F-Secure クライアント セキュリティ

管理者ガイド

目次

第 1 章 : はじめに.....9

システム要件.....10
ポリシー マネージャ サーバ.....10
ポリシー マネージャ コンソール.....11
主要コンポーネント.....12
機能.....13
製品を登録する.....14
アプリケーションの管理.....15
専門用語.....16

第 2 章 : アンインストール.....17

インストール手順.....18
インストール パッケージのダウンロードと実行.....18
インストールするコンポーネントを選択する.....18
インストールを完了する.....19
ポリシー マネージャ コンソールを起動する.....19
Web ブラウザのパスを変更する.....22
アンインストール.....23

第 3 章 : アンチウイルス モード.....25

「ポリシー ドメイン」タブ.....26
管理タブ.....27
「概要」タブ.....27
「設定」タブ.....29
「ステータス」タブ.....38
「警告」タブ.....40
「レポート」タブ.....41
「インストール」タブ.....41
「操作」タブ.....41
ツールバー.....43
メニュー コマンド.....44
設定を継承する.....46
継承された設定の見分け方 (ユーザ インターフェース).....46
ページの設定をすべてロック/ロック解除する.....47
設定を継承する (テーブル).....47

第 4 章 : 管理ネットワークのセットアップ.....49
ログイン.....50
接続プロパティ.....50
通信に関する設定を変更する.....50
ドメインとホストの管理.....52
ポリシー ドメインを追加する.....52
ホストを追加する.....53
Windows ドメインのホストを追加する.....53
自動登録ホストのインポート.....53
インストール情報の送信.....55
ポリシーベース インストール.....58
パッケージを利用したローカル インストール/更新.....60
ローカル インストールとポリシー マネージャ.....63
システム要件.....63
他のセキュリティ製品をアンインストールする.....63
インストール手順.....64
感染しているホストへのインストール.....65
集中管理の接続を確認する.....66

第 5 章 : ウイルスとスパイウェア防御.....67
自動更新.....68
自動更新の動作.....68
自動更新を設定する.....68
ポリシー マネージャ サーバからの自動更新を設定する.....68
ポリシー マネージャ プロキシを設定する.....69
ネイバーキャスト.....70
リアルタイム スキャン.....71
リアルタイム スキャンを設定する.....71
ドメイン全体にリアルタイム スキャンを有効にする.....72
ホストにリアルタイム スキャンの使用を強制する.....73
リアルタイム スキャンから Microsoft Outlook の .pst ファイルを除外する.....73
ディープガード.....74
ディープガードを設定する.....74
ディープガードのサーバ クエリ.....74
ルートキット スキャン (ブラックライト).....76
ルートキット スキャン.....76
ドメイン全体にルートキット スキャンを実行する.....76
メール スキャン.....77
メール スキャンを設定する.....77

受信および送信メールに対してメール スキャンを有効にする....78
Web スキャン....79
Web スキャンを設定する....79
ドメイン全体に Web スキャンを有効にする....79
Web サイトを Web スキャンから除外する....80
スパイウェア スキャン....81
スパイウェア制御を設定する....81
ドメイン全体にスパイウェア制御を設定する....82
スパイウェア スキャンをドメイン全体に実行する....83
スパイウェア/リスクウェアのコンポーネントを許可する....83
隔離保存されたオブジェクトを管理する....84
隔離保存されたオブジェクトを削除する....84
隔離保存されたオブジェクトを解除する....84
エンドユーザによる設定の変更をブロックする....86
ウイルス保護の設定を確定 (ロック) する....86
警告の転送....87
ウイルス警告を特定のメール アドレスに送信する....87
警告のポップアップを無効にする....87
ネットワーク上のウイルスを監視する....88
アンチウイルス保護を検証する....89

第 6 章：インターネット防御....91
ファイアウォールのセキュリティ レベル....92
セキュリティ レベルの構成....93
セキュリティ レベルとルール....94
セキュリティ レベルを選択する....94
ホストのデフォルト セキュリティ レベルを設定する....94
特定のドメインにセキュリティ レベルを追加する....95
ネットワークの隔離保存....97
ネットワークの隔離保存を設定する....97
ドメイン全体にネットワークの隔離保存を有効にする....97
ネットワークの隔離保存を調整する....97
インターネット防御の警告....98
警告ルールを追加する....98
アプリケーション通信制御....101
アプリケーション通信制御を設定する....101
アプリケーション通信制御をはじめて設定する....102
ルート レベルで不明なアプリケーションに対するルール....103
アプリケーション通信制御のルールを変更する....104
アプリケーション通信制御のポップアップを有効/無効にする....105
警告を確認して、インターネット防御の動作を確認する....106

侵入防止 107
侵入防止を設定する 107
デスクトップとノート コンピュータ に IPS を設定する 107

第 7 章：ネットワークを保護する 109
ホストが最新のポリシーを使用しているか確認する 110
サーバが最新のパターン ファイルを使用しているか確認する 111
ホストが最新のパターン ファイルを使用しているか確認する 112
ホストの接続状態を確認する 113
スキャン レポートを表示する 114
警告を表示する 115
週次感染レポートを作成する 116
ネットワーク攻撃の兆候を監視する 117

第 8 章：ソフトウェアのアップグレード 119
インストール エディタを使用する 120

第 9 章：ホストの操作 123
マニュアル スキャン 124
マニュアルスキャンを実行する 124
マルウェアを自動的に駆除する 125
マニュアルスキャンを実行する 126
スケジュール スキャン 127
スケジュール スキャンを設定する 127
スケジュール スキャンをキャンセルする 127
スケジュール スキャンのレポートを表示する 128
ファイアウォールの警告とログ ファイルの保存先 129
ファイアウォールの警告を表示する 129
アクション ログを表示する 130
パケット キャプチャでネットワークを監視する 130
ポリシー マネージャに接続してポリシー ファイルをインポートする 133
ダウンロードと更新を停止する 134
F-Secureのアンロードをユーザに許可する 135

第 10 章：ウイルス情報 137
マルウェア情報とF-Secureの Web ページにあるツール 138
ウイルスのサンプルをF-Secureに送る 139
ウイルス サンプルのパッケージを作成する 139
送信するパッケージについて 139

ウイルスのサンプルをエフセキュアに送る....140
ウイルスば発生した場合....142

第 11 章 : Cisco NAC プラグインの設定....145
Cisco NAC プラグインのインストール....146
Posture 検証属性の定義をインポートする....147
アプリケーション Posture トークンの属性....148

第 12 章 : 高度な機能 - ウイルスとスパイウェア防御....149
スケジュール スキャンを設定する....150
高度な機能 - ディープガード....152
イベントを拒否したときにユーザを通知する....152
他のプログラムからのイベントをを管理者権限のユーザが許可または拒否する....152
特定のプログラムからのイベントを許可または拒否する....152
ポリシー マネージャ プロキシを設定する....154
ポリシー マネージャ プロキシからホストの自動更新を設定する....155
プログラムを Web スキャンから除外する....156

第 13 章 : 高度な機能 - インターネット防御....157
インターネット防御をリモートから管理する....158
パケット ロギング....158
信頼済みのインターフェース....158
パケットのフィルタリング....159
セキュリティ レベルの自動選択....160
接続に関するトラブルシューティング....162
サービスを追加する....163
デフォルトの HTTP サービスに基づいたインターネット サービスを作成する....163
ダイヤルアップ制御の設定....166
電話番号を許可/拒否する....166
番号のロギング....166

第 14 章 : Prodsett.ini を設定する....169
Prodsett.ini を設定する....170

第 15 章 : メール スキャンの警告とエラー メッセージ....179
警告とエラー メッセージ....180

第 16 章 : インストール中に検出される競合製品....183

検出される競合製品.....184

第
1
章

はじめに

トピック：

- *システム要件*
- *主要コンポーネント*
- *機能*
- *製品を登録する*
- *アプリケーションの管理*
- *専門用語*

ポリシー マネージャを使用することで、次のことが可能になります。

- セキュリティ ポリシーの定義
- セキュリティ ポリシーの配布
- アプリケーションのインストール (ローカルおよびリモートのシステムに対して)
- ホストの監視と管理 (ポリシーを順守しているかなどの確認)

システムが設定された後、管理ドメイン全体のステータス情報が1つのウィンドウで表示します。これによって、ドメイン全体の保護状況を一目で確認でき、必要に応じて保護設定を簡単に変更することができます。また、エンドユーザ (ホストのユーザ) によるセキュリティ設定の変更を拒否することも可能で、保護が常に更新されていることを確認できます。

システム要件

ここでは、ポリシー マネージャ サーバおよびポリシー マネージャ コンソールのシステム要件について説明します。

ポリシー マネージャ サーバ

ポリシー マネージャ サーバをインストールするには、システムが少なくとも次の要件を満たしている必要があります。

オペレーティング システム:	Microsoft Windows: • Microsoft Windows Server 2003 SP1 以降 (32ビット)、Standard/Enterprise/Web/Small Business Server • Windows Server 2003 SP1以降 (64 ビット)、Standard/Enterprise • Windows Server 2008 SP1 (32ビット)、Standard/Enterprise/Web Server • Windows Server 2008 SP1 (64ビット)、Standard/Enterprise/Web Server/Small Business Server/Essential Business Server • Windows Server 2008 R2、Standard/Enterprise/Web Server
プロセッサ:	P4 2 GHz 以上のプロセッサ 5000台を超えるホストの管理、または Web レポートの使用には P4 3 GHz 以上のプロセッサが必要。
メモリ:	512 MB (1 GB 推奨) 5000台を超えるホストの管理、または Web レポートの使用には 1 GB 以上のメモリが必要。
ディスク容量:	5 GB の空き容量 (8 GB 以上推奨)。ディスク容量は使用により異なります。 また、警告とポリシーの処理用に、各ホストに 1 MB の容量を割り当てることを推奨します。ホストで必要なディスク容量はポリシーの使用法やインストールしたパッケージの数によって異なります。
ネットワーク:	10 Mbit ネットワーク。 5000台を超えるホストの管理には 100 Mbit ネットワークが必要。

ポリシー マネージャ コンソール

ポリシー マネージャ コンソールをインストールするには、システムが少なくとも次の要件を満たしている必要があります。

オペレーティング システム:	Microsoft Windows : • Windows XP Professional (SP2以降) • Windows Vista (32または64ビット)、Business/Enterprise/Ultimate • Windows 7 (32または64ビット)、Professional/Enterprise/Ultimate • Microsoft Windows Server 2003 SP1以降 (32ビット)、Standard/Enterprise/Web/Small Business Server • Windows Server 2003 SP1以降 (64 ビット)、Standard/Enterprise • Windows Server 2008 SP1 (32ビット)、Standard/Enterprise/Web Server • Windows Server 2008 SP1 (64ビット)、Standard/Enterprise/Web Server/Small Business Server/Essential Business Server • Windows Server 2008 R2、Standard/Enterprise/Web Server
プロセッサ:	P4 2 GHz 以上のプロセッサ 5000台を超えるホストの管理には P4 3 GHz 以上のプロセッサが必要。
メモリ:	512 MB 5000台以上のホストの管理には 1 GB 以上のメモリが必要。
ディスク容量:	200 MB の空き容量
ディスプレイ:	解像度1024x768で16色以上を表示できるディスプレイ (解像度1280x1024以上で32ビット色を推奨)。
ネットワーク:	10 Mbit ネットワーク。 5000台を超えるホストの管理には 100 Mbit ネットワークが必要。

主要コンポーネント

ポリシー マネージャはF-Secureの管理アーキテクチャ (技術) を採用しており、広域に分散されているシステムに強力なスケーラビリティ (拡張性) を提供します。

ポリシー マネージャ コンソール

ポリシー マネージャ コンソールは、ホストのセキュリティを管理するためのコンソール (操作画面) です。この画面から、管理者はネットワークを自由に編成してポリシーを共有することができます。ポリシーは、ポリシー マネージャ コンソールで定義され、ポリシー マネージャ サーバを通じてホストへ配布されます。ポリシー マネージャ コンソールは複数のプラットフォームに対応にしている *Java* ベースのアプリケーションです。コンソールを使用して、リモートからエンドユーザの介入なしで管理エージェント製品を他のワークステーションにインストールすることもできます。

ポリシー マネージャ コンソールには2つのユーザ インターフェースがあります。

- アンチウイルス モード - クライアント セキュリティとアンチウイルス ワークステーションを管理するために最適化なインターフェースです。
- 詳細モード - 他のF-Secure製品を管理するためのインターフェース。

ポリシー マネージャ サーバ

ポリシー マネージャ サーバ は管理者が配布するポリシーやソフトウェアのパッケージ、およびホストが送信するステータス情報や警告のリポジトリ (保存場所) としても機能します。ポリシー マネージャ サーバとホスト間の通信は、標準の *HTTP* プロトコルを介して行われるため、*LAN* および *WAN* 上でのパフォーマンスには影響しません。

管理エージェント

管理エージェントは、管理者が設定したセキュリティ ポリシーをホストに実施し、エンドユーザにユーザ インターフェースおよびその他のサービスを提供します。また、各ホストの管理機能を処理し、すべてのF-Secureアプリケーションに対して共通のインターフェースを提供し、ポリシーベースの管理システムで動作するようにします。

Web レポート

Web レポートは、ポリシー マネージャ サーバに付属する Web ベースの視覚的レポート システムです。 Web レポートを使用して、過去のデータに基づいた視覚的なレポートをすばやく作成できます。レポートから、ウイルスから保護されていないコンピュータや被害を受けやすいコンピュータを識別することができます。

更新サーバ/エージェント

更新サーバ/エージェントは、ホストのパターン ファイルとスパイウェア定義ファイルを更新します。自動更新エージェントを使用すると、ユーザは作業を中断することなく、パターンファイルの更新や情報コンテンツを受信することができます。 エージェントは、システムが使用していない帯域幅を使ってファイルを透過的かつ自動的にダウンロードします。自動更新エージェントがインターネットに常時接続されている場合、新しいパターン ファイルは、F-Secureが発行してからおよそ2時間以内に自動的に受け取ることができます。

機能

ここでは、ポリシー マネージャの主な機能について説明します。

ソフトウェアの配布

- 各ホストに対して、F-Secure製品のインストール、および実行可能ファイルとデータ ファイルの更新 (パターン ファイルの更新も含む)。
- 更新は、複数の方法で実行できます。
  - F-Secure CD を利用して。
  - F-SecureのWebサイトを利用して。更新やアップデートは、自動更新エージェントを通じて送信できます。または、F-SecureのWebサイトから直接入手することも可能です。
- ポリシー マネージャ コンソールを使用して、設定済みのインストール パッケージをエクスポートできます。インストール パッケージは、SMS などのサードパーティ製プログラムや同様のツールを使用してエクスポートすることも可能です。

設定とポリシー管理

- セキュリティ ポリシーの集中化。ポリシー マネージャ サーバが各ホストにポリシーを配布します。ポリシーの保全性は、電子署名によって保証されます。

イベント管理

- イベント ビューワ (ローカルおよびリモート ログ)、メール、およびレポート ファイルに対するレポート機能とイベント統計の作成

パフォーマンス管理

- 統計情報とパフォーマンス データの処理およびレポート

タスク管理

- スキャン タスクと他の操作の管理

製品を登録する

製品を登録すると、ポリシー マネージャの使用に関する情報をF-Secureに提供することができます。

ポリシー マネージャ製品の登録に関して、Q&A 形式で説明します。F-Secureのライセンス条項 (*http://www.f-secure.com/en_EMEA/estore/license-terms/*) とプライバシー に関する方針 (*http://www.f-secure.com/en_EMEA/privacy.html*) をご覧になることも推奨します。

F-Secureはなぜデータを集めますか?

エフセキュアは、サービスを常に改善するためにF-Secureの製品の使用に関する統計データを収集しています。データはお客様を特定できない形で収集されますが、お客様の製品と関連付けるオプションもあります。このオプションを有効にしたら、製品とデータがより簡単に検証できるようになるため、F-Secureのサービスとサポートが向上します。オプションを有効にする場合、ライセンス証明書に記載されている顧客 ID をポリシー マネージャのインストール中に入力してください。

どのような情報が送信されますか?

収集するデータは個人を特定できないように匿名で保存されます。データには、F-Secureのバージョン、オペレーティング システムのバージョン、ホストの数、切断されているホストの数が含まれ、これらはセキュリティのため、暗号化した形で転送されます。

F-Secureに情報の送信を許可するメリットは?

エフセキュアのサポートにお問い合わせする際に、データを照合できるため、問題の解決と対応が速くなります。また、収集したデータをフィードバックとして扱うことで、今後の製品のアップデートやアップグレードの改善に役立ちます。

情報はどこで保存されますか? また、だれがアクセスできますか?

データは、堅牢なセキュリティで保護されているF-Secureのデータ センターで保存され、アクセスは一部のF-Secureスタッフに制限されます。

アプリケーションの管理

ポリシー マネージャはネットワークのアプリケーションを管理するためにさまざまなコンポーネントを使用します。

管理エージェント

「管理エージェント」は、管理者が設定したセキュリティ ポリシーを管理対象の各ホストに適用します。管理エージェントは、ホストの管理設定コンポーネントとして動作し、ポリシー ファイルの解釈、ポリシー マネージャへの自動登録依頼とホスト ステータス情報の送信、およびポリシーベースのインストールを処理します。

Cisco Network Admission Control (NAC) サポート

F-Secure Corporation は Cisco Systems, Inc. が主導する *Network AdmissionControl* (*NAC*) のパートナー プログラムに参加しています。 Cisco NACは、パターン ファイルが更新されていない場合や、アンチウイルスまたはファイアウォールなどのモジュールが無効にされている場合に、ホストのネットワーク アクセスを制限することができる機能です。

専門用語

ここでは、本書で使われている用語について説明します。

ホスト

ポリシー マネージャで集中管理されるコンピュータのことを意味します。

ポリシー

機密情報などのリソースの管理、保護、および配布方法を明確に定めた一連のルールです。 F-Secureの管理アーキテクチャは、最適なセキュリティ管理を実現するために集中設定したポリシーを使用します。

ポリシー マネージャ コンソールとホスト間の通信は、ポリシー ファイルを転送することによって行われます。

ポリシー ドメイン

ポリシードメインとは、類似のセキュリティ ポリシーが設定されているホストまたはサブドメインのグループです。

ポリシーの継承

ポリシーを継承することによって、共通のポリシーを簡単に定義することができます。 ポリシー マネージャ コンソールでは、各ポリシー ドメインが親ドメインの設定を自動的に継承します。これによって、大規模なネットワークの管理が容易に効率よくできるようになります。 継承された設定は、ホストやドメイン単位で上書きできます。 ドメインに継承された設定が変更された場合、変更内容はドメインの全ホストおよびサブドメインに適用されます。

サブドメイン、または個々のホストについて、ポリシーをさらに細かく定義することもできます。 ポリシー定義をどこまで詳細に設定するかは、システムによって異なります。 大規模なドメインに少数の異なるポリシーを定義することもできれば、 個々のホストに直接ポリシーを適用して、非常に細かい管理を実現することも可能です。

第
2
章

アンインストール

トピック：

- *インストール手順*
- *Web ブラウザのパスを変更する*
- *アンインストール*

製品の主要コンポーネント (ポリシー マネージャ サーバとポリシー マネージャ コンソール) をインストール方法を説明します。

インストール手順

ここでは、ポリシー マネージャ サーバとポリシー マネージャ コンソールを同じマシンにインストールする方法について説明します。

インストール パッケージのダウンロードと実行

ポリシー マネージャ をインストールするには、インストール パッケージがまず必要になります。

インストールを開始するには

1. インストール パッケージをダウンロードするために *www.f-secure.com/webclub* にアクセスします。
   ポリシー マネージャのパッケージをダウンロードします。
2. ダウンロードしたファイルを実行します。
   セットアップが開始します。
3. インストールで使用する言語を選択して [次へ] をクリックします。
4. 使用許諾契約を確認します。同意する場合、[同意する] を選択します。 [次へ] をクリックします。

インストールするコンポーネントを選択する

次に、インストールするコンポーネントを選択します。

コンポーネントを設定するには

1. インストールするコンポーネントを選択し、[次へ] をクリックします。
   - ポリシー マネージャ サーバとポリシー マネージャ コンソールを両方選択したら、同じマシンに両コンポーネントをインストールします。
   - ポリシー マネージャ サーバを選択したら、ポリシー マネージャ コンソール を別のマシンにインストールします。
2. インストール先のフォルダを指定して、[次へ] をクリックします。
   デフォルトのフォルダを使用することを推奨します。別のフォルダにインストールする場合、[参照] をクリックしてフォルダを選択します。

   注: 管理エージェントを同じマシンにインストールしている場合、このウィンドウは表示されません。

3. 顧客 ID を入力して [次へ] をクリックします。
   顧客 ID は製品のライセンス証明書に記載されています。
4. ポリシー マネージャの旧バージョンがインストールされているかを確認するメッセージが表示されます。:
   - 旧バージョンがインストールされている場合、[**F-Secure**ポリシーマネージャをインストールしてあります] を選択します。次に、インストールされているポリシーマネージャの通信ディレクトリのパスを指定します。このフォルダの内容は、`<サーバのインストール先フォルダ>\commdir\` (ポリシー マネージャ サーバのインストール先フォルダにある commdir フォルダ) 以下にコピーされ、ポリシー マネージャ サーバはこのフォルダをリポジトリ (データの保存) として使用します。以前の `commdir` はバックアップとして使用できます。また、ポリシー マネージャ サーバが正しくインストールされたことを確認した時点で commdir を削除することもできます。

- 旧バージョンがインストールされていない場合、[**F-Secure**ポリシーマネージャを所有していません] を選択します。

5. [次へ] をクリックします。
6. 既存の設定を使用するか、設定を変更するかを選択します。

   注: このダイアログは、コンピュータにポリシー マネージャ サーバの旧バージョンが検出された場合にのみ表示されます。

   - デフォルトでは、セットアップは既存の設定を使用します。ポリシー マネージャ サーバの構成ファイル (HTTPD.conf) を手動で更新している場合、このオプションを選択してください。オプションを選択したら、各機能 (管理、ホスト、および Web レポート) で設定されているポートも自動的に適用されます。
   - 旧バージョンに設定したポートを変更する場合、[設定を変更する] を選択します。このオプションは HTTPD.conf ファイルを上書きし、設定をデフォルトに戻します。

7. [次へ] をクリックします。
8. ポリシー マネージャ サーバの各モジュールを設定します。

   - ホスト モジュールは、ホストとの通信に使用されます。デフォルトのポートは80です。
   - 管理モジュールは、ポリシー マネージャ コンソールとの通信に使用されます。デフォルトの HTTP ポートは8080です。

     注: 通信用のデフォルトのポートを変更する場合、ポリシー マネージャ コンソールで **HTTP** ポート番号の設定を変更する必要があります。

     デフォルトでは、管理モジュールのアクセスはローカルのコンピュータに制限されています。ネットワーク上の接続を使用する場合、セキュリティ対策としてF-Secureを利用して通信を保護することを検討してください。
   - **Web** レポート モジュールは、Web レポートとの通信に使用されます。この機能は管理モジュールに対してローカルソケット接続を使用し、サーバからデータを入手します。デフォルトのポートは8081です。

     デフォルトでは、Web レポートのアクセスは他のコンピュータからも可能です。[アクセスをローカルマシンに制限する] を選択すると、アクセスをローカルのコンピュータに限定できます。

9. [次へ] をクリックします。
10. インストールするパッケージを選択して、[次へ] をクリックします。

インストールを完了する

次に、インストールを完了させます。

1. 内容を確認し、[開始] をすると選択したコンポーネントがインストールされます。
   画面上にコンポーネントがインストールされたか表示されます。
2. [完了] をクリックしてセットアップ ウィザードを終了します。
3. 必要な場合、コンピュータを再起動します。

ポリシー マネージャ コンソールを起動する

ポリシー マネージャ コンソールをはじめて起動します。

ポリシー マネージャ コンソールを起動するには

1. スタート ➤ プログラム ➤ **F-Secure** ポリシー マネージャ ➤ **F-Secure** ポリシー マネージャ コンソール の順に選択します。

   ポリシー マネージャ コンソールをはじめて起動するときには、コンソール セットアップ ウィザードがサーバへの初期接続を作成するために必要な情報を収集します。

2. [次へ] をクリックします。
3. 必要に応じて、ユーザ モードを選択します。

   - 管理者モード - 管理者の機能をすべて有効にします。
   - 読み取り専用モード - 管理データを表示できますが、管理タスクは実行できません。読み取り専用モードを選択したら、ホストを管理できないようになります。管理者モードを選択した場合、`admin.pub` と `admin.prv` の管理鍵が必要なります。

4. [次へ] をクリックします。
5. 管理ホストとの通信に使用するポリシーマネージャ サーバのアドレスを指定し、[次へ]をクリックします。
6. 管理者の公開鍵ファイルと秘密鍵ファイルを格納するパスを入力します。

   デフォルトでは、鍵ファイルはポリシー マネージャ コンソールのインストール フォルダ (「`Program Files\F-Secure\Administrator`」) に格納されます。

7. [次へ] をクリックします。

   注: 鍵ペアが作成されていない場合、セットアップの後半で鍵ペアが作成されます。

8. マウスのカーソルをウィンドウ内で動かして、管理用鍵ペア ジェネレータで使用する乱数シードを初期化します。

   マウスを移動したときの曲線を使用することにより、鍵ペア生成アルゴリズムのシード値が十分な乱数を得ることができます。

   進行状況を示すインジケータが100%になると、「パスワード」ダイアログ ボックスが自動的に開きます。

9. 管理用秘密鍵を保護するパスワードを指定します。
10. [パスワードの確認] フィールドにパスワードを再入力して [次へ] をクリックします。
11. □完了] をクリックして、セットアップを完了します。
    ポリシーマネージャ コンソールが管理用の鍵ペアを生成します。鍵ペアの生成後、ポリシーマネージャ コンソールが起動します。

    セットアップが「`FSPM users`」のユーザ グループを作成します。インストールを実行したユーザは自動的にこのグループに追加されます。「`FSPM users`」のユーザ グループに追加したユーザはポリシーマネージャを起動できるようになります。

ポリシー マネージャ コンソールがアンチウイルスモードで起動します。アンチウイルス モードは(クライアント セキュリティ、アンチウイルス ワークステーション、およびアンチウイルス Windows サーバの管理に最適なインターフェースです。ポリシーマネージャ コンソールを他のF-Secure製品の管理に使用する場合、詳細モードのインターフェースを使用してください。詳細モードは[ビュー] メニューの [詳細モード] から選択できます。

管理対象のホストには、`admin.pub` キーのコピー (またはキーへのアクセス権) を提供する必要があります。ポリシーマネージャを使用してF-Secure製品をリモートからインストールした場合、`admin.pub` キーのコピーは自動でインストールされています。ただし、インストールを CD から実行した場合、`admin.pub`

キーのコピーを手動で転送する必要があります。これは、外部メディアを利用して行うと安全です。また、`admin.pub` をホストがアクセスできる共有フォルダに置く方法もあります。

Web ブラウザのパスを変更する

ポリシー マネージャ コンソールは、セットアップ中にデフォルトの Web ブラウザのファイル パスを取得します。

Web ブラウザのパスを変更するには

1. メニューからツール ➤ 一般設定 を選択します。
2. 「場所」タブを選択して、新しいファイル パスを入力します。

アンインストール

次の方法でポリシー マネージャのコンポーネントをアンインストールできます。

ポリシー マネージャのコンポーネントをアンインストールするには

1. Windows の [スタート] メニューから [コントロール パネル] を選択します。
2. [プログラムの追加と削除] を選択します。
3. アンインストールするコンポーネント (ポリシー マネージャ コンソールまたはポリシー マネージャ サーバ) を選択して、[追加と削除] ボタンをクリックします。
   アンインストールに関するダイアログ ボックスが表示されます。
4. [開始] をクリックしてアンインストールを開始させます。
5. アンインストールが完了したら、[閉じる] をクリックします。
6. 他のコンポーネントをアンインストールする場合、必要に応じて上記の手順を繰り返します。
7. コンポーネントをすべてアンインストールしたら、「プログラムの追加と削除」ウィンドウを閉じます。
8. コンピュータを再起動します。

   再起動は、アンインストール後のコンピュータに残ったファイルを消去するために必要です。

第
3
章

アンチウイルス モード

トピック：

- *「ポリシー ドメイン」タブ*
- *管理タブ*
- *ツールバー*
- *メニュー コマンド*
- *設定を継承する*

また、アンチウイルス モード全体に使用される共通の機能および画面のコマンドについても説明します。

注: ポリシー マネージャには、もう1つのユーザ インターフェース (詳細モード) があります。「詳細モード」は、クライアント セキュリティおよびアンチウイルス ワークステーション以外の製品の管理に適切です。また、クライアント セキュリティの詳細設定を変更する必要がある場合にも使用されます。[表示] メニューから詳細モードまたはアンチウイルス モードを選択することにより、モードを切り替えることができます。

のアンチウイルス モードは次のように構成されています。

- 「ポリシー ドメイン」タブ - ポリシー ドメインの構造が表示されます。
- 管理タブ: 「概要」、「設定」、「ステータス」、「警告」、「レポート」、「インストール」、および「操作」の各タブでホストにインストールされたクライアント セキュリティの設定と監視、および操作の実行を行うことができます。
- 「メッセージ」ウィンドウ - ポリシー マネージャからのメッセージ (サーバ上のパターン ファイルが更新された時間など) が画面の下に表示されます。

「ポリシー ドメイン」タブ

「ポリシー ドメイン」タブでは、ポリシー ドメインとホストに対して特定の処理を行うことができます。

「ポリシー ドメイン」タブでは、以下の操作を実行できます。

- 新しいポリシー ドメインの追加 (ツールバーにある アイコンをクリック)。新規ポリシー ドメインは、親ドメインを選択している場合にのみ作成できます。
- 新しいホストの追加 (アイコンをクリック)。
- ホストの検索。
- ドメインまたはホストのプロパティ (設定) の表示。ホスト/ドメインには分かりやすい名前を付けると管理がしやすくなります。
- 自動登録したホストのインポート。
- Windows ドメインからのホストの自動検出。
- ホストまたはドメインの削除。
- カット& ペーストを使用したホスト/ドメインの移動。
- ポリシー ファイルのエクスポート。

上記のオプションにアクセスするには、ドメインまたはホストを指定して、[編集] メニューを選択するか、右クリックします。 また、[自動登録] および [自動登録したホストのインポート] の操作は、「インストール」タブからでも実行できます。

注: ここでの「ドメイン」は Windows NT または DNS のドメインのことではありません。「ポリシー ドメイン」とは、類似のセキュリティ ポリシーが設定されているホストまたはサブドメインのグループのことを指します。

管理タブ

ここでは、「概要」、「設定」、「ステータス」、「警告」、「レポート」、「インストール」、および「操作」の各タブを説明します。

「概要」タブ

「概要」タブは、選択したドメイン/ホストに関する最も重要な情報を一目で参照できるように設計されています。

ドメインを選択している場合、「概要」タブはドメイン全体に関する情報を表示します。 ホストを選択している場合、ホストに関する詳細情報が表示されます。

「概要」タブに表示されている設定の中にすぐに対処や処理が必要なものがある場合、設定の横にアイコンが表示されます。

	処理を必要とするエラー状況を示す警告。このエラーは自動的に修復されません。たとえば、最新のポリシーが配布されていない場合や、ホスト上のパターン ファイルが期限切れの場合に、このアイコンが表示されます。
	処理を必要とする可能性のある状況を示す警告。セキュリティ上の問題はまだ発生していませんが、すぐに問題を修復しておかないと後で問題が発生するおそれがあります。 たとえば、切断されたホストがある場合、このアイコンが表示されます。

「概要」タブに表示される情報は、「ポリシー ドメイン」タブで選択した項目によって異なります。

- ドメインを選択している場合、「概要」タブでは「ポリシー マネージャ」、「ドメイン」、「ワークステーションのウイルス保護」、および「インターネット防御」に関する情報が表示されます。
- ホストを選択している場合、「ポリシー マネージャ」、「ホスト」、「ウイルス保護」、および「インターネット防御」に関する情報が表示されます。

「概要」タブ (ドメイン選択時)

「ポリシー ドメイン」タブでドメインを選択すると、「概要」タブに以下の情報が表示されます。

ポリシーマネージャ

「ポリシー マネージャ」ページでは、以下の操作を実行できます。

- 現在のポリシー配布ステータス (保存/未保存、配布/未配布) を確認して、必要に応じてポリシー データを保存し、新しいポリシーをホストに配布する。
- サーバ上のパターンファイルのステータスを確認する。
- サーバ上のスパイウェア定義ファイルのステータスを確認する。
- サーバ上のディープガードの更新ステータスを確認する。
- 新しいホストがある場合、[これらのホストをドメインに追加] をクリックして、ホストをドメインに追加できます。
- [**Windows** ホストを自動検出] をクリックして、Windows ドメインからホストを自動検出する。

ドメイン

「ドメイン」ページでは、以下の操作を実行できます。

- 最新のポリシーが配布されているホストの数を表示する。[ホストの最新のポリシー更新を表示する] をクリックして、最新のポリシー更新の概要にアクセスできます。これによって、「集中管理」ページの「ステータス」タブが表示されます。
- 切断されたホストの数を表示する。[切断されたホストを表示] をクリックして、ホストの接続ステータスを表示する詳細リストにアクセスすることもできます。この操作を実行すると、「ステータス」タブの「集中管理」ウィンドウが表示されます。
- 新しい警告の概要を確認する。警告に関する詳細な情報が必要な場合は、[重大度別に警告を表示] リンクをクリックして 「警告」タブにアクセスできます。

  警告の重大度は、以下のアイコンで示されます。

アイコン	参考	説明
	情報	ホストからの通常の操作情報。
	警告	ホストからの警告。
	エラー	ホスト上の回復可能なエラー。
	重大なエラー	ホスト上の回復不能なエラー。
	セキュリティ警告	ホスト上のセキュリティ危険要因

ウイルス保護

「ワークステーションのウイルス保護」では、以下の操作を実行できます。

- ウイルス保護がインストールされているホストの数を確認する。
- リアルタイム スキャンを有効にしているホストの数を確認する。 ホストでリアルタイム スキャンが有効になっているか確認するには、[ステータス一覧を表示する] をクリックして、「ステータス」タブの「全体の保護」ページに表示される詳細情報にアクセスします。
- ドメインで検出された感染の数を確認する。 ホスト固有の感染情報を表示するには、[ホストの感染状況を表示する] をクリックして、「ステータス」タブの「全体の保護」ページにアクセスします。
- 最新のパターンファイルがインストールされているホストの数、および一部のホスト上のパターンファイルが最近のものか、それとも失効済みかを確認する。
  - [最近] は、パターン ファイルが最新ではないことを意味します。
  - [失効済み] は、設定された期限よりもパターン ファイルが古くなっていることを意味します。

    注: ホストにF-Secureアンチウイルス 5.40 をインストールしている場合、ホスト上のパターンファイルは「不明」と表示されます。

  複数のホストでパターン ファイルを更新する必要がある場合は、[パターン ファイルの更新]をクリックして「操作」タブを表示します。

インターネット防御

「インターネット防御」ページでは、以下の操作を実行できます。

- インターネット防御がインストールされているホストの数を確認する。

- 最も頻度の高い最新の攻撃と、ドメインが影響を受ける確率を確認する。 最新の攻撃に関する詳細情報を入手するには、[インターネット防御のステータスを表示する] をクリックして、「ステータス」タブの「インターネット防御」ページにアクセスします。

「概要」タブ (ホスト選択時)

「ポリシー ドメイン」タブでホストを選択すると、「概要」タブの「ホスト」ページに詳細情報が表示されます。

ホスト

「ホスト」では、以下の操作を実行できます。

- [コンピュータ **ID**] の横に表示される選択したホストの名前を確認する。[ホストのプロパティを表示する]をクリックすると、ホストの詳細情報にアクセスすることもできます。この操作を実行すると、「ステータス」タブの「ホストのプロパティ」ページが表示されます。
- アクティブなプロトコル (「HTTP」または「ファイル共有」)、ポリシー マネージャ サーバのアドレス、および前回の接続の日付と時刻を確認する。
- ホストが使用しているポリシー ファイルが最新か確認する。
- ホストが切断されているかどうかを確認する。
- 警告に関する詳細情報が必要な場合、[重大度別に警告を表示] をクリックして「警告」タブにアクセスします。

ホストの状況 --ウイルス保護

ドメイン選択時の情報に加え、「ワークステーションのウイルス保護」ページではパターン ファイルのバージョン番号も表示されます。

インターネット防御

ドメイン選択時の情報に加え、「インターネット防御」ページでは、ホストで使用中のセキュリティ レベルも表示されます。

「設定」タブ

「設定」タブでは、クライアント セキュリティのコンポーネントを設定できます。

「設定」タブのポップアップ メニュー

「設定」タブにある設定を右クリックすると、以下のオプションを含むポップアップ メニューが表示されます。

初期値に戻す	選択されている設定を初期値に戻します。
強制的に値を適用	このオプションはポリシー ドメインが選択されている場合にのみ使用でき、ドメインの設定をすべてのサブドメインとホストに適用します。サブドメイン/ホストで定義された値はすべて破棄され、復元することはできませんので、このオプションを使用するときには注意が必要です。
ドメインの値を表示	このオプションはポリシー ドメインが選択されている場合にのみ使用でき、ポリシー ドメインのサブドメイン/ホストのリストと選択したフィールドの値を表示します。ドメイン名またはホスト名をクリック

	すると、「ポリシー ドメイン」タブのドメイン/ホストを素早く選択できます。 複数の「ドメインの値」ウィンドウを同時に開くことも可能です。
詳細モードで検索	詳細モードのユーザ インターフェースが開き、設定を選択できます。

自動更新

「自動更新」ページは、「自動更新」と「ネイバーキャスト」の二つの部分に分かれています。

自動更新

「自動更新」ページでは、以下の操作を実行できます。

- 自動更新を有効/ 無効にする。この設定を無効にすると、ホストは自動で更新を取得できないようになります。
- ポリシー マネージャ サーバからの更新ポーリング間隔を指定する。
- ポリシー マネージャ プロキシサーバのリストを確認する。 リストに新しいサーバを追加したり、サーバを削除したり、アドレスと優先度を変更したりすることもできます。
- HTTP プロキシおよび HTTP プロキシ アドレスを指定する。
- サーバとプロキシに加え、ホストが他のホストから更新をダウンロードできるか選択する

ネイバーキャスト

ネイバーキャストは、サーバとプロキシに加え、ホストが他のホストから更新をダウンロードできることを許可します。ここでは、以下の操作を実行できます。

- 更新を提供するクライアント (ホスト) を指定する
- 更新をダウンロードするクライアント (ホスト) を指定する
- 使用するポートを選択する。

リアルタイム スキャン

ここで説明する設定は、ホスト上で行うリアルタイム スキャンを影響します。

以下の設定は、特に明記されていない限り、クライアント セキュリティの全バージョンに適用します。クライアント セキュリティ 9 以降およびアンチウイルス Windows サーバ 9 以降で未対応となった設定については、[旧バージョン **(7.x、8.x)** の設定] をクリックしてください。

共通設定

リアルタイム スキャンを有効/無効にできます。

ファイルのスキャン

以下の操作を実行できます。

- スキャンするファイルを選択して、スキャン対象の拡張子を定義する
- 特定の拡張子をスキャンから除外する
- ユーザがオブジェクトをリアルタイム スキャンの対象外にできるか選択する
- ネットワーク ドライブをリアルタイム スキャンの対象にする
- 感染ファイルの検出時を自動的に処理する (クライアント セキュリティ 9 以降およびアンチウイルス Windows サーバ 9 以降の対応)

- Hosts ファイルの保護を有効/無効にする
- 追跡 Cookie をスキャンに含む

ディープガード

以下の操作を実行できます。

- ディープガードを有効にする
- システムの変更試行が検出されたときの処理を選択する
- 検出の精度を向上するために、リモート サーバにクエリを送る
- 高度なモニタリングを有効/無効にする

マニュアル スキャン

ここで説明する設定は、エンドユーザ (ホストのユーザ) によって実行されるマニュアル スキャンを影響します。

ファイルのマニュアル スキャン

以下のオプションを使用してスキャンの対象を選択できます。

- スキャンするファイルを選択して、スキャン対象の拡張子を定義する
  - すべてのファイル: ファイル拡張子に関係なく、すべてのファイルをスキャンします。これを選択するとシステムのパフォーマンスがかなり低下するため、日常的に使用するオプションとしてはお勧めできません。
  - 次の拡張子のファイル: 指定した拡張子のファイルをスキャンします。拡張子が付いていないファイルを指定するには、ピリオド「.」を入力します。ワイルドカード「?」を使用して、任意の文字を表すこともできます。それぞれのファイル拡張子を、スペースで区切って入力します。
- 圧縮ファイルの内部をスキャンするか指定します。チェックボックスをオンにすると、圧縮ファイルの内部をスキャンします (ZIP、ARJ、LZH、RAR、CAB、TAR、BZ2、GZ、JAR、TGZ などの形式)。圧縮ファイルの内部スキャンは大量のシステム リソースを使用し、システムのパフォーマンスを影響します。
- 一部のファイルをスキャンから除外するか指定します。[対象外の拡張子] フィールドにスキャンから除外するファイルの拡張子を指定できます。
- ユーザがリアルタイム スキャンからオブジェクトを除外できるか指定します。[対象外のオブジェクトを有効にする] を選択したら、ユーザはスキャンの対象外となるファイルまたはフォルダを指定できます。
- [感染時の処理] ドロップダウン リストから感染したファイルが検出されたときにクライアント セキュリティが実行する処理を選択できます。

処理	説明
スキャン後に問い合わせる	感染ファイルを検出すると、駆除ウィザードを起動します。
自動的に駆除	感染ファイルを検出すると、ファイルを自動的に駆除します。
自動的に名前を変更	感染ファイルを検出すると、ファイルの名前を自動的に変更します。

処理	説明
自動的に削除	感染ファイルを検出すると、ファイルを自動的に削除します。このオプションを使用すると、ウイルスが添付されているオブジェクトも一緒に削除されますので、このオプションは推奨しません。
レポートのみ	ウイルス検出を通知し、感染したオブジェクトを開けないようにします。ウイルスに対して処理は行われません。

ルートキット スキャン

以下の操作を実行できます。

- ルートキット スキャンを有効/無効にする
- システムの完全チェック.にルートキットスキャンを含む、または含まない
- 検出された不審なアイテムを駆除ウィザードと完全チェック後のスキャンレポートで表示するかしないかを指定する

スケジュール スキャン

[詳細モードに移り、スケジュール スキャンを設定する] をクリックすると、詳細モードを開き、スケジュール スキャンを設定できます。

ブートセクタのマニュアル スキャン

以下の操作を実行できます。

- フロッピー ディスクのブートセクタに対するマニュアル スキャンを有効/無効にする
- 感染の検出時に実行する処理を選択する

スパイウェア制御

ここで説明する設定は、リアルタイム/マニュアル スキャンのスパイウェア検出と機能に該当します。

スパイウェア スキャンから除外されるアプリケーション

テーブルには、管理者により実行が許可されたスパイウェアとリスクウェアが表示されます。

ホストから報告されているスパイウェアとリスクウェア

ホストが報告したスパイウェアとリスクウェア、およびホストで隔離保存されているスパイウェアとリスクウェアが表示されます。また、各スパイウェアおよびリスクウェア アプリケーションのタイプと重大度も表示されます。[アクティブである可能性] のステータスが指定されているスパイウェアとリスクウェアは管理者の許可を得て、ホストでの実行が許可されています。

[スパイウェア アイテムの定義をユーザに許可する] ドロップダウン リストを選択すると、スパイウェア/リスクウェアの使用をエンドユーザが決定できるようになります。

隔離保存ファイルの管理

このページでは、ホストが隔離保存したマルウェアを管理できます。

隔離コンテンツ

テーブルに、ホストが隔離保存したマルウェアの情報が表示されます。マルウェアのタイプ、名前、パス、ホスト、および対象のマルウェアを隔離保存したホストの数などを確認できます。

隔離保存されたオブジェクトに実行する処理

このテーブルには、処理された隔離保存アイテムの情報が表示されます。隔離保存されたアイテムに対する処理は「解除」または「削除」のいずれかになります。ここで指定されている処理はホストにも適用されます。つまり、テーブルにある特定のマルウェアがホストで検出された場合、テーブルで指定されている処理 (「解除」または「削除」) がホスト上で検出されたマルウェアに適用されます。処理が [解除] の場合、適切の除外ルールがマルウェアのタイプに応じて「スパイウェア制御」または「リアルタイム スキャン」ページで定義されている必要があります。これは、今後のスキャンでマルウェアが隔離保存されることを防ぐための設定です。

隔離保存されているマルウェアが処理され、同じマルウェアが他のホストで隔離保存されていない状態になると、隔離保存アイテムがテーブルから消去されます。

メール スキャン

このページでは、メール スキャンの設定を行うことができます。「共通設定」の設定は、着信および発信スキャンに提供します。

受信メール スキャン

以下の操作を実行できます。

- メール スキャンを有効/無効にする
- 受信した添付ファイルが感染している場合の処理を選択する
- スキャンが失敗した場合の処理を選択する
- 不正な形式のメッセージ部分の処理を選択する

送信メール スキャン

以下の操作を実行できます。

- メール スキャンを有効/無効にする
- 送信する添付ファイルが感染していた場合の処理を選択する
- スキャンが失敗した場合の処理を選択する
- 不正な形式のメッセージ部分の処理を選択する
- ブロックしたメールをエンドユーザの送信トレイに保存するように選択する

共通設定

以下の操作を実行できます。

- 圧縮された添付ファイルもスキャンするかどうかを選択する。
- スキャンの進行状況を表示するか選択して、進行状況を表示するまでの時間を定義する。
- 感染したメールが検出された場合や、スキャンが失敗した場合にスキャン レポートを表示するか選択する。

Web スキャン

ここでは、Web スキャン (Web ページからダウンロードするファイルに対するスキャンなど) の設定について説明します。

共通設定

Web スキャンを有効/無効に設定できます。

Web スキャン

- 感染しているファイルに実行する処理を選択します。
- スキャンに失敗した場合の処理を選択します。
- 圧縮ファイルをスキャンに含めるか選択します。

信頼済みの HTTP サイト

信頼済みと指定された HTTP サイトを表示します。信頼済みの HTTP サイトに関連する Web トラフィックはスキャンされません。

ファイアウォールのセキュリティ レベル

ここで説明する設定は、ホスト/ドメインのファイアウォール セキュリティ レベルを決定するために使用されます。

共通設定

以下の操作を実行できます。

- ホストに適用するプリセットのセキュリティ レベルを指定する。
- [詳細モードでセキュリティ レベルの自動選択を設定] をクリックして、セキュリティ レベルの自動選択を設定する。この操作を実行すると、ユーザ インターフェースが詳細モードに変わります。
- [ファイアウォール エンジンを有効にする] をオンにして、セキュリティ レベルのファイアウォールのルールを着信および発信パケットに適用できるようにする。
- 信頼済みのインターフェースの使用を有効にする。
- アプリケーション通信制御のポップアップを有効/無効にする。

ファイアウォールのセキュリティ レベル テーブル (グローバル)

このテーブルでは、システム全体で使用できるセキュリティ レベルが表示されます。「セキュリティ レベル」テーブルはすべてのポリシー ドメインに共通していますが、セキュリティ レベルはポリシー ドメイン別に有効または無効にできます。

ネットワークの隔離

以下の操作を実行できます。

- ネットワークの隔離を有効/無効にする
- ネットワーク隔離を有効にするために必要なパターン ファイルの経過日数を指定する
- ホストでリアルタイム スキャンが無効になった場合、ネットワーク隔離を有効にするか指定する

侵入防止

以下の操作を実行できます。

- 侵入防止を有効/無効にする
- 悪質なパケットが検出されたときのアクションを設定します。使用可能なオプションは、以下のとおりです。
  - ログおよび削除

  - ログのみ

- 集中管理された警告の重大度を定義する。
- 警告レベルおよびパフォーマンス レベルを定義する。

ファイアウォール ルール

このページでは、ファイアウォール セキュリティ レベルに適用するルールを定義できます。

ファイアウォール ルール テーブル

このテーブルには、さまざまなセキュリティ レベルに対して定義されているルールが表示されます。[編集するインターネット防御セキュリティ レベル] ドロップダウン メニューから、セキュリティ レベルを選択できます。セキュリティ レベルを変更すると、新しいセキュリティ レベルに関連付けられたルールがテーブルに表示されます。

ファイアウォールの使用中には、テーブルに表示された順番で上から下へと、ファイアウォールのルールが確認されます。フィルタリング モードが「標準」のセキュリティ レベルの場合、ドメイン固有またはホスト固有のルールを定義することができます。[新規ルールの定義をユーザに許可] を選択すると、エンドユーザは、そのセキュリティ レベルに対して新しいルールを定義することもできるようになります。また、テーブルにはこれらのルールの場所も表示されます。

「ファイアウォール ルール」テーブルでは、各ルールについて以下の情報が表示されます。

- ルールのステータス (有効または無効)
- ルールの名前およびコメント
- ルールのタイプ(許可/拒否)
- 関連サービスおよび方向: 着信サービスの場合は **<=**、発信サービスの場合は **=>**、双方向サービスの場合は **<=>**
- 影響を受けるリモートホスト
- 警告の転送を有効または無効にする
- ダイヤルアップ リンクの使用時にのみルールを適用するかどうか

[新しい場所を指定] をクリックすると、ルールをテーブル内の別の場所に移動できます。次に、[上へ移動] と [下へ移動] ボタンを使用して、ルールの新しい場所を指定します。

また、ホスト上のアプリケーション通信制御は、許可されているアプリケーションを基に、ルールを自動的に作成します。作成されたルールはテーブルの「残りを拒否」ルールの真上に配置されます。サービスが [すべてのトラフィック]、そしてリモートホストが [すべて] に設定されている場合、一番最初に適用される拒否ルールとなります。ルールは着信するパケットをサーバのアプリケーションに通し、ファイアウォールはサーバ アプリケーションの発信パケットを許可します。通常のアプリケーションから発信されるパケットは [ファイアウォール ルール] テーブルにあるルールで許可することが必要です。

ファイアウォール サービス

ここで言う「サービス」とは、ネットワーク上で利用可能なネットワーク サービスのことです (例: ファイル共有、リモート コントロール アクセス、Web 閲覧など)。 ほとんどの場合、使用するプロトコルとポートで定義されます。

ファイアウォール サービス テーブル (グローバル)

ファイアウォールのために定義されたルールが表示されます。また、ファイアウォールの新しいサービスを作成したり、エンドユーザに新しいサービスの作成を許可したりすることもできます。

[制限] をクリックして、[固定サイズ] をオンにすると、ユーザが新しいサービスを追加できないように設定することが可能です。このチェックボックスをオンにすると、エンドユーザはテーブルで列を追加および削除できなくなります。

アプリケーション通信制御

ここで説明する設定は、着信および発信のネットワーク接続を使用するアプリケーションを制御します。

既知のアプリケーションのルール

「アプリケーション通信制御」ページでは、既知のアプリケーションと接続の試行 (着信および発信) に対して定義されたルールのリストが表示されます。

ホストによってレポートされる不明なアプリケーション

ホストから報告され、ルールがまだ存在しないアプリケーションが表示されます。

このページでは次の操作も実行できます。

- クライアント アプリケーションに対するデフォルトの処理を選択する
- サーバ アプリケーションに対するデフォルトの処理を選択する
- [新しい不明なアプリケーションをレポート] チェックボックスをオンにして、新しいアプリケーションをユーザにレポートするか選択する

自動処理

ディープガードまたはディープガード ネットワークがアプリケーションを認識した場合、ユーザが処理を選択できるように設定できます。

ユーザに対するメッセージ

次のオプションを指定できます。

- 不明なアプリケーションに対して、ユーザにデフォルトのメッセージを表示するか指定する。
- [デフォルトのメッセージを定義] - クリックすると「デフォルトのメッセージ」ウィンドウが開き、既知および不明のアプリケーションに対するメッセージを、[許可]、[拒否]、および [ユーザが決定] に定義できます。

ブラウザ保護

ここで説明する設定は、クライアント セキュリティ 9 以降をインストールしているホストが利用できるブラウザ保護の設定を定義します。

脆弱性シールド

ブラウザ保護が脆弱性シールドを使用して、脆弱性のある Web サイトのアクセスをブロックするか指定する。

脆弱性シールドは、脆弱性を利用する悪質な Web サイトを認識し、そのような Web サイトのアクセスをブロックすることができます。この機能は、システムをマルウェアや感染しているファイルから保護できません。実際のマルウェア ファイルに対する保護は、ウイルスとスパイウェア スキャンが提供します。

評価に基づいた保護

ここの設定は、Web サイトに対する評価の表示方法、および「危険」として評価された Web サイトのアクセスをユーザにブロックするか指定します。 安全性の評価は、F-Secureのマルウェア分析やF-Secureのパートナー、およびエンドユーザからのフィードバックなどに基づいています。

信頼済みのサイト

ブラウザ保護がブロックしたページの中で、安全と判断でき、アクセスを可能にしたいものがあれば、それらを信頼済みのサイトとして指定できます。

詳細設定

[詳細設定を指定する] をクリックすると、詳細モードが開き、ブラウザ保護を設定できるページが表示されます。

警告の転送

ここで説明する設定は、警告の表示と転送設定を定義します。

共通設定

警告で使用する言語を選択します。

メールによる警告送信

- メール サーバのアドレス (SMTP) を指定する
- 警告をメールで転送するときに使用する送信者のメール アドレスおよびメールの件名を指定する

警告の送信

テーブルで、警告の転送先を重大度別に設定できます。

集中管理

このページでは、クライアント セキュリティのネットワーク設定について説明します。

共通設定

次のオプションを指定できます。

- すべての設定の変更をユーザに許可

  このオプションは、アンチウイルス モードおよび詳細モードの全設定を「未確定」の状態にします。つまり、ユーザはすべての設定を変更できるようになります。
- 設定の変更をユーザに許可しない...

  このオプションは、 アンチウイルス モードおよび詳細モードの全設定を「確定」の状態にします。つまり、エンドユーザはどの設定も変更できないようになります。
- すべての設定を初期値に戻す

  このオプションは、クライアント セキュリティの全コンポーネントをデフォルトの設定に戻します。
- すべてのダウンロードおよび更新の中断をユーザに許可

  このオプションは、ユーザがネットワーク通信 (ポリシーの自動ポーリング、統計の送信、自動更新など) を一時的に中止することができるか指定します。

  ダイヤルアップの回線など低速のネットワークから接続するホストを使用している場合に便利です。

- **F-Secure**製品のアンインストールをユーザに許可

  このオプションをオフにすると、エンドユーザはコンピュータからF-Secureソフトウェアをアンインストールできなくなります。アンインストールには必ず管理者権限が必要となります。これは、すべての Windows オペレーティング システム (エンドユーザが管理者権限を持つ Windows NT/2000/XP も含む) に適用されます。

  ローカルでソフトウェアをアンインストールするには、まず、このオプションをオンにするか、または管理エージェントを停止してから、アンインストールを続行する必要があります。

- 製品のアンロードをユーザに許可

  有効な値は、[常に許可する]、[スタンドアロン インストールにのみ許可]、[許可しない] です。

  このオプションは、ユーザがすべてのF-Secure製品を一時的にアンロードできるか指定します (ゲームまたは同様のアプリケーションにメモリを開放する場合など)。F-Secure の製品がアンロードされている間、各製品の主要な機能は無効になります。そのため、コンピュータはウイルスや攻撃に対して脆弱になります。

- 低速接続定義

  この変数は、低速接続であるとみなすネットワーク接続を定義します。使用される単位はキロビット/秒です。接続の公称速度ではなく、実際の速度が測定されます。デフォルトの値は0 (ゼロ) です。0を指定すると、すべての接続が高速であると見なされます。

ポリシー マネージャ サーバを設定する

- ポリシーマネージャサーバ

  ポリシー マネージャ サーバの URL アドレス。

- 受信パッケージのポーリング間隔

  ホストがポリシー マネージャ サーバから受信パッケージ (ベース ポリシー ファイルなど) を取り出す頻度を指定します。10 の場合は取り出しません。

- 送信パッケージの更新間隔

  ホストが、定期的に送信される情報 (統計情報など) の新しいバージョンをポリシー マネージャ サーバへ送信する頻度を指定します。デフォルト値は、10分です。

「ステータス」タブ

「ステータス」タブでは、集中管理されているクライアント セキュリティアプリケーションのステータスに関する詳細情報が表示されます。

「ポリシー ドメイン」タブでドメインを選択している場合、ドメイン内のホストに関するステータスが「ステータス」タブで表示されます。ホストを選択している場合、「ステータス」タブはホストのステータスに関する情報を表示します。

注: 「ステータス」タブにあるテーブルの列見出しを右クリックすると、表示する列を設定できます。

「ステータス」タブのポップアップ メニュー

「ステータス」タブのページにある列を右クリックすると、次のオプションを含むポップアップ メニューが表示されます。

- [テキストとしてコピー] - 選択されているテーブルの行および列見出しをテキストとしてコピーします。
- [すべて選択] - テーブルのすべての行を選択します。

- [ドメイン ツリーでホストを選択] - ホストを選択して、ドメイン ツリーでその場所を表示します。

全体概要一覧

「全体概要一覧」ページでは、各ホストの保護ステータスに関する以下の情報が表示されます。

- リアルタイム スキャンのステータス
- インターネット防御のセキュリティ レベル
- メール スキャン (受信および送信メール) のステータス
- 評価に基づいたブラウザ保護のステータス
- 脆弱性シールドのステータス

自動更新

「自動更新」ページにはホストがインストールしているパターン ファイルに関する情報が表示されます。

- パターン ファイルが最後に更新された日時
- パターン ファイルのバージョン
- F-Secureゲートウェイのパターン ファイルが最後に更新された日時
- ホストがパターン ファイルを最後に更新した日時と、統計情報を最後にポリシー マネージャに送信した日時の差 (差分の更新)
- ゲートウェイのパターン ファイルのバージョン
- スパイウェアの定義ファイルが最後に更新された日時
- スパイウェア定義ファイルのバージョン
- ゲートウェイのスパム定義ファイルが最後に更新された日時
- ゲートウェイのスパム定義ファイルのバージョン

アンチウイルス Citrix サーバ、アンチウイルス Citrix サーバ、インターネット ゲートウェイ、またはアンチウイルス Microsoft Exchangeをインストールしているホストにも、パターン ファイルの更新日とバージョン情報が表示されます。

ウイルス保護一覧

「ウイルス保護一覧」ページでは、以下の情報が表示されます。

- 最後に感染が検出された日時
- 最後に感染したウイルスの名前
- 最後に感染したオブジェクト
- 前回の感染時に実行した処理
- 感染した回数

インターネット防御一覧

「インターネット防御一覧」ページでは、以下の情報が表示されます。

- 最新の攻撃の日付および時刻 ([最新の攻撃のタイムスタンプ] 列)
- 最新の攻撃を受けたサービス
- 最新の攻撃の攻撃元
- 最近の攻撃 (列見出しをクリックすることで並べ替えが可能)
- 最近の攻撃のリセット時刻

コンポーネット ソフトのインストール状況

「コンポーネット ソフトのインストール状況」ページでは、ホストにインストールされているソフトウェアの情報が表示されます。

- クライアント セキュリティソフトウェアのバージョン (ビルド番号およびホットフィックスを含む)
- アンチスパイウェアのホットフィックス
- インターネット防御のインストール状況
- メール スキャンのインストール状況
- Web スキャンのインストール状況
- ブラウザ保護ののインストール状況
- ディープガードののインストール状況
- ポリシー マネージャ プロキシのバージョン

集中管理

「集中管理」ページでは、集中管理に関する情報が表示されます。

- ポリシー ファイルのタイムスタンプ
- ポリシー ファイルのカウンタ (ホストで使用中のポリシー ファイルの数)
- 統計の更新が最後にポリシー マネージャに送信された日付
- ホストの接続状況 (列見出しをクリックすることで並べ替えが可能)
- 新しいセキュリティ警告の数
- 新しい重大なエラーの数

ホストのプロパティ

「ホストのプロパティ」ページでは、各ホストに関する以下の情報が表示されます。

- ホストの WINS 名
- ホストの IP アドレス
- ホストの DNS 名
- ホストのオペレーティングシステム

「警告」タブ

「警告」タブでは、選択したホスト/ドメインにより発生した警告が表示されます。 また、このタブで警告の管理を行うこともできます。

「警告」タブでは、各警告に関する以下の情報が表示されます。

- 重大度
- 日付/時間
- 説明
- ホストおよびユーザ
- 警告に関連する製品

リストから警告を選択すると、ページの下部に警告に関する詳細な情報 (製品、重大度、発信したホストなど) が表示されます。クライアント セキュリティのスキャン警告にレポートが添付されている場合、ページの下部にレポートも表示されます。

[警告の転送を設定する] をクリックすると、「設定」タブの「警告」ページにアクセスして、警告の転送を設定できます。

「レポート」タブ

「レポート」タブでは、選択したホスト/ドメインからのウイルス スキャン レポートが表示されます。 また、このページでスキャン レポートの管理を行うことができます。

「レポート」タブでは、各レポートに関する以下の情報が表示されます。

- 重大度
- 日付/時間
- 説明
- ホストおよびユーザ
- レポートに関連する製品

レポートリストで行を選択すると、該当するスキャンレポートがページの下に表示されます。

「インストール」タブ

「インストール」タブは、ポリシー マネージャ コンソールをインストールした後に最初に表示されるタブです。

「インストール」タブには、インストールに関連する機能のショートカットがあります。 また、使用できるソフトウェア インストール パッケージも表示されます。

Windows ホストを自動検出	Windows ドメインおよびホストを自動的に検出します。検出したドメイン/ホストにソフトウェアのインストール情報を送信し、新しいホストをポリシー ドメイン ツリーにインポートします。
Windows ホストへのインストール情報の送信	IP アドレスまたはホスト名に基づいて、特定の Windows ホストにインストール情報を直接送信することができます。ホストが NT ドメイン (「自動検出」ビュー) に表示されない場合でも、ホストにソフトウェアのインストール情報を送信できます。
自動登録したホストのインポート	ホストに最初の製品がインストールされると、ホストはポリシー マネージャに自動登録メッセージを送信します。 ホストをポリシー ドメイン ツリーにインポートして、ポリシー管理の対象にします。
インストール パッケージ	使用できるインストール パッケージとその内容に関する詳細情報が表示されます。

注: サーバ上のパターン ファイルはポリシー マネージャ コンソールから手動で更新することはできません。ポリシー マネージャ サーバで更新を手動で行うには特別なツールが必要になります。

「操作」タブ

以下の操作は、ネットワークでウイルスが発生した場合や感染の疑いがある場合に使用することを推奨します。

「操作」タブでは、2つの操作を実行できます。

パターン ファイルの更新操作	選択したホストまたはドメイン内のすべてのホストに対し、新しいパターン ファイルを入手するよう指示します。

ウイルスとスパイウェア スキャン処理の操作	選択したホストまたは選択したドメイン内のすべてのホストに対し、ウイルスとスパイウェアをスキャンするように指示します。

LAN でウイルスが発生した場合、これらの操作を使用すると効率的です。

ツールバー

ツールバーには、ポリシー マネージャ コンソールの一般的なタスクを実行するためのボタンがあります。

	ポリシーデータを保存します。
	ポリシーを配布します。
	前のドメインまたはホストに移動します。
	次のドメインまたはホストに移動します。
	親ドメインに移動します。
	ホストまたはドメインを切り取ります。
	ホストまたはドメインを貼り付けます。
	選択されているドメインにドメインを追加します。
	選択されているドメインにホストを追加します。
	ホストまたはドメインのプロパティを表示します。
	「**Windows**ホストの自動検出」ツールを起動します。選択されているポリシー ドメインに新しいホストを追加します。
	Windows ホストへインストール情報の送信を開始します。
	選択されているドメインに、自動登録したホストをインポートします。緑色は、ホストが自動登録依頼を送信したことを示します。
	使用できるインストールパッケージを表示します。
	すべての警告を表示します。新しい警告が発生するとアイコンが強調表示されます。ポリシーマネージャコンソールの起動時には、アイコンが強調表示されます。

メニュー コマンド

ここでは、ポリシー マネージャ コンソールのメニューから実行できるコマンドを説明します。

メニュー	コマンド	処理
ファイル	新規ポリシー	MIB (マネージメント インフォメーション ベース) のデフォルト値を使用して新しいポリシーデータを作成します。通常、既存のポリシーデータを変更し、[名前を付けて保存] コマンドで新しいポリシーを保存するため、このコマンドはほとんど必要ありません。
	ポリシーを開く	保存されているポリシーデータを開きます。
	ポリシーの保存	開いているポリシー データを保存します。
	ポリシーに名前を付けて保存	名前を指定してポリシーデータを保存します。
	ポリシーの配布	ポリシーファイルを配布します。
	ポリシー ファイルのエクスポート	ポリシー ファイルをエクスポートします。
	終了	ポリシー マネージャ コンソールを終了します。
編集	切り取り	選択したアイテムを切り取ります。
	貼り付け	選択した場所にアイテムを貼り付けます。
	削除	選択したアイテムを削除します。
	新規ポリシー ドメイン	新しいドメインを追加します。
	新規ホスト	新しいホストを追加します。
	自動登録したホストをインポート	自動登録依頼を送信したホストをインポートします。
	Windows ホストを自動検出	Windows ドメイン構造からホストをインポートします。
	Windows ホストへインストール情報の送信	ソフトウェアをリモートでインストールし、IP アドレスまたは WINS 名で指定したホストをインポートします。
	検索	ホストのプロパティで文字列を検索します。選択したドメイン内のすべてのホストが検索されます。
	ドメイン/ホストのプロパティ	選択したホストまたはポリシー ドメインの「プロパティ」ウィンドウを表示します。
表示	組み込み制限エディタ	組み込み制限エディタと制限ダイアログボックスを切り換えます。
	メッセージ ウィンドウ	画面の下部に表示される「メッセージ」ウィンドウの表示/非表示を切り替えます。
	新規メッセージ受信時に開く	新しいメッセージを受信した場合、「メッセージ」ウィンドウを自動的に開きます。

メニュー	コマンド	処理
	戻る	前のドメインまたはホストに移動します。
	進む	次のドメインまたはホストに移動します。
	親ドメイン	親ドメインに移動します。
	警告	「警告」ページを開き、すべての警告を表示します。
	詳細モード	詳細モードに変更します。
	アンチウイルス モード	アンチウイルス モードに変更します。このユーザ インターフェースは、クライアント セキュリティの集中管理に最適化です。
	<項目名>の再表示	「ステータス」、「警告」、または「レポート」タブの情報を再表示します。選択されているページ/タブによって、表示されるメニュー項目が異なります。
	すべて再表示	すべてのデータを再表示します(ポリシー、ステータス、警告、レポート、インストールパッケージ、自動登録依頼など)。
ツール	インストール パッケージのサイズ	インストール パッケージの情報をウィンドウに表示します。
	パスワードの変更	ログイン パスワード (ポリシー マネージャ コンソールの秘密鍵を保護するパスワード) を変更します。
	レポート	レポートの詳細設定とレポートに含めるドメイン/ホストと製品を選択できます。
	一般設定	ポリシー マネージャ コンソールのローカル プロパティを設定します。
ヘルプ	目次	ヘルプの目次を表示します。
	登録	製品を認証するためのウィンドウを表示します。
	連絡先	F-Secureの連絡先を表示します。
	F-Secure ポリシー マネージャ コンソールについて	バージョン情報を表示します。

設定を継承する

ここでは、設定の継承がどのように機能するか、および継承された設定と再定義された設定がユーザ インターフェースでどのように表示されるのかについて説明します。

ポリシー マネージャ コンソールの設定は、ポリシー ドメイン構造の上位レベルから継承されているか、またはドメイン/ホスト レベルで直接指定/変更されているかのいずれかの方法で定義されます。ローカルで再定義された設定を「消去」すると (設定の横に表示される [消去] をクリック)、上位ドメイン レベルの値または設定のデフォルト値がその設定に再継承されます。

必要に応じて、設定を「確定」した状態にできます。確定された設定は、ユーザは変更できません。また、[確定] を指定すると、ポリシーが常に強制的に適用されます。 つまり、ポリシー変数がローカル ホストのあらゆる値を上書きし、制限が [確定] に設定されている限り、エンドユーザは値を変更できません。 設定が確定として定義されていない場合、ユーザは設定を変更できます。

継承された設定の見分け方 (ユーザ インターフェース)

継承された設定、および現在のレベルで再定義されている設定は、ポリシー マネージャのユーザ インターフェースで異なる方法で表示されます。

未継承	継承済み	説明
		設定が「確定」されているため、エンドユーザが設定を変更できないことを示します。 鍵の色が青色の場合、設定が再定義されています。鍵の色が灰色の場合、設定は継承されています。
		エンドユーザが設定を変更できることを示します。 鍵の色が青色の場合、設定が再定義されています。鍵の色が灰色の場合、設定は継承されています。
消去		設定が再定義されているため、設定の値を消去できることを示します。設定を消去すると、デフォルト値または継承された値が復元されます。このオプションが表示されない場合、設定が継承されていることになります。 設定の横に何も表示されない場合、設定が継承されていることを示します。
テキスト ボックス		継承された値は灰色の文字で淡色表示されます。

未継承	継承済み	説明
		継承されていない値は、白い背景色に黒い文字で表示されます。
チェック ボックス		継承した値は灰色の背景色で淡色表示されます。 継承されていない値は、白い背景色で表示されます。

ページの設定をすべてロック/ロック解除する

特定のページにある設定を一度にロック/ロック解除できます。

以下のリンクを使用して、ページ上の設定をすべてロックおよびロック解除できます。

ユーザ変更を許可	鍵のアイコンがある設定のロックをすべて解除します。この操作により、ユーザは該当する設定を変更できるようになります。
ユーザ変更を禁止	鍵のアイコンがある設定をすべてロックします。この操作により、ユーザはこれらの設定を変更できなくなります。
初期値に戻す	ページ上の全設定を初期値 (デフォルト値または継承値) に戻します。

設定を継承する (テーブル)

ここでは、テーブルの設定と継承について説明します。

「ファイアウォール セキュリティ レベル」テーブルおよび「ファイアウォール サービス」テーブルはグローバル テーブルと呼ばれ、ドメイン内の全コンピュータに同じ値が適用されます。ルールとサービスは同じでも、セキュリティ レベルはサブドメインとホスト別に違うレベル指定することが可能です。

テーブルで MIB から取り出されたデフォルト値は灰色で、現在のレベルで編集された値は黒で表示されます。

第
4
章

管理ネットワークのセットアップ

トピック：

- *ログイン*
- *ドメインとホストの管理*
- *ホストを追加する*
- *ローカル インストールとポリシー マネージャ*
- *感染しているホストへのインストール*
- *集中管理の接続を確認する*

ポリシー マネージャを使用して、ポリシー マネージャを環境に応じて導入することできます。

- Windows のドメインでは、「自動検出」と「自動登録」機能を使用して、管理ドメインを自動的に作成できます。
- Unix または Linux を実行しているコンピュータや管理対象のサーバがある場合、それらをポリシー マネージャと接続することでセキュリティ アプリケーションの一元集中管理が可能になります。

セキュリティ アプリケーションの一元集中管理を十分に活用する前に、管理対象となるドメイン構造を事前に計画することを推奨します。

同様のセキュリティ要件を持つエンドユーザを同じサブドメインにグループ化したり、それぞれのサブドメインでノートブックおよびデスクトップをグループ化したりするなど、ネットワークの規模や性質に応じてドメインを構造すると効率的です。そうすることで、ネットワークに常時接続しているコンピュータだけでなく、異なる LAN に接続するコンピュータまたはダイヤルアップ接続を使用するコンピュータなどに対しても最適なセキュリティ設定を定義できるようになります。

ログイン

ポリシー マネージャ コンソールを起動すると、「ログイン」ウィンドウが開きます。

ヒント: [オプション] をクリックすると、ログインに関するオプションが表示されます。

[接続] から接続先を選択します。それぞれの接続先は個別の設定を持っています。

1台のサーバに複数の接続を定義することもできます。接続先を選択したら、ポリシーマネージャ コンソールのパスワードを入力します。このパスワードはプログラムのインストール時に設定したもので、ネットワーク管理者のパスワードではありません。

読み取り専用モードでプログラムを起動する場合、パスワードの入力は不要です。ただし、このモードでは変更を加えることはできません。

セットアップ ウィザードが初期接続の構成を作成し、デフォルトの接続情報を [接続] フィールドに表示します。[追加]をクリックすると、接続先を追加できます。[編集]をクリックすると、接続先を編集できます (これらのオプションは [オプション] をクリックしたときに表示されます)。

接続先のコピーを作成することも可能です。この機能は、ポリシー環境の接続や設定の調整や検証が必要の場合に便利です。

接続プロパティ

「接続プロパティ」ウィンドウは、接続先の新規作成または編集を行う際に表示されます。

データ リポジトリ (保存場所) へのリンクは、ポリシー マネージャ サーバの HTTP URL として定義されます。

[名前] フィールドに接続先の名前を入力します。接続先の名前は、「ログイン」ウィンドウの [接続] フィールドで表示されます。フィールドを空のままにしておくと、URL またはフォルダのパスが表示されるようになります。

[公開鍵ファイル] および [秘密鍵ファイル] フィールドに接続で使用する管理用鍵ペアを指定します。指定した鍵ファイルが存在しない場合、ポリシー マネージャ コンソールは新しい鍵ペアを生成します。

通信に関する設定を変更する

「通信」タブでは、ステータス情報のポーリング間隔やホストのタイムアウト値など、通信に関連する設定を指定できます。

「接続プロパティ」ウィンドウを開きます (「ログイン」ウィンドウで [オプション] をクリックするこ)。

通信に関する設定を変更するには

1. 「通信」タブを選択します。
2. 必要の場合、[ホストの接続ステータス] を変更します。

   [ホストの接続ステータス] は、ホストがポリシー マネージャから切断されたと見なされる時間を設定します。指定した時間内にポリシー マネージャ サーバにアクセスしていないホストは、切断されたものと判断されます。切断されたホストのドメイン ツリーには通知アイコンが表示されます。また、「ドメインのステータス」ビューの [接続を切断されたホスト] リストにホストが表示されます。

   注: 1日未満の間隔を定義することが可能です。たとえば、「0.5」に設定すると、12時間以内にサーバに接続しなかったホストが切断されたものと見なされます。ノート コンピュータなどのモバ

イル デバイスが多い環境ではサーバから自然に切断されるホストがあるため、1日未満の値を指定することを推奨しません。

3. [ポーリング間隔のオプション] をクリックすると、ポーリング間隔を変更できます。
「ポーリング間隔」ウィンドウが開きます。
4. ポーリング間隔を指定します。

   通信プロトコルによって、デフォルトのポーリング間隔が異なります。特定の管理情報を必要としない場合、それらに対するポーリングを無効にできます。自動ポーリングは、パフォーマンスの問題が発生した場合にのみ無効にすることを推奨します。[すべてのポーリングを無効にする] をオンにすると、すべてのポーリング項目が無効になります。自動ポーリング機能が無効になっていても、選択したビューの情報を手動で更新できます。

これらの設定は「一般設定」ビューで編集できます。

ドメインとホストの管理

集中管理ネットワークでホストの種類 (ノートブック、デスクトップ、サーバ) やユーザ グループなどに応じて異なるセキュリティ ポリシーを指定する場合、構成と条件に基づいてドメインの構造を計画するとホストの管理が簡単かつ効率的になります。

ポリシーのドメイン構造を事前に設計した場合、ホストをドメインへ直接インポートすることが可能になります。管理環境をすぐに構築したい場合、ルート ドメインにホストをすべてインポートして、必要に応じてドメイン構造を後で作成できます。ホストはカット & ペーストを利用してドメインに追加できます。

各ドメインとホストには一意の名前が指定されている必要があります。

次の例では、各オフィスがサブドメインとして作成されています。

ポリシー ドメインを追加する

ここでは、ポリシー ドメインを追加する方法について説明します。

ポリシー ドメインを追加するには

1. 編集 ➤ 新規ポリシー ドメイン メニューからを選択します。
   または、ツールバーの
   - をクリックします。
   - Ctrl+ Insert を押します。

   追加したポリシー ドメインが選択したドメインのサブドメインになります。
2. ポリシー ドメインの名前を入力します。
   ドメインのアイコンが作成されます。

ホストを追加する

ここでは、ポリシー ドメインにホストを追加する方法について説明します。

ポリシー ドメインにホストを追加する方法は、使用しているオペレーティング システムによって異なります。次の方法でホストを追加できます。

- Windows ドメインからホストを直接インポートする
- 自動登録機能でホストをインポートする (ホストに管理エージェントをインストールしている必要がある。条件を指定して、自動登録したホストを異なるサブドメインにインポートすることも可能)
- [新規ホスト] コマンドを使用して、手動でホストを作成する

Windows ドメインのホストを追加する

Windows ドメインの場合、ポリシー ドメインにホストを追加する最も簡単な方法は、「インテリジェント インストール」を利用することです。

この方法では、インポートしたホストに管理エージェントがインストールされます。次の方法で Windows ドメインからホストをインポートできます。

1. 対象のドメインを選択します。
2. 編集 ➤ **Windows**ホストの自動検出 メニューからを選択します。
   自動検出の処理が完了すると、新しいホストが自動的にポリシー ドメイン ツリーに追加されます。

自動登録ホストのインポート

ホストをポリシー マネージャ コンソールにインポートする別の方法として、*自動登録*機能を利用できます。

この方法は、管理エージェントがホストにインストールされ、ホストが自動登録依頼を送信した後に実行できます。管理エージェントは、CD-ROM やログイン スクリプトなどを使用してインストールする必要があります。

自動登録したホストをインポートするには

1. ツールバーの をクリックします。
   または、
   - 編集 ➤ 自動登録したホストのインポート メニューからを選択します。
   - 「インストール」ビューで [自動登録したホストのインポート] を選択します。

   インポートが完了すると、ホストがドメイン ツリーに追加されます。インポートを行う際に条件 (ホストの IP アドレスや DNS アドレスなど) を指定すると、自動登録ホストを異なるドメインにインポートすることが可能です。「自動登録したホスト」タブでは、ホストが自動登録メッセージで送信するデータを確認できます。データの一覧には、インストール パッケージに含まれる自動登録のプロパティも表示されます
2. 「自動登録」ビューでは、次の操作が可能です。
   - 自動登録メッセージを項目別に並べ替える (項目の見出しをクリック)
   - 項目を自由に配置する (項目の見出しをドラッグ & ドロップ)、列の幅を調整 (項目をドラッグ)
   - テーブルに表示する項目を指定する (テーブルの見出しを右クリック)

自動登録のインポート ルールを使用する

「自動登録したホストのインポート」ウィンドウの「インポート ルール」タブで自動登録したホストのインポート ルールを設定できます。

次の項目をインポートのルールに適用できます。

- [WINS 名]、[DNS 名]、[動的な DNS 名]、[カスタム プロパティ]
  - ワイルドカード「*」 (アスタリスク) を使用できます。「*」は、任意の数の文字を表します。例: `host_test*`、`*.example.com`。
  - 大文字と小文字は区別されません。同じ文字として扱われます。
- [IP アドレス]、[動的な IP アドレス]
  - IP アドレスの一致 (例: `192.1.2.3`)、および IP サブドメインの一致 (例: `10.15.0.0/16`) に対応します。

1. 「インポート ルール」ウィンドウで列の見出しを右クリックしたときに開くポップアップ メニューを使用して、テーブルの列を表示および非表示することができます。

   一覧に表示されていない項目の値は、インポートするときの一致条件として使用されません。表示されている列の値が一致条件に適用されます。

2. また、カスタムのプロパティを追加して、ホスト インポート時の条件に使用することもできます。

   たとえば、ユーザ別に固有のポリシードメインをグループ化するとします。このような場合、カスタムのプロパティを追加して、ユーザとグループ別のインストール パッケージを作成できます。グループ名を識別するカスタムのプロパティを使用するインポート ルールを作成し、ホストを自由自在にインポートすることが可能になります。

   a) 列の見出しを右クリックして、[新しいカスタム プロパティの追加] を選択します。
      「新しいカスタム プロパティ」ウィンドウが開きます。
   b) カスタム プロパティの名前を入力して、[OK] をクリックします。
      新しいカスタム プロパティがテーブルに表示され、自動登録のインポート ルールで使用することが可能になります。

3. 自動登録インポート ルールを作成する

   a) 「インポート ルール」タブで [追加] をクリックします。
      「ルールのインポート先ポリシー ドメインの選択」ウィンドウで既存のドメインとサブドメインが表示されます。
   b) ルールの対象となるドメインを選択して、[**OK**] をクリックします。
   c) インポート条件を指定します。新しく作成された行を選択し、値を追加するセルをクリックしてから [編集] をクリックします。
   d) セルに値を入力します。
      インポート ルールが定義されます。

   - 自動登録したホストをインポートする際には、ルールが上から順に確認され、最初に一致するルールが適用されます。[下へ移動] または [上へ移動] をクリックすると、ルールの順序を変更できます。
   - 1つのドメインに対して複数のルールを作成する場合には [クローン] オプションを使用すると便利です。ドメインのルールを選択して [クローン] をクリックすると、ルールのコピーを作成できます。

4. インポートを開始する準備ができたら、「自動登録したホスト」タブで [インポート] をクリックします。

   定義したインポート ルールが、インポートの開始前に検証されます。

ホストのインポートが完了すると、正常にインポートされたホストの数と失敗したインポートの処理数が表示されます。ルール/条件が空白の場合、すべてのホストに一致すると見なされます。

ホストを手動で作成する

ここでは、ホストを手動で作成する方法について説明します。

ホストを手動で作成するには

1. 対象のドメインを選択します。
2. メニューから 編集 ➤ 新規ホスト を選択します。

   または、ツールバーの

   -
   - Insert を押します。

   ホストを手動で作成することは次のような場合に役立ちます。

   - 製品や機能を試用するため - ポリシー マネージャ コンソールの他にソフトウェアをインストールすることなく、ポリシー マネージャ コンソールの機能を試用することができます。
   - ポリシーを事前に定義するため - ソフトウェアをホストにインストールする前に、ホストのポリシーを定義および生成できます。
   - 特別な場合 - サーバに直接アクセスしないホストに対してポリシーを生成できます (つまり、ホストをインポートできない場合)。たとえば、F-Secure ポリシー マネージャ サーバにアクセスしないコンピュータに対するベース ポリシー ファイルを生成できます。ベース ポリシー ファイルは手動で、または他の方法で転送する必要があります。編集 ➤ ポリシーファイルのエクスポートメニューからを選択して、ベース ポリシー ファイルをエクスポートできます。

   注: 管理エージェントがインストールされていないホストはポリシーを取得できないため、ポリシー マネージャ コンソールを使用して管理することはできません。また、そのようなホストにはステータス情報も表示されません。ポリシー データを保存しないでポリシー マネージャ コンソールを終了しても、ドメイン構造の変更は適用されます。

インストール情報の送信

ここでは、インストール パッケージをホストに送る方法について説明します。

[**Windows**ホストの自動検出] と [**Windows**ホストへのインストール情報の送信] の機能は、インストールの対象となるホストの選択方法で異なります。[Windowsホストの自動検出] では、Windows ドメインを参照して、リストから対象ホストを選択します。[Windowsホストへのインストール情報の送信] では、IPアドレスまたはホスト名を直接指定して、対象ホストを設定します。ホストを選択した後、どちらの方法も同じ操作でインストールを進めます。

注: F-Secureをホストにインストールする前に、競合するアンチウイルスまたはファイアウォール プログラムがホストにインストールされていないことを確認する必要があります。

Windows ホストを自動検出

*自動検出*機能を使用して、ホストを追加できます。

ホストを選択するには

1. 対象のドメインを選択します。
2. 編集 ➤ **Windows** ホストを自動検出 メニューから選択します。

または、ツールバーの をクリックします。

3. [NT ドメイン] のリストからドメインを選択して、[再表示] をクリックします。

   [再表示] をクリックしたらホストのリストが更新されます。[再表示]をクリックしない場合、パフォーマンス上の理由でキャッシュされている情報が表示されます。[再表示] をクリックする前に、次の自動検出オプションを変更できます。

   - [すでに管理対象ホストを非表示] - F-Secureアプリケーションがインストールされていないホストが表示されます。
   - [すべての詳細でホストを解決 (低速)] - オペレーティング システムおよび管理エージェントのバージョンなど、ホストに関する詳細がすべて表示されます。
   - [ホスト名とコメントのみで解決(高速)] - ホストの名前とコメントが表示されます。詳細ビューにすべてのホストが表示されない場合、または一覧を取得するのに時間がかかる場合に便利なオプションです。

4. インストールするホストを選択します。

   インストールの対象となるホストにスペース キーを押します。Shiftキーを押した状態で以下のいずれかの操作を実行すると、複数のホストを簡単に選択できます。

   - 複数のホストをクリックする
   - 複数のホストを選択するようにマウスをドラッグする
   - 上下矢印キーを使用する

   また、マウスを右クリックして、ポップアップ メニューから次の操作を実行できます。

   - [オン] - 選択したホストをインストールの対象にします (スペース キーを押した場合と同じです)。
   - [オフ] - 選択したホストをインストールの対象から外します (スペース キーを押した場合と同じです)。
   - [すべてオン] - 選択した Windows ドメインの全ホストをインストールの対象にします。
   - [すべてオフ] - 選択した Windows ドメインの全ホストをインストールの対象から外します。

5. □インストール□ をクリックします。

ホストを選択した後、インストール情報の送信に進みます。

Windows ホストへのインストール情報の送信

[[Windows ホストへのインストール情報の送信] を使用して、インストールの対象となるホストを選択できます。

ホストを選択するには

1. 対象のドメインを選択します。
2. 編集 ➤ [Windows ホストへのインストール情報の送信メニューからを選択します。

   または、 をクリックします。

3. 対象となるホスト名を入力して、[次へ] をクリックします。

   [参照] をクリックすると、各ホストが使用している管理エージェントのバージョンを確認できます。

対象のホストを選択した後、ホストにアプリケーションのインストール情報を送信できます。

インストール情報の送信 (ホストを選択した後)

インストール先のホストを選択した後、インストールパッケージのインストール情報を送信できます。

インストール パッケージのインストール情報を送信するには

1. インストールで使用する言語を選択して、[次へ] をクリックします。
2. インストールする製品を選択し、[次へ] をクリックします。

   同じバージョンのアプリケーションがすでに存在する場合、強制的に再インストールを実行できます。
3. デフォルトポリシーの使用を選択するか、匿名ポリシーとしてホストまたはドメインポリシーを指定して、[次へ] をクリックします。
4. インストール情報の送信で使用するユーザ アカウントとパスワードを選択します。ユーザ アカウントには [このアカウント] (現在のアカウント) または [別のアカウント] を指定します。

   注: インストール情報の送信を行うには、インストール先マシンの管理者権限が必要になります。ログインしたアカウントが特定のホストの管理者権限を持っていない場合、そのホストに対して「アクセスは拒否されました」というエラーメッセージが表示されます。この状態で、他のホストのインストールは続行されます。

   [このアカウント] - 現在ログオンしているアカウントのセキュリティ権限を使用します。このオプションは、以下のいずれかの場合に適切です。

   - ドメイン管理者としてすでにログインしている場合
   - インストール先ホストでローカル管理者としてログインしている場合

   [別のアカウント] - 適用するアカウントとパスワードを入力します。適切なドメイン管理者のアカウントとパスワードを入力したら、インストールが実行します。

   - ドメイン アカウントを使用して、信頼済みドメインおよび信頼されていないドメインにインストールを行う場合は、必ず `DOMAIN\ACCOUNT` の形式でアカウントを入力してください。
   - ローカルの管理者アカウントを使用する場合、アカウント名をそのまま入力してください (アカウントの一部としてホスト名を入力しないでください。ホスト名を入力すると、そのアカウントは指定のホストにしか認識されません)。

   注: インストール中に、管理者のマシンが別のユーザアカウントでインストール先のマシンに接続している場合、NT 証明書の競合エラー メッセージ (**1219**) が表示されます。エラーを回避するために、インストール先のマシンに対する接続を閉じてから リモート インストールを実行してください。
5. インストールの内容を確認します。
6. 「リモート インストール」ウィザードを起動するために [開始] をクリックします。

   リモート インストール ウィザードにしたがってインストールを進めます。最後のウィンドウで [完了] をクリックすると、ウィザードが終了します。

   ポリシー マネージャが管理エージェントと指定した製品をホストにインストールします。インストールの進捗は [ステータス] で確認できます。[キャンセル] クリックすると、インストールを中止します。
7. ステータスが「完了」になると、インストールが完了したことになります。[インポート] を使用すると、新しく追加したホストをドメインに配置できます。
8. [完了] をクリックします。

   ここで別のドメインを指定しない限り、ポリシー マネージャ コンソールは事前に選択したドメインにホストを配置します。また、ホストをドメインに自動配置しないようにすることも選択できます。その場合、ホストが自動登録情報を送信し、ホストのインポートを可能にします。

   数分後、「製品ビュー」ウィンドウ (右側のウィンドウ) にインストールした製品が表示されます。
9. インストールした製品は、「インストール」タブ、または、「ポリシー ドメイン ツリーの最上位ドメインで確認できます。

ポリシーベース インストール

管理エージェントがインストールされているホストは、「ベース ポリシー ファイル」を利用してソフトウェアをインストールできます。

ポリシー マネージャ コンソールはインストールの操作を指定したインストール パッケージを作成し、ポリシー マネージャ サーバにファイルを格納して、ベース ポリシー ファイルにインストー ルタスクを書き込みます (このため、インストールの開始にはポリシー配布が必要です)。ベース ポリシー ファイルとインストール パッケージはどちらも管理用鍵ペアによって署名され、正規の情報だけがホストに受け付けられるようになっています。

ホスト上の管理エージェントはポリシー マネージャ サーバから新しいポリシーを入手し、インストール タスクを検出します。管理エージェントはその後、タスクのパラメータで指定されたインストール パッケージをサーバから入手し、インストール プログラムを開始します。

インストールが完了したら、管理エージェントはインストールの結果をインクレメンタル ポリシー ファイルに記録し、そのファイルをサーバに送ります。ポリシー マネージャ コンソールにファイルが届いたら、ホストのステータス情報が更新されます。

ベース ポリシー ファイルを利用して、アンインストールを行うことも可能です。その場合、上記と同じ通信方法が使用されます。ただし、アンインストールの結果は報告されません。

インストール エディタを使用する

インストール エディタは、管理エージェントがインストールされているホストで使用する必要があります。

インストール エディタを使用するには

1. 「ポリシー」タブのルート ノード (**F-Secure** サブツリー) を選択します。
   または、「インストール」タブを開きます。
   インストール エディタが開きます。
2. インストール エディタで、対象のホスト/ポリシードメインにインストールする製品を指定します。
   対象のポリシードメイン/ホストについて、次の情報が表示されます。

製品名	ホストまたはドメインにインストールされている製品の名前。またはインストールパッケージを使用してインストールできる製品の名前。
インストール済みのバージョン	製品のバージョン番号。複数のバージョンがインストールされている場合、それぞれのバージョン番号が表示されます。ホストの場合、バージョン番号は1つになります。
インストールするバージョン	インストール パッケージのバージョン番号。
インストール中のバージョン	ホストまたはドメインにインストール中のバージョン。
進行状況	インストールの進行状況。[進行状況] フィールドに表示される情報はホストとドメインによって異なります。

- ホストを選択している場合、[進行状況] フィールドに次のいずれかのメッセージが表示されます。

進行状況	インストールが開始 (ポリシーデータに追加) されたことを示します。インストールが成功したことはホストから報告されていません。`
失敗	インストールまたはアンインストールが失敗したことを示します。[進行状況] フィールドのボタンをクリックして詳細なステータス情報を確認できます。
完了	インストールまたはアンインストールが成功したことを示します。インストール エディタを終了すると、このメッセージは以後表示されません。
(フィールドに何も表示されていない場合)	実行中の操作がないことを示します。[インストール済みのバージョン] フィールドにインストールされている製品のバージョンが表示されます。

- ドメインを選択した場合、[進行状況] フィールドに次のいずれかのメッセージが表示されます。

残りのホスト: **<数>** - 失敗したインストールの数: **<number>**	<数>のインストールが失敗したこと、またはインストールが完了されていないことを示します。[進行状況] フィールドのボタンをクリックして、詳細なステータス情報を確認できます。
完了	全ホストでインストールまたはアンインストールが成功したことを示します。
(フィールドに何も表示されていない場合)	実行中の操作がないことを示します。[インストール済みのバージョン] フィールドにインストールされている製品のバージョンが表示されます。

3. 必要なバージョン番号をすべて選択したら、[開始] をクリックします。
インストール エディタがインストール ウィザードを起動します。ウィザードにしたがって、インストールのパラメータを指定します。次にインストール エディタは、カスタマイズしたインストール パッケージを用意します。新しいパッケージは、ポリシー マネージャ サーバに保存されます。

> 注: [開始] ボタンは、[インストールするバージョン] フィールドで選択した製品のインストールを開始します。[開始] ボタンをクリックせずにインストール エディタを終了すると、変更はすべて破棄されます。

4. インストールにポリシーが使用されるため、新しいポリシーファイルを配布する必要があります。

ポリシー ファイルには、ホストがインストール パッケージを取り出し、インストールを実行するためのエントリが追加されます。

インストールは完了するまで時間がかかることがあります。対象のホストがネットワークに接続していない場合、または実行中のインストール操作で、インストールが完了する前にユーザがホストを再起動するよう要求した場合、特に時間がかかる可能性があります。ホストがネットワークに接続され、ポリシー ファイルを正常に送受信しているにもかかわらず時間がかかる場合、問題が発生している可能性があります。または、ホストの方でインストール操作が正常に認識されていない可能性があります。いずれの場合も、[すべて停止] をクリックすることでポリシーのインストール操作を削除できます。インストール操作を削除した場合、対象のポリシー ドメイン/ホストに対して定義したインストール操作がキャンセルされます。確認ダイアログで [サブドメインおよびホストのインストールを再帰的にキャンセル] オプションを選択すると、対象のドメインとそのサブドメインに対するインストール タスクもすべて停止できます。

[すべて停止] ボタンは、対象のホスト/ドメインにインストール操作が定義されている場合にのみ利用可能です。サブドメインの操作は、ボタンの使用状態に影響しません。[すべて停止] ボタンをクリックすると、ポリシーから操作が削除されますが、ポリシーそのものは削除されません。ホストがすでに前のポリシーファイルをポーリングしている場合、インストール操作がインストール エディタに表示されていなくても、インストール操作が試行される可能性があります。

リモート アンインストール

アンインストールは、更新と同じように簡単に実行できます。製品のアンインストールに必要なソフトウェアしか含まれていない配布パッケージが作成されます。リモート アンインストールをサポートしていない製品には、アンインストールのオプションがインストール エディタで表示されません。

[再インストール] を選択すると、すでにインストールされているバージョンを再インストールします。このオプションは、問題を解決する場合にのみ使用してください。通常、製品を再インストールする必要はありません。

管理エージェントをアンインストールすると、管理エージェントが削除され、情報を送信することができないため、アンインストールが正常に完了したことを知らせる統計情報は送信されません。

1. F-Secureアンチウイルスをアンインストールする
2. アンインストールが成功したかポリシー マネージャ コンソールから報告されるまで待ちます。
3. F-Secureアンチウイルスが正常にアンインストールされた場合、管理エージェントをアンインストールします。
4. 管理エージェントのアンインストールが失敗した場合、ポリシー マネージャ コンソールはアンインストールが失敗したことを示す統計レポートを表示します。正常なアンインストールは報告されませんが、通信が切断されるため明らかになり、管理エージェントの最終レポートは「進行中」と表示します。

パッケージを利用したローカル インストール/更新

設定済みのパッケージを、JAR または MSI (Microsoft Installer) 形式でエクスポートすることができます。

MSI パッケージは、Active Directory 環境の Windows グループ ポリシーなどを使用して配布することができます。

エクスポートする方法はどちらの形式でも同じです。パッケージのファイル形式は、「インストールパッケージのエクスポート」ウィンドウで選択できます。

カスタムのリモート インストール パッケージを使用する

Windows プラットフォームでは、カスタムのリモート インストール パッケージ (JAR または MSI 形式) を使用してインストールを実行できます。

カスタムのインストール パッケージを使用するには

1. ポリシー マネージャ コンソールを起動します。
2. ツール ➤ インストール パッケージメニューからを選択します。
   「インストール パッケージ」ウィンドウが表示されます。
3. インストールする製品が含まれているインストール パッケージを選択して、[エクスポート] をクリックします。
4. ファイルの形式 (JAR または MSI) とカスタマイズしたインストール パッケージの保存場所を指定します。
5. カスタムのインストール パッケージの保存場所を指定して、[保存] をクリックします。
6. インストールする製品を選択して、[次へ] をクリックします。

7. デフォルト ポリシーの使用を選択するか、匿名ポリシーとしてホストまたはドメイン ポリシーを指定して、[次へ] をクリックします。
8. インストールの方法を選択します。

   デフォルトの集中管理インストールを推奨します。スタンドアロンのホストにパッケージを準備することもできます。

   インストールの内容が表示されます。
9. 内容を確認し、[開始] をクリックしてインストール ウィザードに進みます。

   ポリシー マネージャ コンソールは、選択した製品のセットアップに必要な情報を収集するリモート インストール ウィザードを表示します。インストール パッケージには、カスタムの自動登録プロパティを必要な数だけ入れることができます。これらのカスタム プロパティはローカル インストール後にポリシー マネージャに送信される自動登録メッセージに追加されます。カスタム プロパティは標準のホスト プロパティと一緒に「自動登録」ビューに表示されます。カスタムのプロパティ名が項目/列の名前となり、該当する値がセルの値として表示されます。

   異なるサブドメインにホストを追加する場合、個別のインストール パッケージをサブドメインごとに作成すると効率的です。その際、カスタムのプロパティを設定し、値がインストール パッケージごとに異なるようにします。これにより、「自動登録」ビューで列の並べ替えを行うことで各サブドメインにインポートするホストを簡単に判別できるようなります。「自動登録」ビューでインストール先のドメインを変更することができます。
10. ウィザードの最後のページで [完了] をクリックします。
11. エクスポートしたファイル (JAR/MSI) は、`ilaunchr.exe` ツールを実行してホストにインストールすることができます。

    `ilaunchr.exe` ツールは、ポリシー マネージャ コンソールのインストール先フォルダ (`...\Administrator\Bin`) に格納されています。

    a) `ilaunchr.exe` とエクスポートした JAR/MSI を、ログイン スクリプトがアクセスできる場所にコピーします。

    b) `ilaunchr <パッケージ名>.jar` コマンドを実行します。<パッケージ名>には、JAR/MSI パッケージのファイル名を使います。

    インストールが実行されたら、インストールの進捗を示すウィンドウが表示されます。インストール パッケージのエクスポート時に、コンピュータを再起動するように設定したら、ユーザに確認のメッセージが表示されます。次のコマンドを実行すると、インストールをサイレント モードで実行できます (ユーザの操作を必要としない)。`ilaunchr <package name>.jar /Q` サイレント モードの場合でも、インストール後にコンピュータの再起動を確認するメッセージが表示されることがあります。また、インストール中に重大なエラーが発生した場合にはメッセージが表示されます。

    ILAUNCHR は、以下のコマンドラインパラメータを指定できます。

    `/U` - ユーザ介入なしの非対話的モードでインストールを実行します。重大なエラーが発生した場合でもメッセージは表示されません。

    `/F` - 強制的にインストールを実行します。管理エージェントがすでにインストールされている場合でもインストールを完了します。

    コマンド ラインで「`ILAUNCHR /?`」と実行すると、ヘルプが表示されます。

    Windows XP 以降にインストールする場合、以下のパラメータを使用することもできます。

    - `/user:domain\username` (または `/user:username`) - ユーザ アカウントおよびドメイン名を指定します。ドメイン名は必ず指定する必要はありません。
    - `/password:secret` (または `/password:"secret with spaces"`) - ユーザ アカウントのパスワードを指定します。

パラメータを指定しない場合、ilaunchr はそのまま機能します。パラメータを1つしか指定していない、ilaunchr はエラー コードを返します。パラメータを両方指定している場合、ilaunchr はセットアップを実行します。例:

```
ILaunchr <jar ファイル> /user:domain\user_name /password:secret_word
```

ローカル インストールとポリシー マネージャ

クライアント セキュリティをローカルのコンピュータからインストールできます。

インストールを行う前に、ポリシー マネージャをすでにインストールしている必要があります。

注: ポリシー マネージャによって管理されることを前提とした上でクライアント セキュリティをインストールす場合、インストール中の管理オプションで [**F-Secure** ポリシー マネージャによる集中管理] をクリックします。その際に、ポリシー マネージャの公開鍵 (ポリシー マネージャ コンソールのインストール時に作成される「`admin.pub`」) とポリシー マネージャ サーバのネットワーク アドレスを指定する必要があります。

システム要件

ここでは、本製品を使用するためのシステム要件について説明します。

以下のシステム構成は、本製品を使用するための推奨要件です。

システム要件

プロセッサ:	• Windows Vista / Windows7: Intel Pentium 4 2 GHz 以上 • Windows XP: Intel Pentium III 1 GHz 以上
オペレーティング システム:	• Windows7 32 ビット/64 ビット • Windows Vista 32 ビット/64 ビット • Windows XP SP2 以降
メモリ:	• Windows Vista/Windows 7: 1 GB RAM 以上 • Windows XP: 512 MB RAM 以上
ディスク容量:	800 MB の空き容量
ディスプレイ:	• Windows Vista/Windows7: 16 ビット以上 (65000 色) • Windows XP: 16 ビット、65000 色以上
インターネットの接続環境:	ライセンスの認証と更新の受信に必要

他のセキュリティ製品をアンインストールする

クライアント セキュリティをインストールする前に、ホストにインストールされている他のセキュリティ プログラムをアンインストールする必要があります。

他のセキュリティ製品をアンインストールするには

1. スタート ➤ 設定 ➤ コントロール パネル ➤ プログラムの追加と削除 の順に選択します。
2. 関連するセキュリティ プログラムをアンインストールします。
   プログラムのアンインストール中にを問題が発生した場合、該当する取扱説明書を参照してください。
3. コンピュータを再起動します。

インストール手順

インストールを行うには、本製品の CD、正規のライセンス キーコー ド、およびインターネットの接続が必要となります。複数のユーザがコンピュータを共有している場合、管理者権限を持つユーザでログインしている必要があります。

ソフトウェアをインストールするには

1. インストール CD をドライブに挿入します。

   インストールが自動的に立ち上がります。自動的に立ち上がらない場合、Windows エクスプローラから CD-ROM アイコンをダブルクリックして、`setup.exe` を実行します。

   インストールが始まり、インストールの初期画面が表示されます。
2. インストールで使用する言語を選択して、[次へ] をクリックします。
3. 使用許諾契約書を確認します。使用許諾契約に同意する場合、[同意する] をクリックします。
4. ライセンス キーコードを入力して、[次へ] をクリックします。

   注: 本製品を試用する場合、ライセンス キーコードを入力せず [次へ] をクリックします。「試用オプション」ページで、試用するサービスを選択します。

   - 本製品のパッケージ版を購入した場合、ライセンス キー コードはクイック インストール ガイドの表紙に表記されています。
   - 本製品をエフセキュアのオンライン ショップから購入した場合、ライセンス キーコードは発注書の確認メールに表記されています。

   注: 本製品を購入した際に付与されるライセンス キーコードは本製品にのみ使用してください。ライセンス キーコードは購入したライセンス数と同じ台数のコンピュータにインストールできます (本ガイドの『エフセキュアのライセンス』を参照)。認証に問題がございましたら、エフセキュアのテクニカル サポートにお問い合わせください。
5. インストール方法を選択します。

   - 自動インストール: 本製品が自動的にインストールされます。コンピュータに他のセキュリティ製品がインストールされている場合、それらは自動的に削除されます。本製品はデフォルトのフォルダにインストールされます。
   - カスタムインストール:インストール先のフォルダなど、インストール時の細かい選択を指定できます。本製品はデフォルトのフォルダにインストールすることを推奨します。
6. [次へ] をクリックします。
7. インストールが完了したら、インストール CD をドライブから取り出します。
8. しばらくすると、コンピュータが自動的に再起動されます。すぐに再起動するには、[再起動] をクリックします。
9. 再起動後、本製品が自動的に更新をダウンロードできるようにシステムをネットワークに接続します。インターネットの速度によって、更新のダウンロードに時間が多少かかることがあります。更新のダウンロードが完了したら、本製品はご利用できる状態になります。

   ヒント: 本製品の詳細な機能については、製品のオンライン ヘルプを参照してください。ヘルプは、インターフェースにある [ヘルプ] ボタンをクリックすることでアクセスできます。オンライン ヘルプはインストール CD にも含まれています。

感染しているホストへのインストール

クライアント セキュリティのインストール先となるホストが、Klez ウイルスの亜種に感染した場合、インストールを開始する前にホストで Klez 駆除ツールを実行する必要があります。

`launchr.exe` のインストール ツールは、Klez に感染したコンピュータでは実行できませんので注意してください。

Kleztool は以下の場所からダウンロードできます。ftp://ftp.europe.f-secure.com/anti-virus/tools/kleztool.zip

`kleztool.zip` には `kleztool.txt` が含まれています。このファイルから Kleztool を実行する方法を参照できます。

集中管理の接続を確認する

次の方法で、集中管理の接続が正常に動作しているか確認できます。

1. 「概要」タブで [ポリシー配布ステータス] を確認します。
2. 必要に応じてポリシーを保存および配布します。
3. 「設定」タブを開いて、「集中管理」ページを選択します。
4. 使用しているポリシー ファイルの日付およびカウンタを確認します。

第
5
章

ウイルスとスパイウェア防御

トピック：

- *自動更新*
- *リアルタイム スキャン*
- *ディープガード*
- *ルートキット スキャン(ブラックライト)*
- *メール スキャン*
- *Web スキャン*
- *スパイウェア スキャン*
- *隔離保存されたオブジェクトを管理する*
- *エンドユーザによる設定の変更をブロックする*
- *警告の転送*
- *ネットワーク上のウイルスを監視する*
- *アンチウイルス保護を検証する*

ウイルスとスパイウェア防御は、ウイルス、スパイウェア、リスクウェア、ルートキット、メールおよびWebの脅威からコンピュータを保護します。

「自動更新」機能は、ウイルスとスパイウェア防御を常に最新の状態にします。セキュリティ ポリシーを配布し、ウイルスとスパイウェア防御と自動更新の設定を適用すると、ネットワークが保護された状態になります。また、ホストがポリシー マネージャ コンソールに送るスキャンの結果と他の情報を監視できるようにもなります。

コンピュータでウイルスが検出されると、次のいずれかの処理が実行されます。

- 感染したファイルの駆除
- 感染したファイルの名前の変更
- 感染しているファイルの削除
- 感染したファイルの隔離保存
- 感染しているファイルに行う処理をユーザに決定させる
- 感染しているファイルに関するレポートの送信
- 感染している添付ファイルの駆除、削除、またはブロック

自動更新

ここでは、ポリシー マネージャの自動更新に関する設定について説明します。

ここで記されている手順を行うと、ホスト上のウイルスとスパイウェア保護が常に最新の状態に保たれ、ユーザの必要に応じて最良の更新ソースを選択できるようになります。

自動更新の動作

クライアント セキュリティと一緒にインストールされる自動更新エージェントは、指定の更新ソースから更新をダウンロードします。

自動更新エージェントは次の順序で更新のダウンロードを試みます。

1. 企業などの大規模なネットワークでポリシー マネージャ プロキシが使用されている場合、クライアントがポリシー マネージャ プロキシを順番に使用してポリシー マネージャ サーバに接続しようとします。
2. クライアントが HTTP プロキシを使用するように設定されている場合、ポリシー マネージャ サーバは HTTP プロキシを通じて更新をダウンロードしようとします。
3. クライアントが更新をポリシー マネージャ サーバから直接ダウンロードしようとします。
4. 企業などの大規模なネットワークでポリシー マネージャ プロキシが使用されている場合、クライアントがF-Secureを順番に使用して、ポリシー マネージャ プロキシに接続しようとします。
5. クライアントがHTTPプロキシを使用するように設定されている場合、F-SecureのHTTPプロキシを通じて更新をダウンロードしようとします。
6. クライアントが更新をF-Secureから直接ダウンロードしようとします。

注: クライアント セキュリティでネイバーキャストの更新が有効の場合、他のクライアント セキュリティのインストールから更新をダウンロードすることが可能になります(他のマシンでもネイバーキャストが有効の場合)。

自動更新を設定する

「設定」タブの「自動更新」ページでは、クライアント セキュリティがウイルスのパターン ファイルとスパイウェアの定義ファイルの更新を自動的に受信するかどうかを指定できます。

自動更新を許可するには、[自動更新を有効にする]チェックボックスをオンにします。自動更新を常に有効にすることを推奨します。

[**F-Secure** ポリシー マネージャへの更新ポーリング間隔] フィールドに更新を確認する間隔を指定します。

「ポリシー マネージャ プロキシ」は利用できるポリシー マネージャ プロキシサーバのリストです。自動更新エージェントと一緒にインストールされるクライアント セキュリティは、テーブルで指定されているサーバの優先番号に従って、サーバに接続を試みます。

HTTP プロキシを代わりに使用する場合、[**HTTP** プロキシを使用する] ドロップダウン メニューから [ブラウザの設定を検出] または [ユーザ定義] を選択してから、[**HTTP** プロキシ アドレス] を指定します。

ポリシー マネージャ サーバからの自動更新を設定する

集中管理を使用すると、すべてのホストがポリシー マネージャ サーバから更新ファイル (ウイルス パターン ファイルとスパイウェア定義ファイル) を取得できるようになります。

集中管理を利用した自動更新を設定するには

1. 「ポリシー ドメイン」タブで [ルート] を選択します。
2. 「設定」タブに移動して、「アプリケーション通信制御」ページを開きます。
3. [自動更新を有効にする] が選択されていることを確認します。
4. [**F-Secure** ポリシー マネージャへの更新ポーリング間隔] で設定したポーリング間隔がネットワークに適合していることを確認します。
5. HTTP プロキシを使用したい場合、[**HTTP** プロキシを使用] と [**HTTP** プロキシ アドレス] の設定が環境に適合していることを確認します。
6. ポリシー マネージャ プロキシにアクセスできない場合、ポリシー マネージャ サーバまたはF-Secureの更新サーバから更新を入手するように設定できます。[ポリシー マネージャ プロキシに接続できない場合、ポリシー マネージャ サーバへの接続を許可する] または [ポリシー マネージャ プロキシに接続できない場合、エフセキュア更新サーバへの接続を許可する] を選択すると、該当するサーバへのアクセスが許可されます。
7. それぞれの設定の横にある鍵形のアイコンをクリックすると、エンドユーザが設定を変更できないように設定できます。
8. をクリックするとポリシーの保存と配布を行います。

ポリシー マネージャ プロキシを設定する

ネットワークに独自のポリシー マネージャ プロキシが複数ある場合、サブドメインやグループから別のサブドメイン/グループへと移動する特徴のあるノート コンピュータなどに対して、ポリシー マネージャ プロキシを更新ソースとして設定することを推奨します。

注: ポリシー マネージャ プロキシはF-Secureとは異なります。

この例では、ノート コンピュータが「ポリシー ドメイン」タブのサブドメインにインポートされ、ネットワークの様々なグループに独自のポリシーマネージャプロキシがあり、そのすべてにポリシーマネージャプロキシのリストが含まれているものと仮定します。

1. 「ポリシードメイン」タブで、ポリシー マネージャ プロキシを使用するサブドメインを選択します。
2. 「設定」タブに移動して、「アプリケーション通信制御」ページを開きます。
3. [自動更新を有効にする] が選択されていることを確認します。
4. [追加] をクリックして、リストに新しいサーバを追加します。[「**F-Secure** ポリシー マネージャ プロキシ サーバ プロパティ」ウィンドウが開きます。
5. ポリシー マネージャ プロキシの [優先度] テキストボックスに優先番号を入力します。

   優先番号は、ホストがポリシー マネージャ プロキシへの接続を試行する順番を定義します。例えば、普段ホストがあるネットワークのポリシー マネージャ プロキシに対しては10を使用し、その他のプロキシには20、30 などを使用します。
6. [アドレス] テキストボックスでポリシー マネージャ プロキシの URL を入力して、[OK] をクリックします。
7. 他のサーバを追加するために、必要に応じて上記の手順を繰り返します。
8. リストにプロキシをすべて追加したら、それらが正しい順番になっていることを確認します。

   必要な場合、優先番号を変更して順番を変更します。
9. それぞれの設定の横にある鍵形のアイコンをクリックすると、エンドユーザが設定を変更できないように設定できます。
10. をクリックするとポリシーの保存と配布を行います。

👉 **注:** エンドユーザはローカルのユーザ インターフェースのリストにポリシー マネージャ プロキシを追加することもできます。ホストはパターン ファイルとスパイウェアの定義ファイルの更新をダウンロードする時に2つのリストを組み合わせて使用します。エンドユーザが追加したポリシー マネージャ プロキシは、管理者が追加したプロキシより優先され、先に試行されます。

ネイバーキャスト

更新は、サーバとプロキシに加え、他のホストやクライアントからもダウンロードできるように設定できます。

この機能は「ネイバーキャスト」といいます。更新は次のソースからダウンロードすることが可能です。

- ポリシー マネージャ サーバ
- ポリシー マネージャ プロキシ
- HTTP プロキシ
- F-Secureの更新サーバ
- ネイバーキャストを有効にしている他の自動更新エージェント(たとえば クライアント セキュリティ)

ネイバーキャストを有効にするには

1. 対象のドメインを選択します。
2. 「設定」タブから「自動更新」を選択します。
   a) [ネイバーキャスト クライアントを有効にする] を選択すると、他のクライアントから更新をダウンロードできるホストを指定します。
   b) [ネイバーキャスト サーバを有効にする] を有効すると、更新を提供できるクライアントを指定します。
3. [ネイバーキャスト ポート] を選択すると、ネイバーキャストが使用するポートを変更できます。

リアルタイム スキャン

リアルタイムスキャンは、ファイルを開いたり、閉じたりする際にスキャンを行うため、コンピュータを常に保護します。

スキャンはバックグラウンドで実行されます。つまり、スキャン中にユーザの画面には何も表示されません。

リアルタイム スキャンを設定する

ここでは、設定 ➤ リアルタイム スキャンページの設定について説明します。

[リアルタイム スキャンを有効にする] チェックボックスをオンにすると、リアルタイム スキャンを有効にします。[リアルタイム スキャンを有効にする] チェックボックスをオフにすると、リアルタイム スキャンを無効にします。

スキャンに関連するオプション

- すべてのファイル

  すべてのファイルをスキャンします。システムのパフォーマンスがかなり低下するため、日常的に使用するオプションとしてはお勧めできません。

- 次の拡張子のファイル

  指定した拡張子のファイルをスキャンします。ピリオド「.」を入力することで拡張子が付いていないファイルを指定できます。。ワイルドカード「?」を使用して、任意の文字を表すこともできます。それぞれのファイル拡張子を、スペースで区切って指定します。リアルタイム スキャンでは、このオプションを使用し、スキャンの対象となるファイルを絞ることを推奨します。パターン ファイルが更新されたときに危険な拡張子が自動的にリストに追加されます。

- 対象外の拡張子を有効にする

  [対象外の拡張子] フィールドにスキャンから除外するファイルの形式 (拡張子) を入力します。この機能は、スキャンの対象に [すべてのファイル] を指定している場合に効率的です。

- 対象外のオブジェクトを有効にする

  対象外のオブジェクトとは、通常ローカルで設定される個別のファイルまたはフォルダを指します。この設定は、[対象外のオブジェクトを有効にする] チェックボックスを右クリックして、[詳細モードで検索] を選択することにより、ポリシー マネージャ コンソールから設定することもできます。

- ネットワーク ドライブをスキャン

  ネットワーク ドライブのファイルをスキャンの対象に指定します。

  重要: クライアント セキュリティでは、[ネットワーク ドライブをスキャン] はデフォルトで無効に設定されています。

- 作成または変更時にスキャン

  通常、ファイルは開かれる際にスキャンされ、閉じる際にはスキャンされません。この設定を有効にすると、ファイルを閉じる際にもスキャンが行われるようになります (ファイルに変更があった場合にのみスキャンが行われます)。この設定はデフォルトで有効で、有効に残すことを推奨します。

- 感染時の処理を自動的に行う

  クライアント セキュリティ 9 以降、およびアンチウイルス Windows サーバ 9 以降のオプションで、感染を自動的に処理します。

- 感染時のカスタム処理

  自動処理が無効の場合、感染に対して行うデフォルトの処理を指定できます。

処理	説明
スキャン後に問い合わせる	駆除ウィザードを起動します。
自動的に駆除	感染を自動的に駆除します。
自動的に名前を変更	感染しているファイルの名前を変更します。
自動的に削除	感染しているファイルを削除します。ウイルスと関連付けられているファイルが削除されるため、このオプションは推奨しません。
レポートのみ	ウイルス検出を通知し、感染したオブジェクトが開かないようにします。このオプションはウイルスをレポートするだけで、ウイルスに対する処理は何も行われません。
自動的に隔離保存	感染しているファイルを隔離保存フォルダに移動します。

- **Hosts** ファイルを保護する

  Hosts ファイルがスパイウェアによって変更されることをブロックします。マルウェアの中には、Hosts ファイルにある有名な DNS 名の IP アドレスを悪質な Web サイトの IP アドレスと置き換えようとするものがあります。

- 追跡**Cookie** をスキャンする

  追跡 Cookie をスキャンするか指定します。リアルタイム スキャンは、ディスク上の追跡 Cookie のみを検出できます。ブラウザのキャッシュに保存されている Cookie から感染を検出することはできません。マニュアル スキャンは、ブラウザのキャッシュに保存されている Cookie から感染を検出することができます。

ファイル拡張子の処理

クライアント セキュリティには、ポリシーで定義されたスキャン対象の拡張子のリスト (「すべてのファイル」の場合もある) があります。スキャン対象のリストは、対象となっている拡張子から、対象外として指定されている拡張子を除いた拡張子を含み、リアルタイム スキャン、マニュアル スキャン、およびメール スキャンに適用されます。

ドメイン全体にリアルタイム スキャンを有効にする

この例では、リアルタイム スキャンをドメイン全体に有効にします。

1. 「ポリシー ドメイン」タブで [ルート] を選択します。
2. 「設定」タブに移動して、「リアルタイム スキャン」ページを開きます。
3. [リアルタイム スキャンを有効にする] チェックボックスをオンにします。
4. [スキャン対象ファイル] ドロップダウン リストから、[次の拡張子のファイル] を選択します。

5. 感染ファイルの検出時に実行する処理を [ファイル スキャン: 感染時の処理] ドロップダウン リストから選択します。
6. ページの他の設定がシステムに対して適切かどうかを確認し、必要に応じて設定を変更します。
7. をクリックするとポリシーの保存と配布を行います。

ホストにリアルタイム スキャンの使用を強制する

この例では、全ホストでリアルタイム スキャンを有効にし、エンドユーザがその設定を無効にできないようにします。

1. 「ポリシー ドメイン」タブで [ルート] を選択します。
2. 「設定」タブに移動して、「リアルタイム スキャン」ページを開きます。
3. [リアルタイム スキャンを有効にする] チェックボックスをオンにします。
4. [スキャン対象ファイル] ドロップダウン リストから、[次の拡張子のファイル] を選択します。
5. 感染ファイルの検出時に実行する処理を [感染時のカスタム処理] ドロップダウン リストから選択します。

   または、[感染時の処理を自動的に行う] を選択します。
6. ページの他の設定がシステムに対して適切かどうかを確認し、必要に応じて設定を変更します。
7. [ユーザによる変更を禁止する] をクリックして、エンドユーザがリアルタイム スキャンを無効にできないように設定します。
   ロックされた鍵型のアイコンがページ内の全設定の横に表示されます。
8. をクリックするとポリシーの保存と配布を行います。

リアルタイム スキャンから Microsoft Outlook の .pst ファイルを除外する

Microsoft Outlook の PST ファイルは一般的にファイル サイズが大きいため、スキャンに時間がかかり、システムのパフォーマンスを低下する可能性があります。スキャンする必要がない場合、PST ファイルをリアルタイム スキャンの対象から除外することを推奨します。

PST ファイルをドメイン全体のスキャンから除外するには

1. 「ポリシー ドメイン」タブで [ルート] を選択します。
2. 「設定」タブに移動して、「リアルタイム スキャン」ページを開きます。
3. [対象外の拡張子を有効にする] チェックボックスをオンにします。
4. [対象外の拡張子] テキストボックスに、拡張子「PST」を追加します。

   拡張子の前にはドット「.」を付けないでください。
5. それぞれの設定の横にある鍵形のアイコンをクリックすると、エンドユーザが設定を変更できないように設定できます。
6. をクリックするとポリシーの保存と配布を行います。

ディープガード

ディープガードはファイルとプログラムの動作を分析するホスト型侵入防止システムです。

ディープガードは、ブラウザで表示される未承諾広告のポップアップをブロックしたり、システムの重大な設定や Internet Explorer の設定を無断な変更から保護したりすることができます。

アプリケーションが危険性のある処理を試行した場合、処理の安全性が確認されます。安全なアプリケーションの処理は許可され、危険なアプリケーションの処理はブロックされます。

ディープガードが信頼できないアプリケーションを検出した場合、ディープガードはアプリケーション通信制御と通信し、アプリケーションの安全性を確認するメッセージをユーザに表示することができます。

ディープガードを設定する

設定 ➤ リアルタイム スキャンページでディープガードの設定が表示されます。

[ディープガードを有効にする] を選択すると、ディープガードを有効にします。

オプションを有効にすると、システムの変更試行が検出された際に処理を選択できるようになります。

処理	説明
表示画面で操作を確認	ディープガードが安全と判断したアプリケーションでもユーザに許可/ブロックを確認します。
不明な場合に表示画面で操作を確認	ディープガードがアプリケーションの安全性を判断できない場合、ユーザに確認を求めます。デフォルトのオプションです。
自動: 確認しない	ディープガードがアプリケーションを独自に判断し、自動的にアプリケーションを許可/ブロックします。

ディープガードは高度なモニタリング機能を使用して、実行中のプログラムを一時的に変更します。このため、一部のプログラムの動作に問題が発生する可能性があります。問題が発生する場合、[高度なモニタリングを有効にする] を無効にしてください。

ディープガードのサーバ クエリ

ディープガードのサーバ クエリ機能は、マルウェアの検出を支援する最新の情報を提供し、誤検出の可能性を低くします。

[サーバのクエリを使用して検出率を向上する] を選択すると、ディープガードは不明なアプリケーションを検出したときにF-Secureのサーバと確認を行います。次の理由でこのオプションを有効にすることを推奨します。

- サーバ クエリを有効にすると、スキャンの検出率が上がるため、システム全体の保護が向上します。サーバ クエリは、未知の脅威に対する保護が発見されるまでの時間を短くします。
- サーバクエリを有効にすると、確認ダイアログの表示頻度が著しく低くなります。これにより、ユーザの判断ミスなどによってシステムが異常になる可能性も低くなります。また、煩わしいダイアログが表示されにくくなることで、ユーザはより快適にシステムを操作できるようになります。

サーバ クエリについて

サーバ クエリはインターネットに接続している状態でのみ機能します。ネットワークのアクセスが HTTP プロキシに制限されている場合、サーバ クエリを使用する前に自動更新エージェントの HTTP プロキシにプロキシ サーバのアドレスを指定する必要があります。

ルートキット スキャン (ブラックライト)

ルートキットスキャンは、ルートキットによって隠されているファイルやドライブを検出することができます。

ルートキットは、悪質なソフトウェア (スパイウェアなど) をユーザ、システム ツール、およびアンチウイルス スキャナから隠します。ルートキットの中に隠されているファイルはウイルスやワーム、トロイの木馬によって感染されていることがよくあります。

ルートキット スキャン

「設定」タブの「マニュアル スキャン」ページでルートキット スキャンの設定が表示されます。

ルートキット スキャンは手動で実行できます。または [完全チェック] に含むことができます。

[ルートキット スキャンを有効にする] を選択すると、ルートキットによって隠されているファイルやドライブのスキャンを有効にします。オプションを有効にすると、ユーザはローカルでルートキットのクイック スキャンを実行できるようにもなります。

[システムの完全チェックにルートキット スキャンを含む] を選択すると、ホストがコンピュータの完全チェックを実行した際に、またはポリシー マネージャ コンソールがマニュアル スキャンを実行した際に、ルートキットがスキャンの対象に含められるようになります。

[スキャン後に疑わしいファイルを表示する] を選択すると、完全チェックで検出された不審なアイテムが駆除ウィザードとスキャンレポートで表示されるようになります。スキャン レポートから、ホストでルートキットや隠しアイテムが検出されたかどうかを確認できます。

ドメイン全体にルートキット スキャンを実行する

この例では、ルートキット スキャンをドメイン全体に実行します。

1. 「ポリシー ドメイン」タブで [ルート] を選択します。
2. 「設定」タブに移動して、「マニュアル スキャン」ページを開きます。
3. 「ルートキット スキャン」ウィンドウで [ルートキット スキャンを有効にする] チェックボックスが選択されていることを確認します。
4. [完全チェックを行い不審なアイテムを表示] チェックボックスを選択します。
5. ページの他の設定がシステムに対して適切かどうかを確認し、必要に応じて設定を変更します。
6. 「操作」タブに移動して、[ウイルスとスパイウェア スキャン] ボタンをクリックします。

   注: 操作を開始するには、ポリシーを配布する必要があります。

7. をクリックするとポリシーの保存と配布を行います。

スキャンが完了したら、「レポート」タブでスキャン レポートを確認できます。

メール スキャン

メール スキャンは、メールをウイルスから保護する機能です。

メール スキャンを発信メールに対して有効にすると、感染したメールの添付ファイルを誤って送信することを防ぐことができます。ここでは、メール スキャンの設定について説明します。

メール スキャンは POP、IMAP、および SMTP を使用するメールをすべてスキャンします。SSL プロトコルが使用されている場合、SSL 経由の添付ファイルはローカル メールのキャッシュに保存され、その際にスキャンされます。また、送信される添付ファイルもリアルタイム スキャンによってスキャンされます。

メール スキャンを設定する

「設定」タブの「メール スキャン」ページで、メール スキャンの設定が表示されます。

受信するメールと添付ファイルに対するスキャンを有効にする場合、[受信メール スキャンを有効にする] を選択します。

送信するメールと添付ファイルのスキャンを有効にする場合、[送信メール スキャンを有効にする] を選択します。

感染しているメールが検出された時の処理を選択できます。

- 受信メール スキャン
  1. 受信した添付ファイルが感染している場合の処理
     - [添付ファイルを駆除] - 駆除ウィザードを起動します。
     - [添付ファイルを削除] - 添付ファイルを削除します。
     - [レポートのみ] - 管理者へレポートを送ります。
  2. スキャンが失敗した場合の処理
     - [添付ファイルを削除] - 添付ファイルを削除します。
     - [レポートのみ] - 管理者にレポートを送ります。
  3. ヘッダ部に不正な形式がある場合
     - [メッセージ部分を削除] - メッセージを削除します。
     - [レポートのみ] - 管理者にレポートを送ります。

- 送信メール スキャン
  1. 送信する添付ファイルが感染している場合の処理
     - [メールをブロック] - メールを送信できないようにします。
     - [レポートのみ] - 管理者にレポートを送ります。
  2. スキャンが失敗した場合の処理
     - [メールをブロック] - メールを送信できないようにします。
     - [レポートのみ] - 管理者にレポートを送ります。
  3. ヘッダ部に不正な形式がある場合
     - [メッセージ部分を削除] - メッセージを削除します。
     - [レポートのみ] - 管理者にレポートを送ります。

注意: [レポートのみ] オプションは危険なため、通常の操作では使用しないでください。

ブロックされたメールをエンドユーザの送信トレイ フォルダに保存するには、[ブロックされたメールを送信トレイに保存]チェックボックスをオンにします。このオプションを有効すると、ユーザは他のメッセージを送信する前に、送信トレイのブロックされたメッセージを移動、削除、または変更する必要があります。

メール スキャンで対象および対象外となるファイル形式は「リアルタイム スキャン」ページで設定したファイル形式に基づいています。

大きなファイルのスキャン時にエンドユーザに対してダイアログ ボックスを表示する場合、[大きなファイルのスキャン時に進行状況を表示する]チェックボックスをオンにして、[次の時間が経過したら進行状況を表示] フィールドで制限時間を指定します。

スキャンの完了後にエンドユーザに対してスキャン レポートを表示する場合、[感染が見つかった場合にレポートを表示] を選択します。

受信および送信メールに対してメール スキャンを有効にする

この例では、受信および送信メールに対してメール スキャンを有効にします。

1. 「ポリシー ドメイン」タブで [ルート] を選択します。
2. 「設定」タブに移動して、「メール スキャン」ページを開きます。
3. 受信メール スキャンを設定する
   a) [受信メール スキャンを有効にする] を選択します。
   b) [受信した添付ファイルが感染していた場合の処理] ドロップダウン リストから、実行する処理を選択します。
   c) [スキャン失敗時の処理] ドロップダウン リストから、実行する処理を選択します。
   d) [不正な形式のメッセージ部分の処理] ドロップダウン リストから、実行する処理を選択します。
4. 送信メールスキャンを設定する
   a) [送信メール スキャンを有効にする] を選択します。
   b) [送信する添付ファイルが感染していた場合の処理] ドロップダウン リストから、実行する処理を選択します。
   c) [スキャン失敗時の処理] ドロップダウン リストから、実行する処理を選択します。
   d) [不正な形式のメッセージ部分の処理] ドロップダウン リストから、実行する処理を選択します。
5. 一般設定を確認する

   ページの他の設定がシステムに対して適切かどうかを確認し、必要に応じて設定を変更します。
6. をクリックするとポリシーの保存と配布を行います。

Web スキャン

Web スキャンは、HTTP トラフィック/データ通じて (Web ページなどから) 送られてくるウイルスからコンピュータを保護します。

Web スキャンを有効にすると、HTML ファイル、画像ファイル、および Web からダウンロードするアプリケーションや実行可能ファイルなどがスキャンされるようになります。ダウンロードされたファイルからウイルスが検出された場合、ウイルスが自動的に削除されます。Web スキャンは、ウイルスをブロックした際にエンドユーザに通知を送る機能も備えています。

ここでは、Web スキャンの設定について説明します。

Web スキャンを設定する

設定 ➤ **Web** スキャンページで Web スキャンの設定が表示されます。

HTTP スキャン有効にするには、[**HTTP** スキャンを有効にする] チェックボックスをオンにします。

[感染時のアクション] ドロップダウン リストで、HTTP データに感染が検出されたときに実行する処理を選択できます。

- [ブロック] - 感染したファイルのアクセスをブロックします。
- [レポートのみ] - 管理者にレポートを送ります。

[スキャン失敗時の処理] ドロップダウン リストで、HTTP データのスキャンが失敗した場合に実行する処理を選択します。この設定は、パスワードで保護されている圧縮ファイルなどを処理する際に適用されます。

- [ブロック] - スキャンできなかったファイルをブロックします。
- [レポートのみ] - 管理者にレポートを送ります。

[圧縮ファイルのスキャン] を選択にすると、圧縮ファイルの内部をスキャンするようになります (対応ファイル形式は、ZIP、ARJ、LZH、RAR、CAB、TAR、BZ2、GZ、JAR、TGZ)。

「信頼済みの **HTTP** サイト」テーブルでは、信頼されている HTTP サイトを指定することができます。信頼済みと指定されたサイトには HTTPスキャンは実行されません。

ドメイン全体に Web スキャンを有効にする

この例では、Web (HTTP) スキャンをドメイン全体に有効にします。

1. 「ポリシー ドメイン」タブで [ルート] を選択します。
2. 「設定」タブに移動して、「**Web** スキャン」ページを開きます。
3. [**HTTP** スキャンを有効にする] チェックボックスをオンします。
4. [感染時のアクション] が [ブロック] に設定されていることを確認します。
5. [スキャン失敗時の処理] が [ブロック] に設定されていることを確認します。
6. ページの他の設定がシステムに対して適切かどうかを確認し、必要に応じて設定を変更します。
7. をクリックするとポリシーの保存と配布を行います。

Web サイトを Web スキャンから除外する

特定の Web サイト/ページを「信頼済みのサイト」テーブルに指定すると、Web スキャンはそのサイト/ページをスキャンしないようになります。

Web サイトに認識できないストリーム コンテンツなどがあって、スキャンに時間がかかる場合や動作が著しく遅くなる場合、Web サイトを Web スキャンから除外すると効率的です。

次の例では、1つのドメイン (www.example.com)、そして別のドメインのサブディレクトリ (www.example2.com/news) を Web スキャンから除外します。

1. 「ポリシー ドメイン」タブで [ルート] を選択します。
2. 「設定」タブに移動して、「**Web** スキャン」ページを開きます。
3. ドメインを Web スキャンの対象外にする

   ドメイン全体を Web スキャンから除外するには、ドメインの URL を「信頼済みのサイト」テーブルに追加します。

   a) 「信頼済みのサイト」テーブルの下にある [追加] ボタンをクリックします。
      テーブルに新しい行が作成されます。
   b) 新しく作成された行をクリックして、「`http://*.example.com/*`」を入力します。
      アドレスにワイルドカード「*」を入れていることで、「example.com」のすべてのサブドメインとページが信頼済みのサイトとして登録されます。
   c) 「信頼済みのサイト」テーブルの下にある [追加] ボタンをクリックします。
      テーブルに新しい行がもう1つ作成されます。
   d) 新しく作成した行をクリックして、「`http://example.com/*`」を入力します。
      この URL 定義によって、「example.com」の第2レベル ドメインがすべて信頼済みのサイトとして登録されます。
4. サブディレクトリを Web スキャンの対象外にする

   サブディレクトリを HTTP スキャンから除外するには、ディレクトリのパスを含めたドメインの URL を「信頼済みのサイト」テーブルに追加します。

   a) 「信頼済みのサイト」テーブルの下にある [追加] ボタンをクリックします。
      テーブルに新しい行が作成されます。
   b) 新しく作成した行をクリックして、「`http://www.example2.com/news/*`」を入力します。
5. をクリックするとポリシーの保存と配布を行います。

スパイウェア スキャン

スパイウェアスキャンは、ホストを Data Miner、監視ツール、ダイヤラなどのスパイウェアから保護します。

集中管理モードでスパイウェア スキャンを使用している場合、ホストでスパイウェアが検出された際に管理者にレポートを通知する機能やスパイウェアを自動で隔離保存するように設定できます。また、特定のスパイウェア アプリケーションの実行を許可することもできます。

スパイウェアとリスクウェアの駆除について

スパイウェアは、合法かつ正当なアプリケーションとウイルスやトロイの木馬などの悪質なプログラムの間に属する、「グレイゾーン」にあるソフトウェアです。スパイウェアの中には、別のアプリケーションを実行するために必要なものから、単体で動作し、一度も実行してはいけないマルウェアに部類するものがあります。デフォルトでは、スパイウェア スキャンはすべてのスパイウェアの実行を許可します。セキュリティの強化でスパイウェアの実行をすべて拒否する前に、ネットワークでいくつかのスパイウェアを許可する必要があるか確認することを推奨します。

スパイウェア スキャンは、リスクウェアを検出および通知する機能も備えています。リスクウェアは直接被害を与えないが、設定によって危険性のあるプログラムです。代表的なリスクウェアで、IRC などのチャット アプリケーションやファイル転送 ソフトウェアがあります。

スパイウェア制御を設定する

ここでは、スパイウェア スキャンの設定について説明します。

スパイウェア スキャンは、リアルタイム スキャンおよびマニュアル スキャンに統合されています。「リアルタイム スキャン」ページで [リアルタイム スキャンを有効にする] を選択すると、スパイウェアのスキャンがリアルタイム スキャンに含まれます。また、マニュアル スキャンを実行するときには、スパイウェアが自動的にスキャンの対象になります。

「スパイウェア スキャンで対象外のアプリケーション」テーブルには、管理者が許可したスパイウェアとリスクウェアの情報が表示されます。

「ホストから報告されているスパイウェアとリスクウェア」テーブルには以下の情報が含まれます。

ホストから報告されているスパイウェアとリスクウェア	
スパイウェアまたはリスクウェア名	スパイウェアまたはリスクウェアの名前。
種類	スパイウェアの種類。(「アドウェア」、「Data Miner」、「ダイヤラ」、「マルウェア」、「監視ツール」、「不正ダイヤラ」、「リスクウェア」、「脆弱性」、「ワーム」、「Cookie (追跡 Cookie)」、または「その他」)
重大度	スパイウェア/ リスククェアの重大度。(3□10)
ホスト	スパイウェア/リスクウェアが検出されたホストの名前。
スパイウェア ステータス	スパイウェア/リスクウェアのステータス。

ホストから報告されているスパイウェアとリスクウェア	
	[アクティブである可能性] - スパイウェア/リスクウェアがホストでアクティブである可能性を示します。スパイウェア/リスクウェアは処理されていません。 [削除済み] - スパイウェア/リスクウェアがホストから削除されたことを示します。 [隔離保存済み] - スパイウェア/リスクウェアがホストで隔離保存されたことを示します。 [現在隔離済み] - スパイウェア/リスクウェアが隔離保存フォルダに格納されていることを示します。
タイムスタンプ	スパイウェア/リスクウェアがホストで検出された日時。

「ホストから報告されているスパイウェアとリスクウェア」テーブルの項目は、ホスト上でマニュアル スキャンを実行した際に、またはホストから隔離保存されたスパイウェアを削除した際に消去されます。

ドメイン全体にスパイウェア制御を設定する

ホストをスパイウェアと追跡 Cookie から保護する設定について説明します。

スパイウェア制御をネットワークに導入する前に、ホストをいくつか用意して、スパイウェア制御の機能を試験的に検証することを推奨します。特定のスパイウェアを許可/拒否して、システム全体に影響があるかどうかなどを確認できます。検証後、ドメイン全体にポリシーを配布すると効率的です。

スパイウェア制御はリスクウェアも検出します。リスクウェアは直接被害を与えないが、設定によって危険性のあるプログラムです。代表的なリスクウェアに、IRC などのチャット アプリケーションや ファイル転送 ソフトウェアがあります。 これらのプログラムをドメインで使用したい場合、スパイウェアと同じようにテスト環境でまず動作を検証することを推奨します。検証後、「ホストから報告されているスパイウェアとリスクウェア」テーブルでルールを確認および設定して、リスクウェアの使用を許可します。

1. 検証用のドメインを作成して、スパイウェア スキャンを有効にする
   a) 通常使用するプログラムをインストールした複数のコンピュータを用意して、テスト環境を作ります。
   b) これらのコンピュータをホストとして管理ドメインにインポートします。
   c) 「設定」タブに移動して、「リアルタイム スキャン」ページを開きます。
   d) [リアルタイム スキャンを有効にする] が有効になっていることを確認します。
      また、ホストに対してスパイウェアのマニュアル スキャンを実行することもできます。
   e) をクリックするとポリシーの保存と配布を行います。
2. スパイウェアとリスクウェアを確認する
   「ホストから報告されているスパイウェアとリスクウェア」テーブルでは、スキャン中に検出したスパイウェアとリスクウェアが表示されます。このテーブルは「スパイウェア制御」ページで表示されます。
   a) 報告されているスパイウェアとリスクウェアを確認します。
   b) ネットワークで使用する必要があるスパイウェアまたはリスクウェアがある場合、それらを選択して、[アプリケーションを除外] をクリックします。

確認のダイアログが表示されます。

c) 問題がない場合、[**OK**] をクリックして、スパイウェア/リスクウェアを許可します。
指定のスパイウェア/リスクウェアが「スパイウェア スキャンで対象外のアプリケーション」テーブルに表示されるようになります。

3. エンドユーザがスパイウェア/リスクウェアをホストで実行できないようにするには、[ユーザにスパイウェアの使用を許可する] のオプションを [許可しない] に設定します。
4. マニュアル スキャンの設定がドメインで有効かどうかを確認します。
5. をクリックするとポリシーの保存と配布を行います。

スパイウェア スキャンをドメイン全体に実行する

この例では、スパイウェアのマニュアル スキャンをドメイン全体に実行します。

この操作によって、「ホストから報告されているスパイウェアとリスクウェア」テーブルの項目が一部消去されます。

1. 「ポリシー ドメイン」タブで [ルート] を選択します。
2. ウイルスのマニュアル スキャンの設定を「ウイルスのマニュアル スキャン」ページで確認して、必要に応じて設定を変更してください。
3. 「操作」タブに移動して、[ウイルスとスパイウェア スキャン] ボタンをクリックします。

   注: 操作を開始するには、ポリシーを配布する必要があります。

4. をクリックするとポリシーの保存と配布を行います。

スパイウェア/リスクウェアのコンポーネントを許可する

この例では、スパイウェア スキャンで検出されたスパイウェアまたはリスクウェアのコンポーネントを1つのホストに許可します。

1. 「ポリシー ドメイン」タブで、スパイウェア/ リスクウェアの使用を許可するホストを選択します。
2. 「設定」タブに移動して、「スパイウェア制御」ページを開きます。
3. 「ホストから報告されているスパイウェアとリスクウェア」テーブルから許可するスパイウェアのコンポーネントを選択し、[アプリケーションを除外] をクリックします。
   確認のダイアログが表示されます。
4. ダイアログの内容に問題がない場合、[**OK**]をクリックして、スパイウェア/リスクウェアを許可します。
   選択したスパイウェア/リスクウェアが「スパイウェア スキャンで対象外のアプリケーション」テーブルに移動されます。
5. をクリックするとポリシーの保存と配布を行います。

隔離保存されたオブジェクトを管理する

ホストで隔離保存されたオブジェクトを一元的に管理することができます。

ホストで隔離保存されたオブジェクト (感染したファイル、スパイウェアやリスクウェア) は設定 ➤ 隔離保存ファイルの管理ページで表示されます。ここで、オブジェクトを隔離保存フォルダから解除したり、削除することができます。

注: 隔離保存フォルダに関するオプションは、主にトラブルシューティングに使用することを推奨します。たとえば、業務などで重要なアプリケーションがリスクウェアとして判別された場合、そのアプリケーションを隔離保存フォルダから解除することで使用できるように設定できます。

隔離保存されたオブジェクトを削除する

ホストで隔離保存されたオブジェクト (感染したファイル、スパイウェアやリスクウェア) は隔離保存フォルダから削除することができます。

1. 対象のドメインを選択します。
2. 「設定」タブを開いて、「集中管理」ページを選択します。
3. 「隔離保存されたオブジェクト」テーブルから削除するオブジェクトを選択して、[削除] をクリックします。
   オブジェクトが「隔離保存されたオブジェクトに実行する処理」テーブルに移動され、[処理] に [削除] が指定されます。
4. をクリックするとポリシーの保存と配布を行います。

隔離保存されたオブジェクトを解除する

ホストで隔離保存されたオブジェクト (感染したファイル、スパイウェアやリスクウェア) は隔離保存フォルダから解除することができます。解除したオブジェクトはホスト上で実行できるようになります。

1. 対象のドメインを選択します。
2. オブジェクトに対する除外ルールを作成する

   除外ルールは、同じオブジェクトが再び隔離保存されないようにするために必要です。オブジェクトが感染していると表示される場合、次の手順を実行してください。

   a) 設定 ➤ 隔離保存の管理ページに移動して、対象となるオブジェクトのパスをコピーします。
   b) 設定 ➤ リアルタイム スキャンページを開きます。
   c) [対象外のオブジェクトを有効にする] を右クリックして、[詳細モードで検索] を選択します。
      ユーザインターフェースが詳細モードに変わります。
   d) 「ポリシー」タブで [オブジェクトを除外] を選択します。
   e) [追加] をクリックして、隔離保存されたオブジェクトのパスを入力します。
   f) 表示 ➤ アンチウイルス モード を選択して、インターフェースをアンチウイルス モードに切り替えます。[対象外のオブジェクトを有効にする] が 設定 ➤ リアルタイム スキャンページで有効になっていることを確認します。

   オブジェクトがスパイウェアまたはリスクウェアの場合

   a) 設定 ➤ スパイウェア制御ページに移動します。
   b) 「ホストから報告されているスパイウェアとリスクウェア」テーブルで除外するオブジェクトを選択して、[アプリケーションを除外] をクリックします。

処理を確認するダイアログが表示し、指定のアプリケーションが「スパイウェア スキャンで対象外のアプリケーション」テーブルに移動されます。

3. 「設定」タブを開いて、「隔離保存ファイルの管理」ページを選択します。
4. 「隔離されたオブジェクト」テーブルから許可するオブジェクトを選択して、[解除]をクリックします。オブジェクトが「隔離保存されたオブジェクトに実行する処理」テーブルに移動され、「処理」に「解除」が指定されます。
5. をクリックするとポリシーの保存と配布を行います。

エンドユーザによる設定の変更をブロックする

セキュリティのため、エンドユーザがウイルス保護の設定を変更できないように指定できます。

エンドユーザによる設定の変更をブロックするには

- 特定の設定の横にある鍵型のアイコンをクリックすると、エンドユーザがその設定を変更できないようになります。
- 「設定」タブが表示されている時に [ユーザによる変更を禁止する] をクリックすると、ページ内で鍵型のアイコンが付いている設定がすべて「確定」された状態になり、エンドユーザは設定を変更できないようになります。
- 「設定」タブ -> 「一元集中管理」ウィンドウの順に移動して、[設定の変更をユーザに許可しない] をクリックすると、ウイルス保護およびインターネット防御の全設定をエンドユーザからロックできます。この操作は、詳細モードの全設定も「確定」した状態にします。

ウイルス保護の設定を確定 (ロック) する

この例では、ウイルス保護に関する設定をすべて「確定」します。エンドユーザは確定された設定を変更することはできません。

1. 「ポリシー ドメイン」タブで [ルート] を選択します。
2. 「設定」タブに移動して、「自動更新」ページを開きます。
3. ページの設定に問題がないことを確認します。
4. [ユーザによる変更を禁止する] をクリックします。
   ページの設定がすべて確定されます。
5. 「リアルタイム スキャン」を選択します。
6. ページの設定に問題がないことを確認します。
7. [ユーザによる変更を禁止する] をクリックします。
8. 「マニュアル スキャン」を選択します。
9. ページの設定に問題がないことを確認します。
10. [ユーザによる変更を禁止する] をクリックします。
11. 「メール スキャン」ページを選択します。
12. ページの設定に問題がないことを確認します。
13. [ユーザによる変更を禁止する] をクリックします。
14. をクリックするとポリシーの保存と配布を行います。

警告の転送

ここでは、ウイルスに関する警告のポップアップを無効して、警告をメールで送る方法について説明します。

セキュリティの対策として、ウイルスの警告は管理者にメールで通知されるように設定すると便利です。

ウイルス警告を特定のメール アドレスに送信する

この例では、ホストが生成したセキュリティ警告を指定のメール アドレスに転送するように設定します。

1. 「ポリシー ドメイン」タブで [ルート] を選択します。
2. 「設定」タブに移動して、「警告の送信」ページを開きます。
3. 警告のメール送信を設定する

   警告のメール送信を事前に設定していない場合、次の方法で設定できます。

   a) [メール サーバ アドレス **(SMTP)**] フィールドに SMTP サーバのアドレスを入力します。

      以下の形式を使用してください。

      `<host>[:<port>]` - 「`host`」は SMTP サーバの DNS 名または IP アドレス、「`port`」は SMTP サーバのポート番号です。

   b) [送信者のメール アドレス **(From)**] フィールドに警告の転送先となる送信者のアドレスを入力します。

   c) [メールの件名] フィールドにメールの件名を入力します。

      メッセージの件名で使用できるパラメータについては、MIB のヘルプを参照してください。

4. 警告の転送を設定する

   「警告転送」テーブルを使用して、警告のタイプ別に異なる転送先を設定できます。

   a) [セキュリティ警告] 行の [メール] チェックボックスをオンにします。
      [メールの受信者のアドレス (宛先)] ダイアログ ボックスが開きます。

   b) [すべての製品で同じアドレスを使用する]チェックボックスをオンにして、有効なフィールドにメール アドレスを入力します。

      複数のメール アドレスに警告を送信する場合、アドレスをカンマ区切りで入力します。

   c) 入力が完了したら、[**OK**] をクリックします。

5. をクリックするとポリシーの保存と配布を行います。

警告のポップアップを無効にする

この例では、エンドユーザに対して警告ポップアップを表示しないようにクライアント セキュリティを設定します。

1. 「ポリシー ドメイン」タブで [ルート] を選択します。
2. 「設定」タブに移動して、「警告の送信」ページを開きます。
3. [ローカル ユーザ インターフェース] 列ですべての製品のチェックボックスをオフにします。
4. をクリックするとポリシーの保存と配布を行います。

ネットワーク上のウイルスを監視する

ポリシー マネージャを使用して、ネットワーク上のウイルスや感染を監視することができます。

ネットワークでウイルスの存在を監視する最良の方法は、「概要」タブの「ウイルス保護」ウィンドウを確認することです。新しい感染が表示される場合、[ホストの感染状況を表示] をクリックしてください。「ステータス」タブの「ウイルス保護」ページが表示され、各ホストの感染状況の詳細を確認できます。

また、「警告」タブと「レポート」タブで、ホストからのスキャン レポートを確認することもできます。

アンチウイルス保護を検証する

クライアント セキュリティが正常に機能しているか確認するために専用の検証ファイルを使用できます。このファイルは実際のウイルスではないもの、ウイルスが存在しているかのように検出されます。

このファイルは EICAR Standard Anti-Virus Test ファイルといい、他のアンチウイルス プログラムでも検出されます。EICAR 検証ファイルを使用して、メール スキャンの動作を確認することもできます。EICAR とは、European Institute of Computer Anti-virus Research の略です。EICAR の情報ページは次の URL でご覧になれます。*http://www.europe.f-secure.com/virus-info/eicar_test_file.shtml*

アンチウイルス保護の動作を確認するには

1. 必要な場合、EICAR 検証ファイルを *http://www.europe.f-secure.com/virus-info/eicar_test_file.shtml* からダウンロードできます。

   また、テキスト エディタを使用して、以下の1行を持つファイルを作成することで検証ファイルを用意できます。

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

2. ファイルに適当な名前を .com の拡張子とともに付けて保存します (たとえば EICAR.COM)。

   ファイルは標準の MS-DOS ASCII 形式で保存してください。また、拡張子の3番目の文字は数字の "0" ではなく、アルファベットの大文字の "O" であることに注意してください。

3. クライアント セキュリティが正常に動作している場合、ファイルがウイルスとして検出されるはずです。

   当然のことですが、このファイルは本当のウイルスではありません。ウイルス保護が動作していない状態でファイルを実行すると、EICAR.COM は「EICAR-STANDARD-ANTIVIRUS-TEST-FILE!」というメッセージを表示して終了します。

第
6
章

インターネット防御

トピック：

- *ファイアウォールのセキュリティ レベル*
- *セキュリティ レベルの構成*
- *セキュリティ レベルとルール*
- *ネットワークの隔離保存*
- *インターネット防御の警告*
- *アプリケーション通信制御*
- *警告を確認して、インターネット防御の動作を確認する*
- *侵入防止*

インターネット防御は、インターネットからの不正なアクセスを防ぐだけでなく、LAN 内から発信される攻撃からもコンピュータを保護します。

不正なアクセスを禁止し検出することにより、コンピュータに保存されている重要なデータや個人情報の盗用を防ぐことができます。また、有害なアプリケーションからユーザを保護し、ネットワークの使用を制御したり、大量の帯域幅を使用するアプリケーションを禁止したりすることもできます。

インターネット防御に含まれている「ファイアウォール」は、トラフィック (データの転送) をプロトコルに基づいて制限することができます。「アプリケーション通信制御」は、有害なプログラムがコンピュータに関する情報を送信することを防ぎます。また、アプリケーションの IP アドレスやポートに基づいてトラフィックをさらに制限することもできます。「侵入防止」機能は、ホストの空きポートを標的とした有害なパケットを止めることができます。

インターネット防御には7つのセキュリティ レベルがあらかじめ用意されており、各レベルにはプリセットのファイアウォール ルールが関連付けられています。セキュリティ レベルは、セキュリティ ポリシーやエンドユーザの特徴、ネットワークの場所、ユーザの経験などに基づいて、エンドユーザ/ホスト別に割り当てることができます。

ファイアウォールのセキュリティ レベル

ファイアウォールには、すぐに使用できるプリセットのセキュリティ レベルがいくつか用意されています。

プリセットのセキュリティ レベル	
ネットワーク隔離	ネットワークのアクセスを制限します。ポリシー マネージャ サーバの接続と更新の自動ダウンロードのみが許可されます。ネットワークの隔離保存を有効にするための条件がホストで発生した場合 (パターン ファイルが古い、リアルタイム保護が無効)、このセキュリティ レベルが自動的に有効になります。
すべてブロック	ネットワーク トラフィックをすべてブロックします。
モバイル	メール、Usenet (ネット ニュース)、Web サイト、ファイルの取得 (HTTP、HTTPS、FTP) に関するアクセスを許可します。VPN とSSH などの暗号化プログラムの使用も許可します。他のデータは拒否され、着信 TCP トラフィックが拒否される際には警告を発生します。マルウェアが検出されたら、ローカルのルールを追加できます。
ホーム	発信 TCP トラフィックおよび FTP ファイルの取得を許可します。他のデータは拒否され、着信 TCP トラフィックが拒否される際には警告を発生します。ネットワークの機能を拡張するために、ローカルのルールを追加できます。
オフィス	発信 TCP トラフィックおよび FTP ファイルの取得を許可します。他のデータはデフォルトで拒否され、有害な接続を検出した際には警告を発生します。ネットワークの機能を拡張するために、ローカルのルールを追加できます。
高	Web、メールとニュース トラフィックの発信、暗号化通信、FTP ファイル転送、リモート操作による更新を許可します。他のデータを拒否し、マルウェアやTCP 接続が検出された際には警告を発生します。
標準	すべての発信トラフィックを許可し、特定の着信サービスを拒否します。必要なアプリケーションが正常に機能するために、アプリケーション通信制御を利用してルールを追加することが可能です。
無効	すべてのネットワーク トラフィックを許可し、警告は発生しません。ローカルのルールは作成できません。

セキュリティ レベルの構成

ここではセキュリティ レベルの構成について説明します。

各セキュリティ レベルには、プリセットのファイアウォール ルールが含まれています。また、「ファイアウォールのセキュリティ レベル」テーブルで フィルタリング モード ➤ 標準 と表示されているセキュリティ レベルに対して新しいルールを作成することもできます。「ファイアウォールのセキュリティ レベル」テーブルのルールは上から下の順に読み込まれます。

セキュリティ レベルを作成する際のヒント

- セキュリティ レベルを作成するときには、セキュリティの対策として、必要なサービスのみを許可し、他のサービスをすべて拒否してください。新しいサービスが必要になった場合、ファイアウォール ルールを後から編集して、サービスを追加することが可能です。

反対の概念、すなわち危険なサービスのみを拒否して他のサービスをすべて許可するという概念はお勧めできません。なぜなら、新しいセキュリティの問題が発見されたとき、どのサービスが危険であるとか、またはどのサービスが将来危険になるということは、断言できないからです。

適切なセキュリティ レベルの例

1. 最も危険なサービスやホストに対して拒否ルールを設定し、オプションで警告を発する
2. 頻繁に使用する一般的なサービスやホストに対して許可ルールを設定する
3. トロイの木馬など、警告が必要な特定のサービスに対して拒否ルールを設定し、警告を発する
4. 一般的なサービスなどを許可するルール
5. 上記に該当しないものをすべて拒否する

セキュリティ レベルとルール

ここでは、ユーザのニーズに基づいたセキュリティ レベルの設定について説明します。

この例では、ホストがドメイン構造にインポートされていると仮定しています (ノート コンピュータやデスクトップがそれぞれのサブドメインに存在している)。

特定のセキュリティ レベルをドメインに適用する前に、セキュリティ レベルがドメインに対して適切であるか確認する必要があります。ドメイン別に異なるセキュリティ レベルを適用することも可能です。

重要: 特定のホストのセキュリティ レベルを変更した場合、新しいセキュリティ レベルが間違いなく適用されるように、設定の横にある鍵型のアイコンをクリックしてください。

セキュリティ レベルを選択する

この例では、「Desktops/Eng」サブドメインのホストに対して「オフィス」セキュリティ レベルを有効にします。

次の方法で、「Desktops/Eng」サブドメインのセキュリティ レベルを変更できます。

1. 「ポリシー ドメイン」タブで「**Desktops/Eng**」サブドメインを選択します。
2. 「設定」タブに移動して、「ファイアウォールのセキュリティ レベル」ページを選択します。
   ポリシーに含まれているデフォルトのセキュリティ レベルが、ドロップダウン リストの [ホストでのインターネット防御セキュリティ レベル] に表示されます。
3. [ホストでの インターネット防御セキュリティ レベル] ドロップダウン リストから [オフィス] セキュリティ レベルを選択します。
4. 設定の横にある鍵形のアイコンをクリックすると、エンドユーザが設定を変更できないように設定できます。
5. をクリックするとポリシーの保存と配布を行います。

「ステータス」タブに移動し「全体の保護」ウィンドウで変更したセキュリティ レベルが有効になっていることを確認します。

注: 何らかの理由で指定のセキュリティ レベルを使用できない場合、デフォルトのセキュリティ レベルが代わりに使用されます。デフォルトのセキュリティ レベルは、「ファイアウォールのセキュリティ レベル」ウィンドウの「グローバル セキュリティ レベル」テーブルで確認できます。

ホストのデフォルト セキュリティ レベルを設定する

デフォルトのセキュリティ レベルはドメイン全体に対する設定で、指定のセキュリティレベルが無効の場合にのみ使用されます。

この例では、ドメインの全ホストに対して「オフィス」のセキュリティ レベルがデフォルトとして設定されます。

1. 「ポリシー ドメイン」タブで 「**Laptops/Eng**」ドメインを選択します。
2. 「設定」タブに移動して、「ファイアウォールのセキュリティ レベル」ページを選択します。
3. 「ファイアウォールのセキュリティ レベル」テーブルで、[オフィス] 列の [デフォルト] ラジオ ボタンをクリックします。
   ポリシー マネージャがセキュリティ レベルの変更を確認するメッセージを表示します。
4. [**OK**] をクリックします。

5. をクリックするとポリシーの保存と配布を行います。

特定のドメインにセキュリティ レベルを追加する

この例では、関連するルールを2つ持つ新しいセキュリティ レベルが作成されます。

新しいセキュリティ レベルが□つのサブドメインに追加され、各ホストは新しいセキュリティ レベルを使用することが強制されます。サブドメインにはインターネットの閲覧のみに使用されるコンピュータがあって、それらのコンピュータは会社の LAN には接続されていません。

特定のドメインに新しいセキュリティ レベルを追加するには、まずルート レベルのセキュリティ レベルを無効にする必要があります。その後、セキュリティ レベルを適切なドメイン レベルで有効にします。

セキュリティ レベルを作成する

セキュリティ レベルを追加します。

セキュリティ レベルを追加するには

1. 「ポリシー ドメイン」タブで [ルート] を選択します。
2. 「設定」タブに移動して、「ファイアウォールのセキュリティ レベル」ページを選択します。
3. [追加] をクリックします。
   セキュリティ レベルの名前と説明を入力するウィンドウが開きます。
4. 新しいセキュリティ レベルの名前を指定します (たとえば、「ブラウザ セキュリティ」など)。
   [説明] フィールドにセキュリティ レベルに関する説明を入力します。
5. [完了] をクリックします。
6. をクリックするとポリシーの保存と配布を行います。

セキュリティ レベルに使用するルールを作成する

セキュリティ レベルに使用するルールを作成します。

次の方法で、新しいセキュリティ レベルで使用するルールを作成します。

1. 「ファイアウォール ルール」ページに移動します。
2. 作成した [ブラウザ セキュリティ] セキュリティ レベルを選択します。
   セキュリティ レベルに関連するルールが存在していないので、「ファイアウォール ルール テーブル」は空です。
3. [前に追加] をクリックして、発信 HTTP トラフィックを許可するルールをリスト上の最初のルールとして追加します。
   「ファイアウォール ルール」ウィザードが開きます。
4. 「ファイアウォール ルール」ウィザードで設定を行います。
   a) 「ルールのタイプ」ウィンドウでルールのタイプに [許可] を選択します。
   b) 「リモート ホスト」ウィンドウで [任意のリモート ホスト] を選択して、すべてのインターネット接続にルールを適用します。
   c) 「サービス」ウィンドウにある [サービス] 列で [**HTTP**] を選択して、ルールを HTTP トラフィックに適用します。
   d) 「サービス」ウィンドウにある [方向] 列で [**=>**] を選択して、ルールを発信接続に適用します。
   e) 「詳細設定」ウィンドウでデフォルトの設定を使用します。
   f) 「概要」ウィンドウで新しいルールを確認します。

ルールに関するコメントを追加します (たとえば「Web から発信する HTTP トラフィックを許可するルール」など)。

g) [完了] をクリックします。

5. [後に追加] をクリックして、他のトラフィック (発着信の両方) を拒否するルールをリストの最後のルールとして追加します。
6. 「ファイアウォール ルール」ウィザードで設定を行います。
   a) 「ルールのタイプ」ウィンドウでルールのタイプに [拒否] を選択します。
   b) 「リモート ホスト」ウィンドウで [任意のリモート ホスト] を選択して、すべてのインターネット接続にルールを適用します。
   c) 「サービス」ウィンドウにある [サービス] 列で [すべてのトラフィック] を選択して、ルールをすべてのトラフィックに適用します。
   d) 「サービス」ウィンドウにある [方向] 列で [**<=>**] を選択して、ルールを発着信接続に適用します。
   e) 「詳細設定」ウィンドウでデフォルトの設定を使用します。
   f) 「概要」ウィンドウで新しいルールを確認します。

   ルールに関するコメントを追加します (たとえば、「他のトラフィックを拒否するルール」など)。

   g) [完了] をクリックします。

新しいセキュリティ レベルを適用する

新しいセキュリティ レベルを適用します。

新しいセキュリティ レベルを指定のサブドメインにのみ適用するには、ルート レベルでセキュリティ レベルを無効にし、ポリシー ドメイン階層の低レベルでセキュリティ レベルを有効にする必要があります。

1. 「ポリシー ドメイン」タブで [ルート] を選択します。
2. 「ファイアウォール サービス」ページに移動します。
3. 「ファイアウォールのセキュリティ レベル」テーブルの [有効] チェックボックスをオフにして [ブラウザ セキュリティ] セキュリティ レベルを無効にします。
4. 「ポリシードメイン」タブでセキュリティ レベルを使用するサブドメインを選択します。
5. 「ファイアウォールのセキュリティ レベル」テーブルの [有効]チェックボックスをオンにして [ブラウザ セキュリティ] セキュリティ レベルを有効にします。
6. [ホストでのインターネット防御セキュリティ レベル] ドロップダウン リストから新しいセキュリティ レベルを選択します。
7. をクリックするとポリシーの保存と配布を行います。

ネットワークの隔離保存

「ネットワークの隔離保存」は、ホストのパターン ファイルが古くなっている、および/またはリアルタイム スキャンが無効になっている場合、ホストのネットワーク アクセスを制限する機能です。

ネットワークの隔離保存が行われているホストは、パターン ファイルが更新されたとき、および/またはリアルタイム スキャンが有効にされたときに、ネットワークのアクセスが復元されます。

ここでは、ネットワークの隔離保存の機能と設定について説明します。

ネットワークの隔離保存を設定する

ネットワークの隔離保存に関する設定は「ファイアウォールのセキュリティ レベル」ページで確認できます。

「ネットワークの隔離保存」ページでは、以下の設定を指定できます。

- ネットワークの隔離保存を有効/無効にする
- ネットワークの隔離保存を有効にするために必要なパターン ファイルの発効日からの経過日数を指定する
- ホストでリアルタイム スキャンが無効になったときにネットワークの隔離保存を有効にする

ドメイン全体にネットワークの隔離保存を有効にする

ドメイン全体にネットワーク隔離を有効にするには

1. 「ポリシー ドメイン」タブで [ルート] を選択します。
2. 「設定」タブに移動して、「ファイアウォールのセキュリティ レベル」ページを選択します。
3. [ネットワーク隔離を有効にする] を選択します。
4. [ネットワーク隔離を有効にするために必要なパターン ファイルの経過日数] を指定します。
5. [リアルタイム スキャンが無効な場合、ホスト上でネットワーク隔離を有効にする] を選択すると、リアルタイム スキャンが無効にされた際ににネットワークの隔離保存が有効になります。
6. をクリックするとポリシーの保存と配布を行います。

ネットワークの隔離保存を調整する

ネットワークの隔離保存は、ホストのセキュリティ レベルを [ネットワークの隔離保存] に強制変更することによって有効にできます。[ネットワークの隔離保存] のセキュリティ レベルには制限されているファイアウォール ルールが含まれています。

[ネットワークの隔離保存]のセキュリティ レベルにファイアウォールの許可ルールを追加して、ネットワークのアクセスを必要に応じて許可することが可能です。

インターネット防御の警告

インターネット防御は、特定のマルウェアがコンピュータにアクセスしようとした際に警告を表示することができます。

特定のファイアウォール ルールが適用される際に、または不正なデータグラムが受信される際など、特定の動作が行われるときに警告を発生することが可能です。警告を活用することで、システムで転送されているデータの監視が容易になります。

警告の設定を行う際には、セキュリティ レベルが適切に設定されていることが必要です。一般的には、1つの警告に対して1つのルールを設けると効率的です。複数のルールを対象とした警告を設定することも可能ですが、その場合には大量の警告が生成される可能性が高くなります。警告の数が多くなると、管理と運用の負担もその分増えます。

警告ルールを追加する

この例では、警告を発する [拒否] ルールが特定のサブドメインの着信 ICMP トラフィックに対して作成されます。対象のコンピュータに ping を実行すると警告が表示するようになります。

ルールは、サブドメインにあるコンピュータに ping を行うことで検証します。また、ファイアウォールのルール ウィザードでルールを作成する際に選択できるオプションについても説明します。

ルールのタイプと拒否するサービスを選択する

ルールのタイプを選択して、拒否するサービスを定義します。

次のように実行します。

1. 「ポリシー ドメイン」タブでルールの対象となるサブドメインを選択します。
2. 「設定」タブに移動して、「ファイアウォール ルール」ページを開きます。
3. [編集するインターネット防御セキュリティ レベル] ドロップダウン メニューから、ルールの対象となるセキュリティ レベルを選択します。
   選択したセキュリティ レベルに関連しているルールがテーブルに表示されます。
4. [前に追加] をクリックして、新しいルールをリストの最初のルールに指定します。
   「ファイアウォールのルール」ウィザードが開きます。
5. [拒否] を選択して着信 ICMP 接続を拒否します。
6. 対象のホストを指定する

   ルールをすべての接続に適用するか、特定の接続に適用するか選択します。

   - [任意のリモート ホスト] オプションをオンにして、ルールをすべてのインターネット接続に適用します。
   - [ローカル接続しているネットワーク上のすべてのホスト] をオンにすると、ローカル ネットワークからの全接続に対してルールが適用されます。
   - [指定したリモート ホスト] オプションをオンにして、IP アドレス、IP アドレスの範囲、または DNS アドレスにルールを適用します。このオプションを選択すると、テキスト フィールドにアドレスを指定することができます。複数のアドレスまたはアドレス範囲をフィールドに入力する場合、スペースで区切ります。

   ここでは、[任意のリモート ホスト] を選択します。
7. 拒否するサービスと方向を選択する

ルールの対象となるサービスをリストから選択します。複数のサービスを選択することが可能です。すべてのサービスにルールを適用する場合、リストの最上部にある [すべて] を選択します。

選択したサービスの [方向] 列の矢印をクリックしてルールを適用する方向を選択します。クリックを繰り返すと、方向が変わります。次の表を参照してください。

方向	説明
<=>	サービスを着信/発信の両方向で許可/拒否します。
<=	サービスが定義されたリモートホストやネットワークからコンピュータに着信する場合に、サービスを許可/拒否します。
=>	サービスが定義されたリモートホストやネットワークからコンピュータに発信する場合に、サービスを許可/拒否します。

ここでは次をように選択します。

- [サービス] ドロップダウン リストから [**ICMP**] を選びます。
- [方向] 列から「**<=**」を選択します。

詳細オプションを指定する

ルールの詳細オプションを指定します。

次のように実行します。

1. チェックボックスのオン/オフを選択して、ダイヤルアップ リンクが開かれているときだけルールを適用するかどうか定義します。
   a) チェックボックスのオン/オフを選択して、ダイヤルアップ リンクが開かれているときだけルールを適用するかどうか定義します。
   b) [警告を送信] ドロップダウン リストから警告のタイプを選択します。

      ここでは [セキュリティ警告] を選択します。
   c) [警告トラップ] ドロップダウン リストから発信する警告トラップを選択します。
   d) [警告コメント] に警告に関するコメントを入力します。
   e) 他の設定はデフォルトのままにします。
2. [警告を送信] ドロップダウン リストから警告のタイプを選択します。
3. [警告トラップ] ドロップダウン リストから発信する警告トラップを選択します。

   ここでは [ネットワーク イベント: 着信サービスが拒否されました。] を選択します。
4. [警告コメント] に警告に関するコメントを入力します。

   このコメントはクライアント セキュリティのローカル ユーザ インターフェースに表示されます。
5. 他の設定はデフォルトのままにします。
6. ルールを確認および適用する

   作成したルールを確認します。ルールにコメントを追加すると、「ファイアウォール ルール」テーブルにコメントがルールと一緒に表示されるようになります。ルールを変更する必要があれば、[戻る] をクリックして作成画面に戻れます。
7. ルールの内容に問題がない場合、[完了] をクリックします。
   新しいルールが「ファイアウォール ルール」ページにあるルール リストの一番上に表示されます。

警告の転送を設定する

ルールに警告の転送を設定します。

次のように実行します。

1. 「設定」タブに移動して、「警告を送信」ウィンドウを開きます。
2. 「警告転送」ウィンドウでセキュリティ警告がポリシー マネージャ コンソールに送信されることを確認します。
3. 必要の場合、[ポリシー マネージャ コンソール] 列の [セキュリティ警告] チェックボックスをオンにします。

ルールの適用と検証

ルールを適用および検証します。

次のように実行します。

1. 「ポリシー ドメイン」タブでサブドメインが正しく選択されていることを確認します。
2. 「設定」タブで「ファイアウォールのセキュリティ レベル」ページを開きます。
3. ルールの対象となるセキュリティ レベルを [ホストでのインターネット防御セキュリティ レベル] ドロップダウン リストから選択し、有効なセキュリティ レベルとして設定します。
4. をクリックするとポリシーの保存と配布を行います。
5. ルールの動作を確認する

   サブドメインに管理されているホストをドメイン外部のコンピュータから ping することによって、作成したルールの動作を検証することができます。これを行った後、次のようにルールを確認します。

   a) 「ポリシー ドメイン」タブで作成したルールのサブドメインを選択します。
   b) 「概要」タブに進み、新しいセキュリティ警告がドメインに対して表示されているか確認します。
   c) [重大度別に警告を表示] をクリックすると、警告の詳細を表示できます。
      「警告」タブが開き、セキュリティ警告の詳細リストが表示されます。

アプリケーション通信制御

アプリケーション通信制御は、Web ページのアクセスや有害なプログラムに対する保護を提供します。

トロイの木馬などのマルウェアがネットワークに接続することを拒否できるため、有効なツールであります。

アプリケーション通信制御は、ファイアウォール ルールで定義された制限に加え、さらに具体的な制限をネットワーク トラフィックに対して行うことができます。固定ファイアウォール ルールにより拒否されているトラフィックを許可することはできませんが、許可しているネットワーク トラフィックに対しては、アプリケーション通信制御の設定を適用できます。つまり、トラフィックを許可するファイアウォール ルールを作成し、アプリケーション通信制御でそのルールをさらに制限することが可能です。

集中管理の環境では、アプリケーション通信制御を利用して、ホストが使用できるプログラムを指定できます。これにより、ネットワークのセキュリティ ポリシーに反するプログラムが使用されることを阻止でき、エンドユーザがどのプログラムを実際に使用しているかを監視することも可能になります。

アプリケーション通信制御を使用する場合、必要なアプリケーション、および安全と断定できるアプリケーションのみを許可してください。

アプリケーション通信制御とディープガード

アプリケーションの発信接続を検出したときにユーザに確認のメッセージを表示するように設定されている場合、アプリケーション通信制御はディープガードと通信して、接続の許可/拒否を自動的に確認することができます。この機能を使用することで、ユーザに表示されるポップアップの数を減らすことができます。

例:

1. 「既知のアプリケーションのルール」テーブルで、発信接続を試行しているアプリケーションに対するルールがある場合、アプリケーション通信制御はルールに従ってアプリケーションの接続を許可または拒否します。
2. 「既知のアプリケーションのルール」テーブルで、試行しているアプリケーションに適用できるルールがない場合、アプリケーション通信制御は[クライアントアプリケーションに対するデフォルト処理]で設定されている処理を基にアプリケーションの接続を許可または拒否します。
3. 選択されている処理が[ユーザに確認する]で、[システム制御が許可しているアプリケーションにはプロンプトを表示しない]がオンになっている場合、アプリケーション通信制御はディープガードと通信し、接続を許可または拒否するかを確認します。ディープガードがアプリケーションを安全と判断できる場合、エンドユーザに確認メッセージは表示せず、アプリケーションの接続が許可されます。
4. ディープガードがアプリケーションを認識できない場合、確認メッセージが表示され、ユーザが接続の許可または拒否を選ぶことになります。

アプリケーション通信制御を設定する

ここでは、設定 ➤ アプリケーション通信制御ページの設定について説明します。

「アプリケーション通信制御」ページでは、次の情報が表示されます。

既知のアプリケーションに対する通信ルール	
アプリケーション	実行可能ファイルの名前。

既知のアプリケーションに対する通信ルール	
クライアントとして機能 (発信)	次の処理を指定できます。[拒否]、[許可]、[ユーザが決定]
サーバとして機能 (着信)	次の処理を指定できます。[拒否]、[許可]、[ユーザが決定]
説明	実行可能ファイルの説明。通常はアプリケーション名です。この説明を変更することができます。
メッセージ	ルールの作成時に発生したメッセージ(ない場合もあります)。
発行元	アプリケーションの発行元。
バージョン	実行ファイルのバージョンに関する説明。

不明なアプリケーション

不明なアプリケーションに関して表示される情報は、既知のアプリケーションと同じです。ただし、不明なアプリケーションにはルールや関連メッセージが指定されていません。

[クライアント アプリケーションに対するデフォルトの処理] および [サーバ アプリケーションに対するデフォルトの処理] の各オプションで、アプリケーションがネットワークに接続しようとしたときのデフォルト処理を指定できます。

処理	説明
拒否	アプリケーションがネットワークに接続することを拒否します。
許可	アプリケーションがネットワークに接続することを許可します。
ユーザが決定	アプリケーションがネットワークに接続しようとするたびに、ユーザが処理を決定するためのメッセージを表示します。

発信接続の許可/拒否をエンドユーザの判断に任せたい場合、[ディープガードが許可しているアプリケーションにはプロンプトを表示しない] を選択することによってエンドユーザに表示するポップアップの数を減らすことができます。

アプリケーション通信制御は、Netscape や Microsoft Internet Explorer のようなブラウザにあるプラグインを個別に制限することはできません。プラグインを制限するには、ブラウザ本体を制限する方法しかありませんので、エンドユーザには信頼済みのプラグインのみをインストールするよう勧めてください。

アプリケーション通信制御をはじめて設定する

アプリケーション通信制御をはじめて設定する際には、検証用にいくつかのアプリケーションを許可すると効率的です。

許可するアプリケーションをポリシーに含み、ポリシーをドメイン全体に配布します。

1. 既知のアプリケーションのリストを作成する
   a) 許可するプログラムをインストールした2台のコンピュータを用意します。
   b) コンピュータをドメインにインポートし、管理対象のホストにします。
   c) [新しいアプリケーションの通知を送信] ドロップダウン リストから [レポート] を選択します。新しいアプリケーションが「ホストによってレポートされる不明なアプリケーション」リストに表示されるようになります。
   d) アプリケーションに対して許可ルールを定義します。
   e) 必要なアプリケーションに対して既存のルールがある場合、ルールをドメイン全体のポリシーとして配布することができます。
2. アプリケーション通信制御の基本的な設定を指定します。
   a) 不明なアプリケーションが発信接続を試行した場合のデフォルト処理を [クライアント アプリケーションに対するデフォルトの処理] ドロップダウン リストから選択します。
   b) 不明なアプリケーションが着信接続を試行した場合のデフォルト処理を [サーバアプリケーションに対するデフォルトの処理] ドロップダウン リストから選択します。
   c) [新しい不明なアプリケーションをレポート]チェックボックスをオンにして、新しいアプリケーションを管理者にレポートするようにします。
   この設定により、エンドユーザがどのアプリケーションを起動しようとしているのかを知ることができ、必要に応じてアプリケーションに新しいルールを定義できるようになります。
   d) [不明なアプリケーションにはデフォルト メッセージを表示する]チェックボックスをオンにすると、不明なアプリケーションが着発信の接続を試行した際にデフォルトのメッセージをユーザに表示するようになります。
3. 設定の確認と適用

   次の方法で、アプリケーション通信制御をドメイン全体で有効にできます。
   a) 「ポリシー ドメイン」タブで [ルート] を選択します。
   b) 「設定」タブで「ファイアウォールのセキュリティ レベル」を選択し、[アプリケーション通信制御を有効にする] チェックボックスが選択されていることを確認します。
   c) をクリックして、ポリシーを保存および配布します。

ルート レベルで不明なアプリケーションに対するルール

この例では Internet Explorer 4 の使用を拒否するルールを作成します。

[ホストによってレポートされる不明なアプリケーション] リストに Internet Explorer 4 が含まれていることが仮定されます。

1. ルールの対象となるアプリケーションを選択する
   a) 「設定」タブに移動して、「アプリケーション通信制御」ページを開きます。
   b) 「ホストによってレポートされる不明なアプリケーション」テーブルから「**Internet Explorer 4.01**」を選択します。
   c) [ルールの作成] をクリックして、アプリケーション通信制御のルール ウィザードを開始させます。
2. アプリケーションのルール タイプを選択する
   a) アプリケーションがクライアントとして機能し、発信接続を試行した場合の処理に [拒否] を選択します。
   b) アプリケーションがサーバとして機能し、着信接続を試行した場合の処理に [拒否] を選択します。
3. ユーザに表示するメッセージを選択する
   a) 接続の試行が行われたときユーザにメッセージを表示するか選択します。

[メッセージなし]、[デフォルトのメッセージ]、または [カスタマイズされたメッセージ] のいずれかを選択します。

[デフォルトのメッセージ] を選択した場合、[デフォルトのメッセージを定義] をクリックして定義されているデフォルトのメッセージを確認できます。

b) [カスタマイズされたメッセージ] を選択した場合、カスタムのメッセージをテキストボックスに入力することができます。

例: 「`Internet Explorer 4` を使用することは会社のセキュリティ ポリシーによって禁止されています。他のブラウザを代わりに使用してください。」

4. ルールのタイプを選択する

a) ルールの対象となるドメインとホストを選択します。

アプリケーションに対するルールが選択したホストやドメインにすでにある場合、既存のルールを上書きするか確認されます。

この例では、[ルート] を選択します。

b) ルールを設定したら、[完了] をクリックします。
新しいルールが「既知のアプリケーションのアプリケーション ルール」テーブルに表示されます。「ホストによってレポートされる不明なアプリケーション」テーブルが更新されます。

5. をクリックするとポリシーの保存と配布を行います。

アプリケーション通信制御のルールを変更する

この例では、上記で作成したルールを変更し、「`Engineering/Testing`」というサブドメインで Internet Explorer 4 の使用を検証用に一時的に許可します。

1. 変更するルールを選択する

a) 「設定」タブに移動して、「アプリケーション通信制御」ページを開きます。

b) 「既知のアプリケーションのルール」で編集するルールを選択します。

c) [編集] をクリックしてアプリケーション通信制御のルール ウィザードを開始させます。

2. アプリケーション ルールのタイプを変更する

a) クライアントとして機能しているアプリケーションが発信接続を試行した場合の処理を選択します。

ここでは、「クライアントとして機能 (発信)」で [許可] を選択します。

b) サーバとして機能しているアプリケーションが着信接続を試行した場合の処理を選択します。

3. ユーザに表示するメッセージを選択します。

接続の試行が行われたときユーザにメッセージを表示するかどうかを選択します。

4. 新しいルールの対象を選択する

a) ルールの対象となるドメインまたはホストを選択します。

ここでは、[**Engineering/Testing**] を選択します。

アプリケーションに対するルールが選択したホストやドメインにすでにある場合、既存のルールを上書きするか確認されます。

b) ルールを設定したら、[完了] をクリックします。
変更されたルールは「既知のアプリケーションのアプリケーション ルール」テーブルに表示されます。

5. をクリックするとポリシーの保存と配布を行います。

アプリケーション通信制御のポップアップを有効/無効にする

アプリケーション通信制御のポップアップを有効/無効にするには

1. 「ポリシー ドメイン」タブで [ルート] を選択します。
2. 「設定」タブに移動して、「アプリケーション通信制御」ページを開きます。

   次の設定を行います。

   - [サーバ アプリケーションに対するデフォルト処理] ドロップダウン リストから [許可] を選びます。
   - [クライアント アプリケーションに対するデフォルト処理] ドロップダウン リストから [許可] を選びます。

3. 「アプリケーション通信制御のルール」ウィザードを使用して、アプリケーション通信制御のルールを作成する場合

   - 「アプリケーション ルール タイプ」ウィンドウで、着発信接続が試行された場合の処理に [許可] または [拒否] を指定します。
   - 「ユーザに表示するメッセージウィンドウの [メッセージなし] を指定します。

4. をクリックするとポリシーの保存と配布を行います。

警告を確認して、インターネット防御の動作を確認する

通常の使用では、インターネット防御から警告が発生することはありません。警告が多く発生する場合、設定に問題があるかもしれません。

原則として、各警告にルールを□つ設定すると効率的です。複数のルールを対象とする警告を設計すると、無用の警告が大量に発生される可能性があるため、重要な情報を見落としてしまう可能性もあります。

インターネット防御の動作を検証するために特定のルールを作成できます。この例では、ping の使用を許可するルールを作成します。ルールに警告のオプションを含むことで、警告の動作を検証することも可能です。

1. 「設定」タブに移動して、「ファイアウォール ルール」ページを選択します。
2. 検証用に使用するセキュリティ レベルを選択します。
3. [前に追加] をクリックします。
   「ファイアウォールのルール ウィザード」が開始します。
4. 「ルールのタイプ」ウィンドウで [許可] を選択します。
5. 「リモート ホスト」ウィンドウで [任意のリモート ホスト] を選択します。
6. 「サービス」ウィンドウで、 [サービス] ドロップダウン リストから [**Ping**] を選択し、[方向] ドロップダウン リストから [両方] を選択します。
7. 「詳細オプション」ウィンドウから、次のオプションを選択します。
   - [警告を送信] ドロップダウン リストから [セキュリティ警告] を選択します。
   - [警告トラップ] ドロップダウン リストから [ネットワーク イベント: 危険性があるサービスが許可されました] を選択します。
   - [警告コメント] フィールドに警告に関するコメントを入力します。
8. 「概要」ウィンドウでルールを確認して、ルールに関するコメントを入力します。
9. をクリックするとポリシーの保存と配布を行います。
10. ルールを検証します。管理ホストに ping コマンドを送信し、「警告」タブに警告が表示されるか確認します。

侵入防止

侵入防止機能は、着信トラフィックを監視することでシステムに対する不審な侵入や処理を検出します。

また、LAN やコンピュータを攻撃するウイルスを監視するためにも使用できます。侵入防止は、ペイロード (転送されてデータの内容) と IP パケットのヘッダ情報を分析し、情報を既知の攻撃パターンと比較します。情報が既知の攻撃パターンと類似しているか同類である場合、侵入防止機能によって警告が発生し、指定の処理が行われます。

侵入防止を設定する

侵入防止の設定は[ファイアウォールのセキュリティ レベル」ページの「侵入防止」ウィンドウで確認できます。

- 侵入防止を有効にする

  侵入防止を有効にすると、侵入を検出するために着信トラフィックが監視されます。無効にすると、侵入防止はトラフィックを監視しません。

- 有害なパケットの処理

  設定できるオプション

  - [記録してパケットを削除] - パケットのヘッダ情報 (IP、ポート、プロトコル) を警告ログに記録し、パケットをブロックします。
  - [パケットを削除せずに記録] - パケット ヘッダ情報 (IP、ポート、プロトコル) を警告ログに記録し、パケットを許可します。

- 警告の重大度

  使用できるオプション [警告なし]、[情報]、[警告]、[セキュリティ警告] 侵入試行は、管理者またはローカル ユーザへのメッセージを表示する方法に応じて、異なる重大度を使用するように設定できます。

- 検出精度

  このオプションは、発生する警告の数とローカル コンピュータのパフォーマンスを影響します。小さい数値を指定すると、誤検出の数が低くなります。

  - 10 = ネットワーク パフォーマンスを最大にして、警告の数を最小限にします。
  - 50 = 侵入防止パターンの最も重要で悪質なものを検証し、一致した場合に警告を送信します。
  - 100 = 侵入防止のパターンをすべて検証し、一致した場合に警告を送信します。
  - 数値が小さいほど、検証されるパターンの数が少なくなります。
  - ホーム ユーザには100%が推奨値です。
  - ホスト (デスクトップ) ユーザには25%が推奨値です。

誤検出について

「誤検出」は、特定のイベントが発生したことを誤って示す警告のことを指します。「インターネット防御」で表示される警告は、通常「おそらく」または「可能性がある」といった表現で誤検出の可能性を示します。

デスクトップとノート コンピュータ に IPS を設定する

この例では、2つのサブドメインにあるデスクトップとノート コンピュータに対して IPS (侵入防止) を有効にします。

デスクトップとノート コンピュータはそれぞれ異なるサブドメイン (「Desktops/Eng」と「Laptops/Eng」) に割り当てられていると仮定します。デスクトップは会社のファイアウォールで保護されているため、警告の発生頻度は低く設定されます。ノート コンピュータは定期的にセキュリティが保護されていないリモートのネットワークなどに接続するため、警告の発生頻度は高く設定されます。

1. デスクトップに IPS を設定する
   a) 「ポリシー ドメイン」タブで「**Desktops/Eng**」サブドメインを選択します。
   b) 「設定」タブに移動して、「ファイアウォールのセキュリティ レベル」ページを選択します。
   c) [侵入防止を有効にする] チェックボックスをオンにします。
   d) [有害なパケットへの処理] ドロップダウン リストから [パケットを削除せずに記録] を選択します。
   e) [警告の重大度] ドロップダウン リストから [警告] を選択します。
   f) [検出精度] ドロップダウン リストから [**25%**] を選択します。
2. ノート コンピュータに IPS を設定する
   a) 「ポリシー ドメイン」タブで「**Laptops/Eng**」サブドメインを選択します。
   b) 「設定」タブに移動して、「ファイアウォールのセキュリティ レベル」ページを選択します。
   c) [侵入防止を有効にする] チェックボックスをオンにします。
   d) [有害なパケットへの処理] ドロップダウン リストから [パケットを削除せずに記録] を選択します。
   e) [一元集中管理された警告の重大度] ドロップダウン リストから [警告] を選択します。
   f) [警告およびパフォーマンス レベル] ドロップダウン リストから [**100%**] を選択します。
3. をクリックするとポリシーの保存と配布を行います。

第
7
章

ネットワークを保護する

トピック：

- *ホストが最新のポリシーを使用しているか確認する*
- *サーバが最新のパターン ファイルを使用しているか確認する*
- *ホストが最新のパターン ファイルを使用しているか確認する*
- *ホストの接続状態を確認する*
- *スキャン レポートを表示する*
- *警告を表示する*
- *週次感染レポートを作成する*
- *ネットワーク攻撃の兆候を監視する*

ここで紹介するタスクは、ネットワークのセキュリティを監視および管理するために定期的に行うと効率的です。

ホストが最新のポリシーを使用しているか確認する

管理対象のホストが最新のポリシーを使用しているかを確認するには

1. 「ポリシー ドメイン」タブで [ルート] を選択します。
2. 「概要」タブを選択し、最新のポリシーを使用しているホストの数を確認します。
3. すべてのホストが最新のポリシーを使用していない場合、[ホストの最新のポリシー更新を表示] をクリックします。
   「ステータス」タブの「集中管理」ページが表示されます。
4. 「集中管理」ページで、最新のポリシーを使用していないホストを確認できます。

   また、最新ポリシー ファイルが使用されていない理由も確認できます (ホストが切断されている、ホストに重大なエラーが発生したなど)。

サーバが最新のパターン ファイルを使用しているか確認する

サーバが最新のパターン ファイルを使用しているかを確認するには

1. 「ポリシー ドメイン」タブで [ルート] を選択します。
2. 「概要」タブを開き、サーバのパターン ファイルが最新であることを確認します。

ホストが最新のパターン ファイルを使用しているか確認する

ホストが最新のパターン ファイルを使用しているかを確認するには

1. 「ポリシー ドメイン」タブで [ルート] を選択します。
2. 「概要」タブを選択し、「パターン ファイル」 の横にある「ワークステーションのウイルス保護」ウィンドウに表示されている情報を確認します。
3. ホストのパターン ファイルが古い場合、次の2つの方法でパターン ファイルを更新できます。
   - 「全体の保護」ページの「ステータス」タブを選択して、最新のパターンファイルを使用していないホストを確認します。該当するホストが検出された場合、「ポリシードメイン」タブで対象のホストを選択して、「操作」タブにある [パターンファイルの更新] ボタンをクリックすることで、パターン ファイルの更新を実行できます。
   - [パターン ファイルの更新] をクリックし、「操作」タブを表示させます。 「操作」タブが表示されたら、[パターン ファイルの更新] ボタンをクリックします。 対象のホストに対して、最新のパターン ファイルが適用されます。

ホストの接続状態を確認する

ホストの接続状態を確認するには

1. 「ポリシー ドメイン」タブで [ルート] を選択します。
2. 「概要」タブを選択し、[切断されたホスト] の横にある「ドメイン」ウィンドウに表示されている情報を確認します。
3. 切断されたホストが存在する場合、[切断されたホストを表示] をクリックします。
   「ステータス」タブの「集中管理」ページが表示されます。
4. 切断されているホスト、および考えられる理由を確認します。

   注: ホストを切断されているとみなすまでの時間を指定できます。ツール ➤ 共通設定 メニューからを選択し、「通信」タブを開きます。「ホストの接続ステータス」でホストの接続時間を確認できます。

スキャン レポートを表示する

ホストからのスキャン レポートを確認できます。

特定のホストからのスキャンレポートを確認するには

1. 「ポリシー ドメイン」タブで [ルート] を選択します。
2. 「レポート」タブを選択します。
   選択したホストのスキャン情報が [レポート] テーブルに表示されます。
3. テーブルの行をクリックして、1つのホストを選択します。
   ウィンドウ下部に、ホストに関連するスキャン レポートが表示されます。

警告を表示する

プログラムや操作に問題がある場合、ホストは警告とレポートを送信できます。

警告の確認と削除を定期的に行うことを推奨します。

警告を受信すると、ボタンが表示します。警告を表示するには

1. をクリックします。
   または、「概要]タブの [] をクリックして、
   「警告」タブが開きます。受信した警告が次のように表示されます。

確認	警告を確認したことを示します。[確認] をクリックすると警告を確認したことになります。すべての警告を確認すると、ボタンが淡色に変わります。		
重大度	問題の重大度。以下のアイコンで重大度を示します。		
		情報	ホストからの通常の操作情報
		警告	ホストからの警告
		エラー	ホスト上の回復可能なエラー
		重大なエラー	ホスト上の回復不能なエラー
		セキュリティ警告	ホスト上のセキュリティ危険要因
日付/時間	警告が発生した日付と時刻		
説明	警告の説明		
ホスト/ユーザ	ホストまたはユーザの名前。		
製品	警告を送信したF-Secure製品		

   リストから警告を選択すると、テーブルの下に警告の詳細が表示されます。

2. [確認] をクリックすると、指定の警告を確認済みにできます。
3. 「概要」タブに表示される警告の情報は自動的に更新されません。[警告概要の再表示] をクリックして、情報を更新できます。

週次感染レポートを作成する

週次感染レポート (またはその他の定期レポート) を作成するために次の2つのオプションが用意されています。

- Web レポート - Web ベースのツールで、クライアント セキュリティの警告およびステータス情報からグラフィカルなレポートを作成できます。

ネットワーク攻撃の兆候を監視する

ローカル ネットワークがネットワーク攻撃を受けていると思われる場合、次の方法でネットワークを監視できます。

1. 「ポリシー ドメイン」タブで [ルート] を選択します。
2. 「概要タブを開きます。
3. [最も頻度の高い最新の攻撃] の横に表示されている情報を確認します。
4. 攻撃が行われた場合、[インターネット防御のステータスを表示] をクリックして、さらに詳しい情報を参照できます。
   「ステータス」タブの「インターネット防御」ページが表示され、ホストにおける最新および最近の攻撃に関する詳細な情報を確認できます。

第

8

章

ソフトウェアのアップグレード

トピック：

- *インストール エディタを使用する*

インストール エディタを使用して、ホストにインストールされている F-Secure アンチウイルス ソフトウェアをリモートからアップグレードできます。インストール エディタは、指定ドメインのホストが実行するポリシーベースのインストール タスクを作成します。

注: 他のインストール方法を通じて、クライアント セキュリティをアップグレードすることも可能です。

インストール エディタを使用する

インストールエディタは、管理エージェントがインストールされているホストで使用する必要があります。

インストール エディタを使用するには

1. 「ポリシー」タブのルート ノード (**F-Secure** サブツリー) を選択します。
   または、「インストール」タブを開きます。
   インストール エディタが開きます。
2. インストール エディタで、対象のホスト/ポリシードメインにインストールする製品を指定します。
   対象のポリシードメイン/ホストについて、次の情報が表示されます。

製品名	ホストまたはドメインにインストールされている製品の名前。またはインストールパッケージを使用してインストールできる製品の名前。
インストール済みのバージョン	製品のバージョン番号。複数のバージョンがインストールされている場合、それぞれのバージョン番号が表示されます。ホストの場合、バージョン番号は1つになります。
インストールするバージョン	インストール パッケージのバージョン番号。
インストール中のバージョン	ホストまたはドメインにインストール中のバージョン。
進行状況	インストールの進行状況。[進行状況] フィールドに表示される情報はホストとドメインによって異なります。

- ホストを選択している場合、[進行状況] フィールドに次のいずれかのメッセージが表示されます。

進行状況	インストールが開始 (ポリシーデータに追加) されたことを示します。インストールが成功したことはホストから報告されていません。`
失敗	インストールまたはアンインストールが失敗したことを示します。[進行状況] フィールドのボタンをクリックして詳細なステータス情報を確認できます。
完了	インストールまたはアンインストールが成功したことを示します。インストールエディタを終了すると、このメッセージは以後表示されません。
(フィールドに何も表示されていない場合)	実行中の操作がないことを示します。[インストール済みのバージョン] フィールドにインストールされている製品のバージョンが表示されます。

- ドメインを選択した場合、[進行状況] フィールドに次のいずれかのメッセージが表示されます。

残りのホスト: **<数>** - 失敗したインストールの数: **<number>**	<数>のインストールが失敗したこと、またはインストールが完了されていないことを示します。[進行状況] フィールドのボタンをクリックして、詳細なステータス情報を確認できます。

完了	全ホストでインストールまたはアンインストールが成功したことを示します。
(フィールドに何も表示されていない場合)	実行中の操作がないことを示します。[インストール済みのバージョン] フィールドにインストールされている製品のバージョンが表示されます。

3. 必要なバージョン番号をすべて選択したら、[開始] をクリックします。
   インストール エディタがインストール ウィザードを起動します。ウィザードにしたがって、インストールのパラメータを指定します。次にインストール エディタは、カスタマイズしたインストール パッケージを用意します。新しいパッケージは、ポリシー マネージャ サーバに保存されます。

   注: [開始] ボタンは、[インストールするバージョン] フィールドで選択した製品のインストールを開始します。[開始] ボタンをクリックせずにインストール エディタを終了すると、変更はすべて破棄されます。

4. インストールにポリシーが使用されるため、新しいポリシーファイルを配布する必要があります。

   ポリシー ファイルには、ホストがインストール パッケージを取り出し、インストールを実行するためのエントリが追加されます。

   インストールは完了するまで時間がかかることがあります。対象のホストがネットワークに接続していない場合、または実行中のインストール操作で、インストールが完了する前にユーザがホストを再起動するよう要求した場合、特に時間がかかる可能性があります。ホストがネットワークに接続され、ポリシー ファイルを正常に送受信しているにもかかわらず時間がかかる場合、問題が発生している可能性があります。または、ホストの方でインストール操作が正常に認識されていない可能性があります。いずれの場合も、[すべて停止] をクリックすることでポリシーのインストール操作を削除できます。インストール操作を削除した場合、対象のポリシー ドメイン/ホストに対して定義したインストール操作がキャンセルされます。確認ダイアログで [サブドメインおよびホストのインストールを再帰的にキャンセル] オプションを選択すると、対象のドメインとそのサブドメインに対するインストール タスクもすべて停止できます。

   [すべて停止] ボタンは、対象のホスト/ドメインにインストール操作が定義されている場合にのみ利用可能です。サブドメインの操作は、ボタンの使用状態に影響しません。[すべて停止] ボタンをクリックすると、ポリシーから操作が削除されますが、ポリシーそのものは削除されません。ホストがすでに前のポリシーファイルをポーリングしている場合、インストール操作がインストール エディタに表示されていなくても、インストール操作が試行される可能性があります。

リモート アンインストール

アンインストールは、更新と同じように簡単に実行できます。製品のアンインストールに必要なソフトウェアしか含まれていない配布パッケージが作成されます。リモート アンインストールをサポートしていない製品には、アンインストールのオプションがインストール エディタで表示されません。

[再インストール] を選択すると、すでにインストールされているバージョンを再インストールします。このオプションは、問題を解決する場合にのみ使用してください。通常、製品を再インストールする必要はありません。

管理エージェントをアンインストールすると、管理エージェントが削除され、情報を送信することができないため、アンインストールが正常に完了したことを知らせる統計情報は送信されません。

1. F-Secureアンチウイルスをアンインストールする
2. アンインストールが成功したかポリシー マネージャ コンソールから報告されるまで待ちます。
3. F-Secureアンチウイルスが正常にアンインストールされた場合、管理エージェントをアンインストールします。

4. 管理エージェントのアンインストールが失敗した場合、ポリシー マネージャ コンソールはアンインストールが失敗したことを示す統計レポートを表示します。正常なアンインストールは報告されませんが、通信が切断されるため明らかになり、管理エージェントの最終レポートは「進行中」と表示します。

第
9
章

ホストの操作

トピック：

- *マニュアル スキャン*
- *スケジュール スキャン*
- *ファイアウォールの警告とログファイルの保存先*
- *ポリシー マネージャに接続してポリシー ファイルをインポートする*
- *ダウンロードと更新を停止する*
- *F-Secureのアンロードをユーザに許可する*

ホストがウイルスに感染している疑いがあったり、特定のタスクをホスト上で行う必要があったりなど、セキュリティや環境に応じてホスト上で処理を実行しなくてはいけないときもあります。

マニュアル スキャン

コンピュータにマルウェアが侵入している疑いがある場合など、必要に応じて手動でコンピュータにスキャンを実行できます。

マニュアルスキャンを実行する

コンピュータ全体、あるいは特定のドライブやフォルダをスキャンできます。また、特定のマルウェアをスキャンすることも可能です。

特定のマルウェアに感染している疑いがある場合、コンピュータがそのマルウェアに感染しているか確認できます。コンピュータ上の特定の場所 (フォルダ・ドライブなど) に感染の疑いがある場合、その場所のみスキャンすることが可能です。このような特定のファイルや場所に対するマニュアル スキャンは、コンピュータ全体を対象とするスキャンと比べ、短時間で完了します。

マニュアル スキャンを開始するには

1. ユーザ インターフェースで、[スキャン] の下にある矢印をクリックします。
   スキャンのオプションが表示されます。
2. サーバ保護 ➤ マニュアル スキャン の順にクリックします。
3. スキャンの種類を選択します。
   スキャンの設定を変更する場合、[スキャンの設定を変更] を選択します。
4. 「新規スキャン」でスキャンのタイプを選択します。
   スキャンの設定を変更する場合、[変更] をクリックします。
5. [スキャンするオブジェクトを指定] を選択した場合、設定を指定できる別のウィンドウが開きます。
   [スキャン ウィザード] が開きます。
6. [スキャンするオブジェクトを指定] を選択した場合、[選択...] をクリックしてください。
   スキャンのオプションを指定するウィンドウが開きます。
7. [開始] をクリックして、スキャンを開始します。
   マルウェアが検出されなかった場合、ステータスが「完了」と表示されます。マルウェアが検出された場合、スキャン ウィザードが開きます。

👉 **注:** システム トレイの製品アイコンを右クリックして、スキャンを手動で開始することも可能です。

スキャンの種類

コンピュータ全体か特定の場所をスキャン対象としたり、特定のマルウェアをスキャンしたりすることができます。

スキャンの種類

スキャンの種類	スキャンの対象	用途
完全スキャン	コンピュータ全体 (内蔵型および外付けハード ドライブすべて) に対してウイルス、スパイウェア、リスクウェアをスキャンします	コンピュータにマルウェアやリスクウェアが一切存在しないことを確認したい場合最長マルウェアとハード ドライブ スキャンを統合します。また、ルートキットによって隠されているアイテムもチェックします。

スキャンの種類	スキャンの対象	用途
スキャンするオブジェクトを指定...	特定のファイル、フォルダ、またはドライブに対してウイルス、スパイウェア、リスクウェアをスキャンします	コンピュータ上の特定の場所にマルウェアの存在が疑われる場合。たとえば、その場所で不審な活動が見られる場合や、ピア ツー ピア ファイル共有ネットワークなどの有害の可能性のあるソースからダウンロードしたファイルがある場合など。スキャン時間は対象のファイル サイズによります。たとえば、数ファイルしかないフォルダを対象にした場合、スキャンは早く終わります。
ハードディスクをスキャン	コンピュータ内蔵の全ハードドライブに対してウイルス、スパイウェア、リスクウェアをスキャンします	コンピュータのハード ディスクをすべてスキャンします。クイック マルウェア スキャンと違って、ハード ディスク全フォルダがスキャンされます。このスキャンは完了するまで時間がかかるため、通常は推奨しません。クイック マルウェア スキャンでマルウェアが検出されず、コンピュータ全体にマルウェアが潜んでいないことを確認したい場合に適切です。
ハードディスクをスキャン	コンピュータ内蔵の全ハードドライブに対してウイルス、スパイウェア、リスクウェアをスキャンします	コンピュータのハード ディスクをすべてスキャンします。クイック マルウェア スキャンと違って、ハード ディスク全フォルダがスキャンされます。このスキャンは完了するまで時間がかかるため、通常は推奨しません。クイック マルウェア スキャンでマルウェアが検出されず、コンピュータ全体にマルウェアが潜んでいないことを確認したい場合に適切です。
ウイルスとスパイウェア スキャン	コンピュータの一部に対してウイルス、スパイウェア、リスクウェアをスキャンします	完全スキャンより短時間で完了します。インストールされているプログラム ファイルなどが主に格納されているフォルダにのみスキャンを実行します。このスキャンは、コンピュータの安全性をすぐに確認したい場合に適切です。
ルートキットをスキャン	セキュリティ問題を示す可能性があるような、システムの重要な場所に隠れているファイル、フォルダ、ドライブ、プロセスをスキャンします。	ルートキットがコンピュータに潜んでいる疑いがある場合。たとえば、マルウェアが最近検出された場合などにマルウェアがルートキットをインストールしなかったことを確認したい場合に適切です。

マルウェアを自動的に駆除する

スキャン中にマルウェアが検出された場合、自動駆除または処理を手動で選択できます。

1. 次のいずれかを選択します。

オプション	説明
自動 (推奨)	プログラムが各マルウェアに対して実行する処理を自動的に判別して、コンピュータを安全な状態にします。
アイテムごとに決定	各マルウェアに対して実行する処理をユーザに確認します。

2. [次へ] をクリックします。

- [自動 (推奨)] を選択した場合、処理の結果を示すウィンドウが開きます。

注: ステータスが「未処理」と表示されるマルウェアはファイルが圧縮ファイル (ZIP ファイルなど) である可能性があります。圧縮ファイル内の感染ファイルは、手動で開いて削除することができます。また、圧縮ファイルを必要としない場合、圧縮ファイルそのものを削除することで感染を取り除けます。

- [アイテムごとに決定] を選択した場合、各マルウェアに対する処理を指定する必要があります。

3. [完了] をクリックして、スキャン ウィザードを閉じます。

マニュアルスキャンを実行する

スキャンが完了したら、スキャンしたファイルのレポートを確認できます。

注: レポートからスキャン時に選択した処理が正しく実行されたか確認できます。たとえば、感染したファイルの駆除を指定してウイルスの取り除きが失敗した場合、ファイルに対して別の処理が適用された可能性もあります。

レポートを表示するには

1. [レポートを表示] をクリックします。
   レポートには、次の情報が含まれます。
   - 検出されたマルウェアの数。
   - 検出されたマルウェアの種類とマルウェアの詳細リンク
   - マルウェアの各アイテムに適用された処理
   - スキャンから除外されたアイテム
   - マルウェアのスキャンに利用されたスキャン エンジン。

   注: 圧縮ファイルの内部がスキャン対象になっていると、スキャンされるファイルの数は多くなります。圧縮ファイルを以前スキャンした場合、スキャン結果はキャッシュ メモリに保存されている可能性があります。

2. [完了] をクリックして、スキャン ウィザードを閉じます。
3. サーバ保護 ➤ マニュアル スキャン の順にクリックし、「ステータス」タブをクリックします。
4. 「タスク」で [スキャン レポートを表示] をクリックします。

   注: 集中管理モードの場合、スキャン レポートはエフセキュア ポリシー マネージャに送られます。また、エフセキュア ポリシー マネージャ コンソールでスキャン レポートを確認することも可能です。

ヒント: 設定 ➤ コンピュータ ➤ マニュアル スキャン ➤ 前回のスキャン レポートを表示 の順にクリックすると、最後に行ったスキャンのレポートを確認できます。

スケジュール スキャン

スケジュール スキャンでは、コンピュータにマルウェアがないかどうか定期的に (日単位、週単位、月単位など) スキャンします。

マルウェアのスキャンには大量のリソースが使用されます。コンピュータのすべてのリソースを使用し、完了にはしばらく時間がかかります。そのため、スキャンをコンピュータの非使用時に実行されるように設定すると効率的です。

スケジュール スキャンを設定する

スケジュール スキャンを利用すると、指定の時間でコンピュータにスキャンを自動で実行できるようになります。

スケジュール スキャンを設定するには

1. ユーザ インターフェースで [設定] をクリックします。
2. コンピュータ ➤ スケジュール スキャン をクリックします。
3. サーバ保護 ➤ スケジュール スキャン の順にクリックします。
4. [スケジュール スキャン スキャンを有効にする] を選択します。
5. ウイルスとスパイウェアのスケジュール スキャンを実行する頻度を選択します。

オプション	説明
日単位	スキャンを毎日実行します。
週単位	スキャンを指定した曜日に実行します。右側のリストからスキャンを実行する曜日を選択します。
月単位	スキャンを毎月の指定した日 (月3回まで指定可能) に実行します。スキャンを実行する日を選択します。 1. [日] オプションを1つ選択します。 2. リストから日付を選択します。 3. 別の日にもスキャンを実行するには、同じ操作を繰り返します。

6. スキャンを実行する時間を指定します。

オプション	説明
開始時刻	スキャンを開始する時刻。コンピュータを使用する予定のない時刻を選択してください。
指定アイドル時間が経過した場合	コンピュータを触っていない時間がここで指定した時間に到達すると、スキャンが自動的に開始します。

7. [適用] をクリックします。

スケジュール スキャンをキャンセルする

スケジュール スキャンは実行中にいつでもローカルでキャンセルすることができます。一度キャンセルしたスケジュール スキャンは次に設定した実行時間になるまで実行されないようになります。

注: Web コンソールからスケジュール スキャンをキャンセルすることはできません。

スケジュール スキャンはコンピュータの動作を遅くする可能性があります。次の方法でスキャンをキャンセルすることができます。

注: 集中管理モードでは、スケジュール スキャンをキャンセルできないことがあります。

1. [ウイルスとスパイウェア スキャン]の通知にある「スケジュール スキャンを開始しました」リンクをクリックします。

   通知が15秒ほど画面に残ります。通知内のリンクをクリックしない場合、スケジュール スキャンをキャンセルできなくなります。

2. 「ウイルスとスパイウェア スキャン」ウィンドウで [キャンセル] をクリックします。
3. 「閉じる] を選択します。

スケジュール スキャンがキャンセルされます。他のスケジュール スキャンを設定している場合、それらは通常通り開始します。

スケジュール スキャンのレポートを表示する

スケジュール スキャンが完了するときに、マルウェアが検出されたか確認できます。

スケジュール スキャンのレポートを確認するには

1. 「スケジュール スキャンが終了しました」タブで、[ウイルスとスパイウェア スキャン]をクリックします。
2. [レポートを表示] をクリックして、スキャンのレポートを確認します。

   注: ダイアログを 「通知履歴」ウィンドウから開いた場合、[レポートを表示] ボタンは無効になります。過去のスケジュール スキャンのレポートは表示できません。

3. [閉じる] をクリックして、ウィンドウを閉じます。

ヒント: 設定 ➤ コンピュータ ➤ [スケジュール スキャン ➤ 前回のスキャン レポートを表示 の順にクリックすると、最後に行ったスキャンのレポートを確認できます。

ヒント: サーバ保護 ➤ スケジュール スキャン ➤ 前回のスキャン レポートを表示 の順にクリックすると、最後に行ったスキャンのレポートを確認できます。

注: 集中管理モードの場合、スキャン レポートはエフセキュア ポリシー マネージャに送られます。また、エフセキュア ポリシー マネージャ コンソールでスキャン レポートを確認することも可能です。

ファイアウォールの警告とログ ファイルの保存先

ファイアウォールの警告とログ ファイルを確認することで、コンピュータのネットワーク接続がどのように保護されているか確認できます。

ファイアウォールの警告を表示する

本製品が発生したファイアウォールの警告を確認できます。

リストにはファイアウォールと侵入防止機能によって発生された警告が含まれます。

リストを表示するには

1. ユーザ インターフェースで [設定] をクリックします。
2. ネットワーク ➤ ファイアウォール の順に選択します。
3. 「ルール」タブをクリックします。
4. [警告ログを表示] をクリックします。
   「ファイアウォールの警告」ウィンドウは次の情報を表示します。

フィールド	説明
時刻	警告が発生した時間を示します。
リモート アドレス	トラフィックを着信/発信したコンピュータの *IP アドレス*を示します。
ヒット	同様の警告が発生した回数を示します。
説明	*ファイアウォール ルール*のために追加された警告テキストを示します。侵入防止によって警告が発生した場合、フィールドに侵入防止試行のパターン情報が表示されます。

5. 警告の詳細を表示するには、警告を選択して [詳細] をクリックします。
6. 前後の警告に移動するには、[戻る] または [次へ] をクリックします。
7. 詳細を確認したら、[閉じる] をクリックして [ファイアウォールの警告] の詳細ウィンドウを閉じます。
8. [閉じる] をクリックして、「ファイアウォールの警告」ウィンドウを閉じます。

ファイアウォールの警告

ファイアウォールの警告には、警告を発生したデータの情報が含まれています。

ファイアウォールの警告は次の情報を含みます。

フィールド	説明
説明	*ファイアウォール ルール*に警告テキストが追加されました。警告が侵入試行によって発生された場合、警告に侵入試行のパターンを示した情報が表示されます。
処理	実行された処理 (*ファイアウォール*がトラフィックを拒否/許可したことなど) を示します。
時間	警告が生成した日付と時間を示します。

フィールド	説明
方向	トラフィックの方向 (着信または発信) を示します。
プロトコル	使用されている *IP プロトコル*を示します。
サービス	トラフィックに一致している*ファイアウォール サービス*を示します。
リモート アドレス	リモート コンピュータの *IP アドレス*を示します。
リモート ポート	リモート コンピュータのポートを示します。
ローカル アドレス	利用しているコンピュータの *IP アドレス*を示します。
ローカル ポート	利用しているコンピュータのポートを示します。

アクション ログを表示する

ネットワーク ゲームなどのプログラムが動作しなくなった場合、アプリケーション通信制御がプログラムのインターネット アクセスをブロックしたかどうかをアクション ログで確認できます。

アクション ログはインターネット防御の処理に関連する情報を収集したテキスト ファイルです (`action.log`)。アプリケーション通信制御が接続を拒否していることで特定のプログラムがインターネットに接続できない場合などに、は確認のために役に立ちます。ログ ファイルの最大サイズは 10 MB です。ファイルが最大サイズに達すると、古いログが削除されます。

アクション ログを表示するには

1. ユーザ インターフェースで [設定] をクリックします。
2. **[ネットワーク]** ➤ **[ログとパケットキャプチャ]** の順にクリックします。
3. [アクション ログを表示] をクリックします。

アクション ログはメモ帳などのデフォルト テキスト エディタ/ビューワで開くことができます。

パケット キャプチャでネットワークを監視する

パケット キャプチャを使用すると、*IP* ネットワークのトラフィックを収集することができます。

パケット キャプチャの動作

パケット ログは *IP* ネットワークのトラフィックに関連する情報を収集します。

デフォルトでは、パケット キャプチャは無効になっています。パケット キャプチャはネットワークに詳しい上級ユーザを対象にしています。

カスタムの*ファイアウォール ルール*を作成した場合、パケット キャプチャを有効にできます。パケット キャプチャを有効にすると、インターネットの接続に問題がある場合などにパケット ログを採取することで通信に何が起こっているのかを分析することができます。

パケットのログは全部で 10 ファイルに収集されます (`packetlog.0-packetlog.9`)。キャプチャを有効にした際、パケット ログは新たなログ ファイルに保存されます。10 ファイルがいっぱいになったら、次のログは最初のファイル (packetlog.0) に保存されます。このように、新しいログが収集されているときにも以前のログを参照することができます。

パケット ログは*IP* トラフィックに加え、他のネットワーク トラフィックの情報 (*ローカル エリア ネットワーク*(LAN) が必要とするプロトコルなど) も収集します。この情報はルーティング情報なども含みます。

パケット ログは *16*進形式で保存され、*tcpdump* 形式にも対応しています。これによって、デフォルトのパケット ログビューア以外のプログラムでもログ ファイルを開くことが可能です。また、ネットワークのプロトコル 分析プログラムを使用して、コンテンツを詳細に分析することもできます。

パケット キャプチャを開始する

ネットワークの動作に疑いがある場合 (ネットワーク ゲームが動作しなくなったなど)、パケット キャプチャを活用できます。

キャプチャを開始するには

1. ユーザ インターフェースで [設定] をクリックします。
2. **[ネットワーク]** ➤ **[ログとパケットキャプチャ]** の順にクリックします。
3. **[キャプチャする時間]** と [パケットログの最大サイズ] フィールドで表示されている推奨のキャプチャ時間とファイル サイズを使用します。フィールドの値を変更することも可能です。
4. [キャプチャを開始] をクリックします。新しいファイルがログ ファイルのリストに追加されます。情報が収集されるたびにファイルのサイズが大きくなります。リストにログが10 ファイルある場合、次のログは既存のファイルに保存されます。
5. [キャプチャを停止] をクリックしたらキャプチャが停止します。

新しいログ ファイルが生成され、ログ ファイル リストに追加されます。

パケット ログを表示する

パケット ログを作成したら、ログを表示して確認することができます。

パケット ログを表示するには

1. ユーザ インターフェースで [設定] をクリックします。
2. **[ネットワーク]** ➤ **[ログとパケットキャプチャ]** の順にクリックします。
3. 表示したいパケット ログを選択して、[詳細] をクリックします。
   デフォルトのパケット ログビューアが開きます。ウィンドウの上部にログされた接続が表示されます。

次の情報を表示できます。

フィールド	説明
時刻	ログのキャプチャが開始されてからの経過した時間 (秒単位)。キャプチャする時間が60秒と指定されている場合、最初のパケットの開始時間は約0秒、最後のパケットは約60秒になります。
拒否 (dir)	ファイアウォールがパケットを許可または拒否したこと、およびパケットの方向を示します。 • いいえ - パケットを許可 • はい - パケットを拒否 • 着信 - 着信パケット。 • 発信 - 発信パケット。 デフォルトのパケット ログビューア以外のプログラムを使用すると、情報が正常に表示されない可能性があります。
プロトコル	使用された *IP* プロトコル。

フィールド	説明
ソース	*パケットのソース IP アドレス。*
送信先	*パケットの指定 IP アドレス。*
ID	*IP*パケット ヘッダ情報 : パケットの識別子。
時刻	*IP*パケットヘッダ情報 : *継続時間*、パケットの値が、パケットが拒否されるまで通過できるネットワークのデバイス数を指定します。
長さ	*IP*パケット ヘッダ情報 : パケットの長さ。
説明	パケットの説明。

右側のペインにトラフィックのタイプとその情報が表示されます。

下のペインには情報が *16進*と *ASCII* 形式で表示されます。

ネットワーク トラフィックの全タイプ (*IP* トラフィックに限らない) を表示するには、[**IP** 以外をフィルタ] チェックボックスを解除します。

ポリシー マネージャに接続してポリシー ファイルをインポートする

次の方法で、ローカル ホストからポリシー マネージャ サーバへの接続を初期化できます。

1. 「集中管理」ページを開きます。ポリシー マネージャ サーバに最後に接続した日時が表示されます。
2. [今すぐチェック] をクリックして、新しい接続を開始します。
   新しいポリシー ファイルを手動でホストにインポートする必要がある場合、ホスト固有のポリシーをポリシー マネージャ コンソールからエクスポートし、それをホストにインポートする必要があります。
3. ポリシー マネージャ コンソールを開きます。
   a) 「ポリシー ドメイン」タブで対象のホストを選択します。
   b) 指定のホストを右クリックして、メニューから [ポリシー ファイルのエクスポート] を選択します。
   c) ホストのポリシー ファイルをフロッピー ディスクなどの転送メディアに保存します。
4. クライアント セキュリティのローカル ユーザ インターフェースを開きます。
   a) [ポリシーを手動でインポート] をクリックします。
   b) ホストにインポートする `Policy.bpf` ファイルを選択します。

   通常の環境ではポリシー ファイルが自動的に配信されるため、ポリシー ファイルのインポートを行う必要は特にありません。ポリシーの設定ミスなどによりホストがポリシーマネージャの集中管理から切断された場合など、トラブルシューティングが必要な際にこの機能を使用してください。

ダウンロードと更新を停止する

エンドユーザ (ホストのユーザ) がポリシー マネージャとの通信を停止できるように指定できます。

このオプションは、ポリシー マネージャ コンソールで設定できます。低速なダイヤルアップ回線などを使用しているホストに対して便利な機能です。オプションを有効にすると、エンドユーザがポリシー マネージャとのネットワーク通信 (ポリシーの自動ポーリング、統計の送信、自動更新など) を一時的に停止できるようになります。

1. 「ポリシー ドメイン」タブで対象のホストを選択します。
2. 「設定」タブを開いて、「集中管理」ページを選択します。
3. [すべてのダウンロードおよび更新の中断をユーザに許可する] を選択します。
4. をクリックするとポリシーの保存と配布を行います。

F-Secureのアンロードをユーザに許可する

エンドユーザ (ホストのユーザ) が製品をアンロードできるか指定できます。

このオプションは、F-Secureで設定できます。ユーザがポリシー マネージャ コンソール製品を一時的にアンロードできるか指定します。

注: 製品をアンロードするとホストのリソース消費は低くなりますが、セキュリティも無効になりますので注意が必要です。

1. 「ポリシー ドメイン」タブで対象のホストを選択します。
2. 「設定」タブを開いて、「集中管理」ページを選択します。
3. [製品のアンロードをユーザに許可] ドロップダウン メニューから指定のオプションを選択します。
4. をクリックするとポリシーの保存と配布を行います。

第
10
章

ウイルス情報

トピック：

- *マルウェア情報とF-SecureのWeb ページにあるツール*
- *ウイルスのサンプルをF-Secureに送る*
- *ウイルスば発生した場合*

ウイルスの対処法やその他に関する情報を参照できます。

マルウェア情報とF-Secureの Web ページにあるツール

エフセキュアは、マルウェアの情報と便利なセキュリティ ツールを Web 上 (http://www.f-secure.com/security_center/) で公開しています。

次の Web サイトで、最新のセキュリティ脅威に関する情報を確認できます。

- F-Secureのブログ - *http://www.f-secure.com/weblog/*
- 脆弱性に関する情報 - *http://www.f-secure.com/vulnerabilities/*
- 最新の脅威に関する情報は、クライアント セキュリティを通じて各コンピュータに配信することもできます (F-Secureの設定による)。

エフセキュアのリカバリ **CD** を利用してサンプルを分析できる場合もあります。このツールは、独自のオペレーティング システムを搭載しているため、Windows では検出されないマルウェアを検出することが可能です。ツールは Security Center からダウンロードできます。*http://www.f-secure.com/security_center/*

リカバリ **CD** の使い方は、ダウンロード ファイルに含まれています。

ウイルスのサンプルをF-Secureに送る

ここでは、F-Secureのセキュリティ ラボにウイルスのサンプルを送る方法について説明します。

注: ここの説明は上級ユーザ向けです。

ウイルスの説明、問題の内容、お問い合わせは可能な限り英語で説明してください。

通常、エフセキュアは24時間以内に回答できます。問題が複雑な場合、これよりも時間がかかることがあります。1週間以内に回答がない場合、サンプルを再送信してください。

ウイルス サンプルのパッケージを作成する

サンプルは ZIP 形式に圧縮して送信してください。

ZIP ファイルを Windows やオペレーティング システムで作成できない場合、WinZip (*http://www.winzip.com/*) や InfoZIP (*http://www.info-zip.org/pub/infozip/*) などのツールを使用できます。

ZIP ファイルの名前には半角英数字のみを使用してください。ファイル名は長くてもかまいません。

また、ZIP ファイルは、「infected」のパスワードで保護してください。パスワードで保護しない場合、圧縮ファイル内のファイルがセキュリティの理由でメール サーバ側で削除される可能性があります。パスワードで保護された場合、なかのファイルが削除されることはありません。ウイルス サンプルの送信方法については、次の Web ページを参照してください。
http://support.f-secure.com/enu/home/virusproblem/samples/index.shtml

送信するパッケージについて

サンプルのパッケージに含めるものはウイルスの種類によって異なります。

パッケージに含めるもの (ウイルス別)

1. トロイの木馬またはスタンドアロン形式のマルウェア (有害なプログラム)

   スタンドアロン形式のマルウェア (ワーム、バックドア、トロイの木馬、ドロッパなど) の疑いがあるサンプルを送信する場合、ファイルが感染したシステムのどこにあるか (パス)、およびどのようにして起動されたか (レジストリ、`INI` ファイル、`Autoexec.bat` など) を明記してください。

2. F-Secure アンチウイルス製品による誤検出

   クライアント セキュリティによる検出または警告が誤っていた場合、次の情報を送信してください。

   - 問題のファイル
   - クライアント セキュリティのバージョン番号
   - パターン ファイルが最後に更新された日付
   - システムの構成
   - 問題を再現する方法
   - クライアント セキュリティのスキャン レポート ファイルの保存方法については、次の Web サイトを参照してください。*http://support.f-secure.com/enu/home/virusproblem/samples/index.shtml*

3. 新しいウイルスまたはトロイの木馬

   システムがアンチウイルス プログラムでは検出できない未知のウイルスに感染していると思われる場合、次のものを送信してください。

   - Windows XP を実行している場合、**msinfo32** のレポートを作成してください。

1. スタート ➤ ファイル名を指定して実行 を選択します。
2. msinfo32 を入力して、[OK] をクリックします。
3. 「システムの概要」を表示した状態で、ファイル ➤ 保存を選択します。

- Windows 環境設定ファイル (WIN.INI、SYSTEM.INI) と DOS 環境設定ファイル(Autoexec.bat、Config.sys)
- システム レジストリの全部または一部をエクスポートしたもの (この操作は Windows のすべてのバージョンに付属する **Regedit** ユーティリティで実行できます)
- \スタート メニュー\プログラム\スタートアップ\ フォルダのコンテンツ

4. 実行可能ファイルに感染するウイルス

   感染したファイルをシステム内で複数探してください。通常は3□5点のサンプルがあれば十分です。可能であれば、同じファイルを感染していない状態で (バックアップより取得) あわせて送信してください。その場合、ZIP ファイル内には2つのディレクトリを用意してください。

   ORIGINAL\APPPEND.EXE

   ORIGINAL\COMMAND.COM

   INFECTED\APPEND.EXE

   INFECTED\COMMAND.COM

5. マクロ ウイルス

   感染した NORMAL.DOT (グローバル テンプレート) のコピーと感染した DOC ファイルを送信します。Excel のウイルスである場合、感染した XLS ファイルと PERSONAL.XLS (ある場合) を送信します。マクロ ウイルスが他のファイルに感染した場合、それらもパッケージに含めてください。同じ形式のファイルが複数感染されている場合、その形式のファイルを1つだけ含めてください。

6. ブート セクタ ウイルス

   ハード ディスク ドライブが感染している場合、**GetMBR** ユーティリティでブート セクタのサンプルを収集してください。スクリプトが終了したら、mbr.dmp をここで説明した同じ方法でエフセキュアへ送ってください。**GetMBR** は次の FTP サイトからダウンロードできます。
   ftp://ftp.f-secure.com/anti-virus/tools/getmbr.zip

   感染がフロッピー ディスクにある場合、ディスクの DCF イメージを作成して、.DCF イメージ ファイルを送ってください。DCF ユーティリティは次の FTP サイトからダウンロードできます。
   ftp://ftp.f-secure.com/anti-virus/tools/dcf53.zip

   また、感染したディスクをエフセキュアのヘルシンキ オフィス (アドレスは以下参照) に郵送することもできます。郵送する場合、問題を簡単に説明したものを含めてください。なお、フロッピーディスクは返却いたしません。

7. CD の感染または誤検出

   CD の感染や誤検出があった場合、CD をフィンランドのエフセキュア オフィスに送付することができます。

   問題の説明と、可能であればクライアント セキュリティのレポートを印刷して添付してください。感染がなければ CD を返却いたします。

ウイルスのサンプルをエフセキュアに送る

ここでは、ウイルスのサンプルをエフセキュアに送る方法について説明します。

ウイルスのサンプルを送るには

- 最も一般的な方法は、エフセキュアのウイルス サンプル分析ページでウイルスと関連の情報を提供することです。 Web ページのアドレス: *http://www.f-secure.com/samples*
- サンプルのファイル サイズが5MB 以上の場合、次のエフセキュア FTP サイトにサンプルをアップロードしてください。*ftp://ftp.f-secure.com/incoming/*
- サンプルが CD、DVD または USB ドライブなどのメディアに保存されている場合、メディアそのものをエフセキュアに送ることができます。送信先:

  Security Labs

  F-Secure Corporation

  Tammasaarenkatu 7

  PL 24

  00181 Helsinki

  Finland

ウイルスば発生した場合

ここでは、ネットワークでウイルスが発生した場合の対処法と注意点のチェックリストを紹介します。

1. 感染したコンピュータをすぐにネットワークから切断します。

   感染が引き続き拡大している場合、ネットワーク全体をすぐに停止してください。発信トラフィックはすべてブロックする必要があります。また、ホストで不審な挙動が見られた場合は報告するように指示してください。

2. 本当に感染しているのか、それとも誤検出の可能性があるのかを判別します。

   クライアント セキュリティの最新バージョンに最新のパターン ファイルをダウンロードして、コンピュータをスキャンします。本当に感染していると判明した場合、手順3に進みます。感染が「possible new virus」または「, could be an image of a boot sector virus」などのように判定された場合、サンプルとクライアント セキュリティのスキャン レポートをエフセキュアのサンプル分析システムに送信してください。*http://www.f-secure.com/samples* に変更します。

3. 既知のウイルスに感染している場合、F-Secureウイルス情報ページにアクセスして、マルウェアの説明と対処法を参照します。

   駆除ツール(利用可能な場合)をダウンロードして、駆除手順を印刷します。駆除のサポートが必要な場合、Web ページからサポートにお問い合わせください。*http://support.f-secure.com*

   緊急のサポートが必要な場合は、その旨をメッセージに記載してください。

4. 新しいウイルスの場合は、次のURLに掲載されているガイドラインに従ってサンプルを用意し、F-Secure セキュリティ ラボまでサンプルを送信します。*http://www.f-secure.com/samples*

   問題に関する情報はできるだけ多く記載してください。ウイルスに感染したコンピュータの台数は重要な情報です。

5. コンピュータがローカル ネットワークで広がるマルウェアに感染している場合、感染したすべてのコンピュータの駆除が完了するまでネットワークを停止することを推奨します。

   ネットワークはすべてのコンピュータの駆除が完了した場合にのみ再起動できます。感染しているマシンが 1台でもあれば、数分で再びネットワーク全体に感染してしまう可能性があるためです。

6. エフセキュアがマルウェアの分析を終えるまで待ち、提供される駆除の手順に従います。

   感染したコンピュータに駆除処理を行う前に、重要なデータをバックアップします。このバックアップは、ネットワーク経由ではなく外部のバックアップデバイスを使用して作成してください。バックアップの対象はファイルだけで十分です。実行可能ファイルはバックアップしないでください。後でバックアップを復元する必要が生じた場合、復元したファイルが感染していないかどうかを確認してください。

7. 駆除に関する指示が提供されたら、まず1台のコンピュータで試します。正常に機能したら、感染したすべてのコンピュータで実行してください。

   クライアント セキュリティと最新のパターン ファイルを使用して駆除済みのコンピュータをスキャンし、感染ファイルが残っていないことを確認します。

8. 感染したすべてのコンピュータの駆除が完了したら、ネットワークを再起動します。

   マルウェアにバックドアやデータ漏洩機能があった場合、ネットワーク リソースのパスワードとログイン名を変更することを強く推奨します。

9. エンドユーザに対してウイルスの発生を通知し、不明な添付ファイルを実行したり、疑わしいインターネット サイトにアクセスしたりしないよう警告します。

ホストにインストールされているソフトウェアのセキュリティ設定を確認します。メール スキャンやファイアウォールがサーバ上で正常に動作していることを確認します。クライアント セキュリティは常に最新のパターン ファイルをダウンロードしますが、自動更新が動作していることを定期的に確認することも推奨します。

10. パートナーや関連のあるネットワークやユーザに対してウイルスの発生を警告し、クライアント セキュリティと最新のパターン ファイルを使用してコンピュータをスキャンするよう推奨します。これにより、感染がネットワーク外に広がっていないことを確認します。

第
11
章

Cisco NAC プラグインの設定

トピック：

- *Cisco NAC プラグインのインストール*
- *Posture 検証属性の定義をインポートする*
- *アプリケーション Posture トークンの属性*

F-Secure は、Cisco Systems, Inc. が主導する Network Admission Control (NAC) のパートナー プログラムに参加しています。Cisco NAC は、パターン ファイルが更新されていないときやアンチウイルスまたはファイアウォールなどのモジュールが無効にされているときに、ホストのネットワーク アクセスを制限することができる機能です。

F-Secure NAC プラグインは、セキュリティ関連の情報を収集するクライアント ソフトウェアである Cisco Trust Agent (CTA) と通信します。収集したデータは Cisco Secure Access Control Server (ACS) に送信され、データに基づいて適切なアクセス ポリシーがホストに適用されます。

NAC の詳細については、*http://www.cisco.com/go/nac/* を参照してください。

クライアント セキュリティのインストール パッケージには Cisco NAC プラグインをインストールするためのオプションが含まれています。Cisco NAC プラグインをインストールする場合、CTA をホストに事前にインストールしている必要があります。また、ACS サーバがF-Secure の製品に関連するセキュリティの属性を監視するように設定されていることも必要です。

Cisco NAC プラグインのインストール

Cisco NAC プラグインはローカルおよびリモートからホストにインストールすることが可能です。

1. ローカル インストール: クライアント セキュリティをローカルでインストールする際に、「「インストールするコンポーネント」ダイアログにある [**Cisco NAC プラグイン**] を選択します。
2. リモート インストール: クライアント セキュリティをリモートでインストールする際に、「「インストールするコンポーネント」ダイアログにある [**Cisco NAC プラグイン**] を選択します。

👉 **注:** 詳細については、Cisco NAC の取扱説明書を参照してください。

Posture 検証属性の定義をインポートする

Cisco NAC プラグインを使用する場合、F-Secureの製品に関連する Posture 検証属性の定義を Cisco Secure ACS Posture 検証属性の定義ファイルに追加する必要があります。

1. Cisco Secure ACS サーバで **CSUtil** ツールを次のように実行することで定義ファイルを追加できます。
2. `CSUtil.exe -addAVP fsnacpva.def`

   `fsnacpva.def` は製品のインストール パッケージに含まれています。

   注: **CSUtil** の詳細については、Cisco ACS の取扱説明書を参照してください。

アプリケーション Posture トークンの属性

Cisco ACS サーバを使用して、F-Secure の製品に関連するセキュリティの属性を監視することができます。

F-Secure の製品に関連するセキュリティの属性を監視するには

1. Cisco ACS サーバのユーザ インターフェースにある [**External user databases**] ボタンをクリックします。
   「**External user databases**」ページが開きます。
2. [**Database configuration**] をクリックします。
   「**External user databases configuration**」ページが開きます。
3. [**Network admission control**] をクリックします。
4. [**Configure**] をクリックします。
5. [**Create new local policy**] を選択します。
6. *アプリケーション Posture トークンのルールで使用する属性を選択します。*

   - アンチウイルスの Posture 検証属性

属性名	種類	例
Software-Name	文字列	`F-Secure` アンチウイルス
Software-Version	バージョン	`8.0.0.0`
Dat-Date	date	データベースの日付
Protection-Enabled	署名されていない整数	`1`=有効、`0`=無効

   - ファイアウォールの Posture 検証属性

属性名	種類	例
Software-Name	文字列	`F-Secure` インターネット防御
Software-Version	バージョン	`8.0.0.0`
Protection-Enabled	署名されていない整数	`1`=有効、`0`=無効

第
12
章

高度な機能 - ウイルスとスパイウェア防御

トピック：

- *スケジュール スキャンを設定する*
- *高度な機能 - ディープガード*
- *ポリシー マネージャ プロキシを設定する*
- *ポリシー マネージャ プロキシからホストの自動更新を設定する*
- *プログラムを Web スキャンから除外する*

ここでは、アンチウイルス プロキシやスケジュール スキャンなどのウイルス防御に関連するタスクの設定について説明します。

スケジュール スキャンを設定する

スケジュール (予約した) スキャン タスクは、ユーザ インターフェースの詳細モードで追加することができます。

次の例では、スケジュール スキャンのタスクがドメイン全体のポリシーに追加されます。スキャンは2009年8月25日から毎週月曜日の午後8時に実行されるように設定します。

1. 表示 ➤ 詳細モード メニューからを選択します。
   ユーザ インターフェースが詳細モードに変わります。
2. 「ポリシー ドメイン」タブで [ルート] を選択します。
3. 「ポリシー」タブで、**F-Secure ➤ F-Secure Anti-Virus** の順に選択します。
4. 「スケジュール テーブル」を選択します。
   設定されているスケジュール タスクが「スケジュール」に表示されます。ここで、新しいスキャン タスクを追加できます。
5. [追加] ボタンをクリックします。
   「スケジュール」テーブルに新しい行が追加されます。
6. 新しい行の [名前] セルをクリックして、[編集] をクリックします。
7. [名前] セルに新しいタスクの名前を指定します。

   たとえば、「全ホストに対するスケジュール スキャン」のように名前を付けます。
8. 次に、[スケジュール パラメータ] セルをクリックして、[編集] をクリックします。
9. ここで、スケジュール スキャンのパラメータを入力します。

   2009年8月25日から毎週月曜日の午後8時に実行されるスケジュール スキャンを設定するには、「`/t20:00 /b2009-08-25 /rweekly`」と指定します。

   注: [スケジュール パラメータ] セルを選択すると、「スケジュール タスク」テーブルの下にある「メッセージ」ウィンドウで、使用できるパラメータとその形式が参考として表示されます。

10. [タスクの種類] セルをクリックし、[編集] を選択します。
11. ドロップダウン リストから [ローカル ドライブをスキャン] を選択します。
    スキャン タスクが追加されます。
12. をクリックするとポリシーの保存と配布を行います。

特定の日時に実行されるスケジュール スキャンを設定する

特定の日や曜日に実行されるスキャンを設定することができます。特定の日や曜日を指定するには、「`/Snn`」のパラメータを使用します。

- 週単位のスキャンには、「`/rweekly`」を「`/s1`」□「`/s7`」のパラメータと組み合わせることで、細かいスケジュールが指定できるようになります。「`/s1`」は月曜日を、「`/s7`」は日曜日を指しします。

  たとえば、「`/t18:00 /rweekly /s2 /s5`」と指定すると、毎週火曜日と金曜日の18時にスキャンが実行されます。
- 月単位のスキャンには、「`/rmonthly`」と「`/s1`」□「`/s31`」のパラメータを使用します。

  たとえば、「`/t18:00 /rmonthly /s5 /s20`」と指定すると、毎月の5日と20日の18時にスキャンが実行されます。

👉 **注:** 週単位のスケジュール スキャンは毎週月曜日にも自動的に実行されます。月単位のスケジュール スキャンは、毎月の1日に自動的に実行されます。

高度な機能 - ディープガード

ここでは、ディープガードの設定について説明します。

イベントを拒否したときにユーザを通知する

ディープガードがイベント拒否したときにユーザを通知することができます。

ユーザを通知するには

1. 表示 ➤ 詳細モード メニューからを選択します。
   ユーザ インターフェースが詳細モードに変わります。
2. 「ポリシー ドメイン」タブで [ルート] を選択します。
3. 「ポリシー」タブで、**F-Secure** ➤ ディープガード ➤ 設定 ➤ 拒否されたイベントの発生時に通知を表示する の順に選択します。
4. [はい] を選択します。
5. をクリックするとポリシーの保存と配布を行います。

他のプログラムからのイベントをを管理者権限のユーザが許可または拒否する

他のユーザが開始したプログラムのイベントを管理者が許可または拒否するには

1. 表示 ➤ 詳細モード メニューからを選択します。
   ユーザ インターフェースが詳細モードに変わります。
2. 「ポリシー ドメイン」タブで [ルート] を選択します。
3. 「ポリシー」タブで、**F-Secure** ➤ ディープガード ➤ 設定 ➤ ローカル管理者制御 を選択します。
4. [すべてのプロセス] を選択します。
5. をクリックするとポリシーの保存と配布を行います。

特定のプログラムからのイベントを許可または拒否する

特定のプログラムが発生するイベントを許可または拒否することができます。たとえば、安全と判断できるプログラムがある場合、そのプログラムからのイベントをすべて許可できます。また、危険なプログラムからのイベントは拒否するようにも設定できます。

1. プログラムの SHA-1 ハッシュ値をまず計算する必要があります。

   SHA-1 の値はインターネットの無料ツール (「Microsoft File Checksum Integrity Verifier」など) を利用して計算できます。「Microsoft File Checksum Integrity Verifier」は次の URL でアクセスできます。
   http://support.microsoft.com/kb/841290

   注**:** SHA-1 ハッシュ関数は、プログラムを構成する一連の情報を識別します。新しいプログラムを利用できる場合、新しいプログラムが別の SHA-1 ハッシュを持つため、ハッシュ値をもう一度計算する必要があります。

2. SHA-1 ハッシュ値を計算したら、表示 ➤ 詳細モード メニューを開きを選択します。
   ユーザ インターフェースが詳細モードで開きます。
3. 「ポリシー ドメイン」タブで [ルート] を選択します。
4. 「ポリシー」タブで、**F-Secure** ➤ ディープガード ➤ 設定 ➤ アプリケーション の順に選択します。

5. [追加] をクリックして、新しいルールを追加します。
6. る新しいエントリの [**SHA-1 ハッシュ**] セルをダブルクリックして、SHA-1 ハッシュをセルに貼り付けます。
7. [メモ] をダブルクリックして、メモを入力します。

   メモには、SHA-1 ハッシュが認識するアプリケーションの名前を入力すると便利です。
8. [信頼済み] セルをダブルクリックします。
   - [はい] をクリックすると、アプリケーションのイベントをすべて許可します。
   - [いいえ] をクリックすると、アプリケーションのイベントをすべて拒否します。
9. [有効] セルをダブルクリックします。
10. [はい] を選択して、ルールを有効にします。
11. をクリックするとポリシーの保存と配布を行います。

アプリケーションのルールはローカルで変更することはできません。

ポリシー マネージャ プロキシを設定する

ポリシーマネージャは、低速なネットワーク接続での負荷を大幅に減少させることにより、分散インストールにおける帯域幅の問題を解決することができます。

ポリシー マネージャ プロキシは、F-Secure更新サーバまたはポリシー マネージャ サーバから自動的に取得した更新をキャッシュし、対象のホストに対してデータベースの配布ポイントとして機能するためにホストと同じリモート ネットワークに配置されます。ポリシーマネージャ プロキシは低速な回線を使用しているネットワークに適切な機能で、帯域や回線速度に問題があるネットワークに導入することを推奨します。

クライアント セキュリティまたはアンチウイルス ワークステーションを実行しているホストは、パターンファイルをポリシー マネージャ プロキシから取得します。F-Secure ポリシー マネージャ プロキシは必要な際に、F-Secure ポリシー マネージャサーバおよび F-Secure の配布サーバと通信します。

ネットワークにリモートのホストがある場合、それらのホストはメインのポリシー マネージャ サーバと通信しますが、この通信はリモートのポリシー管理、ステータスの監視、および警告に制限されます。大量のデータベース更新のデータ転送が同じローカル ネットワーク内のポリシーマネージャ プロキシによってリダイレクトされるため、ホストとポリシー マネージャ サーバのネットワーク接続の負荷は大幅に軽減されます。

注: ポリシー マネージャ プロキシのインストールと設定については、ポリシー マネージャ プロキシの管理者ガイドを参照してください。

ポリシー マネージャ プロキシからホストの自動更新を設定する

「設定」タブで、ホストが更新の取得に使用するプロキシを設定できます。

次の方法で、ホストユーザ インターフェースから自動更新の設定行うことが可能です。

1. 「自動更新」ページで [詳細] をクリックします。
2. 自動更新 ➤ ポリシー マネージャ プロキシ の順に選択します。

   「ポリシー マネージャ プロキシ」ページで、ローカルのクライアント セキュリティが自動更新を取得するアドレスを表示および編集できます。

   アドレスは上から順番に使用されます。リストの最初のアドレスがデフォルトで使用されます。
3. [追加] をクリックすると、プロキシをリストに追加できます。
4. フィールドにプロキシの名前を入力して、[**OK**] をクリックします。
5. 他のプロキシを追加する場合、上記の手順を繰り返します。

   サーバが利用される順序を変更するには、移動するサーバを選択して、右側にある上矢印または下矢印をクリックします。
6. プロキシをすべて追加したら、[**OK**] をクリックします。

プログラムを Web スキャンから除外する

特定のプログラムを安全と判断できる場合、そのプログラムを Web スキャンから除外することができます。

1. 表示 ➤ 詳細モード メニューからを選択します。
2. 「ポリシー」タブで、**F-Secure Client Security** ➤ プロトコル スキャナの選択 ➤ 信頼済みのアプリケーション ➤ 信頼済みのプロセス の順に選択します。
3. Web スキャンから除外するプロセスの名前を入力します。

   複数のプロセスを入力する場合、各プロセスをカンマで区切ります。各プロセス名の間には空白を入れないでください。

   ヒント: Windows を利用している場合、アプリケーションのプロセス名は Windows のタスク マネージャから確認できます。

   たとえば、Web トラフィック スキャンから 「メモ帳」と「Skype」を除外するには「`notepad.exe,skype.exe`」と入力します。
4. をクリックするとポリシーの保存と配布を行います。

第
13
章

高度な機能 - インターネット防御

トピック：

- *インターネット防御をリモートから管理する*
- *セキュリティ レベルの自動選択*
- *接続に関するトラブルシューティング*
- *サービスを追加する*
- *ダイヤルアップ制御の設定*

また、インターネット防御のトラブルシューティングに関する情報についても説明します。

インターネット防御をリモートから管理する

ここでは、インターネット防御の設定をリモートから管理する方法について説明します。

パケット ロギング

「パケット ロギング」は、ローカル ネットワークの動作や処理を監視するために便利なデバッグ ツールです。

その反面、使い方によって、LAN 上の他のユーザの操作を傍受するためにエンドユーザが悪用できる強力なツールでもあります。次の方法で、パケット ロギングを無効にすることができます。

1. メニューから 表示 ➤ 詳細モード を選択します。
   ユーザ インターフェースが詳細モードに変わります。
2. 「ポリシー ドメイン」タブで [ルート] を選択します。
3. 「ポリシー」タブで [**F-Secure** インターネット防御] を選択します。
4. 「ロギング」タブを選択します。
   この変数は、パケット ロギングのステータスを示します。「無効」の場合、パケット ロギングは実行されていません。「有効」の場合、パケット ロギングがホスト上で実行されています。
5. ロギングを完全に無効にするには、変数が「無効」に設定されていることを確認してから [確定] チェックボックスをオンにします。
6. 変更を有効にするためにポリシーを配布します。

変更を後で元に戻すには、[確定] チェックボックスをオフにして、新しいポリシーを配布します。

注: ドメイン全体に対して変数を [有効] に設定すると、すべての対象ホスト上でロギング セッションが開始しますので、操作を行う際には注意してください。

信頼済みのインターフェース

「信頼済みのインターフェース」は、ホストがファイアウォールなどによってブロックされている場合でもホストを接続共有サーバとして許可します。

信頼済みのインターフェースを利用するトラフィックにはファイアウォールのルールは適用されません。このため、ホストがネットワークから攻撃を受ける可能性がありますので、必要がない場合はセキュリティの対策として信頼済みのインターフェースを無効にすることを推奨します。

信頼済みのインターフェースを有効にするには

1. 表示 ➤ 詳細モード をメニューから選択します。
   ユーザ インターフェースが詳細モードに変わります。
2. ポリシー ドメイン ツリーで、信頼済みインターフェースを有効にするサブドメインを選択します。
3. 「ポリシー」タブで、**F-Secure** インターネット防御 ➤ 設定 ➤ ファイアウォール エンジン ➤ 信頼済みのインターフェースを許可 の順に選択します。
4. [有効] を選択すると、信頼済みのインターフェースが対象のサブドメインで有効になります。
   サブドメイン内のエンドユーザがネットワーク インターフェースを信頼済みのインターフェースとして設定できるようになります。
5. 変更を有効にするためにポリシーを保存および配布してください。

パケットのフィルタリング

「パケット フィルタリング」はファイアウォールの基本的なセキュリティ対策方法の1つで、IP ネットワークのトラフィックをパケットのプロトコル ヘッダの情報に基づいてフィルタリング (分別) します。

パケット フィルタリングは、[ネットワーク保護] の設定にある「詳細」タブで有効または無効にできます。パケット フィルタリングは試験的に無効にする必要がある場合もありますが、無効にしたらセキュリティが危険な状態となります。このため、パケット フィルタリングを常に有効にすることを推奨します。

1. 表示 ➤ 詳細モード をメニューから選択します。
   ユーザ インターフェースが詳細モードに変わります。
2. 「ポリシー ドメイン」タブで [ルート] を選択します。
3. 「ポリシー」タブで、**F-Secure** インターネット防御 ➤ 設定 ➤ ファイアウォール エンジン ➤ ファイアウォール エンジン の順に選択します。
4. パケット フィルタリングを常に有効にするには、変数を [はい] に設定して、[確定] チェックボックスをオンにします。
5. 変更を有効にするためにポリシーを配布します。

セキュリティ レベルの自動選択

この例では、セキュリティ レベルの自動選択が、ノート コンピュータだけが含まれているサブドメインに対して設定されています。ノート コンピュータが企業の LAN に接続されている場合、[オフィス] セキュリティ レベルが使用され、ダイヤルアップ接続を使用する際にはセキュリティ レベルが [モバイル] に変更されます。

セキュリティ レベルの自動選択を指定する前に、DNS サーバの IP アドレスおよびデフォルト ゲートウェイのアドレスを知っている必要があります。IP アドレスとデフォルト ゲートウェイは、コマンドプロンプトから `ipconfig -all` を実行することで確認できます。

1. 表示 ➤ 詳細モード メニューからを選択します。
   ユーザ インターフェースが詳細モードに変わります。
2. [ポリシー ドメイン] ツリーから対象となるサブドメインを選択します。
3. 「ポリシー」タブで、**F-Secure ➤ F-Secure** インターネット防御 の順に選択します。
4. 「セキュリティ レベルの自動選択」を選択します。
5. [セキュリティ レベルの自動選択] が有効になっていることを確認します。

   有効になっていない場合、[自動選択モード] ドロップダウン リストから [ユーザが変更可能] または [管理者のフル コントロール] を選択します。
6. [追加] をクリックして、最初のセキュリティ レベルを追加します (この例では [オフィス])。
7. セルを選択して [編集] をクリックすると、セルにデータを入力できます。

   [オフィス] セキュリティ レベルの場合は、次のデータを追加する必要があります。

   - 優先度 - 優先番号が小さいルールの順に確認されます。
   - セキュリティ レベル - セキュリティ レベルの ID を入力します (番号および名前で構成されます。たとえば、「`40office`」)。
   - 方法**1** - ドロップダウン リストから [**DNS** サーバ **IP** アドレス] を選択します。
   - 引数**1** - ローカル DNS サーバの IP アドレスを入力します (たとえば、「`10.128.129.1`」)。
   - 方法 **2** - ドロップダウン リストから [デフォルト ゲートウェイの **IP** アドレス] を選択します。
   - 引数**2** - デフォルト ゲートウェイの IP アドレスを入力します (たとえば、「`10.128.130.1`」)。

   注**:** [引数] フィールドには、引数を1つだけ入力できます (たとえば1つの IP アドレス)。複数のデフォルト ゲートウェイをセキュリティ レベルの自動選択で使用する場合、各ゲートウェイに対して個別のルールを作成してください。

8. [追加] をクリックして、自動選択の対象となる2つ目のセキュリティ レベルを追加します。この例では、[モバイル] です。
9. セルを選択し、[編集] をクリックして、セルにデータを入力します。

   [モバイル] セキュリティ レベルの場合、次のデータを追加する必要があります。

   - 優先番号 - 優先番号が小さいルールの順から確認されます。
   - セキュリティ レベル - セキュリティ レベルの ID を入力します (たとえば、「`20mobile`」)。
   - 方法**1** - ドロップダウン リストから [ダイヤルアップ] を選択します。
   - 引数**1** - 空白のままにします。
   - 方法**2** - ドロップダウン リストから [常に使用] を選択します。
   - 引数**2** - 空白のままにします。

   これで、設定の準備が整いました。

10. をクリックするとポリシーの保存と配布を行います。

接続に関するトラブルシューティング

接続の問題 (ホストがインターネットにアクセスできないなど) が発生し、インターネット防御が原因と思われる場合、以下の事項を確認してください。

1. コンピュータが正しく接続されていることを確認します。
2. 問題がネットワーク ケーブルでないことを確認します。
3. イーサネットが起動して正しく稼動していることを確認します。
4. DHCP アドレスが有効であることを確認します。

   コマンドプロンプトで `ipconfig` を実行すると、アドレスを確認できます。
5. 次に、デフォルト ゲートウェイに ping コマンドを行います。

   アドレスが分からない場合、コマンド プロンプトで `ipconfig -all` を入力することによりアドレスを確認できます。
6. インターネットの Web サイトなどにアクセスできない場合、DNS サーバに ping を実行します。
   - `nslookup` を実行して、DNS サービスが動作していることを確認します。
   - また、特定の Web アドレスに ping を実行して、対象のコンピュータが動作していることを確認できます。
7. 集中管理ドメインが変更されたか確認します。新しいポリシーが使用されているか、問題を引き起こす可能性がある設定がポリシーに含まれているかなどを確認します。
   - 発信 HTTP 接続が許可されているかファイアウォールのルールで確認します。
   - ユーザが接続しようとしている IP アドレスが拒否されたアドレスのリストに誤って追加されてないか、ホストのアプリケーション通信制御で確認します。
8. 問題が解決されない場合、F-Secureをアンロードするか、インターネット防御を [すべて許可] モードに設定します。

問題がそれでも解決されない場合、ルーティングまたはユーザが接続しようとしているコンピュータ内の他のコンポーネントに問題がある可能性があります。

サービスを追加する

ここで言うサービスとは、ネットワーク上で利用可能なネットワーク サービスのことを意味します (ファイル共有、リモート コントロール アクセス、Web 閲覧など)。

ほとんどのサービスは使用するプロトコルとポートで定義されます。

デフォルトの HTTP サービスに基づいたインターネット サービスを作成する

この例では、Web サーバが非標準のポートを使用した上で起動していると仮定します。

通常、Web サーバは TCP/IP ポート 80 を利用しますが、この例ではポート 8000 を利用するように設定されています。ホストからサーバへの接続を有効にするには、新しいサービスを作成する必要があります。標準の HTTP ポートを使用していないため、標準の HTTP サービスはここでは動作しません。新しいサービスは「`HTTP ポート 8000`」で、デフォルトの「`HTTP`」サービスに基づいています。

1. 「ポリシー ドメイン」タブで新しいサービスの対象となるサブドメインを選択します。
2. 「設定」タブに移動して、「ファイアウォール サービス」を開きます。
   ファイアウォール サービスのテーブルが表示されます。
3. [追加] ボタンをクリックして、ファイアウォール サービスのウィザードを起動させます。
4. サービスの名前を入力します。
   a) [サービス名] フィールドでサービスの名前を指定します。同じ名前を2つのサービスに付けることはできません。
      例: `HTTP port 8000`。
   b) [サービスのコメント] フィールドで、サービスに関するコメントを入力します。
      コメントがファイアウォール サービスのテーブルに表示されます。
5. IP プロトコル番号を選択します。
   a) このサービスの対象となるプロトコル番号を [プロトコル] ドロップダウン リストから選択します。
      リストから一般的のプロトコル (TCP、UDP、ICMP) を選択できます。サービスが他のプロトコルを使用する場合、以下の表を参照して、対応するプロトコルの番号を入力してください。
      この例では、[**IP プロトコル番号**] ドロップダウン リストから [**TCP (6)**] を選択します。

プロトコル	プロトコル番号	説明
ICMP	1	ICMP / Internet Control Message Protocol (インターネット制御通知プロトコル)
IGMP	2	Internet Group Management Protocol (インターネット グループ マネジメント プロトコル)
IPIP	4	IPIP トンネル (IP 内の IP)
TCP	6	Transmission Control Protocol (伝送制御プロトコル)
EGP	8	Exterior Gateway Protocol (エクステリア ゲートウェイ プロトコル)
PUP	12	Xerox PUP ルーティング プロトコル

プロトコル	プロトコル番号	説明
UDP	17	User Datagram Protocol (ユーザ データグラム プロトコル)
IDP	22	Xerox NS Internet Datagram Protocol (インターネット データグラム プロトコル)
IPV6	41	IP バージョン 4 にカプセル化された IP バージョン 6
RSVP	46	Resource Reservation Protocol (リソース リザベーション プロトコル)
GRE	47	Cisco の Generic Routing Encapsulation (総称ルーティング カプセル化) トンネル
ESP	50	Encapsulation Security Payload (暗号ペイロード) プロトコル
AH	51	Authentication Header (認証ヘッダ) プロトコル
PIM	103	Protocol Independent Multicast (プロトコル インディペンデント マルチキャスト)
COMP	108	Compression Header (圧縮ヘッダ) プロトコル
RAW	255	Raw IP パケット

6. イニシエータ ポートを指定します。

   サービスが TCP または UDPプロトコルを使用している場合、サービスのイニシエータ ポートを指定する必要があります。ポートとポート範囲の入力形式は次のとおりです。

   - >ポート番号 - 「ポート番号」より大きいすべてのポート
   - >=ポート番号 - 「ポート番号」以上のすべてのポート
   - <ポート番号 - 「ポート番号」より小さいすべてのポート
   - <=ポート番号 - 「ポート番号」以下のすべてのポート
   - ポート番号 - 指定の「ポート番号」のみ
   - [最小ポート番号-最大ポート番号] - 「最小ポート番号」と「最大ポート番号」およびその間のすべてのポート (ダッシュの両側にはスペースを入れないでください)。

   これらの項目をカンマで区切って一緒に定義することができます。例えば、ポート 10、11、12、100、101、200 および 1023 以上は、「`10-12, 100-101, 200, >1023`」と定義できます。

   この例では、イニシエータ ポートに「`>1023`」を指定します。

7. リスポンダ ポートを指定します。

   サービスが TCP または UDPプロトコルを使用している場合、サービスのリスポンダ ポートを指定する必要があります。

   この例では、リスポンダ ポートに「`8000`」を指定します。

8. サービスに適用する分類番号をドロップダウン リストから選択します。

デフォルトの値を使用します。

9. サービスが許可するトラフィックに、標準のパケット フィルタリングと状態検査フィルタリング以外に他のフィルタリングを適用するか選択します。
この例では、デフォルトの [無効] を選択します。

   注: サービスが TCP プロトコルを使用し、アプリケーション通信制御を有効にしない場合、[その他のフィルタリング] ドロップダウン メニューから [アクティブ モード **FTP**] を選択できます。接続に開く必要があるポートに関する情報が転送されるデータに含まれるため、アクティブ モード **FTP** に対してファイアウォールから特別な操作を行うことが必要です。

10. 作成したルールを確認します。
ルールを変更する必要があれば、[戻る] をクリックしてルール作成画面に戻ってください。

11. [完了] をクリックして、スキャン ウィザードを閉じます。
作成したルールがファイアウォール ルールのテーブルに表示されます。

12. 新しいルールを適用します。
新しいサービスを適用するには、使用中のセキュリティ レベルで「**HTTP 8000**」ファイアウォール サービスの使用を許可する新しいインターネット防御ルールを作成する必要があります。ルール ウィザード ➤ サービスウィンドウで新しいサービスを選択できます。ルール ウィザード ➤ 詳細オプションウィンドウで警告を定義する必要はありません。

ダイヤルアップ制御の設定

ダイヤルアップ制御は、ダイヤルアップによる接続の許可と拒否を行う電話番号を管理します。

ダイヤルアップ制御を有効にするには

1. メニューから 表示 ➤ 詳細モード を選択して、ユーザ インターフェースを詳細モードに切り替えます。
2. 「ポリシー」タブで、**F-Secure** ➤ **F-Secure** インターネット防御 ➤ 設定 ➤ ダイヤルアップ制御 ➤ ダイヤルアップ制御 の順に選択します。
3. [有効] を選択して、ダイヤルアップ制御を有効にします。
4. をクリックするとポリシーの保存と配布を行います。

電話番号を許可/拒否する

特定の電話番号に対するダイヤルアップ接続を許可または拒否できます。

特定の電話番号を許可/拒否するには

1. メニューから 表示 ➤ 詳細モード の順に選択して、詳細モードに切り替えます。
2. 「ポリシー」タブで、**F-Secure** ➤ **F-Secure** インターネット防御 ➤ 設定 ➤ ダイヤルアップ制御 ➤ 電話番号 の順に選択します。
3. [追加] をクリックします。
4. ルールの優先度を設定するために [優先度] セルをダブルクリックします。

   複数のルールが電話番号に一致する場合、優先番号の低いルールが適用されます (たとえば、優先番号「1」のルールは優先番号「3」のルールより優先されます)。
5. ルールの対象となる電話番号を追加するために [電話番号] セルをダブルクリックします。

   複数の電話番号を対象としたい場合、次のワイルドカード (特殊) 文字を利用できます。

文字	意味	例
?	任意の1数字を指定します	「1?3」 - 次の数字・番号を示します。103、113、123、133、143、153、163、173、183、193
*	任意の長さの任意の数字を指定します	「0800*」 -0800 で始まる電話番号にすべて一致します

6. [許可] または [拒否] を選択して、電話番号を許可/拒否します。
7. [コメント] セルをダブルクリックして、電話番号に関するコメントを入力できます。
8. [はい] を選択して、ルールを適用します。
9. をクリックするとポリシーの保存と配布を行います。

番号のロギング

ダイヤルした番号をログに保存することができます。

番号のロギングを有効にするには

1. メニューから 表示 ➤ 詳細モード の順に選択して、詳細モードに切り替えます。

2. 「ポリシー」タブで、**F-Secure** ➤ **F-Secure** インターネット防御 ➤ 設定 ➤ ダイヤルアップ制御 ➤ 番号のロギング の順に選択します。
3. [有効] を選択します。
4. をクリックするとポリシーの保存と配布を行います。

第
14
章

Prodsett.ini を設定する

トピック：

- *Prodsett.ini を設定する*

ここでは、Prodsett.ini で編集できる設定を説明します。

注意: ここで記載されていない Prodsett.ini の設定は変更しないでください。

注: RequestInstallModeはInstallModeの設定を影響します。

RequestInstallModeの設定は、InstallMode=0の設定を無効にします。

Prodsett.ini を設定する

Prodsett.ini で下記の設定を変更することができます。

[F-Secure common]	共通の設定
CD-Key=XXXX-XXXX-XXXX-XXXX-XXXX	インストール パッケージのライセンス キーコード。
SetupLanguage=ENG	インストールで使用する言語。 設定が空または「AUTO」に定義されている場合、インストール言語はホストのデフォルト ロケールによって決まります。選択できる言語は対応言語に限られます(SupportedLanguages を参照)。
SetupMode=1	1 = ネットワーク クライアント (デフォルト)。「SetupMode=1」の場合、該当する集中管理の設定を「PMSUINST.DLL」で定義してください。 2 = スタンドアロン セットアップ モード。
SupportedLanguages=ENG FRA DEU FIN SVE ITA	インストールパッケージで使用できる言語の一覧。 不要な言語を除外することで言語セットを小さくできます。 パッケージに新しい言語を追加する場合、その言語を有効にするために、ここに追加する必要があります。
InstallLanguages=ENG FRA DEU FIN SVE ITA	ホストにインストールされる言語の一覧。通常、この設定は「SupportedLanguages」と同じです。 不要な言語をインストールから除外することで言語セットを小さくできます。 パッケージに新しい言語を追加する場合、インストールするソフトウェアに対してその言語を有効にするために、ここに追加する必要があります。 SetupLanguage で定義された言語の言語ファイルは、常に単独で InstallLanguages の設定にインストールされます。
SecurityPolicy=0 | 1 | 2	NTFS にインストールされたファイルやフォルダ、および製品のレジストリ キーを、定義されている「SecurityPolicy」に従って NT のセキュリティ アクセス許可で保護します。 0 = 特定のポリシーを適用しません。ファイルおよびフォルダは親からセキュリティ アクセス許可を継承します。

[F-Secure common]	共通の設定
	1 = それほど厳密ではないポリシー。ファイルおよびフォルダは許可されている Users と Administrators にはフル アクセス、Everyone には読み取り専用アクセスを与えるアクセス許可で保護されます。 2 = 厳密なポリシー。ファイルおよびフォルダは、Administrators にはフル アクセス、Power Users には読み書きアクセス、Users には読み取り専用アクセスをそれぞれ許可し、Everyone にはアクセスを許可しないアクセス許可で保護されます。 参考: `SecurityPolicy = 1` または 2 の場合、セットアップは既存のファイル、フォルダ、およびレジストリ キーの access control list (ACL) を上書きします。ACL を厳密に設定した場合 (たとえばユーザを追加した場合)、インストール後に再設定する必要があります。

[Silent Setup]	操作の必要がない自動インストールの設定
DestinationDirUnderProgramFiles=F-Secure	デフォルトのインストール パス。特定のインストール ポリシーを順守する必要がある場合などに限り、この設定を変更してください。
Reboot=2	1 = インストール後に自動的に再起動します。 注目: このオプションは、ホストで「強制再起動」を実行します。再起動を行うときにはホストで確認のメッセージは表示されません。インストール先のコンピュータでこのような再起動を実行しても安全と判断できる場合以外は、このオプションを設定しないでください。 2 = 確認のメッセージを表示した後に再起動します (デフォルト)。 注: このオプションはホストで「標準の再起動」を実行します。場合によっては、ユーザが再起動を遅らせたり、中止したりすることもできます。 3 = インストール後に再起動しません。

[FSMAINST.DLL]	管理エージェントの設定
RequestInstallMode=1	ネットワーク クライアントをインストールする際に、コンポーネントを必ずインストールします。コンポーネントの`RequestInstallMode`また`InstallMode`の設定を変更する必要はありません。

[FSMAINST.DLL]	管理エージェントの設定
ManagementKey=\\server\path\admin.pub	管理用公開鍵の場所。
ManagedStandAlone=	スタンドアロンインストールでのみ有効です。 0 = 標準のスタンドアロン インストール。ポリシー ファイルをインポートすることはできません (デフォルト)。 1 = インストールしたコンポーネントは、手動でインポートされたポリシーを使用して管理できます。
win2000renamefiles=fsrec.2k|fsrec.sys;fsfilter.2k|fsfilter.sys;fsgk.2k|fsgk.sys InstallFSPKIH=0 InstallNetworkProvider=0 InstallGINA=0 RedefineSettings=0 ServiceProviderMode=0 MibVersion= GatekeeperVersion= StatisticsFilterPattern1=	これらの設定は>変更しないfc>でください。
UseOnlyUID=	0 = 利用可能な識別情報 (DNS 名、IP アドレス、WINS 名、固有の ID) を使用して、ポリシー マネージャ サーバと通信します。 1 = 固有の ID のみを使用して、管理エージェントと通信します。
Debug=1	0 = デバッグ情報を生成しません (デフォルト)。 1 = インストールおよびアンインストール時にデバッグログにデバッグ情報を書き込みます。
InstallMode=0 | 1	ネットワーク クライアントをインストールする際に、コンポーネントを必ずインストールします。コンポーネントの`RequestInstallMode`または`InstallMode`の設定を変更する必要はありません。

[PMSUINST.DLL]	ポリシー マネージャサポートの設定
RequestInstallMode=0	ネットワーク クライアントをインストールする際に、コンポーネントを必ずインストールします。コンポーネントの`RequestInstallMode`または`InstallMode`の設定を変更する必要はありません。
FsmsServerUrl=http://fsmsserver	ポリシー マネージャ サーバの URL。

[PMSUINST.DLL]	ポリシー マネージャサポートの設定
FsmsExtensionUri=/fsms/fsmsh.dll	この設定は変更しないでください。
FsmsCommdirUri=/commdir	この設定は変更しないでください。
Debug=1	0 = デバッグ情報を生成しません (デフォルト)。 1 = インストールおよびアンインストール時にデバッグログにデバッグ情報を書き込みます。
InstallMode=0 | 1	ネットワーク クライアントをインストールする際に、コンポーネントを必ずインストールします。コンポーネントのRequestInstallModeまたInstallModeの設定を変更する必要はありません。

[FSAVINST.DLL]	クライアント セキュリティ - ウイルス保護の設定
RequestInstallMode=1	0 = コンポーネントをInstallModeの設定で定義されているようにインストールします。 1 = バージョンがより新しい、またはインストールされていない場合に、コンポーネントをインストールします(デフォルト)。 2 = 既存のバージョンがインストールされていない、または同じあるいは旧バージョンが存在している場合に、コンポーネントをインストールします。
EnableRealTimeScanning=1	0 = リアルタイム スキャンを無効にします。 1 = リアルタイム スキャンを有効にします (デフォルト)。
Debug=1	0 = デバッグ情報を生成しません (デフォルト)。 1 = インストールおよびアンインストール時にデバッグ ログにデバッグ情報を書き込みます。
InstallMode=0 | 1	0 = コンポーネントをインストールしません (デフォルト)。 1 = 新しいバージョンがすでに存在している場合を除き、コンポーネントをインストールします

[FSSGSUP.DLL]	競合検出/削除モジュールの設定
RequestInstallMode=1	コンポーネントをインストール中に実行します。コンポーネントのRequestInstallModeまたInstallModeの設定を変更する必要はありません。
Debug=0 | 1	0 = デバッグ情報を生成しません (デフォルト)。

[FSSGSUP.DLL]	競合検出/削除モジュールの設定
	1 = インストールおよびアンインストール時にデバッグログにデバッグ情報を書き込みます。
InstallMode=0 | 1	コンポーネントをインストール中に実行します。コンポーネントのRequestInstallModeまたInstallModeの設定を変更する必要はありません。
SidegradeAction=0	0 = 競合するソフトウェアをすべて自動的に削除します (デフォルト)。 1 = 競合するソフトウェアが検出された場合、インストールをキャンセルします。

[ES_Setup.DLL]	メール スキャンのインストール設定
RequestInstallMode=1	0 = コンポーネントをInstallModeの設定で定義されているようにインストールします。 1 = バージョンがより新しい、またはインストールされていない場合に、コンポーネントをインストールします(デフォルト)。 2 = 既存のバージョンがインストールされていない、または同じあるいは旧バージョンが存在している場合に、コンポーネントをインストールします。
Debug=0 | 1	0 = デバッグ情報を生成しません (デフォルト)。 1 = インストールおよびアンインストール時にデバッグログにデバッグ情報を書き込みます。
InstallMode=0 | 1	0 = コンポーネントをインストールしません (デフォルト)。 1 = 新しいバージョンがすでに存在している場合を除き、コンポーネントをインストールします

[FWESINST.DLL]	共通の内部コンポーネント **FWES** の設定
RequestInstallMode=1	0 = コンポーネントをInstallModeの設定で定義されているようにインストールします。 1 = バージョンがより新しい、またはインストールされていない場合に、コンポーネントをインストールします(デフォルト)。 2 = 既存のバージョンがインストールされていない、または同じあるいは旧バージョンが存在している場合に、コンポーネントをインストールします。
Debug=0 | 1	0 = デバッグ情報を生成しません (デフォルト)

[FWESINST.DLL]	共通の内部コンポーネント **FWES** の設定
	1 = インストールおよびアンインストール時にデバッグログにデバッグ情報を書き込みます。
InstallMode=0 | 1	0 = コンポーネントをインストールしません (デフォルト)。 1 = 新しいバージョンがすでに存在している場合を除き、コンポーネントをインストールします

[FWINST.DLL]	クライアント セキュリティ - インターネット防御の設定
RequestInstallMode=1	0 = コンポーネントを`InstallMode`の設定で定義されているようにインストールします。 1 = バージョンがより新しい、またはインストールされていない場合に、コンポーネントをインストールします(デフォルト)。 2 = 既存のバージョンがインストールされていない、または同じあるいは旧バージョンが存在している場合に、コンポーネントをインストールします。
Debug=0 | 1	0 = デバッグ情報を生成しません (デフォルト)。 1 = インストールおよびアンインストール時にデバッグログにデバッグ情報を書き込みます。
InstallMode=0 | 1	0 = コンポーネントをインストールしません (デフォルト)。 1 = 新しいバージョンがすでに存在している場合を除き、コンポーネントをインストールします
InstallDC=0 | 1	0 = ダイヤルアップ制御をインストールしません (デフォルト)。 1 = ダイヤルアップ制御をインストールします
InstallNetworkQuarantine=0 | 1	0 = ネットワーク隔離をインストールしません (デフォルト)。 1 = ネットワーク隔離をインストールします。
DisableWindowsFirewall=0 | 1	0 = Windows Firewall (XP SP2 以降) を無効にしません (デフォルト)。 1 = インターネット防御のインストール後にWindows Firewall を無効にします。

[FSBWINST.DLL]	自動更新エージェントの設定
RequestInstallMode=1	0 = コンポーネントをInstallModeの設定で定義されているようにインストールします。 1 = バージョンがより新しい、またはインストールされていない場合に、コンポーネントをインストールします(デフォルト)。 2 = 既存のバージョンがインストールされていない、または同じあるいは旧バージョンが存在している場合に、コンポーネントをインストールします。
InstallMode=0 | 1	0 = コンポーネントをインストールしません (デフォルト)。 1 = 新しいバージョンがすでに存在している場合を除き、コンポーネントをインストールします

[FSPSINST.DLL]	クライアント セキュリティ - ネットワーク スキャナの設定
RequestInstallMode=1	0 = コンポーネントをInstallModeの設定で定義されているようにインストールします。 1 = バージョンがより新しい、またはインストールされていない場合に、コンポーネントをインストールします(デフォルト)。 2 = 既存のバージョンがインストールされていない、または同じあるいは旧バージョンが存在している場合に、コンポーネントをインストールします。
Debug=0 | 1	0 = デバッグ情報を生成しません (デフォルト)。 1 = インストールおよびアンインストール時にデバッグログにデバッグ情報を書き込みます。
InstallMode=0 | 1	0 = コンポーネントをインストールしません (デフォルト)。 1 = 新しいバージョンがすでに存在している場合を除き、コンポーネントをインストールします
DisableScanningForApps= Wget.exe,mplayer.exe	特定の実行可能ファイルに対して、ネットワークスキャナを無効にします。 これは、実行可能ファイル名(パスを除く) をカンマで区切った一覧です。 注: 項目の間にスペースは使用できません。
EnableHTTPScanning=1	0 = HTTP スキャンを無効にします。 1 = HTTP スキャンを有効にします。

[FSPSINST.DLL]	クライアント セキュリティ - ネットワーク スキャナの設定
StartImmediatelyForApps= iexplore.exe、firefox.exe、netscape.exe、opera.exe、msimn.exe、outlook.exe、mozilla.exe	この設定はどの実行可能ファイルが HTTP スキャンを開始するか定義します。他の処理は、外部サーバポート (80) への最初のアクセス時にスキャン モードに入るようになります。 これは、実行可能ファイル名 (パスを除く) をカンマで区切った一覧です。 注: 項目の間にスペースは使用できません。

[FSNACINS.DLL]	Cisco NAC プラグインの設定
RequestInstallMode=1	`0` = コンポーネントを`InstallMode`の設定で定義されているようにインストールします。 `1` = バージョンがより新しい、またはインストールされていない場合に、コンポーネントをインストールします(デフォルト)。 `2` = 既存のバージョンがインストールされていない、または同じあるいは旧バージョンが存在している場合に、コンポーネントをインストールします。
CTAversion=1.0.55	`CTAversion`CTA バージョンはパッケージに含まれている Cisco TrustAgent のバージョンを定義します。Cisco Trust Agent のインストール パッケージは、`ctasetup.msi`を`prodsett.ini`が保存されているフォルダと置換することによって更新できます。
Debug=0 | 1	`0` = デバッグ情報を生成しません (デフォルト)。 `1` = インストールおよびアンインストール時にデバッグログにデバッグ情報を書き込みます。
InstallMode=0 | 1	`0` = コンポーネントをインストールしません (デフォルト)。 `1` = 新しいバージョンがすでに存在している場合を除き、コンポーネントをインストールします

第
15
章

メール スキャンの警告とエラー メッセージ

トピック：

- 警告とエラー メッセージ

メールスキャンが生成する警告とエラー メッセージの一覧

警告とエラー メッセージ

ここでは、メール スキャンが生成する警告とエラー メッセージについて説明します。

件名	メッセージ ID	説明	内容
メール スキャンのセッションが失敗しました: システム エラー	602		システム エラーによって、メール スキャンがサーバ(<サーバ名>)の接続を切断しました。メール スキャンは引き続き機能しています。
メール スキャンの誤動作: システム エラー	603		重大なエラーによってメール スキャンが機能していません。引き続き問題が発生する場合、システム管理者に問い合わせしてください。
メール スキャンのメッセージ パーサーが失敗しました: システム エラー	604		パーサー エラーによってメールをスキャンできませんでした。セッションは停止されていません。
メール スキャンの初期化が失敗しました	610		メール スキャンの初期化が失敗しました。原因: <原因については、上記を参照してください>
添付ファイルに対するウイルス警告	620-623	ウイルスが検出された場合、F-Secure クライアント セキュリティの設定に基づいてウイルスが処理されます。 実行できるオプション: • レポートのみ • ウイルスの駆除 • 添付ファイルの削除 • メールのブロック	メール ウイルスの警告 感染: <ウイルスの名前> 添付ファイル: <メールに添付されている感染ファイル> 処理:<実行された処理> メッセージ<メッセージ ID> 送信者: <メール ヘッダ: 送信者のメール アドレス> 送信先: <メール ヘッダ: 送信先のメール アドレス>

件名	メッセージ ID	説明	内容
			件名: <メール ヘッダ: メールの件名>
不正な形式のメールに対する警告	630-633	不正な形式のメッセージが検出された場合、F-Secure クライアント セキュリティの設定に基づいてメールが処理されます。 実行できるオプション: • レポートのみ • 不正な部分の削除 • メールのブロック	不正な形式のメールに対する警告 説明:<不正な形式の説明> メールの部分: <不正な形式の部分> 処理:<実行された処理> メッセージ<メッセージ ID> 送信者: <メール ヘッダ: 送信者のメール アドレス> 送信先: <メール ヘッダ: 送信先のメール アドレス> 件名: <メール ヘッダ: メールの件名>
添付ファイルのスキャン エラー	640-643	スキャンが失敗した場合、メッセージは設定に基づいて処理されます。 スキャン エラーの原因: • ファイルのスキャンでタイムアウトが発生しました。 • メール スキャンでタイムアウトが発生しました。 • 添付ファイルがパスワードで保護されている圧縮ファイルです。 • 添付ファイルのスキャン中にエラーが発生しました(ディスク容量やメモリ不足)。 実行できるオプション • レポートのみ • 添付ファイルの削除 • メールのブロック	添付ファイルのスキャン エラー 原因:<スキャン エラーの説明> 添付ファイル: <スキャン エラーの原因となった添付ファイル> 処理:<実行された処理> メッセージ<メッセージ ID> 送信者: <メール ヘッダ: 送信者のメール アドレス> 送信先: <メール ヘッダ: 送信先のメール アドレス> 件名: <メール ヘッダ: メールの件名>

第
16
章

インストール中に検出される競合製品

トピック：

- *検出される競合製品*

ここで掲載されている製品は、F-Secureクライアント セキュリティのインストール中に検出され、ユーザは手動でアンインストールすることができます。または、自動でアンインストールされます。

検出される競合製品

以下のセキュリティ製品は、本製品のインストール中に検出されます。

- Agnitum Outpost Firewall Pro 1.0
- AOL Safety and Security Center
- avast! Antivirus
- AVG Anti-Virus 7.0
- AVG Free Edition
- AVG Anti-Virus 7.1
- AVG 7.5
- Avira AntiVir PersonalEdition Classic
- Avira AntiVir PersonalEdition Premium
- Avira AntiVir Windows Workstation
- Avira Premium Security Suite
- BitDefender Antivirus v10
- BitDefender Antivirus Plus v10
- BitDefender 8 Free Edition
- BitDefender 9 Internet Security
- BitDefender Internet Security v10
- BitDefender 9 Professional Plus
- BitDefender 9 Standard
- BitDefender Total Security 2008
- Bsecure Internet Protection Services v.4.5
- BullGuard 7.0
- CA Anti-Virus
- CA eTrust Antivirus
- eTrust EZ Antivirus
- ファイアウォール
- CA Internet Security Suite
- Cisco VPN Client Firewall
- Dr Solomon's VirusScan
- EarthLink Protection Control Center
- EarthLink Software
- EarthLink Toolbar
- EMBARQ Toolbar (Powered by EarthLink)
- PC Antivirus
- F-PROT Antivirus for Windows
- FortiClient
- F-Secure Anti-spyware
- F-Secure Anti-Virus Client Security
- 互換性のない F-Secure 製品
- 破損している、またはインストールが不完全の製品
- F-Secure VPN+ Client
- G DATA AntiVirenKit (ドイツ版のみ)
- G DATA InternetSecurity (ドイツ版のみ)
- G DATA TotalCare (ドイツ版のみ)
- AntiVirenKit 2005

- H+BEDV AntiVir Personal Edition
- iProtectYou 7.09
- Jiangmin Antivirus Software (英語版のみ)
- K7 TotalSecurity 2006
- Kaspersky Anti-Spam Personal
- Kaspersky Anti-Virus 6.0 (英語版のみ)
- Kaspersky Internet Security 6.0 (英語版のみ)
- Kaspersky Internet Security 7.0 (英語版のみ)
- Kaspersky(TM) Anti-Virus Personal 4.0
- Kaspersky(TM) Anti-Virus Personal Pro 4.0
- Kaspersky(TM) Anti-Virus Personal 4.5
- Kaspersky Anti-Virus Personal Pro
- Kaspersky Anti-Virus Personal
- Kerio Personal Firewall
- Kingsoft Internet Security (英語版のみ)
- McAfee SecurityCenter
- McAfee VirusScan
- McAfee VirusScan Enterprise
- McAfee VirusScan Home Edition
- McAfee Internet Security
- McAfee Uninstall Wizard
- McAfee Personal Firewall
- McAfee Personal Firewall Plus
- McAfee Privacy Service
- McAfee SecurityCenter
- McAfee SpamKiller
- McAfee VirusScan Professional Edition
- McAfee Total Protection
- McAfee Browser Protection Service
- McAfee Virus and Spyware Protection Service
- McAfee Personal Firewall Express
- McAfee Firewall Protection Service
- McAfee Firewall
- Windows Live OneCare
- NAI ePolicy Orchestrator Agent
- NIC v5.50
- Norman Personal Firewall 1.42
- Norman Virus Control
- NOD32 antivirus system (英語、フランス語、ドイツ語、ハンガリー語、ルーマニア語、スペイン語、簡体字中国語、繁体字中国語、チェコ語、クロアチア語、イタリア語、日本語、オランダ語、ポーランド語、ポルトガル語、ロシア語、スロベニア語の各言語版)
- PureSight Parental Control
- Radialpoint Security Services
- Radialpoint Servicepoint Agent 1.5.11
- Sophos Anti-Virus
- Sophos AutoUpdate
- Sophos Remote Management System
- Sunbelt Personal Firewall
- Norton AntiVirus 2003

- Norton AntiVirus 2005
- Norton 360
- Norton AntiVirus 2004 (Symantec Corporation)
- Norton AntiVirus
- Norton AntiVirus Corporate Edition
- Norton Internet Security
- Norton Internet Security 2005
- Norton Internet Security 2006 (Symantec Corporation)
- Norton Internet Security 2007
- Norton Internet Security 2008
- Norton Security Online
- Norton SystemWorks 2004 Professional (Symantec Corporation)
- Norton SystemWorks 2005 (Symantec Corporation)
- Norton Personal Firewall (Symantec Corporation)
- Norton Personal Firewall 2005
- Symantec AntiVirus
- Symantec AntiVirus Client
- Symantec Client Security
- Symantec Endpoint Protection
- LiveUpdate 1.7 (Symantec Corporation)
- LiveUpdate 1.80 (Symantec Corporation)
- LiveUpdate 2.6 (Symantec Corporation)
- LiveUpdate 1.6 (Symantec Corporation)
- LiveUpdate
- LiveUpdate 2.0 (Symantec Corporation)
- LiveUpdate 3.3 (Symantec Corporation)
- Panda Antivirus 2007
- Panda Antivirus + Firewall 2007
- Panda ClientShield
- Panda Internet Security 2008
- Panda Antivirus Platinum
- Panda Platinum Internet Security
- Panda Platinum 2005 Internet Security (英語版のみ)
- Panda Platinum 2006 Internet Security
- Panda Internet Security 2007
- Panda Titanium Antivirus 2004
- Panda Titanium Antivirus 2005 (英語版、フランス語版、スペイン語版のみ)
- Panda Titanium 2006 Antivirus + Antispyware
- Trend Micro Officescan (Windows 2000 のみ)
- Trend Micro OfficeScan Client
- PC-cillin 2003
- Trend Micro PC-cillin Internet Security 12
- Trend Micro PC-cillin Internet Security 2005
- Trend Micro PC-cillin Internet Security 2006
- Trend Micro Internet Security
- Trend Micro AntiVirus 2007
- Trend Micro PC-cillin Internet Security 2007
- Trend Micro Internet Security Pro
- ZoneAlarm
- ZoneAlarm Security Suite

- ZoomTownInternetSecurity v.4.5