

Trend Micro ビジネスセキュリティ ™



管理者ガイド

安心を、ひとつ上のステージへ。



※注意事項

トレンドマイクロへのお客様情報の送信について

- ・「Webレピュテーションサービス」「フィッシング詐欺対策」「有害サイト規制/URLフィルタリング」では、Webサイトの安全性の判定のために、お客様がアクセスしたURLの情報等(ドメイン、IPアドレス等を含む)を暗号化してトレンドマイクロのサーバに送信します。サーバに送信されたURL情報は、Webサイトの安全性の確認、および本機能の改良の目的にのみ利用されます。また、これらの機能が有効にしたうえで、Webページにアクセスした場合、以下の事象がおこることがあります。
(a)お客様がアクセスしたWebページのWebサーバ側の仕様が、お客様が入力した情報等をURLのオプション情報として付加しWebサーバへ送信する仕様の場合、URLのオプション情報にお客様の入力した情報(ID、パスワード等)などを含んだURLがトレンドマイクロのサーバに送信される。この場合、トレンドマイクロでは、お客様がアクセスするWebページの安全性の確認のため、これらのお客様より受領した情報にもつき、お客様がアクセスするWebページのセキュリティチェックを実施します。
- ・「ファイルレピュテーションサービス」では、ファイルの安全性の判定のために、ファイルのハッシュ値等の情報をトレンドマイクロのサーバに送信します。ファイルそのものや、ファイルの内容に関する情報は送信しません。
- ・「ソフトウェア安全性評価サービス/脅威情報の送信」では、プログラムの安全性の判定のために、プログラムまたはプログラムの情報をトレンドマイクロのサーバに送信します。
- ・「ウイルストラッキング/TrendCareプログラム」では、検出されたウイルス/脅威名、検出数、国/地域、感染元となったWebサイトのURLを、統計を取るためにトレンドマイクロのサーバに送信します。
- ・「迷惑メール対策ツール」では、弊社製品の改良の目的および迷惑メールの判定精度の向上のため、トレンドマイクロのサーバに該当メールを送信します。また、迷惑メールの削減、迷惑メールによる被害の抑制を目指している政府関係機関に対して迷惑メール本体を開示する場合があります。
- ・「E-mailレピュテーションサービス」では、スパムメールの判定のために、送信元のメールサーバの情報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、不正な動きをする可能性があるトレンドマイクロが判断したファイル、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。送信されたファイルはプログラムの安全性の判定のために利用されます。またファイルにお客さまの個人情報や機密情報等が意図せず含まれる可能性があります。トレンドマイクロがファイルに含まれる個人情報や機密情報自体を収集または利用することはありません。お客さまから収集された情報の取り扱いについての詳細は、<<http://jp.trendmicro.com/jp/about/privacy/spn/index.html>>をご覧ください。

輸出規制について

本製品は、外国為替及び外国貿易法、U.S. Export Administration Regulations、およびその他の国における輸出規制品目に該当している場合があります。したがって、本製品が輸出規制品目に該当する場合、適正な政府の許可なくして、禁輸国もしくは貿易制裁国の企業、居住者、国民、または、取引禁止者、取引禁止企業に対して、輸出もしくは再輸出できません。このような規制についての情報は以下のWebサイトから見つけることができます。「<http://www.treas.gov/offices/enforcement/ofac/>」および「<http://www.bis.doc.gov/complianceand/enforcement/ListsToCheck.htm>」
2009年7月現在、米国により定められる禁輸国は、キューバ、イラン、北朝鮮、スーダン、シリアが含まれています。
あなたは本製品に関連した米国輸出管理法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。

商標について

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

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

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

P/N: CSSFFF-AE0900 (2009/12)

目次

第 1 章	Trend Micro ビジネスセキュリティについて	11
	ビジネスセキュリティの概要	12
	新機能	12
	バージョン 6.0	12
	バージョン 6.0 Service Pack 1	14
	主要機能	14
	Trend Micro Smart Protection Network	14
	スマートフィードバック	14
	Web レピュテーション	15
	ファイルレピュテーション	15
	URL フィルタ	16
	保護機能	16
	コンポーネント	17
	脅威について	19
	製品コンポーネントの用語集	22
第 2 章	使用の開始	25
	管理コンソールにアクセスする	26
	最新ステータス	29
	セキュリティ設定を表示する	32
第 3 章	ビジネスセキュリティクライアントのインストール.....	35
	ビジネスセキュリティクライアントのインストールの概要	36
	ビジネスセキュリティクライアントのインストール / アップグレード / 移行の概要	37
	新規インストールを実行する	38

Web ページからインストールする	38
ログオンスクリプトウィザードを使用してインストールする	39
ログオンスクリプトを使用してインストールする	41
Client Packager をを使用してインストールする	41
MSI ファイルを使用してインストールする	45
リモートインストールを使用してインストールする	45
脆弱性検索ツールを使用してインストールする	47
メール通知を使用してインストールする	49
ビジネスセキュリティクライアントのインストール、アップグレード結果を 確認する	49
脆弱性検索ツールを使用してクライアントインストールを確認する	50
ビジネスセキュリティクライアントを削除する	52
アンインストールプログラムを使用してビジネスセキュリティクライアントを 削除する	52
管理コンソールを使用してビジネスセキュリティクライアントを削除する	52
 第 4 章 グループの管理	55
グループの概要	56
グループ内のクライアントを表示する	56
グループの追加	57
管理コンソールからグループとコンピュータを削除する	58
クライアントをグループに追加する	58
クライアントを移動する	60
グループの設定を複製する	61
設定のインポートとエクスポートを実行する	62
 第 5 章 基本的なセキュリティ設定の管理	63
デスクトップ/サーバグループのオプション	64
検索の種類	65
リアルタイム検索を設定する	66

ファイアウォールを管理する	68
侵入検知システム	71
ステートフルインスペクション	72
ファイアウォールを設定する	73
Web レピュテーションを使用する	76
Web レピュテーションを設定する	77
URL フィルタを設定する	78
挙動監視を使用する	79
挙動監視を設定する	81
Trend Secure	84
Trend Secure を設定する	84
POP3 メール検索を管理する	85
メール検索を設定する	85
クライアント権限	86
隔離の設定を行う	89
第 6 章 大規模感染予防の使用	91
大規模感染予防	92
大規模感染予防の現在のステータス	93
クリーンナップ	97
診断 / クリーンナップ	99
[クリーンナップ実行] を実行する	100
大規模感染予防を設定する	101
大規模感染予防設定を設定する	103
自動大規模感染予防の詳細を表示する	105
脆弱性診断設定を設定する	106
第 7 章 検索の管理	109
検索について	110

検索方法	110
検索方法を選択する	111
検索の種類	111
手動検索および予約検索オプションを設定する	112
スパイウェア / グレーウェアの除外リストを編集する	115
予約検索	116
 第 8 章 通知の管理	119
通知	120
通知イベントを設定する	121
通知する内容を設定する	122
トークン (変数) の使用	122
通知方法を設定する	123
 第 9 章 グローバル設定の管理	125
グローバルオプション設定	126
インターネットプロキシのオプション	126
SMTP サーバのオプション	128
デスクトップ / サーバのオプション	128
システムのオプション	135
 第 10 章 アップデートの管理	141
コンポーネントをアップデートする	142
アップデート	142
アップデート可能なコンポーネント	143
ビジネスセキュリティ サーバのアップデート	146
アップデート元	146
アップデート元の設定	148
アップデートエージェントの使用	149

手動アップデート	151
コンポーネントの手動アップデート	151
自動アップデート	152
コンポーネントの自動アップデートのスケジュール設定	152
コンポーネントのロールバックまたは同期	153
HotFix、Patch、および Service Pack	154
 第 11 章 ログとレポートの使用	 157
ログ	158
ログクエリの使用	160
レポート	161
レポートについて	161
レポートを生成する	164
ログとレポートを管理する	166
レポートを管理する	167
ログを削除する	168
 第 12 章 ビジネスセキュリティの管理.....	 171
管理コンソールのパスワードを変更する	172
プラグインマネージャを使用する	173
製品ライセンスの詳細を表示する	173
Trend Micro Smart Protection Network に参加する	175
ビジネスセキュリティ サーバをアンインストールする	176
 付録 A トレンドマイクロ製品除外リスト	 177
 付録 B クライアントの情報.....	 181
クライアントの種類	182

標準モードのクライアントのアイコン	182
ロケーション認識	186
スタンドアロンモードのクライアント	187
32 ビットおよび 64 ビットのクライアント	188
 付録 C トレンドマイクロのサービス	189
大規模感染予防ポリシー	190
ダメージクリーンナップサービス	190
脆弱性診断	191
トレンドマイクロの推奨設定	192
トレンドマイクロの推奨処理	192
IntelliTrap	193
Web レピュテーション	194
 付録 D クライアント保護のベストプラクティス	197
 付録 E 管理ツールおよびクライアントツールの使用	199
ツールの種類	200
管理ツール	201
ログオンスクリプトウィザード	201
脆弱性検索ツール	201
脆弱性検索ツールを使用する	202
クライアントツール	206
Client Packager	206
感染ファイル暗号化処理の復元ツール	206
クライアント移動ツール	208
アドイン	209
SBS アドインと EBS アドインをインストールする	210

付録 F	トラブルシューティングおよび Q&A	213
	トラブルシューティング	214
	Q&A	220
	アクティベーションコードとレジストレーションキーの取得方法	220
	登録	221
	インストール、アップグレード、および互換性	221
	パスワードを忘れた・紛失した場合	222
	設定	222
	パターンファイルまたは Service Pack が最新かどうかの確認	224
	スマートスキャン	224
	既知の制限事項	225
付録 G	ヘルプ情報へのアクセス.....	227
	製品ドキュメント	228
	製品サポート情報	229
	サポートサービスについて	229
	製品 Q&A のご案内	230
	セキュリティ情報	230
	セキュリティ情報の入手先	230
	トレンドマイクロへのウイルス解析依頼	231
	ウイルス解析サポートセンター「TrendLabs」	231
付録 H	用語集	233
索引		237



第1章

Trend Micro ビジネスセキュリティについて

本章では、Trend Micro ビジネスセキュリティ（以下、ビジネスセキュリティ）の主な機能の概要を説明します。

本章で説明する内容には、次の項目が含まれます。

- 12 ページの「ビジネスセキュリティの概要」
- 12 ページの「新機能」
- 14 ページの「主要機能」
- 16 ページの「保護機能」
- 19 ページの「脅威について」
- 22 ページの「製品コンポーネントの用語集」

ビジネスセキュリティの概要

ビジネスセキュリティは、データや個人情報の盗難、および危険な Web サイトから中小企業のユーザおよび資産を保護します。ビジネスセキュリティは、Trend Micro Smart Protection Network を備えることにより、次の点が強化されています。

- **安全性** — ウイルス、スパイウェア、および Web からの脅威がコンピュータやサーバに到達しないよう阻止します。URL フィルタによって、危険な Web サイトへのアクセスがブロックされ、ユーザの生産性向上に役立ちます。
- **高性能** — 迅速な検索と継続的なアップデートにより、新しい脅威を阻止してユーザの PC に対する影響を最小限に抑えます。
- **利便性** — インストールが簡単で、管理の必要性がありません。ビジネスセキュリティは、脅威をより効率的に検出するため、ユーザはセキュリティ以外の業務に専念できます。

新機能

バージョン 6.0

- **スマートスキャン**

スマートスキャンによって、不正プログラムおよびスパイウェアの大規模な検索機能が検索サーバに移行されます。

これによって、クライアントの負荷が軽減され、クライアントでアップデートを定期的にダウンロードする必要が少なくなるため、脅威が前例のない速度でリリースされる状況に対して防衛することができます。

個々のクライアントをアップデートするのではなく、サーバにソリューションを配信することによって、ほとんど即座に最新の保護機能を実現できます。

- **URL Web コンテンツフィルタ**

トレンドマイクロのサポートにより、不適切なコンテンツが含まれる Web サイトをブロックできます。URL フィルタは、従業員の生産性の向上、ネットワークリソースの安全性の確保、および機密情報の保護に役立ちます。

詳細については、78 ページの「URL フィルタを設定する」を参照してください。

- **Trend Micro Smart Protection Network との統合**

Trend Micro Smart Protection Network は、インターネット全体から脅威に関するさまざまな情報を収集するテクノロジーの集合体であり、最新の脅威に対して最新の保護機能を提供します。

URL フィルタ、Web レピュテーション、およびスマートスキャンはすべて、Trend Micro Smart Protection Network の不可欠な構成要素です。

- **最新ステータスの簡易化**

[最新ステータス] ダッシュボードが、さらに使いやすくなりました。

詳細については、29 ページの「最新ステータス」を参照してください。

- **感染ファイル暗号化処理の復元隔離ツールの新しいグラフィカルインターフェース**

隔離に関する管理がより簡単になります。

- **CPU 使用率に応じて変化する検索**

CPU 使用率が高い場合の検索の柔軟性が向上します。ビジネスセキュリティは、CPU に対応して、CPU 使用率が高い場合に一時停止するよう設定できるようになりました。

- **USB 自動実行の脅威からの保護**

USB ドライブがクライアントの USB ポートに挿入されたときに、USB ドライブ上の自動実行ファイルが実行されないようにします。

バージョン 6.0 Service Pack 1

- ・ クライアントのセキュリティの強化
不正なソフトウェアによってビジネスセキュリティクライアントの重要コンポーネントが変更または終了されるのを防止します。
- ・ すべてのクライアントのファイアウォールの無効化
グローバル設定からすべてのクライアントのファイアウォールを無効化できるようになりました。
- ・ 新しい OS のサポート
詳細は、Readme を参照してください。

主要機能

本バージョンの製品機能では、Trend Micro Smart Protection Network との統合が強化されています。

Trend Micro Smart Protection Network



Trend Micro Smart Protection Network は、世界各国で実施されたウイルス検索の結果を収集し、統計情報をリアルタイムで提供しています。これは、お客さまのコンピュータを Web からの脅威に対して保護することを目的としています。次に、Trend Micro Smart Protection Network の主な機能を示します。

スマートフィードバック

トレンドマイクロスマートフィードバックは、トレンドマイクロのテクノロジーおよび 24 時間体制の TrendLabs の運用によって、トレンドマイクロの製品間での継続的な情報交換を実現しています。ユーザの 1 回の定期的なレピュテーションチェックによって新しい脅威が特定されるたびに、トレンドマイクロの脅威に関するデータベースがすべて自動的にアップデートされ、これ以降ユーザで所定の脅威が発生することがないようブロックされます。顧客およびパートナーの広範囲にわたる世界的なネットワークを通して収集された脅威に関する情報を継続的に処理することによって、トレンドマイクロは、最新の脅威に対して自動的なリアルタイムの保護を提供し、住民を保護するために地域で行われる自動化された自警組織と同様に、「団結」することによるセキュリティの強化を実現しています。脅威に関して収集される情報は、特定の通信のコンテンツではなく、送信元の評価に基づいています。

Web レピュテーション

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

トレンドマイクロの Web レピュテーションテクノロジーでは、世界最大級のドメインレピュテーションデータベースを使用して、Web サイトの古さ、位置の履歴的变化、および不正プログラム挙動分析から検出される疑わしい活動の兆候などの要素に基づいて、レピュテーションスコアを割り当てることによって、Web ドメインの信用性が探知されます。また、引き続きサイトが検索され、感染サイトにユーザがアクセスしないようブロックされます。正確性を向上し、誤検出を減らすために、Web レピュテーションテクノロジーでは、サイト全体を分類してブロックするのではなく、サイト内の特定のページやリンクにレピュテーションスコアが割り当てられます。これは、多くの場合、正規サイトの一部のみがハッキングされていて、レピュテーションが時間の経過とともに動的に変化する可能性があるためです。

ファイルレピュテーション

トレンドマイクロのファイルレピュテーションテクノロジーでは、ユーザのアクセスを許可する前に、大規模な in-the-cloud 型データベースを照合して、各ファイルの評価情報が確認されます。不正プログラムに関する情報がクラウドに保存されるため、すべてのユーザが即座に利用できます。高性能のコンテンツ配信ネットワークおよび社内ネットワーク内のスキャンサーバによって、確認プロセス時の遅延が最小限に抑えられます。このクラウドクライアントアーキテクチャによって、より迅速な保護が実現され、クライアント全体のフットプリントが大幅に軽減されるとともにパターンファイル配信の負担が取り除かれます。

スマートスキャン

ビジネスセキュリティでは、スマートスキャンと呼ばれる新しいテクノロジーが使用されます。これまでは、ビジネスセキュリティクライアントでは、従来型スキャンが使用されており、検索を実行するために検索関連コンポーネントを各クライアントでダウンロードする必要がありました。スマートスキャンを使用すると、クライアントは、スマートスキャンサーバ上のパターンファイルを使用できます。

スマートスキャンの利点は次のとおりです。

- ・ ハードウェアリソースの軽減 — ファイルの検索には、スキャンサーバが支援を行うので、クライアント側の使用リソースは削減されます。

URL フィルタ

URL フィルタを使用すると、Web サイトへのアクセスを制御して、従業員の非生産的な時間を削減し、インターネット帯域幅の使用率を軽減して、より安全な作業環境を確立できます。URL フィルタの保護レベルを選択したり、スクリーニングを行う Web サイトの種類をカスタマイズしたりできます。

保護機能

次の表は、ビジネスセキュリティのさまざまなコンポーネントが、各種の脅威からコンピュータをどのように保護しているのかを示しています。

表 1-1. 保護機能

脅威	保護
ウイルス / 不正プログラム — ウイルス、トロイの木馬、ワーム、バックドア、ルートキット スパイウェア / グレーウェア — スパイウェア、ダイヤラー、ハッキングツール、パスワード解読アプリケーション、アドウェア、ジョークプログラム、キーロガー	ウイルス検索エンジンとパターンファイル、スパイウェア検索エンジンとパターンファイル
メールメッセージやスパムメールを通じて送信されるウイルス / 不正プログラムおよびスパイウェア / グレーウェア	POP3 メール検索
ネットワークワーム / ウイルス	ファイアウォール
侵入	ファイアウォール
有害と考えられる Web サイト / フィッシングサイト	Web レピュテーション、Trend プロテクト
不正挙動	挙動監視
インスタントメッセージングアプリケーションでの露骨なコンテンツと禁止コンテンツ	インスタントメッセージコンテンツフィルタ

コンポーネント

ウイルス対策

- **ウイルス検索エンジン (32 ビット /64 ビット):** 検索エンジンは、ウイルスパターンファイルを使用して、ユーザが開いたファイルまたは保存したファイルに潜むウイルス、不正プログラムなどのセキュリティリスクを検出します。
検索エンジンは、ウイルスパターンファイルと連携し、パターンマッチングというプロセスを使用して検出の第 1 レベルを実行します。各ウイルスには一意の「シグニチャ」、つまり他のコードと区別できる特性を表す文字列が含まれているので、トレンドマイクロのウイルス専門家は、このコードの実行機能を持たない断片をパターンファイルに取り込みます。検索エンジンは、各検索対象ファイルの特定領域をウイルスパターンファイルのパターンと比較し、一致するものを探します。
- **ウイルスパターンファイル:** ビジネスセキュリティクライアントでウイルスシグニチャ (ウイルスの存在を示すビットやバイトの一意のパターン) の識別に使用されるファイルです。
- **ウイルスクリーンアップテンプレート:** ウイルスクリーンアップエンジンによって使用され、トロイの木馬のファイルとプロセス、ワーム、およびスパイウェアを識別して削除するために使用されるテンプレートです。
- **ウイルスクリーンアップエンジン (32 ビット /64 ビット):** クリーンアップサービスでトロイの木馬のファイルとプロセス、ワーム、およびスパイウェアの検索および削除に使用されるエンジンです。
- **IntelliTrap 除外パターンファイル:** IntelliTrap と検索エンジンで圧縮ファイル内の不正コードの検索に使用される除外パターンファイルです。
- **IntelliTrap パターンファイル:** IntelliTrap と検索エンジンで圧縮ファイル内の不正コードの検索に使用されるパターンファイルです。
- **スマートスキャンエージェントパターン:** クライアントで脅威の特定に使用されるパターンファイルです。このパターンファイルは、クライアントのコンピュータに保存されます。
- **スマートフィードバックエンジン (32 ビット /64 ビット):** Trend Micro Smart Protection Network にフィードバックを送信するエンジンです。
- **スマートスキャンパターン:** クライアントのコンピュータ上のファイル固有のデータが含まれるパターンファイルです。

スパイウェア対策

- **スパイウェア検索エンジン (32 ビット):** 32 ビット OS を実行する感染コンピュータとサーバからスパイウェアを検出して削除する個別の検索エンジンです。

- **スパイウェア検索エンジン (64 ビット)**: 32 ビットシステム用のスパイウェア検索エンジンと同様に、この検索エンジンは 64 ビット OS 上でスパイウェアを検出し、削除します。
- **スパイウェアパターンファイル**: 既知のスパイウェアを特定するための情報が格納されており、スパイウェア検索エンジン (32 ビットと 64 ビットの両方) でコンピュータとサーバ上のスパイウェアを手動検索および予約検索により検出するのに使用されます。
- **スパイウェア監視パターンファイル**: スパイウェアパターンファイルと似ていますが、ウイルス検索エンジンでスパイウェアを検索する際に使用されます。

大規模感染予防

大規模感染予防は、インターネットの脅威や、その他の世界的な大規模感染状況を早期のうちに警告します。コンピュータとネットワークの安全性を維持するための予防措置を自動的に講じた後、問題を特定し、ダメージを修復します。

- **脆弱性検索診断パターンファイル**: すべての脆弱性のデータベースが格納されたファイルです。脆弱性診断パターンファイルは、既知の脆弱性を検索するように検索エンジンに指示します。

ネットワークウイルス

- **ファイアウォールドライバ (32 ビット /64 ビット)**: ファイアウォールは、このドライバとネットワークウイルスパターンファイルを使用して、ハッカーの攻撃やネットワークウイルスからコンピュータを保護します。
- **ファイアウォールパターンファイル**: ウイルスパターンファイルと同様に、ビジネスセキュリティでネットワークウイルスのシグニチャの識別に使用されます。
- **TDI ドライバ (32 ビット /64 ビット)**: ネットワークトラフィックを検索モジュールにリダイレクトするモジュールです。
- **WFP ドライバ (32 ビット /64 ビット)**: Windows Vista クライアントでは、ファイアウォールはこのドライバとネットワークウイルス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索します。

Web レピュテーション

- **トレンドマイクロ セキュリティデータベース**: Web レピュテーションは、Web ページを開く前に、そのページに潜在するセキュリティリスクを評価します。データベースから返される危険度と、設定されているセキュリティレベルに応じて、ビジネスセキュリティクライアントはその Web ページの閲覧を拒否または許可します。
- **URL フィルタエンジン (32 ビット /64 ビット)**: ページを評価するためのクエリをトレンドマイクロ セキュリティデータベースで実行するエンジンです。

Trend プロテクト

- ・ **トレンドマイクロ セキュリティデータベース**: Trend プロテクトは、Web ページに表示されるハイパーリンクの潜在的なセキュリティリスクを評価します。データベースから返される危険度と、Trend プロテクトに設定されているセキュリティレベルに応じて、Trend プロテクトはリンクの危険度を判定します。

挙動監視

- ・ **挙動監視ドライバ**: このドライバは、クライアント上のプロセスの挙動を検出します。
- ・ **挙動監視コアサービス**: ビジネスセキュリティクライアントは、このサービスを使用して、挙動監視コアドライバを制御します。
- ・ **ポリシー施行パターンファイル**: ビジネスセキュリティサーバに設定され、ビジネスセキュリティクライアントによって施行されるポリシーのリストです。
- ・ **デジタル署名パターンファイル**:トレンドマイクロが認定した、安全なソフトウェアを提供している企業のリストです。
- ・ **挙動監視制御パターンファイル**: このパターンファイルには、初期設定の挙動監視ポリシーが格納されています。このパターンのファイルは、すべてのポリシー照合でスキップされます。
- ・ **挙動監視検出パターンファイル**: 疑わしい脅威の挙動の検出に使用するルールが含まれるパターンファイルです。

コンテンツフィルタ

- ・ **禁止する語句リスト**: 禁止する語句リストには、メッセージャーを介して送信することを許可しない単語が登録されています。

最新ステータスと通知設定

- ・ 最新ステータスを表示すると、大規模感染予防、ウイルス対策、スパイウェア対策、およびネットワークウイルスのセキュリティステータスを一目で確認できます。同様に、ビジネスセキュリティでは、重大なイベントが発生したときに管理者に通知を送信できます。

脅威について

コンピュータのセキュリティは、めまぐるしく変化するテーマです。管理者および情報セキュリティの専門家は、コンピュータとネットワークに対する潜在的なリスクや招かれざる事態の表現にさまざまな用語や語句を発案および採用しています。ここでは、これらの用語について説明し、このマニュアルでそれらがどのような意味で使用されているかを示します。

ウイルス / 不正プログラム

コンピュータウイルスまたは不正プログラムは、実行可能コードの断片であり、自己複製という独特の機能を持つプログラムです。ほとんどの種類の実行可能ファイルに取り付くことができ、ファイルとして、個人間での送受信やコピーによって広がります。

自己複製に加えて、一部のウイルスおよび不正プログラムには別の共通点があります。ウイルスのペイロードを実行するダメージルーチンです。メッセージやイメージを単に表示するだけのペイロードもあれば、ファイルを破壊したり、ハードディスクドライブを再フォーマットするなどの損害をもたらすペイロードもあります。

- ・ **不正プログラム** : 不正プログラムとは、コンピュータシステムの所有者が知らぬ間にシステムに侵入したりダメージを与えたりするように設計されたソフトウェアです。
- ・ **トロイの木馬** : トロイの木馬は、無害なアプリケーションを装う不正プログラムです。ウイルスや不正プログラムとは異なり、トロイの木馬は自己複製しませんが、ウイルスと同様に有害な可能性があります。コンピュータからウイルスや不正プログラムを駆除するように見せかけながら、実際にはコンピュータにウイルスや不正プログラムを持ち込むアプリケーションが、トロイの木馬の一例です。
- ・ **ワーム** : 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別のコンピュータシステムに拡散できます。通常、伝播はネットワーク接続またはメールの添付ファイルを介します。ウイルスや不正プログラムとは異なり、ワームは自分自身をホストプログラムに添付する必要はありません。
- ・ **バックドア** : バックドアとは、自身を検出されないようにしながら、通常の認証をかいくぐったり、コンピュータへのリモートアクセスを確保したり、情報にアクセスしたりする手段です。
- ・ **ルートキット** : ルートキットとは、ユーザによる OS の正当な制御を妨害するように設計されたプログラムの集合です。一般に、ルートキットは自身がインストールされたことを隠し、標準のシステムセキュリティを破壊することで自身が削除されるのを回避します。
- ・ **マクロウイルス** : マクロウイルスは、アプリケーション固有のウイルスです。マクロウイルスは、Microsoft Word (.doc) や Microsoft Excel (.xls) などのアプリケーションファイルに常駐します。したがって、マクロウイルスは、.doc、.xls、.ppt など、マクロ対応アプリケーションに共通する拡張子を持つファイルで検出される可能性があります。マクロウイルスは、アプリケーションのデータファイル間を移動します。また、阻止されない場合は最終的に何百ものファイルに感染するおそれがあります。

ウイルスまたは不正プログラムに推奨される処理は「駆除」です。

スパイウェア / グレーウェア

グレーウェアは、予期しない処理や許可されていない処理を実行するプログラムです。この用語は、スパイウェア、アドウェア、ダイヤラー、ジョークプログラム、リモートアクセスツールなどの好ましくないファイルおよびプログラムの総称として使われています。種類によっては、自己複製する不正コードと自己複製しない不正コードが含まれる場合と、含まれない場合があります。

- **スパイウェア** : スパイウェアは、ユーザが同意も認識もしないうちにコンピュータにインストールされ、個人情報を収集して送信するコンピュータソフトウェアです。
- **ダイヤラー** : ダイヤラー (ダイヤルアップ接続ソフトウェア) は、ブロードバンド接続以外のインターネット接続に必要です。不正なダイヤラーは、ISP に直接接続するのではなく、割増料金のかかる番号を通して接続するように設計されています。このような不正なダイヤラーのプロバイダは、割増料金を自らが搾取します。ダイヤラーは、この他にも、個人情報の送信、不正ソフトウェアのダウンロードに使用されます。
- **ハッキングツール** : ハッキングツールとは、ハッキングを支援するように設計されたプログラム、またはプログラムの集合です。
- **アドウェア** : アドウェア (advertising-supported software) とは、コンピュータにインストールされた後で、またはアプリケーションの使用中に、そのコンピュータで自動的に広告を再生、表示、またはダウンロードするソフトウェアパッケージです。
- **キーロガー** : キーロガーとは、ユーザのキー入力をすべて記録するコンピュータソフトウェアです。この情報は、ハッカーによって取得され、個人的な目的に使用される場合があります。
- **ボット** : ボット (「ロボット」の短縮形) は、ユーザまたは別のプログラムのエージェントとして動作するプログラム、または人の操作をシミュレートするプログラムです。ボットは、1 度実行されると、自身のコピーを作成、圧縮、および配布できます。ネットワークに接続されたコンピュータに対する自動攻撃を仕掛けるときに使用されることがあります。

ビジネスセキュリティクライアントは、グレーウェアを検出できます。スパイウェアまたはグレーウェアに推奨される処理は「駆除」です。

ネットワークウイルス

厳密に言うと、ネットワーク上で広がるウイルスがすべてネットワークウイルスであるというわけではありません。この項で取りあげた脅威のうち、ネットワークウイルスと呼べるのはワームなどの一部のウイルスだけです。特に、ネットワークウイルスは、TCP、FTP、UDP、HTTP などのネットワークプロトコルやメールプロトコルを利用して自己複製します。

ファイアウォールは、ネットワークウイルスパターンファイルを使用してネットワークウイルスを特定し、ブロックします。

スパムメール

スパムメールとは、複数のメーリングリスト、個人、またはニュースグループに一方的に送信されるメール（迷惑メール）のことで、商業目的のものも多数あります。スパムメールには 2 種類あり、1 つは一方的に送信される宣伝用メールメッセージ、もう 1 つは一方的に送信される大量のメールメッセージです。

侵入

侵入とは、ネットワークまたはコンピュータに力づくで、または許可を得ずに入り込むことを指します。ネットワークまたはコンピュータのセキュリティをバイパスすることを指す場合もあります。

不正挙動

不正挙動とは、ソフトウェアが、OS、レジストリエントリ、他のソフトウェア、またはファイルおよびフォルダを許可なく変更することを指します。

インスタントメッセージャーでの不適切な内容の送信

使用するのにふさわしくないキーワードや、組織が送信を禁止しているキーワードを、インスタントメッセージングアプリケーションを介して送信することです。たとえば、社外秘情報がこれに該当します。

Packer

Packer とは、実行可能プログラムを圧縮するツールです。実行可能プログラムを圧縮すると、その中のコードは、従来のウイルス検索製品では検出しにくくなります。Packer によってトロイの木馬やワームが隠されることがあります。

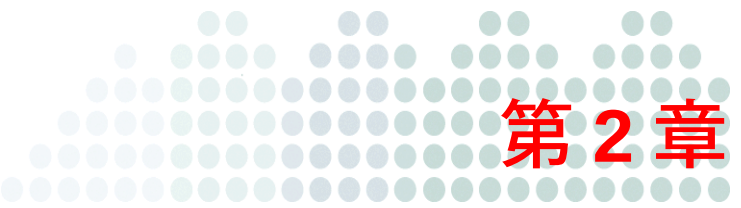
トレンドマイクロの検索エンジンは、圧縮されたファイルを検出できます。圧縮されたファイルに推奨される処理は「隔離」です。

製品コンポーネントの用語集

次の表に、製品ドキュメントで使用されている用語を示します。

表 1-2. 製品コンポーネントの用語集

項目	説明
ビジネスセキュリティサーバ	ビジネスセキュリティサーバは管理コンソールをホストします。この管理コンソールは、製品を集中管理する Web ベースのコンソールです。
スキャンサーバ	スキャンサーバは、スマートスキャン用に設定されているクライアントの検索を支援します。初期設定では、スキャンサーバはビジネスセキュリティサーバにインストールされます。
ビジネスセキュリティクライアント	ビジネスセキュリティクライアントを指します。ビジネスセキュリティクライアントは、自身がインストールされているコンピュータを保護します。
クライアント	クライアントとは、ビジネスセキュリティクライアントがインストールされているデスクトップ、ポータブルコンピュータおよびサーバを示します。
管理コンソール	管理コンソールは、すべてのビジネスセキュリティクライアントの集中管理に使用する Web ベースのコンソールです。管理コンソールはビジネスセキュリティサーバにインストールされます。



第2章

使用の開始

本章では、Trend Micro ビジネスセキュリティ（以下、ビジネスセキュリティ）の起動方法と実行方法について説明します。

本章で説明する内容には、次の項目が含まれます。

- 26 ページの「管理コンソールにアクセスする」
- 29 ページの「最新ステータス」
- 32 ページの「セキュリティ設定を表示する」

管理コンソールにアクセスする

ここでは、管理コンソールの概要と、管理コンソールにアクセスする方法を説明します。

表 2-1. 管理コンソールの主な機能

機能	説明
メインメニュー	管理コンソールの最上部に表示されるのがメインメニューです。このメニューには常にアクセスできます。
設定領域	メインメニュー項目の下には設定領域が表示されます。この領域では、選択したメニュー項目に応じてオプションを選択します。
メニューサイドバー	[セキュリティ設定] 画面でクライアントまたはグループを選択し、[設定] をクリックすると、メニューサイドバーが表示されます。このサイドバーを使用して、デスクトップとサーバのセキュリティおよび検索を設定します。
[セキュリティ設定] ツールバー	[セキュリティ設定] 画面を開くと、多数のアイコンがツールバーに表示されます。[セキュリティ設定] 画面でクライアントまたはグループをクリックしてから、ツールバーのアイコンをクリックすると、関連付けられたタスクがビジネスセキュリティサーバで実行されます。

ウイルスバスター ビジネスセキュリティ (以下、ビジネスセキュリティ) サーバのインストールの際は、集中管理に使用する Web ベースの管理コンソールもインストールします。このコンソールでは、ActiveX、CGI、HTML、HTTP/HTTPS などのインターネット技術が使用されています。

管理コンソールを開くには

1. 管理コンソールを開くには、次のいずれかの方法を使用します。
 - デスクトップ上のショートカット [ビジネスセキュリティ] をクリックします。
 - Windows の [スタート] メニューで、[Trend Micro ビジネスセキュリティ] → [ビジネスセキュリティ] の順にクリックします。
 - 管理コンソールは、ネットワーク上の任意のコンピュータから開くことができます。Web ブラウザを開いて、アドレスバーに次のアドレスを入力します。

`https://{ ビジネスセキュリティサーバ名 }:{ ポート番号 }/SMB`

例を以下に示します。

`https://my-test-server:4343/SMB`

`https://192.168.0.10:4343/SMB`

`http://my-test-server:8059/SMB`

`http://192.168.0.10:8059/SMB`

SSL を使用していない場合は、**https** ではなく **http** と入力します。ポートの初期設定値は、HTTP 接続の場合は 8059、HTTPS 接続の場合は 4343 です。

ヒント： DNS によるサーバ名の解決ができない環境では、{Trend Micro ビジネスセキュリティ名} を {Trend Micro ビジネスセキュリティ IP アドレス} で置き換えてください。

2. ブラウザにビジネスセキュリティのログオン画面が表示されます。



図 2-1. ビジネスセキュリティのログオン画面

3. [パスワード] ボックスにパスワードを入力して、[ログオン] をクリックします。ブラウザに、管理コンソールの [最新ステータス] 画面が表示されます。

管理コンソールのアイコン

次の表は、管理コンソールに表示されるアイコンとその用途を示しています。

表 2-2. 管理コンソールのアイコン

アイコン	説明
	[ヘルプ] アイコン。オンラインヘルプを開きます。
	[表示更新] アイコン。現在の画面の情報を更新します。

表 2-2. 管理コンソールのアイコン (続き)

アイコン	説明
	セクションの展開と折り畳みアイコン。セクションの表示または非表示を切り替えます。一度に展開できるセクションは 1 つのみです。
	[情報] アイコン。特定の項目に関連する情報を表示します。

最新ステータス

[最新ステータス] 画面を使用して、ビジネスセキュリティを管理します。

[最新ステータス] 画面に表示される情報の更新間隔は、セクションによって異なります。通常、更新間隔は 1 ～ 10 分です。画面の情報を手動で更新するには、[表示更新] をクリックします。



図 2-2. [最新ステータス] 画面

アイコンについて

ネットワーク上のコンピュータを保護するための処理が必要な場合は、警告のアイコンが表示されます。セクションを展開すると、詳細情報が表示されます。表の中の項目をクリックして、詳細情報を表示することもできます。特定のクライアントに関する詳細を表示するには、表に表示される数値のリンクをクリックします。

表 2-3. [最新ステータス] のアイコン

アイコン	説明
	通常 対処が必要なクライアントは少数です。コンピュータおよびネットワーク上のウイルス、スパイウェア、およびその他の不正プログラムの活動が発生する危険度は高くありません。
	警告 さらなる危険からネットワークを保護する処理を実行してください。通常、警告アイコンは、ウイルス、またはその他の不正プログラムの検出を多数報告している脆弱なコンピュータが多数あることを意味します。トレンドマイクロからイエローアラートが発行されると、大規模感染予防の警告が表示されます。
	処理が必要です。 警告のアイコンは、管理者がセキュリティ上の問題を解決するための処理を行う必要があることを示しています。

[最新ステータス] 画面に表示される情報は、クライアントから収集されたデータに基づいています。

脅威ステータス

[脅威ステータス] 画面には、次の情報が表示されます。

- ウイルス / 不正プログラム対策** — ウイルスの検出。5 件目からステータスアイコンが警告に変化します。次の場合は処理を実行する必要があります。
 - ビジネスセキュリティクライアントで、実行するよう設定されている処理を正常に実行できなかった場合。数値のリンクをクリックして、ビジネスセキュリティクライアントが処理を実行できなかったコンピュータに関する詳細を表示します。
 - ビジネスセキュリティクライアントでリアルタイム検索が無効になっている場合。[有効化] をクリックして、リアルタイム検索をもう一度開始します。
- スパイウェア対策** — [スパイウェア対策] セクションには、最後に実行されたスパイウェア検索の結果とスパイウェアログエントリが表示されます。

- 特定のクライアントに関する詳細を表示するには、検出された件数の値をクリックします。ここから、クライアントに影響を及ぼしている特定のスパイウェアの脅威に関する情報を確認できます。
- **URL フィルタ** — 管理者による指定によってアクセスが制限されている Web サイト。300 件目からステータスアイコンが警告に変化します。
- **挙動監視** — 挙動監視ポリシー違反。
- **ネットワークウイルス** — ファイアウォール設定で指定されているネットワークウイルスの検出。
- **大規模感染予防** — ネットワーク上での大規模感染発生の可能性。
- **Web レピュテーション** — トレンドマイクロによって指定されている危険な可能性のある Web サイト。200 件目からステータスアイコンが警告に変化します。

システムステータス

アップデートされたコンポーネント、およびビジネスセキュリティクライアントがインストールされているコンピュータの空き領域に関する情報が表示されます。

- **コンポーネントのアップデート** — ビジネスセキュリティサーバのコンポーネントアップデートのステータス、またはビジネスセキュリティクライアントへの最新コンポーネントの配信。
- **システム異常イベント** — ビジネスセキュリティサーバとクライアントが同じサーバにインストールされているときのディスク領域情報。
- **スマートスキャン** — 割り当てられている検索サーバに接続できないクライアント。

ヒント: [オプション設定] → [通知設定] から、管理コンソールでの [警告] または [必要な処理] アイコンの表示をトリガするパラメータをカスタマイズできます。

ライセンス

ライセンスステータスに関する情報が表示されます。

- **ライセンス** — 製品ライセンスのステータス、特に有効期限に関する情報。

最新ステータスのアップデート間隔

[最新ステータス] の情報のアップデート間隔については、次の表を参照してください。

表 2-4. 最新ステータスのアップデート間隔

項目	アップデート間隔 (分)	クライアントからサーバにログが送信される までの時間 (分)
大規模感染予防	3	対応なし
ウイルス / 不正プログラム 対策	1	ビジネスセキュリティクライアント : 直後
スパイウェア対策	3	1
Web レピュテーション	3	60
URL フィルタ	3	60
挙動監視	3	60
ネットワークウイルス	3	60
スマートスキャン	10	対応なし
ライセンス	10	対応なし
コンポーネントのアップ デート	3	対応なし
システム異常イベント	10	"Trend Micro Client/Server Security Agent Listener" サービスが開始できなかったとき

セキュリティ設定を表示する

[セキュリティ設定] 画面では、ビジネスセキュリティクライアントをインストールしたすべてのコンピュータを管理できます。セキュリティ設定のグループツリーからグループを選択すると、そのグループに属するコンピュータが右の表に表示されます。

設定領域

設定領域には、ビジネスセキュリティサーバ情報バー、設定ツールバー、およびツールバーの下でセキュリティ設定のグループツリーとビジネスセキュリティクライアント情報テーブルが含まれます。

ビジネスセキュリティサーバ情報バー — ドメイン名、ポート番号、管理対象のデスクトップとサーバの数など、ビジネスセキュリティサーバに関する情報が表示されます。

ツールバー

- **設定** — [設定] ツールは、セキュリティ設定のグループツリーのいずれかの項目が選択された場合にのみ使用できます。[設定] ツールを使用すると、グループ内のすべてのビジネスセキュリティクライアントの設定を指定できます。1つのグループ内のすべてのコンピュータに、同じ設定を指定する必要があります。次の設定を指定できます。

検索方法、ウイルス / スパイウェア対策、ファイアウォール、Web レピュテーション、URL フィルタ、挙動監視、Trend Secure ツールバー、およびクライアント権限。

- **設定の複製** — [設定の複製] ツールは、セキュリティ設定のグループツリーのいずれかの項目が選択され、セキュリティ設定のグループツリーに同じ種類のその他の項目が1つ以上存在する場合にのみ使用できます。
- **インポート / エクスポート** — 設定を保存するか、すでに保存されている設定をインポートします。
- **グループの追加** — [グループの追加] ツールを使用すると、新しいデスクトップまたはサーバのグループを追加できます。
- **追加** — [追加] ツールを使用すると、指定したコンピュータにビジネスセキュリティクライアントをインストールすることによって、特定のグループにコンピュータを追加できます。
- **削除** — [削除] ツールによって、指定したコンピュータからビジネスセキュリティクライアントが削除されます。
- **移動** — [移動] ツールを使用すると、選択したコンピュータまたはサーバをビジネスセキュリティサーバ間で移動できます。
- **カウンタのリセット** — [カウンタのリセット] ツールは、1つのグループ内のすべてのコンピュータに対して機能します。これをクリックすると、ビジネスセキュリティクライアント情報テーブルの検出されたウイルスの数がゼロにリセットされます。
- **セキュリティ設定のグループツリー** — セキュリティ設定のグループツリーからグループを選択すると、そのグループに属するコンピュータのリストが右側に表示されます。
- **ビジネスセキュリティクライアント情報テーブル** — クライアントを選択して、ツールバーから任意のツールをクリックすると、管理コンソールに新しい設定領域が表示されます。



第3章

ビジネスセキュリティクライアントのインストール

本章では、Trend Micro ビジネスセキュリティ（以下、ビジネスセキュリティ）クライアントをインストールまたはアップグレードするために必要な手順について説明します。また、ビジネスセキュリティクライアントの削除についても説明します。

本章で説明する内容には、次の項目が含まれます。

- 36 ページの「ビジネスセキュリティクライアントのインストールの概要」
- 37 ページの「ビジネスセキュリティクライアントのインストール / アップグレード / 移行の概要」
- 38 ページの「新規インストールを実行する」
- 49 ページの「ビジネスセキュリティクライアントのインストール、アップグレード結果を確認する」
- 52 ページの「ビジネスセキュリティクライアントを削除する」

ビジネスセキュリティクライアントのインストールの概要

ビジネスセキュリティでは、いくつかの方法でビジネスセキュリティクライアントをインストールできます。ここでは、これらの方法の概要を紹介します。

ヒント： 厳しいポリシーが施行されている組織では、リモートインストールまたはログオンスクリプトウィザードをお勧めします。

- ・ **インストール用 Web ページ** — 社内のユーザに、インストール用 Web ページにアクセスしてビジネスセキュリティクライアントのセットアップファイルをダウンロードして、インストールするよう指示します (38 ページの「Web ページからインストールする」を参照)。
- ・ **ログオンスクリプトウィザード** — ウイルス対策が実施されていないコンピュータがドメインにログオンしたときに、これらのコンピュータにビジネスセキュリティクライアントが自動的にインストールされるようにします (39 ページの「ログオンスクリプトウィザードを使用してインストールする」を参照)。
- ・ **Client Packager** — ビジネスセキュリティクライアントのセットアップファイルやアップデートファイルを、メールを使用してクライアントにインストールします (41 ページの「Client Packager を使用してインストールする」を参照)。
- ・ **リモートインストール** — 管理コンソールからビジネスセキュリティクライアントをすべての Windows Vista/2000/XP/Server 2003/Server 2008 クライアントにインストールします (45 ページの「リモートインストールを使用してインストールする」を参照)。
- ・ **脆弱性検索ツール (TMVS)** — 脆弱性検索ツールを使用してウイルス対策が実施されていないコンピュータを検索し、ビジネスセキュリティクライアントをすべての Windows 2000/Server 2003 クライアントにインストールします (47 ページの「脆弱性検索ツールを使用してインストールする」参照)。

表 3-1. ビジネスセキュリティクライアントのインストール方法

	Web ページ	ログオン スクリプト ウィザード	Client Packager	リモートイン ストール	TMVS
WAN 経由のインストールに適している	はい	いいえ	はい	いいえ	いいえ
集中管理に適している	はい	はい	いいえ	はい	はい
ユーザの介入が必要	はい	いいえ	はい	いいえ	いいえ

表 3-1. ビジネスセキュリティクライアントのインストール方法（続き）

	Web ページ	ログオン スクリプト ウィザード	Client Packager	リモートイン ストール	TMVS
IT リソースが必要	いいえ	はい	はい	はい	はい
大量インストールに適 している	いいえ	はい	いいえ	はい	はい
帯域幅の消費量	少ない (予約される 場合)	多い (各クラ イアントが同 時に起動され る場合)	少ない (予約される場 合)	少ない (予約される場 合)	少ない (予約される場 合)
必要な権限	管理者権限 (すべてのインストール方法に必要な)				

注意： これらのビジネスセキュリティクライアントのインストール方法のいずれかを使用するに
は、インストール先のクライアント上でローカル管理者権限を有している必要があります。

ビジネスセキュリティクライアントのインストール / アップグレード / 移行の概要

ここでは、次の項目について説明します。

- ・ 選択したインストール方法を使用したビジネスセキュリティクライアントの新規インストール
の実行（36 ページの「ビジネスセキュリティクライアントのインストールの概要」を参照）
- ・ ビジネスセキュリティクライアントの旧バージョンから最新バージョンへのアップグレード
（49 ページの「ビジネスセキュリティクライアントのインストール、アップグレード結果を確
認する」を参照）
- ・ インストール済みの他社製ウイルス対策製品から最新バージョンのビジネスセキュリティへの
移行（49 ページの「ビジネスセキュリティクライアントのインストール、アップグレード結果
を確認する」を参照）

注意： ビジネスセキュリティクライアントをインストールする前に、クライアントで実行中のア
プリケーションをすべて終了してください。他のアプリケーションの実行中にインストー
ルした場合、インストールプロセスに通常より長い時間がかかることがあります。

新規インストールを実行する

インストール先コンピュータにビジネスセキュリティクライアントを今回初めてインストールする場合は、次のいずれかの手順を実行してください。

Web ページからインストールする

Windows 2000、Windows XP、または Windows Server 2003、および Internet Information Services (IIS) 5.0/6.0/7.0 または Apache 2.0.63 を実行しているコンピュータにビジネスセキュリティサーバをインストールした場合は、マスタセットアップ時に作成されたインストール用 Web サイトからビジネスセキュリティクライアントをインストールできます。

この方法では、ビジネスセキュリティクライアントを簡単にインストールできます。管理者は、ユーザがインストール用 Web ページにアクセスして、ビジネスセキュリティクライアントのセットアップファイルをダウンロードするように指示するだけです。

ヒント： 脆弱性検索ツールを使用すると、管理コンソールからインストールするという指示に従っていないユーザを確認できます（詳細については、50 ページの「脆弱性検索ツールを使用してクライアントインストールを確認する」を参照）。

ビジネスセキュリティクライアントのセットアップファイルを正常にダウンロードするには、クライアントコンピュータに Microsoft Internet Explorer 5.5 以降がインストールされている必要があります。また、Internet Explorer のセキュリティレベルの設定で ActiveX コントロールを有効にしておく必要があります。次の手順は、ユーザの観点から記述されています。ビジネスセキュリティクライアントを Web サーバからインストールするための次の手順をユーザにメールで通知してください。

インストール用 Web ページからインストールするには

1. Internet Explorer を起動して、次のように入力します。

```
https://{ビジネスセキュリティサーバ名}:{ポート番号}  
}/SMB/console/html/client
```

例を以下に示します。

```
https://my-test-server:4343/SMB/console/html/client  
http://my-test-server:8059/SMB/console/html/client  
https://192.168.0.10:4343/SMB/console/html/client  
http://192.168.0.10:8059/SMB/console/html/client
```

または管理コンソールの URL を使用します。パスワード画面で、クライアントのインストール用にここをクリックすることを示すリンクが表示されます。

SSL を使用していない場合は、「https」ではなく「http」と入力します。

2. [インストール] をクリックして、ビジネスセキュリティクライアントのインストールを開始します。

注意： Windows Vista の場合は、保護モードが有効になっていることを確認してください。
保護モードを有効にするには、Internet Explorer で [ツール] → [インターネット オプション] → [セキュリティ] の順にクリックします。

インストールが開始します。インストールが完了すると、画面にクライアントのインストールが完了したことを知らせるメッセージが表示されます。

3. 正常にインストールされたことを確かめるため、Windows のタスクトレイにビジネスセキュリティクライアントのアイコンが表示されていることを確認します。
- 従来型スキャン: 
 - スマートスキャン: 

ログオンスクリプトウィザードを使用してインストールする

ログオンスクリプトウィザードを使用すると、ウイルス対策が実施されていないコンピュータがドメインにログオンしたときに、ビジネスセキュリティクライアントが自動的にインストールされます。ログオンスクリプトウィザードを実行すると、サーバのログオンスクリプトに **autopcc.exe** というプログラムが追加されます。**autopcc.exe** は、次の機能を実行するプログラムです。

- ウイルス対策が実施されていないコンピュータとビジネスセキュリティクライアントの OS を特定します。
- 検索エンジン、ウイルスパターンファイル、ダメージクリーンアップサービスのコンポーネント、クリーンアップファイル、およびプログラムファイルをアップデートします。

注意： ログオンスクリプトによるインストールを実行するには、クライアントがインストール実行サーバの Active Directory に参加している必要があります。

ログオンスクリプトウィザードを使用して autopcc.exe をログオンスクリプトに追加するには

1. ビジネスセキュリティをインストールしたコンピュータで、**C:\Program Files\Trend Micro\Security Server\PCCSRV\Admin\SetupUsr.exe** を開きます。ログオンスクリプトウィザードが起動します。コンソールには、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. 変更するログオンスクリプトがある Windows 2000/Server 2003/Server 2008 コンピュータを参照して選択し、[選択] をクリックします。サーバはプライマリドメインコントローラである必要があり、ユーザは管理者のアクセス権限を有している必要があります。
ユーザ名とパスワードの入力が求められます。
3. ユーザ名とパスワードを入力します。[OK] をクリックして続行します。
[ユーザ選択] 画面が表示されます。[ユーザ] リストには、このサーバにログオンしているコンピュータの一覧が表示されます。[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が表示されます。
 - 単一または複数のユーザのログオンスクリプトを変更するには、[ユーザ] から該当するユーザを選択し、[追加] をクリックします。
 - 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。
 - すでに変更したコンピュータのユーザを除外するには、[選択したユーザ] から該当するユーザを選択して [削除] をクリックします。
 - 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。
4. すべての対象ユーザが [選択したユーザ] リストに追加されたら、[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知らせるメッセージが表示されます。
5. [OK] をクリックします。ログオンスクリプトウィザードの初期画面に戻ります。
 - 他のサーバのログオンスクリプトを変更するには、手順 2 ～ 4 を繰り返します。
 - 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。

注意： ログオンスクリプトが変更されたサーバに、ウイルス対策が実施されていないコンピュータがログオンすると、**autopcc.exe** によって自動的にそのコンピュータにクライアントがインストールされます。

ログオンスクリプトを使用してインストールする

Windows 2000/Server 2003/Server 2008 用の既存のログオンスクリプトがある場合、ログオンスクリプトウィザードは **autopcc.exe** を実行するコマンドを追加します。スクリプトがない場合、ログオンスクリプトウィザードは **ofcscan.bat** という名前のバッチファイルを作成します（このファイルには **autopcc.exe** を実行するコマンドが含まれます）。

ログオンスクリプトウィザードにより、次の行がスクリプトの末尾に追加されます。

%%{ サーバ名 }%ofcscan

{サーバ名} は、ビジネスセキュリティサーバがインストールされているコンピュータの名前または IP アドレスです。

ヒント： DNS によるサーバ名の解決ができない環境では、{サーバ名} を {サーバ IP アドレス} で置き換えてください。

Windows 2000 のログオンスクリプトは、Windows 2000 サーバ上の次の場所にあります（ネットログオンの共有ディレクトリ経由）。

%%{ システムドライブ }%WINNT%SYSVOL%domain%scripts%ofcscan.bat

Server 2003 のログオンスクリプトは、Server 2003 サーバ上の次の場所にあります（ネットログオンの共有ディレクトリ経由）。

%%{ システムドライブ }%windir%sysvol%domain%scripts%ofcscan.bat

Server 2008 のログオンスクリプトは、Server 2008 サーバ上の次の場所にあります（ネットログオンの共有ディレクトリ経由）。

%%{ システムドライブ }%windir%sysvol%domain%scripts%ofcscan.bat

Client Packager を使用してインストールする

Client Packager を使用すると、セットアップファイルおよびアップデートファイルを圧縮して、1 つの自己解凍ファイルを作成できます。これにより、メールや CD-ROM などの記録媒体を使用してファイルを簡単に配布できます。

ユーザがパッケージを受信すると、そのファイルをダブルクリックするだけでセットアッププログラムが実行されます。Client Packager を使用してインストールされたビジネスセキュリティクライアントにより、Client Packager がセットアップパッケージを作成した場所がサーバに報告されます。このツールは、遠隔地にある低帯域幅のオフィスのクライアントコンピュータに、ビジネスセキュリティクライアントやアップデートファイルをインストールする際に特に便利です。

Client Packager インストールに関する考慮事項

- **インストール**: ビジネスセキュリティクライアントからビジネスセキュリティサーバに接続できない場合、クライアントでは初期設定が維持されます。ビジネスセキュリティクライアントからビジネスセキュリティサーバに接続できる場合にのみ、クライアントはグループ設定を取得します。
- **アップグレード**: Client Packager を使用したビジネスセキュリティクライアントのアップグレードの際に問題が発生した場合は、まず前のバージョンのビジネスセキュリティクライアントをアンインストールしてから新しいバージョンをインストールすることをお勧めします。

注意: Client Packager を使用するには、クライアント上に 370MB 以上の空きディスク領域が必要です。クライアントで MSI パッケージを実行するには、Windows インストーラ 3.0 が必要です。

Client Packager では、次の 2 種類の自己解凍ファイルを作成できます。

- **実行可能形式**

注意: Windows Vista では、管理者権限でプログラムを実行する必要があります (管理者として実行)。

- **Microsoft インストーラパッケージ形式 (MSI)**: このファイルタイプは、Microsoft Windows インストーラパッケージ仕様に準拠しており、サイレント インストールまたは Active Directory インストールに使用できます。MSI の詳細については、Microsoft の Web サイトを参照してください。

ヒント: Active Directory を使用して MSI パッケージをインストールする場合は、[ユーザーの構成] 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。これにより、どのユーザがコンピュータにログオンしているかにかかわらず、MSI パッケージを確実にインストールできます。

Client Packager の GUI を使用してパッケージを作成するには

1. ビジネスセキュリティサーバで、エクスプローラを開きます。
2. ¥PCCSRV¥Admin¥Utility¥ClientPackager に移動します。
3. ClnPack.exe をダブルクリックしてツールを実行します。Client Packager のコンソールが開きます。

注意： このツールは、常にビジネスセキュリティサーバをインストールしたコンピュータから実行する必要があります。

4. [対象 OS] で、パッケージの作成対象の OS を選択します。
5. [検索方法] を選択します。
 - ・ **従来型スキャン：** クライアント上のローカル検索エンジンで、クライアントコンピュータを検索します。
 - ・ **スマートスキャン：** スキャンサーバがクライアントの検索を支援します。スキャンサーバは、セキュリティサーバで自動的にインストールされます。検索方法を [セキュリティ設定] 画面で選択できます。検索モードごとに異なるパターンファイルが使用されます。従来型スキャンでは、従来のウイルスパターンファイルが使用されます。
6. 作成するパッケージの種類として、次のいずれかを選択します。
 - ・ **セットアップ** — ビジネスセキュリティクライアントをインストールする場合に選択します。
 - ・ **アップデート** — ビジネスセキュリティクライアントのコンポーネントのみをアップデートする場合に選択します。
7. [オプション] で、次のいずれかのインストールオプションを選択します。
 - ・ **サイレントモード** — バックグラウンドでクライアントにインストールされるパッケージを作成します。クライアント側ではインストールが実行されていることは認識されず、インストール状況ウィンドウは表示されません。
 - ・ **MSI パッケージ** — Microsoft Windows インストーラパッケージ形式に準拠したパッケージを作成します。

注意： MSI パッケージは、Active Directory インストール専用です。ローカルインストールの場合は、.exe パッケージを作成してください。

- ・ **インストール前のウイルス検索の無効化 (新規インストールのみ)** — セットアップ開始前にビジネスセキュリティが実行する通常のファイル検索を無効にします。

8. [コンポーネント] で、インストールパッケージに組み込むコンポーネントを選択します。
 - **プログラム** — すべてのコンポーネント
 - **検索エンジン** — ビジネスセキュリティサーバの最新検索エンジン
 - **ウイルスパターンファイル** — ビジネスセキュリティサーバの最新ウイルスパターンファイル
 - **脆弱性検索診断パターンファイル** — ビジネスセキュリティサーバの最新脆弱性診断パターンファイル
 - **スパイウェアコンポーネント** — ビジネスセキュリティサーバの最新スパイウェアコンポーネント
 - **ファイアウォールドライバ** — ファイアウォールのドライバ
 - **ネットワークウイルスパターンファイル** — ネットワークウイルス専用の最新パターンファイル
 - **ダメージクリーンナップエンジン/テンプレート** — ビジネスセキュリティサーバの最新ウイルスクリーンナップエンジンおよびテンプレート
 - **IntelliTrap パターンファイル** — ビジネスセキュリティサーバの最新 IntelliTrap パターンファイル
9. [ソースファイル] の横に表示されている、**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、このファイルはビジネスセキュリティサーバの **¥PCCSRV** フォルダに格納されています。
10. [出力ファイル] で  をクリックして、パッケージのファイル名 (例: **ClientSetup.exe**) および作成場所を指定します。
11. [作成] をクリックしてパッケージを作成します。パッケージの作成が完了すると、「パッケージは正常に作成されました。」という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。
12. 作成したパッケージをメールでユーザに送信するか、CD-ROM などの記録媒体にコピーしてユーザに配布します。

警告： パッケージは、そのパッケージが作成されたサーバの管理下にあるビジネスセキュリティクライアントにのみ送信できます。パッケージを、他のビジネスセキュリティサーバの管理下にあるビジネスセキュリティクライアントには送信しないでください。

MSI ファイルを使用してインストールする

Active Directory を使用している場合は、Microsoft Windows インストーラファイルを作成することにより、ビジネスセキュリティクライアントをインストールできます。Client Packager を使用して、.msi 拡張子を持つファイルを作成してください。MSI ファイルを使用して、ビジネスセキュリティクライアントをすべてのクライアントに同時に自動インストールすることで、Active Directory の機能を活用できます。これにより、各ユーザ自身でビジネスセキュリティクライアントをインストールする必要がなくなります。

MSI の詳細については、Microsoft の Web サイトを参照してください。MSI ファイルの作成手順については、41 ページの「Client Packager を使用してインストールする」を参照してください。

リモートインストールを使用してインストールする

リモートインストールを使用すると、ネットワークに接続された Windows Vista/2000/XP (Professional Edition のみ)/Server 2003/Server 2008/SBS 2008/EBS 2008 コンピュータにビジネスセキュリティクライアントをリモートでインストールできます。複数のコンピュータに同時にインストールすることも可能です。

注意： リモートインストールを使用するには、インストール先コンピュータの管理者権限が必要です。Windows Vista、Server 2008、SBS 2008、および EBS 2008 の場合、Windows User Account Control (UAC) のためにビルトインのドメイン管理者パスワードを使用する必要があります。

リモートインストールを使用してビジネスセキュリティクライアントをインストールするには

注意： Windows Vista にビジネスセキュリティクライアントをインストールする場合、追加の手順が必要になります。詳細については、46 ページの「Windows Vista クライアントでビジネスセキュリティクライアントのリモートインストールを有効にする」を参照してください。

1. 管理コンソールのメインメニューから、[セキュリティ設定] → [追加] の順に選択します。[コンピュータの追加] 画面が表示されます。
2. [コンピュータの種類] セクションで、[デスクトップまたはサーバ] を選択します。
3. [クライアントのインストール方法] で、[リモートインストール] を選択します。
4. [次へ] をクリックします。[リモートインストール] 画面が表示されます。

5. [グループとコンピュータ] ボックスのコンピュータリストからクライアントを選択して、[追加] 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られます。
6. ユーザ名とパスワードを入力して、[ログイン] をクリックします。[選択したコンピュータ] リストボックスに、インストール先コンピュータが表示されます。
7. これらの手順を繰り返して、すべての Windows コンピュータを [選択したコンピュータ] リストボックスに追加します。
8. [インストール] をクリックして、ビジネスセキュリティクライアントをインストール先コンピュータにインストールします。確認ボックスが表示されます。
9. [はい] をクリックして、ビジネスセキュリティ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ことを確認します。ビジネスセキュリティクライアントのファイルが各インストール先コンピュータにコピーされている間、進行状況画面が表示されます。

ビジネスセキュリティによりインストール先コンピュータへのインストールを完了すると、選択されたコンピュータリストの [結果] にインストール状況が表示されて、コンピュータ名が緑のチェックマーク付きで表示されます。

注意： リモートインストールでは、ビジネスセキュリティサーバがすでに稼働しているコンピュータにビジネスセキュリティクライアントをインストールできません。

Windows Vista クライアントでビジネスセキュリティクライアントのリモートインストールを有効にする

Windows Vista クライアントにビジネスセキュリティクライアントをインストールするには、次の追加手順が必要です。

Windows Vista クライアントでリモートインストールを有効にするには

1. クライアントで、[ファイルとプリンタの共有] を一時的に有効にします。

注意： 社内のセキュリティポリシーで Windows ファイアウォールが無効になっている場合は、手順 2 に進んで Remote Registry サービスを開始します。

- a. コントロールパネルで Windows ファイアウォールを開きます。
- b. [Windows ファイアウォールによるプログラムの許可] をクリックします。管理者パスワードまたは確認を求められたら、パスワードを入力するか、確認します。[Windows ファイアウォール設定] 画面が表示されます。

- c. [例外] タブのプログラムまたはポートリストの下の [ファイルとプリンタの共有] チェックボックスがオンになっていることを確認します。
 - d. [OK] をクリックします。
2. Remote Registry サービスを一時的に有効にします。
- a. マイクロソフト管理コンソールを起動します。

ヒント： マイクロソフト管理コンソールを起動するには、[ファイル名を指定して実行] で「**services.msc**」と入力します。

- b. [Remote Registry] を右クリックして、[開始] を選択します。
3. Windows Vista クライアントにビジネスセキュリティクライアントをインストールしたら、必要に応じて元の設定に戻します。

脆弱性検索ツールを使用してインストールする

脆弱性検索ツールを使用すると、インストール済みのウイルス対策製品を検出したり、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たり、これらのコンピュータにビジネスセキュリティクライアントをインストールしたりできます。コンピュータが保護を必要としているかどうかを調べるため、脆弱性検索ツールは、ウイルス対策製品が通常使用するポートに対して ping コマンドを送信します。

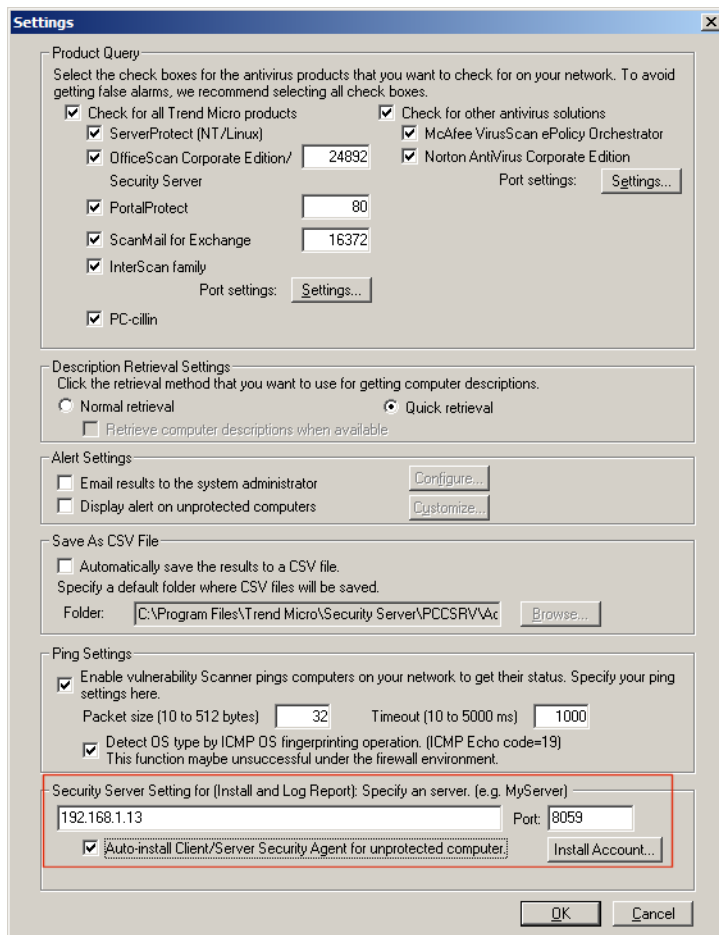
ここでは、脆弱性検索ツールを使用してビジネスセキュリティクライアントをインストールする方法を説明します。脆弱性検索ツールを使用してウイルス対策製品を検出する方法の手順については、50 ページの「脆弱性検索ツールを使用してクライアントインストールを確認する」を参照してください。

注意： Windows 2000 または Windows Server 2003 が稼働しているコンピュータでは脆弱性検索ツールを使用できますが、ターミナルサーバを実行しているコンピュータでは使用できません。

ビジネスセキュリティサーバがクライアントコンピュータにすでにインストールされている場合には、脆弱性検索ツールを使用してそのクライアントコンピュータにビジネスセキュリティクライアントをインストールすることはできません。

脆弱性検索ツールを使用してビジネスセキュリティクライアントをインストールするには

1. ビジネスセキュリティサーバがインストールされているドライブで、{ビジネスセキュリティサーバの場所}\PCCSRV\Admin\Utility\TMVS に移動します。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. [Settings] をクリックします。[Settings] 画面が表示されます。

**図 3-1. TMVS の [Settings] 画面**

3. [Security Server Setting (Specify a Server name or IP address)] の下に、ビジネスセキュリティサーバの名前または IP アドレスとポート番号を入力します。
4. [Auto-install Client/Server Security Agent on unprotected computer] チェックボックスをオンにします。
5. [Install Account] をクリックします。
6. サーバ (またはドメイン) に対する管理者権限があるユーザの名前とパスワードを入力し、[OK] をクリックします。
7. [OK] をクリックして、メインの TMVS 画面に戻ります。
8. [Start] 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、ビジネスセキュリティクライアントのインストールを開始します。

メール通知を使用してインストールする

これを使用して、インストーラへのリンクのあるメールメッセージを送信します。

コンソールからパッケージの場所を通知するには

1. 管理コンソールのメインメニューから、[セキュリティ設定] → [追加] の順に選択します。[コンピュータの追加] 画面が表示されます。
2. [コンピュータの種類] セクションで、[デスクトップまたはサーバ] を選択します。
3. [クライアントのインストール方法] で、[メール通知によるインストール] を選択します。
4. [次へ] をクリックします。[メール通知によるインストール] 画面が表示されます。
5. メール の件名と受信者を入力します。
6. [適用] をクリックします。初期設定のメールクライアントで、受信者、件名、およびインストーラへのリンクのあるメールが開きます。

ビジネスセキュリティクライアントのインストール、アップグレード結果を確認する

インストールまたはアップグレードの完了後に、ビジネスセキュリティクライアントが正しくインストールされていることを確認します。

インストールを確認するには

- ・ ビジネスセキュリティクライアントを実行しているクライアントコンピュータの Windows の [スタート] メニューに、ビジネスセキュリティクライアントプログラムのショートカットが表示されることを確認します。

- クライアントコンピュータのコントロールパネルの [アプリケーションの追加と削除] (または [プログラムの追加と削除]) リストにビジネスセキュリティクライアントが含まれていることを確認します。
- 脆弱性検索ツールを使用します (50 ページの「脆弱性検索ツールを使用してクライアントインストールを確認する」を参照)。
- クライアント移動ツールを使用します。

脆弱性検索ツールを使用してクライアントインストールを確認する

ネットワーク内のすべてのクライアントコンピュータにビジネスセキュリティクライアントがインストールされたことを確認します。予約タスクを作成すると、脆弱性検索ツールが自動化されます。脆弱性検索ツールを自動化する方法については、ビジネスセキュリティのオンラインヘルプを参照してください。

注意： Windows 2000 および Windows Server 2003 が稼働しているコンピュータでは脆弱性検索ツールを使用できますが、ターミナルサーバを実行しているコンピュータでは使用できません。

脆弱性検索ツールを使用してインストール済みクライアントを確認するには

1. ビジネスセキュリティサーバがインストールされているドライブで、Trend Micro® Security Server¥PCCSRV¥Admin¥Utility¥TMVS に移動します。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. [Settings] をクリックします。[Settings] 画面が表示されます。
3. [Product Query] で、[Security Server] チェックボックスをオンにして、サーバがクライアントと通信するために使用するポートを指定します。
4. [Description Retrieval Settings] で、使用する取得検索方法を選択します。[Normal retrieval] の方が正確ですが、完了までに時間がかかります。
[Normal retrieval] をクリックした場合は、コンピュータの説明があれば取得するかどうかを指定できます。取得する場合は、[Retrieve computer descriptions when available] チェックボックスをオンにします。
5. 管理者または組織内の他の管理者に結果を自動的に送信するには、[Alert Settings] で [Email results to the system administrator] チェックボックスをオンにします。次に [Configure] をクリックして、メールを設定します。
 - [To] テキストボックスに、受信者のメールアドレスを入力します。
 - [From] テキストボックスに、管理者自身のメールアドレスを入力します。

- [SMTP server] テキストボックスに SMTP サーバのアドレスを入力します。たとえば、「smtp.example.com」と入力します。SMTP サーバ情報は必須です。
 - [Subject] テキストボックスに新しい件名を入力するか、または初期設定を適用します。
6. [OK] をクリックして、設定内容を保存します。
 7. 保護されていないコンピュータに警告を表示する場合、[Display alert on unprotected computers] チェックボックスをオンにします。次に [Customize] をクリックして、警告メッセージを設定します。[Alert Message] 画面が表示されます。
 8. 新しい警告メッセージをテキストボックスに入力するか、初期設定のメッセージをそのまま使用して、[OK] をクリックします。
 9. 結果を CSV 形式で保存する場合は、[Automatically save the results to a CSV file] チェックボックスをオンにします。初期設定では、脆弱性検索ツールは CSV データファイルを TMVS フォルダに保存します。初期設定の CSV フォルダを変更するには、[Browse] をクリックして、コンピュータまたはネットワーク上の保存先フォルダを選択して、[OK] をクリックします。
 10. [Ping Settings] で、脆弱性検索ツールがコンピュータにパケットを送信し、応答を待機する方法を設定します。初期設定をそのまま使用するか、[Packet size] と [Timeout] のフィールドに新しい値を入力します。
 11. [OK] をクリックします。脆弱性検索ツールのコンソールが表示されます。
 12. IP アドレスの範囲を指定して手動で脆弱性検索を実行するには、次のようにします。
 - a. [IP Range to Check] に、インストール済みウイルス対策製品および保護されていないコンピュータの有無をチェックする IP アドレスの範囲を入力します。
 - b. [Start] をクリックし、ネットワーク上のコンピュータに対する調査を開始します。
 13. DHCP サーバに IP アドレスをリクエストするコンピュータに対して手動で脆弱性検索を実行するには、次のようにします。
 - a. [Results] ボックスで [DHCP Scan] タブをクリックします。[DHCP Start] ボタンが表示されます。
 - b. [DHCP Start] をクリックします。脆弱性検索ツールは DHCP リクエストの待機を開始し、クライアントコンピュータがネットワークにログオンしたら、そのコンピュータに対して脆弱性検索を実行します。

脆弱性検索ツールによりネットワークがチェックされ、その結果が [Results] テーブルに表示されます。すべてのサーバ、デスクトップ、およびノートブック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ことを確認してください。

保護されていないサーバ、デスクトップまたはノートブックコンピュータが検出された場合は、希望のクライアントインストール方法を使用して、それらのコンピュータにクライアントをインストールしてください。

ビジネスセキュリティクライアントを削除する

ビジネスセキュリティクライアントを削除するには、次の 2 つの方法があります。

- アンインストールプログラムを実行する
- 管理コンソールを使用する

警告： ビジネスセキュリティクライアントを削除すると、クライアントコンピュータは脅威に対して脆弱になります。

アンインストールプログラムを使用してビジネスセキュリティクライアントを削除する

ユーザにビジネスセキュリティクライアントを削除する権限を付与している場合は、ビジネスセキュリティクライアントのアンインストールプログラムを各自のコンピュータから実行するように指示してください。

ビジネスセキュリティクライアントの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、[コントロールパネル] → [プログラムの追加と削除] の順に選択します。
2. ビジネスセキュリティクライアントを選択して、[変更と削除] をクリックします。[ビジネスセキュリティクライアントのアンインストール] 画面が表示され、アンインストールパスワードを設定してある場合はそのパスワードを入力するよう求められます。
3. アンインストールパスワードを入力して、[OK] をクリックします。

管理コンソールを使用してビジネスセキュリティクライアントを削除する

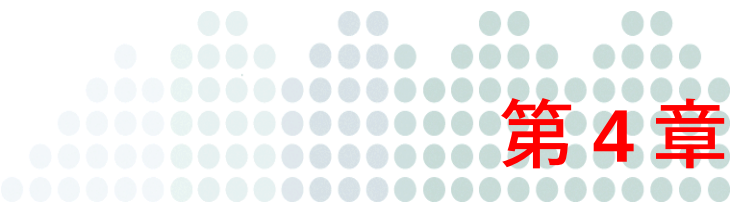
管理コンソールを使用して、ビジネスセキュリティクライアントをリモートで削除することもできます。

管理コンソールを使用してビジネスセキュリティクライアントをリモートで削除するには

1. 管理コンソールにログオンします。
2. [セキュリティ設定] タブをクリックします。

3. セキュリティ設定のグループツリーで、ビジネスセキュリティクライアントを削除するクライアントコンピュータを選択し、[削除] をクリックします。[コンピュータの削除] 画面が表示されます。
4. [削除の種類] で [選択したクライアントをアンインストール] をクリックし、[適用] をクリックします。確認のメッセージが表示されます。
5. [OK] をクリックします。ポップアップ画面が表示され、サーバが送信しクライアントコンピュータが受信したアンインストール通知の数が表示されます。
6. [OK] をクリックします。

ビジネスセキュリティクライアントが削除されたことを確認するには、[セキュリティ設定] 画面を更新します。そのクライアントは、セキュリティ設定のグループツリーには表示されなくなります。



第4章

グループの管理

本章では、Trend Micro ビジネスセキュリティ（以下、ビジネスセキュリティ）のグループの概念と使用方法について説明します。

本章で説明する内容には、次の項目が含まれます。

- 56 ページの「グループの概要」
- 56 ページの「グループ内のクライアントを表示する」
- 57 ページの「グループの追加」
- 58 ページの「管理コンソールからグループとコンピュータを削除する」
- 58 ページの「クライアントをグループに追加する」
- 60 ページの「クライアントを移動する」
- 61 ページの「グループの設定を複製する」
- 62 ページの「設定のインポートとエクスポートを実行する」

グループの概要

ビジネスセキュリティのグループとは、同じ設定を共有し同じタスクを実行するコンピュータとサーバの集合体を指します。クライアントをグループ化すると、複数のビジネスセキュリティクライアントが同時に設定され、管理されます。

管理を簡単にするために、所属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化します。また、感染リスクの高いクライアントをグループ化し、高いセキュリティ設定をグループ内のすべてのクライアントに適用します。

初期設定では、インストールされているビジネスセキュリティクライアントの種類に基づいて、ビジネスセキュリティサーバでクライアントをグループ（デスクトップまたはサーバ）に割り当てます。

グループ内のクライアントを表示する

手順: [セキュリティ設定] → グループを選択 → [設定の複製]

[セキュリティ設定] 画面で、ビジネスセキュリティクライアントをインストールしたすべてのクライアントを管理し、これらのセキュリティ設定をカスタマイズできます。

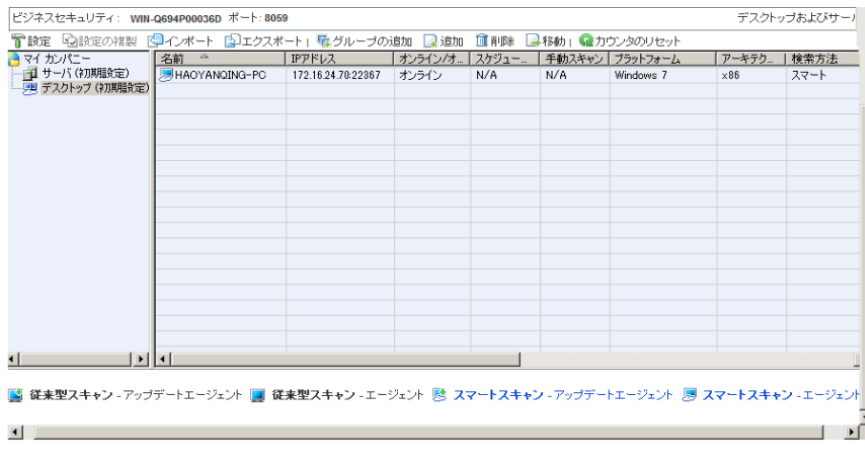


図 4-1. グループ内のクライアントを表示する [セキュリティ設定] 画面

クライアントは、セキュリティ設定のグループツリーの各グループに従って表示されます。セキュリティ設定のグループツリーとは、展開可能なクライアントの論理グループのリストです。

画面の左側からグループを選択して [設定] をクリックすると、管理コンソールに新しい設定領域が表示されます。

グループの追加

手順: [セキュリティ設定] → [グループの追加]

グループを作成して、複数のクライアントをまとめて管理します。

注意: クライアントは、グループに関連付けられている必要があります。クライアントをグループ外に配置することはできません。

セキュリティ設定 > グループの追加

グループの種類

追加するグループの種類を選択してください。

☐ デスクトップ

☒ サーバ

グループ名

新しいグループの名前を指定してください。

名前:

設定

既存グループから設定をインポートできます。インポート後に、利用状況にあわせて設定を変更できます。

☐ 次のグループから設定をインポートする

図 4-2. [グループの追加] 画面

グループを追加するには

- [グループの追加] 画面で、必要に応じて次の項目をアップデートします。
 - グループの種類: [デスクトップまたはサーバ] を選択します。
 - 次のグループから設定をインポートする: 選択したグループからセキュリティ設定をインポートします。
- [保存] をクリックします。

管理コンソールからグループとコンピュータを削除する

手順: [セキュリティ設定]→グループを選択

[削除] を使用すると、次の 2 つの目的を実現できます。

- **管理コンソールからの [クライアント] アイコンの削除**: 状況によっては、クライアントがオフラインになる場合があります。たとえば、コンピュータがフォーマットされたり、ユーザがビジネスセキュリティクライアントを長期間停止・無効にした場合があります。このような場合は、そのコンピュータのアイコンを管理コンソールから削除できます。
- **クライアントからのビジネスセキュリティクライアントのアンインストール** (これによって、[クライアント] アイコンが管理コンソールから削除されます): コンピュータやサーバにビジネスセキュリティクライアントがインストールされていれば、アクティブにして管理コンソールに表示できます。オフラインのクライアントを永久に削除するには、最初にビジネスセキュリティクライアントをアンインストールします。

管理コンソールから 1 つのコンピュータまたはグループを削除できます。

警告: ビジネスセキュリティクライアントをコンピュータから削除すると、ウイルスなどの不正プログラムにコンピュータが感染する危険性が高くなります。

クライアントまたはグループを削除するには

1. 削除対象となるグループまたはコンピュータをクリックします。
2. ツールバーの [削除] をクリックします。
3. [OK] をクリックします。

注意: クライアントがグループに登録されたままの場合、そのグループを削除することはできません。グループを削除する前に、ビジネスセキュリティクライアントを削除するかアンインストールしてください。

クライアントをグループに追加する

ビジネスセキュリティでは、いくつかの方法でビジネスセキュリティクライアントをインストールできます。ここでは、これらの方法の概要を紹介します。

ヒント： IT ポリシーを厳格に施行している組織では、リモートインストールとログオンスクリプトウィザードをお勧めします。

- **インストール用 Web ページ** — 社内のユーザに、インストール用 Web ページにアクセスしてビジネスセキュリティクライアントのセットアップファイルをダウンロードして、インストールするよう指示します。
- **ログオンスクリプトウィザード** — ウイルス対策が実施されていないコンピュータがドメインにログオンしたときに、これらのコンピュータにビジネスセキュリティクライアントが自動的にインストールされるようにします。
- **Client Packager** — ビジネスセキュリティクライアントのセットアップファイルやアップデートファイルを、メールや Exe (実行) ファイルを使用して、インストール先のコンピュータに送ります。
- **メール通知によるインストール** — インストーラへのリンクのあるメールメッセージを送信します。
- **リモートインストール** — 管理コンソールからビジネスセキュリティクライアントをすべての Windows Vista/2000/XP/Server 2003/Server 2008 クライアントにインストールします。
- **脆弱性検索ツール (TMVS)** — ビジネスセキュリティクライアントをすべての Windows Vista/2000/XP (Professional) /Server 2003/Server 2008 クライアントにインストールします。

デスクトップまたはサーバを追加すると、ビジネスセキュリティサーバではビジネスセキュリティクライアントがコンピュータにインストールされ、そのクライアントのアイコンが [セキュリティ設定] 画面に追加されます。ビジネスセキュリティクライアントがクライアントにインストールされると、ビジネスセキュリティサーバへのセキュリティ情報の報告が開始されます。

初期設定では、ビジネスセキュリティサーバで既存の Windows ドメインに基づいてグループが作成され、コンピュータ名に従って各クライアントが参照されます。ビジネスセキュリティサーバで作成したグループの削除、またはグループ間でのクライアントの移動が可能です。

クライアントをグループに追加するには

1. [セキュリティ設定] 画面で、ツールバーの [追加] をクリックします。
2. 必要に応じて次の項目をアップデートします。
 - **コンピュータの種類**: クライアントの種類です。
 - デスクトップまたはサーバ
 - **クライアントのインストール方法**

- ・ **リモートインストール**: クライアントコンピュータにビジネスセキュリティクライアントをリモートでインストールします。詳細については、45 ページの「リモートインストールを使用してインストールする」を参照してください。
 - ・ **ログオンスクリプトの作成**: ログオンスクリプトを使用して、ビジネスセキュリティクライアントをインストールします。次にクライアントコンピュータがネットワークにログオンすると、ビジネスセキュリティクライアントがインストールされています。詳細については、39 ページの「ログオンスクリプトウィザードを使用してインストールする」を参照してください。
3. [次へ] をクリックします。画面の指示に従います。

クライアントを移動する

手順: [セキュリティ設定] → グループを選択

ビジネスセキュリティには、グループ間またはビジネスセキュリティサーバ間でクライアントを移動するオプションが用意されています。

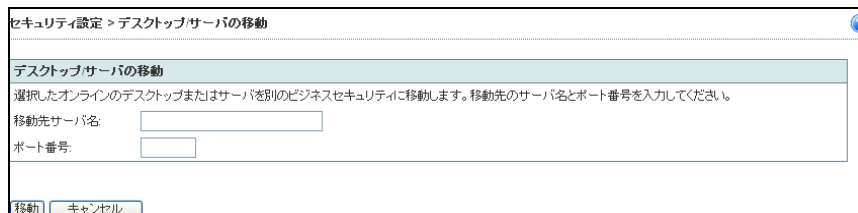


図 4-3. [デスクトップ/サーバの移動] 画面

クライアントをグループ間で移動するには

1. [セキュリティ設定] 画面でグループを選択し、次にクライアントを選択します。
2. そのクライアントを別のグループにドラッグします。クライアントは、新しいグループの設定を継承します。

クライアントをビジネスセキュリティサーバ間で移動するには

1. [セキュリティ設定] 画面でグループを選択し、次にクライアントを選択します。
2. [移動] をクリックします。
3. 新しいサーバ名とポート番号を入力します。サーバをクリックすると、ポート番号を [セキュリティ設定] 画面で取得できます (図 4-1. を参照)。ポート番号は上部に表示されます。

4. [移動] をクリックします。

グループの設定を複製する

[設定の複製] を使用して、設定を 1 つのグループから別のグループへコピーします。その設定は、複製先のグループに属するすべてのクライアントに適用されます。

手順: [セキュリティ設定] → グループを選択

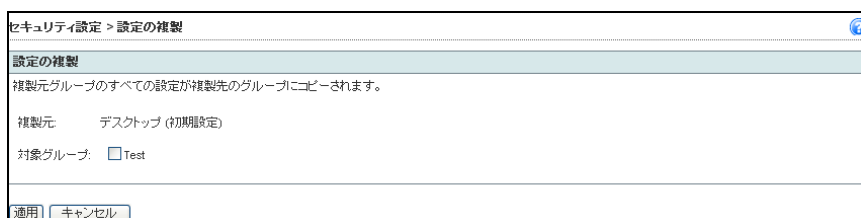


図 4-4. [設定の複製] 画面

グループ間で設定を複製するには

1. [セキュリティ設定] 画面で、グループの設定を別のグループに複製する必要がある、複製元のグループを選択します。
2. [設定の複製] をクリックします。
3. 複製元の設定を継承する必要がある複製先のグループを選択します。
4. [適用] をクリックします。

設定のインポートとエクスポートを実行する

デスクトップとサーバの設定を保存すると、後で新しいデスクトップやサーバ用に設定をインポートできます。設定はデータファイル (.dat) として保存されます。次の設定のインポートとエクスポートができます。

- セキュリティ設定：
ウイルス / スパイウェア対策、ファイアウォール設定、Web レピュテーション、URL フィルタ、挙動監視、TrendSecure ツールバー、メール検索、クライアントの権限、隔離
- 検索：
手動検索、予約検索

注意： 複数のデスクトップおよびサーバ間で、設定のインポートとエクスポートができます。設定はグループの種類に依存しません。

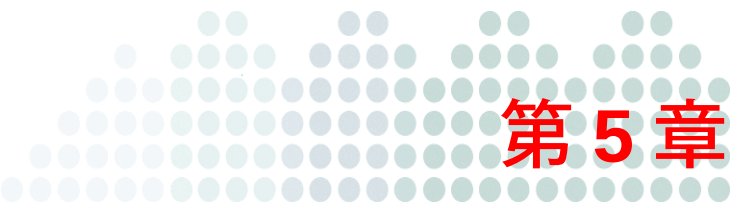
設定をインポートするには

1. [セキュリティ設定] 画面で、デスクトップまたはサーバを選択します。
2. [インポート] をクリックします。[設定のインポート] 画面が表示されます。
3. [参照] をクリックして、ファイルを検索し、[インポート] をクリックします。

設定をエクスポートするには

1. [セキュリティ設定] 画面で、デスクトップまたはサーバを選択します。
2. [エクスポート] をクリックします。[設定のエクスポート] 画面が表示されます。
3. [エクスポート] をクリックします。

Windows のダイアログボックスで [保存] をクリックして、場所を選択します。対象サーバが管理している 1 つまたは複数のドメインに設定をエクスポートするには、[設定の複製] を使用します。



第5章

基本的なセキュリティ設定の管理

本章では、ネットワークを保護するための設定方法について説明します。

本章で説明する内容には、次の項目が含まれます。

- 64 ページの「デスクトップ / サーバグループのオプション」
- 65 ページの「検索の種類」
- 66 ページの「リアルタイム検索を設定する」
- 68 ページの「ファイアウォールを管理する」
- 76 ページの「Web レピュテーションを使用する」
- 78 ページの「URL フィルタを設定する」
- 79 ページの「挙動監視を使用する」
- 84 ページの「Trend Secure」
- 85 ページの「POP3 メール検索を管理する」
- 86 ページの「クライアント権限」
- 89 ページの「隔離の設定を行う」

デスクトップ / サーバグループのオプション

Trend Micro ビジネスセキュリティ（以下、ビジネスセキュリティ）のグループとは、同一の設定内容で実行するクライアントの集まりです。クライアントをグループ化すると、複数のクライアントが同時に設定され、管理されます。詳細については、56 ページの「グループの概要」を参照してください。

[セキュリティ設定] 画面でグループを選択し、[設定] をクリックすると、次の項目にアクセスできます。

表 5-1. デスクトップ / サーバグループの設定オプション

オプション	説明	初期設定
検索方法	スマートスキャンと従来型スキャンを切り替えます。	従来型スキャン
ウイルス / スパイウェア対策	リアルタイム検索、ウイルス対策、スパイウェア対策に関するオプションを設定します。	有効 (リアルタイム検索)
ファイアウォール設定	ファイアウォールオプションを設定します。	無効
Web レピュテーション	オフィス内外の Web レピュテーションに関するオプションを設定します。	オフィス内：有効、低 オフィス外：有効、中
挙動監視	挙動監視オプションを設定します。	有効
URL フィルタ	URL フィルタによって、設定されているポリシーに違反する Web サイトがブロックされます。	有効
Trend Secure ツールバー	Trend プロテクトに関するオフィス内外のオプションを設定します。	オフィス内：無効 オフィス外：有効
メール検索	POP3 メールメッセージの検索を設定します。	無効
クライアント権限	クライアントのコンソールから各種設定にアクセスできるかどうかを設定します。	対応なし
隔離設定	隔離フォルダを指定します。	対応なし

注意： インスタントメッセージコンテンツフィルタなどの他のクライアント設定は、すべてのクライアントに適用されます。それらの設定には、[オプション設定] → [グローバル設定] 画面の [デスクトップ / サーバ] タブからアクセスできます。

検索の種類

ウイルス検索は、ビジネスセキュリティ戦略の中心的な部分です。検索中に、トレンドマイクロの検索エンジンは、ウイルスパターンファイルと連携し、パターンマッチングというプロセスを使用して検出の第 1 レベルを実行します。各ウイルスには一意の「シグニチャ」、つまり他のコードと区別できる特性を表す文字列が含まれているので、TrendLabs (トレンドラボ) のウイルス専門家は、このコードの実行機能を持たない断片をパターンファイルに取り込みます。検索エンジンは、各検索対象ファイルの特定領域をウイルスパターンファイルのパターンと比較し、一致するものを探します。

検索エンジンは、ウイルスなどの不正プログラムを含むファイルを検出すると、駆除、隔離、削除、テキスト / ファイルでの置換などの処理を実行します。これらの処理は、検索作業の設定時にカスタマイズできます。

ビジネスセキュリティには、インターネット上の脅威からクライアントを保護するための 3 種類の検索があります。

- **リアルタイム検索** — リアルタイム検索とは、永続的に継続して実行される検索です。リアルタイム検索は、ファイルが開かれたり、受信、ダウンロード、コピー、または変更されたりするたびに、ファイルを検索し脅威が含まれていないかどうかを確認します。
- **手動検索** — 手動検索とは、必要に応じて実行する検索です。手動検索では、ファイルから脅威を排除します。また、再感染の可能性を最小限にするために、以前の感染ファイルを根絶します。手動検索の間、ビジネスセキュリティクライアントは、管理者またはユーザが設定した処理に従って脅威を処理します。検索を停止するには、検索の進行中に [検索停止] をクリックします。

注意： 検索に要する時間は、クライアントのハードウェアリソースと検索するファイル数によって異なります。

- **予約検索** — 予約検索は手動検索と似ています。ただし、設定した時刻と頻度ですべてのファイルとメールメッセージを検索します。予約検索を使用することで、クライアントでの日常の検索を自動化し、脅威管理の効率を高めることができます。

予約検索を設定するには、[検索] → [予約検索] をクリックします。詳細については、「予約検索」を参照してください。

注意： 前述の検索の種類を検索方法と混同しないでください。検索方法は、スマートスキャンと従来型スキャンを指します (110 ページの「検索方法」)。

リアルタイム検索を設定する

手順: [セキュリティ設定] → グループを選択 → [設定] → [ウイルス / スパイウェア対策]

ウイルス / スパイウェア対策 

☒ リアルタイムのウイルス対策 / スパイウェア対策を有効にする

検索対象

処理

検索方法:

☐ すべての検索可能ファイル
☒ **トレンドマイクロの推奨設定** 実際のファイルタイプによる識別 
☐ 検索対象の拡張子の選択 (拡張子はそれぞれカンマで区切ってください)

検索条件:

☒ 作成、変更、または取得されるファイルを検索
☐ 取得されるファイルを検索
☐ 作成または変更されるファイルを検索

 検索除外

 詳細設定

 保存

図 5-1. [セキュリティ設定] → [ウイルス / スパイウェア対策] 画面

リアルタイム検索を設定するには

- [ウイルス / スパイウェア対策] 画面の [検索対象] タブで、必要に応じて次の項目をアップデートします。
 - リアルタイムのウイルス対策 / スパイウェア対策を有効にする
 - 検索方法
 - すべての検索可能ファイル** — 暗号化されたファイルやパスワードで保護されたファイルのみが除外されます。
 - トレンドマイクロの推奨設定** — 実際のファイルタイプに基づいてファイルを検索します。詳細については、192 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。
 - 検索対象の拡張子の選択** — ビジネスセキュリティは、選択した拡張子を持つファイルを検索します。拡張子が複数ある場合はカンマ (,) で区切ります。

- 検索条件
 - 作成、変更、または取得されるファイルを検索
 - 取得されるファイルを検索
 - 作成または変更されるファイルを検索
 - 検索除外: 特定のファイル、フォルダ、または特定の拡張子を持つファイルを検索対象から除外します。
 - 検索除外を有効にする
 - トレンドマイクロ製品がインストールされているフォルダを検索から除外する
 - 特定フォルダの検索除外 — 検索対象から除外するフォルダの名前を入力します。[追加] をクリックします。フォルダを削除するには、フォルダを選択して [削除] をクリックします。
 - 特定ファイルの検索除外 — 検索対象から除外するファイルの名前を入力します。[追加] をクリックします。ファイルを削除するには、ファイルを選択して [削除] をクリックします。
 - 特定の拡張子を持つファイルの検索除外 — 検索対象から除外する拡張子の名前を入力します。[追加] をクリックします。拡張子を削除するには、拡張子を選択して [削除] をクリックします。
 - 詳細設定
 - IntelliTrap を有効にする (ウイルス対策の場合) — IntelliTrap は、圧縮ファイル内のボットなどの不正なコードを検出します。詳細については、193 ページの「IntelliTrap」を参照してください。
 - ネットワークドライブおよび共有フォルダを検索する (ウイルス対策の場合)
 - システムのシャットダウン時にフロッピーディスクを検索する (ウイルス対策の場合)
 - 圧縮ファイルを検索する (ウイルス対策の場合) — 検索する階層の数を選択します。
 - スパイウェアの除外リストの変更 (ウイルス対策の場合) — このリストには、使用を許可するスパイウェア / グレーウェアプログラムの詳細が含まれます。リストをアップデートするには、リンクをクリックします。詳細については、115 ページの「スパイウェア / グレーウェアの除外リストを編集する」を参照してください。
2. [ウイルス / スパイウェア対策] 画面の [処理] タブで、ビジネスセキュリティが検出した脅威を処理する方法を指定します。
- ウイルス検出の場合
 - トレンドマイクロの推奨処理: 脅威に対して、トレンドマイクロが事前定義した処理を実行します。詳細については、192 ページの「トレンドマイクロの推奨処理」を参照してください。

- **すべての種類に同じ処理を使用**: 放置、削除、拡張子変更、隔離、または駆除のいずれかを選択します。駆除を選択した場合は、駆除できない脅威に対する処理も設定してください。
- **検索処理の指定**: 脅威の種類ごとに、放置、削除、拡張子変更、隔離、または駆除のいずれかを選択します。駆除を選択した場合は、駆除できない脅威に対する処理も設定してください。
- **ウイルス駆除実行前にバックアップを作成**: 感染したファイルの暗号化されたコピーを、クライアントの次のフォルダに保存します。

C:\Program Files\Trend Micro\Client Server Security Agent\Backup

- **スパイウェア検出の場合**
 - **駆除**: ビジネスセキュリティは、スパイウェア / グレーウェアを駆除するときに、関連するレジストリエントリ、ファイル、Cookie、およびショートカットを削除することがあります。スパイウェア / グレーウェアに関連するプロセスも終了されます。
 - **アクセス拒否**

警告: スパイウェア / グレーウェアのクライアントへのアクセスを拒否しても、感染したクライアントからスパイウェア / グレーウェアの脅威が削除されるわけではありません。

- **詳細設定**
 - **ウイルス / スパイウェアの検出時にデスクトップまたはサーバに警告メッセージを表示する**

3. [保存] をクリックします。

また、イベントの発生時に通知を受信するユーザも設定します。詳細については、121 ページの「通知イベントを設定する」を参照してください。

ファイアウォールを管理する

クライアントとネットワークの間に障壁を作成することにより、クライアントをハッカーの攻撃やネットワークウイルスから保護します。ファイアウォールを使用すると、特定の種類のネットワークトラフィックを拒否または許可できます。また、クライアントに対する攻撃が疑われるネットワークパケットのパターンを特定できます。

ビジネスセキュリティには、ファイアウォールの設定時に選択できる2つのオプションがあります。それらは、簡単モードと詳細モードです。簡単モードでは、推奨されている初期設定でファイアウォールを使用できます。詳細モードは、ファイアウォールの設定をカスタマイズするために使用します。

ヒント： ファイアウォールをインストールして有効化する前に、その他のファイアウォールソフトウェアをアンインストールすることをお勧めします。

ファイアウォールの簡単モードの初期設定

ファイアウォールの初期設定によって、クライアントのファイアウォールによる保護を開始するための基本的な設定が提供されます。初期設定は、インターネットにアクセスする必要性やFTPを使用したファイルのダウンロードまたはアップロードなど、クライアント上で生じる可能性のある一般的な状況に対応することを目的としています。

注意： ビジネスセキュリティの初期設定では、すべての新しいグループとクライアント上でファイアウォールは無効になっています。

表 5-2. ファイアウォールの初期設定

セキュリティレベル	説明
低	受信トラフィックと送信トラフィックが許可され、ネットワークウイルスだけがブロックされます。

設定	ステータス
侵入検知システム	無効
警告メッセージ (送信)	無効

除外設定名	処理	方向	プロトコル	ポート番号
DNS	許可	送受信	TCP/UDP	53
NetBIOS	許可	送受信	TCP/UDP	137、138、139、445
HTTPS	許可	送受信	TCP	443
HTTP	許可	送受信	TCP	80
Telnet	許可	送受信	TCP	23
SMTP	許可	送受信	TCP	25
FTP	許可	送受信	TCP	21
POP3	許可	送受信	TCP	110
MSA	許可	送受信	TCP	16732、16373

場所	ファイアウォールの設定
オフィス内	オフ
オフィス外	オフ

トラフィックのフィルタリング

ファイアウォールは、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を備えており、すべての送受信トラフィックを監視します。

- 方向（受信または送信）
- プロトコル（TCP/UDP/ICMP）
- 宛先ポート
- 宛先コンピュータ

ネットワークウイルスの検索

ファイアウォールでは、データパケットがネットワークウイルスに感染していないかが検査されます。

ステートフルインスペクション

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あり、トランザクションが有効であることを確認するため、クライアント上のすべての接続を監視します。ファイアウォールは、トランザクション内の特定の状況を識別し、どのトランザクションを追跡する必要があるかを予測して、通常の状態から逸脱した時点でそれを検出できます。したがって、フィルタリングを実行するかどうかは、プロファイルとポリシーだけでなく、接続の分析とすでにファイアウォールを通過したパケットのフィルタリングによって確立されたコンテキストにも基づいて決定されます。

侵入検知システム

ファイアウォールには、侵入検知システム（IDS）も含まれます。侵入検知システムは、クライアントへの攻撃の兆候があるネットワークパケットのパターンを特定するのに役立ちます。ファイアウォールを使用すると、次の既知の侵入を防止できます。

- **過大フラグメント**: これには、極端にサイズの大きい IP データグラムのフラグメントが含まれます。OS によっては、サイズの大きいフラグメントを適切に処理せず、例外としてスローしたり、他の望ましくない方法で取り扱ったりすることがあります。
- **Ping of Death**: Ping of Death（POD）は、不正な形式の ping またはその他の不正な ping をコンピュータに送信する、コンピュータに対する攻撃の一種です。ping のサイズは、通常は 64 バイトで、IP ヘッダを考慮した場合は 84 バイトです。コンピュータシステムの多くは、最大 IP パケットサイズの 65,535 バイトを超える ping は処理できません。このサイズの ping を送信すると、送信先のコンピュータがクラッシュすることがあります。
- **重複 ARP**: これは、送信元と宛先の IP アドレスが同一の場合に発生します。

- **SYN フラッド (SYN Flood):** SYN フラッドは、攻撃者がターゲットのシステムに SYN リクエストを連続して送りつけるサービス妨害攻撃の 1 つです。
- **オーバーラッピングフラグメント:** この場合、同一の IP データグラムに 2 つのフラグメントが含まれ、それらがデータグラム内で同じ位置を占めることを示すオフセットが付いています。これは、フラグメント A がフラグメント B によって完全に上書きされるか、フラグメント A が部分的にフラグメント B によって上書きされることを意味しています。OS によっては、重複しているフラグメントを適切に処理せず、例外としてスローしたり、他の望ましくない方法で取り扱ったりすることがあります。これは、ティアドロップサービス妨害攻撃の原因となります。
- **ティアドロップ攻撃:** ティアドロップ攻撃では、重複したサイズの大きいペイロードを持つ IP フラグメントがターゲットのコンピュータに送信されます。各種 OS の TCP/IP フラグメント再アセンブリコードのバグが原因で、フラグメントが不正に処理され、その結果システムがクラッシュすることがあります。
- **タイニーフラグメント攻撃:** 最終フラグメント以外のフラグメントが 400 バイト未満の場合は、そのフラグメントが意図的に作成された可能性があることを示しています。サイズの小さいフラグメントは、サービス妨害攻撃や、セキュリティ対策または検出を回避しようとする試行で使用されることがあります。
- **フラグメント化 IGMP:** クライアントがフラグメント化された IGMP (Internet Group Management Protocol) パケットを受信すると、クライアントのパフォーマンスが低下したり、コンピュータが応答しなくなったり (ハング) して、機能を回復するために再起動が必要となることがあります。
- **ランドアタック:** ランドアタックは、特殊で有害な偽装パケットをコンピュータに送りつけ、望まない動作を引き起こす DoS (サービス妨害) 攻撃の 1 つです。この攻撃では、送信元および宛先の両方として、ターゲットホストの IP アドレスとオープンポートを持つ偽装 TCP SYN パケット (接続の開始) を送信します。

ステートフルインスペクション

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あり、トランザクションが有効であることを確認するため、クライアント上のすべての接続を監視します。ファイアウォールは、トランザクション内の特定の状況を特定し、どのトランザクションを追跡する必要があるかを予測して、通常の状態から逸脱した時点でそれを検出できます。したがって、フィルタリングを実行するかどうかは、プロファイルとポリシーだけでなく、接続の分析とすでにファイアウォールを通過したパケットのフィルタリングによって確立されたコンテキストにも基づいて決定されます。

ファイアウォールを設定する

注意： オフィス内およびオフィス外に対してファイアウォールを設定します。[ロケーション認識]が無効な場合は、オフィス外の接続にオフィス内の設定が適用されます。

手順:[セキュリティ設定]→グループを選択→[設定]→[ファイアウォール設定]
→[オフィス内]/[オフィス外]

ファイアウォール - オフィス内

ロケーション認識が無効にされている場合、[オフィス内]設定は初期設定として動作します。
ロケーション認識の設定を確認してください。

☐ ファイアウォールを有効にする

☐ 簡単モード: トレンドマイクロの初期設定を使用

☒ 詳細モード: セキュリティレベル、IDS、通知、および除外を設定

セキュリティレベル

トラフィックのルールを選択してください (除外リストのポート以外に適用)。

☐ 高: すべての送受信トラフィックがブロック (拒否) されます。

☐ 中: 受信トラフィックがブロック (拒否) され、送信トラフィックが許可されます。

☒ 低: すべての送受信トラフィックが許可されます。

設定

☐ IDS (侵入検知システム) を有効にする

☐ 警告メッセージを有効にする

除外設定

除外設定を追加または編集します。

ID	名前	処理	方向	プロトコル	ポート/ポート範囲	コンピュータ
1	DNS	許可	送受信	TCP/UDP	指定: 53	すべて
2	NetBIOS	許可	送受信	TCP/UDP	指定: 137, 139	すべて

図 5-2. [ファイアウォール - オフィス内] 画面

ファイアウォールを設定するには

- [ファイアウォール] 画面で、必要に応じて次のオプションをアップデートします。
 - ファイアウォールを有効にする** — 選択すると、グループとロケーションに対してファイアウォールが有効になります。
 - 簡単モード** — ファイアウォールを初期設定で有効にします。詳細については、70 ページの「ファイアウォールの初期設定」を参照してください。
 - 詳細モード** — ファイアウォールをカスタム設定で有効にします。設定オプションについては、74 ページの「ファイアウォールの詳細オプション」を参照してください。

2. [保存] をクリックします。変更内容はすぐに反映されます。

ファイアウォールの詳細オプション

ファイアウォールの詳細オプションを使用して、クライアントの特定のグループに対してファイアウォールのカスタム設定を設定できます。

ファイアウォールの詳細オプションを設定するには

1. [ファイアウォール] 画面で、[詳細モード] を選択します。
2. 必要に応じて次のオプションをアップデートします。
 - **セキュリティレベル** — セキュリティレベルは、除外リストにないポートに適用されるトラフィックルールを制御します。
 - **高** — 受信トラフィックと送信トラフィックをブロックします。
 - **中** — 受信トラフィックをブロックし、送信トラフィックを許可します。
 - **低** — 受信トラフィックと送信トラフィックを許可します。
 - **設定**
 - **IDS (侵入検知システム) を有効にする** — 侵入検知システムが、攻撃すると疑われるネットワークパケットのパターンを特定します。詳細については、71 ページの「侵入検知システム」を参照してください。
 - **警告メッセージを有効にする** — ビジネスセキュリティが違反を検出すると、クライアントは通知を受け取ります。
 - **除外設定** — 除外リストに含まれるポートはブロックされません。詳細については、75 ページの「ファイアウォールの除外設定を操作する」を参照してください。
3. [保存] をクリックします。

ファイアウォールを無効にする

手順: [セキュリティ設定] → グループを選択 → [設定] → [ファイアウォール設定] → [オフィス内] [オフィス外]

ファイアウォールを無効にするには

1. 特定のグループおよび接続の種類についてファイアウォールを無効にするには、[ファイアウォールを有効にする] チェックボックスをオフにします。
2. [保存] をクリックします。

注意： ファイアウォールを完全に無効にするには、両方の種類の接続（オフィス内およびオフィス外）について上記のプロセスを繰り返します。

ファイアウォールの除外設定を操作する

除外設定は、各種トラフィックを方向、プロトコル、ポート、およびコンピュータに基づいて許可またはブロックする特定の設定から構成されています。

たとえば、大規模感染が発生したときに、HTTP ポート（80 番ポート）を含むすべてのクライアントトラフィックをブロックするように選択したとします。この場合でも、ブロック設定を適用したクライアントに対してインターネットへのアクセスを許可したい場合は、除外リストにその Web プロキシサーバを追加できます。

除外設定を追加する

除外設定を追加するには

1. [ファイアウォール — オフィス内（またはオフィス外）] 画面で [詳細モード] をクリックし、[除外設定] セクションで、[追加] をクリックします。
2. 必要に応じて次のオプションをアップデートします。
 - **名前：**除外対象の一意の名前を指定します。
 - **処理：**選択したプロトコル、ポート、およびクライアントのトラフィックをブロックする場合は [ネットワークトラフィックを拒否]、許可する場合は [ネットワークトラフィックを許可] を選択します。
 - **方向：**「受信」は、インターネットからネットワークへ流れるトラフィックを指しています。「送信」は、ネットワークからインターネットへ流れるトラフィックを指しています。
 - **プロトコル：**除外対象とするネットワークトラフィックプロトコル。
 - **ポート**
 - **すべてのポート**（初期設定）
 - **範囲**
 - **指定ポート** — 個々のエントリはカンマ（,）で区切ります。
 - **コンピュータ**
 - **すべての IP アドレス**（初期設定）
 - **IP 範囲**
 - **単一 IP** — 特定のクライアントの IP アドレス。

3. [保存] をクリックします。[ファイアウォール — オフィス内 (またはオフィス外)] 画面で、除外リスト内に新しい除外設定が表示されます。

除外設定を編集する

除外設定を編集するには

1. [ファイアウォール設定 — 詳細モード] 画面の [除外設定] セクションで、編集する除外設定を選択します。
2. [編集] をクリックします。
3. 必要に応じて次のオプションをアップデートします。詳細については、75 ページの「除外設定を追加する」を参照してください。
4. [保存] をクリックします。

除外設定を削除する

除外設定を削除するには

1. [ファイアウォール設定 — 詳細モード] 画面の [除外設定] セクションで、削除する除外設定を選択します。
2. [削除] をクリックします。

Web レピュテーションを使用する

Web レピュテーションでは、要求された URL についてトレンドマイクロ Web セキュリティデータベースに照会することで、セキュリティリスクの危険性のある URL へのアクセスを防止します。クライアントの場所 (オフィス内 / オフィス外) に応じて、異なるレベルのセキュリティを設定します。

Web レピュテーションが URL をブロックしても、その URL が安全であると判断した場合は、承認済み URL リストにその URL を追加します。承認済み URL リストに URL を追加する方法の詳細については、132 ページの「Web レピュテーションと承認済み URL」を参照してください。

Web レピュテーションを設定する

手順: [セキュリティ設定] → グループを選択 → [設定] → [Web レピュテーション] → [オフィス内] [オフィス外]

Web レピュテーションは、HTTP リクエストごとにトレンドマイクロのセキュリティデータベースにクエリを実行し、要求された各 URL のセキュリティリスクを評価します。

注意: オフィス内およびオフィス外に対して Web レピュテーションの設定を行います。[ロケーション認識] が無効な場合は、オフィス外の接続にオフィス内の設定が適用されます。

Webレピュテーション - オフィス内

[ロケーション認識] が無効になっている場合、[オフィス内設定] が初期設定で動作します。
ロケーション認識の設定を確認してください。

☒ Webレピュテーションを有効にする

セキュリティレベル

☐ 高 ブロックするページは次のとおりです。

- 詐欺サイトや脅威の送信元と確認されたページ
- 詐欺サイトや脅威の送信元の疑いのあるページ
- スпамメールに関連付けられたページや危険にさらされる可能性のあるページ
- 評価のないページ

☐ 中 ブロックするページは次のとおりです。

- 詐欺サイトや脅威の送信元と確認されたページ
- 詐欺サイトや脅威の送信元の疑いのあるページ

☒ 低 ブロックするページは次のとおりです。

- 詐欺サイトや脅威の送信元と確認されたページ

[グローバル承認済みURL](#)

図 5-3. [セキュリティ設定] → [Web レピュテーション] 画面

Web レピュテーション設定を編集するには

1. [Web レピュテーション] 画面で、必要に応じて次の項目の設定を変更します。

- Web レピュテーションを有効にする
- セキュリティレベル
 - 高 — 詐欺サイトや脅威の送信元と確認されたページ、詐欺サイトや脅威の送信元の疑いがあるページ、スパムメールに関連付けられたページや危険にさらされる可能性のあるページ、および評価のないページをブロックします。
 - 中 — 詐欺サイトや脅威の送信元と確認されたページ、および詐欺サイトや脅威の送信元の疑いがあるページをブロックします。
 - 低 — 詐欺サイトや脅威の送信元と確認されたページをブロックします。

- 承認済み Web サイトのリストを変更するには、[グローバル承認済み URL] をクリックして、[グローバル設定] 画面で設定を変更します。
- [保存] をクリックします。

URL フィルタを設定する

手順: [セキュリティ設定] → グループを選択 → [設定] → [URL フィルタ]

URL フィルタを使用すると、インターネットからの不要なコンテンツをブロックできます。[カスタム] を選択すると、1 日のさまざまな時間帯でブロックする特定の種類の Web サイトを選択できます。また、1 日のさまざまな時間帯で Web サイトをブロックする業務時間と業務時間外を定義できます。

URL フィルタ ?

URL フィルタでは、トレンドマイクロのサーバでコンテンツカテゴリを使用することにより Web ページが検査されます。1 日のさまざまな時間帯でブロックする特定の種類の Web サイトを選択する[カスタム]を選択して、次のテーブルを設定します。

☒ URL フィルタを有効にする

フィルタ強度	
☐ 高	既知のまたは潜在的なセキュリティ上の脅威、不適切なコンテンツまたは攻撃的な可能性のあるコンテンツ、生産性または帯域幅に影響を与える可能性のあるコンテンツ、および未評価のページをブロックします。
☐ 中	既知のセキュリティ上の脅威および不適切なコンテンツをブロックします。
☒ 低	既知のセキュリティ上の脅威をブロックします。
☐ カスタム	ブロックする特定のページカテゴリを選択します。

フィルタルール		
URL カテゴリ	☐ 業務時間	☐ 業務時間外
☒ 成人向け	☐	☐
☒ ビジネス	☐	☐

図 5-4. [セキュリティ設定] → [URL フィルタ] 画面

URL フィルタを設定するには

- [URL フィルタ] 画面で、必要に応じて次の項目の設定を変更します。
 - URL フィルタを有効にする
 - フィルタ強度
 - 高 — 既知のまたは潜在的なセキュリティ上の脅威、不適切なコンテンツまたは攻撃的な可能性のあるコンテンツ、生産性または帯域幅に影響を与える可能性のあるコンテンツ、および評価のないページをブロックします。

- ・ **中** — 既知のセキュリティ上の脅威および不適切なコンテンツをブロックします。
 - ・ **低** — 既知のセキュリティ上の脅威をブロックします。
 - ・ **カスタム** — 独自のカテゴリを選択し、業務時間または業務時間外にそれらのカテゴリをブロックするかどうかを指定します。
2. [業務時間] を定義します。
 3. 承認済み Web サイトのリストを変更するには、[グローバル承認済み URL] をクリックして、[グローバル設定] 画面で設定を変更します。
 4. [保存] をクリックします。

挙動監視を使用する

ビジネスセキュリティクライアントは常にクライアントを監視し、OS やインストール済みのソフトウェアに異常な変更が加えられていないかどうかを確認します。管理者またはユーザは、監視対象の変更違反する場合に特定のプログラムを起動できるように除外リストを作成するか、または特定のプログラムを完全にブロックすることができます。また、有効なデジタル署名を持つプログラムは常に起動が許可されます。

監視対象の変更の説明と初期設定については、次の表を参照してください。

表 5-3. 監視対象と考えられる変更

監視対象の変更	説明	初期設定値
システムファイルの複製	多くの不正プログラムは、Windows システムファイルが使用しているファイル名を使って、自分自身または他の不正プログラムのコピーを作成します。これは、通常、システムファイルの上書きまたは置換、検出の回避、またはユーザによる不正ファイルの削除を阻止する目的で実行されます。	必要に応じて問い合わせ
Hosts ファイルの変更	Hosts ファイルは、ドメイン名と IP アドレスを比較し、一致しているかどうかを確認します。不正プログラムの多くは、感染した Web サイト、存在しない Web サイト、または偽の Web サイトに Web ブラウザをリダイレクトするように Hosts ファイルを変更します。	常にブロック
不審な挙動	不審な挙動とは、正規プログラムではほとんど実行されることがない特定の処理または一連の処理です。疑わしい挙動を示すプログラムは、注意して使用する必要があります。	常に許可

表 5-3. 監視対象と考えられる変更 (続き)

監視対象の変更	説明	初期設定値
システムファイルの変更	特定の Windows システムファイルは、スタートアッププログラムやスクリーンセーバの設定を含む、システムの挙動を決定します。多くの不正プログラムは、システムファイルを変更することで、スタートアップ時に自動的に起動し、システムの挙動を制御できるようにします。	常にブロック
Internet Explorer プラグインの追加	スパイウェア / グレーウェアは、多くの場合、ツールバーやブラウザヘルパーオブジェクトを含む不要な Internet Explorer プラグインをインストールします。	必要に応じて問い合わせ
Internet Explorer 設定の変更	多くのウイルス / 不正プログラムは、ホームページ、信頼する Web サイト、プロキシサーバの設定、メニュー拡張などの Internet Explorer の設定を変更します。	常にブロック
セキュリティポリシー設定の変更	Windows セキュリティポリシーを変更して、不要なアプリケーションを実行し、システム設定を変更させる場合があります。	常にブロック
ファイアウォールポリシー設定の変更	Windows ファイアウォールポリシーは、ネットワークにアクセス可能なアプリケーション、通信用に開くポート、コンピュータと通信可能な IP アドレスを決定します。多くの不正プログラムは、このポリシーを変更して、自身がネットワークとインターネットへアクセスできるようにします。	必要に応じて問い合わせ
DLL (プログラムライブラリ) インジェクション	不正プログラムの多くは、すべてのアプリケーションがプログラムライブラリ (DLL) を自動的にロードするように、Windows を設定します。これにより、アプリケーションが起動するたびに、DLL 内の不正なルーチンが実行されるようになります。	必要に応じて問い合わせ
シェル設定の変更	多くの不正プログラムは、Windows シェルの設定を変更し、それらを特定のファイルタイプに関連付けます。ユーザが Windows エクスプローラで関連付けられたファイルを開くと、このルーチンによって不正プログラムが自動的に起動します。不正プログラムは、Windows シェルの設定を変更することで、使用されているプログラムの追跡を可能にしたり、正規のアプリケーションと一緒に自身を起動できるようにしたりします。	必要に応じて問い合わせ

表 5-3. 監視対象と考えられる変更（続き）

監視対象の変更	説明	初期設定値
サービスの追加	Windows サービスは、特殊な機能を持ち、通常は、フル管理アクセス権でバックグラウンドで継続して実行されるプロセスです。不正プログラムは、自身をサービスとしてインストールし、隠れた状態のままでいることがあります。	必要に応じて問い合わせ
システムプロセスの変更	不正プログラムの多くは、ビルトインの Windows プロセスに対してさまざまな処理を実行します。これらの処理には、実行されているプロセスの強制終了や変更が含まれます。	常に許可
スタートアッププログラムの追加	不正プログラムの多くは、すべてのアプリケーションがプログラムライブラリ (DLL) を自動的にロードするように、Windows を設定します。これにより、アプリケーションが起動するたびに、DLL 内の不正なルーチンが実行されるようになります。	必要に応じて問い合わせ

挙動監視のもう 1 つの機能は、EXE および DLL ファイルが削除または変更されないよう保護することです。この権限を持つユーザは、保護するフォルダを指定できます。

挙動監視を設定する

手順: [セキュリティ設定] → グループを選択 → [設定] → [挙動監視]

挙動監視は、OS、レジストリエントリ、他のソフトウェア、またはファイルとフォルダが不正に変更されないようにクライアントを保護します。

挙動監視

☐ 挙動監視を有効にする

監視対象と考えられる変更	処理	詳細
☒ システムファイルの複製	必要に応じて問い合わせ	さまざまな不正プログラムに利用される手法で、Windowsのシステムファイル名を使用して、自身または他のプログラムのコピーを作成することがあります。システムファイルと置き換えることで、検出されないようしたり、ユーザーによって削除されないようにするためです。
☒ Hostsファイルの変更	常にブロック	
☒ 不審な挙動	常に許可	
☒ システムファイルの変更	常にブロック	
☒ Internet Explorerプラグインの追加	必要に応じて問い合わせ	
☒ Internet Explorer設定の変更	常にブロック	
☒ セキュリティポリシー設定の変更	常にブロック	
☒ ファイアウォールポリシー設定の変更	必要に応じて問い合わせ	
☒ DLL (プログラムライブラリ) インジェクション	必要に応じて問い合わせ	
☒ シェル設定の変更	必要に応じて問い合わせ	
☒ サービスの追加	必要に応じて問い合わせ	
☒ システムプロセスの変更	常に許可	
☒ スタートアッププログラムの追加	必要に応じて問い合わせ	

除外設定

プログラムのフルパスを指定し、それを [承認済みプログラム] リストまたは [ブロックするプログラム] リストに追加します。[承認済みプログラム] リスト内のプログラムは起動できますが、[ブロックするプログラム] リスト内のプログラムは起動できません。

プログラムのフルパスを入力してください
例: C:\Program Files\MSN Messenger\MSVS.exe (項目はセミコロンで区切ってください)

図 5-5. [挙動監視] 画面

挙動監視の設定を編集するには

1. [挙動監視] 画面で、必要に応じて次の項目の設定を変更します。

- **挙動監視を有効にする**

注意： [セキュリティ設定] →グループを選択→ [設定] → [クライアント権限] をクリックし、[挙動監視] セクションで [挙動監視タブを表示し、ユーザーによるリストのカスタマイズを許可する] を選択します。

- **監視対象と考えられる変更** — 監視対象の変更ごとに、[常に許可]、[必要に応じて問い合わせ]、または [常にブロック] を選択します。さまざまな変更の詳細については、79 ページの表 5-3 を参照してください。
- **除外設定** — 除外設定には、承認済みプログラムリストとブロックするプログラムリストが含まれます。承認済みプログラムリスト内のプログラムは、監視対象の変更には違反する場合でも起動できます。一方、ブロックするプログラムリスト内のプログラムはいかなる場合でも起動することはできません。

- **プログラムのフルパスを入力してください**: プログラムのフルパスを入力します。複数のエントリはセミコロン (;) で区切ります。[承認済みリストに追加] または [ブロックするリストに追加] をクリックします。必要に応じて、環境変数を使用してパスを指定します。サポートされる変数のリストについては、83 ページの表 5-4 を参照してください。
- **承認済みプログラムリスト**: このリスト内のプログラム (最大 100 個) は起動できます。エントリを削除するには、対応する  アイコンをクリックします。
- **ブロックするプログラムリスト**: このリスト内のプログラム (最大 100 個) は起動できません。エントリを削除するには、対応する  アイコンをクリックします。

2. [保存] をクリックします。

環境変数

ビジネスセキュリティでは、環境変数を使用してクライアント上の特定のフォルダを指定できます。これらの変数を使用して、特定のフォルダの除外設定を作成できます。次の表に、使用可能な変数を示します。

表 5-4. サポートされる変数

環境変数	指定されるフォルダ
\$windir\$	Windows フォルダ
\$rootdir\$	ルートフォルダ
\$tempdir\$	Windows 一時フォルダ
\$programdir\$	Program Files フォルダ

Trend Secure

Trend Secure は、ブラウザベースのツール (Trend プロテクト) で構成されており、それによってユーザは安全に Web を閲覧できます。

ブラウザには、ワイヤレス接続の安全性に応じて色が変わるツールバーが追加されます。

注意： オフィス内およびオフィス外に対して Trend Secure 設定を設定します。[ロケーション認識] が無効な場合は、オフィス外の接続にオフィス内の設定が適用されます。

Trend Secure を設定する

手順: [セキュリティ設定] → グループを選択 → [設定] → [Trend Secure ツールバー] → [オフィス内] [オフィス外]

ユーザのロケーションに応じて Trend Secure ツールを使用できるかどうかを設定します。



図 5-6. [Trend Secure ツールバー - オフィス内] 画面

Trend Secure ツールの使用可能性を編集するには

1. [Trend Secure ツールバー - オフィス内] / [Trend Secure ツールバー - オフィス外] 画面で、必要に応じて次の項目の設定を変更します。
 - ・ ページレイティングの有効化 — 現在のページの安全性を判断します。
2. [保存] をクリックします。

注意： Trend Secure ツールバーは、管理コンソールからのみビジネスセキュリティクライアントに対して使用可能にすることができます。ユーザはビジネスセキュリティクライアントのコンソールからツールをインストールまたはアンインストールする必要があります。

POP3 メール検索を管理する

POP3 メール検索とトレンドマイクロ迷惑メール対策ツールバープラグインは、POP3 メールメッセージによってもたらされるセキュリティリスクやスパムメールに対して、クライアントをリアルタイムに保護します。

注意： 初期設定では、POP3 メール検索は、110 番ポートを介して送信された新規メッセージで受信ボックスと迷惑メールフォルダにあるメッセージのみを検索できます。Exchange Server 2007 の初期設定で使用されているセキュア POP3 (SSL-POP3) はサポートされていません。

注意： POP3 メール検索では、IMAP 方式を使った受信におけるセキュリティリスクおよびスパムメールは検出できません。

メール検索を設定する

手順： [セキュリティ設定] → グループを選択 → [設定] → [メール検索]

メール検索の使用可能性を編集するには

1. [メール検索] 画面で、必要に応じて次の項目をアップデートします。
 - ・ POP3 メールのリアルタイム検索を有効にする
 - ・トレンドマイクロ 迷惑メール対策ツールバーを有効にする

2. [保存] をクリックします。

クライアント権限

手順: [セキュリティ設定] → グループを選択 → [設定] → [クライアント権限]

クライアント権限を許可すると、ユーザはコンピュータにインストールされているビジネスセキュリティクライアントの設定を変更できるようになります。

ヒント: 組織全体に統制されたセキュリティポリシーを適用するには、ユーザには限定的な権限のみ与えることをお勧めします。これによって、ユーザが検索設定を変更したり、ビジネスセキュリティクライアントをアンロードしたりするのを防ぐことができます。

クライアント権限を設定する

クライアント権限

次の設定を変更する権限をクライアントに与えます。

ウイルススバイウェア対策

- ☐ 手動検索の設定
- ☐ 予約検索の停止
- ☐ 予約検索の設定
- ☐ スタンドアロンモードの有効化
- ☐ リアルタイム検索の設定

ファイアウォール設定

- ☐ ファイアウォールタブの表示
- ☐ クライアントによるファイアウォールの有効化/無効化を許可

Webレディケーション

- ☐ 承認済みURLリストの編集

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
- ☒ 自動アップデートを有効にする
- ☐ プログラムのアップグレードとHotfixの配信を無効にする
(このチェックボックスをオンにすると、次のプログラムアップグレードからプログラムのアップグレードが禁止されます)

クライアントのセキュリティ

- ☐ 高: ビジネスセキュリティクライアントのファイルとレジストリへのアクセス権限が制限されます。
- ☒ 通常: ビジネスセキュリティクライアントのファイルとレジストリへの通常のアクセス権限が保持されます。

保存

図 5-7. [クライアント権限] 画面

クライアントに権限を与えるには

1. [クライアント権限] 画面で、必要に応じて次の項目をアップデートします。

- **ウイルス / スパイウェア対策**
 - 手動検索の設定
 - 予約検索の設定
 - リアルタイム検索の設定
 - 予約検索の停止
 - スタンドアロンモードの有効化
- **ファイアウォール設定**
 - ファイアウォールタブの表示
 - クライアントによるファイアウォールの有効化 / 無効化を許可

注意： ユーザがファイアウォールを有効化 / 無効化するのを許可した場合、管理コンソールではこれらの設定を変更できません。ユーザにこの権限を与えない場合は、管理コンソールでこれらの設定を変更できます。ビジネスセキュリティクライアントの [ローカルファイアウォール設定] の情報には、管理コンソールではなく、ビジネスセキュリティクライアントで構成された設定が反映されます。

- **Web レピュテーション**
 - 承認済み URL リストの編集
- **挙動監視**
 - 挙動監視タブを表示し、ユーザによるリストのカスタマイズを許可する : ユーザによる挙動監視の有効化 / 無効化、および除外設定リストの設定を許可します。
- **メール検索**
 - ユーザによるリアルタイム POP3 メール検索の設定を許可する
- **プロキシ設定**
 - ユーザによるプロキシ設定を許可する
- **アップデート権限**
 - 手動アップデートを実行する
 - 自動アップデートを有効 / 無効にする
- **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 — ユーザがアップデートを開始すると、ビジネスセキュリティクライアントは、[アップデート元] 画面で指定したアップデート元から最新ファイルを取得します。アップデートに失敗した場合は、ビジネスセキュリティサーバからのアップデートを試みます。[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] をオンにすると、クライアントは、ビジネスセキュリティサーバからのアップデートに失敗した場合に、トレンドマイクロのアップデートサーバからのアップデートを試みます。

ヒント： オフィス外のポータブルクライアント上のビジネスセキュリティクライアントが確実にアップデートされるようにするには、[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] をオンにしてください。

- ・ 自動アップデートを有効にする
- ・ プログラムのアップグレードと HotFix のインストールを無効にする
- ・ **クライアントのセキュリティ**
 - ・ 高
 - ・ クライアントのレジストリキーとクライアントのインストールフォルダへの書き込みアクセスを禁止します。
 - ・ クライアントのプロセスとサービスが停止しないようにします。
 - ・ 通常 — ビジネスセキュリティクライアントのフォルダ、ファイル、およびレジストリエントリへの読み取り / 書き込みアクセスを許可します。

注意： [高] を選択した場合は、ビジネスセキュリティクライアントのフォルダ、ファイル、およびレジストリエントリのアクセス権限設定が Program Files フォルダ (Windows 2000/XP/Vista/Server 2003 を実行しているクライアントの場合) から継承されます。そのため、Windows ファイルまたは 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に設定されている場合は、[高] を選択しても、クライアントにビジネスセキュリティクライアントのフォルダ、ファイル、およびレジストリエントリへの完全な読み取り / 書き込みアクセスが許可されます。

2. [保存] をクリックします。

隔離の設定を行う

隔離フォルダは、感染したファイルを格納します。隔離フォルダは、クライアント自身または別のサーバに配置できます。無効な隔離フォルダを指定した場合、ビジネスセキュリティクライアントは、次のクライアント上の初期設定の隔離フォルダを使用します。

`C:\Program Files\Trend Micro\Client Server Security Agent\SUSPECT`

サーバの初期設定のフォルダは、以下のとおりです。

`C:\Program Files\Trend Micro\Security Server\PCCSRV\Virus`

注意： ネットワーク接続に問題があるなど、何らかの理由でビジネスセキュリティクライアントがビジネスセキュリティサーバにファイルを送信できない場合、ファイルはクライアントの隔離フォルダに残されます。ビジネスセキュリティクライアントは、ビジネスセキュリティサーバに再び接続されたときに、ファイルの再送信を試みます。

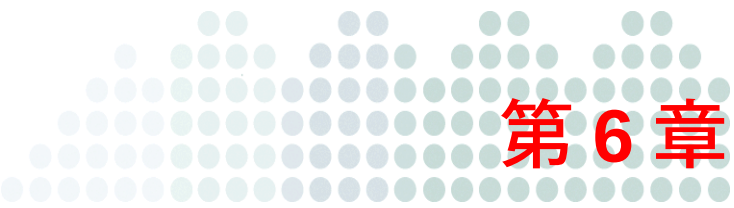
隔離ディレクトリを設定する

手順: [セキュリティ設定] → グループを選択 → [設定] → [隔離設定]

図 5-8. [隔離ディレクトリ設定] 画面

隔離ディレクトリを設定するには

1. [隔離ディレクトリ設定] 画面で、必要に応じて次の項目の設定を変更します。
 - ・ 隔離ディレクトリ: 感染ファイルを保存する URL または UNC パスを入力します。たとえば、`http://www.example.com/quarantine` または `\\TempServer\Quarantine`などを指定します。
2. [保存] をクリックします。



第6章

大規模感染予防の使用

本章では、大規模感染予防の概念と設定方法について説明し、大規模感染予防を使用してネットワークおよびクライアントを保護する方法を示します。

本章で説明する内容には、次の項目が含まれます。

- 92 ページの「大規模感染予防」
- 93 ページの「大規模感染予防の現在のステータス」
- 99 ページの「診断 / クリーンナップ」
- 101 ページの「大規模感染予防を設定する」
- 106 ページの「脆弱性診断設定を設定する」

大規模感染予防

大規模感染予防は、Trend Micro ビジネスセキュリティ（以下、ビジネスセキュリティ）ソリューションの重要なコンポーネントであり、世界的な大規模感染の発生時にビジネスを保護します。

大規模感染予防は、インターネット全体の大規模感染にライフサイクルがあるという考え方に基づいています。大規模感染のライフサイクルには、「脅威の予防」、「脅威からの保護」、および「脅威のクリーンナップ」の3段階があります。トレンドマイクロでは、大規模感染予防と呼ばれる予防戦略で、ライフサイクルの各段階を阻止します。

表 6-1. 大規模感染ライフサイクルの各段階に対応する大規模感染予防

大規模感染の段階	大規模感染予防の段階
大規模感染ライフサイクルの第1段階では、トレンドマイクロの専門家がインターネット上で活発に流布している脅威を監視します。この時点では、脅威に対する既知のソリューションはありません。	脅威の予防 大規模感染予防は、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た大規模感染ポリシーに従って処理することで、脅威によるコンピュータやネットワークへの攻撃を阻止します。これらの処理には、警告の送信、ポートのブロック、フォルダおよびファイルへのアクセスの拒否などが含まれます。
大規模感染の第2段階では、脅威の影響を受けたコンピュータが他のコンピュータに脅威を感染させます。脅威はローカルネットワーク内で急速に広がり、ビジネスの中断やコンピュータの損傷を引き起こします。	保護 大規模感染予防は、リスクのあるコンピュータに最新のコンポーネントと Patch をダウンロードするように通知することで、それらのコンピュータを保護します。
大規模感染の第3段階では、報告される件数が減り脅威は鎮まります。	クリーンナップ 大規模感染予防は、クリーンナップサービスを実行してダメージを修復します。その他の検索機能は、管理者が将来の脅威に備えるために使用できる情報を提供します。

大規模感染予防の処理

大規模感染予防は、大規模感染のライフサイクルの各段階で大規模感染を制御できるように設計されました。自動対応は、通常、大規模感染予防ポリシーに基づき、次の予防的な手順を実行します。

- 共有フォルダをブロックして、共有フォルダ内のファイルにウイルス / 不正プログラムが感染しないようにします。
- ポートをブロックし、ウイルス / 不正プログラムが脆弱なポートを利用してネットワークやクライアントに感染を広げるのを防ぎます。

注意： 大規模感染予防は、ビジネスセキュリティサーバがクライアントとの通信に使用しているポートをブロックしません。

- ファイルおよびフォルダへの書き込みアクセスを禁止して、ファイルがウイルス / 不正プログラムによって変更されないようにします。
- ネットワーク上のクライアントに、現在の大規模感染の影響を受けやすい脆弱性があるかどうかを診断します。
- ウイルスパターンファイルやウイルスクリーンアップエンジンなどの最新のコンポーネントを配信します。
- 大規模感染の影響を受けたすべてのクライアントで、クリーンアップを実行します。
- 有効な場合は、クライアントとネットワークを検索し、検出された脅威に対して処理を実行します。

大規模感染予防の現在のステータス

手順：[大規模感染予防] → [現在のステータス]

管理コンソールの [現在のステータス] 画面で、世界的なウイルス / 不正プログラムの大規模感染の脅威が表示および追跡されます。ステータスは、おおよそ大規模感染のライフサイクルに対応しています。

大規模感染時には、大規模感染予防が大規模感染予防を使用して、コンピュータとネットワークを保護します。段階ごとに、[現在のステータス] ページの情報が更新されます。大規模感染予防の 3 段階：

1. 予防
2. 保護
3. クリーンアップ

大規模感染予防 > 現在のステータス

予防

保護

クリーンナップ

Trend Microビジネスセキュリティでは、ウイルス大規模感染に対するポリシーを自動的に配信することができます。ウイルス不正プログラムに関する詳細情報および必要な処理を以下で確認できます。システムが自動的に処理を実行できない場合、その情報または脆弱なコンピュータとクリーンナップが必要なコンピュータに表示されます。

前回のアップデート: 2008/06/17 15:26:31 | 表示更新

予防

レッドアラート有効

現在、BICAR_TEST_FILEによる感染がインターネット上で拡大しています。トレンドマイクロでは、このウイルス不正プログラムからお使いのネットワークを保護するための対策を、すでに実施しています。新しいコンポーネントがまもなく公開されます。このウイルス不正プログラムに関する情報は、以下をお読みください。

ウイルス不正プログラムの情報					
ウイルス不正プログラム名	アラートの種類	危険度	感染経路	利用される脆弱性	自動対応
BICAR_TEST_FILE	レッドアラート	高	Email, Exploit, Shared Drives		無効
開始日時		終了日時		自動対応の詳細	
2008/06/17 15:26:24		2008/06/19 15:26:24		N/A	
dddddddddddddddddddd					

ネットワーク上のアラートステータス

オンラインコンピュータのアラートステータス

コンピュータの種類	有効	無効
デスクトップサーバ	N/A	N/A

図 6-1. [大規模感染予防] 画面-脅威なし

脅威の予防

[現在のステータス] 画面の脅威の予防段階では、最近の脅威、アラートが有効になっているクライアント、および現在の脅威に対して脆弱なクライアントに関する情報が表示されます。

大規模感染予防 > 現在のステータス



Trend Microビジネスセキュリティでは、ウイルス大規模感染に対するポリシーを自動的に配信することができます。ウイルス不正プログラムに関する詳細情報および必要な処理を以下で確認できます。システムが自動的に処理を実行できない場合、その情報は [脆弱なコンピュータ] と [クリーンナップが必要なコンピュータ] に表示されます。
 前回のアップデート: 2005/09/02 19:35:34 | [表示更新](#)

コ 予防 **レッドアラート有効**

現在、TEST_MALWARE.AIによる感染がインターネット上で拡大しています。トレンドマイクロでは、このウイルス不正プログラムからお使いのネットワークを保護するための対策を、すでに実施しています。新しいコンポーネントがまもなく公開されます。このウイルス不正プログラムに関する情報は、以下をお読みください。

ウイルス不正プログラム名	アラートの種類	危険度	感染経路	利用される脆弱性	自動対応
TEST_MALWARE.AI	レッドアラート	中	Share, Email	MS05-036	無効
開始日時		終了日時		自動対応の詳細	
2005/09/02 18:48:55		2005/09/04 18:48:55		表示	

*** Testing No.300 *** From CSM QA,this message will show on thread info. Using VA pattern version 1. Require Virus Pattern. Testing for TEST_MALWARE.AI with a fake ID MS05-036 (modified, for testing). Need TMVAINFO.xml to create a fake to support and using special tsc.exe, tsc.pth

ネットワークのアラートステータス

オンラインコンピュータのアラートステータス

コンピュータの種類	有効	無効
デスクトップサーバ	1	2

TEST_MALWARE.AIが利用される可能性のある次の脆弱性がお使いのネットワークから検出されました。ネットワークを安全に保つために、指示に従って必要な処理を実行してください。

TEST_MALWARE.AIに対して脆弱なコンピュータ

[エクスポート](#) 合計2件 1/1 ページ

危険度	コンピュータ	IPアドレス	コンピュータグループ	脆弱性の数
非常に緊急	L10N-BLZ5-C7	10.3.243.58	テストgroupデスクトップ	114
非常に緊急	L10N-BLZ5-5	10.3.242.232	テストgroupデスクトップ	114

非常に緊急 緊急 重要 警告 低

図 6-2. 【大規模感染予防】画面-脅威の予防段階

ウイルス / 不正プログラムの情報

[ウイルス / 不正プログラムの情報] には、現在インターネットに存在するウイルス / 不正プログラムと、ネットワークおよびクライアントに影響を与える可能性のあるウイルス / 不正プログラムに関する情報が表示されます。トレンドマイクロがソリューションを開発している間、大規模感染予防ポリシーが、この情報に基づいて、ネットワークとクライアントを保護するための手順を実行します (190 ページの「大規模感染予防ポリシー」を参照)。トレンドマイクロのセキュリティ情報サイトにアクセスするには、メインメニューから [ヘルプ] → [セキュリティ情報] をクリックします。

このセクションには、次の情報が表示されます。

- 危険度** — ウイルス / 不正プログラムの検出数や重要度を基に、クライアントコンピュータやネットワークに与える影響の危険度を示します。

- **自動対応** — クリックすると、現在の脅威からクライアントを保護するために使用している大規模感染予防の特定の処理が表示されます。サーバ側およびビジネスセキュリティクライアント側から自動対応を無効にするには、[無効] をクリックします。

注意： 大規模感染予防を無効にした後、トロイの木馬およびトロイの木馬関連の実行プロセス、または他の種類の不正コードをクライアントから削除するためにクリーンアップを実行することをお勧めします（190 ページの「ダメージクリーンアップサービス」を参照）。

オンラインコンピュータのアラートステータス

[オンラインコンピュータのアラートステータス] には、自動アラートが有効になっているクライアントの数と有効になっていないクライアントの数の合計が表示されます。[有効] 列と [無効] 列の下の数値リンクをクリックすると、特定のクライアントに関する詳細が表示されます。

脆弱なコンピュータ

[脆弱なコンピュータ] セクションには、[ウイルス / 不正プログラムの情報] セクションに表示されたウイルス / 不正プログラムに対して脆弱なクライアントのリストが表示されます。

脅威からの保護

[現在のステータス] 画面の脅威からの保護段階では、トレンドマイクロのアップデートコンポーネントに関する有効なコンポーネントダウンロードのステータス、およびすべてのビジネスセキュリティクライアントに関する有効なコンポーネント配信のステータスについての情報が表示されます。

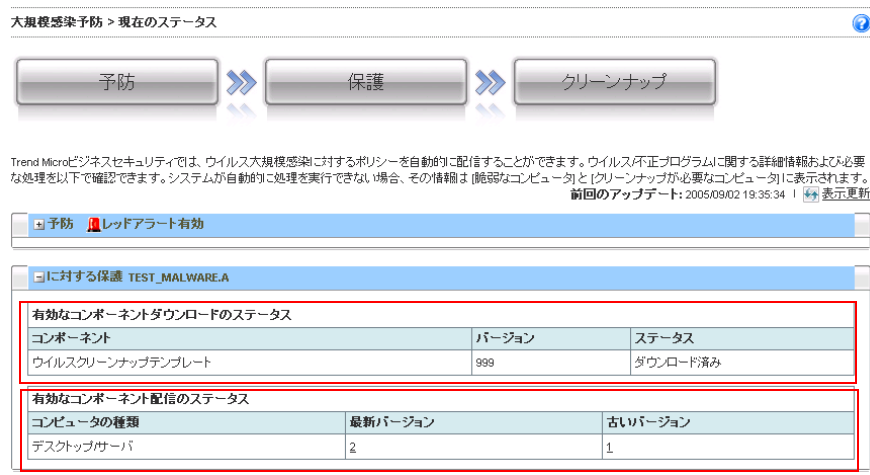


図 6-3. [大規模感染予防] 画面-保護段階

有効なコンポーネントダウンロードのステータス

[ウイルス / 不正プログラムの情報] セクションに示されているウイルス / 不正プログラムに応じてアップデートが必要なコンポーネントのリストが表示されます。

有効なコンポーネント配信のステータス

アップデートされたコンポーネントを持つビジネスセキュリティクライアントの数と、古いコンポーネントを持つビジネスセキュリティクライアントの数が表示されます。また、アップデートされたコンポーネントを持つクライアントと、古いコンポーネントを持つクライアントを表示するリンクも提供されます。

クリーンナップ

[現在のステータス] 画面の脅威のクリーンナップ段階では、アップデートされたコンポーネントの配信後に実行される検索のステータスが表示されます。脅威のクリーンナップ段階では、検索後のクライアントのステータスも表示され、最新のコンポーネントによってすべて駆除されたかどうかが表示されます。

大規模感染予防 > 現在のステータス

予防 → 保護 → クリーンナップ

Trend Microビジネスセキュリティでは、ウイルス大規模感染に対するポリシーを自動的に配信することができます。ウイルス不正プログラムに関する詳細情報および必要な処理を以下で確認できます。システムが自動的に処理を実行できない場合、その情報は (脆弱なコンピュータ) と (クリーンナップが必要なコンピュータ) に表示されます。
 前回のアップデート: 2005/09/02 19:35:34 | [表示更新](#)

☒ 予防 ☒ レッドアラート有効

☒ に対する保護 TEST_MALWARE.A

☒ TEST_MALWARE.AIに対するクリーンナップ

最新の有効なコンポーネントでお使いのネットワークを検索しました。検索が実行されたコンピュータは、以下の一覧で確認できます。

TEST_MALWARE.AIに対するコンピュータ検索のステータス	検索済み	未検索
コンピュータの種類		
デスクトップサーバ	0	2

ビジネスセキュリティ最新の有効なコンポーネントでお使いのネットワークを検索しました。検索が実行されたコンピュータは、以下の一覧で確認できます。

TEST_MALWARE.AIに対するコンピュータクリーンナップステータス

実行済み/合計: 2/3

[エクスポート](#) 合計: 2 件 1 / 1

コンピュータ	日時	IPアドレス	コンピュータグループ	脅威名	クリーンナップ結果
L10N-VISTA-H2	2005/09/02 19:25:27	10.3.242.229	テストgroupデスクトップ	TEST_MALWARE.A	駆除に成功しました。
L10N-BIZ5-5	2005/09/02 19:25:20	10.3.242.232	テストgroupデスクトップ	TEST_MALWARE.A	駆除に成功しました。

図 6-4. [大規模感染予防] 画面 - クリーンナップ段階

注意: 新しいコンポーネントが配信された後に自動的に検索が実行されるようにするには、[大規模感染予防] → [設定] 画面でこれを有効にする必要があります。

コンピュータ検索のステータス

検索実行の通知を受信した、またはまだ受信していないクライアントを確認するには、リンクをクリックします。起動していない、またはネットワークから切断されているクライアントでは、通知を受信できません。

コンピュータクリーンナップステータス

このセクションには、クリーンナップの結果が表示されます。[エクスポート] をクリックすると、この情報をエクスポートできます。

診断 / クリーンナップ

手順 : [大規模感染予防] → [診断 / クリーンナップ]

[診断 / クリーンナップ] 画面には、クライアントとネットワークに対するセキュリティリスクに関する情報が表示されます。ビジネスセキュリティサーバは、脆弱性診断およびクリーンナップサービスを実行して、脅威に関する情報を収集します。

大規模感染予防 > 診断/クリーンナップ

お使いのネットワークの安全性を確保するために、脆弱性のあるコンピュータを検出し、手動でクリーンナップを実行する必要があるコンピュータの一覧を提供します。注意が必要なコンピュータを以下で確認してください。

前回のアップデート: 2008/06/25 11:11:13 [表示更新](#)

脆弱なコンピュータ

脆弱性診断の前回の実行時刻: 2008/06/25 0:00:34

お使いのネットワークから脆弱性のあるコンピュータが検出されました。検出された脆弱性への対策の詳細については、リンクをクリックしてください。すべてのコンピュータに対して脆弱性診断を今すぐ実行するには、[脆弱性診断を実行] をクリックします。

[エクスポート](#) [脆弱性診断を実行](#) 合計: 3 件 1 / 1

危険度	コンピュータ	IPアドレス	コンピュータグループ	脆弱性の数
■■■■■	L10N-BIZS-C10	10.3.243.93	TestデスクトップPC	114
■■■■■	L10N-BIZS-C8	10.3.242.14	TestデスクトップPC	114
■■■■■	L10N-BIZS-TEST	10.3.243.31	サーバ (初期設定)	20

■■■■■ 非常に緊急 ■■■■■ 緊急 ■■■■■ 重要 ■■■■■ 警告 ■■■■■ 低

クリーンナップするコンピュータ

ダメージクリーンナップの前回の実行時刻: 2008/06/25 11:06:27

最新のバスターンファイルでコンピュータのクリーンナップを実行しました。以下の結果を参照してください。新しいバージョンで手動でクリーンナップを実行するには、[クリーンナップ実行] をクリックします。

[エクスポート](#) [クリーンナップ実行](#) 合計: 2 件 1 / 1

コンピュータ	日時	IPアドレス	コンピュータグループ	脅威名	クリーンナップ結果
L10N-BIZS-C8	2008/06/18 11:08:30	10.3.242.14	TestデスクトップPC	TSCTESTFILE	駆除に成功しました。
L10N-BIZS-C10	2008/06/18 11:08:50	10.3.243.93	TestデスクトップPC	TSCTESTFILE	駆除に成功しました。

図 6-5. [診断 / クリーンナップ] セクション

現在のウイルス / 不正プログラムに関する情報のみを表示する画面と異なり、[診断 / クリーンナップ] 画面には、クライアントとネットワークに対する未解決のすべての脅威に関する情報が表示されます。

脆弱なコンピュータ

脆弱なコンピュータとは、使用している OS またはアプリケーションに弱点があるコンピュータのことです。多くの脅威がこれらの脆弱性を悪用して、損傷を招いたり、許可されていない権限を取得したりします。つまり、脆弱性は、脆弱性のある個々のコンピュータだけではなく、ネットワークの他のコンピュータにもリスクをもたらします。

[脆弱なコンピュータ] には、最後の脆弱性診断以降に、脆弱性が検出されたネットワーク上のすべてのクライアントが一覧表示されます。最終アップデート時刻は、画面右上隅に表示されます。

[診断 / クリーンナップ] 画面では、ネットワークにもたらす危険度に応じてクライアントをランク付けします。危険度はトレンドマイクロによって計算され、クライアントごとに脆弱性を示す相対的な数値とその重要度が表示されます。

[脆弱性診断を実行] をクリックすると、ビジネスセキュリティが脆弱性診断を実行します。脆弱性診断は、ネットワーク上のすべてのクライアントについて脆弱性をチェックし、結果を [診断 / クリーンナップ] 画面に表示します。脆弱性診断は、ネットワーク上のクライアントに関する次の情報を提供します。

- 標準の命名規則に従って脆弱性を特定します。脆弱性の名前をクリックすると、脆弱性に関する詳細と解決方法が表示されます。
- クライアントおよび IP アドレス別に脆弱性を表示します。結果には、脆弱性がクライアントにもたらす危険度と、ネットワーク全体にもたらす危険度が含まれます。
- 脆弱性をレポートします。個々のクライアントについて脆弱性をレポートし、それらのクライアントがネットワーク全体にもたらすセキュリティリスクについて説明します。

[クリーンナップ実行] を実行する

[クリーンナップ実行] を実行すると、クリーンナップを手動で開始できます。

[クリーンナップ実行] を実行するには

1. [大規模感染予防] → [診断 / クリーンナップ] をクリックします。
2. [クリーンナップ実行] リンクをクリックします。初期設定では、ビジネスセキュリティサーバにより、すべてのビジネスセキュリティクライアントに [クリーンナップ実行] の実行が通知されます。

大規模感染予防を設定する

[設定] 画面を使用して、大規模感染予防と脆弱性診断のオプションを設定できます。

大規模感染予防の設定

ビジネスセキュリティは、大規模感染ポリシーで受け取った命令に応じて大規模感染予防を開始します。トレンドマイクロの大規模感染予防ポリシーは、大規模感染の発生時にクライアントとネットワークを最適に保護する目的で、トレンドマイクロによって設計され発行されます。トレンドマイクロは、インターネット上で活発に流布される頻繁で深刻なウイルス / 不正プログラムの発生に気付いたときに、大規模感染予防ポリシーを発行します。

初期設定では、ビジネスセキュリティサーバは、大規模感染予防ポリシーをトレンドマイクロのアップデートサーバから 30 分ごとにダウンロードします。また、ビジネスセキュリティサーバの起動時にもダウンロードします。

大規模感染予防の間、ビジネスセキュリティサーバは大規模感染予防ポリシーを制定して、クライアントとネットワークを保護するための処理を実行します。このような場合、ネットワークの通常の機能は、ブロックされたポートやアクセス不能なディレクトリなどが原因で中断されます。大規模感染予防設定を使用してクライアントとネットワークの大規模感染予防をカスタマイズし、大規模感染予防の間に制定されるポリシーに起因する予想外の結果を回避できます。

レッドアラート

急速に拡大しているウイルスや不正プログラムが複数のビジネスユニットから報告されています。それに応じて、トレンドマイクロは 45 分のレッドアラートソリューションプロセスを開始します。このプロセスには、予防的なソリューションや検索パターンファイルのリリース、関連する通知の送信などが含まれます。さらに、関連する脆弱性および脅威に関する修正ツールや情報も配信されます。

イエローアラート

多数のビジネスユニットから感染が報告されており、サポートセンターにも、感染拡大を裏付ける問い合わせが寄せられています。オフィシャルパターンファイルが自動的に配信サーバに送信され、ダウンロードできるようになります。

大規模感染予防の推奨設定

最適な保護を提供するため、次の設定が用意されています。

表 6-2. 大規模感染予防の推奨設定

設定	推奨値
トレンドマイクロから発令されたレッドアラートに対する自動大規模感染予防を有効にする	有効
次の日数が経過したらレッドアラートを無効にする	2 日間
必要なパターンファイル / 検索エンジン配信後に、レッドアラートを無効にする	有効
必要なコンポーネントの配信後に、自動的にウイルス検索を実行する	有効
トレンドマイクロから発令されたイエローアラートに対する自動大規模感染予防を有効にする	無効
次の日数が経過したらイエローアラートを無効にする	NA
必要なパターンファイル / 検索エンジン配信後に、イエローアラートを無効にする	NA
必要なパターンファイル / 検索エンジン配信後に、イエローアラートを無効にする。	NA
必要なコンポーネントの配信後に、自動的にウイルス検索を実行する	有効
除外設定	大規模感染予防の自動対応の間、次のサービス用のポートはブロックされません。 DNS NetBios HTTPS (安全な Web サーバ) HTTP (Web サーバ) Telnet SMTP (Simple mail protocol) FTP (File Transfer Protocol) インターネットメール (POP3)
ポリシーの予約ダウンロード設定	ダウンロード間隔: 30 分ごと 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

大規模感染予防設定を設定する

注意： 大規模感染予防の初期設定は、クライアントとネットワークを最適に保護する目的で設計されています。大規模感染予防設定をカスタマイズする前に、設定値を慎重に検討し、結果がわかっている場合にだけ値を変更してください。

手順：[大規模感染予防] → [設定] → [大規模感染予防] タブ

大規模感染予防 > 設定 

ネットワーク全体に対する脆弱性診断および大規模感染予防の設定を行います。

大規模感染予防	脆弱性診断
自動大規模感染予防	
☒ トrendマイクロから発令されたレッドアラートに対する自動大規模感染予防を有効にする 	
次の日数が経過したらレッドアラートを無効にする: 2 日	
☒ 必要なパターンファイル/検索エンジン配信後、レッドアラートを無効にする	
必要なコンポーネントの配信後、自動的にウイルス検索を実行する	
☒ デスクトップサーバ	
☐ Trendマイクロから発令されたイエローアラートに対する自動大規模感染予防を有効にする 	
次の日数が経過したらイエローアラートを無効にする: 2 日	
☒ 必要なパターンファイル/検索エンジン配信後、イエローアラートを無効にする	
必要なコンポーネントの配信後、自動的にウイルス検索を実行する	
☐ デスクトップサーバ	
除外設定	
ポリシーの予約ダウンロード設定	

 保存

図 6-6. [大規模感染予防] → [設定] 画面の [大規模感染予防] タブ

大規模感染予防設定を設定するには

- 必要に応じて次のオプションをアップデートします。
 - トレンドマイクロから発令されたレッドアラートに対する自動大規模感染予防を有効にする：[大規模感染予防] → [現在のステータス] → [無効] をクリックするか、無効な設定値のいずれかの条件が満たされるまで、大規模感染予防ポリシーは有効なままです。ビジネスセキュリティサーバが大規模感染予防ポリシーをダウンロードすると、古いポリシーは停止します。
 - 次の日数が経過したらレッドアラートを無効にする：大規模感染予防のアラートの期間。

- 必要なコンポーネントの配信後に、自動的にウイルス検索を実行する
 - デスクトップ / サーバ
- イエローアラートの設定** : イエローアラートのオプションを設定します。詳細については、101 ページの「イエローアラート」を参照してください。
- 除外設定** — 大規模感染予防の自動対応の間、ポートはブロックされません。除外設定の使用方法については、104 ページの「大規模感染予防の除外設定を使用する」を参照してください。

注意： 新しい除外設定を追加した場合は、必ず、[この除外設定を有効にする] をオンにしてください。

- ポリシーの予約ダウンロード設定 — アップデートされたコンポーネントを定期的にダウンロードするための設定。
 - ダウンロード間隔
 - アップデート元** : アップデートのダウンロード元。
 - トレンドマイクロのアップデートサーバ (初期設定)
 - 最新ファイルのコピーが格納されたイントラネット上のフォルダ
 - その他のアップデート元 : その他の Web 上のアップデートのダウンロード元。

2. [保存] をクリックします。

大規模感染予防の除外設定を使用する

手順 : [大規模感染予防] → [設定] → [大規模感染予防] タブ

除外設定を使用して、ブロックから除外するポートを追加、編集、または削除できます。

除外設定			
☒ 常に次のポートのブロックを除外する			
名前	プロトコルの種類	ポート/ポート範囲	有効
☐ DNS	TCP	53	
☐ DNS	UDP	53	
☐ NetBIOS	TCP	137,138,139,445	
☐ NetBIOS	UDP	137,138,139,445	
☐ HTTPS	TCP	443	

図 6-7. [大規模感染予防] → [設定] 画面の [除外設定] セクション

除外設定を追加するには

1. [除外設定] セクションの [+] をクリックします。
2. [追加] をクリックします。
3. [大規模感染予防] → [設定] → [除外設定の追加] 画面で、必要に応じて次のオプションをアップデートします。
 - この除外設定を有効にする
 - **説明**: 除外設定を見分けやすくする簡単な説明です。
 - **プロトコル**: 除外設定を適用する必要があるプロトコルを選択します。
 - **ポート**: 除外するポートの範囲または個々のポートを入力します。複数のエントリはセミコロン (;) で区切ります。
4. [追加] をクリックします。

除外設定を編集するには

1. [除外設定] セクションの [+] をクリックします。
2. 除外設定を選択して、[編集] をクリックします。
3. [保存] をクリックします。

除外設定を削除するには

除外設定は、削除する代わりに無効にすることができます。

1. [除外設定] セクションの [+] をクリックします。
2. 除外設定を選択して、[削除] をクリックします。
3. [OK] をクリックして確定します。

自動大規模感染予防の詳細を表示する

手順: [大規模感染予防] → [現在のステータス] → [予防] パネル

大規模感染時には、ビジネスセキュリティサーバでは大規模感染予防が起動されます。自動大規模感染予防により、TrendLabs が現在の大規模感染に対するソリューションを構築している緊急時に、コンピュータとネットワークが現在の大規模感染による損害を受けるのを回避できます。

自動大規模感染予防では、ウイルス大規模感染時に次の処理が実行されます。

- 共有フォルダをブロックして、共有フォルダ内のファイルにウイルスが感染しないようにします。
- ポートをブロックして、脆弱なポートを利用してネットワークとクライアントのファイルにウイルスが感染することを防ぎます。

注意： 大規模感染予防は、ビジネスセキュリティサーバがクライアントとの通信に使用しているポートをブロックしません。

- ・ ファイルおよびフォルダへの書き込みアクセスを禁止して、ファイルがウイルスによって変更されないようにします。
- ・ 添付ファイルをブロックする機能が有効になり、疑わしい添付ファイルがブロックされます。
- ・ コンテンツフィルタが有効になり、「すべてに一致」または「いずれかに一致」のルールが作成されます。これによって、脅威に感染したコンテンツがフィルタされます。

脆弱性診断設定を設定する

手順：[大規模感染予防] → [設定] → [脆弱性診断] タブ

脆弱性診断の設定によって、脆弱性診断の頻度と対象が決まります。

大規模感染予防 > 設定 

ネットワーク全体に対する脆弱性診断および大規模感染予防の設定を行います。

大規模感染予防

脆弱性診断

スケジュール

☒ 予約脆弱性診断を有効にする

☐ 毎日
 ☒ 毎週

水曜日 ▼

☐ 毎月

2 ▼ 日

開始時刻

00 ▼ : 00 ▼ (時:分)

検索対象

☒ すべてのグループ
 ☐ 指定のグループ

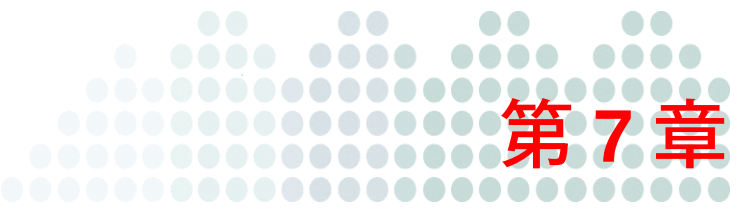
☐ サーバ (初期設定)
 ☐ デスクトップ (初期設定)
 ☐ Test

保存

図 6-8. [大規模感染予防] → [設定] 画面の [脆弱性診断] タブ

脆弱性診断の間隔を設定するには

1. [大規模感染予防] → [設定] 画面の [脆弱性診断] タブで、必要に応じて次のオプションをアップデートします。
 - **予約脆弱性診断を有効にする**
 - **実行間隔**: [毎日]、[毎週]、または [毎月] のいずれかを選択します。[毎週] または [毎月] を選択した場合は、曜日または月の中の日付を設定します。
 - **開始時刻**
 - **検索対象**
 - **すべてのグループ**: [セキュリティ設定] 画面のグループ管理ツリーに表示されるすべてのクライアントを検索します。
 - **指定のグループ**: 脆弱性診断のための検索を選択されたグループのみに限定します。
2. [保存] をクリックします。



第7章

検索の管理

本章では、スマートスキャン、従来型スキャン、および手動検索と予約検索を使用して、ネットワークとクライアントをウイルス、不正プログラム、およびその他の脅威から保護する方法について説明します。

本章で説明する内容には、次の項目が含まれます。

- 110 ページの「検索について」
- 110 ページの「検索方法」
- 111 ページの「検索の種類」
- 112 ページの「手動検索および予約検索オプションを設定する」
- 116 ページの「予約検索」

検索について

Trend Micro ビジネスセキュリティ (以下、ビジネスセキュリティ) には、インターネット上の脅威からクライアントを保護するための 3 種類の検索があります。手動検索、予約検索、およびリアルタイム検索です。検索の種類によって目的と用途は異なりますが、設定の方法はほぼ同様です。本章では、手動検索と予約検索について説明します。

検索方法

クライアント検索は、次の 2 つの方法で実行されます。

- **従来型スキャン**: クライアントでは、脅威の特定に、独自の検索エンジンとローカルパターンファイルが使用されます。
- **スマートスキャン**: クライアントでは、脅威の特定に独自の検索エンジンが使用されますが、ローカルパターンファイルのみを使用するのではなく、スキャンサーバに格納されているパターンファイルを主に利用します。

注意: ビジネスセキュリティのこの実装では、ビジネスセキュリティサーバがスキャンサーバとして機能します。スキャンサーバは、ビジネスセキュリティサーバで実行されるサービスです。スキャンサーバサービスは、ビジネスセキュリティサーバのインストール時に自動的にインストールされます。スキャンサーバを個別にインストールする必要はありません。クライアントがスマートスキャン用に設定されているが、スマートスキャンサービスに接続できない場合、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への接続を試みます。

検索方法を選択する

クライアントの検索によってクライアントコンピュータのパフォーマンスが低下する場合は、スマートスキャンに切り替えることを検討してください。初期設定で、スマートスキャンは無効になっています。[一般検索設定] の [オプション設定] → [グローバル設定] 画面で、すべてのクライアントのスマートスキャンを有効にできます。

検索方法を選択するには

1. [セキュリティ設定] をクリックして、サーバまたはデスクトップをクリックします。
2. [設定] をクリックします。
3. 画面上部の [スマートスキャン] または [従来型スキャン] をクリックします。

注意： クライアントがスマートスキャン用に設定されているが、ネットワーク上のスキャンサーバに接続できない場合、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への接続を試みます。

検索の種類

ビジネスセキュリティでは、次の種類の検索を実行できます。

- リアルタイム検索：クライアントユーザが、ファイルをダウンロードする、保存する、コピーする、変更する、または開くたびに実行される継続的な検索です。
- 手動検索：管理者またはクライアントユーザが開始するオンデマンドの検索です。
- 予約検索：定期的にスケジュールされた時間に開始する検索です。

詳細については、65 ページの「検索の種類」を参照してください。

手動検索および予約検索オプションを設定する

検索オプションの設定では、検索対象（検索するファイル）と処理（検出された脅威に対する処理）を設定します。

手順：[検索] → [手動検索] または [予約検索] → グループをクリック

検索 > 手動検索 > デスクトップ (初期設定) : ウイルススキャン対象

検索対象 処理

☒ 検索可能なすべてのファイル

☐ トレンドマイクロの推奨設定 (実際のファイルタイプによる選択) (i)

☐ 検索対象の拡張子の選択 (拡張子はそれぞれカンマで区切ってください)

ACE, ARJ, ASF, BAT, BIN, BOO, CAB, CHM, CLA, CLASS, COM, CSC, DAT, DLL, DOC, DOT, DRV, EXE, GZ, HLP, HTA, HTML, HTT, IN, JAR, JSP, JS, JSE, LNK, LZH, MSB, MPD, MPP, MPT, MSG, MSO, NRG, OCK, OFF, OVL, PDF, PHP, PL, POT, PPS, RPT, PRC, RAR, REG, RTP, SCR, SHS, SPS, TAF, VBE, VBS, VSD, VST, XLS, XLSX, XLT, XML, ZIP

☐ ネットワークドライブおよび共有フォルダを検索する

☒ 圧縮ファイルの検索: 検索レベル (2) 階層

検索除外

☒ 検索除外を有効にする

特定ディレクトリの検索除外

☒ 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を検索から除外する

ディレクトリのパスを入力してください (例: c:\temp\excludeDir)

追加 削除

特定ファイルの検索除外

ファイル名またはファイルのフルパスを入力してください
(例: ExcludeDoc.Txt, c:\temp\exclude\ExcludeDoc.Txt)

追加 削除

特定の拡張子を持つファイルの検索除外

リストから拡張子を選択してください

選択された拡張子:

ACCEB
ACE
AMJ
ARJ
BAT
BIN

追加 削除

拡張子を入力してください

詳細設定

ウイルス対策の場合のみ

☒ InterTrapを有効にする (i)

☒ システム情報を検索する

スキャン対象の場合のみ

特定の種類のスキャン対象のアプリケーションまたはファイルを検索リストに追加して、検索対象から除外します。

これは、すべての種類の検索に適用されます。

スキャン対象の除外リストの変更

保存 キャンセル

検索オプションを設定するには

1. グループの検索オプション画面で、必要に応じて次の項目をアップデートします。

- **検索対象のファイル**
 - **すべての検索可能ファイル** — 暗号化されたファイルやパスワードで保護されたファイルのみが除外されます。
 - **トレンドマイクロの推奨設定** — 実際のファイルタイプに基づいてファイルを検索します。詳細については、192 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。
 - **検索対象の拡張子の選択** — ビジネスセキュリティは、選択した拡張子を持つファイルを検索します。拡張子が複数ある場合はカンマ (,) で区切ります。
 - **ネットワークドライブおよび共有フォルダを検索する**
 - **圧縮ファイルの検索** — 検索する階層の数を設定します。
- **検索除外**: 特定のファイル、フォルダ、または特定の拡張子を持つファイルを検索対象から除外します。
 - **検索除外を有効にする**
 - **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を検索から除外する**
 - **特定ディレクトリの検索除外** — 検索対象から除外するフォルダの名前を入力します。[追加] をクリックします。フォルダを削除するには、フォルダを選択して [削除] をクリックします。
 - **特定ファイルの検索除外** — 検索対象から除外するファイルの名前を入力します。[追加] をクリックします。ファイルを削除するには、ファイルを選択して [削除] をクリックします。
 - **特定の拡張子を持つファイルの検索除外** — 検索対象から除外する拡張子の名前を入力します。[追加] をクリックします。拡張子を削除するには、拡張子を選択して [削除] をクリックします。
- **詳細設定**
 - **IntelliTrap を有効にする** (ウイルス対策の場合) — IntelliTrap は、圧縮ファイル内のボットなどの不正なコードを検出します。詳細については、193 ページの「IntelliTrap」を参照してください。
 - **システム領域を検索する** (ウイルス対策の場合) — ブートセクタには、クライアントが OS をロードして初期化するために使用するデータが格納されています。システム領域感染型ウイルスは、パーティションまたはディスクのブートセクタに感染します。

- **スパイウェアの除外リストの変更** (ウイルス対策の場合) — このリストには、使用を許可するスパイウェア / グレーウェアプログラムの詳細が含まれます。リストをアップデートするには、リンクをクリックします。詳細については、115 ページの「スパイウェア / グレーウェアの除外リストを編集する」を参照してください。
2. [処理] タブで、ビジネスセキュリティが検出された脅威を処理する方法を指定します。
- **CPU 使用率**: 各ファイルを検索する間にビジネスセキュリティサーバが待機している時間は、CPU 使用率に影響します。各ファイル検索の間の待機時間を増やし、CPU を開放して他のタスクを実行できるようにするには、低レベルの CPU 使用率を選択します。
 - **ウイルス検出に対する処理**
 - **トレンドマイクロの推奨処理**: 脅威に対して、トレンドマイクロが事前定義した処理を実行します。詳細については、192 ページの「トレンドマイクロの推奨処理」を参照してください。

すべての種類に同じ処理を使用: 放置、削除、拡張子変更、隔離、または駆除のいずれかを選択します。駆除を選択した場合は、駆除できない脅威に対する処理も設定してください。

検索処理の指定: 脅威の種類ごとに、放置、削除、拡張子変更、隔離、または駆除のいずれかを選択します。駆除を選択した場合は、駆除できない脅威に対する処理も設定してください。
 - **ウイルス駆除実行前にバックアップを作成**: ビジネスセキュリティは、駆除する前に脅威のバックアップを作成します。バックアップファイルは暗号化され、クライアントの次のディレクトリに格納されます。

C:\Program Files\Trend Micro\Client Server Security Agent\Backup

ファイルを復号するには、206 ページの「感染ファイル暗号化処理の復元ツール」を参照してください。
 - **スパイウェア / グレーウェアの検出に対する処理**
 - **駆除**: ビジネスセキュリティは、スパイウェア / グレーウェアを駆除するときに、関連するレジストリエントリ、ファイル、Cookie、およびショートカットを削除することがあります。スパイウェア / グレーウェアに関連するプロセスも終了されます。
 - **放置**: さらに評価するため、感染をログに記録するだけに留めます。詳細については、158 ページの「ログ」を参照してください。
3. [保存] をクリックします。
- また、イベントの発生時に通知を受信するユーザも設定します。

スパイウェア / グレーウェアの除外リストを編集する

スパイウェア / グレーウェアの除外リストによって、ユーザがどのスパイウェアまたはグレーウェアアプリケーションを使用できるかが決まります。リストをアップデートできるのは、管理者だけです。さまざまな種類のスパイウェアの情報については、21 ページの「スパイウェア / グレーウェア」を参照してください。

注意： 特定のグループに対しては、リアルタイム検索、予約検索、および手動検索で同一のリストが使用されます。

手順：[検索] → [手動検索] または [予約検索] → グループをクリック → [詳細設定] → [スパイウェアの除外リストの変更]

スパイウェア/グレーウェアの除外リスト デスクトップ (初期設定)

スパイウェア/グレーウェアの詳細については、トレンドマイクロの「スパイウェア/グレーウェアデータベース」を参照してください。

除外リスト

検索

簡単検索: A~E | F~J | K~Q | P~T | U~Z | その他

除外リスト (最大アイテム数1024)

アイテム数 0

1 / 57

Adware_123Banners
Adware_123Mania
Adware_17LeLe
Adware_180Solutions
Adware_180Solutions.SearchAssistant
Adware_180Solutions.Seekmo
Adware_180Solutions.Zango
Adware_2020Search
Adware_2Call
Adware_2ndThought
Adware_2Search
Adware_3721
Adware_7Ads
Adware_888Casino
Adware_Aaddzz
Adware_ABCSearch
Adware_ABetterInternet
Adware_Above
Adware_Accoonna
Adware_AcroymFinder
Adware_ActiveSearch

追加 >

< 削除

保存 キャンセル

図 7-1. [スパイウェア / グレーウェアの除外リスト] 画面

スパイウェア / グレーウェアの除外リストをアップデートするには

1. [詳細設定] セクションで、[スパイウェアの除外リストの変更] をクリックします。
2. [スパイウェア / グレーウェアの除外リスト] 画面で、必要に応じて次の項目をアップデートします。
 - **左側の画面** : 認識済みのスパイウェアまたはグレーウェアアプリケーション。許可するスパイウェア / グレーウェアアプリケーションを検索する場合は、[検索] リンクまたは [簡単検索] リンクを使用します。

注意： アプリケーションは、アプリケーションの種類別にソートされ、その後アプリケーション名順にソートされます。

- **右側の画面** : 使用を許可するスパイウェアまたはグレーウェアプログラム。
 - **追加 >** : 左側の画面でアプリケーション名を選択し、[追加 >] をクリックします。複数のアプリケーションを選択するには、<Ctrl> キーを押しながらアプリケーション名をクリックします。
3. [保存] をクリックします。

予約検索

手順 : [検索] → [予約検索] → [スケジュール] タブ

予約検索は、クライアントを定期的に検索して脅威がないかどうか確認します。

ヒント： 予約検索と自動アップデートは、同じ時刻に実行するようにスケジュールしないことをお勧めします。自動アップデートと同じ時刻にスケジュールすると、予約検索が途中で中断される可能性があります。同様に、予約検索の実行中に手動検索を開始すると、予約検索が中断されます。予約検索は中断されますが、スケジュールに応じて再度実行されます。

注意： 予約検索を無効にするには、特定のグループすべてのオプションをオフにして、[保存] をクリックします。

検索 > 予約検索

設定 スケジュール

サーバ (初期設定)

☐ 毎日

☒ 毎週 月曜日

☐ 毎月 1

開始時刻 12 : 30 (時:分)

デスクトップ (初期設定)

☐ 毎日

☒ 毎週 月曜日

☐ 毎月 1

開始時刻 12 : 30 (時:分)

保存

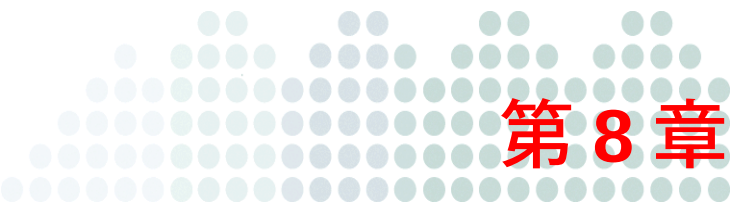
図 7-2. 【予約検索】画面

検索をスケジュールするには

1. 検索をスケジュールする前に、検索の設定を行います。詳細については、112 ページの「[手動検索および予約検索オプションを設定する](#)」を参照してください。
2. [スケジュール] タブで、必要に応じて各グループの次のオプションをアップデートします。
 - **毎日** — 予約検索は、毎日、[開始時刻] に指定された時刻に実行されます。
 - **毎週** — 予約検索は、週 1 回、指定された曜日の [開始時刻] に指定された時刻に実行されます。
 - **毎月: 日** — 予約検索は、月 1 回、指定された日付の [開始時刻] に指定された時刻に実行されます。31 を選択した場合、30 日しかない月は、クライアントは検索されません。
 - **開始時刻**: 予約検索を開始する時刻。
3. [保存] をクリックします。

また、イベントの発生時に通知を受信するユーザも設定します。詳細については、121 ページの「[通知イベントを設定する](#)」を参照してください。

ヒント: 最適に保護するために、予約検索を定期的に行うことをお勧めします。



第8章

通知の管理

本章では、さまざまな通知オプションの使用方法について説明します。

本章で説明する内容には、次の項目が含まれます。

- 120 ページの「通知」
- 121 ページの「通知イベントを設定する」
- 122 ページの「通知する内容を設定する」
- 123 ページの「通知方法を設定する」

通知

管理者が Trend Micro ビジネスセキュリティ（以下、ビジネスセキュリティ）の監視に要する時間を最小限に抑え、さらに大規模感染発生の兆しについて早くかつ確実に管理者が警告を受け取れるようにするために、ネットワークで異常なイベントが発生したときは常に通知を送信するようにビジネスセキュリティサーバを設定します。ビジネスセキュリティは、メール、SNMP、または Windows イベントログを使用して通知を送信できます。

通知条件は [最新ステータス] 画面に影響します。条件に合致すると、ステータスアイコンは「通常」状態から「警告」または「必要な処理」な状態に変化します。

初期設定では、[通知] 画面に一覧表示されるすべてのイベントが選択されており、これらのイベントが発生すると、ビジネスセキュリティサーバから管理者に通知が送信されます。

脅威イベント

- **大規模感染予防**：TrendLabs によってアラートが宣言されたとき、または非常に危険な脆弱性が検出されたときに発生します。
- **ウイルス対策**：クライアントで検出されたウイルス / 不正プログラムの数が一定数を超えたとき、ウイルス / 不正プログラムに対する処理に失敗したとき、クライアントのリアルタイム検索が無効なときに発生します。
- **スパイウェア対策**：クライアントでスパイウェア / グレーウェアが検出されたときに発生します。これらの中には、スパイウェア / グレーウェアの脅威を完全に取り除くために、感染したクライアントの再起動が必要となるものもあります。スパイウェア / グレーウェア通知のしきい値、つまり指定した期間内（初期設定は 1 時間）に検出されたスパイウェア / グレーウェア数を設定することもできます。
- **Web レビューション**：URL 違反の数が、一定期間内に設定した数を超えたときに発生します。
- **URL フィルタ**：設定されたフィルタールールに基づき、URL 違反が一定期間内に設定した数を超えたときに発生します。
- **挙動監視**：ポリシー違反の数が、一定期間に設定した数を超えたときに発生します。
- **ネットワークウイルス**：検出されたネットワークウイルスの数が一定数を超えたときに発生します。

システムイベント

- **スマートスキャン**：スマートスキャン用に設定されている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か、サーバが利用できません。

- ・ **コンポーネントアップデート**：コンポーネントが最後にアップデートされてからの日数が一定の日数を超えたとき、またはアップデートされたコンポーネントが即座にビジネスセキュリティクライアントに配信されなかったときに発生します。
- ・ **システム異常イベント**：Windows Server OS を実行するクライアントのディスクの空き領域が設定した量を下回ると発生します。

ライセンスイベント

- ・ **ライセンス**：製品ライセンスの有効期限が切れそうなきまたは切れたときに発生します。

通知イベントを設定する

手順：[オプション設定]→[通知設定]→[イベント]タブ

通知は2段階を経て設定します。最初に、通知が必要なイベントを選択し、次に、配信方法を設定します。ビジネスセキュリティには、メール通知、SNMP通知、およびWindows イベントログの3通りの配信方法があります。



図 8-1. [通知設定]の[イベント]画面

通知イベントを設定するには

1. [通知設定] 画面の [イベント] タブで、必要に応じて次の項目をアップデートします。
 - **脅威イベント**: すべてのイベントについて通知を受信するには、[種類] チェックボックスをオンにします。別の方法として、個々のイベントに対応するチェックボックスをオンにすることもできます。
 -  をクリックすると、各イベントが展開され、イベントのしきい値や期間を設定できます。
2. [保存] をクリックします。

通知する内容を設定する

手順: [オプション設定] → [通知設定] → 通知をクリック

イベント通知の件名行とメッセージ本文をカスタマイズします。

トークン (変数) の使用

次のトークン (変数) を使用して、デスクトップやサーバ、および Exchange サーバで検出された脅威イベントを表示できます。[オプション設定] → [通知設定] 画面で選択した内容が参照されます。

- <\$CSM_SERVERNAME>: 脅威が検出されたビジネスセキュリティサーバや Exchange サーバの名前です。
- %CV: 検出数です。
- %CU: 時間の単位です (分や時間)。
- %CT: %CU の数値です。

次に通知例を示します。

お使いのコンピュータから %CT%CU の間に %CV 件を超えるウイルスが検出されました。ウイルス検出数が多い場合や頻繁な場合には、大規模感染の疑いがあります。ビジネスセキュリティサーバの [最新ステータス] 画面で、詳細を確認してください。

通知メッセージの内容をカスタマイズするには

1. [件名] フィールドに新しい件名行を入力します。
2. [メッセージ本文] フィールドに新しいメッセージを入力します。
3. [保存] をクリックします。

通知方法を設定する

手順: [オプション設定] → [通知設定] → [設定] タブ

図 8-2. [通知設定] 画面

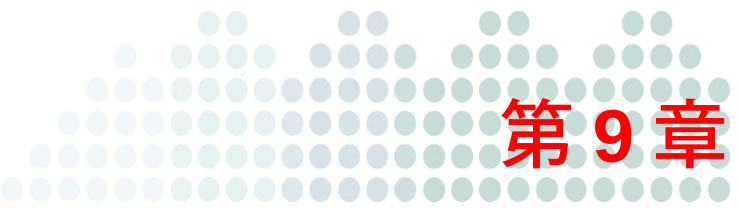
通知の配信方法を設定するには

1. [通知設定] 画面の [設定] タブで、必要に応じて次の項目をアップデートします。

- **メール通知**: 通知の送信者と受信者のメールアドレスを設定します。[イベント] タブで、メールメッセージの内容を設定します。
 - **送信元**
 - **送信先**: 複数のメールアドレスはセミコロン (;) で区切ります。
- **SNMP 通知**: SNMP は、ネットワークホストがネットワークの管理に使用する情報を交換するためのプロトコルです。SNMP トラップ内のデータを表示するには、Management Information Base ブラウザを使用します。
 - **SNMP 通知を有効にする**
 - **IP アドレス**: SNMP トラップの IP アドレス。
 - **コミュニティ名**: SNMP コミュニティ文字列。
- **ログ**: Windows イベントログを使用する通知です。
 - **Windows のイベントログによる通知を有効にする**

注意： 上記の通知方法のいずれか、またはすべてを使用できます。

2. [保存] をクリックします。



第9章

グローバル設定の管理

本章では、グローバル設定の使用方法について説明します。

本章で説明する内容には、次の項目が含まれます。

- 126 ページの「インターネットプロキシのオプション」
- 128 ページの「SMTP サーバのオプション」
- 128 ページの「デスクトップ / サーバのオプション」
- 135 ページの「システムのオプション」

グローバルオプション設定

管理コンソールから、Trend Micro ビジネスセキュリティ（以下、ビジネスセキュリティ）サーバ、およびビジネスセキュリティクライアントによって保護されているデスクトップとサーバについて、グローバル設定を実行できます。

インターネットプロキシのオプション

手順: [オプション設定] → [グローバル設定] → [プロキシ] タブ

ネットワークで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、次のサービスに関してプロキシサーバの設定を指定します。

- コンポーネントのアップデートおよびライセンス通知
- Web レピュテーション、挙動監視、スマートフィードバック、スマートスキャン、および URL フィルタ

同じアップデートプロキシ設定を使用したり、新しい資格情報を入力できます。

注意： ビジネスセキュリティクライアントでは Web レピュテーション、挙動監視、および Trend Micro Smart Protection Network のために、常に Internet Explorer と同じプロキシサーバとポートを使用してインターネットに接続します。クライアントコンピュータの Internet Explorer が同じプロキシサーバとポートを使用する場合のみ、アップデートサービス用に指定したログイン資格情報を複製してください。

プロキシ SMTP デスクトップサーバ システム

アップデートおよびライセンス通知の設定

☐ アップデートおよびライセンス通知にプロキシサーバを使用する

☒ SOCKS 4/5を使用する

サーバアドレス:

(例: proxy.trend.com.tw または 123.123.123.123)

ポート番号:

プロキシサーバ認証

ユーザ名:

パスワード:

Webレピュテーション、挙動監視、およびスマートスキャンの設定

Webレピュテーション、挙動監視、およびスマートスキャンサービスでは、クライアントコンピュータ上のInternet Explorerで使用しているプロキシサーバのアドレスとポートを使用します。
プロキシサーバから認証を求められたら、ログイン情報を入力してください。

☒ アップデートプロキシ (上記) で指定した資格情報を使用します

ユーザ名:

パスワード:

図 9-1. [グローバル設定] のプロキシサーバ設定画面

プロキシを設定するには

- [グローバル設定] 画面の [プロキシ] タブで、必要に応じて次のオプションをアップデートします。
 - アップデートおよびライセンス通知の設定
 - アップデートおよびライセンス通知にプロキシサーバを使用する
 - SOCKS 4/5 を使用する
 - サーバアドレス
 - ポート番号
 - プロキシサーバ認証
 - ユーザ名
 - パスワード
 - Web レピュテーション、挙動監視、およびスマートスキャンの設定
 - アップデートプロキシで指定した資格情報の使用
 - ユーザ名
 - パスワード
- [保存] をクリックします。

SMTP サーバのオプション

SMTP サーバ設定は、ビジネスセキュリティによって生成されるすべての通知とレポートに適用されます。

手順: [オプション設定] → [グローバル設定] → [SMTP] タブ

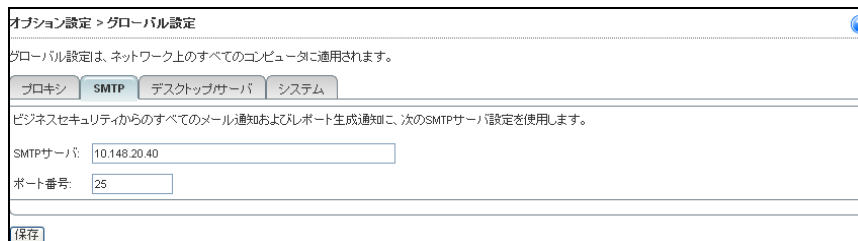


図 9-2. [グローバル設定] 画面の [SMTP] タブ

SMTP サーバを設定するには

- [グローバル設定] 画面の [SMTP] タブで、必要に応じて次のオプションをアップデートします。
 - SMTP サーバ メールサーバの IP アドレスまたは名前を入力します。
 - ポート
- [保存] をクリックします。

デスクトップ / サーバのオプション

手順: [オプション設定] → [グローバル設定] → [デスクトップ / サーバ] タブ

デスクトップ / サーバのオプションは、ビジネスセキュリティのグローバル設定に属しています。この設定よりも、個々のグループの設定が優先されます。グループの特定のオプションが未設定の場合は、デスクトップ / サーバのオプションが使用されます。たとえば、あるグループに対して承認済み URL が 1 つも定義されていない場合は、この画面で設定されたすべての承認済み URL がそのグループに適用されます。

オプション設定 > グローバル設定

グローバル設定は、ネットワーク上のすべてのコンピュータに適用されます。

プロキシ SMTP **デスクトップ/サーバ** システム

ロケーション認識

ロケーション認識は、クライアントのロケーションに応じて適切なセキュリティ保護を適用する機能です。ビジネスセキュリティのゲートウェイ情報に基づいて、ビジネスセキュリティがクライアントのロケーションを自動的に特定します。
VPN接続のデフォルト設定は「外部」です。設定を「内部接続」に変更する場合は、ゲートウェイアドレスとMACアドレスを手動で追加してください。

☒ ロケーション認識を有効にする（ファイアウォール、Web評価、およびTrendSecureのオフィス内外の設定に影響）

ゲートウェイアドレス:

MACアドレス (オプション):

ゲートウェイアドレス	MACアドレス
10.148.20.1	00:1A:6C:9F:21:91

一般検索設定

☒ ビジネスセキュリティのデータベースフォルダを除外する

☒ Microsoft Exchange サーバにインストールされている場合はMicrosoft Exchange Server フォルダを除外する

☒ Microsoftドメインコントローラフォルダを除外する
(手動および予約のスワイウェア検索には適用できません)

☒ シャドウコピーの除外セクション

監視サービス設定

☒ ビジネスセキュリティクライアント監視サービスを有効にする:

クライアントステータスを 分ごとに確認

クライアントを起動できない場合、 回まで再試行

アンインストール設定

☐ クライアントのユーザがビジネスセキュリティクライアントのアンインストールを許可する

☒ ビジネスセキュリティクライアントのアンインストールにパスワードを要求する

パスワード:

パスワードの確認:

プログラム終了設定

☐ クライアントのユーザがビジネスセキュリティクライアントのアンロードを許可する

☒ ビジネスセキュリティクライアントのアンロードにパスワードを要求する

パスワード:

パスワードの確認:

図 9-3. [グローバル設定] 画面の[デスクトップ/サーバ] タブ

デスクトップ/サーバのオプションを設定するには

1. [グローバル設定] 画面の [デスクトップ/サーバ] タブで、必要に応じて次のオプションをアップデートします。
 - 130 ページの「ロケーション認識」
 - 130 ページの「一般検索設定」
 - 131 ページの「ウイルス検索設定」

- 132 ページの「スパイウェア検索設定」
- 132 ページの「ファイアウォールを無効にする」
- 132 ページの「Web レピュテーションと承認済み URL」
- 133 ページの「挙動監視」
- 133 ページの「インスタントメッセージコンテンツフィルタ」
- 133 ページの「警告設定」
- 134 ページの「監視サービス設定」
- 134 ページの「アンインストール設定」
- 135 ページの「エージェントプログラム」

2. [保存] をクリックします。

ロケーション認識

ロケーション認識は、オフィス内とオフィス外の接続設定を制御します。

[グローバル設定] 画面の [デスクトップ / サーバ] タブで、必要に応じて次のオプションをアップデートします。

- **ロケーション認識を有効にする** : ここでの設定が、ファイアウォール、Web レピュテーション、Trend Secure、およびスマートスキャンのオフィス内 / オフィス外接続設定に影響するようになります。
- **ゲートウェイの情報** : このリストに登録されているクライアントおよび接続は、ネットワークにリモートで接続するときに (VPN を使用) ロケーション認識が有効化されていれば、内部接続設定を使用します。
 - **ゲートウェイ IP アドレス**
 - **MAC アドレス** : MAC アドレスを追加すると、指定のデバイスのみが接続できるようになるため、セキュリティが強化されます。

エントリを削除するには、対応するごみ箱アイコンをクリックします。

一般検索設定

[グローバル設定] 画面の [デスクトップ / サーバ] タブで、必要に応じて次のオプションをアップデートします。

- **スマートスキャンサービスを無効にする** : すべてのクライアントが従来型スキャンモードに切り替えられます。スマートスキャンは、ここで再度有効にされるまで使用できません。

- ・ **ビジネスセキュリティのデータベースフォルダを除外する**：このオプションがオンの場合、ビジネスセキュリティサーバにインストールされているビジネスセキュリティクライアントは、リアルタイム検索の実行時に限って、自身のデータベースを検索しません。

注意： 初期設定では、ビジネスセキュリティのデータベースは検索対象外です。検索時に発生する可能性があるデータベースの破損を回避するために、このチェックボックスはそのままオンにしておくようお勧めします。

- ・ **Microsoft Exchange サーバにインストールされている場合は Microsoft Exchange Server フォルダを除外する**：このオプションがオンの場合、Microsoft Exchange サーバにインストールされているビジネスセキュリティクライアントが検索を実行するときに、Microsoft Exchange のフォルダは検索対象外となります。
- ・ **Microsoft ドメインコントローラフォルダを除外する**：このオプションがオンの場合、ドメインコントローラにインストールされているビジネスセキュリティクライアントが検索を実行するときに、ドメインコントローラのフォルダは検索対象外となります。このフォルダには、ユーザ情報、ユーザ名、パスワードなどの重要な情報が保存されています。
- ・ **シャドウコピーの除外セクション**：シャドウコピーまたはボリュームスナップショットのサービスによって、指定のボリューム上のファイルまたはフォルダのバックアップコピーまたはスナップショットが手動または自動で作成されます。

ウイルス検索設定

[グローバル設定] 画面の [デスクトップ / サーバ] タブで、必要に応じて次のオプションをアップデートします。

- ・ **圧縮ファイルの検索制限**：検索対象の圧縮ファイルにおける、解凍後のファイルサイズおよび圧縮ファイル内のファイル数の最大値を指定します。
- ・ **圧縮ファイルのウイルス駆除**：圧縮ファイル内の感染ファイルに対して駆除が試行されます。
- ・ **OLE オブジェクトを {} 階層まで検索**：ここで指定した数の OLE 階層が検索対象となります。OLE は、1 つのアプリケーションでオブジェクトを作成し、別のアプリケーションでそのオブジェクトをリンクしたり埋め込んだりするために使用されます。たとえば、.xls ファイルを .doc ファイルの中に埋め込むことができます。
- ・ **手動検索をクライアントのショートカットメニューに追加**：[ウイルス検索の実行] リンクを右クリックメニューに追加します。このオプションをオンにすると、ユーザはデスクトップ上または Windows エクスプローラ内のファイルまたはフォルダを右クリックしてそのファイルまたはフォルダの手動検索を実行できるようになります。

スパイウェア検索設定

[グローバル設定] 画面の [デスクトップ / サーバ] タブで、必要に応じて次のオプションをアップデートします。

- **Cookie の検索** : Web サイトへのアクセスによってクライアントにダウンロードされたトラッキング Cookie を検索して削除します。検出されたトラッキング Cookie は、[最新ステータス] 画面のスパイウェアカウンタに加算されます。
- **Cookie の数をスパイウェアログに記録する** : 検出されたスパイウェア Cookie をスパイウェアログに追加します。

ファイアウォールを無効にする

[ファイアウォールを無効にしてドライバをアンインストールする] チェックボックスをオンにすると、ビジネスセキュリティクライアントのファイアウォールがアンインストールされ、ファイアウォール関連のドライバが削除されます。別のファイアウォールによりクライアントを保護する場合のみ、これを実行してください。

注意： ファイアウォールを無効にした場合、ファイアウォールを再び有効にするまで関連する設定は使用できません。

Web レピュテーションと承認済み URL

[グローバル設定] 画面の [デスクトップ / サーバ] タブで、必要に応じて次のオプションをアップデートします。

- **ビジネスセキュリティクライアント使用ログを有効にする** : アクセスされた URL の詳細情報をビジネスセキュリティサーバに送信します。
- **承認する URL** : URL を複数指定する場合はセミコロン (;) で区切ります。[追加] をクリックします。

注意： URL を承認リストに追加すると、そのサブドメインもすべて承認されたことになります。

承認済み URL リスト : このリストの URL はブロックされません。エントリを削除するには、対応するごみ箱アイコンをクリックします。

挙動監視

挙動監視は、OS、レジストリエントリ、他のソフトウェア、またはファイルとフォルダが不正に変更されないようにクライアントを保護します。

危険度の低い変更およびその他の監視対象処理に対して、警告メッセージを有効にする： 低リスクの変更または監視対象の操作をユーザに警告します。

インスタントメッセージコンテンツフィルタ

管理者は、インスタントメッセージングアプリケーションでの特定の単語や語句の使用を制限できます。インスタントメッセージングとは、リアルタイムコミュニケーションの一形態で、複数のユーザがテキストを入力してコミュニケーションします。テキストは、ネットワークを介して接続されたクライアントを通して送信されます。

次のインスタントメッセージングアプリケーションで使用されている単語は、ビジネスセキュリティクライアントによって制限できます。

- America Online インスタントメッセージング (AIM) 6 (2008 年 3 月以降にリリースされたビルドはサポート対象外)
- ICQ 6 (2008 年 3 月以降にリリースされたビルドはサポート対象外)
- MSN メッセンジャー 7.5/8.1
- Windows Live メッセンジャー 8.1/8.5
- Yahoo! メッセンジャー 8.1

[グローバル設定] 画面の [デスクトップ / サーバ] タブで、次のようにフィールドを使用します。

- **禁止する単語** — 禁止する単語または語句を追加する場合、このフィールドを使用します。制限する単語または語句は、31 個まで指定できます。1 つの単語または語句の長さは 35 文字までです (2 バイト文字の場合は 17 文字まで)。単一のエントリ、または複数のエントリをセミコロン (;) で区切って入力し、[追加 >>] をクリックします。
- **[禁止する語句] リスト** — このリストの単語や語句は、インスタントメッセージングでの会話では使用できません。エントリを削除するには、対応するごみ箱アイコンをクリックします。

警告設定

[グローバル設定] 画面の [デスクトップ / サーバ] タブで、必要に応じて次のオプションをアップデートします。

- ・ ウイルスパターンファイルがアップデートされていない場合、Windows タスクトレイに警告アイコンを表示 { } 日を経過してもアップデートされていない場合に警告する — 指定の日数が経過してもパターンファイルがアップデートされていないときに、クライアントの画面に警告アイコンを表示します。

監視サービス設定

監視サービスのオプションを設定することで、クライアントが常にビジネスセキュリティクライアントによって保護されます。監視サービスが有効化されているときは、ビジネスセキュリティクライアントが動作しているかどうかの確認が指定の間隔で実行されます。ビジネスセキュリティクライアントが動作していないときは、監視サービスにより再起動が試行されます。

ヒント： ビジネスセキュリティクライアントによってクライアントを確実に保護するために、監視サービスを有効化しておくことをお勧めします。クライアントがハッカーから攻撃されていると、ビジネスセキュリティクライアントが突然停止することがあります。その場合には、監視サービスにより、ビジネスセキュリティクライアントが再起動されます。

[グローバル設定] 画面の [デスクトップ / サーバ] タブで、必要に応じて次のオプションをアップデートします。

- ・ クライアント監視サービスを有効にする
- ・ **クライアントステータスを { } 分ごとに確認** — 監視サービスによるクライアントステータスの確認の間隔を指定します。
- ・ **クライアントを起動できない場合、{ } 回まで再試行** — 監視サービスによるビジネスセキュリティクライアントの再起動を何回試行するかを指定します。

アンインストール設定

[グローバル設定] 画面の [デスクトップ / サーバ] タブで、必要に応じて次のオプションをアップデートします。

- ・ **クライアントユーザによるパスワードを使用しない** — ビジネスセキュリティクライアントのアンインストールを許可する — ユーザがビジネスセキュリティクライアントをアンインストールできるようになります。
- ・ **ビジネスセキュリティクライアントのアンインストールにパスワードを要求する** — 指定のパスワードをユーザが入力するとビジネスセキュリティクライアントをアンインストールできるようになります。

エージェントプログラム

[グローバル設定] 画面の [デスクトップ / サーバ] タブで、必要に応じて次のオプションをアップデートします。

- ・ **クライアントユーザによるパスワードを使用しないコンピュータ上のエージェントプログラムの終了を許可する** — ユーザはビジネスセキュリティクライアントプログラムを終了できるようになります。
- ・ **クライアントユーザにエージェントプログラムを終了するためのパスワードの入力を要求する** — 指定のパスワードをユーザが入力するとビジネスセキュリティクライアントプログラムを終了できるようになります。

システムのオプション

手順: [オプション設定] → [グローバル設定] → [システム] タブ

[グローバル設定] 画面の [システム] セクションには、オフラインのビジネスセキュリティクライアントの自動削除、ビジネスセキュリティクライアントの接続ステータスの確認、および隔離フォルダの保守に関するオプションがあります。

オプション設定 > グローバル設定

グローバル設定は、ネットワーク上のすべてのコンピュータに適用されます。

プロキシ SMTP デスクトップサーバ システム

オフラインビジネスセキュリティクライアントの削除

☐ オフラインビジネスセキュリティクライアントの自動削除機能を有効にする

30 日以上アクセスのないビジネスセキュリティクライアントを自動削除する

接続状態の確認

☒ 接続状態を定期的に確認する

☐ 毎時間
☒ 毎日: 開始時刻 14 : 00 (時:分)
☐ 毎週: 日曜日

接続状態を確認

隔離フォルダ設定

隔離フォルダの容量、および隔離を実行するウイルス感染ファイルの最大サイズを指定してください。この設定は、大規模感染発生時のビジネスセキュリティの処理速度に影響します。

隔離ディレクトリ設定: C:\Program Files (x86)\Trend Micro\Security Server\PCSSRV\Virus

隔離されたファイルの総数: 5

ファイルサイズの合計: 2K バイト

隔離フォルダの容量: 10240 MB

隔離ファイルの最大サイズ: 64 MB

すべての隔離ファイルを削除

保存

図 9-4. [グローバル設定] 画面の [システム] タブ

システムのオプションを設定するには

- [グローバル設定] 画面の [システム] タブで、必要に応じて次のオプションをアップデートします。
 - 136 ページの「オフラインのビジネスセキュリティクライアントを削除する」
 - 137 ページの「クライアントとサーバの接続状態を確認する」
 - 138 ページの「隔離フォルダを管理する」
- [保存] をクリックします。

オフラインのビジネスセキュリティクライアントを削除する

ビジネスセキュリティクライアントをクライアントから削除するためにアンインストールプログラムを実行すると、ビジネスセキュリティサーバへの通知が自動的に送信されます。ビジネスセキュリティサーバがこの通知を受け取ると、クライアントが存在しなくなったことを示すために、セキュリティ設定のグループツリーからクライアントのアイコンが削除されます。

ただし、ビジネスセキュリティクライアントが別の方法（ハードディスクの再フォーマット、クライアントファイルの手動削除など）で削除された場合は、削除されたことをビジネスセキュリティサーバが認識しないため、ビジネスセキュリティクライアントのステータスはオフラインと表示されます。ユーザがビジネスセキュリティクライアントを長期間終了または無効化した場合も、サーバにはビジネスセキュリティクライアントがオフライン状態として表示されます。

セキュリティ設定のグループツリーにアクティブなクライアントだけを表示するには、オフラインのビジネスセキュリティクライアントをセキュリティ設定のグループツリーから自動的に削除するようにビジネスセキュリティサーバを設定します。

オフラインのクライアントを削除するには

1. [グローバル設定] 画面の [システム] タブで、必要に応じて次のオプションをアップデートします。
 - ・ **オフラインビジネスセキュリティクライアントの自動削除機能を有効にする** — ビジネスセキュリティサーバにアクセスしていない期間が指定の日数に達したクライアントを自動的に削除します。
 - ・ **{ } 日以上アクセスのないビジネスセキュリティクライアントを自動削除する** — 許容されるクライアントのオフライン日数を指定します。この日数に達すると、クライアントは管理コンソールから削除されます。
2. [保存] をクリックします。

クライアントとサーバの接続状態を確認する

ビジネスセキュリティでは、クライアントの接続ステータスはセキュリティ設定のグループツリーのアイコンとして表示されます。ただし、何らかの条件によって、セキュリティ設定のグループツリーで表示されているステータスと、クライアントの接続状態が異なる場合があります。たとえば、クライアントのネットワークケーブルが誤って抜かれた場合、クライアントはオフラインであることをビジネスセキュリティサーバに通知できません。このため、セキュリティ設定のグループツリーではこのクライアントはオンラインとして表示されます。

クライアントとサーバの接続状態は手動で確認するか、確認のスケジュールを管理コンソールで設定できます。

注意： 接続状態の確認では、特定のグループまたはクライアントの選択はできません。ビジネスセキュリティサーバに登録されたすべてのクライアントとの接続状態が確認されます。

クライアントとサーバの接続状態を確認するには

1. [グローバル設定] 画面の [システム] タブで、必要に応じて次のオプションをアップデートします。
 - **接続状態の確認** — クライアントとサーバの通信状態の確認をスケジュールに従って自動的に実行します。クライアントとサーバの接続状態の確認をすぐに開始する場合は、[接続状態を確認] をクリックします。
 - **毎時間**
 - **毎日**
 - **毎週**
 - **開始時刻** : 確認を開始する時刻です。
 - **接続状態を確認** — クライアントとサーバの接続状態の確認をすぐに開始します。
2. [保存] をクリックします。

隔離フォルダを管理する

ビジネスセキュリティクライアントが、ファイル中にインターネットからの脅威を検出し、その種類の脅威に対する処理が隔離の場合は、感染したファイルが暗号化されてクライアントの隔離フォルダに移動され、さらにビジネスセキュリティサーバの隔離フォルダに送られます。感染ファイルがビジネスセキュリティによって暗号化されるのは、他のファイルへの感染を防ぐためです。

初期設定では、ビジネスセキュリティクライアントの隔離フォルダは次のディレクトリに設定されます。

C:\Program Files\Trend Micro\Client Server Security Agent\Suspect

初期設定では、ビジネスセキュリティサーバの隔離フォルダは次のディレクトリに設定されます。

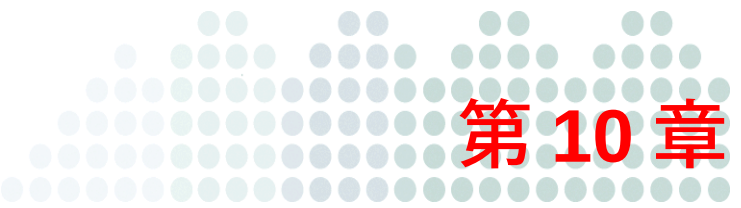
C:\Program Files\Trend Micro\Security Server\PCCSRV\Virus

注意： ネットワーク接続に問題があるなど、何らかの理由で暗号化されたファイルをビジネスセキュリティクライアントがビジネスセキュリティ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されます。ビジネスセキュリティクライアントは、ビジネスセキュリティサーバに再び接続されたときに、ファイルの再送信を試みます。

検索設定、または隔離フォルダの場所変更の詳細については、131 ページの「ウイルス検索設定」を参照してください。

隔離ディレクトリを管理するには

1. [グローバル設定] 画面の [システム] タブで、必要に応じて次のオプションをアップデートします。
 - **隔離フォルダの容量** — 隔離フォルダのサイズを MB 単位で指定します。
 - **隔離ファイルの最大サイズ** — 隔離フォルダに保存される 1 ファイルあたりの最大サイズを MB 単位で指定します。
 - **すべての隔離ファイルを削除** — 隔離フォルダ内のファイルをすべて削除します。フォルダに空き領域がないときは、新しいファイルがアップロードされても、そのファイルは保存されません。
2. [保存] をクリックします。



第10章

アップデートの管理

本章では、手動アップデートと自動アップデートの使用方法和設定方法について説明します。

本章で説明する内容には、次の項目が含まれます。

- 142 ページの「コンポーネントをアップデートする」
- 143 ページの「アップデート可能なコンポーネント」
- 146 ページの「ビジネスセキュリティ サーバのアップデート」
- 146 ページの「アップデート元」
- 151 ページの「手動アップデート」
- 152 ページの「自動アップデート」
- 153 ページの「コンポーネントのロールバックまたは同期」

コンポーネントをアップデートする

Trend Micro ビジネスセキュリティ (以下、ビジネスセキュリティ) では、最新コンポーネントへ容易にアップグレードできるように、ビジネスセキュリティクライアントがアップデートされたコンポーネントを自動的にビジネスセキュリティサーバから取得します。

ビジネスセキュリティのコンポーネントは、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。

- 製品を初めてインストールしたときに、ビジネスセキュリティサーバおよびクライアントのすべてのコンポーネントがただち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されます。
- ビジネスセキュリティマスターサービスの起動ごとに、アップデートサーバにアップデートがあるかどうかの確認が実行されます。
- 初期設定では、自動アップデートが 1 時間ごとに実行され、ビジネスセキュリティサーバがアップデートされます。
- 初期設定では、ビジネスセキュリティクライアントの自動アップデートは 8 時間ごとに実行されます。

ヒント： ビジネスセキュリティサーバに接続していないときも常にビジネスセキュリティクライアントが最新であるようにするには、クライアントがアップデートを代替アップデート元から受け取るように設定します (148 ページの「アップデート元の設定」)。この設定は、頻繁に外出し、ローカル ネットワークに接続できないエンドユーザに便利です。

コンポーネントのアップデートについてトレンドマイクロの推奨設定を使用することにより、中小企業のビジネス環境が適切に保護されます。必要に応じて、手動アップデートを実行したり、自動アップデートの設定を変更したりすることもできます。

アップデート

アップデートは、多くのトレンドマイクロ製品に共通の機能です。トレンドマイクロのアップデート用 Web サイトに接続すると、最新のウイルスパターンファイル、検索エンジン、およびプログラムファイルをインターネット経由でダウンロードできます。ネットワークサービスが中断されたり、OS の再起動が要求されることはありません。

パターンファイルの差分アップデート

アップデートでは、パターンファイルの差分アップデートが可能です。パターンファイル全体を毎回ダウンロードする代わりに、ファイルの新しい部分だけをダウンロードして既存のパターンファイルに付加できます。このような効率的なアップデート方法によって、ウイルス対策ソフトウェアのアップデートに必要な帯域幅が大幅に削減されています。

[アップデート] → [アップデート元] 画面で、トレンドマイクロのアップデートサーバをクリックすると、ビジネスセキュリティサーバの手動および自動コンポーネントアップデートのアップデート元として設定されます。コンポーネントアップデートの時間になると、ビジネスセキュリティサーバからアップデートサーバに直接ポーリングが実行されます。ダウンロード可能な新しいコンポーネントがある場合は、コンポーネントがアップデートサーバからダウンロードされます。

アップデート可能なコンポーネント

最新の脅威から確実にクライアントを保護するには、ビジネスセキュリティのコンポーネントを定期的にアップデートしてください。

トレンドマイクロのアップデートサーバからビジネスセキュリティコンポーネントをダウンロードするようにビジネスセキュリティサーバを設定します。アップデートサーバからは、アップデートされたコンポーネント、たとえばウイルスパターンファイル、検索エンジン、およびプログラムファイルをダウンロードできます。アップデートされたコンポーネントがサーバによってダウンロードされると、自動的にサーバからクライアントに配信されます。

ビジネスセキュリティのコンポーネントをアップデートするには、次の2つの方法があります。

- コンポーネントを手動でアップデートします。151 ページの「コンポーネントの手動アップデート」を参照してください。
- スケジュールに基づいて自動的にコンポーネントをアップデートします。152 ページの「コンポーネントの自動アップデートのスケジュール設定」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する場合は、コンポーネントを正常にダウンロードできるようにプロキシを適切に設定する必要があります。詳細については、126 ページの「インターネットプロキシのオプション」を参照してください。

表 10-1. アップデート可能なコンポーネント

コンポーネント	サブコンポーネント
ウイルス対策	ウイルスパターンファイル ウイルス検索エンジン (32 ビット) ウイルス検索エンジン (64 ビット) 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エンジン (32 ビット) ウイルスクリーンナップエンジン (64 ビット) IntelliTrap 除外パターンファイル IntelliTrap パターンファイル スマートフィードバックエンジン (32 ビット) スマートフィードバックエンジン (64 ビット) スマートスキャンパターン スマートスキャンエージェントパターン
スパイウェア対策	スパイウェア検索エンジン (32 ビット) スパイウェア検索エンジン (64 ビット) 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
Web レピュテーション	URL フィルタエンジン (32 ビット) URL フィルタエンジン (64 ビット)
挙動監視	挙動監視ドライバ 挙動監視コアサービス ポリシー施行パターンファイル デジタル署名パターンファイル 挙動監視制御パターンファイル 挙動監視検出パターンファイル
大規模感染予防	脆弱性診断パターンファイル

表 10-1. アップデート可能なコンポーネント（続き）

コンポーネント	サブコンポーネント
ネットワークウイルス	ファイアウォールパターンファイル ファイアウォールドライバ (32 ビット) ファイアウォールドライバ (64 ビット) TDI ドライバ (32 ビット) TDI ドライバ (64 ビット) WFP ドライバ (32 ビット) WFP ドライバ (64 ビット)

各コンポーネントの詳細については、17 ページの「コンポーネント」を参照してください。

初期設定のアップデート時刻

ビジネスセキュリティの初期設定では、必要に応じてコンポーネントのアップデートがチェックされ、次のような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がダウンロードされます。

- 製品を初めてインストールしたときに、ビジネスセキュリティサーバおよびクライアントのすべてのコンポーネントがただち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されます。
- ビジネスセキュリティのマスターサービスが起動したときは常に、ビジネスセキュリティサーバによって大規模感染予防ポリシーがアップデートされます。
- 初期設定では、自動アップデートが 1 時間ごとに実行され、ビジネスセキュリティサーバがアップデートされます。
- クライアントを最新の状態に保つために、ビジネスセキュリティクライアントでは、8 時間ごとに自動アップデートが実行されます。

コンポーネントのアップデートについてトレンドマイクロの推奨設定を使用することにより、中小企業のビジネス環境が適切に保護されます。必要に応じて、手動アップデートを実行したり、自動アップデートの設定を変更したりすることもできます。

基本的に、検索エンジンやプログラムがアップデートされるのはビジネスセキュリティの新しいバージョンがリリースされるときだけです。ただし、パターンファイルは頻繁にリリースされます。

ビジネスセキュリティ サーバのアップデート

ビジネスセキュリティでは、以下のアップデートが自動的に実行されます。

- ・ 製品を初めてインストールしたときに、ビジネスセキュリティサーバおよびクライアントのすべてのコンポーネントがただち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されます。
- ・ ビジネスセキュリティが起動するたびに、ビジネスセキュリティサーバによってコンポーネントおよび大規模感染予防ポリシーがアップデートされます。
- ・ 初期設定では、自動アップデートは 1 時間ごとに実行されます。
- ・ クライアントを常に最新の状態に保つために、ビジネスセキュリティクライアントによって自動アップデートが 8 時間ごとに実行されます。

アップデートを実行するようにビジネスセキュリティサーバを設定するには

1. アップデート元を選択します。詳細については、146 ページの「アップデート元」を参照してください。
2. 手動または自動のアップデートを実行するようにビジネスセキュリティサーバを設定します。詳細については、151 ページの「手動アップデート」および 152 ページの「自動アップデート」を参照してください。
3. [クライアント権限] を使用して、クライアントのアップデートオプションを設定します。

アップデート元

ビジネスセキュリティクライアントのアップデート場所を選択するときは、クライアントとアップデート元との間の帯域幅を考慮します。次の表は、さまざまなコンポーネントのアップデートオプションとそれらを使用する場合の推奨事項を示しています。

表 10-2. アップデート元のオプション

アップデートオプション	説明	推奨使用場面
[アップデート] → [アップデート元] → [サーバ]	ビジネスセキュリティサーバは、アップデートサーバ (または別のアップデート元) からアップデートされたコンポーネントを受信して、それらを直接クライアントに配信します。	ビジネスセキュリティサーバとクライアントの間のネットワークに「低帯域幅」の部分がない場合に、この方法を使用します。

表 10-2. アップデート元のオプション（続き）

アップデートオプション	説明	推奨使用場面
[アップデート] → [アップデート元] → [アップデートエージェント]	ビジネスセキュリティサーバは、アップデートサーバ（または別のアップデート元）からアップデートされたコンポーネントを受信して、それらを直接アップデートエージェントに配信します。アップデートエージェントがクライアントにコンポーネントを配信します。	ビジネスセキュリティサーバとクライアントの間のネットワークに「低帯域幅」の部分がある場合に、この方法を使用するとネットワークのトラフィック負荷を分散させることができます。
[アップデート] → [アップデート元] → [アップデートエージェント]	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直接アップデートサーバ（または他のアップデートエージェント）から受信してクライアントに配信します。	アップデートエージェントをビジネスセキュリティ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できない場合にのみ、この方法を使用します。ほとんどの場合、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アップデートを受信するよりも、ビジネスセキュリティサーバまたは別のアップデートエージェントからアップデートを受信した方が高速です。

アップデート元の設定

手順: [アップデート] → [アップデート元]

アップデート元

コンポーネントのアップデート元を選択する場合は、クライアントとアップデート元との間のネットワークのセクションの帯域幅を考慮してください。

サーバ アップデートエージェント

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
(<http://beta.external.trendmicro.com/activeupdate/activeupdate.ashx>)

☐ 最新ファイルのコピーが格納されたイントラネット上のフォルダ
UNCパス:
例: \\w-server\download
ユーザ名:
パスワード:

☐ 代替のアップデート元
URL:

保存

図 10-1. [アップデート元] 画面

ビジネスセキュリティサーバのアップデート元を設定するには

1. [アップデート元] 画面で、必要に応じて次のオプションをアップデートします。
 - **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] は、ダウンロード元の初期設定です。新しいコンポーネントは、ダウンロード可能になるとすぐに、トレンドマイクロのアップデートサーバにアップロードされます。アップロードを頻繁に、適切なタイミングで実行する必要がある場合は、トレンドマイクロのアップデートサーバをアップデート元として選択してください。

注意： 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を設定する場合は、アップデートを受け取るすべてのサーバがそのアップデート元にアクセスできる必要があります。

- **最新ファイルのコピーが格納されたイントラネット上のフォルダ** アップデートされたコンポーネントをイントラネット内のアップデート元が受信し、このアップデート元からコンポーネントをダウンロードします。ネットワーク上の別のサーバの UNC パスを入力し、このサーバ上にディレクトリを共有フォルダとして用意して、アップデートを受け取るすべてのサーバからアクセスできるように設定します (たとえば ¥Web¥ActiveUpdate)。

- ・ **代替のアップデート元** — インターネットまたはその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します。最新コンポーネントを受け取るすべてのサーバからアップデート元の HTTP 仮想ディレクトリ (Web 共有) にアクセスできるようにします。

2. [保存] をクリックします。

アップデートエージェントの使用

手順: [アップデート] → [アップデート元] → [アップデートエージェント] タブ

ビジネスセキュリティクライアントとビジネスセキュリティサーバ間のネットワーク部分が「帯域幅が狭い」または「トラフィックが大きい」と認識された場合、特定のビジネスセキュリティクライアントをアップデートエージェントとして指定して、他のビジネスセキュリティクライアントに対するアップデート元の役割を持たせることができます。これにより、すべてのクライアントにコンポーネントを配信する際の負荷を分散できます。

たとえば、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のトラフィック負荷が大きい場合は、セグメントごとに 1 つ以上のビジネスセキュリティクライアントをアップデートエージェントとして機能させることをお勧めします。

ビジネスセキュリティクライアントにアップデートエージェントの役割を持たせるには

1. [アップデート元] 画面の [アップデートエージェント] タブを選択し、[アップデートエージェントの割り当て] セクションの [追加] をクリックします。
2. [クライアントの選択] リストボックスから、アップデートエージェントとして機能させる 1 つ以上のビジネスセキュリティクライアントを選択します。
3. [保存] をクリックします。
アップデートエージェントを削除するには、[コンピュータ名] の対応するチェックボックスをオンにして [削除] をクリックします。

注意: [代替のアップデート元] セクションが特に指定されていない場合は、すべてのアップデートエージェントがアップデートをビジネスセキュリティサーバから受け取ります。

ビジネスセキュリティクライアントが別のアップデート元からアップデートを取得できるようにするには

1. [アップデート元] 画面の [アップデートエージェント] タブで、必要に応じて次のオプションをアップデートします。
 - ・ ビジネスセキュリティクライアントおよびアップデートエージェントの代替のアップデート元を有効にします。

- 必ずビジネスセキュリティからアップデートエージェントをアップデートします — この手順は省略可能です。アップデートエージェントがアップデートをビジネスセキュリティサーバからのみ受け取るようにする場合に指定します。

注意： このオプションが選択されている場合、アップデートエージェントは、IP アドレスが [代替アップデート元の追加] 画面で指定した範囲内にあっても、ビジネスセキュリティサーバからアップデートをダウンロードします。このオプションを有効にするには、[ビジネスセキュリティクライアントおよびアップデートエージェントの代替のアップデート元を有効にします] を選択する必要があります。

2. [保存] をクリックします。

代替アップデート元を追加するには

1. [アップデート元] 画面の [アップデートエージェント] タブを選択し、[代替のアップデート元] セクションの [追加] をクリックします。
2. 必要に応じて次のオプションをアップデートします。
 - [開始 IP アドレス] と [終了 IP アドレス]。クライアントの IP アドレスがこの範囲にある場合は、そのクライアントはアップデートを指定のアップデート元から受け取ります。

注意： 単一のビジネスセキュリティクライアントを指定するには、[開始 IP アドレス] と [終了 IP アドレス] の両フィールドにビジネスセキュリティクライアントの IP アドレスを入力します。

- アップデート元

アップデートエージェント — ドロップダウンリストが使用できない場合は、アップデートエージェントが設定されていません。

指定 — アップデートエージェントまたはアップデートサーバへのパスです。

3. [保存] をクリックします。

代替アップデート元を削除するには、[IP 範囲] の対応するチェックボックスをオンにして [削除] をクリックします。

注意： 指定されていないビジネスセキュリティクライアントは自動的に、アップデートをビジネスセキュリティサーバから受け取ります。

手動アップデート

手順:[アップデート]→[手動アップデート]

ビジネスセキュリティサーバでは、コンポーネントを使用して、脅威の検索と特定、およびデスクトップとサーバの保護とウイルス駆除に役立つようにダメージクリーンアップが実行されます。コンポーネントを最新に保つことが不可欠です。[今すぐアップデート]をクリックすると、ビジネスセキュリティサーバでは、アップデートされたコンポーネントが検索されます。アップデートされたコンポーネントが利用可能な場合、ビジネスセキュリティサーバはそれらのコンポーネントをダウンロードして、クライアントへの配信を開始します。

[手動アップデート] 画面には、次の項目が含まれます。

- ・ **コンポーネント** — 画面上のすべての項目を選択またはクリアします。
- ・ **現在のバージョン** — コンポーネントの現在のバージョンが表示されます。必ずしも最新バージョンではありません。
- ・ **前回のアップデート** — ビジネスセキュリティサーバがコンポーネントをダウンロードした前回の情報が表示されます。

コンポーネントの手動アップデート

手順:[アップデート]→[手動アップデート]

アップデートするコンポーネントを選択して、[今すぐアップデート]をクリックします。

☒ コンポーネント	現在のバージョン	前回のアップデート
☐ ☒ ウイルス対策		
☐ ☒ スパイウェア対策		
☒ スパイウェア検索エンジン (32ビット)	6.2.3009	2009/07/07 12:38:08
☒ スパイウェア検索エンジン (64ビット)	6.2.3009	2009/07/07 12:38:09
☒ スパイウェアパターンファイル	6.39	2009/07/07 12:41:50
☒ スパイウェア監視/パターンファイル	0.771.00	2009/07/07 12:35:35
☐ ☒ Webレピュテーション		
☐ ☒ 挙動監視		
☐ ☒ 大規模感染予防		
☐ ☒ ネットワークウイルス		

今すぐアップデート

図 10-2. 手動アップデート画面

コンポーネントを手動でアップデートするには

1. [手動アップデート] 画面で、必要に応じて次のオプションをアップデートします。
 - ・ **コンポーネント** — すべてのコンポーネントを選択するには、[コンポーネント] チェックボックスをオンにします。コンポーネントを1つずつ選択するには、 をクリックしてアップデートするコンポーネントを表示してから、対応するチェックボックスをオンにします。各コンポーネントの詳細については、143 ページの「アップデート可能なコンポーネント」を参照してください。
2. [今すぐアップデート] をクリックします。自動アップデートの場合は、152 ページの「コンポーネントの自動アップデートのスケジュール設定」を参照してください。

注意： アップデートされたコンポーネントがサーバにダウンロードされると、自動的にサーバからビジネスセキュリティクライアントにインストールされます。

自動アップデート

ビジネスセキュリティサーバでは、コンポーネントを使用して、脅威の検索と特定、およびデスクトップとサーバの保護とウイルス駆除に役立つようにダメージクリーンアップタスクが実行されます。コンポーネントを最新に保つことが不可欠です。[今すぐアップデート] をクリックすると、ビジネスセキュリティサーバでは、アップデートされたコンポーネントが検索されます。アップデートされたコンポーネントが利用可能な場合、ビジネスセキュリティサーバはそれらのコンポーネントをダウンロードして、クライアントへのインストールを開始します。

コンポーネントの自動アップデートのスケジュール設定

手順： [アップデート] → [自動アップデート] → [スケジュール] タブ

脅威に対処するための最新のコンポーネントを自動的に受け取るように、アップデートのスケジュールを設定します。

ヒント： 検索と更新を同時に実行するようにスケジュールしないでください。自動アップデートと同じ時刻にスケジュールすると、予約検索が途中で中断される可能性があります。

アップデート > 自動アップデート

コンポーネント スケジュール

☐ 毎時間

☒ 毎日

☐ 毎週: 日曜日

☐ 毎月: 日 1

開始時刻 14:45 (時分) アップデート期間 1 時間

保存

図 10-3. [自動アップデート] 画面

自動アップデートのスケジュールを設定するには

1. [コンポーネント] タブで、アップデートするコンポーネントを選択します。すべてのコンポーネントを選択するには、[コンポーネント] の横のチェックボックスをオンにします。
2. [スケジュール] タブで、コンポーネントをアップデートする頻度を選択します。
3. [保存] をクリックします。

ヒント： ウイルス大規模感染の発生時に、トレンドマイクロではウイルスパターンファイルを迅速にアップデートして対応します。アップデートが週に 2 回以上発行される場合もあります。検索エンジンおよびその他のコンポーネントも、定期的にアップデートされます。ビジネスセキュリティクライアントのコンポーネントを常に最新にするために、コンポーネントのアップデートは 1 日に 1 回 (大規模感染の発生時はそれよりも頻繁に) 行うことをお勧めします。

コンポーネントのロールバックまたは同期

手順: [アップデート] → [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または検索エンジンを 1 つ前のバージョンに戻すことを指します。使用しているパターンファイルや検索エンジンが正常に機能しない場合に、これらのコンポーネントを 1 つ前のバージョンに戻します。

同期とは、アップデートされたコンポーネントをすべてのビジネスセキュリティクライアントにインストールすることです。

ビジネスセキュリティクライアントで使用する検索エンジンは次のとおりです。

- 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
- ウイルス検索エンジン (32 ビット)
- ウイルス検索エンジン (64 ビット)

検索エンジンごとにロールバックを実行する必要があります。ロールバックの手順はすべて同じです。ビジネスセキュリティサーバでは、使用中のバージョンと 1 つ前のバージョンの検索エンジンとパターンファイルのみを保持します。

コンポーネントのステータス						
コンポーネント	現在のバージョン	前回のアップデート	前のバージョン	前回のアップデート	同期	1つ前のバージョンにロールバック
ウイルスパターンファイル	6.143.50	2009/07/07 17:00:32	5.259.00	2009/07/07 12:35:31	同期	ロールバック
ウイルス検索エンジン (32ビット)	8.950.1094	2009/07/07 12:38:06	N/A	N/A	同期	ロールバック
スマートスキャンエージェントパターン	6.213.00	2009/07/07 14:26:46	6.143.00	2009/05/22 6:37:46	同期	ロールバック
ウイルス検索エンジン (64ビット)	8.950.1094	2009/07/07 12:38:06	N/A	N/A	同期	ロールバック

図 10-4. [ロールバック] 画面

パターンファイルまたは検索エンジンのロールバックまたは同期を実行するには

[ロールバック] 画面で、必要に応じて次のオプションを選択します。

- **ロールバック** — ビジネスセキュリティサーバおよびクライアントのコンポーネントを、前のバージョンに戻します。
- **同期** — アップデートされたコンポーネントをビジネスセキュリティクライアントにインストールします。

HotFix、Patch、および Service Pack

製品の正式リリース後、トレンドマイクロでは、問題への対処、製品のパフォーマンスの強化、または新機能の追加のために、HotFix、Patch、および Service Pack を開発しています。

トレンドマイクロでリリースする可能性のあるものの概要は、次のとおりです。

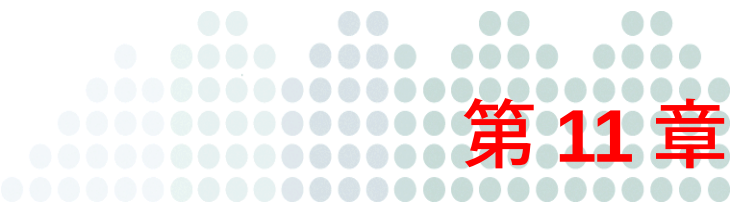
- **HotFix:** お客さまから報告された問題に対する回避策や解決方法です。HotFix は、お客さま固有の問題に対応するものであるため、すべてのお客さまに配布されるものではありません。
- **Critical Patch / Security Patch:** セキュリティ上の問題に対応する修正モジュールで、すべてのお客さまに対して公開されます。

- Patch: HotFix と Security Patch が 1 つにまとめられたもので、複数の問題を解決します。トレンドマイクロは、定期的に Patch を公開しています。
- Service Pack: HotFix と Patch が統合され、大幅な機能拡張が含まれている修正プログラムで、製品のアップグレードに相当します。

これらのリリースが可能になったときに、ベンダーまたはサポートプロバイダから連絡がくる場合があります。下記のトレンドマイクロの Web サイトで、新しい HotFix、Patch、または Service Pack のリリースに関する情報を確認してください。

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

すべてのリリースには、製品のインストール、インストール、および設定に必要な情報を記載した Readme ファイルが含まれています。Readme ファイルをよくお読みのうえ、HotFix、Patch、または Service Pack のファイルをインストールしてください。



第11章

ログとレポートの使用

本章では、ログとレポートを使用してシステムを監視しウイルス対策を分析する方法について説明します。

本章で説明する内容には、次の項目が含まれます。

- 158 ページの「ログ」
- 161 ページの「レポート」
- 166 ページの「ログとレポートを管理する」

ログ

Trend Micro ビジネスセキュリティ (以下、ビジネスセキュリティ) 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が保存されます。これらのログは、組織のウイルス対策ポリシーの査定や、感染リスクの高いクライアントの特定に使用します。また、アップデートが正常にインストールされたかどうかを確認するときもこれらのログを使用します。

注意： CSV ログファイルを表示するには、Microsoft Excel などの表計算ソフトなどを使用してください。

ビジネスセキュリティでは、次の種類のログが管理されます。

- 管理コンソールイベントログ
- デスクトップ / サーバログ

表 11-1. ログの種類と内容

種類 (ログエントリを生成したイベントまたは項目)	ログの内容 (内容を取得するログの種類)
管理コンソールイベント	手動検索 アップデート 大規模感染予防 コンソールイベント

表 11-1. ログの種類と内容（続き）

種類 (ログエントリを生成した イベントまたは項目)	ログの内容 (内容を取得するログの種類)
デスクトップ / サーバイベント	ウイルスログ 手動検索 リアルタイム検索 予約検索 クリーンナップ スパイウェアログ 手動検索 リアルタイム検索 予約検索 Web レピュテーションログ URL フィルタログ 挙動監視ログ アップデートログ ネットワークウイルスログ 大規模感染予防ログ イベントログ

ログクエリの使用

手順:[レポート]→[ログクエリ]

ログクエリは、ログデータベースから情報を収集するときに実行します。クエリの設定と実行には、[ログクエリ] 画面を使用します。結果は、CSV ファイル形式でエクスポートするか、印刷できます。

図 11-1. 初期設定の [ログクエリ] 画面

ログを表示するには

- [ログクエリ] 画面で、必要に応じて次のオプションをアップデートします。
 - クエリ対象
 - プルダウンメニューから選択
 - 表示期間を指定: クエリを特定の期間に限定する場合に指定します。
 - 種類 — 各ログの種類の内容については、158 ページの表 11-1 を参照してください。
 - 管理コンソールイベント
 - デスクトップ/サーバ
 - ログの内容 — 選択できるオプションは、ログの [種類] によって異なります。
- [ログの表示] をクリックします。

ログを CSV 形式で保存するには、[エクスポート] をクリックします。CSV ファイルを表示するには、表計算ソフトウェアを使用してください。

レポート > ログクエリ > 管理コンソールイベントログ		
開始日 2008/06/06 0:00:00 終了日 2008/06/13 23:59:59		ページごとの表示数 10
エクスポート		合計: 8 件 14 ページ 1 / 1
日時	コンピュータ	説明
2008/06/13 14:47:46		大規模感染予防BICAR_TEST_FILEが有効になりました。
2008/06/13 14:45:30		大規模感染予防BICAR_TEST_FILEが有効になりました。
2008/06/13 14:42:53		大規模感染予防BICAR_TEST_FILEが無効になりました。
2008/06/13 14:40:15		大規模感染予防BICAR_TEST_FILEが有効になりました。
2008/06/13 14:35:55		大規模感染予防BICAR_TEST_FILEが無効になりました。
2008/06/13 14:25:34		大規模感染予防BICAR_TEST_FILEが有効になりました。
2008/06/13 14:25:27		大規模感染予防BICAR_TEST_FILEが無効になりました。
2008/06/13 12:36:22		大規模感染予防BICAR_TEST_FILEが有効になりました。

図 11-2. [ログクエリ] 画面の例

レポート

ここでは、1 回限りのレポートと予約レポートの両方の設定方法を説明します。

1 回限りのレポート

「1 回限りのレポート」は、ログ情報を整理して視覚的にわかりやすくまとめた形式で表示するときに生成します。

予約レポート

予約レポートの内容は 1 回限りのレポートに似ていますが、日時と頻度を指定して生成する点異なります。予約レポートを生成するには、レポートの内容を選択してテンプレートとして保存します。このテンプレートが使用され、指定の日時と頻度でレポートが生成されます。

レポートについて

ビジネスセキュリティのレポートには、以下に示す情報が表示されます。表示される情報は、選択されたオプションによって異なることがあります。

表 11-2. レポートの内容

レポート項目	説明
ウイルス対策	デスクトップ / サーバのウイルス概要 ウイルスレポートには、検索エンジンによって検出されて処理が実行されたウイルス / 不正プログラムの数と種類に関する詳細情報が表示されます。また、検出数の多いウイルス / 不正プログラムの名前の一覧も表示されます。ウイルス / 不正プログラムの名前をクリックすると、新しい Web ブラウザページが開いてトレンドマイクロのウイルス情報ページが表示され、そのウイルス / 不正プログラムの詳細情報を読むことができます。 ウイルスが検出されたデスクトップ / サーバの上位 5 件 ウイルス / 不正プログラムの検出を報告しているデスクトップまたはサーバの上位 5 件が表示されます。同じクライアントでウイルス / 不正プログラムが頻繁に検出される場合は、高いセキュリティリスクがあることを示している可能性があります、詳細の調査が必要です。
大規模感染予防の履歴	大規模感染予防の履歴 最近の大規模感染の一覧とその重大度が表示されます。また、大規模感染を引き起こしたウイルス / 不正プログラムの名前と、その伝播手段（メールまたはファイル）も表示されます。
スパイウェア対策	デスクトップ / サーバのスパイウェア / グレーウェア概要 スパイウェア / グレーウェアレポートには、クライアントで検出されたスパイウェア / グレーウェアの詳細情報（検出数やビジネスセキュリティによって実行された処理など）が表示されます。このレポートには、スパイウェア検索時に実行された各処理の比率を表す円グラフも表示されます。 スパイウェアが検出されたデスクトップ / サーバの上位 5 件 検出されたスパイウェア / グレーウェアの上位 5 件、およびスパイウェア / グレーウェア検出数の多いデスクトップ / サーバの上位 5 件もレポートに表示されます。検出されたスパイウェア / グレーウェアの詳細情報を参照するには、スパイウェア / グレーウェアの名前をクリックします。新しい Web ブラウザページが開き、トレンドマイクロ Web サイトに掲載されているそのスパイウェア / グレーウェアの関連情報が表示されます。
Web レピュテーション	Web レピュテーションポリシー違反のあったコンピュータの上位 10 件 Web レピュテーションポリシーに違反したクライアントの上位 10 件のリストです。

表 11-2. レポートの内容 (続き)

レポート項目	説明
URL カテゴリ	違反のあった URL カテゴリポリシーの上位 5 件 最も頻繁にアクセスされたポリシー違反 Web サイトカテゴリのリストです。 URL カテゴリポリシー違反のあったコンピュータの上位 10 件 URL フィルタポリシーに違反したコンピュータの上位 10 件のリストです。
挙動監視	挙動監視ポリシー違反のあったプログラムの上位 5 件 挙動監視ポリシーに違反したプログラムの上位 5 件のリストです。 挙動監視ポリシー違反のあったコンピュータの上位 10 件 挙動監視ポリシーに違反したクライアントの上位 10 件のリストです。
ネットワークウイルス	検出されたネットワークウイルスの上位 10 件 ファイアウォールドライバによって検出されたネットワークウイルスの中で頻度の多い上位 10 件のリストです。 ウイルスの名前をクリックすると、新しい Web ブラウザページが開いてトレンドマイクロのウイルス情報ページが表示され、そのウイルスの詳細情報を読むことができます。 攻撃されたコンピュータ上位 10 件 ネットワーク上のクライアントのうち、報告されたウイルスの検出数が多かった上位 10 件のリストです。

レポートを生成する

手順: [レポート] → [1 回限りのレポート] または [予約レポート]

1 回限りのレポートとは、選択されているコンテンツを 1 回だけ集計するものです。予約レポートでは、選択されているコンテンツの集計が定期的に作成されます。

レポート > 1回限りのレポート > レポートテンプレートの追加 

レポート名:

レポート生成期間

開始日: :
yyyy/MM/dd 時 分

終了日: :
yyyy/MM/dd 時 分

レポートの内容 ☐ すべて選択

☐	ウイルス対策
☐	大規模感染予防の履歴
☐	スパイウェア対策
☐	Webレピュテーション
☐	URLカテゴリ
☐	挙動監視
☐	コンテンツフィルタ
☐	ネットワークウイルス

レポートの送信

☐ レポートの送信先:
例: user1@domain.com;user2@domain.com
(複数の項目を指定する場合は、セミコロン (;) で区切って入力してください)

☒ PDF添付ファイルとして

☐ レポートへのリンクとして

図 11-3. [レポート] 画面

レポートを作成または予約するには

1. [1 回限りのレポート] 画面または [予約レポート] 画面で、[追加] をクリックします。
2. 必要に応じて次のオプションをアップデートします。
 - ・ レポート名 / レポートテンプレート名: レポート / テンプレートを区別するための短いタイトルです。

- **スケジュール** — 設定できるのは予約レポートの場合のみです。
 - **毎日** — 毎日、指定の時刻に予約検索を実行します。
 - **毎週** — 週 1 回、指定の曜日の指定の時刻に予約検索を実行します。
 - **毎月** : 日 — 月 1 回、指定の日の指定の時刻に予約検索を実行します。31 を選択した場合は、30 日しかない月のレポートは生成されません。
 - **生成開始時刻** — ビジネスセキュリティがレポート生成を実行する時刻です。
 - **レポート生成期間** — 日付を限定してレポートを作成します。
 - **レポートの内容** — すべての脅威を選択するには、[すべて選択] チェックボックスをオンにします。脅威を 1 つずつ選択するには、対応するチェックボックスをオンにします。 をクリックすると内容が展開されます。
 - **レポートの送信先** — ビジネスセキュリティによって生成レポートを指定の受信者に送信します。複数のエントリはセミコロン (;) で区切ります。
 - PDF 添付ファイルとして
 - レポートへのリンクとして
3. [追加] をクリックします。レポートを [1 回限りのレポート] 画面または [予約レポート] 画面で表示するには、レポートの名前をクリックします。[レポートの送信先] がオンの場合は、PDF 形式の添付ファイルまたはリンクが受信者に送信されます。
- レポートを削除するには、[1 回限りのレポート] 画面または [予約レポート] 画面でそのレポートに対応するチェックボックスをオンにして [削除] をクリックします。
- 予約レポートのテンプレートを編集するには、[予約レポート] 画面でテンプレートの名前をクリックし、オプションを必要に応じてアップデートします。

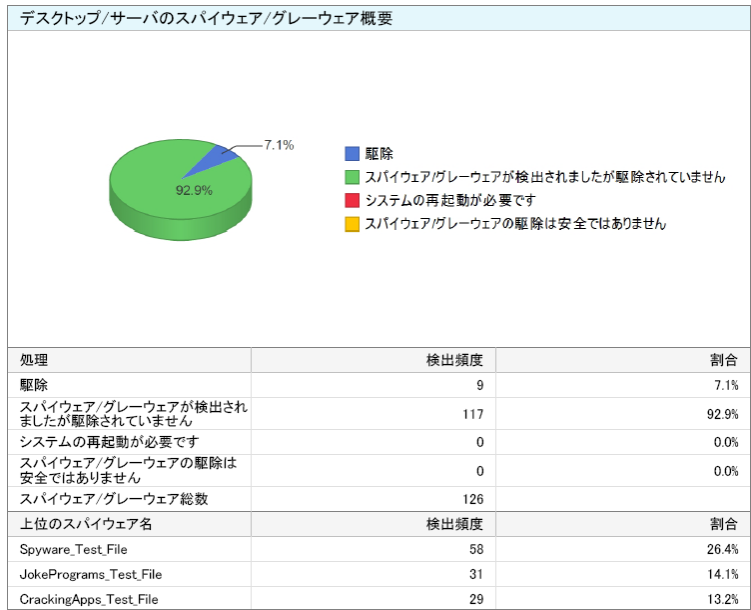


図 11-4. スパイウェア/グレーウェアの集計が表示されているレポートの例

ログとレポートを管理する

レポートは、定期的に削除しないと、量が急激に増えることがあります。レポートの削除には時間と手間がかかりますが、ビジネスセキュリティにはこの作業を自動化する機能があります。レポートはログを基に作成されるので、ログの情報が削除されると、それ以降レポートは生成されなくなります。

レポートを管理する

手順: [レポート] → [管理] → [レポート] タブ

レポート > 管理

レポート

ログの自動削除

ログの手動削除

保持するレポートの最大数を指定します。

レポートの種類	保持するレポートの最大数 (1~100)
1回限りのレポート	10
各テンプレートに保存された予約レポート	10
レポートテンプレート	10

保存

図 11-5. レポート管理画面

レポートは、定期的に削除しないと、量が急激に増えることがあります。レポートの削除には時間と手間がかかりますが、ビジネスセキュリティにはこの作業を自動化する機能があります。レポートはログを基に作成されるので、ログの情報が削除されると、それ以降レポートは生成されなくなります。この画面では、次のことが可能です。

レポートの管理

保持するレポートの最大数を設定するには

- [管理] 画面の [レポート] タブで、次の項目についてレポートの最大数を設定します。
 - 1 回限りのレポート
 - 各テンプレートに保存された予約レポート
 - レポートテンプレート
- [保存] をクリックします。

ログの自動削除

ログを自動的に削除するには

- [管理] 画面の [ログの自動削除] タブで、[ログの種類] を選択し、その種類のログを保存する日数を指定します。
- [保存] をクリックします。

ログの手動削除

手動でログを削除するには

1. [管理] 画面の [ログの手動削除] タブで、ログの種類を選択して保存日数を指定し、ログの種類に対応する [削除] をクリックします。
2. [保存] をクリックします。

ヒント： ログをすべて削除するには、日数に 0 を指定して [削除] をクリックします。

ログを削除する

[レポート] → [管理] 画面を使用して、ログファイルの保存期間を設定し、定期的なログ管理のスケジュールを設定します。

手順：[レポート] → [管理] → [ログの自動削除] タブ

レポート > 管理

レポート ログの自動削除 ログの手動削除

古いログの自動削除基準を設定します。
注意レポート作成の際、ログから情報を取得します。ログを削除すると、レポート作成に必要な情報が削除される可能性があります。

ビジネスセキュリティ

ログの種類	最初のログエントリ	最新のログエントリ	次の日数を経過したログを削除
☒ 手動検索ログ	N/A	N/A	30 日
☒ アップデートログ	2008/06/12 14:48:57	2008/06/13 15:26:49	30 日
☒ 大規模感染予防ログ	2008/06/13 12:36:22	2008/06/13 14:47:46	30 日
☒ コンソールイベントログ	2008/06/12 14:49:02	2008/06/12 16:06:04	30 日

デスクトップサーバ

ログの種類	最初のログエントリ	最新のログエントリ	次の日数を経過したログを削除
☒ デスクトップサーバログ	2008/06/12 15:25:16	2008/06/12 15:25:16	30 日

図 11-6. [ログの自動削除] 画面

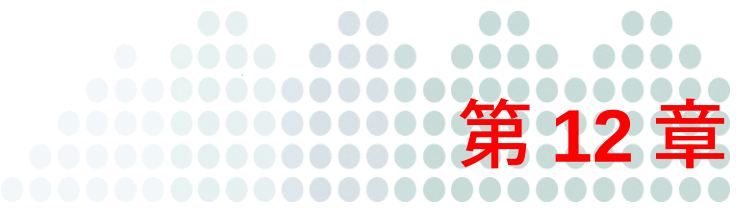
設定時間制限を超過したログを削除するようにビジネスセキュリティサーバを設定するには

1. [レポート] → [管理] をクリックします。
2. [ログの自動削除] をクリックします。
3. 削除するログを選択します。

4. [次の日数を経過したログを削除] で、ビジネスセキュリティサーバがログを保持する日数を入力します。
5. [保存] をクリックします。手順 4 で指定した日数より古いすべてのログがビジネスセキュリティサーバで削除されます。

手動でログを削除するには

1. [ログの手動削除] をクリックします。
2. 削除するログの種類が表示されている行を検索します。時間制限を示す日数の横にあるフィールドで数値を入力します。
3. [削除] をクリックします。手順 2 で指定した日数より古いすべてのログが削除されます。



第12章

ビジネスセキュリティの管理

本章では、製品ライセンスの表示、プラグインマネージャの操作、ビジネスセキュリティサーバのアンインストールなどの管理タスクの実行方法について説明します。

本章で説明する内容には、次の項目が含まれます。

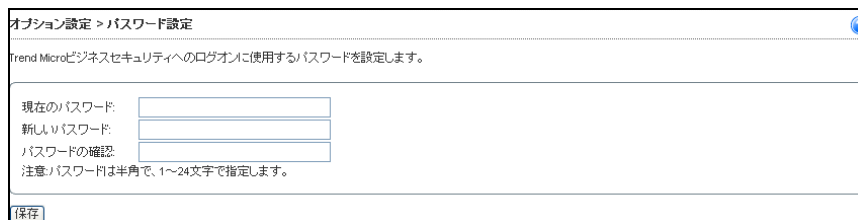
- 172 ページの「管理コンソールのパスワードを変更する」
- 173 ページの「プラグインマネージャを使用する」
- 173 ページの「製品ライセンスの詳細を表示する」
- 175 ページの「Trend Micro Smart Protection Network に参加する」
- 176 ページの「ビジネスセキュリティ サーバをアンインストールする」
- 176 ページの「ビジネスセキュリティ サーバをアンインストールする」

管理コンソールのパスワードを変更する

権限のないユーザが設定内容を変更したり、ビジネスセキュリティクライアントをコンピュータから削除したりできないように、管理コンソールはパスワードで保護されています。パスワードは Trend Micro ビジネスセキュリティ（以下、ビジネスセキュリティ）のインストール時に指定しますが、管理コンソールから変更することもできます。

ヒント： 管理コンソールのパスワードには、複雑なパスワードを使用することをお勧めします。複雑なパスワードとは、1 つ以上の大文字（A ～ Z）、1 つ以上の小文字（a ～ z）、1 つ以上の数字（0 ～ 9）、および 1 つ以上の特殊記号または句読点（!@#\$\$%^&.,;:?'）を含む 8 文字以上のパスワードです。このパスワードには、ユーザのログイン名と同じものではなく、パスワードそのものにログイン名が含まれていないことも要求されます。また、ユーザの姓名や生年月日など、ユーザを簡単に特定できるような項目を含めることもできません。

手順：[オプション設定] → [パスワード設定]



オプション設定 > パスワード設定

Trend Microビジネスセキュリティへのログインに使用するパスワードを設定します。

現在のパスワード:

新しいパスワード:

パスワードの確認:

注意/パスワードは半角で、1～24文字で指定します。

図 12-1. [オプション設定]-[パスワード設定] 画面

管理コンソールのパスワードを変更するには

- [パスワード設定] 画面で、必要に応じて次のオプションをアップデートします。
 - 現在のパスワード
 - 新しいパスワード
 - パスワードの確認 確認のために、新しいパスワードをもう一度入力します。
- [保存] をクリックします。

注意： 管理コンソールのパスワードを忘れた場合は、ビジネスセキュリティを削除して再インストールする必要があります。詳細については、176 ページの「ビジネスセキュリティ サーバをアンインストールする」を参照してください。

プラグインマネージャを使用する

手順：[オプション設定]→[プラグインマネージャ]

プラグインマネージャとは、ビジネスセキュリティとビジネスセキュリティクライアントのプログラムが利用可能になったとき、すぐに管理コンソールに表示するための機能です。これらのプログラムのインストールと管理は管理コンソールから実行できます。たとえば、クライアント用プラグインプログラムをビジネスセキュリティクライアントにインストールできます。

プラグインマネージャをダウンロードしてインストールするには、管理コンソールのメインメニューの [プラグインマネージャ] をクリックします。インストールが完了すると、利用可能なプラグインプログラムの確認ができるようになります。

詳細については、プラグインのドキュメントを参照してください。

2009 年 8 月現在、使用できるプラグインは公開されていません。

製品ライセンスの詳細を表示する

手順：[オプション設定]→[製品ライセンス]

製品ライセンス画面では、製品ライセンスの更新、アップグレード、および詳細情報の表示を実行できます。



図 12-2. [オプション設定] の [製品ライセンス] 画面

[製品ライセンス] 画面には、ライセンスの詳細情報が表示されます。インストール時に選択したオプションによって、ライセンスは製品版または体験版のいずれかになります。どちらの場合でも、ライセンスによってサポート契約の権利が与えられます。サポート契約の期間が終了すると、ネットワーク上のクライアントは非常に限られた方法でしか保護されません。[製品ライセンス] 画面でライセンスの期限を確認し、失効前にライセンスを更新してください。

ライセンスの期限切れによる影響

製品版のアクティベーションコードの有効期限が切れると、アップデートされたコンポーネントのダウンロードや Web レピュテーションの使用などの重要なタスクを実行できなくなります。ただし、体験版とは異なり、製品版のアクティベーションコードの有効期限が切れても、既存の構成設定およびその他の設定はすべて有効なままです。これにより、意図せずにライセンスが期限切れになった場合でも、保護のレベルは維持されますが、最新の脅威に対抗することはできないため危険です。

製品ライセンスを更新するには

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。

ライセンスの変更

ライセンスの種類は、アクティベーションコードによって決まります。ライセンスの種類には体験版と製品版があります。また、製品版にはビジネスセキュリティ アドバンス版のライセンスまたはビジネスセキュリティ版のライセンスの 2 つがあります。ライセンスを変更する場合は、[製品ライセンス] 画面を使用して新しいアクティベーションコードを入力してください。

体験版から製品版にライセンスを変更するには

1. [新規入力] をクリックします。
2. 新しいアクティベーションコードを入力します。
3. [アクティベート] をクリックします。

Trend Micro Smart Protection Network に参加する

手順: [オプション設定] → [Smart Protection Network]

トレンドマイクロスマートフィードバックにより脅威に関する情報を継続的に収集して分析することで、保護の強化ができます。トレンドマイクロスマートフィードバックに参加すると、ご使用のコンピュータから情報が収集され、新しい脅威の特定に役立ちます。ご使用のコンピュータから収集する情報を、次に示します。

- ファイルのチェックサム
- アクセスされた Web アドレス
- サイズやパスなどのファイル情報
- 実行可能ファイルの名前

ヒント: ご使用のコンピュータを保護するためにスマートフィードバックに参加することは必須ではありません。参加は任意であり、いつでも参加の取り消しができます。トレンドマイクロ製品のすべてのお客さまに対する全体的な保護の強化に役立つので、スマートフィードバックへの参加をお勧めします。

Trend Micro Smart Protection Network の詳細については、次の Web ページを参照してください。

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

トレンドマイクロスマートフィードバックを有効にするには

1. [トレンドマイクロスマートフィードバックを有効にする] をクリックします。
2. クライアントコンピュータ上にあるファイルの潜在的なセキュリティ上の脅威に関する情報を送信するには、[疑わしいプログラムファイルのフィードバックを有効にする] チェックボックスをオンにします。
3. 所属の組織をトレンドマイクロで判別するのを容易にするために、[業種] で種類を選択します。
4. [保存] をクリックします。

ビジネスセキュリティ サーバをアンインストールする

警告： ビジネスセキュリティサーバをアンインストールすると、スキャンサーバもアンインストールされます。

ビジネスセキュリティでは、ビジネスセキュリティサーバを安全にコンピュータから削除するためのアンインストールプログラムが用意されています。ビジネスセキュリティサーバを削除する前に、すべてのクライアントからビジネスセキュリティクライアントを削除してください。

注意： ビジネスセキュリティサーバをアンインストールしても、ビジネスセキュリティクライアントはアンインストールされません。ビジネスセキュリティサーバをアンインストールする前に、すべてのビジネスセキュリティクライアントをアンインストールするか移動する必要があります。52 ページの「ビジネスセキュリティクライアントを削除する」を参照してください。

ビジネスセキュリティサーバを削除するには

1. サーバをインストールしたコンピュータで、[スタート] → [コントロールパネル] → [プログラムの追加と削除] の順に選択します。
2. ビジネスセキュリティサーバを選択して、[変更と削除] をクリックします。確認画面が表示されます。
3. [次へ] をクリックします。サーバのアンインストールプログラムから、管理者パスワードを入力するよう求められます。
4. テキストボックスに管理者パスワードを入力し、[次へ] をクリックします。サーバのファイルの削除が開始されます。ビジネスセキュリティサーバのアンインストールが完了すると、確認メッセージが表示されます。
5. [終了] をクリックして、アンインストールプログラムを閉じます。

トレンドマイクロ製品除外リスト

初期設定で検索から除外されるトレンドマイクロ製品の一覧を以下に示します。

表 A-1.トレンドマイクロ製品除外リスト

製品名	インストールパスの場所
InterScan eManager 3.5x	HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥InterScan eManager¥CurrentVersion ProgramDirectory=
InterScan eManager (InterScan for Microsoft Exchange eManager) 3.11, 5.1, 5.11, 5.12	HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥ScanMail for Microsoft Exchange eManager¥CurrentVersion ProgramDirectory=
InterScan for Lotus Notes eManager NT	HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥ScanMail for Lotus Notes¥CurrentVersion AppDir= DataDir= IniDir=
Interscan Web Security Suite	HKEY_LOCAL_MACHINE¥Software¥TrendMicro¥Interscan Web Security Suite Program Directory= C:¥Program Files¥Trend Mircro¥IWSS
InterScan WebProtect	HKEY_LOCAL_MACHINE SOFTWARE¥TrendMicro¥InterScan WebProtect¥CurrentVersion ProgramDirectory=

表 A-1. トレンドマイクロ製品除外リスト (続き)

製品名	インストールパスの場所
InterScan FTP VirusWall	HKEY_LOCAL_MACHINE SOFTWARE¥TrendMicro¥InterScan FTP VirusWall¥CurrentVersion ProgramDirectory=
InterScan Web VirusWall	HKEY_LOCAL_MACHINE SOFTWARE¥TrendMicro¥InterScan Web VirusWall¥CurrentVersion ProgramDirectory=
InterScan E-Mail VirusWall	HKEY_LOCAL_MACHINE SOFTWARE¥TrendMicro¥InterScan E-Mail VirusWall¥CurrentVersion ProgramDirectory={Installation Drive};¥INTERScan~1
InterScan NSAPI Plug-In	HKEY_LOCAL_MACHINE SOFTWARE¥TrendMicro¥InterScan NSAPI Plug-In¥CurrentVersion ProgramDirectory=
InterScan E-Mail VirusWall	HKEY_LOCAL_MACHINE SOFTWARE¥TrendMicro¥InterScan E-Mail VirusWall¥CurrentVersion ProgramDirectory=
IM Security (IMS)	HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥IM Security¥CurrentVersion HomeDir= VSQuarantineDir= VSBakupDir= FBArchiveDir= FTCFArchiveDir=

表 A-1. トrendマイクロ製品除外リスト（続き）

製品名	インストールパスの場所
InterScan for Microsoft Exchange	HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥ScanMail for Microsoft Exchange¥CurrentVersion TempDir= DebugDir=
	HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥ScanMail for Microsoft Exchange¥RealTimeScan¥ScanOption BackupDir= MoveToQuarantineDir=
	HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥ScanMail for Microsoft Exchange¥RealTimeScan¥ScanOption¥Advance QuarantineFolder=
	HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥ScanMail for Microsoft Exchange¥RealTimeScan¥IMCScan¥ScanOption BackupDir= MoveToQuarantineDir=
	HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥ScanMail for Microsoft Exchange¥RealTimeScan¥IMCScan¥ScanOption¥Advance QuarantineFolder=
InterScan for Microsoft Exchange	HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥ScanMail for Microsoft Exchange¥ManualScan¥ScanOption BackupDir= MoveToQuarantineDir=
	HKEY_LOCAL_MACHINE¥SOFTWARE¥TrendMicro¥ScanMail for Microsoft Exchange¥QuarantineManager QMDir=

表 A-1. トレンドマイクロ製品除外リスト (続き)

製品名	インストールパスの場所
InterScan for Microsoft Exchange 続き	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Scan Mail for Microsoft Exchange\CurrentVersion\HomeDirから exclusion.txt ファイルのパスを取得します。 HomeDir のパス (C:\Program Files\Trend Micro\Messaging Security Agent\ など) に移動します。 exclusion.txt を開きます。 C:\Program Files\Trend Micro\Messaging Security Agent\Temp\ C:\Program Files\Trend Micro\Messaging Security Agent\storage\quarantine\ C:\Program Files\Trend Micro\Messaging Security Agent\storage\backup\ C:\Program Files\Trend Micro\Messaging Security Agent\storage\archive\ C:\Program Files\Trend Micro\Messaging Security Agent\SharedResPool

クライアントの情報

本付録では、さまざまな種類のクライアント、およびタスクトレイに表示されるクライアントアイコンについて説明します。

本付録で説明する内容には、次の項目が含まれます。

- 182 ページの「クライアントの種類」
- 182 ページの「標準モードのクライアントのアイコン」
- 186 ページの「ロケーション認識」
- 187 ページの「スタンドアロンモードのクライアント」
- 188 ページの「32 ビットおよび 64 ビットのクライアント」

クライアントの種類

Trend Micro ビジネスセキュリティ (以下、ビジネスセキュリティ) では、次の観点でクライアントが識別されます。

- ・ 標準モードとスタンドアロンモードのクライアント
- ・ 32 ビットと 64 ビットのクライアント

標準モードのクライアントとは、ビジネスセキュリティクライアントがインストールされ、ビジネスセキュリティサーバと常時ネットワーク接続される固定コンピュータのことです。

クライアントのタスクトレイに表示されるアイコンは、標準モードのクライアントのステータスを示します。

標準モードのクライアントのアイコン

従来型スキャンのクライアントステータス : 正常

従来型スキャン用に設定されたクライアントではすべてが正常であることが、以下のアイコンで示されます。

表 B-1. 正常な状況にあるクライアントのアイコン (従来型スキャン)

アイコン	説明
	従来型スキャン用に設定された標準モードのクライアント
	従来型スキャンが実行されている

場合によっては、パターンファイルが最新でないことがあります。このアイコン  が表示された場合、クライアントはビジネスセキュリティサーバに接続されているが、パターンファイルが最新でないことを意味します。Windows のタスクトレイでアイコンを右クリックしてから [今すぐアップデート] を選択してすみやかに保護状態をアップデートするように、クライアントユーザに指示してください。

従来型スキャンのクライアントステータス：クライアントはビジネスセキュリティサーバから切断されているが、リアルタイム検索により保護されている

クライアントがビジネスセキュリティサーバから切断されている場合が時々あります。リアルタイム検索が有効化されており検索サービスが正常に実行されている場合、クライアントは引き続き保護されます。ただし、パターンファイルがすでに古くなっているか間もなく古くなる場合があります。以下のアイコンのクライアントは、リアルタイム検索により引き続き保護されます。

以下のアイコンが表示されている場合、ビジネスセキュリティサーバが実行されていること、およびクライアントがネットワークに接続されていることを確認してください。

表 B-2. ビジネスセキュリティサーバから切断されているクライアントのアイコン
(従来型スキャン)

アイコン	説明
	ビジネスセキュリティサーバから切断されているが、リアルタイム検索が実行されており、切断が発生したときにパターンファイルは最新であった
	ビジネスセキュリティサーバから切断されているが、リアルタイム検索が実行されている。ただし、切断が発生したときにパターンファイルは最新ではなかった

従来型スキャンのクライアントステータス：リアルタイム検索が動作していない

リアルタイム検索を有効にすることをお勧めします。無効にもできますが、お勧めしません。リアルタイム検索が無効にされていると、以下のアイコンがクライアントに表示されます。

表 B-3. リアルタイム検索が無効にされているクライアントのアイコン
(従来型スキャン)

アイコン	説明
	リアルタイム検索が無効
	リアルタイム検索が無効になっていて、パターンファイルが最新でない
	リアルタイム検索が無効になっていて、クライアントがビジネスセキュリティサーバから切断されている

表 B-3. リアルタイム検索が無効にされているクライアントのアイコン
(従来型スキャン)

アイコン	説明
	リアルタイム検索が無効になっていて、クライアントがビジネスセキュリティサーバから切断されており、パターンファイルが最新でない

以下の赤いアイコンのクライアントは、非常に脆弱です。リアルタイム検索サービスが終了しているか、正常に動作していません。

表 B-4. リアルタイム検索が正常に動作していないクライアントのアイコン
(従来型スキャン)

アイコン	説明
	リアルタイム検索サービスが正常に実行されていない
	リアルタイム検索サービスが正常に実行されておらず、パターンファイルが最新でない
	リアルタイム検索サービスが正常に実行されておらず、クライアントがサーバから切断されている
	リアルタイム検索サービスが正常に実行されておらず、クライアントがサーバから切断されており、パターンファイルが最新でない

スマートスキャンのクライアントステータス : 正常

以下のアイコンが表示されている場合、スマートスキャン用に設定されたクライアントではすべてが正常です。

表 B-5. 正常な状況にあるクライアントのアイコン (スマートスキャン)

アイコン	説明
	スマートスキャン用に設定された標準モードのクライアント
	スマートスキャンが実行されている

スマートスキャンのクライアントステータス：スマートスキャンサーバまたはビジネスセキュリティサーバから切断されている

スマートスキャンテクノロジーでは、スマートスキャンサーバを利用して、クライアントを保護します。クライアントがスマートスキャン用に設定されているが、スマートスキャンサーバから切断されている場合、クライアントは最小限のレベルでのみ保護されます。以下のアイコンが表示されている場合、スマートスキャンのサービスである **TMiCRCScanService** が実行されていること、およびクライアントがビジネスセキュリティサーバに接続されていることを確認してください。

表 B-6. スマートスキャンサーバまたはビジネスセキュリティサーバに接続されていないクライアントを示すアイコン (スマートスキャン)

アイコン	説明
	スキャンサーバから切断されているが、ビジネスセキュリティサーバに接続されている
	スキャンサーバから切断されており、ビジネスセキュリティサーバからも切断されている
	ビジネスセキュリティサーバから切断されているが、スキャンサーバに接続されている

スマートスキャンのクライアントステータス：リアルタイム検索が動作していない

リアルタイム検索を有効にすることをお勧めします。無効にもできますが、お勧めしません。リアルタイム検索が無効にされていると、以下のアイコンがクライアントに表示されます。

表 B-7. リアルタイム検索が無効にされているクライアントのアイコン (スマートスキャン)

アイコン	説明
	リアルタイム検索が無効になっているが、クライアントがスキャンサーバとビジネスセキュリティサーバに接続されている
	リアルタイム検索が無効になっていて、クライアントがスキャンサーバに接続されているが、ビジネスセキュリティサーバに接続されていない
	リアルタイム検索が無効になっていて、クライアントがスキャンサーバに接続されていないが、ビジネスセキュリティサーバに接続されている

表 B-7. リアルタイム検索が無効にされているクライアントのアイコン
(スマートスキャン)

アイコン	説明
	リアルタイム検索が無効になっていて、クライアントがスキャンサーバまたはビジネスセキュリティサーバのいずれかに接続されていない

以下の赤いアイコンのクライアントは、非常に脆弱です。リアルタイム検索サービスが終了しているか、正常に動作していません。

表 B-8. リアルタイム検索が正常に動作していないクライアントのアイコン
(スマートスキャン)

アイコン	説明
	リアルタイム検索サービスが正常に実行されていないが、クライアントがスキャンサーバとビジネスセキュリティサーバに接続されている
	リアルタイム検索サービスが正常に実行されておらず、クライアントがスキャンサーバに接続されているが、ビジネスセキュリティサーバに接続されていない
	リアルタイム検索サービスが正常に実行されておらず、クライアントがスキャンサーバに接続されていないが、ビジネスセキュリティサーバに接続されている
	リアルタイム検索サービスが正常に実行されておらず、クライアントがスキャンサーバまたはビジネスセキュリティサーバのいずれかに接続されていない

ロケーション認識

ロケーション認識を使用すると、管理者は、クライアントがどのようにネットワークに接続されているかに応じて、セキュリティ設定を制御できます。

ビジネスセキュリティでは、ビジネスセキュリティサーバのゲートウェイ情報に基づいて自動的にクライアントの場所を識別し、ユーザがアクセスできる Web サイトを制御します。ユーザの場所に応じて制限内容が異なります。

- ・ 標準モードのクライアントとは、ビジネスセキュリティサーバと常時ネットワークで接続されているコンピュータです。
- ・ スタンドアロンモードのクライアントとは、一時的にネットワーク接続を確立するコンピュータです。

スタンドアロンモードのクライアント

管理者はスタンドアロンモード権限をクライアントに割り当てることができます。これによって、ユーザはこれらのクライアントをスタンドアロンモードに変更できます。スタンドアロンモードのビジネスセキュリティクライアントはスタンドアロンクライアントと呼ばれます。このモードでもコンピュータは保護されます。ただし、スタンドアロンクライアントはサーバからのメッセージを受信しません。そして、次の状況でのみアップデートできます。

- ・ クライアントで [手動アップデート] または [自動アップデート] を実行する場合
- ・ ビジネスセキュリティクライアントがビジネスセキュリティサーバに接続したとき

サーバコマンドによって干渉を受けないように機能をコンピュータで使用する場合、そのコンピュータ上のビジネスセキュリティクライアントにスタンドアロンモード権限が付与されていることを確認してください。

クライアントの権限を変更する方法の詳細については、86 ページの「クライアント権限」を参照してください。

スタンドアロンモードのクライアントのステータスは、タスクトレイに表示されるアイコンで示されます。スタンドアロンモードのクライアントで表示されるアイコンの一覧については、以下の表を参照してください。

表 B-9. スタンドアロンモードのクライアントで表示されるアイコン (従来型スキャン)

アイコン	説明
	スタンドアロンモードのクライアント (青いアイコン)
	リアルタイム検索が無効
	パターンファイルが最新でない
	リアルタイム検索が無効になっていて、パターンファイルが最新でない
	リアルタイム検索サービスが停止している (赤いアイコン)

表 B-9. スタンドアロンモードのクライアントで表示されるアイコン (従来型スキャン)

アイコン	説明
	リアルタイム検索サービスが停止していて、パターンファイルが最新でない (赤いアイコン)

表 B-10. スタンドアロンモードのクライアントで表示されるアイコン (スマートスキャン)

アイコン	説明
	スマートスキャンのスタンドアロンモードのクライアント (青いアイコン)
	スマートスキャンサーバに接続されているが、リアルタイム検索が動作していない
	スマートスキャンサーバに接続されているが、リアルタイム検索が無効
	スマートスキャンサーバに接続されていない
	スマートスキャンサーバに接続されておらず、リアルタイム検索が動作していない
	スマートスキャンサーバに接続されておらず、リアルタイム検索が無効

32 ビットおよび 64 ビットのクライアント

ビジネスセキュリティクライアントでは、x86 プロセッサアーキテクチャ、および x64 プロセッサアーキテクチャを使用するコンピュータがサポートされます。これらの OS とアーキテクチャでは、ルートキット対策を除いてすべての機能が利用できます。

注意： ビジネスセキュリティクライアントでは、Itanium 2 アーキテクチャ (IA-64) はサポートされません。

トレンドマイクロのサービス

本付録ではトレンドマイクロが提供しているサービスについて説明します。

本付録で説明する内容には、次の項目が含まれます。

- 190 ページの「大規模感染予防ポリシー」
- 190 ページの「ダメージクリーンナップサービス」
- 191 ページの「脆弱性診断」
- 192 ページの「トレンドマイクロの推奨設定」
- 192 ページの「トレンドマイクロの推奨処理」
- 193 ページの「IntelliTrap」
- 194 ページの「Web レピュテーション」

大規模感染予防ポリシー

トレンドマイクロの大規模感染予防ポリシーは、セキュリティ設定におけるトレンドマイクロ推奨の初期設定であり、ネットワーク上の大規模感染に応じて適用されます。

大規模感染予防ポリシーは、トレンドマイクロから Trend Micro ビジネスセキュリティ (以下、ビジネスセキュリティ) サーバにダウンロードされます。

ビジネスセキュリティサーバでは、大規模感染が検出されると、大規模感染の程度が判別され、大規模感染予防ポリシーで指定されているとおりに適切なセキュリティ措置がすぐに実行されます。

大規模感染予防ポリシーに基づいて、大規模感染の発生時にはネットワークを保護するために、自動対応によって次の先制的な処理が行われます。

- 共有フォルダをブロックして、共有フォルダ内のファイルにウイルス / 不正プログラムが感染しないようにします。
- ポートをブロックして、脆弱なポートを利用してネットワークとクライアントのファイルにウイルス / 不正プログラムが感染することを防ぎます。
- ファイルおよびフォルダへの書き込みアクセスを禁止して、ファイルがウイルス / 不正プログラムによって変更されないようにします。
- 大規模感染が検出されると、クライアントにアラートメッセージが表示されます。

ダメージクリーンアップサービス

ビジネスセキュリティでは、ダメージクリーンアップサービスを使用して、トロイの木馬およびウイルス / 不正プログラムから Windows コンピュータを保護します。

ダメージクリーンアップサービス

ダメージクリーンアップサービスでは、ウイルスや不正プログラム、またはスパイウェアやグレーウェアがもたらす脅威に対し、次のように対処します。

- 脅威を検出し、削除します。
- 脅威が作成したプロセスを強制終了します。
- 脅威が変更したシステムファイルを修復します。
- 脅威が作成したファイルおよびアプリケーションを削除します。

ダメージクリーンナップサービスでは、上記のタスクを実行するために、以下のコンポーネントを使用します。

- ・ **ウイルスクリーンナップエンジン**: ダメージクリーンナップサービスで、脅威と関連するプロセスを検索し、削除するために使用されるエンジンです。
- ・ **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エンジンが、脅威と関連するプロセスを識別して削除するために使用するテンプレートです。

ビジネスセキュリティでは、ダメージクリーンナップサービスは、次の場合にクライアントで実行されます。

- ・ ユーザがビジネスセキュリティクライアントコンソールから手動でクリーンナップを実行した場合
- ・ 管理者が管理コンソールからクライアント上でクリーンナップを実行した場合
- ・ ユーザが手動検索または予約検索を実行した場合
- ・ HotFix または Patch のインストール後
- ・ ビジネスセキュリティサービスの再起動後 (ビジネスセキュリティでは、ビジネスセキュリティクライアントが異常終了した場合に自動的に再起動するよう、クライアントの監視サービスを有効にしておく必要があります。この機能は、[グローバル設定] 画面で有効にします。詳細については、134 ページの「監視サービス設定」を参照してください)。

クリーンナップは自動で実行されるため、設定は不要です。ビジネスセキュリティクライアントの起動中にバックグラウンドで実行されるため、ユーザはクリーンナップが実行されていることも意識しません。ただし、脅威を削除する処理を完了するために、クライアントの再起動を促す通知がビジネスセキュリティから送信される場合があります。

脆弱性診断

脆弱性診断とは、システム管理者がネットワークに対するセキュリティリスクを診断するための機能です。脆弱性診断を使用して生成される情報によって、既知の脆弱性を解決し、ネットワークを保護する方法が明確に示されます。

脆弱性診断の使用目的は次のとおりです。

- ・ ネットワークに接続されている任意のまたはすべてのコンピュータに対する検索作業を構成します。個々の脆弱性を検索することも、既知の脆弱性の全リストを検索することもできます。
- ・ 診断を手動で実行するか、定期的に診断を実行するように設定します。
- ・ ネットワークセキュリティに対して許容できないレベルのリスクが認められたコンピュータのブロックを要求します。

- 個々のコンピュータについての脆弱性を特定するレポートを作成し、これらのコンピュータで認められたネットワーク全体に対するセキュリティリスクを示します。レポートでは標準の命名規則に従って脆弱性が特定されるため、管理者は詳細まで調査して、脆弱性の解決やネットワーク保護を実施できます。
- 診断履歴を表示し、レポートを比較して、脆弱性とネットワークセキュリティに対するリスク要因の変化をよりよく理解できるようにします。

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、検索するファイルを特定する方法です。実行可能ファイル (.exe など) では、ファイルの種類はファイルの内容に基づいて判断されます。その他のファイルの種類 (.txt など) は、ファイルのヘッダに基づいて判断されます。

トレンドマイクロの推奨設定には、次の利点があります。

- 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、最小限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は影響しません。
- 検索時間の短縮:トレンドマイクロの推奨設定では実際のファイルタイプを識別するため、感染の危険性があるファイルだけが検索されます。そのため、すべてのファイルを検索する場合に比べ、検索時間が大幅に短縮されます。

トレンドマイクロの推奨処理

ウイルスや不正プログラムの種類が異なれば、適用すべき検索処理も異なります。ウイルスや不正プログラムの種類に応じて検索処理をカスタマイズするにはウイルスについての知識が必要となり、場合によっては面倒な作業を伴います。トレンドマイクロでは、「トレンドマイクロの推奨処理」を使用してこれらの問題を解決します。

トレンドマイクロの推奨処理は、ウイルスや不正プログラム、その他の種類の脅威に対する各種の検索処理をあらかじめ設定したものです。ウイルスや不正プログラムに対する推奨処理は、1 次処理が [駆除] で、駆除できない場合の 2 次処理が [隔離] です。トロイの木馬とジョークプログラムに対する推奨処理は [隔離] です。

検索処理に不慣れな場合、または特定の種類のウイルス / 不正プログラムに対する適切な検索処理が不明な場合には、トレンドマイクロの推奨処理の使用をお勧めします。

トレンドマイクロの推奨処理には、次の利点があります。

- 時間の節約と容易な保守:「トレンドマイクロの推奨処理」では、トレンドマイクロが推奨する検索処理が使用されます。そのため、検索処理を設定するための時間を節約できます。

- ・ アップデート可能な検索処理: ウイルスの作成者はウイルスによるコンピュータへの攻撃方法を常に変化させています。ウイルスによる最新の脅威と最新の攻撃方法からクライアントを保護できるよう、トレンドマイクロの新しい推奨処理の設定内容が、ウイルスパターンファイルのアップデートにより適用されます。

トレンドマイクロの推奨処理の初期設定

各脅威に対するトレンドマイクロの推奨処理は、次のように初期設定されています。

表 C-1. トレンドマイクロの推奨処理の初期設定

脅威	処理	2 次処理
Possible_Virus	放置	適用なし
ジョークプログラム	隔離	適用なし
その他の脅威	駆除	隔離
Packer	隔離	適用なし
テストウイルス	放置	適用なし
ウイルス	駆除	隔離
ワーム / トロイの木馬	隔離	適用なし

注意: 初期設定の処理は、今後のパターンファイルのアップデートで変更される可能性があります。

IntelliTrap

IntelliTrap は、トレンドマイクロ独自のヒューリスティックテクノロジーであり、リアルタイム圧縮と、Packer などの他の不正プログラムの性質を組み合わせた脅威を検出するのに使用されます。このテクノロジーは、ウイルス、不正プログラム、ワーム、トロイの木馬、バックドア、およびボットの検出に使用できます。ウイルス作成者は、通常、さまざまなファイル圧縮スキームを使用して、ウイルスや不正プログラムのフィルタを回避しようとします。IntelliTrap は、ルールとパターンファイルを使用したリアルタイムの検索エンジン技術です。16 種類の一般的な圧縮タイプのいずれかを使用した、最大 6 層の圧縮ファイルに存在する既知のウイルスまたは不正プログラムを検出し、削除します。

IntelliTrap は、ボットやその他の不正プログラムを検索する際に、次のコンポーネントを使用します。

- ・ トレンドマイクロのウイルス検索エンジンとウイルスパターンファイル
- ・ IntelliTrap パターンファイルと IntelliTrap 除外パターンファイル

実際のファイルの種類

「実際のファイルの種類」を検索するよう設定すると、検索エンジンではファイル名ではなくファイルのヘッダを調べて実際のファイルの種類が確認されます。たとえば、すべての実行可能ファイルを検索するよう検索エンジンを設定した場合、検索エンジンは、「family.gif」という名前のファイルを検出したときに、このファイルを画像ファイルとは見なしません。代わりに、検索エンジンはファイルのヘッダを開いて内部登録されているデータの種類の調べ、このファイルが実際に画像ファイルであるか、または、たとえば検出を避けるためにこのように名付けられている実行可能ファイルであるかを判別します。

実際のファイルの種類による検索は、トレンドマイクロの推奨設定と協調して機能し、潜在的に危険であると認識されているファイルの種類のみを検索します。これらの技術によって、検索エンジンで調べる必要のあるファイルの総数が 3 分の 2 程度に削減されますが、削減されることによって、潜在的な危険性が高まります。

たとえば、.gif ファイルは、Web トラフィック全体から見るとかなりの部分を占めていますが、ウイルスや不正プログラムを潜伏させたり、実行可能コードを起動したり、既知のまたは理論上の脆弱性を悪用したりする可能性はあまりありません。だからといって、.gif ファイルは安全であると言えるでしょうか。そうとは言い切れません。悪意あるハッカーは、有害なファイルに「安全な」ファイル名を付け、検索エンジンを通過させて、ネットワークに持ち込むことが可能です。このファイルが名前変更され、実行された場合には、損傷を招く可能性があります。

Web レピュテーション

Web レピュテーションでは、要求された URL についてトレンドマイクロ Web セキュリティデータベースに照会することで、セキュリティリスクの危険性のある URL へのアクセスを防止します。クライアントの場所（オフィス内 / オフィス外）に応じて、異なるレベルのセキュリティを設定します。

Web レピュテーションが URL をブロックしても、その URL が安全であると判断した場合は、承認済み URL リストにその URL を追加します。承認済み URL リストに URL を追加する方法の詳細については、「オプション設定」を参照してください。

評価スコア

URL が Web からの脅威かどうかは、その URL の「評価スコア」によって判定されます。このスコアは、トレンドマイクロ独自の基準値を使用して計算されます。トレンドマイクロでは Web レビューテーションの対象 URL を、「Web からの脅威」、「Web からの脅威の可能性が非常に高い」、「Web からの脅威の可能性が高い」のカテゴリにわけています。

トレンドマイクロでは、定義済みのしきい値をスコアが超えている場合に、その URL はアクセスしても安全であると見なします。URL へのアクセスを許可するかブロックするかを判定するためのセキュリティレベルは、次の 3 つです。

- **高** — ブロックするページは次のとおりです。
 - 詐欺サイトや脅威の送信元と確認されたページ
 - 詐欺サイトや脅威の送信元の疑いのあるページ
 - スパムメールに関連付けられたページや危険にさらされる可能性のあるページ
 - 評価のないページ
- **中** — ブロックするページは次のとおりです。
 - 詐欺サイトや脅威の送信元と確認されたページ
 - 詐欺サイトや脅威の送信元の疑いのあるページ
- **低** — 詐欺サイトや脅威の送信元と確認されたページをブロックします。

クライアント保護のベストプラクティス

コンピュータセキュリティのベストプラクティスの詳細については、トレンドマイクロの Web サイトにアクセスして、「Safe Computing Guide」またはその他のセキュリティ情報を参照してください。

<http://www.trendmicro.com/en/security/general/virus/overview.htm>

管理ツールおよびクライアントツールの使用

本付録では、Trend Micro ビジネスセキュリティ（以下、ビジネスセキュリティ）に付属する管理ツールおよびクライアントツールの使用方法について説明します。

本付録で説明する内容には、次の項目が含まれます。

- 200 ページの「ツールの種類」
- 201 ページの「管理ツール」
- 206 ページの「クライアントツール」
- 209 ページの「アドイン」

ツールの種類

ビジネスセキュリティには、サーバの設定やクライアントの管理など、さまざまな操作を簡単に実行できるようにするためのツールがあります。

注意： これらのツールは、管理コンソールから使用することはできません。ツールの使用方法については、次の関連するセクションを参照してください。

これらのツールは、次の 3 種類に分類されます。

- **管理ツール** — ビジネスセキュリティサーバの設定およびビジネスセキュリティクライアントの管理を支援するツールです。
 - **ログオンスクリプトウィザード (autopcc.exe)** — ビジネスセキュリティクライアントのインストールを自動化します。
 - **脆弱性検索ツール (TMVS.exe)** — ネットワーク上の保護されていないコンピュータを特定します。
- **クライアントツール** — ビジネスセキュリティクライアントのパフォーマンス強化を支援するツールです。
 - **Client Packager (ClnPack.exe)** — ビジネスセキュリティクライアントとコンポーネントを含む自己解凍ファイルを作成します。
 - **感染ファイル暗号化処理の復元ツール (VSEncode.exe)** — ビジネスセキュリティによって暗号化された感染ファイルを開きます。
 - **クライアント移動ツール (IpXfer.exe)** — クライアントを別のビジネスセキュリティサーバに移動します。移動元のサーバと移動先のサーバでは、同一バージョンのビジネスセキュリティおよび OS が実行されている必要があります。
- **アドイン** — Windows Small Business Server (SBS) 2008 と Windows Essential Business (EBS) Server 2008 のアドインにより、管理者は最新のセキュリティ情報とシステム情報を SBS コンソールと EBS コンソールで表示できます。これらは [最新ステータス] 画面に表示されるのと同様の高いレベルの情報です。

注意： 旧バージョンのビジネスセキュリティに付属するツールの中には、このバージョンでは利用できないものがあります。これらのツールが必要な場合は、テクニカルサポートにお問い合わせください。詳細については、229 ページの「サポートサービスについて」を参照してください。

管理ツール

ここでは、ビジネスセキュリティの管理ツールについて説明します。

ログオンスクリプトウィザード

ログオンスクリプトウィザードを使用すると、ウイルス対策が実施されていないコンピュータがネットワークにログオンしたときに、ビジネスセキュリティクライアントを自動でインストールできます。ログオンスクリプトウィザードを実行すると、サーバのログオンスクリプトに **autopcc.exe** というプログラムが追加されます。**autopcc.exe** は、次の機能を実行するプログラムです。

- ・ ウイルス対策の実施されていないコンピュータの OS を識別し、ビジネスセキュリティクライアントの適切なバージョンをインストールします。
- ・ ウイルスパターンファイルおよびプログラムファイルをアップデートします。

ビジネスセキュリティクライアントのインストール手順については、39 ページの「ログオンスクリプトウィザードを使用してインストールする」を参照してください。

脆弱性検索ツール

脆弱性検索ツール (Vulnerability Scanner) を利用して、インストールされたウイルス対策製品を検出し、ウイルス対策の実施されていないコンピュータをネットワーク内で検索できます。コンピュータが保護されているかどうかを調べるため、脆弱性検索ツールは、ウイルス対策製品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。

脆弱性検索ツールでは、次の機能を実行できます。

- ・ コンピュータがネットワークに最初にログオンしたときに、脆弱性検索ツールがコンピュータのステータスを判断できるように、DHCP リクエストについてネットワークを監視します。
- ・ ネットワーク上のコンピュータに ping コマンドを実行し、ステータスを調べ、コンピュータ名、プラットフォームのバージョン、説明を取得します。
- ・ ネットワーク上にインストールされているウイルス対策製品を調べます。トレンドマイクロ製品 (ウイルスバスター Corp.、ServerProtect for Windows NT、ServerProtect for Linux、InterScan for Microsoft Exchange、InterScan Messaging Security Suite、PortalProtect など) および他社製のウイルス対策製品 (Norton AntiVirus Corporate Edition v7.5/7.6、McAfee VirusScan ePolicy Orchestrator など) を検出できます。

- ・ サーバ名と各コンポーネントのバージョン (パターンファイル、検索エンジン、ウイルスバスター Corp.、ウイルスバスター 2005、および ServerProtect for Windows NT のプログラム) を表示できます。
- ・ 検索結果をメールで送信します。
- ・ サイレントモード (コマンドプロンプトモード) で実行します。
- ・ ビジネスセキュリティクライアントを、Windows 2000/Server 2003 (R2) が稼働しているコンピュータにリモートでインストールします。

予約タスクを作成して、脆弱性検索ツールを自動化することもできます。脆弱性検索ツールを自動化する方法の詳細については、脆弱性検索ツールのオンラインヘルプを参照してください。

ビジネスセキュリティサーバ以外のコンピュータで脆弱性検索ツールを実行するには、ビジネスセキュリティサーバの ¥PCCSRV¥Admin¥Utility フォルダから、実行するコンピュータに TMVS フォルダをコピーします。

注意： ビジネスセキュリティのサーバコンポーネントが同一コンピュータ上に存在する場合は、脆弱性検索ツールでビジネスセキュリティクライアントをインストールすることはできません。

ビジネスセキュリティのサーバコンポーネントをすでに実行しているコンピュータに対しては、脆弱性検索ツールからビジネスセキュリティクライアントをインストールできます。

脆弱性検索ツールを使用する

脆弱性検索ツールを設定するには

1. ビジネスセキュリティのサーバコンポーネントをインストールしたドライブで、ビジネスセキュリティサーバの ¥PCCSRV¥Admin¥Utility¥TMVS フォルダを開きます。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. [Settings] をクリックします。[Settings] 画面が表示されます。
3. [Product Query] から、ネットワーク上で調べる製品を選択します。[Check for all Trend Micro products] を選択すると、すべての製品が選択されます。

InterScan および Norton AntiVirus Corporate Edition がネットワークにインストールされている場合は、製品名の横にある [Settings] をクリックして、脆弱性検索ツールが調べるポート番号を確認します。

4. [Description Retrieval Settings] で、使用する検索方法を選択します。[Normal retrieval] の方が正確ですが、完了までに時間がかかります。
[Normal retrieval] をクリックした場合は、コンピュータの説明があれば取得するかどうかを指定できます。取得する場合は、[Retrieve computer descriptions when available] チェックボックスをオンにします。
5. 管理者に結果を自動的に送信するには、[Alert Settings] で [Email results to the system administrator] チェックボックスをオンにし、[Configure] をクリックしてメールの設定を指定します。
 - To
 - From
 - SMTP サーバー SMTP サーバのアドレスです。たとえば、「smtp.example.com」と指定します。SMTP サーバ情報は必須です。
 - Subject
6. ウイルス対策の実施されていないコンピュータに警告を表示する場合、[Display alert on unprotected computers] チェックボックスをオンにします。次に、[Customize] をクリックして、警告メッセージを設定します。[Alert Message] 画面が表示されます。新しい警告メッセージを入力するか、または初期設定のメッセージを適用します。[OK] をクリックします。
7. 結果を CSV 形式で保存する場合は、[Automatically save the results to a CSV file] チェックボックスをオンにします。初期設定では、CSV データファイルは TMVS フォルダに保存されます。CSV の出力先を変更するには、[Browse] をクリックします。[フォルダの参照] 画面が表示されます。ローカルコンピュータ上またはネットワーク上の対象フォルダを選択し、[OK] をクリックします。
8. ネットワーク上のコンピュータに ping を実行してステータスを取得できます。[Ping Settings] で、脆弱性検索ツールがコンピュータにパケットを送信し、応答を待機する方法を設定します。初期設定を適用するか、または [Packet size] と [Timeout] ボックスに新しい値を入力します。
9. ビジネスセキュリティクライアントをリモートでインストールしてログをサーバに送信するには、サーバ名とポート番号を入力します。ビジネスセキュリティクライアントをリモートで自動的にインストールするには、[Auto-install Client/Server Security Client on unprotected computer] チェックボックスをオンにします。
10. [Install Account] をクリックしてアカウントを設定します。[Account Information] 画面が表示されます。
11. ユーザ名とパスワードを入力して、[OK] をクリックします。
12. [OK] をクリックして、設定内容を保存します。脆弱性検索ツールのコンソールが表示されます。

IP アドレスの範囲を指定して手動で脆弱性検索を実行するには

1. インストールされているウイルス対策製品、およびウイルス対策製品のインストールされていないコンピュータを調べる IP アドレスの範囲を、[IP Range to Check] に入力します。

注意： 脆弱性検索ツールでサポートされるのは、クラス B の IP アドレスのみです。

2. [Start] をクリックし、ネットワーク上のコンピュータに対する調査を開始します。結果が [Results] に表示されます。

DHCP サーバに IP アドレスをリクエストしているコンピュータに対して脆弱性検索を実行するには

1. [Results] ボックスで [DHCP Scan] タブをクリックします。[DHCP Start] ボタンが表示されます。
2. [DHCP Start] をクリックします。脆弱性検索ツールは、DHCP リクエストの受信を監視して、ネットワークにログオンするコンピュータに対して脆弱性チェックを実行します。

予約タスクを作成するには

1. [Scheduled Tasks] で [Add/Edit] をクリックします。[Scheduled Task] 画面が表示されます。
2. [Task Name] で、作成するタスクの名前を入力します。
3. インストールされているウイルス対策製品、およびウイルス対策製品のインストールされていないコンピュータを調べる IP アドレスの範囲を、[IP Address Range] に入力します。
4. [Task Schedule] で、作成するタスクを実行する頻度を選択します。毎日 ([Daily])、週 1 回 ([Weekly, every])、または月 1 回 ([Monthly, every]) の頻度で実行するようにタスクを設定できます。[Weekly, every] をクリックした場合は、リストボックスで曜日を指定する必要があります。[Monthly, every] をクリックした場合は、リストボックスで日付を指定する必要があります。
5. [Start time] ボックスで、タスクを実行する時間を入力または選択します。24 時間形式を使用します。
6. 既存の設定を使用する場合は、[Settings] で [Use current settings] をクリックします。設定を変更するには、[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。設定手順については、202 ページの「脆弱性検索ツールを設定するには」のステップ 3 ～ステップ 12 を参照してください。
7. [OK] をクリックして、設定内容を保存します。作成したタスクが [Scheduled Tasks] の下に表示されます。

その他の設定

次の設定を変更するには、TMVS.ini を編集する必要があります。

- **EchoNum** — 脆弱性検索ツールによって ping を同時に実行するクライアントの数を設定します。
- **ThreadNumManual** — 脆弱性検索ツールで、ウイルス対策ソフトウェアの有無を同時にチェックするクライアントの数を設定します。
- **ThreadNumSchedule** — 予約タスクの実行時に脆弱性検索ツールで、ウイルス対策ソフトウェアの有無を同時にチェックするクライアントの数を設定します。

設定を変更するには

1. TMVS フォルダを開いて **TMVS.ini** ファイルを見つけます。
2. 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。
3. 脆弱性検索ツールによって ping コマンドを同時に実行するコンピュータの数を設定するには、**EchoNum** の値を変更します。1 ～ 64 の値を指定します。

たとえば、脆弱性検索ツールが同時に 60 台のコンピュータに ping コマンドを実行するように指定するには、「**EchoNum=60**」と入力します。

4. 脆弱性検索ツールが同時にウイルス対策製品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、ウイルス対策製品のチェックを 60 台のコンピュータに対して同時に実行するには、「**ThreadNumManual=60**」と入力します。

5. 予約されたタスクを実行するときに、脆弱性検索ツールが同時にウイルス対策製品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、脆弱性検索ツールが予約されたタスクを実行するときに、ウイルス対策製品のチェックを 60 台のコンピュータに対して同時に実行するには、「**ThreadNumSchedule=60**」と入力します。

6. **TMVS.ini** を保存します。

クライアントツール

ここでは、ビジネスセキュリティのクライアントツールについて説明します。

Client Packager

Client Packager は、セットアップファイルおよびアップデートファイルを圧縮し、1 つの自己解凍ファイルを作成できるツールです。これにより、メールまたは CD-ROM などの記録媒体を使用してファイルを簡単に配布できます。Client Packager には Microsoft Outlook のアドレス帳と連動し、自己解凍ファイルを Client Packager のコンソールからメールで送信できる機能もあります。

Client Packager を実行するには、ファイルをダブルクリックします。Client Packager を使用してインストールされたビジネスセキュリティクライアントは、セットアップパッケージを作成したサーバにレポートを送信します。

感染ファイル暗号化処理の復元ツール

ビジネスセキュリティクライアントでは、感染しているファイルと添付ファイルが暗号化されます。これは、ユーザがそのファイルを開いてウイルスや不正プログラムをクライアント上の他のファイルに感染させることを防ぐためです。

ビジネスセキュリティクライアントでは、感染したファイルのバックアップ、隔離、または名前の変更が実行されるとき、常にファイルが暗号化されます。隔離されたファイルはクライアントの ¥Suspect フォルダに保存され、次に隔離ディレクトリに送られます。バックアップファイルはクライアントの ¥Backup フォルダに保存されます (通常は C:¥Program Files¥Trend Micro¥Client Server Security Agent¥Backup¥)。

ただし、場合によっては、感染していることを承知のうえでファイルを開かなくてはならないことがあります。たとえば、重要な文書が感染し、その文書内の情報を取得する必要がある場合、情報を取得するためには、感染したファイルの暗号化処理を復号する必要があります。感染ファイル暗号化処理の復元ツールを使用すると、感染したファイルの暗号化処理を復号し、開くことができます。

注意： 感染ファイル暗号化処理の復元ツールを使用するときに、ビジネスセキュリティクライアントが再度同じウイルス / 不正プログラムを検出しないようにするには、リアルタイム検索からファイルの復号先フォルダを除外してください。

警告： 感染したファイルを復号すると、他のファイルにウイルス / 不正プログラムの感染が拡大するおそれがあります。

感染ファイル暗号化処理の復元ツールには、次のファイルが必要です。

- **メインファイル：** VSEncode.exe
- **必要な DLL ファイル：** VSAPI32.dll

グラフィックユーザインタフェースを使用する

コマンドラインから **Suspect** フォルダ内のファイルを復元するには

1. ツールが格納されているフォルダ (例: c:\VSEncrypt) に進み、「VSEncode.exe /u」と入力します。
2. 復元するファイルを選択します。
3. [復元] をクリックします。

コマンドラインインタフェースを使用する

コマンドラインから **Suspect** フォルダ内のファイルを復元するには

1. VSEncrypt をビジネスセキュリティサーバからクライアントにコピーします。
¥PCCSRV¥Admin¥Utility¥VSEncrypt

警告： VSEncrypt フォルダはビジネスセキュリティフォルダにコピーしないでください。感染ファイル暗号化処理の復元ツールの VSAPI32.dll ファイルは、元の VSAPI32.dll と競合します。

2. コマンドプロンプトを開き、VSEncrypt フォルダをコピーした場所に移動します。
3. 次のパラメータを使用して、感染ファイル暗号化処理の復元ツールを実行します。
 - **パラメータなし** — 隔離フォルダ内のファイルを暗号化します。
 - **-d** — 隔離フォルダ内のファイルを復号します。
 - **-debug** — デバッグログを作成してクライアントのルートフォルダに出力します。
 - **/o** — 暗号化または復号されたファイルがすでに存在する場合、ファイルを上書きします。
 - **/f {ファイル名}** — ファイルを 1 つだけ暗号化または復号します。
 - **/nr** — 元のファイル名を復元しません。

たとえば、隔離フォルダのファイルを復号して、デバッグログを作成するには、「VSEncode -d -debug」と入力します。ファイルの復号または暗号化を行うと、復号されたファイルまたは暗号化されたファイルが同じフォルダ内に作成されます。

注意： ロックされているファイルの暗号化または復号を行うことはできません。

感染ファイル暗号化処理の復元ツールでは、次のログが提供されます。

- VSEncrypt.log — 暗号化または復号の詳細が含まれています。このファイルは、コンピュータにログオンしているユーザの一時フォルダ (通常は C: ドライブ内) に自動的に作成されます。
- VSEncDbg.log — デバッグの詳細が含まれています。-debug パラメータを指定して VSEncode.exe を実行すると、このファイルが、コンピュータにログオンしているユーザの一時フォルダ (通常は C: ドライブ内) に自動的に作成されます。

他の場所にあるファイルを暗号化または復号するには

1. テキストファイルを作成し、暗号化または復号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 にあるファイルを暗号化または復号する場合、テキストファイルに「C:\My Documents\Reports*. *」と入力します。次に、テキストファイルを INI 拡張子または TXT 拡張子で保存します。たとえば、ForEncryption.ini というファイル名で C: ドライブに保存します。
2. コマンドプロンプトで、「VSEncode.exe -d -i {INI または TXT ファイルの場所}」と入力して、感染ファイル暗号化処理の復元ツールを実行します。ここで、{INI または TXT ファイルの場所} 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 となります。

クライアント移動ツール

ネットワークにビジネスセキュリティサーバが複数ある場合、クライアント移動ツールを使用してクライアントを別のビジネスセキュリティサーバに移動できます。

このツールは、ネットワークに新しいビジネスセキュリティサーバを追加した後で、そのサーバに既存のクライアントを移動するときに特に便利です。移動元のサーバと移動先のサーバでは、同一バージョンのビジネスセキュリティおよび OS が実行されている必要があります。

クライアント移動ツールを実行するには、IpXfer.exe ファイルが必要です。

クライアント移動ツールを実行するには

1. ビジネスセキュリティサーバで、次のディレクトリに移動します。
¥PCCSRV¥Admin¥Utility¥IpXfer
2. IpXfer.exe ファイルを、移動するクライアントにコピーします。
3. クライアントでコマンドプロンプトを開き、ファイルをコピーしたフォルダに移動します。
4. 次の構文を使用してクライアント移動ツールを実行します。

```
IpXfer.exe -s <サーバ名> -p <サーバ待機ポート番号> -m 1  
-c <クライアント待機ポート番号>
```

変数には以下の値を入力します。

- <サーバ名> = 移動先ビジネスセキュリティ (クライアントの転送先のサーバ) のサーバ名
- <サーバ待機ポート番号> = 移動先ビジネスセキュリティサーバの信頼する待機ポート番号。管理コンソールの待機ポートを表示するには、[セキュリティ設定] をクリックします。待機ポートは、ビジネスセキュリティサーバ名の横に表示されます。
- 1 = 「-m」の後に数字「1」を入力する必要があります。
- <クライアント待機ポート番号> = クライアントのポート番号

クライアントの報告先が別のサーバになったことを確認するには

1. クライアントで、システムトレイのビジネスセキュリティクライアントアイコンを右クリックします。
2. [ビジネスセキュリティクライアント メイン] を選択します。
3. [ヘルプ] タブの [バージョン情報] セクションで [情報] をクリックします。
4. ビジネスセキュリティクライアントの報告先であるビジネスセキュリティサーバが正しいことを確認します。

アドイン

ビジネスセキュリティには、Windows Small Business Server (SBS) 2008 と Windows Essential Business Server (EBS) 2008 のアドインが用意されています。これらのアドインにより、最新のセキュリティステータス情報とシステムステータス情報を SBS コンソールと EBS コンソールで表示できます。

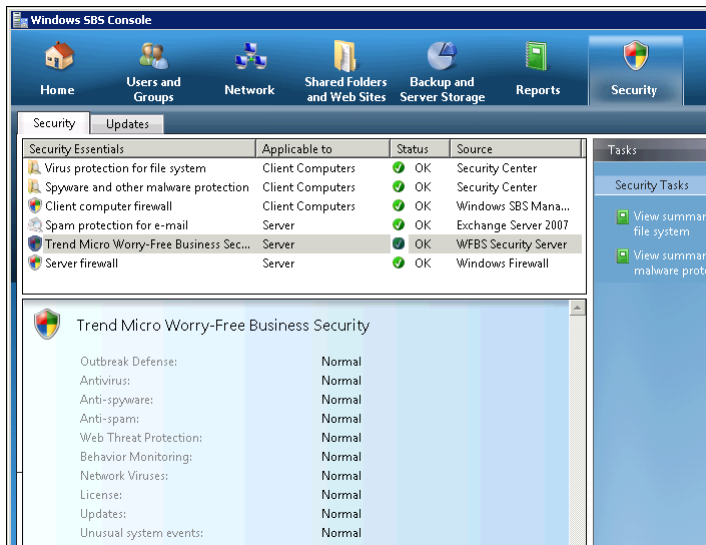


図 E-1. 最新ステータス情報を表示する SBS コンソール

SBS アドインと EBS アドインをインストールする

SBS アドインまたは EBS アドインは、SBS 2008 または EBS 2008 が稼働しているコンピュータにビジネスセキュリティサーバをインストールすると、自動的にインストールされます。別のコンピュータでアドインを使用する場合は、手動でアドインをインストールする必要があります。

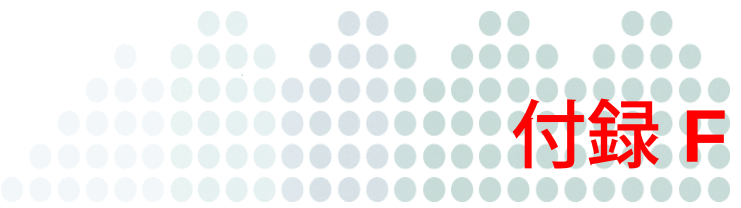
SBS 2008 または EBS 2008 のアドインを手動でインストールするには

1. SBS 2008 または EBS 2008 が稼働しているコンピュータから管理コンソールにアクセスします。
2. [オプション設定] → [ツール] をクリックし、[アドイン] タブをクリックします。
3. 対応する [ダウンロード] リンクをクリックし、SBS 2008 アドインまたは EBS 2008 アドインを取得します。
4. ローカルコンピュータで、ダウンロードしたファイルを開き、インストールを完了します。

SBS アドインと EBS アドインを使用する

SBS アドインと EBS アドインにより、管理者は高いレベルのセキュリティステータス情報とシステムステータス情報を SBS コンソールと EBS コンソールで表示できます。

SBS アドインまたは EBS アドインを使用するには、SBS コンソールまたは EBS コンソールを開きます。[セキュリティ] タブで、[Trend Micro ビジネスセキュリティ] をクリックしステータス情報を表示します。



付録 F

トラブルシューティングおよび Q&A

本付録では、一般的な問題に対する解決策とよくある質問に対する回答を示しています。

本付録で説明する内容には、次の項目が含まれます。

- 214 ページの「トラブルシューティング」
- 220 ページの「Q&A」
- 225 ページの「既知の制限事項」

トラブルシューティング

ここでは、Trend Micro ビジネスセキュリティ（以下、ビジネスセキュリティ）のインストール時または使用時に発生する可能性のある問題のトラブルシューティングに役立つ情報を示します。

接続が制限されている環境

インターネットへの接続に関して制限が設けられている環境、つまりクローズド LAN の場合やインターネット接続ができない環境の場合は、次の手順を使用してください。

ビジネスセキュリティクライアントからサーバにアクセスできる場合

1. Client Packager を使用して新しいパッケージを作成します（41 ページの「Client Packager を使用してインストールする」）。
2. このパッケージを手動でコンピュータにインストールします。

これで、サーバ上で設定されているとおりのセキュリティ設定がビジネスセキュリティクライアントに適用されます。

ビジネスセキュリティクライアントからサーバにアクセスできない場合

1. Client Packager を使用して新しいパッケージを作成します。
2. このパッケージを手動でコンピュータにインストールします。

Client Packager によるインストール後の問題

Client Packager を使用してビジネスセキュリティクライアントをインストールして、問題が発生した場合は、次の点について考慮してください。

- ・ **インストール**：ビジネスセキュリティクライアントからビジネスセキュリティサーバに接続できない場合、クライアントでは初期設定が維持されます。ビジネスセキュリティクライアントからビジネスセキュリティサーバに接続できる場合にのみ、クライアントはグループ設定を取得します。また、ビジネスセキュリティサーバに接続できない場合、再接続を試みるために頻繁にサービスを再起動することがあります。
- ・ **アップグレード**：Client Packager を使用したビジネスセキュリティクライアントのアップグレードの際に問題が発生した場合は、まず前のバージョンのビジネスセキュリティクライアントをアンインストールしてから新しいバージョンをインストールすることをお勧めします。

プログラム設定の保存と復元

ビジネスセキュリティプログラムをロールバックできるように、ビジネスセキュリティデータベースと重要な設定ファイルのコピーを保存できます。プログラム設定の復元が必要になるのは、問題が発生したためにビジネスセキュリティを再インストールする場合や、直前の設定に戻す必要が生じた場合です。

ロールバック後または再インストール後にプログラム設定を復元するには

1. ビジネスセキュリティサーバの「Trend Micro Security Server Master Service」を停止します。
2. 以下のファイルおよびフォルダを、別の場所に手動でコピーします。

警告： この作業にバックアップ用のツールやアプリケーションを使用しないでください。

C:\Program Files\Trend Micro\Security Server\PCCSRV

- **ofcscan.ini** — グローバル設定を含んでいます。
 - **ous.ini** — ウイルス対策コンポーネント インストールのアップデート元のテーブルを含んでいます。
 - **Private** フォルダ — ファイアウォールおよびアップデート元の設定を含んでいます。
 - **Web\TmOPP** フォルダ — 大規模感染予防の設定を含んでいます。
 - **Pccnt\Common\OfcPfw.dat** — ファイアウォールの設定を含んでいます。
 - **Download\OfcPfw.dat** — ファイアウォール インストール設定を含んでいます。
 - **Log** フォルダ — システムイベントおよび接続状態の確認ログを含んでいます。
 - **Virus** フォルダ — ビジネスセキュリティによって感染ファイルが隔離されるフォルダです。
 - **HTTPDB** フォルダ — ビジネスセキュリティデータベースを含んでいます。
3. ビジネスセキュリティをアンインストールします。
 4. 新規インストールを実行します。45 ページの「サーバのインストール」を参照してください。
 5. セットアッププログラムが完了したら、復元先コンピュータ上の「Trend Micro Security Server Master Service」を停止します。

6. バックアップファイルに記載されているウイルスパターンファイルのバージョンを更新します。
 - a. 再インストール後のサーバから現在のウイルスパターンファイルのバージョンを確認します。¥Trend Micro¥Security Server¥PCCSRV¥Private¥component.ini.を開き、以下の項目を探します。

```
-----  
ComponentName= ウイルスパターンファイル  
Version=xxxxxx 0 0  
-----
```

xxxxxx の部分がウイルスパターンファイルのバージョンです。

- b. バックアップファイル内のウイルスパターンファイルのバージョンをアップデートします。
¥Private¥component.ini

注意： ビジネスセキュリティサーバのインストール先を変更している場合、バックアップファイルの ofcscan.ini と ¥private¥ofcserver.ini のパス情報を更新する必要があります。

7. 作成したバックアップを使用して、ビジネスセキュリティデータベースと対象コンピュータ上の PCCSRV フォルダ内の関連ファイルと関連フォルダを上書きします。
8. ビジネスセキュリティサーバマスターサービスを再起動します。

一部のコンポーネントをインストールできない

トレンドマイクロ製品の各種コンポーネントに対するライセンスは、地域によって異なります。インストール完了後、ご使用のレジストレーションキー / アクティベーションコードで利用可能なコンポーネントの概要を参照できます。ライセンスを所有しているコンポーネントについて確認するには、トレンドマイクロの営業部または販売代理店にお問い合わせください。

管理コンソールにアクセスできない

ここでは、管理コンソールにアクセスできない場合に考えられる原因について説明します。

ブラウザのキャッシュ

以前のバージョンのビジネスセキュリティからアップグレードした場合は、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管理コンソールをロードできないことがあります。ブラウザのキャッシュファイルをクリアしてください。また、管理コンソールへのアクセスに使用するコンピュータとビジネスセキュリティサーバとの間にプロキシサーバがある場合は、プロキシサーバのキャッシュファイルもクリアしてください。

SSL 証明書

Web サーバが正常に機能していることも確認します。SSL を使用する場合は、SSL 証明書が有効であることも確認します。詳細については、Web サーバのドキュメントを参照してください。

仮想ディレクトリの設定

管理コンソールを IIS サーバ上で実行しているときに、次に示すメッセージが表示される場合は、仮想ディレクトリの設定に問題がある可能性があります。

ページを表示できません。

HTTP エラー 403.1 - 許可されていません：実行のアクセスが拒否されました。

インターネット インフォメーション サービス (IIS)

このメッセージは、次のいずれかのアドレスを使用して管理コンソールにアクセスしたときに表示される可能性があります。

`http://<サーバ名>/SMB/`

`http://<サーバ名>/SMB/default.htm`

ただし、次のアドレスを使用した場合には、管理コンソールは問題なく開きます。

`http://<サーバ名>/SMB/console/cgi/cgichkmasterpwd.exe`

この問題を解決するには、SMB 仮想ディレクトリの実行アクセス許可を確認してください。

スクリプトを実行できるようにするには

1. インターネット インフォメーション サービス (IIS) マネージャを起動します。
2. SMB 仮想ディレクトリで、[プロパティ] を選択します。
3. [仮想ディレクトリ] タブを選択し、[なし] から [スクリプト] に実行アクセス許可を変更します。クライアントのインストール仮想ディレクトリの実行アクセス許可も変更します。

管理コンソールに表示されるクライアントの数が正しくない

管理コンソールに表示されるクライアント数は、正しくない場合があります。

この問題は、クライアントプログラムの削除後もデータベースにそのクライアントのレコードが残ってしまった場合に起こります。たとえば、ビジネスセキュリティクライアントを削除しているときにサーバ/クライアント間の通信が切断されると、サーバはビジネスセキュリティクライアントが削除されたことを認識できません。サーバはデータベースにクライアント情報を保存し、削除されたクライアントのアイコンを管理コンソールに表示し続けます。ビジネスセキュリティクライアントを再インストールすると、サーバのデータベース内に新しいレコードが作成され、管理コンソールに新しいアイコンが表示されます。

管理コンソールから接続状態の確認機能を使用し、重複したクライアントレコードがないかを確認します。

インストールしたクライアントのアイコンが表示されない

ビジネスセキュリティクライアントをインストールした後に、そのクライアントのアイコンが管理コンソールに表示されないことがあります。この問題は、クライアントがステータスをサーバに送信できないときに起こります。

クライアントと管理コンソールとの通信を確認するには

- クライアントで Web ブラウザを起動し、アドレスバーに「`https://{ビジネスセキュリティサーバ名}:{ポート番号}/SMB/cgi/cgionstart.exe`」と入力して <Enter> キーを押します。次の画面に「-2」が表示されている場合、クライアントはサーバと通信できることを意味しています。また、これはサーバのデータベースにクライアントの記録がなく、サーバデータベース側に問題がある可能性を示しています。
- ping コマンドおよび telnet コマンドを使用してクライアント/サーバ間が接続されているかどうかを確認します。
- 帯域幅が制限されている場合、それによってサーバ/クライアント間に接続タイムアウトが発生していないかを確認します。
- サーバの ¥PCCSRV フォルダに共有権限があるかどうか、およびすべてのユーザにこのフォルダのフルコントロール権限が付与されているかどうかを確認します。
- ビジネスセキュリティサーバのプロキシ設定が正しいことを確認します。

他のウイルス対策ソフトウェアからの移行時の問題

ここでは、他社製ウイルス対策ソフトウェアから移行するときに発生する可能性がある問題について説明します。

ビジネスセキュリティクライアントのセットアッププログラムは、他社製ソフトウェアのアンインストールプログラムを使用して、ユーザのシステムからこのソフトウェアを自動的に削除し、ビジネスセキュリティクライアントに置き換えます。自動アンインストールが失敗すると、ユーザは次のメッセージを受け取ります。

Uninstallation failed.

このエラーには、いくつかの原因が考えられます。

- ・ 他社製ソフトウェアのバージョン番号またはプロダクトキーが不整合である
- ・ 他社製ソフトウェアのアンインストールプログラムが動作しない
- ・ 他社製ソフトウェアの特定のファイルがないか破損している
- ・ 他社製ソフトウェアのレジストリキーを削除できない
- ・ 他社製ソフトウェアにアンインストールプログラムがない

このエラーには、いくつかの解決策が考えられます。

- ・ 他社製ソフトウェアを手動で削除します。
- ・ 他社製ソフトウェアのサービスを停止する
- ・ 他社製ソフトウェアのサービスまたはプロセスをアンロードする

Web ページまたはリモートからのインストールの失敗

Web ページからのインストールができない、またはリモートインストールに失敗したという報告がユーザから寄せられたら、次の方法を試してください。

- ・ ネットワーク接続のプロパティから「Microsoft ネットワーク用ファイルとプリンタ共有」を有効に設定します。
- ・ ping コマンドおよび telnet コマンドを使用してクライアント / サーバ間が接続されているかどうかを確認します。
- ・ クライアントで TCP/IP が有効になっているか、またその設定が正しいかを確認します。
- ・ クライアント / サーバ間の通信にプロキシサーバを使用している場合は、プロキシ設定が正しいかどうかを確認します。
- ・ Web ブラウザで、トレンドマイクロのアドオンおよび表示履歴を削除します。

Q&A

次のリストは、よくある質問とその回答をまとめたものです。

アクティベーションコードとレジストレーションキーの取得方法

ビジネスセキュリティは、インストールプロセス中にまたは後で管理コンソールを使用してアクティベートできます。ビジネスセキュリティをアクティベートするには、アクティベーションコードが必要です。

アクティベーションコードを取得する

トレンドマイクロの Web サイトからビジネスセキュリティをダウンロードすると、体験版のアクティベーションコードが自動的に送信されてきます。

レジストレーションキーを使用して、アクティベーションコードをオンラインで取得することができます。

アクティベーションコードは、次のように 37 文字で構成されます。

XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

レジストレーションキーを取得する

レジストレーションキーは、次の場所から取得できます。

- 製品 CD
- ライセンス証明書（製品の購入後に取得）

レジストレーションキーは、次のように 22 文字で構成されます。

XX-XXXX-XXXX-XXXX-XXXX

製品版の使用期限が切れた場合、セキュリティのアップデート機能は無効になります。体験版の使用期限が切れた場合、セキュリティのアップデートと検索機能の両方が無効になります。[製品ライセンス] 画面で、アクティベーションコードのオンラインでの取得、更新手順の表示、および製品ステータスの確認を実行できます。

登録

ビジネスセキュリティの登録に関していくつか質問があります。どこで回答を得られますか。

登録に関するよくある質問については、次の Web サイトにアクセスして、キーワード検索を実行してください。

<http://esupport.trendmicro.co.jp/corporate/default.aspx>

インストール、アップグレード、および互換性

このバージョンのビジネスセキュリティにアップグレードできるビジネスセキュリティのバージョンを教えてください。

詳細については、「インストールガイド」を参照してください。

自分のネットワーク環境ではどのクライアントインストール方法が最適ですか。

「管理者ガイド」を参照してください。さまざまなクライアントインストール方法の概要と比較が記載されています。

Citrix または Windows ターミナルサービスを使用して、リモートにビジネスセキュリティサーバをインストールできますか。

はい。Citrix または Windows ターミナルサービスでリモートにビジネスセキュリティサーバをインストールできます。

ビジネスセキュリティは 64 ビットプラットフォームをサポートしていますか。

はい。ビジネスセキュリティクライアントは、X64 ビットプラットフォームで使用できます。しかし、現在 IA-64 プラットフォームでは使用できません。

Trend Micro ServerProtect からビジネスセキュリティにアップグレードできますか。

いいえ。まず ServerProtect をアンインストールする必要があります。そのうえでビジネスセキュリティをインストールできます。

ビジネスセキュリティサーバのインストール先コンピュータに前もってインストールされている Apache Web サーバを使用できますか。

前もってインストールされている Apache は使用しないことをお勧めします。ビジネスセキュリティサーバのインストールと同時に、正しいバージョンの Apache がインストールされます。

パスワードを忘れた・紛失した場合

ビジネスセキュリティのコンソールにアクセスするにはパスワードが必要です。このパスワードはインストール時に定義され、後でいつでも変更できます。パスワードを紛失したまたは忘れた場合は、ビジネスセキュリティサーバ・クライアントの再インストールをお願いいたします。

設定

ビジネスセキュリティの設定に関していくつか質問があります。どこで回答を得られますか。

次のサイトから、ビジネスセキュリティのドキュメントをダウンロードできます。

<http://www.trendmicro.co.jp/download/product.asp?productid=49>

よくあるご質問をまとめたページもご用意しています。

<http://esupport.trendmicro.co.jp/Pages/JP-2062710.aspx>

ウイルス対策ソフトウェアを **Small Business Server (SBS) 2003** とともに使用するときは、どのフォルダを除外すればよいでしょうか。

Small Business Server 2003 の除外設定については、次の表を参照してください。

表 F-1. IIS 除外設定

IIS システムファイル	C:\WINDOWS\system32\inet_srv
IIS 圧縮フォルダ	C:\WINDOWS\IIS Temporary Compressed Files

表 F-2. ドメインコントローラ除外設定

Active Directory データベース ファイル	C:\WINDOWS\NTDS
SYSVOL	C:\WINDOWS\SYSVOL
NTFRS データベースファイル	C:\WINDOWS\ntfrs

表 F-3. Windows SharePoint Services 除外設定

SharePoint 一時フォルダ	C:\windows\temp\FrontPageTempDir
-------------------	----------------------------------

表 F-4. クライアントデスクトップフォルダ除外設定

Windows Update Store	C:\WINDOWS\SoftwareDistribution\DataStore
----------------------	---

表 F-5. その他の除外設定

リムーバブル記憶域データベース (Small Business Server のバックアップで使用)	C:\Windows\system32\NtmsData
Small Business Server POP3 接続エラーメール	C:\Program Files\Microsoft Windows Small Business Server\Networking\POP3\Failed Mail
Small Business Server POP3 接続受信メール	C:\Program Files\Microsoft Windows Small Business Server\Networking\POP3\Incoming Mail
Windows Update Store	C:\WINDOWS\SoftwareDistribution\DataStore
DHCP データベースストア	C:\WINDOWS\system32\dhcp
WINS データベースストア	C:\WINDOWS\system32\wins

パターンファイルまたは Service Pack が最新かどうかの確認

アップデート可能なファイルは、インストールされている製品によって異なります。

最新のパターンファイルまたは Service Pack を使用しているかどうかを確認するには

1. 管理コンソールで、[オプション設定] → [製品ライセンス] の順にクリックします。[製品ライセンス] 画面が表示されます。
2. 現在の製品バージョンなどの製品ライセンスの詳細が表示されます。

取得可能な最新のパターンファイルがあるかどうかを確認するには、Web ブラウザで次のいずれかの URL にアクセスします。

- トレンドマイクロのアップデートセンター：
<http://www.trendmicro.co.jp/download/product.asp?productid=49>
- トレンドマイクロのパターンファイル：
<http://www.trendmicro.co.jp/support/pattern.asp>

スマートスキャン

スマートスキャンとは何ですか。

スマートスキャンは、トレンドマイクロの新しいテクノロジーであり、Trend Micro グローバルスマートスキャンサーバを使用することによってクライアントでの検索の負担を軽減する機能です。

スマートスキャンの信頼性は高いですか。

はい。スマートスキャンでは、別のコンピュータであるスマートスキャンサーバを使用して、クライアントの検索を支援します。クライアントがスマートスキャン用に設定されているが、スマートスキャンサーバに接続できない場合、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への接続を試みます。

スマートスキャンサーバが正常に動作していることを確認する方法を教えてください。

ビジネスセキュリティサーバで次のサービスが実行されていることを確認します。

Trend Micro Smart Scan Service

スマートスキャンサーバをアンインストールすることやインストールしないことを選択できますか。

いいえ。スマートスキャンを使用しない場合は、スマートスキャンのサービスを無効にしてください。これによって、すべてのクライアントが従来型スキャンモードに切り替わり、ビジネスセキュリティサーバ上のスマートスキャンサービスが停止します。これによって、ビジネスセキュリティサーバのパフォーマンスを向上できます。

既知の制限事項

既知の制限事項とは、ビジネスセキュリティソフトウェアにおいて、一時的に回避策が必要となる機能を指します。既知の制限事項は一般に、製品付属の Readme ドキュメントに記載されています。トレンドマイクロ製品の Readme ファイルは、最新版ダウンロードのページからダウンロードすることもできます。

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

テクニカルサポートの製品 Q&A のページでも、既知の制限事項を検索できます。

<http://esupport.trendmicro.co.jp/corporate/default.aspx>

Readme には必ず目を通すことをお勧めします。Readme には、インストールやパフォーマンスに影響する既知の問題に加えて、そのリリースの新機能の説明や、システム要件、およびその他のヒントも記載されています。

ヘルプ情報へのアクセス

本付録では、オンラインヘルプのアクセス方法、詳細情報の検索方法、およびトレンドマイクロへの問い合わせ方法について説明します。

本付録で説明する内容には、次の項目が含まれます。

- 228 ページの「製品ドキュメント」
- 229 ページの「製品サポート情報」
- 229 ページの「サポートサービスについて」
- 230 ページの「製品 Q&A のご案内」
- 230 ページの「セキュリティ情報」
- 231 ページの「トレンドマイクロへのウイルス解析依頼」
- 231 ページの「ウイルス解析サポートセンター「TrendLabs」」

製品ドキュメント

Trend Micro ビジネスセキュリティ (以下、ビジネスセキュリティ) には、次のドキュメントがあります。

- オンラインヘルプ

管理コンソールからアクセスできる Web ベースのドキュメントです。

ビジネスセキュリティのオンラインヘルプでは、製品の機能とその使用方法を説明しています。設定をカスタマイズしたり、セキュリティタスクを実行したりするための詳細な情報も含まれています。状況依存ヘルプを表示するには、アイコンをクリックしてください。

オンラインヘルプの対象者

特定の画面について詳しい説明を必要とするビジネスセキュリティの管理者

- インストールガイド

インストールガイドは、図解を多く使ってインストール操作の手助けを行います。

- クイックスタートガイド

「クイックスタートガイド」には、製品をインストールまたはアップグレードして使い始めるための手順が記載されています。ビジネスセキュリティの基本的な機能と初期設定についても説明しています。

「クイックスタートガイド」は製品 CD-ROM に含まれています。また、次の最新版ダウンロードページからもダウンロードできます。

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

このガイドの対象者

ビジネスセキュリティをインストールして使い始めるビジネスセキュリティの管理者

- 管理者ガイド

「管理者ガイド」には、製品を設定および管理するための全般的な手順が示されています。

「管理者ガイド」は製品 CD-ROM に含まれています。また、次の最新版ダウンロードページからもダウンロードできます。

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

このガイドの対象者

ビジネスセキュリティをカスタマイズ、管理、または使用する必要があるビジネスセキュリティの管理者

- Readme ファイル

Readme ファイルには、オンラインまたは印刷ドキュメントに記載されていない、最新の製品情報が記載されています。新機能、インストールのヒント、既知の問題、ライセンス情報などのトピックがあります。

- 製品 Q&A

製品 Q&A は、問題の解決策およびトラブルシューティングの情報を提供するオンラインデータベースです。製品の既知の問題に関する最新情報を参照できます。製品 Q&A には、次の Web サイトからアクセスできます。

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

製品サポート情報

ビジネスセキュリティのユーザ登録により、さまざまなサポートサービスを受けることができます。

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

サポートサービスについて

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

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

契約の有効期限は、ユーザ登録完了から 1 年間です（ライセンス形態によって異なる場合があります）。契約を更新しないと、パターンファイルや検索エンジンの更新などのサポートサービスが受けられなくなりますので、契約満了前に必ず更新してください。更新手続きの詳細は、トレンドマイクロの営業部、または販売代理店までお問い合わせください。

注意： サポートセンターへの問い合わせ時に発生する通信料金は、お客さまの負担とさせていただきます。

製品 Q&A のご案内

トレンドマイクロの Web サイトでは、製品 Q&A の情報を提供しています。これは、トレンドマイクロの製品に関する技術的な質問と、それに対する回答を集めたものです。製品 Q&A には、次の URL からアクセスできます。

製品 Q&A

<http://esupport.trendmicro.co.jp/corporate/search.aspx>

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

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

セキュリティ情報

セキュリティ情報の入手先

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

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

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

セキュリティ情報 Web サイトでは、次の情報を閲覧できます。

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

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

トレンドマイクロへのウイルス解析依頼

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

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

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

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

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

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

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

ウイルス解析サポートセンター「TrendLabs」

トレンドマイクロのウイルス解析サポートセンター「TrendLabs」(トレンドラボ) は、フィリピンセンターを本部として、米国、日本、台湾、ドイツ、アイルランド、中国、フランス、メキシコの各国センターで構成されています。24 時間体制でウイルスの活動を監視するウイルス解析エンジニアを含む 1000 名以上のスタッフが、セキュリティに関する最新の情報を収集し、高品質なサービスとソリューションを迅速かつ効果的に世界各国のトレンドマイクロのパートナーとお客さまに提供しています。

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

用語集

用語集では、このマニュアルで使用されている重要な用語と概念について説明します。セキュリティ上の脅威の詳細については、次の Web ページを参照してください。

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

Trend Micro Smart Protection Network による保護方法の詳細については、次の Web ページを参照してください。

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

用語	説明
アクティベーションコード	脅威の検索と製品のアップデートを有効にするために必要な数値コードです。製品のアクティベートは、インストール中、またはインストール後いつでも実行できます。アクティベーションコードをお持ちでない場合は、製品に付属のレジストレーションキーを使用して、トレンドマイクロの Web サイトで登録し、アクティベーションコードを取得してください。
トレンドマイクロのアップデートサーバ	アップデート実行時には、トレンドマイクロのアップデートサーバに接続され、アップデートサーバから、ウイルスパターンファイル、検索エンジン、プログラムファイルなどの最新コンポーネントをダウンロードできます。アップデートは、多くのトレンドマイクロ製品に共通の機能です。
管理者	新しいハードウェアおよびソフトウェアの設定、ユーザ名とパスワードの割り当て、ディスク領域などの IT リソースの監視、バックアップの実行、およびネットワークセキュリティの管理などの作業の責任を担う組織内の担当者です。
エージェント	クライアント上で実行されるビジネスセキュリティプログラムです。
駆除	ファイルまたはメッセージからウイルスコードを削除することです。
クリーンナップ	クリーンナップは、トロイの木馬およびトロイの木馬によってインストールされたアプリケーションやプロセスを検出し、削除します。トロイの木馬によって変更されたファイルも修復します。
クライアント	クライアントとは、コンピュータを保護するためのビジネスセキュリティクライアントプログラムがインストールされているコンピュータ、およびサーバのことです。
設定	たとえばウイルスに感染したメールメッセージを隔離するかそれとも削除するかを選択するなど、トレンドマイクロ製品が機能する方法を指定するオプションを選択します。
コンテンツフィルタ	メールに、所属組織の人事ポリシーや IT メッセージポリシーで禁止されたコンテンツ（語句）が含まれていないかどうかを検索することです。禁止されるコンテンツの例としては、憎悪のメール、冒瀆的言動、ポルノなどがあります。
従来型スキャン	クライアント上のローカル検索エンジンで、クライアントのコンピュータを検索することです。

用語	説明
エンドユーザ使用許諾契約書 (EULA)	エンドユーザ使用許諾契約書 (EULA) は、ソフトウェア発行元とソフトウェアユーザ間の法的な契約書です。この契約書では通常、ユーザ側における制限事項の概要が示されます。ユーザはインストール時に「同意します」をクリックしないで、契約の同意を拒否できます。「同意しません」をクリックすると、ソフトウェア製品のインストールは中止されます。 フリーソフトなどでは、インストール時に表示されるエンドユーザ使用許諾契約書で不用意に「同意します」をクリックすると、スパイウェアやグレーウェアが気付かぬうちにコンピュータにインストールされてしまう場合があります。
最新ステータス	最新ステータスを表示すると、大規模感染予防、ウイルス対策、スパイウェア対策、およびネットワークウイルスのセキュリティステータスを一目で確認できます。
パターンマッチング	各ウイルスには一意の「シグニチャ」、つまり他のコードと区別できる特性を表す文字列が含まれているので、トレンドマイクロのウイルス専門家は、この文字列から実行機能を持たない断片を取り出してパターンファイルに取り込みます。検索エンジンは、各検索対象ファイルの特定領域をウイルスパターンファイルのパターンと比較し、一致するものを探します。一致が見つかった場合、ウイルスが検出され、管理者にメールで通知が送信されます。
権限 (クライアント権限)	ビジネスセキュリティクライアントの権限はまず、管理者が管理コンソールで設定します。その後、エンドユーザは許可された権限に従って、クライアントを検索するようにビジネスセキュリティクライアントを設定できます。組織全体で一貫したウイルス対策ポリシーを実施するには、クライアント権限を使用します。
レジストレーションキー	トレンドマイクロに登録してアクティベーションコードを取得するために必要な数値コードです。
スキャンサーバ	クライアントの検索を支援するサーバです。これにより、クライアントでは検索プロセス全体をクライアント自体で実行する必要がなくなります。
ビジネス セキュリティサーバ	ビジネスセキュリティを初めてインストールしたときに、インストール先のコンピュータがビジネスセキュリティサーバとなります。ビジネスセキュリティサーバは、クライアントにインストールされたビジネスセキュリティクライアントと通信します。ビジネスセキュリティサーバは管理コンソールもホストします。この管理コンソールは、ビジネスセキュリティ全体を集中管理する Web ベースのコンソールです。
スマートスキャン	スキャンサーバがクライアントの検索を支援します。

用語	説明
TrendLabs (トレンドラボ)	TrendLabs は、トレンドマイクロが誇る、ウイルス対策研究および製品サポートセンターのグローバルネットワークです。このセンターでは、世界中のトレンドマイクロのお客さまに対して、年中無休でサービスを提供しています。
Trend Secure	Trend Secure は、ブラウザベースのプラグインツールのセット (Trend プロテクト) で構成されており、それらによってユーザは安全に Web を閲覧できます。Trend プロテクトは、不正な Web サイトやフィッシング Web サイトに関する警告を表示します。
アップデート エージェント	他のエージェントに対するアップデート元としての役割を持つエージェントです。
管理コンソール	管理コンソールは、集中管理を行うための Web ベースのコンソールです。管理コンソールでは、コンピュータを保護するビジネスセキュリティクライアントの設定内容を指定できます。管理コンソールは、ビジネスセキュリティサーバのインストール時にインストールされます。このコンソールでは、ActiveX、CGI、HTML、HTTP などのインターネット技術が使用されます。

索引

英数字

1 回限りのレポート 161

AOL インスタントメッセージャー 133

autopcc.exe 40、41

Client Packager 41、206

グラフィックユーザインタフェースの使用 43

CPU

使用率 114

適合して変化する検索 13

DLL (プログラムライブラリ) インジェクション 80

Hosts ファイルの変更 79

HotFix 154

ICQ インスタントメッセージャー 133

IntelliTrap 67、113、193

Internet Explorer 設定の変更 80

Internet Explorer プラグインの追加 80

Itanium 2 アーキテクチャ 188

MSI ファイル 45

MSN メッセージャー 133

OLE 階層 131

Packer 22

Patch 154

Ping of Death 71

POP3 メール検索 85

設定 85

Readme ファイル 228

Safe Computing Guide 197

SBS アドインおよび EBS アドイン 210

Service Pack 154

SMTP サーバ 128

SSL 証明書 217

SYN フラッド 72

TMVS.ini 205

Trend Micro Smart Protection Network 12、14、175

Trend Secure 84

設定 84

TrendLabs 231

定義 236

Trend プロテクト

コンポーネント 19

URL フィルタ 12、16

脅威ステータスの表示 31

設定 78

レポート 163

ログ 159

USB デバイス 13

脅威 79

VSAPI.dll 207

VSEncode.exe 207

Web からの脅威 15

Web レピュテーションの使用 77

Web レピュテーション 15、132、194

脅威ステータスの表示 31

コンポーネント 18、144

スコア 195

セキュリティレベル 77

設定 76

フィルタ強度 78

- レポート 162
- ログ 159
- Windows Essential Business Server 209
- Windows Live メッセンジャー 133
- Windows Small Business Server 209
- Windows ショートカットメニュー
 - 手動検索の追加 131
- Windows スクリプト 41
- Windows リモートインストール 45
 - Windows Vista 46
- Yahoo! メッセンジャー 133

あ

- アイコン
 - 管理コンソール 27
 - クライアント 182
 - [最新ステータス] 画面 30
- アクティベーションコード 220
- 新しい機能 12
- 圧縮ファイル 113
 - 検索 131
 - 検索階層数 67
- アップデート 142、148
 - HotFix、Patch、および Service Pack 154
 - アップデート 142
 - アップデートエージェントの使用 149
 - アップデートサーバの使用 148
 - アップデート元 146
 - アップデート元の選択 148
 - コンポーネント 143
 - システムステータスの表示 31

- 手動 151
- 初期設定のアップデート 145
- 設定 146
- 大規模感染予防 104
- 同期 153
- 予約 152
- ロールバック 153
- ログ 159
- アップデートエージェント 149
- アドイン 209
- アドウェア 21
- アラート
 - イベントのメール通知 122
 - クライアントでのウイルス / スパイウェアの検出 68
 - クライアントでのファイアウォール違反 74
 - グローバル設定 133
 - 大規模感染予防のステータスアラート 96
- アンインストール
 - ビジネスセキュリティサーバ 176
- 暗号化ファイルの検索 66
- イエローアラート 101
- クイックスタートガイド 228
- インスタントメッセンジャー
 - 脅威 22
 - コンテンツフィルタ 133
- インストール用 Web ページ 38
- [ウイルス / スパイウェア対策] 画面 66
- ウイルス対策
 - 脅威ステータスの表示 30
 - コンポーネント 17

レポート 162
ウイルス対策コンポーネント 144
ウイルスログ 159
エージェント
 使用ログ 132
 定義 23
 プログラム 135
エージェントの終了
 設定 135
オーバーラッピングフラグメント 72
オフラインのビジネスセキュリティクライアント
 135

か

概要、製品 12
拡張子 113
確認
 クライアントとサーバの接続 137
隔離
 管理 89
 グローバル設定 138
 すべてのファイルの削除 139
 ディレクトリの設定 89
 ファイルの最大サイズ 139
 フォルダの容量 139
隔離ツール 13
仮想ディレクトリの設定 217
過大フラグメント 71
環境変数 83
監視サービス 134
感染ファイル暗号化処理の復元ツール 206

感染ファイルの駆除 68
管理コンソール
 URL 26
 アイコン 27
 イベントログ 158
 説明 26
 定義 23
 パスワード 172
 開く 26
管理者ガイド 228
管理ツール 200
キーロガー 21
機能 12
機能、製品 14
脅威 19
 Packer 22
 Ping of Death 71
 SYN フラッド 72
 Web からの脅威 15
 アドウェア 21
 ウイルス 20
 オーバーラッピングフラグメント 72
 過大フラグメント 71
 キーロガー 21
 重複 ARP 71
 侵入 22
 スパイウェア 21
 スパムメール 22
 タイニーフラグメント攻撃 72
 ダイヤルアップ接続ソフトウェア 21
 ティアドロップ攻撃 72

- トロイの木馬 20
- ネットワークウイルス 21
- ハッキングツール 21
- バックドアプログラム 20
- 不正挙動 22
- 不正プログラム 20
- フラグメント化 IGMP 72
- ボット 21
- マクロウイルス 20
- メッセンジャープログラム 22
- ランドアタック 72
- ルートキット 20
- ワーム 20
- 脅威に対する処理 67、114
- 脅威の通知 120
- 挙動監視 79
 - USB からの脅威に対する保護 79
 - 脅威ステータスの表示 31
 - グローバル設定 133
 - コンポーネント 19、144
 - 設定 81
 - レポート 163
- クライアント
 - 32 ビットおよび 64 ビット 188
 - USB からの脅威に対する保護 79
 - アイコン 182
 - 管理コンソールからの削除 58
 - グループ間の移動 60
 - グループ内の表示 56
 - グループへの追加 58
 - 権限 86
 - 種類 182
 - スタンドアロンモード 187
 - 設定のインポートとエクスポート 62
 - 定義 23
 - ロケーション認識 186
 - クライアント移動ツール 208
 - クライアントツール 206
 - クリーンナップ実行 100
 - グループ
 - 概要 56
 - クライアントの移動 60
 - クライアントの削除 58
 - クライアントの追加 58
 - クライアントの表示 56
 - 設定の複製 61
 - 追加 57
 - グローバル設定 125
 - SMTP サーバ 128
 - Web レピュテーション 132
 - アラート 133
 - 一般検索設定 130
 - ウイルス検索設定 131
 - エージェント終了 135
 - 隔離フォルダ 138
 - 監視サービス設定 134
 - 挙動監視 133
 - 承認済み URL 132
 - スパイウェア / グレーウェア設定 132
 - デスクトップ / サーバ 128
 - ビジネスセキュリティクライアントのアンインストール 134

- プロキシサーバ 126
- メッセージコンテンツフィルタ 133
- ロケーション認識 130
- 権限
 - クライアント 86
- 検索
 - CPU 使用率 114
 - CPU 使用率に適合 13
 - IntelliTrap の使用 67、113
 - OLE 階層 131
 - POP3 メール 85
 - 圧縮ファイル 67、113、131
 - 一般検索設定 130
 - 拡張子 113
 - 脅威に対する処理の実行 67
 - 検索可能ファイル 66
 - 検索されないトレンドマイクロ製品 177
 - [検索対象] タブ 66
 - 検索の種類 111
 - システム領域 113
 - 従来型スキャン 110
 - 手動 (オンデマンド) 65
 - 手動検索ショートカットの追加 131
 - 除外 67、113
 - スパイウェア / グレーウェア 114
 - スマートスキャン 12、15、110
 - 設定 112
 - 特定の拡張子 66
 - ドライブ 67
 - トレンドマイクロ製品のフォルダ 67、113
 - トレンドマイクロの推奨処理の使用 67
 - トレンドマイクロの推奨設定の使用 66、113
 - ネットワークドライブ 67、113
 - ファイルのバックアップ 68、114
 - 予約 65、116
 - リアルタイム 65、66
 - オプション 67
 - 設定 66
 - ログ 159
- 検索、USB デバイス 13
- 検索可能ファイル 66
- 検索の種類 65、111
- 検索方法 110
- 互換性 221
- コンテンツフィルタ 12
 - コンポーネント 19
 - メッセンジャープログラムのグローバル設定 133
- コンポーネント
 - Trend プロテクト 19
 - Web レピュテーション 18、144
 - アップデート 142、143
 - アップデート可能 144
 - アップデートサーバを使用したアップデート 142
 - ウイルス対策 17、144
 - 挙動監視 19、144
 - コンテンツフィルタ 19
 - スパイウェア対策 17、144
 - 大規模感染予防 18、144
 - 同期 153
 - ネットワークウイルス 18、145

ロールバック 153

さ

サービスの追加 81

最新ステータス 13、19

アイコン 30

アップデート間隔 31

画面の概要 29

脅威ステータス 30

システムステータス 31

ライセンスステータス 31

シェル設定の変更 80

システム異常イベント

システムステータスの表示 31

システムイベント通知 120

システムファイルの複製 79

システムファイルの変更 80

システム領域の検索 113

実際のファイルの種類 194

自動アップデート 152

自動実行ファイル 79

重複 ARP 71

従来型スキャン 110

手動アップデート 151

手動検索 65、112

Windows メニューのショートカット 131

承認済み URL

グローバル設定 132

承認済みプログラムリスト 83

除外

検索 67

検索されないトレンドマイクロ製品 177

手動検索とリアルタイム検索 113

除外設定

環境変数の使用 83

挙動監視 82

大規模感染予防 104

ファイアウォール 74、75

初期設定 64

新機能 12

侵入検知システム 71

スキャンサーバ

定義 23

スタートアッププログラムの追加 81

スタンドアロンモードのクライアント 187

ステートフルインスペクション 71

スパイウェア / グレーウェア

グローバル設定 132

検索 114

除外リスト 115

処理の実行 114

スパイウェア / グレーウェアの除外リスト 115

スパイウェア対策

脅威ステータスの表示 30

コンポーネント 17、144

レポート 162

スパムメール 22

スパムメール対策

POP3 メール検索 85

スマートスキャン 12、15、110

システムステータスの表示 31

スマートフィードバック 14、175

脆弱性検索ツール 47、50、201

- 設定 202
 - 脆弱性診断 106、191
 - 脆弱なコンピュータ 96、99
 - 脆弱性診断設定 106
 - 製品
 - 概要 12
 - 機能 14
 - コンポーネントの用語集 23
 - ドキュメント 228
 - 製品 Q&A 229
 - セキュリティ設定 32
 - セキュリティポリシー設定の変更 80
 - 接続
 - クライアントとサーバ 137
 - 設定 222
 - ウイルス検索設定 131
 - 設定のインポート 62
 - 設定のエクスポート 62
 - 設定の複製 61
- た
- 大規模感染予防
 - イエローアラート 101
 - 脅威からの保護 96
 - 脅威ステータスの表示 31
 - 脅威に関する情報 95
 - 脅威の予防 94
 - クリーンナップ 97
 - 現在のステータスの表示 93
 - コンポーネント 18、144
 - 詳細の表示 105
 - 除外設定 104
 - 処理 93
 - 診断 / クリーンナップ 99
 - 推奨設定 102
 - ステータスアラート 96
 - 脆弱なコンピュータ 96、99
 - 設定 103
 - 戦略 92
 - レッドアラート 101
 - レポート 162
 - ログ 159
 - 大規模感染予防ポリシー 190
 - タイニーフラグメント攻撃 72
 - ダイヤルアップ接続ソフトウェア 21
 - ダウンロード
 - プログラムのアップデート 155
 - ダメージクリーンナップサービス 190
 - ツール 200
 - Client Packager 206
 - 感染ファイル暗号化処理の復元ツール 206
 - クライアント移動ツール 208
 - 脆弱性検索ツール 201
 - ログオンスクリプトウィザード 201
 - 通知 19、120
 - イベント設定 121
 - 脅威 120
 - システムタイプ 120
 - 設定 123
 - ライセンスイベント 121
 - ティアドロップ攻撃 72
 - テクニカルサポート 229

登録 221

ドキュメント 228

トラフィックのフィルタリング 71

トラブルシューティング 214

Client Packager 214

アクティベーションコードとレジストレーションキー 220

管理コンソール 216

管理コンソールに表示されるクライアント 218

クライアントのアイコン 218

コンポーネント 216

接続が制限されている環境 214

プログラム設定 215

トレンドマイクロのサービス

脆弱性診断 191

大規模感染予防ポリシー 190

ダメージクリーンナップサービス 190

トレンドマイクロの推奨処理 67、114、192

トレンドマイクロの推奨設定 66、113、192

トロイの木馬 20

な

ネットワークウイルス 21、71

脅威ステータスの表示 31

コンポーネント 18、145

レポート 163

ログ 159

ネットワークドライブ 67、113

は

パスワード 222

管理コンソール用に変更する 172

パスワードで保護されたファイルの検索 66

ハッキングツール 21

バックアップファイル 68、114

バックアッププログラム 20

ビジネスセキュリティクライアント 23

アンインストール 134

オフラインの削除 135

使用ログ 132

ビジネスセキュリティクライアントのアンインストール 52

エージェントプログラム 52

管理コンソール 52

設定 134

ビジネスセキュリティクライアントのインストール 37

Client Packager 41

MSI ファイル 45

Windows スクリプト 41

Windows リモートインストール 45

インストール方法 36

インストール用 Web ページ 38

概要 36

確認 49

脆弱性検索ツール 47、50

ビジネスセキュリティクライアントのアップグレードの阻止 88

メール通知 49

ログオンスクリプトウィザード 39

ビジネスセキュリティクライアントの削除 52

ビジネスセキュリティサーバ

定義 23

ファイアウォール 68

除外設定 74、75

初期設定 70

侵入検知システム 71

ステートフルインスペクション 71

セキュリティレベル 74

設定 73

トラフィックのフィルタリング 71

ネットワークウイルス 71

ポリシー設定の変更 80

モード 73

有効または無効 73

ファイル拡張子 66

ファイルレピュテーション 15

フィルタ、Web コンテンツ 12

不正挙動 22

不正プログラム 20

ブラウザのキャッシュ 217

プラグインマネージャ 173

フラグメント化 IGMP 72

プロキシサーバ

設定 126

プログラムの許可 83

ブロック

Web からの脅威 77

不要な Web コンテンツ 78

プログラム 83

プログラムリスト 83

ヘルプアイコン 27

ヘルプ情報へのアクセス 27

ヘルプファイル 228

変化する検索 13

変数 83

ポート

大規模感染予防の除外設定 104

保護機能 16

ボット 21

ま

マクロウイルス 20

メール通知によるビジネスセキュリティクライアントのインストール 49

メインメニュー 26

や

用語集 23

予約

レポート 161

予約検索 65、112、116

ら

ライセンス

イベント通知 121

期限切れ 174

更新 174

表示 173

変更 174

ライセンスステータスの表示 31

ランドアタック 72

リアルタイム検索 65

IntelliTrap の使用 67
詳細設定 67
設定 66
ルートキット 20
レジストレーションキー 220
レッドアラート 101
レポート 161
URL フィルタ 163
Web レピュテーション 162
ウイルス対策 162
解釈 161
管理 167
挙動監視 163
スパイウェア対策 162
生成 164
設定 164
大規模感染予防 162
ネットワークウイルス 163
ログ 158
クエリ 160
コンソールイベント 158
削除 168
自動削除 168
手動削除 169
デスクトップ/サーバ 159
ビジネスセキュリティクライアント、使用
132
ログオンスクリプトウィザード 39、201
ロケーション認識 130、186

わ

ワーム 20