F-Secure Linux Security

目次

はじめに

トピック：

本書では、F-Secure Anti-Virus Linux Securityの設定、機能、操作方法、サポート情報などについて説明しています。

コンピュータウイルスは、コンピュータに保存されたデータを脅かす重大の脅威の1つです。一部には無害なウイルスもありますが、多くは実際に脅威でありデータを破壊します。

本製品は、ネットワークからの不正アクセス、不正なシステム改ざん、ユーザスペースおよびカーネルルートキットから保護する、強力なリアルタイムウイルス・リスクウェア保護機能、ホスト型侵入防止システム(HIPS)機能を、すぐに利用できる統合セキュリティソリューションとして提供します。本製品はウェブインターフェースまたは「F-Secureポリシーマネージャ」を使用することによって、配備と管理を簡単に行えます。

F-Secureポリシーマネージャはセキュリティポリシーの定義と配布を行い、アプリケーションのセキュリティを総合的に監視する集中管理ツールです。

本製品はF-Secureプロテクションサービスビジネスと連携し、複数のコンピュータをウェブインターフェースから監視することが可能です。

1.1 特長

本製品は侵入を検知して防止する機能を備えており、コンピュータをマルウェア (悪意のあるソフトウェア) から保護します。

インストール後の初期状態では、細かい設定をする必要はなく、サーバはすでに保護されている状態になります。

1.1.1 マルウェア対策

本製品はシステムをウイルスや危険性のあるファイルから保護します。

ユーザがインターネットからファイルをダウンロードすると (たとえば電子メールのリンクをクリックして)、そのファイルは開く前に自動的にスキャンされます。

- 「*リアルタイムスキャン*」はファイルを開いたり、コピーしたり、インターネットからダウンロードしたりするときに実行されるウイルスとリスクウェアから常に保護します。この機能は透過的に動作し、ハードディスク、CDなどのメディアやネットワークドライブがアクセスされるたびにウイルスの検出を行います。感染したファイルにアクセスしようとすると、リアルタイムスキャンは自動的にウイルスの実行を阻止します。
- リアルタイムスキャンが特定のファイル/ディレクトリをスキャンするように設定されている場合、「*マニュアルスキャン*」を使用してシステム全体をスキャンすることができます。また、「スケジュールスキャン」を使用してシステム全体に定期的なスキャンを設定することも可能です。
- 「*自動更新*」はウイルス定義ファイルとスパイウェアの定義ファイルを自動的に更新して、本製品の保護機能を常に最新の状態にします。本製品をインストールした後、この機能は有効になり、ウイルス定義ファイルは自動的に更新されるようになります。更新されるウイルス定義ファイルはF-Secureのアンチウイルス研究チームによって署名されています。

1.1.2 ホスト型侵入防止システム (HIPS)

「ホスト型侵入防止システム (*HIPS*)」はホスト上の不審な動きを検知し、システムを保護します。

- 「*完全性検査*」はシステムを不正な変更から保護します。この機能は既知の構成 (正常で問題がないシステムの状態) に基づいて、システムの安全性を確認します。安全で問題がない既知の構成を記録するためには、ネットワークに接続していない状態で本製品をインストールすることを推奨します。

  保護したいファイルのベースラインを作成して、すべてのユーザに対してファイルの変更を阻止することができます。
- 「*ファイアウォール*」は、Netfilterとiptablesに基づいたパケットフィルタで処理状態を把握する機能です。この機能はコンピュータを不正なアクセスから保護するためにお役に立ちます。ファイアウォールにはオフィスや外出先などの環境に適したセキュリティレベルがいくつかプリセットされています。
- 第三者がシステムに侵入してユーザアカウントを追加しようとすると、ホスト型侵入防止システム (*HIPS*) は変更されたシステムファイルを検知し、管理者に警告を送ります。
- 第三者がシステムに侵入して、各種ユーティリティを置き換えるユーザスペースのルートキットをインストールしようとすると、ホスト型侵入防止システム (*HIPS*) は変更処理されたシステムファイルを検知し、管理者に警告を送ります。

1.2 主な機能

本製品はウイルスやワームなどマルウェアに対する強力な保護機能を備え、透過的に動作します。

1.2.1 ウイルス/ワーム対策

本製品はLinux対応のファイルシステムにあるファイルをスキャンします。複数のオペレーティングシステムを搭載したマルチブート環境のコンピュータに最適なソリューションです。

- Linux上の対応ファイルシステムに対するスキャン機能

  注: NFSサーバ上ではリアルタイムスキャンを利用できません。他のスキャン (マニュアルスキャンやスケジュールスキャン) は実行できます。

- 複数のスキャンエンジンを使用した高性能検出機能
- 不審で危険性のあるファイルを検出するヒューリスティックスキャンエンジン
- リスクウェアの検出とカテゴリへの分類
- ユーザが保護をバイパスできないように設定可能
- ファイルを開く/閉じる、実行する前に行われるウイルススキャン
- スキャン対象 (ファイル/ディレクトリ)、スキャン方法およびマルウェアを検出した場合の処理と通知方法
- 圧縮ファイルの再帰的スキャン
- デジタル署名を利用したウイルス定義ファイルの更新
- プリセットセキュリティレベル搭載のファイアウォール。プロトコル別のネットワークトラフィックを許可/拒否するルールセット機能

1.2.2 透過的な処理

エンドユーザに対して透過的の動作

- 使いやすいウェブインターフェース
- ウイルス定義ファイルの自動更新

1.2.3 重要なファイルに対する保護機能

重大なシステムファイルの情報を保存し、アクセスされる前にファイルを自動で確認

- ファイルの無断変更 (トロイの木馬からなど) を阻止
- システムファイルの変更を検出し、管理者に警告を通知

1.2.4 設定、配備、管理

インストール後の初期状態で多くのシステムを十分に保護

- セキュリティポリシーを1つの場所から一元的に配布

1.2.5 警告オプション

感染ファイルの情報を管理者に通知するための豊富な監視と警告機能

- F-Secureポリシーマネージャコンソール、指定のメールアドレス、syslogに警告を通知

配備

トピック：

本製品はスタンドアロンまたは集中管理されたLinuxのコンピュータに配備することができます。

2.1 多数のスタンドアロンLinuxワークステーションへの配備

ポリシーマネージャまたはプロテクションサービスビジネスを通じて本製品を複数のワークステーションに導入できます。

ポリシーマネージャの管理モードでインストールを行う場合、F-SecureポリシーマネージャがすべてのLinuxマシンを管理します。各ユーザに該当するマシンのインストールを担当させ、F-Secureポリシーマネージャコンソールからインストールの進捗を監視することを推奨します。ホスト上のインストールが完了したら、ホストが自動登録の要求をF-Secureポリシーマネージャに送ります。F-Secureポリシーマネージャコンソールを使用して、どのホストが要求を送信したか確認できます。

プロテクションサービスビジネスの管理モードでインストールを行う場合、プロテクションサービスビジネスのポータルがすべてのLinuxマシンを管理します。各ユーザに該当するマシンのインストールを担当させ、プロテクションサービスビジネスのポータルから登録したホストを監視することを推奨します。登録済みのホストに製品の最新版が送られ、アップデートを利用できるときにはホストに通知が送信されます。

複数のLinuxマシンを集中管理されていない環境に配備した場合、各マシンのユーザはソフトウェアをそれぞれのマシンにインストールすることができます。

Linuxマシンが少ないネットワークでは、プロテクションサービスビジネスのポータルまたはF-Secureポリシーマネージャの代わりにウェブインターフェースを管理用に使用できます。

2.2 多数の集中管理されたLinuxワークステーションへの配備

特定の管理システムで多数のコンピュータを管理している場合、製品を各ワークステーションにインストールすることができます。

複数のLinuxマシンをRed Hatネットワークや Ximian Red Carpetなどで管理している場合、既存の管理システムからソフトウェアをサーバに配布できます。

2.3 イメージファイルを使用した集中配備

複数のコンピュータを集中管理している環境では、本ソフトウェアを一元的に各コンピュータにインストールすることができます。

本製品を複数のコンピュータにインストールする場合、本製品を含めたディスクのイメージファイルを作成して、それぞれのコンピュータにソフトウェアを複製することができます。

ディスクイメージソフトウェアの使用中に各コンピュータが一意のIDを使用していることを確認します。

1. イメージファイルに本製品を含むソフトウェアとシステムをインストールします。
2. 本製品が指定のF-Secureポリシーマネージャサーバを使用するように設定します。ただし、ホストがF-Secureポリシーマネージャサーバに自動登録の要求を送信した場合、F-Secureポリシーマネージャサーバコンソールにホストをインポートしないでください。イメージファイルをインストールするホストのみインポートします。
3. 次のコマンドを実行します。`/etc/init.d/fsma clearuid`
   ユーティリティプログラムによって、一意のIDがリセットされます。
4. コンピュータをシャットダウンして、イメージファイルが作成されるまでは再起動を控えます。
5. ディスクイメージファイルを作成します。

システムの再起動中に一意のIDが自動的に作成されます。この処理はイメージファイルがインストールされた各マシン上で個別に実行されます。

各コンピュータの再起動後に自動登録の要求がF-Secureポリシーマネージャに送られます。これらの要求は通常通りに処理できます。

インストール

トピック：

本製品はスタンドアロンまたは集中管理でインストールすることができます。

3.1 システム要件

システム要件の一覧

OS:	対応しているディストリビューションの一覧は製品のリリースノーツに記載されています。
プロセッサ:	686
メモリ:	フルインストール: 1024 MB 以上 コマンドラインモード: 512 MB 以上 (1024 MB 以上推奨) 注: スワップメモリが十分あることを推奨します。
ディスク容量:	3 GB
必須コンポーネント:	Linuxカーネル2.6以降 Glibc 2.3.4以降 64ビットのディストリビューションでは32ビットの互換ライブラリが必要です。

注: ウェブインターフェースはFirefox 2 以降とInternet Explorer 6/7のブラウザで利用できます。

Dazukoのバージョンについて

リアルタイムウイルススキャン、完全性検査、およびルートキット保護の機能を使用するにはDazukoカーネルモジュールが必要になります。Dazukoはオープンソースのカーネルモジュールで、ファイルを操作するためのインターフェースを提供します。詳細については、*http://www.dazuko.org*を参照してください。

本製品のインストール中にDazukoのドライバがインストールされます。

本製品は付属のDazukoを使用するように広範囲にわたって検証されています。他のDazukoバージョン、または特定のLinuxディストリビューションで提供されているDazukoはサポートされていません。また、そのようなDazukoのバージョンを使用することを推奨しません。

3.1.1 システムリソース

本製品が使用するシステムリソースの一覧

インストールファイル/ディレクトリ

本製品のインストール時に生成されるファイルは以下のディレクトリにそれぞれ格納されます。

- `/opt/f-secure`
- `/etc/opt/f-secure`
- `/var/opt/f-secure`

また、以下のシンボリックリンクもインストール時に作成されます。

- `/usr/bin/fsav -> /opt/f-secure/fssp/bin/fsav`
- `/usr/bin/fsic -> /opt/f-secure/fsav/bin/fsic`
- `/usr/share/man/man1/fsav.1 -> /opt/f-secure/fssp/man/fsav.1`

- `/usr/share/man/man8/fsavd.8 -> /opt/f-secure/fssp/man/fsavd.8`

logrotate設定ファイルのインストール先:

- `/etc/logrotate.d/fs-linux-security`

initスクリプトのインストール先:

- `/etc/init.d/fsma`

変更されるシステムファイル

- `/etc/passwd`: ユーザ アカウント (fsma と fsaua) がインストール中に作成されます
- `/etc/group`: グループ (fsc) インストール中に作成されます
- rootユーザのcrontab : スケジュールスキャンのタスクは作成されるたびにcrontabに追加されます。

ネットワークリソース

以下のIPポートは本製品の起動中に使用されます。

インターフェース	プロトコル	ポート	コメント
lo	tcp	28005	ウェブインターフェースの内部通信ポート
lo	tcp	28078	PostgreSQLの警データベース
lo	tcp	28080	ウェブインターフェースのローカルアクセス
任意	tcp	28082	リモートSSLウェブインターフェースのアクセス (有効の場合)

メモリ

ウェブインターフェースは200MB以上のメモリを確保しますが、常時使用されないため通常はスワップされます。他のコンポーネントは合計128MBほどのメモリを使用し、その大部分はオンアクセスのスキャナに使用されます。

メモリの消費はファイルのアクセス量によって異なります。複数のユーザがシステムにログインし、多くのファイルをアクセスしている場合、メモリの消費は多くなります。

CPU

プロセッサの負荷もファイルのアクセス量によって異なります。

多くのユーザがシステムにログインしている場合、CPUの負荷は高くなります。

アプリケーションの中には仕様で多くのファイルをアクセスするものがあり、リアルタイムでのファイルアクセス検査が非常に遅くなることがあります。

3.2 スタンドアロンインストール

「スタンドアロンインストールモード」はLinuxワークステーション/サーバが少ない環境、またはF-Secureポリシーマネージャによる集中管理が不要な場合に適切です。

インストールする前に、コンパイラとカーネルのソースを事前にインストールしている必要があります。インストールの確認方法については、製品のリリース ノーツにあるF-Secureコミュニティ ページを開いて該当するディストリビューションの指示を参照してください。

インストールを実行するにはroot権限のあるアカウントが必要です。

1. インストールファイルをハードディスクの任意の場所にコピーします。次のコマンドを使用してインストールファイルを解凍します。`tar zxvf f-secure-linux-security-<version>.<build>.tgz`
2. インストールファイルが実行可能か確認します。`chmod a+x f-secure-linux-security-<version>.<build>`
3. 次のコマンドを実行して、インストールを開始します。`./f-secure-linux-security-<version>.<build>`
4. ライセンス使用許諾契約が表示されます。同意する場合は`yes`と入力して、ENTERを押します。

インストールが完了します。

インストール後、ウェブインターフェースで製品の設定を変更できます。ウェブインターフェースはブラウザに次のURLを入力するとアクセスできます。http://localhost:28080/fsecure/webui/

ウェブインターフェースのリモートアクセスは、`fsav-config`をコマンドラインから実行することで設定できます。リモートアクセスを有効にしたら、ウェブインターフェースは https://host.domain:28082/fsecure/webui/でアクセスできるようになります。

host.domainには、本製品がインストールされているコンピュータのホスト名またはIPアドレスが指定されます。

`fsav-config`の詳細については、付録Aのfsav-configページを参照してください。

注: `fschooser`をコマンドラインから実行すると、本製品の機能をいくつか無効にできます。

3.3 ポリシーマネージャによる集中管理

ポリシーマネージャによる集中管理を実行している場合、本製品はローカルでインストールされ、別のコンピュータにインストールされているF-Secureポリシーマネージャによって管理されます。

インストールする前に、コンパイラとカーネルのソースを事前にインストールしている必要があります。インストールの確認方法については、製品のリリース ノーツにあるF-Secureコミュニティ ページを開いて該当するディストリビューションの指示を参照してください。

本製品をインストールする前にF-Secureポリシーマネージャが別のコンピュータにインストールされている必要があります。F-Secureポリシーマネージャコンソールのインストールについては、『F-Secure ポリシーマネージャの管理者ガイド』 を参照してください。

注: 本製品をF-Secureポリシーマネージャ (Windows版 9.1、aqualnx32チャネルをデフォルトで含めていない) で使用するには、`C:\ProgramFiles\F-Secure\FSAUA\program\fsauarep.cfg` に次の行を挿入する必要があります。`subscribe 0,aqualnx32`

注: F-SecureポリシーマネージャコンソールのアンチウイルスモードではLinux製品を管理できません。管理を実施するには、詳細モードを使用してください。

インストールを実行するにはroot権限のあるアカウントが必要です。

1. インストールファイルをハードディスクにコピーします。次のコマンドを実行してインストールファイルを解凍します。`tar zxvf f-secure-linux-security-<version>.<build>.tgz`
2. インストールファイルが実行可能か確認します。`chmod a+x f-secure-linux-security-<version>.<build>`
3. 次のコマンドを実行して、インストールを開始します。`./f-secure-linux-security-<version>.<build>`
4. ライセンス使用許諾契約が表示されます。同意する場合は`yes`と入力して、ENTERを押します。

インストールが完了します。

インストール後、ウェブインターフェースで製品の設定を変更できます。ウェブインターフェースはブラウザに次のURLを入力するとアクセスできます。http://localhost:28080/fsecure/webui/

ウェブインターフェースのリモートアクセスは、`fsav-config`をコマンドラインから実行することで設定できます。リモートアクセスを有効にしたら、ウェブインターフェースは https://host.domain:28082/fsecure/webui/でアクセスできるようになります。

host.domainには、本製品がインストールされているコンピュータのホスト名またはIPアドレスが指定されます。

`fsav-config`の詳細については、付録Aのfsav-configページを参照してください。

注: `fschooser`をコマンドラインから実行すると、本製品の機能をいくつか無効にできます。

3.4 プロテクションサービスビジネスの管理モードのインストール

プロテクションサービスビジネスの管理モードを使用する場合、本製品はローカルでインストールされ、プロテクションサービスビジネスのポータルを通じて管理されます。

インストールする前に、コンパイラとカーネルのソースを事前にインストールしている必要があります。インストールの確認方法については、製品のリリース ノーツにあるF-Secureコミュニティ ページを開いて該当するディストリビューションの指示を参照してください。

製品をインストールするにはプロテクションサービスビジネスのポータルアドレスキーコードが必要です。

インストールを実行するにはroot権限のあるアカウントが必要です。

1. インストールファイルをハードディスクにコピーします。次のコマンドを実行してインストールファイルを解凍します。`tar zxvf f-secure-linux-security-<version>.<build>.tgz`
2. インストールファイルが実行可能か確認します。`chmod a+x f-secure-linux-security-<version>.<build>`
3. 次のコマンドを実行して、インストールを開始します。`./f-secure-linux-security-<バージョン>.<ビルド> --auto psb fspsbs=<プロテクションサービスビジネスバックウェブサーバのアドレス> keycode=<キーコード>`
   プロテクションサービスビジネスバックウェブのサーバがライセンスを認証します。

インストールが完了します。

インストール後、`fsav-config`またはウェブインターフェースから製品を設定できます。

3.5 アップグレード

本製品の評価版またはの旧バージョンを使用している場合、それらをアンインストールする必要はなく、本製品をそのままインストールすることによってアップグレードが可能です。

3.5.1 旧バージョンからのアップグレード

F-Secure Linux Security 7以降を使用している場合、旧バージョンをアンインストールする必要はなく、本製品をそのままインストールすることによってアップグレードが行われます。それ以前のバージョンを使用している場合、アップグレードを行う前に旧バージョンをアンインストールしてください。

旧バージョンをアンインストールする際にはすべての設定とホストIDが保存されるため、F-Secureポリシーマネージャでホストを再度インポートする必要はありません。

重要: 集中管理されている環境では、F-SecureポリシーマネージャのMIBをアップグレードすることを忘れないでください。

旧バージョンのアンインストール

本製品の旧バージョンはアンインストールのコマンドまたはディレクトリとファイルを削除することでアンインストールできます。

1. バージョン5.x を使用している場合、次のコマンドでアンインストールを実行できます。`/opt/f-secure/fsav/bin/uninstall-fsav`
2. バージョン4.x を使用している場合、以下のディレクトリとファイルを削除することで製品をアンインストールできます。

   `/opt/f-secure/fsav/`

   `/var/opt/f-secure/fsav/`

   `/etc/opt/f-secure/fsav/`

   `/usr/bin/fsav`

   `/usr/share/man/man1/fsav.1`

   `/usr/share/man/man5/fsav.conf.5`

   `/usr/share/man/man5/fsavd.conf.5`

   `/usr/share/man/man8/dbupdate.8`

   `/usr/share/man/man8/fsavd.8`

   `/usr/share/man/man8/fsavschedule.8`

3.5.2 評価版のアップグレード

本製品の評価版をライセンス版にアップグレードすることができます。

評価期間が過ぎている場合、評価版をまずアンインストールする必要があります。

評価版をライセンス版にアップグレードするには、次の手順を実行します。

1. ウェブインターフェースを開きます。
2. 「バージョン情報」ページを開きます。
3. [キーコード] フィールドにライセンスキーコードをハイフンを含めた形で入力します。
4. 次のコマンドを実行すると、コマンドラインからプロテクションサービスビジネスの管理モードにアップグレードできます。`/opt/f-secure/fsav/sbin/convert_to_full_installation.sh --fspsbs=<プロテクションサービスビジネスバックウェブサーバのアドレス>`

   プロテクションサービスビジネスバックウェブサーバのアドレスとキーコードを入力します。

次のコマンドを実行すると、コマンドラインからもアップグレードを実行できます。`/opt/f-secure/fsav/sbin/convert_to_full_installation.sh`

👉 注: 評価期間が過ぎている状態でアップグレードを実行した場合、キーコードを入力した後に製品を再起動する必要があります。

3.5.3 プロテクションサービスビジネスのアップグレード

プロテクションサービスビジネスの管理モードを使用している場合、製品の新しいバージョンがプロテクションサービスビジネスのポータルから自動的にダウンロードされます。

新しいバージョンを利用できる際にはウェブユーザインターフェース上に通知が表示されます。インストーラを実行すると製品をアップグレードできます。

3.6 カスタムインストール

スタンドアロンまたは集中管理インストールを行う場合、デフォルトのオプションを変更したカスタムのインストールを実行することができます。

3.6.1 カスタムインストールの用意

本製品のインストールパッケージからRPMを解凍して、カスタムのインストールパッケージを作成することができます。

本製品のインストールパッケージはRPMを含めた自己解凍パッケージです。パッケージからRPMファイルを解凍するには、以下の手順を実行します。

1. `./f-secure-linux-security-<version>.<build> rpm`を実行します。
2. RPMパッケージをインストールします。
3. `/opt/f-secure/fsav/fsav-config`を実行します。

3.6.2 自動インストール

本製品はすべての手順を自動化した自動モードでインストールすることもできます。自動モードではコマンドラインからインストール情報を指定して、インストールを実行します。また、インストール中に確認のメッセージは一度も表示されません。

インストール時に次のコマンドラインオプションを実行します。

```
--auto MODE [fspms=FSPMSURL adminkey=/PATH/TO/ADMIN.PUB] [fspsbs=FSPSBURL]
lang=en|de|ja [no]remotewui [no]locallogin user=USER
kernelverify|nokernelverify pass=PASSPHRASE keycode=KEYCODE
```

`MODE`パラメータがスタンドアロンモードの場合、`standalone`を指定します。ポリシーマネージャの管理モードの場合、`managed`を指定します。プロテクションサービスビジネスの管理モードの場合、`psb`を指定します。

`MODE`に`managed`を指定した場合、F-Secureポリシーマネージャサーバの*URL*と管理者の*公開鍵*の場所を次のように指定する必要があります。`fspms=http://fspms.company.com/adminkey=/root/admin.pub`

`MODE`に`psb`を指定した場合、次のようにプロテクションサービスビジネスのポータルアドレスを指定する必要があります。`fspsbs=http://fspsb-bw.example.com`

使用できるオプション

lang	ウェブインターフェースの言語を選択します。
remotewui	ウェブインターフェースのリモートアクセスを許可します。
noremotewui	ウェブインターフェースのリモートアクセスを拒否します。
nolocallogin	ウェブインターフェースのローカルアクセスをログインなしで許可します。
locallogin	ウェブインターフェースのローカルアクセスにログインを必要とします。
user=USER	ウェブインターフェースのログインで使用するローカルアカウントを指定します。

pass=PASS	ベースラインの作成に必要なパスワードを指定します。
keycode=KEYCODE	ライセンスの認証に必要なキーコードを指定します。キーコードが指定されない場合、本製品は評価モードでインストールされます。
nofirewall	ファイアウォールを無効にします。

たとえば、1) スタンドアロンモードで、2) 英語のウェブインターフェース、3) リモートアクセスは無効、4) ローカルユーザはログイン不要の各種設定で本製品をインストールするには、以下のコマンドを使用します。

```
./f-secure-linux-security-<version>.<build> --auto standalone lang=en
noremotewui nolocallogin
```

3.6.3 コマンドライン専用モードでのインストール

コマンドライン専用モードインストールはコマンドラインスキャナと自動更新エージェントのみインストールします。

このインストールモードはF-Secureアンチウイルス Linux版4.6xから移行するユーザやリアルタイム保護、完全性検査、ウェブインターフェース、または集中管理の各機能 (AMaViS メールウイルススキャナを実行しているユーザなど) を必要としないユーザに適切です。

コマンドラインスキャナをインストールするには、インストール中に次のコマンドを実行します。

```
./f-secure-linux-security-<version>.<build> --command-line-only
```

旧バージョンからコマンドラインスキャナをアップグレードする場合、旧バージョンを先にアンインストールする必要があります。

コマンドライン専用モードでインストールした場合の設定は、設定ファイル (`/etc/opt/f-secure/fssp/fssp.conf`) を使用します。設定ファイルの詳細については、ファイルをご覧ください。

3.6.4 Sambaサーバ

本製品はSambaサーバや共有ディレクトリのデータを完全に保護することができます。

Sambaサーバに対して、本製品の機能をすべて利用できます。

1. F-Secure アンチウイルスSambaサーバ版をインストールしている場合、アンインストールしてから本製品をインストールしてください。`/opt/f-secure/fsav/bin/uninstall-fsav`でアンインストールを実行できます。
2. インストールを通常と同じように開始します。
   インストール後、Sambaの共有ディレクトリ/ファイルは保護されている状態になります。Windows ネットワーク (Samba) からのアクセスはファイアウォールによってブロックされますので、Samba の共有を有効にするにはファイアウォールルールを変更する必要があります。
3. ファイアウォールルールを変更して、Sambaの共有アクセスを許可します。
   - ウェブユーザインターフェースのファイアウォールルールウィザードを利用する場合 :
     1. 「一般タスク」ページを開いて、[ファイアウォールルールの作成] をクリックします。
     2. [使用しているコンピュータのサービスへのアクセスを許可します] を選択します。
     3. **[Windows networking (1)]** を選択します。
     4. ウィザードを終了します。
     5. **[Windows networking (2)]** のサービスを追加するためにウィザードをもう一度実行します。
   - ウェブインターフェースの詳細モードでファイアウォールルールエディタを利用する場合 :

1. ウェブインターフェースから [詳細モード] に移動します。
2. [ファイアウォール] を選択します。
3. 「ファイアウォールルール」ページで、利用するセキュリティレベルを [編集するセキュリティレベル] フィールドに指定します。
4. [新しいルールの追加] をクリックします。
5. [リモートホスト] フィールドにルール名 (`[myNetwork]` など) を指定して、ルールの説明も入力します。
6. ドロップダウンメニューから **[Windows networking (1)]** を選択して、サービスに追加するために [このルールにサービスを追加する] をクリックします。
7. ドロップダウンメニューから **[Windows networking (2)]** を選択して、サービスに追加するために [このルールにサービスを追加する] をクリックします。
8. テーブルの右側にある矢印を使用して、ルールを拒否ルールの上に移動します。
9. [保存] をクリックして、新しいルールを適用します。

- F-Secureポリシーマネージャコンソールでファイアウォールのルールエディタを利用する場合：

1. F-Secureポリシーマネージャコンソールの詳細モードで、管理するホストまたドメインを選択します。
2. **[Linux Security]** を選択して、「ファイアウォール」ページを開きます。
3. 「ルール」で、編集したいセキュリティレベルが指定されていることを確認します。
4. [前に追加] をクリックします。
5. ルールウィザードで、**[Windows networking (1)]** に対する着信トラフィックを許可します。
6. **Windows networking (2)**を追加するためにルールウィザードをもう一度実行します。
7. ポリシーを配布します。

   👉 **注:** ファイアウォールルールがローカルで編集された場合、ポリシーを配布する前に設定を確定してください。

新しいルールを追加するには、ファイアウォールを一時的に無効にする必要があります。

1. [ファイアウォール保護] を [無効] にします。または、コマンドラインから`/opt/f-secure/fsav/bin/fsfwc --mode bypass`を実行します。
2. セキュリティレベルを選択して、ファイアウォールルールを編集します。
3. ウェブインターフェースでファイアウォールを有効にします。コマンドラインの場合、次を実行します。`/opt/f-secure/fsav/bin/fsfwc --mode your_profile`(「`your_pfofile`」はプロフィール (block, mobile, home, office, strict, normal) を指します)

3.7 バックアップの作成

本製品に関連するデータはバックアップすることができます。

データをすべてバックアップするには、次のコマンドを実行します。

```
# /etc/init.d/fsma stop

# /etc/init.d/fsaua stop

# tar cpsf <backup-filename>.tar /etc/init.d/fsma /etc/init.d/fsaua
/etc/opt/f-secure /var/opt/f-secure /opt/f-secure

# /etc/init.d/fsaua start

# /etc/init.d/fsma start
```

バックアップからデータを復元するには、次のコマンドを実行します。

```
# /etc/init.d/fsma stop
```

```
# /etc/init.d/fsaua stop
# cd /
# rm -rf /var/opt/f-secure
# tar xpsf <backup-filename>.tar
# /etc/init.d/fsaua start
# /etc/init.d/fsma start
```

バックアップを復元した後、fsmaとfsauaユーザ、およびfscグループが存在していることを確認します(/etc/passwd、/etc/shadow、/etc/groupのファイルをバックアップすることで可能です)。

3.8 アンインストール

uninstall-fsavのコマンドを実行すると、本製品をアンインストールすることができます。

/opt/f-secure/fsav/bin/uninstall-fsavをrootで実行すると本製品はアンインストールされます。

アンインストール処理は設定ファイルを削除しません。設定ファイルが必要ない場合、/etc/opt/f-secure/fsmaにあるファイルをすべて削除してください。

本製品を使用する

トピック：

本製品はF-Secureポリシーマネージャコンソールまたはウェブインターフェースを使用して、管理を行うことができます。

4.1 F-Secureポリシーマネージャの基本

集中管理モードでは、F-Secureポリシーマネージャコンソールが F-Secure 製品の設定変更と統計を表示するために使用されます。

F-Secureポリシーマネージャで集中管理を行っている場合、本製品を F-Secureポリシーマネージャの環境に追加することができます。

注: F-Secureポリシーマネージャコンソールで Linux製品を管理するには詳細モードを使用する必要があります。アンチウイルスモードでは Linux製品を管理することはできません。

「**F-Secure Linux Security** > 設定」ページにある設定を使用して、本製品を構成してください。

注: [**F-Secure** セキュリティ プラットフォーム **Linux**]、[**F-Secure** 管理エージェント]、[**F-Secure** 自動更新エージェント] の下にある設定を編集して、本製品の動作を変更することができます。

F-Secureポリシーマネージャの詳細については、『F-Secure ポリシーマネージャ管理者ガイド』を参照してください。

4.2 ウェブインターフェースのアクセス

ウェブインターフェースはウェブアドレスからアクセスできます。

ウェブインターフェースは次のローカルアドレスからアクセスできます :

```
http://localhost:28080/fsecure/webui/
```

リモートアクセスを有効にした場合、次の HTTPSアドレスからウェブインターフェースをアクセスできるようになります :

```
https://<host.domain>:28082/
```

F-Secureポリシーマネージャとウェブインターフェースを同時に使用することも可能です。

注: 通常、ユーザは F-Secureポリシーマネージャが適用した設定をローカルのマシンで変更することができます。管理者が F-Secureポリシーマネージャの設定画面で [確定] のチェックボックスを選択している場合、ローカルユーザは設定を変更できなくなります。

4.3 アンチウイルス保護の動作確認

本製品が正常に機能しているか確認するために、ウイルスとして検出される専用のテストファイルを使用できます。

テストファイルは EICAR (European Institute of Computer Anti-virus Research) 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の情報は以下の URLでご覧になれます。*http://www.europe.f-secure.com/virus-info/eicar_test_file.shtml*

1. EICARのテストファイルをダウンロードまたは作成します。
   - EICAR テスト ファイルを次の URL からダウンロードします。*http://www.europe.f-secure.com/virus-info/eicar_test_file.shtml* または、
   - テキストエディタを使用して、次の1行を持つ eicar.comファイルを作成します。
     `X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`
2. `fsav eicar.com` を実行します。

ウイルスがファイル内に検出されます。

基本操作

トピック：

ウェブインターフェースを使用して、ステータスとレポートを確認し、製品の設定を変更することもできます。

ウェブインターフェースは次のローカルアドレスからアクセスできます：

```
http://localhost:28080/fsecure/webui/
```

リモートアクセスを有効にした場合、次のHTTPSアドレスからウェブインターフェースをアクセスできるようになります：

```
https://<host.domain>:28082/
```

host.domainには、本製品がインストールされているコンピュータのホスト名またはIPアドレスが指定されます。リモートアクセスについては、`fsav-config`を参照してください。

5.1 サマリ

「サマリ」ページでは、本製品のステータスと最新の情報を確認することができます。

[製品のステータス] では、各機能の保護状況とエラーや不具合が表示されます。

[サマリ] では、ウイルス保護と完全性保護を有効/無効にしたり、ファイアウォールの保護レベルを変更したりすることができます。

[レポート] では、すぐに対処や処理を必要とするものが表示されます。

5.1.1 一般タスク

「一般タスク」ページでは、マニュアルスキャンやファイアウォールを設定したり、ウイルス定義ファイルを確認したりできます。

👉 注: [詳細] をクリックすると、詳細設定モードが開きます。

マニュアルスキャン

ウェブインターフェースからコンピュータ全体にマルウェアのスキャンを実行することができます。

ファイルをスキャンするには読み取りのアクセス権が必要です。感染したファイルを駆除するには、書き込みのアクセス権が必要になります。

スキャンを開始する前にマニュアルスキャンの設定を確認します。

1. ウェブインターフェースから [一般タスク] を選択します。
2. [マルウェアとリスクウェアをスキャンする] をクリックします。

ファイアウォールサービスとルールの作成

ファイアウォールのサービスとルールを新しく作成して、ブロックされているトラフィックを許可できます。また、特定のトラフィックをブロックするようにも設定できます。ファイアウォールルールを編集するときには、セキュリティのリスクを最小限に抑えるために、必要なサービスのみを許可して、他のサービスはブロックすることを推奨します。

ファイアウォールのウィザードを使用するには、「一般タスク」から、[ファイアウォールルールの作成] をクリックして、画面の指示を実行します。

詳細モードで新しいサービスとルールを作成するには、次の手順を実行します。

1. 新しいサービスを作成します。
   a) [詳細モード] から [ネットワークサービス] を選択します。
   b) [サービス名] フィールドに固有のサービス名を指定します。
   c) [説明] フィールドにサービスを識別するための説明を入力します。
   d) [プロトコル] からサービスのプロトコル番号を選択します。
      サービスがICMP、TCP、UDPのプロトコルを使用しない場合、[番号] を選択してプロトコル番号を指定のフィールドに入力してください。
   e) サービスが TCP または UDP プロトコルを使用する場合、サービスに該当する開始ポートを指定する必要があります。
   f) サービスがTCPまたはUDPプロトコルを使用する場合には、サービスの [応答ポート] を指定します。
   g) [新しいサービスの追加] をクリックして、サービスをネットワークサービスのリストに追加します。
   h) [保存] をクリックします。
      新しいサービスはサービスリストに保存されました。

2. サービスが利用する新しいルールを作成します。
   a) 詳細モードから [ファイアウォールルール] を選択して、新しく作成したサービスを使用するファイアウォールルールを作成します。
   b) 新しいルールの対象となるセキュリティレベルを選択して、[新しいルールの追加] をクリックします。新しいルールを作成します。
   c) ルールのタイプに [許可] または [拒否] を指定します。
   d) ターゲットアドレスの情報を [リモートホスト] に入力します。IPアドレスとサブネットはビットネットマスク形式で入力します。
   例：`192.168.88.0/29`
   以下のエイリアスをターゲットアドレスに使用できます。
   - `[myNetwork]` - ローカルネットワーク。
   - `[myDNS]` - 設定されているすべてのDNSサーバ。

   e) [説明] フィールドにルールを識別するための説明を入力します。
   f) 新しく作成したサービスを [サービス] フィールドから選択して、トラフィックの [方向] を指定します。
   - イン = インターネットから受信するすべてのトラフィック。
   - アウト = コンピュータから発信されるすべてのトラフィック。

   g) ルールの対象となるネットワークインターフェースを選択します。[フラグ] フィールドにネットワークインターフェースをそれぞれ入力します。[フラグ] フィールドが空白の場合、ルールがすべてのネットワークインターフェースに適用されます。
   例：`[if:eth0]`、`[if:eth3]`
   h) [このルールにサービスを追加する] をクリックします。
   サービスが新しいルールに追加されます。
   i) 他のサービスをルールに追加しない場合、[ファイアウォールルールの追加] をクリックします。
   各ルールは少なくても1つのサービスを適用している必要があります。ルールが新しいサービスを含んでいる場合、「ネットワークサービス」ページでサービスリストを保存したことを確認してください。
   ルールがファイアウォールルールに追加され、有効になります。
   j) [保存] をクリックして、新しいルールリストを保存します。

ファイルシステムの完全性検査

システムの安全性とベースラインを確認するために、ベースラインを手動で検査することができます。

1. パスワードを入力して、ベースラインを検査します。
2. ベースラインを検査している際には別の完全性検査を実行しないでください。

ベースラインが第三者によって更新された場合、ベースラインを新たに検査するときにパスワードが既存のパスワードと一致されないようになります。

ウイルス定義ファイルの自動更新

F-Secure自動更新エージェントはコンピュータを常に最新の保護状態にする機能です。

F-Secure自動更新エージェントはインターネットに接続しているときに最新のウイルス定義ファイルをコンピュータにダウンロードします。

ウイルス定義ファイルの最新情報は次のURLでご覧になれます。
http://www.F-Secure.com/download-purchase/updates.shtml

注: プロテクションサービスビジネスの管理モードでは、F-Secure自動更新エージェントが最新のLinuxセキュリティのインストーラをプロテクションサービスビジネスポータルのサーバから入手します。

ソフトウェアのインストール

システムファイルやプログラムの変更を行う場合、「ソフトウェアインストールモード」を使用します。

完全性検査はシステムのファイルとプログラムの不正な変更処理を阻止します。OSの更新、パッチの更新やソフトウェアのアップグレードをする際には、完全性検査が監視しているファイルを変更する必要があります。

ソフトウェアインストールモードを有効にしたら、リアルタイムスキャンは通常と同じように動作し、マルウェア検出時に警告を送信します。

ソフトウェアインストールモードを終了するときに本製品は既知のリストを更新して、ベースラインを新しく作成します。

重要: ソフトウェアインストールモードを使用しないでソフトウェアをインストールした場合、完全性検査は変更されたファイルを監視してソフトウェアのインストールまたは起動を阻止することがあります。例えば、カーネルを手動で更新した場合、ベースラインに新しいドライバが含まれていないため、カーネルの更新が阻止される可能性があります。

ベースラインの作成

完全性検査は、保護したいファイルのベースラインを作成することで設定されます。

本製品をインストールするときには標準のシステムファイルが*既知のリスト*に一式追加されますが、デフォルトの設定ではそれらのファイルに対するベースラインは作成されません。ベースラインをインストール時に作成するには、`pass=PASS`パラメータ、またはウェブインターフェース、もしくはコマンドラインクライント(`fsic`) を使用してください。

インストール中にベースラインに追加されたファイルはすべて [許可] と [警告] の保護モードに設定されます。

注: 本製品をインストールした時に既知のファイルは作成されます。初期状態では、システムの重大なファイルが含まれ、格納されるファイルとその数はディストリビューションによって異なります。既知のファイルを表示するには、`/opt/f-secure/fsav/bin/fslistfiles`を実行してください。

5.2 ウイルスのスキャン

本製品はウイルスとマルウェアを阻止します。

5.2.1 ウイルスとマルウェア

「マルウェア」は、コンピュータの破壊、侵入、悪用、情報の窃盗などその他の悪質な活動を展開するプログラムのことを表します。

マルウェアがさらす脅威には、以下の例があります。

- ウェブブラウザの乗っ取り
- ウェブ検索のリダイレクト
- 望ましくない広告の表示
- サイト履歴の監視
- 銀行口座情報など個人情報の窃盗
- コンピュータを利用したスパムの送信
- コンピュータに侵入して他のコンピュータに脅威をさらす

コンピュータの動作を遅くしたり不安定にする

ウイルス

「ウイルス」は自らファイルやディスクに付加し、継続的に自己増殖する寄生型のプログラムです。データを変更して、コンピュータを破壊する危険性をもっています。

ウイルスはほとんどの場合ユーザの知らないうちに感染します。一旦システムに侵入すると、ウイルスは増殖を試みます。ウイルスには次の特徴があります。

- システムのリソースを悪用する
- コンピュータのファイルを変更または破壊したりする
- 侵入したコンピュータを利用して他のコンピュータに感染を移そうとする
- コンピュータを不正な目的で利用する

リスクウェア

「リスクウェア」は厳密に言うとマルウェアではありませんが、使い方によってコンピュータに害を及ぼせる可能性をもっているプログラムです。

リスクウェアの多くは便利なプログラムですが、その機能に危険性があります。以下のプログラムはリスクウェアの例です。

- インスタントメッセージ・チャットプログラム (IRCなど)
- インターネットやネットワークを使用するファイル転送プログラム
- インターネット電話プログラム (VoIP: *Voice Over Internet Protocol*)

リスクウェアとして認識されたプログラムでも、明示的にインストールし正しく設定したプログラムであれば、危険性は低くなります。

リスクウェアの種類

リスクウェアのカテゴリとプラットフォーム

カテゴリ

- Adware
- AVTool
- Client-IRC
- Client-SMTP
- CrackTool
- Dialer
- Downloader
- Effect
- FalseAlarm
- Joke
- Monitor
- NetTool
- Porn-Dialer
- Porn-Downloader
- Porn-Tool
- Proxy
- PSWTool
- RemoteAdmin
- RiskTool
- Server-FTP
- Server-Proxy
- Server-Telnet
- Server-Web
- Tool

プラットフォーム

- Apropos
- BAT
- Casino
- ClearSearch
- DOS
- DrWeb
- Dudu
- ESafe
- HTML
- Java
- JS
- Linux
- Lop
- Macro
- Maxifiles
- NAI
- NaviPromo
- NewDotNet
- Palm
- Perl
- PHP
- Searcher
- Solomon
- Symantec
- TrendMicro
- UNIX
- VBA
- VBS
- Win16
- Win32
- Wintol
- ZenoSearch

ルートキット

「ルートキット」はマルウェアの検出を困難にするプログラムです。

ルートキットはシステムに侵入したあとに第三者によって使用される一連のプログラムです。通常、ルートキットはユーザに気づかれないように侵入し、検出および削除されないように実行中のプロセスやファイルとデータをOSから隠ぺいします。ルートキットはほとんどの場合、悪質な目的に利用されます。

ユーザスペースのルートキットに対する保護

第三者がシステムのアクセスを得て、システムの各種ユーティリティを置き換えてユーザスペースのルートキットをインストールしようとすると、ホスト型侵入防止システム (*HIPS*) が変更処理されたシステムファイルを検知し、管理者に通知します。

5.2.2 ウイルス、その他のマルウェアの停止

本製品はコンピュータをファイルの破壊、個人情報の搾取、不正な目的などから保護します。

デフォルトの設定ではリアルタイムのマルウェアスキャンが有効で、コンピュータはマルウェアから保護されている状態にあります。

本製品は特定のファイル、ディレクトリ、リムーバブルドライブ(USBドライブなど)をスキャンして、コンテンツを自動でダウンロードすることもできます。マルウェアの可能性があるファイルを検出した場合、本製品は無断な変更を阻止します。

リアルタイムスキャンの保護

「リアルタイムスキャン」はファイルを開く際に自動でスキャンが実行される継続的なウイルス保護です。リアルタイムスキャンがマルウェアを検出した場合、ファイルのアクセスは自動的にブロックされます。

リアルタイムスキャンは次のように動作します。

1. コンピュータ上でファイルがアクセスされます。
2. コンピュータがファイルをアクセスできる前に、ファイルに対してマルウェアのスキャンがすぐに行われます。
3. マルウェアを検出した場合、マルウェアがシステムに蔓延できないようにファイルのアクセスがブロックされます。
4. リアルタイムスキャンの設定によって感染ファイルが処理されます(名前の変更、削除、駆除など)。

リアルタイムスキャンとシステムのパフォーマンス

リアルタイムスキャンがファイルのスキャンにかける時間と使用するシステムリソースはファイルのコンテンツ、場所、およびタイプによって異なります。

次のようなファイルはスキャンが通常より長くかかります。

- ZIP形式などの圧縮ファイル (デフォルトでは圧縮ファイルはスキャン対象外)
- ネットワーク上のファイル
- ファイルサイズが大きいファイル

リアルタイムスキャンが多くのファイルを同時に処理している場合、システムの動作は低下することがあります。

マニュアルスキャン

ウェブインターフェースからコンピュータ全体にマルウェアのスキャンを実行することができます。

ファイルをスキャンするには読み取りのアクセス権が必要です。感染したファイルを駆除するには、書き込みのアクセス権が必要になります。

スキャンを開始する前にマニュアルスキャンの設定を確認します。

1. ウェブインターフェースから [一般タスク] を選択します。
2. [マルウェアとリスクウェアをスキャンする] をクリックします。

5.2.3 システムをマルウェアから保護する方法

本製品を使用してシステムをマルウェアから保護する方法はいくつかあります。どの方法を選択するかはシステムの性能と保護の水準によります。

すべてのウイルス保護機能を有効にすると、システムの動作が著しく低下することがあります。

リアルタイムスキャン

「リアルタイムスキャン」はマルウェアをリアルタイムでスキャンすることによってコンピュータを常に保護します。

感染時のアクション

ウイルスを検出したときに実行する1次および2次アクションを選択します。

ウェブインターフェースの「一般タスク」ページで [詳細] をクリックして、詳細モードを開きます。

1. ウイルスを検出したときに実行する1次アクションを選択します。以下のいずれかを選択できます。
   - レポート/アクセスをブロック - 検出したウイルスのスキャン結果を表示して、感染ファイルのアクセスをブロックします。感染したファイルに対して他のアクションはありません。ウイルスレポートを確認するには、[警告] を表示します。
   - 駆除 - 検出したウイルスを駆除します。なかには駆除できないウイルスもあります。ウイルスが駆除できない場合、感染ファイルのアクセスはブロックされます。
   - 名前の変更 - 感染したファイルの名前を変更して、ファイルの実行権限も取り除きます。名前が変更された感染ファイルはコンピュータに残りますが、直接実行することはできません。また、名前が変更されたファイルには.virusの拡張子が設定されます。
   - 削除 - 感染したファイルを削除します。
   - アクセスをブロック - 感染したファイルのアクセスをブロックします。警告とレポートは送信されません。

   デフォルトの設定では、1次アクションは [駆除] になります。
2. ウイルスを検出したときに実行する2次アクションを選択します。2次アクションは1次アクションが実行できない場合にのみ実行されます。
   デフォルトの設定では、2次アクションは [名前の変更] になります。

ウイルス感染時の設定を完了したら、「警告」ページで警告と通知法を設定してください。

不審なファイル

不審なファイルを検出したときに実行する1次および2次アクションを選択します。

ウェブインターフェースの「一般タスク」ページで [詳細] をクリックして、詳細モードを開きます。

1. 不審なファイルを検出したときに実行する1次アクションを選択します。以下のいずれかを指定できます。
   - レポート/アクセスをブロック - 不審なファイルのスキャン結果を表示して、ファイルのアクセスをブロックします。ファイルに対して他のアクションはありません。セキュリティレポートを確認するには、[警告] を表示します。
   - 名前の変更 - 不審なファイルのファイル名を変更して、ファイルの実行権限も取り除きます。名前が変更されたファイルはコンピュータに残りますが、直接実行することはできません。名前が変更されたファイルには.suspectedの拡張子が設定されます。
   - 削除 - 不審なファイルを削除します。
   - アクセスをブロック - 不審なファイルのアクセスをブロックします。警告とレポートは送信されません。

   デフォルトの設定では、1次アクションは [レポートのみ] になります。
2. 2次アクションを指定します。2次アクションは1次アクションが実行できない場合にのみ実行されます。
   デフォルトの設定では、2次アクションは [アクセスをブロック] になります。

不審なファイルの設定を完了したら、「警告」ページで警告と通知法を設定してください。

スキャンの対象

マルウェアスキャンの対象となるファイル/ディレクトリを指定します。

ウェブインターフェースの「一般タスク」ページで [詳細] をクリックして、詳細モードを開きます。

1. [スキャン対象外のディレクトリ] でウイルススキャンから除外するファイルとディレクトリを指定できます。各ディレクトリは行別に入力します。

   安全と判断できるディレクトリをウイルススキャンから除外すると、スキャン時間を短くすることができます。また、誤った警告を受けている場合には、それらを回避することも可能になります。

   
   ヒント: 特定のファイルを [スキャン対象外のディレクトリ] に追加すると、ファイルをスキャンから除外します。

2. 実行可能ファイルのみをスキャンしたい場合、[実行可能ファイルのみスキャン] を有効にします。指定のファイルやディレクトリをスキャンの対象にしたい場合、このオプションを無効にします。

   注: [ファイルを開くときにスキャン] および [実行可能ファイルの起動時にスキャン] が無効に設定されている場合、何もスキャンされないことになります。[実行可能ファイルのみスキャン] が有効に設定されていても、スキャンは実行されません。

3. 安全な実行可能ファイルを指定します。ウイルススキャンは安全とみなされた実行可能ファイルに対するファイルアクセスをブロックしません。

   注: 実行可能ファイルを安全とみなす場合、ファイルを本当に信頼できるか確認してください。アプリケーションを安全とみなすことは危険性がありますので、指定するときには注意してください。

4. 安全な実行可能ファイルの設定を*完全性検査*と併用するには、[安全な実行可能ファイルはベースラインと一致している必要がある] を有効にします。このオプションを適用すると、安全な実行可能ファイルが*既知のファイル*に追加され、変更されていないことが必要になります。また、オプションを有効にした際に実行可能ファイルが完全性検査のベースラインに見つからない場合、実行可能ファイルは安全とみなされません。

   注: アプリケーションを安全と指定した場合、このオプションを有効にすることを推奨します。

5. [ファイルを開くときにスキャン] を有効にすると、ファイルを開く際にスキャンが実行されます。
6. [ファイルを閉じるときにスキャン] を有効にすると、ファイルを閉じる際にスキャンが実行されます。
7. [実行可能ファイルの起動時にスキャン] を有効にすると、ファイルを実行する際にスキャンが実行されます。

注: 本製品はマウントされたファイルシステムにあるファイルしかスキャンできません。CD-ROMやDATデバイス (/dev/st0, /dev/hda and such) などの特別なファイルはファイルシステムとしてマウント、またはあらかじめ解凍/展開されている場合に限り、スキャンできます。

圧縮ファイルのスキャン

圧縮ファイルのスキャンを有効にすると、ZIP、ARJ、LZH、RAR、CAB、TAR、BZ2、GZ、JAR、TGZ形式のファイル内をスキャンすることが可能になります。

ウェブインターフェースの「一般タスク」ページで [詳細] をクリックして、詳細モードを開きます。

1. [圧縮ファイル内をスキャン] を有効にすると、圧縮ファイル内のスキャンを有効にします。

   注: [圧縮ファイル内をスキャン] を有効に設定すると、感染したメールを開くときにメールの処理が停止する電子メールプログラムがあります。

2. スキャン対象となる圧縮ファイルの最大ネスト数を指定します。圧縮ファイル内に圧縮ファイルがあることを「ネスト」と呼びます。
3. パスワード保護された圧縮ファイルに対する動作を指定します。なお、パスワード保護された圧縮ファイルに対するウイルス検査は行えません。

   - [パスワード保護された圧縮ファイルを安全だとみなす] を有効にすると、パスワードで保護された圧縮ファイルをアクセスできるようになります。この設定は危険性がありますので、有効にした場合、圧縮ファイルを開くユーザのコンピュータに最新のウイルス定義ファイルが適用されていることを確認してください。
   - [パスワード保護された圧縮ファイルを安全だとみなす] を無効にすると、パスワードで保護された圧縮ファイルへのアクセスを拒否します。

4. 圧縮ファイル内に感染を検出したときにスキャンを停止したい場合、[圧縮ファイル内で最初の感染を見つけたら停止する] を有効にします。このオプションが無効の場合、圧縮ファイル内全体がスキャンされます。

リスクウェアスキャン

リスクウェアを検出したときに実行する1次および2次アクションを指定します。

ウェブインターフェースの「一般タスク」ページで [詳細] をクリックして、詳細モードを開きます。

1. リスクウェアを検出したときに実行する1次アクションを指定します。以下のいずれかを選択できます。
   - レポート/アクセスをブロック - 検出したリスクウェアのスキャン結果を表示して、リスクウェアのアクセスをブロックします。感染ファイルに対して他のアクションはありません。セキュリティ警告を確認するには、[警告] を表示します。(マニュアルスキャン中には利用できません)
   - 名前の変更 - リスクウェアのファイル名を変更して、ファイルの実行権限を取り除きます。名前が変更されたリスクウェアはコンピュータに残りますが、直接実行することはできません。名前が変更されたファイルには.riskwareの拡張子が設定されます。
   - 削除- リスクウェアを削除します。
   - アクセスをブロック - リスクウェアのアクセスをブロックしますが、警告とレポートは送信されません。(マニュアルスキャン中には利用できません)
   - レポートのみ

   デフォルトの設定では、1次アクションは [レポートのみ] になります。
2. 2次アクションを指定します。2次アクションは1次アクションが実行できない場合にのみ実行されます。
   デフォルトの設定では、2次アクションは [アクセスをブロック] になります。
3. [除外されたリスクウェア] フィールドでは、スキャンから除外するリスクウェアを指定できます。
   次の形式を使用して除外するリスクウェアを指定します。各エントリはセミコロン (;) で区切ります。Category.Platform.Family という名前で指定し、 category、platform、familyにはワイルドカード (*) を使用できます。
   たとえば、「Client-IRC.*.*」はClient-IRCのカテゴリにあるすべてのリスクウェアをスキャン対象外にします。

リスクウェアスキャンの設定を完了したら、「警告」ページで警告と通知法を設定してください。

システムのマニュアルスキャン

マニュアルスキャンを利用することで、特定のファイルやすべてのファイルをスキャンして、システムの安全性を確認できます。

マニュアルスキャン中にウイルス感染が検出された場合

ウイルスを検出したときに実行する1次および2次アクションを選択します。

ウェブインターフェースの「一般タスク」ページで [詳細] をクリックして、詳細モードを開きます。

1. ウイルスを検出したときに実行する1次アクションを選択します。以下のいずれかを選択できます。
   - 駆除 - ウイルスを駆除します。なかには駆除できないウイルスもあります。ウイルスが駆除できない場合、感染ファイルへのアクセスはブロックされます。
   - [名前の変更] を選択すると、感染したファイルの名前を変更して、ファイルの実行権限を取り除きます。名前が変更されたファイルはコンピュータに残りますが、害を及ぼすことはできません。また、名前が変更されたファイルの拡張子は.virusになります。
   - 削除 - 感染したファイルを削除します。

   デフォルトの設定では、1次アクションは [駆除] になります。
2. 2次アクションを指定します。2次アクションは1次アクションが実行できない場合にのみ実行されます。

デフォルトの設定では、2次アクションは [名前の変更] になります。

ウイルスが感染されたときの設定を完了したら、「警告」ページで警告とレポートの設定を行ってください。

マニュアルスキャン中に不審なファイルが検出された場合

マニュアルスキャン中に不審なファイルが検出された場合、実行する1次および2次アクションを選択します。

ウェブインターフェースの「一般タスク」ページで [詳細] をクリックして、詳細モードを開きます。

1. 不審なファイルが検出されたときに実行する1次および2次アクションを選択します。
   - [名前の変更] を選択すると、不審なファイルの名前を変更して、ファイルの実行権限を取り除きます。名前が変更されたファイルはコンピュータに残りますが、害を及ぼすことはできません。また、名前が変更されたファイルの拡張子は.suspectedになります。
   - [削除]をクリックすると、不審なファイルを削除します。

   デフォルトの設定では、1次アクションは [レポートのみ] になります。
2. 2次アクションを指定します。2次アクションは1次アクションが実行できない場合にのみ実行されます。

不審なファイルの設定を完了したら、「警告」ページで警告とレポートの設定を行ってください。

マニュアルスキャンのスキャン対象

マニュアルスキャンを実行する際に、特定のファイルやディレクトリを指定することができます。

ウェブインターフェースの「一般タスク」ページで [詳細] をクリックして、詳細モードを開きます。

1. [ファイルのスキャン] の設定で、すべてのファイルまたは特定の拡張子のファイルをマニュアルスキャンの対象にするか指定します。
   [指定した拡張のファイルのみ] をスキャンの対象にした場合、[対象とする拡張子] フィールドが開きます。フィールドに拡張子を指定します。複数の拡張子を指定する場合、半角のカンマ (,) で区切ります。
2. スキャンから特定のファイルやディレクトリを除外するには、[スキャン対象外のファイルとディレクトリ] を指定します。

   特定のディレクトリにファイルが感染する可能性がないことを知り、スキャンに時間がかかることまたは誤った警告を受ける場合、そのディレクトリをウイルススキャンから除外できます。

   
   ヒント: ディレクトリだけではなく、特定のファイルもスキャンから除外することができます。

3. 実行可能ファイルのみスキャンしたい場合、[実行可能ファイルのみスキャン] のオプションをオンにします。指定のファイルをすべてスキャンする場合、オプションをオフにします。

   
   注: [ファイルを開くときにスキャン] と [実行可能ファイルの起動時にスキャン] が無効の場合、[実行可能ファイルのみスキャン] が設定されていても、スキャンは開始しません。

4. スキャン対象のファイルのアクセス日時が更新されないように設定するには、[アクセス時間の保存] のオプションをオンにします。


注: 本製品はマウントされたファイルシステムにあるファイルしかスキャンできません。CD-ROMやDATデバイス (/dev/st0, /dev/hda and such) などの特別なファイルはファイルシステムとしてマウント、またはあらかじめ解凍/展開されている場合に限り、スキャンできます。

圧縮ファイルのスキャン

圧縮ファイルのスキャンを有効にすると、ZIP、ARJ、LZH、RAR、CAB、TAR、BZ2、GZ、JAR、TGZ形式のファイル内をスキャンすることが可能になります。

ウェブインターフェースの「一般タスク」ページで [詳細] をクリックして、詳細モードを開きます。

1. [圧縮ファイル内をスキャン] を有効にすると、圧縮ファイル内のスキャンを有効にします。

   👉 注: [圧縮ファイル内をスキャン] を有効に設定すると、感染したメールを開くときにメールの処理が停止する電子メールプログラムがあります。

2. スキャン対象となる圧縮ファイルの最大ネスト数を指定します。圧縮ファイル内に圧縮ファイルがあることを「ネスト」と呼びます。
3. パスワード保護された圧縮ファイルに対する動作を指定します。なお、パスワード保護された圧縮ファイルに対するウイルス検査は行えません。
   - [パスワード保護された圧縮ファイルを安全だとみなす] を有効にすると、パスワードで保護された圧縮ファイルをアクセスできるようになります。この設定は危険性がありますので、有効にした場合、圧縮ファイルを開くユーザのコンピュータに最新のウイルス定義ファイルが適用されていることを確認してください。
   - [パスワード保護された圧縮ファイルを安全だとみなす] を無効にすると、パスワードで保護された圧縮ファイルへのアクセスを拒否します。
4. 圧縮ファイル内に感染を検出したときにスキャンを停止したい場合、[圧縮ファイル内で最初の感染を見つけたら停止する] を有効にします。このオプションが無効の場合、圧縮ファイル内全体がスキャンされます。

マニュアルスキャン中にリスクウェアが検出された場合

マニュアルスキャン中にリスクウェアが検出された場合、実行する1次および2次アクションを選択します。

ウェブインターフェースの「一般タスク」ページで [詳細] をクリックして、詳細モードを開きます。

1. リスクウェアを検出したときに実行する1次アクションを指定します。以下のいずれかを選択できます。
   - [名前の変更] を選択すると、リスクウェアの名前を変更して、ファイルの実行権限を取り除きます。名前が変更されたファイルはコンピュータに残りますが、害を及ぼすことはできません。また、名前が変更されたファイルの拡張子は.riskwareになります。
   - リスクウェアを削除するには、[削除] を選択します。
   - [レポートのみ] を選択します。

   デフォルトの設定では、1次アクションは [レポートのみ] になります。
2. 2次アクションを指定します。2次アクションは1次アクションが実行できない場合にのみ実行されます。
3. [除外されたリスクウェア] フィールドでは、スキャンから除外するリスクウェアをできます。

   次の形式を使用して、除外するリスクウェアを指定してください。各エントリはセミコロン (;) で区切ってください。Category.Platform.Family、カテゴリ、プラットフォーム、ファミリには * を指定できます。

   たとえば、「Client-IRC.*.*」はClient-IRCカテゴリにある全リスクウェアをスキャン対象外にします。

リスクウェアスキャンの設定を完了したら、「警告」ページで警告と通知法を設定してください。

スケジュールスキャン

スケジュール スキャンを使うと、マルウェアの定期的スキャン (毎日、毎週、または毎月の決まった日など) を設定することができます。

スケジュールスキャンの作成

スケジュールスキャンを作成して、定期的にマルウェアのスキャンを実行します。

ウェブインターフェースの「一般タスク」ページで [詳細] をクリックして、詳細モードを開きます。

スケジュールスキャンはマニュアルスキャンの設定を使用します。スキャン時間を設定するには、以下の手順を実行します。

1. [新しいタスクの追加] をクリックします。
2. スケジュールスキャンを開始する日時を設定します。
   各設定はcrontabのエントリと同じように指定されます。例：
   - スキャンを毎週日曜日の4時に実行する。

     ```
     Minute: 0, Hour: 4, Day of the Month: *, Month: *, Day of the Week: sun
     ```
   - スキャンを毎日5時30分に実行する。

     ```
     Minute: 30, Hour: 5, Day of the Month: *, Month: *, Day of the Week: *
     ```

   注: 曜日には次の値を入力できます。
   - 「Mon」、「1」 = 月曜日
   - 「Tue」、「2」 = 火曜日
   - 「Wed」、「3」 = 水曜日
   - 「Thu」、「4」 = 木曜日
   - 「Fri」、「5」 = 金曜日
   - 「Sat」、「6」 = 土曜日
   - 「Sun」、「7」、「0」 = 日曜日

   「*」を指定すると、毎日実行するスケジュールスキャンを指定できます。
3. スキャンするディレクトリを [スキャン対象のディレクトリ] に指定します。各ディレクトリを行別に入力します。
4. [タスクの保存] をクリックして、スケジュールスキャンを保存します。

スケジュールスキャンは数時間かかることがあります。この理由で、コンピュータの使用率が低いときにスケジュールスキャンを指定することを推奨します。また、複数のスケジュールスキャンを作成して、それぞれが異なるディレクトリをスキャンするようにも指定できます。

スケジュールスキャンの設定を完了したら、「警告」ページで警告と通知方法を設定します。

5.3 ファイアウォール保護

「ファイアウォール」は、システムをインターネットとネットワークからの不正トラフィックを阻止する機能です。

本製品のファイアウォールには次の特長があります。

- システムを権限のないユーザや侵入者から守ります。
- 不正なアクセスを阻止および検出して、情報の窃盗から保護します。

本製品のインストール後、ファイアウォールは自動的に有効になり、システムは保護されます。

5.3.1 ファイアウォール

*ファイアウォール*は、インターネットから送信されるデータを区別してコンピュータを保護する機能です。

本製品の*ファイアウォール*はコンピュータからインターネットへの発信トラフィックを許可しますが、インターネットからコンピュータへの着信トラフィックはあらかじめ特定していない限りブロックする傾向があります。着信トラフィックをブロックすることによって、ファイアウォールはコンピュータを*ワーム*などの*悪質*なソフトウェアから保護し、第三者がコンピュータに侵入することも阻止できます。

初期状態では、*ファイアウォール*はシステムを十分保護します。通常、設定を変更する必要はありませんが、厳重な*セキュリティレベル*を使用する場合やカスタムの*ファイアウォールルール*またはサービスを追加した場合には設定を変更する必要があるかもしれません。

⚠ 注意: *ファイアウォール*を無効にすると、ネットワークに危険性が生じます。

5.3.2 セキュリティレベル

*ファイアウォール*の*セキュリティレベル*はシステムの保護状態を表します。

各*セキュリティレベル*にはトラフィックを制御するプリセットの*ファイアウォールルール*が含まれています。セキュリティレベルによっては、新しいルールを追加することもできます。

セキュリティレベルと該当するトラフィック

セキュリティレベル	説明
すべてブロック	すべてのネットワークトラフィックをブロックします (ループバックを除く)。
サーバ	DHCP、DNS lookup、ssh プロトコルによるIP設定のアクセスのみ許可します。 👉 重要: このセキュリティレベルは、使用する前にカスタマイズが必要になることがあります。
モバイル	通常のウェブアクセス、ファイルのアクセス (HTTP、HTTPS、FTP)、および電子メールとニュースグループのトラフィックを許可します。VPNとSSHなどの暗号化されたプログラムも許可します。それ以外は拒否されます。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	TCPとFTPのトラフィックをすべて許可します。それ以外は拒否されます。ネットワーク機能を拡張するために、ローカルルールを追加できます。
オフィス	TCPとFTPのトラフィックをすべて許可します。デフォルトの設定では、それ以外はブロックされます。このセキュリティレベルはインターネットとホストの間にファイアウォールがあることを想定しています。
強化	ウェブアクセス、電子メールとニュースグループ、暗号化された通信、FTPファイル転送、およびリモート更新を許可します。それ以外は拒否されます。
通常	外部への送信をすべて許可し、特定の受信サービスを拒否します。
すべて許可	外部からの受信、外部への送信をすべて許可します。

セキュリティレベル、ファイアウォールルール、ファイアウォールサービスについて

セキュリティレベルはいくつかのファイアウォールルールで構成されています。ファイアウォールルールはいくつかのファイアウォールサービスで構成されています。サービスはプロトコルとポートで構成されています。

たとえば、[通常] セキュリティレベルには「**Web browsing**」というファイアウォールルールが含まれています。このルールはウェブの閲覧を可能にする「**HTTP**」のサービスを利用しています。そしてこのサービスはTCPのポート80を使用します。

セキュリティレベルの変更

ファイアウォールのセキュリティレベルを使用すると、ファイアウォールルールの設定をすぐに変更することができます。

1. ウェブインターフェースで「一般タスク」ページを開きます。
2. [ファイアウォール保護] で使用するセキュリティレベルを選択します。

セキュリティレベルの編集

ユーザ別に異なるセキュリティレベルを指定およびカスタマイズすることができます。

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。

1. 「サマリ」ページで現在のセキュリティレベルを編集したいファイアウォールセキュリティレベルに変更します。

   現在のセキュリティレベルは「ファイアウォールルール」ページの上に表示されます。
2. ルールリストでは、使用中のルールが表示されます。
   - [有効] のオプションからチェックを外して、ルールを一時的に無効にします。
   - 上下の矢印ボタンを使用してルールの順序を変更できます。

     注: ルールの順序を変更すると作成済みの他のルールが影響を受ける可能性があります。
   - **[X]** をクリックすると、ルールを完全に削除します。
   - ルールを編集するには、リストからルールをクリックします。選択したルールはリスト下の [ルールの編集] ペインに表示されます。
3. セキュリティレベルのルール数が10を超える場合、**[<<]**、**[<]**、**[>]** と **[>>]** を使用してルールを切り替えできます。

5.3.3 ファイアウォールルール

「ファイアウォールルール」は、ファイアウォールを細かく設定するためのファイアウォールサービスで、インターネットのトラフィックを制御します。

各セキュリティレベルは変更することができないプリセットのファイアウォールルールを含めています。指定しているセキュリティレベルによってファイアウォールルールの優先度は異なります。

ファイアウォールルールはインターネットからコンピュータへのトラフィック (着信トラフィック)、コンピュータからインターネットへのトラフィック (発信トラフィック)、または双方向のトラフィック (着発信トラフィック) に適用することが可能です。

ファイアウォールルールはトラフィックの方向と使用ポートを指定するファイアウォールサービスを含みます。たとえば、「**Web browsing**」と言うルールがTCPプロトコルとポート80を使用する「**HTTP**」サービスを利用します。

ファイアウォールルールはファイアウォールに関連する警告の表示設定 (ファイアウォールルールと一致するトラフィックに対して) も指定します。

ファイアウォールルールの追加

ブロックされているトラフィックを許可、または特定のインターネットトラフィックを拒否する必要があるときなどに新しいファイアウォールルールを作成します。

プログラム/デバイスが必要とするサービスを同じルールに適用すると、次のことが簡単に行えるようになります。

- ルールを有効または無効にする
- プログラムをアンインストールまたはデバイスを取り除いた際にルールを削除する

特定のトラフィックを拒否した状態で特定のIPアドレスを許可したい場合にも、新しいルールを追加する必要があります。この場合、既存の「拒否」*ファイアウォールルール*を利用できます。特定のIPアドレスにトラフィックを許可するには、より明確な「許可」ルールを作成する必要があります。

ファイアウォールサービス

*ファイアウォールサービス*は*ファイアウォールルール*に適用されるトラフィックを指定します。

ネットワークサービス (ウェブアクセス、*ファイル共有*、*リモートコンソールアクセス*など) もファイアウォールサービスの一種です。

各サービスには特定の*プロトコル*と*ポート*が指定されています。たとえば、「HTTP」サービスはTCP *プロトコル*と*ポート*80を使用します。

ファイアウォールのサービスは二種類のポートを使用します。

- *開始ポート*: 接続の開始に使用されるコンピュータの*ポート*。
- *応答ポート*: 接続の終了に使用されるコンピュータの*ポート*。

コンピュータの*ポート*が*開始ポート*または*応答ポート*のどちらかになるかはトラフィックの方向により ます。

- *ファイアウォールサービス*の方向が「アウト」 (発信) の場合、コンピュータの*ポート*が*開始ポート*になり、リモートコンピュータの*ポート*が*応答ポート*になります。
- *ファイアウォールサービス*の方向が「イン」 (着信) の場合、リモートコンピュータの*ポート*が*開始ポート*になり、コンピュータの*ポート*が*応答ポート*になります。

*応答ポート*は該当するソフトウェアのマニュアルに記載されていることがよくあります。*開始ポート*には通常1023より高い*ポート*が使用されますが、ゲームなど一部のアプリケーションには特定の*開始ポート*を指定する必要があります。

新しい*ファイアウォールルール*を作成する場合、プリセットのサービスを必要に応じてルールに追加できます。また、サービスを新たに作成してルールに追加することも可能です。

ファイアウォールサービスとルールの作成

ファイアウォールのサービスとルールを新しく作成して、ブロックされているトラフィックを許可できます。また、特定のトラフィックをブロックするようにも設定できます。ファイアウォールルールを編集するときには、セキュリティのリスクを最小限に抑えるために、必要なサービスのみを許可して、他のサービスはブロックすることを推奨します。

ファイアウォールのウィザードを使用するには、「一般タスク」から、[ファイアウォールルールの作成] をクリックして、画面の指示を実行します。

詳細モードで新しいサービスとルールを作成するには、次の手順を実行します。

1. 新しいサービスを作成します。
   a) [詳細モード] から [ネットワークサービス] を選択します。
   b) [サービス名] フィールドに固有のサービス名を指定します。

c) [説明] フィールドにサービスを識別するための説明を入力します。
d) [プロトコル] からサービスのプロトコル番号を選択します。
サービスがICMP、TCP、UDPのプロトコルを使用しない場合、[番号] を選択してプロトコル番号を指定のフィールドに入力してください。
e) サービスが TCP または UDP プロトコルを使用する場合、サービスに該当する開始ポートを指定する必要があります。
f) サービスがTCPまたはUDPプロトコルを使用する場合には、サービスの [応答ポート] を指定します。
g) [新しいサービスの追加] をクリックして、サービスをネットワークサービスのリストに追加します。
h) [保存] をクリックします。
新しいサービスはサービスリストに保存されました。

2. サービスが利用する新しいルールを作成します。
a) 詳細モードから [ファイアウォールルール] を選択して、新しく作成したサービスを使用するファイアウォールルールを作成します。
b) 新しいルールの対象となるセキュリティレベルを選択して、[新しいルールの追加] をクリックします。新しいルールを作成します。
c) ルールのタイプに [許可] または [拒否] を指定します。
d) ターゲットアドレスの情報を [リモートホスト] に入力します。IPアドレスとサブネットはビットネットマスク形式で入力します。
例：`192.168.88.0/29`
以下のエイリアスをターゲットアドレスに使用できます。
- `[myNetwork]` - ローカルネットワーク。
- `[myDNS]` - 設定されているすべてのDNSサーバ。

e) [説明] フィールドにルールを識別するための説明を入力します。
f) 新しく作成したサービスを [サービス] フィールドから選択して、トラフィックの [方向] を指定します。
- イン = インターネットから受信するすべてのトラフィック。
- アウト = コンピュータから発信されるすべてのトラフィック。

g) ルールの対象となるネットワークインターフェースを選択します。[フラグ] フィールドにネットワークインターフェースをそれぞれ入力します。[フラグ] フィールドが空白の場合、ルールがすべてのネットワークインターフェースに適用されます。
例：`[if:eth0]`、`[if:eth3]`
h) [このルールにサービスを追加する] をクリックします。
サービスが新しいルールに追加されます。
i) 他のサービスをルールに追加しない場合、[ファイアウォールルールの追加] をクリックします。
各ルールは少なくても1つのサービスを適用している必要があります。ルールが新しいサービスを含んでいる場合、「ネットワークサービス」ページでサービスリストを保存したことを確認してください。
ルールがファイアウォールルールに追加され、有効になります。
j) [保存] をクリックして、新しいルールリストを保存します。

ファイアウォールルールの優先度

各ファイアウォールルールには優先度があります。ルールは上から下へと読み込まれ、接続に関連する最初のルールが実行されます。

ファイアウォールルールは「ルール」ページで一覧表示されます。ルールは上から下の順に読み込まれ、トラフィックと一致するルールが見つかり次第、そのルールが実行されます。原則として、必要な

トラフィックのみを許可して、それ以外はブロックします。セキュリティレベルのルールリストの一番下にあるルール (優先度がもっとも低い) を [**Deny rest**] にすると、不要なトラフィックを安全にブロックすることが可能です。

> ルールの優先度の例
>
> 次の例では、ファイアウォールルールの優先度を変更することで、特定のネットワークトラフィックに適用されるルールを制御します。
>
> - *FTP*の発信トラフィックをすべてブロックするルールがあるとします。ルールリストで、このルールの上にプロバイダーのIPアドレスへ*FTP*接続を許可するルールがあります。このルールのほうが前者より優先度が高いため、プロバイダーのIPアドレスへの*FTP*接続は許可されます。
> - プロバイダーIPアドレスへ*FTP*接続を許可するルールがあるとします。ルールリストで、このルールの上に*FTP*接続をすべて拒否するルールがあります。このルールのほうが前者より優先度が高いため、プロバイダーのIPアドレスへの*FTP*接続はブロックされます。

5.3.4 ファイアウォールを設定する

「基本設定」ページでは、ネットワークパケットのログと信頼できるネットワークインターフェースを設定することができます。

未処理のネットワークパケットをログする

未処理のネットワークパケットをログに保存にして、ネットワークの分析や問題解決の参考として利用できます。

未処理のネットワークパケットは通常ログする必要はありません。

1. ウェブインターフェースを開きます。
2. 詳細モードに移動します。
3. [ファイアウォール > 基本設定] に移動します。
4. [未処理のネットワークパケットをログする] オプションを有効にすると、ファイアウォールルールに一致しないネットワークパケットをログすることができます。

ファイアウォールルールと一致しないネットワークパケットはsyslogを使用してログされます (ご利用のLinuxディストリビューションによって異なる可能性があります)。

信頼済みのネットワークインターフェースの編集

ファイアウォールルールはホスト上の全ネットワークインターフェースに適用します。信頼済みのネットワークインターフェースにはトラフィックをすべて許可するルールが自動的に付加されます。

1. ウェブインターフェースを開きます。
2. 詳細モードに移動します。
3. [ファイアウォール > 基本設定] に移動します。
4. 信頼済みのネットワークインターフェースに新しいネットワークインターフェースをカンマ区切りで追加します。

信頼済みネットワークへのネットワークトラフィックはすべて許可されます。

5.4 完全性検査

「完全性検査」は、重要なファイルを不正な変更処理から保護します。

保護しているファイルのパーミッション (アクセス権) がどのように指定されていても、保護しているファイルに対する変更をブロックするように設定できます。

「一般タスク」ページから完全性ウィザードを実行すると、ファイルシステムのベースラインを作成および検査できます。ベースラインはコンピュータを無断な変更から保護します。完全性検査のオプションは、詳細モードで設定できます。

完全性検査はディスク上のファイルを「ベースライン」と比較します。ベースラインは暗号化および電子署名されたファイルのデータを表します。監視および保護対象のファイルに対して変更処理があった場合、管理者へ通知を送信するように設定できます。

5.4.1 既知のファイル

「*既知のファイル*」は、監視および保護しているファイルのことを表します。

ベースラインは、*既知のファイル*に含まれている各ファイルのデータを暗号化かつ署名することで作成されます。完全性検査はベースラインをリアルタイムで行われるファイルアクセスと比較します。

👉 注: *既知のファイル*はウェブインターフェースで現在保存されているベースラインの状態を表示します。ファイルシステムの実際の状態を表示するには、ベースラインを検査する必要があります。ベースラインの検査はウェブインターフェースまたはfsicのコマンドを使用して行えます。

既知のファイルを検索する

検索機能を使用して、*既知のファイル*のリスト内からファイルを確認することができます。

1. 既知のファイルリストから表示するファイルを選択します。
   - 変更および新規 - 変更およびベースラインに追加されたファイルを表示します。
   - 変更 - 変更されたファイルを表示します。
   - 新規 - ベースラインに追加されたファイルを表示します。
   - 未変更 - 変更されていないファイルを表示します。
   - すべて - 既知のファイルをすべて表示します。
2. 検索をファイル名で絞るには、ファイル名に含まれている文字を [ファイル名] に入力します。
3. [検索] をクリックします。
   検索に一致した*既知のファイル*がリストに表示されます。
4. 検索結果を確認します。

オプション	説明
ファイル名	ファイル名を表示します。
検出時間	変更が検出された時間を表示します。
検出されたプロセス	変更を実施したプロセスのファイル名を表示します。
処理	ファイルの変更を許可またはブロックしているか表示します。
警告	ファイルの変更を検出した場合に、警告を送信するか表示します。

オプション	説明
保護	ファイルが監視または保護されているか表示します。保護されているファイルは変更することができません。監視されているファイルは変更することができます。

5. 実行する処理を選択します。
   - To regenerate the baseline, select new and modified files you want to baseline and click **Regenerate baseline for highlighted files**.
   - ベースラインからファイルを削除するにはファイルを選択してから、[選択したファイルをベースラインから削除する] をクリックします。削除したファイルは監視されなくなります。

注: 完全性検査はベースラインを更新するまでファイル (新規および変更) を保護しません。*既知のファイル*が追加または変更された場合、ファイルを保護するためにベースラインを更新してください。

既知のファイルを追加する

既知のファイルに保護したいファイルを追加することで、ファイルを無断な変更から保護することができます。

1. 監視するファイルのファイル名を入力します。複数のファイルを追加する場合、各ファイル名をスペースで区切ります。
2. 保護方法を選択します。
   - 監視 - ファイルを監視します。ファイルは変更可能です。
   - 保護 - ファイルに対する変更をすべて拒否します。ファイルを開くことはできますが、変更することはできません。
3. 変更されたファイルのアクセスを指定します。
   - 許可 - 変更されたファイルが実行または開いたときのアクセスを許可します。
   - 拒否 - 変更されたファイルのアクセスを拒否します。変更されたファイルは開くことも、実行することもできません。
4. ファイルの属性の変更を無視するには、[対象外の属性] から該当する属性のチェックボックスをオンにします。
   - モード : 権限の変更を対象外にします
   - ユーザ : 所有者の変更を対象外にします
   - グループ : グループの変更を対象外にします
   - サイズ : ファイルサイズの変更を対象外にします
   - 更新時間 : 更新日時の変更を対象外にします
   - ハッシュ : ファイル内容の変更を対象外にします

   注: 通常、ファイルの内容が変更された際にファイルの更新日時とサイズも変わることで、ハッシュ属性のみ対象外にするのは推奨しません。
5. [既知のファイルへ追加] をクリックして、ファイルを*既知のファイル*に追加します。

完全性検査はベースラインが更新されるまでは追加/変更されたファイルを保護しません。追加/変更されたファイルを保護するにはベースラインを更新してください。

注: ベースラインに複数のファイルを同時に追加することも可能です。

5.4.2 ソフトウェアのインストール

システムファイルやプログラムの変更を行う場合、「ソフトウェアインストールモード」を使用します。

完全性検査はシステムのファイルとプログラムの不正な変更処理を阻止します。OSの更新、パッチの更新やソフトウェアのアップグレードをする際には、完全性検査が監視しているファイルを変更する必要があります。

ソフトウェアインストールモードを有効にしたら、リアルタイムスキャンは通常と同じように動作し、マルウェア検出時に警告を送信します。

ソフトウェアインストールモードを終了するときに本製品は既知のリストを更新して、ベースラインを新しく作成します。

重要: ソフトウェアインストールモードを使用しないでソフトウェアをインストールした場合、完全性検査は変更されたファイルを監視してソフトウェアのインストールまたは起動を阻止することがあります。例えば、カーネルを手動で更新した場合、ベースラインに新しいドライバが含まれていないため、カーネルの更新が阻止される可能性があります。

ソフトウェアインストールモードを有効にする

保護しているファイルを更新または変更する場合、ソフトウェアインストールモードを有効にしてください。

ソフトウェアインストールモードを起動するには、以下の手順を実行します。

1. ウェブインターフェースを開きます。
2. 「一般タスク」ページに移動します。
3. [ソフトウェアをインストールします。] をクリックします。
   ソフトウェアインストールモードのウィザードが開きます。

ソフトウェアインストールモードのウィザードは、ソフトウェアのインストールとシステムの変更に伴うベースラインの更新をガイドします。

また、`fsims`を使用して、ソフトウェアインストールモードをシェルから実行できます。

5.4.3 ベースラインの作成

完全性検査は、保護したいファイルのベースラインを作成することで設定されます。

本製品をインストールするときには標準のシステムファイルが*既知のリスト*に一式追加されますが、デフォルトの設定ではそれらのファイルに対するベースラインは作成されません。ベースラインをインストール時に作成するには、`pass=PASS`パラメータ、またはウェブインターフェース、もしくはコマンドラインクライント(`fsic`) を使用してください。

インストール中にベースラインに追加されたファイルはすべて [許可] と [警告] の保護モードに設定されます。

注: 本製品をインストールした時に既知のファイルは作成されます。初期状態では、システムの重大なファイルが含まれ、格納されるファイルとその数はディストリビューションによって異なります。既知のファイルを表示するには、`/opt/f-secure/fsav/bin/fslistfiles`を実行してください。

ベースラインのパスワード

保護しているファイルに対する変更処理を阻止するために、作成したベースラインを暗号化する必要があります。

本製品はベースラインとシステムの完全性を暗号化して検査します。ベースラインの署名 (HMAC署名) を作成するために、ベースラインのコンテンツとパスワードに暗号化されたアルゴリズムが適用されます。

重要: パスワードは後から回復できませんので忘れないように注意してください。また、ベースラインに指定のパスワードを認証しない限り、ベースラインの検査を実行することはできません。

注: ベースラインはパスワードを使用して再設定ができるため、パスワードの管理には注意が必要です。

ファイルシステムの完全性検査

システムの安全性とベースラインを確認するために、ベースラインを手動で検査することができます。

1. パスワードを入力して、ベースラインを検査します。
2. ベースラインを検査している際には別の完全性検査を実行しないでください。

ベースラインが第三者によって更新された場合、ベースラインを新たに検査するときにパスワードが既存のパスワードと一致されないようになります。

5.5 基本設定

[基本設定] のページでは、警告の通知方法と自動更新の設定を行うことができます。また、本製品のバージョン情報も確認できます。

5.5.1 警告

「警告」ページでは、警告メッセージを読んだり、削除したりすることができます。

警告の深刻度

警告には次の深刻度があります。

深刻度	Syslog priority	説明
情報	info	ホストからの通常の操作情報。
警告	warning	ホストからの警告。 ファイルの読み込みにエラーが発生した場合などに発生します。
エラー	err	ホスト上の回復可能なエラー。 ウイルス定義ファイルの更新が以前に受信したものよ

深刻度	Syslog priority	説明
		りも古いときなどに発生します。
重大なエラー	emerg	ホスト上の回復不能なエラー。 処理の実行エラー、カーネルモジュールのエラーなどに発生します。
セキュリティ警告	alert	ホスト上のセキュリティ警告。 感染および実行された処理の情報を含みます。

警告の処理

「警告」ページでは、警告を読んだり、削除したりすることができます。

警告を検索するには、以下の手順を実行します。

1. 表示したい警告のステータスを選択します。
   - すべての警告を表示するには、[すべて] を選択します。
   - 新しい警告を表示するには、[未読] を選択します。
   - すでに読んだ警告を表示するには、[既読] を選択します。
2. 表示したい警告の [深刻度] を選択します。
3. 複数のメッセージを同時に削除、または既読としてマークできます。
   - [警告] をクリックして強調した後に [強調表示された項目を既読としてマーク] をクリックしたら、メッセージを既読にできます。
   - [強調表示された項目を削除] をクリックしたら、強調された警告をすべて削除します。

注: 複数のメッセージを同時に削除、または既読としてマークできます。編集するセキュリティ警告メッセージ、およびメッセージの経過日数を選択して、[アクションの実行] をクリックしたら、メッセージを削除または既読としてマークできます。

警告の転送

「通知方法」ページでは、警告の送り先を設定することができます。

集中管理モードを使用している場合、[サーバアドレス] フィールドに表示されているアドレスがF-Secureポリシーマネージャサーバのアドレスと一致しているか確認してください。[ポリシーマネージャサーバ証明書のアップロード] フィールドにadmin.pubキーの場所を指定します。これはF-Secureポリシーマネージャコンソールをインストールした際に作成したキーです。

1. 警告レベルでは、深刻度別に警告の送り先を指定できます。警告は以下に送信することができます。
   - 電子メールの送信先 - 警告を指定の電子メールアドレスに送信します。
   - ローカル - 警告をウェブインターフェースに表示します。
   - **Syslog** - 警告をシステムのログに書き込みます。Syslog facilityはLOG_DAEMONを使用し、警告のpriorityはそれぞれ異なります。
   - ポリシーマネージャ - 警告をF-Secureポリシーマネージャコンソールに送信します。

2. 電子メールの設定

   電子メールの設定では、電子メールで転送される警告の設定を指定できます。

   a) SMTPサーバアドレスのアドレスを [サーバ] フィールドに入力します。DNS名またはIPアドレスを使用できます。サーバは常にポート25番を使用し、変更することはできません。

   > 注: メールサーバが稼動していないまたはネットワークがダウンしている場合、警告が正常に通知されないことがあります。この問題を防ぐにはローカルのポート25でメールサーバを稼動し、警告送信用のメールサーバとして利用します。

   b) 警告の差出人となる電子メールアドレス (例: sender@example.com) を [送信元] フィールドに入力します。

   c) 警告メールの件名を入力します。[件名] フィールドに%DESCRIPTION%を使用したら、警告の簡単な説明を件名に表示することができます。

5.5.2 ウイルス定義ファイルの自動更新

F-Secure自動更新エージェントはコンピュータを常に最新の保護状態にする機能です。

F-Secure自動更新エージェントはインターネットに接続しているときに最新のウイルス定義ファイルをコンピュータにダウンロードします。

ウイルス定義ファイルの最新情報は次のURLでご覧になれます。
http://www.F-Secure.com/download-purchase/updates.shtml

> 注: プロテクションサービスビジネスの管理モードでは、F-Secure自動更新エージェントが最新のLinuxセキュリティのインストーラをプロテクションサービスビジネスポータルのサーバから入手します。

自動更新

プロキシサーバを利用する場合や、定義ファイルの自動更新を変更する場合に設定を行います。

1. [更新は有効] をオンにすると、ウイルス定義ファイルの自動更新を有効にします。デフォルトの設定では、この機能は有効です。
2. F-Secureポリシーマネージャプロキシを設定します。

   ポリシーマネージャプロキシのリストはウイルス定義ファイルの更新ソースとF-Secureポリシーマネージャプロキシを表示します。更新サーバを設定していない場合、最新のウイルス定義ファイルはF-Secureの更新サーバから自動的に更新されます。

   a) リストに新しいアドレスを追加するには、URLを [**PM**プロキシアドレス] に入力します。

   b) [**PM**プロキシを追加する] をクリックして、新しい項目をリストに追加します。
3. インターネットのアクセスにプロキシを必要とする場合、HTTPプロキシを設定します。

   a) ウイルス定義ファイルの更新にHTTPプロキシサーバを利用する場合、[**HTTP**プロキシを使用する] をオンにします。

   b) [**HTTP**プロキシアドレス] にHTTPプロキシのサーバアドレスを次の形式で入力します。
   `http://[username:password@]host[:port]`
   例：`http://user:password@example.com:8080`
4. 定期更新

   a) [自動更新間隔] にウイルス定義ファイルの更新を確認する頻度を分単位で指定します。

   b) [仲介サーバのフェールオーバ時間] に更新サーバへ接続する際のフェールオーバ時間を分単位で指定します。

   [**F-Secure**更新サーバからの自動更新を有効にする] が有効の状態で、指定した時間の間に更新サーバへ接続できない場合 、F-Secure更新サーバから自動的に最新のウイルス定義ファイルがダウンロードされます。

c) [F-Secure更新サーバからの自動更新を有効にする] をオンにすると、指定の更新サーバに接続できない場合、F-Secure更新サーバへ代わりに接続してウイルス定義ファイルを更新するようになります。

d) ウイルス定義ファイルを更新した後にウイルススキャンを自動的に実行するか指定します。このウイルススキャンはローカルのファイルとディレクトリをすべてスキャンしますので時間がかかることがあります。また、スキャンの設定にはマニュアルスキャンの設定が適用されます。デフォルトではスキャンは実行されません。

5. リマインダを設定します。

a) ウイルス定義ファイルが最近更新されていない場合、リマインダを送信するように設定できます。リマインダを有効にするには、[リマインダの送信] にチェックを入れ、リマインダが送信されるための経過日数を指定します。

リマインダの深刻度は「セキュリティ警告」になります。

ウイルス定義ファイルの経過日数が表示されます。

b) ウイルス定義ファイルを「古い」とみなすために必要な経過日数を指定します (3-30日の間、デフォルトでは7日)。ウイルス定義ファイルが指定の日数より古くなったら、警告がリマインダとして送られます。

5.5.3 F-Secureアンチウイルスプロキシ

F-Secureアンチウイルスプロキシは低速なネットワーク接続の負荷を大幅に減少できるツールで、配布したF-Secure製品の帯域問題を解決することができます。

F-Secureアンチウイルスプロキシを更新ソースに指定すると、ウイルス定義ファイルの更新をF-Secureポリシーマネージャサーバからではなく、LANからダウンロードするように設定できます。

👉 注: F-Secureアンチウイルスプロキシのインストールと設定については、『F-Secureポリシーマネージャ管理者ガイド』の「F-Secureアンチウイルスプロキシ」を参照してください。

5.5.4 バージョン情報

「バージョン情報」ページでは、ライセンスとバージョン情報、およびデータベースのバージョンが表示されます。

評価版を使用している場合、「バージョン情報」ページでライセンスキーコードを入力することで製品をライセンス版にアップグレードできます。本製品をプロテクションサービスビジネスの管理モードにアップグレードする場合、プロテクションサービスビジネスのキーコードとバックウェブサーバのアドレスを入力してください。

👉 注: 評価期間が過ぎた場合、本製品を使用する前にキーコードを入力する必要があります。

トラブルシューティング

トピック：

ここでは、本製品の設定、機能、一般的な問題や質問などに関連するサポート情報をまとめています。

6.1 カーネルモジュールの手動インストール

カーネルモジュールをインストールする前に、次のことを実行する必要があります。›起動しているカーネルバージョンがインストールしたカーネルソースと同じバージョンであることを確認してください。カーネルの設定も同じである必要があります。›ディストリビューションによっては(SUSEディストリビューションの旧バージョンなど)、カーネルソースがインストールされたカーネルと一致するために、/usr/src/linuxに移動して、 make cloneconfigとmake modules_prepareのコマンドを実行する必要があります。

起動しているカーネルのバージョンがインストールしたカーネルソースと同じバージョンであることを確認します。カーネルの設定も同じである必要があります。ディストリビューションによっては(SUSEの旧バージョンなど)、カーネルを一致するために、/usr/src/linuxに移動して、次のコマンドを実行する必要があります。

```
make cloneconfigmake modules_prepare
```

カーネルモジュールをインストールするには、以下の手順を実行します。

root権限で次のコマンドを実行します。/opt/f-secure/fsav/bin/fsav-compile-drivers
ウェブインターフェースの「サマリ」ページでエラーが表示されていない場合、本製品は正常に動作していることになります。

fsav-compile-driversはDazukoドライバをシステムに自動的に設定およびコンパイルするシェルスクリプトです。Dazukoの詳細については、*www.dazuko.org*を参照してください。

👉 注: Dazukoのドライバは*www.dazuko.org*からダウンロードして本製品で使用できますが、推奨しません。本製品に付属するDazukoのバージョンは(/opt/f-secure/fsav/dazuko.tar.gzにインストールされる) 広範囲にわたってテスティングが行われております。

ご利用のLinuxディストリビューションにDazukoがプレインストールされている場合、パッチと構成が本製品のDazukoと異なる可能性が高いため、使用することを推奨しません。プレインストールのDazukoをアンインストール、またはシステム起動時に実行しないように設定して、上記のインストール手順に従って本製品付属のDazukoを必要なパッチと構成オプションを指定した状態でインストールしてください。

6.2 ウェブインターフェース

トラブルシューティング - ウェブインターフェース

ウェブインターフェースにログインできません。どうすればいいですか?

ディストリビューションによって、/etc/pam.d/loginにある次の行をコメントアウトする必要があります (行の始まりに # 記号を追加します)。

```
# auth requisite pam_securetty.so
```

ウェブインターフェースでデバッグログを有効にするにはどうすればいいですか?

/opt/f-secure/fsav/tomcat/conf/logging.propertiesに次の設定を追加します。

```
.level=FINEST
```

ログファイルは/var/opt/f-secure/fsav/tomcat/catalina.outにあります。

6.3 F-Secureポリシーマネージャとプロテクションサービスビジネスポータル

トラブルシューティング - F-Secure Policy Manager

製品をアップグレードしたらネットワークに問題が発生しました。どうすればいいですか?

F-Secureポリシーマネージャの MIBファイルをアップグレードする必要があります。MIBファイルをアップグレードしていない場合、本製品は「サーバ」のファイアウォールプロフィールを使用し、ほぼすべてのネットワークトラフィックをブロックします。

製品にプロテクションサービスビジネスのキーコードを適用できません。どうすればいいですか?

プロテクションサービスビジネスのキーコードを認証するためにプロテクションサービスビジネスのサーバに接続できることが必要です。サーバに接続できない場合、製品を評価版としてインストールして、後からプロテクションサービスビジネスの管理モードにアップグレードできます。詳細については、『インストール』のアップグレードに関する情報を参照してください。

プロテクションサービスビジネスのライセンスが切れました。どうすればいいですか?

プロバイダーに連絡してプロテクションサービスビジネスのライセンスを更新するか、スタンドアロンのライセンス版、またはポリシーマネージャによる集中管理で製品を引き続き使用できます。

製品をスタンドアロンまたはポリシーマネージャによる集中管理で使用する場合、fsav-configツールで製品を設定する必要があります。ツールがキーコードを確認するときに有効なライセンスを入力してください。

👉 注: プロテクション サービス ビジネスのライセンスが切れたら製品を評価モードで動作することはできません。

6.4 完全性検査

トラブルシューティング - 完全性検査

ソフトウェアインストールモードを使用しなかったことで、システムが正常に動作しなくなりました。どうすればいいですか?

新しいベースラインを作成する必要があります。次のコマンドを実行してください。

```
/opt/f-secure/fsav/bin/fslistfiles | fsic --add -fsic --baseline
```

完全性検査を使用しているときにLinuxカーネルを更新できますか?

カーネルを更新する場合、ソフトウェアインストールモードを使用してください。カーネルを更新した後、ソフトウェアインストールモードを無効にして、セキュリティレベルを以前の設定に戻してください。

ベースライン上のファイルで、更新が必要なものが多くあります。どうすればいいですか?

新しいベースラインを作成する必要があります。次のコマンドを実行してください。

```
/opt/f-secure/fsav/bin/fslistfiles | fsic --add -fsic --baseline
```

ベースラインを作成するときに同じパスワードを毎回使用しないとだめですか?

いいえ。ベースラインの検査には作成時に使用したパスワードを入力する必要がありますが、ベースラインを新たに作成した場合には同じパスワードを使用する必要はありません。

6.5 ファイアウォール

トラブルシューティング - ファイアウォール

製品をインストールした後、ユーザがSambaの共有ファイルをアクセスできません。どうすればいいですか?

[オフィス]のファイアウォールセキュリティレベルは「Windows Networking」のルールを含めていますが、デフォルトでは無効になっています。ルールを有効にすると、sambaの共有を許可できます。

製品をインストールした後、LANのドメインとワークグループ (SMB) を参照できません。どうすればいいですか?

LAN内のWindows共有オブジェクトを許可するファイアウォールルールを追加する必要があります。以下の手順を実行します。

1. ウェブインターフェースの詳細モードで、「ファイアウォール > ネットワークサービス」ページに移動します。
2. [新しいサービスの追加] をクリックします。
3. 次のサービスを作成します。
   - サービス名: `Windows Networking Local Browsing`
   - プロトコル: `UDP`
   - 開始ポート: `137-138`
   - 応答ポート: `>1023`
   - 説明: `SMB LAN browsing`
4. [] -> [保存.
5. ファイアウォールのメニューで、[ファイアウォールルール] をクリックします。
6. [新しいルールの追加] をクリックします。
7. 次のルールを作成します。
   - タイプ: `ACCEPT`
   - リモートホスト: `[myNetwork]`
   - 説明: `Windows Networking Local Browsing`
   - サービス (ボックスを選択): `Windows Networking Local Browsing`
   - 方向: `in`
8. [このルールにサービスを追加する] -> [ファイアウォールルールの追加] の順にクリックします。新しいルールがルールリストの一番下に追加されます。ルールが表示されない場合、[>>] をクリックして、ルールをリストの一番下に移動します。
9. 新しいルールの横にある上矢印をクリックして、「Deny rest」ルールの上に移動します。
10. [保存] をクリックしたら、新しいルールが保存され、ファイアウォールに適用されます。

SMB LANブラウジングが利用できるようになります。

NFSサーバのアクセスを許可するには、どうすればいいですか?

以下のネットワークトラフィックを許可する必要があります。

- portmapper (tcpおよびudpポート111)
- nfsd (tcpおよびudpポート2049)

- mountd (portmapperからの可変ポート)

MountdはNFSの共有がマウントされた場合にのみ必要になります。マウントが完了したら、すべてのトラフィックはnsfdにいきます。

mountdのポートは固定されていないため、次の手順を実行してNFSの共有をマウントします。

- ファイアウォールを無効にして、NFSの共有をマウント(またはアンマウント)してからファイアウォールを有効にします。
- NFSサーバ上でmountdを`--port PORT`のオプションを付けて実行します。mountdに固定のポート番号が指定されます。
- ポート番号にudpとtcpの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ます。

6.6 ウイルス保護

トラブルシューティング - ウイルス保護

リアルタイムスキャンでデバッグログを有効にするにはどうすればいいですか?

ポリシーマネージャコンソールで、[製品 > 基本設定 > 詳細] に移動して、[**fsoasd**ログレベル] を [デバッグ] に設定します。

スタンドアロンインストールでは、次のコマンドを実行します。

```
/opt/f-secure/fsma/bin/chtest s 44.1.100.11 9
```

ログファイルは`/var/opt/f-secure/fsav/fsoasd.log`にあります。

HTTPプロキシサーバを使用して更新はダウンロードできますか?

ポリシーマネージャコンソールを利用する場合、[**F-Secure**自動更新エージェント > 基本設定 > 通知方法 > **HTTP**設定 > ユーザ定義のプロキシ設定] に移動して、[アドレス] を [`http://[[user][:pass]@]proxyhost[:port]`] に設定します。

ウェブインターフェースで、「自動更新」ページの詳細設定を使用してください。

リアルタイムスキャンは**NFS**サーバで動作しますか?

本製品がNFSサーバにインストールされている場合、クライアントがサーバ上のファイルにアクセスするときにリアルタイムスキャンは実行されません。

リアルタイムスキャンを一時的に無効にするにはどうすればいいですか?

特定のシステムツール (バックアップ、復元など) を実行する場合において、リアルタイムスキャンを一時的に無効にすることができます。

ウイルススキャンおよび完全性検査を無効にするには、以下のコマンドを実行します。

```
/opt/f-secure/fsma/bin/chtest s 45.1.40.10 0/opt/f-secure/fsma/bin/chtest
s 45.1.70.10 0
```

リアルタイムスキャンと完全性検査をもう一度有効にするには、以下のコマンドを実行します。

```
/opt/f-secure/fsma/bin/chtest s 45.1.40.10 1/opt/f-secure/fsma/bin/chtest
s 45.1.70.10 1
```

ファイルの名前を変更するときや、リンクするときにリアルタイムスキャンは実行されますか?

リアルタイムスキャンはファイルを開く、閉じる、実行するたびに実行されます。ファイル名を変更したり、リンクを削除したりする際にはスキャンされません。

6.7 他のセキュリティ製品との互換性

本製品との互換性の問題

本製品のオンアクセス ファイル スキャンは低レベルのカーネル機能を使用しています。他のセキュリティやアクセス制御を行う製品が同様の機能を持っている場合、競合する可能性があります。互換性に問題がある製品を同時に使用すると、システムのパフォーマンスが低下し、不安定になることもあります。

互換性の問題および解消法の最新情報については、リリース ノーツを参照してください。

6.8 一般

一般的な問題に関連するサポート情報です。

中断されたインストールを続行するにはどうすればいいですか?

本製品のインストールが途中で中断された場合、本製品のコンポーネントを手動で削除する必要があるかもしれません。

1. インストールされたRPMパッケージを表示します。

```
rpm -qa | grep f-securerpm -qa | grep fsav
```

2. インストールされたパッケージを削除します。各パッケージに次のコマンドを実行します。

```
rpm -e --noscripts <package_name>
```

3. コンポーネントのインストールディレクトリをそれぞれ削除します。

```
rm -rf /var/opt/f-secure/fsavrm -rf /var/opt/f-secure/fsmarm -rf
/etc/opt/f-secure/fsavrm -rf /etc/opt/f-secure/fsmarm -rf
/opt/f-secure/fsavrm -rf /opt/f-secure/fsma
```

システムの動作が遅く感じます。原因はなんですか?

リアルタイムスキャンと完全性検査によってシステムの動作が遅くなることがあります。

1. Linuxの基本ツール (topとvmstat) を使用して、原因を確認してください。
2. 本製品付属のDazukoを使用していることを確認してください。
3. スキャン時間の長いファイルがある場合、それらのファイルをスキャンから対象外にすることによって動作が軽くなることもあります。
4. 集中管理モードを使用している場合、DNSクエリに対する応答がすぐ返るか確認してください。またはIPアドレスを利用してF-Secure ポリシーマネージャと通信してください。

製品がデータベースにアクセスできません。どうすればいいですか?

システムに強制終了や異常が発生した場合、データベースを一時的にアクセスできなくなることがあります。問題を解決するには、次の手順を実行します。

1. root権限でデータベースのPIDファイルを削除します。

```
rm /var/opt/f-secure/fsav/pgsql/data/postmaster.pid
```

2. root権限で製品を再起動します。

```
/etc/init.d/fsma restart
```

「F-Secureステータスデーモンが起動していません」というエラー警告が発生しています。デーモンを起動するにはどうすればいいですか?

システムに強制終了や異常が発生した場合、F-Secureステータスデーモンが起動しなくなることがあります。問題を解決するには、本製品を再起動します。

```
/etc/init.d/fsma restart
```

以下の場合において、必要なカーネルドライバを手動でコンパイルする必要があります。

```
/opt/f-secure/fsav/bin/fstatusd
```

Linuxカーネルがモジュールを読み込めない場合、どうすればいいですか?

たとえば、カーネルをアップグレードした後にカーネルのモジュールが自動的に再構築されないため、モジュールを再コンパイルする必要があります。次の場合、カーネルのドライバを手動でコンパイルする必要があります。

- インストール時にコンパイラまたは必要なツールが不足している
- インストール時にカーネルヘッダまたはソースが不足している
- カーネルをアップグレードして、ドライバをコンパイルする必要がある

ドライバのコンパイルとインストールを行うために次のコマンドを実行します。:

```
/opt/f-secure/fsav/bin/fsav-compile-drivers
```

コマンドラインのツール

トピック：

本製品とその機能はコマンドラインから実行することができます。

コマンドラインオプションの詳細については、『Manページ』を参照してください。

A.1 fsav

fsavはウイルスとマルウェアをスキャンするためのプログラムです。

fsavは指定のターゲット (ファイルまたはディレクトリ) をスキャンし、悪質な/不正なコードを検出した際に警告を通知します。感染したファイルが検出された場合、ファイルに対して駆除、名前の変更、削除の処理を実行することが可能です。

シェルからファイルをスキャンするには、次の手順を実行します。

- デフォルトで設定されているスキャン対象のファイル形式をすべてのローカルディスクでスキャンするには、次を入力します。`fsav /`
- ディレクトリおよびサブディレクトリ内にあるすべてのファイルをスキャンするには、ディレクトリ名を入力します。例：`fsav mydirectory`
- 特定のファイルを1つスキャンするには、ファイル名を入力します(ワイルドカードは含めない)。例：`fsav myfile.exe`

再帰的スキャンはマウントされたネットワークのサブディレクトリを検知しますが、ネットワークのファイルシステムをスキャンしません。クライアントからネットワークのファイルシステムをスキャンすると、ネットワークに無駄な負担が発生します。また、ネットワークに対するスキャンはローカルシステムに対するスキャンより時間がかかる可能性があります。

ネットワークのファイルシステムをスキャンするには、サーバ上で `fsav /` を実行してください。

fsavをサーバで実行できない場合、マウントされたネットワークのディレクトリをfsavのコマンドラインに指定することでクライアントからネットワークをスキャンできます。

たとえば、NFSファイルシステムが`/mnt/server1`にマウントされている場合、次のコマンドでファイルシステムをスキャンすることができます。`fsav /mnt/server1`

> 注: 本製品はマウントされたファイルシステムにあるファイルしかスキャンできません。CD-ROMやDATデバイス (/dev/st0, /dev/hda and such) などの特別なファイルはファイルシステムとしてマウント、またはあらかじめ解凍/展開されている場合に限り、スキャンできます。

コマンドラインオプションの詳細については、fsavの『Man』ページを参照してください。また、コマンドラインから`fsav --help`を入力して、ヘルプをご覧になれます。

A.2 fsav-config

`fsav-config`は本製品を初期化します。

RPMパッケージから本製品をインストールする場合、`fsav-config`を使用する必要があります。

1. 本製品を初期化するには、次のコマンドを実行します。`/opt/f-secure/fsav/fsav-config`
   画面上に質問が続けて表示されます。デフォルトの値は括弧の中にあります。`ENTER`を押すと、デフォルトの値を選択します。
2. ウェブインターフェースの言語を選択します。

```
Select language to use in Web User Interface [1] English (default) [2]
Japanese [3] German
```

3. インストールのモード(スタンドアロン、ポリシーマネージャによる集中管理、プロテクションサービスビジネスによる集中管理) を選択します。
   - プロテクションサービスビジネスによる集中管理を選択した場合、プロテクションサービスビジネスバックウェブサーバのアドレスを入力します。

- ポリシーマネージャによる集中管理を選択した場合、ポリシーマネージャサーバのアドレスとadmin.pubキーの場所を入力します。このファイルはF-Secureポリシーマネージャコンソールをインストールした際に作成したキーです。

4. キーコードを入力して、本製品のライセンス版を構成します。キーコードはハイフンを含めた形で入力します。製品を評価する場合、ENTERを押します。

   注: プロテクションサービスビジネスによる集中管理を選択した場合、製品を評価することはできません。

5. インターフェースのリモートアクセスを許可するか選択します。

```
Allow remote access to the web user interface? [no]
```

6. インターフェースをログインしないでローカルのホストからアクセスできるか選択します。

```
Allow connections from localhost to the web user interface without login?
 [yes]
```

7. インターフェースを使用できるユーザ名を入力します。

```
Please enter the user name who is allowed to use the web user interface.
```

   注: ユーザ名にはローカルのLinuxアカウントを指定してください。ユーザが存在しない場合、アカウントを作成する必要があります。rootのアカウントは使用しないでください。

A.3 dbupdate

dbupdateはF-Secure Anti-Virusのウイルス定義ファイルを更新するためのシェルスクリプトです。

コマンドラインからウイルス定義ファイルを手動で更新するには、以下の手順を実行します。

1. fsdbupdate9.runを*http://download.f-secure.com/latest/fsdbupdate9.run*からダウンロードします。fsdbupdate9.runは自動更新エージェントのデーモンを中止して、データベースの更新と自動更新エージェントの再起動を行う自己解凍ファイルです。
2. root権限のあるユーザでdbupdate fsdbupdate9.runを実行します。fsdbupdate9.runにはfsdbupdate9.runの絶対また相対パスを指定してください

コマンドラインオプションの詳細については、dbupdateの『Man』ページを参照してください。また、コマンドラインからdbupdate --helpを入力して、ヘルプをご覧になれます。

A.4 fsfwc

fsfwcはファイアウォールのセキュリティレベルを変更するためのコマンドラインツールです。

セキュリティレベルを変更するには、以下のコマンドを使用します。/opt/f-secure/fsav/bin/fsfwc --mode {block, mobile, home, office, strict, normal, bypass}

A.5 fsic

fsicのコマンドラインツールを使用すると、ベースラインの作成、ベースラインへのファイルの追加、およびベースラインの検査を実行できます。

1. ベースラインを作成するには、以下の手順を実行します。
   a) fsicツールを--baselineオプションで実行します。`fsic --baseline`
   b) パスワードを入力して、署名を作成します。

   新しいベースラインが作成されます。
2. ベースラインにファイルを追加するには、以下の手順を実行します。
   a) fsicコマンドを、--add、--alert、--protect optionsのオプションで実行します。`/opt/f-secure/fsav/bin/fsic --add --alert=yes --protect=yes /etc/passwd /etc/shadow`
   b) ベースラインを再設定します。ベースラインの更新進捗が表示され、途中でベースラインに新しいファイルを追加するか確認メッセージも表示されます。`/opt/f-secure/fsav/bin/fsic --baseline`
   c) パスワードを入力して、署名を作成します。

   この例では、保護ファイルに対する不正な変更処理の警告も送信されるように設定されています。
3. ベースラインの検査
   a) 以下のコマンドを実行します。`/opt/f-secure/fsav/bin/fsic`
   b) ベースラインを作成した際に使用したパスワードを入力します。

   ベースラインのファイルが認証され、終了したらベースラインの状態が表示されます。

A.6 fsims

fsimsはソフトウェアインストールモードをコマンドラインから実行します。

新しいソフトウェアをインストールするには、以下のコマンドを実行します。

1. ソフトウェアインストールモードを有効にするには、以下のコマンドを実行します。`:/opt/f-secure/fsav/bin/fsims on`
2. 新しいソフトウェアをインストールします。
3. ソフトウェアインストールモードを無効にして、通常のセキュリティレベルを設定します。`/opt/f-secure/fsav/bin/fsims off`

A.7 fsma

fsmaは各モジュールのステータスを確認します。

次のコマンドを実行します。`/etc/init.d/fsma status`

モジュール	コマンド	説明
F-Secure警告データベースハンドラデーモン (F-Secure Alert Database Handler Daemon)	`/opt/f-secure/fsav/sbin/fsadhd`	ローカルのデータベースに警告を保存します。警告はウェブインターフェースで表示することができます。
F-Secure FSAVポリシーマネージャデーモン (F-Secure FSAV Policy Manager Daemon)	`/opt/f-secure/fsav/bin/fsavpmd`	F-Secureポリシーマネージャコンソールの操作をすべて処理し

モジュール	コマンド	説明
		ます([すべてのハードディスクのスキャン]、[データベースを今すぐ更新]、[統計情報のリセット]など)。
F-Secureファイアウォールデーモン (F-Secure Firewall Daemon)	/opt/f-secure/fsav/bin/fsfwd.run	F-Secure管理エージェントとnetfi l ter/iptablesファイアウォールの間のインターフェースです。
F-Secure FSAVライセンス警告ハンドラ (F-Secure FSAV License Alerter)	/opt/f-secure/fsav/libexec/fslmalerter	本製品の評価版をインストールした場合、評価期間の残り日数を確認します。
F-Secure FSAVオンアクセススキャナデーモン (F-Secure FSAV On-Access Scanner Daemon)	/opt/f-secure/fsav/sbin/fsoasd	すべてのリアルタイム保護機能を提供します(リアルタイムウイルススキャン、完全性検査、ルートキット保護を含む)。
F-Secure FSAVステータスデーモン (F-Secure FSAV Status Daemon)	/opt/f-secure/fsav/bin/fstatusd	各コンポーネントのステータスを確認して、デスクトップのパネルアプリケーションおよびウェブインターフェースで最新の状態を表示します。
F-Secure FSAVウェブUI (F-Secure FSAV Web UI)	/opt/f-secure/fsav/tomcat/bin/catalina.sh start	ウェブインターフェースの操作を処理します。
F-Secure FSAV PostgreSQLデーモン (F-Secure FSAV PostgreSQL daemon)	/opt/f-secure/common/postgresql/bin/startup.sh	ウェブインターフェースで表示できる警告を保存します。
F-Secure更新デーモン	/opt/f-secure/fssp/libexec/fsupdated	製品の更新を自動的に適用します。

A.8 fssetlanguage

fssetlanguageはインターフェースの言語を設定します。

言語を設定するには、次のコマンドを実行します。/opt/f-secure/fsav/bin/fssetlanguage <language>

以下の言語を指定することができます。

- en - 英語
- ja - 日本語
- de - ドイツ語

A.9 fschooser

fschooserは製品の機能を有効または無効にするためのコマンドラインです。

不要なコンポーネントやシステムのリソースを開放する必要がある場合、便利な機能です。

1. 以下のコマンドを実行します。/opt/f-secure/fsav/sbin/fschooser
   画面に製品のセキュリティコンポーネントが表示されます。
2. 画面の指示に従い、コンポーネントを有効または無効にします。

   ```
   Firewall - ENABLED, press f+RET to toggle
   Web User Interface - ENABLED, press w+RET to toggle
   ```

3. 設定を適用するには、[RETURN] を押します。

   注: 設定をキャンセルする場合、[ctrl+C] を押します。

ウェブインターフェース

トピック：

ウェブインターフェースのオプション

ウェブインターフェースで設定できるオプション

B.1 ウェブインターフェース

ウェブインターフェースのオプション

ウェブインターフェースで設定できるオプション

B.1.1 一般タスク

ウェブインターフェース > 一般タスク ページのオプション

オプション	説明
マルウェアをスキャンする	マルウェアを手動でスキャンするウィザードを開きます。対象となるファイル/ディレクトリを選択できます。
ファイアウォールルールの作成	ファイアウォールルールを作成するウィザードを開きます。ルールに対して新しいサービスを作成する必要がある場合、詳細モードの「ファイアウォールルール」ページで設定を行ってください。
ファイルシステムの完全性を確認する	ファイルシステムに対して完全性検査を実行するウィザードを開きます。完全性検査のベースラインに指定されているファイルが変更されていないか検証します。
ウイルス定義ファイルを更新する	詳細モードの「自動更新」ページを開きます。ウイルス定義ファイルの更新に関する設定を変更できます。
ソフトウェアをインストールする	このウィザードは、システムのアップグレードを行うために製品をソフトウェアインストールモードに設定します。システムをアップグレードした後、ウィザードに戻り、完全性検査のベースラインを更新することができます。これにより、アップデートしたシステムファイルが不要な警告を発生することを回避できます。
ベースラインの作成	完全性検査のベースラインを作成するウィザードを開きます。

B.2 ウェブインターフェースの詳細モード

ウェブインターフェースの詳細モード

ウェブインターフェースの詳細モードで設定できるオプション

B.2.1 サマリ

詳細モード > サマリ ページのオプション

オプション	説明
ウイルス保護	有効の場合、システム上の全ファイルアクセスに対してマルウェアのスキャンが実行されます。オ

オプション	説明
	ンアクセスの完全性検査を行うために有効にする必要があります。 選択されているセキュリティレベルを指定します。セキュリティレベルに応じてファイアウォールルールとアプリケーション通信制御が動作します。
ファイアウォール保護	有効の場合、完全性検査はベースラインしたファイルが変更されていないか検出します。

B.2.2 警告

詳細モード > 警告 ページのオプション

オプション	説明
警告テーブル	「警告」ページでは、警告メッセージを読んだり、削除したりすることができます。以下の方法で警告を検索できます。1. 表示したい警告のステータスを選択します。*すべての警告を表示するには、[すべて] を選択します。* 新しい警告を表示するには、[未読] を選択します。* すでに読んだ警告を表示するには、[既読] を選択します。2. 表示したい警告の [深刻度] を選択します。詳細については、『警告の深刻度』 (P. 38) を参照してください。警告を選択した後に [強調表示された項目を既読としてマーク] をクリックしたら、メッセージを既読にできます。[強調表示された項目を削除] をクリックしたら、強調された警告をすべて削除します。
警告データベースの管理	複数のメッセージを同時に削除、または既読としてマークできます。対象となる警告メッセージの深刻度、およびメッセージの経過日数を選択して、[アクションの実行] をクリックしたらメッセージを削除または既読としてマークできます。

B.2.3 ウイルス保護

ウイルス保護のオプション

リアルタイムスキャン

詳細モード > ウイルス保護 > リアルタイムスキャン ページのオプション

オプション	説明
1次アクション	感染を検出したときに実行する1次アクションを設定します。レポート/アクセスをブロック = アクセスを拒否し、警告を送信します。駆除 = アクセスを拒否します。ファイルを駆除し、成功した場合にはアクセスを許可します。名前の変更 = アクセスを拒否し、感染したファイルの拡張子を .virus に変更します。削除 = アクセスを拒否し、感染したファイルを削除します。アクセスをブロック = アクセスを拒否し、警告を送信しません。1次およ

オプション	説明
	び2次アクションが失敗した場合、アクセスを拒否し、セキュリティ警告を送信します。
不審なファイルに対する1次アクション	不審なファイルを検出したときに実行する1次アクションを設定します。レポート/アクセスをブロック = アクセスを拒否し、警告を送信します。名前の変更 = 不審なファイルの拡張子を .suspected に変更します。削除 = 感染したファイルを削除します。アクセスをブロック = アクセスを拒否し、警告を送信しません。1次アクションが失敗した場合、2次アクションを実行します。2次アクションが失敗した場合、失敗したアクションを記述した警告を送信します。
不審なファイルに対する2次アクション	不審なファイルを検出し、1次アクションが失敗したときに実行する2次アクションを設定します。レポート/アクセスをブロック = アクセスを拒否し、警告を送信します。名前の変更 = 不審なファイルの拡張子を .suspected に変更します。削除 = 感染したファイルを削除します。アクセスをブロック = アクセスを拒否し、警告を送信しません。1次アクションが失敗した場合、2次アクションを実行します。2次アクションが失敗した場合、失敗したアクションを記述した警告を送信します。
スキャン対象外のファイルとディレクトリ	スキャンの対象外となるディレクトリを指定します。絶対パス名を使用し、各ディレクトリをそれぞれ別の行に入力してください。ディレクトリ名には空白を使用できます。
実行可能ファイルのみスキャン	スキャンの対象を実行可能ファイルに限定します。マルウェアは文書作成ソフトのマクロなど他の形式のファイルから広がる可能性があるため、この設定は一般的に推奨しません。
安全な実行可能ファイル 安全な実行可能ファイルはベースラインと一致している必要があります	すべてのファイルアクセスが許可されている実行可能ファイルのリスト。実行可能ファイルへのフルパスを1行ずつ入力してください。
ベースラインと一致する場合にのみ安全とみなす	安全とみなされた実行可能ファイルはベースラインと一致する場合にのみファイルアクセスが許可されます。
ファイルを開くときにスキャン	ファイルを開くときにスキャンを実行するか指定します。
ファイルを閉じるときにスキャン	ファイルを閉じるときにスキャンを実行するか指定します。
ファイルを実行したときにスキャン	ファイルを実行したときにスキャンも実行するか指定します。
圧縮ファイル内をスキャン	圧縮ファイルをリアルタイムスキャンの対象にするか指定します。対応している圧縮ファイルには、TAR.GZ、ZIPなどの形式が含まれています。

オプション	説明
圧縮ファイルの最大ネスト数	圧縮ファイルでスキャン対象となるネスト数を指定します。ネスト数を高い数値に設定すると、DoS (Denial of Service: サービス拒否) 攻撃にシステムをさらすことになります。圧縮ファイルが設定されている最大ネスト数を超えている場合、スキャンエラーが生成されます。スキャンエラーが発生した後のアクションは「リアルタイム保護/エラー処理/スキャンエラー後のアクション」の設定で指定できます。
パスワード保護された圧縮ファイルを安全だとみなす	パスワードで保護されている圧縮ファイルの処理方法を指定します。有効に設定した場合、パスワードで保護されている圧縮ファイルを安全とみなし、アクセスを許可します。無効の場合、アクセスを拒否します。
圧縮ファイル内で最初の感染を見つけた時点で停止する	圧縮ファイル内で最初の感染を検出した時点で実行するアクションを指定します。有効に設定した場合、ウイルスを検出した時点でスキャンが停止されます。無効の場合、圧縮ファイル内のスキャンが完全に終わるまでスキャンが続行します。
リスクウェアをスキャン	はいに設定すると、リスクウェアの検出と処理を有効にします。リスクウェアはスパイウェアまたは他の悪質なプログラムである可能性があります。
リスクウェアに対する1次アクション	リスクウェアを検出したときに実行する1次アクションを設定します。レポート/アクセスをブロック = アクセスを拒否し、警告を送信します。名前の変更 = 感染したファイルの拡張子を .riskware に変更します。削除 = 感染したファイルを削除します。アクセスをブロック = アクセスを拒否し、警告を送信しません。1次アクションが失敗した場合、2次アクションを実行します。2次アクションが失敗した場合、失敗したアクションを記述した警告を送信します。
リスクウェアに対する2次アクション	リスクウェアを検出し、1次アクションが失敗したときに実行する2次アクションを設定します。レポート/アクセスをブロック = アクセスを拒否し、警告を送信します。名前の変更 = 感染したファイルの拡張子を .riskware に変更します。削除 = 感染したファイルを削除します。アクセスをブロック = アクセスを拒否し、警告を送信しません。1次アクションが失敗した場合、2次アクションを実行します。2次アクションが失敗した場合、失敗したアクションを記述した警告を送信します。
除外されたリスクウェア	スキャンの対象外となるリスクウェアを指定します。

スケジュールスキャン

詳細モード > ウイルス保護 > スケジュールスキャン ページのオプション

オプション	説明
スケジュール	スケジュールしたスキャンタスクを crontab と同じような形式で表示します。スケジュールスキャンはマニュアルスキャンの設定を使用します。分、時間、日、月名および曜日名のフィールド値については、『man crontab』を参照してください。

マニュアルスキャン

詳細モード > ウイルス保護 > マニュアルスキャン ページのオプション

オプション	説明
1次アクション	感染を検出したときに実行する1次アクションを設定します。何もしない = 何もしません (ユーザに感染を表示し、処理をしない)。レポートのみ = 警告のみ送信します。ファイルの駆除を試行します。名前の変更 = 感染したファイルの拡張子を .virus に変更します。削除 = 感染したファイルを削除します。カスタム = カスタムの1次アクションフィールドに指定されているコマンドを実行します。スキャンの停止 = スキャンを停止します。1次および2次アクションが失敗した場合、エラーを説明した警告が送信されます。
カスタムの1次アクション	「カスタム」が1次アクションとして選択されている場合、ここでカスタムアクションを設定する必要があります。カスタムアクションはシステムの super user として実行されますので、指定するコマンドに問題がないことを確認してください。カスタムのアクションスクリプトまたはプログラムは、感染したファイルの絶対パスを1つのパラメーターとして受けます。
2次アクション	感染を検出し、1次アクションが失敗したときに実行する2次アクションを設定します。何もしない = 何もしません (ユーザに感染を表示し、処理をしない)。レポートのみ = 警告のみ送信します。ファイルの駆除を試行します。名前の変更 = 感染したファイルの拡張子を .virus に変更します。削除 = 感染したファイルを削除します。カスタム = カスタムの1次アクションフィールドに指定されているコマンドを実行します。スキャンの停止 = スキャンを停止します。1次および2次アクションが失敗した場合、エラーを説明した警告が送信されます。
カスタムの2次アクション	「カスタム」が2次アクションとして選択されている場合、ここでカスタムアクションを設定する必要があります。カスタムアクションはシステムの super user として実行されますので、指定するコマンドに問題がないことを確認してください。カスタムのアクションスクリプトまたはプログラムは、

オプション	説明
	感染したファイルの絶対パスを1つのパラメーターとして受けます。
不審なファイルに対する1次アクション	不審なファイルを検出したときに実行する1次アクションを設定します。何もしない = 何もしません(ユーザに感染を表示し、処理をしない)。レポートのみ = 警告のみ送信します。名前の変更 = 感染したファイルの拡張子を .suspected に変更します。削除 = 感染したファイルを削除します。1次アクションが失敗した場合、2次アクションを実行します。2次アクションが失敗した場合、失敗したアクションを記述した警告を送信します。
不審なファイルに対する2次アクション	不審なファイルを検出し、1次アクションが失敗したときに実行する2次アクションを設定します。何もしない = 何もしません(ユーザに感染を表示し、処理をしない)。レポートのみ = 警告のみ送信します。名前の変更 = 感染したファイルの拡張子を .suspected に変更します。削除 = 感染したファイルを削除します。1次アクションが失敗した場合、2次アクションを実行します。2次アクションが失敗した場合、失敗したアクションを記述した警告を送信します。
ファイルをスキャンすべてのファイル指定した拡張子のファイルのみ	すべてのファイルまたは[スキャンの対象となる拡張子]で選択した拡張子のファイルのみスキャンするか指定します。
対象とする拡張子	スキャンの対象となるファイルの拡張子を指定します。ワイルドカードも使用できます。「?」は1つの文字、「*」はゼロ (0) 文字を含む多数の文字を指定します。「.」は拡張子がないファイルを指定することになります。大小文字の区別はありません。
除外機能を有効にする	スキャンの対象外となるファイルを指定します。ここで指定するファイルはスキャンの対象外 (スキャンの対象に含められている場合でも)になるため、注意が必要です。
スキャン対象外のファイルとディレクトリ	スキャンの対象外となるパスを指定します(ファイルまたはディレクトリ)。絶対パス名を使用してください。各パスをそれぞれ別の行に入力します。パス名には空白を使用できます。
実行可能ファイルをスキャン	実行可能ファイルをスキャンするか指定します。ファイルにユーザやグループなどの実行可能なビットがある場合、ファイルは拡張子に関係なくスキャンされます。
圧縮ファイル内をスキャン	圧縮ファイルをマニュアルスキャンの対象にするか指定します。対応している圧縮ファイルには、TAR.GZ、ZIPなどの形式が含まれています。

オプション	説明
圧縮ファイルの最大ネスト数	圧縮ファイルでスキャン対象となるネスト数を指定します。ネスト数を高い数値に設定すると、DoS (Denial of Service: サービス拒否) 攻撃にシステムをさらすことになります。圧縮ファイルが設定されている最大ネスト数を超えている場合、スキャンエラーが生成されます。
パスワード保護された圧縮ファイルを安全だとみなす	パスワードで保護されている圧縮ファイルの処理方法を指定します。有効に設定した場合、パスワードで保護されている圧縮ファイルを安全とみなし、アクセスを許可します。無効の場合、アクセスを拒否します。
圧縮ファイル内で最初の感染を見つけた時点で停止する	圧縮ファイル内で最初の感染を検出した時点で実行するアクションを指定します。有効に設定した場合、ウイルスを検出した時点でスキャンが停止されます。無効の場合、圧縮ファイル内のスキャンが完全に終わるまでスキャンが続行します。
リスクウェアをスキャン	はいに設定すると、リスクウェアの検出と処理を有効にします。リスクウェアはスパイウェアである可能性があります。
リスクウェアに対する1次アクション	リスクウェアを検出したときに実行する1次アクションを設定します。何もしない = 何もしません (ユーザに感染を表示し、処理をしない)。レポートのみ = 警告のみ送信します。名前の変更 = 感染したファイルの拡張子を .riskware に変更します。削除 = 感染したファイルを削除します。1次アクションが失敗した場合、2次アクションを実行します。2次アクションが失敗した場合、失敗したアクションを記述した警告を送信します。
リスクウェアに対する2次アクション	リスクウェアを検出したときに実行する1次アクションを設定します。何もしない = 何もしません (ユーザに感染を表示し、処理をしない)。レポートのみ = 警告のみ送信します。名前の変更 = 感染したファイルの拡張子を .riskware に変更します。削除 = 感染したファイルを削除します。1次アクションが失敗した場合、2次アクションを実行します。2次アクションが失敗した場合、失敗したアクションを記述した警告を送信します。
除外されたリスクウェア	スキャンの対象外となるリスクウェアを指定します。
アクセス時間の保存	有効に設定した場合、スキャン時にファイルのアクセス時間を変更しません。ウイルス駆除によってファイルを変更した場合、ファイルのアクセス/変更時間が変更されます。

B.2.4 ファイアウォール

ファイアウォールのオプション

基本設定

詳細モード > ファイアウォール > 基本設定 ページのオプション

オプション	説明
ファイアウォールを有効にする	ファイアウォールを有効または無効にするか指定します。有効に設定した場合、使用中のセキュリティレベルに関するファイアウォールルールが着信と発信の両パケットに適用されます。無効に設定した場合、すべてのトラフィックが許可されます。fschooserを使用すると、ファイアウォールの機能そのものを無効にできます。
未処理のネットワークパケットをログする	有効に設定した場合、使用中のファイアウォールルールが対応していない全パケットを syslog に書き込むルールが作成されます。これによってログが増える可能性があります。
信頼済みのネットワークインターフェース (カンマ区切りのリスト)	信頼済みのインタフェース名を指定できます。複数のインタフェース名を入力する場合、カンマで区切ります。インタフェースから発信および着信するトラフィックは許可されます。

ルール

詳細モード > ファイアウォール > ファイアウォールルール ページのオプション

オプション	説明
編集するセキュリティレベル	セキュリティレベルの名前と説明を表示します。プリセットのセキュリティレベルを利用して独自の管理環境を作成することができます。プリセットのセキュリティレベルはデフォルトで有効/無効になっているものがあります。
ファイアウォールルール	ファイアウォールのルールを表示します。ファイアウォールルールはIPアドレス、ポート番号などに基づいてIPパケットをフィルタリング (分別) します。通常、複数のセキュリティレベルから選択できますが、複数のセキュリティレベルに関連するルールを同時に設定することはできません。

ネットワークサービス

詳細モード > ファイアウォール > ネットワークサービス ページのオプション

オプション	説明
ネットワークサービス	ファイアウォールのルールを設定するためのサービスを表示します。プロトコルはIANAまたは"grep IPPROTO.*= /usr/include/netinet/in.h" で検索できます (includes をインストールしていることが必

オプション	説明
	要)。正式に割り当てられたポートは ftp://ftp.iana.org/assignments/port-numbers から入手できます。

B.2.5 完全性検査

完全性検査のオプション

既知のファイル

詳細モード > 完全性検査 > 既知のファイル ページのオプション

オプション	説明
既知のファイル	完全性検査に追加されたファイルを表示します。

B.2.6 基本設定

基本設定のオプション

通信

詳細モード > 基本設定 > 通知方法 ページのオプション

オプション	説明
サーバアドレス	F-Secure管理サーバのURL。HTTP GETの処理中に通信ディレクトリの内容およびサーバのディレクトリとファイル名がこのアドレスに追加されます。他のサーバ機能のアクセス中にはURLの最後尾が追加されます。
ポリシーマネージャサーバ証明書のアップロード	この設定から管理者は管理キーを変更できます。
警告の転送	深刻度別に警告の送り先を指定できます。
サーバ	SMTPサーバのアドレス <ホスト>[:<ポート>] を指定します。"ホスト" はSMTPサーバのDNS名またはIPアドレスで、"ポート" はSMTPサーバのポート番号を示します。詳細については、RFC 2821の仕様を参照してください。
送信元	警告メールで表示される「送信元:」フィールドのメールのアドレス。
件名	SMTP警告メールの件名。次の記号を使用できます。- %SEVERITY% (情報、警告、エラー、重大なエラー、セキュリティ警告) - %HOST_DNS% (送信元のDNSアドレス) - %HOST_IP% (送信元のIPアドレス) - %USER% (ユーザのログイン名) - %PRODUCT_NAME% (警告を発生した製品名) - %PRODUCT_OID% (警告を発生した製品のOID) - %DESCRIPTION% (警告の内容) - %DATE% (警告の送信日、YYYY-MM-DD形式) - %TIME% (警告の

オプション	説明
	送品時間、HH:MM:SS+GMT形式) - %ALERT_NUMBER% (セッションの警告番号)

ウイルス定義ファイルの自動更新

詳細モード > 基本設定 > 自動更新 ページのオプション

オプション	説明
更新を有効にする	自動更新を有効/無効にします。無効の場合、自動更新エージェントは更新を自動的に確認しないようになります。[今すぐ確認] ボタンを利用して更新を手動で確認することは可能です。この設定はワークステーション向けの製品で設定できます。
ポリシーマネージャプロキシ	ポリシーマネージャプロキシの優先順序を表示します。ポリシーマネージャプロキシは、サーバの負荷を減らすためにポリシーマネージャのコンテンツをプロキシにキャッシュします。優先順序は、1) F-Secure自動更新エージェントがポリシーマネージャプロキシを通じてポリシーマネージャの更新サーバに接続します。2) ポリシーマネージャの更新サーバに直接接続します。3)ポリシーマネージャプロキシを通じてF-Secureの更新サーバに接続します。4) F-Secureの更新サーバに直接接続します。
HTTPプロキシを使用する	HTTPプロキシを使用します。Windows NT/2000/XP/2003を使用している場合、ブラウザのプロキシ設定はユーザに依存し、ユーザがログインしていないときには通常確認できません。自動更新エージェントから更新サーバまたはポリシーマネージャプロキシへの接続はHTTPプロキシを利用します。HTTPプロキシを利用できない場合、自動更新エージェントは直接接続しようとします。
HTTPプロキシアドレス	ユーザ定義のHTTPプロキシアドレス - [HTTPプロキシを使用する] が [ユーザ定義] に設定されている場合、有効になります。指定方法はhttp://[ユーザ[:パスワード]@]ホスト:ポート (例: http://myproxy.com、http://myproxy.com:8080、http://johndoe@myproxy.com、http://johndoe:secretpassword@myproxy.com)。ユーザ名とパスワードは任意のフィールドです。インタフェースで認証方法を設定することもできます。
仲介サーバのフェールオーバ時間 (分)	F-Secure自動更新エージェントが仲介サーバに接続できない場合、F-Secureの更新サーバに切り替わるまでの時間を指定します。
F-Secure更新サーバからの自動更新を有効にする	自動更新エージェントがF-Secureの更新サーバに接続できるか指定します。無効の場合、自動更新

オプション	説明
	エージェントはF-Secureの更新サーバに接続しないようになります。
アップデート後にスキャンする	ウイルス定義ファイルの更新後にローカルディスクをスキャンするか指定します。
リマインダの送信	ウイルス定義ファイルが指定期間より古くなったときに手動で更新することのリマインダをユーザに送るか指定します。
リマインダを送るために必要な経過日数	ウイルス定義ファイルを発行してからユーザに更新のリマインダを送るために必要な経過日数を指定します。

トラップ一覧

トラップ番号、深刻度、トラップの説明。

完全性検査

FSICトラップ一覧。

トラップ番号	深刻度	説明
710	セキュリティ警告	ベースラインがホストで作成されました。
711	セキュリティ警告	ベースラインの検査でエラーが発生しました。ベースラインに異常があるか、ベースラインの検査に使用したパスワードが間違っています。
730	セキュリティ警告	ファイルが完全性検査に失敗しました。
799	エラー	ベースラインをポリシーに保存できませんでした。

ポリシーマネージャ

FSAVPMDのトラップ一覧。Perlスクリプトから送信される警告はERRORレベルになります。

トラップ番号	深刻度	説明
50	情報	スキャンが開始されました。
51	情報	スキャンが終了しました。
60	情報	データベースの更新が開始されました。
61	情報	データベースの更新が終了しました。
100	セキュリティ警告	オンアクセスのウイルス警告
150	情報	処理が開始されました。
151	情報	処理が停止しました。
152	重大なエラー	処理がクラッシュしました。
153	重大なエラー	処理の開始が失敗しました。
158	情報	F-Secure Anti-Virus Linux Securityが起動しました。
159	情報	F-Secure Anti-Virus Linux Securityが停止しました。
170	セキュリティ警告	評価版の有効期限が過ぎました。

トラップ番号	深刻度	説明
171	情報	評価版
180	セキュリティ警告	ライセンスが切れました
181	情報	ライセンスが近日中に切れます
190	情報	製品の新しいバージョンを利用できます
200	セキュリティ警告	ウイルス警告
201	セキュリティ警告	ウイルス警告：駆除しました
202	セキュリティ警告	ウイルス警告：ファイルを削除しました
203	セキュリティ警告	ウイルス警告：ファイルの名前を変更しました
204	セキュリティ警告	ウイルス警告：駆除していません
205	セキュリティ警告	ウイルス警告：処理が失敗しました
206	セキュリティ警告	ウイルス警告：カスタムアクションを実行しました
207	セキュリティ警告	ウイルス警告：スキャンを停止しました
322	情報	ウイルス定義ファイルの更新を受信しました。
500	情報	ウイルス定義ファイルの完全性を確認しました。
999	情報	デバッグの出力

ウイルス定義ファイルの確認

DAASトラップ一覧

トラップ番号	深刻度	説明
506	警告	ウイルス定義ファイルの更新パッケージに追加ファイルが検出されました。
512	警告	パッケージが変更されました。
513	警告	目録ファイルが無効または見つかりません。
514	警告	目録ファイルの証明書が無効または見つかりません。
515	警告	ウイルス定義ファイルの更新は前回受信したものよりも古いものです。
516	警告	目録ファイルに一致する証明書がありません。
518	警告	F-Secure Corporationの証明書が無効または見つかりません。

トラップ番号	深刻度	説明
519	警告	ウイルス定義ファイルの発行元の証明書が無効また見つかりません。
520	警告	発行元の証明書の中で、目録ファイルの証明書と一致するものはありません。
521	警告	パッケージ内の証明書はF-Secure Corporationが発行したものではありません。
522	警告	ウイルス定義ファイルの更新が発行された際に、発行元の証明書が無効でした。
523	警告	パッケージ内の発行元の証明書は、データベースの更新を発行する権限がありません。
530	警告	パッケージ内の発行元の証明書は、データベースの更新が発行された際に無効でした。
531	警告	パッケージ内の発行元の証明書は、深刻な問題により無効になっています。
535	警告	取り消しファイルが無効または見つかりません。
550	警告	処理を完了するにはメモリが不足しています。
551	警告	処理中にファイル I/O エラーが発生しました。
552	警告	非対応のウイルス定義ファイル

DBTool

DBToolトラップ一覧。

トラップ番号	深刻度	説明
4	エラー	ファイルが見つかりません
308	エラー	ファイルを開くことができません
309	エラー	ファイルが暗号化されています
310	エラー	ファイルのスキャンを完了できませんでした
311	エラー	ファイルに書き込むことができません
323	エラー	ウイルス定義ファイルが無効です
324	エラー	ウイルス定義ファイルが無効です。完全性検査は失敗しました。

ファイアウォール

ファイアウォールデーモントラップの一覧。

トラップ番号	深刻度	説明
153	重大なエラー	処理の起動が失敗しました。
801	情報	ファイアウォールが有効になりました。
802	エラー	ファイアウォールが無効になりました。
803	エラー	ファイアウォールルールを設定できませんでした。
804	情報	ファイアウォールのルールが更新されました。

アンチウイルス

オンアクセススキャナのトラップ一覧。

トラップ番号	深刻度	説明
150	情報	処理が起動されました。
153	重大なエラー	処理の起動が失敗しました。
200	セキュリティ警告	ウイルス警告
201	セキュリティ警告	ウイルス警告 : 駆除しました
202	セキュリティ警告	ウイルス警告 : ファイルを削除しました
203	セキュリティ警告	ウイルス警告 : ファイルの名前を変更しました
205	セキュリティ警告	ウイルス警告 : 処理が失敗しました
220	セキュリティ警告	リスクウェア警告
221	セキュリティ警告	リスクウェア警告 : 駆除しました。
222	セキュリティ警告	リスクウェア警告 : ファイルを削除しました。
223	セキュリティ警告	リスクウェア警告 : ファイル名を変更しました。
225	セキュリティ警告	リスクウェア警告 : 処理が失敗しました。
301	エラー	スキャンエラー
309	エラー	ファイルが暗号化されています。
318	エラー	スキャンが中断されました。
600	セキュリティ警告	リアルタイム保護の重大なエラー。
700	セキュリティ警告	完全性検査の重大なエラー。

トラップ番号	深刻度	説明
720	セキュリティ警告	完全性検査のハッシュ計算が失敗しました。
721	セキュリティ警告	完全性検査のファイル属性が失敗しました。
730	セキュリティ警告	完全性検査のファイルが異常です。
731	セキュリティ警告	完全性検査が保護されているファイルに対する変更処理を防止しました。
733	セキュリティ警告	製品のバージョン9.10以降では使用されていません。
734	セキュリティ警告	製品のバージョン9.10以降では使用されていません。
735	セキュリティ警告	製品のバージョン9.10以降では使用されていません。
736	セキュリティ警告	カーネルが変更処理から保護されています。
741	セキュリティ警告	カーネルが変更されました。

サポート

このマニュアルで解決できないことがありましたら、インターネットまたは電話を通じてサポートを得られます。

F-Secure の診断ツールで作成される `fsdiag`レポートはシステムの重要な情報を含めています。システムに問題が発生した際にこの情報をF-Secureのサポートエンジニアに提供すると、問題が解決しやすくなります。`fsdiag`を実行したら、`fsdiag.tar.gz`のレポートファイルが現在のディレクトリに作成されます。

このレポートには、ご利用のF-Secure製品の情報およびオペレーティングシステムのログとシステムの設定が含まれます。場合によって、この情報は機密性があります。FSDIAGが収集したデータはローカルのディスクにのみ保存されます。

トラブルシューティングやF-Secureのサポート情報の詳細については、*http://support.f-secure.com*でご覧になれます。