、次のフィルタ処理のいずれかを選択します。
 - ・ 許可 対象サーバへの接続が許可され、ユーザはその Web サイトにアクセスできます。
 - ・ ブロック 対象サーバへの接続が確立されず、ユーザはその Web サイトにアクセスできません。このイベントについてはログエントリも作成されます。
 - ・ 次のポリシーに一致 対象サーバへの接続は、次のレベルで設定されたポリシーに応じて異なります。
 - ・ オーバーライド付きブロック ユーザがカテゴリブロックを無効にするための特定のパスワードを入力可能でない限り、対象のサービスへの接続は確立されません。
 - ・ 監視 対象サーバへの接続が許可され、ユーザはその Web サイトにアクセスできます。
 - ・ 時間制限 管理者によって設定された期間に、選択したカテゴリの URL へアクセスする対象サーバへの接続が許可されます。
 - ・ 警告 対象サーバへの接続は許可されますが、会社のポリシーに違反するカテゴリに属する URL にアクセスしようとするすると警告する通知が表示されます。ユーザは、ページへのアクセスを続行するか、前のページに戻るか選択できます。
8. 予約期間オブジェクトで定義された期間中フィルタ処理を適用するよう選択します。
 - ・ スケジュールの選択 適用するフィルタ処理を選択してから、予約を設定します。グループの全カテゴリを選択するには、グループのチェックボックスをクリックします。グループ内のすべてのカテゴリを選択するのに、グループを展開する必要はありません。アクセスを制限する期間は、[URL フィルタ設定] 画面 ([業務時間] タブ) で定義されます。詳細については、206 ページの「予約期間の設定」を参照してください。
9. [適用] をクリックして、選択したカテゴリにフィルタ処理を適用します。

注意： 同じグループのサブカテゴリに別のフィルタ処理を適用する場合は、手順 8 と 9 を繰り返します。

10. (オプション) [パスワードの上書きの設定] で、ブロック処理を無効にするために使用されるパスワードを入力する必要があります。これは、URL フィルタカテゴリに対して「オーバーライドによるブロック」処理設定を使用するためのポリシーを設定する場合にのみ必要です。

注意： パスワードはポリシーごとに個別に設定できます。

11. 今後の参照のためにこのポリシーに関して役立つ情報を含めるには、オプションの [備考] を入力します。
12. [次へ] をクリックします。
13. 各検索エンジンに安全な検索の設定を選択し、[次へ] をクリックします。
 - ・ 厳密 すべての検索結果 (画像、ビデオ、Web 検索を含む) からアダルトコンテンツを排除します。
 - ・ 適度 Web 検索のみの結果 (イメージ検索を除く) からアダルトコンテンツを排除します。
 - ・ オフ 検索結果のフィルタを行いません。このオプションは初期設定です。
14. 除外リストを適用する場合、[除外リストの指定] 画面で、ドロップダウンリストボックスから除外 URL リスト名を選択します。除外リストにある URL は、URL フィルタ処理が省略されません。
15. [保存] をクリックします。
16. [URL フィルタポリシー] 画面で、[優先度] 列に表示されている上向きまたは下向きの矢印をクリックして、新しいポリシーの優先順位を設定します。

2 つ以上のポリシーに属するアカウントがある場合、[優先度] の設定により、どのポリシーが適用されるかが決まります。複数のポリシーに属するアカウントに対しては、最初に一致したポリシーが実行されます。最初に一致したポリシーが実行された後は、そのアカウントを含むポリシーは省略されます。
17. [保存] をクリックします。
18. ポリシーをただちに適用するには、[ポリシーの配信] をクリックします。すぐに適用しない場合、データベースキャッシュの有効期限が切れた後に、このポリシーが適用されます。

ポリシーの変更と削除

IWSS では、使用する環境により適合するように、任意で既存のポリシーを編集するオプションが用意されています。ポリシーから不要なアカウントを削除することもできます。

既存のポリシーを変更するには

1. 管理コンソールから [HTTP] [URL フィルタ] [ポリシー] の順に選択します。
2. 変更するポリシーの [アカウント名] リンクまたは [ポリシー名] リンクをクリックします。
3. [URL フィルタポリシー : ポリシーの編集] 画面が開きます。

- ・ [アカウント] タブでクライアントを追加または削除することにより、ポリシーの範囲を変更します。
 - ・ [ルール] タブから、URL カテゴリのフィルタ処理を変更します。
 - ・ [安全な検索エンジン] タブから、検索エンジンごとに安全な検索モードを変更します。
 - ・ [除外設定] タブから、このポリシーに適用する除外リストを選択します。
4. [保存] をクリックします。
 5. [HTTP] [URL フィルタ] [ポリシー] の順に選択し、矢印を使用してポリシーの優先順位を設定します。2 つ以上のポリシーに属するアカウントがある場合、[優先度] の設定により、どのポリシーが適用されるかが決まります。
 6. [保存] をクリックします。
 7. ポリシーをただちに適用するには、[ポリシーの配信] をクリックします。すぐに適用しない場合、データベースキャッシュの有効期限が切れた後に、このポリシーが適用されます。

URL フィルタの設定

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

- ・ 7 つの論理グループに分けられた 82 を超える事前定義された Web サイトカテゴリ
- ・ 独自のカスタムカテゴリの設定
- ・ [予約期間] で定義された時間オブジェクトを選択します。

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

カスタムカテゴリの作成

トレンドマイクロからあらかじめ提供されているカテゴリのほかに、新しい URL カテゴリを定義することができます。たとえば、競合企業の URL を格納する、「競合他社の Web サイト」というカテゴリを作成することができます。

[HTTP] [設定] [カスタムカテゴリ] 画面には、ユーザ定義カテゴリのリストが表示されます。[追加] をクリックして新しいカテゴリを作成するか、カテゴリ名をクリックして既存のカテゴリを編集します。

- ・ カテゴリ名 短くてわかりやすいカスタムカテゴリ名を入力します。名前は一意に指定する必要があります。

- ・ 一致 フィールドに、Web サイト、キーワードまたはフレーズ、あるいは文字列を入力してから、一致条件を適用する方法を指定します。このフィールドには、ワイルドカードとして「?」および「*」を使用できます。このフィールドに入力された内容はカスタムカテゴリに1つずつ追加されます。

注意： HTTPS 復号化ポリシーの場合、一致対象の文字列は、IWSS の設定がプロキシモードかどうかによって異なります。プロキシモードの場合、完全な URL ではなく、ドメイン名が一致対象となります。そのため、ドメイン名を指定するだけで済みます。

- ・ 前方一致 文字列全体が検索対象となるように制限します。この設定を1つ以上のワイルドカードとともに使用すると、設定した URL フィルタ処理を Web サイト全体に適用する場合に特に便利です。URL に「http://」や「https://」を入力する必要はありません（自動的に削除されます）。
- ・ 部分一致 URL 内の任意の文字または数値から成る文字列を検索します。文字列が存在する場所に関係なく一致対象となります。たとえば「http://www.encyclopedia/content/sextan.htm」は、文字列「sex」の一致対象と見なされ、このページはブロックされます。このフィールドにワイルドカードを使用すると、誤検出や予期しない結果になる可能性が非常に高くなります。
- ・ 完全一致 文字列全体が検索対象となるように制限します。たとえば、特定のサイト、ページ、ファイル、その他のアイテムを検索対象にします。
- ・ カスタムカテゴリリストのインポート カテゴリに追加する URL の既存のリストをインポートできます。たとえば、テキストエディタを使用して編集した競合他社の URL のリストがある場合、それらの URL を1つ1つ入力する代わりに、そのリストをインポートすることができます。インポートリストは、規定の基準に適合する必要があります（詳細については、オンラインヘルプを参照してください）。

URL カテゴリの見直しの依頼と URL 検索

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「インターネットセキュリティ」グループの「ジョークプログラム」カテゴリに属しています。

初期設定の URL 分類に同意できない場合は、トレンドマイクロにカテゴリの見直しを提案できます。除外リストやカスタムカテゴリを使用して、トレンドマイクロの URL フィルタデータベースで分類されたドメインおよび Web サイトの評価を省略することもできます。

URL フィルタポリシーを適用する前に、初期設定の分類が組織に対して適切かどうか確認することをお勧めします。たとえば、衣料販売業者は、正当な市場調査や競合他社の調査ができるように、「アダルト」グループに分類された「下着 / 水着」カテゴリから水着の Web サイトを除外する必要がある場合があります。

URL のカテゴリを知りたい場合には、[HTTP] [URL フィルタ] [設定] | [URL の再分類と検索] タブで URL フィルタ設定を指定すると調べることができます。

未評価の URL および不明 URL

トレンドマイクロが認識していながら、まだフィルタカテゴリに加えられていない Web サイトの評価は「未評価」の URL とされます。

次に該当する場合は、Web サイトの評価は「不明」URL とされます。

- ・ トレンドマイクロが認識しておらず、Web レピュテーションデータベースに存在していない Web サイト
- ・ サービスが機能していないか、URL を評価するリモート評価サーバにアクセスできない場合
不明 URL の評価は「0」となり、ブロックできません。

URL カテゴリの見直し依頼

URL カテゴリの見直しを依頼するには

1. 管理コンソールから [HTTP] [URL フィルタ] [設定] の順に選択します。
2. [URL の再分類と検索] タブを選択します。
3. [Trend Micro Site Safety Center](#) へのリンクをクリックします。
[Trend Micro Online URL Query - Feedback System] 画面が表示されます。
4. フィールドに疑わしい URL を入力し、[今すぐ確認] をクリックします。



図 9-1. [Trend Micro Online URL Query - Site Safety Center] 画面

5. 変更を提案するには、[評価内容変更のリクエスト] をクリックして、必要な情報を入力します。

注意： トrendマイクロからの回答を保証するものではありません。

予約期間の設定

IWSS では、異なる処理に対する日数と時間を設定できます。

URL フィルタのポリシーを作成する際に、特定の時間範囲に対して有効になるようポリシーを設定します。

組織内で URL フィルタポリシーを実装する前に、予約期間に対して新しい時間オブジェクトを作成することをお勧めします。

URL フィルタポリシーのスケジュールを設定するには

1. IWSS Web コンソールを開き、[管理] [一般設定] [予約期間] の順に選択します。
2. 時間オブジェクトの名前と説明を指定します。処理を適用する期間を選択します。

3. [保存] をクリックします。

URL 警告の TTL

URL アクセスの警告の有効期間 (TTL) 設定を使用すると、管理者は、ユーザが再表示を選択した場合に、初回の警告メッセージが表示されてから次の警告メッセージが表示されるまでの時間間隔を設定できます。

注意： 警告メッセージの反復表示は、初回の警告メッセージの表示後にユーザがその Web ページの続行を選択した場合にのみ実行されます。

[HTTP] [URL フィルタ] [設定] [URL 警告の TTL] タブの順に選択して、URL アクセスの警告の有効期間 (TTL) を変更できます。

初期設定値は、5 分です。これは、ユーザ別 / カテゴリ別に設定できます。

警告メッセージは、URL フィルタのポリシーで処理が [警告] に設定されている場合に表示されません。詳細については、200 ページの「新しいポリシーの作成」を参照してください。

通知の詳細については、257 ページの「URL アクセスの警告通知の設定」を参照してください。

URL フィルタの除外設定

IWSS では、除外リストによって URL フィルタに例外を設定することができます (178 ページの「除外リストの指定」を参照)。除外リスト内の URL は、ブロックも監視もされません。URL フィルタによってブロックまたは監視されている Web サイトをクライアントで表示する正当な必要性がある場合、その URL を除外 URL リストに含めて、そのリストをポリシーに適用します。

注意： IWSS は、安全な検索のフィルタを、除外 URL リストにある Web サイトに適用します。

除外 URL リストを URL フィルタポリシーに適用するには

1. IWSS Web コンソールを開き、[HTTP] [URL フィルタ] [ポリシー] の順に選択して、ポリシー名をクリックしポリシーを編集します。
2. [除外設定] タブで、除外 URL リスト名を選択します。

注意： URL が除外リストに登録されていると、警告は行われません。詳細については、257 ページの「URL アクセスの警告通知の設定」を参照してください。

3. [保存] をクリックします。

URL フィルタの割り当てた時間の延長

時間割り当ての延長は、「時間制限」処理が指定された URL フィルタポリシーに使用されます。IWSS システム管理者が制限時間の経過後も特定の個人にインターネットの閲覧を許可する場合は、ここで時間を延長できます。割り当てられた時間に達すると、ユーザに通知が送信されます。各自の割り当てを使い果たしたユーザはログに記録されます。

このページには次の情報が表示されます。

- ・ ユーザ 名前または IP アドレスによってユーザが識別されます。管理者は、ユーザの検索や、ユーザ名を基準にした並べ替えも実行できます。
- ・ 毎日の時間割り当て 閲覧に使用可能な時間量に関するポリシーで割り当てられた時間を表示します。
- ・ 割り当てられた時間の延長 すでに時間が延長されている場合にその時間を表示します。
- ・ 毎日使用される時間割り当て 閲覧に使用された時間の合計を表示します。これには元来割り当てられていた時間と延長された時間、または、使用された時間延長部分を含めることができます。
- ・ 割り当ての延長 延長を設定する場所で、次の指定が可能です。
 - ・ チェックボックス 時間を延長するにはオンにします。
 - ・ 値 延長したい時間を指定します。
 - ・ 単位 延長時間の単位で、分または時間を指定します。

注意： 時間は、URL フィルタポリシーでポリシールールの構成部分として「時間制限」処理が含まれている場合にのみ延長できます。

インターネット閲覧の割り当て時間を延長するには

1. [HTTP] [アクセス割り当てポリシー] [URL フィルタの割り当てた時間の延長] に移動します。
2. ユーザ列を並べ替えるか、検索フィールドを使用して該当するユーザを見つけます。

3. 該当するユーザの行の [割り当ての延長] 列に移動します。
4. 時間の延長を可能にするには、チェックボックスをオンにします。
5. 延長の範囲とする時間数を入力し、適切な単位 (時間または分) を選択します。
6. [保存] をクリックして、延長を適用します。



第10章

FTP 検索

本章では、InterScan Web Security Suite (以下、IWSS) の FTP ウイルス検索について説明します。また、お使いの環境に合わせて FTP 検索を導入し、設定するさまざまな方法についても説明します。

本章で説明する内容には、次の項目が含まれます。

- ・ 212 ページの「FTP 検索について」
- ・ 212 ページの「FTP 設定」
- ・ 214 ページの「FTP 検索オプション」
- ・ 217 ページの「FTP 検索の設定」
- ・ 219 ページの「ウイルスに対する検索処理の設定」
- ・ 222 ページの「FTP アクセス管理設定」

FTP 検索について

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コネクションの種類（パッシブモードまたはアクティブモード。213 ページの「パッシブおよびアクティブモード」を参照）を制御する FTP 設定を実行します。次に、検索するトラフィックの方向、ブロックまたは検索するファイルのタイプ、圧縮ファイルおよびサイズの大きいファイルの処理方法、および不正コードの検出時に実行する処理を制御する検索ルールを設定します。

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

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 プロキシを使用するプロキシ設定のオプション、アクティブモードとパッシブモードを選択するデータコネクションのオプションが含まれています。

プロキシ設定

IWSS の FTP 検索には、2 つのプロキシ設定オプションがあります。1 つはクライアントが 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 プロキシ設定で FTP サーバのホスト名または IP アドレスとポート番号を指定することによって、単一の FTP サーバを保護するために使用することもできます。この場合、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。

パッシブおよびアクティブモード

IWSS では、ファイアウォール設定に応じて、データコネクシオンにアクティブモードまたはパッシブモード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。アクティブモードでは、サーバがクライアントに接続してデータコネクシオンを確立します。パッシブモードでは、クライアントがサーバに接続します。

IWSS の設定でパッシブモードが選択されると、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。

クライアント要求

FTP を設定するには、プロキシ設定とデータコネクシオンを指定する必要があります。

FTP プロキシでは、IPv4 FTP プロキシの場合と同様に IPv6 FTP プロキシがサポートされ、Web コンソールでは IPv4 アドレスと IPv6 アドレスの両方が受け入れられます。

IWSS は、FTP プロキシサーバとして実行することもできます。複数のサーバの FTP アップロードを保護するには、サーバごとに IWSS FTP モジュールをインストールしてください。

FTP の設定を行うには

1. 管理コンソールから [FTP] [設定] [一般] の順に選択します。
2. [プロキシ設定] で、構成に基づいて適切な FTP 設定を選択します。ネイティブ 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る場合は、[FTP プロキシを使用] を選択し、[プロキシサーバ] にホスト名を入力して、[ポート番号] を指定します。
3. 使用するデータコネクシオンの種類を、[パッシブモード] または [アクティブモード] のいずれかから選択します。
4. [保存] をクリックします。

FTP 検索オプション

IWSS では、事前定義されたポリシーに従って、IPv4 と IPv6 の両サーバの FTP トラフィックを検索できます。

プロキシ転送モードの場合、IWSS は以下に説明する配信シナリオをサポートしており、IWSS をデュアルスタックネットワーク環境に展開したときには、FTP、HTTP、HTTPS トラフィックについて IPv4 ネットワークと IPv6 ネットワーク間の自動切り替えを実行できます。このため、IPv4 クライアントから IPv4 クライアントへのアクセスや IPv6 クライアントから IPv4 サーバへのアクセスだけでなく、IWSS プロキシによって IPv4 クライアントから IPv6 サーバ、または IPv6 クライアントから IPv4 サーバへのアクセスも可能になります。

表 10-1. サポートされているプロキシ転送モードの検索シナリオ

番号	クライアント	サーバ	サポートの有無
1	IPv4	IPv4	有
2	IPv6	IPv6	有
3	IPv4	IPv6	有
4	IPv6	IPv4	有

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

- FTP 検索では、ユーザまたはグループベースのポリシーはサポートされません。そのため、1 つの設定が 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 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。

検索対象

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。

ブロックするファイルタイプ

セキュリティ、監視、またはパフォーマンス上の目的のためにブロックするファイルのタイプを指定できます。ブロックできるのは、Java クラスファイル、Microsoft Office 文書、オーディオ / ビデオ、実行可能ファイル、画像、アーカイブ、または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 は該当するファイルをブロックします。

検索するファイルタイプ

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

- すべての検索可能ファイル — すべてのファイルが検索されます。最も安全なオプションです。
- トレンドマイクロの推奨設定 — ウイルスが潜むことがわかっているファイルタイプのみが検索されます。ファイルタイプはファイルヘッダを確認することによって決定されます。詳細については、163 ページの「トレンドマイクロの推奨設定について」を参照してください。
- 指定のファイル拡張子 — 指定したファイル拡張子を持つファイルのみが検索されます。

パフォーマンス上の理由で他のオプションを選択する必要がある場合を除き、すべてのファイルを検索することをお勧めします。詳細については、217 ページの「FTP 検索の設定」を参照してください。

FTP 検索設定の優先順位

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

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

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、隔離、または放置するオプションが用意されています。

また、次の条件のいずれかを満たす圧縮ファイルに選択した処理を適用するように IWSS を設定することもできます。

- ・ 解凍後のファイル数が設定した最大値を超える場合
- ・ 解凍後のファイルの累積サイズが設定した最大値を超える場合
- ・ 多重圧縮されたファイルの圧縮レイヤ数が設定した最大値を超える場合

注意： IWSS では、FTP 検索中も圧縮ファイル内の指定したファイルタイプをブロックできます。

サイズの大きいファイルの処理

サイズの大きいファイルのダウンロード時に遅延を発生させたくない場合、設定したしきい値より大きいファイルの検索を省略するように 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、170 ページの「遅延検索」を参照してください。

注意： FTP 検索モジュールでは、サイズの大きいファイルを処理する方法として HTTP 検索モジュールで使用される「配信前に検索」はサポートされていません。

隔離ファイルの暗号化

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、誰かが隔離ディレクトリを参照中に誤ってファイルを実行しないように、オプションでファイルを暗号化できます。暗号化されたファイルは、トレンドマイクロのサポート部門の担当者以外は暗号化を解除できないため注意してください。

スパイウェアの検索

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を使用してスパイウェアを検索することもできます。これらのリスクの概要については、173 ページの「スパイウェア検索ルール」を参照してください。

情報漏えい対策

IWSS の FTP 検索では、[HTTP] [情報漏えい対策] [テンプレート] で作成した DLP テンプレートを使用して情報漏えいを検索できます。[FTP] [検索ルール] | [情報漏えい対策] タブで、DLP テンプレートの名前を選択し、適用する特定のフィルタを使用して許可、ブロック、または監視するかどうかに基づいて検索条件を変更します。

FTP 検索除外リスト

ファイルタイプブロックから除外するファイル名を、除外リストに含めることができます。さらに、除外リストにあるファイルに対してウイルス / スパイウェア検索および圧縮ファイルの処理を省略するように、IWSS を設定することもできます。

詳細については、178 ページの「除外リストの指定」を参照してください。

FTP 検索の設定

FTP 検索の設定を行うには

1. 管理コンソールから [FTP] [検索ルール] の順に選択します。
2. [FTP 検索を有効にする] チェックボックスをオンにします。
3. [アップロード]、[ダウンロード]、またはその両方から、検索する FTP 転送の種類を選択します。

4. [ブロックするファイルタイプ] で、ブロックするファイルタイプを選択します。
5. 検索するファイルを選択します。
 - ・ 拡張子に関係なく、すべてのファイルを検索するには、[すべての検索可能ファイル] を選択します。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。すべてのファイルを検索するのは最も安全な設定です。
 - ・ 実際のファイルタイプによる識別を使用するには、[トレンドマイクロの推奨設定] を選択します。トレンドマイクロの推奨設定では、実際の添付ファイルタイプの検索と正確な拡張子名の検索を組み合わせ使用します。実際の添付ファイルタイプの検索では、ファイルの拡張子の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] 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、処理 (ブロック、隔離、放置) を選択して、処理を次のいずれかに適用することを選択します。
 - ・ すべての圧縮ファイル
 - ・ 圧縮ファイルが次の場合「圧縮ファイルが次の場合」を有効にする場合は、次のパラメータの値を入力します。
 - ・ 解凍ファイルの数が次を超える場合 (初期設定は 50000)
 - ・ 解凍ファイルのサイズが次を超える場合 (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)
 - 「0」を指定した場合は、本機能が無効になります。
 - ・ 圧縮率が 99% を超えている場合 (圧縮率 99% 未満のファイルは IWSS で自動的に許可されます)。
7. [サイズの大きいファイルの処理] で、[検索するファイルサイズの上限] チェックボックスをオンにし、ファイルサイズを入力します。

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

警告： 検索実行前にファイルの一部を配信することで、ウイルス感染の可能性も生じます。そのため、パフォーマンスとセキュリティのバランスは管理者の判断に左右されます。このオプションは、現在タイムアウトの問題が発生している場合にのみ使用してください。

9. 隔離ディレクトリに送信されるファイルを暗号化して、不注意で開かれたり実行されたりするのを防ぐには、[隔離ファイルを暗号化する] を選択します。
10. [保存] をクリックして、[スパイウェア検索ルール] タブに切り替えます。
11. 検索するその他のリスクの種類を選択して、[保存] をクリックします。
12. [情報漏えい対策] タブで、[HTTP] [情報漏えい対策] [テンプレート] で作成した DLP テンプレートを、DLP テンプレートリストから選択します。
13. フィルタルールを変更し、フィルタを使用して検索、ブロック、または監視するかどうかを決定します。[保存] をクリックします。
14. [除外設定] タブで、ドロップダウンリストから除外ファイル名リストを選択します。
除外リストにあるファイルの内容についてウイルス検索をしないようにするには、[選択した除外リストの内容を検索しない] を選択します。この場合、圧縮ファイルの処理は適用されません。
15. [処理] タブに切り替え、検索に対して IWSS で実行する処理を選択します。
16. [保存] をクリックします。

ウイルスに対する検索処理の設定

([FTP] [検索ルール] [処理] タブ) 感染ファイル (1 次処理) 感染ファイルの検出時に FTP 検索で実行する処理を指定できます。推奨される処理設定は [駆除] です。

- ・ 感染ファイル (1 次処理) - 感染ファイルを駆除せずに隔離ディレクトリに移動するには、[隔離] を選択します。要求元クライアントはファイルを受信しません。
- ・ 感染ファイルを削除するには、[削除] を選択します。要求元クライアントはファイルを受信しません。

- ・ 感染ファイルを自動的に駆除して処理するには、[駆除] を選択します。ファイルが駆除可能な場合、要求元クライアントは駆除されたファイルを受信します。

2次処理 ワームやトロイの木馬などの駆除不能ファイルの検出時に FTP 検索で実行する処理を指定できます。推奨される処理設定は [削除] です。

- ・ 駆除できないファイルを駆除せずにクライアントに送信するには、[放置] を選択します。感染ファイルがネットワークに侵入する可能性があるため、この設定はお勧めしません。
- ・ 駆除できないファイルを駆除せずに隔離ディレクトリに移動するには、[隔離] を選択します。要求元クライアントはファイルを受信しません。
- ・ 駆除不能なファイルを削除するには、[削除] を選択します。要求元クライアントはファイルを受信しません。

パスワードで保護されたファイル パスワードで保護された圧縮ファイルに対して FTP 検索で実行する処理を指定できます。推奨される処理設定は [放置] です。

- ・ パスワードで保護されたファイルを駆除せずにクライアントに送信するには、[放置] を選択します。
- ・ パスワードで保護されたファイルを駆除せずに隔離ディレクトリに移動するには、[隔離] を選択します。要求元クライアントはファイルを受信しません。
- ・ パスワードで保護されたファイルを削除するには、[削除] を選択します。要求元クライアントはファイルを受信しません。

マクロ FTP 転送中にマクロ (マクロウイルスに限らず) を含むファイルが検出された場合は、次の処理を実行できます。推奨される処理設定は [放置] です。

- ・ マクロを含むファイルを隔離ディレクトリに移動するには、[隔離] を選択します。
- ・ ファイルの配信前にマクロを削除するには、[駆除] を選択します。
- ・ マクロを含むファイルの特別な処理を無効にするには、[放置] を選択します。

FTP 一般設定

FTP を設定するには、プロキシ設定とデータコネクションを指定する必要があります。

FTP プロキシでは、IPv4 FTP プロキシの場合と同様に IPv6 FTP プロキシがサポートされ、Web コンソールでは IPv4 アドレスと IPv6 アドレスの両方が受け入れられます。

IWSS は、FTP プロキシサーバとして実行することもできます。複数のサーバの FTP アップロードを保護するには、サーバごとに IWSS FTP モジュールをインストールしてください。

プロキシ設定

- ・ スタンドアロンモードを使用 ネットワーク上の唯一の FTP プロキシとして IWSS をインストールする場合は、このオプションを選択します。
- ・ FTP プロキシを使用 ネットワーク上に既存の FTP プロキシとともに IWSS をインストールする場合は、このオプションを選択します。IWSS を FTP プロキシと同一のコンピュータにインストールするか異なるコンピュータにインストールするかによって、次のフィールドの入力値が異なります。
 - ・ プロキシサーバ IWSS が FTP トラフィックを受信する FTP プロキシのホスト名または IP アドレスを指定します。IWSS FTP 検索機能を FTP サーバと同じコンピュータにインストールする場合は、「localhost」を使用します。
 - ・ ポート FTP プロキシが IWSS に FTP トラフィックを送信する際に使用するポート番号を示します。通常はポート 21 です。

データコネクション

ほとんどのファイアウォールは、LAN 外部からの無用なポート要求を拒否するように設定されているため、IWSS ではアクティブ転送とパッシブ転送の両方をサポートしています。パッシブ転送が通常必要となるのは、LAN にファイアウォールがある場合、またはアクティブ FTP を設定する際にデータチャンネルに障害が発生した場合です。

管理コンソールから [FTP] [設定] [一般] の順に選択します。

- ・ パッシブモード パッシブ FTP のみを許可するファイアウォール内で IWSS を実行する場合は、このオプションを選択します。

パッシブ FTP (PASV モード) では、FTP クライアントから FTP サーバに対して問い合わせが開始されます。FTP サーバがこのクライアントに対してデータ転送に使用する接続ポートを通知し、クライアントがこのポート上のサーバに対して別の接続を開きます。

- ・ アクティブモード スタンドアロンでインストールした IWSS をアクティブ FTP を許可するファイアウォール内で実行する場合、またはファイアウォール外で実行するようにインストールした場合 (推奨しません)、このオプションを選択します。

アクティブ FTP では、FTP クライアントから FTP サーバに対して問い合わせが開始され、次にお互いのデータ転送ポートを取り決めます。IWSS では通常はポート 22020 が使用されます。取り決めたポートを使用して、サーバはクライアントに接続しなおします。

注意: このポートに対してはファイアウォールを開き、FTP サーバがクライアントと通信できるようにする必要があります。または、ポートを手動で開く必要があります。

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。
- ・ コンテンツの厳しい管理が可能な信頼するサーバに頻繁にアクセスする場合、そのサーバを許可リストに追加できます。転送が検索されなくなるため、パフォーマンスが向上します。
- ・ 設定したポートへのアクセスを拒否することによって、IWSS の FTP サーバを制限できます。

クライアント IP による設定

初期設定では、FTP トラフィックが有効な場合、ネットワーク上のすべてのクライアントが IWSS デバイス経由で FTP サイトにアクセスできます (214 ページの「FTP トラフィックおよび FTP 検索の有効化」を参照)

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

クライアントの IP アドレスに基づいて **FTP** アクセスを制限するには

1. 管理コンソールで [FTP] [設定] [アクセス管理の設定] の順に選択します。
2. [クライアント IP] タブに切り替えます。
3. [クライアント IP に基づく FTP アクセス管理を有効にする] チェックボックスをオンにします。
4. 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/ ホスト名 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 サブセット 指定したサブネット内の単一のクライアント。たとえば、IP に「192.168.1.0」、マスクに「255.255.255.0」と入力すると、192.168.1.x サブネット内のすべてのコンピュータが識別されます。または、マスクをビット数 (0 ~ 32) で指定することもできます。

5. [説明] にわかりやすい名前を入力します (40 文字以内)。
6. [追加] をクリックして、FTP サイトへのアクセスを許可する他のクライアントの入力を続けます。
7. [保存] をクリックします。

サーバ IP の除外リストによる設定

コンテンツの直接管理が可能な信頼する FTP サイトの場合、サイトへのアクセス時にパフォーマンスの問題が発生する可能性を少なくするために、一部の FTP サイトの IP アドレスを許可リストに追加して、これらのサイトを検索から除外できます。

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

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

信頼するサーバを許可リストに追加するには

1. 管理コンソールで [FTP] [設定] [アクセス管理の設定] の順に選択します。
2. [サーバ IP の除外リスト] タブに切り替えます。
3. 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。サーバの識別方法および例については、97 ページの「クライアントとサーバの識別」を参照してください。
4. [説明] にわかりやすい名前を入力します (40 文字以内)。
5. [追加] をクリックして、除外する他の FTP サイトの入力を続けます。
6. [保存] をクリックします。

宛先ポートによる設定

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

クライアントが接続できる **IWSS FTP** ポートを設定するには

1. 管理コンソールで [FTP] [設定] [アクセス管理の設定] の順に選択します。
2. [宛先ポート] タブに切り替えます。

3. [拒否] または [許可] のいずれかから、ポートに適用する処理を選択します。
4. 処理を適用する [ポート] または [ポート範囲] を入力します。
5. [説明] にわかりやすい名前を入力します (40 文字以内)。
6. [追加] をクリックします。
7. 許可または拒否する他のポートの追加を続けます。
8. [保存] をクリックします。

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



第11章

レポート、ログおよび通知

本章では、管理者が InterScan Web Security Suite (以下、IWSS) のレポート、ログ、および通知により、ゲートウェイのセキュリティに関する情報をタイムリーに取得する方法について説明します。

本章で説明する内容には、次の項目が含まれます。

- ・ 226 ページの「レポートについて」
- ・ 227 ページの「レポートの種類」
- ・ 226 ページの「レポート設定」
- ・ 229 ページの「レポートの生成」
- ・ 233 ページの「ログについて」
- ・ 240 ページの「syslog 設定」
- ・ 240 ページの「通知について」
- ・ 248 ページの「C&C コンタクトコールバック通知の設定」

レポートについて

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、およびアクセスされた URL に関するレポートを生成できます。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、すべてまたは特定のユーザ、ユーザグループ、またはデバイスグループに対するレポートを必要に応じてリアルタイムに、またはスケジュールに従って生成できます。

選択したレポート情報を必要とする人と共有できるように、IWSS では、生成されたレポートをメールに添付して送信できます。

IWSS ユーザアカウントでは、アカウントに関連付けられた役割に基づいてレポートを生成できません。つまり、役割で IP アドレス範囲に関連するデータへのアクセスが許可されている場合、そのユーザアカウントでは、その IP アドレスのみに関するレポートを生成できます。

レポート情報

目的のレポート名と、そのレポートの短い説明を入力します。[使用可] または [使用不可] のいずれかを選択して、レポートを有効にします。

レポート設定

レポートテンプレートを生成する際は、次の情報を指定する必要があります。

- 特定のスケジュールに基づいてレポートを生成するかどうか
- 特定の期間に基づいてレポートを生成するかどうか
- レポートを生成する時間（業務時間、業務時間外、またはカスタマイズした期間フィルタ）
- レポートを生成するデバイスグループ
- 出力の種類（PDF、HTML、または CSV ファイル）
- 保存して保持するレポート数

注意： [レポートの設定] では、時間は次のように指定されます。

過去 1 日間：その日の 00:00 から前に 1 日間

このレポートをメールで送信

すべてのレポートで、

[このレポートをメールで送信] を選択し、次の設定を行います。

- ・ 「送信者」のメールアドレスを入力します。
- ・ 「受信者」のメールアドレスを入力して、レポートの生成後、特定の個人またはメール配信リストにそのレポートのコピーを送信します。
- ・ 目的のメッセージを入力します。
- ・ レポートを添付ファイルとして送信することを「有効」にします。
- ・ メッセージ配信に失敗した場合の通知の選択内容を示します。

作成対象 (ユーザおよびグループ)

レポートを生成する対象のユーザを選択します。次のオプションがあります。

- ・ すべてのユーザ: 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
- ・ 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 [管理] [一般設定] [ユーザの識別 | ユーザの識別] タブ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、108 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、次のカテゴリのレポートを示す棒グラフまたは表を生成できます。

- ・ インターネットセキュリティ 次のインターネットセキュリティの検出上位 n 件を示したレポートが生成されます。
 - ・ 不正プログラム / スパイウェア検出
 - ・ ボットネット検出
 - ・ ドキュメントセキュリティホール APT (標的型サイバー攻撃) 検出
 - ・ カスタム保護 APT ブロック
 - ・ C&C コンタクトアラート件数 (日付別)
 - ・ C&C アドレス

- C&C コンタクトアラートで検出されたユーザ / ホスト
- C&C コンタクトアラートで検出されたグループ
- 最もブロックの多い不正サイト
- 最もブロックの多いユーザ (不正プログラム / スパイウェア別)
- 最もブロックの多いユーザ (不正サイト別)
- 最もブロックの多いグループ (不正プログラム / スパイウェア別)
- 最もブロックの多いグループ (不正サイト別)
- ユーザ (ボットネット検出別)
- HTTP 不正プログラム検索ポリシーに対する最も多い違反
- ブロックされた不正サイト (日付別)
- 不正プログラム / スパイウェア検出 (日付別)
- 不正プログラム / スパイウェア検出傾向
- インターネットアクセス 次のインターネットアクセスの検出上位 n 件を示したレポートが生成されます。
 - 最もアクセスの多いアプリケーション
 - 最もアクセスの多い URL カテゴリ
 - 最もアクセスの多いサイト
 - ユーザ (要求別)
 - グループ (要求別)
 - URL カテゴリ (参照時間別)
 - アクセスサイト (参照時間別)
 - ユーザ (参照時間別)
 - アクセス数 (時間別)
- 帯域幅 次の帯域幅の検出上位 n 件を示したレポートが生成されます。
 - URL カテゴリ (帯域幅別)
 - アプリケーション (帯域幅別)
 - ユーザ (帯域幅別)
 - グループ (帯域幅別)
 - サイト (帯域幅別)
 - 合計トラフィック (日付別)

- ・ ポリシー施行 次のポリシー施行の検出上位 n 件を示したレポートが生成されます。
 - ・ 最もブロックの多い URL カテゴリ
 - ・ 最もブロックの多いアプリケーション
 - ・ 最も施行の多いユーザ
 - ・ 最も施行の多いグループ
 - ・ 最もブロックの多いサイト
 - ・ ユーザ (HTTP 検査別)
 - ・ URL フィルタポリシーに対する最も多い違反
 - ・ アプリケーション制御ポリシーに対する最も多い違反
 - ・ アクセス割り当て管理ポリシーに対する最も多い違反
 - ・ HTTP 検査ポリシーに対する最も多い違反
- ・ データセキュリティ 次のデータセキュリティの検出上位 n 件を示したレポートが生成されます。
 - ・ 最もブロックの多い DLP テンプレート (要求別)
 - ・ 最もブロックの多いユーザ
 - ・ 最もブロックの多いグループ
 - ・ 情報漏えい対策ポリシーに対する最も多い違反
- ・ カスタムレポート レポート対象の定義済みの [お気に入りログ] が含まれます。詳細については、231 ページの「レポートの種類」を参照してください。

レポートの生成

IPv4 の動作と同様に、特定の IPv6 ユーザまたは IPv6 ユーザグループ別にレポートを生成できます。選択したユーザまたはユーザグループのページは、IPv6 アドレスまたは IPv6 アドレス範囲もサポートします。

レポートは、IPv4 ユーザと IPv6 ユーザのどちらの場合も、レイアウト問題が生じることなく、CSV 形式、PDF 形式、または HTML 形式で生成できます。IPv4 の動作と同様に、ユーザ関連のレポートを生成するとき、レポート内ですべての IPv6 ユーザを使用できます。

レポートの設定

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レポートを生成できます。生成したレポートは、PDF 形式、HTML 形式、または CSV 形式で保存できます。

レポートを設定するには

1. 管理コンソールで [レポート] をクリックします。
2. 新しいレポートテンプレートを追加するには、[追加] をクリックします。
3. レポートテンプレートの名前と説明を入力します。テンプレートを有効にする準備ができたら、[はい] をクリックして有効にします。
4. [レポートの設定] でレポートのスケジュールを選択し ([今回のみ]、[今後 1 回のみ]、[毎日]、[毎週]、または [毎月] のいずれか)、次に [レポート期間] を選択します。特定の時間帯にレポートを生成するには [カスタム時間帯] をクリックし、[開始] および [終了] の日付を選択します。
5. 予約期間フィルタ ([常時]、[業務時間]、[業務時間外]、または [管理] [一般設定] [予約期間] でカスタマイズした期間フィルタ) を選択します。
6. デバイスグループを選択します。

注意： デバイスグループを追加するには、[管理] [一般設定] [集中管理ログ / レポート] を選択し、[デバイスグループ管理] の下で [追加] をクリックします。初期設定では、すべてのデバイスが同じグループに追加されます。

7. レポートの出力を選択します。
8. メールの受信者、件名、およびメッセージをオプションとともに設定します。
9. [作成対象] で、レポートを生成する対象として [すべてのユーザ]、[特定のユーザ / グループ] のいずれかを選択します。[指定するユーザ]、[すべてのグループ]、または [指定するグループ] の選択時には IPv6 アドレスも定義できます。指定するユーザまたはグループに対するレポートの詳細については、「特定のユーザまたはグループを選択するには」を参照してください。
10. [レポートの種類] でレポートの種類を選択し、目的のレポートのレコード番号を入力します。

注意： 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。

11. メニューから、グラフの種類 (棒グラフ、表グラフ、または両方) を選択します。
12. [レポートの保存] をクリックします。

次の表は、レポートを構成するパラメータの情報を示しています。

表 11-1. レポートタイプによって異なる使用可能なレポートパラメータ

作成対象	含まれるレポートパラメータ
すべてのユーザ	「個別ユーザレポート」以外のレポートが利用可能です。
特定のユーザ / グループ	「個別ユーザレポート」のレポートのみが利用可能です。
* Web レピュテーションの場合（ファーミング対策、フィッシング対策など）、ブロックされたサイトはこれらのレポートに表示されます。ただし、ブロックされたサイトを検索する場合、情報が記載されているのは「最もブロックの多い不正サイト上位 N 件」のみです。	

特定のユーザまたはグループを選択するには

1. 管理コンソールで [レポート] をクリックします。
2. [作成対象] で [特定のユーザ / グループ] を選択し、[選択] をクリックします。
[管理] [一般設定] [ユーザの識別 | ユーザの識別] で設定したユーザの識別方法に従って、[ユーザの選択] または [グループの選択] ポップアップ画面が表示されます。
3. IP ホスト名またはアドレス範囲を入力するか、「ユーザ / グループ名認証」による識別方法を使用している場合は LDAP ディレクトリでグループ名を検索します。
4. 特定のユーザまたはグループを入力して、[検索] をクリックします。
5. [追加] をクリックします。
6. レポートに含めるグループを追加したら、[保存] をクリックします。

レポートの種類

それぞれのレポートパラメータについて、レポートに出力するレコード数を指定できます。それぞれのレポートの種類について、初期設定には、上位のユーザ、URL、カテゴリなどのレコードが含まれています。99 などの大きな数値を指定すると、レポートサイズと作成時間が影響を受けます。

[上位カテゴリ (重み付け)] というレポートパラメータは、ブロックまたは監視された URL カテゴリも含めて、URL カテゴリに関する情報を提供します。URL カテゴリおよびアクセスされた URL ごとの要求数も示します。この情報は、各種のインターネットグループに対して、どの URL カテゴリをブロックまたは監視する必要があるかを判断する上で参考になります。

レポートパラメータには、次の条件が当てはまります。

- ・ ユーザはアドレス、ユーザ名、またはホスト名です。

- HTTP については、URL アドレスは、トップレベルドメインのみでなく、アドレス全体です。HTTPS については、URL アドレスは、トップレベルドメインのみです。
- 内容は、ユーザ指定の最も頻繁にアクセスされた URL ごとにリストされ、アクセス回数順に表示されます。

管理者はこのアクセスを確認して、要求を許可するかどうかを決定できます。

カスタムレポートでは、カスタマイズしたレポートに保存済みのログまたは「お気に入り」のログを含めることができます。カスタムレポートには、レポートテンプレートの時間範囲および指定されたユーザが使用されます。その他の設定は、お気に入りログの設定と同じです。

レポートの予約

予約レポートを今回のみ、今後 1 回のみ、毎日、毎週、または毎月生成するように IWSS を設定できます。

予約レポートを設定するには

1. 管理コンソールの [レポート] で新しいレポートを作成します。
2. [追加] をクリックするか、レポート名をクリックして編集します。
3. 新しいレポートの名前を入力します。[レポートの設定] で、予約レポートを生成する時間および日付を設定します。
4. [メール] および添付ファイルの形式を選択して、IWSS が生成したレポートを添付ファイルとして送信する先のメールアドレスを入力します。また、[送信者] フィールドと [件名] フィールドにも入力する必要があります。複数のメールアドレスはカンマ (,) で区切ります。

注意： SMTP サーバに関する設定は、[通知] [通知先の設定 ...] で行います。

5. [保存] をクリックします。

作成された予約レポートを削除するには

1. 管理コンソールで [レポート] をクリックします。
2. 削除するレポートテンプレートを選択して [削除] をクリックします。

保存されている予約レポート

予約レポートが生成されると、IWSS は指定されている受信者にレポートを送信し、コピーをデータベースに保存します。保存したレポートを表示またはダウンロードするには、[レポート] の [保存されているレポート] タブをクリックします。IWSS がデータベースに保存する、保存されているレポートの数を設定できます。

ログについて

IWSS データベースは、ログデータを保存しますが、ログデータを CSV ファイルとしてテキストログファイルに保存することもできます。

これにより、以前の IWSS バージョンで使用したり、外部のレポートツールで使用したりすることができます。

注意： [ログ分析] では、時間は次のように指定されます。

過去 1 時間：現在の時刻から、その時刻の 0 分まで

過去 1 日間：現在の時刻から、その時刻の 0 分から前に 23 時間

ログはログのタイプによってカテゴリ分類され、次のようにマップおよびグループ化されます。

- ・ アプリケーション帯域幅
- ・ ポリシー施行
- ・ インターネットアクセス
- ・ インターネットセキュリティ
- ・ データセキュリティ
- ・ アクセス管理

アプリケーション帯域幅

それぞれのログの表示で次のいずれかのフィルタを利用できます。

- ・ 受信トラフィック
- ・ 送信トラフィック
- ・ すべてのトラフィック
- ・ ユーザ名

- ・ デバイスグループ
- ・ クライアント IP
- ・ アプリ ID

時間範囲のフィルタを使用してソートを続行します。[今日]、[過去 1 時間]、[過去 12 時間]、[過去 1 日間]、[過去 7 日間]、または指定した時間範囲を選択できます。表示するインスタンス数を上位 5 件 ~ 20 件の範囲で設定します。結果の出力形式を棒グラフ、線グラフ、円グラフなどから選択します。

ポリシー施行

それぞれのログの表示で次のいずれかのフィルタを利用できます。

- ・ 処理
- ・ メッセージの種類
- ・ デバイスグループ
- ・ クライアント IP
- ・ チャンネル
- ・ アプリ ID
- ・ ポリシー名
- ・ ユーザ名
- ・ URL カテゴリ

時間範囲のフィルタを使用してソートを続行します。[今日]、[過去 1 時間]、[過去 12 時間]、[過去 1 日間]、[過去 7 日間]、または指定した時間範囲を選択できます。表示するインスタンス数を上位 5 件 ~ 20 件の範囲で設定します。結果の出力形式を棒グラフ、線グラフ、円グラフなどから選択します。

インターネットアクセス

それぞれのログの表示で次のいずれかのフィルタを利用できます。

- ・ ドメイン
- ・ デバイスグループ
- ・ クライアント IP
- ・ ユーザ名
- ・ URL カテゴリ

時間範囲のフィルタを使用してソートを続行します。[今日]、[過去 1 時間]、[過去 12 時間]、[過去 1 日間]、[過去 7 日間]、または指定した時間範囲を選択できます。表示するインスタンス数を上位 5 件 ~ 20 件の範囲で設定します。結果の出力形式を棒グラフ、線グラフ、円グラフなどから選択します。

インターネットセキュリティ

それぞれのログの表示で次のいずれかのフィルタを利用できます。

- 処理
- メッセージの種類
- 不正プログラム名
- デバイスグループ
- クライアント IP
- チャンネル
- ポリシー名
- ユーザ名

時間範囲のフィルタを使用してソートを続行します。[今日]、[過去 1 時間]、[過去 12 時間]、[過去 1 日間]、[過去 7 日間]、または指定した時間範囲を選択できます。表示するインスタンス数を上位 5 件 ~ 20 件の範囲で設定します。結果の出力形式を棒グラフ、線グラフ、円グラフなどから選択します。

データセキュリティ

それぞれのログの表示で次のいずれかのフィルタを利用できます。

- 処理
- デバイスグループ
- クライアント IP
- チャンネル
- ポリシー名
- ユーザ名
- ルール名

時間範囲のフィルタを使用してソートを続行します。[今日]、[過去 1 時間]、[過去 12 時間]、[過去 1 日間]、[過去 7 日間]、または指定した時間範囲を選択できます。表示するインスタンス数を上位 5 件 ~ 20 件の範囲で設定します。結果の出力形式を棒グラフ、線グラフ、円グラフなどから選択します。

アクセス管理

それぞれのログの表示で次のいずれかのフィルタを利用できます。

- 処理
- メッセージの種類
- デバイスグループ
- クライアント IP
- チャンネル
- ポリシー名
- ユーザ名

時間範囲のフィルタを使用してソートを続行します。[今日]、[過去 1 時間]、[過去 12 時間]、[過去 1 日間]、[過去 7 日間]、または指定した時間範囲を選択できます。表示するインスタンス数を上位 5 件 ~ 20 件の範囲で設定します。結果の出力形式を棒グラフ、線グラフ、円グラフなどから選択します。

データ記録のオプション

ログ設定の詳細は、IWSS Web コンソールの [ログ] [ログ設定] で確認できます (詳細については、237 ページの「ログの設定」を参照)。

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。

- ログ検索 IWSS には個々のファセットの検索ボックスが用意されています。これには、検索用語を強調表示して、可能性のある結果を表示する「オートコンプリート」機能も含まれます。
- タイムゾーン すべてのログは、クライアントに元々設定されている同じタイムゾーンで表示されます。

- ・ 円グラフ 円グラフに「その他」のカテゴリが含まれるようになりました。たとえば、上位 5 件の不正プログラムインスタンスを表示する場合、各不正プログラムにはグラフのくさび状の部分が 1 つずつ割り当てられ、上位 5 件以外のすべての不正プログラムはまとめて「その他」のくさびに表示されます。不正プログラムインスタンスが 5 件のみの場合、「その他」のくさびは表示されません。
- ・ お気に入りとして保存 よく使用するログ設定を [お気に入りのログ分析] に保存できます。「お気に入り」のログは、[ログ] [お気に入り] にあります。

注意： 折れ線グラフと円グラフにはいずれも「ドリルダウン」機能があり、グラフ内で詳細を知りたいと思う箇所をクリックすると、その詳細情報が表示されます。

ログの設定

[ログ設定] 画面から、次の内容を設定できます。

- ・ ログの保存期間や保存する最大ログサイズなどのグローバルログ設定。
- ・ ポリシー施行、インターネットアクセス、インターネットセキュリティ、データセキュリティ、およびアクセス管理フィルタを使用するユーザ名とドメインの両方を基準としたグローバルログフィルタ、および帯域幅フィルタを使用するユーザ名を基準としたグローバルログフィルタ。
- ・ 匿名ログを有効または無効にできるかどうか。
- ・ ログのタイプと優先度に基づいて追加のログストレージに使用する Syslog サーバ。
- ・ ローカルまたは外部の場所のマウント、以前のログ（少なくとも過去 45 日間のログ）のマウントされた場所へのアンロード、およびその場所からのログのインポート。

グローバルログを設定するには

1. [ログ] [ログ設定] に移動します。
[ログ設定] 画面が表示されます。
2. [グローバルログ設定] で以下を設定します。
 - a. 次のログを保存：削除するまでログを保持する日数を入力します。

注意： この値を 62 日より大きく設定すると、蓄積されたデータが大きくなりすぎてパフォーマンスに影響を及ぼす可能性があります。

- b. **最大ログディスクサイズ**: 保存するログデータの最大ファイルサイズを設定します。ログデータが指定されたサイズを超えると、最も古いログが最初に削除されます。
- c. **ログのアンロード**: マウントされた場所にログを保存する場合は、このオプションをオンにします。

注意: ログをアンロードして後から取得するには、Linux バックエンドで `/var/offload` というディレクトリを作成し、このディレクトリにストレージデバイスをマウントします。マウント場所に対する読み取りおよび書き込み権限が IWSS (iscan) にあることを確認してください。

別の種類の外部デバイスをマウントするためのコマンドなど、追加の設定オプションや情報の詳細については、Web コンソールからオンラインヘルプを参照してください。

- d. **ログのインポート**: マウントされた場所に保存されている履歴ログを分析のためにインポートして使用する場合は、このオプションをオンにします。
 - e. [保存] をクリックします。
3. [グローバルログフィルタ] で以下を設定します。
- a. ドロップダウンリストからポリシーとユーザを選択して、表示されるテキストフィールドにフィルタ名を入力します。
 - b. + アイコンをクリックします。
 - c. [保存] をクリックします。
4. すべてのログを Syslog サーバに転送する場合は、[Syslog サーバ] で次の手順を実行します。
- a. [追加] をクリックします。
[Syslog 設定] の [サーバの追加] 画面が表示されます。
 - b. [Syslog を有効にする] を選択します。
 - c. Syslog の転送先のサーバの IP アドレスとポート番号を入力します。
 - d. 保存するログのタイプまたは Syslog 優先度レベルを選択します。
 - e. [保存] をクリックして設定を保存し、[ログ設定] 画面に戻ります。
 - f. Syslog サーバを選択します。
5. [保存] をクリックします。

グローバルログフィルタ

ログから特定のデータを省略したい場合、グローバルログフィルタを使用します。たとえば、John Smith というユーザのインターネットアクセスログや、www.google.com にアクセスしたユーザの帯域幅使用率をログに記録する必要がない場合は、このフィルタを使用します。

匿名ログ

欧州の一部の国では、ユーザ名をログに記録することを禁じる法律があります。この機能を有効にすると、ログ内のユーザ名は、実際のユーザ名の代わりに MD5 値で記録されます。

ログのアンロードと取得

IWSS にはログストレージ制限があります。古いログを削除したくない場合は、それらのログをデバイスにアンロードして永続的に保存できます。将来ログを分析する場合は、これらのログをデバイスから取得して IWSS で復元できます。

ログおよびレポートデータの CSV ファイルへのエクスポート

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。表のアイコンをクリックし、[CSV ファイルのエクスポート] をクリックして、IWSS サーバからファイルをダウンロードします。

PDF 形式でのレポートデータの出力

CSV 出力機能に加えて、IWSS ではレポートデータ（最大 1000 行までのログ）を PDF 形式で出力することもできます。PDF 形式のデータは PDF リーダーアプリケーションを使用してあらゆるプラットフォームで表示できます。IWSS サーバからファイルをダウンロードするには、[PDF] をクリックして、画面上のプロンプトに従ってください。

syslog 設定

IWSS は syslog サーバをサポートしているため、外部の syslog サーバにログを送信できます。syslog サーバは最大 4 つまで設定でき、ログの種類や優先度を指定して、各 syslog サーバに送信できます。

syslog サーバを設定するには

1. 管理コンソールから [ログ] [ログ設定] [Syslog サーバ] の順に選択します。
2. [追加] をクリックします。
3. [Syslog サーバの設定] で次の設定を行います。
 - a. [Syslog を有効にする] を選択して、IWSS でこの syslog サーバにログを送信できるようにします。
 - b. [サーバ名 /IP アドレス] を指定します。IWSS は、IPv4 と IPv6 の両方のホストへの Syslog メッセージの送信をサポートしています。Web コンソールは、IPv4 と同様に、IPv6 のホスト名とアドレスの両方を受け入れることができます。
 - c. [UDP ポート番号] を指定します (初期設定は 514)。
4. [次のログを保存する] で、送信するログを指定します。ログの種類別または syslog 優先度別に、syslog サーバにイベントを送信するように選択できます。
 - ・ [ログタイプ別] をクリックしてログの種類を選択します。または、
 - ・ [Syslog 優先度別] をクリックしてレベルを選択します。
5. [保存] をクリックします。

通知について

通知は、検索、ブロック、アラート、およびプログラムアップデートイベントに対して発行できます。通知には、管理者への通知とユーザへの通知の 2 種類があります。通知は、次に示すように、メインメニューの [通知] で設定できます。

- ・ 管理者への通知により、多様な情報が提供されます。それらの情報には、HTTP/HTTPS 検索、HTTP/HTTPS のファイルタイプによるブロック、FTP のファイルタイプによるブロック、FTP 検索、しきい値アラート、C&C コールバック試行検出、情報漏えい対策、スマートスキャンイベント、パターンファイルや検索エンジンのアップデートなどがあります。IWSS は、管理者への通知を [通知先の設定 ...] 画面で設定したアドレスにメールで送信します。

- ・ ユーザへの通知では、HTTPS アクセスエラー、HTTPS 証明書に関する警告、HTTP/HTTPS 検索、HTTP/HTTPS ファイルブロック、FTP 検索、URL ブロック、FTP ファイルタイプによるブロック、C&C コールバック試行検出、情報漏えい対策、およびアプリケーション制御による HTTP/HTTPS アクセス拒否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。

注意： IPv4 と同様に、以下を含むすべての変数を IPv6 アクセスに適用できます。

%N ユーザ名

%c: 「Error!Hyperlink reference not valid」の後ろの IP アドレス : ポート (HTTPS 復号化用)。IPv6 の場合は、https:// [IPv6 アドレス] : ポートになります。IPv4 は、https://IPv4 アドレス : ポートを維持します。

通知先の設定

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 [通知] [通知先の設定 ...] 画面でも変更できます。

管理者への通知用のメール設定を行うには

1. 管理コンソールで [通知] をクリックします。
2. [通知] 画面で、[通知先の設定 ...] をクリックします。
3. 通知の送信先メールアドレス、送信者のメールアドレス、DLP 通知の送信先アドレス、SMTP サーバ、SMTP サーバポート、およびメールキューを確認する間隔を入力します。IWSS は、IPv4 ホストと IPv6 ホストへの通知の送信をサポートしています。Web コンソールは、IPv4 と同様に、ホスト名と IPv6 アドレスの両方を受け入れることができます。
4. メールサーバで ESMTP が必要な場合は、IWSS で EHLO コマンドを使用して SMTP セッションを初期化できるように、[EHLO (Extended Hello) コマンドを使用する] チェックボックスをオンにします。
5. [保存] をクリックします。

通知の変数

より意味のある通知にするために、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せんが、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ていました。

この通知は、たとえば次のようになります。

08/05/28 6:31:56 PM に、IWSS がファイル EXT_JS.JS. 10.2.203.130 でセキュリティリスク JS_TEST_VIRUS を検出しました。10.2.203.130 が http://10.2.203.130/TESTDATA/virus/NonCleanable/EXT_JS.JS からファイルをダウンロードしようとしていました。

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 11-2. 変数の説明

変数	変数の意味	変数の使用方法
HTTPS アクセス拒否および HTTPS 証明書エラー		
%o	IWSS ホスト名	イベントが発生した IWSS ホスト名
%u	URL/URI	
%c	「https://」の後の IP アドレス:ポート	%c の使用例については、初期設定のメッセージを参照してください
\$\$DETAILS	証明書エラーの理由 / アクセス拒否の理由の詳細	
FTP 検索および HTTP/HTTPS 検索		
%A	実行された処理	IWSS によって実行された処理

表 11-2. 変数の説明 (続き)

変数	変数の意味	変数の使用方法
%F	ファイル名	anti_virus_test_file.htm など、リスクが検出されたファイルの名前
%H	IWSS ホスト名	イベントが発生した IWSS ホスト名
%L	ファイル名および理由の詳細	
%M	移動先	ファイルが移動された隔離ディレクトリの場所
%N	ユーザ名	
%R	転送方向	
%U	URL/URI	
%V	不正プログラム名 (ウイルス、トロイの木馬、またはボット名)	検出されたリスクの名前
%X	理由 / ブロックタイプ	
%Y	日付と時刻	イベントが発生した日時
アプリケーション制御による HTTP/HTTPS アクセス拒否		
%N	ユーザ名	
%A	処理	
%P	パスおよびファイル名	
%C	カテゴリ	
%Z	ポリシー名	
%Y	日付と時刻	
%H	IWSS ホスト名	
データ漏えい保護		
%T	テンプレート名	
%U	URL/URI	
%Y	日付と時刻	イベントが発生した日時
%A	実行された処理	
%N	ユーザ名	

表 11-2. 変数の説明 (続き)

変数	変数の意味	変数の使用方法
%Z	ポリシー名	
%H	IWSS ホスト名	
C&C コールバック試行検出		
%Z	ポリシー名	
%N	ユーザ名	
%U	URL/URI	
%A	処理	
%K	リスクレベル	
FTP ファイルタイプブロックおよび HTTP/HTTPS ファイルタイプブロック		
%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、トロイの木馬、またはボット名	
時間割り当てによる URL フィルタ		
%U	URL/URI	
%C	カテゴリ	
%H	IWSS ホスト名	
%N	ユーザ名	
%Q	時間数	
%Y	日付と時刻	

表 11-2. 変数の説明 (続き)

変数	変数の意味	変数の使用方法
アクセス管理による URL ブロック		
%H	IWSS ホスト名 (ヘッダフィールドでのみ機能)	
%N	ユーザ名	
%U	URL/URI (本文でのみ機能)	
%Y	日付と時刻	
%X	理由 (本文でのみ機能)	
HTTP 検査による URL ブロック		
%H	IWSS ホスト名	
%I	フィルタ名	
%N	ユーザ名	
%U	URL/URI	
%Y	日付と時刻	
URL フィルタによる URL ブロック		
%C	カテゴリ	
%H	IWSS ホスト名 (ヘッダフィールドでのみ機能)	
%N	ユーザ名	
%U	URL/URI	
%Y	日付と時刻	
URL アクセスの警告		
%A	処理	
%B	警告と続行	
%C	カテゴリ	
%H	IWSS ホスト名 (ヘッダフィールドでのみ機能)	
%N	ユーザ名	
%U	URL/URI (本文でのみ機能)	

表 11-2. 変数の説明 (続き)

変数	変数の意味	変数の使用方法
%Y	日付と時刻	
<p>URL アクセスの警告通知をカスタマイズするには、メッセージテンプレートに次のフォームを含め、[続行する] オプションを表示する必要があります。</p> <pre><form id="warncontinue" method="post" action="%B\$\$\$IWSS_URL_ACTION\$\$\$"> <INPUT type="hidden" value="%A" name="data"> </form></pre> <p>カスタマイズした通知では、ユーザが続行できるようにフォームを送信するためのボタンまたはハイパーリンクを定義する必要があります。例：</p> <pre><input name="button2" type="button" value="Continue at your own risk" style="width:195px" onclick="document.getElementById('warncontinue').submit(); return false;"></input></pre>		
URL アクセスのオーバーライド		
%A	処理	
%B	URL/URI を続行	
%C	カテゴリ	
%E	ポリシーの初期設定の時間制限	
%H	IWSS ホスト名	
%J	ポリシーの最大時間制限	
%N	ユーザ名	
%U	URL/URI (本文でのみ機能)	
%Y	日付と時刻	
%Z	ポリシー名	

表 11-2. 変数の説明 (続き)

変数	変数の意味	変数の使用方法
	URL アクセスのオーバーライドの通知をカスタマイズする場合は、メッセージテンプレートにパスワードを base64 コードで暗号化する Java スクリプトコードを組み込む必要があります。パスワード、時間制限、および ttl_type などの要素を組み込みます。このようにしないと、カスタマイズした通知ページが機能しません。	<pre><form id="overridecontinue" method="post" action="%B[Warn and Continue URL/URI]/\$\$S\$IWSX_URL_ACTION\$\$\$"> <INPUT type=hidden value="%A[Action]" name=data></pre>
	カスタマイズした通知では、ユーザが続行できるようにフォームを送信するためのボタンまたはハイパーリンクを定義する必要があります。例：	<pre><input type="button" name="Button22" value="Submit" class="style3" onclick="doSubmit();" /></pre>
	しきい値アラート	
%m	基準	
%t	しきい値	

通知の設定

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

ユーザへの通知での HTML タグの使用

ユーザへの通知メッセージは、HTML を使用して書式を設定できます。HTML ファイルには外部の画像またはスタイルへの参照リンクを含めることができますが、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。

C&C コンタクトコールバック通知の設定

IWSS は、セキュリティポリシーに違反する C&C コンタクトオブジェクトのダウンロードを検出すると、管理者への通知をメールで送信し、ユーザへの通知メッセージを要求元クライアントのブラウザに表示します。

C&C コンタクトコールバック通知を設定するには

1. 管理コンソールで [通知] をクリックし、[C&C コールバック試行通知] をクリックします。
2. [管理者への通知] で、[C&C コールバック試行が検出された場合に通知を送信する] をオンにします。
3. 各インシデントごとに、または特定のリスクレベル（低、中、または高）を超えた場合にルート受信者にメッセージを送信するように選択します。
4. 初期設定の通知メッセージを使用しない場合は、初期設定のテキストを選択して、任意のテキストを入力します。該当する場合は、242 ページの「通知の変数」で説明されているように、テキストに変数を挿入します。
5. [ユーザへの通知] は、次のように設定します。
 - a. 初期設定の警告メッセージを表示するには、[初期設定] チェックボックスをオンにします。
 - b. 独自のメッセージを表示するには [カスタマイズ] チェックボックスをオンにし、カスタマイズしたメッセージの内容を入力するか、[インポート] を使用してインポートします。
 - ・ 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSS に [インポート] できません。
 - ・ IWSS 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。
6. [保存] をクリックします。

情報漏えい対策通知の設定

IWSS は、セキュリティポリシーに違反するデータ漏えいを検出すると、管理者への通知をメールで送信し、ユーザへの通知メッセージを要求元クライアントのブラウザに表示します。

情報漏えい対策通知を設定するには

1. 管理コンソールで [通知] をクリックし、[情報漏えい対策] をクリックします。
2. [管理者への通知] で、[データ漏えいが検出された場合に通知を送信する] をオンにします。

3. 初期設定の通知メッセージを使用しない場合は、初期設定のテキストを選択して、任意のテキストを入力します。該当する場合は、242 ページの「通知の変数」で説明されているように、テキストに変数を挿入します。
4. [ユーザへの通知] は、次のように設定します。
 - a. 初期設定の警告メッセージを表示するには、[初期設定] チェックボックスをオンにします。
 - b. 独自のメッセージを表示するには [カスタマイズ] チェックボックスをオンにし、カスタマイズしたメッセージの内容を入力するか、[インポート] を使用してインポートします。
 - ・ 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSS に [インポート] できません。
 - ・ IWSS 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。
5. [保存] をクリックします。

FTP 情報漏えい対策通知の設定

IWSS は、セキュリティポリシーに違反する FTP データ漏えいを検出すると、管理者への通知をメールで送信し、ユーザへの通知メッセージを要求元クライアントのブラウザに表示します。

FTP 情報漏えい対策通知を設定するには

1. 管理コンソールで [通知] をクリックし、[FTP 情報漏えい対策] をクリックします。
2. [管理者への通知] で、[データ漏えいが検出された場合に通知を送信する] をオンにします。
3. 初期設定の通知メッセージを使用しない場合は、初期設定のテキストを選択して、任意のテキストを入力します。該当する場合は、242 ページの「通知の変数」で説明されているように、テキストに変数を挿入します。
4. [ユーザへの通知] は、次のように設定します。
 - a. 初期設定の警告メッセージを表示するには、[初期設定] チェックボックスをオンにします。
 - b. 独自のメッセージを表示するには [カスタマイズ] チェックボックスをオンにし、カスタマイズしたメッセージの内容を入力するか、[インポート] を使用してインポートします。
 - ・ 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSS に [インポート] できません。

- ・ IWSS 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。
5. [保存] をクリックします。

FTP ファイルタイプによるブロック通知の設定

IWSS では、FTP でのアップロードおよびダウンロードの検索に加えて、FTP のゲートウェイでファイルタイプによるブロックも実行できます。パフォーマンスの問題を避けるため、FTP の検索モジュールには圧縮ファイルおよびサイズの大きいファイルについての特別な設定が用意されています。スパイウェア検索もサポートされています。

IWSS の FTP 検索は、他の FTP プロキシサーバと連携する環境または IWSS が自身の FTP プロキシとして動作する環境に配置できます。IWSS サーバのセキュリティを確保するために、IWSS サーバとそのポートへのアクセスを制御する複数のセキュリティ関連の設定が用意されています。

FTP ファイルタイプによるブロック通知を設定するには

1. 管理コンソールから [通知] を選択し、[FTP ファイルタイプブロック] をクリックします。
2. [管理者への通知] で、[FTP でブロックするファイルタイプがアクセスされた場合に通知を送信する] チェックボックスをオンにします。

IWSS のブロック対象の設定によっては、このオプションによって初期設定の受信者に大量の通知メッセージが送信される場合があります。個別の通知の代わりに、ブロックされたファイルはログに記録されるので、それを IWSS が生成するレポートの 1 つに含めることも可能です。
3. 初期設定の通知メッセージを使用しない場合は、初期設定のテキストを選択して、任意のテキストを入力します。該当する場合は、242 ページの「通知の変数」で説明されているように、テキストに変数を挿入します。
4. [ユーザへの通知] は、次のように設定します。
 - a. 初期設定の警告メッセージを表示するには、[初期設定] チェックボックスをオンにします。
 - b. 独自のメッセージを表示するには [カスタマイズ] チェックボックスをオンにして、カスタマイズした内容を入力します。
 - ・ 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSS に [インポート] できます。
 - ・ IWSS 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。
5. [保存] をクリックします。

FTP 検索通知の設定

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. 管理コンソールから [通知] を選択し、[FTP 検索] をクリックします。
2. [管理者への通知] で、通知の対象とする検出イベントのチェックボックスをオンにします ([ウイルス]、[トロイの木馬]、[その他の不正プログラム] のいずれかまたはすべて)。
3. 初期設定の通知メッセージを使用しない場合は、初期設定のテキストを選択して、任意のテキストを入力します。該当する場合は、242 ページの「通知の変数」で説明されているように、テキストに変数を挿入します。
4. [ユーザへの通知] は、次のように設定します。
 - a. 初期設定の警告メッセージを表示するには、[初期設定] チェックボックスをオンにします。
 - b. 独自のメッセージを表示するには [カスタマイズ] チェックボックスをオンにして、カスタマイズした内容を入力します。
 - ・ 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSS に [インポート] できます。
 - ・ IWSS 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。
5. [保存] をクリックします。

HTTP/HTTPS ファイルタイプによるブロック通知の設定

IWSS は、ファイルをブロックすると、管理者への通知をメールで送信します。ユーザへの通知メッセージは要求元クライアントのブラウザに表示されます。

HTTP/HTTPS ファイルタイプによるブロック通知を設定するには

1. 管理コンソールから [通知] をクリックし、[HTTP/HTTPS ファイルタイプブロック] をクリックします。
2. [管理者への通知] で、[HTTP でファイルタイプによりブロック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、242 ページの「通知の変数」で説明されているように、テキストに変数を挿入します。
4. ブラウザに表示する [タイトル] を入力します。
初期設定のタイトルは、「Trend Micro InterScan Web Security イベント」です。タイトルは、ウイルス感染メッセージ、ファイルタイプブロック、および URL ブロックメッセージで共通です。
5. [ユーザへの通知] は、次のように設定します。
 - a. 初期設定の警告メッセージを表示するには、[初期設定] チェックボックスをオンにします。
 - b. 独自のメッセージを表示するには [カスタマイズ] チェックボックスをオンにし、メッセージの内容を入力するか、HTML ファイルからインポートします。
 - ・ 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSS に [インポート] できません。
 - ・ IWSS 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。
6. [プレビュー] をクリックして、通知が正しく表示されることを確認します。
7. [保存] をクリックします。

HTTP/HTTPS 検索通知の設定

クライアントが要求したファイル中に不正コードを検出すると、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 は一種のセキュリティの脅威と見なされるため、HTTP/HTTPS 検索と同じ通知が使用されません。

HTTP/HTTPS 検索通知を設定するには

1. 管理コンソールから [通知] [HTTP/HTTPS 検索] の順に選択します。
2. [管理者への通知] で、通知の対象とする検出イベントのチェックボックスをオンにします ([ウイルス]、[トロイの木馬]、[その他のインターネット上の脅威]、[ボット]、[高度な脅威] 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、242 ページの「通知の変数」で説明されているように、メッセージに変数を挿入します。
4. ブラウザに表示する [タイトル] を入力します。
初期設定のタイトルは、「Trend Micro InterScan Web Security イベント」です。タイトルは、ウイルス感染メッセージ、ファイルタイプブロック、および URL ブロックメッセージで共通です。
5. [ダウンロードファイルに対するメッセージ] および [アップロードファイルに対するメッセージ] のユーザ通知メッセージは、次のように設定します。
 - a. 初期設定の警告メッセージを表示するには、[初期設定] チェックボックスをオンにします。
 - b. 独自のメッセージを表示するには [カスタマイズ] チェックボックスをオンにし、カスタマイズしたメッセージの内容を入力するか、HTML ファイルからインポートします。
 - ・ 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSS に [インポート] できません。
 - ・ IWSS 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。
 - c. [プレビュー] をクリックして、通知が正しく表示されることを確認します。
6. [保存] をクリックします。

HTTPS アクセス拒否通知の設定

HTTPS 接続を介した Web サイトへのアクセスが拒否されたユーザには、要求が拒否されたことを示す HTML ページが表示されます。

HTTPS アクセス拒否通知を設定するには

1. 管理コンソールから [通知] [HTTPS アクセス拒否] の順に選択します。
2. ブラウザに表示する [タイトル] を入力します。

初期設定のタイトルは、「Trend Micro InterScan Web Security イベント」です。タイトルは、ウイルス感染メッセージ、ファイルタイプブロック、および URL ブロックメッセージで共通です。

3. [ユーザへの通知] は、次のように設定します。
 - a. 初期設定の警告メッセージを表示するには、[初期設定] チェックボックスをオンにします。
 - b. 独自のメッセージを表示するには [カスタマイズ] チェックボックスをオンにし、メッセージの内容を入力するか、HTML ファイルからインポートします。
 - ・ 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSS に [インポート] できます。
 - ・ IWSS 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。
4. [プレビュー] をクリックして、通知が正しく表示されることを確認します。
5. [保存] をクリックします。

HTTPS 証明書エラー通知の設定

証明書が検証テストに合格していない Web サイトへのアクセスが拒否されたユーザには、警告メッセージを示す HTML 画面が表示されます。ユーザは、HTTPS トラフィックを復号化およびチェックせずに、Web サイトへのアクセスを継続することもできます。

HTTPS 証明書エラー通知を設定するには

1. 管理コンソールから [通知] [HTTPS 証明書エラー] の順に選択します。
2. ブラウザに表示する [タイトル] を入力します。

初期設定のタイトルは、「Trend Micro InterScan Web Security イベント」です。タイトルは、ウイルス感染メッセージ、ファイルタイプブロック、および URL ブロックメッセージで共通です。
3. [ユーザへの通知] は、次のように設定します。
 - a. 初期設定の警告メッセージを表示するには、[初期設定] チェックボックスをオンにします。
 - b. 独自のメッセージを表示するには [カスタマイズ] チェックボックスをオンにし、メッセージの内容を入力するか、HTML ファイルからインポートします。

- ・ 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSS に [インポート] できません。
 - ・ IWSS 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。
4. [プレビュー] をクリックして、通知が正しく表示されることを確認します。
 5. [保存] をクリックします。

アプリケーション制御通知による HTTP/HTTPS アクセス拒否の設定

検証テストに合格しない証明書を持つ HTTP/HTTPS Web サイトへのアクセスをユーザが拒否されるたびに、警告メッセージが示された HTML 画面が表示されます。ユーザは、HTTP/HTTPS トラフィックを復号化およびチェックせずに、HTTP/HTTPS Web サイトへのアクセスを継続することもできます。

HTTPS 証明書エラー通知を設定するには

1. [通知] [アプリケーション制御による HTTP/HTTPS アクセス拒否] の順に選択します。
2. ブラウザに表示する [タイトル] を入力します。
初期設定のタイトルは、「Trend Micro InterScan Web Security イベント」です。タイトルは、ウイルス感染メッセージ、ファイルタイプブロック、および URL ブロックメッセージで共通です。
3. [ユーザへの通知] は、次のように設定します。
 - a. 初期設定の警告メッセージを表示するには、[初期設定] チェックボックスをオンにします。
 - b. 独自のメッセージを表示するには [カスタマイズ] チェックボックスをオンにし、メッセージの内容を入力するか、HTML ファイルからインポートします。
 - ・ 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSS に [インポート] できません。
 - ・ IWSS 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。
4. [プレビュー] をクリックして、通知が正しく表示されることを確認します。
5. [保存] をクリックします。

パターンファイルのアップデート通知の有効化

IWSS では、パターンファイルの予約アップデートに基づいた検索エンジンまたはパターンファイルのアップデート試行の際に通知を送信できます。

注意： IWSS では、手動によるパターンファイルアップデートの通知は送信されません。

パターンファイルのアップデート通知を有効にするには

1. 管理コンソールから [通知] を選択し、[パターンファイルのアップデート] をクリックします。
2. パターンファイルのアップデート試行は、次のように設定します。
 - a. 通知の対象とするアップデートイベントを選択します。[成功]、[失敗]、または [アップデート不要] のアップデート試行に対して通知を設定できます。
 - b. 通知メッセージの [件名] を入力します。初期設定は、「IWSS パターンファイルのアップデート結果」です。
3. [保存] をクリックします。

しきい値アラートの設定

IWSS では、設定したしきい値を超えた場合に通知を送信できます。

しきい値アラートの通知を有効にするには

1. 管理コンソールから [通知] を選択し、[しきい値アラート] をクリックします。
2. しきい値アラートについて、次の設定を行います。
 - a. 通知メッセージのしきい値アラートの種類、値、および頻度の制限を有効にします。
 - b. 通知先を変更するには、管理コンソールの [通知] をクリックして、画面右上の [通知先の設定 ...] をクリックします。
 - c. 初期設定のメッセージを使用するか、[通知メッセージ] で独自のメッセージを作成します。
3. [保存] をクリックします。

URL アクセスの警告通知の設定

URL フィルタルール処理が「警告」に設定されている場合に、会社ポリシーによって禁止されているカテゴリに属する URL にアクセスしようとする、URL アクセスの警告モードにより通知が送信されます（詳細については、200 ページの「新しいポリシーの作成」を参照してください）。該当の Web ページの表示前に、ユーザに警告が送信されます。

必要に応じて警告メッセージの次のリンクのいずれかを選択できます。

- ・ 安全に前の Web ページに戻る
- ・ 自己責任で続行する（非推奨）

URL アクセスの警告通知を設定するには

1. 管理コンソールから [通知] を選択し、[URL アクセスの警告] をクリックします。
2. ブラウザに表示する [タイトル] を入力します。

初期設定のタイトルは、「Trend Micro InterScan Web Security イベント」です。タイトルは、ウイルス感染メッセージ、ファイルタイプブロック、および URL ブロックメッセージで共通です。

3. [ユーザへの通知] は、次のように設定します。
 - a. 初期設定の警告メッセージを表示するには、[初期設定] チェックボックスをオンにします。
 - b. 独自のメッセージを表示するには [カスタマイズ] チェックボックスをオンにし、メッセージの内容を入力するか、HTML ファイルからインポートします。
 - ・ 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSS に [インポート] できません。
 - ・ IWSS 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。
 - ・ 通知には、エンドユーザが続行を選択する場合に必要な情報を IWSS に送信するためのフォームを含める必要があります。このフォーマットは、次のとおりです。

```
<form id="warncontinue" method="post" action="%B$$$IWSS_URL_ACTION$$$">
<INPUT type=hidden value="%A" name=data>
</form>
```

- ・ カスタマイズした通知では、ユーザが続行を求めてフォームを送信するためのボタンまたはハイパーリンクを定義する必要があります。例：

```
<a href="javascript:void(0)"
onclick="document.getElementById('warncontinue').submit();"
return false;">Continue to this website (not recommended)</a>
```

4. [プレビュー] をクリックして、通知が正しく表示されることを確認します。
5. [保存] をクリックします。

URL アクセスのオーバーライドの通知の設定

会社ポリシーによって「オーバーライドによるブロック」処理が設定されたカテゴリ内の URL にアクセスしようとする、ユーザに URL アクセスのオーバーライドモード通知が送信されます。オーバーライドの警告が表示され、続行するにはパスワードの入力が必要です。この通知では、閲覧が許容される残り時間量が表示されます。正しいパスワードを入力した後に、要求する Web ページを続行できます。

必要に応じて警告メッセージの次のリンクのいずれかを選択できます。

- ・ パスワードが不明の場合、ページの参照を中止
- ・ パスワードを入力して、指定された期間内で閲覧を続行

管理者は、あらかじめポリシーでカテゴリ処理を「オーバーライドによるブロック」の処理に設定しておく必要があります。詳細については、200 ページの「新しいポリシーの作成」を参照してください。

URL アクセスのオーバーライドのユーザ通知メッセージを設定するには

1. 管理コンソールから [通知] を選択し、[URL アクセスのオーバーライド] をクリックします。
2. [ユーザへの通知 URL アクセスのオーバーライド用] で、次の操作を実行します。
 - a. ブラウザに表示する [タイトル] を入力します。

初期設定のタイトルは、「Trend Micro InterScan Web Security イベント」です。タイトルは、ウイルス感染メッセージ、ファイルタイプブロック、および URL ブロックメッセージで共通です。
 - b. 初期設定の警告メッセージを表示するには [初期設定] チェックボックスをオンにします。
 - c. 独自の警告メッセージを表示するには [カスタマイズ] チェックボックスをオンにします。メッセージをテキストボックスに入力するか、ローカルコンピュータの HTML ファイルからメッセージをインポートします。
 - ・ 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSS に [インポート] できます。

- ・ IWSS 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。
- d. URL アクセスのオーバーライドの通知をカスタマイズする場合は、メッセージテンプレートにパスワードを base64 コードで暗号化する Java スクリプトコードを組み込む必要があります。パスワード、時間制限、および ttl_type などの要素を組み込みます。このようにしないと、カスタマイズした通知ページが機能しません。

例：

```
<form id="overridecontinue" method="post" action="%B[Warn and Continue
URL/URI]$$$$IWSX_URL_ACTION$$$$">
<INPUT type=hidden value="%A[Action]" name=data>
..
</form>
```

- e. カスタマイズした通知では、ユーザが続行を求めてフォームを送信するためのボタンまたはハイパーリンクを定義する必要があります。

例：

```
<input type="button" name="Button22"
value="Submit" class="style3"
onclick="doSubmit();" />
```

3. [プレビュー] をクリックして、通知が正しく表示されることを確認します。
4. [保存] をクリックします。

アクセス管理通知による URL ブロックの設定

IWSS で、ローカル IWSS リストからフィッシング対策シグネチャデータベースにある 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を表示します。

アクセス管理による URL ブロックのユーザ通知メッセージを設定するには

1. 管理コンソールから [通知] を選択し、[アクセス管理による URL ブロック] をクリックします。
2. [制限された URL やブロックされた URL のユーザ通知メッセージ] で、次の操作を実行します。
 - a. ブラウザに表示する [タイトル] を入力します。

初期設定のタイトルは、「Trend Micro InterScan Web Security イベント」です。タイトルは、ウイルス感染メッセージ、ファイルタイプブロック、および URL ブロックメッセージで共通です。

- b. 初期設定の警告メッセージを表示するには [初期設定] チェックボックスをオンにします。
 - c. 独自の警告メッセージを表示するには [カスタマイズ] チェックボックスをオンにします。メッセージをテキストボックスに入力するか、ローカルコンピュータの HTML ファイルからメッセージをインポートします。
 - ・ 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSS に [インポート] できません。
 - ・ IWSS 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。
3. [プレビュー] をクリックして、通知が正しく表示されることを確認します。
 4. [保存] をクリックします。

HTTP 検査通知による URL ブロックの設定

IWSS で、ブロック処理により、HTTP 検査ポリシーに違反している URL へのアクセスが検出されると、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を表示します。

HTTP 検査のユーザ通知メッセージを設定するには

1. 管理コンソールから [通知] を選択し、[HTTP 検査による URL ブロック] をクリックします。
2. [制限された URL やブロックされた URL のユーザ通知メッセージ] で、次の操作を実行します。
 - a. ブラウザに表示する [タイトル] を入力します。

初期設定のタイトルは、「Trend Micro InterScan Web Security イベント」です。タイトルは、ウイルス感染メッセージ、ファイルタイプブロック、および URL ブロックメッセージで共通です。
 - b. 初期設定の警告メッセージを表示するには [初期設定] チェックボックスをオンにします。
 - c. 独自の警告メッセージを表示するには [カスタマイズ] チェックボックスをオンにします。メッセージをテキストボックスに入力するか、ローカルコンピュータの HTML ファイルからメッセージをインポートします。
 - ・ 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSS に [インポート] できません。
 - ・ IWSS 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。
3. [プレビュー] をクリックして、通知が正しく表示されることを確認します。

URL フィルタ通知による URL ブロックの設定

IWSS で、ローカル IWSS リストからフィッシング対策シグネチャデータベースにある 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を表示します。

URL フィルタによる URL ブロックのユーザ通知メッセージを設定するには

1. 管理コンソールから [通知] を選択し、[URL フィルタによる URL ブロック] をクリックします。
2. [制限された URL やブロックされた URL のユーザ通知メッセージ] で、次の操作を実行します。
 - a. ブラウザに表示する [タイトル] を入力します。

初期設定のタイトルは、「Trend Micro InterScan Web Security イベント」です。タイトルは、ウイルス感染、ファイルタイプによるブロック、および URL ブロックのメッセージで共通です。
 - b. 初期設定の警告メッセージを表示するには [初期設定] チェックボックスをオンにします。
 - c. 独自の警告メッセージを表示するには [カスタマイズ] チェックボックスをオンにします。メッセージをテキストボックスに入力するか、ローカルコンピュータの HTML ファイルからメッセージをインポートします。
 - ・ 会社の商標やその他のリソースへのリンクを表示する場合など、HTML エディタを使用して独自の通知ページをデザインし、そのページを IWSS に [インポート] できます。
 - ・ IWSS 初期設定にカスタムメッセージを追加するには、[初期設定] と [カスタマイズ] オプションの両方を選択します。
3. [プレビュー] をクリックして、通知が正しく表示されることを確認します。
4. [保存] をクリックします。

URL フィルタエンジンおよび検索エンジンのアップデートの通知の有効化

パターンファイルのアップデートほど頻繁ではありませんが、トレンドマイクロでは、ウイルスおよび不正コードの検出方法の進化を反映するために、定期的に新しいバージョンの検索エンジンをリリースします。IWSS では、検索エンジンの予約アップデートに応じて、管理者への通知を発行できます。

注意： IWSS では、手動によるエンジンのアップデートの通知は送信されません。

URL フィルタおよび検索エンジンのアップデート通知を有効にするには

1. 管理コンソールから [通知] を選択し、[URL フィルタエンジンおよび検索エンジンのアップデート] をクリックします。
2. 検索エンジンまたは URL フィルタエンジンについて、通知の対象とするアップデートイベントを選択します。
[成功]、[失敗]、または [アップデート不要] のアップデート試行に対して通知を設定できます。
3. 検索エンジンまたは URL フィルタエンジンについて、通知メールメッセージの [件名] を入力します。
4. [保存] をクリックします。

時間割り当て通知による URL フィルタの設定

URL フィルタポリシーのルールで時間制限の処理が設定されている場合は、ユーザに時間割り当て通知による URL フィルタを送信できます。[URL フィルタ] [ポリシー] | [ルール] タブで、ポリシーに [時間制限] 処理が設定されている場合は、常にエンドユーザの Web ブラウザに表示されません。詳細については、200 ページの「新しいポリシーの作成」を参照してください。

このオプションが有効化されている場合、IWSS で時間制限処理が設定されているページをダウンロードしようとした場合、および制限時間が経過した場合は、必ず要求が拒否されたことを示す HTML ページが表示されます。詳細については、208 ページの「URL フィルタの割り当てた時間の延長」を参照してください。

時間割り当て通知による URL フィルタを設定するには

1. 管理コンソールから [通知] を選択し、[時間割り当てによる URL フィルタ] をクリックします。
2. 初期設定の通知メッセージを使用しない場合は、[カスタマイズ] チェックボックスをオンにして、任意のテキストを入力します。該当する場合は、242 ページの「通知の変数」で説明されているように、テキストに変数を挿入します。
3. [保存] をクリックします。

スマートスキャンイベント通知の設定

IWSS では、Trend Micro Global Smart Protection Server が利用できない場合に通知メールを送信し、従来型の検索に切り替えることができます。

Smart Protection Server 接続状況通知を有効にするには

1. 管理コンソールから [通知] を選択し、[スマートスキャンイベント] をクリックします。
2. [Smart Protection Server に接続できない場合に通知を送信する] チェックボックスをオンにします。
3. [保存] をクリックします。

注意： IWSS では、Smart Protection Server にアクセスできず、従来型の検索に切り替える場合のみメール通知を送信します。スマートスキャンから従来型スキャンに手動で変更した場合、通知は送信されません。

注意： スマートスキャンイベント通知では変数を使用しません。

SNMP トラップ通知の有効化

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。

注意： SNMP が有効でなければ、[通知] 画面に SNMP 設定は表示されません。SNMP トラップを送信するには、[管理] [SNMP 設定] で SNMP を設定して、この機能を有効にする必要があります。

SNMP 通知の送信を有効にするには

1. 管理コンソールから [通知] を選択し、画面の下部に表示される [SNMP 通知の設定] で [通知の設定 ...] をクリックします。
2. SNMP 通知を実行するイベントの種類を選択します。イベントには次のような種類があります。
 - ・ ウイルスまたはインターネット上の脅威の検出 ウイルスまたは不正コードの検出に関連するイベントです。
 - ・ セキュリティ違反 ウイルス検出以外の、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 リクエストおよびレスポンス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12章

管理

本章では、InterScan Web Security Suite（以下、IWSS）で使用可能な管理機能について説明します。

本章で説明する内容には、次の項目が含まれます。

- ・ 266 ページの「概要」
- ・ 267 ページの「監査ログ」
- ・ 268 ページの「一般設定」
- ・ 281 ページの「検索方法」
- ・ 293 ページの「サポート情報」
- ・ 287 ページの「設定のバックアップと復元」
- ・ 288 ページの「システムアップデート」
- ・ 289 ページの「システムイベントログ」
- ・ 289 ページの「製品ライセンス」
- ・ 293 ページの「サポート情報」

概要

[管理] メニューには、次のオプションが含まれます。

- 267 ページの「監査ログ」
- 268 ページの「一般設定」
 - 268 ページの「ユーザの識別」
 - 276 ページの「ポリシー配信」
 - 277 ページの「データベース接続」
 - 277 ページの「隔離管理」
 - 278 ページの「予約期間」
 - 279 ページの「Control Manager への登録」
 - 279 ページの「複製の設定」
 - 280 ページの「集中管理ログ / レポート」
 - 281 ページの「検索方法」
 - 281 ページの「PAC ファイル管理」
- 282 ページの「管理コンソール」
 - 282 ページの「アカウント管理」
 - 283 ページの「役割ベースの管理」
 - 284 ページの「役割の管理」
- 287 ページの「設定のバックアップと復元」
- 288 ページの「システムアップデート」
- 289 ページの「システムイベントログ」
- 289 ページの「製品ライセンス」
- 292 ページの「SNMP の設定」
- 293 ページの「Web コンソール」
- 293 ページの「サポート情報」

監査ログ

監査ログには、ユーザが変更したアプリケーションの設定を説明する情報が記載されています。たとえば、ユーザが移行またはロールバックの手順を実施した場合、移行活動を記録するエントリが監査ログに作成されます。

注意： IPv4 監査ログの場合と同様に、IPv6 関連の設定変更はすべてログに記録されます。

監査ログを表示するには

1. 管理コンソールから [管理] [監査ログ] の順に選択します。
2. [期間] で、レポートを生成する時間を選択します。
任意の期間のウイルスログを表示するには、[範囲] をクリックし、開始と終了の日付を選択します。
3. [ユーザ] で、ログエントリを表示するユーザを選択します。[追加] をクリックします。リストにあるすべてのユーザを追加する場合は、[すべて追加] をクリックします。ユーザを右側のリストボックスから削除するには、[削除] をクリックします。リストにあるすべてのユーザを削除する場合は、[すべて削除] をクリックします。
4. [並べ替え基準] で、ログの並べ替えの基準とするオプションを選択します。オプションは、[ユーザ] および [日付] です。
5. [ログ表示] をクリックします。[監査ログ] 画面が開きます。
6. 画面を更新するには、[表示更新] をクリックします。

一般設定

[一般設定]には、次の項目が含まれます。

- 268 ページの「ユーザの識別」
- 275 ページの「ポリシー確認画面」
- 276 ページの「認証の許可リスト」
- 276 ページの「ポリシー配信」
- 277 ページの「データベース接続」
- 277 ページの「隔離管理」
- 278 ページの「予約期間」
- 279 ページの「Control Manager への登録」
- 279 ページの「複製の設定」
- 280 ページの「集中管理ログ / レポート」
- 281 ページの「検索方法」
- 281 ページの「PAC ファイル管理」

ユーザの識別

IWSS では、次の複数のユーザ識別方法がサポートされます。

- IP アドレス
- ホスト名
- ユーザ / グループ名

注意： ユーザの識別方法を変更すると、ログやレポートのほか、今まで作成した既存ポリシーに影響を及ぼすことがあります。

IWSS でユーザ / グループベースのポリシーを使用する必要があり、ネットワーク上に LDAP サーバがある場合は、[ユーザ / グループ認証の設定] を選択し、各種の属性設定に関する情報について LDAP 管理者に問い合わせてください。

レポート、ログ、通知メッセージ、および検索ポリシーの作成に任意のユーザの識別方法を選択します。

ユーザ / グループ認証の設定

基本 (単一の Active Directory サーバ)

IWSS では LDAP 機能が強化され、Microsoft の Active Directory のいくつかの設定が自動的に検出できるようになりました。これにより、設定作業が簡素化されます。Microsoft Active Directory は多くのユーザに使用されているので、これは、あまり複雑な設定を必要としないユーザにとって最適なオプションとなります。

基本 (単一の Active Directory サーバ) を使用するには、[ユーザの識別] 画面で [管理] [一般設定] [ユーザの識別] の順に選択して、[基本 (単一の Active Directory サーバ)] チェックボックスをオンにします。

[基本 (単一の Active Directory サーバ)] ビューでは、次の設定のみが必要になります。

- ・ ドメイン名
- ・ サービスアカウント
- ・ パスワード

自動検出機能を正しく機能させるには、LDAP ベンダーで Microsoft Active Directory を使用する必要があります。IWSS によって特定のドメインに対して使用可能なすべてのサーバが自動的に検出され、ユーザの設定に最適なサーバが、他の重要な設定とともに選択されます。

IWSS では、次のように自動検出が実行されます。

- ・ DNS クエリによって LDAP サーバのリストを取得します。
- ・ 接続していないサーバを排除します。
- ・ LDAP サーバの中に複数の GC または DC が配置されている場合は、レスポンス速度が速い GC または DC がプライマリ LDAP サーバとして選択されます。
- ・ ドメイン名が BDN に変換されます。
- ・ Kerberos 情報が生成され、認証されます。

詳細 (他の / 複数の LDAP サーバ)

[詳細 (他の / 複数の LDAP サーバ)] は、管理コンソールから [管理] [一般設定] [ユーザの識別] を選択し、[詳細 (他の / 複数の LDAP サーバ)] にチェックを入れて設定します。

このオプションは、詳細または複雑な LDAP 設定を使用する場合に選択します。[詳細 (その他の / 複数の LDAP サーバ)] ビューでは、Active Directory 以外にも、その他の LDAP サーバと複数ドメインフォレスト、および冗長 LDAP サーバがサポートされます。ユーザ / グループ認証用に複数のドメインを追加できます。IWSS は、これらのドメインに対するクエリを順次実行して、ユーザを識別し、ポリシーを適用します。

Web コンソールで [詳細 (その他の / 複数の LDAP サーバ)] を使用するには、[管理] [一般設定] [ユーザの識別] の順に選択し、[ユーザの識別] で [詳細 (その他の / 複数の LDAP サーバ)] チェックボックスをオンにします。

[詳細 (その他の / 複数の LDAP サーバ)] ビューでドメインの設定を追加、削除、または編集し、設定されているすべてのドメインが記載されるリストを作成できます。ドメイン名をクリックするか、下向き矢印ボタンをクリックすると、そのドメインの詳細が表示されます。

注意： IWSS では、ドメインがサブドメインであるかどうかを確認できません。一方が他方のサブドメインである 2 つのドメインを指定しても、IWSS では両方とも独立したドメインとして処理されます。

新規 LDAP の設定画面で設定するには

1. [詳細 (その他の / 複数の LDAP サーバ)] を有効にして、[新規ドメインの追加] をクリックするか、既存の LDAP ドメイン名をクリックして詳細を表示します。
2. 次の情報を入力または編集します。
 - ・ ドメイン名
 - ・ サーバの種類
 - ・ サービスアカウント
 - ・ パスワード
 - ・ LDAP サーバのホスト名
 - ・ 待機ポート番号
 - ・ LDAP ポート番号
 - ・ LDAP 暗号化
 - ・ 基本識別名 (BDN)

注意： 初期設定の暗号化方式は [なし] です。LDAP サーバで LDAPv3 StartTLS 拡張または LDAPS (LDAP over SSL) がサポートされる場合は、対応する暗号化方式を選択します。

3. [認証方法] で、必要なものを 1 つ選択し、Kerberos ドメインまたはレルム、Kerberos サーバ、および Kerberos ポートを入力します。
4. [認証の高可用性] では、[同じドメインで追加の LDAP サーバを有効にする] を選択することによって、同じドメインに対して追加するサーバの関係を有効にできます。サーバの関係 (ラウ

ンドロピンまたはフェイルオーバ)を設定し、追加するバックアップ LDAP サーバの名前を入力します。

ドメインの設定作業は、かなりの量になります。単純な設定を実行するには、基本ビューの自動検出ボタンを使用します。これで、フォームに自動入力されます。自動検出設定の出力をベースとしてドメインの設定を変更できます。このボタンは、Microsoft Active Directory ユーザが基本ビューでのみ使用できます。

認証方法の設定はある程度 LDAP ベンダーに依存します。一部の認証方法は、特定のベンダーでのみ有効です。次の表は、この関係を示しています。

表 12-1. LDAP ベンダーと認証方法の関係

	Active Directory	OpenLDAP
簡易	使用不可	使用可能
Kerberos	使用可能	使用可能
ダイジェスト - MD5	使用不可	使用可能

IWSS では LDAP 認証の高可用性をサポートしています。プライマリサーバと同じ設定を共有するバックアップの LDAP サーバを 1 つ指定できます。ただし、次の 2 つの高可用性モードがサポートされています。

- ・ ラウンドロビン: IWSS の初期設定では、すべての LDAP サーバで交互にユーザの認証が実行されます。
- ・ フェイルオーバ: プライマリサーバがダウンした場合、IWSS は他のサーバを参照してユーザを認証します。

注意: ドメインのそれぞれで設定可能な BDN と LDAP サーバの種類は 1 つのみです。BDN はドメイン間で一意である必要があります。

複数のドメインがサポートされる場合は、任意のドメインに属するアカウントを使用してログインできます。IWSS はまずドメイン名を確認し、次に一致したドメイン名サーバに対するユーザの認証を実行します。ドメイン名が入力されていない場合は、最初のドメインが初期設定のログインドメイン名として使用されます。

5. 設定の準備が完了したら、[保存] をクリックします。最初からやり直す場合は、[キャンセル] をクリックします。設定が正常に保存されたら、LDAP サーバのリストに戻ります。

次に該当する場合は保存できません。対応するエラーメッセージが表示されます。

- LDAP サーバが存在しない
- BDN がリストされていない
- 管理者アカウントまたはパスワードが入力されていない
- 詳細認証モードの選択時に認証情報が入力されていない
- LDAP 接続テストに失敗した

グローバルな認証キャッシュの設定

固定 TTL Client IP to User ID キャッシュに含まれるレコードの生存期間はそれぞれ異なります。レコードの生存期間が終了すると、そのレコードは削除されます。レコードの生存期間は次のように計算されます。

生存期間 = レコードの生成時間 + 固定 TTL

前回アクティブな TTL Client IP to User ID キャッシュにレコードを追加する際、そのレコードに 360 秒など事前設定された生存期間が設定されます。生存期間が終了する前にレコードがヒットすると、その生存期間が更新されて再度 360 秒になります。生存期間内にヒットしなければレコードは削除されます。

前回アクティブな TTL は初期設定で有効になっています。

標準認証

標準認証は、Web コンソールの [管理] [一般設定] [ユーザの識別] 画面で [標準認証 (OS またはブラウザが実行)] オプションを選択することによって設定できます。

標準認証の認証は、OS またはブラウザによって提供される認証機能を介して実装されます。

ドメインに参加するクライアントが NTLM 認証をサポートするブラウザを介して Web にアクセスする場合、認証情報はブラウザから自動的に送信されるため、認証情報の入力を求めるポップアップ画面は表示されません。

クライアントがドメインに参加していない、ブラウザが NTLM 認証をサポートしていない、またはブラウザで自動認証が無効になっている場合は、自動認証が実装されないため、認証情報の入力を求めるポップアップ画面が表示されます。

キャプティブポータル

キャプティブポータルを設定するには、Web コンソールの [管理] [一般設定] [ユーザの識別] 画面で [キャプティブポータル (IWSS によってブラウザに提供されるカスタム認証ページ)] オプションを選択します。

キャプティブポータルが設定されていると、カスタム認証ページが表示され、ドメインに参加しているクライアントが Web に初めてアクセスする際に認証情報の入力を求められます (自動認証は過剰的には実装されません)。

ログインインタフェース画面はカスタマイズできます。この画面は、制限されたネットワークにユーザが初めてアクセスする際、またはユーザが IWSS で認識されない場合に表示されます。

IWSS には、カスタムのキャプティブポータルを作成するための詳細モードも用意されています。詳細モードでは、独自の HTML を作成できます。ただし、少なくとも次の JavaScript をカスタムのキャプティブポータルの最初に挿入する必要があります。

```
<SCRIPT LANGUAGE="JavaScript">function accesspolicy () {var str1 =
window.location.href;//alert (str1);var s=str1.indexOf ("?forward=") ;//alert (s) ;var
d=str1.indexOf ("&IP") ;//alert (d) ;var
uri=str1.substring (s+9,d) +"/$$$GUEST_POLICY$$$";//alert (uri) ;return uri;}</SCRIPT><form
name="loginForm" method="POST" action="com.trend.iwss.gui.servlet.captiveportal"><tr><td>User
name:</td><td><input name="username" type="text" class="button" size="24"
/></td><td>&nbsp;</td></tr><tr><td>Password:</td><td><input name="password" type="password"
class="button" size="24" /></td><td><input name="Submit" type="submit"></td></tr></form><div
class="accessmsg" [Display GuestPolicy Message...]>If you are a guest, please select the Guest Access
option to access the Internet</div><input name="Access" type="button"
onclick="window.location.href=accesspolicy () ;" [Display GuestPolicy...] />
```

認証フォームにゲストアクセスボタンとイベントハンドラを表示するには、この Java スクリプトが必要で、このスクリプトがないと、ユーザは認証を通過できません。

注意： キャプティブポータルは、ICAP モードではサポートされません。

ゲストログインの許可

ゲストアクセスは、[ゲストログインの許可] ボックスがオンの場合に有効になります。有効である場合は、[ゲスト] と表示されたボタンが追加表示されます。ゲストはこのボタンを選択することでインターネットにアクセスできますが、その操作はゲストポリシーによって管理されます。ゲストポリシーは、ポリシーリストでゲストアクセスが有効である場合に自動的に表示されます。これ以外の場合には表示されません。

ゲストアクセスを許可するには

1. [認証方法] セクションで、[キャプティブポータル (IWSS によってブラウザに提供されるカスタム認証ページ)] オプションを選択します。
2. [ゲストログインの許可] チェックボックスをオンにします。
3. [キャプティブポータル] 画面の外観をあらかじめ設計して、HTML 形式で保存することができます。色、ロゴ、およびテキストを使用して、企業のブランドイメージに合わせます。カスタマイズした HTML コードをコピーして空白のボックスに貼り付けます。ログイン認証方法とゲストアクセスボタンを表示するには、`<%T%>` タグを使用します。
4. [ログインのプレビュー画面] をクリックして、設定結果を表示します。
5. [保存] をクリックして、設定を保存します。

Cookie モード

Cookie モードは、NAT およびターミナルサーバ環境におけるユーザの識別に使用されます。Cookie モードを使用するには、クライアントコンピュータに Adobe Flash Player がインストールされ、ブラウザの Cookie が有効であることを確認します。

Cookie モードは、ユーザ / グループ認証が有効でキャプティブポータルを選択した場合にのみ使用できます。

[キャプティブポータル] ログイン画面の [サインインを保持する] オプションを使用すると、Cookie の「有効期間」を最大で 1 年間、有効にできます。[サインインを保持する] オプションが選択されていない場合、Cookie の「有効期間」は 1 日です。

なし

(推奨しません) ログイベントおよびレポートに出力されるユーザが匿名になり、URL フィルタとその他のポリシーが IP アドレスに基づいて作成されます。

注意： ホスト名の識別は、Microsoft Windows プラットフォームの Internet Explorer で閲覧するエンドユーザに対してのみサポートされています。

```
/etc/iscan/intscan.ini ファイルの [user-identification] に  
use_mac_address=yes を設定して、クライアントコンピュータのマシンアドレス  
(MAC) をイベントログ、レポート、および通知に記録できます。設定を変更したら、  
/etc/iscan/S99ISproxy stop を実行してから /etc/iscan/S99ISproxy  
start を実行し、設定を適用します。
```

警告： [ホスト名] を選択する前に、クライアントごとに register_user_agent_header.exe ファイルを実行して、LAN 上のすべてのクライアントを準備しておく必要があります。このファイルはインストールパッケージの付属品です。Windows ドメインのログインスクリプトにこれを追加しておくか、この目的のためにスクリプトを作成しておくことファイルの実行に便利です。

ポリシー確認画面

[ポリシー確認] 画面タブは、企業のネットワークユーザにインターネット使用ポリシーを知らせません。

基本モード

[ポリシー確認] 画面 (PAS) が有効であると、会社のインターネットアクセスポリシーのコピーがユーザに表示されます。ただし、[ポリシー確認] 画面を使用可能にするには、事前に LDAP 認証を有効にしておく必要があります。

PAS は、Web コンソールの [管理] [一般設定] [ユーザの識別] タブの [ポリシー確認画面] タブを使用してカスタマイズできます。この場所で、[ポリシー確認] 画面の有効と無効を切り替えることもできます。

ポリシー確認画面をカスタマイズする

1. ポリシー確認画面の表示 このボックスをオンにすると、IWSS がユーザを透過的に認証できるかどうかにかかわらず、すべてのユーザが PAS に転送されます。IWSS でユーザを透過的に認証できなかった場合は、キャプティブポータルで、続行する前にユーザ名とパスワードを入力するよう求められます。IWSS がユーザを透過的に認証した場合は、[OK] と表示されたボ

タンをクリックすると続行できます。いずれの場合も、PAS が表示されて会社のインターネットアクセスの使用ポリシーが示されます。PAS は、ユーザが初めてインターネットにアクセスする際にのみ表示されます。その後は、キャッシュの有効期限が切れるまで表示されません。

基本設定でポリシー確認画面をカスタマイズする

1. ようこそメッセージを入力します。
2. Trend Micro、Google など、自社名を入力します。
3. 会社のロゴをアップロードします。画像サイズは 1MB 未満にする必要があります。
4. 外部 HTTP リンクを入力します。
5. ポリシーメッセージを入力します。
6. [保存] をクリックします。

ポリシー確認画面を表示する

1. [管理] [一般設定] [ユーザの識別] | [ポリシー確認画面] の画面オプションにアクセスします。
2. [ポリシー確認画面の表示] のチェックボックスをオンにします。24 時間サイクルでユーザがインターネットにアクセスするたびに適切な使用ポリシーメッセージが、別画面で示されます。
3. この画面は、次に説明するように、基本モードまたは詳細モードのいずれかの方法で設定します。

認証の許可リスト

LDAP 認証を有効にした後は、会社の認証の許可リストに IP アドレスが登録されているユーザを除き、すべてのユーザがユーザ名とパスワードを提供する必要があります。このリストには、特定の IP/ ホスト名、IP 範囲、または IP サブセットを定義できます。会社の許可リストを作成または編集するには、[管理] [一般設定] [ユーザの識別] [認証の許可リスト] の順に選択します。

ポリシー配信

作成または変更したポリシーは、[ポリシーの配信] ボタンをクリックすることによって、ただちに IWSS ポリシーデータベースに配信できます。または、何も実行しなくても、[管理] [ポリシー配信] 画面で設定されている生存期限 (TTL) 間隔に従って、ポリシーは自動的に配信されます。

初期設定では、IWSS から 30 分ごとに次の最新ポリシーが自動的に配信されます。

- ・ ウイルス検索ポリシー
- ・ HTTPS ポリシー

- ・ HTTP 検査ポリシー
- ・ URL フィルタポリシー
- ・ アクセス割り当てポリシー
- ・ アプリケーション制御ポリシー
- ・ 情報漏えい対策ポリシー

データベース接続

IWSS は独自の PostgreSQL データベースをインストールします。データベースにはポリシー設定とログデータが格納されています。データベース接続は、Web コンソールの [管理] [一般設定] [データベース接続] タブで確認できます。データベースの設定は `/etc/iscan/intscan.ini` ファイルに保存されます。次のフィールドは、Linux の ODBC データソースと関係なく変更しないでください。

データベース接続設定

- ・ ODBC データソース名 ODBC 名を表示します。
- ・ ユーザ名 ODBC データソースのユーザ名を表示します。初期設定は「sa」です。
- ・ パスワード 暗号化された ODBC パスワードを「*****」で表示します。
- ・ データベース接続のテスト ポリシーデータベースおよびログデータベースの接続が正しいこと、および接続が機能していることを確認するには、これをクリックします。応答メッセージが ODBC データソースから生成されます。

隔離管理

スパイウェア、トロイの木馬、ワームなどのインターネット上の脅威のほとんどは、ファイルに感染しないため「駆除」の対象になりません。IWSS の検出対象に設定しておいたワームは（膨大な数になる可能性があるため）削除し、スパイウェア、トロイの木馬、その他の不要なプログラムは隔離または削除することをお勧めします。

隔離ディレクトリ

隔離先のディレクトリ [HTTP 検索] または [FTP 検索] の [処理] を [隔離] に設定している場合は、隔離されるファイルがここで指定したディレクトリに移動されます。初期設定のディレクトリは、次のとおりです。

```
/var/iwss/quarantine
```

注意： 278 ページの「隔離ファイルの暗号化」で説明しているように、隔離ファイルはすべて暗号化することをお勧めします。

隔離ファイルの暗号化

隔離ファイルは危険です。隔離ファイルを暗号化すれば、不注意による再感染および他の種類の悪意のあるコードから保護できます。

疑わしいファイルを削除せずに隔離する場合は、隔離ディレクトリに保存する前にファイルを暗号化することをお勧めします。

注意： 隔離ファイルを復号化する手順については、IWSS オンラインヘルプの「操作方法」セクションを参照してください。

HTTP 隔離ファイルを暗号化するには

1. [HTTP] [高度な脅威保護] [ポリシー] の順に選択し、リストから既存のポリシーを選択するか、または [追加] をクリックして新しいポリシーを作成します。
2. [ウイルス / 不正プログラム検索ルール] タブを開きます。画面の下部で、[隔離ファイルを暗号化する] チェックボックスをオンにします。

FTP 隔離ファイルを暗号化するには

1. [FTP] [検索ルール] をクリックします。
2. [ウイルス検索ルール] タブを開きます。画面の下部で、[隔離ファイルを暗号化する] チェックボックスをオンにします。

予約期間

URL フィルタ、アプリケーション制御、または HTTP 検査のポリシーを設定する場合、複数の予約期間で IWSS に異なる動作をさせることができます。たとえば、業務時間外にレクリエーション目的の Web アクセスやインスタントメッセージの使用を許可することができます。URL フィルタのポリシーは、この業務時間の設定に基づいて実行でき、異なる個人またはグループに異なる設定を適用できます。

Control Manager への登録

注意： IWSS は、Trend Micro Control Manager (以下、Control Manager) または Trend Micro Apex Central (以下、Apex Central) への IPv4 アドレスでの接続のみをサポートします。

[管理] [一般設定] [Control Manager への登録] 画面を使用して、管理通信プロトコル (MCP) エージェントと Control Manager または Apex Central サーバとの間の通信を設定します。

- ・ 接続設定 エンティティ名 (特定のコンピュータ上の IWSS インスタンス) を指定します。エンティティ名が Control Manager または Apex Central の製品ツリーに表示されるので、製品の識別に役立ちます。
- ・ Control Manager サーバ設定 Control Manager または Apex Central サーバの完全修飾ドメイン名 (FQDN) または IP アドレスを指定します。Web サーバの認証ユーザ名は、Internet Information Services (IIS) サーバで認証に使用されます。この情報は Control Manager または Apex Central では使用されません。
- ・ MCP プロキシ設定 このセクションでは、Control Manager または Apex Central サーバとの通信に使用するプロキシサーバを指定します。
- ・ 双方向通信ポート転送 双方向通信にすると、Control Manager または Apex Central サーバから IWSS にリアルタイムでコマンドを送信できます。この情報を指定しない場合、エージェントの初期設定は一方通信になるため、IWSS は、コマンドを受信するために所定の間隔で Control Manager または Apex Central サーバをポーリングします。

複製の設定

IWSS 複製元インスタンスから IWSS 複製先インスタンスへの、IWSS デバイスの登録および設定の複製を提供します。1 つの IWSS デバイスから 1 つ以上の IWSS 複製先に、手動または定期的な間隔でポリシーと設定ファイルをコピーしたい場合は [設定の複製] を使用します。ポリシーを設定して、複製の頻度を設定し、ルートアカウントを選択して、設定ファイルを複製元からエクスポートできます。

設定の複製ポリシーを設定するには

1. IWSS Web コンソールを開き、[管理] [一般設定] [複製の設定] の順に選択します。
2. スタンドアロン (初期設定)、複製元、または複製先のいずれかのサーバの役割を選択します。複製元を選択する場合は、[設定の複製元] チェックボックスをオンにして、[保存] をクリックします。複製元が正常に確立されたことを確認するポップアップメッセージが表示されますの

で、[OK] をクリックします。

複製先の場合は、次の手順を実行します。

3. [設定の受信者] チェックボックスをオンにして、複製元の管理 IP アドレス、ポート、およびセキュリティプロトコルを入力します。

複製元から設定ファイルをエクスポートするために使用する複製元の管理者アカウント (admin) のパスワードを指定します。ポリシーと設定の複製は、初期設定では 1 時間ごとに行われます。

4. [保存] をクリックします。

注意： 手動で同期できるのは「マスター管理者」のみです。

集中管理ログ / レポート

IWSS では、ログ送信元リストと、サーバから利用可能なステータスを使用します。集中管理ログ / レポート機能は複数の IWSS サーバでサポートされます。IWSS サーバの 1 つを選択して、ログ / レポートコンソール (ログサーバ) として使用できます。IWSS はログをこのサーバに送信します。ログサーバ上のログ / レポートは、デバイスグループを使用して管理できます。

集中管理ログ / レポートを設定するには

1. IWSS メニューから、[管理] [一般設定] [集中管理ログ / レポート] の順に選択します。
2. 初期設定のサーバの役割はスタンドアロンです。ログサーバまたはログ送信元のどちらかのサーバの役割を選択します。
 - ログサーバ
 - i. ログを受信するサーバとして使用する場合は、[ログサーバ] チェックボックスをオンにして [保存] をクリックします。
 - ii. 表示されるポップアップ画面で [OK] をクリックします。
 - iii. IWSS Web コンソールを開き、[管理] [一般設定] [集中管理ログ / レポート] の順に選択して、[デバイスグループ管理] でデバイスグループを選択します。
 - iv. 新規グループを追加するには、[追加] をクリックし、グループ名と説明を指定し、IP アドレスを選択して、[保存] をクリックします。
 - ログ送信元
 - i. ログ送信元サーバとして使用する場合は、[ログ送信元] チェックボックスをオンにして、ログを受信するサーバの管理 IP、管理ポート、および管理者アカウントのパスワードを指定します。

- ii. [保存] をクリックします。

既存のすべてのデバイスグループが [デバイスグループ管理] に表示されます。デバイスグループは [ログ]、[レポート]、[ダッシュボード] 画面にも表示され、これらの画面でログとレポートのクエリを実行できます。

検索方法

この画面を使用して、データおよび Web サイトの検索方法を設定できます。IWSS には次の 3 種類の検索方法があります。

- ・ Trend Micro Global Smart Protection Server (SPS) を使用したスマートスキャン Trend Micro Smart Protection Network を使用して Web サイトやデータを検索します。クラウドに保存された脅威のシグネチャを利用して最新の保護を提供します。
- ・ ローカル Smart Protection Server (SPS) を使用したスマートスキャン クラウド検索における遅延を回避するため、検索リクエストをローカルの Smart Protection Server に送信します。ローカル Smart Protection Server を使用することで、プライバシーがより強化され、処理速度も向上します。ネットワークにアクセスする製品、サービス、およびユーザーが増えるにつれて、セキュリティ保護は自動的に更新および強化され、ユーザーに対するリアルタイムのネイパーフドウォッチ (近隣監視活動) 保護サービスが形成されます。
- ・ 従来型の検索 従来型の検索では、ローカルに保存された不正プログラム対策コンポーネントやスパイウェア対策コンポーネントを使用します。

注意： スマートスキャンを使用するには、IWSS で Trend Micro Smart Protection Network に継続的に接続する必要があります。3 回連続して Trend Micro Smart Protection Network に接続できなかった場合、IWSS は自動的に従来型スキャンに切り替え、継続して保護を提供できるようにします。自動的に従来型の検索に切り替わった場合は、[管理] [一般設定] [検索方法] から [スマートスキャン] を選択する必要があります。

PAC ファイル管理

この画面を使用して、PAC (Proxy Auto-configuration) ファイルの追加、編集、コピー、および削除を含む、PAC ファイルの管理を実行できます。

各 PAC ファイルに対して、ファイルの名前、説明、および内容を指定できます。IWSS では、PAC ファイルの内容については確認しません。

サンプルの PAC ファイルが用意されています。サンプルファイルを使用するには、IWSS-HOSTNAME を実際の IWSS ホスト名で置き換えます。サンプル PAC ファイルは編集のみ可能で、削除することはできません。

管理コンソール

[管理コンソール] 画面では、admin アカウントがログインアカウントを追加または削除できます。ログインアカウントは、Web コンソールの [管理] [管理コンソール] [アカウント管理] 画面で設定できます。

管理コンソールには、次のオプションが用意されています。

- 282 ページの「アカウント管理」
- 283 ページの「役割ベースの管理」
- 284 ページの「役割の管理」

アカウント管理

アカウント管理を使用して、アカウントの追加および削除を実行できます。アカウント管理では、既存のすべてのアカウントをユーザ名と説明とともに表示し、役割を割り当てます。

ログインアカウントを追加する

ログインアカウントを追加するには

1. 管理コンソールから [管理] [管理コンソール] [アカウント管理] の順に選択します。
2. [アカウント管理] 画面で、[追加] をクリックします。
3. [ログインアカウント] 画面で、必要な情報を入力します。
 - [ローカルアカウント] または [LDAP アカウント] アカウントの種類を選択します。

注意： IWSS Web コンソールで LDAP が設定されていない場合、[LDAP アカウント] オプションは無効になります。

[LDAP アカウント] を選択すると、[ユーザ名] と [パスワード] が無効になり、代わりに LDAP アカウント情報が使用されます。

- ユーザ名 ログインアカウントに割り当てられたユーザの名前。

- ・ パスワード 4 ~ 32 文字の英数字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の簡単な説明。
 - ・ 役割 ドロップダウンリストから役割を選択します。286 ページの「組み込みのユーザの役割」を参照してください。
4. [保存] をクリックします。
[アカウント管理] 画面に、新しいログインアカウントが表示されます。

ログインアカウントを変更する

ログインアカウントを変更するには

1. 管理コンソールから [管理] [管理コンソール] [アカウント管理] の順に選択します。
2. 対象のユーザ名をクリックします。
3. [ログインアカウント] 画面で、必要な情報を変更します。
 - ・ パスワード 4 ~ 32 文字の英数字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の簡単な説明。
 - ・ 役割 ドロップダウンリストから役割を選択します。286 ページの「組み込みのユーザの役割」を参照してください。
4. [保存] をクリックします。
[ログインアカウント] 画面に、変更されたログインアカウントが表示されます。

役割ベースの管理

IWSS Web コンソールへのアクセスを許可および制御するには、役割ベースの管理を使用します。組織内に IWSS 管理者が複数いる場合は、この機能を使用して Web コンソールの権限を管理者に個別に割り当て、特定のタスクの実行に必要なツールと権限のみを付与できます。1 つ以上のドメインを管理対象として割り当てることにより、エージェントツリーへのアクセスを制御することもできます。さらに、Web コンソールへの「閲覧のみ」のアクセス権を管理者以外のユーザに付与できます。

各ユーザ (管理者または非管理者) に特定の役割が割り当てられます。役割とは、Web コンソールへのアクセスレベルを定義するものです。ユーザは、カスタムユーザアカウントまたは Active Directory アカウントを使用して Web コンソールにログオンします。

役割ベースの管理には、次のタスクがあります。

1. ユーザの役割を定義します。詳細については、284 ページの「役割の管理」を参照してください。
 - ・ ユーザアカウントを設定し、各ユーザアカウントに特定の役割を割り当てます。詳細については、282 ページの「アカウント管理」を参照してください。

役割の管理

役割の管理により、必要に応じて役割を追加または削除できます。これらの役割には次のものがあります。

- ・ **管理者** システムへの制限のない完全なアクセスが許可されます。コンソールからアクセスして、ユーザアカウントやユーザの役割の作成、削除、変更を除く、設定の読み取りと変更が可能です。
- ・ **監査担当者** 設定の変更はできませんが、設定、ログ、およびレポートの表示と、自身のパスワードの変更はできます。
- ・ **レポート専用** システムステータス、ダッシュボード、ログ、およびレポートの各画面の閲覧のみ可能です。ログのクエリ、レポートの生成、およびユーザ自身のパスワードの変更を行います。
- ・ **カスタムの役割** 一部あるいはすべての管理ドメインに対する完全なアクセス、読み取り専用、またはアクセスなしで、手動で追加されます。ユーザは、自身の役割に割り当てられたアクセス権に基づいてさまざまなページを変更または表示できます。

詳細については、283 ページの「役割ベースの管理」を参照してください。

メニュー項目の権限

ユーザの役割により、ユーザがアクセス可能な Web コンソールのメニュー項目が決まります。役割には各メニュー項目の権限が割り当てられています。

権限は各メニュー項目へのアクセスレベルを決定します。メニュー項目の権限は次のいずれかに設定できます。

- ・ **フルアクセス**：メニュー項目への完全なアクセスが許可されます。ユーザはメニュー項目ですべての設定およびタスクを実行し、データを表示することができます。
- ・ **読み取り専用**：メニュー項目の設定、タスク、およびデータを表示することのみが許可されます。
- ・ **アクセスなし**：メニュー項目を非表示にします。

管理メニュー項目のアクセス

次の表に、管理者が利用できるメニュー項目のリストを示します。

表 12-2. 管理メニュー項目

管理ドメイン	メニュー項目
ステータス監視	<ul style="list-style-type: none">・ システムステータス・ ダッシュボード
ポリシー管理	<ul style="list-style-type: none">・ アプリケーション制御・ HTTP・ FTP
ログ	<ul style="list-style-type: none">・ ログ分析・ お気に入りログ・ 設定
レポート	<ul style="list-style-type: none">・ 選択されたユーザ / グループのレポート
システム管理	<ul style="list-style-type: none">・ アップデート・ 通知・ 管理 <hr/> <p>注意： 組み込みの管理者アカウント (Admin) を使用するユーザのみが、ユーザアカウントおよびユーザの役割にアクセスできます。</p> <hr/>

組み込みのユーザの役割

IWSS には一連の組み込みのユーザの役割が用意されており、これらを変更または削除することはできません。組み込みの役割は次のとおりです。

表 12-3. 管理メニュー項目

管理ドメイン	説明
管理者	ユーザには、システムへの制限のないアクセスが許可されます。コンソールからアクセスして、ユーザアカウントやユーザの役割の作成、削除、変更を除く、設定の読み取りと変更が可能です。
監査担当者	設定変更はできませんが、設定、ログ、レポートの閲覧が可能です。自分のパスワードを変更することもできます。
レポート専用	システムステータス、ダッシュボード、ログ、およびレポートの各画面の閲覧のみ可能です。ログのクエリ、レポートの生成、およびユーザ自身のパスワードの変更を行えます。

カスタムの役割

要件を満たす組み込みの役割がない場合、カスタムの役割を作成できます。組み込みの管理者の役割を持つユーザのみが、カスタムのユーザの役割を作成して、その役割をユーザアカウントに割り当てることができます。

カスタムの役割の追加

カスタムの役割を追加するには

1. メインメニューから、[管理] [管理コンソール] [役割の管理] の順に選択します。
2. [追加] をクリックします。
新しい画面が表示されます。
3. 役割の名前およびオプションで説明を入力します。
4. [役割の権限] で各管理ドメインのアクセス権を選択します。アクセスの詳細については、285 ページの「管理メニュー項目のアクセス」参照を参照してください。
5. [保存] をクリックします。

新しい役割が役割リストに表示されます。

カスタムの役割の変更

カスタムの役割を変更するには

1. メインメニューから、[管理] [管理コンソール] [役割の管理] の順に選択します。
2. 役割の名前をクリックします。
新しい画面が表示されます。
3. 次のいずれかを変更します。
 - ・ 役割の名前
 - ・ 役割の説明 (任意)
 - ・ 役割の権限: 各管理ドメインのアクセス権を変更します。
4. [保存] をクリックします。

カスタムの役割の削除

カスタムの役割を削除するには

1. メインメニューから、[管理] [管理コンソール] [役割の管理] の順に選択します。
2. 削除する役割を選択します。
3. [削除] をクリックします。
確認メッセージが表示されます。
4. [OK] をクリックします。

設定のバックアップと復元

[設定のバックアップ / 復元] 画面では、バックアップ用の IWSS 設定ファイルを生成できます。また、この画面から、次のバージョンの設定情報とポリシー情報を IWSS 6.5 に移行できます。

- ・ IWSS 6.5 Patch 2
- ・ IWSS 6.5 Patch 3
- ・ IWSVA 6.5 Service Pack 2
- ・ IWSVA 6.5 Service Pack 3

次の設定とデータは移行できません。

- ・ データベースに格納されているログ、テキストベースのログファイル、レポート、および隔離ファイル

- ・ パターンファイル、検索エンジンファイル、および設定ファイル内の関連バージョン情報
- ・ データベースのパスワードと設定
- ・ ライセンスプロファイル
- ・ Web コンソールの [管理] セクションの下にある LDAP 設定、PAC ファイル管理、ポリシー配信設定、および予約期間を除くすべての設定
- ・ IP アドレス、ホスト名など、システムレベルの設定
- ・ IWSS のパッチ

システムアップデート

以下のトレンドマイクロの最新版ダウンロードサイトで、システムアップデートを入手できます。
https://www.trendmicro.com/ja_jp/business/products/downloads.html

システムアップデートでは、アプリケーションパッチが提供されます。

パッチは、[管理] [システムアップデート] 画面の [履歴] に表示されます。このユーティリティでは、正しくフォーマットされ、暗号化されたトレンドマイクロのアップデートのみアップロードできます。

システムアップデートをインストールするには

1. 以下のトレンドマイクロの最新版ダウンロードサイトから最新のアップデートを入手します。
https://www.trendmicro.com/ja_jp/business/products/downloads.html
2. [管理] [システムアップデート] に移動します。
3. [参照] をクリックして、ダウンロードしたファイルを選択します。
4. [アップロード] をクリックします。
5. [概要] 画面で、[インストール] をクリックします。
6. 正常にインストールされたことを示すメッセージを受け取ったら、別の画面に移動できます。

注意： アプリケーションパッチを削除する手順については、311 ページの「アプリケーションパッチの適用またはアプリケーションパッチの削除」を参照してください。

警告： 他のソースからのアップデートファイルは、IWSS サーバに適用しないでください。

注意： アップデート後に、IWSS サーバは再起動することがあります。

システムイベントログ

システムイベントログには、システムで発生する状態の変化やエラーに関する情報が含まれます。次のような種類のイベントが記録されます。

- ・ アップデート
- ・ 製品の登録

システムイベントログを表示するには

1. 管理コンソールから [管理] [システムイベントログ] の順に選択します。
2. [期間] で期間を選択します ([すべて]、[今日]、[過去 7 日間]、[過去 30 日間])。任意の期間を選択するには、[範囲] をクリックし、開始と終了の日付を選択します。
3. [レベル] で、ログエントリを表示するイベントレベルを選択します。[追加] をクリックします。リストにあるすべてのスパイウェアを追加する場合は、[すべて追加] をクリックします。イベントレベルを右側のリストボックスから削除するには、[削除] をクリックします。リストにあるすべてのレベルを削除する場合は、[すべて削除] をクリックします。
4. [並べ替え基準] で、ログの並べ替えの基準とする項目を選択します。[サーバ]、[日付]、[レベル]、[送信元] のオプションがあります。
5. [ログ表示] をクリックします。[システムイベントログ] 画面が開きます。
6. 表示を更新するには、[表示更新] をクリックします。

製品ライセンス

製品ライセンス機能を使用して、IWSS の登録およびライセンス確認を実行できます。IWSS の完全なアクティベーションプロセスは、2 つの手順で構成されます。まず、トレンドマイクロに IWSS を登録する必要があります。登録後、製品の使用を許可する有効な IWSS アクティベーションコード (AC) が提供されます。

トレンドマイクロ製品に対するライセンスには通常、購入日から 1 年間のみ、製品のアップデート、パターンファイルのアップデート、および基本的なテクニカルサポート (「サポート契約」) を得る権利が含まれます。

IWSS をアクティベートするには、まず、製品の登録時に取得するレジストレーションキーが必要です。これを使用してアクティベーションコードを取得できます。配置ウィザードを使用して、または後で IWSS 管理コンソールを使用して、IWSS をアクティベートできます。

ライセンス期限切れの警告

通常、サポート契約の有効期限が切れる 90 日前から、期限切れが近付いていることを警告するメール通知を受信し始めます。サポート契約の更新については、販売代理店またはトレンドマイクロの営業担当にお問い合わせください。以下のトレンドマイクロオンライン登録の URL から更新できます。

<https://clp.trendmicro.com/fullregistration>

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

レジストレーションキーの取得

レジストレーションキーは、以下の場所にあります。

- Trend Micro Enterprise Solution DVD
- ライセンス証明書（製品の購入後に取得）

次の機能をご利用いただくために、お客さまのレジストレーションキーを登録およびアクティベートしていただく必要があります。

- IWSS パターンファイルおよび検索エンジンのアップデート
- テクニカルサポート
- ライセンスの有効期限の更新、登録、および詳細情報の表示

レジストレーションキーは 31 文字であり、以下のようになります。

XX-XXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX

アクティベーションコードの取得と入力

アクティベーションコードの有効期限が切れた場合、IWSS のセキュリティアップデートは無効になります。[製品ライセンス] 画面では、製品ライセンスの更新手順やステータスを確認できます。

IWSS をアクティベートするには、アクティベーションコードが必要です。

アクティベーションコードは 31 文字であり、以下のようになります。

xx-xxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx

ライセンスの更新

Web から最新のライセンスを取得するには、[管理] [製品ライセンス] に移動して、[ステータス更新] をクリックします。

更新手順の詳細については、次を参照してください。

https://www.trendmicro.com/ja_jp/buy/renewal.html

サポート契約の更新

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

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

- ・ サポート契約を更新するには、製品をお買い上げいただいた購入元にお問い合わせください。契約期間を 1 年間延長したサポート契約は、登録プロフィールに表示される企業の担当者宛てに郵送されます。
- ・ 企業の登録プロフィールを表示または変更するには、次のトレンドマイクロオンライン登録の Web サイトからアカウントにログインします。

<https://clp.trendmicro.com/fullregistration>

SNMP の設定

SNMP 通知は、IWSS サービスの状況を監視するのに特に役立ちます。サービスが予期せず停止した場合、IWSS が SNMP 通知を送信します。IWSS は、IPv4 または IPv6 のいずれかのアドレスを使用して、トラップの宛先ネットワークの管理システムをサポートします。IWSS では、以下のイベントに関する SNMP エージェントの通知をサポートしています。

- IWSS サービスの予期しない停止
- ウイルスパターンファイル、検索エンジン、および URL フィルタエンジンの各アップデート
- セキュリティイベント

注意： IWSS は、HTTP または FTP 検索サービスの停止を検出した場合、サービスの再開を 2 回試みます。それでもサービスを再開できない場合は、サービスが再開されるまで、指定しておいた宛先に 30 分ごとに SNMP 通知が発行されます。

注意： IWSS は、SNMP バージョン 3 の SNMP 通知をサポートします。

システム情報の設定

必要なシステム情報はすべて、[管理] [SNMP の設定] 画面の [システム情報] で指定します。

[コミュニティ名] および [初期設定のコミュニティ] に指定するコミュニティは、SNMP オブジェクトが属するコミュニティを識別します。SNMP では、すべての管理対象オブジェクトがコミュニティに属します。これにより、コミュニティを指定して通信可能な SNMP エージェントを定義できるようになるため、最低限のセキュリティが確保されます。

アクセス管理設定

必要なアクセス管理情報はすべて、[管理] [SNMP の設定] 画面の [アクセス管理の設定] で指定します。

IWSS が簡単なステータスメッセージやアラートメッセージを送信するため、このセクションのフィールドは読み取り専用です。[読み取り専用オブジェクト ID (OID)] のオブジェクト ID (OID) は、特定のメッセージ、アラート、またはアラームのコードです。「オブジェクト」とは、実際のメッセージ、アラート、またはアラームです。

Web コンソール

初期設定で、IWSS 管理コンソールへのアクセスは、ポート 8443 上の HTTP 接続を介して行われます。セキュリティを高めるため、セキュアソケットレイヤ接続 (HTTPS) の使用をお勧めします。Web コンソールへの接続は、Web コンソールの [管理] [Web コンソール] 画面で設定できます。

注意： Web コンソールの初期設定の秘密鍵に対する初期設定のパスワードは「adminIWSS85」です。

Web コンソールを非 SSL モードから SSL モードに変更する場合、証明書と秘密鍵のインポートは不要です。初期設定のパスワードを入力して処理を続行できます。

IWSS は、次のように指定されたポートを使用します。

- ・ 非 SSL モード たとえば、セキュリティで保護されていない以下のような URL を使用して、IWSS 管理コンソールにアクセスします。
`http://<IWSS サーバ IP アドレス : ポート >`
 - ・ ポート番号 初期設定は 1812 です。ファイアウォールで認識されている未使用のポートに変更することができます。
- ・ SSL モード 初期設定の推奨モードです。セキュリティで保護された、IWSS 管理コンソールへの接続を有効にするには、このオプションを選択します。
 - ・ SSL 証明書 IWSS で SSL をサポートするには、公開鍵と証明書が必要です。使用する証明書を指定し、IWSS サーバにアップロードします。
 - ・ SSL パスワード SSL 証明書に関連付けられたパスワードがあれば入力します。
 - ・ ポート番号 初期設定は 8443 です。IWSS 管理コンソールを開くために使用するポートを次のように入力します。

`https://<IWSS サーバ IP アドレス : ポート >`

サポート情報

IWSS では、ケース診断ツール (CDT) を使用して、プロセスが異常終了したときのメモリ内のシステムデータを含むコアおよびシステム情報ファイルが生成されます。[システム情報ファイルの生成] ボタンはこの機能を拡張したもので、クリックすると現在のコンピュータの「状態」をパッケージ化することができます。

IWSS によって生成されるコアおよびシステム情報ファイルには次の情報が含まれます。

- ・ IWSS 情報 IWSS 製品バージョン、検索エンジンのバージョン、ビルド番号、および IWSS HotFix と Service Pack の情報。製品設定および統合設定もこの情報に含まれます。
- ・ IWSS/ システムログ IWSS ログとデバッグログ、syslogd デーモンによって生成されたログ (システムログが有効の場合)、およびコアダンプファイル。
- ・ システム / ネットワーク情報 ハードウェア設定、OS、ビルド、システムリソースのステータス、他のインストール済みアプリケーション、およびネットワーク情報。
- ・ CDT 対応設定 / プラグイン情報 Contorl Manager または MCP エージェントなどの新しいコンポーネントを IWSS に追加したことによる、CDT への変更に関する情報。
- ・ デバッグログ IP フィルタを使用して作成されたデバッグログ。

デバッグログ

デバッグログでは、ローカルコンピュータおよびそのコンピュータにログオンしているユーザに、グループポリシーやその拡張子を使用して適用されたすべての変更と設定を追跡します。デバッグログを有効にすると、デバッグログにレジストリキーが追加されます。

デバッグログを有効にするには

1. デバッグログで追跡する IP アドレスまたは IP 範囲を入力します。
2. [選択済み] ボックスにエントリを追加します。
3. [取り込みの開始] をクリックします。
4. ダウンロード対象の生成済みデバッグログの種類を 1 つ選択します。
5. ログを削除するか、今後の評価のためにコンピュータにダウンロードするかを選択します。

配信診断

トレンドマイクロのサポートサービスを利用して配信の問題の原因を診断する場合は、配信診断ファイルを使用します。

IWSS でシステムファイルの生成中に、すべての診断情報の収集の妨げになる状況がアプリケーションで発生することがあります。この場合、IWSS では、利用可能な情報を収集し、発生したエラーを包括的なメッセージとともにログファイルに記録します。このメッセージは、削除することも、今後評価するためにコンピュータにダウンロードすることもできます。

製品のテストと設定

InterScan Web Security Suite (以下、IWSS) コンソールを開いてから、次のテストを実施してプログラムが正しく動作していることを確認します。この章で説明するテストは次のとおりです。

- 296 ページの「EICAR テストファイル」
- 296 ページの「Web レピュテーションのテスト」
- 297 ページの「アップロード検索のテスト」
- 298 ページの「HTTPS 復号化検索のテスト」
- 301 ページの「FTP 検索のテスト」
- 302 ページの「アプリケーション制御のテスト」
- 303 ページの「HTTP 検査のテスト」
- 304 ページの「URL 監視のテスト」
- 306 ページの「ダウンロード検索のテスト」
- 307 ページの「URL フィルタのテスト」
- 308 ページの「スパイウェア検索のテスト」
- 309 ページの「その他の IWSS の設定」
- 315 ページの「IWSS パフォーマンスの調整」

EICAR テストファイル

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

警告： インターネットの安全性をテストするために実際のウイルスは使用しないでください。

EICAR テストウイルスは、次の URL からダウンロードできます。

<https://secure.eicar.org/eicar.com>

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

```
X50!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

注意： テストの前に、URL キャッシュ ([HTTP] [設定] [WRS/URL キャッシュ]) およびローカルブラウザのキャッシュをクリアします。いずれかのキャッシュにテストウイルスのコピーが保存されていると、ファイルをダウンロードしようとする際インターネットからではなくキャッシュからファイルを読み込もうとして、IWSS によりファイルが検出されない場合があります。

Web レピュテーションのテスト

IWSS の Web レピュテーション機能をテストするには、Web ブラウザを開いて、アドレスフィールドに次のように入力します。

<http://wrs21.winshipway.com>

テストが正常に実行されると、「この URL には、企業ポリシーに基づいてアクセスを禁止する Web セキュリティレーティングが設定されています。」という IWSS セキュリティイベントが表示されません。

アップロード検索のテスト

ウイルスのアップロードをテストするには、次の手順に従います。

1. IWSS コンソールの管理コンソールで [HTTP] [高度な脅威保護] [ポリシー] の順に選択します。[ウイルス検索を有効にする] チェックボックスをオフにしてから [保存] をクリックします。
2. 次の Web サイトからテストウイルス (eicar.com) をダウンロードします。
`http://www.eicar.org/anti_virus_test_file.htm`
3. ダウンロードしたテストウイルスをローカルコンピュータに保存します。
4. IWSS コンソールをもう一度開き、管理コンソールで [HTTP] [高度な脅威保護] [ポリシー] の順に選択します。[ウイルス検索を有効にする] チェックボックスをオンにして、[保存] をクリックします。
5. テストウイルスを Web サイトにアップロードします。図 13-1 に示すようなメッセージがブラウザに表示されます。

Trend Micro InterScan Web Security イベント

HTTP/HTTPSアップロードファイルがブロックされました

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

イベント詳細:

URL: `http://172.16.122.184/Upload/upload.cgi`

処理: 削除

詳細:

-- ファイル: eicar.com、不正プログラム: **Eicar_test_file**

駆除不能なファイルが削除されました。

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

Trend Micro InterScan Web Security Suite: iwss65.jp78

図 13-1. EICAR テストウイルスを検出したことを示す警告画面

HTTPS 復号化検索のテスト

この項では、スタンドアロンモードの IWSS で HTTPS 復号化をテストする手順について説明します。

復号化された **HTTPS** トラフィックのウイルス検索をテストするには

1. Web クライアントの HTTP プロキシが IWSS を使用するように設定します。たとえば、Internet Explorer を開き、[ツール] [インターネット オプション] [接続] [LAN の設定] [LAN にプロキシサーバを使用する] の順に選択します。
2. IWSS Web コンソールを開いて、[HTTP] [HTTPS 復号化] [設定] の [サーバ証明書の検証] で、すべてのオプションがオンになっていることを確認します。
3. [HTTP] [HTTPS 復号化] [ポリシー] の順に選択し、[HTTPS 復号化を有効にする] をオンにします。
4. [追加] をクリックして、新しい HTTPS 復号化ポリシーを作成します。[カテゴリの指定] で、[一般] の [コンピュータ / インターネット] を選択します。
5. クライアントコンピュータから、次の URL を使用してテストウイルスファイルにアクセスします。

<https://secure.eicar.org/eicar.com>

6. セキュリティ警告画面が表示されます。警告メッセージは、URL フィルタも有効か無効かによって異なります。

Trend Micro InterScan Web Security イベント

HTTP/HTTPSダウンロードファイルがブロックされました

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

イベント詳細:

URL: <https://secure.eicar.org/eicar.com>

処理: 削除

詳細:

-- ファイル: eicar.com、不正プログラム: **Eicar_test_file**
軽微なファイルが削除されました。

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

Trend Micro InterScan Web Security Suite: iwss65.jp78

図 13-2. URL フィルタが無効な場合のセキュリティ警告画面

Trend Micro InterScan Web Security イベント

URLがブロックされました

このWebサイトへのアクセスは、次のカテゴリに該当したためITのURLフィルタポリシーによってブロックされました。

イベント詳細:

URL: <https://secure.eicar.org/eicar.com>

カテゴリ: コンピュータ/インターネット

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

Trend Micro InterScan Web Security Suite: iwss65.jp78

図 13-3. URL フィルタも有効な場合のセキュリティ警告画面

管理コンソールの [ログ] [ログ分析] [インターネットセキュリティ] にて URL フィルタによるブロック情報を確認できます。

Figure 13-4 shows the log analysis interface for 'インターネットセキュリティ' (Internet Security) with the filter set to 'URL'. The table displays the following data:

時間	メッセージの種類	デバイス名	ユーザ名	URL	クライアントIP
2016/4/8 22:30:37	ウイルスログ	localhost.localdom...	Qiong Zhang (QA...	www.qq.com/www.q...	10.64.78.122
2016/4/8 22:30:37	ウイルスログ	localhost.localdom...	Handy Wang (RD...	www.google.com/w...	10.64.78.126
2016/4/8 22:30:37	ウイルスログ	localhost.localdom...	Helen Zhou (QA-C...	www.sina.com/w...	10.64.78.126
2016/4/8 22:30:37	ウイルスログ	localhost.localdom...	Jim J Wang (RD-C...	www.qq.com/w...	10.64.78.120
2016/4/8 22:30:37	ウイルスログ	localhost.localdom...	Cloud Wang (RD...	www.twitter.com/w...	10.64.78.126
2016/4/8 22:30:37	ボット検出ログ	localhost.localdom...	Cloud Wang (RD...	www.qq.com/w...	10.64.79.120
2016/4/8 22:30:37	ボット検出ログ	localhost.localdom...	Qiong Zhang (QA...	www.yourite.com/w...	10.64.79.128
2016/4/8 22:30:37	ボット検出ログ	localhost.localdom...	Jim J Wang (RD-C...	www.yourite.com/w...	10.64.79.125
2016/4/8 22:30:37	ボット検出ログ	localhost.localdom...	Handy Wang (RD...	www.yourite.com/w...	10.64.79.123
2016/4/8 22:30:37	ボット検出ログ	localhost.localdom...	Qiong Zhang (QA...	www.mysite.com/w...	10.64.79.126
2016/4/8 22:30:37	ウイルス感染-検出ログ	localhost.localdom...	David Zhang (RD...	www.virusinfected...	10.64.80.122
2016/4/8 22:30:37	ウイルス感染-検出ログ	localhost.localdom...	Cloud Wang (RD...	www.pywareinfec...	10.64.80.124
2016/4/8 22:30:37	ウイルス感染-検出ログ	localhost.localdom...	Akai Lv (QA-CN)	www.virusinfected...	10.64.80.128
2016/4/8 22:30:37	ウイルス感染-検出ログ	localhost.localdom...	Figo Cui (RD-CN)	www.virusinfected...	10.64.80.125
2016/4/8 22:30:37	ウイルス感染-検出ログ	localhost.localdom...	Helen Zhou (QA-C...	www.pywareinfec...	10.64.80.125
2016/4/8 22:30:37	APT検出	localhost.localdom...	Qiong Zhang (QA...	www.google.com/w...	10.64.78.127
2016/4/8 22:30:37	APT検出	localhost.localdom...	Qiong Zhang (QA...	www.qq.com/w...	10.64.78.122
2016/4/8 22:30:37	APT検出	localhost.localdom...	Handy Wang (RD...	www.sina.com/w...	10.64.78.122
2016/4/8 22:30:37	APT検出	localhost.localdom...	Helen Zhou (QA-C...	www.sina.com/w...	10.64.78.128
2016/4/8 22:30:37	APT検出	localhost.localdom...	Handy Wang (RD...	www.qq.com/w...	10.64.78.126

図 13-4. インターネットセキュリティログ画面の HTTPS 復号化テストのログ (URL フィルタが無効な場合)

Figure 13-5 shows the log analysis interface for 'ポリシー実行' (Policy Execution) with the filter set to 'URL'. The table displays the following data:

時間	メッセージの種類	デバイス名	ユーザ名	URL	クライアントIP	URLカテゴリ
2016/4/8 22:35	HTTP検査ログ	localhost.localdo...	Helen Zhou (QA...	www.twitter.com/w...	10.64.78.121	汎用
2016/4/8 22:35	HTTP検査ログ	localhost.localdo...	Handy Wang (R...	www.sina.com/w...	10.64.78.126	汎用
2016/4/8 22:35	HTTP検査ログ	localhost.localdo...	Handy Wang (R...	www.google.com/w...	10.64.78.123	汎用
2016/4/8 22:35	HTTP検査ログ	localhost.localdo...	Akai Lv (QA-CN)	www.qq.com/w...	10.64.78.121	汎用
2016/4/8 22:35	URLフィルタログ	localhost.localdo...	Cloud Wang (RD...	www.qq.com/w...	10.64.78.120	アダルト/成人向け
2016/4/8 22:35	URLフィルタログ	localhost.localdo...	Jim J Wang (RD...	www.sina.com/w...	10.64.78.121	アダルト/成人向け
2016/4/8 22:35	URLフィルタログ	localhost.localdo...	Akai Lv (QA-CN)	www.sina.com/w...	10.64.78.122	検索エンジン/ポータル
2016/4/8 22:35	URLフィルタログ	localhost.localdo...	Andy Wang (RD...	www.google.com...	10.64.78.128	検索エンジン/ポータル
2016/4/8 22:35	URLフィルタログ	localhost.localdo...	Cloud Wang (RD...	www.google.com...	10.64.78.129	検索エンジン/ポータル
2016/4/8 22:35	URLフィルタログ	localhost.localdo...	Qiong Zhang (Q...	www.qq.com/w...	10.64.78.127	アダルト/成人向け
2016/4/8 22:35	グループURLブロッ...	localhost.localdo...	Cloud Wang (RD...	www.renren.com...	10.64.78.126	汎用
2016/4/8 22:35	グループURLブロッ...	localhost.localdo...	Qiong Zhang (Q...	www.renren.com...	10.64.78.128	汎用
2016/4/8 22:35	グループURLブロッ...	localhost.localdo...	Akai Lv (QA-CN)	www.renren.com...	10.64.78.122	汎用
2016/4/8 22:35	グループURLブロッ...	localhost.localdo...	Jim J Wang (RD...	www.renren.com...	10.64.78.123	汎用
2016/4/8 22:35	グループURLブロッ...	localhost.localdo...	Avery Sun (RD-C...	www.renren.com...	10.64.78.126	汎用
2016/4/8 22:35	グループURLブロッ...	localhost.localdo...	Cloud Wang (RD...	--	--	URL Blocking
2016/4/8 22:35	グループURLブロッ...	localhost.localdo...	Qiong Zhang (Q...	--	--	URL Blocking
2016/4/8 22:35	グループURLブロッ...	localhost.localdo...	Cloud Wang (RD...	--	--	URL Blocking
2016/4/8 22:35	グループURLブロッ...	localhost.localdo...	Figo Cui (RD-CN)	--	--	URL Blocking
2016/4/8 22:35	グループURLブロッ...	localhost.localdo...	Akai Lv (QA-CN)	--	--	URL Blocking

図 13-5. ポリシー実行ログ画面の HTTPS 復号化テストのログ (URL フィルタが有効な場合)

FTP 検索のテスト

スタンドアロンモードでFTP ウイルス検索機能をテストするには、次の手順に従います。

FTP トラフィックのウイルス検索をテストするには

1. 次のページからテストウイルスをダウンロードします。

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

2. FTP プロキシとして動作する IWSS を介して FTP サーバにアクセスします。

たとえば、次のような IP アドレスを想定します。IWSS FTP プロキシサーバ (10.2.203.126)、FTP サーバ (10.2.202.168)

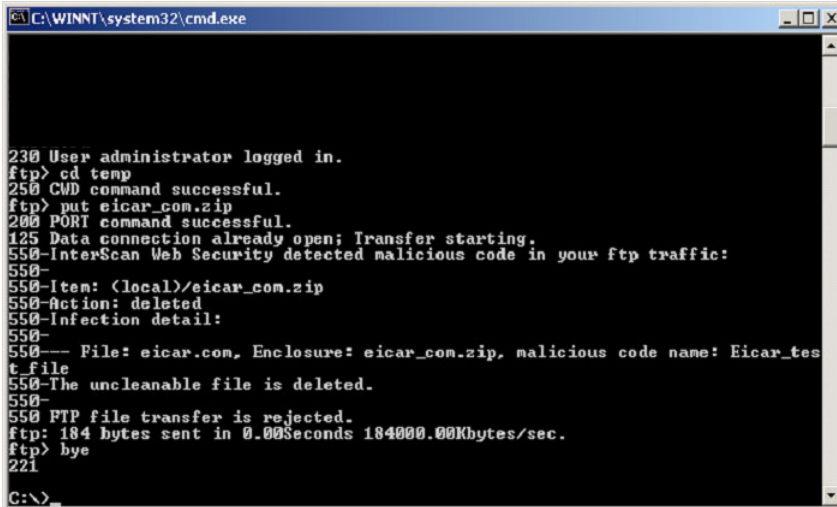
コマンドラインプロンプトを開き、次のように入力します。

```
ftp 10.2.203.126
```

3. user@host としてログオンします。たとえば、FTP アカウント名が anonymous で FTP サーバの IP アドレスが 10.2.202.168 の場合は、anonymous@10.2.202.168 としてログオンします。
4. 次のコマンドを入力して、テストウイルス (例: eicar_com.zip) をアップロードします。

```
put eicar_com.zip
```

5. IWSS の FTP プロキシモード設定が完了したら、図 13-6 に示すようなメッセージが表示されま



```
C:\WINNT\system32\cmd.exe

230 User administrator logged in.
ftp> cd temp
250 CMD command successful.
ftp> put eicar_com.zip
200 PORT command successful.
125 Data connection already open; Transfer starting.
550-InterScan Web Security detected malicious code in your ftp traffic:
550-
550-Item: (local)/eicar_com.zip
550-Action: deleted
550-Infection detail:
550-
550- File: eicar.com, Enclosure: eicar_com.zip, malicious code name: Eicar_test_file
550-The uncleanable file is deleted.
550-
550 FTP file transfer is rejected.
ftp: 184 bytes sent in 0.00Seconds 184000.00Kbytes/sec.
ftp> bye
221
C:\>
```

図 13-6. eicar_com.zip でウイルスが検出されたことを示す警告メッセージ

アプリケーション制御のテスト

アプリケーション制御機能を使用するには、IWSS をプロキシ転送モードで配信する必要があります。

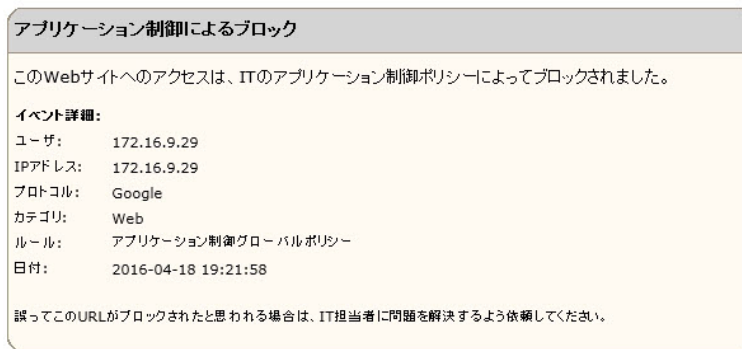
次の手順を使用すると、アプリケーション制御グローバルポリシーを変更して、エンドユーザーによる Google Web サイトへのアクセスをブロックできます。

アプリケーション制御をテストするには

1. IWSS コンソールを開き、[アプリケーション制御] [ポリシー] に移動します。
2. [アプリケーション制御を有効にする] チェックボックスをオンにして、[保存] をクリックします。
3. [アプリケーション制御グローバルポリシー] 名をクリックして変更します。
4. 次の 2 つの方法のいずれかを使用して、Google プロトコルを検索します。
 - a. [アプリケーション検索] フィールドに「Google」と入力して、[検索] ボタンをクリックします。
検索結果で、Web カテゴリに「Google」とリストされます。
 - b. Web カテゴリを下にスクロールして、カテゴリを展開し、エントリから Google を探します。
5. Web サイトのカテゴリ名の右側の列で、処理のドロップダウンメニューから、[ブロック] の処理を選択します。
6. [スケジュール] で予約期間のいずれかのオブジェクトを選択します。
7. [適用] をクリックします。
8. [保存] をクリックして、[アプリケーション制御ポリシー] 画面に戻ります。
9. [ポリシーの配信] をクリックして、更新後のポリシーを配信します。
10. ブラウザを開き、<http://www.google.com> へのアクセスを試行します。

ブラウザに、アプリケーション制御ポリシー侵害を確認する通知メッセージが表示されます。

Trend Micro InterScan Web Security イベント



Trend Micro InterScan Web Security Suite: localhost.localdomain

図 13-7. アプリケーション制御ポリシー通知の例

HTTP 検査のテスト

この手順を使用して、HTTP 検査ブラウザタイプフィルタをテストします。このフィルタは一致する FireFox ブラウザから送信される要求を識別します。

HTTP 検査をテストするには

1. IWSS コンソールを開き、[HTTP] [HTTP 検査] [ポリシー] に移動します。
2. [HTTP 検査を有効にする] チェックボックスをオンにして、[保存] をクリックします。
3. [HTTP 検査のグローバルポリシー] 名をクリックして、変更するポリシーにアクセスします。
4. HTTP 検査フィルタのリストの上にある処理のドロップダウンメニューから、[ブロック] の処理を選択します。
5. [スケジュール] で予約期間のいずれかのオブジェクトを選択します。
6. [適用] をクリックします。
7. [保存] をクリックして、[HTTP 検査ポリシー] 画面に戻ります。
8. [ポリシーの配信] をクリックして、更新後のポリシーを配信します。

9. Firefox ブラウザを使用して、<http://www.google.com> などの `http://` URL にアクセスしてみます。図 13-8 に示すような通知メッセージがブラウザに表示されます。

Trend Micro InterScan Web Security イベント

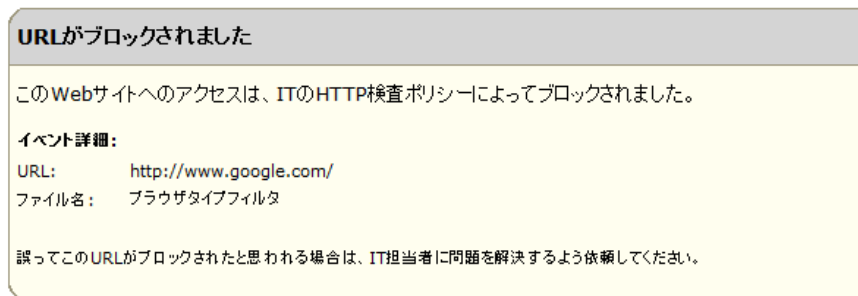


図 13-8. HTTP 検査のポリシー侵害通知

URL 監視のテスト

URL フィルタの監視機能をテストする前に、Web クライアントの HTTP プロキシが IWSS を使用するよう設定する必要があります。

URL フィルタをテストするには

1. IWSS Web コンソールを開き、[HTTP] [設定] [カスタムカテゴリ] の順に選択し、次の URL 用の新しいカテゴリ「監視」を作成します。

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

2. [HTTP] [URL フィルタ] [ポリシー] の順に選択し、[URL フィルタを有効にする] をオンにし、[URL フィルタのグローバルポリシー] 名をクリックしてポリシーにアクセスし、編集します。

注意： 時間オブジェクトは、[管理] [一般設定] [予約期間] で作成します。

3. カスタムカテゴリ [監視] とカテゴリ [コミュニケーション / メディア] > [検索エンジン / ポータル] のチェックボックスをオンにして、[監視] を選択して適用をクリックします。



図 13-9. URL 監視のテストのための [ルール] 画面の設定

4. このポリシーを保存して配信します。
5. クライアントコンピュータから次の Web サイトにアクセスします。

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

<http://www.google.com>

<http://www.yahoo.com>

これで、警告メッセージが表示されずに Web サイトにアクセスできるようになるはずですが。URL フィルタログをクエリおよび表示するには、IWSS Web コンソールにアクセスして [ログ] [ログ分析] [ポリシー施行] の順に選択します。

ダウンロード検索のテスト

HTTP または FTP over HTTP を使用したダウンロード時のウイルス検索をテストするには、次の Web サイトからテストウイルスをダウンロードします。

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

Trend Micro InterScan Web Security イベント



Trend Micro InterScan Web Security Suite: iwss65.jp78

図 13-10. システムが正しくセットアップされている場合に表示されるウイルス警告画面

クライアントが感染ファイルをダウンロードしようとする時、IWSS は初期設定で、そのサイトへの他のユーザのアクセスを 4 時間ブロックします。その後も、他のクライアントがウイルスを含む同じ URL にアクセスしようとする時、ウイルス警告メッセージではなく、URL ブロックメッセージが表示されます。

初期設定のブロック期間 (時間単位) を設定するには、`/etc/iscan/intscan.ini` ファイルの `[Scan-configuration]` セクションにあるパラメータ `infected_url_block_length` を変更して、`/etc/iscan/S99ISproxy stop` および `/etc/iscan/S99ISproxy start` を実行します。

自動 URL ブロックを無効にするには、`/etc/iscan/intscan.ini` ファイルの `[Scan-configuration]` セクションにあるパラメータ `disable_infected_url_block` を変更して、`/etc/iscan/S99ISproxy stop` および `/etc/iscan/S99ISproxy start` を実行します。

`disable_infected_url_block` パラメータについて

no: 自動 URL ブロックを有効にする

yes: 自動 URL ブロックを無効にする

注意: セキュリティレベルが低下するため、この機能は無効にしないことをお勧めします。

URL フィルタのテスト

URL フィルタをテストする場合は、初期設定を使用することをお勧めします。

URL フィルタをテストするには

1. 管理コンソールから [HTTP] [URL フィルタ] [ポリシー] の順に選択します。
2. [URL フィルタを有効にする] を有効にしてから [保存] をクリックします。
3. [URL フィルタのグローバルポリシー] をクリックして、ブロックするカテゴリに適用するブロック処理を選択します。
[安全な検索エンジン] および [除外] タブの初期設定をそのまま受け入れます。
4. [保存] をクリックして変更を保存します。[ポリシーの配信] をクリックして、ポリシーをただちに有効にします。
5. ブラウザを開いて、ブロックするように指定したサイトにアクセスします。IWSS は、ブロックされるように設定されているカテゴリに属する URL へのアクセスをブロックします。

スパイウェア検索のテスト

スパイウェア検索をテストするには

1. [HTTP] [高度な脅威保護] [ポリシー]の順に選択します。
2. [ウイルス検索のグローバルポリシー]をクリックします。
3. [スパイウェア検索ルール] タブをクリックし、検索対象のスパイウェア / 不正プログラムの種類を選択します。
4. [保存] をクリックします。
5. [ウイルス検索のグローバルポリシー] をクリックします。
6. [処理] タブをクリックします。
7. [2次処理] フィールドで、削除、隔離、放置から処理設定を選択します。
8. [保存] をクリックします。
9. [ポリシーの配信] をクリックして、ポリシーをただちに有効にします。

スパイウェアの検出が正常に機能していれば、例に示すようなメッセージが表示されます。

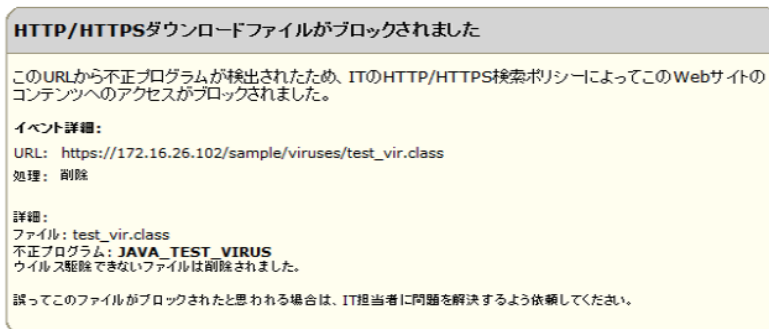


図 13-11. 設定の「削除」処理を伴うスパイウェアを検出後のメッセージ例

その他の IWSS の設定

本項では、IWSS の一般的な設定タスクについて簡単に説明します。

高度な脅威保護検索の指定

高度な脅威保護検索は、初期設定で有効になっています。クライアントが Web を閲覧したり、その他の HTTP 処理を実行するための HTTP トラフィックフローを有効 / 無効にすることができます (88 ページの「HTTP/HTTPS トラフィックフローの有効化」を参照)。

ユーザの識別方法の指定

IWSS では、ポリシーの範囲を設定するときにクライアントを識別する方法を複数サポートしています (108 ページの「ユーザ識別方法の設定」を参照)。初期設定の識別方法は、クライアントの IP アドレスを経由する方法です。また、IWSS では、ホスト名や MAC アドレスを経由してクライアントを識別することも、LDAP ディレクトリを経由してクライアントを識別することもできます。

ゲストアカウントの有効化 (LDAP のみ)

ユーザ / グループ名認証による識別方法を使用する場合、HTTPS 復号化、HTTP ウイルス検索、HTTP 検査、情報漏えい対策、URL フィルタ、およびアクセス割り当てのポリシーで、一時的にネットワークにアクセスするユーザ向けのポリシー設定がサポートされます。ゲストアカウントは、初期設定で無効になっています。ゲストアカウントのインターネットへのアクセスを許可する場合はこのアカウントを有効にします。ゲストアカウントを有効にするには、IWSS をユーザ / グループ名認証 (LDAP) 対応として設定する必要があります。

ゲストアカウントを有効にするには

1. ゲストアカウントを有効にするには、[管理] [一般設定] [ユーザの識別] タブに移動します。
2. [認証方法] で、[キャプティブポータル] を選択し、[ゲストログインの許可] をオンにして [保存] をクリックします。

検索ポリシーとフィルタポリシーの見直し

IWSS は、基本的なゲートウェイセキュリティを提供するように事前設定されています。HTTP ウィルス検索のグローバルポリシーとゲストポリシーの設定を見直して、組織のセキュリティポリシーを反映しているかどうかを確認することをお勧めします。

また、URL フィルタモジュール、および FTP 検索モジュールを実行している場合、これらの設定を見直して必要に応じて変更してください。

アクセス割り当てポリシーの有効化

帯域幅の使用を制限するには、アクセスの割り当て管理を有効にして、クライアントが指定された期間内に取得またはダウンロードできるデータ量の上限を設定します。

アクセス割り当て管理を有効にするには

1. 管理コンソールから [HTTP] [アクセス割り当てポリシー] の順に選択します。
2. [アクセス割り当てを有効にする] チェックボックスをオンにします。
3. ネットワークのゲストユーザに対するアクセス割り当て管理を設定するには、[アクセス割り当てポリシー] をクリックして設定値を指定します。その他のネットワークユーザに対してアクセス割り当て制御を設定するには、[追加] をクリックして新しいポリシーを設定します。
4. [保存] をクリックします。

新しいポリシーをただちに有効にするために、[HTTP] [アクセス割り当てポリシー] 画面で [ポリシーの配信] をクリックします。

インターネットアクセス管理の設定

IWSS の初期設定では、ゲストクライアント以外のクライアントはインターネットアクセスが許可されます。一部のクライアントに対してインターネットアクセスを許可するには、[アクセス管理設定] 画面で対象のクライアントの IP アドレスを設定します。

また、信頼するサイトへのアクセス時の閲覧パフォーマンスを高めるために、IWSS では、一部のサーバを検索から除外するように設定できます。たとえば、イントラネットサイトの IP アドレス範囲をサーバ IP の除外リストに追加して、頻繁にアクセスされるサイトを検索とフィルタから除外することを検討します。

インターネットアクセスを許可するクライアントを設定するには

1. 管理コンソールで [HTTP] [設定] [アクセス管理の設定] の順に選択します。
2. [クライアント IP] タブで [クライアント IP に基づく HTTP アクセス管理を有効にする] を選択して、インターネットアクセスを許可する IP アドレス / ホスト名を入力します。
3. 簡単な説明を入力します。
4. [追加] をクリックします。
5. [保存] をクリックします。

フィルタと検索から除外するサーバを設定するには

1. 管理コンソールで [HTTP] [設定] [アクセス管理の設定] の順に選択します。
2. [サーバ IP の除外リスト] タブをクリックし、HTTP 検索、URL フィルタ、および URL ブロックから除外するサーバの IP アドレスを設定します。
3. 簡単な説明を入力します。
4. [追加] をクリックします。
5. [保存] をクリックします。

アプリケーションパッチの適用またはアプリケーションパッチの削除

トレンドマイクロのダウンロードサイトで、アップデートを入手できます。最新のアップデートをダウンロードサイトからデスクトップまたはその他のコンピュータにダウンロードしたら、それを IWSS デバイスにアップロードすれば自動的にインストールされます。

アプリケーションパッチを適用するには

1. https://www.trendmicro.com/ja_jp/business/products/downloads.html から最新のアップデートをダウンロードします。
2. 管理コンソールで [管理] [システムアップデート] の順に選択してから、[参照] ボタンをクリックします。
3. トレンドマイクロのダウンロードサイトからダウンロードしたアップデートを検索します。
4. [アップロード] をクリックすると、IWSS がアップデートを IWSS デバイスにコピーし、インストールを開始します。

このユーティリティでは、正しくフォーマットされ暗号化されたトレンドマイクロの Patch のみアップロードできます。

アプリケーションパッチを削除するには

1. 管理コンソールから [管理] [システムアップデート] の順に選択します。
2. [履歴] で [アプリケーションのパッチ] タブをクリックします。
3. アプリケーションパッチ番号の横にある [アンインストール] リンクをクリックします。
4. 表示されたプレビュー画面で、アンインストールするパッチのバージョンを確認します。
インストール済みの最も新しいアプリケーションパッチはいつでもアンインストールできます。
5. [アンインストール] をクリックします。進行ステータス画面が表示されます。パッチがアンインストールされると、ウィンドウが閉じ、IWSS コンソールのメイン画面に戻ります。

HotFix、Patch、および Service Pack について

トレンドマイクロでは、公式の製品リリース後に、問題を解決したり、製品のパフォーマンスを向上させたり、新しい機能を追加するために、HotFix、Patch、および Service Pack を提供することがあります。

トレンドマイクロによりリリースされるアイテムを次に示します。

- HotFix お客さまから報告された単独の問題に対する次善策または解決策。HotFix は、問題固有であるため、すべてのお客さまにリリースされるわけではありません。Windows の HotFix には、セットアッププログラムが含まれています。
- Critical Patch/Security Patch 至急対策の必要がある問題のみを修正する目的で一般公開されるプログラムです。特定の問題を修正するプログラムであるため、基本的に、他の修正は含まれませんが、同時期に発見された問題に対する複数の修正が含まれる場合があります。一般公開時期に応じて、後述の Patch に統合されます。
- Patch 複数のプログラム上の問題を解決する HotFix と Security Patch のグループ。トレンドマイクロでは定期的に Patch を提供しています。
- Service Pack HotFix、Patch、および機能強化を組み合わせたもので、製品のアップグレードに相当します。

Patch や Service Pack は、次のトレンドマイクロの Web サイトを定期的にチェックしてダウンロードしてください。

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

すべてのリリースには、対象製品のインストール、展開、および設定に必要な情報を含む Readme ファイルが付属しています。HotFix、Patch、または Service Pack ファイルをインストールする前に、Readme ファイルを読んでください。

データベース接続の確認

データベース接続設定を確認するには

1. [管理] [一般設定] [データベース接続] の順に選択します。
2. [ポリシーデータベースの接続設定] でデータベース設定を確認します。
3. [データベース接続のテスト] をクリックします。

ポリシー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、時間間隔を指定する [ポリシー配信設定 (分)] オプション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。

[ポリシー配信設定 (分)] を設定するには

1. IWSS Web コンソールを開き、[管理] [一般設定] [ポリシー配信] 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
 - ・ HTTPS ポリシー
 - ・ HTTP 検査ポリシー
 - ・ URL フィルタポリシー
 - ・ アクセス割り当てポリシー
 - ・ アプリケーション制御ポリシー
 - ・ 情報漏えい対策ポリシー
3. [保存] をクリックします。

管理コンソールパスワードの変更

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

Web コンソールパスワードを変更するには

1. IWSS コンソールを開いて、管理コンソールで [管理] [管理コンソール] [アカウント管理] の順に選択します。
2. パスワードを変更するユーザアカウントをクリックします。
3. [ログインアカウント] 画面で、[パスワード] に新しいパスワードを入力してから、[パスワードの確認入力] にもう一度同じパスワードを入力します。

4. [保存] をクリックします。

管理コンソールの待機ポート変更後の設定

ユーザが [管理] [Web コンソール] 画面にアクセスして、SSL モード用のポート番号を他のアプリケーションで使用されていないポート (8443 など) に設定することで HTTPS Web コンソールの管理モードを有効にする場合、[HTTP] [設定] [アクセス管理の設定] 画面でもこの SSL 管理ポート番号を指定する必要があります。

[アクセス管理設定] 画面でこのポート番号が指定されていないと、HTTPS Web コンソールを使用する際、IWSS によって IWSS 進行ステータス画面が自動的にブロックされます。つまり、クライアントが URL にアクセスしようとすると、IWSS によってブロックされた進行ステータスバーが表示されます。

URL フィルタ設定の確認

URL フィルタモジュールを実行している場合、設置後のタスクを見直して IWSS を環境に合わせて調整します。

IWSS では、「ギャンブル」、「ゲーム」、「出会い系」など 80 を超えるカテゴリに属する URL を格納する Web レピュテーションデータベースにアクセスできます。これらのカテゴリは論理グループに含まれます。

トレンドマイクロでは、URL フィルタ設定を見直すことをお勧めします。それにより、社内で禁止サイトと見なすカテゴリが、組織の価値を反映しており、従業員が業務で使用する Web 閲覧に支障がないか確認してください。URL フィルタポリシーを適用する前に、初期設定の分類が組織に対して適切かどうか確認することをお勧めします。たとえば、衣料販売業者は、正当な市場調査や競合他社の調査ができるように、「アダルト」グループに分類された「下着 / 水着」カテゴリから水着の Web サイトを除外する必要がある場合があります。

また、除外 URL を設定して、本来はブロックすべき特定のサイトへの従業員のアクセスを有効にしたり、「業務時間」の定義を見直して、職場のスケジュールを反映したりする必要がある場合もあります。

URL フィルタ設定を見直すには

1. 管理コンソールから [HTTP] [URL フィルタ] [ポリシー] [<ポリシー名>] [除外設定] の順に選択します。
2. URL フィルタから除外する Web サイトを含む除外 URL リストをドロップダウンリストから選択して、これらの Web サイトにクライアントから常にアクセスができるようにします。

3. [保存] をクリックします。
4. 管理コンソールで、[管理] [一般設定] [予約期間] をクリックします。

注意：「業務時間」の初期設定は、月曜から金曜の 8 時から 12 時 00 分までと 13 時から 17 時までになっています。

5. 職場の従業員のスケジュールに応じてこれらの時間設定を変更します。
6. 管理コンソールで [HTTP] [URL フィルタ] [ポリシー] の順に選択して、URL フィルタのゲストポリシーとグローバルポリシーのカテゴリ設定を見直します。

IWSS パフォーマンスの調整

閲覧パフォーマンスが遅くて困る場合は、本項で説明する変更内容を検討してください。

LDAP パフォーマンスの調整

ユーザ / グループ名認証による識別方法 (LDAP) を使用する IWSS を実行する場合、HTTP プロキシのパフォーマンスは、LDAP ディレクトリサーバの応答に依存します。最悪の場合、HTTP 要求ごとに、ユーザ認証を求める LDAP クエリや、対象ユーザのグループメンバーシップ情報の取得を求める別の LDAP クエリが必要になります。こうしたクエリによって、IWSS と LDAP サーバ間の送受信に遅延が発生し、LDAP サーバ自体の負荷が増大します。

LDAP の内部キャッシュ

必要な LDAP クエリ量を減らすために、IWSS は複数の内部キャッシュを提供しています。

- ・ ユーザグループメンバーシップキャッシュ ユーザグループメンバーシップ用キャッシュには、数百人のユーザのグループメンバーシップ情報を格納できます。このキャッシュ内のエントリの同期間隔は、`/etc/iscan/commonldap/LdapSetting.ini` ファイルの `LDAP_Setting` にあるパラメータ `SyncInterval` で設定できます。初期設定値は 1440 (24 時間) です。0 を設定すると同期は無効になります。
- ・ クライアント IP アドレスとユーザ ID 間のキャッシュ このキャッシュは、クライアント IP アドレスと同じ IP アドレスで最近認証されたユーザを関連付けます。過去に認証された要求と同じ IP アドレスから発行された要求は、新しい要求が設定可能な期間内 (初期設定で HTTP の場合は 15 分、ICAP の場合は 90 分) に認証から発行された場合であれば、同じユーザのものであると見なされます。その期間中、IWSS が認識するクライアント IP アドレスはユーザごとに

一意でなければなりません。したがって、このキャッシュは、クライアントと IWSS の間にプロキシサーバやソース NAT が存在する環境や DHCP が頻繁にクライアント IP アドレスを再割り当てする環境では使用できません。このキャッシュを有効 / 無効にするには、`/etc/iscan/intscan.ini` 設定ファイルの `[user-identification]` セクションにある `enable_ip_user_cache` 設定を変更します。

- ・ ユーザ認証キャッシュ このキャッシュは、接続中に発行された複数の HTTP 要求の再認証を回避します。接続中にユーザの認証情報が確認されると、IWSS はユーザ認証キャッシュにエントリ (1 つのキャッシュエントリ内の 2 つの重要な鍵はクライアントの IP アドレスとユーザ名) を追加して、接続中に次の要求が来ても再認証しないようにします。クライアントの IP アドレスとユーザ名は、それぞれ「クライアント IP アドレスとユーザ ID 間のキャッシュ」と「ユーザグループメンバーシップキャッシュ」に対する前方参照またはリンクとしての役割を果たします。つまり、IWSS はユーザの接続情報を IP アドレスとユーザ ID のキャッシュおよびユーザグループキャッシュの両方から取得できます。このキャッシュを有効 / 無効にするには、`/etc/iscan/intscan.ini` 設定ファイルの `[user-identification]` セクションにある `enable_ip_user_cache` 設定を変更します。このキャッシュの生存期限 (TTL) を変更するには、`/etc/iscan/commonldap/LdapCache.ini` 設定ファイルの `expire_interval` を変更します (秒単位)。初期設定値は 7200 (2 時間) です。

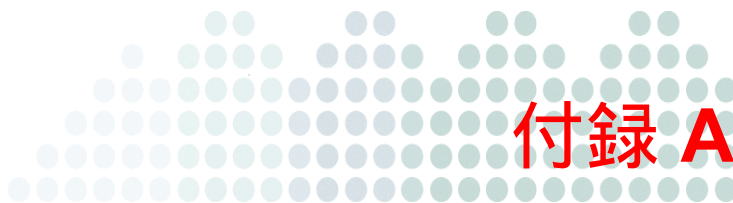
IWSS を LDAP と連携して展開する場合、HTTP 要求の認証により LDAP ディレクトリサーバに課せられる追加の負荷を考慮する必要があります。クライアント IP アドレスとユーザ ID 間のキャッシュを効果的に使用できない環境では、IWSS が HTTP 要求を受信する速度と同じ速度でディレクトリサーバがクエリを処理できる必要があります。

LDAP が有効な場合の冗長ログの無効化

LDAP が有効になっている場合、サーバのパフォーマンスを考慮して、

`/etc/iscan/intscan.ini` ファイルの `[http]` セクションにある「verbose」パラメータで冗長ログをオフにすることをお勧めします。本来、冗長ログは、ソフトウェア開発者が、異常なアプリケーション動作の特定やトラブルシューティングに使用します。製品展開では、通常、冗長ログは必要ありません。

冗長ログと LDAP がともに有効になっている場合は、IWSS が、ユーザ認証情報とグループメンバーシップ情報を Log フォルダ内の HTTP ログに記録します。ログには、ユーザごとに何百行もの情報が含まれるため、内部トラフィック量やユーザが属しているグループ数によっては、大量のハードディスク容量が必要になる場合があります。冗長ログは、OS に対して I/O 処理を要求することによって、サービスをビジー状態にします。これにより、サービスが HTTP 要求にタイムリーに応答できなくなり、その結果、遅延が発生する場合があります。極端に HTTP トラフィックが集中する環境では、IWSS を冗長モードで起動した場合に大きな遅延が発生します。



サポート情報

本付録では、InterScan Web Security Suite (以下、IWSS) のパフォーマンスを最適化し、技術的な問題に関するさらなる支援を受けるための情報を提供します。

本付録で説明する内容には、次の項目が含まれます。

- ・ 318 ページの「トラブルシューティングのリソース」
- ・ 319 ページの「製品サポート情報」
- ・ 319 ページの「サポートサービスについて」
- ・ 320 ページの「セキュリティニュース」
- ・ 321 ページの「その他のリソース」
- ・ 322 ページの「脅威解析・サポートセンター TrendLabs (トレンドラボ)」

トラブルシューティングのリソース

トレンドマイクロでは以下のオンラインリソースを提供しています。テクニカルサポートに問い合わせる前に、こちらのサイトも参考にしてください。

サポートポータルの利用

サポートポータルでは、よく寄せられるお問い合わせや、障害発生時の参考となる情報、リリース後に更新された製品情報などを提供しています。

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

脅威データベース

現在、不正プログラムの多くは、コンピュータのセキュリティプロトコルを回避するために、2つ以上の技術を組み合わせた複合型脅威で構成されています。トレンドマイクロは、カスタマイズされた防御戦略を策定した製品で、この複雑な不正プログラムに対抗します。脅威データベースは、既知の不正プログラム、スパム、悪意のある URL、および既知の脆弱性など、さまざまな混合型脅威の名前や兆候を包括的に提供します。

詳細については、<https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/> をご覧ください。

- ・ 現在アクティブまたは「in the Wild」と呼ばれている生きた不正プログラムと悪意のあるモバイルコード
- ・ これまでの Web 攻撃の記録を記載した、相関性のある脅威の情報ページ
- ・ 対象となる攻撃やセキュリティの脅威に関するオンライン勧告
- ・ Web 攻撃およびオンラインのトレンド情報
- ・ 不正プログラムの週次レポート

製品サポート情報

製品のユーザ登録により、さまざまなサポートサービスを受けることができます。

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

サポートサービスについて

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

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

サポート契約の有効期限は、ユーザ登録完了から 1 年間です（ライセンス形態によって異なる場合があります）。契約を更新しないと、パターンファイルや検索エンジンの更新などのサポートサービスが受けられなくなりますので、サポートサービス継続を希望される場合は契約満了前に必ず更新してください。更新手続きの詳細は、トレンドマイクロの営業部、または販売代理店までお問い合わせください。

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

セキュリティニュース

トレンドマイクロ「セキュリティニュース」

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

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

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

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

トレンドマイクロへのウイルス解析依頼

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

ファイルを送信いただく前に、トレンドマイクロの不正プログラム情報検索サイト「脅威データベース」にアクセスして、ウイルスを特定できる情報がないかどうか確認してください。

<https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/>

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

<https://success.trendmicro.com/dcx/s/threat?language=ja>

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

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

メールレピュテーションについて

スパムメールやフィッシングメールなどの送信元を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

ファイルレピュテーションについて

不正プログラムなどのファイル情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

Web レピュテーションについて

不正な Web サイトや URL などの情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

その他のリソース

製品やサービスについてのその他の情報として、次のようなものがあります。

最新版ダウンロード

製品やドキュメントの最新版は、次の Web ページからダウンロードできます。

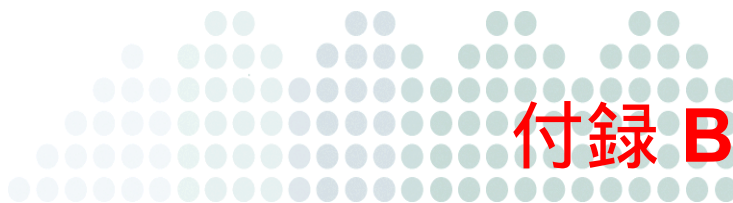
<http://downloadcenter.trendmicro.com/index.php?regs=jp>

注意： サービス製品、販売代理店経由での販売製品、または異なる提供形態をとる製品など、一部対象外の製品があります。

脅威解析・サポートセンター TrendLabs (トレンドラボ)

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

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



ファイルタイプと MIME コンテンツタイプの の対応

次の表は、対応する MIME コンテンツタイプの検索を省略するために、HTTP ウイルス検索ポリシーの [検索を省略する MIME コンテントタイプ] フィールドに入力できるファイルタイプを示しています。

- ・ 324 ページの「概要」
- ・ 326 ページの「MIME コンテンツファイルのファイルタイプマッピングテーブル」

概要

MIME 名は表 B-1 に限定されているわけではありません。つまり、IWSS UI 除外リストには任意の名前を入力できます (詳細については、164 ページの「検索するファイルタイプを選択するには」を参照してください)。ただし、次の依存関係がある場合には、検索を省略できるのは MIME タイプのみです。

InterScan Web Security Suite (以下、IWSS) はファイルを受信すると、次の点を判別します。

- MIME 名が UI で検索を省略するように設定されているか
- ファイルタイプ (MIME 名ではなく) がマッピングテーブルにリストされているか
- MIME 名がマッピングテーブルにリストされている場合、MIME 名は UI 除外リストに含まれているか

IWSS は一致を見つけると、検索を省略します。IWSS で一致を見つけないことができなかった場合、検索は省略されません。

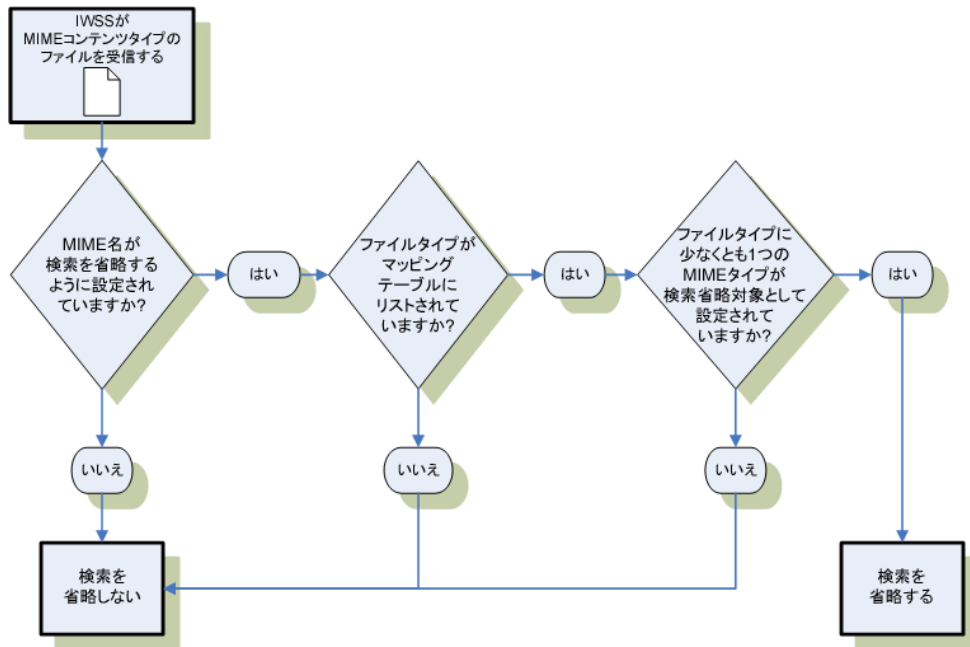


図 B-1. 検索が省略されるファイルの MIME コンテンツタイプのフロー

管理者が MIME 名を入力し、IWSS にとってそのファイルタイプが不明の場合、そのファイルの検索は省略されます。MIME タイプが IWSS で検索を省略するように設定されており、ファイルタイプ-MIME テーブルに存在しない場合は、検索は省略されます。これは、ファイルタイプ-MIME テーブルで、すべての可能なファイルタイプについてすべての可能な MIME タイプをリストすることができないからです。

1 つのファイルタイプに対して少なくとも 1 つの MIME タイプが検索省略対象として設定されている場合も、検索は省略されます。MIME 名が標準というわけではないからです。ファイルタイプ-MIME テーブルで、既知のファイルタイプに対するすべての MIME タイプをリストすることはできません。

たとえば、ファイルタイプ-MIME テーブルには FLV ファイルのマッピングとして、video/flv と video/x-flv が含まれていますが、「application/flv」は含まれていません。ただし、一部の Web サイトは「application/flv」を使用しています。IWSS は該当するマッピングエントリを見つけることはできませんが、ファイルタイプのチェックを実行して、これが FLV ファイルであることを認識します。このファイルの検索は省略されます。

管理者が「video/flv」と「application/flv」を除外リストに入力している場合は、次のチェックが実行されます。

- ・ MIME 名が検索を省略するように設定されている (MIME タイプ: application/flv) > はい >
- ・ ファイルタイプがマッピングテーブルにリストされているかどうかチェックする (ファイルタイプ: flv) > ある >
- ・ ファイルタイプに少なくとも 1 つの MIME タイプが検索省略対象として設定されている > はい > 検索を省略する

MIME コンテンツファイルのファイルタイプマッピングテーブル

表 B-1. MIME コンテンツファイルのファイルタイプマッピングテーブル

ファイルタイプ	MIME コンテンツタイプ
ACE 圧縮ファイル	application/x-ace
ACE 圧縮ファイル	application/x-compressed
Apple サウンド	audio/aiff
Apple サウンド	audio/x-aiff
Apple/SGI の Audio InterChange File Format (以下、AIFF)	audio/aiff
Apple/SGI の Audio InterChange File Format (以下、AIFF)	audio/x-aiff
Apple/SGI の AIFF	sound/aiff
Apple/SGI の AIFF	audio/rmf
Apple/SGI の AIFF	audio/x-rmf
Apple/SGI の AIFF	audio/x-pn-aiff
Apple/SGI の AIFF	audio/x-gsm
Apple/SGI の AIFF	audio/x-midi
Apple/SGI の AIFF	audio/vnd.qcelp
ARJ	application/arj
ARJ	application/x-arj
ARJ	application/x-compress
ARJ	application/x-compressed
ARJ	zz-application/zz-winassoc-arj
Advanced Systems Format (以下、ASF)	video/x-ms-asf

表 B-1. MIME コンテンツファイルのファイルタイプマッピングテーブル (続き)

ファイルタイプ	MIME コンテンツタイプ
ASF	video/x-ms-asf-plugin
ASF	video/x-ms-wm
ASF	video/x-ms-wmx
ASF	audio/asf
ASF	application/asx
ASF	application/x-mplayer2
ASF	application/vnd.ms-as"
Nullsoft AVS	video/avs-video
Mime Base 64	application/base64
Macintosh MacBinary アーカイブ	application/mac-binary
Macintosh MacBinary アーカイブ	application/macbinary
Macintosh MacBinary アーカイブ	application/octet-stream
Macintosh MacBinary アーカイブ	application/x-binary
Macintosh MacBinary アーカイブ	application/x-macbinary
BINHEX	application/binhex
BINHEX	application/binhex4
BINHEX	application/mac-binhex
BINHEX	application/mac-binhex40
BINHEX	application/x-binhex40
Windows BMP	image/bmp
Windows BMP	image/x-bmp

表 B-1. MIME コンテンツファイルのファイルタイプマッピングテーブル (続き)

ファイルタイプ	MIME コンテンツタイプ
Windows BMP	image/x-bitmap
Windows BMP	image/x-xbitmap
Windows BMP	image/x-win-bitmap
Windows BMP	image/x-windows-bmp
Windows BMP	image/ms-bmp
Windows BMP	image/x-ms-bmp
SGI イメージ	image/x-sgi-bw
GNU BZIP2	application/x-bzip2
GNU BZIP3	application/bzip2
GNU BZIP4	application/x-bz2
GNU BZIP5	application/x-compressed
Computer Graphics Metafiles	image/cgm
COM	application/octet-stream
COM	application/x-msdos-program
COM	application/x-msdownload
UNIX cpio アーカイブ	application/x-cpio
Adobe Director Shockwave Movie	application/x-director
WordPerfect	application/wordperfect
AutoCAD DWG	application/acad
AutoCAD DWG	application/x-acad
AutoCAD DWG	drawing/x-dwg

表 B-1. MIME コンテンツファイルのファイルタイプマッピングテーブル (続き)

ファイルタイプ	MIME コンテンツタイプ
AutoCAD DWG	image/vnd.dwg
AutoCAD DWG	image/x-dwg
Encapsulated Postscript (以下、EPS)	application/postscript
EPS	image/x-eps
EPS	image/eps
EPS	application/x-eps
EPS	application/eps
EXE	application/octet-stream
EXE	application/exe
EXE	application/x-msdownload
EXE	application/x-exe
EXE	application/dos-exe
EXE	vms/exe
EXE	application/x-winexe
EXE	application/msdos-windows
FreeHand ドキュメント	image/x-freehand
AutoDesk Animator (FLI または FLC)	video/x-fli
AutoDesk Animator (FLI または FLC)	video/flc
AutoDesk Animator (FLI または FLC)	video/fli
AutoDesk Animator (FLI または FLC)	video/x-acad-anim
Adobe Flash FLV ビデオ	video/flv

表 B-1. MIME コンテンツファイルのファイルタイプマッピングテーブル (続き)

ファイルタイプ	MIME コンテンツタイプ
Adobe Flash FLV ビデオ	video/x-flv
Adobe Flash FLV ビデオ	flv-application/octet-stream
Frame Maker	application/vnd.framemaker
GIF	image/gif
GNU ZIP	application/gzip
GNU ZIP	application/x-gzip
GNU ZIP	application/x-gunzip
GNU ZIP	application/gzipped
GNU ZIP	application/gzip-compressed
GNU ZIP	application/x-compressed
GNU ZIP	application/x-compress
GNU ZIP	gzip/document
GNU ZIP	encoding/x-gzip
Windows アイコン	image/ico
Windows アイコン	image/x-icon
Windows アイコン	application/ico
Windows アイコン	application/x-ico
Windows アイコン	application/x-win-bitmap
Windows アイコン	image/x-win-bitmap
Amiga 8SVX Audio Interchange File Format (以下、AIFF)	audio/x-aiff

表 B-1. MIME コンテンツファイルのファイルタイプマッピングテーブル (続き)

ファイルタイプ	MIME コンテンツタイプ
Amiga 9SVX AIFF	image/iff
Amiga 10SVX AIFF	image/x-iff
Amiga 11SVX AIFF	application/iff
JAVA アプレット	text/x-java-source
JAVA アプレット	application/java-class
JAVA アプレット	application/x-java-applet
JAVA アプレット	application/x-java-vm
JPEG	image/jpeg
JPEG	image/jpg
JPEG	image/jp_
JPEG	image/pipeg
JPEG	image/pjpeg
LHA	application/x-lha
LHA	application/lha
LHA	application/x-compress
LHA	application/x-compressed
LHA	application/mac1ha
Compiled LISP	application/x-lisp
NT/95 ショートカット (*.lnk)	application/x-ms-shortcut
LightWave 3D オブジェクト	image/x-lwo
MAUD Sample Format	audio/x-maud

表 B-1. MIME コンテンツファイルのファイルタイプマッピングテーブル (続き)

ファイルタイプ	MIME コンテンツタイプ
Microsoft Document Imaging	image/vnd.ms-modi
MIDI	audio/midi
Magick Image File Format (MIFF)	application/x-mif
Multi-image Network Graphics	video/x-mng
Multi-image Network Graphics	video/mng
MP3	audio/mpeg
MP3	audio/mpeg3
MP3	audio/x-mpeg-3
MPEG	video/mpeg
MPEG	video/mpg
MPEG	video/x-mpg
MPEG	video/mpeg2
MPEG	video/x-mpeg
MPEG	video/x-mpeg2a
Microsoft Cabinet	application/x-cabinet-win32-x86
Windows Word	application/msword
Windows Word	application/doc
Windows Word	application/vnd.msword
Windows Word	application/vnd.ms-word
Windows Word	application/x-msw6
Windows Word	application/x-msword

表 B-1. MIME コンテンツファイルのファイルタイプマッピングテーブル (続き)

ファイルタイプ	MIME コンテンツタイプ
Windows Excel	application/excel
Windows Excel	application/x-msexcel
Windows Excel	application/x-ms-excel
Windows Excel	application/x-excel
Windows Excel	application/vnd.ms-excel
Windows Excel	application/xls
Windows Excel	application/x-xls
Windows Installer	application/x-ole-storage
Microsoft Access (MDB)	application/x-msaccess
Microsoft Access (MDB)	application/msaccess
Microsoft Access (MDB)	application/vnd.msaccess
Microsoft Access (MDB)	application/vnd.ms-access
Microsoft Access (MDB)	application/mdb
Microsoft Access (MDB)	application/x-mdb
Microsoft Access (MDB)	zz-application/zz-winassoc-mdb
Microsoft Office 12	application/vnd.ms-word.document.macroEnabled.12
Microsoft Office 12	application/vnd.openxmlformats-officedocument.wordprocessingml.document
Microsoft Office 12	application/vnd.ms-word.template.macroEnabled.12
Microsoft Office 12	application/vnd.openxmlformats-officedocument.wordprocessingml.template

表 B-1. MIME コンテンツファイルのファイルタイプマッピングテーブル (続き)

ファイルタイプ	MIME コンテンツタイプ
Microsoft Office 12	application/vnd.ms-powerpoint.template.macroEnabled.12
Microsoft Office 12	application/vnd.openxmlformats-officedocument.presentationml.template
Microsoft Office 12	application/vnd.ms-powerpoint.addin.macroEnabled.12
Microsoft Office 12	application/vnd.ms-powerpoint.slideshow.macroEnabled.12
Microsoft Office 12	application/vnd.openxmlformats-officedocument.presentationml.slideshow
Microsoft Office 12	application/vnd.ms-powerpoint.presentation.macroEnabled.12
Microsoft Office 12	application/vnd.openxmlformats-officedocument.presentationml.presentation
Microsoft Office 12	application/vnd.ms-excel.addin.macroEnabled.12
Microsoft Office 12	application/vnd.ms-excel.sheet.binary.macroEnabled.12
Microsoft Office 12	application/vnd.ms-excel.sheet.macroEnabled.12
Microsoft Office 12	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
Microsoft Office 12	application/vnd.ms-excel.template.macroEnabled.12
Microsoft Office 12	application/vnd.openxmlformats-officedocument.spreadsheetml.template
Microsoft Office 12	application/vnd.openxmlformats

表 B-1. MIME コンテンツファイルのファイルタイプマッピングテーブル (続き)

ファイルタイプ	MIME コンテンツタイプ
Windows PowerPoint	application/mspowerpoint
Windows PowerPoint	application/powerpoint
Windows PowerPoint	application/vnd.ms-powerpoint
Windows PowerPoint	application/ms-powerpoint
Windows PowerPoint	application/mspowerpnt
Windows PowerPoint	application/vnd-mspowerpoint
Windows PowerPoint	application/x-powerpoint
Windows PowerPoint	application/x-mspowerpoint
Windows Project	application/vnd.ms-project
Windows Project	application/x-msproject
Windows Project	application/x-project
Windows Project	application/msproj
Windows Project	application/msproject
Windows Project	application/x-ms-project
Windows Project	application/x-dos_ms_project
Windows Project	application/mpp
Windows Project	zz-application/zz-winassoc-mpp
Windows Write	application/mswrite
Windows Write	application/x-mswrite
Windows Write	application/wri
Windows Write	application/x-wri

表 B-1. MIME コンテンツファイルのファイルタイプマッピングテーブル (続き)

ファイルタイプ	MIME コンテンツタイプ
Windows Write	application/msword
Windows Write	application/microsoft_word
Windows Write	zz-application/zz-winassoc-wri
OpenDocument	application/vnd.oasis.opendocument.text
OpenDocument	application/vnd.oasis.opendocument.text-template
OpenDocument	application/vnd.oasis.opendocument.graphics
OpenDocument	application/vnd.oasis.opendocument.graphics-template
OpenDocument	application/vnd.oasis.opendocument.presentation
OpenDocument	application/vnd.oasis.opendocument.presentation-template
OpenDocument	application/vnd.oasis.opendocument.spreadsheet
OpenDocument	application/vnd.oasis.opendocument.spreadsheet-template
OpenDocument	application/vnd.oasis.opendocument.chart
OpenDocument	application/vnd.oasis.opendocument.chart-template
OpenDocument	application/vnd.oasis.opendocument.image
OpenDocument	application/vnd.oasis.opendocument.image-template
OpenDocument	application/vnd.oasis.opendocument.formula

表 B-1. MIME コンテンツファイルのファイルタイプマッピングテーブル (続き)

ファイルタイプ	MIME コンテンツタイプ
OpenDocument	application/vnd.oasis.opendocument.formula-template
OpenDocument	application/vnd.oasis.opendocument.text-master
OpenDocument	application/vnd.oasis.opendocument.text-web
Gravis Patch ファイル	audio/pat
Gravis Patch ファイル	audio/x-pat
Microsoft Paint v1.x	image/x-pcx
Microsoft Paint v1.x	image/pcx
Microsoft Paint v1.x	image/x-pc-paintbrush
Microsoft Paint v1.x	application/x-pcx
Microsoft Paint v1.x	application/pcx
Microsoft Paint v1.x	zz-application/zz-winassoc-pcx
Microsoft Paint v2.x	image/x-pcx
Microsoft Paint v2.x	image/pcx
Microsoft Paint v2.x	image/x-pc-paintbrush
Microsoft Paint v2.x	application/x-pcx
Microsoft Paint v2.x	application/pcx
Microsoft Paint v2.x	zz-application/zz-winassoc-pcx
PCX	image/x-pcx
PCX	image/pcx
PCX	image/x-pc-paintbrush

表 B-1. MIME コンテンツファイルのファイルタイプマッピングテーブル (続き)

ファイルタイプ	MIME コンテンツタイプ
PCX	application/x-pcx
PCX	application/pcx
PCX	zz-application/zz-winassoc-pcx
Palm Pilot Image	application/x-pilot-pdb
Adobe Portable Document Format (PDF)	application/pdf
Adobe PDF	application/x-pdf
Adobe フォントファイル	application/x-font
Macintosh ビットマップ	image/pict
Macintosh ビットマップ	image/x-pict
Portable Network Graphics	image/png
PPM Image	image/x-portable-pixmap
PPM Image	image/x-p
PPM Image	image/x-ppm
PPM Image	application/ppm
PPM Image	application/x-ppm
Postscript	application/postscript
Adobe Photoshop (PSD)	application/octet-stream
Paint Shop Pro	image/bmp
Quick Time Media	video/quicktime
Quick Time Media	video/x-quicktime
Quick Time Media	image/mov

表 B-1. MIME コンテンツファイルのファイルタイプマッピングテーブル (続き)

ファイルタイプ	MIME コンテンツタイプ
Quick Time Media	audio/aiff
Quick Time Media	audio/x-midi
QuarkXPress Document (QXD)	application/quarkxpress
QuarkXPress Document (QXD)	application/x-quark-express
Real Audio	audio/vnd.rn-realaudio
Real Audio	audio/x-pn-realaudio
Real Audio	audio/x-realaudio
Real Audio	audio/x-pm-realaudio-plugin
Real Audio	video/x-pn-realvideo
RAR	application/rar
Sun Raster (RAS)	image/x-cmu-raster
Sun Raster (RAS)	image/cmu-raster
Real Media	application/vnd.rn-realmedia
Microsoft RTF	application/rtf
Microsoft RTF	application/x-rtf
Microsoft RTF	text/richtext
Lotus ScreenCam ムービー	application/vnd.lotus-screencam
Lotus ScreenCam ムービー	application/x-lotusscreencam
Lotus ScreenCam ムービー	application/x-screencam
Lotus ScreenCam ムービー	video/x-scm
Lotus ScreenCam ムービー	video/x-screencam

表 B-1. MIME コンテンツファイルのファイルタイプマッピングテーブル (続き)

ファイルタイプ	MIME コンテンツタイプ
IRCAM サウンドファイル	audio/x-sf
Sonic Foundry ファイル	audio/sfr
Adobe Flash	application/x-shockwave-flash
TAR	application/x-tar
TAR	application/tar
TAR	application/x-gtar
TAR	multipart/x-tar
TAR	application/x-compress
TAR	application/x-compressed
Targa Image	image/tga
Targa Image	image/x-tga
Targa Image	image/targa
Targa Image	image/x-targa
TIFF	image/tiff
TNEF ファイル	application/ms-tnef
TNEF ファイル	application/vnd.ms-tne
ASCII テキスト	text/plain
ASCII テキスト	application/txt
ASCII テキスト	text/html
ASCII テキスト	text/css
UUENCODE	text/x-uuencode

表 B-1. MIME コンテンツファイルのファイルタイプマッピングテーブル (続き)

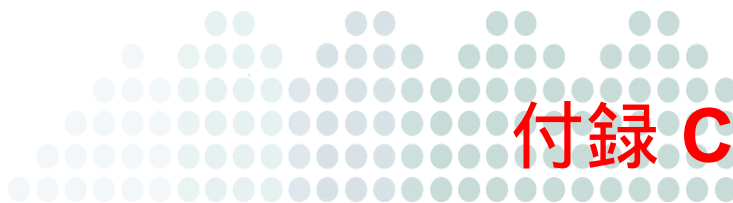
ファイルタイプ	MIME コンテンツタイプ
VBScript	text/vbscript
VBScript	text/vbs
VBScript	application/x-vbs
Creative Voice Format (VOC)	audio/voc
Creative Voice Format (VOC)	audio/x-voc
Microsoft RIFF	audio/wav
Microsoft RIFF	application/x-cdf
Microsoft RIFF	application/x-cmx
Microsoft RIFF	image/x-cmx
Microsoft RIFF	drawing/cmx
Microsoft RIFF	application/cmx
Webshots Picture Collection	application/x-webshots
Webshots Picture Collection	application/wbc
Windows Metafile	application/x-msmetafile
Windows Metafile	application/wmf
Windows Metafile	application/x-wmf
Windows Metafile	image/x-wmf
Windows Metafile	zz-application/zz-winassoc-wmf
PKZIP	application/zip
PKZIP	application/x-zip
PKZIP	application/x-zip-compressed

表 B-1. MIME コンテンツファイルのファイルタイプマッピングテーブル (続き)

ファイルタイプ	MIME コンテンツタイプ
PKZIP	multipart/x-zip
PKZIP	application/x-compress
PKZIP	application/x-compressed
ACE 圧縮ファイル	application/x-ace
ACE 圧縮ファイル	application/x-compressed
Apple サウンド	audio/aiff
Apple サウンド	audio/x-aiff
Apple/SGI の AIFF	audio/aiff
Apple/SGI の AIFF	audio/x-aiff
Apple/SGI の AIFF	sound/aiff
Apple/SGI の AIFF	audio/rmf
Apple/SGI の AIFF	audio/x-rmf
Apple/SGI の AIFF	audio/x-pn-aiff
Apple/SGI の AIFF	audio/x-gsm
Apple/SGI の AIFF	audio/x-midi
Apple/SGI の AIFF	audio/vnd.qcelp
ARJ	application/arj
ARJ	application/x-arj
ARJ	application/x-compress
ARJ	application/x-compressed
ARJ	zz-application/zz-winassoc-arj

表 B-1. MIME コンテンツファイルのファイルタイプマッピングテーブル (続き)

ファイルタイプ	MIME コンテンツタイプ
ASF	video/x-ms-asf
ASF	video/x-ms-asf-plugin
ASF	video/x-ms-wm
ASF	video/x-ms-wmx
ASF	audio/asf
ASF	application/asx
ASF	application/x-mplayer2



アーキテクチャと設定ファイル

本付録で説明する内容には、次の項目が含まれます。

- ・ 346 ページの「モジュールの構成」
- ・ 346 ページの「サービス」
- ・ 348 ページの「予約タスク」
- ・ 350 ページの「設定ファイルについて」
- ・ 351 ページの「プロトコルハンドラ」
- ・ 352 ページの「検索モジュール」

モジュールの構成

InterScan Web Security Suite (以下、IWSS) は次のモジュールで構成されます。

- ・ メインプログラム — Web コンソールと、IWSS に必要な基本ライブラリファイルが含まれます。
- ・ 高度な脅威保護 — ICAP 検索または HTTP 検索のいずれかの HTTP 検索と、URL ブロックに必要なサービスが含まれます。
- ・ アプリケーション制御 — インターネットアプリケーションを自動的に検出し、管理者がポリシーを使用してそれらのアプリケーションを管理できるようにするセキュリティテクノロジーを提供します。
- ・ HTTP 検査 — 管理者は動作を識別して、HTTP メソッド、URL、およびヘッダに基づいて Web トラフィックをフィルタできます。
- ・ 情報漏えい対策 — 有効 / 無効に関係なく、システム上のすべての情報漏えい対策ポリシーが表示されます。
- ・ FTP 検索 — FTP 検索に必要なサービスが含まれます。
- ・ URL フィルタ — Web セキュリティ強化フィルタオプションの機能が含まれます。
- ・ SNMP 通知 — SNMP 対応ネットワーク管理ソフトウェアに SNMP トラップを送信するサービスが含まれます。
- ・ IWSS 用 Control Manager エージェント — Trend Micro Control Manager (以下、Control Manager) からの監視および設定を可能にする Control Manager エージェントに必要なファイルが含まれます。

サービス

ここで示すサービスを開始または停止するには、ローカルターミナルまたは SSH を使用して、`root` として IWSS にログオンする必要があります。88 ページの「HTTP/HTTPS トラフィックフローの有効化」および 214 ページの「FTP トラフィックおよび FTP 検索の有効化」を参照してください。

IWSS で実行されるサービスは次のとおりです。

- ・ Trend Micro IWSS Console (java) — Web コンソールをホストする Web サーバです。
- ・ Trend Micro IWSS 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 IWSS 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。
- 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 (snmpd) — SNMP トラップ通知を SNMP 対応ネットワーク監視デバイスに送信するサービスです。
- Trend Micro Service Monitor (svcmmonitor) — HTTP、FTP、アプリケーション制御、Tomcat、および WMI のデーモンの状態を確認するサービスです。
- Trend Micro Database Service (postgres、postmaster) — IWSS のローカル PostgreSQL データベースを管理するサービスです。このデータベースには、ポリシー設定、レポートログ、および [概要] 画面の統計データが保存されます。
- Trend Micro Authentication Service (AuthDaemon) — iwssd デーモンまたは appd デーモンから認証要求を受け取り、認証結果を返すサービスです。
- Trend Micro Syslog Service (tmsyslogd) — 企業クラスのログ機能を提供し、Syslog イベントを複数の異なるサーバに送信するサービスです。
- Trend Micro Control Manager Service (En_Main) — Control Manager または Apex Central を使用している場合、Control Manager または Apex Central 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 IWSS 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。

表 C-1. IWSS のセットアップ中に作成される予約タスク

タスク	機能	間隔
archive_debug_log.py	デバッグログのアーカイブ時期かどうかを確認します。	毎分
bifconnect.sh	bif サーバに製品情報を送信します。	毎週土曜日午前 1 時 15 分
cleanfile	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。	毎時
clear_tmpfs.py	tmpfs をクリアします。	毎日午前 3 時
ddi_agent.sh	DDI 拒否リストを IWSS と同期します。	5 分ごと
DbOldDataCleanup.sh	データベース内で古くなったレポート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アップします。	毎日午前 2 時 5 分
db_reindex.sh	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。	毎週日曜日午前 3 時 28 分
db_vacuum.sh	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。	毎週日曜日午前 5 時 58 分
IniRecover.sh	/etc/iscan/intscan.ini ファイルを回復する必要があるかどうかを確認します。	毎日午前 3 時 55 分
log_purge.py	古くなった commonlog のステータスまたは未処理のログファイルを削除します。	毎日午前 1 時 30 分
logbackup.sh	バックアップログのスケジュールを設定します。	毎日午前 0 時 20 分
logpurge.sh	/etc/iscan/commonlog_data/agent/failed ディレクトリにあるアップロード失敗のログをクリアします。	毎日午前 1 時 20 分

表 C-1. IWSS のセットアップ中に作成される予約タスク (続き)

タスク	機能	間隔
month_table.sh	ログやレポート機能で利用される月次のテーブル作成のスケジュールを設定します。	毎日午前 0 時 30 分
purgefile	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。	毎日午前 2 時
reverse_proxy_log_purge.sh	リバースプロキシモードのログを削除します。	毎日午前 1 時 29 分
reverse_proxy_monitor.sh	リバースプロキシモードでの nginx デーモンの状態を監視します。	2 分ごと
S99ISSnmpd restart	SNMP デーモンを再起動します。	毎日午前 1 時 48 分
schedule_au	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。	15 分ごと
schedulepr_update	製品ライセンスのステータスを確認します。	毎日
scheduler.py	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。	毎時
svc_snmpmonitor.sh	logtodb、mail、postgres、および metric の各デーモンが動作していることを確認します。これらのデーモンが動作していない場合は、それらを再起動します。	5 分ごと
tomcatchecker.sh	Apache Tomcat サービスの再起動が必要かどうかを確認します。	毎日午前 0 時 18 分、午前 4 時 18 分、午前 6 時 18 分、午後 10 時 18 分
/usr/iwss/iwsva_https_cron.sh	証明書失効リスト (CRL) をアップデートします。	毎日午前 1 時

設定ファイルについて

設定ファイルにアクセスするには、ローカルターミナルまたは SSH を使用して、root としてアプリケーションにログオンする必要があります。

設定ファイルには、メイン、プロトコルモジュール、検索モジュール用の 3 種類があります。すべての設定ファイルは {IWSS root} ディレクトリにあります。{IWSS root} の初期設定は /etc/iscan/ です。メインの設定ファイルは、intscan.ini です。

- ウイルス検索固有の設定は、次のファイルにあります。
`{IWSS root}/IWSSPIScanVsapi.dsc`
- ICAP プロトコル固有の設定は、次のファイルにあります。
`{IWSS root}/IWSSPIProtocolIcap.pni`
- スタンドアロンプロキシ固有の設定は、次のファイルにあります。
`{IWSS root}/IWSSPIProtocolHttpProxy.pni`
- URL フィルタ検索モジュールの設定は、次のファイルにあります。
`{IWSS root}/IWSSPIUrlFilter.dsc`
- レポート固有の設定は、次のファイルにあります。
`{IWSS root}/report.ini`
- ボットネット検索固有の設定は、次のファイルにあります。
`{IWSS root}/IWSSPINcieScan.dsc`
- DLP 検索の設定は、次のファイルにあります。
`{IWSS root}/IWSSPIDlpFilter.dsc`
- HTTP 検査固有の設定は、次のファイルにあります。
`{IWSS root}/IWSSPISigScan.dsc`
- FTP 検索固有の設定は、次のファイルにあります。
`{IWSS root}/IWSSPIProtocolFtp.pni`
- アプリケーション制御固有の設定は、次のファイルにあります。
`{IWSS root}/appcMapping.ini`
- URL 分類データベースの設定は、次のファイルにあります。
`{IWSS root}/urlfxIFX.ini`
- 初期設定の URL カテゴリと、そのマッピング情報の設定は、次のファイルにあります。

```
{IWSS root}/urlfcMapping.ini
```

- IP アドレスと、IWSS デバイスにアクセスできるすべてのコンピュータの IP アドレスおよび IP の範囲のリストの設定は、次のファイルにあります。

```
{IWSS root}/ClientACL_http.ini (HTTP の場合)
```

```
{IWSS root}/ClientACL_ftp.ini (FTP の場合)
```

- IWSS で HTTP 要求を転送するポートを定義するルールの設定は、次のファイルにあります。

```
{IWSS root}/HttpPortPermission_http.ini (HTTP の場合)
```

```
{IWSS root}/HttpPortPermission_ftp.ini (FTP の場合)
```

- 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 (HTTP の場合)
```

```
{IWSS root}/ServerIPWhiteList_ftp.ini (FTP の場合)
```

IWSS Web コンソールは、使用されているモジュールによって異なります。これまで旧バージョンの 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。

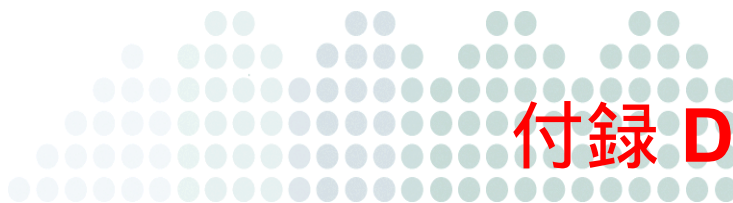
プロトコルのアクティブな設定ファイルの完全なパスを、`/etc/iscan/intscan.ini` ファイルの [main] セクションにある「`protocol_config_path`」パラメータに入力します。

プロトコルハンドラには、固有の設定ファイルが必要です。このファイルには、そのプロトコルのみに関連するエントリが含まれます。これらのプロトコル設定ファイルは、ファイル名の .pni という拡張子で示されます。

検索モジュール

トラフィックの検索機能は、検索モジュールとして知られるダイナミックライブラリを使用して提供されます。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、`/etc/iscan/intscan.ini` ファイルの `[scan]` セクションにある「`plugin_dir`」パラメータに示されるディレクトリで `.dsc` ファイルを探すことにより、使用可能な検索モジュールを検出します。



IWSS のベストプラクティス

本付録では、InterScan Web Security Suite (以下、IWSS) を使用するためのベストプラクティスについて説明します。

内容は次のとおりです。

- ・ 354 ページの「共有パーソナルコンピュータで複数のユーザを認証する (標準認証)」
- ・ 355 ページの「検索に関する考慮事項」

共有パーソナルコンピュータで複数のユーザを認証する (標準認証)

認証に Microsoft Active Directory サーバを使用して 1 つの共有パーソナルコンピュータ (PC) で複数のユーザをサポートすることが、IT マネージャとユーザにとっての課題になることがあります。IWSS は、ブラウザの機能に基づく認証機能を提供し、Microsoft Internet Explorer を初期設定のブラウザとして使用することで、共有 PC における複数ユーザの認証をサポートします。

ベストプラクティスの提案

Microsoft ShellRunas ユーティリティの利用

- 共有 PC では、Microsoft ShellRunas ユーティリティを利用して、Microsoft Internet Explorer が開始されるたびにユーザ認証を強制することができます。ユーザの認証には AD 認証情報が使用されます。Internet Explorer はその認証情報を使用して、HTTP ヘッダにユーザ ID 情報を自動的に入力するため、IWSS は、ログ記録、レポート作成、およびポリシー適用の目的でユーザを識別できるようになります。
- 次のサイトから MS ShellRunas ユーティリティをダウンロードします。
<http://technet.microsoft.com/ja-jp/sysinternals/cc300361.aspx>
- コンピュータの使用が終了したら、ユーザは、必ず IE ブラウザセッションをシャットダウンする必要があります。これにより、Microsoft Internet Explorer は次のユーザに認証情報の入力を促すことができます。このツールが正常に機能するためには、ユーザがこのことを認識していることが重要です。
- 認証されたユーザキャッシュのキャッシュ間隔を延長または短縮するように IP ユーザキャッシュパラメータを変更して、ユーザに認証情報の入力を促すタイミングを微調整することもできます。IWSS の初期設定のユーザキャッシュ値は 2 時間 (120 分) です。
`/etc/iscan/commonldap/ldapCache.ini` ファイルの `[expire-cache]` にある `expire_interval=` の値を設定します。

検索に関する考慮事項

IWSS の不正プログラム検索アーキテクチャはハイブリッドソリューションで、トレンドマイクロの Smart Protection Network (SPN) などのクラウドベースの不正プログラム検出方法、ローカルなオンボックス検索テクノロジー、およびシグネチャファイルを使用します。

Smart Protection Network — クラウドベースのサービス

IWSS の Smart Protection Network (SPN) は、業界最高のパフォーマンスを備えたクラウドベースの不正プログラム対策サービスです。Smart Protection Network には、以下のような不正プログラム検出コンポーネントがあります。

- Web レピュテーションサービス (WRS) は、既知の不正な Web サイト、ドメイン、ファイル、オブジェクト、およびメール関連項目の事前検出とブロック機能 (ファームング / フィッシング検出など) を提供する相関性のあるいくつかのサービスから構成されています。
 - ドメインレピュテーション
 - ページレピュテーション
 - メールレピュテーション
 - ファイルレピュテーション
- URL フィルタサービスでは、URL データベースをクラウドに格納してデータベースの迅速な更新を実現し、トレンドマイクロのグローバルなユーザベースを保護します。このとき、IWSS サーバで URL データベースファイルのダウンロードや更新を行う必要はありません。これにより最新の URL 情報がすべてのお客さまに提供されます。また事前保護機能の迅速化が図られ、不正サイトが発見されてから不正サイトが URL データベースに追加されるまでの時間が短縮されることで、すべてのお客さまが保護されます。
- フィードバックループは、すべてのトレンドマイクロ製品からのリアルタイムの情報を提供し、SPN のクラウドベースのコンポーネントと URL フィルタデータベースを更新します。顧客端末で発見された不正プログラムは、クラウドアーキテクチャにフィードバックされ、情報をリアルタイムに微調整するために使用されます。これにより、トレンドマイクロのグローバルなユーザベースで、誤警告の少ない迅速な事前防止機能が実現します。

ベストプラクティスの提案

Smart Protection Network (SPN) は、クラウドベースのサービスを使用し、検索に DNS クエリを利用します。迅速な応答と最小限の待ち時間を実現するために、IWSS デバイスはプライマリおよびセカンダリ DNS サーバで構成されている必要があります。

DNS サーバは、IWSS による多くの DNS 要求をサポートできる必要があります。通常、IWSS によってローカルな DNS キャッシュが作成されるまでは、アクセスされる URL ごとに 2 つの DNS 要求が作成されます。DNS サーバが、必要以上の DNS を処理できるだけのリソースとパフォーマンスを備えたサーバに設置されていることを確認します。

待ち時間を少なくするには、DNS サーバが高速なネットワークカードを保有し、高速なネットワークスイッチに取り付けられている必要があります。

トレンドマイクロは、現地 DNS サーバと、企業ネットワーク外に設置された ISP 提供の DNS サーバを使用することをお勧めします。通常、IPS DNS サーバは待ち時間が長く、単一の IP アドレスからの多量の DNS クエリはサポートしません。多くの IPS DNS サーバは、1 秒あたりの DNS 要求数を制限する調整メカニズムを備え、IWSS の Web レピュテーションサービス (WRS) のパフォーマンスに影響を与える可能性があります。

ネットワーク応答時間とパフォーマンスを向上させるには、DNS サーバを IWSS ユニットのできるだけ近くに設置し、デバイス間の不要なネットワークホップを削減するようにしてください。

WRS と URL フィルタ要求は、HTTP ポート 80 を介して作成されます。ファイアウォール上のこれらのポートでは、IWSS 管理 IP アドレスをブロックしないでください。

ローカルな IWSS 検索エンジン

IWSS は、ローカルなオンボックス検索機能を備え、インターネットからダウンロードされたコンテンツに対して不正プログラムの検索が実行されるようにします。Smart Protection Network の Web レピュテーションサービスと URL フィルタサービスでは、既知の不正サイトとコンテンツおよび新たに発見された不正サイトとコンテンツの大部分をフィルタできますが、ローカルなファイル検索では、受信したファイルとオブジェクトにウイルス、ワームや、トロイの木馬などの不正プログラムが埋め込まれていないことを確認します。

IWSS には、以下のローカル検索エンジンがあります。

- ファイルタイプブロックでは、60 を超えるさまざまなファイルの MIME タイプを識別してブロックすることができます。このファイルには、Java アプレット、実行可能ファイル、Microsoft Office ドキュメントなどの一般的なファイルが含まれます。サポートされているファイルタイプの詳細については、323 ページの「ファイルタイプと MIME コンテンツタイプの対応」を参照してください。

- ・ ウイルス検索 (VSAPI) では、シグネチャベースのウイルス検索と不正プログラム検索を実行します。
- ・ トレンドマイクロの推奨設定では、実際のファイルタイプに基づいてファイルの特定と検索を実行するため、ファイル拡張子を変更したり他の形式のファイル操作を使用したりして、ユーザが検索エンジンをバイパスするのを防ぐことができます。
- ・ IntelliTrap はヒューリスティックな検索機能を提供し、ネットワーク内を移動するときに状態を変える不正プログラムを特定して防御します。
- ・ 圧縮ファイルの検索は、何度も圧縮された高度な圧縮ファイルに潜む不正プログラムを防御します。不正プログラムの作成者たちは、この一般的な配信方法を使用して、従来のウイルス対策検索ソフトウェアから逃れようとしています。
- ・ スパイウェア検索は、スパイウェア、ダイアラー、ハッキングツール、パスワードクラックソフト、アドウェア、ジョークプログラム、リモートアクセスツール、およびその他のグレーウェアを防御します。このローカル検索エンジンは、スパイウェアシグネチャに基づく防御機能を提供し、URL フィルタ機能にあるスパイウェア URL カテゴリの補完に使用されます。ローカルなスパイウェア検索エンジンは、スパイウェアやグレーウェアに感染している可能性のある、インターネットからダウンロードされたファイルまたはインターネットにアップロードされたファイルの検索に使用されます。一方、URL フィルタのスパイウェアカテゴリは、スパイウェアに関連するファイルとオブジェクトを含んでいることがわかっているサイトへのアクセスを事前にブロックするために使用されます。
- ・ サイズの大きいファイルの検索を使用すると、管理者は、多くのシステムリソースを消費する可能性のあるサイズの大きいファイルの検索をバイパスすることができます。従来、不正プログラムの作成者たちは、多くの注意をファイルに向けさせることなく不正プログラムをすばやく拡散させたいため、サイズの大きいファイルにウイルスを埋め込みません。

ベストプラクティスの提案

- ・ IWSS のローカル検索サービスは、不必要な検索を減らすために、特定の順番で動作します。IWSS でのインターネットトラフィックの検索は、Smart Protection Network のクラウドベースの予防的サービスから始まって、次の順序で行われます。
 - ・ Web レピュテーションサービス (WRS)
 - ・ URL フィルタサービス
 - ・ ファイルタイプブロック
 - ・ ウイルス検索
 - ・ IntelliTrap ヒューリスティック
 - ・ MacroTrap

- ・ トレンドマイクロの推奨設定の実際のファイルタイプ
- ・ ウイルス検索 (VSAPI) の検索エンジンは、多くのリソースを消費します。Web レピュテーションサービス (WRS) を有効にし、URL フィルタサービスに加入し、そのコンピュータ / 危険カテゴリを有効にすると、従来の VSAPI ベースのウイルス検索を実行する必要性を大幅に低減することができます。このような変更を行うと、サーバリソースを削減し、使用環境に新たな拡張性をもたらすことができます。
- ・ 高い整合性評価を持つ、許可リストにある信頼されたサイトとファイルについては、不正プログラム検索を無効にすると、パフォーマンスを向上させサーバリソースの使用を軽減することができます。[除外設定] タブの [グローバル URL の信頼]、[承認する URL]、および [除外ファイル] の許可リストを使用して、信頼するサイトとファイルの検索をバイパスします。
- ・ 特定のサイズを超えるファイルの検索を省略するように、サイズの大きいファイルの検索を設定できます。これにより、大きなファイルの不要な検索を減らし、リソース使用率を下げて、能力とパフォーマンスを向上させることができます。
- ・ 大きなファイルのダウンロードに対するユーザ応答時間を向上させるには、[サイズの大きいファイルの処理] 機能の [遅延検索] オプションを有効にし、要求元ホストに検索されたファイルの一部を少しずつ配信するようにします。これにより、ブラウザのファイル転送状態のインジケータが維持され、ファイルの検索中の進行状況がユーザに表示されます。少量ずつ配信されているファイルの中で不正プログラムが見つかったら、IWSS はファイルの残りをブロックします。その結果、実行できない不完全なファイルが生成されます。マルチメディアファイルや、YouTube コンテンツなどの HTTP ポート 80 を使用するストリーミングコンテンツの場合は、[遅延検索] を有効にし、メディアの一部が流れるようにする必要があります。[配信前に検索] オプションを選択すると、ストリーミングコンテンツは完全に検索されるまでブロックされるため、ユーザの操作性が悪くなります。
- ・ ユーザに配信する前にファイル全体を検索する必要のあるお客さまの場合は、[サイズの大きいファイルの処理] 機能の [配信前に検索] オプションを選択してください。これにより、IWSS はファイルをバッファに格納し、ファイルをユーザに配信する前に検索を完了します。この方法は、エンドユーザのパフォーマンスの認識の点では若干遅くなりますが、感染ファイルは一部たりとも侵入できません。
- ・ グローバル URL の信頼の許可リストに登録されているエントリは検索されないということに留意してください。許可リストの項目を検索する場合は、[除外リスト] オブジェクトを作成して、ポリシーの [除外設定] タブでそのオブジェクトを使用します。[除外設定] タブには、HTTP/FTP 検索ポリシーにある許可リストの項目を検索するオプションがあります。

URL フィルタカテゴリのグループ

URL カテゴリは、表 E-1 に示される URL フィルタグループに分類されます。

表 E-1. URL カテゴリのグループ定義

カテゴリのグループ	説明
アダルト	子供には不適切であると一般的に見なされる Web サイト
ビジネス	ビジネス、雇用、またはコマースと関連する Web サイト
コミュニケーション / メディア	オンライン通信および検索のためのツールとサービスを提供する Web サイト
一般	その他のカテゴリに当てはまらない Web サイト
インターネット セキュリティ	不正ソフトウェアをばらまくことで知られるサイトを含む、危険な可能性のある Web サイト
ライフスタイル	宗教的、政治的、または性的な好み、あるいは娯楽とエンターテインメントについての Web サイト
ネットワーク帯域幅	コンピュータのインターネット接続の速度に著しい影響を与える可能性のあるサービスを提供する Web サイト
カスタムカテゴリ	カスタマイズした特定のカテゴリに対して管理者が定義した Web サイト

注意： URL フィルタが適切に動作するには、IWSS はトレンドマイクロサービスに HTTP 要求を送信する必要があります。HTTP プロキシが必要な場合は、[管理] [配置ウィザード] の順に選択してプロキシを設定します。

URL フィルタのカテゴリ

表 E-2 は、URL フィルタのカテゴリの定義と、割り当てられるグループを示しています。

表 E-2. URL フィルタカテゴリの定義

カテゴリのグループ	カテゴリのタイプ	カテゴリの定義
アダルト	アダルト / 成人向け	子どもが閲覧するのに不適切だと広く一般に思われている、性的に露骨なコンテンツを表示する成人向けコンテンツのある Web サイトです。
アダルト	違法または禁止されたコンテンツ	国際法上で禁止されている、または違法性があるコンテンツに関する情報を提供する Web サイトです。関連情報の共有や転送のためのソフトウェアを提供する Web サイトも含まれます。
アダルト	ポルノ	性的に露骨なコンテンツを表示する成人向けコンテンツのある Web サイトです。
アダルト	性教育	性教育（セーフセックス、避妊法）、人工中絶、性に関する Web サイトです。
アダルト	下着 / 水着	水着、下着などのイメージを扱った Web サイトです。販売商品の 1 つとして水着や下着が扱われている Web サイトは含まれません。
アダルト	ヌード	人体の裸体描写や半裸描写を扱った Web サイトです（ヌーディストサイトも含まれません）。

表 E-2. URL フィルタカテゴリの定義 (続き)

カテゴリのグループ	カテゴリのタイプ	カテゴリの定義
アダルト	酒 / タバコ	アルコールやタバコの製造、販売促進に関する Web サイトです。飲酒や喫煙を勧める Web サイトも含まれます。販売商品の 1 つとしてアルコールやタバコが扱われている Web サイトは含まれません。
アダルト	違法と思われる行為	違法行為 (強盗、窃盗、法の適用の回避、詐欺、盗作など) に関連すると思われる Web サイトです。違法行為を擁護する Web サイト、アドバイスする Web サイト、レポートを販売する Web サイトが含まれます。
アダルト	低俗	一般的に不適切と思われる表現や画像などを含む Web サイトです。
アダルト	ギャンブル	ギャンブルに関する情報を提供する Web サイトです。ギャンブルを勧める Web サイト、オンラインカジノの Web サイトも含まれます。ギャンブル関連の製品や機械を販売する Web サイトは含まれません。
アダルト	暴力 / 差別	暴力や差別に関する記述や描写がある Web サイトです。暴力や差別を助長する Web サイト、援護する Web サイトも含まれます。
アダルト	武器	武器、兵器などに関する Web サイトです。軍事関連組織や、ハンティング、射撃に関する Web サイトは含まれません。
アダルト	妊娠中絶	人工中絶 (手順の説明、サポート、影響など) に関する Web サイトです。
コミュニケーション / メディア	ダイナミック DNS	ダイナミック DNS サービスを利用して、ドメイン名を動的 IP アドレスに割り当てている Web サイトです。
ライフスタイル	レジャー / 趣味	ガーデニング、アウトドア、コレクション、ゲーム (テレビゲームを除く)、手工芸などのレジャーや趣味に関する Web サイトです。ペットやレジャー関連施設 / 団体の Web サイトも含まれます。

表 E-2. URL フィルタカテゴリの定義 (続き)

カテゴリのグループ	カテゴリのタイプ	カテゴリの定義
ライフスタイル	アート	絵画、彫刻などの視覚芸術に関する Web サイトです。
ライフスタイル	エンターテインメント	映画、音楽、ラジオ番組やテレビ番組 (ニュースを除く)、書籍や雑誌などに関する情報を提供する Web サイトです。
ビジネス	ビジネス / 経済	起業、マーケティングなどのビジネスや経済に関する Web サイトです。他のカテゴリに当てはまらない企業 Web サイトも含まれます。
ライフスタイル	特定の宗教 / オカルト	特定の宗教や信仰に関する表記、信念、科学的に証明できない呪文、魔術、超常現象に関する情報を提供する Web サイトです。
ネットワーク	インターネットラジオ / テレビ	ストリーミングラジオやテレビを主に配信する Web サイトです。
コミュニケーション / メディア	インターネット電話	インターネット電話に関する Web サイトです。
アダルト	違法と思われる薬物	違法と思われる薬物の宣伝、販売および、処方薬などの不適切な使用や方法に関する Web サイトです。
アダルト	マリファナ	マリファナの栽培、使用、調合方法に関する Web サイトです。関連器材に関する Web サイトも含まれます。
一般	教育	学校、通信教育などの教育に関する Web サイトです。
インターネットのセキュリティ	安全でない IoT 機器の接続	IoT デバイスにダメージを与えたり、感染させたり、または悪用したりする潜在的な可能性のある、安全でないインターネット接続です。

表 E-2. URL フィルタカテゴリの定義 (続き)

カテゴリのグループ	カテゴリのタイプ	カテゴリの定義
ライフスタイル	文化団体	図書館、美術館、博物館などの文化遺産保護を目的とした団体が運営する Web サイトです。ボーイスカウト、ガールスカウト、国際ロータリークラブなどの組織が管理する Web サイトも含まれます。
ライフスタイル	一般団体	公共政策、世論、社会的慣習、経済活動などに関する意見を提言する Web サイトです。サービス団体、慈善団体、専門家集団、労働団体が運営する Web サイトも含まれます。
ビジネス	金融サービス	金融サービス全般の情報やサービスを提供する Web サイトです。金融業界の企業が運営する Web サイトも含まれます。
ビジネス	貿易 / 仲介	株式や債券への投資に関する Web サイトです。オンライントレードや自動車保険に関する Web サイトも含まれます。
ライフスタイル	ゲーム	テレビゲーム、コンピュータゲーム、ボードゲームの Web サイトです。賞金や賞品をプレゼントする Web サイト、競技やダウンロードに関する Web サイトは含まれません。
一般	政府 / 法律	法律や政治など、政府に関する Web サイトです。軍隊、医療に関する Web サイトは含まれません。
一般	軍隊	軍隊に関する Web サイトです。武器や軍装備品の情報提供や販売を行う Web サイトは含まれません。
一般	政治	政党、政党後援組織、その他政治的団体に関する Web サイトです。政治に関連する話題の Web サイトも含まれます。政治に関連のない団体 / 集団による Web サイトは含まれません。
一般	健康	健康、フィットネス、美容 / 健康促進に関する Web サイトです

表 E-2. URL フィルタカテゴリの定義 (続き)

カテゴリのグループ	カテゴリのタイプ	カテゴリの定義
一般	コンピュータ / インターネット	コンピュータ、インターネット、その他の関連技術に関する Web サイトです。電子機器の販売や評価を行う Web サイトも含まれません。
コミュニケーション / メディア	プロキシ回避システム / 匿名化ソフトウェア	プロキシサーバや Web フィルタリングシステムの回避に使用される可能性がある、またはインターネットを匿名や追跡されない状態で使用することを可能にする Web サイトです。これらを目的としたツールを提供する Web サイトも含まれます。
コミュニケーション / メディア	検索エンジン / ポータル	Web 上の情報検索システムを提供する検索エンジンサイトやポータルです。
コミュニケーション / メディア	インターネット インフラストラクチャ	データやデータ分析の収集、処理、提示に使用されるコンテンツサーバ、イメージサーバ、または Web サイトです。Web の分析ツールやネットワーク監視を行う Web サイトも含まれます。
コミュニケーション / メディア	ブログ / 掲示板 / コミュニケーション	ブログ、掲示板など、Web ベースのコミュニケーションを行う Web サイトです。
ネットワーク	画像検索	画像を検索する Web サイトです。
ライフスタイル	その他出版物	タブロイド誌や時事の話題などに関する出版物の Web サイトです。
ビジネス	就職 / 転職	就職や雇用サービスに関する Web サイトです。
一般	ニュース / メディア	ニュース、時事問題、天気に関する Web サイトです。他のカテゴリに当てはまらないオンラインマガジンも含まれます。
ライフスタイル	出会い	恋愛、デート、交際などの目的で人と出会うための Web サイトです。

表 E-2. URL フィルタカテゴリの定義 (続き)

カテゴリのグループ	カテゴリのタイプ	カテゴリの定義
一般	翻訳 / キャッシュページ	オンライン翻訳や検索エンジンにおける キャッシュされた Web ページです。プロキ シサーバや Web フィルタリングシステムの 回避に使用される可能性があります。
一般	レファレンス / 参照情報	地図、百科事典、辞書、天気、実用書、数値 の換算など、一般的または専門的な情報を照 会するための Web サイトです。
コミュニケーション / メディア	ソーシャルネット ワーキング	人と人とのつながりを促進 / サポートする、 コミュニティ型の Web サイトです。
コミュニケーション / メディア	チャット / メッセージ	チャットやインスタントメッセージの Web サイトです。インスタントメッセ ンジャーのソフトウェアを提供する Web サイ トも含まれます。
コミュニケーション / メディア	メール	Web メール、グリーティングカード、メー リングリストなど、Web ベースのメール サービスの Web サイトです。
コミュニケーション / メディア	ニュースグループ / フォーラム	ニュースグループ、フォーラム、または BBS に関する Web サイトです。
ライフスタイル	宗教	一般的な宗教、信仰、宗教建築物に関する Web サイトです。
ライフスタイル	個人 Web サイト	個人が開設した趣味などに関する Web サイ トです。ソーシャルネットワーキング、プロ グサイトなどのサービスに登録されている個 人ページは含まれません。
ネットワーク	ファイル共有サービス	ファイルやデータを共有できる Web サイト です。
ネットワーク	ピアツーピア	ピアツーピア (P2P) ネットワーク内でファ イルを共有 / 転送するための情報やソフトウ ェアを提供する Web サイトです。
ビジネス	ショッピング	ショッピング関係の Web サイトです。

表 E-2. URL フィルタカテゴリの定義 (続き)

カテゴリのグループ	カテゴリのタイプ	カテゴリの定義
ビジネス	オークション	オークション関係の Web サイトです。
ビジネス	不動産	不動産に関する Web サイトです。物件の販売、購入、賃貸に関するサービスを提供する Web サイトも含まれます。
ライフスタイル	生活 / ライフスタイル	日常生活に関する情報を提供する Web サイトです。化粧品やファッションに関する Web サイトも含まれます。エンターテインメント、趣味、性、スポーツに関する Web サイトは含まれません。
ライフスタイル	ガンクラブ / ハンティング	ガンクラブなどの団体に関する Web サイトです。ハンティング、射撃、サバイバルゲーム、ペイントボールの施設に関する Web サイトも含まれます。
ライフスタイル	レストラン / フード	食品、ケータリング、ダイニングサービス、料理、レシピに関する宣伝、説明、評価などを行う Web サイトです。
ライフスタイル	スポーツ	スポーツや各種競技に関する Web サイトです。ファンサイト、スポーツ用品を販売する Web サイトも含まれます。
ライフスタイル	旅行	旅行や観光地に関する Web サイトです。旅行の予約や計画を行う Web サイトも含まれます。
一般	乗り物	乗り物に関する Web サイトです。車両本体や部品のカスタマイズ、購入、修理サービスなども含まれます。軍用車両に関する Web サイトは含まれません。
ライフスタイル	ユーモア	ユーモアに関する Web サイトです。
ネットワーク	ストリーミングメディア /MP3	ラジオ番組やテレビ番組以外のストリーミング映像や音声を提供する Web サイトです。MP3、AVI ファイル形式などの音楽や動画のダウンロードを行う Web サイトも含まれます。

表 E-2. URL フィルタカテゴリの定義 (続き)

カテゴリのグループ	カテゴリのタイプ	カテゴリの定義
ネットワーク	着信メロディ / 携帯電話向けダウンロードサービス	携帯電話向けに着信メロディ、ゲーム、動画などを配信する Web サイトです。
ネットワーク	ソフトウェアダウンロード	ソフトウェアのダウンロードに関する Web サイトです。
ネットワーク	懸賞 / サイドビジネス	Web サイト、メール、オンライン広告などの閲覧、リンクのクリック、アンケートの回答などに対して報酬を得る Web サイトです。
インターネットのセキュリティ	不正と思われるプログラム (グレーウェア)	コンピュータに害を与える可能性のある Web サイトです。
インターネットのセキュリティ	スパイウェア	ユーザに無断でデータを収集し転送するソフトウェアをダウンロードする可能性がある Web サイトです。
インターネットのセキュリティ	フィッシング	正規の Web サイトを偽装してユーザ名やパスワードなどの情報を収集する詐欺サイトです。
インターネットのセキュリティ	スパム	スパムメールを配信している疑いのある Web サイトです。
インターネットのセキュリティ	アドウェア	広告などの宣伝用コンテンツを表示するソフトウェアをダウンロードする可能性のある Web サイトです。ブラウザヘルパーオブジェクト (BHO) をインストールする Web サイトも含まれます。
インターネットのセキュリティ	不正プログラムによる外部アクセス	不正プログラムによって利用される、不正プログラムのアップデートや盗み取った情報の格納に使用される Web サイトです。
インターネットのセキュリティ	不正プログラム配信	有害なプログラムやソースコードの配布を直接的または間接的に促す Web サイトです。

表 E-2. URL フィルタカテゴリの定義 (続き)

カテゴリのグループ	カテゴリのタイプ	カテゴリの定義
コミュニケーション / メディア	コインマイナー	スクリプトまたは実行ファイルで、コインマイニングなどの仮想通貨に関する処理を実行します。
インターネットのセキュリティ	MFA (MadeforAdSense) サイト	独自のコンテンツを持たずに、GoogleAdSense 広告を表示するために開設された Web サイトです。
ライフスタイル	子ども向け	子どもを対象として提供されている Web サイトです。
インターネットのセキュリティ	Web 広告	広告の表示を主に行う Web サイトです。バナー広告、ポップアップ広告の表示に使用される Web サイトも含まれます。
コミュニケーション / メディア	Web ホスティング	トップレベルドメインや Web ホスティング サービスを提供する組織の Web サイトです。
一般	未評価	カテゴリが未分類の Web サイトです。
インターネットのセキュリティ	C&C サーバ	コマンド & コントロール (C&C) サーバやスパイウェアが収集したデータを保管するサーバ (ドロップゾーン) です。
インターネットのセキュリティ	不正ドメイン	悪質な実行コード (ペイロード) をホストするドメインです。
インターネットのセキュリティ	新たに確認されたドメイン	最近アクティブになった、もしくは新たに確認されたドメインで、トレンドマイクロによる分類がまだ行われていないドメインです。使い捨てドメインなど、以前からドメイン登録されていたものも含まれます。
インターネットのセキュリティ	詐欺サイト	個人または団体から信用を得た上で金銭などをだまし取るようとする Web サイトです。多くの場合、人間誰もが持つような欲望や同情などにつけ込む巧みな手口が使われます。

表 E-2. URL フィルタカテゴリの定義 (続き)

カテゴリのグループ	カテゴリのタイプ	カテゴリの定義
インターネットのセキュリティ	ランサムウェア	ランサムウェア (身代金要求型不正プログラム) を広めるため、直接的または間接的に利用される Web サイトです。
一般	その他	他のカテゴリに分類できない評価済みの Web サイトです。
一般	情報不足	情報が十分ではない Web サイトです。必要な情報が得られた場合、本カテゴリは自動的に更新されます。
内部使用	クラウドアプリケーション	クラウドコンピューティング用のアプリケーションで使用される Web サイトです。

用語集

この用語集では、本書またはオンラインヘルプで使用される用語を説明しています。

用語	説明
ActiveX (アクティブ エックス)	OLE (Object Linking and Embedding) を実装するオープンソフトウェアアーキテクチャのタイプ。Web ページのダウンロードなどの一部の標準インタフェースを有効にします。
ActiveX 不正コード	<p>ActiveX コントロールは Web ページに埋め込まれたコンポーネントオブジェクトで、ページが表示されると自動的に実行されます。ActiveX コントロールを使用することにより、Web 開発者は、たとえばトレンドマイクロの無料オンライン検索であるウイルスバスターオンラインスキャンなど、幅広い機能を使用して、インタラクティブで動的な Web ページを作成できます。</p> <p>ハッカー、ウイルス作成者、および悪質ないたずらを目的とする他の人間は、システムを攻撃するための媒体として ActiveX 不正コードを使用することがあります。多くの場合、Web ブラウザのセキュリティ設定を「高」に変更することで、こうした ActiveX コントロールを実行しないように設定できます。</p>
Audio/Video ファイル	音楽などの音声やビデオ映像を含むファイルです。
cookie	インターネットユーザについての情報、たとえば名前、好み、興味などを保持するメカニズムで、後で使用するために Web ブラウザに保存されます。次回、ブラウザが cookie を保存している Web サイトにアクセスすると、ブラウザは Web サーバに cookie を送信します。Web サーバはその cookie を使用して、カスタマイズされた Web ページを表示できます。たとえば、名前を表示して開始する Web サイトなどです。

用語	説明
DNS	ドメインネームシステム (Domain Name System) ホスト名を IP アドレスに変換するために主にインターネット上で使用されている汎用的なデータクエリサービスです。
DNS 名前解決	DNS クライアントが DNS サーバにホスト名とアドレスデータを要求するときのプロセス。基本的な DNS 設定では、サーバが初期設定された名前解決プロセスを実行します。たとえば、リモートサーバは、現在のゾーンにあるコンピュータ上のデータについて別のサーバに問い合わせます。リモートサーバ上のクライアントソフトウェアはリゾルバに問い合わせます。リゾルバは、データベースファイルからの要求に応答します。
DOS ウイルス	「COM」および「EXE」ファイル感染型ウイルスとも呼ばれます。DOS ウイルスは、拡張子 *.COM または *.EXE が付く、DOS の実行可能プログラムファイルに感染します。元のプログラムのコードの一部を上書きしたり不注意により破壊するほか、ほとんどの DOS ウイルスは、他のホストプログラムに感染することで増殖および伝染を図ります。
ELF	Executable and Linkable Format の略。UNIX および Linux プラットフォーム用の実行可能ファイル形式です。
Ethernet	Xerox Corporation と Palo Alto Research Center が考案したローカルエリアネットワーク (LAN) 技術です。Ethernet は、バスエフォート型通信システムで、CSMA/CD 技術を使用しています。Ethernet は、太い同軸ケーブル、細い同軸ケーブル、ツイストペアケーブル、および光ファイバーケーブルなど、さまざまなケーブルスキームで使用できます。Ethernet は、コンピュータをローカルエリアネットワークに接続するための規格です。
EXE ファイル感染型ウイルス	ファイル拡張子が .exe の実行可能プログラムです。「DOS ウイルス」も参照してください。
FAQ	Frequently Asked Questions の略。特定のトピックに関する質問とその回答のリストです。

用語	説明
FTP	あるコンピュータのユーザが別のコンピュータとの間で TCP/IP ネットワークを介してファイルを双方向に転送できるクライアント / サーバのプロトコル。また、ユーザがファイルを転送するために実行するクライアントプログラムのことも表します。
GUI	グラフィカルユーザインタフェース (Graphical User Interface) プログラムの入出力を表すために言葉のみではなく絵を使用すること。これは、やり取りをテキストの文字列で行うコマンドラインインタフェースと対比されます。
HTTP	ハイパーテキスト転送プロトコル (Hypertext Transfer Protocol) HTML 文書の交換のために WWW (World Wide Web) 上で使用されるクライアント / サーバの TCP/IP プロトコル。通常はポート 80 を使用します。
HTTPS	ハイパーテキスト転送プロトコルセキュリティ (Hypertext Transfer Protocol Secure) セキュリティで保護されたトランザクションの処理に使用される HTTP の強化版。
ICSA	ICSA Labs は、TruSecure Corporation の独立した部門です。10 年以上にわたり、製品テストの調査、情報収集、および認定に関する、セキュリティ業界の中心的な権威として存在しています。ICSA Labs は情報セキュリティ製品の基準を設定し、現在、インストールベースで世界の 90% 以上のウイルス対策、ファイアウォール、IPSec、暗号技術、およびコンピュータファイアウォール製品を認定しています。
IP	Internet Protocol の略。「IP アドレス」を参照してください。
IP アドレス	ネットワーク上のデバイス用のインターネットアドレスです。通常、IPv4 では 123.123.123.123 のようにピリオドで区切る表記方法、IPv6 ではコロンで区切る表記方法で表されます。
IP ゲートウェイ	ゲートウェイは、最終的な送信先に到達するまで、あるネットワークから別のネットワークへと IP データグラムを転送するプログラム、または特殊な目的のデバイスです。
IT	情報技術のことで、ハードウェア、ソフトウェア、ネットワーク、電気通信、およびユーザサポートを含みます。

用語	説明
JavaScript ウィルス	<p>JavaScript は、Netscape が開発した簡単なプログラミング言語です。これを使用することにより、Web 開発者は、ブラウザに表示される HTML ページに、スクリプトを使用して動的なコンテンツを追加できます。JavaScript は、Sun Microsystems の Java プログラミング言語の一部の機能を共有していますが、独立して開発されました。</p> <p>JavaScript ウィルスは、HTML コードのこれらの JavaScript を標的にするウィルスです。これにより Web ページにウィルスを潜ませ、ユーザのブラウザを使用してウィルスをユーザのデスクトップにダウンロードできます。</p> <p>「VBScript ウィルス」も参照してください。</p>
Java アプレット	<p>HTML ページに埋め込まれた小さくポータブルな Java プログラムで、ページが表示されるときに自動的に実行できます。Java アプレットを使用することで、Web 開発者は、幅広い機能を使用して、インタラクティブで動的な Web ページを作成できます。</p> <p>Java アプレットは、不正コードの作成者たちによる攻撃媒体として使用されてきました。しかし多くの場合、Web ブラウザのセキュリティ設定を「高」に変更することなどにより、簡単に、こうしたアプレットを実行しないように設定できます。</p>
Java ファイル	<p>Java は、Sun Microsystems が開発した汎用プログラミング言語です。Java ファイルには、Java コードが含まれます。Java は、プラットフォームに依存しない Java 「アプレット」の形式で、インターネット用のプログラミングをサポートしています (アプレットとは、HTML ページに含めることができる、Java プログラミング言語で記述されたプログラムです。Java 技術が有効になっているブラウザを使用して、アプレットを含むページを表示すると、そのアプレットのコードがシステムに転送され、ブラウザの Java Virtual Machine により実行されます)。</p>
Java 不正コード	<p>Java で記述された、または埋め込まれたウィルスコードです。「Java ファイル」も参照してください。</p>
KB	<p>キロバイト (Kilobyte) 1024 バイトのデータです。</p>

用語	説明
LAN (Local Area Network)	地理的に制限されたデータ通信ネットワークです。これを使用することにより、同じ建物内のコンピュータを簡単に相互接続できます。
LDAP (Lightweight Directory Access Protocol)	メールプログラムが、サーバから連絡先情報を取得するために使用するインターネットプロトコルです。
MAC (Media Access Control) アドレス	Ethernet アダプタなどのネットワークインタフェースカードを一意に識別するアドレスのことをいいます。Ethernet では、MAC アドレスは IEEE により割り当てられる 6 オクテットのアドレスです。LAN またはその他のネットワークでは、MAC アドレスはコンピュータの一意のハードウェア番号です (Ethernet LAN では、Ethernet アドレスと同じです)。コンピュータからインターネットに接続すると (または、インターネットプロトコルでのホスト)、対応テーブルでその IP アドレスが LAN 上のコンピュータの物理的 (MAC) アドレスに関連付けられます。MAC アドレスは、電気通信プロトコルのデータリンク層のメディアアクセス制御の副層で使用されます。各物理的装置タイプに対して、MAC 副層が異なります。
MacroTrap	トレンドマイクロのユーティリティです。文書に関連して保存されるすべてのマクロコードに対してルールベースの検査を実行します。マクロウイルスのコードは通常、多くの文書とともに運ばれる、非表示のテンプレートの一部に含まれます (たとえば、Microsoft Word 文書では .dot)。MacroTrap は、テンプレートをチェックし、ウイルスのような行動をする主な命令を探して、マクロウイルスの兆候があるかどうかを確認します。命令とは、テンプレートの一部を別のテンプレートにコピー (複製) する命令や、潜在的に有害なコマンド (破壊) を実行する命令などです。
MB	メガバイト (Megabyte) 1024 キロバイトのデータ
Mbps	100 万ビット毎秒。データ通信の帯域幅の単位です。
Microsoft Office ファイル	Excel や Word など、Microsoft Office ツールで作成されたファイルです。

用語	説明
NAT (Network Address Translation)	セキュア IP アドレスを、アドレスプールにある一時的な外部の登録 IP アドレスに変換するための規格です。これにより、信頼するネットワークに非公開の IP アドレスを割り当てて、インターネットにアクセスさせることができます。これは、ネットワーク内のすべてのコンピュータについて登録済みの IP アドレスを取得する必要がないことも意味します。
Network Content Inspection Engine (NCIE)	ボットや Web ロボットを検出できるトレンドマイクロのエンジンです。
OS	周辺機器のインタフェース、タスクのスケジュール管理、および記憶装置の割り当てなどのタスクを処理するソフトウェアです。このドキュメントでは、ウィンドウシステムおよびグラフィカルユーザインタフェースを提供するソフトウェアも指します。
SMTP	Simple Mail Transfer Protocol の略。通常は Ethernet を介して、コンピュータ間で電子メールを送受信するために使用するプロトコルです。サーバ対サーバのプロトコルであるため、メッセージのアクセスには別のプロトコルを使用します。
SMTP サーバ	メールメッセージを送信先にリレーするサーバです。
SNMP	Simple Network Management Protocol の略。管理上注意すべき状態について、ネットワークに接続されたデバイスの監視をサポートするプロトコルです。
SNMP トラップ	トラップとは、コンピュータプログラムのエラーまたはその他の問題を処理するプログラミングメカニズムです。SNMP トラップは、ネットワークデバイスの監視に関するエラーを処理します。 「SNMP」を参照してください。
SSL (Secure Socket Layer)	SSL (Secure Socket Layer) は、アプリケーションプロトコル (HTTP、Telnet、FTP など) と TCP/IP の間に層をなすデータセキュリティを提供するために Netscape が設計したプロトコルです。このセキュリティプロトコルは、データの暗号化、サーバの認証、メッセージの完全性、およびオプションで TCP/IP 接続のクライアント認証を提供します。

用語	説明
TCP	Transmission Control Protocol の略。TCP は、IP (Internet Protocol) と組み合わせて最も一般的に使用されるネットワークプロトコルで、コンピュータシステムからインターネットへの接続を管理します。
TCP/IP (Transmission Control Protocol/Internet Protocol)	ローカルおよび広域ネットワークの両方で、ピアツーピア接続機能をサポートする通信プロトコルのセットです。この通信プロトコルは、異なる OS を使用するコンピュータ間の通信を可能にします。インターネット上のコンピュータ間でデータを伝達する方法を制御します。
Telnet	TCP/IP (Transmission Control Protocol/Internet Protocol) の上で実行されるリモートログインのインターネット標準プロトコルです。リモートログインセッションのターミナルエミュレータとして動作するネットワークソフトウェアを指すこともあります。
URL	Uniform Resource Locator の略。インターネット上のオブジェクト、通常は Web ページの場所を指定する標準的な方法です。たとえば、「www.trendmicro.com」のようになります。URL は、DNS を使用して IP アドレスに変換されます。
VBscript ウィルス	<p>VBscript (Microsoft Visual Basic スクリプト言語) は簡単なプログラム言語で、これを使用することにより、Web 開発者は、ブラウザに表示される HTML ページにインタラクティブな機能を追加できます。たとえば VBscript を使用して、Web ページに「詳細についてはここをクリックしてください」というボタンを追加できます。</p> <p>VBscript ウィルスは、HTML コードのこれらの JavaScript を標的にするウィルスです。これにより Web ページにウィルスを潜ませ、ユーザのブラウザを使用してウィルスをユーザのデスクトップにダウンロードできます。</p> <p>「JavaScript ウィルス」も参照してください。</p>
VLAN (Virtual Local Area Network)	デバイスの (物理的でなく) 論理的なグループで、単一のブロードキャストドメインを構成します。VLAN のメンバーは、物理的なサブネットワーク上の場所ではなく、送信データのフレームヘッダにあるタグの使用によって識別されます。VLAN は、IEEE 802.1Q 規格で記述されます。

用語	説明
VPN (Virtual Private Network)	VPN は、在宅勤務者およびモバイルプロフェッショナルが、企業のネットワークまたは別のインターネットサービスプロバイダ (ISP) に市内通話のダイヤルアップでアクセスできるようにする、簡単で費用効果が高く、安全な方法です。インターネットを介する安全なプライベート接続は、専用プライベート回線よりも費用効果が高くなります。VPN は、トンネリングや暗号化などの技術と規格によって可能になりました。
Web	インターネットのことです。
Web コンソール	トレンドマイクロ製品のユーザインタフェースです。
Web サーバ	Web サイトで実行されるサーバプロセスで、リモートブラウザからの HTTP 要求に応じて Web ページを送信します。
アーカイブ	1 つのファイル、または通常は複数の個別ファイルと情報を含む単一のファイルです。zip ファイルなどがあります。適切なプログラムを使用して解凍 (分離) できます。
アクセス	コンピュータやサーバなどの記憶装置との間で、データの読み取りまたは書き込みを行うことをいいます。
アクセス権	データの読み取りまたは書き込みを行う権限です。ほとんどの OS では、仕事に対する責任に応じて、異なるレベルのアクセス権を定義できます。
アクティブモード	FTP プロトコルの設定です。クライアントにコマンドセッションの「ハンドシェイク」信号の開始を許可しますが、ホストではデータセッションが開始されます。
アクティベーション	アクティベーションコードを入力して製品をアクティベートすることをいいます。製品の機能は、アクティベートが完了するまで使用できません。アクティベーションは、インストール時またはインストール後に Web コンソールの [製品ライセンス] 画面で行います。
アクティベーションコード	ハイフンを含む 37 文字のコードで、トレンドマイクロ製品のアクティベーションに使用します。アクティベーションコードの例は、次のとおりです。 SM-9UE7-HG5B3-8577B-TD5P4-Q2XT5-48PG4 「レジストレーションキー」も参照してください。

用語	説明
圧縮ファイル	1 つまたは複数の個別ファイルと情報を含む単一のファイルです。WinZip などの適切なプログラムを使用して解凍できます。
圧縮ファイル	1 つまたは複数の個別ファイルと情報を含む単一のファイルです。WinZip などの適切なプログラムを使用して解凍できます。
アップデート	アップデート機能は、多くのトレンドマイクロ製品に共通の機能です。トレンドマイクロのアップデートサーバに接続し、インターネットを介して最新のウイルスパターンファイル、検索エンジン、およびプログラムファイルをダウンロードできます。
アドウェア	広告を目的としたソフトウェアで、プログラムの実行中に広告バナーを表示します。「バックドア」をインストールし、ユーザが知らない間にユーザのコンピュータのメカニズムを追跡するアドウェアを「スパイウェア」と呼びます。
アドレス	ネットワークアドレス（「IP アドレス」を参照）またはメールアドレスを指します。メールアドレスは、メールメッセージの発信元または送信先を指定する文字列です。
暗号化	データを目的の受信者のみが読み取れる形式に変更する処理を指します。メッセージを解読するには、暗号化されたデータの受信者は、適切な解読キーを持っている必要があります。従来の暗号化スキームでは、送信者と受信者が同じキーを使用してデータを暗号化および解読します。公開鍵暗号化スキームでは、2 つの鍵を使用します。公開鍵は誰でも使用でき、対応する秘密鍵は作成者のみが所有します。この方法では、所有者の公開鍵を使用して誰もがメッセージを暗号化して送信できますが、解読に必要な秘密鍵は所有者のみが持っています。
インスタンスレベルの設定	個々のインスタンスにのみ適用される IWSS のポリシーと設定です。
インストールスクリプト	トレンドマイクロ製品の UNIX バージョンのインストールに使用されるインストールプロシージャです。

用語	説明
インターネット	クライアントサーバ間のハイパーテキスト情報取得システムで、ルータにより接続された一連のネットワークを基礎としています。インターネットは現代の情報システムで、大学やその他多くの研究ネットワークだけでなく、広告、オンライン販売、およびサービスの媒体も幅広く受け入れています。World Wide Web は、インターネットで最も多く使用されているアプリケーションです。
インターネット プロトコル (IP)	インターネットの標準プロトコルで、データグラムと呼ばれる、データの基本単位を定義します。データグラムは、コネクションレス型で、ベストエフォート型の配信システムで使用されます。インターネットプロトコルは、インターネット上のシステム間で情報を伝達する方法を定義します。
インターネットボット	Web ロボットまたは単にボットは、DDoS 攻撃などの特定の標的に対する攻撃を開始するためによく使用されるソフトウェアアプリケーションです。これらは一般に、企業ネットワーク、個人、およびインターネットに対する脅威となり、増加の一途をたどっています。ボットが企業環境に存在すると、かなりの量のネットワーク帯域幅と処理能力が消費される可能性があります。またボットは、企業に法的責任を負わせる可能性があります。
イントラネット	外部のインターネットで提供されるものと似たサービスを組織内で提供するネットワークを指します。必ずしもインターネットには接続されていません。
ウイルス	コンピュータウイルスは、感染するという独特な能力を持つプログラム、つまり 1 つの実行可能コードです。生物学上のウイルスと同様に、コンピュータウイルスは急速に広がり、多くの場合、撲滅が困難です。
	増殖することに加え、一部のコンピュータウイルスには別の共通点があります。それは、ウイルスのペイロードを配信するダメージルーチンです。ペイロードはメッセージや画像を表示するだけかもしれませんが、ファイルの破壊、ハードディスクドライブの再フォーマット、またはその他の被害を引き起こす可能性もあります。ウイルスにダメージルーチンが含まれていない場合でも、記憶領域およびメモリを消費し、コンピュータの全体的なパフォーマンスを低下させることにより、問題を引き起こすことがあります。

用語	説明
ウイルスキット	ウイルスの構築および実行のためのソースコードのテンプレートで、インターネットで入手できます。
ウイルス作成者	コンピュータハッカーとも呼ばれる、ウイルスコードを記述する人のことを指します。
ウイルスシグネチャ	ウイルスシグネチャとは、特定のウイルスを識別するビットの一意の列です。ウイルスシグネチャは、トレンドマイクロのウイルスパターンファイルに保存されています。トレンドマイクロの検索エンジンは、メールメッセージの本文やHTTPダウンロードの内容など、ファイル内のコードをパターンファイル内のシグネチャと比較します。一致が検出されると、ウイルスが検出され、セキュリティポリシーに従って処理が実行されます（駆除、削除、または隔離など）。
ウイルス対策	コンピュータウイルスを検出および駆除するために設計されたコンピュータプログラムです。
ウイルストラップ	ウイルスコードのサンプルを分析用に捕獲するために使用するソフトウェアです。
オープンソース	一般ユーザが、ライセンスによる制限を受けずに無料で使用または変更できるプログラミングコードです。
オンラインヘルプ	IWSS の管理コンソールから参照できるヘルプです。
隔離	メールメッセージ、感染した添付ファイル、感染したHTTPダウンロード、または感染したFTPファイルなど、感染したデータをサーバの隔離されたディレクトリ（隔離ディレクトリ）に置くことをいいます。
仮想 IP アドレス (VIP アドレス)	VIP アドレスは、ある IP アドレスで受信したトラフィックを、パケットヘッダの送信先のポート番号に基づいて、別のアドレスに割り当てます。
画像ファイル	2次元で表されるデータ、つまり画像を含むファイルです。画像は、たとえばデジタルカメラを使用して現実の世界から取り込まれたり、グラフィックソフトウェアを使用してコンピュータで作成されます。
完全性のチェック	「チェックサム」を参照してください。

用語	説明
感染報告のあるウイルス	活発に移動する既知のウイルスを指します。「出回っていないウイルス」も参照してください。
管理者	「システム管理者」を指します。システム管理者とは、組織の一員で、新しいハードウェアおよびソフトウェアの設定、ユーザ名およびパスワードの割り当て、ディスク容量やその他のITリソースの監視、バックアップの実施、およびネットワークセキュリティの管理について責任を持ちます。
管理者アカウント	管理者レベルの権限を持つ、ユーザ名およびパスワードです。
管理者メールアドレス	トレンドマイクロ製品の管理者が、通知および警告の管理に使用するアドレスです。
管理ドメイン	共通のデータベースおよびセキュリティポリシーを共有するコンピュータのグループです。
キーロガー	キーロガーは、キーボードのすべての動きを捕捉して保存するプログラムです。企業が従業員を監視したり、親が子供を監視するために使用する、合法的なキーロギングプログラムもあります。しかし、犯罪者によってキーストロークのログが使用され、ログオン認証情報やクレジットカード番号などの重要な情報が利用されることもあります。
キャッシュ	最近アクセスしたデータを保持する、小さく高速なメモリ。同じデータに続けてアクセスする際の速度を上げるように設計されています。この用語は、プロセッサとメモリの間のアクセスに適用される場合が最も多いのですが、ネットワークを介してアクセス可能なデータのローカルコピーなどにも適用されます。
キュー	メールが処理可能な速度よりも速く受信される場合に、1つのリソースに対する複数の要求を一定の順序で配列するために使用するデータ構造です。FIFO (一番新しく格納されたものを一番最後に処理する) アプローチを使用して、メッセージはキューの末尾に追加され、キューの先頭にあるメッセージから処理されます。
共有ドライブ	複数のユーザが使用するコンピュータ周辺デバイスです。そのため、ウイルスにさらされる危険性が高まります。

用語	説明
駆除	ファイルまたはメッセージからウイルスコードを削除することをいいます。
クライアント	ある種のプロトコルを使用し、別のコンピュータシステムまたはプロセス (「サーバ」) のサービスを要求してサーバの応答を受け取る、コンピュータシステムまたはプロセスです。クライアントは、クライアントサーバソフトウェアアーキテクチャの一部です。
クライアント / サーバ環境	分散型システムの一般的な形式で、ソフトウェアがサーバのタスクとクライアントのタスクに分離されます。クライアントは、一定のプロトコルに従い、情報または処理を求めてサーバに要求を送信し、その要求にサーバが応答します。
グレーウェア	正規なプログラムではあるが、望ましくない、または不正な可能性のあるソフトウェアのカテゴリです。ウイルス、ワーム、およびトロイの木馬などの脅威とは異なり、感染、増殖、またはデータの破壊は行いませんが、プライバシーを侵害する可能性があります。グレーウェアの例には、スパイウェア、アドウェア、およびリモートアクセスツールなどがあります。
警告	システムのユーザまたは管理者に、システムの稼働状態の変化や、ある種のエラー状態について知らせることを目的としたメッセージです。
ゲートウェイ	情報源と Web サーバとの間のインターフェースです。
原因	URL ブロックやファイルブロックなど、保護処理が開始された理由です。この情報は、ログファイルに表示されます。
検索	ファイル内のアイテムを順番に調べて、特定の条件に一致するアイテムを探すことをいいます。
検索エンジン	ウイルス対策検索を実行したり、統合されているホスト製品の検出を実行するモジュールです。

用語	説明
公開鍵暗号方式	暗号化のスキームで、各ユーザは公開鍵と秘密鍵と呼ばれる一対の「鍵」を取得します。各ユーザの公開鍵は公開されていますが、秘密鍵は秘密にされています。メッセージは、目的の受信者の公開鍵を使用して暗号化され、受信者の秘密鍵を使用してのみ解読されます。「認証」および「デジタル署名」も参照してください。
サーバ	あるサービスを他の (クライアント) プログラムに提供するプログラムです。クライアントとサーバの間の接続は、通常、メッセージの伝達により実行されます。多くの場合ネットワークを介し、特定のプロトコルを使用してクライアントの要求とサーバの応答をエンコードします。サーバは、要求の到着を待って継続的に (デーモンとして) 稼働するか、または、いくつかの特定のサーバを制御するより高いレベルのプロセスによって呼び出されます。
サブネットマスク	<p>比較的大規模なネットワークでは、サブネットマスクを使用してサブネットワークを定義できます。たとえば、クラス B のネットワークがある場合、サブネットマスク 255.255.255.0 は、ピリオドで区切られた最初の 2 つの部分がネットワーク番号、3 番目の部分がサブネット番号を指定します。4 番目の部分はホスト番号です。クラス B のネットワークでサブネットを使用しない場合は、サブネットマスク 255.255.0.0 を使用します。</p> <p>1 つのネットワークは、メインネットワークのサブセットを形成する、1 つ以上の物理ネットワークにサブネット化できます。サブネットマスクは IP アドレスの一部であり、ネットワーク内のサブネットワークを表すのに使用します。サブネットマスクを使用して、通常は使用できないネットワークアドレスの領域を使用できるようにしたり、意図しない限りネットワークトラフィックがネットワーク全体に送信されないようにします。サブネットマスクは複雑な機能であり、使用する際には細心の注意を払う必要があります。「IP アドレス」も参照してください。</p>
シート	1 人のユーザがトレンドマイクロ製品を使用するためのライセンスのことです。
シグネチャ	「ウイルスシグネチャ」を参照してください。

用語	説明
実行可能ファイル	機械語のプログラムを含む、すぐに実行可能なバイナリファイルです。
実際のファイルタイプ	ウイルス検索技術で、ファイル名拡張子に関係なく（だまされる場合があります）、ファイルヘッダを調べることによってファイル内の情報の種類を特定します。
受信	お使いのネットワークに送信されてくる、メールメッセージまたはその他のデータです。
受信者	メールメッセージの宛先となるユーザまたはエンティティです。
使用許諾契約書 (EULA)	使用許諾契約書は、ソフトウェア公開者とソフトウェアユーザとの間の法的契約です。通常はユーザ側の規定について述べられています。ユーザはインストールの際に「同意します」をクリックしなければ、その契約を拒否できません。もちろん「同意しません」をクリックすると、ソフトウェア製品のインストールは終了します。 多くのユーザは、ある種のフリーソフトウェアのインストールの際に表示される使用許諾契約書の同意を求める画面で「同意します」をクリックして、スパイウェアやアドウェアのコンピュータへのインストールに不注意で同意してしまいます。
ジョークプログラム	ユーザを困らせたり不適切な警告を発したりする実行可能プログラムです。ウイルスとは異なり自己増殖しないので、システムから簡単に削除できます。
初期設定	Web コンソールのインタフェースで、あらかじめ入力されている値のことを指します。初期設定値は論理的な選択を表し、便宜上入力されています。初期設定値はそのまま使用することも、変更することもできます。
スクリプト	呼び出して一緒に実行できる、プログラミングコマンドのセットです。「スクリプト」と同義で使用される他の用語には、「マクロ」や「バッチファイル」があります。
スパイウェア	広告を目的としたソフトウェアで、通常はシステムに追跡ソフトウェアをインストールします。追跡ソフトウェアは、個人に関する情報を第三者に送信できます。スパイウェアの脅威は、収集されるデータやその使用目的をユーザが管理できないことにあります。

用語	説明
スパムメール	製品またはサービスの宣伝販売を目的として、無差別に送信されるメールメッセージです。
セキュリティホール	ソフトウェアの脆弱性などを利用するコードです。セキュリティホールは、脆弱なコンピュータの間で広まり、複雑なルーチンを実行できます。
セクタ	ディスクを物理的に分割した部分です（「パーティション」についても参照してください。パーティションは、ディスクを論理的に分割した部分です）。
設定	トレンドマイクロ製品をどのように機能させるかについてオプションを選択することをいいます。たとえば、ウイルスに感染したメールメッセージを隔離するか削除するかを選択します。
ゾーン	ゾーンには、セキュリティ基準が適用されるネットワークスペースのセグメント（セキュリティゾーン）、VPN トンネルインタフェースがバインドされる論理セグメント（トンネルゾーン）、または、特定の機能を実行する物理的または論理的エンティティ（機能ゾーン）があります。
増殖	自己複製することをいいます。このドキュメントでは、自己複製するウイルスやワームについて使用されます。
送信	お使いのネットワークからインターネットに送信される、メールメッセージまたはその他のデータです。
待機ポート	データ交換についてクライアント接続要求に使用するポートです。
対象 （「処理」および「通知」も参照）	メールメッセージで検出されるウイルスなど、イベントの違反について監視する活動の範囲を指します。たとえば、ウイルス検索について、ネットワークを通過するすべてのファイルを対象にしたり、特定のファイル名拡張子を含むファイルのみを対象にできます。
ダイヤラー	トロイの木馬の一種で、実行されると、ユーザのシステムをペイパーコールの通話先に接続します。疑いを持たないユーザは、知らない間に、その通話に対して請求されます。

用語	説明
ダウンロード	あるコンピュータから別のコンピュータへ、データまたはコードを転送することをいいます。ダウンロードとは、多くの場合、より大きな「ホスト」システム（特にサーバまたはメインフレーム）から、より小さな「クライアント」システムに転送することをいいます。
ダメージルーチン	ウイルスコードの破壊的な部分のことで、ペイロードとも呼ばれます。
通知 (「処理」および「対象」も参照)	次のいずれかまたは複数の宛先に送信されるメッセージです。 - システム管理者 - メッセージの送信者 - メッセージ、ファイルのダウンロード、またはファイル転送の受信者 通知の目的は、HTTP でのファイルダウンロードを試みた際に検出されたウイルスなど、禁止された処理が発生した、または試みられたことを知らせることです。
ディスクレマー	メールの先頭または最後尾に挿入されるメッセージ。メッセージは、メールの内容に関する法律厳守や守秘義務の条項を表します。
ディレクトリ	階層型のコンピュータファイルシステム構造の一部であるノードを指します。ディレクトリには、通常、別のノード、フォルダ、またはファイルが含まれます。たとえば、C:\Windows は、C ドライブの Windows ディレクトリです。
ディレクトリパス	ディレクトリ内の続いている層で、その先にファイルなどが存在します。
デーモン	明示的には実行されませんが、ある条件が発生するのを待って休止しているプログラムです。
デジタル署名	メッセージに付加される追加データです。公開鍵暗号方式という技術を使用して、メールの送信者とメッセージデータを識別し、認証します。「公開鍵暗号方式」および「認証」も参照してください。
出回っていないウイルス	現在ウイルス対策製品で制御されている、既知のウイルスを指します。「感染報告のあるウイルス」も参照してください。

用語	説明
添付ファイル	メールメッセージに添付されて一緒に送信されるファイルです。
トータルソリューション CD/DVD	最新製品バージョンとすべてのパッチが格納されている CD または DVD です。それらのパッチは、前の期間において適用されているものです。トータルソリューション CD または DVD は、トレンドマイクロ プレミアム サポートを受けるすべてのお客さまで利用できます。
登録	[ユーザ登録] 画面で製品のレジストレーションキーを使用して、お客さまをトレンドマイクロのユーザとして認識する処理です。 https://olr.trendmicro.com/registration
トップレベルドメイン	インターネットの完全修飾ドメイン名の最後にある最も重要な構成要素で、最後の「.」の後の部分です。たとえば、ホスト「trendmicro.co.jp」のトップレベルドメインは「jp」です。
ドメイン名	システムの完全な名前で、ローカルホスト名とドメイン名で構成されます。たとえば、example.com などです。ドメイン名は、インターネット上のすべてのホストに一意的インターネットアドレスを定めるのに十分なものである必要があります。この処理は「名前解決」と呼ばれ、Domain Name System (DNS) を使用します。
トラフィック	インターネットとお使いのネットワークの間を流れる送受信データです。
トリガ	活動の発生を引き起こすイベントです。たとえば、トレンドマイクロ製品がメールメッセージでウイルスを検出したとします。この「トリガ」により、メッセージが隔離ディレクトリに置かれ、システム管理者、メッセージの送信者、およびメッセージの受信者に通知が送信されます。
トレンドマイクロの推奨設定	トレンドマイクロの検索技術です。実際のファイルタイプによる認識を使用してファイルヘッダを調べ、潜在的に不正コードが潜んでいる可能性があると思われるファイルタイプのみを検索することにより、パフォーマンスを最適化します。実際のファイルタイプによる認識は、無害な拡張子名で偽装している可能性のある不正コードの識別に役立ちます。

用語	説明
トロイの木馬	害のないプログラムを装う不正プログラムです。トロイの木馬は実行可能プログラムです。増殖はせず、代わりにシステムに常駐して、侵入者に対してポートを開くなどの不正な行為を実行します。
ドロップ	ウイルス、トロイの木馬、またはワームをシステムに運ぶ送信メカニズムとして機能するプログラムです。
トンネリング	あるネットワークが別のネットワークの接続を介してデータを送信できる、データの送信方法です。トンネリングは、インターネットでサポートされないプロトコルを使用する管理ドメイン間のデータを、そのドメイン間でやり取りするために使用されます。 VPN トンネリングでは、モバイルプロフェッショナルは企業のネットワークに直接ダイヤルするのではなく、市内のインターネットサービスプロバイダのアクセスポイントにダイヤルします。これは、モバイルプロフェッショナルがどこにいても、VPN トンネリング技術をサポートする市内のインターネットサービスプロバイダにダイヤルして、市内通話の電話料金のみで企業のネットワークにアクセスできることを意味します。 リモートユーザが、VPN トンネリングをサポートするインターネットサービスプロバイダを使用して企業のネットワークにダイヤルすると、組織だけでなく、リモートユーザもその接続が安全であるとわかります。すべてのリモートダイヤルインユーザは、インターネットサービスプロバイダのサイトの認証サーバで認証されてから、企業のネットワークにある別の認証サーバで再度認証されます。これは、許可されたリモートユーザのみが企業のネットワークにアクセスでき、そのユーザによる使用が許可されたホストのみにアクセスできることを意味します。

用語	説明
トンネル インタフェース	トンネルインタフェースとは、トラフィックがVPN トンネルを通過するための通路または戸口を指します。トンネルインタフェースには、番号を付ける（つまり、IP アドレスを割り当てる）ことも、付けなくてもできます。番号の付いたトンネルインタフェースは、トンネルゾーンまたはセキュリティゾーンのいずれかに配置できます。番号の付いていないトンネルインタフェースは、少なくとも1つのセキュリティゾーンインタフェースを含むセキュリティゾーンにのみ配置できます。番号の付いていないトンネルインタフェースは、セキュリティゾーンインタフェースからIP アドレスを借用します。「VPN (Virtual Private Network)」も参照してください。
トンネルゾーン	1つ以上のトンネルインタフェースをホストする論理セグメントです。トンネルゾーンは、キャリアとして動作するセキュリティゾーンに関連付けられます。
認証	人またはプロセスの同一性の確認を行います。認証を使用することで、デジタルデータ伝送が、目的の受信者に対して確実に行われます。受信者側では、メッセージとその送信元（どこの誰から送られてきたか）が改変されていないことが保証されます。 認証の最も単純な形式では、特定のアカウントにアクセスするために、ユーザ名とパスワードが必要です。認証プロトコルは、秘密鍵暗号方式や、デジタル署名を使用する公開鍵システムを基にすることもできます。 「公開鍵暗号方式」および「デジタル署名」も参照してください。
ネットワークウイルス	TCP、FTP、UDP、HTTP、およびメールプロトコルなどのネットワークプロトコルを使用して増殖するタイプのウイルスです。ネットワークウイルスは、多くの場合、システムファイルの改ざんやハードディスクのブートセクタの変更は行いません。代わりにクライアントコンピュータのメモリに感染し、そのコンピュータを使用してネットワークのトラフィックをあふれさせて、ネットワークの速度低下や完全な機能不全さえも引き起こす可能性があります。
ページ	ログで古いエントリを削除することによりすべて削除することを指します。

用語	説明
配置ウィザード	Web コンソールベースのウィザードで、配信を容易にするために使用されます。配信関連の設定は、製品インストールからこのウィザードに移動されました。
バイナリ	数字の 0 と 1 で構成されるデータで、デジタル電子工学およびブール代数を使用した実装が容易なため、事実上すべてのコンピュータで使用されます。
パーティション	ディスクを論理的に分割した部分です（「セクタ」についても参照してください。セクタは、ディスクを物理的に分割した部分です）。
ハードディスク (またはハードディスク ドライブ)	中央の軸を中心に回転する、1 つまたは複数の固定された磁気ディスクです。ハードディスクまたはフロッピーディスクの読み書きやデータの保存に使用される、読み書き用のヘッドと電子機器を備えています。ほとんどのハードディスクはドライブ（固定されたディスク）に常時接続されていますが、取り外し可能なディスクもあります。
パスワード解析 アプリケーション	失効した、または忘れてしまったパスワードを取り戻すために使用するアプリケーションプログラムです。こうしたアプリケーションは、侵入者がコンピュータまたはネットワークリソースに権限を持たずにアクセスするために使用されることもあります。
パターンファイル (またはオフィシャル パターンリリース)	パターンファイルはオフィシャルパターンリリース（OPR）とも呼ばれ、確認済みのウイルスパターンを編集した最新版です。最新のウイルスの脅威から確実に保護されるよう、いくつもの厳しいテストを通過したことが保証されています。このパターンファイルは、最新の検索エンジンと併用すると最も効果的です。
ハッキングツール	不当に使用される恐れのあるセキュリティの脆弱性を発見する目的で、コンピュータシステムまたはネットワークへの侵入テストを実行できるようにする、ハードウェアおよびソフトウェアなどのツールです。
パッシブモード	FTP プロトコルの設定です。ローカルエリアネットワーク内のクライアントに、ランダムな上位ポート番号（1024 以上）を使用したファイル転送の開始を許可します。
パラメータ	値の範囲（1 ~ 10 の数）などの変数です。

用語	説明
非武装地帯 (DMZ)	元は軍事用語で、敵同士の間で戦闘が行われていない領域のことを指します。DMZ Ethernet は、異なる組織によって制御されているネットワークおよびコンピュータを接続します。これらの組織は外部または内部の可能性があり、外部 DMZ Ethernet は、ルータで地域のネットワークにリンクします。
ヒューリスティック ルールベースの検索	プロパティの論理分析を使用したネットワークトラフィックの検索で、ソリューションの検索を減らすまたは制限します。
ファイアウォール	特殊なセキュリティ対策を施したゲートウェイコンピュータで、外部ネットワーク (特にインターネット) の接続およびダイヤルイン回線に使用されます。
ファイル	データの要素で、メールメッセージや HTTP ダウンロードなどを指します。
ファイル感染型 ウイルス	<p>ファイル感染型ウイルスは、実行可能プログラム (一般的には、.com または .exe の拡張子を持つファイル) に感染します。こうしたウイルスのほとんどは、他のホストのプログラムに感染して増殖し、拡散しようとしませんが、ウイルスによっては、感染したプログラムのオリジナルコードの一部を上書きして不注意により破壊するものもあります。こうした少数のウイルスは非常に破壊的で、あらかじめ設定された時刻にハードディスクドライブをフォーマットしようとしたり、その他の不正な処理を実行しようとしたりします。</p> <p>多くの場合、ファイル感染型ウイルスは、感染ファイルから正常に削除できます。ただし、ウイルスがプログラムコードの一部を上書きした場合、オリジナルファイルは元に戻せません。</p>
ファイルタイプ	ファイルに保存されるデータの種類の種類です。ほとんどの OS では、ファイル名拡張子を使用してファイルタイプを特定します。ファイルタイプにより、そのファイルを表すユーザインタフェース上の適切なアイコンと、ファイルの表示、編集、実行、または印刷に使用する適切なアプリケーションが選択されます。

用語	説明
ファイルタイプグループ	共通のテーマを持つファイルの種類です。たとえば、次のものがあります。 オーディオ / ビデオ 圧縮 実行可能 画像 Java Microsoft Office
ファイル名拡張子	「.dll」や「.xml」など、ファイル名の一部で、ファイルに保存されているデータの種類を表します。ファイル名拡張子は、ファイル内の情報の種類を示すだけでなく、通常、ファイルの実行時に起動するプログラムを識別するのに使用されます。
不快なコンテンツ	冒涇、セクシュアルハラメント、人種に関する嫌がらせ、または中傷など、他人にとって不快と見なされるメッセージの語句または添付ファイルです。
負荷分散	負荷分散とは、同時に発生するコンピュータ処理の効率を高める目的で、複数のプロセッサに仕事を割り当てる（再割り当てする）ことをいいます。
複合的な脅威による攻撃	企業ネットワークの複数の侵入ポイントおよび脆弱性を利用する複合的な攻撃で、「Nimda」や「Code Red」などの脅威があります。
不正プログラム (不正ソフトウェア)	ウイルス、ワーム、およびトロイの木馬など、危害を与えることを目的として開発されるプログラムまたはファイルです。
ブラウザ	人間がハイパーテキストを読むようにするプログラムで、Internet Explorer などがあります。ブラウザを使用することにより、ノード（または「ページ」）の内容を表示したり、ノード間の移動が可能になります。ブラウザは、リモート Web サーバに対してはクライアントとして動作します。
プロキシサーバ	特殊な接頭辞が付いた URL を受け入れる Web サーバです。ローカルキャッシュまたはリモートサーバのいずれかから文書を取得して、その URL を要求者に返すために使用されます。

用語	説明
プログラム ディレクトリ	メインのアプリケーションファイルを保存する、インストール先のディレクトリです。たとえば、C:/Program Files/Trend Micro/IWSS などです。
ブロック	ネットワークへの侵入を防ぐことをいいます。
ヘッダ (ネットワーク定義)	ファイルまたは伝送に関する暗号化されていない情報を含む、データパケットの一部です。
ポート	通信システムの論理チャンネルまたはチャンネルの終点で、同じコンピュータの同じネットワークインタフェースにおいて、異なる論理チャンネルを区別するために使用されません。
保護された ネットワーク	IWSS (InterScan Web Security Suite) によって保護されたネットワークです。
ホスト	ネットワークに接続されたコンピュータ。
ポリシー	ポリシーは、ファイアウォールに対して最初の保護メカニズムを提供します。これを使用することにより、IP セッションの詳細に基づいて、どのトラフィックを通過させるかを決めることができます。ポリシーは、信頼するサーバの検索など、外部の攻撃から信頼するネットワークを保護します。ポリシーにより、ファイアウォールを通過しようとするトラフィックを監視するセキュリティポリシーを設定した環境を作成できます。
マクロ	アプリケーション内で特定の機能を自動的に実行するために使用されるコマンドです。
マクロウイルス	マクロウイルスは多くの場合、アプリケーションのマクロとしてコード化され、文書に含まれています。他のウイルスタイプと異なり、マクロウイルスは OS 特有のものではなく、メールの添付ファイル、Web ダウンロード、ファイル転送、および連携アプリケーションを介して広がる可能性があります。
マスメーリング型 ウイルス	大量のネットワークトラフィックを発生させるため大きな損害を与える可能性が高い、不正プログラムです。
ライセンス	トレンドマイクロ製品を使用するための法的な許可です。

用語	説明
ライセンス証明書	トレンドマイクロ製品の認定ユーザであることを証明する文書です。
リムーバブルドライブ	コンピュータの取り外し可能なハードウェアコンポーネントまたは周辺デバイスです。
リモート アクセスツール (RAT)	正当なシステム管理者がネットワークをリモートで管理できるようにする、ハードウェアおよびソフトウェアです。ただし、このようなツールは、侵入者がシステムのセキュリティを突破するために使用される可能性もあります。
リレー	さまざまな他のポイントを通過して伝送することをいいます。
リンク (ハイパーリンク とも呼ばれます)	あるハイパーテキスト文書内のポイントから、別の文書または同じ文書内の別のポイントへの参照です。リンクは通常、下線を引いた青いテキストなど、異なる色またはテキストスタイルで区別されます。たとえばマウスでリンクをクリックするなど、リンクをアクティブにすると、ブラウザにリンク先が表示されます。
ルータ	このハードウェア装置は、ローカルエリアネットワーク (LAN) から長距離回線にデータを発送します。
レジストレーション キー	ハイフンを含む 22 文字のコードで、トレンドマイクロの顧客データベースでの登録時に使用されます。レジストレーションキーの例 :SM-27RT-UY4Z-39HB-MNW8 「アクティベーションコード」も参照してください。
ローカルエリア ネットワーク (LAN)	Ethernet など、通常は高速でオフィス環境内のリソースを相互接続するネットワーク技術です。ローカルエリアネットワークは短距離のネットワークで、同じ建物内のコンピュータグループを互いに接続するために使用します。
ログ保存ディレクトリ	ログファイルを保存する、サーバ上のディレクトリです。
論理爆弾	アプリケーションまたは OS に不正に挿入されたコードで、指定された条件に一致するたびに、破壊的な、またはセキュリティを危険にさらす活動を実行します。

用語	説明
ワイルドカード	コンテンツフィルタの参照に関する用語で、アスタリスク (*) が任意の文字を表します。たとえば、*ber という表現は、barber、number、plumber、timber などを表すことができます。この用語は、トランプのゲームに由来します。トランプのゲームでは、特定のカードが「ワイルドカード」として識別されます。ワイルドカードは、ゲームで任意の数や組に使用できます。
ワークステーション (またはクライアント)	一度に 1 人のユーザが使用するよう設計された汎用コンピュータで、特に画像、処理能力、および複数のタスクを同時に実行する能力において、通常はパーソナルコンピュータよりも高いパフォーマンスを提供します。
ワーム	他のプログラムに寄生しないプログラム (またはプログラムセット) で、自身の機能のコピーを広めたり、セグメントを別のコンピュータシステムに送信します。
割り込み	通常の処理を中断し、「割り込みハンドラ」ルーチンを通じて制御の流れを一時的に変える、非同期のイベントです。

索引

英数字

AC 291

APT ブロック
レポート 227

Blue Coat アプライアンス
設定 56

C&C コールバック試行検出 158

C&C コンタクトアラート 38

C&C コンタクトアラート件数
レポート 227

C&C コンタクト検出 158
通知 248

ルール 178

Cisco CE ICAP サーバ 58

Control Manager
登録 279

CPU 使用率の表示 34

EICAR テストファイル 296

ESMTP 241

exception lists
file name 178

FTP

サービスのオン / オフ 214

匿名 96

ポートの制限 223

FTP over HTTP 92、172

FTP アクセス管理設定 222

宛先ポート 223

クライアント IP 222

除外するサーバ IP 223

FTP 検索 28

アクティブ 213

圧縮ファイル 216、218

ウイルスに対する検索処理 219

オプション 214

概要 212

隔離 217

検索するファイル 215

検索方向 215

サーバ IP の除外リスト 223

サイズの大きいファイル 216

除外リスト 217

スパイウェア 217

設定 212、213、216、217

通知 251

テスト 301

トラフィックの有効化 214

バッシュ 213

ファイルのブロック 215

プロキシ設定 212

有効化 214

優先順位 216

FTP ファイルタイプによるブロック通知 250

FTP プロキシ 213

HotFix 312

HTTP

検索するファイルタイプ 163

サービスのオン / オフ 88

セキュリティ脅威 39

- トラフィックの有効化 / 無効化 88
- ブロックするファイルタイプ 163
- ポート制限 100
- HTTP scanning
 - trusted URLs 189
- HTTPS
 - アクセス拒否
 - 通知 253
 - 暗号化ポリシー 147
 - 検索 96
 - 証明書エラー通知 254
 - セキュリティ 27
 - ポートの制限 101
- HTTPS 復号化 27、144
 - 検索
 - テスト 298
 - 設定 149
 - プロセスフロー 146
 - ポリシー
 - 作成 147
- HTTP 検査 24
 - 概要 120
 - 除外 125
 - テスト 303
 - フィルタ 125
 - フィルタ、エクスポート 140
 - フィルタ、PCRE フラグ 134
 - フィルタ、インポート 138
 - フィルタ、基本ビュー 129
 - フィルタ、詳細ビュー 135
 - フィルタ、初期設定 126、127
 - フィルタ、追加 129
 - フィルタ、パケットの取り込み 130
 - フィルタ、編集 138
 - フィルタ、メソッドの値 131
 - ポリシー 121
 - ポリシーの追加 121
 - ルールの指定 122
- HTTP 検索
 - 圧縮ファイル 167
 - イントラネットサイト 189
 - 隔離 173
 - 検索イベント 183
 - 検索処理 182
 - 検索するファイル 163
 - サイズの大きいファイル 168
 - 指定 309
 - セキュリティ設定 168
 - 設定 87
 - 遅延検索 170、172
 - 通知 252
 - 配信前に検索 169、172
 - パフォーマンス 174
 - ファイルの除外 174
 - ファイルのブロック 163
 - ポリシーの作成 / 変更 155
 - 優先順位 167
 - ルール 162
- ICAP
 - 設定 50
 - 要求
 - 待機 61

- ICAP モード 45
 - 応答 61
 - キャッシュサーバ 56
 - 設置後のタスク 55
 - 要求 61
- IntelliTrap
 - 除外パターンファイル 71
 - パターンファイル 71
- IWSS
 - 主な機能 24
 - 機能 24
 - コンポーネント 346
 - サービス 346
 - 設定 268、295
 - テスト 295、314
 - モジュール 346
- Java Runtime 57
- LDAP
 - AD グローバルカタログ 115
 - サポートされるディレクトリ 110
 - 接続のテスト 115
 - 設定 113
 - 通信フロー 111
 - 内部キャッシュ 315
 - 認証 110
 - パフォーマンスの調整 315
- logs
 - configure syslog server 240
- MIME タイプ 165、175、323
- Readme 20
- RealAudio 165
 - register_user_agent_header.exe 110
- REQMOD 99
- RESPMOD 99
- Smart Protection Network 355、356、357
- SNMP 29
 - 設定 292
 - トラップ通知 263
- SolutionBank - 製品 Q&A Web サイトを参照 20
- SSL ハンドシェイク
 - 概要 145
- syslog 30
 - syslog サーバ
 - 設定 240
- TTL 186
- URL
 - 登録 66
- URL アクセス
 - オーバーライド
 - 通知 258
 - 概要 188
 - 警告 207
 - 警告通知 257
 - 設定 189
- URL 監視
 - テスト 304
- URL キャッシュ
 - クリア 162
- URL 検索 204
- URL の再分類 204
- URL フィルタ 28、73、314
 - 安全な検索 202

- 概要 196
- カスタマイズ 196
- カスタムカテゴリ 203
- カテゴリ 359
- カテゴリの管理 204
- 再分類 205
- 時間制限処理 197
- 時間設定 206
- 時間割り当て通知 262
- 時間割り当てによる延長 208
- 仕組み 198
- 除外 206、207
- 処理 197
- スケジュール 206
- 設定 203
- 設定の見直し 314
- 通知 260、261
- データベース 73
- テスト 307
- パスワードオーバーライド処理 197
- ポリシー、概要 199
- ポリシーの管理 199
- ポリシーの作成 200
- 有効化 199、200
- URL ブロック 191
- HTTP 検査通知 260
- URL フィルタ通知 261
- アクセス管理通知 259、261
- インポート 193
- リストのインポート 194
- ローカルリスト 192

- ワイルドカード 193
- Visual Policy Manager 57
- Web
 - 脅威
 - 情報 36
 - コンソール 293
- Web レピュテーション
 - 結果の管理 160
 - 設定 159
 - テスト 296
 - フィードバックオプション 160
 - ルールの指定 157
- WRS キャッシュ
 - クリア 162
- X-Forwarded-For HTTP ヘッダ 175
 - 設定 177
 - 配信シナリオ 176
 - 利用可能な処理 176
- 検索エンジン 72
- 予約 232

あ

- あいさつの受信 219
- アカウント
 - 管理 282
 - 追加 282
 - 変更 283
- アクセス管理
 - FTP 222
 - クライアント IP 98
 - クライアント / サーバの識別 97

- 設定 97、292、310
- アクセス管理通知による URL ブロック 259
- アクセスの警告
 - 生存期限 (TTL) 207
- アクセス割り当て 185
 - 概要 186
 - 管理 186
 - ダウンロード中の超過 186
 - 追加 186
 - ポリシーの削除 187
 - ポリシーの無効化 187
- アクセス割り当てポリシー 310
- アクティブモード 213
- アクティブーションコード 291
- 圧縮ファイル 218
 - セキュリティ設定 168
- アップデート 66、74
 - Control Manager を使用しない 67
 - 強制 75
 - 検索エンジン 72
 - コンポーネント 68、74
 - 差分 74
 - 差分アップデート 74
 - システムアップデート 288
 - 手動 74
 - 推奨 67
 - 通知 77、256
 - プロキシ設定 67
 - 予約 67、76
 - 予約アップデートの無効化 76
 - ロールバック 77
- アップロード検索
 - テスト 297
- 宛先ポート (FTP) 224
- アプリケーション制御 24
 - 概要 80
 - テスト 302
 - ポリシーの追加 82
 - ポリシーの表示 81
 - ポリシーの編集 83
 - ポリシーリスト 80
 - ルールの指定 84
- アプリケーションパッチ
 - 削除 311
 - 追加 311
- 安全な検索 202
- 依存モード 90
- インターネットアクセス
 - レポート 228
- インターネットセキュリティ
 - レポート 227
- ウイルス
 - 感染報告のあるウイルス 72
 - 検索 27
 - 処理 219
 - 設定 88
 - 検索エンジン 69
 - サーバクラスタの検索 59
 - 処理 182
 - 出回っていないウイルス 72
 - パターンファイルの提供 70
 - ウイルス対策検索エンジン 69

- オンラインヘルプ 20
- か
 - 隔離
 - 管理 277
 - ディレクトリ 277
 - ファイル
 - 暗号化 217、278
 - カスタムカテゴリ 203
 - カスタム保護
 - 設定 159
 - 監査ログ 267
 - 管理
 - アカウント 282
 - メニュー
 - 概要 266
 - 管理コンソール 282
 - パスワード 313
 - 期限切れの警告 290
 - キャッシュ
 - コンテンツ 61
 - 消去 61
 - ポリシー設定 313
 - キャッシュ生存期限 186
 - キャッシュの消去 61
 - 強制アップデート 77
 - クライアント IP アドレスとユーザ ID 間のキャッシュ 315
 - クライアント証明書の処理 150
 - クラウドベースのサービス 355
 - クラスタ
 - 設定 60
 - グループ
 - レポート 227
 - グローバルポリシー 105
 - ゲスト
 - アカウント 309
 - ポート
 - 有効化 107
 - ポリシー 106
 - 概要 106
 - 検索
 - 考慮事項 355
 - ファイルタイプの選択 164
 - モジュール 352
 - ルール
 - スパイウェア 173
 - 検索エンジン 356
 - アップデート 73
 - アップデートを開始するイベント 73
 - 検索エンジンのアップデート通知 260、261
 - 検証 149
 - 誤警報 77
 - コマンド & コントロールコンタクトアラート
 - C&C コンタクトアラートを参照 38
 - さ
 - サーバ IP アドレスの許可リスト
 - ICAP モード 99
 - サーバの追加 99
 - サーバクラスタ 59
 - 削除 60

- サーバ証明書の検証 149
 - サービスバック 312
 - サイズの大きいファイルの処理
 - HTTP 97、168
 - 重要な注意 172
 - 遅延検索 172
 - 差分パターンファイルアップデート 74
 - サポート 293
 - サポート契約
 - 更新 66、291
 - しきい値アラートの通知 32
 - システム
 - アップデート 288
 - イベント 289
 - 情報の設定 292
 - 実際のファイルタイプ 164
 - 上位プロキシ (依存) モードの設定 48
 - 冗長ログ 316
 - 証明書
 - インポート 151
 - 機関 151
 - エクスポート 153
 - 除外 URL
 - リスト形式 181
 - 除外リスト
 - URL 178
 - 作成 179
 - 処理
 - 駆除不能ファイル (FTP) 220
 - パスワードで保護されたファイル (FTP) 220
 - マクロの検索 (FTP) 220
 - 新機能 31
 - 信頼する URL 189
 - インポート 190
 - 管理 190
 - スタンドアロンプロキシモードの設定 47
 - スパイウェア
 - 検索ルール 173
 - 定義済み 173
 - パターンファイル 70、71
 - スパイウェア検索
 - テスト 308
 - 製品
 - ライセンス 289
 - 製品 Q&A 20
 - セキュリティ情報センター 315
 - セキュリティパッチ 312
 - 設置
 - Blue Coat アプライアンス 56、58
 - 設定 295
 - カスタム保護 159
 - バックアップと復元 287
 - ファイル 345、350
 - レポート 226
 - その他の脅威
 - 定義 173
- た
- 帯域幅
 - レポート 228
 - 待機ポート 95、314
 - ダウンロード検索

- テスト 306
- ダッシュボード 54
- 通常の透過モード 46
- 通知 29、219
 - C&C コンタクト検出 248
 - ESMTP のサポート 241
 - FTP 検索 251
 - FTP ファイルタイプによるブロック 250
 - HTML タグの使用 247
 - HTTP/HTTPS 検索 252
 - HTTP/HTTPS ファイルタイプによるブロック 251
 - HTTPS アクセス拒否 253
 - HTTPS 証明書エラー 254
 - HTTP 検査通知による URL ブロック 260
 - SNMP トラップ 263
 - URL アクセスのオーバーライド 258
 - URL アクセスの警告 257
 - URL フィルタ 260、261
 - URL フィルタエンジンの有効化 261
 - URL フィルタ通知による URL ブロック 261
 - アクセス管理による URL ブロック 259
- 概要 240
- 管理者とユーザ 240
- 検索エンジンのアップデート 260、261
- 検索エンジンのアップデートの有効化 261
- 時間割り当てによる URL フィルタ 262
- しきい値アラート 32
- 設定 247
 - パターンファイルアップデート 256
 - パラメータ 242
 - 変数 242
 - 変数の使用 242
 - メール設定 241
- 通知の変数 242
- データセキュリティレポート 229
- データベース
 - 接続 277
 - 接続設定 313
 - 接続のテスト 313
- データベース接続テスト 313
- ディレクトリ (LDAP) サーバパフォーマンス 315
- テスト 295
 - FTP 検索 301
 - HTTPS 復号化検索 298
 - HTTP 検査 303
 - URL 監視 304
 - URL フィルタ 304、307
 - Web レピュテーション 296
 - アップロード検索 297
 - アプリケーション制御 302
 - スパイウェア検索 308
 - ダウンロード検索 306
 - データベース接続 313
- 透過 92
- 同時接続数の表示 33
- 登録
 - URL 66
 - プロファイル 66

ドキュメント 20
匿名 FTP 96
トレンドマイクロの推奨設定 163

は

ハードディスクドライブの表示 35
配置 42
 配置ウィザード 42
配置ウィザード 41
 ICAP の設定 50
 ICAP モード 45
 概要 42
 上位プロキシ (依存) モードの設定 48
 スタンドアロンプロキシモードの設定 47
 通常の透過モード 46
 フロー 42
 プロキシ設定 47
 プロキシ転送モード 43、47
 モード固有の設定 47
 モード選択 42
 リバースプロキシの設定 49
 リバースプロキシモード 44
パスワード 313
 作成のヒント 313
パターンファイル 68、69
 一致 69
サーバ上に複数 70
削除 78
 手動削除 78
スパイウェア 70、71
番号 70

バックアップと復元 287
バッシュモード 213
パッチ 312
ハニーネット 158
パフォーマンスの調整 315
 LDAP 315
ファイルタイプ 164
 指定 (FTP) 215
 ブロック 163
ファイル名
 リスト形式 181
復元 287
複合型脅威 39
複数設置 31
不正プログラム検索 27
物理メモリ使用率の表示 34
プロキシ
 キャッシュ 90
 上位プロキシあり (依存モード) 90
 スタンドアロンモード 89
 設定 47、67、88、90、95
 待機ポート 95
 リバース 31、94
プロキシ転送モード 43、47
プロトコルハンドラ 351
ベイロード 38
ベストプラクティス
 検索エンジン 356
 検索に関する考慮事項 355
 提案 356
変数

- 通知の使用 242
 - ボット 380
 - ボットネット検出 158
 - レポート 227
 - ポリシー
 - 仕組み 104
 - 実例 104
 - 初期設定 105
 - 配信 276
 - 範囲の設定 116
 - 備考欄への入力 184
 - リクエストモード 58
 - レスポンスモード 57
 - ポリシー施行
 - レポート 229
 - ま
 - マクロ検索 183
 - 処理 182
 - モード固有の設定 47
 - や
 - ユーザ
 - レポート 227
 - ユーザ / グループ名認証 (LDAP) 309
 - ユーザグループメンバーシップキャッシュ 315
 - ユーザ識別方法 29、103
 - IP アドレス 117、109
 - クライアント登録ユーティリティ 109
 - 種類 108
 - 設定 108、309
 - ホスト名 109
 - ユーザ / グループ名認証 110
 - ユーザ認証キャッシュ 316
 - 用語集 371
 - 予約タスク 348
 - 予約レポート 232
- ら
- ライセンス
 - アップデート 291
 - 期限切れの警告 290
 - 製品 289
 - リバースプロキシ 94
 - 設定 94
 - モード 44
 - モードの設定 49
 - レジストレーション
 - キー 290
 - レポート 30
 - APT ブロック 227
 - C&C コンタクトアラート件数 227
 - CPU 使用率の表示 34
 - インターネットアクセス 228
 - インターネットセキュリティ 227
 - 概要 226
 - カスタマイズ 233
 - グループ 227
 - 種類 226、227、231
 - 使用可能 231
 - 設定 226、227
 - 帯域幅 228

- 追加設定 227
 - データセキュリティ 229
 - 同時接続数の表示 33
 - ハードディスクドライブの表示 35
 - 物理メモリ使用率の表示 34
 - ポットネット検出 227
 - ポリシー施行 229
 - ユーザ 227
 - 予約 232
 - 予約の削除 232
 - リアルタイム 230
 - ロールバック 77
 - ログ 30
 - CSV ファイル形式でのエクスポート 239
 - PDF ファイル形式でのエクスポート 239
 - 概要 233
 - クエリ / 表示 236
 - システムイベント 289
 - 設定 237
 - ログの設定 237
 - ログファイル
 - 命名規則 239
- わ
- ワイルドカード 193

