F-Secure Internet Gatekeeper

目次

第 章
1

F-Secure インターネット ゲートキーパーの概要

トピック：

ネットワークのゲートウェイでセキュリティを保護する効率的で操作がシンプルなソリューション。

マルウェア (悪質なソフトウェア) はさまざまな方法でネットワークに侵入することができます。少し前まではメールを通じて感染する方法が最も一般的でしたが今では Web サイトに危険なプログラムやコンテンツが直接埋め込まれています。ユーザは、サイトにある悪質なコンテンツをダウンロードしたり、サイトにアクセスするだけで感染する可能性があります。このような悪質で危険なデータはセキュリティを脅かすだけではなく、個人と企業の生産性、法的責任の懸念、ネットワークの帯域幅などにも影響します。

システムとネットワークをインターネットを通じて広がる悪質なコンテンツから保護するために最も有効な方法は、ネットワークのゲートウェイでマルウェアを防ぐことです。F-Secureインターネット ゲートキーパは、社内サーバおよびエンドユーザのデスクトップに広がる前に受信するメール、Web データおよびファイル転送データをスキャンし、ウイルスや悪質なソフトウェアをブロックします

本製品は、企業の機密データを危険にさらし、ネットワーク帯域幅を浪費し、法的責任に関する懸念を高める可能性のあるマルウェアをブロックします。また、組織の生産性に影響を及ぼす可能性のある、業務に関係のない動画やオーディオ コンテンツなど、指定された種類のファイルを分別することもできます。インターネット ゲートキーパは、柔軟性が高く、導入が容易で、透過的なプロキシとして使用することもできます。

本製品は、企業ネットワークのニーズに応えるセキュリティソリューションで、高いコストパフォーマンスとシンプルな導入/管理機能を提供します。

1.1 機能

本製品の主な機能と特長

本製品は多様多種なネットワークをウイルスから保護します。

- 企業の内部ネットワーク
- ISP (プロバイダ/事業者) ネットワーク
- 企業内/ISP のすべてのコンピュータのネットワーク アクセスを監視する1台のコンピュータ
- ネットワーク内の他のコンピュータのリソースを使用しない
- 既存のネットワークにインストールと管理が簡単
- 大規模、小規模ネットワークおよび性能が低いコンピュータでも利用可能

Web ブラウジングとメールの監視

- HTTP
- FTP
- SMTP
- POP

シンプルなインストール

- ほぼすべてのLinux環境に対応
- 一台のコンピュータにすべての機能を凝縮
- rpmパッケージでインストール可能。rpmパッケージはRed Hat Linuxなどのディストリビューションに使用されているLinux Standard Baseに準拠。
- .tar.gzパッケージ でインストール可能 (Linuxの全ディストリビューションに対応)

シンプルな構成

- メールサーバの設定は不要
- ネットワークの設定は不要
- ユーザ別の設定変更は必要最低限のみ
- 製品の設定ファイルですべての構成が設定可能

認証機能

- POP before SMTP認証に対応
- 各種プロトコルのプロキシ認証に対応

  (HTTPプロキシ認証、SMTPプロキシ認証、POP/FTPユーザ制限)

  - プロキシ認証はPAMs (Pluggable Authentication Modules) で動作し、UNIXアカウント、LDAP、NIS、Radiusなどの認証方法と連携が可能
- IPアドレス、ホスト名、ドメイン名に応じたアクセス制御をすべてのプロトコルに設定可能
- SMTP受信ドメインに対するサードパーティ経由リレーの阻止
- メールサーバにある既存SMTP認証機能の使用
- メールサーバにある既存APOP機能の使用

ウイルス検出の通知

- 通知内容のカスタマイズ
- メッセージにUTF-8文字 (例: 日本語) の使用
- ウイルス検出時に管理者へメール通知

- 通知メールのヘッダと本文のカスタマイズ

柔軟な構成

- 透過プロキシ (HTTP、SMTP、POP、FTP) の使用
- ユーザ別にPOPサーバの選択
- HTTPプロトコルで送受信されるファイルに対するウイルススキャン。POSTよPUTメソッドに対応。
- 専用FTPクライアントの送受信に対応
- 親プロキシ設定によるマルチレベル接続に対応
- 親プロキシ設定 (リバースプロキシ) の使用により専用 Web サーバへの接続がすべて監視可能
- 任意のメールサーバへ接続が可能
- 同コンピュータ内で動作しているメールサーバがすべて使用可能
- SMTP受信とSMTP送信の個別設定

アンチウイルス

- 受賞歴と実績のあるF-Secureエンジンを搭載
- 既存のウイルスをほぼすべて処理できる性能
- Windows、DOS、Microsoft Office、VBS、Linux、その他の環境のウイルスに対応
- 複数のエンジン (FS-Engine (Hydra)、Aquarius) との連携で、未知のウイルスに対する迅速な対応
- 低い誤検知の数
- 各種アーカイブ (圧縮) 形式 (ZIP、ARJ、LZH、CAB、RAR、TAR、GZIP、BZIP2 / 6階層) に対応
- ウイルス定義ファイルの自動更新
- クラウドベースの検出サービスSecurity Cloud を使用し、安全なアプリケーションと Web サイトを特定しながらマルウェアや Web サイトの脆弱性に対する保護を提供します。

スパムブロック

- SMTPとPOPに対するスパム検出に対応
- 優先的ブラックリストとホワイトリストを通じてヘッダとメール本文をスキャンし、カスタムの条件を使用してスパムの検出
- スパム検出エンジンを搭載
- Realtime Black List (RBL) を利用して送信者のメールアドレスからスパムの検出
- SPAM URL Realtime Black List (SURBL) を利用してメール本文にあるスパムドメインURLを含むスパムの検出
- メールの整理を簡潔にするためにメールにカスタム文字の追加 ("[[SPAM]]" など)

ICAPサービスによるウイルススキャン

- ICAPサービスによるウイルススキャンに対応
- fsicapdデーモンがICAPプロトコルを実行 (RFC 3507 を参照)
- F-Secureテクノロジによるデータスキャン
- ICAPクライアントとして機能できるサードパーティHTTPプロキシとの連携

Web コンテンツ制御

- Security Cloud からサイトの評価を確認して危険な Web サイトに対する保護を提供
- HTTP と FTP 通信で指定したコンテンツ カテゴリをブロック (コンテンツは Security Cloud が確認)
- 信頼済みのサイトから Web コンテンツ制御を除外

その他の機能

- 拡張子、User-Agent、ファイルサイズなどによるファイルの通過・拒否設定が可能

- ActiveX スクリプト (JavaScript VBScript) のブロック機能
- squid互換ログによるアクセス統計処理が可能
- syslogなどへのログの外部出力が可能
- https (暗号化http) のプロキシ機能に対応。ただし、https (SSL) については、暗号化されているためウイルススキャンは行いません
- ウイルス検出通知メールにウイルス識別ヘッダ (X-Virus-Status: infected) を追加することにより、容易な振り分けが可能

第 章
2

導入

トピック：

ここでは、製品のネットワーク環境への導入とインストールを行う方法について説明します。

2.1 システム要件

最小および推奨のシステム要件については、製品のリリース ノートを参照してください

F-Secure Internet Gatekeeperは、以下のシステム要件を満たすコンピュータにインストールする必要があります。

- x86互換 2Ghz以上を推奨
- 512MB以上のRAM 1GB以上を推奨
- 5GB以上のの空きディスク容量 20GBを推奨
- インストールするファイルには少なくとも1GBの空きディスク容量が必要であり、実行中のシステムには一時ファイル、ログ、およびその他の同様のファイル用に多くの容量が必要です。

2.2 製品をインストールする

製品の導入とインストールに関連する説明

rpm パッケージまたは tar.gz パッケージを使用して製品をインストールします。

注： rpm パッケージを使用して製品をインストールすることを推奨します。

2.2.1 インストール前のチェックリスト

一部のLinuxディストリビューションやLinuxのインストールでは、F-Secure Internet Gatekeeperを正常にインストールする前に、特定のソフトウェアパッケージをインストールするか、回避策を適用する必要がある場合があります。

Debian 8.8には、壊れた`libpam-modules`パッケージ https://bugs.debian.org/851650 があります。次のコマンドを使用して、異なるmanページを強制的に上書きすることでインストールできます。

```
apt-get -o Dpkg::Options::="--force-overwrite" install libpam-modules: i386
```

RHEL 8.xおよびCentO S8.xには追加の依存関係があり、Internet Gatekeeper用に作成された別のSELinuxポリシーモジュールも必要です。詳細については、関連のヘルプトピックを参照してください。

以下のソフトウェアがオペレーティングシステムで使用可能である必要があります。

- Linux kernel 2.6 以降
- Perl 5.8以降
- Make
- 32ビットCおよびC++ランタイム環境。 64ビット環境に互換性ライブラリをインストールする方法については、OSのドキュメントを参照してください。
  - `glibc`
  - `libstdc++`
  - `libgcc1`
  - `zlib`
  - `libpam-modules` プロキシ認証にPAMを使用する場合
  - `libnsl` RHEL/CentOS 8にのみ必要
- `policycoreutils-python`パッケージを使用して、SELinuxが**Enforcing**モードに設定されている環境でログローテーションのサポートを有効にします。
- `zlib`ライブラリ

関連タスク

製品をRHEL8およびCentOS8にインストールするページ13

RHEL 8.xおよびCentO S8.xには追加の依存関係があり、Internet Gatekeeper用に作成された別のSELinuxポリシーモジュールも必要です。

2.2.2 rpm パッケージをインストールする

Red Hat Linux のディストリビューションを使用している場合、rpm パッケージを使用して製品をインストールしてください。

rpm パッケージを使用して製品をインストールするには

インストール パッケージをダブルクリックして、root 権限で次のコマンドを実行します:

```
# rpm -Uvh fsigk-XXX.i386.rpm
```

2.2.3 tar.gz パッケージをインストールする

rpm パッケージを使用できない場合には tar.gz パッケージを使用して本製品をインストールしてください。また、tar.gz パッケージを使用するとインストール時に特定のオプションを指定できます。

tar.gz パッケージを使用して製品をインストールするには

root 権限でコマンドラインから次のコマンドを実行します:

```
# tar -zxvf fsigk-XXX.tar.gz
# cd fsigk-XXX/
# make install
```


重要: インストールには `make install` コマンドを使用し、デフォルトのインストールにはインストール オプションを指定しないことを推奨します。

インストール オプションの一覧:

オプション	動作	説明
`prefix=[dir]`	インストール ディレクトリを指定します。	本製品をデフォルトのインストール ディレクトリ (`/opt/f-secure/fsigk`) にインストールすることを推奨します。
`suffix=[名前]`	実行可能ファイルと他のコマンド名 (fsigk) を区別するために接尾辞を追加します。	同じサーバに製品の複数のコピーをインストールした場合にこのオプションを使用してください。接尾辞は2文字以内である必要があります。
`lang=[ja|en|de|fr]`	本製品の表示言語を指定します。"ja" (日本)、"en" (英語)、 "de" (ドイツ語), and "fr" (フランス語) を指定できます。	インストール中に言語がを設定することを推奨します。言語の設定を指定せず、システムのタイムゾーンが JST または LANG 環境変数が "ja" で始まる場合、本製品は日本語でインストールされます。それ以外の場合にはインストール言語が英語になります。

オプション	動作	説明
`adminport=[num]`	Webコンソールのポート番号を指定します。	同じサーバに製品の複数のコピーをインストールした場合にこのオプションを使用してください。ポートを指定しない場合、デフォルトのポート9012が使用されます。

コマンドの例

製品を完全にインストールする場合、root 権限でコマンドラインから次のコマンドを実行します:

```
# make install
```

同じサーバに製品の別のコピーをインストールする場合、root権限でコマンドラインから次のコマンドを実行します:

```
# make prefix=/opt/f-secure/fsigk2 suffix=2 install
```

2.2.4 製品をRHEL8およびCentOS8にインストールする

RHEL 8.xおよびCentO S8.xには追加の依存関係があり、Internet Gatekeeper用に作成された別のSELinuxポリシーモジュールも必要です。

ホットフィックスをインストールするとき以降にSELinuxエラーが発生しないように、次の順序で製品をインストールします。

1. インストール前のチェックリストに記載されている依存関係をインストールします。
2. 次のコマンドを実行して、32ビットバージョンの `libnsl` レガシーバージョン をインストールします。これは、RHEL/CentOS8の追加要件です。

   ```
   dnf -y install libnsl.i686
   ```

3. 使用するインストール方法に応じて、`rpm`パッケージまたは`tar.gz`パッケージとして製品をインストールするための指示に従います。

   インストーラーが`policycoreutils-python`をインストールするように要求した場合は、メッセージを無視できます。

4. https://download.sp.f-secure.com/fsigk/rhel8/fsigk.ppから`fsigk.pp`ポリシーモジュールを取得し、ホストにアップロードします。
5. 次のコマンドを実行して、ポリシーモジュールをインストールし、インストールディレクトリを再帰的に再ラベル付けします。

   ```
   semodule -i ./fsigk.pp
   restorecon -FR /opt/f-secure/fsigk
   ```

6. 最新のF-SecureInternetGatekeeperホットフィックスをインストールしてください。

関連概念

インストール前のチェックリストページ11

一部のLinuxディストリビューションやLinuxのインストールでは、F-Secure Internet Gatekeeperを正常にインストールする前に、特定のソフトウェアパッケージをインストールするか、回避策を適用する必要がある場合があります。

関連タスク

rpm パッケージをインストールするページ12
Red Hat Linux のディストリビューションを使用している場合、rpm パッケージを使用して製品をインストールしてください。

tar.gz パッケージをインストールするページ12
rpm パッケージを使用できない場合には tar.gz パッケージを使用して本製品をインストールしてください。また、tar.gz パッケージを使用するとインストール時に特定のオプションを指定できます。

2.3 製品をアップグレードする

インストールされている製品のバージョンに応じて、次のいずれかの方法で製品をアップグレードしてください。

2.3.1 インターネット ゲートキーパ (国際版) のアップグレード

次のインストール方法で F-Secure インターネット ゲートキーパの国際版をアップグレードできます。

インターネット ゲートキーパ バージョン4.06 以降を使用している場合、アップグレードの際に旧バージョンをアンインストールする必要はありません。バージョン 4.06 以前を使用している場合、最新のバージョンをインストールする前に旧バージョンをアンインストールしてください。

2.3.2 インターネット ゲートキーパ (日本語版) のアップグレード

本製品の日本語版を使用している場合、次の方法で製品の新しい国際版をインストールできます。

rpm パッケージでアップグレードを行う

Red Hat Linux のディストリビューションを使用している場合、rpm パッケージを使用して製品をアップグレードしてください。

注： root 権限で次のコマンドを実行します。

注： `rpm` パッケージで製品をインストールすると、`fsikk.ini` の設定は工場出荷時のデフォルトにリセットされます。 以前の設定ファイルは `.rpmorig` 拡張子を使用するように名前が変更されているため、必要に応じてファイルを置き換えることができます。 以前の設定を保持するには、`tar` パッケージを使用して製品をアップグレードします。

rpm パッケージを使用して製品をアップグレードするには

1. 既存の構成/設定をバックアップします。

```
# cd /opt/f-secure/fsigk
# tar zcvf conf-bak.tgz conf/
# cp conf-bak.tgz <back up directory>
```

2. 製品の旧バージョンをアンインストールします。

```
# rpm -e virusgw
```

3. 新しいバージョンのためにシステムを用意します。

a) インストール ディレクトリを作成します。

```
# mkdir -p /opt/f-secure/fsigk
```

注： rpm パッケージを使用して製品をインストールする場合、デフォルトのインストール ディレクトリを使用する必要があります。

b) 以前の構成をインストール ディレクトリにコピーします。

```
# cd /opt/f-secure/fsigk
# cp <back up directory>/conf-bak.tgz /opt/f-secure/fsigk/
# tar zxvf conf-bak.tgz
```

c) 構成ファイルの名前を変更します。

```
# cd conf
# mv virusgw.ini fsigk.ini
```

4. 製品の新しいバージョンをインストールします。

```
#rpm -Uvh fsigk-xxx.i386.rpm
```

tar.gz パッケージでアップグレードを行う

rpmパッケージを使用できない場合、tar.gzパッケージを使用して製品をアップグレードしてください。

注： root 権限で次のコマンドを実行します。

tar.gz パッケージを使用して製品をアップグレードするには

1. 既存の構成/設定をバックアップします。

```
# cd <installation directory>
# tar zcvf conf-bak.tgz conf/
# cp conf-bak.tgz <back up directory>
```

2. 製品の旧バージョンをアンインストールします。

```
# cd <installation directory>
# make uninstall
# rm -rf <installation directory>
```

3. 新しいバージョンのためにシステムを用意します。

a) インストール ディレクトリを作成します。

```
# mkdir -p <installation directory>
```

b) 以前の構成をインストール ディレクトリにコピーします。

```
# cd <installation directory>
# cp <back up directory>/conf-bak.tgz <installation directory>/
# tar zxvf conf-bak.tgz
```

c) 構成ファイルの名前を変更します。

```
# cd conf
# mv virusgw.ini fsigk.ini
```

4. 製品の新しいバージョンをインストールします。

```
# tar zxvf fsigk-xxx.tar.gz
# cd fsigk-xxx
# make install prefix=<installation directory>
```

注： 製品をデフォルトのインストール ディレクトリ (/opt/f-secure/fsigk) にインストールする場合、インストール コマンドに接頭辞オプションを使用する必要はありません。

2.4 アンインストール

インストールに使用したパッケージ (rpm または tar.gz) に応じたアンインストールの説明に従ってください。

2.4.1 rpm パッケージをアンインストールする

ここでは、rpm パッケージでインストールした製品のアンインストール方法について説明します。

rpm パッケージをアンインストールするには

1. コマンドラインを開きます。
2. root 権限でコマンドラインから次のコマンドを実行します:

```
# rpm -e fsigk
```

インストールしたファイルと設定が削除され、サービスも停止されます。

2.4.2 tar.gz パッケージをアンインストールする

ここでは、tar.gz パッケージでインストールした製品のアンインストール方法について説明します。

tar.gz パッケージをアンインストールするには

1. コマンドラインを開きます。
2. root 権限でコマンドラインから次のコマンドを実行します:

```
# cd /opt/f-secure/fsigk
# make uninstall
# rm -rf /opt/f-secure/fsigk
```

インストールしたファイルと設定が削除され、サービスも停止されます。

第章

3

一般的な設定例

トピック：

インストールが完了したら、適切な場所に「インターネットゲートキーパ・サーバ」を設置し、必要に応じて設定を変更します。次に、クライアントマシンの設定を行います。

3.1 トラフィック スキャン

HTTP、SMTP、POP、およびFTP接続について、ウイルススキャンを行わない場合(通常)の接続例と、インターネットゲートキーパを設置してウイルススキャンを行う場合の接続例を示します。

3.1.1 HTTP接続

ウェブブラウザのトラフィックに対するウイルススキャンの仕組むについて説明します。

ウイルススキャンなし 通常、ウェブブラウザは、ウェブサーバに直接接続してページを取得します。

ウイルススキャンあり ウイルススキャンを行う場合は、インターネットゲートキーパをウェブサーバとクライアントの間に設置し、ウェブブラウザのプロキシサーバとします。ウェブブラウザは、インターネットゲートキーパを経由してウェブサーバに接続し、ウイルススキャンを行ったページを取得します。インターネットゲートキーパは、クライアントから要求されたURLに応じて適切なウェブサーバに接続します。

HTTP接続例

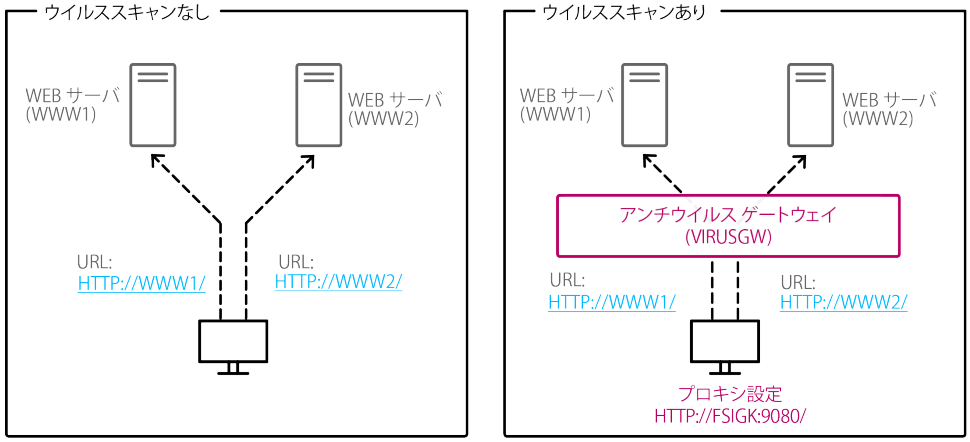


図1: HTTP接続の動作 (ウイルススキャンなし・ウイルススキャンあり)

3.1.2 SMTP接続

SMTPプロトコルのメールトラフィックに対するウイルススキャンの仕組むについて説明します。

ウイルススキャンなし 通常、メールクライアントは送信用のSMTPサーバを経由して、インターネット上のメールサーバにメールを送信します。

ウイルススキャンあり ウイルススキャンを行う場合、インターネットゲートキーパをクライアントとメールサーバの間に設置し、メールクライアントのSMTPサーバとします。クライアントはインターネットゲートキーパを経由して送信用のSMTPサーバに接続し、インターネット上のメールサーバにメールの送信を行います。インターネットゲートキーパは送信用メールサーバを経由してメールを送信します。

SMTP接続例

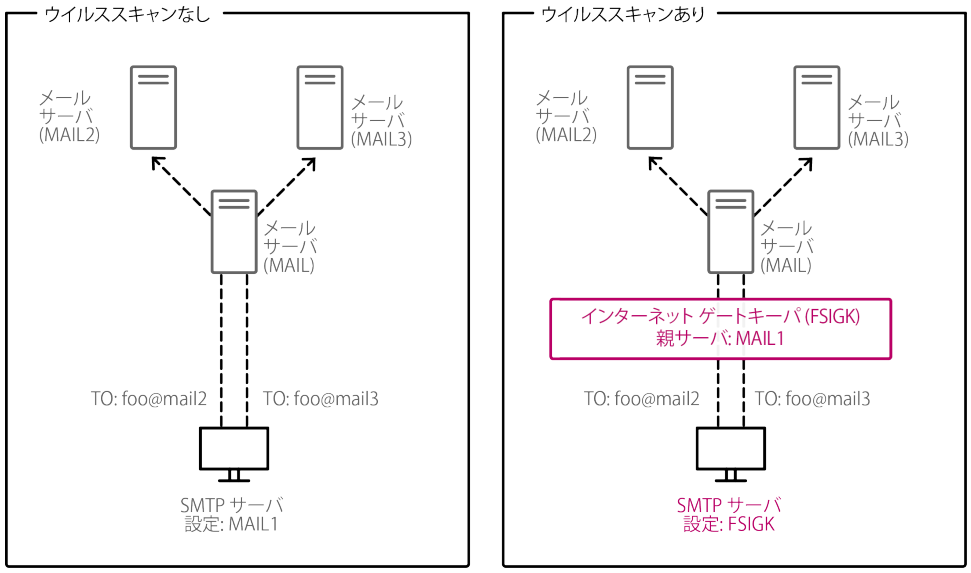


図 2 : SMTP接続の動作 (ウイルススキャンなし・ウイルススキャンあり)

3.1.3 POP接続

POPプロトコルのメールトラフィックに対するウイルススキャンの仕組むについて説明します。

ウイルススキャンなし 通常、メールクライアントは、メールサーバにPOPプロトコルで直接接続してメールを取得します。

ウイルススキャンあり ウイルススキャンを行う場合、インターネットゲートキーパをクライアントとメールサーバの間に設置し、メールクライアントのPOPサーバとします。クライアントはインターネットゲートキーパを経由してメールサーバと接続し、ウイルススキャンを行ったメールを取得します。インターネットゲートキーパは通常は設定された親サーバに接続しますが、POPユーザ名を「POPサーバのユーザ名@POPサーバ名」と指定することで、任意のPOPサーバに接続することができます。

POP接続例

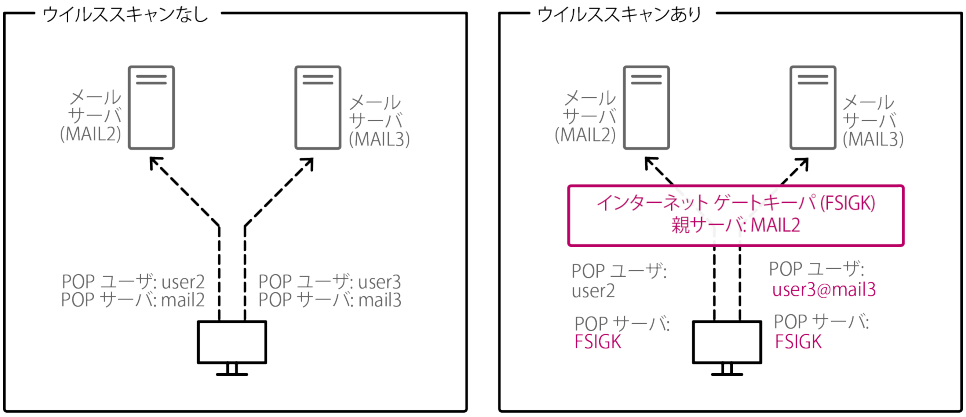


図 3 : POP接続の動作 (ウイルススキャンなし・ウイルススキャンあり)

3.1.4 FTP接続

FTPファイル転送に対するウイルススキャンの仕組むについて説明します。

ウイルススキャンなし 通常、FTP専用クライアントは、FTPサーバにFTPプロトコルで直接接続してファイルの送受信を行います。

ウイルススキャンあり ウイルススキャンを行う場合、インターネットゲートキーパをクライアントとメールサーバの間に設置し、FTPクライアントのプロキシサーバとします。クライアントはインターネットゲートキーパを経由してFTPサーバと接続し、ウイルススキャンを行ったファイルの送受信時を行います。FTPクライアントがプロキシサーバを設定できない場合、インターネットゲートキーパは通常は設定された親サーバに接続しますが、FTPユーザ名を「FTPサーバのユーザ名@FTPサーバ名」と指定することで、任意のFTPサーバに接続することができます。

FTP接続例

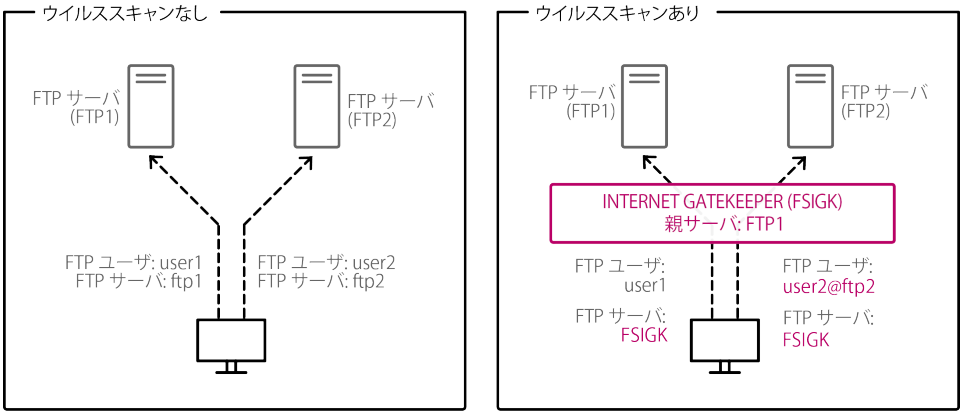


図 4 : FTP接続の動作 (ウイルススキャンなし・ウイルススキャンあり)

3.2 ネットワーク構成例

本製品は、ウェブサーバ・メールサーバとクライアント間のプロキシサーバとして設置します。ここでは、以下のような一般的なネットワーク構成に本製品を設置する場合を想定します。

注: 以下のネットワーク構成ではDMZネットワークに設置していますが、インターネットからの接続が不要な場合はDMZに設置する必要はありません。

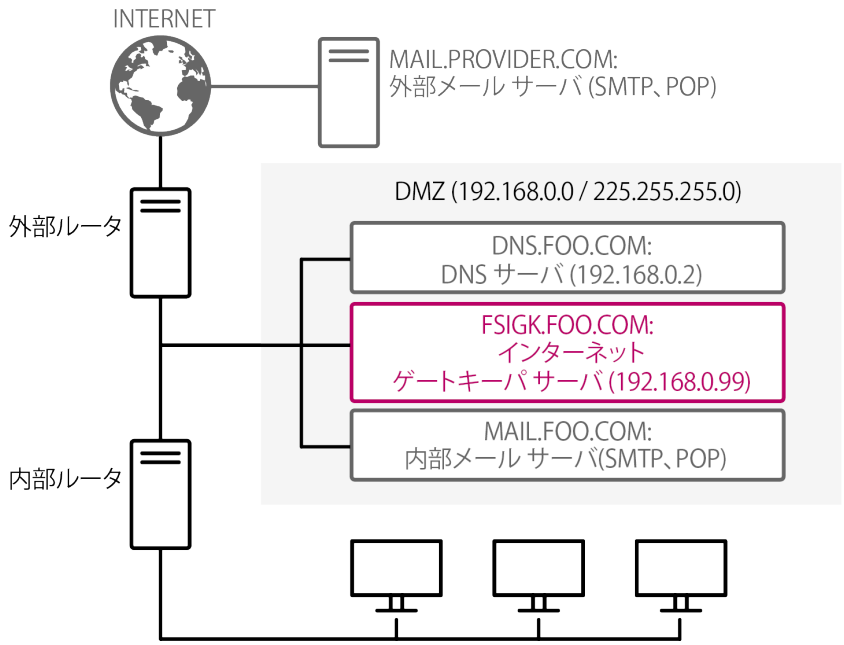


図 5 : DMZネットワーク内にある製品のネットワーク構成

3.3 インターネットゲートキーパ・サーバの設定例

本製品を使用してウイルススキャンを行うには、本製品をインストールしたインターネットゲートキーパ・サーバで以下の設定を行います。

3.3.1 ウェブ インターフェースをアクセスする

ウェブ インターフェースから製品の設定を変更できます。

ウェブ インターフェースにアクセスするには

1. Web ブラウザで次の URL を開きます: `http://<ホスト名>:9012/`
   <ホスト名> は製品がインストールされているサーバのドメイン名または IP アドレスを示します。
2. ユーザ名とパスワードを入力してログインします。
   デフォルトでは、ユーザ名は `admin`、パスワードは `admin` です。

   
   ヒント : ログイン ページにある地球儀アイコンをクリックすると言語を変更できます。ログインした後、[**言語を変更**] をクリックするとウェブ インタフェースの表示言語を選択できます。

   ログイン後、ウェブ コンソールの「**ホーム**」画面が開きます。

「**管理者パスワード**」ページでパスワードを変更します。

製品を登録する

製品の完全ライセンス版を使用するために購入したライセンス キーを入力します。

製品のインストール後、体験モードが有効になります。次の方法で製品をフルライセンス版にアップグレードできます。

1. ウェブ インターフェースを開きます。
2. [**ライセンス**] 設定を開きます。
3. 購入したライセンス キを [**ライセンス キー**] フィールドに入力します。

4. [**保存**] をクリックします。
5. フル ライセンスを適用するために製品を再起動します。

3.3.2 一般的な設定例

インストール後、ご使用のネットワーク環境に合わせてプロキシ設定を編集します。

製品を設定するには

1. ウェブ インターフェースを開きます。
2. Web トラフィックに対してマルウェア スキャンを行うために HTTP プロキシの設定を編集します。
   a) [**HTTP**] 設定を開きます。
   b) [**HTTP プロキシ**] を有効にします。
   c) [**プロキシ ポート**] が `9080` であることを確認します。
3. SMTP プロトコルを使用するメールに対してマルウェア スキャンを行うために SMTP プロキシの設定を編集します。
   a) [**SMTP**] 設定を開きます。
   [**一般**] 設定タブが開きます。
   b) [**SMTP プロキシ**] を有効にします。
   c) [**プロキシ ポート**] が `9025` であることを確認します。
   d) 「**グローバル設定**」タブを開きます。
   e) 使用する SMTP サーバの名前を [**親サーバのホスト名**] フィールドに設定します。
   例: `mail.example.com`
   f) 使用するメール サーバのポート番号を [**親サーバのポート番号**] フィールドに設定します。
   例: `25`
4. POP プロトコルを使用するメールに対してマルウェア スキャンを行うために POP プロキシの設定を編集します。
   a) [**POP**] 設定を開きます。
   [**一般**] 設定タブが開きます。
   b) [**POP プロキシ**] を有効にします。
   c) [**プロキシ ポート**] が `9110` であることを確認します。
   d) [**親サーバ**] をオンにします。
   e) 使用する POP サーバの名前を [**親サーバのホスト名**] フィールドに設定します。
   例: `mail.example.com`
   f) 使用するメール サーバのポート番号を [**親サーバのポート番号**] フィールドに設定します。
   例: `110`
5. FTP プロトコルを使用して転送されるファイルに対してマルウェア スキャンを行うために FTP プロキシの設定を編集します。
   a) [**FTP**] 設定を開きます。
   b) [**FTP プロキシ**] を有効にします。
   c) [**プロキシ ポート**] が `9021` であることを確認します。
6. 管理者の通知設定を編集します。
   a) [**全体設定**] を開きます。
   「**管理者の通知設定**」が開きます。
   b) 通知の送り先となるメール アドレスを [**メール アドレス**] フィールドで設定します。
   例: `fsigkadmin@example.com`
   c) 通知の送信元となるメール サーバを [**SMTP サーバのホスト名**] フィールドで設定します。
   例: `mail.example.com`

d) メール サーバのポート番号を [**ポート番号**] フィールドに設定します。
例: 25

新しい設定を適用するために製品を再起動します。

3.3.3 クライアントマシンの設定例

本製品を使用してウイルススキャンを行う場合、クライアント側では、ウェブブラウザのプロキシ設定およびメールクライアントのサーバ設定を変更します。

製品を使いはじめるためにご使用のネットワーク環境で次の設定を編集してください。

1. Web ブラウザの設定を編集します。
   a) Web ブラウザのプロキシ設定を開きます。
   b) 製品をインストールした場所のホスト名とポート番号をプロキシに設定します (例: `fsigk.example.com` と `9080`)。
2. メール クライアントの設定を編集します。
   a) メール クライアントのメール サーバ設定を開きます。
   b) 製品をインストールした場所のホスト名を内部および外部メールを対象としたSMTPサーバとPOPサーバに設定します (例: `fsigk.example.com`)。

注: POP ユーザ名を変更する必要はありません。

3.4 ネットワークアクセスを必要とするサービスのHTTPプロキシ使用

自動更新 (fsaua) スパム検出 (fsasd) などF-SecureサービスへのHTTPアクセスを必要とする機能は/opt/f-secure/fsigk/conf/fsigk.ini で設定できます。

`/opt/f-secure/fsigk/conf/fsigk.ini`設定ファイルにある次の設定を編集します。

use_proxy=[yes|no]	プロキシ利用の有無
http_proxy_host	プロキシサーバのホスト名
http_proxy_port	プロキシサーバのポート番号
http_proxyauth	プロキシ認証を利用の有無
http_proxyauth_user	プロキシ認証のユーザ名
http_proxyauth_pass	プロキシ認証のパスワード

注: Security Cloud (OrspService) は`/opt/f-secure/fsigk/conf/fsigk.ini`にある`orspservice_http_proxy`構成オプションを使用します。

3.5 製品の設定を確認する

プロキシの設定後、本製品が正常に動作していることを確認してください。

製品のインストール後、プロキシの設定を確認するには

1. EICAR web サイトからアンチマルウェアのテスト ファイルをダウンロードします: http://www.eicar.org/anti_virus_test_file.htm.
2. SMTP プロキシの設定を確認するために SMTP を使用し、EICAR テスト ファイルが添付されているメールを送信します。

3. POP プロキシの設定を確認するために POP を使用し、EICAR テスト ファイルが添付されているメールを送信します。
4. FTP プロキシの設定を確認するために FTP を使用し、EICAR テスト ファイルの送信と受信を行います。

製品が対象のトラフィック (データ) をスキャンしない場合、エラー ログを参照してください: `/opt/f-secure/fsigk/log/{http,smtp,pop,ftp}/error.log`.

第 章

4

製品を使用する

トピック：

製品が正しくインストールされ、正常に動作していることを確認したら、設定を環境に応じてカスタマイズできます

4.1 HTTP プロキシ

本製品を Web データに対してウイルスをスキャンする HTTP プロキシとして使用する場合、Web ブラウザは製品を通じて Web サーバに接続し、危険なコンテンツに対するスキャンの実行後に Web ページを受信します。

4.1.1 HTTP プロキシ設定を編集する

次の方法で HTTP プロキシの設定を編集できます。

1. ウェブ インターフェースで [**HTTP**] を開きます。
2. HTTP プロキシ設定を編集します。
3. 設定を変更したら、[**保存して更新**] をクリックします。

HTTPプロキシ設定

ここで説明される設定はウェブ インターフェースの「**HTTP**」ページにあります。

HTTP プロキシ
HTTP プロキシを有効または無効にします

プロキシ ポート
プロキシ サービスのポート番号を指定します。

標準ポート番号は9080です。

通常、ポート番号を1つ指定する必要があります。次の形式でポート番号、IP アドレス、インターフェース名を指定できます:
`[ADDRESS%EEE:PPP|ADDRESS:PPP|%EEE:PPP|PPP]`、`PPP`: ポート番号、`ADDRESS`: IPv4/IPv6 アドレス、`EEE`: インターフェース

例: `9080`、`1.2.3.4:9080`、`::1:9080` `%eth0:9080`、`1.2.3.4%eth0:9080`

IPv6 アドレス を使用するには、IPv6 構成を有効にする必要があります。

注: 単一のインターフェースまたは IP アドレスおよびポートを指定できます。複数のポートに応答するには、Linux の iptables 機能にある REDIRECT 設定を使用してください。たとえば、ポート9080とポート12345に応答する場合、9080をインバウンドポート番号に設定し、iptables を使用してポート12345をポート9080にリダイレクトします。

次のコマンドで iptables を設定できます:

```
# iptables -t nat -A PREROUTING -p tcp --dport 12345 -j REDIRECT
 --to-port 9080
```

次に iptables の構成を保存します。詳細な説明については、Linux ディストリビューションのマニュアルを参考にしてください。

ウイルス スキャン
ウイルス スキャンを有効または無効にします。

注: HTTPS (SSL) のデータは暗号化されているため、ウイルス スキャンの対象にはなりません。

POST/PUTメソッドで送信されたファイルをスキャン
HTTPプロトコルのPOSTおよびPUTメソッドを通じて送信されるファイルをスキャンするか指定します。

最大同時接続数
クライアントの最大同時接続数を指定します。指定したプロセス数がクライアントからの接続に応答します。

注： 最大同時接続数を増やすにはメモリがより多く必要になります。つのプロセスは500 KBほどのメモリを使用します。

ヒント： 初期値を200に設定し、パフォーマンスを監視することを推奨します。通常、この値は2000より低く設定されます。設定できる最大値は9999です。

感染・拒否されているコンテンツを検出した際の処理

ウイルス スキャンが感染したコンテンツまたはアクセスしたURLが[**拒否したサイト**]リストのパターンに一致した場合に管理者に通知を送信します。

メール アドレスとメール サーバは **全体設定** > **管理者の通知設定** 画面で指定できます。

`/opt/f-secure/fsigk/conf/` にある `template_admin*.txt` を編集することで通知メッセージを変更できます。`X-Admin-Notification-Id` フィールドが通知メッセージのヘッダに追加されます。

注： 通知メッセージを編集した場合、変更を適用するためにサービスを再起動する必要があります。

ウイルス スキャンから除外するコンテンツ

ユーザ エージェント (Web ブラウザ): ウイルススキャンから除外するWebブラウザを指定します。

ホスト名: ウイルススキャンから除外するホストを指定します。

ファイル名または拡張子: ファイル名または拡張子に応じてウイルススキャンから除外するファイルを指定します。

ファイルの最大サイズ (バイト): ファイルのサイズに応じてウイルススキャンから除外するファイルを指定します。

最大スキャン時間 (秒)

ファイルのスキャンに使用できる最大時間を指定します。

時間を超過するとウイルススキャンを停止できます。デフォルトは90秒です。0に設定するとスキャン時間に制限はありません。

注： 圧縮ファイルと大きなファイルは小さいファイルと比べ、スキャンにかかる時間が長くなります。

親サーバ

本製品がペアレント プロキシを通じて Web に接続する場合、この設定をオンにし、ペアレント プロキシのホスト名とサーバ ポートを設定してください。製品が Web に直接接続する場合、この設定を無効にしてください。

親サーバのホスト名

ペアレント プロキシ サーバのホスト名を指定します。

親サーバのポート番号

ペアレント プロキシ サーバのポート番号を指定します。

4.2 SMTP プロキシ

本製品をメールに対してウイルスをスキャンするSMTPプロキシとして使用する場合、メール クライアントは製品を通じてSMTPサーバに接続し、スパムと危険なコンテンツに対するスキャンの実行後にメールの受信と送信を行います。

4.2.1 SMTP プロキシ設定を編集する

次の方法でSMTPプロキシの設定を編集できます。

1. ウェブ インターフェースで[**SMTP**]を開きます。
2. 「**一般**」タブでSMTPプロキシの設定を編集します。

3. 「**全体設定**」タブで [**LAN 設定**] で指定されていないすべての接続に対する設定を変更します。
4. 「**LAN 設定**」タブで特定のネットワークまたはホストに該当する接続に対して異なる処理を指定します。
5. 「**SPAM フィルタの設定**」タブでスパムの検出設定を指定します。
6. 設定を変更したら、[**保存して更新**] をクリックします。

SMTP プロキシの一般設定

ここで説明される設定はウェブ インターフェースの**SMTP** > **一般**タブにあります。

SMTP プロキシ
SMTP プロキシを有効または無効にします

プロキシ ポート
プロキシ サービスのポート番号を指定します。

標準ポート番号は9025です。

通常、ポート番号を1つ指定する必要があります。次の形式でポート番号、IP アドレス、インターフェース名を指定できます:
`[ADDRESS%EEE:PPP|ADDRESS:PPP|%EEE:PPP|PPP]`、`PPP`: ポート番号、`ADDRESS`: IPv4/IPv6 アドレス、`EEE`: インターフェース

例: `9025`、`1.2.3.4:9025`、`::1:9025 %eth0:9025`、`1.2.3.4%eth0:9025`

IPv6 アドレス を使用するには、IPv6 構成を有効にする必要があります。

注: 単一のインターフェースまたは IP アドレスおよびポートを指定できます。複数のポートに応答するには、Linux の iptables 機能にある REDIRECT 設定を使用してください。たとえば、ポート9025とポート12345に応答する場合、9025をインバウンド ポート番号に設定し、iptables を使用してポート12345をポート9025にリダイレクトします。

次のコマンドで iptables を設定できます:

```
# iptables -t nat -A PREROUTING -p tcp --dport 12345 -j REDIRECT
 --to-port 9025
```

次に iptables の構成を保存します。詳細な説明については、Linux ディストリビューションのマニュアルを参考にしてください。

本製品は SMTPS (TCP/ポート番号465) などのような暗号化されたデータを直接受信することはできません (iptables でリダイレクトされている接続も含む)。暗号化されたデータをスキャンするには、SSL プロキシまたはアクセラレータを使用してデータを事前に復号化する必要があります。

ウイルス スキャン
ウイルス スキャンを有効または無効にします。

最大同時接続数
クライアントの最大同時接続数を指定します。指定したプロセス数がクライアントからの接続に応答します。

注: 最大同時接続数を増やすにはメモリがより多く必要になります。 つのプロセスは500 KBほどのメモリを使用します。

ヒント: 初期値を200に設定し、パフォーマンスを監視することを推奨します。通常、この値は2000より低く設定されます。設定できる最大値は9999です。

拒否するメール添付ファイル
暗号化および圧縮されたファイル: 暗号化された圧縮ファイル (ZIP、RAR) を含むメールをすべて拒否します。

ファイル名または拡張子

ウイルス スキャンから除外するコンテンツ

ファイル名または拡張子: ファイル名または拡張子に応じてウイルススキャンから除外するファイルを指定します。

最大スキャン時間(秒)

ファイルのスキャンに使用できる最大時間を指定します。

時間を超過するとウイルス スキャンを停止できます。デフォルトは90秒です。0に設定するとスキャン時間に制限はありません。

注: 圧縮ファイルと大きなファイルは小さいファイルと比べ、スキャンにかかる時間が長くなります。

SMTP プロキシの全体設定

ここで説明される設定はウェブ インターフェースの**SMTP** › **全体設定**タブにあります。

親サーバのホスト名

ペアレント プロキシ サーバのホスト名を指定します。

親サーバのポート番号

ペアレント プロキシ サーバのポート番号を指定します。

ウイルス検出時の処理

ウイルス検出時の処理を選択します。

許可: 感染したコンテンツを許可し、イベントをログします。

ブロックして送信者に通知: 感染したコンテンツをブロックして「`554 Infected by [ウイルス名]`」エラーを送信者に送ります。

削除: 感染したメールを通知なしで削除します。

メールを削除して送信先に通知: 感染したコンテンツを削除し、ウイルス検出メッセージをメッセージのあて先に送ります。

メールを削除して送信者に通知: 感染したコンテンツを削除し、ウイルス検出メッセージをメッセージの送信者に送ります。

管理者へメールで通知:

ウイルス スキャンが感染したコンテンツまたはアクセスした URL が [**拒否したサイト**] リストのパターンに一致した場合に管理者に通知を送信します。

メール アドレスとメール サーバは **全体設定** › **管理者の通知設定** 画面で指定できます。

`/opt/f-secure/fsigk/conf/` にある `template_admin*.txt` を編集することで通知メッセージを変更できます。`X-Admin-Notification-Id` フィールドが通知メッセージのヘッダに追加されます。

注: 通知メッセージを編集した場合、変更を適用するためにサービスを再起動する必要があります。

隔離保存: 隔離保存を有効または無効にします。

隔離保存ディレクトリを使用すると、本製品は感染したコンテンツとスパムメッセージを隔離保存ディレクトリに移動します。感染したメールとスパムメッセージは Maildir形式で保存されます。

隔離保存ディレクトリは **全体設定** › **ディレクトリ設定** の [**隔離保存ディレクトリ**] で指定できます。

SMTP プロキシの LAN 設定

ここで説明される設定はウェブ インターフェースの**SMTP** › **LAN 設定**タブにあります。

LAN 設定
LAN 接続に異なるウイルス スキャンを設定する場合にこの設定を有効にしてください。

LAN 内のホストとネットワーク
LAN 設定に該当するホストとネットワークを指定します。DNS 逆引きを使用する場合、次の形式を使用してください: <ホスト名>.<ドメイン名>.

親サーバ
本製品がペアレント プロキシを通じて Web に接続する場合、この設定をオンにし、ペアレント プロキシのホスト名とサーバポートを設定してください。製品が Web に直接接続する場合、この設定を無効にしてください。

親サーバのホスト名
ペアレント プロキシ サーバのホスト名を指定します。

親サーバのポート番号
ペアレント プロキシ サーバのポート番号を指定します。

ウイルス検出時の処理
ウイルス検出時の処理を選択します。

許可: 感染したコンテンツを許可し、イベントをログします。

ブロックして送信者に通知:感染したコンテンツをブロックして「`554 Infected by [ウイルス名]`」エラーを送信者に送ります。

削除: 感染したメールを通知なしで削除します。

メールを削除して送信先に通知:感染したコンテンツを削除し、ウイルス検出メッセージをメッセージのあて先に送ります。

メールを削除して送信者に通知:感染したコンテンツを削除し、ウイルス検出メッセージをメッセージの送信者に送ります。

管理者へメールで通知:

ウイルススキャンが感染したコンテンツまたはアクセスしたURLが[**拒否したサイト**]リストのパターンに一致した場合に管理者に通知を送信します。

メールアドレスとメールサーバは **全体設定** › **管理者の通知設定** 画面で指定できます。

`/opt/f-secure/fsigk/conf/` にある `template_admin*.txt` を編集することで通知メッセージを変更できます。`X-Admin-Notification-Id` フィールドが通知メッセージのヘッダに追加されます。

注: 通知メッセージを編集した場合、変更を適用するためにサービスを再起動する必要があります。

隔離保存: 隔離保存を有効または無効にします。

隔離保存ディレクトリを使用すると、本製品は感染したコンテンツとスパムメッセージを隔離保存ディレクトリに移動します。感染したメールとスパムメッセージはMaildir形式で保存されます。

隔離保存ディレクトリは **全体設定** › **ディレクトリ設定** の [**隔離保存ディレクトリ**] で指定できます。

SMTP プロキシのスパム フィルタ設定

ここで説明される設定はウェブ インターフェースの**SMTP** > **スパム フィルタ**タブにあります。

スパム フィルタリング

スパム フィルタを有効または無効にします。製品が `X-Spam-Status` フィールドを検出したスパム メッセージのヘッダに追加します。

ヒント: LAN設定を使用すると、受信するスパムをブロックして、送信メールをスパム フィルタから除外できます。

ウイルス検出時の処理

スパム メッセージ検出時の処理を選択します。

許可: スパム メッセージを許可します。メールクライアントは `X-Spam-Status` メッセージ ヘッダ フィールドを使用してスパムを分別できます。

メッセージの件名を変更:スパムメッセージの `Subject` フィールドを変更します。メッセージの件名に文字列を追加します。

注: 先頭の文字列は UTF-8 で暗号化されます。スパム メッセージの件名が他の文字エンコードの場合、メール クライアントによって正しく表示されない場合があります。

削除: スパム メールを削除します。

ヒント: スパムとして間違って認識されたメールが不意に削除されることを防ぐため、ゲートウェイでメールを削除しないでください。スパム メッセージを許可して、メール クライアントでスパムを分別するように設定してください。

管理者へメールで通知: スパム フィルタがスパムを検出した際に検出メッセージを管理者に送ります。

メール アドレスとメール サーバは **全体設定** > **管理者の通知設定** 画面で指定できます。

`/opt/f-secure/fsigk/conf/` にある `template_admin*.txt` を編集することで通知メッセージを変更できます。`X-Admin-Notification-Id` フィールドが通知メッセージのヘッダに追加されます。

注: 通知メッセージを編集した場合、変更を適用するためにサービスを再起動する必要があります。

隔離保存: 隔離保存を有効または無効にします。

隔離保存ディレクトリを使用すると、本製品は感染したコンテンツとスパムメッセージを隔離保存ディレクトリに移動します。感染したメールとスパムメッセージはMaildir形式で保存されます。

隔離保存ディレクトリは **全体設定** > **ディレクトリ設定** の [**隔離保存ディレクトリ**] で指定できます。

4.3 POP プロキシ

本製品をメールに対してウイルスをスキャンするPOPプロキシとして使用する場合、メールクライアントは製品を通じてメールサーバに接続し、スパムと危険なコンテンツに対するスキャンの実行後にメールを受信します。

4.3.1 POP プロキシ設定を編集する

次の方法で POP プロキシの設定を編集できます。

1. ウェブ インターフェースで [**POP**] を開きます。

2. 「**一般**」タブで POP プロキシの設定を編集します。
3. 「**SPAM フィルタの設定**」タブでスパムの検出設定を指定します。
4. 設定を変更したら、[**保存して更新**] をクリックします。

POP プロキシ設定

ここで説明される設定はウェブ インターフェースの**POP** > **一般**タブにあります。

POP プロキシ POP プロキシを有効または無効にします

プロキシ ポート プロキシ サービスのポート番号を指定します。

標準ポート番号は9110です。

通常、ポート番号を1つ指定する必要があります。次の形式でポート番号、IP アドレス、インターフェース名を指定できます:
`[ADDRESS%EEE:PPP|ADDRESS:PPP|%EEE:PPP|PPP]`、`PPP`: ポート番号、`ADDRESS`: IPv4/IPv6 アドレス、`EEE`: インターフェース

例: `9110`、`1.2.3.4:9110`、`::1:9110 %eth0:9110`、`1.2.3.4%eth0:9110`

IPv6 アドレス を使用するには、IPv6 構成を有効にする必要があります。

注: 単一のインターフェースまたは IP アドレスおよびポートを指定できます。複数のポートに応答するには、Linux の iptables 機能にある REDIRECT 設定を使用してください。たとえば、ポート9110とポート12345に応答する場合、9110をインバウンド ポート番号に設定し、iptables を使用してポート12345をポート9110にリダイレクトします。

次のコマンドで iptables を設定できます:

```
# iptables -t nat -A PREROUTING -p tcp --dport 12345 -j REDIRECT
--to-port 9110
```

次に iptables の構成を保存します。詳細な説明については、Linux ディストリビューションのマニュアルを参考にしてください。

本製品は SMTPS (TCP/ポート番号465) などのような暗号化されたデータを直接受信することはできません (iptables でリダイレクトされている接続も含む)。暗号化されたデータをスキャンするには、SSL プロキシまたはアクセラレータを使用してデータを事前に復号化する必要があります。

ウイルス スキャン ウイルス スキャンを有効または無効にします。

最大同時接続数 クライアントの最大同時接続数を指定します。指定したプロセス数がクライアントからの接続に応答します。

注: 最大同時接続数を増やすにはメモリがより多く必要になります。 つのプロセスは500 KBほどのメモリを使用します。

ヒント: 初期値を200に設定し、パフォーマンスを監視することを推奨します。通常、この値は2000より低く設定されます。設定できる最大値は9999です。

ウイルス検出時の処理 ウイルス検出時の処理を選択します。

注: POP プロトコルは特定のユーザがメールを受信することを完全にブロックできません。

削除: 感染したメールをウイルス検出のメッセージに置換します。また、メッセージを削除しなくても感染したメールのヘッダに`X-Virus-Status`フィールドが追加されます。

管理者へメールで通知:

ウイルス スキャンが感染したコンテンツまたはアクセスしたURLが[**拒否したサイト**]リストのパターンに一致した場合に管理者に通知を送信します。

メール アドレスとメール サーバは**全体設定**›**管理者の通知設定**画面で指定できます。

`/opt/f-secure/fsigk/conf/`にある`template_admin*.txt`を編集することで通知メッセージを変更できます。`X-Admin-Notification-Id`フィールドが通知メッセージのヘッダに追加されます。

注: 通知メッセージを編集した場合、変更を適用するためにサービスを再起動する必要があります。

隔離保存: 隔離保存を有効または無効にします。

隔離保存ディレクトリを使用すると、本製品は感染したコンテンツとスパムメッセージを隔離保存ディレクトリに移動します。感染したメールとスパムメッセージはMaildir形式で保存されます。

隔離保存ディレクトリは**全体設定**›**ディレクトリ設定**の[**隔離保存ディレクトリ**]で指定できます。

ウイルス スキャンから除外するコンテンツ

ファイル名または拡張子: ファイル名または拡張子に応じてウイルススキャンから除外するファイルを指定します。

最大スキャン時間(秒)

ファイルのスキャンに使用できる最大時間を指定します。

時間を超過するとウイルス スキャンを停止できます。デフォルトは90秒です。0に設定するとスキャン時間に制限はありません。

注: 圧縮ファイルと大きなファイルは小さいファイルと比べ、スキャンにかかる時間が長くなります。

親サーバ

本製品がペアレント プロキシを通じてWebに接続する場合、この設定をオンにし、ペアレント プロキシのホスト名とサーバ ポートを設定してください。製品がWebに直接接続する場合、この設定を無効にしてください。

注: 製品は通常、指定の親サーバに接続しますが、任意のFTPサーバへの接続を指定することが可能です。その場合にはPOPユーザ名を次の形式で指定してください: `<POP サーバのユーザ名>@<POP サーバ名>`.

親サーバのホスト名

ペアレント プロキシ サーバのホスト名を指定します。

親サーバのポート番号

ペアレント プロキシ サーバのポート番号を指定します。

POP プロキシのスパム フィルタ設定

ここで説明される設定はウェブ インターフェースの**POP**›**スパム フィルタ**タブにあります。

スパム フィルタリング

スパム フィルタを有効または無効にします。製品が`X-Spam-Status`フィールドを検出したスパム メッセージのヘッダに追加します。

ウイルス検出時の処理 スパム メッセージ検出時の処理を選択します。

> **注：** POP プロトコルは特定のユーザがメールを受信することを完全にブロックできません。メールクライアントでメッセージの件名の接頭辞を使用してスパムを分別してください。

許可: スパム メッセージを許可します。メールクライアントは `X-Spam-Status` メッセージ ヘッダ フィールドを使用してスパムを分別できます。

メッセージの件名を変更: スパムメッセージの `Subject` フィールドを変更します。メッセージの件名に文字列を追加します。

> **注：** 先頭の文字列は UTF-8 で暗号化されます。スパム メッセージの件名が他の文字エンコードの場合、メールクライアントによって正しく表示されない場合があります。

管理者へメールで通知: スパムフィルタがスパムを検出した際に検出メッセージを管理者に送ります。

メール アドレスとメール サーバは **全体設定** > **管理者の通知設定** 画面で指定できます。

`/opt/f-secure/fsigk/conf/` にある `template_admin*.txt` を編集することで通知メッセージを変更できます。`X-Admin-Notification-Id` フィールドが通知メッセージのヘッダに追加されます。

> **注：** 通知メッセージを編集した場合、変更を適用するためにサービスを再起動する必要があります。

隔離保存: 隔離保存を有効または無効にします。

隔離保存ディレクトリを使用すると、本製品は感染したコンテンツとスパムメッセージを隔離保存ディレクトリに移動します。感染したメールとスパムメッセージは Maildir 形式で保存されます。

隔離保存ディレクトリは **全体設定** > **ディレクトリ設定** の [**隔離保存ディレクトリ**] で指定できます。

4.4 FTP プロキシ

本製品をファイル転送に対してウイルスをスキャンする FTP プロキシとして使用する場合、クライアントは製品を通じて FTP サーバに接続します。危険なコンテンツに対するスキャンの実行後にクライアントはファイルの受信と送信を行うことができます。

4.4.1 FTP プロキシ設定を編集する

次の方法で FTP プロキシの設定を編集できます。

1. ウェブ インターフェースで [**FTP**] を開きます。
2. 「**一般**」タブで POP プロキシの設定を編集します。
3. 設定を変更したら、[**保存して更新**] をクリックします。

FTP プロキシ設定

ここで説明される設定はウェブ インターフェースの **FTP** > **一般 タブ** にあります。

FTP プロキシ FTP プロキシを有効または無効にします

プロキシ ポート プロキシ サービスのポート番号を指定します。

標準ポート番号は9021です。

通常、ポート番号を1つ指定する必要があります。次の形式でポート番号、IPアドレス、インターフェース名を指定できます:
`[ADDRESS%EEE:PPP|ADDRESS:PPP|%EEE:PPP|PPP]`、`PPP`: ポート番号、`ADDRESS`: IPv4/IPv6 アドレス、`EEE`: インターフェース

例: `9021`、`1.2.3.4:9021`、`::1:9021 %eth0:9021`、`1.2.3.4%eth0:9021`

IPv6 アドレス を使用するには、IPv6 構成を有効にする必要があります。

注: 単一のインターフェースまたはIPアドレスおよびポートを指定できます。複数のポートに応答するには、Linuxのiptables機能にあるREDIRECT設定を使用してください。たとえば、ポート9021とポート12345に応答する場合、9021をインバウンド ポート番号に設定し、iptables を使用してポート12345をポート9021にリダイレクトします。

次のコマンドで iptables を設定できます:

```
# iptables -t nat -A PREROUTING -p tcp --dport 12345 -j REDIRECT
--to-port 9021
```

次に iptables の構成を保存します。詳細な説明については、Linux ディストリビューションのマニュアルを参考にしてください。

ウイルス スキャン ウイルス スキャンを有効または無効にします。

最大同時接続数 クライアントの最大同時接続数を指定します。指定したプロセス数がクライアントからの接続に応答します。

注: 最大同時接続数を増やすにはメモリがより多く必要になります。 つのプロセスは500 KBほどのメモリを使用します。

ヒント: 初期値を200に設定し、パフォーマンスを監視することを推奨します。通常、この値は2000より低く設定されます。設定できる最大値は9999です。

ウイルス検出時の処理 ウイルス検出時の処理を選択します。

削除: 感染したメールを通知なしで削除します。

管理者へメールで通知:

ウイルススキャンが感染したコンテンツまたはアクセスしたURLが[**拒否したサイト**]リストのパターンに一致した場合に管理者に通知を送信します。

メールアドレスとメールサーバは **全体設定** > **管理者の通知設定** 画面で指定できます。

`/opt/f-secure/fsigk/conf/` にある `template_admin*.txt` を編集することで通知メッセージを変更できます。`X-Admin-Notification-Id` フィールドが通知メッセージのヘッダに追加されます。

注: 通知メッセージを編集した場合、変更を適用するためにサービスを再起動する必要があります。

隔離保存: 隔離保存を有効または無効にします。

隔離保存ディレクトリを使用すると、本製品は感染したコンテンツとスパムメッセージを隔離保存ディレクトリに移動します。感染したメールとスパムメッセージはMaildir形式で保存されます。

隔離保存ディレクトリは **全体設定** > **ディレクトリ設定** の [**隔離保存ディレクトリ**] で指定できます。

ウイルス スキャンから除外するコンテンツ

ホスト名: ウイルススキャンから除外するホストを指定します。

ファイル名または拡張子: ファイル名または拡張子に応じてウイルススキャンから除外するファイルを指定します。

ファイルの最大サイズ (バイト): ファイルのサイズに応じてウイルススキャンから除外するファイルを指定します。

最大スキャン時間 (秒)

ファイルのスキャンに使用できる最大時間を指定します。

時間を超過するとウイルス スキャンを停止できます。デフォルトは90秒です。0 に設定するとスキャン時間に制限はありません。

注: 圧縮ファイルと大きなファイルは小さいファイルと比べ、スキャンにかかる時間が長くなります。

親サーバ

本製品がペアレント プロキシを通じて Web に接続する場合、この設定をオンにし、ペアレントプロキシのホスト名とサーバポートを設定してください。製品が Web に直接接続する場合、この設定を無効にしてください。

注: 製品は通常、指定の親サーバに接続しますが、任意の FTP サーバへの接続を指定することが可能です。その場合には FTP ユーザ名を次の形式で指定してください: `<FTP サーバのユーザ名>@<FTP サーバ名>`.

親サーバのホスト名

ペアレント プロキシ サーバのホスト名を指定します。

親サーバのポート番号

ペアレント プロキシ サーバのポート番号を指定します。

4.5 ICAP サービス

ICAP (Internet Content Adaptation Protocol) はウイルス スキャンを透過プロキシ サーバに導入するために使用されます。

ICAP デーモンは ICAP プロトコルの REQMOD、RESPMOD、OPTIONS メソッドを導入します。

REQMOD または RESPMOD要求が包含されているHTTPボディを含めている場合、ウイルス スキャンが実行されます。危険なコンテンツが検出された場合、コンテンツがブロックされたことを示すWebページが代わりに表示されます。

4.5.1 ICAP サービスの設定を編集する

次の方法で ICAP サービスの設定を編集できます。

ICAP サービスは fsicapd がシステムで実行していることを必要とします。

1. ウェブ インターフェースで [**ICAP**] を開きます。
2. 「**一般**」タブで ICAP プロキシの設定を編集します。
3. 設定を変更したら、[**保存して更新**] をクリックします。

ICAP サービスの一般設定

ここで説明される設定はウェブ インターフェースの**ICAP** > **一般**タブにあります。

ICAP サービス
ICAP サービスのウイルス スキャンを有効または無効にします。デフォルトでは ICAP サービスはポート1344を通じて ICAP要求に応答します。デーモンに要求を送信する ICAP サービスを使用するプロキシを設定します。

バインド アドレス
ICAP デーモンがバインドするネットワーク アドレスまたはホスト名を指定します。

デフォルトではセキュリティの強化のためにデーモンはローカルインターフェース (127.0.0.1) にのみバインドします。0.0.0.0 を指定すると、デーモンをすべてのアドレスにバインドできます。

バインド ポート
ICAP サービスが応答するポート番号を指定します。デフォルトは1344です。

最大同時接続数
ICAPデーモンの最大接続数を指定します。上限に達した場合、新しいクライアントにはステータス コード503 (オーバーロードを示す) を持つ ICAP 応答が表示されます。デフォルトは500です。

注:

最大接続数を変更した場合、OSレベルで開けるファイルの制限を調整する必要があるかもしれません。制限により、`fsicapd` が起動しない場合、`/opt/f-secure/fsigk/log/fsicapd/fsicapd.log`のログファイルを開き、必要な最小数を確認してください: `RLIMIT_NOFILE を必要な値に調整できません。終了します。fsicapd のハードリミットが1300以上であることを確認してください。`

制限を上げるためには `/etc/security/limits.conf` にある次の行を変更・追加します:

```
root soft nofile 1024
root hard nofile 4096
```

変更を適用するために一度ログアウトして再度ログインします。

最大スキャン時間 (秒)
ファイルのスキャンに使用できる最大時間を指定します。

時間を超過するとウイルス スキャンを停止できます。デフォルトは90秒です。0 に設定するとスキャン時間に制限はありません。

注: 圧縮ファイルと大きなファイルは小さいファイルと比べ、スキャンにかかる時間が長くなります。

接続タイムアウト (秒)
接続をタイムアウトする値を指定します。タイムアウトの前にICAP要求が完了していない場合、クライアントとの接続が切断されます。デフォルトは600秒です。

4.5.2 EMC Isilon スケールアウト ストレージ サポート

ICAP デーモンは EMC Isilon スケールアウト ストレージ プラットフォーム (OneFS OS バージョン 8.0.0 以降で動作) 上でアンチウイルス サービスとして利用できます。

EMC Isilon スケールアウト ストレージ サポートを有効にするには

1. ICAP サービスを有効にするには `0.0.0.0` を指定するか、パブリック ネットワーク アドレスまたはサービスのホスト名をバインド アドレスとして指定し、外部ホストがサービスに接続できるようにします。

2. ICAP サーバをアンチウイルス サーバとして使用するためには OneFS システムを設定してください。詳細については、CLI または EMC から提供されている Web 管理者ガイドを参照してください。

4.6 全体設定

全体設定を編集すると、管理者のメールアドレス、作業ディレクトリの場所、隔離保存ディレクトリ、およびすべてのスパム フィルタに適用する設定を指定できます。

4.6.1 グローバルの設定を編集する

次の方法でグローバルの設定を編集できます。

1. ウェブ インターフェースで [**全体設定**] を選択します。
2. 「**Web コンテンツ制御**」タブの設定を変更するとブロック対象のコンテンツ カテゴリおよび信頼済み、拒否するサイトを指定できます。
3. 「**管理者の通知設定**」タブで管理者のメール アドレスと通知を送るメール サーバを指定します。
4. 「**ディレクトリの設定**」タブで一時保存ファイルと隔離保存コンテンツの保存場所を変更します。
5. 「**スパム フィルタの設定**」タブで SMTP と POP プロキシを対象としたスパム フィルタの設定を変更します。
6. 「**グローバルのカスタム スパム フィルタ設定**」タブで新しいスパムのフィルタリング設定を追加できます。
7. 設定を変更したら、[**保存して更新**] をクリックします。

グローバル Web コンテンツの制御設定

ここで説明される設定はウェブ インターフェースの **全体設定** > **Web コンテンツ制御の設定** タブにあります。

Web コンテンツ制御は Security Cloud にある F-Secure の評価分析システムを使用して Web サイトを分類化し、危険なコンテンツを含むサイトをブロックします。Web コンテンツを使用して不適切なコンテンツを含む Web サイト/ページのアクセスをブロックすることもできます。

Web コンテンツ制御	Web コンテンツ制御を有効/無効にします。 デフォルトでは Web コンテンツ制御は有効です。
拒否したサイト カテゴリ	ブロックするコンテンツ制御カテゴリを選択します。
信頼済みのサイト	Web コンテンツ制御がブロックしない Web サイトを指定します。特定のサイトにはウイルス スキャンや ICAP リクエストは実行されます。
拒否したサイト	アクセスを拒否する Web サイトを指定します。

信頼済み/拒否するサイトに必要な構文

- すべてのエントリにはプロトコル名を含む完全なURL(例:`http://`、`https://`、`ftp://`)をが必要とされます。
- エントリは大小文字を区別しません。
- エントリにはワイルドカード (* と ?) を使用できます。
  - ? は常に任意の1文字と一致します。
  - ホスト名では * は0以上の文字と一致します。
  - パスの場合、* は / 文字で区切られているセグメントと一致します。

注： URL の一部にクエリ文字列を追加する場合、最初のはてな マーク (?) の前にバックスラッシュ (/) を付ける必要があります。

例: `http://example.com/path\?parameter=value`

- # で始まる行 (先頭文字が空白以外) はコメントとして扱われます。
- ポート番号、プロトコル、認証情報 (ユーザ名とパスワード) は URL の一致には利用されません。
- URL の一致にはパスのコンポーネントは利用されます。HTTPS リクエストの場合、ホスト名と関連するパスが暗号化されます。
- エントリが先頭文字の場合、URL と同じパターンおよび最初の不一致文字が / または ? である場合、URL と一致するとみなされます。

注： エントリの最後の文字が / である場合、エントリは接頭辞として使用されません。

たとえば、`http://example.com/trusted-path/` を信頼済みのリストに追加した場合、`http://example.com/trusted-path/another_path` の 最初の不一致文字が / ではないため、信頼済みとしてみなされません。

注： エントリの最後の文字が * の場合、エントリは接頭辞として使用されず、1つの URL パスにのみ一致します。

たとえば、`http://example.com/trusted-path/*` を信頼済みのリストに追加した場合、`http://example.com/trusted-path/another_path` は信頼済みとしてみなされ、`http://example.com/trusted-path/another_path/yet_another_path` は信頼済みとしてみなされません。

Web コンテンツ カテゴリ

以下のカテゴリを指定することで F-Secure Network Reputation Service (NRS) コンテンツ分析の結果に応じて Web サイトをブロックできます。

注： ini ファイルで使用されているカテゴリ名は括弧で区切られています。

中絶 (abortion)	中絶、中絶手術を行う病院やクリニックなど中絶の一般的な情報を含むWeb サイト。例: 中絶反対派や賛成派のインターネット掲示板。
広告 (adserving)	Flash、テキスト、動画や画像ファイルなどの広告コンテンツをユーザに誘導する Web リンク。
成人 (adult)	成人向けなページや性的な要素があるページ。例:アダルトグッズショップや性的描写。
お酒とタバコ (alcohol and tobacco)	お酒とたばこ製品、および製造者、製造所、ブドウ園、醸造所などを紹介する Web サイト。例: ビールの祭り (ビアガーデンなど) を紹介するサイトやバーやナイトクラブの Web サイトなど。
アノニマイザ (anonymizers)	ネットワークのフィルタを回避する方法を説明する Web サイト、Web ベースの翻訳サイトを含む。例: 公開プロキシの一覧を記載しているサイト。
オークション (auctions)	オンライン オークションなど、ユーザがインターネットで製品やサービスを売買できる Web サイト。製品やサービスの取引が実際には別の場所で行われるサイトも含まれる。
バンキング (banking)	銀行や金融機関の Web サイト。投資銀行や証券取引、為替取引に関するサイトを含む。

ブログ (blogs)	ニュース、動画、写真などに関する情報を発信・共有できるインターネットのブログサイト。ブログは個人が情報を発信するためのものであるため、トピックやコンテンツが大きく異なることがある。
チャット (chat)	オンライン ポータルやメッセンジャーなど、ユーザがパソコンからテキスト、音声、動画を通じてチャットできるサイト。例:Webベースのチャットとインスタント メッセージ アプリケーション、チャット サイト。
出会い系 (dating)	出会い系の Web サイト。例: 出会い系サイトや結婚相談所サイト。
麻薬 (drugs)	麻薬の使用を推奨するサイト。例:違法薬物の購入、栽培、販売に関する情報を提供するサイト。
芸能 (entertainment)	テレビ番組、書籍、漫画、映画、画廊など、芸能界に関する Web サイト。例: テレビやラジオ番組のガイドや音楽/テレビ/映画のレビュー サイト。
ギャンブル (gambling)	ユーザが実際にお金や電子マネーなどをインターネットで賭けることができるWebサイト。例:オンラインギャンブル、宝くじサイトやインターネットおよび実世界のギャンブルに関する情報を含むブログ/掲示板。
ゲーム (games)	ユーザがゲームのプレイ、ダウンロード、購入を行えるサイトやオンライン ゲームの Web サイト。
ハッキング (hacking)	コンピュータのシステムやネットワークへの侵入に関する情報を説明する Web サイト。例: ハッキング ガイドやツールを紹介/含むサイト。
憎悪表現 (hate)	宗教、人種、国籍、性別、年齢、障害、性的指向などに対して差別を行っているWebサイト。例: 人権侵害、動物虐待などに関する情報や暴行を想起させるサイト。
就活 (job search)	求人サイトなど仕事情報を掲載しているサイト。例:キャリアに特化した検索エンジン、ネットワーキング グループ。
支払いサービス (paymentservice)	クレジットカードなどのショッピングサイト、銀行あるいはその他の金融サービス間の支払い処理向け Web サイト。一般的な支払いに使用されるサイトが含まれる。
詐欺 (scam)	オンライン調査、クイズもしくは同類のものに記入後にユーザを賞品で誘導しようとするWebサイト。例:賞品を配っている大企業と提携していると思わせるようなサイト。
ショッピング (shopping)	オンライン ショッピング向け商品カタログを掲載しており、ユーザがオンラインで商品やサービスを購入できる Web サイト。もしくはオンラインで注文や購入できる商品の情報を提供しているサイト。
SNS (social networking)	一般ユーザ同士を結びつけたり、特定のグループのメンバー間の交流、ビジネス交流などを助けるネットワーク ポータル。例えば、自分の個人的、仕事上の関心事などをシェアするためのメンバー プロフィールを作成できるようなサイト。Twitter などのソーシャルメディア サイトがこれに含まれる。
ソフトウェア ダウンロード (software download)	各種ソフトウェアをダウンロードするためのオンライン ポータル。
スパム (spam)	スパム メールから収集されたWeb サイト。

ストリーミング メディア (streaming media)	ストリーミング動画または音声コンテンツを無料あるいはライセンス形式で提供する Web サイト。
暴力 (violence)	暴力を扇動したり、陰惨で暴力的な画像もしくは動画を含む Web サイト。例えば、レイプ、ハラスメント、スナッフ、爆弾、暴行、殺人あるいは自殺についての情報を含むサイト。
違法ダウンロード (warez)	不正ファイル共有やソフトウェアの違法コピーに用いられる Web サイト。例えば、ソフトウェアへの違法または疑わしいアクセスを提供するサイト、そしてネットワークおよびシステムへ損害を与える可能性のあるプログラムを開発、配布するサイト。
武器 (weapons)	人間、もしくは動物に害を与える武器等に使用可能な情報、画像、もしくは動画などを含む Web サイト。これには狩猟や射撃クラブなど、これらの武器の普及を援助している組織が含まれる。またこのカテゴリにはペイントボール ガンや BB ガンなどのおもちゃの武器も含まれる。
Web メール (webmail)	Web ブラウザを通じてメール アカウントの作成とアクセスを提供する Web サイト。例: Yahoo! Mail、Gmail やローカル プロバイダの Web メール サービス。

グローバル管理者の通知設定

ここで説明される設定はウェブ インターフェースの **全体設定** > **管理者の通知設定** タブにあります。

メール アドレス	管理者のメール アドレスを指定します。 管理者へのメール通知機能を有効にしている場合、指定したメールアドレスに通知が送信されます。このメールアドレスはSMTPプロキシ設定の通知メールの送信者アドレスにも使用されます。複数のメールアドレスを指定した場合、最初のアドレスが送信者のアドレスになります。
SMTPサーバのホスト名	ウイルス検出の通知を管理者へ送信するメール サーバを指定します。
ポート番号	ウイルス検出の通知を管理者へ送信するメールサーバのポート番号を指定します。デフォルトのポート番号は25です。

グローバル ディレクトリの設定

ここで説明される設定はウェブ インターフェースの **全体設定** > **ディレクトリの設定** タブにあります。

一時ディレクトリ	ウイルス スキャンされている一時ファイルを保存する作業ディレクトリを指定します。デフォルトは `/var/tmp/fsigk` です。
隔離保存ディレクトリ	検出されたウイルスを保存する隔離保存ディレクトリを指定します。デフォルトは `/var/tmp/quarantine` です。

グローバルのスパム フィルタ設定

ここで説明される設定はウェブインターフェースの**全体設定**>**スパム フィルタの設定**タブにあります。

クラウド ベースのスパム スキャン	クラウドベースのスキャンを有効または無効にします。クラウドベースのスパムスキャンは SMTP と POP プロキシを使用するメールに対するスパム (迷惑メール) の検出精度を高めます。
リアルタイム ブラック リスト (RBL: Real-time black list)	リアルタイム ブラック リストはスパムに関連するコンピュータまたはネットワークのアドレスを公開するために使用されます。リアルタイム ブラック リストをオンにすると、スパム フィルタ機能はリアルタイム

ブラック リストを使用してスパム メッセージを検出するようになります。

ソース IP アドレス (SMTP を使用した場合) と受信したヘッダ フィールドの IP アドレスが RBL サーバに登録されているメールはスパムとして検出されます。RBLサービスはサードパーティのベンダーから提供されます。

注: RBL 処理がタイムアウト (1秒の間に返信がない) した場合、メールはスパムとして識別されません。

リアルタイム ブラック リストのサーバ

使用するリアルタイム ブラック リストを指定します。

一般的によく利用されている2つの RBL サービス:

- Spamhaus (https://www.spamhaus.org/organization/dnsblusage/): サーバは `sbl-xbl.spamhaus.org`.
- SpamCop (https://www.spamcop.net/): サーバは `bl.spamcop.net`.

デフォルトでは製品は RBL サーバを使用しません。

注: RBL を使用するには該当する利用規約に同意する必要があります。

除外するアドレス

リアルタイム ブラック リストを特定のアドレスの確認に使用しないでください。デフォルトでは `127.0.0.1 10. 192.168. 172.16.0.0/255.240.0.0` のアドレスは除外されます。

スパム URL リアルタイム ブラック リスト (SURBL: Spam URL real-time black list)

SURBL サーバはスパム メッセージで頻繁に表示されるホストの収集と管理を行います。この設定をオンにすると、メールの本文にスパムホストに該当するリンクがあるか検索されます。

スパム URL リアルタイム ブラック リストのサーバ

使用するSURBLサーバを指定します。デフォルトは`multi.surbl.org`です。

グローバルのカスタム スパム フィルタ設定

ここで説明される設定はウェブ インターフェースの **全体設定** > **カスタム スパム フィルタ設定** タブにあります。

カスタム フィルタリング ルールを使用することでメッセージ ヘッダまたは本文にある文字列を検索して分別されたメッセージを許可/拒否できます。

カスタム スパム フィルタ ルール

カスタム スパム フィルタリング ルールを有効/無効にします。

ルール範囲

検索する文字列の対象となるメッセージの部分 (ヘッダまたは本文) を選択します。

ヒント: [**常に一致**]を選択するとルールが常に一致します。たとえば、拒否対象のメッセージをすべて拒否するためにこのルールを指定できます。

ルール範囲: 他のメッセージ ヘッダ

ルール範囲に [**その他**] を選択して、検索の対象となる代替メッセージ ヘッダを指定します。

文字列を一致

メッセージで検索の対象となる文字列を指定します。指定した文字列が一致する場合、ルールの処理が実行されます。

先頭と末尾のスペースは無視されます。

一致オプション	文字列の一致に関して追加オプションを選択します。	
	前方一致	フィールドの先頭またはメッセージ
	後方一致	文字列がフィールドまたはメッセージ部分の末尾にある必要があります。
	大文字小文字を区別	文字列の大文字と小文字が一致する必要があります。
	不一致	このルールはヘッダフィールドまたはメッセージ部分に文字列が含まれていない場合に適用されます。
	「AND」および前のルール	このルールは前のルールが適用された場合に適用されます。
	「AND」および MIME 部分の前のルール	このルールは前のルールがメッセージの同じMIME部分適用された場合に適用されます。
動作	ルールに一致する場合、メッセージを許可 (非スパム) または拒否 (スパム) として扱うか選択します。[**次のルールとつなぐ**] を選択すると、現在のフィルタリングルールをルールリストにある次のフィルタリングルールと組み合わせます。	
新しいルール番号	フィルタリング ルールの優先度を選択します。	

カスタム スパムフィルタリング ルールを作成する

次の方法でカスタムのスパム フィルタリング ルールを作成できます。

1. ウェブ インターフェースで **全体設定** > **カスタム スパム フィルタ設定** の順に選択します。
2. [**カスタム スパム フィルタリング ルール**] が [**有効**] であることを確認します。
3. [**ルール範囲**]で、文字列の検索対象となるメッセージのヘッダフィールドまたは本文を選択します。
4. [**文字列を一致**] で、一致する文字列を入力します。
5. 必要に応じて [**一致オプション**] で検索の設定を調整します。
6. 「処理」で、ルールがメッセージを許可 (非スパムとして扱う) または拒否 (スパムとして扱う) するか選択します。[**何もしない**] を選択すると他のルールを組み合わせることができます。
7. [**新しいルール番号**] で、フィルタリング ルールが適用される順序を選択します。
   ルールの順序は重要です。最初に一致するルールが適用されます。
8. [**ルールの追加**] をクリックすると選択した位置にルールが追加されます。

   
   ヒント : ルールの順序は [**ルールを上へ移動**] および [**ルールを下へ移動**] ボタンで調整できます。
9. [**保存してリロード**] をクリックして新しいルールを適用します。

4.7 パターン ファイルのアップデート

最新の脅威に対して最新のセキュリティ状態を維持するために、ウイルス定義ファイルのデータベースを常に最新の状態にしてください。

F-Secureはウイルス定義データベースを1日に数回アップデートします。自動更新を有効にしたら、最新のアップデートが自動的に適用されます。

4.7.1 ウイルス定義ファイルのアップデート設定

ここで説明される設定はウェブインターフェースの**ウイルス定義アップデート**›**設定**タブにあります。

自動更新	ウイルス定義ファイルの自動アップデートを有効または無効にします。設定を有効にすると、ウイルス定義データベースが自動的に最新の状態になります。
ウイルス データベースのバージョン	スキャン エンジンのデータベース バージョンを表示します。
プロキシ サーバ	本製品がプロキシを通じてWebに接続する場合、この設定を有効にし、プロキシのホスト名とサーバ ポートを設定してください。製品がWebに直接接続する場合、この設定を無効にしてください。
プロキシのホスト名	プロキシ サーバのホスト名を指定します。
ポート番号	プロキシ サーバのポート番号を指定します。
HTTP プロキシ認証	プロキシが認証を使用する場合、この設定を有効にし、ユーザ名とパスワードを設定してください。
ユーザ名	プロキシの認証に使用するユーザ名を指定します。
パスワード	プロキシの認証に使用するパスワードを指定します。

4.8 システム情報

「システム情報」ではインストールされている製品の情報を確認したり、診断ツールを実行したり、設定のバックアップと復元を行ったりすることができます。

4.8.1 システムの情報を表示する

システムの情報を表示するには

ウェブ インターフェースで [**システム情報**] を選択します。

4.8.2 システム情報のステータス

これらの統計情報はウェブ インターフェースの **システム情報**›**ステータス** タブにあります。

製品のバージョン	インストールされている製品のバージョンとビルド番号を表示します。
ライセンスの有効期限	ライセンスのステータスと有効期限を表示します。
ウイルス定義データベースのバージョン	スキャン エンジンのデータベース バージョンを表示します。
スキャンエンジン	インストールされているスキャン エンジンを表示します。
日付	製品がインストールされているシステムの日付と時刻を表示します。

4.8.3 診断ツールを実行する

製品のサポートにお問い合わせいただく際には診断情報ファイル(`diag.tar.gz`)を提供してください。

診断情報ファイルを作成するには

1. ウェブ インターフェースで **システム情報**›**診断情報** の順に選択します。

2. [**診断情報ファイルをダウンロード**] リンクをクリックします。

4.8.4 ログ ファイルをダウンロード

ウェブ インターフェースから製品のログ ファイルをダウンロードして確認できます。

次の方法でログ ファイルをダウンロードできます。

1. ウェブ インターフェースで [**ログ ファイルをダウンロード**] を開きます。
   ウェブ インターフェースで製品ディレクトリにあるログ ファイルが表示されます。
2. 表示するログの名前をクリックします。
   HTTP、SMTP、POP、FTP、ICAP ログはそれぞれ別のディレクトリに格納されています。

4.8.5 構成のバックアップと復元

製品の構成をバックアップして後から設定を復元することができます。たとえば、製品をアップグレードした後に前の設定を読み込むことが可能です。

バックアップ構成を作成する

すべての設定を圧縮ファイルにバックアップすることができます。

設定をバックアップするには

1. ウェブ インターフェースで**バックアップと復元** > **バックアップ**タブの順に選択します。
2. [**構成をバックアップ**] をクリックします。
   `tar.gz` ファイルに設定が圧縮されます。
3. 後で使用することを考慮して、圧縮ファイルを大事に保管します。

バックアップした構成を復元する

保存した設定をいつでも復元することができます。

設定を復元するには

1. ウェブ インターフェースで**バックアップと復元** > **復元**タブの順に選択します。
2. [**ファイルを選択**] をクリックし、復元する圧縮ファイルを選択します。
3. [**アップロード**] をクリックし、バックアップした設定を適用します。

4.9 ライセンス

「**ライセンス情報**」画面ではライセンスのアップデートとプライバシー ポリシーの表示を行えます。

4.9.1 製品のライセンスをアップデートする

製品のインストール後、体験モードが有効になります。ウェブ インターフェースから製品をフル ライセンス版にアップグレードできます。

ライセンスの確認とアップデートを行うには

1. ウェブ インターフェースで **ライセンス** > **ライセンス** の順に選択します。
   [**ライセンス ステータス**] でライセンスのステータスと有効期限が表示されます。
2. 新しいライセンス キは [**ライセンス キー**] フィールドに入力できます。
3. [**保存**] をクリックします。

4.9.2 プライバシー ポリシーを表示する

F-Secure はお客様のプライバシーを守ります。当社のプライバシー ポリシーには顧客の個人情報保護に関する F-Secure の基本原則が記載されています。

プライバシー ポリシーを表示するには

ウェブ インターフェースで **ライセンス** > **プライバシー ポリシー** の順に選択します。

4.10 管理パスワード

ウェブ インターフェースへログインするにはパスワードが必要になります。

4.10.1 パスワードを変更する

次の方法で管理者のパスワードを変更できます。

1. ウェブ インターフェースで [**管理者パスワード**] を選択します。
2. [**使用中のパスワード**] フィールドに現在のパスワードを入力します。
3. [**新しいパスワード**] フィールドに新しいパスワードを入力し、[**パスワードの確認**] フィールドに新しいパスワードをもう一度入力します。
4. [**保存**] をクリックします。

4.11 ウェブ インターフェースの言語

ウェブ インターフェースの表示言語を変更することができます。

4.11.1 言語を変更する

次の方法でウェブユーザインタフェースの言語を変更できます。

1. ログイン ページで**地球儀**のアイコンをクリックします。
2. ウェブユーザインタフェースで使用する言語を選択します。

注： ログインした後、[**言語を変更**] をクリックすると表示言語を選択できます。

第章

5

詳細設定

トピック：

設定ファイルにはウェブインターフェースでは設定できない詳細設定が含まれています。

設定を変更する場合、必要に応じて`/opt/f-secure/fsigk/conf/fsigk.ini`設定ファイルを変更します。

設定を変更した後、設定ファイルを保存し、`/opt/f-secure/fsigk/rc.fsigk_{http,smtp,pop,ftp} restart`コマンドを実行して対象のサービスを再起動します。

5.1 プロキシ設定

ウイルススキャンプロキシの動作を設定します。

5.1.1 HTTP プロキシ

HTTPプロキシの詳細設定。

ウイルス検出時の処理

Delete (action={pass,delete})

検出したウイルスを削除するか指定します。

削除しない場合も、ログへの記録・管理者通知は行います。

通常は有効にします。

Quarantine (quarantine)

`quarantine=yes`を設定するとウイルスの隔離保存を有効にします。

ウイルスの隔離保存場所は設定ファイルの共通設定にある`quarantine_dir`オプションで設定できます。

十分なディスク容量がある場合のみ指定してください。

HTTP プロキシ認証

Proxy authentication (proxyauth_pam_auth)

`proxyauth_pam_auth=yes`を設定するとプロキシの認証にPAM (Pluggable Authentication Modules) を使用します。

認証方法は`/etc/pam.d/fsigk_http`ファイルで変更できます。

Add or remove users

`/opt/f-secure/fsigk/conf/pam/`ディレクトリにあるファイルに次のコマンドを実行するとユーザおよびパスワードの追加・削除・編集が可能です。

```
# echo -e username'\t'password >>
/opt/f-secure/fsigk/conf/pam/userdb_http.txt
# ./create_userdb userdb_http.db < userdb_http.txt
```

アクセス制御

From these hosts (acl_from)

`acl_from=yes`を設定すると指定したホスト一覧からの接続のみ受け付けます。

ヒント: DNS 逆引きを有効にすると<ホスト名>.<ドメイン名>形式の指定も可能になります。

注: 設定ファイルでこの設定を有効にする場合、`/opt/f-secure/fsigk/conf/fsigk.ini`ファイルにある`<protocol>_from`フィールドで対象のホストを指定してください。`/opt/f-secure/fsigk/libexec/fsigk-reload.sh`コマンドを実行して設定を更新します。構文については、hosts_access(5)のmanページを参照してください。

To these hosts (acl_to)

`acl_to=yes`を設定すると指定したホスト一覧への接続のみ受け付けます。

注: 設定ファイルでこの設定を有効にする場合、`/opt/f-secure/fsigk/conf/fsigk.ini`ファイルにある`<protocol>_to`フィールドで対象のホストを指定してください。`/opt/f-secure/fsigk/libexec/fsigk-reload.sh`コマンドを実

行して設定を更新します。構文については、hosts_access(5)のmanページを参照してください。

DNS逆引き

DNS reverse lookup (reverselookup)

`reverselookup=yes/no`を設定すると接続元のIPアドレスのDNSの逆引きを行います。

この設定を有効すると動作速度が多少低下します。

ヒント: DNS逆引きを有効にすると`[Access control]=[From these hosts]`の設定に対して<ホスト名>.<ドメイン名>形式の指定が可能になり、アクセスログのアクセス元をホスト名で表示します。

リスクウェアスキャン

Scan riskware (riskware_check)

`riskware_check=yes`を設定するとリスクウェアスキャンを有効にします。

明らかなウイルス以外にリスクウェアも検出するようになります。

Skip these targets (pass_riskware)

指定したリスクウェアについては検出しなくなります。

リスクウェアは"`Category.Platform.Family`"という名前で指定します。

最大で1999バイトまで指定できます。設定ファイル中では、セミコロン(";")区切りで指定します。

ヒント: 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カテゴリのすべてのリスクウェアをスキャン対象外にします。

Keep-Alive connection (keepalive)

`keepalive=yes`を設定するとKeep-Alive接続(Persistent Connection)を利用します。

キープアライブの接続は、サーバとクライアントがキープアライブに対応し、次の条件を満たしている必要があります。

- `Keep-Alive`接続設定が有効
- HTTP/1.1応答で応答ヘッダで`Connection`が`close`ではない、またはHTTP/1.0応答で`Connection`または`Proxy-Connection`が`keep-alive`で始まる。
- 応答ヘッダで、Content-Lengthが1以上、または応答コードが304か204か1xx
- 要求ヘッダ、応答ヘッダにContent-Lengthが2回以上存在しない。
- ウイルス検出応答でない
- サーバへの接続が成功し、エラーが発生していない
- FTP over HTTPでない
- CONNECTメソッドでない

Timeout (keepalive_timeout)

Keep-Alive接続のタイムアウト時間(秒数)を1以上で指定します。

HTTP応答が終了してから指定時間が経過すると該当セッションを切断します。なお、Keep-Alive接続を行っている間、処理を行うプロキシプロセスが1つ占有します。増加させる場合は、最大同時接続数に余裕があることをご確認ください。

匿名と透過プロキシモード

Anonymous proxy (anonymous)

`anonymous=yes`を設定すると匿名プロキシを有効にします。匿名プロキシはサーバにプロキシおよびクライアントに関する情報(Via、X-Forwarded-Forヘッダ)を送付しません。

Transparent proxy mode (transparent)

`transparent=yes`を設定すると透過プロキシモードを有効にします。

透過プロキシとして動作させる場合、NATのリダイレクト設定が必要です。NATのリダイレクト設定は、コマンドラインからiptablesコマンドで以下のように設定します。

```
# iptables -t nat -A PREROUTING -i eth1 -p tcp \
 --dport 80 -j REDIRECT --to-port 9080
```

5.1.2 SMTP プロキシ

SMTPプロキシの詳細設定。

SMTP プロキシ認証

SMTP authentication (proxyauth_pam_auth)

`proxyauth_pam_auth=yes`を設定するとユーザ個別にプロキシ認証を行います。

認証にはPAM (Pluggable Authentication Modules) を使用しており、認証方式は`/etc/pam.d/fsigk_smtp`ファイルで変更可能です。

注: [POP before SMTP認証]も同時に有効にした場合、SMTP認証とPOP before SMTP認証のいずれかに成功した場合に送信できます。

[受信先 (RCPT) ドメインの制限]も同時に有効にした場合、指定ドメインについては認証なしでも送信できます。

Add or remove users

`/opt/f-secure/fsigk/conf/pam/`ディレクトリにあるファイルに次のコマンドを実行するとユーザおよびパスワードの追加・削除・編集が可能です。

```
# echo -e username'\t'password >>
/opt/f-secure/fsigk/conf/pam/userdb_smtp.txt
# ./create_userdb userdb_smtp.db < userdb_smtp.txt
```

POP before SMTP認証

POP-before-SMTP authentication (pbs)

`pbs=yes`を設定するとPOP-before-SMTP認証を有効にします。

SMTPプロキシでPOP before SMTP認証を行う場合、POPプロキシと同時に動作させます。POPプロキシを通じて認証されたクライアントホスト (IPアドレス) に対して、一定期間SMTPプロキシの利用が許可されます。

インターネット ゲートキーパまたはメールサーバのSMTP認証も同時に利用する場合、SMTP認証とPOP before SMTP認証のいずれかに成功した場合に送信できます。

注: [受信先(RCPT)ドメインの制限]も同時に有効にした場合、指定ドメインについては認証なしでも送信できます。

Timeout (pbs_lifetime)

POP-before-SMTP認証が有効な時間(分)を設定します。

アクセス制御

From these hosts (acl_from)

`acl_from=yes`を設定すると指定したホスト一覧からの接続のみ受け付けます。

ヒント: DNS 逆引きを有効にすると<ホスト名>.<ドメイン名>形式の指定も可能になります。

注： 設定ファイルでこの設定を有効にする場合、/opt/f-secure/fsigk/conf/fsigk.iniファイルにある<protocol>_fromフィールドで対象のホストを指定してください。/opt/f-secure/fsigk/libexec/fsigk-reload.shコマンドを実行して設定を更新します。構文については、hosts_access(5)のmanページを参照してください。

To these hosts (acl_to)

acl_to=yesを設定すると指定したホスト一覧への接続のみ受け付けます。

注： 設定ファイルでこの設定を有効にする場合、/opt/f-secure/fsigk/conf/fsigk.iniファイルにある<protocol>_toフィールドで対象のホストを指定してください。/opt/f-secure/fsigk/libexec/fsigk-reload.shコマンドを実行して設定を更新します。構文については、hosts_access(5)のmanページを参照してください。

DNS逆引き

DNS reverse lookup (reverselookup)

reverselookup=yes/noを設定すると接続元のIPアドレスのDNSの逆引きを行います。

この設定を有効すると動作速度が多少低下します。

ヒント： DNS逆引きを有効にすると[Access control]=[From these hosts]の設定に対して<ホスト名>.<ドメイン名>形式の指定が可能になり、アクセスログのアクセス元をホスト名で表示します。

拒否対象

ActiveX (block_activex)

block_activex=yesを設定するとActiveXが埋め込まれたHTMLメールを拒否します。

検出時はウイルス検出と同様の動作になり、検出時の動作もウイルスの[検出時の動作]に従います。また、ウイルススキャンが無効の場合、この項目でのスキャンはできません。

検出名称は"FSIGK/POLICY_BLOCK_ACTIVEX"になります。

Scripts (block_script)

block_script=yesを設定するとスクリプト(JavaScript、VBScriptなど)を含むHTMLメールを拒否します。

検出時はウイルス検出と同様の動作になり、検出時の動作もウイルスの[検出時の動作]に従います。また、ウイルススキャンが無効の場合、この項目でのスキャンはできません。

検出名称は"FSIGK/POLICY_BLOCK_SCRIPT"になります。

Partial messages (block_partial_message)

block_partial_messge=yesを設定すると分割メールを拒否します。メールヘッダのContent-Typeフィールドにmessage/partialを含むメールを拒否します。

検出時はウイルス検出と同様の動作になり、検出時の動作もウイルスの[検出時の動作]に従います

検出名称は"FSIGK/POLICY_BLOCK_PARTIAL_MESSAGE"になります。

リスクウェアスキャン

Scan riskware (riskware_check)

`riskware_check=yes`を設定するとリスクウェアスキャンを有効にします。

明らかなウイルス以外にリスクウェアも検出するようになります。

Skip these targets (pass_riskware)

指定したリスクウェアについては検出しなくなります。

リスクウェアは"`Category.Platform.Family`"という名前で指定します。

最大で1999バイトまで指定できます。設定ファイル中では、セミコロン(";")区切りで指定します。

ヒント: 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カテゴリのすべてのリスクウェアをスキャン対象外にします。

メール本文のスキャン

Scan text body part (virus_check_text)

`virus_check_text=yes`を設定するとメールのテキスト本文のスキャンを行います。この設定の有無に関わらず、テキスト形式の添付ファイルやHTML形式の本文などスキャンします。

有効にすると、危険性のないウイルスの残骸などの一部を検出できることがあります。有効にすると動作速度が多少低下します。

テキスト形式の本文に対しては実行されないため、通常この項目を設定する必要はありません。

Scan whole html part (virus_check_wholehtml)

`virus_check_wholehtml=yes`を設定するとメールのHTML部分について、スクリプトやActiveXを呼び出す部分などのウイルスが動作する部分以外についてもスキャンを行います。

有効にすることで、ウイルス以外の疑わしいメール(詐欺メールや壊れたウイルスなど)の一部を検出します。有効にすると動作速度が多少低下します。

この設定の有無に関わらず、HTMLに含まれるウイルスは検出されるため、通常この項目を設定する必要はありません。

匿名と透過プロキシモード

Anonymous proxy (anonymous)

`anonymous=yes`を設定すると匿名プロキシモードを有効にします。

匿名プロキシはヘッダ情報(Receivedヘッダ)を追加しません。

Transparent proxy mode (transparent)

`transparent=yes`を設定すると透過プロキシモードを有効にします。

透過プロキシとして動作させる場合、NATのリダイレクト設定が必要です。NATのリダイレクト設定は、コマンドラインからiptablesコマンドで以下のように設定します。

```
# iptables -t nat -A PREROUTING -i eth1 -p tcp \
 --dport 25 -j REDIRECT --to-port 9025
```

5.1.3 POP プロキシ

POPプロキシの詳細設定。

POPユーザ制限

PAM-based account verification (proxyauth_pam_account)

`proxyauth_pam_account=yes`を設定すると接続できるユーザを制限できます。

認証にはPAM (Pluggable Authentication Modules) を使用しており、認証方式は`/etc/pam.d/fsigk_pop`ファイルで変更可能です。

Add or remove users

`/opt/f-secure/fsigk/conf/pam/`ディレクトリにあるファイルに次のコマンドを実行するとユーザおよびパスワードの追加・削除・編集が可能です。

```
# echo -e username'\t'password >>
/opt/f-secure/fsigk/conf/pam/userdb_pop.txt
# ./create_userdb userdb_pop.db < userdb_pop.txt
```

アクセス制御

From these hosts (acl_from)

`acl_from=yes`を設定すると指定したホスト一覧からの接続のみ受け付けます。

ヒント: DNS 逆引きを有効にすると<ホスト名>.<ドメイン名>形式の指定も可能になります。

注: 設定ファイルでこの設定を有効にする場合、`/opt/f-secure/fsigk/conf/fsigk.ini`ファイルにある`<protocol>_from`フィールドで対象のホストを指定してください。`/opt/f-secure/fsigk/libexec/fsigk-reload.sh`コマンドを実行して設定を更新します。構文については、hosts_access(5)のmanページを参照してください。

To these hosts (acl_to)

`acl_to=yes`を設定すると指定したホスト一覧への接続のみ受け付けます。

注: 設定ファイルでこの設定を有効にする場合、`/opt/f-secure/fsigk/conf/fsigk.ini`ファイルにある`<protocol>_to`フィールドで対象のホストを指定してください。`/opt/f-secure/fsigk/libexec/fsigk-reload.sh`コマンドを実行して設定を更新します。構文については、hosts_access(5)のmanページを参照してください。

DNS逆引き

DNS reverse lookup (reverselookup)

`reverselookup=yes/no`を設定すると接続元のIPアドレスのDNSの逆引きを行います。

この設定を有効すると動作速度が多少低下します。

ヒント: DNS逆引きを有効にすると`[Access control]=[From these hosts]`の設定に対して<ホスト名>.<ドメイン名>形式の指定が可能になり、アクセスログのアクセス元をホスト名で表示します。

拒否対象

ActiveX (block_activex)

block_activex=yesを設定するとActiveXが埋め込まれたHTMLメールを拒否します。

検出時はウイルス検出と同様の動作になり、検出時の動作もウイルスの[検出時の動作]に従います。また、ウイルススキャンが無効の場合、この項目でのスキャンはできません。

検出名称は"FSIGK/POLICY_BLOCK_ACTIVEX"になります。

Scripts (block_script)

block_script=yesを設定するとスクリプト(JavaScript、VBScriptなど)を含むHTMLメールを拒否します。

検出時はウイルス検出と同様の動作になり、検出時の動作もウイルスの[検出時の動作]に従います。また、ウイルススキャンが無効の場合、この項目でのスキャンはできません。

検出名称は"FSIGK/POLICY_BLOCK_SCRIPT"になります。

Partial messages (block_partial_message)

block_partial_messge=yesを設定すると分割メールを拒否します。メールヘッダのContent-Typeフィールドにmessage/partialを含むメールを拒否します。

検出時はウイルス検出と同様の動作になり、検出時の動作もウイルスの[検出時の動作]に従います

検出名称は"FSIGK/POLICY_BLOCK_PARTIAL_MESSAGE"になります。

Encrypted archive files (block_encrypted)

block_encrypted=yesを設定すると暗号化された圧縮ファイル(ZIP、RAR)を含むメールを拒否します。

検出時はウイルススキャンと同様の動作になります。ウイルススキャンが無効の場合、暗号化された圧縮ファイルはスキャンされません。

検出名称は"FSIGK/POLICY_BLOCK_ENCRYPTED"になります。

File name or extension (block_ext,block_ext_list)

block_ext=yesを設定すると指定したファイル名、拡張子の添付ファイルを含むメールを拒否します。

コンマ(",")区切りの後方一致で指定し、大文字小文字は区別しません。設定例: .COM,.PIF,.EXE,.BAT

"ALL"を指定すると、ファイルを含むメール全てを拒否します。圧縮ファイル内のファイルのファイル名には適用されません。

検出時はウイルス検出と同様の動作になり、検出時の動作もウイルスの[検出時の動作]に従います

最大で1999バイトまで設定できます。

検出名称は"FSIGK/POLICY_BLOCK_EXT"になります。

リスクウェアスキャン

Scan riskware (riskware_check)

riskware_check=yesを設定するとリスクウェアスキャンを有効にします。

明らかなウイルス以外にリスクウェアも検出するようになります。

Skip these targets (pass_riskware)

指定したリスクウェアについては検出しなくなります。

リスクウェアは"Category.Platform.Family"という名前で指定します。

最大で1999バイトまで指定できます。設定ファイル中では、セミコロン(";")区切りで指定します。

ヒント: 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カテゴリのすべてのリスクウェアをスキャン対象外にします。

メール本文のスキャン

Scan text body part (virus_check_text)

`virus_check_text=yes`を設定するとメールのテキスト本文のスキャンを行います。この設定の有無に関わらず、テキスト形式の添付ファイルやHTML形式の本文などスキャンします。

有効にすると、危険性のないウイルスの残骸などの一部を検出できることがあります。有効にすると動作速度が多少低下します。

テキスト形式の本文に対しては実行されないため、通常この項目を設定する必要はありません。

Scan whole html part (virus_check_wholehtml)

`virus_check_wholehtml=yes`を設定するとメールのHTML部分について、スクリプトやActiveXを呼び出す部分などのウイルスが動作する部分以外についてもスキャンを行います。

有効にすることで、ウイルス以外の疑わしいメール(詐欺メールや壊れたウイルスなど)の一部を検出します。有効にすると動作速度が多少低下します。

この設定の有無に関わらず、HTMLに含まれるウイルスは検出されるため、通常この項目を設定する必要はありません。

透過プロキシ モード

Transparent proxy (transparent)

`transparent=yes`を設定すると透過プロキシモードを有効にします。

透過プロキシとして動作させる場合、NATのリダイレクト設定が必要です。NATのリダイレクト設定は、コマンドラインからiptablesコマンドで以下のように設定します。

```
# iptables -t nat -A PREROUTING -i eth1 -p tcp \
 --dport 110 -j REDIRECT --to-port 9110
```

5.1.4 FTP プロキシ

FTPプロキシの詳細設定。

FTPユーザ制限

PAM-based account verification (proxyauth_pam_account)

`proxyauth_pam_account=yes`を設定すると接続できるユーザを制限できます。

認証にはPAM (Pluggable Authentication Modules) を使用しており、認証方式は`/etc/pam.d/fsigk_ftp`ファイルで変更可能です。

Add or remove users

`/opt/f-secure/fsigk/conf/pam/`ディレクトリにあるファイルに次のコマンドを実行するとユーザおよびパスワードの追加・削除・編集が可能です。

```
# echo -e username'\t'password >>
/opt/f-secure/fsigk/conf/pam/userdb_ftp.txt
# ./create_userdb userdb_ftp.db < userdb_ftp.txt
```

アクセス制御

From these hosts (acl_from)

`acl_from=yes`を設定すると指定したホスト一覧からの接続のみ受け付けます。

ヒント: `DNS 逆引き`を有効にすると`<ホスト名>.<ドメイン名>`形式の指定も可能になります。

注: 設定ファイルでこの設定を有効にする場合、`/opt/f-secure/fsigk/conf/fsigk.ini`ファイルにある`<protocol>_from`フィールドで対象のホストを指定してください。`/opt/f-secure/fsigk/libexec/fsigk-reload.sh`コマンドを実行して設定を更新します。構文については、hosts_access(5)のmanページを参照してください。

To these hosts (acl_to)

`acl_to=yes`を設定すると指定したホスト一覧への接続のみ受け付けます。

注: 設定ファイルでこの設定を有効にする場合、`/opt/f-secure/fsigk/conf/fsigk.ini`ファイルにある`<protocol>_to`フィールドで対象のホストを指定してください。`/opt/f-secure/fsigk/libexec/fsigk-reload.sh`コマンドを実行して設定を更新します。構文については、hosts_access(5)のmanページを参照してください。

DNS逆引き

DNS reverse lookup (reverselookup)

`reverselookup=yes/no`を設定すると接続元のIPアドレスのDNSの逆引きを行います。

この設定を有効すると動作速度が多少低下します。

ヒント: `DNS逆引き`を有効にすると`[Access control]=[From these hosts]`の設定に対して`<ホスト名>.<ドメイン名>`形式の指定が可能になり、アクセスログのアクセス元をホスト名で表示します。

リスクウェアスキャン

Scan riskware (riskware_check)

`riskware_check=yes`を設定するとリスクウェアスキャンを有効にします。

明らかなウイルス以外にリスクウェアも検出するようになります。

Skip these targets (pass_riskware)

指定したリスクウェアについては検出しなくなります。

リスクウェアは`"Category.Platform.Family"`という名前で指定します。

最大で1999バイトまで指定できます。設定ファイル中では、セミコロン(";")区切りで指定します。

ヒント: 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カテゴリのすべてのリスクウェアをスキャン対象外にします。

透過プロキシ モード

Transparent proxy (transparent)

`transparent=yes`を設定すると透過プロキシモードを有効にします。

透過プロキシとして動作させる場合、NATのリダイレクト設定が必要です。NATのリダイレクト設定は、コマンドラインからiptablesコマンドで以下のように設定します。

```
# iptables -t nat -A PREROUTING -i eth1 -p tcp \
 --dport 21 -j REDIRECT --to-port 9021
```

5.1.5 共通の設定

本製品のコンポーネントに共通する詳細設定。

RBL (spam_rbl)

`spam_rbl=yes`を設定するとスパムスキャンにRealtime Black Lists (RBL)を使用します。

コンマ区切り(",")で199文字までで指定します。

スパムスキャンにRBLsを使用すると、接続元IPアドレス(SMTPの場合)およびReceivedヘッダに記載されているIPアドレスがRBLサーバに登録されているか確認されます。

各メールについて、問い合わせ数の最大は32です。デフォルトでは、RBLサーバは3個ですので、`Received`ヘッダの上から9 10個(SMTPの場合、接続元についてもスキャンするため)または10 11個(POPの場合)についてスキャンを行います。(ただし、除外アドレスに指定したアドレスは除いて数えます。)

デフォルトでは無効です。

RBLでの検出名称は"`FSIGK/SPAM_RBL/(検出アドレス)[(RBLサーバ名):(RBL応答アドレス)]`"です。

- 検出アドレス: RBLサーバに登録されていたアドレス
- RBLサーバ名: 検出したRBLサーバ名
- RBL応答アドレス: 検出時のRBLサーバからの応答アドレス

Server (spam_surbl_list)

RBLサーバ一覧を指定します。コンマ (",") 区切りで複数指定できます。

初期設定: bl.spamcop.net, sbl-xbl.spamhaus.org

除外するアドレス

`/opt/f-secure/fsigk/conf/fsigk.ini`ファイルにある`spam_rbl_pass`フィールドで指定したアドレスに対してRBLスキャンを無効にできます。

初期設定: 127.0.0.1 10. 192.168. 172.16.0.0/255.240.0.0

SURBL (spam_surbl)

SURBL (SPAM URL Realtime Black List) によるスパムスキャンの有無と、スパムスキャンで参照するSURBLサーバを指定します。

`spam_surbl=yes/no`を設定するとこの設定を有効/無効にします。

コンマ区切り(",")で199文字までで指定します。

スパムスキャンにSURBLsを使用すると、テキスト本文とHTMLボディに含まれるURLのドメイン名部分がSURBLサーバに登録されているか確認されます。

注: 各メールについて、RBLおよびSURBLの問い合わせは一斉に行いますが、サーバからの応答待ちにより数100ms程度未満の遅延が発生します。1秒以内に応答がない場合は、タイムアウトし、スパムではないと判断します。

SURBLの問合せ先DNSサーバは`/etc/resolv.conf`の最初のnameserverになります。

各メールについて、問い合わせ数の最大は32です。

デフォルトでは無効です。

SURBLでの検出名称は"FSIGK/SPAM_SURBL/(検出ドメイン名)[(SURBLサーバ名):(SURBL応答アドレス)]"です。

- 検出ドメイン名: SURBLサーバに登録されていたドメイン名
- SURBLサーバ名: 検出したSURBLサーバ名
- SURBL応答アドレス: 検出時のSURBLサーバからの応答アドレス

Server (spam_surbl_list)

SURBLサーバー一覧を指定します。コンマ(",")区切りで複数指定できます。

初期設定: multi.surbl.org

5.2 Web コンテンツ制御

Web コンテンツ制御の設定。

Security Cloud でファイルの評価確認

注: orsp_の設定を使用するには、orspservice_serviceがyesに設定されていることを確認してください。

ORSP file check (orsp_file_check)

orsp_file_check=yesを設定するとF-SecureのSecurity Cloudを利用してファイルを定期的に更新されるホワイト・ブラックリストと照合します。

新しい脅威に対する対応時間を向上してシステムリソースの負荷(一般的なファイルのスキャンに使用される)を軽減できます。デフォルトでは値は"yes"ですが、設定が省略されている場合には"no"になります。

注: この機能を通じてF-Secureのサーバへ送信される情報はすべて匿名で処理されます。詳細は、製品と一緒にインストールされるreal-time-protection-network-policy.txtを参照してください。

File reputation check timeout (orsp_timeout)

orsp_file_checkがyesに設定されている場合、製品がファイルをローカルでスキャンを行う前にSecurity Cloudからの応答時間を設定します。

デフォルトの値は5000 (5秒)です。

URL 評価を Security Cloud で確認

ORSP URL check (orsp_url_check)

orsp_url_check=yes を設定すると Web コンテンツ制御を使用して orsp_url_blocked_cats で指定されているコンテンツカテゴリをブロックできます。

Blocked content categories (orsp_url_blocked_cats)

Webコンテンツ制御でブロックする任意のカテゴリを指定します。各カテゴリ名をカンマ(",")で区切ります。空白は使用できません。カテゴリ名については Web コンテンツ カテゴリを参照してください。

5.2.1 信頼済み/拒否するサイトを設定する

信頼済み/拒否するサイトのリストは設定ファイルに保存されます。

- /opt/f-secure/fsigk/conf/trusted-sites.txtにはWebコンテンツ制御がブロックしない Web サイトが含まれています。

- `/opt/f-secure/fsigk/conf/disallowed-sites.txt` にはアクセスが拒否されている Web サイトが含まれています。

信頼済み/拒否するサイトを設定するには

1. 新しいサイトを追加する際には別々の行に各 URL を入力してください。
2. 信頼済み/拒否するサイトに次の構文を使用してください:
   - すべてのエントリにはプロトコル名を含む完全な URL (例: `http://`、`https://`、`ftp://`) をが必要とされます。
   - エントリは大小文字を区別しません。
   - エントリにはワイルドカード (* と ?) を使用できます。
     - ? は常に任意の1文字と一致します。
     - ホスト名では * は0以上の文字と一致します。
     - パスの場合、* は / 文字で区切られているセグメントと一致します。

     注: URL の一部にクエリ文字列を追加する場合、最初のはてな マーク (?) の前にバックスラッシュ (\) を付ける必要があります。

     例: `http://example.com/path\?parameter=value`
   - # で始まる行 (先頭文字が空白以外) はコメントとして扱われます。
   - ポート番号、プロトコル、認証情報 (ユーザ名とパスワード) は URL の一致には利用されません。
   - URL の一致にはパスのコンポーネントは利用されます。HTTPS リクエストの場合、ホスト名と関連するパスが暗号化されます。
   - エントリ が先頭文字の場合、URL と同じパターンおよび最初の不一致文字が / または ? である場合、URL と一致するとみなされます。

     注: エントリの最後の文字が / である場合、エントリは接頭辞として使用されません。

     たとえば、`http://example.com/trusted-path/` を信頼済みのリストに追加した場合、`http://example.com/trusted-path/another_path` の 最初の不一致文字が / ではないため、信頼済みとしてみなされません。

     注: エントリの最後の文字が * の場合、エントリは接頭辞として使用されず、1つの URL パスにのみ一致します。

     たとえば、`http://example.com/trusted-path/*` を信頼済みのリストに追加した場合、`http://example.com/trusted-path/another_path` は信頼済みとしてみなされ、`http://example.com/trusted-path/another_path/yet_another_path` は信頼済みとしてみなされません。

3. リストを変更した後に `/opt/f-secure/fsigk/libexec/fsigk-reload.sh` コマンドを実行すると、製品を再ロードして新しい設定が適用されます。

5.3 ICAPサービスウイルススキャンの設定

ICAPデーモンはICAPプロトコルのREQMOD、RESPMODおよびOPTIONSメソッドを導入します。REQMODまたはRESPMOD要求に包含されたHTTPボディが含まれている場合、ウイルススキャンが実行されます。

感染ファイルが検出された場合、ICAPデーモンによりコンテンツがブロックされたことを示すHTMLページが応答コンテンツと置き換えられます。ウイルス通知テンプレートを編集することでこのHTMLページを変更できます。

ICAPデーモンはオプションのAllow: 204 ICAPヘッダを識別し、ヘッダが存在し、変更が必要ない場合にはステータスコード204を返します。ネットワークの負荷とディスク容量を低くするためにクライアントプロキシが204応答を許可することを推奨します。

ICAPサービスはfsicapdデーモンが実行されていることを必要とします。設定ファイル/opt/f-secure/fsigk/conf/fsigk.iniに次の[ICAP]部分を追加することでICAP関連の設定を変更できます。

設定の変更後、/opt/f-secure/fsigk/rc.fsigk_fsicapd restartコマンドを実行してデーモンを再起動してください。

5.3.1 ICAPデーモン設定

スキャン制限

最大スキャンサイズ (max_scan_size)

スキャンするコンテンツのサイズを制限します。ICAP要求にこの値より大きいHTTPボディが含まれている場合、スキャンを行わずに要求が許可されます。-1を指定すると制限を無効にします。

長いスキャン時間によるプロキシの遅延を避けるためにスキャンサイズの制限およびICAPデーモンが使用する一時ディスク容量の制限を設定することを推奨します。デフォルト値は2147483648 (2 GB) です。

スキャンタイムアウトのブロック (scan_timeout_block)

スキャン中に最大スキャン時間が達した場合、コンテンツを感染しているとみなし、コンテンツをブロックします。デフォルトの"no"ではスキャン時間内に感染が検出されなかった場合にコンテンツはブロックされません。

Security Cloud でファイルの評価確認

注: orsp_ の設定を使用するには、orspservice_service が yes に設定されていることを確認してください。

ORSP file check (orsp_file_check)

orsp_file_check=yesを設定するとF-SecureのSecurity Cloudを利用してファイルを定期的に更新されるホワイト・ブラックリストと照合します。

新しい脅威に対する対応時間を向上してシステムリソースの負荷(一般的なファイルのスキャンに使用される) を軽減できます。デフォルトでは値は "yes" ですが、設定が省略されている場合には "no" になります。

注: この機能を通じてF-Secureのサーバへ送信される情報はすべて匿名で処理されます。詳細は、製品と一緒にインストールされるreal-time-protection-network-policy.txtを参照してください。

File reputation check timeout (orsp_timeout)

orsp_file_checkがyesに設定されている場合、製品がファイルをローカルでスキャンを行う前にSecurity Cloudからの応答時間を設定します。

デフォルトの値は5000 (5秒)です。

メールスキャン

メールスキャンを有効にする (enable_email_services)

enable_email_services=yesを設定するとICAPサービスを利用したメールとスパムのスキャンが有効になります。

デフォルトでは有効です。

アンチスパムデーモンのソケットパス (fsasd_sockpath)

fsasdサーバソケットのパスを設定します。

指定したパスは絶対パス

fsasdソケットをデフォルトから変更した場合にのみ変更してください。

リスクウェアスキャン

リスクウェアのブロック (block_riskware)

`block_riskware=yes`を設定するとリスクウェアとグレイウェア検出を有効にします。

デフォルトでは無効です。

圧縮ファイルのスキャン

圧縮ファイルのスキャン (scan_archives)

`scan_archives=yes`を設定すると圧縮ファイルの内部をスキャンします。

圧縮ファイルのスキャンを無効にすると、ICAPサービスは圧縮ファイルをスキャンしますが圧縮ファイルの内部を展開しません。

暗号化されている圧縮ファイルのブロック (block_encrypted_archives)

`block_encrypted_archives=yes`を設定すると暗号化された圧縮ファイルを拒否します。

設定を有効にし、圧縮ファイルが暗号化されている理由でスキャンを実行できない場合、感染名`Encrypted_archive`が報告されます。設定を無効にすると、スキャンの失敗時に暗号化された圧縮ファイルは安全とみなされます。

圧縮ファイルの最大ネスト数 (max_nested)

圧縮ファイルのスキャンの対象となる最大ネスト数(階層構造)を設定します。指定したネスト(階層)以内にあるファイルがスキャンされます。

この設定は`scan_archives`の設定が有効な場合にのみ適用されます。

ネストされている圧縮ファイルのブロック (block_archive_max_nested)

`block_archive_max_nested=yes`を設定すると最大ネスト数を超える圧縮ファイルをブロックします。設定を有効にすると、最大ネスト数(`max_nested`の値)を超えた場合に`Archive_max_nested`の感染名が報告されます。

この設定は`scan_archives`の設定が有効な場合にのみ適用されます。

ロギング

アクセスロギングを有効にする (enable_accesslog_file)

`enable_accesslog_file=yes`を設定するとICAPリクエストを`/opt/f-secure/fsigk/log/fsicapd/access.log`ファイルにログできます。

ログファイルにはICAPのリクエストごとに1つの行が記録されています。各行にはリクエスト行、結果コードおよび他の情報が含まれています。

デフォルトでは設定は無効です。

トリックリング

Enable response trickle (enable_response_trickle)

`enable_response_trickle=yes`を設定するとICAPのレスポンストリックリングを使用できます。

トリックリングを実行している場合、fsicapdはICAPレスポンス ヘッダまた場合によってはカプセル化されたHTTPヘッダもクライアントにただちに送信して、カプセル化されたボディデータを1バイトごとに対してトリックリングを行います。スキャンが完了したら、変更されていない残りのボディ データはただちに送信されるか、または危険なコンテンツが検出された場合にはICAPの接続が切断されます。

スキャンが完了される前にICAPレスポンスヘッダが送信されるため、検出情報を含む`X-FSecure-*`ヘッダはトリックリングの使用中にICAPレスポンスに含まれません。

トリックリングは次の場合に発生します。

- ICAPのリクエストタイプがRESPMODであり、
- レスポンスにNULL(空)のボディが含まれてなく、
- fsicapdが判断できないことで、ICAPのリクエストヘッダコンテンツに基いてレスポンス204が送信される。

デフォルトでは設定は無効です。

トリックリングの間隔 (trickle_interval)

トリックリングの有効時にクライアントにシングルバイトのデータを送る頻度 (秒単位で) を設定します。

デフォルトの値は30です。

トリックリングする最大バイト数 (trickle_max_bytes)

スキャン結果が利用できる前にトリックリングされる最大バイト数を設定します。小さい値を設定すると、クライアントに危険なコンテンツが送信されることを防げられます。

デフォルトの値は120です。

アクセスログエントリをカスタマイズする

ICAPのリクエストヘッダとHTTP reqhdrおよびreshdrヘッダフィールドをアクセスログエントリに追加することができます。

```
log_icap_fields=<header-field-list>
log_req_fields=<header-field-list>
log_res_fields=<header-field-list>
```

`<header-field-list>`はオプションラベルを含むICAPとHTTPフィールド名のカンマ区切り一覧です。

`:method`、`:uri`、`:version`、`:status` を使用してICAPとHTTPヘッダフィールドの開始行を参照できます。

注:

- フィールド名は大文字と小文字を区別しません。また空白は無視されます。
- カスタム フィールドは ICAP リクエストで表示されるているように注文されます。
- ICAP リクエストが特定フィールドを含めていない場合、アクセス ログ エントリにも該当のフィールドは含まれません。フィールドが複数ある場合、アクセスログエントリにも複数回追加されます。
- 印刷可能な (7ビット)ASCIIバイトは、バックスラッシュ (\) とダブルクォーテーション (") を除いて、そのままコピーされます。他のバイトはバックスラッシュと8進数で暗号化されます (例: "\177" は DEL、"\000" は NUL)。

- フィールド値が長い場合、値は数キロバイトに省略されます。またアクセスログエントリが長い場合、エントリは10キロバイトほどに省略されます。

カスタマイズしたログの例

たとえば、ICAPリクエストのHTTP reqhdr部分に次のフィールドが含まれています。

```
Host: example.com
Content-Type: text/html; charset=utf-8
```

次のカスタマイズ設定を設定します。

```
log_req_fields=host, content-type:CT
```

アクセスログエントリに次の情報が追加されます。

```
host="example.com" CT="text/html; charset=utf-8"
```

5.3.2 ICAP応答ヘッダ

ICAPクライアントが'Allow:204' ICAPヘッダを使用することを推奨します。サーバが短期間でクリーン(安全な)要求に対応できるようになります。

感染が検出された場合、fsicapdはICAPの結果コード200を返します(エラーが発生していないことを想定)。次のICAP応答ヘッダから感染に関連する情報を確認できます。

ヘッダ	概要	値	参考
X-Fsecure-Scan-Result	スキャンの結果を報告します。REQMODとRESPMODのすべての応答にヘッダが含まれます。	'clean', 'infected', 'suspected', 'grayware', 'spam', 'whitelisted'	メッセージがスパムおよびマルウェアである場合、マルウェアの検出が優先されます
X-Fsecure-Infection-Name	感染名を報告します	感染名(文字列)	感染が検出されない場合、ヘッダは含まれません
X-Fsecure-FSAV-Duration	fsavdデーモンがウイルススキャンにかかった実際の時間を報告します	スキャン時間(秒)	スキャンを完了するために必要ヘッダのみ含まれます
X-Fsecure-Transaction-Duration	単一の要求を処理するために費やした時間を報告します。サーバがICAP要求ヘッダを受信してからICAP応答ヘッダが作成されるまでの秒数です。	スキャン時間(秒)	
X-Fsecure-Spamcheck-Duration	fsasdデーモンがスパムスキャンにかかった実際の時間を報告します	スキャン時間(秒)	

ヘッダ	概要	値	参考
X-Fsecure-Infected-Filename	感染したファイルの名前を報告します	ファイル名 (文字列)	ファイルの名前が知られている場合、ヘッダは含まれません。ファイル名は、圧縮ファイル内のファイルまたはMIMEのメール添付ファイルにより感染が検出された場合に報告されます。ファイル名は非ASCII文字を含めるためにURLエンコードされます。

5.3.3 ICAPサービスデーモン一時ファイル

ICAPサービスデーモン(fsicapd)がHTTP要求・応答をスキャンする場合、包含されたボディはchunkedエンコード形式から解読され、一時ファイルに書き込まれます。一時ファイルはICAP要求が完了するまで残ります。

一時ファイルの数と最大サイズはfsicapd設定とICAPクライアントの動作に依存します。

- 一時ファイルの最大数は接続しているクライアント数 (max_conn) になります。ICAP要求が`Allow: 204`ヘッダを含めている場合、一時ファイルの最大サイズはスキャンサイズの制限(max_scan_size)に設定されます。
- ICAP要求が`Allow: 204`ヘッダを含まない、またはサイズ制限が設定されていない場合、ボディ全体が保管されます。その場合、一時ファイルのサイズに上限はありません。

一時ディスク容量の不足を防ぐために適切なディスク容量を割り当て、スキャン制限と最大接続数を慎重に設定してください。fsicapdがICAP要求の処理中に一時ファイルの書き込みに失敗した場合、クライアントにエラーコード500が返されます。ICAPサービスを使用しているプロキシは感染しているコンテンツを誤って許可しないように適切に設定してください。

5.3.4 ICAPエラーとステータスコード

次の表は、ICAPサービスデーモンより返されるエラーICAPのステータスとエラーコードを示します。

コード	応答理由
200	ICAPサーバが変更された可能性のある応答または要求を返す。 OPTIONS応答
204	HTTP要求・応答に問題がない。 プロキシが元の要求・応答を変更なしで使うべき
400	ICAPプロトコルエラー。クライアントからのICAP要求の解析が失敗

コード	応答理由
500	内部エラー。ICAPデーモンのディスク容量またはメモリが不足している可能性が高い
503	最大接続数に達し、サービスの過負荷

注: ICAPプロトコルの詳細については、RFC3507およびICAPクライアントとして使用するHTTPプロキシのドキュメンテーションを参照してください。

5.3.5 ICAPメールスキャンサービス

スキャンサービスはメールに対してマルウェアとスパムのスキャンを実行できます。

メールスキャンには次のサービスを使用してください。

- reqmod-smtp,
- respmod-smtp,
- reqmod-pop
- respmod-pop

注: メールスキャンとスパムの確認サービスを使用するにはenable_email_servicesを設定ファイルで有効にする必要があります。詳細については、「ICAPデーモン設定」を参照してください。

マルウェアのスキャンサービスはクラウドベースの評価サービスとは関係なく動作します。スパムフィルタは評価ベースの分析を使用するため、スパムの分別には評価サービスを使用する必要があります。

注: スパムスキャンはHTTPSの接続を必要とします。ファイアウォールはHTTPSをフィルタを介さずに許可するように設定してください。

- 製品の構成により、アンチマルウェア機能によるF-Secureクラウドサービスの使用は異なります。アンチスパムのスキャンはF-Secureクラウドサービスを使用します。
- アンチマルウェアのスキャンおよびアンチスパムはHTTPSを使用します。ファイアウォールはHTTPSをフィルタを介さずに許可するように設定してください。

メールスキャンのリクエスト

メールは次の方法でICAPリクエストでカプセル化する必要があります。

- 全体のメールデータ部分はカプセル化されたボディに対してリクエストタイプに適切なタイプでカプセル化してください (req-bodyまたはres-body)。
- リクエストにカプセル化されたヘッダを含まないでください (req-hdrまたはres-hdr)。
- SMTPやPOPコマンドなど他のデータは含まないでください。クライアントは追加のリクエストヘッダにある関連データを解析・送信してください。

メールスキャンサービスは次の追加リクエストヘッダを認識します。

注: これらのヘッダはオプションで、スパム検出エンジンはヘッダが正しく整形され、情報が正しいことを必要とします。

メールリクエストの追加リクエストヘッダ

X-Client-IP SMTP/POPクライアントのIPアドレス。

例:

```
X-Client-IP: 127.0.0.1
```

X-Mail-From

クライアントアプリケーションにより解析されたメール送信者のアドレス(例:SMTP "MAIL FROM" コマンドラインまたは他のソース)。

例:

```
X-Mail-From: sender.address@example.com
```

X-Rcpt-To

メールの宛先のアドレスを含むカンマ区切り一覧。クライアントアプリケーションはこれらを解析できます (例: 一連のSMTP "RCPT TO" コマンドから)。

例:

```
X-Rcpt-To: rcpt1@domain.com,rcpt2@another-domain.org
```

メールスキャンのレスポンス

メールスキャンサービスに送信されるメールにはウイルススキャンの実行後にスパムスキャンが実行されます。メールがスパムとして検出された場合、次が行われます。

- X-FSecure-Scan-Resultレスポンスヘッダはspamになります
- X-FSecure-Infection-Nameレスポンスヘッダは Email_Spamになります

メールにマルウェアが検出され、スパムとしても認識された場合、これらのサービスからのICAPレスポンスには空のボディだけ含まれます。

例: メールスキャンのリクエスト

```
RESPMOD icap://localhost:1344/respmod-smtp ICAP/1.0
Host: localhost
Encapsulated: res-body=0
X-Client-IP: 1.3.5.7
X-Mail-From: testuser@some-domain.com
X-Rcpt-To: another.user@example.com, third@testuser.example.org

2f8
Received: (from root@localhost)
 by test.unix.example.com (8.11.6/8.8.7) id g0SGYuU04125
 for foo@bar.example.com; Mon, 28 Jan 2002 18:34:56 +0200
Date: Mon, 28 Jan 2002 18:34:56 +0200
From: root <root@freddy.unix.dflab.com>
To: foo@darkstar.css.dflab.com
Subject: eicar test file
Message-ID: <20020128183456.C4074@freddy.unix.dflab.com>
Mime-Version: 1.0
Content-Type: multipart/mixed; boundary="m51xatjYGsM+13rf"
X-Mailer: Mutt 1.0.1i

--m51xatjYGsM+13rf
Content-Type: text/plain; charset=us-ascii
eicar

--m51xatjYGsM+13rf
Content-Type: application/x-com; charset=us-ascii
Content-Disposition: attachment; filename="eicar.com"
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
--m51xatjYGsM+13rf--
.
0
```

5.4 アクセス制御

プロキシの設定などで、ホスト、ネットワークによるアクセス制御を行うことができます。

設定は以下のように記述します。

注： アクセス制御はtcpwrapperで行います。tcpwrapperについての詳細は、コマンドラインから `man 5 hosts access` を実行して確認してください。

以下の設定例は`/opt/f-secure/fsigk/conf/fsigk.ini`ファイルで次の設定に関するプロキシサービスの指定方法を示します。

- From these hosts (`acl_from`)
- To these hosts (`acl_to`)
- Restrict email recipients (`acl_rcpt`)
- Host name (`acl_pass_to`)
- Address to be excluded (`spam_rbl_pass`)

記述例

123.456.789.123 999.999.999.999	IPアドレスが "123.456.789.123" または "999.999.999.999" の時に接続を許可します。
host.domain.com	ホスト名がhost.domain.jpの時に接続を許可します。 xxx.host.domain.jpは許可しません。
.domain.com	ホスト名が.domain.jpで終わるときに接続を許可します。 "xxx.domain.jp" は許可しますが、"domain.jp" 自身は許可しません。
domain.com .domain.com	domain.jp及びdomain.jp配下のドメインを許可します。 "xxx.domain.jp"、"domain.jp"の両方を許可します。
192.168. (または: 192.168.0.0/255.255.0.0)	IPアドレスが192.168.3.4のように指定されたネットワークに含まれるときに接続を許可します。 ネットマスクに "255.255.255.255" は記述できません。
ALL	全てのホストからの接続を許可します。
ALL EXCEPT 1.2.3.4 4.5.6.7	IPアドレスが "1.2.3.4" または "4.5.6.7" 以外を許可します。
ALL EXCEPT 192.168.0.0/255.255.0.0	ネットワークが192.168.0.0/255.255.0.0以外を許可します。
.domain.com EXCEPT 999.999.999.999 987.654.321.123	ホスト名が.domain.jpで終わり、かつIPアドレスが999.999.999.999でも987.654.321.123でもない時に接続を許可します。
/etc/fsigk_allow_list.txt	一覧ファイル(/etc/fsigk_allow_list.txt)に記述されたアドレスからの接続を許可します。一覧ファイルは各アドレスを1行ずつ、または空白区切りで記述します。
ALL EXCEPT /etc/fsigk_deny_list.txt	一覧ファイル(/etc/fsigk_deny_list.txt)に記述されたアドレス・ホストからの接続を拒否し、それ以外を許可します。一覧ファイルは各アドレスを1行ずつ、または空白区切りで記述します。

1行が2000バイトを超える場合の注意事項

アクセス制御の設定ファイル(/opt/f-secure/fsigk/conf/fsigk.ini)では、1行に最大2000バイトまで記述できます。それを超える場合、以下のような方法で設定してください。

1. 別ファイルに一覧を記述する方法 別ファイル(例: /etc/fsigk_smtp_rcpt_allow_list.txt)に、以下のようにホスト・ドメイン一覧を記述します。

```
aaa.com
bbb.com
ccc.com
```

2. アクセス制御の設定で、ファイル(/etc/fsigk_smtp_rcpt_allow_list.txt)を指定します。これは、アクセス制御の設定ファイル(/opt/f-secure/fsigk/conf/fsigk.ini)に記述することで行います。

```
smtp_rcpt: /etc/fsigk_smtp_rcpt_allow_list.txt
```

5.5 通知テンプレート

通知テンプレートは危険なコンテンツまたはエラーの報告を提供 します。テンプレートは /opt/f-secure/fsigk/conf ディレクトリに格納され、システム管理者は変更することが可能です。

注: テンプレートをコマンドラインから編集する場合、編集した後に対象のサービスを再起動する必要があります。

5.5.1 管理者通知テンプレート

管理者通知テンプレート(template_admin.txt)および template_admin_disallowed.txtを編集して、管理者へ送信される通知のメッセージを変更できます。

検出通知テンプレートの先頭行には、ヘッダを記述できます。

SMTPサービスで送信者へ通知、及び管理者へメールで通知を行う場合は、先頭部分に"From: name@domain"を指定することで、ヘッダのFrom行とエンベロープFrom("MAIL FROM:"コマンドのアドレス)を変更・指定できます。受信者へ通知の場合はエンベロープFromは変更できません。

"Subject:"、"From:"は、日本語でも指定できます。

注: テンプレート編集後はサービスの再起動が必要です。

検出通知で使用できる変数

${SERVICE_TYPE}	サービスの種類("http"、"smtp"、"pop"、"ftp")
${DETECTION_NAME}	ウイルスなどの検出名(W95/Klez.H@mmなど)
${VIRUS_INFO_URL}	ウイルス情報へのURL 例: "http://cgi.f-secure.com/cgi-bin/search.cgi?q=W32/NetSky.D@mm"
${CLIENT_HOST}	クライアントホスト名  **注:** ホスト名を表示する場合は、[DNSの逆引き]をオンにする必要があります。
${CLIENT_ADDR}	クライアントIPアドレス
${SERVER_HOST}	サーバホスト名(インターネット ゲートキーパからの接続先サーバ)

${SERVER_ADDR}	サーバIPアドレス(インターネット ゲートキーパからの接続先サーバ)
${STATUS}	応答コード (アクセスログと同じ値になります)
${METHOD}	要求メソッド **注:** HTTPではHTTPの要求メソッド (GET、POSTなど) です。FTPでは送信時はPUT、受信時はGETです。他のサービスでは常にGETです。
${URL}	アクセスしたサイトのURL
${CONTENT_TYPE}	Content-Typeが示す項目 (例: text/html)
${CONTENT_LENGTH}	送受信したファイルのサイズ (バイト数)
${FILENAME}	検出したファイル名
${QUARANTINE_FILE}	隔離保存ファイル名
${TIME}	アクセス時刻 (1970/01/01を基点とした秒数)
${TIME_STR}	アクセス時刻文字 (例: 'Tue May 7 16:16:17 2002')
${HEADER}	ヘッダの内容
${TEXT}	テキストメッセージの内容
${MAILFROM}	SMTPの送信者アドレス ("MAIL FROM:"コマンドの引数アドレス)
${RCPTTO}	SMTPの受信者アドレス ("RCPT TO:"コマンドの引数アドレス一覧 (","区切り))
${MESSAGE_ID}	SMTPのメールヘッダのMessage-Idフィールドの値
${ERROR_STR}	エラーメッセージ (アクセスログのPROXY-ERRORと同じ内容)
${ACTION}	検出した際の動作(アクセスログと同じ内容)
${PATH_QUERY}	URLのパスおよびクエリ部分 (HTTPサービスのみで有効)

5.5.2 ウイルス検出通知テンプレート

HTTP、SMTP、POPプロキシのウイルス検出通知テンプレートは`conf`ディレクトリにあります。

`conf`ディレクトリ (`/opt/f-secure/fsigk/conf/`) はデフォルトで`template_http.html`、`template_http_post.html`、`template_http_blocked.html`、`template_smtp.txt`、`template_smtp_lan.txt`、`template_pop.txt`を含みます。

ICAP検出通知テンプレーは`/opt/f-secure/fsigk/fsicapd/templates/fsicapd_infected.html`にあります。

テンプレートはウイルス検出時に表示されるメッセージを含みます。

UTF-8文字セットを使用してメッセージを入力してください。メッセージは最大で900バイトまで指定できます

注: インターネット ゲートキーパのデフォルトインストールディレクトリは`/opt/f-secure/fsigk/`です。

5.5.3 エラーメッセージテンプレート

エラーメッセージテンプレート(template_http_error.html)を編集して、エラー発生時のメッセージを変更できます。

UTF-8文字セットを使用してメッセージを入力してください。メッセージは最大で900バイトまで指定できます

5.6 上級者向けオプション

参考情報のご提供

本製品のご利用にあたって、マニュアルに記載されている設定ファイルの設定項目以外に、通常設定が必要な項目はありません。しかしながら、特別な状況・要求に対応するため、上級者向けオプションも用意しています。上級者向けオプションの参考情報は、以下のファイルで提供いたします。
/opt/f-secure/fsigk/doc/expert-options-fsigk-EN.txt

上級者向けオプションのご利用にあたって

上級者向けオプションは、今後のバージョンで仕様変更などを行う可能性が高いものもあり、また通常は設定が必要なものはありません。環境に依存する可能性や、お客様の認識と動作が異なる可能性もありますので、必ずお客様の環境で正常に動作することを確認の上ご利用ください。

なお、上級者向けオプションを利用する必要があり、実際に利用される場合は、弊社サポートセンターまでご連絡いただきますようお願いいたします。ご利用状況を把握し、必要性が高いものについては、ウェブ管理画面への追加など、公式オプションへの追加を検討いたします。

第章

6

コマンドラインでの操作

トピック：

コマンドラインのツールを使用して製品をコマンドラインから操作できます。

通常はコマンドラインでの操作は必要ありません。特にコマンドラインでの操作が必要な場合のみ、この章を参照してください。

6.1 新しい設定の適用

設定ファイルを変更した場合、新しい設定を適用するためにプロキシを再起動する必要があります。

注： ウェブ管理画面で設定を変更する際にプロキシが自動的に再起動します。

プロキシの再起動

proxy auto-start コマンドを実行します: `rc.fsigk_{http,smtp,pop,ftp}`
auto-start コマンドがプロキシ (`fsigk`) の初期化と開始を行います。

6.2 自動起動コマンド

自動起動コマンドを使用してプロキシとウイルススキャンデーモンの起動・終了・再起動を行うことができます。

動作概要

自動起動コマンド(`initscript`)により、プロキシ実行コマンド(`fsigk`)またはウイルススキャンデーモン(`fsavd`)の起動・終了・再起動を行います。

注: ウイルススキャンエンジンプロセスは、各プロキシサービスの起動前に実行する必要があります。

コマンド名

`/opt/f-secure/fsigk/rc.fsigk_http`	httpプロキシ自動起動コマンド
`/opt/f-secure/fsigk/rc.fsigk_smtp`	smtpプロキシ自動起動コマンド
`/opt/f-secure/fsigk/rc.fsigk_pop`	popプロキシ自動起動コマンド
`/opt/f-secure/fsigk/rc.fsigk_ftp`	ftpプロキシ自動起動コマンド
`/opt/f-secure/fsigk/rc.fsigk_fsavd`	ウイルススキャンエンジンプロセス
`/opt/f-secure/fsigk/rc.fsigk_fsigkwebui`	ウェブ管理画面 自動起動コマンド

オプション

`start`	プロキシの開始
`stop`	プロキシの終了
`restart`	プロキシの再起動

status	プロキシの動作状況表示

httpプロキシの再起動

```
# /opt/f-secure/fsigk/rc.fsigk_http restart
```

httpプロキシの自動起動を設定

```
# ln -s /opt/f-secure/fsigk/rc.fsigk_http /etc/init.d/fsigk_http
# chkconfig --add fsigk_http
# chkconfig fsigk_http on
```

また、systemdの場合:

```
# systemctl enable fsigk_http
```

6.3 プロキシ実行コマンド本体

動作概要

指定した設定ファイルのオプションに従い、プロキシを実行します。

通常、設定ファイルとして/opt/f-secure/fsigk/conf/fsigk.iniを指定します。

コマンド名

```
cd /opt/f-secure/fsigk; ./fsigk
```

注： fsigkコマンドはインストールディレクトリに移動してから実行してください。

オプション

オプションを複数指定した場合は最後のオプションが優先となります。

--http	httpプロトコルを使用(fsigk_httpで起動時のデフォルト)
--smtp	smtpプロトコルを使用(fsigk_smtpで起動時のデフォルト)
--pop	popプロトコルを使用(fsigk_popで起動時のデフォルト)
--ftp	ftpプロトコルを使用(fsigk_ftpで起動時のデフォルト)
-f <inifile>	inifileを設定ファイルとして設定を読み込みます。

通常は/opt/f-secure/fsigk/conf/fsigk.iniを指定します。プロトコルはこのオプションより前に指定する必要があります。

--daemon	バックグラウンドで起動
-q	詳細表示をやめる
-P <port>	指定したポート番号で待ち受ける
-h	オプション一覧を表示

コマンドの例

HTTPプロキシの起動 (通常)

```
# cd /opt/f-secure/fsigk; ./fsigk --daemon --http -f conf/fsigk.ini
```

- フォアグラウンドで起動

```
# cd /opt/f-secure/fsigk; ./fsigk --http -f conf/fsigk.ini
```

- フォアグラウンドで起動
- 詳細情報も表示

```
# cd /opt/f-secure/fsigk; ./fsigk -v --http -f conf/fsigk.ini
```

- フォアグラウンドで起動
- 詳細情報も表示
- ポート9080で待ち受け

```
# cd /opt/f-secure/fsigk; ./fsigk -v --http -f conf/fsigk.ini -P 9080
```

6.4 パターン ファイルのアップデート

ウイルス定義ファイルを最新に更新します。

動作概要

ウイルス定義ファイルはインターネット経由でダウンロードするため、時間がかかることがあります。

プロキシ設定の更新は、/opt/f-secure/fsigk/conf/fsigk.iniの更新に関連する箇所で指定します。

ウイルス定義ファイル更新動作

dbupdateコマンドは、AUA(Automatic Update Agent(自動更新エージェント),コマンド名:fsaua)を通じて、http://fsbwserver.f-secure.com/からファイルを取得し、一度updateディレクトリに保存した後、databasesディレクトリにコピーします。

注: ウイルス定義ファイルのダウンロードが失敗する場合、本製品を導入したサーバから、http://fsbwserver.f-secure.com/に接続してファイルがダウンロードできるかご確認ください。また、ログファイル (/opt/f-secure/fsigk/log/dbupdate.log、/opt/f-secure/fsigk/log/fsaua.log) の内容もご確認ください。

注：設定したプロキシ情報は/opt/f-secure/fsigk/conf/fsigk.iniに以下の項目で保存します。

use_proxy=[yes|no]	プロキシ利用の有無
http_proxy_host	プロキシサーバのホスト名
http_proxy_port	プロキシサーバのポート番号
http_proxyauth	プロキシ認証を利用の有無
http_proxyauth_user	プロキシ認証のユーザ名
http_proxyauth_pass	プロキシ認証のパスワード

注：ポリシマネージャから定義ファイルをダウンロードする場合は、/opt/f-secure/fsigk/conf/fsigk.iniでupdateurl= http://host name:port number/ として指定します。

注：ウイルス定義ファイルのバージョンは"cd /opt/f-secure/fsigk; make show-dbversion"コマンドで確認いただけます。

各エンジン(Aquarius,Hydra(FS-Engine))の定義ファイルのバージョンは、databases/aqulnx32/aquarius-linux-update.ini、databases/fse/FS@hydra.iniの"[Version]... File_set_visible_version=YYYY-MM-DD_XX"を参照します。ウイルス定義ファイル全体のバージョンは、各エンジンのバージョンの中で最大のバージョンになります。

設定ファイル(conf/fsigk.ini)でプロキシ設定を変更した場合、/opt/f-secure/fsigk/libexec/fsigk-reload.shコマンドを実行して設定を更新します。

コマンド名

/opt/f-secure/fsigk/dbupdate

オプション

--help	コマンドラインオプションのクイックヘルプを表示します。

fsdbupdate.run

定義ファイルの更新を、インターネットからダウンロードするのではなく、指定した定義ファイル(fsdbupdate.run)を用いて行います。(定義ファイルのインポートを行います。)

設定ファイル

/opt/f-secure/fsigk/conf/fsigk.ini

use_proxy=[yes|no]	プロキシ利用の有無

`http_proxy_host`	プロキシサーバのホスト名
`http_proxy_port`	プロキシサーバのポート番号
`http_proxyauth`	プロキシ認証を利用の有無
`http_proxyauth_user`	プロキシ認証のユーザ名
`http_proxyauth_pass`	プロキシ認証のパスワード
`updateurl=http://host name:port number/`	ポリシマネージャから定義ファイルをダウンロードする場合のURL

ログファイル

更新結果は、以下のログファイルに記録されます。問題発生時はこちらを参照してください。

- `/opt/f-secure/fsigk/log/dbupdate.log`
- `/opt/f-secure/fsigk/log/fsaua.log`

終了コード

更新結果は以下のコマンド終了コードを使用します。

終了コード	概要
0	新しい更新はありません。何も更新されていません。
1	定義ファイル更新に失敗しました。詳細については、プログラムの出力および/opt/f-secure/fsigk/log/dbupdate.log、/opt/f-secure/fsigk/log/fsaua.logを参照してください。
2	ウイルス定義ファイルは正常に更新されました。

注：128以上の数字はシグナルにより終了した場合です。たとえば143の場合、143-128=15(SIGTERM)がシグナルです。詳細が必要な場合、Linuxのシグナル番号を"`man 7 signal`"コマンドなどで確認してください。

コマンド例

ウイルス定義ファイルを更新します。

```
# cd /opt/f-secure/fsigk; ./dbupdate
```

指定した定義ファイル(fsdbupdate.run)からインポートします。

```
# cd /opt/f-secure/fsigk; ./dbupdate fsdbupdate.run
```

6.5 全サービス再起動コマンド

動作概要

全ての有効なサービス(http、smtp、pop、ftp、admin)を再起動します。

コマンド名

```
cd /opt/f-secure/fsigk; make restart
```

コマンド例

全ての有効なサービスを再起動します。

```
# cd /opt/f-secure/fsigk; make restart
```

6.6 診断情報作成コマンド

動作概要

診断情報ファイル(diag.tar.gz)を、/opt/f-secure/fsigkディレクトリに作成します。診断情報ファイルには本製品の設定情報・マシンの設定情報・各種ログ情報が含まれます。これらの情報は、問題解析のために必要です。

ヒント:サポートセンターへお問い合わせの際は、なるべくこの診断情報ファイル(diag.tar.gz)をお送りいただきますようお願いします。

コマンド名

```
cd /opt/f-secure/fsigk; make diag
```

コマンド例

診断情報ファイルを作成します。

```
# cd /opt/f-secure/fsigk; make diag
```

第 章
7

ログ

トピック：

本製品では、アクセス状況の把握、ウイルス検出状況、エラー発生状況などの情報をログファイルとして残します。

ログファイルは、`/opt/f-secure/fsigk/log/`の各サービスごとのディレクトリに保存されます。必要に応じて参照してください。

7.1 ログファイル

7.1.1 アクセスログ (access.log)

本製品を通じてサーバへの接続を行った記録を全て保存します。

本製品のログはSquidログと互換性のある形式で保存されます。ログの形式は以下のとおりです。

ログフォーマット

接続状況が1行ずつ記録されます。以下の各項目がスペースで区切られています。

時刻 クライアントから接続された時刻です。エポックタイム(1970/01/0100:00:00(UTC))からの秒数をミリ秒単位で表示します。

接続時間 クライアントとの接続時間をミリ秒単位で表示します。

クライアントホスト クライアントのホストが表示されます。逆引きが可能な場合はホスト名が表示され、それ以外はIPアドレスが表示されます。

処理結果 [キャッシュ状況]/[HTTP状態コード]を返します。

キャッシュ状況は利用しません。常にTCP_MISSです。HTTP状態コードは、クライアントに送信するHTTP応答の状態コード(3桁の数字)です。HTTP以外では成功時は200、エラー時は500、それ以外(データ中継を行わずに接続直後に切断した場合など)は000を返します。

ファイルサイズ 転送したファイルのサイズです。

要求メソッド HTTPではHTTPの要求メソッド(GET, POSTなど)です。FTPのデータ送信時はPUTです。それ以外では常にGETです。

URL 接続先のURLです。popの場合は、"pop://POPユーザ名@POPサーバ名:ポート番号"になります。 smtpの場合は"mail:送信先"になります。

ユーザ名 プロキシ認証を行った場合のユーザ名が記録されます。認証を行っていない場合は"-"です。

Hierarchy code "[Hierarchy文字列]/接続先IPアドレス"を返します。[Hierarchy文字列]は利用しません。常に"DIRECT"です。

Content-Type 送受信するファイルのContent-Typeを表示します。利用できない場合は"-"となります。

検出情報 "DETECT-STAT:[スキャン結果]:[ウイルス名]:[ファイル名]:[隔離保存ファイル名]::"を返します。

スキャン結果	INFECTED(ウイルス検出)、SPAM(スパム検出)、CLEAN(ウイルス検出なし)のいずれか
ウイルス名	ウイルス名称
ファイル名	送受信ファイルにつけられた名前

	隔離保存ファイル名	隔離保存したファイル名 感染ファイルの隔離を有効にした場合のみ設定されます。

動作

"ACTION:[動作]:" を返します。

動作	スキャン結果に応じた以下の動作のいずれかを返します。

NONE	何もしない(検出しなかった)
PASS	検出したが何もしなかった (ログした)
DELETE	削除した (SMTP の場合、削除後受信者へ通知)
DENY	SMTPまたはアクセスした URL で検出してブロックした
SENDBACK	SMTPで送信者へ通知した
BLACKHOLE	SMTP で削除した(送受信者への通知なし)
CHANGE_SUBJECT	SMTPでスパム検出により件名を変更した

プロキシ情報

"PROXY-STAT:[サービスの種類]:[内部プロセスID]: [プロセスID]: [接続元IPアドレス]: [処理ファイル数] :[スキャン回数]: [スキャン時間]:[スキャン情報詳細]:" を返します。

サービスの種類	サービスの種類 (http、 smtp、 pop、 ftp)
内部プロセスID	プロセスで使用される内部プロセスID(識別子は 0 で始まります) を示します。
プロセスID	処理を行ったプロセスID
接続元IPアドレス	接続元のIPアドレス
処理ファイル数	同一セッション内で処理した要求の数。1 から始まり、同一セッション内でアクセスログに出力する度に づつ増えます。POP では常に1です。

スキャン回数	このリクエストは対して実行されたウイルスのチェック
スキャン時間	リクエストから過ぎたスキャン時間(ミリ秒)
スキャン情報詳細	スキャン状況を表す以下の文字列をコンマ区切りで表示します。

VSD_ENCRYPTED	暗号化ファイル
VSD_MAXNESTED	最大スキャン階層に到達した
VSD_SCANTIMEOUT	スキャン時間が最大スキャン時間を越えた
OVER_FILESIZE	スキャン除外対象で指定したファイルサイズを超えた
PASS_TO	スキャン除外対象のホスト名に一致した
PASS_USER_AGENT	スキャン除外対象のUser-Agentに一致した
PASS_EXT	スキャン除外対象のファイル名・拡張子に一致した (HTTP、FTPのみ)

プロトコル情報

各プロトコル独自の情報を記録します。現在HTTP/SMTPサービスのみで有効です。

- **SMTPサービスの場合**

  "PROTOCOL-STAT:[送信元アドレス]:[Message-ID]:" を返します。

送信元アドレス	SMTPの送信者アドレス ("MAIL FROM:" コマンドの引数アドレス) (URLエンコードを行い表示します。)
Message-ID	メールヘッダのMessage-Idフィールド (URLエンコードを行い表示します。)

- **HTTPサービスの場合**

  "PROTOCOL-STAT:[プロトコル情報詳細]:[X-Forwarded-For]:" を返します。

KEEPALIVE	スキャン状況を表す以下の文字列をコンマ区切りで表示します。 **KEEPALIVE** 該当セッションでKeep-Alive Persistent-Connection 接続を行った。 **PROGRESS** 該当セッションでダウンロード状況表示ダイアログを表示した。(上級者向けオプションで"progress"の設定を行った場合) **TRICKLE** 該当セッションでtrickleによりダウンロード完了前に転送を開始した。(上級者向けオプションで"trickle"の設定を行った場合)
X-Forwarded-For	要求ヘッダのX-Forwarded-Forフィールドの値(URLエンコードを行い表示します。)

エラー情報 プロキシ処理により発生したエラーメッセージを表示します。"PROXY-ERROR:[エラーメッセージ]:" を返します。

エラーメッセージ	以下のエラーメッセージが表示されます(URLエンコードを行い表示します。) **CONNECT** ホスト名: ポート番号/接続エラーメッセージ。HTTPとSMTPプロトコルに共通。 **HTTP** HTTPエラー応答メッセージが表示されます。 **SMTP** **SERVER/ERROR Reply(MAIL)** buf=[XXX] SMTPサーバへ"MAIL FROM"コマンドを送信した際のエラー応答 **SERVER/ERROR Reply(RCPT)** buf=[XXX] SMTPサーバへ"RCPT TO"コマンドを送信した際のエラー応答 **SERVER/ERROR Reply(AUTH)** buf=[XXX] SMTPサーバへ"AUTH"コマンドを送信した際のエラー応答 **PROXY/550 Relaying denied** インターネット ゲートキーパが中継を拒否した。受信先ドメインの制限や認証により拒否された場合に表示されます。(クライアントからの中継を許可する場合、該当クライアントアドレスをLAN内からのホストに設定するか、PbS/SMTP認証を有効にします。外部からの中継を許可する場合、受信先ドメインを設定します。)

7.1.2 ウイルス・スパム検出ログ detect.log

ウイルス・スパムの送受信を検出した場合に記録します。

注: ログの形式はアクセスログと同じです。

7.1.3 エラーログ (error.log)

エラー発生時に記録されます。本製品の動作に問題がある場合などに参照してください。

エラーメッセージの形式は以下のとおりです。

エラーメッセージの形式

- 時刻 (秒数)

- 内部プロセスID
- ログレベル
- [内部パス情報]
- [クライアントアドレス/クライアントポート番号/クライアント側のファイル情報]
- [サーバアドレス/サーバポート番号/サーバ側のファイル情報]
- エラーメッセージ

時刻はエラー発生時の時刻です。時刻はエポックタイム (1970/01/01 00:00:00(UTC)) からの秒数を秒単位とマイクロ秒単位で表示します。

また、OSのシステムコールに関係するエラーが発生した場合、エラーメッセージの前に以下の記述が追加されます。`System call=Error message(Error code)`

- System call: the call that failed
- Error message: error message for system calls
- Error code: error code for system calls

注： エラーメッセージの内容についてはF-Secureのナレッジベースを参照してください。
http://community.f-secure.com/t5/E-mail-and-Web/Internet-Gatekeeper-error-logs/ta-p/17436

7.1.4 情報ログ (info.log)

その他の一般的な情報が情報ログ (`info.log`) に記録されます。

メッセージの形式

- 時刻 (秒数)
- 内部プロセスID
- ログレベル
- [内部パス情報]
- [クライアントアドレス/クライアントポート番号/クライアント側のファイル情報]
- [サーバアドレス/サーバポート番号/サーバ側のファイル情報]
- メッセージ

日時はエラー発生時の時刻です。最初の時刻はエポックタイム (1970/01/01 00:00:00(UTC)) からの秒数をミリ秒単位で表示します。

注： メッセージの内容についてはF-Secureのナレッジベースを参照してください。
http://community.f-secure.com/t5/E-mail-and-Web/Internet-Gatekeeper-error-logs/ta-p/17438

7.2 F-Secure Anti-Spam デーモンとSyslogの使用

F-Secure Anti-Spam デーモンの処理はデフォルトのシステムログに記録できます。

F-Secure Anti-Spam デーモン (fsasd) のSyslogオプションを設定する方法

`/opt/f-secure/fsigk/conf/fsigk.ini`設定ファイルを編集し、`fsasd_syslog_facility`オプションを指定します。
ログされる値はデフォルトで `LOG_LOCAL0` です。

注： 詳細についてはSyslogのドキュメンテーションを参照してください。

7.3 ログの分割 ローテート

ログファイルは通常1つのファイルとして保存し、分割されることはありません。分割を行う場合は `logrotate`コマンドを使用します。

サンプル用の設定ファイルを元に以下の手順で設定を行ってください。

1. 設定ファイルの設置
   サンプル設定ファイル(`/opt/f-secure/fsigk/misc/logrotate.fsigk`)を `/etc/logrotate.d/fsigk`. にコピーしてください。

```
# cp /opt/f-secure/fsigk/misc/logrotate.fsigk /etc/logrotate.d/fsigk
```

2. 設定ファイルの編集
   必要に応じてローテート間隔などを設定してください。
3. 動作確認
   以下のコマンドを実行し、ローテートが行われることを確認してください。

```
# logrotate -f /etc/logrotate.d/fsigk
```

7.4 時刻表示変換ツール (logconv)

多くのログの時刻表示がエポックタイムからの秒数で表示されていますが、logconvツールで年月日時分秒表示を行頭に追加できます。

logconvツールは以下のように実行します。オプションは省略可能です。

```
# /opt/f-secure/fsigk/misc/logconv <Log file name>
```

Windows上で実行する場合、"`/opt/f-secure/fsigk/misc/logconv.exe`" を利用いただけます。

オプション

`--tail [num]`	最後の [num] 行を出力します
`--tailsec [sec]`	最後の [sec] 秒分を出力します。
`--cgi`	CGIから呼び出す場合に利用します。
`--today`	本日分のログを出力します。
`--noconv`	時刻変換を行いません。
`-r`	変換後のデータを変換前のデータに戻します。

変換結果は標準出力に表示されます。`--tail <num>`オプションを指定するとログの最後からの指定行数のみ表示します。

7.5 アクセス解析ツールの設定 (webalizerなど)

本製品のアクセスログはSquid互換形式となっているため、webalizerなどのSquidに対応したログ解析ツールを利用いただけます。

webalizerを使用して毎日アクセス解析を行う場合、以下のコマンドで空の設定ファイルを作成します。

```
# touch /opt/f-secure/fsigk/log/{http,smtp,pop,ftp}/logtool/webalizer.conf
```

また、crontabを以下のように設定します。

```
0 1 * * * cd /opt/f-secure/fsigk/log/http/logtool/;
/usr/bin/webalizer ../access.log -F squid -o .
```

ログの結果は/opt/f-secure/fsigk /log/http/logtool/ディレクトリに保存されます。

注: 必要に応じてウイルス情報も追加表示するソースパッチ(misc/webalizer-xxx.detect-stat.patch-xxx)もご利用ください。 パッチの適用例

```
# tar -zxvf webalizer-2.xx-xx-src.tgz
# patch -p1 < webalizer-2.xx-xx.detect-stat.patch-x.xx
# ./configure
# make
# make install
```

ヒント: また、商用ログ解析ツールとしてSawmillなどが本製品に対応しています。ウイルス情報を含めた詳細なログ解析を行う場合など、必要に応じて導入してください。Sawmillの製品情報は以下を参照してください。http://www.sawmill.net/.

7.6 ログの外部出力設定 (syslogなど)

ログは通常ファイルとして保存されますが、必要に応じてsyslogなどのファイル以外への出力が可能です。外部への出力は、外部コマンドにパイプを通じて送信することで行います。

設定は、設定ファイル(/opt/f-secure/fsigk/conf/fsigk.ini)に以下のように記述することで行います。

- アクセスログの場合: access_log=|<外部コマンド>
- ウイルスログの場合: detect_log=|<外部コマンド>
- 情報ログの場合: info_log=|<外部コマンド>
- エラーログの場合: error_log=|<外部コマンド>

たとえば、SMTPのウイルス検出情報、エラー情報をsyslogのlocal0ファシリティ、errレベルに出力する場合、/opt/f-secure/fsigk/conf/fsigk.iniの[smtp]グループに以下のように設定を追加します。

```
[smtp]
detect_log=|logger -t fsigk -p local0.err
error_log=|logger -t fsigk -p local0.err
```

ファイル出力も同時に行う場合は、以下のように設定します。

```
[smtp]
detect_log=|tee -a log/smtp/detect.log | logger -t fsigk -p local0.err
error_log=|tee -a log/smtp/error.log | logger -t fsigk -p local0.err
```

設定ファイル変更後は、/opt/f-secure/fsigk/rc.fsigk_{http,smtp,pop,ftp} restartコマンドによりサービスの再起動を行います。

第 章

8

その他の設定例

トピック：

ここでは、製品に設定できるその他の設定について説明します。

通常は一般的な設定例で十分なセキュリティ対策を構築できますが、その他の設定方法が必要な場合はこの章をご利用ください。

8.1 接続元認証の設定例

インターネットからインターネットゲートキーパへの接続を行う場合、不正利用を防ぐため、必要に応じて接続元の認証を行います。

8.1.1 アクセス元ホスト (IPアドレス、ホスト名) による認証

アクセス元ホストが固定されている場合、IPアドレスまたはホスト名によるアクセス制限が可能です。

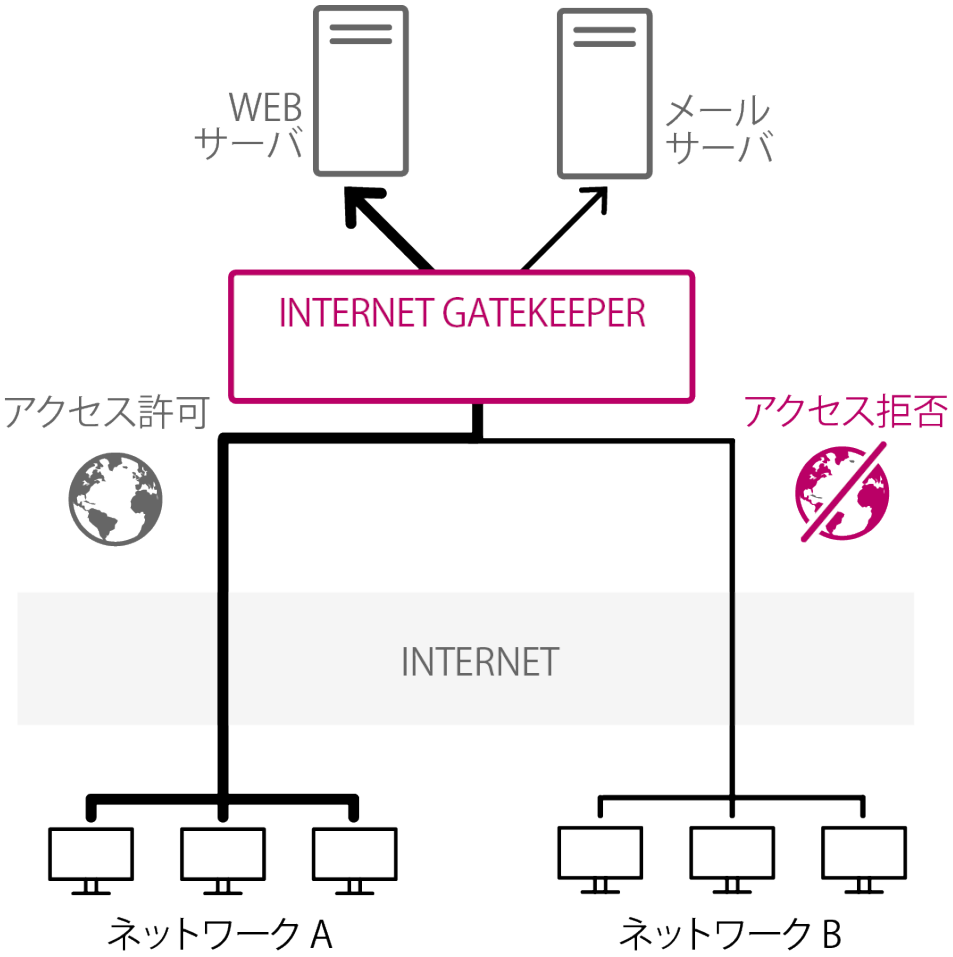


図 6 : IPアドレスによるアクセス制御の設定

また、LinuxのIPフィルタリング設定 (iptables) でアクセス制限を行うことも可能です。

プロキシのアクセス制御による設定

ここでは、192.168.1.0/255.255.255.0からの接続のみ受け付ける場合についての設定例を示します。

設定は、[**Access Control**] または [アクセス制御] 項目で行います。また、ホスト名による制限を行う場合は、[DNS Reverse Lookup] または [**DNS逆引き**] を有効にする必要があります。

HTTPプロキシ、**SMTPプロキシ**、**POPプロキシ**、**FTPプロキシ**の**アクセス制御**設定を編集します。

- **接続元 (acl_from)**: 有効 (例: 192.168.1.0/255.255.255.0)
- **DNS逆引き (reverselookup)**: ホスト名で制限する場合は有効にする

IPフィルタリングによる設定 (iptables)

IPアドレスによる制限はiptablesを使用して行うことも可能です。この場合、以下のように設定を行ってください。

```
# iptables -A INPUT -s 192.168.1.0/255.255.255.0 -j ACCEPT
# iptables -A INPUT -j DROP
```

8.1.2 仮想ネットワーク SSH/VPNなど を利用した認証

まず、クライアントとインターネットゲートキーパ間で、あらかじめ仮想ネットワーク (SSH/VPNなど) を使用して認証済みのTCP/IP通信路を構築します。

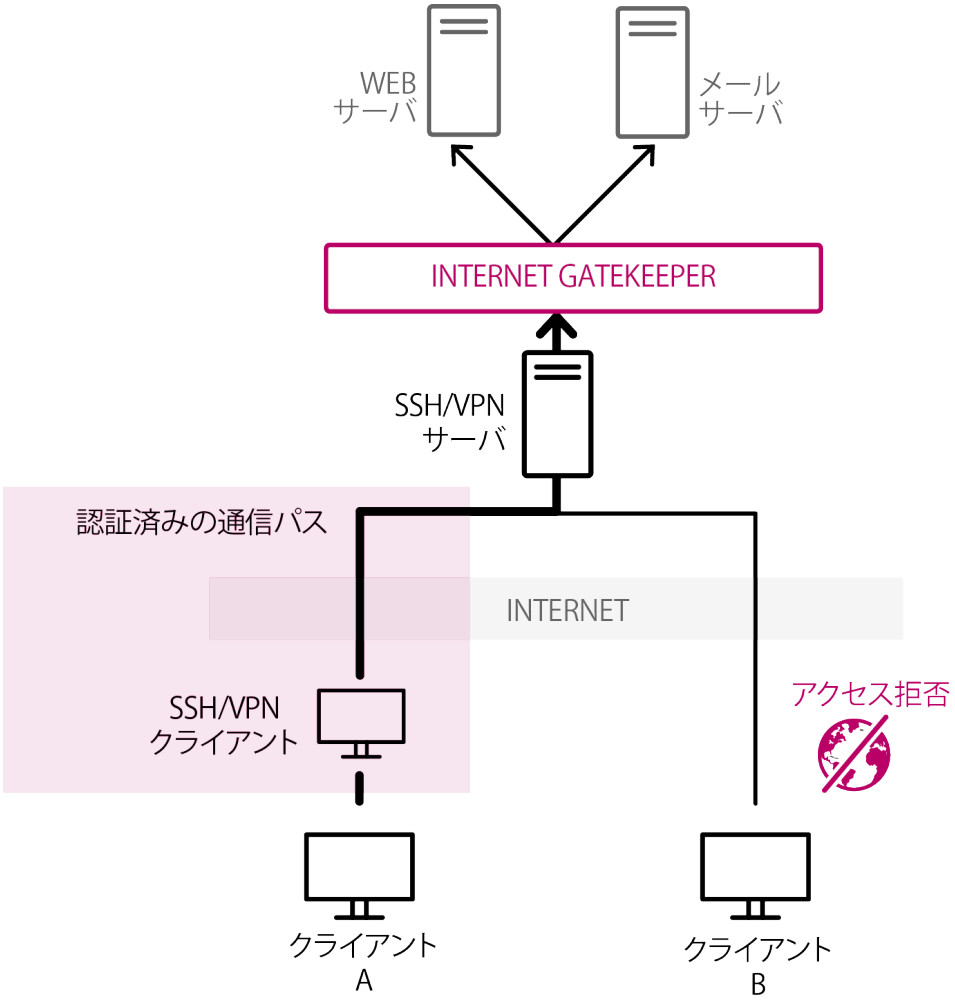


図7: クライアントからインターネットゲートキーパへの接続は、この認証済みの通信路上で行います。これにより、認証されたクライアントからの接続のみを受け付けるようになります。

ここでは、SSH (openssh, TTSSHなど) を使用した場合の設定の概略を説明します。

設定

1. インターネットゲートキーパまたはインターネットゲートキーパを含む接続先ネットワーク上のマシンに、SSHサーバをインストールします。

   注: 特定の Linux ディストリビューション (Red Hat7以降など) では、opensshがデフォルトで導入済みです。

2. クライアントまたはクライアントを含む接続元ネットワーク上のマシンに、SSHクライアントをインストールします。

3. SSHクライアントのポートフォワード設定により、localhost宛の接続がインターネットゲートキーパ宛になるように設定します。

   Configファイルは以下のように設定します。

   この例では、SSHサーバホストがssh-server、SSHのユーザ名がssh-username、インターネットゲートキーパホストがfsigkになります。

```
Host ssh-server
 User ssh-username
 LocalForward 25 fsigk:25
 LocalForward 110 fsigk:110
 LocalForward 9080 fsigk:9080
```

4. SSHクライアントからSSHサーバに接続します。
5. ウェブブラウザのプロキシ設定、メールクライアントの設定を変更します。
   - ウェブブラウザのプロキシ設定: http://localhost:9080/
   - SMTPメールサーバ: localhost
   - POPメールサーバ: localhost
6. ウェブの閲覧、メールの送受信でウイルススキャンが行えることを確認してください。

8.1.3インターネットゲートキーパでのプロキシ認証(HTTP、SMTP、POP、FTP)

インターネットゲートキーパが、各ユーザの入力によるパスワード認証を行います。HTTPサービスではHTTPプロキシ認証、SMTPサービスではSMTP認証、POPサービスではPOPユーザ名、FTPサービスではFTPユーザ名による認証が行えます。

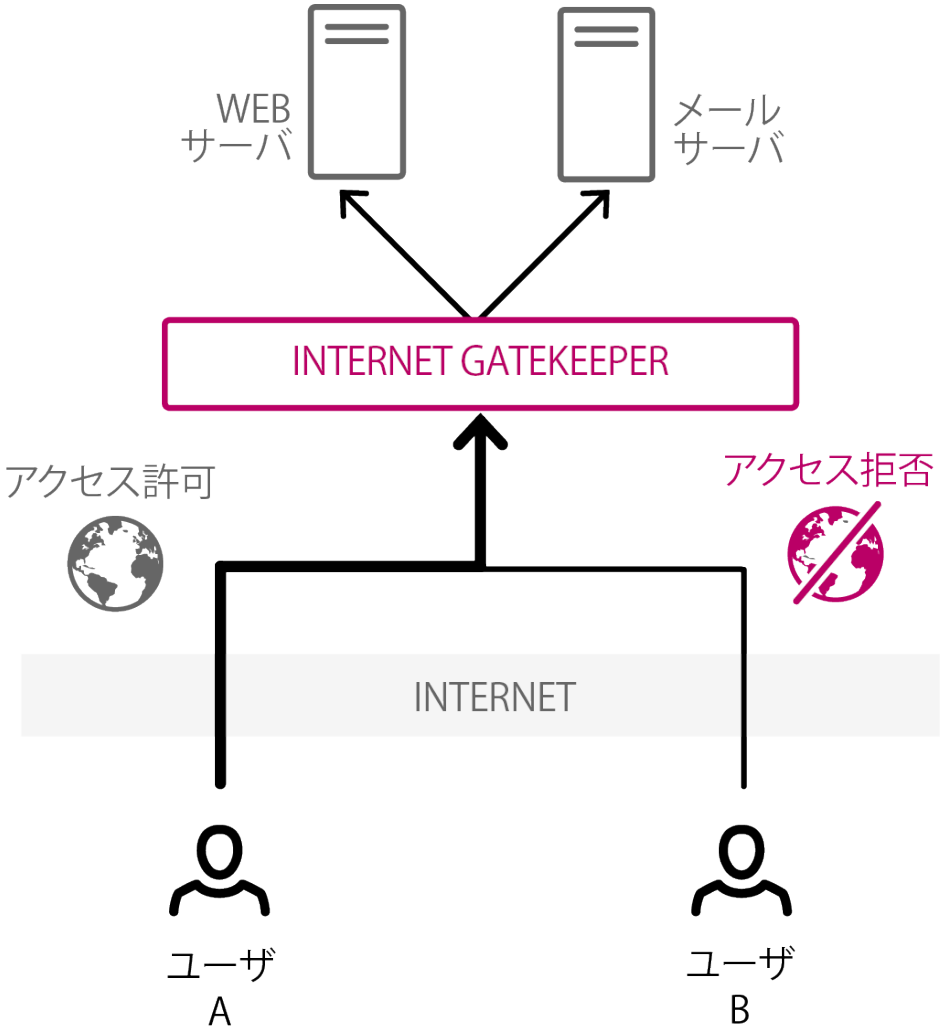


図 8 : ユーザの認証

ユーザ認証 (PAM認証)

各プロキシの設定で接続を許可するユーザを編集できます。

POP、FTPサービス

POP、FTPについては、「ユーザデータベース」でユーザ名を確認し、必要に応じて設定します。

複数サーバを使用する場合は、"ユーザ名@サーバ名" を指定します。指定したサーバの全てのユーザの利用を許可する場合は、"@サーバ名" と入力します。

👉 **注:** ユーザ名は、クライアント側で設定するユーザ名です。パスワードは、サーバ側の認証をそのまま利用します。

設定内容は、`/opt/f-secure/fsigk/conf/pam/userdb.txt` ファイルに保存されます。

直接編集する場合は、`create_userdb userdb.db < userdb.txt`コマンドでデータベースファイルのuserdb.dbを更新します。

さらに、PAM設定ファイル(/etc/pam.d/fsigk_{http,smtp,pop,ftp})を編集することで、UNIXアカウント、NIS、LDAP、Radiusなどの外部の認証方式を使用できるようになります。

PAM設定ファイルは、/opt/f-secure/fsigk/conf/pam/fsigk_{http,smtp,pop,ftp}.pamのシンボリックリンクとなっています。PAM設定を変更した場合、/etc/pam.d/fsigk_{http,smtp,pop,ftp}のシンボリックリンクを削除し、/opt/f-secure/fsigk/conf/pam/fsigk_{http,smtp,pop,ftp}.pamのコピーを作成し、別ファイルとして編集してください。

注: /opt/f-secure/fsigk/conf/pam/fsigk_{http,smtp,pop,ftp}.pamのファイルはアップデート時に上書きされるため、編集しないでください。アップデート時の上書きを防ぐため、編集する場合はシンボリックリンクを切り離してコピーを作成してから編集してください。

HTTPプロキシ、**SMTPプロキシ**、**POPプロキシ**、**FTPプロキシ**にある次のプロキシ設定を編集します。

- **{HTTP,SMTP,POP,FTP} proxy authentication (proxyauth_pam_auth)=yes**
- **(ユーザ情報)**: **ユーザデータベース**でユーザの追加・削除・編集を行います。

8.1.4 メールサーバによる認証 (POP認証、SMTP認証)

メールサーバ側でのPOP認証、SMTP認証を利用します。インターネットゲートキーパはクライアントからの接続時にメールサーバと接続するプロキシとして動作するため、メールサーバ側のPOP認証、SMTP認証によるユーザ認証機能をそのまま利用することができます。

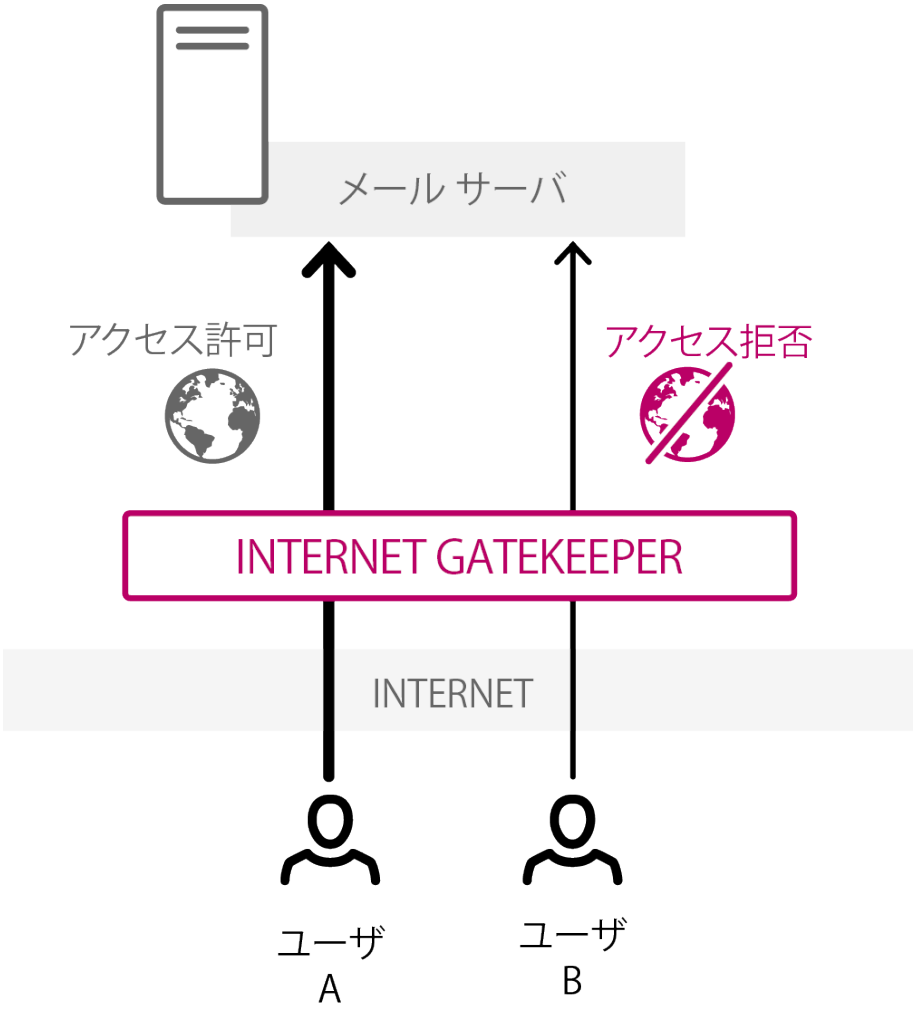


図 9 : メールサーバ上のSMTP認証。

なお、メールサーバ側のSMTP認証を利用する場合は、インターネットゲートキーパでのSMTP認証設定を無効にしてください。以下の方法で行います。

1. 設定ファイル`/opt/f-secure/fsigk/conf/fsigk.ini`をコマンドラインから開きます。
2. [**SMTPプロキシ**] で`proxyauth_pam_auth=no`を設定するとSMTP認証を無効にします。

また、APOPを利用する場合は、インターネット ゲートキーパでの親サーバのユーザによる指定を無効にしてください。以下の方法で行います。

1. 設定ファイル`/opt/f-secure/fsigk/conf/fsigk.ini`をコマンドラインから開きます。
2. **POPプロキシ**で、`self_proxy=no`を設定すると[**親サーバのユーザによる指定**]を無効にできます。

注: APOPについては、プロトコル仕様上、プロキシ型で[**親サーバのユーザによる指定**]を有効にした場合利用できません。APOPを利用する場合、以下のいずれかの方法で対応してください。

- [**親サーバのユーザによる指定**] を無効にする。
- POPプロキシで`self_proxy=no`を設定します。
- 透過プロキシを利用する。

8.1.5 POP before SMTPによる認証

SMTPサービスへの接続をPOP before SMTPにより行うことができます。この場合ユーザは、まずPOPサービスへの接続でユーザ認証を行い、その後SMTPサービスへの接続を行います。

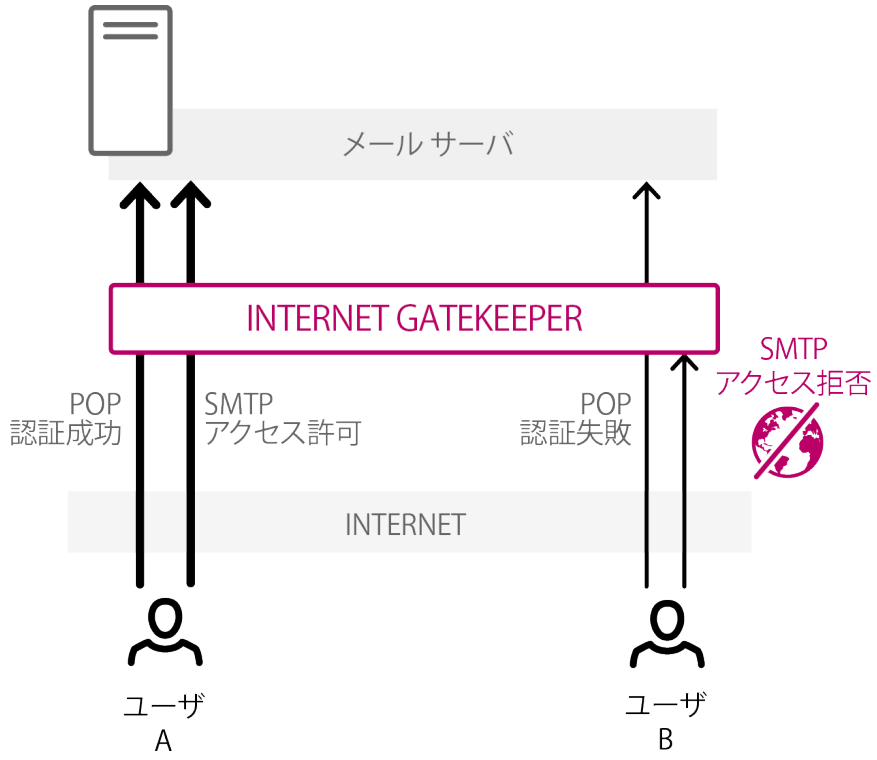


図 10 : POP before SMTP認証。

SMTPサービスへは、一定時間内にPOPサービスでのユーザ認証に成功したIPアドレスからの接続のみに制限されます。また、メールサーバの接続元IPアドレスは常にインターネットゲートキーパになるため、POP before SMTP認証はインターネットゲートキーパで行います。

POP-before-SMTP 認証を使用するには、SMTP と POP サービスを有効にし、`/opt/f-secure/fsigk/conf/fsigk.ini` ファイルに次の変更を適用します:

1. POP-before-SMTP 認証を有効にするには、`smtp` と `pop` の下にある `pbs=yes` を両方設定します。
2. `smtp` の下にある `pbs_lifetime` フィールドで認証を有効にする時間 (分単位) を指定します。

   例: `pbs_lifetime=2`

3. `/opt/f-secure/fsigk/libexec/fsigk-reload.sh` コマンドを実行して構成を再ロードします。

POP before SMTP認証のデータベースファイルは以下のように保存されます。

データベース形式:	BerkeleyDB 1.85
保存先ディレクトリ:	一時ディレクトリ (デフォルト: `/var/tmp/fsigk`)
保存ファイル名:	`pbs.db`
キー:	クライアントIPアドレス

データ:	POP認証時刻 (エポックタイム (1970/1/1 00:00:00) からの秒数)

注： 現在のデータベースの内容は、"db1_dump -p pbs.db" で確認できます。

重要： サービス再起動時は、POP before SMTPデータベースの内容は全て削除されます。

8.1.6 SMTP アクセス制御

SMTPプロキシはドメインベースのアクセス制御に対応しています。アクセス制御を有効にすると、ユーザが認証されていない場合にはプロキシはメールを許可されているドメインにのみ配信します。

アクセス制御を使用するには、/opt/f-secure/fsigk/conf/fsigk.ini ファイルの smtp の部分で次の変更を適用してください:

1. acl_rcpt=yes を有効にするとドメイン ベースのアクセス制御を有効にできます。
2. smtp_rcpt フィールドを変更すると許可するドメインを指定できます。
3. /opt/f-secure/fsigk/libexec/fsigk-reload.sh コマンドを実行して構成を再ロードします。

製品はローカル ネットワーク内でアクセス制御から除外されているクライアントの一覧を管理できます。

LAN機能を使用するには、/opt/f-secure/fsigk/conf/fsigk.ini ファイルのsmtpの部分で次の変更を適用してください:

1. lan=yes を設定すると LAN 機能を有効にできます。
2. lan_hosts フィールドを編集するとローカル エリア ネットワークにあるホストを指定えきます。
3. /opt/f-secure/fsigk/libexec/fsigk-reload.sh コマンドを実行して構成を再ロードします。

また、ウェブ インタフェースの [**SMTP**] から次の変更を適用することでも設定を変更できます。

1. **LAN アクセス**の設定を有効にします。
2. [**Hosts and networks within LAN**] フィールドを編集するとローカル エリア ネットワークにあるホストを指定えきます。

ドメインとホストの構文については、アクセス制御の説明を参照してください。

8.2 透過プロキシの設定例

本製品は、HTTP, FTP, SMTP, POPの各サービスに対して透過プロキシとして動作することができます。これにより各ユーザの設定を全く変更することなしに、任意のHTTP, FTP, SMTP, POPサーバへの接続に対してウイルススキャンを行うことができます。

通常のプロキシ設定、DNS設定によりインターネットゲートキーパのホスト名をメールサーバのホスト名にした場合、透過プロキシ (ルータ型、ブリッジ型) で必要な設定範囲は以下の表のとおりです。

設定	プロキシ型		透過プロキシ モード	
	設置のみ	メールサーバのDNS設定変更	ルータ型	ブリッジ型

設定				プロキシ型		透過プロキシ モード	
クライアント	POP	ユーザ名	特定サーバ	○	○	○	○
			任意サーバ	x	x	○	○
		サーバホスト名	特定サーバ	x	○	○	○
			任意サーバ	x	x	○	○
	SMTP	サーバホスト名	特定サーバ	x	○	○	○
			任意サーバ	該当なし	該当なし	○	○
	HTTP/FTP	プロキシサーバ名		x	x	○	○
	ウイルススキャンの解除			はい	はい	該当なし	該当なし
ネットワーク	DNS			○	x	○	○
	ルーティング			○	○	x	○
Proxy	親サーバ設定			x	x	○	○
	IP アドレス設定			x	x	x	x
	NAT (iptables) 設定			○	○	x	x
	カーネル設定			○	○	○	x

注: ネットワークの構成にサブネットが存在する場合、必要に応じてルータの設定を適用してください。

注： FTP over HTTPは透過プロキシモードでは対応されていません。

8.2.1 透過プロキシの設定の概要

通常、クライアントはウェブサーバやメールサーバに直接接続します。インターネットゲートキーパを透過プロキシとして利用し、ウイルススキャンを行う場合、インターネットゲートキーパをサーバとクライアント間のIPルーティング上に設置する必要があります。

インターネットゲートキーパはクライアントからサーバへの接続を横取りし、インターネットゲートキーパから改めてサーバに接続することでサーバへの接続を強制的に中継し、中継時にウイルススキャンを行います。クライアントは、設定を変更せずに通常どおり任意のサーバに直接接続するだけでウイルススキャンを行えます。

接続例

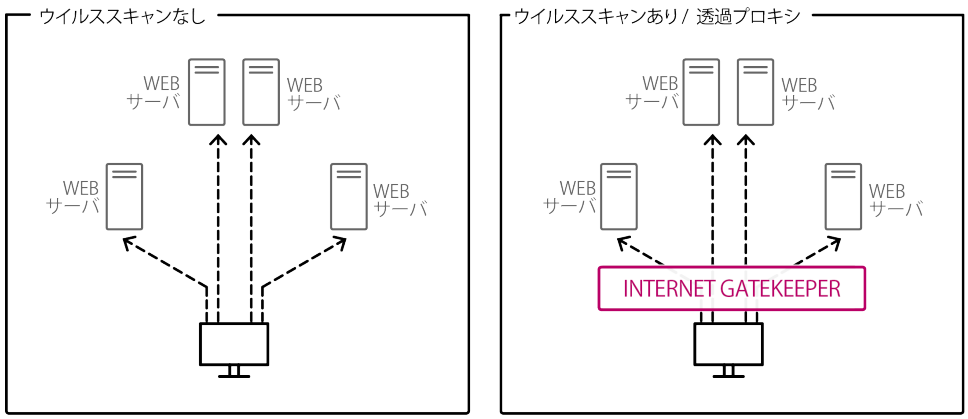


図 11 : 透過プロキシのウェブサーバアクセス方法

8.2.2 透過プロキシの設定例 (ルータ型)

透過プロキシをルータ型で利用する場合は、クライアントから各サーバへのルーティング上にインターネットゲートキーパを設置する必要があります。

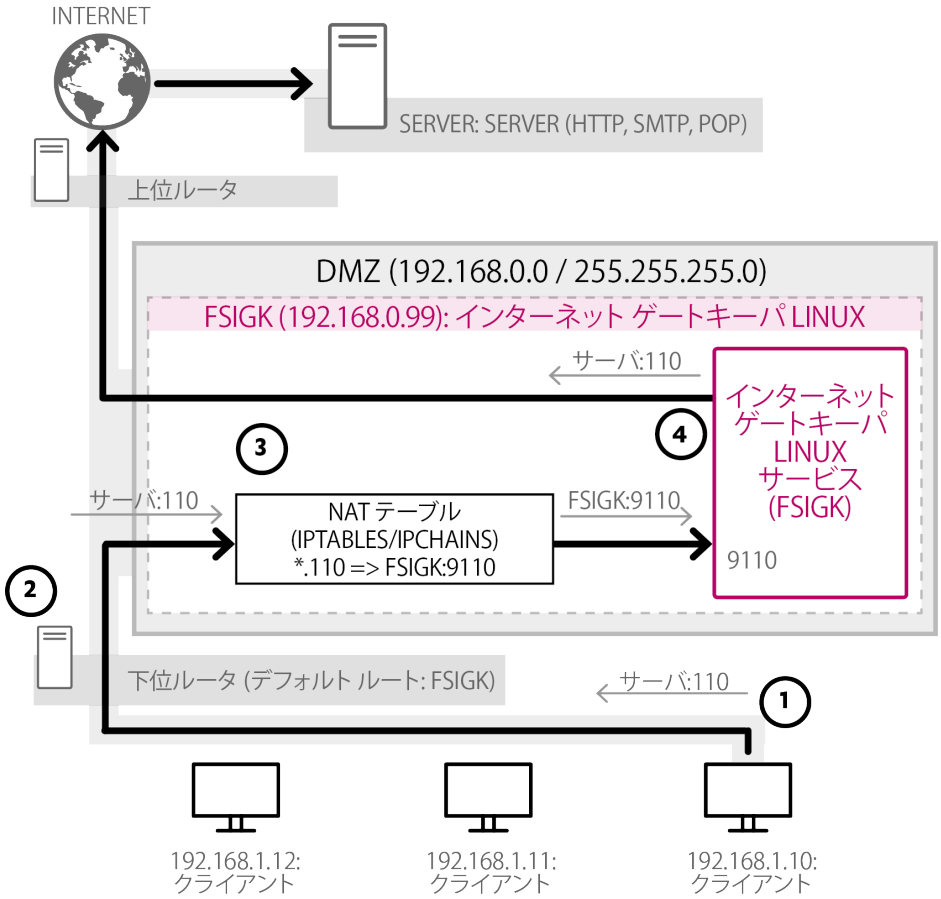


図 12 : DMZネットワークで透過プロキシの設定 (ルータ型)

動作概要

本製品を透過プロキシとして動作させた場合、クライアントからサーバへの接続は以下のように処理します。

1. クライアントは、サーバ (SERVER) のサービスポート番号 (例: 110) に向けて接続を開始する。

2. 下位ルータは、クライアントからの接続要求を、デフォルトルートに設定されたインターネットゲートキーパ・サーバ (FSIGK) に中継する。
3. FSIGKではiptablesのNAT設定により、クライアントからSERVER:110への接続要求をFSIGK:9110への接続要求に置き換え、元の接続先 (SERVER:110) を記憶する。
4. インターネットゲートキーパ・サービス (FSIGK) は、FSIGK:9110で接続を待ち受け、iptablesで置き換えられた接続要求を受け付ける。その後、iptablesから記憶された元の接続先 (SERVER:110) を取り出し、元の接続先 (SERVER:110) に接続要求を出す。

設定

本製品を透過プロキシモードで動作させる場合、以下の手順でネットワークおよびインターネットゲートキーパ・サーバの設定を行います。

1. 設定ファイル`/opt/f-secure/fsigk/conf/fsigk.ini`のプロキシ設定で、各サービスを透過プロキシモードで立ち上げます。
   - **HTTP proxy (http_service)=yes**
     - Port Number (svcport)=9080
     - Transparent proxy (transparent)=yes
   - **SMTP proxy (smtp_service)=yes**
     - Proxy port (svcport)=9025
     - Transparent proxy (transparent)=yes
   - **POP proxy (pop_service)=yes**
     - Port Number (svcport)=9110
     - Transparent proxy (transparent)=yes
   - **FTP proxy (ftp_service)=yes**
     - Port Number (svcport)=9021
     - Transparent proxy (transparent)=yes

   設定を行った後は、クライアントからインターネットゲートキーパ・サーバの各サービスのポート番号 (9080、9025、9110、9021) に接続できることを確認してください。
2. インターネットゲートキーパ・サーバのiptablesを変更することで、クライアントからの接続先を接続先サーバからFSIGK:9110に変更します。
   a. 不要なipchainsが動いていてiptablesが動作していない場合、以下のようなコマンドでiptablesを正しく動作させます。

   ```
   FSIGK# /etc/rc.d/init.d/ipchains stop
   FSIGK# chkconfig ipchains off
   FSIGK# /etc/rc.d/init.d/iptables restart
   ```

   また、`systemd`の場合:

   ```
   FSIGK# systemctl stop ipchains
   FSIGK# systemctl disable ipchains
   FSIGK# systemctl restart iptables
   ```

   b. 任意のサーバへの各サービス (http(80)、smtp(25)、pop(110)、ftp(21)) への接続を、FSIGKの9080, 9025、9110、9021に変更するため、以下のようなコマンドを実行します。

   ```
   FSIGK# iptables -t nat -A PREROUTING -p tcp --dport 80 \
    -j REDIRECT --to-port 9080
   FSIGK# iptables -t nat -A PREROUTING -p tcp --dport 25 \
    -j REDIRECT --to-port 9025
   FSIGK# iptables -t nat -A PREROUTING -p tcp --dport 110 \
    -j REDIRECT --to-port 9110
   ```

```
FSIGK# iptables -t nat -A PREROUTING -p tcp --dport 21 \
 -j REDIRECT --to-port 9021
```

c. iptables の構成を保存します。詳細な説明については、Linux ディストリビューションのマニュアルを参考にしてください。

注： これらのiptablesの設定は "/opt/f-secure/fsigk/misc/rc.transparent" コマンドを利用して実行することもできます。

iptablesの設定を行った後は、クライアントからインターネットゲートキーパの変換元のサービス (FSIGK: 80、FSIGK: 25、FSIGK: 110、FSIGK: 21) に接続したとき、変換後のポート (FSIGK: 9080、FSIGK: 9025、FSIGK: 9110、FSIGK:9021) で動作しているインターネットゲートキーパ・サービスに接続できることを確認してください。

3. 下位ルータのデフォルトルートをFSIGKに変更し、全ての通信がFSIGKを通るようにします。Linuxの場合、下位ルータで以下のようなコマンドを実行します。

```
NAT-router# route del -net default
NAT-router# route add -net default gw 192.168.0.99
```

4. 再起動後も設定を有効にするため、下位ルータで/etc/sysconfig/network, /etc/sysconfig/network-scripts/ifcfg-eth0のGATEWAY変数も変更し、設定を保存します。

   クライアントからの任意のサーバのサービス(http(80)、smtp(25)、pop(110)、ftp(21)) への接続をインターネットゲートキーパ・サービス (FSIGK: 9080、FSIGK: 9025、FSIGK: 9110、FSIGK: 9021) が受けることを確認してください。

5. FSIGK側ではウイルススキャンを行うサービス (http、smtp、pop、ftp) 以外の通信も可能にするため、以下のコマンドでルーティングを可能にします。

```
FSIGK# echo 1 > /proc/sys/net/ipv4/ip_forward
```

6. 再起動後もルーティングを有効にするため、FSIGKで、/etc/sysctl.confを以下のとおり設定します。

```
net.ipv4.ip_forward = 1
```

   クライアントから任意の通信が可能なことを確認してください。

7. 任意のクライアントから任意のサーバへの接続をウイルス監視できることを確認してください。

注：

各サービスについて、通常インターネットゲートキーパからサーバへ接続する際の接続元IPアドレスは、インターネット ゲートキーパのIPアドレスになります。

また、FTPのデータセッションについては、通常、Passiveモードではクライアントからの接続先アドレスとインターネットゲートキーパからサーバへの接続元アドレス、Activeモードではサーバからの接続先アドレスとインターネット ゲートキーパからクライアントへの接続元アドレスがインターネット ゲートキーパのアドレスになります。FTPの通信ができない場合、このような場合にファイアウォールで拒否していないかご確認ください。

インターネット ゲートキーパからサーバへの接続時、およびFTPのデータセッションでIPアドレスを保持する必要がある場合、tproxyパッチ適用済みカーネルが必要になります。

注：

Linuxのファイアウォール設定 (iptables) で必要な通信を拒否しないように設定してください。

少なくとも以下の通信は許可してください

- OUTPUTチェインの全ての通信
- FORWARDチェインの全ての通信
- INPUTチェインの、インターネットゲートキーパの待ちうけポート(9080,9025,9110,9021)などへの通信。及び、FTPの場合、FTPに関連するデータセッションの通信
- 正しく通信できない場合、切り分けのためファイアウォールを無効にして動作を確認ください。

8.2.3 透過プロキシの設定例 (ブリッジ型)

本製品は、設定によりブリッジ型の透過プロキシとして動作することができます。ブリッジ型の透過プロキシとして設置すると、クライアントの設定、各ネットワーク設定などを一切変更せずにウイルススキャン機能を各クライアントに提供できます。

ブリッジ型の透過プロキシとして設置する場合、2つ(以上)のインターフェースがあるインターネットゲートキーパ・マシンをクライアントとサーバの間に設置する必要があります。また、カーネルの再コンパイルが必要です。ブリッジとして動作しますので、2つのインターフェースともに同一のネットワークとなります。

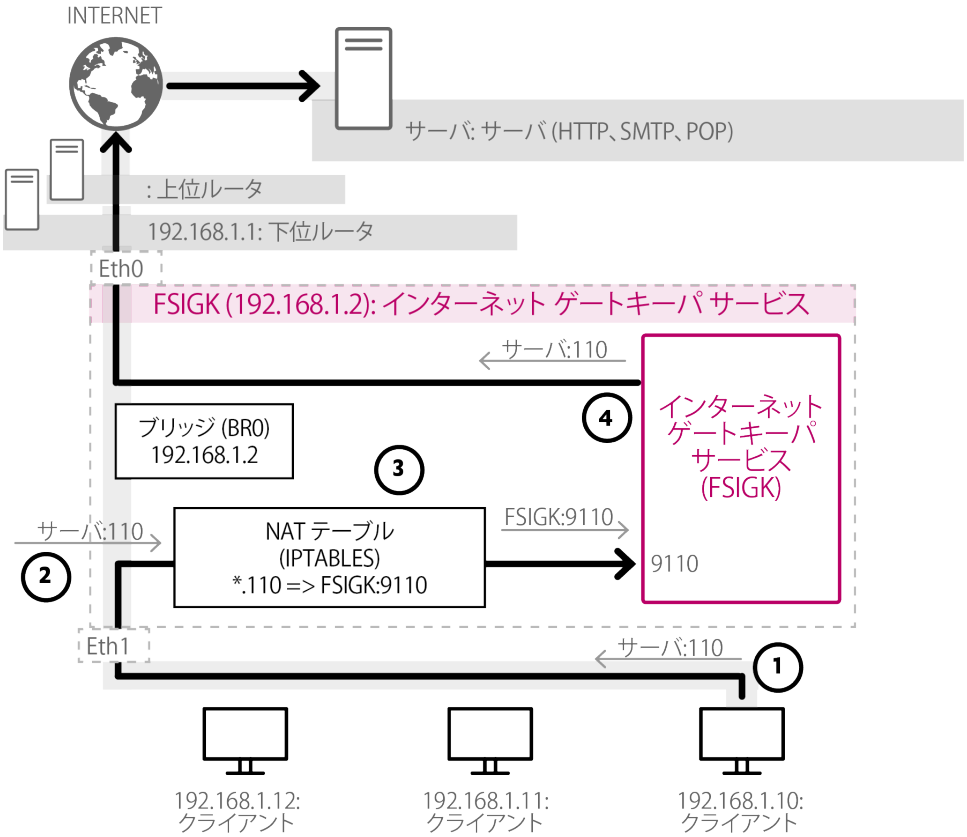


図 13 : 透過プロキシの設定 (ブリッジ型)。

動作概要

本製品を透過プロキシとして動作させた場合、クライアントからサーバへの接続は以下のように処理します。

1. クライアントは、サーバ (SERVER) のサービスポート番号 (例: 110) に向けて接続を開始する。
2. クライアントは下位ルータとの間にブリッジとして設置されたインターネットゲートキーパを通過する。

3. FSIGKではiptablesのNAT設定により、クライアントからSERVER:110への接続要求をFSIGK:9110への接続要求に置き換え、元の接続先 (SERVER: 110) を記憶する。
4. インターネットゲートキーパ・サービス (FSIGK) は、FSIGK:9110で接続を待ち受け、iptablesで置き換えられた接続要求を受け付ける。その後、iptablesから記憶された元の接続先 (SERVER:110) を取り出し、元の接続先 (SERVER:110) に接続要求を出す。

設定

本製品をブリッジ型の透過プロキシモードで動作させる場合、以下の手順でネットワークおよびインターネットゲートキーパ・サーバの設定を行います。

1. 設定ファイル`/opt/f-secure/fsigk/conf/fsigk.ini`のプロキシ設定で、各サービスを透過プロキシモードで立ち上げます。
   - **HTTP proxy (http_service)=yes**
     - Port Number (svcport)=9080
     - Transparent proxy (transparent)=yes
   - **SMTP proxy (smtp_service)=yes**
     - Proxy port (svcport)=9025
     - Transparent proxy (transparent)=yes
   - **POP proxy (pop_service)=yes**
     - Port Number (svcport)=9110
     - Transparent proxy (transparent)=yes
   - **FTP proxy (ftp_service)=yes**
     - Port Number (svcport)=9021
     - Transparent proxy (transparent)=yes

   設定を行った後は、クライアントからインターネットゲートキーパ・サーバの各サービスのポート番号 (9080、9025、9110、9021) に接続できることを確認してください。
2. ブリッジを設定します。`/opt/f-secure/fsigk/misc/rc.bridge`からIPアドレス、ネットマスク、デフォルトルート、インターフェース名を変更して起動スクリプトとして起動します。 なお、brctlコマンドが必要ですので、存在しない場合は"bridge-utils"パッケージなどbrctlコマンドを含むパッケージをインストールしてください。

```
# cp /opt/f-secure/fsigk/misc/rc.bridge /etc/rc.d/init.d/bridge
# /etc/rc.d/init.d/bridge start
# chkconfig --add bridge
```

   両側のインターフェース (eth0,eth1) 間で通信できることを確認してください。
3. インターネットゲートキーパ・サーバのiptablesを変更することで、クライアントからの接続先を接続先サーバからFSIGK:9110に変更します。
4. 任意のサーバへの各サービス (http(80), smtp(25), pop(110), ftp(21)) への接続を、FSIGKの9080、9025、9110、9021に変更するため、以下のようなコマンドを実行します。

```
FSIGK# iptables -t nat -A PREROUTING -p tcp --dport 80 \
 -j REDIRECT --to-port 9080
FSIGK# iptables -t nat -A PREROUTING -p tcp --dport 25 \
 -j REDIRECT --to-port 9025
FSIGK# iptables -t nat -A PREROUTING -p tcp --dport 110 \
 -j REDIRECT --to-port 9110
FSIGK# iptables -t nat -A PREROUTING -p tcp --dport 21 \
 -j REDIRECT --to-port 9021
```

5. iptablesの構成を保存します。詳細な説明については、Linuxディストリビューションのマニュアルを参考にしてください。

注: これらのiptablesの設定は"/opt/f-secure/fsigk/misc/rc.transparent"コマンドを利用して実行することもできます。

6. 任意のクライアントから任意のサーバへの接続をウイルス監視できることを確認してください。

注:

各サービスについて、通常インターネットゲートキーパからサーバへ接続する際の接続元IPアドレスは、インターネット ゲートキーパのIPアドレスになります。したがって、インターネットゲートキーパ サーバでは、IPアドレス、ルーティング設定などが必要になります。

また、FTPのデータセッションについては通常、Passiveモードではクライアントからの接続先アドレスとインターネットゲートキーパからサーバへの接続元アドレス、Activeモードではサーバからの接続先アドレスとインターネット ゲートキーパからクライアントへの接続元アドレス、がインターネット ゲートキーパのアドレスになります。FTPの通信ができない場合、このような場合にファイアウォールで拒否していないかご確認ください。

インターネット ゲートキーパからサーバへの接続時、およびFTPのデータセッションでIPアドレスを保持する必要がある場合、tproxyパッチ適用済みカーネルが必要になります。

注:

Linuxのファイアウォール設定 (iptables) で必要な通信を拒否しないように設定してください。

少なくとも以下の通信は許可してください

- OUTPUTチェインの全ての通信
- FORWARDチェインの全ての通信
- INPUTチェインの、インターネットゲートキーパの待ちうけポート(9080,9025,9110,9021)などへの通信。及び、FTPの場合、FTPに関連するデータセッションの通信
- 正しく通信できない場合、切り分けのためファイアウォールを無効にして動作を確認ください。

注: 参考URL(URLはサイトの都合などにより随時変更される可能性があります) Net:Bridge - The Linux Foundation http://www.linuxfoundation.org/collaborate/workgroups/networking/bridge

8.3 メールサーバと同居する場合の設定例

本製品は、メールサーバと同じマシンで動作させることも可能です。

メールサーバと同居する場合、メールサーバまたはインターネットゲートキーパのいずれかのIPアドレス、またはポート番号を通常の25番、110番から変更する必要があります。通常はインターネットゲートキーパのポート番号変更を行ってください。

8.3.1 インターネットゲートキーパのポート番号変更

メールサーバとインターネットゲートキーパを同じサーバに同居させる場合、インターネットゲートキーパを別のポート番号で待ち受ける方法が利用できます。

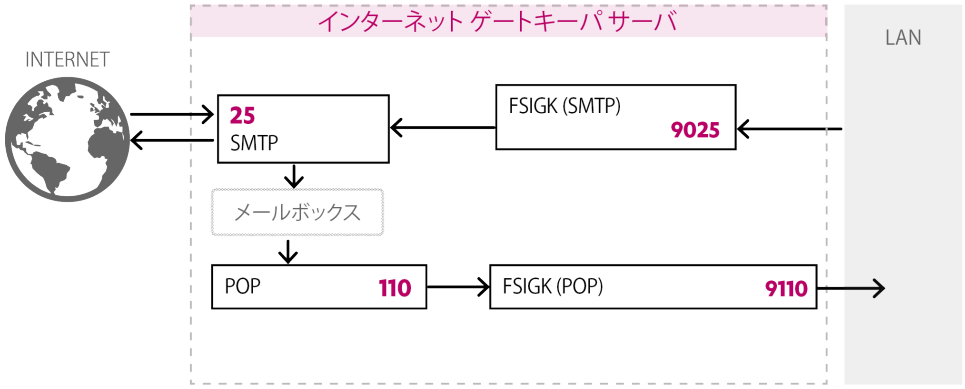


図 14 : インターネット ゲートキーパによるポート9025と9110の使用。

たとえばインターネットゲートキーパをポート9025, 9110で待ち受ける場合、以下の設定を行います。

1. F-Secure インターネット ゲートキーパの設定ファイル`/opt/f-secure/fsigk/conf/fsigk.ini`で、待ち受けポート番号を9025、9110に設定します。
   - **プロキシ設定 > SMTPプロキシ**
     - **Proxy port (svcport)=9025**
     - **親サーバ**: (parent_server_host=localhost , parent_server_port=25)
   - **プロキシ設定 > POPプロキシ**
     - **Proxy port (svcport)=9110**
     - **親サーバ**: (parent_server_host=localhost , parent_server_port=25)
2. クライアントの設定で、SMTPサーバ、POPサーバのポート番号を9025と9110に設定します。

8.3.2 メールサーバのポート番号変更

メールサーバとインターネットゲートキーパを同じサーバに同居させる場合、メールサーバを通常と別のポート番号で待ち受ける方法が利用できます。

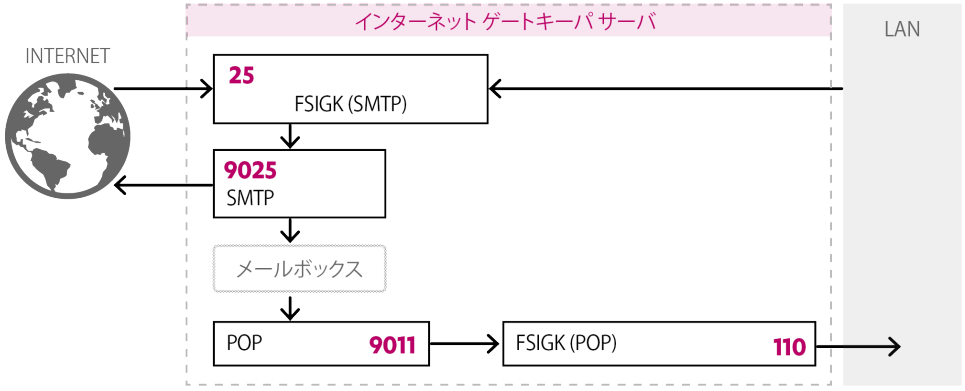


図 15 : メールサーバによるポート9025と9110の使用。

たとえば、メールサーバをポート9025, 9110で待ち受ける場合、以下の設定を行います。また、SMTPでのウイルスチェックを行うため、POPについてはインターネットゲートキーパを利用しないことも可能です。

1. メールサーバで、SMTPサーバの待ち受けポートを9025に、POPサーバの待ち受けポートを9110に変更します。

   - **sendmail**の場合

     a. `/etc/sendmail.cf`または`/etc/mail/sendmail.cf`で以下のように変更します。

     ```
     DaemonPortOptions=Port=9025
     ```

     b. sendmailを再起動します。

     ```
     # /etc/rc.d/init.d/sendmail restart
     ```

     また、`systemd` の場合:

     ```
     # systemctl restart sendmail
     ```

   - **ipop3d + xinetd**の場合

     a. `/etc/xinetd.d/ipop3`で、以下のように設定を追加または変更します。

     ```
     port = 9110
     ```

     b. xinetdを再起動します。

     ```
     # /etc/rc.d/init.d/xinetd restart
     ```

     また、`systemd` の場合:

     ```
     # systemctl restart xinetd
     ```

   - **qmail+tcpserver**の場合

     a. `/var/qmail/rc`で以下のように変更します。

     ```
     /usr/local/bin/tcpserver -R -x /etc/tcp.smtp.cdb -u qmaild \
      -g qmail 0 9025 /var/qmail/bin/qmail-smtpd | \
      /var/qmail/bin/splogger smtpd 3 &
     ```

   - **qmail-popup + xinetd**の場合

     a. `/etc/xinetd.d/qmail-popup`で、次の変更を行います。

     ```
     port = 9110
     ```

     b. xinetdを再起動します。

     ```
     # /etc/rc.d/init.d/xinetd restart
     ```

     また、`systemd` の場合:

     ```
     # systemctl restart xinetd
     ```

   - **postfix**の場合

     a. 1`/etc/postfix/master.cf`のsmtpdサービスの待ち受けポート設定を、以下のように変更します。

     ```
     9025 inet n - n - - smtpd
     ```

b. postfixを再起動します。

```
# postfix reload
```

2. F-Secure インターネット ゲートキーパの設定ファイル/opt/f-secure/fsigk/conf/fsigk.iniで、親サーバのポート番号を9025、9110に設定します。
   - **プロキシ設定 › SMTP proxy (smtp_service)=yes**
     - **Proxy port (svcport)=25**
     - **全体設定 › 親サーバ**
       - **Host name (parent_server_host)=localhost**
       - **Port number (parent_server_port)=9025**
   - **プロキシ設定 › POP proxy (pop_service)=yes**
     - **Proxy port (svcport)=110**
     - **親サーバ**:
       - **Host name (parent_server_host)=localhost**
       - **Port number (parent_server_port)=9110**

8.3.3 IPアドレスの変更 (各サービスで待ち受けアドレス設定)

メールサーバとインターネットゲートキーパを同じサーバに同居させる場合、メールサーバとインターネットゲートキーパが別のインターフェース (IPアドレス) の同じポート番号で接続を待ち受ける方法を利用できます。

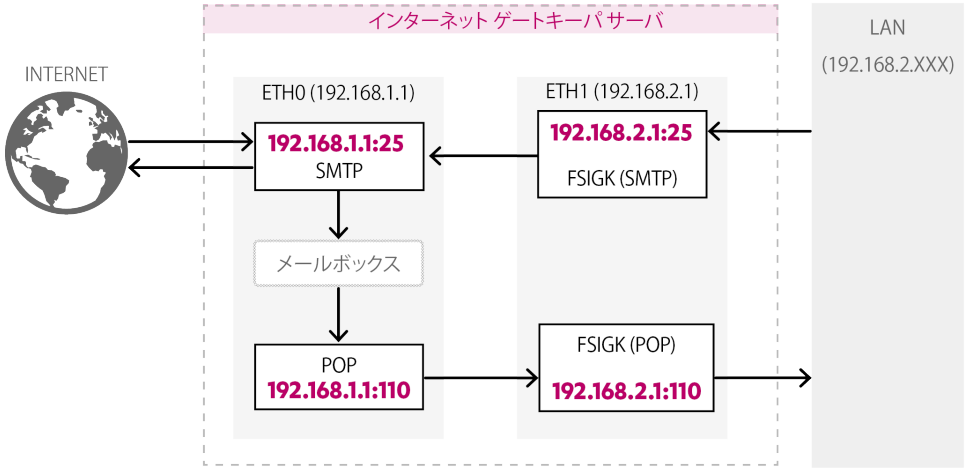


図 16 : メールサーバがeth0(192.168.1.1)、インターネットゲートキーパがeth1(192.168.2.1) で待ち受けています

物理的なネットワークインターフェースが1つしかない場合、IPAlias機能を使用して仮想インターフェースを作成できます。たとえば、仮想インターフェース eth0:1(192.168.1.2) を作成する場合は以下のコマンドを利用します。

```
# ifconfig eth0:1 192.168.1.2 netmask 255.255.255.0
```

起動時に、この仮想インターフェースを作成する場合は、/etc/sysconfig/network-scripts/ifcfg-eth0をifcfg-eth0:1にコピーし、ファイル内をDEVICE="eth0:1"と書き換え、ファイル内のIPADDR, NETMASK, NETWORK, BROADCAST変数を設定します。

1. メールサーバの待ち受けインターフェースを`eth0(192.168.1.1)`に設定します。
   - **sendmail**の場合
     a. `/etc/sendmail.cf`または`/etc/mail/sendmail.cf`で以下のように変更します。

     ```
     DaemonPortOptions=Port=smtp,Addr=192.168.1.1
     ```

     b. sendmailを再起動します。

     ```
     # /etc/rc.d/init.d/sendmail restart
     ```

     また、`systemd`の場合:

     ```
     # systemctl restart sendmail
     ```

   - **ipop3d + xinetd**の場合
     a. `/etc/xinetd.d/ipop3`で、以下のように設定を追加または変更します。

     ```
     bind=192.168.1.1
     ```

     b. xinetdを再起動します。

     ```
     # /etc/rc.d/init.d/xinetd restart
     ```

     また、`systemd`の場合:

     ```
     # systemctl restart xinetd
     ```

   - **qmail+tcpserver**の場合
     a. `/var/qmail/rc`で以下のように変更します。

     ```
     /usr/local/bin/tcpserver -R -x /etc/tcp.smtp.cdb -u qmaild \
      -g qmail 192.1.168.1.1 25 /var/qmail/bin/qmail-smtpd | \
      /var/qmail/bin/splogger smtpd 3 &
     ```

   - **qmail-popup + xinetd**の場合
     a. `/etc/xinetd.d/qmail-popup`で、次の変更を行います。

     ```
     bind=192.168.1.1
     ```

     b. xinetdを再起動します。

     ```
     # /etc/rc.d/init.d/xinetd restart
     ```

     また、`systemd`の場合:

     ```
     # systemctl restart xinetd
     ```

   - **postfix**の場合
     a. 1`/etc/postfix/master.cf`のsmtpdサービスの待ち受けポート設定を、以下のように変更します。

     ```
     192.168.1.1:25 inet n - n - - smtpd
     ```

b. postfixを再起動します。

```
# postfix reload
```

2. 設定ファイル/opt/f-secure/fsigk/conf/fsigk.iniで、親サーバの待ち受けポート番号を192.168.2.1:25, 192.168.2.1:110に設定し、親サーバをメールサーバ(192.168.1.1:25、192.168.1.1:110)に設定します。
   - **プロキシ設定 > SMTP proxy (smtp_service)=yes**
     - **Proxy port (svcport)=192.168.2.1:25**
     - **全体設定 > 親サーバ**
       - **Host name (parent_server_host)=192.168.1.1**
       - **Port number (parent_server_port)=25**
   - **プロキシ設定 > POP proxy (pop_service)=yes**
     - **Proxy port (svcport)=192.168.2.1:110**
     - **親サーバ**:
       - **Host name (parent_server_host)=192.168.1.1**
       - **Port number (parent_server_port)=110**

3. メールサーバを192.168.2.1に設定します。

   以上で設定が完了です。クライアントからメールの送受信ができることを確認してください。

IPアドレスの変更 (iptablesによる設定)

メールサーバとインターネット ゲートキーパを同じサーバに同居させる場合、インターネット ゲートキーパとメールサーバへの接続を別のインターフェースの同じポートで待ち受ける方法があります。

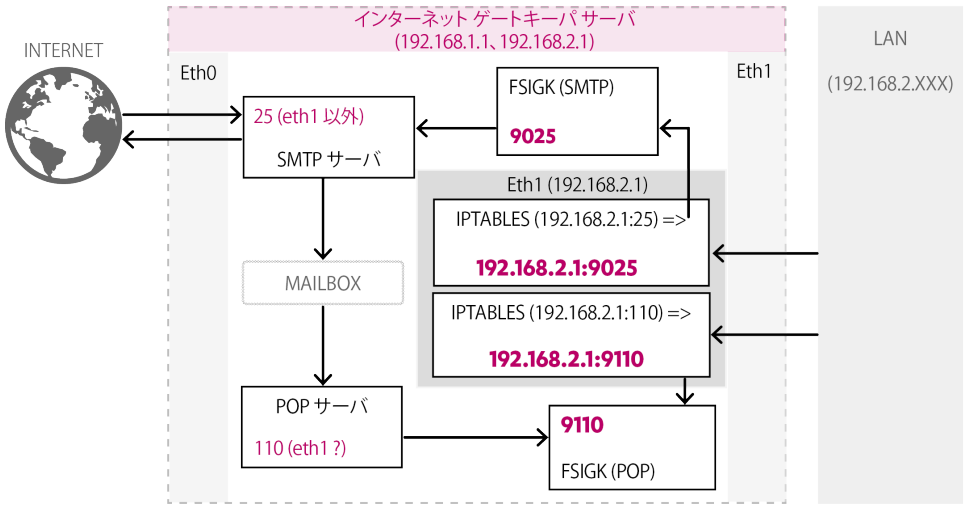


図 17 : デフォルトポートにアクセスのリダイレクト

これには、インターネットゲートキーパを通常(25, 110)と別のポート(9025, 9110など)で動かし、iptablesコマンドによるNAT設定により、特定のインターフェースの通常のポート(25, 110)への接続をインターネットゲートキーパが動作しているポート(9025, 9110など)に振り分けを行う方法が利用できます。

ここでは、eth0(192.168.1.1)とeth1(192.168.2.1)の2つのインターフェースを持つ状態で、eth1のポート25, 110への接続をポート9025, 9110に変更し、インターネットゲートキーパへの接続にeth1をメールサーバへの接続はその他のインターフェース(eth0(192.168.1.1), lo(localhost))を使用する場合について説明します。

物理的なネットワークインターフェースが1つしかない場合、IPAlias機能を使用して仮想インターフェースを作成できます。たとえば、仮想インターフェース eth0:1(192.168.1.2) を作成する場合は以下のコマンドを利用します。

```
# ifconfig eth0:1 192.168.1.2 netmask 255.255.255.0
```

起動時に、この仮想インターフェースを作成する場合は、/etc/sysconfig/network-scripts/ifcfg-eth0をifcfg-eth0:1にコピーし、ファイル内をDEVICE="eth0:1"と書き換え、ファイル内のIPADDR, NETMASK, NETWORK, BROADCAST変数を設定します。

ゲートウェイサーバのiptablesの設定

次のiptablesコマンドでアクセスをeth1(192.168.2.1)のポート25と110から9025と9110へリダイレクトします。

```
# iptables -t nat -A PREROUTING -d 192.168.2.1 -p tcp --dport 25 \
 -j REDIRECT --to-port 9025
# iptables -t nat -A PREROUTING -d 192.168.2.1 -p tcp --dport 110 \
 -j REDIRECT --to-port 9110
```

次に iptables の構成を保存します。詳細な説明については、Linux ディストリビューションのマニュアルを参考にしてください。

インターネットゲートキーパの設定

設定ファイル/opt/f-secure/fsigkconf/fsigk.iniで、親サーバのポート番号を9025、9110に設定し、親サーバをメールサーバ(localhost:25、localhost:110)に設定します。

- **プロキシ設定 > SMTP proxy (smtp_service)=yes**
  - **Proxy port (svcport)=9025**
  - **全体設定 > 親サーバ**
    - **Host name (parent_server_host)=localhost**
    - **Port number (parent_server_port)=25**
- **プロキシ設定 > POP proxy (pop_service)=yes**
  - **Proxy port (svcport)=9110**
  - **親サーバ**:
    - **Host name (parent_server_host)=localhost**
    - **Port number (parent_server_port)=110**

クライアントマシンの設定例

メールサーバを192.168.2.1に設定します。以上で設定が完了です。クライアントからメールの送受信ができることを確認してください。

8.4 メールサーバへ保存する前にウイルススキャンする場合の設定例

本製品を使用して受信メールのウイルススキャンを行う場合、通常はメールサーバからPOPで受信する時にウイルススキャンを行います。これにより、メールサーバなどの変更が不要になり、導入が簡単です。しかし、何らかの理由でメール受信時もメールサーバに保存する前にSMTPでウイルススキャンを行う必要がある場合、そのような設定も可能です。

ここでは、一台のインターネットゲートキーパ・サーバで、送信用メールと受信用メールのウイルススキャンを行う場合について説明します。

動作概要

ウイルススキャンなし インターネットゲートキーパを導入していない場合は、送信メールは自組織のメールサーバを経由して他組織のメールサーバに転送します。また、受信メールは自組織のメールサーバのメールボックスに蓄えられた後、ユーザがPOP接続により受信します。

ウイルススキャンあり インターネットゲートキーパを導入した場合は、送信メールはインターネットゲートキーパでウイルススキャンを行った後、自組織のメールサーバにより他組織のメールサーバに配信します。受信メールはインターネットゲートキーパでスキャンを行った後、自組織のメールサーバに蓄えられ、ユーザがPOP接続により受信します。また、他組織から他組織へのメールの不正中継 (第三者中継, Third Party Relay) に利用されることを防止するため、送信メールの制限を行います。

接続例

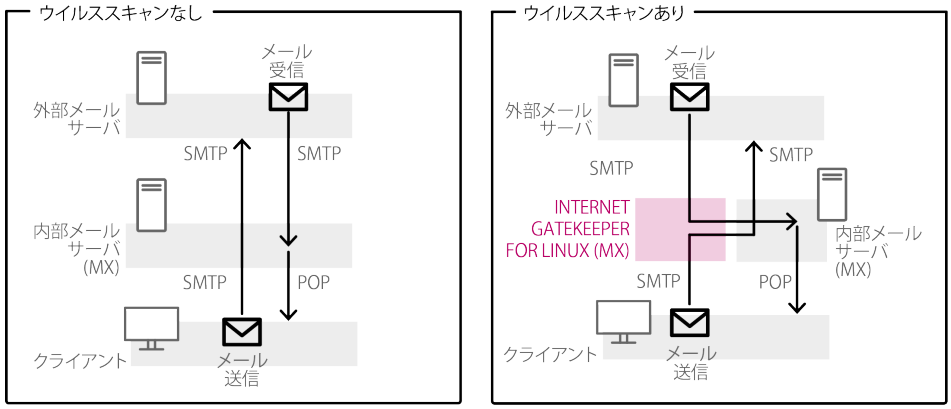


図 18 : メールサーバへ保存する前に受信メールのスキャン。

設定

1. インターネットゲートキーパを暫定的なホスト名(fsigk)で設置し、以下のプロキシ設定を設定ファイルに行います。
   - **プロキシ設定 > SMTP proxy (smtp_service)=yes**
     - **Proxy port (svcport)=25**
     - **全体設定 > 親サーバ**
       - **Host name (parent_server_host)=<内部メールサーバのIPアドレス>**
       - **Port number (parent_server_port)=25**
     - SMTP アクセス制御での説明にしたがってドメインへのメール配信を制限し、内部ネットワークにあるクライアント一覧を設定します。

2. 自組織メールサーバの設定で、fsigkからのメールが任意の他組織メールサーバに送信できるようにします。
   - **sendmail**の場合
     a. `/etc/mail/access`に以下の行を追加します。

     ```
     <IP address of fsigk (Example: 192.168.0.99)> RELAY
     ```

     b. `/etc/mail`でmakeを実行します。

     ```
     # cd /etc/mail/ ; make
     ```

c. sendmailを再起動します。

```
# /etc/rc.d/init.d/sendmail restart
```

また、systemd の場合:

```
# systemctl restart sendmail
```

- **qmail+tcpserver**の場合

a. /var/qmail/rcで以下のように記述します。

```
/usr/local/bin/tcpserver -R -x /etc/tcp.smtp.cdb -u qmaild \
 -g qmail 0 smtp /var/qmail/bin/qmail-smtpd | \
 /var/qmail/bin/splogger smtpd 3 &
```

b. /etc/tcp.smtpに以下のように記述します。

```
<IP address of fsigk (Example: 192.168.0.99)>:allow,RELAYCLIENT=""
<Network within LAN (Example: 192.168.1.)>:allow,RELAYCLIENT=""
:allow
```

c. 以下のコマンドでcdbに変換します。

```
# tcprules tcp.smtp.cdb tcp.smtp.tmp < tcp.smtp
```

- **postfix**の場合

a. /etc/postfix/main.cfに以下の行を設定します。

```
mynetworks=<IP address of fsigk (Example: 192.168.0.99)>,<Network within LAN>
```

(例: 192.168.1.0/24.)

b. postfixを再起動します。

```
# postfix reload
```

3. 社内からはfsigkを中継して社外にメールが送信できること、および社外からは自組織ドメイン宛のメールのみ送信できることを確認します。
4. DNSの設定で、自組織メールサーバのホスト名をmx2に変更し、インターネットゲートキーパのホスト名をmxとします。また、自組織ドメインのメールサーバ(DNSのMXレコード)をmx(インターネットゲートキーパのホスト)にします。
5. 社内からはmxを中継して社外にメールが送信できること、および社外から自組織ドメイン宛のメールのみ送信できることを確認します。
6. DNSキャッシュの有効期限が切れた後、社外のメールサーバを経由して自組織宛にメールが送信できることを確認します。また、社内から社外へのメール、社外から社内へのメールが共にウイルススキャンできることを確認します。

8.5 リバースプロキシの設定例

特定のウェブサーバに対する任意のクライアントからの接続をスキャンする場合、以下の方法で、本製品をリバースプロキシとして導入できます。

なお、複数のウェブサーバに対するスキャンを1台のインターネット ゲートキーパで行う場合など、必要に応じて透過プロキシとして導入することも可能です。

8.5.1 リバースプロキシの一般的な設定例

インターネット ゲートキーパをウェブサーバと別サーバで導入する場合、インターネット ゲートキーパをウェブサーバの前に設置し、インターネットから見たウェブサーバとして導入します。この場合の設定は以下のとおりです。

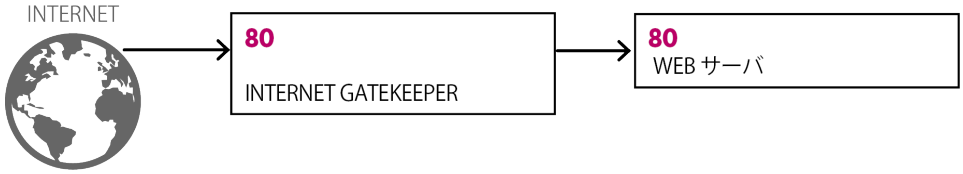


図 19 : リバースプロキシの設定。

インターネットゲートキーパの設定例

設定ファイル`/opt/f-secure/fsigk/conf/fsigk.ini`で、待ち受けポート番号を80に、親サーバのポート番号を80に設定します。

- **プロキシ設定 › HTTP proxy (http_service)=yes**
  - **Proxy port (svcport)=80**
  - **親サーバ**:
    - **Host name (parent_server_host)=Web server**
    - **Port number (parentServer_port)=80**

DNS・ウェブサーバの設定例

インターネットから見たウェブサーバのIPアドレスをインターネット ゲートキーパのアドレスに設定します。これは、以下のいずれかの方法で行います。

- ウェブサーバで、IPアドレス設定を変更

  元のウェブサーバのIPアドレスを変更し、インターネット ゲートキーパのIPアドレスを元のIPアドレスに設定します。

- DNSサーバで、ウェブサーバに対応するIPアドレスの登録を変更

  DNSサーバの設定で、インターネットから見たウェブサーバのIPアドレスをインターネット ゲートキーパのIPアドレスに設定します。

8.5.2 ウェブサーバと同居する場合の設定例

本製品は、ウェブサーバと同じサーバで動作させることも可能です。ウェブサーバとインターネットゲートキーパを同じサーバに同居させる場合、ウェブサーバを通常と別のポート番号で待ち受ける方法が利用できます。

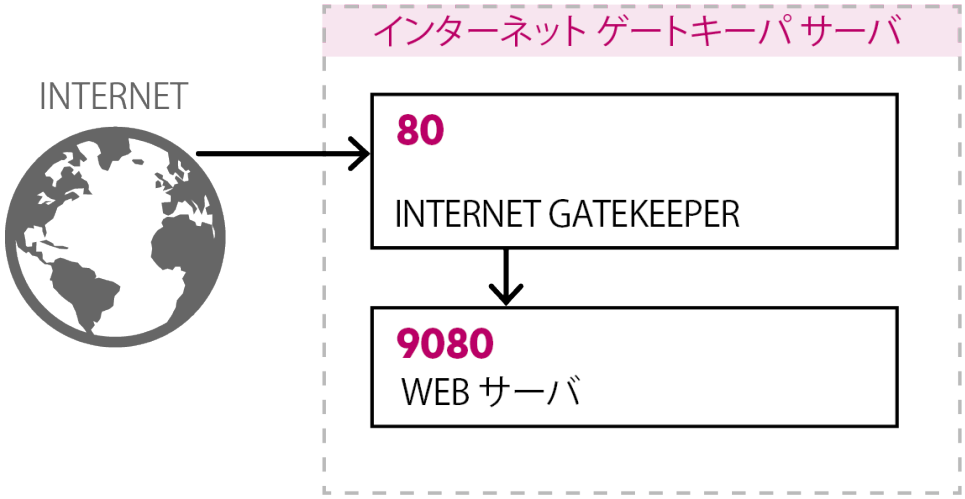


図 20 : ウェブサーバによるポート9080の使用。

ウェブサーバの設定例

ApacheのHTTPサーバの待ち受けポートを9080に変更します。

1. `/etc/httpd/conf/httpd.conf`を以下のように変更します。

```
Listen 9080
```

2. Apacheを再起動します。

```
# /etc/rc.d/init.d/httpd restart
```

また、`systemd`の場合:

```
# systemctl restart httpd
```

インターネットゲートキーパの設定例

設定ファイル`/opt/f-secure/fsigk/conf/fsigk.ini`で、プロキシポートと親サーバのポート番号を80に設定します。

- **プロキシ設定 › HTTP proxy (http_service)=yes**
  - **Proxy port (svcport)=80**
  - **親サーバ**:
    - **Host name (parent_server_host)=localhost**
    - **Port number (parentServer_port)=9080**

8.5.3 HTTPS (SSL) サーバでの導入方法

HTTPS(SSL)の通信については暗号化されているため、直接通信内容のスキャンを行うことができません。特定のHTTPS(SSL)サーバへの接続に対してスキャンを行う場合は、SSLプロキシ・SSLアクセラレータで復号した後に本製品でスキャンを行います。

たとえばApacheを利用している場合、ApacheをSSLプロキシとして動作させ、HTTP通信部分に本製品を導入することができます。

Apache-SSLプロキシ、インターネット ゲートキーパ、ウェブサーバは別のマシン、は同一マシンでも別のマシンでも利用できます。

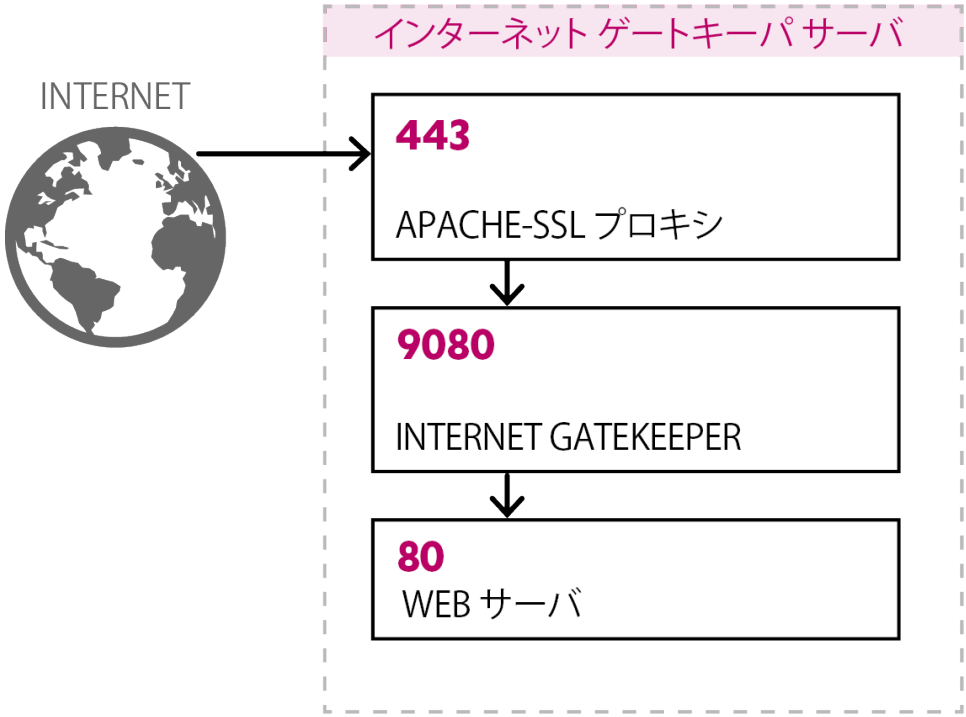


図 21 : SSLプロキシとWebサーバを使用した場合のApache設定ファイル

Apache-SSLの設定例

以下のように、443番で待ち受け、復号後9080番に中継する設定を行います。

```
# https access
Listen 443
<VirtualHost _default_:443>
 AddDefaultCharset Off
 ProxyPass / http://127.0.0.1:9080/
 ProxyPassReverse / http://127.0.0.1:9080/
 SSLEngine on
 SSLCertificateFile /etc/pki/tls/certs/localhost.crt
 SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
# SSLCertificateFile /etc/httpd/conf/ssl.crt/server.crt
# SSLCertificateKeyFile /etc/httpd/conf/ssl.key/server.key
 SSLOptions +StdEnvVars
 SetEnvIf User-Agent ".*MSIE.*" nokeepalive ssl-unclean-shutdown
</VirtualHost>
```

インターネットゲートキーパの設定例

設定ファイル`/opt/f-secure/fsigk/conf/fsigk.ini`で、待ち受けポート番号を9080に、親サーバのポート番号を9080に設定します。

- **Proxy settings > HTTP proxy (http_service)=yes**
  - **Proxy port (svcport)=9080**

- **親サーバ**:
  - **Host name (parent_server_host)=localhost**
  - **Port number (parentServer_port)=9080**

ウェブサーバの設定例

80番で待ち受けます。

第章

9

製品動作仕様

トピック：

本製品の動作仕様は以下のとおりです。

9.1 仕様

インストーラ	rpm、tar.gz
対応ネットワーク プロトコル	IPv4(RFC791)、TCP(RFC793)
対応アプリケーション プロトコル	HTTP、FTP、SMTP、POP、ICAP
対応モード	プロキシ、透過ルータ、ブリッジ
HTTPスキャン対象メソッド	GET/POST/PUT
使用可能な HTTP メソッド	GET/POST/PUT/HEAD/CONNECT/OPTIONS/DELETE/TRACE/PROPFIND/PROPPATCH/COPY/MOVE/LOCK/UNLOCK、その他同様の要求応答型のメソッド • データが暗号化されているため、ウイルス スキャンは CONNECT (SSL/HTTPS) に実行できません • 拒否したサイトへの CONNECT はホスト名にのみ検証されます
対応 HTTP プロキシ スキーマ	http://,ftp://
対応 HTTP プロトコル仕様	HTTP/1.0(RFC1945)、HTTP/0.9(RFC1945)、HTTP/1.1(RFC2616)、WEBDAV(RFC2518) (HTTP/1.1 レスポンスは自動的に HTTP/1.0 に変換されます)
対応 HTTP 認証方式	HTTP プロキシ認証 (ベーシック)
HTTP 最大転送サイズ	ディスクの空き容量に依存します
HTTP URL 最大長	24 KB
SMTPスキャン対象コマンド	DATA
SMTP利用可能コマンド	HELO/EHLO/MAIL/RCPT/DATA/RSET/VRFY/EXPN/HELP/NOOP/QUIT/XFORWARD/AUTH
SMTP対応プロトコル仕様	SMTP(RFC 2821)、SMTP Auth(RFC2554)

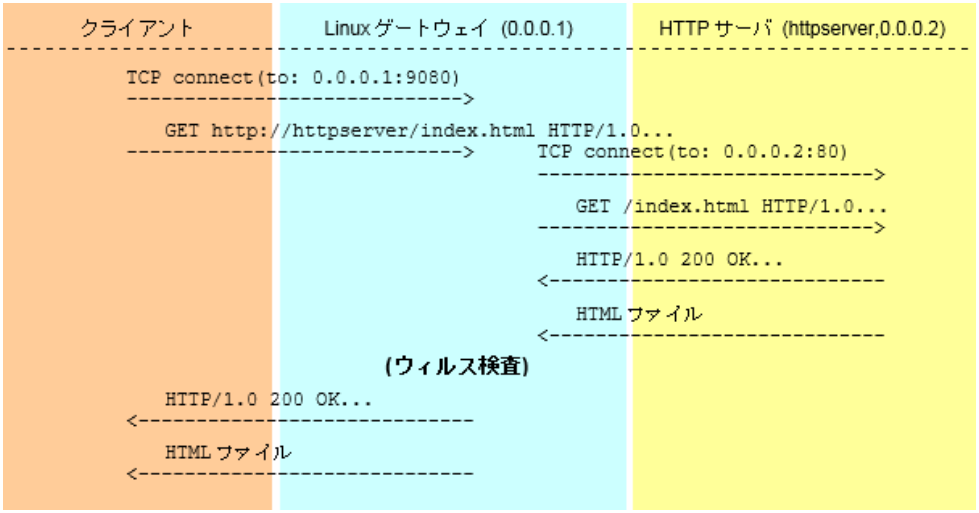
SMTP対応認証方式	SMTP Auth(PLAIN, LOGIN)、 POP-before-SMTP
SMTP最大転送メールサイズ	2,000,000,000バイト
POPスキャン対象コマンド	RETR/STOR
POP利用可能コマンド	USER/PASS/APOP/UIDL/TOP/STAT/LIST/RETR/DELE/NOOP/RSET/QUIT/AUTH、その他同様の要求応答型コマンド • “Defining parent server by user” 設定が有効かつ製品がプロキシとして実行している場合、APOPは使用できません。
POP対応プロトコル仕様	POP3(RFC1939)、 POP3 Auth(RFC1734) • “Defining parent server by user” 設定が有効かつ製品がプロキシとして実行している場合、APOPは使用できません。
POP対応認証方式	ユーザ名 (USER コマンドの引数)
POP最大転送サイズ	2,000,000,000バイト
FTPスキャン対象コマンド	RETR/STOR/STOU/APPE
FTP利用可能コマンド	USER/PASS/RETR/LIST/NLST/STOR/STOU/APPE/QUIT/PORT/PASV、その他同様の要求応答型コマンド
FTP対応プロトコル仕様	FTP (RFC959)
FTP対応認証方式	ユーザ名 (USER コマンドの引数)
FTP最大転送サイズ	ディスクの空き容量に依存します
スキャン可能最大サイズ	2GB (圧縮ファイルの場合、展開前・展開後ともに2GBが上限)
スキャン圧縮形式	ZIP、ARJ、LZH、CAB、RAR、TAR、GZIP、BZIP2 / 6階層

利用するセマフォ	セマフォ集合ごとのセマフォ数(SEMMS): 250 以内 セマフォ識別子の数(SEMMNI): 各サービス(http,smtp,ftp,pop)ごとに、(最大同時接続数 / 25) +10 以内
利用する共有メモリ	共有メモリ識別子の数(SHMMNI): 各サービス(http,smtp,ftp,pop)ごとに10以内 メモリサイズ(SHMMAX):各サービス(http,smtp,ftp,pop)ごとに1MB以下

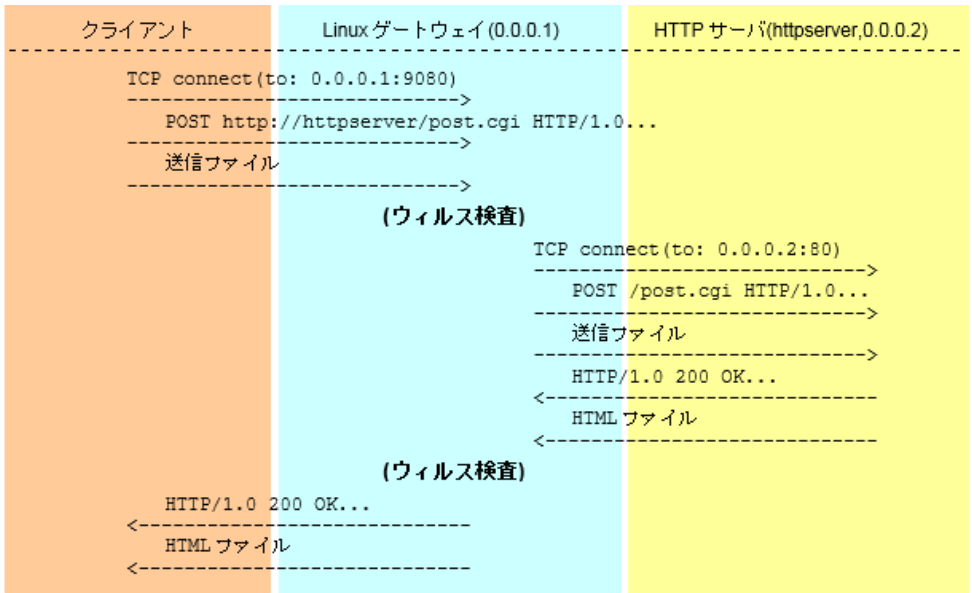
9.2 HTTPプロキシのプロトコル処理例

HTTPプロキシでの一般的なプロトコル処理例は以下のとおりです。

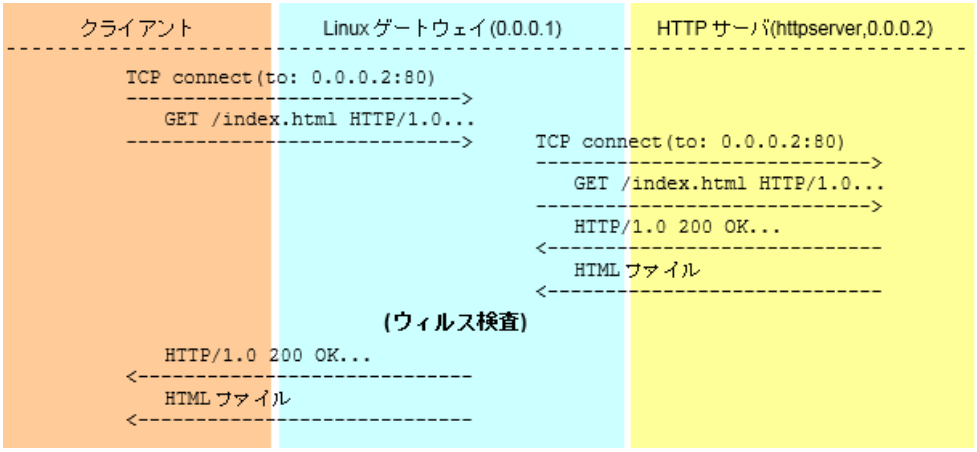
プロキシ型、GETメソッドの場合



プロキシ型、POSTメソッド(ファイル送信時、送信ファイルのスキャンあり)の場合



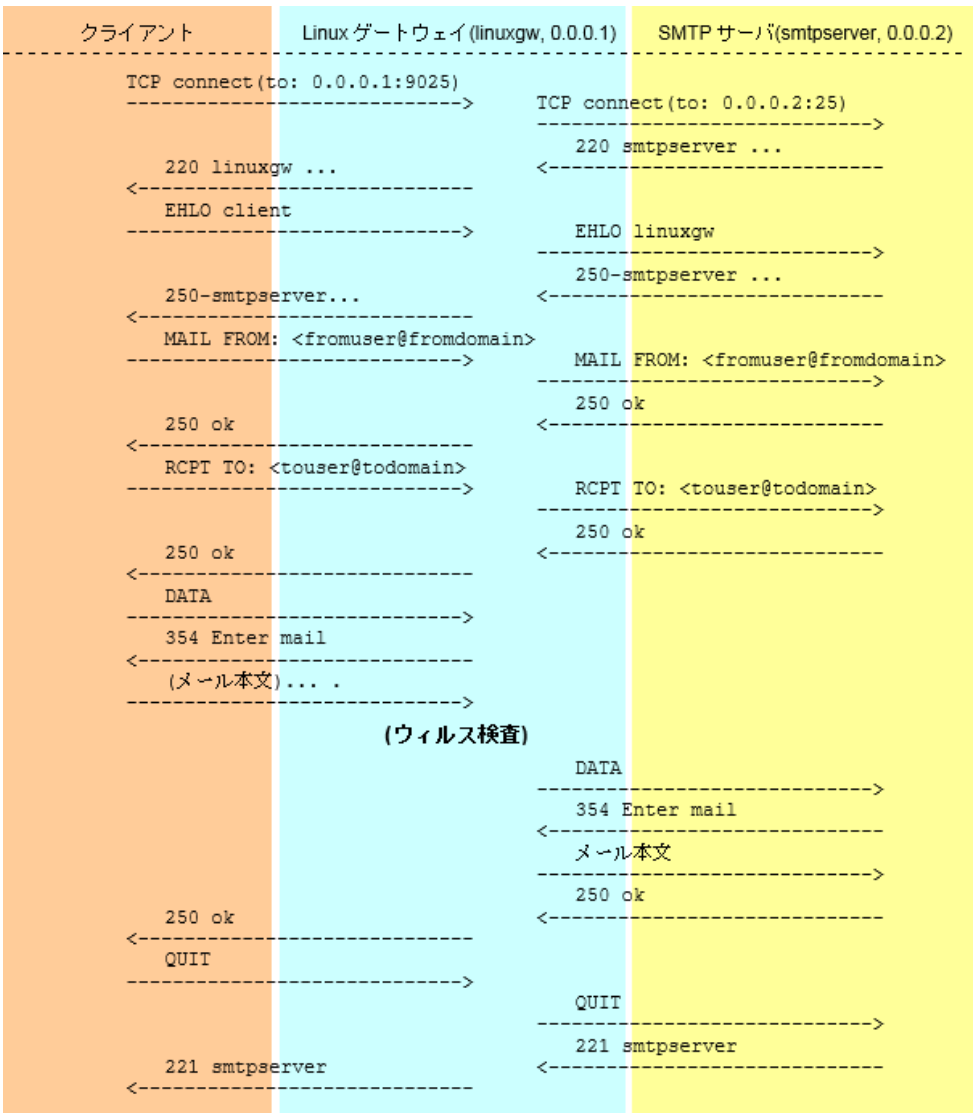
透過型(ルータまたはブリッジ)、GETメソッドの場合



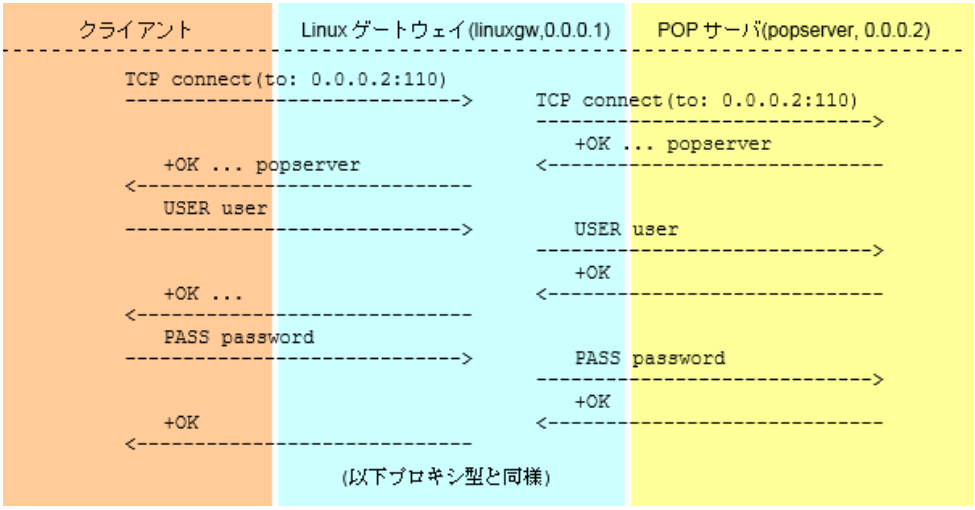
9.3 SMTPプロキシのプロトコル処理例

SMTPプロキシでの一般的なプロトコル処理例は以下のとおりです。

プロキシ型の場合



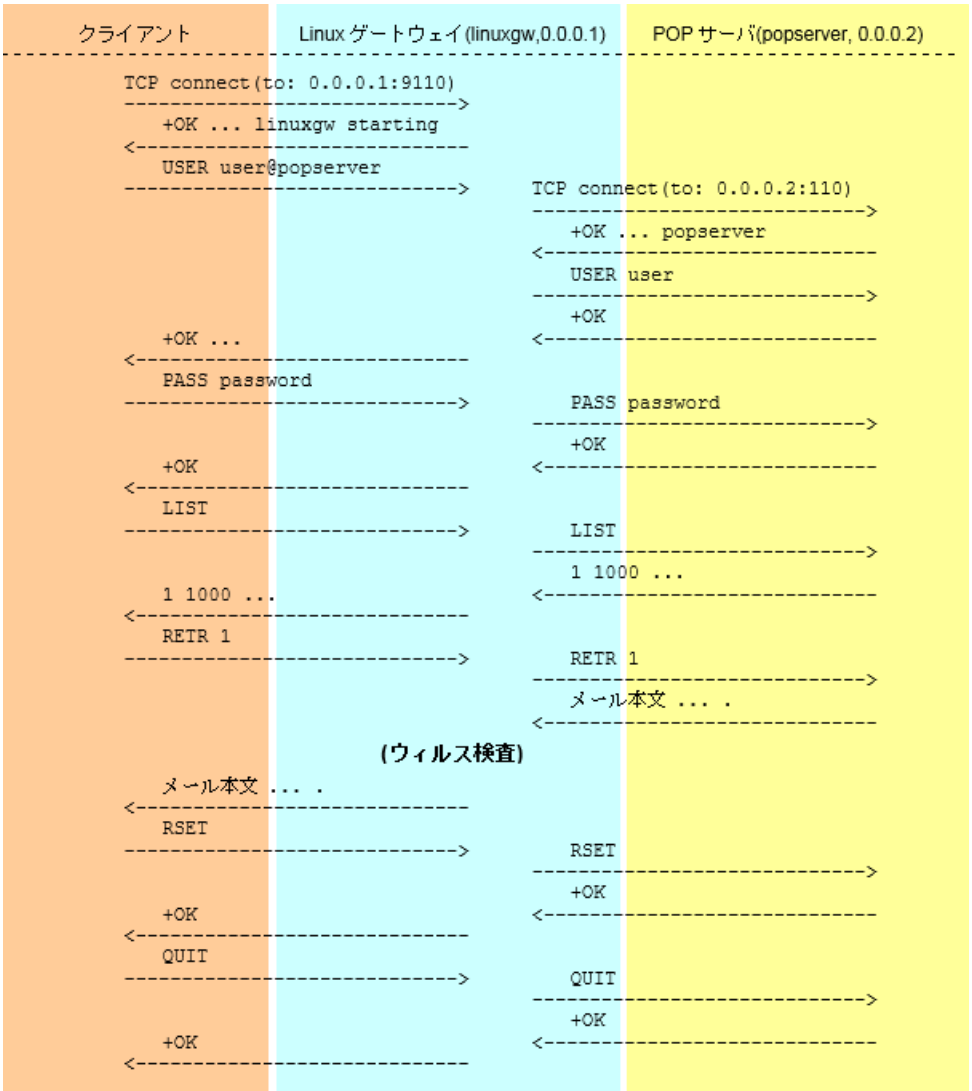
透過型(ルータまたはブリッジ)の場合



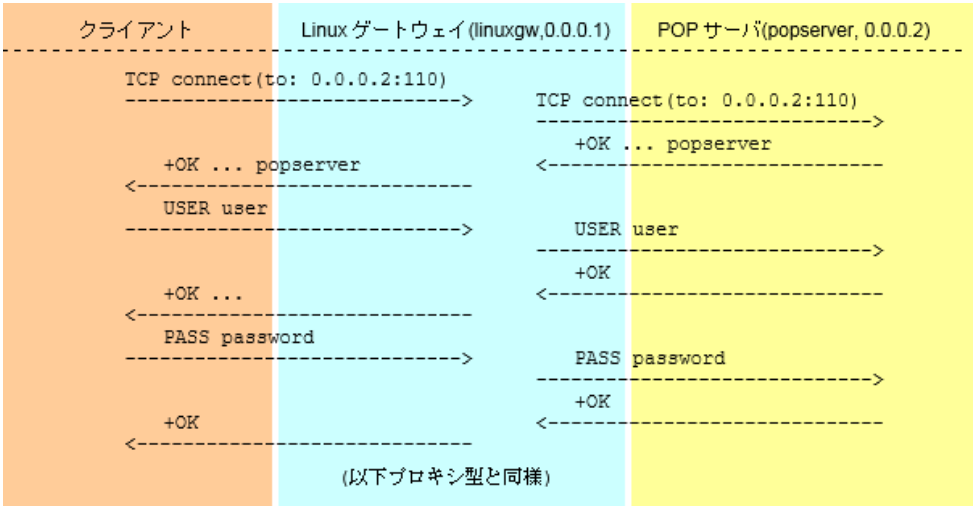
9.4 POPプロキシのプロトコル処理例

POPプロキシでの一般的なプロトコル処理例は以下のとおりです。

プロキシ型の場合



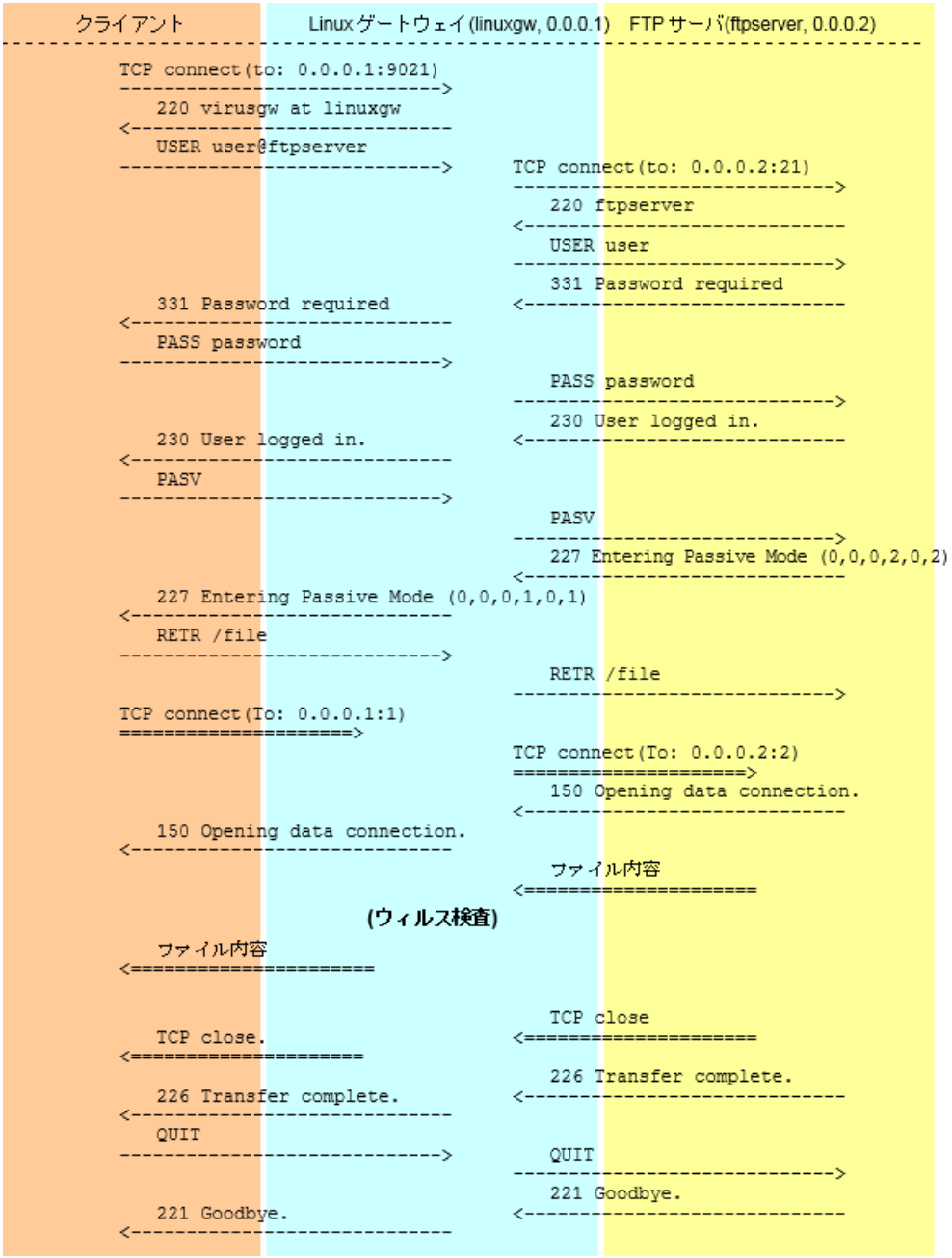
透過型(ルータまたはブリッジ)の場合



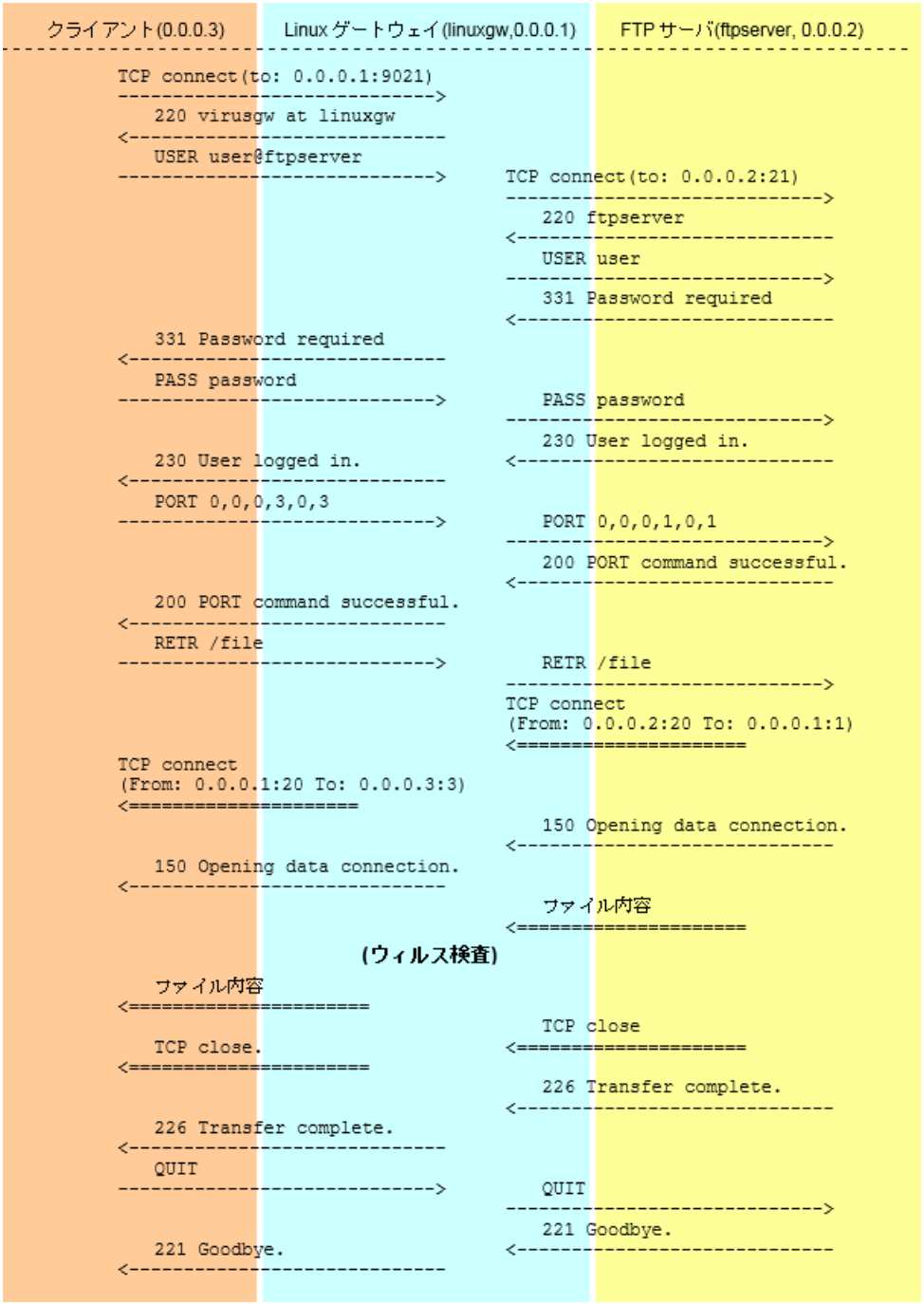
9.5 FTPプロキシのプロトコル処理例

FTPサービスでは、コントロールセッションとデータセッションの両方を中継します。FTPプロキシでの一般的なプロトコル処理例は以下のとおりです。

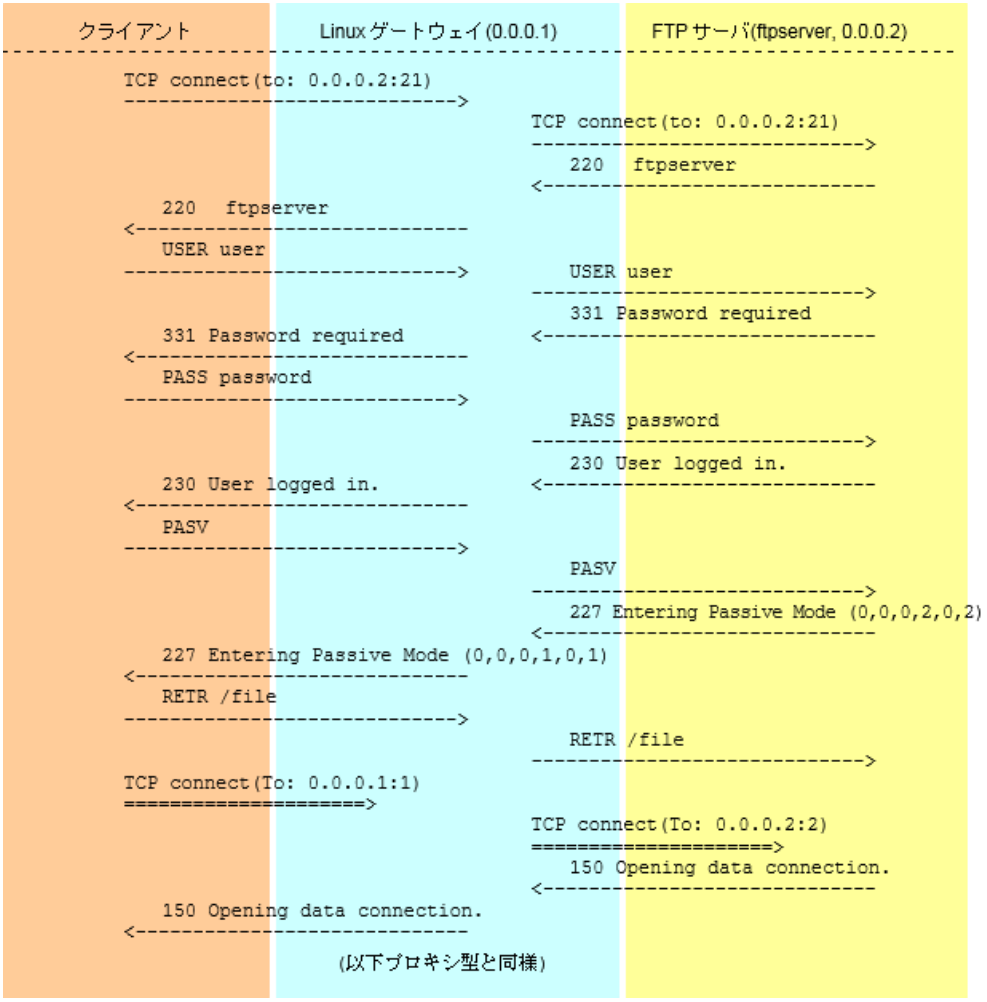
プロキシ型、パッシブモードFTPの場合



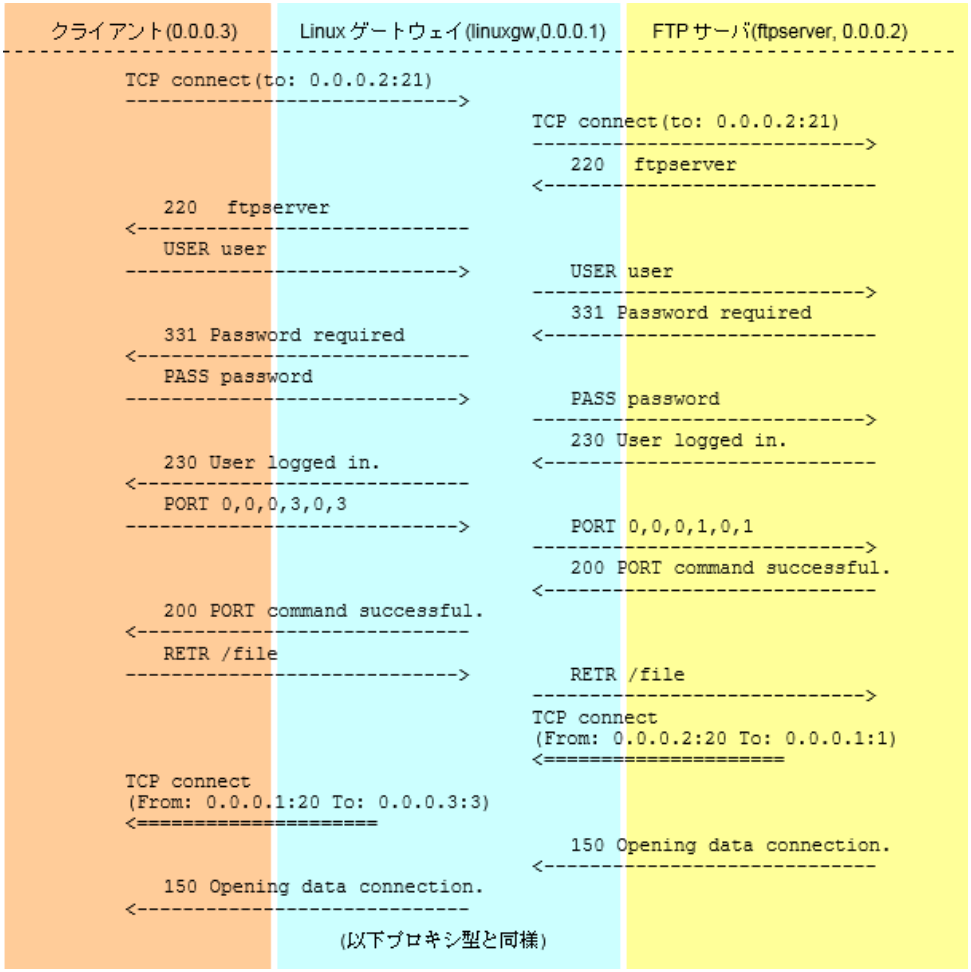
プロキシ型、アクティブFTPの場合



透過型(ルータまたはブリッジ)、パッシブモードFTPの場合



透過型(ルータまたはブリッジ)、アクティブFTPの場合



9.6 HTTPエラー応答一覧

HTTP接続時にエラーが発生した場合の、応答内容一覧は以下のとおりです。クライアントに表示されるメッセージは、エラーメッセージのテンプレートファイル (`/opt/f-secure/fsigk/conf/template_http_error.html`) で編集できます。

サーバ接続エラー

概要	サーバへの接続に失敗した
応答コード	503
応答理由	Service Unavailable
応答メッセージ	接続エラーメッセージです。

要求メソッド長エラー

概要	要求メソッドが最大長 (98バイト) を超えた

応答コード	400
応答理由	Bad Request
応答メッセージ	Too long Request Method

要求メソッド文字エラー

概要	要求メソッドに不正な文字(文字コード0x20未満の文字)が使われていた
応答コード	400
応答理由	Bad Request
応答メッセージ	Illegal method character.

要求URL長エラー

概要	要求URLが最大長 (24 KB) を超えた
応答コード	414
応答理由	Request-URI Too Long
応答メッセージ	Request-URI Too Long

要求URL文字エラー

概要	要求URLに不正な文字(文字コード0x20未満の文字)が使われていた
応答コード	400
応答理由	Bad Request
応答メッセージ	Illegal URL character.

要求URLフォーマット エラー

概要	要求URLの形式が不正
応答コード	400
応答理由	Bad Request
応答メッセージ	Invalid URL format

要求バージョン長エラー

概要	要求HTTPバージョンが最大長 (98バイト) を超えた
応答コード	400
応答理由	Bad Request
応答メッセージ	Too long Request Version

要求バージョンエラー

概要	要求HTTPバージョンとして、"HTTP/1.0"、"HTTP/1.1"、""(HTTP/0.9)以外が指定された。
応答コード	505
応答理由	HTTP Version Not Supported
応答メッセージ	Only support HTTP/0.9, HTTP/1.0, HTTP/1.1

プロキシ認証エラー

概要	プロキシ認証に失敗した
応答コード	407
応答理由	Proxy Authentication Required
応答メッセージ	Proxy Authentication Required

追加ヘッダ	Proxy-Authenticate: Basic realm="input proxy user/pass"

9.7 HTTP 要求・応答ヘッダの扱い

HTTPの要求ヘッダ・応答ヘッダの内容は基本的に変更しませんが、以下のヘッダについては変更を行います。

要求ヘッダの変更

- 要求行

  要求バージョンが"HTTP/1.1"の場合、"HTTP/1.0"に変更

  親サーバ設定がなく透過型でない場合、URLのパス名より前の部分は削除。(例:http://xxx:yyy/aaa/iii/uuu => /aaa/iii/uuu)

- Connection

  既存のConnectionヘッダは削除。Keep-Alive接続の場合、Connection: Keep-Aliveを追加。

- Proxy-Connection

  既存のProxy-Connectionヘッダは削除。

- Via

  匿名プロキシの場合は変更なし。それ以外の場合は以下の内容で追加します。

  Via : 1.0 ホスト名: 待ち受けポート (製品名)

  既存のViaヘッダが存在する場合は","区切りで後ろに追加します。

- X-Forwarded-For

  匿名プロキシの場合は変更なし。 それ以外の場合は、以下のように接続元のIPアドレスを追加します。

  X-Forwarded-For: 接続元IPアドレス

  既存のX-Forwarded-Forヘッダが存在する場合は","区切りで後ろに追加します。

- Keep-Alive

  既存のKeep-Aliveヘッダは削除。

- Trailer

  既存のTrailerヘッダは削除。

- Proxy-Authorization

  プロキシ認証が有効な場合は削除。

応答ヘッダの変更

- 応答行

  バージョンが"HTTP/1.1"の場合、"HTTP/1.0"に変更

- Connection

  既存のConnectionヘッダは削除。

  Keep-Alive接続の場合は、以下の内容で追加。

Connection: Keep-Alive

- Proxy-Connection

  既存のProxy-Connectionヘッダは削除。

- Proxy-Support

  "WWW-Authenticate"ヘッダがあり、透過型でなく、親サーバがない場合に以下の内容で追加します。

  Proxy-Support Session-Based-Authentication

  ("Proxy-Support: Session-Based-Authentication "はNTLM認証などをプロキシで利用する場合に必要です。RFC-4559を参照してください。)

9.8 SMTPコマンド応答一覧

SMTP接続時には基本的にサーバからの応答をクライアントに中継しますが、インターネットゲートキーパが生成する応答もあります。以下のメッセージがインターネットゲートキーパが生成する応答一覧になります。

[応答メッセージ] (製品名)

(例: 500 Unknown Command: "TEST" (F-Secure/fsigk_smtp/230/gwdev.gw.f-secure.co.jp))

応答メッセージ	応答理由
DATAコマンド応答	
`354 Enter mail`	送信メールデータ受信を開始します。
`250 Message accepted for delivery`	送信メールデータ受信を完了しました。
`554 SENDBACK:smtp error[COMMAND] (Server Reply: XXX)`	送信者へ通知を行う場合に送信したコマンド(COMMAND)でエラー応答(XXX)が返りました。 COMMANDはRSET/MAIL FROM/RCPT TOのいずれかです。
`554 Too long message`	データサイズが指定した最大サイズを超えました。 最大サイズは、上級者向けオプションのblock_messagesize/block_message_lenで指定した数字、または2,000,000,000バイトです。
`554 Infected by [検出名]`	ウイルス検出時の動作が"拒否"の場合に、ウイルスを検出した際に表示されます。
接続時応答	
`421 server open error (ホスト:ポート) errmsg=[XXX]`	指定したホスト、ポートへの接続に失敗しました。 ERRMSGには接続エラーメッセージの内容が表示されます。

応答メッセージ	応答理由
421 Cannot get correct greeting message from mail server (ホスト:ポート). return code=DDD	SMTPサーバ接続後のグリーティングメッセージが正しくありませんでした。SMTPサーバからの応答コードが220以外の場合に表示されます。
任意のコマンドの応答	
500 Too long line	コマンド行の長さが9999バイト以上でした。
HELO、EHLO、AUTH、QUIT、RSETコマンド以外の応答	
500 Authentication Required	メール送信に必要な認証が完了していません。以下の場合に表示されます。 • POP before SMTP認証またはSMTP認証が有効 • 認証が成功していない • LAN内からの接続ではない • 受信ドメインの制限を行っていない
HELO/EHLOコマンドの応答	
421 (COMMAND) disconnected from (ホスト:ポート)	COMMAND送信時にサーバが切断していた。 COMMANDはHELO、EHLOのいずれか。
MAILコマンドの応答	
501 Syntax error ("MAIL FROM:").	MAILコマンドが不正。(FROMがない)
RCPTコマンドの応答	
500 RCPT command must begin with "RCPT TO:."	RCPTコマンドが不正。(TOがない)
250 Recipient ok	中継を拒否しました。 受信ドメインの制限を行っており、必要な認証が終了していない場合に表示されます。
AUTHコマンドの応答	
504 this mechanism not available	指定の認証方式(PLAIN、LOGIN以外)はサポートしていません。
235 ok authed	認証に成功しました。 インターネット ゲートキーパ自身でSMTP認証を行っている場合のみ表示します。SMTPサーバ側で認証を行っている場合、SMTPサーバの応答を中継します。

応答メッセージ	応答理由
`535 authorization failed`	認証に失敗しました。 インターネット ゲートキーパ自身でSMTP認証を行っている場合のみ表示します。SMTPサーバ側で認証を行っている場合、SMTPサーバの応答を中継します。
`500 disconnected from server(AUTH).`	認証中にサーバが切断しました。
未知のコマンド受信時	
`500 Unknown Command: "COMMAND"`	指定したコマンド(COMMAND)はサポートしていない

9.9 SMTPコマンド動作概要一覧

SMTP接続時に、クライアントから送信されたコマンドに対する動作概要は以下のとおりです。

注: [製品名]は、デフォルトで"F-Secure/fsigk_smtp/バージョン/ホスト名"になります。上級者向けオプションの"product_name="で設定変更可能です。

クライアント接続時

1. サーバに接続
2. サーバ接続失敗時
   a. クライアントへ送信: `421 server open error([サーバホスト]:[サーバポート]) errmsg=[connection error message]`
   b. セッション終了
3. サーバ応答受信
4. 応答コードが220以外の場合は接続終了
5. クライアントへ送信: `200 [ホスト名] [製品名]`

各コマンド行受信時

1. 1行が9998バイト以上の場合
   a. クライアントへ送信: `500 Too long line ([製品名])`
   b. 接続終了
2. 以下の全ての条件を見たし、`HELO`、`EHLO`、`AUTH`、`QUIT`、`RSET`コマンド以外を受け取った場合
   - POP before SMTP認証またはSMTP認証が有効
   - 認証が成功していない
   - LAN内からの接続ではない
   - 受信ドメインの制限を行っていない

   クライアントへ送信: `500 Authentication Required ([製品名])`
3. 1,2以外の場合は各コマンドを処理する。

HELOコマンド受信時

1. サーバへ送信: `HELO [ホスト名]`
2. サーバ応答受信
3. クライアントへ送信: `[サーバ応答内容]`

EHLOコマンド受信時

1. サーバへ送信: `EHLO [ホスト名]`
2. サーバ応答受信
3. 応答内容から以下のオプション行を削除する。`CHUNKING`、`BINARYMIME`、`PIPELINING`、`STARTTLS`
4. 応答内容のSIZEオプションに、サーバからのSIZEオプション応答と最大メッセージサイズ(デフォルト:2,000,000,000)の小さい方を設定する。
5. プロキシ認証が有効の場合、応答内容に以下のオプション行を追加する。`250-AUTH PLAIN LOGIN`
6. クライアントへ送信: `[応答内容]`

MAILコマンド受信時

1. コマンド構文が正しくない場合

   クライアントへ送信: `501 Syntax error (MAIL FROM:) ([製品名])`

2. サーバへ送信: `[クライアント受信内容]`
3. サーバ応答受信
4. クライアントへ送信: `[サーバ応答内容]`

RCPTコマンド受信時

1. コマンド構文が正しくない場合

   クライアントへ送信: `500 RCPT command must begin with "RCPT TO:" ([製品名])`

2. 受信ドメインの制限を行っており、必要な認証が終了していない場合

   (受信先(RCPT)ドメインの制限が有効で指定ドメイン宛でなく、LANからの接続でなく、PbS(POP before SMTP)/SMTP認証が終了していない場合)

   クライアントへ送信: `550 Relaying denied. ([製品名])`

3. サーバへ送信: `[クライアント受信内容]`
4. サーバ応答受信
5. クライアントへ送信: `[サーバ応答内容]`
6. 応答コードが250以外の場合、セッション終了

AUTHコマンド受信時

1. SMTP認証設定が有効の場合
   - 認証成功した場合、クライアントへ送信: `235 ok authed ([製品名])`
   - 認証失敗した場合、クライアントへ送信: `535 authorization failed ([製品名])`
   - サポートしていない認証の場合、(`PLAIN`または`LOGIN`)、クライアントへ送信: 504 this mechanism not available ([製品名])
2. SMTP認証設定が無効の場合、認証要求、認証応答をサーバとクライアント間で転送

DATAコマンド受信時

1. クライアントへ送信: `354 Enter mail ([製品名])`

2. メールデータ受信
3. ウイルス・スパムスキャン
4. ウイルス・スパム検出した場合
   a. ウイルスログへの記録
   b. 管理者への通知(有効な場合)
5. メールサイズが最大メッセージサイズを超えた場合、クライアントへ送信:`554 Too long message ([製品名])`
6. ウイルス・スパム検出した場合で、検出時の動作が"駆除"、"何もしない"、"件名変更"以外の場合
   a. 検出時の動作が拒否の場合
      1. サーバへ送信: `RSET`
      2. サーバ応答受信
      3. 応答コードが250以外の場合、セッション終了
      4. クライアントへ送信: `554 Infected by [検出名称] ([製品名])`
   b. 検出時の動作が送信者へ通知の場合
      1. サーバへ送信: `RSET`
      2. 応答コードが250以外の場合: `554 :SENDBACK:smtp error[RSET]: (Server Reply: [サーバ応答内容]) ([製品名])`
      3. サーバへ送信: `MAIL FROM: [テンプレートの送信者アドレスまたは管理者アドレス]`
      4. 応答コードが250以外の場合、クライアントへ送信: `554 SENDBACK:smtp error[MAIL FROM] (Server Reply: [サーバ応答内容]) ([製品名])`
      5. サーバへ送信: `RCPT TO: <メール送信者アドレス>`
      6. 応答コードが250以外の場合、クライアントへ送信:`554 SENDBACK:smtp error[RCPT TO] (Server Reply: [サーバ応答内容]) ([製品名])`
   c. 検出時の動作が、[送信者へ通知] または [受信者へ通知] の場合
      1. サーバへ送信: `DATA`
      2. 応答コードが354以外の場合、コマンド処理終了
      3. サーバへ送信: `Received: from [クライアントホスト名] ([クライアントIPアドレス]) by [ホスト名] ([製品名])□ [現在時刻 (RFC822 形式)]`
      4. スパム検出した場合、サーバへ送信: `X-Spam-Status: Yes(製品名) with [検出名称]`
      5. ウイルス検出した場合、サーバへ送信: `X-Virus-Status: infected(製品名) with [検出名称]`
      6. サーバへ送信: `Data: [受信メールのDateフィールド内容]`
      7. 検出時の動作が送信者へ通知の場合、サーバへ送信: `To: [受信メールの送信元アドレス]`
      8. 検出時の動作が受信者へ通知の場合
         a. サーバへ送信: `To: [受信メールのToアドレス]`
         b. サーバへ送信: `CC: [受信メールのCcアドレス]`
      9. 感染メール通知テンプレートにFromフィールドがない場合、サーバへ送信:`From: [管理者のメールアドレス]`
      10. サーバへ送信: Content-Transfer-Encoding: 7bit
      11. 感染通知メッセージの内容を送信
      12. サーバへ送信: `"\r\n.\r\n"`
      13. サーバへ送信: サーバ応答内容
      14. 応答コードが250以外の場合、セッション終了

d. 検出時の動作が [削除] の場合

1. サーバへ送信: `RSET`
2. 応答コードが250以外の場合、セッション終了
3. クライアントへ送信: `250 Message accepted for delivery ([製品名])`

7. それ以外の場合

a. サーバへ送信: `DATA`
b. 応答コードが354以外

1. クライアントへ送信: `[サーバ応答内容]`
2. コマンド処理終了

c. 匿名プロキシモードではない場合

1. サーバへ送信: `Received: from [クライアントホスト名] ([クライアントIPアドレス]) by [ホスト名] ([製品名])□ [現在時刻 (RFC822 形式)]`
2. スパム検出した場合、サーバへ送信: `X-Spam-Status: Yes([製品名]) with [検出名称]`
3. ウイルス駆除した場合、サーバへ送信:`X-Virus-Status: disinfected([製品名]) from [検出名称]`
4. ウイルス感染していた場合、サーバへ送信:`X-Virus-Status: infected([製品名]) with [検出名称]`
5. ウイルスを検出しない場合、サーバへ送信: `X-Virus-Status: clean([製品名])`

d. サーバへ送信: メール内容
e. サーバへ送信: サーバ応答内容

8. アクセスログに記録

RSET /XFORWARD /NOOP /EXPNコマンド受信時

1. サーバへ送信: `[クライアント受信内容]`
2. サーバ応答受信
3. クライアントへ送信: `[サーバ応答内容]`

未知のコマンド受信時

1. クライアントへ送信: `500 Unknown Command: "[受信コマンド]" ([製品名])`

9.10 POPコマンド動作概要一覧

POP接続時に、クライアントから送信されたコマンドに対する動作概要は以下のとおりです。

👉 **注:** [製品名] はデフォルトで "F-Secure/fsigk_pop/バージョン/ホスト名" になります。上級者向けオプションの "product_name=" で設定変更可能です。

クライアント接続時

1. "親サーバのユーザによる指定" が無効または透過型の場合

a. サーバへ接続
b. 接続失敗時

1. クライアントへ送信:`-ERR Can't Connect to (サーバホスト: サーバポート) errmsg=[接続エラーメッセージ]`

2. セッション終了

c. サーバ応答受信
d. クライアントへ送信: [サーバ応答内容]

2. それ以外の場合、クライアントへ送信: +OK [製品名] starting.

各コマンド行受信時

1. 1行が998バイト以上の場合、クライアントへ送信: -ERR Too long line
2. サーバに接続しておらず、USER/QUIT以外のコマンドが送信された場合: -ERR please use USER command at first.
3. 1,2以外の場合は各コマンドを処理する。

USERコマンド受信時

1. "親サーバのユーザによる指定" が無効または透過型の場合、サーバへ送信: クライアント受信内容
2. それ以外の場合

a. ユーザ認証が有効でユーザが登録されていない場合、クライアントへ送信: -ERR Invalid Account Auth.
b. ユーザ名に "@" または "#" が含まれる場合、最後の "@" または "#" 以降で指定されたサーバに接続
c. それ以外の場合

1. 親サーバが空の場合、クライアントへ送信: -ERR USER format is USER username@hostname or username#hostname、コマンド処理終了
2. それ以外の場合、親サーバに接続

d. 接続に失敗した場合、クライアントへ送信: -ERR Can't Connect to (サーバホスト: サーバポート) errmsg=[接続エラーメッセージ]
e. サーバへ送信: USER [ユーザ名]
f. サーバ応答受信
g. クライアントへ送信: [サーバ応答内容]

QUITコマンド受信時

1. サーバ接続済みの場合

a. サーバへ送信: [クライアント要求内容]
b. サーバ応答受信
c. クライアントへ送信: [サーバ応答内容]

2. サーバに接続していない場合、クライアントへ送信: +OK Quit

PASS /APOP /AUTHコマンド受信時

1. APOPコマンドでユーザ制限が有効でユーザが登録されていない場合、クライアントへ送信: -ERR Invalid Account Auth.
2. サーバへ送信: クライアント受信内容
3. サーバ応答受信
4. サーバ応答が成功の場合、POP-before-SMTPデータベースに接続元クライアントIPを登録

RETRコマンド受信時

1. サーバへ送信: クライアント受信内容
2. メール受信

3. ウイルススキャン・スパムスキャン
4. ウイルス・スパム検出した場合
   a. ウイルスログへの記録
   b. 管理者への通知(有効な場合)
5. ウイルスを検出し、駆除を行わず、検出時の動作が削除の場合、次のメッセージがクライアントへ送信されます。

   `Received from FSIGK: 現在時刻(RFC822 形式) X-Virus-Status: infected([製品名]) with [検出名称] Date: [ヘッダのDate] (存在する場合) To: [ヘッダのTo] (存在する場合) Cc: [ヘッダのCc] (存在する場合) [感染通知メッセージの内容]`
6. それ以外の場合
   - スパム・ウイルス検出時、クライアントへ送信: Received: from FSIGK: 現在時刻(RFC822形式)
   - スパム検出時、クライアントへ送信: `X-Spam-Status: Yes(製品名) with [検出名称]`
   - ウイルス駆除時、クライアントへ送信:`X-Virus-Status: disinfected(%s) from [検出名称]`
   - ウイルス駆除時、クライアントへ送信:`X-Virus-Status: infected(%s) with [検出名称]`
   - ウイルスを検出しない場合、次のメッセージがクライアントへ送信されます。サーバへ送信: `X-Virus-Status: clean([製品名])`

   クライアントへ送信: メール内容

上記以外のコマンド受信時

1. サーバへ送信: [クライアント受信内容]
2. サーバ応答受信
3. クライアントへ送信: [サーバ応答内容]

9.11 FTPコマンド動作概要一覧

FTP接続時に、クライアントから送信されたコマンドに対する動作概要は以下のとおりです。

注: [製品名]はデフォルトで"F-Secure/fsigk_ftp/バージョン/ホスト名"になります。 上級者向けオプションの"product_name="で設定変更可能です。

クライアント接続時

1. "親サーバのユーザによる指定"が無効または透過型の場合
   a. サーバへ接続
   b. 接続に失敗した場合、クライアントへ送信: `-500 Can't Connect to (サーバホスト: サーバポート) errmsg=[接続エラーメッセージ]`、セッション終了
   c. サーバ応答受信
   d. クライアントへ送信: [サーバ応答内容]
2. それ以外の場合、クライアントへ送信: 220 [製品名] at ホスト名 starting.

各コマンド行受信時

1. 1行が998バイト以上の場合、クライアントへ送信: `500 Too long line`
2. サーバに接続しておらず、USER/QUIT以外のコマンドが送信された場合: `530 please use USER command at first.`
3. 1,2以外の場合は各コマンドを処理する。

USERコマンド受信時

1. "親サーバのユーザによる指定" が無効または透過型の場合、サーバへ送信: クライアント受信内容
2. それ以外の場合
   a. ユーザ認証が有効でユーザが登録されていない場合、クライアントへ送信:`500 Invalid Account Auth.`
   b. ユーザ名に "@" または "#" が含まれる場合、最後の "@" または "#" 以降で指定されたサーバに接続
   c. それ以外の場合
      1. 親サーバが空の場合、クライアントへ送信: `500 USER format is USER username@hostname or username#hostname`、コマンド処理終了
      2. それ以外の場合、親サーバに接続
   d. 接続に失敗した場合、クライアントへ送信: `-500 Can't Connect to (サーバホスト: サーバポート) errmsg=[接続エラーメッセージ]`
   e. サーバへ送信: `USER [ユーザ名]`
   f. サーバ応答受信
   g. クライアントへ送信: `[サーバ応答内容]`

QUITコマンド受信時

1. サーバ接続済みの場合
   a. サーバへ送信: `[クライアント要求内容]`
   b. サーバ応答受信
   c. クライアントへ送信: `[サーバ応答内容]`
2. サーバに接続していない場合、クライアントへ送信: `221 Quit`

PASVコマンド受信時

1. サーバへ送信: `PASV`
2. サーバ応答受信
3. クライアントへ送信: `227 Entering Passive Mode (xx,xx,xx,xx,yy,yy)`

   (xx、yyはプロキシのIPアドレス、ポート番号)

PORTコマンド受信時

1. クライアントへ送信: `PORT (xx,xx,xx,xx,yy,yy)`

   (xx、yyはプロキシのIPアドレス、ポート番号)
2. サーバ応答受信
3. クライアントへ送信: `[サーバ応答内容]`

RETR/LIST/NLST/STOR/STOU/APPEコマンド受信時

1. PASV/PORTを実行していない場合
   a. クライアントへ送信: `530 please use PORT/PASV command at first.`
   b. コマンド処理終了
2. PASVモードの場合
   a. データセッション接続受付

b. データセッションとコントロールセッションの接続元が違う場合、クライアントへ送信: `530 Invalid Connection Source`、コマンド処理終了
c. データセッションでサーバに接続
d. サーバ応答受信
e. サーバへ送信: サーバ応答内容
f. 応答コードが1xx以外の場合、コマンド処理終了

3. Activeモードの場合
   a. サーバ応答受信
   b. 応答コードが1xx以外の場合、コマンド処理終了
   c. データセッションでクライアントへ接続
   d. クライアント接続失敗時
      1. 検出通知メッセージの情報: `530 Cannot connect client`
      2. セッション終了
4. ファイル受信
5. LIST/NLSTコマンド以外でウイルス検出時の場合、クライアントへ送信: `530 Infected by` [検出名]、コマンド終了
6. ファイル転送

上記以外のコマンド受信時

1. サーバへ送信: [クライアント受信内容]
2. サーバ応答受信
3. クライアントへ送信: [サーバ応答内容]

9.12 接続エラーメッセージ一覧

サーバへの接続に失敗した際に表示されるエラーメッセージの一覧です。

CONNECT (ホスト: ポート) /connect: [接続エラー詳細]	サーバのIPアドレスへ接続要求を行ったが失敗した。 接続はLinuxのconnect()システムコールを通じて行います。"接続エラー詳細" には、connect()システムコールのエラーメッセージが含まれ、通常以下のいずれかになります。 **Connection refused** サーバが接続を拒否した。 **Connection timed out** 接続タイムアウトが発生した。 **接続タイムアウトが発生した。** サーバのネットワークに接続できなかった。
CONNECT (ホスト: ポート) /connect timeout (>$1 sec)	接続が指定秒数 ($1) 以内に確立せず、タイムアウトした。 上級者向けオプションのサーバ接続タイムアウト設定 ("connect_timeout=yes, connect_timeout_sec=nnn") を有効にした場合のみ表示されます。
CONNECT (ホスト: ポート) /connect cancelled	接続中にクライアントから切断してキャンセルした場合に表示されます。

CONNECT(ホスト：ポート**)/hostname lookup error:** [名前引きエラー詳細]	ホスト名の名前引きに失敗した。 ホスト名の名前引きはLinux(glibc)のgetaddrinfo()関数を通じて行います。エラーの詳細には、gai_strerror()により人間が読める文字列が含まれます。
CONNECT(ホスト：ポート**)/Access Inhibited by Proxy(FSIGK)**	アクセス制御設定(接続先)により、接続が拒否された。

9.13 サービスプロセス一覧

本製品ではサービス提供のために以下のプロセスが動作します。

fsigk_http HTTPサービス用のプロセス

クライアント、サーバとのHTTP通信を行います。

セッション処理用に最大同時接続数で設定した数のプロセスが動作し、管理用に1プロセスが動作します。

必要に応じて、スキャンエンジンプロセス(fsavd)と通信を行います。通信はUNIXドメインソケット(インストールディレクトリfsavd-socket-0-fsavファイル)を通じて行います。

処理プロセス1個あたりの、共有できないメモリ消費量は500KB未満です。

fsigk_smtp SMTPサービス用のプロセス

クライアント、サーバとのSMTP通信を行います。

セッション処理用に最大同時接続数で設定した数のプロセスが動作し、管理用に1プロセスが動作します。

必要に応じて、スキャンエンジンプロセス(fsavd)と通信を行います。通信はUNIXドメインソケット(インストールディレクトリfsavd-socket-0-fsavファイル)を通じて行います。

処理プロセス1個あたりの、共有できないメモリ消費量は500KB未満です。

fsigk_pop POPサービス用のプロセス

クライアント、サーバとのPOP通信を行います。

セッション処理用に最大同時接続数で設定した数のプロセスが動作し、管理用に1プロセスが動作します。

必要に応じて、スキャンエンジンプロセス(fsavd)と通信を行います。通信はUNIXドメインソケット(インストールディレクトリfsavd-socket-0-fsavファイル)を通じて行います。

処理プロセス1個あたりの、共有できないメモリ消費量は500KB未満です。

fsigk_ftp FTPサービス用のプロセス

クライアント、サーバとのFTP通信を行います。

セッション処理用に最大同時接続数で設定した数のプロセスが動作し、管理用に1プロセスが動作します。

必要に応じて、スキャンエンジンプロセス(fsavd)と通信を行います。通信はUNIXドメインソケット(インストールディレクトリfsavd-socket-0-fsavファイル)を通じて行います。

処理プロセス1個あたりの、共有できないメモリ消費量は500KB未満です。

fsavd スキャンエンジンプロセス

fsavdのプロセス数は/opt/f-secure/fsigk/fssp/etc/fssp.confファイルのdaemonMaxScanProcessesオプションで設定します。デフォルトの値は40です。サービスは/opt/f-secure/fsigk/rc.fsigk_fsavdが制御します。

処理プロセス1個あたりの、共有できないメモリ消費量は50MB未満です。

fsicapd_service ICAPウイルススキャンサービスを提供するプロセスです。

ICAPサービスをHTTPプロキシで利用可能にします。

セッション処理用に最大同時接続数で設定した数のプロセスが動作します。

9.14 検出名称

本製品でウイルスを検出した場合、ウイルス名をログなどに出力します。各ウイルスの情報については以下のウェブページで情報提供しています。

http://www.f-secure.com/en/web/labs_global/threats/descriptions

また、一般的なウイルス以外でも、各種条件により検出する場合があります。この場合の検出名称は"FSIGK/" で始まり、以下のとおりです。

FSIGK/POLICY_FORMAT_MIME_BOUNDARY 不正な文字をメールヘッダのboundary部分に含む

(不正な文字: '"'、0x1f以下のコード、0x7f以上のコード)

FSIGK/POLICY_FORMAT_MIME_FILENAME 不正な文字をメールヘッダのfilename部分に含む

(不正な文字: 0x1f以下のコード(0x1bを除く))

FSIGK/POLICY_BLOCK_ENCRYPTED 暗号化されたファイル(暗号化された圧縮ファイルを拒否する設定の場合)

FSIGK/POLICY_BLOCK_SCRIPT スクリプトを含むHTMLを検出 (スクリプトを拒否する設定の場合)

FSIGK/POLICY_BLOCK_ACTIVEX ACTIVE-Xを含むHTMLを検出 (Active-Xを拒否する設定の場合)

FSIGK/POLICY_BLOCK_PARTIAL_MESSAGE 分割メール (分割メールを拒否する設定にした場合)

FSIGK/POLICY_BLOCK_MAXNESTED 最大圧縮階層を越えた

(上級者向けオプションで、最大圧縮階層を越えた場合に拒否する設定をした場合 (block_maxnested=yes))

FSIGK/POLICY_BLOCK_SCANTIMEOUT 最大スキャン時間以上のスキャン時間が経過した

(上級者向けオプションで、最大スキャン時間を越えた場合に拒否する設定をした場合 (block_scantimeout=yes))

FSIGK/POLICY_BLOCK_MESSAGESIZE メールサイズが指定サイズより大きい場合

(上級者向けオプションでメールサイズ設定を行った場合、または2GBを超えた場合 (block_messagesize_len=xxx))

FSIGK/POLICY_BLOCK_FILESIZE	ファイルサイズが指定サイズより大きい場合 (上級者向けオプションで指定サイズより大きい場合に拒否する設定を行った場合 (block_filesize=yes))
FSIGK/SPAM_LIST/CUSTOM/(条件番号)/(ヘッダフィールド名)	スパムをカスタム条件で検出した。 条件番号はデータベースファイル中で検出した行数です。
FSIGK/SPAM_LIST/UCE/([条件番号])/(ヘッダフィールド名)	スパムをデータベース(未承諾広告)で検出した 条件番号はデータベースファイル中で検出した行数です。
FSIGK/SPAM_LIST/ADVERTISEMENT/(条件番号)/ (ヘッダフィールド名)	スパムをデータベース(広告一般)で検出した 条件番号はデータベースファイル中で検出した行数です。
FSIGK/SPAM_LIST/HTMLMAIL/(条件番号)/ (ヘッダフィールド名)	スパムをデータベース(HTML主体メール)で検出した 条件番号はデータベースファイル中で検出した行数です。
FSIGK/SPAM_LIST/VIRUSERROR /(条件番号)/ (ヘッダフィールド名)	スパムをデータベース(ウイルス・スパム通知メール)で検出した 条件番号はデータベースファイル中で検出した行数です。
FSIGK/SPAM_LIST/ERROR/(条件番号)/ (ヘッダフィールド名)	スパムをデータベース(エラーメール)で検出した 条件番号はデータベースファイル中で検出した行数です。
FSIGK/SPAM_RBL/(検出アドレス)[(RBLサーバ名): (RBL応答アドレス)]	スパムをRBLスキャンで検出した **検出アドレス** RBLサーバに登録されていたアドレス **RBLサーバ名** 検出したRBLサーバ名 **RBL応答アドレス** 検出時のRBLサーバからの応答アドレス
FSIGK/SPAM_SURBL/(検出ドメイン名)[(SURBLサーバ名): (SURBL応答アドレス)]	スパムをSURBLスキャンで検出した **検出ドメイン名** SURBLサーバに登録されていたドメイン名 **SURBLサーバ名** 検出したSURBLサーバ名 **SURBL応答アドレス** 検出時のSURBLサーバからの応答アドレス
FSIGK/DISALLOWED_SITE	URL が拒否したサイトの URL パターンに一致します。
FSIGK/DISALLOWED_CATEGORY/(カテゴリ名)	URL が拒否したサイトのカテゴリと一致します。

9.15 リスクウェア

リスクウェアはマルウェア(悪意のあるソフトウェア)ではありません。リスクウェアはコンピュータに害を与えるためのプログラムではありませんが、誤って用いることで、セキュリティ上の害を与えるこ

とが可能な機能を持っています。これらのプログラムは役に立が、悪用される可能性のある機能を持っています。

これらのプログラムの例は以下のようになります。

- リモート管理プログラム(例: VNC)
- インスタント・メッセンジャー(例: IRC)
- インターネットを通じてファイル転送を行うプログラム
- インターネット電話プログラム(VoIP)

プログラムがリスクウェアとして判定されても、意図して送受信している場合には害はありません。

リスクウェアの検出名称は、"Catagoriy.Platform.Family"という名前になります。

Categoryは以下のいずれかになります。

- 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

Platformは以下のいずれかになります。

- 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

9.16 クラウドサービス

インターネットゲートキーパーは、ネットワーク上のさまざまなサービスに接続して、マルウェア定義アップデートのチェックなどを行います。

注：下記の表に記載されている内容は変更される場合があります。

サービスアドレス	プロトコル	ポート	アクセス済み
aspam.sp.f-secure.com	HTTPS	443	サービスの再起動時に、スパムスキャン中に非常に頻繁に発生する
fsbwserver.f-secure.com	HTTP	80	Every hour
[*.]orsp.f-secure.com 現在使用されている完全なDNS名は次のとおりです。 orsp-c1-ew1.aws.orsp.f-secure.com orsp-c1-ec1.aws.orsp.f-secure.com orsp-c2-ec1.aws.orsp.f-secure.com orsp-c1-ue1.aws.orsp.f-secure.com orsp-c1-ane1.aws.orsp.f-secure.com	HTTP	80	リクエストに応じて、非常に頻繁に発生する