

ウイルスバスター™ コーポレートエディション



管理者ガイド

安心を、ひとつ上のステージへ。



トレンドマイクロへのお客様情報の送信について

「Web レビューテーションサービス」「フィッシング詐欺対策」「URL フィルタ」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、コモンゲートウェイインタフェースアプリケーションを使用しているサーバで構築されている Web サイトにアクセスし、ID、パスワード等を入力した場合には、お客様がアクセスした Web ページの URL にお客様が入力した ID、パスワード等が含まれた状態でトレンドマイクロのサーバに送信される場合があります。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。

「ファイルレビュー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」では、プログラムの安全性の判定のために、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場合があります。

「E-mail レビュー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等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/ofac/>」、および「<http://www.bis.doc.gov/complianceandenforcement/ListsToCheck.htm>」

2008 年 12 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令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。

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 WebManager、ISWM、InterScan Message Security Suite、InterScan Web Security Suite、IWSS、TRENDMICRO SERVERPROTECT、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、Trend Micro Policy Server、トレンドマイクロ・プレミアム・サポート・プログラム、License for Enterprise Information Security、LEISec、Trend Park、Trend Labs、Trend Micro Enterprise Protection Strategy、InterScan Gateway Security Appliance、Trend Micro Network VirusWall、Network VirusWall Enforcer、Trend Flex Security、EPS、Trend Micro EPS、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 USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、SPN、および Trend Micro Threat Discovery Appliance は、トレンドマイクロ株式会社の登録商標です。

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

Copyright © 1998-2009 Trend Micro Incorporated. All rights reserved.

目次

はじめに	19
ウイルスバスター Corp. 付属のドキュメント	20
対象読者	21
ドキュメントの表記規則	21
用語	22
 第 1 章 ウイルスバスター Corp. の導入	25
製品の概要	26
このリリースの新機能	26
主要機能と利点	29
ウイルスバスター Corp. サーバ	31
ウイルスバスター Corp. クライアント	33
スマートスキャンサーバ	34
 第 2 章 ウイルスバスター Corp. の使用開始	37
Web コンソール	38
セキュリティの概要	40
ウイルスバスター Corp. クライアントツリー	46
クライアントツリーの一般的なタスク	47
詳細検索オプション	48
クライアントツリーの特定のタスク	48
ウイルスバスター Corp. ドメイン	54
セキュリティコンプライアンス	56

第 1 部：ネットワーク上のコンピュータの保護

第 3 章 ウイルスバスター Corp. クライアントのインストール 65

インストール要件	66
インストール方法	72
Web インストールページからのインストール	74
ブラウザベースのインストールの開始	76
ログオンスク립トウィザードを使用したインストール	76
Client Packager を使用したインストール	79
Client Packager の設定	81
Active Directory を使用した MSI パッケージの配信	84
Microsoft SMS を使用した MSI パッケージの配信	85
ウイルスバスター Corp. Web コンソールからのインストール	88
クライアントのディスクイメージからのインストール	90
脆弱性検索ツールの使用	91
ウイルスバスター Corp. クライアントのインストール	95
一般設定の管理	96
脆弱性検索の実行	99
予約タスクの作成	102
その他の脆弱性検索ツールの設定	102
ウイルスバスター Corp. クライアントへの移行	104
他のエンドポイントセキュリティソフトウェアからの移行	104
ServerProtect 一般サーバからの移行	105
ポストインストール	108
推奨されるポストインストールタスク	109
クライアントのアンインストール	110
Web コンソールからのクライアントのアンインストール	110
クライアントアンインストールプログラムの実行	111
クライアントの手動アンインストール	112

第 4 章 最新の保護状態の維持	117
トレンドマイクロ ウイルスバスター コーポレートエディションの コンポーネントとプログラム	118
ウイルス対策コンポーネント	118
ダメージクリーンナップサービスコンポーネント	121
スパイウェア対策コンポーネント	122
ファイアウォールコンポーネント	122
Web レピュテーションコンポーネント	123
挙動監視コンポーネント	123
プログラム	124
アップデートの概要	126
ウイルスバスター Corp. サーバのアップデート	129
サーバアップデート元	131
サーバアップデートのプロキシ	132
サーバコンポーネントの複製	132
サーバのアップデート方法	135
予約アップデート	135
手動アップデート	135
サーバアップデートログ	136
スマートスキャンサーバのアップデート	137
サーバのアップデート設定	137
クライアントアップデート	139
ウイルスバスター Corp. サーバおよびユーザ指定のアップデート元からの アップデート	140
ユーザ指定アップデート元	141
標準のアップデート元	142
クライアントのアップデート方法	143
自動アップデート	143
手動アップデート	147
アップデート権限	149

クライアントコンポーネントのアップデートのプロキシ	149
クライアントアップデートログ	150
クライアントアップデート通知	151
コンポーネントのロールバック	151
アップデートエージェント	153
アップデートエージェントのシステム要件	153
アップデートエージェント設定	154
アップデートエージェントのアップデート元	154
アップデートエージェントのユーザ指定アップデート元	155
アップデートエージェントの標準アップデート元	156
アップデートエージェントのコンポーネントの複製	157
アップデートエージェントのアップデート方法	157
コンポーネントアップデートの概要	158
 第 5 章 セキュリティリスクからのコンピュータの保護.....	159
セキュリティリスクについて	160
ウイルスと不正プログラム	160
スパイウェアとグレーウェア	162
スパイウェア / グレーウェアがネットワークに入り込む方法	163
潜在的リスクと脅威	163
スパイウェア / グレーウェアに対する防御	164
検索方法	165
スマートスキャンソース	172
標準リスト	173
カスタムリスト	174
検索の種類	176
リアルタイム検索	176
手動検索	177
予約検索	178

ScanNow	179
ScanNow の開始	180
すべての検索の種類に共通の設定	181
検索条件	181
検索除外	184
検出時の処理	186
ウイルス / 不正プログラムの検出時の処理	186
スパイウェア / グレーウェアの検出時の処理	194
検索関連の権限	197
グローバル検索設定	197
セキュリティリスク通知	198
管理者通知設定	198
管理者向けのセキュリティリスクの通知	199
クライアントユーザ向けのセキュリティリスクの通知	201
セキュリティリスクログ	202
ウイルス / 不正プログラムログ	202
スパイウェア / グレーウェアログ	208
スパイウェア / グレーウェア復元ログ	210
大規模感染予防サービス	210
大規模感染の基準と通知	211
大規模感染予防サービス	213
大規模感染予防ポリシー	214
共有フォルダへのアクセスを制限 / 禁止	214
ポートのブロック	214
ファイルおよびフォルダへの書き込みを禁止	216
大規模感染予防サービスの無効化	216
デバイスコントロール	218
デバイスコントロールログ	219

第 6 章 Web ベースの脅威からのコンピュータの保護 221

Web からの脅威について	222
Web レピュテーション	222
位置認識機能	223
Web レピュテーションポリシー	223
承認済み URL	225
Web レピュテーション用プロキシ	225
クライアントユーザ向けの Web からの脅威の通知	226
Web レピュテーションログ	227

第 7 章 ウイルスバスター Corp. ファイアウォールの使用 229

ウイルスバスター Corp. ファイアウォールについて	230
ファイアウォールプロファイルおよびポリシー	232
ファイアウォールポリシー	233
ファイアウォールポリシーの追加および変更	234
ファイアウォール除外テンプレートの編集	236
ファイアウォールプロファイル	239
ファイアウォールプロファイルの追加および編集	242
ファイアウォール権限	243
クライアントユーザ向けのファイアウォール違反通知	243
ファイアウォールログ	244
ウイルスバスター Corp. ファイアウォールのテスト	245
ウイルスバスター Corp. ファイアウォールの無効化	247

第2部：ウイルスバスター CORP. サーバおよびクライアントの管理

第8章 ウイルスバスター Corp. サーバの管理	251
役割ベースの管理	252
ユーザの役割	252
カスタムの役割の追加および変更	255
ユーザアカウント	256
ユーザアカウントの追加および変更	257
1つ以上の Active Directory アカウントの追加	259
Trend Micro Control Manager	260
参照サーバ	263
システムイベントログ	264
ログの管理	265
ログ管理	267
ライセンス	268
ウイルスバスター Corp. データベースバックアップ	270
ウイルスバスター Corp. Web サーバ情報	272
Web コンソールパスワード	272
隔離フォルダ設定	273
Server Tuner	274
ウイルストラッキングセンターへのウイルス情報送信	277
第9章 クライアントの管理	279
コンピュータの位置	280
ゲートウェイ設定インポートツール	282
クライアントの権限とその他の設定	283
スタンドアロン権限	284

検索権限	285
予約検索権限	286
ファイアウォール権限	288
メール検索権限	289
ツールボックス権限	291
プロキシ設定権限	291
コンポーネントアップデート権限	292
アンインストール	292
アンロード	292
アップデート設定	292
Web レピュテーション設定	293
予約検索の設定	293
クライアントセキュリティ設定	294
POP3 メール検索設定	294
クライアントコンソールアクセス制限	294
再起動の通知	295
グローバルクライアント設定	295
検索設定	296
予約検索の設定	300
ファイアウォールログ設定	301
警告設定	302
ウイルスバスター Corp. サービスの再起動	303
クライアントセルフプロテクション	304
ディスク空き容量	305
ネットワークウイルスログ統合の有効化	306
ウイルス / 不正プログラムログ帯域幅設定	306
自動プロキシ設定	306
クライアントのグループ設定	307
サーバとのクライアント接続	307

必要な処理	312
クライアントとサーバ間の接続の確認	314
接続状態の確認ログ	315
クライアントプロキシ設定	315
内部プロキシ	315
外部プロキシ	317
クライアント情報	317
クライアント設定のインポートおよびエクスポート	318
オフラインクライアントの管理	319

第 3 部 : その他の保護の提供

第 10 章 Policy Server for Cisco NAC	323
Policy Server for Cisco NAC について	324
コンポーネントおよび用語	324
Cisco NAC 構成	327
クライアント検証シーケンス	328
ポリシーサーバ	330
ポリシーサーバのポリシーとルール	331
ルール構成	331
初期設定のルール	333
ポリシー構成	336
初期設定のポリシー	337
同期	338
証明書	338
CA 証明書について	339
ポリシーサーバのシステム要件	340
Cisco Trust Agent (CTA) の要件	341

サポートされるプラットフォームと要件	342
ポリシーサーバのインストール	343
Cisco Secure ACS サーバ登録	344
CA 証明書のインストール	344
Cisco Trust Agent の配信	346
ウイルスバスター Corp. サーバをインストールする際の CTA の配信	346
ウイルスバスター Corp. Web コンソールからの CTA の配信	347
Cisco Trust Agent のインストールの確認	350
Cisco NAC 用ポリシーサーバのインストール	350
ポリシーサーバ SSL 証明書の準備	353
ACS サーバ設定	354
ポリシーサーバの設定	355
ウイルスバスター Corp. からのポリシーサーバ設定	355
ポリシーサーバの概要情報の表示	356
ポリシーサーバ登録	357
ルール	358
ポリシー	358
クライアント検証ログ	358
クライアントログのメンテナンス	358
管理タスク	359

第 11 章 サードパーティソフトウェアでのウイルスバスター Corp. の設定361

Check Point ファイアウォールのアーキテクチャの概要と設定	362
ウイルスバスター Corp. の統合	363
ウイルスバスター Corp. 用 Check Point の設定	364
SecureClient サポートのインストール	366

第 12 章 サポート情報.....	367
トラブルシューティングのリソース	368
ケース診断ツール	368
ウイルスバスター Corp. サーバログ	368
LogServer.exe を使用するサーバデバッグログ	368
インストールログ	370
コンポーネントアップデートログ	370
クライアントパッケージ作成ログ	371
ServerProtect 一般サーバ移行ツールログ	371
VSEncrypt ログ	372
Control Manager MCP エージェントデバッグログ	372
ウイルス検索エンジンログ	373
アウトブレイクログ	373
ウイルストラッキングセンターログ	374
ウイルスバスター Corp. クライアントログ	374
LogServer.exe を使用するクライアントデバッグログ	374
新規インストールログ	375
アップグレード /HotFix ログ	375
ダメージクリーンナップサービスデバッグログ	375
メール検索ログ	376
クライアント接続ログ	376
クライアントアップデートログ	376
大規模感染予防サービスログ	376
ウイルスバスター Corp. ファイアウォールログ	377
Web 評価および POP3 メール検索のログ	378
転送ドライバインタフェース (TDI) デバッグログ	378
製品サポート情報	380
サポートサービスについて	380
製品 Q&A のご案内	381

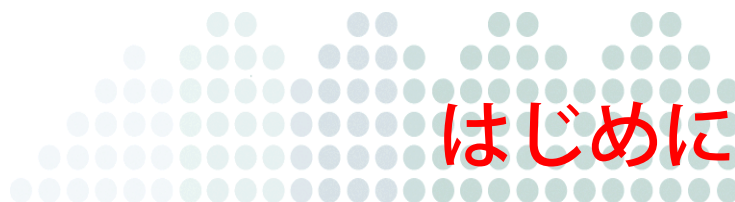
ウイルス解析サポートセンター「TrendLabs」	381
セキュリティ情報	381
セキュリティ情報の入手先	381
トレンドマイクロへのウイルス解析依頼	382
 付録 A 用語集	 383
 索引	 399

表の一覧

表 1: ウイルスバスター Corp. 付属のドキュメント	20
表 2: ドキュメントの表記規則	21
表 3: ウイルスバスター Corp. の用語	22
表 1-1: クライアントの機能	33
表 1-2: スマートスキャンサーバの種類の比較	36
表 2-1: ウイルスバスター Corp. Web コンソールの URL	38
表 2-2: クライアント管理タスク	49
表 2-3: コンピュータ保護ステータス	58
表 3-1: Windows 2000	66
表 3-2: Windows XP/2003 (32 ビットバージョン)	67
表 3-3: Windows XP/2003 (64 ビットバージョン)	68
表 3-4: Windows Vista (32 ビットおよび 64 ビットバージョン)	69
表 3-5: Windows 2008 (32 ビットバージョン)	70
表 3-6: Windows 2008 (64 ビットバージョン)	71
表 3-7: インストール方法	72
表 3-8: クライアントパッケージの種類	79
表 3-9: ネットワーク管理	91
表 3-10: ネットワークトポロジとアーキテクチャ	92
表 3-11: ソフトウェア / ハードウェア仕様	92
表 3-12: ドメイン構造	93

表 3-13: ネットワークトラフィック	93
表 3-14: ネットワークサイズ.....	94
表 3-15: 脆弱性検索ツールでチェックされるセキュリティ製品.....	96
表 3-16: TMVS.ini ファイルの DHCP 設定.....	101
表 4-1: サーバとクライアントのアップデートオプション	127
表 4-2: スマートスキャンサーバのアップデート処理.....	128
表 4-3: ウイルスバスター Corp. サーバがダウンロード可能なコンポーネント	129
表 4-4: サーバコンポーネントの複製のシナリオ.....	133
表 4-5: クライアントによって保存されるウイルスバスター Corp. の コンポーネント	139
表 4-6: イベント起動配信のオプション.....	145
表 4-7: クライアントコンポーネントのアップデート時に使用するプロシキ設定	149
表 4-8: アップデートエージェントのシステム要件.....	153
表 5-1: 従来型スキャンとスマートスキャンの比較.....	166
表 5-2: 検索の種類.....	176
表 5-3: 未通知のクライアントのシナリオ.....	181
表 5-4: ウイルス / 不正プログラムに適用されるトレンドマイクロの推奨処理.....	188
表 5-5: 隔離ディレクトリ.....	189
表 5-6: ウイルスバスター Corp. が復号化および復元可能なファイル	191
表 5-7: 復元パラメータ	193
表 5-8: セキュリティリスク通知のトークン変数.....	200
表 5-9: 大規模感染通知のトークン変数.....	212

表 5-10: デバイスの権限	218
表 7-1: 初期設定のファイアウォールポリシー	233
表 7-2: 初期ファイアウォールポリシー除外	237
表 9-1: 圧縮ファイルのシナリオと結果	298
表 9-2: オンラインクライアントのアイコン	308
表 9-3: オフラインクライアントのアイコン	309
表 9-4: スタンドアロンクライアントのアイコン	311
表 10-1: Cisco NAC ポリシーサーバのコンポーネント	324
表 10-2: Cisco NAC 用ポリシーサーバに関する用語	325
表 10-3: 初期設定のルール	333
表 10-4: 初期設定のポリシー	337
表 10-5: Cisco NAC 証明書	338
表 10-6: サポートされるプラットフォームと要件	342
表 11-1: SCV ファイルパラメータ名と値	365
表 A-1: トロイポート	392



はじめに

トレンドマイクロ ウイルスバスター コーポレートエディション (以下、ウイルスバスター Corp.) 管理者ガイドへようこそ。このドキュメントでは、使用開始の手順、クライアントのインストール手順、およびウイルスバスター Corp. サーバとクライアントの管理について説明します。

この章で説明する内容には、次の項目が含まれます。

- 20 ページの「ウイルスバスター Corp. 付属のドキュメント」
- 21 ページの「対象読者」
- 21 ページの「ドキュメントの表記規則」
- 22 ページの「用語」

ウイルスバスター Corp. 付属のドキュメント

ウイルスバスター Corp. に付属するドキュメントは以下のとおりです。

表 1. ウイルスバスター Corp. 付属のドキュメント

ドキュメント	説明
インストールガイド	ウイルスバスター Corp. サーバをインストールし、サーバとクライアントをアップグレードするための要件および手順を説明した PDF ドキュメント
管理者ガイド	使用開始にあたっての情報、クライアントのインストール手順、およびウイルスバスター Corp. サーバとクライアントの管理について説明した PDF ドキュメント
ウイルスバスター Corp. 用スマートスキャン クイックスタートガイド	スマートスキャンの概念、スマートスキャンを使用するために必要な環境の準備、およびスマートスキャンクライアントの管理について説明した PDF ドキュメント
ヘルプ	WebHelp 形式または CHM 形式にコンパイルされた、操作手順、使用にあたってのアドバイス、および目的別の作業手順を提供するオンラインヘルプ。このヘルプには、ウイルスバスター Corp. サーバ、ウイルスバスター Corp. クライアント、ポリシーサーバのコンソール、およびウイルスバスター Corp. サーバセットアップからアクセスできます。
Readme ファイル	既知の問題のリストと基本的なインストール手順が含まれています。ヘルプや印刷物では見られない、最新の製品情報も含まれています。
製品 Q&A	問題解決およびトラブルシューティング情報のオンラインデータベースです。製品の既知の問題に関する最新の情報を得ることができます。製品 Q&A にアクセスするには、以下の Web サイトをご覧ください。 http://esupport.trendmicro.co.jp/

最新のドキュメントおよび Readme ファイルは、次の Web サイトからダウンロードできます。

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

対象読者

ウイルスバスター Corp. 付属のドキュメントは、次のユーザを対象としています。

- ウイルスバスター Corp. 管理者：サーバおよびクライアントのインストールと管理を含むウイルスバスター Corp. 管理の責任者。ネットワークおよびサーバ管理についての高度な知識を持つユーザであることが想定されています。
- Cisco NAC 管理者：Cisco NAC サーバおよび Cisco ネットワーク機器を使用したセキュリティシステムの設計およびメンテナンスの責任者。対象機器の使用経験があるユーザであることが想定されています。
- エンドユーザ：使用しているコンピュータにウイルスバスター Corp. クライアントをインストールしているユーザ。コンピュータ初心者から上級ユーザまでを対象としています。

ドキュメントの表記規則

情報を簡単に特定して理解できるようにするため、ウイルスバスター Corp. 付属のドキュメントでは次の表記規則を使用しています。

表 2. ドキュメントの表記規則

表記規則	説明
注意： テキスト	設定上の注意事項または推奨事項について説明します。
ヒント： テキスト	ベストプラクティス情報およびトレンドマイクロの推奨事項について説明します。
警告： テキスト	ネットワーク上のコンピュータが損傷を受ける可能性のある操作について警告します。

用語

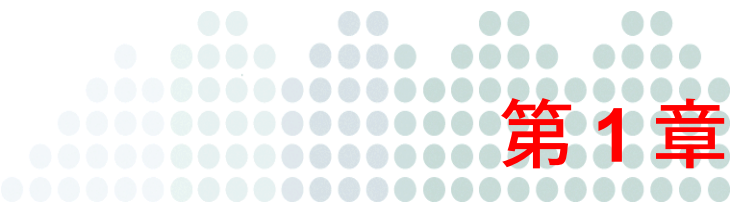
次の表は、ウイルスバスター Corp. 付属のドキュメントで使用されている正式な用語を示しています。

表 3. ウイルスバスター Corp. の用語

用語	説明
クライアント	ウイルスバスター Corp. クライアントプログラム
クライアントコンピュータまたはエンドポイント	ウイルスバスター Corp. クライアントがインストールされているコンピュータ
クライアントユーザ (またはユーザ)	クライアントコンピュータでウイルスバスター Corp. クライアントを使用する人
サーバ	ウイルスバスター Corp. サーバプログラム
サーバコンピュータ	ウイルスバスター Corp. サーバがインストールされているコンピュータ
管理者 (またはウイルスバスター Corp. 管理者)	ウイルスバスター Corp. サーバを管理する人
コンソール	ウイルスバスター Corp. サーバおよびクライアントを設定および管理するためのユーザインタフェース。 ウイルスバスター Corp. サーバプログラム用のコンソールを「Web コンソール」、クライアントプログラム用のコンソールを「クライアントコンソール」と呼びます。
セキュリティリスク	ウイルス / 不正プログラム、スパイウェア / グレーウェア、および Web からの脅威の総称
製品サービス	ウイルス対策、ダメージクリーンナップサービス、Web レピュテーションおよびスパイウェア対策を含みます。これらはすべてウイルスバスター Corp. サーバのインストール時にアクティベートされます。
ウイルスバスター Corp. サービス	Microsoft 管理コンソール (MMC) によってホストされるサービス。たとえば、OfficeScan Master Service の ofcservice.exe などです。
プログラム	ウイルスバスター Corp. クライアント、Cisco Trust Agent、およびプラグインマネージャを含みます。

表 3. ウイルスバスター Corp. の用語 (続き)

用語	説明
コンポーネント	セキュリティ上の脅威の検索、検出、および処理を実行するものです。
クライアントのインストールフォルダ	ウイルスバスター Corp. クライアントのファイルが含まれるコンピュータ上のフォルダ。インストール時の初期設定を受け入れると、インストールフォルダは次のいずれかの場所に設定されます。 C:¥Program Files¥Trend Micro¥OfficeScan Client C:¥Program Files (x86)¥Trend Micro¥OfficeScan Client
サーバのインストールフォルダ	ウイルスバスター Corp. サーバのファイルが含まれるコンピュータ上のフォルダ。インストール時の初期設定を受け入れると、インストールフォルダは次のいずれかの場所に設定されます。 C:¥Program Files¥Trend Micro¥OfficeScan C:¥Program Files (x86)¥Trend Micro¥OfficeScan たとえば、サーバのインストールフォルダで ¥PCCSRV の下にあるファイルのフルパスは次のようになります。 C:¥Program Files¥Trend Micro¥OfficeScan¥PCCSRV¥< ファイル名 >
スマートスキャンクライアント	スマートスキャンを使用するように設定されているウイルスバスター Corp. クライアント
従来型スキャンクライアント	従来型スキャンを使用するように設定されているウイルスバスター Corp. クライアント



第1章

ウイルスバスター Corp. の導入

この章で説明する内容には、次の項目が含まれます。

- 26 ページの「製品の概要」
- 26 ページの「このリリースの新機能」
- 29 ページの「主要機能と利点」
- 31 ページの「ウイルスバスター Corp. サーバ」
- 33 ページの「ウイルスバスター Corp. クライアント」
- 34 ページの「スマートスキャンサーバ」

製品の概要

トレンドマイクロ ウイルスバスター コーポレートエディション（以下、ウイルスバスター Corp.）は、不正プログラム、ネットワークウイルス、Web ベースの脅威、スパイウェア、および複合型の脅威の攻撃から企業のネットワークを保護します。統合ソリューションであるウイルスバスター Corp. は、エンドポイントに配置されたクライアントプログラムと、それらすべてのクライアントを管理するサーバプログラムで構成されます。クライアントプログラムはエンドポイントを保護し、そのセキュリティステータスをサーバに報告します。サーバでは、Web ベースの管理コンソールによって、統一されたセキュリティポリシーの設定と各クライアントへのアップデートの配信を容易に行えます。

ウイルスバスター Corp. は、次世代のクラウド - クライアント型インフラストラクチャである Trend Micro Smart Protection Network を備え、従来型の手法よりも高性能なセキュリティの配信を実現します。独自の In the cloud テクノロジーとより軽量なクライアントを使用することで、パターンファイルのダウンロードに依存していた従来の負担を軽減し、デスクトップのアップデートに伴う一般的な遅延を解消します。使用可能なネットワーク帯域幅の増加、処理電力の低減、および関連コストの削減によって、多くのビジネスにメリットがもたらされます。ユーザは、企業ネットワーク内、自宅、外出先のいずれの場所からでも、最新のセキュリティ対策に直接アクセスすることができま

このリリースの新機能

ウイルスバスター Corp. に含まれる新しい機能および強化は次のとおりです。

スマートスキャン

スマートスキャンは、セキュリティ機能をエンドポイントからクラウドに移行します。Trend Micro Smart Protection Network に不可欠な部分として、スマートスキャンは以下のメリットを提供します。

- ・ クラウド内での高速でリアルタイムなセキュリティステータススルックアップ機能（自身のセキュリティステータスを確認する機能）の提供
- ・ 新たな脅威に対する保護を提供するのにかかる全体時間の短縮
- ・ パターンアップデートで消費されるネットワーク帯域幅の削減。パターン定義の大部分のアップデートはクラウドにのみ配信します。多数のエンドポイントに配信する必要はありません。
- ・ 企業全体のパターン配信に伴うコストとオーバーヘッドの削減
- ・ エンドポイントにおけるカーネルメモリ消費量の低下。

スマートスキャンの配信情報については、ウイルスバスター Corp. 用スマートスキャン クイックスタートガイドを参照してください。

Active Directory の統合

ウイルスバスター Corp. では、Microsoft Active Directory サービスを利用して組織内にセキュリティコンプライアンスを適用します。Active Directory に定期的にポーリングを行うことで、セキュリティソフトウェアを搭載していないコンピュータを検出し、クライアントを対象コンピュータにインストールできます。また各自の Active Directory アカウントを使用して、ユーザに Web コンソールのアクセス権を割り当てることもできます。

詳細については、次の項を参照してください。

- 56 ページの「セキュリティコンプライアンス」
- 252 ページの「役割ベースの管理」

役割ベースの管理

役割ベースの管理では、Web コンソールの管理タスクを他の管理者に委任したり、管理者以外のユーザに Web コンソール項目の表示を許可することができます。最初に、ウイルスバスター Corp. Web コンソールの機能に対して特定のアクセス権を持つ役割を作成し、それらの役割をユーザに割り当てます。各ユーザは、カスタムユーザアカウントを作成するか、既存の Active Directory アカウントを使用して管理します。

シングルサインオン機能のサポートにより、ユーザは、Trend Micro Control Manager（以下、Control Manager）からウイルスバスター Corp. Web コンソールにログインできます。

詳細については、252 ページの「役割ベースの管理」を参照してください。

挙動監視

挙動監視は、外部ストレージデバイスやネットワークリソースへのアクセスを制御し、データ漏えいや不正プログラム感染などの潜在的な経路を規制します。またセキュリティ関連のプロセスを常に稼働させておき、ウイルスバスター Corp. クライアントのファイルやレジストリキーを保護することで、エンドポイントのセキュリティ対策を強化します。

挙動監視は次の機能を提供します。

- 218 ページの「デバイスコントロール」
- 304 ページの「クライアントセルフプロテクション」

プラットフォームのサポート

今回の製品リリースでは、サーバおよびクライアントを、Windows Server 2008 や VMware などの仮想アプリケーションにインストールできるようになりました。

クライアントのインストール要件については 66 ページの「インストール要件」を、サーバのインストール要件については「インストールガイド」を参照してください。

製品機能の強化

今回の製品リリースでは、次の機能が強化されています。

パフォーマンス管理

パフォーマンス管理では、検索時に以下を実行することで CPU リソースが効率的に使用されるようになります。

- ウイルスバスター Corp. Web コンソールで設定した CPU 使用率レベルと、コンピュータでの実際の CPU 使用率を確認する
- 次の場合に検索速度を調整する
 - CPU 使用率レベルが中または低に設定されている
 - 実際の CPU 使用率が特定のしきい値を超過している

詳細については、183 ページの「CPU 使用率」を参照してください。

予約検索機能の強化

予約検索権限を持つユーザは、予約検索の遅延、スキップ、および停止を実行できるようになりました。詳細については、286 ページの「予約検索権限」を参照してください。

Web レピュテーションの対象設定

Web レピュテーションポリシーを設定して、それらを 1 台、複数、またはすべてのウイルスバスター Corp. クライアントに割り当てることができます。詳細については、223 ページの「Web レピュテーションポリシー」を参照してください。

注意： 以前の製品で「Web 評価」と呼んでいた機能を、本製品から「Web レピュテーション」に名称変更しています。

主要機能と利点

ウイルスバスター Corp. は、以下の機能および利点を提供します。

セキュリティリスク保護

ウイルスバスター Corp. は、ファイルを検索して、検出されたセキュリティリスクごとに特定の処理を実行することでセキュリティリスクからコンピュータを保護します。短期間に大量の数のセキュリティ上の脅威が検出された場合は大規模感染の兆候を示しています。ウイルスバスター Corp. は、大規模感染予防ポリシーを実行して、感染したコンピュータが完全に危険な状態でなくなるまで隔離することで大規模感染を抑制します。

ウイルスバスター Corp. では、スマートスキャンを使用して、より効率的な検索プロセスを実行します。このテクノロジーは、これまでローカルコンピュータに保存されていた大量のシグネチャを「スマートスキャンサーバ」に移行することで機能します。この手法により、増加し続けるシグネチャアップデートのエンドポイントシステムへの反映がシステムやネットワークに与える影響を著しく低減できます。

スマートスキャンの詳細とクライアントへの配布方法については、ウイルスバスター Corp. 用スマートスキャン クイックスタートガイドを参照してください。

Web レピュテーション

ウイルスバスター Corp. に統合された Web レピュテーションテクノロジーは、企業ネットワークの内部または外部に存在するクライアントコンピュータを、予防措置によって不正な Web サイトや危険と考えられる Web サイトから保護します。Web レピュテーションにより感染経路は遮断され、不正コードのダウンロードも阻止されます。

ダメージクリーンナップサービス

ダメージクリーンナップサービスは、ファイルベースのコンピュータウイルス、ネットワークウイルス、およびウイルスやワームの残骸（トロイの木馬、レジストリ侵入、ウイルスファイル）を完全に自動化されたプロセスを使用して駆除します。ダメージクリーンナップサービスでは、トロイの木馬の脅威および妨害に対して次のように対処します。

- ・ 活動中のトロイの木馬を検出および削除
- ・ トロイの木馬が作成したプロセスを中止
- ・ トロイの木馬が変更したシステムファイルを修復
- ・ トロイの木馬により作成されたファイルとアプリケーションを削除

ダメージクリーンナップサービスはバックグラウンドで自動的に実行されるので、設定の必要はありません。ユーザは実行されていることにすら気が付きません。ただしウイルスバスター Corp. では、トロイの木馬を削除するプロセスを完了するために、ユーザにコンピュータの再起動を通知することがあります。

ウイルスバスター Corp. のファイアウォール

ウイルスバスター Corp. ファイアウォールは、ステートフルインスペクション、高性能なネットワークウイルス検索、および駆除機能を使用して、ネットワーク上のクライアントとサーバを保護します。IP アドレス、ポート番号、プロトコルなどによって接続をフィルタする複数のルールを作成し、それらのルールを異なるユーザのグループに適用します。

注意： Windows のファイアウォールが有効になっている Windows XP コンピュータにおいて、ウイルスバスター Corp. のファイアウォールをインストール、設定、および使用できます。ただし、ポリシーを注意深く管理し、ファイアウォールポリシーの競合とそれによる予期しない結果の発生を防ぐ必要があります。たとえば、一方のファイアウォールが特定のポートからのトラフィックを許可し、もう一方のファイアウォールが同じポートからのトラフィックを拒否した場合、ウイルスバスター Corp. はそのトラフィックをブロックします。Windows のファイアウォールの詳細については、Microsoft 社から提供されているマニュアルを参照してください。

セキュリティとポリシー強化

ウイルスバスター Corp. は、Cisco Trust Agent とのシームレスな統合を提供し、Cisco の自己防御ネットワーク内で最も有効なポリシー強化を可能にしています。ウイルスバスター Corp. には、Cisco Access Control Server と自動通信を行うためのポリシーサーバも含まれています。ウイルスバスター Corp. を Trend Micro Network VirusWall または任意の Network Admission Control (NAC) デバイスと統合すると、ネットワークに侵入しようとしているクライアントをチェックして、アクセスを是正、リダイレクト、制限、拒否、または許可することができます。コンピュータが脆弱であったり感染したりすると、ウイルスバスター Corp. は、コンピュータとそのネットワークセグメントを、すべてのコンピュータがアップデートされるかクリーンナップが完了するまで自動的に隔離できます。

一元管理

Web ベースの管理コンソールによって、管理者はネットワーク上のすべてのクライアントやサーバへの透過的アクセスが可能になります。Web コンソールは、すべてのクライアントおよびサーバ上のセキュリティポリシー、パターンファイル、およびソフトウェアアップデートの自動配信を調節

します。また大規模感染予防サービスにより、感染媒体を停止し、攻撃別のセキュリティポリシーを迅速に配信して、大規模感染をパターンファイルが使用可能になるまで防止および阻止します。ウイルスバスター Corp. は、リアルタイムの監視、イベント通知、および包括的なレポートの配布を行います。管理者はリモート管理を行い、個々のデスクトップやグループにカスタマイズされたポリシーを設定し、クライアントセキュリティ設定をロックすることができます。

プラグインマネージャとプラグインプログラム

新しい製品バージョン、Service Pack、および Patch に付属しているプラグインプログラムは、ウイルスバスター Corp. に新しい機能とセキュリティ対策を追加し、製品のパフォーマンスを強化するように設計されています。プラグインプログラムのインストール、配信、および管理は、プラグインマネージャから実行できます。

ウイルスバスター Corp. サーバでは、新しいバージョンのプログラムとともに、プラグインマネージャとプラグインプログラムがトレンドマイクロのアップデートサーバからダウンロードされます。

ウイルスバスター Corp. サーバ

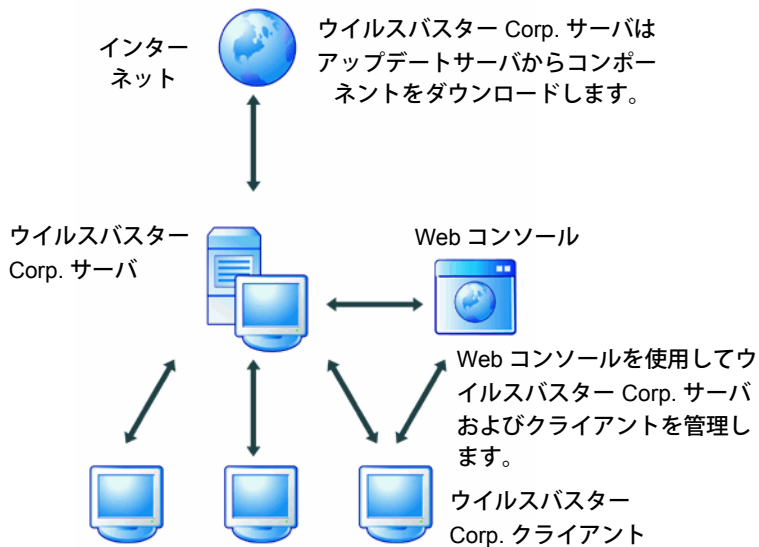
ウイルスバスター Corp. HTTP ベースサーバは、すべてのクライアント設定、セキュリティリスクログ、およびアップデートの中央リポジトリです。

サーバは、次の 2 つの重要な機能を実行します。

- ウイルスバスター Corp. クライアントのインストール、監視、および管理
- クライアントに必要な大半のコンポーネントのダウンロード。ウイルスバスター Corp. サーバでは、コンポーネントがトレンドマイクロのアップデートサーバからダウンロードされ、クライアントに配信されます。

注意： 一部のコンポーネントはスマートスキャンサーバによってダウンロードされます。詳細については、34 ページの「スマートスキャンサーバ」を参照してください。

図 1-1. ウイルスバスター Corp. サーバの動作



ウイルスバスター Corp. サーバは、サーバとクライアント間にリアルタイムの双方向通信を提供できます。クライアントは、ネットワーク上のどこからでも仮想的にアクセス可能なブラウザベースの Web コンソールで管理します。サーバは、ハイパーテキスト転送プロトコル (HTTP) を通してクライアントと通信します。

ウイルスバスター Corp. クライアント

それぞれのコンピュータにウイルスバスター Corp. クライアントをインストールすることで、セキュリティ上の脅威から Windows コンピュータを保護します。クライアントは、リアルタイム検索オプション、予約検索オプション、および手動検索オプションの3つの検索オプションを提供します。

クライアントは、ウイルスバスター Corp. サーバにステータスを報告します。クライアントは、イベントおよびステータス情報をリアルタイムでサーバに送信します。イベントには、ウイルス / 不正プログラムの検出、クライアントの起動、クライアントの終了、検索の開始、アップデートの完了などがあります。

クライアントの主要機能

使用可能なウイルスバスター Corp. クライアントの機能は、コンピュータのオペレーティングシステムによって異なります。

表 1-1. クライアントの機能

機能	Windows オペレーティングシステム				
	2000	XP/ Server 2003 (32 ビット)	XP/ Server 2003 (64 ビット)	2008	Vista
手動検索、リアルタイム検索、予約検索	可	可	可	可	可
コンポーネントアップデート (手動および予約アップデート)	可	可	可	可	可
アップデートエージェント	可	可	可	可	可
Web レピュテーション	可	可	可	可	可
Microsoft Outlook メール検索	可	可	不可	不可	不可
POP3 メール検索	可	可	可	可	可

表 1-1. クライアントの機能 (続き)

機能	Windows オペレーティングシステム				
	2000	XP/ Server 2003 (32 ビット)	XP/ Server 2003 (64 ビット)	2008	Vista
ウイルスバスター Corp. の ファイアウォール	可	可	可	可	可
ダメージクリーンナップ サービス	可	可	可	可	可
Cisco NAC のサポート	可	可	不可	不可	不可
プラグインマネージャ	可	可	可	不可	可
スタンドアロンモード	可	可	可	可	可
SecureClient サポート	可	可	不可	不可	不可

スマートスキャンサーバ

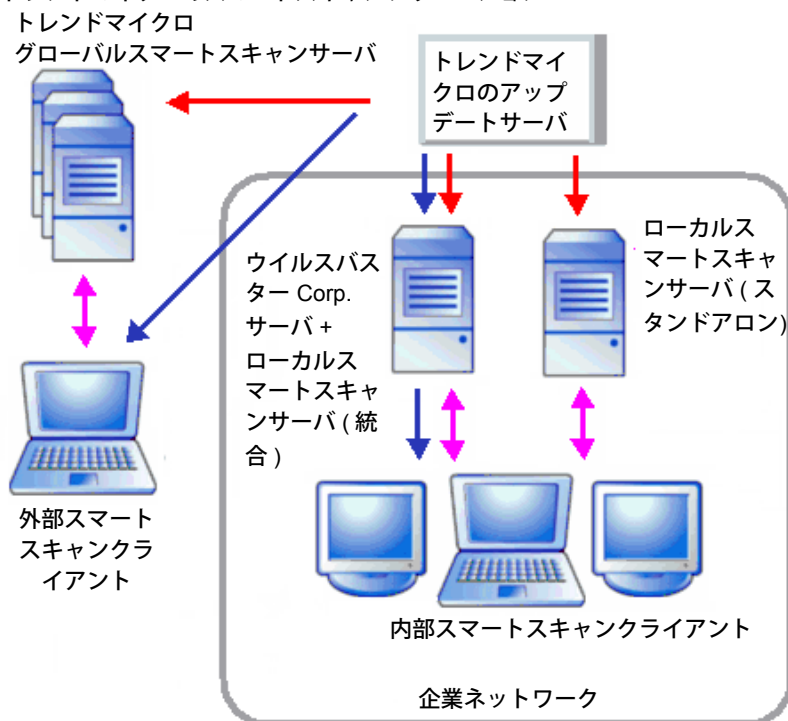
スマートスキャンソリューションでは、連携して動作する軽量のパターンファイルを利用して、従来の不正プログラム対策およびスパイウェア対策パターンファイルと同等のセキュリティ対策を提供します。これらのパターンファイルは、トレンドマイクロのアップデートサーバから配信され、スマートスキャンサーバおよびウイルスバスター Corp. サーバで使用することができます。

スマートスキャンサーバはスマートスキャンパターンを保持します。このパターンファイルは毎時間アップデートされ、パターン定義の大部分が含まれます。スマートスキャンクライアントでは、このパターンファイルはダウンロードされません。クライアントでは、スマートスキャンサーバに検索クエリを送信し、潜在的脅威が検証されます。スマートスキャンソリューションでは、クライアントはトレンドマイクロのテクノロジーによって判別された識別情報をスマートスキャンサーバに送信します。クライアントからファイル全体が送信されることはありません。ファイルの危険性はこの識別情報を使用して判別されます。

注意： スマートスキャンソリューションで使用される別のパターンであるスマートスキャンエージェントパターンは、クライアントのアップデート元（ウイルスバスター Corp. サーバまたはユーザ指定アップデート元）でホストされ、クライアントにダウンロードされます。

スマートスキャンサーバとウイルスバスター Corp. サーバとの間でダウンロードするコンポーネントが重複することはありません。これは、それぞれのサーバが固有のコンポーネントセットをダウンロードするためです。スマートスキャンサーバにはスマートスキャンパターンのみがダウンロードされ、ウイルスバスター Corp. サーバには他のすべてのコンポーネントがダウンロードされます。コンポーネントの詳細については、118 ページの「トレンドマイクロ ウイルスバスター コーポレートエディションのコンポーネントとプログラム」を参照してください。

図 1-2. トレンドマイクロのスマートスキャンソリューション



>> スマートスキャンパターンのアップデート

>> 検索クエリ

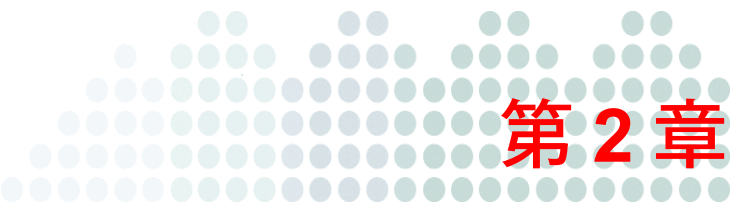
>> スマートスキャンエージェントパターンのアップデート

スマートスキャンサーバの種類

クライアントが接続するスマートスキャンサーバは、クライアントの位置によって異なります。内部スマートスキャンクライアントはローカルのスマートスキャンサーバに接続し、外部スマートスキャンクライアントは Trend Micro グローバルスマートスキャンサーバに接続します。次の表は、2つのスマートスキャンサーバの種類を比較したものです。

表 1-2. スマートスキャンサーバの種類の比較

比較基準	ローカルスマートスキャンサーバ	Trend Micro グローバルスマートスキャンサーバ
利用可能性	内部クライアント、つまりウイルスバスター Corp. Web コンソールで指定した位置の基準に一致するクライアントで使用可能。 位置の条件については、280 ページの「コンピュータの位置」を参照してください。	外部クライアント、つまりウイルスバスター Corp. Web コンソールで指定した位置の基準に一致しないクライアントで使用可能。
目的	効率性を最適化するために、企業ネットワークに合わせて検索操作をローカライズするよう設計されている。	企業ネットワークに直接アクセスできないユーザにスマートスキャンサービスを提供する、グローバル規模のインターネットベースインフラストラクチャ。
サーバ管理者	ウイルスバスター Corp. 管理者がこれらのサーバをインストールおよび管理する。	トレンドマイクロがこのサーバを管理する。
パターンアップデート元	トレンドマイクロのアップデートサーバ	トレンドマイクロのアップデートサーバ
クライアント接続プロトコル	HTTP および HTTPS	HTTPS



第2章

ウイルスバスター Corp. の使用開始

この章で説明する内容には、次の項目が含まれます。

- 38 ページの「Web コンソール」
- 40 ページの「セキュリティの概要」
- 46 ページの「ウイルスバスター Corp. クライアントツリー」
- 54 ページの「ウイルスバスター Corp. ドメイン」
- 56 ページの「セキュリティコンプライアンス」

Web コンソール

Web コンソールは、組織ネットワークを通してウイルスバスター コーポレートエディション（以下、ウイルスバスター Corp.）を監視するための中心点です。コンソールには一連の初期設定と値が搭載されており、セキュリティ要件と仕様に基づき設定を行うことができます。Web コンソールは、Java、CGI、HTML、および HTTP などの、標準のインターネットテクノロジーを使用します。

Web コンソールを使って、以下を実行できます。

- ・ ネットワーク上のコンピュータにインストールされたクライアントの管理
- ・ クライアントを論理ドメインにグループ分けして同時設定と管理を実行
- ・ 検索設定をセットして、単一または複数のネットワーク上のコンピュータで手動検索を開始
- ・ ネットワーク上のセキュリティリスクに関する通知を設定し、クライアントから送信されたログを表示
- ・ 大規模感染の基準と通知を設定
- ・ 役割およびユーザアカウントの設定により他のウイルスバスター Corp. 管理者に Web コンソール管理タスクを委任

Web コンソールを開く

次のリソースを持つネットワーク上で、任意のコンピュータから Web コンソールを開きます。

- ・ 300MHz Intel Pentium II プロセッサまたは同等の CPU
- ・ 128MB の RAM
- ・ 30MB 以上のハードディスク空き容量
- ・ 解像度 800x600、256 色以上をサポートするモニタ
- ・ Microsoft Internet Explorer 6.0 以降

Web ブラウザで、ウイルスバスター Corp. サーバのインストールの種類に基づき、アドレスバーに次のいずれかを入力します。

表 2-1. ウイルスバスター Corp. Web コンソールの URL

インストールの種類	URL
既定サイトに SSL がない	http://< ウイルスバスター Corp. サーバ >/OfficeScan
仮想サイトに SSL がない	http://< ウイルスバスター Corp. サーバ >:<SSL ポート番号 >/ ウイルスバスター Corp.

表 2-1. ウイルスバスター Corp. Web コンソールの URL

インストールの種類	URL
既定サイトに SSL がある	https://< ウイルスバスター Corp. サーバ >/OfficeScan
仮想サイトに SSL がある	https://< ウイルスバスター Corp. サーバ >:<SSL ポート番号 >/ ウイルスバスター Corp.

注意： 旧バージョンのウイルスバスター Corp. からアップグレードした場合、Web ブラウザおよびプロキシサーバのキャッシュファイルが原因で、ウイルスバスター Corp. の Web コンソールが正常に読み込まれない場合があります。Web コンソールに正常にアクセスするには、ブラウザのキャッシュメモリ、およびウイルスバスター Corp. サーバとお使いのコンピュータの間に配置されたすべてのプロキシサーバのキャッシュメモリを消去してください。

ログオンアカウント

ウイルスバスター Corp. サーバのインストール時、セットアップによってルートアカウントが作成され、このアカウントのパスワードを入力するよう求められます。初めて Web コンソールを開く場合は、ユーザ名に「root」と入力して、このルートアカウントのパスワードを入力します。パスワードを忘れた場合は、パスワードの再設定についてサポート担当者にお問い合わせください。

ユーザの役割を定義し、ユーザアカウントを設定して、他のユーザがルートアカウントを使用せずに Web コンソールにアクセスできるようにします。ユーザは、コンソールにログオンする際、各自に設定されたユーザアカウントを使用できます。詳細については、252 ページの「役割ベースの管理」を参照してください。

Web コンソールのバナー

Web コンソールのバナー領域には、次のオプションがあります。

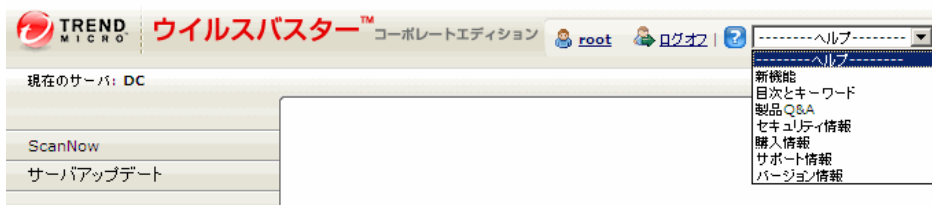


図 2-1. Web コンソールのバナー領域

<アカウント名>: パスワードなど、このアカウントの詳細を変更するにはアカウント名 (例: root) をクリックします。

ログオフ: Web コンソールからログオフします。

ヘルプ

- **新機能**: この製品リリースに含まれる新機能リストを表示したページが開きます。
- **目次とキーワード**: ウイルスバスター Corp. サーバのヘルプが開きます。
- **製品 Q&A**: トレンドマイクロの製品 Q&A が開きます。ここでは、よくある質問や更新された製品情報を表示したり、カスタマーサポートにアクセスしたり、ウイルスバスター Corp. を登録できます。
- **セキュリティ情報**: トレンドマイクロの [セキュリティ情報] Web ページが表示されます。ここでは、最新のセキュリティリスクについて確認できます。
- **購入情報**: トレンドマイクロの [購入情報] Web ページが表示されます。ここから、地域の販売代理店に問い合わせることができます。
- **サポート情報**: トレンドマイクロの [サポート情報] Web ページが表示されます。ここでは、質問を送信したり、トレンドマイクロ製品に関する一般的な質問への回答を見つけることができます。
- **バージョン情報**: 製品の概要が記載されたページが表示されます。ここには、コンポーネントのバージョンの確認方法が示されています。

セキュリティの概要

ウイルスバスター Corp. Web コンソールを開くかメインメニューで [概要] をクリックすると、[概要] 画面が表示されます。ここでは、製品ライセンスや全体的なセキュリティリスク保護の現在のステータスを表示したり、大規模感染や旧版コンポーネントなど、迅速な対応が必要な項目について処理を実行できます。

ヒント: 画面表示を定期的に更新して、最新情報を入手してください。

製品ライセンスのステータス

このセクションには、製品ライセンスのステータスが表示されます。

概要

 表示更新  ヘルプ

アクティベート済みのサービス: デスクトップ/サーバウイルス対策, デスクトップ/サーバ用Webレビュテーションおよび
スパイウェア対策, ファイルレビュテーション, ファイアウォール, ダメージクリーンナップサービス

ステータス概要 (2009/06/16 13:13:20現在)

図 2-2. [概要]画面 - 「製品ライセンスのステータス」セクション

次の場合にはメッセージが表示されます。

製品版ライセンスを使用しているとき

- ・ ライセンスの有効期限の 60 日前である場合。
- ・ 製品の更新猶予期間である場合。更新猶予期間は地域によって異なります。更新猶予期間については、トレンドマイクロの販売代理店にお問い合わせください。
- ・ ライセンスの有効期間が終了し、更新猶予期間が経過した場合。この間、テクニカルサポートを受けたり、コンポーネントのアップデートを実行することはできません。その場合、検索エンジンでは、古いバージョンのパターンファイルを使用して検索が行われます。これらの旧版コンポーネントでは、最新のセキュリティリスクから完全には保護できない可能性があります。

体験版ライセンスを使用しているとき

- ・ ライセンスの有効期限の 14 日前である場合。
- ・ ライセンスの有効期限が切れた場合。この間、ウイルスバスター Corp. では、コンポーネントのアップデート、検索、およびすべてのクライアント機能が無効になります。

アクティベーションコードを取得している場合は、[管理] → [製品ライセンス] に移動してライセンスを更新してください。

ネットワーク上のコンピュータ

[すべて] タブには次の情報が表示されます。



図 2-3. 【概要】画面 - [すべて] タブ

- すべてのウイルスバスター Corp. クライアントとウイルスバスター Corp. サーバとの接続ステータス
- 検出されたセキュリティリスクの数
- セキュリティリスクが検出されたコンピュータ

[従来型スキャン] タブには次の情報が表示されます。

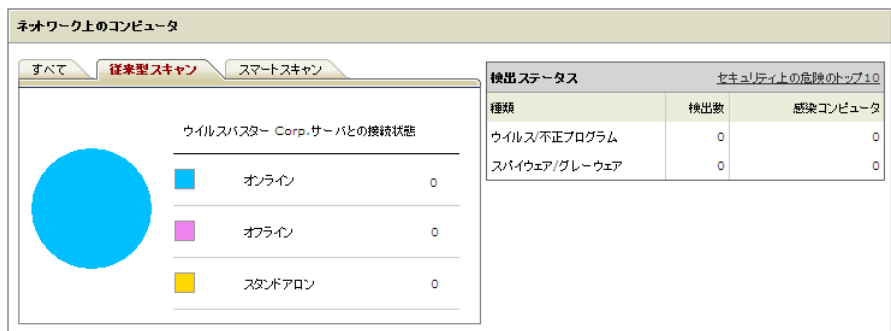


図 2-4. 【概要】画面 - [従来型スキャン] タブ

- 従来型スキャンクライアントとウイルスバスター Corp. サーバとの接続ステータス
- 検出されたセキュリティリスクの数

- ・ セキュリティリスクが検出されたコンピュータ

[スマートスキャン] タブには次の情報が表示されます。

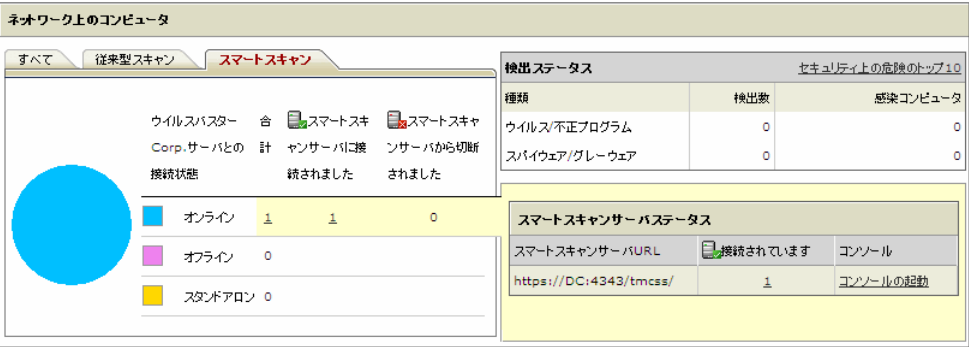


図 2-5. [概要] 画面 - [スマートスキャン] タブ

- ・ スマートスキャンクライアントとウイルスバスター Corp. サーバとの接続ステータス
- ・ オンラインスマートスキャンクライアントとウイルスバスター Corp. サーバとの接続ステータス

注意： スマートスキャンサーバとの接続ステータスを報告できるのはオンラインのクライアントのみです。

クライアントがスマートスキャンサーバから切断されている場合は、313 ページの「クライアントがスマートスキャンサーバに接続できない」の手順を実行して接続を復元してください。

- ・ 検出されたセキュリティリスクの数
- ・ セキュリティリスクが検出されたコンピュータ
- ・ スマートスキャンサーバのリスト
- ・ 各スマートスキャンサーバに接続されているクライアントの数。数字をクリックすると、クライアント設定を管理できるクライアントツリーが表示されます。
- ・ 各スマートスキャンサーバのコンソールを起動するリンク
- ・ [詳細] リンク (2 つ以上のスマートスキャンサーバに接続しているクライアントがある場合)。このリンクをクリックして表示される画面では、以下を実行できます。

- ・ クライアントが接続されているすべてのローカルスマートスキャンサーバと、各サーバに接続されているクライアント数の表示。数字をクリックすると、クライアント設定を管理できるクライアントツリーが表示されます。
- ・ サーバコンソールの起動。コンソールを起動するにはサーバのリンクをクリックします。

セキュリティ上の危険トップ 10

[検出ステータス] 表のリンクをクリックすると、セキュリティリスク統計情報トップ 10 の記載された画面が表示されます。

ネットワーク上のコンピュータのセキュリティ上の危険ステータスのトップ10

概要 > ネットワーク上のコンピュータのセキュリティ上の危険ステータスのトップ10

ウイルス/不正プログラムの統計:

ウイルス/不正プログラム		感染コンピュータ		
名前	感染	名前	検出数	ログ

前回のリセット日:
 前回のリセット日:

スパイウェア/グレーウェアの統計:

スパイウェア/グレーウェア		感染コンピュータ		
名前	感染	名前	検出数	ログ

前回のリセット日:
 前回のリセット日:

図 2-6. 「セキュリティ上の危険トップ 10」画面

この画面のタスクは次のとおりです。

- ・ セキュリティリスク名をクリックすると、セキュリティリスクに関する詳細情報が表示されます。
- ・ コンピュータ名をクリックすると、特定コンピュータの全体的なステータスが表示されます。
- ・ コンピュータ名に対応する [表示] をクリックすると、対象コンピュータのセキュリティリスクログが表示されます。

- ・ [リセット] をクリックすると、各表の統計情報がリセットされます。

アウトブレイクステータス

[アウトブレイクステータス] 表には、現在のセキュリティリスク大規模感染と前回の大規模感染警告のステータスが表示されます。

⚠️ アウトブレイクステータス				
	種類	現在のアウトブレイク	前回のアウトブレイク	
	ウイルス/不正プログラム	なし	なし	リセット
	スパイウェア/グレーウェア	なし	なし	リセット
	ファイアウォール侵害	なし	なし	リセット

図 2-7. 【概要】画面 - 「アウトブレイクステータス」セクション

警告の日時リンクをクリックすると、大規模感染の詳細が表示されます。ウイルスバスター Corp. で大規模感染が検出されたら、大規模感染警告情報のステータスをリセットして、ただちに大規模感染予防策を実行してください。

コンポーネントとプログラム

「アップデートステータス」表には、ネットワーク上のコンピュータをセキュリティリスクから保護するために使用可能なコンポーネントとプログラムが表示されます。

ネットワーク上のコンピュータのアップデートステータス (オンラインクライアント: 1 スマートスキャン: 1 従来型スキャン: 0) ⚠️ すべて折りたたむ ⚙️ すべて展開				
⚠️ ウイルス対策	現在のバージョン	最新	旧版	アップデート率
スマートスキャンエージェントパターン	6.191.00	1	0	100%
ウイルスパターンファイル	6.195.00	0	0	0%
IntelliTrap パターンファイル	0.116.90	1	0	100%
IntelliTrap 除外パターンファイル	0.441.00	1	0	100%
ウイルス検索エンジン (32ビット)	8.950.1092	1	0	100%
ウイルス検索エンジン (64ビット)	8.950.1092	0	0	0%
⚠️ スパイウェア対策	現在のバージョン	最新	旧版	アップデート率
スパイウェアパターンファイル	7.81	1	0	100%
スパイウェア監視パターンファイル	0.781.00	0	0	0%
スパイウェア検索エンジン (32ビット)	6.2.3009	1	0	100%
スパイウェア検索エンジン (64ビット)	6.2.3009	0	0	0%

図 2-8. 【概要】画面 - 「アップデートステータス」セクション

各コンポーネントの現在のバージョンが表示されます。[旧版] 列には、旧版コンポーネントを持つクライアントの数が表示されます。アップデートが必要なクライアントがある場合は、数字のリンクをクリックしてアップデートを開始してください。

プログラムごとにアップグレードされていないクライアントを表示するには、プログラムに対応する数字のリンクをクリックします。

注意： Cisco Trust Agent をアップグレードするには、[Cisco NAC] → [エージェント配信] に移動します。

ウイルスバスター Corp. クライアントツリー

この Java ベースのクライアントツリーには、現在サーバで管理している（「ウイルスバスター Corp. ドメイン」にグループ分けされた）すべてのクライアントが表示されます。クライアントはドメインにグループ分けされているため、同じ設定をすべてのドメインメンバーに同時に設定、管理、および適用できます。

メインメニューから特定の機能にアクセスすると、クライアントツリーがメインフレームに表示されます。

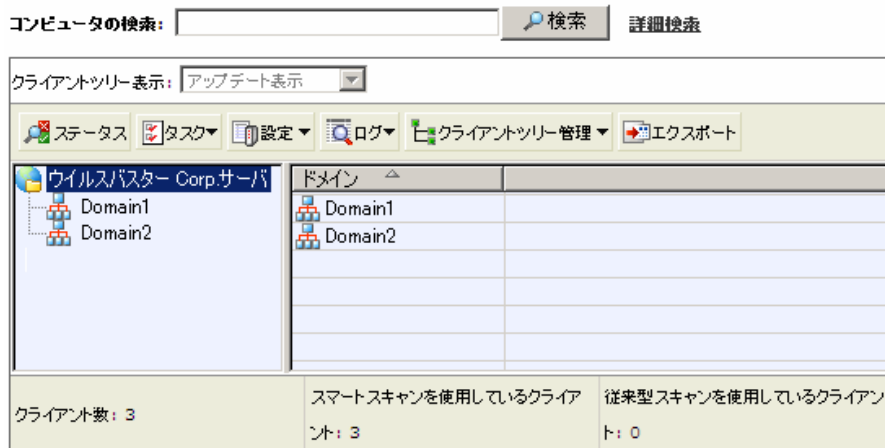


図 2-9. ウイルスバスター Corp. クライアントツリー

クライアントツリーの一般的なタスク

クライアントツリーで実行できる一般的なタスクは次のとおりです。

- すべてのドメインおよびクライアントを選択するには、ルートアイコン  をクリックします。ルートアイコンを選択してからクライアントツリーの上にあるタスクを選択すると、設定画面が表示されます。この画面では、次の一般的なオプションを選択できます。
 - **すべてのクライアントに適用**：すべての既存のクライアント、および既存または将来追加されるドメインに加えられる新しいクライアントに、設定を適用します。将来追加されるドメインとは、設定を指定した時点で作成されていないドメインのことです。
 - **将来追加されるドメインにのみ適用**：将来追加されるドメインに加えられるクライアントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいクライアントには設定を適用しません。
- 複数の隣り合ったドメインやクライアントを選択するには、選択範囲の最初のドメインまたはクライアントをクリックし、<Shift> キーを押しながら最後のドメインまたはクライアントをクリックします。
- 連続していない複数のドメインまたはクライアントを選択するには、<Ctrl> キーを押しながら目的のドメインまたはクライアントをクリックします。
- 管理対象クライアントを検索するには、[コンピュータの検索] ボックスにクライアント名を入力します。一致するクライアント名のリストがクライアントツリーで強調表示されます。より詳細に検索オプションを指定するには、[詳細検索] をクリックします。
- ドメインを選択するとそのクライアントツリー表が展開され、ドメインに属するクライアントと各クライアントの関連情報を含むすべての列が表示されます。特定の関連する列のみを表示するには、[クライアントツリー表示] で項目を選択します。
 - **アップデート表示**：すべてのコンポーネントとプログラムを表示
 - **ウイルス対策表示**：ウイルス対策コンポーネントを表示
 - **ファイアウォール表示**：ファイアウォールコンポーネントを表示
 - **スパイウェア対策**：スパイウェア対策コンポーネントを表示
 - **スマートスキャン表示**：クライアント（従来型 / スマートスキャン）とスマートスキャンコンポーネントで使用されている検索方法を表示
 - **すべて表示**：すべての列を表示
- 列の位置を変えるには、列タイトルをドラッグして、クライアントツリー内の別の場所に移動します。新しい列の位置は自動的に保存されます。
- 列情報に基づいてクライアントを並べ替えるには、列名をクリックします。

- ・ クライアントツリーの表示を更新するには、 をクリックします。
- ・ クライアントツリーの下には、クライアント総数、スマートスキャンクライアントの数、および従来型スキャンクライアントの数などクライアントの統計情報が表示されます。

詳細検索オプション

次の条件に基づいてクライアントを検索します。

- ・ **基本**：IP アドレス、OS、および MAC アドレスなど、コンピュータの基本的な情報を含みます。

注意： IP セグメントで検索する場合は、先頭オクテットで始まる IP アドレスの一部を指定する必要があります。結果として、指定した値を含む IP アドレスを持つすべてのコンピュータが返されます。たとえば「10.5」と入力すると、10.5.0.0 ～ 10.5.255.255 の IP アドレス範囲内のすべてのコンピュータが返されます。

MAC アドレスで検索する場合は、「000F3E341D51」など 16 進表記の MAC アドレス範囲を指定する必要があります。

- ・ **コンポーネントのバージョン**：コンポーネント名の横にあるチェックボックスをオンにし、[次より古い (指定値を含まない)] または [次と同じか、より古い] を選択してバージョン番号を入力することで条件を絞ります。初期設定では現在のバージョン番号が表示されます。
- ・ **ステータス**：クライアント設定とリアルタイムステータスを含みます。

検索条件を指定してから [検索] をクリックします。条件を満たすコンピュータ名のリストがクライアントツリーに表示されます。

クライアントツリーの特定のタスク

クライアントツリーは、Web コンソールで特定の画面にアクセスすると表示されます。クライアントツリーの上部には、アクセスした画面に固有のメニュー項目が表示されます。これらのメニュー項目を使用して、クライアントの設定やクライアントタスクの起動など、特定のタスクを実行できます。タスクを実行するには、最初にタスクの対象 (すべてのクライアントに設定が適用されるルートアイコン、1 つ以上のドメイン、または 1 つ以上のクライアント) を選択し、次にメニュー項目を選択します。

[ネットワーク上のコンピュータ] → [クライアント管理]

この画面では、一般的なクライアント設定を管理します。

クライアント管理

 表示更新  ヘルプ

クライアントツリー からドメインまたはコンピュータ名を選択し、次に、クライアントツリー 上に表示されるタスクのうち1つを選択してください。

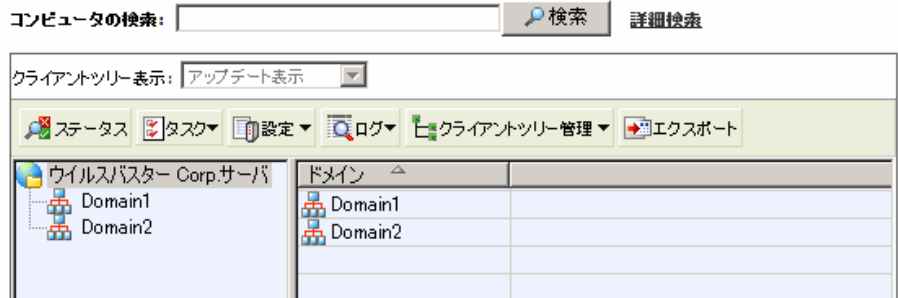


図 2-10. [クライアント管理] 画面

タスク :

表 2-2. クライアント管理タスク

メニューボタン	タスク
ステータス	詳細なクライアント情報を表示します。詳細については、317 ページの「クライアント情報」を参照してください。
タスク	- クライアントコンピュータで手動検索を実行します。詳細については、180 ページの「ScanNow の開始」を参照してください。 - クライアントをアンインストールします。詳細については、110 ページの「Web コンソールからのクライアントのアンインストール」を参照してください。 - スパイウェア / グレーウェアコンポーネントを復元します。詳細については、196 ページの「スパイウェア / グレーウェアの復元」を参照してください。

表 2-2. クライアント管理タスク (続き)

メニューボタン	タスク
設定	• 使用可能な検索方法を選択します。詳細については、165 ページの「検索方法」を参照してください。 • 各検索の種類を設定します。詳細については、次の項目を参照してください。 • 177 ページの「手動検索」 • 176 ページの「リアルタイム検索」 • 178 ページの「予約検索」 • 179 ページの「ScanNow」 • クライアントをアップデートエージェントとして割り当てます。詳細については、154 ページの「アップデートエージェント設定」を参照してください。 • クライアントの権限とその他の設定を行います。詳細については、283 ページの「クライアントの権限とその他の設定」を参照してください。 • Web レピュテーションポリシーを設定します。詳細については、223 ページの「Web レピュテーションポリシー」を参照してください。 • デバイスコントロール設定を行います。詳細については、218 ページの「デバイスコントロール」を参照してください。 • スパイウェア / グレーウェアの承認済みリストを設定します。詳細については、195 ページの「スパイウェア / グレーウェアの承認リスト」を参照してください。 • クライアント設定をインポートおよびエクスポートします。詳細については、318 ページの「クライアント設定のインポートおよびエクスポート」を参照してください。
ログ	次のログを表示します。 • 202 ページの「ウイルス / 不正プログラムログ」 • 208 ページの「スパイウェア / グレーウェアログ」 • 244 ページの「ファイアウォールログ」 • 227 ページの「Web レピュテーションログ」 • 219 ページの「デバイスコントロールログ」 管理ログ。詳細については、267 ページの「ログ管理」を参照してください。
クライアントツリー管理	ウイルスバスター Corp. ドメインを管理します。詳細については、54 ページの「ウイルスバスター Corp. ドメイン」を参照してください。

表 2-2. クライアント管理タスク (続き)

メニューボタン	タスク
エクスポート	クライアントのリストをカンマ区切り形式 (.csv) のファイルにエクスポートします。

[ネットワーク上のコンピュータ] → [大規模感染予防サービス]

タスク：大規模感染予防サービスの設定を指定してアクティベートします。

大規模感染予防

[表示更新](#) [ヘルプ](#)

クライアントツリーからドメインまたはコンピュータ名を選択し、次に、クライアントツリー上に表示されるタスクのうち1つを選択してください。

コンピュータの検索: [詳細検索](#)

クライアントツリー表示:

[大規模感染予防の開始](#) [設定の復元](#)

ウイルスバスター Corp.サーバ	ドメイン	
Domain1	Domain1	
Domain2	Domain2	

図 2-11. [大規模感染予防サービス] 画面

[アップデート]→[ネットワーク上のコンピュータ]→[手動アップデート]→[クライアントを手動で選択する]

タスク：手動アップデートをクライアントで起動します。

ネットワーク上のコンピュータのコンポーネントアップデート

[表示更新](#) [ヘルプ](#)

ウイルスバスター Corp.サーバは、選択されたコンピュータにインストールされたウイルスバスター Corp.クライアントへコンポーネントを更新するよう通知します。続行するには、コンポーネントアップデート開始をクリックしてください。

コンピュータの検索: [検索](#) [詳細検索](#)

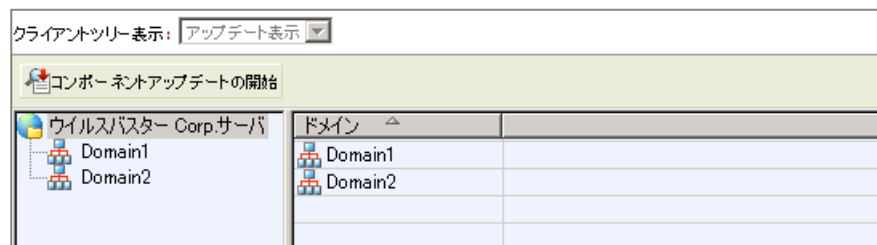


図 2-12. [コンポーネントアップデート] 画面

[アップデート]→[ロールバック]→[サーバとの同期]

タスク：コンポーネントのロールバックを実行します。

ロールバック

[表示更新](#) [ヘルプ](#)

クライアントツリーからドメインまたはコンピュータ選択して、クライアントツリー上のロールバックを選択してください。

コンピュータの検索: [検索](#) [詳細検索](#)



図 2-13. [ロールバック] 画面

【ログ】→【ネットワーク上のコンピュータのログ】→【セキュリティ上の危険】

この画面では、ログの表示および管理を行います。

セキュリティ上の危険ログ

 表示更新  ヘルプ

クライアントツリーからドメインまたはコンピュータ名を選択し、次に、クライアントツリー上に表示されるタスクのうち1つを選択してください。

コンピュータの検索:  検索 [詳細検索](#)

クライアントツリー表示:

 ログの表示▼
  ログの削除

ウイルスバスター Corp.サーバ	ドメイン	
Domain1	Domain1	
Domain2	Domain2	

図 2-14. 【セキュリティ上の危険ログ】画面

タスク：

- 次のログを表示します。
 - 「ウイルス / 不正プログラムログ」
 - 「スパイウェア / グレーウェアログ」
 - 「ファイアウォールログ」
 - 「Web レピュテーションログ」
 - 「デバイスコントロールログ」
- ログ管理を実行します。

[Cisco NAC] → [エージェント配信]

タスク：「Cisco Trust Agent の配信」を実行します。

エージェント配信

[表示更新](#) [ヘルプ](#)

クライアントツリーからドメインまたはコンピュータを選択して、クライアントツリー上の [エージェント配信] をクリックしてください。

コンピュータの検索: [検索](#) [詳細検索](#)

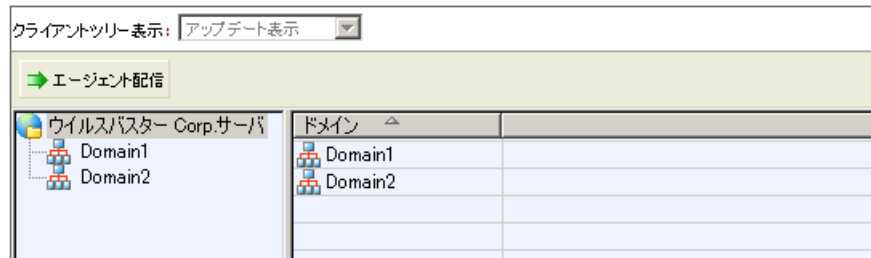


図 2-15. [エージェント配信] 画面

ウイルスバスター Corp. ドメイン

ウイルスバスター Corp. のドメインは、同じ設定を共有し、同じタスクを実行するクライアントのグループです。クライアントをドメインでグループ別にして、同じ設定をすべてのドメインメンバーに対して同時に設定、管理、および適用できます。

管理を簡素化するために、部門または実行する機能に基づいてクライアントをグループ分けします。感染のリスクが高いクライアントにはすべてより安全な設定を適用するために、これらのクライアントもグループ分けします。

初期設定により、ウイルスバスター Corp. では、ネットワークのドメインがシミュレーションされます。クライアントツリーのドメイン名およびクライアント名には、ネットワーク内のドメイン名およびコンピュータ名と同じ名前があります。ウイルスバスター Corp. では、またネットワークのドメイン構成に基づいてクライアントが割り当てられます。ウイルスバスター Corp. が作成したドメインの削除、名前変更、新規ドメインの作成、クライアントのドメイン間の移動を行うことができます。

ドメインを追加するには

パス: [ネットワーク上のコンピュータ] → [クライアント管理] → [クライアントツリー管理] → [ドメインの追加]

1. 追加するドメインの名前を入力します。
2. [追加] をクリックします。新しいドメインがクライアントツリーに表示されます。

ドメインまたはクライアントを削除するには

パス: [ネットワーク上のコンピュータ] → [クライアント管理] → [クライアントツリー管理] → [クライアント / ドメインの削除]

1. ドメインを削除するには、そのドメインに属しているすべてのクライアントを削除または移動します。クライアントを別のドメインに移動するには、それらを目的のドメインにドラッグアンドドロップします。
2. ドメインが空になったら、[クライアント / ドメインの削除] をクリックします。
3. クライアントを削除するには、[クライアント / ドメインの削除] をクリックします。ドメインを選択して [クライアント / ドメインの削除] をクリックすると、そのドメインに属しているすべてのクライアントが削除されます。

注意: 削除されたクライアントはクライアントツリーに表示されなくなりますが、クライアントコンピュータからアンインストールされたわけではありません。ウイルスバスター Corp. クライアントでは、コンポーネントのアップデートなどサーバ依存タスクを引き続き実行できます。ただし、サーバではそのクライアントが認識されなくなるため、設定や通知がクライアントに送信されなくなります。

ドメイン名を変更するには

パス: [ネットワーク上のコンピュータ] → [クライアント管理] → [クライアントツリー管理] → [ドメイン名の変更]

1. このドメインの新しい名前を入力します。
2. [変更] をクリックします。新しいドメイン名がクライアントツリーに表示されます。

クライアントを移動するには

パス: [ネットワーク上のコンピュータ]→[クライアント管理]→[クライアントツリー管理]→[クライアントの移動]

1. クライアントを別のドメインに移動するか、別のウイルスバスター Corp. サーバに移動するかを選択します。
 - a. クライアントを別のドメインに移動するには、[選択したクライアントを別のドメインに移動する]を選択し、ドロップダウンリストからドメインを選択して、新しいドメインの設定を移動クライアントに適用するかどうかを決定します。

ヒント: クライアントツリー内でクライアントをドラッグアンドドロップして別のドメインに移動することもできます。

- b. クライアントを別のウイルスバスター Corp. サーバに移動するには、[選択したクライアントを別のウイルスバスター Corp. サーバに移動する]でサーバ名と HTTP ポート番号を入力します。
2. [移動]をクリックします。

セキュリティコンプライアンス

セキュリティコンプライアンスでは、Microsoft Active Directory サービスを利用して、ネットワーク上のコンピュータのセキュリティステータスが判定されます。Active Directory のクエリを実行した後、コンピュータのセキュリティステータスが Web コンソールに表示されます。セキュリティステータスは、次のいずれかになります。

- このウイルスバスター Corp. サーバの管理下
- 他のウイルスバスター Corp. サーバの管理下
- ウイルスバスター Corp. クライアントが未インストール
- 到達不能

セキュリティコンプライアンスを使用するには、ウイルスバスター Corp. サーバコンピュータが Active Directory ドメインのメンバーであることを確認します。

セキュリティコンプライアンスを適用するには、次のタスクを実行します。

1. 「Active Directory の範囲とクエリ」を定義します。
2. 「Active Directory クエリの結果」から保護されていないコンピュータを確認します。
3. 「ウイルスバスター Corp. クライアントのインストール」を実行します。

4. 「予約クエリ」を設定します。

Active Directory の範囲とクエリ

セキュリティコンプライアンスを初めて使用する場合は、Active Directory の範囲を定義します。この範囲には、ウイルスバスター Corp. サーバで必要に応じてまたは定期的にクエリを実行する Active Directory オブジェクトが含まれます。対象範囲を定義したら、クエリ処理を開始します。

Active Directory の範囲を定義してクエリ処理を開始するには

パス：[セキュリティコンプライアンス]

1. [Active Directory の範囲] セクションで [定義] をクリックします。
2. 開いた画面に Active Directory 構造が表示されます。クエリを実行するオブジェクトを選択します。

ヒント： 初めてクエリを実行する場合は、1,000 アカウント未満のオブジェクトを選択して、クエリの完了にかかった時間を記録してください。このデータをパフォーマンスベンチマークとして使用します。

3. [詳細設定] で、ウイルスバスター Corp. サーバでクライアントとの通信に使用するポートを指定します。ウイルスバスター Corp. サーバのインストール時、ポート番号はセットアップによってランダムに生成されます。

ヒント： ウイルスバスター Corp. サーバで使用される通信ポートを確認するには、[ネットワーク上のコンピュータ] → [クライアント管理] に移動してドメインを選択します。[IP アドレス] 列を確認します。ポート番号は IP アドレスの後ろに表示されています。参照用にポート番号を記録しておいてください。

- a. [ポートの指定] をクリックします。
 - b. ポート番号を入力して [追加] をクリックします。目的のポート番号がすべて追加されるまで、このステップを繰り返します。
 - c. [保存] をクリックします。
4. 特定のポート番号を使用してコンピュータの接続を確認するかどうかを選択します。接続を確立できない場合、ウイルスバスター Corp. はそのコンピュータを到達不能としてただちに処理します。初期設定のポート番号は 135 です。

ヒント： この設定を有効にすることで、Active Directory クエリを迅速に行えるようになります。これは、あるコンピュータとの接続を確立できない場合に、他のすべての接続状態の確認タスクを実行した上でコンピュータを到達不能として処理する必要がなくなるためです。

- Active Directory の範囲を保存してクエリを開始するには、[保存して再診断] をクリックします。設定の保存のみを実行するには、[保存のみ] をクリックします。

[セキュリティコンプライアンス] 画面にクエリの結果が表示されます。

注意： 特にクエリ範囲が広い場合、クエリの完了に時間がかかる場合があります。[セキュリティコンプライアンス] 画面に結果が表示されるまで、別のクエリは実行しないでください。結果が表示される前に別のクエリを実行すると、現在のクエリセッションが終了し、クエリ処理が再度開始されます。

Active Directory クエリの結果

[セキュリティステータス] セクションでは、コンピュータが次のように分類されます。

表 2-3. コンピュータ保護ステータス

ステータス	説明
このウイルスバスター Corp. サーバの管理下	コンピュータにインストールされているウイルスバスター Corp. クライアントは、このウイルスバスター Corp. サーバによって管理されています。クライアントはオンライン、オフライン、またはスタンドアロンモードで、このウイルスバスター Corp. のバージョンかそれ以前のバージョンを実行しています。
他のウイルスバスター Corp. サーバの管理下	コンピュータにインストールされているウイルスバスター Corp. クライアントは、他のウイルスバスター Corp. サーバによって管理されています。クライアントはオンラインで、このウイルスバスター Corp. のバージョンかそれ以前のバージョンを実行しています。
ウイルスバスター Corp. クライアントが未インストール	コンピュータにはウイルスバスター Corp. クライアントがインストールされていません。

表 2-3. コンピュータ保護ステータス (続き)

ステータス	説明
到達不能	ウイルスバスター Corp. サーバからコンピュータに接続できません。そのため、コンピュータにクライアントがインストールされているかどうか、インストールされている場合はクライアントが他のウイルスバスター Corp. サーバによって管理されているか、または管理されていないかどうかを判定できません。 注意： ウイルスバスター Corp. サーバのデータベースには、そのサーバで管理しているクライアントのリストがあります。クライアントコンピュータに到達できないが、そのコンピュータにインストールされているクライアントをウイルスバスター Corp. サーバで管理していることが検出された場合、そのコンピュータのステータスは「このウイルスバスター Corp. サーバの管理下」になります。

推奨されるタスク：

1. [セキュリティステータス] セクションで、数字のリンクをクリックし、クライアントツリーで影響を受けるすべてのコンピュータを表示します。
2. 検索および詳細検索機能を使用して、条件に一致するコンピュータのみを検索して表示します。

詳細検索機能を使用する場合は、次の項目に完全な名前を指定します。

- コンピュータ名
- ウイルスバスター Corp. サーバ
- ウイルスバスター Corp. ドメイン
- Active Directory ツリー

完全な名前が不明な場合は、ワイルドカード文字 (*) を使用してください。

名前が完全でなくワイルドカード文字も指定されていない場合は、結果が返されません。

3. コンピュータのリストをファイルに保存するには、[エクスポート] をクリックします。
4. 他のウイルスバスター Corp. サーバによって管理されているクライアントを、現在のウイルスバスター Corp. サーバで管理するには、クライアント移動ツールを使用します。

ウイルスバスター Corp. クライアントのインストール

クライアントをインストールする前に、次の点に注意してください。

1. 各コンピュータのログオン情報を記録しておきます。インストール時、ウイルスバスター Corp. によってこのログオン情報を指定するよう求められます。
2. 次の場合、コンピュータにウイルスバスター Corp. クライアントはインストールされません。
 - コンピュータにウイルスバスター Corp. サーバがインストールされている。
 - コンピュータで、Windows XP Home、Windows Vista Home Basic、および Windows Vista Home Premium が実行されている。これらのプラットフォームを実行しているコンピュータでは、別のインストール方法を選択します。詳細については、72 ページの「インストール方法」を参照してください。
3. 対象コンピュータで Windows Vista Business、Enterprise、または Ultimate Edition が実行されている場合は、そのコンピュータで次の手順を実行します。
 - a. ビルトインの管理者アカウントを有効にして、そのアカウントのパスワードを設定します。
 - b. Windows のファイアウォールを無効にします。
 - c. [スタート] → [プログラム] → [管理ツール] → [セキュリティが強化された Windows ファイアウォール] をクリックします。
 - d. 「ドメイン プロファイル」、「プライベート プロファイル」、および「パブリック プロファイル」で、ファイアウォールの状態をオフにします。
 - e. Microsoft 管理コンソール ([スタート] → [ファイル名を指定して実行] をクリックして「services.msc」と入力) を開いて、リモートレジストリサービスを起動します。ウイルスバスター Corp. クライアントのインストールには、ビルトインの管理者アカウントとパスワードを使用します。
4. トレンドマイクロまたはサードパーティのエンドポイントセキュリティプログラムがコンピュータにインストールされている場合は、ウイルスバスター Corp. でそのソフトウェアを自動的にアンインストールしてからウイルスバスター Corp. クライアントに置き換えることが可能であるかどうかを確認します。ウイルスバスター Corp. で自動的にアンインストールされるエンドポイントセキュリティソフトウェアのリストについては、<「サーバのインストールフォルダ」>%PCCSRV%\Admin にある次のファイルを開いて確認してください。これらのファイルはメモ帳などのテキストエディタで開くことができます。
 - tmuninst.ptn
 - tmuninst_as.ptn

対象コンピュータのソフトウェアがリストに含まれていない場合は、そのソフトウェアを最初に手動でアンインストールします。ソフトウェアのアンインストール処理によっては、アンインストールの終了後、コンピュータの再起動が必要になる場合があります。

ウイルスバスター Corp. クライアントをインストールするには

パス: [セキュリティコンプライアンス]

1. クライアントツリーの上で、[インストール] をクリックします。

ウイルスバスター Corp. クライアントの前のバージョンがコンピュータにすでにインストールされている場合、[インストール] をクリックしても、インストールはスキップされ、クライアントがこのバージョンにアップグレードされません。クライアントをアップグレードするには、292 ページの「アップデート設定」を参照してください。

2. コンピュータごとに管理者のログオンアカウントを指定して、[ログオン] をクリックします。対象コンピュータへのクライアントのインストールが開始されます。
3. インストールステータスを表示します。

予約クエリ

ウイルスバスター Corp. では、Active Directory のクエリをスケジュールに基づいて自動的に実行できます。

クエリのスケジュールを設定するには

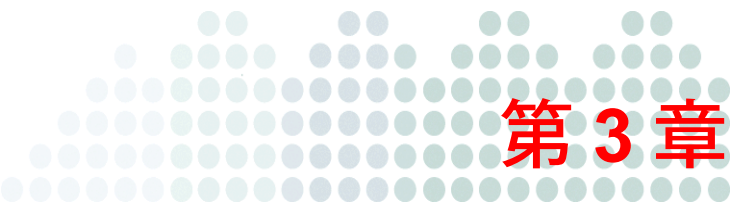
パス: [セキュリティコンプライアンス]

1. [セキュリティコンプライアンス] クライアントツリーの上で、[設定] をクリックします。
2. 予約クエリを有効にします。
3. スケジュールを指定します。すべての月に 31 日を指定した場合、最終日が 31 日でない月では末日に診断が実施されます。
4. スケジュールを保存するには、[保存のみ] をクリックします。スケジュールを保存せずにクエリを実行するには、[すぐにクエリ] をクリックします。

第 1 部

ネットワーク上のコンピュータの 保護





第3章

ウイルスバスター Corp. クライアントのインストール

この章で説明する内容には、次の項目が含まれます。

- 66 ページの「インストール要件」
- 72 ページの「インストール方法」
- 104 ページの「ウイルスバスター Corp. クライアントへの移行」
- 108 ページの「ポストインストール」
- 110 ページの「クライアントのアンインストール」

注意： システム要件に記載されているオペレーティングシステムの種類やハードディスク容量などは、本ドキュメント作成時点の情報です。システム要件は、OS のサポート終了や、弊社製品の改良、検索エンジンやパターンファイルのバージョンアップなどに伴い、変更、追加、または削除される場合があります。

また、製品の運用環境によっては、ログファイルの保存、他のソフトウェアとの共存などにより、必要となるメモリサイズやハードディスク容量も異なりますので、ご注意ください。最新のシステム要件については、弊社 Web サイトやサポート窓口にご確認ください。

インストール要件

ウイルスバスター コーポレートエディション (以下、ウイルスバスター Corp.) クライアントは、以下のプラットフォームを実行しているコンピュータにインストールできます。

- ・ 「Windows 2000」
- ・ 「Windows XP/2003 (32 ビットバージョン)」
- ・ 「Windows XP/2003 (64 ビットバージョン)」
- ・ 「Windows Vista (32 ビットおよび 64 ビットバージョン)」
- ・ 「Windows 2008 (32 ビットバージョン)」
- ・ 「Windows 2008 (64 ビットバージョン)」

表 3-1. Windows 2000

リソース	要件
OS	・ Windows 2000 Service Pack 4 ・ Windows 2000 Professional Service Pack 4 ・ Windows 2000 Server Service Pack 4 ・ Windows 2000 Advanced Server Service Pack 4 ・ ウイルスバスター Corp. クライアントは、次の仮想アプリケーションでホストされる Windows 2000 のゲスト OS にインストールできます。 ・ Microsoft Virtual Server 2005 R2 Service Pack 1 ・ VMware ESX/ESXi Server 3.5 (サーバエディション) ・ VMware Server 1.0.3 以降 (サーバエディション) ・ VMware Workstation および Workstation ACE Edition 6.0
ハードウェア	プロセッサ 300MHz Intel Pentium または同等の CPU RAM 256MB 以上 (512MB を推奨) ハードディスク空き容量 350MB 以上 その他 解像度 800x600、256 色以上をサポートするモニタ

表 3-2. Windows XP/2003 (32 ビットバージョン)

リソース	要件
OS	- Windows XP Professional Service Pack 2/3 - Windows XP Home Service Pack 3 - Windows Server 2003 (Standard、Enterprise、Datacenter、および Web Edition) Service Pack 2 - Windows Server 2003 R2 (Standard、Enterprise、および Datacenter Edition) Service Pack 2 - Windows Storage Server 2003 - ウイルスバスター Corp. クライアントは、次の仮想アプリケーションでホストされる Windows XP/2003 のゲスト OS にインストールできます。 - Microsoft Virtual Server 2005 R2 (Service Pack 1) - VMware ESX/ESXi Server 3.5 (サーバエディション) - VMware Server 1.0.3 以降 (サーバエディション) - VMware Workstation および Workstation ACE Edition 6.0
ハードウェア	プロセッサ 300MHz Intel Pentium または同等の CPU AMD 64 または Intel 64 アーキテクチャ RAM 256MB 以上 (512MB を推奨) ハードディスク空き容量 350MB 以上 その他 解像度 800x600、256 色をサポートするモニタ
その他	- Microsoft Internet Explorer 6.0 以上 (Web セットアップを実行する場合) - ユーザがウイルスバスター Corp. クライアントプログラムを正常にインストールするには、Windows XP コンピュータで簡易ファイルの共有を無効にします (手順については、Windows のマニュアルを参照してください)。

表 3-3. Windows XP/2003 (64 ビットバージョン)

リソース	要件
OS	• Windows XP Professional Service Pack 2/3 • Windows Server 2003 (Standard、Enterprise、Datacenter、および Web Edition) Service Pack 2 • Windows Server 2003 R2 (Standard、Enterprise、および Datacenter Edition) Service Pack 2 • Windows Storage Server 2003 • ウイルスバスター Corp. クライアントは、次の仮想アプリケーションでホストされる Windows XP/2003 のゲスト OS にインストールできます。 • VMware ESX/ESXi Server 3.5 (サーバエディション) • VMware Server 1.0.3 以降 (サーバエディション) • VMware Workstation および Workstation ACE Edition 6.0
ハードウェア	プロセッサ • Intel x64 • AMD64 RAM 256MB 以上 (512MB を推奨) ハードディスク空き容量 350MB 以上 その他 解像度 800x600、256 色をサポートするモニタ
その他	• Microsoft Internet Explorer 6.0 以上 (Web セットアップを実行する場合) • ユーザがウイルスバスター Corp. クライアントプログラムを正常にインストールするには、Windows XP コンピュータで簡易ファイルの共有を無効にします (手順については、Windows のマニュアルを参照してください)。

表 3-4. Windows Vista (32 ビットおよび 64 ビットバージョン)

リソース	要件
OS	- Windows Vista Business Edition Service Pack 1 - Windows Vista Enterprise Edition Service Pack 1 - Windows Vista Ultimate Edition Service Pack 1 - Windows Vista Home Premium Edition Service Pack 1 - Windows Vista Home Basic Edition Service Pack 1 - ウイルスバスター Corp. クライアントは、次の仮想アプリケーションでホストされる Windows Vista のゲスト OS にインストールできます。 - VMware ESX/ESXi Server 3.5 (サーバエディション) - VMware Server 1.0.3 以降 (サーバエディション) - VMware Workstation および Workstation ACE Edition 6.0
ハードウェア	プロセッサ 800MHz Intel Pentium または同等の CPU - AMD64 または Intel 64 アーキテクチャ RAM 1GB 以上 (1.5GB を推奨) ハードディスク空き容量 350MB 以上 その他 解像度 800x600、256 色をサポートするモニタ
その他	Windows Internet Explorer 7.0 以上 (Web セットアップを実行する場合)

表 3-5. Windows 2008 (32 ビットバージョン)

リソース	要件
OS	- Windows Server 2008 (Standard、Enterprise、Datacenter、および Web Edition) Service Pack 1 - ウイルスバスター Corp. クライアントは、次の仮想アプリケーションでホストされる Windows 2008 のゲスト OS にインストールできます。 - VMware ESX/ESXi Server 3.5 (サーバエディション) - VMware Server 1.0.3 以降 (サーバエディション) - VMware Workstation および Workstation ACE Edition 6.0 ※ Windows 2008 が、Server Core 環境で実行されている場合はウイルスバスター Corp. をインストールできません。
ハードウェア	プロセッサ 1GHz Intel Pentium 以上の CPU (2GHz を推奨) - AMD64 および Intel 64 アーキテクチャ RAM 最低 512MB、2GB を推奨 ハードディスク空き容量 350MB 以上 その他 解像度 800x600、256 色をサポートするモニタ
その他	Windows Internet Explorer 7.0 以上 (Web セットアップを実行する場合)

表 3-6. Windows 2008 (64 ビットバージョン)

リソース	要件
OS	- Windows Server 2008 (Standard、Enterprise、Datacenter、および Web Edition) Service Pack 1 - ウイルスバスター Corp. クライアントは、次の仮想アプリケーションでホストされる Windows 2008 のゲスト OS にインストールできます。 - VMware ESX/ESXi Server 3.5 (サーバエディション) - VMware Server 1.0.3 以降 (サーバエディション) - VMware Workstation および Workstation ACE Edition 6.0 ※ Windows 2008 が、Server Core 環境で実行されている場合はウイルスバスター Corp. をインストールできません。
ハードウェア	プロセッサ 1.4GHz Intel Pentium 以上の CPU (2GHz を推奨) - AMD64 および Intel 64 アーキテクチャ RAM 最低 512MB、2GB を推奨) ハードディスク空き容量 350MB 以上 その他 解像度 800x600、256 色をサポートするモニタ
その他	Windows Internet Explorer 7.0 以上 (Web セットアップを実行する場合)

互換性リスト

ウイルスバスター Corp. は、次の製品に対応しています。

- Citrix XenApp Server 4.5 および 5.0 (32 ビットおよび 64 ビット)
- Microsoft ActiveSync 4.2、4.5
- Microsoft Cluster Server 2000
- Microsoft Cluster Server 2003
- Microsoft Office 2000、XP、2003
- Microsoft SQL Server 7.0、2000、2008
- Microsoft Systems Management Server (SMS) 2003 (Service Pack 2 以上)
- Nortel VPN Client (制限あり)

- Outlook メール検索では Microsoft Office Outlook 2000、2002、2003、2007 をサポート
- POP3 メール検索では次のメールプログラムをサポート
 - Becky! Internet Mail 2.0
 - Eudora 6.2
 - Microsoft Outlook Express 6.0
 - Microsoft Office Outlook 2000、2002、2003、2007
 - Mozilla Thunderbird 1.5、2.0
 - Netscape 7.2
 - Windows Mail (Windows Vista のみ)
 - Foxmail 5.0、6.0
- Windows 2000、2003、および 2008 でのターミナルサービス
- Windows Mobile Device Center 6 (32 ビット)
- Windows Mobile Device Center 6.1 (32 ビットおよび 64 ビット)
- Windows Server 2008 のフェイルオーバークラスタ
- Windows XP Tablet PC Edition (Service Pack 2)

インストール方法

このセクションでは、ウイルスバスター Corp. クライアントの新規インストールを実行するさまざまな方法について概要を説明します。すべてのインストール方法で、対象コンピュータのローカル管理者権限が必要になります。

表 3-7. インストール方法

インストール方法 / OS サポート	配信時の考慮事項					
	WAN 配信	集中 管理	ユーザ 操作が必要	IT リソース が必要	大量 配信	帯域幅の 消費
Web インストールページ すべての OS でサポート	不可	不可	はい	いいえ	不可	多い

表 3-7. インストール方法 (続き)

インストール方法 / OS サポート	配信時の考慮事項					
	WAN 配信	集中 管理	ユーザ 操作が必要	IT リソース が必要	大量 配信	帯域幅の 消費
ログオンスクリプトウィ ザード すべての OS でサポート	不可	不可	はい	はい	不可	多い (複数の インストール が同時に開始 される場合)
Client Packager すべての OS でサポート	不可	不可	はい	はい	不可	少ない (予約 されている場 合)
Client Packager (Microsoft SMS を使用して配信され る MSI パッケージ) すべての OS でサポート	可	可	はい / いい え	はい	可	少ない (予約 されている場 合)
Client Packager (Active Directory を使用して配信 される MSI パッケージ) すべての OS でサポート	可	可	はい / いい え	はい	可	多い (複数の インストール が同時に開始 される場合)
ウイルスバスター Corp. Web コンソールから 次を除くすべての OS でサ ポート : - Windows Vista Home Basic および Home Premium Edition - Windows XP Home Edition	不可	可	いいえ	はい	不可	多い

表 3-7. インストール方法 (続き)

インストール方法 / OS サポート	配信時の考慮事項					
	WAN 配信	集中 管理	ユーザ 操作が必要	IT リソース が必要	大量 配信	帯域幅の 消費
クライアントのディスクイメージ 次を除くすべての OS でサポート : • Windows Vista • Windows 2008 • 64 ビットプラットフォーム	不可	不可	いいえ	はい	不可	少ない
トレンドマイクロ脆弱性検索ツール (TMVS) 次を除くすべての OS でサポート : • Windows Vista Home Basic および Home Premium Edition • Windows XP Home Edition	不可	可	いいえ	はい	不可	多い

Web インストールページからのインストール

次のプラットフォームを実行しているコンピュータにウイルスバスター Corp. サーバをインストールした場合、ユーザは Web インストールページからクライアントプログラムをインストールできます。

- Windows 2000 Server
- Internet Information Server (IIS) 6.0 または Apache 2.0.x を搭載した Windows Server 2003

Web インストールページからインストールするには、次のアイテムが必要です。

- ActiveX コントロールを許可するようにセキュリティレベルが設定されている Internet Explorer。必要なバージョンは次のとおりです。
 - 5.0 (Windows 2000 の場合)

- 6.0 (Windows XP/Server 2003 の場合)
- 7.0 (Windows Vista/2008 の場合)
- 対象コンピュータの管理者権限

ウイルスバスター Corp. クライアントを Web インストールページからインストールするには、次の手順をユーザに通知してください。メールを使用してクライアントインストール通知を送信するには、76 ページの「ブラウザベースのインストールの開始」を参照してください。

Web インストールページからインストールするには

1. ビルトインの管理者アカウントを使用して、コンピュータにログオンします。
2. Windows XP、Vista、および 2008 を実行しているコンピュータにインストールする場合は、次の手順を実行します。
 - a. Internet Explorer を起動して、信頼済みサイトの一覧にウイルスバスター Corp. サーバの URL (<https://<ウイルスバスター Corp. サーバ名>:4343/officescan> など) を追加します。Windows XP Home では、[ツール] → [インターネット オプション] → [セキュリティ] タブに移動して [信頼済みサイト] アイコンを選択し、[サイト] をクリックして一覧にアクセスします。
 - b. Internet Explorer のセキュリティ設定を変更して、[ActiveX コントロールに対して自動的にダイアログを表示] を有効にします。Windows XP では、[ツール] → [インターネット オプション] → [セキュリティ] タブに移動して、[カスタム レベル] をクリックします。
3. Internet Explorer ウィンドウを開いて、次のいずれかを入力します。
 - SSL が有効なウイルスバスター Corp. サーバ：
<https://<ウイルスバスター Corp. サーバ名>:<ポート>/officescan>
 - SSL が無効なウイルスバスター Corp. サーバ：
<http://<ウイルスバスター Corp. サーバ名>:<ポート>/officescan>
4. ログオンページのリンクをクリックします。
5. 新しいページが表示されたら、[インストール] をクリックしてウイルスバスター Corp. クライアントのインストールを開始します。クライアントのインストールが開始されます。ダイアログが表示されたら、ActiveX コントロールのインストールを許可します。インストール後、Windows のタスクトレイにウイルスバスター Corp. クライアントのアイコンが表示されます。

注意： タスクトレイに表示されるアイコンの一覧については、307 ページの「サーバとのクライアント接続」を参照してください。

ブラウザベースのインストールの開始

ウイルスバスター Corp. クライアントをインストールするようネットワーク上のユーザに指示するメールメッセージを設定します。ユーザは、このメールに記載されているクライアントインストールのリンクをクリックしてインストールを開始します。

クライアントをインストールする前に、次の処理を実行します。

- クライアントのインストール要件を確認します。
- セキュリティ上の脅威から現在保護されていないネットワーク上のコンピュータを識別します。次のタスクを実行します。
 - トレンドマイクロ脆弱性検索ツールを実行します。このツールは、指定された IP アドレス範囲に基づき、インストールされているウイルス対策ソフトウェアについてコンピュータを分析します。詳細については、91 ページの「脆弱性検索ツールの使用」を参照してください。
 - Active Directory のクエリを実行します。詳細については、56 ページの「セキュリティコンプライアンス」を参照してください。

ブラウザベースのインストールを開始するには

パス: [ネットワーク上のコンピュータ] → [クライアントのインストール] → [ブラウザベース]

1. 必要に応じてメールメッセージの件名を修正します。
2. [メールの作成] をクリックします。初期設定のメールプログラムが起動します。
3. 目的の受信者にメールを送信します。

ログオンスクリプトウィザードを使用したインストール

ログオンスクリプトウィザードでは、保護されていないコンピュータがネットワークにログオンする際にウイルスバスター Corp. クライアントを自動インストールします。ログオンスクリプトウィザードでは、AutoPcc.exe と呼ばれるプログラムをサーバログインスクリプトに追加します。

AutoPcc.exe は、保護されていないコンピュータにクライアントをインストールし、プログラムファイルとコンポーネントをアップデートします。ログオンスクリプトを使用して AutoPcc を実行するには、コンピュータが対象ドメインのメンバーである必要があります。

クライアントインストール

AutoPcc.exe は、保護されていない Windows 2000/Server 2003 コンピュータが、ログオンスクリプトが変更されたサーバにログオンするときに、このコンピュータにウイルスバスター Corp. クライアントを自動的にインストールします。ただし、Windows XP/Vista/2008 コンピュータには自動

的にインストールしません。ユーザがサーバコンピュータに接続し、¥¥<サーバコンピュータ名>¥ofcscan に移動して AutoPcc.exe を右クリックし、[管理者として実行] を選択する必要があります。

AutoPcc.exe を使用したリモートデスクトップインストールの場合

- コンピュータを Mstsc.exe /console モードで実行する必要があります。これにより、AutoPcc.exe のインストールがセッション 0 で実行されるようになります。
- 「ofcscan」フォルダにドライブをマップし、そこから AutoPcc.exe を実行します。

プログラムとコンポーネントのアップデート

AutoPcc.exe は、プログラムファイルとウイルス対策コンポーネント、スパイウェア対策コンポーネント、およびダメージクリーンナップサービスコンポーネントをアップデートします。

Windows 2000/Server 2003/2008 スクリプト

すでに既存のログオンスクリプトがある場合は、ログオンスクリプトウィザードによって、AutoPcc.exe を実行するコマンドがスクリプトに追加されます。既存のログオンスクリプトがない場合は、AutoPcc.exe を実行するコマンドを含む ofcscan.bat と呼ばれるバッチファイルが作成されます。

ログオンスクリプトウィザードによって、スクリプトの末尾に次のコマンドが追加されます。

¥¥<サーバ名>¥ofcscan¥autopcc

説明:

- <サーバ名> は、ウイルスバスター Corp. サーバコンピュータのコンピュータ名または IP アドレスです。
- 「ofcscan」は、サーバ上のウイルスバスター Corp. ディレクトリです。
- 「autopcc」は、ウイルスバスター Corp. クライアントをインストールする autopcc 実行可能ファイルへのリンクです。

ログオンスクリプトの場所 (ネットログオン共有ディレクトリ経由):

- Windows 2000 サーバ: ¥¥Windows 2000 server¥system drive¥WINNT¥SYSVOL¥domain¥scripts¥ofcscan.bat
- Windows Server 2003: ¥¥Windows 2003 server¥system drive¥windir¥sysvol¥domain¥scripts¥ofcscan.bat
- Windows Server 2008: ¥¥Windows 2008 server¥system drive¥windir¥sysvol¥domain¥scripts¥ofcscan.bat

ログオンスクリプトウィザードを使用してログオンスクリプトに **AutoPcc.exe を追加するには**

1. サーバインストールの実行に使用したコンピュータで、Windows の [スタート] メニューから [プログラム] → [ウイルスバスター Corp. サーバ <サーバ名>] → [システムログオンスクリプト] の順に選択します。
ログオンスクリプトウィザードユーティリティがロードされます。コンソールに、ネットワーク上のすべてのドメインを示すツリーが表示されます。
2. ログオンスクリプトを変更するサーバを検索して選択し、[選択] をクリックします。選択したサーバがプライマリドメインコントローラであり、そのサーバに対して管理者権限を持っていることを確認します。ダイアログが表示され、ユーザ名とパスワードを入力するよう求められます。
3. ユーザ名とパスワードを入力します。[OK] をクリックして操作を続行します。
[ユーザの選択] 画面が表示されます。[ユーザ] リストには、サーバにログオンするユーザのプロファイルが表示されます。[選択したユーザ] リストには、ログオンスクリプトを変更するユーザのプロファイルが表示されます。
4. 1 つのユーザプロファイルのログオンスクリプトを変更するには、[ユーザ] リストからそのユーザプロファイルを選択して、[追加] をクリックします。
5. すべてのユーザのログオンスクリプトを変更するには、[すべて追加] をクリックします。
6. 前に選択したユーザプロファイルを除外するには、[選択したユーザ] リストで名前を選択して、[削除] をクリックします。
7. 選択内容をリセットするには、[すべて削除] をクリックします。
8. 対象ユーザのプロファイルがすべて [選択したユーザ] リストにある場合は、[適用] をクリックします。
サーバのログオンスクリプトが正常に変更されたことを示すメッセージが表示されます。
9. [OK] をクリックします。ログオンスクリプトウィザードがその初期画面に戻ります。
10. 他のサーバのログオンスクリプトを変更するには、ステップ 2 ~ 4 を繰り返します。
11. ログオンスクリプトウィザードを閉じるには、[終了] をクリックします。

Client Packager を使用したインストール

Client Packager は、セットアップファイルやアップデートファイルを自己解凍型ファイルに圧縮し、この圧縮ファイルを CD-ROM などの従来のメディアを使用してユーザに配布することができます。このパッケージを受け取ったユーザは、セットアッププログラムをクライアントコンピュータで実行するだけクライアントをインストールできます。

Client Packager は、クライアントプログラムやコンポーネントを、帯域幅が十分でない遠隔地のオフィスに配布する場合に特に便利です。Client Packager を使用してインストールしたウイルスバスター Corp. クライアントは、そのセットアップパッケージが作成されたサーバにレポートします。

Client Packager には次のアイテムが必要です。

- 350MB のハードディスク空き容量
- Windows Installer 2.0 (MSI パッケージを実行)

Client Packager を使用してパッケージを作成するには

1. ウイルスバスター Corp. サーバコンピュータで、<サーバのインストールフォルダ>%PCCSRV¥Admin¥Utility¥ClientPackager に移動します。
2. ClnPack.exe をダブルクリックして、ツールを実行します。Client Packager コンソールが開きます。
3. 作成するパッケージの種類を選択します。

表 3-8. クライアントパッケージの種類

パッケージの種類	説明
Setup	パッケージを実行可能ファイルとして作成する場合に選択します。このパッケージでは、現在サーバで使用可能なコンポーネントとともに、ウイルスバスター Corp. クライアントプログラムがインストールされます。対象コンピュータにウイルスバスター Corp. クライアントの前のバージョンがインストールされている場合は、この実行可能ファイルを実行することでクライアントがアップグレードされます。
Update	現在サーバで使用可能なコンポーネントを含むパッケージを作成する場合に選択します。パッケージは実行可能ファイルとして作成されます。クライアントコンピュータでコンポーネントをアップデートする際に問題が発生する場合には、このパッケージを使用します。

表 3-8. クライアントパッケージの種類 (続き)

パッケージの種類	説明
MSI	Microsoft Installer Package 形式に準拠するパッケージを作成する場合に選択します。このパッケージでも、現在サーバで使用可能なコンポーネントとともに、ウイルスバスター Corp. クライアントプログラムがインストールされます。対象コンピュータにウイルスバスター Corp. クライアントの前のバージョンがインストールされている場合は、この MSI ファイルを実行することでクライアントがアップグレードされます。

4. 次の設定を行います (パッケージの種類によっては使用できない設定があります) :
 - ・ 「Windows Operating System Type」
 - ・ 「Scan Method」
 - ・ 「Silent Mode」
 - ・ 「Update Agent」
 - ・ 「Force Overwrite with Latest Version」
 - ・ 「Disable Prescan (Only for Fresh Installation)」
 - ・ 「Outlook Mail Scan」
 - ・ 「Check Point SecureClient Support」
 - ・ 「Components」
5. [Source file] で、ofcscan.ini ファイルの場所が正しいことを確認します。パスを変更するには、をクリックして ofcscan.ini ファイルを参照します。初期設定では、このファイルはウイルスバスター Corp. サーバの<「サーバのインストールフォルダ」>\PCCSRV フォルダにあります。
6. [Output file] で をクリックして、クライアントパッケージを作成する場所と、ファイル名 (例 : ClientSetup.exe) を指定します。
7. [Create] をクリックします。Client Packager でパッケージの作成が終了すると、「Package created successfully!」という内容のメッセージが表示されます。パッケージが正常に作成されたことを確認するには、指定した出力ディレクトリをチェックしてください。
8. パッケージを配信します。

パッケージ配信のガイドライン

1. パッケージをユーザに配信し、.exe または .msi ファイルをダブルクリックして、コンピュータ上でクライアントパッケージを実行するよう指示します。

警告： パッケージを作成したサーバにレポートするウイルスバスター Corp. クライアントのユーザにのみ、パッケージを送信してください。

2. Windows Vista および 2008 を実行するコンピュータに .exe パッケージをインストールするユーザには、.exe ファイルを右クリックして [管理者として実行] を選択するように指示します。
3. .msi ファイルを作成した場合は、次のタスクを実行してパッケージを配信します。
 - Active Directory または Microsoft SMS を使用します。84 ページの「Active Directory を使用した MSI パッケージの配信」または 85 ページの「Microsoft SMS を使用した MSI パッケージの配信」を参照してください。
 - コマンドプロンプトで MSI パッケージを起動して、Windows XP、Vista、および 2008 を実行するリモートコンピュータに、ウイルスバスター Corp. クライアントをサイレントインストールします。

Client Packager の設定

Windows Operating System Type

パッケージを作成する OS を選択します。作成したパッケージは、ここで選択した OS を実行するコンピュータにのみ配信してください。別の種類の OS を対象に配信するには、別のパッケージを作成します。

Scan Method

パッケージの検索方法を選択します。詳細については、165 ページの「検索方法」を参照してください。

選択した検索方法によって、パッケージに含まれるコンポーネントは異なります。詳細については、139 ページの「クライアントアップデート」を参照してください。

検索方法を選択する前に、パッケージの効率的な配信に役立つ次のガイドラインに注目してください。

- パッケージを使用して、クライアントをこのウイルスバスター Corp. のバージョンにアップグレードする場合は、Web コンソールでドメインレベルの検索方法を確認してください。コンソールで [ネットワーク上のコンピュータ] → [クライアント管理] に移動して、クライアントが属するクライアントツリードメインを選択し、[設定] → [検索方法] の順にクリックします。ドメインレベルの検索方法とパッケージの検索方法は、一致している必要があります。
- パッケージを使用して、ウイルスバスター Corp. クライアントの新規インストールを実行する場合は、クライアントのグループ設定を確認してください。Web コンソールで、[ネットワーク上のコンピュータ] → [グローバルクライアント設定] に移動します。対象コンピュータが属する NetBIOS/Active Directory/DNS ドメインが、クライアントツリーに存在することを確認します。存在する場合は、そのドメインに設定されている検索方法を確認します。ドメインが存在しない場合は、クライアントツリーでルートアイコン  を選択して [設定] → [検索方法] の順にクリックし、ルートレベルの検索方法を確認します。ドメインまたはルートレベルの検索方法とパッケージの検索方法は、一致している必要があります。
- パッケージを使用して、クライアントのコンポーネントをこのウイルスバスター Corp. のバージョンでアップデートする場合は、クライアントが属するクライアントツリードメインに設定されている検索方法を確認してください。ドメインレベルの検索方法とパッケージの検索方法は、一致している必要があります。

Silent Mode

このオプションでは、クライアントコンピュータにバックグラウンドでインストールするパッケージが作成されます。このとき、クライアントに通知されることはなく、インストールステータスウィンドウも表示されません。パッケージをリモートで対象コンピュータに配布する場合は、このオプションを有効にします。

Update Agent

このオプションでは、アップデートエージェントの権限が対象コンピュータのクライアントに割り当てられます。アップデートエージェントは、ウイルスバスター Corp. サーバでクライアントにコンポーネントを配信するのに役立ちます。詳細については、153 ページの「アップデートエージェント」を参照してください。

[アップデートエージェント] オプションを有効にする場合

1. 予約アップデート設定ツールを使用して、エージェントの予約アップデートを有効にし、設定します。詳細については、157 ページの「アップデートエージェントのアップデート方法」を参照してください。
2. アップデートエージェントを管理するウイルスバスター Corp. サーバでは、エージェントに対して次の設定を同期したり、配信することができません。

- アップデートエージェント権限
- クライアントの予約アップデート
- トレンドマイクロのアップデートサーバからのアップデート
- 他のアップデート元からのアップデート

そのため、クライアントパッケージは、ウイルスバスター Corp. サーバによって管理されていないコンピュータにのみ配信してください。その後、ユーザ指定のアップデート元など、ウイルスバスター Corp. サーバ以外のアップデート元からアップデートを取得するように、アップデートエージェントを設定します。ウイルスバスター Corp. サーバの設定とアップデートエージェントの設定を同期する場合は、Client Packager 以外のクライアントインストール方法を選択してください。

Force Overwrite with Latest Version

このオプションでは、クライアントのコンポーネントのバージョンを、現在サーバで使用可能なバージョンで上書きします。このオプションを有効にすると、サーバとクライアントのコンポーネントが同期されます。

Disable Prescan (Only for Fresh Installation)

対象コンピュータにウイルスバスター Corp. クライアントがインストールされていない場合は、クライアントのインストールを実行する前に、最初にパッケージによってこのコンピュータのセキュリティ上の脅威が検索されます。対象コンピュータがセキュリティ上の脅威に感染していないことが明らかな場合は、事前検索を無効にします。

事前検索が有効な場合は、セットアップによって、次に示すようなコンピュータ上の最も攻撃を受けやすい領域でウイルス / 不正プログラムの検索が実行されます。

- システム領域とシステムディレクトリ (システム領域感染型ウイルスが対象)
- Windows フォルダ
- [Program Files] フォルダ

Outlook Mail Scan

このオプションでは、Outlook メール検索プログラムがインストールされます。このプログラムにより、Microsoft Outlook のメールボックスのセキュリティ上の脅威が検索されます。詳細については、290 ページの「Outlook メール検索」を参照してください。

Check Point SecureClient Support

このツールを使用すると、Windows 2000/XP/Server 2003 用 Check Point SecureClient のサポートが追加されます。SecureClient では、ウイルスパターンファイルのバージョンを確認した上でネットワーク接続が許可されます。詳細については、362 ページの「Check Point ファイアウォールのアーキテクチャの概要と設定」を参照してください。

注意： SecureClient では、スマートスキャンを使用するクライアントに対してウイルスパターンファイルのバージョンを確認しません。

Components

パッケージに含めるコンポーネントを選択します。詳細については、118 ページの「トレンドマイクロ ウイルスバスター コーポレートエディションのコンポーネントとプログラム」を参照してください。

Active Directory を使用した MSI パッケージの配信

Active Directory の機能を利用すれば、複数のクライアントコンピュータに MSI パッケージを同時に配信することができます。MSI ファイルの作成手順については、79 ページの「Client Packager を使用したインストール」を参照してください。

Active Directory を使用して MSI パッケージを配信するには

1. Active Directory コンソールを開きます。
2. MSI パッケージを配信する組織単位 (OU) を右クリックして、[プロパティ] をクリックします。
3. [グループ ポリシー] タブで [新規] をクリックします。
4. [コンピュータの構成] または [ユーザの構成] のいずれかを選択して、その下にある [ソフトウェアの設定] を開きます。

ヒント： コンピュータにログオンするユーザの種類に関係なく MSI パッケージをインストールするために、[ユーザの構成] ではなく [コンピュータの構成] を使用することをお勧めします。

5. [ソフトウェアの設定] で [ソフトウェア インストール] を右クリックして、[新規作成] および [パッケージ] を選択します。
6. MSI パッケージを探して選択します。

7. 配信方法を選択して、[OK] をクリックします。

- **割り当て**：MSI パッケージは、ユーザが次回コンピュータにログオンするとき（[ユーザの構成] を選択した場合）、またはコンピュータが再起動するとき（[コンピュータの構成] を選択した場合）に、自動的に配信されます。この方法では、ユーザの操作は必要ありません。
- **公開**：MSI パッケージを実行するには、[コントロール パネル] に進み、[プログラムの追加と削除] 画面を開き、ネットワーク上のプログラムを追加 / インストールするオプションを選択するようにユーザに通知します。ウイルスバスター Corp. クライアントの MSI パッケージが表示されたら、ユーザはクライアントのインストールを続行できます。

Microsoft SMS を使用した MSI パッケージの配信

サーバに Microsoft BackOffice SMS がインストールされている場合は、Microsoft SMS (Systems Management Server) を使用して、MSI パッケージを配信します。MSI ファイルの作成手順については、79 ページの「Client Packager を使用したインストール」を参照してください。

SMS サーバでは、パッケージを対象コンピュータに配信する前に、ウイルスバスター Corp. サーバから MSI ファイルを取得する必要があります。

- ローカル：SMS サーバとウイルスバスター Corp. サーバが、同一コンピュータ上にある場合です。
- リモート：SMS サーバとウイルスバスター Corp. サーバが、異なるコンピュータ上にある場合です。

Microsoft SMS を使用してインストールする場合の既知の問題

- SMS コンソールの [実行時間] 列に「不明」と表示されます。
- インストールが成功しなかった場合でも、インストールステータスは、SMS プログラムモニタ上でインストールが完了したことを示す場合があります。インストールが完了したかどうかを確認する方法については、108 ページの「ポストインストール」を参照してください。

以下の手順は、Microsoft SMS 2.0 および 2003 を使用する場合を対象としています。

パッケージをローカルで取得するには

1. SMS 管理コンソールを開きます。
2. [ツリー] タブの [パッケージ] をクリックします。
3. [操作] メニューから、[新規作成] → [定義に基づくパッケージ] の順にクリックします。定義に基づくパッケージの作成ウィザードの [ようこそ] 画面が表示されます。
4. [次へ] をクリックします。[パッケージ定義] 画面が表示されます。
5. [参照] をクリックします。[ファイルを開く] 画面が表示されます。

6. Client Packager によって作成された MSI パッケージファイルを参照して選択し、[ファイルを開く] をクリックします。[パッケージ定義] 画面に、MSI パッケージ名が表示されます。パッケージには、「ウイルスバスター Corp. クライアント」とプログラムのバージョンが表示されています。
7. [次へ] をクリックします。[ソース ファイル] 画面が表示されます。
8. [常にソース ディレクトリからファイルを取得する] をクリックし、[次へ] をクリックします。[ソース ディレクトリ] 画面が表示されます。この画面には、作成するパッケージの名前とソース ディレクトリが表示されています。
9. [サイト サーバのローカル ドライブ] をクリックします。
10. [参照] をクリックして、MSI ファイルが含まれているソースディレクトリを選択します。
11. [次へ] をクリックします。ウィザードによりパッケージが作成されます。パッケージの作成が完了すると、パッケージの名前が SMS 管理コンソールに表示されます。

パッケージをリモートで取得するには

1. ウイルスバスター Corp. サーバで、Client Packager を使用し、.exe 拡張子が付いたセットアップパッケージを作成します (.msi パッケージは作成できません)。詳細については、79 ページの「Client Packager を使用したインストール」を参照してください。
2. ソースを格納するコンピュータで、共有フォルダを作成します。
3. SMS 管理コンソールを開きます。
4. [ツリー] タブの [パッケージ] をクリックします。
5. [操作] メニューから、[新規作成] → [定義に基づくパッケージ] の順にクリックします。定義に基づくパッケージの作成ウィザードの [ようこそ] 画面が表示されます。
6. [次へ] をクリックします。[パッケージ定義] 画面が表示されます。
7. [参照] をクリックします。[ファイルを開く] 画面が表示されます。
8. MSI パッケージファイルを参照します。MSI パッケージファイルは、作成した共有フォルダにあります。
9. [次へ] をクリックします。[ソース ファイル] 画面が表示されます。
10. [常にソース ディレクトリからファイルを取得する] をクリックし、[次へ] をクリックします。[ソース ディレクトリ] 画面が表示されます。
11. [ネットワーク パス (UNC 名)] をクリックします。
12. [参照] をクリックして、MSI ファイルが含まれているソースディレクトリ (作成した共有フォルダ) を選択します。
13. [次へ] をクリックします。ウィザードによりパッケージが作成されます。パッケージの作成が完了すると、パッケージの名前が SMS 管理コンソールに表示されます。

対象コンピュータにパッケージを配信するには

1. [ツリー] タブの [提供情報] をクリックします。
2. [操作] メニューから、[すべてのタスク] → [ソフトウェアの配布] の順にクリックします。ソフトウェアの配布ウィザードの [よろこ] 画面が表示されます。
3. [次へ] をクリックします。[パッケージ] 画面が表示されます。
4. [既存のパッケージを配布する] をクリックし、作成したセットアップパッケージの名前をクリックします。
5. [次へ] をクリックします。[配布ポイント] 画面が表示されます。
6. パッケージをコピーする配布ポイントを選択し、[次へ] をクリックします。[プログラムの提供] 画面が表示されます。
7. クライアントのセットアップパッケージを提供するには、[はい] をクリックしてから [次へ] をクリックします。[提供情報のターゲット] 画面が表示されます。
8. [参照] をクリックして対象コンピュータを選択します。[コレクションの参照] 画面が表示されます。
9. [すべての Windows NT システム] をクリックします。
10. [OK] をクリックします。[提供情報のターゲット] 画面が再度表示されます。
11. [次へ] をクリックします。[提供情報の名前] 画面が表示されます。
12. テキストボックスに提供情報の名前とコメントを入力して、[次へ] をクリックします。[サブコレクションへの提供] 画面が表示されます。
13. パッケージをサブコレクションに提供するかどうかを決定します。指定したコレクションのメンバーだけにプログラムを提供するか、またはサブコレクションのメンバーにプログラムを提供するかを選択できます。
14. [次へ] をクリックします。[提供情報のスケジュール] 画面が表示されます。
15. 日時を入力するか選択して、クライアントセットアップパッケージをいつ提供するかを指定します。

特定の日付にパッケージの提供を停止するように Microsoft SMS を設定するには、[はい] をクリックします。この提供情報に有効期限を設定する場合、[有効期限の日時] のリストボックスで日時を指定します。
16. [次へ] をクリックします。[プログラムの割り当て] 画面が表示されます。
17. [はい、プログラムを割り当てます] をクリックしてから [次へ] をクリックします。

Microsoft SMS によって提供情報が作成され、SMS 管理コンソールに表示されます。
18. Microsoft SMS によって、提供されたプログラム (ウイルスバスター Corp. クライアントプログラム) が対象コンピュータに配布されると、対象コンピュータごとに画面が表示されます。[は

い] をクリックし、ウィザードの指示に従ってウイルスバスター Corp. クライアントをコンピュータにインストールするように、ユーザに指示します。

ウイルスバスター Corp. Web コンソールからのインストール

ウイルスバスター Corp. クライアントを、ネットワークに接続された 1 台以上のコンピュータにリモートインストールします。リモートインストールを行うためには、インストール先コンピュータに対して管理者権限があることを確認してください。リモートインストールでは、すでにウイルスバスター Corp. サーバが動作しているコンピュータには、ウイルスバスター Corp. クライアントをインストールしません。

注意： このインストール方法は、Windows XP Home、Windows Vista Home Basic および Home Premium Editions (32 ビットバージョンと 64 ビットバージョン) が動作しているコンピュータでは使用できません。

ウイルスバスター Corp. Web コンソールからインストールするには

1. コンピュータで Windows Vista を実行していない場合は、この手順を省略します。Windows Vista Business、Enterprise、または Ultimate Edition を実行している場合は、次の手順を実行します。
 - a. ビルトインの管理者アカウントを有効にして、そのアカウントのパスワードを設定します。
 - b. [スタート] → [プログラム] → [管理ツール] → [セキュリティが強化された Windows ファイアウォール] をクリックします。
 - c. 「ドメイン プロファイル」、「プライベート プロファイル」、および「パブリック プロファイル」で、ファイアウォールの状態をオフにします。
 - d. Microsoft 管理コンソール ([スタート] → [ファイル名を指定して実行] をクリックして「services.msc」と入力) を開いて、リモートレジストリサービスを起動します。ウイルスバスター Corp. クライアントのインストールには、ビルトインの管理者アカウントとパスワードを使用します。
2. Web コンソールで、[ネットワーク上のコンピュータ] → [クライアントのインストール] → [リモート] の順にクリックします。
3. インストール先コンピュータを選択します。
 - [ドメインとコンピュータ] リストに、ネットワーク上のすべての Windows ドメインが表示されます。ドメインのコンピュータを表示するには、ドメイン名をダブルクリックします。コンピュータを選択して、[追加] をクリックします。

- 特定のコンピュータ名を指定したい場合は、そのコンピュータ名をページ最上部のフィールドに入力して [検索] をクリックします。

インストール先コンピュータのユーザ名とパスワードを入力するよう求めるメッセージが表示されます。管理者アカウントのユーザ名とパスワードを使用して、続行してください。

4. ユーザ名とパスワードを入力してから、[ログオン] をクリックします。インストール先コンピュータが [選択したコンピュータ] 表に表示されます。
5. さらにコンピュータを追加するには、手順 3 と 4 を繰り返します。
6. クライアントをインストール先コンピュータへインストールする準備ができたなら、[インストール] をクリックします。確認ボックスが表示されます。
7. [はい] をクリックして、クライアントをインストール先コンピュータへインストールすることを確認します。各インストール先コンピュータへプログラムファイルがコピーされるときに、進捗状況画面が表示されます。

インストール先コンピュータへのインストールが完了すると、ダイアログが表示されます。[OK] をクリックし、ダイアログを閉じてリモートインストールは完了です。また、[選択したコンピュータ] リストで結果を確認することができます。

注意： 複数のコンピュータにインストールする場合、ウイルスバスター Corp. は失敗したインストールがあればログに記録しますが、他のインストールは続行します。[インストール] をクリックした後は、インストールを監視する必要はありません。後でログをチェックして、インストール結果を確認してください。

クライアントのディスクイメージからのインストール

ディスクイメージング技術により、ディスクイメージングソフトウェアを使用してウイルスバスター Corp. クライアントのイメージを作成し、そのイメージのクローンをネットワーク上の他のコンピュータに作成できます。

サーバがクライアントを個々に識別できるように、各クライアントのインストールでは GUID (Globally Unique Identifier) が必要になります。ウイルスバスター Corp. のプログラム ImgSetup.exe を使用して、クローンごとに異なる GUID を作成します。

注意： このインストール方法は、Windows Vista および 2008 を実行しているコンピュータでは使用できません。

ウイルスバスター Corp. クライアントのディスクイメージを作成するには

1. ウイルスバスター Corp. クライアントをコンピュータにインストールします。
2. ImgSetup.exe を、<「サーバのインストールフォルダ」>¥PCCSRV¥Admin¥Utility¥ImgSetup フォルダからこのコンピュータにコピーします。
3. ImgSetup.exe をこのコンピュータで実行します。RUN レジストリキーが HKEY_LOCAL_MACHINE の下に作成されます。
4. ディスクイメージングソフトウェアを使用して、ウイルスバスター Corp. クライアントのディスクイメージを作成します。
5. クローンを再起動します。ImgSetup.exe が自動的に起動され、新しい GUID 値が 1 つ作成されます。クライアントはこの新しい GUID をサーバにレポートし、サーバは新しいクライアントの新しいレコードを作成します。

警告： ウイルスバスター Corp. データベースに同じ名前を持つ 2 つのコンピュータが存在しないように、複製したウイルスバスター Corp. クライアントのコンピュータ名またはドメイン名を手動で変更してください。

脆弱性検索ツールの使用

脆弱性検索ツールを使用して、インストールされているウイルス対策ソリューションを検出し、ネットワーク上の保護されていないコンピュータを検索して、コンピュータにウイルスバスター Corp. クライアントをインストールします。コンピュータを保護するかどうかを判断するために、脆弱性検索ツールは、ウイルス対策ソリューションが通常使用するポートに対して Ping コマンドを実行します。

脆弱性検索ツールの機能

脆弱性検索ツールでは、次の機能を実行します。

- ・ ネットワークにコンピュータが初めてログオンしたときに、その状態を判断できるように、ネットワーク上で DHCP 要求を監視します。
- ・ ネットワーク上のコンピュータに対して Ping コマンドを実行して状態を確認し、コンピュータ名、プラットフォームバージョン、および説明を取得します。
- ・ ネットワークにインストールされているウイルス対策ソリューションを判断します。脆弱性検索ツールでは、トレンドマイクロ製品とサードパーティのウイルス対策ソリューション (Norton AntiVirus Corporate Edition、McAfee VirusScan ePolicy Orchestrator など) を検出できます。
- ・ メールを使用して検索結果を送信するか、結果をカンマ区切り形式 (CSV) ファイルにエクスポートします。

脆弱性検索ツール使用時の考慮事項

脆弱性検索ツールを使用するかどうかを決定する際には、次のことを考慮に入れてください。

ネットワーク管理

表 3-9. ネットワーク管理

環境	脆弱性検索ツールの効果
厳しいセキュリティポリシーによる管理	非常に効果的。脆弱性検索ツールは、すべてのコンピュータにウイルス対策ソフトウェアがインストールされているかどうかをレポートします。
各拠点ごとに管理	やや効果的
一元管理	やや効果的
アウトソーシング	やや効果的

表 3-9. ネットワーク管理 (続き)

環境	脆弱性検索ツールの効果
各ユーザによるコンピュータ管理	効果なし。脆弱性検索ツールは、ネットワーク上のウイルス対策ソフトウェアを検索するため、ユーザが独自のコンピュータを検索するのには適していません。

ネットワークトポロジとアーキテクチャ

表 3-10. ネットワークトポロジとアーキテクチャ

環境	脆弱性検索ツールの効果
単一の場合	非常に効果的。脆弱性検索ツールを使用すると、IP セグメント全体を検索し、LAN にウイルスバスター Corp. クライアントを簡単にインストールできます。
高速接続の複数の場所	やや効果的
低速接続の複数の場所	効果なし。各場所で脆弱性検索ツールを実行する必要があり、ウイルスバスター Corp. クライアントのインストールは、ローカルのウイルスバスター Corp. サーバを対象に行う必要があります。
リモートおよび単独のコンピュータ	効果なし。脆弱性検索ツールは、ネットワークに接続されていないコンピュータを検索できません。

ソフトウェア / ハードウェア仕様

表 3-11. ソフトウェア / ハードウェア仕様

環境	脆弱性検索ツールの効果
Windows NT ベースの OS	非常に効果的。脆弱性検索ツールは、NT ベースの OS (Windows XP Home を除く) が動作しているコンピュータに、ウイルスバスター Corp. クライアントを簡単にリモートインストールできます。
混合 OS	やや効果的。脆弱性検索ツールでは、Windows NT ベースの OS が動作しているコンピュータにのみインストールを実行できます。
デスクトップ管理ソフトウェア	効果なし。脆弱性検索ツールは、デスクトップ管理ソフトウェアでは使用できません。ただし、ウイルスバスター Corp. クライアントインストールの進捗状況の監視に役立ちます。

ドメイン構造

表 3-12. ドメイン構造

環境	脆弱性検索ツールの効果
Microsoft Active Directory	非常に効果的。脆弱性検索ツールでドメイン管理者アカウントを指定し、ウイルスバスター Corp. クライアントのリモートインストールを実行できるようにします。
ワークグループ	効果なし。脆弱性検索ツールでは、異なる管理アカウントとパスワードを使用したコンピュータへのインストールが困難な場合があります。
Novell Directory Service	効果なし。脆弱性検索ツールでは、ウイルスバスター Corp. クライアントをインストールするために Windows ドメインアカウントが必要です。
ピアツーピア	効果なし。脆弱性検索ツールでは、異なる管理アカウントとパスワードを使用したコンピュータへのインストールが困難な場合があります。

ネットワークトラフィック

表 3-13. ネットワークトラフィック

環境	脆弱性検索ツールの効果
LAN 接続	非常に効果的
512 Kbps	やや効果的
T1 接続以上	やや効果的
ダイヤルアップ	効果なし。ウイルスバスター Corp. クライアントのインストールに長時間要します。

ネットワークサイズ

表 3-14. ネットワークサイズ

環境	脆弱性検索ツールの効果
大規模企業	非常に効果的。ネットワークが大きくなればなるほど、ウイルスバスター Corp. クライアントインストールのチェックのために、脆弱性検索ツールの必要性が高まります。
中小企業	やや効果的。小規模ネットワークでは、脆弱性検索ツールは、ウイルスバスター Corp. クライアントをインストールする際の 1 つの選択肢になります。他のクライアントインストール方法の方が、実装が簡単なことがあります。

ユーザタスク

脆弱性検索ツールから、以下のタスクを実行します。

- ・ 95 ページの「ウイルスバスター Corp. クライアントのインストール」
- ・ 96 ページの「一般設定の管理」
- ・ 99 ページの「脆弱性検索の実行」
- ・ 102 ページの「予約タスクの作成」
- ・ 102 ページの「その他の脆弱性検索ツールの設定」

別のコンピュータでの脆弱性検索ツールの起動

ウイルスバスター Corp. サーバコンピュータ以外のコンピュータで、脆弱性検索ツールを起動できます。他のコンピュータで Windows 2000、2003、および 2008 が動作していることを確認します。Windows XP、Vsta、または Terminal Server では、ツールを起動できません。

別のコンピュータで脆弱性検索ツールを起動するには

1. ウイルスバスター Corp. サーバコンピュータに接続します。
2. <「サーバのインストールフォルダ」>¥PCCSRV¥Admin¥Utility の TMVS フォルダを、別のコンピュータにコピーします。
3. TMVS フォルダをコピーしたら、TMVS.exe をダブルクリックします。

ウイルスバスター Corp. クライアントのインストール

脆弱性検索ツールを使用すると、ウイルスバスター Corp. クライアントをリモートコンピュータにインストールできます。ただし次の場合、ウイルスバスター Corp. クライアントはインストールされません。

- リモートコンピュータに、ウイルスバスター Corp. サーバまたはその他のウイルス対策製品がすでにインストールされている場合。
- リモートコンピュータで、Windows XP Home、Windows Vista Home Basic、および Windows Vista Home Premium が動作している場合。

脆弱性検索ツールを使用してウイルスバスター Corp. クライアントをインストールするには

1. Windows Vista Business、Enterprise、または Ultimate Edition を実行している場合は、次の手順を実行します。
 - a. ビルトインの管理者アカウントを有効にして、そのアカウントのパスワードを設定します。
 - b. [スタート] → [プログラム] → [管理ツール] → [セキュリティが強化された Windows ファイアウォール] をクリックします。
 - c. 「ドメイン プロファイル」、「プライベート プロファイル」、および「パブリック プロファイル」で、ファイアウォールの状態をオフにします。
 - d. Microsoft 管理コンソール ([スタート] → [ファイル名を指定して実行] をクリックして「services.msc」と入力) を開いて、リモートレジストリサービスを起動します。ウイルスバスター Corp. クライアントのインストールには、ビルトインの管理者アカウントとパスワードを使用します。
2. Windows XP Professional (32 ビット版または 64 ビット版) を実行している場合は、次の手順を実行します。
 - a. Windows エクスプローラを開いて、[ツール] → [フォルダ オプション] の順にクリックします。
 - b. [表示] タブをクリックして、[簡易ファイルの共有を使用する (推奨)] を無効にします。
3. TMVS フォルダに移動して、TMVS.exe をダブルクリックします。脆弱性検索ツールのコンソールが表示されます。

注意： ウイルスバスター Corp. サーバコンピュータでは、TMVS フォルダは<「サーバのインストールフォルダ」>%PCCSRV%\Admin\Utility にあります。TMVS フォルダを別のコンピュータにコピーした場合は、そのコンピュータの TMVS フォルダに移動します。

4. [Settings] をクリックします。

5. [OfficeScan server settings] で、ウイルスバスター Corp. サーバの名前とポート番号を入力します。
6. [Auto-Install OfficeScan client on unprotected computers] を選択します。
7. [OK] をクリックして、ネットワーク上のコンピュータのチェックと、ウイルスバスター Corp. クライアントのインストールを開始します。

一般設定の管理

脆弱性検索ツールの次の設定を設定および管理するには、<「サーバのインストールフォルダ」>¥PCCSRV¥Admin¥Utility¥TMVS に移動し、TMVS.exe をダブルクリックします。

製品クエリ

ネットワーク上のチェックする製品を選択します。誤検出を回避するために、すべてのチェックボックスをオンにします。製品名の横にある [Settings] をクリックして、脆弱性検索ツールでチェックするポート番号を確認します。

各製品 (ServerProtect for Windows、ServerProtect for Linux、および McAfee VirusScan ePolicy Orchestrator は除く) のポート設定を手動で設定します。

次の表は、脆弱性検索ツールによるセキュリティ製品のチェック方法を示しています。

表 3-15. 脆弱性検索ツールでチェックされるセキュリティ製品

製品	説明
ウイルスバスター Corp. クライアント	脆弱性検索ツールは、ウイルスバスター Corp. クライアントポートを使用して、ウイルスバスター Corp. クライアントがインストールされているかどうかをチェックします。また、TMListen.exe プロセスが動作しているのかもチェックします。初期設定の場所から実行された場合は、自動的にポート番号を取得します。 ウイルスバスター Corp. サーバ以外のコンピュータで TMVS を起動した場合は、他のコンピュータの通信ポートをチェックしてから使用してください。
Trend Micro Internet Security (ウイルスバスター)	脆弱性検索ツールは、ポート 40116 を使用して、ウイルスバスターがインストールされているかどうかをチェックします。

表 3-15. 脆弱性検索ツールでチェックされるセキュリティ製品 (続き)

製品	説明
ServerProtect for Windows	脆弱性検索ツールは、RPC エンドポイントを使用して、SPNTSVC.exe が動作しているかどうかをチェックします。また、OS、ウイルス検索エンジン、ウイルスパターンファイル、製品バージョンなどの情報を返します。ServerProtect インフォメーションサーバまたは ServerProtect 管理コンソールは検出できません。
ServerProtect for Linux	対象のコンピュータで Windows が実行されていない場合、脆弱性検索ツールは、ポート 14942 への接続を試みて、ServerProtect for Linux がインストールされているかどうかをチェックします。
InterScan for Microsoft Exchange	脆弱性検索ツールは、Web ページ http://ipaddress:port/scanmail.html をロードして、InterScan のインストールをチェックします。InterScan で使用される初期設定のポート番号は 16372 です。InterScan で別のポート番号が使用される場合は、そのポート番号を指定してください。指定しない場合、脆弱性検索ツールで InterScan for Exchange を検出できません。
InterScan ファミリ	脆弱性検索ツールは、さまざまな製品の各 Web ページをロードして、製品のインストールをチェックします。 - InterScan Messaging Security Suite 5.x: http://localhost:port/eManager/cgi-bin/eManager.htm - InterScan eManager 3.x: http://localhost:port/eManager/cgi-bin/eManager.htm - InterScan VirusWall 3.x: http://localhost:port/InterScan/cgi-bin/interscan.dll
PortalProtect	脆弱性検索ツールは、Web ページ http://localhost:port/PortalProtect/index.html をロードして、製品のインストールをチェックします。
Norton Antivirus Corporate Edition	脆弱性検索ツールは、特殊なトークンを UDP ポート 2967 (Norton Antivirus Corporate Edition RTVScan の初期設定ポート) に送信します。このウイルス対策製品がインストールされているコンピュータは、特殊なトークンタイプを使用して返信します。Norton Antivirus Corporate Edition は UDP を使用して通信するため、精度は保証されません。さらに、ネットワークトラフィックが UDP の待機時間に影響する場合があります。

表 3-15. 脆弱性検索ツールでチェックされるセキュリティ製品 (続き)

製品	説明
McAfee VirusScan ePolicy Orchestrator	脆弱性検索ツールは、特殊なトークンを TCP ポート 8081 (サーバとクライアントを接続するための ePolicy Orchestrator の初期設定ポート) に送信します。このウイルス対策製品がインストールされているコンピュータは、特殊なトークンタイプを使用して返信します。脆弱性検索ツールは、スタンドアロンの McAfee VirusScan を検出できません。

プロトコル

脆弱性検索ツールでは、以下のプロトコルを使用する製品とコンピュータを検出します。

- **RPC:** ServerProtect for Windows NT を検出します。
- **UDP:** Norton AntiVirus Corporate Edition クライアントを検出します。
- **TCP:** McAfee VirusScan ePolicy Orchestrator を検出します。
- **ICMP:** ICMP パケットを送信することによりコンピュータを検出します。
- **HTTP:** ウイルスバスター Corp. クライアントを検出します。
- **DHCP:** DHCP 要求を検出すると、脆弱性検出ツールは、要求元のコンピュータにウイルス対策ソフトウェアがインストールされているかどうかをチェックします。

コンピュータの説明を取得する方法

[Quick retrieval] は、コンピュータ名のみを取得します。[Normal retrieval] は、ドメインとコンピュータの両方の情報を取得するため、完了までの時間が長くなります。[Normal retrieval] を選択した場合は、コンピュータの説明があればそれを取得するように脆弱性検索ツールを設定します。

通知

検索結果を管理者自身または同じ組織内の他の管理者に自動的に送信するには、[Email results to the system administrator] を選択し、[Configure] をクリックしてメールの設定を指定します。

1. [To] に、受信者のメールアドレスを入力します。
2. [From] に、メッセージの送信者を受信者に知らせるためのメールアドレスを入力します。
3. [SMTP server] に、SMTP サーバのアドレスを入力します。たとえば、「smtp.company.com」と入力します。SMTP サーバ情報が必要です。
4. [Subject] に、メッセージの新しい件名を入力するか、初期設定の件名をそのまま使用します。
5. [OK] をクリックします。

6. 保護されていないコンピュータに通知を表示するように選択します。[Customize] をクリックして、通知メッセージを設定します。[Notification Message] 画面で、新しいメッセージを入力するか、初期設定のメッセージをそのまま使用します。[OK] をクリックします。

脆弱性検索結果

検索結果を、カンマ区切り形式 (.csv) のファイルに保存します。CSV ファイルを保存する初期設定のフォルダを変更するには、[Browse] をクリックし、コンピュータまたはネットワーク上の対象フォルダを選択して、[OK] をクリックします。

Ping 設定

脆弱性検索ツールで、ネットワーク上のコンピュータに Ping コマンドを実行し、その状態を取得することができます。脆弱性検索ツールがコンピュータにパケットを送信し応答を待つ方法を指定するには、[Allow Vulnerability Scanner to ping computers on your network to check their status] を選択して初期設定をそのまま使用するか、[Packet size] テキストボックスと [Timeout] テキストボックスに新しい値を入力します。

脆弱性検索ツールは、ICMP OS フィンガープリントを使用して、OS の種類を検出することもできます。

ウイルスバスター Corp. サーバの設定

ウイルスバスター Corp. サーバの名前とポート番号を入力します。脆弱性検索ツールは、ウイルスバスター Corp. クライアントを、保護されていないコンピュータに自動インストールできます。

[Install to Account] をクリックしてアカウントを設定します。[Account Information] 画面で、インストールを許可するユーザ名とパスワードを入力します。[OK] をクリックします。

脆弱性検索ツールは、ログをウイルスバスター Corp. サーバへ送信することもできます。

脆弱性検索の実行

IP アドレス範囲を指定して、複数のコンピュータで脆弱性検索を実行します。

脆弱性検索は、DHCP サーバに IP アドレスを要求するコンピュータ上でも実行できます。脆弱性検索ツールは、ポート 67 (DHCP 要求用の DHCP サーバ待機ポート) で待機します。DHCP 要求を検出すると、脆弱性検索ツールは、要求元コンピュータにウイルス対策ソフトウェアがインストールされているかどうかを確認できます。

IP アドレスの範囲に対して手動で脆弱性検索を実行するには

1. <「サーバのインストールフォルダ」>¥PCCSRV¥Admin¥Utility¥TMVS に移動し、TMVS.exe をダブルクリックします。脆弱性検索ツールのコンソールが表示されます。
2. [Manual Scan] で、チェックするコンピュータの IP アドレス範囲を入力します。

注意： 脆弱性検索ツールでは、クラス B の IP アドレス範囲（例：168.212.1.1 から 168.212.254.254）のみをサポートします。

3. [Start] をクリックします。脆弱性検索結果が、[Manual Scan] タブの [Results] 表に表示されます。

注意： コンピュータで Windows 2008 が動作している場合は、MAC アドレス情報は [Results] 表に表示されません。

4. 検索結果をカンマ区切り形式（.csv）のファイルに保存するには、[Export] をクリックして、ファイルを保存するフォルダの場所を指定し、ファイル名を入力して [Save] をクリックします。

DHCP サーバに IP アドレスを要求するコンピュータで脆弱性検索を実行するには

1. <「サーバのインストールフォルダ」>¥PCCSRV¥Admin¥Utility¥TMVS フォルダにある TMVS.ini ファイルで、DHCP 設定を構成します。

表 3-16. TMVS.ini ファイルの DHCP 設定

設定	説明
DhcpThreadNum=x	DHCP モードのスレッド番号を指定します。最小は 3、最大は 100、初期設定は 3 です。
DhcpDelayScan=x	要求元コンピュータでインストールされたウイルス対策ソフトウェアのチェックを行うまでの遅延時間 (秒) です。 最小は 0 (待機なし)、最大は 600、初期設定は 60 です。
LogReport=x	0 を指定するとログが無効になり、1 を指定するとログが有効になります。 脆弱性検索ツールによって検索結果がウイルスバスター Corp. サーバに送信され、ログは Web コンソールの [システムイベントログ] 画面に表示されます。
OsceServer=x	ウイルスバスター Corp. サーバの IP アドレスまたは DNS 名です。
OsceServerPort=x	ウイルスバスター Corp. サーバの Web サーバポートです。

2. <「サーバのインストールフォルダ」>¥PCCSRV¥Admin¥Utility¥TMVS に移動し、TMVS.exe をダブルクリックします。脆弱性検索ツールのコンソールが表示されます。
3. [Results] 表で [DHCP Scan] タブをクリックします。

注意： Windows 2008 が動作しているコンピュータでは、[DHCP Scan] タブは利用できません。

4. [Start] をクリックします。コンピュータがネットワークにログオンすると、脆弱性検索ツールは、DHCP 要求の待機とコンピュータの脆弱性チェックを開始します。保護されていないコンピュータを検出し、コンピュータの IP アドレスが定義された IP アドレス範囲内にあることを確認すると、脆弱性検索ツールは、リモートインストールを実行してウイルスバスター Corp. クライアントをインストールします。
5. 検索結果をカンマ区切り形式 (.csv) のファイルに保存するには、[Export] をクリックして、ファイルを保存するフォルダの場所を指定し、ファイル名を入力して [Save] をクリックします。

予約タスクの作成

脆弱性検索ツールで予約タスクを作成すると、ネットワーク上でインストールされているウイルス対策ソリューションのチェックを定期的に行うことができます。これはタスクを自動的に実行するのに便利な方法であり、脆弱性検索ツールを毎回設定する必要がありません。

予約タスクを作成するには

1. <「サーバのインストールフォルダ」>¥PCCSRV¥Admin¥Utility¥TMVS に移動し、TMVS.exe をダブルクリックします。脆弱性検索ツールのコンソールが表示されます。
2. [Results] 表で [DHCP Scan] タブをクリックします。

注意： Windows 2008 が動作しているコンピュータでは、[DHCP Scan] タブは利用できません。

3. [Scheduled Scan] で、[Add/Edit] をクリックします。[Scheduled Scan] 画面が表示されます。次の設定を行います。
 - Name: 予約検索の名前を入力します。
 - IP address range: チェックするコンピュータの IP アドレス範囲を入力します。
 - Start time: 検索を実行する時刻を入力するか選択します。24 時間形式を使用します。
 - Frequency: 検索が実行される頻度を選択します。日次、週次、月次から選択します。
 - Settings: [Use current settings] をクリックして既存の設定を使用するか、[Modify settings] をクリックします。[Modify settings] をクリックした場合は、[Settings] をクリックして設定を変更します。
4. [OK] をクリックします。作成した予約検索が [Scheduled Scan] に表示されます。
5. 予約検索をただちに実行するには、[Run Now] をクリックします。

その他の脆弱性検索ツールの設定

一部の脆弱性検索ツールの設定は、TMVS.ini ファイルでのみ設定できます。

TMVS.ini ファイルで設定を変更するには

1. <「サーバのインストールフォルダ」>¥PCCSRV¥Admin¥Utility¥TMVS に移動して、メモ帳などのテキストエディタを使用して TMVS.ini を開きます。
2. 脆弱性検索ツールが同時に ping コマンドを実行するコンピュータ数を設定するには、EchoNum の値を変更します。1 ～ 64 の値を指定します。

たとえば、同時に 60 台のコンピュータに ping コマンドを実行するようにするには、「EchoNum=60」と入力します。

3. 脆弱性検索ツールが、同時にウイルス対策ソフトウェアをチェックするコンピュータ数を設定するには、ThreadNumManual の値を変更します。8 ～ 64 の値を指定します。

たとえば、同時に 60 台のコンピュータのウイルス対策ソフトウェアをチェックするには、「ThreadNumManual=60」と入力します。

4. 予約タスクを実行中に、脆弱性検索ツールが同時にウイルス対策ソフトウェアをチェックするコンピュータ数を設定するには、ThreadNumSchedule の値を変更します。8 ～ 64 の値を指定します。

たとえば、予約タスクを実行中に、同時に 60 台のコンピュータのウイルス対策ソフトウェアをチェックするには、「ThreadNumSchedule=60」と入力します。

5. TMVS.ini を保存します。

注意： 脆弱性検索ツールのデバッグログを収集する方法については、368 ページの「LogServer.exe を使用するサーバデバッグログ」を参照してください。

ウイルスバスター Corp. クライアントへの移行

対象コンピュータにインストールされているエンドポイントセキュリティソフトウェアを、ウイルスバスター Corp. クライアントへ移行します。

他のエンドポイントセキュリティソフトウェアからの移行

ウイルスバスター Corp. クライアントをインストールするときに、インストールプログラムによって、トレンドマイクロまたはサードパーティのエンドポイントセキュリティソフトウェアが対象コンピュータにインストールされているかどうかチェックされます。インストールプログラムでは、ソフトウェアを自動的にアンインストールし、ウイルスバスター Corp. クライアントに置き換えることができます。

ウイルスバスター Corp. で自動的にアンインストールされるエンドポイントセキュリティソフトウェアのリストについては、<「サーバーのインストールフォルダ」>%PCCSRV%\Admin にある次のファイルを開いて確認してください。メモ帳などのテキストエディタを使用して、これらのファイルを開きます。

- tmuninst.ptn
- tmuninst_as.ptn

対象コンピュータのソフトウェアがリストに含まれていない場合は、そのソフトウェアを最初に手動でアンインストールします。ソフトウェアのアンインストール処理によっては、アンインストールの終了後、コンピュータの再起動が必要になる場合があります。

クライアントの移行の問題

- 自動的なクライアントの移行は正常に実行されたが、インストールの直後にウイルスバスター Corp. クライアントで問題が発生した場合は、コンピュータを再起動します。
- ウイルスバスター Corp. インストールプログラムでウイルスバスター Corp. クライアントのインストールを続行したが、他のセキュリティソフトウェアをアンインストールできなかった場合は、2つのソフトウェアの間に競合が発生します。両方のソフトウェアをアンインストールしてから、72 ページの「インストール方法」に記載されているインストール方法のいずれかを使用して、ウイルスバスター Corp. クライアントをインストールします。

ServerProtect 一般サーバからの移行

ServerProtect 一般サーバ移行ツールを使用すると、ServerProtect 一般サーバが動作しているコンピュータを、ウイルスバスター Corp. クライアントに移行できます。

ServerProtect 一般サーバ移行ツールは、ウイルスバスター Corp. サーバと同じハードウェアとソフトウェアの仕様を共有します。Windows 2000、2003、および 2008 コンピュータでツールを実行します。

ServerProtect 一般サーバのアンインストールが成功すると、ツールはウイルスバスター Corp. クライアントをインストールします。また、すべての検索タイプの検索除外リストの設定を、ウイルスバスター Corp. クライアントに移行します。

ウイルスバスター Corp. クライアントをインストール中に、移行ツールクライアントインストーラがタイムアウトになり、インストールが成功しなかったことが通知されることがありますが、クライアントは正常にインストールされている場合があります。この場合、ウイルスバスター Corp. Web コンソールから、クライアントコンピュータのインストールを確認してください。

次の状況では、移行は失敗します。

- ・ リモートクライアントが NetBIOS プロトコルを使用できない場合
- ・ ポート 455、337、および 339 がブロックされている場合
- ・ リモートクライアントが RPC プロトコルを使用できない場合
- ・ リモートレジストリサービスが停止している場合

注意： ServerProtect 一般サーバ移行ツールでは、ServerProtect 用の Control Manager エージェントはアンインストールされません。エージェントをアンインストールする方法については、ServerProtect または Control Manager のドキュメントを参照してください。

ServerProtect 一般サーバ移行ツールを使用するには

1. ウイルスバスター Corp. サーバコンピュータで、<「サーバのインストールフォルダ」>¥PCCSRV¥Admin¥Utility¥SPNSXfr を開き、ファイル SPNSXfr.exe と SPNSXfr.ini を <「サーバのインストールフォルダ」>¥PCCSRV¥Admin にコピーします。
2. SPNSXfr.exe ファイルをダブルクリックして、ツールを開きます。ServerProtect 一般サーバ移行ツールのコンソールが開きます。
3. ウイルスバスター Corp. サーバを選択します。ウイルスバスター Corp. サーバのパスが、ウイルスバスター Corp. サーバパスの下に表示されます。このパスが正しくない場合は、[選択] をクリックして、ウイルスバスター Corp. をインストールしたディレクトリの PCCSRV フォルダ

を選択します。

次回ツールを開いたときに、ウイルスバスター Corp. サーバが再度自動的に検索されるようにするには、[自動検索サーバパス] チェックボックスをオンにします（初期設定ではオンになっています）。

4. [対象コンピュータの選択] で次のいずれかをクリックし、移行を実行する、ServerProtect 一般サーバが動作しているコンピュータを選択します。
 - **Windows ネットワークツリー**：ネットワークのドメインのツリーを表示します。この方法を使用してコンピュータを選択するには、クライアントコンピュータを検索するドメインをクリックします。
 - **インフォメーションサーバ名**：インフォメーションサーバ名で検索します。この方法でコンピュータを選択するには、テキストボックスにネットワーク上のインフォメーションサーバの名前を入力します。複数のインフォメーションサーバを検索するには、サーバ名の間にセミコロン「;」を挿入します。
 - **特定の一般サーバ名**：一般サーバ名で検索します。この方法でコンピュータを選択するには、テキストボックスにネットワーク上の一般サーバの名前を入力します。複数の一般サーバを検索するには、サーバ名の間にセミコロン「;」を入力します。
 - **IP アドレス範囲検索**：IP アドレスの範囲で検索します。この方法でコンピュータを選択するには、IP 範囲でクラス B の IP アドレスの範囲を入力します。

注意： ネットワーク上の DNS サーバがクライアントの検索時に応答しない場合、検索は応答を停止します。検索がタイムアウトになるのを待ちます。

5. Windows Server 2003 が動作しているコンピュータを検索に含めることを選択します。
6. Windows Server 2003 が動作しているコンピュータの再起動を選択します。このコンピュータで移行を正常に完了させるには、コンピュータを再起動する必要があります。このチェックボックスをオンにすると、コンピュータは確実に自動的に再起動されます。[インストールした後に再起動します] チェックボックスをオンにしない場合は、移行後にコンピュータを手動で再起動します。
7. [検索] をクリックします。検索結果が、ServerProtect 一般サーバの下に表示されます。
8. 移行を実行するコンピュータをクリックします。
 - a. すべてのコンピュータを選択するには、[すべて選択] をクリックします。
 - b. すべてのコンピュータの選択を解除するには、[すべて選択解除] をクリックします。
 - c. リストをカンマ区切り形式（CSV）ファイルにエクスポートするには、[CSV 形式でエクスポート] をクリックします。

9. 対象コンピュータへのログインにユーザ名とパスワードが必要な場合は、次の操作を実行します。
 - a. [グループアカウント / パスワードの使用] チェックボックスをオンにします。
 - b. [ログオンアカウントの設定] をクリックします。[管理者情報の入力] ウィンドウが表示されます。
 - c. ユーザ名とパスワードを入力します。

注意： ローカル / ドメイン管理者アカウントを使用して、対象コンピュータにログオンします。「ゲスト」や「通常のユーザ」のような不十分な権限でログオンすると、インストールを実行できません。

- d. [OK] をクリックします。
 - e. [ログオンに失敗した場合再度入力] をクリックすると、ログオンできなかった場合、移行処理中に再度ユーザ名とパスワードを入力できます。
10. [移行] をクリックします。
11. コンピュータが Windows Server 2003 を実行している場合は、コンピュータを再起動して移行を完了します。

ポストインストール

インストール完了後に、以下のことを確認してください。

ウイルスバスター Corp. クライアントのショートカット

クライアントコンピュータの Windows の [スタート] メニューに、ウイルスバスター Corp. クライアントのショートカットが作成されている。

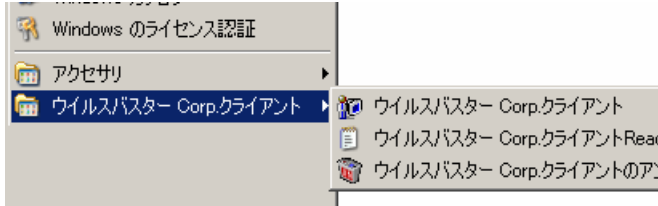


図 3-1. ウイルスバスター Corp. クライアントのショートカット

プログラムのリスト

クライアントコンピュータの [コントロール パネル] の [プログラムの追加と削除] に、[ウイルスバスター Corp. クライアント] が表示されている。

ウイルスバスター Corp. クライアントサービス

Microsoft 管理コンソールに、次のウイルスバスター Corp. クライアントサービスが表示されている。

- ウイルスバスター Corp. NT リスナー
- ウイルスバスター Corp. NT ファイアウォール (インストール中にファイアウォールを有効にした場合)
- ウイルスバスター Corp. NT プロキシサービス
- ウイルスバスター Corp. WinNT RealTime Scan
- Trend Micro Unauthorized Change Prevention Service (x86 タイプのプロセッサを実行しているコンピュータの場合のみ)

クライアントインストールログ

クライアントインストールログ OFCNT.LOG が、以下の場所に格納されている。

- MSI パッケージインストールを除くすべてのインストール方法の場合は、%windir%
- MSI パッケージインストール方法の場合は、%temp%

推奨されるポストインストールタスク

以下のポストインストールタスクを実行することをお勧めします。

コンポーネントのアップデート

セキュリティ上の脅威に対して最新の保護を実現するために、コンポーネントをアップデートするようにクライアントに通知します。

詳細については、139 ページの「クライアントアップデート」を参照してください。

EICAR テストスクリプトによるテスト検索

ヨーロッパコンピュータウイルス対策研究所 (EICAR) は、ウイルス対策ソフトウェアの適切なインストールと設定を確認する安全な方法として、EICAR テストスクリプトを開発しました。詳細については、次の EICAR Web サイトを参照してください。

<http://www.eicar.org>

EICAR テストスクリプトは、.com 拡張子のある不活性なテキストファイルです。このスクリプトはウイルスではなく、ウイルスコードのフラグメントを含みませんが、大部分のウイルス対策ソフトウェアは、このスクリプトがウイルスであるかのように反応します。これを使用してウイルス感染をシミュレーションし、メール通知およびウイルスログが正常に機能することを確認します。

警告： ウイルス対策製品のテストに、決して本物のウイルスを使用しないでください。

テスト検索を実行するには

1. クライアントでリアルタイム検索を有効にします。
2. 次の文字列をコピーし、メモ帳やテキストエディタに貼り付けます。
X5O!P%@AP [4PZX54 (P^) 7CC) 7>\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*
3. ファイルを EICAR.com として一時ディレクトリに保存します。ウイルスバスター Corp. がただちにファイルを検出します。
4. ネットワーク上の他のコンピュータをテストするには、EICAR.com ファイルをメールメッセージに添付し、ネットワーク上のコンピュータのいずれかに送信します。

ヒント： WinZip などの圧縮ソフトウェアを使用して EICAR ファイルをパッケージ化してから、別のテスト検索を実行することをお勧めします。

クライアントのアンインストール

クライアントからウイルスバスター Corp. プログラムをアンインストールするには、次の 2 つの方法があります。

- 110 ページの「Web コンソールからのクライアントのアンインストール」
- 111 ページの「クライアントアンインストールプログラムの実行」

クライアントに Cisco Trust Agent (CTA) がインストールされている場合は、ウイルスバスター Corp. クライアントプログラムのアンインストール時に Cisco Trust Agent が削除される場合と削除されない場合があります。これは、Cisco Trust Agent 配信時に設定した内容によって異なります。詳細については、349 ページの「Cisco Trust Agent の配信」を参照してください。

ウイルスバスター Corp. クライアントのアンインストール後に Cisco Trust Agent が存在する場合は、[プログラムの追加と削除] 画面から手動で削除します。

上記の方法でクライアントをアンインストールできない場合は、手動でアンインストールします。詳細については、112 ページの「クライアントの手動アンインストール」を参照してください。

Web コンソールからのクライアントのアンインストール

クライアントプログラムを Web コンソールからアンインストールします。プログラムで問題が発生した場合に限りアンインストールを実行し、その後ただちに再インストールして、セキュリティ上の脅威からコンピュータを保護します。

クライアントを Web コンソールからアンインストールするには

1. ウイルスバスター Corp. Web コンソールのメインメニューから、[ネットワーク上のコンピュータ] → [クライアント管理] の順にクリックします。クライアントツリーが表示されます。
2. クライアントツリーで、アンインストールするクライアントを選択します。
3. [タスク] → [クライアントのアンインストール] の順にクリックします。
4. [クライアントのアンインストール] で、[アンインストールの開始] をクリックします。サーバからクライアントに通知が送信されます。
5. 通知のステータスをチェックし、通知を受信していないクライアントがあるかどうかを確認します。
 - a. [未通知のコンピュータを選択] → [アンインストールの開始] の順にクリックすると、未通知のクライアントに対してただちに通知が再送信されます。

- b. [アンインストールの中止] をクリックすると、現在通知されているクライアントへの通知を停止するようにウイルスバスター Corp. に指示します。すでに通知されたクライアントおよびアンインストールを実行しているクライアントは、このコマンドを無視します。

クライアントアンインストールプログラムの実行

ユーザにクライアントプログラムをアンインストールする権限を付与した場合は、ユーザに、コンピュータからクライアントアンインストールプログラムを実行するように指示します。

この手順では、ユーザはアンインストールパスワードを指定する必要があります。アンインストールプログラムを実行するユーザとのみパスワードを共有し、パスワードが他のユーザに漏れた場合は、ただちにパスワードを変更してください。クライアントがアンインストールされるコンピュータで、パスワードを無効にすることもできます。詳細については、283 ページの「クライアントの権限とその他の設定」を参照してください。

クライアントアンインストールプログラムを実行するには

1. Windows の [スタート] メニューで、[プログラム] → [ウイルスバスター Corp. クライアント] → [ウイルスバスター Corp. クライアントのアンインストール] の順にクリックします。
次の手順を実行することもできます。
 - a. コントロールパネルの [プログラムの追加と削除] をクリックします。
 - b. [ウイルスバスター Corp. クライアント] を探し、[削除] をクリックします。
 - c. 画面の指示に従います。
2. アンインストールパスワードを要求された場合は、そのパスワードを入力します。アンインストールの進捗状況と完了がユーザに通知されます。ユーザは、アンインストールを完了するために、クライアントコンピュータを再起動する必要はありません。

クライアントの手動アンインストール

クライアントを Web コンソールからアンインストールする際、またはアンインストールプログラムの実行後に問題が発生した場合に限り、手動アンインストールを実行してください。

手動アンインストールを実行するには

1. 管理者権限のあるアカウントを使用して、クライアントコンピュータにログオンします。
2. タスクトレイの [ウイルスバスター Corp. クライアント] アイコンを右クリックして、[ウイルスバスター Corp. のアンロード] を選択します。パスワードの入力を要求されたら、アンロードパスワードを指定して [OK] をクリックします。

注意： クライアントがアンロードされるコンピュータで、パスワードを無効にします。詳細については、283 ページの「クライアントの権限とその他の設定」を参照してください。

3. アンロードパスワードを指定しなかった場合は、Microsoft 管理コンソールから以下のサービスを停止します。
 - OfficeScan NT Listener
 - OfficeScan NT Firewall
 - OfficeScanNT RealTime Scan
 - OfficeScan NT Proxy Service
 - Trend Micro Unauthorized Change Prevention Service (コンピュータが x86 タイプのプラットフォームを実行している場合)
4. [スタート] → [プログラム] の順にクリックし、[ウイルスバスター Corp. クライアント] を右クリックして [削除] をクリックします。
5. レジストリエディタ (regedit.exe) を開きます。

警告： 次の手順ではレジストリキーの削除が必要です。レジストリキーを正しく変更しないと、システムに重大な問題が生じる可能性があります。常にバックアップコピーを作成してからレジストリキーを変更してください。詳細については、レジストリエディタのヘルプを参照してください。

6. 次のレジストリキーを削除します。
コンピュータに他のトレンドマイクロ製品がインストールされていない場合：
 - HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro

64 ビットコンピュータの場合：

HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432node¥Trend Micro

コンピュータに他のトレンドマイクロ製品がインストールされている場合は、以下のキーのみを削除します。

- HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥NSC
- HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥OfcWatchDog

64 ビットコンピュータの場合：

HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432node¥Trend Micro¥OfcWatchDog

- HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥PC-cillinNTCorp

64 ビットコンピュータの場合：

HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432node¥Trend Micro¥PC-cillinNTCorp

7. 次のレジストリキー / 値を削除します。

- HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Uninstall¥OfficeScanNT
- HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run の OfficeScanNT Monitor (REG_SZ)

8. 次の位置にある下記のレジストリキーのインスタンスをすべて削除します。

位置：

- HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services
- HKEY_LOCAL_MACHINE¥SYSTEM¥ControlSet001¥Services
- HKEY_LOCAL_MACHINE¥SYSTEM¥ControlSet002¥Services
- HKEY_LOCAL_MACHINE¥SYSTEM¥ControlSet003¥Services

キー：

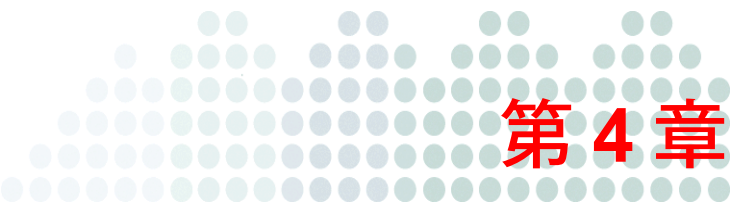
- ntrtscan
- tmcfw
- tmcomm
- TmFilter
- Tmlisten
- tmpfw
- TmPreFilter
- TmProxy

- tmtdi
 - VSApiNt
 - tmlwf (Windows Vista/2008 コンピュータの場合)
 - tmwfp (Windows Vista/2008 コンピュータの場合)
 - tmactmon
 - TMBMServer
 - tmevtmgr
9. レジストリエディタを終了します。
10. [スタート] → [設定] → [コントロール パネル] の順にクリックし、[システム] をダブルクリックします。
11. [ハードウェア] タブをクリックし、[デバイス マネージャ] をクリックします。
12. [表示] → [非表示のデバイスの表示] の順にクリックします。
13. [プラグ アンド プレイではないドライバ] を展開し、次のデバイスをアンインストールします。
- tmcomm
 - tmactmon
 - tmevtmgr
 - Trend Micro Filter
 - Trend Micro PreFilter
 - Trend Micro TDI Driver
 - Trend Micro VSAPI NT
 - Trend Micro Unauthorized Change Prevention Service
 - Trend Micro WFP Callout Driver (Windows Vista/2008 コンピュータの場合)
14. ファイアウォールドライバをアンインストールします。
- a. [マイ ネットワーク] を右クリックして、[プロパティ] をクリックします。
 - b. [ローカル エリア接続] を右クリックして、[プロパティ] をクリックします。
 - c. [全般] タブで [Trend Micro Common Firewall Driver] を選択し、[アンインストール] をクリックします。

Windows Vista コンピュータで、次の操作を実行します。

- a. [ネットワーク] を右クリックして、[プロパティ] をクリックします。
- b. [ネットワーク接続の管理] をクリックします。
- c. [ローカル エリア接続] を右クリックして、[プロパティ] をクリックします。

- d. [ネットワーク] タブで [Trend Micro NDIS 6.0 Filter Driver] を選択し、[アンインストール] をクリックします。
15. クライアントコンピュータを再起動します。
16. コンピュータに他のトレンドマイクロ製品がインストールされていない場合は、Trend Micro インストールフォルダ (通常 C:\Program Files¥Trend Micro) を削除します。64 ビットコンピュータの場合、インストールフォルダは C:\Program Files (x86)\Trend Micro の下にあります。
17. 他のトレンドマイクロ製品がインストールされている場合は、次のフォルダを削除します。
 - <「クライアントのインストールフォルダ」>
 - Trend Micro インストールフォルダの下に BM フォルダ (通常 C:\Program Files ¥Trend Micro¥BM)



第4章

最新の保護状態の維持

この章で説明する内容には、次の項目が含まれます。

- 118 ページの「トレンドマイクロ ウイルスバスター コーポレートエディションのコンポーネントとプログラム」
- 126 ページの「アップデートの概要」
- 129 ページの「ウイルスバスター Corp. サーバのアップデート」
- 137 ページの「スマートスキャンサーバのアップデート」
- 139 ページの「クライアントアップデート」
- 153 ページの「アップデートエージェント」
- 158 ページの「コンポーネントアップデートの概要」

トレンドマイクロ ウイルスバスター コーポレートエディションのコンポーネントとプログラム

トレンドマイクロ ウイルスバスター コーポレートエディション（以下、ウイルスバスター Corp.）では、最新のセキュリティリスクからクライアントコンピュータを保護するために、さまざまなコンポーネントとプログラムを使用しています。これらのコンポーネントとプログラムを最新状態に保つには、手動アップデートまたは予約アップデートを実行します。

ウイルスバスター Corp. クライアントでは、コンポーネントだけでなく、アップデートされた設定ファイルをウイルスバスター Corp. サーバから受け取ります。クライアントは、新しい設定を適用するために設定ファイルが必要になります。Web コンソールを使用してウイルスバスター Corp. 設定を変更するたびに、設定ファイルが変更されます。

コンポーネントは、次のグループに分けられます。

- 「ウイルス対策コンポーネント」
- 「ダメージクリーンナップサービスコンポーネント」
- 「スパイウェア対策コンポーネント」
- 「ファイアウォールコンポーネント」
- 「Web レピュテーションコンポーネント」
- 「挙動監視コンポーネント」
- 「プログラム」

ウイルス対策コンポーネント

ウイルスパターンファイル

クライアントコンピュータで使用可能なウイルスパターンファイルは、クライアントで使用されている検索方法によって異なります。検索方法の詳細については、165 ページの「検索方法」を参照してください。

従来型スキャン

従来型スキャンで使用されているパターンファイルは、ウイルスパターンファイルと呼ばれ、ウイルスバスター Corp. が最新のウイルス / 不正プログラムおよび複合型の脅威の攻撃を特定するために利用する情報が含まれています。トレンドマイクロは、1 週間に数回、および有害なウイルス / 不正プログラムが発見されたときに、新しいバージョンのウイルスパターンファイルを作成および公開しています。

ヒント： 少なくとも 1 週間に 1 回、自動アップデートを実行するようスケジュールを設定することをお勧めします。これは、すべての製品の初期設定です。

ウイルスパターンファイルおよびその他のウイルスバスター Corp. のパターンファイルは、次の Web サイトで確認します。このサイトでは、最新のバージョン、リリース日、新たに対応されたウイルスのリストを確認できます。

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

スマートスキャン

スマートスキャンモードでは、ウイルスバスター Corp. クライアントが、連携して動作する 2 つの軽量のパターンファイルを利用して、従来の不正プログラム対策およびスパイウェア対策パターンファイルと同等のセキュリティ対策を提供します。

スマートスキャンサーバは**スマートスキャンパターン**を保持します。このパターンファイルは毎時間アップデートされ、パターン定義の大部分が含まれます。スマートスキャンクライアントでは、このパターンファイルはダウンロードされません。クライアントでは、スマートスキャンサーバに検索クエリを送信し、潜在的脅威が検証されます。

クライアントのアップデート元（ウイルスバスター Corp. サーバまたはユーザ指定アップデート元）は、**スマートスキャンエージェントパターン**を保持します。このスマートスキャンパターンは毎日アップデートされ、スマートスキャンパターンにないその他のすべてのパターン定義がすべて含まれます。クライアントは、他のウイルスバスター Corp. コンポーネントの場合と同じ方法で、アップデート元からこのパターンファイルをダウンロードします。

ウイルスバスター Corp. クライアントでは、スマートスキャンエージェントパターンおよび高度なフィルタテクノロジーを使用して、スマートスキャンサーバに検索クエリを送信することなく、ファイルが感染しているかどうかを確認できます。クライアントは、検索時にファイルの危険性を判定できない場合にのみ検索クエリを送信します。クライアントは、ファイルの危険性をローカルで検証できず、数回試行してもスマートスキャンサーバに接続できない場合は、次の処理を実行します。

- ・ 検証するファイルにフラグを付ける
- ・ ファイルへの一時アクセスを許可する

スマートスキャンサーバへの接続が回復すると、フラグが付けられたすべてのファイルが再検索されます。感染していることが確認されたファイルに、適切な検出時の処理が実行されます。

ウイルス検索エンジン

すべてのトレンドマイクロ製品は、検索エンジンを中心に構成されています。当初、検索エンジンは、初歩的なファイルベースのコンピュータウイルスに対応するために開発されました。今日の検索エンジンは、飛躍的に高度化され、さまざまな種類のウイルスと不正プログラムを検出する能力があります。また、調査用に開発され使用されている管理ウイルスも検出します。

全ファイルの全バイトを検索するのではなく、次の項目を識別するためにエンジンとパターンファイルが連携します。

- ・ ウイルスコードを示唆する特性
- ・ ウイルスが存在するファイル内の正確な場所

ウイルスバスター Corp. は、ウイルス / 不正プログラムを検出すると設定に基づき処理を行います。

トレンドマイクロの検索エンジンは、ICSA (International Computer Security Association) などの国際的なコンピュータセキュリティ機関で、認定を毎年取得しています。

検索エンジンのアップデート

ウイルスパターンファイルに最も新しいウイルス / 不正プログラムの情報を格納することで、セキュリティ対策の状態を最新に維持しながら、検索エンジンのアップデート数を最小限にとどめています。それにもかかわらず、定期的に新しい検索エンジンのバージョンが使用可能になります。トレンドマイクロは、次の状況で新しいエンジンを公開します。

- ・ ソフトウェアへの新しい検索および検出テクノロジーの導入
- ・ 検索エンジンで処理できない、潜在的に有害な新しいウイルス / 不正プログラムの発見
- ・ 検索パフォーマンスの向上
- ・ ファイル形式、スクリプト言語、エンコード、または圧縮形式の追加

ウイルス検索ドライバ

ウイルス検索ドライバは、ファイルに対するユーザ操作を監視します。ファイルを開いたり閉じたりする操作やアプリケーションを実行する操作などが対象となります。このドライバには 3 つのバージョンがあります。バージョンの 1 つは Windows 2000 用で、ファイル名は TmFilter.sys です。他の 2 つのバージョンは、TmXPFlt.sys と TmPreFlt.sys で、Windows 2000 以外の OS 用です。TmXPFlt.sys は、ウイルス検索エンジンのリアルタイム設定に使用し、TmPreFlt.sys はユーザ操作の監視に使用します。

注意： このコンポーネントは、コンソールには表示されません。そのバージョンを確認するには、
<「サーバのインストールフォルダ」>¥PCCSRV¥Pccnt¥Drv に移動します。.sys ファイルを右クリックして、[プロパティ] を選択し、[バージョン情報] タブを選択します。

IntelliTrap パターンファイル

「IntelliTrap」パターンファイルは、実行可能ファイルとしてパックされたリアルタイム圧縮ファイルを検出します。

IntelliTrap 除外パターンファイル

IntelliTrap 除外パターンファイルには、「承諾済み」の圧縮ファイルリストが含まれています。

ダメージクリーンナップサービスコンポーネント

ウイルスクリーンナップエンジン

ウイルスクリーンナップエンジンは、トロイの木馬とそのプロセスを検索し、削除します。このエンジンでは、32 ビットと 64 ビットのプラットフォームがサポートされています。

ウイルスクリーンナップテンプレート

ウイルスクリーンナップテンプレートは、ウイルスクリーンナップエンジンで、トロイの木馬とそのプロセスを認識し除去するために使用されます。

スパイウェア対策コンポーネント

スパイウェアパターンファイル

スパイウェアパターンファイルは、ファイルやプログラム、メモリのモジュール、Windows レジストリ、URL ショートカットなどにあるスパイウェア / グレーウェアを認識します。

スパイウェア検索エンジン

スパイウェア検索エンジンは、スパイウェア / グレーウェアを検出し、適切な検索時の処理を実行します。このエンジンでは、32 ビットと 64 ビットのプラットフォームがサポートされています。

スパイウェア監視パターンファイル

スパイウェア監視パターンファイルは、リアルタイムスパイウェア / グレーウェア検索に使用されます。このパターンファイルは従来型スキャンクライアントのみが使用します。

スマートスキャンクライアントは、スマートスキャンエージェントパターンをリアルタイムスパイウェア / グレーウェア検索に使用します。クライアントが検索時に検索対象の危険性を判定できない場合には、スマートスキャンサーバに検索クエリを送信します。

ファイアウォールコンポーネント

ファイアウォールドライバ

ファイアウォールドライバは、ファイアウォールパターンファイルとともに、クライアントコンピュータのネットワークウイルスを検索するために使用されます。このドライバでは、32 ビットと 64 ビットのプラットフォームがサポートされています。

ファイアウォールパターンファイル

ファイアウォールパターンファイルは、ウイルスパターンファイルと同様に、ウイルスバスター Corp. がウイルスの兆候や存在を示す独特のビットやバイトのパターンを認識するために使用されます。

Web レピュテーションコンポーネント

URL フィルタエンジン

URL フィルタエンジンは、ウイルスバスター Corp. とトレンドマイクロ URL フィルタリングサービスの間の通信を助けます。URL フィルタリングサービスは、URL を格付けし、格付け情報をウイルスバスター Corp. に提供するシステムです。

挙動監視コンポーネント

挙動監視ドライバ

このカーネルモードドライバは、システムイベントを監視し、ポリシー施行のために挙動監視コアサービスにシステムイベントを渡します。

挙動監視コアサービス

このユーザモードサービスには次の機能があります。

- ルートキット検出の提供
- 外部デバイスへのアクセスの規制
- ファイル、レジストリキー、およびサービスの保護

挙動監視設定パターンファイル

挙動監視ドライバは、通常のシステムイベントを識別し、ポリシー施行から除外するためにこのパターンファイルを使用します。

デジタル署名パターンファイル

このパターンファイルには、有効なデジタル署名のリストが含まれており、システムイベントを処理するプログラムが安全かどうか判定するために挙動監視コアサービスによって使用されます。

ポリシー施行パターンファイル

挙動監視コアサービスは、このパターンファイル内のポリシーと照合して、システムイベントを確認します。

プログラム

クライアントプログラム

ウイルスバスター Corp. クライアントプログラムは、セキュリティリスクからの実際の保護を提供します。

Cisco Trust Agent

Cisco Trust Agent は、クライアントと Cisco NAC をサポートするルータとの通信を可能にします。このエージェントは、Policy Server for Cisco NAC をインストールしている場合にのみ機能します。

Hot Fix、Patch、および Service Pack

トレンドマイクロは、正式な製品リリースの後で、問題への対応、製品パフォーマンスの向上、新しい機能の追加のために次のアイテムを開発することが多くあります。

- 「HotFix」
- 「Patch」
- 「Security Patch」
- 「Service Pack」

これらのアイテムが準備されたときには、サポートセンターより連絡があります。新しい HotFix、Patch、および Service Pack のリリースについては、次のトレンドマイクロの Web サイトを確認してください。

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

すべてのリリースには、インストール、配信、および設定についての情報を含む Readme が添付されています。インストールを実行する前に、Readme ファイルをよくお読みください。

HotFix と Patch の履歴

ウイルスバスター Corp. サーバが HotFix や Patch ファイルをウイルスバスター Corp. クライアントに配信するときに、クライアントプログラムでは、レジストリエディタに HotFix と Patch に関する情報が記録されます。Microsoft SMS、LANDesk、BigFix などのロジスティクスソフトウェアを使用して、複数のクライアントに対してこの情報をクエリできます。

注意： この機能では、サーバにのみ配信された HotFix や Patch は記録されません。

この機能は、ウイルスバスター Corp. 8.0 Service Pack 1 Patch 3.1 から使用可能です。

- 8.0 Service Pack 1 Patch 3 以降のバージョンからアップグレードされたクライアントでは、バージョン 8 と 10 のインストール済みの HotFix と Patch が記録されます。
- 8.0 Service Pack 1 Patch 3 より前のバージョンからアップグレードされたクライアントでは、バージョン 10 のみのインストール済みの HotFix と Patch が記録されます。

情報は、次のキーに格納されます。

- HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥PC-cillinNTCorp¥CurrentVersion¥HotfixHistory¥< 製品バージョン >
- x64 タイプのプラットフォームを実行するコンピュータの場合：
HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥TrendMicro¥PC-cillinNTCorp¥CurrentVersion¥HotfixHistory¥< 製品バージョン >

次のキーを確認してください。

- キー : HotFix_installed
種類 : REG_SZ
値 : <HotFix または Patch 名 >
- キー : HotfixInstalledNum
種類 : DWORD
値 : <HotFix または Patch 番号 >

アップデートの概要

すべてのコンポーネントのアップデートは、トレンドマイクロのアップデートサーバから取得されます。新しいコンポーネントが入手可能になると、ウイルスバスター Corp. サーバおよびスマートスキャンサーバ（ローカルまたはグローバル）は、アップデートされたコンポーネントをダウンロードします。2つのサーバの間でダウンロードするコンポーネントが重複することはありません。これは、それぞれのサーバが固有のコンポーネントセットをダウンロードするためです。

注意： ウイルスバスター Corp. サーバとスマートスキャンサーバは両方とも、トレンドマイクロのアップデートサーバ以外のアップデート元からアップデートするように設定できます。これを行うには、ユーザ指定のアップデート元を設定する必要があります。アップデート元の設定について支援が必要な場合には、サポートセンターまでお問い合わせください。

ウイルスバスター Corp. サーバとクライアントのアップデート

ウイルスバスター Corp. サーバは、クライアントに必要な大半のコンポーネントをダウンロードします。ダウンロードしない唯一のコンポーネントは、スマートスキャンサーバによってダウンロードされるスマートスキャンパターンです。

ウイルスバスター Corp. サーバが多数のクライアントを管理している場合、アップデートに大量のサーバコンピュータリソースが使用される場合があります、サーバの安定性とパフォーマンスに影響する可能性があります。この問題に対応するために、ウイルスバスター Corp. にはアップデートエージェント機能が用意されています。この機能により、特定の複数のクライアントが、他のクライアントにアップデートを配信するタスクを共有することができます。

次の表は、ウイルスバスター Corp. サーバおよびクライアントに対するさまざまなコンポーネントアップデートのオプションと、これらを使用する際の推奨事項について説明しています。

表 4-1. サーバとクライアントのアップデートオプション

アップデートオプション	説明	推奨事項
トレンドマイクロ のアップデート サーバ ↓ ウイルスバスター Corp. サーバ ↓ クライアント	ウイルスバスター Corp. サーバは、アップデートされたコンポーネントをトレンドマイクロのアップデートサーバ (またはその他のアップデート元) から受信し、クライアントでコンポーネントのアップデートを開始します。	ウイルスバスター Corp. サーバとクライアントの間に低帯域幅のセグメントがない場合、この方法を使用します。
トレンドマイクロ のアップデート サーバ ↓ ウイルスバスター Corp. サーバ ↓ アップデートエー ジェント ↓ クライアント	ウイルスバスター Corp. サーバが、アップデートされたコンポーネントをトレンドマイクロのアップデートサーバ (またはその他のアップデート元) から受信し、クライアントでコンポーネントのアップデートを開始します。次に、アップデートエージェントとして機能するクライアントが、クライアントにコンポーネントをアップデートするように通知します。	ウイルスバスター Corp. サーバとクライアントの間に低帯域幅のセグメントがある場合、ネットワークのトラフィック負荷を分散するためにこの方法を使用します。
トレンドマイクロ のアップデート サーバ ↓ アップデートエー ジェント ↓ クライアント	アップデートエージェントが、アップデートされたコンポーネントをトレンドマイクロのアップデートサーバ (またはその他のアップデート元) から直接受信し、クライアントにコンポーネントをアップデートするように通知します。	アップデートエージェントをウイルスバスター Corp. サーバまたは他のアップデートエージェントからアップデートする際に問題が発生する場合にのみ、この方法を使用します。ほとんどの環境では、アップデートエージェントは、外部のアップデート元からよりも、ウイルスバスター Corp. サーバまたは他のアップデートエージェントからの方がアップデートを速く受信できます。

表 4-1. サーバとクライアントのアップデートオプション (続き)

アップデートオプション	説明	推奨事項
トレンドマイクロ のアップデート サーバ ↓ クライアント	ウイルスバスター Corp. クライアントが、アップデートされたコンポーネントをトレンドマイクロのアップデートサーバ (またはその他のアップデート元) から直接受信します。	クライアントをウイルスバスター Corp. サーバまたはアップデートエージェントからアップデートする際に問題が発生する場合にのみ、この方法を使用します。 ほとんどの環境では、クライアントは、外部のアップデート元からよりも、ウイルスバスター Corp. サーバまたはアップデートエージェントからの方がアップデートを速く受信できます。

スマートスキャンサーバのアップデート

スマートスキャンサーバが、スマートスキャンパターンをダウンロードします。スマートスキャンクライアントでは、このパターンファイルをダウンロードしません。クライアントでは、スマートスキャンサーバに検索クエリを送信し、潜在的脅威が検証されます。

注意： スマートスキャンサーバの詳細については、34 ページの「スマートスキャンサーバ」を参照してください。また、サーバのアップデートの詳細については、137 ページの「スマートスキャンサーバのアップデート」を参照してください。

次の表は、スマートスキャンサーバのアップデート処理について説明しています。

表 4-2. スマートスキャンサーバのアップデート処理

アップデート処理	説明
トレンドマイクロのアップデートサーバ ↓ グローバルスマートスキャンサーバ	グローバルスマートスキャンサーバは、トレンドマイクロのアップデートサーバからアップデートを受信します。企業ネットワークに接続されていないスマートスキャンクライアントは、グローバルスマートスキャンサーバに検索クエリを送信します。

表 4-2. スマートスキャンサーバのアップデート処理 (続き)

アップデート処理	説明
トレンドマイクロのアップ デートサーバ ↓ ローカルスマートスキャン サーバ	ローカルスマートスキャンサーバ (統合またはスタンドアロン) は、トレンドマイクロのアップデートサーバからアップデートを受信します。企業ネットワークに接続されているスマートスキャンクライアントは、ローカルスマートスキャンサーバに検索クエリを送信します。

ウイルスバスター Corp. サーバのアップデート

ウイルスバスター Corp. サーバは、次のコンポーネントをダウンロードして、クライアントに配信します。

表 4-3. ウイルスバスター Corp. サーバがダウンロード可能なコンポーネント

コンポーネント	配信	
	従来型スキャン クライアント	スマートスキャン クライアント
スマートスキャンエージェントパターン	不可	可
ウイルスパターンファイル	可	不可
ウイルス検索エンジン	可	可
ウイルス検索ドライバ	可	可
IntelliTrap パターンファイル	可	可
IntelliTrap 除外パターンファイル	可	可
ウイルススクリーンナップエンジン	可	可
ウイルススクリーンナップテンプレート	可	可
スパイウェアパターンファイル	可	可
スパイウェア検索エンジン	可	可
スパイウェア監視パターンファイル	可	不可

表 4-3. ウイルスバスター Corp. サーバがダウンロード可能なコンポーネント (続き)

コンポーネント	配信	
	従来型スキャン クライアント	スマートスキャン クライアント
ファイアウォールドライバ	可	可
ファイアウォールパターンファイル	可	可
URL フィルタエンジン	可	可
挙動監視ドライバ	可	可
挙動監視コアサービス	可	可
挙動監視設定パターンファイル	可	可
デジタル署名パターンファイル	可	可
ポリシー施行パターンファイル	可	可

サーバがアップデートされたコンポーネントをクライアントに配信できるようにするには、自動アップデート設定を行います。自動アップデートが無効の場合でも、サーバはアップデートをダウンロードしますが、クライアントに配信することはありません。詳細については、143 ページの「自動アップデート」を参照してください。

Web コンソールの [概要] 画面で最新バージョンのコンポーネントを参照して、コンポーネントがアップデートされているクライアントの数と、古いままのクライアントの数を確認します。

トレンドマイクロでは、定期的にパターンファイルをリリースして、クライアントの保護を最新状態に維持しています。パターンファイルのアップデートは定期的に入手可能になるので、ウイルスバスター Corp. ではコンポーネントの複製というメカニズムを使用して、パターンファイルの高速なダウンロードを実現しています。詳細については、132 ページの「サーバコンポーネントの複製」を参照してください。

プロキシサーバを使用してインターネットに接続している場合、アップデートを正常にダウンロードするように正しいプロキシ設定を使用してください。

サーバアップデート元

トレンドマイクロのアップデートサーバまたは他のアップデート元からコンポーネントをダウンロードするように、ウイルスバスター Corp. サーバを設定します。

サーバは、使用可能なアップデートをダウンロードすると、[アップデート] → [ネットワーク上のコンピュータ] → [自動アップデート] で指定された設定に基づいて、クライアントにコンポーネントをアップデートするように自動的に通知できます。コンポーネントのアップデートが重要な場合は、[アップデート] → [ネットワーク上のコンピュータ] → [手動アップデート] に進んで、クライアントに一度に通知するようにサーバを設定できます。

注意： [アップデート] → [ネットワーク上のコンピュータ] → [自動アップデート] で、配信スケジュールや、イベント起動配信の設定を指定していない場合には、サーバがアップデートをダウンロードしても、クライアントへのアップデートの通知は実行されません。

サーバのアップデート元を設定するには

パス：[アップデート]→[サーバ]→[アップデート元]

1. コンポーネントのアップデートのダウンロード元になる場所を選択します。

トレンドマイクロのアップデートサーバを選択する場合は、サーバがインターネットに接続されていることを確認し、プロキシサーバを使用している場合は、プロキシ設定を使用してインターネット接続が可能かどうかをテストしてください。詳細については、132 ページの「サーバアップデートのプロキシ」を参照してください。

ユーザ指定のアップデート元を選択する場合は、適切な環境を設定して、このアップデート元のリソースをアップデートしてください。また、サーバコンピュータとこのアップデート元との接続が機能することも確認してください。アップデート元の設定について支援が必要な場合には、サポートセンターまでお問い合わせください。

注意： ウイルスバスター Corp. サーバは、アップデート元からコンポーネントをダウンロードするときに、コンポーネントの複製を使用します。詳細については、132 ページの「サーバコンポーネントの複製」を参照してください。

2. [保存] をクリックします。

サーバアップデートのプロキシ

トレンドマイクロのアップデートサーバからアップデートをダウンロードするときにプロキシ設定を使用するように、サーバコンピュータでホストされたサーバプログラムを設定します。サーバプログラムには、ウイルスバスター Corp. サーバと統合スマートスキャンサーバがあります。

プロキシ設定を行うには

パス: [管理] → [プロキシ設定] → [外部プロキシ] タブ

1. [ウイルスバスター Corp. サーバコンピュータのアップデート] セクションで、プロキシサーバの使用を有効にするチェックボックスをオンにします。
2. プロキシプロトコル、サーバの名前または IP アドレス、およびポート番号を指定します。
3. プロキシサーバに認証が必要な場合、所定のフィールドにユーザ名とパスワードを入力します。
4. [保存] をクリックします。

サーバコンポーネントの複製

トレンドマイクロのアップデートサーバからのダウンロード用に、最新バージョンの完全なパターンファイルが入手可能になったときには、14 個の「差分パターンファイル」も入手可能になります。差分パターンファイルは、完全なパターンファイルよりもサイズが小さなバージョンで、以前の完全なパターンファイルと最新バージョンの差分に相当します。たとえば、最新バージョンが 175 の場合、差分パターンファイル v_173.175 には、バージョン 173 に存在しないバージョン 175 のシグネチャが含まれています。パターンファイル番号は 2 ずつ増やされるため、バージョン 173 は前の完全なパターンファイルのバージョンです。差分パターンファイル v_171.175 には、バージョン 171 に存在しないバージョン 175 のシグネチャが含まれています。

ウイルスバスター Corp. では、最新パターンファイルをダウンロードするときに生じるネットワークトラフィックを軽減するために、コンポーネントの複製が実行されます。これは、ウイルスバスター Corp. サーバまたはアップデートエージェントが差分パターンファイルのみをダウンロードするコンポーネントのアップデート方法です。アップデートエージェントがコンポーネントの複製を実行する方法については、157 ページの「アップデートエージェントのコンポーネントの複製」を参照してください。

コンポーネントの複製は、次のコンポーネントに適用されます。

- ウイルスパターンファイル
- スマートスキャンエージェントパターン
- ウイルスクリーンナップテンプレート
- IntelliTrap 除外パターンファイル

- スパイウェアパターンファイル
- スパイウェア監視パターンファイル

コンポーネントの複製のシナリオ

サーバのコンポーネントの複製については、次のシナリオを参照してください。

表 4.4. サーバコンポーネントの複製のシナリオ

ウイルスバスター Corp. サーバの完全なパターンファイル	現在のバージョン: 171 利用可能なその他のバージョン: 169 167 165 163 161 159					
トレンドマイクロのアップデートサーバの最新バージョン	173.175	171.175	169.175	167.175	165.175	
	163.175	161.175	159.175	157.175	155.175	
	153.175	151.175	149.175	147.175		

1. ウイルスバスター Corp. サーバは、現在の完全なパターンファイルのバージョンと、トレンドマイクロのアップデートサーバの最新バージョンを比較します。2つのバージョンの差が 14 以下の場合、サーバは、2つのバージョンの差分に相当する差分パターンファイルのみをダウンロードします。

注意： 差が 14 を超える場合、サーバは自動的にパターンファイルの完全なバージョンと、14 個の差分パターンファイルをダウンロードします。

実際の例では次のようになります。

- バージョン 171 と 175 の差は 2 です。つまり、サーバにはバージョン 173 と 175 がありません。
 - このサーバは、差分パターンファイル 171.175 をダウンロードします。この差分パターンファイルは、バージョン 171 と 175 の差分に相当します。
2. サーバで差分パターンファイルと現在の完全なパターンファイルが結合されて、最新の完全なパターンファイルが生成されます。

実際の例では次のようになります。

- サーバで、ウイルスバスター Corp. がバージョン 171 と差分パターンファイル 171.175 を結合して、バージョン 175 を生成します。
- このサーバには、1つの差分パターンファイル (171.175) と、最新の完全なパターンファイル (バージョン 175) が存在します。

3. サーバでは、サーバ上にある他の完全なパターンファイルに基づいて、差分パターンファイルが生成されます。サーバがこれらの差分パターンファイルを生成しない場合、以前の差分パターンファイルをダウンロードできなかったクライアントは、自動的に完全なパターンファイルをダウンロードします。これにより、ネットワークトラフィックが増加します。

実際の例では次のようになります。

- サーバには、169、167、165、163、161、159 のパターンファイルバージョンがあるため、次の差分パターンファイルを生成できます。

169.175 167.175 165.175 163.175 161.175 159.175

- このサーバには差分パターンファイル 171.175 がすでにあるため、バージョン 171 を使用する必要はありません。
- 現在サーバには、次の 7 つの差分パターンファイルが存在します。

171.175 169.175 167.175 165.175 163.175 161.175 159.175

- このサーバでは、最近の 7 つの完全なパターンファイルバージョン (バージョン 175、171、169、165、163、161) が保持されます。これよりも古いバージョン (バージョン 159) は削除されます。

4. サーバで、現在の差分パターンファイルと、トレンドマイクロのアップデートサーバにある差分パターンファイルが比較されます。サーバにない、差分パターンファイルがダウンロードされます。

実際の例では次のようになります。

- トレンドマイクロのアップデートサーバには、次の 14 個の差分パターンファイルが存在します。

173.175 171.175 169.175 167.175 165.175 163.175 161.175

159.175 157.175 155.175 153.175 151.175 149.175 147.175

- ウイルスバスター Corp. サーバには、次の 7 つの差分パターンファイルが存在します。
- ウイルスバスター Corp. サーバは、追加として次の 7 つの差分パターンファイルをダウンロードします。

171.175 169.175 167.175 165.175 163.175 161.175 159.175

173.175 157.175 155.175 153.175 151.175 149.175 147.175

- これで、トレンドマイクロのアップデートサーバにあるすべての差分パターンファイルが、このサーバに存在することになります。

5. 最新の完全なパターンファイルと 14 個の差分パターンファイルが、クライアントから使用可能になります。

サーバのアップデート方法

ウイルスバスター Corp. サーバのコンポーネントのアップデートは、手動で行うか、またはアップデートスケジュールを設定することによって行います。

サーバがアップデートされたコンポーネントをクライアントに配信できるようにするには、自動アップデート設定を行います。自動アップデートが無効の場合でも、サーバはアップデートをダウンロードしますが、クライアントに配信することはありません。詳細については、143 ページの「自動アップデート」を参照してください。

手動アップデート

重要なアップデートがある場合には、手動アップデートを実行することによりサーバでただちにアップデートを取得できます。詳細については、135 ページの「手動アップデート」を参照してください。

予約アップデート

ウイルスバスター Corp. サーバは、予約された日時にアップデート元に接続して、最新のコンポーネントを取得します。詳細については、135 ページの「予約アップデート」を参照してください。

予約アップデート

定期的にアップデート元をチェックして、利用可能なアップデートを自動的にダウンロードするように、ウイルスバスター Corp. サーバを設定します。クライアントは通常、サーバからアップデートを取得するため、予約アップデートを使用することは、セキュリティリスクに対する保護を常に最新に維持する簡単かつ効率的な方法となります。

サーバのアップデートスケジュールを設定するには

パス: [アップデート] → [サーバ] → [予約アップデート]

1. [ウイルスバスター Corp. サーバの予約アップデートを有効にする] を選択します。
2. アップデート対象コンポーネントを選択します。
3. アップデートスケジュールを指定します。毎日、毎週、毎月のアップデートの場合、ウイルスバスター Corp. がアップデートを実行する期間を時間単位で指定します。ウイルスバスター Corp. は、この期間の任意の時間に更新します。
4. [保存] をクリックします。

手動アップデート

サーバをインストールまたはアップグレードした後、および大規模感染が発生したときには、ウイルスバスター Corp. サーバでコンポーネントを手動でアップデートします。

サーバを手動でアップデートするには

パス: [アップデート]→[サーバ]→[手動アップデート]

Web コンソールのメインメニューで、[サーバアップデート]をクリックします。

1. アップデート対象コンポーネントを選択します。
2. [アップデート]をクリックします。サーバがアップデートされたコンポーネントをダウンロードします。

サーバアップデートログ

特定のコンポーネントをアップデートする際に問題が発生するかどうかを判断するには、サーバアップデートログを確認します。ログには、ウイルスバスター Corp. サーバのコンポーネントのアップデートについて記録されています。

ハードディスク上の領域を大量に占有しないようにログのサイズを維持するには、手動でログを削除するか、またはログの削除スケジュールを設定します。ログの管理方法の詳細については、265 ページの「ログの管理」を参照してください。

サーバアップデートログを表示するには

パス: [ログ]→[サーバアップデートログ]

1. [結果] 列で、アップデートされていないコンポーネントがあるかどうかを確認します。
2. ログを CSV ファイルに保存するには、[CSV 形式でエクスポート] をクリックします。ファイルを開くか、特定の場所に保存します。CSV ファイルは、通常、Microsoft Excel などのスプレッドシートアプリケーションで開きます。

スマートスキャンサーバのアップデート

このセクションでは、統合スマートスキャンサーバでコンポーネントをアップデートする方法について説明します。スタンドアロンサーバでコンポーネントをアップデートする方法の詳細については、ウイルスバスター Corp. 用スマートスキャン クイックスタートガイドを参照してください。

スマートスキャンサーバは、スマートスキャンパターンをダウンロードします。クライアントでは、スマートスキャンサーバに検索クエリを送信し、潜在的脅威が検証されます。クライアントは、スマートスキャンパターンをダウンロードしません。

注意： スマートスキャンソリューションでは、他にもスマートスキャンエージェントパターンというパターンファイルが使用されます。このパターンファイルは、クライアントのアップデート元（ウイルスバスター Corp. サーバまたはユーザ指定アップデート元）でホストされており、クライアントによってダウンロードされます。

トレンドマイクロでは、スマートスキャンパターンを 1 時間ごとにアップデートしています。ウイルスバスター Corp. サーバと同様に、スマートスキャンサーバでもコンポーネントの複製というメカニズムを使用して、パターンファイルの高速なダウンロードを実現しています。詳細については、132 ページの「サーバコンポーネントの複製」を参照してください。

サーバのアップデート設定

トレンドマイクロのアップデートサーバまたは他のアップデート元からスマートスキャンパターンをダウンロードするように、スマートスキャンサーバを設定します。手動でパターンファイルをアップデートするか、アップデートスケジュールを設定します。

サーバのアップデート設定を行うには

パス：[スマートスキャン]→[統合サーバ]

1. 統合スマートスキャンサーバを使用するように選択します。このチェックボックスをオンにしない場合には次のようになります。
 - Trend Micro Smart Scan Server サービス (iCRCSERVICE.exe) が停止します。
 - 統合サーバが、トレンドマイクロのアップデートサーバからのコンポーネントのアップデートを停止します。
 - クライアントが、統合サーバに検索クエリを送信できなくなります。
2. スマートスキャンサーバリストを設定するときには、[サーバアドレス] の情報を使用します。リストの詳細については、172 ページの「スマートスキャンソース」を参照してください。

クライアントは、HTTP および HTTPS プロトコルを使用して、統合サーバに接続できます。HTTPS ではより安全な接続が可能ですが、HTTP では消費される帯域幅が少なくなります。クライアントが特定のプロトコルを使用して接続するときには、サーバアドレスを使用して統合サーバを識別します。

ヒント： 別のウイルスバスター Corp. サーバによって管理されるクライアントも、統合サーバに接続することができます。他のウイルスバスター Corp. サーバの Web コンソールで、統合サーバのアドレスをスマートスキャンサーバのリストに追加します。

3. スマートスキャンパターンのバージョンを表示します。スマートスキャンパターンを手動でアップデートするには、[アップデート] をクリックします。画面の上部にアップデートの結果が表示されます。
4. パターンを自動的にアップデートするには、予約アップデートを有効にして、アップデートスケジュールを設定します。
5. コンポーネントのアップデートのダウンロード元になる場所を選択します。

トレンドマイクロのアップデートサーバを選択する場合は、サーバがインターネットに接続されていることを確認し、プロキシサーバを使用している場合は、プロキシ設定を使用してインターネット接続が可能かどうかをテストしてください。詳細については、132 ページの「サーバアップデートのプロキシ」を参照してください。

ユーザ指定のアップデート元を選択する場合は、適切な環境を設定して、このアップデート元のリソースをアップデートしてください。また、サーバコンピュータとこのアップデート元との接続が機能することも確認してください。アップデート元の設定について支援が必要な場合には、サポートセンターまでお問い合わせください。

6. [保存] をクリックします。

クライアントアップデート

最新のセキュリティリスクに対するクライアントの保護状態を維持するには、クライアントのコンポーネントを定期的にアップデートします。クライアントをアップデートする前に、アップデート元に最新のコンポーネントがあるかどうかを確認してください。通常のアップデート元（ウイルスバスター Corp. サーバ）をアップデートする方法については、129 ページの「ウイルスバスター Corp. サーバのアップデート」を参照してください。

次の表は、クライアントがコンピュータに保存するコンポーネントと、特定の検索方法で使用されるコンポーネントをすべて示しています。各コンポーネントのアップデート元は、ウイルスバスター Corp. サーバまたはユーザ指定のアップデート元になります。

注意： スマートスキャンサーバは、スマートスキャンパターンをダウンロードしますが、このパターンがクライアントに配信されることはありません。スマートスキャンパターンは、スマートスキャンクライアントが検索クエリをスマートスキャンサーバに送信するときに使用されます。

表 4-5. クライアントによって保存されるウイルスバスター Corp. のコンポーネント

コンポーネント	使用可否	
	従来型スキャン クライアント	スマートスキャン クライアント
スマートスキャンエージェントパターン	不可	可
ウイルスパターンファイル	可	不可
ウイルス検索エンジン	可	可
ウイルス検索ドライバ	可	可
IntelliTrap パターンファイル	可	可
IntelliTrap 除外パターンファイル	可	可
ウイルスクリーンアップエンジン	可	可
ウイルスクリーンアップテンプレート	可	可

表 4-5. クライアントによって保存されるウイルスバスター Corp. のコンポーネント (続き)

コンポーネント	使用可否	
	従来型スキャン クライアント	スマートスキャン クライアント
スパイウェアパターンファイル	可	可
スパイウェア検索エンジン	可	可
スパイウェア監視パターンファイル	可	不可
ファイアウォールドライバ	可	可
ファイアウォールパターンファイル	可	可
URL フィルタエンジン	可	可
挙動監視ドライバ	可	可
挙動監視コアサービス	可	可
挙動監視設定パターンファイル	可	可
デジタル署名パターンファイル	可	可
ポリシー施行パターンファイル	可	可

ウイルスバスター Corp. サーバおよびユーザ指定のアップデート元からのアップデート

クライアントは、ウイルスバスター Corp. サーバやユーザ指定のアップデート元など、さまざまなアップデート元からアップデートを取得できます。

クライアントのアップデート元を設定するには

パス: [アップデート] → [ネットワーク上のコンピュータ] → [アップデート元]

1. 標準のアップデート元 (ウイルスバスター Corp. サーバ) とユーザ指定アップデート元のどちらからアップデートするかを選択します。
2. [すべてのクライアントへ通知] をクリックします。

ユーザ指定アップデート元

クライアントは、ウイルスバスター Corp. サーバの他に、ユーザ指定のアップデート元からもアップデートできます。ユーザ指定のアップデート元を使用すると、クライアントからウイルスバスター Corp. サーバへのアップデートトラフィックを減らすことができ、ウイルスバスター Corp. サーバに接続できないクライアントでも適切なタイミングでのアップデートが可能になります。[ユーザ指定アップデート元] でユーザ指定のアップデート元を指定します。ここでは、1024 までのアップデート元を指定できます。

ヒント：「アップデートエージェント」としていくつかのクライアントを割り当てて、それらをこの一覧に追加することをお勧めします。

ユーザ指定のアップデート元の一覧を設定するには

パス：[アップデート]→[ネットワーク上のコンピュータ]→[アップデート元]

1. [ユーザ指定アップデート元] を選択して、[追加] をクリックします。
2. 表示された画面で、アップデート元からアップデートを受信するクライアント IP アドレスの範囲を入力します。
3. アップデート元を指定します。アップデートエージェントを選択するか（アップデートエージェントが割り当て済みの場合）、または特定のアップデート元の URL を入力します。
4. [保存] をクリックします。
5. [IP 範囲] のリンクをクリックして、アップデート元を編集します。表示された画面で設定を変更し、[保存] をクリックします。
6. アップデート元をリストから削除するには、そ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。
7. アップデート元を移動するには、上矢印または下矢印をクリックします。一度に移動できるのは 1 つのアップデート元のみです。

リストを設定し保存したら、次のようにアップデート処理が実行されます。

1. クライアントが、リスト上の 1 番目のエントリからアップデートされます。
2. 1 番目のエントリからアップデートできない場合には、2 番目のエントリからアップデートされ、アップデートできない場合には、以下同様の処理が続けられます。
3. すべてのエントリからアップデートできない場合、クライアントは、[利用できるユーザ指定アップデート元が見つからない場合、ウイルスバスター Corp. サーバからアップデートする] オプションが有効かどうかを確認します。有効な場合、クライアントはウイルスバスター Corp. サーバからアップデートされます。

このオプションが無効な場合、次のいずれかの項目に該当するときには、クライアントはトレンドマイクロのアップデートサーバへの直接接続を試行します。

- [ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → [権限とその他の設定] → [その他の設定] タブの [アップデート設定] で、[トレンドマイクロのアップデートサーバからのアップデートの実行] オプションが有効になっている。
 - トレンドマイクロのアップデートサーバ
(<http://osce10-p.activeupdate.trendmicro.co.jp/activeupdate/japan/>) が [ユーザ指定アップデート元] に含まれていない。
4. すべての使用可能なアップデート元からアップデートできない場合、クライアントはアップデート処理を終了します。

標準のアップデート元

ウイルスバスター Corp. サーバは、クライアントの標準のアップデート元です。クライアントをウイルスバスター Corp. サーバから直接アップデートするように設定した場合、アップデート処理は次のように実行されます。

1. クライアントがウイルスバスター Corp. サーバからアップデートを取得します。
2. ウイルスバスター Corp. サーバからアップデートできない場合、次のいずれかの項目に該当するときには、クライアントはトレンドマイクロのアップデートサーバへの直接接続を試行します。
 - [ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → [権限とその他の設定] → [その他の設定] タブの [アップデート設定] で、[トレンドマイクロのアップデートサーバからのアップデートの実行] オプションが有効になっている。
 - トレンドマイクロのアップデートサーバ
(<http://osce10-p.activeupdate.trendmicro.co.jp/activeupdate/japan/>) が [ユーザ指定アップデート元] の最初のエントリとなっている。

ヒント： ウイルスバスター Corp. サーバからアップデートする際に問題が発生した場合には、トレンドマイクロのアップデートサーバをリストの先頭に指定してください。クライアントがトレンドマイクロのアップデートサーバから直接アップデートすると、ネットワークとインターネット間で大量の帯域幅が消費されます。

3. すべての使用可能なアップデート元からアップデートできない場合、クライアントはアップデート処理を終了します。

クライアントのアップデート方法

ウイルスバスター Corp. サーバまたはユーザ指定のアップデート元からコンポーネントをアップデートするクライアントでは、次のアップデート方法を使用することができます。

自動アップデート

クライアントのアップデートは、特定のイベントが発生したとき、または予約に基づいて自動的に実行されます。詳細については、143 ページの「自動アップデート」を参照してください。

手動アップデート

重要なアップデートがある場合には、手動アップデートを使用して、ただちにクライアントにコンポーネントのアップデートを実行するように通知します。詳細については、147 ページの「手動アップデート」を参照してください。

権限ベースのアップデート

アップデート権限のあるユーザは、コンピュータ上のウイルスバスター Corp. クライアントのアップデート方法をより詳細に制御できます。詳細については、149 ページの「アップデート権限」を参照してください。

自動アップデート

自動アップデートを使用すると、すべてのクライアントにアップデートを通知する負荷が軽減され、クライアントコンピュータに最新のコンポーネントがインストールされないというリスクが解消されます。

ウイルスバスター Corp. クライアントでは、自動アップデート時にコンポーネントだけでなく、アップデートされた設定ファイルも受信します。クライアントは、新しい設定を適用するために設定ファイルが必要になります。Web コンソールを使用してウイルスバスター Corp. 設定を変更するたびに、設定ファイルが変更されます。設定ファイルをクライアントに適用する頻度を指定する方法については、以下のステップ 3 を参照してください。

注意： 自動アップデートの実行時にプロキシ設定を使用するようにクライアントを設定できます。詳細については、149 ページの「クライアントコンポーネントのアップデートのプロキシ」を参照してください。

自動アップデートには 2 種類あります。

イベント起動配信

サーバは、最新コンポーネントのダウンロード後に、コンポーネントをアップデートするようにオンラインのクライアントに通知することができます。また、オフラインのクライアントには、再起動してサーバに接続したときに通知することができます。必要に応じて、アップデート後にクライアントコンピュータで ScanNow（手動検索）を開始できます。

注意： ウイルスバスター Corp. サーバは、コンポーネントのダウンロード後にアップデート通知を正常に送信できない場合には、15 分後に通知を自動的に再送信します。サーバは、クライアントが応答するまで最大 5 回、アップデート通知の送信を継続します。5 回目の試行に失敗した場合、サーバは通知の送信を停止します。クライアントが再起動してサーバに接続したときにコンポーネントをアップデートするオプションを選択した場合には、引き続きコンポーネントのアップデートが実行されます。

予約アップデート

予約アップデートの実行には権限が必要です。最初に、権限を与えるクライアントを選択する必要があります。これにより、これらのクライアントで予約に基づいてアップデートが実行されます。

注意： 予約アップデートでネットワークアドレス変換を使用する方法については、148 ページの「NAT によるクライアントの予約アップデート」を参照してください。

ネットワーク上のコンピュータのコンポーネントを自動的にアップデートするには

パス: [アップデート]→[ネットワーク上のコンピュータ]→[自動アップデート]

1. コンポーネントのアップデートを起動するイベントを選択します。

表 4-6. イベント起動配信のオプション

オプション	説明
ウイルスバスター Corp. サーバが新しいコンポーネントをダウンロード後、ただちにクライアントのコンポーネントのアップデートを開始する	サーバが、アップデートの完了後、ただちにクライアントにアップデートするように通知します。頻繁にアップデートされているクライアントは、差分パターンファイルをダウンロードするだけで済み、これによりアップデートにかかる時間も短縮されます (差分パターンファイルの詳細は、132 ページの「サーバコンポーネントの複製」を参照してください)。ただし、頻繁にアップデートを実行すると、サーバのパフォーマンスに悪影響を及ぼす可能性があります。特に多数のクライアントを同時にアップデートする場合には注意が必要です。 スタンドアロンモードのクライアントが存在し、これらのクライアントも同様にアップデートする場合には、[スタンドアロンモードのクライアントを含む] を選択してください。スタンドアロンモードの詳細については、310 ページの「スタンドアロンクライアント」を参照してください。
再起動時、またはウイルスバスター Corp. サーバへの接続時にコンポーネントアップデートの開始を許可する (スタンドアロンモードのクライアントを除く)	アップデートを取得していないクライアントは、サーバとの接続を確立したときに、ただちにコンポーネントをダウンロードします。クライアントがオフラインの場合や、クライアントがインストールされたコンピュータが起動されていない場合には、クライアントがアップデートを取得しないことがあります。
アップデート後、Scan Now を実行する (スタンドアロンモードのクライアントを除く)	サーバは、イベント起動配信後にクライアントに検索を実行するように通知します。特定のアップデートが、ネットワーク内にすでに拡散しているセキュリティリスクに対応するものである場合には、このオプションを有効にすることを検討してください。

2. 予約アップデートの権限を持つクライアントが、予約アップデートを実行する頻度を選択します。

クライアントに予約アップデートの権限が与えられている場合には、次の手順に進みます。

クライアントに予約アップデートの権限が与えられていない場合には、最初に次の手順を実行します。

- a. [ネットワーク上のコンピュータ] → [クライアント管理] に移動し、権限を与えるクライアントを選択します。
- b. [設定] → [権限とその他の設定] の順にクリックします。

オプション 1: [権限設定] タブの [コンポーネントアップデート権限] セクションに移動します。[予約アップデートを有効にする] オプションが表示されます。

オプション 2: [その他の設定] タブの [アップデート設定] セクションに移動します。別の [予約アップデートの有効化] オプションが表示されます。

クライアントユーザに、クライアントコンソールで予約アップデートを有効または無効にできる権限を与える場合には、オプション 1 と 2 を有効にします。この設定を保存すると、アップデートがクライアントコンピュータで予約に従って実行されます。予約アップデートは、クライアントユーザがタスクトレイの [ウイルスバスター Corp.] アイコンを右クリックして、[予約アップデートの無効化] を選択した場合にのみ実行を停止します。

予約アップデートを常に実行し、クライアントユーザが予約アップデートを無効にできないようにするには、オプション 1 を有効にし、オプション 2 を無効にします。

- c. 設定を保存します。
3. 予約を設定します。
- a. [分] または [時間] を選択した場合には、[指定時間 (時) ごとに 1 回] オプションを選択できます。このオプションを選択しない場合、ウイルスバスター Corp. クライアントは、サーバにあるアップデートされたコンポーネントとアップデートされた設定ファイルの両方を、指定された間隔で取得します。このオプションを選択した場合、ウイルスバスター Corp. は、指定された間隔でコンポーネントのみをアップデートし、設定ファイルは 1 日に 1 回アップデートします。

ヒント： コンポーネントは頻繁にアップデートされますが、ウイルスバスター Corp. の設定はほとんどの場合、あまり頻繁に変更されません。コンポーネントとともに設定ファイルをアップデートすると、帯域幅の消費量が多くなり、アップデートに必要な時間が増加します。このため、クライアント設定は 1 日に 1 回だけアップデートするように選択することをお勧めします。

- b. [毎日] または [毎週] を選択した場合、アップデートする時刻と、ウイルスバスター Corp. サーバがクライアントにコンポーネントを更新するように通知する期間を指定します。たとえば、開始時刻が午後 12 時で、期間が 2 時間の場合、ウイルスバスター Corp. は午後 12 時から午後 2 時までの間、すべてのオンラインクライアントにランダムにコンポーネ

ントをアップデートするように通知します。この設定により、指定された開始時刻にすべてのオンラインクライアントがサーバに同時に接続することを防ぐため、サーバへのトラフィック量が大幅に削減されます。

4. [保存] をクリックします。

オフラインクライアントには通知されません。一定の期間後にオンラインになるオフラインクライアントの場合でも、[イベント起動配信] の [再起動時、またはウイルスバスター Corp. サーバへの接続時にコンポーネントアップデートの開始を許可する] を選択しているときには、コンポーネントのアップデートが可能です。選択していない場合は、次のスケジュールのとき、または手動アップデートを開始した場合に、コンポーネントがアップデートされます。

手動アップデート

クライアントのコンポーネントが著しく古いバージョンの場合、および大規模感染が発生したときには、手動でクライアントのコンポーネントをアップデートします。クライアントがアップデート元からコンポーネントを長期間アップデートできないまましていると、クライアントのコンポーネントのバージョンが著しく古くなります。

ウイルスバスター Corp. クライアントは、手動アップデート時にコンポーネントだけでなく、アップデートされた設定ファイルも自動的に受信します。クライアントは、新しい設定を適用するために設定ファイルが必要になります。Web コンソールを使用してウイルスバスター Corp. 設定を変更するたびに、設定ファイルが変更されます。

クライアントを手動でアップデートするには

パス: [アップデート] → [ネットワーク上のコンピュータ] → [手動アップデート]

1. ウイルスバスター Corp. サーバで現在入手可能になっているコンポーネントと、これらのコンポーネントが最後にアップデートされた日付が、画面の上部に表示されます。クライアントにアップデートするように通知する前に、コンポーネントが最新であることを確認してください。

注意: サーバ上の旧版のコンポーネントは、手動でアップデートしてください。詳細については、135 ページの「手動アップデート」を参照してください。

2. アップデートするクライアントを選択します。旧版のコンポーネントを使用しているクライアントをアップデートするか、特定のクライアントをクライアントツリーから選択します。

- 旧版のコンポーネントを使用しているクライアントを選択: サーバは、このサーバのバージョンよりも古いバージョンのコンポーネントを持つクライアントを検索し、これらのクライアントにアップデートするように通知します。サーバとの接続が確立されているスタンドアロンクライアントも検索する場合には、[スタンドアロンモードのクライアントを含む] を選択します。[アップデートを開始] をクリックします。
- クライアントを手動で選択する: このオプションの選択後、[選択] をクリックします。表示されたクライアントツリーで、アップデートするクライアントを選択し、クライアントツリーの最上部で [コンポーネントアップデートの開始] をクリックします。

サーバは各クライアントに、アップデートされたコンポーネントをダウンロードするように通知を開始します。通知のステータスを確認するには、[アップデート] → [概要] 画面に移動します。

NAT によるクライアントの予約アップデート

ローカルネットワークで「NAT」を使用している場合には、次の問題が発生する可能性があります。

- Web コンソールでクライアントがオフラインと表示される
- ウイルスバスター Corp. サーバからクライアントに、アップデートと設定変更について正常に通知できない

これらの問題に対処するには、サーバからクライアントに、アップデートされたコンポーネントと設定ファイルを予約アップデートで配信します。

次の手順を実行します。

1. ウイルスバスター Corp. クライアントをクライアントコンピュータにインストールする前:
 - a. クライアントのアップデートスケジュールを、[アップデート] → [ネットワーク上のコンピュータ] → [自動アップデート] → [予約アップデート] で設定します。
 - b. [ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → [権限とその他の設定] → [権限設定] タブ → [コンポーネントアップデート権限] で、予約アップデートを有効にする権限をクライアントに与えます。
2. ウイルスバスター Corp. クライアントがクライアントコンピュータにすでに存在する場合:
 - a. [ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → [権限とその他の設定] → [権限設定] タブ → [コンポーネントアップデート権限] で、[アップデートの実行] の権限をクライアントに与えます。
 - b. ユーザに、クライアントコンピュータで手動でコンポーネントをアップデートし（タスクトレイで [ウイルスバスター Corp.] アイコンを右クリックして、[アップデート] をクリック）、アップデートされた設定を取得するように指示します。

クライアントはアップデートするときに、アップデートされたコンポーネントと設定ファイルの両方を受信します。

アップデート権限

クライアントユーザに、手動アップデートの実行や、予約アップデートの有効化などの特定の権限を与えます。詳細については、292 ページの「コンポーネントアップデート権限」を参照してください。

クライアントにアップデート権限を与えるには

1. [ネットワーク上のコンピュータ] → [クライアント管理] に移動します。
2. クライアントツリーで、アップデート権限を与えるクライアントを選択します。
3. [設定] → [権限とその他の設定] の順にクリックし、[権限設定] タブの [コンポーネントアップデート権限] セクションに移動します。
4. アップデート権限だけでなく、[その他の設定] タブをクリックし [アップデート設定] セクションに移動して、クライアントのアップデート関連の設定を行います。詳細については、292 ページの「アップデート設定」を参照してください。

クライアントコンポーネントのアップデートのプロキシ

ウイルスバスター Corp. クライアントは、自動アップデートの実行時や、[アップデート] を実行する権限を与えられた場合に、プロキシ設定を使用することができます。

表 4-7. クライアントコンポーネントのアップデート時に使用するプロキシ設定

アップデート方法	使用するプロキシ設定	使用方法
自動アップデート 詳細については、 143 ページの「自動アップデート」 を参照してください。	- 自動プロキシ設定。詳細については、306 ページの「自動プロキシ設定」を参照してください。 - 内部プロキシ設定。詳細については、315 ページの「内部プロキシ」を参照してください。	- ウイルスバスター Corp. クライアントは、コンポーネントのアップデートに自動プロキシ設定を最初に使用します。 - 自動プロキシ設定が使用できない場合には、内部プロキシ設定が使用されます。 - 両方とも使用できない場合、クライアントはプロキシ設定を使用しません。

表 4-7. クライアントコンポーネントのアップデート時に使用するプロキシ設定 (続き)

アップデート方法	使用するプロキシ設定	使用方法
アップデート (詳細については、 292 ページの「コン ポーネントアッ プデート権限」を 参照してくださ い)	- 自動プロキシ設定。詳細につい ては、306 ページの「自動プロ キシ設定」を参照してくださ い。 - ユーザが行うプロキシ設定。ク ライアントユーザには、プロキ シ設定を行う権限を付与できま す。詳細については、291 ペー ジの「プロキシ設定権限」を参 照してください。	- ウイルスバスター Corp. クライ アントは、コンポーネントの アップデートに自動プロキシ設 定を最初に使用します。 - 自動プロキシ設定が使用できな い場合には、ユーザが行うプロ キシ設定が使用されます。 - 両方とも使用できない場合、ま たは自動プロキシ設定が使用で きず、クライアントユーザが必 要な権限を持っていない場合に は、クライアントはコンポーネ ントのアップデート時にプロキ シを使用しません。

クライアントアップデートログ

クライアントでウイルスパターンファイルをアップデートする際に問題が発生するかどうかを判断するには、クライアントアップデートログを確認します。

注意： この製品バージョンで Web コンソールからクエリできるのは、ウイルスパターンファイルのアップデートログのみです。

ハードディスク上の領域を大量に占有しないようにログのサイズを維持するには、手動でログを削除するか、またはログの削除スケジュールを設定します。ログの管理方法の詳細については、265 ページの「ログの管理」を参照してください。

クライアントアップデートログを表示するには：

パス：[ログ]→[ネットワーク上のコンピュータログ]→[コンポーネントアップデート]

1. クライアントのアップデート数を表示するには、[進行状況] 列の [表示] をクリックします。表示された [コンポーネントのアップデート状況] 画面で、15 分ごとの間隔でアップデートされたクライアント数、およびアップデートされたクライアントの総数を確認します。
2. ウイルスパターンファイルをアップデートしたクライアントを表示するには、[詳細] 列の [表示] をクリックします。

3. ログを CSV ファイルに保存するには、[CSV 形式でエクスポート] をクリックします。ファイルを開くか、特定の場所に保存します。CSV ファイルは、通常、Microsoft Excel などのスプレッドシートアプリケーションで開きます。

クライアントアップデート通知

ウイルスバスター Corp. は、次のアップデート関連のイベントが発生したときに、クライアントユーザに通知します。

- ・ 指定された日数を超えた後もウイルスパターンファイルが古いままである
- ・ HotFix をインストールするには、コンピュータを再起動して、新しいバージョンのカーネルモードドライバをロードする必要があります。

詳細については、302 ページの「警告設定」を参照してください。

コンポーネントのロールバック

ロールバックとは、ウイルスパターンファイル、スマートスキャンエージェントパターン、およびウイルス検索エンジンを以前のバージョンに戻すことです。これらのコンポーネントが適切に機能しない場合には、前のバージョンにロールバックします。ウイルスバスター Corp. では、現在のバージョンと以前のバージョンのウイルス検索エンジンが保持されており、さらに最近の 5 バージョンのウイルスパターンファイルとスマートスキャンエージェントパターンが保持されています。

注意： ロールバックできるのは上記のコンポーネントのみです。

ウイルスバスター Corp. は、32 ビットのプラットフォームを実行するクライアントと 64 ビットのプラットフォームを実行するクライアントでは、異なる検索エンジンを使用しています。これらの検索エンジンは個別にロールバックする必要があります。すべての種類の検索エンジンに対するロールバック手順は同じです。

ウイルスパターンファイル、スマートスキャンエージェントパターン、およびウイルス検索エンジンをロールバックするには

パス： [アップデート] → [ロールバック]

1. 該当するセクションの [サーバとの同期] をクリックします。
 - a. 表示されたクライアントツリーで、ロールバックが必要なコンポーネントを持つクライアントを選択します。
 - b. [ロールバック] をクリックします。画面の下部にある [戻る] をクリックして、[ロールバック] 画面に戻ります。

2. サーバに古いバージョンのパターンファイルがある場合は、[サーバとクライアントのバージョンのロールバック] をクリックすることで、クライアントとサーバの両方のパターンファイルをロールバックします。

アップデートエージェント

ウイルスバスター Corp. クライアントにコンポーネントを配信するタスクを分散するには、アップデートエージェントとして機能する複数のウイルスバスター Corp. クライアントを割り当てるか、または他のクライアントのアップデート元を割り当てます。これにより、クライアントは適切なタイミングでコンポーネントのアップデートを受信でき、ウイルスバスター Corp. サーバに大量のネットワークトラフィックが集中することはありません。

ネットワークが場所によってセグメント化され、セグメント間のネットワークリンクに大量のトラフィックの負荷がかかっている場合には、それぞれの場所に少なくとも 1 つアップデートエージェントを割り当ててください。

アップデートエージェントのシステム要件

アップデートエージェントとして機能するクライアントは、次の要件を満たす必要があります。

表 4-8. アップデートエージェントのシステム要件

リソース	要件
OS	Windows 2000、XP、Vista、Server 2003、2008
ハードウェア	プロセッサ 800MHz Intel Pentium または同等の CPU RAM ・ 最低 512MB、1GB を推奨 (Windows 2000、XP、Server 2003) ・ 最低 1GB、1.5GB を推奨 (Windows Vista、Server 2008) ハードディスク空き容量 700MB アップデートエージェントは、ハードディスク空き容量が不十分な場合、コンポーネントの取得や配信に失敗する場合があります。アップデートエージェントには、ハードディスク空き容量が十分あるクライアントを割り当ててください。 その他 解像度 800x600、256 色以上をサポートするモニター
アップデート要求のキャパシティ	コンピュータのハードウェア仕様に依存

アップデートエージェント設定

アップデートエージェント設定は、次の2つのステップで実行します。

1. クライアントをアップデートエージェントとして割り当てます。
2. このアップデートエージェントからアップデートするクライアントを指定します。

注意： 1つのアップデートエージェントが処理できるクライアントの同時接続数は、コンピュータのハードウェア仕様によって異なります。

クライアントをアップデートエージェントとして割り当てるには

パス：[ネットワーク上のコンピュータ]→[クライアント管理]→[設定]→[アップデートエージェント設定]

1. [アップデートエージェント]を選択します。
2. [保存]をクリックします。

アップデートエージェントからアップデートするクライアントを指定するには

パス：[アップデート]→[ネットワーク上のコンピュータ]→[アップデート元]→[ユーザ指定アップデート元]

1. [追加]をクリックします。表示された画面で、クライアント IP アドレスの範囲を入力します。
2. [アップデートエージェント] フィールドで、クライアントに割り当てるアップデートエージェントを選択します。
3. [保存]をクリックします。

アップデートエージェントのアップデート元

アップデートエージェントは、ウイルスバスター Corp. サーバやユーザ指定のアップデート元など、さまざまなアップデート元からアップデートを取得できます。アップデート元は、Web コンソールの [アップデート元] 画面で設定します。

アップデートエージェントのアップデート元を設定するには

パス：[アップデート]→[ネットワーク上のコンピュータ]→[アップデート元]

1. アップデートエージェントの標準アップデート元（ウイルスバスター Corp. サーバ）とアップデートエージェントのユーザ指定アップデート元のどちらからアップデートするかを選択します。
2. [すべてのクライアントへ通知]をクリックします。

アップデートエージェントのユーザ指定アップデート元

アップデートエージェントは、ウイルスバスター Corp. サーバの他に、ユーザ指定のアップデート元からもアップデートできます。ユーザ指定のアップデート元により、クライアントからウイルスバスター Corp. サーバへのアップデートトラフィックを減らすことができます。[ユーザ指定アップデート元] でユーザ指定のアップデート元を指定します。ここでは、1024 までのアップデート元を指定できます。リストの設定手順については、141 ページの「ユーザ指定アップデート元」を参照してください。

リストを設定し保存したら、次のようにアップデート処理が実行されます。

1. アップデートエージェントが、リスト上の 1 番目のエントリからアップデートされます。
2. 1 番目のエントリからアップデートできない場合には、2 番目のエントリからアップデートされ、アップデートできない場合には、以下同様の処理が続けられます。
3. すべてのエントリからアップデートできない場合、エージェントは、[利用できるユーザ指定アップデート元が見つからない場合、ウイルスバスター Corp. サーバからアップデートする] オプションが有効かどうかを確認します。有効な場合、エージェントはウイルスバスター Corp. サーバからアップデートされます。

このオプションが無効な場合、次のいずれかの項目に該当するときには、エージェントはトレンドマイクロのアップデートサーバへの直接接続を試行します。

- [ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → [権限とその他の設定] → [その他の設定] タブの [アップデート設定] で、[トレンドマイクロのアップデートサーバからのアップデートの実行] オプションが有効になっている。
 - トレンドマイクロのアップデートサーバ
(<http://osce10-p.activeupdate.trendmicro.co.jp/activeupdate/japan/>) が [ユーザ指定アップデート元] に含まれていない。
4. すべての使用可能なアップデート元からアップデートできない場合、アップデートエージェントはアップデート処理を終了します。

[アップデートエージェント: 常に標準アップデート元 (ウイルスバスター Corp. サーバ) を使用する] オプションが有効で、ウイルスバスター Corp. サーバがアップデートエージェントにコンポーネントをアップデートするように通知する場合には、アップデート処理が異なったものになります。この処理は次のとおりです。

1. アップデートエージェントが直接ウイルスバスター Corp. サーバからアップデートされ、アップデート元のリストは無視されます。
2. サーバからアップデートできない場合、次のいずれかの項目に該当するときには、エージェントはトレンドマイクロのアップデートサーバへの直接接続を試行します。

- ・ [ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → [権限とその他の設定] → [その他の設定] タブの [アップデート設定] で、[トレンドマイクロのアップデートサーバからのアップデートの実行] オプションが有効になっている。
- ・ トレンドマイクロのアップデートサーバ
(<http://osce10-p.activeupdate.trendmicro.co.jp/activeupdate/japan/>) が [ユーザ指定アップデート元] の最初のエン트리となっている。

ヒント： ウイルスバスター Corp. サーバからアップデートする際に問題が発生した場合のみ、トレンドマイクロのアップデートサーバをリストの先頭に指定してください。クライアントがトレンドマイクロのアップデートサーバから直接アップデートすると、ネットワークとインターネット間で大量の帯域幅が消費されます。

3. すべての使用可能なアップデート元からアップデートできない場合、アップデートエージェントはアップデート処理を終了します。

アップデートエージェントの標準アップデート元

ウイルスバスター Corp. サーバは、アップデートエージェントの標準のアップデート元です。アップデートエージェントをウイルスバスター Corp. サーバから直接アップデートするように設定した場合、アップデート処理は次のように実行されます。

1. アップデートエージェントがウイルスバスター Corp. サーバからアップデートを取得します。
2. ウイルスバスター Corp. サーバからアップデートできない場合、次のいずれかの項目に該当するときには、エージェントはトレンドマイクロのアップデートサーバへの直接接続を試行します。
 - ・ [ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → [権限とその他の設定] → [その他の設定] タブの [アップデート設定] で、[トレンドマイクロのアップデートサーバからのアップデートの実行] オプションが有効になっている。
 - ・ トレンドマイクロのアップデートサーバ
(<http://osce10-p.activeupdate.trendmicro.co.jp/activeupdate/japan/>) が [ユーザ指定アップデート元] の最初のエン트리となっている。

ヒント： ウイルスバスター Corp. サーバからアップデートする際に問題が発生した場合のみ、トレンドマイクロのアップデートサーバをリストの先頭に指定してください。アップデートエージェントがトレンドマイクロのアップデートサーバから直接アップデートすると、ネットワークとインターネット間で大量の帯域幅が消費されます。

3. すべての使用可能なアップデート元からアップデートできない場合、アップデートエージェントはアップデート処理を終了します。

アップデートエージェントのコンポーネントの複製

ウィルスバスター Corp. サーバと同様に、アップデートエージェントでもコンポーネントのダウンロード時にコンポーネントの複製が使用されます。サーバがコンポーネントの複製を実行する方法の詳細については、132 ページの「サーバコンポーネントの複製」を参照してください。

アップデートエージェントのコンポーネントの複製処理は、次のようになります。

1. アップデートエージェントは、現在の完全なパターンファイルのバージョンと、アップデート元の最新バージョンを比較します。2 つのバージョンの差が 14 以下の場合、アップデートエージェントは、2 つのバージョンの差分に相当する差分パターンファイルをダウンロードします。

注意： 差が 14 を超える場合、アップデートエージェントは自動的にパターンファイルの完全なバージョンをダウンロードします。

2. アップデートエージェントで、ダウンロードした差分パターンファイルと現在の完全なパターンファイルが結合されて、最新の完全なパターンファイルが生成されます。
3. アップデートエージェントは、アップデート元の残りの差分パターンファイルをすべてダウンロードします。
4. 最新の完全なパターンファイルとすべての差分パターンファイルが、クライアントから使用可能になります。

アップデートエージェントのアップデート方法

アップデートエージェントは、通常のクライアントが使用可能なアップデート方法と同じ方法を使用します。詳細については、143 ページの「クライアントのアップデート方法」を参照してください。

Client Packager を使用してインストールされたアップデートエージェントでは、予約アップデート設定ツールを使用して、予約アップデートを有効にし、設定することもできます。

注意： アップデートエージェントが他のインストール方法でインストールされている場合には、このツールを使用することはできません。詳細については、72 ページの「インストール方法」を参照してください。

予約アップデート設定ツールを使用するには

1. アップデートエージェントコンピュータで、< クライアントのインストールフォルダ > に移動します。
2. SUCTool.exe をダブルクリックして、ツールを実行します。予約アップデート設定ツールのコンソールが開きます。
3. [予約アップデートの有効化] を選択します。
4. アップデートの頻度と時刻を指定します。
5. [適用] をクリックします。

コンポーネントアップデートの概要

パス: [アップデート] → [概要]

Web コンソールには、コンポーネントアップデートの全般的なステータスを表示するアップデートの概要画面があります。この画面で旧版のコンポーネントをアップデートできます。サーバの予約アップデートを有効にしている場合は、この画面に次のアップデートスケジュールも表示されます。

画面を定期的に更新して、最新のコンポーネントアップデートステータスを表示します。

注意: 統合スマートスキャンサーバでコンポーネントのアップデートを表示するには、[スマートスキャン] → [統合サーバ] に移動します。

ネットワーク上のコンピュータのアップデートステータス

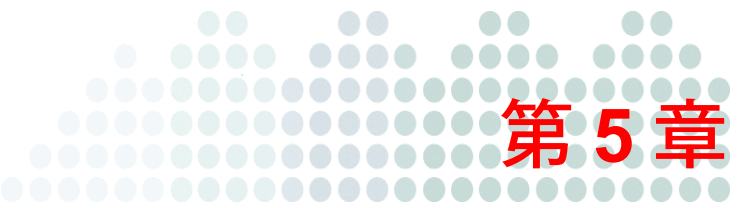
クライアントへのコンポーネントアップデートを開始した場合、このセクションで次の情報を参照します。

- コンポーネントをアップデートするように通知したクライアントの数
- まだ通知されていないが、すでに通知キューに入っているクライアントの数。これらのクライアントへの通知をキャンセルするには、[通知のキャンセル] をクリックします。

コンポーネント

[アップデート状況] 表で、ウイルスバスター Corp. サーバがダウンロードおよび配信した、各コンポーネントのアップデート状況を参照します。

コンポーネントごとに、現在のバージョンと最新アップデート日付が表示されます。古いバージョンのコンポーネントを持つクライアントを表示するには、数字のリンクをクリックします。古いバージョンのコンポーネントを持つクライアントを手動でアップデートします。



第5章

セキュリティリスクからのコンピュータの保護

この章で説明する内容には、次の項目が含まれます。

- 160 ページの「セキュリティリスクについて」
- 165 ページの「検索方法」
- 176 ページの「検索の種類」
- 181 ページの「すべての検索の種類に共通の設定」
- 197 ページの「検索関連の権限」
- 197 ページの「グローバル検索設定」
- 198 ページの「セキュリティリスク通知」
- 202 ページの「セキュリティリスクログ」
- 210 ページの「大規模感染予防サービス」
- 218 ページの「デバイスコントロール」

セキュリティリスクについて

セキュリティリスクとは、ウイルス / 不正プログラムおよびスパイウェア / グレーウェアの総称です。トレンドマイクロ ウイルスバスター コーポレートエディション (以下、ウイルスバスター Corp.) は、ファイルを検索して、検出されたセキュリティリスクごとに特定の処理を実行することでセキュリティリスクからコンピュータを保護します。短期間に大量の数のセキュリティリスクが検出された場合には大規模感染の兆候を表し、ウイルスバスター Corp. は大規模感染予防ポリシーを実行して、完全にリスクがなくなるまで感染したコンピュータを隔離することで大規模感染を抑制することが可能です。通知やログは、セキュリティリスクを監視するために利用でき、さらに即座に処理が必要な場合の警告となります。

ウイルスと不正プログラム

いまや無数のウイルス / 不正プログラムが存在し、毎日作成されています。今日、ウイルス / 不正プログラムは企業のネットワークやメールシステム、Web サイトの脆弱性などに対し、非常に大きなダメージを与えています。

ウイルスバスター Corp. は、次の種類のウイルス / 不正プログラムからコンピュータを保護します。

ジョークプログラム

ジョークプログラムは、ウイルスのようなプログラムで、コンピュータの画面上にいたずらな表現を表示したりします。

トロイの木馬プログラム

トロイの木馬は、実行形式のプログラムで複製はしないが、その代わり、コンピュータの中に住み込み、不正な行動を起こします。たとえば、ポートを開けてハッカーを侵入させたりします。このプログラムは、コンピュータへアクセスするために「トロイポート」を使用することがよくあります。コンピュータからウイルスを取り除くというアプリケーションが実際にはコンピュータにウイルスを導入したというのがトロイの木馬の例です。これまでのウイルス対策ソリューションはウイルスを検出し、削除できるものですが、トロイの木馬のように、特にシステムで作動するようなものは今までとは違います。

ウイルス

ウイルスは、複製するプログラムです。複製するために、ウイルスは自分自身を他のプログラムファイルに添付してホストプログラムが動作するときにはいつも動作します。

- **ActiveX 不正コード**: Web ページに内在し、ActiveX コントロールを実行します。

- ・ **起動ウイルス**：パーティションやディスクの起動セクタに感染するウイルスです。
- ・ **COM ファイルおよび EXE ファイルのウイルス**：.com や .exe などの拡張子を持った実行ファイルプログラムです。
- ・ **Java 不正コード**：OS 独自のウイルスで、Java で書かれ、埋め込まれています。
- ・ **マクロウイルス**：アプリケーションマクロとして暗号化され、ドキュメントに含まれているウイルスです。
- ・ **VB スクリプト、Java スクリプト、HTML ウィルス**：Web ページに内在し、ブラウザを通じてダウンロードされるウイルスです。
- ・ **ワーム**：自己完結型プログラムまたはプログラムセットで、ワーム自体またはワームの一部の動作可能なコピーを、通常はメール を介して別のコンピュータシステムに拡散できます。

テストウイルス

テストウイルスは不活性のファイルで、ウイルス検索ソフトにより検出されます。EICAR テストスクリプトのようにウイルス検索ソフトが適切に検索するかどうかテストするのに使います。

Packer

Packer は、圧縮され、暗号化された Windows、Linux の実行可能プログラムで、トロイの木馬などがそうです。実行ファイルを圧縮すると、ウイルス検索製品が検出するのは難しくなります。

潜在的なウイルス / 不正プログラム

ウイルス / 不正プログラムの特性がある不審ファイルは、このウイルス / 不正プログラムの種類に分類されます。潜在的なウイルス / 不正プログラムの詳細については、トレンドマイクロのオンラインウイルスデータベースの次のページを参照してください。

http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=POSSIBLE_VIRUS

ネットワークウイルス

ネットワーク上で蔓延するウイルスは厳密な意味ではネットワークウイルスではありません。ウイルス / 不正プログラムのうちでも、ワームのように、ほんのわずかしかなネットワークウイルスに該当しません。特にネットワークウイルスは、TCP、FTP、UDP、HTTP、メールプロトコルのようなネットワークプロトコルを使い、複製します。それらはシステムファイルを変えたり、ハードディスクの起動セクタを変更したりすることはめったにありません。その代わり、ネットワークウイルスはクライアントコンピュータのメモリに感染し、トラフィックの増加をもたらし、ネットワークを遅くしさらにはネットワークダウンを引き起こします。ネットワークウイルスはメモリにとどまるので、通常のファイル I/O ベースの検索方法では検出できません。

ウイルスバスター Corp. ファイアウォールはファイアウォールパターンファイルを使用してネットワークウイルスを検出しブロックします。詳細については、230 ページの「ウイルスバスター Corp. ファイアウォールについて」を参照してください。

その他

「その他」に該当するのは、いずれのウイルス / 不正プログラムの種類にも分類されないウイルス / 不正プログラムです。

スパイウェアとグレーウェア

スパイウェアおよびグレーウェアはウイルスやトロイの木馬とは異なりますが、不正な処理を実行する可能性のあるソフトウェアです。ネットワーク上のコンピュータのパフォーマンスに悪影響を与えたり、セキュリティ、機密、および法律に関する重大なリスクを企業に与えたりする可能性があります。多くの場合、スパイウェア / グレーウェアは、煩わしいポップアップウィンドウの表示、ユーザのキー入力の記録、コンピュータの脆弱性を露呈させ攻撃を受けやすくするなど、さまざまな好ましくない脅威につながる動作を実行します。

ウイルスバスター Corp. は、次の種類のスパイウェア / グレーウェアからコンピュータを保護します。

スパイウェア

スパイウェアは、アカウントユーザ名、パスワード、クレジットカード番号などのデータ、およびその他の機密情報を収集し、第三者に送信します。

アドウェア

アドウェアは、広告を表示、Web サーフィンの嗜好などのデータを収集します。このデータは、今後そのユーザへの広告内容の設定に使用されることがあります。

ダイヤラー

ダイヤラーは、クライアントのインターネット設定を変更し、あらかじめ設定された電話番号にコンピュータからモデム経由でダイヤルするよう強制します。この番号は、多くの場合、ペイパーコール (pay-per-call) や国際電話の番号となっており、企業に多大な費用を負わせる可能性があります。

ジョークプログラム

ジョークプログラムは、CD-ROM トレイの開閉、多数のメッセージボックスを表示するなどコンピュータに異常な挙動をさせます。

ハッキングツール

ハッキングツールは、ハッカーがコンピュータに入るのを助けます。

リモートアクセスツール

リモートアクセスツールは、ハッカーがリモートアクセスしてコンピュータをコントロールするのを助けます。

パスワード解読アプリケーション

この種類のアプリケーションは、ユーザ名およびパスワードを解読するために使用します。

その他

「その他」に該当するのは、いずれのスパイウェア / グレーウェアの種類にも分類されない潜在的に不正なプログラムです。

スパイウェア / グレーウェアがネットワークに入り込む方法

ユーザが正規のルートでソフトウェアをダウンロードする際に、そのソフトのインストーラにグレーウェアが含まれていると、その間にスパイウェア / グレーウェアは企業のネットワークに入り込みます。ほとんどのソフトウェアプログラムには、エンドユーザライセンス契約書（EULA）があり、ダウンロードする前にユーザは承諾処理をしなければなりません。EULA はしばしばアプリケーションの情報を含み、その意図的使用として個人データを集めます。しかし、ユーザはこのことを見落とすか、あるいは用語を理解できません。

潜在的リスクと脅威

ネットワーク上のスパイウェアや他のグレーウェアの存在は、次のような事象が潜在的に導入されます。

コンピュータのパフォーマンス低下

これらのタスクを実行するために、スパイウェア / グレーウェアはしばしばかなりの CPU とシステムメモリリソースを必要とします。

増加する Web ブラウザのクラッシュ：

ある種のグレーウェアは、アドウェアのようにブラウザフレームや Windows に情報を何度も表示します。これらのアプリケーションのコードがシステムプロセスとどのような相互作用をするかによって、グレーウェアは時々ブラウザをクラッシュさせたり、フリーズさせたり、さらにはコンピュータの再起動を要求することもあります。

ユーザ効率の低下

頻繁に生じるポップアップ広告やジョークプログラムのマイナス効果に悩まされ、ユーザはその主たる業務が必要以上に散漫になってしまいます。

ネットワーク速度の低下

スパイウェア / グレーウェアは集めた情報をネットワーク上で動作する他のアプリケーションや、外部に定期的に伝えたりします。

個人情報、企業情報の損失

スパイウェア / グレーウェアが集めるデータは、ユーザが訪問する Web サイトのリストのような情報だけではありません。スパイウェア / グレーウェアは、オンライン銀行口座や企業ネットワークにアクセスするためなどに使用するユーザアカウント情報を集める場合もあります。

法的責任のリスク増加

ネットワーク上のコンピュータリソースがハイジャックされると、ハッカーは企業のクライアントコンピュータを利用して攻撃をしかけたり、ネットワーク外のコンピュータにスパイウェア / グレーウェアをインストールすることもあります。このような活動でネットワークリソースに関与した場合、他の団体が受ける損害に対して、企業に法的な責任が発生する可能性があります。

スパイウェア / グレーウェアに対する防御

コンピュータにスパイウェア / グレーウェアをインストールすることを防御する方法はいくつかあります。トレンドマイクロは次のような対策を強く提案します。

- すべての種類の検索（手動検索、リアルタイム検索、予約検索、および ScanNow）を設定して、スパイウェア / グレーウェアのファイルとアプリケーションを検索および削除できるようにします。詳細については、176 ページの「検索の種類」を参照してください。
- クライアントユーザに、次のようなことを指導します。

- ・ クライアントユーザがダウンロードして自分たちのコンピュータにインストールするアプリケーションのエンドユーザ使用許諾契約書 (EULA) と付属ドキュメントを読むこと。
- ・ ソフトウェアをダウンロードしてインストールする許可を求めるメッセージに対しては、クライアントユーザがソフトウェアの作成者と閲覧している Web サイトを信頼できると確信できない場合は、[いいえ] をクリックすること。
- ・ 未承諾広告メール (スパムメール)、特にスパムメールがユーザにボタンやハイパーリンクをクリックするよう求めている場合は無視すること。
- ・ Web ブラウザを厳しいセキュリティレベルに設定してください。ActiveX コントロールをインストールする前に Web ブラウザがユーザに確認を求めるように設定します。Internet Explorer (IE) のセキュリティレベルを上げるには、[ツール] → [インターネット オプション] → [セキュリティ] タブをクリックし、スライダを上げてください。この設定により、アクセスしたい Web サイトで問題が生じる場合には、[サイト] をクリックしてアクセスしたい Web サイトを信頼するサイトリストに追加してください。
- ・ Microsoft Outlook を使っている場合は、スパムメールで送られる画像ファイルのように Microsoft Outlook が HTML アイテムを自動的にダウンロードしないようなセキュリティ設定にしてください。
- ・ ピアツーピアのファイル共有サービスを使用できないようにしてください。スパイウェアや他のグレーウェアアプリケーションは、MP3 ミュージックファイルなどのように、ユーザがダウンロードしたくなるような別の種類のファイルにマスクされている場合があります。
- ・ クライアントコンピュータにインストールされたソフトウェアを定期的に調べて、スパイウェアや他のグレーウェアの可能性のあるアプリケーションを探してください。ウイルスバスター Corp. でグレーウェアとして検出されないが、グレーウェアと思えるようなアプリケーションやファイルがある場合は、トレンドマイクロの次のサイトにご連絡ください。
<http://subwiz.trendmicro.com/SubWiz>
提出されたファイルおよびアプリケーションはトレンドラボで分析します。
- ・ Windows OS を Microsoft 社から提供される最新 Patch を使用して更新してください。詳細は Microsoft の Web サイトを参照してください。

検索方法

ウイルスバスター Corp. クライアントでは、セキュリティリスクを検索するとき、従来型スキャンとスマートスキャンのいずれかを使用することができます。

従来型スキャン

従来型スキャンは、以前のすべてのウイルスバスター Corp. バージョンで使用されていた検索方法です。従来型スキャンクライアントでは、クライアントコンピュータ上にすべてのウイルスバスター Corp. コンポーネントが格納され、ローカルのすべてのファイルが検索されます。

スマートスキャン

スマートスキャンは、次世代の In the cloud ベースのエンドポイント保護ソリューションです。このソリューションは、クラウドに保存された脅威のシグネチャを利用する、高度な検索アーキテクチャを中核に構成されています。

検索方法の比較

次の表は、2つの検索方法を比較したものです。

表 5-1. 従来型スキャンとスマートスキャンの比較

比較基準	従来型スキャン	スマートスキャン
利用可能なバージョン	ウイルスバスター Corp. の以前のすべてのバージョンと現在のバージョン	今回のウイルスバスター Corp. バージョンより対応開始

表 5-1. 従来型スキャンとスマートスキャンの比較 (続き)

比較基準	従来型スキャン	スマートスキャン
検索動作	従来型スキャンクライアントが、ローカルコンピュータで検索を実行します。	・ スマートスキャンクライアントが、ローカルコンピュータで検索を実行します。 ・ クライアントが検索時にファイルの危険性を判定できない場合には、検索クエリをスマートスキャンサーバに送信して危険性を検証します。 ・ 高度なフィルタテクノロジーの使用により、クライアントは検索クエリの結果を「キャッシュ」できます。クライアントは同じ検索クエリをスマートスキャンサーバに送信する必要がないため、検索のパフォーマンスが向上します。 ・ クライアントで、ファイルの危険性をローカルで検証できず、さらにスマートスキャンサーバに接続できない場合、次の処理が実行されます。 ・ クライアントによって、検証するファイルにフラグが付けられます。 ・ クライアントがファイルへの一時アクセスを許可します。 ・ スマートスキャンサーバへの接続が回復すると、フラグが付けられたすべてのファイルが再検索されます。感染していることが確認されたファイルに、適切な検出時の処理が実行されます。
使用中および更新されたコンポーネント	アップデート元で利用可能なすべてのコンポーネント (スマートスキャンエージェントパターンを除く)	アップデート元で利用可能なすべてのコンポーネント (ウイルスパターンファイルおよびスパイウェア監視パターンファイルを除く)
通常のアップデート元	ウイルスバスター Corp. サーバ	ウイルスバスター Corp. サーバ

従来型スキャンからスマートスキャンへの切り替え

従来型スキャンからスマートスキャンへクライアントを切り替える場合には、次の事項について注意してください。

1. 製品ライセンス

スマートスキャンを使用するには、ライセンスが次のサービスに対してアクティベート済みで、さらに期限切れでないことを確認します。

- ウイルス対策
- Web レピュテーションおよびスパイウェア対策

2. スマートスキャンサーバ

スマートスキャンクライアントは、「スマートスキャンサーバ」に接続して検索クエリを送信し、スマートスキャンパターンファイルと照合して、ファイルの危険性を検証します。クライアントが接続するスマートスキャンサーバは、クライアントの位置によって異なります。内部クライアントはローカルのスマートスキャンサーバに接続し、外部クライアントは Trend Micro グローバルスマートスキャンサーバに接続します。

グローバルスマートスキャンサーバ

グローバルスマートスキャンサーバへの接続にプロキシ認証が必要な場合には、認証用の資格情報を指定します。詳細については、317 ページの「外部プロキシ」を参照してください。

ローカルスマートスキャンサーバ

ウイルスバスター Corp. では、2 種類のローカルスマートスキャンサーバを利用できます。両方のサーバは同じ機能を備えています。

- **統合サーバ:** セットアップには統合スマートスキャンサーバが含まれており、ウイルスバスター Corp. サーバがインストールされているコンピュータに統合スマートスキャンサーバがインストールされます。

ウイルスバスター Corp. サーバのインストール時に統合サーバをインストールした場合には、このサーバにアップデート設定を行い、サーバに最新のアップデートが適用されていることを確認します。このサーバのアップデート方法の詳細については、137 ページの「スマートスキャンサーバのアップデート」を参照してください。

このサーバにプロキシサーバ経由で接続する場合には、プロキシ設定を指定します。詳細については、315 ページの「内部プロキシ」を参照してください。

ヒント: サーバコンピュータのウイルスバスター Corp. ファイアウォールを無効にすることを検討してください。有効になっている場合、ウイルスバスター Corp. ファイアウォールが統合サーバのパフォーマンスに影響することがあります。ウイルスバスター Corp. ファイアウォールを無効にする方法については、247 ページの「ウイルスバスター Corp. ファイアウォールの無効化」を参照してください。

- ・ **スタンドアロンサーバ**: スタンドアロンスマートスキャンサーバは、VMware サーバにインストールします。スタンドアロンサーバには個別の管理コンソールがあり、ウイルスバスター Corp. Web コンソールからは管理されません。

これらのサーバを設定していない場合には、クライアントをスマートスキャンに切り替える前に、まずサーバをインストールしてください。統合サーバの再アクティベートおよびスタンドアロンサーバのインストールと管理については、ウイルスバスター Corp. 用スマートスキャン クイックスタートガイドを参照してください。

ヒント: フェイルオーバーの目的で複数のサーバをインストールすることをお勧めします。クライアントは、特定のサーバに接続できない場合、設定済みの別のサーバへの接続を試行します。

3. スマートスキャンサーバリスト

設定したスマートスキャンサーバは、スマートスキャンサーバリストに追加します。クライアントはこのリストを参照して、接続先のスマートスキャンサーバを決定します。特定のサーバに接続できない場合には、他のサーバへの接続を試行します。

リストの設定方法の詳細については、172 ページの「スマートスキャンソース」を参照してください。

4. コンピュータ位置の設定

ウイルスバスター Corp. には、クライアントコンピュータの位置を識別し、クライアントがグローバルとローカルのどちらのスマートスキャンサーバに接続するかを決定するための位置認識機能があります。これにより、クライアントはその位置に関係なく保護されます。

位置設定の指定方法については、280 ページの「コンピュータの位置」を参照してください。

5. ウイルスバスター Corp. サーバ

クライアントがウイルスバスター Corp. サーバに接続可能であることを確認します。スマートスキャンへ切り替わったことが通知されるのは、オンラインクライアントのみです。オフラインクライアントは、オンラインになったときに通知されます。スタンドアロンモードのクライアントは、オンラインになったときに通知されるか、またはクライアントに予約アップデートの権限がある場合には、予約アップデートの実行時に通知されます。

また、ウイルスバスター Corp. サーバに最新のコンポーネントがインストールされていることも確認してください。これは、スマートスキャンクライアントが、サーバからスマートスキャンエージェントパターンファイルをダウンロードする必要があるためです。コンポーネントをアップデートする方法については、129 ページの「ウイルスバスター Corp. サーバのアップデート」を参照してください。

6. その他のトレンドマイクロ製品

Trend Micro Network VirusWall Enforcer がインストールされている場合には、次の作業を実行してください。

- HotFix (Network VirusWall Enforcer 2500 用のビルド 1047、および Network VirusWall Enforcer 1200 用のビルド 1013) をインストールします。
- OPSWAT エンジンバージョン 2.5.1017 にアップデートし、クライアントの検索方法が検出されるようにします。

7. 切り替えるクライアントの数

一度に切り替えるクライアントの数を比較的少数にすることで、ウイルスバスター Corp. サーバとスマートスキャンサーバリソースを効率的に使用することができます。これらのサーバは、クライアントが検索方法を変更しても、他の重要なタスクを実行できます。

8. タイミング

クライアントは、初めてスマートスキャンに切り替えるときに、ウイルスバスター Corp. サーバから完全バージョンのスマートスキャンエージェントパターンファイルをダウンロードする必要があります。スマートスキャンパターンファイルは、スマートスキャンクライアントでのみ使用されます。

ダウンロードプロセスを短時間で終了させるために、オフピーク時に切り替えることを検討してください。また、サーバからクライアントをアップデートする予定がないときに切り替えることを検討してください。さらに、クライアントでの手動アップデートを一時的に無効にして、クライアントがスマートスキャンに切り替わってから再度有効にしてください。

9. クライアントツリー設定

検索方法は、ルート、ドメイン、または個別のクライアントレベルで設定できる、細かい設定です。スマートスキャンに切り替えると次の操作が可能になります。

- 新しいクライアントツリードメインを作成し、その検索方法としてスマートスキャンを割り当てます。このドメインに移動したすべてのクライアントは、スマートスキャンを使用します。

注意： クライアントを移動するときは、[新しいドメインの設定を選択したクライアントに適用する] の設定を有効にします。

- ドメインを選択し、スマートスキャンを使用するように設定します。そのドメインに属する従来型スキャンクライアントは、スマートスキャンに切り替わります。
- ドメインから 1 つ以上の従来型スキャンクライアントを選択し、スマートスキャンに切り替えます。

注意： ドメインの検索方法に対する変更は、個々のクライアントに設定した検索方法よりも優先されます。

スマートスキャンから従来型スキャンへの切り替え

クライアントを従来型スキャンに戻すときには、次の点を考慮してください。

1. 切り替えるクライアントの数

一度に切り替えるクライアントの数を比較的少数にすることで、ウイルスバスター Corp. サーバとスマートスキャンサーバリソースを効率的に使用することができます。これらのサーバは、クライアントが検索方法を変更しても、他の重要なタスクを実行できます。

2. タイミング

従来型スキャンに戻すときに、クライアントはウイルスバスター Corp. サーバから、完全バージョンのウイルスパターンファイルとスパイウェア監視パターンファイルをダウンロードする可能性があります。これらのパターンファイルは、従来型スキャンクライアントでのみ使用されます。

ダウンロードプロセスを短時間で終了させるために、オフピーク時に切り替えることを検討してください。また、サーバからクライアントをアップデートする予定がないときに切り替えることを検討してください。さらに、クライアントでの手動アップデートを一時的に無効にして、クライアントがスマートスキャンに切り替わってから再度有効にしてください。

3. クライアントツリー設定

検索方法は、ルート、ドメイン、または個別のクライアントレベルで設定できる、細かい設定です。従来型スキャンに切り替えると次の操作が可能になります。

- 新しいクライアントツリードメインを作成し、その検索方法として従来型スキャンを割り当てます。このドメインに移動したすべてのクライアントは、従来型スキャンを使用します。

注意： クライアントを移動するときは、[新しいドメインの設定を選択したクライアントに適用する] の設定を有効にします。

- ドメインを選択し、従来型スキャンを使用するように設定します。そのドメインに属するスマートスキャンクライアントは、従来型スキャンに切り替わります。
- ドメインから 1 つ以上のスマートスキャンクライアントを選択し、従来型スキャンに切り替えます。

注意： ドメインの検索方法に対する変更は、個々のクライアントに設定した検索方法よりも優先されます。

検索方法を変更するには

パス：[ネットワーク上のコンピュータ]→[クライアント管理]→[設定]→[検索方法]

1. 従来型スキャンまたはスマートスキャンを選択します。
2. クライアントツリーのドメインまたはクライアントを選択している場合は、[保存] をクリックすると設定がドメインまたはクライアントに適用されます。ルートアイコン  を選択した場合は、次のオプションのいずれかを選択します。
 - **すべてのクライアントに適用：** すべての既存のクライアント、および既存または将来追加されるドメインに加えられる新しいクライアントに、設定を適用します。将来追加されるドメインとは、設定を指定した時点で作成されていないドメインのことです。
 - **将来追加されるドメインにのみ適用：** 将来追加されるドメインに加えられるクライアントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいクライアントには設定を適用しません。

スマートスキャンソース

スマートスキャンモードでは、ウイルスバスター Corp. クライアントが最初にセキュリティリスクをローカルで検索します。クライアントが検索時にファイルの危険性を判定できない場合には、スマートスキャンサーバに接続します。

クライアントが接続するスマートスキャンサーバは、クライアントコンピュータの位置によって異なります。内部クライアントは、ローカルのスマートスキャンサーバ（統合またはスタンドアロン）に接続し、外部クライアントは、グローバルスマートスキャンサーバに接続します。位置設定の指定方法については、280 ページの「コンピュータの位置」を参照してください。

グローバルスマートスキャンサーバに接続するときにプロキシ設定を使用するように、クライアントを設定することができます。詳細については、317 ページの「外部プロキシ」を参照してください。

ローカルのスマートスキャンサーバをインストールした場合には、ウイルスバスター Corp. Web コンソールでスマートスキャンサーバリストを設定します。内部クライアントは、検索クエリの送信が必要になった場合、このリストからサーバを選択します。クライアントが最初のサーバに接続できない場合には、別のサーバをリストから選択し、接続できない場合には、以下同様の選択を繰り返します。

ヒント： スタンドアロンのスマートスキャンサーバをプライマリ検索ソースとして割り当てて、統合サーバをバックアップとして割り当てます。これにより、ウイルスバスター Corp. サーバと統合サーバをホストするコンピュータへの検索クエリトラフィックが削減されます。また、スタンドアロンサーバで、より多くの検索クエリ処理が可能になります。

スマートスキャンサーバリストを設定するには

パス：[スマートスキャン]→[検索ソース]→[内部クライアント]

1. クライアントが標準リストとカスタムリストのどちらを使用するかを選択します。
2. [すべてのクライアントへ通知] をクリックします。スマートスキャンクライアントは、設定したリストを自動的に参照します。

標準リスト

標準リストは、すべての内部スマートスキャンクライアントによって使用されます。リスト上のスマートスキャンサーバに接続するときにプロキシ設定を使用するように、クライアントを設定することができます。詳細については、315 ページの「内部プロキシ」を参照してください。

標準リストを設定するには

パス：[スマートスキャン]→[検索ソース]→[内部クライアント]

1. [標準リスト] リンクをクリックします。
2. 開いた画面で、[追加] をクリックし、URL 形式で、スマートスキャンサーバのアドレスを指定します。

スマートスキャンサーバのアドレスを取得するには

- 統合スマートスキャンサーバの場合、ウイルスバスター Corp. Web コンソールを開き、[スマートスキャン] → [統合サーバ] に進みます。
- スタンドアロンスマートスキャンサーバの場合、スタンドアロンサーバのコンソールを開き、[概要] 画面に進みます。

ヒント： 統合スマートスキャンサーバとウイルスバスター Corp. サーバは同じコンピュータ上で実行されるため、2つのサーバのトラフィックがピークになるときは、コンピュータのパフォーマンスが著しく低下する場合があります。ウイルスバスター Corp. サーバへのトラフィックを減らすには、スタンドアロンスマートスキャンサーバをプライマリ検索ソースに割り当てて、統合サーバをバックアップソースに割り当てます。

3. [接続テスト] をクリックして、サーバへの接続が確立できることを確認します。テスト接続に成功したら [保存] をクリックします。
4. [スマートスキャンサーバのアドレス] の下のリンクをクリックして、サーバのアドレスを変更します。
5. ローカルのスマートスキャンサーバのコンソールを開くには、[コンソールの起動] をクリックします。
 - 統合スマートスキャンサーバの場合は、サーバの設定画面が表示されます。
 - スタンドアロンのスマートスキャンサーバ、および別のウイルスバスター Corp. サーバの統合スマートスキャンサーバの場合は、コンソールのログオン画面が表示されます。
6. エントリを削除するには、サーバ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。
7. リストを .dat ファイルにエクスポートするには、[エクスポート] をクリックし、[保存] をクリックします。
8. 別のサーバからリストをエクスポートしている場合、この画面にインポートするときは、[インポート] をクリックして、.dat ファイルの場所を探します。リストが画面にロードされます。
9. 画面の上部で、クライアントがサーバをリストの順番どおりに参照するか、ランダムに参照するかを選択します。[順序] を選択する場合は、[順序] 列の下の方印を使用して、サーバをリストで上下に移動します。
10. [保存] をクリックします。

カスタムリスト

カスタムリストを選択した場合は、カスタムリストの IP アドレスの範囲を指定します。あるクライアントの IP アドレスが範囲内にある場合、そのクライアントはカスタムリストを使用します。

カスタムリストを設定するには

パス: [スマートスキャン] → [検索ソース] → [内部クライアント]

1. [追加] をクリックします。
2. 表示された画面で、次の値を指定します。
 - IP アドレスの範囲
 - クライアントがローカルのスマートスキャンサーバに接続する際に使用するプロキシ設定
3. スマートスキャンサーバのアドレス (URL 形式) を指定します。

スマートスキャンサーバのアドレスを取得するには

 - 統合スマートスキャンサーバの場合、ウイルスバスター Corp. Web コンソールを開き、[スマートスキャン] → [統合サーバ] に進みます。

- スタンドアロンスマートスキャンサーバの場合、スタンドアロンサーバのコンソールを開き、[概要] 画面に進みます。

ヒント： 統合スマートスキャンサーバとウイルスバスター Corp. サーバは同じコンピュータ上で実行されるため、2つのサーバのトラフィックがピークになるときは、コンピュータのパフォーマンスが著しく低下する場合があります。ウイルスバスター Corp. サーバへのトラフィックを減らすには、スタンドアロンスマートスキャンサーバをプライマリスキャンソースに割り当てて、統合サーバをバックアップソースに割り当てます。

4. [接続テスト] をクリックして、サーバへの接続が確立できることを確認します。テスト接続に成功したら [保存] をクリックします。
5. ローカルのスマートスキャンサーバのコンソールを開くには、[コンソールの起動] をクリックします。
 - 統合スマートスキャンサーバの場合は、サーバの設定画面が表示されます。
 - スタンドアロンのスマートスキャンサーバ、および別のウイルスバスター Corp. サーバの統合スマートスキャンサーバの場合は、コンソールのログオン画面が表示されます。
6. エントリを削除するには、[削除] の下のアイコンをクリックします。
7. クライアントがサーバをリストの順番どおりに参照するか、ランダムに参照するかを選択します。[順序] を選択する場合は、[順序] 列の下の矢印を使用して、サーバをリストで上下に移動します。
8. [保存] をクリックします。
9. [スマートスキャンソース] 画面に戻って、クライアントがカスタムリスト上のいずれのサーバとも接続できない場合に、標準リストを参照するかどうかを選択します。
10. IP アドレスの範囲とそれに対応するカスタムリストを変更するには、[IP 範囲] の下のリンクをクリックします。
11. カスタムリストを .dat ファイルにエクスポートするには、[エクスポート] をクリックし、[保存] をクリックします。
12. 別のサーバからカスタムリストをエクスポートしている場合、この画面にインポートするときは、[インポート] をクリックして、.dat ファイルの場所を探します。リストが画面にロードされます。

検索の種類

ウイルスバスター Corp. では、クライアントコンピュータをセキュリティリスクから保護するために、次の検索の種類を提供しています。

表 5-2. 検索の種類

検索の種類	説明
リアルタイム検索	コンピュータ内のファイルが、受信時、開いたとき、ダウンロード時、コピー時、および変更時に自動的に検索されます。 詳細については、176 ページの「リアルタイム検索」を参照してください。
手動検索	ユーザが要求したファイル（またはファイルのセット）を検索する手動の検索です。 詳細については、177 ページの「手動検索」を参照してください。
予約検索	管理者やエンドユーザが設定したスケジュールに従って、コンピュータ内のファイルが自動的に検索されます。 詳細については、178 ページの「予約検索」を参照してください。
ScanNow	1 つ以上の対象コンピュータ内にあるファイルを検索する、管理者が開始する検索です。 詳細については、179 ページの「ScanNow」を参照してください。

リアルタイム検索

リアルタイム検索は、継続的に実行される検索です。ファイルの受信時、開かれたとき、ダウンロード時、コピー時、または変更時に毎回、ファイルにセキュリティリスクが存在するかどうかを調べるリアルタイム検索が実行されます。ウイルスバスター Corp. でセキュリティリスクが検出されなかった場合、ファイルはその場所に残され、ユーザはそのファイルへのアクセスを続けることができます。ウイルスバスター Corp. がセキュリティリスクを検出した場合、通知メッセージが表示され、感染ファイルの名前と該当するセキュリティリスクが表示されます。

注意： 通知メッセージを変更するには、Web コンソールを開いて、[通知] → [クライアントユーザ通知] に進みます。

リアルタイム検索の設定を、1 つ以上のクライアントおよびドメインに設定および適用するか、またはサーバが管理するすべてのクライアントに設定および適用します。

リアルタイム検索を設定するには

パス: [ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → [リアルタイム検索設定]

1. [対象] タブで、ウイルス / 不正プログラムおよびスパイウェア / グレーウェアのリアルタイム検索を有効にするチェックボックスをオンにします。ウイルス / 不正プログラムの検索を無効にすると、スパイウェア / グレーウェアの検索も無効になります。

注意: ウイルスの大規模感染の間は、ウイルスによってクライアントコンピュータ上のファイルやフォルダが変更または削除されるのを防ぐために、リアルタイム検索を無効にすることはできません (初期状態で無効の場合には、自動的に有効になります)。

2. 次の検索基準を設定します。
 - リアルタイム検索をトリガする「ファイルに対するユーザのアクティビティ」
 - 「検索対象ファイル」
 - 「検索設定」
3. 検索除外を指定します。
4. [処理] タブをクリックして、検出されたセキュリティリスクに対して実行する検出時の処理を設定します。
5. クライアントツリーのドメインまたはクライアントを選択している場合は、[保存] をクリックすると設定がドメインまたはクライアントに適用されます。ルートアイコン  を選択した場合は、次のオプションのいずれかを選択します。
 - **すべてのクライアントに適用:** すべての既存のクライアント、および既存または将来追加されるドメインに加えられる新しいクライアントに、設定を適用します。将来追加されるドメインとは、設定を指定した時点で作成されていないドメインのことです。
 - **将来追加されるドメインにのみ適用:** 将来追加されるドメインに加えられるクライアントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいクライアントには設定を適用しません。

手動検索

手動検索はオンデマンドの検索であり、ユーザがクライアントコンソールで検索を実行するとただちに開始されます。検索にかかる時間は、検索するファイル数やコンピュータのハードウェアリソースによって異なります。

手動検索の設定を、1 つ以上のクライアントおよびドメインに設定および適用するか、またはサーバが管理するすべてのクライアントに設定および適用します。

手動検索を設定するには

パス: [ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → [手動検索設定]

1. [対象] タブで、次の検索基準を設定します。
 - ・ 「検索対象ファイル」
 - ・ 「検索設定」
 - ・ 「CPU 使用率」
2. 検索除外を指定します。
3. [処理] タブをクリックして、検出されたセキュリティリスクに対して実行する検出時の処理を設定します。
4. クライアントツリーのドメインまたはクライアントを選択している場合は、[保存] をクリックすると設定がドメインまたはクライアントに適用されます。ルートアイコン  を選択した場合は、次のオプションのいずれかを選択します。
 - ・ **すべてのクライアントに適用**: すべての既存のクライアント、および既存または将来追加されるドメインに加えられる新しいクライアントに、設定を適用します。将来追加されるドメインとは、設定を指定した時点で作成されていないドメインのことです。
 - ・ **将来追加されるドメインにのみ適用**: 将来追加されるドメインに加えられるクライアントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいクライアントには設定を適用しません。

予約検索

予約検索は指定された日時に自動的に実行されます。クライアントの予約検索により検索ルーチンを自動化すれば、検索の管理効率を改善できます。

予約検索の設定を、1 つ以上のクライアントおよびドメインに設定および適用するか、またはサーバが管理するすべてのクライアントに設定および適用します。

予約検索を設定するには

パス: [ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → [予約検索設定]

1. [対象] タブで、ウイルス / 不正プログラムおよびスパイウェア / グレーウェアの検索を有効にするチェックボックスをオンにします。ウイルス / 不正プログラムの検索を無効にすると、スパイウェア / グレーウェアの検索も無効になります。
2. 次の検索基準を設定します。
 - ・ 「スケジュール」
 - ・ 「検索対象ファイル」

- 「検索設定」
 - 「CPU 使用率」
3. 検索除外を指定します。
 4. [処理] タブをクリックして、検出されたセキュリティリスクに対して実行する検出時の処理を設定します。
 5. クライアントツリーのドメインまたはクライアントを選択している場合は、[保存] をクリックすると設定がドメインまたはクライアントに適用されます。ルートアイコン  を選択した場合は、次のオプションのいずれかを選択します。
 - **すべてのクライアントに適用**: すべての既存のクライアント、および既存または将来追加されるドメインに加えられる新しいクライアントに、設定を適用します。将来追加されるドメインとは、設定を指定した時点で作成されていないドメインのことです。
 - **将来追加されるドメインにのみ適用**: 将来追加されるドメインに加えられるクライアントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいクライアントには設定を適用しません。

ScanNow

ScanNow は、ウイルスバスター Corp. 管理者によって Web コンソールを通してリモートで開始され、1 つ以上のクライアントコンピュータを対象にすることができます。

ScanNow の設定を、1 つ以上のクライアントおよびドメインに設定および適用するか、またはサーバが管理するすべてのクライアントに設定および適用します。

ScanNow を設定するには

パス: [ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → [ScanNow 設定]

1. [対象] タブで、ウイルス / 不正プログラムおよびスパイウェア / グレーウェアの検索を有効にするチェックボックスをオンにします。ウイルス / 不正プログラムの検索を無効にすると、スパイウェア / グレーウェアの検索も無効になります。
2. 次の検索基準を設定します。
 - 「検索対象ファイル」
 - 「検索設定」
 - 「CPU 使用率」
3. 検索除外を指定します。
4. [処理] タブをクリックして、検出されたセキュリティリスクに対して実行する検出時の処理を設定します。

5. クライアントツリーのドメインまたはクライアントを選択している場合は、[保存] をクリックすると設定がドメインまたはクライアントに適用されます。ルートアイコン  を選択した場合は、次のオプションのいずれかを選択します。
 - **すべてのクライアントに適用** : すべての既存のクライアント、および既存または将来追加されるドメインに加えられる新しいクライアントに、設定を適用します。将来追加されるドメインとは、設定を指定した時点で作成されていないドメインのことです。
 - **将来追加されるドメインにのみ適用** : 将来追加されるドメインに加えられるクライアントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいクライアントには設定を適用しません。

ScanNow の開始

感染の疑いがあるコンピュータで ScanNow を開始します。

ScanNow を開始するには

パス: [ネットワーク上のコンピュータ] → [クライアント管理] → [タスク] → [ScanNow]

ScanNow ショートカット (メインメニューの一番上)

1. 検索を開始する前に、事前設定された ScanNow 設定を変更するには、[設定] をクリックします。[ScanNow の設定] 画面が開きます。詳細については、179 ページの「ScanNow」を参照してください。
2. クライアントツリーで、検索を実行するクライアントを選択し、[Scan Now を開始] をクリックします。サーバからクライアントに通知が送信されます。

注意: クライアントを選択していない場合は、自動的にクライアントツリー内のすべてのクライアントに通知されます。

3. 通知のステータスをチェックし、通知を受信していないクライアントがあるかどうかを確認します。
4. [未通知のコンピュータを選択] → [Scan Now を開始] の順にクリックすると、未通知のクライアントに対してただちに通知が再送信されます。

例：クライアント総数：50

表 5-3. 未通知のクライアントのシナリオ

クライアントツリーの選択	通知済みのクライアント ([Scan Now を開始] のク リック後)	未通知のクライアント
なし (50 のクライアントす べてを自動的に選択)	50 のクライアントのうち 35 のクライアント	15 のクライアント
手動選択 (50 のクライア ントのうち 45 のクライアント を選択)	45 のクライアントうち 40 のクライアント	5 つのクライアント、およ び手動選択に含まれない別 の 5 つのクライアント

- [通知の中止] をクリックして、現在通知されているクライアントへの通知を停止するようにウィルスバスター Corp. に指示します。通知済みのクライアントおよび検索処理中のクライアントでは、このコマンドが無視されます。
- 検索処理がすでに実行されているクライアントには、[ScanNow を中止] をクリックして検索の停止を通知します。

すべての検索の種類に共通の設定

検索の種類ごとに、検索条件、検索除外、および検出時の処理の 3 つの設定を行います。これらの設定を 1 つ以上のクライアントおよびドメインに配信するか、またはサーバが管理するすべてのクライアントに配信します。

検索条件

ファイルの種類や拡張子などのファイル属性を使用して、特定の検索の種類で検索するファイルを指定します。また、検索をトリガする条件を指定します。たとえば、ファイルがコンピュータにダウンロードされるたびに検索するよう、リアルタイム検索を設定します。

ファイルに対するユーザのアクティビティ

リアルタイム検索をトリガするファイルに対するアクティビティを指定します。次のオプションから選択します。

- ・ **作成 / 変更中のファイル**：コンピュータに（ファイルのダウンロード後などに）取り込まれた新しいファイル、または変更中のファイルを検索します。
- ・ **読み込み中**：ファイルを開くときに検索します。
- ・ **作成中 / 変更中および読み込み中**

たとえば、3 番目のオプションを選択した場合、コンピュータにダウンロードされた新しいファイルが検索され、セキュリティリスクが検出されない場合には現在の場所に残されます。この残されたファイルは、ユーザがそのファイルを開いたとき、およびユーザがそのファイルを変更した場合は変更内容が保存される前に、検索されます。

検索対象ファイル

次のオプションから選択します。

- ・ **検索可能なすべてのファイル**：すべてのファイルを検索します。
- ・ **トレンドマイクロの推奨設定で検索されたファイルタイプ**：不正コードが含まれている可能性のあるファイルのみを検索します。これには無害な拡張子名で偽装されたファイルも含まれます。詳細については、386 ページの「トレンドマイクロの推奨設定」を参照してください。
- ・ **対象の拡張子の選択**：拡張子がファイル拡張子リストに含まれているファイルのみを検索します。新しい拡張子を追加するか、既存の任意の拡張子を削除します。

検索設定

次のオプションから選択します（複数可）。

- ・ **ネットワークドライブの検索**：手動検索時またはリアルタイム検索時に、クライアントコンピュータにマップされたネットワークドライブやフォルダを検索します。
- ・ **隠しフォルダの検索**：手動検索時に、コンピュータ内の隠しフォルダの検出および検索を許可します。
- ・ **圧縮ファイルの検索**：ウイルスバスター Corp. では指定された圧縮レイヤ数まで検索でき、その数を超えるレイヤの検索は省略できます。たとえば、最大レイヤ数が 2 の場合、検索対象の圧縮ファイルに 6 レイヤあったとすると、2 レイヤのみが検索され、残りの 4 レイヤの検索は省略されます。

注意： ウイルスバスター Corp. では、Office Open XML 形式の Microsoft Office 2007 ファイルは、圧縮ファイルとして扱われます。Office Open XML は Office 2007 アプリケーション用のファイル形式であり、ZIP 圧縮技術を使用しています。これらのアプリケーションを使用して作成されたファイルをウイルス / 不正プログラムの検索対象にする場合、圧縮ファイルの検索を有効にする必要があります。

- ・ **シャットダウン時のフロッピーディスク検索**：コンピュータをシャットダウンする前に、フロッピーディスクでシステム領域感染型ウイルスを検索します。これにより、ユーザがディスクからコンピュータを再起動するときに、ウイルス / 不正プログラムが実行されるのを防止します。
- ・ **IntelliTrap を有効にする**：圧縮された実行可能ファイルでウイルス / 不正プログラムを検出および削除します。詳細については、387 ページの「IntelliTrap」を参照してください。
- ・ **システム領域の検索**：手動検索、予約検索、および ScanNow の間に、クライアントコンピュータのハードディスクのシステム領域でウイルス / 不正プログラムを検索します。

CPU 使用率

ウイルスバスター Corp. は、あるファイルを検索した後、次のファイルを検索する前に一時停止することができます。この設定は、手動検索、予約検索、および ScanNow の際に使用します。

次のオプションから選択します。

- ・ **高**：検索を中断しない
- ・ **中**：CPU 使用率が 50% を超える場合はファイル検索の合間に一時中断し、50% 以下の場合は一時中断しない
- ・ **低**：CPU 使用率が 20% を超える場合はファイル検索の合間に一時中断し、20% 以下の場合は一時中断しない

[中] または [低] を選択した場合、検索の開始時に CPU 使用率がしきい値 (50% または 20%) 以内の場合、検索の合間に一時中断されないため、検索時間が短くなります。ウイルスバスター Corp. はこの処理でより多くの CPU リソースを使用しますが、CPU 使用率が最適化されるため、コンピュータのパフォーマンスにはそれ程大きく影響しません。CPU 使用率がしきい値を超え始めると、ウイルスバスター Corp. は、一時中断して CPU 使用率を低下させます。再度使用率がしきい値の範囲内になると一時中断を終了します。

[高] を選択した場合、ウイルスバスター Corp. は実際の CPU 使用率をチェックせず、一時中断しないでファイルを検索します。

スケジュール

予約検索を実行する頻度や時刻を設定します。次のオプションから選択し、続いて開始時刻を選択します。

- ・ 毎日
- ・ 毎週
- ・ 毎月

検索除外

検索除外を設定すると、検索パフォーマンスを向上させ、誤った警告の原因となるファイルの検索を除外させることができます。特定の種類の検索を実行するときに、ウイルスバスター Corp. は検索除外リストをチェックして、ウイルス / 不正プログラムおよびスパイウェア / グレーウェアの両方の検索から除外するコンピュータ内のファイルを決定します。

検索除外を有効にすると、次の条件を満たすファイルは検索されません。

- 特定のディレクトリ内にあるファイル。
- ファイル名が除外リストにあるいずれかの名前と一致するもの。
- ファイル拡張子が除外リストにあるいずれかの拡張子と一致するもの。

検索除外リスト (ディレクトリ)

ウイルスバスター Corp. は、コンピュータ上の特定のディレクトリにあるすべてのファイルを検索しなくなります。最大 250 ディレクトリを指定できます。

[トレンドマイクロ製品がインストールされているディレクトリの除外] のオプションを使用することができます。このオプションを選択すると、次のトレンドマイクロ製品のディレクトリが検索から自動的に除外されます。

- InterScan for Microsoft Exchange (バージョン 7 以外のすべてのバージョン)。バージョン 7 を使用している場合は、次のフォルダを検索除外リストに追加します。
 - ¥Smex¥Temp
 - ¥Smex¥Storage
 - ¥Smex¥ShareResPool
- InterScan eManager 3.11、5.1、5.11、5.12
- InterScan for Lotus Notes eManager NT
- InterScan Messaging Security Suite
- InterScan Web Security Suite
- InterScan WebProtect
- InterScan VirusWall 3.53
- InterScan FTP VirusWall
- InterScan Web VirusWall
- InterScan E-mail VirusWall
- InterScan NSAPI Plug-in
- InterScan eManager 3.5x

リストにないトレンドマイクロ製品を使用している場合には、その製品ディレクトリを検索除外リストに追加します。

さらに、[ネットワーク上のコンピュータ] → [グローバルクライアント設定] → [検索設定] の順に選択し、Microsoft Exchange 2000/2003 ディレクトリを除外するように設定します。Microsoft Exchange 2007 を使用している場合は、該当するディレクトリを検索除外リストに手動で追加します。検索除外の詳細については、次のサイトを参照してください。

<http://technet.microsoft.com/ja-jp/library/bb332342.aspx>

検索除外リスト (ファイル)

ウイルスバスター Corp. は、この除外リストに含まれているいずれかのファイル名に一致するファイルがある場合、そのファイルを検索しません。コンピュータ上の特定の場所にあるファイルを除外する場合は、C:\Temp\sample.jpg のようにファイルパスを含めます。

最大 250 ファイルを指定できます。

検索除外リスト (ファイル拡張子)

ウイルスバスター Corp. は、この除外リストに含まれているいずれかのファイル拡張子に一致するファイルがある場合、そのファイルを検索しません。最大 250 のファイル拡張子を指定できます。拡張子の前にピリオド (.) を付ける必要はありません。

リアルタイム検索の場合、拡張子を指定するときにワイルドカードとしてアスタリスク (*) を使用します。たとえば、DOC、DOT、DAT など、D で始まる拡張子を持つすべてのファイルを検索しない場合は、「D*」と入力します。

手動検索、予約検索、および ScanNow の場合、ワイルドカード文字として疑問符 (?) かアスタリスク (*) を使用します。

すべての検索タイプに検索除外設定を適用する

ウイルスバスター Corp. では、特定の検索の種類に対して検索除外設定を行い、同じ設定を他のすべての検索の種類に適用することができます。

例：

1 月 1 日に、ウイルスバスター Corp. 管理者の Chris が、クライアントコンピュータに大量の JPG ファイルがあることを見つけて、これらのファイルにセキュリティ上の脅威がないことを確認しました。Chris は、手動検索のファイル除外リストに JPG を追加し、次にこの設定をすべての検索の種類に適用しました。これにより、リアルタイム検索、ScanNow、および予約検索は、.jpg ファイルの検索を省略するように設定されました。

1 週間後、Chris は、リアルタイム検索の除外リストから JPG を削除しましたが、すべての検索の種類には検索除外の設定を適用しませんでした。これにより、JPG ファイルはリアルタイム検索の場合にのみ検索されるようになります。

検出時の処理

特定の検索の種類でセキュリティリスクを検出したときに、ウイルスバスター Corp. が実行する処理を指定します。ウイルスバスター Corp. で実行される検出時の処理は、ウイルス / 不正プログラムとスパイウェア / グレーウェアで異なります。

ウイルス / 不正プログラムの検出時の処理

実行される処理は、ウイルス / 不正プログラムの種類と、これらを検出した検索の種類によって異なります。たとえば、手動検索 (検索の種類) によってトロイの木馬プログラム (ウイルス / 不正プログラムの種類) が検出された場合は、感染ファイルが駆除 (処理) されます。

ウイルス / 不正プログラムの種類については、160 ページの「ウイルスと不正プログラム」を参照してください。

検出時の処理

ウイルスバスター Corp. がウイルス / 不正プログラムに対して実行可能な処理は次のとおりです。

削除

ウイルスバスター Corp. では、感染したファイルを削除します。

隔離

ウイルスバスター Corp. では、感染ファイルの名前を変更し、クライアントコンピュータの一時隔離ディレクトリである <「クライアントのインストールフォルダ」>\Suspect に、発見された感染ファイルを移動します。

ウイルスバスター Corp. のクライアントでは、指定された隔離ディレクトリに隔離ファイルを送信します。詳細については、189 ページの「隔離ディレクトリ」を参照してください。

初期設定の隔離ディレクトリは、ウイルスバスター Corp. サーバの <「サーバのインストールフォルダ」>\PCCSRV\Virus の下にあります。ウイルスバスター Corp. では、このディレクトリに送信された隔離ファイルを暗号化します。

隔離ファイルのいずれかを復元する必要がある場合には、VSEncrypt ツールを使用します。

駆除

ウイルスバスター Corp. では、感染ファイルへの全アクセスを許可する前に駆除します。

ファイルを駆除できない場合、ウイルスバスター Corp. では 2 次処理を実行します。2 次処理は、隔離、削除、拡張子変更、または放置のいずれかの処理にできます。2 次処理を設定するには、[ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → { 検索の種類 } → [処理] タブに移動します。

拡張子変更

ウイルスバスター Corp. では、感染ファイルの拡張子を「vir」に変更します。ユーザは拡張子が変わったファイルを開くことはできませんが、復号化し一定のアプリケーションと関連付ければ開くことは可能です。

拡張子を変更した感染ファイルを開くと、ウイルス / 不正プログラムが作動する可能性があります。

放置

ウイルスバスター Corp. では、感染ファイルには処理は実行されません。ただし、ウイルス / 不正プログラム検出のログが記録されます。ファイルは元の場所にあります。

ウイルスバスター Corp. では、手動検索、予約検索、および ScanNow を実行中に、(潜在的なウイルス / 不正プログラムを除く) いずれかの種類のウイルスが検出された場合のみ、この検出時処理を使用できます。ウイルスバスター Corp. では、リアルタイム検索中にこの検出時処理を使用できません。

「潜在的なウイルス / 不正プログラム」の場合、検索の種類に関係なくウイルスバスター Corp. では必ず、**誤検出**に対処するために、検出ファイルに対して何も処理を実行しません。潜在的なウイルス / 不正プログラムが実際にセキュリティリスクであることをその後の解析で確認すると、新しいパターンファイルがリリースされ、ウイルスバスター Corp. で適切な検出時処理を実行できます。実際に無害の場合、潜在的なウイルス / 不正プログラムは検出されません。

:

ウイルスバスター Corp. で「x_probable_virus」が「123.exe」ファイルから検出されましたが、検出時に処理は何も実行していないと仮定します。「x_probable_virus」がトロイの木馬のプログラムであることが確認されると、新しいウイルスパターンファイルがリリースされます。新しいパターンファイルがロードされると、ウイルスバスター Corp. では「x_probable_virus」がトロイの木馬のプログラムとして検出されます。トロイの木馬のプログラムに対する処理が「駆除」の場合、「123.exe」は駆除されます。

アクセス拒否

この検出時の処理は、リアルタイム検索の場合にのみ実行可能です。感染ファイルを開こうとした実行しようとする操作をウイルスバスター Corp. が検出すると、即座にこの操作はブロックされます。

ユーザは感染ファイルを手動で削除できます。

検出時の処理のオプション

検出時の処理を設定するときには、次のオプションから選択します。

トレンドマイクロの推奨処理を使用

トレンドマイクロの推奨処理とは、特定のウイルス / 不正プログラムの種類に事前に割り当てられている一連の処理です。各ウイルス / 不正プログラムの種類に適した処理がわからない場合は、トレンドマイクロの推奨処理を使用してください。トレンドマイクロの推奨処理を使用すると、検出時の処理をカスタマイズする手間が省けます。

注意： トrendマイクロの推奨処理は、スパイウェア / グレーウェア検索には使用できません。

次の表は、ウイルス / 不正プログラムの種類に応じて適用されるトレンドマイクロの推奨処理を示しています。

表 5-4. ウイルス / 不正プログラムに適用されるトレンドマイクロの推奨処理

ウイルス / 不正プログラムの種類	リアルタイム検索		手動検索 / 予約検索 / ScanNow	
	1 次処理	2 次処理	1 次処理	2 次処理
ジョークプログラム	隔離	該当なし	隔離	該当なし
トロイの木馬プログラム	隔離	該当なし	隔離	該当なし
ウイルス	駆除	隔離	駆除	隔離
テストウイルス	アクセス拒否	該当なし	放置	該当なし
Packer	隔離	該当なし	隔離	該当なし
その他	駆除	隔離	駆除	隔離
潜在的なウイルス / 不正プログラム	放置	該当なし	放置	該当なし

すべての種類の検出されたウイルス / 不正プログラムに同じ処理を使用

このオプションは、潜在的なウイルス / 不正プログラムを除く、すべての種類のウイルス / 不正プログラムに同じ処理を実行する場合に選択します。潜在的なウイルス / 不正プログラムに対しては、処理が常に「放置」になります。

特定の処理を検出されたウイルス / 不正プログラムの種類ごとに使用：

ウイルス / 不正プログラムの種類ごとに検索時の処理を手動で選択します。潜在的なウイルス / 不正プログラムに対しては、処理を設定することができず、処理は常に「放置」になります。

1 次処理として「駆除」を選択した場合、駆除に失敗した場合に実行する 2 次処理を選択します。

1 次処理が「駆除」ではない場合、2 次処理を設定することはできません。

隔離ディレクトリ

感染ファイルの処理が「隔離」の場合、ウイルスバスター Corp. クライアントはそのファイルを暗号化し、<「サーバのインストールフォルダ」>%SUSPECT にある一時隔離フォルダに移動します。次に、指定された隔離ディレクトリにファイルを送信します。ウイルスバスター Corp. サーバコンピュータにある初期設定の隔離ディレクトリをそのまま使用するか、または URL、UNC パス、または絶対ファイルパスの形式で場所を入力して別のディレクトリを指定します。

注意： 後から、暗号化された隔離ファイルにアクセスする必要がある場合には、そのファイルを復元することができます。詳細については、191 ページの「暗号化ファイルの復元」を参照してください。

次の表は、URL、UNC パス、または絶対ファイルパスを使用する状況について説明しています。

表 5-5. 隔離ディレクトリ

隔離ディレクトリ	使用可能形式	例	備考
ウイルスバスター Corp. サーバコンピュータのディレクトリ	URL	https://<osceserver>	これは初期設定のディレクトリです。隔離フォルダのサイズなど、このディレクトリの設定を行います。詳細については、273 ページの「隔離フォルダ設定」を参照してください。
	UNC パス	¥¥<osceserver>¥ofcscan¥Virus	

表 5-5. 隔離ディレクトリ (続き)

隔離ディレクトリ	使用可能形式	例	備考
他のウイルスバスター Corp. サーバコンピュータのディレクトリ (ネットワーク上に他のウイルスバスター Corp. サーバがある場合)	URL	https://<osceserver2>	クライアントがこのディレクトリに接続可能であることを確認します。間違ったディレクトリを指定した場合、ウイルスバスター Corp. クライアントは正しい隔離ディレクトリが指定されるまで、¥Suspect フォルダに隔離ファイルを保存します。サーバのウイルス / 不正プログラムログには、隔離ファイルを指定された隔離フォルダに移動できなかったことが記録されます。 UNC パスを使用している場合、隔離ディレクトリフォルダが「Everyone」グループで共有されていることと、このグループに対して読み取り / 書き込み許可を割り当てていることを確認してください。
	UNC パス	¥¥<osceserver2>¥ofcscan¥Virus	
ネットワーク上の他のコンピュータ	UNC パス	¥¥<computer_name>¥temp	
クライアントコンピュータの異なるディレクトリ	絶対パス	C:¥temp	

ウイルス駆除実行前にバックアップを作成

ウイルスバスター Corp. が感染ファイルを駆除するように設定されている場合、最初にファイルをバックアップすることができます。これにより、後でこのファイルが必要になった場合にファイルを復元できます。バックアップファイルは開かれないように暗号化され、<「クライアントのインストールフォルダ」>¥Backup フォルダに保存されます。

暗号化されたバックアップファイルを復元する方法については、191 ページの「暗号化ファイルの復元」を参照してください。

ウイルス / 不正プログラムの検出時に通知を表示する

ウイルスバスター Corp. では、リアルタイム検索および予約検索時にウイルス / 不正プログラムを検出した場合に、検出したことをユーザに知らせる通知メッセージを表示できます。

通知メッセージを変更するには、[通知] → [クライアントユーザ通知] → [ウイルス / 不正プログラム] タブに移動します。

暗号化ファイルの復元

ウイルスバスター Corp. では、感染ファイルが開かれないように、次の時点でファイルを暗号化します。

- ファイルを隔離する前
- ファイルのウイルス駆除実行前のバックアップ時

ウイルスバスター Corp. には、ファイルから情報を取得する必要がある場合に、ファイルを復号化して復元するツールが用意されています。ウイルスバスター Corp. では、次のファイルの復号化および復元が可能です。

表 5-6. ウイルスバスター Corp. が復号化および復元可能なファイル

ファイル	説明
クライアントコンピュータ上の隔離されたファイル	このファイルは、<「クライアントのインストールフォルダ」>¥SUSPECT¥Backup フォルダにあり、7 日後に自動的に削除されます。また、ウイルスバスター Corp. サーバの指定された隔離ディレクトリにアップロードされます。
指定された隔離ディレクトリの隔離ファイル	初期設定では、この隔離ディレクトリは、ウイルスバスター Corp. サーバコンピュータに配置されます。詳細については、189 ページの「隔離ディレクトリ」を参照してください。
バックアップされた暗号化ファイル	ウイルスバスター Corp. で駆除可能な感染ファイルのバックアップです。このファイルは、<「クライアントのインストールフォルダ」>¥Backup フォルダにあります。ユーザがこのファイルを復元する場合、<「クライアントのインストールフォルダ」>¥SUSPECT¥Backup フォルダに移動する必要があります。 ウイルスバスター Corp. では、[ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → { 検索の種類 } → [処理] タブの [ウイルス駆除実行前にバックアップを作成] を選択した場合にのみ、駆除前にバックアップと暗号化が実行されます。

警告： 感染ファイルを復元すると、ウイルス / 不正プログラムが他のファイルやコンピュータに感染が拡大する可能性があります。ファイルを復元する前に、感染したコンピュータを隔離して、そのコンピュータにある重要なファイルをバックアップの場所に移動してください。

ファイルの復号化と復元を行うには

ファイルがウイルスバスター Corp. クライアントコンピュータにある場合：

1. コマンドプロンプトを開き、<「クライアントのインストールフォルダ」>に移動します。
2. 次のコマンド入力して、VSEncode.exe を実行します。

```
VSEncode.exe /u
```

このパラメータは、<「クライアントのインストールフォルダ」>%SUSPECT%Backup にあるファイルのリストを画面に表示します。

3. 復元するファイルを選択して、[復元] をクリックします。このツールで復元できるのは、一度に 1 つのファイルのみです。
4. 表示された画面で、ファイルを復元するフォルダを指定します。
5. [OK] をクリックします。指定されたフォルダにファイルが復元されます。

注意： ウイルスバスター Corp. によってファイルが再度検索され、復元後ただちにファイルが感染ファイルとして処理される場合もあります。ファイルが検索されないようにするには、そのファイルを検索除外リストに追加します。詳細については、184 ページの「検索除外」を参照してください。

6. ファイルの復元が終了したら、[閉じる] をクリックします。

ファイルがウイルスバスター Corp. サーバまたはカスタム隔離ディレクトリにある場合：

1. ファイルがウイルスバスター Corp. サーバコンピュータにある場合は、コマンドプロンプトを開いて、<「サーバのインストールフォルダ」>%PCCSRV%Admin%Utility%VSEncrypt に移動します。

ファイルがカスタム隔離ディレクトリにある場合は、<「サーバのインストールフォルダ」>%PCCSRV%Admin%Utility に移動して、カスタム隔離ディレクトリがあるコンピュータに VSEncrypt フォルダをコピーします。

2. テキストファイルを作成して、暗号化または復号化するファイルの完全パスを入力します。
たとえば、C:\My Documents\Reports にあるファイルを復元するには、テキストファイルに「C:\My Documents\Reports*.」と記述します。

ウイルスバスター Corp. サーバコンピュータの隔離ファイルは、<「サーバのインストールフォルダ」>%PCCSRV%Virus にあります。

3. テキストファイルを INI または TXT の拡張子を付けて保存します。たとえば、C: ドライブに ForEncryption.ini として保存します。
4. コマンドプロンプトを開き、VSEncrypt フォルダのあるディレクトリに移動します。

5. 次のコマンド入力して、VSEncode.exe を実行します。

```
VSEncode.exe /d /i <location of the INI or TXT file>
```

説明：

<location of the INI or TXT file> は、作成した INI または TXT ファイルのパスです（たとえば、C:\¥ForEncryption.ini）。

6. その他のパラメータを使用して、さまざまなコマンドを実行できます。

表 5-7. 復元パラメータ

パラメータ	説明
なし（パラメータなし）	ファイルを暗号化します。
/d	ファイルを復号化します。
/debug	デバッグログを作成し、コンピュータに保存します。クライアントコンピュータの <「クライアントのインストールフォルダ」> に、デバッグログ (VSEncrypt.log) が作成されます。
/o	暗号化または復号化されたファイルがすでに存在する場合に、そのファイルを上書きします。
/f <ファイル名>	1 つのファイルを暗号化または復号化します。
/nr	元のファイル名を復元しません。
/v	ツールに関する情報を表示します。
/u	ツールのユーザインタフェースを起動します。
/r <復元先フォルダ>	ファイルを復元するフォルダ
/s <元のファイル名>	暗号化された元のファイルのファイル名

たとえば、「VSEncode [/d] [/debug]」と入力して、Suspect フォルダ内のファイルを復号化し、デバッグログを作成します。ファイルを復号化または暗号化すると、同じフォルダに復号化または暗号化されたファイルが作成されます。ファイルを復号化または暗号化する前に、ロックされていないことを確認してください。

スパイウェア / グレーウェアの検出時の処理

実行される検出時の処理は、スパイウェア / グレーウェアを検出した検索の種類によって異なります。ウイルス / 不正プログラムの種類ごとに特定の処理を設定できますが、すべての種類のスパイウェア / グレーウェアに対して 1 つの処理のみを設定することもできます（各種スパイウェア / グレーウェアの情報については、162 ページの「スパイウェアとグレーウェア」を参照してください）。たとえば、手動検索（検索の種類）によっていずれかのスパイウェア / グレーウェアが検出された場合は、影響を受けたシステムリソースが駆除（処理）されます。

検出時の処理

ウイルスバスター Corp. がスパイウェア / グレーウェアに対して実行可能な処理は次のとおりです。

駆除

プロセスを終了するか、レジストリ、ファイル、Cookie およびショートカットを削除します。

スパイウェア / グレーウェアを駆除した後、ウイルスバスター Corp. クライアントでスパイウェア / グレーウェアのデータをバックアップし、スパイウェア / グレーウェアに安全にアクセスできると考えられる場合、復元することができます。詳細については、196 ページの「スパイウェア / グレーウェアの復元」を参照してください。

放置

検出されたスパイウェア / グレーウェアコンポーネントには処理は実行されません。ただし、スパイウェア / グレーウェア検出のログが記録されます。この処理は、手動検索、予約検索、および ScanNow の場合にのみ実行可能です。リアルタイム検索のときには、処理が「アクセス拒否」になります。

検出されたスパイウェア / グレーウェアが承認済みリストに含まれている場合、いずれの処理も実行されません。詳細については、195 ページの「スパイウェア / グレーウェアの承認リスト」を参照してください。

アクセス拒否

検出されたスパイウェア / グレーウェアコンポーネントへのアクセス（コピー、開く）を拒否します。この処理は、リアルタイム検索の場合にのみ実行可能です。手動検索、予約検索、および ScanNow の場合は、処理が「放置」になります。

スパイウェア / グレーウェアの検出時に通知を表示する

ウイルスバスター Corp. では、リアルタイム検索および予約検索時にスパイウェア / グレーウェアを検出した場合に、検出したことをユーザに知らせる通知メッセージを表示できます。

通知メッセージを変更するには、[通知] → [クライアントユーザ通知] → [スパイウェア / グレーウェア] タブに移動します。

スパイウェア / グレーウェアの承認リスト

ウイルスバスター Corp. には、「承認済み」のスパイウェア / グレーウェアのリストが用意されています。このリストには、スパイウェアまたはグレーウェアとして処理しないファイルまたはアプリケーションが含まれます。検索時に特定のスパイウェア / グレーウェアが検出されると、ウイルスバスター Corp. ではこの承認済みリストをチェックし、リスト内に一致する項目がある場合は処理を実行しません。

承認済みリストを、1 つ以上のクライアントおよびドメインに適用するか、またはサーバが管理するすべてのクライアントに適用します。承認済みリストをすべての検索の種類に適用するということは、手動検索、リアルタイム検索、予約検索、および ScanNow の際に同じ承認済みリストを使用するということを意味します。

検出済みのスパイウェア / グレーウェアを承認済みリストに追加するには

パス: [ネットワーク上のコンピュータ] → [クライアント管理] → [ログ] → [スパイウェア / グレーウェアログ] → [ログ表示] → [スパイウェア / グレーウェアログ] → [承認リストに追加]

[ログ] → [ネットワーク上のコンピュータのログ] → [セキュリティ上の危険] → [ログの表示] → [スパイウェア / グレーウェアログ] → [ログ表示] → [スパイウェア / グレーウェアログ] → [承認リストに追加]

1. 承認済みスパイウェア / グレーウェアを、選択したクライアントコンピュータのみに適用するか、特定のドメインに適用するかを指定します。
2. [追加] をクリックします。[ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → [スパイウェア / グレーウェアの承認リスト] の承認済みリストに、スパイウェア / グレーウェアが追加されます。

注意: ウイルスバスター Corp. では、最大 1024 のスパイウェア / グレーウェアを承認済みリストに追加できます。

スパイウェア / グレーウェアの承認済みリストを管理するには

パス: [ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → [スパイウェア / グレーウェアの承認リスト]

1. [スパイウェア名] テーブルで、スパイウェア / グレーウェア名を選択します。複数の名前を選択するには、<Ctrl> キーを押しながら選択します。
また、「検索」フィールドにキーワードを入力して、[検索開始] をクリックすることもできます。キーワードに一致する名前でテーブルが更新されます。
2. [追加] をクリックします。これらの名前が [承認リスト] テーブルに移動します。
3. 承認済みリストから名前を削除するには、名前を選択して [削除] をクリックします。複数の名前を選択するには、<Ctrl> キーを押しながら選択します。
4. クライアントツリーのドメインまたはクライアントを選択している場合は、[保存] をクリックすると設定がドメインまたはクライアントに適用されます。ルートアイコン  を選択した場合は、次のオプションのいずれかを選択します。
 - **すべてのクライアントに適用**: すべての既存のクライアント、および既存または将来追加されるドメインに加えられる新しいクライアントに、設定を適用します。将来追加されるドメインとは、設定を指定した時点で作成されていないドメインのことです。
 - **将来追加されるドメインにのみ適用**: 将来追加されるドメインに加えられるクライアントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいクライアントには設定を適用しません。

スパイウェア / グレーウェアの復元

スパイウェア / グレーウェアの駆除後、ウイルスバスター Corp. クライアントはスパイウェア / グレーウェアのデータをバックアップします。データが無害であると考えられる場合は、オンラインクライアントにバックアップされたデータを復元するように通知します。バックアップ時間に基づいて復元するスパイウェア / グレーウェアのデータを選択します。

注意: ウイルスバスター Corp. クライアントのユーザは、スパイウェア / グレーウェアの復元を開始することができません。また、クライアントで復元できたバックアップデータについて通知されません。

スパイウェア / グレーウェアを復元するには

パス: [ネットワーク上のコンピュータ] → [クライアント管理] → [タスク] → [スパイウェア / グレーウェアの復元]

1. 復元するアイテムをデータセグメントごとに表示するには、[表示] をクリックします。新しい画面が表示されます。[戻る] をクリックして前の画面に戻ります。
2. 復元するデータセグメントを選択します。

注意: 手順 1 と 2 には、データを CSV ファイルにエクスポートするオプションがあります。

3. [復元] をクリックします。復元のステータスが通知されます。完全なレポートについては、スパイウェア / グレーウェアの復元ログを確認してください。詳細については、210 ページの「スパイウェア / グレーウェア復元ログ」を参照してください。

検索関連の権限

検索権限のあるユーザは、コンピュータ上のファイルの検索方法をより詳細に制御できます。

検索権限を持つユーザは次の操作を実行できます。

- 手動検索、予約検索、およびリアルタイム検索の設定。詳細については、285 ページの「検索権限」を参照してください。
- 予約検索の遅延、停止、またはスキップ。詳細については、286 ページの「予約検索権限」を参照してください。
- Microsoft Outlook および POP3 メールメッセージでのウイルス / 不正プログラムの検索の有効化。詳細については、289 ページの「メール検索権限」を参照してください。

グローバル検索設定

クライアントにグローバル検索設定を適用する方法はいくつかあります。

- 特定の検索設定を、サーバが管理するすべてのクライアントに適用したり、特定の検索権限を持つクライアントにのみ適用することができます。たとえば、予約検索の遅延期間を設定した場合、予約検索の遅延権限を持つクライアントのみがこの設定を使用します。

- 特定の検索設定を、すべての検索の種類に適用したり、特定の検索の種類にのみ適用することができます。たとえば、ウイルスバスター Corp. サーバおよびクライアントの両方がインストールされているコンピュータでは、検索からウイルスバスター Corp. サーバデータベースを除外することができます。ただし、この設定は、リアルタイム検索の場合にのみ適用されます。
- 特定の検索設定を、ウイルス / 不正プログラムまたはスパイウェア / グレーウェア (あるいはその両方) を検索するときに適用できます。たとえば、診断モードはスパイウェア / グレーウェアの検索時にのみ適用されます。

グローバル検索設定を表示する方法については、296 ページの「検索設定」を参照してください。

セキュリティリスク通知

ウイルスバスター Corp. には、検出されたセキュリティリスクや発生した大規模感染に関する情報を、管理者、他のウイルスバスター Corp. 管理者、およびクライアントユーザに知らせるために、一連の初期設定の通知メッセージが用意されています。必要に応じてこれらのメッセージを修正してください。

管理者通知設定

ウイルスバスター Corp. 管理者は、セキュリティリスクが検出されたり大規模感染が発生した場合に、次の方法で通知を受信できます。

- メール
- ポケットベル
- 「SNMP トラップ」
- Windows イベントログ

セキュリティリスクの通知の詳細については、199 ページの「管理者向けのセキュリティリスクの通知」を参照してください。アウトブレイク通知の詳細については、211 ページの「大規模感染の基準と通知」を参照してください。

ウイルスバスター Corp. がメール、ポケットベル、および SNMP トラップで通知を正常に送信できるように、管理者通知設定を行ってください。

管理者通知設定を行うには

パス: [通知] → [管理者通知] → [一般設定]

1. 所定のフィールドに情報を指定します。
2. [SMTP サーバ] および SNMP トラップの [サーバ IP アドレス] フィールドで、IP アドレスまたはコンピュータ名を指定します。
3. 1 ～ 65535 の値でポート番号を指定してください。
4. [ポケットベル] フィールドには、次の数字や記号を指定することができます。
0 ～ 9

*
,
5. 1 ～ 16 の値で COM ポートを指定してください。
6. コミュニティ名には、推測しにくいものを指定してください。
7. [保存] をクリックします。

管理者向けのセキュリティリスクの通知

ウイルスバスター Corp. を設定し、セキュリティリスクを検知するか、セキュリティリスクに対する処理が失敗し、介入を必要とする場合に通知メッセージを送信するようにします。

注意: クライアントコンピュータで表示する通知設定を行うには、201 ページの「クライアントユーザ向けのセキュリティリスクの通知」を参照してください。

管理者用のセキュリティリスク通知を設定するには

パス: [通知] → [管理者通知] → [標準通知]

1. [条件] タブで、ウイルス / 不正プログラムおよびスパイウェア / グレーウェアが検出されたときに通知を送信するか、またはこれらのセキュリティリスクの処理が失敗した場合にのみ通知を送信するかを指定します。
2. [メール]、[ポケットベル]、[SNMP トラップ]、および [イベントログ] タブで、次の操作を行います。
 - a. ウイルス / 不正プログラムおよびスパイウェア / グレーウェアの通知を有効にします。
 - b. メール通知の場合は、メールの受信者を指定し、初期設定の件名をそのまま使用するか、変更します。

- c. 初期設定の通知メッセージをそのまま使用するか変更します。
- d. [メッセージ] および [件名] フィールドでデータを表現するには、トークン変数を使用します。

表 5-8. セキュリティリスク通知のトークン変数

変数	説明
ウイルス / 不正プログラムの検出	
%v	ウイルス / 不正プログラム名
%s	ウイルス / 不正プログラムに感染したコンピュータ
%i	コンピュータの IP アドレス
%m	コンピュータのドメイン
%p	ウイルス / 不正プログラムの場所
%y	ウイルス / 不正プログラム検出の日時
%a	セキュリティリスクに対して実行された処理
%n	感染したコンピュータにログオンしているユーザの名前
スパイウェア / グレーウェアの検出	
%s	スパイウェア / グレーウェアに感染しているコンピュータ
%i	コンピュータの IP アドレス
%m	コンピュータのドメイン
%y	スパイウェア / グレーウェア検出の日時
%T	スパイウェア / グレーウェアと検索結果

- e. [保存] をクリックします。

クライアントユーザ向けのセキュリティリスクの通知

ウイルスバスター Corp. では、リアルタイム検索および予約検索でウイルス / 不正プログラムおよびスパイウェア / グレーウェアが検出された直後に、クライアントコンピュータに通知メッセージを表示できます。通知メッセージを有効にして、必要に応じてメッセージの内容を修正してください。

通知メッセージを有効にするには

パス: [ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → {リアルタイム検索または予約検索の設定} → [処理] タブ

1. ウイルス / 不正プログラムまたはスパイウェア / グレーウェアが検出されたときに通知メッセージを表示するように選択します。
2. クライアントツリーのドメインまたはクライアントを選択している場合は、[保存] をクリックすると設定がドメインまたはクライアントに適用されます。ルートアイコン  を選択した場合は、次のオプションのいずれかを選択します。
 - **すべてのクライアントに適用**: すべての既存のクライアント、および既存または将来追加されるドメインに加えられる新しいクライアントに、設定を適用します。将来追加されるドメインとは、設定を指定した時点で作成されていないドメインのことです。
 - **将来追加されるドメインにのみ適用**: 将来追加されるドメインに加えられるクライアントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいクライアントには設定を適用しません。

通知メッセージの内容を変更するには

パス: [通知] → [クライアントユーザ通知]

1. [ウイルス / 不正プログラム] タブまたは [スパイウェア / グレーウェア] タブをクリックします。
2. 表示されたテキストボックスで初期設定のメッセージを修正します。
3. [保存] をクリックします。

セキュリティリスクログ

ウイルスバスター Corp. では、ウイルス / 不正プログラムまたはスパイウェア / グレーウェアの検出時と、スパイウェア / グレーウェアの復元時にログが生成されます。

ハードディスク上の領域を大量に占有しないようにログのサイズを維持するには、手動でログを削除するか、またはログの削除スケジュールを設定します。ログの管理方法の詳細については、265 ページの「ログの管理」を参照してください。

ウイルス / 不正プログラムログ

ウイルスバスター Corp. では、ウイルス / 不正プログラムの検出時にログが生成されます。

ウイルス / 不正プログラムログを表示するには

パス: [ログ] → [ネットワーク上のコンピュータのログ] → [セキュリティ上の危険] → [ログの表示] → [ウイルス / 不正プログラムログ]

[ネットワーク上のコンピュータ] → [クライアント管理] → [ログ] → [ウイルス / 不正プログラムログ]

1. ログの基準を指定して [ログ表示] をクリックします。
2. ログが表示されます。ログには、次の情報が含まれています。
 - ウイルス / 不正プログラム検出の日時
 - 感染したコンピュータ
 - ウイルス / 不正プログラム名
 - 感染元
 - 感染ファイル
 - ウイルス / 不正プログラムを検出した検索の種類
 - 「ウイルス / 不正プログラムの検索結果」 (検出時の処理が正常に実行されたかどうか)
 - ログの詳細 (詳細を表示するには [表示] をクリックします)。
3. ログを CSV ファイルに保存するには、[CSV 形式でエクスポート] をクリックします。ファイルを開くか、特定の場所に保存します。CSV ファイルは、通常、Microsoft Excel などのスプレッドシートアプリケーションで開きます。

ウイルス / 不正プログラムの検索結果

A. 検出時の処理に成功した場合

ウイルスバスター Corp. が設定された検出時の処理を実行できた場合、次の結果が表示されます。

削除

- ・ 1 次処理は「削除」で、感染ファイルが削除されました。
- ・ 1 次処理は「削除」ですが、駆除は失敗しました。2 次処理は削除で、感染ファイルが削除されました。

隔離

- ・ 1 次処理は「隔離」で、感染ファイルが隔離されました。
- ・ 1 次処理は駆除ですが、駆除は失敗しました。2 次処理は隔離で、感染ファイルが隔離されました。

駆除済み

感染ファイルが駆除されました。

拡張子変更

- ・ 1 次処理は「拡張子変更」で、感染ファイルの拡張子に変更されました。
- ・ 1 次処理は駆除ですが、駆除は失敗しました。2 次処理は拡張子変更で、感染ファイルの拡張子に変更されました。

アクセス拒否

- ・ 1 次処理は「アクセス拒否」で、ユーザが感染ファイルを開こうとしたときに、このファイルへのアクセスが拒否されました。
- ・ 1 次処理は駆除ですが、駆除は失敗しました。1 次処理はアクセス拒否で、ユーザが感染ファイルを開こうとしたときに、このファイルへのアクセスが拒否されました。
- ・ リアルタイム検索時に「潜在的なウイルス / 不正プログラム」が検出されました。
- ・ リアルタイム検索では、検出時の処理が駆除 (1 次処理) と隔離 (2 次処理) の場合でも、システム領域感染型ウイルスに感染しているファイルへのアクセスが拒否される場合があります。これは、システム領域感染型ウイルスを駆除しようとする、感染したコンピュータのマスタースタートレコード (MBR) を破損させる可能性があるためです。手動検索を実行して、ウイルスバスター Corp. でファイルの駆除または隔離をできるようにしてください。

放置 (手動処理)

- ・ 1 次処理は「放置」です。ウイルスバスター Corp. は、感染ファイルに何も処理を実行しませんでした。

- ・ 1 次処理は駆除ですが、駆除は失敗しました。2 次処理は放置のため、ウイルスバスター Corp. は感染ファイルに何も処理を実行しませんでした。

セキュリティ上の危険の可能性があるものを放置しました

この検索結果は、手動検索、予約検索、および ScanNow の実行時に「潜在的なウイルス / 不正プログラム」が検出された場合にのみ表示されます。ウイルスバスター Corp. が、潜在的なウイルス / 不正プログラムを検出したときには、検出時の処理として自動的に放置を使用します。潜在的なウイルス / 不正プログラムに関する情報と、トレンドマイクロに疑わしいファイルを送信して分析を依頼する方法については、トレンドマイクロのオンラインウイルスデータベースの次のページを参照してください。

http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=POSSIBLE_VIRUS&Vsect=Sn

B. 検出時の処理に失敗した場合

ウイルスバスター Corp. が設定された検出時の処理を実行できなかった場合、次の結果が表示されます。

ファイルのウイルスを駆除、またはファイルを隔離できません。

駆除が 1 次処理です。隔離が 2 次処理ですが、両方の処理が失敗しました。

解決策: 以下の「ファイルを隔離できません。」を参照してください。

ファイルのウイルスを駆除、またはファイルを削除できません。

駆除が 1 次処理です。削除が 2 次処理ですが、両方の処理が失敗しました。

解決策: 以下の「ファイルを削除できません。」を参照してください。

ファイルのウイルスを駆除、またはファイルの名前を変更できません。

駆除が 1 次処理です。拡張子変更が 2 次処理ですが、両方の処理が失敗しました。

解決策: 以下の「ファイルの名前を変更できません。」を参照してください。

ファイルを隔離できません。 / ファイルの名前を変更できません。

説明 1

感染ファイルは、別のアプリケーションによりロックされているか、実行中か、または CD 内にあります。使用しているアプリケーションがファイルを解放した後かそのファイルを実行した後に、ウイルスバスター Corp. はそのファイルを隔離するか拡張子を変更します。

解決策

CD 内に感染したファイルがある場合、そのウイルスがネットワーク上の他のコンピュータに感染する可能性もあるので、その CD は使用しないことを検討してください。

説明 2

感染ファイルがクライアントコンピュータの一時インターネットファイルフォルダにあります。Web を参照しているときに、コンピュータにファイルがダウンロードされたため、Web ブラウザは感染ファイルをロックした可能性があります。Web ブラウザがそのファイルを解放すると、ウイルスバスター Corp. はそのファイルを隔離するか拡張子を変更します。

解決策: なし

ファイルを削除できません。

説明 1

感染ファイルが圧縮ファイル内に存在する可能性があり、[ネットワーク上のコンピュータ] → [グローバルクライアント設定] の [圧縮ファイル内の感染ファイルのウイルス駆除 / 削除] の設定が無効になっています。

解決策

[圧縮ファイル内の感染ファイルのウイルス駆除 / 削除] オプションを有効にします。この設定を有効にすると、ウイルスバスター Corp. が圧縮ファイルを解凍し、圧縮ファイル内の感染ファイルを駆除 / 削除して、再度ファイルを圧縮します。

注意: この設定を有効にすると、検索時にコンピュータのリソースの使用量が増加し、検索の実行に時間がかかる場合があります。

説明 2

感染ファイルは、別のアプリケーションによりロックされているか、実行中か、または CD 内にあります。使用しているアプリケーションがファイルを解放した後かそのファイルを実行した後に、ウイルスバスター Corp. はそのファイルを削除します。

解決策

CD 内に感染したファイルがある場合、そのウイルスがネットワーク上の他のコンピュータに感染する可能性もあるので、その CD は使用しないことを検討してください。

説明 3

感染ファイルがクライアントコンピュータの一時インターネットファイルフォルダにあります。Web を参照しているときに、コンピュータにファイルがダウンロードされたため、Web ブラウザは感染ファイルをロックした可能性があります。Web ブラウザがそのファイルを解放すると、ウイルスバスター Corp. はそのファイルを削除します。

解決策: なし

指定された隔離フォルダに隔離ファイルを送信できません。

ウイルスバスター Corp. はファイルをクライアントコンピュータの ¥Suspect フォルダに正常に隔離しましたが、指定された隔離ディレクトリにファイルを送信できませんでした。

解決策

ウイルス / 不正プログラムを検出した検索の種類 (手動検索、リアルタイム検索、予約検索、または ScanNow) を特定し、[ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → { 検索の種類 } → [処理] タブに指定されている隔離ディレクトリを確認します。

隔離ディレクトリが、ウイルスバスター Corp. サーバコンピュータ上または別のウイルスバスター Corp. サーバコンピュータ上にある場合：

1. クライアントがサーバに接続可能であるかどうかを確認します。
2. 隔離ディレクトリの形式として URL を使用している場合：
 - a. 「http://」の後に指定したコンピュータ名が正しいことを確認します。
 - b. 感染ファイルのサイズを確認します。感染ファイルが、[管理] → [隔離フォルダ設定] で指定されている最大ファイルサイズを超えている場合、ファイルを格納できるように設定を調整します。また、ファイルを削除するなど、他の処理を実行することも可能です。
 - c. 隔離ディレクトリフォルダのサイズを確認し、[管理] → [隔離フォルダ設定] で指定されているフォルダの容量を超えているかどうかを判断します。フォルダの容量を調整するか、手動で隔離ディレクトリ内のファイルを削除します。
3. UNC パスを使用している場合、隔離ディレクトリフォルダが「Everyone」グループで共有されていることと、このグループに対して読み取り / 書き込み許可を割り当てていることを確認してください。また、隔離ディレクトリフォルダが存在し、UNC パスが正しいかどうかを確認します。

隔離ディレクトリがネットワーク上の別のコンピュータにある場合 (この状況では UNC パスのみを使用することができます)：

1. クライアントがコンピュータに接続可能であるかどうかを確認します。
2. 隔離ディレクトリフォルダが「Everyone」グループで共有されていることと、このグループに対して読み取り / 書き込み許可を割り当てていることを確認します。
3. 隔離ディレクトリフォルダが存在するかどうかを確認します。
4. UNC パスが正しいかどうかを確認します。

隔離ディレクトリがクライアントコンピュータ上の別のディレクトリにある場合 (この状況では絶対パスのみを使用することができます) は、隔離ディレクトリフォルダが存在するかどうかを確認します。

ファイルのウイルスを駆除できません。

説明 1

感染ファイルが圧縮ファイル内に存在する可能性があり、[ネットワーク上のコンピュータ] → [グローバルクライアント設定] の [圧縮ファイル内の感染ファイルのウイルス駆除 / 削除] の設定が無効になっています。

解決策

[圧縮ファイル内の感染ファイルのウイルス駆除 / 削除] オプションを有効にします。この設定を有効にすると、ウイルスバスター Corp. が圧縮ファイルを解凍し、圧縮ファイル内の感染ファイルを駆除 / 削除して、再度ファイルを圧縮します。

注意： この設定を有効にすると、検索時にコンピュータのリソースの使用量が増加し、検索の実行に時間がかかる場合があります。

説明 2

感染ファイルがクライアントコンピュータの一時インターネットファイルフォルダにあります。Web を参照しているときに、コンピュータにファイルがダウンロードされたため、Web ブラウザは感染ファイルをロックした可能性があります。Web ブラウザがそのファイルを解放すると、ウイルスバスター Corp. はそのファイルを駆除します。

解決策：なし

説明 3

このファイルのウイルスは駆除できない可能性があります。解決策と詳細については、394 ページの「駆除できないファイル」を参照してください。

スパイウェア / グレーウェアログ

ウイルスバスター Corp. では、スパイウェア / グレーウェアの検出時にログが生成されます。

スパイウェア / グレーウェアログを表示するには

パス: [ログ]→[ネットワーク上のコンピュータのログ]→[セキュリティ上の危険]→[ログの表示]→
[スパイウェア / グレーウェアログ]

[ネットワーク上のコンピュータ]→[クライアント管理]→[ログ]→[スパイウェア / グレーウェアログ]

1. ログの基準を指定して [ログ表示] をクリックします。
2. ログが表示されます。ログには、次の情報が含まれています。
 - スパイウェア / グレーウェア検出の日時
 - 感染したコンピュータ
 - スパイウェア / グレーウェア名
 - スパイウェア / グレーウェアを検出した検索の種類
 - スパイウェア / グレーウェアの検索結果の詳細 (検出時の処理が正常に実行されたかどうか)
 - ログの詳細 (詳細を表示するには [表示] をクリックします)。
3. 無害と見なされたスパイウェア / グレーウェアをスパイウェア / グレーウェアの承認リストに追加します。
4. ログを CSV ファイルに保存するには、[CSV 形式でエクスポート] をクリックします。ファイルを開くか、特定の場所に保存します。CSV ファイルは、通常、Microsoft Excel などのスプレッドシートアプリケーションで開きます。

スパイウェア / グレーウェアの検索結果

A. 検出時の処理に成功した場合

第 1 レベルの結果は「完了しました。処理は必要ありません」です。第 2 レベルの結果は次のとおりです。

駆除済み

ウイルスバスター Corp. は、プロセスを終了したか、レジストリ、ファイル、Cookie、およびショートカットを削除しました。

放置 (手動処理)

ウイルスバスター Corp. は、何も処理は実行しませんでした、評価用にスパイウェア / グレーウェアの検出をログに記録しました。

アクセス拒否

ウイルスバスター Corp. は、検出されたスパイウェア / グレーウェアコンポーネントへのアクセス (コピー、開く) を拒否しました。

B. 検出時の処理に失敗した場合

第 1 レベルの結果は「この後の処理が必要です」です。第 2 レベルの結果は、次のメッセージのいずれかになります。

スパイウェア / グレーウェアは安全でない状態で駆除されました。

スパイウェア検索エンジンが単一フォルダを駆除しようとした場合に、次の基準に一致したときにこのメッセージが表示されます。

- ・ 駆除する対象が 250MB を超えています。
- ・ OS がフォルダのファイルを使用しています。このフォルダが通常のシステム操作に必要な可能性もあります。
- ・ そのフォルダはルートディレクトリ (¥C:、または ¥F:) です。

解決策: サポートセンターに問い合わせてください。

スパイウェア / グレーウェアの検索は手動で停止されました。検索を完了してください。

検索が完了する前に、ユーザが中止しました。

解決策: 手動検索を実行し、検索が終了するまで待機します。

スパイウェア / グレーウェアは駆除されました。再起動する必要があります。コンピュータを再起動してください。

ウイルスバスター Corp. はスパイウェア / グレーウェアのコンポーネントを駆除しましたが、タスクを完了するためにコンピュータの再起動が必要です。

解決策: コンピュータをすぐに再起動します。

スパイウェア / グレーウェアを駆除できません。

スパイウェア / グレーウェアが、CD-ROM またはネットワークドライブで検出されました。ウイルスバスター Corp. では、これらの場所で検出されたスパイウェア / グレーウェアを駆除できません。

解決策: 感染ファイルを手動で削除します。

スパイウェア / グレーウェアの検索結果を特定できません。サポートセンターに問い合わせてください。

新しいバージョンのスパイウェア検索エンジンでは、ウイルスバスター Corp. で処理するように設定されていなかった新しい検索結果が出力されます。

解決策：新しい検索結果の判断については、サポートセンターに問い合わせてください。

スパイウェア / グレーウェア復元ログ

スパイウェア / グレーウェアの駆除後、ウイルスバスター Corp. クライアントはスパイウェア / グレーウェアのデータをバックアップします。データが無害であると考えられる場合は、オンラインクライアントにバックアップされたデータを復元するように通知します。バックアップデータが復元されたスパイウェア / グレーウェア、影響を受けるコンピュータ、および復元結果に関する情報は、ログで確認できます。

スパイウェア / グレーウェア復元ログを表示するには

パス：[ログ]→[ネットワーク上のコンピュータのログ]→[スパイウェア / グレーウェアの復元]

1. [結果] 列で、スパイウェア / グレーウェアのデータの復元が成功しているかどうかを確認します。
2. ログを CSV ファイルに保存するには、[CSV 形式でエクスポート] をクリックします。ファイルを開くか、特定の場所に保存します。CSV ファイルは、通常、Microsoft Excel などのスプレッドシートアプリケーションで開きます。

大規模感染予防サービス

特定の期間におけるウイルス / 不正プログラムまたはスパイウェア / グレーウェア検出の件数が、所定のしきい値を超えると、大規模感染が発生します。ネットワークでの大規模感染に対応し、これを阻止するには、次のようないくつかの方法があります。

- ウイルスバスター Corp. を有効にしてネットワークの不審な活動を監視する
- 重大なクライアントコンピュータのポートとフォルダをブロックする
- 大規模感染警告メッセージをクライアントに発信する
- 感染したコンピュータをクリーンアップする

大規模感染の基準と通知

大規模感染をセキュリティリスクの検出数と検出期間によって定義します。大規模感染基準を定義したら、ウイルスバスター Corp. 管理者に対して大規模感染について通知するようにウイルスバスター Corp. を設定し、早期に対応できるようにします。

通知は次の方法で受信できます。

- メール
- ポケットベル
- 「SNMP トラップ」
- Windows イベントログ

ウイルスバスター Corp. がメール、ポケットベル、および SNMP トラップで通知を正常に送信できるように、管理者通知設定を行ってください。詳細については、198 ページの「管理者通知設定」を参照してください。

大規模感染の基準と通知を設定するには

パス: [通知] → [管理者通知] → [アウトブレイク通知]

[通知] → [管理者通知] → [アウトブレイク通知] → [共有フォルダセッション]

1. [条件] タブで、セキュリティリスクごとに検出数と検出期間を指定します。

ヒント: この画面では初期設定値を使用することをお勧めします。

検出数を超えると通知メッセージが送信されます。たとえば、100 に設定した場合、ウイルス / 不正プログラムの 101 番目の検出後に通知が送信されます。

2. ウイルスバスター Corp. を有効にして、ネットワークでのファイアウォール違反と共有フォルダセッションを監視します。[共有フォルダセッション] で、共有フォルダがあるコンピュータと、共有フォルダにアクセスするコンピュータを表示する数字のリンクをクリックします。
3. [メール]、[ポケットベル]、[SNMP トラップ]、および [イベントログ] タブで、次の操作を行います。
 - a. ウイルス / 不正プログラムおよびスパイウェア / グレーウェアの検出の通知を有効にします。

注意: ファイアウォール違反と共有フォルダセッションの大規模感染は、メールでのみ報告されます。

- b. メール通知の場合は、メールの受信者を指定し、初期設定のメールの件名をそのまま使用するか、変更します。必要に応じて、メールに含めるウイルス / 不正プログラムおよびスパイウェア / グレーウェアの追加情報を選択します。クライアント / ドメイン名、セキュリティリスク名、検出日時、パスと感染ファイル、および検索結果を含めることができます。
- c. 初期設定の通知メッセージをそのまま使用するか変更します。
- d. [メッセージ] および [件名] フィールドでデータを表現するには、トークン変数を使用します。

表 5-9. 大規模感染通知のトークン変数

変数	説明
ウイルス / 不正プログラムの大規模感染	
%CV	検出されたウイルス / 不正プログラムの総数
%CC	ウイルス / 不正プログラムを含むコンピュータの総数
スパイウェア / グレーウェアの大規模感染	
%CV	検出されたスパイウェア / グレーウェアの総数
%CC	スパイウェア / グレーウェアを含むコンピュータの総数
ファイアウォール違反の大規模感染	
%A	規定数を越えたログの種類
%C	ファイアウォール違反ログの数
%T	ファイアウォール違反ログを累積する期間
共有フォルダセッションの大規模感染	
%S	共有フォルダセッションの数
%T	共有フォルダセッションを累積する期間
%M	期間 (分単位)

4. [保存] をクリックします。

大規模感染予防サービス

大規模感染が発生したら、大規模感染に対応し、これを阻止するために大規模感染予防策を実行します。予防設定は慎重に行う必要があります。設定が不適切なために、予期しないネットワークの問題が発生する可能性があるからです。

大規模感染予防の設定と有効化を行うには

パス: [ネットワーク上のコンピュータ] → [大規模感染予防サービス] → [大規模感染予防の開始]

1. 次の大規模感染予防ポリシーのいずれかを実行します。
 - 「共有フォルダへのアクセスを制限 / 禁止」
 - 「ポートのブロック」
 - 「ファイルおよびフォルダへの書き込みを禁止」
2. 大規模感染予防を有効にしておく期間 (単位: 時間) を選択します。初期設定は 48 時間です。大規模感染予防の期間が終了する前に、手動でネットワーク設定を復元することができます。

警告: 大規模感染予防の有効期間が、無期限にならないようにしてください。特定のファイル、フォルダ、またはポートを無期限にブロックしたりアクセスを拒否するには、ウイルスバスター Corp. を使用するのではなく、コンピュータとネットワークの設定を直接変更してください。

3. 初期設定のクライアント通知メッセージをそのまま使用するか変更します。

注意: 大規模感染時に管理者に通知するようにウイルスバスター Corp. を設定するには、[通知] → [管理者通知] → [アウトブレイク通知] の順に選択します。

4. [大規模感染予防の開始] をクリックします。選択した大規模感染予防策は、新しいウィンドウに表示されます。
5. クライアントツリーに戻り、[OPP] 列を確認します。大規模感染予防策が適用されているコンピュータには、チェックマークが表示されます。

ウイルスバスター Corp. では、次のイベントをシステムイベントログに記録します。

- サーバイベント (大規模感染予防の開始と、大規模感染予防の有効化のクライアントへの通知)
- クライアントイベント (大規模感染予防の有効化)

大規模感染予防ポリシー

大規模感染が発生したら、次のポリシーのいずれかを実行します。

- ・ 「共有フォルダへのアクセスを制限 / 禁止」
- ・ 「ポートのブロック」
- ・ 「ファイルおよびフォルダへの書き込みを禁止」

共有フォルダへのアクセスを制限 / 禁止

大規模感染時は、共有フォルダを介してセキュリティリスクが拡大するのを防ぐために、ネットワーク上の共有フォルダへのアクセスを制限または拒否します。

このポリシーが有効であっても、ユーザはフォルダを共有できますが、新たに共有されたフォルダにはポリシーが適用されません。このため、大規模感染時はフォルダを共有しないようにユーザに通知するか、または新たに共有されたフォルダにポリシーを適用するために、ポリシーを再度配布してください。

共有フォルダへのアクセスを制限 / 禁止するには

パス: [ネットワーク上のコンピュータ] → [大規模感染予防サービス] → [大規模感染予防の開始] → [共有フォルダへのアクセスを制限 / 禁止]

1. 次のオプションから選択します。
 - ・ **読み取りのみ許可**: 共有フォルダへのアクセスを制限します。
 - ・ **アクセスを禁止**

注意: 読み取りのみの設定は、アクセスを完全に拒否するようにすでに設定されている共有フォルダには適用できません。

2. [保存] をクリックします。[大規模感染予防の設定] 画面が再度表示されます。

ポートのブロック

大規模感染時に、ウイルス / 不正プログラムがクライアントコンピュータにアクセスするために使用する脆弱なポートをブロックします。

警告： 大規模感染予防設定の構成を注意深く行ってください。使用中のポートをブロックすると、それらのポートを使用しているネットワークサービスが使用できなくなります。たとえば、**信頼されたポート**をブロックすると、ウイルスバスター Corp. は大規模感染の間はクライアントと通信できなくなります。

脆弱なポートをブロックするには

パス：[ネットワーク上のコンピュータ]→[大規模感染予防サービス]→[大規模感染予防の開始]→[ポートのブロック]

1. 信頼されたポートをブロックするかどうか選択します。
2. ブロックするポートを [ポートのブロック] 列で選択します。
 - a. テーブルにポートが表示されない場合には、[追加] をクリックします。表示された画面で、ブロックするポート選択して、[保存] をクリックします。
 - **すべてのポート (ICMP を含む)：** 信頼されたポートを除くすべてのポートをブロックします。信頼されたポートもブロックする場合は、前の画面で [信頼されたポートをブロック] チェックボックスをオンにします。
 - **代表的なポート：** ウイルスバスター Corp. のポート番号を少なくとも 1 つ選択して、ポートのブロック設定を保存します。
 - **トロイの木馬プログラムに使用される代表的なポート：** トロイの木馬プログラムに使用される代表的なポートをブロックします。詳細については、392 ページの「トロイポート」を参照してください。
 - **1 から 65535 の間のポート、またはポート範囲：** 必要に応じて、ブロックするトラフィックの方向と、指定したポートをブロックする理由などのコメントを指定します。
 - **Ping プロトコル (ICMP を拒否)：** ping 要求などの ICMP パケットのみをブロックする場合にクリックします。
 - b. ブロック済みのポートの設定を編集するには、ポート番号をクリックします。
 - c. 表示された画面で、設定を変更して、[保存] をクリックします。
 - d. リストからポートを削除するには、ポート番号の横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。[大規模感染予防の設定] 画面が再度表示されます。

ファイルおよびフォルダへの書き込みを禁止

ウイルス / 不正プログラムは、ホストコンピュータ上のファイルやフォルダを変更または削除する可能性があります。大規模感染時には、ウイルス / 不正プログラムがクライアントコンピュータ上のファイルやフォルダを変更または削除するのを防ぐように、ウイルスバスター Corp. を設定します。

ファイルおよびフォルダへの書き込みを禁止するには

パス: [ネットワーク上のコンピュータ] → [大規模感染予防サービス] → [大規模感染予防の開始] → [ファイルおよびフォルダへの書き込みを禁止]

1. ディレクトリパスを入力します。保護するディレクトリパスの入力が終わったら、[追加] をクリックします。

注意: ディレクトリのパスは、仮想パスではなく、絶対パスを入力してください。

2. 保護ディレクトリで保護するファイルを指定します。すべてのファイルを選択するか、特定のファイル拡張子に基づいてファイルを選択します。ファイル拡張子の場合、リストにない拡張子を指定して、テキストボックスに入力し、[追加] をクリックします。
3. 特定のファイルを保護するには、[ファイルの指定] で、完全なファイル名を入力し、[追加] をクリックします。
4. [保存] をクリックします。[大規模感染予防の設定] 画面が再度表示されます。

大規模感染予防サービスの無効化

大規模感染が抑制され、ウイルスバスター Corp. によりすべての感染ファイルがすでに駆除または隔離されたと確信できる場合には、大規模感染予防サービスを無効にしてネットワークの設定を通常の状態に戻します。

大規模感染予防サービスを手動で無効にするには

パス: [ネットワーク上のコンピュータ] → [大規模感染予防サービス] → [設定の復元]

1. ユーザに大規模感染が終了したことを通知するには、[初期設定を復元後、クライアントに通知します。] を選択します。
2. 初期設定のクライアント通知メッセージをそのまま使用するか変更します。
3. [設定の復元] をクリックします。

注意： ネットワーク設定を手動で復元しない場合には、[大規模感染予防の設定] 画面の [自動的に大規模感染予防措置を停止する] に指定されている時間が経過した後に、ウイルスバスター Corp. により自動的にこれらの設定が復元されます。初期設定は 48 時間です。

ウイルスバスター Corp. では、次のイベントをシステムイベントログに記録します。

- サーバイベント (大規模感染予防の開始と、大規模感染予防の有効化のクライアントへの通知)
 - クライアントイベント (大規模感染予防の有効化)
4. 大規模感染予防を無効にした後、大規模感染が抑制されたことを確認するために、ネットワーク上のコンピュータのセキュリティリスクを検索します。

デバイスコントロール

ウイルスバスター Corp. では、コンピュータに接続されている外部のストレージデバイスやネットワークリソースへのアクセスを規制する、デバイスコントロール機能が提供されています。デバイスコントロール機能により、データの損失や漏えいを防ぐことができ、またファイル検索と併用することでセキュリティリスクからの保護が実現されます。

デバイスコントロールは、x86 タイプのプラットフォームを実行するコンピュータでのみ利用できます。

外部デバイスへのアクセスを管理するには

パス: [ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → [デバイスコントロール]

1. チェックボックスをオンにして、デバイスコントロールを有効にします。
2. コンピュータに接続されている USB デバイスの自動実行機能 (autorun.inf) をブロックするか許可するかを選択します。
3. デバイスの種類ごとに権限を選択します。

表 5-10. デバイスの権限

権限	デバイス上のファイル	受信ファイル
全アクセス	許可される操作: コピー、移動、開く、保存、削除、実行	許可される操作: 保存、移動、コピー これは、デバイスにファイルを保存、移動、およびコピーできることを意味します。
読み取り および書き込み	許可される操作: コピー、移動、開く、保存、削除 ブロックされる操作: 実行	許可される操作: 保存、移動、コピー
読み取り および実行	許可される操作: コピー、開く、実行 ブロックされる操作: 保存、移動、削除	ブロックされる操作: 保存、移動、コピー
読み取り	許可される操作: コピー、開く ブロックされる操作: 保存、移動、削除、実行	ブロックされる操作: 保存、移動、コピー
アクセス拒否	デバイスまたはネットワークリソースへのすべてのアクセスが自動的にブロックされます。	ブロックされる操作: 保存、移動、コピー

注意： ウイルスバスター Corp. の検索機能は、デバイスの権限を補完し、これらの権限よりも優先される場合があります。たとえば、権限ではファイルを開くことが可能でも、ウイルスバスター Corp. によってファイルが不正プログラムに感染していることが検出された場合、不正プログラムを排除するために特定の検出時の処理がそのファイルに実行されます。検出時の処理が駆除の場合、ファイルは駆除後に開かれます。ただし、検出時の処理が削除の場合、ファイルは削除されます。

4. ウイルスバスター Corp. によりデバイスへの不正アクセスが検出された場合、クライアントコンピュータに通知メッセージを表示するかどうかを選択します。不正アクセスにはウイルスバスター Corp. がブロックするすべての操作が含まれます。
5. クライアントツリーのドメインまたはクライアントを選択している場合は、[保存] をクリックすると設定がドメインまたはクライアントに適用されます。ルートアイコン  を選択した場合は、次のオプションのいずれかを選択します。
 - **すべてのクライアントに適用：**すべての既存のクライアント、および既存または将来追加されるドメインに加えられる新しいクライアントに、設定を適用します。将来追加されるドメインとは、設定を指定した時点で作成されていないドメインのことです。
 - **将来追加されるドメインにのみ適用：**将来追加されるドメインに加えられるクライアントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいクライアントには設定を適用しません。

デバイスコントロールログ

クライアントでは、デバイスへの不正アクセスがログに記録され、サーバに送信されます。継続的に実行されているクライアントではログが集約され、24 時間経過してから送信されます。再起動されたクライアントは、最後にログがサーバに送信された時刻を確認します。24 時間以上経過している場合は、ただちにクライアントからログが送信されます。

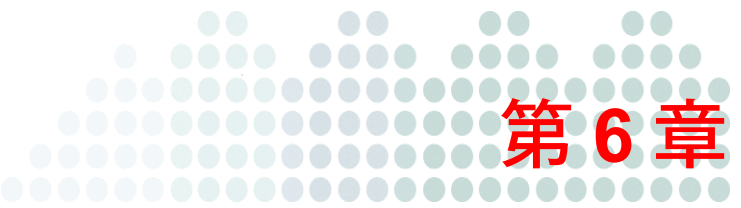
ハードディスク上の領域を大量に占有しないようにログのサイズを維持するには、手動でログを削除するか、またはログの削除スケジュールを設定します。ログの管理方法の詳細については、265 ページの「ログの管理」を参照してください。

デバイスコントロールログを表示するには

パス: [ログ]→[ネットワーク上のコンピュータのログ]→[セキュリティ上の危険]→[ログの表示]→
[デバイスコントロールログ]

[ネットワーク上のコンピュータ]→[クライアント管理]→[ログ]→[デバイスコントロールログ]

1. ログの基準を指定して [ログを表示] をクリックします。
2. ログが表示されます。ログには、次の情報が含まれています。
 - 不正アクセスが検出された日時
 - 外部デバイスが接続されているかまたはネットワークリソースがマップされているコンピュータ
 - アクセスされたデバイスの種類またはネットワークリソース
 - 対象 (アクセスされたデバイスまたはネットワークリソースのアイテム)
 - アクセス元 (アクセスが開始された場所)
 - 対象に設定されている権限



第6章

Web ベースの脅威からのコンピュータの保護

この章で説明する内容には、次の項目が含まれます。

- 222 ページの「Web からの脅威について」
- 222 ページの「Web レピュテーション」
- 223 ページの「位置認識機能」
- 223 ページの「Web レピュテーションポリシー」
- 225 ページの「承認済み URL」
- 225 ページの「Web レピュテーション用プロキシ」
- 226 ページの「クライアントユーザ向けの Web からの脅威の通知」
- 227 ページの「Web レピュテーションログ」

Web からの脅威について

Web からの脅威には、インターネットで発生する広範囲にわたる脅威が含まれます。Web からの脅威はその手法が巧妙化しており、単独のファイルや手法ではなく、さまざまなファイルやテクニックが併用されています。たとえば、Web からの脅威の作成者は、使用するバージョンや亜種を絶えず変えています。Web からの脅威は、感染したコンピュータ上ではなく Web サイトの一定の場所に存在するため、作成者は検出を逃れるために定期的にそのコードを変更しています。

かつて、ハッカー、ウイルスライター、スパムメール送信者、スパイウェア作成者と呼ばれていた人たちは、最近ではサイバー犯罪者と呼ばれるようになりました。Web からの脅威は、このような犯罪者が 2 つの目的のいずれかを達成するために利用されます。目的の 1 つは、今後の営業に関する情報を盗難することです。これにより、個人情報の損失という形で、機密情報の漏えいが発生します。また、感染したコンピュータは、フィッシング攻撃やその他の情報収集活動を拡大するための媒介物として利用される場合もあります。さらに、この脅威によって、Web 商取引での信用を喪失し、インターネット取引に必要な信頼関係が崩壊してしまう危険性もあります。第 2 の目的は、ユーザの CPU の処理能力を奪い取って、金儲け活動の道具として利用することです。この活動には、分散型のサービス拒否攻撃やペイパークリック活動という形をとった、スパムメールの送信や支払いの強要などがあります。

Web レピュテーション

ウイルスバスター Corp. は、トレンドマイクロの大規模な Web セキュリティデータベースを利用して、ユーザがアクセスしようとしている Web サイトのレピュテーションをチェックします。Web サイトのレピュテーションは、コンピュータに適用される特定の Web レピュテーションポリシーと関連付けられています。使用しているポリシーに応じて、Web サイトへのアクセスがブロックまたは許可されます。ポリシーは、クライアントの位置に基づいて適用されます。

注意： 以前の製品で「Web 評価」と呼んでいた機能を、本製品から「Web レピュテーション」に名称変更しています。

位置認識機能

多くの組織では、従業員は職務を行うのにデスクトップコンピュータおよびノート型パソコンの両方を使用します。ノート型パソコンはさまざまなネットワークに接続され、物理的に組織の建物の外に持ち出されるため、ネットワークに接続されていない場合でも保護されるよう、ウイルスバスター コーポレートエディション（以下、ウイルスバスター Corp.）の保護範囲を拡張する必要があります。「Web レピュテーションポリシー」では、位置に関係なくクライアントコンピュータの保護を保証します。

コンピュータに適用されるポリシーは、クライアントの位置（「内部」または「外部」）によって決まります。その位置を、クライアントコンピュータのゲートウェイの IP アドレスに基づいて判断するか、ウイルスバスター Corp. サーバや参照サーバとのクライアントの接続状況に基づいて判断するかを指定する必要があります。

位置認識機能の設定方法については、280 ページの「コンピュータの位置」を参照してください。

Web レピュテーションポリシー

Web レピュテーションポリシーにより、Web サイトへのアクセスをブロックするか許可するかが決まります。ウイルスバスター Corp. は、使用する適切なポリシーを決定するために、クライアントの位置をチェックします。位置は、クライアントコンピュータのゲートウェイ IP アドレスに基づいて判断されるか、クライアントのウイルスバスター Corp. サーバや参照サーバとの接続状況に基づいて判断されます。

次の場合、クライアントの位置は「内部」になります。

- ・ クライアントのゲートウェイ IP アドレスが、[コンピュータの位置] 画面で指定されているいずれかのゲートウェイ IP アドレスと一致する
- ・ クライアントがウイルスバスター Corp. サーバまたはいずれかの参照サーバに接続可能

これら以外の場合、コンピュータの位置は「外部」とみなされます。

Web レピュテーションポリシーを設定するには

パス: [ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → [Web レピュテーション設定]

1. [外部クライアント] と [内部クライアント] にポリシーを設定します。
2. チェックボックスを選択して、Web レピュテーションポリシーを有効または無効にします。

ヒント： Web レピュテーション機能を持つ InterScan Gateway Security Appliance などのトレンドマイクロ製品をすでに使用している場合には、内部クライアントの Web レピュテーションは無効にすることをお勧めします。

3. Web レピュテーションセキュリティレベルを [高]、[中]、[低] から選択します。
ウイルスバスター Corp. は、セキュリティレベルに従って URL へのアクセスを許可するかブロックするかを決定します。たとえば、セキュリティレベルを低に設定すると、ウイルスバスター Corp. は Web からの脅威と認識されている URL のみをブロックします。セキュリティレベルをより高く設定すると、Web からの脅威の検出率が増加しますが、誤検出の可能性も増加します。
4. Web レピュテーションのフィードバックを送信するには、指定された URL を使用します。この URL を指定すると、Trend Micro Web Reputation Query システムが開きます。
5. ウイルスバスター Corp. クライアントから「Web レピュテーションログ」をサーバに送信できるようにするかどうかを選択します。ウイルスバスター Corp. にブロックされている URL を分析して、安全にアクセス可能と考えられる URL に対して適切な処理を実行する場合には、クライアントからのログの送信を許可してください。
6. [保存] をクリックします。

承認済み URL

承認済み URL には、Web レピュテーションポリシーが適用されません。Web レピュテーションポリシーがこれらの URL をブロックするように設定されていても、ウイルスバスター Corp. はブロックしません。安全と考える URL は、承認済み URL リストに追加します。

承認済み URL リストを設定するには

パス: [ネットワーク上のコンピュータ] → [グローバルクライアント設定]

1. [Web レピュテーション承認済み URL リスト] セクションに移動して、その下のリンクをクリックします。
2. 外部クライアントと内部クライアントのどちらのリストを設定するのを選択します。
3. テキストボックスに URL を指定します。
4. URL のサブサイトも承認するか、その Web ページのみを承認するかを選択します。URL が `www.example.com/update` の場合、ウイルスバスター Corp. はこの URL の下のすべてのページを承認しますが、`www.example.com` は承認しません。
5. [追加] をクリックします。
承認するすべての URL をリストに追加するまで、ステップ 3 からステップ 5 を繰り返します。
6. [保存] をクリックします。

Web レピュテーション用プロキシ

組織の HTTP 通信を処理するプロキシサーバを設定しており、Web アクセスを許可する前に認証を要求する場合は、プロキシサーバ認証の資格情報を指定します。ウイルスバスター Corp. は、トレンドマイクロのレピュテーションサーバへの接続時にこの資格情報を使用して、ユーザがアクセスしようとしている Web サイトが安全かどうかを確認します。

このバージョンのウイルスバスター Corp. では、認証用に 1 種類の資格情報のみを使用できます。

プロキシの設定方法については、317 ページの「外部プロキシ」を参照してください。

クライアントユーザ向けの Web からの脅威の通知

ウイルスバスター Corp. では、Web レピュテーションポリシーに違反する URL をブロックした直後に、クライアントコンピュータに通知メッセージを表示できます。通知メッセージを有効にして、必要に応じて通知メッセージの内容を修正してください。

通知メッセージを有効にするには

パス: [ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → [権限とその他の設定] → [その他の設定] タブ

1. [Web レピュテーション設定] で、Web サイトがブロックされたときに通知を表示するように選択します。
2. クライアントツリーのドメインまたはクライアントを選択している場合は、[保存] をクリックすると設定がドメインまたはクライアントに適用されます。ルートアイコン  を選択した場合は、次のオプションのいずれかを選択します。
 - **すべてのクライアントに適用**: すべての既存のクライアント、および既存または将来追加されるドメインに加えられる新しいクライアントに、設定を適用します。将来追加されるドメインとは、設定を指定した時点で作成されていないドメインのことです。
 - **将来追加されるドメインにのみ適用**: 将来追加されるドメインに加えられるクライアントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいクライアントには設定を適用しません。

通知メッセージの内容を変更するには

パス: [通知] → [クライアントユーザ通知] → [Web レピュテーションポリシー違反] タブ

1. 表示されたテキストボックスで初期設定のメッセージを修正します。

注意: 通知メッセージがクライアントコンピュータに表示された後、ブラウザに別のメッセージが表示されます。このメッセージは、URL にアクセスしても安全だと判断した場合、ウイルスバスター Corp. 管理者にその URL を報告するようにユーザに通知します。

2. [保存] をクリックします。

Web レピュテーションログ

サーバに Web レピュテーションログを送信するように、内部および外部クライアントの両方を設定します。ウイルスバスター Corp. にブロックされている URL を分析して、安全にアクセス可能と考えられる URL に対して適切な処理を実行する場合には、この設定を行います。

ハードディスク上の領域を大量に占有しないようにログのサイズを維持するには、手動でログを削除するか、またはログの削除スケジュールを設定します。ログの管理方法の詳細については、265 ページの「ログの管理」を参照してください。

Web レピュテーションログを表示するには

パス: [ログ] → [ネットワーク上のコンピュータログ] → [セキュリティ上の危険] → [ログの表示] → [Web レピュテーションログ]

[ネットワーク上のコンピュータ] → [クライアント管理] → [ログ] → [Web レピュテーションログ]

1. ログの基準を指定して [ログを表示] をクリックします。
2. ログが表示されます。ログには、次の情報が含まれています。
 - ウイルスバスター Corp. が URL をブロックした日時
 - ユーザが URL へのアクセスに使用したコンピュータ
 - ブロックされた URL
 - URL の危険度
 - ブロックされた URL に関する詳細情報を提供する Trend Micro Web Reputation Query システムへのリンク
3. ログを CSV ファイルに保存するには、[CSV 形式でエクスポート] をクリックします。ファイルを開くか、特定の場所に保存します。CSV ファイルは、通常、Microsoft Excel などのスプレッドシートアプリケーションで開きます。



第7章

ウイルスバスター Corp. ファイアウォールの使用

この章で説明する内容には、次の項目が含まれます。

- 230 ページの「ウイルスバスター Corp. ファイアウォールについて」
- 232 ページの「ファイアウォールプロファイルおよびポリシー」
- 243 ページの「ファイアウォール権限」
- 243 ページの「クライアントユーザ向けのファイアウォール違反通知」
- 244 ページの「ファイアウォールログ」
- 245 ページの「ウイルスバスター Corp. ファイアウォールのテスト」
- 247 ページの「ウイルスバスター Corp. ファイアウォールの無効化」

ウイルスバスター Corp. ファイアウォールについて

ウイルスバスター Corp. ファイアウォールは、ステートフルインスペクション、高性能なネットワークウイルス検索、および駆除機能を使用して、ネットワーク上のクライアントとサーバを保護します。中央管理コンソールを介して、接続を IP アドレス、ポート番号、またはプロトコルでフィルタリングするルールを作成し、そのルールをさまざまなユーザグループに適用することができます。

ウイルスバスター Corp. ファイアウォールに含まれる主要な機能および利点は次のとおりです。

トラフィックフィルタリング

ウイルスバスター Corp. ファイアウォールでは、次の条件に基づいて特定の種類のトラフィックをブロックする機能が用意されており、すべての受信および送信トラフィックをフィルタします。

- 方向 (受信 / 送信)
- プロトコル (TCP/UDP/ICMP)
- 宛先ポート
- 送信元および送信先のコンピュータ

ネットワークウイルスの検索

ウイルスバスター Corp. ファイアウォールでは、ネットワークウイルスに感染しているかどうかを判断するために各パケットを検査します。詳細については、161 ページの「ネットワークウイルス」を参照してください。

カスタマイズ可能なプロファイルとポリシー

ウイルスバスター Corp. ファイアウォールには、指定したネットワークトラフィックをブロックまたは許可するためのポリシーを設定する機能があります。1 つまたは複数のプロファイルにポリシーを割り当てると、指定したウイルスバスター Corp. クライアントに配信できます。この機能では、クライアントのファイアウォール設定を高度にカスタマイズできます。

ステートフルインスペクション

ウイルスバスター Corp. ファイアウォールは、ステートフルインスペクションファイアウォールです。クライアントへのすべての接続を監視し、すべての接続状態を記録します。あらゆる接続における特定の状態の識別、後続動作の予測、および正常な接続が侵された場合の検出ができます。そ

のため、フィルタの判定は、プロファイルとポリシーのみを基準に実行されるのではなく、接続を分析し、ファイアウォールを通過したパケットをフィルタして確立したコンテキストも基準として実行されます。

侵入検知システム

ウイルスバスター Corp. ファイアウォールには、IDS（侵入検知システム）も用意されています。IDS を使用すると、クライアントでの攻撃の手がかりとなるネットワークパケットのパターンを識別できます。ウイルスバスター Corp. ファイアウォールでは、以下のような既知の侵入を防ぐことができます。

- **過大フラグメント**：ハッカーが対象コンピュータに対して、特大の TCP/UDP パケットを送りつけるといふ「サービス拒否攻撃」。これによりコンピュータのバッファがオーバーフローするため、フリーズしたり、再起動したりします。
- **Ping of Death**：ハッカーが対象コンピュータに対して、特大の ICMP パケットを送りつけるといふサービス拒否攻撃。これによりコンピュータのバッファがオーバーフローするため、フリーズしたり、再起動したりします。
- **重複 ARP**：ハッカーが送信元と送信先が同じ IP アドレスで ARP リクエストを送るような攻撃。対象コンピュータが頻繁に ARP 応答（MAC アドレス）を自分に送り、しまいにはフリーズしたりクラッシュしたりします。
- **SYN フラッド**：あるプログラムがマルチプル TCP (SYN) パケットをコンピュータに送り、そのコンピュータは SYN/ACK 応答を頻繁に送るといふサービス拒否攻撃。これはコンピュータのメモリを著しく消費し、結局クラッシュします。
- **オーバーラッピングフラグメント**：このサービス拒否攻撃はティアドロップ攻撃と同様、コンピュータに重複する TCP フラグメントを送ります。これは最初の TCP フラグメントのヘッダー情報を上書きして、ファイアウォールを通過します。ファイアウォールは不正のコードを有する後続フラグメントを通過させます。
- **ティアドロップ**：重複フラグメント攻撃と同じで、このサービス拒否攻撃は IP フラグメントを操作します。2 番目以降の IP フラグメントのオフセット値を混乱させ、コンピュータの OS がフラグメントを再編成しようとするときに、クラッシュさせます。
- **タイニーフラグメント攻撃**：この型の攻撃では、小さいサイズの TCP フラグメントが 1 番目の TCP パケットヘッダー情報を次のフラグメントに押し込みます。このためトラフィックをフィルタするルータが、不正のデータを含む可能性のある後続のフラグメントを無視してしまいます。
- **フラグメント化 IGMP**：サービス拒否攻撃で、IGMP パケットを適当に処理できない対象コンピュータに対して、フラグメント化した IGMP パケットを送ります。これによりコンピュータはフリーズするか処理が遅くなります。

- **Land 攻撃**: この攻撃は、送信元と送信先のアドレスが同じ IP SYN パケットを送るため、コンピュータが SYN/ACK 応答を自分に対して送ることになります。これによりコンピュータはフリーズするか処理が遅くなります。

ファイアウォール侵害アウトブレイクの監視

ウイルスバスター Corp. ファイアウォールは、ファイアウォール侵害が一定のしきい値を超えた特定の受信者に、カスタマイズした警告メッセージを送ります。これは攻撃の信号です。

クライアントファイアウォールの権限

ウイルスバスター Corp. クライアントのコンソール上で、ファイアウォールの設定をクライアントユーザに見せることができます。またユーザは、ファイアウォール、IDS（侵入検知システム）、そしてファイアウォール違反通知メッセージを有効 / 無効にすることができます。

ファイアウォールプロファイルおよびポリシー

ウイルスバスター Corp. ファイアウォールでは、ポリシーおよびプロファイルを使用して、ネットワーク上のクライアントを保護する方法を構成し、カスタマイズできます。

ヒント: 複数のベンダのファイアウォールを 1 つのコンピュータにインストールすると、予期せぬ結果を招く恐れがあります。ウイルスバスター Corp. ファイアウォールを配信し有効にする前に、ウイルスバスター Corp. クライアント上の異なるソフトウェアベースのファイアウォールアプリケーションを削除することを検討してください。

ウイルスバスター Corp. ファイアウォールを正常にインストールして使用するために必要な手順は、以下ようになります。

1. ポリシーの作成。ポリシーによってセキュリティレベルを選択できます。セキュリティレベルに応じて、ネットワーク上のコンピュータのトラフィックがブロックまたは許可され、ファイアウォール機能が有効になります。
2. 新規ポリシーを追加する場合、除外設定によって、ポリシーの除外をクライアントに設定できます。ポリシーで全体的なブロックまたは許可のセキュリティレベルが設定されていても、クライアントに除外設定を指定すると、特定の種類のトラフィックを許可またはブロックできます。たとえば、ポリシーで一連のクライアントに対するすべてのトラフィックをブロックしても、HTTP トラフィックを許可する除外設定を作成すると、クライアントは Web サーバにアクセスできます。

3. クライアントがプロファイル内に指定されている属性と一致した場合、関連ポリシーを起動します。

ファイアウォールポリシー

ファイアウォールポリシーを使用すると、ポリシーの除外設定に指定されていない特定の種類のネットワークトラフィックをブロックまたは許可することができます。また、ポリシーでは、どのファイアウォールの機能を有効または無効にするかを定義できます。1 つまたは複数のファイアウォールプロファイルにポリシーを割り当てます。

ウイルスバスター Corp. には、一連の初期設定のポリシーが搭載されており、変更または削除することができます。

初期設定のファイアウォールポリシーは、次のとおりです。

表 7-1. 初期設定のファイアウォールポリシー

ポリシー名	セキュリティレベル	クライアント設定	除外	使用を推奨するケース
オールアクセスポリシー	低	ファイアウォールを有効にする	なし	クライアントにネットワークへの無制限のアクセスを許可するとき
Cisco Trust Agent for Cisco NAC	低	ファイアウォールを有効にする	ポート 21862 を経由する受信 / 送信の UDP トラフィックを許可する	クライアントに Cisco Trust Agent (CTA) がインストールされているとき
Trend Micro Control Manager 用通信ポート	低	ファイアウォールを有効にする	ポート 80 および 10319 を経由するすべての受信 / 送信の TCP/UDP トラフィックを許可する	クライアントに MCP エージェントがインストールされているとき
InterScan for Microsoft Exchange コンソール	低	ファイアウォールを有効にする	ポート 16372 を経由するすべての受信 / 送信の TCP トラフィックを許可する	クライアントが InterScan for Microsoft Exchange コンソールにアクセスする必要があるとき

表 7-1. 初期設定のファイアウォールポリシー（続き）

ポリシー名	セキュリティレベル	クライアント設定	除外	使用を推奨するケース
InterScan Messaging Security Suite コンソール	低	ファイアウォールを有効にする	ポート 80 を経由するすべての受信 / 送信の TCP トラフィックを許可する	クライアントが InterScan MSS コンソールにアクセスする必要があるとき

初期設定のポリシーで指定されていない要件がある場合は、新しいポリシーを作成してください。

初期設定およびユーザが作成したファイアウォールポリシーは、Web コンソールのファイアウォールポリシーリストにすべて表示されます。

ファイアウォールポリシーリストを設定するには

パス：[ネットワーク上のコンピュータ]→[ファイアウォール]→[ポリシー]

1. 新しいポリシーを追加するには、[追加] をクリックします。新しく作成するポリシーの設定が既存のポリシーの設定と類似の場合は、既存のポリシーを選択し、[コピー] をクリックします。

既存のポリシーを編集するには、ポリシー名をクリックします。

ポリシーの設定画面が表示されます。詳細については、234 ページの「ファイアウォールポリシーの追加および変更」を参照してください。

2. 既存のポリシーを削除するには、ポリシーの横のチェックボックスを選択し、[削除] をクリックします。
3. ファイアウォール除外テンプレートを編集するには、[除外テンプレートを編集] をクリックします。除外テンプレートエディタが表示されます。詳細については、236 ページの「ファイアウォール除外テンプレートの編集」を参照してください。

ファイアウォールポリシーの追加および変更

次のそれぞれのポリシーを設定します。

- **セキュリティレベル**：クライアントコンピュータのすべての送受信トラフィックをブロックあるいは許可する一般的な設定です。
- **ファイアウォール機能**：ウイルスバスター Corp. ファイアウォール、侵入検知システム（IDS）、およびファイアウォール違反通知メッセージの有効化 / 無効化を切り替えます。IDS の詳細については、231 ページの「侵入検知システム」を参照してください。

- ・ **ポリシー除外リスト**：さまざまな種類のネットワークトラフィックをブロックまたは許可するために設定できる、除外設定のリストです。

ポリシーを追加するには

パス：[ネットワーク上のコンピュータ]→[ファイアウォール]→[ポリシー]→[追加]

[ネットワーク上のコンピュータ]→[ファイアウォール]→[ポリシー]→[コピー]

1. このポリシーの新しい名前を入力します。
2. セキュリティレベルを選択します。選択されたセキュリティレベルは、ファイアウォールポリシーの除外設定の条件に一致するトラフィックには適用されません。
3. ポリシーに使用するファイアウォール機能を選択します。
 - ・ ファイアウォールが送信パケットをブロックすると、ファイアウォール違反通知メッセージが表示されます。メッセージを変更するには、244 ページの「通知メッセージの内容を変更するには」を参照してください。
 - ・ ファイアウォール機能をすべて有効にすると、機能を有効 / 無効する権限や、クライアントコンソールのファイアウォール設定を変更する権限がクライアントユーザに付与されます。

警告： ウイルスバスター Corp. サーバの Web コンソールを使用して、ユーザが設定するクライアントコンソール設定を無効にすることはできません。

- ・ この機能を有効にしない場合、ウイルスバスター Corp. サーバの Web コンソールで行われたファイアウォール設定が、クライアントコンソールの [ネットワークカードのリスト] の下に表示されます。
 - ・ クライアントコンソールの [ファイアウォール] タブの [設定] の下にある情報には、サーバの Web コンソールからの設定ではなく、クライアントコンソールからの設定が常に反映されます。
4. [除外] でファイアウォールポリシーの除外設定を選択します。ここに含まれるポリシーの除外設定は、ファイアウォール除外テンプレートに基づいています。詳細については、236 ページの「ファイアウォール除外テンプレートの編集」を参照してください。
 - ・ ポリシーの除外名をクリックし、開いたページで設定を変更して、既存のポリシーの除外設定を変更してください。

注意： 変更されたポリシーの除外設定は、これから作成されるポリシーにのみ適用されます。ポリシーの除外設定に対する変更を常に適用したい場合は、ファイアウォール除外テンプレートでポリシーの除外設定に対して同じ変更を行う必要があります。

- [追加] をクリックして、新しいポリシーの除外設定を作成します。開いたページで設定を指定します。

注意： ポリシーの除外設定は、これから作成されるポリシーにのみ適用されます。このポリシーの除外設定を他のポリシーに適用したい場合は、ファイアウォール除外テンプレートにあるポリシーの除外設定リストにまずこのポリシーを追加する必要があります。

5. [保存] をクリックします。

既存のポリシーを変更するには

パス: [ネットワーク上のコンピュータ] → [ファイアウォール] → [ポリシー] → [< ポリシー名 >]

1. 次を変更します。

- ポリシー名
- セキュリティレベル
- ポリシーに使用するファイアウォール機能
- ポリシーに含めるファイアウォールポリシーの除外設定
 - ポリシーの除外名をクリックし、開いたページで設定を変更して、既存のポリシーの除外設定を編集してください。
 - [追加] をクリックして、新しいポリシーの除外設定を作成します。開いたページで設定を指定します。

2. [保存] をクリックして、既存のポリシーに変更を適用します。

ファイアウォール除外テンプレートの編集

ファイアウォール除外テンプレートには、クライアントコンピュータのポート番号または IP アドレスに基づいてさまざまな種類のネットワークトラフィックを許可またはブロックするよう設定できるポリシーの除外設定が含まれます。ポリシーの除外設定を作成してから、ポリシーの除外設定が適用されるポリシーを編集します。

使用するポリシーの除外設定の種類を決定します。2 種類の設定があります。

制限

指定された種類のネットワークトラフィックのみをブロックし、すべてのネットワークトラフィックを許可するポリシーに適用します。制限ポリシー除外の一例は、トロイの木馬がしばしば使用するポートなど、攻撃を受けやすいクライアントポートをブロックすることです。

許可

指定された種類のネットワークトラフィックのみを許可し、すべてのネットワークトラフィックをブロックするポリシーに適用します。たとえば、ウイルスバスター Corp. サーバおよび Web サーバのみにアクセスするクライアントを許可することができます。許可するには、信頼されたポート (ウイルスバスター Corp. サーバとの通信に使用される) および HTTP 通信でクライアントが使用するポートからのトラフィックを許可します。

クライアント待機ポート： [ネットワーク上のコンピュータ] → [クライアント管理] → [ステータス] の順に選択します。ポート番号は「基本的な情報」の下にあります。

サーバ待機ポート： [管理] → [接続設定] の順に選択します。ポート番号は「ネットワーク上のコンピュータの接続設定」の下にあります。

ウイルスバスター Corp. には、一連の初期設定のファイアウォールポリシー除外が搭載されており、変更または削除することができます。

表 7-2. 初期ファイアウォールポリシー除外

除外名	処理	プロトコル	ポート番号	方向
DNS	許可	TCP/UDP	53	送受信
NetBIOS	許可	TCP/UDP	137, 138, 139, 445	送受信
HTTPS	許可	TCP	443	送受信
HTTP	許可	TCP	80	送受信
Telnet	許可	TCP	23	送受信
SMTP	許可	TCP	25	送受信
FTP	許可	TCP	21	送受信
POP3	許可	TCP	110	送受信
LDAP	許可	TCP/UDP	389	送受信

注意： 初期設定の除外設定は、すべてのクライアントに適用されます。初期設定の除外設定を特定のクライアントのみに適用したい場合は、除外設定を編集し、そのクライアントの IP アドレスを指定してください。

以前のウイルスバスター Corp. バージョンからアップグレードした場合は、LDAP 除外設定は使用できません。この除外設定が除外リストにない場合、手動で追加してください。

ポリシーの除外設定を追加するには

パス：[ネットワーク上のコンピュータ]→[ファイアウォール]→[ポリシー]→[除外テンプレートを編集]→[追加]

1. このポリシーの除外設定の新しい名前を入力します。
2. ネットワークトラフィック上でウイルスバスター Corp. が実行する処理 (除外条件に一致するトラフィックをブロックまたは許可) およびトラフィックの方向 (クライアントコンピュータ上の送受信ネットワークトラフィック) を選択します。
3. TCP、UDP、または ICMP から、ネットワークプロトコルの種類を選択します。
4. 処理を実行するクライアントコンピュータのポートを指定します。
5. 除外に含めるクライアントコンピュータの IP アドレスを選択します。たとえば、すべてのネットワークトラフィック (送受信) を拒否することを選択していて、ネットワーク上の 1 つのコンピュータの IP アドレスを入力している場合、ポリシーにこの除外設定があるすべてのクライアントはその IP アドレスとの間でデータの送受信ができなくなります。
6. [保存] をクリックします。

ポリシーの除外設定を編集するには

パス：[ネットワーク上のコンピュータ]→[ファイアウォール]→[ポリシー]→[除外テンプレートを編集]→<除外ポリシーの名前>

1. 次を変更します。
 - ・ ポリシー除外名
 - ・ ネットワークトラフィック上でウイルスバスター Corp. が実行する処理およびトラフィックの方向
 - ・ ネットワークプロトコルの種類
 - ・ ポリシーの除外設定のポート番号
 - ・ クライアントコンピュータの IP アドレス
2. [保存] をクリックします。

エントリを削除するには

パス: [ネットワーク上のコンピュータ] → [ファイアウォール] → [ポリシー] → [除外テンプレートを編集]

1. 削除する除外の横にあるチェックボックスを選択します。
2. [削除] をクリックします。

リスト内で除外の順序を変更するには

パス: [ネットワーク上のコンピュータ] → [ファイアウォール] → [ポリシー] → [除外テンプレートを編集]

1. 移動する除外の横にあるチェックボックスを選択します。
2. [▲] または [▼] をクリックします。新しい位置を反映するために除外の ID 番号が変更されます。

除外リストの設定を保存するには

パス: [ネットワーク上のコンピュータ] → [ファイアウォール] → [ポリシー] → [除外テンプレートを編集]

次の保存オプションから選択します。

- テンプレートの変更を保存: 現在のポリシー除外および設定で除外テンプレートを保存します。このオプションは、既存のポリシーではなく、今後作成されるポリシーに対するテンプレートに適用されます。
- 保存してすべての既存ポリシーに適用: 現在のポリシー除外および設定で除外テンプレートを保存します。このオプションは、既存のポリシーおよび今後作成されるポリシーに対するテンプレートに適用されます。

ファイアウォールプロファイル

ファイアウォールプロファイルによって、クライアントまたはクライアントグループがポリシーを適用する前に持つべき属性を選択できるようになります。プロファイルには、次のものが含まれます。

- **関連ポリシー:** それぞれのプロファイルは 1 つのポリシーを使用します。
- **クライアント属性:** 以下の属性を持つクライアントは関連ポリシーを適用します。
 - **IP アドレス:** 特定の IP アドレスを持つクライアント、IP アドレスの範囲内にある IP アドレス、または IP アドレスが指定されたサブネットに属するクライアント
 - **ドメイン:** 特定のウイルスバスター Corp. ドメインに属するクライアント
 - **コンピュータ名:** 特定のコンピュータ名を持つクライアント

- ・ **プラットフォーム**：特定のプラットフォームを実行しているクライアント
- ・ **ログオン名**：指定されたユーザがログオンしたクライアントコンピュータ
- ・ **クライアントの接続状態**：クライアントが、オンラインとオフラインのいずれであるかを示します。

注意： クライアントがオンラインの場合はウイルスバスター Corp. サーバまたは[参照サーバ](#)のいずれかに接続できますが、オフラインの場合はどのサーバにも接続できません。

- ・ **ユーザ権限**：クライアントユーザによる次の操作の実行を許可または禁止します。
 - ・ ポリシーで指定されたセキュリティレベルの変更
 - ・ ポリシーに関連付けられている除外リストの編集

注意： これらの権限は、プロファイルで指定された属性に一致するクライアントに対してのみ適用されます。選択したクライアントユーザに対して他のファイアウォール権限を割り当てることもできます。詳細については、243 ページの「ファイアウォール権限」を参照してください。

ウイルスバスター Corp. には、「オールアクセスポリシー」ポリシーを使用する「すべてのクライアントプロファイル」という初期設定のプロファイルが用意されています。この初期設定のプロファイルを変更または削除できます。また、新しいプロファイルを作成することもできます。各プロファイルおよび現在のプロファイルステータスに関連付けられたポリシーを含めて、初期設定およびユーザが作成したファイアウォールプロファイルは、Web コンソールのファイアウォールプロファイルリストにすべて表示されます。プロファイルリストを管理し、すべてのプロファイルをウイルスバスター Corp. クライアントに配信します。ウイルスバスター Corp. クライアントは、クライアントコンピュータに対するすべてのファイアウォールプロファイルを保存します。

ファイアウォールプロファイルリストを設定するには

パス：[ネットワーク上のコンピュータ]→[ファイアウォール]→[プロファイル]

1. 新しいプロファイルを追加するには、[追加] をクリックします。既存のプロファイルを編集するには、プロファイル名を選択します。

プロファイルの設定画面が表示されます。詳細については、242 ページの「ファイアウォールプロファイルの追加および編集」を参照してください。

2. 既存のポリシーを削除するには、ポリシーの横のチェックボックスを選択し、[削除] をクリックします。
3. リスト内でプロファイルの順序を変更するには、移動するプロファイルの横にあるチェックボックスを選択して、[▲] または [▼] をクリックします。

ウイルスバスター Corp. は、プロファイルリストに表示される順序で、ファイアウォールプロファイルをクライアントに適用します。たとえば、クライアントが最初のプロファイルに一致する場合、ウイルスバスター Corp. はそのプロファイルに設定された処理をクライアントに適用します。ウイルスバスター Corp. はクライアントに設定されたその他のプロファイルについては無視します。

ヒント： ポリシーが排他的であればあるだけ、リストの上位に表示する必要があります。たとえば、単一クライアントに対して作成したポリシーは最上位に表示され、その後、その範囲のクライアント、ネットワークドメイン、およびすべてのクライアントが続きます。

4. 参照サーバを管理するには、[参照サーバリストを編集] をクリックします。

参照サーバは、ファイアウォールのプロファイルを適用するときに、ウイルスバスター Corp. サーバの代わりとして動作するコンピュータです。ネットワーク上のコンピュータであれば、参照サーバとして機能することができます。参照サーバを有効にしたとき、ウイルスバスター Corp. は次のように想定します。

- 参照サーバに接続されたクライアントは、ウイルスバスター Corp. サーバと通信できない場合でもオンラインです。
- オンラインクライアントに適用されるファイアウォールプロファイルは、参照サーバに接続されているクライアントにも適用されます。

詳細については、263 ページの「参照サーバ」を参照してください。

5. 現在の設定を保存し、クライアントにプロファイルを割り当てるには

- a. [クライアントのセキュリティレベル / 除外リストを上書き] をオンまたはオフにします。このオプションは、すべてのユーザ設定のファイアウォール設定を上書きします。
- b. [クライアントにプロファイルを割り当てる] をクリックします。ウイルスバスター Corp. は、すべてのクライアントに対してプロファイルリストのすべてのプロファイルを割り当てます。

6. プロファイルをクライアントに正常に割り当てたことを確認するには

- a. [ネットワーク上のコンピュータ] → [クライアント管理] に移動します。クライアントツリービュードロップダウンボックスから、[ファイアウォール表示] を選択します。
- b. クライアントツリーの [ファイアウォール] 列の下に緑色のチェックマークが付いていることを確認します。プロファイルに関連付けられているポリシーで侵入検知システムを有効にしている場合にも、[IDS] 列の下に緑色のチェックマークが付いています。
- c. クライアントが正しいファイアウォールポリシーを適用しているかを確認します。ポリシーがクライアントツリーの [ファイアウォールポリシー] 列の下に表示されます。

ファイアウォールプロファイルの追加および編集

クライアントコンピュータは、さまざまなレベルの保護を必要とする場合があります。ファイアウォールプロファイルを使用すると、関連ポリシーを適用するクライアントコンピュータを指定し、ファイアウォール設定を変更する権限をクライアントユーザに付与できます。通常、使用中の各ポリシーに必要なプロファイルは 1 つです。

プロファイルを追加するには

パス: [ネットワーク上のコンピュータ] → [ファイアウォール] → [プロファイル] → [追加]

1. [このプロファイルを有効にする] をクリックして、ウイルスバスター Corp. クライアントにプロファイルを配信できるようにします。
2. プロファイルを識別する名前とオプションの説明を入力します。
3. このプロファイルのポリシーを選択します。
4. ポリシーを適用するクライアントコンピュータを指定します。次の条件に基づいてコンピュータを選択します。
 - IP アドレス
 - ドメイン: ボタンをクリックして開き、クライアントツリーからドメインを選択します。
 - コンピュータ名: ボタンをクリックして開き、クライアントツリーからクライアントコンピュータを選択します。
 - プラットフォーム
 - ログオン名
 - クライアントの接続状況を基準とする場合
5. ファイアウォールセキュリティレベルを変更する権限、または指定した種類のトラフィックを許可する除外設定の設定可能なリストを編集する権限をユーザに付与するかどうかを選択します。これらのオプションの詳細については、234 ページの「ファイアウォールポリシーの追加および変更」を参照してください。
6. [保存] をクリックします。

プロファイルを編集するには

パス: [ネットワーク上のコンピュータ] → [ファイアウォール] → [プロファイル] → [< プロファイル名 >]

1. [このプロファイルを有効にする] をクリックして、ウイルスバスター Corp. クライアントにこのプロファイルを配信できるようにします。

次を変更します。

- プロファイル名および説明

- プロファイルに割り当てられたポリシー
- 次の条件に基づくクライアントコンピュータ：
 - IP アドレス
 - ドメイン：ボタンをクリックしてクライアントツリーを開き、そこからドメインを選択します。
 - コンピュータ名：ボタンをクリックしてクライアントツリーを開き、クライアントツリーからクライアントコンピュータを選択します。
 - プラットフォーム
 - ログオン名
 - クライアントの接続状況を基準とする場合
- 権限：ファイアウォールセキュリティレベルを変更する権限、または指定した種類のトラフィックを許可する除外設定の設定可能リストを編集する権限をユーザに付与するかどうかを選択します。これらのオプションの詳細については、234 ページの「ファイアウォールポリシーの追加および変更」を参照してください。

2. [保存] をクリックします。

ファイアウォール権限

ユーザに次の権限を付与します。

- クライアントコンソールの [ファイアウォール] タブの表示
- ウイルスバスター Corp. ファイアウォールおよびファイアウォール機能の有効化 / 無効化
- クライアントにサーバへのファイアウォールログの送信を許可する

これらの権限の詳細については、288 ページの「ファイアウォール権限」を参照してください。

クライアントユーザ向けのファイアウォール違反通知

ウイルスバスター Corp. では、ファイアウォールポリシーに違反する送信トラフィックをブロックした直後にクライアントコンピュータに通知メッセージを表示できます。特定のファイアウォールポリシーの設定時に、通知メッセージを有効にするまたは通知を有効にする権限をユーザに付与します。必要に応じて、通知メッセージの内容を変更します。

ファイアウォールポリシーを設定するには、234 ページの「ファイアウォールポリシーの追加および変更」を参照してください。

通知メッセージを有効にする権限をユーザに付与するには

パス: [ネットワーク上のコンピュータ] → [クライアント管理] → [権限とその他の設定] → [権限設定] タブ

1. [ファイアウォール権限] の下で、ウイルスバスター Corp. ファイアウォール、IDS（侵入検知システム）、およびファイアウォール違反通知メッセージを有効にすることができます。
2. クライアントツリーのドメインまたはクライアントを選択している場合は、[保存] をクリックすると設定がドメインまたはクライアントに適用されます。ルートアイコンを選択した場合は、次のオプションのいずれかを選択します。
 - **すべてのクライアントに適用**: すべての既存のクライアント、および既存または将来追加されるドメインに加えられる新しいクライアントに、設定を適用します。将来追加されるドメインとは、設定を指定した時点で作成されていないドメインのことです。
 - **将来追加されるドメインにのみ適用**: 将来追加されるドメインに加えられるクライアントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいクライアントには設定を適用しません。

通知メッセージの内容を変更するには

パス: [通知] → [クライアントユーザ通知]

1. [ファイアウォール侵害] タブをクリックします。
2. 表示されたテキストボックスで初期設定のメッセージを変更します。
3. [保存] をクリックします。

ファイアウォールログ

サーバで使用可能なファイアウォールログは、ファイアウォールログの送信権限を持つクライアントによって送信されます。特定のクライアントにこの権限を付与して、ウイルスバスター Corp. ファイアウォールがブロックしているクライアントコンピュータ上のトラフィックを監視および分析します。

ファイアウォール権限の詳細については、288 ページの「ファイアウォール権限」を参照してください。

ハードディスク上の領域を大量に占有しないようにログのサイズを維持するには、手動でログを削除するか、またはログの削除スケジュールを設定します。ログの管理方法の詳細については、265 ページの「ログの管理」を参照してください。

ファイアウォールログを表示するには

パス: [ログ]→[ネットワーク上のコンピュータのログ]→[セキュリティ上の危険]→[ログの表示]→
[ファイアウォールログ]

[ネットワーク上のコンピュータ]→[クライアント管理]→[ログ]→[ファイアウォールログ]

1. 最新のログが使用可能であるかを確認するには、[クライアントに通知する]をクリックします。クライアントがファイアウォールログを送信して次の手順に進むまでには、しばらく時間がかかります。
2. ログの基準を指定して [ログ表示] をクリックします。
3. ログが表示されます。ログには、次の情報が含まれています。
 - ファイアウォール侵害検出の日時
 - ファイアウォール侵害が発生したコンピュータ
 - リモートホスト IP アドレス
 - ローカルホスト IP アドレス
 - プロトコル
 - ポート番号
 - 説明: 実際のセキュリティリスク (ネットワークウイルスまたは IDS 攻撃など) またはファイアウォールポリシー侵害を指定します。
 - 方向: 受信または送信トラフィックがファイアウォールポリシーを侵害した場合
 - プロセス名: ファイアウォール侵害が発生したコンピュータで実行可能なプログラムまたは実行されているサービス
4. ログを CSV ファイルに保存するには、[CSV 形式でエクスポート] をクリックします。ファイルを開くか、特定の場所に保存します。CSV ファイルは、通常、Microsoft Excel などのスプレッドシートアプリケーションで開きます。

ウイルスバスター Corp. ファイアウォールのテスト

ウイルスバスター Corp. ファイアウォールが正常に機能することを確認するために、クライアントまたはクライアントグループでテストします。

警告： ウイルスバスター Corp. クライアントプログラムの設定は、制御された環境でのみテストしてください。ネットワークまたはインターネットに接続しているクライアントコンピュータ上ではテストしないでください。これにより、クライアントコンピュータが、ウイルス、ハッカーの攻撃またはその他のリスクにさらされる可能性があります。

ファイアウォールをテストするには

1. テストポリシーを作成して保存します。テストするトラフィックの種類をブロックするよう設定します。たとえば、クライアントがインターネットにアクセスしないようにするには、次の処理を実行します。
 - a. セキュリティレベルを [低] に設定します (すべての受信 / 送信トラフィックを許可)。
 - b. [ファイアウォールを有効にする] および [ファイアウォール侵害の発生時にユーザに通知する] を選択します。
 - c. HTTP (または HTTPS) トラフィックをブロックする除外設定を作成します。
2. テストプロファイルを作成して保存し、ファイアウォール機能をテストするクライアントを選択します。テストポリシーをテストプロファイルに関連付けます。
3. [クライアントにプロファイルを割り当てる] をクリックします。
4. 配信を確認します。
 - a. [ネットワーク上のコンピュータ] → [クライアント管理] をクリックします。
 - b. クライアントが属するドメインを選択します。
 - c. クライアントツリービューから、[ファイアウォール表示] を選択します。
 - d. クライアントツリーの [ファイアウォール] 列の下に緑色のチェックマークが付いているかを確認します。そのクライアントの侵入検知システムを有効にしている場合にも、[IDS] 列の下に緑色のチェックマークが付いているかを確認します。
 - e. クライアントが正しいファイアウォールポリシーを適用しているかを確認します。ポリシーがクライアントツリーの [ファイアウォールポリシー] 列の下に表示されます。
5. ポリシーで設定した種類のトラフィックの送信または受信を試行して、クライアントコンピュータのファイアウォールをテストします。
6. クライアントがインターネットにアクセスしないように設定したポリシーをテストするには、クライアントコンピュータで Web ブラウザを開きます。ファイアウォール侵害の通知メッセージを表示するよう設定した場合は、送信トラフィックの侵害が発生すると、クライアントコンピュータにメッセージが表示されます。

ウイルスバスター Corp. ファイアウォールの無効化

すべてまたは選択したクライアントコンピュータでウイルスバスター Corp. ファイアウォールを無効にすることができます。

選択したコンピュータでウイルスバスター Corp. ファイアウォールを無効にするには

方法 A: 新しいポリシーを作成し、クライアントに適用します。

1. ファイアウォールを有効にしない新しいポリシーを作成します。新しいポリシーを作成する手順については、234 ページの「ファイアウォールポリシーの追加および変更」を参照してください。
2. クライアントにポリシーを適用します。

方法 B: ファイアウォールドライバおよびサービスを無効にします。

1. ファイアウォールドライバを無効にします。
 - a. [Windows ネットワーク接続のプロパティ] を開きます。
 - b. ネットワークカードの [Trend Micro Common Firewall Driver] チェックボックスをオフにします。
2. ファイアウォールサービスを無効にします。
 - a. コマンドプロンプトを開き、「services.msc」と入力します。
 - b. Microsoft Management Console (MMC) の [OfficeScan NT Firewall] を無効にします。

すべてのクライアントコンピュータでウイルスバスター Corp. ファイアウォールを無効にするには

1. Web コンソールで、[管理] → [製品ライセンス] → [追加サービス] に移動します。
2. [ネットワーク上のコンピュータに対するファイアウォール] 行で、[無効] をクリックします。

第 2 部

ウイルスバスター Corp. サーバ およびクライアントの管理





第8章

ウイルスバスター Corp. サーバの管理

この章で説明する内容には、次の項目が含まれます。

- 252 ページの「役割ベースの管理」
- 260 ページの「Trend Micro Control Manager」
- 263 ページの「参照サーバ」
- 264 ページの「システムイベントログ」
- 265 ページの「ログの管理」
- 268 ページの「ライセンス」
- 270 ページの「ウイルスバスター Corp. データベースバックアップ」
- 272 ページの「ウイルスバスター Corp. Web サーバ情報」
- 272 ページの「Web コンソールパスワード」
- 273 ページの「隔離フォルダ設定」
- 274 ページの「Server Tuner」
- 277 ページの「ウイルストラッキングセンターへのウイルス情報送信」

役割ベースの管理

役割ベースの管理機能を使用して、ウイルスバスター Corp. Web コンソールのメニュー項目およびサブメニュー項目へのアクセス権を付与および制御します。組織に複数のウイルスバスター Corp. 管理者がいる場合、この機能を使用するとサーバ管理タスクをその管理者に委任したり、各管理者がアクセスできるメニュー項目を管理することができます。また、管理者以外には Web コンソールの「表示専用」のアクセス権を付与することができます。

役割ベースの管理には、次のタスクがあります。

1. ユーザの役割の定義。
2. ユーザアカウントの設定および各ユーザへの特定の役割の割り当て。

すべてのユーザが Web コンソールで行った処理は、システムイベントログで確認できます。次の処理がログに記録されます。

- コンソールへのログイン
- パスワードの変更
- コンソールからのログオフ
- セッションタイムアウト (ユーザの自動ログオフ)

ユーザの役割

ユーザの役割により、ユーザがアクセスできる Web コンソールのメニュー項目が決まります。ウイルスバスター Corp. には一連のビルトインのユーザの役割が用意されており、これは変更または削除することができません。ビルトインの役割に要件を満たすものがない場合、カスタムの役割を追加します。それぞれのカスタムの役割は、Web コンソールの特定のメニュー項目およびサブメニュー項目に対して「表示」または「設定」アクセス権を持つように設定します。

ビルトインおよびカスタムの役割は、Web コンソールの [ユーザの役割] リストに表示されます。

注意： クライアントツリー上の特定のウイルスバスター Corp. ドメインへのアクセス権を、役割ごとに制御することはできません。クライアントツリーが表示されていれば、すべてのドメインが表示されます。

ビルトインの役割は次のとおりです。

管理者

管理者の役割を持つユーザは、すべてのメニュー項目を設定できます。この役割は、他のウイルスバスター Corp. 管理者またはウイルスバスター Corp. について十分な知識を持つユーザに委任します。

パワーユーザ

この役割は、Web コンソールで特定の管理タスクを行う管理者に委任します。

1. パワーユーザの役割を持つユーザは、次のメニュー項目およびサブメニュー項目を設定できます。

[ネットワーク上のコンピュータ] → [クライアントインストール]

このメニュー項目は、ユーザに、ウイルスバスター Corp. クライアントの2つのインストール方法を提供します。詳細については、88 ページの「ウイルスバスター Corp. Web コンソールからのインストール」および 76 ページの「ブラウザベースのインストールの開始」を参照してください。

[ネットワーク上のコンピュータ] → [ファイアウォール]

ユーザはこのメニュー項目を使用して、ファイアウォールポリシーおよびプロファイルを管理できます。詳細については、232 ページの「ファイアウォールプロファイルおよびポリシー」を参照してください。

ログ

ユーザはこのメニュー項目を使用して、ログを表示および管理できます。詳細については、265 ページの「ログの管理」を参照してください。

ScanNow (メインメニューの一番上)

ユーザはこのメニュー項目を使用して、対象コンピュータ上で手動検索を開始できます。詳細については、180 ページの「ScanNow の開始」を参照してください。

クライアントツリー設定

クライアントツリーが表示されていれば、ユーザに表示されるすべての設定を行うことができます。詳細については、48 ページの「クライアントツリーの特定のタスク」を参照してください。

2. ユーザは、次のメニュー項目にアクセスできません。
 - プラグインマネージャ
 - [管理] → [ユーザの役割]
 - [管理] → [ユーザアカウント]

3. ユーザは、他のすべてのメニュー項目にアクセスできます。

ゲストユーザ

この役割は、Web コンソールを参照用に表示するユーザに委任します。

1. ゲストユーザの役割を持つユーザは、次のメニュー項目にアクセスできません。

- プラグインマネージャ
- [管理] → [ユーザの役割]
- [管理] → [ユーザアカウント]

2. ユーザは、他のすべてのメニュー項目にアクセスできます。

ユーザの役割リストを設定するには

パス: [管理] → [ユーザの役割]

1. カスタムの役割を追加するには、[追加] をクリックします。追加する役割に既存のカスタムの役割と類似した設定がある場合、既存の役割を選択し、[コピー] をクリックします。

カスタムの役割を変更するには、役割の名前をクリックします。

役割の設定画面が表示されます。詳細については、255 ページの「カスタムの役割の追加および変更」を参照してください。

2. カスタムの役割を削除するには、役割の横のチェックボックスを選択し、[削除] をクリックします。
3. カスタムの役割を .dat ファイルに保存するには、カスタムの役割を選択し、[エクスポート] をクリックします。別のウイルスバスター Corp. サーバを管理している場合、.dat ファイルを使用して、カスタムの役割をそのサーバにインポートします。
4. 他のウイルスバスター Corp. サーバでカスタムの役割を保存し、その役割を現在のウイルスバスター Corp. サーバにインポートする場合、[インポート] をクリックして、カスタムの役割が格納された .dat ファイルの場所を探します。

注意： [ユーザの役割] 画面に表示される役割は、同じ名前の役割をインポートしたときに上書きされます。

カスタムの役割の追加および変更

カスタムの役割を追加するには

パス: [管理] → [ユーザの役割] → [追加]

[管理] → [ユーザの役割] → [コピー]

1. 役割の名前を入力します。必要に応じて説明も入力します。
2. [使用可能なメニュー項目] リストに、Web コンソールのメインメニューとサブメニュー項目が表示されます。1 つ以上のメニュー項目に対して「表示」または「設定」アクセス権を持つように役割を設定します。

注意: [設定] の下のチェックボックスをオンにすると、[表示] の下のチェックボックスも自動的にオンになります。

ビルトインの管理者の役割を持つユーザと、ウイルスバスター Corp. のインストール時に作成されたルートアカウントを使用するユーザのみが、役割とアカウントを設定できます。

カスタムの役割に、プラグインマネージャに対する「設定」アクセス権を持たせたり、アクセス権を持たせないようにすることもできます。これは、プラグインマネージャが独立したプログラムであり、ウイルスバスター Corp. によってその機能が制御されることはないためです。

3. [保存] をクリックします。新しい役割が [ユーザの役割] リストに表示されます。

カスタムの役割を変更するには

パス: [管理] → [ユーザの役割] → <役割名>

1. 次の項目を変更します。
 - 説明
 - アクセスできるメニュー項目
2. [保存] をクリックします。

ユーザアカウント

ユーザアカウントを設定して、各ユーザに特定の役割を割り当てます。ユーザの役割により、ユーザが表示または設定できる Web コンソールのメニュー項目が決まります。

ウイルスバスター Corp. サーバのインストール時に、「ルート」というビルトインのアカウントが自動的に作成されます。ルートアカウントを使用してログオンするユーザは、すべてのメニュー項目にアクセスできます。ルートアカウントは削除できませんが、パスワードや表示名などのアカウントの詳細は変更できます。ルートアカウントのパスワードを忘れた場合は、パスワードの再設定についてサポート担当者にお問い合わせください。

カスタムアカウントまたは Active Directory アカウントを追加します。すべてのユーザアカウントは、Web コンソールの [ユーザアカウント] リストに表示されます。

ウイルスバスター Corp. のユーザアカウントを使用して、「シングルサインオン」を実行できます。シングルサインオン機能により、ユーザは、Trend Micro Control Manager (以下、Control Manager) のコンソールからウイルスバスター Corp. Web コンソールにアクセスできます。詳細については、次の手順を参照してください。

ユーザアカウントリストを設定するには

パス: [管理] → [ユーザアカウント]

1. カスタムまたは Active Directory アカウントを追加するには、[追加] をクリックします。カスタムアカウントを変更するには、アカウント名をクリックします。
アカウントの設定画面が表示されます。詳細については、257 ページの「ユーザアカウントの追加および変更」を参照してください。
2. 1 つ以上の Active Directory アカウントを追加するには、[Active Directory から追加] をクリックします。詳細については、259 ページの「1 つ以上の Active Directory アカウントの追加」を参照してください。
3. 1 つ以上のアカウントの役割を変更するには、アカウントを選択して [役割の変更] をクリックします。表示された画面で、新しい役割を選択し、[保存] をクリックします。
4. アカウントを有効または無効にするには、[有効] の下のアイコンをクリックします。

注意: ルートアカウントを無効にすることはできません。

5. アカウントを削除するには、アカウントを選択して、[削除] をクリックします。

Control Manager でウイルスバスター Corp. のユーザアカウントを使用するには

詳細な手順については、Control Manager のドキュメントを参照してください。

1. Control Manager で新しいユーザアカウントを作成します。ユーザ名を指定する場合、ウイルスバスター Corp. Web コンソールに表示されているアカウント名を入力します。
2. 新しいアカウントの「アクセス」権限および「設定」権限を、ウイルスバスター Corp. サーバに割り当てます。

注意： Control Manager ユーザに、ウイルスバスター Corp. に対する「アクセス」権限および「設定」権限があっても、ウイルスバスター Corp. のアカウントがない場合、そのユーザはウイルスバスター Corp. にアクセスできません。そのユーザには、ウイルスバスター Corp. Web コンソールのログオン画面を開くためのリンクを含むメッセージが表示されます。

Control Manager のルートアカウントを使用してログオンするユーザは、ウイルスバスター Corp. のアカウントがなくてもウイルスバスター Corp. にアクセスできます。

ユーザアカウントの追加および変更

Web コンソールのアクセス権限をユーザに割り当てるには、Active Directory アカウントを [ユーザアカウント] リストに追加します。

カスタムまたは Active Directory アカウントを追加するには

パス: [管理] → [ユーザアカウント] → [追加]

1. [このアカウントを有効にする] をクリックすると、ユーザはこのアカウントを使用できます。

注意： ユーザのログオン中にそのアカウントを無効にすると、ユーザがログアウトした後にアカウントが無効になります。

2. カスタムアカウントまたは Active Directory アカウントを追加するかどうかを選択します。
 - ・ カスタムアカウントの場合、ユーザ名、名前、およびパスワード (確認用も入力する必要があります) を入力します。必要に応じて、このアカウントのメールアドレスも入力します。

注意： メールアドレスは、参照のみに使用されます。メールアカウントの所有者に、作成されたアカウントについてメールで通知されることはありません。

- Active Directory アカウントの場合、アカウント名（ユーザ名またはグループ）、およびアカウントが属するドメインを指定します。

完全なアカウント名およびドメイン名を入力してください。アカウント名およびドメイン名が完全でない場合、結果は返されません。

グループに属するすべてのメンバーは、同じ役割を取得します。特定のアカウントが少なくとも 2 つのグループに属し、両方のグループの役割が異なる場合、次のように処理されます。

- 両方の役割の権限はマージされます。ユーザが特定の設定を行い、その設定の権限の間に競合が発生した場合、高い方の権限が適用されます。
- すべてのユーザの役割は、システムイベントログに表示されます。例：「ユーザ「JohnDoe」が次の役割を使用してログインしました：パワーユーザ（ビルトイン）」

3. アカウントの役割を選択します。
4. [保存] をクリックします。
5. カスタムアカウントを追加した場合、アカウントの詳細をユーザに送信します。Active Directory アカウントを追加した場合、各自のドメイン名とパスワードを使用して Web コンソールにログオンするようユーザに通知します。
6. ユーザのコンピュータで Windows 2000 が稼働している場合、ユーザに次の項目をインストールするよう通知します。
 - Microsoft パッチ KB890859
 - Microsoft パッチ KB924270
 - Windows 2000 Authorization Manager Runtime

注意： Authorization Manager Runtime は、英語、フランス語、ドイツ語、および日本語バージョンのみをサポートします。

カスタムアカウントを変更するには

パス：[管理]→[ユーザアカウント]→<ユーザ名>

1. 所定のチェック ボックスを使用して、アカウントを有効または無効にします。

注意： Active Directory グループアカウントを無効にすることはできません。グループのユーザを Web コンソールにアクセスさせないようにするには、ユーザアカウントリストからそのグループを削除します。

2. 次の項目を変更します。

- 名前
 - パスワード
 - メールアドレス
 - 役割
3. [保存] をクリックします。

1 つ以上の Active Directory アカウントの追加

1 つ以上の Active Directory アカウントを追加するには

パス: [管理] → [ユーザアカウント] → [Active Directory から追加]

1. アカウントが属するドメインとユーザ名を指定して、アカウント (ユーザ名またはグループ) を検索します。

複数のアカウントを検索するには、ワイルドカード文字 (*) を使用します。ワイルドカード文字を指定しない場合、完全なアカウント名を指定します。アカウント名が完全でない場合、結果は返されません。

2. 有効なアカウントが見つかると、[ユーザおよびグループ] の下にアカウント名が表示されます。転送アイコン (->) をクリックすると、[選択されたユーザおよびグループ] の下にアカウントが移動します。

Active Directory グループを指定すると、グループに属するすべてのメンバーは同じ役割を取得します。特定のアカウントが少なくとも 2 つのグループに属し、両方のグループの役割が異なる場合、次のように処理されます。

- 両方の役割の権限はマージされます。ユーザが特定の設定を行い、その設定の権限の間に競合が発生した場合、高い方の権限が適用されます。
- すべてのユーザの役割は、システムイベントログに表示されます。例: 「ユーザ「JohnDoe」が次の役割を使用してログインしました: パワーユーザ (ビルトイン)」

3. アカウントの役割を選択します。
4. [保存] をクリックします。
5. 各自のドメイン名とパスワードを使用して、Web コンソールにログオンするようユーザに通知します。
6. ユーザのコンピュータで Windows 2000 が稼働している場合、ユーザに次の項目をインストールするよう通知します。
 - Microsoft パッチ KB890859
 - Microsoft パッチ KB924270

- Windows 2000 Authorization Manager Runtime

注意： Authorization Manager Runtime は、英語、フランス語、ドイツ語、および日本語バージョンのみをサポートします。

Trend Micro Control Manager

Control Manager は、ゲートウェイ、メールサーバ、ファイルサーバ、および企業のデスクトップレベルで、トレンドマイクロ製品およびサービス、サードパーティのウイルス対策製品、およびコンテンツセキュリティ製品を管理する中央管理コンソールです。Control Manager は Web ベースの管理コンソールであり、ネットワークを介して管理対象の製品およびサービスを一元的に監視できます。

システム管理者は Control Manager を使用して、感染、セキュリティ違反、ウイルスの侵入ポイントなどの処理を監視およびレポートできます。システム管理者は、ネットワークを介してコンポーネントをダウンロードおよび配信して、保護機能が一貫して最新に保たれるようにすることができます。Control Manager では手動または事前予約アップデートが可能で、グループとしてまたは個別に製品を設定および管理できることで柔軟性が加わります。

サポートされる Control Manager のバージョン

このバージョンのウイルスバスター Corp. では、Control Manager 5.0 および 3.5 をサポートしています。これらの Control Manager のバージョンには最新の Patch および重要な HotFix を適用して、Control Manager でウイルスバスター Corp. を管理できるようにしてください。最新の Patch と HotFix を入手するには、次のトレンドマイクロの最新版ダウンロードサイトにアクセスするか、サポート担当者にお問い合わせください。

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

ウイルスバスター Corp. をインストールしたら、Control Manager に登録して Control Manager 管理コンソールでウイルスバスター Corp. の設定を行います。ウイルスバスター Corp. サーバの管理については、Control Manager のドキュメントを参照してください。

このウイルスバスター Corp. のリリースでの Control Manager との統合

このウイルスバスター Corp. のリリースには、Control Manager からウイルスバスター Corp. サーバを管理するために次の機能が用意されています。

- Control Manager コンソールでは、次の情報を表示できます。
 - 「挙動監視コンポーネント」およびバージョン情報
 - クライアントで使用される検索方法（従来型またはスマートスキャン）

- スマートスキャンサーバとのクライアント接続状態
- スマートスキャンサーバのアドレス (URL 形式)。
- スマートスキャンエージェントパターンファイル情報
- スマートスキャンエージェントパターンファイルは、Control Manager コンソールからアップデイトできます。
- Control Manager コンソールを使用して、次の設定をあるウイルスバスター Corp. サーバから別のウイルスバスター Corp. サーバに複製します。
 - すべての検索の種類に対する検索設定 (「リアルタイム検索」、「手動検索」、「予約検索」、および「ScanNow」)
 - 「クライアントの権限とその他の設定」
 - 「Web レピュテーションポリシー」
 - 「ファイアウォールポリシー」
 - 「ファイアウォールプロファイル」

注意： 特定のサービスのライセンスがアクティベートされていないウイルスバスター Corp. サーバに、これらの設定が複製された場合、その設定はライセンスがアクティベートされたときに有効になります。たとえば、Web レピュテーションおよびスパイウェア対策のライセンスがアクティベートされていない場合、Web レピュテーションポリシーはウイルスバスター Corp. サーバに複製されますが、ライセンスがアクティベートされたときに初めて有効になります。

ウイルスバスター Corp. を Control Manager に登録するには

パス：[管理] → [Control Manager 設定]

1. エンティティ表示名を指定します。これは、Control Manager に表示されるウイルスバスター Corp. サーバの名前です。初期設定では、エンティティ表示名には、サーバコンピュータのホスト名とこの製品の名前が表示されます (例：Server01_OSCE)。

注意： Control Manager では、Control Manager によって管理されるウイルスバスター Corp. サーバやその他の製品を「エンティティ」と呼んでいます。

2. このサーバとの接続に使用される Control Manager サーバの FQDN または IP アドレスとポート番号を指定します。必要に応じて、HTTPS を使用すると接続時のセキュリティが高まります。
3. Control Manager の IIS Web サーバに認証が必要な場合、ユーザ名とパスワードを入力します。

4. プロキシサーバを使用して Control Manager サーバに接続する場合、次のプロキシ設定を指定します。
 - プロキシプロトコル
 - サーバの FQDN または IP アドレスとポート
 - プロキシサーバ認証用のユーザ ID とパスワード
5. ポート転送に**一方向通信**と**双方向通信**のどちらを使用するかを決定し、IP アドレスとポートを指定します。
6. ウイルスバスター Corp. が、指定した設定に基づいて Control Manager サーバに接続できるかどうかをチェックするには、[接続テスト] をクリックします。接続が正しく確立されていれば、[登録] をクリックします。
7. 登録後にこの画面のいずれかの設定を変更した場合、設定を変更した後に [アップデート設定] をクリックして、Control Manager サーバに変更を通知します。
8. Control Manager サーバでウイルスバスター Corp. を管理しないようにする場合、[登録取り消し] をクリックします。

Control Manager 管理コンソールでウイルスバスター Corp. の状態を確認するには

1. Control Manager 管理コンソールを開きます。

Control Manager コンソールを開くには、ネットワーク上の任意のコンピュータで Web ブラウザを開き、次の URL を入力します。

Control Manager 3.5 の場合

`https://<Control Manager server name>/ControlManager`

Control Manager 5.0 の場合

`https://<Control Manager server name>/Webapp/login.aspx`

ここで、<Control Manager server name> は Control Manager サーバの IP アドレスまたはホスト名です。
2. メインメニューで、[製品] をクリックします。
3. リストから [管理下の製品] を選択します。
4. ウイルスバスター Corp. サーバアイコンが表示されているかどうかを確認します。

参照サーバ

ウイルスバスター Corp. クライアントでファイアウォールプロファイルと「Web レピュテーションポリシー」のどちらを使用しているかを確認する方法の 1 つは、ウイルスバスター Corp. サーバとの接続状態をチェックすることです。内部クライアント（企業のネットワーク内のクライアント）がサーバに接続できない場合、クライアントの状態はオフラインになります。この場合、このクライアントには、外部クライアント用のファイアウォールプロファイルまたは Web レピュテーションポリシーが適用されます。この問題に対処するのが参照サーバです。

ウイルスバスター Corp. サーバとの接続が切断されたクライアントは、参照サーバとの接続を試行します。クライアントが参照サーバとの接続の確立に成功すると、内部クライアント用のファイアウォールプロファイルまたは Web レピュテーションポリシーが適用されます。

次の点に注意してください。

- サーバの機能（Web サーバ、SQL サーバ、FTP サーバなど）を持つコンピュータを、参照サーバとして割り当てます。最大 32 の参照サーバを指定できます。
- クライアントは、参照サーバリスト上の 1 番目の参照サーバに接続します。接続が確立できない場合、クライアントはリスト上の 2 番目のサーバへの接続を試行します。
- ウイルスバスター Corp. クライアントは、使用するファイアウォールプロファイルまたは Web レピュテーションポリシーを決定する場合のみ参照サーバを使用します。参照サーバでは、クライアントを管理したり、アップデートやクライアント設定を配信することはありません。このようなタスクは、ウイルスバスター Corp. サーバが実行します。
- クライアントは、ログを参照サーバに送信したり、参照サーバをアップデート元として使用することはできません。

参照サーバリストを管理するには

パス: [ネットワーク上のコンピュータ] → [ファイアウォール] → [プロファイル] → [参照サーバリストを編集]

[ネットワーク上のコンピュータ] → [コンピュータの位置] → [参照サーバリストの編集]

1. [参照サーバリストを有効にする] を選択します。
2. コンピュータをリストに追加するには、[追加] をクリックします。
 - a. 次のように、コンピュータの IP アドレス、名前、または完全修飾ドメイン名 (FQDN) を指定します。
 - computer.networkname
 - 12.10.10.10
 - mycomputer.domain.com

- b. クライアントがこのコンピュータとの通信に使用するポートを入力します。参照サーバで開いている任意の接続ポート（ポート 20、23、80 など）を指定します。

注意： 同じ参照サーバに別のポート番号を指定するには、手順 2a と 2b を繰り返します。クライアントはリスト上の 1 番目のポート番号を使用し、接続に失敗すると、2 番目のポート番号を使用します。

- c. [保存] をクリックします。
3. リスト上のコンピュータの設定を編集するには、コンピュータ名をクリックします。コンピュータ名またはポートを変更して、[保存] をクリックします。
4. コンピュータをリストから削除するには、コンピュータ名を選択して [削除] をクリックします。
5. コンピュータを参照サーバとして機能できるようにするには、[クライアントに割り当てる] をクリックします。

システムイベントログ

ウイルスバスター Corp. では、起動や終了などのサーバプログラムに関するイベントを記録します。これらのログを使用して、ウイルスバスター Corp. サーバおよびサービスが適切に稼働していることを確認します。

ハードディスク上の領域を大量に占有しないようにログのサイズを維持するには、手動でログを削除するか、またはログの削除スケジュールを設定します。ログの管理方法の詳細については、265 ページの「ログの管理」を参照してください。

システムイベントログを表示するには

パス: [ログ] → [システムイベントログ]

1. [詳細] で、詳細な処理が必要なログを確認します。ウイルスバスター Corp. では次のイベントをログに記録します。

ウイルスバスター Corp. マスターサービスおよびデータベースサーバ:

- マスターサービスの起動
- マスターサービスの正常停止
- マスターサービスの異常停止

大規模感染予防サービス:

- 大規模感染予防サービスの有効化

- 大規模感染予防サービスの無効化
- 最後の <number of minutes> 分の共有フォルダセッションの数

データベースバックアップ:

- データベースバックアップの成功
- データベースバックアップの失敗

役割ベースの Web コンソールのアクセス:

- コンソールへのログオン
- パスワードの変更
- コンソールからのログオフ
- セッションタイムアウト (ユーザの自動ログオフ)

2. ログを CSV ファイルに保存するには、[CSV 形式でエクスポート] をクリックします。ファイルを開くか、特定の場所に保存します。CSV ファイルは、通常、Microsoft Excel などのスプレッドシートアプリケーションで開きます。

ログの管理

ウイルスバスター Corp. では、セキュリティリスクの検出、イベント、およびアップデートに関する包括的なログを保持します。これらのログを使用して、組織の保護ポリシーを評価し、感染や攻撃のリスクが高いクライアントを特定します。また、これらのログは、クライアントとサーバ間の接続のチェック、およびコンポーネントのアップデートが成功したかどうかの確認にも使用できます。

ウイルスバスター Corp. では次のログを生成します。

セキュリティリスクログ

ウイルスバスター Corp. では、ウイルス / 不正プログラムまたはスパイウェア / グレーウェアの検出時と、スパイウェア / グレーウェアの復元時にログが生成されます。セキュリティリスクログの詳細については、次の項目を参照してください。

- 202 ページの「ウイルス / 不正プログラムログ」
- 208 ページの「スパイウェア / グレーウェアログ」
- 210 ページの「スパイウェア / グレーウェア復元ログ」

ファイアウォールログ

ウイルスバスター Corp. では、ファイアウォールポリシーの違反の検出時にログが生成されます。詳細については、244 ページの「ファイアウォールログ」を参照してください。

Web レピュテーションログ

ウイルスバスター Corp. では、既知のまたは潜在的に不正な Web サイトをブロックしたときにログが生成されます。詳細については、227 ページの「Web レピュテーションログ」を参照してください。

接続状態の確認ログ

ウイルスバスター Corp. では接続状態の確認ログを生成して、ウイルスバスター Corp. サーバが、登録されているすべてのクライアントと通信できるかどうかを確認できます。詳細については、315 ページの「接続状態の確認ログ」を参照してください。

コンポーネントアップデートログ

ウイルスバスター Corp. では、サーバおよびクライアントがコンポーネントのアップデートを実行したときにログが生成されます。このログを表示して、ウイルスバスター Corp. で保護機能を最新に保持するのに必要なコンポーネントのダウンロードが成功したかどうかを確認します。アップデートログの詳細については、次の項目を参照してください。

- 136 ページの「サーバアップデートログ」
- 150 ページの「クライアントアップデートログ」

デバイスコントロールログ

ウイルスバスター Corp. では、クライアントコンピュータに接続されたデバイスへの不正アクセスが検出されたときにログが生成されます。この場合、クライアントは 1 日 1 回サーバにログを送信します。詳細については、219 ページの「デバイスコントロールログ」を参照してください。

システムイベントログ

ウイルスバスター Corp. ではシステムアップデートログを生成して、ウイルスバスター Corp. サーバが正常に機能し続けるためのイベント（データベースバックアップやマスターサービスの再起動など）に関する情報を提供しています。詳細については、264 ページの「システムイベントログ」を参照してください。

デバッグログ

デバッグログを使用して、ウイルスバスター Corp. サーバおよびクライアントに関する問題のトラブルシューティングを行います。デバッグログの詳細については、次の項目を参照してください。

- 368 ページの「ウイルスバスター Corp. サーバログ」
- 374 ページの「ウイルスバスター Corp. クライアントログ」

ログ管理

ハードディスク上の領域を大量に占有しないようにログのサイズを維持するには、Web コンソールで手動でログを削除するか、またはログの削除スケジュールを設定します。

注意： デバッグログの場合、デバッグログを無効にしてログの収集を停止します。

スケジュールに基づいてログを削除するには

パス：[ログ]→[ログ管理]

1. [ログの自動削除を有効にする] を選択します。
2. 削除するログタイプを選択します。
3. 選択したすべてのログタイプのログを削除するか、特定の日数より古いログのみを削除するかを選択します。
4. ログを削除する頻度と時刻を指定します。
5. [保存] をクリックします。

手動でログを削除するには

パス：[ログ]→[ネットワーク上のコンピュータのログ]→[セキュリティ上の危険]→[ログの削除]

[ネットワーク上のコンピュータ]→[クライアント管理]→[ログ]→[ログの削除]

1. 削除するログタイプを選択します。
2. 選択したすべてのログタイプのログを削除するか、特定の日数より古いログのみを削除するかを選択します。
3. [削除] をクリックします。

ライセンス

Web コンソールでは、ウイルスバスター Corp. 製品のサービスライセンスを表示、アクティベート、および更新したり、ウイルスバスター Corp. ファイアウォールを有効または無効にします。ウイルスバスター Corp. のファイアウォールはウイルス対策サービスに含まれています。このサービスには、Cisco NAC および大規模感染予防のサポートも含まれています。

注意： インストール時にウイルスバスター Corp. ファイアウォールを有効にできます。ファイアウォールを無効にすると、サーバおよびクライアントでファイアウォール機能がすべて非表示になります。

次の場合、Web コンソールをログオフした後、再度ログオンします。

- 次の製品サービスのライセンスをアクティベートした後
 - ウイルス対策
 - Web レピュテーションおよびスパイウェア対策

注意： サービスの機能を完全に有効にするには、再ログインが必要です。

- ウイルスバスター Corp. ファイアウォールを有効または無効にした後

ライセンス情報を表示するには

パス：[管理]→[製品ライセンス]

[管理]→[製品ライセンス]→[製品ライセンス情報]

[管理]→[製品ライセンス]→[製品ライセンス情報]→[製品ライセンスの新しいアクティベーションコード]

1. 画面の一番上にライセンスステータス概要が表示されます。

次の場合、ライセンスに関するメッセージが表示されます。

製品版ライセンスを使用しているとき

- 製品の更新猶予期間である場合。更新猶予期間は地域によって異なります。更新猶予期間については、トレンドマイクロの販売代理店にお問い合わせください。

- ・ ライセンスの有効期間が終了し、更新猶予期間が経過した場合。この間、テクニカルサポートを受けたり、コンポーネントのアップデートを実行することはできません。検索エンジンでコンピュータを検索することはできますが、その際には旧版コンポーネントが使用されます。これらの旧版コンポーネントでは、最新のセキュリティリスクから完全には保護できない可能性があります。

体験版ライセンスを使用しているとき

- ・ ライセンスの有効期限が切れた場合。この間、ウイルスバスター Corp. では、コンポーネントのアップデート、検索、およびすべてのクライアント機能が無効になります。
2. ライセンス情報を表示します。[ライセンス情報] セクションには次の情報が表示されます。
- ・ サービス: ウイルスバスター Corp. 製品のすべてのサービスが表示されます。
 - ・ ステータス: [アクティベーション完了]、[アクティベーション未完了]、または [サポート契約終了] が表示されます。製品のサービスに複数のライセンスがある場合、少なくとも 1 つのライセンスがアクティブであれば、表示されるステータスは [アクティベーション完了] になります。
 - ・ バージョン: [完全] または [体験版] バージョンのいずれかが表示されます。製品版と体験版の両方がある場合、表示されるバージョンは [完全] になります。
 - ・ 失効日: 製品サービスに複数のライセンスがある場合、最も遅い日付の有効期限が表示されます。たとえば、2007 年 12 月 31 日と 2008 年 6 月 30 日の有効期限のライセンスがある場合、2008 年 6 月 30 日が表示されます。

注意: アクティベートされていない製品サービスのバージョンおよび有効期限は、[該当なし] と表示されます。

3. ウイルスバスター Corp. では、製品サービスの複数のライセンスをアクティベートすることができます。製品サービス名をクリックすると、そのサービスのすべてのライセンス (アクティブおよび期限切れ) が表示されます。

ライセンスをアクティベートまたは更新するには

パス: [管理] → [製品ライセンス]

[管理] → [製品ライセンス] → [製品ライセンス情報]

[管理] → [製品ライセンス] → [製品ライセンス情報] → [製品ライセンスの新しいアクティベーションコード]

1. 製品サービスの名前をクリックします。
2. 開いた [製品ライセンス情報] 画面で、[新しいコード] をクリックします。

3. 表示された画面で、アクティベーションコードを入力して、[保存]をクリックします。

注意： サービスをアクティベートする前に登録してください。レジストレーションキーおよびアクティベーションコードの詳細については、トレンドマイクロの販売代理店にお問い合わせください。

4. [製品ライセンス情報] 画面に戻ったら、[ステータスをオンラインで確認]をクリックして、新しいライセンスの詳細とサービスの状態で画面を更新します。この画面には、トレンドマイクロの Web サイトへのリンクも表示されます。このリンクに進むと、ライセンスに関する詳細情報を表示できます。

ウイルスバスター Corp. データベースバックアップ

ウイルスバスター Corp. サーバデータベースには、検索設定や権限など、すべてのウイルスバスター Corp. の設定が格納されています。サーバデータベースが破損した場合でも、バックアップがあれば復元できます。データベースのバックアップはいつでも手動で実行できます。また、バックアップのスケジュールを設定することもできます。

データベースをバックアップする際、ウイルスバスター Corp. により自動的にデータベースがデフラグされ、インデックスファイルの潜在的な破損が修復されます。

システムイベントログをチェックして、バックアップの状態を確認します。詳細については、264 ページの「システムイベントログ」を参照してください。

ヒント： 自動バックアップのスケジュールを設定することをお勧めします。データベースのバックアップは、サーバのトラフィックが小さいオフピーク時に実行してください。

警告： 他のツールまたはソフトウェアでバックアップを実行しないでください。データベースバックアップの設定は、ウイルスバスター Corp. Web コンソールでのみ行ってください。

ウイルスバスター Corp. データベースをバックアップするには

パス：[管理]→[データベースバックアップ]

1. データベースを保存する場所を入力します。フォルダが存在しない場合、[フォルダが存在しない場合フォルダを作成する]を選択します。ドライブと完全なディレクトリのパスを入力しま

す (例: C:\OfficeScan\DatabaseBackup)。初期設定では、<「サーバのインストールフォルダ」>\DBBackup ディレクトリにバックアップが保存されます。

バックアップパスの下にサブフォルダが作成されます。フォルダ名はバックアップの日時を示し、YYYYMMDD_HHMMSS という形式になります。7 個の最新のバックアップフォルダが保存され、それより古いフォルダは自動的に削除されます。

2. バックアップパスが (UNC パスを使用して) リモートコンピュータ上にある場合、適切なアカウント名と対応するパスワードを入力します。このアカウントにコンピュータへの書き込み権限があることを確認してください。
3. バックアップスケジュールを設定するには
 - a. [自動データベースバックアップを有効にする] を選択します。
 - b. バックアップの頻度と時刻を指定します。
 - c. データベースをバックアップして、変更を保存するには、[バックアップ] をクリックします。データベースをバックアップせずに保存のみを行う場合は、[保存] をクリックします。

データベースバックアップファイルを復元するには

1. OfficeScan Master Service を停止します。
2. <「サーバのインストールフォルダ」>\PCCSRV\HTTPDB にあるデータベースファイルを、バックアップファイルで上書きします。
3. OfficeScan Master Service を再起動します。

ウイルスバスター Corp. Web サーバ情報

ウイルスバスター Corp. サーバのインストール時に、Web サーバ (IIS または Apache Web サーバ) の設定が自動的に行われます。これにより、ネットワーク上のコンピュータをウイルスバスター Corp. サーバに接続できます。ネットワーク上のコンピュータクライアントが接続する Web サーバを設定します。

Web サーバの設定を外部から (たとえば、IIS 管理コンソールから) 変更する場合、ウイルスバスター Corp. で変更を複製し、サーバとクライアント間の通信が維持され、Web コンソールにアクセスできるようにします。たとえば、ネットワーク上のコンピュータのサーバの IP アドレスを手動で変更した場合、または動的 IP アドレスを割り当てる場合、ウイルスバスター Corp. のサーバ設定を再設定する必要があります。

接続設定を行うには

パス: [管理] → [接続設定]

1. Web サーバのドメイン名 /IP アドレスおよびポート番号を入力します。

注意: ポート番号は、ウイルスバスター Corp. サーバがウイルスバスター Corp. クライアントとの通信に使用する [信頼されたポート](#) です。

2. [保存] をクリックします。

Web コンソールパスワード

Web コンソールのパスワード (またはウイルスバスター Corp. サーバのインストール時に作成したルートアカウントのパスワード) を管理する画面は、役割ベースの管理を使用するのに必要なリソースがサーバコンピュータにない場合にのみアクセスできます。たとえば、サーバコンピュータで Windows 2000 が稼働しており、Authorization Manager Runtime がインストールされていない場合、この画面にアクセスできます。リソースが十分であれば、この画面は表示されず、「ユーザアカウント」画面でルートアカウントを変更してパスワードを管理できます。

コンソールのパスワードを忘れた場合、ウイルスバスター Corp. サーバが Control Manager に登録されていれば、ルートアカウントを使用して Control Manager コンソールにログオンし、パスワードを変更します。または、ウイルスバスター Corp. サーバにアクセスできる Control Manager アカウントがある場合、パスワードを変更することができます。

ウイルスバスター Corp. が Control Manager に登録されていない場合、サポート担当者に Web コンソールへのアクセス方法をお問い合わせください。

Web コンソールのパスワードを変更するには

パス: [管理] → [コンソールパスワード]

1. 所定のテキストボックスに現在のパスワードと新しいパスワードを入力します。

注意: 新しいパスワードには、最小で 1 文字、最大で 128 文字の英数字を指定する必要があります。

2. 確認用の新しいパスワードを入力します。
3. [保存] をクリックします。

隔離フォルダ設定

ウイルスバスター Corp. クライアントでセキュリティリスクを検出し、検出時の処理が隔離であった場合、感染ファイルを暗号化して、<「クライアントのインストールフォルダ」>¥SUSPECT にあるローカルの隔離フォルダに移動します。

ファイルをローカルの隔離ディレクトリに移動した後、クライアントはそれを指定された隔離ディレクトリに送信します。[ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → {検索の種類} → [処理] タブで、ディレクトリを指定します。指定された隔離ディレクトリのファイルは、他のファイルに感染しないように暗号化されます。詳細については、189 ページの「隔離ディレクトリ」を参照してください。

指定された隔離ディレクトリが、ウイルスバスター Corp. サーバコンピュータ上にある場合、Web コンソールでサーバの隔離ディレクトリ設定を変更します。サーバでは、隔離ファイルを<「サーバのインストールフォルダ」>¥PCCSRV¥Virus に保存します。

注意: ウイルスバスター Corp. クライアントが、何らかの理由で（ネットワーク接続の問題など）暗号化されたファイルをウイルスバスター Corp. サーバに送信できない場合、暗号化されたファイルはクライアントの隔離フォルダに残ります。クライアントがウイルスバスター Corp. サーバに接続すると、ファイルの再送信を試行します。

隔離ディレクトリ設定を行うには

パス: [管理] → [隔離フォルダ設定]

1. 隔離フォルダの初期設定の容量、およびウイルスバスター Corp. で隔離フォルダに保存可能な感染ファイルの最大サイズを、そのまま使用するか変更します。初期設定値が画面に表示されます。
2. [隔離フォルダ設定を保存] をクリックします。
3. 隔離フォルダにあるすべての既存ファイルを削除するには、[すべての隔離ファイルを削除] をクリックします。

Server Tuner

Server Tuner を使用すると、次のようなサーバ関連のパフォーマンス問題に対して、パラメータを使用してウイルスバスター Corp. サーバのパフォーマンスを最適化することができます。

Download

ウイルスバスター Corp. サーバにアップデートを要求するクライアント数 (アップデートエージェントを含む) が、サーバの使用可能なリソースを超えた場合、サーバはクライアントのアップデート要求をキューに移動して、リソースが使用可能になったときに要求を処理します。クライアントがウイルスバスター Corp. サーバからのコンポーネントのアップデートに成功したら、クライアントはサーバにアップデートが完了したことを通知します。ウイルスバスター Corp. サーバがクライアントからのアップデート通知の受信を待機する最大時間を、分単位で設定します。また、サーバがクライアントに、アップデートの実行と新しい設定の適用の通知を試行する最大回数も設定します。サーバは、クライアントからの通知を受け取らない場合のみ、試行を続けます。

Buffer

ウイルスバスター Corp. サーバは、クライアントから複数の要求 (アップデートを実行する要求など) を受け取ると、できる限り多くの要求を処理し、残りの要求はバッファに置きます。その後、リソースが使用可能になったら、バッファに保存されている要求を 1 つずつ処理します。イベント (クライアントのアップデート要求など)、およびクライアントログレポートのためのバッファのサイズを指定します。

Network Traffic

ネットワークトラフィックの量は、1 日を通して変動します。ウイルスバスター Corp. サーバおよび他のアップデート元へのネットワークトラフィックフローを制御するには、任意の時点で同時にアップデート可能なクライアント数を指定します。

Server Tuner には、次のファイルが必要です。SvrTune.exe

Server Tuner を実行するには

パス : [ツール] → [管理ツール] → [Server Tuner]

1. ウイルスバスター Corp. サーバコンピュータで、<「サーバのインストールフォルダ」>¥PCCSRV¥Admin¥Utility¥SvrTune に移動します。
2. SvrTune.exe をダブルクリックして、Server Tuner を起動します。Server Tuner コンソールが開きます。
3. [Download] で、次の設定を変更します。

Timeout for client

ウイルスバスター Corp. サーバがクライアントからのアップデートの応答の受信を待機する時間を、分単位で入力します。クライアントがこの時間内に応答しない場合、ウイルスバスター Corp. サーバは、そのクライアントに最新のコンポーネントがインストールされていないとみなします。通知を受けたクライアントがタイムアウトすると、通知を待機している別のクライアントのスロットが使用可能になります。

Timeout for update agent

ウイルスバスター Corp. サーバがアップデートエージェントからのアップデートの応答の受信を待機する時間を、分単位で入力します。通知を受けたクライアントがタイムアウトすると、通知を待機している別のクライアントのスロットが使用可能になります。

Retry count

ウイルスバスター Corp. サーバがクライアントに、アップデートの実行または新しい設定の適用の通知を試行する最大回数を設定します。

Retry interval

ウイルスバスター Corp. サーバが通知の試行の間に待機する時間を、分単位で指定します。

4. [Buffer] で、次の設定を変更します。

Event Buffer

ウイルスバスター Corp. がバッファに保持する、サーバへのクライアントイベントレポート (コンポーネントのアップデートなど) の最大数を入力します。クライアントの要求がバッファで待機している間、クライアントとの接続は切断されます。ウイルスバスター Corp. は、クライアントのレポートを処理してバッファから削除したら、クライアントとの接続を確立します。

Log Buffer

ウイルスバスター Corp. がバッファに保持する、サーバへのクライアントログ情報レポートの最大数を入力します。クライアントの要求がバッファで待機している間、クライアントとの接

続は切断されます。ウイルスバスター Corp. は、クライアントのレポートを処理してバッファから削除したら、クライアントとの接続を確立します。

注意： 大量のクライアントがサーバにレポートを送信する場合は、バッファサイズを増やしてください。ただし、バッファサイズを増やすと、サーバのメモリの使用量も増えます。

5. [Network Traffic] で、次の設定を変更します。

Normal hours

ネットワークトラフィックの量を通常と判断する時間帯を表すラジオボタンをクリックします。

Off-peak hours

ネットワークトラフィックの量を最低と判断する時間帯を表すラジオボタンをクリックします。

Peak hours

ネットワークトラフィックの量をピークと判断する時間帯を表すラジオボタンをクリックします。

Maximum client connections

「その他のアップデートサーバ」とウイルスバスター Corp. サーバの両方から同時にコンポーネントをアップデートできる、クライアントの最大数を入力します。それぞれの期間に対してクライアントの最大数を入力します。最大接続数に達したとき、クライアントがコンポーネントをアップデートできるのは、(アップデートが完了するか、あるいはクライアントの応答が [Timeout for client] または [Timeout for Update Agent] フィールドで指定したタイムアウト値に達したことにより) 現在のクライアント接続が閉じられた場合のみです。

6. [OK] をクリックします。ウイルスバスター Corp. マスターサービスを再起動するよう求めるメッセージが表示されます。

注意： 再起動するのはサービスのみであり、コンピュータではありません。

7. [Yes] をクリックすると、Server Tuner 設定が保存され、サービスが再起動されます。再起動するとただちに設定が有効になります。

[No] をクリックすると、Server Tuner 設定は保存されますが、サービスは再起動されません。設定を有効にするには、ウイルスバスター Corp. マスターサービスまたはウイルスバスター Corp. サーバコンピュータを再起動してください。

ウイルストラッキングセンターへのウイルス情報送信

セキュリティリスク大規模感染の動向を正確に追跡するために、ウイルストラッキングセンターにセキュリティリスクの検索結果を送信します。このプログラムに参加すると、セキュリティリスクの進行および拡散について詳しい情報を入手できます。

ウイルスバスター Corp. をインストールすると、ウイルストラッキングプログラムに参加するかどうかを尋ねられます。この設定は、Web コンソールからいつでも変更できます。

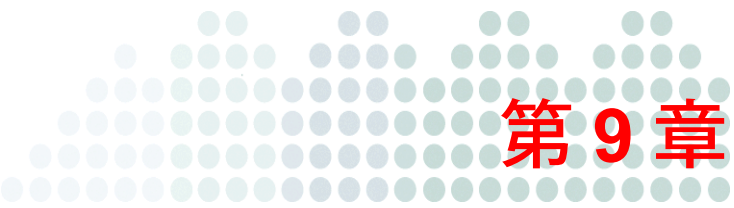
現在のトレンドマイクロのウイルスマップを確認するには、次のサイトにアクセスします。

<http://wtc.trendmicro.com/japanese/>

プログラムへの参加を変更するには

パス: [管理] → [ウイルストラッキングセンター]

1. プログラムに参加するか参加を取りやめるかを選択します。
2. [保存] をクリックします。



第9章

クライアントの管理

この章で説明する内容には、次の項目が含まれます。

- 280 ページの「コンピュータの位置」
- 283 ページの「クライアントの権限とその他の設定」
- 295 ページの「グローバルクライアント設定」
- 307 ページの「サーバとのクライアント接続」
- 315 ページの「クライアントプロキシ設定」
- 317 ページの「クライアント情報」
- 318 ページの「クライアント設定のインポートおよびエクスポート」
- 319 ページの「オフラインクライアントの管理」

コンピュータの位置

ウイルスバスター Corp. には、クライアントに適用される Web レピュテーションポリシーおよびクライアントの接続先スマートスキャンサーバを決定するための位置認識機能が用意されています。ウイルスバスター Corp. サーバまたはいずれかの参照サーバに接続できるウイルスバスター Corp. クライアントは内部に配置されています。つまり、以下のことを意味します。

- これらのクライアントには、内部クライアントに対する Web レピュテーションポリシーが適用されます。
- これらのクライアントでスマートスキャンが使用される場合、クライアントはローカルのスマートスキャンサーバに接続されます。

接続を確立できない場合、クライアントには外部クライアントに対する Web レピュテーションポリシーが適用されます。クライアントでスマートスキャンを使用すると、これらのクライアントは Trend Micro グローバルスマートスキャンサーバに接続されます。

ヒント： より厳格な外部クライアントに対する Web レピュテーションポリシーを実行することをお勧めします。

その位置を、クライアントコンピュータのゲートウェイ IP アドレスに基づいて判断するか、ウイルスバスター Corp. サーバや参照サーバとのクライアントの接続状況に基づいて判断するかを指定します。

ゲートウェイの IP アドレスを基準とする場合

クライアントコンピュータのゲートウェイの IP アドレスが、[コンピュータの位置] 画面で指定したゲートウェイの IP アドレスのいずれかと一致する場合、そのコンピュータの位置は「内部」とみなされます。一致しない場合は、コンピュータの位置は「外部」とみなされます。

クライアントの接続状況を基準とする場合

ウイルスバスター Corp. クライアントがイントラネット上のウイルスバスター Corp. サーバまたは参照サーバに接続できる場合、そのコンピュータの位置は「内部」とみなされます。さらに、企業のネットワークの外部にあるコンピュータがウイルスバスター Corp. サーバまたは参照サーバと接続を確立できる場合も、そのコンピュータの位置は「内部」とみなされます。これら以外の場合、コンピュータの位置は「外部」とみなされます。

位置を設定するには

パス: [ネットワーク上のコンピュータ] → [コンピュータの位置]

1. 位置の基準を、[クライアントの接続状態] にするか、または [ゲートウェイ IP アドレス] および [MAC アドレス] にするか選択します。
2. [クライアントの接続状態] を選択した場合、参照サーバを使用するかどうかを決定します。詳細については、263 ページの「参照サーバ」を参照してください。
 - a. 参照サーバを指定しなかった場合、次のイベントが発生したときに、クライアントはウイルスバスター Corp. サーバとの接続状態をチェックします。
 - ・ クライアントがスタンバイモードから通常の (オンライン / オフライン) モードに切り替えたとき
 - ・ クライアントがある検索方法から別の検索方法に切り替えたとき 詳細については、165 ページの「検索方法」を参照してください。
 - ・ クライアントがコンピュータの IP アドレスの変更を検出したとき
 - ・ クライアントが再起動したとき
 - ・ サーバが接続状態の確認を開始したとき 詳細については、307 ページの「サーバとのクライアント接続」を参照してください。
 - ・ グローバル設定を適用する際に Web レピュテーションの位置の基準が変更されたとき
 - ・ 大規模感染予防ポリシーが実行されなくなり、大規模感染前の設定が復元されたとき
 - b. 参照サーバを指定した場合、クライアントではまずウイルスバスター Corp. サーバとの接続状態がチェックされ、ウイルスバスター Corp. サーバとの接続が成功していない場合は参照サーバとの接続状態がチェックされます。クライアントによる接続状態のチェックは 1 時間ごとに行われ、さらに前述のいずれかのイベントが発生したときも行われます。
3. [ゲートウェイ IP アドレス] および [MAC アドレス] を選択した場合、次の処理を実行します。
 - a. 表示されたテキストボックスにゲートウェイ IP アドレスを入力します。
 - b. 必要に応じて、MAC アドレスを入力します。MAC アドレスを入力しない場合、ウイルスバスター Corp. には指定された IP アドレスに属するすべての MAC アドレスが指定されます。
 - c. [追加] をクリックします。
 - d. 追加するすべてのゲートウェイ IP アドレスに対してステップ a ～ステップ c を繰り返します。
 - e. ゲートウェイ設定インポートツールを使用して、ゲートウェイ設定のリストをインポートします。詳細については、282 ページの「ゲートウェイ設定インポートツール」を参照してください。

4. [保存] をクリックします。

ゲートウェイ設定インポートツール

ウイルスバスター Corp. では、コンピュータの位置をチェックして、使用する Web レピュテーションポリシーおよび接続先スマートスキャンサーバを決定します。ウイルスバスター Corp. で位置を識別する方法の 1 つは、コンピュータのゲートウェイ IP アドレスと MAC アドレスをチェックすることです。

[コンピュータの位置] 画面でゲートウェイの設定を行うか、ゲートウェイ設定インポートツールを使用してゲートウェイ設定のリストを [コンピュータの位置] 画面にインポートします。

ゲートウェイ設定インポートツールを使用するには

1. ゲートウェイ設定のリストが格納されたテキストファイル (.txt) を用意します。各行には IP アドレスを入力し、必要に応じて MAC アドレスを入力します。IP アドレスと MAC アドレスは、カンマで区切ります。エントリの最大数は 4096 です。

例：

10.1.111.222,00:17:31:06:e6:e7

10.1.111.223

10.1.111.224,00:17:31:06:e6:e7

2. サーバコンピュータ上で、<「サーバのインストールフォルダ」>¥PCCSRV¥Admin¥Utility¥GatewaySettingsImporter に移動し、GSImporter.exe をダブルクリックします。

注意： ターミナルサービスからゲートウェイ設定インポートツールを実行することはできません。

3. [ゲートウェイ設定インポートツール] 画面で、ステップ 1 で作成したファイルを指定して [インポート] をクリックします。
4. [OK] をクリックします。[コンピュータの位置] 画面にゲートウェイの設定が表示され、ウイルスバスター Corp. サーバはクライアントに設定を配信します。
5. すべてのエントリを削除するには、[すべてクリア] をクリックします。特定のエントリのみを削除する必要がある場合、「コンピュータの位置」画面からそのエントリを削除します。
6. 設定をファイルにエクスポートするには、[すべてエクスポート] をクリックし、ファイルの名前と種類を指定します。

クライアントの権限とその他の設定

ウイルスバスター Corp. クライアントで特定の設定を変更したり高度なタスクを実行する権限をユーザに付与します。

ヒント： 組織全体で一貫した設定およびポリシーを実行するには、ユーザに権限を限定して付与します。

権限とその他の設定を構成するには

パス：[ネットワーク上のコンピュータ]→[クライアント管理]→[設定]→[権限とその他の設定]

1. [権限設定] タブをクリックして、次のユーザの権限を設定します。
 - 「スタンドアロン権限」
 - 「検索権限」
 - 「予約検索権限」
 - 「ファイアウォール権限」
 - 「メール検索権限」
 - 「ツールボックス権限」
 - 「プロキシ設定権限」
 - 「コンポーネントアップデート権限」
 - 「アンインストール」
 - 「アンロード」
2. [その他の設定] タブをクリックして、次の設定を行います。
 - 「アップデート設定」
 - 「Web レピュテーション設定」
 - 「予約検索の設定」
 - 「クライアントセキュリティ設定」
 - 「POP3 メール検索設定」
 - 「クライアントコンソールアクセス制限」
 - 「再起動の通知」
3. クライアントツリーのドメインまたはクライアントを選択している場合は、[保存] をクリックすると設定がドメインまたはクライアントに適用されます。ルートアイコン  を選択した場合は、次のオプションのいずれかを選択します。

- **すべてのクライアントに適用**：すべての既存のクライアント、および既存または将来追加されるドメインに加えられる新しいクライアントに、設定を適用します。将来追加されるドメインとは、設定を指定した時点で作成されていないドメインのことです。
- **将来追加されるドメインにのみ適用**：将来追加されるドメインに加えられるクライアントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいクライアントには設定を適用しません。

スタンドアロン権限

この権限を付与すると、ユーザはスタンドアロンモードを有効にできます。スタンドアロンモードでは、ウイルスバスター Corp. サーバからコンポーネントをアップデートしたり、ウイルスバスター Corp. サーバにログを送信したりすることはできません。ウイルスバスター Corp. サーバでも、タスクの開始やクライアント設定の配信など、スタンドアロンクライアントの管理ができません。詳細については、310 ページの「スタンドアロンクライアント」を参照してください。

検索権限

この権限を付与すると、ユーザはクライアントコンソールを開いて [設定] → { 検索の種類 } を選択することにより、独自の手動検索、リアルタイム検索、および予約検索の設定を行うことができます。

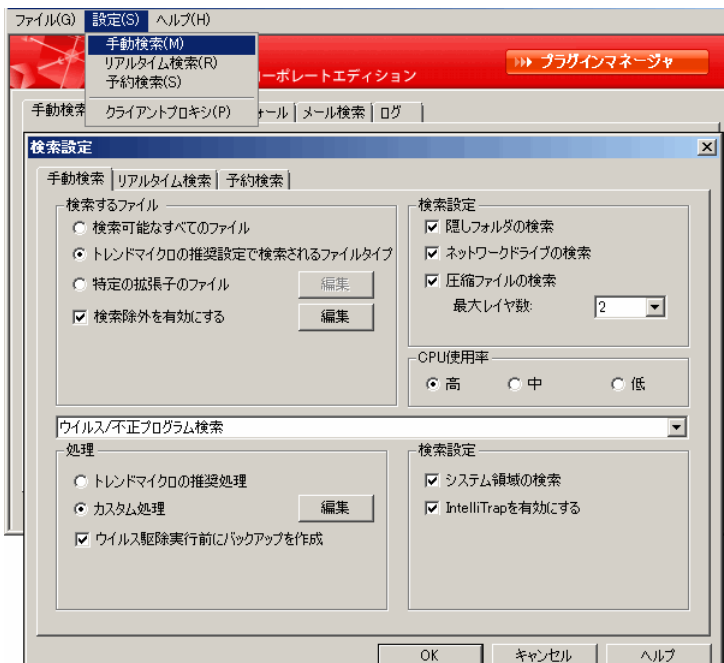


図 9-1. クライアントコンソールでの検索設定

次の設定を実行できます。

- 手動検索：「検索対象ファイル」、「検索設定」、「CPU 使用率」、「検索除外」、「検出時の処理」
- リアルタイム検索：「ファイルに対するユーザのアクティビティ」、「検索対象ファイル」、「検索設定」、「検索除外」、「検出時の処理」
- 予約検索：「スケジュール」、「検索対象ファイル」、「検索設定」、「CPU 使用率」、「検索除外」、「検出時の処理」

予約検索権限

予約検索を実行するよう設定されたクライアントは、予約検索を遅延およびスキップ / 停止する権限を持つことができます。ユーザがこれらの権限を利用できるようにするには、予約検索が実行される前に通知メッセージを表示するようにウイルスバスター Corp. を設定して、ユーザに付与した権限について通知します。

通知メッセージを表示するには、[ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → [権限とその他の設定] → [その他の設定] タブ → [予約検索の設定] に進んで、[予約検索の実行前に通知を表示します] を有効にします。

通知メッセージには、予約検索が実行されるまでの時間（分単位）が表示されます。この時間を設定するには、[ネットワーク上のコンピュータ] → [グローバルクライアント設定] → [予約検索の設定] → [予約検索の実行__分前にユーザに知らせる] に進みます。

予約検索の遅延

「予約検索の遅延」権限を持つユーザは、次の処理を実行できます。

- 予約検索を実行する前にそれを遅延させて、その遅延期間を指定できます。予約検索は一度だけ遅延できます。
- 予約検索が実行されている場合、ユーザは検索を停止して後で再開できます。この場合、ユーザは検索が再開されるまでの時間を指定します。検索が再開されると、以前に検索されていたファイルもすべて再度検索されます。予約検索の停止と再開は一度だけ実行できます。

注意： ユーザが指定可能な最小遅延時間は、15 分です。最大は 12 時間 45 分です。この時間は、[ネットワーク上のコンピュータ] → [グローバルクライアント設定] → [予約検索を最大__時間__分延期します] に移動して短縮することができます。

予約検索のスキップおよび停止

このオプションを有効にすると、ユーザは次の処理を実行できます。

- 予約検索が実行される前にそれをスキップできます。
- 予約検索の実行中にそれを停止できます。

クライアントコンピュータで予約検索を遅延 / スキップおよび停止するには

予約検索が起動していない場合、次の処理を実行します。

1. タスクトレイの [ウイルスバスター Corp. クライアント] アイコンを右クリックして、[予約検索の詳細設定] を選択します。

注意： 通知メッセージが有効であり、予約検索が実行されるまでの時間が表示されるよう設定されている場合、ユーザはこの手順を実行する必要はありません。

2. 表示される通知ウィンドウ上で、次のいずれかのオプションを選択します。
 - 検索遅延時間__時間__分
 - この予約検索をスキップします。次回の予約検索は < 日付 > の < 時刻 > に実行されます。

予約検索が実行されている場合、次の処理を実行します。

1. タスクトレイの [ウイルスバスター Corp. クライアント] アイコンを右クリックして、[予約検索の詳細設定] を選択します。
2. 表示される通知ウィンドウ上で、次のいずれかのオプションを選択します。
 - 検索を停止します。検索再開までの時間__時間__分
 - 検索を停止します。次回の予約検索は < 日付 > の < 時刻 > に実行されます。

ファイアウォール権限

ファイアウォール権限を付与すると、ユーザは独自のファイアウォール設定を行うことができます。ユーザが行う設定はすべて、ウイルスバスター Corp. サーバから配信される設定で上書きすることはできません。たとえば、ユーザが侵入検知システム (IDS) を無効にした場合、管理者がウイルスバスター Corp. サーバで IDS を有効にしても、クライアントコンピュータでは IDS は無効のままです。

クライアントコンソールにファイアウォールタブを表示

[ファイアウォール] タブにはクライアント上のすべてのファイアウォール設定が表示され、ファイアウォール権限を持つユーザは独自の設定を行うことができます。



図 9-2. クライアントコンソールの [ファイアウォール] タブ

ユーザにファイアウォール / IDS / 警告メッセージの有効化 / 無効化を許可

ウイルスバスター Corp. ファイアウォールは、ステートフルインスペクション、高性能なネットワークウイルス検索、および駆除機能を使用して、ネットワーク上のクライアントとサーバを保護します。ファイアウォールとその機能を有効化または無効化する権限をユーザに付与する場合、コンピュータが侵入やハッカーの攻撃にさらされることを防ぐため、長期間ファイアウォールを無効にしないよう、ユーザに注意してください。

この権限をユーザに付与しない場合、ウイルスバスター Corp. サーバの Web コンソールで行われたファイアウォール設定が、クライアントコンソールの [ネットワークカードのリスト] の下に表示されます。

クライアントにウイルスバスター Corp. サーバへのファイアウォールログの送信を許可

ウイルスバスター Corp. ファイアウォールでブロックおよび許可したトラフィックを分析するには、このオプションを選択します。このオプションを選択する場合、[ネットワーク上のコンピュータ] → [グローバルクライアント設定] → [ファイアウォールログ設定] セクションでログの送信スケジュールを設定します。このスケジュールは、ファイアウォールログ送信権限を持つクライアントにのみ適用されます。

ファイアウォールログを表示する方法については、244 ページの「ファイアウォールログ」を参照してください。

メール検索権限

クライアントにメール検索権限がある場合、クライアントコンソールに [メール検索] タブが表示されます。メール検索には、Outlook メール検索と POP3 メール検索があります。



図 9-3. クライアントコンソールの [メール検索] タブ

ウイルスバスター Corp. クライアントでは、クライアントコンソールの [ログ] 画面にメール検索の結果は表示されず、メール検索ログはサーバに送信されません。Outlook および POP3 メール検索ログは、クライアントコンピュータ上の個別のログファイルに保存されます。メール検索ログの詳細については、376 ページの「メール検索ログ」および 378 ページの「Web 評価および POP3 メール検索のログ」を参照してください。

Outlook メール検索

クライアントコンソールに [メール検索] タブが表示されている場合、クライアントユーザは速やかに Outlook メール検索設定を行い、手動検索を実行して、Microsoft Outlook メールメッセージおよび添付ファイルのウイルス / 不正プログラムを検索できます。

注意： Outlook メール検索では、スパイウェア / グレーウェアの検索を行いません。

Outlook メール検索ではユーザが検索を起動します。つまり、ユーザが [メール検索] タブで手動検索を実行することで、初めて検索が行われることになります。また、リアルタイムのメールメッセージの検索は行われず、スケジュールに基づいて自動的に実行するように設定することはできません。

POP3 メール検索

POP3 メール検索では、メールメッセージおよび添付ファイルのウイルス / 不正プログラムをリアルタイムに（つまり、メールメッセージが POP3 メールサーバからダウンロードされたときに）検査します。[メール検索] タブに [POP3 メール検索] 設定オプションを表示するには、[ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → [権限とその他の設定] → [その他の設定] タブに進んで、[POP3 メール検索] を選択します。

注意： POP3 メール検索では、スパイウェア / グレーウェアの検索を行いません。

POP3 メール検索では、メールメッセージをリアルタイムでのみ検索します。ユーザは、クライアントコンソールから手動で検索を起動したり、検索がスケジュールに基づいて自動的に実行されるように設定することはできません。

Web コンソールからは、ウイルスバスター Corp. がウイルス / 不正プログラムに対して実行する処理を設定することはできません。ユーザは、クライアントコンソールでこの処理を設定します。

POP3 メール検索プログラムは、ウイルスバスター Corp. NT プロキシサービス (TMProxy.exe) を Web レビューテーションプログラムと共有します。

ツールボックス権限

この権限を有効にすると、クライアントコンソールに [ツールボックス] タブが表示されます。ユーザは [ツールボックス] タブを使用して、Check Point SecureClient Support をインストールできます。ウイルスバスター Corp. には、Check Point SecureClient でクライアントのウイルスパターンファイルおよびウイルス検索エンジンが最新かどうかをチェックするツールが用意されています。



図 9-4. クライアントコンソールの [ツールボックス] タブ

プロキシ設定権限

この権限を付与すると、クライアントユーザはプロキシ設定を行うことができます。ウイルスバスター Corp. では、次のような場合にのみユーザが行うプロキシ設定を使用します。

- ・ クライアントが手動アップデートを実行した場合。手動アップデート機能の詳細は、292 ページの「コンポーネントアップデート権限」を参照してください。
- ・ ユーザが自動プロキシ設定を無効にした場合、またはウイルスバスター Corp. で自動プロキシ設定を検出できない場合。詳細については、306 ページの「自動プロキシ設定」を参照してください。

コンポーネントアップデート権限

アップデート権限を付与すると、クライアントユーザは独自のアップデート設定を行うことができます。

アップデートの実行

この権限を持つユーザは、タスクトレイで [ウイルスバスター Corp.] アイコンを右クリックして、[アップデート] を選択することで、必要なときにコンポーネントをアップデートできます。手動アップデートの実行時にプロキシ設定を使用するようにクライアントを設定できます。詳細については、306 ページの「自動プロキシ設定」を参照してください。

予約アップデートの有効化

この権限を付与すると、クライアントユーザは予約アップデートを有効または無効にできます。この権限を持つユーザは予約アップデートを有効または無効にできますが、実際のスケジュールを設定することはできません。スケジュールは管理者が [アップデート] → [ネットワーク上のコンピュータ] → [自動アップデート] → [予約アップデート] で指定する必要があります。

アンインストール

この権限を付与すると、ユーザはパスワードの有無に関係なくウイルスバスター Corp. クライアントをアンインストールできます。Web コンソールでクライアントのサイレントアンインストールを開始するには、[ネットワーク上のコンピュータ] → [クライアント管理] → [タスク] → [クライアントアンインストールパスワード画面] に進みます。

アンロード

この権限を付与すると、ユーザはパスワードの有無に関係なくウイルスバスター Corp. クライアントを一時的に停止できます。

アップデート設定

トレンドマイクロのアップデートサーバからのアップデートの実行

アップデートを開始する場合、ウイルスバスター Corp. クライアントはまず [アップデート] → [ネットワーク上のコンピュータ] → [アップデート元] 画面で指定したアップデート元からアップデートを取得します。このアップデートが失敗すると、クライアントは次にウイルスバスター

Corp. サーバからのアップデートを試行します。このオプションを選択すると、クライアントはウイルスバスター Corp. サーバからのアップデートが失敗した場合に、トレンドマイクロのアップデートサーバからアップデートを試行できます。

予約アップデートの有効化

このオプションを選択すると、選択したクライアントは常に予約アップデートが実行されます。ただし、予約アップデートを有効または無効にする権限を持つユーザが、予約アップデートを無効にしている場合を除きます。この権限の詳細については、292 ページの「コンポーネントアップデート権限」を参照してください。

アップデートスケジュールは、[アップデート] → [ネットワーク上のコンピュータ] → [自動アップデート] → [予約アップデート] で指定します。

クライアントはコンポーネントのアップデートが可能ですが、クライアントプログラムのアップグレードと HotFix の配信を禁止

このオプションを使用すると、コンポーネントのアップデートは処理されますが、HotFix の配信とクライアントのアップグレードは行われません。

このオプションを選択しない場合、すべてのクライアントはサーバに同時に接続して HotFix をアップグレードまたはインストールします。これは、多数のクライアントがある場合、サーバのパフォーマンスに大きく影響することがあります。このオプションを選択する場合、クライアントのアップグレードまたはサーバ上の HotFix の配信の影響を最小化する方法を計画して、その計画を実行します。

Web レピュテーション設定

ウイルスバスター Corp. では、Web レピュテーションポリシーに違反する URL をブロックした直後に、クライアントコンピュータに通知メッセージを表示します。必要に応じて、[通知] → [クライアントユーザ通知] → [Web レピュテーションポリシー違反] タブに移動して、通知メッセージの内容を変更できます。

予約検索の設定

このオプションを有効にすると、予約検索実行の指定時間（分単位）前に、クライアントコンピュータに通知メッセージが表示されます。ユーザには、検索のスケジュール（日時）および予約検索権限（予約検索の遅延、スキップ、停止など）が通知されます。予約検索権限の詳細については、286 ページの「予約検索権限」を参照してください。

メッセージを表示する時間を設定できます (分単位)。この時間を設定するには、[ネットワーク上のコンピュータ] → [グローバルクライアント設定] → [予約検索の設定] → [予約検索の実行__分前にユーザに知らせる]に進みます。

クライアントセキュリティ設定

この設定を使用して、ユーザのウイルスバスター Corp. クライアントファイルおよびレジストリへのアクセスを許可または制限します。

[高] を選択すると、ウイルスバスター Corp. のフォルダ、ファイル、およびレジストリのアクセス権限設定は、Windows 2000/XP/Server 2003 が稼働するクライアントコンピュータの Program Files フォルダと同じになります。

そのため、Program Files フォルダの権限設定 (Windows のセキュリティ設定) が、完全な読み取り / 書き込みアクセスを許可するよう設定されている場合、[高] を選択してもウイルスバスター Corp. クライアントのフォルダ、ファイル、およびレジストリへの完全な読み取り / 書き込みアクセスをユーザに許可することになります。

POP3 メール検索設定

これを選択すると、クライアントコンソールで POP3 メール検索が可能になります。この設定は、メール検索権限を持つクライアントにのみ適用されます。詳細については、289 ページの「メール検索権限」を参照してください。

クライアントコンソールアクセス制限

この設定により、タスクトレイまたは Windows スタートメニューからのクライアントコンソールへのアクセスが無効になります。ユーザは、<「クライアントのインストールフォルダ」>から「PccNT.exe」をクリックすることによってのみ、クライアントコンソールにアクセスできます。この設定を行った後、クライアントを再起動して設定を有効にします。

この設定により、ウイルスバスター Corp. クライアントが使用できなくなることはありません。ウイルスバスター Corp. クライアントはセキュリティ上の脅威からコンピュータを保護するため、バックグラウンドで実行されます。

再起動の通知

このオプションを選択すると、感染ファイルの駆除処理を完了するために、クライアントコンピュータを再起動するようユーザに促すメッセージを表示します。

リアルタイム検索の場合、特定のセキュリティリスクが検索された後にメッセージが表示されます。手動検索、予約検索、および ScanNow の場合、ウイルスバスター Corp. がすべての検索対象を検索し終えた後に一度だけメッセージが表示されます。

グローバルクライアント設定

ウイルスバスター Corp. では、グローバルクライアント設定を、すべてのクライアントまたは特定の権限を持つクライアントにのみ適用します。

グローバルクライアント設定を行うには

パス: [ネットワーク上のコンピュータ] → [グローバルクライアント設定]

1. 次の設定を行います。
 - ・ 「検索設定」
 - ・ 「予約検索の設定」
 - ・ 「承認済み URL」
 - ・ 「ファイアウォールログ設定」
 - ・ 「警告設定」
 - ・ 「ウイルスバスター Corp. サービスの再起動」
 - ・ 「クライアントセルフプロテクション」
 - ・ 「ディスク空き容量」
 - ・ 「ネットワークウイルスログ統合の有効化」
 - ・ 「ウイルス / 不正プログラムログ帯域幅設定」
 - ・ 「自動プロキシ設定」
 - ・ 「クライアントのグループ設定」
2. [保存] をクリックします。

検索設定

圧縮ファイルの検索制限

サーバの管理対象となるすべてのクライアントは、手動検索、リアルタイム検索、予約検索、および ScanNow の実行時に、圧縮ファイルのウイルス / 不正プログラムおよびスパイウェア / グレーウェアを検索する際、次の設定をチェックします。

解凍後のサイズが __ MB を超える場合は検索しない

ウイルスバスター Corp. は、この制限を超えるファイルを検索しません。

圧縮ファイルでは最初の __ ファイルのみを検索

圧縮ファイルを解凍した後、ウイルスバスター Corp. は指定された個数のファイルを検索し、それ以上ファイルがあっても残りは無視します。

OLE オブジェクトを次の階層まで検索

ファイルに複数のオブジェクトのリンクと埋め込み (OLE) の層がある場合、ウイルスバスター Corp. は指定された最大層数まで検索を行い、残りの層は行いません。

サーバの管理対象となるすべてのクライアントは、手動検索、リアルタイム検索、予約検索、および ScanNow の実行時に、この設定をチェックします。各層では、ウイルス / 不正プログラムおよびスパイウェア / グレーウェアが検索されます。

例：

層数として 2 を指定した場合、あるファイルの中に Microsoft Word ドキュメント (第 1 層) が埋め込まれており、この Word ドキュメントの中に Microsoft Excel スプレッドシートがあり (第 2 層)、さらにこのスプレッドシートの中に JPEG ファイル (第 3 層) があるとする、ウイルスバスター Corp. は Word ドキュメントと Excel スプレッドシートを検索しますが、JPG ファイルは検索しません。

手動検索をクライアントコンピュータのショートカットメニューに追加

この設定を有効にすると、サーバの管理対象となるすべてのクライアントで、Windows エクスプローラの右クリックメニューに [ウイルスバスター Corp. クライアントでの検索] オプションが追加されます。ユーザが Windows デスクトップまたは Windows エクスプローラでファイルまたはフォルダを右クリックして、このオプションを選択すると、手動検索によりファイルまたはフォルダのウイルス / 不正プログラムおよびスパイウェア / グレーウェアが検索されます。

ウイルスバスター Corp. サーバのデータベースフォルダをリアルタイム検索の対象から除外

ウイルスバスター Corp. クライアントとサーバが同じコンピュータ上に存在する場合、このクライアントではリアルタイム検索時に、サーバデータベースのウイルス / 不正プログラムおよびスパイウェア / グレーウェアの検索は行われません。

ヒント： 検索時のデータベースの破損を防ぐには、この設定を有効にします。

Microsoft Exchange サーバにインストールされる場合は Microsoft Exchange サーバのフォルダを除外

ウイルスバスター Corp. クライアントと Microsoft Exchange 2000/2003 サーバが同じコンピュータ上に存在する場合、ウイルスバスター Corp. では手動検索、リアルタイム検索、予約検索、および ScanNow の実行時に、Exchange サーバフォルダのウイルス / 不正プログラムおよびスパイウェア / グレーウェアの検索は行われません。

Microsoft Exchange 2007 を使用している場合は、検索除外リストに手動でフォルダを追加する必要があります。検索除外リストの詳細については、次の Web サイトを参照してください。

<http://technet.microsoft.com/ja-jp/library/bb332342.aspx>

検索除外リストの設定方法の詳細については、184 ページの「検索除外」を参照してください。

圧縮ファイル内の感染ファイルのウイルス駆除 / 削除

サーバの管理対象となるすべてのクライアントは、手動検索、リアルタイム検索、予約検索、および ScanNow の実行時に、圧縮ファイル内のウイルス / 不正プログラムを検出して、次の条件に適合すると、感染ファイルを駆除または削除します。

- "ウイルスバスター Corp. で実行するように設定されている処理が「駆除」または「削除」である。感染ファイルにウイルスバスター Corp. が実行する処理は、[ネットワーク上のコンピュータ] → [クライアント管理] → { 検索の種類 } → [処理] タブで確認できます。
- [圧縮ファイル内の感染ファイルのウイルス駆除 / 削除] 設定を有効にしている。この設定を有効にすると、検索時にコンピュータのリソースの使用量が増加し、検索の実行に時間がかかる場合があります。これは、ウイルスバスター Corp. が圧縮ファイルを解凍して、圧縮ファイル内の感染ファイルを駆除 / 削除してから、再度そのファイルを圧縮する必要があるためです。

- ・ 圧縮ファイル形式がサポートされている。ウイルスバスター Corp. では、ZIP や、ZIP 圧縮技術を使用する Office Open XML など、特定の圧縮ファイル形式のみがサポートされています。Excel、PowerPoint、Word などの Microsoft Office 2007 アプリケーションでは、Office Open XML が初期設定の形式として使用されます。

注意： サポートされる圧縮ファイル形式の全リストについては、サポート担当者にお問い合わせください。

たとえば、リアルタイム検索で、ウイルスに感染したファイルは削除するよう設定されているとします。リアルタイム検索で「abc.zip」という圧縮ファイルを解凍し、その中の「123.doc」というファイルで感染を検出した場合、ウイルスバスター Corp. は「123.doc」ファイルを削除し、再び「abc.zip」として圧縮します。再圧縮された「abc.zip」ファイルは安全にアクセスできるようになります。

次の表は、上記のいずれかの条件が成立しない場合に実行される処理を示しています。

表 9-1. 圧縮ファイルのシナリオと結果

[圧縮ファイル内の感染ファイルのウイルス駆除 / 削除] のステータス	ウイルスバスター Corp. で実行するように設定された処理	圧縮ファイル形式	結果
有効	駆除または削除	サポートなし 例：「def.rar」に感染ファイル「123.doc」が含まれている場合。	ウイルスバスター Corp. は「def.rar」を暗号化しますが、「123.doc」に対して駆除、削除、またはその他の処理を行いません。
無効	駆除または削除	サポートあり / サポートなし 例：「abc.zip」に感染ファイル「123.doc」が含まれている場合。	ウイルスバスター Corp. は「abc.zip」および「123.doc」に対して、駆除、削除、またはその他の処理を行います。

表 9-1. 圧縮ファイルのシナリオと結果 (続き)

[圧縮ファイル内の 感染ファイルのウ イルス駆除 / 削除] のステータス	ウイルスバス ター Corp. で実行 するように設定 された処理	圧縮ファイル形式	結果
有効 / 無効	駆除や削除は実 行されません。 つまり、拡張子 変更、隔離、ア クセス拒否、ま たは放置のいづ れかになります。	サポートあり / サ ポートなし 例: 「abc.zip」に感 染ファイル 「123.doc」が含ま れている場合。	ウイルスバスター Corp. は 「abc.zip」に対して設定され た処理 (拡張子変更、隔離、 アクセス拒否、または放置) を実行しますが、「123.doc」 に対しては実行しません。 各設定によって、次の処理を 実行します。 拡張子変更: ウイルスバス ター Corp. は「abc.zip」の名 前を「abc.vir」に変更しま す。「123.doc」の名前は変更 しません。 隔離: ウイルスバスター Corp. は「abc.zip」を隔離し ます (「123.doc」と他のすべ ての未感染ファイルも隔離し ます)。 放置: ウイルスバスター Corp. は「abc.zip」および 「123.doc」に対して処理を実 行せず、ウイルスが検出され たことをログに記録します。 アクセス拒否: ウイルスバス ター Corp. は、「abc.zip」を 開くときにアクセスを拒否し ます (「123.doc」と他のすべ ての未感染ファイルも開くこ とはできません)。

診断モードを有効にする

診断モードでは、サーバの管理対象となるすべてのクライアントは、手動検索、予約検索、リアルタイム検索、および ScanNow の実行時に検出されたスパイウェア / グレーウェアをログに記録しますが、スパイウェア / グレーウェアのコンポーネントは駆除しません。駆除は、プロセスを終了するか、レジストリ、ファイル、Cookie およびショートカットを削除します。

トレンドマイクロの診断モードにより、トレンドマイクロが検出したスパイウェア / グレーウェアを評価し、その結果に基づいて適切な処理を実行できます。たとえば、検出されたスパイウェア / グレーウェアのうち、セキュリティリスクではないと判断されるものはスパイウェア / グレーウェアの承認リストに追加できます。

診断モード時に実行される検出時の処理は次のとおりです。

- ・ 「放置」: 手動検索、予約検索、ScanNow の場合
- ・ 「アクセス拒否」: リアルタイム検索の場合

注意: 診断モードは、どのユーザ設定の検索時の処理よりも優先されます。たとえば、管理者が手動検索時の検索時の処理として「駆除」を選択しても、クライアントが診断モードであれば検索時の処理は「放置」のままになります。

Cookie の検索

Cookie が潜在的なセキュリティリスクと考えられる場合、このオプションを選択します。これを選択すると、サーバの管理対象となるすべてのクライアントは、手動検索、予約検索、リアルタイム検索、および ScanNow の実行時に、Cookie のスパイウェア / グレーウェアを検索します。

予約検索の設定

予約検索を実行するよう設定されたクライアントのみが、次の設定を使用します。予約検索では、ウイルス / 不正プログラムおよびスパイウェア / グレーウェアを検索できます。

予約検索の実行__分前にユーザに知らせる

ウイルスバスター Corp. は、検索実行の指定時間 (分単位) 前に、ユーザに、検索スケジュール (日時) とユーザに付与した予約検索権限を示す通知メッセージを表示します。

通知メッセージを有効または無効にするには、[ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → [権限とその他の設定] → [その他の設定] タブ → [予約検索の設定] に移動します。これを無効にすると、この通知メッセージは表示されません。

予約検索を最大__時間__分延期します

「予約検索の遅延」権限を持つユーザのみが、次の処理を実行できます。

- 予約検索を実行する前にそれを遅延させて、その遅延期間を指定できます。
- 予約検索が実行されている場合、ユーザは検索を停止して後で再開できます。この場合、ユーザは検索が再開されるまでの時間を指定します。検索が再開されると、以前に検索されていたファイルもすべて再度検索されます。

ユーザが指定可能な最大遅延時間は 12 時間 45 分です。これを短縮するには、所定のフィールドに時間と分数を指定します。

検索を__時間__分を超えて実行し続けた場合、予約検索を自動的に停止します

ウイルスバスター Corp. は、指定された時間が経過しても検索が終了しない場合、検索を停止します。検索時に検出されたセキュリティリスクは、すべてユーザにただちに通知されます。

クライアントコンピュータのバッテリー残量が__%未満で、かつ AC アダプタが接続されていない場合には、予約検索をスキップします

ウイルスバスター Corp. は、ワイヤレスコンピュータが電源につながっておらず、バッテリーが残り少ないことを検出した場合、予約検索が起動したときに検索をただちにスキップします。バッテリーの残りが少なくても電源につながっていれば、検索は行われます。

実行されなかった予約検索を開始します

予約検索の日時にウイルスバスター Corp. が実行されていなかったために予約検索が起動しなかった場合、ウイルスバスター Corp. が予約検索を実行するよう設定した時刻に実行されていれば、日付に関係なく検索が起動されます。

ファイアウォールログ設定

ファイアウォールログをウイルスバスター Corp. サーバに送信する権限を、特定のクライアントに付与することができます。このセクションでログ送信スケジュールを設定します。ファイアウォールログを送信する権限を持つクライアントのみが、このスケジュールを使用します。

選択したクライアントで使用可能なファイアウォール権限については、288 ページの「ファイアウォール権限」を参照してください。

警告設定

ウイルスバスター Corp. では、次の場合に通知を表示できます。

指定された日数を超えた後もウイルスパターンファイルが古いままである

警告アイコンが Windows タスクバーに表示され、ユーザにウイルスパターンファイルがアップデートされたことを通知します。サーバの管理対象となるすべてのクライアントに、この設定が適用されます。

クライアントユーザはコンピュータを再起動してカーネルモードドライバをロードする必要がある

カーネルモードドライバの新バージョンを含む HotFix またはアップグレードパッケージをインストールしても、前バージョンのドライバはコンピュータから削除されません。前バージョンをアンロードして新バージョンをロードするには、コンピュータを再起動します。コンピュータを再起動すると、新バージョンが自動的にインストールされます。それ以降の再起動は不要です。

クライアントコンピュータに HotFix またはアップグレードパッケージがインストールされた直後に、通知メッセージが表示されます。

ウイルスバスター Corp. サービスの再起動

ウイルスバスター Corp. は、予期せず応答を停止したが、通常のシステムプロセスでは停止しなかったクライアントサービスを再起動します。

クライアントサービスの再起動を有効にするには、次の設定を行います。

サービスの停止時にはウイルスバスター Corp. クライアントサービスを自動的に再起動する

ウイルスバスター Corp. は次のサービスを再起動します。

- OfficeScan NT Listener (tmlisten.exe)：ウイルスバスター Corp. サーバからコマンドと通知を受信して、クライアントとウイルスバスター Corp. サーバ間の通信を容易にします。
- OfficeScanNT RealTime Scan (ntrtscan.exe)：ウイルスバスター Corp. クライアントでリアルタイム検索、予約検索、および手動検索を実行します。
- OfficeScan NT Proxy Service (TmProxy.exe)：対象アプリケーションに移転する前にネットワークトラフィックを検索します。

__ 分後にサービスを再起動

サービスが停止した場合、ウイルスバスター Corp. は指定されたサービスを再起動するまでの時間(分単位) 待機します。

サービスの再起動に失敗した後、__ 回まで再試行する

サービスを再起動するまでの再試行の最大回数を指定します。再試行を最大回数実行しても停止したままであれば、サービスを手動で再起動します。

__ 時間後に再起動の失敗回数をリセットする

再試行を最大回数実行してもサービスが停止したままである場合、ウイルスバスター Corp. は指定された時間 (時単位) 待機して、失敗のカウントをリセットします。指定された時間が経過してもサービスが停止したままであれば、ウイルスバスター Corp. はサービスを再起動します。

クライアントセルフプロテクション

クライアントセルフプロテクションでは、ウイルスバスター Corp. クライアントが、正常に機能するために必要なプロセスおよびその他のリソースを保護する手段を提供します。クライアントセルフプロテクションは、プログラムや実際のユーザが不正プログラム対策保護を無効にしようとする試みを阻止するのに役立ちます。

ウイルスバスター Corp. クライアントのインストールフォルダ内のファイルを保護する

他のプログラムまたはユーザによりウイルスバスター Corp. ファイルが変更または削除されないようにするには、ウイルスバスター Corp. でルート <「クライアントのインストールフォルダ」> にある次のファイルをロックします。

- 拡張子が .exe、.dll、および .sys のデジタル署名ファイル
- 次のファイルを含む、デジタル署名のない一部のファイル
 - bspatch.exe
 - bzip2.exe
 - INETWH32.dll
 - libcurl.dll
 - libeay32.dll
 - libMsgUtilExt.mt.dll
 - msvcm80.dll
 - MSVCP60.DLL
 - msvcp80.dll
 - msucr80.dll
 - OfceSCV.dll
 - OFCESCVPack.exe
 - patchbld.dll
 - patchw32.dll
 - patchw64.dll
 - PiReg.exe
 - ssleay32.dll
 - Tmeng.dll
 - TMNotify.dll

- zlibwapi.dll

ウイルスバスター Corp. クライアントプロセスを保護する

ウイルスバスター Corp. では、次のプロセスを停止させようとする試行をすべてブロックします。

- **tmlisten.exe**: ウイルスバスター Corp. サーバからコマンドと通知を受信して、クライアントとウイルスバスター Corp. サーバ間の通信を容易にします。
- **ntrtscan.exe**: ウイルスバスター Corp. クライアントでリアルタイム検索、予約検索、および手動検索を実行します。
- **TmProxy.exe**: 対象アプリケーションに移転する前にネットワークトラフィックを検索します。
- **TmPfw.exe**: パケットレベルファイアウォール、ネットワークウイルス検索および侵入検知機能を提供します。
- **TMBMSRV.exe**: 外部ストレージデバイスへのアクセスを規制し、レジストリキーおよびプロセスへの不正な変更を回避します。

注意: このリリースでは、x86 タイプのプロセッサが稼働するクライアントにのみこの設定を配信できます。

ウイルスバスター Corp. クライアントのレジストリキーを保護する

ウイルスバスター Corp. では、次のレジストリキーおよびサブキーの下のエントリを変更、削除、または新規追加しようとする試行をすべてブロックします。

- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TMCSS

注意: このリリースでは、x86 タイプのプロセッサが稼働するクライアントにのみこの設定を配信できます。

ディスク空き容量

ウイルスバスター Corp. では、HotFix、パターンファイル、検索エンジン、およびプログラムアップデート用に一定量のクライアントのディスク容量を割り当てることができます。初期設定では、60MB のディスク容量が確保されます。

ネットワークウイルスログ統合の有効化

このオプションを有効にすると、ウイルスバスター Corp. クライアントは 1 時間ごとにサーバにネットワークウイルスログを送信します。ネットワークウイルスの詳細については、161 ページの「ネットワークウイルス」を参照してください。

ウイルス / 不正プログラムログ帯域幅設定

ウイルスバスター Corp. では、短時間に同じウイルス / 不正プログラムから複数の感染を検出した場合、ウイルスログエントリを統合します。1 つのウイルス / 不正プログラムを複数回検出すると、すぐにウイルス / 不正プログラムのログが作成され、クライアントがログ情報をサーバに送信するときにネットワーク帯域幅を消費する可能性があります。この機能を有効にすると、作成されるウイルス / 不正プログラムのログエントリ数、およびクライアントがウイルスログ情報をサーバに送信する際に消費するネットワーク帯域幅の量の両方を軽減できます。

自動プロキシ設定

手動のプロキシ設定は、多くのエンドユーザにとって複雑なタスクになる場合があります。自動プロキシ設定を使用すると、ユーザの操作を必要とせずに、正しいプロキシ設定が適用されるようになります。

これを有効にすると、クライアントが自動アップデートまたは手動アップデートでコンポーネントをアップデートしたときに、自動プロキシ設定がプライマリプロキシ設定になります。自動アップデートおよび手動アップデートの詳細については、143 ページの「クライアントのアップデート方法」を参照してください。

クライアントが自動プロキシ設定を使用して接続できない場合、プロキシ設定を行う権限を持つクライアントユーザは、ユーザが行ったプロキシ設定を使用できます。そうしないと、自動プロキシ設定を使用した接続は失敗します。

注意： プロキシ認証はサポートされていません。

設定を自動で検出する

ウイルスバスター Corp. では、管理者が行った DHCP または DNS によるプロキシ設定を自動的に検出します。

自動設定スクリプトを使用する

ウイルスバスター Corp. では、ネットワーク管理者が設定したプロキシ自動設定 (PAC) スクリプトを使用して、適切なプロキシサーバを検出します。

クライアントのグループ設定

この設定は、クライアントのインストール時にのみ使用されます。インストールプログラムは、対象コンピュータが属するネットワークドメインをチェックします。ドメイン名がクライアントツリーに存在している場合、対象コンピュータ上のクライアントはそのドメインの下でグループ化され、そのドメインの設定が適用されます。ドメイン名が存在しない場合、ウイルスバスター Corp. はクライアントツリーにドメインを追加し、そのドメインの下のクライアントをグループ化して、ルート設定をドメインおよびクライアントに適用します。

インストールプログラムで NetBIOS、Active Directory、または DNS ドメイン名をチェックするかどうかを指定します。

サーバとのクライアント接続

クライアントコンピュータのタスクトレイのアイコンは、ウイルスバスター Corp. サーバおよびスマートスキャンサーバ (クライアントがスマートスキャンを使用している場合) とのクライアントの接続状態を示します。

アイコンが次のいずれかの状態を示している場合、ユーザはそれに対処する必要があります。

- ・ パターンファイルがしばらくアップデートされていない。
- ・ リアルタイム検索が無効。
- ・ リアルタイム検索サービスが停止している。ウイルスバスター Corp. は、リアルタイム検索サービスをリアルタイム検索だけでなく、手動検索や予約検索にも使用します。つまり、リアルタイム検索サービスが停止すると、クライアントコンピュータは保護されなくなります。
- ・ スマートスキャンクライアントが、スマートスキャンサーバに接続されていない。

これらのいずれかの状態が発生した場合のユーザの対処方法については、312 ページの「必要な処理」を参照してください。

オンラインクライアント

オンラインクライアントはウイルスバスター Corp. サーバと常に接続しています。ウイルスバスター Corp. サーバでは、これらのクライアントに対してタスクを起動したり、設定を配信したりできます。

表 9-2. オンラインクライアントのアイコン

アイコン	検索方法	説明
	従来型スキャン	すべてのコンポーネントは最新で、サービスは正常に稼働しています。
	従来型スキャン	パターンファイルがしばらくアップデートされていません。リアルタイム検索が有効です。
	従来型スキャン	リアルタイム検索が無効です。
	従来型スキャン	パターンファイルがしばらくアップデートされていません。リアルタイム検索が無効です。
	従来型スキャン	リアルタイム検索サービスが停止しています。
	従来型スキャン	パターンファイルがしばらくアップデートされていません。リアルタイム検索サービスが停止しています。
	スマートスキャン	クライアントはスマートスキャンサーバに接続できます。すべてのサービスは正常に稼働しています。
	スマートスキャン	クライアントはスマートスキャンサーバに接続できます。リアルタイム検索が無効です。
	スマートスキャン	クライアントはスマートスキャンサーバに接続できます。リアルタイム検索サービスが停止しています。
	スマートスキャン	クライアントはスマートスキャンサーバに接続できません。リアルタイム検索が有効です。
	スマートスキャン	クライアントはスマートスキャンサーバに接続できません。リアルタイム検索が無効です。

表 9-2. オンラインクライアントのアイコン (続き)

アイコン	検索方法	説明
	スマートスキャン	クライアントはスマートスキャンサーバに接続できません。 リアルタイム検索サービスが停止しています。

オフラインクライアント

オフラインクライアントは、ウイルスバスター Corp. サーバと接続されていません。ウイルスバスター Corp. サーバでは、このようなクライアントは管理できません。

表 9-3. オフラインクライアントのアイコン

アイコン	検索方法	説明
	従来型スキャン	リアルタイム検索が有効です。
	従来型スキャン	パターンファイルがしばらくアップデートされていません。 リアルタイム検索が有効です。
	従来型スキャン	リアルタイム検索が無効です。
	従来型スキャン	パターンファイルがしばらくアップデートされていません。 リアルタイム検索が無効です。
	従来型スキャン	リアルタイム検索サービスが停止しています。
	従来型スキャン	パターンファイルがしばらくアップデートされていません。 リアルタイム検索サービスが停止しています。
	スマートスキャン	クライアントはスマートスキャンサーバに接続できます。 リアルタイム検索が有効です。
	スマートスキャン	クライアントはスマートスキャンサーバに接続できます。 リアルタイム検索が無効です。
	スマートスキャン	クライアントはスマートスキャンサーバに接続できます。 リアルタイム検索サービスが停止しています。

表 9-3. オフラインクライアントのアイコン (続き)

アイコン	検索方法	説明
	スマートスキャン	クライアントはスマートスキャンサーバに接続できません。
	スマートスキャン	クライアントはスマートスキャンサーバに接続できません。 リアルタイム検索が無効です。
	スマートスキャン	クライアントはスマートスキャンサーバに接続できません。 リアルタイム検索サービスが停止しています。

スタンドアロンクライアント

スタンドアロンクライアントは、ウイルスバスター Corp. サーバからコンポーネントをアップデートしたり、ウイルスバスター Corp. サーバにログを送信したりすることはできません。ウイルスバスター Corp. サーバは、スタンドアロンクライアントに対してタスクを起動したり、クライアント設定を配信したりすることができません。スタンドアロンクライアントとウイルスバスター Corp. サーバとの接続は、クライアントコンピュータの位置やネットワーク接続状況などにより、確立できる場合とできない場合があります。

スタンドアロン権限を持つユーザは、ウイルスバスター Corp. サーバの介入 (サーバで起動する検索など) により、プレゼンテーションの実行時などにタスクの実行が妨げられる場合、スタンドアロンモードを有効にできます。スタンドアロンクライアントでも、インターネットに接続されていれば、コンポーネントをアップデートできます。ただし、アップデートエージェントやトレンドマイクロのアップデートサーバからアップデートを取得するように設定されている場合に限りです。

長期間ウイルスバスター Corp. サーバと接続しないクライアントには、スタンドアロン権限を割り当てる必要があります。権限を割り当てるには、[ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → [権限とその他の設定] → [権限設定] タブに移動します。

スタンドアロンクライアントへのアップデートは、次の場合のみ実行されます。

- ・ クライアントユーザが手動アップデートを実行するとき
- ・ アップデートの自動配信を設定し、配信先クライアントにスタンドアロンモードのクライアントを含めるとき
- ・ 予約アップデートを有効にする権限をクライアントに付与したとき

クライアントのアップデート方法の詳細については、139 ページの「クライアントアップデート」を参照してください。

表 9-4. スタンドアロンクライアントのアイコン

アイコン	検索方法	説明
	従来型スキャン	リアルタイム検索が有効です。
	従来型スキャン	リアルタイム検索が無効です。
	従来型スキャン	パターンファイルがしばらくアップデートされていません。 リアルタイム検索が有効です。
	従来型スキャン	パターンファイルがしばらくアップデートされていません。 リアルタイム検索が無効です。
	従来型スキャン	リアルタイム検索サービスが停止しています。
	従来型スキャン	パターンファイルがしばらくアップデートされていません。 リアルタイム検索サービスが停止しています。
	スマートスキャン	クライアントはスマートスキャンサーバに接続できます。 リアルタイム検索が有効です。
	スマートスキャン	クライアントはスマートスキャンサーバに接続できます。 リアルタイム検索が無効です。
	スマートスキャン	クライアントはスマートスキャンサーバに接続できます。 リアルタイム検索サービスが停止しています。
	スマートスキャン	クライアントはスマートスキャンサーバに接続できません。 リアルタイム検索が無効です。
	スマートスキャン	クライアントはスマートスキャンサーバに接続できません。 リアルタイム検索が無効です。
	スマートスキャン	クライアントはスマートスキャンサーバに接続できません。 リアルタイム検索サービスが停止しています。

必要な処理

クライアントのアイコンが次のいずれかの状態を示している場合、必要な処理を実行します。

パターンファイルがしばらくアップデートされていない

クライアントユーザはコンポーネントをアップデートする必要があります。Web コンソールから、[アップデート] → [ネットワーク上のコンピュータ] に進んでコンポーネントのアップデートの設定を行うか、または [ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → [権限とその他の設定] → [権限設定] タブ → [コンポーネントアップデート権限] に進んでユーザにアップデートする権限を付与します。

リアルタイム検索サービスが停止している

ユーザは、[スタート] → [ファイル名を指定して実行] をクリックし、「services.msc」と入力して起動した Microsoft 管理コンソールから、サービス (ウイルスバスター Corp. WinNT RealTime Scan) を手動で開始できます。

リアルタイム検索が無効

Web コンソールからリアルタイム検索を有効にします ([ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → [リアルタイム検索設定])。

リアルタイム検索が無効で、クライアントがスタンドアロンモード

ユーザは、まずスタンドアロンモードを無効にする必要があります。スタンドアロンモードを無効にしたら、Web コンソールからリアルタイム検索を有効にします。

企業のネットワーク内のクライアントがサーバに接続されていない

Web コンソールから接続を確認し ([ネットワーク上のコンピュータ] → [接続状態の確認])、接続状態の確認ログをチェックします ([ログ] → [ネットワーク上のコンピュータのログ] → [接続状態の確認])。

確認後もクライアントが接続されていない場合は、次の手順を実行します。

1. 接続状態が、クライアントとサーバの両方ともオフラインの場合、ネットワーク接続をチェックします。
2. 接続状態が、クライアント側がオフラインでサーバ側がオンラインの場合、サーバのドメイン名が変更されている可能性があり、クライアントはそのドメイン名を使用してサーバに接続します (サーバインストール時にドメイン名を選択した場合)。ウイルスバスター Corp. サーバのドメイン名を DNS または WINS サーバに登録するか、またはドメイン名および IP 情報をクラ

クライアントコンピュータの <Windows フォルダ>%system32%drivers%etc フォルダの「hosts」ファイルに追加します。

3. 接続状態が、クライアント側がオンラインでサーバ側がオフラインの場合、ウイルスバスター Corp. のファイアウォール設定をチェックします。ファイアウォールで、サーバからクライアントへの通信をブロックし、クライアントからサーバへの通信を許可している可能性があります。
4. 接続状態が、クライアント側でオンラインでサーバ側がオフラインの場合、クライアントの IP アドレスが変更されている可能性があります。その状態はサーバに反映されません（クライアントを再ロードした場合など）。クライアントの再配信を実行してください。

クライアントがスマートスキャンサーバに接続できない

1. 次の「コンピュータの位置」の設定が正しく行われているかどうかをチェックします。
 - ・ 参照サーバおよびポート番号
 - ・ ゲートウェイ IP アドレス
2. スキャンサーバの標準またはカスタムのリストにあるスマートスキャンサーバのアドレスが、正しいかどうかをチェックします。
3. そのサーバアドレスを使用して接続が確立できるかどうかをテストします。また、リストを設定した後、[すべてのクライアントへ通知] を必ずクリックしてください。詳細については、172 ページの「スマートスキャンソース」を参照してください。
4. スマートスキャンサーバとウイルスバスター Corp. クライアント上の次の設定ファイルが、同期されているかどうかを確認します。
 - ・ sscfg.ini
 - ・ ssnotify.ini
5. 次のレジストリを調べて、クライアントが企業のネットワークに接続されているかどうかを確認します。

キー：
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\iCRC
Scan\Scan Server

 - ・ LocationProfile=1 の場合、クライアントはネットワークに接続されており、ローカルのスマートスキャンサーバに接続する必要があります。
 - ・ LocationProfile=2 の場合、クライアントはネットワークに接続されておらず、グローバルスマートスキャンサーバに接続する必要があります。クライアントコンピュータで、Internet Explorer からインターネットの Web ページを表示できるかどうかをチェックします。

6. スマートスキャンサーバとの接続に使用する内部プロキシおよび外部プロキシの設定をチェックします（ローカルおよびグローバル）。

クライアントとサーバ間の接続の確認

ウイルスバスター Corp. サーバとのクライアントの接続状態は、ウイルスバスター Corp. Web コンソールのクライアントツリーに表示されます。



図 9-5. ウイルスバスター Corp. サーバとのクライアントの接続状態を示すクライアントツリー

場合によっては、クライアントツリーがクライアントの正しい接続状態を示さないことがあります。たとえば、誤ってクライアントコンピュータからネットワークケーブルが抜かれると、クライアントはオフラインになったことをサーバに通知することはできません。このクライアントは、クライアントツリーにオンラインとして表示されたままになります。

クライアントとサーバの接続を手動で確認するか、またはウイルスバスター Corp. で予約確認を実行します。特定のドメインまたはクライアントを選択してから、接続状態を確認することはできません。ウイルスバスター Corp. は、登録されているすべてのクライアントの接続状態を確認します。

クライアントとサーバ間の接続を確認するには

パス: [ネットワーク上のコンピュータ] → [接続状態の確認]

1. クライアントとサーバ間の接続を手動で確認するには、[接続状態の確認] タブに移動して、[接続状態を確認する] をクリックします。
2. クライアントとサーバ間の接続を自動的に確認するには、[接続状態確認の間隔] タブに移動します。
 - a. [接続状態確認の予約を有効にする] を選択します。
 - b. 確認の頻度と開始時刻を選択します。

- c. [保存] をクリックして、確認スケジュールを保存します。
3. クライアントツリーを調べて状態を確認するか、または接続状態の確認ログを確認します。

接続状態の確認ログ

ウイルスバスター Corp. では接続状態の確認ログを保持しており、ウイルスバスター Corp. サーバが、登録されているすべてのクライアントと通信できるかどうかを確認できます。ウイルスバスター Corp. では、Web コンソールからクライアントとサーバ間の接続を確認するたびに、ログエントリを作成します。

ハードディスク上の領域を大量に占有しないようにログのサイズを維持するには、手動でログを削除するか、またはログの削除スケジュールを設定します。ログの管理方法の詳細については、265 ページの「ログの管理」を参照してください。

接続状態の確認ログを表示するには

パス: [ログ] → [ネットワーク上のコンピュータログ] → [接続状態の確認]

1. 接続状態の確認の結果を表示するには、[ステータス] 列をチェックします。
2. ログを CSV ファイルに保存するには、[CSV 形式でエクスポート] をクリックします。ファイルを開くか、特定の場所に保存します。CSV ファイルは、通常、Microsoft Excel などのスプレッドシートアプリケーションで開きます。

クライアントプロキシ設定

ウイルスバスター Corp. クライアントを、内部サーバおよび外部サーバに接続する際にプロキシ設定を使用するように設定します。

内部プロキシ

クライアントは、内部プロキシ設定を使用して、ネットワーク上の次のサーバに接続できます。

ウイルスバスター Corp. サーバコンピュータ

サーバコンピュータは、ウイルスバスター Corp. サーバおよび統合スマートスキャンサーバをホストします。クライアントはウイルスバスター Corp. サーバに接続して、コンポーネントのアップデート、設定の取得、およびログの送信を行います。クライアントは統合スマートスキャンサーバに接続して、検索クエリを送信します。

ローカルスマートスキャンサーバ

ローカルスマートスキャンサーバには、すべてのスタンドアロンのスマートスキャンサーバ、および別のウイルスバスター Corp. サーバの統合スマートスキャンサーバが含まれます。クライアントはサーバに接続して、検索クエリを送信します。

内部プロキシ設定を行うには

パス: [管理] → [プロキシ設定] → [内部プロキシ] タブ

1. プロキシサーバの使用を有効にするチェックボックスをオンにします。
2. プロキシサーバの名前または IP アドレス、およびポート番号を指定します。
3. プロキシサーバに認証が必要な場合、所定のフィールドにユーザ名とパスワードを入力します。
4. [保存] をクリックします。

外部プロキシ

ウイルスバスター Corp. サーバおよびクライアントは、トレンドマイクロがホストするサーバに接続するときに、外部プロキシ設定を使用できます。このトピックでは、クライアントの外部プロキシ設定について説明します。サーバの外部プロキシ設定の詳細については、132 ページの「サーバアップデートのプロキシ」を参照してください。

クライアントは、Internet Explorer で設定されたプロキシ設定を使用して、Trend Micro グローバルスマートスキャンサーバおよび Web レピュテーションサーバに接続します。プロキシサーバ認証が必要な場合、クライアントはこの画面で指定した認証アカウント情報（ユーザ ID とパスワード）を使用します。

Trend Micro グローバルスマートスキャンサーバ

スマートスキャンクライアントが企業のネットワークの外部にある場合、グローバルスマートスキャンサーバに接続して検索クエリを送信します。

Web レピュテーションサーバ

クライアントは、トレンドマイクロの Web レピュテーションサーバに接続して、ユーザがアクセスしようとしている Web サイトが安全かどうかを確認します。

プロキシサーバの認証アカウント情報を設定するには

パス: [管理] → [プロキシ設定] → [外部プロキシ]

1. [トレンドマイクロのサーバとのクライアント接続] セクションで、プロキシサーバの認証に必要なユーザ ID とパスワードを入力します。

次のプロキシ認証プロトコルがサポートされます。

- 基本アクセス認証
- ダイジェストアクセス認証
- 統合 Windows 認証

2. 確認用のパスワードを入力します。
3. [保存] をクリックします。

クライアント情報

権限、クライアントソフトウェアの詳細、システムイベントなどのウイルスバスター Corp. クライアントに関する重要な情報を表示します。

クライアント情報を表示するには

パス: [ネットワーク上のコンピュータ] → [クライアント管理] → [ステータス]

1. 選択したクライアントの状態を表示するには、クライアントコンピュータの名前を展開します。[リセット] ボタンを使用すると、セキュリティリスクのカウントを 0 に戻すことができます。
2. 複数のクライアントを選択した場合、[設定の表示] をクリックすると、選択したすべてのクライアントの詳細が表示されます。

クライアント設定のインポートおよびエクスポート

複数のウイルスバスター Corp. クライアントに、同じ検索設定またはクライアントの権限設定を行うことが必要になる場合があります。ウイルスバスター Corp. では、特定のクライアントの検索設定および権限を保存 (エクスポート) して、それを複数のクライアントに複製 (インポート) できます。これにより、複数のクライアントに簡単に同一の設定を行うことができます。

複数のクライアントの検索および権限設定をエクスポートすることはできません。単一のクライアント、ドメイン、またはルートの設定のみをエクスポートできます。

ヒント: 同様の保護要件を持つ複数のクライアントを 1 つのドメインにグループ化した場合は、1 つのクライアントの設定を行い、その設定をエクスポートして、その設定ファイルをドメイン内の残りのクライアントにインポートすることをお勧めします。

クライアント設定をファイルにエクスポートするには

パス: [ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → [設定のエクスポート]

1. 任意のリンクをクリックして、選択したクライアントまたはドメインの設定を表示します。
2. [エクスポート] をクリックして、設定を保存します。設定は .dat ファイルに保存されます。
3. [保存] をクリックして、.dat ファイルの保存先を指定します。
4. [保存] をクリックします。

クライアント設定をインポートするには

パス: [ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → [設定のインポート]

1. [参照] をクリックしてコンピュータ上で .dat ファイルを探し、[インポート] をクリックします。[設定のインポート] 画面が開き、設定の概要が表示されます。
2. 検索または権限の設定リンクのいずれかをクリックして、該当する設定の詳細を表示します。
3. 設定をインポートします。

- ・ クライアントツリーでルートアイコンを選択した場合、[すべてのドメインに適用] を選択して [適用] をクリックし、設定をインポートします。
- ・ ドメインを選択した場合、[選択されたドメインに属するすべてのコンピュータに適用] を選択して [適用] をクリックし、設定をインポートします。
- ・ 複数のクライアントを選択した場合、[適用] をクリックして、設定をインポートします。

オフラインクライアントの管理

クライアントのアンインストールプログラムを使用して、コンピュータからクライアントプログラムを削除すると、プログラムは自動的にサーバに通知します。サーバがこの通知を受信すると、クライアントツリーからそのクライアントのアイコンが削除され、そのクライアントはもはや存在しないことが示されます。

ただし、コンピュータのハードディスクを再フォーマットしたり、クライアントファイルを手動で削除するなどの別の方法を使用してクライアントを削除した場合、ウイルスバスター Corp. では削除されたことを認識できず、クライアントはオフラインとして表示されます。ユーザが長期間クライアントをアンロードしたり無効にした場合も、クライアントはオフラインとして表示されます。

クライアントツリーにオンラインのクライアントのみを表示させるには、クライアントツリーからオフラインクライアントを自動的に削除するように、ウイルスバスター Corp. を設定します。

オフラインクライアントを自動的に削除するには

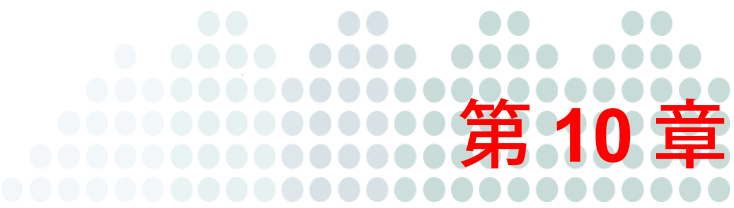
パス: [管理] → [オフラインクライアント]

1. [オフラインクライアントの自動削除機能を有効にする] を選択します。
2. ウイルスバスター Corp. がクライアントをオフラインとみなすまでの経過日数を選択します。
3. [保存] をクリックします。

第 3 部

その他の保護の提供





第10章

Policy Server for Cisco NAC

この章で説明する内容には、次の項目が含まれます。

- 324 ページの「Policy Server for Cisco NAC について」
- 324 ページの「コンポーネントおよび用語」
- 327 ページの「Cisco NAC 構成」
- 328 ページの「クライアント検証シーケンス」
- 330 ページの「ポリシーサーバ」
- 338 ページの「同期」
- 338 ページの「証明書」
- 340 ページの「ポリシーサーバのシステム要件」
- 341 ページの「Cisco Trust Agent (CTA) の要件」
- 342 ページの「サポートされるプラットフォームと要件」
- 343 ページの「ポリシーサーバのインストール」

この章には、ポリシーサーバを設定するための基本的な手順についての説明があります。Cisco Secure Access Control Server (以下、Cisco Secure ACS) およびその他の Cisco 製品の設定と管理の詳細については、次の Web サイトにある最新の Cisco マニュアルを参照してください。

<http://www.cisco.com/univercd/home/home.htm>

Policy Server for Cisco NAC について

ポリシーサーバは、ネットワーク上にあるクライアントコンピュータのウイルス対策コンポーネントのステータスを評価します。ポリシーサーバ設定オプションにより、リスク状態のクライアントへの処理の実行を設定することができ、クライアントは組織のセキュリティポリシーを承諾します。これらの処理には、以下のものが含まれます。

- ・ クライアントのコンピュータに対し、ウイルスバスター コーポレートエディション（以下、ウイルスバスター Corp.）クライアントコンポーネントのアップデートを指示します。
- ・ リアルタイム検索を有効にします。
- ・ ScanNow を実行します。
- ・ ポリシーサーバには、ユーザにウイルス対策ポリシー違反を知らせる通知メッセージを、クライアントコンピュータに表示する機能も含まれています。

Cisco NAC テクノロジについての詳細は、以下の Cisco Web サイトを参照してください。

<http://www.cisco.com/go/nac>

コンポーネントおよび用語

次のリストは、Cisco NAC のポリシーサーバを理解し使用するために必要となる、さまざまなコンポーネントと重要な用語を表しています。

コンポーネント

以下のコンポーネントは、トレンドマイクロ製品を Cisco NAC のポリシーサーバ内に実現するのに必要なコンポーネントです。

表 10-1. Cisco NAC ポリシーサーバのコンポーネント

コンポーネント	説明
Cisco Trust Agent (CTA)	他の Cisco NAC コンポーネントとの通信を可能にするためにクライアントコンピュータにインストールされたプログラム。
ウイルスバスター Corp. クライアントコンピュータ	インストール済みのウイルスバスター Corp. クライアントプログラムを所持するコンピュータ。Cisco NAC と連携するには、クライアントコンピュータも Cisco Trust Agent が必要です。

表 10-1. Cisco NAC ポリシーサーバのコンポーネント (続き)

コンポーネント	説明
ネットワークアクセスデバイス	Cisco NAC 機能をサポートするネットワークデバイス。サポートされているネットワークアクセスデバイスには、さまざまな Cisco ルータ、ファイアウォール、およびアクセスポイントだけでなく、Terminal Access Controller Access Control System (TACACS+) または Remote Authentication Dial-In User Service (RADIUS) プロトコルを使用して設定可能な他社製デバイスも含まれます。 サポートしているデバイスの一覧については、342 ページの「サポートされるプラットフォームと要件」を参照してください。
Cisco Secure Access Control Server (ACS)	ネットワークアクセスデバイスによりクライアントからウイルスバスター Corp. クライアントのウイルス対策データを受け取るためのサーバで、それを検証するために外部ユーザデータベースに受け渡します。また、ACS サーバは、処理後に、評価の結果をネットワークアクセスデバイスに渡します。評価結果には、ウイルスバスター Corp. クライアントへの命令が含まれている場合もあります。
ポリシーサーバ	ウイルスバスター Corp. クライアントのウイルス対策データを受けて検証するプログラム。検証の実行後、ポリシーサーバはウイルスバスター Corp. クライアントが実行する処理を決定し、クライアントに通知します。
ウイルスバスター Corp. サーバ	現在のウイルスパターンファイルとウイルス検索エンジンのバージョンをポリシーサーバに報告し、ポリシーサーバはこの情報を用いてウイルスバスター Corp. クライアントのウイルス対策ステータスを検証します。

用語

Cisco NAC のポリシーサーバに関連する次の用語をよく理解してください。

表 10-2. Cisco NAC 用ポリシーサーバに関する用語

用語	定義
セキュリティ状態	クライアントのウイルス対策ソフトの存在と通用。ここでのセキュリティ状態は、ウイルスバスター Corp. クライアントのプログラムがクライアントのコンピュータに存在しているか、ウイルスバスター Corp. クライアントの特定の設定のステータス、およびウイルス検索エンジンとウイルスパターンファイルが最新版かどうかを参照します。

表 10-2. Cisco NAC 用ポリシーサーバに関する用語 (続き)

用語	定義
セキュリティ状態 トークン	ウイルスバスター Corp. クライアント検証後ポリシーサーバにより作成されます。そこには、権限を与えるリアルタイム検索やアップデートウイルス対策コンポーネントなど、ウイルスバスター Corp. クライアントに一組の特定処理を実行するように伝える情報が含まれます。
クライアントの検証	クライアントセキュリティ状態の検証やセキュリティ状態トークンをクライアントに返還するプロセス
ポリシーサーバの ルール	ガイドラインには設定可能な基準が含まれています。これはウイルスバスター Corp. クライアントのセキュリティ状態をポリシーサーバが評価するために利用できます。ルールにはセキュリティ状態情報が基準と一致する場合に実行する、クライアントおよびポリシーサーバに対する処理も含まれています (331 ページの「ポリシーサーバのポリシーとルール」を参照)。
ポリシーサーバのポ リシー	ポリシーサーバがウイルスバスター Corp. クライアントのセキュリティ状態を評価する一連のルール。また、ポリシーには、ポリシーに関連付けられているルールの条件がセキュリティ状態に一致しない場合に、クライアントおよびポリシーサーバで実行される処理も含まれています (331 ページの「ポリシーサーバのポリシーとルール」を参照)。
AAA (Authentication, Authorization, and Accounting: 認証、承認、およびアカウント ティング)	エンドユーザクライアントのコンピュータリソースへのアクセスをコントロールするのに利用される 3 つの主なサービスについて記述します。認証とは、通常はユーザにユーザ名およびパスワードを入力させて、クライアントを識別することです。承認とは、特定のコマンドを発行するためにユーザが持つ権限のことです。アカウントティングとは、セッション中に使用されたりリソースの測定のことです。通常はログに記録が残されます。Cisco Secure Access Control Server (ACS) は、Cisco が実装した AAA サーバです。
CA (Certificate Authority: 証明機関)	コンピュータまたはサーバ間の認証を実行して、接続を確保するためにデジタル証明書を送信するネットワーク上の認定局です。
デジタル 証明書	セキュリティに利用される添付書類です。通常、証明書により、クライアントが Web サーバなどのサーバで認証されます。証明書には、ユーザ ID 情報、公開鍵 (暗号化に使用)、および証明書が有効なことを確認するための証明機関 (CA) のデジタル署名があります。
RADIUS (Remote Authentication Dial-In User Service)	クライアントのユーザ名とパスワードの入力を要求する認証システムです。Cisco Secure ACS サーバは RADIUS をサポートします。

表 10-2. Cisco NAC 用ポリシーサーバに関する用語 (続き)

用語	定義
TACACS+ (Terminal Access Controller Access Control System)	エンドユーザクライアントの認証に使われる AAA コマンドにより有効になるセキュリティプロトコル。Cisco ACS サーバは TACACS+ をサポートします。

Cisco NAC 構成

次の図は、基本的な Cisco NAC 構成を示しています。

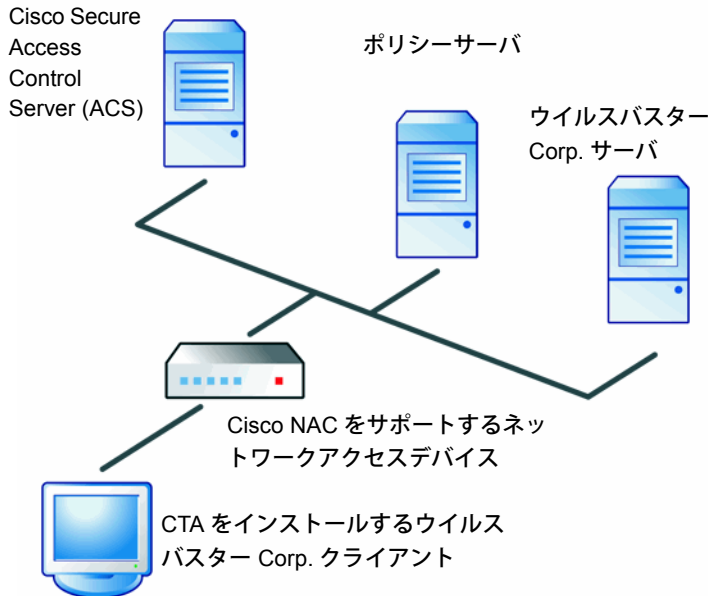


図 10-1. 基本的な Cisco NAC 構成

この図のウイルスバスター Corp. クライアントには CTA がインストールされており、Cisco NAC をサポートするネットワークアクセスデバイスを經由してのみネットワークにアクセスできます。ネットワークアクセスデバイスは、クライアントと他の Cisco NAC コンポーネントの間にあります。

注意： ネットワークの構成は、プロキシサーバ、ルータ、またはファイアウォールの有無に応じて異なる場合があります。

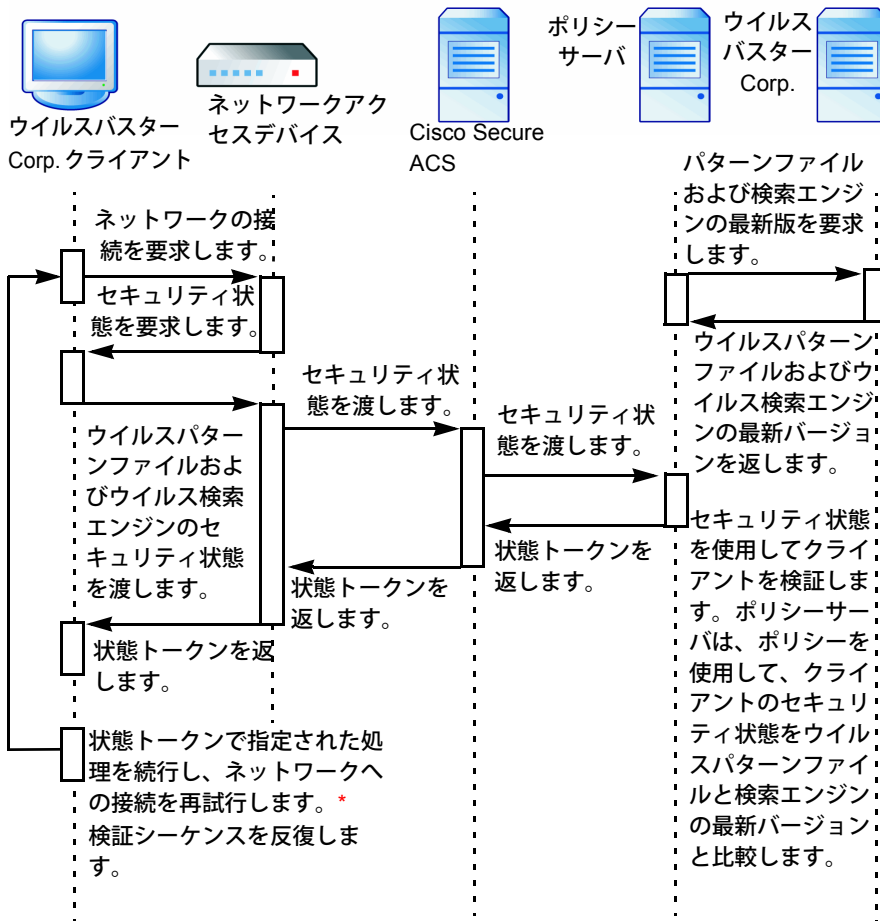
クライアント検証シーケンス

クライアント検証とは、ウイルスバスター Corp. クライアントのセキュリティ状態を評価し、ポリシーサーバでリスクが高いと判断された場合にクライアントが実行する処理の指示を返すプロセスのことです。ポリシーサーバでは、設定可能なルールおよびポリシーを使用して、ウイルスバスター Corp. クライアントを検証します。

以下は、ウイルスバスター Corp. クライアントがネットワークにアクセスを試みるときに発生する一連のイベントを示しています。

1. Cisco ネットワークアクセスデバイスは、クライアントのセキュリティ状態を要求することで検証シーケンスを開始します。
2. 次にネットワークアクセスデバイスはこのデータを ACS サーバに渡します。
3. ACS サーバは、セキュリティ状態をポリシーサーバに渡します。ここで評価が実行されます。
4. 別のプロセスで、ポリシーサーバは定期的にウイルスバスター Corp. サーバのウイルスパターンやウイルス検索エンジンのバージョン情報を調査し、データを更新しています。次に、ポリシーサーバは、設定されたポリシーを使用して、取得した情報と ACS サーバから受け取ったクライアントのセキュリティ状態のデータを比較します。
5. 続いて、ポリシーサーバは状態トークンを作成して、それを ACS サーバおよびネットワークアクセスデバイスを経由してウイルスバスター Corp. クライアントに渡します。

6. クライアントは状態トークンに設定されている処理を実行します。



* クライアントはネットワークアクセスデバイスタイマーが期限切れになった時点でネットワークへのアクセスを再試行します。タイマーの設定に関する情報は、Cisco ルータのドキュメントを参照してください。

図 10-2. ネットワークアクセス検証シーケンス

ポリシーサーバ

ポリシーサーバは、ウイルスバスター Corp. クライアントのセキュリティ状態を評価し、状態トークンを作成します。クライアントが所属するウイルスバスター Corp. サーバから受け取った、最新バージョンのウイルスパターンファイルやウイルス検索エンジンとセキュリティ状態を比較します。ポリシーサーバは状態トークンを Cisco Secure ACS サーバに返し、Cisco Secure ACS サーバは状態トークンを Cisco ネットワークアクセスデバイス経由でクライアントに渡します。

単一のネットワーク上に追加のポリシーサーバをインストールすると、多数のクライアントが同時にネットワークへのアクセスを試みた場合のパフォーマンスを向上させることができます。これらのポリシーサーバは、1 台のポリシーサーバが動作不能になった場合のバックアップとしても機能します。複数のウイルスバスター Corp. サーバが 1 つのネットワーク上にある場合、単一のポリシーサーバで、登録されているすべてのウイルスバスター Corp. サーバの要求が処理されます。同様に、複数のポリシーサーバで、すべてのポリシーサーバに登録されている単一のウイルスバスター Corp. サーバの要求を処理できます。

次の図は、複数のウイルスバスター Corp. サーバとポリシーサーバの関係を図にしたものです。

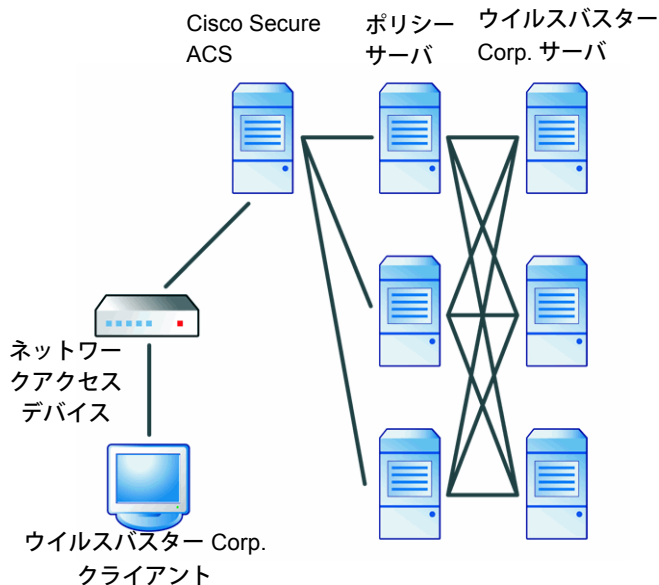


図 10-3. 複数のポリシーサーバ / ウイルスバスター Corp. サーバの関係

ポリシーサーバは、ウイルスバスター Corp. サーバと同じコンピュータにインストールすることもできます。

ポリシーサーバのポリシーとルール

ポリシーサーバは、設定可能なルールとポリシーを使用して、組織のセキュリティガイドラインを実施します。

ルールは、ポリシーサーバでウイルスバスター Corp. クライアントのセキュリティ状態と比較するために使用される特定の条件を含みます。クライアントのセキュリティ状態がルールで設定された条件に一致している場合は、クライアントとサーバはそのルールで指定された処理を実行します (332 ページの「ポリシーサーバとウイルスバスター Corp. クライアント処理」を参照)。

ポリシーは、1 つ以上のルールによって構成されています。ネットワーク上の登録されたウイルスバスター Corp. サーバごとに、大規模感染予防モードと通常モードの両方に対して、1 つのポリシーを割り当てます (ネットワークモードについての詳細は、210 ページの「大規模感染予防サービス」を参照してください)。

ウイルスバスター Corp. クライアントのセキュリティ状態が、ポリシーに含まれるルールの条件に一致する場合には、そのルールに設定されている処理がウイルスバスター Corp. クライアントで実行されます。ただし、クライアントのセキュリティ状態が、ポリシーに関連付けられているすべてのルールのどの条件にも一致しない場合は、ポリシーの初期設定の処理をクライアントとサーバで実行するように設定できます (332 ページの「ポリシーサーバとウイルスバスター Corp. クライアント処理」を参照)。

ヒント： ウイルスバスター Corp. ドメイン内の特定のクライアントに対し、同一ドメイン内の他のクライアントと異なる大規模感染モードポリシーと通常モードポリシーを適用したい場合は、似通った要求を持つクライアントごとにグループ分けするようドメインを再構成することをお勧めします (54 ページの「ウイルスバスター Corp. ドメイン」を参照)。

ルール構成

ルールは、セキュリティ状態の基準、基準が一致したときの応答、およびクライアントとポリシーサーバで実行する処理を含んでいます。

セキュリティ状態の基準

ルールには以下のセキュリティ状態の基準が含まれます。

- ・ **クライアントコンピュータの状態：** クライアントコンピュータが起動中かそうでないか
- ・ **クライアントのリアルタイム検索状態：** リアルタイム検索が有効か無効か
- ・ **クライアント検索エンジンのバージョン：** ウイルス検索エンジンは最新かどうか

- ・ **クライアントのウイルスパターンファイル状態**: ウイルスパターンファイルが最新であるということ。ポリシーサーバは次のうち 1 つをチェックしてこれを決定します。
 - ・ ウイルスパターンファイルがポリシーサーバのバージョンよりも一定以上古い場合
 - ・ ウイルスパターンファイルが有効期限より、特定の日数以前に入手可能になった場合

ルールに対する初期設定の応答メッセージ

応答により、クライアント検証が発生した場合に、ネットワーク上のウイルスバスター Corp. クライアントの状態を把握できます。応答は、ポリシーサーバのクライアント検証ログに記録され、状態トークンに対応します。次の初期設定の応答から選択します。

- ・ **Healthy (正常)**: クライアントコンピュータはセキュリティポリシーに一致し、ウイルスに感染していません。
- ・ **Checkup (要検査)**: クライアントのウイルス検索コンポーネントは更新する必要があります。
- ・ **Infected (感染)**: クライアントコンピュータは感染したか、感染の危険性があります。
- ・ **Transition (起動中)**: クライアントのコンピュータは起動状態です。
- ・ **Quarantine (隔離)**: クライアントのコンピュータは非常に感染の危険性があり、隔離が必要です。
- ・ **Unknown (不明)**: その他の状況

注意: 応答メッセージの追加、削除、変更はできません。

ポリシーサーバとウイルスバスター Corp. クライアント処理

クライアントのセキュリティ状態がルール基準に一致する場合、ポリシーサーバは次の処理を実行できます。

- ・ ポリシーサーバクライアント検証ログにエントリを作成します (358 ページの「クライアント検証ログ」を参照)。

クライアントのセキュリティ状態がルールの条件と一致する場合、ウイルスバスター Corp. クライアントでは、次の処理を実行できます。

- ・ クライアントが開いているファイルまたは保存されたファイルをすべて検索できるように、クライアントのリアルタイム検索を有効にします (176 ページの「リアルタイム検索」を参照)。
- ・ すべてのウイルスバスター Corp. コンポーネントをアップデートします (118 ページの「トレンドマイクロ ウイルスバスター コーポレートエディションのコンポーネントとプログラム」を参照)。

- リアルタイム検索が有効になった後か、アップデート後にクライアントを検索 (ScanNow) します。
- クライアントコンピュータに通知メッセージを表示します。

初期設定のルール

ポリシーサーバでは、ルールを設定する基準となる初期設定のルールが提供されています。このルールは一般的かつ推奨されるセキュリティ状態の条件および処理をカバーしています。次のルールは初期設定で利用可能です。

表 10-3. 初期設定のルール

ルール名	照合基準	基準に一致した場合の 応答メッセージ	サーバ 処理	クライアント処理
正常	リアルタイム検索が有効になっており、最新版のウイルス検索エンジンとウイルスパターンファイルが使用されています。	Healthy	なし	なし

表 10-3. 初期設定のルール (続き)

ルール名	照合基準	基準に一致した場合の 応答メッ セージ	サーバ 処理	クライアント処理
要検査	ウイルスパターンファイルのバージョンは、クライアントが登録しているウイルスバスター Corp. サーバ上のバージョンより少なくとも 1 つ古いバージョンです。	Checkup	クライアント検証ログにエントリを作成	- コンポーネントのアップデート - リアルタイム検索を有効化、またはアップデート実行後、クライアントに対して自動でクリーンナップを実行します。 - クライアントコンピュータに通知メッセージを表示します。 ヒント： このルールを使用する場合は、自動配信を使用してください。これにより、ウイルスバスター Corp. が新しいコンポーネントをダウンロードした後、ただちにクライアントが最新のウイルスパターンファイルを入手できるようになります。
起動中	クライアントコンピュータは起動中です。	Transition	なし	なし
隔離	ウイルスパターンファイルのバージョンは、クライアントが登録しているウイルスバスター Corp. サーバ上のバージョンより少なくとも 5 つ古いバージョンです。	Quarantine	クライアント検証ログにエントリを作成	- コンポーネントのアップデート - リアルタイム検索を有効化、またはアップデート実行後、クライアントに対して自動でクリーンナップまたは Scan Now を実行します。 - クライアントコンピュータに通知メッセージを表示します。

表 10-3. 初期設定のルール (続き)

ルール名	照合基準	基準に一致した場合の 応答メッ セージ	サーバ 処理	クライアント処理
未保護	リアルタイム検 索が無効です。	Unprotecte d	クライア ント検証 ログにエ ントリを 作成	・ クライアントのリアルタイム 検索を有効にします。 ・ クライアントコンピュータに 通知メッセージを表示します。

ポリシー構成

ポリシーは、任意の数のルールと、ルールで使用するものと同様な初期設定の応答および処理を含んでいます。

ルールの実行

ポリシーサーバは優先順位を指定した特定の順でルールを実行します。ルールの順序を変更したり、新規ルールを追加したり、既存のルールを削除したりできます。

ポリシーに対する初期設定の応答メッセージ

ルールと同様に、ポリシーでは初期設定の応答が用意されており、クライアント検証が発生した場合に、ネットワーク上のウイルスバスター Corp. クライアントの状態を把握するのに役立ちます。しかし初期設定の応答メッセージは、クライアントのセキュリティ状態がポリシーのルールに一致しない場合にのみクライアントと関連付けられます。

ポリシーの応答はルールの応答と同様です（応答のリストについては、332 ページの「ルールに対する初期設定の応答メッセージ」を参照）。

ポリシーサーバとウイルスバスター Corp. クライアント処理

ポリシーサーバは、クライアントの状況情報をポリシーに関連する各ルールに沿ったものにするこ
とで、クライアントに対してルールを実行します。ルールは Web コンソールで指定した使用ルール
に基づき、トップダウンで適用されます。クライアント状況がそのルールと一致する場合、ルール
に対応した処理がクライアントに配信されます。ルールと一致しない場合は、初期設定のルールと
それに対応する処理がクライアントに配信されます。

初期設定の大規模感染モードポリシーが、「正常」のルールを用いたウイルスバスター Corp. クライ
アントを評価します。初期設定の大規模感染モードポリシーによって、ルールに一致しないクライ
アントはすべて、「Infected」応答に対する処理をただちに実行します。

初期設定の通常モードポリシーは、「正常」でないすべてのルール（起動中、未保護、隔離、要検査）
を用いてウイルスバスター Corp. クライアントを評価します。これらのルールに一致しないクライ
アントはすべて「正常」と分類され、「正常」のルールに対する処理が適用されます。

初期設定のポリシー

ポリシーサーバは初期設定のポリシーにより基本的な設定を提供します。利用可能なポリシーは、一般モードと大規模感染モードの2つです。

表 10-4. 初期設定のポリシー

ポリシー名	説明
初期設定の一般モードポリシー	• ポリシーに関係のある初期設定のルール: 起動中、未保護、隔離、要検査 • ルールが一致しない場合の応答: Healthy (正常) • サーバ処理: なし • クライアント処理: なし
初期設定の大規模感染モードポリシー	• ポリシーに関係のある初期設定のルール: 正常 • ルールが一致しない場合の応答: Unprotected (未保護) • サーバ処理: クライアント検証ログにエントリを作成 • クライアント処理: • クライアントのリアルタイム検索を有効にします。 • コンポーネントをアップデートします。 • リアルタイム検索を有効にした後、またはアップデート実行後、クライアントに対して ScanNow を実行します。 • クライアントコンピュータに通知メッセージを表示します。

同期

ポリシーサーバを、登録されたウイルスバスター Corp. サーバと定期的に同期させ、ポリシーサーバのウイルスパターンファイル、ウイルス検索エンジン、サーバの大規模感染予防ステータス（通常モードまたは大規模感染予防モード）をウイルスバスター Corp. サーバと同じ最新バージョンに保ちます。同期を取るためには、以下の方法を使用します。

- **手動**: [概要] 画面でいつでも同期を取ることができます（356 ページの「ポリシーサーバの概要情報の表示」を参照）。
- **予約**: 同期の計画を立てます（359 ページの「管理タスク」を参照）。

証明書

Cisco NAC テクノロジーでは、さまざまなコンポーネント間の正常な通信を確立するために次のデジタル証明書が使用されます。

表 10-5. Cisco NAC 証明書

証明書	説明
ACS 証明書	ACS サーバと証明機関 (CA) サーバ間に信頼された通信を確立します。証明機関サーバが ACS 証明書に署名してから、署名された ACS 証明書を ACS サーバに保存します。
CA 証明書	Cisco ACS サーバによってウイルスバスター Corp. クライアントを認証します。ウイルスバスター Corp. サーバは CA 証明書を ACS サーバとウイルスバスター Corp. クライアント（Cisco Trust Agent と同梱）に配信します。
ポリシーサーバ SSL 証明書	ポリシーサーバと ACS サーバ間の安全な HTTPS 通信を確立します。ポリシーサーバの SSL 証明書は、ポリシーサーバのインストール時に自動的に生成されます。 ポリシーサーバの SSL 証明書の使用は任意です。ただし、これを使用してポリシーサーバと ACS サーバ間で暗号化されたデータのみを送信することをお勧めします。

次の図は、ACS 証明書および CA 証明書の作成と配信に関するステップを示しています。

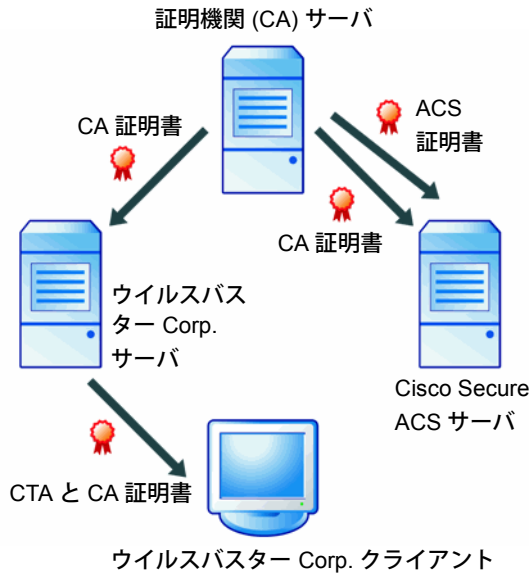


図 10-4. ACS および CA 証明書の作成と配信

1. ACS サーバは CA サーバに対して証明書の署名要求を発行し、CA は ACS 証明書という証明書を発行します。次に ACS 証明書は ACS サーバにインストールされます。詳細については、344 ページの「Cisco Secure ACS サーバ登録」を参照してください。
2. CA 証明書は CA サーバからエクスポートされ、ACS サーバにインストールされます。詳細については、344 ページの「CA 証明書のインストール」を参照してください。
3. CA 証明書のコピーはウイルスバスター Corp. サーバに保存されます。
4. ウイルスバスター Corp. サーバは CA 証明書を CTA によりクライアントに配信します。詳細については、346 ページの「Cisco Trust Agent の配信」を参照してください。

CA 証明書について

CTA がインストールされたウイルスバスター Corp. クライアントでは、ACS サーバが認証されてからクライアントのセキュリティ状態を伝達します。認証にはいくつかの方法があります（詳細については、Cisco Secure ACS のマニュアルを参照してください）。たとえば、Cisco Secure ACS に対するコンピュータの認証が、Windows の Active Directory を使用してすでに有効になっている場合に

は、新しいコンピュータが Active Directory に追加されたときに、エンドユーザクライアント証明書を自動的に作成するよう設定できます。詳細については、Microsoft サポート技術情報 313407「HOWTO: Windows のグループポリシーで自動証明書要求を作成する方法」を参照してください。

独自の証明機関 (CA) サーバを使用しているが、エンドユーザのクライアントはまだ証明書を持っていないユーザには、ウイルスバスター Corp. クライアントに対してルート証明書を配布するメカニズムを提供しています。ウイルスバスター Corp. のインストール中、あるいは Web コンソールから証明書を配布します。ウイルスバスター Corp. では、クライアントへの Cisco Trust Agent の配信時に証明書が配布されます (346 ページの「Cisco Trust Agent の配信」を参照)。

注意： 証明機関 (VeriSign など) からすでに証明書を取得したか、または独自の証明書を作成してエンドユーザクライアントに配布した場合は、これらの作業を再度行う必要はありません。

証明書をクライアントに配布する前に、ACS サーバを CA サーバに登録し、証明書を準備します (344 ページの「Cisco Secure ACS サーバ登録」を参照)。

ポリシーサーバのシステム要件

ポリシーサーバをインストールする前に、コンピュータが次の要件を満たしているか確認してください。

OS

- Windows 2000 Professional (Service Pack 4)
- Windows 2000 Server (Service Pack 4)
- Windows 2000 Advanced Server service Pack 4
- Windows XP Professional (Service Pack 2 以上、32 ビットおよび 64 ビット)
- Windows Server 2003 (Standard および Enterprise Edition) (Service Pack 2 以上、32 ビットおよび 64 ビット)
- Windows Cluster Server 2000

ハードウェア

- 300MHz Intel Pentium II プロセッサまたは同等の CPU
- 128MB の RAM
- 300MB のハードディスク空き容量
- 解像度 800x600、256 色以上をサポートするモニタ

Web サーバ

- Microsoft Internet Information Server (IIS) バージョン 5.0 または 6.0
- Apache Web サーバ 2.0.54 (Windows 2000/XP/Server 2003 の場合のみ)

Web コンソール

Web コンソールを使用するための要件は、以下のとおりです。

- 133MHz Intel Pentium または同等の CPU
- 64MB の RAM
- 30MB のハードディスク空き容量
- 解像度 800x600、256 色以上をサポートするモニタ
- Microsoft Internet Explorer 5.5 以降

Cisco Trust Agent (CTA) の要件

Cisco Trust Agent を配信する前に、コンピュータが以下の要件を満たしていることを確認してください。

OS

- Windows 2000 Professional および Server (Service Pack 4)
- Windows XP Professional (Service Pack 2 以上、32 ビット)
- Windows Server 2003 (Standard および Enterprise Edition) (Service Pack 2 以上、32 ビット)

ハードウェア

- 1 つまたは複数の 200MHz Intel Pentium プロセッサ
- Windows 2000 の場合 : 128MB の RAM
- Windows XP および 2003 の場合 : 256MB の RAM
- 5MB のハードディスク空き容量 (20MB を推奨)

その他

- Windows Installer 2.0 以降

サポートされるプラットフォームと要件

次のプラットフォームは Cisco NAC 機能性をサポートします。

表 10-6. サポートされるプラットフォームと要件

サポートされるプラットフォーム	モデル	IOS イメージ	最小メモリ / フラッシュ
ルータ			
Cisco 830、870 シリーズ	831, 836, 837	IOS 12.3 (8) 以降	48MB/8MB
Cisco 1700 シリーズ	1701、1711、1712、1721、1751、1751-V、1760	IOS 12.3 (8) 以降	64MB/16MB
Cisco 1800 シリーズ	1841	IOS 12.3 (8) 以降	128MB/32MB
Cisco 2600 シリーズ	2600XM、2691	IOS 12.3 (8) 以降	96MB/32MB
Cisco 2800 シリーズ	2801, 2811, 2821, 2851	IOS 12.3 (8) 以降	128MB/64MB
Cisco 3600 シリーズ	3640/3640A、3660-ENT シリーズ	IOS 12.3 (8) 以降	48MB/16MB
Cisco 3700 シリーズ	3745, 3725	IOS 12.3 (8) 以降	128MB/32MB
Cisco 3800 シリーズ	3845, 3825	IOS 12.3 (8) 以降	256MB/64MB
Cisco 7200 シリーズ	720x、75xx	IOS 12.3 (8) 以降	128MB/48MB
VPN コンセントレータ			
Cisco VPN 3000 シリーズ	3005 - 3080	V4.7 以降	該当なし
スイッチ			
Cisco Catalyst 2900	2950, 2970	IOS 12.1 (22) EA5	該当なし

表 10-6. サポートされるプラットフォームと要件 (続き)

サポートされるプラットフォーム	モデル	IOS イメージ	最小メモリ / フラッシュ
Cisco Catalyst 3x00	3550, 3560, 3750	IOS 12.2 (25) SEC	該当なし
Cisco Catalyst 4x00	Supervisor 2+ 以上	IOS 12.2 (25) EWA	該当なし
Cisco Catalyst 6500	6503、6509、 スーパーバイザー 2 以上	CatOS 8.5 以上	Sup2 - 128MB、 Sup32 - 256MB、 Sup720 - 512MB
ワイヤレスアクセスポイント			
Cisco AP1200 シリーズ	1230	該当なし	該当なし

ポリシーサーバのインストール

次の手順は参照用としてのみ示されており、Microsoft と Cisco のいずれかまたは両方のインタフェースのアップデートによって変更される可能性があります。

作業を実行する前に、ネットワーク上のネットワークアクセスデバイスで Cisco NAC がサポート可能になっていることを確認してください (342 ページの「サポートされるプラットフォームと要件」を参照)。設定方法については、デバイスのマニュアルを参照してください。ネットワーク上に ACS サーバもインストールします。方法については、Cisco Secure ACS のマニュアルを参照してください。

1. ネットワーク上にウイルスバスター コーポレートエディション (以下、ウイルスバスター Corp.) サーバをインストールします「インストールガイド」を参照)。
2. ウイルスバスター Corp. クライアントプログラムを、ポリシーサーバでウイルス対策を評価するすべてのクライアントにインストールします。
3. Cisco Secure ACS サーバを登録します。ACS サーバで証明書署名要求を発行することによって、ACS サーバと証明機関 (CA) サーバ間に信頼関係を確立します。その後、CA によって署名された証明書 (ACS 証明書と呼ばれます) を ACS サーバに保存します (344 ページの「Cisco Secure ACS サーバ登録」を参照)。
4. CA 証明書を ACS サーバにエクスポートし、ウイルスバスター Corp. サーバにコピーを保存します。このステップは、クライアントおよび Cisco ACS サーバに証明書を配信していない場合にのみ必要です (344 ページの「CA 証明書のインストール」を参照)。

5. Cisco Trust Agent と CA 証明書をすべてのウイルスバスター Corp. クライアントに配信します。それにより、クライアントはポリシーサーバにセキュリティ状態の情報を提出できます (346 ページの「Cisco Trust Agent の配信」を参照)。
6. Cisco NAC 用ポリシーサーバをインストールし、ACS サーバからのリクエストを管理します (350 ページの「Cisco NAC 用ポリシーサーバのインストール」を参照)。
7. SSL 証明書をポリシーサーバから Cisco ACS サーバへエクスポートして、2 つのサーバ間の安全な SSL 通信を確立します (350 ページの「Cisco NAC 用ポリシーサーバのインストール」を参照)。
8. ACS サーバを設定してセキュリティ状態の検証要求をポリシーサーバに転送するようにします (354 ページの「ACS サーバ設定」を参照)。
9. Cisco NAC 用ポリシーサーバを設定します。ルールやポリシーを作成、変更してウイルスバスター Corp. クライアントに対して組織のセキュリティ戦略を実行します (355 ページの「ポリシーサーバの設定」を参照)。

Cisco Secure ACS サーバ登録

Cisco Secure ACS サーバを証明機関 (CA) サーバに登録して、2 つのサーバ間に信頼関係を確立します。次の手順は、ネットワーク上で証明書を管理するために Windows の証明機関サーバを実行しているユーザを対象としています。他の証明機関アプリケーションまたはサービスを使用している場合はベンダのドキュメントを参照し、証明書の登録方法についての ACS サーバの説明書を参照してください。

CA 証明書のインストール

ウイルスバスター Corp. クライアントでは、ACS サーバが認証されてからセキュリティ状態のデータが送信されます。この認証の実行には、CA 証明書が必要です。まず、CA サーバから CA 証明書を ACS サーバとウイルスバスター Corp. サーバの両方にエクスポートし、次に CTA エージェント配信パッケージを作成します。このパッケージには CA 証明書が含まれています (339 ページの「CA 証明書について」および 346 ページの「Cisco Trust Agent の配信」を参照してください)。

CA 証明書をエクスポートしてインストールするには、次の手順に従ってください。

- CA 証明書を証明機関サーバからエクスポートします。
- それを Cisco Secure ACS サーバにインストールします。
- ウイルスバスター Corp. サーバにコピーを保存します。

注意： 次の手順は、ネットワーク上で証明書を管理するために Windows の証明機関サーバを実行しているユーザを対象としています。別の証明機関のアプリケーションまたはサービスを使用している場合は、ベンダのマニュアルを参照してください。

配置ルート証明書をエクスポートおよびインストールするには

1. 証明書を証明機関 (CA) サーバからエクスポートします。
 - a. CA サーバで、[スタート] → [ファイル名を指定して実行] の順にクリックします。[ファイル名を指定して実行] 画面が表示されます。
 - b. [名前] ボックスに [mmc] を入力します。新しい管理コンソール画面が開きます。
 - c. [ファイル] → [スナップインの追加と削除] の順にクリックします。[スナップインの追加と削除] 画面が表示されます。
 - d. [証明書] をクリックして、[追加] をクリックします。[証明書スナップイン] 画面が表示されます。
 - e. [コンピュータアカウント] をクリックして、[次へ] をクリックします。[コンピュータの選択] 画面が表示されます。
 - f. [ローカルコンピュータ] をクリックして、[完了] をクリックします。
 - g. [閉じる] をクリックして、[スタンドアロンスナップインの追加] 画面を閉じます。
 - h. [OK] をクリックして、[スナップインの追加と削除] 画面を閉じます。
 - i. コンソールのツリービューで、[証明書] → [信頼されたルート証明機関] → [証明書] の順にクリックします。
 - j. クライアントと ACS サーバに配布する証明書を、リストから選択します。
 - k. [操作] → [すべてのタスク] → [エクスポート ...] の順にクリックします。証明書のエクスポートウィザードが開きます。
 - l. [次へ] をクリックします。
 - m. [DER encoded binary x.509] をクリックして、[次へ] をクリックします。
 - n. ファイル名を入力して、証明書のエクスポート先のディレクトリを参照します。
 - o. [次へ] をクリックします。
 - p. [終了] をクリックします。確認画面が表示されます。
 - q. [OK] をクリックします。
2. 証明書を Cisco Secure ACS にインストールします。
 - a. [システム設定] → [ACS 証明書セットアップ] → [ACS 証明書認証セットアップ] の順にクリックします。

- b. 証明書の完全なパスとファイル名を、[CA 証明書ファイル] フィールドに入力します。
 - c. [送信] をクリックします。Cisco Secure ACS の再起動を求められます。
 - d. [システム設定] → [サービスコントロール] の順にクリックします。
 - e. [再起動] をクリックします。Cisco Secure ACS が再起動します。
 - f. [システム設定] → [ACS 証明書セットアップ] → [証明書信頼性リストの編集] の順にクリックします。[証明書信頼性リストの編集] 画面が表示されます。
 - g. ステップ b でインポートした証明書に対応するチェックボックスをオンにして、[送信] をクリックします。Cisco Secure ACS の再起動を求められます。
 - h. [システム設定] → [サービスコントロール] の順にクリックします。
 - i. [再起動] をクリックします。Cisco Secure ACS が再起動します。
3. 証明書 (CER ファイル) を CTA と一緒にクライアントに配信できるように、ウイルスバスター Corp. サーバがインストールされているコンピュータにコピーします (346 ページの「Cisco Trust Agent の配信」を参照)。

注意： 証明書をローカルドライブに保存してください。割り当てドライブには保存できません。

Cisco Trust Agent の配信

Cisco Trust Agent (CTA) は、ウイルスバスター Corp. サーバ内でホストされるプログラムであり、クライアントにインストールされます。CTA により、ウイルスバスター Corp. クライアントが、Cisco ACS にウイルス対策情報をレポートできるようになります。

ウイルスバスター Corp. サーバをインストールする際の CTA の配信

ウイルスバスター Corp. サーバをインストールする前に、すでに CA 証明書が準備されている場合は、ウイルスバスター Corp. サーバをインストールする際に、CTA エージェントを配信します。CTA 配信オプションは、セットアップの [その他のウイルスバスター Corp. プログラムをインストールする] 画面にあります。ウイルスバスター Corp. サーバのインストールの手順については、「インストールガイド」を参照してください。

ウイルスバスター Corp. サーバのインストールプログラムを使用して CTA をクライアントにインストールするには

1. [その他のウイルスバスター Corp. プログラムをインストールする] 画面で、[Cisco NAC 用 Cisco Trust Agent] を選択します。
2. 次のいずれかを実行します。

- 証明書をすでに Cisco Secure NAC エンドユーザクライアントに配布した場合は、[次へ] をクリックします。
 - 証明書をクライアントに配布する必要がある場合は、次の手順に従ってください。
 - i. [証明書のインポート] をクリックします。
 - ii. 準備した証明書ファイルを参照、選択し、[OK] をクリックしてください。CA 証明書の準備方法については、344 ページの「CA 証明書のインストール」を参照してください。
 - iii. [次へ] をクリックします。
3. ウイルスバスター Corp. サーバインストールプログラムを続行します。

ウイルスバスター Corp. Web コンソールからの CTA の配信

サーバをインストールする際に、CTA のインストールまたはアップグレードのオプションを選択しなかった場合は、Web コンソールからそれを実行することができます。CTA をインストールまたはアップグレードする前に、クライアントにクライアント証明書を配信してください。

注意： 証明機関 (CA) サーバは、クライアント証明書ファイルを生成します。トレンドマイクロの販売代理店を通じて証明書ファイルを要求してください。

インストールまたはアップグレードの準備ができたなら、インストールする CTA のバージョンを [Cisco NAC] → [エージェント管理] で確認してから、[Cisco NAC] → [エージェント配信] で CTA をクライアントにインストールします。[エージェント配信] 画面には、CTA をアンインストールするためのオプションもあります。

Windows 2000/XP を実行しているウイルスバスター Corp. クライアント上に Windows Installer 2.0 for NT 4.0 をインストールしてから、CTA を配信します。

クライアント証明書のインポート

クライアント (または CA) 証明書は、Cisco ACS サーバによってエンドユーザクライアントを認証します。ウイルスバスター Corp. サーバは、CA 証明書を Cisco Trust Agent (CTA) とともにクライアントに配信します。そのため、CTA を配信する前に、ウイルスバスター Corp. サーバに証明書をインポートします。

証明書をインポートするには

1. ウイルスバスター Corp. サーバの Web コンソールを開き、[Cisco NAC] → [クライアント認証ファイル] の順にクリックします。
2. 証明書の正確なファイルパスを入力します。
3. サーバ上に保存されている、準備した CA 証明書の完全なパスとファイル名を入力します (例: C:\¥CiscoNAC¥certificate.cer)。CA 証明書の準備方法については、344 ページの「CA 証明書のインストール」を参照してください。
4. [インポート] をクリックします。フィールドをクリアするには、[リセット] をクリックします。

Cisco Trust Agent のバージョン

CTA をクライアントにインストールする前に、インストールする CTA のバージョン (Cisco Trust Agent または Cisco Trust Agent Supplicant) を確認してください。これらの 2 つのバージョン間の唯一の違いは、Supplicant パッケージがコンピュータとエンドユーザに対するレイヤ 2 認証を提供することです。

Cisco NAC Access Control Server (ACS) がバージョン 4.0 以降の場合は、クライアント上の Cisco Trust Agent をバージョン 2.0 以降にアップグレードしてください。

CTA のバージョンを確認するには

1. ウイルスバスター Corp. サーバの Web コンソールを開き、[Cisco NAC] → [エージェント管理] の順にクリックします。
2. [<CTA のバージョン> を使用] をクリックします。ウイルスバスター Corp. サーバが、新しいバージョンの使用を開始します。

CTA パッケージを手動で置換するには

使用したい特定のバージョンの CTA がある場合は、ウイルスバスター Corp. サーバ上の CTA パッケージを手動で置換します。

1. 使用したい CTA バージョンで、CTA .msi ファイルを次のフォルダへコピーします。
＜「サーバのインストールフォルダ」＞¥PCCSRV¥Admin¥Utility¥CTA¥CTA-Package
(または)
＜「サーバのインストールフォルダ」＞¥PCCSRV¥Admin¥Utility¥CTA¥CTA-Supplicant-Package
2. 次のファイルを＜「サーバのインストールフォルダ」＞¥PCCSRV¥Admin¥Utility¥CTA¥PosturePlugin にコピーします。TmabPP.dll、tmabpp.inf、および TmAbPpAct.exe

3. Web コンソールで、[Cisco NAC] → [エージェント管理] を選択し、[<CTA のバージョン> を使用] をクリックします。

エージェントのアップグレード後、CTA は配信ファイルを PostureAgent.zip としてパッケージにして、<「サーバのインストールフォルダ」>%PCCSRV%download%Product の下に保存します。

Cisco Trust Agent の配信

ウイルスバスター Corp. クライアントが Cisco ACS にウイルス対策情報をレポートできるようにするには、Cisco Trust Agent を配信します。

ウイルスバスター Corp. Web コンソールから CTA をクライアントに配信するには

1. ウイルスバスター Corp. サーバの Web コンソールを開き、[エージェント配信] をクリックします。クライアントツリーが表示されます。

注意： ウイルスバスター Corp. サーバのインストール時に Cisco の使用許諾契約書に同意しなかった場合、エージェントを配信することはできません。[エージェント配信] をクリックすると、ライセンス情報が再び表示されます。使用許諾契約書を読み、条件に同意する場合は [はい] をクリックします。

2. CTA をインストールするクライアントまたはドメインを選択して、サイドバーの [エージェント配信] をクリックします。[エージェントのインストール / アンインストール] 画面が表示されます。
3. [Cisco Trust Agent をインストール / アップグレードする] をクリックします。必要に応じて、ウイルスバスター Corp. クライアントのアンインストール時に、Cisco Trust Agent をアンインストールするように選択します。

注意： また、クライアント上の CTA ステータスをアンインストールまたは保持するためにも、この画面を使用します。

4. クライアントツリーのドメインまたはクライアントを選択している場合は、[保存] をクリックすると設定がドメインまたはクライアントに適用されます。ルートアイコン  を選択した場合は、次のオプションのいずれかを選択します。
 - **すべてのクライアントに適用：** すべての既存のクライアント、および既存または将来追加されるドメインに加えられる新しいクライアントに、設定を適用します。将来追加されるドメインとは、設定を指定した時点で作成されていないドメインのことです。

- **将来追加されるドメインにのみ適用**：将来追加されるドメインに加えられるクライアントにのみ設定を適用します。このオプションでは、既存のドメインに加えられる新しいクライアントには設定を適用しません。

注意： [Cisco Trust Agent をインストールする] をクリックするときにエージェントの配信先クライアントがオンラインになっていない場合は、そのクライアントがオンラインになったときに、ウイルスバスター Corp. によって配信リクエストが自動的に実行されます。

Cisco Trust Agent のインストールの確認

CTA をクライアントにインストールしたら、クライアントツリーを表示してインストールが正常に実行されたことを確認します。クライアントツリーには、[アップデート表示]、[すべて表示]、または [ウイルス対策表示] の各表示で [CTA プログラム] という名前の列が表示されます。正常な CTA インストールには、CTA プログラムのバージョン番号が含まれます。

また、クライアントのコンピュータに以下のプロセスが起動しているかどうかを確認することもできます。

- ctapsd.exe
- ctaEoU.exe
- ctatransapt.exe
- ctalogd.exe

Cisco NAC 用ポリシーサーバのインストール

ポリシーサーバをインストールする方法は、2 つあります。

- 製品 DVD にあるポリシーサーバインストール
- ウイルスバスター Corp. サーバセットアッププログラム（これによって、ウイルスバスター Corp. サーバとポリシーサーバの両方が同一のコンピュータにインストールされます）。

注意： セットアッププログラムにより、ウイルスバスター Corp. サーバとポリシーサーバ Web コンソールの両方が IIS Web サーバまたは Apache Web サーバにインストールされます。インストールプログラムがシステム上に Apache サーバを見つけないことができないか、既存の Apache サーバのインストールが 2.0.54 のバージョンでない場合、インストールプログラムは自動的に Apache 2.0.54 をインストールします。

有効な通信環境を確保するには、ACS サーバ、ポリシーサーバ、およびウイルスバスター Corp. サーバを同一のネットワークセグメントに配置してください。

Apache Web サーバをインストールする前に、次の Apache の Web サイトで、アップグレード、Patch、およびセキュリティに関する問題についての最新情報を調べてください。

<http://www.apache.org>

ポリシーサーバインストーラを使用してポリシーサーバをインストールするには

1. ポリシーサーバをインストールするコンピュータにログオンします。
2. 製品 CD-ROM 内のポリシーサーバ インストーラパッケージを探します。
3. setup.exe をダブルクリックして、インストーラパッケージを実行します。
4. インストール手順に従います。

ポリシーサーバは、ウイルスバスター Corp. サーバと同じコンピュータにインストールすることもできます。

ウイルスバスター Corp. サーバインストーラからポリシーサーバをインストールするには

1. ウイルスバスター Corp. サーバインストールプログラムの [他のウイルスバスター Corp. プログラムをインストール] 画面で、[Policy Server for Cisco NAC] を選択します。
2. [次へ] をクリックします。
3. ポリシーサーバの「ようこそ」画面が表示されるまで、ウイルスバスター Corp. サーバのインストールを続行します。
4. [次へ] をクリックします。ポリシーサーバ使用許諾契約画面が表示されます。
5. 使用許諾契約を読み、[はい] をクリックして次に進みます。インストール先の選択画面が表示されます。
6. 必要に応じて、[参照] をクリックしてポリシーサーバの新しいインストール先を選択し、初期設定のインストール先を変更します。
7. [次へ] をクリックします。Web サーバ画面が表示されます。
8. ポリシーサーバの Web サーバを選択します。

- IIS サーバ: 既存の IIS Web サーバにインストールされます。
 - Apache 2.0 Web サーバ: Apache 2.0.54 Web サーバにインストールされます。
9. [次へ] をクリックします。Web サーバ設定画面が表示されます。
10. 以下の情報を設定します。
- a. ポリシーサーバを IIS サーバにインストールすることを選択した場合、以下のうちの 1 つを選択してください。
 - **IIS 既定 Web サイト**: IIS 既定 Web サイトとしてインストールします。
 - **IIS 仮想 Web サイト**: IIS 仮想 Web サイトとしてインストールします。
 - b. [ポート番号] で、サーバ待機ポートのポート番号を入力します。ポリシーサーバとウイルスバスター Corp. サーバが同じコンピュータおよび同じ Web サーバにインストールされている場合、次のようにポートが使用されます。
 - **既定 Web サイトの Apache Web サーバまたは IIS Web サーバの場合**: ポリシーサーバとウイルスバスター Corp. サーバは同じポートを共有します。
 - **両方が仮想 Web サイトの IIS Web サーバにある場合**: ポリシーサーバの初期設定の待機ポートは 8081、SSL ポートは 4344 です。ウイルスバスター Corp. サーバの初期設定の待機ポートは 8080、SSL ポートは 4343 です。
 - c. ポリシーサーバを IIS サーバにインストールすることを選択した場合、SSL (Secure Socket Layer) を使用できます。SSL 証明書を有効にする年数 (初期設定は 3 年) および SSL ポート番号を入力します。SSL を有効にした場合、このポート番号はサーバの待機ポートとして機能します。ポリシーサーバの URL は、次のようになります。
 - http://< ポリシーサーバ名 >:< ポート番号 > または
 - https://< ポリシーサーバ名 >:< ポート番号 > (SSL が有効な場合)
11. [次へ] をクリックします。
12. ポリシーサーバコンソールパスワードを指定し、[次へ] をクリックします。
13. ACS サーバ認証パスワードを指定し、[次へ] をクリックします。
14. インストール設定を確認します。設定を確認したら、[次へ] をクリックしてインストールを開始します。または、[戻る] をクリックして前の画面に戻ります。
15. インストールが完了したら、[閉じる] をクリックします。ウイルスバスター Corp. サーバセットアッププログラムは、インストールの残りを続行します。

ポリシーサーバ SSL 証明書の準備

ACS サーバとポリシーサーバ間に安全な SSL 接続を確立するには、SSL の使用を目的とした証明書を準備します。SSL 証明書は、ポリシーサーバのセットアップ時に自動的に生成されます。

配布のためにポリシーサーバの SSL 証明書を準備するには

1. mmc のポリシーサーバから証明書をエクスポートします。

ポリシーサーバが IIS を起動している場合：

- a. ポリシーサーバで、[スタート] → [ファイル名を指定して実行] の順にクリックします。
[ファイル名を指定して実行] 画面が表示されます。
- b. [名前] ボックスに [mmc] を入力します。新しい管理コンソール画面が開きます。
- c. [コンソール] → [スナップインの追加と削除] の順にクリックします。[スナップインの追加と削除] 画面が表示されます。
- d. [追加] をクリックします。[スタンドアロンスナップインの追加] 画面が表示されます。
- e. [証明書] をクリックして、[追加] をクリックします。[証明書スナップイン] 画面が表示されます。
- f. [コンピュータアカウント] をクリックして、[次へ] をクリックします。[コンピュータの選択] 画面が表示されます。
- g. [ローカルコンピュータ] をクリックして、[完了] をクリックします。
- h. [閉じる] をクリックして、[スタンドアロンスナップインの追加] 画面を閉じます。
- i. [OK] をクリックして、[スナップインの追加と削除] 画面を閉じます。
- j. コンソールのツリービューで、[証明書 (ローカルコンピュータ)] → [信頼されたルート証明機関] → [証明書] の順にクリックします。
- k. リストから証明書を選択します。

注意： 証明書の拇印を確認するには、該当する証明書を右クリックして、[プロパティ] を選択します。拇印は、IIS コンソールに配置された証明書の拇印と同一でなければなりません。

これを確認するには、IIS コンソールを開き、インストールしたポリシーサーバの Web サイトに応じて仮想 Web サイトまたは既定 Web サイトのいずれかを右クリックし、[プロパティ] を選択します。[ディレクトリセキュリティ] をクリックしてから [証明書] [表示] をクリックして、拇印などの証明書の詳細を確認します。

- l. [操作] → [すべてのタスク] → [エクスポート ...] の順にクリックします。証明書のエクスポートウィザードが開きます。
- m. [次へ] をクリックします。
- n. [DER encoded binary x.509] または [Base 64 encoded X.509] をクリックして、[次へ] をクリックします。
- o. ファイル名を入力して、証明書のエクスポート先のディレクトリを参照します。
- p. [次へ] をクリックします。
- q. [終了] をクリックします。確認画面が表示されます。
- r. [OK] をクリックします。

ポリシーサーバが Apache 2.0.54 を起動している場合：

- a. 証明書ファイル server.cer を取得します。ファイルの場所は、ウイルスバスター Corp. サーバとポリシーサーバのどちらを先にインストールしたかによって異なります。
 - ウイルスバスター Corp. サーバをポリシーサーバより先にインストールした場合、ファイルは以下のディレクトリにあります。
<「サーバのインストールフォルダ」>%PCCSRV%\Private%\certificate
 - ポリシーサーバをウイルスバスター Corp. サーバより先にインストールした場合、ファイルは以下のディレクトリにあります。
<「サーバのインストールフォルダ」>%PolicyServer%\Private%\certificate
 - b. 証明書ファイルを ACS サーバにコピーします。
2. 証明書を Cisco Secure ACS にインストールします。
- a. ACS 管理コンソールで、[システム設定] → [ACS 証明書セットアップ] → [ACS 証明書認証セットアップ] の順にクリックします。
 - b. 証明書の完全なパスとファイル名を、[CA 証明書ファイル] フィールドに入力します。
 - c. [送信] をクリックします。Cisco Secure ACS の再起動を求められます。
 - d. [システム設定] → [サービスコントロール] の順にクリックします。
 - e. [再起動] をクリックします。Cisco Secure ACS が再起動します。

ACS サーバ設定

認証要求を Cisco Secure ACS からポリシーサーバに渡せるようにするには、ポリシーサーバを認証に使用する外部ユーザデータベースの [外部ポリシー] に追加します。新規の外部ポリシーにポリシーサーバを追加する方法については、ACS サーバのドキュメントを参照してください。

注意： ACS サーバを設定して、ネットワークへのクライアントのアクセスをブロックするなどのタスクを実行します。このような ACS 機能はトレンドマイクロのポリシーサーバ実装の領域を超えるので、このマニュアルでは説明しません。その他の ACS の機能設定の詳細については、ACS のマニュアルを参照してください。

ポリシーサーバの設定

ウイルスバスター Corp. およびポリシーサーバをインストールして、ウイルスバスター Corp. クライアントおよび Cisco Trust Agent を配信した後で、ポリシーサーバを設定します。ポリシーサーバを設定するには、[Cisco NAC] → [ポリシーサーバ] でウイルスバスター Corp. Web コンソールのポリシーサーバ Web コンソールにアクセスし、ポリシーサーバリンクをクリックします。

ここでは、ポリシーサーバの設定に関する次の内容について説明します。

- 355 ページの「ウイルスバスター Corp. からのポリシーサーバ設定」は、ウイルスバスター Corp. Web コンソールでポリシーサーバを管理する方法について説明します。
- 356 ページの「ポリシーサーバの概要情報の表示」では、ネットワーク上のポリシーサーバの概要を把握する方法について説明します。
- 357 ページの「ポリシーサーバ登録」は、ポリシーサーバの設定の最初のステップです。
- 358 ページの「ルール」では、ポリシーを構成するルールを作成および編集する方法について説明します。
- 358 ページの「ポリシー」では、ポリシーサーバがクライアントのセキュリティ状態を測定し最終的に判定するためのポリシーを作成および編集する方法について説明します。
- 358 ページの「クライアント検証ログ」では、ログを使用して、ネットワーク上のクライアントのセキュリティ状態を理解する方法の概要を示します。
- 359 ページの「管理タスク」では、ポリシーサーバのパスワードの変更方法と同期スケジュールの設定方法について説明します。

ウイルスバスター Corp. からのポリシーサーバ設定

ポリシーサーバ設定の最初のステップは、インストールしたポリシーサーバをウイルスバスター Corp. サーバに追加することです。これによって、ウイルスバスター Corp. Web コンソールからポリシーサーバ Web コンソールを開くことができます。

ポリシーサーバを追加するには

1. ウイルスバスター Corp. Web コンソールのメインメニューから、[Cisco NAC] → [ポリシーサーバ] をクリックします。[ポリシーサーバ] 画面が表示され、ポリシーサーバのサーバ名 (URL) のリストが表示されます。
2. [追加] をクリックします。[ポリシーサーバ] 画面が表示されます。
3. ポリシーサーバのアドレス (URL)、およびポリシーサーバで HTTPS 通信に使用するポート番号を入力します (例: https://{ポリシーサーバ}:4343/)。サーバのオプション情報も入力します。
4. ポリシーサーバ Web コンソールにログオンするときに使用するパスワードを入力します。
5. [追加] をクリックします。

ポリシーサーバを削除するには

1. ウイルスバスター Corp. Web コンソールのメインメニューから、[Cisco NAC] → [ポリシーサーバ] をクリックします。[ポリシーサーバ] 画面が表示され、ポリシーサーバのサーバ名 (URL) のリストが表示されます。
2. 削除するポリシーサーバのチェックボックスを選択します。
3. [削除] をクリックします。

注意： ネットワーク上の全クライアントを検証するには、すべてのウイルスバスター Corp. サーバに少なくとも 1 台のポリシーサーバを追加する必要があります。

ポリシーサーバの概要情報の表示

[概要] 画面には、ポリシーとルール、クライアント検証ログ、ポリシーサーバに登録されたウイルスバスター Corp. サーバの環境設定を含むポリシーサーバの情報が表示されます。

Cisco NAC 用ポリシーサーバの IP アドレスとポート番号は概要画面のトップに表示されます。

[設定の概要] 表には、ポリシーサーバに登録されたウイルスバスター Corp. サーバの数、ポリシーサーバのポリシー数、およびポリシーを構成するルール数が表示されます。

ポリシーサーバに対する設定詳細を表示 / 変更するには

1. ウイルスバスター Corp. Web コンソールのメインメニューから、[Cisco NAC] → [ポリシーサーバ] をクリックします。[ポリシーサーバ] 画面が表示され、ポリシーサーバのサーバ名 (URL) のリストが表示されます。
2. 詳細を表示するポリシーサーバのサーバ名をクリックします。[概要] 画面に、[設定の概要] 表が表示されます。
3. 環境設定を表示する項目の隣にあるリンクをクリックします。

- **登録済みウイルスバスター Corp. サーバ**：現在ポリシーサーバに登録されているウイルスバスター Corp. サーバの数
- **ポリシー**：登録済みウイルスバスター Corp. サーバが使用できるポリシーサーバポリシー
- **ルール**：ポリシーを構成するポリシーサーバルール

ヒント： ネットワーク上の複数のポリシーサーバに同一設定、同一ルールおよびポリシーを持たせる場合、1 台のサーバから設定をエクスポートし、それらを残りのサーバにインポートします。

トレンドマイクロはネットワーク上のすべてのポリシーサーバに同じ設定をするように推奨します。それは首尾一貫したウイルス対策ポリシーをサポートするためです。

ポリシーサーバと登録済みウイルスバスター Corp. サーバを同期するには

概要画面で、[ウイルスバスター Corp. サーバと同期] をクリックします。[概要 - 同期の結果] 画面に、次の読み取り専用情報が表示されます。

- **ウイルスバスター Corp. サーバ名**：登録済みのウイルスバスター Corp. サーバのホスト名または IP アドレスとポート番号
- **同期の結果**：同期化に成功したかどうかを表示します。
- **最終同期日**：正常に実行された前回の同期の日時

同期の詳細については、338 ページの「同期」を参照してください。

ポリシーサーバ登録

ウイルスパターンファイルおよびウイルス検索エンジンのバージョン情報を取得するためには、ポリシーサーバを少なくとも 1 台のウイルスバスター Corp. サーバに登録する必要があります。検証プロセスにおいてウイルスバスター Corp. サーバが実行する役割の詳細については、328 ページの「クライアント検証シーケンス」を参照してください。

注意： ポリシーサーバがネットワーク上のすべてのクライアントを検証するには、すべてのウイルスバスター Corp. サーバを少なくとも 1 台のポリシーサーバに追加します。

ポリシーサーバ Web コンソールで、[設定] → [ウイルスバスター Corp. サーバ] をクリックし、ウイルスバスター Corp. サーバ画面から、新規のウイルスバスター Corp. サーバを追加または既存の設定を編集します。

ルール

ルールはポリシーの構成要素です。次のステップではポリシーサーバ設定でルールを設定します。ルールの詳細については、331 ページの「ルール構成」を参照してください。

Cisco ACS ルールの Web コンソール画面にアクセスするには、ポリシーサーバの Web コンソールのメインメニューから、[設定] → [ルール] をクリックします。

ポリシー

新規ルール設定するか、セキュリティ強化のニーズに初期設定のルールが適していることを確認した後、登録済みのウイルスバスター Corp. サーバが使用可能なポリシーを設定します。ポリシーの詳細については、336 ページの「ポリシー構成」を参照してください。

新しいポリシーを追加するか、または既存のポリシーを編集して、実行するルールを決定し、また、クライアントのセキュリティ状態がルールに一致しない場合のクライアントでの処理を設定します。

Cisco ACS ルールの Web コンソール画面にアクセスするには、ポリシーサーバの Web コンソールのメインメニューから [設定] → [ポリシー] をクリックします。

クライアント検証ログ

ポリシーサーバによりクライアントを検証すると、クライアント検証ログにクライアントの詳細情報が表示されます。検証が発生するのは、ACS サーバがクライアントのセキュリティ状態のデータを取得し、そのデータをポリシーサーバに送信して、ポリシーサーバでデータがポリシーおよびルールと比較される場合です (328 ページの「クライアント検証シーケンス」を参照)。

注意： クライアント検証ログを生成するには、新規ルールまたはポリシーを追加または編集時に、[サーバ側の処理] の下のチェックボックスを選択します。

Cisco ACS ログの Web コンソール画面にアクセスするには、ポリシーサーバの Web コンソールのメインメニューから、[ログ] → [クライアント検証ログの表示] をクリックします。

クライアントログのメンテナンス

クライアント検証ログは、指定したサイズに達するとアーカイブされます。また、蓄積したログファイルの数が一定以上になった場合にログファイルを削除することもできます。ポリシーサーバによるクライアント検証ログのメンテナンス方法を指定するには、ポリシーサーバ Web コンソールから、[ログ] → [ログメンテナンス] をクリックします。

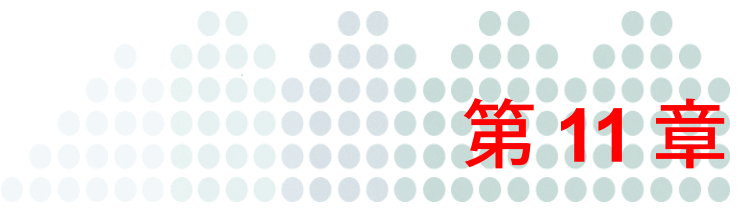
管理タスク

ポリシーサーバで次の管理作業を実行します。

- パスワードの変更: ポリシーサーバの追加時に設定したパスワードを変更します (355 ページの「ウイルスバスター Corp. からのポリシーサーバ設定」を参照)。
- 同期スケジュールの設定: ポリシーサーバでは、ウイルスバスター Corp. クライアントのセキュリティ状態を評価するために、ウイルスバスター Corp. サーバのウイルスパターンファイルおよびウイルス検索エンジンのバージョンを定期的に取得する必要があります。したがって、同期設定を無効にすることはできません。初期設定では、ポリシーサーバはウイルスバスター Corp. サーバと 5 分ごとに同期されます (詳細については、338 ページの「同期」を参照してください)。

注意: [概要] 画面で、ウイルスバスター Corp. サーバとポリシーサーバをいつでも手動で同期できます (356 ページの「ポリシーサーバの概要情報の表示」を参照)。

Cisco ACS 管理タスクの Web コンソール画面にアクセスするには、ポリシーサーバの Web コンソールのメインメニューから [管理] をクリックします。



第11章

サードパーティソフトウェアでのウイルス バスター Corp. の設定

この章で説明する内容には、次の項目が含まれます。

- 362 ページの「Check Point ファイアウォールのアーキテクチャの概要と設定」
- 364 ページの「ウイルスバスター Corp. 用 Check Point の設定」
- 366 ページの「SecureClient サポートのインストール」

Check Point ファイアウォールのアーキテクチャの概要と設定

OPSEC フレームワーク内の SVC を使用することで、ウイルスバスター コーポレートエディション (以下、ウイルスバスター Corp.) を Check Point Secure Client に統合します。このセクションを開始する前に、Check Point SecureClient OPSEC のドキュメントをよく読んでください。OPSEC のドキュメントに関する詳細は、次のサイトを参照してください。

<http://www.opsec.com>

Check Point SecureClient は、Secure Configuration Verification (SCV) を使用して、ネットワークに接続されているコンピュータのセキュリティ機能を検証します。SCV チェックとは、セキュリティ対策が安全に設定されているクライアントを定義する条件のセットです。ウイルス対策製品は、安全な設定を定義する条件値を SecureClient に伝達することができます。SecureClient は、ウイルス対策製品から伝達された情報を SCV ファイルの値と比較し、クライアントが安全かどうかを判別します。

SCV チェックは定期的に実行され、セキュリティ対策が適切に設定されたクライアントだけがネットワークに接続できるようにします。

SecureClient は、ポリシーサーバを使用して、システムに登録されたすべてのクライアントに SCV チェックを適用します。管理者は、SCV Editor を使用して、ポリシーサーバの SCV チェックを設定することができます。

SCV Editor は、クライアントに伝播する SCV ファイルを変更するためのツールで、Check Point 社から提供されます。SCV Editor を起動するには、ポリシーサーバ上で SCVeditor.exe を実行します。SCV Editor を起動したら、C:\FW1\NG\Conf (初期設定を変更している場合、C:\FW1 を Check Point ファイアウォールのインストールパスに変更) フォルダの local.scv ファイルを開きます。

SCV Editor を使用して SCV ファイルを変更する方法の詳細については、364 ページの「ウイルスバスター Corp. 用 Check Point の設定」を参照してください。

ウイルスバスター Corp. の統合

ウイルスバスター Corp. クライアントは、検証のために、パターンファイル番号と検索エンジンバージョンの情報を定期的に SecureClient に渡します。SecureClient はその情報をクライアントの local.scv ファイルと比較します。

テキストエディタで local.scv ファイルを開くと、次のように表示されます。

```
(SCVObject
:SCVNames (
: (OfceSCV
:type (plugin)
:parameters (
:CheckType (OfceVersionCheck)
:LatestPatternVersion (701)
:LatestEngineVersion (7.1)
:PatternCompareOp (">=")
:EngineCompareOp (">=")
)
)
)
:SCVPolicy (
: (OfceSCV)
)
:SCVGlobalParams (
:block_connections_on_unverified (true)
:scv_policy_timeout_hours (24)
)
)
```

この例では、パターンファイルのバージョンが 701 以降で、検索エンジンのバージョンが 7.1 以降である場合、CheckPoint ファイアウォールを介したコンピュータの接続が許可されます。検索エンジンまたはパターンファイルがそれよりも古い場合、ファイアウォールを介しての通信はブロックされます。これらの値を変更するには、SCV Editor を使用して、ポリシーサーバ上の local.scv ファイルを変更します。

注意： SCV ファイル内のパターンファイルおよび検索エンジンのバージョン番号は自動的に更新されません。検索エンジンまたはパターンファイルをアップデートした場合、local.scv ファイル内の値を手動で変更する必要があります。local.scv ファイル内の検索エンジンとパターンファイルの情報を最新にしないと、前のバージョンの検索エンジンまたはパターンファイルを使用しているクライアントからの接続が許可され、システムに新規ウイルスが侵入してしまう危険性があります。

ウイルスバスター Corp. 用 Check Point の設定

local.scv ファイルを変更するには、SCV Editor (SCVeditor.exe) をダウンロードし、実行してください。

SCV ファイルを設定するには

1. Check Point 社の Web サイトから、SCVeditor.exe をダウンロードします。SCV Editor は OPSEC SDK パッケージの一部です。
2. ポリシーサーバ上で SCVeditor.exe を実行します。SCV Editor コンソールが開きます。
3. [Products] フォルダを開き、[user_policy_scv] を選択します。
4. [Edit] → [Product] → [Modify] の順にクリックし、[Modify] テキストボックスに OfceSCV を入力します。[OK] をクリックします。

注意： local.scv にすでに別製品のポリシーが含まれる場合は、[Edit] → [Product] → [Add] の順にクリックし、[Add] テキストボックスに「OfceSCV」と入力し、ウイルスバスター Corp. 用に新規ポリシーを作成します。

5. [Edit] → [Parameters] → [Add] の順にクリックし、該当する [Name] および [Value] をそれぞれのテキストボックスに入力して、パラメータを追加します。次の表は、パラメータの名前と

値をリストしたものです。パラメータ名および値の入力では大文字と小文字が区別されます。表の順番どおりに入力してください。

表 11-1. SCV ファイルパラメータ名と値

管理下の製品 / フォルダ名	値
CheckType	OfceVersionCheck
LatestPatternVersion	< 現在のパターンファイルの番号 >
LatestEngineVersion	< 現在の検索エンジンの番号 >
LatestPatternDate	< 現在のパターンファイルの配布日 >
PatternCompareOp	>=
EngineCompareOp	>=
PatternMismatchMessage	
EngineMismatchMessage	

中カッコのテキストの部分、最新のパターンファイル番号と検索エンジンバージョン番号に置き換えます。最新のパターンファイルおよび検索エンジンのバージョン番号は、ウイルスバスター Corp. 管理コンソールのサイドバーで [アップデート] をクリックすることによって表示します。パターンファイルのバージョン番号は、クライアントの保護の割合を表す円グラフの右上に表示されます。

6. [Block connections on SCV unverified] を選択します。
7. [Edit] → [Product] → [Enforce] の順にクリックします。
8. [File] → [Generate Policy File] の順にクリックして、ファイルを生成します。既存の local.scv ファイルを選択して、上書きします。

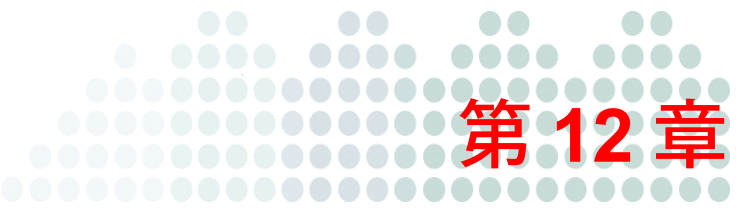
SecureClient サポートのインストール

SecureClient サポートは、VPN (Virtual Private Network) を使用したオフィスネットワークで、Check Point SecureClient がインストールされたクライアントコンピュータにインストール可能なモジュールです。このモジュールにより、SecureClient は VPN クライアントに対する SCV チェックが実行でき、セキュリティ対策が適切に設定されたクライアントだけがネットワークに接続できるようになります。

Check Point SecureClient がコンピュータにインストールされているかどうかを確認するには、Windows のタスクトレイに  アイコンが表示されているかどうかで確認できます。または、Windows の [アプリケーションの追加と削除] を使用しても確認できます。

SecureClient サポートをインストールするには

1. ウイルスバスター Corp. クライアントのメイン画面を起動します。
2. [ツールボックス] タブをクリックします。
3. [Check Point SecureClient サポート] グループの [SecureClient サポートのインストール] をクリックします。確認画面が表示されます。
4. [Yes] をクリックします。クライアントはサーバに接続し、モジュールをダウンロードします。ダウンロードが完了すると、メッセージが表示されます。
5. [OK] をクリックします。



第12章

サポート情報

この章で説明する内容には、次の項目が含まれます。

- 368 ページの「トラブルシューティングのリソース」
- 380 ページの「製品サポート情報」
- 380 ページの「サポートサービスについて」
- 381 ページの「製品 Q&A のご案内」
- 381 ページの「ウイルス解析サポートセンター「TrendLabs」」
- 381 ページの「セキュリティ情報」

トラブルシューティングのリソース

このセクションでは、ウイルスバスター Corp. サーバのトラブルシューティングと、クライアントの問題において使用できるリソースのリストを提供します。

- 「ケース診断ツール」
- 「ウイルスバスター Corp. サーバログ」
- 「ウイルスバスター Corp. クライアントログ」

ケース診断ツール

トレンドマイクロのケース診断ツール (cdt) は、問題が発生した場合にお客さまの製品から必要なデバッグ情報を収集します。そして、製品のデバッグステータスをオンまたはオフに自動的に切り替えて、問題のカテゴリに従って必要なファイルを収集します。トレンドマイクロはこの情報を使用して、製品に関連する問題をトラブルシューティングします。

ウイルスバスター Corp. でサポートされるすべてのプラットフォームでツールを実行します。このツールと関連マニュアルの入手については、サポート担当者にお問い合わせください。

ウイルスバスター Corp. サーバログ

Web コンソールで利用可能なログの他にも、製品の問題に対するトラブルシューティングに、その他の種類のログ（デバッグログなど）を使用できます。

警告： デバッグログはサーバの性能に影響を与え、大量のディスク空き容量を消費する可能性があります。必要な時にのみデバッグログ生成を有効にし、デバッグデータが不要になった場合はただちに無効にしてください。ファイルサイズが巨大になった場合はログファイルを削除してください。

LogServer.exe を使用するサーバデバッグログ

LogServer.exe を使用して以下に対するデバッグログを収集します。

- ウイルスバスター Corp. サーバの基本ログ
- トレンドマイクロ脆弱性検索ツール
- Active Directory を利用するウイルスバスター Corp. の機能
- 役割ベースの管理

- スマートスキャン
- ポリシーサーバ

デバッグログを有効にするには

1. Web コンソールにログオンします。
2. Web コンソールのバナーで、[ウイルスバスター] の [ル] をクリックしてください。
3. デバッグログ設定を指定し、
4. [保存] をクリックします。
5. 次の初期設定の場所にあるログファイルをチェックします。<「サーバのインストールフォルダ」>¥PCCSRV¥Log.

デバッグログを無効にするには

1. Web コンソールにログオンします。
2. Web コンソールのバナーで、[ウイルスバスター] の [ル] をクリックしてください。
3. [デバッグログを有効にする] をオフにして、
4. [保存] をクリックします。

サーバのインストールとアップグレードのデバッグログを有効にするには

次のタスクを実行する前に、デバッグログを有効にできます。

- サーバをアンインストールして、再度インストールします。
- ウイルスバスター Corp. を最新バージョンにアップグレードします。
- リモートインストール / アップグレードを実行してください (デバッグログはセットアップを起動したコンピュータでのみ有効となり、リモートコンピュータには適用されません)。

次の手順を実行します。

1. <「サーバのインストールフォルダ」>¥PCCSRV¥Private にある [LogServer] フォルダを C:¥へコピーします。
2. ofcdebug.ini という名前で、次のコンテンツを含むファイルを作成してください。

```
[debug]
debuglevel=9
debuglog=c:¥LogServer¥ofcdebug.log
debugLevel_new=D
debugSplitSize=10485760
debugSplitPeriod=12
```

debugRemoveAfterSplit=1

3. ofcdebug.ini を C:\LogServer へ保存します。
4. 適切なタスクを実行します (サーバのアンインストール / 再インストール、新しいサーババージョンへのアップグレード、またはリモートでのインストール / アップグレード)。
5. C:\LogServer で ofcdebug.log を確認します。

インストールログ

ローカルインストール / アップグレードログ

ファイル名 : OFCMAS.LOG

位置 : %windir%

リモートインストール / アップグレードログ

セットアップを起動したコンピュータ上

ファイル名 : ofcmasr.log

位置 : %windir%

インストール先コンピュータ

ファイル名 : OFCMAS.LOG

位置 : %windir%

コンポーネントアップデートログ

ファイル名 : TmuDump.txt

位置 : <「サーバのインストールフォルダ」>\PCCSRV\Web\Service\AU_Data\AU_Log

サーバのアップデート情報詳細を取得するには

1. aucfg.ini という名前のファイルを作成し、次の内容を入力します。

[Debug]

level=-1

[Downloader]

ProxyCache=0

2. ファイルを <「サーバのインストールフォルダ」>\PCCSRV\Web\Service に保存します。

3. OfficeScan Master Service を再起動します。

サーバのアップデート情報詳細の取得を中止するには

1. aucfg.ini を削除します。
2. OfficeScan Master Service を再起動します。

クライアントパッケージ作成ログ

クライアントパッケージ作成のログを有効にするには

1. <「サーバのインストールフォルダ」>¥PCCSRV¥Admin¥Utility¥ClientPackager にある ClnExtor.ini を次のように変更します。

```
[Common]
DebugMode=1
```

2. C:¥ の ClnPack.log を確認します。

クライアントパッケージ作成のログを無効にするには

1. ClnExtor.ini ファイルを開きます。
2. [DebugMode] 値を 3 から 0 に変更します。

ServerProtect 一般サーバ移行ツールログ

ServerProtect 一般サーバ移行ツールのデバッグログを有効にするには

1. ofcdebug.ini ファイルという名前のファイルを作成し、次の内容を入力します。

```
[Debug]
DebugLog=C:¥ofcdebug.log
DebugLevel=9
```

2. ファイルを C:¥ に保存します。
3. C:¥ の ofcdebug.ini を確認します。

ServerProtect 一般サーバ移行ツールのデバッグログを無効にするには

ofcdebug.ini ファイルを削除します。

VSEncrypt ログ

ウイルスバスター Corp. は自動的にデバッグログ (VSEncrypt.log) をユーザアカウントの一時フォルダ内に作成します。たとえば、C:\Documents and Settings\<ユーザ名>\Local Settings\Temp となります。

Control Manager MCP エージェントデバッグログ

<「サーバのインストールフォルダ」>\PCCSRV\CMAgent フォルダに次のデバッグファイルが作成されます。

- Agent.ini
- Product.ini
- [Control Manager 設定] ページのスクリーンショット
- ProductUI.zip

MCP エージェントのデバッグログを有効にするには

1. <「サーバのインストールフォルダ」>\PCCSRV\CmAgent 内の product.ini ファイルを次のように修正します。

```
[Debug]

debugmode = 3

debuglevel= 3

debugtype = 0

debugsize = 10000

debuglog = C:\CMAgent_debug.log
```

2. ウイルスバスター Corp. 用 Control Manager エージェントサービスを Microsoft Management Console から手動で開始してください。
3. C:\ の CMAgent_debug.log を確認します。

MCP エージェントのデバッグログを無効にするには

1. product.ini ファイルを開いて次の行を削除します。

```
debugmode = 3

debuglevel= 3

debugtype = 0
```

```
debugsize = 10000
```

```
debuglog = C:\CMAgent_debug.log
```

2. ウイルスバスター Corp. 用 Control Manager サービスを再起動します。

ウイルス検索エンジンログ

ウイルス検索エンジンのデバッグログを有効にするには

1. レジストリエディタ (Regedit.exe) を開きます。
2. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMFilter\Parameters を開きます。
3. [DebugLogFlags] の値を「00003eff」に変更します。
4. 表示される検索問題に沿って手順を実行します。
5. %windir% の TMFilter.log を確認します。

ウイルス検索エンジンのデバッグログを無効にするには

[DebugLogFlags] の値を「00000000」に変更します。

アウトブレイクログ

現在のファイアウォール侵害アウトブレイクログ

ファイル名 : Cfw_Outbreak_Current.log

位置 : <「サーバのインストールフォルダ」>\PCCSRV\Log\

前回のファイアウォール侵害アウトブレイクログ

ファイル名 : Cfw_Outbreak_Last.log

位置 : <「サーバのインストールフォルダ」>\PCCSRV\Log\

現在のウイルス / 不正プログラムのアウトブレイクログ

ファイル名 : Outbreak_Current.log

位置 : <「サーバのインストールフォルダ」>\PCCSRV\Log\

前回のウイルス / 不正プログラムのアウトブレイクログ

ファイル名 : Outbreak_Last.log

現在のアウトブレイク : <「サーバのインストールフォルダ」>%PCCSRV%\Log%

ウイルストラッキングセンターログ

ファイル名 : wtc.log

位置 : <「サーバのインストールフォルダ」>%PCCSRV%\Log%\temp

ウイルスバスター Corp. クライアントログ

クライアントの問題のトラブルシューティングにクライアントログ (デバッグログなど) を使用できます。

警告： デバッグログはクライアントの性能に影響を与え、大量のディスク空き容量を消費する可能性があります。必要な時にのみデバッグログ生成を有効にし、デバッグデータが不要になった場合はただちに無効にしてください。ファイルサイズが巨大になった場合はログファイルを削除してください。

LogServer.exe を使用するクライアントデバッグログ

ウイルスバスター Corp. クライアントのデバッグログを有効にするには

1. ofcdebug.ini という名前で、次のコンテンツを含むファイルを作成してください。
[Debug]
Debuglog=C:\ofcdebug.log
debuglevel=9
debugLevel_new=D
debugSplitSize=10485760
debugSplitPeriod=12
debugRemoveAfterSplit=1
2. ofcdebug.ini ファイルをクライアントに送信し、C:\ フォルダ内に保存するように指示してください。

LogServer.exe ファイルは、クライアントのコンピュータが起動するたびに自動的に起動します。コンピュータの起動時に LogServer.exe コマンドウィンドウが開き、ウイルスバスター Corp. に対してデバッグログ生成の中止を要求しますが、ユーザに対してこのウィンドウを閉

じないように指示してください。。ユーザがコマンドウィンドウを閉じると、<「クライアントのインストールフォルダ」>内にある LogServer.exe を起動して再度デバッグログを開始できます。

3. それぞれのクライアントコンピュータに対し、C:\ 内の ofcdebug.log を確認します。

ウイルスバスター Corp. クライアントのデバッグログを無効にするには

ofcdebug.ini ファイルを削除します。

新規インストールログ

ファイル名 : OFCNT.LOG

位置 :

- ・ MSI パッケージを除いてすべてのインストール方法は %windir%
- ・ MSI パッケージインストール方法の場合は、%temp%

アップグレード /HotFix ログ

ファイル名 : upgrade.log

位置 : <「クライアントのインストールフォルダ」>%Temp

ダメージクリーンアップサービスデバッグログ

ダメージクリーンアップサービスに対するデバッグログを有効にするには

1. <「クライアントのインストールフォルダ」> の TSC.ini ファイルを開きます。
2. 次の行を以下のように修正してください。

DebugInfoLevel=3

3. <「クライアントのインストールフォルダ」>%debug の TSCDebug.log を確認します。

ダメージクリーンアップサービスに対するデバッグログを無効にするには

TSC.ini ファイルを開いて「DebugInfoLebel」の値を 3 から 0 に変更します。

クリーンアップログ

ファイル名 : yyyyymmdd.log

位置 : <「クライアントのインストールフォルダ」>%report%

メール検索ログ

ファイル名 : SmolDbg.txt

位置 : <「クライアントのインストールフォルダ」>

クライアント接続ログ

ファイル名 : Conn_YYYYMMDD.log

位置 : <「クライアントのインストールフォルダ」>%ConnLog

クライアントアップデートログ

ファイル名 : Tmudump.txt

位置 : <「クライアントのインストールフォルダ」>%AU_Data%AU_Log

クライアントのアップデート情報詳細を取得するには

1. aucfg.ini という名前のファイルを作成し、次の内容を入力します。

[Debug]

level=-1

[Downloader]

ProxyCache=0

2. <「クライアントのインストールフォルダ」>にファイルを保存してください。
3. クライアントを再起動します。

クライアントのアップデート情報詳細の取得を中止するには

1. aucfg.ini を削除します。
2. クライアントを再起動します。

大規模感染予防サービスログ

ファイル名 : OPPLogs.log

位置 : <「クライアントのインストールフォルダ」>%OppLog

ウイルスバスター Corp. ファイアウォールログ

一般的なファイアウォールドライバのデバッグログを有効にするには (Windows Vista/2008 の場合)

1. 次の各ファイルに、指定されたデータを追加します。
 - a. HKEY_LOCAL_MACHINE¥System¥CurrentControlSet¥Services¥tmwfp¥Parameters:
 - 種類: DWORD 値 (REG_DWORD)
 - 名前: DebugCtrl
 - 値: 0x00001111
 - b. HKEY_LOCAL_MACHINE¥System¥CurrentControlSet¥Services¥tmlwfp¥Parameters:
 - 種類: DWORD 値 (REG_DWORD)
 - 名前: DebugCtrl
 - 値: 0x00001111
2. コンピュータを再起動します。
3. C:¥ の wfp_log.txt および lwf_log.txt を確認します。

一般的なファイアウォールドライバのデバッグログを有効にするには (Windows 2000/XP/2003 の場合)

1. 次のファイルに、指定されたデータを追加します。
HKEY_LOCAL_MACHINE¥System¥CurrentControlSet¥Services¥tmcfw¥Parameters:
 - 種類: DWORD 値 (REG_DWORD)
 - 名前: DebugCtrl
 - 値: 0x00001111
2. コンピュータを再起動します。
3. C:¥ の cfw_log.txt を確認します。

一般的なファイアウォールドライバのデバッグログを無効にするには (すべての OS の場合)

1. レジストリキーの [DebugCtrl] を削除します。
2. コンピュータを再起動します。

ウイルスバスター Corp. NT ファイアウォールサービスのデバッグログを有効にするには

1. <「クライアントのインストールフォルダ」>の TmPfw.ini ファイルを次のように編集します。
[ServiceSession]
Enable=1

2. クライアントを再起動します。
3. C:\temp の TmPfw.log ファイルを確認します。

ウイルスバスター Corp. NT ファイアウォールサービスのデバッグログを無効にするには

1. TmPfw.ini ファイルを開き、「Enable」の値を 1 から 0 に変更します。
2. クライアントを再起動します。

Web 評価および POP3 メール検索のログ

Web 評価機能と POP3 メール検索機能のデバッグログを有効にするには

1. <「クライアントのインストールフォルダ」>の TmProxy.ini ファイルを次のように編集します。

```
[ServiceSession]
Enable=1
LogFolder=C:\temp
```

2. クライアントを再起動します。
3. C:\temp の ddmmyyyy_NSC_TmProxy.log ファイルを確認します。

Web 評価機能と POP3 メール検索機能のデバッグログを無効にするには

1. TmProxy.ini ファイルを開き、「Enable」の値を 1 から 0 に変更します。
2. クライアントを再起動します。

転送ドライバインタフェース (TDI) デバッグログ

TDI のデバッグログを有効にするには

1. 次のファイルに、指定されたデータを追加します。
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\tmltdi\Parameters:

キー 1

- ・ 種類: DWORD 値 (REG_DWORD)
- ・ 名前: Debug
- ・ 値: 1111 (16 進数)

キー 2

- ・ 種類: String 値 (REG_SZ)

- 名前 : LogFile
 - 値 : C:\tmttdi.log
2. コンピュータを再起動します。
 3. C:\ の tmttdi.log を確認します。

TDI のデバッグログを無効にするには

1. レジストリキーの [Debug] および [LogFile] を削除します。
2. コンピュータを再起動します。

製品サポート情報

ウイルスバスター Corp. のユーザ登録により、さまざまなサポートサービスを受けることができます。

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

サポートサービスについて

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

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

サポート契約の有効期限は、ユーザ登録完了から 1 年間です（ライセンス形態によって異なる場合があります）。契約を更新しないと、パターンファイルや検索エンジンの更新などのサポートサービスが受けられなくなりますので、契約満了前に必ず更新してください。更新手続きの詳細は、トレンドマイクロの営業部、または販売代理店までお問い合わせください。

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

製品 Q&A のご案内

ウイルスバスター Corp. 10 に関するよくあるお問い合わせを、以下の製品 Q&A にまとめています。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ので、是非ご活用ください

<http://esupport.trendmicro.co.jp/Pages/JP-2074993.aspx>

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。

セキュリティ情報

セキュリティ情報の入手先

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

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

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

セキュリティ情報 Web サイトでは、次の情報を閲覧できます。

- ・ ウイルス名やキーワードから検索できるウイルスデータベース

- ・ コンピュータウイルスの最新動向に関するニュース
- ・ 現在流行中のウイルスや不正プログラムの情報
- ・ デマウイルスまたは誤警告に関する情報
- ・ ウイルスやネットワークセキュリティの予備知識

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

トレンドマイクロへのウイルス解析依頼

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

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

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

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

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

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

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

用語集

アップデート

アップデートは、多くのトレンドマイクロ製品に共通の機能です。トレンドマイクロのアップデート Web サイトに接続すると、アップデートによって、パターンファイル、検索エンジン、プログラム、その他のトレンドマイクロコンポーネントファイルの最新のダウンロードが、インターネット経由で提供されます。

圧縮ファイル

1 つまたは複数の個別ファイルと情報を含む単一のファイルで、WinZip などの対応プログラムで展開できます。

Cookie

名前、傾向、趣味などのインターネットユーザに関する情報を格納するメカニズム。この情報は、後から使用できるように Web ブラウザに格納されます。ブラウザに cookie が保存されている Web サイトに次回アクセスすると、ブラウザは cookie を Web サーバに送信します。Web サーバはその cookie を使用して、カスタマイズされた Web ページを表示できます。たとえば、名前を表示してユーザを受け入れる Web サイトにアクセスする場合などです。

サービス拒否攻撃

サービス拒否 (DoS) 攻撃は、「サービス」、つまりネットワーク接続の中断を発生させるコンピュータまたはネットワークに対する攻撃のことをさします。通常、DoS 攻撃は、ネットワーク帯域幅に悪影響を与えたり、コンピュータメモリなどのシステムリソースをオーバーロードさせます。

DHCP

DHCP (Dynamic Host control Protocol) は、動的 IP アドレスをネットワーク内のデバイスに割り当てるためのプロトコルです。動的アドレス指定により、デバイスは、ネットワークに接続するたびに異なる IP アドレスを持つことができます。一部のシステムでは、デバイスの IP アドレスは、ネットワークに接続中でも変更できます。DHCP では、静的 IP アドレスと動的 IP アドレスの混在もサポートします。

DNS

ドメインネームシステム (DNS) は、ホスト名を IP アドレスに変換するために主にインターネットで使用される汎用的なデータクエリサービスです。

DNS クライアントが、DNS サーバにホスト名とアドレスデータを要求するときのプロセスは、解決と呼ばれます。基本的な DNS 設定では、サーバは初期設定の解決プロセスを実行します。たとえばリモートサーバは、現在のゾーンにあるコンピュータのデータについて、別のサーバに問い合わせます。リモートサーバ上のクライアントソフトウェアはリゾルバに問い合わせます。リゾルバは、データベースファイルからの要求に応答します。

ドメイン名

tellsitall.com のようにローカルホスト名とドメイン名で構成されるシステムの完全名。ドメイン名は、インターネット上の任意のホストに対して一意のインターネットアドレスを特定できるものである必要があります。「名前解決」と呼ばれるこのプロセスでは、ドメインネームシステム (DNS) を使用します。

動的 IP アドレス

動的 IP アドレスは、DHCP サーバが割り当てる IP アドレスです。コンピュータの MAC アドレスは固定ですが、IP アドレスについては、空き状況に応じて DHCP サーバにより新しいアドレスが割り当てられることがあります。

使用許諾契約書

使用許諾契約書あるいは EULA は、ソフトウェア発行者とソフトウェアのユーザの間の法的な契約です。一般的には、ユーザ側の制限について説明したもので、ユーザはインストール時に [同意します] をクリックしなければ契約の締結を拒否できます。もちろん [同意しません] ボタンをクリックした場合は、ソフトウェア製品のインストールは終了します。

特定のフリーソフトのインストールの際に表示される [使用許諾契約書] ウィンドウで、うっかり [同意します] をクリックしてしまい、スパイウェアやその他の種類のグレーウェアをユーザのコンピュータにインストールすることに同意してしまうことがよくあります。

誤検出

ファイルが感染していると誤ってセキュリティソフトウェアで検出されたときに、誤検出は発生します。

FTP

ファイル転送プロトコル (FTP) は、インターネットを介して、ファイルをサーバからクライアントへ転送する際に使用される標準プロトコルです。詳細については、Network Working Group の RFC 959 を参照してください。

HotFix

HotFix は、お客さまから報告された問題に対する回避策や解決方法です。HotFix は、お客さま固有の問題に対応するものであるため、すべてのお客さまにリリースされるものではありません。

Windows 版製品の HotFix にはセットアッププログラムが含まれますが、その他のプラットフォーム版の HotFix には含まれません (一般的にはプロセスを停止、ファイルをコピーしてインストール対象ファイルに上書きし、プロセスを再起動する必要があります)。

初期設定では、ウイルスバスター Corp. クライアントには HotFix がインストールされます。HotFix をクライアントにインストールしたくない場合は、Web コンソールにおいて、[ネットワーク上のコンピュータ] → [クライアント管理] → [設定] → [権限とその他の設定] → [その他の設定] タブでクライアントのアップデート設定を変更してください。

HTTP

ハイパーテキスト転送プロトコル (HTTP) はインターネットを介して、グラフィックやマルチメディアコンテンツを含む Web ページをサーバからクライアントへ転送する際に使用される標準プロトコルです。

HTTPS

SSL (Secure Socket Layer) を使用するハイパーテキスト転送プロトコル。HTTPS は、セキュリティで保護されたトランザクションの処理に使用される HTTP の変形です。

ICMP

ゲートウェイあるいは宛先のホストとソースホスト間の通信において、ICMP (Internet Control Message Protocol) を使用する場合があります。たとえば、データグラムプロセスにおけるエラー通知などです。ICMP は IP の基本的サポートを上位のプロトコルであるかのように使用しますが、ICMP は実際には IP の不可欠な部分で、各 IP モジュールに実装されています。ICMP メッセージはさまざまな状況で送信されます。たとえば、データグラムが宛先に届かない場合、ゲートウェイのバッファ容量がデータグラム転送に必要な容量に不足している場合、より短いルートでトラフィックを送信するようにゲートウェイがホストに指示できる場合などです。インターネットプロトコルは、信頼性が完全であるように設計されていません。これらのコントロールメッセージの目的は、通信環境における問題に対するフィードバックを提供することで、IP の信頼性を高めることではありません。

トレンドマイクロの推奨設定

トレンドマイクロの推奨設定は、検索対象ファイルを特定する方法です。実行可能ファイル (例: .exe) については、ファイルの内容に基づいて実際のファイルタイプが決定されます。実行可能ファイル以外のファイル (例: .txt) については、ファイルヘッダーに基づいて実際のファイルタイプが決定されます。

トレンドマイクロの推奨設定を使用する利点は、次のとおりです。

- ・ パフォーマンスの最適化: トレンドマイクロの推奨設定は、最小のシステムリソースを使用するため、クライアントのアプリケーションに影響しません。
- ・ 検索期間の短縮: トレンドマイクロの推奨設定は、実際のファイルタイプの識別情報を使用するため、感染を受けやすいファイルのみを検索します。したがって、検索時間は、すべてのファイルを検索する場合より大幅に短縮されます。

IntelliTrap

ウイルス作成者は、リアルタイム圧縮のアルゴリズムを使用して、ウイルスフィルタを回避しようとする場合があります。IntelliTrap は、リアルタイムの圧縮済み実行ファイルを遮断し、他の不正プログラムの特性とファイルを組み合わせ、ユーザのネットワークに入り込むというようなウイルスのリスクを減らすのに役立っています。IntelliTrap は、このようなファイルをセキュリティリスクとみなし、安全なファイルを誤ってブロックする場合がありますため、IntelliTrap を有効にするときは、ファイルを削除または消去せずに隔離することを検討してください。ユーザが定期的にリアルタイムの圧縮された実行ファイルをやりとりする場合は、IntelliTrap を無効にします。

IntelliTrap では、以下のコンポーネントを使用します。

- ウイルス検索エンジン
- IntelliTrap パターンファイル
- IntelliTrap 除外パターンファイル

IP

「インターネットプロトコル (IP) は、データグラムと呼ばれるデータブロックの送信を送信元から宛先へ提供する。そこでの送信元と宛先は、固定長アドレスによって識別されるホストである。」(RFC 791)

Java ファイル

Java は、Sun Microsystems によって開発された汎用プログラミング言語です。Java ファイルは Java コードを含みます。Java は、プラットフォームに依存しない Java 「アプレット」の形式で、インターネットのプログラミングをサポートします。アプレットは、HTML ページに挿入できる、Java プログラミング言語で記述されたプログラムです。Java 技術対応のブラウザを使用してアプレットを含むページを表示すると、アプレットのコードはコンピュータに転送され、ブラウザの Java 仮想マシンでアプレットが実行されます。

LDAP

LDAP (Lightweight Directory Access Protocol) は、TCP/IP 上で動作するディレクトリサービスの問い合わせおよび変更を行うアプリケーションプロトコルです。

待機ポート

待機ポートは、データ交換のためのクライアント接続要求に利用されます。

MCP エージェント

MCP (Trend Micro Management Communication Protocol) は、管理対象製品用のトレンドマイクロの次世代のエージェントです。MCP は、Control Manager がウイルスバスター Corp. と通信するように TMI (Trend Micro Management Infrastructure) を置き換えます。MCP には多くの新しい機能があります。

- ネットワークの負荷とパッケージサイズの削減
- NAT とファイアウォールの横断サポート
- HTTPS のサポート
- 一方向 / 双方向通信サポート
- シングルサインオン (SSO) のサポート
- クラスタノードのサポート

複合型の脅威の攻撃

複合型の脅威の攻撃は、企業のネットワークにある複数の侵入ポイントと脆弱性を利用します。このような脅威の攻撃には、「Nimda」や「Code Red」などがあります。

NAT

ネットワークアドレス変換 (NAT) は、セキュリティで保護された IP アドレスを、アドレスプールにある一時的な外部の登録 IP アドレスに変換するための規格です。これにより、非公開に IP アドレスが割り当てられた信頼するネットワークが、インターネットにアクセスできるようになります。つまり、ネットワーク内のすべてのコンピュータに対応する登録 IP アドレスを取得する必要はありません。

NetBIOS

ネットワーク基本入出力システム (NetBIOS) は、ネットワーク機能などの機能をディスクオペレーティングシステム (DOS) の基本入出力システム (BIOS) に追加するアプリケーションプログラムインタフェース (API) です。

一方向通信

NAT 妨害は現在のネットワーク環境でますます重要な問題になっています。この問題に取り組むために、MCP では一方向通信を用いています。一方向通信では、MCP エージェントがサーバとの接続を開始し、コマンドをやりとりします。それぞれの要求は、CGI に似たコマンドクエリまたはロ

グ伝送です。ネットワークへの影響を軽減するために、接続を維持し、できる限り開放しています。その後の要求は、既存の開いた接続を使用します。接続が切断されると、同じホストに対する SSL 接続はすべてセッション ID キャッシュのメリットを利用して、再接続時間を大幅に短縮します。

Patch

Patch は、複数のプログラムの問題を解決できる HotFix と Security Patch のグループです。トレンドマイクロでは定期的に Patch を配布しています。Windows 版の Patch にはセットアッププログラムが含まれますが、Windows 版以外の Patch には一般的にはセットアップスクリプトが含まれています。

フィッシング攻撃

フィッシングというのは、急速に増加している詐欺形式のもので、合法的な Web サイトを真似、Web ユーザから個人情報を暴露するものです。

典型的なシナリオでは、ユーザが突然驚くような (どう見ても本物) のメールを受け取ります。内容は、「口座に問題が発生して、ただちに口座解約の回避を決定しなければならない」という内容です。メールにはいかにも本物らしく見える Web サイトへの URL が記載されています。本物のメールと本物の Web サイトをコピーするのは簡単ですが、収集されたデータを受信するいわゆるバックエンドを変更するのも簡単です。

メールはサイトにログオンしてアカウント情報を確認するようにユーザに指示します。ユーザが提供する、ログオン名、パスワード、クレジットカード番号などのデータをハッカーは受け取ります。

フィッシング詐欺は早く、安く、継続が容易です。これはまた、犯人にとってお金儲けにつながる可能性があります。フィッシングはコンピュータに詳しいユーザでさえ検出が難しいのです。これは法的に規制するのも容易ではありません。さらに悪いことに、起訴することはほとんど不可能です。

フィッシングサイトの疑いがある Web サイトを発見したときは、トレンドマイクロに報告してください。詳細については、382 ページの「トレンドマイクロへのウイルス解析依頼」を参照してください。

Ping

Ping は、IP アドレスに対して ICMP エコー要求を送信し、応答を待つユーティリティです。Ping ユーティリティは、指定した IP アドレスを持つコンピュータがオンラインかどうかを決定します。

POP3

POP3 (Post Office Protocol 3) は、サーバからのメールメッセージを格納し、クライアントのメールアプリケーションへ転送する標準プロトコルです。

プロキシサーバ

特殊な接頭辞が付いた URL を受け入れる WWW サーバ。ローカルキャッシュまたはリモートサーバのいずれかから文書を取得するために使用され、その URL を要求元に返します。

RPC

リモートプロシージャコール (RPC) は、あるホストで動作するコンピュータプログラムがコードを別のホストで実行させることができるようにするネットワークプロトコルです。

Security Patch

Security Patch は、セキュリティ上の問題に対応し、すべてのお客さまに配布されます。Windows の Security Patch にはセットアッププログラムが含まれますが、Windows 以外の Patch には一般的にはセットアップスクリプトが含まれています。

Service Pack

Service Pack は、HotFix、Patch、大幅な機能拡張を組み合わせたもので、製品のアップグレードに相当します。Windows/Windows 以外の両方の Service Pack に、セットアッププログラムおよびセットアップスクリプトが含まれています。

SMTP

簡易メール転送プロトコル (SMTP) は、インターネットを介して、メールメッセージをサーバからサーバおよびクライアントからサーバに転送するために使用する標準プロトコルです。

snmp

簡易ネットワーク管理プロトコル (SNMP) は、管理上注意すべき状態について、ネットワークに接続されているデバイスの管理をサポートするプロトコルです。

SNMP トラップ

SNMP (Small Network Management Protocol) トラップは、SNMP プロトコルをサポートする管理コンソールを使用しているネットワーク管理者に通知を送信する方法です。

ウイルスバスター Corp では、通知を管理情報ベース (MIB) に格納できます。MIB ブラウザを使用して、SNMP トラップ通知を表示できます。

ただし、ウイルスバスター Corp ではローカルな MIB ファイルは保持されません。Control Manager をインストールしている場合は、Control Manager の MIB ファイルをダウンロードし、ウイルスバスター Corp で、SNMP プロトコルをサポートするアプリケーション (例: HP OpenView) と共に使用できます。

Control Manager の MIB ファイルを使用するには

1. Control Manager の管理コンソールにアクセスします。
2. メインメニューで、[運用管理] をクリックします。ドロップダウンメニューが表示されます。
3. [ツール] をクリックします。
4. 作業領域で、[Control Manager の MIB ファイル] をクリックします。
5. ファイルのダウンロード画面で [保存] を選択してサーバの場所を指定し、[OK] をクリックします。
6. ファイルをウイルスバスター Corp. サーバにコピーし、管理情報ベース (MIB) ファイルである Control Manager の MIB ファイルの cm2.mib を解凍します。
7. SNMP プロトコルをサポートするアプリケーション (例: HP OpenView) を使用して、cm2.mib をインポートします。

SOCKS 4

SOCKS 4 は、内部ネットワーク間のクライアント間、あるいは LAN とコンピュータまたは LAN の外部にあるサーバ間の通信を確立するために使用される TCP プロトコルです。SOCKS 4 プロトコルは接続要求を作成し、プロキシ回路を設定して、OSI モデルのアプリケーション層にデータを伝送します。

SSL

SSL (Secure Socket Layer) は、アプリケーションプロトコル (HTTP、Telnet、FTP など) と TCP/IP の間に層をなすデータセキュリティを提供するため、Netscape によって設計されたプロトコルです。

このセキュリティプロトコルは、データの暗号化、サーバの認証、メッセージの完全性、および任意の TCP/IP 接続のクライアント認証を実現します。

SSL 証明書

セキュリティで保護された HTTPS 通信を確立するデジタル証明書です。

TCP

伝送制御プロトコル (TCP) は、マルチネットワークアプリケーションをサポートするプロトコルの階層に対応するように設計された、接続志向のエンドツーエンドの信頼性のあるプロトコルです。TCP は IP データグラムを利用してアドレス解決を行います。詳細については、DARPA インターネットプログラムの RFC 793 を参照してください。

Telnet

Telnet は「ネットワーク仮想端末」を作成して、端末デバイスを TCP に接続させる標準的な方法です。詳細については、Network Working Group の RFC 854 を参照してください。

トロイポート

トロイポートは、一般的に、トロイの木馬プログラムがコンピュータに接続するために使用します。大規模感染の間、ウイルスバスター Corp. では、トロイの木馬プログラムが使用する可能性のある以下のポート番号をブロックします。

表 A-1. トロイポート

ポート番号	トロイの木馬プログラム	ポート番号	トロイの木馬プログラム
23432	Asylum	31338	Net Spy
31337	Back Orifice	31339	Net Spy
18006	Back Orifice 2000	139	Nuker
12349	Bionet	44444	Prosiak
6667	Bionet	8012	Ptakks
80	Codered	7597	Qaz

表 A-1. トロイポート (続き)

ポート番号	トロイの木馬プログラム	ポート番号	トロイの木馬プログラム
21	DarkFTP	4000	RA
3150	Deep Throat	666	Ripper
2140	Deep Throat	1026	RSM
10048	Delf	64666	RSM
23	EliteWrap	22222	Rux
6969	GateCrash	11000	Senna Spy
7626	Gdoor	113	Shiver
10100	Gift	1001	Silencer
21544	Girl Friend	3131	SubSari
7777	GodMsg	1243	Sub Seven
6267	GW Girl	6711	Sub Seven
25	Jesrto	6776	Sub Seven
25685	Moon Pie	27374	Sub Seven
68	Mspy	6400	Thing
1120	Net Bus	12345	Valvo line
7300	Net Spy	1234	Valvo line

信頼されたポート

サーバとクライアントは、信頼されたポートを使用して互いに通信します。

信頼されたポートをブロックし、大規模感染後にネットワーク設定を通常の状態に戻しても、クライアントはサーバとの通信をただちに再開しません。クライアントとサーバの通信は、[大規模感染予防の設定] 画面で指定した時間が経過してからでないと、元に戻りません。

ウイルスバスター Corp. では、HTTP ポート (初期設定では 8080) をサーバの信頼されたポートとして使用します。インストール中に、別のポート番号を入力できます。この信頼されたポートと、クライアント上の信頼されたポートをブロックするには、[ブロックされるポート] 画面で [信頼されたポートをブロック] チェックボックスをオンにします。

マスターインストーラは、インストール中にクライアントの信頼されたポートをランダムに生成します。

信頼されたポートを決定するには

1. <「サーバのインストールフォルダ」>%PCCSRV にアクセスします。
2. メモ帳などのテキストエディタを使用して、ofcscan.ini を開きます。
3. サーバの信頼されたポートについては、文字列「Master_DomainPort」を検索し、その横の値を確認します。たとえば、Master_DomainPort=80 という文字列がある場合は、サーバの信頼されたポートはポート 80であることを示します。
4. クライアントの信頼されたポートについては、文字列「Client_LocalServer_Port」を検索し、その横の値を確認します。たとえば、Client_LocalServer_Port=41375 という文字列がある場合は、クライアントの信頼されたポートはポート 41375であることを示します。

双方向通信

双方向通信は、一方向通信に代わる方法です。双方向通信は一方向通信に基づいていますが、サーバ通知を受信する HTTP ベースのチャンネルが追加されています。双方向通信では、MCP エージェントによる、サーバからのコマンドのリアルタイムな送信と処理が向上します。

UDP

ユーザデータグラムプロトコル (UDP) は、アプリケーションプログラムが他のプログラムにメッセージを送信するために、IP と共に使用されるコネクションレス通信です。詳細については、DARPA インターネットプログラムの RFC 768 を参照してください。

駆除できないファイル

ウイルス検索エンジンは、以下のファイルを駆除できません。

トロイの木馬に感染したファイル

トロイの木馬は、メッセージの表示、ファイルの削除、ディスクのフォーマットなど、予期しないまたは許可されない、通常は不正な動作を実行するプログラムです。トロイの木馬はファイルに感染しないので、ファイルの駆除は不要です。

解決策: ウイルスバスター Corp. では、ウイルスクリーンアップエンジンとウイルスクリーンアップテンプレートを使用して、トロイの木馬を除去します。

ワームに感染したファイル

コンピュータワームは自己完結型プログラム（またはプログラムセット）で、ワーム自体またはワームの一部の動作可能なコピーを他のコンピュータシステムに拡散できます。通常、ネットワーク接続またはメールの添付ファイルを通じて伝播されます。ワームは、自己完結型のプログラムであるため駆除できません。

解決策: トレンドマイクロはワームを削除することを推奨します。

書き込み保護された感染ファイル

解決策: 書き込み保護を解除して、ウイルスバスター Corp. がファイルを駆除できるようにします。

パスワードで保護されたファイル

パスワードで保護された圧縮ファイルまたはパスワードで保護された Microsoft Office ファイルを追加します。

解決策: パスワード保護を解除し、ウイルスバスター Corp. がこれらのファイルを駆除できるようにします。

バックアップファイル

RB0 ～ RB9 の拡張子が付いたファイルは、感染されたファイルのバックアップコピーです。ウイルスバスター Corp. では、駆除プロセス中にウイルス / 不正プログラムによってファイルが破損された場合、感染ファイルのバックアップを作成します。

解決策: ウイルスバスター Corp. が感染ファイルを正常に駆除した場合は、バックアップコピーを保持する必要はありません。コンピュータが正常に動作すれば、バックアップファイルを削除できます。

ごみ箱の感染ファイル

システムが実行中のため、ウイルスバスター Corp. はごみ箱の感染ファイルを削除できません。

解決策:

NTFS ファイルシステムの Windows 2000/XP/Server 2003 を実行しているコンピュータの場合、以下の手順を実行します。

1. 管理者権限でコンピュータにログオンします。
2. アプリケーションによるファイルのロックを回避するために、実行中のすべてのアプリケーションを閉じます。ファイルがロックされると、Windows ではそのファイルを削除できなくなります。
3. コマンドプロンプトを開き、以下を入力してファイルを削除します。

```
cd %
```

```
cd recycled
```

```
del *.* /S
```

最後のコマンドで、ごみ箱のすべてのファイルが削除されます。

4. ファイルが削除されたかどうかを確認します。

他の OS（つまり NTFS でない NT プラットフォーム）の場合は、以下の手順を実行します。

1. MS-DOS モードでコンピュータを再起動します。
2. コマンドプロンプトを開き、以下を入力してファイルを削除します。

```
cd %
```

```
cd recycled
```

```
del *.* /S
```

最後のコマンドで、ごみ箱のすべてのファイルが削除されます。

3. 通常モードでコンピュータを再起動します。

Windows の Temp フォルダまたは Internet Explorer の一時フォルダにある感染ファイル

Windows の Temp フォルダまたは Internet Explorer の一時フォルダにある感染ファイルは、コンピュータによって使用されているため、ウイルスバスター Corp. で駆除できません。駆除対象のファイルは、Windows 操作に必要な一時ファイルの可能性があります。

解決策：

NTFS ファイルシステムの Windows 2000/XP/Server 2003 を実行しているコンピュータの場合、以下の手順を実行します。

1. 管理者権限でコンピュータにログオンします。
2. アプリケーションによるファイルのロックを回避するために、実行中のすべてのアプリケーションを閉じます。ファイルがロックされると、Windows ではそのファイルを削除できなくなります。

3. Windows の Temp フォルダに感染ファイルがある場合

- a. コマンドプロンプトを開き、Windows の Temp フォルダ (初期設定では、Windows XP/Server 2003 コンピュータの場合は C:\Windows\Temp、Windows NT/2000 コンピュータの場合は C:\WinNT\Temp) に移動します。
- b. 以下を入力してファイルを削除します。

```
cd temp
attrib -h
del *.* /S
```

最後のコマンドで、Windows の Temp フォルダにあるすべてのファイルが削除されます。

4. Internet Explorer の一時フォルダに感染ファイルがある場合

- a. コマンドプロンプトを開き、Internet Explorer の一時フォルダ (Windows 2000/XP/Server 2003 コンピュータの場合、初期設定では C:\Documents and Settings\< ユーザ名 >\Local Settings\Temporary Internet Files) に移動します。
- b. 以下を入力してファイルを削除します。

```
cd tempor~1
attrib -h
del *.* /S
```

最後のコマンドで、Internet Explorer の一時フォルダにあるすべてのファイルが削除されます。

- c. ファイルが削除されたかどうかを確認します。

他の OS (つまり NTFS でない OS) を実行しているコンピュータの場合

1. MS-DOS モードでコンピュータを再起動します。
2. Windows の Temp フォルダに感染ファイルがある場合
 - a. コマンドプロンプトで、Windows の Temp フォルダに移動します。Windows XP/Server 2003 では、初期設定の Windows の Temp フォルダは C:\Windows\Temp です。Windows 2000 では、初期設定の Windows の Temp フォルダは C:\WinNT\Temp です。

- b. コマンドプロンプトを開き、以下を入力してファイルを削除します。

```
cd temp
```

```
attrib -h
```

```
del *.* /S
```

最後のコマンドで、Windows の Temp フォルダにあるすべてのファイルが削除されます。

- c. 通常モードでコンピュータを再起動します。

3. Internet Explorer の一時フォルダに感染ファイルがある場合

- a. コマンドプロンプトで、Internet Explorer の一時フォルダに移動します。Windows 2000/XP/Server 2003 では、初期設定の Internet Explorer の一時フォルダは C:\Documents and Settings\< ユーザ名 >\Local Settings\Temporary Internet Files です。

- b. 次のコマンドを入力します。

```
cd tempor~1
```

```
attrib -h
```

```
del *.* /S
```

最後のコマンドで、Internet Explorer の一時フォルダにあるすべてのファイルが削除されます。

- c. 通常モードでコンピュータを再起動します。

索引

英数字

- Access Control Server (ACS) 325
- ACS 証明書 338
- Active Directory 27、56、73、84、259
 - クエリ結果 58
 - 範囲とクエリ 57
 - 予約クエリ 61
- AutoPcc.exe 73、76、77
- CA 証明書 338、339
- Check Point SecureClient 84
- Cisco NAC
 - アーキテクチャ 327
 - 概要 323
 - コンポーネントおよび用語 324
 - ポリシーサーバのインストール 343
- Cisco Trust Agent 30、124、324
- Client Packager 73、79、84、85
 - 設定 81
 - 配信 81
- Control Manager 260
 - ウイルスバスター Corp. との統合 260
 - コンソール 262
 - 登録 261
- Cookie の検索 300
- CPU 使用率 28、183
- DHCP 設定 101
- EICAR テストウイルス 109、161
- HotFix 124
- ICSA 認定 120
- IDS 231
- IntelliTrap 183
- IntelliTrap 除外パターンファイル 121
- IntelliTrap パターンファイル 121
- Java 不正コード 161
- Land コウゲキ 232
- LogServer.exe 368、374
- MAC アドレス 280
- mail scan 83
- Microsoft Exchange Server の検索 297
- Microsoft SMS 73、85
- MSI パッケージ 73、84、85
- OLE 層 296
- Outlook メール検索 290
- Packer 161
- Patch 124
- Ping of Death 231
- POP3 メール検索 290、294
- Remote Authentication Dial-In User Service (RADIUS) 326
- scan method 81
- ScanNow 179
- SCV Editor 362
- SecureClient 34、362
 - SCV Editor 362
 - ウイルスバスター Corp. との統合 363
 - ポリシーサーバ 362
- Server Tuner 274
- ServerProtect 105
- SSL 証明書 353
- SYN フラッド 231

Terminal Access Controller Access Control System
(TACACS+) 327

TrendLabs 381

Update Agent 82

URL フィルタエンジン 123

VSEncode.exe 192

Web インストールページ 72、74

Web からの脅威 222

Web コンソール 30、38

URL 38

バナー 39

要件 38

ログオンアカウント 39

Web サーバ情報 272

Web レピュテーション 29、33、222

位置認識機能 223

承認済み URL 225

ポリシー 223、280

Windows Vista

インストール前タスク 60、75、95

あ

圧縮ファイル 182、296、297

アップデート

アップデートエージェント 153

ウイルスバスター Corp. サーバ 129

クライアント 139

スマートスキャンサーバ 137

アップデートエージェント 33、153

アップデート方法 157

コンポーネントの複製 157

システム要件 153

割り当て 154

アップデート方法

アップデートエージェント 157

ウイルスバスター Corp. サーバ 135

クライアント 143

アップデート元

アップデートエージェント 154

ウイルスバスター Corp. サーバ 131

クライアント 140

スマートスキャンサーバ 137

アドウェア 162

アンインストール 110

Web コンソールから 110

アンインストールプログラムの使用 111

権限 292

手動 112

暗号化ファイル 191

安全な設定の検証 362

移行

ServerProtect 一般サーバから 105

サードパーティのセキュリティソフトウェア
から 104

位置認識機能 169、172、223、280

インストール

クライアント 66

ポリシーサーバ 350

ウイルスクリーンアップエンジン 121

ウイルスクリーンアップテンプレート 121

ウイルス検索エンジン 120、373

アップデート 120

- ウイルス検索ドライバ 120
 - ウイルストラッキングセンターへのウイルス情報送信 277
 - ウイルスバスター Corp.
 - SecureClient の統合 363
 - Web コンソール 38
 - Web サーバ 272
 - 概要 26
 - クライアント 33
 - クライアントサービス 303
 - コンポーネント 45、118
 - コンポーネントのアップデート 109
 - サーバ 31
 - 主要機能と利点 29
 - データベースの検索 297
 - データベースバックアップ 270
 - プログラム 45
 - ライセンス 268
 - ログ 265
 - ウイルスバスター Corp. クライアント 33
 - アンインストール 110
 - インストール方法 72
 - ウイルスバスター Corp. サーバとの接続 307、312
 - オフライン 309
 - オフラインクライアント 319
 - オンライン 308
 - 機能 33
 - グループ設定 307
 - グローバル設定 295
 - 権限とその他の設定 283
 - 互換製品 71
 - 詳細なクライアント情報 317
 - スタンドアロン 310
 - スマートスキャンサーバとの接続 313
 - 設定のインポートおよびエクスポート 318
 - ディスク空き容量 305
 - ファイル 304
 - プロセス 305
 - レジストリキー 305
 - ウイルスバスター Corp. サーバ 31
 - 機能 31
 - ウイルスパターンファイル 118、151、302
 - ウイルス / 不正プログラム 160
 - ウイルス / 不正プログラム検索
 - グローバル設定 197
 - 結果 203
 - オーバーラッピングフラグメント 231
 - オフラインクライアント 309、319
 - オンラインクライアント 308
- か
- カーネルモードドライバ 302
 - 外部デバイスの権限 218
 - 外部デバイスの保護 123、218
 - 概要
 - アップデート 158
 - セキュリティ 40
 - 隔離ディレクトリ 189、191、274
 - 隔離フォルダ設定 273
 - 過大フラグメント 231
 - 挙動監視 27

- 挙動監視コアサービス 123
- 挙動監視設定パターンファイル 123
- 挙動監視ドライバ 123
- クライアントアップグレード
 - 無効 293
- クライアントアップデート
 - NAT による予約アップデート 148
 - アップデートサーバ 292
 - イベント起動 144
 - 権限 149
 - 自動 143
 - 手動 147
 - 予約アップデート 144、292、293
- クライアントインストール
 - Client Packager の使用 79
 - Web インストールページから 74
 - Web コンソールから 88
 - クライアントのディスクイメージの使用 90
 - システム要件 66
 - 脆弱性検索ツールの使用 91
 - セキュリティコンプライアンスの使用 60
 - ブラウザベース 76
 - ポストインストール 108
 - ログオンスクリプトウィザードの使用 76
- クライアントコンソール
 - アクセス制限 294
- クライアントセキュリティレベル 294
- クライアントセルフプロテクション 27、304
- クライアントツリー 46
 - 一般的なタスク 47
 - 詳細検索 48
 - 特定のタスク 48
- クライアントのアンインストール 110
- クライアントの検証 326
- クライアントのディスクイメージ 74、90
- クライアントログ
 - DCS デバッグログ 375
 - TDI デバッグログ 378
 - Web 評価のデバッグログ 378
 - アップグレード /HotFix ログ 375
 - ウイルスバスター Corp. ファイアウォールデバッグログ 377
 - クライアントアップデートログ 376
 - クライアント接続ログ 376
 - 新規インストールログ 375
 - 大規模感染予防サービスデバッグログ 376
 - デバッグログ 374
 - メール検索ログ 376
- グローバルクライアント設定 295
- グローバルスマートスキャンサーバ 36、317
- ケース診断ツール 368
- ゲートウェイ設定インポートツール 282
- ゲートウェイの IP アドレス 280
- 権限
 - アップデート権限 292
 - アンインストール権限 292
 - アンロード権限 292
 - 検索権限 285
 - スタンドアロン権限 284
 - ツールボックス権限 291
 - ファイアウォール権限 288、301
 - プロキシ設定権限 291

メール検索権限 289
予約検索権限 286、293
権限とその他の設定 283
検索エンジン
 ICSA 認定 120
検索権限 197
検索条件
 CPU 使用率 183
 検索対象ファイル 182
 スケジュール 183
 ファイル圧縮 182
 ファイルに対するユーザのアクティビティ 181
検索除外 184
 ディレクトリ 184
 ファイル 185
 ファイル拡張子 185
検索の種類 33、176
検索方法 165
 切り替え 167、171
検出時の処理 186
 ウイルス / 不正プログラム 297
 スパイウェア / グレーウェア 194
更新猶予期間 41、268
コンポーネント 45、109、118
 アップデートエージェント 153
 アップデート権限および設定 149、292
 アップデートの概要 158
 ウイルスバスター Corp. サーバ 129
 クライアント 139
 スマートスキャンサーバ 137

コンポーネントの複製 132、157

さ

サーバアップデート
 アップデート方法 135
 コンポーネントの複製 132
 手動アップデート 135
 プロキシ設定 132
 予約アップデート 135
 ログ 136
サーバログ
 MCP エージェントデバッグログ 372
 ServerProtect 移行ツールデバッグログ 371
 VSEncrypt デバッグログ 372
 ウイルス検索エンジンデバッグログ 373
 クライアントパッケージ作成ログ 371
 コンポーネントアップデートログ 370
 デバッグログ 368
 リモートインストール / アップグレードログ 370
 ローカルインストール / アップグレードログ 370
サービスの再起動 303
差分パターンファイル 132
参照サーバ 241、263
システム要件
 アップデートエージェント 153
 ポリシーサーバ 340
自動実行機能 218
従来型スキャン 42、165、166
手動アップデート 292

手動検索 177

ショートカット 296

ジョークプログラム 160、163

使用許諾契約書 (EULA) 385

承認済み URL 225

承認済みリスト 195

証明機関 (CA) 326

証明書 338

CA 339

SSL 353

新機能 26

診断モード 300

侵入検知システム 231

スタンドアロンクライアント 34、310

スタンドアロンスマートスキャンサーバ 169

スパイウェア 162

スパイウェア監視パターンファイル 122

スパイウェア / グレーウェア

潜在的なリスク 163

復元 196

防御 164

スパイウェア / グレーウェア検索

結果 208

承認済みリスト 195

処理 194

スパイウェア検索エンジン 122

スパイウェアパターンファイル 122

スマートスキャン 26、29、34、43、166

スマートスキャンエージェントパターン 119

スマートスキャンサーバ 34、137、168

アップデート元 137

種類 36

予約アップデート 137

スマートスキャンサーバリスト 169、172

カスタム 174

標準 173

スマートスキャンパターン 34、119

脆弱性検索ツール 74、91

DHCP 設定 101

Ping 設定 99

機能 91

クライアントインストール 95

効果 91

コンソール上のタスク 94

コンピュータの説明の取得 98

サポートされているプロトコル 98

製品クエリ 96

別のコンピュータでの起動 94

予約タスク 102

製品機能の強化 28

セキュリティ Patch 124

セキュリティコンプライアンス 27、56

セキュリティ状態 325

セキュリティ状態トークン 326

セキュリティの概要 40

アウトブレイクステータス 45

コンポーネントとプログラム 45

製品ライセンスのステータス 41

セキュリティ上の危険トップ 10 44

ネットワーク上のコンピュータ 42

セキュリティリスク

ウイルス / 不正プログラム 160

スパイウェアとグレーウェア 162

フィッシング攻撃 389
保護 29
接続の確認 314
設定のインポート 318
設定のエクスポート 318
潜在的なウイルス / 不正プログラム 161、204

た

大規模感染の基準 211
大規模感染予防 213
 ポリシー 214
 無効化 216
大規模感染予防サービス 45、210
大規模感染予防ポリシー
 書き込みアクセスの禁止 216
 共有フォルダへのアクセスを制限 / 禁止 214
 ポートのブロック 214
体験版 41、268、269
タイニーフラグメント攻撃 231
ダイヤラー 162
他社製のセキュリティソフトウェア 60
ダメージクリーンナップサービス 29、34
重複 ARP 231
通知
 Web からの脅威の検出 226、293
 ウイルス / 不正プログラム 190
 管理者 198
 クライアントアップデート 151
 クライアントユーザ向け 201
 コンピュータの再起動 295、302
 スパイウェア / グレーウェアの検出 194

大規模感染 211
ファイアウォール侵害 243
古いウイルスパターンファイル 302
予約検索 293
データベースの検索 297
データベースバックアップ 270
ティアドロップ 231
テクニカルサポート 380
デジタル証明書 326
デジタル署名パターンファイル 123
テストウイルス 161
テスト検索 109
デバイスコントロール 27、218
デバイスの権限 218
デバッグログ
 クライアント 374
 サーバ 368
トークン変数 200、212
同期化 359
ドメイン 46、54、307
トラブルシューティングのリソース 368
トレンドマイクロの推奨処理 188
トレンドマイクロの推奨設定 182
トロイの木馬プログラム 29、121、160

な

認証、承認、およびアカウンティング (AAA)
326
ネットワークアクセスデバイス 325
ネットワークウイルス 161、230、306

は

パスワード 39、272
パスワード解読アプリケーション 163
ハッキングツール 163
パフォーマンス管理 28、183
ファイアウォール 30、34、230
アウトブレイクモニタ 232
権限 232、243、288
初期設定のポリシーの除外設定 237
タスク 232
テスト 245
プロファイル 230、239
ポリシー 233
ポリシーの除外設定 236
無効化 247
利点 230
ファイアウォールドライバ 122、377
ファイアウォールパターンファイル 122、162
ファイル感染型ウイルス 161
フィッシング 389
プラグインマネージャ 31、34
フラグメント化 IGMP 231
プロキシ設定
 Web レピュテーション用 225
 外部接続用 317
 権限 291
 自動プロキシ設定 306
 内部接続用 315
プログラム 45、118
プロキシ設定
 クライアントコンポーネントのアップデート

149

 サーバコンポーネントのアップデート 132
ポートのブロック 214
保護ステータス 58
ポリシー
 Web レピュテーション 223
 ファイアウォール 230、233
ポリシーサーバ、Cisco NAC 325
 CA 証明書 339
 SSL 証明書 338
 インストールの概要 343
 クライアント検証プロセス 328
 システム要件 340
 証明書 338
 初期設定のポリシー 337
 初期設定のルール 333
 同期化 359
 ポリシー 358
 ポリシー構成 336
 ポリシーサーバのインストール 350
 ポリシーとルール 331
 ルール 358
 ルール構成 331
ポリシー施行パターンファイル 123

ま

 マクロウイルス 161
 メール検索 33、289

や

 役割ベースの管理 27、252

Active Directory ユーザアカウント 259

Control Manager 257

カスタムのユーザの役割 255

ユーザアカウント 256

ユーザの役割 252

ユーザの役割

管理者 253

ゲストユーザ 254

パワーユーザ 253

予約検索 178

再開 301

自動的に停止 301

スキップおよび停止 286、301

遅延 286、301

通知 300

スパイウェア / グレーウェアログ 208

セキュリティリスクログ 202、265

接続状態の確認ログ 266、315

デバイスコントロールログ 219

ネットワークウイルスログ 306

ファイアウォールログ 244、289、301

ログオンスクリプトウィザード 73、76

わ

ワーク 161

ら

ライセンス 41、268

リアルタイム検索 176

リアルタイム検索サービス 312

リモートアクセスツール 163

ルートキット検出 123

ローカルスマートスキャンサーバ 36

ログ 265

Web レピュテーションログ 227

ウイルス / 不正プログラムログ 202、306

概要 265

管理 267

クライアントアップデートログ 150

システムイベントログ 264

スパイウェア / グレーウェア復元ログ 210

