

Trend Micro InterScan VirusWall™ スタンダードエディション



安心を、ひとつ上のステージへ。



管理者ガイド

※注意事項

トレンドマイクロへのお客様情報の送信について

- 「Webレピュテーションサービス」「フィッシング詐欺対策」「有害サイト規制/URLフィルタリング」では、Webサイトの安全性の判定のために、お客様がアクセスしたURLの情報等(ドメイン、IPアドレス等を含む)を暗号化してトレンドマイクロのサーバに送信します。サーバに送信されたURL情報は、Webサイトの安全性の確認、および本機能の改良の目的にのみ利用されます。また、これらの機能を有効にしたうえで、Webページにアクセスした場合、以下の事象がおこることがあります。
(a)お客様がアクセスしたWebページのWebサーバ側の仕様が、お客様が入力した情報等をURLのオプション情報として付加しWebサーバへ送信する仕様の場合、URLのオプション情報にお客様の入力した情報(ID、パスワード等)などを含んだURLがトレンドマイクロのサーバに送信される。この場合、トレンドマイクロでは、お客様がアクセスするWebページの安全性の確認のため、これらのお客様より受領した情報にもとづき、お客様がアクセスするWebページのセキュリティチェックを実施します。
- 「ファイルレピュテーションサービス」では、ファイルの安全性の判定のために、ファイルのハッシュ値等の情報をトレンドマイクロのサーバに送信します。ファイルそのものや、ファイルの内容に関する情報は送信しません。
- 「ソフトウェア安全性評価サービス/脅威情報の送信」では、プログラムの安全性の判定のために、プログラムまたはプログラムの情報をトレンドマイクロのサーバに送信します。
- 「ウイルストラッキング/TrendCareプログラム」では、検出されたウイルス/脅威名、検出数、国/地域、感染元となったWebサイトのURLを、統計を取るためにトレンドマイクロのサーバに送信します。
- 「迷惑メール対策ツール」では、弊社製品の改良の目的および迷惑メールの判定精度の向上のため、トレンドマイクロのサーバに該当メールを送信します。また、迷惑メールの削減、迷惑メールによる被害の抑制を目指している政府関係機関に対して迷惑メール本体を開示する場合があります。
- 「E-mailレピュテーションサービス」では、スパムメールの判定のために、送信元のメールサーバの情報をトレンドマイクロのサーバに送信します。
- 「スマートフィードバック」では、脅威に関する情報を収集、分析し保護を強化するために、ファイルのチェックサム、アクセスされたWebアドレス、サイズやパス等のファイル情報、実行ファイルの名前等の情報をトレンドマイクロのサーバに送信します。

輸出規制について

本製品は、外国為替及び外国貿易法、U.S. Export Administration Regulations、およびその他の国における輸出規制品目に該当している場合があります。したがって、本製品が輸出規制品目に該当する場合、適正な政府の許可なくして、禁輸国もしくは貿易制裁国の企業、居住者、国民、または、取引禁止者、取引禁止企業に対して、輸出もしくは再輸出できません。このような規制についての情報は以下のWebサイトから見つけることができます。
「<http://www.treas.gov/offices/enforcement/ofac/>」および「<http://www.bis.doc.gov/complianceand enforcement/ListsToCheck.htm>」

2009年7月現在、米国により定められる禁輸国は、キューバ、イラン、北朝鮮、スーダン、シリアが含まれています。

あなたは本製品に関連した米国輸出管理法の違法行為に対して責任があります。本契約の同意により、あなたは、あなたが米国により現時点で禁止されている国の居住者もしくは国民ではないこと、別途本製品を受け取ることが禁止されていないことを確認します。また、大量破壊を目的とした、核兵器、化学兵器、生物兵器、ミサイルの開発、設計、製造、生産を行うために使用しないことに同意します。

複数年契約について

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

著作権について

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

商標について

TRENDMICRO、ウイルスバスター、ウイルスバスター On-Line-Scan、PC-cillin、InterScan、INTERSCAN VIRUSWALL、ISVW、InterScan Web Manager、ISWM、InterScan Message Security Suite、InterScan Web Security Suite、IWSS、TRENDMICRO SERVERPROTECT、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、トレンドマイクロ・プレミアム・サポート・プログラム、License for Enterprise Information Security、LEISec、Trend Park、Trend Labs、InterScan Gateway Security Appliance、Trend Micro Network VirusWall、Network VirusWall Enforcer、Trend Flex Security、LEAKPROOF、Trend プロテクト、Expert on Guard、InterScan Messaging Security Appliance、InterScan Web Security Appliance、InterScan Messaging Hosted Security、DataDNA、Trend Micro Threat Management Solution、Trend Micro Threat Management Services、Trend Micro Threat Management Agent、Trend Micro Threat Mitigator、Trend Micro Threat Discovery Appliance、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、Smart Protection Network、およびSPNは、トレンドマイクロ株式会社の登録商標です。

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

Copyright © 2003-2009 Trend Micro Incorporated. All rights reserved.

P/N: ISSENT-AE0300 (2009/10)

目次

はじめに	17
InterScan VirusWall のドキュメント	18
対象読者	19
ドキュメントの表記規則	19
 第 1 章 製品の概要	21
機能と利点	22
新機能	24
InterScan VirusWall のしくみ	25
通知	26
InterScan VirusWall によるウイルスの検出方法	26
MacroTrap	26
圧縮ファイル	27
トレンドマイクロの推奨設定	27
InterScan VirusWall によるフィッシングの脅威の検出方法	28
 第 2 章 インストールの計画	29
インストールの概要	29
システム要件	30
ドメインコントローラエージェントの要件	31
事前計画	32
インストール先を決定する	33
セットアップの選択	33
インストールのトポロジ	34
SMTP	34
POP3	36

POP3 (ポートマッピング)	37
FTP	38
HTTP	40
HTTP リバースプロキシ	42
InterScan VirusWall のインストール前の作業	43
 第 3 章 インストール	45
インストールシナリオ	45
InterScan VirusWall を新規インストールする	46
以前のバージョンがインストールされているコンピュータに インストールする	50
新しいコンピュータにインストールして以前のバージョンの設定を 移行する	54
新しいコンピュータにインストールしてバージョン 6.0 または 6.02 の 設定を移行する	54
以前のバージョンからのコマンドラインによる移行	58
InterScan VirusWall 6.0 または 6.02 から InterScan VirusWall 7.0 への コマンドラインによる移行	58
インストール後の作業	59
Web コンソールを開く	61
InterScan VirusWall を起動 / 停止する	61
InterScan VirusWall をテストする	62
InterScan VirusWall を削除する	62
 第 4 章 SMTP サービスの設定	63
SMTP サービスを有効または無効にする	64
SMTP ウイルス検索を設定する	64
SMTP ウイルス検索機能	65
SMTP ウイルス検索を有効にする	65
検索するファイルタイプを指定する	65

圧縮ファイルの処理を設定する	67
マクロ検索を有効にする	68
ウイルス検出時に実行する処理を指定する	69
ウイルス検索通知を設定する	71
ウイルス検出時の通知設定を指定する	71
インライン通知設定を指定する	72
SMTP ファイル全体検索	73
IntelliTrap を設定する	75
SMTP IntelliTrap 検索を有効または無効にする	76
IntelliTrap による検出時の処理を指定する	76
IntelliTrap 通知を設定する	77
SMTP フィッシング対策を設定する	79
SMTP フィッシング対策を有効にする	80
フィッシングメールの検出時に実行する処理を指定する	80
フィッシングメール検出時の通知を指定する	82
フィッシングサイトの可能性のある URL を報告する	83
SMTP スпамメール対策を設定する	84
SMTP スпамメール対策 (メールレピュテーション) を有効にする	85
サービスレベルを設定する	85
承認する IP アドレスリストを管理する	86
メールレピュテーションの処理を設定する	86
SMTP スпамメール対策 (コンテンツ検索) を有効にする	87
スパムメール検出レベルを設定する (フィルタ調整)	87
スパムメール検出レベル	88
スパムメール検出レベルを決定する	88
スパムメールフィルタを調整する	89
キーワード除外を指定する	89
承認する送信者およびブロックする送信者のリストを管理する	90
スパムメールと見なされたメッセージに対する処理を指定する	91
スパムメール検出時の通知を指定する	93

SMTP スパイウェア対策を設定する	94
SMTP スパイウェア検索 (受信または送信) を有効にする	96
スパイウェア検索の除外リストを設定する	97
検索するスパイウェアおよびグレーウェアの種類を指定する	97
スパイウェア検出時に実行する処理を指定する	98
スパイウェアの検出時の通知を指定する	99
SMTP コンテンツフィルタ	101
SMTP コンテンツフィルタを有効にする	101
SMTP コンテンツフィルタを無効にする	102
ポリシーを作成する	102
キーワードに基づいた SMTP コンテンツフィルタポリシーを作成する	102
キーワードフィルタに基づいたポリシーを追加する	106
コンテンツフィルタ用の SMTP 添付ファイルフィルタポリシーを 作成する	111
SMTP コンテンツフィルタ添付ファイルポリシーの処理を設定する	114
SMTP コンテンツフィルタポリシーをコピーまたは削除する	116
SMTP 設定	117
SMTP サービスを設定する	118
受信メッセージを設定する	118
InterScan VirusWall と SMTP サーバが同じコンピュータ上にある場合	119
InterScan VirusWall と SMTP サーバが異なるコンピュータ上に ある場合	119
送信メッセージを設定する	119
メールキューを使用する	120
詳細設定のオプション	120
同時 SMTP クライアント接続数の上限 : __	121
受信メッセージ / 送信メッセージの最大サイズ : __	121
DNS 配信が使用されている場合は、最長で __ 時間、__ 分ごとに メッセージ送信を試行する	121
処理済みメッセージに InterScan の「Received」ヘッダを挿入しない	121

次のドメイン宛ての受信メールのみを許可して、リレーされた メッセージをブロックする：__	122
接続が確立されたときに次の SMTP グリーティングメッセージを 送信する：__	122
SMTP トランザクションログを有効にする	122
 第 5 章 HTTP サービスの設定	125
HTTP サービスを有効または無効にする	126
HTTP ウイルス検索を設定する	126
HTTP ウイルス検索を有効にする	127
検索するファイルタイプを指定する	127
圧縮ファイルの処理	129
MIME タイプの除外	130
サイズの大きいファイルの処理	134
ウイルス検出時に実行する処理を指定する	135
ウイルス検索の通知メッセージを指定する	137
HTTP フィッシング対策を設定する	137
HTTP フィッシング対策を有効にする	138
フィッシング検出時に実行する処理を指定する	138
フィッシングサイト検出時の通知メッセージを指定する	139
ユーザ通知を指定する	139
フィッシングサイトの可能性のある URL を報告する	139
HTTP スパイウェア対策を設定する	139
HTTP スパイウェア検索を有効にする	140
スパイウェア検索の除外リストを設定する	141
検索するスパイウェアおよびグレーウェアの種類を指定する	142
スパイウェア検出時に実行する処理を指定する	142
スパイウェア / グレーウェア検出時のユーザ通知メッセージを指定する	143
HTTP URL ブロックおよび URL フィルタ	143
URL ブロックおよび URL フィルタのグローバルポリシーを管理する	144

URL ブロックおよび URL フィルタのポリシーの優先順位を管理する	145
新しい URL ブロックおよび URL フィルタのポリシーを作成する	145
既存の URL ブロックおよび URL フィルタのポリシーを変更する	151
URL ブロックおよび URL フィルタの設定	152
URL ブロックおよび URL フィルタを有効にする	152
URL フィルタのスケジュールを設定する	152
ブロックされた URL についてのメッセージを指定する	153
URL の見直し	153
URL ブロックおよび URL フィルタのポリシーを削除する	156
Web レピュテーション	156
Web レピュテーションを使用したフィッシング対策	157
Web レピュテーションデータベース	157
Web レピュテーション設定	158
セキュリティ検出レベル	158
Web レピュテーションの除外	158
HTTP 設定	159
スタンドアロンモード	160
依存プロキシモード	160
リバースプロキシモード	161
透過モード	161
HTTP プロキシを設定する	162
特定のネットワークインタフェースにバインドする	163
クライアントブラウザでプロキシを設定する (Internet Explorer)	163
HTTP トランザクションログを有効にする	165
 第 6 章 FTP サービスの設定	 167
FTP サービスを有効または無効にする	167
FTP ウイルス検索を設定する	168
FTP ウイルス検索を有効にする	169

検索するファイルタイプを指定する	169
圧縮ファイルの処理	170
ウイルス検出時に実行する処理を指定する	171
ウイルス検索の通知メッセージを指定する	172
FTP スパイウェア対策を設定する	173
FTP スパイウェア検索を有効にする	174
スパイウェア検索の除外リストを設定する	175
検索するスパイウェアおよびグレーウェアの種類を指定する	176
スパイウェア検出時に実行する処理を指定する	176
スパイウェア / グレーウェア検出時のユーザ通知メッセージを指定する	176
FTP 設定	177
スタンドアロンモード	177
FTP プロキシモードを使用する	178
FTP プロキシサーバを設定する	179
FTP トランザクションログを有効にする	180
第 7 章 POP3 サービスの設定.....	183
POP3 サービスを有効または無効にする	184
POP3 ウイルス検索を設定する	184
POP3 ウイルス検索機能	185
POP3 ウイルス検索を有効にする	185
検索するファイルタイプを指定する	185
圧縮ファイルの処理を設定する	186
ウイルス検出時に実行する処理を指定する	187
ウイルス検索通知を設定する	187
InterScan VirusWall によるウイルス検出時の通知設定を指定する	188
インライン通知設定を指定する	188
POP3 ファイル全体検索	189
ファイル全体検索の動作	190

POP3 ファイル全体検索を設定する	190
ファイル全体検索を有効または無効にする	190
処理を設定する	191
通知を送信する	193
ディスクレーマー文を変更する	194
IntelliTrap を設定する	194
POP3 IntelliTrap 検索を有効または無効にする	195
IntelliTrap の検出時の処理を指定する	195
IntelliTrap 通知を設定する	195
POP3 フィッシング対策を設定する	196
POP3 フィッシング対策を有効にする	197
フィッシング検出時の処理を指定する	197
フィッシングサイトの検出時の通知を設定する	197
フィッシングサイトの可能性のある URL を報告する	198
POP3 スパムメール対策を設定する	198
POP3 スパムメール対策を有効にする	199
スパムメール検出レベルを設定する (フィルタ調整)	200
スパムメール検出レベル	201
スパムメール検出レベルを決定する	201
スパムメールフィルタを調整する	202
キーワード除外を指定する	202
承認する送信者およびブロックする送信者のリストを管理する	203
スパムメールと見なされたメッセージに対する処理を指定する	205
InterScan VirusWall によるスパムメールの検出時の通知を指定する	206
POP3 スパイウェア対策を設定する	207
POP3 スパイウェア検索を有効にする	208
スパイウェア検索の除外リストを設定する	208
検索するスパイウェアおよびグレーウェアの種類を指定する	209
スパイウェア検出時に実行する処理を指定する	209

スパイウェア検出時の通知を指定する	210
POP3 コンテンツフィルタ	211
POP3 コンテンツフィルタを有効にする	211
POP3 コンテンツフィルタを無効にする	211
ポリシーを作成する	212
キーワードに基づいた POP3 コンテンツフィルタポリシーを作成する	212
キーワードフィルタに基づいたポリシーを追加する	215
添付ファイルフィルタに基づいた POP3 コンテンツフィルタポリシーを 作成する	217
POP3 コンテンツフィルタポリシーの処理を設定する	219
POP3 コンテンツフィルタポリシーをコピーまたは削除する	220
POP3 設定	220
POP3 IP アドレスを指定する	221
同時接続の最大数を設定する	221
POP3 接続を指定する	221
POP3 ポートマッピング	221
Outlook Express を設定する	222
POP3 トランザクションログを有効にする	224
 第 8 章 大規模感染予防サービス	 225
大規模感染予防サービスを有効にする	225
表示可能な現在のステータス	226
大規模感染予防サービスを設定する	227
 第 9 章 隔離	 229
隔離クエリ	229
クエリを生成する	230
クエリ結果を操作する	231
隔離ディレクトリの設定	232

隔離ディレクトリの管理	233
自動メンテナンス	233
手動メンテナンス	234
第 10 章 アップデート	237
アップデートに対応したコンポーネント	238
トレンドマイクロ製品によるセキュリティの脅威の検出方法	239
ウイルスパターンファイルの差分アップデート	239
コンポーネントを手動でアップデートする	239
[概要] 画面でコンポーネントを表示およびアップデートする	240
手動アップデートを使用してコンポーネントをアップデートする	241
アップデートを予約する	242
InterScan VirusWall をアップデートする	242
第 11 章 ローカルレポート	245
レポートプロファイルの管理	245
新しいレポートプロファイルを作成する	246
レポートの頻度を指定する	247
既存のレポートプロファイルを変更する	248
レポートプロファイルを削除する	248
生成されたレポートの管理	248
生成されたレポートを表示する	249
生成されたレポートを削除する	249
レポート管理の実行	250
第 12 章 ログ	251
ログクエリ	252
クエリ結果テーブルのフィールド	255
ログ管理	257

ログの自動削除	257
ログの手動削除	259
デバッグログとシステムログ	260
第 13 章 管理	261
InterScan VirusWall のアクティベート	261
InterScan VirusWall をアクティベートする	261
アクティベーションの詳細	264
管理機能の使用	264
Control Manager を設定する	264
InterScan VirusWall がサポートする Control Manager の機能	267
通知設定	268
パスワード	270
プロキシ設定	270
ウイルストラッキングセンター	272
ユーザ ID 設定	272
ユーザ識別方法を選択する	272
ドメインコントローラエージェントについて	274
ドメインコントローラエージェントをインストールする	275
InterScan VirusWall にドメインコントローラエージェントを 追加する	277
InterScan VirusWall からドメインコントローラエージェントを 削除する	278
InterScan VirusWall のドメインコントローラサーバを検出する	279
ドメインコントローラサーバの資格情報を追加する	279

第 14 章 リアルタイム検索モニタの使用..... 281**第 15 章 トラブルシューティングとサポート..... 285**

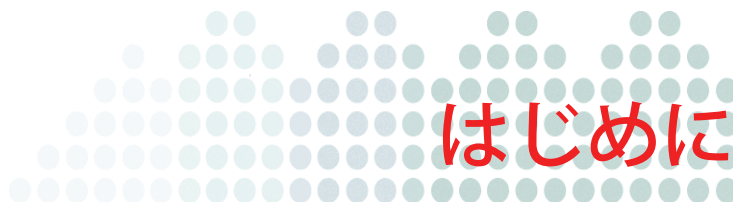
トラブルシューティング	286
ドメインコントローラエージェントのデバッグ	294
ドメインコントローラエージェントのデバッグを有効にする	294
コンソールモード	294
ドメインコントローラエージェント、Active Directory、およびユーザ識別の トラブルシューティング	296
ドメインコントローラエージェントのインストールまたはサービスでの エラー	296
ドメインコントローラエージェントの接続	296
ドメインコントローラサーバの接続	300
ドメインコントローラサーバの自動検出	301
接続	302
Windows Active Directory によるユーザ / グループの検索	305
ユーザ識別	305
データを収集してトレンドマイクロのサポートに送信する	307
製品サポート情報	307
サポートサービスについて	307
製品 Q&A のご案内	308
セキュリティ情報	308
セキュリティ情報の入手先	308
トレンドマイクロへのウイルス解析依頼	309
ウイルス解析サポートセンター「TrendLabs」	309

付録 A システムチェックリスト..... 311

サーバアドレスのチェックリスト	311
ポートのチェックリスト	312

サポートされているコマンド	313
SMTP	313
FTP	313
POP3	314
 付録 B 初期設定値	 315
SMTP ウイルス / スパイウェア / IntelliTrap および設定	316
SMTP コンテンツフィルタ	335
SMTP スпамメール対策	336
SMTP フィッシング対策	338
POP3 ウイルス / スパイウェア / IntelliTrap 検索	339
POP3 コンテンツフィルタ	349
POP3 スпамメール対策	349
POP3 フィッシング対策	350
POP3 設定	352
HTTP	352
FTP	360
ログ	363
隔離	365
大規模感染予防サービス	365
アップデート	366
パターンファイルのアップデート通知の初期設定値	366
 付録 C InterScan VirusWall 6.0 または 6.02 からの移行	 369
 付録 D Trend Micro Control Manager の複製制限	 371
複製されないプロトコル固有の設定	372
複製されない SMTP 固有の設定	372
複製されない HTTP 固有の設定	372

複製されない FTP 固有の設定	373
複製されない POP3 固有の設定	373
複製されない InterScan VirusWall 固有の設定	375
大規模感染予防	375
隔離	375
アップデート	375
ログ	375
管理	376
複製されないその他の InterScan VirusWall ユーザインタフェース項目と 設定	376



はじめに

Trend Micro InterScan VirusWall スタンダードエディション（以下、InterScan VirusWall）管理者ガイドへようこそ。本書では、InterScan VirusWall の設定オプションについて詳しく説明します。インストールおよび配信オプション、セキュリティアップデートを最新に維持する方法、Web およびメールトラフィックを不正なウイルス / スパイウェア / スパムメールやフィッシングトラフィックから保護する方法、ユーザのセキュリティ方針に応じたポリシーの設定および使用方法、検索の設定、URL ブロックと URL フィルタの設定、およびセキュリティイベントのレポートの生成に関するトピックが含まれています。

ここでは、次のトピックについて説明します。

- 「InterScan VirusWall のドキュメント」
- 「対象読者」
- 「ドキュメントの表記規則」

InterScan VirusWall のドキュメント

InterScan VirusWall には、次のドキュメントが付属しています。

- **クイックスタートガイド** — InterScan VirusWall の紹介、インストールの計画 / 導入 / 設定の支援、およびアップグレード後の主な設定タスクの説明を通じて、InterScan VirusWall の導入や運用の開始を可能にします。無害なテストウイルスを使用したプログラムのテスト、トラブルシューティング、およびサポートへの問い合わせの各手順についても説明します。
- **オンラインヘルプ** — オンラインヘルプの目的は、製品の主要なタスク、使用方法のヒント、および有効なパラメータ範囲や最適値などの実際の運用環境特有の情報を提供することです。オンラインヘルプは、InterScan VirusWall の Web コンソールからアクセスできます。
- **Readme ファイル** — オンラインドキュメントやマニュアルにはない最新の製品情報が記載されています。新しい機能、インストールのヒント、既知の問題、およびリリースの履歴などについて説明します。

クイックスタートガイド、管理者ガイド、および Readme ファイルの最新版は次の Web サイトからダウンロードできます。

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

- **製品 Q&A** — 問題の解決方法やトラブルシューティング情報を集めたオンラインデータベースです。製品の既知の問題に関する最新情報が提供されています。製品 Q&A には、次の Web サイトからアクセスできます。

<http://esupport.trendmicro.co.jp/>

ヒント： ドキュメントおよびプログラムファイルの最新版については、最新版ダウンロードサイト (<http://www.trendmicro.co.jp/download/>) から該当するリンクにアクセスしてチェックすることをお勧めします。

対象読者

InterScan VirusWall のドキュメントは、以下を含むセキュリティシステムについて基本的な知識があることを前提としています。

- HTTP、SMTP、POP3、および FTP プロトコル
- Windows ネットワーク、メールのセットアップ、および Microsoft Active Directory の管理についての経験

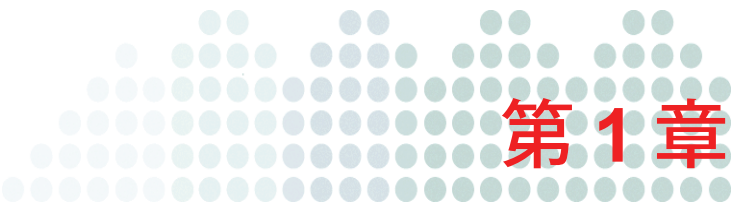
ウイルス対策や Web セキュリティテクノロジーに関する知識は必要ありません。

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



第1章

製品の概要

Trend Micro InterScan VirusWall スタンダードエディション（以下、InterScan VirusWall）は、企業ネットワークのゲートウェイウイルス対策、スパムメール対策、スパイウェア / グレーウェア対策、およびコンテンツ検索またはコンテンツフィルタの機能を提供するオールインワンのソリューションです。たとえば、ウイルス対策、スパムメール検出、またはコンテンツフィルタのためにアプリケーションを個々にインストールする必要はありません。使いやすい1つのアプリケーションでこれらの機能をすべて利用できます。InterScan VirusWall では、SMTP、POP3、HTTP、および FTP トラフィックの保護機能が提供され、社内でこれらのプロトコルを使用して送受信されるメールやダウンロードファイルからウイルスに感染することがないようにします。さらに、InterScan VirusWall では、SMTP および POP3 トラフィックに対するヒューリスティック方式によるスパムメール対策とコンテンツ検索を利用できます。

InterScan VirusWall は、容易にセットアップできるように設定が簡素化され、毎日の保守を最低限に抑えられるので、時間や IT リソースが限られ、リアルタイムのウイルス / スパムメール予防サービスを必要とする管理者に特に有用です。

既存の InterScan VirusWall の管理者が以前の製品バージョンから移行できるように、移行ツールが提供されています。

機能と利点

InterScan VirusWall の機能および利点は、次のとおりです。

表 1-1. InterScan VirusWall 機能と利点

機能	説明
オールインワンの防御	ウイルス対策、スパムメール対策、スパイウェア / グレーウェア対策、フィッシング対策、IntelliTrap (ボット対策)、コンテンツフィルタ、大規模感染予防サービス、URL ブロック、URL フィルタ、および SMTP 用メールレピュテーション IntelliTrap は、リアルタイム、ルールベース、およびパターン認識の検索エンジンのテクノロジーです。IntelliTrap は、最大で 20 階層の深さまで圧縮された、16 の主要な圧縮形式のファイルで既知のウイルスを検出して削除します。
自動的な脅威対策	大規模感染予防を Trend Micro Control Manager (以下、Control Manager) と組み合わせて使用することにより全面的な保護を提供
スケーラビリティ	4 つの全サービスを 1 つのサーバにインストールするか、または複数のサーバに分散インストールするかを選択することにより、中小企業にも大企業にも適した配置が可能
ゲートウェイ保護	インターネットゲートウェイでの不正プログラムの予防
柔軟な設定	検索対象ファイル、感染ファイル / メッセージに対する処理、および感染ファイル / メッセージの通知メッセージの受信者を指定可能
集中管理	全社的なインターネットセキュリティポリシーを実施する、ローカルシステムまたはリモートシステムからアクセス可能な Web ベースのコンソール
自動的な保守	自社固有のニーズを満たすように設定および自動化された、アップデート、レポート、警告などの定型業務

表 1-1. InterScan VirusWall 機能と利点 (続き)

機能	説明
簡単なインストール	インストールウィザードがインストールおよび一部の設定タスクを簡素化 InterScan VirusWall のセットアッププログラムには、システム要件、ディスク容量要件、必要な Service Pack または Patch、および使用可能である必要のあるポートについて互換性を確認する機能があります。この機能を使用すると、InterScan VirusWall は、体験版環境で他の製品と共存できるようになります。
ローカルレポート	レポートでは、多くの種類のトラフィック違反の概要を示すことができるようになりました。レポートには、発生したウイルスおよびウイルスの発生日時と場所が含まれます。レポートに、指定した期間内に違反が生じたユーザを、違反の種類と頻度と共に含めることもできます。InterScan VirusWall では、SMTP、HTTP、POP3、および FTP プロトコルについてレポートを生成できます。レポートを予約することも、1 回限りのレポートを生成することもできます。
InterScan VirusWall 6.0、6.02 ユーザ向けの移行ツール	InterScan VirusWall 6.0、6.02 のユーザは、InterScan VirusWall 7.0 へのアップグレード時に設定を簡単に移行できます。

新機能

InterScan VirusWall は最新の不正プログラムの脅威からネットワークを保護する新機能を備えています。今回のリリースで追加された機能には、スパムメール、スパイウェア、グレーウェア、ボット、およびフィッシングへの対策、URL フィルタおよび URL ブロック、および大規模感染予防サービスによる保護などがあります。

バージョン 7.0 の新機能のリスト

新機能	説明
Web レピュテーションを使用したフィッシング対策	本製品には、Web レピュテーション、URL フィルタ、およびフィッシングパターンファイルを使用したフィッシング対策が用意されています。Web レピュテーションでは、新たな Web からの脅威に対してエンドユーザが保護されます。また、Web レピュテーションでは、評価スコアが URL に割り当てられます。アクセスされる URL ごとに、Web レピュテーションで評価スコアがクエリされ、このスコアがユーザ指定の検出レベルより上か下かによって、その URL へのアクセスの許可やブロック、またはウイルス検索の実行が決定されます。
Windows ユーザ / グループのサポート (ドメインコントローラエージェントおよびサーバを使用したユーザの識別)	ユーザ ID 設定では、InterScan VirusWall 経由で HTTP 接続を行っている組織内の個々のユーザおよびグループを識別できます。トレンドマイクロのドメインコントローラエージェントは、Windows ベースのディレクトリサービスでユーザに透過的なユーザ識別を提供します。ドメインコントローラエージェントは、ドメインコントローラサーバと通信し、最新のユーザログオン情報を収集して InterScan VirusWall に提供します。この情報は、特定のユーザおよびグループに適用される URL フィルタおよび URL ブロックのポリシーの作成に使用できます。
ユーザ / グループベースの URL ブロックおよび URL フィルタのポリシー設定	URL ブロックおよび URL フィルタのルールを、特定のコンピュータ、ユーザ、またはグループに適用できます。InterScan VirusWall は、ネットワーク内の Active Directory サーバと通信するドメインコントローラエージェントと呼ばれるプラグインを使用して、ポリシーを設定できるユーザまたはグループを特定します。この機能には、ID 設定、Microsoft Active Directory サービスのサポート、ポリシーアイテムの管理、およびユーザまたはグループ単位のログおよびレポートが含まれます。

バージョン 7.0 の新機能のリスト (続き)

新機能	説明
改善されたレポート作成機能	レポートでは、多くの種類のトラフィック違反の概要を示すことができるようになりました。レポートには、発生したウイルスおよびウイルスの発生日時と場所が含まれます。レポートに、指定した期間内に違反が生じたユーザを、違反の種類と頻度と共に含めることもできます。InterScan VirusWall では、SMTP、HTTP、POP3、および FTP プロトコルについてレポートを生成できます。レポートを予約することも、1 回限りのレポートを生成することもできます。
インストール時のシステム要件確認機能	InterScan VirusWall のセットアッププログラムには、同時にインストールされるすべての製品のシステム要件、ディスク容量要件、必要な Service Pack または Patch、実行する必要があるサービス、および使用可能である必要のあるポートに関して、他のトレンドマイクロ製品およびサードパーティ製コンポーネントとの互換性を確認する機能が追加されました。この機能を使用すると、InterScan VirusWall は、体験版環境で他の製品と共存できるようになります。
以前のバージョンからの容易な移行	バージョン 6.0 または 6.02 から本バージョンへ簡単に移行できます。
Trend Micro Control Manager 5.0 のサポート	Trend Micro Control Manager 5.0 がサポートされます。

InterScan VirusWall のしくみ

InterScan VirusWall は、企業ネットワークとインターネットの間のすべての SMTP、POP3、HTTP、および FTP トラフィックでウイルスを検索します。検索するよう設定されているファイルタイプ (zip、.exe、.doc など) が検出されると、InterScan VirusWall はファイルを一時的な場所にコピーして、ウイルスを検索します。ファイルに問題がなければ、InterScan VirusWall はファイルのコピーを削除し、元のファイルを送信先に転送します。ウイルスが見つかった場合は、通知が発行され、InterScan VirusWall は次のいずれかの設定された処理を実行します。

- ・ 感染ファイルを自動駆除して元のサーバに送信します。ファイルは通常どおり配信されます。
- ・ 感染ファイルを駆除せずに隔離して、隔離ディレクトリに配置します。ファイルは配信されません。
- ・ 感染ファイルをブロックします。ファイルは配信されません。
- ・ 感染ファイルを削除します。ファイルは配信されません。

- ・ 感染ファイルを駆除せずに配信します。感染ファイルは、オプションの通知メッセージと共に配信されます。

通知

SMTP および POP3 トラフィックの場合、InterScan VirusWall では、システム管理者、送信者、および対象の受信者に通知を自動的に送信できます。ウイルスが見つからなかった場合は、メールが検索済みでウイルスが含まれていないことを示すメッセージを追加できます。HTTP および FTP トラフィックの場合、通知はエンドユーザのみに表示される「インライン通知」になります。

InterScan VirusWall によるウイルスの検出方法

パターンマッチングと呼ばれる処理を使用して、ウイルスパターンが多数蓄積されたデータベースを基に、既知のウイルスシグネチャが識別されます。疑わしいファイルの重要な領域で、ウイルスコード特有の文字列が検査され、トレンドマイクロで記録に載せている何万ものウイルスシグネチャと比較されます。

ポリモーフィック型ウイルス、つまりミューテーション型ウイルスについては、InterScan VirusWall の検索エンジンでは疑わしいファイルの一時的な環境での実行が許可されます。ファイルを実行すると、ファイル内に埋め込まれている暗号化されたウイルスコードが復号化されます。InterScan VirusWall は、復号化したコードも含めてファイル全体を検索し、ミューテーション型ウイルスの文字列がないか調べ、駆除、削除、隔離、配信など、指定されている処理を実行します。

新しい脅威は絶えず発見されているため、ウイルスパターンファイルを最新の状態にしておくことが重要です。トレンドマイクロでは、自動アップデート機能をサポートすることによって、ウイルスパターンファイルを簡単にアップデートできるようにしています。

MacroTrap

マクロウイルスは、特定の OS に限定されず、アプリケーション固有であるため、DOS、Windows、Macintosh、さらには OS/2 システムの間で広がるおそれがあります。マクロウイルスに対抗するため、トレンドマイクロでは、企業ネットワークを保護する能力を大幅に強化するインテリジェントテクノロジー MacroTrap を開発しました。

MacroTrap のしくみ

MacroTrap は、文書に関連付けて保存されているすべてのマクロコードにルールベースの検査を行います。マクロウイルスのコードは通常、文書に付随している見えないテンプレート (Microsoft Word の場合は .DOT など) の一部として組み込まれています。トレンドマイクロの MacroTrap は、テンプレートの各部分を他のテンプレートにコピーしたり (複製)、有害なコマンドを実行したり (破壊) するなど、ウイルスと同じような動作を実行する命令を探し出すことで、テンプレートに不明なマクロウイルスの兆候がないかどうかを調べます。

圧縮ファイル

InterScan VirusWall は、圧縮ファイルを開き、各 InterScan VirusWall のファイル検索オプションで指定されている条件に従って内容を検査します。複数階層の圧縮ファイルの場合は、各圧縮ファイルの解凍を最大 20 回繰り返します。たとえば、アーカイブに、pk-zip や winzip のような一般的な圧縮ツールを使用して圧縮されている .cab ファイルが含まれる場合、InterScan VirusWall は、圧縮されたファイルがなくなるまで (この時点で、圧縮ファイルに含まれているすべてのファイルは検査済みです)、または上限の 20 回に達するまで、各層を解凍します。

トレンドマイクロの推奨設定

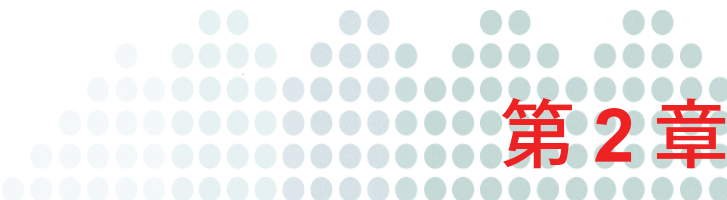
パフォーマンスを最大化するため、トレンドマイクロの推奨設定では、検索するファイルおよび検索方法がインテリジェントな方法で選択されます。感染し、ウイルスを運ぶ可能性があるタイプのファイルのみが検索されます。また、これらのファイルの重要な領域のみでウイルスシグネチャの照合が実行されます。膨大な既知のウイルス情報が含まれているトレンドマイクロ独自のデータベースと比較して、ファイルが検査されます。InterScan VirusWall は、ヒューリスティックロジックを使用して、特定の不明コード (ポリモーフィック型ウイルスに固有のコードなど) の性質がウイルスに似ているかどうかを分析し、テストを実行します。

InterScan VirusWall によるフィッシングの脅威の検出方法

InterScan VirusWall では、フィッシングの脅威が次の方法で検出されます。

- パターンファイルベースのフィルタが SMTP、HTTP、および POP3 メールに適用されます。
- フィッシング対策は InterScan VirusWall と連携して機能し、クライアントの送信 URL リクエストを監視して、既知のフィッシングサイトのリストと比較します。リストに一致するサイトがある場合、フィッシング対策では、そのサイトへのアクセスをブロックします。
- URL フィルタでは、フィッシングのカテゴリに従って URL がブロックされます。
- Web レピュテーションでは、評価スコアに従って URL がブロックされます。

パターンファイルベースのフィルタのみで、フィッシング固有の通知メッセージを使用できます。最後の 2 つの方法には、サイトをブロックする理由としてフィッシングを個別に識別しない、一般的な通知メッセージが使用されます。



第2章

インストールの計画

Trend Micro InterScan VirusWall スタンダードエディション（以下、InterScan VirusWall）のインストールに要する時間は約 10 分です。インストールは、InterScan VirusWall を配置するコンピュータで実行する必要があります。既存のサーバと連携して機能するように InterScan VirusWall を設定するには、さらに 10 ～ 15 分を必要とします。

InterScan VirusWall 6.0x から本バージョンに移行する場合、InterScan VirusWall には移行ツールが用意されており、以前のバージョンから設定をエクスポートして本バージョンにインポートできます。

インストールの概要

InterScan VirusWall のゲートウェイ用アプリケーションには、LAN との間のメール（SMTP と POP3）、Web（HTTP）、およびファイル転送（FTP）のウイルスを調べるリアルタイム検索サービスが含まれています。

すべてのサービスを同一コンピュータにインストールできます。ただし、通常は、複数のサービスを同一サーバにインストールしないことをお勧めします。サーバの通常の動作に加え、リアルタイムでネットワークトラフィックストリームを検索すると、CPU およびディスクへの負担が大きくなる可能性があるためです。セットアップを数回繰り返し実行して InterScan VirusWall を複数のサーバにインストールしてから、各サーバの各サービスをアクティブにする方法がより一般的です。たとえば、セットアップを 1 回実行して SMTP サービスと POP3 サービスを SMTP サーバにインス

トールし、セットアップをもう一度実行して HTTP サービスを別の HTTP プロキシサーバにインストールし、さらにセットアップを実行して、FTP サービスを別の FTP サーバにインストールします。

システム要件

注意： 詳細は、弊社の「最新版ダウンロード」サイトにある最新の Readme を参照してください。

ドメインコントローラエージェントの要件

表 2-1. ドメインコントローラエージェントの要件

要件	説明
ドメインコントローラエージェント	- ドメインコントローラエージェントを実行するよう指定されたコンピュータ (ドメインコントローラサーバと同じ OS 上で実行することをお勧めします)。 - ドメインコントローラエージェントのコンピュータは Windows ドメインに属している必要があります。 - ドメインコントローラエージェントコンピュータで、TCP ポート 65015 上の受信トラフィックを許可するようにファイアウォールを設定する必要があります。
ドメインコントローラサーバ	- Active Directory がインストールされている Windows 2000、2003、または 2008 プラットフォーム。 - ドメインコントローラサーバのログオンイベントの監査を有効にします。 [スタート] → [コントロール パネル] → [管理ツール] の順に選択します。 [ドメイン コントローラ セキュリティ ポリシー] をクリックします。 - 左側の画面で [ローカル ポリシー] を開き、[監査ポリシー] を選択します。 [アカウント ログオン イベントの監査] が有効になっていることを確認します。 305 ページの「ユーザ識別」を参照してください。 - ドメインコントローラサーバのセキュリティログのログローテーション / リサイクルを有効にします。 [スタート] → [コントロール パネル] → [管理ツール] の順に選択します。 [イベント ビューア] をクリックします。 - 左側の画面で [イベント ビューア] を開き、[セキュリティ] を選択します。 [操作] → [プロパティ] の順に選択し、[セキュリティのプロパティ] 画面を開きます。 - ログサイズが適切に設定されていて、[イベントを上書きする] オプションが選択されていることを確認します。 - ドメインコントローラサーバにファイアウォールが設定されている場合は、RPC およびリモートイベントアクセス用に TCP ポート 135 および TCP ポート 445 で受信トラフィックを許可するように除外を設定します。
InterScan VirusWall	- InterScan VirusWall のユーザ ID 設定を IP アドレスおよびユーザ名に設定します (272 ページの「ユーザ識別方法を選択する」を参照してください)。 - ドメインコントローラエージェントコンピュータの IP アドレス。 - ドメイン管理者権限のあるユーザアカウント。

表 2-1. ドメインコントローラエージェントの要件 (続き)

要件	説明
Windows クライアント	- クライアントコンピュータで実行されているリモートレジストリサービス。 - ドメインアカウントを使用したログオン。 - ファイアウォールが設定されている場合は、TCP ポート 445 で受信 RPC トラフィックを許可するように除外を設定します。

事前計画

初期設定では、InterScan VirusWall は、処理する SMTP メッセージの受信にポート 25、HTTP プロキシにポート 8080、FTP プロキシサーバにポート 21、POP3 受信メッセージにポート 110 をそれぞれ使用します。

インストールされているサービスおよびシステムで使用しているプロキシサーバに応じて、次の情報の把握が必要な場合があります。

- 現在の SMTP サーバの IP アドレス
- 現在の SMTP サーバのポート番号 (通常は 25)
- 現在の POP3 サーバの IP アドレス
- 現在の POP3 サーバのポート番号 (通常は 110)
- 現在の HTTP プロキシサーバの IP アドレス (設定する場合)
- 現在の HTTP プロキシサーバのポート番号
- InterScan VirusWall を HTTP プロキシサーバとして設定する場合に InterScan VirusWall で使用するポート番号
- 現在の FTP プロキシサーバの IP アドレス (設定する場合)
- 現在の FTP プロキシサーバのポート番号
- InterScan VirusWall を FTP プロキシサーバとして設定する場合に InterScan VirusWall で使用するポート番号

付録 A に、適切なサーバアドレスおよびポートの指定に役立つチェックリストがあります。

インストール先を決定する

InterScan VirusWall は、元のサーバと同じコンピュータにインストールすることも、別のコンピュータにインストールすることもできます。ほとんどの場合、インストール先を決めるうえで最も重要な点は、追加負荷を適切に処理できるだけの十分なリソースがインストール先のコンピュータにあるかどうかということです。

InterScan VirusWall をインストールする前に、サーバで処理するピークトラフィック負荷と平均トラフィック負荷を評価し、結果をコンピュータ全体の能力と比較する必要があります。両者の測定値に近いほど、InterScan VirusWall を専用コンピュータにインストールする可能性が大きくなります。考慮する別の要素として、ネットワーク帯域幅、現在の CPU 負荷、CPU 速度、システムメモリの総容量と使用可能な容量、および仮想メモリスパースの総量があります。リアルタイムでウイルスのネットワークプロトコルを 1 つ以上検索すると、リソースを集中利用する可能性があります。追加負荷を処理する能力がないコンピュータには、InterScan VirusWall をインストールしないでください。

セットアップの選択

同じコンピュータ — InterScan VirusWall をメールサーバまたは Web サーバと同じコンピュータにインストールする際、ほとんどの場合に、元のサーバが使用するポートの変更と InterScan VirusWall での初期設定の使用が必要になります。

通常の初期設定は次のとおりです。FTP: 21、SMTP: 25、HTTP: 80、POP3: 110。

専用コンピュータ — InterScan VirusWall が検索するサーバとは別のコンピュータに InterScan VirusWall をインストールする場合、既存サーバのポート番号を変更する必要はありません。ただし、InterScan VirusWall コンピュータの新しい IP アドレス（またはホスト名）を反映するようにクライアントの変更が必要になる場合があります。クライアントを変更しない場合は、次の点を検討してください。

- 2 台のコンピュータ間で IP アドレス（またはホスト名）を入れ替えて、InterScan VirusWall で元の IP アドレス（またはホスト名）を使用できるようにします。
- 論理上、インターネット、メールサーバ、および HTTP プロキシサーバの間になるように InterScan VirusWall をインストールします。

インストールのトポロジ

トレンドマイクロは、適切に設定されたファイアウォールの直後、またはネットワークアドレス変換 (NAT) とファイアウォールタイプと同等の他の保護を提供するセキュリティデバイスの直後に InterScan VirusWall をインストールすることをお勧めします。

目的に応じて InterScan VirusWall を設定することにより、多様なトポロジに対応できます。これらのトポロジは、1 つのサーバに InterScan VirusWall をインストールして全サービスをそのサーバ上で有効にする統合配置から、複数のサーバで InterScan VirusWall インストールを実行して各サーバ上の目的のサービスだけを有効にする、スタンドアロンまで多岐にわたります。

想定されるトポロジには次のようなものがあります。

- 統合配置 : InterScan VirusWall を 1 つのサーバにインストールし、そのサーバ上で SMTP VirusWall、POP3 VirusWall、FTP VirusWall、および HTTP VirusWall を有効化
- メッセージング /Web 配置 :
 - メッセージングサーバの場合は、InterScan VirusWall を別のハードウェアにインストールし、インストール時に SMTP および POP3 ウイルス検索を有効化
 - Web セキュリティ配置の場合は、InterScan VirusWall のインストール時に HTTP および FTP ウイルス検索オプションを有効化
- スタンドアロン配置 : InterScan VirusWall を 4 つの異なるサーバにインストールし、各サーバで 1 つのサービスだけを有効化

以降のページでは、InterScan VirusWall のインストール前後の一般的なネットワークセットアップを示しながら、想定されるいくつかのインストールトポロジを説明します。ニーズに最適なトポロジを使用するか、ネットワークに固有のインストール方法にこれらの原理を適用してください。

SMTP

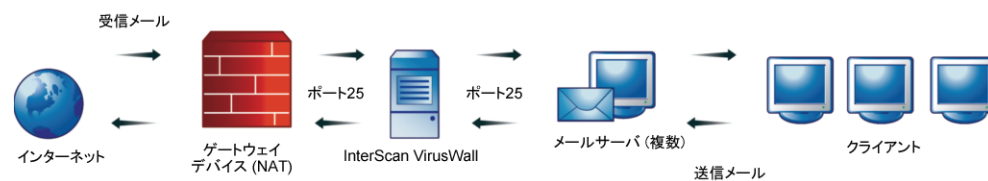
新規にインストールした、待機ポート 25 の InterScan VirusWall サーバにファイアウォールの SMTP サービス (ポート 25) を再度割り当てます。次に、受信メール転送 (シングルサーバ環境) または DNS (マルチサーバ環境) を使用して、検索済みのメールを 1 つ以上の内部メールサーバに転送します。DNS を使用する場合は、内部 MX レコードが正しく設定されていることを確認します。

これらの作業で、内部メールサーバの IP アドレスを変更する必要はありません。また、クライアントコンピュータではそれぞれのメールサーバへの接続が継続されるため、これらのコンピュータの設定も変更不要です。

InterScan VirusWall のインストール前



InterScan VirusWall のインストール後 (InterScan VirusWall とメールサーバを異なるコンピュータにインストール)



サーバ構成	
メインサービスポート:	25
受信メール	
☐ 次のSMTPサーバにメールを転送する:	ポート 25
☒ メール配信にDNSを使用する	
☒ 受信メッセージのIDをログに記録	

転送 — 検索されるメールは1つのメールサーバにのみ転送されます。
 DNS — 複数のメールサーバが対象

InterScan VirusWall のインストール後 (InterScan VirusWall とメールサーバを同じコンピュータにインストール)

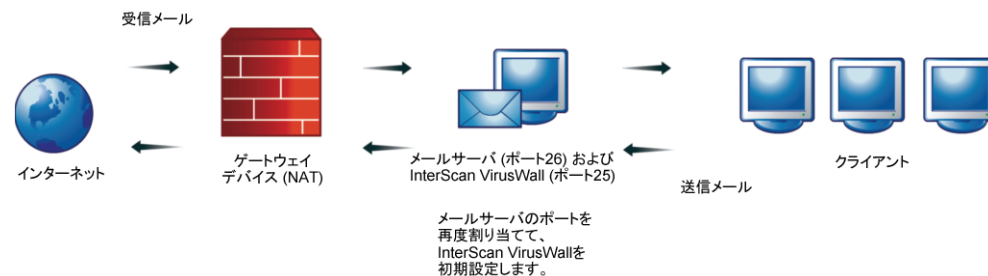


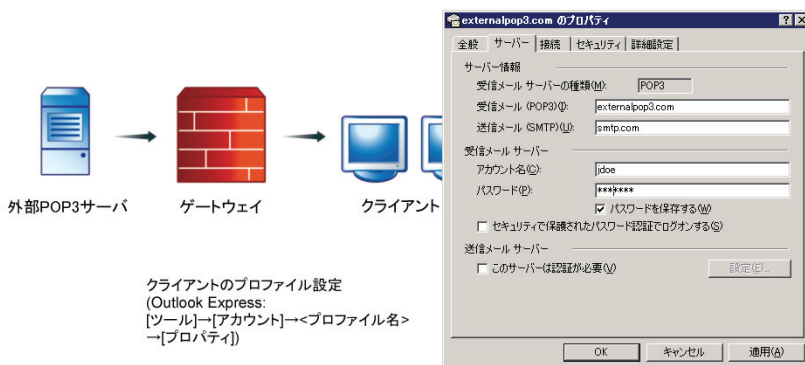
図 2-1. SMTP インストールプロセス

POP3

標準的な POP3 トポロジでは、クライアントが InterScan VirusWall からメールを直接受信できるようにクライアントコンピュータの POP3 設定を変更する必要があります。クライアントのメールボックス名を {メールボックス名} {POP3 サーバ} {ポート番号} に変更します。

たとえば、「joedoe」から「joedoe#externalpop3.com#110」に変更します。

InterScan VirusWall のインストール前



InterScan VirusWall のインストール後

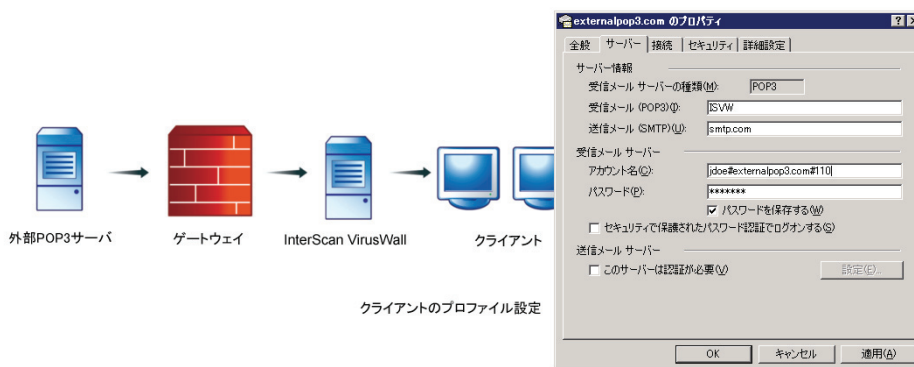


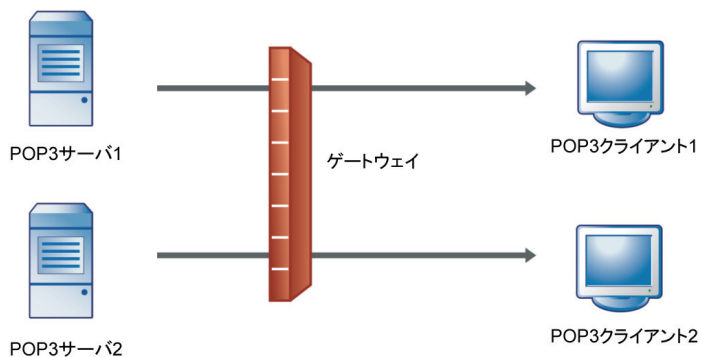
図 2-2. 標準的な POP3 インストールトポロジ

POP3 (ポートマッピング)

InterScan VirusWall をポートマッピングサーバとして設定する場合、ポートは InterScan VirusWall および特定の POP3 サーバの待機ポートにマップされます。このトポロジに必要な変更は次のとおりです。

- Web コンソールで [POP3] → [設定] の順に選択し、InterScan VirusWall で使用するポートを受信 POP3 ポートとして指定します。
- クライアントコンピュータの POP3 設定で、InterScan VirusWall サーバの名前とポート番号を受信メールサーバの名前とポート番号として指定します。

InterScan VirusWall のインストール前



InterScan VirusWall のインストール後

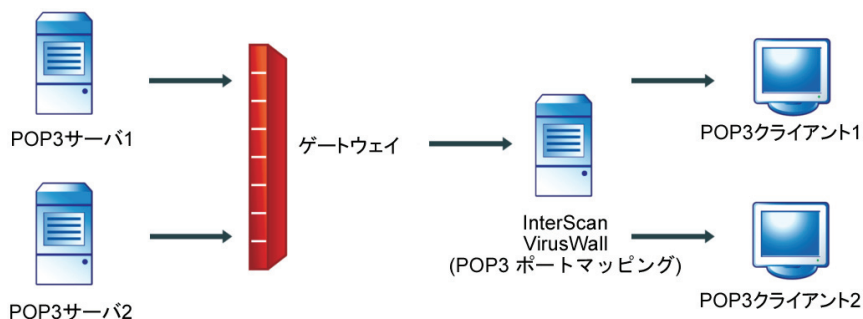


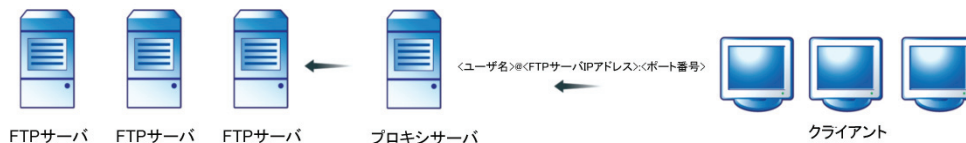
図 2-3. InterScan VirusWall がポートマッピングサーバとして機能する POP3

FTP

スタンドアロンモードの場合、InterScan VirusWall は FTP プロキシサーバとして機能します。指定された FTP サーバに FTP VirusWall 経由で接続するには、ユーザは次のように入力します。<ユーザ名>@<FTP サーバ IP アドレス>:<ポート番号>

依存プロキシモード（既存の FTP プロキシサーバと連動）では、InterScan VirusWall は既存の FTP プロキシサーバを補完する役割を果たします。プロキシサーバを使用しない場合、FTP VirusWall に接続しているクライアントは、InterScan VirusWall の Web コンソールの [FTP] の [設定] 画面で指定されている実際の FTP サーバにリダイレクトされます。FTP サーバとクライアントコンピュータ間のすべての FTP セッションは FTP VirusWall 経由で渡されますが、エンドユーザはこの処理を認識しません。

InterScan VirusWall のインストール前 (プロキシサーバあり)



InterScan VirusWall のインストール後 (プロキシサーバあり)

スタンドアロンモード



依存プロキシモード

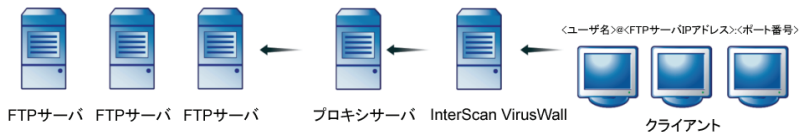
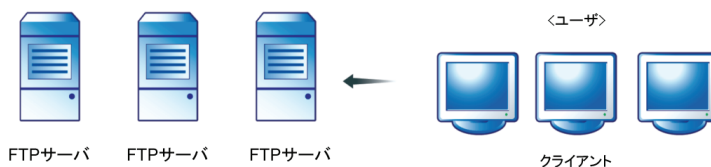
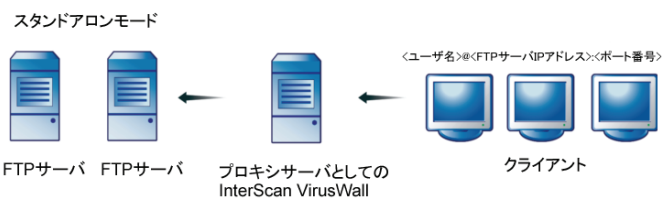


図 2-4. プロキシサーバを使用した FTP のインストールトポロジ

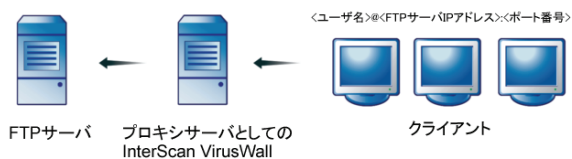
InterScan VirusWall のインストール前 (プロキシサーバなし)



InterScan VirusWall のインストール後 (プロキシサーバなし)



依存プロキシモード



設定

【スタンドアロンモードを使用する】を選択した場合、InterScan VirusWall はネットワークの単独FTPプロキシサーバとして機能します。【FTPプロキシを使用する】を選択した場合、InterScan VirusWall は既存のFTPプロキシサーバを補間して動作します。

☐ スタンドアロンモードを使用する

☒ FTPプロキシを使用する: <FTPサーバのIPアドレス> ポート: 21

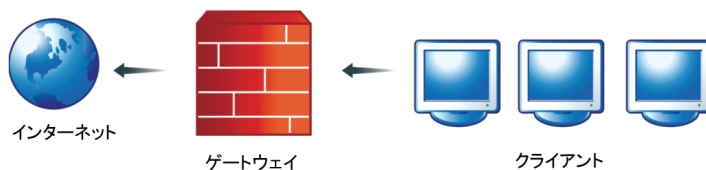
図 2-5. プロキシサーバを使用しない FTP のインストールポロジ

HTTP

スタンドアロンモードの場合、InterScan VirusWall は、HTTP プロキシサーバとして機能する、または既存サーバから HTTP トラフィックを受信するゲートウェイデバイスの直後に配置されます。

依存プロキシモードの場合、InterScan VirusWall は、クライアントコンピュータと HTTP プロキシサーバの間に配置されます。

InterScan VirusWall のインストール前 (プロキシなし)



InterScan VirusWall のインストール後 (プロキシなし) スタンドアロンモード

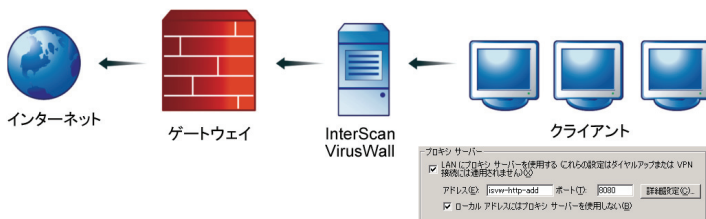
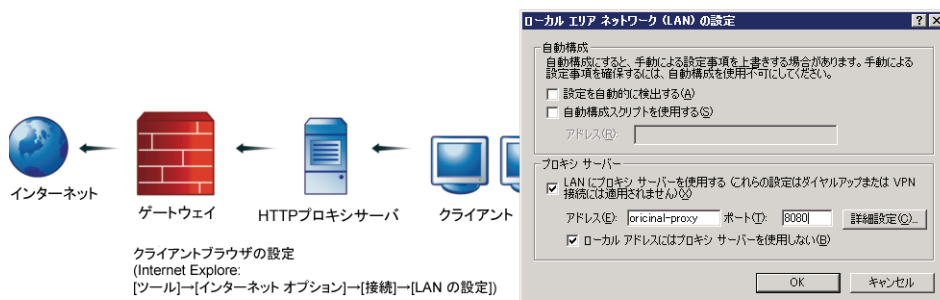


図 2-6. プロキシサーバを使用しない HTTP のインストールボロジ (スタンドアロンモード)

InterScan VirusWall のインストール後、InterScan VirusWall を指すようにブラウザクライアントのプロキシ設定を変更する必要があります。

InterScan VirusWall のインストール前 (プロキシあり)



InterScan VirusWall のインストール後 (プロキシあり)

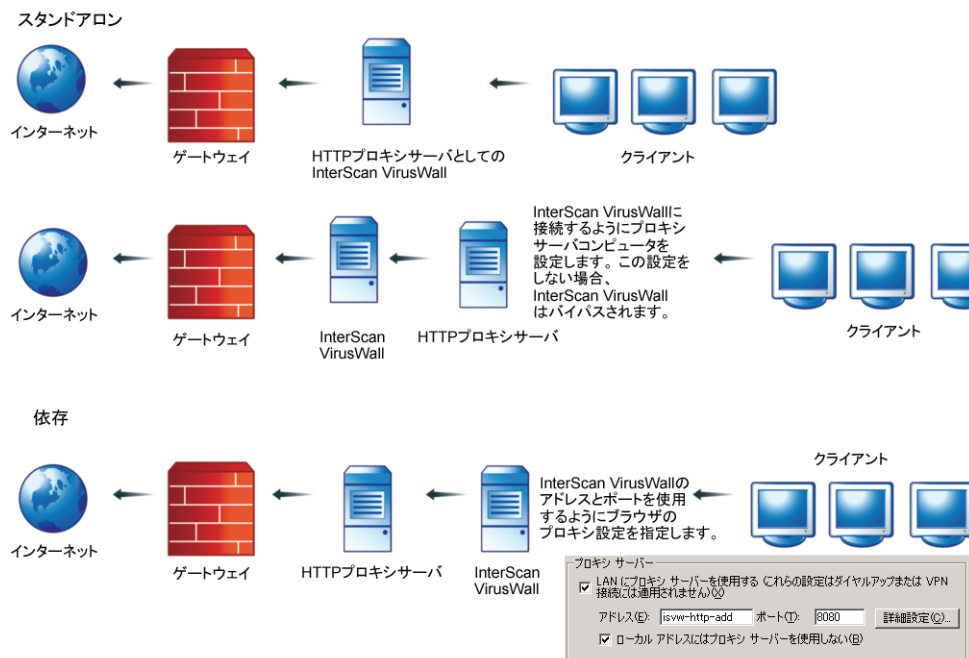
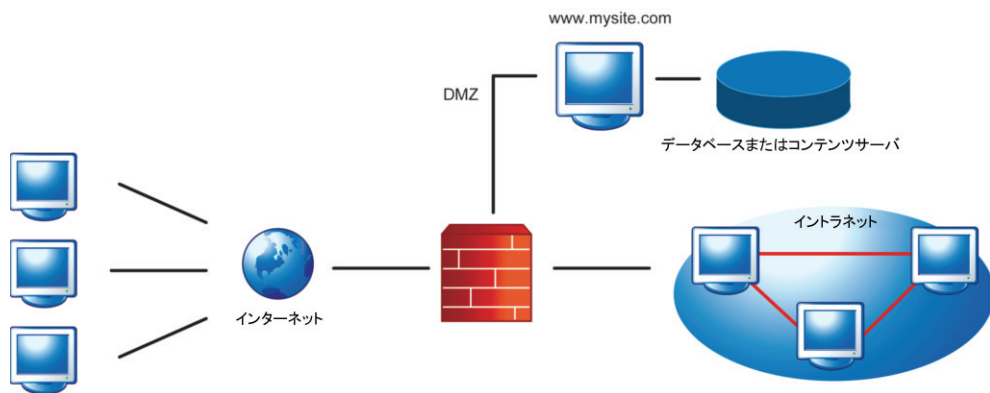


図 2-7. プロキシサーバを使用した HTTP のインストールポロジ (依存プロキシモード)

HTTP リバースプロキシ

リバースプロキシ配置では、内部および外部のユーザはコンテンツサーバを利用できますが、このコンテンツサーバへの監視されていない、直接的なアクセスはファイアウォールによって阻止されます。このトポロジの場合、InterScan VirusWall は、コンテンツサーバからネットワーク内外のクライアントへ送られる HTTP トラフィックを検索します。

InterScan VirusWall のインストール前



InterScan VirusWall のインストール後

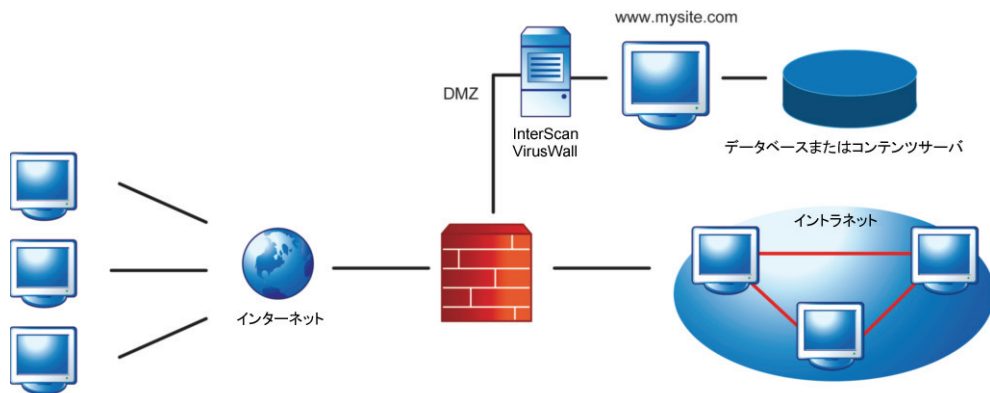


図 2-8. InterScan VirusWall をリバースプロキシとして使用した HTTP のインストールトポロジ

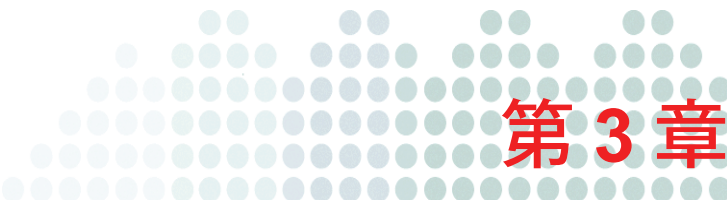
InterScan VirusWall のインストール前の作業

1. InterScan VirusWall をインストールするコンピュータで、ウイルス対策製品やスパイウェア対策製品など、リアルタイム検索を実行している他の製品を削除します。製品の削除を望まない場合は、その製品の検索除外リストに次の事項を追加します。
 - InterScan VirusWall のインストール先のパス
 - SMTP、POP3、HTTP、および FTP プロトコルの隔離パス
 - Windows の Temp フォルダ
2. 管理者権限でコンピュータにログオンします。
3. InterScan VirusWall で使用する次の初期設定のポート番号が使用されていないことを確認します。
 - SMTP: 25
 - POP3: 110
 - HTTP: 8080
 - FTP: 21

注意： Web コンソールの場合、初期設定のポート番号は HTTP では 9240、HTTPS では 9241 です。ただし、インストール時に別のポート番号を指定できます。

4. InterScan VirusWall を初めてインストールする場合、および SMTP をインストールする場合は、SMTP VirusWall が有効なドメインとして認識するドメインのリストを作成します。
SMTP は、これらのドメインにアドレス指定された受信メールだけを配信します。

InterScan VirusWall のインストールに役立つ関連システム情報のチェックリストについては、[付録 A](#) を参照してください。



第3章

インストール

Trend Micro InterScan VirusWall スタンダードエディション（以下、InterScan VirusWall）をインストールし設定して、物理ネットワークのさまざまなセットアップをサポートできます。InterScan VirusWall は、容易にセットアップできるように設定が簡素化され、毎日の保守を最低限に抑えられるので、時間や IT リソースが限られ、リアルタイムのウイルス / スпамメール予防サービスを必要とする管理者に特に有用です。

InterScan VirusWall のセットアッププログラムには、システム要件、ディスク容量要件、必要な Service Pack または Patch、および使用可能である必要のあるポートについて互換性を確認するインストール時のシステム要件確認機能があります。インストール時のシステム要件確認機能を使用すると、InterScan VirusWall は、体験版環境で他の製品と共存できるようになります。

この章では、InterScan VirusWall をインストールするためのステップごとの手順を示します。また、InterScan VirusWall 6.0 または 6.02 から本バージョンに移行する手順についても説明します。

インストールシナリオ

InterScan VirusWall をセットアップするには、セットアップファイルを起動して InstallWizard の指示に従います。

次のインストールシナリオを利用できます。

- 46 ページの「InterScan VirusWall を新規インストールする」
InterScan VirusWall を初めてインストールする場合は、この手順を使用します。
- 「以前のバージョンがインストールされているコンピュータにインストールする」

InterScan VirusWall 6.0 または 6.02 がインストールされているコンピュータに本バージョンをインストールする場合で、以前のバージョンの設定を本バージョンに移行するときは、この手順を使用します。

- ・ 「新しいコンピュータにインストールして以前のバージョンの設定を移行する」

新しいコンピュータに本バージョンをインストールする場合で、以前のバージョンの InterScan VirusWall がインストールされている別のコンピュータから設定を移行するときは、この手順を使用します。移行ツールまたはコマンドラインを使用してバージョン 6.0 または 6.02 の設定を移行し、インストール時にインポートできます。

- ・ 「以前のバージョンからのコマンドラインによる移行」

新しいコンピュータに本バージョンをインストールする場合で、以前のバージョンの InterScan VirusWall がインストールされているコンピュータからコマンドラインを使用して設定を移行するときは、この手順を使用します。移行ツールを使用して以前のバージョンの設定を移行し、インストール時にインポートします。

InterScan VirusWall を新規インストールする

新規インストール時の URL ブロックおよびフィルタのグローバルポリシーについては、インターネットセキュリティグループに対して初期設定で 12 のカテゴリが選択されます（144 ページの「URL ブロックおよび URL フィルタのグローバルポリシーを管理する」を参照）。

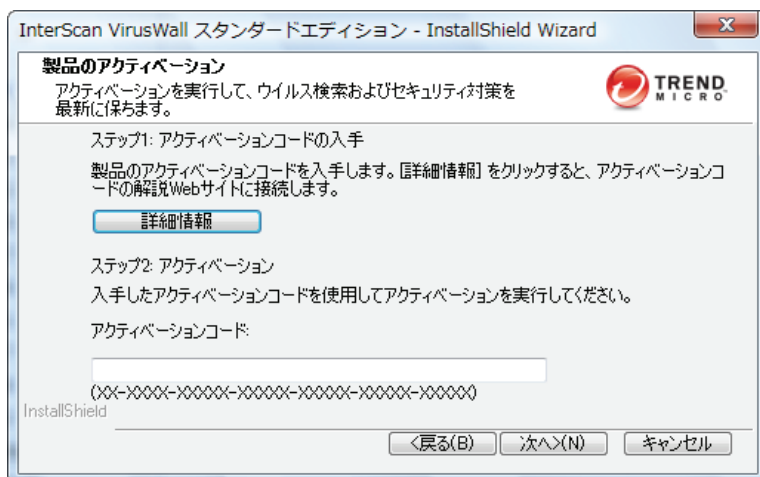
InterScan VirusWall を新規インストールするには

1. setup.exe をダブルクリックしてインストールプロセスを開始します。
2. 開始ウィンドウが表示されたら、[次へ] をクリックします。
3. [使用許諾契約] 画面で、契約書全体をよく読み、[使用許諾契約の内容に同意します] を選択して、インストールを続行します。

画面上で契約書全体をスクロールするか、または契約書を印刷できます。[使用許諾契約の内容に同意しません] を選択すると、インストールプロセスは終了します。

4. [セットアップの種類] 画面で、[新規インストール] を選択して [次へ] をクリックします。
5. 図 3-1 の [製品のアクティベーション] 画面で、以下のいずれかの手順を実行します。
 - ・ [アクティベーションコード] テキストボックスに製品のアクティベーションコードを入力して [次へ] をクリックします。
 - ・ アクティベーションコードを入力しないで [次へ] をクリックします。

図 3-1. 【製品のアクティベーション】画面



アクティベーションコードを入力しないで [次へ] をクリックすると、情報が不足していることを警告するメッセージと、30 日間有効の InterScan VirusWall 体験版がインストールされることを通知するメッセージが表示されます。[OK] をクリックしてインストールを続行します。

[インストール先フォルダの指定] 画面が表示され、InterScan VirusWall のインストール先ディレクトリのパスを示します。

6. このインストール先のパスを変更する場合は、[参照] をクリックして別の場所を指定します。
7. 初期設定のパスを受け入れるか、新しいインストール先を選択したら、[次へ] をクリックします。
8. [Web コンソール URL の設定] 画面で、Web コンソールのバインド先を指定します。

初期設定を図 3-2 に示します。

図 3-2. [Web コンソール URL の設定] 画面

InterScan VirusWall スタンダードエディション - InstallShield Wizard

WebコンソールURLの設定

TREND MICRO

WebコンソールがバインドするIPアドレスを選択して、対応するポート番号を入力してください。

HTTP IPアドレス:

HTTP ポート番号:

HTTPS IPアドレス:

HTTPS ポート番号:

InstallShield

<戻る(B) 次へ>(N) キャンセル

9. [次へ] をクリックします。
10. [管理者パスワードの設定] 画面で、4 ～ 32 文字のパスワードを入力して確認し、[次へ] をクリックします。
11. [検索サービスの設定] 画面で、インストール完了後に開始する InterScan VirusWall サービスを選択します。

初期設定では、すべてのサービスが選択されています (図 3-3 を参照)。選択したら、[次へ] をクリックします。

図 3-3. [検索サービスの設定] 画面



12. [リレー先の設定] 画面で、受信メールを受け入れるドメインを指定します。
InterScan VirusWall では、これらのドメインにアドレス指定された受信メールだけが受け入れられます。
13. [HTTP Web レピュテーションの情報を送る] 画面で、感染 URL に関するフィードバックを匿名で送信するかどうかを指定し、[次へ] をクリックします。
14. [ウイルストラッキングセンターの設定] 画面で、ウイルストラッキングセンターに InterScan VirusWall で検出されたウイルスの情報を送信するかどうかを指定し、[次へ] をクリックします。
15. [設定の確認] 画面で、現在の設定を確認して [次へ] をクリックします。
設定を変更する場合は、[戻る] をクリックして前の画面に戻ります。
[インストールステータス] 画面には、このソフトウェアのインストールの進行状況が表示されます。
16. [セットアップの完了] 画面で、Readme ファイルの表示または Web コンソールの起動を選択して [終了] をクリックします。
 - Readme ファイルの表示を選択すると、新しいウィンドウで Readme ファイルが表示されます。
 - Web コンソールの起動を選択すると、Web ブラウザのウィンドウが自動的に開き、InterScan VirusWall のログオンページが表示されます。

以前のバージョンがインストールされているコンピュータにインストールする

セットアッププログラムでは、以前のバージョンの InterScan VirusWall がインストールされているコンピュータに本バージョンの InterScan VirusWall をインストールできます。サポートされているバージョンは次のとおりです。

- InterScan VirusWall 6.0 または 6.02

このいずれかのバージョンの InterScan VirusWall がインストールされているコンピュータに本バージョンの InterScan VirusWall をインストールする場合は、インストール時に以前のバージョンの設定を移行できます (54 ページの「新しいコンピュータにインストールして以前のバージョンの設定を移行する」を参照)。

設定を移行する場合は、インストールの開始前に設定ファイルのバックアップを作成することをお勧めします。InterScan VirusWall のインストールプログラムによって以前のバージョンの InterScan VirusWall が完全に削除されます。

注意： InterScan VirusWall 7.0 のセットアッププログラムで InterScan VirusWall 6.0 または 6.02 が検出され、それらが同じ言語バージョンである場合、セットアッププログラムによりビルドのアップグレードを確認するようプロンプトが表示されます。InterScan VirusWall 7.0 のセットアッププログラムにより、InterScan VirusWall 6.0 または 6.02 が異なる言語バージョンであることが検出された場合、異なる言語バージョンをアンインストールしてから、インストールを続行するようにプロンプトが表示されます。

以前のバージョンがインストールされているコンピュータにインストールするには

1. setup.exe をダブルクリックしてインストールプロセスを開始します。
2. 開始画面が表示されたら、[次へ] をクリックします。
3. [使用許諾契約] 画面が表示されたら、契約書全体をよく読み、[使用許諾契約の内容に同意します] を選択して、インストールを続行します。

画面上で契約書全体をスクロールするか、または契約書を印刷できます。[使用許諾契約の内容に同意しません] を選択すると、インストールプロセスは終了します。

4. 以前のバージョンから設定を移行するには、[アップグレードインストール] チェックボックスをオンにします。

設定を移行する場合は、インストールの開始前に設定ファイルのバックアップを作成することをお勧めします。InterScan VirusWall のインストールプログラムによって以前のバージョンの InterScan VirusWall が完全に削除されます。

移行した設定をすべて表示するレポートを作成しない場合は、[移行レポートを作成する] チェックボックスをオフにします。

5. [次へ] をクリックします。

[製品のアクティベーション] 画面が表示されます。

6. [製品のアクティベーション] 画面で、次のいずれかを選択します。

- [アクティベーションコード] フィールドに製品のアクティベーションコードを入力して [次へ] をクリックします。

- アクティベーションコードを入力しないで [次へ] をクリックします。

アクティベーションコードを入力しないで [次へ] をクリックすると、情報が不足していることを警告するメッセージと、30 日間有効の InterScan VirusWall 体験版がインストールされることを通知するメッセージが表示されます。[OK] をクリックしてインストールを続行します。

[インストール先の指定] 画面が表示され、InterScan VirusWall のインストール先ディレクトリのパスを示します。

7. このインストール先のパスを変更する場合は、[参照] をクリックして別の場所を指定します。
8. 初期設定のパスを受け入れるか、新しいインストール先を選択したら、[次へ] をクリックします。

[Web コンソール URL の設定] 画面が表示されます。

9. [Web コンソール URL の設定] 画面で、Web コンソールのバインド先を指定します。

10. [次へ] をクリックします。

[管理者パスワード] 画面が表示されます。

11. 4 ～ 32 文字のパスワードを入力して確認し、[次へ] をクリックします。

[検索サービスの設定] 画面が表示されます。

12. インストール完了後に開始する InterScan VirusWall サービスを選択します。

初期設定では、すべてのサービスが選択されています。選択したら、[次へ] をクリックします。

[リレー先の設定] 画面が表示されます。

13. リレーされるメールをブロックするには、受信メールを受け入れるドメインを [ドメイン名] フィールドで指定します。

14. [次へ] をクリックします。

[HTTP Web レピュテーションの情報を送る] 画面が表示されます。

15. Web レピュテーションデータベースの向上に役立てるため、このチェックボックスをオンにして、感染した URL についての匿名情報を送信してください。

16. [次へ] をクリックします。

[ウイルストラッキングセンターの設定] 画面が表示されます。

17. トレンドマイクロのウイルストラッキングセンターに InterScan VirusWall で検出されたウイルスの情報を送信するかどうかを選択し、[次へ] をクリックします。

[設定の確認] 画面が表示されます。セットアッププログラムは、隔離されたデータを C:\\$Relocated_ISVW6_Quarantine_Folder ディレクトリに移動します。このデータは移動するか、削除することができます。インストール後に、隔離設定を更新します (第 9 章「隔離」を参照)。

18. 現在の設定を確認します。

- 設定が正しい場合は [次へ] をクリックします。
- 設定の変更が必要な場合は、適切な前画面が表示されるまで [戻る] をクリックし、設定を変更します。[設定の確認] 画面が再度表示されるまで [次へ] をクリックし、[次へ] をもう一度クリックして処理を続行します。

[設定の確認] 画面で [次へ] をクリックすると、以前のバージョンの InterScan VirusWall がアンインストールされることを示すメッセージが表示されます。

- [はい] をクリックして以前のバージョンの InterScan VirusWall をアンインストールします。
- セットアップを終了する場合は、[いいえ] をクリックします。

注意： 警告メッセージは、移行元の InterScan VirusWall のバージョンによって異なる場合があります。

アンインストールが完了すると、[インストールステータス] 画面が表示されます。[インストールステータス] 画面には、InterScan VirusWall のインストールの進行状況が表示されます。

19. [セットアップの完了] 画面で、Readme ファイルの表示、Web コンソールの起動、または移行レポートの表示を選択して [終了] をクリックします。

- Readme ファイルの表示を選択すると、新しいウィンドウで Readme ファイルが表示されます。
- Web コンソールの起動を選択すると、Web ブラウザのウィンドウが自動的に開き、InterScan VirusWall のログオンページが表示されます。
- インストールの開始時に移行レポートの作成を選択した場合は、[ファイル出力] をクリックします。図 3-4 のようなレポートが新しいウィンドウで表示されます。

注意： 移行レポートの内容は、移行元の InterScan VirusWall のバージョンによって異なる場合があります。



```

isvw_migration_report.txt - メモ帳
ファイル(F) 編集(E) 書式(O) ヘルプ(H)

***** InterScan VirusWall 移行レポート *****
InterScan VirusWall バージョン:<6.02> ビルド:<7169> 03/13/07 11:32:58
このレポートはWeb管理画面に基づいています。

***** HTTP関連の移行 開始 *****
Summary > Web (HTTP) > On/Off status
Web (HTTP) > Virus Scan > Target > On/Off status
Web (HTTP) > Virus Scan > Target > File Type > Virus scan these file types
Web (HTTP) > Configuration > Compressed File Scanning > Maximum number of files to scan per archive
Web (HTTP) > Configuration > Compressed File Scanning > Maximum decompressed file size
Web (HTTP) > Virus Scan > Target > File Type > File types
Web (HTTP) > Virus Scan > Action > Action for infected HTTP files
Web (HTTP) > Virus Scan > Action > Action for uncleanable files
Web (HTTP) > Virus Scan > Notification > Notification for infected HTTP files
Web (HTTP) > URL Blocking > URL > On/Off status
Web (HTTP) > URL Blocking > Notification > Notifications for Blocked URLs
Web (HTTP) > Configuration > HTTP Settings > Enable/Disable "If download size"
Web (HTTP) > Configuration > HTTP Settings > Size threshold
Web (HTTP) > Configuration > HTTP Settings > Present page...
Web (HTTP) > URL Blocking > URL > All URL blocking and exception settings
Web (HTTP) > Configuration > HTTP Settings > HTTP Listening Port
Web (HTTP) > Configuration > HTTP Settings > Anonymous FTP over HTTP logon email
***** HTTP関連の移行 終了 *****
***** SMTP関連の移行 開始 *****
Mail (SMTP) > Virus Scan > Incoming > Target > SMTP Incoming Virus Scan
Mail (SMTP) > Virus Scan > Incoming > Target > File Type > Virus scan these incoming file types
Mail (SMTP) > Virus Scan > Incoming > Target > File Type > File types

```

図 3-4. 移行レポートの例

注意： インストールプロセスの完了後に移行レポートを印刷する場合は、次のレポートの場所に移動します。

< インストールフォルダ > \isvw_migration_report.txt

新しいコンピュータにインストールして以前のバージョンの設定を移行する

新しいコンピュータに本バージョンをインストールしたら、セットアッププログラムを使用して、以前のバージョンの InterScan VirusWall がインストールされている別のコンピュータから設定を移行できます。移行は次のバージョンについてサポートされています。

- InterScan VirusWall 6.0 または 6.02

本バージョンの InterScan VirusWall では、隔離ファイルをバージョン 6.0 および 6.02 の InterScan VirusWall から移行できます。この移行は、次の 2 つのシナリオのいずれかに該当します。

- 初期設定の隔離パスが変更されていない場合は、以前のバージョンの隔離ファイルが、本バージョンの InterScan VirusWall によって、その初期設定のパスのルートパスに移動されます。たとえば、InterScan VirusWall を D:\ISVW にインストールして隔離ファイルの初期設定を変更しなかった場合は、本バージョンの InterScan VirusWall によって、
D:\¥Relocated_ISVW6_Quarantine_Folder¥xxx にあるすべての隔離ファイルが
D:\¥Relocated_ISVW6_Quarantine_Folder¥xxx に移動されます。さらに、本バージョンの InterScan VirusWall で使用される隔離パスは、元のインストールのまま維持されます。
- 初期設定の隔離パスを変更した場合は、InterScan VirusWall 6.x の隔離ファイルは、本バージョンの InterScan VirusWall によって新しい場所に移動されません。本バージョンの InterScan VirusWall によって生成される新しい隔離ファイルは、InterScan VirusWall 6.x の場合と同じパスに保存されます。

注意： 以前のバージョンから本バージョンに設定を移行する際、インストールプログラムにより、URL フィルタのルールについて以前のバージョンで選択した URL カテゴリが移行されません。

新しいコンピュータにインストールしてバージョン 6.0 または 6.02 の設定を移行する

以前に InterScan VirusWall をインストールしたことがないコンピュータに本バージョンをインストールして、バージョン 6.0 または 6.02 がインストールされているコンピュータの設定を使用する場合は、その設定をファイルにエクスポートできます。このファイルはインストールプロセスで使用され、保存された設定がインストール先コンピュータにインポートされます。

インストールパッケージに付属の移行ツールで設定をファイルにエクスポートできます。この移行ツールを使用すると、InterScan VirusWall 6.0 または 6.02 の設定をエクスポートできます。

移行ツールを実行するコンピュータに InterScan VirusWall 6.0 または 6.02 が存在しない場合は、メッセージが表示されてインストールのセットアップが終了します。

本バージョンをインストールしてバージョン 6.0 または 6.02 の設定を移行するには

1. InterScan VirusWall 7.0 のインストールパッケージのディレクトリ < インストールパッケージ > %other にある isvw-migr6to7.exe という名前のツールを見つけて、それを InterScan VirusWall 6.0x がインストールされているコンピュータにコピーしてください。
2. コマンドラインで次のように入力します。

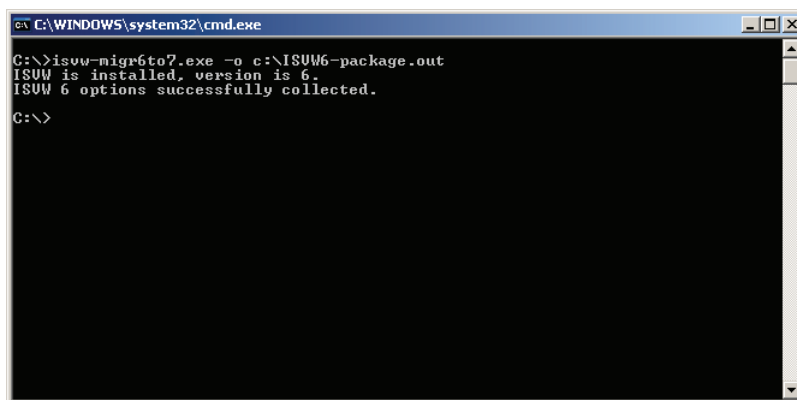
isvw-migr6to7 -o [< 移行設定ファイル名 >]

例 : isvw-migr6to7 -o c:\ISVW6-package.out

図 3-5 を参照してください。

注意： InterScan VirusWall 7.0 の移行ツールでは、絶対パス名と相対パス名の両方がサポートされています。

図 3-5. InterScan VirusWall 6.0x の移行で使用される移行ツールエクスポートユーティリティの画面



3. ネットワーク経由でこのファイルにアクセスできない場合は、< 移行設定ファイル名 > のファイルをリムーバブルメディアにコピーします。これにより、InterScan VirusWall をインストールするコンピュータでそのファイルにアクセスできます。
4. InterScan VirusWall をインストールするコンピュータで、setup.exe をダブルクリックしてインストールプロセスを開始します。
5. 開始画面が表示されたら、[次へ] をクリックします。

6. [使用許諾契約] 画面が表示されたら、契約書全体をよく読み、[使用許諾契約の内容に同意します] を選択して、インストールを続行します。
画面上で契約書全体をスクロールするか、または契約書を印刷できます。[使用許諾契約の内容に同意しません] を選択すると、インストールプロセスは終了します。
7. [セットアップの種類] 画面が表示されたら、[リモートコンピュータの以前のバージョンから設定を移行する] チェックボックスをオンにします。
移行した設定をすべて表示するレポートを作成しない場合は、[移行レポートを作成する] チェックボックスをオフにします。
8. [次へ] をクリックします。
[製品のアクティベーション] 画面が表示されます。
9. [製品のアクティベーション] 画面で、次のいずれかを選択します。
 - [アクティベーションコード] フィールドに製品のアクティベーションコードを入力して [次へ] をクリックします。
 - アクティベーションコードを入力しないで [次へ] をクリックします。
アクティベーションコードを入力しないで [次へ] をクリックすると、情報が不足していることを警告するメッセージと、30 日間有効の InterScan VirusWall 体験版がインストールされることを通知するメッセージが表示されます。[OK] をクリックしてインストールを続行します。

[インストール先の指定] 画面が表示され、InterScan VirusWall のインストール先ディレクトリのパスを示します。
10. このインストール先のパスを変更する場合は、[参照] をクリックして別の場所を指定します。
11. 初期設定のパスを受け入れるか、新しいインストール先を選択したら、[次へ] をクリックします。
[Web コンソール URL の設定] 画面が表示されます。
12. [Web コンソール URL の設定] 画面で、Web コンソールのバインド先を指定します。
13. [次へ] をクリックします。
[管理者パスワード] 画面が表示されます。
14. 4 ～ 32 文字のパスワードを入力して確認し、[次へ] をクリックします。
[検索サービスの設定] 画面が表示されます。
15. インストール完了後に開始する InterScan VirusWall サービスを選択します。
初期設定では、すべてのサービスが選択されています。選択したら、[次へ] をクリックします。

[リレー先の設定] 画面が表示されます。

16. リレーされるメールをブロックするには、受信メールを受け入れるドメインを [ドメイン名] フィールドで指定します。
17. [次へ] をクリックします。
[HTTP Web レピュテーションの情報を送る] 画面が表示されます。
18. Web レピュテーションデータベースの向上に役立てるため、このチェックボックスをオンにして、感染した URL についての匿名情報を送信してください。
19. [次へ] をクリックします。
[ウイルストラッキングセンターの設定] 画面が表示されます。
20. トレンドマイクロのウイルストラッキングセンターに InterScan VirusWall で検出されたウイルスの情報を送信するかどうかを選択し、[次へ] をクリックします。
[設定の確認] 画面が表示されます。
21. 現在の設定を確認します。
 - 設定が正しい場合は [次へ] をクリックします。
 - 設定の変更が必要な場合は、適切な前画面が表示されるまで [戻る] をクリックし、設定を変更します。[設定の確認] 画面が再度表示されるまで [次へ] をクリックし、[次へ] をもう一度クリックして処理を続行します。

[インストールステータス] 画面が表示されます。[インストールステータス] 画面には、InterScan VirusWall のインストールの進行状況が表示されます。
22. [セットアップの完了] 画面で、Readme ファイルの表示、Web コンソールの起動、または移行レポートの表示を選択して [終了] をクリックします。
 - Readme ファイルの表示を選択すると、新しいウィンドウで Readme ファイルが表示されます。
 - Web コンソールの起動を選択すると、Web ブラウザのウィンドウが自動的に開き、InterScan VirusWall のログオンページが表示されます。
 - インストールの開始時に移行レポートの作成を選択した場合は、[ファイル出力] をクリックします。図 3-4 のようなレポートが新しいウィンドウで表示されます。

注意： インストールプロセスの完了後に移行レポートを印刷する場合は、次のレポートの場所に移動します。

< インストールフォルダ > \isvw_migration_report.txt

以前のバージョンからのコマンドラインによる移行

新しいコンピュータに本バージョンをインストールしたら、コマンドラインを使用して、以前のバージョンの InterScan VirusWall がインストールされている別のコンピュータから設定を移行できます。移行は次のバージョンについてサポートされています。

- InterScan VirusWall 6.0 または 6.02

InterScan VirusWall 6.0 または 6.02 から InterScan VirusWall 7.0 へのコマンドラインによる移行

InterScan VirusWall 6.0x の設定を InterScan VirusWall 7.0 がインストールされているコンピュータに移行するには

1. InterScan VirusWall 7.0 のインストールパッケージのディレクトリ <インストールパッケージ>%other にある isvw-migr6to7.exe という名前のツールを見つけて、それを InterScan VirusWall 6.0x がインストールされているコンピュータにコピーしてください。
2. コマンドラインで次のように入力します。

```
isvw-migr6to7 -o [< 移行設定ファイル名 >]
```

例 : isvw-migr6to7 -o c:\ISVW6-package.out

図 3-5 を参照してください。

注意： InterScan VirusWall 7.0 の移行ツールでは、絶対パス名と相対パス名の両方がサポートされています。

3. ネットワーク経由でこのファイルにアクセスできない場合は、<移行設定ファイル名>のファイルをリムーバブルメディアにコピーします。これにより、InterScan VirusWall をインストールするコンピュータでそのファイルにアクセスできます。
4. InterScan VirusWall 7.0 がインストールされているコンピュータで、コマンドウィンドウを開きます。
5. <InterScan VirusWall 7.0 インストールパス>%Others に移動し、コマンドウィンドウで、次のコマンドで移行ツールを実行します。

```
isvw-migr6to7 -p [< 移行設定ファイル名 >] -i [<InterScan VirusWall 7.0 インストールパス >]
```

例 : isvw-migr6to7 -p c:\ISVW5-package.out -i "c:\Program Files\Trend Micro\InterScan VirusWall 7"

移行が正常に終了すると、移行の成功メッセージが表示されます。また、InterScan VirusWall 7.0 インストールディレクトリに移行レポートが作成されます。

6. InterScan VirusWall サービスを再起動します。

インストール後の作業

InterScan VirusWall をアクティベートすると、インストール完了後に次の操作が可能になります。

- 自社のニーズに合わせて InterScan VirusWall の初期設定を変更できます。
- インストール時に選択した初期設定を使用して、ウイルス検索、スパムメール検出、およびコンテンツフィルタを直ちに開始できます。

また、インストール後すぐに次の操作を実行する必要があります。

- パターンファイルと検索エンジンのアップデート
- ウイルス検索が有効になっていることの確認
- 通知メッセージのカスタマイズ
- アラートの設定
- ウイルスパターンファイル、検索エンジン、およびスパムメール判定ルールとエンジンの予約アップデートの設定

インストールによっては、次のタスクの実行が必要な場合があります。

- 同じコンピュータにインストールされているウイルス対策ソフトウェアと連動するようにサーバを設定します。

InterScan VirusWall サーバにウイルス対策製品がインストールされている場合は、次のフォルダを検索しないように InterScan VirusWall サーバを設定します。

- インストール後の InterScan VirusWall のプログラムフォルダ
- InterScan VirusWall の隔離ディレクトリ（初期設定から変更した場合）
- Windows の Temp フォルダ
- InterScan VirusWall のパターンファイルアップデートにアクセスする際にキャッシュメカニズムまたはファイルサイズの制限を無効にするようにプロキシサーバを設定します。パターンファイルアップデートにアクセスするためにプロキシサーバを使用してインターネットにアクセスし、さらにそのプロキシサーバではサイズの大きいファイルのダウンロードにキャッシュメカニズムが使用されている場合、パターンファイルアップデートをダウンロードするときに、キャッシュメカニズムまたはファイルサイズの制限を無効にする必要があります。InterScan VirusWall のウイルスパターンファイルと URL フィルタデータベースのファイルは、予想以上に大きい可能性があります。

この設定は、InterScan VirusWall がミドルウェア（ファイアウォールや SOCKS/ プロキシサーバ）を介して URL に接続し、アップデートファイルをダウンロードする際に適用されます。アップデートファイルにアクセスするには、次の URL に移動します。

<http://isvw602-av.activeupdate.trendmicro.co.jp/activeupdate/japan/>
<http://isvw602-as.activeupdate.trendmicro.co.jp/activeupdate/japan/>

- InterScan VirusWall が他のサービスと共存している場合は、待機ポートの競合を回避します。InterScan VirusWall では、待機ポート用に次の初期設定のポートが使用されます。

- SMTP: 25
- HTTP: 8080
- FTP: 21
- POP3: 110

同じサーバの他のサービスが、すでにこれらのポートを使用している場合があります。

Windows Small Business Server（以下、Windows SBS）2003 Standard/Enterprise Edition では、次のポートがシステム自体で使用されている可能性があります。

- 25: SMTP ポート。Exchange サーバに使用されている可能性があります。
- 8080: HTTP プロキシポート。ISA HTTP プロキシに使用されている可能性があります。
- 110: POP3 ポート。Exchange サーバに使用されている可能性があります。
- 21: FTP ポート。Internet Information Server（以下、IIS）に使用されている可能性があります。

IIS は常に、Windows 2000/2003/Windows SBS などの Windows サーバシステムに付属しています。

Exchange サーバは、Windows SBS の基本コンポーネントです。

ISA サーバは、SBS Enterprise Edition のコンポーネントです。

トレンドマイクロでは、同じサーバ上の他のコンポーネントが初期設定のポートを使用している場合は、InterScan VirusWall の Web コンソールを使用して、関連プロトコルの待機ポートを変更することを強くお勧めします。

- インストール後に SMTP VirusWall を使用する場合は、リレー対策設定を指定します。

InterScan VirusWall は、メールリレーサーバとして機能できます。サーバがあらゆるドメインに宛てられた受信メールを受け入れる場合は、メールをリレーできますが、これによってスパムメールの量が増える可能性があります。オープンリレーの不正利用からサーバを守るために、特定のドメインのみに宛てられた受信メールを受け入れることによって、リレーメッセージをブロックします。

次の手順に従って、Web コンソールから正しい設定を指定できます。

- a. 左側のメニューで [SMTP] → [設定] の順に選択します。
- b. [詳細設定] で [次のドメイン宛ての受信メールのみを許可して、リレーされたメッセージをブロックする] チェックボックスをオンにします。
- c. メールを受信できるドメイン名を入力します。各ドメインはセミコロン (;) で区切ります。
- d. [保存] をクリックします。

Web コンソールを開く

InterScan VirusWall のインストールが完了すると、インストール時に選択したサービスと基本サービスが自動的に開始されます。InterScan VirusWall は適切な一連の初期設定値で実行されるように設定されていますが、InterScan VirusWall の Web コンソールを開いて設定を確認する必要があります。

サポートされているブラウザは次のとおりです。

- Internet Explorer 6.0 以上
1. Web ブラウザを開いて InterScan VirusWall の URL を入力し、続けてインストール時に設定したポート番号を入力します (初期設定値: HTTP: 9240、HTTPS: 9241)。

`http://<IP アドレス>:<ポート番号>`

`https://<IP アドレス>:<ポート番号>`

この URL は、インストール時に Web コンソールにバインドした IP アドレスとポート番号によって決まります。

2. InterScan VirusWall のコンソールは、パスワードで保護されています。

InterScan VirusWall を起動 / 停止する

InterScan VirusWall には、次の 4 つのサービスがあります。SMTP VirusWall、POP3 VirusWall、FTP VirusWall および、HTTP VirusWall です。初期設定では、インストールの完了後、インストール時に選択した InterScan VirusWall のすべてのサービスが自動的に開始されます。ただし、特定のサービスのリアルタイム検索を有効または無効にすることにより、InterScan VirusWall の各サービスを個別に制御することもできます。インストール時に選択していないサービスを開始する場合、またはインストール時に選択したサービスを停止する場合は、Web コンソールの [概要] 画面で対象のサービスを手動で有効または無効にします。

すべてのサービスを再起動する

1. [コントロール パネル] で [管理ツール] をクリックし、[管理ツール] 画面を開きます。
2. [サービス] アイコンをクリックし、[サービス] 画面を開きます。
3. [TrendMicro InterScan VirusWall] に移動し、[サービスの再起動] をクリックします。

通常、[InterScan VirusWall] は [自動] に設定されています。

InterScan VirusWall をテストする

インストールの完了後は、InterScan VirusWall 設定に習熟し、プログラムのしくみを理解するために InterScan VirusWall のインストールをテストします。

EICAR (European Institute of Computer Antivirus Research) とウイルス対策ベンダは、インストールと設定の検査に使用できるテストファイルを開発しました。

テストファイルは実際のウイルスではありません。危害を加えたり、増殖したりすることはありません。シグネチャがトレンドマイクロのウイルスパターンファイルに含まれている特別に作成されたテストファイルです。このファイルは、次のトレンドマイクロのサイトからダウンロードできます。

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

コンピュータにダウンロードすると、メールでテストウイルスを使用して、SMTP 検索や POP3 検索のテスト、および FTP と HTTP のファイル転送のチェックを実行できます。

InterScan VirusWall を削除する

コンピュータからソフトウェアを削除するには

1. [スタート] → [設定] → [コントロール パネル] の順にクリックします。
2. [コントロール パネル] の [アプリケーションの追加と削除] をクリックします。
3. [アプリケーションの追加と削除] 画面で、[Trend Micro InterScan VirusWall スタンダードエディション] を選択します。
4. [変更と削除] をクリックします。

確認のダイアログボックスが表示されます。

5. [はい] をクリックして、アプリケーションとそのすべての機能を完全に削除するか、または [いいえ] をクリックしてアンインストールプロセスを中止します。

SMTP サービスの設定

Trend Micro InterScan VirusWall スタンダードエディション（以下、InterScan VirusWall）を使用すると、SMTP 送受信メールトラフィックを監視できます。SMTP トラフィックの検索は、インストールプロセス中に有効または無効にすることも、インストール後の任意の時点で InterScan VirusWall Web コンソールの [概要] 画面で有効または無効にすることもできます。

次の SMTP サービスを使用できます。

- ウイルスおよびその他の種類の不正プログラムの検出
- 不正プログラムコードが含まれる可能性がある圧縮形式の実行ファイルに対する IntelliTrap 検索
- フィッシングサイトの検出
- スパムメールの検出
- スパイウェアなどのグレーウェアの検出
- コンテンツフィルタ
- メッセージと添付ファイルのサイズによるフィルタ
- 送受信メールの SMTP サーバポートと配信オプションの設定
- SMTP トランザクションログ

InterScan VirusWall の [概要] 画面の [メール (SMTP)] タブには、InterScan VirusWall の SMTP 検索によって送受信メール通信で検出された、ウイルス、スパイウェア、スパムメールメッセージ、およびフィッシングメールの数に関する統計情報が表示されます。

SMTP サービスを有効または無効にする

SMTP サービスを有効または無効にするには、[概要] 画面の [メール (SMTP)] タブで [SMTP トラフィックの検索を有効にする] チェックボックスをオンまたはオフにします (図 4-1 を参照)。

図 4-1. [概要] 画面の [メール (SMTP)] タブ

The screenshot shows the Trend Micro InterScan VirusWall management console. The left sidebar contains navigation links: 概要 (Overview), SMTP, HTTP, FTP, POP3, 大規模感染予防 (Large-scale infection prevention), 隔離 (Isolation), アップデート (Update), レポート (Report), ログ (Log), and 管理 (Management). The main content area has tabs for ステータス (Status), メール (SMTP), メール (POP3), Web (HTTP), and ファイル転送 (FTP). The 'メール (SMTP)' tab is selected, displaying a warning message: 'InterScan VirusWallの使用期限まで残り4日です。詳細な情報...' (InterScan VirusWall's license expires in 4 days. For more information...). Below the warning, there are sections for 'SMTP受信メール検索状況' (SMTP Incoming Mail Search Status) and 'SMTP送信メール検索状況' (SMTP Outgoing Mail Search Status). Each section includes a table with columns for '今日' (Today), '過去7日間' (Last 7 days), and '過去30日間' (Last 30 days). The tables show counts for various items like '不正なファイル' (Malicious files), 'スパイウェア/グレーウェア' (Spyware/Grayware), 'スパムメール' (Spam mail), and 'フィッシング活動' (Phishing activity).

SMTP ウイルス検索を設定する

InterScan VirusWall では、管理者が自由に SMTP サービスの動作を設定できます。たとえば、次のような項目を指定できます。

- 検索する添付ファイルタイプ
- InterScan VirusWall によるウイルス検出時の通知の受信者
- ウイルス検出時に InterScan VirusWall で実行する処理 (駆除、削除、隔離、放置)

SMTP ウイルス検索機能

InterScan VirusWall の SMTP ウイルス検索には、次の機能があります。

- SMTP 送受信メールトラフィックのリアルタイム検索
- カスタマイズ可能な自動ウイルス通知
- 感染ファイルをウイルス駆除、削除、隔離、またはそのまま配信するオプション
- メッセージと添付ファイルのサイズによるフィルタ
- ファイル名チェック（「メールセキュリティ欠陥」の防止）
- 感染メッセージを削除するオプション
- カスタマイズされたタグラインをメッセージに挿入する機能

SMTP ウイルス検索を有効にする

SMTP ウイルス検索を有効にするには

1. 左側のメニューで [SMTP] → [検索] → [受信]（または [送信]）の順に選択します。
2. [対象] タブを選択します。
3. [SMTP 検索 (受信) を有効にする]（または [SMTP 検索 (送信) を有効にする]）チェックボックスをオンにします。
4. [保存] をクリックします。

検索するファイルタイプを指定する

InterScan VirusWall は、圧縮ボリューム内の個別ファイルを含め、すべてのまたは指定した添付ファイルタイプでウイルスを検索できます。図 4-2 に、添付ファイルの検索時に指定できる設定を示します。

図 4-2. [SMTP] → [検索] → [対象] タブ



検索するファイルタイプを選択するには

1. 左側のメニューで [SMTP] → [検索] → [受信] (または [送信]) の順に選択し、[対象] タブを選択します。
2. [検索対象ファイル] で、必要なオプションを選択します。

- a. ファイルタイプにかかわらず、すべての添付ファイルを検索するには、[検索可能なすべてのファイル] を選択します。この設定が最も安全です。
- b. 検索する添付ファイルを実際のファイルタイプで識別できるようにするには、[トレンドマイクロの推奨設定: 実際のファイルタイプによる識別] を選択します。

このオプションでは一部のファイルタイプをそのまま配信するため、すべての添付ファイルを検索する場合よりもパフォーマンスは高くなりますが、安全度は低くなります。

- c. 選択した添付ファイルタイプのみを検索するには、[指定のファイル] を選択して、[拡張子] をクリックします。[その他の拡張子] テキストボックスで明示的に指定したファイルタイプのみが検索されます。

初期設定では、次のファイル名拡張子を持つファイルが検索されます。

"";ARJ;BAT;BIN;BOO;CAB;CHM;CLA;CLASS;COM;CSC;DLL;DOC;DOT;DRV;EML;EXE;GZ;HLP;HTA;HTM;HTML;HTT;INI;JAR;JPEG;JPG;JS;JSE;LNK;LZH;MDB;MPD;MPP;MPT;MSG;MSO;

NWS;OCX;OFT;OVL;PDF;PHP;PIF;PL;POT;PPS;PPT;PRC;RAR;REG;RTF;SCR;SHS;SYS;TAR;
VBE;VBS;VSD;VSS;VST;VXD;WML;WSF;XLA;XLS;XLT;XML;Z;ZIP;{*;

ヒント： 初期設定の検索リストを変更する場合は、[指定のファイル] を選択して [拡張子] をクリックします。

3. [保存] をクリックします。

注意： ウイルス検索設定は、ウイルス / 不正プログラム、IntelliTrap、スパイウェアの検索など、SMTP のあらゆる種類の不正ファイル検索に適用されます。

圧縮ファイルの処理を設定する

SMTP 検索時の圧縮ファイルの処理方法を指定するには

1. 左側のメニューで [SMTP] → [検索] → [受信] (または [送信]) の順に選択し、[対象] タブを選択します。
2. [圧縮ファイルの処理] で、必要なオプションを選択します。
 - a. すべての圧縮ファイルを検索するには、[すべての圧縮ファイルの検索] を選択します。この設定が最も安全です。
 - b. すべての圧縮ファイルをスキップするには、[圧縮ファイルを検索しない] を選択します。圧縮ファイルはいっさい検索されません。
 - c. ファイル数、解凍後のサイズ、圧縮階層数、および圧縮率に基づいて圧縮添付ファイルを検索するには、[次の場合は圧縮ファイルを検索しない] を選択します。次に、圧縮添付ファイルを検索する際の条件を指定します。
 - **解凍後のファイル数が次の数を超える場合：** 圧縮添付ファイル内のファイルの最大数 (0 の場合は無制限)。制限に到達するまで、圧縮ファイル内のファイルが検索されます。
 - **解凍後のファイルサイズが次を超える場合：** 解凍後の最大ファイルサイズ。制限内の個別ファイルのみが検索されます。
 - **圧縮レイヤが次の数を超える場合：** 圧縮階層の最大数。制限に到達するまで、圧縮ファイル内のファイルが検索されます。
 - **圧縮ファイルに対する解凍後のファイルサイズが次の割合を超える場合：** 制限内の個別ファイルのみが検索されます。
3. [保存] をクリックします。

マクロ検索を有効にする

InterScan VirusWall では、マクロを含む添付ファイルを隔離できます。添付ファイルは SMTP 隔離ディレクトリに移動されます。これにより、マクロウイルスの脅威に対するセキュリティが強化されます。この機能が有効な場合、元のメールメッセージは受信者に送信され、添付ファイルのみが隔離されます。

添付ファイルを隔離するには

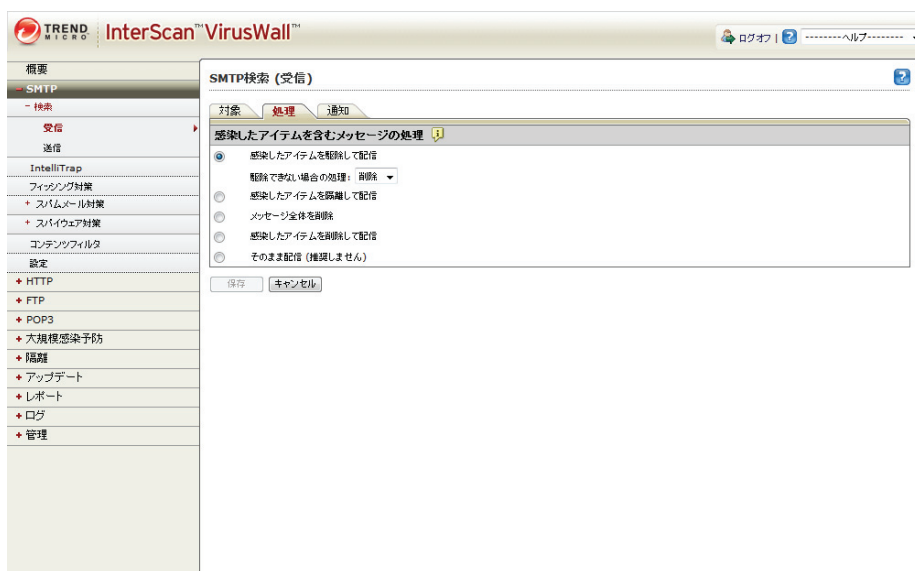
1. 左側のメニューで [SMTP] → [検索] → [受信] (または [送信]) の順に選択し、[対象] タブを選択します。
2. [マクロ検索] で [マクロを含むすべての Microsoft Office ファイルを隔離する] を選択します。
3. [保存] をクリックします。

注意： 初期設定の SMTP 検索用隔離フォルダは、インストールフォルダ下の %quarantine%smtp です。

ウイルス検出時に実行する処理を指定する

InterScan VirusWall では、ウイルス検出時に 5 つの処理のうちの 1 つを実行できます。図 4-3 に示している [SMTP] → [検索] → [処理] タブで利用可能な処理を指定できます。

図 4-3. [SMTP] → [検索] → [処理] タブ



InterScan VirusWall による感染添付ファイルの検出時に実行する処理を指定するには

1. 左側のメニューで [SMTP] → [検索] → [受信] (または [送信]) の順に選択し、[処理] タブを選択します。
2. [感染したアイテムを含むメッセージの処理] で、必要なオプションを選択します。
 - 感染した添付ファイルをウイルス駆除して、メッセージを配信するには、[感染したアイテムを駆除して配信] を選択します。次に、感染した添付ファイルをウイルス駆除できない場合に実行する処理を選択します。
 - **隔離**: 添付ファイルを取り除いて隔離します。
 - **削除**: 添付ファイルを隔離せずに削除します。
 - **放置**: 添付ファイルをメッセージと一緒に配信します。
 - 添付ファイルをウイルス駆除せずに隔離し、メッセージを配信するには、[感染したアイテムを隔離して配信] を選択します。
 - メッセージを削除するには、[メッセージ全体を削除] を選択します。

- 添付ファイルを削除して、メッセージを配信するには、[感染したアイテムを削除して配信] を選択します。
 - 感染した添付ファイルと一緒にメッセージを配信するには、[そのまま配信 (推奨しません)] を選択します。
3. [保存] をクリックします。

注意： 初期設定の SMTP 検索用隔離フォルダは、インストールフォルダ下の %quarantine%smtp です。

ウイルス検索通知を設定する

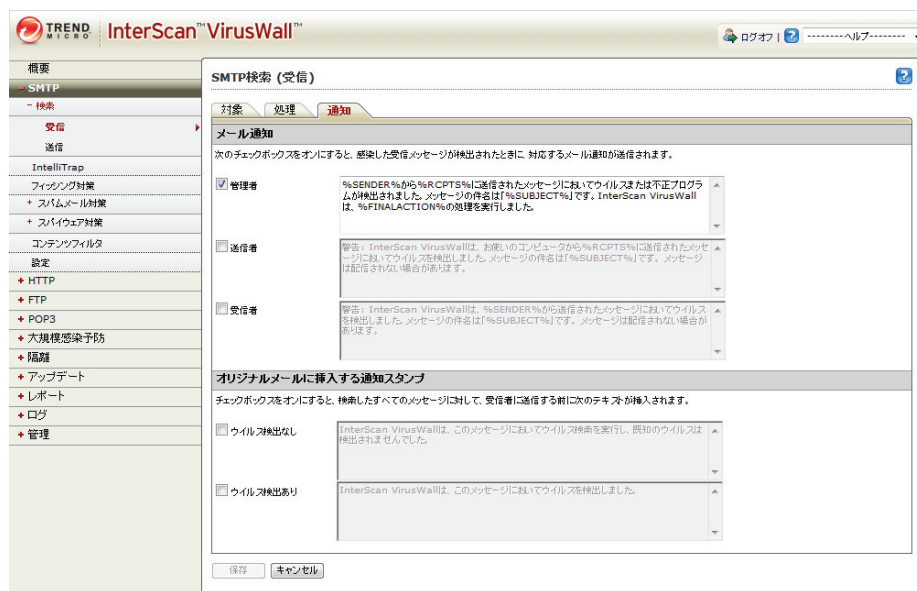
ウイルスの検出時に、InterScan VirusWall から管理者、メッセージ受信者、または送信者に通知が送信されるように設定できます。設定を指定したり、検索したすべてのメッセージにインライン通知を含めたり、受信メッセージと送信メッセージに別個の通知設定を指定することができます。

ウイルス検出時の通知設定を指定する

送受信メッセージの添付ファイルでウイルスが検出された場合の通知設定を指定するには

1. 左側のメニューで [SMTP] → [検索] → [受信] (または [送信]) の順に選択し、図 4-4 に示している [通知] タブを選択します。

図 4-4. [SMTP] → [検索] → [通知] タブ



2. [メール通知] で、ウイルス検出時に送信する通知の受信者を選択します。
3. 各受信者に送信するメッセージを作成します。メッセージ内に次の任意のタグを使用します。

タグ	説明
%SENDER%	送信者アドレス
%RCPTS%	受信者アドレス

タグ	説明
%SUBJECT%	メールの件名
%DATETIME%	検索日時
%MAILID%	メールメッセージ ID
%PROTOCOL%	メールプロトコル
%FILTERNAME%	処理を実行するフィルタの名前
%FINALACTION%	実行された処理
%QUARANTINE_AREA%	隔離場所
%MACHINENAME%	InterScan VirusWall コンピュータのホスト名

4. [保存] をクリックします。

インライン通知設定を指定する

InterScan VirusWall では、インライン通知と呼ばれるテキストを送受信メッセージのメッセージ本文に挿入できます。メッセージの種類の [ウイルス検出なし] および [ウイルス検出あり] を選択すると、検索されたすべてのメッセージにインライン通知が表示されます。

受信または送信メッセージのインライン通知設定を指定するには

1. 左側のメニューで [SMTP] → [検索] → [受信] (または [送信]) の順に選択し、[通知] タブをクリックします。
2. [オリジナルメールに挿入する通知スタンプ] (図 4-5 を参照) で、インライン通知を含めるメッセージの種類 ([ウイルス検出なし] および [ウイルス検出あり]) を選択します。
3. メッセージ本文に挿入するインライン通知を入力します。
4. [保存] をクリックします。

注意： 通知は、InterScan_SafeStamp.txt ファイルとして元のメッセージに添付されます。

図 4-5. 【オリジナルメールに挿入する通知スタンプ】

オリジナルメールに挿入する通知スタンプ

チェックボックスをオンにすると、検索したすべてのメッセージに対して、受信者に送信する前に次のテキストが挿入されます。

☐ ウイルス検出なし	InterScan VirusWallは、このメッセージに対してウイルス検索を実行し、既知のウイルスは検出されませんでした。
☐ ウイルス検出あり	InterScan VirusWallは、このメッセージに対してウイルスを検出しました。

保存 キャンセル

SMTP ファイル全体検索

SMTP ファイル全体検索は、通常のメールのウイルス検索を補足する検索です。ファイル全体検索では、通常の検索方法では検出できない特別な種類のメールのウイルスを検出することができます。ファイル全体検索は、製品フォルダにある intscan.ini ファイルから設定できます。

注意： SMTP ファイル全体検索は、InterScan VirusWall の Web コンソールから設定することができません。SMTP ファイル全体検索の設定には、InterScan VirusWall 製品フォルダにある intscan.ini ファイルを使用してください。

ファイル全体検索の動作

InterScan VirusWall で受信メールまたは送信メールが受領されると、まずウイルスフィルタでテストされます。ウイルスフィルタでウイルスが検出されなかった場合には、次にファイル全体フィルタでテストされます。メールによってファイル全体フィルタがトリガされた場合、メールにはウイルスが含まれており、このメッセージに対する処理が実行され、通知送信が有効化されている場合には管理者、送信者、および受信者への通知が送信されます。

SMTP ファイル全体検索を設定する

ファイル全体検索の設定は、4つのステッププロセスにより行います。まず、ファイル全体検索を有効化します。次に、ウイルス検出時に実行する処理を設定します。次に、ウイルスが検出されたことを管理者と受信者に通知する通知メッセージを設定します。

注意： ファイル全体検索は初期設定で無効にされています。

ファイル全体検索を有効または無効にする

ファイル全体検索を有効 / 無効にするには

1. InterScan VirusWall 製品フォルダを開き、intscan.ini ファイルを見つけます。
2. 任意のテキストエディタプログラムで、intscan.ini ファイルを開きます。
3. 画面を下方方向にスクロールし、次の値を見つけます。
InboundWholeMailVirusScan
OutboundWholeMailVirusScan
4. ファイル全体検索を有効にするには、値を「yes」に、無効にするには値を「no」に設定します。
5. ファイルを保存し、閉じます。
6. InterScan VirusWall サーバを再起動すると、変更が適用されます。

処理を設定する

ファイル全体フィルタでウイルスが検出されたときに実行できる処理は、[削除] か [隔離] のどちらかです。初期設定は [削除] です。メールを隔離するには、[隔離] を設定します。

ファイル全体フィルタでのウイルス検出時に実行する処理を設定するには

1. InterScan VirusWall 製品フォルダを開き、intscan.ini ファイルを見つけます。
2. 任意のテキストエディタプログラムで、intscan.ini ファイルを開きます。
3. 画面を下方方向にスクロールし、次の値を見つけます。

WholeMailScanAction

注意： ファイル全体フィルタでウイルスが検出されたときに実行できる処理は 2 つあります。ファイル全体フィルタの初期設定は [削除] です。

4. ファイル全体フィルタでのウイルス検出時に実行する処理を設定します。
 - Delete
 - Quarantine
5. ファイルを保存し、閉じます。
6. InterScan VirusWall サーバを再起動すると、変更が適用されます。

通知を送信する

ファイル全体フィルタでウイルスが検出された場合、通知メッセージを管理者、送信者、および受信者へ送信することができます。Web コンソールから、これらの一部または全部の人々に対する通知の有効化 / 無効化が可能です。InterScan VirusWall には初期設定の通知メッセージが備わっています。この通知メッセージを Web コンソールから修正できます。通知の設定手順については、71 ページの「ウイルス検索通知を設定する」参照を参照してください。

IntelliTrap を設定する

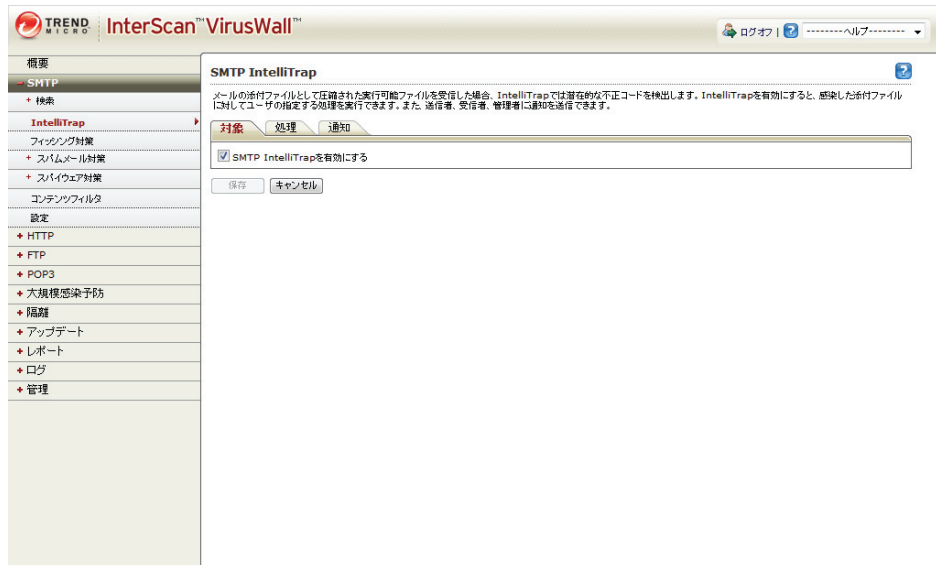
IntelliTrap では、メールの添付ファイルとして着信した、リアルタイム圧縮された実行可能ファイル内で、不正プログラムコードと疑われるものが検出されます。IntelliTrap を有効にすると、感染している添付ファイルに対しユーザ定義の処理を実行し、送信者、受信者、または管理者に通知を送信できます。

SMTP IntelliTrap 検索を有効または無効にする

SMTP IntelliTrap 検索を有効または無効にするには

1. 図 4-6 に示すように、左側のメニューで [SMTP] → [IntelliTrap] の順に選択し、[対象] タブを選択します。

図 4-6. [SMTP] → [IntelliTrap] → [対象] タブ



2. IntelliTrap 検索を有効または無効にするには、[SMTP IntelliTrap を有効にする] チェックボックスをオンまたはオフにします。
3. [保存] をクリックします。

IntelliTrap による検出時の処理を指定する

IntelliTrap によって不正プログラムコードと疑われるものが検出された場合に実行する処理を 3 つの中から 1 つ選択できます。

IntelliTrap によって不正プログラムコードと疑われるものが検出された場合に実行する処理を指定するには

1. 図 4-7 に示すように、左側のメニューで [SMTP] → [IntelliTrap] の順に選択し、[処理] タブを選択します。

図 4-7. [IntelliTrap] → [処理] タブ



2. [感染した添付ファイルを含むメッセージの処理] で、必要なオプションを選択します。

- 添付ファイルを隔離して、メッセージを配信するには、[感染した添付ファイルを隔離して配信] を選択します。ユーザは添付ファイルのないメッセージを受信します。添付ファイルは隔離フォルダに保存されます。
- 添付ファイルを削除して、メッセージを配信するには、[感染した添付ファイルを削除して配信] を選択します。ユーザは添付ファイルのないメッセージを受信します。
- 感染した添付ファイルと一緒にメッセージを配信するには、[そのまま配信 (推奨しません)] を選択します。ユーザは添付ファイルの付いたメッセージとインライン警告を受信します。

3. [保存] をクリックします。

注意： 初期設定の SMTP 検索用隔離フォルダは、インストールフォルダ下の ¥quarantine¥smtp です。

IntelliTrap 通知を設定する

InterScan VirusWall では、IntelliTrap によって圧縮形式の実行ファイルで不正プログラムコードと疑われるものが検出された場合に、選択した受信者に自動的に通知できます。

IntelliTrap によってメッセージの添付ファイルでセキュリティの脅威が検出された場合の通知設定を指定するには

1. 図 4-8 に示すように、左側のメニューで [SMTP] → [IntelliTrap] の順に選択し、[通知] タブを選択します。

図 4-8. [SMTP] → [IntelliTrap] → [通知] タブ



2. IntelliTrap によってセキュリティリスクが検出された場合に送信する通知の受信者を選択します。
3. 各受信者に送信するメッセージを作成します。メッセージ内に次の任意のタグを使用します。

タグ	説明
%SENDER%	送信者アドレス
%RCPTS%	受信者アドレス
%SUBJECT%	メールの件名
%DATETIME%	検索日時
%MAILID%	メールメッセージ ID

タグ	説明
%PROTOCOL%	メールプロトコル
%FILTERNAME%	処理を実行するフィルタの名前
%FINALACTION%	実行された処理
%QUARANTINE_AREA%	隔離場所
%MACHINENAME%	InterScan VirusWall コンピュータのホスト名

4. [保存] をクリックします。

SMTP フィッシング対策を設定する

フィッシングとは、急増している詐欺の 1 つで、正規の Web サイトを模倣し、Web ユーザに個人情報を開示させることです。フィッシング攻撃は、既存の正規の組織を偽装したメールメッセージから始まります。メッセージには通常、リンクが記載されており、受信者にこのリンクをクリックさせるように仕向け、ブラウザを偽の Web サイトに誘導します。Web サイトでは個人情報をアップデートするよう求められます。疑いを持たないユーザは、パスワード、クレジットカード番号などを提供してしまいます。

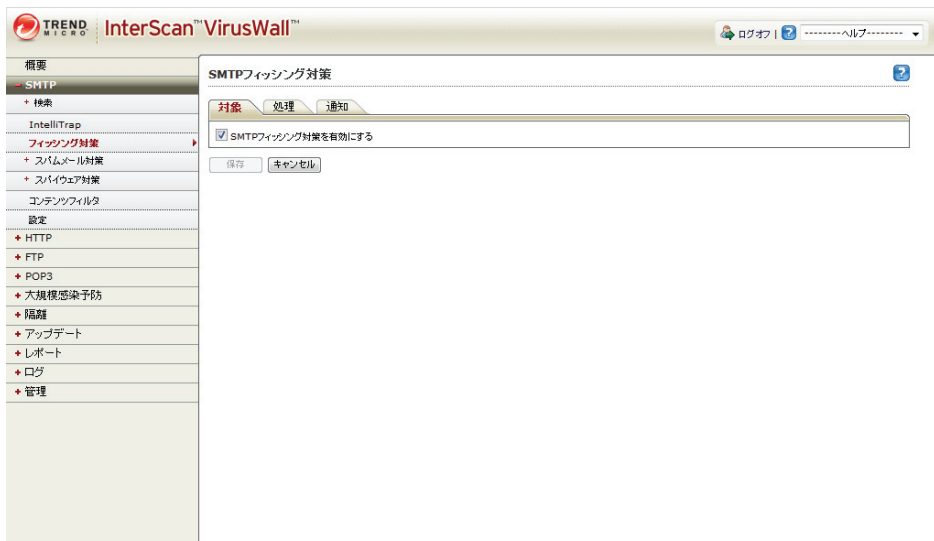
典型的なシナリオでは、疑いを持たないユーザが緊急を装う（本物のような）メールを受信します。そこには、ユーザのアカウントにすぐに解決しなければならない問題があり、解決しなければアカウントが閉じられると書かれています。そのメールには、本物に非常によく似た Web サイトの URL が含まれています。正規のメールと正規の Web サイトをコピーした後、バックエンドを変更するのは簡単です。収集したデータは実際にはこのバックエンドに送信されます。

SMTP フィッシング対策を有効にする

SMTP フィッシング対策機能を有効にするには

1. 図 4-9 に示すように、左側のメニューで [SMTP] → [フィッシング対策] の順に選択し、[対象] タブを選択します。
2. [SMTP フィッシング対策を有効にする] チェックボックスをオンにします。
3. [保存] をクリックします。

図 4-9. [SMTP] → [フィッシング対策] → [対象] タブ



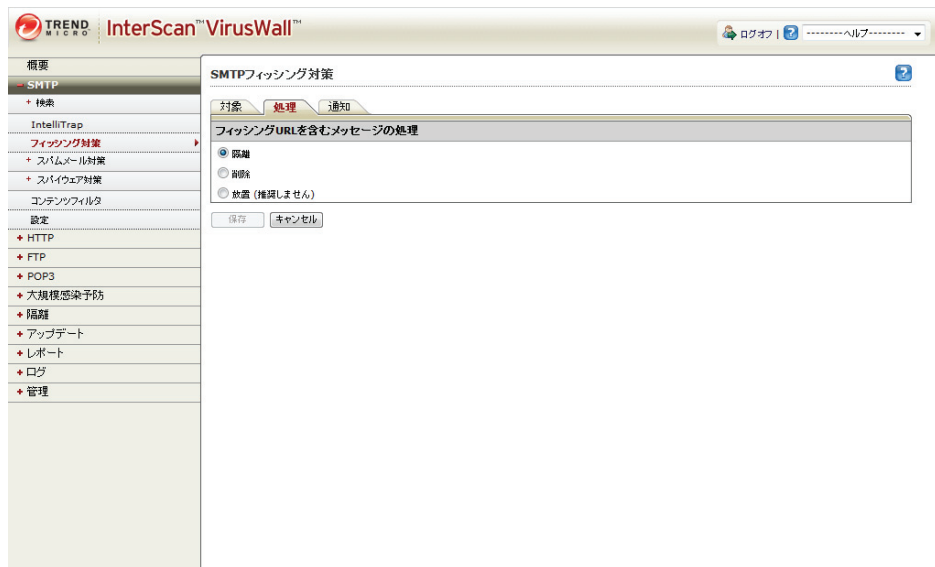
フィッシングメールの検出時に実行する処理を指定する

フィッシングメールに対する処理を指定するには

1. 図 4-10 に示すように、左側のメニューで [SMTP] → [フィッシング対策] の順に選択し、[処理] タブを選択します。
2. フィッシングメールに対する処理を選択します。
 - メッセージを隔離フォルダに移動する場合は、[隔離] を選択します。
 - メッセージを配信せずに削除する場合は、[削除] を選択します。
 - フィッシングメールを通常どおりに配信する場合は、[放置] を選択します。

3. [保存] をクリックします。

図 4-10. [SMTP] → [フィッシング対策] → [処理] タブ



フィッシングメール検出時の通知を指定する

InterScan VirusWall では、フィッシングメールの検出時に、管理者または受信者、あるいはその両方にメール通知を送信できます。フィッシングサイトの疑いのあるサイトや既知のフィッシングサイトを TrendLabs に報告できます。図 4-11 の [SMTP] → [フィッシング対策] → [通知] タブでは、InterScan VirusWall によるフィッシングサイトの検出時にメール通知を送信するかどうかを指定できます。

図 4-11. [SMTP] → [フィッシング対策] → [通知] タブ



フィッシング URL 検出時の通知設定を指定するには

1. 左側のメニューで [SMTP] → [フィッシング対策] の順に選択し、[通知] タブを選択します。
2. InterScan VirusWall によるフィッシングメールの検出時に通知を送信する受信者を選択します。
3. 各受信者に送信するメッセージを作成します。メッセージ内に次の任意のタグを使用します。

タグ	説明
%SENDER%	送信者アドレス
%RCPTS%	受信者アドレス

タグ	説明
%SUBJECT%	メールの件名
%HEADERS%	メールヘッダ
%DATETIME%	検索日時
%MAILID%	メールメッセージ ID
%PROTOCOL%	メールプロトコル
%FILTERNAME%	処理を実行するフィルタの名前
%DETECTED%	検出されたセキュリティリスクの名前
%FINALACTION%	実行された処理
%QUARANTINE_AREA%	隔離場所
%MACHINENAME%	InterScan VirusWall コンピュータのホスト名

4. [保存] をクリックします。

フィッシングサイトの可能性のある URL を報告する

フィッシングサイトの疑いのあるサイトまたは既知のフィッシングサイトを TrendLabs に報告するには、[TrendLabs (トレンドラボ) への疑わしいフィッシング URL の送信] をクリックし、メールにそのサイトの URL を記載して、antifraud@support.trendmicro.com に送信してください。

TrendLabs では、詐欺目的のために情報を取得するサイトを監視し、InterScan VirusWall のユーザにトレンドマイクロから提供される自動アップデートの一部として既知のフィッシングサイトの情報を配布します。

SMTP スпамメール対策を設定する

InterScan VirusWall では、次の機能を使用して、SMTP メール通信でスパムメールをフィルタします。

- **Trend Micro Email Reputation Services:** スпамメール、フィッシングメール、その他の疑わしいメールからの保護をそれらがネットワークに到達する前に提供します。このサービスを有効化すると IP アドレスの包括的なデータベースへオンラインでアクセスし、スパムメール、オープンプロキシ、オープンリレー、動的 IP アドレスの既知の発信元などの情報を取得します。また、スパムメールの送信元に対して、動的かつリアルタイムの検出とブロックを行い、ネットワークをボットネットやゾンビ攻撃などから保護します。
- **承認する送信者およびブロックする送信者リスト:** これらのリストでは、コンテンツではなく、送信者のメールアドレスに基づいてフィルタされます。InterScan VirusWall では、承認する送信者のメッセージは常に配信され、ブロックする送信者のメッセージは常にスパムメールとして分類されます。

注意： Exchange 管理者は、Exchange サーバ用の [承認する送信者] および [ブロックする送信者] の個別のリストを管理します。エンドユーザが承認する送信者を登録し、その送信者が管理者の [ブロックする送信者] リストに登録されている場合、その送信者からのメッセージはブロックされます。

- **スパムメールフィルタ:** 管理者はスパムメールのフィルタに使用するスパムメール検出レベルを設定します。検出レベルが高いほど、スパムメールとして分類されるメッセージは多くなります。すべてのメッセージに共通の検出レベルを設定するか、スパムメールカテゴリごとに 1 つの検出レベルを設定できます。

検出レベルによって、InterScan VirusWall が疑わしいメールメッセージをどの程度許容するかが決まります。

- ◆ 「高」の検出レベルでは、多数のメールがスパムメールとして隔離されます。ただし、正規のメールメッセージがスパムメールと誤認識されて隔離され、「誤検出された」スパムメールとなる可能性もあります。
- ◆ 「低」の検出レベルでは、メールメッセージの選別は厳しくなく、スパムメールメッセージの誤検出が多数発生することはありません。

SMTP スпамメール対策 (メールレピュテーション) を有効にする

[SMTP] → [スパムメール対策] → [対象] タブにより、メールレピュテーションを有効にして、希望するサービスレベルを指定できます。

SMTP スпамメール対策 (メールレピュテーション) を有効にするには

1. 左側のメニューで [SMTP] → [スパムメール対策] → [メールレピュテーション] の順に選択します。
2. [対象] タブを選択します。
3. [SMTP スпамメール対策を有効にする (メールレピュテーション)] チェックボックスをオンにします。
4. [保存] をクリックします。

サービスレベルを設定する

メールレピュテーションのサービスレベルを設定するには

1. 左側のメニューで [SMTP] → [スパムメール対策] → [メールレピュテーション] の順に選択します。
2. [対象] タブを選択します。
3. [SMTP スпамメール対策を有効にする (メールレピュテーション)] チェックボックスをオンにします。
4. サービスレベルを選択します。
 - **標準 (推奨)**: InterScan VirusWall は RBL データベースにのみクエリを実行します。この設定では、正当なメールを誤ってスパムメールと特定する (誤検出) 可能性は低くなります。誤検出の可能性を考慮する場合はこの設定を使用します。
 - **詳細**: InterScan VirusWall は RBL データベースにクエリを実行し、問題ない場合は次に QIL データベースにクエリを実行します。この設定では、正当なメールを誤ってスパムメールと特定する (誤検出) 可能性が高くなります。
5. [保存] をクリックします。

承認する IP アドレスリストを管理する

承認する IP アドレスリストを管理するには

1. 左側のメニューで [SMTP] → [スパムメール対策] → [メールレピュテーション] の順に選択します。
2. [対象] タブを選択します。
3. [SMTP スパムメール対策を有効にする (メールレピュテーション)] チェックボックスをオンにします。
4. 承認する IP アドレスを追加します。
 - a. [許可する IP アドレス] に、検索対象から除外する IP アドレスを 1 つまたは複数入力します。
 - b. [追加] をクリックします。
5. [保存] をクリックします。

メールレピュテーションの処理を設定する

SMTP スパムメール対策 (メールレピュテーション) の処理を有効にするには

1. 左側のメニューで [SMTP] → [スパムメール対策] → [メールレピュテーション] の順に選択し、[処理] タブを選択します。
2. 既知のスパムメールソースである IP アドレスから送信されたメッセージを検出したときに InterScan VirusWall が実行する処理を、以下の中から 1 つ選択します。

RBL+ についての処理 (低設定および高設定の両方に適用)

- 接続が拒否され、エラーメッセージがユーザに送信されます。ユーザは SMTP エラーコードを受信します (400 - 599 の範囲、初期設定 =550)。
- 接続が拒否され、エラーメッセージはユーザに送信されません。
- そのまま配信 (推奨しません)

QIL+ についての処理 (高設定に適用)

- 接続が拒否され、エラーメッセージがユーザに送信されます。ユーザは SMTP エラーコードを受信します (400 - 599 の範囲、初期設定 =450)。
- 接続が拒否され、エラーメッセージはユーザに送信されません。
- そのまま配信 (推奨しません)

3. [保存] をクリックします。

SMTP スпамメール対策 (コンテンツ検索) を有効にする

図 4-12 に示している [SMTP] → [スパムメール対策] → [対象] タブでは、スパムメールのフィルタを有効にできます。

図 4-12. [SMTP] → [スパムメール対策] → [対象] タブ



SMTP スпамメール対策コンテンツ検索を有効にするには

1. 左側のメニューで [SMTP] → [スパムメール対策] → [コンテンツ検索] の順に選択します。
2. [対象] タブを選択します。
3. [SMTP スпамメール対策を有効にする] (コンテンツ検索) チェックボックスをオンにします。
4. [保存] をクリックします。

スパムメール検出レベルを設定する (フィルタ調整)

スパムメール検出レベルを指定するには

1. 左側のメニューで [SMTP] → [スパムメール対策] → [コンテンツ検索] の順に選択します。
2. [対象] タブを選択します。
3. [フィルタ調整] で、任意のスパムメール検出レベルを選択します。

スパムメール検出レベル

InterScan VirusWall では、次の検出レベルが使用されます。

検出レベル	フィルタ基準
低	最も明白で一般的なスパムメールメッセージのみがフィルタされ、誤検出の確率も非常に低くなります。これは、最も寛容なスパムメール検出レベルです。
中	高いスパムメール検出レベルで監視が実行されます。誤検出の可能性は中程度です。これは、初期設定です。
高	すべてのメールメッセージで疑わしいファイルまたはテキストが監視されますが、誤検出の可能性も非常に高くなります。これは、最も厳しいスパムメール検出レベルです。

スパムメール検出レベルを決定する

InterScan VirusWall スパムメール検索エンジンでは、ヒューリスティックとアルゴリズムを使用してスパムメール検出レベルが計算されます。このエンジンでは、メッセージまたはファイルが検索され、検索されたアイテムにスパムメールスコアが割り当てられます。対象のアイテムがスパムメールかどうかの判断は、割り当てられたスパムメールスコアと、指定されたスパムメール検出レベルおよび確実性レベルに基づきます。

しきい値の例は、次のとおりです。

	低の確実性	中の確実性	高の確実性
低の検出レベル	6	7	10
中の検出レベル	4.5	6	10
高の検出レベル	4	5	7

注意： スパムメールしきい値設定テーブルのスコアは、使用中のスパムメール判定ルールにより異なることがあります。

- 低の検出レベルを指定し、スパムメールスコアが 6.5 の場合は、低の確実性レベルに指定された処理が実行されます。
- スパムメールスコアが 8 の場合は、中の確実性レベルに指定された処理が実行されます。

- スпамメールスコアが 11 の場合は、高の確実性レベルに指定された処理が実行されます。

スパムメールスコアを確認するには、スパムメールログを参照してください。次に、エントリの例を示します。

```
04.02.09 20:10:32, SMTP, , Stamp, Success, "LastName¥, FirstName"
<FirstName.LastName@Level3.com>, "SPAM@TrendMicro.com"
<SPAM@TrendMicro.com>, FW:How are you doing?
<D7626E4452B0F745B4C7C15BC97EA052D66887@idcllexc0005.corp.global.
level3.com>, 3.51.0.1033, 13974000, Spam, ,14.594000
```

スパムメールフィルタを調整する

過剰な数の誤検出がある場合は、スパムメール検出レベルの設定を低くします。逆に、スパムメールを多く受け取りすぎるとユーザが報告する場合は、検出レベルの設定が高くなるように調整します。

キーワード除外を指定する

キーワードの除外を指定して、スパムメールフィルタから特定のテキストを含むメッセージを除外できます。例外リスト内の各キーワードはカンマで区切ります。図 4-13 に示している [キーワード除外設定] ボックスに、スパムメールとは見なさないキーワードを入力します。

注意： キーワード間には単一のカンマ (,) 以外の記号を挿入できません。スペースや改行を挿入しないでください。

キーワード除外設定 指定されたキーワードを含むメッセージは、スパムメールと判定されません。複数入力する場合は、カンマ(,)で区切ってください。
承認する送信者 承認する送信者のメールアドレスまたはドメイン名を追加します (例: example.com, abc@example.com, @example.com)。複数入力する場合は、カンマ(,)で区切ってください。
ブロックする送信者 ブロックする送信者のメールアドレスまたはドメイン名を追加します (例: example.com, abc@example.com, @example.com)。複数入力する場合は、カンマ(,)で区切ってください。
保存 キャンセル

図 4-13. [SMTP]→[スパムメール対策]→[キーワード除外設定]、[承認する送信者]、および[ブロックする送信者]リスト

承認する送信者およびブロックする送信者のリストを管理する

[承認する送信者] リストには、信頼されたメールアドレスが含まれます。InterScan VirusWall は、フィッシング対策が有効になっている場合を除いて、これらのアドレスから受信したメッセージをスパムメールとしてフィルタしません。

[ブロックする送信者] リストには、信頼できないメールアドレスが含まれます。これらのアドレスから着信したメッセージは、自動的にスパムメールと見なされて削除されます。メッセージが削除されたことは通知されません。

同じメールアドレスが [承認する送信者] リストと [ブロックする送信者] リストの両方に含まれる場合、そのアドレスから着信したメッセージはスパムメールと見なされて削除されます。

メールアドレスをリストに追加するときは、アドレスをカンマで区切ります。図 4-13 に示しているように、該当するリストにすべてのメールアドレスを入力します。

InterScan VirusWall は、[承認する送信者] および [ブロックする送信者] リストで、ワイルドカード (*) 照合をサポートします。パターンの例を表 4-1 に示します。

表 4-1. 送信者リストでのワイルドカード (*) の使用

パターン	一致する例	一致しない例
john@trend.com	john@trend.com john@trend.com.	一致する例以外のすべてのパターン
@trend.com *@trend.com	john@trend.com mary@trend.com.	john@ms1.trend.com john@trend.com.tw mary@trend.comon
trend.com	john@trend.com john@ms1.trend.com mary@ms1.rd.trend.com mary@trend.com.	john@trend.com.tw mary@mytrend.com joe@trend.comon
*.trend.com	john@ms1.trend.com mary@ms1.rd.trend.com joe@ms1.trend.com.	john@trend.com john@trend.com.tw mary@ms1.trend.comon

表 4-1. 送信者リストでのワイルドカード (*) の使用

パターン	一致する例	一致しない例
trend.com.*	john@trend.com.tw john@ms1.trend.com.tw john@ms1.rd.trend.com.tw mary@trend.com.tw.	john@trend.com john@ms1.trend.com. john@mytrend.com.tw
.trend.com.	john@ms1.trend.com.tw john@ms1.rd.trend.com.tw mary@ms1.trend.com.tw.	john@trend.com john@ms1.trend.com john@trend.com.tw john@ms1.trend.com.
..*trend.com *****trend.com	「*.trend.com」と同じ	「*.trend.com」と同じ
trend.com trend.com trend.*.com @*.trend.com	これらはすべて無効	これらはすべて無効

スパムメールと見なされたメッセージに対する処理を指定する

InterScan VirusWall では、メッセージがスパムメールと見なされた場合にいくつかの処理のうちの 1 つを実行できます。この処理は、[対象] タブで設定した検出レベルによって決まります。図 4-14 に、[SMTP] → [スパムメール対策] → [コンテンツ検索] → [処理] タブを示します。

図 4-14. [SMTP] → [スパムメール対策] → [コンテンツ検索] → [処理] タブ



スパムメールメッセージに対する処理を指定するには

1. 左側のメニューで [SMTP] → [スパムメール対策] → [コンテンツ検索] の順に選択し、[処理] タブを選択します。
2. 判定の確実性レベルに基づいて実行する処理を指定します。
 - ・ **高**: メールは確実にスパムメールであると思われます。
 - ・ **中**: メールはおそらくスパムメールであると思われます。
 - ・ **低**: メールはおそらくスパムメールではないと思われます。

それぞれの確実性レベルで、次の 4 つの処理の中の 1 つを選択できます。

- ・ **削除**: メッセージ全体が削除されます。
- ・ **隔離**: メッセージが隔離されます。
- ・ **スタンプの挿入**: 通知コンテンツスタンプがメッセージの件名行に挿入されます。
- ・ **放置**: InterScan VirusWall はメッセージに対して何も実行せず、通常どおり処理します。

スパムメール検出時の通知を指定する

InterScan VirusWall では、スパムメールメッセージの検出時に管理者または受信者に通知できます。メール通知の受信者を指定し、管理者およびメール受信者に送信するメッセージを作成できます。

図 4-15 に、[SMTP] → [スパムメール対策] → [コンテンツ検索] → [通知] 設定タブを示します。

図 4-15. [SMTP] → [スパムメール対策] → [コンテンツ検索] → [通知] 設定タブ



InterScan VirusWall によるスパムメールの検出時の通知設定を指定するには

1. 左側のメニューで [SMTP] → [スパムメール対策] → [コンテンツ検索] の順に選択し、[通知] タブを選択します。
2. [メール通知] で、スパムメールが検出された場合に通知を受ける受信者を選択します。
3. 各受信者に送信するメッセージを作成します。メッセージ内に次の任意のタグを使用します。

タグ	説明
%SENDER%	送信者アドレス
%RCPTS%	受信者アドレス
%SUBJECT%	メールの件名
%HEADERS%	メールヘッダ

タグ	説明
%DATETIME%	検索日時
%MAILID%	メールメッセージ ID
%PROTOCOL%	メールプロトコル
%FILTERNAME%	処理を実行するフィルタの名前
%DETECTED%	検出されたセキュリティリスクの名前
%FINALACTION%	実行された処理
%QUARANTINE_AREA%	隔離場所
%MACHINENAME%	InterScan VirusWall コンピュータのホスト名

4. [保存] をクリックします。

SMTP スパイウェア対策を設定する

スパイウェア / グレーウェアにはさまざまな形があり、多くの場合正規のソフトウェアプログラムのように見えます。トレンドマイクロは、スパイウェア / グレーウェアを追跡調査して、パターンファイルの定期アップデートを提供しています。

一般的なグレーウェアの種類は次のとおりです。

グレーウェアの種類	一般的な動作
スパイウェア	アカウントのユーザ名やパスワードなどのデータを収集して第三者に転送します。
アドウェア	広告を表示して、ユーザのネットサーフィンの傾向などについてデータを収集し、Web ブラウザを介してユーザを広告のターゲットにします。
ダイヤラー	コンピュータのインターネット設定を変更し、事前設定された電話番号にコンピュータがモデム経由で電話するように強制します。
ジョークプログラム	CD-ROM トレイの開閉や多数のメッセージボックスの表示など、コンピュータの異常動作を引き起こします。
ハッキングツール	ハッカーがコンピュータに侵入するのを助けます。

グレーウェアの種類	一般的な動作
リモートアクセス ツール	ハッカーがコンピュータにリモートアクセスして制御 するのを助けます。
パスワード解読 アプリケーション	ハッカーがアカウントのユーザ名とパスワードを解読 するのを助けます。
その他	ここに記載されていないその他の種類

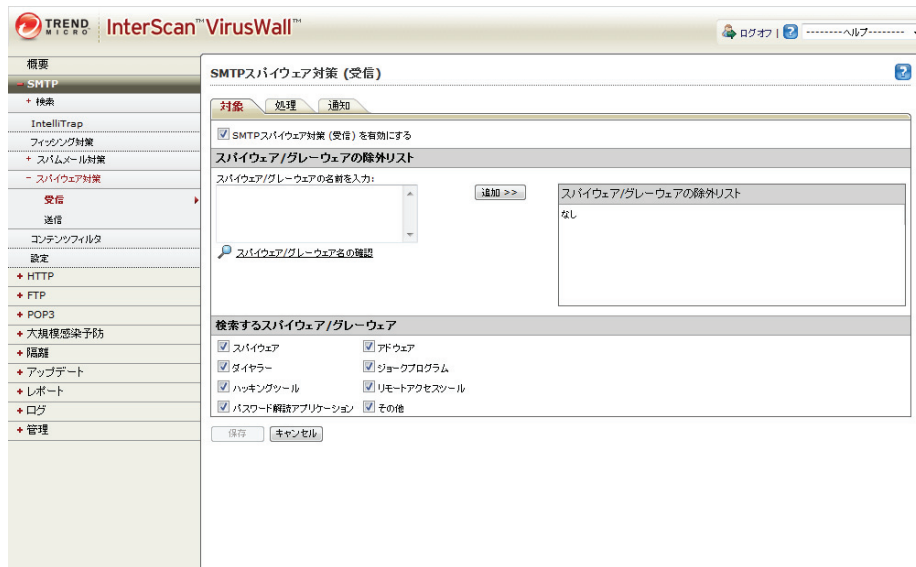
SMTP スパイウェア検索 (受信または送信) を有効にする

SMTP スパイウェア検索を有効にするには

1. 左側のメニューで [SMTP] → [スパイウェア対策] → [受信] (または [送信]) の順に選択し、[対象] タブを選択します。
2. [SMTP スパイウェア対策 (受信) を有効にする] または [SMTP スパイウェア対策 (送信) 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。

図 4-16 に、[SMTP] → [スパイウェア対策] → [対象] タブを示します。ここでは、SMTP スパイウェア検索を有効にして、スパイウェアの種類と除外対象を指定できます。

図 4-16. [SMTP] → [スパイウェア対策] → [受信] → [対象] タブ



スパイウェア検索の除外リストを設定する

スパイウェア / グレーウェアの検索から除外する特定のファイル名またはファイル名拡張子をリストするには

1. 左側のメニューで [SMTP] → [スパイウェア対策] → [受信] (または [送信]) の順に選択し、[対象] タブを選択します。
2. [スパイウェア / グレーウェアの名前を入力] に、スパイウェア / グレーウェア検索の対象から除外するスパイウェア名を入力します。
スパイウェア名が不明な場合は、[スパイウェア / グレーウェア名の確認] リンクをクリックします。
3. [追加] をクリックします。
4. [保存] をクリックします。

注意： 除外リストのエントリを削除するには、ごみ箱アイコンをクリックします。[保存] をクリックして変更内容を確定します。

検索するスパイウェアおよびグレーウェアの種類を指定する

InterScan VirusWall の SMTP サービスで検索するスパイウェアおよびグレーウェアの種類を指定するには

1. 左側のメニューで [SMTP] → [スパイウェア対策] → [受信] (または [送信]) の順に選択し、[対象] タブを選択します。
2. [検索するスパイウェア / グレーウェア] で、SMTP サービスで検索するスパイウェアとグレーウェアの種類を指定します。
3. [保存] をクリックします。

スパイウェア検出時に実行する処理を指定する

InterScan VirusWall では、スパイウェアなどのグレーウェアの検出時に、3つの処理のうちの1つを実行できます (図 4-17 を参照)。

図 4-17. [SMTP] → [スパイウェア対策] → [受信] → [処理] タブ



スパイウェア / グレーウェアの検出時に実行する処理を指定するには

1. 左側のメニューで [SMTP] → [スパイウェア対策] → [受信] (または [送信]) の順に選択し、[処理] タブを選択します。
2. [スパイウェア / グレーウェアを含むメッセージの処理] で、必要なオプションを選択します。
 - 添付ファイルを隔離して、メッセージを配信するには、[スパイウェア / グレーウェアを隔離して配信] を選択します。ユーザは添付ファイルのないメッセージを受信します。添付ファイルは隔離フォルダに保存されます。
 - 検出された添付ファイルを削除して、メッセージを配信するには、[スパイウェア / グレーウェアを削除して配信] を選択します。ユーザは添付ファイルのないメッセージを受信します。
 - 検出された添付ファイルと一緒にメッセージを配信するには、[そのまま配信 (推奨しません)] を選択します。
3. [保存] をクリックします。

スパイウェアの検出時の通知を指定する

受信メッセージまたは送信メッセージでスパイウェアなどのグレーウェアが検出された場合に、受信者、および管理者に通知を送信するかどうかを指定できます (図 4-18 を参照)。

図 4-18. [SMTP] → [スパイウェア対策] → [受信] → [通知] タブ



スパイウェア / グレーウェア検出時の通知設定を指定するには

1. 左側のメニューで [SMTP] → [スパイウェア対策] → [受信] (または [送信]) の順に選択し、[通知] タブを選択します。
2. スパイウェアまたはグレーウェアの検出時に送信される通知の受信者を選択します。
3. 各受信者に送信するメッセージを作成します。メッセージ内に次の任意のタグを使用します。

タグ	説明
%SENDER%	送信者アドレス
%RCPTS%	受信者アドレス
%SUBJECT%	メールの件名
%DATETIME%	検索日時
%MAILID%	メールメッセージ ID

タグ	説明
%PROTOCOL%	メールプロトコル
%FILTERNAME%	処理を実行するフィルタの名前
%FINALACTION%	実行された処理
%QUARANTINE_AREA%	隔離場所
%MACHINENAME%	InterScan VirusWall コンピュータのホスト名

4. [保存] をクリックします。

SMTP コンテンツフィルタ

InterScan VirusWall には、SMTP 用のメールコンテンツフィルタが用意されています。この機能は、SMTP を使用してネットワーク上で送受信される情報の監視および管理をリアルタイムに実行します。

SMTP コンテンツフィルタを有効にする

SMTP コンテンツフィルタを有効にすると、SMTP を介してネットワーク上で送受信されるすべての情報で、SMTP トラフィックのコンテンツフィルタ用に定義したポリシーと一致するものが検索されます。図 4-19 に、コンテンツフィルタ設定を示します。[ポリシー] には、コンテンツフィルタ用に定義されているすべてのポリシーが一覧表示されます。

図 4-19. SMTP コンテンツフィルタ設定



SMTP コンテンツフィルタを有効にするには

1. 左側のメニューで [SMTP] → [コンテンツフィルタ] の順に選択します。
2. [コンテンツフィルタ設定] で、[SMTP コンテンツ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。

SMTP コンテンツフィルタを無効にする

SMTP コンテンツフィルタを無効にすると、SMTP トラフィックのコンテンツは監視されなくなります。有効化されている他の SMTP 検索機能は、指定されたとおりに引き続き機能します。

SMTP コンテンツフィルタを無効にするには

1. 左側のメニューで [SMTP] → [コンテンツフィルタ] の順に選択します。
2. [コンテンツフィルタ設定] で、[SMTP コンテンツフィルタを有効にする] チェックボックスをオフにします。
3. [保存] をクリックします。

ポリシーを作成する

InterScan VirusWall では、キーワードフィルタまたは添付ファイルフィルタを使用できるポリシーを使用します。

ポリシーを作成するには

ポリシーを作成するには、[キーワードフィルタの追加] または [添付ファイルフィルタの追加] をクリックします。

キーワードに基づいた SMTP コンテンツフィルタポリシーを作成する

キーワードフィルタを使用すると、InterScan VirusWall の管理者は、メールメッセージの配信をメッセージの内容自体に基づいて評価し、制御できます。キーワードフィルタを使用すれば、受信メッセージと送信メッセージの両方を監視して、機密扱いまたは不快なコンテンツの有無をチェックできます。キーワードフィルタでは、ポリシーの対象範囲を拡大する類義語チェック機能も利用できます。キーワードフィルタは、中国語や日本語によるメッセージなど、2 バイト文字によるコンテンツ検索をサポートしています。

キーワードリスト

所定のキーワードフィルタのキーワードリストには、メッセージ内容に対してフィルタで照合される語句が含まれます。複数のキーワードをポリシーの同一行に指定すると、その行のキーワードすべてが評価対象のメッセージに含まれている場合にのみ一致と見なされます。次にキーワードの例を示します。

例 1:

resume, position

resume, job

resume, experience

resume, enclosed

例 1 では、「resume」という単語が単一エントリとして 1 回だけ使用されるのではなく、追加の単語とともに 4 回使用されています。resume だけを使用すると、信頼できない結果が生じる可能性があります。これは、resume という単語に「履歴書」と「再開する」の両方の意味があるためです。こうした誤った一致が生じる可能性を最小限に抑えるには、最初の語と一般的に関連する語を追加して最初の語を限定すると効果的です。この例では、求職文書で使われることが多い enclosed (同封の)、position (職)、job (仕事)、experience (経験) などの単語が使用されています。複数のキーワードグループを指定すると、フィルタの対象範囲が増大します。

この例の設定では、いずれかのキーワードペアを含むメッセージが一致と見なされます。

または、1 つの送信メッセージで 5 つの単語全部が検出された場合にのみ、設定した処理を開始させることもできます。これを実行するには、1 行にすべてのキーワードを指定します。

例 2:

Resume, position, job, experience, enclosed

例 1 で示した「resume」に基づく複数のルールセットで構成されたポリシーと比べると、このフィルタに基づいてすべての resume が送信メッセージで検出される可能性は明らかに低下します。

例 3 に、例 2 の 4 つの単語のいずれかが検出されると一致と見なされるポリシーを示します。

例 3:

job

resume

enclosed

position

experience

一般に、AND 演算子で結合するキーワード数は 4 ～ 5 語以内にします。そうしないと、ポリシーが過度に制限されるおそれがあります。一方、特定の行で 1 つのキーワードしか指定しない場合 (OR 演算子)、ポリシーの許容範囲が広くなりすぎて、一致対象として検出されるメールメッセージの数が非常に多くなります。当然ですが、前述のとおり、これはフィルタ処理の対象にも大きく依存します。

指定する条件は、スペースや句読点を含めて入力したとおりに評価されます。カンマで区切られた句は、1 つの単位として扱われます。その句のそれぞれの語やスペースなどが入力した順序でメッセージに出現する場合にのみ一致が発生します。

キーワードリストの演算子

キーワード、およびキーワードの位置に基づいてキーワードに適用される論理演算子について、次に例を示します。

表 4-2. 論理演算子で示すキーワードリストと一致結果の例

ケース	結果
以下の例にあるブラケット [...] で囲まれた項目は、例示目的のみで示したものであり、キーワードリスト作成時には含めないようにしてください。	
ケース 1: 複数のキーワードを 1 行で指定 例 :Apple Juice, [AND] Pear, [AND] Orange 論理演算子「AND」と同じ機能を提供します。	「Apple Juice」(リンゴジュース)、「Pear」(ナシ)、「Orange」(オレンジ) のアイテムすべてを含むメッセージだけが一致と見なされます。その際、メッセージテキスト内の順序と場所は問われません。
ケース 2: 複数のキーワードを個別の行で指定 例 : Apple Juice [OR] Pear [OR] Orange 論理演算子「OR」と同じ機能を提供します。	「Apple Juice」を含むすべてのメッセージ、「Pear」を含むすべてのメッセージ、および「Orange」を含むすべてのメッセージがそれぞれ一致と見なされます。
ケース 3: 複数のキーワードを 1 行で指定し、類義語チェックを「Orange」に対して有効化 例 : Apple Juice, [AND] Pear, [AND] Orange (* 類義語リストにある「orangish」(オレンジがかった)、「red」(赤)、「yellow」(黄) の各語は、「Orange」(オレンジ色) と意味が似ています)。 論理演算子「AND」および「OR」と同じ機能を提供します。	類義語チェックを有効にすると、「Apple Juice」、「Pear」、および「Orange」、「orangish」、「red」、「yellow」のいずれかの語を含むメッセージが一致と見なされます。

その他のキーワードについて

Apple Juice は 1 つの語句と見なされます。これは、Apple と Juice の各語がカンマで区切られていないためです。Apple と Juice の両方の語がメッセージ内で使用されていても、Apple Juice のように一緒に使用されていない限り、一致は発生しません。

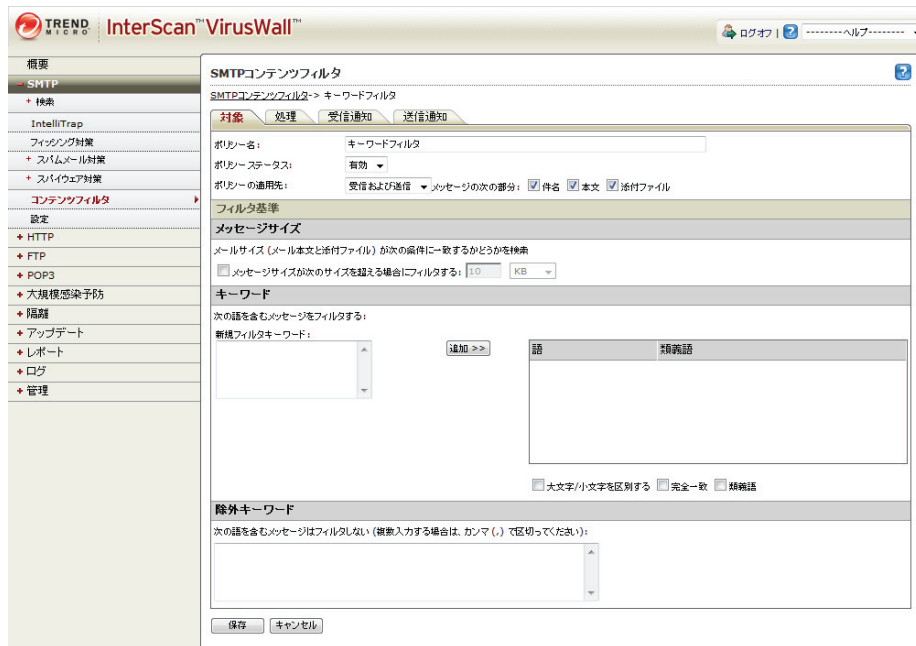
類義語の大文字 / 小文字および完全一致の属性は、キーワード自体に対して定義された属性と一致します。つまり、完全一致がオフのときに類義語リストで「red」が指定されている場合は、「Red」でも一致が発生します。同様に、大文字 / 小文字の区別がオフのときにメッセージテキスト内に「Red」がある場合は、「red」で一致が発生します。

カンマで区切られた単一行に複数のキーワードを追加すると、その行にあるすべてのキーワードがメールの同じ箇所で使用されている場合にのみポリシーがトリガされるようになります。たとえば、ユーザがキーワード「apple, pear」を追加し、apple がメッセージの件名で使用され、pear が本文で使用されている場合、ポリシーはトリガされません。

キーワードフィルタに基づいたポリシーを追加する

SMTP コンテンツフィルタのフィルタ基準としてキーワードを使用するポリシーを作成するには、図 4-20 の [SMTP コンテンツフィルタ] → [キーワードフィルタ] → [対象] タブを使用してポリシールールを指定します。

図 4-20. [SMTP コンテンツフィルタ] → [キーワードフィルタ] → [対象] タブ



キーワードフィルタに基づいたポリシーを追加するには

1. 左側のメニューで [SMTP] → [コンテンツフィルタ] の順に選択します。
2. [ポリシー] で、[キーワードフィルタの追加] を選択します。
3. [キーワードフィルタ] 画面が表示されたら、[対象] タブを選択します。
4. [ポリシー名] ボックスにポリシー名を入力します。
5. [ポリシーステータス] で、[有効] を選択してポリシーを適用するか、ポリシーを適用しない場合は [無効] を選択します。
6. [ポリシーの適用先] で、このポリシーを適用するメッセージの種類 ([受信]、[送信]、または [受信および送信]) とメッセージのセクション ([件名]、[本文]、または [添付ファイル]) を選択します。

7. このポリシーで、添付ファイルを含めて指定したサイズより大きいメッセージをブロックする場合は、[メッセージサイズが次のサイズを超える場合にフィルタする] を選択し、サイズ制限を指定します。
8. [キーワード] に、メッセージ内で検索するキーワードを入力し、[追加] をクリックします。各キーワードの類義語を指定するには、[類義語] 列の下リンクをクリックします（初期設定は[なし] です）。
必要に応じて、[大文字 / 小文字の区別]、[完全一致]、[類義語] のいずれかを有効にします。

注意： ポリシーのキーワードリスト作成の詳細については、102 ページの「キーワードに基づいた SMTP コンテンツフィルタポリシーを作成する」を参照してください。

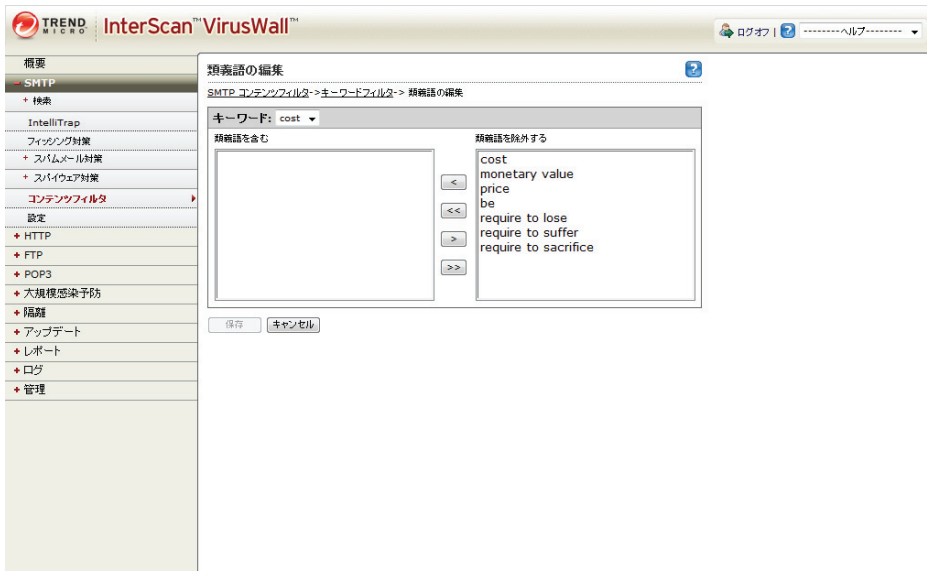
9. そのまま配信する必要があるメッセージがブロックされる可能性を減らすには、[除外キーワード] にそのまま配信するメッセージを識別するキーワードを入力します。
キーワードフィルタに一致する語がある場合でも、ここで入力したキーワードを含むメッセージはブロックされません。
10. [保存] をクリックします。

キーワードの類義語リストを変更する

InterScan VirusWall には、特定のキーワードの定義済みの類義語リストがあります。定義済みのリストの表示、およびキーワードの類義語としての単語の追加を実行するには、図 4-21 に示している [類義語の編集] 画面を使用します。

定義済みの類義語リストに対する変更または追加は実行できません。

図 4-21. [類義語の編集] 画面



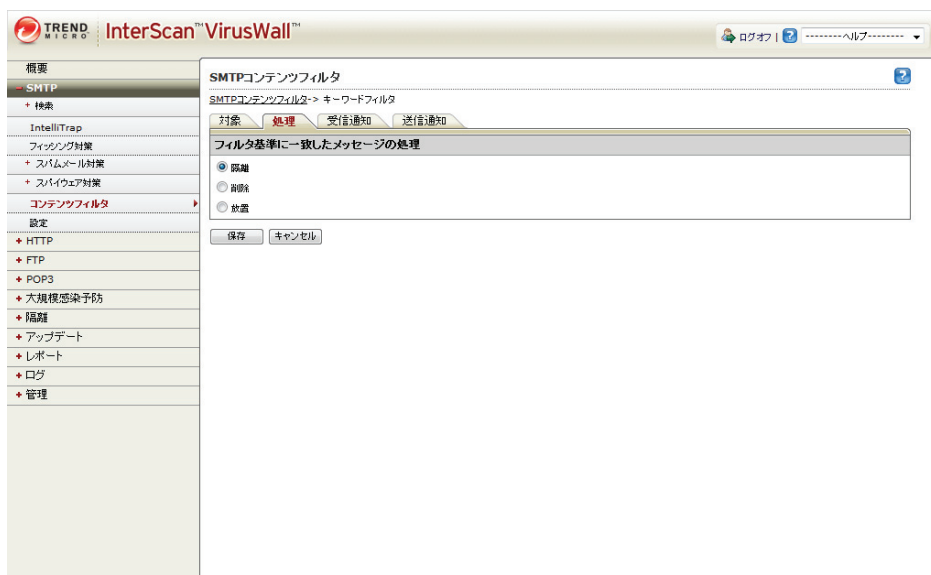
キーワードの類義語リストを変更するには

1. [SMTP コンテンツフィルタ] ([対象] タブ) 画面で、[キーワード] 領域の [類義語] 列に表示されている変更する類義語のハイパーリンクをクリックします。
2. プロンプトが表示されたら、[OK] をクリックして、[類義語の編集] 画面に進みます。
複数のキーワードをカンマで区切って入力した場合は、ドロップダウンリストにすべてのキーワードが表示されます。
3. 類義語を表示するキーワードを 1 つ選択します。
4. [類義語を除外する] 列の類義語のリストから、キーワードに使用する類義語を選択します。[<] をクリックして、選択した類義語を [類義語を含む] 列に移動します。
5. [保存] をクリックします。

キーワードフィルタポリシーに一致するメッセージに対する処理を設定する

指定したフィルタ基準に SMTP メッセージが一致した場合、そのメッセージに対して図 4-22 に示す 3 つの処理のうち 1 つを実行できます。

図 4-22. [SMTP コンテンツフィルタ] → [キーワードフィルタ] → [処理] タブ



コンテンツフィルタポリシーと一致するメッセージに対する処理を設定するには

1. 左側のメニューで [SMTP] → [コンテンツフィルタ] の順に選択します。
2. [ポリシー] で、[キーワードフィルタの追加] を選択します。
3. [キーワードフィルタ] 画面が表示されたら、[処理] タブを選択します。
4. [フィルタ基準に一致したメッセージの処理] で、次のオプションのうちの 1 つを選択します。
 - メッセージを隔離するには、[隔離] を選択します。
 - メッセージを削除するには、[削除] を選択します。メッセージは配信されません。
 - メッセージを配信するには、[放置] を選択します。ユーザはメッセージを受信します。
5. [保存] をクリックします。

メッセージがフィルタ条件に一致した場合の通知設定を指定する

受信 (図 4-23) または送信 (図 4-24) メールメッセージの添付ファイルで禁止コンテンツが検出されたことを知らせる通知を管理者と受信者に送信できます。

図 4-23. [SMTP コンテンツフィルタ] → [キーワードフィルタ] → [受信通知] タブ



図 4-24. [SMTP コンテンツフィルタ] → [キーワードフィルタ] → [送信通知] タブ



メッセージによってポリシーがトリガされた場合の通知設定を指定するには

1. 左側のメニューで [SMTP] → [コンテンツフィルタ] の順に選択します。
2. [ポリシー] で、[キーワードフィルタの追加] を選択します。
3. [キーワードフィルタ] 画面が表示されたら、必要に応じて [受信通知] または [送信通知] タブを選択します。

4. 通知の受信者を選択します。
5. 各受信者に送信するメッセージを作成します。メッセージ内に次の任意のタグを使用できます。

タグ	説明
%SENDER%	送信者アドレス
%RCPTS%	受信者アドレス
%SUBJECT%	メールの件名
%HEADERS%	メールヘッダ
%DATETIME%	検索日時
%MAILID%	メールメッセージ ID
%PROTOCOL%	メールプロトコル
%FILTERNAME%	常に「コンテンツフィルタ」
%DETECTED%	トリガされたポリシーの名前
%FINALACTION%	実行された処理
%QUARANTINE_AREA%	隔離場所
%MACHINENAME%	InterScan VirusWall コンピュータのホスト名

6. [保存] をクリックします。

コンテンツフィルタ用の SMTP 添付ファイルフィルタポリシーを作成する

SMTP コンテンツのフィルタ基準として添付ファイルまたはメッセージヘッダを使用するポリシーを作成するには、図 4-25 に示す [SMTP コンテンツフィルタ] → [添付ファイルフィルタ] → [対象] タブを使用してポリシールールを指定します。

図 4-25. [SMTP コンテンツフィルタ] → [添付ファイルフィルタ] → [対象] タブ

SMTPコンテンツフィルタ

SMTPコンテンツフィルタ -> 添付ファイルフィルタ

対象 処理 受信通知 送信通知

ポリシー名: 添付ファイルフィルタ

ポリシーステータス: 有効

ポリシーの適用先: 受信メッセージおよび送信メッセージ

フィルタ基準

添付ファイルサイズ

次の添付ファイルサイズに基づいてメッセージをフィルタする

☐ 添付ファイルサイズが次のサイズを超える場合にフィルタする: 10 KB

メッセージヘッダ

テキストボックスにメールアドレスまたはドメイン名を入力できます (例: abc@hotmail.comまたは@abc_company.com)。複数入力する場合は、カンマ(,)で区切ってください。

☒ メッセージヘッダが次の条件に一致する場合にルールを適用する

☐ メッセージヘッダが次の条件に一致する場合にルールを適用しない

Fromに次が含まれる: 大文字/小文字の区別 完全一致

Toに次が含まれる: 大文字/小文字の区別 完全一致

Ccに次が含まれる: 大文字/小文字の区別 完全一致

Reply-toに次が含まれる: 大文字/小文字の区別 完全一致

添付ファイルの指定

添付ファイル名、MIMEタイプ、および添付ファイルタイプに基づいて、メッセージをフィルタします。ファイル名のフィルタの定義に、ワイルドカードとしてアスタリスク(*)を使用できます。

☐ ファイル名

☐ MIME タイプ

☒ 添付ファイルタイプ

☐ オーディオ/ビデオファイル ☐ 画像

☐ 圧縮ファイル ☐ Java

☐ 実行可能ファイル ☐ Microsoft Office

保存 キャンセル

添付ファイルフィルタに基づいたポリシーを追加するには

1. 左側のメニューで [SMTP] → [コンテンツフィルタ] の順に選択します。
2. [ポリシー] で、[添付ファイルフィルタの追加] を選択します。
3. [添付ファイルフィルタ] 画面が表示されたら、[対象] タブを選択します。
4. [ポリシー名] ボックスにポリシー名を入力します。
5. [ポリシーステータス] で、[有効] を選択してポリシーを適用するか、ポリシーを適用しない場合は [無効] を選択します。

6. [ポリシーの適用先] で、このポリシーを適用するメッセージの種類を選択します ([受信メッセージ]、[送信メッセージ]、または [受信メッセージおよび送信メッセージ])。
 7. このポリシーで、添付ファイルが指定したサイズより大きいメッセージをブロックする場合は、[添付ファイルサイズが次のサイズを超える場合にフィルタする] を選択し、サイズ制限を指定します。
 8. [メッセージヘッダ] で、[From に次が含まれる]、[To に次が含まれる]、[Cc に次が含まれる]、[Reply-to に次が含まれる] など、メッセージヘッダ内の文字列が特定の条件に一致した場合にこのルールを適用するかどうかを指定できます。ヘッダ文字列に基づいてメッセージをブロックするかそのまま配信するかを選択します。

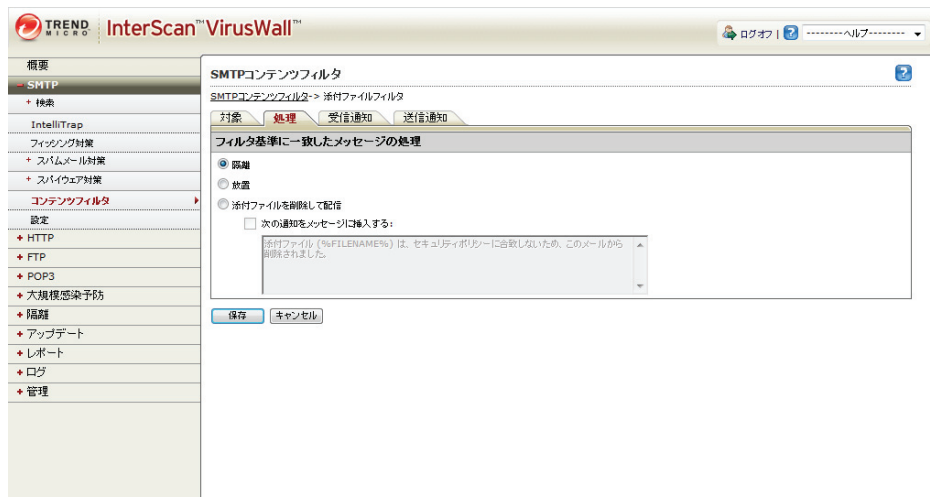
メッセージヘッダのテキストボックスに複数のエントリを指定するには、たとえば、「user1@isvw.com,user2@isvw.com」のように、各エントリをカンマで区切ります。

 - 指定したヘッダ文字列に一致するメッセージヘッダに [添付ファイルの指定] の設定を適用するには、[メッセージヘッダが次の条件に一致する場合にルールを適用する] を選択します。
 - 指定したヘッダ文字列に一致しないメッセージヘッダに [添付ファイルの指定] の設定を適用するには、[メッセージヘッダが次の条件に一致する場合にルールを適用しない] を選択します。
 9. ヘッダルールを指定します。
 10. [添付ファイルの指定] で、メッセージ添付ファイルのフィルタ条件を選択します。
 - **ファイル名**: ファイル名またはワイルドカード (*) を使用した文字列を指定します。ここで指定した名前または文字列に一致するファイル名を持つすべての添付ファイルがフィルタされます。
 - **MIME タイプ**: フィルタする MIME タイプを指定します。
 - **添付ファイルタイプ**: ブロックするファイルタイプのカテゴリを指定します。ここで指定したファイルタイプカテゴリに属するすべての添付ファイルがブロックされます。
-
- 注意:** [ファイル名] および [MIME タイプ] ボックスで複数のエントリを指定するには、各エントリをカンマで区切ります。たとえば、「*.jpg*.txt」や「text/plain,image/jpeg」のように指定します。
-
11. [保存] をクリックします。

SMTP コンテンツフィルタ添付ファイルポリシーの処理を設定する

指定したフィルタ基準に SMTP メッセージが一致した場合、そのメッセージに対して図 4-26 に示す 3 つの処理のうち 1 つを実行できます。

図 4-26. [SMTP コンテンツフィルタ] → [添付ファイルフィルタ] → [処理] タブ



添付ファイルのポリシーと一致するメッセージに対する処理を設定するには

1. 左側のメニューで [SMTP] → [コンテンツフィルタ] の順に選択します。
2. [ポリシー] で、[添付ファイルフィルタの追加] を選択します。
3. [添付ファイルフィルタ] 画面が表示されたら、[処理] タブを選択します。
4. [フィルタ基準に一致したメッセージの処理] で、次のオプションのうちの 1 つを選択します。
 - メッセージを隔離するには、[隔離] を選択します。
 - メッセージを配信するには、[放置] を選択します。ユーザはメッセージを受信します。
 - 添付ファイルを削除するには、[添付ファイルを削除して配信] を選択します。ユーザは添付ファイルのないメッセージを受信します。
5. メッセージの本文に通知を挿入するには、[次の通知をメッセージに挿入する] を選択します。挿入するメッセージのテキストは変更できます。また、次の任意のタグを使用できます。
 - %FILENAME%: 削除された添付ファイルの名前
 - %RULENAME%: ポリシーの名前
6. [保存] をクリックします。

メッセージの添付ファイルがフィルタ条件に一致した場合の通知設定を指定する

受信 (図 4-27) または送信 (図 4-28) メールメッセージの添付ファイルで禁止コンテンツが検出されたことを知らせる通知を管理者と受信者に送信できます。

図 4-27. [SMTP コンテンツフィルタ] → [添付ファイルフィルタ] → [受信通知] タブ



図 4-28. [SMTP コンテンツフィルタ] → [添付ファイルフィルタ] → [送信通知] タブ



メッセージによってポリシーがトリガされた場合の通知設定を指定するには

1. 左側のメニューで [SMTP] → [コンテンツフィルタ] の順に選択します。
2. [ポリシー] で、[添付ファイルフィルタの追加] を選択します。
3. [添付ファイルフィルタ] 画面が表示されたら、必要に応じて [受信通知] または [送信通知] タブを選択します。
4. 通知の受信者を選択します。
5. 各受信者に送信するメッセージを作成します。メッセージ内に次の任意のタグを使用できます。

タグ	説明
%SENDER%	送信者アドレス
%RCPTS%	受信者アドレス
%SUBJECT%	メールの件名
%HEADERS%	メールヘッダ
%DATETIME%	検索日時
%MAILID%	メールメッセージ ID
%PROTOCOL%	メールプロトコル
%FILTERNAME%	常に「コンテンツフィルタ」
%DETECTED%	トリガされたポリシーの名前
%FINALACTION%	実行された処理
%QUARANTINE_AREA%	隔離場所
%MACHINENAME%	InterScan VirusWall コンピュータのホスト名

6. [保存] をクリックします。

SMTP コンテンツフィルタポリシーをコピーまたは削除する

既存の SMTP コンテンツフィルタポリシーをコピーして変更するか、または不要になったポリシーを削除するには

1. 左側のメニューで [SMTP] → [コンテンツフィルタ] の順に選択します。
2. [ポリシー] で、ポリシーを選択して [コピー] または [削除] をクリックします。
3. ポップアップメッセージボックスで [OK] をクリックして変更を確定します。

SMTP 設定

SMTP トラフィックの検索を有効にする場合、送受信トラフィックの処理方法を設定する必要があります。図 4-29 に、指定する必要がある設定内容を示します。

図 4-29. SMTP 設定

TREND MICRO InterScan™ VirusWall™

ログオフ ヘルプ

概要

- SMTP
- 検索
- IntelliTrap
- フィッシング対策
- スパムメール対策
- スパイウェア対策
- コンテンツフィルタ
- 設定
 - HTTP
 - FTP
 - POP3
 - 大規模感染予防
 - 隔離
 - アップデート
 - レポート
 - ログ
 - 管理

SMTP設定

サーバ構成

メインサービスポート: 25

受信メール

☐ 次のSMTPサーバにメールを転送する: [] ポート 25

☒ メール配信にDNSを使用する

☒ 受信メッセージのIDをログに記録

送信メール

1. InterScanサーバに送信メールを送信するSMTPサーバ/クライアントのIPアドレスを指定します (複数のアドレスを指定する場合は、セミコロン (:) で区切ってください)。InterScanサーバが含まれる場合は、127.0.0.1とローカルホストのIPアドレスを含めます。

[]

☐ カスタマイズしたディスクレマータキスすべての送信メールに追加する

[]

2. 送信メールの配信方法を指定します。

☐ 次のSMTPサーバにメールを送信する: [] ポート 25

☒ メール配信にDNSを使用する

メールキュー

警告: メールキューを有効にすると、メールは配信されません。メールは、設定が無効になるまでQUEUEディレクトリに保管されます。詳細については、オンラインヘルプを参照してください。

☐ メールキューを有効にする

☐ 受信メール ☐ 送信メール

詳細設定

同時SMTPクライアント接続数の上限 (0は無制限): 25

受信メッセージの最大サイズ (0は無制限): 0 KB

送信メッセージの最大サイズ (0は無制限): 0 KB

DNS配信が使用されている場合は、最長で 24 時間、1 分ごとにメッセージ送信を試行する

☐ 処理済みメッセージにInterScanの「Received」ヘッダを挿入しない

☒ 次のドメイン宛での受信メールのみを許可して、リレーされたメッセージをブロックする

123.com

[]

ドメインはセミコロン (:) で区切って入力してください。

☒ 接続が確立されたときに次のSMTPクライアントメッセージを送信する

Welcome to ISVW SMTP service!

[]

保存 キャンセル

SMTP サービスを設定する

SMTP サービスを設定するには

1. 左側のメニューで [SMTP] → [設定] の順に選択します。
2. [サーバ構成] の [メインサービスポート] に、InterScan VirusWall が処理するメッセージの受信に使用する SMTP ポート番号を入力します。通常、SMTP ポートは 25 です。InterScan VirusWall では、このポートでメールを受信し、ウイルス検索を実行してからメッセージを転送します。

受信メッセージを設定する

受信メッセージを設定するには

1. [受信メール] で、受信メールの転送方法を選択します。
 - SMTP サーバと、その SMTP サーバが使用する特定のポートを指定するには、[次の SMTP サーバにメールを転送する] を選択します。
 - DNS サーバを使用して受信メールをネットワークメールサーバに転送できるようにするには、[メールの配信に DNS を使用する] を選択します。

注意： ここで指定する IP アドレスとポートは、InterScan VirusWall が SMTP サーバと同じコンピュータにインストールされているかどうかによって異なります。

2. 処理済みのメッセージを追跡するには、[受信メッセージの ID をログに記録] を選択します。

注意： 受信メッセージの ID は、デバッグログに記録されます。デバッグログを有効にするには

1. インストールフォルダに格納されている config.xml を変更します。
¥root¥Common¥Logging¥DebugEnabled の値を 1 に設定します。
 2. サービスを再起動します。
-

InterScan VirusWall と SMTP サーバが同じコンピュータ上にある場合

SMTP VirusWall では、受信 SMTP トラフィックをポート 25 で受信し、ウイルス検索を実行した後、25 以外のポートで元の SMTP サーバにルーティングします。この SMTP サーバで、トラフィックは通常どおりに受信および処理されます。

1. ポート 25 で SMTP トラフィックを受信しないように、元の SMTP サーバの設定を変更します。6000 以上などの空きポートに変更します。
2. [サーバ構成] 画面で、[次の SMTP サーバにメールを転送する] に「localhost」または「127.0.0.1」と入力します。
3. [ポート] で、元の SMTP サーバの新しいポート番号を指定します。

InterScan VirusWall と SMTP サーバが異なるコンピュータ上にある場合

InterScan VirusWall と SMTP サーバが異なるコンピュータ上にある場合は、InterScan VirusWall サーバが最初に受信メッセージを受信する必要があります。InterScan VirusWall が元の SMTP サーバに置き換わるように MX レコードを編集したり、2 つのサーバの IP アドレスを交換するなど、これを実現する方法はいくつかあります。

配信のために検索済みメッセージを元の SMTP サーバに転送するように InterScan VirusWall を設定する前に、方法を選択し、受信メッセージの宛て先を設定します。

送信メッセージを設定する

1. [InterScan サーバに送信メールを ...] フィールドに、処理のために送信メールを InterScan VirusWall に送信する各 SMTP サーバの IP アドレスを入力します。

複数の IP アドレスを入力する場合は、各 IP アドレスをセミコロンで区切ります。InterScan VirusWall では、次の形式がサポートされます。

- 192.168.5.*
- 192.168.5.1-158
- 192.168.5.242

1 つまたは複数の形式を組み合わせ、セミコロンで区切ることができます。たとえば、次のように入力します。192.168.3.*;192.168.5.2;192.168.5.148-245

送信メールを送信する SMTP サーバと同じコンピュータに InterScan VirusWall がインストールされている場合は、実際の IP アドレスと 127.0.0.1 の両方を入力します。

InterScan VirusWall では、これらの IP アドレスに基づいて受信メッセージと送信メッセージを区別し、受信メッセージはウイルス検索後に受信 SMTP サーバに、送信メッセージはウイルス検索後に送信 SMTP サーバにルーティングされます。通常、元の SMTP サーバの IP アドレスは、このフィールドに入力された IP アドレスのいずれかです。

[カスタマイズしたディスクレーマーテキストをすべての送信メールに追加する] を選択し、カスタマイズしたディスクレーマーテキストを表示されたテキストフィールドに入力します。

2. [送信メールの配信方法を指定します] で、次の条件に応じてオプションを選択します。
 - InterScan VirusWall が検索済みの送信メールの配信を扱う場合は、[メールの配信に DNS を使用する] を選択します。これは、SMTP VirusWall が SMTP サーバと同じコンピュータにインストールされているか別のコンピュータにインストールされているかにかかわらず、検索後に送信メールを処理する標準的な方法です。
 - InterScan VirusWall の代わりに別のメールゲートウェイまたはメールハブが検索済みメッセージの配信を扱う場合は、[次の SMTP サーバにメールを転送する] を選択し、そのメールゲートウェイまたはメールハブの IP アドレスとポートを入力します。

メールキューを使用する

このオプションでは、メッセージを受け入れてキューに保管し、後で検索を実行するよう InterScan VirusWall を設定できます。この機能は緊急時に使用できます。たとえば、ウイルス大規模感染が発生した場合、ウイルス大規模感染への対応方法が実施されるまでメッセージを保管できます。

メールキューを使用するには

1. 左側のメニューで [SMTP] → [設定] の順に選択します。
2. [メールキュー] で、[メールキューを有効にする] を選択してメールキューを起動し、キューに保管するメールを選択します (受信メール、送信メール、またはその両方)。

注意： メールをウイルス検索して転送するには、メールキューを無効にする必要があります。

詳細設定のオプション

次に、その他の設定オプションを示します。

- 「同時 SMTP クライアント接続数の上限：__」
- 「受信メッセージ / 送信メッセージの最大サイズ：__」
- 「DNS 配信が使用されている場合は、最長で __ 時間、__ 分ごとにメッセージ送信を試行する」
- 「処理済みメッセージに InterScan の「Received」ヘッダを挿入しない」

- ・ 「次のドメイン宛ての受信メールのみを許可して、リレーされたメッセージをブロックする :
__」
- ・ 「接続が確立されたときに次の SMTP グリーティングメッセージを送信する : __」

同時 SMTP クライアント接続数の上限 : __

InterScan VirusWall では、SMTP 同時接続の合計数を制限できます。

初期設定値は 25 です。このフィールドにゼロ (0) を入力すると、接続数は制限されません。パフォーマンスの問題が発生している場合は、SMTP クライアントの同時接続数を減らすことをお勧めします。

受信メッセージ/送信メッセージの最大サイズ : __

InterScan VirusWall では、一定のサイズを超える受信メッセージまたは送信メッセージを拒否できます。拒否は、リモート SMTP サーバと InterScan VirusWall の間の SMTP トランザクション中に発生します。リモート SMTP サーバは配信不能レポートを生成します。

DNS 配信が使用されている場合は、最長で __ 時間、__ 分ごとにメッセージ送信を試行する

InterScan VirusWall が DNS の使用時にメッセージ送信を試行する間隔を指定できます。InterScan VirusWall がメッセージを配信不能メッセージとして返送する前に、そのメッセージの送信を試行する期間を指定することもできます。

配信試行の回数とその結果は、InterScan VirusWall ログファイルに記録されます。

処理済みメッセージに InterScan の「Received」ヘッダを挿入しない

InterScan VirusWall では、メッセージを処理した後、SMTP サーバに転送する前にヘッダ情報が挿入されます。つまり、メッセージが「署名」されます。このヘッダ情報には、InterScan VirusWall がメールメッセージを受信した日時と、メールメッセージの送信元が含まれます。

- ・ このオプションを有効にすると、InterScan VirusWall によって処理が行われても、メールヘッダに情報が書き込まれません。
- ・ このオプションを無効にすると、処理中に追加のヘッダ情報が書き込まれ、InterScan VirusWall によって処理が行われたことが分かります。

InterScan VirusWall のメッセージヘッダの例を次に示します。

[Received:from 100.10.113.10 by us-washington.us-states
(InterScan VirusWall) ; Mon, 15 Jun 2009 11:49:34 -0800]

次のドメイン宛ての受信メールのみを許可して、リレーされたメッセージをブロックする：__

オープンリレーの不正利用からサーバを守るために、指定したドメインのみを宛て先とする受信メールを受け入れて、リレーメッセージをブロックします。このオプションを選択して、SMTP サーバにメッセージのリレーを許可するドメインを指定します。たとえば、会社名が Company1 で、ドメインが Company1.com である場合は、テキストフィールドに「Company1.com」と入力します。

次のヒントに留意してください。

- 複数のアドレスはセミコロンで区切ります（たとえば、*.isvw.com; isvwtest.com）。
- エントリは大文字 / 小文字が区別されません。
- 複数のサブドメインを指定する場合はワイルドカード (*) を使用します。

接続が確立されたときに次の SMTP グリーティングメッセージを送信する：__

初期設定では、SMTP サービスを使用する InterScan VirusWall に接続すると、次のグリーティングが返信されます。

```
->telnet [ コンピュータ名 ] 25
```

```
<-220 ISVW-EN2K3ET-A5 InterScan VirusWall ESMTP ready at [ 日時 ]
```

このオプションを無効にできます。また、このオプションを有効にした場合、オプションをカスタマイズできます。

SMTP トランザクションログを有効にする

InterScan VirusWall では現在、SMTP のトランザクションログがサポートされています。SMTP のトランザクションログは、初期設定で有効になっています。

SMTP トランザクションログを有効または無効にするには

1. Config.xml ファイルを開きます。
2. 「SMTP」の下にある「WriteConnectionMsg」という名前のキーを検索します。

3. 「WriteConnectionMsg」の値を「1」(有効) または「0」(無効) に設定します。
4. サービスを再起動します。



第5章

HTTP サービスの設定

Trend Micro InterScan VirusWall スタンダードエディション（以下、InterScan VirusWall）では、HTTP トラフィックを監視して、ネットワークゲートウェイのセキュリティを保持できます。HTTP トラフィックの検索は、インストールプロセス中に有効または無効にすることも、インストール後の任意の時点で InterScan VirusWall Web コンソールの [概要] 画面で有効または無効にすることもできます。

次の HTTP サービスを使用できます。

- アップロードおよびダウンロード時のウイルスとセキュリティリスクの検索
- フィッシングサイトの検出
- スパイウェアなどのグレーウェアの検出
- URL ブロック
- URL フィルタ
- Web レビューテーション
- HTTP サーバモードと待機ポートの設定

InterScan VirusWall の [概要] 画面の [Web (HTTP)] タブには、InterScan VirusWall の HTTP 検索によってアップロードファイルおよびダウンロードファイルで検出された、感染ファイル、スパイウェア、グレーウェア、およびフィッシングインシデントの数についての統計情報が表示されます。[概要] 画面には、ブロックおよびフィルタされた URL の数も表示されます。

HTTP サービスを有効または無効にする

HTTP プロトコルを介したファイルのダウンロードとアップロードに対する検索サービスを有効または無効にするには、図 5-1 の [概要] 画面の [Web (HTTP)] タブで、[HTTP トラフィックを有効にする] チェックボックスをオンまたはオフにします。

図 5-1. [概要] 画面の [Web (HTTP)] タブ



ウイルス / 不正プログラム検出、スパイウェア / グレーウェア検出、URL ブロック / フィッシング対策、および URL コンテンツフィルタの HTTP 検索統計情報が [HTTP 概要] テーブルに表示されます。

HTTP ウイルス検索を設定する

InterScan VirusWall は、HTTP トラフィックフローを検索して、アップロードおよびダウンロード時にウイルスなどのセキュリティリスクを検出します。HTTP 検索は高度な設定が可能です。たとえば、HTTP ゲートウェイでさまざまな検索方法を設定したり、InterScan VirusWall が圧縮ファイルやサイズの大きいファイルを検索する方法を設定して、パフォーマンス上の問題やブラウザのタイムアウトを回避できます。

管理者は、[HTTP] → [検索] の順に選択して、ウイルスや不正プログラムに対する HTTP 検索を設定できます。

HTTP ウイルス検索を有効にする

HTTP ウイルス検索を有効にするには

1. 左側のメニューで [HTTP] → [検索] の順に選択します。
2. [対象] タブを選択します。
3. [HTTP 検索を有効にする] チェックボックスをオンにします。
4. [保存] をクリックします。

検索するファイルタイプを指定する

InterScan VirusWall は、圧縮ボリューム内の個別ファイルを含めて、すべてのまたは指定したファイルタイプでウイルスをチェックできます。図 5-2 に、ファイルの検索時に指定できる設定内容を示します。

図 5-2. [HTTP] → [検索] → [対象] タブ

InterScan™ VirusWall™

ログオフ ヘルプ

HTTP検索

対象 処理 通知

☒ HTTP検索を有効にする

検索対象ファイル

☒ 検索可能なすべてのファイル

☐ トrendマイクロの推奨設定: 実際のファイルタイプによる識別

☐ 指定のファイル 拡張子

圧縮ファイルの処理

☒ すべての圧縮ファイルの検索

☐ 圧縮ファイルを検索しない

☐ 次の場合は圧縮ファイルを検索しない

解凍後のファイル数が次の数を超える場合: 0 (0の場合は無制限)

解凍後のファイルサイズが次の数を超える場合: 1 GB

圧縮レイヤが次の数を超える場合: 20 (2-20)

圧縮ファイルに対する解凍後のファイルサイズが次の割合を超える場合: 0 (0~100, 0の場合は無制限)

MIMEタイプの除外

次のMIMEタイプはウイルス検索しない:

複数の項目を指定する場合は、セミコロン (;) で区切って入力してください (例: text/plain; text/fancy)。

サイズの大きいファイルの処理

☒ 検索するファイルサイズの上限を設定する: 1 GB

☒ ファイルが次の数値より大きい場合は特異処理を有効にする: 512 KB

☒ 遅延検索

InterScan VirusWallサーバが 96 KB を受信するたび

未検索のデータのうち 65536 バイトをクライアントに配信する

☐ 配信後に検索 (感染の危険性が高くなります)

保存 キャンセル

検索するファイルタイプを選択するには

1. 左側のメニューで [HTTP] → [検索] の順に選択し、[対象] タブを選択します。
2. [検索対象ファイル] で、必要なオプションを選択します。
 - a. ファイルタイプにかかわらず、すべてのファイルを検索するには、[検索可能なすべてのファイル] を選択します。この設定が最も安全です。
 - b. 検索するファイルを実際のファイルタイプで識別できるようにするには、[トレンドマイクロの推奨設定: 実際のファイルタイプによる識別] を選択します。
このオプションでは、一部のファイルタイプをそのまま配信するため、すべてのファイルを検索する場合よりも安全度は低くなります。
 - c. 特定のファイルタイプのみを検索するには、[指定のファイル] を選択して、[拡張子] をクリックします。[その他の拡張子] テキストボックスに指定した拡張子を持つファイルのみが検索されます。

初期設定では、次のファイル名拡張子を持つファイルが検索されます。

"";ARJ;BAT;BIN;BOO;CAB;CHM;CLA;CLASS;COM;CSC;DLL;DOC;DOT;DRV;EML;EXE;GZ;HLP;HTA;HTM;HTML;HTT;INI;JAR;JPEG;JPG;JS;JSE;LNK;LZH;MDB;MPD;MPP;MPT;MSG;MSO;NWS;OCX;OFT;OVL;PDF;PHP;PIF;PL;POT;PPS;PPT;PRC;RAR;REG;RTF;SCR;SHS;SYS;TAR;VBE;VBS;VSD;VSS;VST;VXD;WML;WSF;XLA;XLS;XLT;XML;Z;ZIP;{*;

ヒント： 初期設定の検索リストを修正する場合は、[その他の拡張子] オプションを使用します。

3. [保存] をクリックします。

注意： 検索タイプと圧縮ファイル処理のオプションは、ウイルスおよびスパイウェアを含む全タイプのファイル検索に適用されます。

圧縮ファイルの処理

HTTP 検索時の圧縮ファイルの処理方法を指定するには

左側のメニューで [HTTP] → [検索] の順に選択し、[対象] タブを選択します。

- すべての圧縮ファイルを検索するには、[すべての圧縮ファイルの検索] を選択します。この設定が最も安全です。
- すべての圧縮ファイルの検索をスキップするには、[圧縮ファイルを検索しない] を選択します。InterScan VirusWall は、圧縮ファイルを検索しません。
- ユーザが指定した制限内で圧縮ファイルを検索するには、[次の場合は圧縮ファイルを検索しない] を選択してから、圧縮ファイルを検索しない条件を指定します。
 - ◆ **解凍後のファイル数が次の数を超える場合：** 圧縮ファイル内のファイルの最大数 (0 の場合は無制限)。圧縮ファイル内のファイルはいっさい検索されません。
 - ◆ **解凍後のファイルサイズが次を超える場合：** 解凍後の最大ファイルサイズ。制限内の個別ファイルのみが検索されます。
 - ◆ **圧縮レイヤが次の数を超える場合：** 圧縮階層の最大数。たとえば、ZIP ファイルに RAR ファイルが含まれ、さらに RAR ファイルに別の圧縮ファイルが含まれている場合は、3 層の圧縮になります。圧縮ファイル内のファイルはいっさい検索されません。
 - ◆ **圧縮ファイルに対する解凍後のファイルサイズが次の割合を超える場合：** 圧縮前後の最大サイズ比率。制限内の個別ファイルのみが検索されます。

注意： 検索タイプと圧縮ファイル処理のオプションは、ウイルス、スパイウェア / グレーウェアを含む全タイプのファイル検索に適用されます。

MIME タイプの除外

データスループット率を向上させるために、ウイルスに感染するリスクが低い MIME タイプのファイル検索を省略するように、InterScan VirusWall を設定できます。たとえば、「audio/aiff」と入力すると、afc ファイルは検索されません。

ただし、MIME タイプは簡単に偽造できるので、InterScan VirusWall は、実際のファイルタイプをチェックする機能を使用して、ファイルが指定された MIME タイプであることを確認します。検索を省略する MIME タイプであっても、小さいファイルは常に検索されます。

表 5-1 は、HTTP ウイルス検索ポリシーの [MIME タイプの除外] に入力して、対応する MIME コンテンツタイプを検索しないように指定できるファイルタイプを示しています。

表 5-1. MIME タイプへのファイルタイプのマッピング

ファイル タイプ	MIME コンテ ンツタイプ	ファイル タイプ	MIME コンテ ンツタイプ	ファイル タイプ	MIME コンテ ンツタイプ
afc	audio/aiff	av	video/avs-video	bin	application/x-binary
afc	audio/x-aiff	audiovideo	video/	binhex	application/binhex
ani	application/octetstream	base64	application/base64	binhex	application/binhex4
arc	application/octetstream	bin	application/mac-binary	binhex	application/macbinhex
arj	application/octetstream	bin	application/mac-binary	binhex	application/macbinhex40
asf	video/x-ms-asf	bin	application/octetstream	binhex	application/x-binhex40

表 5-1. MIME タイプへのファイルタイプのマッピング (続き)

ファイル タイプ	MIME コンテ ンツタイプ	ファイル タイプ	MIME コンテ ンツタイプ	ファイル タイプ	MIME コンテ ンツタイプ
bin	application/ x-macbinary	bmp	image/bmp	bmp	image/ x-windowsbm p
bw	image/x-sgi-b w	bzip2	application/x- bzi2	cgm	image/cgm
cmx	application/x- cmx	cmx	image/x-cmx	com	application/ octetstream
core	application/ octetstream	cpio	application/x- cpio	dcr	application/ x-director
doc	application/ wordperfect	dwg	application/ac ad	dwg	application/x- acad
dwg	drawing/x-dw g	dwg	image/vnd.dw g	dwg	image/x-dwg
eps	application/ postscript	eps	image/x-eps	exec	application/ octetstream
exec	application/ x-msdownload	exe	application/ octetstream	fh9	image/x-freeh and
fli	video/x-fli	fm	application/ vnd.framemak er	gif	image/gif
gzip	application/x- gzip	gzip	encoding/x-g	hpexe	application/ octetstream
iff	audio/x-aiff	java	text/x-javasou rce	java	application/ java-class
java	application/ x-javaapplet	java	application/ x-javavm	java	text/x-javasou rce

表 5-1. MIME タイプへのファイルタイプのマッピング (続き)

ファイル タイプ	MIME コンテ ンツタイプ	ファイル タイプ	MIME コンテ ンツタイプ	ファイル タイプ	MIME コンテ ンツタイプ
java	application/ java-class	java	application/ x-javaapplet	java	application/ x-javavm
jpeg	image/jpeg	jpeg	image/pjpeg	lha	application/x-l ha
lisp	application/x-l isp	maud	audio/x-ma	ud	midi audio/midi
mif	application/x-m if	mng	video/x-mng	mp3	audio/mpeg
mp3	audio/mpeg3	mp3	audio/x-mpeg- 3	mp3	video/mpeg
mp3	video/x-mpeg	mpeg	video/mpeg	mscab	application/ x-cainetwin32- x86
msdoc	application/ msword	msexl	application/ex cel	msexl	application/ x-msexcel
msexl	application/ x-excel	msexl	application/ vnd.ms-excel	msmdb	application/ x-msaccess
msppt	application/ mspowerpoint	msppt	application/ powerpoint	msppt	application/ vnd.mspowerp oint
msproj	application/ vnd.msproject	msproj	application/ x-msproject	msproj	application/ x-project
mswri	application/ mswrite	pcx	image/x-pcx	pdb	application/ x-pilot-pdb
pdf	application/pd f	pdf	application/x- pdf	pfb	application/x-f ont
pict	image/pict	pict	image/x-pict	picture	image

表 5-1. MIME タイプへのファイルタイプのマッピング (続き)

ファイル タイプ	MIME コンテ ンツタイプ	ファイル タイプ	MIME コンテ ンツタイプ	ファイル タイプ	MIME コンテ ンツタイプ
png	image/png	ppm	image/ x-portablepix map	ps	application/ postscript
psd	application/ octetstream	qtm	video/quickti me	ra	audio/ vnd.mrealaudi o
ra	audio/ xpnrealaudio	ra	audio/xrealau dio	rar	application/rar
ras	image/ x-cmuraster	ras	image/cmu-ra ster	risc	application/ octetstream
rmf	application/ vnd.m-realme dia、 g_audiovideo	rtf	application/rtf	rtf	application/x-r tf
rtf	text/rich text	scm	application/ vnd.lotusscree ncam	scm	application/ x-lotusscreenc am
scm	application/ x-screencam	scm	video/x-scm	sf	audio/x-sf
swf	application/ x-shockwave-fl ash	tar	application/x-t ar	tga	image/tga
tiff	image/tiff	tnef	application/m s-tnef	tnef	application/ vnd.mstnef

表 5-1. MIME タイプへのファイルタイプのマッピング (続き)

ファイル タイプ	MIME コンテ ンツタイプ	ファイル タイプ	MIME コンテ ンツタイプ	ファイル タイプ	MIME コンテ ンツタイプ
txt	text/plain	uuencod e	text/x-uuenco de	zip	application/zi p
voc	audio/voc	voc	audio/x-voc	wav	audio/wav
wbc	application/ x-webshots	wmf	application/ x-msmetafile	wmf	image/x-wmf

サイズの大きいファイルの処理

ウイルス検索の性質上、サイズの大きいファイルではダウンロード時間が長くなります。つまり、ファイル全体を InterScan VirusWall へ転送した後、ファイルを検索して、ファイル全体をクライアントへ転送する時間が必要になります。環境によっては、この時間を容認できないことがあります。ネットワーク速度やサーバ能力など、その他の要因も考慮する必要があります。ファイルサイズがそれほど大きくなく、サイズの大きいファイルの処理設定が起動されない場合は、通常ファイルとして検索されます。

サイズの大きいファイルをダウンロードすると、ファイルのダウンロードとウイルス検索に長時間を要し、ブラウザがタイムアウトする場合があります。「大きい」と見なされるファイルサイズは、InterScan VirusWall がインストールされているハードウェア、および特定の環境におけるファイルタイプの組み合わせなどの要因によって異なります。トレンドマイクロは、512KB (初期設定値) を超えるファイルはサイズの大きいファイルと見なして、2,097,151KB (約 2GB) を超えるファイルを検索対象から除外することをお勧めします。ただし、これらの値は、ネットワーク速度、サーバ能力、およびセキュリティ要件に応じて異なる場合があります。

サイズの大きいファイルの処理には、次の設定が適用されます。

- **検索するファイルサイズの上限を設定する** : 検索する最大ファイルサイズを設定します。ファイルのサイズがここで指定した値よりも大きい場合、そのファイルは検索対象から除外されます。初期設定は 1GB です。
- **ファイルが次の数値よりも大きい場合は特殊処理を有効にする** : ファイルが大型サイズと見なされ特別な処理を受ける場合の最小サイズを定義します。特別な処理には、次の 2 種類があります。
 - ◆ **遅延検索** : 検索中にページの一部を読み込みます。ウイルスが見つかった場合は接続を停止します。

- [InterScan VirusWall サーバが〜を受信するたび] は、InterScan VirusWall サーバへのファイルのダウンロードとして、要求しているクライアントにデータが配信される頻度を制御します。このデータが、要求しているブラウザがタイムアウトするのを防ぎます。
 - [未検索のデータのうち〜バイトをクライアントに送信する] は、要求しているクライアントに送信されるデータ量を制御します。たとえば、次の設定だと仮定します。
 - InterScan VirusWall が 512KB を受信するたび
 - 未検索のデータのうち 1024 バイトをクライアントに送信する
サイズの大きいファイルをダウンロードすると、InterScan VirusWall サーバに 512KB がダウンロードされるたびに、要求しているクライアントに 1024 バイトのデータが送信されます。
- ◆ **配信後に検索:** 最初にページを読み込んでから検索を実行します (感染のリスクが最も高くなります)。サイズの大きいファイルに対する特別な処理を有効にしない場合は、InterScan VirusWall はファイルを最初に検索してからページを読み込みます。

4. [保存] をクリックします。

ウイルス検出時に実行する処理を指定する

InterScan VirusWall が感染ファイルを検出した場合は、図 5-3 に示す 6 つの処理のいずれかを実行できます。

図 5-3. [HTTP] → [検索] → [処理] タブ



- ・ **駆除 + 隔離** : InterScan VirusWall は感染ファイルを駆除しようとします。駆除できない場合は、そのファイルを隔離ディレクトリに移動し、ユーザーに通知します。
- ・ **駆除 + ブロック** : InterScan VirusWall は感染ファイルを駆除しようとします。駆除できない場合は、そのファイルを削除し、ユーザーに通知します。
- ・ **駆除 + 放置** : InterScan VirusWall は感染ファイルを駆除しようとします。駆除できない場合は、感染ファイルをそのまま配信します。
- ・ **隔離** : InterScan VirusWall は、このファイルを隔離し、ユーザーに通知します。
- ・ **ブロック** : InterScan VirusWall は感染ファイルを削除します。
- ・ **そのまま配信 (推奨しません)** : InterScan VirusWall は感染ファイルをそのまま配信します。

感染ファイルの検出時に実行する処理を指定するには

1. 左側のメニューで [HTTP] → [検索] の順に選択し、[処理] タブを選択します。
2. [ウイルス感染ファイルに対する処理] で、必要なオプションを選択します。
 - ・ 感染ファイルを常に駆除して受信者に配信するには、[駆除] を選択します。次に、感染ファイルを駆除できない場合に実行する処理を選択します。
 - ・ **隔離** : 感染ファイルを削除して隔離します。
 - ・ **ブロック** : 感染ファイルを隔離せずに削除します。
 - ・ **そのまま配信 (推奨しません)** : 感染ファイルを配信します。

- ・ 感染ファイルを駆除せずに隔離ディレクトリに移動するには、[隔離] を選択します。受信者は感染ファイルを受信しません。
 - ・ 感染ファイルを削除するには、[ブロック] を選択します。受信者は感染ファイルを受信しません。
 - ・ 感染ファイルを受信者に配信するには、[そのまま配信 (推奨しません)] を選択します。
3. [保存] をクリックします。

注意： 初期設定の HTTP 検索用隔離フォルダは、インストールフォルダ下の %quarantine%http です。

ウイルス検索の通知メッセージを指定する

InterScan VirusWall は、ファイルを隔離またはブロックするときにユーザの Web ブラウザに通知メッセージを表示します。ユーザ通知のメッセージテキストを変更できます。

通知メッセージを設定するには

1. 左側のメニューで [HTTP] → [検索] の順に選択し、[通知] タブを選択します。
2. InterScan VirusWall から送信するメッセージを入力します。
3. [保存] をクリックします。

HTTP フィッシング対策を設定する

フィッシングとは、急増している詐欺の 1 つで、正規の Web サイトを模倣し、Web ユーザに個人情報を開示させることです。フィッシング攻撃は、既存の正規の組織を偽装したメールメッセージから始まります。メッセージには通常、リンクが記載されており、受信者にこのリンクをクリックさせるように仕向け、ブラウザを偽の Web サイトに誘導します。Web サイトでは個人情報をアップデートするよう求められます。疑いを持たないユーザは、パスワード、クレジットカード番号などを提供してしまいます。

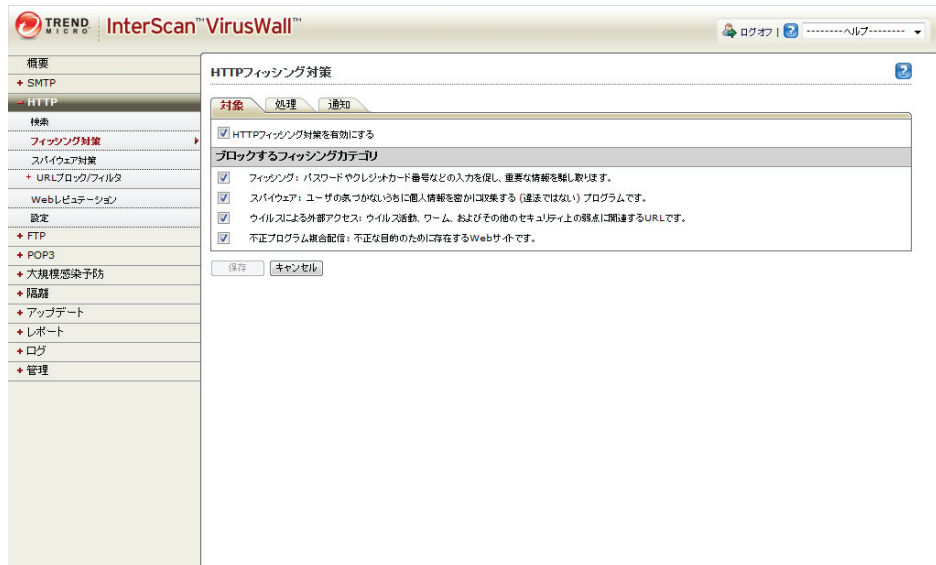
典型的なシナリオでは、疑いを持たないユーザが緊急を装う（本物のような）メールを受信します。そこには、ユーザのアカウントにすぐに解決しなければならない問題があり、解決しなければアカウントが閉じられると書かれています。そのメールには、本物に非常によく似た Web サイトの URL が含まれています。正規のメールと正規の Web サイトをコピーした後、バックエンドを変更するのは簡単です。収集したデータは実際にはこのバックエンドに送信されます。

HTTP フィッシング対策を有効にする

HTTP フィッシング対策機能を有効にするには

1. 図 5-4 に示すように、左側のメニューで [HTTP] → [フィッシング対策] の順に選択し、[対象] タブを選択します。

図 5-4. [HTTP] → [フィッシング対策] → [対象] タブ



2. [HTTP フィッシング対策を有効にする] チェックボックスをオンにします。
3. InterScan VirusWall が防御するフィッシングカテゴリのタイプを選択します。

注意： このスパイウェアオプションは、[HTTP] → [スパイウェア対策] → [処理] のスパイウェア検索オプションとは異なります。

4. [保存] をクリックします。

フィッシング検出時に実行する処理を指定する

検出したフィッシングサイトをブロックするか、アクセスを許可するかを指定できます。

フィッシングサイトに対する処理を指定するには

1. 左側のメニューで [HTTP] → [フィッシング対策] の順に選択し、[処理] タブを選択します。
2. フィッシングサイトに対する処理を選択します。
 - サイトへのアクセスをブロックするには、[ブロック] を選択します。
 - サイトへのユーザアクセスを許可するには、[許可 (推奨しません)] を選択します。
3. [保存] をクリックします。

フィッシングサイト検出時の通知メッセージを指定する

InterScan VirusWall は、フィッシングサイトの検出時にユーザの Web ブラウザに通知メッセージを表示します。ユーザ通知のメッセージテキストを変更できます。フィッシングサイトの疑いのあるサイトや既知のフィッシングサイトを TrendLabs に報告することもできます。

ユーザ通知を指定する

通知メッセージを設定するには

1. 左側のメニューで [HTTP] → [フィッシング対策] の順に選択し、[通知] タブを選択します。
2. InterScan VirusWall から送信するメッセージを入力します。
3. [保存] をクリックします。

フィッシングサイトの可能性のある URL を報告する

フィッシングサイトの疑いのあるサイトまたは既知のフィッシングサイトを TrendLabs に報告するには、[TrendLabs (トレンドラボ) への疑わしいフィッシング URL の送信] をクリックし、メールにそのサイトの URL を記載して、antifraud@support.trendmicro.com に送信してください。

TrendLabs では、詐欺目的のために情報を取得するサイトを監視し、InterScan VirusWall のユーザにトレンドマイクロから提供される自動アップデートの一部として既知のフィッシングサイトの情報を配布します。

HTTP スパイウェア対策を設定する

スパイウェア / グレーウェアにはさまざまな形があり、多くの場合正規のソフトウェアプログラムのように見えます。トレンドマイクロは、スパイウェア / グレーウェアを追跡調査して、パターンファイルの定期アップデートを提供しています。

一般的なグレーウェアの種類は次のとおりです。

グレーウェアの種類	一般的な動作
スパイウェア	アカウントのユーザ名やパスワードなどのデータを収集して第三者に転送します。
アドウェア	広告を表示して、ユーザのネットサーフィンの傾向などについてデータを収集し、Web ブラウザを介してユーザを広告のターゲットにします。
ダイヤラー	コンピュータのインターネット設定を変更し、事前設定された電話番号にコンピュータがモデム経由で電話するように強制します。
ジョークプログラム	CD-ROM トレイの開閉や多数のメッセージボックスの表示など、コンピュータの異常動作を引き起こします。
ハッキングツール	ハッカーがコンピュータに侵入するのを助けます。
リモートアクセスツール	ハッカーがコンピュータにリモートアクセスして制御するのを助けます。
パスワード解読アプリケーション	ハッカーがアカウントのユーザ名とパスワードを解読するのを助けます。
その他	ここに記載されていないその他の種類

HTTP スパイウェア検索を有効にする

HTTP スパイウェア検索を有効にするには

1. 左側のメニューで [HTTP] → [スパイウェア対策] の順に選択し、[対象] タブを選択します。
2. [HTTP スパイウェア対策を有効にする] チェックボックスをオンにします。
3. [保存] をクリックします。

図 5-5 に、[HTTP] → [スパイウェア対策] → [対象] タブを示します。ここでは、HTTP スパイウェア検索を有効にして、スパイウェア検索の除外対象を指定できます。

図 5-5. [HTTP] → [スパイウェア対策] → [対象] タブ



スパイウェア検索の除外リストを設定する

スパイウェア / グレーウェアの検索から除外する特定のファイル名またはファイル名拡張子をリストするには

1. 左側のメニューで [HTTP] → [スパイウェア対策] の順に選択し、[対象] タブを選択します。
2. [スパイウェア / グレーウェアの名前を入力] に、スパイウェア / グレーウェア検索の対象から除外するスパイウェア名を入力します。

スパイウェア名が不明な場合は、[スパイウェア / グレーウェア名の確認] リンクをクリックします。

3. [追加] をクリックします。
4. [保存] をクリックします。

注意： 除外リストのエントリを削除するには、ごみ箱アイコンをクリックします。[保存] をクリックして変更内容を確定します。

検索するスパイウェアおよびグレーウェアの種類を指定する

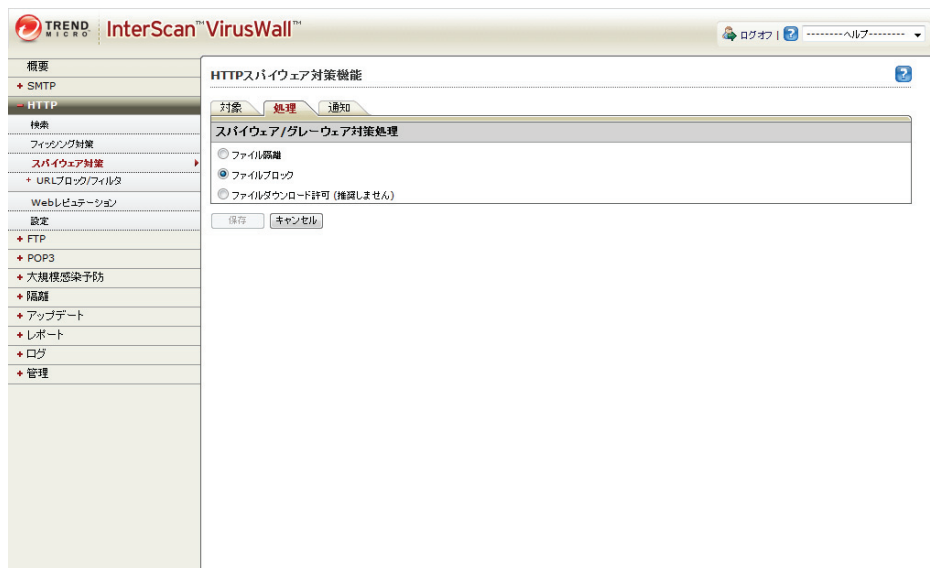
InterScan VirusWall の HTTP サービスで検索するスパイウェアおよびグレーウェアの種類を指定するには

1. 左側のメニューで [HTTP] → [スパイウェア対策] の順に選択し、[対象] タブを選択します。
2. [検索するスパイウェア / グレーウェア] で、HTTP サービスで検索するスパイウェアとグレーウェアの種類を指定します。
3. [保存] をクリックします。

スパイウェア検出時に実行する処理を指定する

スパイウェアなどのグレーウェアの検出時に InterScan VirusWall が実行する処理を、3 つの処理の中から 1 つ選択できます。

図 5-6. [HTTP] → [スパイウェア対策] → [処理] タブ



スパイウェア / グレーウェアの検出時に実行する処理を指定するには

1. 左側のメニューで [HTTP] → [スパイウェア対策] の順に選択し、[処理] タブを選択します。
2. [スパイウェア / グレーウェア対策処理] で、次のいずれかのオプションを選択します。

- スパイウェア / グレーウェアファイルを隔離ディレクトリに移動する場合は、[ファイル隔離] を選択します。ユーザはファイルを受信しません。
- スパイウェア / グレーウェアプログラムのファイル転送を回避する場合は、[ブロック] を選択します。ユーザはファイルを受信しません。
- スパイウェア / グレーウェアを対象の受信者に送信する場合は、[ダウンロード許可 (推奨しません)] を選択します。

3. [保存] をクリックします。

スパイウェア / グレーウェア検出時のユーザ通知メッセージを指定する

InterScan VirusWall は、ファイルを隔離またはブロックするときにユーザの Web ブラウザに通知メッセージを表示します。ユーザ通知のメッセージテキストを変更できます。

スパイウェア / グレーウェアの検出時に実行する処理を指定するには

1. 左側のメニューで [HTTP] → [スパイウェア対策] の順に選択し、[通知] タブを選択します。
2. InterScan VirusWall から送信するメッセージを入力します。
3. [保存] をクリックします。

HTTP URL ブロックおよび URL フィルタ

InterScan VirusWall は、ユーザが設定したブロックリストを使用して、望ましくないコンテンツを持つ Web サイトへのアクセスをブロックできます。また、このリストに除外を適用することもできます。

InterScan VirusWall にはポリシーフレームワークが用意されており、特定のグループまたは個々のユーザの ID に基づいてこれらのグループまたはユーザに URL フィルタおよび URL ブロックのポリシーを関連付けることができます (272 ページの「ユーザ識別方法を選択する」を参照)。この機能には、次の項目が含まれます。

- ID 設定
- Microsoft Active Directory サービスのサポート
- ポリシーアイテムの管理
- ユーザまたはグループ単位のログおよびレポート

InterScan VirusWall では、ユーザおよびグループに対して URL フィルタおよび URL ブロックのポリシーが最大 20 までサポートされます。ドメインコントローラエージェントソフトウェアをドメインコントローラサーバまたはイントラネット上の Windows コンピュータに配置できます。ドメインコントローラエージェントは、安全な TCP ポートであるポート 65015 経由で InterScan VirusWall と通信し、Microsoft Active Directory と連動します。

注意： 1 つのユーザまたはグループに対して複数のポリシーが存在する場合、トラフィックが優先順位のより高いポリシーに一致すると、このポリシーに基づいて処理が実行され、他のポリシーは無視されます。

URL ブロックおよび URL フィルタのグローバルポリシーを管理する

InterScan VirusWall は、初期設定の URL ブロックおよび URL フィルタポリシー（グローバルポリシー）で事前設定されます。このポリシーは、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。ポリシーでは、待機ポート 8080 が使用されます。

グローバルポリシーには、インターネットセキュリティグループに対して選択された、次に示す 12 の初期設定のカテゴリがあります。

- プロキシ回避システム
- スパイウェア
- フィッシング
- アドウェア
- 不正プログラム流布
- 不正サイト
- cookie
- ダイヤラー
- ハッキング
- ジョークプログラム
- パスワード解読
- リモートアクセスプログラム

グローバルポリシーを変更するには、151 ページの「既存の URL ブロックおよび URL フィルタのポリシーを変更する」を参照してください。

URL ブロックおよび URL フィルタのポリシーの優先順位を管理する

ポリシーの優先順位を変更するには

1. [HTTP] → [URL ブロック / フィルタ] → [ポリシー] の順に選択します。
2. [優先順位] 列で、ポリシーの優先順位を下げるには下向き矢印をクリックし、優先順位を上げるには上向き矢印をクリックします。

ポリシーがリストの上にあるほど、その優先順位は高くなります。

新しい URL ブロックおよび URL フィルタのポリシーを作成する

新しい URL ブロックおよび URL フィルタのポリシーは、次の 4 つの手順で作成します。

- ポリシー情報の指定
- 対象クライアントの指定
- URL ブロックルールの指定
- URL フィルタルールの指定

新しい URL ブロックおよび URL フィルタのポリシーを作成するには

手順 1. ポリシー情報を指定します。

1. [HTTP] → [URL ブロック / フィルタ] → [ポリシー] の順に選択します。
2. [HTTP URL ブロック / フィルタポリシー] 画面で [新規ポリシー] をクリックします。

[HTTP URL ブロック / フィルタポリシー] 画面に、最初の手順が表示されます (図 5-7 を参照)。

図 5-7. [HTTP URL ブロック / フィルタポリシー] 画面 (手順 1: ポリシー情報の指定)



3. [テンプレート] で、既存のポリシーに基づいて新しいポリシーを作成するかどうかを指定します。
4. [ポリシー情報] で、新しいポリシーの名前を指定して、ポリシーの作成完了時にそのポリシーを有効にするかどうかを指定します。
5. [次へ] をクリックします。

[HTTP URL ブロック / フィルタポリシー] 画面に、2 つ目の手順が表示されます (図 5-8 を参照)。

図 5-8. [HTTP URL ブロック / フィルタポリシー] 画面 (手順 2: 対象クライアントの指定)



手順 2. URL ブロックおよび URL フィルタのポリシーの対象クライアントを指定します。

6. URL ブロックおよび URL フィルタのポリシーの対象クライアントを指定します。

URL フィルタおよび URL ブロックのポリシーに対して個々のユーザおよびグループを識別するには、272 ページの「ユーザ識別方法を選択する」を参照してください。

注意： [ユーザ / グループを検索するキーワードの入力] フィールドを使用して、ユーザまたはグループを検索できます。InterScan VirusWall では、検索範囲を広げるために、入力したテキストの末尾に非表示のアスタリスク (*) が自動的に追加されます。一致するものが見つからなかった場合、[ユーザ / グループ] ボックスに、「レコードが見つかりません」と表示されます。

IP アドレスで対象クライアントを指定するには

- [IP/IP の範囲] の [IP/IP の範囲の入力] に、IP アドレスまたは IP アドレス範囲を入力します。

- [追加] をクリックすると、[IP/IP の範囲] テーブルに、入力した IP アドレスまたは IP アドレス範囲が表示されます。

IP アドレスまたは IP アドレス範囲を削除するには、目的の IP アドレスまたは IP アドレス範囲と同じ行にあるゴミ箱アイコンをクリックします。

ユーザまたはグループ名で対象クライアントを指定するには

- [Windows ユーザ / グループ] の検索フィールドに目的のクライアントの名前を入力し、[検索] をクリックして目的のクライアントを見つけます。リストに、指定した対象クライアントが表示されます。
- [追加] をクリックすると、[ユーザ / グループ] テーブルに対象クライアントが表示されます。

ユーザまたはグループ名を削除するには、目的のユーザまたはグループ名と同じ行にあるゴミ箱アイコンをクリックします。

7. 対象クライアントの情報を指定したら、[次へ] をクリックします。

[HTTP URL ブロック / フィルタポリシー] 画面に、3 つ目の手順が表示されます (図 5-9 を参照)。

図 5-9. [HTTP URL ブロック / フィルタポリシー] 画面 (手順 3: URL ブロックルールの指定)



手順 3. ブロックする URL を指定します。

8. ブロックする URL を指定するには、[URL ブロック] の [照合の種類] ドロップダウンリストから照合の種類を選択して、[ブロックする URL] スクロールボックスに適切な情報を入力します。

照合の種類には次の項目が含まれます。

- **Web サイト** — ブロックする Web サイトの URL
- **URL キーワード** — ブロックする複数の Web サイトの URL で使用されている語
- **文字列** — 完全一致の URL 文字列

9. [追加] をクリックします。

[ブロックする URL] テーブルに URL が表示されます。テーブルの下には、URL の種類の説明が表示されます。

10. URL 除外を指定するには、[URL ブロック除外リスト] に必要な情報を入力します。

この手順は、ブロックする URL の指定と似ています (詳細については、ステップ 8 とステップ 9 を参照してください)。

11. [次へ] をクリックします。

[HTTP URL ブロック / フィルタポリシー] 画面に、4 つ目の手順が表示されます (図 5-10 を参照)。

図 5-10. [HTTP URL ブロック / フィルタポリシー] 画面 (手順 4: URL フィルタルールの指定)

手順 4. アクセスを制限する URL カテゴリを選択します。

12. [URL フィルタルール] で、アクセスを制限する URL カテゴリを選択します。

- 業務時間中にブロックするカテゴリのチェックボックスをオンにします。グループ内のすべてのカテゴリを選択するためにグループを展開する必要はありません。
- 業務時間外にブロックするカテゴリのチェックボックスをオンにします。グループ内のすべてのカテゴリを選択するためにグループを展開する必要はありません。未指定の期間は、「業務時間外」と見なされます。

日時の制限を指定するには、152 ページの「URL フィルタのスケジュールを設定する」を参照してください。

13. URL カテゴリの例外を指定するには、[URL 除外リスト] に必要な情報を入力します。

この手順は、ブロックする URL の指定と似ています (詳細については、149 ページのステップ 8 と 149 ページのステップ 9 を参照してください)。

14. [完了] をクリックします。

[HTTP URL ブロック / フィルタポリシー] 画面の [ユーザグループポリシー] 表示に戻ります。ここに新しいポリシーが表示されています。作成したポリシーは、後から変更を加えることができます (151 ページの「既存の URL ブロックおよび URL フィルタのポリシーを変更する」を参照)。

URL フィルタおよび URL ブロックをグローバルレベルで有効にするには、検索スケジュールを設定して通知メッセージを指定します (152 ページの「URL ブロックおよび URL フィルタの設定」を参照)。

既存の URL ブロックおよび URL フィルタのポリシーを変更する

このセクションの手順を使用して、グローバルポリシーや作成したポリシーを変更できます。

URL ブロックおよび URL フィルタのポリシーを変更するには

1. [HTTP] → [URL ブロック / フィルタ] → [ポリシー] の順に選択します。
[HTTP URL ブロック / フィルタポリシー] 画面が表示されます。
2. [ユーザグループポリシー] テーブルで目的のポリシーをクリックします。
[HTTP URL ブロック / フィルタポリシー] 画面が、[対象クライアント] タブをアクティブにした状態で表示されます。
3. ポリシーの名前を変更するには、目的の名前を [ポリシー名] に入力します。
この名前変更は、[HTTP URL ブロック / フィルタポリシー] 画面のいずれのタブがアクティブになっていても実行できます。
4. ポリシーを無効にするには、[このポリシーを有効にする] チェックボックスをオフにします。
この変更は、[HTTP URL ブロック / フィルタポリシー] 画面のいずれのタブがアクティブになっていても実行できます。

注意： 作成した URL ブロックおよび URL フィルタのポリシーを使用するには、[HTTP URL ブロック / フィルタ設定] 画面でグローバルレベルで URL ブロックおよび URL フィルタを有効にする必要があります (152 ページの「URL ブロックおよび URL フィルタを有効にする」を参照)。

5. 対象クライアントを追加または削除するには、[HTTP URL ブロック / フィルタポリシー] 画面の [対象クライアント] タブで適切な変更を加えてから、[保存] をクリックします。
詳細については、ステップ 2 を参照してください。
6. URL ブロックルールを追加または削除するには
 - [URL ブロックルール] タブをクリックして、[HTTP URL ブロック / フィルタポリシー] 画面 ([URL ブロックルール] タブ) で適切な変更を加えます。
 - 変更を加えたら、[保存] をクリックします。詳細については、ステップ 3 を参照してください。
7. URL フィルタルールを追加または削除するには
 - [URL フィルタルール] タブをクリックして、[HTTP URL ブロック / フィルタポリシー] 画面 ([URL フィルタルール] タブ) で適切な変更を加えます。
 - 変更を加えたら、[保存] をクリックします。詳細については、ステップ 4 を参照してください。

URL ブロックおよび URL フィルタの設定

URL ブロックおよび URL フィルタを有効にする

作成した URL ブロックおよび URL フィルタのポリシーを使用するには、[HTTP URL ブロック / フィルタ設定] 画面でグローバルレベルで URL ブロックおよび URL フィルタを有効にする必要があります。InterScan VirusWall では、URL ブロックと URL フィルタのいずれかまたは両方を有効にできます。

URL ブロックおよび URL フィルタを有効にするには

1. [HTTP] → [URL ブロック / フィルタ] → [設定] の順に選択します。
2. [HTTP URL ブロック / フィルタ設定] 画面の [検索状況] で、目的の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。

URL フィルタのスケジュールを設定する

URL フィルタのスケジュールを設定するには

1. [HTTP] → [URL ブロック / フィルタ] → [設定] の順に選択します。
[HTTP URL ブロック / フィルタ設定] 画面が表示されます。

2. [URL フィルタ起動時間] で、就業日および業務時間を選択します。
3. [保存] をクリックします。

ブロックされた URL についてのメッセージを指定する

ブロックされた URL についてのメッセージを指定するには

1. [HTTP] → [URL ブロック / フィルタ] → [設定] の順に選択します。
[HTTP URL ブロック / フィルタ設定] 画面が表示されます。
2. [ユーザへの通知] で、URL のブロックの発生時に表示するメッセージをテキストボックスに入力します。
3. [保存] をクリックします。

URL の見直し

URL を見直すには

1. [HTTP] → [URL ブロック / フィルタ] → [設定] の順に選択します。
[HTTP URL ブロック / フィルタ設定] 画面が表示されます。
2. [URL カテゴリ見直し依頼] で、[TrendLabs (トレンドラボ) への URL カテゴリ見直し依頼] をクリックします。
[Trend Micro Online URL Query - Feedback System] 画面が開きます。

図 5-11. [Trend Micro Online URL Query - Feedback System] 画面

TREND MICRO Online URL Query - Feedback System

Trend Micro Online URL Query - Feedback System

Type a URL in the field below to:

- Check which category it belongs to or
- Submit feedback about the current category it belongs to

Complete URL*:

Only HTTP and HTTPS are supported. (e.g., http://www.trendmicro.com)

Copyright 1989-2009 Trend Micro, Inc. All rights reserved. [Legal Notice](#) | [Privacy Policy](#) | [Contact Us](#)

3. [Complete URL] フィールドに、問題になっている URL を入力します。
[Check category] をクリックすると、問題になっている URL の現在のカテゴリを確認できます。
4. [Submit feedback] をクリックします。
[URL Feedback Submission Form] 画面が開きます。

図 5-12. [URL Feedback Submission Form] 画面

TREND MICRO URL Feedback

URL Feedback Submission Form

URL : **www.yahoo.com**

Suggested Category *: Search Engines / Portals

Additional comments :

If you are a Home / Home Office user, please enter your serial number here *:

If you are using products other than Trend Micro Internet Security or Trend Anti Virus please enter your Activation Code *:

Your email address (optional) :

Please provide your email address so we can contact you for follow up inquiries regarding your submission.
Note: Trend Micro highly values privacy and will never share your email address with other companies.
Fields marked with an asterisk * are required.

Enter the characters shown in the picture:

0380

Copyright 1989-2009 Trend Micro, Inc. All rights reserved. [Legal Notice](#) | [Privacy Policy](#) | [Contact Us](#)

5. [Select...] をクリックして、別の URL カテゴリを選択します。
6. [Additional Comments] テキストフィールドにコメントを入力します。
7. [Enter the characters shown in the picture] フィールドに、図に表示されている文字を入力します。
8. [Submit] をクリックします。
[URL Feedback] 画面が開きます。この画面には、さらにサポートが必要な場合のために、トレンドマイクロのその他の Web サイトへのリンクが用意されています。
9. [Return Home] をクリックします。
10. [Trend Micro Online URL Query - Feedback System] 画面を終了して、[HTTP URL ブロック / フィルタ設定] 画面に戻ります。

URL ブロックおよび URL フィルタのポリシーを削除する

URL ブロックおよびフィルタのポリシーを削除するには

1. [HTTP] → [URL ブロック / フィルタ] → [ポリシー] の順に選択します。
[HTTP URL ブロック / フィルタポリシー] 画面が表示されます。
2. [ユーザグループポリシー] テーブルで、目的のポリシーのチェックボックスをオンにして、[削除] をクリックします。
3. [保存] をクリックします。
削除を取り消すには [キャンセル] をクリックします。

Web レピュテーション

Web レピュテーションでは、新たな Web からの脅威に対してエンドユーザが保護されます。Web レピュテーションのクエリでは、URL カテゴリに関する情報 (URL フィルタで使用) が返されるため、InterScan VirusWall ではローカルに保存された URL データベースは使用されません。

また、Web レピュテーションでは、評価スコアが URL に割り当てられます。アクセスされた URL ごとに、Web レピュテーションで評価スコアがクエリされ、このスコアがユーザ指定の検出レベルより上か下かに基づいて、必要な処理が実行されます。

InterScan VirusWall には、感染した URL に関するフィードバックをデバイスから自動的に送信できる機能があり、これは Web レピュテーションデータベースの向上に役立ちます。有効になっている場合、このフィードバックには製品名とバージョン、URL、およびウイルス名が含まれます (IP アドレス情報は含まれないため、すべてのフィードバックは匿名で、企業情報が保護されます)。Web レピュテーションの結果は、Web レピュテーションログ ([ログ] → [クエリ] → [HTTP] → [Web レピュテーション]) および [概要] → [Web (HTTP)] タブで確認できます。

トレンドマイクロの Web レピュテーションテクノロジー (Smart Protection Network の一部) を使用すると、さまざまな保護レベル (低、中、高) で Web サイトの検索を実行したり、Web サイトを除外リストに追加することによって (yourcompany.com など) Web サイトを検索やブロックなしに表示できるようにしたりできます。

注意： Web サイトの事前許可は慎重に行う必要があります。Web サイトの検索やブロックを実行しないと、セキュリティリスクをもたらす可能性があります。

Web レピュテーションを使用したフィッシング対策

InterScan VirusWall には、次の機能を使用した HTTP フィッシング対策が用意されています。

- **フィッシング対策** — InterScan VirusWall で使用される第一のフィッシング対策テクノロジーです。[HTTP] → [フィッシング対策] 画面から、フィッシング対策の動作を指定します。フィッシング対策は InterScan VirusWall と連携して機能し、クライアントの送信 URL リクエストを監視して、既知のフィッシングサイトのリストと比較します。リストに一致するサイトがある場合、フィッシング対策では、そのサイトへのアクセスをブロックします。フィッシング対策によりサイトがブロックされた場合、ユーザは通知メッセージを受け取ります。
- **URL フィルタのフィッシング対策カテゴリ** — InterScan VirusWall で使用される第二のフィッシング対策テクノロジーです。InterScan VirusWall は、ユーザが設定したブロックリストを使用して、望ましくないコンテンツを持つ Web サイトへのアクセスをブロックできます。すべてのカテゴリについて、すべての URL ブロックと URL フィルタに使用される通知メッセージは 1 つしかないため、URL フィルタを使用したフィッシング対策の検出に関する通知メッセージを、フィッシング対策に特化することはできません（ただし、URL ブロックが無効化され、URL フィルタのフィッシング対策カテゴリのみが有効化されている場合を除く）。
- **Web レピュテーション** — InterScan VirusWall で使用される第三のフィッシング対策テクノロジーです。アクセスされた URL ごとに、Web レピュテーションで評価スコアがクエリされ、このスコアがユーザ指定の検出レベルより上か下かに基づいて、必要な処理が実行されます。Web レピュテーションによりブロックされるサイトが、必ずしもフィッシング対策カテゴリに分類されるとは限りません。Web レピュテーションによってブロックされたフィッシングサイト（およびその他のサイト）には、「低評価」メッセージが表示されます。

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、リモートサーバに配置されています。ユーザが特定の URL にアクセスしようとする、InterScan VirusWall はその URL に関する情報を 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リモートサーバに配置し、このデータベース情報のローカルキャッシュを構築することで、InterScan VirusWall のオーバーヘッドを削減し、パフォーマンスを向上できます。

Web レピュテーションデータベースは、Web ページの最新のセキュリティ情報によって更新されます。URL の評価が間違っていると考える場合や、特定の URL の評価を確認したい場合は、次のリンクを使用してトレンドマイクロに連絡してください。

<http://reclassify.wrs.trendmicro.com/submit-files/wrsonlinequery.asp>

また、[HTTP] → [Web レピュテーション] → [通知] → [TrendLabs（トレンドラボ）への URL カテゴリ見直し依頼] をクリックしてアクセスすることもできます。

Web レピュテーション設定

セキュリティ検出レベルを設定すると、不正な Web サイトに誤って導かれないようにユーザが保護され、管理者は保護レベルを設定できるようになります。

Web レピュテーションでは、次を設定します。

- Web レピュテーションの有効化または無効化
- 会社に適したセキュリティ検出レベルの選択
- (オプション) 感染 URL に関するフィードバックを匿名でトレンドマイクロへ送信するかどうか

セキュリティ検出レベル

InterScan VirusWall は、Web レピュテーションのスコアを受信すると、そのスコアが指定されているしきい値より下か上かを判断します。検出レベルのしきい値はユーザが定義します。中が初期設定の検出レベルです。トレンドマイクロではこの設定をお勧めします。誤検出が多くなりすぎないようにほとんどの Web からの脅威がブロックされるためです。

セキュリティ検出レベルを設定するには

1. [HTTP] → [Web レピュテーション] → [対象] タブの順に選択します。
2. [HTTP リアルタイム Web レピュテーションの検索を有効にする] チェックボックスをオンにします。

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 ブロックの検出レベル (高、中、または低) を指定します。
4. [保存] をクリックします。

Web レピュテーションの除外

Web レピュテーションの除外リストに Web サイトを追加すると、InterScan VirusWall によるその Web サイトに対する不正コードの検索を省略できます。Web レピュテーションの検索除外は、Web サイトの完全な URL または IP アドレス、URL キーワード、または文字列を入力するか、既存の URL 除外リストをインポートすることによって定義できます。

警告： 検索を実行しないと、除外リスト内の Web サイトがハッキングされたり、Web サイトに不正コードが注入された場合に、セキュリティの弱点となるおそれがあります。

Web レピュテーションの除外を指定するには

1. [HTTP] → [Web レピュテーション] → [対象] タブ → [URL 除外リスト] の順に選択します。
2. [除外する URL] ボックスに、URL テキストを入力します。
3. [照合の種類] ドロップダウンリストで、URL テキストを表すオプションを選択します。
4. [追加] をクリックして、[URL 除外リスト] に URL を追加します。
5. [保存] をクリックします。

Web レピュテーションの除外として URL を指定した後に、除外リストでその URL を選択し、[削除] をクリックしてリストから削除することによって、Web レピュテーション検索にその URL を追加することができます。

HTTP 設定

HTTP トラフィックの監視を開始する前に、HTTP サーバの設定を指定しておく必要があります。InterScan VirusWall は、次のいずれかのモードで、HTTP に含まれるセキュリティリスクからユーザおよびネットワークリソースを保護できます。

- スタンドアロンモードのフォワードプロキシ
- 依存プロキシモードのセカンダリプロキシ
- リバースプロキシモードのリバースプロキシ
- L4 スイッチがインストールされている場合に透過プロキシ

InterScan VirusWall は、すべての設定でクライアントと Web サーバの間に配置されます。

スタンドアロンモード

スタンドアロンモードの設定では、不正な HTTP に含まれているセキュリティリスクをクライアントがサーバから受信しないように防御します。これは最も一般的な設定であり、通常の使用例では、インターネットの不正なダウンロードファイルを受信しないよう、ネットワーク上の Web ユーザを保護します。図 5-13 に示すスタンドアロンのプロキシトポロジでは、通常、InterScan VirusWall は保護するクライアントと同じ LAN 内にインストールされます。

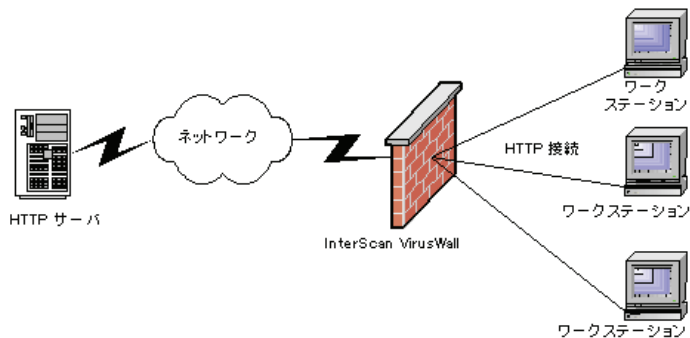


図 5-13. スタンドアロンモードのトポロジ

依存プロキシモード

依存プロキシモードはスタンドアロンモードに似ていますが、InterScan VirusWall は図 5-14 に示すように上位プロキシに依存しながら HTTP サーバにアクセスします。

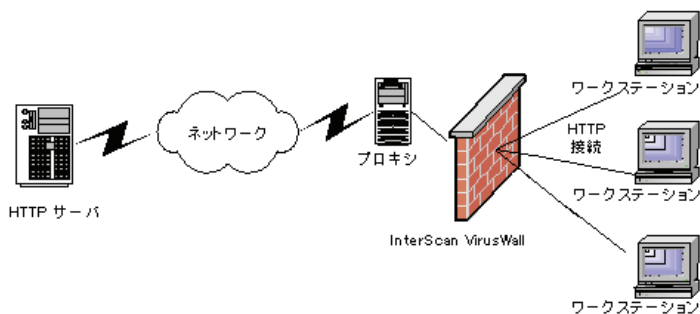


図 5-14. 依存プロキシモードのトポロジ

リバースプロキシモード

リバースプロキシモードの設定では、InterScan VirusWall は Web サーバと Web サーバのクライアントとの間に配置されます。この設定はあまり一般的ではありませんが、通常は、Web サーバに不正なコンテンツがアップロードされるのを回避するために使用されます。リバースプロキシモードのトポロジでは通常、InterScan VirusWall は InterScan VirusWall が保護する Web サーバの近くにインストールされ、インターネットによってクライアントから分離されます。

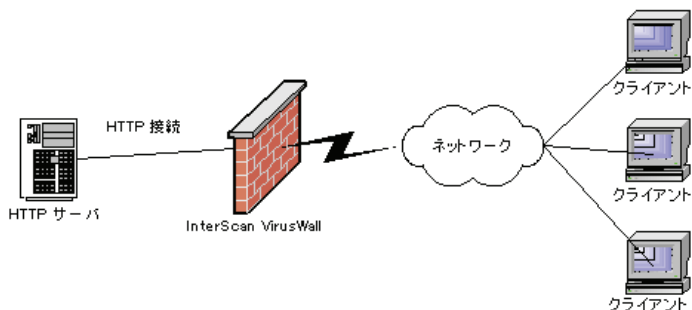


図 5-15. リバースプロキシモードのトポロジ

透過モード

InterScan VirusWall では、レイヤ 4 スイッチを使用する場合に、HTTP プロキシの透過モードがサポートされます。InterScan VirusWall がユーザに対して透過的になります。このモードでは、InterScan VirusWall の設定はリバースプロキシモード、またはネットワークトポロジによってはスタンドアロンモードの場合と同じです。

注意： WCCP (Web Cache Control Protocol) はサポートされません。

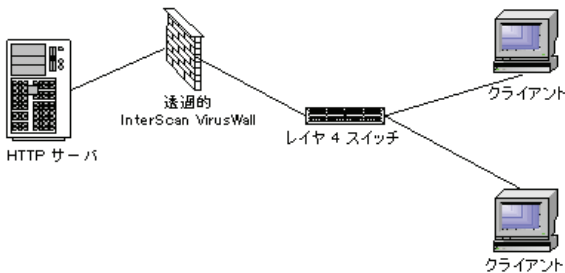


図 5-16. 透過モードのトポロジ

HTTP プロキシを設定する

InterScan VirusWall が HTTP トラフィックを監視する前に、HTTP サーバの設定を指定しておく必要があります。

InterScan VirusWall の HTTP プロキシを設定するには

1. 左側のメニューで、[HTTP] → [設定] の順に選択します。
2. モードを選択します。
 - InterScan VirusWall をネットワークの単独 HTTP プロキシサーバにする場合は、[スタンドアロンモードを使用する] を使用します。
 - [依存プロキシモード] を使用する場合は、上位プロキシ名とポート番号を入力します。

依存プロキシモードでは、不正な HTTP に含まれているセキュリティリスクをクライアントがサーバから受信しないように防御します。一般的な使用例としては、インターネットの不正なダウンロードファイルを受信しないよう、ネットワーク上の Web ユーザを保護することがあります。依存プロキシモードでは通常、InterScan VirusWall と InterScan VirusWall が保護するクライアントは同じ LAN 内にインストールされ、InterScan VirusWall は上位プロキシに依存しながら HTTP サーバにアクセスします。
 - リバースプロキシモードを使用する場合は、保護の対象とする HTTP サーバのアドレスを入力します。

リバースプロキシモードでは、InterScan VirusWall は Web サーバと Web サーバのクライアントとの間に配置されます。この設定はあまり一般的ではありませんが、通常は、Web サーバに不正なコンテンツがアップロードされるのを回避するために使用されます。リバースプロキシモードのトポロジでは通常、InterScan VirusWall は InterScan VirusWall が保護する Web サーバの近くにインストールされ、インターネットによってクライアントから分離されます。

3. HTTP 待機ポート (初期設定 8080) を入力します。
FTP over HTTP 匿名ユーザが有効な場合、設定アドレスはログオンメールアドレスとして使用されます。
4. すべての HTTP 要求をログファイルに記録する場合は、[HTTP 要求を記録する] を選択します。
この機能は、初期設定では無効になっています。

特定のネットワークインタフェースにバインドする

初期設定のインストール後に、HTTP はすべてのネットワークインタフェース上で待機します。

特定のネットワークインタフェースに対する待機を制限するには

1. 次のように Config.xml を修正します。

```
<Key Name="Http">
<Key Name="Main">
<Key Name="http">
<Value Name="listening_interface" string="IP" type="string" int="0" />
```

IP には、バインド対象のネットワークインタフェースの IPv4 アドレスが入ります。
2. InterScan VirusWall サービスを再起動します。

クライアントブラウザでプロキシを設定する (Internet Explorer)

InterScan VirusWall を使用して HTTP トラフィックを検索する場合に、**Internet Explorer** ブラウザのプロキシを設定するには

1. Internet Explorer ブラウザを開きます。
2. ブラウザのツールバーで、[ツール] → [インターネット オプション] の順に選択します。

3. [接続] タブをクリックし、図 5-17 に示すように [LAN の設定] をクリックします。

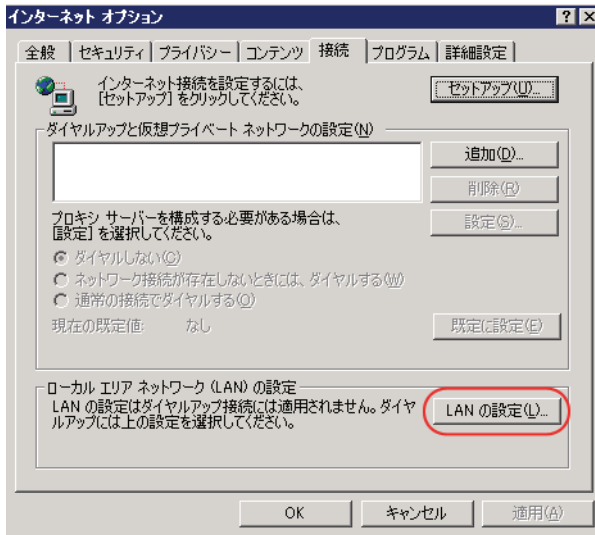


図 5-17. [インターネット オプション] → [接続] → [LAN の設定]

4. [ローカルエリア ネットワーク (LAN) の設定] ダイアログボックスで、[LAN にプロキシサーバを使用する (これらの設定はダイヤルアップまたは VPN 接続には適用されません)] の前のオプションを選択します。[アドレス] に InterScan VirusWall サーバの IP アドレスまたサーバ名を入力し、[ポート] に InterScan VirusWall サービスのポート番号 (初期設定値は 8080) を入力します。

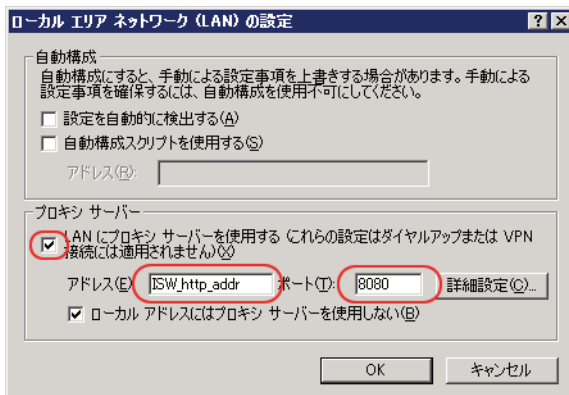


図 5-18. ローカル エリア ネットワーク (LAN) の設定

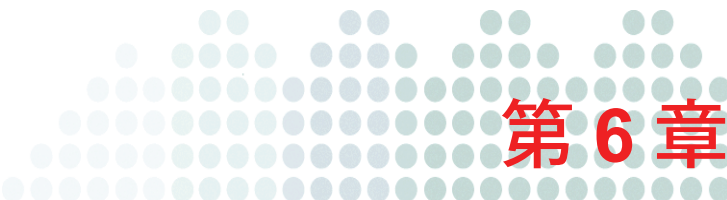
5. [OK] をクリックして設定を保存します。

HTTP トランザクションログを有効にする

InterScan VirusWall では現在、HTTP のトランザクションログがサポートされています。HTTP のトランザクションログは、初期設定で有効になっています。

HTTP トランザクションログを有効または無効にするには

1. Config.xml ファイルを開きます。
2. 「HTTP」の下にある「WriteConnectionMsg」という名前のキーを検索します。
3. 「WriteConnectionMsg」の値を「1」(有効) または「0」(無効) に設定します。
4. サービスを再起動します。



第6章

FTP サービスの設定

Trend Micro InterScan VirusWall スタンダードエディション (以下、InterScan VirusWall) では、FTP トラフィックを監視して、ネットワークゲートウェイのセキュリティを保持できます。FTP トラフィックの検索は、インストールプロセス中に有効または無効にすることも、インストール後の任意の時点で InterScan VirusWall Web コンソールの [概要] 画面で有効または無効にすることもできます。

次の FTP サービスを使用できます。

- アップロードおよびダウンロード時のウイルスとセキュリティリスクの検索
- スパイウェアなどのグレーウェアの検出
- FTP サーバモードと待機ポートの設定

InterScan VirusWall の [概要] 画面の [ファイル転送 (FTP)] タブでは、送受信されるファイルトラフィックで InterScan VirusWall の FTP 検索によって検出されたウイルスおよびスパイウェアのファイル数に関する統計情報が表示されます。

FTP サービスを有効または無効にする

FTP プロトコルを介したファイルのダウンロードとアップロードに対する検索サービスを有効または無効にするには、図 6-1 の [概要] 画面の [ファイル転送 (FTP)] タブで [FTP トラフィックを有効にする] チェックボックスをオンまたはオフにします。

図 6-1. [概要] 画面の [ファイル転送 (FTP)] タブ



[ファイル転送 (FTP)] タブには、検出された感染ファイルおよびスパイウェア / グレーウェアの検出に関する検索統計情報も表示されます。

注意： [FTP トラフィックを有効にする] チェックボックスがオフになっている場合、クライアントは InterScan VirusWall 経由で FTP サーバに接続できなくなります。[FTP 検索を有効にする] が無効になっていても、クライアントは InterScan VirusWall 経由で FTP サーバに接続でき、FTP サーバからアイテムをダウンロードできますが、アイテムのウイルス検索は行われません。

FTP ウイルス検索を設定する

InterScan VirusWall は、FTP トラフィックフローを検索して、アップロードおよびダウンロード時にウイルスなどのセキュリティリスクを検出します。FTP 検索は高度な設定が可能です。たとえば、ブロックするファイルタイプや、InterScan VirusWall が圧縮ファイルやサイズの大きいファイルを検索する方法を設定して、パフォーマンス上の問題やブラウザのタイムアウトを回避できます。

管理者は、[FTP] → [検索] の順に選択して、ウイルスや不正プログラムに対する FTP 検索を設定できます。

FTP ウイルス検索を有効にする

FTP ウイルス検索を有効にするには

1. 左のメニューから [FTP] → [検索] の順に選択します。
2. [対象] タブを選択します。
3. [FTP 検索を有効にする] チェックボックスをオンにします。
4. [保存] をクリックします。

検索するファイルタイプを指定する

InterScan VirusWall は、圧縮ボリューム内の個別ファイルを含めて、すべてのまたは指定したファイルタイプでウイルスを検索できます。図 6-2 に、ファイル検索時に指定できる設定を示します。

図 6-2. [FTP] → [検索] → [対象] タブ



検索するファイルタイプを選択するには

1. 左側のメニューで [FTP] → [検索] の順に選択し、[対象] タブを選択します。
2. [検索対象ファイル] で、必要なオプションを選択します。

- a. ファイルタイプにかかわらず、すべてのファイルを検索するには、[検索可能なすべてのファイル] を選択します。この設定が最も安全です。
- b. 検索するファイルを実際のファイルタイプで識別できるようにするには、[トレンドマイクロの推奨設定: 実際のファイルタイプによる識別] を選択します。

このオプションでは、一部のファイルタイプをそのまま配信するため、すべてのファイルを検索する場合よりも安全度は低くなります。

- c. 特定の拡張子のファイルのみを検索するには、[指定のファイル] を選択して、[拡張子] をクリックします。[その他の拡張子] テキストボックスで指定した拡張子を持つファイルのみが検索されます。

初期設定では、次のファイル名拡張子を持つファイルが検索されます。

"";ARJ;BAT;BIN;BOO;CAB;CHM;CLA;CLASS;COM;CSC;DLL;DOC;DOT;DRV;EML;EXE;GZ;HLP;HTA;HTM;HTML;HTT;INI;JAR;JPEG;JPG;JS;JSE;LNK;LZH;MDB;MPD;MPP;MPT;MSG;MSO;NWS;OCX;OFT;OVL;PDF;PHP;PIF;PL;POT;PPS;PPT;PRC;RAR;REG;RTF;SCR;SHS;SYS;TAR;VBE;VBS;VSD;VSS;VST;VXD;WML;WSF;XLA;XLS;XLT;XML;Z;ZIP;{*;

ヒント: 初期設定の検索リストを修正する場合は、[その他の拡張子] オプションを使用します。

- 3. [保存] をクリックします。

注意: 検索タイプと圧縮ファイル処理のオプションは、ウイルスおよびスパイウェアを含む全タイプのファイル検索に適用されます。

圧縮ファイルの処理

FTP 検索時の圧縮ファイルの処理方法を指定するには

左のメニューから [FTP] → [検索] の順に選択し、[対象] タブを選択します。

- すべての圧縮ファイルを検索するには、[すべての圧縮ファイルの検索] を選択します。この設定が最も安全です。
- すべての圧縮ファイルの検索をスキップするには、[圧縮ファイルを検索しない] を選択します。InterScan VirusWall は、圧縮ファイルを検索しません。
- ユーザが指定した制限内で圧縮ファイルを検索するには、[次の場合は圧縮ファイルを検索しない] を選択してから、圧縮ファイルを検索しない条件を指定します。

- ◆ 解凍後のファイル数が次の数を超える場合：圧縮ファイル内のファイルの最大数 (0 の場合は無制限)。制限に到達するまで、圧縮ファイル内のファイルが検索されます。
- ◆ 解凍後のファイルサイズが次を超える場合：解凍後の最大ファイルサイズ。制限内の個別ファイルのみが検索されます。
- ◆ 圧縮レイヤが次の数を超える場合：圧縮階層の最大数。たとえば、ZIP ファイルに RAR ファイルが含まれ、さらに RAR ファイルに別の圧縮ファイルが含まれている場合は、3 層の圧縮になります。制限に到達するまで、圧縮ファイル内のファイルが検索されます。
- ◆ 圧縮ファイルに対する解凍後のファイルサイズが次の割合を超える場合：圧縮前後の最大サイズ比率。制限内の個別ファイルのみが検索されます。

注意： 検索タイプと圧縮ファイル処理のオプションは、ウイルス、スパイウェア / グレーウェアを含む全タイプのファイル検索に適用されます。

ウイルス検出時に実行する処理を指定する

InterScan VirusWall が感染ファイルを検出した場合は、図 6-3 に示す 6 つの処理のいずれかを実行できます。

図 6-3. [FTP] → [検索] → [処理] タブ



感染ファイルの検出時に実行する処理を指定するには

1. 左のメニューから [FTP] → [検索] の順に選択し、[処理] タブを選択します。
2. [ウイルス感染ファイルに対する処理] で、必要なオプションを選択します。
 - 感染ファイルを常に駆除して受信者に配信するには、[駆除] を選択します。次に、感染ファイルを駆除できない場合に実行する処理を選択します。
 - 隔離 : 感染ファイルを削除して隔離します。
 - ブロック : 感染ファイルを隔離せずに削除します。
 - そのまま配信 (推奨しません) : 感染ファイルを配信します。
 - 感染ファイルを駆除せずに隔離ディレクトリに移動するには、[隔離] を選択します。受信者は感染ファイルを受信しません。
 - 感染ファイルを削除するには、[ブロック] を選択します。受信者は感染ファイルを受信しません。
 - 感染ファイルを受信者に配信するには、[そのまま配信 (推奨しません)] を選択します。
3. [保存] をクリックします。

注意： 初期設定の FTP 検索用隔離フォルダはフォルダは、インストールフォルダ下の、¥quarantine¥ftp です。

ウイルス検索の通知メッセージを指定する

InterScan VirusWall は、セキュリティリスクを検出すると、FTP クライアントを通じてユーザに通知します。ユーザ通知のメッセージテキストを変更したり、管理者にメールで通知することができます。

通知メッセージを設定するには

1. 左のメニューから [FTP] → [検索] の順に選択し、[通知] タブを選択します。
2. ユーザ通知の場合は、InterScan VirusWall から送信するメッセージテキストを入力します。

3. [管理者] を選択して、管理者への通知の送信を有効にします。必要に応じて、メッセージの内容を変更できます。FTP 検索の管理者通知では、次の任意のタグがサポートされています。

表 6-1.

タグ	説明
%DATETIME%	検索日時
%PROTOCOL%	プロトコル
%FILTERNAME%	処理を実行するフィルタの名前
%FINALACTION%	実行された処理
%QUARANTINE_AREA%	隔離場所
%MACHINENAME%	InterScan VirusWall コンピュータのホスト名

4. [保存] をクリックします。

FTP スパイウェア対策を設定する

スパイウェア / グレーウェアにはさまざまな形があり、多くの場合正規のソフトウェアプログラムのように見えます。トレンドマイクロは、スパイウェア / グレーウェアを追跡調査して、パターンファイルの定期アップデートを提供しています。

一般的なグレーウェアの種類は次のとおりです。

表 6-2. InterScan VirusWall によって追跡されるグレーウェアの種類

グレーウェアの種類	一般的な動作
スパイウェア	アカウントのユーザ名やパスワードなどのデータを収集して第三者に転送します。
アドウェア	広告を表示して、ユーザのネットサーフィンの傾向などについてデータを収集し、Web ブラウザを介してユーザを広告のターゲットにします。
ダイヤラー	コンピュータのインターネット設定を変更し、事前設定された電話番号にコンピュータがモデム経由で電話するように強制します。
ジョークプログラム	CD-ROM トレイの開閉や多数のメッセージボックスの表示など、コンピュータの異常動作を引き起こします。
ハッキングツール	ハッカーがコンピュータに侵入するのを助けます。
リモートアクセスツール	ハッカーがコンピュータにリモートアクセスして制御するのを助けます。
パスワード解読アプリケーション	ハッカーがアカウントのユーザ名とパスワードを解読するのを助けます。
その他	ここに記載されていないその他の種類

FTP スパイウェア検索を有効にする

FTP スパイウェア検索を有効にするには

1. 左のメニューから [FTP] → [スパイウェア対策] の順に選択し、[対象] タブを選択します。
2. [FTP スパイウェア対策を有効にする] チェックボックスをオンにします。
3. [保存] をクリックします。

図 6-5 に、[FTP] → [スパイウェア対策] → [対象] タブを示します。ここでは、FTP スパイウェア検索を有効にして、スパイウェア検索の除外対象を指定できます。

図 6-4. [FTP] → [スパイウェア対策] → [対象] タブ



スパイウェア検索の除外リストを設定する

スパイウェア / グレーウェアの検索から除外する特定のファイル名またはファイル名拡張子をリストするには

1. 左のメニューから [FTP] → [スパイウェア対策] の順に選択し、[対象] タブを選択します。
2. [スパイウェア / グレーウェアの名前を入力] に、スパイウェア / グレーウェア検索の対象から除外するスパイウェア名を入力します。

スパイウェア名が不明な場合は、[スパイウェア / グレーウェア名の確認] リンクをクリックします。

3. [追加] をクリックします。
4. [保存] をクリックします。

注意： 除外リストのエントリを削除するには、ごみ箱アイコンをクリックします。[保存] をクリックして変更内容を確認します。

検索するスパイウェアおよびグレーウェアの種類を指定する

InterScan VirusWall の FTP サービスで検索するスパイウェアおよびグレーウェアの種類を指定するには

1. 左のメニューから [FTP] → [スパイウェア対策] の順に選択し、[対象] タブを選択します。
2. [検索するスパイウェア / グレーウェア] で、FTP サービスで検索するスパイウェアとグレーウェアの種類を指定します。
3. [保存] をクリックします。

スパイウェア検出時に実行する処理を指定する

スパイウェアなどのグレーウェアの検出時に InterScan VirusWall が実行する処理を、3 つの処理の中から 1 つ選択できます。

スパイウェア / グレーウェアの検出時に実行する処理を指定するには

1. 左のメニューから [FTP] → [スパイウェア対策] の順に選択し、[処理] タブを選択します。
2. [スパイウェア / グレーウェア対策処理] で、次のいずれかのオプションを選択します。
 - スパイウェア / グレーウェアファイルを隔離ディレクトリに移動する場合は、[隔離] を選択します。ユーザはファイルを受信しません。
 - スパイウェア / グレーウェアプログラムのファイル転送を回避する場合は、[ブロック] を選択します。ユーザはファイルを受信しません。
 - スパイウェア / グレーウェアを対象の受信者に送信する場合は、[ダウンロード許可 (推奨しません)] を選択します。
3. [保存] をクリックします。

スパイウェア / グレーウェア検出時のユーザ通知メッセージを指定する

InterScan VirusWall は、ファイルを隔離またはブロックするときにユーザに通知します。ユーザ通知のメッセージテキストを変更できます。

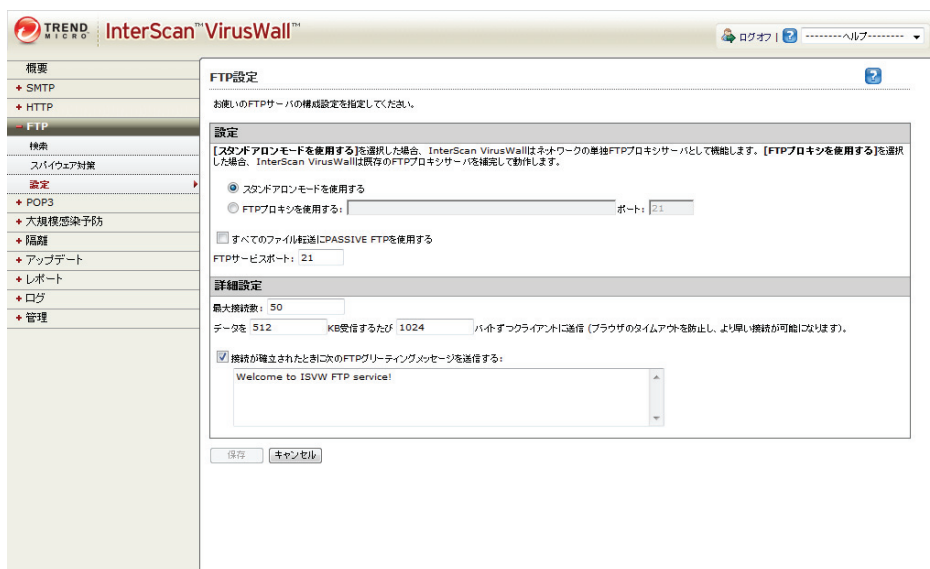
スパイウェア / グレーウェア検出時の通知設定を指定するには

1. 左のメニューから [FTP] → [スパイウェア対策] の順に選択し、[通知] タブを選択します。
2. InterScan VirusWall から送信するメッセージを入力します。
3. [保存] をクリックします。

FTP 設定

InterScan VirusWall で FTP トラフィックを監視するには、FTP サーバの設定を指定しておく必要があります。図 6-5 に、指定できる設定内容を示します。

図 6-5. FTP 設定



- ネットワーク上に既存の FTP プロキシサーバがなく、FTP VirusWall をシステムの FTP プロキシサーバとして機能するよう指定する場合は、[スタンドアロンモードを使用する] を選択します。
- システムに既存の FTP プロキシサーバがあり、そのサーバを引き続き使用する場合は、[FTP プロキシを使用する] を選択します。InterScan VirusWall をインストールすると、その後の FTP セッションはすべて InterScan VirusWall を通して実行されます。この処理はエンドユーザには見えません。

スタンドアロンモード

スタンドアロンモード用に設定した場合、クライアントは常に FTP VirusWall を使用して (その IP アドレスを使用して) FTP セッションを開きます。ユーザ名とパスワードの入力を求められたら、クライアントはコンピュータ名を含む、一定の規則に従ったユーザ名を入力する必要があります。

FTP プロキシモードを使用する

システムに既存の FTP プロキシサーバがあり、そのサーバを引き続き使用する場合は、[FTP プロキシを使用する] を選択します。InterScan VirusWall をインストールすると、その後の FTP セッションはすべて InterScan VirusWall を通して実行されます。この処理はエンドユーザには見えません。

FTP を使用してサイトとの間でファイルを転送するには

1. FTP コマンドを使用して InterScan VirusWall に接続します。

```
- > ftp [ コンピュータ名 ]
```

セッションから次の応答があります。

```
< - 220 InterScan VirusWall (Stand-alone Mode), セキュリティリスクの検索が有効です。Welcome to ISVW FTP service!
```

```
User (ISVW-test:(none)):
```

FTP サービスポートが 21 でない場合は、open コマンドを使用できます。

```
- > ftp
```

```
ftp> open [ コンピュータ名 ] [FTP サービスポート]
```

セッションから次の応答があります。

```
< - Connected to [ コンピュータ名 ]
```

```
220 InterScan VirusWall (Stand-alone Mode), セキュリティリスクの検索が有効です。Welcome to ISVW FTP service!
```

2. ログインプロンプトが表示されたら、ユーザ名とパスワードを入力します。ユーザ名は、< 元の名前 >@<FTP サイト>:<FTP ポート> という形式で入力する必要があります。

たとえば、FTP ログイン名が john、FTP サイトが antivirus.com、ポートが 21 の場合は、ユーザプロンプトに対して「john@antivirus.com:21」と入力し、パスワードプロンプトに対して元のパスワードを入力します。

セッションから次の応答があります。

```
User (ISVW-test:(none)):john@antivirus.com:21
```

```
Password: opensesame
```

注意： アクセス先の FTP サイトでポート 21 を使用している場合は、FTP ポートを省略できるため、この例では「john@antivirus.com」というユーザ名でログインすることもできます。

3. 正常にログインできたら、get または put コマンドを使用して、ファイルをダウンロードまたはアップロードします。コマンドウィンドウでファイルをアップロードまたはダウンロードすると、ウイルス検出情報が表示されます。

```
ftp> get eicar.com
```

```
200 PORT コマンド成功
```

```
150 Opening BINARY mode data connection for eicar.com (68 bytes) .
```

```
451-InterScan VirusWall からのメッセージ
```

```
451-InterScan は eicar.com からウイルスを検出しました。
```

```
451-
```

```
451- ウイルス Eicar_test_file が検出されました。
```

```
451-
```

```
451-Trend Micro InterScan VirusWall has determined that the file you are attempting to transfer is infected. It has taken action on the file.
```

```
451-
```

```
451 ファイルは拒否されました。
```

```
ftp>
```

4. ファイルのダウンロードまたはアップロードが完了したら、quit コマンドを使用して終了します。

注意： FTP VirusWall では、Proxy OPEN および匿名ユーザがサポートされています。

FTP プロキシサーバを設定する

FTP プロキシサーバ設定を設定するには

1. 左のメニューから [FTP] → [設定] の順に選択します。
2. モードを選択します。
既存のプロキシサーバを使用する場合は、次の操作も行います。
 - 既存の FTP プロキシサーバの IP アドレス（名前または数値）を入力します。
 - ポートを入力します。通常は 21 です。
3. 次の場合は、[すべてのファイル転送に PASSIVE FTP を使用する] (PASV モード) を選択します。
 - クライアントが NAT の背後にある場合
 - ネットワーク上にパケットフィルタを実行するファイアウォールがあり、そのファイアウォールがインターネットから LAN への（通常は 1024 より上のポートに対する）受信接続を拒否するように設定されている場合

アクティブモード (PORT モード): アクティブモードの FTP では、クライアントは、ランダムな非特権ポート (ポート番号 $N > 1023$) から FTP サーバのコマンドポートであるポート 21 に接続します。クライアントは、ポート $N+1$ に対する受信待機を開始して、FTP コマンド PORT $N+1$ を FTP サーバに送信します。サーバは、自身のローカルデータポートであるポート 20 から、クライアントの指定されたデータポートに接続します。

パッシブモード (PASV モード): パッシブモードの FTP では、クライアントは、サーバに対する両方の接続を開始して、サーバからクライアントへの受信データポート接続がファイアウォールによってフィルタされるという問題を解決します。FTP 接続の開始時に、クライアントは、2 つのランダムな非特権ポート (ポート番号 $N > 1023$ および $N+1$) をローカルに開きます。1 つ目のポートはサーバのポート 21 に接続しますが、クライアントは、PORT コマンドを発行してサーバに自身のデータポートへの接続を許可する代わりに、PASV コマンドを発行します。サーバは、ランダムな非特権ポート (ポート番号 $P > 1023$) を開いて、PORT P コマンドをクライアントに送信します。クライアントは、ポート $N+1$ からサーバのポート P への接続を開始して、データを転送します。

4. [FTP サービスポート] に入力します (通常は 21)。
これは FTP トラフィックの待機ポートです。
5. [最大接続数] に、InterScan VirusWall で受け入れを許可する同時 FTP 接続の最大数を入力します。

この制限に達すると、サイトにアクセスしようとしたユーザはキューに入れます。これにより、システム内のプロセッサの数によって、特定の状況においてスループットが向上します。システム上で利用可能な物理リソースと、予測される接続の数および頻度の平等なバランスを表す数値を選択します。
6. [データを、X KB を受信するたびに Y バイトずつクライアントに送信] に、トリクル転送の受信単位と送信単位を入力します。これにより、転送中のファイルを InterScan VirusWall で検索している間に接続が失われるのを防げます。非常に少ない量を使用できます。
7. FTP クライアントへのグリーティングメッセージの送信を有効にするには、[接続が確立されたときに次の FTP グリーティングメッセージを送信する] を選択します。グリーティングメッセージの内容はテキストボックスでカスタマイズできます。
8. [保存] をクリックします。

FTP トランザクションログを有効にする

InterScan VirusWall では現在、FTP のトランザクションログがサポートされています。FTP のトランザクションログは、初期設定で有効になっています。

FTP トランザクションログを有効または無効にするには

1. Config.xml ファイルを開きます。
2. 「FTP」の下にある「WriteConnectionMsg」という名前のキーを探します。
3. 「WriteConnectionMsg」の値を「1」(有効) または「0」(無効) に設定します。
4. サービスを再起動します。

POP3 サービスの設定

Trend Micro InterScan VirusWall スタンダードエディション（以下、InterScan VirusWall）を使用すると、POP3 受信メールトラフィックを監視できます。POP3 トラフィックの検索は、インストールプロセス中に有効または無効にすることも、インストール後の任意の時点で InterScan VirusWall Web コンソールの [概要] 画面で有効または無効にすることもできます。

次の POP3 サービスを使用できます。

- ウイルスおよびその他の種類の不正プログラムの検出
- 不正プログラムコードが含まれる可能性がある圧縮形式の実行ファイルに対する IntelliTrap 検索
- フィッシングサイトの検出
- 管理者がカテゴリおよびコンテンツレベルを設定できる、スパムメールの検出
- スパイウェアなどのグレーウェアの検出
- コンテンツフィルタ
- メッセージと添付ファイルのサイズによるフィルタ
- 受信メールの POP3 サーバポートと配信オプションの設定
- POP3 ファイル全体検索

InterScan VirusWall の [概要] 画面の [メール (POP3)] タブには、InterScan VirusWall の POP3 検索によって受信メール通信内で検出された、ウイルス、スパイウェア、スパムメールメッセージ、およびフィッシングメールの数に関する統計情報が表示されます。

POP3 サービスを有効または無効にする

POP3 メールメッセージトラフィックの検索サービスを有効または無効にするには、図 7-1 に示している [概要] 画面の [メール (POP3)] タブで [POP3 トラフィックを有効にする] チェックボックスをオンまたはオフにします。

図 7-1. [概要] 画面の [メール (POP3)] タブ



POP3 ウイルス検索を設定する

InterScan VirusWall では、管理者が自由に POP3 サービスの動作を設定できます。たとえば、次のような項目を指定できます。

- 検索する添付ファイルタイプ
- ウイルス検出時の通知の受信者
- ウイルス検出時に InterScan VirusWall で実行する処理 (駆除、削除、隔離、放置)

POP3 ウイルス検索機能

InterScan VirusWall の POP3 ウイルス検索には、次の機能があります。

- ・ カスタマイズ可能な自動ウイルス通知
- ・ 感染ファイルをウイルス駆除、削除、隔離、またはそのまま配信するオプション
- ・ カスタマイズされたタグラインをメッセージに挿入する機能

POP3 ウイルス検索を有効にする

POP3 ウイルス検索を有効にするには

1. 左側のメニューで [POP3] → [検索] の順に選択します。
2. [対象] タブを選択します。
3. [POP3 メール検索を有効にする] チェックボックスをオンにします。
4. [保存] をクリックします。

検索するファイルタイプを指定する

InterScan VirusWall は、圧縮ボリューム内の個別ファイルを含め、すべてのまたは指定した添付ファイルタイプでウイルスを検索できます。

検索するファイルタイプを選択するには

1. 左側のメニューで [POP3] → [検索] の順に選択し、[対象] タブを選択します。
2. [検索対象ファイル] で、必要なオプションを選択します。
 - a. ファイルタイプにかかわらず、すべての添付ファイルを検索するには、[検索可能なすべてのファイル] を選択します。この設定が最も安全です。
 - b. 検索する添付ファイルを実際のファイルタイプで識別できるようにするには、[トレンドマイクロの推奨設定: 実際のファイルタイプによる識別] を選択します。

このオプションでは、一部のファイルタイプをそのまま配信するため、すべての添付ファイルを検索する場合よりも安全度は低くなります。
 - c. 選択した添付ファイルタイプのみを検索するには、[指定のファイル] を選択して、[拡張子] をクリックします。[その他の拡張子] テキストボックスで明示的に指定したファイルタイプのみが検索されます。

初期設定では、次のファイル名拡張子を持つファイルが検索されます。

"";ARJ;BAT;BIN;BOO;CAB;CHM;CLA;CLASS;COM;CSC;DLL;DOC;DOT;DRV;EML;EXE;GZ;HLP;HTA;HTM;HTML;HTT;INI;JAR;JPEG;JPG;JS;JSE;LNK;LZH;MDB;MPD;MPP;MPT;MSG;MSO;

NWS;OCX;OFT;OVL;PDF;PHP;PIF;PL;POT;PPS;PPT;PRC;RAR;REG;RTF;SCR;SHS;SYS;TAR;
VBE;VBS;VSD;VSS;VST;VXD;WML;WSF;XLA;XLS;XLT;XML;Z;ZIP;{*;

ヒント： 初期設定の検索リストを修正する場合は、[その他の拡張子] オプションを使用します。

3. [保存] をクリックします。

注意： ウイルス検索設定は、ウイルス / 不正プログラム、IntelliTrap、スパイウェア検索など、すべての種類の POP3 不正ファイル検索に適用されます。

圧縮ファイルの処理を設定する

POP3 検索時の圧縮ファイルの処理方法を指定するには

1. 左側のメニューで [POP3] → [検索] の順に選択し、[対象] タブを選択します。
2. [圧縮ファイルの処理] で、必要なオプションを選択します。
 - a. すべての圧縮ファイルを検索するには、[すべての圧縮ファイルの検索] を選択します。この設定が最も安全です。
 - b. すべての圧縮ファイルをスキップするには、[圧縮ファイルを検索しない] を選択します。圧縮ファイルはいっさい検索されません。
 - c. ファイル数、解凍後のサイズ、圧縮階層数、および圧縮率に基づいて圧縮添付ファイルを検索するには、[次の場合は圧縮ファイルを検索しない] を選択します。次に、圧縮添付ファイルを検索する際の条件を指定します。
 - **解凍後のファイル数が次の数を超える場合：** 圧縮添付ファイル内のファイルの最大数 (0 の場合は無制限)。圧縮ファイル内のファイルはいっさい検索されません。
 - **解凍後のファイルサイズが次を超える場合：** 解凍後の最大ファイルサイズ。InterScan VirusWall は、制限内の個別のファイルのみ検索します (0 の場合は無制限)。
 - **圧縮レイヤが次の数を超える場合：** 圧縮階層の最大数。圧縮ファイル内のファイルはいっさい検索されません。
 - **圧縮ファイルに対する解凍後のファイルサイズが次の割合を超える場合：** 圧縮前後の最大サイズ比率。制限内の個別ファイルのみが検索されます。
3. [保存] をクリックします。

ウイルス検出時に実行する処理を指定する

InterScan VirusWall では、ウイルス検出時に 5 つの処理のうちの 1 つを実行できます。

感染した添付ファイルの検出時に実行する処理を指定するには

1. 左側のメニューで [POP3] → [検索] の順に選択し、[処理] タブを選択します。
2. [感染したアイテムを含むメッセージの処理] で、必要なオプションを選択します。
 - 感染した添付ファイルをウイルス駆除して、メッセージを配信するには、[感染したアイテムを駆除して配信] を選択します。次に、感染した添付ファイルをウイルス駆除できない場合に実行する処理を選択します。
 - **隔離**: 添付ファイルを取り除いて隔離します。
 - **削除**: 添付ファイルを隔離せずに削除します。
 - **放置**: 添付ファイルをメッセージと一緒に配信します。
 - 添付ファイルをウイルス駆除せずに隔離し、メッセージを配信するには、[感染したアイテムを隔離して配信] を選択します。
 - メッセージを削除するには、[メッセージ全体を削除] を選択します。
 - 添付ファイルを削除して、メッセージを配信するには、[感染したアイテムを削除して配信] を選択します。
 - 感染した添付ファイルと一緒にメッセージを配信するには、[そのまま配信 (推奨しません)] を選択します。
3. [保存] をクリックします。

注意: POP3 検索の初期設定の隔離フォルダは、インストールフォルダ下の ¥quarantine¥pop3 です。

ウイルス検索通知を設定する

ウイルスの検出時に、InterScan VirusWall から管理者、メッセージ受信者、または送信者に通知が送信されるように設定できます。設定を指定したり、検索したすべてのメッセージにインライン通知を含めたり、通知設定を指定することができます。

InterScan VirusWall によるウイルス検出時の通知設定を指定する

受信メッセージの添付ファイルでウイルスが検出された場合の通知設定を指定するには

1. 左側のメニューで [POP3] → [検索] の順に選択し、[通知] タブを選択します。
2. [メール通知] で、ウイルス検出時に送信する通知の受信者を選択します。
3. 各受信者に送信するメッセージを作成します。メッセージ内に次の任意のタグを使用します。

タグ	説明
%SENDER%	送信者アドレス
%RCPTS%	受信者アドレス
%SUBJECT%	メールの件名
%HEADERS%	メールヘッダ
%DATETIME%	検索日時
%MAILID%	メールメッセージ ID
%PROTOCOL%	メールプロトコル
%FILTERNAME%	処理を実行するフィルタの名前
%DETECTED%	検出されたセキュリティリスクの名前
%FINALACTION%	メッセージに対して実行された処理
%QUARANTINE_AREA%	隔離場所
%MACHINENAME%	InterScan VirusWall コンピュータのホスト名

4. [保存] をクリックします。

インライン通知設定を指定する

InterScan VirusWall では、インライン通知と呼ばれるテキストを受信メッセージのメッセージ本文に挿入できます。メッセージの種類の [ウイルス検出なし] および [ウイルス検出あり] を選択すると、検索されたすべてのメッセージにインライン通知が表示されます。

受信メッセージのインライン通知設定を指定するには

1. 左側のメニューで [POP3] → [検索] の順に選択し、[通知] タブを選択します。
2. [オリジナルメールに挿入する通知スタンプ] (図 7-2 を参照) で、インライン通知を含めるメッセージの種類 ([ウイルス検出なし] および [ウイルス検出あり]) を選択します。

オリジナルメールに挿入する通知スタンプ

チェックボックスをオンにすると、検索したすべてのメッセージに対して、受信者に送信する前に次のテキストが挿入されます。

☐ ウイルス検出なし InterScan VirusWallは、このメッセージにおいてウイルス検索を実行し、既知のウイルスは検出されませんでした。

☒ ウイルス検出あり InterScan VirusWallは、このメッセージにおいてウイルスを検出しました。

図 7-2. 【オリジナルメールに挿入する通知スタンプ】

3. メッセージ本文に挿入するインライン通知を入力します。次の任意のタグを使用します。

タグ	説明
%VIRUSNAME%	検出されたウイルスの名前
%FILENAME%	感染ファイルの名前
%CONTAINERNAME%	アーカイブなど、圧縮ファイルが含まれているファイルの名前
%ACTION%	感染添付ファイルに対して実行された処理

4. [保存] をクリックします。

POP3 ファイル全体検索

POP3 ファイル全体検索は、通常のメールのウイルス検索を補足する検索です。ファイル全体検索では、通常の検索方法では検出できない特別な種類のメールのウイルスを検出することができます。ファイル全体検索は、InterScan VirusWall 製品フォルダにある Config.xml ファイルから設定できます。

ファイル全体検索の動作

InterScan VirusWall でメールが受信されると、まずウイルスフィルタでテストされます。ウイルスフィルタでウイルスが検出されなかった場合には、次にファイル全体フィルタでテストされます。メールによってファイル全体フィルタがトリガされた場合、メールにはウイルスが含まれており、このメッセージに対する処理が実行され、通知送信が有効化されている場合には管理者や受信者への通知が送信されます。実行する処理として配信が設定されている場合、受信メールにウイルスが含まれることをユーザに警告するように設定することができます。

POP3 ファイル全体検索を設定する

ファイル全体検索の設定は、4つのステッププロセスにより行います。まず、ファイル全体検索を有効化します。次に、ウイルス検出時に実行する処理を設定（有効化）します。次に、ウイルスが検出されたことを管理者と受信者に通知する通知メッセージを設定します。最後に、検出ウイルス時の処理として配信が設定されている場合、メールに挿入されるディスクレマー文を設定します。

注意： ファイル全体検索は初期設定で無効にされています。

ファイル全体検索を有効または無効にする

ファイル全体検索を有効 / 無効にするには

1. InterScan VirusWall 製品フォルダを開き、Config.xml ファイルを見つけます。
2. 任意のテキストエディタプログラムで、Config.xml ファイルを開きます。
3. 画面を下方方向にスクロールし、次の値を見つけます。

```
<Value Name="EnableWholeFileScan" string="" type="int"
int="0" />
```

表 7-1. 「EnableWholeFileScan」 値のパス

```
<Key Name="POP3">
  <Key Name="Policies">
    <Key Name="Rule1">
      <Key Name="MailVirusScan">
        <Value Name="EnableWholeFileScan" string="" type="int" int="0" />
```

4. ファイル全体検索を有効にするには「Int」の値を「1」、無効にするには「0」に設定します。
5. ファイルを保存し、閉じます。
6. InterScan VirusWall サーバを再起動すると、変更が適用されます。

処理を設定する

ファイル全体フィルタでウイルスが検出されたときに実行できる処理は、配信、削除、隔離のいずれかです。初期設定の処理は、隔離です。処理を配信に変更した場合、InterScan VirusWall は元の受信者にメールを配信します。メールの本文にディスクレーマーを挿入し、受信メールにウイルスが含まれることを受信者に警告することもできます。処理を削除に設定すると、メールは削除されます。

ファイル全体フィルタでのウイルス検出時に実行する処理を設定するには

1. InterScan VirusWall 製品フォルダを開き、Config.xml ファイルを見つけます。
2. 任意のテキストエディタプログラムで、Config.xml ファイルを開きます。
3. 画面を下方方向にスクロールし、次のキーを見つけます。

```
<Key Name="Deliver">
<Key Name="Delete">
<Key Name="Quarantine">
```

表 7-2. Deliver、Delete、および Quarantine キーのパス

```

<Key Name="POP3">
<Key Name="Policies">
<Key Name="Rule1">
<Key Name="MailVirusScan">
<Key Name="Outcomes">
<Key Name="OutcomeWholeFileScanVirus">
<Key Name="Actions">
<Key Name="Deliver">
<Value Name="Enable" string="" type="int" int="0" />
<Key Name="Delete">
<Value Name="Enable" string="" type="int" int="0" />
<Key Name="Quarantine">
<Value Name="Enable" string="" type="int" int="1" />

```

注意： ファイル全体フィルタでウイルスが検出されたときに実行できる処理は 3 つあります。Config.xml ファイルで、3 つの処理のうちの 1 つだけが有効になっていることを確認してください。ファイル全体検索の初期設定の処理は、[隔離] です。

4. ファイル全体フィルタでのウイルス検出時に実行する処理を設定します。

表 7-3. ファイル全体検索に対する処理

処理の種類	処理の設定		
	配信するには	削除するには	隔離するには
配信	1	0	0
削除	0	1	0
隔離	0	0	1

5. ファイルを保存し、閉じます。
6. InterScan VirusWall サーバを再起動すると、変更が適用されます。

通知を送信する

ファイル全体フィルタでウイルスが検出された場合、通知メッセージを管理者や受信者へ送信することができます。Config.xml ファイルから、これらのユーザに対する通知を有効または無効にすることができます。InterScan VirusWall には初期設定の通知メッセージが用意されていますが、Config.xml ファイルから変更することもできます。

ファイル全体フィルタでのウイルス検出時に通知が送信されるようにするには

1. InterScan VirusWall 製品フォルダを開き、Config.xml ファイルを見つけます。
2. 任意のテキストエディタプログラムで、Config.xml ファイルを開きます。
3. 画面を下方向にスクロールし、次のキーを見つけます。

```
<Key Name="NotificationAdmin">
<Key Name="NotificationRecipient">
```

表 7-4. NotificationAdmin および NotificationRecipient キーのパス

```
<Key Name="POP3">
<Key Name="Policies">
  <Key Name="Incoming"> または <Key Name="Outgoing">
    <Key Name="Rule1">
      <Key Name="MailVirusScan">
        <Key Name="Outcomes">
          <Key Name="OutcomeWholeFileScanVirus">
            <Key Name="Actions">
              <Key Name="NotificationAdmin">
                <Value Name="Enable" string="" type="int" int="0" />
              <Key Name="NotificationRecipient">
                <Value Name="Enable" string="" type="int" int="1" />
```

4. 通知を有効にするには、「Enable」の値を「1」に設定します。特定のユーザに対する通知を無効にするには、「Enable」の値を「0」に設定します。
5. (オプション) 次のタグを見つけます。


```
<Value Name="Body"string="..."
```

 各受信者に送信するメッセージを変更するか、初期設定をそのまま使用します。
6. ファイルを保存し、閉じます。
7. InterScan VirusWall サーバを再起動すると、変更が適用されます。

ディスクレーマー文を変更する

ウイルスを含むメッセージに対する処理が配信の場合、元のメールにディスクレーマー通知を追加することができます。ディスクレーマーをメールに追加するには、最初に InterScan VirusWall Web コンソールで [オリジナルメールに挿入する通知スタンプ] を有効にします。次に、ファイル全体検索の処理を配信に設定します。

ディスクレーマー文の内容を変更するには

1. InterScan VirusWall 製品フォルダを開き、Config.xml ファイルを見つけます。
2. 任意のテキストエディタプログラムで、Config.xml ファイルを開きます。
3. 画面を下方方向にスクロールし、次のタグを見つけます。

```
<Value Name="VirusAlert4WholeFileScan" string="..."
```

表 7-5. 「VirusAlert4WholeFileScan」タグのパス

```
<Key Name="POP3">
<Key Name="Policies">
  <Key Name="Rule1">
    <Key Name="MailVirusScan">
      <Value Name="VirusAlert4WholeFileScan" string="..."
```

4. string の値である引用符内のテキストを変更または置換します。

注意： ディスクレーマー文では、ウイルス名を識別する「%VIRUSNAME%」というタグを使用できます。

5. ファイルを保存し、閉じます。
6. InterScan VirusWall サーバを再起動すると、変更が適用されます。

IntelliTrap を設定する

IntelliTrap では、メールの添付ファイルとして着信した、リアルタイム圧縮された実行可能ファイル内で、不正プログラムコードと疑われるものが検出されます。IntelliTrap を有効にすると、感染している添付ファイルに対しユーザ定義の処理を実行し、受信者、または管理者に通知を送信できます。

POP3 IntelliTrap 検索を有効または無効にする

POP3 IntelliTrap 検索を有効または無効にするには

1. 左側のメニューで [POP3] → [IntelliTrap] の順に選択し、[対象] タブを選択します。
2. IntelliTrap 検索を有効または無効にするには、[POP3 IntelliTrap を有効にする] チェックボックスをオンまたはオフにします。
3. [保存] をクリックします。

IntelliTrap の検出時の処理を指定する

InterScan VirusWall では、IntelliTrap が不正プログラムコードと疑われるものを検出したときに、3 つの処理のうちの 1 つを実行できます。

IntelliTrap によって不正プログラムコードと疑われるものが検出された場合に実行する処理を指定するには

1. 左側のメニューで [POP3] → [IntelliTrap] の順に選択し、[処理] タブを選択します。
2. [感染した添付ファイルを含むメッセージの処理] で、必要なオプションを選択します。
 - 添付ファイルを隔離して、メッセージを配信するには、[感染した添付ファイルを隔離して配信] を選択します。ユーザは添付ファイルのないメッセージを受信します。添付ファイルは隔離フォルダに保存されます。
 - 添付ファイルを削除して、メッセージを配信するには、[感染した添付ファイルを削除して配信] を選択します。ユーザは添付ファイルのないメッセージを受信します。
 - 感染した添付ファイルと一緒にメッセージを配信するには、[そのまま配信 (推奨しません)] を選択します。ユーザは添付ファイルの付いたメッセージとインライン警告を受信します。
3. [保存] をクリックします。

注意： POP3 検索の初期設定の隔離フォルダは、インストールフォルダ下の ¥quarantine¥pop3 です。

IntelliTrap 通知を設定する

InterScan VirusWall では、IntelliTrap によって圧縮形式の実行ファイルで不正プログラムコードと疑われるものが検出された場合に、選択した受信者に自動的に通知できます。

IntelliTrap によってメッセージの添付ファイルでセキュリティの脅威が検出された場合の通知設定を指定するには

1. 左側のメニューで [POP3] → [IntelliTrap] の順に選択し、[通知] タブを選択します。
2. IntelliTrap によってセキュリティリスクが検出された場合に送信する通知の受信者を選択します。
3. 各受信者に送信するメッセージを作成します。メッセージ内に次の任意のタグを使用します。

タグ	説明
%SENDER%	送信者アドレス
%RCPTS%	受信者アドレス
%SUBJECT%	メールの件名
%HEADERS%	メールヘッダ
%DATETIME%	検索日時
%MAILID%	メールメッセージ ID
%PROTOCOL%	メールプロトコル
%FILTERNAME%	処理を実行するフィルタの名前
%DETECTED%	検出されたセキュリティリスクの名前
%FINALACTION%	メッセージに対して実行された処理
%QUARANTINE_AREA%	隔離場所
%MACHINENAME%	InterScan VirusWall コンピュータのホスト名

4. [保存] をクリックします。

POP3 フィッシング対策を設定する

フィッシングとは、急増している詐欺の 1 つで、正規の Web サイトを模倣し、Web ユーザに個人情報を開示させることです。フィッシング攻撃は、既存の正規の組織を偽装したメールメッセージから始まります。メッセージには通常、リンクが記載されており、受信者にこのリンクをクリックさせるように仕向け、ブラウザを偽の Web サイトに誘導します。Web サイトでは個人情報をアップデートするよう求められます。疑いを持たないユーザは、パスワード、クレジットカード番号などを提供してしまいます。

典型的なシナリオでは、疑いを持たないユーザが緊急を装う（本物のような）メールを受信します。そこには、ユーザのアカウントにすぐに解決しなければならない問題があり、解決しなければアカウントが閉じられると書かれています。そのメールには、本物に非常によく似た Web サイトの URL が含まれています。正規のメールと正規の Web サイトをコピーした後、バックエンドを変更するのは簡単です。収集したデータは実際にはこのバックエンドに送信されます。

POP3 フィッシング対策を有効にする

POP3 フィッシング対策機能を有効にするには

1. 左側のメニューで [POP3] → [フィッシング対策] の順に選択し、[対象] タブを選択します。
2. [POP3 フィッシング対策を有効にする] チェックボックスをオンにします。
3. [保存] をクリックします。

フィッシング検出時の処理を指定する

フィッシングメールに対する処理を指定するには

1. 左側のメニューで [POP3] → [フィッシング対策] の順に選択し、[処理] タブを選択します。
2. フィッシングメールに対する処理を選択します。
 - メッセージを隔離フォルダに移動する場合は、[隔離] を選択します。
 - メッセージを配信せずに削除する場合は、[削除] を選択します。
 - フィッシングメールを通常どおりに配信する場合は、[放置] を選択します。
3. [保存] をクリックします。

フィッシングサイトの検出時の通知を設定する

InterScan VirusWall では、フィッシングメールの検出時に、管理者または受信者、あるいはその両方にメール通知を送信できます。フィッシングサイトの疑いのあるサイトや既知のフィッシングサイトを TrendLabs に報告することもできます。[POP3] → [フィッシング対策] → [通知] タブでは、InterScan VirusWall によるフィッシングサイトの検出時にメール通知を送信するかどうかを指定できます。

フィッシング URL 検出時の通知設定を指定するには

1. 左側のメニューで [POP3] → [フィッシング対策] の順に選択し、[通知] タブを選択します。
2. フィッシング URL 検出時に送信される通知の受信者を選択します。

3. 各受信者に送信するメッセージを作成します。メッセージ内に次の任意のタグを使用します。

タグ	説明
%SENDER%	送信者アドレス
%RCPTS%	受信者アドレス
%SUBJECT%	メールの件名
%HEADERS%	メールヘッダ
%DATETIME%	検索日時
%MAILID%	メールメッセージ ID
%PROTOCOL%	メールプロトコル
%FILTERNAME%	処理を実行するフィルタの名前
%DETECTED%	検出されたセキュリティリスクの名前
%FINALACTION%	実行された処理
%QUARANTINE_AREA%	隔離場所
%MACHINENAME%	InterScan VirusWall コンピュータのホスト名

4. [保存] をクリックします。

フィッシングサイトの可能性のある URL を報告する

フィッシングサイトの疑いのあるサイトまたは既知のフィッシングサイトを TrendLabs に報告するには、[TrendLabs (トレンドラボ) への疑わしいフィッシング URL の送信] をクリックし、メールにそのサイトの URL を記載して、antifraud@support.trendmicro.com に送信してください。

TrendLabs では、詐欺目的のために情報を取得するサイトを監視し、InterScan VirusWall のユーザーにトレンドマイクロから提供される自動アップデートの一部として既知のフィッシングサイトの情報を配布します。

POP3 スпамメール対策を設定する

InterScan VirusWall では、POP3 メール通信でのスパムメールのフィルタに、次の基本的な機能が使用されます。

- ・ **承認する送信者およびブロックする送信者リスト** : これらのリストでは、コンテンツではなく、送信者のメールアドレスに基づいてフィルタされます。InterScan VirusWall では、承認する送信者のメッセージは常に配信され、ブロックする送信者のメッセージは常にスパムメールとして分類されます。

注意： Exchange 管理者は、Exchange サーバ用の [承認する送信者] および [ブロックする送信者] の個別のリストを管理します。エンドユーザが承認する送信者を登録し、その送信者が管理者の [ブロックする送信者] リストに登録されている場合、その送信者からのメッセージはブロックされます。

- ・ **スパムメールフィルタ** : 管理者はスパムメールのフィルタに使用するスパムメール検出レベルを設定します。検出レベルが高いほど、スパムメールとして分類されるメッセージは多くなります。すべてのメッセージに共通の検出レベルを設定するか、スパムメールカテゴリごとに 1 つの検出レベルを設定できます。

検出レベルによって、InterScan VirusWall が疑わしいメールメッセージをどの程度許容するかが決まります。

- ◆ 「高」の検出レベルでは、多数のメールがスパムメールとして隔離されます。ただし、正規のメールメッセージがスパムメールと誤認識されて隔離され、「誤検出された」スパムメールとなる可能性もあります。
- ◆ 低い検出レベルでは、メールメッセージの選別は厳しくなく、スパムメールメッセージの誤検出が多数発生することはありません。

POP3 スパムメール対策を有効にする

図 7-3 に示している [POP3] → [スパムメール対策] → [対象] タブでは、スパムメールのフィルタを有効にし、定義済みのさまざまなスパムメールカテゴリに検出レベルを指定できます。



図 7-3. [POP3] → [スパムメール対策] → [対象] タブ

POP3 スпамメール対策フィルタを有効にするには

1. 左側のメニューで [POP3] → [スパムメール対策] の順に選択します。
2. [対象] タブを選択します。
3. [POP3 スпамメール対策を有効にする] チェックボックスをオンにします。
4. [保存] をクリックします。

スパムメール検出レベルを設定する (フィルタ調整)

スパムメール検出レベルを指定するには

1. 左側のメニューで [POP3] → [スパムメール対策] の順に選択します。
2. [対象] タブを選択します。
3. [フィルタ調整] で、任意のスパムメール検出レベルを選択します。

スパムメール検出レベル

InterScan VirusWall では、次の検出レベルが使用されます。

検出レベル	フィルタ基準
低	最も明白で一般的なスパムメールメッセージのみがフィルタされ、誤検出の確率も非常に低くなります。これは、最も寛容なスパムメール検出レベルです。
中	高いスパムメール検出レベルで監視が実行されます。誤検出の可能性は中程度です。これは、初期設定です。
高	すべてのメールメッセージで疑わしいファイルまたはテキストが監視されますが、誤検出の可能性も非常に高くなります。これは、最も厳しいスパムメール検出レベルです。

スパムメール検出レベルを決定する

InterScan VirusWall スパムメール検索エンジンでは、ヒューリスティックとアルゴリズムを使用してスパムメール検出レベルが計算されます。このエンジンでは、メッセージまたはファイルが検索され、検索されたアイテムにスパムメールスコアが割り当てられます。対象のアイテムがスパムメールかどうかの判断は、割り当てられたスパムメールスコアと、指定されたスパムメール検出レベルおよび確実性レベルに基づきます。

しきい値の例は、次のとおりです。

	低の確実性	中の確実性	高の確実性
低の検出レベル	6	7	10
中の検出レベル	4.5	6	10
高の検出レベル	4	5	7

注意： スパムメールしきい値設定テーブルのスコアは、使用中のスパムメール判定ルールにより異なることがあります。

- ・ 低の検出レベルを指定し、スパムメールスコアが 6.5 の場合は、低の確実性レベルに指定された処理が実行されます。
- ・ スパムメールスコアが 8 の場合は、中の確実性レベルに指定された処理が実行されます。
- ・ スパムメールスコアが 11 の場合は、高の確実性レベルに指定された処理が実行されます。

スパムメールスコアを確認するには、スパムメールログを参照してください。次に、エントリの例を示します。

```
2006/02/04 20:10:32, SMTP, , Stamp, Success, "LastName¥, FirstName"
<FirstName.LastName@Level3.com>, "SPAM@TrendMicro.com"
<SPAM@TrendMicro.com>, FW:How are you doing?
<D7626E4452B0F745B4C7C15BC97EA052D66887@idclexc0005.corp.global.
level3.com>, 3.51.0.1033, 13974000, Spam, ,14.594000
```

スパムメールフィルタを調整する

過剰な数の誤検出がある場合は、スパムメール検出レベルの設定を低くします。逆に、スパムメールを多く受け取りすぎるとユーザが報告する場合は、検出レベルの設定が高くなるように調整します。

キーワード除外を指定する

キーワード除外を使用して、スパムメールフィルタから特定のテキストを含むメッセージを除外できます。例外リスト内の各キーワードはカンマで区切ります。図 7-4 に示している [キーワード除外設定] ボックスに、スパムメールとは見なさないキーワードを入力します。

注意： キーワード間には単一のカンマ (,) 以外の記号を挿入できません。スペースや改行を挿入しないでください。

キーワード除外設定

指定されたキーワードを含むメッセージは、スパムメールと判定されません。複数入力する場合は、カンマ (,) で区切ってください。

承認する送信者

承認する送信者のメールアドレスまたはドメイン名を追加します (例: example.com, abc@example.com, @example.com)。複数入力する場合は、カンマ (,) で区切ってください。

ブロックする送信者

ブロックする送信者のメールアドレスまたはドメイン名を追加します (例: example.com, abc@example.com, @example.com)。複数入力する場合は、カンマ (,) で区切ってください。

保存 キャンセル

図 7-4. [POP3] → [スパムメール対策] → [キーワード除外設定]、[承認する送信者]、および [ブロックする送信者] リスト

承認する送信者およびブロックする送信者のリストを管理する

[承認する送信者] リストには、信頼されたメールアドレスが含まれます。InterScan VirusWall は、フィッシング対策が有効になっている場合を除いて、これらのアドレスから受信したメッセージをスパムメールとしてフィルタしません。

[ブロックする送信者] リストには、信頼できないメールアドレスが含まれます。これらのアドレスから着信したメッセージは、自動的にスパムメールと見なされて削除されます。メッセージが削除されたことは通知されません。

同じメールアドレスが [承認する送信者] リストと [ブロックする送信者] リストの両方に含まれる場合、そのアドレスから着信したメッセージはスパムメールと見なされて削除されます。

メールアドレスをリストに追加するときは、アドレスをカンマで区切ります。図 7-4 に示しているように、該当するリストにすべてのメールアドレスを入力します。

InterScan VirusWall は、[承認する送信者] および [ブロックする送信者] リストで、ワイルドカード (*) 照合をサポートします。パターンの例を表 7-6 に示します。

表 7-6. 送信者リストでのワイルドカード (*) の使用

パターン	一致する例	一致しない例
john@trend.com	john@trend.com john@trend.com.	パターンと一致しないすべてのアドレス
@trend.com *@trend.com	john@trend.com mary@trend.com.	john@ms1.trend.com john@trend.com.tw mary@trend.comon
trend.com	john@trend.com john@ms1.trend.com mary@ms1.rd.trend.com mary@trend.com.	john@trend.com.tw mary@mytrend.com joe@trend.comon
*.trend.com	john@ms1.trend.com mary@ms1.rd.trend.com joe@ms1.trend.com.	john@trend.com john@trend.com.tw mary@ms1.trend.comon
trend.com.*	john@trend.com.tw john@ms1.trend.com.tw john@ms1.rd.trend.com.tw mary@trend.com.tw.	john@trend.com john@ms1.trend.com. john@mytrend.com.tw
.trend.com.	john@ms1.trend.com.tw john@ms1.rd.trend.com.tw mary@ms1.trend.com.tw.	john@trend.com john@ms1.trend.com john@trend.com.tw john@ms1.trend.com.
.trend.com *.trend.com	「*.trend.com」と同じ	「*.trend.com」と同じ
trend.com trend.com trend*.com @*.trend.com	これらはすべて無効	これらはすべて無効

スパムメールと見なされたメッセージに対する処理を指定する

InterScan VirusWall では、メッセージがスパムメールと見なされた場合にいくつかの処理のうちの 1 つを実行できます。この処理は、[対象] タブで設定した検出レベルに基づきます。図 7-5 に、[POP3] → [スパムメール対策] → [処理] タブを示します。



図 7-5. [POP3] → [スパムメール対策] → [処理] タブ

スパムメールメッセージに対する処理を指定するには

1. 左側のメニューで [POP3] → [スパムメール対策] の順に選択し、[処理] タブを選択します。
2. 判定の確実性レベルに基づいて実行する処理を指定します。
 - ・ **高**: メールは確実にスパムメールであると思われます。
 - ・ **中**: メールはおそらくスパムメールであると思われます。
 - ・ **低**: メールはおそらくスパムメールではないと思われます。

それぞれの確実性レベルで、次の 4 つの処理の中の 1 つを選択できます。

- ・ **削除**: メッセージ全体が削除されます。
- ・ **隔離**: メッセージが隔離されます。
- ・ **スタンプの挿入**: 通知コンテンツスタンプがメッセージの件名行に挿入されます。
- ・ **放置**: InterScan VirusWall はメッセージに対して何も実行せず、通常どおり処理します。

InterScan VirusWall によるスパムメールの検出時の通知を指定する

InterScan VirusWall では、スパムメールメッセージの検出時に管理者または受信者に通知できます。メール通知の受信者を指定し、管理者およびメール受信者に送信するメッセージを作成できます。図 7-6 に、[POP3] → [スパムメール対策] → [通知] タブを示します。



図 7-6. [POP3] → [スパムメール対策] → [通知] タブ

InterScan VirusWall によるスパムメールの検出時の通知設定を指定するには

1. 左側のメニューで [POP3] → [スパムメール対策] の順に選択し、[通知] タブを選択します。
2. [メール通知] で、スパムメールが検出された場合に通知を受ける受信者を選択します。
3. 各受信者に送信するメッセージを作成します。メッセージ内に次の任意のタグを使用します。

タグ	説明
%SENDER%	送信者アドレス
%RCPTS%	受信者アドレス
%SUBJECT%	メールの件名
%HEADERS%	メールヘッダ
%DATETIME%	検索日時
%MAILID%	メールメッセージ ID
%PROTOCOL%	メールプロトコル
%FILTERNAME%	処理を実行するフィルタの名前

タグ	説明
%DETECTED%	検出されたセキュリティリスクの名前
%FINALACTION%	実行された処理
%QUARANTINE_AREA%	隔離場所
%MACHINENAME%	InterScan VirusWall コンピュータのホスト名

4. [保存] をクリックします。

POP3 スパイウェア対策を設定する

スパイウェア / グレーウェアにはさまざまな形があり、多くの場合正規のソフトウェアプログラムのように見えます。トレンドマイクロは、スパイウェア / グレーウェアを追跡調査して、パターンファイルの定期アップデートを提供しています。

一般的なグレーウェアの種類は次のとおりです。

グレーウェアの種類	一般的な動作
スパイウェア	アカウントのユーザ名やパスワードなどのデータを収集して第三者に転送します。
アドウェア	広告を表示して、ユーザのネットサーフィンの傾向などについてデータを収集し、Web ブラウザを介してユーザを広告のターゲットにします。
ダイヤラー	コンピュータのインターネット設定を変更し、事前設定された電話番号にコンピュータがモデム経由で電話するように強制します。
ジョークプログラム	CD-ROM トレイの開閉や多数のメッセージボックスの表示など、コンピュータの異常動作を引き起こします。
ハッキングツール	ハッカーがコンピュータに侵入するのを助けます。
リモートアクセスツール	ハッカーがコンピュータにリモートアクセスして制御するのを助けます。
パスワード解読アプリケーション	ハッカーがアカウントのユーザ名とパスワードを解読するのを助けます。
その他	ここに記載されていないその他の種類

POP3 スパイウェア検索を有効にする

POP3 スパイウェア検索を有効にするには

1. 左側のメニューで [POP3] → [スパイウェア対策] の順に選択し、[対象] タブを選択します。
2. [POP3 スパイウェア対策を有効にする] チェックボックスをオンにします。
3. [保存] をクリックします。

図 7-7 に、[POP3] → [スパイウェア対策] → [対象] タブを示します。ここでは、POP3 スパイウェア検索を有効にして、スパイウェア検索の除外対象を指定できます。

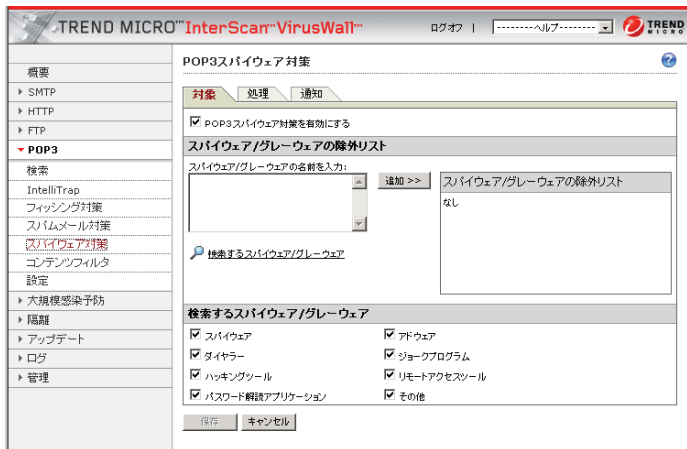


図 7-7. [POP3] → [スパイウェア対策] → [対象] タブ

スパイウェア検索の除外リストを設定する

スパイウェア / グレーウェアの検索から除外する特定のファイル名またはファイル名拡張子をリストするには

1. 左側のメニューで [POP3] → [スパイウェア対策] の順に選択し、[対象] タブを選択します。
2. [スパイウェア / グレーウェアの名前を入力] に、スパイウェア / グレーウェア検索の対象から除外するスパイウェア名を入力します。

スパイウェア名が不明な場合は、[スパイウェア / グレーウェア名の確認] リンクをクリックします。

3. [追加] をクリックします。
4. [保存] をクリックします。

注意： 除外リストのエントリを削除するには、ごみ箱アイコンをクリックします。[保存] をクリックして変更内容を確認します。

検索するスパイウェアおよびグレーウェアの種類を指定する

InterScan VirusWall の POP3 サービスで検索を実行するスパイウェアおよびグレーウェアの種類を指定するには

1. 左側のメニューで [POP3] → [スパイウェア対策] の順に選択し、[対象] タブを選択します。
2. [検索するスパイウェア / グレーウェア] で、POP3 サービスで検索するスパイウェアとグレーウェアの種類を指定します。
3. [保存] をクリックします。

スパイウェア検出時に実行する処理を指定する

スパイウェアなどのグレーウェアの検出時に InterScan VirusWall が実行する処理を、3 つの処理の中から 1 つ選択できます (図 7-8 を参照)。



図 7-8. [POP3] → [スパイウェア対策] → [処理] タブ

スパイウェア / グレーウェアの検出時に実行する処理を指定するには

1. 左側のメニューで [POP3] → [スパイウェア対策] の順に選択し、[処理] タブを選択します。
2. [スパイウェア / グレーウェアを含むメッセージの処理] で、必要なオプションを選択します。

- 添付ファイルを隔離して、メッセージを配信するには、[スパイウェア / グレーウェアを隔離して配信] を選択します。ユーザは添付ファイルのないメッセージを受信します。添付ファイルは隔離フォルダに保存されます。
 - 検出された添付ファイルを削除して、メッセージを配信するには、[スパイウェア / グレーウェアを削除して配信] を選択します。ユーザは添付ファイルのないメッセージを受信します。
 - 検出された添付ファイルと一緒にメッセージを配信するには、[そのまま配信 (推奨しません)] を選択します。
3. [保存] をクリックします。

スパイウェア検出時の通知を指定する

受信メッセージまたは送信メッセージでスパイウェアなどのグレーウェアが検出された場合に、受信者、および管理者に通知を送信するかどうかを指定できます。

InterScan VirusWall によるスパイウェアまたはグレーウェア検出時の通知設定を指定するには

- 左側のメニューで [POP3] → [スパイウェア対策] の順に選択し、[通知] タブを選択します。
- スパイウェアまたはグレーウェアの検出時に送信される通知の受信者を選択します。
- 各受信者に送信するメッセージを作成します。メッセージ内に次の任意のタグを使用します。

タグ	説明
%SENDER%	送信者アドレス
%RCPTS%	受信者アドレス
%SUBJECT%	メールの件名
%HEADERS%	メールヘッダ
%DATETIME%	検索日時
%MAILID%	メールメッセージ ID
%PROTOCOL%	メールプロトコル
%FILTERNAME%	処理を実行するフィルタの名前
%DETECTED%	検出されたセキュリティリスクの名前
%FINALACTION%	メッセージに対して実行された処理
%QUARANTINE_AREA%	隔離場所
%MACHINENAME%	InterScan VirusWall コンピュータのホスト名

4. [保存] をクリックします。

POP3 コンテンツフィルタ

InterScan VirusWall には、POP3 用のメールコンテンツフィルタが用意されています。この機能は、POP3 を使用してネットワーク上で送受信される情報の監視および管理をリアルタイムに実行します。

POP3 コンテンツフィルタを有効にする

POP3 コンテンツフィルタを有効にすると、POP3 を介してネットワーク上で送受信されるすべての情報で、POP3 トラフィックのコンテンツフィルタ用に定義したポリシーと一致するものが検索されます。[ポリシー] には、コンテンツフィルタ用に定義されているすべてのポリシーが一覧表示されます。

POP3 コンテンツフィルタを有効にするには

1. 左側のメニューで [POP3] → [コンテンツフィルタ] の順に選択します。
2. [コンテンツフィルタ設定] で、[POP3 コンテンツ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。

POP3 コンテンツフィルタを無効にする

POP3 コンテンツフィルタを無効にすると、POP3 トラフィックのコンテンツが監視されなくなります。有効化されている他の POP3 検索機能は、指定されたとおりに引き続き機能します。

POP3 コンテンツフィルタを無効にするには

1. 左側のメニューで [POP3] → [コンテンツフィルタ] の順に選択します。
2. [コンテンツフィルタ設定] で、[POP3 コンテンツフィルタを有効にする] チェックボックスをオフにします。
3. [保存] をクリックします。

ポリシーを作成する

InterScan VirusWall では、キーワードフィルタまたは添付ファイルフィルタを使用できるポリシーを使用します。

ポリシーを作成するには

ポリシーを作成するには、[キーワードフィルタの追加] または [添付ファイルフィルタの追加] をクリックします。

キーワードに基づいた POP3 コンテンツフィルタポリシーを作成する

キーワードフィルタを使用すると、InterScan VirusWall の管理者は、メールメッセージの配信をメッセージの内容自体に基づいて評価し、制御できます。キーワードフィルタを使用すれば、受信メッセージと送信メッセージの両方を監視して、機密扱いまたは不快なコンテンツの有無をチェックできます。キーワードフィルタでは、ポリシーの対象範囲を拡大する類義語チェック機能も利用できます。キーワードフィルタは、中国語や日本語によるメッセージなど、2 バイト文字によるコンテンツ検索をサポートしています。

キーワードリスト

所定のキーワードフィルタのキーワードリストには、メッセージ内容に対してフィルタで照合される語句が含まれます。複数のキーワードをポリシーの同一行に指定すると、その行のキーワードすべてが評価対象のメッセージに含まれている場合にのみ一致と見なされます。たとえば、次のキーワードをリストで使用できます。

例 1:

resume, position

resume, job

resume, experience

resume, enclosed

この例では、「resume」という単語が単一エントリとして 1 回だけ使用されるのではなく、追加の単語とともに 4 回使用されています。resume だけを使用すると、信頼できない結果が生じる可能性があります。これは、resume という単語に「履歴書」と「再開する」の両方の意味があるためです。こうした誤った一致が生じる可能性を最小限に抑えるには、最初の語と一般的に関連する語を追加して最初の語を限定すると効果的です。この例では、求職文書で使われることが多い enclosed (同封の)、position (職)、job (仕事)、experience (経験) などの単語が使用されています。複数のキーワードグループを指定すると、フィルタの対象範囲が増大します。

この例の設定では、いずれかのキーワードペアを含むメッセージが一致と見なされます。

または、1 つの送信メッセージで 5 つの単語全部が検出された場合にのみ、設定した処理を開始させることもできます。これを実行するには、1 行にすべてのキーワードを指定します。

例 2:

Resume, position, job, experience, enclosed

例 1 で示した「resume」に基づく複数のルールセットで構成されたポリシーと比べると、このフィルタに基づいてすべての resume が送信メッセージで検出される可能性は明らかに低下します。

例 3 に、例 2 の 4 つの単語のいずれかが検出されると一致と見なされるポリシーを示します。

例 3:

job

resume

enclosed

position

experience

一般に、AND 演算子で結合するキーワード数は 4 ～ 5 語以内にします。そうしないと、ポリシーが過度に制限されるおそれがあります。一方、特定の行に 1 つのキーワードしか指定しない場合 (OR 演算子) は、ポリシーの許容範囲が広くなりすぎて、一致として検出されるメールメッセージの数が非常に多くなります。当然ですが、前述のとおり、これはフィルタ処理の対象にも大きく依存します。

指定する条件は、スペースや句読点を含めて入力したとおりに評価されます。カンマで区切られた句は、1 つの単位として扱われます。その句のそれぞれの語やスペースなどが入力した順序でメッセージに出現する場合にのみ一致が発生します。

キーワードリストの演算子

キーワード、およびキーワードの位置に基づいてキーワードに適用される論理演算子について、次に例を示します。

表 7-7. 論理演算子で示すキーワードリストと一致結果の例

ケース	結果
以下の例にあるブラケット [...] で囲まれた項目は、例示目的のみで示したものであり、キーワードリスト作成時には含めないようにしてください。	
ケース 1: 複数のキーワードを 1 行で指定 例 : Apple Juice, [AND] Pear, [AND] Orange 論理演算子「AND」と同じ機能を提供します。	「Apple Juice」(リンゴジュース)、「Pear」(ナシ)、「Orange」(オレンジ) のアイテムすべてを含むメッセージだけが一致と見なされます。その際、メッセージテキスト内の順序と場所は問われません。
ケース 2: 複数のキーワードを個別の行で指定 例 : Apple Juice [OR] Pear [OR] Orange 論理演算子「OR」と同じ機能を提供します。	「Apple Juice」を含むすべてのメッセージ、「Pear」を含むすべてのメッセージ、および「Orange」を含むすべてのメッセージがそれぞれ一致と見なされます。
ケース 3: 複数のキーワードを 1 行で指定し、類義語チェックを「Orange」に対して有効化 例 : Apple Juice, [AND] Pear, [AND] Orange (* 類義語リストにある「orangish」(オレンジがかった)、「red」(赤)、「yellow」(黄) の各語は、「Orange」(オレンジ色) と意味が似ています)。 論理演算子「AND」および「OR」と同じ機能を提供します。	類義語チェックを有効にすると、「Apple Juice」、「Pear」、および「Orange」、「orangish」、「red」、「yellow」のいずれかの語を含むメッセージが一致と見なされます。

その他のキーワードについて

Apple Juice は 1 つの語句と見なされます。これは、Apple と Juice の各語がカンマで区切られていないためです。Apple と Juice の両方の語がメッセージ内で使用されていても、Apple Juice のように一緒に使用されていない限り、一致は発生しません。

類義語の大文字 / 小文字および完全一致の属性は、キーワード自体に対して定義された属性と一致します。つまり、完全一致がオフのときに類義語リストで「red」が指定されている場合は、「Red」でも一致が発生します。同様に、大文字 / 小文字の区別がオフのときにメッセージテキスト内に「Red」がある場合は、「red」で一致が発生します。

カンマで区切られた単一行に複数のキーワードを追加すると、その行にあるすべてのキーワードがメールの同じ箇所で使用されている場合にのみポリシーがトリガされるようになります。たとえば、ユーザがキーワード「apple, pear」を追加し、apple がメッセージの件名で使用され、pear が本文で使用されている場合、ポリシーはトリガされません。

キーワードフィルタに基づいたポリシーを追加する

POP3 コンテンツのフィルタ基準としてキーワードを使用するポリシーを作成するには、[POP3 コンテンツフィルタ] → [キーワードフィルタ] → [対象] タブを使用してポリシールールを指定します。

キーワードフィルタに基づいたポリシーを追加するには

1. 左側のメニューで [POP3] → [コンテンツフィルタ] の順に選択します。
2. [ポリシー] で、[キーワードフィルタの追加] を選択します。
3. [キーワードフィルタ] 画面が表示されたら、[対象] タブを選択します。
4. [ポリシー名] ボックスにポリシー名を入力します。
5. [ポリシーステータス] で、[有効] を選択してポリシーを適用するか、ポリシーを適用しない場合は [無効] を選択します。
6. [メッセージのポリシーの適用先] で、選択したポリシーを適用するメッセージのセクションを選択します ([件名]、[本文]、または [添付ファイル])。
7. このポリシーで、添付ファイルを含めて指定したサイズより大きいメッセージをブロックする場合は、[メッセージサイズが次のサイズを超える場合にフィルタする] を選択し、サイズ制限を指定します。
8. [キーワード] に、メッセージ内で検索するキーワードを入力し、[追加] をクリックします。各キーワードの類義語を指定するには、[類義語] 列の下リンクをクリックします (初期設定は [なし] です)。

必要に応じて、[大文字 / 小文字の区別]、[完全一致]、[類義語] のいずれかを有効にします。

注意： ポリシーのキーワードリスト作成の詳細については、212 ページの「キーワードに基づいた POP3 コンテンツフィルタポリシーを作成する」を参照してください。

9. そのまま配信を許可すべきメッセージがブロックされる可能性を減らすには、[除外キーワード] にそのまま配信を許可するメッセージを識別するキーワードを入力します。キーワードフィルタに一致する語があった場合でも、[除外キーワード] に入力したキーワードを含むメッセージはポリシーによってブロックされることはありません。
10. [保存] をクリックします。

キーワードの類義語リストを変更する

InterScan VirusWall には、特定のキーワードの定義済みの類義語リストがあります。定義済みのリストの表示、およびキーワードの類義語としての単語の追加を実行するには、[類義語の編集] 画面を使用します。

定義済みの類義語リストに対する変更または追加は実行できません。

キーワードの類義語リストを変更するには

1. [キーワードフィルタ] → [対象] タブで、同義語を変更するキーワードの [類義語] 列の値を選択します。
2. メッセージボックスが表示されたら、[OK] をクリックして、[類義語の編集] 画面に進みます。
3. 複数のキーワードをカンマで区切って入力した場合は、ドロップダウンボックスにすべてのキーワードが表示されます。類義語を表示するキーワードを 1 つ選択します。
4. [類義語を除外する] 列の類義語のリストから、キーワードに使用する類義語を選択します。 < をクリックして、選択した類義語を [類義語を含む] 列に移動します。
5. [保存] をクリックします。

キーワードフィルタポリシーに一致するメッセージに対する処理を設定する

指定したフィルタ基準に POP3 メッセージが一致した場合、そのメッセージに対して、3 つの処理のうちの 1 つを実行できます。

コンテンツフィルタポリシーと一致するメッセージに対する処理を設定するには

1. 左側のメニューで [POP3] → [コンテンツフィルタ] の順に選択します。
2. [ポリシー] で、[キーワードフィルタの追加] を選択します。
3. [キーワードフィルタ] 画面が表示されたら、[処理] タブを選択します。
4. [フィルタ基準に一致したメッセージの処理] で、次のオプションのうちの 1 つを選択します。
 - メッセージを隔離するには、[隔離] を選択します。
 - メッセージを削除するには、[削除] を選択します。メッセージは配信されません。
 - メッセージを配信するには、[放置] を選択します。ユーザはメッセージを受信します。
5. [保存] をクリックします。

メッセージがフィルタ条件に一致した場合の通知設定を指定する

受信メールメッセージの添付ファイルで禁止コンテンツが検出されたことを知らせる通知を管理者と受信者に送信できます。

メッセージによってポリシーがトリガされた場合の通知設定を指定するには

1. 左側のメニューで [POP3] → [コンテンツフィルタ] の順に選択します。
2. [ポリシー] で、[キーワードフィルタの追加] を選択します。
3. [キーワードフィルタ] 画面が開いたら、[通知] タブを選択します。
4. 通知の受信者を選択します。
5. 各受信者に送信するメッセージを作成します。メッセージ内に次の任意のタグを使用できます。

タグ	説明
%SENDER%	送信者アドレス
%RCPTS%	受信者アドレス
%SUBJECT%	メールの件名
%HEADERS%	メールヘッダ
%DATETIME%	検索日時
%MAILID%	メールメッセージ ID
%PROTOCOL%	メールプロトコル
%FILTERNAME%	常に「コンテンツフィルタ」
%DETECTED%	トリガされたポリシーの名前
%FINALACTION%	実行された処理
%QUARANTINE_AREA%	隔離場所
%MACHINENAME%	InterScan VirusWall コンピュータのホスト名

6. [保存] をクリックします。

添付ファイルフィルタに基づいた POP3 コンテンツフィルタポリシーを作成する

POP3 コンテンツのフィルタ基準として添付ファイルまたはメッセージヘッダを使用するポリシーを作成するには、[POP3 コンテンツフィルタ] → [添付ファイルフィルタ] → [対象] タブを使用してポリシールールを指定します。

添付ファイルフィルタに基づいたポリシーを追加するには

1. 左側のメニューで [POP3] → [コンテンツフィルタ] の順に選択します。
2. [ポリシー] で、[添付ファイルフィルタの追加] を選択します。
3. [添付ファイルフィルタ] 画面が表示されたら、[対象] タブを選択します。
4. [ポリシー名] ボックスにポリシー名を入力します。
5. [ポリシーステータス] で、[有効] を選択してポリシーを適用するか、ポリシーを適用しない場合は [無効] を選択します。
6. このポリシーで、添付ファイルが指定したサイズより大きいメッセージをブロックする場合は、[添付ファイルサイズが次のサイズを超える場合にフィルタする] を選択し、サイズ制限を指定します。
7. [メッセージヘッダ] で、[From に次が含まれる]、[To に次が含まれる]、[Cc に次が含まれる]、[Reply-to に次が含まれる] など、メッセージヘッダ内の文字列が特定の条件に一致した場合にこのルールを適用するかどうかを指定できます。ヘッダ文字列に基づいてメッセージをブロックするかそのまま配信するかを選択します。

メッセージヘッダのテキストボックスに複数のエントリを指定できます。各エントリはカンマで区切ってください。たとえば、「user1@isvw.com,user2@isvw.com」のように入力します。

- 指定したヘッダ文字列に一致するメッセージヘッダに [添付ファイルの指定] の設定を適用するには、[メッセージヘッダが次の条件に一致する場合にルールを適用する] を選択します。
 - 指定したヘッダ文字列に一致しないメッセージヘッダに [添付ファイルの指定] の設定を適用するには、[メッセージヘッダが次の条件に一致する場合にルールを適用しない] を選択します。
8. ヘッダルールを指定します。
 9. [添付ファイルの指定] で、メッセージ添付ファイルのフィルタ条件を選択します。
 - **ファイル名**: ファイル名またはワイルドカード (*) を使用した文字列を指定します。ここで指定した名前または文字列に一致するファイル名を持つすべての添付ファイルがフィルタされます。
 - **MIME タイプ**: フィルタする MIME タイプを指定します。
 - **添付ファイルタイプ**: ブロックするファイルタイプのカテゴリを指定します。ここで指定したファイルタイプカテゴリに属するすべての添付ファイルがブロックされます。

注意： [ファイル名] および [MIME タイプ] ボックスで複数のエントリを指定するには、各エントリをカンマで区切ります。たとえば、「*.jpg*.txt」や「text/plain,image/jpeg」のように指定します。

10. [保存] をクリックします。

POP3 コンテンツフィルタポリシーの処理を設定する

指定したフィルタ基準に POP3 メッセージが一致した場合、そのメッセージに対して、3 つの処理のうちの 1 つを実行できます。

添付ファイルのポリシーと一致するメッセージに対する処理を設定するには

1. 左側のメニューで [POP3] → [コンテンツフィルタ] の順に選択します。
2. [ポリシー] で、[添付ファイルフィルタの追加] を選択します。
3. [添付ファイルフィルタ] 画面が表示されたら、[処理] タブを選択します。
4. [フィルタ基準に一致したメッセージの処理] で、次のオプションのうちの 1 つを選択します。
 - メッセージを隔離するには、[隔離] を選択します。
 - メッセージを配信するには、[放置] を選択します。ユーザはメッセージを受信します。
 - 添付ファイルを削除するには、[添付ファイルを削除して配信] を選択します。ユーザは添付ファイルのないメッセージを受信します。
5. メッセージの本文に通知を挿入するには、[次の通知をメッセージに挿入する] を選択します。挿入するメッセージのテキストは変更できます。また、次の任意のタグを使用できます。
 - %FILENAME%: 削除された添付ファイルの名前
 - %RULENAME%: ポリシーの名前
6. [保存] をクリックします。

メッセージの添付ファイルがフィルタ条件に一致した場合の通知設定を指定する

受信メールメッセージの添付ファイル内に禁止されたコンテンツが検出された場合に、管理者または受信者に通知できます。

メッセージによってポリシーがトリガされた場合の通知設定を指定するには

1. 左側のメニューで [POP3] → [コンテンツフィルタ] の順に選択します。
2. [ポリシー] で、[添付ファイルフィルタの追加] を選択します。
3. [添付ファイルフィルタ] 画面が開いたら、[通知] タブを選択します。

4. 通知の受信者を選択します。
5. 各受信者に送信するメッセージを作成します。メッセージ内に次の任意のタグを使用できます。

タグ	説明
%SENDER%	送信者アドレス
%RCPTS%	受信者アドレス
%SUBJECT%	メールの件名
%HEADERS%	メールヘッダ
%DATETIME%	検索日時
%MAILID%	メールメッセージ ID
%PROTOCOL%	メールプロトコル
%FILTERNAME%	常に「コンテンツフィルタ」
%DETECTED%	トリガされたポリシーの名前
%FINALACTION%	実行された処理
%QUARANTINE_AREA%	隔離場所
%MACHINENAME%	InterScan VirusWall コンピュータのホスト名

6. [保存] をクリックします。

POP3 コンテンツフィルタポリシーをコピーまたは削除する

既存の POP3 コンテンツフィルタポリシーをコピーして変更するか、または不要になったポリシーを削除するには

1. 左側のメニューで [POP3] → [コンテンツフィルタ] の順に選択します。
2. [ポリシー] で、ポリシーを選択して [コピー] または [削除] をクリックします。
3. ポップアップメッセージボックスで [OK] をクリックして変更を確定します。

POP3 設定

InterScan VirusWall の POP3 サービスを設定するには、これを有効にしておく必要があります。
[POP3 設定] 画面にアクセスするには、左側のメニューで [POP3] → [設定] を選択します。

[POP3 設定] 画面では、次の内容を設定できます。

- ドロップダウンリストから POP3 IP アドレスを選択するか、またはサーバに関連付けられているすべての IP アドレスにバインドする場合は [すべてのインタフェース] を選択します。
- 同時エンドユーザメールクライアント接続の最大数を設定します。
- POP3 メールサーバ接続を指定します。
- 特定の POP3 サーバのポートを InterScan VirusWall の待機ポートにマップします。

POP3 IP アドレスを指定する

バインドおよび待機するよう InterScan VirusWall の POP3 サービスを設定する IP アドレスを [IP] ドロップダウンリストから指定します。

- [すべてのインタフェース] を選択すると、InterScan VirusWall のインストール先コンピュータに割り当てられたすべての IP アドレスを待機するよう POP3 サービスが設定されます。
- [127.0.0.1] を選択すると、ローカルホストを待機するよう POP3 サービスが設定され、他のコンピュータからは POP3 サービスにアクセスできません。
- 特定の IP アドレスを選択して、他のコンピュータがこの IP アドレスを経由して POP3 サービスにアクセスできるように設定することもできます。

同時接続の最大数を設定する

許可される同時クライアント接続の最大数を指定するには、テキストボックスに 1 ～ 100 の整数値を入力します。

POP3 接続を指定する

InterScan VirusWall の POP3 サービスは、2 種類の POP3 接続をサポートしています。通常は、[ユーザのメールクライアントから要求されたすべての POP3 サーバに接続する] を選択し、ポートを POP3 サービスに割り当てます。

POP3 ポートマッピング

InterScan VirusWall がポートマッピングサーバとして動作する場合、特定の POP3 サーバのポートを InterScan VirusWall の待機ポートにマップします。

サーバがセキュリティで保護されたパスワード認証をサポートしており、セキュリティで保護されたパスワード認証を使用する場合は、ポートマッピングモードを使用する必要があります。

特定の POP3 サーバのポートを InterScan VirusWall の待機ポートにマップするには

1. [指定された POP3 サーバに接続する (安全なパスワード認証)] チェックボックスをオンにし、項目を追加します。
2. 各項目に対して、次の項目を指定します。
 - ・ **インバウンド POP3 ポート** : InterScan VirusWall の POP3 サービスが待機するポート
 - ・ **IP アドレス** : 特定の POP3 サーバのアドレス
 - ・ **POP3 サーバポート** : サーバが POP3 に使用するポート
3. [追加] をクリックして、右側のリストに各項目を追加します。特定の項目を削除するには、ごみ箱アイコンをクリックします。
4. [保存] をクリックして変更内容を確定します。

注意： 指定されたポートが使用されていると、InterScan VirusWall の POP3 サービスで、そのポートをバインドおよび待機できなくなるため、指定した IP アドレスとポートを他のプログラムが使用するのを許可しないでください。

Outlook Express を設定する

エンドユーザメールクライアントとして Outlook Express を設定するには

1. Outlook Express で [ツール] → [アカウント] の順にクリックします。[インターネット アカウント] 画面が表示されます。
2. [追加] → [メール] の順にクリックします。インターネット接続ウィザードが起動します。
3. インターネット接続ウィザードの [名前] 画面でユーザ名 (例: John Smith) を入力します。[次へ] をクリックします。
4. [インターネット電子メール アドレス] 画面でユーザのメールアドレスを入力します (例: John_Smith@anycompany.com)。[次へ] をクリックします。[電子メール サーバー名] 画面が表示されます。
5. [受信メール サーバーの種類] で [POP3] を選択します。
6. [受信メール (POP3、IMAP または HTTP) サーバー] に InterScan VirusWall サーバのアドレス (例: 192.168.5.139) を入力します。

-
7. [送信メール (SMTP) サーバー] に InterScan VirusWall サーバのアドレスを入力します。[次へ] をクリックします。
 8. セキュリティで保護されたパスワード認証を POP3 サーバで必要としない場合：
 - a. [インターネット メール ログオン] 画面で、POP3 メールの取得に使用するアカウント名を [アカウント名] に入力します。この書式は、名前、ポンド記号 (#)、POP3 サーバ名、それに続くポンド記号とポート番号 (110 でない場合) の順序で構成されます。次に例を示します。
`someusername#pop3.earthlink.net`
`someusername#pop3.earthlink.net#111`
 - b. ユーザの POP3 メールアカウントのパスワードを入力します。該当する場合は、[パスワードを保存する] にチェックマークを付けます。セキュリティで保護されたパスワード認証を POP3 サーバで必要とする場合：
 - a. [インターネット メール ログオン] 画面で、POP3 メールの取得に使用するアカウント名を [アカウント名] に入力します。
 - b. [セキュリティで保護されたパスワード認証 (SPA) を使用する] を選択します。
 - c. [次へ] をクリックします。
 9. [完了] 画面で [完了] をクリックします。[インターネット アカウント] 画面をもう一度開くと、POP3 接続が表示されます。
-

注意： セキュリティで保護されたパスワード認証では、対応する項目 (受信ポート、サーバ、ポート) を InterScan VirusWall の [POP3 設定] 画面で設定する必要があります。図 7-9 に示すように、メールクライアントの POP3 ポートの初期設定を特定の項目の「受信ポート」に変更しなければならないこともあります。

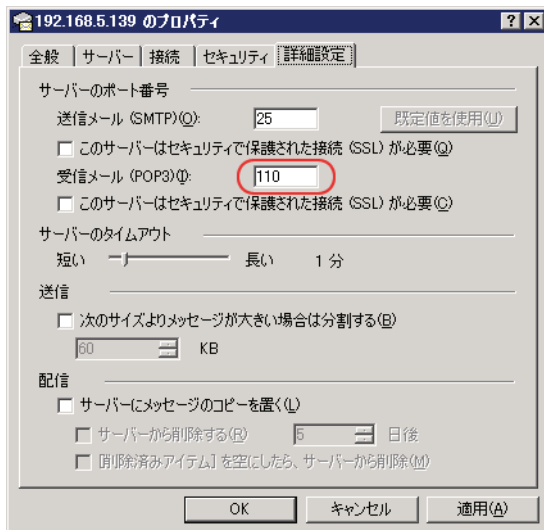


図 7-9. 【詳細設定】タブ

POP3 トランザクションログを有効にする

InterScan VirusWall では現在、POP3 のトランザクションログがサポートされています。POP3 のトランザクションログは、初期設定で有効になっています。

POP3 トランザクションログを有効または無効にするには

1. Config.xml ファイルを開きます。
2. 「POP3」の下にある「WriteConnectionMsg」という名前のキーを探します。
3. 「WriteConnectionMsg」の値を「1」(有効) または「0」(無効) に設定します。
4. サービスを再起動します。

大規模感染予防サービス

大規模感染予防サービスとは、最新のパターンファイルでも未対応の新たなウイルスによる広範囲の感染が報告された際に、ウイルスの蔓延からネットワークを保護するための予防策を実施するサービスです。大規模感染予防サービスには、大規模感染予防ポリシーを有効にするタイミングや、ポリシーの有効期間など、管理者が使用できる自動配信オプションがあります。

大規模感染予防ポリシーは、ポリシー内で設定された発効日および失効日に応じて、アクティベートされます。大規模感染予防サービスが有効になっており、トレンドマイクロが発行した大規模感染予防ポリシーにおいて現在のシステム時間より後に失効日が設定されている場合、ポリシーは有効になります。トレンドマイクロはポリシーの期間を指定しますが、ユーザは必要に応じて手動でその期間を上書きできます。

POP3、SMTP、HTTP、および FTP サービスの大規模感染予防ポリシーを受け取るには、対応する大規模感染予防ポリシーを有効にするためにこれらのサービスを有効にしておく必要があります。

大規模感染予防サービスを有効にする

大規模感染予防サービスを有効にして詳細なステータス情報を表示するには

1. 左側のメニューで [大規模感染予防] → [ステータス] の順に選択します。
2. [大規模感染予防サービスを有効にする] 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。

大規模感染予防サービスが有効になっているかどうかを確認するには

1. 左側のメニューで [概要] を選択してから、[ステータス] タブを選択します。
2. 必要に応じて、右のアイコンをクリックして大規模感染予防サービス情報を展開し、サービスのステータスを確認できます。

図 8-1 に、大規模感染予防サービスに関する情報が表示された [概要] → [ステータス] タブの例を示します。

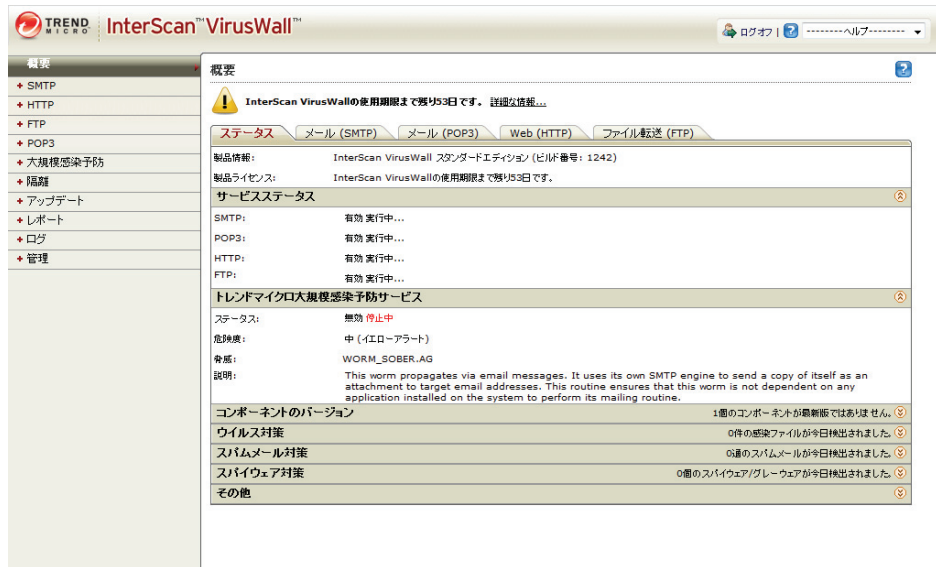


図 8-1. [概要] → [ステータス] タブ

表示可能な現在のステータス

トレンドマイクロが大規模感染予防ポリシーを発行および管理しているため、ユーザはこの画面の残りの情報を表示できますが変更はできません。

- [脅威のステータス] には、現在の脅威のステータスが表示されます。
- [添付ファイルフィルタ] には、POP3/SMTP サービス経由でブロックされたメールメッセージ内のファイルの種類が一覧表示されます。
 - ◆ [ブロックするファイル名] では、ファイルの拡張子だけが照合されます (* ワイルドカードは、拡張子ではなく名前にのみ使用できます)。

- ◆ [ブロックするファイルタイプ] では、実際のファイルコンテンツから実際のファイルタイプが検出され、タイプによってブロックされます。ここに表示される数は、InterScan VirusWall の内部ファイルタイプ表現です。
- [コンテンツフィルタ] には、大規模感染予防サービスが POP3/SMTP サービス経由でブロックしているメールメッセージコンテンツが表示されます。これは、メールの添付ファイル名の正規表現フィルタです。ワイルドカード文字「*」および「?」を、表現の中で使用できます。
- [URL ブロック] には、大規模感染予防サービスが HTTP サービス経由でブロックしている URL が一覧表示されます。
- [ファイルブロック] には、大規模感染予防サービスが HTTP および FTP サービス経由でブロックしているファイルタイプが表示されます。

大規模感染予防サービスを設定する

トレンドマイクロでは大規模感染予防ポリシーの失効日を指定しますが、ユーザは時間を手動で変更できます。

大規模感染予防サービスを設定するには

1. 左側のメニューで、[大規模感染予防] → [設定] の順に選択します。
2. [大規模感染予防サービスの有効期限] で、大規模感染予防サービスの警告を無効にするまでの日数を指定します。日数は、大規模感染予防ポリシーの発行日に基づいています。
3. ポリシーのダウンロード設定を予約するには、[ポリシーの予約ダウンロード設定] チェックボックスをオンにし、大規模感染予防ポリシーのダウンロードの頻度 (分単位) を選択します。
4. [保存] をクリックします。

注意： InterScan VirusWall で新しい大規模感染予防ポリシーがダウンロードされ有効になると、この設定は上書きされます。大規模感染予防ポリシーの有効期間を手動で管理するには、個別の大規模感染予防ポリシーそれぞれについて失効までの期間を変更します。

隔離

Trend Micro InterScan VirusWall スタンダードエディション（以下、InterScan VirusWall）がセキュリティリスクを検出したときにファイルやメールメッセージを隔離するように指定した場合は、すべての感染ファイルが隔離ディレクトリに移動されます。InterScan VirusWall では、プロトコルごとに個別の隔離ディレクトリが使用されます。

InterScan VirusWall の隔離機能を使用すると、次の操作を実行できます。

- SMTP/POP3 の隔離ディレクトリに検索を実行して、これらのディレクトリ内のファイルに関する情報を取得します。
- SMTP、HTTP、FTP、および POP3 の隔離フォルダのディレクトリパスを指定します。
- 隔離ディレクトリ内のファイルを自動的に削除するか、必要に応じて手動で削除するかを指定します。

隔離クエリ

InterScan VirusWall のクエリ機能を使用すると、SMTP および POP3 プロトコルについて、隔離されたファイルのタイプおよびファイルが隔離された理由に関するレポートを生成できます。たとえば、2 週間の間に特定のメールアドレスで受信されたすべてのスパムメールメッセージに関するレポートを生成する条件を指定できます。

注意： クエリは、SMTP および POP3 隔離フォルダに現在格納されているファイルに対してのみ実行できます。これらのフォルダを削除した場合は、削除されたファイルに関する情報は取得できません。

クエリを生成する

隔離された SMTP/POP3 メールメッセージおよび添付ファイルの詳細を表示するには、クエリ条件を指定して結果を表示します。図 9-1 に、クエリ条件を指定できる [隔離クエリ] 画面を示します。

隔離クエリ 

条件	
日時:	年月日 (yyyy/mm/dd) 時 分 年月日 (yyyy/mm/dd) 時 分 2007/02/14 14 55 から 2007/02/21 11 39
タイプ:	メールメッセージとファイル
原因:	☒ すべての原因: ☐ 特定の原因: ☒ ウイルス検索 ☒ コンテンツフィルタ ☒ IntelliTrap ☒ スパイウェア/グレーウェア ☒ スпамメール ☒ フィッシング
送信者:	
受信者:	
件名:	
添付ファイル:	
ログ表示:	日時
1ページあたりの件数:	10
検索	
クエリ結果	
移動 削除 再送信 検索および再送信 ☐ 合計0件 0-0 / 0 14 4 11	
☐ 日時 ▲ 送信者 受信者 件名 原因 プロトコル	
移動 削除 再送信 検索および再送信 ☐ 合計0件 0-0 / 0 14 4 11	

図 9-1. [隔離クエリ] 画面

クエリを生成するには

1. 左側のメニューから [隔離] → [クエリ] の順に選択します。
2. クエリ条件を指定します。
 - ・ **日時**: 表示する日時の範囲を入力します。

- ・ **タイプ**: 隔離されたメールメッセージとファイルの両方をクエリするのか、どちらかをクエリするのかを選択します。
- ・ **原因**: 隔離の理由として [すべての原因] または [特定の原因] を選択します。[特定の原因] の場合は、[ウイルス / 不正プログラム]、[スパイウェア / グレーウェア]、[コンテンツフィルタ]、[スパムメール]、[IntelliTrap]、および [フィッシング] のうち該当するチェックボックスをオンにします。
- ・ **送信者**: メールメッセージの [送信者] フィールドに含まれているキーワードを入力します。
- ・ **受信者**: メールメッセージの [受信者] フィールドに含まれているキーワードを入力します。
- ・ **件名**: メールメッセージの [件名] フィールドに含まれているキーワードを入力します。
- ・ **添付ファイル**: 添付ファイルのファイル名に含まれているキーワードを入力します。
- ・ **ソートの種類**: クエリ結果のソート条件として、[日時]、[送信者]、[受信者]、[件名]、または [理由] を選択します。
- ・ **1 ページあたりの件数**: 1 ~ 100 の数値を入力して、1 つの画面に表示する項目数を指定します。

3. [検索] をクリックして結果を表示します。

クエリ結果を操作する

クエリ結果を再ソートするには、クエリ結果テーブルの列ヘッダをクリックします。

アイテムを移動または削除するには、1 つ以上の対応するチェックボックスをオンにして、[移動] または [削除] をクリックします。

[移動] をクリックすると、[隔離アイテムの移動] 画面が開きます。アイテムの移動先のディレクトリを指定して、[移動] をクリックします。

隔離された SMTP メールメッセージを再送信、または検索して再送信するには、対応するチェックボックスを選択して、[再送信] または [検索および再送信] をクリックします。

[再送信] をクリックした場合、隔離された SMTP メールメッセージの最初の受信者への送信が試行されます。[検索および再送信] をクリックした場合、隔離された SMTP メールメッセージの選択されたメッセージが検索されます。その後、脅威が検出されなければ、最初の受信者にその項目が送信されます。

注意： 再送信、および、検索して再送信の処理は、実行に時間がかかることがあります。その時間は、選択された項目の数、ネットワーク速度、InterScan VirusWall サーバの処理能力、およびその他の多数の要因に依存します。

隔離ディレクトリの設定

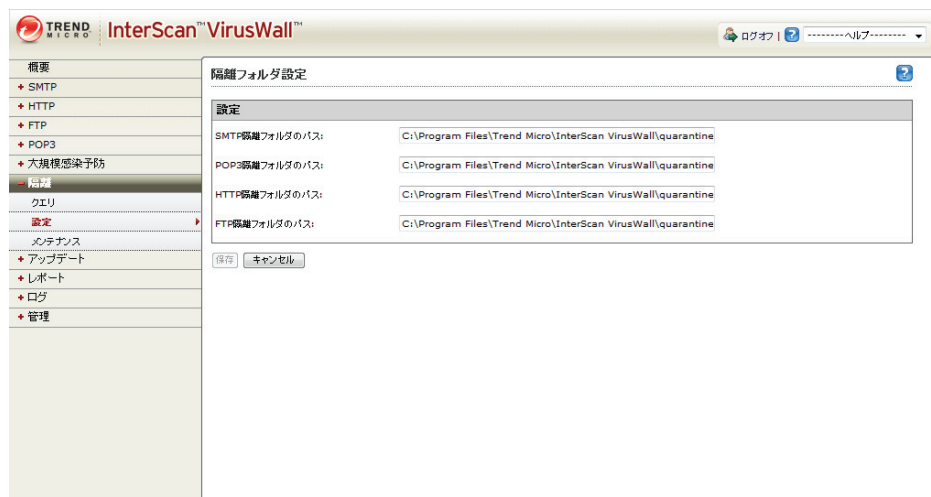
初期設定では、InterScan VirusWall では次のようにプロトコルごとに個別の隔離ディレクトリが作成されます。

- %quarantine%smtp
- %quarantine%http
- %quarantine%ftp
- %quarantine%pop3

これらとは異なる隔離フォルダを指定するには、隔離フォルダ設定機能を使用します。絶対パスが必要です。また、プロトコルごとに異なるパスを指定する必要があります。

図 9-2 に示している [隔離フォルダ設定] 画面では、隔離ファイルが格納される初期設定のディレクトリパスを変更できます。

図 9-2. [隔離フォルダ設定] 画面



SMTP 検索、POP3 検索、HTTP 検索、または FTP 検索用の隔離ディレクトリを変更するには

1. 左側のメニューで [隔離] → [設定] の順に選択します。
2. 隔離ディレクトリを変更する各プロトコルの絶対パスを入力します。
各プロトコルには、それぞれの隔離アイテム用に個別のフォルダが必要です。
3. [保存] をクリックします。

隔離ディレクトリの管理

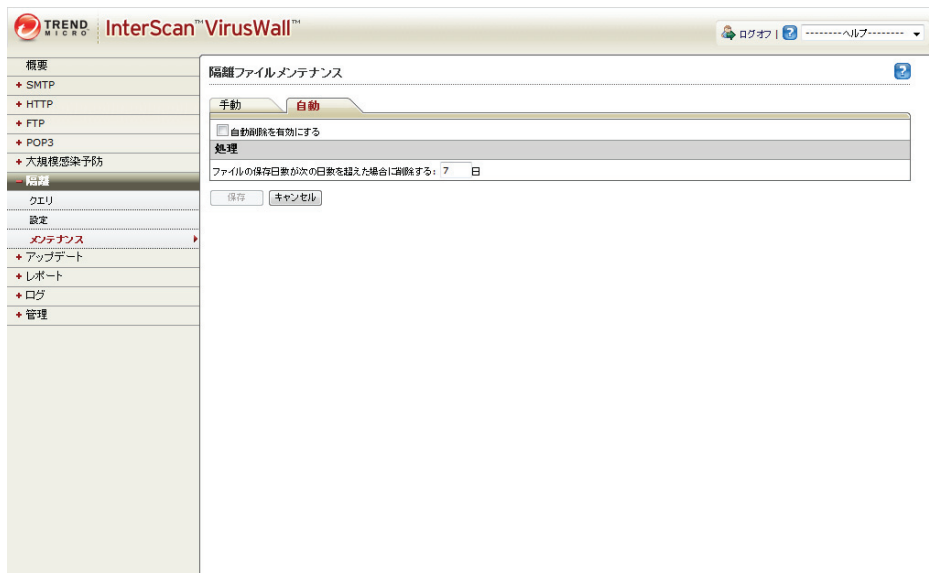
大量の不要なファイルが蓄積することを避けるために、隔離ディレクトリ内のファイルを定期的に削除する必要があります。InterScan VirusWall では、隔離ディレクトリの定期メンテナンスを予約できます。隔離ファイルを削除する頻度として、任意の間隔を日単位で最大 360 日間に 1 回の頻度で指定できます。

隔離ファイルを手動で削除することもできます。指定した期間を超えてフォルダに格納されているファイルは、InterScan VirusWall によってすべて自動的に削除されます。

自動メンテナンス

隔離フォルダ内のファイルを削除するための自動メンテナンスを予約するには、図 9-3 に示す自動隔離メンテナンス機能を使用します。

図 9-3. [隔離] → [メンテナンス] → [自動] タブ



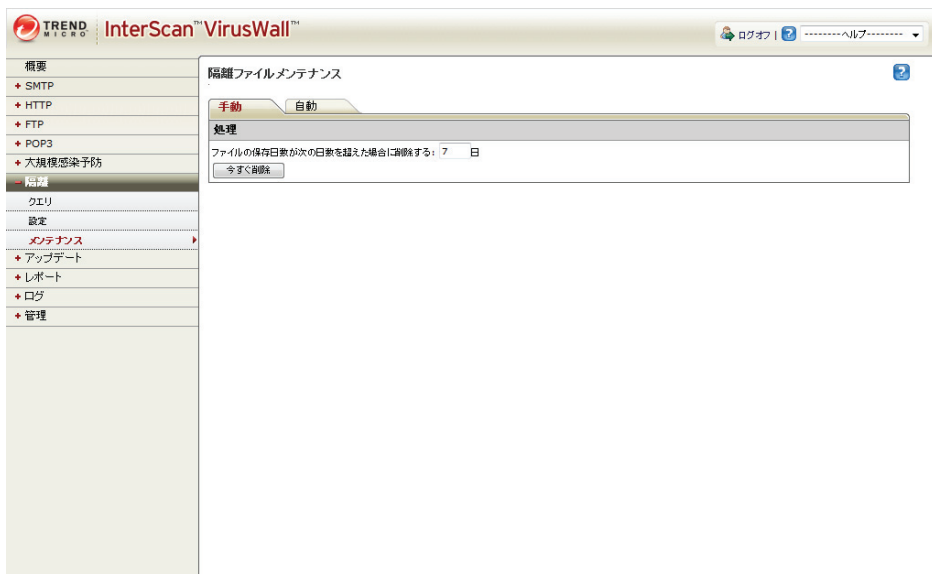
隔離ファイルの自動削除を予約するには

1. 左側のメニューで [隔離] → [メンテナンス] の順に選択します。
2. [自動] タブを選択します。
3. [自動削除を有効にする] チェックボックスをオンにします。
4. テキストボックスに有効期間を日単位で入力します (0 ~ 360 の範囲)。
SMTP、POP3、HTTP、または FTP を使用して受信されたメールメッセージ、添付ファイル、およびファイルなど、この期間より長く隔離されているすべてのファイルが削除されます。
5. [保存] をクリックします。

手動メンテナンス

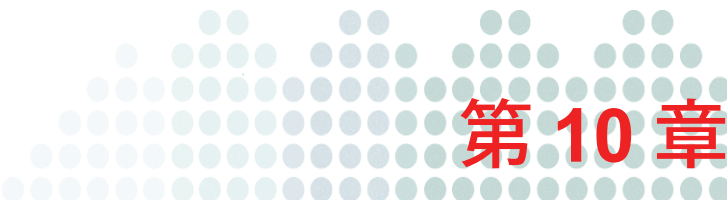
隔離フォルダ内のファイルを手動で削除するには、図 9-4 に示す手動隔離メンテナンス機能を使用します。

図 9-4. [隔離] → [メンテナンス] → [手動] タブ



手動で隔離ファイルを削除するには

1. 左側のメニューで [隔離] → [メンテナンス] の順に選択します。
2. [手動] タブを選択します。
3. テキストボックスに有効期間を日単位で入力します (0 ～ 360 の範囲)。
SMTP、POP3、HTTP、または FTP を使用して受信されたメールメッセージ、添付ファイル、およびファイルなど、この期間より長く隔離されているすべてのファイルが削除されます。
4. [今すぐ削除] をクリックします。



第10章

アップデート

新たな不正プログラムや不快な Web サイトは日々開発されているため、最新のパターンファイル、検索エンジン、および URL フィルタデータベースによって、使用しているソフトウェアを常にアップデートすることが不可欠です。

トレンドマイクロが提供する自動アップデートを使用すると、お使いのコンピュータに、セキュリティの脅威に対する最新の保護機能を確実に組み込むことができます。アップデートは、多くのトレンドマイクロ製品に共通のサービスです。アップデートは、トレンドマイクロのインターネットアップデートサーバに接続して、パターンファイル、検索エンジン、および URL フィルタデータベースをダウンロードします。

アップデートは、ネットワークサービスを中断することも、コンピュータの再起動を必要とすることもありません。アップデートは、設定した定期的な間隔に従って実行することも、必要に応じて適宜実行することもできます。

Trend Micro InterScan VirusWall スタンダードエディション（以下、InterScan VirusWall）では、アップデートサーバに直接ポーリングして、アップデートされたコンポーネントがないか確認できます。これらのアップデートされたコンポーネントは、次のような単位で定義したスケジュールに従って InterScan VirusWall に配信されます。

- 分
- 時間
- 日
- 曜日

アップデートに対応したコンポーネント

InterScan VirusWall の次のコンポーネントに対して定期的な自動アップデートを予約することも、これらのコンポーネントを手動でアップデートすることもできます。特定のコンポーネントを前のバージョンにロールバックすることもできます。

コンポーネント	説明
ウイルスパターンファイル	既知のセキュリティリスクのバイナリ「シグネチャ」またはパターンが含まれたファイルです。検索エンジンと組み合わせて使用すると、InterScan VirusWall は、既知のリスクがインターネットゲートウェイを通過する際にこれらのリスクを検出できます。新しいウイルスパターンファイルは通常、一週間に数回の頻度でリリースされます。
ウイルス検索エンジン (32 ビット)	各ファイルのバイナリパターンを分析して、パターンファイル内のバイナリ情報と比較するためのモジュールです。一致する場合、そのファイルは不正と見なされます。
IntelliTrap パターンファイル /IntelliTrap 除外パターンファイル	既知のウイルスのバイナリ「シグネチャ」またはパターンが含まれたファイルであり、16 種類の一般的な圧縮方式のいずれかを使用して最大で 20 階層に圧縮されたファイルとして提供されます。IntelliTrap のパターンファイルは、新しい脅威情報が入手されるたびにアップデートされます。
スパイウェア監視パターンファイル	既知のスパイウェア / グレーウェアセキュリティリスクのバイナリ「シグネチャ」またはパターンが含まれたファイルです。検索エンジンと組み合わせて使用すると、InterScan VirusWall は、既知のリスクがインターネットゲートウェイを通過する際にこれらのリスクを検出できます。スパイウェア監視パターンファイルは、新しい脅威情報が入手されるたびにアップデートされます。
フィッシングパターンファイル	既知のフィッシングサイトセキュリティリスクのバイナリ「シグネチャ」またはパターンが含まれたファイルです。検索エンジンと組み合わせて使用すると、InterScan VirusWall は、既知のリスクがインターネットゲートウェイを通過する際にこれらのリスクを検出できます。フィッシングパターンファイルは、新しい脅威情報が入手されるたびにアップデートされます。
スパムメール判定ルール / スパムメール検索エンジン	メッセージまたは添付ファイルの内容を分析して、事前定義されたスパムメールのカテゴリ、初期設定の検出レベル、および承認された送信者とブロックされた送信者のリストと比較するためのモジュールです。

トレンドマイクロ製品によるセキュリティの脅威の検出方法

検索エンジンは、ウイルスパターンファイルと連動し、パターンマッチングと呼ばれるプロセスを使用して第1段階の検出を実行します。各ウイルスには、他のコードと区別される証拠となる特徴である固有のバイナリ「シグネチャ」または文字列が含まれているため、TrendLabsのウイルス専門家は、このコードから単独では実行できない断片を取得してパターンファイルに組み込みます。次に、検索エンジンが、各検索対象ファイルの一定部分をウイルスパターンファイル内のデータと比較して、一致を探します。

パターンファイルには、lpt\$vpn.### という形式で名前が付けられ、### はパターンバージョン(400 など)を表します。パターンバージョンは同じでビルド番号が異なる特定のパターンファイルを区別するために、また 999 より大きいパターンバージョンに対応するために、InterScan VirusWall の Web コンソールには次の形式で表示されます。

ロール番号 . パターンバージョン . ビルド番号 (形式 : xxxxx.###.xx)

- ・ **ロール番号**は、パターンバージョンが 999 を超えた回数を表し、最大 5 桁で構成されます。
- ・ **パターンバージョン**は、lpt\$vpn.### の ### 部分と同じであり、3 桁で構成されます。
- ・ **ビルド番号**は、Patch または特別リリースの番号を表し、2 桁で構成されます。

複数のパターンファイルが同一ディレクトリ内に存在する場合は、最も大きい番号のファイルのみが使用されます。トレンドマイクロは、新しいウイルスパターンファイルを定期的に (通常は週に数回) 発行しており、[アップデート] → [予約アップデート] 画面で自動アップデートの頻度を毎日を設定することをお勧めします。有効なサポート契約を結んでいるトレンドマイクロのすべてのユーザが、アップデートを利用できます。

ウイルスパターンファイルの差分アップデート

アップデートでは、ウイルスパターンファイルの差分アップデートがサポートされます。アップデートは、パターンファイル全体を毎回ダウンロードする代わりに、パターンファイルの新規部分のみをダウンロードして、既存のパターンファイルに追加できます。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をアップデートしてパターンファイルを環境全体に配信するために必要な帯域幅を大幅に低減できます。

コンポーネントを手動でアップデートする

パターンファイル、エンジン、およびデータベースは、[概要] 画面または [手動アップデート] 画面を使用して、任意の時点で手動でアップデートできます。また、必要に応じて、ウイルスパターンファイル、スパイウェア監視パターンファイル、または IntelliTrap パターンファイルを前のバー

ジョンにロールバックすることもできます。前のバージョンにロールバックすると、ロールバックの前にインストールしていたバージョンにアップデートできなくなります。アップデートするには、ロールバックしたコンポーネントの新しいバージョンが利用可能になるまで待つ必要があります。

[概要] 画面でコンポーネントを表示およびアップデートする

[概要] 画面には、図 10-1 に示す [コンポーネントのバージョン] のように、各コンポーネントのパターンのバージョンステータスとアップデートの利用可能性が表示されます。

The screenshot shows the Trend Micro InterScan VirusWall management console. The left sidebar contains navigation links: 概要 (Summary), SMTP, HTTP, FTP, POP3, 大規模感染予防 (Large-scale infection prevention), 隔離 (Isolation), アップデート (Update), レポート (Report), ログ (Log), and 管理 (Management). The main content area is titled '概要' and includes a warning about the usage period. Below this, there are tabs for 'ステータス' (Status), 'メール (SMTP)', 'メール (POP3)', 'Web (HTTP)', and 'ファイル転送 (FTP)'. The 'ステータス' tab is active, showing product information, service status, and a table of component versions.

コンポーネント	現在のバージョン	前回のアップデート
☒ ウイルスパターンファイル	5.725.00	
☒ ウイルス検索エンジン (32ビット)	8.700.1004	
☒ IntelliTrap パターンファイル	10300	
☒ IntelliTrap 除外パターンファイル	13500	
☒ スパイウェア監視パターンファイル	41700	
☒ フィッシングパターンファイル	592	
☒ スпамメール判定ルール	14788.002	
☒ スпамメール検索エンジン	5.6.1016	

Below the table, there are status indicators for various services: ウイルス対策 (0件), スпамメール対策 (0件), and スパイウェア対策 (0件).

図 10-1. [概要] 画面の [コンポーネントのバージョン]

最新のパターンファイルにアップデートすることも、前のバージョンにロールバックすることもできます。以前のパターンファイルにロールバックすると、現在のバージョンより新しいバージョンが利用可能になるまで、そのパターンファイルをアップデートできません。

注意： ロールバックをサポートしているのは、ウイルスパターンファイル、スパイウェア監視パターンファイル、Intellitrap パターンファイルの 3 つのパターンファイルのみです。

コンポーネントをアップデートまたはロールバックするには

1. [概要] 画面の [ステータス] タブを表示します。
2. アップデートまたはロールバックするコンポーネントの横のチェックボックスをオンにします。
すべてのコンポーネントを選択するには、[コンポーネント] 列名の横にあるチェックボックスをオンにするか、次のいずれかを選択します。
 - ウイルスパターンファイル *
 - IntelliTrap パターンファイル *
 - IntelliTrap 除外パターンファイル *
 - スパイウェア監視パターンファイル *
 - ウイルス検索エンジン (32 ビット)
 - フィッシングパターンファイル
 - スпамメール判定ルール
 - スпамメール検索エンジン
3. [アップデート] または [ロールバック] をクリックして、選択したファイルを更新します。
4. コンポーネントの新しいバージョンと変更日を表示するには、[表示更新] をクリックします。

注意： ロールバックできるのは、手順 2 で「*」が付いているコンポーネントのみです。

手動アップデートを使用してコンポーネントをアップデートする

手動アップデート機能では、利用可能な最新コンポーネントを確認して、現在インストールされているコンポーネントのバージョン番号と利用可能なアップデートすべてのバージョン番号が表示されます。

コンポーネントを手動でアップデートするには

1. 左側のメニューで [アップデート] → [手動アップデート] の順に選択します。
[手動アップデート] 画面が開くと、「使用可能な新しいコンポーネントを確認しています。お待ちください ...」というメッセージが表示され、最新のアップデートが検索されます。
2. [アップデート対象コンポーネントの選択] 画面が表示されたら、アップデートを入手するパターンファイルとエンジンを選択します。
3. [アップデート] をクリックします。

注意： 前のバージョンのパターンファイルにロールバックすることもできます。ただし、ロールバックした場合は、ロールバックしたバージョンより新しいバージョンが利用可能になるまで、現バージョンのパターンファイルをアップデートできません。ロールバックをサポートしているのは、ウイルスパターンファイル、スパイウェア監視パターンファイル、Intellitrapp パターンファイルの 3 つのパターンファイルのみです。

アップデートを予約する

コンポーネントのアップデートは、毎日、なるべくトラフィック量が少ない時間帯に実行するようにします。[予約アップデート] 画面では、パターンファイル、検索エンジン、およびデータベースコンポーネントを自動アップデートするように設定できます。

パターンファイル、検索エンジン、および URL フィルタデータベースの自動アップデートを予約するには

1. 左側のメニューで [アップデート] → [予約アップデート] の順に選択します。
2. [予約アップデートを有効にする] チェックボックスをオンにします。
3. アップデートする各コンポーネントの横のチェックボックスをオンにします。
4. アップデート周期を選択します。左側で [分]、[時間]、[日]、または [曜日] のいずれを選択したかに応じて、右側の表示内容は変化します。
5. [保存] をクリックします。

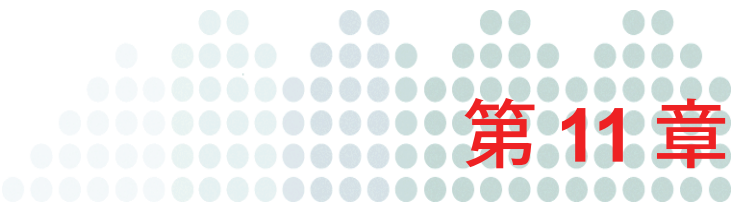
InterScan VirusWall は、指定した間隔でアップデートサーバをチェックして、自動アップデートの対象として選択されているコンポーネントの新しいアップデートが利用可能な場合は、そのアップデートを自動的にダウンロードします。

InterScan VirusWall をアップデートする

トレンドマイクロは随時、報告された既知の問題に対応する Patch、または各製品に適用されるアップグレードをリリースしています。利用可能な Patch がリリースされているかどうかは、次の URL で確認できます。

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

[最新版ダウンロード] 画面が表示されたら、この画面の [InterScan VirusWall スタンダードエディション] リンクをクリックします。日付の付いた各 Patch が表示されます。まだ適用していない Patch がある場合は、この Readme ドキュメントを開き、この Patch の適用が必要かどうかを判断してください。適用が必要な場合は、Readme の指示に従ってインストールします。



第11章

ローカルレポート

Trend Micro InterScan VirusWall スタンダードエディション（以下、InterScan VirusWall）のレポートには、すべての種類のトラフィック違反をまとめることができます。HTTP Web 違反について、指定した期間内に違反したユーザを表示することもできます。レポートには次の情報を含めることができます。

- 発生したウイルス
- ウイルスの発生日時と送信元
- 指定された期間（最大6ヵ月）の違反ユーザおよび違反の種類と頻度

この章では、次のトピックについて説明します。

- 「レポートプロファイルの管理」
- 「生成されたレポートの管理」
- 「レポート管理の実行」

レポートプロファイルの管理

ここでは、新しいレポートプロファイルの作成、レポートの生成頻度の指定、既存のレポートプロファイルの変更、およびレポートプロファイルの削除を実行する方法について説明します。

新しいレポートプロファイルを作成する

新しいレポートプロファイルを作成するには

1. [レポート] → [すべてのレポート] の順に選択します。
2. [新規レポート] をクリックします。

[すべてのレポート] 画面が表示されます (図 11-1 を参照)。

図 11-1. [すべてのレポート] 画面

TREND Micro InterScan™ VirusWall™ ログオフ ヘルプ

すべてのレポート

すべてのレポート > レポートプロファイル

レポートプロファイル情報:

☒ このレポートプロファイルを有効にする

レポートプロファイル名:

レポートの内容

すべてのプロトコルレポート

☒ ブロックされたウイルス/不正プログラムの数

☒ ブロックされたスパイウェア/グレーウェアの数

☒ 上位のブロックされたウイルス/不正プログラムを次の順位まで表示

☒ 上位のブロックされたスパイウェア/グレーウェアを次の順位まで表示

SMTPLレポート	POP3レポート
送信 ☐ 上位のコンテンツフィルタを送信者別に次の順位まで表示 10 ☐ 上位のウイルス/不正プログラムを送信者別に次の順位まで表示 10 ☐ 上位のスパムメールを送信者別に次の順位まで表示 10 ☐ 上位のコンテンツフィルタを送信者別に次の順位まで表示 10 ☐ 上位のメールレピュテーション違反をIPアドレス別に次の順位まで表示 10 受信 ☐ メッセージの数 ☐ メールレピュテーションで検出されたスパムメールの割合 ☐ コンテンツ検索で検出されたスパムメールの割合	☐ 上位のスパムメールを送信者別に次の順位まで表示 10 ☐ 上位のウイルス/不正プログラムを送信者別に次の順位まで表示 10 ☐ 上位のコンテンツフィルタを送信者別に次の順位まで表示 10

HTTPレポート	FTPレポート
☐ 上位の違反を送信者別に次の順位まで表示 10 ☐ 上位のブロック/フィルタされたURLをユーザ別に次の順位まで表示 10 ☐ 上位のブロック/フィルタされたURLをグループ別に次の順位まで表示 10 ☐ Webレピュテーションサービス違反の数	☐ 上位のウイルス/不正プログラムをクライアントIP別に次の順位まで表示 10 ☐ 上位のスパイウェア/グレーウェアをクライアントIP別に次の順位まで表示 10

頻度

すべてのレポート内のコンテンツに、前日の 23:59:59 までのデータを含めます。

レポートの生成: ☒ 1回限り ☐ 毎日 ☐ 毎週 ☐ 毎月

レポートの内容

開始: 2009/06/30

年月日 (yyyy/mm/dd)

終了: 2009/07/07

年月日 (yyyy/mm/dd)

3. [レポートプロファイル情報] で、レポートプロファイル名と、そのレポートプロファイルを有効にするかどうかを指定します。

[このレポートプロファイルを有効にする] チェックボックスをオンにすると、InterScan VirusWall によって、指定されたレポートプロファイルに基づいて新しいレポートが生成されます。

4. [レポートの内容] で、レポートプロファイルに含めるレポートオプションを選択します。
変数を指定するすべてのオプションでは、10 が初期設定値となっています。
5. レポートを生成するタイミングを指定します。
詳細については、247 ページの「レポートの頻度を指定する」を参照してください。
6. [保存] をクリックします。
新しいレポートプロファイルが、[すべてのレポート] 画面の [レポート] テーブルに表示されます。

レポートの頻度を指定する

ここでは、新しいレポートのレポート生成頻度を指定する方法と、既存レポートのレポート生成頻度を変更する方法について説明します。

レポートの頻度を指定するには

1. [すべてのレポート] 画面の [頻度] に進みます。
 - 新しいレポートプロファイルの場合は、[レポート] → [すべてのレポート] の順に選択して、[新規レポート] をクリックします。
 - 既存のレポートプロファイルの場合は、[レポート] → [すべてのレポート] の順に選択して、[レポート] テーブル内のレポートプロファイルをクリックします。
2. [レポートの生成] で、レポートの生成頻度を指定します。
 - 1 回限り — このオプションでは、期間、つまりレポート生成の開始日と終了日を指定する必要があります。
 - 毎日 — このオプションでは、レポートを生成する毎日の開始時刻を指定する必要があります（[開始時刻] ドロップダウンリストで指定する値は 24 時間制です）。
 - 毎週 — このオプションでは、レポートを生成する曜日と時刻を指定する必要があります（[開始時刻] ドロップダウンリストで指定する値は 24 時間制です）。
 - 毎月 — このオプションでは、レポートを生成する毎月の日と時刻を指定する必要があります（[開始時刻] ドロップダウンリストで指定する値は 24 時間制です）。

既存のレポートプロファイルを変更する

既存のレポートプロファイルを変更するには

1. [レポート] → [すべてのレポート] の順に選択します。
2. [レポート] テーブルで、目的のレポートプロファイルのリンクをクリックします。
[すべてのレポート] 画面が表示されます (図 11-1 を参照)。
3. [レポートプロファイル情報] で、レポートプロファイル名を変更したり、レポートプロファイルの有効 / 無効を変更したりします。
[このレポートプロファイルを有効にする] チェックボックスをオンにすると、InterScan VirusWall によって、指定されたレポートプロファイルに基づいて新しいレポートが生成されます。
4. [レポートの内容] で、レポートオプションをオンまたはオフにして、必要な変更を行います。
5. レポートの生成時間を変更するには、247 ページの「レポートの頻度を指定する」を参照してください。
6. [保存] をクリックします。
アップデートされたレポートプロファイルが、[すべてのレポート] 画面の [レポート] テーブルに表示されます。

レポートプロファイルを削除する

レポートプロファイルを削除するには

1. [レポート] → [すべてのレポート] の順に選択します。
2. [レポート] テーブル (チェックボックスの列) で、目的のレポートプロファイルのチェックボックスをオンにして、[削除] をクリックします。
[レポート] テーブルから、目的のレポートプロファイルが削除されます。

生成されたレポートの管理

ここでは、生成されたレポートを表示および削除する方法について説明します。

生成されたレポートを表示する

生成されたレポートを表示するには

1. [レポート] → [すべてのレポート] の順に選択します。
[すべてのレポート] 画面が表示されます。
2. [レポート] テーブル ([レポートの履歴] 列) で、目的のレポートアイコンの横にある数値をクリックします (図 11-2 を参照)。

図 11-2. [レポート] テーブルに表示されたレポートアイコン



[レポートの履歴] 画面が開き、特定のレポートプロファイルのすべてのレポートが表示されます。レポートは、HTML と XML のいずれかで生成できます。

3. [レポートの履歴] テーブル ([レポートの表示] 列) で、目的のレポートのリンクをクリックします。
レポートが開きます。
4. レポートを終了するには、レポートの最下部までスクロールして、[閉じる] をクリックします。

生成されたレポートを削除する

生成されたレポートを削除するには

1. [レポート] → [すべてのレポート] の順に選択します。
[すべてのレポート] 画面が表示されます。
2. [レポート] テーブル ([レポートの履歴] 列) で、目的のレポートアイコンの横にある数値をクリックします (図 11-2 を参照)。

[すべてのレポート] 画面に [レポートの履歴] テーブルが表示され、特定のレポートプロファイルのすべてのレポートが表示されます。

3. [レポートの履歴] テーブル (チェックボックスの列) で、目的のレポートのチェックボックスをオンにして、[削除] をクリックします。
4. [戻る] をクリックして、[レポートの履歴] を終了します。

レポート管理の実行

レポート管理では、InterScan VirusWall で保持するレポートの最大数を指定します。指定したこの値によって、[すべてのレポート] 画面に表示できるレポートの数が制御されます (248 ページの「生成されたレポートの管理」を参照)。

InterScan VirusWall で保持するレポートの最大数を指定するには

1. [レポート] → [メンテナンス] の順に選択します。
[すべてのレポート] 画面が表示されます。
2. [保持するレポートの最大数] 列に、1 ～ 30 の値を指定して、[保存] をクリックします。

第12章

ログ

Trend Micro InterScan VirusWall スタンダードエディション（以下、InterScan VirusWall）では、実行したすべての検索および検出活動を追跡し、その情報をさまざまなログに書き込みます。ログクエリ機能によって、InterScan VirusWall が実行するさまざまな種類の検索タスクの、異なるプロトコルについての検出活動を表示するレポートを作成できます。イベントログを表示することもできます。

ログが蓄積されるとディスク容量がいっぱいになるため、InterScan VirusWall では、ログの自動削除を予約したり、ログを手動で削除することができます。

{インストールフォルダ}\Log にあるすべてのログファイルにアクセスできます。ログの種類は次のとおりです。

表 12-1. ログファイルの説明

ログの種類	説明
DebugLog	すべてのプロトコルについてのデバッグ情報を提供します。初期設定では公開されません。
Eventlog	このログにはイベント情報が書き込まれます。
Systemlog	このログにはシステムレベル情報が書き込まれます。
Viruslog	検出されたすべてのウイルスがログに記録されます。
Antispylog	検出されたすべてのスパイウェア / グレーウェアがログに記録されます。
Antispamlog	SMTP および POP3 トラフィックで検出されたスパムメールとフィッシングメールがログに記録されます。

表 12-1. ログファイルの説明

ログの種類	説明
Emanagerlog	SMTP および POP3 トラフィックで、キーワードフィルタ / 添付ファイルフィルタを起動するメールをログに記録します。
UrlAccesslog	HTTP トラフィックにおける要求をログに記録します。
urlblocklog	HTTP URL ブロック、URL フィルタ、およびフィッシングによってブロックされたページまたはファイルをログに記録します。
connectlog	SMTP、POP3、HTTP、および FTP トランザクションをログに記録します。
nrslog	メールレピュテーションによってブロックされたメールをログに記録します。

ログファイルを手動で開くには、メモ帳などのテキストエディタを使用します。Web コンソールを使用してログをクエリすることもできます。

注意： デバッグログ、システムログ、イベントログ、および接続ログ以外のログの統計情報を、Web コンソールの [概要] 画面から表示できます。

ログクエリ

ログクエリ機能によって、さまざまな検索活動のログを表示したり、その結果を Excel スプレッドシートなどのプログラムにエクスポートすることができます。図 12-1. に、ログクエリを生成する場合に選択可能なオプションを示します。

図 12-1. [ログクエリ] 画面



ログをクエリしてレポートを生成するには

1. 左側のメニューで、[ログ] → [クエリ] の順に選択します。
2. InterScan VirusWall ログでクエリ対象とするプロトコルを選択します。
3. [ログの種類] を選択します。

異なるプロトコルには、異なるログの種類が存在します。

プロトコル	使用可能なログの種類
SMTP/POP3	ウイルス / 不正プログラム スパイウェア / グレーウェア 添付ファイルフィルタ キーワードフィルタ スпамメール対策 フィッシング対策 メールレピュテーション (SMTP のみ)
HTTP	ウイルス / 不正プログラム スパイウェア / グレーウェア URL ブロック URL フィルタ URL アクセス Web レピュテーション

プロトコル	使用可能なログの種類
FTP	ウイルス / 不正プログラム スパイウェア / グレーウェア
その他	イベントログ

4. 事前定義された期間を選択するか、ログエントリを表示する日付の範囲を指定します。
5. 1 ページに表示されるログエントリの数を指定します。
6. [ログ表示] をクリックし、クエリ結果を表示します。

クエリ結果をテキスト、XML、または CSV 形式のファイルにエクスポートするには、[ファイル出力] をクリックし、[ログファイルの出力] 画面からエクスポートするファイルの種類を選択します。

クエリ結果を操作するには

1 ページに表示される結果のエントリの変更するには、[1 ページあたりの件数] ドロップダウンリストから選択します。

他の結果ページに切り替えるには、矢印ボタンをクリックするか、[ページ] インデックスリストから選択します。

クエリされたログをテキスト / XML / CSV ファイルにエクスポートするには、[ファイル出力] をクリックします。

注意： 表示するログエントリが多数ある場合にログクエリの速度を向上するために、[ページ] ドロップダウンリストでは、すべてのページインデックスを表示しません。つまり、現在のページの前後の 200 のインデックスが表示されますが、それ以降のインデックスは一定の間隔でスキップされます。

クエリ結果テーブルのフィールド

さまざまなログをクエリすると、結果が次のように表示されます。

表 12-2. ログクエリ結果テーブルのフィールド

ログの種類	クエリ結果テーブルのフィールドと説明
SMTP/POP3 ウイルスログ	日時: アイテムがログに記録された日時 ウイルス / 不正プログラム名: InterScan VirusWall が検出したウイルス / 不正プログラムの名前 種類: 検出されたウイルス / 不正プログラムの種類 送信者: 送信者のメールアドレス 受信者: 全受信者のメールアドレスのリスト 件名: メールの件名 コンテンツの処理: ウイルス / 不正プログラムが検出された場合の添付ファイルに対する処理
SMTP/POP3 スパイウェア / グレーウェアログ	日時: アイテムがログに記録された日時 スパイウェア / グレーウェア名: InterScan VirusWall が検出したスパイウェア / グレーウェアの名前 種類: 検出されたスパイウェア / グレーウェアの種類 送信者: 送信者のメールアドレス 受信者: 全受信者のメールアドレスのリスト 件名: メールの件名 コンテンツの処理: スパイウェア / グレーウェアが検出された添付ファイルに対する処理
SMTP/POP3 添付ファイルフィルタのログ	日時: アイテムがログに記録された日時 送信者: 送信者のメールアドレス 受信者: 全受信者のメールアドレスのリスト 件名: メールの件名 処理: 添付ファイルフィルタが一致した場合の処理
SMTP/POP3 コンテンツ (キーワード) フィルタのログ	日時: アイテムがログに記録された日時 送信者: 送信者のメールアドレス 受信者: 全受信者のメールアドレスのリスト 件名: メールの件名 処理: キーワードフィルタが一致した場合の処理

表 12-2. ログクエリ結果テーブルのフィールド (続き)

ログの種類	クエリ結果テーブルのフィールドと説明
SMTP/POP3 スпамメール検出ログ	日時: アイテムがログに記録された日時 送信者: 送信者のメールアドレス 受信者: 全受信者のメールアドレスのリスト 件名: メールの件名 メッセージの処理: スпамメールと見なされたメールメッセージに対する処理
SMTP/POP3 フィッシング検出ログ	日時: アイテムがログに記録された日時 送信者: 送信者のメールアドレス 受信者: 全受信者のメールアドレスのリスト 件名: メールの件名 メッセージの処理: フィッシングタイプのメッセージであると見なされたメールメッセージに対する処理
SMTP メールレピュテーションログ	日時: アイテムがログに記録された日時 IP アドレス: クライアントの IP アドレス 処理: この接続に対する処理 結果: 接続に対する処理の結果 (放置または拒否)
HTTP/FTP ウイルスログ	日時: アイテムがログに記録された日時 ウイルス / 不正プログラム名: InterScan VirusWall が検出したウイルス / 不正プログラムの名前 種類: 検出されたウイルス / 不正プログラムの種類 ファイル名: ウイルス / 不正プログラムを含んでいたファイルの名前 クライアント IP / ユーザ ID: ファイルを転送しようとしたクライアントの IP アドレスまたはユーザ名 処理: ウイルス / 不正プログラムが検出された場合のファイルに対する処理
HTTP/FTP スパイウェア / グレーウェアログ	日時: アイテムがログに記録された日時 スパイウェア / グレーウェア名: InterScan VirusWall が検出したスパイウェア / グレーウェアの名前 種類: 検出されたスパイウェア / グレーウェアの種類 ファイル名: スパイウェア / グレーウェアを含んでいたファイル クライアント IP / ユーザ ID: ファイルを転送しようとしたクライアントの IP アドレスまたはユーザ名 処理: スパイウェア / グレーウェアが検出された場合のファイルに対する処理

表 12-2. ログクエリ結果テーブルのフィールド (続き)

ログの種類	クエリ結果テーブルのフィールドと説明
URL ブロックログ	日時 : アイテムがログに記録された日時 クライアント IP : この URL に接続しようとしたクライアントの IP アドレス URL : ブロックされた Web ページのリンク ブロックルール : この URL がブロックされた理由
URL フィルタログ	日時 : アイテムがログに記録された日時 クライアント IP : この URL に接続しようとしたクライアントの IP アドレス URL : フィルタされた Web ページのリンク ブロックルール : この URL のフィルタが許可された理由
Web レピュテーションログ	日時 : アイテムがログに記録された日時 クライアント IP : この URL に接続しようとしたクライアントの IP アドレス URL : フィルタされた Web ページのリンク 予想される障害 : ブロック対象の URL によって引き起こされる可能性のある障害
URL アクセスログ	日時 : アイテムがログに記録された日時 クライアント IP : この URL に接続しようとしたクライアントの IP アドレス ドメイン名 : アクセスされた Web ページのドメイン名 パス : アクセスされた Web ページのパス
イベントログ	日時 : アイテムがログに記録された日時 イベント : その時点の InterScan VirusWall の活動

ログ管理

InterScan VirusWall では、システムに保存されるログの数を管理できます。ログファイルの自動削除を予約したり、ログファイルを手動で削除することができます。

ログの自動削除

ログファイルの自動削除を予約するには、図 12-2 に示すように [ログ] → [メンテナンス] → [自動] タブを選択します。

図 12-2. [ログ] → [メンテナンス] → [自動] タブ



ログの自動削除を予約するには

1. 左側のメニューで、[ログ] → [メンテナンス] の順に選択します。
2. [自動] タブを選択します。
3. [自動削除を有効にする] チェックボックスをオンにします。
4. [対象] で、[すべてのログ] または [指定されたログ] を選択して、削除の対象を指定します。
[指定されたログ] を選択した場合は、削除するログの該当するチェックボックスをオンにします。
 - ウイルス / 不正プログラム
 - スпамメール (コンテンツ検索) / フィッシング
 - コンテンツフィルタ
 - URL アクセス
 - スパイウェア / グレーウェア
 - スпамメール (メールレピュテーション)
 - URL フィルタ / ブロック / Web レピュテーション
5. 選択した種類のすべてのログを削除するか、または指定した日付より古いログだけを削除するかを指定します。
6. [保存] をクリックします。

ログの手動削除

ログファイルを手動で削除するには、図 12-3 に示すように [ログ] → [メンテナンス] → [手動] タブを選択します。

図 12-3. [ログ] → [メンテナンス] → [手動] タブ



ログを手動で削除するには

1. 左側のメニューで、[ログ] → [メンテナンス] の順に選択します。
2. [手動] タブを選択します。
3. [対象] で、[すべてのログ] または [指定されたログ] を選択して、削除の対象を指定します。
[指定されたログ] を選択した場合は、削除するログの該当するチェックボックスをオンにします。
 - ウイルス / 不正プログラム
 - スпамメール (コンテンツ検索) / フィッシング
 - コンテンツフィルタ
 - URL アクセス
 - スパイウェア / グレーウェア
 - スпамメール (メールレピュテーション)
 - URL フィルタ / ブロック / Web レピュテーション
4. 選択した種類のすべてのログを削除するか、または指定した日付より古いログだけを削除するかを指定します。
5. [今すぐ削除] をクリックします。

デバッグログとシステムログ

Web コンソールから生成できるログの他に、すべてのプロトコルについてのデバッグログおよびシステムログを取得することもできます。InterScan VirusWall では、1 日の初めに、または最初のログが指定のサイズを超えたときに、新しいログが作成されます。

システムログには、次のものが含まれます。

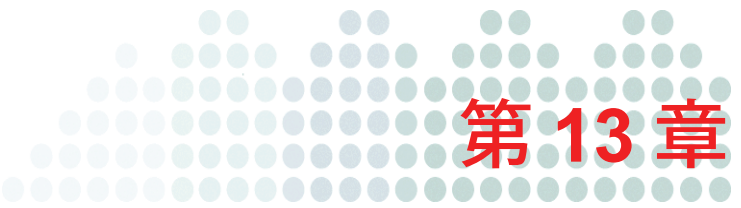
- InterScan VirusWall サービスの開始 / 停止
- プロトコルサービスの開始 / 停止
- 簡単な説明付きの致命的エラー（「致命的」とは、エラーが原因でプログラムが開始できないこと）
- システムエラーと例外

{ インストールフォルダ }¥log から、InterScan VirusWall のすべてのログに加えてデバッグログとシステムログにアクセスできます。デバッグログのファイル名は、debuglog.{yyyymmdd.nnnn} です。「yyyymmdd」には日付、「nnnn」には連続番号が入ります。これらのファイルを開くには、メモ帳などのテキストエディタを使用します。

注意： 初期設定では、デバッグログは有効になっていません。

デバッグログを手動で有効にするには

1. インストールパス ({ ローカルドライブ }¥Program Files¥Trend Micro¥InterScan VirusWall など) にある Config.xml ファイルを開きます。
2. 次のテキストを検索します。<Value Name="DebugEnabled" string="" type="int" int="0" />
3. このテキストを次のように変更します。<Value Name="DebugEnabled" string="" type="int" int="1" />
4. ファイルを保存して閉じてから、SMTP/POP3/HTTP/FTP プロセスのいずれか、または InterScan VirusWall サービス全体を再起動します。



第13章

管理

InterScan VirusWall のアクティベート

Trend Micro InterScan VirusWall スタンダードエディション (以下、InterScan VirusWall) を購入すると、製品機能を有効にするためのアクティベーションコードが発行されます。アクティベーションコードは通常、製品に同梱された使用許諾契約書に記載されています。使用許諾契約書が手元にない場合は、トレンドマイクロにお問い合わせください。

InterScan VirusWall をアクティベートする

製品の購入時に入手したアクティベーションコードを使用して、InterScan VirusWall をアクティベートできます。

インストール時にアクティベートするには

[製品のアクティベーション] 画面でアクティベーションコードを入力します。

図 13-1. インストール時の [製品のアクティベーション] 画面



注意： InterScan VirusWall をアクティベートせずにインストールした場合は、30 日間の猶予期間が与えられます。この期間中は、すべての機能を使用したり、パターンファイルをアップデートしたりすることができます。ただし、猶予期間が終了すると、これらの機能は使用できなくなります。

InterScan VirusWall をアクティベートせずにインストールした場合、InterScan VirusWall がアクティベートされていないことを示すメッセージが Web コンソールに表示されます。

インストール後 30 日たっても InterScan VirusWall をアクティベートしない場合、InterScan VirusWall の設定は変更できますが、製品の機能はすべて使用できなくなり、パターンファイルのアップデートも実行されません。

インストール後にアクティベートするには

1. [管理] → [製品ライセンス情報] の順に選択し、[製品ライセンス情報] 画面を表示します。
2. [新規入力] をクリックします。
[アクティベーションコードの新規入力] 画面が表示されます。
3. [新しいコード] フィールドにアクティベーションコードを入力します。
4. [アクティベート] をクリックします。

アクティベートすると、[製品ライセンス情報] 画面の上部にあるメッセージが、正常にアクティベートされたことを示す内容に変わります。

InterScan VirusWall をアクティベートすると、セキュリティの初期設定に従ってただちに検索が開始されます。コンテンツフィルタ、URL ブロック、およびファイルブロックを有効にする場合は、組織の通信ポリシーと購入したライセンスに従ってこれらの機能を設定します。

InterScan VirusWall をアクティベートしたアクティベーションコードが製品版のアクティベーションコードであり、その失効日が変更されている場合、InterScan VirusWall では自動オンラインアップデートがサポートされます。

手動でオンラインアップデートを実行するには

1. ネットワークステータスおよびプロキシ設定を必要に応じて確認します。
2. [管理] → [製品ライセンス情報] の順に選択し、[製品ライセンス情報] 画面を表示します (図 13-2 を参照)。
3. [ステータスをオンラインで確認] をクリックします。

図 13-2. [製品ライセンス情報] 画面

製品ライセンス情報

InterScan VirusWallの使用期限まで残り54日です。 [製品の更新について](#)

ステータスの最終更新日: 2009年7月8日 [ステータスをオンラインで確認](#)

ライセンス情報		詳細情報をオンラインで確認
製品:	InterScan VirusWall スタンドエディション	
バージョン:	7.0 (製品版)	
アクティベーションコード:	VW-332H-YXPDS-UQNXH-4BP87-Q465L-LBWQK	新規入力
ステータス:	アクティベーション完了	
有効期限:	2009年8月31日	

販売店情報	
販売店名:	N/A
メールアドレス:	N/A
担当者:	N/A
電話番号:	N/A
追加情報:	N/A

更新手順を表示するには、[製品の更新について] をクリックします。

現在のライセンスに関する詳細情報を表示するには、[詳細情報をオンラインで確認] をクリックします。

アクティベーションの詳細

アクティベーションの詳細については、次のサイトを参照してください。

<http://esupport.trendmicro.co.jp/>

管理機能の使用

Control Manager を設定する

[Control Manager 設定] 画面は、InterScan VirusWall と Control Manager サーバ間の接続設定を行い、InterScan VirusWall を Control Manager に登録するために使用します。設定を適用し、InterScan VirusWall を Control Manager サーバに登録した後、InterScan VirusWall を Control Manager の Web コンソールから管理できるようになります。

図 13-3. Control Manager 設定

Control Manager設定

ISVW MCPエージェントとControl Managerサーバ間の通信を設定します。(*)の項目は入力必須です。

接続ステータス

登録済みのControl Managerサーバ: 未登録

接続設定

エンティティ表示名 *: isvw79_ISVW

Control Managerサーバ設定

サーバのFQDNまたはIPアドレス *:

ポート *: 443 ; ☒ 接続にHTTPSを使用する

Webサーバ認証:

ユーザー:

パスワード:

MCPプロキシ設定

☐ Control Managerサーバとの通信にプロキシサーバを使用する

プロトコル: ☒ HTTP ☐ SOCKS 4 ☐ SOCKS 5

サーバのFQDNまたはIPアドレス:

ポート:

プロキシサーバ認証:

ユーザID:

パスワード:

双方向通信のポート転送

☐ 双方向通信のポート転送を有効にする

IPアドレス:

ポート:

登録 接続のテスト キャンセル

注意: InterScan VirusWall の管理手順については、Control Manager のドキュメントを参照してください。

Control Manager を設定するには

1. [管理] → [Control Manager 設定] の順に選択し、[Control Manager 設定] 画面を表示します。
2. InterScan VirusWall を示す名前を入力すると、その名前が Control Manager サーバの製品ツリーに表示されます。
3. Control Manager サーバのサーバ FQDN または IP アドレスおよびポート情報を入力します。
4. Control Manager サーバをホストする IIS サーバにアクセスするために使用するユーザ名とパスワードを入力します。

5. MCP プロキシ設定を行います。

InterScan VirusWall と Control Manager サーバ間の通信にプロキシサーバが必要な場合は、[Control Manager サーバとの通信にプロキシサーバを使用する] を選択して、プロキシサーバを有効にし、選択します。プロキシサーバの FQDN または IP アドレスおよびポート番号を入力します。プロキシサーバに認証が必要な場合は、プロキシサーバを介して通信するために使用するユーザ名とパスワードを入力します。

6. 双方向通信ポート転送を設定します。

InterScan VirusWall と Control Manager サーバ間に NAT またはファイアウォールがあり、Control Manager サーバから InterScan VirusWall にコマンド通知を送信できるようにしたい場合、接続を InterScan VirusWall に転送するように NAT またはファイアウォールを設定する必要があります。双方向通信ポート転送を設定するには、[双方向通信のポート転送を有効にする] を選択して、NAT またはファイアウォールの IP アドレスとポート番号を入力します。

7. [登録] をクリックします。

注意： InterScan VirusWall の管理手順については、Control Manager のドキュメントを参照してください。

InterScan VirusWall がサポートする Control Manager の機能

表 13-1 は、Control Manager Web コンソールから実行できる InterScan VirusWall 管理タスクの一部です。

表 13-1. InterScan VirusWall がサポートする Control Manager の機能

InterScan VirusWall がサポートする Control Manager の機能	サポートされるタスク
ステータスマニタ	Control Manager では、Control Manager サーバに登録された InterScan VirusWall サーバのステータス (コンポーネントとシステム情報) を監視できます。
AC の更新 / 配信	Control Manager では、Control Manager サーバに登録された InterScan VirusWall サーバの製品 AC を更新または配信できます。
パターンファイル / エンジンの配信	Control Manager は、Control Manager サーバに登録された InterScan VirusWall サーバに新しいパターンファイルとエンジンを配信できます。
シングルサインオン	Control Manager Web コンソールを使用して、管理者は Control Manager サーバに登録された InterScan VirusWall サーバを設定できます。
グループ設定	Control Manager Web コンソールを使用して、管理者は登録された InterScan VirusWall サーバから別の登録された InterScan VirusWall サーバに設定を複製できます。
ログのアップロード	登録された InterScan VirusWall サーバは、イベントログとセキュリティログを Control Manager サーバにアップロードして、集中監視を可能にすることができます。
大規模感染予防ポリシー	Control Manager サーバは、Control Manager サーバに登録された InterScan VirusWall サーバに大規模感染予防ポリシーを配信できます。

通知設定

SMTP/POP3/FTP/HTTP の各モジュールは、セキュリティリスクを検出したとき、あるいはメッセージまたはファイルによってコンテンツフィルタ設定がトリガされたときに、通知設定を使用してメール通知を送信します。

図 13-4. 通知設定

通知設定

次の設定は、InterScan VirusWallがメール通知を送信するときに使用します。

通知先設定

SMTPサーバ:

ポート: 25

管理者メールアドレス

管理者メールアドレス:

送信者メールアドレス:

文字コード: Unicode (UTF-8)

初期設定では、InterScan VirusWall はそのインストール先コンピュータの完全修飾ドメイン名 (FQDN) を検出して、この FQDN を通知の送信時に使用します。たとえば、インストール先コンピュータが sample.com というドメインに属している場合、InterScan VirusWall の通知メールアドレスは isvw@sample.com になります。インストール先コンピュータがどのドメインにも属していない場合、InterScan VirusWall は isvw@localdomain をアドレスとして使用します。

警告： FQDN を使用して通知メッセージを送信すると、その FQDN がネットワーク外部のユーザに知られる可能性があります。この問題に対処するには、通知メールのアドレスを別のメールアドレスに置き換えます。

通知を設定するには

1. 通知の送信に使用する SMTP サーバ名または IP アドレスとポートを設定します。ドメイン名を入力する場合は、次のいずれかの操作を実行してください。
 - a. 次に示すように、nslookup コマンドを使用して、ドメイン名を正しく解決できるようにします。
 - nslookup
 - notification.domainname

または

- b. ドメイン名と IP アドレスのマッピング情報を
%windir%\system32\drivers\etc\hosts にあるホストファイルに追加します。例：
 - notificationIP notification.domainname

InterScan VirusWall がこの SMTP サーバを介してすべての通知を正しく送信できるようにするには、InterScan VirusWall サーバの IP アドレスを SMTP サーバの信頼された IP アドレスのリストに追加します。管理者宛ての通知の受信に使用する管理メールアドレスを設定します。複数の通知アドレスがある場合は、次のようにセミコロン (;) で区切ります。

```
admin1@isvctest.com;admin2@isvctest.com
```

2. InterScan VirusWall が通知の送信に使用する送信者メールアドレスを設定します。
3. 使用する文字コードを選択します。
 - 英語 (US-ASCII)
 - Unicode (UTF-8)
 - ISO (ISO-8859-1)
 - ISO (ISO-8859-2)
 - ISO (ISO-8859-3)
 - 簡体字中国語 (GB2312)
 - 繁体字中国語 (Big5)
 - 中国語 (ISO-2022-CN)
 - 韓国語 (ISO-2022-KR)
 - 日本語 (ISO-2022-JP)
 - 日本語 (Shift_JIS)

注意： UTF-8 はほとんどの言語で使用できます。

送信者のメールアドレスを置き換えるには

1. Web コンソールの [管理] → [通知設定] ページに移動します。
2. [送信者メールアドレス] フィールドを変更します。
3. [保存] をクリックします。

パスワード

[管理] → [パスワード] の順に選択して表示される画面では、Web コンソールを管理するためのパスワードを設定できます。

図 13-5. [パスワードの変更] 画面

パスワードは、スペースを含まない 4 ～ 32 の英数字である必要があります。パスワードが正常に変更されると、通知メッセージが表示されます。

プロキシ設定

プロキシサーバを使用してインターネットに接続する場合は、プロキシ設定を指定します。InterScan VirusWall では、次の処理を実行するためにプロキシ情報が必要です。

- ・ パターンファイル / エンジンのアップデート

- ・ ライセンス情報のアップデート
- ・ ウイルストラッキングセンターへのウイルスログの送信
- ・ TrendLabs (トレンドラボ) からの大規模感染予防ポリシーのダウンロード

図 13-6. プロキシ設定

プロキシ設定を設定するには

1. [管理] → [プロキシ設定] の順に選択します。
2. プロキシサーバの種類を選択します。
3. プロキシサーバの名前または IP アドレスとポートを指定します。
4. プロキシサーバで認証が必要な場合は、有効なユーザ ID およびパスワードを入力します。
5. [接続のテスト] をクリックします。
設定が正しい場合は、確認の通知を受け取ります。
6. [保存] をクリックします。

ウイルストラッキングセンター

トレンドマイクロは、ウイルストラッキングセンターを通じて、脅威の大規模感染を監視し、より強力な保護機能を提供しています。[情報を送信する]を選択すると、InterScan VirusWall で検出されたウイルスの情報が定期的にウイルストラッキングセンターに送信されます。[送信するサンプルデータ]をクリックすると、送信されるデータのサンプルが表示されます。

詳細については、次の URL からアクセスできるウイルストラッキングセンターの Web サイトを参照してください。<http://wtc.trendmicro.com/japanese/>

ユーザ ID 設定

ユーザ ID 設定では、InterScan VirusWall 経由で HTTP 接続を行っている組織内の個々のユーザおよびグループを識別できます。ドメインユーザの識別では、次の操作を実行できます。

- ユーザの役割の識別
- グループへの HTTP アクセスルールの適用
- ユーザまたはグループ固有の URL フィルタ / ブロックのポリシーの作成

トレンドマイクロのドメインコントローラエージェントは、Windows ベースのディレクトリサービスでユーザに透過的なユーザ識別を提供します。ドメインコントローラエージェントは、ドメインコントローラと通信し、最新のユーザログオン情報を収集して InterScan VirusWall に提供します。この情報は、特定のユーザおよびグループに適用される URL フィルタおよび URL ブロックのポリシーの作成に使用できます。

[ユーザ ID] 画面には、次の情報が表示されます。

- 「ユーザ識別方法を選択する」
- 「ドメインコントローラエージェントについて」
- 「ドメインコントローラエージェントについて」
- 「ドメインコントローラサーバの資格情報を追加する」

ユーザ識別方法を選択する

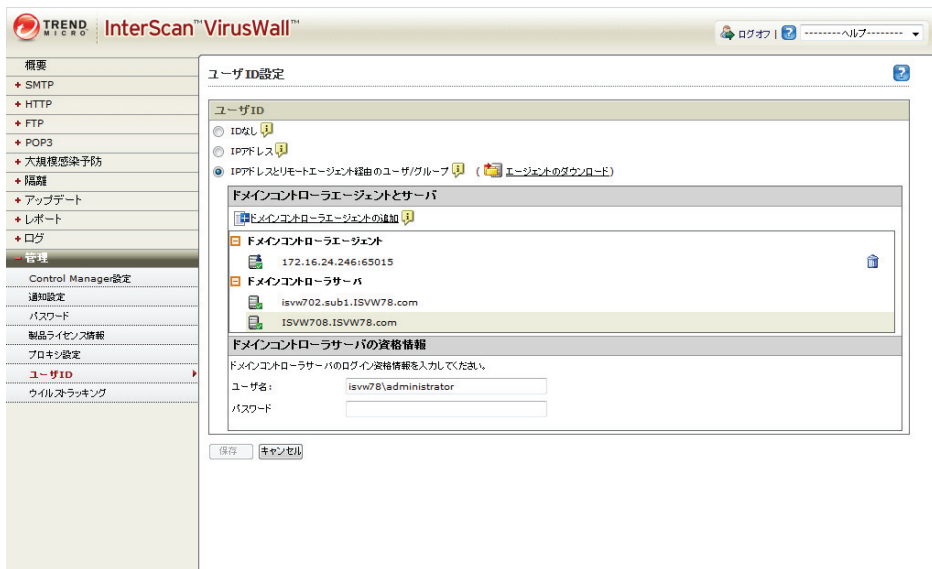
ユーザは、図 13-7 に示すように、IP アドレスか、プロキシ認証を使用したユーザ / グループ名によって識別できます。

ユーザを識別することにより、次のことが可能になります。

- URL フィルタおよび URL ブロックのユーザ / グループベースのポリシー設定

- ・ 違反ログでのユーザ情報の表示
- ・ HTTP デバッグログでのドメイン名およびアカウント情報の表示

図 13-7. [ユーザ ID 設定] 画面



ユーザ ID 設定を設定するには

1. [管理] → [ユーザ ID] の順に選択します。
2. 次のいずれかのオプションを選択します。
 - ・ **ID なし** — 接続にユーザまたはグループ ID は使用されず、グローバルユーザポリシーが適用されます。
 - ・ **IP アドレス** — ユーザは IP アドレスによって識別されます。
 - ・ **IP アドレスとリモートエージェント経由のユーザ / グループ** — この設定を使用すると、個々のユーザとグループの両方を名前 (第 1) または IP アドレス (第 2) で識別できます。ドメインコントローラエージェントおよびサーバを設定する必要があります。

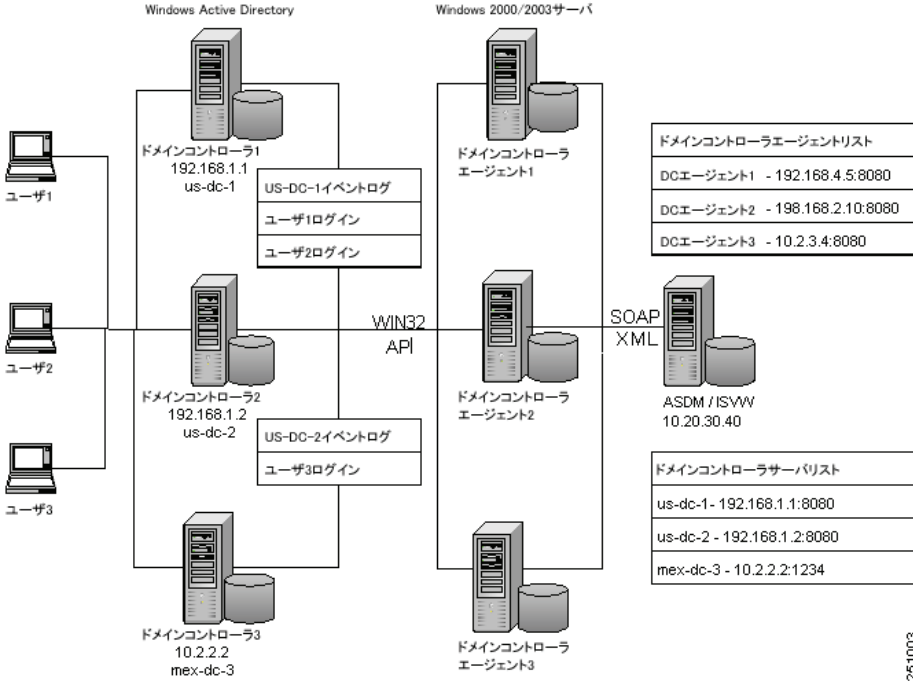
ドメインコントローラエージェントについて

トレンドマイクロのドメインコントローラエージェントは、初期設定で 10 秒おきにユーザログオンセッションについて各ドメインコントローラにクエリを実行し、各ログオンセッションのユーザ名およびワークステーション名を取得します。識別されたログオンセッションごとにドメインコントローラエージェントは DNS 参照を実行し、ワークステーション名を IP アドレスに解決して、結果としてのユーザ名と IP アドレスのペアを記録します。

ドメインコントローラエージェントでは、ドメインコントローラとの通信に Win32 API が使用され、ログオンデータの InterScan VirusWall への送信に SOAP/XML が使用されます。ドメインコントローラエージェントから InterScan VirusWall ソフトウェアコンポーネントに送信されるユーザデータは、1 つのユーザ名と IP アドレスのペアごとに約 80 バイトになります。平均して、ドメインコントローラエージェントでは 10MB の RAM が使用されますが、これはドメインコントローラのネットワークごとのログオンセッション数によって異なります。

InterScan VirusWall では、最大 32 個のドメインコントローラがサポートされ、最大 8 個のドメインコントローラエージェントを InterScan VirusWall に割り当てることができます。複数のエージェントと使用すると冗長性を実現できます。1 つのエージェントに障害が発生した場合も、他のエージェントがバックアップとして機能します。InterScan VirusWall には 8 個のドメインコントローラエージェントを割り当てることができますが、ほとんどのネットワーク設定で必要になるのは 2 つか 3 つのみです。

図 13-8. ドメインコントローラエージェントをインストールするためのネットワーク設定



ドメインコントローラエージェントをインストールする

ドメインコントローラエージェントは、ドメインコントローラサーバおよび InterScan VirusWall コンピュータとは別の、Active Directory ドメインの一部である Windows 2000、2003、または 2008 サーバにインストールしてください。Windows 2000 以降のサーバでは、Windows 2000 以降のサーバで実行されているすべての Windows Active Directory ドメインコントローラサーバで、InterScan VirusWall 自動検出機能がサポートされます。

インストールされると、ドメインコントローラエージェントは、10 秒おきに新しいログオン情報についてドメインコントローラに対してポーリングを実行します。このログオン情報は、ユーザーおよびグループの URL フィルタおよび URL ブロックのポリシーの設定および施行に使用されます。

ドメインコントローラエージェントをインストールするには

1. インストールする前に、ログがログオンイベントに対して有効になっていることを確認します。
有効になっていないと、ドメインコントローラエージェントは、ドメインコントローラのログのユーザ情報にアクセスできません。
 - a. ドメインコントローライベントログの Windows サーバイベントを有効にするには、各ドメインコントローラコンピュータで、[スタート] → [管理ツール] → [ドメイン コントローラ セキュリティ ポリシー] の順に選択します。
 - b. [セキュリティの設定] → [ローカル ポリシー] → [監査ポリシー] の順に選択します。
 - c. [アカウント ログオン イベントの監査] ポリシー (監査成功) のポリシー設定を定義します。
2. 管理者権限を使用して、ドメインコントローラエージェントのインストール先サーバ (Windows 2000 または Windows 2003) にログオンします。
3. isvw: http://<ip>:9240 から InterScan VirusWall の UI にアクセスして、ログオンします。
4. [管理] → [ユーザ ID] の順に選択します。
5. [エージェントのダウンロード] リンクをクリックして、画面に表示される指示に従います。
 - a. [実行] または [保存] をクリックします。

注意： この操作は、Internet Explorer 6.0 以上で完全にサポートされています。Mozilla Firefox を使用している場合、インストールを保存できますが、実行はできません。

- [実行] を選択した場合、エージェントのインストールは一時フォルダに保存され、起動されます。
- [保存] を選択した場合は、後から手動で起動する必要があります。

注意： エージェントのインストールを後から起動する場合は、保存したフォルダを参照して、IdAgentInst.msi という名前のファイルをダブルクリックします。

- b. セットアップウィザードで、[次へ] をクリックします。
- c. 使用許諾契約のチェックボックスをオンにして、[次へ] をクリックします。
- d. [インストール先フォルダ] 画面で [次へ] をクリックします。

注意： インストール先フォルダを変更することはできません。インストーラによって、適切なシステムドライブが自動的に検出されます。

- e. [続行] をクリックします。
進捗バーが表示されます。
 - f. セットアップが終了したら、[完了] をクリックします。
6. ドメインコントローラエージェントをさらにインストールする場合は、手順 1 ～ 5 を繰り返します。
- 最大 8 個のドメインコントローラエージェントで 1 つの InterScan VirusWall を指すことができます。
7. 277 ページの「InterScan VirusWall にドメインコントローラエージェントを追加する」の手順に従って、ドメインコントローラエージェントとドメインコントローラを InterScan VirusWall に追加します。
8. 279 ページの「ドメインコントローラサーバの資格情報を追加する」の手順に従って、ドメインコントローラのログオン資格情報を追加します。

InterScan VirusWall にドメインコントローラエージェントを追加する

InterScan VirusWall には、ユーザまたはグループ固有の URL フィルタおよび URL ブロックのポリシーを許可するために、ドメインコントローラエージェントおよびドメインコントローラサーバを追加する必要があります。

ドメインコントローラエージェントを追加すると、InterScan VirusWall ではドメインコントローラエージェントからユーザログオン情報にアクセスできるようになります。ドメインコントローラサーバは、ドメインコントローラエージェントの組み込み自動検出機能を使用して InterScan VirusWall に設定されます。

ドメインコントローラエージェントは手動で追加され、ドメインコントローラサーバのように自動検出されることはありません。ドメインコントローラサーバは手動で追加することはできません。

注意： Windows 2000 Pro、Windows 2000、Windows 2003、Windows XP、または Windows 2008 サーバにインストールされているドメインコントローラエージェントでは、自動検出機能を使用できます。Windows Active Directory ドメインコントローラサーバはすべて自動検出されます。

ドメインコントローラエージェントを InterScan VirusWall で設定すると、InterScan VirusWall のフェイルオーバーデバイスに同じ設定が自動的に伝搬されます。

ドメインコントローラエージェントを追加するには

1. [管理] → [ユーザ ID] の順に選択します。
[ユーザ ID 設定] 画面が表示されます (図 13-7 を参照)。
2. [IP アドレスとリモートエージェント経由のユーザ / グループ] オプションをオンにして、[エージェントのダウンロード] リンクをクリックします。
3. [ドメインコントローラエージェントとサーバ] の [ドメインコントローラエージェントの追加] リンクをクリックします。
[ユーザ ID 設定] 画面に [ドメインコントローラエージェント] が表示されます。
4. ドメインコントローラエージェントについて、次の情報を入力します。
 - ・ ホスト名 / IP アドレス — ドメインコントローラエージェントがインストールされているコンピュータのホスト名または IP アドレス (図 13-7 を参照)。ポート番号は、ドメインコントローラエージェントがインストールされているコンピュータのポート番号です。初期設定のポート番号 65015 は、IdAgent.ini ファイルの [Setting] / AgentPort パラメータで指定されています。
5. [保存] をクリックします。
図 13-7 のリストに、追加したドメインコントローラエージェントの名前が表示されます。
6. [保存] をクリックします。
ドメインコントローラエージェントを InterScan VirusWall で設定すると、InterScan VirusWall のフェイルオーバーコンピュータに同じ設定が自動的に伝搬されます。

InterScan VirusWall からドメインコントローラエージェントを削除する

リストからドメインコントローラエージェントを削除するには

1. [管理] → [ユーザ ID] の順に選択します。
2. リスト内で目的のエージェントを見つけます。
3. 名前の横にあるごみ箱アイコンをクリックします。
削除を取り消すには [キャンセル] をクリックします。
4. [保存] をクリックすると、削除を取り消すことはできなくなります。

注意： ドメインコントローラエージェントをアンインストールするには、インストール先のコンピュータに移動します。[スタート] → [設定] → [コントロール パネル] → [プログラムの追加と削除] → [Trend Micro IdAgent] の順に選択します。

InterScan VirusWall のドメインコントローラサーバを検出する

InterScan VirusWall には、ユーザまたはグループ固有の URL フィルタおよび URL ブロックのポリシーを許可するために、ドメインコントローラエージェントおよびドメインコントローラサーバを追加する必要があります。

ドメインコントローラサーバは、ドメインコントローラログオンイベントにアクセスしてユーザ情報を取得するドメインコントローラエージェントに情報を提供します。

注意： InterScan VirusWall では、ドメインコントローラサーバを手動で追加することはできません。ドメインコントローラサーバは、InterScan VirusWall の自動検出メカニズムによって自動的に追加されます。ドメインコントローラサーバは削除できません。

- ドメインコントローラサーバを追加するには、ユーザ識別方法として、[IP アドレスとリモートエージェント経由のユーザ / グループ] オプションを選択する必要があります。
- Windows 2000 Pro、Windows 2000、Windows 2003、Windows XP、または Windows 2008 サーバにインストールされているドメインコントローラエージェントでは、自動検出機能を使用できます。Windows Active Directory ドメインコントローラサーバはすべて自動検出されます。
- 複数のドメインコントローラサーバを追加する場合、[ドメインコントローラサーバの資格情報] セクションを使用するためには、資格情報のすべてのログが同一である必要があります (279 ページの「ドメインコントローラサーバの資格情報を追加する」を参照)。

ドメインコントローラサーバの資格情報を追加する

ドメインコントローラサーバの資格情報を追加することにより、シングルサインオンが可能になり、認証が 1 回で済みます。

ドメインコントローラエージェントのインストールには管理者権限が必要です。ドメインコントローラエージェントが Windows コンピュータにインストールされている場合、ローカルシステムアカウントにはドメインコントローラへのアクセス権がないため、InterScan VirusWall ではドメイ

ンユーザおよびグループにクエリを実行できません。InterScan VirusWall ユーザは、[ユーザ ID 設定] 画面の [ドメインコントローラサーバの資格情報] のユーザ名およびパスワードのフィールドにドメインコントローラの資格情報を入力することによってアクセス権を有効にできます。

注意： この画面に資格情報を入力する場合、すべてのドメインコントローラサーバで同一のユーザ名およびパスワードの資格情報が共有されていることが重要です。

クライアントコンピュータのファイアウォールに要件を指定するには

1. クライアントコンピュータでリモートレジストリサービスを実行します。
2. ドメインアカウントを使用してログインします。
3. ファイアウォールが設定されている場合は、TCP ポート 445 で受信 RPC トラフィックを許可するように除外を設定します。

Windows XP SP2 でポート 445 を開くには

- a. [スタート] をクリックして [コントロール パネル] を開き、[Windows ファイアウォール] を選択します。
- b. [例外] タブを選択します。
- c. [ファイルとプリンタの共有] をオンにして [OK] をクリックします。

その他のファイアウォールについては、ポートを開く方法に関して製品マニュアルを参照してください。

ドメインコントローラサーバの資格情報を追加するには

1. [管理] → [ユーザ ID] の順に選択します。
2. 画面の下部にある [ドメインコントローラサーバの資格情報] に進みます (図 13-7 を参照)。
3. 「ドメイン名 ¥ ユーザ名」の形式でユーザ名を入力します。
4. パスワードを入力します。
5. [保存] をクリックします。

リアルタイム検索モニタの使用

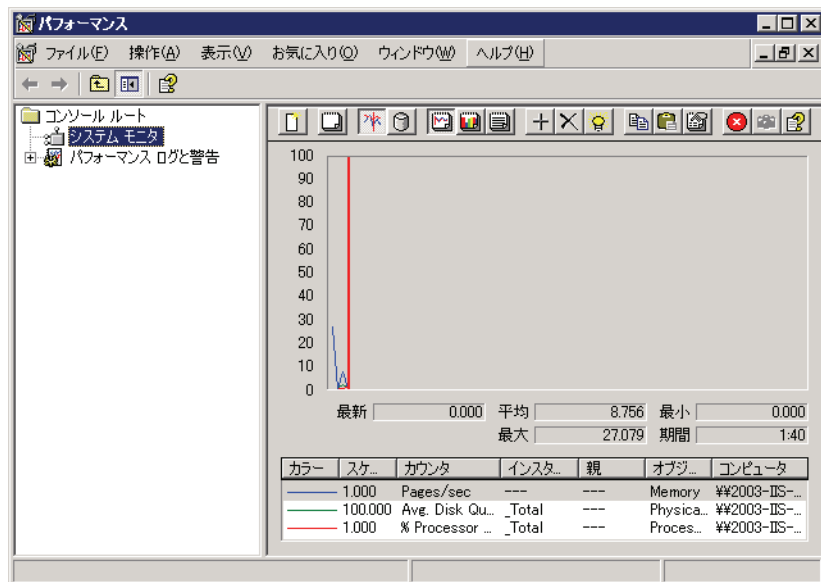
Trend Micro InterScan VirusWall スタンダードエディション（以下、InterScan VirusWall）のリアルタイム検索モニタでは、SMTP 検索機能のリアルタイム監視と、Windows パフォーマンスモニタを使用した SMTP および FTP パフォーマンスデータへのアクセスが可能です。

注意： リモートで監視するには、Windows 2003 Server Remote Desktop、または Remote Administrator などのリモート制御ソフトウェアを使用します。

リアルタイム検索モニタを実行するには

1. Windows の [スタート] メニューで、[プログラム] → [InterScan VirusWall] → [InterScan VirusWall リアルタイム検索モニタ] の順に選択します。
SMTP 経由でメールを送信すると、統計および活動に関するリアルタイムの情報がモニタパネルに表示されます。
2. Windows パフォーマンスモニタを開くには、[パフォーマンスモニタ] をクリックします。

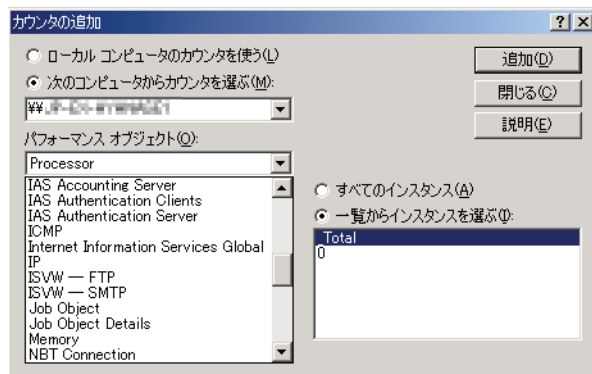
図 14-1. Windows パフォーマンスモニタ



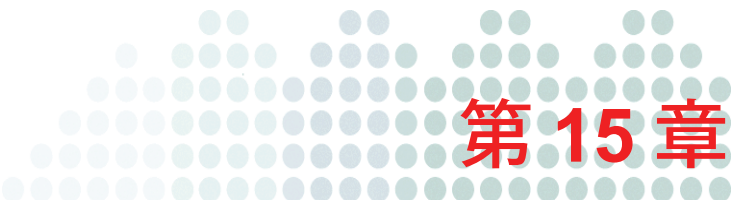
Windows パフォーマンスモニタにカウンタを追加するには

1. Windows パフォーマンスモニタの画面で「+」をクリックします (図 14-2 の丸で囲まれたアイコンを参照)。[カウンタの追加] 画面が表示されます。

図 14-2. [カウンタの追加] 画面



2. [次のコンピュータからカウンタを選ぶ] オプションを選択して、InterScan VirusWall がインストールされているコンピュータを選択します。
3. [パフォーマンス オブジェクト] ドロップダウンリストから [InterScan VirusWall – FTP] または [InterScan VirusWall – SMTP] を選択します。
4. [すべてのカウンタ] を選択するか、[一覧からカウンタを選ぶ] を選択して追加するカウンタを選択します。
5. [追加] をクリックします。
6. [閉じる] をクリックして、Windows パフォーマンスモニタに戻ります。
7. グラフ表示、ヒストグラム表示、またはレポート表示でパフォーマンスデータを表示します。



第 15 章

トラブルシューティングとサポート

この章では、Trend Micro InterScan VirusWall スタンダードエディション (以下、InterScan VirusWall) のインストール時、設定時、または使用時に発生する可能性のある問題の解決に役立つ情報を提供します。この章で取り上げているもの以外の問題が発生した場合は、オンラインヘルプを参照してください。さらに支援を必要とする場合は、307 ページの「製品サポート情報」を参照してください。

トラブルシューティング

表 15-1. 問題のトラブルシューティング

問題	説明、考えられる原因、対策
インストールに失敗します。	- システム要件を満たしていません。30 ページの「システム要件」を参照してください。 - OS のバージョンや Service Pack が要件を満たしていない場合、インストールは続行されますが、警告メッセージが表示されます。 - インストール先ディスクの空き領域が不足しています。InterScan VirusWall をインストールするハードディスクには 1GB 以上の空き領域が必要です。空き領域を増やすか、十分なディスク領域があるサーバに InterScan VirusWall をインストールしてください。 - InterScan VirusWall のインストールに必要な権限がありません。管理者権限でログオンしてインストールを実行してください。 - これらの要件を満たしていてもインストールに失敗する場合は、トレンドマイクロのサポートにお問い合わせください。
インストール直後に CPU 使用率が 100% になります。	これは正常な現象であり、InterScan VirusWall を正しく実行する前に、検索エンジン、スパムメール検索エンジン、設定ファイル、ログファイル、読み込みパターンファイルなどのコンポーネントの初期化が必要のために発生します。推奨環境の場合、初期化は数分で完了します。その後、CPU の使用率は正常な状態に戻ります。
サービスを開始 / 停止できません。	61 ページの「InterScan VirusWall を起動 / 停止する」の手順の実行後にサービスを停止できない場合は、次の操作を実行します。 [コントロール パネル] → [管理ツール] → [サービス] の順に選択し、サービスを右クリックして [停止] をクリックします。 - それでも停止しない場合は、[コントロール パネル] → [管理ツール] → [サービス] の順に選択し、サービスを右クリックして [プロパティ] をクリックします。[全般] タブの [スタートアップの種類] に移動し、[手動] を選択します。システムを再起動します。 - 再起動後、状態は「停止」になります。 61 ページの「InterScan VirusWall を起動 / 停止する」の手順の実行後にサービスを開始できない場合は、トレンドマイクロのテクニカルサポートにお問い合わせください。

表 15-1. 問題のトラブルシューティング (続き)

問題	説明、考えられる原因、対策
ライセンスをアップデートできません。	・ライセンスをアップデートする前に製品をアクティベートしてください。 ・体験版の InterScan VirusWall を使用してライセンスをアップデートすることはできません。 ・バックエンドのライセンスのオンラインアップデートサーバでシステムまたはプログラムの例外エラーが発生する場合は、数分待ってから再試行してください。問題が解決しない場合は、トレンドマイクロのテクニカルサポートにお問い合わせください。 ・Config.xml¥Common¥ProductRegistration¥OnLineUpdate¥Server¥Source に格納されている不適切なサーバ URL が原因でライセンスをアップデートできない場合は、設定をチェックしてから再試行してください。 ・使用しているアクティベーションコードがオンラインアップデートのライセンスサーバにない場合は、有効なアクティベーションコードを入力してから再試行してください。 ・ライセンスをオンラインでアップデートできない場合は、ネットワークの状態を確認してください。プロキシサーバを使用している場合は、そのプロキシサーバが製品登録サーバに接続できるかどうかをチェックしてください。問題が解決しない場合は、トレンドマイクロのテクニカルサポートにお問い合わせください。
アクティベーションに関する問題	・無効なアクティベーションコードを使用しています。製品版または体験版のアクティベーションコードを使用して製品を再度アクティベートしないでください。 ・使用している体験版または製品版のアクティベーションコードが失効しています。 ・製品版をインストールしている場合は、体験版のアクティベーションコードを使用しないでください。その逆も同様です。 ・引き続きアクティベーションに失敗する場合は、トレンドマイクロのサポートにお問い合わせください。

表 15-1. 問題のトラブルシューティング (続き)

問題	説明、考えられる原因、対策
Web コンソールの問題	• テキストボックスに日本語を入力した後に Web コンソールが正しく表示されない場合は、ブラウザのエンコードをチェックしてください。Internet Explorer では、[表示] → [エンコード] の順にクリックして [UTF-8] を選択すると、Web ユーザインタフェースで中国語や日本語などの 2 バイト文字を正しく表示できます。 • Web コンソールが開かない場合は、InterScan VirusWall がインストールされているコンピュータを確認します。Web コンソールを開く前に、クエリキャッシュファイルを保存するための十分な領域を確保しておく必要があります。 • Web コンソールのパスワードを忘れた場合は、トレンドマイクロのテクニカルサポートへ連絡し、パスワードの再設定を要請してください。テクニカルサポートを受けることができるのは、登録済みのお客さまに限られます。InterScan VirusWall が登録されていない場合は、パスワードを回復できません。
InterScan VirusWall のコンポーネントに関する問題	•トレンドマイクロでは、検索エンジンおよびパターンファイルが自動アップデートされるように InterScan VirusWall を予約することを推奨しています。ただし、これらを手動でアップデートすることもできます。 • 左側のメニューで [アップデート] → [手動アップデート] の順に選択します。 • InterScan VirusWall が利用可能な新規コンポーネントを確認するまで待ちます。 • アップデート可能なエンジンおよびパターンファイルのリストが表示されます。このリストで、アップデートの必要なコンポーネントの横のチェックボックスをオンにします。 • [アップデート] をクリックします。 • 一部のプロセスで、コンポーネントのロールバックが無効になります。 • Web コンソールの [概要] 画面を開き、いずれかのプロセス (SMTP、POP3、HTTP、FTP) が無効になっていないかどうかを確認してください。また、Windows タスクマネージャ、または Process Explorer を開き、プロセスが実行しているかどうかを確認することもできます。ロールバック中にプロセスが実行されていない場合は、このプロセスではコンポーネントのロールバックが無効になることを意味します。

表 15-1. 問題のトラブルシューティング (続き)

問題	説明、考えられる原因、対策
プライマリ SMTP サーバで認証が必要となる場合に、InterScan VirusWall で認証が実行されないと、メールがキュー内で一時保管されます。	一般に、送信先で認証が要求される場合、InterScan VirusWall はメールをキューに保管しません。このメールは、「530 server needs authentication」のようなメッセージとともに送信者に返されます。また、認証を必要とする Exchange サーバにメールが転送された場合は、「454 server needs authentication」というメッセージが返されます。InterScan VirusWall はこれをエラーの発生と見なし、再試行回数の上限に達するまで再試行します。 InterScan VirusWall は認証をサポートしません。このため、メールサーバの認証機能を使用するには、Exchange サーバなどのメールサーバを InterScan VirusWall の前に配置する必要があります。SMTP VirusWall の配置の詳細については、34 ページの「インストールのトポロジ」を参照してください。
送信者または受信者への通知が機能していません。	- 通知機能が正しく設定されているかどうかを確認してください。268 ページの「通知設定」を参照してください。 - 設定がすべて正しいにもかかわらず、通知メッセージを受信できない場合は、通知サーバの設定を確認してください。初期設定では、InterScan VirusWall はローカルコンピュータの完全修飾ドメイン名を検知し、これを通知メールアドレスのドメイン名として使用します。どのドメインにも属していないローカルコンピュータの場合、InterScan VirusWall は通知メールアドレスとして <code>isvw@localdomain</code> を使用します。 この問題に対しては、2つの解決策があります。 - 通知サーバの有効なアドレスを指定します。詳細については、270 ページの「送信者のメールアドレスを置き換えるには」を参照してください。 - 通知サーバの信頼できる IP のリストに、InterScan VirusWall の IP アドレスを追加します。
いくつかの隔離ファイルが、隔離クエリの結果に含まれません。	HTTP または FTP トラフィックからの隔離ファイルは、クエリ結果テーブルに表示されません。これは、InterScan VirusWall が HTTP および FTP での隔離クエリをサポートしていないためです。 SMTP または POP3 トラフィックからの隔離ファイルがクエリ結果に含まれない場合は、クエリ期間の日時の設定を確認してください。隔離クエリでは、コンソールで最初に実行されたクエリの実行時間が記憶されます。ログオフせずに 2 度目のクエリを実行すると、実行期間が最初のクエリ期間のままとなり、新たに隔離されたアイテムが含まれなくなります。クエリ時間を変更して、クエリ期間全体が正しく指定されたことを確認してから、クエリを再実行してください。

表 15-1. 問題のトラブルシューティング (続き)

問題	説明、考えられる原因、対策
OKB のファイルが FTP ダウンロードフォルダに残っています。	これは、FTP トリクル機能の制限です。FTP トリクル機能を使用すると、接続タイムアウトを防止できます。ただし、クライアントでファイルが作成された後は、このファイルに対する処理が隔離または削除だったとしても、InterScan VirusWall がクライアントにこのファイルの削除を要求する手段はありません。
有効になっているにもかかわらず、一部のプロセスが実行されません。	システムログおよびイベントログを調べ、プロセスの初期化中に致命的エラーが発生していないかどうかを確認してください。ほとんどの場合、プロセスが実行できない原因はポートの競合です。この場合は、「SMTP: 特定のポートまたは IP アドレスをバインドできません」といったログが記録されます。 システムログまたはイベントログから必要な情報を得ることができない場合は、config.xml でデバッグログを有効にしてから、プロセスを再起動します。 デバッグログを有効にするには 1. config.xml ファイルを InterScan VirusWall のインストールフォルダで開きます。 2. 次のテキストを検索します。<Value Name="DebugEnabled" string="" type="int" int="0" /> 3. このテキストを次のように変更します。<Value Name="DebugEnabled" string="" type="int" int="1" /> 4. ファイルを保存して閉じてから、SMTP/POP3/HTTP/FTP プロセスのいずれか、または InterScan VirusWall サービス全体を再起動します。 これで、問題が再現され、ログフォルダからデバッグログの情報を取得できるようになります。
メールの送信時、または SMTP ポートへの接続時に、SMTP サーバが突然接続を終了します。	システムログまたはリアルタイム検索モニタを開き、エラーの有無を確認します。たとえば、システムログに「サーバエラーが発生しました。接続を受け付けられません。」と記録されている場合、またはリアルタイム検索モニタに「インバウンド (またはアウトバウンド) サーバエラー。InterScan Virus Wall は接続を許可しませんでした。」といったエラーが表示されている場合は、Web コンソールを開きます。 ここで、受信サーバ、送信サーバ、および通知サーバの設定が正しいかどうかを確認してください。

表 15-1. 問題のトラブルシューティング (続き)

問題	説明、考えられる原因、対策
Outlook Express 6.0 では、InterScan_SafeStamp.txt が安全ではない添付ファイルとして認識されます。	Outlook では、安全ではないファイルのリスト、および指定したファイルに対する [ダウンロード後に開く確認をする] 設定に基づき、ファイルが安全かどうか判断されます。 InterScan_SafeStamp.txt ファイルが安全な添付ファイルとして認識されるようにするには、[設定] → [コントロール パネル] → [フォルダ オプション] の順に選択して、[ファイルの種類] タブを選択し、「TXT」を選択します。次に、[詳細設定] をクリックして、新たに開いたウィンドウで [ダウンロード後に開く確認をする] をオフにします。
送受信メールのドメイン制御の設定方法	InterScan VirusWall には、送受信メッセージを制御するための 2 つの設定項目があります。 1. Web コンソールで、[SMTP] → [設定] の順に選択します。[送信メール] の下の項目 [1.] で、テキストボックスに IP アドレスを入力します。InterScan VirusWall ではすべてのメッセージがここに指定した IP アドレスから中継されます。 サポートされる IP アドレスの形式は次のとおりです。 - 192.168.5.* - 192.168.5.1-158 - 192.168.5.242 複数の IP アドレスを指定する場合は、次のようにセミコロン (;) で区切ります。 192.168.3.*;192.168.5.2;192.168.5.148-245 2. 指定された内部ドメイン宛てに送られたメールメッセージのみが受け入れられるように InterScan VirusWall を設定するには、[SMTP] → [設定] の順に選択します。[詳細設定] から [次のドメイン宛ての受信メールのみを許可して、リレーされたメッセージをブロックする] を選択し、テキストボックスにドメイン名を入力します。 複数のドメイン名を指定する場合は、セミコロンで区切って指定します。次に示すように、ドメイン名の先頭にワイルドカードを指定できます。 *.isvw.com;isvwbeta.com

表 15-1. 問題のトラブルシューティング (続き)

問題	説明、考えられる原因、対策
InterScan VirusWall のアンインストール後も、一部のフォルダが削除されません。	アンインストール中に開かれたままになっていたフォルダは削除されません。手動で削除してください。「ログ」フォルダおよび「隔離」フォルダは、アンインストール後も保持されます。
Helo コマンドが拒否されたという NDR メッセージをユーザが InterScan VirusWall から受け取ります。	HELO コマンドを受け取ったときにリモートメール転送エージェント (MTA) が完全修飾ドメイン名 (FQDN) を要求していると、ユーザは InterScan VirusWall から配信不能レポート (NDR) を受け取る場合があります。 この問題を解決するには、intscan.ini ファイルの DomainHostName キーの値を InterScan VirusWall コンピュータの FQDN 名に変更して、InterScan VirusWall を再起動します。
プロセスのクラッシュ時など、障害やエラーのログはどこで確認できるのでしょうか。	Windows のシステムログおよび InterScan VirusWall のシステムログを使用してください。 InterScan VirusWall のシステムログで、「終了処理中です ...」行を間に挟まずに 2 つの「初期化中です ...」行が続いている場合は、クラッシュの発生を意味します。 デバッグログが有効になっている場合は、デバッグログにさらに詳しい情報が含まれています。

表 15-1. 問題のトラブルシューティング (続き)

問題	説明、考えられる原因、対策
Trend Micro Control Manager (以下、Control Manager) - Control Manager Web コンソールから InterScan VirusWall にアクセスしようとするとエラーを受け取りま	InterScan VirusWall と Control Manager は互いに通信する場合、公開鍵を使用してセキュリティを確保します。Control Manager の IIS 設定により公開鍵がダウンロードできない場合、Control Manager Web コンソールから InterScan VirusWall デバイスにアクセスしようとするとエラーを受け取る場合があります。 Control Manager が公開鍵をダウンロードできるようにするには、次の手順に従います。 • IIS コンソールを開きます。 • 初期設定の Web サイトを右クリックして、状況依存メニューから [プロパティ] を選択します。 • [HTTP ヘッダー] タブを選択します。 • 実行している IIS のバージョンに応じて、ウィンドウの右下に [ファイルの種類] または [MIME の種類] というボタンが表示されます。ボタンをクリックすると、[ファイルの種類] 画面が表示されます。 • [ファイルの種類] 画面で [新しい種類] ボタンをクリックします。[ファイルの種類] ダイアログボックスが表示されます。 • [関連付けられている拡張子] フィールドに「.pem」と入力します。 • [コンテンツの種類 (MIME)] フィールドに「pem」と入力します。 • [OK] をクリックし [OK] を再度クリックします。最後にもう 1 度 [OK] をクリックします。 • これで問題が解決しない場合は、手動で Control Manager サーバ側にある (ディレクトリは <Control Manager サーバのディレクトリ>/WebUI/Download/SSO_PKI_Publickey.pem) SSO_PKI_Publickey.pem を手動で <InterScan VirusWall のディレクトリ>/CMAgent にコピーし、再試行します。

ドメインコントローラエージェントのデバッグ

ユーザグループポリシーに関する問題をトラブルシューティングする際には、ドメインコントローラエージェントのデバッグログをオンにします。デバッグログは有用であり、ユーザ / グループ機能のテクニカルサポートを受ける場合に必要です。

ドメインコントローラエージェントのデバッグを有効にする

ドメインコントローラエージェントのデバッグを有効にするには

1. ドメインコントローラエージェントプログラムを実行しているサーバにログオンします。
2. レジストリエディタを開くか、そのサーバのレジストリにリモートで接続します。
3. 次のレジストリ値にゼロ以外の値を割り当てます。
 - a. [スタート] → [ファイル名を指定して実行] の順に選択します。
 - b. 「regedit」と入力します。
 - c. HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥IdAgent¥に移動します。
 - d. DebugLevel をダブルクリックします。
 - e. 値のデータを 0 から 1 に変更します。
4. services.msc を実行して TMIdAgent を選択し、[再起動] () をクリックして、ドメインコントローラエージェントサービスを停止してから再起動します。
5. ドメインコントローラエージェントのインストールフォルダでデバッグログファイル (IdAgentDebug.log) を見つけます。

コンソールモード

ドメインコントローラエージェントのデバッグログを有効にすることに加えて、エージェントをコンソールモードで実行できます。エージェントプログラムがコンソールモードで実行されている場合、コンソール画面にはログオンユーザとデバッグメッセージが表示されます。コンソールモードは、エージェントの接続に関する問題の診断に役立ちます。要求と応答のログをすぐに確認できます。図 15-1 に、コンソールモードのインタフェースを示します。

図 15-1. コンソールモードで実行されているドメインコントローラエージェント

```

IdAgent Service Console ( Quit with Ctrl+C )
2009-08-13T15:29:37+-900 <4896-3824> Agent version is [1.0.0.1086]
2009-08-13T15:29:37+-900 <4896-3824> Agent is listening on port [65015]
2009-08-13T15:29:37+-900 <4896-3824> Minimum agent client version [1.0.0.1076]
2009-08-13T15:29:37+-900 <4896-3824> Auto-discover is [enabled]
2009-08-13T15:29:37+-900 <4896-3824> UID cache TTL is [15] minutes
2009-08-13T15:29:37+-900 <4896-3824> Uid server started
2009-08-13T15:29:37+-900 <4896-3824> Agent soap server started
2009-08-13T15:29:37+-900 <4896-3824> Failed to login with account [isvw71¥admini
strator], err = 1326
2009-08-13T15:29:37+-900 <4896-3824> Logon as new user [isvw71¥administrator]
2009-08-13T15:29:37+-900 <4896-3824> GC RootDSE binded
2009-08-13T15:29:37+-900 <4896-3824> [DiscoverSiteDCs] Started
2009-08-13T15:29:37+-900 <4896-3824> [DiscoverDC] Added [isvw701.ISVW71.com]
2009-08-13T15:29:37+-900 <4896-3824> [DiscoverDC] Added [isvw702.sub2.ISVW71.com
]
2009-08-13T15:29:37+-900 <4896-3824> [DiscoverSiteDCs] Done
2009-08-13T15:29:37+-900 <4896-3824> Uid DC servers (count = 2) set
  
```

コンソールモードを開始するには

1. 実行されているドメインコントローラエージェントサービスを停止します。
2. トレンドマイクロのドメインコントローラエージェントのインストールディレクトリで、DebugMode ショートカットをダブルクリックします。
初期設定のディレクトリは、C:\Program Files\Trend Micro\IdAgent¥です。
3. [Ctrl+C] キーを押して、実行されているコンソールを終了します。

ドメインコントローラエージェント、Active Directory、およびユーザ識別のトラブルシューティング

ここでは、次のトピックについて説明します。

- 「ドメインコントローラエージェントのインストールまたはサービスでのエラー」
- 「ドメインコントローラエージェントの接続」
- 「ドメインコントローラサーバの接続」

ドメインコントローラエージェントのインストールまたはサービスでのエラー

ドメインコントローラエージェントは、ドメインにインストールする必要があります。また、インストールには管理者権限が必要です。ほとんどの場合、ドメインコントローラエージェントは、ドメインコントローラサーバにインストールします。これにより、ドメインコントローラエージェントがドメインコントローラサーバにアクセスするために別の資格情報を割り当てる必要がなくなります。ただし、ドメインコントローラエージェントを、ドメインに属する別のサーバにインストールすることもできます。

ドメインコントローラエージェントのインストールに関する問題をトラブルシューティングする前に、次の点を確認してください。

- サポートされている OS であること。ドメインコントローラエージェントは、Windows Server 2000、Windows Server 2003、Windows Server 2008、Windows 2000 Pro、および Windows XP にインストールできます。
- エージェントインストールプログラム (MSI) を起動するためのローカル管理者権限を持っていること。
- 以前のバージョンのドメインコントローラエージェントがある場合は、[コントロール パネル] の [プログラムの追加と削除] からそれを削除すること。

ドメインコントローラエージェントの接続

ドメインコントローラエージェントサービスは「Trend Micro IdAgent」と表示されます。サービス名は「TMIDAgent」です。ドメインコントローラエージェントをサーバにインストールすると、`services.msc` コマンドからサービスの実行を確認できます。

ドメインコントローラエージェントをインストールして起動すると、InterScan VirusWall はエージェントにアクセスできるようになり、エージェントはユーザ識別要求に応答できるようになります。

ドメインコントローラサーバを設定するには、300 ページの「ドメインコントローラサーバの接続」を参照してください。

表 15-2 は、ドメインコントローラエージェントに関する問題について、発生する可能性のあるエラー、考えられる原因、および可能な解決策を示しています。

表 15-2. ドメインコントローラエージェントに関する問題

エラー	考えられる原因	可能な解決策または診断の手順
ホストまたは IP アドレスが無効です	不適切なエージェントアドレスが指定されている。	- エージェントのホスト名または IP アドレスとポート番号を確認します。 - ホスト名を使用している場合は、InterScan VirusWall で DNS が機能していることを確認します。
バージョンはサポートされていません	InterScan VirusWall で新しいバージョンのエージェントが必要である。	InterScan VirusWall の Web コンソールからエージェントをダウンロードして、対象サーバに再インストールします。詳細については、275 ページの「ドメインコントローラエージェントをインストールする」を参照してください。
その他のエラー	予期しないエラー	- ドメインコントローラエージェントのデバッグを有効にします。294 ページの「ドメインコントローラエージェントのデバッグを有効にする」を参照してください。 - ログファイルをトレンドマイクロのサポートに送信します。

表 15-2. ドメインコントローラエージェントに関する問題 (続き)

エラー	考えられる原因	可能な解決策または診断の手順
接続できませんで した	- ファイアウォールが接続をブロックした。 - サービスが停止している。	- ドメインコントローラエージェントのコンピュータにファイアウォールが設定されている場合は、受信 TCP ポート 65015 を除外リストに追加してください。 - サーバが動作していることを確認します。 - エージェントのホスト名または IP アドレスとポート番号を確認します。 - ホスト名を使用している場合は、InterScan VirusWall で DNS が機能していることを確認します。
接続は拒否されま した	- エージェントがアクセスルールの設定に基づいて要求を拒否した。 - ファイアウォールがドメインコントローラサーバの RPC をブロックした。	エージェントは、ID または IP アドレスがアクセスリストにないクライアントには応答しません。エージェントが最初に起動したとき、エージェントのアクセスリストは空です。最初に登録されたクライアントがエージェントを占有し、このエージェントへのアクセスを許可するその他のクライアントを決定します。別の InterScan VirusWall を登録する方法の 1 つとして、フェイルオーバーデバイスの設定があります。ただし、常に、エージェント側でアクセスリストを手動で設定できます。 アクセスリストを手動で設定するには、次の手順を実行します。 1. 管理者アカウントを使用して、ドメインコントローラエージェントのサーバコンピュータにログオンします。 2. エージェントのインストールフォルダ C:\Program Files\Trend Micro\IdAgent\ を参照します。 3. IdAgent.ini という名前のエージェント設定 INI ファイルを見つけて開きます。 4. [ClientList] セクションで、次の形式の値のペア (キーと値) が含まれる新しい行を追加します。

表 15-2. ドメインコントローラエージェントに関する問題 (続き)

エラー	考えられる原因	可能な解決策または診断の手順
		<Your-Temp-ID>=<host:port> 0 ここで • <Your-Temp-ID> = xxxx など任意の一意のキー名。既存の文字列とは異なるキー名を指定する必要があります。 • <host:port> 0 = ドメインコントローラエージェントのサーバの IP アドレスおよびポート番号。後ろにパイプ文字とゼロ (0) が続きます。 例: [ClientList] ?????=192.168.1.1:65014 0 一時クライアント ID は一意である必要があります。一意でない場合、既存の ID に取って代わります。初期設定のポートは、65014 です。 5. エージェントサービスを再起動します。 • ドメインコントローラサーバのファイアウォールを確認し、受信 TCP ポート 445 を除外リストに追加してください。
I/O に失敗しました	ネットワークエラー	ネットワーク接続を確認します。
初期設定のドメインコントローラまたはグローバルカタログが見つかりません	• エージェントがインストールされているコンピュータが Active Directory ドメインに属していない。 • エージェントが Vista 以前のシステムにインストールされており、Active Directory サーバは Windows Server 2008 上にある。	• コンピュータを Active Directory ドメインに追加します。 • ドメインコントローラエージェントを Windows Server 2008 にインストールします。

表 15-2. ドメインコントローラエージェントに関する問題 (続き)

エラー	考えられる原因	可能な解決策または診断の手順
ドメインコントローラが接続されていません	ドメインコントローラエージェントが Active Directory でドメインコントローラサーバを検索している。	数分間待機してから、再度実行してください。
ログオンできませんでした	[ユーザ ID 設定] 画面に入力されたユーザ名とパスワードが正しくない。	・ [ドメインコントローラサーバの資格情報] で、[管理] → [ユーザ ID 設定] の順に選択して表示される、エージェントで現在使用されているユーザ名を確認します。 ・ 正しいユーザ名とパスワードを入力します。

ドメインコントローラサーバの接続

エージェントでユーザ識別を実行できるようにドメインコントローラサーバを設定する必要があります。ドメインコントローラサーバのリストによって、ドメインコントローラエージェントで監視する認証サーバが指定されます。ユーザログオン情報はすべてこれらのサーバから取得されます。ドメインコントローラサーバが設定されていないと、ドメインコントローラエージェントではそのサーバからのユーザ情報が検出されません。

ドメインコントローラサーバを設定するには

1. InterScan VirusWall の Web コンソールを開きます。
2. [管理] → [ユーザ ID] の順に選択します。
3. [ユーザ ID 設定] 画面で、次のタスクを実行します。
 - ・ ドメインコントローラエージェントを追加します (277 ページの「InterScan VirusWall にドメインコントローラエージェントを追加する」を参照)。
 - ・ 設定を保存します。
 - ・ ドメインコントローラエージェントのステータスを確認します。
4. ドメインコントローラサーバの資格情報を指定します (279 ページの「ドメインコントローラサーバの資格情報を追加する」を参照)。
5. 約 30 秒待機してから画面の表示を更新します。

ドメインコントローラエージェントおよびサーバの両方が緑になります。これは、エージェントでユーザ識別要求に応答する準備ができたことを示します。

接続エラーが発生した場合は、図 15-2 に示すように、マウスポインタを置いたときに表示されるツールヒントに詳細なメッセージが表示されます。

図 15-2. 接続エラーメッセージ



ドメインコントローラサーバの自動検出

ドメインコントローラサーバは手動で追加することはできません。ドメインコントローラサーバは、InterScan VirusWall の自動検出メカニズムによって自動的に追加されます。この機能によって、エージェントでは同一サイトのドメインコントローラサーバを検出して評価できます。自動検出によってエラーが解消されます。

ドメインコントローラサーバには、Active Directory への接続およびドメインコントローライベントログの表示を実行するための適切な権限が必要です。エージェントに適切なドメイン資格情報を与える必要があります。エージェントに適切な権限がないと、Active Directory を使用して適切なドメインコントローラサーバを検出できません。

自動検出に関する問題については、ドメインコントローラエージェントの権限を確認してください。

接続

[ユーザ ID 設定] 画面に表示されるドメインコントローラサーバは、正しく設定されている場合、動作可能として表示されます。エラーが発生した場合は、図 15-2 のドメインコントローラエージェントのエラーのように詳細が表示されます。

表 15-3 は、発生する可能性のあるエラーと考えられる原因を示しています。

図 15-3. ドメインコントローラサーバの接続に関する問題の診断と解決

エラー	考えられる原因	可能な解決策または診断の手順
その他のエラー	予期しないエラー	- ドメインコントローラエージェントのデバッグを有効にします。294 ページの「ドメインコントローラエージェントのデバッグを有効にする」を参照してください。 - ログファイルをトレンドマイクロのサポートに送信します。
接続できませんでした	- ファイアウォールが接続をブロックした。 - サービスが停止している。	- ドメインコントローラサーバにファイアウォールが設定されている場合は、受信 TCP ポート 135 および 445 を除外リストに追加してください。 - サーバが動作していることを確認します。

図 15-3. ドメインコントローラサーバの接続に関する問題の診断と解決 (続き)

エラー	考えられる原因	可能な解決策または診断の手順
接続は拒否されました	- エージェントに、ドメインコントローラサーバのイベントログを表示するための適切なアクセス権がない。 - ファイアウォールがドメインコントローラサーバの RPC をブロックした。	[ドメインコントローラサーバの資格情報] で、[管理] → [ユーザ ID 設定] の順に選択して表示される、エージェントで現在使用されているユーザ名を確認します。 - エージェントが適切なアクセス権で実行されていることを確認します。 - 必要に応じてログオンユーザを変更します。 - イベントビューアを使用して、アクセス権に問題があるのかどうかを判別します。 - 問題がアクセス権にあるかどうかを判別するには、ドメインコントローラエージェントの資格情報を使用してドメインコントローラエージェントのサーバにログオンし、イベントビューア (eventvwr.msc) を開き、ドメインコントローラサーバへの接続を試行してアクセスできるかどうかを確認します。 - ドメインコントローラサーバのファイアウォールを確認し、受信 TCP ポート 445 を除外リストに追加してください。
I/O に失敗しました	ネットワークエラー	ネットワーク条件を確認します。

図 15-3. ドメインコントローラサーバの接続に関する問題の診断と解決 (続き)

エラー	考えられる原因	可能な解決策または診断の手順
ログオンイベントが検出されませんでした	ログオン監査がドメインコントローラサーバで無効になっている。	アカウントログオンイベントの監査を有効にして、接続または権限以外の問題がないか調べるには、次の手順を実行してください。 1. [スタート] → [コントロール パネル] → [管理ツール] の順に選択します。 2. [ドメイン コントローラ セキュリティ ポリシー] をクリックします。 3. 左側の画面で [ローカル ポリシー] を開き、[監査ポリシー] を選択します。 4. [アカウント ログオン イベントの監査] が有効になっていることを確認します。
ログオンイベントの設定が正しくありません	イベントログのサイズと上書きの設定が正しくない。	適切なイベントログのサイズを設定して、イベントログの上書きを有効にします。
クライアントの検証に失敗しました	・ ドメインコントローラエージェントにクライアントコンピュータへのアクセス権がない。 ・ クライアントのファイアウォールが RPC をブロックしている。	・ ドメインコントローラエージェントに現在の資格情報を提供します。 ・ クライアントのファイアウォール設定を確認し、受信 TCP ポート 445 を除外リストに追加してください。
ステータスが保留になっています	資格情報の変更やドメインコントローラサーバの再検出など、新しい設定をメインコントローラエージェントに適用するにはしばらく時間がかかります。	画面の表示を更新します。

Windows Active Directory によるユーザ / グループの検索

Active Directory のユーザ / グループ検索機能では、ユーザ ID 設定が正しく設定されている必要があります。

AD/LDAP 検索機能をトラブルシューティングするには

1. [管理] → [ユーザ ID 設定] 画面で、[IP アドレスとリモートエージェント経由のユーザ / グループ] オプションがオンになっていることを確認します。図 15-2 を参照してください。
2. ドメインコントローラエージェントおよびドメインコントローラサーバが正しく設定されていること、および [管理] → [ユーザ ID 設定] 画面にエージェントおよびサーバのエラーメッセージが表示されていないことを確認します。エラーが表示されている場合は、前述のセクションで示している解決策からそのエラーメッセージに適合するものを見つけます。解決策の一覧については、表 15-2 および図 15-3 を参照してください。
3. ドメインコントローラエージェントおよびドメインコントローラサーバが機能しているにもかかわらず、検索結果を取得できない場合は、ドメインコントローラエージェントのデバッグログを有効にして、検索要求が正しく処理されているかどうかを確認します。294 ページの「ドメインコントローラエージェントのデバッグを有効にする」を参照してください。Active Directory Service Interfaces Editor (ADSI Edit) を使用して、検索に有効な結果が含まれていることを確認することもできます。
4. クライアントのタイムアウト値を確認します。初期設定のタイムアウト値は 10 秒です。この値を変更するには、InterScan VirusWall で、< インストールディレクトリ >¥http¥conf にある IdLib.ini ファイルの AcceptTimeoutSecs=10 パラメータを編集します。
RecvTimeoutSecs パラメータによって、InterScan VirusWall が検索結果を待機する時間が定義されます。

InterScan VirusWall のデバッグを有効にする必要があります。また、必要に応じてデバッグログをトレンドマイクロのサポートに送信してください。294 ページの「ドメインコントローラエージェントのデバッグを有効にする」を参照してください。

ユーザ識別

ユーザ識別は、ユーザ / グループポリシー機能の使用時に重要です。ユーザ識別に関する問題をトラブルシューティングする場合、詳細を確認するために、InterScan VirusWall 側およびドメインコントローラエージェント側の両方でデバッグを有効にする必要があります。

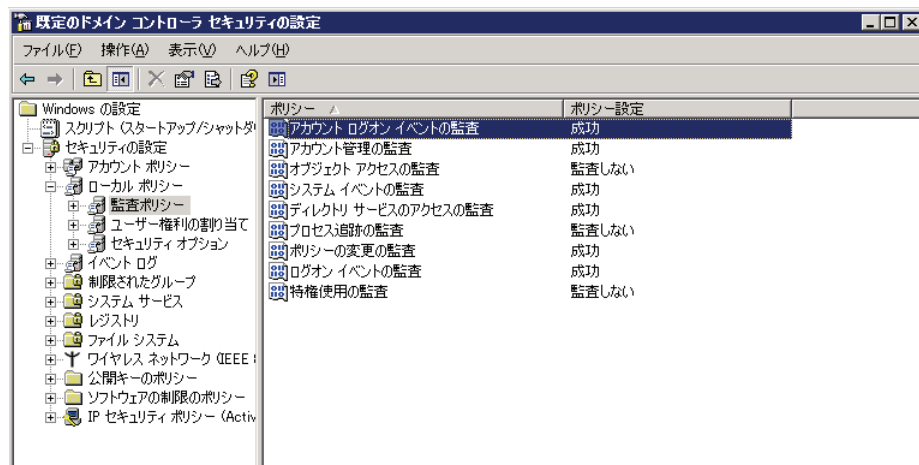
ユーザ識別に関する問題を診断するには

1. [管理] → [ユーザ ID 設定] の順に選択します。
2. ドメインコントローラエージェントおよびドメインコントローラサーバが正しく設定されていることを確認します。

エラーが発生している場合は、トラブルシューティングのための解決策として表 15-2 および図 15-3 を参照してください。

3. アカウントログオンイベントの監査を有効にして、接続または権限以外の問題を検出します。
 - a. [スタート] → [コントロール パネル] → [管理ツール] の順に選択します。
 - b. [ドメイン コントローラ セキュリティ ポリシー] をクリックします。
 - c. 左側の画面で [ローカル ポリシー] を開き、[監査ポリシー] を選択します。
 - d. [アカウント ログオン イベントの監査] が有効になっていることを確認します。図 15-4 を参照してください。

図 15-4. 有効になっているログオンアカウントの監査



データを収集してトレンドマイクロのサポートに送信する

トレンドマイクロのテクニカルサポートに問い合わせる前に、必ず、ドメインコントローラエージェントのデバッグログおよび InterScan VirusWall HTTP デーモンのデバッグログを収集してください。詳細については、294 ページの「ドメインコントローラエージェントのデバッグ」を参照してください。

製品サポート情報

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

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

サポートサービスについて

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

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

契約の有効期限は、ユーザ登録完了から 1 年間です（ライセンス形態によって異なる場合があります）。契約を更新しないと、パターンファイルや検索エンジンの更新などのサポートサービスが受けられなくなりますので、契約満了前に必ず更新してください。更新手続きの詳細は、トレンドマイクロの営業部、または販売代理店までお問い合わせください。

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

製品 Q&A のご案内

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

製品 Q&A

<http://esupport.trendmicro.co.jp/corporate/search.aspx>

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

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

セキュリティ情報

セキュリティ情報の入手先

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

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

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

セキュリティ情報 Web サイトでは、次の情報を閲覧できます。

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

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

トレンドマイクロへのウイルス解析依頼

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

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

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

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

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

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

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

ウイルス解析サポートセンター「TrendLabs」

トレンドマイクロのウイルス解析サポートセンター「TrendLabs」(トレンドラボ) は、フィリピンセンターを本部として、米国、日本、台湾、ドイツ、アイルランド、中国、フランス、メキシコの各国センターで構成されています。24 時間体制でウイルスの活動を監視するウイルス解析エンジニアを含む 1000 名以上のスタッフが、セキュリティに関する最新の情報を収集し、高品質なサービスとソリューションを迅速かつ効果的に世界各国のトレンドマイクロのパートナーとお客さまに提供しています。

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

システムチェックリスト

この付録のチェックリストを使用し、参照として関連システム情報を記録します。

サーバアドレスのチェックリスト

Trend Micro InterScan VirusWall スタンダードエディション（以下、InterScan VirusWall）をインストールする際、およびネットワークで使用するよう設定する際に、次のサーバアドレス情報を入力する必要があります。簡単に参照できるように、これらの情報をここに記録します。

表 A-1. サーバアドレスのチェックリスト

必須情報	例	ユーザの値
InterScan VirusWall のサーバ情報		
IP アドレス	10.1.104.255	
完全修飾ドメイン名 (FQDN)	server.company.com	
NetBIOS (ホスト) 名	yourserver	
コンポーネントのダウンロードに使用するプロキシサーバ		
IP アドレス	10.1.174.225	

表 A-1. サーバアドレスのチェックリスト (続き)

必須情報	例	ユーザの値
完全修飾ドメイン名 (FQDN)	proxy.company.com	
NetBIOS (ホスト) 名	proxyserver	
通知サーバ情報		
IP アドレス	10.1.123.225	
完全修飾ドメイン名 (FQDN)	mail.company.com	
NetBIOS (ホスト) 名	mailserver	

ポートのチェックリスト

InterScan VirusWall では、次のポートを使用します。

表 A-2. ポートのチェックリスト

ポート	例	ユーザの値
SMTP	25	
POP3	110	
HTTP	8080	
FTP	21	
Web コンソール	9240	
Web コンソール (SSL)	9241	

サポートされているコマンド

SMTP

InterScan VirusWall の SMTP モジュールでは、ESMTP コマンド (size 以外) および SMTP SSL はサポートされていません。

表 A-3. サポートされている SMTP コマンド

コマンド名	説明
HELO	helo: グリーティング
MAIL	mail: 送信者の指定
RCPT	rcpt: 受信者の指定
DATA	data: メッセージテキストの送信
RSET	rset: 状態のリセット
HELP	help: 使用方法に関する情報の要求
NOOP	noop: 何も実行しない
QUIT	quit: 接続の終了
SAML	saml: send AND mail の実行
SOML	soml: send OR mail の実行
EHLO	SMTP 拡張 hello コマンド

FTP

InterScan VirusWall は、一般的な FTP サーバおよびクライアントでサポートされている、ほとんどの FTP コマンドをサポートしています。既知のサポートされていないコマンドは、STOU です。

Store unique が on の場合、FTP の put コマンドは実装されません。

互換性に関する既知の問題

- Linux システムで Kerberos 認証を使用して FTP サイトにログオンするときの問題
- FTP ユーザ通知が、InterScan VirusWall サーバからの FTP 接続切断の原因となる問題
- FTP ウイルス / スパイウェア通知がクライアントの NetAnts に表示されない問題

POP3

サポートされている POP3 コマンドには、CAPA、AUTH のほか、RFC 1939 で指定されているすべてのコマンドが含まれます。POP3 SSL はサポートされていません。

表 A-4. サポートされている POP3 コマンド

コマンド名	説明	RFC
CAPA	サポート機能の一覧表示	RFC 2449
APOP	MD5 を使用したログオン	RFC 1939
AUTH	Exchange サーバ用	RFC 1734/3206
USER	ユーザ名の送信	RFC 1939
PASS	パスワードの送信	RFC 1939
QUIT	セッションの終了	RFC 1939
STAT	メールボックスのステータスの一覧表示	RFC 1939
LIST	メールの情報の一覧表示	RFC 1939
UIDL	メールの UID の一覧表示	RFC 1939
TOP	メールのヘッダ情報の取得	RFC 1939
RETR	メールの取得	RFC 1939
DELE	メールを削除済みとしてマーク	RFC 1939
RSET	削除済みメールのマーク解除	RFC 1939
NOOP	何も実行しない	RFC 1939

初期設定値

Trend Micro InterScan VirusWall スタンダードエディション (以下、InterScan VirusWall) Web コンソールにはさまざまなオプションが用意されており、これらのオプションを使用すると、ユーザは指定内容に従って簡単に InterScan VirusWall を設定できます。

この付録では、InterScan VirusWall の設定ファイル (`intscan.ini` および `config.xml`) を変更する必要が生じた場合の参照情報を提供します。初期設定値によっては、対応する値から派生しているか、または対応する値に依存しているため、直接変更できないものがあります。関連した状況を考慮せずにこのような値を変更すると、無効な設定や予期しない結果を引き起こす可能性があります。

注意： 設定ファイルを編集する前にバックアップを作成することをお勧めします。

この付録には、InterScan VirusWall の設定オプションのリストが含まれています。各パラメータについて、説明、初期設定値、その他の指定可能な値のリスト、およびそれら指定可能な値の説明を示します。

SMTP ウイルス / スパイウェア /IntelliTrap および設定

パラメータ	初期設定値	指定可能な値	説明
intscan.ini [common] NotificationFromAddress	isvw@FQDN	任意のメールアドレス	SMTP プロトコルおよび FTP プロトコルの場合に、InterScan VirusWall 通知の [送信者] フィールドに表示されます。
intscan.ini [Scan-Configuration] MailScan	Yes	Yes、No	Yes: 検索はオン。 No: このアイテムがオフの場合、検索はオフ。ウイルス / スパイウェア /IntelliTrap 検索はすべて無効になります。
Intscan.ini [EMail-Scan] MaxScanningThreadsProc	25		プロセッサあたりの検索メッセージ数を制限します。
Intscan.ini [EMail-Scan] MaxSMTPClient-ThreadsProc	50		検索後メール配信のために作成されるスレッドの数を制限します。
Intscan.ini [EMail-Scan] BackgroundMqueueInThreadsProc	2		検索後 mqueue 内の受信メールを配信するために作成される、プロセッサあたりのバックグラウンドスレッドの固定数。 mqueue をバックアップする場合、この数を増やせます。

パラメータ	初期設定値	指定可能な値	説明
Intscan.ini [EMail-Scan] BackgroundMqueueOutThreadsProc	2		検索後 mqueue 内の送信メールを配信するために作成される、プロセッサあたりのバックグラウンドスレッドの固定数。
Intscan.ini [EMail-Scan] BackgroundBMqueueThreadsProc	1		bmqueue 内の InterScan VirusWall 生成メッセージを配信するためのスレッドの固定数
Intscan.ini [EMail-Scan] MaxClientConnections	25		InterScan VirusWall で受け入れられる同時接続の最大数
Intscan.ini [EMail-Scan] DisableReceivedHeader	No		
Intscan.ini [EMail-Scan] InterScanSMTPServicePort	25		
Intscan.ini [EMail-Scan] InboundUseDNS	Yes	Yes、No	
Intscan.ini [EMail-Scan] OutboundUseDNS	Yes	Yes、No	
Intscan.ini [EMail-Scan] EOrg		IP アドレス	SMTP サーバの受信メール用 IP アドレス
Intscan.ini [EMail-Scan] EOrgPort	25		SMTP サーバの受信メール用ポート
Intscan.ini [EMail-Scan] NotificationSMTPAddr	default	初期設定値または IP アドレス	通知サーバの IP アドレス

パラメータ	初期設定値	指定可能な値	説明
Intscan.ini [EMail-Scan] NotificationSMTPPort	25	1 ～ 65535 の任意の数値	通知サーバのポート
Intscan.ini [EMail-Scan] InterScanSMTPServiceIP		IP アドレス	
Intscan.ini [EMail-Scan] OutboundMailScan	Yes	Yes、No	送信メール検索処理を有効または無効にします。
Intscan.ini [EMail-Scan] OutboundMailVirusScan	Yes	Yes、No	送信メールのウイルス検索を有効または無効にします。
Intscan.ini [EMail-Scan] OutboundMailClientIP		IP アドレス	
Intscan.ini [EMail-Scan] OutboundMailSMTPAddr			SMTP サーバの送信メール用 IP アドレス
Intscan.ini [EMail-Scan] OutboundMailSMTPPort	25	1 ～ 65535 の数値	SMTP サーバの送信メール用ポート
Intscan.ini [EMail-Scan] DeliveryMaxHours	24		
Intscan.ini [EMail-Scan] DeliveryRetryMinutes	1		
Intscan.ini [EMail-Scan] ScanExtensions			ユーザが Level を scanExt に設定した場合に検索される受信の拡張子
Intscan.ini [EMail-Scan] OutgoingScanExtensions			ユーザが Level を scanExt に設定した場合に検索される送信の拡張子

パラメータ	初期設定値	指定可能な値	説明
Intscan.ini [EMail-Scan] Level	ScanAll	ScanAll、ScanExt、 IntelliScan	
Intscan.ini [EMail-Scan] OutgoingLevel	ScanAll	ScanAll、ScanExt、 IntelliScan	
Intscan.ini [EMail-Scan] EMail	Yes	Yes、No	受信メッセージ内で ウイルスが検出され た場合に、管理者に 通知を送信するかど うかを指定します。
Intscan.ini [EMail-Scan] Addr		メールアドレス	ウイルス / スパイ ウェア / IntelliTrap の 検出時に、管理者が 通知を受信するた めに使用するメール アドレス
Intscan.ini [EMail-Scan] Message1	%SENDER% から %RCPTS% に送信され たメッセージにおい てウイルスまたは不 正プログラムが検出 されました。メッ セージの件名は 「%SUBJECT%」です。 InterScan VirusWall は、 %FINALACTION% の 処理を実行しました。		受信メッセージ内で ウイルスが検出され た場合に管理者に送 信されるメッセージ の内容
Intscan.ini [EMail-Scan] EWarning	No	Yes、No	受信メッセージ内で ウイルスが検出され た場合に、受信者に 通知を送信するかど うかを指定します。

パラメータ	初期設定値	指定可能な値	説明
Intscan.ini [EMail-Scan] EMessage	警告 : InterScan VirusWall は、%SENDER% から送信されたメッセージにおいてウイルスを検出しました。メッセージの件名は「%SUBJECT%」です。メッセージは配信されない場合があります。		受信メッセージ内でウイルスが検出された場合に受信者に送信されるメッセージの内容
Intscan.ini [EMail-Scan] EWarningSender	No	Yes、No	受信メッセージ内でウイルスが検出された場合に、送信者に通知を送信するかどうかを指定します。
Intscan.ini [EMail-Scan] EMessageSender	警告 : InterScan VirusWall は、お使いのコンピュータから %RCPTS% に送信されたメッセージにおいてウイルスを検出しました。メッセージの件名は「%SUBJECT%」です。メッセージは配信されない場合があります。		受信メッセージ内でウイルスが検出された場合に送信者に送信されるメッセージの内容
Intscan.ini [EMail-Scan] Stamp	No	Yes、No	受信メッセージにウイルス検出なしのメッセージを追加するかどうかを指定します。
Intscan.ini [EMail-Scan] StampMessage	InterScan VirusWall は、このメッセージにおいてウイルス検索を実行し、既知のウイルスは検出されませんでした。		ウイルスが検出されなかった受信メッセージに追加されるメッセージの内容

パラメータ	初期設定値	指定可能な値	説明
Intscan.ini [EMail-Scan] VirusMessage	No	Yes、No	受信メッセージにウイルス検出ありのメッセージを追加するかどうかを指定します。
Intscan.ini [EMail-Scan] VirusMessageText	InterScan VirusWall は、このメッセージ においてウイルスを 検出しました。		ウイルスが検出された場合に受信メッセージに追加されるメッセージの内容
Intscan.ini [EMail-Scan] StampOutGoing	No	Yes、No	送信メッセージにウイルス検出なしのメッセージを追加するかどうかを指定します。
Intscan.ini [EMail-Scan] StampMessageOutGoing	InterScan VirusWall は、このメッセージ においてウイルス検 索を実行し、既知の ウイルスは検出され ませんでした。	文字列	ウイルスが検出されなかった送信メッセージに追加されるメッセージの内容
Intscan.ini [EMail-Scan] VirusMessageOutGoing	No	Yes、No	送信メッセージにウイルス検出ありのメッセージを追加するかどうかを指定します。
Intscan.ini [EMail-Scan] VirusMessageTextOutGoing	InterScan VirusWall は、このメッセージ においてウイルスを 検出しました。	文字列	ウイルスが検出された場合に送信メッセージに追加されるメッセージの内容
Intscan.ini [EMail-Scan] EnableOutgoingNotiToAdmin	Yes	Yes、No	送信メッセージ内でウイルスが検出された場合に、管理者に通知を送信するかどうかを指定します。

パラメータ	初期設定値	指定可能な値	説明
Intscan.ini [EMail-Scan] MsgOutgoingNotiToAdmin	%SENDER% から %RCPTS% に送信され たメッセージにおい てウイルスまたは不正 プログラムが検出 されました。メッ セージの件名は 「%SUBJECT%」です。 InterScan VirusWall は、 %FINALACTION% の 処理を実行しました。	文字列	送信メッセージ内で ウイルスが検出され た場合に管理者に送 信されるメッセージ の内容
Intscan.ini [EMail-Scan] EnableOutgoingNotiToRecipient	No	Yes、No	送信メッセージ内で ウイルスが検出され た場合に、受信者に 通知を送信するかど うかを指定します。
Intscan.ini [EMail-Scan] MsgOutgoingNotiToRecipient	警告 : InterScan VirusWall は、 %SENDER% から送信 されたメッセージに おいてウイルスを検 出しました。メッ セージの件名は 「%SUBJECT%」です。 メッセージは配信さ れない場合があります。	文字列	送信メッセージ内で ウイルスが検出され た場合に受信者に送 信されるメッセージ の内容
Intscan.ini [EMail-Scan] EnableOutgoingNotiToSender	No	Yes、No	送信メッセージ内で ウイルスが検出され た場合に、送信者に 通知を送信するかど うかを指定します。

パラメータ	初期設定値	指定可能な値	説明
Intscan.ini [EMail-Scan] MsgOutgoingNotiToSender	警告 : InterScan VirusWall は、お使い のコンピュータから %RCPTS% に送信され たメッセージにおい てウイルスを検出し ました。メッセージ の件名は 「%SUBJECT%」です。 メッセージは配信さ れない場合があります。	文字列	送信メッセージ内で ウイルスが検出され た場合に送信者に送 信されるメッセージ の内容
Intscan.ini [EMail-Scan] Action	autoclean	Pass、move、delete、 autoclean、blockmsg	ウイルスが検出され た受信メッセージに 対して実行される処 理
Intscan.ini [EMail-Scan] OutgoingAction	autoclean	Pass、move、delete、 autoclean、blockmsg	ウイルスが検出され た送信メッセージに 対して実行される処 理
Intscan.ini [EMail-Scan] UncleanedFileRecipientAction	Delete	Pass、move、delete	ウイルス駆除不能な 受信ファイルに対す る処理
Intscan.ini [EMail-Scan] OutgoingUncleanedFileRecipient Action	Delete	Pass、move、delete	ウイルス駆除不能な 送信ファイルに対す る処理
Intscan.ini [EMail-Scan] InESMTPSIZE	0		受信メッセージの最 大サイズ (0 は無制 限)
Intscan.ini [EMail-Scan] OutESMTPSIZE	0		送信メッセージの最 大サイズ (0 は無制 限)
Intscan.ini [EMail-Scan] RestrictInDomain	Yes	Yes、No	指定したドメインか らの受信メッセージ のみを受け入れます。

パラメータ	初期設定値	指定可能な値	説明
Intscan.ini [EMail-Scan] RestrictInDomainList	ユーザ指定		受け入れるドメインのリスト
Intscan.ini [EMail-Scan] QuarantineOfficeMacros	No	Yes、No	マクロを含む受信 Microsoft Office ドキュメントを隔離するかどうかを指定します。
Intscan.ini [EMail-Scan] OutgoingQuarantineOfficeMacros	No	Yes、No	マクロを含む送信 Microsoft Office ドキュメントを隔離するかどうかを指定します。
Intscan.ini [EMail-Scan] Greeting	Welcome to InterScan VirusWall SMTP service!		ユーザが SMTP ポートに接続したときに表示されるグリーティングメッセージ
Intscan.ini [EMail-Scan] EnableGreeting	Yes	Yes、No	カスタマイズしたグリーティングメッセージを送信します。
Intscan.ini [EMail-Scan] DecompressionLayerLimit	14	1~20	特定の条件を満たすファイルのみを検索するよう設定されている場合の、受信圧縮ファイルの最大検索階層数
Intscan.ini [EMail-Scan] OutgoingDecompressionLayerLimit	14	1~20	特定の条件を満たすファイルのみを検索するよう設定されている場合の、送信圧縮ファイルの最大検索階層数

パラメータ	初期設定値	指定可能な値	説明
Intscan.ini [EMail-Scan] ExtractFileSizeLimit	1073741824		特定の条件を満たすファイルのみを検索するよう設定されている場合の、受信圧縮ファイルの最大ファイルサイズ
Intscan.ini [EMail-Scan] OutgoingExtractFileSizeLimit	1073741824		特定の条件を満たすファイルのみを検索するよう設定されている場合の、送信圧縮ファイルの最大ファイルサイズ
Intscan.ini [EMail-Scan] BlockMethod	BlockNone	BlockNone、 BlockAll、 BlockIf	BlockNone: すべての受信圧縮ファイルを検索します。 BlockAll: すべての受信圧縮ファイルを検索しません。 BlockIf: 特定の条件が満たされた場合は受信圧縮ファイルを検索しません。
Intscan.ini [EMail-Scan] OutgoingBlockMethod	BlockNone	BlockNone、 BlockAll、 BlockIf	BlockNone: すべての送信圧縮ファイルを検索します。 BlockAll: すべての送信圧縮ファイルを検索しません。 BlockIf: 特定の条件が満たされた場合は送信圧縮ファイルを検索しません。

パラメータ	初期設定値	指定可能な値	説明
Intscan.ini [EMail-Scan] MaxDecompressCount	100	0 ~ 0x7fffffff	特定の条件を満たすファイルのみを検索するよう設定されている場合の、送信圧縮ファイルの最大検索回数
Intscan.ini [EMail-Scan] OutgoingMaxDecompressCount	100	0 ~ 0x7fffffff	特定の条件を満たすファイルのみを検索するよう設定されている場合の、送信圧縮ファイルの最大検索回数
Intscan.ini [EMail-Scan] MaxDecompressRatio	100	0~100	特定の条件を満たす受信ファイルのみを検索するよう設定されている場合は、SMTP は圧縮率がここで指定された値を下回るファイルを検索します。
Intscan.ini [EMail-Scan] OutgoingMaxDecompressRatio	100	0~100	特定の条件を満たす送信ファイルのみを検索するよう設定されている場合は、SMTP は圧縮率がここで指定された値を下回るファイルを検索します。
Intscan.ini [EMail-Scan] NotifyCharSet			SMTP 通知で優先する文字セット
Intscan.ini [EMail-Scan] AntiVirus	Yes	Yes、No	受信ウイルス検索を有効にするかどうかを指定します。
Intscan.ini [EMail-Scan] OutgoingAntiVirus	Yes	Yes、No	送信ウイルス検索を有効にするかどうかを指定します。

パラメータ	初期設定値	指定可能な値	説明
Intscan.ini [EMail-Scan] LoggingMsgID	Yes	Yes、No	受信メッセージ ID をログに記録するかどうかを指定します。
Intscan.ini [EMail-Scan] EnableSpywareNotiToAdmin	Yes	Yes、No	受信スパイウェアの検出時に管理者に通知を送信するかどうかを指定します。
Intscan.ini [EMail-Scan] OutgoingEnableSpywareNotiToAdmin	Yes	Yes、No	送信スパイウェアの検出時に管理者に通知を送信するかどうかを指定します。
Intscan.ini [EMail-Scan] MsgSpywareNotiToAdmin	%SENDER% から %RCPTS% に送信されたメッセージにおいてスパイウェアまたはグレーウェアが検出されました。メッセージの件名は「%SUBJECT%」です。 InterScan VirusWall は、 %FINALACTION% の処理を実行しました。	文字列	受信スパイウェアの検出時に管理者に送信される通知の内容
Intscan.ini [EMail-Scan] OutgoingMsgSpywareNotiToAdmin	%SENDER% から %RCPTS% に送信されたメッセージにおいてスパイウェアまたはグレーウェアが検出されました。メッセージの件名は「%SUBJECT%」です。 InterScan VirusWall は、 %FINALACTION% の処理を実行しました。	文字列	送信スパイウェアの検出時に管理者に送信される通知の内容

パラメータ	初期設定値	指定可能な値	説明
Intscan.ini [EMail-Scan] EnableSpywareNotiToRecipient	No	Yes、No	受信スパイウェアの検出時に受信者に通知を送信するかどうかを指定します。
Intscan.ini [EMail-Scan] OutgoingEnableSpywareNotiToRecipient	No	Yes、No	送信スパイウェアの検出時に受信者に通知を送信するかどうかを指定します。
Intscan.ini [EMail-Scan] MsgSpywareNotiToRecipient	警告 : InterScan VirusWall は、%SENDER% から送信されたメッセージにおいてスパイウェアまたはグレーウェアを検出しました。メッセージの件名は「%SUBJECT%」です。メッセージは配信されない場合があります。	文字列	受信スパイウェアの検出時に受信者に送信される通知の内容
Intscan.ini [EMail-Scan] OutgoingMsgSpywareNotiToRecipient	警告 : InterScan VirusWall は、%SENDER% から送信されたメッセージにおいてスパイウェアまたはグレーウェアを検出しました。メッセージの件名は「%SUBJECT%」です。メッセージは配信されない場合があります。	文字列	送信スパイウェアの検出時に受信者に送信される通知の内容
Intscan.ini [EMail-Scan] EnableSpywareNotiToSender	No	Yes、No	受信スパイウェアの検出時に送信者に通知を送信するかどうかを指定します。

パラメータ	初期設定値	指定可能な値	説明
Intscan.ini [EMail-Scan] OutgoingEnableSpywareNotiToSender	No	Yes、No	送信スパイウェアの検出時に送信者に通知を送信するかどうかを指定します。
Intscan.ini [EMail-Scan] MsgSpywareNotiToSender	警告 : InterScan VirusWall は、お使いのコンピュータから %RCPTS% に送信されたメッセージにおいてスパイウェアまたはグレーウェアを検出しました。メッセージの件名は「%SUBJECT%」です。メッセージは配信されない場合があります。セキュリティリスクを調べるためにお使いのコンピュータにおいてウイルス検索を実行することをお勧めします。	文字列	受信スパイウェアの検出時に送信者に送信される通知の内容

パラメータ	初期設定値	指定可能な値	説明
Intscan.ini [EMail-Scan] OutgoingMsgSpywareNotiToSend er	警告 : InterScan VirusWall は、お使い のコンピュータから %RCPTS% に送信され たメッセージにおい てスパイウェアまた はグレーウェアを検 出しました。メッ セージの件名は 「%SUBJECT%」です。 メッセージは配信さ れない場合があります。 セキュリティリ スクを調べるため にお使いのコンピ ュータにおいてウ イルス検索を実行 することをお勧め します。	文字列	送信スパイウェア の検出時に送信者 に送信される通知 の内容
Intscan.ini [EMail-Scan] EnableBotTrapNotiToAdmin	Yes	Yes、No	ボットの脅威の検 出時に管理者に通 知を送信するかと うかを指定します。
Intscan.ini [EMail-Scan] MsgBotTrapNotiToAdmin	IntelliTrap は、 %SENDER% から %RCPTS% に送信さ れたメッセージにお いて不審な不正プ ログラムを検出し ました。メッセージ の件名は「%SUBJ ECT%」です。Inter Scan VirusWall は、 %FINALACTION% の 処理を実行しまし た。	文字列	ボットの脅威の検 出時に管理者に送 信される通知の内 容
Intscan.ini [EMail-Scan] EnableBotTrapNotiToRecipient	No	Yes、No	ボットの脅威の検 出時に受信者に通 知を送信するかと うかを指定します。

パラメータ	初期設定値	指定可能な値	説明
Intscan.ini [EMail-Scan] MsgBotTrapNotiToRecipient	警告 : InterScan VirusWall は、 %SENDER% から送信 されたメッセージに おいて不正プログラ ムが含まれている ファイルを検出しま した。メッセージの 件名は 「%SUBJECT%」です。 メッセージは配信さ れない場合があります。	文字列	ボットの脅威の検出 時に受信者に送信さ れる通知の内容
Intscan.ini [EMail-Scan] EnableBotTrapNotiToSender	No	Yes、No	ボットの脅威の検出 時に送信者に通知を 送信するかどうかを 指定します。
Intscan.ini [EMail-Scan] MsgBotTrapNotiToSender	警告 : InterScan VirusWall は、ご使用 のコンピュータから %RCPTS% に送信され たメッセージ内で不 正プログラムアプリ ケーションを含む ファイルを検出しま した。メッセージの 件名は 「%SUBJECT%」です。 メッセージは配信さ れない場合があります。	文字列	ボットの脅威の検出 時に送信者に送信さ れる通知の内容
Intscan.ini [Email-Scan] WholeMailScanAction	Delete	Delete、Quarantine	SMTP ファイル全体 の検索処理を削除に 設定します。
Intscan.ini [Email-Scan] OutboundWholeMailVirusScan	no	yes、no	POP3 ファイル全体 の検索機能を無効ま たは有効にします。

パラメータ	初期設定値	指定可能な値	説明
Intscan.ini [Email-Scan] EnableOutgoingNotiToAdmin	yes	yes、no	SMTP 送信でのウイルス検出時に通知を管理者に送信するかどうかを指定します。
Intscan.ini [Email-Scan] MsgOutgoingNotiToAdmin	%SENDER% から %RCPTS% に送信されたメッセージにおいてウイルスまたは不正プログラムが検出されました。メッセージの件名は「%SUBJECT%」です。InterScan VirusWall は、%FINALACTION% の処理を実行しました。	文字列	管理者に送信される通知の本文
Intscan.ini [Email-Scan] EnableOutgoingNotiToRecipient	no	yes、no	SMTP 送信でのウイルス検出時に通知を受信者に送信するかどうかを指定します。
Intscan.ini [Email-Scan] MsgOutgoingNotiToRecipient	警告 : InterScan VirusWall は、%SENDER% から送信されたメッセージにおいてウイルスを検出しました。メッセージの件名は「%SUBJECT%」です。メッセージは配信されない場合があります。	文字列	受信者に送信される通知の本文
Intscan.ini [Email-Scan] EnableOutgoingNotiToSender	no	yes、no	SMTP 送信でのウイルス検出時に通知を送信者に送信するかどうかを指定します。

パラメータ	初期設定値	指定可能な値	説明
Intscan.ini [Email-Scan] MsgOutgoingNotiToSender	警告 : InterScan VirusWall は、お使い のコンピュータから %RCPTS% に送信され たメッセージにおい てウイルスを検出し ました。メッセージ の件名は 「%SUBJECT%」です。 メッセージは配信さ れない場合があります。	文字列	送信者に送信される 通知の本文
Intscan.ini [Email-Scan] InboundWholeMailVirusScan	no	yes、no	SMTP 受信ファイル 全体の検索機能を無 効または有効にしま す。
Intscan.ini [Email-Scan] Email	yes	yes、no	SMTP 受信でのウイル ス検出時に通知を 管理者に送信するか どうかを指定します。
Intscan.ini [Email-Scan] Message 1	%SENDER% から %RCPTS% に送信され たメッセージにおい てウイルスまたは不 正プログラムが検出 されました。メッ セージの件名は 「%SUBJECT%」です。 InterScan VirusWall は、 %FINALACTION% の 処理を実行しました。	文字列	管理者に送信される 通知の本文
Intscan.ini [Email-Scan] Ewarning	no	yes、no	SMTP 受信でウイル スが検出された場合 に、受信者に通知を 送信するかどうか

パラメータ	初期設定値	指定可能な値	説明
Intscan.ini [Email-Scan] Emessage	警告 : InterScan VirusWall は、%SENDER% から送信されたメッセージにおいてウイルスを検出しました。メッセージの件名は「%SUBJECT%」です。メッセージは配信されない場合があります。	文字列	受信者に送信される通知の本文
Intscan.ini [Email-Scan] EWarningSender	no	yes、no	SMTP 受信でのウイルス検出時に通知を送信者に送信するかどうかを指定します。
Intscan.ini [Email-Scan] EMessageSender	警告 : InterScan VirusWall は、お使いのコンピュータから %RCPTS% に送信されたメッセージにおいてウイルスを検出しました。メッセージの件名は「%SUBJECT%」です。メッセージは配信されない場合があります。	文字列	送信者に送信される通知の本文
Config.xml SMTP¥AntiSpyware¥Enable	1	1,0	SMTP スパイウェア検索を有効にするかどうかを指定します。
Config.xml SMTP¥AntiSpyware¥SpywareTypes	255	0~255	検索されるスパイウェアの種類
Config.xml SMTP¥AntiSpyware¥Action	delete	Pass、Quarantine、Delete	スパイウェア検出時に添付ファイルに対して実行される処理

パラメータ	初期設定値	指定可能な値	説明
Config.xml SMTP¥AntiSpyware¥SpywareExceptions		文字列	SMTP のスパイウェア除外ファイル名のリスト
Config.xml SMTP¥AntiBotTrap¥Enable	1	1,0	SMTP IntelliTrap 検索を有効にするかどうかを指定します。
Config.xml SMTP¥AntiBotTrap¥Action	Quarantine	Pass、Quarantine、Delete	ボットの脅威検出時の添付ファイルに対する処理
Config.xml SMTP¥AntiSpyware¥OutgoingEnable	1	1,0	SMTP スパイウェア送信検索を有効にするかどうかを指定します。
Config.xml SMTP¥AntiSpyware¥OutgoingSpywareTypes	255	0~255	検索されるスパイウェアの種類
Config.xml SMTP¥AntiSpyware¥OutgoingAction	Delete	Pass、Quarantine、Delete	スパイウェア検出時に添付ファイルに対して実行される処理
Config.xml SMTP¥AntiSpyware¥OutgoingSpywareExceptions		文字列	SMTP 送信のスパイウェア除外ファイル名のリスト

SMTP コンテンツフィルタ

パラメータ	初期設定値	指定可能な値	説明
config.xml Smtpp¥Emanager¥Enable	1	1,0	SMTP コンテンツフィルタを有効にします。

SMTP スパムメール対策

パラメータ	初期設定値	指定可能な値	説明
SmtptmaseantiSpamEnable	1	0,1	SMTP スパムメール対策機能を有効または無効にします。
SmtptmaseantiSpamWhiteList	なし	文字列	SMTP スパムメール対策の承認する送信者リスト
SmtptmaseantiSpamBlackList	なし	文字列	SMTP スパムメール対策のブロックする送信者リスト
SmtptmaseantiSpamWhiteKeyword	なし	文字列	SMTP スパムメール対策の除外リスト
SmtptmaseantiSpamMostConfidentAction	Stamp	StampDeleteDeliverQuarantine	高の確実性レベルのメッセージに対するSMTP スパムメール対策処理
SmtptmaseantiSpamConfidentAction	Stamp	StampDeleteDeliverQuarantine	中の確実性レベルのメッセージに対するSMTP スパムメール対策処理
SmtptmaseantiSpamLeastConfidentAction	Stamp	StampDeleteDeliverQuarantine	低の確実性レベルのメッセージに対するSMTP スパムメール対策処理
SmtptmaseantiSpamNotificationsAdministratorEnable	1	0,1	管理者に送信されるSMTP 通知を有効または無効にします。
SmtptmaseantiSpamNotificationsAdministratorFromUser	isvw@FQDN	文字列	管理者に送信されるSMTP スパムメール対策通知メールに使用する送信者のアドレス

パラメータ	初期設定値	指定可能な値	説明
Smtp¥TMASE¥AntiSpam¥Notifications¥Administrator¥Body	%SENDER% から %RCPTS% に送信され たメッセージが、ス パムメールと判定さ れました。メッセー ジの件名は 「%SUBJECT%」です。 InterScan VirusWall は、 %FINALACTION% の 処理を実行しました。	文字列	管理者に送信される SMTP スパムメール 対策通知メールの本 文
Smtp¥TMASE¥AntiSpam¥Notifications¥Administrator¥Charset	UTF-8	文字列	管理者に送信される SMTP スパムメール 対策通知メールの文 字セット
Smtp¥TMASE¥AntiSpam¥Notifications¥Administrator¥Subject	スパムメールが検出 されました。	文字列	管理者に送信される SMTP スパムメール 対策通知メールの件 名
intscan.ini [EMail-Scan] NRSEnable	yes	yes、no	メールレピュテー ションの有効化また は無効化
intscan.ini [EMail-Scan] ServiceLevel	low	low、high	メールレピュテー ションサービスレベ ル
intscan.ini [EMail-Scan] ApprovedIpAddresses		IP アドレス	承認する IP アドレス リスト
intscan.ini [EMail-Scan] RBLSpamAction	1	0/1/2	RBL+ に対する処理。 0 は放置、1 は接続 解除 (エラーコードあ り)、2 は接続解除 (エラーコードなし) を意味します。
intscan.ini [EMail-Scan] RBLErrorCode	550	400~599	返信エラーコード

パラメータ	初期設定値	指定可能な値	説明
intscan.ini [EMail-Scan] QILSpamAction	1	0/1/2	QIL+ に対する処理。 0 は放置、1 は接続解除 (エラーコードあり)、2 は接続解除 (エラーコードなし) を意味します。
intscan.ini [EMail-Scan] QILErrorCode	450	400~599	返信エラーコード

SMTP フィッシング対策

パラメータ	初期設定値	指定可能な値	説明
Smtpp¥TMASE¥AntiPhish¥Enable	1	0,1	SMTP のフィッシング対策を有効または無効にします。
Smtpp¥TMASE¥AntiPhish¥AntiPhishAction	Quarantine	QuarantineDeliverDelete	SMTP フィッシング対策処理
Smtpp¥TMASE¥AntiPhish¥Notifications¥Administrator¥Enable	1	0,1	管理者に送信される SMTP 通知を有効または無効にします。
Smtpp¥TMASE¥AntiPhish¥Notifications¥Administrator¥FromUser	isvw@FQDN	文字列	管理者に送信される SMTP フィッシング対策通知メールに使用する送信者のアドレス

パラメータ	初期設定値	指定可能な値	説明
SmtptfTMASEfAntiPhishfNotifica tionsfAdministratorfBody	%SENDER% から %RCPTS% に送信され たメッセージにおい てフィッシングサイ トが検出されました。 メッセージの件名は 「%SUBJECT%」です。 InterScan VirusWall は、 %FINALACTION% の 処理を実行しました。	文字列	管理者に送信される SMTP フィッシング 対策通知メールの本 文
SmtptfTMASEfAntiPhishfNotifica tionsfAdministratorfCharset	UTF-8	文字列	管理者に送信される SMTP フィッシング 対策通知メールの文 字セット
SmtptfTMASEfAntiPhishfNotifica tionsfAdministratorfSubject	潜在的にフィッシン グされるセキュリ ティリスクが、メッ セージにおいて検出 されました。	文字列	管理者に送信される SMTP フィッシング 対策メールの件名

POP3 ウィルス / スパイウェア / IntelliTrap 検索

パラメータ	初期設定値	指定可能な値	説明
Pop3fPoliciesfRule1fMailVirusS canfEnable	1	0,1	ウィルス検索を有効 にするかどうかを指 定します。無効にす ると、すべてのマク ロ検索 / メールト ラップ / スパイウェア対策 / ウィルスのフィルタ が無効になります。

パラメータ	初期設定値	指定可能な値	説明
Pop3¥Policies¥Rule1¥MailVirusScan¥AddAlert	1	0,1	ユーザのメッセージ内にウイルス警告またはマクロ除去警告を挿入するかどうかを指定します。
Pop3¥Policies¥Rule1¥MailVirusScan¥AddInfo	1	0,1	ユーザのメール内にディスクレーマーメッセージを挿入するかどうかを指定します。
Pop3¥Policies¥Rule1¥MailVirusScan¥Additional	1	0,1	ユーザのメッセージ内に追加のメッセージを挿入するかどうかを指定します。
Pop3¥Policies¥Rule1¥MailVirusScan¥AdditionalMsg	「詳細については、管理者にお問い合わせください。」	文字列	Additional が有効になっていて、警告メッセージの最後の行として挿入されたその他のメッセージが存在する場合に表示されます。この文はメール全体に対して一度だけ挿入されます。
Pop3¥Policies¥Rule1¥MailVirusScan¥CleanLayerExceedMsg	警告：ファイル %CONTAINERNAME% は多数のウイルスに感染しています。 InterScan VirusWall は駆除を試みましたが中断しました。 ファイルにはまだ多数のウイルスが含まれている可能性があります。	文字列	MultipleCleanLayer に関連します。駆除の回数が MultipleCleanLayer に指定されている値を超えると、感染ファイルは完全には駆除されない可能性があります。このメッセージはユーザのメッセージ内に挿入されます。

パラメータ	初期設定値	指定可能な値	説明
Pop3¥Policies¥Rule1¥MailVirusScan¥CompressScan	1	0,1	圧縮ファイル / 添付ファイルの検索を有効または無効にします。
Pop3¥Policies¥Rule1¥MailVirusScan¥EnableMailTrap	1	0,1	メールトラップ検索を実行するかどうかを指定します。
Pop3¥Policies¥Rule1¥MailVirusScan¥EnableSpywareScan	1	0,1	スパイウェア検索を実行するかどうかを指定します。
Pop3¥Policies¥Rule1¥MailVirusScan¥EnableTrendExt	1	0,1	有効になっている場合に、ファイル / 添付ファイルの拡張子が検索エンジンの推奨する拡張子と一致すると、そのファイル / 添付ファイルに対して検索が実行されます。
Pop3¥Policies¥Rule1¥MailVirusScan¥EnableUserExcludeExt	1	0,1	有効になっている場合に、ファイル / 添付ファイルの拡張子が UserExcludeExtensions に指定されている値と一致すると、そのファイル / 添付ファイルに対しては検索は実行されません。CheckExtension も参照してください。

パラメータ	初期設定値	指定可能な値	説明
Pop3¥Policies¥Rule1¥MailVirusScan¥EnableUserExt	1	0,1	有効になっている場合に、ファイル / 添付ファイルの拡張子が UserExtensions に指定されている値と一致すると、そのファイル / 添付ファイルに対して検索が実行されます。CheckExtension も参照してください。
EnableVirusScanPop3¥Policies¥Rule1¥MailVirusScan¥EnableVirusScan	1	0,1	ウイルス検索を実行するかどうかを指定します。
Pop3¥Policies¥Rule1¥MailVirusScan¥EnableWholeFileScan	0	0,1	POP3 ファイル全体の検索機能を無効または有効にします。
Pop3¥Polices¥Rule1¥MailVirusScan¥VirusAlert4WholeFileScan	InterScan VirusWall	文字列	メールの本文に挿入されるディスクレーム
Pop3¥Polices¥Rule1¥MailVirusScan¥Outcomes¥OutcomeWholeFileScanVirus¥Actions¥Deliver¥Enable	0	0,1	POP3 ファイル全体検索に対する処理を deliver にするかどうかを設定します。
Pop3¥Polices¥Rule1¥MailVirusScan¥Outcomes¥OutcomeWholeFileScanVirus¥Actions¥Delete¥Enable	0	0,1	POP3 ファイル全体検索に対する処理を delete にするかどうかを設定します。
Pop3¥Polices¥Rule1¥MailVirusScan¥Outcomes¥OutcomeWholeFileScanVirus¥Actions¥Delete¥CreateReplaceMail	1	0,1	ファイル全体検索でのウイルス検出時に置換メールを受信者に送信するかどうかを指定します。
Pop3¥Polices¥Rule1¥MailVirusScan¥Outcomes¥OutcomeWholeFileScanVirus¥Actions¥Delete¥Subject	メッセージは隔離されました。	文字列	置換メールの件名

パラメータ	初期設定値	指定可能な値	説明
Pop3¥Polices¥Rule1 ¥MailVirusScan¥Outcomes ¥OutcomeWholeFileScanVirus ¥Actions¥Delete¥Body	ウイルスが検出されました。メッセージは削除されました。	文字列	置換メールの内容
Pop3¥Polices¥Rule1 ¥MailVirusScan¥Outcomes ¥OutcomeWholeFileScanVirus ¥Actions¥Quarantine ¥CreateReplaceMail	1	0,1	ファイル全体検索でのウイルス検出時に置換メールを受信者に送信するかどうかを指定します。
Pop3¥Polices¥Rule1 ¥MailVirusScan¥Outcomes ¥OutcomeWholeFileScanVirus ¥Actions¥Quarantine¥Subject	メッセージは隔離されました。	文字列	置換メールの件名
Pop3¥Polices¥Rule1 ¥MailVirusScan¥Outcomes ¥OutcomeWholeFileScanVirus ¥Actions¥Quarantine¥Body	ウイルスが検出されました。メッセージは隔離されました。	文字列	置換メールの内容
Pop3¥Polices¥Rule1 ¥MailVirusScan¥Outcomes ¥OutcomeWholeFileScanVirus ¥Actions¥NotificationAdmin¥Enable	1	0,1	ファイル全体検索でのウイルス検出時に通知を管理者に送信するかどうかを指定します。
Pop3¥Polices¥Rule1 ¥MailVirusScan¥Outcomes ¥OutcomeWholeFileScanVirus ¥Actions¥NotificationAdmin¥Body	%SENDER% から %RCPTS% に送信されたメッセージにおいてウイルスまたは不正プログラムが検出されました。メッセージの件名は「%SUBJECT%」です。InterScan VirusWall は、 %FINALACTION% の処理を実行しました。	文字列	通知の内容

パラメータ	初期設定値	指定可能な値	説明
Pop3¥Polices¥Rule1 ¥MailVirusScan¥Outcomes ¥OutcomeWholeFileScanVirus ¥Actions¥NotificationAdmin¥Subject	ウイルスが検出されました。	文字列	通知の件名
Pop3¥Polices¥Rule1 ¥MailVirusScan¥Outcomes ¥OutcomeWholeFileScanVirus ¥Actions¥NotificationRecipient ¥Enable	0	0,1	ファイル全体検索でのウイルス検出時に通知を管理者に送信するかどうかを指定します。
Pop3¥Polices¥Rule1 ¥MailVirusScan¥Outcomes ¥OutcomeWholeFileScanVirus ¥Actions¥NotificationRecipient¥Body	警告： InterScan VirusWall は、%SENDER% から送信されたメッセージにおいてウイルスを検出しました。メッセージの件名は「%SUBJECT%」です。メッセージは配信されない場合があります。	文字列	通知の内容
Pop3¥Polices¥Rule1 ¥MailVirusScan¥Outcomes ¥OutcomeWholeFileScanVirus ¥Actions¥NotificationRecipient ¥Subject	ウイルスが検出されました。	文字列	通知の件名
Pop3¥Policies¥Rule1¥MailVirusScan¥IntelliScan	1	0,1	有効になっている場合に、InterScan VirusWall は、拡張子ではなく実際のファイルタイプに基づいてファイル / 添付ファイルを検索しようとします。

パラメータ	初期設定値	指定可能な値	説明
Pop3¥Policies¥Rule1¥MailVirusScan¥MaxDecompressCount	0	0~2148473647	InterScan VirusWallは、ここで指定されている値を超えない圧縮ファイルに対して検索を実行します。
Pop3¥Policies¥Rule1¥MailVirusScan¥MaxDecompressDepth	20	1~20	InterScan VirusWallは、ここで指定されている値を超えない圧縮ファイルに対して検索を実行します。
Pop3¥Policies¥Rule1¥MailVirusScan¥MaxDecompressSize	2147483647	1~2147483647	InterScan VirusWallは、ここで指定されている値を超えない圧縮ファイルに対して検索を実行します。
Pop3¥Policies¥Rule1¥MailVirusScan¥MaxEntityCount	50	10~2148473647	InterScan VirusWallは、ここで指定されている値を下回る数のエンティティを持つ圧縮メールに対して検索を実行します。
Pop3¥Policies¥Rule1¥MailVirusScan¥MaxScanSize	0	0~2148473647	InterScan VirusWallが処理するファイル / 添付ファイルの最大サイズ
Pop3¥Policies¥Rule1¥MailVirusScan¥MaxVirusCount	20	0~50	表示されるウイルスの数
Pop3¥Policies¥Rule1¥MailVirusScan¥MultipleClean	1	0,1	ファイル / 添付ファイルがウイルスに感染している場合に、循環検査と駆除を実行するかどうかを指定します。

パラメータ	初期設定値	指定可能な値	説明
Pop3¥Policies¥Rule1¥MailVirusScan¥MultipleCleanLayer	5	0~2148473647	MultipleClean オプションが有効になっている場合、ウイルスフィルタは、駆除できるウイルスがなくなるまで、感染ファイルに対して繰り返し駆除を実行します。このオプションにより繰り返しの回数を制限できます。
Pop3¥Policies¥Rule1¥MailVirusScan¥NoVirusAlert	0	0,1	添付ファイルにウイルスが含まれていない場合に、ユーザのメッセージに NoVirusMsg のメッセージを挿入するかどうかを指定します。
Pop3¥Policies¥Rule1¥MailVirusScan¥NoVirusMsg	添付ファイル (%CONTAINERNAME%) はウイルス対策ソフトウェアにより検索されました。ウイルスは検出されませんでした。	文字列	NoVirusAlert が有効になっていて、添付ファイルにウイルスが含まれない場合に表示されます。このメッセージは各メール添付ファイルに挿入されます。
Pop3¥Policies¥Rule1¥MailVirusScan¥ReplaceWarning	1	0,1	削除された添付ファイルをこの警告メッセージで置き換えるかどうかを指定します。

パラメータ	初期設定値	指定可能な値	説明
Pop3¥Policies¥Rule1¥MailVirusScan¥ReplaceWarningMsg	このメッセージに添付されたファイル (%CONTAINERNAME%) は、コンピュータウイルス %VIRUSNAME% に感染していたため、削除されました。	文字列	添付ファイルが削除され、ReplaceWarning が 1 (ゼロ以外 = 有効) に設定されている場合、削除された添付ファイルを置き換えるためにこのメッセージがユーザのメッセージに挿入されます。
Pop3¥Policies¥Rule1¥MailVirusScan¥SafeStamp	1	0,1	ユーザのメッセージに SafeStampMsg のメッセージを挿入するかどうかを指定します。
Pop3¥Policies¥Rule1¥MailVirusScan¥SafeStampMsg	"InterScan VirusWall は、このメッセージにおいてウイルス検索を実行し、既知のウイルスは検出されませんでした。	文字列	SafeStamp が有効になっていて、メッセージがウイルスフィルタによって安全と見なされる場合に表示されます。この文はメール全体に対して一度だけ挿入されます。
Pop3¥Policies¥Rule1¥MailVirusScan¥ScanAll	1	0,1	有効になっている場合、各ファイル / 添付ファイルは検索のため検索エンジンに渡されます。CheckExtension も参照してください。

パラメータ	初期設定値	指定可能な値	説明
Pop3¥Policies¥Rule1¥MailVirusScan¥UserExcludeExtensions	なし	文字列	各アイテムをセミコロンで区切った拡張子名のリスト。たとえば、「exe;zip;r??」のようになります。ワイルドカード「*」および「?」がサポートされます。余分なスペースは挿入しないでください。 EnableUserExcludeExt を参照してください。
Pop3¥Policies¥Rule1¥MailVirusScan¥UserExtensions	なし	文字列	各アイテムをセミコロンで区切った拡張子名のリスト。たとえば、「exe;zip;r??」のようになります。ワイルドカード「*」および「?」がサポートされます。余分なスペースは挿入しないでください。 EnableUserExt を参照してください。
Pop3¥Policies¥Rule1¥MailVirusScan¥VirusAlert	"InterScan VirusWall は、このメッセージにおいてウイルス検索を実行し、既知のウイルスは検出されませんでした。	文字列	検索結果に含まれます。このメッセージは、ユーザのメッセージ、および各メール添付ファイルに挿入されます。

POP3 コンテンツフィルタ

パラメータ	初期設定値	指定可能な値	説明
config.xml Pop3¥Policies¥Rule1¥MailContentScan¥Enable	1	1,0	POP3 コンテンツフィルタが有効になります。

POP3 スпамメール対策

パラメータ	初期設定値	指定可能な値	説明
Scan¥TMASE¥AntiSpam¥Enable	1	0,1	POP3 スпамメール対策を有効または無効にします。
Scan¥TMASE¥AntiSpam¥WhiteList	なし	文字列	POP3 スпамメール対策の承認する送信者リスト
Scan¥TMASE¥AntiSpam¥BlackList	なし	文字列	POP3 スпамメール対策のブロックする送信者リスト
Scan¥TMASE¥AntiSpam¥WhiteKeyword	なし	文字列	POP3 スпамメール対策の除外リスト
Scan¥TMASE¥AntiSpam¥MostConfidentAction	Stamp	Stamp Delete Deliver Quarantine	高の確実性レベルのメッセージに対するPOP3 スпамメール対策処理
Scan¥TMASE¥AntiSpam¥ConfidentAction	Stamp	Stamp Delete Deliver Quarantine	中の確実性レベルのメッセージに対するPOP3 スпамメール対策処理
Scan¥TMASE¥AntiSpam¥LeastConfidentAction	Stamp	Stamp Delete Deliver Quarantine	低の確実性レベルのメッセージに対するPOP3 スпамメール対策処理

パラメータ	初期設定値	指定可能な値	説明
Scan¥TMASE¥AntiSpam¥Notifications¥Administrator¥Enable	1	0,1	管理者に送信されるPOP3 通知を有効または無効にします。
Scan¥TMASE¥AntiSpam¥Notifications¥Administrator¥FromUser	isvw@FQDN	文字列	管理者に送信されるPOP3 スпамメール対策通知メールに使用する送信者のアドレス
Scan¥TMASE¥AntiSpam¥Notifications¥Administrator¥Body	%SENDER% から %RCPTS% に送信されたメッセージが、スパムメールと判定されました。メッセージの件名は「%SUBJECT%」です。InterScan VirusWall は、%FINALACTION% の処理を実行しました。	文字列	管理者に送信されるPOP3 スпамメール対策通知メールの本文
Scan¥TMASE¥AntiSpam¥Notifications¥Administrator¥Charset	UTF-8	文字列	管理者に送信されるPOP3 スпамメール対策通知メールの文字セット
Scan¥TMASE¥AntiSpam¥Notifications¥Administrator¥Subject	スパムメールが検出されました。	文字列	管理者に送信されるPOP3 スпамメール対策通知メールの件名

POP3 フィッシング対策

パラメータ	初期設定値	指定可能な値	説明
Scan¥TMASE¥AntiPhish¥Enable	1	0,1	POP3 のフィッシング対策を有効または無効にします。

パラメータ	初期設定値	指定可能な値	説明
Scan¥TMASE¥AntiPhish¥AntiPhishAction	Quarantine	Quarantine Deliver Delete	POP3 フィッシング対策処理
Scan¥TMASE¥AntiPhish¥Notifications¥Administrator¥Enable	1	0,1	管理者に送信されるPOP3 通知を有効または無効にします。
Scan¥TMASE¥AntiPhish¥Notifications¥Administrator¥FromUser	isvw@FQDN	文字列	管理者に送信されるPOP3 フィッシング対策通知メールに使用する送信者のアドレス
Scan¥TMASE¥AntiPhish¥Notifications¥Administrator¥Body	%SENDER% から %RCPTS% に送信されたメッセージにおいてフィッシングサイトが検出されました。メッセージの件名は「%SUBJECT%」です。 InterScan VirusWall は、 %FINALACTION% の処理を実行しました。	文字列	管理者に送信されるPOP3 フィッシング対策通知メールの本文
Scan¥TMASE¥AntiPhish¥Notifications¥Administrator¥Charset	UTF-8	文字列	管理者に送信されるPOP3 フィッシング対策通知メールの文字セット
Scan¥TMASE¥AntiPhish¥Notifications¥Administrator¥Subject	潜在的にフィッシングされるセキュリティリスクが、メッセージにおいて検出されました。	文字列	管理者に送信されるPOP3 フィッシング対策通知メールの件名

POP3 設定

パラメータ	初期設定値	指定可能な値	説明
config.xml root/Pop3/IPAddressToBind	INADDR_ANY		待機 IP アドレス
config.xml root/Pop3/MaxSimultaneous ClientConnections	100	1~100	同時クライアント数
config.xml root/Pop3/AllowLoginParameter	1	0/1	プロキシモードを有効または無効にします。
config.xml root/Pop3/InboundPort	110		プロキシモードでの待機ポート
config.xml root/Pop3/AllowServerPort Mapping	0	0/1	ポートマッピングを有効または無効にします。
config.xml root/Pop3/ServerPortMapping Count	0		マップされるポートの数

HTTP

パラメータ	初期設定値	指定可能な値	説明
Config.xml HTTP¥Main¥http¥virus_scan_ enabled	Yes	Yes、No	ウイルス検索を有効または無効にします。

パラメータ	初期設定値	指定可能な値	説明
Config.xml HTTP¥Main¥http¥skiptype		MIME タイプのリスト	これによってパフォーマンスは向上しますが、コンテンツタイプのヘッダはコンテンツの種類を完全には表していない場合があるため、セキュリティは低下します。
Config.xml HTTP¥Main¥http¥action	clean	Pass/ Delete/ Move/ Clean	Pass: ユーザにそのまま配信します。 Delete: 転送をブロックします。 Move: データをプロキシホスト上の一時ファイルに移動します。 Clean: 駆除が可能な場合、ファイルを駆除してから転送を続行します。駆除できない場合は、ucaction を設定する必要があります。 ucaction は、pass、move、delete のいずれかに設定できます。初期設定値は、delete です。
Config.xml HTTP¥Main¥http¥ucaction	delete	Pass/ Move/ Delete	ucaction は、pass、move、delete のいずれかに設定できます。初期設定値は、delete です。

パラメータ	初期設定値	指定可能な値	説明
Config.xml HTTP¥Main¥http¥movedir	C:¥Program Files¥Trend Micro¥InterScan VirusWall¥ quarantine¥http	パス	ウイルスを隔離する ための移動先ディレ クトリ
Config.xml HTTP¥Main¥http¥spyware_scan_ enabled	Yes	Yes、No	スパイウェア検索を 有効または無効にし ます。
Config.xml HTTP¥Main¥http¥spyaction	delete	処理は pass、move、 delete のいずれかに 設定できます。	スパイウェアの処理 方法
Config.xml HTTP¥Main¥http¥virus_notificati on	InterScan VirusWall は、転送しようとし ているファイルがウ イルスに感染してい ることを検出しまし た。ファイルに対し て処理を実行しまし た。	文字列	ウイルスの検出時に 表示される通知
Config.xml HTTP¥Main¥http¥spyware_ notification	InterScan VirusWall は、転送しようとし ているファイルにス パイウェアまたはグ レーウェアが含まれ ていることを検出し ました。ファイルに 対して処理を実行し ました。	文字列	スパイウェアの検出 時に表示される通知
Config.xml HTTP¥Main¥http¥reject_notificati on	転送しようとしてい るファイルはブロッ クされました。組 織のポリシーでは、こ のタイプのファイル の転送は禁止されて います。	文字列	要求がブロックされ たときに表示される 通知 (URL ブロック、 URL フィルタ、また は大規模感染予防ポ リシーのブロックに より引き起こされま す)。

パラメータ	初期設定値	指定可能な値	説明
Config.xml HTTP¥Main¥http¥phish_notification	アクセスしようとしている URL は、サイトにリダイレクトされ個人機密データが収集される可能性があります。この URL へのアクセスは、セキュリティ上の理由でブロックされました。不明な点がある場合は、管理者にご連絡ください。	文字列	URL へのアクセスがフィッシング対策によってブロックされたときに表示される通知
Config.xml HTTP¥Main¥http¥url_blocking_enabled	Yes	Yes、No	すべての URL ブロック機能を有効または無効にします。
Config.xml HTTP¥Main¥scan¥special_handling	Yes	Yes、No	Yes: サイズの大きいファイルを進捗ページまたは「配信後に検索」機能を使用して処理します。 No: サイズの大きいファイルは、他のすべてのコンテンツと同様に処理されます。 ファイルがファイルサイズ制限を超える場合の「遅延検索」または「配信後に検索」を有効または無効にします。

パラメータ	初期設定値	指定可能な値	説明
Config.xml HTTP¥Main¥scan¥scan_huge_file	Yes	Yes、No	サイズの大きいファイルの検索を有効または無効にします。 Yes に設定されている場合、 max_scan_size の値より大きなサイズのファイルは検索されません。
Config.xml HTTP¥Main¥scan¥max_scan_size	1048576	かなりサイズの大きいファイルサイズ	検索されるファイルのファイルサイズ制限を KB で指定します。
Config.xml HTTP¥Main¥scan¥deferred_scanning	Late	Yes、No、Late	遅延検索の設定
Config.xml Http¥Main¥scan¥trickle_rate	512K	2M-1 より小さいファイルサイズ	InterScan VirusWall サーバが受信するファイルサイズ
Config.xml Http¥Main¥scan¥trickle_max_size	1024 バイト	2M-1 より小さいファイルサイズ	InterScan VirusWall サーバがクライアントに送信するファイルサイズ
Config.xml HTTP¥Main¥scan¥max_synchronous_scan_size	524288	遅延検索のファイルサイズの設定	遅延検索のファイルサイズ
Config.xml HTTP¥Main¥internet-access-monitoring¥ enable	No	Yes、No	アクセスログをオンまたはオフにします。

パラメータ	初期設定値	指定可能な値	説明
Config.xml HTTP¥Protocol¥HttpProxy¥http¥ self_proxy	Yes	Yes、No	self_proxy には、InterScan VirusWall が直接 HTTP プロキシ (ブラウザ→InterScan VirusWall → Web サーバ) として動作するか、または依存プロキシ (ブラウザ→InterScan VirusWall →上位 HTTP プロキシ→ Web サーバ) として動作するかを指定します。これを Yes に設定すると直接プロキシとして動作し、No に設定すると依存プロキシとして動作します。No に設定する場合、original_server と original_server_port に、上位プロキシの名前とポート番号をそれぞれ指定する必要があります。
Config.xml HTTP¥Protocol¥HttpProxy¥http¥ original_server		IP アドレスまたはホスト名	original_server には、InterScan VirusWall が依存プロキシモードでインストールされている場合にトラフィックが経由する上位 HTTP プロキシサーバの名前を指定します。

パラメータ	初期設定値	指定可能な値	説明
Config.xml HTTP¥Protocol¥HttpProxy¥http¥ original_server_port	8080	ポート番号	original_server_port には、上位 HTTP プ ロキシサーバが HTTP トラフィック を待機するポート番 号を指定します。
Config.xml HTTP¥Protocol¥HttpProxy¥http¥ anonymous_ftp_mail_address		匿名 FTP メールアド レス	anonymous_ftp_mail _address には、FTP over HTTP 要求のため に FTP サーバに匿名 で接続する際に InterScan VirusWall が指定するメールア ドレスを設定します。
Config.xml HTTP¥Protocol¥HttpProxy¥http¥ reverse_proxy	No	Yes、No	self_proxy=no の場合 に確認します。これ が Yes に設定されて いると、リバースプ ロキシモードがアク ティベートされ、元 のサーバ / ポートが、 上位プロキシではな く通常の HTTP サー バとして使用されま す。

パラメータ	初期設定値	指定可能な値	説明
Config.xml HTTP¥plugin¥ScanVsapi¥http¥level	scanall	scanall/ scanintelli/ scanext	scanall: すべてのトラフィックが検索されます。 scanintelli: 検索エンジンにより、実際のファイルタイプに基づいて検索されるファイルが決まります。 scanext: 特定の拡張子を持つファイルのみが検索されます。
Config.xml HTTP¥plugin¥ScanVsapi¥http¥extensions		拡張子のリスト	level が scanext に設定されている場合に検索される拡張子の初期設定のリスト。アイテムはセミコロン (;) で区切る必要があります。各拡張子にはドット (.) を付けません。
Config.xml HTTP¥plugin¥ScanVsapi¥http¥spyware_exceptions		「,」で区切られた文字列のリスト	スパイウェア検索の除外ファイル名のリスト。ファイル名拡張子を使用するには、「*」を付けます。たとえば、「filename.exe;*.ext1」のように指定します。
Config.xml HTTP¥Plugin¥URLFilter¥plug-in¥enabled	No	Yes、No	検索モジュールを有効または無効にします。

FTP

パラメータ	初期設定値	指定可能な値	説明
intscan.ini [FTP-Scan] MaxThreads	50	>= 0	[FTP] → [設定] → [最大接続数]
intscan.ini [FTP-Scan] InterScanFTPServicePort	21	1 ~ 65535	InterScan VirusWall の FTP サービスポート。Web コンソールから変更することはできません。
intscan.ini [FTP-Scan] UseFTPProxy	No	Yes、No	[FTP] → [設定] → [FTP プロキシを使用する]
intscan.ini [FTP-Scan] FOrgPort	21	1 ~ 65535	[FTP] → [設定] → [FTP プロキシを使用する] の順に選択し、既存の FTP プロキシのポート番号を指定します。
intscan.ini [FTP-Scan] ForcePassiveFTP	No	Yes、No	[FTP] → [設定] → [すべてのファイル転送に PASSIVE FTP を使用する]
intscan.ini [FTP-Scan] Level	ScanAll (すべての検索可能なファイル)	ScanAll、IntelliScan、ScanExt	[FTP] → [検索] → [対象] → [検索対象ファイル]
intscan.ini [FTP-Scan] SMTPServerPort	25	1 ~ 65535	[管理] → [通知設定] の順に選択し、SMTP サーバのポート番号を指定します。
intscan.ini [FTP-Scan] EMail	Yes	Yes、No	[FTP] → [検索] → [通知] → [管理者]

パラメータ	初期設定値	指定可能な値	説明
intscan.ini [FTP-Scan] Action	Cleandetele (ファイルを駆除します。駆除できない場合は、ブロックします。)	Cleanmove、 Cleandetele、 Cleanpass、Move、 Delete、Pass	[FTP] → [検索] → [処理]
intscan.ini [FTP-Scan] TrickleAmount	1024	>= 0	[FTP] → [設定] → [データを x KB を受信するたび x バイトずつクライアントに送信]
intscan.ini [FTP-Scan] TricklePeriod	512	>= 0	[FTP] → [設定] → [データを x KB を受信するたび x バイトずつクライアントに送信]
intscan.ini [FTP-Scan] DecompressionLayerLimit	14	2 ~ 20	[FTP] → [検索] → [対象] → [圧縮レイヤが次の数を超える場合]
intscan.ini [FTP-Scan] ExtractFileSizeLimit	1073741824 (1GB)	0 ~ 2147483647	[FTP] → [検索] → [対象] → [解凍後のファイルサイズが次の数を超える場合]
intscan.ini [FTP-Scan] AntiVirus	Yes	Yes、No	[FTP] → [検索] → [対象] → [FTP 検索を有効にする]
intscan.ini [FTP-Scan] BlockMethod	BlockNone (すべての圧縮ファイルが検索されます。)	BlockNone、 BlockAll、BlockIf	[FTP] → [検索] → [対象] → [圧縮ファイルの処理]
intscan.ini [FTP-Scan] MaxDecompressCount	100	>= 0	[FTP] → [検索] → [対象] → [解凍後のファイル数が次の数を超える場合]

パラメータ	初期設定値	指定可能な値	説明
intscan.ini [FTP-Scan] MaxDecompressRatio	100	0 ~ 100	[FTP] → [検索] → [対象] → [圧縮ファイルに対する解凍後のファイルサイズが次の割合を超える場合]
intscan.ini [FTP-Scan] EnableGreeting	Yes	Yes、No	[FTP] → [設定] → [接続が確立されたときに次の FTP グリーティングメッセージを送信する]
config.xml [FTP] Enable	1	1 / 0	[概要] → [FTP] → [FTP トラフィックを有効にする]
config.xml [FTP¥AntiSpyware] Enable	1	1 / 0	[FTP] → [スパイウェア対策] → [FTP スパイウェア対策を有効にする]
config.xml [FTP¥AntiSpyware] SpywareTypes	255 (すべてのタイプのスパイウェア / グレーウェアが検索されます。)	Web コンソールからオプションを選択します。	[FTP] → [スパイウェア対策] → [検索するスパイウェア / グレーウェア]
config.xml [FTP¥AntiSpyware] Action	Delete	Quarantine、Delete、Pass	[FTP] → [スパイウェア対策] → [処理]
config.xml [Webui¥FTP] MaxDecompressSizeUnit	1073741824 (1GB)	Web コンソールからオプションを選択します。	[FTP] → [検索] → [対象] → [解凍後のファイルサイズが次の割合を超える場合] の順に選択し、単位のオプションを選択します。
config.xml Webui¥FTP¥AntiVirus¥SecondAction	delete	move、delete、pass	[FTP] → [検索] → [処理] → [駆除できない場合の処理]

ログ

パラメータ	初期設定値	指定可能な値	説明
config.xml [Common¥Logging] LogDir	log		ログファイルの相対パス。Web コンソールから変更することはできません。
config.xml [Common¥Logging] EnableMaintenance	1	1 / 0	[ログ] → [メンテナンス] → [自動] → [自動削除を有効にする]
config.xml [Common¥Logging] WhatMaintenance	63 (すべてのタイプのログ)	Web コンソールからオプションを選択します。	[ログ] → [メンテナンス] → [自動] → [対象]
config.xml [Common¥Logging] ExpiredDays	30	0 ~ 360	[ログ] → [メンテナンス] → [自動] → [処理]
config.xml [Common¥Logging] DebugEnabled	0	1 / 0	デバッグログを有効にするかどうかを指定します。
config.xml [Webui¥Log¥Query] プロトコル	1 (SMTP)	Web コンソールからオプションを選択します。	[ログ] → [クエリ] → [プロトコル]
config.xml [Webui¥Log¥Query] logtype	1 (ウイルス / 不正プログラム)	Web コンソールからオプションを選択します。	[ログ] → [クエリ] → [ログの種類]
config.xml [Webui¥Log¥Query] timeperiod	1 (すべて)	Web コンソールからオプションを選択します。	[ログ] → [クエリ] → [期間]
config.xml [Webui¥Log¥Query] ItemPerPage	25	10 / 25 / 50 / 100	[ログ] → [クエリ] → [1 ページあたりの件数]
config.xml [Webui¥Log¥Maintenance¥Auto] Enable	0	1 / 0	[ログ] → [メンテナンス] → [自動] → [自動削除を有効にする]

パラメータ	初期設定値	指定可能な値	説明
config.xml [Webui¥Log¥Maintenance¥Auto] Action	1 (上で選択したすべてのログを削除)	Web コンソールからオプションを選択します。	[ログ] → [メンテナンス] → [自動] → [処理]
config.xml [Webui¥Log¥Maintenance¥Auto] LogTypes	63 (すべてのタイプのログ)	Web コンソールからオプションを選択します。	[ログ] → [メンテナンス] → [自動] → [対象]
config.xml [Webui¥Log¥Maintenance¥Auto] ExpiredDays	30	0 ~ 360	[ログ] → [メンテナンス] → [自動] → [処理]
config.xml [Webui¥Log¥Maintenance¥Manual] Action	1 (上で選択したすべてのログを削除)	Web コンソールからオプションを選択します。	[ログ] → [メンテナンス] → [手動] → [処理]
config.xml [Webui¥Log¥Maintenance¥Manual] LogTypes	63 (すべてのタイプのログ)	Web コンソールからオプションを選択します。	[ログ] → [メンテナンス] → [手動] → [対象]
config.xml [Webui¥Log¥Maintenance¥Manual] ExpiredDays	30	0 ~ 360	[ログ] → [メンテナンス] → [手動] → [処理]
config.xml [SMTP] [HTTP] [POP3] [FTP] WriteConnectionMsg	1	0/1	SMTP/HTTP/POP3/FTP のトランザクションログを有効または無効にします。
config.xml [SMTP] [HTTP] [POP3] [FTP] ConnectionLogLevel	10	10/0	SMTP/HTTP/POP3/FTP トランザクションログに粗いレベル (10) または診断レベル (0) を設定します。

隔離

パラメータ	初期設定値	指定可能な値	説明
config.xml [Webui¥Quarantine¥Maintenance] ManualDelete	7	0 ~ 360	[隔離] → [メンテナンス] → [手動] → [処理]

大規模感染予防サービス

パラメータ	初期設定値	指定可能な値	説明
config.xml root/Scan/OPP/Enable	0	0/1	大規模感染予防ポリシーを無効または有効にします。
config.xml root/Scan/OPP/IssueDuration	2880	1440 ~ 7200	大規模感染予防ポリシーの有効期限
config.xml root/Common/ActiveUpdate/ScheduleUpdate/OPSUpdate/EnableUpdate	1	0/1	予約アップデートを有効または無効にします。
config.xml root/Common/ActiveUpdate/ScheduleUpdate/OPSUpdate/Minutes	10	1 ~ 120	予約アップデートの間隔
config.xml root/Common/ActiveUpdate/UpdateServers/Server.3/Source	http://oc.activeupdate.trendmicro.com/activeupdate/	アップデートサーバの URL	大規模感染予防ポリシーのアップデートサーバ

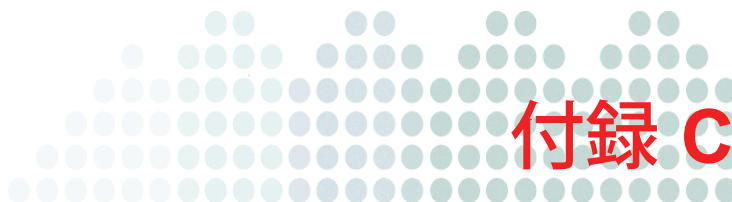
アップデート

パラメータ	初期設定値	指定可能な値	説明
Root¥common¥ActiveUpdate¥UpdateServers¥Server.1¥Source	http://isvw602-av.activeupdate.trendmicro.com/activeupdate/	アップデートサーバの URL	ウイルス / スパイウェア検出パターンファイルおよびエンジンのアップデートに使用するアップデートサーバ
common¥ActiveUpdate¥UpdateServers¥Server.2¥Source	http://isvw602-as.activeupdate.trendmicro.com/activeupdate/	アップデートサーバの URL	スパムメールの判定ルールおよびエンジンのアップデートに使用するアップデートサーバ
common¥ActiveUpdate¥UpdateServers¥Server.3¥Source	http://oc.activeupdate.trendmicro.com/activeupdate/	アップデートサーバの URL	大規模感染予防ポリシーのアップデートに使用するアップデートサーバ
common¥ActiveUpdate¥ScheduleUpdate¥virusUpdate¥EnableUpdate	1	1/0	予約アップデートを有効または無効にします。

パターンファイルのアップデート通知の初期設定値

パラメータ	初期設定値	指定可能な値	説明
Config.xml root/Common/ActiveUpdate/Notification/tmpdir	temp	一時フォルダの相對パス	InterScan VirusWall が使用する一時フォルダ
Config.xml root/Common/ActiveUpdate/Notification/FromUser	isvw@localdomain	メールアドレス	通知送信者メールアドレス

パラメータ	初期設定値	指定可能な値	説明
Config.xml root/Common/ActiveUpdate/Notification/SuccessEnable	0	0/1	アップデート成功通知機能を有効または無効にします。
Config.xml root/Common/ActiveUpdate/Notification/SuccessSubject	ActiveUpdate 成功通知	文字列	アップデート成功通知メールの件名
Config.xml root/Common/ActiveUpdate/Notification/SuccessBody	InterScan VirusWall では、次のコンポーネントがアップデートされました。	文字列	アップデート成功通知メールのメール本文
Config.xml root/Common/ActiveUpdate/Notification/FailEnable	0	0/1	アップデート失敗通知機能を有効または無効にします。
Config.xml root/Common/ActiveUpdate/Notification/FailSubject	ActiveUpdate 失敗通知	文字列	アップデート失敗通知メールの件名
Config.xml root/Common/ActiveUpdate/Notification/FailBody	InterScan VirusWall では、次のコンポーネントのアップデートに失敗しました。	文字列	アップデート失敗通知メールのメール本文



InterScan VirusWall 6.0 または 6.02 からの移行

この付録は、Trend Micro InterScan VirusWall スタンダードエディション（以下、InterScan VirusWall）6.0 または 6.02 から本バージョンの InterScan VirusWall に設定を移行する際の参考資料として使用してください。

表 C-1 では、InterScan VirusWall 6.0 から InterScan VirusWall 7.0 に移行されない設定について説明します。

表 C-1. InterScan VirusWall 6.0 から移行されないキー

キー	設定
config.xml: Http¥Main¥scan¥trickle_rate	InterScan VirusWall 7.0 の初期設定値 : 96。 Web コンソールの場所 (6.0x/7.0) : [HTTP] → [検索] → [サイズの大きいファイルの処理] [ISVW サーバが次のサイズのファイルを受信するたび]
config.xml: Http¥Main¥scan¥trickle_max_size	InterScan VirusWall 7.0 の初期設定値 : 65536。 Web コンソールの場所 (6.0x/7.0) : [HTTP] → [検索] → [サイズの大きいファイルの処理] [ファイルのうち次のバイトをクライアントに送信する]
Config.xml: Http¥Main¥Http¥reject_notification	InterScan VirusWall 7.0 で使用するキー : Http¥ Notification¥URLBlockFilter。 初期設定値 : 「要求された URL はこのネットワークのセキュリティポリシーによってブロックされました」。不明な点がある場合は、管理者にご連絡ください。 Web コンソールの場所 (6.0x) : [HTTP] → [URL ブロック] → [通知]。 Web コンソールの場所 (7.0) : [HTTP] → [HTTP URL ブロック / フィルタ] → [設定] [ユーザへの通知]。
隔離	隔離ファイル : InterScan VirusWall 6.0x の隔離パスが InterScan VirusWall 6.0 のルートパスの下にある場合、本バージョンの InterScan VirusWall では、前の隔離フォルダがルートドライブパスに移動します。たとえば、製品が D:¥ISVW6 の下にインストールされ、隔離ファイルが D:¥ISVW¥quarantine にある場合、本バージョンの InterScan VirusWall ではこの隔離ファイルが D:¥Relocated_ISVW6_Quarantine_Folder¥xxx に移動されます。前の隔離パスが InterScan VirusWall 6.0 のルートパスの下にない場合、本バージョンの InterScan VirusWall では、隔離ファイルはユーザが設定したパスの下に格納されます。 隔離フォルダ設定 : 隔離パスが InterScan VirusWall 6.0x で変更された場合、本バージョンの InterScan VirusWall ではユーザ設定が保持されます。隔離パスが InterScan VirusWall 6.0x で変更されなかった場合、本バージョンの InterScan VirusWall では隔離ファイルのパスは次のようになります。<InterScan VirusWall 7 インストールパス >¥quarantine

Trend Micro Control Manager の複製制限

Trend Micro Control Manager (以下、Control Manager) Web コンソールを使用して設定の複製を行う場合、すべての項目が複製されるわけではありません。この付録では、複製されない項目と設定を一覧表示します。

次の各セクションでは、複製されないプロトコル固有の設定の一部について説明します。

- 「複製されない SMTP 固有の設定」
- 「複製されない HTTP 固有の設定」
- 「複製されない FTP 固有の設定」
- 「複製されない POP3 固有の設定」

次の各セクションでは、複製されない Trend Micro InterScan VirusWall (以下、InterScan VirusWall) 固有の設定の一部について説明します。

- 「大規模感染予防」
- 「隔離」
- 「アップデート」
- 「ログ」
- 「管理」
- 「複製されないその他の InterScan VirusWall ユーザインタフェース項目と設定」

複製されないプロトコル固有の設定

複製されない SMTP 固有の設定

Control Manager Web コンソールを使用すると、SMTP 検索、IntelliTrap、フィッシング対策、スパムメール対策、スパイウェア対策、およびコンテンツフィルタ関連の設定はすべて複製されます。SMTP 設定に関連する固有の設定だけが Control Manager Web コンソールの使用時に複製されません。

表 D-1. 複製されない [SMTP 設定] 画面設定

SMTP 設定
サーバ構成
メインサービスポート
受信メール ([受信メッセージの ID をログに記録] を含まない)
送信メール - 項目 1 と 2 ([カスタマイズしたディスクレーマーテキストをすべての送信メールに追加する] を含まない)
メールキュー
このセクションの項目はすべて複製されます
詳細設定
次のドメイン宛ての受信メールのみを許可して、リレーされたメッセージをブロックする (このセクションのその他の項目はすべて複製されます)

複製されない HTTP 固有の設定

Control Manager Web コンソールを使用すると、HTTP 検索、フィッシング対策、スパイウェア対策、URL ブロック、URL フィルタルール、および URL フィルタ設定関連の設定はすべて複製されます。HTTP 設定に関連する固有の設定だけが Control Manager Web コンソールの使用時に複製されません。

表 D-2. 複製されない [HTTP 設定] 画面設定

HTTP 設定
設定
InterScan VirusWall の動作モード
待機するポート番号
FTP over HTTP の匿名ログオンで使用するメールアドレス
[HTTP 要求を記録する] は複製されます

複製されない FTP 固有の設定

Control Manager Web コンソールを使用すると、FTP 検索およびスパイウェア対策関連の設定はすべて複製されます。FTP 設定に関連する固有の設定だけが Control Manager Web コンソールの使用時に複製されません。

表 D-3. 複製されない [FTP 設定] 画面設定

FTP 設定
設定
InterScan VirusWall の動作モード情報
すべてのファイル転送に PASSIVE FTP を使用する
FTP サービスポート
詳細設定
[詳細設定] セクションの項目はすべて複製されます

複製されない POP3 固有の設定

Control Manager Web コンソールを使用すると、POP3 検索、IntelliTrap、フィッシング対策、スパムメール対策、スパイウェア対策、およびコンテンツフィルタ関連の設定はすべて複製されます。POP3 設定に関連する固有の設定だけが Control Manager Web コンソールの使用時に複製されません。

表 D-4. 複製されない [POP3 設定] 画面設定

POP3 設定
POP3 IP アドレス
IP
ユーザのメールクライアント接続
このフィールドは複製されます
POP3 サーバ接続
ユーザのメールクライアントから要求されたすべての POP3 サーバに接続する
POP3 クライアントが InterScan VirusWall の接続に使用するポート
POP3 ポートマッピング
指定された POP3 サーバに接続する（安全なパスワード認証）
インバウンド POP3 ポート
IP アドレス
POP3 サーバポート

複製されない InterScan VirusWall 固有の設定

大規模感染予防

表 D-5. 複製されない [大規模感染予防] 設定

大規模感染予防
ステータス - [大規模感染予防サービスを有効にする] は複製されます
設定 - [設定] 画面の設定はすべて複製されます

隔離

表 D-6. 複製されない [隔離] 設定

隔離
設定 - 設定はすべて複製されません
メンテナンス (手動および自動) - 設定はすべて複製されます

アップデート

表 D-7. 複製されない [アップデート] 設定

アップデート
手動アップデート - N/A
予約アップデート - 設定はすべて複製されます

ログ

表 D-8. 複製されない [ログ] 設定

ログ
クエリ - N/A
メンテナンス (手動および予約) - 設定はすべて複製されます

管理

表 D-9. 複製されない [管理] 設定

管理
Control Manager 設定 - 設定はすべて複製されません
通知設定 - 設定はすべて複製されません
パスワード - 設定はすべて複製されません
製品ライセンス情報 - 情報はすべて複製されません
プロキシ設定 - 設定はすべて複製されません
ウイルストラッキング - 設定はすべて複製されません

複製されないその他の InterScan VirusWall ユーザインタフェース項目と設定

- ・ パターンファイルおよびエンジン
- ・ 隔離ファイル
- ・ ログ
- ・ Control Manager 設定
- ・ トレンドマイクロ ウイルストラッキングセンター設定
- ・ Web コンソールのパスワード
- ・ 製品登録プロファイル

索引

英数字

Active Directory 144

DNS、SMTP メッセージ送信間隔の指定 121

EICAR 62

EICAR (European Institute of Computer Antivirus Research) 62

FTP

サポートされているコマンド 313

初期設定値 360、362

スタンドアロンモード 38

想定されるインストール設定 38-39

トリクル転送 290

プロキシサーバ 38

HTTP

圧縮ファイルの検索 129

依存プロキシモードのトポロジ 160

依存プロキシモード 40

隔離処理 136、143

許可処理 143

駆除処理 136

サービス 125

指定、検索するファイルタイプ 127-135

初期設定値 352-359

処理、検出したフィッシングサイト 139

処理、スパイウェア / グレーウェア検出時
142

スタンドアロンモードのプロキシトポロジ
160

設定、クライアントブラウザでのプロキシ
163-165

設定、サービス 125-165

設定、トラフィック処理 159-165

想定されるインストール設定 40

そのまま配信処理 136

待機、ネットワークインタフェース上 163

透過モードのトポロジ 161

フィッシングサイトの通知 139

プロキシサーバ 40

ブロック処理 136、143

有効化、ウイルス検索 127

有効化、サービス 126

有効化、スパイウェア検索 140

有効化、フィッシング対策 138

リバースプロキシモード 42

リバースプロキシモードのトポロジ 161

IntelliTrap 22

POP3 194-196

SMTP 75-79

隔離処理 77、195

削除処理 77、195

そのまま配信処理 77、195

タグ、通知メッセージ 78、196

通知設定 78、196

パターンファイル 238

無効化、検索 76、195

有効化、検索 76、195

InterScan 29

InterScan VirusWall

FTP プロキシサーバ、スタンドアロンモード

38、40

IntelliTrap 通知設定 78、196

POP3 ウイルス検索通知設定 187-189

POP3 コンテンツフィルタ 220

POP3 フィッシング対策 197-198

POP3 フィッシング通知設定 197-198

SMTP ウイルス検索通知設定 71

SMTP コンテンツフィルタ 116

SMTP フィッシング対策 80-83

SMTP フィッシング通知設定 82-83

SMTP メールキュー 120

アクティベート 261-263

アップデート、コンポーネント 241

依存プロキシモード 38

インストール手順 45

インストール、InterScan VirusWall の以前の
バージョンがインストールされている場合の
InterScan VirusWall 53

初期インストール 46-49

新規インストール 46-49

インストールと InterScan VirusWall の以前の
バージョンからの移行 53、57

インストールの概要 29

インストールのトポロジ 34

インストール前のチェックリスト 43

ウイルス検出方法 26

同じコンピュータへのインストール 33

隔離機能 229

機能、ポートマッピングサーバ 37

計画、インストール 29

決定、インストール先 33

検索、圧縮ファイル 27

コンポーネント、アップデートに対応 238

サイズの大きいファイルの処理 134

最大化、パフォーマンス 27

システム要件 30

指定、DNS でのメッセージ送信間隔 121

指定、同時 SMTP クライアント接続数 121

承認する送信者およびブロックする送信者リ
スト 90、203

初期設定値 315-366

初期設定の隔離ディレクトリ 232

処理、POP3 検索時の圧縮ファイル 186

処理、SMTP 検索時の圧縮ファイル 67

スパムメール検出レベル 88-89、201-202

スパムメールフィルタ 84、199

製品管理 261

製品の概要 27

設定、HTTP サービス 125-165

設定、HTTP プロキシ設定 162

設定、POP3 IntelliTrap 設定 194-196

設定、POP3 ウイルス検索設定 189

設定、POP3 サービス 183

設定、POP3 スпамメール対策設定 207

設定、SMTP IntelliTrap 設定 75-79

設定、SMTP ウイルス検索設定 64

設定、SMTP サービス 63、122

設定、SMTP スпамメール対策設定 84-94

専用コンピュータへのインストール 33

挿入、SMTP メッセージのヘッダ情報 121

トラブルシューティング 292

ポート、使用 32

- リアルタイム検索モニタ 281-283
- ロールバック、コンポーネント 241
- InterScan VirusWall 6.0x
 - 本バージョンへの移行 369
- InterScan VirusWall の機能と利点 22
- InterScan VirusWall の製品概要 21
- IP アドレス
 - 指定、POP3 サービス 221
- MacroTrap 27
- Microsoft Active Directory 144
- MIME コンテンツタイプ 130-134
- Network VirusWall 2500
 - ドキュメント
 - 表記規則 19
 - ドキュメントの表記規則 19
- Outlook Express
 - InterScan VirusWall の安全なスタンプファイル
を安全な添付ファイルにする 291
 - 設定、エンドユーザメールクライアント
222-223
- POP3
 - インライン通知 188
 - 隔離処理 187、195、197、205、210、216、
219
 - キーワードの類義語リストを変更する 216
 - 検索、圧縮ファイル 186
 - 検索処理 187
 - コピーまたは削除、コンテンツフィルタポリ
シー 220
 - コンテンツフィルタ 220
 - コンテンツフィルタ通知設定 216
- サービス 183
- 削除処理 187、195、197、205、210、216、
219
- サポートされているコマンド 314
- 指定、POP3 サービスの IP アドレス 221
- 指定、許可する同時クライアント接続の最大
数 221
- 指定、接続の種類 221
- 初期設定値 352
- 初期設定値、ウイルス / スパイウェア
/IntelliTrap および設定 339-348
- 初期設定値、コンテンツフィルタ 349
- 初期設定値、スパムメール対策 349-350
- 初期設定値、フィッシング対策 350
- 処理、IntelliTrap 195
- 処理、コンテンツフィルタ 216
- 処理、スパイウェア / グレーウェア検出時
209
- 処理、スパムメールメッセージ 205
- 処理、添付ファイルコンテンツフィルタ 219
- 処理、フィッシングメール 197
- スタンプ処理 205
- 設定、IntelliTrap 設定 194-196
- 設定、ウイルス検索設定 189
- 設定、サービス 183
- 設定、スパムメール対策設定 207
- 設定、トラフィック処理 220-222
- 選択、検索するファイルタイプ 185
- 想定されるインストール設定 36-37
- そのまま配信処理 187、195、210
- 追加、キーワードフィルタポリシー 215

添付ファイルフィルタ通知設定 220

フィッシング対策 197-198

放置処理 197、205、216、219

マップ、サーバのポート 221

無効化、IntelliTrap 195

無効化、コンテンツフィルタ 211

無効化、サービス 184

有効化、IntelliTrap 195

有効化、ウイルス検索 185

有効化、コンテンツフィルタ 211

有効化、サービス 184

有効化、スパイウェア検索 208

有効化、スパムメール検出 200

Readme 18

Smart Protection Network 156

SMTP

インライン通知 72

隔離処理 69、77、80、92、98、109、114

キーワードの類義語リストを変更する

107-108

検索、圧縮ファイル 67

検索処理 69

コピーまたは削除、コンテンツフィルタポリ

シー 116

コンテンツフィルタ 116

コンテンツフィルタ通知設定 109

サーバ認証 289

サービス 63

削除処理 69、77、80、92、98、109、114

サポートされているコマンド 313

指定、DNS でのメッセージ送信間隔 121

指定、同時クライアント接続数 121

詳細設定のオプション 120-122

初期設定値、ウイルス / スパイウェア

/IntelliTrap および設定 316-335

初期設定値、コンテンツフィルタ 335

初期設定値、スパムメール対策 336-337

初期設定値、フィッシング対策 338-339

処理、IntelliTrap 77

処理、コンテンツフィルタ 109

処理、スパイウェア / グレーウェア検出時 98

処理、スパムメールメッセージ 91

処理、添付ファイルコンテンツフィルタ 114

処理、フィッシングメール 80

スタンプ処理 92

接続サービスのグリーティング 122

設定、IntelliTrap 設定 75-79

設定、ウイルス検索設定 64

設定、サービス 63、122

設定、サービス設定 118

設定、受信メッセージ 118-119

設定、スパムメール対策設定 84-94

設定、送信メッセージ 119-120

設定、トラフィック処理 117-122

選択、検索するファイルタイプ 66

想定されるインストール設定 34-35

挿入、メッセージのヘッダ情報 121

そのまま配信処理 77、98

追加、キーワードフィルタポリシー 106-107

添付ファイルフィルタ通知設定 115-116

トラブルシューティング、メールの送信時

または SMTP ポートへの接続時にサーバが突然

接続を終了する 290
フィッシング対策 80-83
ブロック、リレーメッセージ 122
放置処理 69、80、92、109、114
無効化、IntelliTrap 76
無効化、コンテンツフィルタ 102
無効化、サービス 64
メールキュー 120
有効化、IntelliTrap 76
有効化、ウイルス検索 65
有効化、コンテンツフィルタ 101
有効化、サービス 64
有効化、スパイウェア検索 96
有効化、スパムメール検出 87
SMTP VirusWall 43
TrendLabs 309
URL
製品 Q&A 18
報告された疑わしいフィッシングサイト 83、
139、198
WCCP (Web Cache Control Protocol) 161
Windows パフォーマンスモニタ
カウンタの追加 282
開く 281
対象読者 19

あ

アクティベーション、製品 261-263
圧縮ファイル
HTTP 検索 129
POP3 検索 186

SMTP 検索 67
検索方法 27
アップデート 237、288
コンポーネント 241
サポート、差分アップデート 239
手動 239
初期設定値 366
製品 239
予約、自動 242
移行、InterScan VirusWall の以前のバージョン
から本バージョン 53、57
移行、本バージョンへ 369
移行レポート
エクスポート 53、57
場所 53、57
依存プロキシモード
HTTP プロキシサーバ 40、160
HTTP プロキシ設定 162
インストール 45
InterScan VirusWall、元のサーバと同じコン
ピュータ 33
InterScan VirusWall、元のサーバとは別のコン
ピュータ 33
移行、同一ホスト上の InterScan VirusWall の
以前のバージョンから本バージョン 53、57
移行、前のバージョンの設定 50、56
移行レポート 53、57
インストール、InterScan VirusWall の以前の
バージョンがインストールされている場合の
InterScan VirusWall 53
インストール前のチェックリスト 43

概要 29

計画、インストール 29

決定、InterScan VirusWall のインストール先

33

新規インストール、InterScan VirusWall 46-49

想定されるトポロジ 34

FTP 38-39

HTTP 40

POP3 36-37

SMTP 34-35

インストール前のチェックリスト、InterScan
VirusWall 43

インターネットセキュリティグループ 144

インライン通知

POP3 188

SMTP 72

ウイルス

InterScan VirusWall の検出方法 26

POP3 通知設定 187-189

SMTP 通知設定 71

隔離 69、187

削除 69、187

そのまま配信 187

放置 69

有効化、HTTP 検索 127

有効化、POP3 検索 185

有効化、SMTP 検索 65

ウイルス検出 26

HTTP 検索処理 137

POP3 検索処理 187

SMTP 検索処理 69

ウイルスシグネチャ 26

ウイルスパターンファイル 238

差分アップデート 239

ウイルス流布、HTTP フィッシングカテゴリ
138

同じコンピュータへのインストール 33

オンラインヘルプ 18

か

カウンタ、Windows パフォーマンスモニタ 282

隔離 229

HTTP ウイルス検索処理 136

HTTP スパイウェア / グレーウェア対策処理
143

POP3 IntelliTrap 処理 195

POP3 ウイルス検索処理 187

POP3 コンテンツフィルタ処理 216

POP3 スパイウェア / グレーウェア処理 210

POP3 スпамメール対策処理 205

POP3 添付ファイルコンテンツフィルタ処理
219

POP3 フィッシング対策処理 197

SMTP IntelliTrap 処理 77

SMTP ウイルス検索処理 69

SMTP コンテンツフィルタ処理 109

SMTP スパイウェア / グレーウェアの処理 98

SMTP スпамメール対策処理 92

SMTP 添付ファイルコンテンツフィルタ処理
114

SMTP フィッシング対策処理 80

検索機能 229-231

- 初期設定値 365
- 初期設定ディレクトリ、各プロトコル 232
- 生成、クエリ 230
- ディレクトリとファイルの管理 233-235
- ファイルが表示されない、クエリ結果テーブル 289
- 変更、検索用の隔離ディレクトリ 233
- カテゴリ
 - フィッシング 138
- 管理 261
 - 隔離 233-235
 - ログ 257-259
- キーワード除外、指定 89、202
- キーワードフィルタ 102-111、212-217
- キーワードポリシー 106-107、215
- キーワードリスト 102-105、212-215
- 機能
 - HTTP サービス 125
 - InterScan VirusWall 22
 - POP3 サービス 183
 - SMTP 63
- キュー、SMTP メール 120
- 許可
 - HTTP スパイウェア / グレーウェア対策処理 143
 - HTTP フィッシングサイト 139
- クエリ
 - ログ 252-257
- 駆除
 - HTTP ウイルス検索処理 136
- クライアント
 - 数、同時 SMTP 接続 121
 - 数、同時 POP3 接続 221
- グリーティング、SMTP サービス 122
- グレーウェア 94、140、207
- 計画、InterScan VirusWall のインストール 29
- 検索
 - HTTP または FTP トラフィックが結果に表示されない 289
 - POP3 圧縮ファイル 186
 - POP3 隔離処理 187
 - POP3 削除処理 187
 - POP3 処理 187
 - POP3 そのまま配信処理 187
 - SMTP 圧縮ファイル 67
 - SMTP 隔離処理 69
 - SMTP 削除処理 69
 - SMTP 処理 69
 - SMTP 放置処理 69
 - 圧縮ファイル 27
 - 隔離 229-231
 - 結果テーブルのフィールド 255-257
 - 指定、隔離ディレクトリ 233
 - 指定、スパイウェア / グレーウェアの種類 97、142、209
 - 生成、隔離クエリ 230
 - 選択、HTTP 検索のファイルタイプ 127-135
 - 選択、POP3 検索のファイルタイプ 185
 - 選択、SMTP 検索のファイルタイプ 66
 - 操作、結果テーブル 231
- 検索エンジン 238
- 検出レベル、スパムメール 88-89、201-202

コマンド、サポート 313-314

コンテンツフィルタ

POP3 220

POP3 初期設定値 349

SMTP 116

SMTP 初期設定値 335

ポリシー、キーワードベース 102-111、

212-217

ポリシー、添付ファイルベース 111-116、

217-220

さ

サーバ

POP3 ポートマッピング 37

SMTP 認証 289

設定、SMTP 118

トラブルシューティング、メールの送信時または SMTP ポートへの接続時に SMTP サーバが突然接続を終了する 290

トレンドマイクロのアップデート 237

サーバアドレス情報のチェックリスト 311-312

サービス

HTTP 125、126

POP3 183

SMTP 63

サイズの大きいファイルの処理 134

最大数、同時 POP3 接続 221

削除

POP3 IntelliTrap 処理 195

POP3 ウイルス検索処理 187

POP3 コンテンツフィルタ処理 216

POP3 スパイウェア / グレーウェア処理 210

POP3 スпамメール対策処理 205

POP3 添付ファイルコンテンツフィルタ処理 219

POP3 フィッシング対策処理 197

SMTP IntelliTrap 処理 77

SMTP ウイルス検索処理 69

SMTP コンテンツフィルタ処理 109

SMTP スパイウェア / グレーウェアの処理 98

SMTP スпамメール対策処理 92

SMTP 添付ファイルコンテンツフィルタ処理 114

SMTP フィッシング対策処理 80

ログ 257、259

削除、隔離ファイル 233-235

自動削除 234

手動 234

作成、ポリシー 102-108、212-216

サポートされているコマンド 313-314

システムチェックリスト 311-314

システム要件 30

システムログ 260

実際のファイルタイプによる識別 66、128、185

自動アップデート

トレンドマイクロ 237

自動アップデート、パターンファイル、検索エンジン、および URL フィルタデータベース 242

受信メール

受け入れ、特定のドメインのみ 122

- 指定、最大サイズ 121
- 設定、SMTP 118-119
- 承認する送信者およびブロックする送信者リスト 90、203
- ワイルドカードのサポート 90、204
- 証明書
 - 製品ライセンス 261
- 初期設定値 315-366
- 処理
 - HTTP 隔離 136、143
 - HTTP 許可 139、143
 - HTTP 駆除 136
 - HTTP スパイウェア / グレーウェア 142
 - HTTP そのまま配信 136
 - HTTP ブロック 136、139、143
 - POP3 IntelliTrap 195
 - POP3 ウイルス検出 187
 - POP3 隔離 187、195、197、205、210、216、219
 - POP3 コンテンツフィルタ 216
 - POP3 削除 187、195、197、205、210、216、219
 - POP3 スパイウェア / グレーウェア 209
 - POP3 スпамメール対策 205
 - POP3 スпамメール通知スタンプ 205
 - POP3 そのまま配信 187、195、210
 - POP3 添付ファイルコンテンツフィルタ 219
 - POP3 フィッシングメール 197
 - POP3 放置 197、205、216、219
 - SMTP IntelliTrap 77
 - SMTP ウイルス検出 69
 - SMTP 隔離 69、77、80、92、98、109、114
 - SMTP コンテンツフィルタ 109
 - SMTP 削除 69、77、80、92、98、109、114
 - SMTP スパイウェア / グレーウェア 98
 - SMTP スпамメール対策 91
 - SMTP スпамメール通知スタンプ 92
 - SMTP そのまま配信 77、98
 - SMTP 添付ファイルコンテンツフィルタ 114
 - SMTP フィッシングメール 80
 - SMTP 放置 69、80、92、109、114
- 処理、サイズの大きいファイル 134
- スタンドアロンモード
 - FTP プロキシサーバ 38
 - HTTP プロキシサーバ 40、160
 - HTTP プロキシ設定 162
- スタンプ
 - POP3 スпамメール対策処理 205
 - SMTP スпамメール対策処理 92
- ステータス、大規模感染予防サービスの確認 226
- スパイウェア / グレーウェア
 - 指定、検索する種類 97
 - 種類 94
 - 指定、検索する種類 142、209
 - 種類 140、207
 - 設定、HTTP の設定 139-143
 - 設定、POP3 設定 207-211
 - 設定、SMTP の設定 94-100
 - 通知設定 99、143、210
 - パターンファイル 238
- スパムメール

- 検出レベル 88-89、201-202
- 設定、検出レベル 87、200
- ルールとエンジンのモジュール、スパムメールの検出 238
- スパムメール対策
 - POP3 初期設定値 349-350
 - SMTP 初期設定値 336-337
 - 設定、POP3 設定 207
 - 設定、SMTP の設定 84-94
 - ルールおよびエンジン 238
- スパムメールフィルタ 84、199
- 製品 Q&A 18
 - URL 18
- 製品のアクティベーション 261-263
- 製品の概要 21、27
- 製品ライセンス証明書 261
- セキュリティの脅威
 - トレンドマイクロ製品による検出方法 239
- 接続
 - 指定、POP3 の種類 221
 - 指定、同時クライアント数 121、221
- 設定
 - HTTP サービス 125-165
 - HTTP スパイウェア / グレーウェアの設定 139-143
 - HTTP トラフィック 159-165
 - HTTP プロキシ設定 162
 - InterScan VirusWall の配置 34
 - POP3 IntelliTrap 設定 194-196
 - POP3 ウイルス検索設定 189
 - POP3 サービス 183
 - POP3 初期設定値 339-348、352
 - POP3 スパイウェア / グレーウェア設定 207-211
 - POP3 スпамメール対策設定 207
 - POP3 トラフィック 220-222
 - SMTP IntelliTrap 設定 75-79
 - SMTP ウイルス検索設定 64
 - SMTP サービス 63、118、122
 - SMTP 受信メッセージ 118-119
 - SMTP 詳細オプション 120-122
 - SMTP 初期設定値 316-335
 - SMTP スパイウェア / グレーウェアの設定 94-100
 - SMTP スпамメール対策設定 84-94
 - SMTP 送信メッセージ 119-120
 - SMTP トラフィック 117-122
 - 移行、InterScan VirusWall の以前のバージョンから本バージョン 53、57
 - 指定、エンドユーザメールクライアントとしての Outlook Express 222-223
 - 初期設定値 315-366
 - 初期設定値、FTP 360、362
 - 初期設定値、HTTP 352-359
 - 初期設定値、アップデート 366
 - 初期設定値、隔離フォルダの管理 365
 - 初期設定値、大規模感染予防サービス 365
 - 初期設定値、ログ 363-364
 - 大規模感染予防サービス 227
 - 設定、HTTP のプロキシ 163-165
 - 専用コンピュータへのインストール 33
 - 送信メール

指定、最大サイズ 121
設定、SMTP 119-120
そのまま配信
HTTP ウイルス検索処理 136
POP3 IntelliTrap 処理 195
POP3 ウイルス検索処理 187
POP3 スパイウェア / グレーウェア処理 210
SMTP IntelliTrap 処理 77
SMTP スパイウェア / グレーウェアの処理 98
ソリューションバンク、「製品 Q&A」を参照
18

た

待機ポート、POP3 221
大規模感染予防サービス 22、225
確認、ステータス 226
初期設定値 365
設定 227
表示、現在のポリシーステータス 226
有効化 225
タグ
POP3 IntelliTrap 通知 196
POP3 インライン通知 189
POP3 ウイルス検索通知メッセージ 188
POP3 コンテンツフィルタ通知 217
POP3 スパイウェア / グレーウェア通知 210
POP3 スпамメール通知 206
POP3 添付ファイルフィルタ通知 220
POP3 フィッシング通知 198
SMTP IntelliTrap 通知 78
SMTP ウイルス検索受信通知メッセージ 71

SMTP コンテンツフィルタ通知 111
SMTP スパイウェア / グレーウェアの通知 99
SMTP スпамメール通知 93
SMTP 添付ファイルフィルタ通知 116
SMTP フィッシング通知 82
チェックリスト
記録、システム情報 311-314
サーバアドレス 311-312
ポート、使用 312
通知
HTTP フィッシングサイト検出 139
POP3 インライン 188
SMTP インライン 72
SMTP 設定、受信メッセージ添付ファイル 71
コンテンツフィルタ 116、220
タグ、IntelliTrap が検出したセキュリティリスク 78、196
タグ、POP3 インライン通知 189
タグ、POP3 コンテンツフィルタ 217
タグ、POP3 スパイウェア / グレーウェア 210
タグ、SMTP コンテンツフィルタ 111
タグ、SMTP スパイウェア / グレーウェア 99
タグ、ウイルス検索メッセージ 71、188
タグ、スパムメール 93、206
タグ、フィッシング検出 82、198
トラブルシューティング、機能していない場合 289
通知設定
HTTP スパイウェア / グレーウェア 143
POP3 IntelliTrap 196
POP3 ウイルス検索 187-189

POP3 コンテンツフィルタ 216
 POP3 スパイウェア / グレーウェア 210
 POP3 スпамメール検出 206
 POP3 添付ファイルフィルタ 220
 POP3 フィッシング 197-198
 SMTP IntelliTrap 78
 SMTP ウイルス検索 71
 SMTP コンテンツフィルタ 109
 SMTP スパイウェア / グレーウェア 99
 SMTP スпамメール検出 93
 SMTP 添付ファイルフィルタ 115-116
 SMTP フィッシング 82-83
 テクニカルサポート 307
 デバッグログ 260、292
 添付ファイルフィルタ 111-116、217-220
 透過モード
 HTTP プロキシサーバ 161
 ドキュメントの表記規則 19
 トポロジ、InterScan VirusWall のインストール 34
 FTP 38-39
 HTTP 40
 POP3 36-37
 SMTP 34-35
 ドメイン制御
 設定、送受信メール 291
 トラブルシューティング 292
 Active Directory 296
 SMTP サーバで認証が必要な場合 289
 SMTP サーバの突然の接続終了、メールの送信時または SMTP ポートへの接続時 290

Windows Active Directory での検索 305
 安全なスタンプファイルを Outlook Express の安全な添付ファイルにする 291
 隔離ファイルが含まれない、隔離クエリ結果 289
 コンポーネントのロールバックが無効になる場合 288
 削除されないフォルダ、InterScan VirusWall のアンインストール後 292
 接続に関する問題 302
 設定、送受信メールのドメイン 291
 送信者または受信者への通知が機能していない 289
 デバッグログ 292
 ドメインコントローラエージェントサービス 296
 ドメインコントローラエージェントに関する問題の解決策 297
 ドメインコントローラエージェントのインストール 296
 ドメインコントローラサーバの接続 300
 ドメインコントローラの自動検出 301
 ファイルが FTP ダウンロードフォルダに残る 290
 ユーザ識別 296、305
 トリクル転送、FTP 290
 トレンドマイクロの自動アップデート 237
 トレンドマイクロの推奨設定 66、128、185

な

認証、InterScan VirusWall で実行されない場合

のトラブルシューティング 289

ネットワーク

HTTP 待機 163

は

配置、InterScan VirusWall 34

バインド、HTTP のネットワークインタフェース 163

パターンファイル

アップデート、手動 239

予約、自動アップデート 242

パターンマッチング 26

表記規則 19

ファイル

HTTP 圧縮ファイル検索 129

POP3 圧縮ファイル検索 186

SMTP 圧縮ファイル検索 67

安全なスタンプファイルを Outlook Express の

安全な添付ファイルにする 291

削除、隔離ファイル 233-235

処理、大きい 134

ログ 251

フィッシング 79、137、196

HTTP カテゴリ 138

POP3 処理 197

SMTP 処理 80

報告された疑わしいまたは既知のサイト 83、

139、198

フィッシング対策

POP3 初期設定値 350

SMTP 初期設定値 338-339

有効化 138

フィッシングパターンファイル 238

フィルタ

POP3 キーワードポリシー 212-217

POP3 添付ファイルフィルタポリシー 217-220

SMTP キーワードポリシー 102-111

SMTP 添付ファイルフィルタポリシー

111-116

コピーまたは削除、コンテンツフィルタポリ
シー 116、220

コンテンツ 116、220

スパムメール 87、200

フィルタ調整、スパムメール 88-89、201-202

ブラウザ 163-165

プロキシ

設定、HTTP のクライアントブラウザ
163-165

設定、InterScan VirusWall の HTTP 設定 162

プロキシサーバ

FTP 38

HTTP 40

プロセス、有効でも実行されない場合のトラブ
ルシューティング 290

ブロック

HTTP ウイルス検索処理 136

HTTP スパイウェア / グレーウェア対策処理
143

HTTP フィッシングサイト 139

ブロック、リレーメッセージ 122

ヘッダ情報、SMTP メッセージ 121

ポートのチェックリスト 312

ポートマッピングサーバ 37、221

報告、フィッシングサイトの可能性のある URL
83、139、198

放置

POP3 コンテンツフィルタポリシー 216

POP3 スпамメール対策処理 205

POP3 添付ファイルコンテンツフィルタポリ
シー 219

POP3 フィッシング対策処理 197

SMTP ウイルス検索処理 69

SMTP コンテンツフィルタポリシー 109

SMTP スпамメール対策処理 92

SMTP 添付ファイルコンテンツフィルタポリ
シー 114

SMTP フィッシング対策処理 80

ポリシー

コピーまたは削除、POP3 コンテンツフィルタ
220

コピーまたは削除、SMTP コンテンツフィル
タ 116

作成 102-108、212-216

追加、POP3 キーワードフィルタ 215

追加、SMTP キーワードフィルタ 106-107

表示、大規模感染予防サービスの現在のス
テータス 226

ま

マップ、POP3 サーバのポート 221

無効化

HTTP サービス 126

POP3 コンテンツフィルタ 211

POP3 サービス 184

SMTP コンテンツフィルタ 102

SMTP サービス 64

メールクライアント、Outlook Express の設定
222-223

メッセージ

設定、受信 SMTP 118-119

設定、送受信メールのドメイン 291

設定、送信 SMTP 119-120

挿入、ヘッダ情報 121

ブロック リレー 122

や

有効化

HTTP ウイルス検索 127

HTTP サービス 126

HTTP スパイウェア検索 140

HTTP フィッシング対策機能 138

IntelliTrap 検索、POP3 195

IntelliTrap 検索、SMTP 76

POP3 ウイルス検索 185

POP3 コンテンツフィルタ 211

POP3 サービス 184

POP3 スパイウェア検索 208

POP3 スпамメール検出 200

SMTP ウイルス検索 65

SMTP コンテンツフィルタ 101

SMTP サービス 64

SMTP スパイウェア検索 96

SMTP スпамメール検出 87

自動削除、ログファイル 258

大規模感染予防サービス 225

デバッグログ 260

予約アップデート 242

要件、システム 30

予約

自動アップデート 242

自動削除、ログ 257

ら

リアルタイム検索モニタ 281-283

リスト

キーワード 102-105、212-215

キーワードの類義語 107-108、216

承認する送信者およびブロックする送信者
90、203

リバースプロキシ 42

リバースプロキシモード

HTTP プロキシサーバ 161

HTTP プロキシ設定 162

リレーメッセージ

ブロック 122

類義語、キーワード 107-108、216

ロールバック

コンポーネント 241

トラブルシューティング、ロールバックが無
効になる場合 288

ログ 251-260

検索結果 255-257

削除、自動 257

削除、手動 259

システム 260

初期設定値 363-364

デバッグ 260

特定、障害とエラー 292

ログクエリ 252-257

ログの種類 251

わ

ワイルドカード

使用、コンテンツのフィルタ時の添付ファイ
ル名 113、218

使用、承認する送信者およびブロックする送
信者リスト 90、204

