F-Secure Endpoint Proxy

F-Secure Endpoint Proxy は Policy Manager Proxy (PMP) の別名称であり、お客様が使用している Computer Protection 製品を最新の状態にするためにパターンファイルや更新モジュールのダウンロードが行われる際のネットワーク帯域の使用率を低減させるために F-Secure から提供されています。このプロキシは、マルウェアのシグネチャ・データベースである GUTS2 アップデートをキャシュ処理します。万が一、このプロキシが動作していない場合は、Computer Protection クライアントはクラウドにある GUTS2 サーバに直接アクセスして GUTS2 アップデートを取得します。

本書では F-Secure Endpoint Proxy（以降 PMP）の設定方法の詳細を紹介します。また、以下の「ステップ2」で Computer Protection のプロフィールでの利用方法も紹介します。

ステップ1 Policy Manager Proxy のインストール方法

Windows の場合

- 以下のリンクから F-Secure Policy Manager Proxy (PMP) の最新版をダウンロードしてインストールします。

  https://www.f-secure.com/en/web/business_global/downloads/policy-manager

- Windows 版ではインストーラを実行するとウィザードにおいて Policy Manager Server のアドレスを聞かれたら、0.0.0.0 を指定してください。

Linux の場合

- 以下のリンクから F-Secure Policy Manager Proxy (PMP) の最新版をダウンロードしてインストールします。
  https://www.f-secure.com/en/web/business_global/downloads/policy-manager-for-linux

- Policy Manager Proxy のインストール前に以下のように yum コマンドを使用して libstdc++ パッケージをインストールする必要があります。
  - yum install libstdc++.i686
  - yum install libstdc++.x86_64

- Linux ではパッケージのインストール後に以下のコマンドでプロキシを設定します。このコマンドを実行すると質問がいくつかありますが Policy Manager のアドレスには 0.0.0.0 を指定してください。
  - /opt/f-secure/fspms/bin/fspms-config

- 以下のコマンドで PMP の開始、停止、再起動、ステータス表示を管理できます。
  - /etc/init.d/fspms {start|stop|restart|status}

  例えば、開始する場合は以下のコマンドを実行します。

  /etc/init.d.fspms start

アクセスログ

PMP のアクセスログは以下でアクセスできます。アクセスログではクライアントに提供したアップデート情報を確認できます。

Windows

<installation_directory>/F-Secure/Management Server 5/logs

Linux

/var/opt/f-secure/fspms/logs

このフォルダに以下のログファイルがあります。

request.log – クライアントから受け取った要求とその応答ステータス

例えば、503 は "come later, the update is not downloaded from GUTS2 yet" を意味します。

fspms-server-updates.log – クライアントからの要求された内容

fspms-download-updates.log – GUTS2 サーバからのダウンロード情報

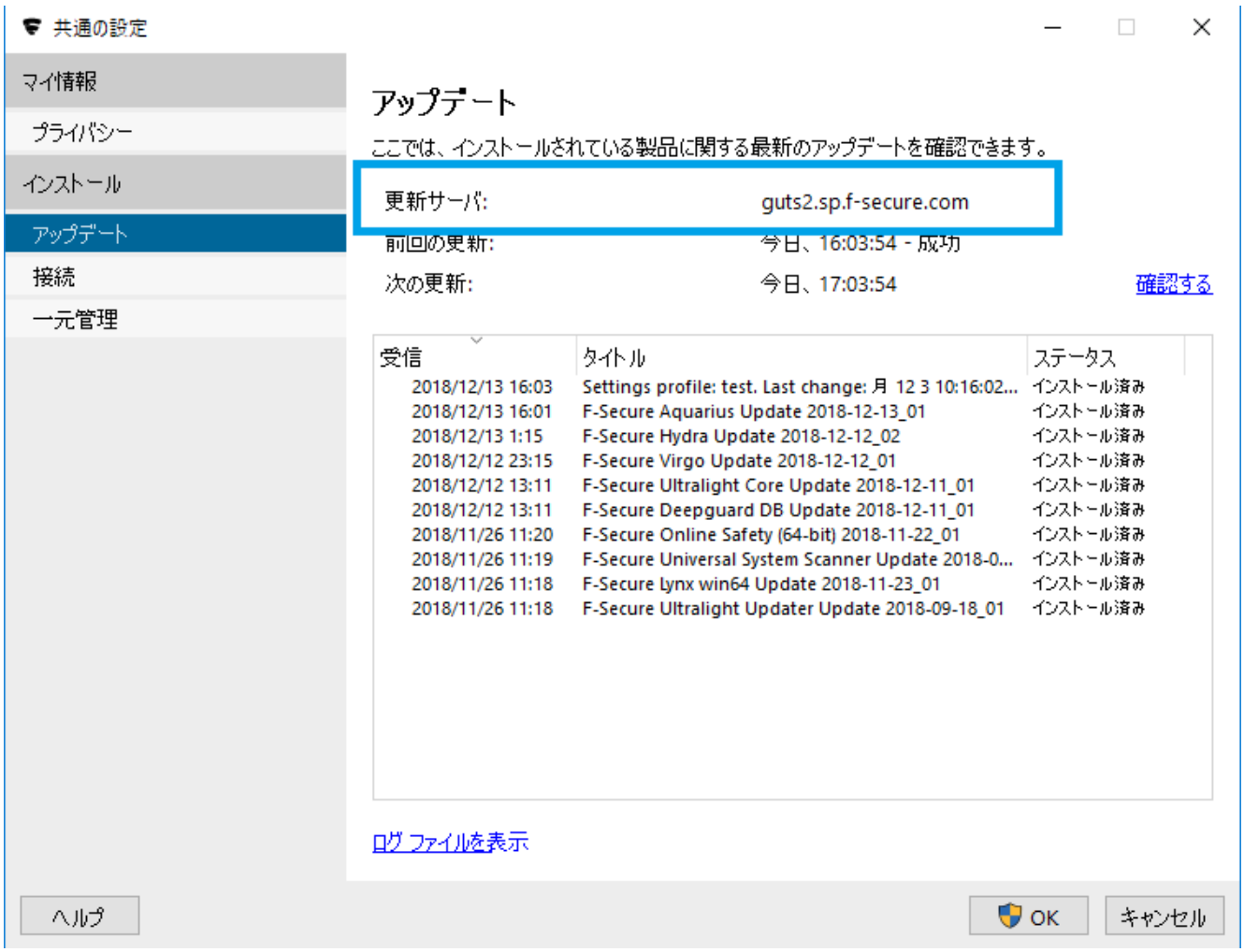
ステップ2 Computer Protection プロフィールにおいて、プロキシを使用するように設定する

PSB 管理ポータルにおいて、プロフィールエディタを使って目的のプロフォールを編集します。

「プロフィール」→「Computer Protection for Windows」タブをアクセスし、変更したいプロフィールを選択してください。以下の図にように「一般設定」における「F-Secure Endpoint Proxy」項目を探し、そのアドレスを入力します。

この設定は、当該プロフィールを発行し、そのプロフィールが適用された Computer Protection クライアント側でも確認することができます。

クライアント側での確認方法
クライアントの UI において「ツール」→「更新」をクリックします。



アップデートの画面の「更新サーバ」の部分が、プロフィールにて設定した PMP のアドレスになっているかどうかで確認が可能です。

上記の画面はデフォルトの GUTS2 サーバの場合ですが、PMP を使用するように設定したプロフィールでは、この項目が対象のアドレスになります。

この状態で「確認する」をクリックし、更新がエラーなく行われるかを確認してください。

注意:

F-Secure Endpoint Proxy (Policy Manager Proxy) はデフォルトでポートを利用します。Windows ファイアウォールでこのポートがブロックされないようにご注意ください。

本書は以下の英文　Community の記事の日本語版となります。

F-Secure Endpoint Proxy

https://community.f-secure.com/t5/Protection/F-Secure-Endpoint-Proxy/m-p/109699#M1148

以上