F-Secure ポリシー マネージャ

管理者ガイド

目次

第 1 章：はじめに.....7

システム要件.....8

ポリシー マネージャ サーバ.....8

ポリシー マネージャ コンソール.....9

主要コンポーネント.....10

機能.....10

製品を登録する.....11

ポリシーベース管理.....12

マネージメント インフォメーション ベース.....13

第 2 章：インストール.....15

セキュリティに関する問題.....16

ポリシー マネージャをインストールする.....16

インストールの順序.....16

ポリシー マネージャ サーバをインストールする.....17

インストール パッケージのダウンロードと実行.....17

インストールするコンポーネントを選択する.....17

移行ウィザード.....18

インストールを完了する.....19

インストール後に製品の動作を確認する.....19

Web ブラウザのパスを変更する.....19

アンインストール.....19

第 3 章：ポリシー マネージャ コンソールの使用.....21

概要.....22

基本操作.....23

ログイン.....23

クライアント セキュリティの管理.....24

詳細モード.....24

ポリシー ドメイン ツリー.....24

詳細モードのコンテンツ.....25

「メッセージ」ウィンドウ.....26

ツールバー.....27

メニュー コマンド.....27

ドメインとホストの管理.....29

ポリシー ドメインを追加する....29
ホストを追加する....30
ソフトウェアの配布....33
インストール情報の送信....34
ポリシーベース インストール....36
パッケージを利用したローカル インストール/更新....38
情報の転送....40
ポリシーの管理....40
設定....40
配布していない変更を破棄する....41
制限....41
設定を変更する....41
ポリシーの継承....41
操作とタスクの管理....42
警告....42
警告とレポートの表示....42
警告転送の設定....43
レポート ツール....44
「ポリシー ドメイン/ホスト セレクタ」ウィンドウ....44
「レポート タイプ セレクタ」ウィンドウ....44
「レポート」ウィンドウ....45
下部ウィンドウ....45
レポートを表示およびエクスポートする....45
一般設定....46
一般設定 - 接続固有....46
一般設定 - 共有....47

第 4 章 : ポリシー マネージャ サーバのメンテナンス....49
ポリシー マネージャのデータをバックアップ/復元する....50
バックアップを作成する....50
バックアップを復元する....50
署名鍵をエクスポート/インポートする....51
イメージ ファイルを使用したソフトウェアの複製....51

第 5 章 : ウイルスのパターン ファイルを更新する....53
自動更新エージェントによる自動更新....54
自動更新エージェントの動作....54
自動更新エージェントのメリット....54
自動更新エージェントを使用する....55
自動更新エージェントを設定する....55

ログ ファイルを確認する....56
自動更新エージェントを使用して、新しい更新を確認する....57
手動更新....57
トラブルシューティング....57

第 6 章 : Linux での使用....59
概要....60
インストール....60
自動更新エージェントとポリシー マネージャ サーバをインストールする....61
ポリシー マネージャ コンソールをインストールする....62
アンインストール....63
FAQ....64

第 7 章 : Web レポート....69
レポートを生成/表示する....70
レポートを生成する....70
印刷用のレポートの作成....70
レポートを自動的に生成する....71
Web レポートの管理....71
Web レポートのエラー メッセージとトラブルシューティング....71
エラー メッセージ....71
トラブルシューティング....72
Web レポートのポートを変更する....72

第 8 章 : ポリシー マネージャ プロキシ....73
概要....74

第 9 章 : トラブルシューティング....75
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....76
ポリシー マネージャWeb レポート....79
ポリシーの配布....80

第 10 章 : llaunchr のエラー コード....81
エラー コード....82

第 11 章 : FSII リモート インストールのエラー コード....85
エラー コード....86

第 12 章 : ネットマスクの NSC 表記.....89
NSC 表記について.....90

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*
- *ポリシーベース管理*

「ポリシー マネージャ」は、ネットワークに分散している複数のコンピュータとアプリケーションのセキュリティを一元集中管理するプログラムです。

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 ポリシー設定および配布
- 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)

システムを設定した後、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されます。この画面で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素早く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 Linux : • Red Hat Enterprise Linux 4/5/6 • CentOS 5 • openSUSE Linux 11 • SUSE Linux Enterprise Server 10/11 • SUSE Linux Enterprise Desktop 11 • Debian GNU Linux 5 • Ubuntu 8.04/10.04
プロセッサ:	P4 2Ghz またはマルチコア 3GHz 以上のプロセッサ (オペレーティング システムと管理環境のサイズによる)。
メモリ:	1□2 GB RAM (オペレーティング システムと管理環境のサイズによる)。
ディスク容量:	6□10 GB の空き容量 (管理環境のサイズによる)。
ネットワーク:	100 Mbit ネットワーク。

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 Linux: • Red Hat Enterprise Linux 4/5/6 • CentOS 5 • openSUSE Linux 11 • SUSE Linux Enterprise Server 10/11 • SUSE Linux Enterprise Desktop 11 • Debian GNU Linux 5 • Ubuntu 8.04/10.04
プロセッサ:	P4 2 GHz 以上のプロセッサ。
メモリ:	512 MB□1 GB 以上 (オペレーティング システムと管理環境のサイズによる)。
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:	100 Mbit ネットワーク。

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。

ポリシーベース管理

「セキュリティ ポリシー」は、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、企業や大規模な環境で最適なセキュリティ管理を実現するために、管理者が設定したポリシーを使用します。ポリシーベース管理では、以下のような機能が実行されます。

- 製品のリモート制御と動作の監視
- 製品と管理エージェントから提供される統計情報の監視
- 定義済み操作のリモート起動
- 警告と通知の転送

ポリシー マネージャ コンソールとホストの間の通信は、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 ファイルには、以下の3種類があります。

- *デフォルト ポリシー ファイル* (`.dpf`)
- *ベース ポリシー ファイル* (`.bpf`)
- *インクレメンタル ポリシー ファイル* (`.ipf`)

製品の設定は、この3種類のポリシー ファイルで構成されます。

デフォルト ポリシー ファイル	デフォルト ポリシー ファイルには、セットアップ プログラムによってインストールされた製品のデフォルト値が含まれます。デフォルト ポリシーは、ホストでのみ使用されます。ベース ポリシー ファイルとインクレメンタル ポリシー ファイルのどちらにも変数のエントリがない場合、デフォルト ポリシー ファイルの値が使用されます。製品がバージョン アップすると、デフォルト ポリシー ファイルも新しく更新されます。
ベース ポリシー ファイル	ベース ポリシー ファイルには、特定のホストにあるF-Secure製品のすべての変数の管理設定と制限が含まれます (ドメイン レベルのポリシーでは、ホスト グループが同じファイルを共有する場合があります)。ベース ポリシー ファイルはポリシー マネージャ コンソールにより署名され、ネットワークを通過している間、およびホストのファイル システムに格納されている間、変更されないように保護されます。これらのファイルは、ポリシー マネージャ コンソールからポリシー マネージャ サーバに送信されます。ホストは、新しいポリシーがあるか、ポリシー マネージャ コンソールを定期的にポーリング (確認) します。
インクレメンタル ポリシー ファイル	インクレメンタル ポリシー ファイルは、ベース ポリシーに対してローカルで行った変更を保存するために使用されます。ベース ポリシーで指定した制限の範囲内であれば、変更が可能です。インクレメンタル ポリシー ファイルは、管理者が設定と統計を参照できるように、定期的にポリシー マネージャ コンソールへ送信されます。

マネージメント インフォメーション ベース

MIB (*Management Information Base: マネージメント インフォメーション ベース*) は、*SNMP* (*Simple Network Management Protocol: 簡易ネットワーク管理プロトコル*) で使用される階層管理用のデータ構造です。

ポリシー マネージャは、ポリシーファイルの内容を定義するために MIB 構造を使用します。個々の変数にはオブジェクト*識別子* (*OID*) と*ポリシー API* を使用してアクセスできる値があります。F-Secure MIB のコンセプトには、SNMP MIB の基本的な定義に加え、完全なポリシーベース管理を実現するために必要な拡張機能が数多く含まれています。

以下のカテゴリが製品の MIB で定義されます。

設定	ワークステーションを SNMP 方式で管理するために使用されます。管理される製品の動作は、このカテゴリで指定した内容によって制限されます。
統計	製品の統計情報をポリシー マネージャ コンソールへ送信します。
操作	操作は2つのポリシー変数で処理されます。1つは操作の識別子をホストへ転送する変数です。もう1つは、実行された操作をポリシー マネージャ コンソールに通知する変数です。後者の変数は通常の統計情報を使用して転送され、前に行われた操作がすべて同時に認識されます。操作を編集するカスタム エディタはサブツリーに関連付けられており、2つの変数はエディタで非表示になります。
プライベート	管理コンセプトの MIB には、製品がセッションの内部で使用される変数も含まれています。これにより、本製品は Windows レジストリ ファイルのような外部サービスに依存する必要はありません。
トラップ	「トラップ」は、ローカル コンソール、ログ ファイル、リモート管理プロセスなどに送られる、警告やイベントに関するメッセージです。ほとんどのF-Secure製品は、以下のトラップを送信します。 情報。ホストからの操作情報を示します。 警告。ホストからの警告を示します。 エラー。ホスト上の回復可能なエラーを示します。 重大なエラー。ホスト上の回復不可能なエラーを示します。 セキュリティ警告。ホスト上のセキュリティ アラート (警告) を示します。

第
2
章

インストール

トピック：

- *セキュリティに関する問題*
- *ポリシー マネージャをインストールする*
- *インストールの順序*
- *ポリシー マネージャ サーバをインストールする*
- *Web ブラウザのパスを変更する*
- *アンインストール*

ここでは、ポリシー マネージャをアンインストールする方法について説明します。

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。

セキュリティに関する問題

ポリシー マネージャ サーバは *Jetty Web* のサーバテクノロジを使用しています。Jetty やセキュリティに関する情報は、次のサイトで参照できます。

Jetty セキュリティ レポート - *http://docs.codehaus.org/display/JETTY/Jetty+Security*.

注: リリースノートには、インストールおよびセキュリティに関する重要な情報が記載されているので、必ずお読みください。

ポリシー マネージャをインストールする

ポリシー マネージャは、複雑なネットワークにおいて、F-Secureのアンチウイルス製品を集中管理するために設計されており、インターネットなどの公共ネットワークで使用することは推奨されていません。

注: 高いセキュリティが必要とされる環境でポリシー マネージャをインストールする場合、*管理ポート* (デフォルトでは8080) と*ホストのポート* (デフォルトでは80) がインターネットに表示されないようにしてください。

セキュリティ機能

ポリシー マネージャのアクセスはアカウントのあるユーザに限られます。権限のないユーザはホストに変更を適用することはできません。

コンポーネントを別々にインストールする代わりに、ポリシー マネージャ コンソールとポリシー マネージャ サーバを同じマシンにインストールした上で、アクセスをローカルに限定し、ポリシーマネージャ コンソールへのリモート アクセスをリモート デスクトップのプログラムに制限する方法があります。

ポリシー マネージャ サーバは HTTPS プロトコルを利用してポリシー マネージャ コンソールと保護された状態で通信します。

Web レポートをインストールする

Web レポートは、ウイルス保護のステータスや警告などに関する視覚的なレポートを生成する機能で、インターネットなどの公共ネットワークで使用することは推奨されていません。

高度なセキュリティが必要とされる場合、ポリシー マネージャ コンソールのアクセスをローカルに限定することでセキュリティを強化できます。

インストールの順序

ポリシー マネージャを別々のマシンにインストールする場合、関連するコンポーネントを特定の順序でインストールする必要があります。

ポリシー マネージャのインストールを行う際には、各コンポーネントを次の順序でインストールしてください。(ポリシー マネージャ サーバとポリシー マネージャ コンソールを同じコンピュータにインストールしている場合、両方のコンポーネントがまとめてインストールされます)。

1. ポリシー マネージャ サーバ

2. ポリシー マネージャ コンソール
3. 管理対象の各アプリケーション

ポリシー マネージャ サーバをインストールする

ここでは、ポリシー マネージャ コンソールをインストールする方法について説明します。

ポリシー マネージャ サーバをインストールする前に、対象となるマシンにアクセスできることを確認します。

ポリシー マネージャ サーバは HTTPS プロトコルを利用してコンポーネントと保護された状態で通信します。

ポリシー マネージャ サーバが保存する情報には次のものが含まれています。

- ポリシー ドメイン構造
- ポリシー データ
- ユーザ アカウントの情報
- ポリシー データから生成されるベース ポリシー ファイル
- ステータス情報 (インクレメンタル ポリシー ファイル、警告、レポートなど)
- ホストから送信される自動登録依頼
- 製品のインストール パッケージとパターン ファイルの更新パッケージ
- ホストに関するデータ

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. admin アカウントのパスワードを指定して、[次へ] をクリックします。

   このパスワードを admin アカウントと使用して ポリシー マネージャ コンソール にログインしてください。

5. 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 ポートを変更する場合、ポリシー マネージャ コンソールにログインするときに新しいポート番号を [接続] の URL に含める必要があります。

     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。

6. [次へ] をクリックします。

移行ウィザード

インストール中に移行ウィザードが自動で立ち上がり、以前インストールしたポリシー マネージャのデータをインポートできます。

移行ウィザードは、ポリシー マネージャの旧バージョンからアップグレードしているときに表示されますが、ポリシー マネージャの旧データが見つからない場合、ウィザードは立ち上がりません。

移行ウィザードが表示されない場合、またはデータを後でインポートしたい場合、`<F-Secure>\Management Server 5\bin\fspms-migration-wizard.exe` を実行することで移行ウィザードをいつでも起動できます。

1. 旧バージョンの通信ディレクトリと鍵ペアのパスを入力して、[次へ] をクリックします。
2. ポリシー ドメインの情報を確認して、[スタート] をクリックします。
3. データのインポートが完了したら、[閉じる] をクリックしてウィザードを閉じます。

インストール ウィザードが再度表示されます。

注: ポリシー マネージャの旧バージョンの通信ディレクトリと署名鍵はアップグレード後に削除されません。旧バージョンにデータに戻すことは可能です。

注: アップグレード中に、ポリシー ベースのインストール操作とホストが切断とみなされるまでの時間に関連する設定はインポートされません。時間の設定は、ツール > サーバの構成 ウィンドウで指定できます。

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。

インストール後に製品の動作を確認する

インストールが完了したら、製品の動作を確認します。

インストール後に製品の動作を確認するには

1. ポリシー マネージャ サーバをインストールしたマシンの Web ブラウザを開きます。
2. Web ブラウザのアドレス フィールドに `https://localhost:8080` を入力します (「8080」はポート番号。別のポート番号を指定した場合、その番号を指定します)。
   インストールが正常に完了している場合、次のページが表示されます。

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。また、F-Secureの同製品をインストールする場合にも必要です。

第
3
章

ポリシー マネージャ コンソールの使用

トピック：

- *概要*
- *基本操作*
- *ドメインとホストの管理*
- *ソフトウェアの配布*
- *ポリシーの管理*
- *操作とタスクの管理*
- *警告*
- *レポート ツール*
- *一般設定*

ここではポリシー マネージャ コンソールの機能と設定について説明します。

ポリシー マネージャ コンソールは、F-Secureのセキュリティ製品をリモート管理するためのツールで、ネットワークに必要なセキュリティ管理機能と共通のプラットフォームを提供します。

概要

ここでは、ポリシー マネージャ コンソールのコンセプトについて説明します。

ポリシーマネージャコンソールを利用して、複数のホストをポリシードメイン内でグループ化して、管理を行うことが可能です。ポリシーはホスト別に指定できます。特定のホストに複数のユーザがある場合、ホストの全ユーザが同じポリシー (設定) を共有することになります。

管理者は、それぞれのホストに対して異なるセキュリティポリシーを作成できます。また、複数のホストに1つのポリシーを作成することもできます。ポリシーはネットワークを通じてホスト、サーバ、セキュリティ ゲートウェイに配布できます。

管理者はポリシー マネージャ コンソールで次の操作を行うことができます。

- 管理対象製品の属性値の設定
- 属性値を、ユーザが表示または変更できるように設定決定
- ホストのグループ化
- ホストとドメインの管理
- 属性値や制限など、署名されたポリシーの生成
- ステータスの表示
- 警告の処理
- F-Secureのスキャン レポートの処理
- リモート インストール
- レポートを HTML 表示、エクスポート

ポリシー マネージャ コンソールはポリシーを生成し、ステータスと警告を表示します。各ホストは、ポリシーを実施するために管理エージェントを利用します。

読み取り専用のユーザは次の操作を行うことができます。

- ポリシー、統計情報、操作ステータス、インストールされている製品のバージョン番号、警告、およびレポートの表示
- ポリシー マネージャ コンソールの設定の変更 (ユーザ単位でインストールされるので、変更は他のユーザには影響しません)

読み取り専用モードでは、次のタスクを実行することはできません。

- ドメイン構造やドメインとホストの設定の変更
- 製品の設定の変更
- 操作の実行
- 製品のインストール
- ポリシーデータの保存
- ポリシーの配布
- 警告やレポートの削除

基本操作

ここでは、ポリシーマネージャコンソールのログイン方法、メニューコマンド、基本操作について説明します。

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設定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ユーザ名とパスワードを入力します。ユーザ名とパスワードはポリシーマネージャに特有の情報でネットワーク管理者のパスワードではありません。`admin` ユーザ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す。他のユーザはポリシー マネージャ コンソールで作成できます。

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 HTTPS URL として定義されます。

[表示] 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。

ユーザを追加する

ポリシー マネージャにアクセスできるユーザ (管理者/読み取り専用) を追加または削除できます。

1. メニューから ツール > ユーザ を選択します。
   「ユーザ」ウィンドウが表示されます。
2. [追加] をクリックして、新しいユーザを追加します。
3. 新しいユーザのユーザ名とパスワードを指定します。
4. ユーザのアクセスを制限する場合、[読み取り専用アクセス] を選択して [**OK**] をクリックします。
   新しいユーザがユーザの一覧に表示され、ポリシー マネージャにアクセスできるようになります。

注: 管理者権限のあるユーザは他のユーザを削除することができます。管理者権限のあるユーザは少なくても1人必要です。ログイン中のユーザが削除された場合、そのユーザはポリシー マネージャからログオフされます。

パスワードを変更する

ポリシー マネージャにログインしているときに、ユーザ アカウントのパスワードを変更できます。

1. メニューから ツール > パスワードを変更 を選択します。
2. 新しいパスワードを指定して [**OK**] をクリックします。

パスワードが変更されます。

クライアント セキュリティの管理

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、アンチウイルス モードのユーザ インターフェースが開きます。

このモードは、クライアントセキュリティを管理するために最適です。アンチウイルスモードのユーザインターフェースでは、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 サーバを管理するためのタスクをほとんど実行できます。

アンチウイルス モードのユーザ インターフェースからほとんどの管理タスクを実行できますが、クライアント セキュリティ以外の製品を管理する場合、詳細モードのユーザ インターフェースが必要になります。

詳細モード

ユーザインターフェースを「アンチウイルスモード」から「詳細モード」に変更すると、ポリシーマネージャの機能をすべて使用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 [表示] メニューの [詳細モード] から選択できます。

ポリシー ドメイン ツリー

ポリシー ドメイン ツリーで、ポリシー ドメインとホストに関連する処理を行うことができます。

ポリシー ドメイン ツリーでは、以下の操作を実行できます。

- ポリシー ドメインの追加 (ツールバーの 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。
- ホストの追加 (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。
- 新しいホストをインポート。
- 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。

ドメイン/ホストを選択し、[編集] メニューから上記の操作を行えます。

上記の「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。

詳細モードのコンテンツ

詳細モードのメイン ウィンドウの機能は、開いているタブによって異なります。

- 「ポリシー」タブ - ポリシー変数の値を設定することができます。指定/変更した値は選択したポリシー ドメインとホストに反映されます。ポリシー変数に、あらかじめ定義されたエディタが用意されています。
- 「ステータス」タブ - ホストが報告したローカルの変更を表す「設定」と統計情報が表示されます。
- 「警告」タブ - 警告に関する情報の詳細を確認できます。
- 「スキャン レポート」タブ - レポートに関する情報や詳細を確認できます。
- 「インストール」タブ - インストール情報を表示および編集できます。

ポリシー マネージャ コンソールの従来の **MIB** ツリーでは、すべての設定/操作 (ポリシー) とローカル設定/統計情報 (ステータス) が製品コンポーネント固有の **MIB** ツリーで表示されます。

ヘルプを使用する

「ポリシー」タブで **MIB** ツリー モードを選択すると、参考用の説明が表示されます。

ポリシーの設定を編集する

共通のポリシー設定を変更できます。

管理対象の製品 (管理エージェントなど) と「ポリシー」タブを選択します。ツリー ノードをクリックすると、選択した製品の設定を編集できる画面が表示されます。

ポリシーの設定を編集して、エンドユーザのアクセス権 (変更の許可/拒否) を指定できます。

ポリシーの設定を指定する

ほとんどのポリシー設定ページではテキストまたはドロップダウン フィールドを使用して設定を指定できます。

フィールドに加え、次の3つのボタンを使用してポリシーの値を設定できます: 消去、強制的に値を適用、ドメインの値を表示

消去

[値を消去] は指定の値を消去します。値を消去すると、継承された値 (グレーのテキスト) がフィールドに表示されるか、または何も表示されません。[値を消去] は、指定のドメイン/ホストに対して値が定義されている場合に使用できます。

強制的に値を適用

[強制的に値を適用] 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ます。このコマンドは、指定した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。この操作は、ドメインの下にあるサブドメインとホストの設定を消去して、サブドメインとホストにドメインの値を継承できるようにします。サブドメインとホストの値はすべて破棄され、復元することができませんので、このコマンドを使用するときには注意してください。

ドメインの値を表示

[ドメインの値を表示] 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ます。このコマンドは指定したポリシー ドメインの下にあるポリシー 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。

ドメイン名やホスト名をクリックすると、ドメイン/ホストをすばやく選択できます。また、「ドメインの値」ウィンドウを同時に複数開くことが可能です。

ステータスを表示する

メイン ウィンドウでポリシー ドメインの設定と統計情報を表示できます。

ステータスを表示するには

1. 「ステータス」タブを開きます。
2. 製品を選択します。
   ポリシー マネージャ コンソール選択した製品に対する「製品ビュー」が表示され、重要なローカル設定と統計情報を確認できます。

   注: 値を編集することはできませんが、フィールドまたはフィールド ラベルをクリックして **MIB** ヘルプを表示することはできます。

   対象がポリシー ドメインの場合、「ステータス」タブにドメイン レベルのステータス概要 (ドメイン内のホスト数と切断されたホスト) が表示されます。
3. 切断されたホストをクリックすると、表示対象が指定のホストに切り替わります。
   これにより、切断されたホストが切断前に警告や統計情報を送信したか調べることができます。この情報から、ホストが切断した原因を探ることができます。原因が明確の場合、(たとえば、ホストのF-Secure製品がアンインストールされたなど) ホストを安全に削除できます。
4. 切断されたホストを調べ終わった後にツールバーの ボタンをクリックすると、以前選択していたドメイン レベルに戻ることができます。
   「ドメインのステータス」ビューで、切断されたホストを一括で処理できるオプションが2つあります。1) 切断されたすべてのホストを選択する、2) 切断されたすべてのホストを削除する。どちらの操作も切断されたホスト ツリーのルートを選択した状態のポップアップ メニューから実行できます。

   注意: 切断されたホストを削除する際には注意が必要です。ホストがモバイルのデバイスなどである場合、ホストが制限されている日数以上にネットワークから切断されている可能性があります。ホストを削除する前に、ツール > サーバの構成 > ホスト で切断に関する設定を必ず確認してください。ホストを削除すると、ホストに関連する警告、レポート、ステータス、およびポリシー設定のデータがなくなります。ポリシー マネージャからされたホストは自動要求メッセージを送信します。ドメイン ツリーでホストをもう一度インポートできますが、ポリシー マネージャは新しいホストが追加されたとみなします。

「メッセージ」ウィンドウ

ポリシー マネージャ コンソールは、イベントのメッセージを「メッセージ」ウィンドウに出力します。

「警告」ウィンドウや「スキャン レポート」ウィンドウとは異なり、「メッセージ」ウィンドウのイベントはポリシー マネージャ コンソールによって生成されます。

メッセージには、「情報」、「警告」、および「エラー」の3つのカテゴリ (重大度) があります。「メッセージ」タブには、カテゴリ別でメッセージが表示されます。ポップアップ メニューで表示されるカテゴリは、タブを右クリックすることで削除できます。個別のメッセージを右クリックすると、[切り取り]、[コピー]、および [削除] を実行できるポップアップ メニューが表示されます。

デフォルトでは、メッセージはポリシー マネージャ コンソールのローカル インストール先フォルダの「message」サブフォルダ内にある2ファイルに記録されます。メッセージのログは英語とポリシー マネージャ コンソールで指定した言語 (日本語) で保存されます。ログ ファイルは、各メッセージ カテゴリ (「メッ

セージ」ウィンドウのタブ名) に対して個別に作成されます。一般設定 > 場所ウィンドウからログ ファイルのフォルダを指定できます。

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、新規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。
または	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	ポリシーの配布	ポリシーを配布します。
	ポリシーの変更を破棄	配布されていないポリシーを破棄します。
	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。

メニュー	コマンド	処理
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。
	アクティブディレクトリの構成をインポートする	アクティブ ディレクトリのインポート ウィザードを開始します。
	新しいホストをインポート	ポリシー ドメインに追加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	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。
	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。
	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。

メニュー	コマンド	処理
	ユーザ	ポリシー マネージャのユーザを追加/削除できる「ユーザ」ウィンドウを開きます。
	パスワードを変更する	ユーザ アカウントのパスワード変更できる「パスワードを変更する」ウィンドウを開きます。
	サーバの構成	署名鍵のエクスポート/インポートおよびホストの切断/接続に関連する設定を指定できる「サーバの構成」ウィンドウを開きます。
	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。

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

アクティブ ディレクトリの構成からホストをインポートする

アクティブディレクトリの構成からポリシードメインの構成とホストをポリシーマネージャにインポートできます。

1. メニューから 編集 > アクティブ ディレクトリの構成をインポートする を選択します。
   「アクティブ ディレクトリの構成をインポートする」ウィザードが立ち上がります。
2. アクティブ ディレクトリ サーバの場所および読み取りアクセス以上の権限を持つユーザ名とパスワードを入力して、[次へ] をクリックします。
3. アクティブ ディレクトリのドメイン、インポートするコンテナおよびポリシー ドメインを指定して、[次へ] をクリックします。

   ホストを含むコンテナは強調されます。
4. インポート ルールを確認し、作成するルールを選択して [開始] をクリックします。
   ルールがホストに適用され、ポリシー マネージャに管理されるようになります。
5. インポートが完了したら、[閉じる] をクリックしてウィザードを閉じます。

アクティブディレクトリからインポートされたホストとアイテムがポリシーマネージャに表示されます。

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。

新しいホストをインポートする

「*新しいホストをインポート*」機能を使用することでもポリシー マネージャ コンソールにホストを追加できます。

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。

新しい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、

   - メニューから 編集 > 新しいホストをインポート を選択します。
   - 「インストール」ビューで [新しいホストをインポート] 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、新規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。「新規ホスト」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カスタムのプロパティも表示されます

2. 「新規ホスト」ビューでは、次の操作が可能です。

   - 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)
   - テーブルで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)

インポート ルール

「新しいホストをインポート」ウィンドウの「インポート ルール」タブで新規ホストのインポート ルールを設定できます。

インポート ルールは、サーバに接続する新規ホストに自動で適用できます。これにより、新規ホストがポリシー マネージャ サーバに接続するときにインポート ルールを手動で実行する必要はありません。新規ホストがルールに応じてドメインに追加されます。

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、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
  - 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。ポリシー マネージャ コンソールを閉じたら、非表示のカスタムのプロパティ名は削除されます。

   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、インポート ルールで使用することが可能になります。

3. 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。
   e) [新規ホストのサーバ接続時にルールを適用] を選択すると、新規ホストがサーバへ接続するときにルールが適用されます。

   ポリシー マネージャが新規インストールされた場合、このオプションは有効になります。アップグレードの場合、オプションは無効になります。

   - 新規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、「新規ホスト」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みなされます。

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 をクリックします。
   - 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。

切断したホストを自動的に処理する

ホストが切断とみなされるまでの日数と切断したホストの自動削除を設定することができます。

1. メニューから ツール > サーバの構成 を選択します。
2. [ホスト] を選択します。
3. ホストのステータスが「切断」になるまでの日数を [ホストを「切断」として判別するために必要な日数] に入力してください。
4. 切断しているホストがポリシー ドメインから自動で削除されるために必要な日数を [切断しているホストを削除するために必要な日数] に入力してください。
5. [**OK**] をクリックしてウィンドウを閉じます。

ホストのプロパティ

ここでは、ポリシー マネージャ コンソールで表示および編集できるホストのプロパティについて説明します。

ホストのプロパティを表示するには、対象のホストを右クリックして表示されるメニューから [プロパティ] を選択します (または Alt+Enter キーを押します)。

各ホストには UID が指定されています。OID はホストのステータスから取得された一意の識別子で、ポリシー マネージャ コンソールで変更することはできません。

[表示] フィールドでホストの表示名を指定できます。表示名を指定した場合、ドメイン ツリーで指定した表示名がホスト名の代わりに表示されます。

ソフトウェアの配布

ポリシー マネージャは、次のいずれかの方法で管理対象アプリケーションのインストールと更新を行うことができます。

インストール情報の送信	ポリシー マネージャはワークステーションにソフトウェアをインストールすることができます。[**Windows** ホストを自動検出] 機能を使用してワークステーションを参照するか、または [**Windows** ホストへのインストール情報の送信] 機能を使用して、対象となるワークステーションを WINS 名または IP アドレスで直接指定できます。インストール情報の送信機能は、初期インストール時以外に、インストール済みのソフトウェアを更新または修復するためにも使用できます。
ポリシーベース インストール	ポリシー マネージャは、ポリシーを使用したインストールと更新処理を実行できます。この機能を使用するには、ホストがすでに管理対象になっている (つまり、ポリシー マネージャ コンソールのポリシー ドメインに含まれている) 必要があります。

CD-ROM を利用したローカルでのインストール/更新	CD-ROM からセットアッププログラムを実行することで、ホストにソフトウェアをインストールできます。インストールの完了後、管理エージェントはポリシー マネージャに登録メッセージを送信します。管理者は、ポリシー マネージャ コンソールの [編集] メニューから [新しいホストをインポート] コマンドを選択してホストをドメインに追加することができます。
パッケージを使用したローカルインストール/更新	カスタムのインストールパッケージ (JAR または MSI 形式、ポリシー マネージャから作成できる) を使用して、インストールを行うことができます。パッケージにはインストールの設定が事前に含まれているため、インストール先のコンピュータはサイレントモードで設定されます (インストール中にユーザの操作は不要になります)。
F-Secure パターン ファイルの更新	ポリシー マネージャは、F-Secureから最新のパターン ファイルを自動的にダウンロードして、更新を行うことができます。ホストは、ポリシーに従ってポリシーマネージャから更新ファイルを取得します。この処理は自動的に実行できます。または、リモートの操作で開始できます。

「インストール」タブで、インストールに関連する機能のショートカットを利用できます。

ホストへのソフトウェアの配布で公開鍵のアクセスが必要な場合、ポリシー マネージャ サーバ のトップページから公開鍵をダウンロードできます。

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、 ボタンを開きます。
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、 ボタンをクリックします。
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。

   必要に応じて新しいインストール パッケージをインポートできます。強制再インストールこのオプションはすべてのインストール パッケージで有効のため、ホストで同バージョンのアプリケーションがすでにインストールされている場合にはアプリケーションが再インストールされます。
2. 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。
3. 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 (「ACCOUNT」など、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ないようになります)。

> 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。

4. インストールの内容を確認します。
5. 「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。
6. 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。
7. [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。
8. 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ポリシー マネージャのポリシーを利用して集中管理できます。

ポリシー マネージャはインストールの操作を指定したインストール パッケージを作成および保存し、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。

ポリシーベース インストール

ポリシー ベース インストールは、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。

ポリシー ベースのインストールを使用して特定のドメインやホストに製品をインストールすることができます。また、Hotfix の適用、製品のアップグレード/アンインストールを実行することも可能です。

インストール操作が完了したら、「ポリシー ベース インストール」テーブルで操作が表示され、同じ操作をドメインに追加される新しいホストに実行することができます。

ポリシーベース インストールを使用するには

1. 「インストール」タブを開きます。
   「インストール」タブにある「ポリシー ベース インストール」テーブルで進行しているインストール捜査のステータスを確認できます。また、「インストールされている製品」テーブルではホストでインストールされている製品が表示されます。
2. 「ポリシー ベース インストール」テーブルの下にある [インストール] をクリックしてリモート インストール ウィザードを開始します。
3. リモート インストール ウィザードで必要な情報を入力します。

   リモート インストール ウィザードで入力した情報をもとにカスタム パッケージが用意されます。ポリシーが配布されるときに指定のドメインとホストにインストール パッケージが配布されます。

   リモート インストール ウィザードが完了したら、インストール操作とステータスが「ポリシー ベース インストール」テーブルの新しい行で表示されます。
4. ポリシーを配布します。
   インストール操作が完了したら、製品名、バージョン、およびインストールしたホスト数が「インストールされている製品」テーブルで表示されます。

   注: インストールが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、[消去] をクリックし、ポリシーを配布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。これにより、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。

他のインストール操作 (アップグレード、アンインストールなど) を実行する場合、「インストールされている製品」テーブルの隣にあるリンクを使用できます。リンクは利用できる場合に自動で表示されます。
リンクのオプション: **Hotfix**, アップグレード、修理、アンインストール

「インストールされている製品」テーブルでリンクが表示されない場合、「ポリシー ベース インストール」テーブルの下にある [インストール] または [アンインストール] を選択して必要なパッケージが利用できるか確認してください。製品がリモートからのアンインストールに対応していない場合、アンインストールのオプションは利用できません。

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. メニューから ツール > インストール パッケージ 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 (MSI または JAR) 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「新規ホスト」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、「新規ホスト」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。「新規ホスト」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) 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`

情報の転送

インストールに関する情報はファイルに格納され、ポリシー マネージャ サーバを通じて転送されます。

インストール パッケージは JAR 形式の圧縮ファイル (WinZip などで表示可能) になりますが、実際のインストールを実行する際にはポリシー ファイルや `INI` ファイルなど、他のファイル形式も使用されます。

ポリシーマネージャコンソールを利用してインストールを開始するには、最初のインストールパッケージをポリシーマネージャサーバに転送する必要があります。インストールパッケージは、次のいずれかの場所から入手できます。

- 製品のインストール CD-ROM
- F-Secure の Web サイト

通常、インストール パッケージは CD-ROM からインストールされ、ポリシー マネージャのセットアップ中にサーバへ移動されます。インストール パッケージを他の方法で入手した場合、「インストール パッケージ」ウィンドウの [インポート] をクリックしてファイルをインポートできます。

ポリシーマネージャコンソールは、新しいインストールパッケージの使用を許可する前に、パッケージがF-Secureの秘密鍵で署名されているか確認します。

ポリシーの管理

ここでは、ポリシーの設定と配布について説明します。

複数のユーザが同時にログインしてポリシーを変更することができます。ユーザによる変更は自動的に保存され、手動で変更を保存する必要はありません。ポリシーの変更は、ポリシーが配布されるときに適用されます。

> 注: 別々のユーザが同じポリシーを変更した場合、最後に変更が行われたポリシーが適用されます。

ポリシーの変更が配布されたときには要求別にポリシー ファイルが各ホストで自動的に作成されます。このことにより、ドメイン構造が変わっても (ホストを追加するときやホスト上の管理対象ソフトウェアをアップグレードするときなど) ポリシーをもう一度配布する必要ありません。

設定

設定を行うには、ポリシーのツリーを参照してポリシー変数の値を変更します。

ポリシー変数には、デフォルト値が定義されているものがあります。デフォルト値は、ルート ドメインの上位から継承されたような形で適用されます。つまり、最上位(ルート) ドメインが選択されていても、デフォルト値は継承される値のように扱われます。デフォルト値は、他の値と同じように上書きできます。

ポリシー ドメイン/ホストの設定値は、以下のように色分けされます。

- 黒 - ポリシー ドメイン/ホスト レベルで指定/変更された値
- 灰色 - 継承された値
- 赤 - 無効な値
- くすんだ赤 - 継承された無効な値

配布していない変更を破棄する

適用していない設定の変更を破棄することができます。

メニューから ファイル > ポリシーの変更を破棄 を選択します。
設定がポリシーを最後に配布したときの状態に戻ります。変更をすでに配布した場合、設定を手動で変更してポリシーを再配布する必要がります。

制限

制限を適用することで、管理者はユーザがポリシー変数の値に対するアクセスを制限することができます。

[ユーザ変更を禁止] が指定されているポリシー変数は、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 [ユーザ変更を禁止] 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。

設定を変更する

ポリシー変数を編集することで設定を変更できます。

設定を変更するには

1. ポリシー ツリーを参照します。
2. ポリシー変数の値を変更します。
3. ポリシーを配布します。

   ドメインおよびホストの環境を設定したら、ホストに新しい環境の設定を配布する必要があります。この操作は次の方法で行うことができます。

   - ツールバーの をクリックします。
   - メニューから ファイル > ポリシーの配布 の順に選択します。
   - CTRL + D を押します。

   設定を配布すると、更新されたポリシーがデータベースに保存され、ホスト上の F-Secure 製品がアップデートを自動的に確認するようになります。

   注: ポリシー ファイルを配布して、ホストがそのファイルを取り出すまで、変更は反映されません。

ポリシーの継承

ポリシーマネージャコンソールでは、各ポリシー ドメインが自動的に親ドメインの設定を継承します。この仕様により、大規模なネットワークを簡単に管理することが可能です。

継承された設定は、ホストやドメイン単位で上書きすることができます。特定のドメインで、継承された設定が変更された場合、その変更はドメインのホストとサブドメインにも継承されます。上書きされた設定は、[消去] 操作で再び継承可能にできます。

ポリシーの継承によって、共通のポリシーを簡単に定義することができます。サブドメイン、または個々のホストに対して、ポリシーをさらに細かく定義できます。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あれば、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。

一部の製品は大規模なドメインからポリシーを継承し、他の製品はサブドメインからポリシーを継承する、または固有のポリシーを取得するといったポリシー環境を構築することもできます。

[ドメインの値を表示] を選択すると、特定のポリシーの設定に適用された変更を確認できます。

[強制的に値を適用] を選択すると、サブドメインまたはホストの値をドメインの値にリセットできます。

ヒント: 「レポート ツール」を使用して「継承レポート」を作成できます。継承レポートは、継承された設定がどこで反映されたか表示します。

テーブルで値を継承する

[行を消去] を使用してテーブルの行を消去すると、選択している行の値は消去され、親ドメインと MIB で定義されているデフォルトの行が適用されます。

- 消去した行と同じインデックス値を持つ行が存在する場合、行が再継承されます。
- 消去した行と同じインデックス値を持つ行が存在しない場合、行は空のままになります。

注: 行は、親ドメインまたは MIB (設定の定義と全設定のデフォルト値を含めているデータベース) のデフォルト行から継承できます。行の継承に関して、MIB は「ルートドメインより上位のドメイン」とみなすことができます。MIB のデフォルト値は、ドメイン レベルで上書きしない限り、サブドメインに継承されます。継承された行を上書きするには、同じインデックス値を持つ行を定義する必要があります。MIB のデフォルト値はホストにインストールされている製品のバージョンに基づいて、取得されます。ドメインに対しては、最新バージョンの値が使用されます。

操作とタスクの管理

ポリシー マネージャ コンソールを利用して、製品に関する操作を実行できます。

ポリシー マネージャ コンソールから操作を実行するには

1. 「操作」タブから実行する操作を選択します。

   また、「詳細モード」ビューで「ポリシー」タブを開いて、ポリシー ドメイン ツリーにある [操作] からも実行する操作を選択します。

2. [開始] をクリックします。
3. 新しいポリシーを配布して、ホストがそのポリシー ファイルを取り出すと、操作がホスト上で開始されます。

   [キャンセル] ボタンをクリックすると、いつでも操作を中止できます。

警告

ここでは、警告とレポートの設定について説明します。

警告とレポートの表示

プログラムまたは操作に問題が発生した場合、ホストは警告とレポートを送信することができます。

警告を受信したら、 ボタンが点灯します。警告を表示するには

1. をクリックすると、警告を表示できます。
   「警告」タブが開きます。受信した警告は、以下の形式で表示されます。

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、[確認] 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 アラート。
日付/時間	警告の日付と時刻。		
説明	問題の説明。		
ホスト/ユーザ	ホストまたはユーザの名前。		
製品	警告の送信したF-Secure製品。		

リストから警告を選択すると、警告の詳細情報が表示されます。F-Secureアンチウイルスのスキャン警告には、レポートが添付されている場合があります。

2. レポートを表示するには、「スキャン レポート」タブをクリックするか、製品ビュー > メッセージメニューからを選択します。

   「スキャン レポート」タブは、「警告」タブと同じ構造になっています。「警告」テーブルと「スキャン レポート」テーブルの情報は、列の見出しをクリックすることで並び替えできます。

警告転送の設定

「警告の転送」テーブルを編集して、警告を設定することができます。このテーブルは、**F-Secure** 管理エージェント > 設定 > 警告の送信 > 警告の転送 の順にクリックすると表示できます。

また、「警告の転送」タブにある管理エージェントの製品ビューでも確認できます。

警告の転送を設定するには

1. メニューから **F-Secure** 管理エージェント > 設定 > 警告の送信 > 警告転送 の順に選択します。
2. 警告の重大度に応じて、警告の送信先を個別に指定できます。

   転送先には、ポリシー マネージャ コンソール、ローカル ユーザのインターフェース、警告エージェント (イベント ビューア、ログ ファイル、SMTP など)、または管理エクステンションを指定できます。

   デフォルトでは、重大度が「情報」と「警告」の警告はポリシー マネージャ コンソールに送信されません。また、ユーザにも表示されません。これらはトラブルシューティング時に役立つ場合もありますが、転送を有効にすると、転送される警告の数が大幅に増加します。ドメインの構造が大きく、厳密な警告転送ルールが設定されている環境では、大量の警告がポリシー マネージャ コンソールに送信される可能性があります。

   デフォルトでは、重大度が「情報」と「警告」の警告はポリシー マネージャ コンソールに送信されません。また、ユーザにも表示されません。これらの警告はトラブルシューティング時に役立つ場合もありますが、警告の転送を有効にすると転送される警告の数が大幅に増加するため、ドメインの構造が大きく、厳密な警告転送ルールが設定されている環境では大量の警告がポリシー マネージャ コンソールに送信される可能性があります。
3. 送信先のポリシー変数などを設定して、警告の送信先を細かく設定することができます。

たとえば、設定 > 警告 > **F-Secure** ポリシー マネージャ コンソール > 再送試行間隔 の設定は、ホストからポリシー マネージャ コンソールへの警告の送信が失敗した場合、再試行するまでの間隔を指定します。

レポート ツール

レポートツールを使用して、ポリシーマネージャコンソールで管理されているデータのレポートを表示したり、エクスポートしたりすることができます。

この機能により、複数のホストやドメインのデータを同時に確認できます。

「ポリシー ドメイン/ホスト セレクタ」ウィンドウ

「ポリシードメイン/ホストセレクタ」ウィンドウでは、レポートの対象とするドメインやホストを選択できます。

レポートツールはポリシー ドメイン ツリーで選択されているドメインを表示します。

[再帰的] チェックボックスをオンにすると、ドメインに含まれているホストがレポートに含まれます。

「レポート タイプ セレクタ」ウィンドウ

このウィンドウでは、表示するレポートを選択できます。

「レポート タイプ セレクタ」ウィンドウでは、以下の操作を実行できます。

- 作成するレポートタイプの選択
- 製品別のフィルタリング (レポートに選択した製品の情報だけを含める)

選択できるレポート タイプ

レポート タイプ	説明
ポリシー	選択したドメインと製品のポリシー変数を含んでいるレポートをエクスポート/表示します。[継承]チェックボックスをオンにして、レポートに継承情報を含めることもできます。
継承	選択したドメインと製品の上位レベルのドメインから継承されていないすべてのポリシー変数 (つまり、選択したドメインで上書きされているすべてのポリシー変数) の値を含んでいるレポートをエクスポート/表示します。
ステータス	選択したドメインと製品のローカル設定とステータス変数を含んでいるレポートをエクスポート/表示します。
プロパティ...	ドメイン コンポーネントの [プロパティ] フィールドの値を含んでいるレポートをエクスポート/表示します。[プロパティ セレクタ] チェックボックスを使用して、レポートに含めるフィールドを選択することもできます。
警告	ドメインの警告情報を含んでいるレポートをエクスポート/表示します。[ソート順セレクタ] を使用して、

レポート タイプ	説明
	警告をソートできます。また、[重大度セレクタ] を使用して、レポートに含める警告の重大度を選択できます。
設定	選択したドメインと製品でインストールされているプログラムの情報を含んでいるレポートをエクスポート/表示します。
アンチウイルス	製品のバージョンとパターンファイルのドメインステータスを含んでいるレポートをエクスポート/表示します。

「レポート」ウィンドウ

レポート タイプを選択した後、このウィンドウでレポートに関する詳細設定を指定できます。

「レポート」ウィンドウでは、次の操作を行うことができます。

- 選択したレポート タイプに関する詳細な設定を指定する
- 選択したレポート タイプの説明を検索する

レポートの詳細設定

- 「ポリシー」レポート タイプに対する設定 - レポートに含めるポリシー値の継承情報を選択できます。
- 「プロパティ」レポート タイプに対する設定 - ID、プラットフォーム、ポーリング プロパティなどの情報をレポートに含めるか選択できます。
- 「警告」レポートタイプに対する設定 - 警告の説明フィールド順に警告をソートしたり、特定の重大度の警告をレポートに含めたりできます。

下部ウィンドウ

レポートを設定した後、レポート ツールの下にあるウィンドウで実行する処理を選択できます。

下部ウィンドウでは、次の操作を行うことができます。

- ユーザ インターフェースのコンポーネントをデフォルトに戻す
- レポートのエクスポート処理を起動する
- レポートの表示処理を起動する
- レポートの生成処理を停止する
- レポート ツールのユーザ インターフェースを終了する (レポートの生成/エクスポートは停止されません。レポートの生成は表示されるウィンドウで停止できます)

レポートを表示およびエクスポートする

レポート ツールを使用して、レポートを表示およびエクスポートできます。

レポート ツールを使用するには

1. メニューから ツール > レポート を選択します。

   または、

   - メイン ウィンドウのポップアップ メニューからレポート ツールを実行します。

   レポート ツールが開きます。

2. レポートの対象となるドメインまたはホストを選択します。
   - [再帰的] を選択すると、ドメインに含まれているすべてのホストがレポートに含まれます。
3. 警告タイプを選択します
4. レポートに含める製品を選択します。
5. 必要に応じて、レポート タイプの詳細設定を選択します。
6. 警告を表示/エクスポートする
   - 下のウィンドウにある [表示] をクリックして、レポートを作成します。HTML 形式のレポートが Web ブラウザで表示されます。デフォルトの Web ブラウザが設定されていない場合、Web ブラウザを設定するためのウィンドウが表示されます。
   - [エクスポート] をクリックすると、レポートをファイルとして保存します。ファイルの保存先と形式は「ファイルの保存」ウィンドウで指定されます。

一般設定

「一般設定」では、接続に関する設定を指定できます。設定はすべての接続、または特定の接続に適用されます。

一般設定 - 接続固有

以下の設定は、[ツール] メニューの [一般設定] で変更できます。これらの設定は、選択している接続オブジェクトに適用されます。

タブ	設定	説明
警告とレポート		警告とレポートに関する次の設定を指定します。 • 警告を表示する期間 • レポートを表示する期間
リモートインストール	インストールのタイムアウト	ポリシー マネージャ コンソールがインストール操作の結果を待機する最大時間を指定します。
	ブラウズのタイムアウト	詳細モード
	同時に行うネットワーク操作の最大数	ネットワーク操作を同時に行える数を調整します。デフォルトの値を推奨します。ただし、ネットワークの接続が低速でインストール情報の送信時に問題が発生する場合、接続速度に応じて同時ネットワーク接続の数を低くしてください。
	進行状況インジケータ	リモートインストール中に、エンドユーザに対して進捗を示すインジケータを表示できます。

一般設定 - 共有

以下の設定は、ポリシー マネージャ コンソールで定義されているすべての接続に適用されます。

タブ	設定	説明
表示設定 > 一般オプション	言語	言語の指定。オペレーティング システムの言語、またはデフォルトの英語を指定できます。システムの言語に対応していないオブジェクトは英語で表示されます。変更を有効にするには、ポリシー マネージャ コンソールを再起動する必要があります。
	フォント	ポリシー マネージャ コンソール全体で使用するフォント。フォントの変更は、プログラムの再起動後に適用されます。
	ルック アンド フィール	ユーザ インターフェースの外観と動作を指定します。プログラムの再起動後に変更が適用されます。
インストール情報の送信	キャッシュの消去	表示したホストやインストールしたソフトウェアに関するキャッシュ (保存情報) をすべて消去して、ディスクの空き容量を増やします。
所在地	**HTML** ブラウザのパス	HTML ブラウザのフルパスを指定します。ブラウザは、オンライン ヘルプページとアンチウイルス レポートのページを表示する際に使用されます。
	メッセージ ログのパス	「メッセージ」ビューの各タブに対するログ ファイルを保存するフォルダのパスを指定します。各ログ ファイルには、関連するタブのタイトル、重大度と作成時間を含むメッセージが1行あたり1つ含まれます。
アンチウイルス	パターン ファイル	アンチウイルス モードでパターン ファイルを期限切れとみなすまでの経過時間を指定します。

第
4
章

ポリシー マネージャ サーバのメンテナンス

トピック：

- *ポリシー マネージャのデータをバックアップ/復元する*
- *バックアップを作成する*
- *バックアップを復元する*
- *署名鍵をエクスポート/インポートする*
- *イメージ ファイルを使用したソフトウェアの複製*

ここでは、ポリシー マネージャ サーバのメンテナンスについて説明します。

また、ポリシー マネージャ サーバ.のコンソール データをバックアップおよび復元する行う方法も紹介します。

ポリシー マネージャのデータをバックアップ/復元する

サーバのデータを定期的にバックアップすることで、ポリシー マネージャ サーバのメンテナンスを効率的に行えます。

重要なデータを定期的にバックアップすることは大事なことです。ドメイン、ポリシー データ、署名鍵は H2 データベースに保存されます。

注: データをバックアップする前に、ポリシー マネージャ サーバ サービスを停止する必要があります。

また、ポリシー マネージャ サーバで使用中の署名鍵をネットワークにエクスポートして、必要に応じて後からインポートできるようにできます。

ポリシー マネージャ コンソールの設定を保存する場合、ローカルのインストール先フォルダから `lib\Administrator.properties` ファイルをバックアップしてください。

注: `Administrator.properties` は、ポリシー マネージャ コンソールを最初に実行したときに作成され、ウィンドウ サイズ、通信ディレクトリのパス、サーバの URL など、セッションに関連する情報を含んでいます。

バックアップを作成する

ここでは、ポリシー データとドメインの構造をバックアップする方法について説明します。

1. ポリシー マネージャ サーバのサービスを停止します。
2. `<F-Secure installation folder>\Management Server 5\data\h2db` ディレクトリをバックアップします。
3. ポリシー マネージャ サーバのサービスを再起動します。
4. ポリシー マネージャ コンソールの管理セッションを再度開きます。

バックアップを復元する

ポリシー マネージャのデータを紛失した場合、バックアップからデータを復元することができます。

ポリシー マネージャのデータを復元するには

1. ポリシー マネージャ サーバを停止します。
2. `<F-Secure installation folder>\Management Server 5\data\h2db` のバックアップを適切の場所にコピーします。
3. ポリシー マネージャ サーバのサービスを再起動します。
4. ポリシー マネージャ コンソールの管理セッションを再度開きます。

署名鍵をエクスポート/インポートする

署名鍵を外部の場所にエクスポートしたり、インポートしたりすることができます。

署名鍵のエクスポートは、大規模な環境で複数のポリシー マネージャを導入している状況でネットワーク全体で同じ署名鍵を使用したい場合などで必要になるかもしれません。

1. メニューから ツール > サーバの構成 を選択します。
2. [鍵] を選択します。

   使用中の署名鍵を変更するには

   a) [エクスポート] をクリックします。
   b) 鍵をエクスポートする場所を指定して、[保存] をクリックします。
   c) エクスポートする秘密鍵のパスワードを入力して、[**OK**] をクリックします。

   署名鍵をインポートするには

   a) [置換] をクリックします。
   b) インポートする鍵を指定して、[**OK**] をクリックします。
   c) インポートする署名鍵のパスワードを入力して、[**OK**] をクリックします。

   署名鍵のエクスポート/インポートが完了したことを知らせるメッセージが表示されます。
3. [**OK**] をクリックして「サーバの構成」ウィンドウを閉じます。

イメージ ファイルを使用したソフトウェアの複製

イメージ ファイルを利用して製品をインストールする場合、固有の ID がないことを確認する必要があります。

ディスクのイメージ ファイルを使用してソフトウェアを複製する場合、アンチウイルスを含めることができます。その際、インストールしたすべての製品にポリシー マネージャで使用される固有の識別コード (固有の ID) が割り当てられます。ディスク イメージ ソフトウェアを使用して新しいコンピュータをインストールすると、複数のコンピュータが同じ ID を使用しようとする場合があります。このような状況になると、ポリシー マネージャは正常に機能しなくなります。

次の方法で、ディスク イメージ ソフトウェアの使用時に、各コンピュータに専用の固有 ID を使用するようにできます。

1. イメージファイルに含むソフトウェアとシステムをインストールします (アンチウイルスを含む)。
2. ポリシー マネージャ サーバを正しく使用するように.アンチウイルスを設定します。

   注: ただし、ホストがポリシー マネージャ コンソールに自動登録を依頼した場合、ポリシー マネージャ サーバにホストをインポートしないでください。インポートの対象は、イメージ ファイルをインストールするホストに限定する必要があります。

3. コマンドプロンプトから `fsmautil resetuid` を実行します。

   通常、このユーティリティは `C:\Program Files\F-Secure\Common` ディレクトリにあります (他言語の Windows を使用している場合、またはデフォルト以外のインストール パスを指定した場合、ディレクトリが異なる可能性があります)。
4. コンピュータをシャットダウンします。

👉 **注:** コンピュータの再起動は行わないでください。

5. ディスクのイメージ ファイルを作成します。
ユーティリティ プログラムがアンチウイルスの固有 ID をリセットします。イメージ ファイルがインストールされた各マシンの再起動中に、新しい固有 ID が自動的に作成されます。これらのマシンはポリシー マネージャに自動登録依頼を送信し、依頼は正常に処理されます。

第
5
章

ウイルスのパターン ファイルを更新する

トピック：

- *自動更新エージェントによる自動更新*
- *自動更新エージェントを使用する*
- *自動更新エージェントを使用して、新しい更新を確認する*
- *手動更新*
- *トラブルシューティング*

ここでは、パターン ファイルの更新について説明します。

システムを最新の脅威から保護するために、パターン ファイルは常に最新の状態にしてください。

自動更新エージェントによる自動更新

自動更新エージェントを使用すると、パターンファイルと情報コンテンツを自動的にWebからダウンロードできるようになります。

自動更新エージェントは、他のインターネット アプリケーションが使用していない帯域幅を使用してファイルを透過的にダウンロードします。これにより、ユーザはインターネットを検索しなくても最新のセキュリティ更新や情報を常に入手することができます。

自動更新エージェントがインターネットに常時接続している場合、新しい更新は、F-Secureが発行してから約2時間後に自動で受信します。インターネットに常時接続していない場合、自動更新が遅れることがあります。

自動更新エージェントは、管理対象およびスタンドアロンのF-Secure製品を更新します。デフォルトでは、ウイルス ニュースもダウンロードされます。必要に応じて、ダウンロードを無効にすることも可能です。自動更新エージェントを使用するには、ライセンスが認証されたアンチウイルスやセキュリティ製品が必要です。

自動更新エージェントの動作

自動更新エージェントは、サーバと定期的に通信し、新しいコンテンツが入手可能か確認します。

自動更新エージェントは、サービスの開始時にF-Secureの自動更新サーバに接続するようになります。サーバと定期的に通信し、新しいコンテンツが入手可能か確認します。新しいコンテンツが存在する場合、それらが自動的にダウンロードされます。ポーリング間隔 (通信する頻度) はサーバ側で設定し、クライアント側からは調整できません。

F-Secureは次の順序で更新をダウンロードしようとします。この順序はポリシー マネージャ 6.0 以降の仕様です。

1. 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、各ポリシー マネージャ プロキシを順番に使用して、ポリシー マネージャに接続しようとします。
2. HTTP プロキシが設定されている場合、HTTP プロキシを通じて更新をポリシー マネージャ サーバからダウンロードしようとします
3. 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. 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、ポリシー マネージャプロキシを順番に使用して、F-Secure更新サーバに接続しようとします。
5. HTTP プロキシが設定されている場合、HTTP プロキシを通じて、更新をF-Secure更新サーバからダウンロードしようとします。
6. F-Secure更新サーバから更新を直接ダウンロードしようとします。

自動更新エージェントのメリット

自動更新エージェントは、更新を自動で行い、その際に帯域も節約します。

最適化されたパターンファイルのダウンロード

自動更新エージェントは、パターンファイルの変更を検出します。高度なアルゴリズム (バイト単位で動作するもの) を使用して、ファイルまたはデータベース全体ではなく、変更された部分だけをダウンロードします。通常、変更部分は更新ファイルのほんの一部分であるため、低速のダイヤルアップ回線を使用しているユーザでも更新を簡単に入手でき、常時接続しているユーザは帯域幅を大幅に節約できます。

再開可能のデータ転送

自動更新エージェントは、複数のセッションにまたがるダウンロードを実行することが可能です。更新のダウンロードを中断した場合、自動更新エージェントはダウンロードの内容を保存し、次回接続したときにファイルの残りをダウンロードします。

自動化された更新

更新ファイルを探したり、手動でダウンロードしたりする必要はありません。自動更新エージェントを使用すると、F-Secureがパターンファイルの更新を作成したときにそれを自動的にダウンロードします。

自動更新エージェントを使用する

`fsaua.cfg` を編集することで自動更新エージェントを設定できます。

自動更新エージェントを設定する

ポリシー マネージャ バージョン 7.0 以降の 自動更新エージェント (ポリシー マネージャと一緒にインストールされる) は、構成ファイルである `fsaua.cfg` を編集することによって設定できます。

重要: ここの設定は、ポリシー マネージャ サーバと一緒にインストールされる自動更新エージェントに適用します。構成ファイルを編集するときには、以下に記載した設定以外の設定事項を編集しないでください。.

自動更新エージェントを設定するには

1. `fsaua.cfg` を開きます (`C:\Program Files\F-Secure\FSAUA\program\fsaua.cfg` に保存されている)。
2. HTTP プロキシを指定する

   `http_proxies` のディレクティブは、自動更新エージェントが使用する HTTP プロキシを制御します。次の形式を使用してください。

   ```
   http_proxies=[http://][[domain\]user[:passwd]@]<address>[:port]
   [,[http://][[domain\]user[:passwd]@]<address>[:port]]
   ```

   例:

   ```
   http_proxies=http://proxy1:8080/,http://backup_proxy:8880/,
   http://domain\username:usernamespassword@ntlmproxy.domain.com:80
   ```

3. ポーリング間隔を指定する

   `poll_interval` のディレクティブは、自動更新エージェントが更新を確認する頻度を指定します。デフォルトでは1800秒 (30分) に設定されています。

   ```
   poll_interval=1800
   ```

   注: 自動更新エージェントの構成ファイルで設定する最小ポーリング間隔にはF-Secureの更新サーバで設定されている最小ポーリング間隔より低い数値を指定していることはできません。更新サーバで指定されている間隔より低い数値を指定しても、その設定は反映されません。

4. ファイルを保存して閉じます。
5. 変更を適用するには、 のサービスを一旦停止して、再起動する必要があります。

   これは、次のコマンドをコマンドラインから実行することで可能です。

```
net stop fsaua
net start fsaua
```

ログ ファイルを確認する

自動更新エージェントが生成したメッセージは fsaua.log と言うファイルに保存されます。

メッセージの中には、エラーを表示するもの以外に、起動/シャットダウンなどの通常操作に関する情報を示すものもあります。

fsaua.log は C:\Program Files\F-Secure\FSAUA\program に保存されています。

ログに保存されるメッセージには次の情報が含まれます。

- メッセージが生成された日付。

```
[ 3988]Thu Oct 26 12:40:39 2006(3): Downloaded'F-Secure Anti-Virus Update
2006-10-26_04' - 'DFUpdates' version '1161851933' from fsbwserver.f-secure.com,
 12445450 bytes (download size 3853577)
```

- 発生したイベントに関する短い説明。更新がダウンロードされた場合、更新の名前とバージョンが保存されます。

```
[ 3988]Thu Oct 26 12:40:39 2006(3): Downloaded 'F-Secure Anti-Virus Update
2006-10-26_04' - 'DFUpdates' version '1161851933' from fsbwserver.f-secure.com,
 12445450 bytes (download size 3853577)
```

- イベントが更新である場合、更新のソースとダウンロード サイズも保存されます。

```
[ 3988]Thu Oct 26 12:40:39 2006(3): Downloaded 'F-Secure Anti-Virus Update
2006-10-26_04' - 'DFUpdates' version '1161851933' from fsbwserver.f-secure.com,
 12445450 bytes (download size 3853577)
```

fsaua.log の例

以下は、ログ ファイルに保存されるメッセージの例です。

メッセージ	説明
Update check completed successfully	更新ソースに接続できました。
Update check completed successfully. No updates are available.	更新ソースに接続しました。新しい更新はありませんでした。
Downloaded 'F-Secure Anti-Virus Update 2006-10-26_04' - 'DFUpdates' version '1161851933' from fsbwserver.f-secure.com, 12445450 bytes (download size 3853577)	更新ソースに接続しました。いくつかのファイルがダウンロードされました。
Installation of 'F-Secure Anti-Virus Update 2006-10-26_04' : Success	ファイルがダウンロード先フォルダに格納されたこと、および既存のファイルが削除されたことを示します。自動更新エージェントは、ホストが新しいファイル適用しているか表示できません。
Update check failed. There was an error connecting fsbwserver.f-secure.com (DNS lookup failure)	更新の確認が失敗したことを示します。

ログから製品の動作を確認する

本製品が正常に動作している場合、ダウンロードした更新のインストール結果が「Success」としてログファイルに保存されます。

```
Installation of 'F-Secure Anti-Virus Update 2006-10-26_04' : Success
```

ポリシー マネージャ コンソールの「概要」タブで、ウイルス、スパイウェア、ディープガードの更新ステータスを確認することもできます。

管理されているホストの更新ステータスは、ポリシー マネージャ コンソールのステータス > 全体の保護で確認できます。

自動更新エージェントを使用して、新しい更新を確認する

自動更新エージェントは新しい更新を自動更新エージェントのインターフェースから確認できます。

次のように実行します。

1. スタート > プログラム > **F-Secure** ポリシー マネージャ > **F-Secure** 自動更新エージェント の順にクリックして、自動更新エージェントのユーザ インターフェースを開きます。
2. [今すぐ確認する] をクリックします。
   「通信」に更新のステータスが表示されます。

手動更新

コンピュータがインターネットに接続していない場合、更新を手動で行えます。

1. 別のコンピュータから http://support.f-secure.com/ にアクセス。
2. `fsdbupdate.exe` ツールをダウンロードします。
3. メモリスティックやリムーバブル メディアを使用して、`fsdbupdate.exe` をコンピュータに移します。

トラブルシューティング

以下は、エラー メッセージとして`fsaua.log`に記録される可能性がある問題の例です。

問題	原因	解決方法
DNS ルックアップに失敗しました。あるいは接続が失敗、切断、または拒否されました。	ネットワークの問題です。	ネットワークの設定を確認してください。
プロキシの認証に失敗しました。	入力した HTTP プロキシ用のパスワードが無効です。	`fsaua.cfg` 内の `http_proxies` ディレクティブにある HTTP プロキシ パスワードを確認および修正します。

問題	原因	解決方法
ディスクがいっぱいです。または I/O エラーが発生しました。	指定ディレクトリのディスク空き容量が不足しています。	更新版をダウンロードできるようにドライブの空き領域を増やしてください。
サーバ エラー、または不明なエラーが発生しました。	原因は不明です。	-

第
6
章

Linux での使用

トピック：

- *概要*
- *インストール*
- *アンインストール*
- *FAQ*

ポリシー マネージャは Linux を搭載しているシステムにインストールすることもできます。

ポリシー マネージャの Linux 版は、同製品の Windows 版とほぼ同じように動作しますが、Windows 版の一部の機能は利用できません。また、インストール方法が異なります。

概要

ここでは、本製品の Linux 版に関する一般的な情報を紹介します。

Windows 版との違い

ポリシー マネージャ コンソールの Linux 版では、次のサービス/機能を利用できません。

- リモート インストール機能
- Windows インストール パッケージ (MSI) のエクスポート
- ネットワークにあるワークステーション/ホストの自動検出

対応ディストリビューション

ポリシー マネージャは、Debian パッケージ管理システム (DEB) および Redhat パッケージ管理システム (RPM) に基づいた Linux ディストリビューションに対応しています。32および64ビットのディストリビューションで利用できます。

対応ディストリビューション	パッケージ システム
Red Hat Enterprise Linux 4/5/6	RPM
CentOS 5	RPM
SUSE Linux Enterprise Server 10/11	RPM
SUSE Linux Enterprise Desktop 11	RPM
openSUSE 11	RPM
Debian GNU Linux 5	DEB
Ubuntu 8.04/10.04	DEB

インストール

ポリシー マネージャのインストール方法について説明します。

以下のコンポーネントを決まった順でインストールする必要があります。

1. 自動更新エージェント
2. ポリシー マネージャ サーバ
3. ポリシー マネージャ コンソール

ポリシー マネージャ サーバと自動更新エージェントは同じマシンにインストールされている必要があります。

ポリシー マネージャ コンソールは同じマシン、または別のマシンにインストールできます。

注: ポリシー マネージャの旧バージョンからアップグレードする場合、ポリシー マネージャ サーバのアップグレードを行う前に Web レポートをアンインストールする必要があります (Web レポートが旧バージョンにインストールされている場合)。

注: ポリシー マネージャのアップグレードとインストール方法については、リリース ノーツを参照してください。

インストールの参考

Red Hat/Suse ディストリビューションの場合

- プラットフォームによって、`libstdc++` の互換ライブラリが必要です。ポリシー マネージャ サーバをインストールする前に次のパッケージをインストールしてください。
  - Red Hat Enterprise Linux 4/5/6: `compat-libstdc++-33`
  - openSuse 11 (32ビット): `libstdc++33`
  - openSuse 11 (64ビット): `libstdc++33` と `libstdc++33-32bit`
- 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64ビットのプラットフォームにインストールする場合、64ビット版のインストール パッケージをインストールする必要があります。

Debian/Ubuntu ディストリビューションの場合

- ポリシー マネージャ サーバは、`libstdc++` 互換ライブラリを必要とします。ポリシー マネージャ サーバをインストールする前に `libstdc++5` をインストールしてください。互換ライブラリをインストールせずにポリシー マネージャ サーバのインストールを実行したことでエラーが発生した場合、ライブラリをインストールし、`apt-get install -f` コマンドを使用してインストールを完了することができます。
- 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64ビットのプラットフォームにインストールする場合、64ビット版のインストール パッケージをインストールする必要があります。また、
  - ポリシー マネージャ サーバをインストールする前に `ia32-libs` パッケージを ia32/i386 アーキテクチャのランタイム ライブラリと一緒にインストールしてください。
  - 自動更新エージェントは、`--force-architecture` オプションを指定してインストールします。

自動更新エージェントとポリシー マネージャ サーバをインストールする

まず、F-Secure 自動更新エージェントとポリシー マネージャ サーバをインストールします。

1. `root`としてログインします。

   Ubuntu ディストリビューションを使用している場合、`/etc/sudoers` に追加された通常のユーザでログインします。
2. ターミナルを開きます。
3. 次のコマンドでインストールを実行します。

ディストリビューション	コマンド
Debian ベース	`dpkg -i f-secure-automatic-update-agent_<バージョン番号>.<ビルド番号>_i386.deb` `dpkg -i f-secure-policy-manager-server_<バージョン番号>.<ビルド番号>_i386.deb`
RPM ベース	`rpm -i f-secure-automatic-update-agent-<バージョン番号>.<ビルド番号>-1.i386.rpm` `rpm -i f-secure-policy-manager-server-<バージョン番号>.<ビルド番号>-1.i386.rpm`

ディストリビューション	コマンド
Ubuntu	`sudo dpkg -i f-secure-automatic-update-agent_<バージョン番号>.<ビルド番号>_i386.deb` `sudo dpkg -i f-secure-policy-manager-server_<バージョン番号>.<ビルド番号>_i386.deb`

4. 設定を行うために、`/opt/f-secure/fspms/bin/fspms-config` を実行します。
   Ubuntu を使用している場合、`sudo /opt/f-secure/fspms/bin/fspms-config` を入力します。
   デフォルトの設定を選択する場合、Enter を押します (デフォルトの設定は角カッコ内で表示されます)。
5. 通常のユーザでログインし、次のコマンドを実行してコンポーネントのステータスを確認します。
   - `/etc/init.d/fsaua status`
   - `/etc/init.d/fspms status`

   ステータスは、ブラウザから次の URL にアクセスすることでも確認できます。
   - `http://localhost` - ポリシー マネージャ サーバのステータス
   - `http://localhost/B` - 自動更新サーバのステータス
   - `http://localhost:8081` - Web レポートのステータス

設定スクリプトが終了したら、自動更新エージェントとポリシー マネージャ サーバが起動します。また、コンピュータの起動時に自動で開始するようにもなります。

ポリシー マネージャ コンソールをインストールする

次に、ポリシー マネージャ コンソールをインストールする必要があります。

1. `root`としてログインします。
   Ubuntu ディストリビューションを使用している場合、`/etc/sudoers` に追加された通常のユーザでログインします。
2. ターミナルを開きます。
3. 次のコマンドを実行してインストールを開始します。

ディストリビューション	コマンド
Debian ベース	`dpkg -i f-secure-policy-manager-console_<バージョン番号>.<ビルド番号>_i386.deb`
RPM ベース	`rpm -i f-secure-policy-manager-console-<バージョン番号>.<ビルド番号>-1.i386.rpm`
Ubuntu	`sudo dpkg -i f-secure-policy-manager-console_<バージョン番号>.<ビルド番号>_i386.deb`

   ポリシー マネージャ コンソールは `/opt/f-secure/fspmc/` にインストールされます。その際に `fspmc` というユーザ グループが自動的に作成されます。
4. `fspmc` グループにユーザを追加します。
   グループに追加されたユーザは、ポリシー マネージャ コンソールを実行できるようになります。
   a) ユーザが所属しているグループを確認します。

groups <ユーザ ID>

たとえば、ユーザが Taro の場合、

groups Taro

b) このユーザを fspmc グループに追加します。

/usr/sbin/usermod -G fspmc,<ユーザが所属しているグループ (複数の場合、カンマで区切る)> <ユーザ ID>

Taro が normal_users と administrators のグループに所属している場合、次のコマンドを実行します。

/usr/sbin/usermod -G fspmc,normal_users,administrators Taro

注: 指定のカンマ区切りグループ リストが、ユーザが以前所属していたグループを置換します。

5. [プログラム] メニューの [F-Secure]サブメニューから [ポリシー マネージャ コンソール] を選択します。

コマンドラインから sg fspmc -c /opt/f-secure/fspmc/fspmc を実行することでもポリシー マネージャ コンソールを開始できます。

注: Red Hat Enterprise Linux 4 を使用している場合、[プログラム] メニューを使用できる前に一度ログアウトする必要があります。また、sg コマンドが <command> の引数を受け付けないため、newgrp をコマンドラインで代用します。

- newgrp fspmc
- /opt/f-secure/fspmc/fspmc

ポリシー マネージャ コンソールをはじめて起動する際には、構成を完了するために必要な質問がいくつか表示されます。質問は Windows 版と同じです。

アンインストール

ポリシー マネージャの Linux 版をアンインストールするには、コンポーネントを決まった順序でアンインストールする必要があります。

次のコンポーネントを順にアンインストールします。

1. ポリシー マネージャ サーバ
2. 自動更新エージェント
3. ポリシー マネージャ コンソール

1. rootとしてログインします。

   Ubuntu ディストリビューションを使用している場合、/etc/sudoers に追加された通常のユーザでログインします。

2. ターミナルを開きます。
3. 次のコマンドを順に実行します。

ディストリビューション	コマンド
Debian ベース	1. dpkg -r f-secure-policy-manager-server 2. dpkg -r f-secure-automatic-update-agent 3. dpkg -r f-secure-policy-manager-console

ディストリビューション	コマンド
RPM ベース	**1.** `rpm -e f-secure-policy-manager-server` **2.** `rpm -e f-secure-automatic-update-agent` **3.** `rpm -e f-secure-policy-manager-console`
Ubuntu	**1.** `sudo dpkg -r f-secure-policy-manager-server` **2.** `sudo dpkg -r f-secure-automatic-update-agent` **3.** `sudo dpkg -r f-secure-policy-manager-console`

注: ポリシー マネージャが作成した再生不可能なデータ (ログ ファイル、MIB ファイル、ドメイン ツリー、設定ファイルなど) が誤って削除されることを防ぐために、次のディレクトリはアンインストール中に削除されません。今後必要となる可能性があるキーは削除しないことを推奨します。製品を完全にアンインストールするには、`root` としてログインし、次のコマンドを実行します。

```
rm -rf /var/opt/f-secure/fspms
rm -rf /var/opt/f-secure/fsaus
rm -rf /etc/opt/f-secure/fspms
rm -rf /etc/opt/f-secure/fsaus
rm -rf /opt/f-secure/fspmc
```

FAQ

ここでは、本製品の Linux 版に関する FAQ (よくある質問) を紹介します。

Q	A
Linux 版では、ログ ファイルと設定ファイルはどこに保存されていますか?	全ファイルと該当するファイル パスは次のコマンドを実行することで表示できます。 • RPM-based distributions: `rpm -ql f-secure-<component_name>`. • Debian-based distributions: `dpkg -L f-secure-<component_name>`. ログ ファイルの場所: • ポリシー マネージャ コンソール: `/opt/f-secure/fspmc/lib/Administrator.error.log` • 自動更新エージェントは、ランタイムエラー、警告、およびその他の情報を `syslog` に保存します (syslog は通常の環境で `/var/log/messages` にあります)。 • ポリシー マネージャ サーバ: `/var/opt/f-secure/fspms/logs` と `/var/opt/f-secure/fsaus/log`.

Q	A
	設定ファイルの場所: • ポリシー マネージャ コンソール: /opt/f-secure/fspmc/lib/Administrator.properties. • 自動更新エージェント: /etc/opt/f-secure/fsaua/fsaua_config • ポリシー マネージャ サーバ: /etc/opt/f-secure/fspms/fspms.conf.
ファイルの保存場所、フォルダの構成について教えてください。	ポリシー マネージャの全ファイルは、FHS (Filesystem Hierarchy Standard、ファイルシステム階層標準 □の仕様従っています。FHS の詳細については、*http://www.pathname.com/fhs/* をご覧ください。
ポリシーマネージャ サーバを起動することができません。	設定スクリプトが実行されていることを確認ください: /opt/f-secure/fspms/bin/fspms-config また、root としてログインして、netstat -lnpt コマンドを実行することでポリシーマネージャ サーバのポートの状態を確認できます。
ポリシーマネージャのコンポーネントの開始、停止、再開、ステータスの確認はどうやって実行できますか?	自動更新エージェント: /etc/init.d/fsaua {start|stop|restart|status} ポリシー マネージャ サーバ: /etc/init.d/fspms {start|stop|restart|status}
どうすれば HTTP プロキシを設定できますか?	設定スクリプト (/opt/f-secure/fsaua/bin/fsaua-config) を実行することで、または設定ファイルを手動で編集することで HTTP プロキシを設定できます。該当のディレクティブは http_proxies=http://address:port/ です。 新しい設定を適用するには、自動更新エージェントを再起動する必要があります。
ポリシー マネージャ サーバ が使用するデフォルトのポート (80 と 8080) はどうすれば変更できますか?	ポートは設定スクリプトで指定されています: /opt/f-secure/fspms/bin/fspms-config
Web レポートが使用するデフォルトのポート (8081) はどうすれば変更できますか?	Web レポートの使用ポートは、ポリシーマネージャ サーバの設定スクリプトで指定されています: /opt/f-secure/fspms/bin/fspms-config
F-Secureのパターン ファイルの更新が行われる日時を設定することは可能ですか?	はい。自動更新はOS のスケジュール デーモン cron を利用します。/etc/crontab にエントリを編集/追加することで自動更新が行われる日時を設定できます。

Q	A
	たとえば、パターン ファイルの更新を10分ごとに確認するには、次の行を `/etc/crontab` に追加します。 `*/10 * * * * fspms /opt/f-secure/fspms/bin/fsavupd` 自動更新と `cron` については、`man cron` と `man 5 crontab` を参照してください。ほとんどの場合、F-Secureのパターン ファイルの更新を行う時間は、`/opt/f-secure/fspms/bin/fspms-config` コマンドで設定できます。
F-Secureのパターン ファイルはどうすれば手動で更新できますか?	`fspms` のユーザとしてログインし、次のコマンドで更新ツールを実行します。 `sudo -u fspms /opt/f-secure/fspms/bin/fsavupd --debug` オプションの `--debug` によって詳細な診断メッセージが表示されます。

最新の `fsdbupdate` パッケージからF-Secureのパターン ファイルを手動で発行するには?	*http://download.f-secure.com/latest/fsdbupdate.run* から最新の `fsdbupdate.run` ツールをダウンロードして、`root` としてツールを実行します。
	`./fsdbupdate.run`
	自動更新エージェントのデータベースがすべてアップデートされます。アップデートの後、更新サーバとポリシー マネージャ サーバにこれらの更新を発行する必要があります。これは、`crontab` に `fsavupd` を指定すること、または`fsavupd` を手動で実行することで可能です。
	`sudo -u fspms /opt/f-secure/fspms/bin/fsavupd`

使用できる診断ツールはありますか?	はい。`fsdiag` を使用して、システムと関連するパッケージの情報を収集できます。root で次のコマンドを入力することで fsdiag を実行できます。 `/opt/f-secure/fspms/bin/fsdiag` 収集した情報は現在のディレクトリにある `fsdiag.tar.gz` に保存されます。このファイルは、F-Secureのカスタマー サポートを依頼するときに必要になります。

起動時に「`...`別の自動更新サーバが見つかりました`...`」と示すメッセージが表示されます。どうすれば良いですか	**1.** 別の自動更新サーバが実行中で TCP ソケットを使用しているか確認してください。
	`netstat -anp | grep bwserver`
	`ps axuww | grep bwserver`

Q	A
	2. 次のコマンドで自動更新サーバを停止させます。 `kill `pidof bwserver`` `kill -9 `pidof bwserver`` **3.** ポリシー マネージャ サーバを再起動します。 `/etc/init.d/fspms stop` `rm -f /var/lock/subsys/fsaus /var/run/fsaus.pid` `/etc/init.d/fspms start`
ポリシーマネージャ コンソールからホストにソフトウェアをインストールするにはどうすれば良いですか?	インストール パッケージを JAR ファイルにエクスポートして、`ilaunchr.exe` ツールとログイン スクリプトなどを使用してソフトウェアをホストにインストールできます。ソフトウェアのインストールは本書で説明されている通りに行ってください。`ilaunchr.exe` ツールは`/opt/f-secure/fspmc/bin` ディレクトリにあります。
ポリシー マネージャを大規模な環境で使用する場合の設定について教えてください。	• ポリシーマネージャ コンソールで、[受信パッケージのポーリング間隔] と [送信パッケージの更新間隔] の値を30□60分に設定します。 • ポリシー マネージャ プロキシを使用して、ポリシー マネージャ サーバの負担を軽くします。

第
7
章

Web レポート

トピック：

- *レポートを生成/表示する*
- *Web レポートの管理*
- *Web レポートのエラー メッセージとトラブルシューティング*

Web レポートは、ポリシー マネージャ サーバに付属する視覚的なレポート ツールです。

Web レポート機能を使用すると、ウイルスに対して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したり、過去のデータに基づいたグラフ形式のレポートをすばやく作成したりすることができます。また、管理エージェントからポリシー マネージャ サーバに送信されたクライアント セキュリティの警告やステータス情報を利用して、カスタムのレポートとクエリを作成することも可能です。作成したレポートは HTML 形式でエクスポートできます。

Web レポート機能が生成するレポートを表示するには、コンピュータに InternetExplorer、Mozilla Firefox などのインターネット ブラウザがインストールされている必要があります。

レポートを生成/表示する

生成できるレポートのタイプには、現在のセキュリティ状況を示す棒グラフや円グラフ、トレンド レポート、詳細なリスト レポートなどがあります。

正確なレポートおよび使用できるレポートテンプレートを表示するには、Web レポートのユーザ インターフェースでいずれかのページを選択します (「ウイルス保護の概要」、「インターネット防御の概要」、[警告」、「インストールされているソフトウェア」、および「ホストのプロパティ」)。

レポートを生成する

Web レポートの ユーザ インターフェースから、トレンド データに基づいてグラフィカルなレポートをすばやく作成することができます。

Web レポートを生成するには

1. Web レポートのメイン ページを開きます。
2. ブラウザで、ポリシー マネージャ サーバのアドレスまたは IP アドレスをWeb レポートのポート (コロンで区切って) と一緒に入力します。
   たとえば、「`fspms.example.com:8081`」と入力します。

   また、Web レポートをローカルからアクセスする場合、Web レポートを [スタート] メニューからにアクセスすることもできます (スタート > **F-Secure** ポリシー マネージャ > **F-Secure** ポリシー マネージャ **Web** レポート)。
3. Web レポートのページが開くまで待ちます。

   大規模な環境では、ページの表示に時間がかかる場合があります。

   ページが表示されると、選択されているカテゴリのデフォルト レポートが表示されます。デフォルトでは、「ポリシードメイン」ツリーの [ルート] が選択されています。
4. 新規レポートを表示するには、対象となるドメイン、サブドメイン、またはホストをまず選択します。
5. 次に、レポートのカテゴリ (「ウイルス保護の概要」、「インターネット防御の概要」、「警告」、「インストールされているソフトウェア」、および「ホストのプロパティ」) とレポートのタイプを選択します。
6. メイン ウィンドウの下部にレポートが表示されます。

印刷用のレポートの作成

レポートを印刷に適した形式で表示できます。

印刷用のレポートを表示するには

1. ページの右上にある [印刷用] リンクをクリックします。
   新しいウィンドウが開き、レポートが印刷に適した形式で表示されます。
2. ブラウザの印刷機能を使用して、レポートを印刷します。

ブラウザの [名前を付けて保存] または [ページに名前を付けて保存] オプションを使用して、レポートを保存して後で表示したり、印刷したりすることも可能です。 レポートを保存する場合、ページを完全に (画像を含む) 保存するようにしてください。

- Microsoft Internet Explorer を使用している場合、ファイル > 名前を付けて保存 メニューからを選択します。表示するウィンドウの [ファイルの種類] で [**Web**ページ、完全] を選択します。
- Mozilla を使用している場合、ファイル > ページに名前を付けて保存 メニューのを選択します。

レポートを自動的に生成する

ポリシーマネージャ Web レポートはレポートを自動で生成し、固有の URL で表示することができます。

URL にはレポートの分類、レポートのタイプ、ポリシー ドメインが含まれるため、次回同じレポートを生成する際には、これらの情報を新たに選択する必要はありません。

この機能では、次の2つの操作が可能です。

- 監視対象を含むレポートを生成し、そのレポートへのリンクをコンピュータ (デスクトップ、ブックマーク、またはその他の場所) に追加します。このリンクを使用してWeb レポートにアクセスすると、レポートは更新され、最新のデータが表示されます。
- 生成したレポートを保存して、今後生成するレポートと比較することもできます。まず、印刷用ページを生成し、ブラウザでページ全体を保存します。こうすると、いつでも「古い」レポートを参照できます。

Web レポートの管理

ここでは、Web レポートの管理タスクについて説明します。

注: Web レポートはポリシー マネージャ サーバのインストール中に有効および無効になります。また、インストール中にアクセスがローカル マシンに制限されます。Web レポートはポリシー マネージャ サーバを再インストールすることで、またはレジストリを通じて有効または無効にできます。

Web レポートの全データはポリシー マネージャ サーバが使用している H2 データベースに保存されるため、H2 データベースをバックアップするたびにWeb レポートのデータもバックアップされます。

Web レポートのエラー メッセージとトラブルシューティング

ここでは、Web レポートのエラー メッセージとWeb レポート データベースのトラブルシューティングについて説明します。

エラー メッセージ

ここでは、Web レポートで発生するエラー メッセージについて説明します。

- ブラウザのエラー メッセージ: 「**<location>**のアクセス中に接続が拒否されました」

  ブラウザがポリシー マネージャ サーバにアクセスできません。リンク先のマシンまたはポートが間違っているか、ポリシー マネージャ サーバがそのマシンにインストールされていないか、またはポリシー マネージャ サーバが起動されていない可能性があります。それぞれを順に確認してください。ファイアウォールによって接続がブロックされている可能性もあります。

- エラーメッセージ: 「**Web** レポートはデータベースとの接続を失いました。ポリシー マネージャ サーバを再起動する必要があります。」

  Web レポートがデータベースにアクセスできない場合、ポリシー マネージャ サーバのサービスを再起動する必要があります。それでも解決されない場合、既存のデータベースを保持したままポリシー マネージャ サーバを再インストールできます。

トラブルシューティング

Web レポートの動作に問題が発生した場合、次の方法で問題を解消できるかか試してください。

問題を確認するには

1. ページを再ロードします。
2. すべての処理が完全に起動していないことで問題が発生している場合、しばらく待ってからページを再ロードしてください。

   また、不要な警告を削除することで起動時間を短縮できます。
3. Web レポートのサービスを再起動します。
4. ポリシー マネージャ サーバを再起動します。
5. 自動登録したホストのインポート
6. 既存の設定を残したまま、ポリシー マネージャ サーバを再インストールします。
7. 問題が解決されない場合、Web レポートのデータベースをリセットするか、バックアップ コピーから復元します。

Web レポートのポートを変更する

Web レポートのポートを変更したい場合、ポリシー マネージャのセットアップを再実行して、セットアップ ウィザーでのWeb レポートのポートを変更することを推奨します。

また、`HKEY_LOCAL_MACHINE\SOFTWARE\Data Fellows\F-Secure\Management Server 5` のレジストリ キーを編集して、Web レポートのポートを変更することも可能です。

1. ポリシー マネージャ サーバを停止します。
2. `HKEY_LOCAL_MACHINE\SOFTWARE\Data Fellows\F-Secure\Management Server 5` のレジストリ キーを開きます。
3. `WRPortNum` の値を新しいポート番号に変更します。

   ポートを指定する際には、**Decimal** が **Base** オプションとして選択されていることを確認してください。
4. ポリシー マネージャ サーバを起動します。

   ポートが競合していると、ポリシー マネージャ サーバは起動することができません。その際にはログ ファイルにエラー メッセージが出力されます。

第
8
章

ポリシー マネージャ プロキシ

トピック：

- *概要*

ここでは、ポリシー マネージャ プロキシについて説明します。

ポリシー マネージャ プロキシに関する基本的な情報を参照できます。

概要

ポリシー マネージャ プロキシは、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ってポリシー マネージャ プロキシの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 プロキシはポリシー マネージャ プロキシまたはポリシー マネージャ プロキシの更新サーバから取得したパターン ファイルの更新をキャッシュします。ポリシーマネージャ プロキシは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、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。ポリシー マネージャ プロキシはポリシー マネージャ プロキシの配布サーバからパターン ファイルを直接入手し、ポリシー マネージャ プロキシを実行しているホストはパターン ファイルをローカルのポリシーマネージャ プロキシから取得します。

第
9
章

トラブルシューティング

トピック：

- *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*
- *ポリシー マネージャ**Web** レポート*
- *ポリシーの配布*

ここでは、ポリシー マネージャ サーバに関するトラブルシューティング情報と FAQ (よくある問い合わせ) を紹介します。

製品で問題が発生した場合、ここで解決方法を見つけられるかもしれません。

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

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 コンソールに関するトラブルシューティング情報と FAQ (よくある問い合わせ) を紹介します。

Q	A
ポリシー マネージャ サーバが起動しません。	次のファイルに、ランタイムエラー、警告、およびその他の情報が含まれています。 `<F-Secure>\Management Server 5\logs\fspms-webapp-errors.log` と `<F-Secure>\Management Server 5\logs\fspms-sersvice.log` アクセス権 (`properties/security/permissions`) にローカルのユーザ アカウントが含まれていることを確認します。アカウントが認証済みのユーザとして含まれていない場合、ユーザを手動で追加し、アクセス権を [フル コントロール] に設定します。管理サーバ5のフォルダ (デフォルトでは`C:\Program Files\F-Secure\Management Server 5`) とサブフォルダにアクセス権を同様に設定します。変更後、ポリシー マネージャ サーバを再開します。または、コンピュータを再起動します。 ローカル サービスのアカウントは Windows のシステム アカウントで、ポリシー マネージャ サーバのサービスはこのユーザ アカウントで起動されます。通常のインストールでは、管理サーバ5フォルダのアクセス権限が自動的に設定されますが、フォルダをコピーしたり、復元したりした場合、アクセス権が正しく設定されていない可能性があります。そのような場合、上記の方法でアクセス権を正しく設定してください。

ポリシー マネージャ サーバ機能のログ ファイルと設定ファイルはどこにありますか?	ログファイルは次の場所にあります。
	`<F-Secure>\Management Server 5\logs`
	設定ファイルは次の場所にあります。
	`<F-Secure>\Management Server 5\conf`

ポリシー マネージャ コンソールのログ ファイルはどこにありますか?	ログファイルは次の場所にあります。
	`<F-Secure>\Administrator\lib\administrator.error.log`
	[ポリシーを配布] で適用されるポリシーの変更は次のログに記録されます。
	`fspms-policy-audit.log`

Q	A
インストール中に移行ウィザードが表示されませんでした。単体でウィザードを実行できますか?	移行ウィザードは次のファイルを実行することで起動できます。 `<F-Secure>\Management Server 5\bin\fspms-migration-wizard.exe`
管理者のパスワードを忘れました。パスワードを回復またはリセットできますか?	`admin` ユーザのパスワードを忘れた場合、またはアカウントを削除した場合、次のツールでユーザ アカウントをリセットできます。 `<F-Secure>\bin\reset-admin-account.bat` 注: リセット ツールを実行する前にポリシー マネージャ サーバを停止する必要があります。
サーバの機能を変更したら、ポリシー マネージャ サーバは停止しますか?	ドメイン コントローラのサーバとメンバー/スタンドアロンのサーバは異なるアカウントを使用します。ドメインコントローラではドメイン アカウントが、メンバー サーバではローカルのアカウントが使用されます。ポリシーマネージャ サーバは固有のアカウントを使用するため、サーバの機能を変更したらこのアカウントは無効になります。 サーバの機能を変更した場合、ポリシー マネージャ サーバを最も簡単に復元する方法は、ポリシーマネージャ サーバを [既存の設定を保存する] を選択した状態で再インストールすることです。これを行うと、ポリシー マネージャ サーバのアカウントは更新され、ファイルのアクセス権限も正しい設定にリセットされます。

Windows のセキュリティを強化すると、ポリシーマネージャ サーバの動作はどのように影響されますか?	アクセス権の制限、特に `%SystemRoot%` フォルダ (`c:\windows` または `c:\winnt`) で指定される制限がポリシーマネージャ サーバの起動を停止する可能性があります。ポリシーマネージャ固有のアカウント (ローカル サービス) はネットワーク関連の DLL と SYS ファイルを読み取る権限が必要です。
	ローカル サービス のアカウントに、次のフォルダを読み取れる権限を許可してください。
	`%SystemRoot%`
	`%SystemRoot%\system32`
	`%SystemRoot%\system32\drivers`
	サービス制限の中では、ポリシーマネージャ サーバの起動を拒否するものもあります。詳細については、Microsoft Windows Server の取扱説明を参照してください。

Q	A
ポリシー マネージャ コンソールとポリシー マネージャ サーバの接続が切断します。	ポリシー マネージャ コンソールとポリシー マネージャ サーバが別々のコンピュータで動作している場合、ネットワークの問題で接続が影響される可能性があります。ネットワークスイッチの変更などで、ポリシー マネージャ コンソールとポリシー マネージャ サーバの間で接続が失われた問題がいくつかあります。通常、このような問題は影響されているマシンのネットワークドライバを更新すること、またはポリシーマネージャ コンソールとポリシーマネージャ サーバの新しいスイッチとネットワークカードを更新することによって解消されます。 ポリシー マネージャ コンソールがポリシー マネージャ サーバと同じコンピュータにインストールされている場合、ポリシー マネージャ サーバのネットワーク負荷が多い理由で、利用可能のネットワーク接続が1つもない可能性があります。その結果、ポリシーマネージャ コンソールとすべてのホストがネットワークのリソースを競合している可能性もあります。 また、ホストのポーリング間隔を長くしたり、Windows のネットワーク タイムアウト設定を短くしたり、Windows のネットワーク ポート数を増やしたりすることで、ネットワークの負荷を軽くすることができます。 下記の設定は本製品を効率的に使用するための Windows のネットワーク設定です。 `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\MaxUserPort` (ネットワークの最大ポート数、デフォルト=5000) `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpTimedWaitDelay` (非アクティブのネットワーク接続を閉じるまでの待ち時間、デフォルト=240 seconds). `netstat -an` のコマンドを使用すると、サーバの接続数を確認できます。
サーバが要求を受信するポートを変更するにはどうすれば良いですか?	デフォルトでは、管理モジュール (ポリシー マネージャ コンソールからの要求を処理するコンポーネント) はポート8080を利用し、ホスト モジュール (ワークステーションからの要求を処理するコンポーネント) はポート80を利用します。これらのポートはインストール中に変更できます。 次の方法で、インストール後にポートを変更できます。 **1.** ポリシー マネージャ サーバを停止します。

Q	A
	2. `HKEY_LOCAL_MACHINE\SOFTWARE\Data Fellows\F-Secure\Management Server 5` のレジストリ キーを開きます。 **3.** `AdminPortNum` (管理モジュール) と `HttpPortNum` (ホストモジュール) の値を変更し、新しいポート番号を指定します。 ポートを指定する際には、**Decimal** が **Base** オプションとして選択されていることを確認してください。 **4.** ポリシー マネージャ サーバを起動します。 注意: ホストが (ホスト モジュールを通じて) ポリシー マネージャ サーバにアクセスするように設定されている場合、ホスト ポートを変更しないでください。エージェントがこのポートを通信に使用しているため、ワークステーションがサーバに接続できなくなる可能性があります。

ポリシー マネージャ Web レポート

ログ ファイルと設定ファイルのパスについて説明します。

Q	A

Web レポート機能のログ ファイルと設定ファイルはどこにありますか?	ログファイルは次の場所にあります。
	`<F-Secure>\Management Server 5\Web Reporting\logs`
	設定ファイルは次の場所にあります。
	`HKEY_LOCAL_MACHINE\SOFTWARE\Data Fellows\F-Secure\Management Server 5` のレジストリ キー
	次の場所にあるポリシー マネージャ サーバの設定ファイルを確認します。
	`<F-Secure>\Management Server 5\conf`

ポリシーの配布

ここでは、ポリシーの配布に関するエラー メッセージについて説明します。

Q	A
ポリシーを配布しているときに、ポリシーマネージャ コンソールが無効なポリシー値に関するエラー メッセージを表示します。どうすれば良いですか?	該当するエラー メッセージに関する情報を以下から参照してください。

エラーメッセージ	原因	解決方法
"<setting name>" に制限外の値があります。 "<setting name>" に無効な制限があります。 "<setting name>" に無効な値があります: "<value>"	原因1: 指定した値がサブドメインまたはホストで選択できる値ではない可能性があります。または、値が制限範囲より低いまたは高い値であること。あるいは、選択した値が空であります。 ドメインに異なるバージョンの製品をインストールしているホストがある場合、製品の最新バージョンのMIB設定がポリシー値の編集に使用されます。製品の旧バージョンは新しいポリシーの設定や値に対応していないため、旧バージョンをインストールしているホストに対するポリシーの配布は失敗する可能性があります。	ホストをサブドメイン別にグループ化します。最新のバージョンには新しいポリシー値を、旧バージョンには別のポリシー値を使用できるようになります。次の方法でこのドメイン構造を構築できます。 **1.** ホストを、使用している製品のバージョンに応じてグループ化します。たとえば、クライアント セキュリティ 6.x をインストールしている各ホストを1つのサブドメインに指定して、クライアント セキュリティ 7.x をインストールしている各ホストを別のサブドメインに指定することができます。 **2.** 主な設定をルート ドメインで指定して、例外を処理するためのサブドメインを作成します。このドメイン構造は旧バージョンをインストールしているホストの数が少ない場合に効率的です。
	原因2: 入力した整数がポリシー値が制限外である可能性があります。	
"<settingname>" が必要ですが、定義されていません。	設定に対する値が指定されていません。	値を入力するか、または [消去] の操作を適用して、親ドメインまたは MIB から値を再継承します。値が複数のドメイン階層で空の場合、[消去] の操作を数回実行する必要があるかもしれません。

第
10
章

llaunchr のエラー コード

トピック：

- *エラー コード*

ここでは、**llaunchr** コンポーネントで発生するエラーについて説明します。

llaunchr コンポーネントに関するエラー コードを確認して、問題解決を行うことができます。

エラー コード

`Ilaunchr.exe`でインストールをサイレント モードで実行すると、インストールの結果を示す終了コードが表示されます。

ログイン スクリプトを使用して、インストールの問題解決を行うことができます。例:

```
Start /Wait ILaunchr.exe \\server\share\mysuite.jar /U if errorlevel 100 Go to
Some_Setup_Error_occurred if errorlevel 5 Go to Some_Ilaunchr_Error_occurred if
 errorlevel 3 Go to Problem_with_JAR_package if errorlevel 2 Go to
User_does_not_have_admin_rights if errorlevel 1 Go to FSMA_was_already_installed
 if errorlevel 0 Echo Installation was OK!
```

エラー コード

エラー コード	説明
0	インストールが完了しました。
1	FSMA はすでにインストールされています。
2	ユーザに管理者権限がありません。
3	JAR が見つかりません。
4	JAR が壊れています。
6	インストール パッケージの解凍中にエラーが発生しました。
7	インストール先のディスクに空き容量がありません。
8	`package.ini` が JAR ファイルに含まれていません。
9	`package.ini`に作業プロセスが含まれていません。
10	コマンドラインまたは `.ini` ファイルに不正なパラメータがあります。
11	新しい作業プロセスの初期化中にエラーが発生しました。
12	インストール プロセスの作成中にエラーが発生しました。
13	一時ディレクトリを作成できませんでした。
14	不明なエラーです。
100	サイレント モードでインストールを行うために必要なデータが不足しています。JAR ファイルが無効です。
101	更新が無効になっています (セットアップはインストールを更新しようとしました)。
102	`product.ini` の読み取りが失敗しました。
103	`prodsett.ini`に無効なデータが検出されました。
104	管理エージェントによりインストールがキャンセルされたか、競合するソフトウェアが検出されました。インストールは中止されました。

エラー コード	説明
105	ライセンス キーコードが間違っているか、入力されていません。インストールは中止されました。
110	ディスクの空き容量が不足しています。
111	インストール先のドライブがローカル ドライブではありません。
120	ユーザがマシンに対する管理者権限を持っていません。
130	解凍したファイルをインストール先のディレクトリにコピーできませんでした。
131	アンインストール プラグインを製品のインストール先ディレクトリにコピーできませんでした。
132	`product.ini` を一時ディレクトリにコピーできませんでした。
133	製品ファイルをインストール先ディレクトリへコピーしている最中にエラーが発生しました。
134	`prodsett.ini` をコピーできません。
140	スイートの新しいバージョンが検出されました。
150	製品のプラグイン dll を読み込みできませんでした。
151	インストール サポート dll を読み込みできませんでした。
152	ラッパー dll を読み込みできませんでした。
160	キャビネット ファイルを初期化できませんでした。
170	管理エージェントのセットアッププラグインがエラーを返しました。
171	プラグインが予期しないコードを返しました。
172	プラグインがラッパー コードを返しました。
173	前回のインストール操作またはアンインストール操作が完了していません。操作を完了するために再起動が必要です。
174	前回のインストール操作またはアンインストール操作を完了させるために、インストール先のマシンが再起動されました。インストール情報を再送信してください。
200	部分的に成功しました。一部の製品のインストールが失敗しました。

第
11
章

FSII リモート インストールのエラー コード

トピック：

- *エラー コード*

リモート インストールの実行中に問題が発生した場合、ここに記載されている情報を参照することでトラブルシューティングを行えます。

ここでは、「**Windows** ホストを自動検出」で発生するエラー コードとメッセージについて説明します。

エラー コード

ここでは、リモート インストールで発生する一般的なエラーコードとメッセージについて説明します。

Windows エラー コード

エラー コード	説明
1057	ユーザ アカウント名が無効、または存在しません。
5	アクセスが拒否されています。[このアカウント] を使用している場合、管理者はドメイン権限でポリシー マネージャ コンソールにログインしている必要があります。ドメインの信頼レベルで、信頼済みドメインのアカウントを使用してポリシー マネージャ コンソールにログインしていることを確認してください。
1069	ログインが失敗しました。ログインとパスワードを確認してください。
1722	RPC サーバを利用できません。インストール中にホストをすぐに再起動したことでポリシー マネージャ コンソールがインストールの完了を確認する時間がなかった可能性があります。
1219	ポリシー マネージャ コンソールがインストール先のワークステーションに対してネットワークの接続を開いています。別のユーザアカウントで接続を開く前に、この接続を切断してください。

エラー メッセージ

エラーメッセージ	説明
必要な権限が使用中のアカウントに与えられていません。権限を手動で追加してください。	デフォルトでは、管理者もポリシー マネージャ コンソールで必要な「オペレーティングシステムの一部として機能」権限を持っていません。この権限を持っていない場合、Windows NT は FSII によるユーザアカウントの認証を許可することができません。権限は、Windows NTの ユーザ マネージャ > 原則 > ユーザの権利 から追加できます。
管理エージェントによりインストールがキャンセルされました。または、競合するソフトウェアが検出されました。	以下のような場合、管理エージェントはインストールをキャンセルします。 • 競合するサードパーティのソフトウェアが検出された場合 • ポリシー マネージャ サーバ の URL が無効の場合
CD キーが無効または入力されていないため、インストールが中止しました。	入力したライセンス キーコードが無効の場合、リモート ホストでインストールを開始することはできません。キーコードを確認してください。

エラーメッセージ	説明
ホストのディスク空容量が不足しています。	通常の環境では、ホストの空き容量が少なくても 20 MB 必要です。
重大な **FSMAINST (F-Secure** 管理エージェント インストール プラグイン**)** エラーにより、管理エージェントのインストールが失敗しました。詳細は、ホストのログ ファイルを参照してください。	管理エージェントのインストール中に重大なインストールエラーが発生ました。管理エージェントを手動でホストにインストールすることを推奨します。また、エラーエラー キーワードを`fswssdbg.log`で調べることもできます。このファイルは Windows フォルダにあります。
F-Secure 製品の新しいバージョンが検出されました。インストールを中止します。	インストール先のホストに製品の新しいバージョンがすでにインストールされている場合、その製品をアンインストールしない限りインストールを実行することはできません。
prodsett.ini で無効なデータが検出されました。	`prodsett.ini` に含まれている情報が無効です。ファイルを手動で編集した場合は、設定が正しいことを確認してください。`prodsett.ini`を直接編集するより、JARファイルをエクスポートし、**ILAUNCHR**を使用してインストールを行うことを推奨します。

第
12
章

ネットマスクの NSC 表記

トピック：

- *NSC 表記について*

ここでは、NSC 表記について説明します。

ネットワーク アドレスとネットマスクを組み合わせた表記方法を紹介します。

NSC 表記について

NSC 表記は、ネットワーク アドレスとネットマスクを組み合わせた表記方法です。

NSC 表記は、ネットワーク アドレスの後にスラッシュとネットマスクの1ビットの数を追加します。例:

ネットワーク アドレス	ネットマスク	**NSC** 表記
192.168.0.0	255.255.0.0	192.168.0.0/16
192.168.1.0	255.255.255.0	192.168.1.0/24
192.168.1.255	255.255.255.255	192.168.1.255/32

NSC 表記は、1ビットが先頭から連続して立てていないネットマスクを使用しているネットワークでは使用できません。以下の表に、使用できるネットマスクのビット数を示します。

0.0.0.0/0 は、デフォルトのルート用に予約された特殊なネットワーク定義です。

ネットマスク	ビット数
128.0.0.0	1
192.0.0.0	2
224.0.0.0	3
240.0.0.0	4
248.0.0.0	5
252.0.0.0	6
254.0.0.0	7
255.0.0.0	8
255.128.0.0	9
255.192.0.0	10
255.224.0.0	11
255.240.0.0	12
255.248.0.0	13
255.252.0.0	14
255.254.0.0	15
255.255.0.0	16
255.255.128.0	17
255.255.192.0	18
255.255.224.0	19
255.255.240.0	20
255.255.248.0	21
255.255.252.0	22
255.255.254.0	23
255.255.255.0	24
255.255.255.128	25
255.255.255.192	26
255.255.255.224	27

ネットマスク	ビット数
255.255.255.240	28
255.255.255.248	29
255.255.255.252	30
255.255.255.254	31
255.255.255.255	32