ESET File Security for Linux
マニュアル

目次

■本書について

○本書は、各ライセンス製品に含まれる「ESET File Security for Linux」プログラムの共通のマニュアルのため、ご購入いただきました製品によっては、一部ご利用いただけない機能があります。

■お断り

[Chapter 1]
はじめに

1.1 ESET File Security for Linuxについて

ESET File Security for Linuxは、Linuxサーバー専用に設計された軽量かつ強力な保護機能を提供するウイルス・スパイウェア対策製品です。ESET File Security for Linuxは、既知または未知のウイルス、ワーム、トロイの木馬、スパイウェアなどのインターネットの脅威からLinuxサーバーを効率的に保護します。ESET File Security for Linuxには、次のような主要機能があります。

●オンデマンドスキャン
コマンドラインまたはWebインターフェースを使用して、選択したディレクトリを検査したり、定期的な検査タスクを設定できます。

●オンアクセススキャン（リアルタイムスキャン）
標準Cライブラリを使用するアプリケーションによってアクセスされるファイルを監視します。

●集中管理　※1
ESET Remote Administratorを利用して、ESET File Security for Linuxをリモートで管理できます。

●Webインターフェース
コマンドラインインターフェースに代わる使いやすいGUIベースの管理画面を搭載しています。ESET File Security for Linuxのさまざまな設定をWebブラウザーで行うことができます。

●スケジューラ
ソフトウェアの管理を簡素化し、さまざまなプログラムのコンポーネントに対して複数のタスクとアクションを設定できます。

●ミラーサーバー機能　※1
ローカル環境にアップデートサーバーを作成できます。クライアントコンピューターは、インターネット上にあるESETのサーバーからウイルス定義データベースをダウンロードせずに、ローカルネットワーク上に作成したアップデートサーバーからダウンロードすることが可能です。

※1　サーバー専用ウイルス・スパイウェア対策ソフトESET File Security for Linux／Windows Serverでは、本機能はご利用いただけません。

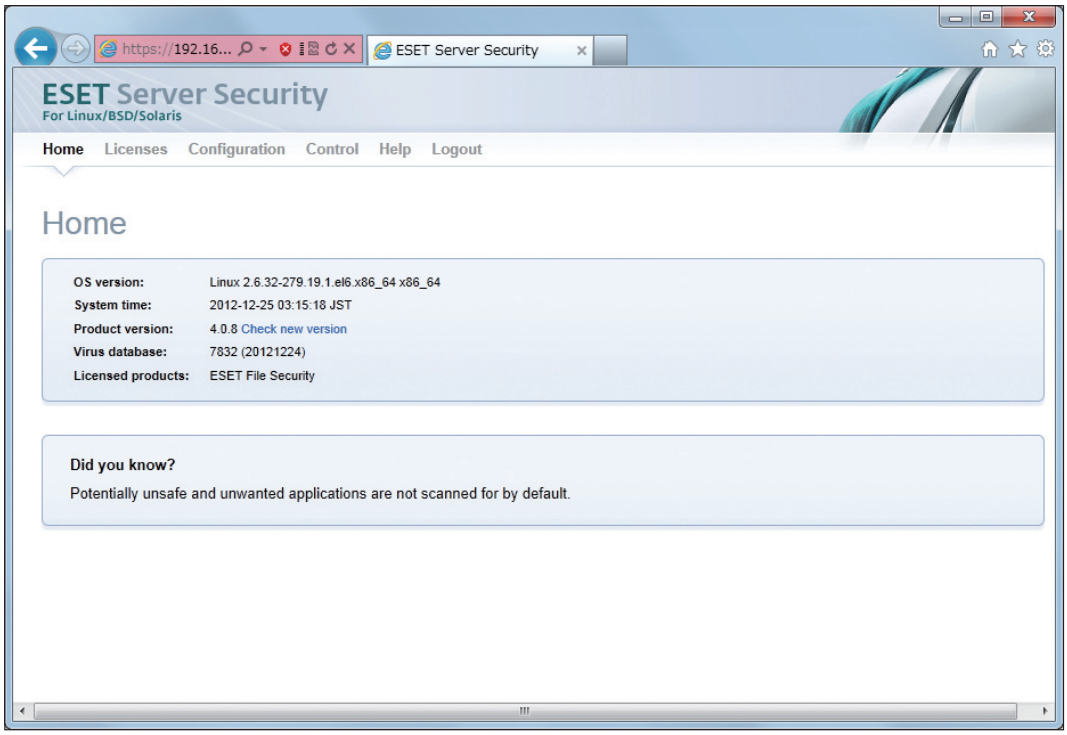
1.2 保護の種類

ESET File Security for Linuxは、オンデマンドスキャンまたはオンアクセススキャン（リアルタイムスキャン）によってさまざまな脅威から保護します。オンデマンドスキャンでは、コマンドラインまたはWebインターフェースを使用して、選択したディレクトリを検査できます。

オンアクセススキャン（リアルタイムスキャン）では、標準Cライブラリを使用するアプリケーションによって発生するファイルシステムへのアクセスを監視し、リアルタイムで検査を実施します。これによって、ウイルスなどの侵入を防ぎます。また、悪意のあるコードを含むウイルスが検出されると、あらかじめ定義しておいたルールに応じて処理を行います。

1.3 ユーザーインターフェース

ESET File Security for Linuxには、上級者向けのコマンドラインインターフェースとWebインターフェースが準備されています。既定値では、コマンドラインインターフェースのみが利用できます。Webインターフェースを利用するには、本製品の各種設定を管理する「eset.cfg」ファイルを編集する必要があります。Webインターフェースでは、簡単に本製品の各種設定を変更できるほか、オンデマンドスキャンやウイルス定義データベースのダウンロードなどを実行できます。



[Chapter 2]
インストール

2.1 インストールについて

ESET File Security for Linuxのインストールは、コマンドラインで行います。root権限（スーパーユーザー）でインストール作業を行ってください。グラフィカルデスクトップを利用しているときは、ターミナルウィンドウを開いて作業を行ってください。また、本製品のインストールの前に以下のものをご準備ください。

●インストーラー

本製品のインストーラーは、弊社ユーザーズサイトからダウンロードできます。32bit版と64bit版が準備されていますので、ご利用の環境に合わせてインストーラーを準備してください。

●ライセンスキーファイル（.licファイル）

本製品を新規インストールする場合は、「ライセンスキーファイル（.licファイル）」が必要になります。「ESETライセンス製品 ご利用の手引」※1を参考にライセンスキーファイル（.licファイル）をユーザーズサイトからダウンロードしてください。

●ユーザー名とパスワード

ウイルス定義データベースなどをダウンロードする際に、「ユーザー名」と「パスワード」を利用します。ユーザー名とパスワードは、弊社ユーザーズサイトで確認できます。

▸▸▸ POINT

インストーラー、ライセンスキーファイル、ユーザー名、パスワードは、ユーザーズサイトから入手できます。入手方法につきましては、「ESETライセンス製品　ご利用の手引」※1をご参照ください。

※1　サーバー専用ウイルス・スパイウェア対策ソフトESET File Security for Linux／Windows Serverをお持ちの方は、「ご利用までの流れ」をご参照ください。

2.1.1 ESET File Security for Linuxのディレクトリ構成

本製品をインストールすると、以下のディレクトリが作成され各種ファイルが保存されます。

名称	パス	概要
ウイルス定義データベースディレクトリ	/var/opt/eset/esets/lib	このディレクトリには、ウイルス定義データベースなどを含むロータブルモジュールが保存されています。
コンフィグレーションディレクトリ	/etc/opt/eset/esets	このディレクトリには、本製品の設定ファイルが保存されています。
プログラムディレクトリ	/opt/eset/esets/bin	このディレクトリには、本製品のプログラムが保存されています。
システムプログラムディレクトリ	/opt/eset/esets/sbin	このディレクトリには、本製品のシステムプログラムが保存されています。
ライブラリディレクトリ	/opt/eset/esets/lib /opt/eset/esets/lib64	このディレクトリには、本製品のライブラリが保存されています。32bit版の場合は/libのみ、64bit版の場合は/lib、/lib64のディレクトリが両方作成されます。
ERAログデータディレクトリ	/var/log/esets	このディレクトリには、ESET Remote Administratorに送信するログが保存されています。
隔離データディレクトリ	/var/opt/eset/esets/cache/quarantine	このディレクトリには、ウイルスが隔離された場合のデータが保存されています。

2.2 インストール要件

ESET File Security for Linuxは、Linux専用の製品です。動作環境については、弊社ホームページをご参照ください。

2.3 インストール手順

ここでは、ESET File Security for Linuxのインストール手順を説明します。本製品のインストールは、弊社ユーザーズサイトからダウンロードしたインストーラーを利用して、コマンドラインで行います。インストール作業は、root権限（スーパーユーザー）で行ってください。また、他社製のアンチウイルスソフトがインストールされている場合は、必ずアンインストールを行ってください。

2.3.1 インストール手順

ここでは、「/tmp」にインストーラーが保存されている場合を例にインストール手順を紹介します。

1 コマンドラインで以下のように入力し、[Enter] キーを押します。

```
#sh /tmp/ インストーラーファイル名
```

サンプル例

インストーラーのファイル名が、「esets.x86_64.rpm.bin」である場合は、以下のように入力します。

```
#sh /tmp/esets.x86_64.rpm.bin
```

2 画面にメッセージが表示されます。[Enter] キーを押すと使用許諾契約書が表示されます。[Enter] キーを押し、使用許諾契約書を読みます。

3 画面に以下のように表示されます。[y] キーを押します。

```
Do you accept this Agreement? (y/n)
```

4

```
We will only use this information and data to study the threat and will take
reasonable steps to preserve the confidentiality of such information.

Do you accept this Agreement? (y/n) y
Verifying MD5 checksum: ok
Unpacking esets modules ...

To COMPLETE INSTALLATION or UPDATE the Product:
   * Import the license file: /opt/eset/esets/sbin/esets_lic --import file.lic
   * Enter acquired username/password information into the global section
     of main configuration file /etc/opt/eset/esets/esets.cfg
   * Start main daemon service: /etc/init.d/esets start

To UNINSTALL the Product:
   * Uninstall the package: rpm -e esets

To KEEP your KNOWLEDGE Up-To-Date:
   * Read the User's Guide in /opt/eset/esets/share/doc.
   * Read manual page esets.cfg(5) (use 'man esets.cfg').

To REPORT Bugs or Problems:
   * Please, visit: www.eset.com/support

[root@localhost ~]#
```

インストール作業が行われ、左の画面が表示されます。

CAUTION

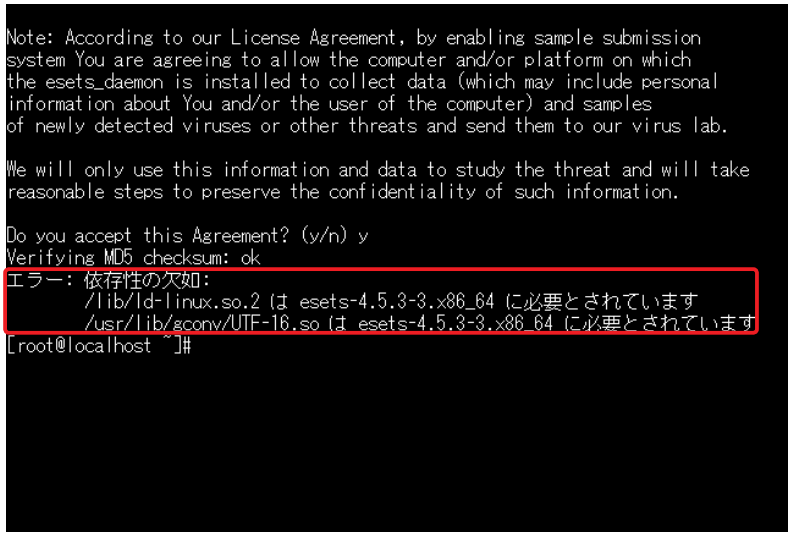
64bitのLinuxサーバーへ本製品をインストールする場合は、64bitと32bitのglibcが必要になります。以下の画面が表示され、依存性のエラーが出力された場合は、15ページの「64bit 版OS にインストールする時の注意点」を参照してください。

```
Note: According to our License Agreement, by enabling sample submission
system You are agreeing to allow the computer and/or platform on which
the esets_daemon is installed to collect data (which may include personal
information about You and/or the user of the computer) and samples
of newly detected viruses or other threats and send them to our virus lab.

We will only use this information and data to study the threat and will take
reasonable steps to preserve the confidentiality of such information.

Do you accept this Agreement? (y/n) y
Verifying MD5 checksum: ok
エラー: 依存性の欠如:
        /lib/ld-linux.so.2 は esets-4.5.3-3.x86_64 に必要とされています
        /usr/lib/gconv/UTF-16.so は esets-4.5.3-3.x86_64 に必要とされています
[root@localhost ~]#
```

2.3.2　64bit版のLinuxにインストールする場合の注意点

64bit版LinuxにESET File Security for Linuxをインストールする場合、以下のような依存性の欠如エラーが表示されインストールできないことがあります。このエラーは32bitのglibcがインストールされていない場合に表示されます。この画面が表示されたときは、以下のパッケージをインストールしてから再度インストールを実行してください。なお、Linuxのインストール時に「互換性ライブラリ」のパッケージを選択することでも32bitのglibcがインストールされます。

・glibc-2.17-106.e17_2.4.rpm
・nss-softokn-freebl-3.16.2.3-13.e17_1.i686.rpm
（※環境によってバージョンが異なる場合があります。）



2.4 ライセンスキーファイルのインポート

ESET File Security for Linuxを利用するには、ライセンスキーファイルのインポートを行う必要があります。ここでは、ライセンスキーファイルのインポート手順を説明します。ライセンスキーファイルは、弊社ユーザーズサイトからダウンロードできます。

2.4.1 ライセンスキーファイルのインポート手順

ここでは、「/tmp」にライセンスキーファイルが保存されている場合を例にインポート手順を紹介します。ライセンスキーファイルのインポートは、root権限（スーパーユーザー）で行う必要があります。コマンドラインで以下のように入力し、[Enter] キーを押します。

```
#/opt/eset/esets/sbin/esets_lic --import /tmp/ ライセンスキーファイル名
```

サンプル例

ライセンスキーファイルのファイル名が、「nod32.lic」である場合は、以下のように入力します。

```
#/opt/eset/esets/sbin/esets_lic --import /tmp/nod32.lic
```

2.4.2 インポートしたライセンスキーファイルの確認

コマンドラインで以下のように入力し [Enter] キーを押すと、インポートしたライセンスキーファイルの情報を確認できます。

```
#/opt/eset/esets/sbin/esets_lic --list
```

2.4.3 ESET File Security for Linuxの起動

ライセンスキーファイルのインポートが完了すると、ESET File Security for Linuxを起動することができます。
コマンドラインで以下のように入力し [Enter] キーを押すと、ESET File Security for Linuxを起動できます。この作業は、root権限（スーパーユーザー）で行う必要があります。

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

2.5 Webインターフェースの初期設定

ESET File Security for Linuxの既定値では、コマンドラインインターフェースのみが利用でき、Webブラウザーで各種設定を行うWebインターフェースは利用できません。Webインターフェースを利用する場合は、ESET File Security for Linuxの各種設定を管理している「esets.cfg」ファイルの編集を行います。ここでは、Webインターフェースの初期設定について説明します。

2.5.1 Webインターフェースの設定

Webインターフェースを利用する場合は、「esets.cfg」ファイルの［wwwi］セクションの以下の5項目を変更します。この作業は、root権限（スーパーユーザー）で行ってください。

「esets.cfg」ファイル保存ディレクトリ:/etc/opt/eset/esets

```
[wwwi]
agent_enabled = yes          ------- Web インターフェースの利用の有無の設定
listen_addr = "IP アドレス "  ------- Web インターフェースへの接続を受けつける
                                     ネットワークインターフェースの IP アドレス
listen_port = ポート番号      ------- 接続に利用するポート番号
username = " ユーザー名 "     ------- ログインに利用するユーザー名
password = " パスワード "     ------- ログインに利用するパスワード
```

サンプル例

ESET File Security for Linuxをインストールしたコンピューターの IPアドレスが「192.168.1.100」、接続に利用するポート番号が「38000」、ログインに利用するユーザー名が「user」、パスワードが「password」の場合は、以下のように入力します。

```
[wwwi]
agent_enabled = yes
listen_addr = "0.0.0.0"
listen_port = 38000
username = "user"
password = "password"
```

▸▸▸ POINT

listen_addr に「0.0.0.0」を入力すると、ESET File Security for Linuxをインストールしたコンピューターの全てのネットワークインターフェースでWebインターフェースへの接続を受けつけます。Webインターフェースへの接続を受けつけるネットワークインターフェースを限定したい場合、そのネットワークインターフェースに設定されているIPアドレスをlisten_addrに入力してください。（上記の例では「192.168.1.10」を入力してください。）

2.5.2 ESET File Security for Linuxの再起動

「esets.cfg」ファイルの変更内容を反映するためには、ESET File Security for Linuxを再起動する必要があります。コマンドラインで以下のように入力し [Enter] キーを押すと、ESET File Security for Linuxを起動できます。この作業は、root権限（スーパーユーザー）で行う必要があります。

```
#/etc/init.d/esets restart
```

2.5.3 Webインターフェースの利用

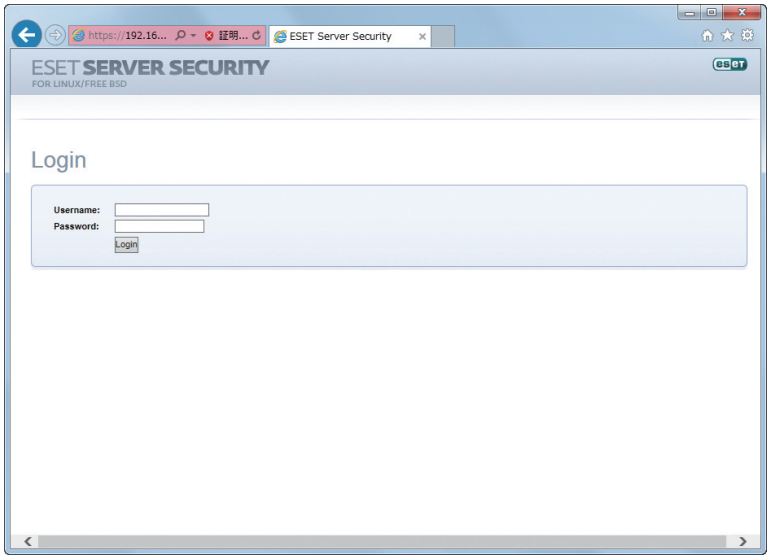
Webインターフェースを利用するときは、Webブラウザーを起動し、「https://IPアドレス:ポート番号」でページを開くと、ログイン画面が表示されるので、2.6.1で設定したユーザー名とパスワードを入力してログインします。Webインターフェースでは、暗号化通信のみがサポートされています。

実行例

IPアドレスが「192.168.1.10」、接続に利用するポート番号が「38000」の場合は、Webブラウザーのアドレスバーに以下のように入力します。

```
https://192.168.1.10:38000
```

以下のような画面が表示されたら、「esets.cfg」ファイルの [wwwi] セクションにて、username、password に設定したユーザー名とパスワードを入力して「login」をクリックしてログインしてください。



POINT

ログイン画面が表示されない場合は、ESET File Security for Linuxをインストールしたコンピューターのファイアウォールの設定を確認してください。設定したポート番号が外部からの通信を受け付ける設定になっていないとログイン画面が表示されません。

CAUTION

ESET File Security for LinuxのWebインターフェースは既定では自己署名証明書を利用しているため、Webブラウザによっては警告画面が表示される場合があります。

2.6 アンインストール手順

ここでは、ESET File Security for Linuxのアンインストール手順を説明します。アンインストール作業は、コマンドラインで行います。また、root権限（スーパーユーザー）で作業してください。

アンインストールは、コマンドラインで以下のように入力し、［Enter］キーを押します。

```
#rpm -e esets
```

2.7 バージョンアップ

ここでは、ESET File Security for Linuxのバージョンアップの方法を説明します。
バージョンアップの手順は新規インストール手順と同様です。バージョンアップではライセンスや設定が引き継がれます。

CAUTION

ESET File Security for Linux V4.0.XからV4.5.3へバージョンアップする場合は、バージョンアップ作業を行う前に以下の手順を実施し、旧バージョンのウイルス定義データベースの領域をリネームしてください。

1. ESET File Security for Linuxのプロセスを停止
   # /etc/init.d/esets stop

2. ウイルス定義データベースの領域をリネーム
   # mv /var/opt/eset/esets/lib /var/opt/eset/esets/bak.lib

ウイルス定義データベース領域のリネーム完了後に「2.7.1 バージョンアップ手順」に従いバージョンアップを実施してください。
なお、バージョンアップ完了後は/var/opt/eset/esets/bak.libは使用しません。

2.7.1 バージョンアップ手順

ここでは「/tmp」にバージョンアップ用のインストーラーが保存れている場合を例にバージョンアップ手順を紹介します。

1 コマンドラインで以下のように入力し、[Enter] キーを押します。

```
#sh /tmp/ インストーラーファイル名
```

サンプル例

インストーラーのファイル名が、「esets.x86_64.rpm.bin」である場合は、以下のように入力します。

```
# sh /tmp/esets.x86_64.rpm.bin
```

2 画面にメッセージが表示されます。[Enter] キーを押すと使用許諾契約書が表示されます。[Enter] キーを押し、使用許諾契約書を読みます。

3 画面に以下のように表示されます。同意したら [y] キーを押し、[Enter] キーを押します。

```
Do you accept Agreement?(y/n)
```

POINT

[n] キーを押した場合、本製品のインストールがキャンセルされます。

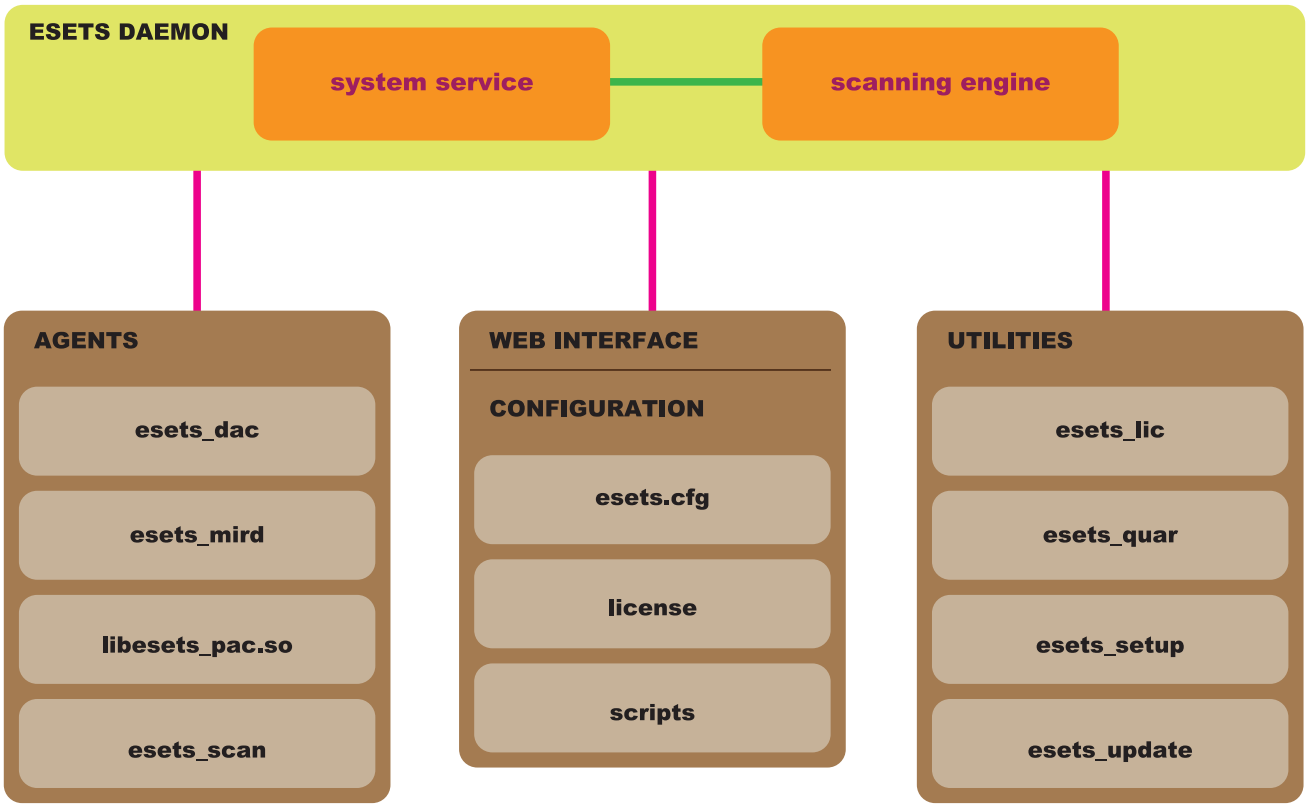
4

```
We will only use this information and data to study the threat and will take
reasonable steps to preserve the confidentiality of such information.

Do you accept this Agreement? (y/n) y
Verifying MD5 checksum: ok
Unpacking esets modules ...

To COMPLETE INSTALLATION or UPDATE the Product:
   * Import the license file: /opt/eset/esets/sbin/esets_lic --import file.lic
   * Enter acquired username/password information into the global section
     of main configuration file /etc/opt/eset/esets/esets.cfg
   * Start main daemon service: /etc/init.d/esets start

To UNINSTALL the Product:
   * Uninstall the package: rpm -e esets

To KEEP your KNOWLEDGE Up-To-Date:
   * Read the User's Guide in /opt/eset/esets/share/doc.
   * Read manual page esets.cfg(5) (use 'man esets.cfg').

To REPORT Bugs or Problems:
   * Please, visit: www.eset.com/support

[root@localhost ~]#
```

左の画面に遷移したらバージョンアップ終了です。

2.8 プログラムの基本構成

ここでは、ESET File Security for Linuxの基本構成を説明します。



●ESETS DAEMON

ESET File Security for Linuxのメインプログラムは、ESETS daemonです。ESETS daemonは、ESETS APIライブラリや各種モジュールの維持、システムの保守、ログの取得、通知などの基本的なシステムタスクを提供しています。ESETS daemonの起動や停止、再起動などの操作は、コマンドラインで以下のように入力します。

・ESETS daemonの起動

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

・ESETS daemonの停止

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

・ESETS daemonの再起動

```
#/etc/init.d/esets restart
```

●AGENTS

オンデマンドスキャンやオンアクセススキャン（リアルタイムスキャン）、ミラーサーバーなどの機能を提供するモジュールで構成されています。

●UTILITIES

ライセンス管理や隔離したウイルスの管理、システムのセットアップやアップデートなどのシステムタスクの管理を行うためのモジュールです。これらのユーティリティは、コマンドラインで利用できます。

●CONFIGURATION

ESET File Security for Linuxでは、以下のようなファイルやディレクトリが各種管理に利用されています。

/etc/opt/eset/esets/esets.cfg
ESET File Security for Linuxの動作に関する重要なファイルです。このファイルを編集することでESET File Security for Linuxの各種設定を変更できます。

/etc/opt/eset/esets/scripts/license_warning_script
このスクリプトは、ライセンスの有効期限が30日前になると一日一回、システム管理者に有効期限のステータスに関する電子メールを送信します。このスクリプトは、「license expiration」という名称でスケジューラに登録されており、既定値で「オン」に設定されています。

/etc/opt/eset/esets/scripts/daemon_notification_script
このスクリプトは、オンアクセススキャン（リアルタイムスキャン）でウイルスが検出された場合にシステム管理者に電子メールで通知します。このスクリプトは、「Threat notification」という名称でスケジューラに登録されており、既定値で「オフ」に設定されています。

●Web INTERFACE

ESET File Security for Linuxの動作に関する各種設定やライセンス管理などをWebブラウザーで行うための機能です。ESET File Security for Linuxの設定は、「esets.cfg」ファイルを直接編集することでも行えますが、Webインターフェースを利用することでより簡単に各種設定を行えます。

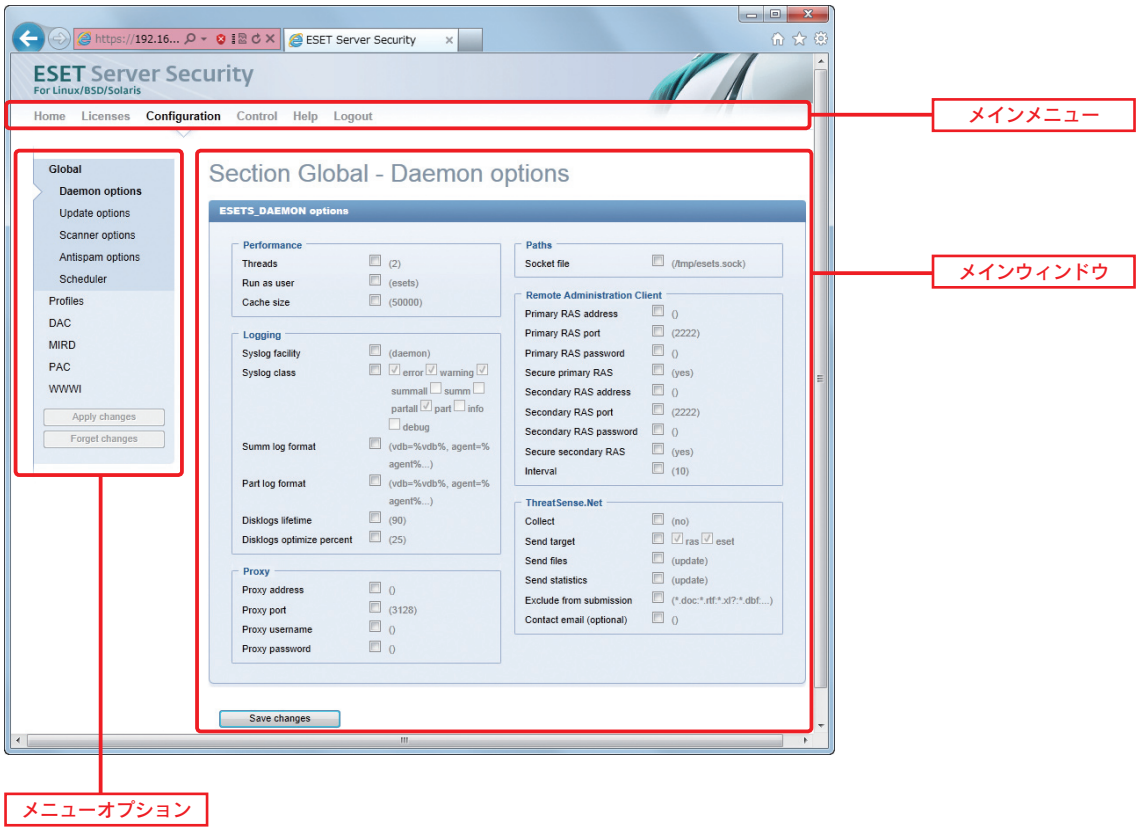
[Chapter 3]
設定ガイド

3.1 Webインターフェースの概要

3.1.1 Webインターフェースのデザイン概要

ESET File Security for LinuxのWebインターフェースは、画面上部にメインメニューが並び、画面中央に選択したメニューの内容を表示するメインウィンドウが配置されています。また、選択したメインメニューの項目によっては、メニューオプションが画面左に表示される場合があります。メインメニューには、以下の項目が準備されています。

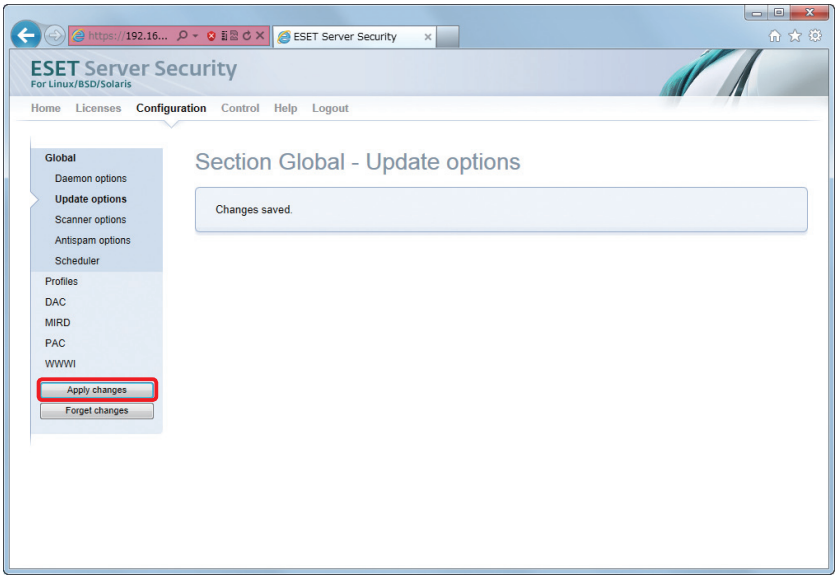
項目名	概要
Home	利用しているコンピューターの基本的なシステム情報とESETの製品情報が表示されます。
Licenses	ライセンスの管理を行えます。
Configuration	ESET File Security for Linuxの動作に関する各種設定を行えます。
Control	ウイルス定義データベースの手動アップデートやオンデマンドスキャンの実行、スキャン結果の統計情報、隔離ファイル管理などが行えます。
Help	Webインターフェースに関するヘルプが表示されます。 [Help]→[Links]のSupport formでは弊社のサポートを受けられないため、お問い合わせの際は弊社ホームページのサポートフォームをご利用ください。
Logout	Webインターフェースからログアウトします。



3.1.2 Webインターフェースでの設定の反映

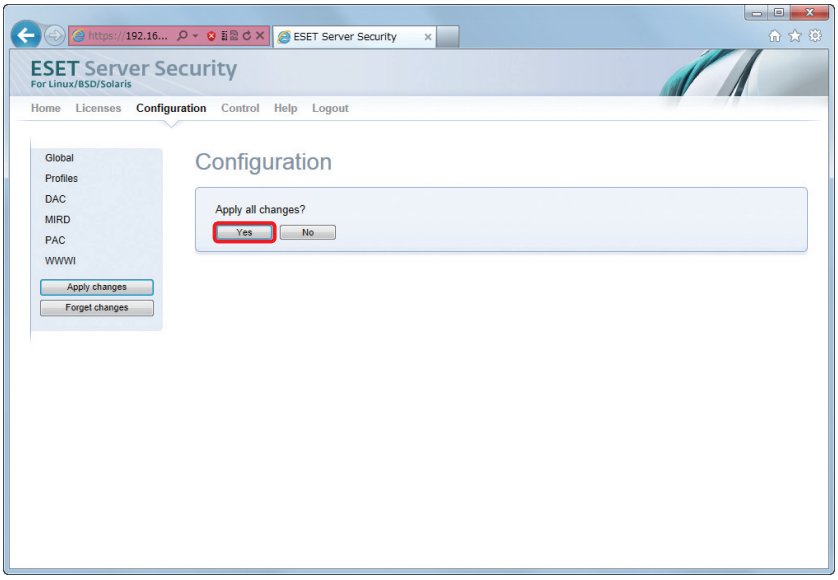
Webインターフェースで [Configuration] の変更を行った場合は、設定の反映が必要になります。各設定変更後は、メインウィンドウの [Save changes] ボタンをクリックして設定の変更を保存しますが、このままでは反映されません。ここでは、すべての設定の変更を保存した後、反映させるための手順を説明します。

1



[Apply changes] ボタンをクリックします。

2



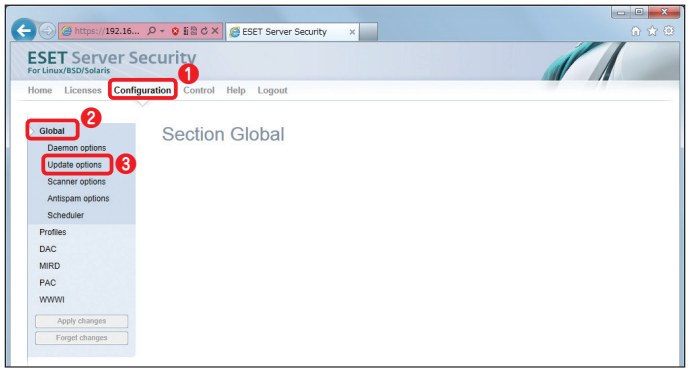
[Yes] ボタンをクリックします。

3.2 ウイルス定義データベースのアップデート

3.2.1 アップデートの設定

ここでは、ウイルス定義データベースのアップデート設定の手順を説明します。

1

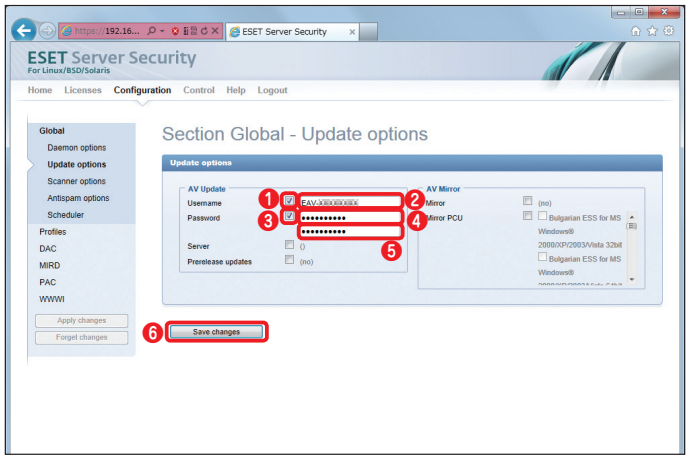


Webブラウザーを開き、Webインターフェースのページを開きます。❶[Configuration]をクリックします。❷[Global]をクリックし、❸[Update options]をクリックします。

POINT

ウイルス定義データベースのアップデートには、「ユーザー名」と「パスワード」が必要です。ユーザー名とパスワードは、弊社ユーザーズサイトで確認できます。事前にチェックしておいてください。

2



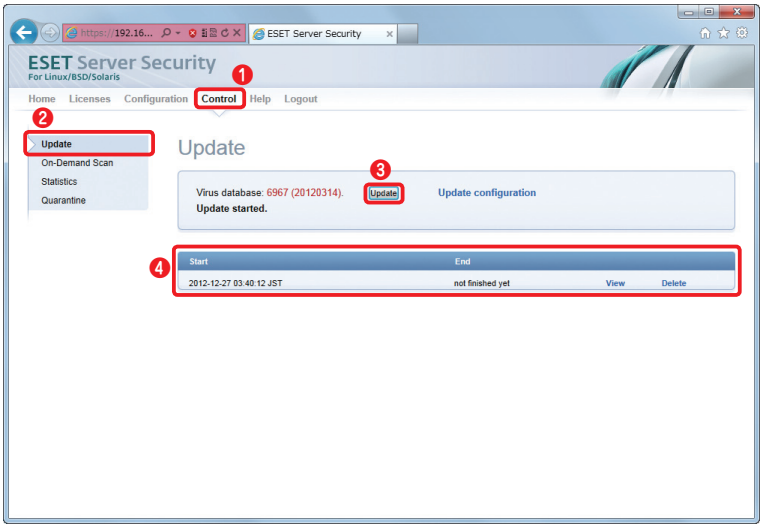
❶[Username]にチェックを入れ、❷「ユーザー名」を入力します。❸[Password]にチェックを入れ、❹パスワードを入力して、❺パスワードを再入力します。❻[Save changes]ボタンをクリックします。

設定を反映させるために、メニューオプションの[Apply changes]ボタンをクリックします。問題がなければメインウィンドウに表示される[Yes]ボタンをクリックします。(参考情報「3.1.2 Webインターフェースでの設定の反映」)

3.2.2　アップデートの手順

ここでは、ウイルス定義データベースのアップデート手順を説明します。

1



❶ [Control] をクリックし、❷ [Update] をクリックします。❸ [Update] ボタンをクリックします。❹ウイルス定義データベースのアップデートが開始されます。[View] をクリックすると、アップデートの状況を確認できます。

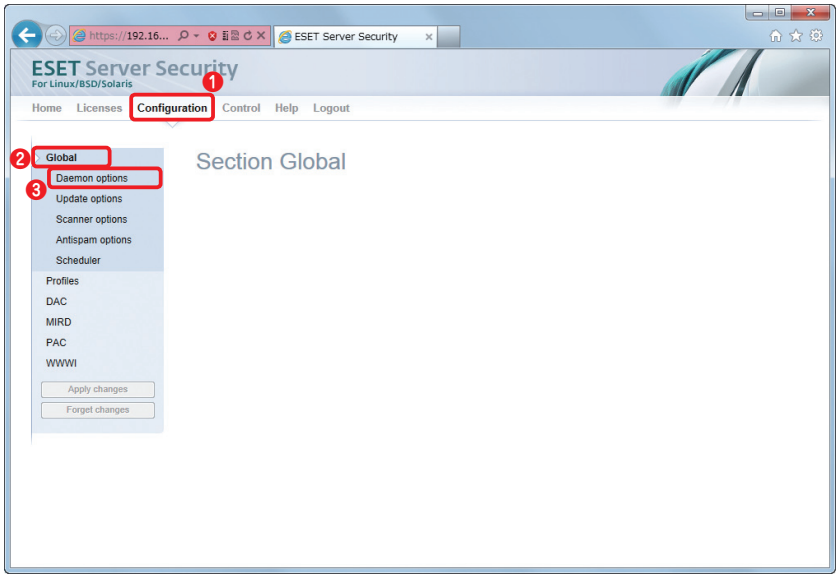
POINT

ウイルス定義データベースのアップデートは、既定値で1時間に1回自動的に行うようにスケジュール設定がなされています。スケジュールの設定については、「3.8　スケジューラの設定」をご参照ください。

3.3 プロキシサーバーの設定

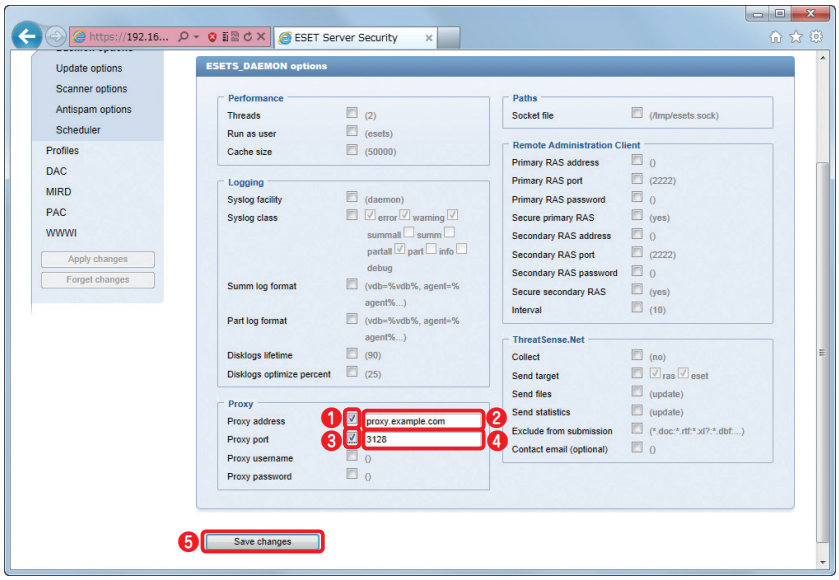
インターネットへのアクセスの際にプロキシサーバーを経由する必要があるネットワーク環境でESET File Security for Linuxを利用する場合は、プロキシサーバーの設定を行う必要があります。ここでは、プロキシサーバーの設定手順を説明します。

1



Webブラウザーを開き、Webインターフェースのページを開きます。❶[Configuration]をクリックします。❷[Global]をクリックし、❸[Daemon options]をクリックします。

2



❶[Proxy address]にチェックを入れ、❷プロキシサーバーのIPアドレスまたはサーバー名を入力します。❸[Proxy port]にチェックを入れ、❹ポート番号を入力します。❺[Save changes]ボタンをクリックします。

設定を反映させるために、メニューオプションの[Apply changes]ボタンをクリックします。問題がなければメインウィンドウに表示される[Yes]ボタンをクリックします。(参考情報「3.1.2 Webインターフェースでの設定の反映」)

3.4 基本的なウイルス対策の設定

ESET File Security for Linuxでは、オンアクセススキャン（リアルタイムスキャン）とオンデマンドスキャンの二種類のウイルス検査方法があります。ここでは、ウイルス検査を行う対象の設定やウイルスを検出したときの処理など、二種類のウイルス検査方法に共通する基本的なウイルス対策の設定をWebインターフェースから行う方法を説明します。それぞれ固有の設定に関しては、オンデマンドスキャンは30ページ、オンアクセススキャン（リアルタイムスキャン）は33ページから説明します。

3.4.1 ウイルス対策の基本設定項目

ウイルス対策の基本設定は、Webインターフェースを開き、[Configuration]→[Global]→[Scanner options]をクリックして設定を行います。ここでは、ESET File Security for Linuxでウイルス対策を行うための基本的な設定項目について説明します。ここに記載されていない項目については、ESET Security for Linux設定リファレンスをご参照ください。

▸▸▸ POINT

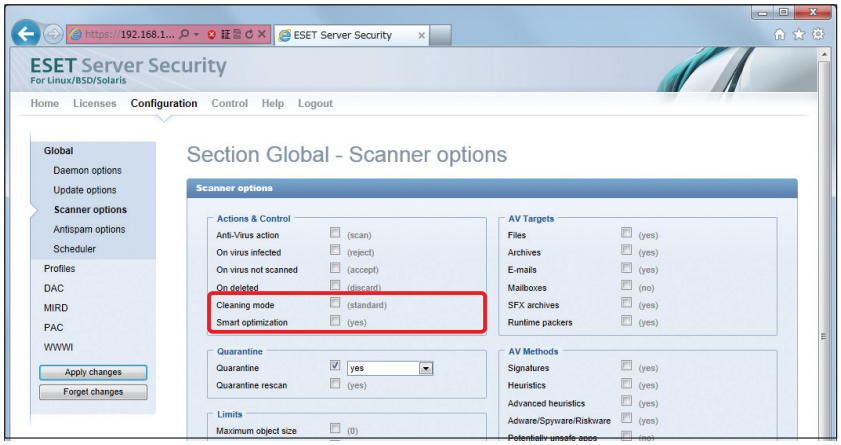
設定リファレンスのリンクについては「3.15 設定リファレンスについて」をご参照ください。

CAUTION

[Configuration]→[Global]→[Scanner options]で設定した項目は、[Profile]、[PAC]などの既定値を変更するためのものであり、実際には[Profile]、[PAC]で設定した値に基づいて検査されます。

Scanner options - Actions & Control

このセクションでは、ファイル検査時のオプションやウイルスを検出したときの駆除モード（「Cleaning mode」）などの設定を行います。また、Smart optimizationが有効な場合、システムへの負荷を最小限にするために、検査済みのファイルは、新たなウイルス定義データベースが提供されるかファイルが変更されていない限り再検査されません。

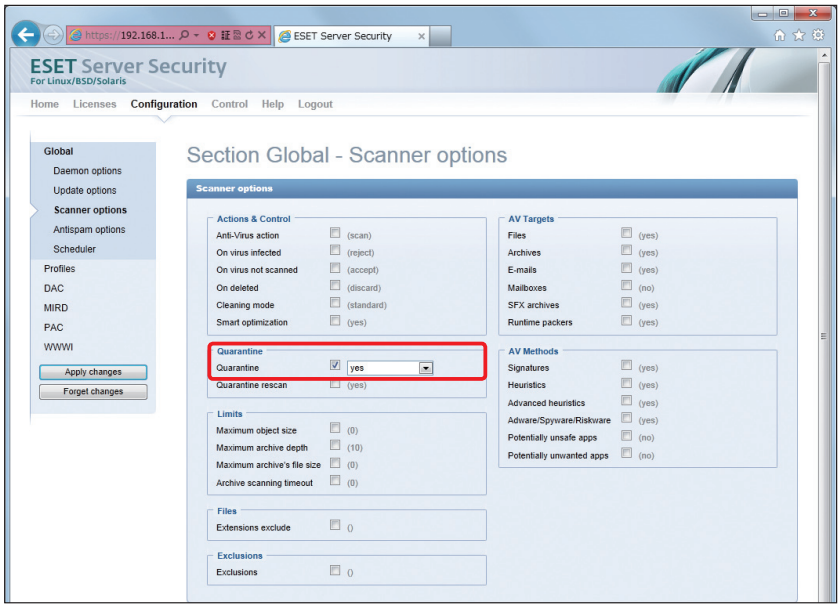


項目	既定値	概要
Cleaning mode	Standard	駆除モードの設定
Smart optimization	yes	Smart optimizationの設定

Cleaning modeの設定	スキャン時の動作
none	ウイルス感染したファイルを削除しない
standard	ウイルス感染したファイルのみを削除する
strict/rigorous/delete	ウイルス感染したファイル、アーカイブファイルを削除する

Scanner options - Quarantine

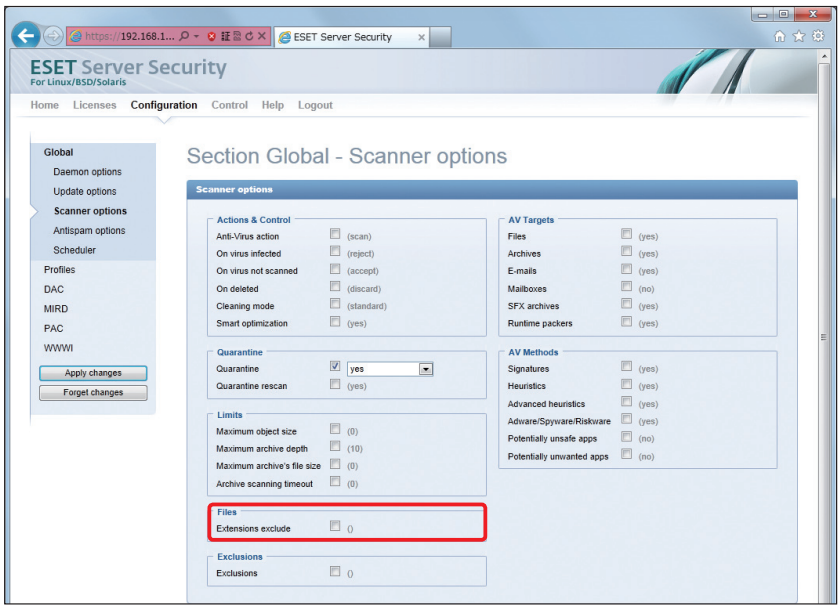
このセクションでは、隔離に関しての設定を行います。



項目	既定値	概要
Quarantine	no	ウイルスとして検知したファイルを隔離する/しないの設定

Scanner options - Files

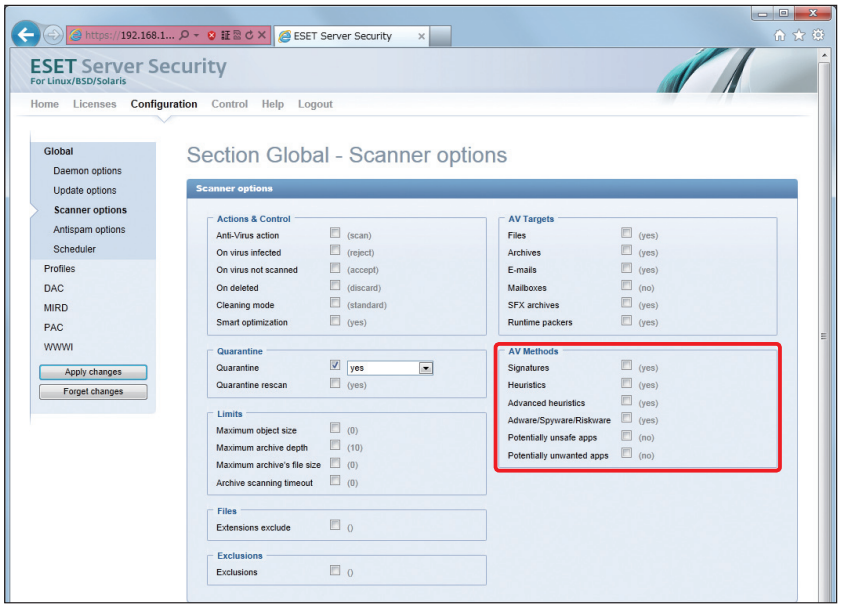
このセクションでは、検査を除外したいファイルの拡張子を登録できます。複数の拡張子の登録を行う場合は、「:（コロン）」で区切って入力します。



項目	既定値	概要
Extensions exclude	–	検査を除外したいファイルの拡張子の設定

Scanner options - AV Methods

このセクションでは、検査方法の設定を行います。既定値では、ウイルス定義データベースを利用したウイルスシグネチャの検査とヒューリスティックによる検査、アドバンスドヒューリスティックによる検査、Adware/Spyware/Riskwareの検査が設定されています。



項目	既定値	概要
Signatures	yes	ウイルスシグネチャ検査を実行する/しないの設定
Heuristics	yes	ヒューリスティック検査を実行する/しないの設定
Advanced heuristics	yes	アドバンスドヒューリスティック検査を実行する/しないの設定
Adware/Spyware/Riskware	yes	Adware/Spyware/Riskwareの検査の有効/無効の設定
Potentially unsafe apps	no	安全でない可能性があるアプリケーションの検出の有効/無効の設定
Potentially unwanted apps	no	望ましくない可能性があるアプリケーションの検出の有効/無効の設定

3.5 オンデマンドスキャン

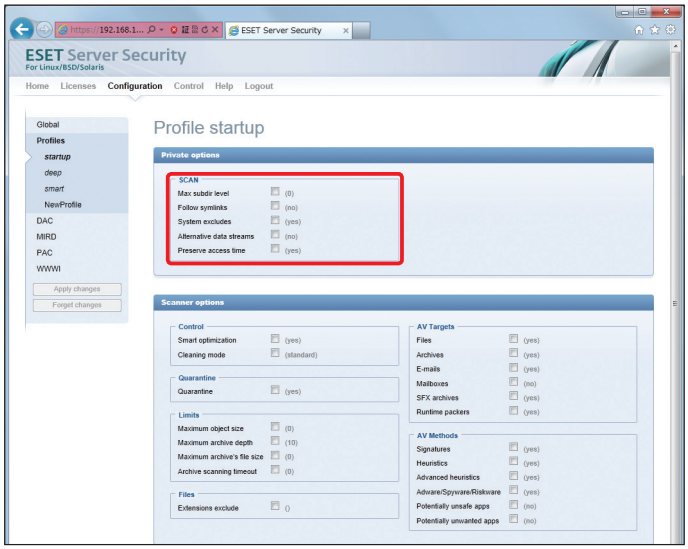
ESET File Security for Linuxは、指定したディレクトリの検査を行えるオンデマンドスキャンを搭載しています。ここでは、オンデマンドスキャンの設定と実行方法を説明します。

3.5.1 プロファイルの設定

ESET File Security for Linuxには、あらかじめ、[startup]、[deep]、[smart]の三種類のプロファイルが用意されています。オンデマンドスキャンではプロファイルの設定値に基づいて検査を行います。各プロファイルの設定は[Configuration]→[Profiles]→設定変更したいプロファイルをクリックして設定を行います。

Private options - SCAN

このセクションでは、検査の対象となるサブディレクトリの階層、シンボリックリンク先の検査、システムコントロールディレクトリ、代替データストリーム、検査時にファイルのアクセス時間を更新するかどうかを設定します。



プロファイル[startup]

項目	既定値	概要
Max subdir level	0	サブディレクトリの最大階層の設定([0]は制限なし)
Follow symlinks	no	シンボリックリンク先を検査する/しないの設定
System excludes	yes	システムコントロールディレクトリを検査する/しないの設定
Alternative data streams	no	代替データストリーム(ADS)を検査する/しないの設定
Preserve access time	yes	検査したファイルの最終アクセス時間を保持する/しないの設定 ※[yes]を選択するとスキャン時に最終アクセス時間が変更されません

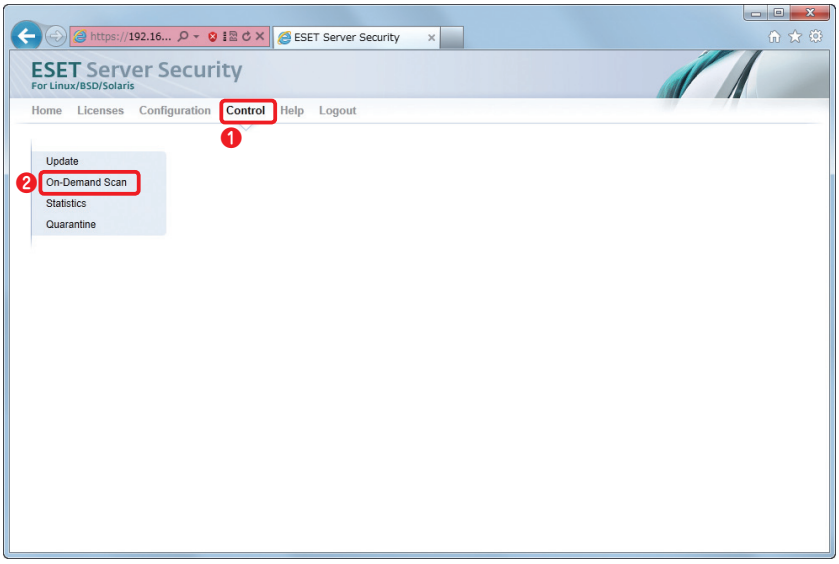
Scanner options

このセクションの設定内容は「3.4.1 ウイルス対策の基本設定」のScanner options、またはESET File Security for Linux設定リファレンスをご参照ください。

3.5.2 オンデマンドスキャンの実行

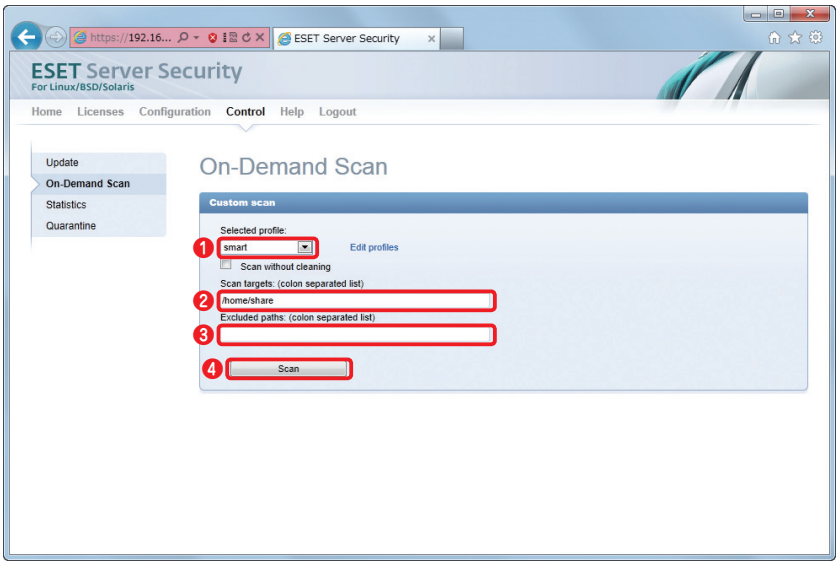
Webインターフェースを使ったオンデマンドスキャンの実行方法を説明します。

1



Webブラウザーを開き、Webインターフェースのページを開きます。
❶ [Control] をクリックし、
❷ [On-Demand Scan] をクリックしクします。

2



❶スキャンに利用するプロファイルを選択し、❷検査を行うディレクトリをフルパスで入力します。複数のディレクトリの検査を行うときは、「:(コロン)」で区切って、ディレクトリ名を入力します。
❸検査を除外したいファイルがあればフルパスで入力します。複数のファイルを除外したい場合は、「:(コロン)」で区切ってファイル名を入力します。❹ [Scan] ボタンをクリックします。

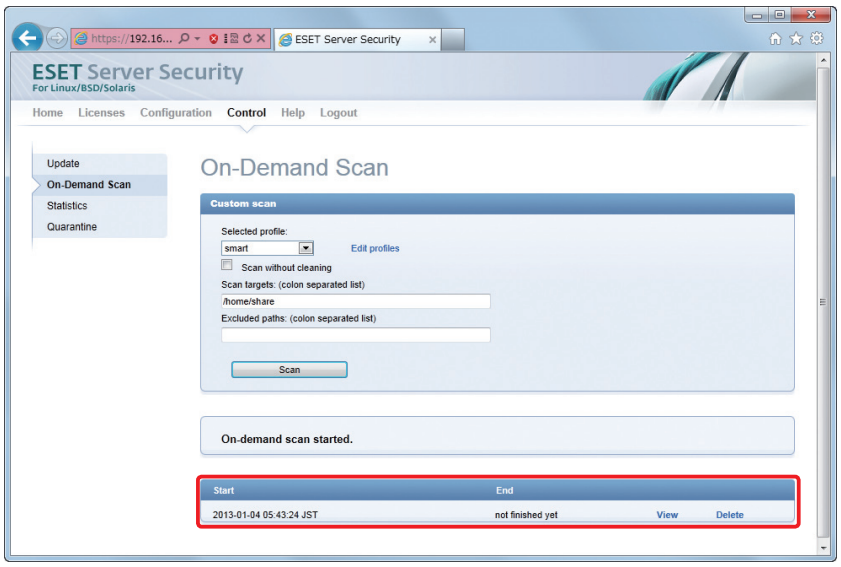
入力例

「deep」プロファイルを利用し、「/usr/local」以下のファイルを除外したすべてのファイルに対してオンデマンドスキャンを実行したい場合、❶で「deep」を選択し、❷に「/」、❸に「/usr/local/*」と入力します。

››› POINT

ここでは検査範囲はディレクトリ、除外したい場合はファイル名をフルパスで入力します。したがって「/usr/local」以下のすべてのファイルを除外したい場合は、「/usr/local/*」と入力してください。

3



指定したディレクトリのウイルス検査が実行されます。[View] をクリックすると、検査中の状況を確認できます。

3.6 オンアクセススキャン（リアルタイムスキャン）

オンアクセススキャン（リアルタイムスキャン）とは、ファイルをコンピューター上で開いたり、新規作成または実行したりするときに、悪意のあるコードがないかを検査してウイルスを検出する機能です。ESET File Security for Linuxのオンアクセススキャン（リアルタイムスキャン）はESET社が開発したオンアクセススキャン用ライブラリ（libesets_pac.so）をLinuxの環境変数である「LD_PRELOAD」※1に指定することで実現しています。そのため、ESET File Security for Linuxは「LD_PRELOAD」が有効な標準Cライブラリ（LIBC）を呼び出すように実装されたアプリケーションに対してオンアクセススキャン（リアルタイムスキャン）を行うことが可能です。ここでは、この機能を有効にする手順を説明します。

※1 LD_PRELOADの詳細はld.soのマニュアル（man ld.so）をご参照ください。

CAUTION

Dazuko（DAC）を利用したオンアクセススキャン（リアルタイムスキャン）は、弊社ではサポート対象外です。

3.6.1 オンアクセススキャンの設定

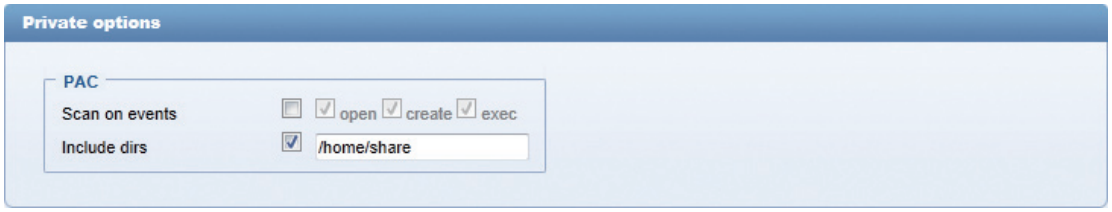
オンアクセススキャン（リアルタイムスキャン）の設定は、Webインターフェースを開き、［Configuration］→［PAC］をクリックして設定を行います。ここでは、オンアクセススキャン（リアルタイムスキャン）固有の設定項目について説明します。ここに説明のない設定項目については「3.4.1 ウイルス対策の基本」またはESET File Security for Linux設定リファレンスをご参照ください。

CAUTION

オンアクセススキャン（リアルタイムスキャン）では仕様上、アーカイブファイル（zip形式、tar形式、電子メール形式など）は検査しません。そのため［Scanner options – AV Targets］で［Archives］、［E-mails］、［Mailboxes］の項目を［yes］に変更しても検査しません。

Private options – PAC

このセクションでは、［Scan on events］で検査を行うイベントの設定を行い、［Include dirs］で検査を行うディレクトリを設定します。既定値では、ファイルのオープン、作成、実行のすべてイベントで検査を実施します。



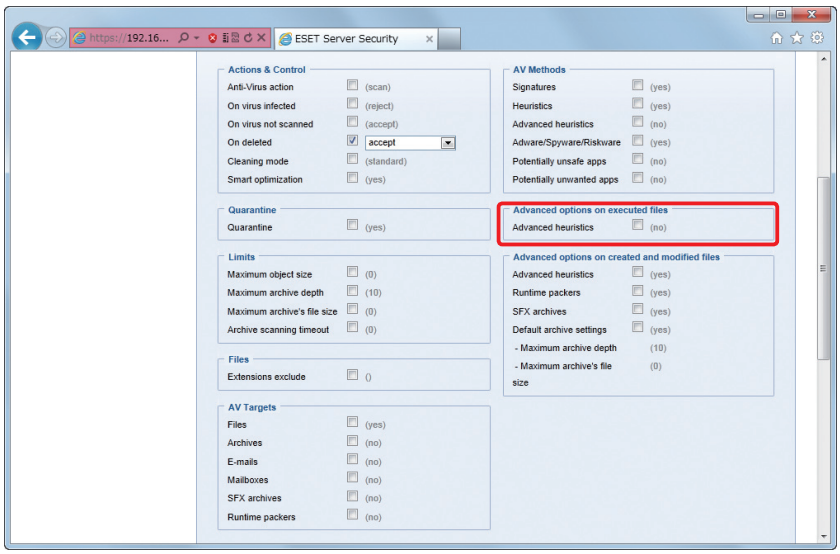
項目	既定値	概要
Scan on events	open,create,exec	検査を行うイベントの設定
Include dirs	–	ファイルを検査するディレクトリの設定

CAUTION

オンアクセススキャン（リアルタイムスキャン）を行うには、必ず［Include dirs］で検査を行うディレクトリの設定を行う必要があります。複数のディレクトリを設定する場合は「:（コロン）」で区切って、ディレクトリ名をフルパスで入力します。

Scanner options – Advanced options on executed files

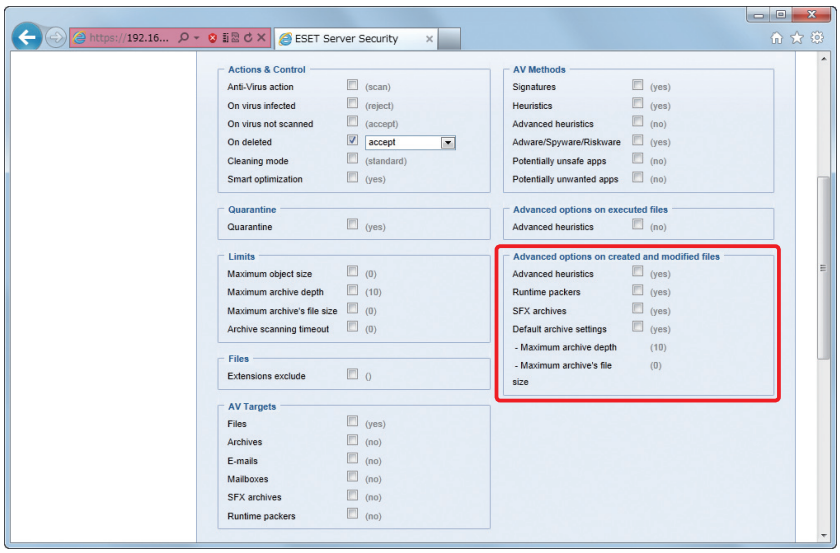
このセクションでは、ファイルを実行する時に、アドバンスドヒューリスティック検査を有効にするかどうかを設定します。既定値では、アドバンスドヒューリスティック検査を利用しない設定になっています。



項目	既定値	概要
Advanced heuristics	no	ファイルの実行時にアドバンスドヒューリスティック検査を実行する/しないの設定

Scanner options – Advanced options on created and modified files

このセクションでは、新規作成または変更されたファイルに適用する追加の検査パラメーターを設定します。



項目	既定値	概要
Advanced heuristics	yes	ファイルを新規作成または変更した時にアドバンスドヒューリスティック検査を実行する/しないの設定
Runtime packers	yes	圧縮された実行形式のファイルの検査をする/しないの設定
SFX archives	yes	自己解凍アーカイブの検査をする/しないの設定
Default archive settings	yes	アーカイブ検査に既定の設定を使用するかどうかの設定
- Maximum archive depth	10	アーカイブファイルの検査を行う場合の最大階層の設定
- Maximum archive's file size	0	アーカイブ内の最大ファイルサイズ(0は無制限)

3.6.2　オンアクセススキャン用ライブラリの指定

3.6.1の検査設定が完了後に、オンアクセススキャン（リアルタイムスキャン）を有効にしたいアプリケーションに対してオンアクセススキャン用ライブラリが事前にロードされるように「LD_PRELOAD」に指定する方法を説明します。

オンアクセススキャン（リアルタイムスキャン）を有効にしたいアプリケーションの起動スクリプトを以下のように編集します。
ここでは、起動スクリプト内でアプリケーションを起動させるためのコマンド名をCOMMAND、起動オプションをCOMMAND-ARGUMENTSとします。

32bit版の場合の例

```
LD_PRELOAD = /opt/eset/esets/lib/libesets_pac.so COMMAND COMMAND-ARGUMENTS
```

64bit版の場合の例

```
LD_PRELOAD = /opt/eset/esets/lib64/libesets_pac.so COMMAND COMMAND-ARGUMENTS
```

設定例

CentOS5.3 64bit版でSambaに対してオンアクセススキャン用ライブラリをロードする設定例

（編集前）

```
daemon smbd &SMBDOPTIONS
```

（編集後）

```
LD_PRELOAD = /opt/eset/esets/lib64/libesets_pac.so daemon smbd &SMBDOPTIONS
```

3.6.3　Sambaに対するオンアクセススキャンの設定

Sambaに対するオンアクセススキャン（リアルタイムスキャン）の設定は、Sambaの起動スクリプト（/etc/init.d/smb）に修正を加えます。ここでは、例としてCentOS/Red Hat Enterprise LinuxおよびSUSE Linux Enterpriseの64bit版の場合を説明します。

CentOS/Red Hat Enterprise Linux5.3での修正例

Sambaの起動スクリプト（/etc/init.d/smb）を以下のように修正します。

```
start() {
        KIND="SMB"
        echo -n $"Starting $KIND services: "
        LD_PRELOAD=/opt/eset/esets/lib64/libesets_pac.so daemon smbd $SMBDOPTIONS
        RETVAL= $?
        echo
        [ $RETVAL -eq 0 ] && touch /var/lock/subsys/smb ¦¦ ¥
          RETVAL=1
        return $RETVAL
}
```

CentOS/Red Hat Enterprise Linux7.2 での修正例

Sambaの起動オプションを設定するファイル（/etc/sysconfig/samba）を以下のように修正します。

```
## Path:           Network/Samba
## Description:    Samba process options
## Type:           string
## Default:        ""
## ServiceRestart: samba
SAMBAOPTIONS=""
## Type:           string
## Default:        ""
## ServiceRestart: smb
LD_PRELOAD=/opt/eset/esets/lib64/libesets_pac.so
SMBDOPTIONS=""

## Type:           string
## Default:        ""
## ServiceRestart: nmb
NMBDOPTIONS=""
## Type:           string
## Default:        ""
## ServiceRestart: winbind
WINBINDOPTIONS=""
```

SUSE Linux Enterprise10 sp3での修正例

Sambaの起動スクリプト（/etc/init.d/smb）を以下のように修正します。

```
        start)
                echo -n "Starting Samba SMB daemon "
                if [ ! -f ${SMB_CONF} ]; then
                        echo -n >&2 "Samba configuration file, ${SMB_CONF} does not exist. "
                        rc_status -s
                        exit 6
                fi
                checkproc -p ${PID_FILE} ${SMBD_BIN}
                case $? in
                        0) echo -n "- Warning: daemon already running. " ;;
                        1) echo -n "- Warning: ${PID_FILE} exists. " ;;
                esac
                test -d " ${PID_FILE% /smbd.pid}" ¦¦ ¥
                        mkdir -m 0755 -p " ${PID_FILE% /smbd.pid}"
                test -f /etc/sysconfig/language && ¥
                        . /etc/sysconfig/language
                " ${SMB_APPARMOR_UPDATE}"
                export LC_ALL=" $RC_LC_ALL"
                export LC_CTYPE=" $RC_LC_CTYPE"
                export LANG=" $RC_LANG"
                LD_PRELOAD=/opt/eset/esets/lib64/libesets_pac.so startproc -p ${PID_FILE} -W
${PID_FILE} ${SMBD_BIN} -D -s ${SMB_CONF}
                rc_status -v
                unset LC_ALL LC_CTYPE LANG
                ;;
```

3.6.4 Apacheに対するオンアクセススキャンの設定

Apacheに対するオンアクセススキャン（リアルタイムスキャン）の設定は、Apacheの起動スクリプトに修正を加えます。ここでは、例としてCentOS/Red Hat Enterprise LinuxおよびSUSE Linux Enterpriseの64bit版の場合を説明します。

CentOS/Red Hat Enterprise Linux5.3での修正例

Apacheの起動スクリプト（/etc/init.d/httpd）を以下のように修正します。

```
start() {
        echo -n $"Starting $prog: "
        LD_PRELOAD=/opt/eset/esets/lib64/libesets_pac.so LANG= $HTTPD_LANG daemon
--pidfile= ${pidfile} $httpd $OPTIONS
        RETVAL= $?
        echo
        [ $RETVAL = 0 ] && touch ${lockfile}
        return $RETVAL
}
```

CentOS/Red Hat Enterprise Linux7.2での修正例

Apacheの起動オプションを設定するファイル（/etc/sysconfig/httpd）を以下のように修正します。

```
#
# This file can be used to set additional environment variables for
# the httpd process, or pass additional options to the httpd
# executable.
#
# Note: With previous versions of httpd, the MPM could be changed by
# editing an "HTTPD" variable here.  With the current version, that
# variable is now ignored.  The MPM is a loadable module, and the
# choice of MPM can be changed by editing the configuration file
# /etc/httpd/conf.modules.d/00-mpm.conf.
#

#
# To pass additional options (for instance, -D definitions) to the
# httpd binary at startup, set OPTIONS here.
#
#OPTIONS=

#
# This setting ensures the httpd process is started in the "C" locale
# by default.  (Some modules will not behave correctly if
# case-sensitive string comparisons are performed in a different
# locale.)
#
LANG=C
LD_PRELOAD=/opt/eset/esets/lib64/libesets_pac.so
```

SUSE Linux Enterprise10 sp3での修正例

Apacheの起動スクリプト（/etc/init.d/apache2）を以下のように修正します。

```
    start*)
        if [ -e $pidfile ]; then
                $0 status &>/dev/null
                ret= $?
                if [ $ret = 1 ]; then
                        echo "Warning: found stale pidfile (unclean shutdown?)"
                elif [ $ret = 0 ]; then
                        echo "Apache is already running ($pidfile)"
                        rc_failed $ret
                        rc_status -v1
                        rc_exit
                fi
        fi

        echo -n "Starting httpd2 (${APACHE_MPM:- ${apache_bin#*-})"
        cmdline= $(echo $apache_bin -f $httpd_conf $server_flags " $@")
        if eval $cmdline -t > $logdir/rc $pname.out 2>&1 ; then
                export -n ${!APACHE_*}
                LD_PRELOAD=/opt/eset/esets/lib64/libesets_pac.so eval startproc -f -t ${APACHE_
START_TIMEOUT:-2} $cmdline
                ret= $?

                if test -t 1 && stty -a 2>/dev/null ¦ grep -q -- -echo ¥ ; then
                        # this means that apache was still waiting for a passphrase to be entered
                        stty echo 2>/dev/null
                        echo;echo
                        echo >&2 An SSL passphrase has not been entered within ${APACHE_START_
```

3.6.5　ユーザーのコマンド操作に対するオンアクセススキャンの設定

ESET File Security for Linuxは、各ユーザーの環境変数「LD_PRELOAD」にオンアクセススキャン用ライブラリ（libesets_pac.so）を指定することで、ユーザーのコマンド操作に対してオンアクセススキャン（リアルタイムスキャン）を実施することができます。ここでは、例として64bit版の場合を説明します。

一時的にオンアクセススキャンを有効にする場合

一時的にコマンド操作に対してオンアクセススキャン（リアルタイムスキャン）を有効にする場合は、以下のコマンドを入力します。なお、この操作は、ログアウトするとリセットされ、無効の状態に戻ります。

rootユーザーの場合の例

```
# LD_PRELOAD=/opt/eset/esets/lib64/libesets_pac.so
# export LD_PRELOAD
```

自動的にオンアクセススキャンを有効にする場合

自動的にオンアクセススキャン（リアルタイムスキャン）を有効にする場合、各ユーザーの「.bash_profile」ファイルに以下の2行を追記します。たとえば、rootユーザーの場合は、「/root/.bash_profile」ファイルに以下の2行を追記します。なお「.bash_profile」ファイルが存在しない場合は、以下の2行が書かれた「.bash_profile」ファイルを作成してください。

```
LD_PRELOAD=/opt/eset/esets/lib64/libesets_pac.so
export LD_PRELOAD
```

3.6.6　システム全体へのオンアクセススキャンの設定

ESET File Security for Linuxは、/etc/ld.so.preloadにオンアクセススキャン用ライブラリ（libesets_pac.so）を指定することで、システム全体の標準Cライブラリ（LIBC）を呼び出すように実装されたアプリケーションに対してオンアクセススキャン（リアルタイムスキャン）を有効にすることができます。ここでは、例として64bit版の場合を説明します。

CAUTION

/etc/ld.so.preloadに指定し、システム全体へのオンアクセススキャンを有効にした場合は、本来ウイルス検査を行う必要のないファイルアクセスを検査するためシステム全体の負荷があがります。サーバーのパフォーマンス低下の原因にもなりますので、ファイルアクセスの多いサーバーなどで設定を有効にする場合は十分にご注意ください。「3.6.1　オンアクセススキャンの設定」の「Include dirs」の設定でウイルス検査の必要なファイルがあるディレクトリだけを指定するなどの対策をしてください。

システム全体にオンアクセススキャンを有効にする場合

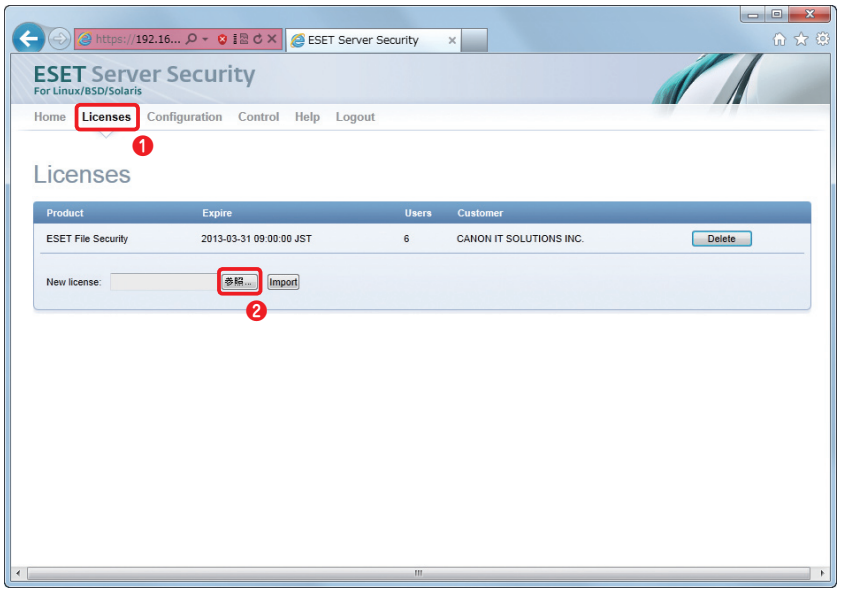
システム全体にオンアクセススキャンを有効にしたい場合は、「/etc/ld.so.preload」ファイルを作成し以下の1行を記入します。

```
/opt/eset/esets/lib64/libesets_pac.so
```

3.7 ライセンス管理

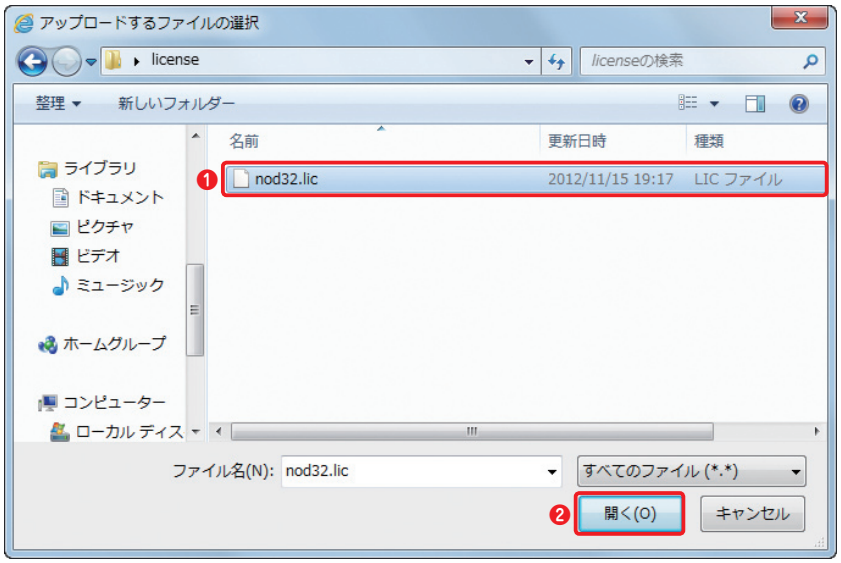
ライセンスの更新を行った場合は、ライセンスキーファイルの入れ替えが必要になります。ここでは、Webインターフェースを利用したライセンスキーファイルの入れ替え方法を説明します。

1



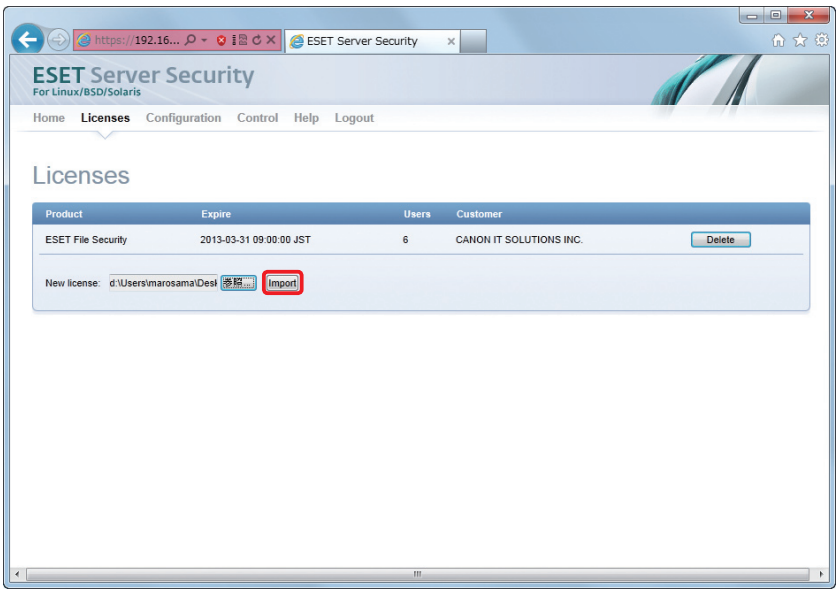
Webブラウザーを開き、Webインターフェースのページを開きます。❶[Licenses]をクリックし、❷[参照]をクリックします。

2



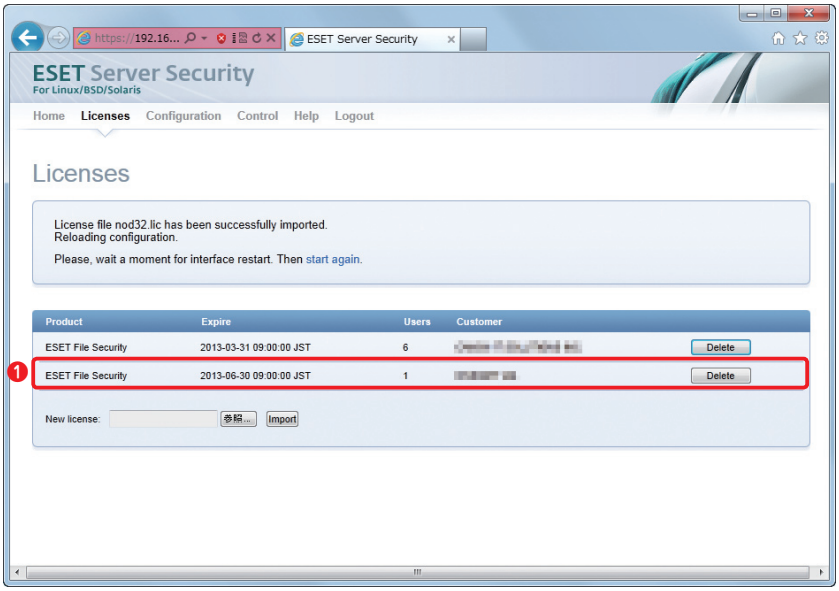
「アップロードするファイルの選択」ダイアログが開きます。❶インポートするライセンスキーファイルを選択し、❷[開く]ボタンをクリックします。

3



[Import] ボタンをクリックします。

4



❶選択したライセンスキーファイルが登録されます。

▸▸▸ POINT

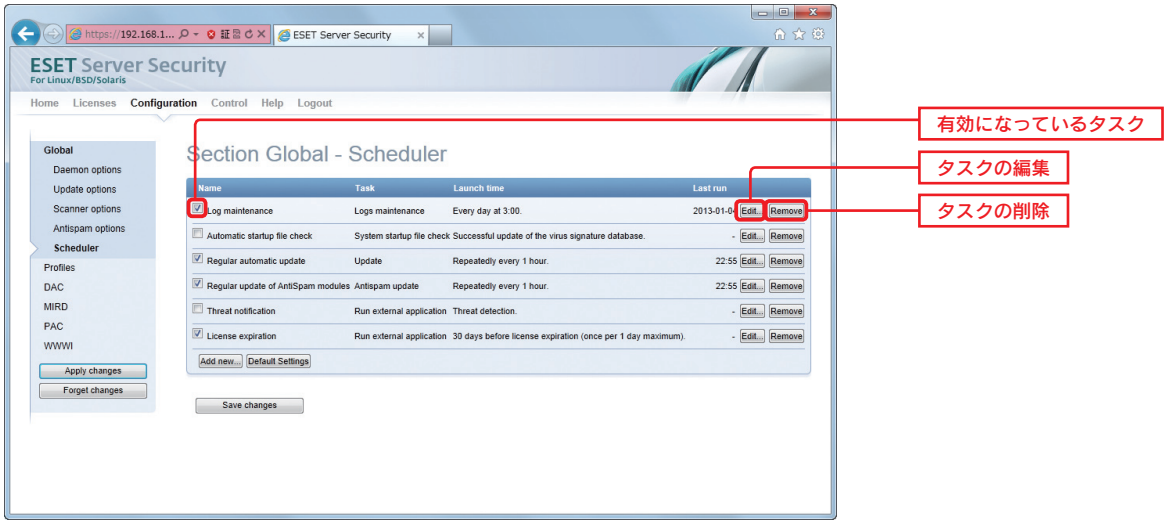
「Delete」ボタンをクリックすると、登録済みのライセンスキーファイルを削除できます。

3.8 スケジューラの設定

スケジューラを利用すると、設定した日時に特定のタスクを実行できます。ESET File Security for Linuxでは、ウイルス定義データベースの自動アップデートなどがあらかじめスケジュールされていますが、必要に応じて、新たなスケジュールを追加できます。

3.8.1 事前登録されているスケジュール

スケジューラは、Webインターフェースを開き、[Configuration] → [Global] → [Scheduler] をクリックすることで表示できます。既定値では、6個のスケジュールが登録されています。また、有効に設定されている項目には、チェックが付けられています。登録済みのタスクの編集を行うには、[Edit] ボタンをクリックします。[Remove] ボタンをクリックすると、そのタスクを削除できます。

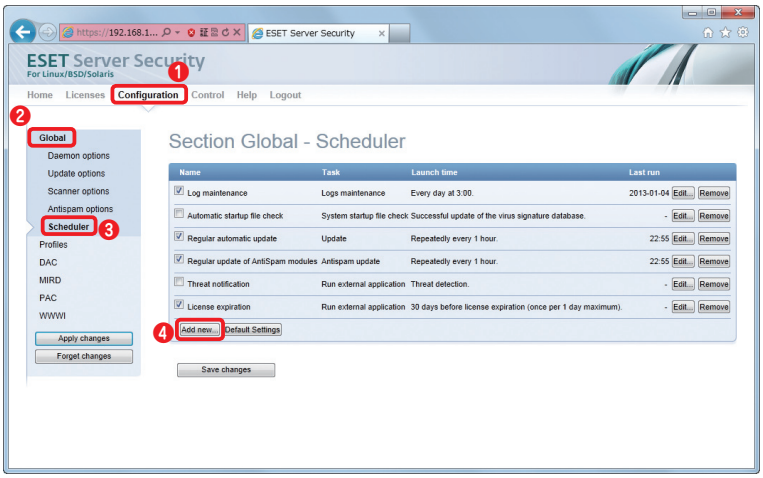


タスクの名称	既定の実行タイミング	タスクの内容
Log maintenance	毎日午前3:00に実行	ログのメンテナンス。この項目は既定値で有効に設定されています
Automatic startup file check	ウイルス定義データベースのアップデートが成功した場合	システムの自動スタートアップファイルの検査。この項目は既定値で無効に設定されています
Regular automatic update	1時間毎	ウイルス定義データベースの自動アップデート。この項目は既定値で有効に設定されています
Regular update of AntiSpam modules	1時間毎	アンチスパムモジュールのアップデート。この項目は既定値で有効に設定されています ※ESET File Security for Linuxでは使用しません。
Threat notification	ウイルスを検出した場合	オンアクセススキャン(リアルタイムスキャン)でのウイルス検出の報告。この項目は既定値で無効に設定されています
License expiration	ライセンスの有効期限が30日未満になった場合	ライセンスの有効期限の警告。この項目は既定値で有効に設定されています

3.8.2 スケジュールの新規登録

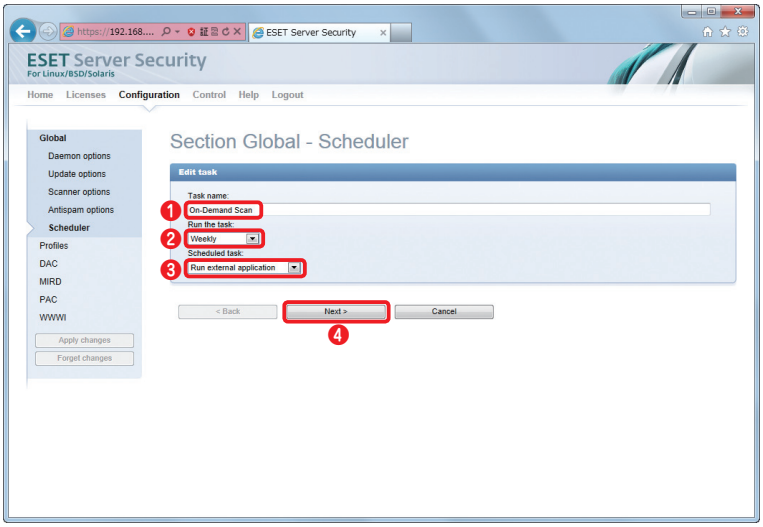
スケジューラで新規タスクを登録するときは、[Add new] ボタンをクリックします。ここでは、指定したディレクトリに対して定期的にオンデマンドスキャンを実施するタスクの作成手順を例に、新規タスクの作成手順を説明します。

1



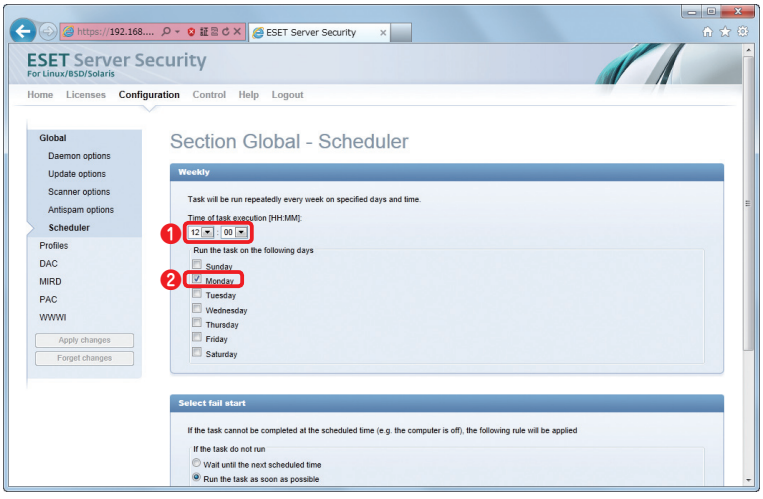
Webブラウザーを開き、Webインターフェースのページを開きます。
❶ [Configuration] をクリックし、
❷ [Global] をクリックします。
❸ [Scheduler] をクリックし、❹ [Add new] ボタンをクリックします。

2



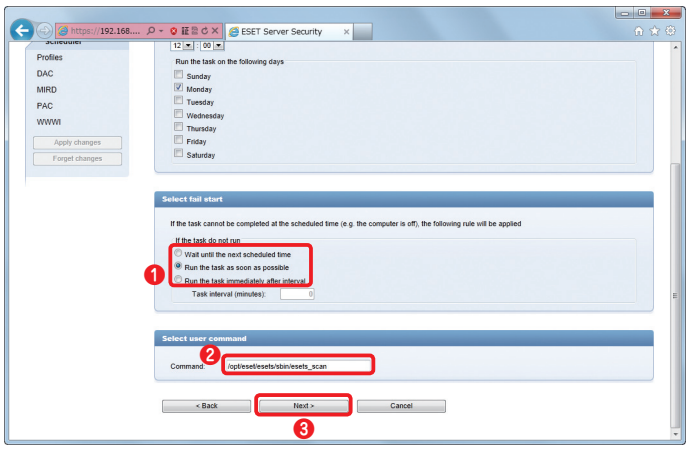
❶ [Task name] にタスク名（ここでは、[On-Demand Scan]）を入力し、❷ [Run the task] のドロップダウンリストで実行間隔（ここでは、[Weekly]）を設定します。❸ [task] のドロップダウンリストで実行するタスク（ここでは、[Run external application]）を選択します。❹ [Next>] ボタンをクリックします。

3



❶タスクを実行する時間をドロップダウンリスト（ここでは、[12:00]）を設定し、❷タスクを実行する曜日（ここでは、[Monday]）にチェックを入れます。

4



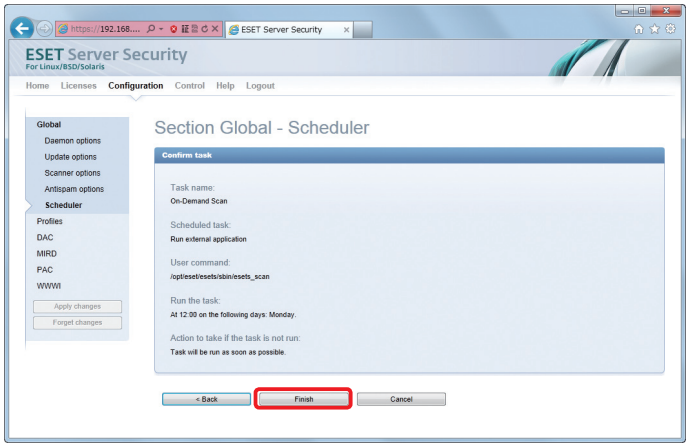
❶タスクが実行されなかったときのアクションにチェックを入れます。❷[Command:]に「3.14.1 オンデマンドスキャン」を参照して実行させたいコマンドを入力します。(例:「smart」プロファイルで「/home/share」ディレクトリを検査してログを出力する場合、/opt/eset/esets/sbin/esets_scan --profile=scan_smart --log-file=/var/log/esetscan.log /home/share)

❸[Next>]ボタンをクリックします。

POINT

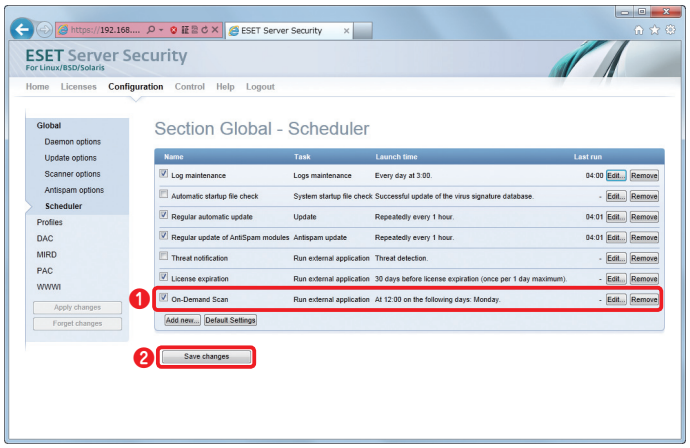
スケジューラでオンデマンドスキャンを実行した結果を残したい場合は、オプションでログを出力するように設定してください。

5



設定内容の確認を行います。設定に誤りがある場合は[<Back]ボタンをクリックして再設定を行ってください。問題がなければ[Finish]ボタンをクリックします。

6



❶スケジュールタスクの一覧に、新たなタスクが追加されます。❷[Save changes]ボタンをクリックします。

POINT

新規タスクを作成した場合は、必ず、[Save changes]ボタンをクリックして設定の保存を行ってください。この操作を行わないと、作成した新規タスクは保存されません。

設定を反映させるために、メニューオプションの[Apply changes]ボタンをクリックします。問題がなければメインウィンドウに表示される[Yes]ボタンをクリックします。(参考情報「3.1.2 Webインターフェースでの設定の反映」)

CAUTION

[Scheduled task]内の[On-demand computer scan]を選択した場合、検査結果のログはESET Remote Administratorに送信され、ESET Remote Administrator以外ではログの確認ができません。

3.9 ミラーサーバー機能

ミラーサーバー機能とはローカル環境にウイルス定義データベースのアップデートサーバーを作成する機能です。この機能を利用すると、クライアントコンピューターは、インターネット上にあるESETのサーバーからウイルス定義データベースをダウンロードせずに、ローカルネットワーク上に作成したアップデートサーバーからダウンロードすることが可能です。ここでは、ミラーサーバー機能を利用する手順を説明します。

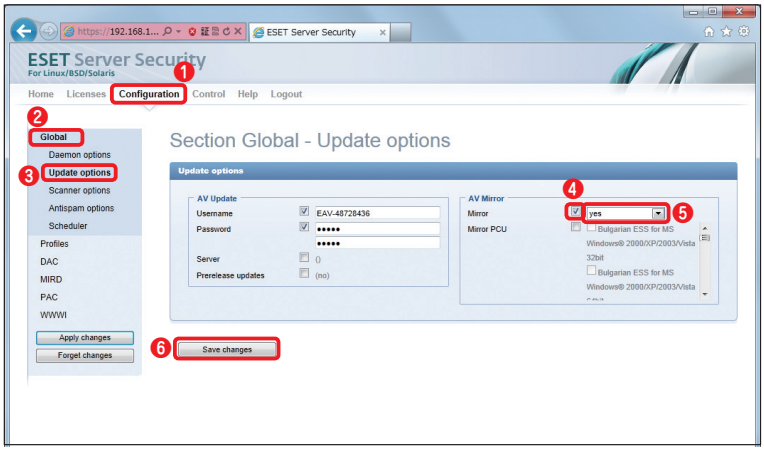
CAUTION

本機能は、サーバー専用ウイルス・スパイウェア対策ソフトESET File Security for Linux / Windows Serverではご利用いただけません。

3.9.1 ミラーサーバー機能の設定

ESET File Security for Linuxのミラーサーバー機能を設定する手順を説明します。

1



Webブラウザーを開き、Webインターフェースのページを開きます。

❶ [Configuration] をクリックし、

❷ [Global] をクリックします。

❸ [Update options] をクリックします。

❹「AV Mirror」セクションの [Mirror] にチェックを入れ、❺ドロップダウンリストから [yes] を選択します。❻ [Save changes] ボタンをクリックして設定を保存します。

設定を反映させるために、メニューオプションの [Apply changes] ボタンをクリックします。問題がなければメインウィンドウに表示される [Yes] ボタンをクリックします。(参考情報「3.1.2 Webインターフェースでの設定の反映」)

POINT

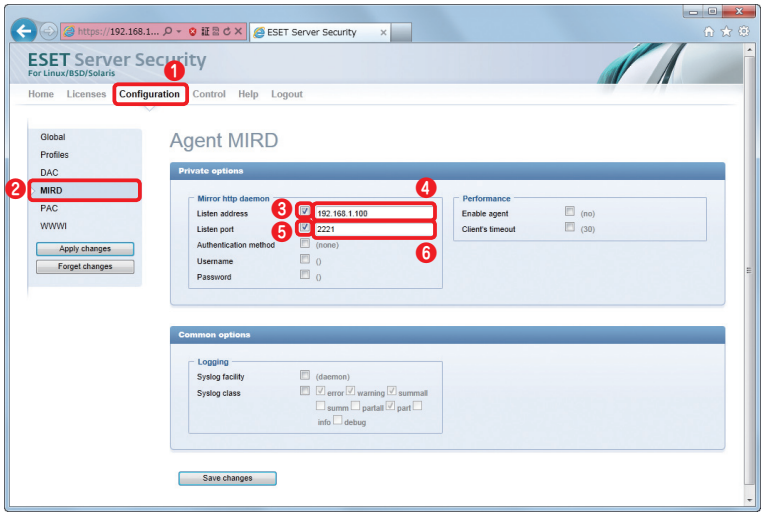
ミラーサーバー機能を有効にすると、以下のディレクトリが作成され、そのディレクトリにアップデート用ウイルス定義データベースが保存されます。

/var/opt/eset/esets/lib/mirror

3.9.2 内部HTTPサーバーの設定

ミラーサーバー機能を利用するためには、クライアントコンピューターへウイルス定義データベースを配布するためのHTTPサーバーが必要になります。ここでは、ESET File Security for Linuxの内部HTTPサーバーである「ESET Mirror http daemon」を設定する手順を説明します。

1



Webブラウザーを開き、Webインターフェースのページを開きます。

❶ [Configuration] をクリックし、

❷ [MIRD] をクリックします。「Mirror http daemon」セクションの❸ [Listen address] にチェックを入れ、❹IPアドレスまたはホスト名を入力します。

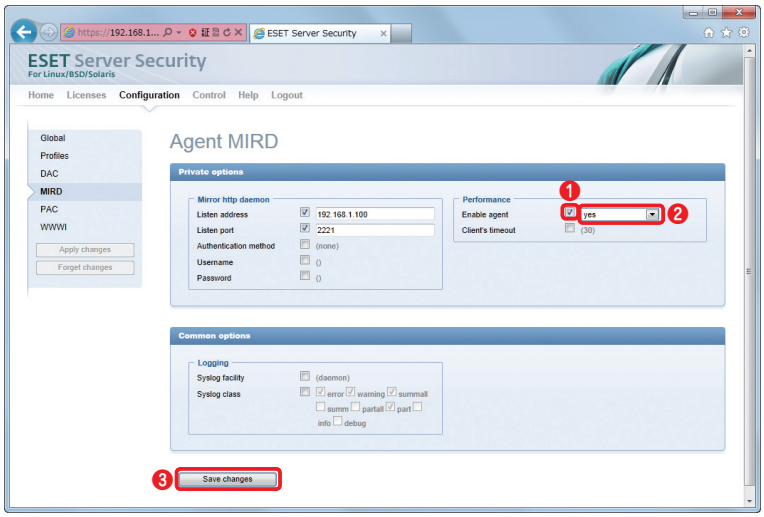
❺ [Listen port] にチェックを入れ、

❻ポート番号を入力します。

POINT

ウイルス定義データベースのアップデートにユーザー認証を設定したいときは、[Authentication method] にチェックを入れ、ドロップダウンリストから [basic] を選択します。[Username] にチェックを入れ、ユーザー名を入力し、[Password] にチェックを入れ、パスワードを入力します。

2



「Performance」セクションの❶ [Enable agent] にチェックを入れ、❷ドロップダウンリストから [yes] を選択します。

❸ [Save changes] ボタンをクリックして設定を保存します。

設定を反映させるために、メニューオプションの [Apply changes] ボタンをクリックします。問題がなければメインウィンドウに表示される [Yes] ボタンをクリックします。（参考情報「3.1.2 Webインターフェースでの設定の反映」）

POINT

ミラーサーバー機能を利用してウイルス定義データベースの配信を行うには、ミラーサーバー機能を有効にしたあとにウイルス定義データベースのアップデートを実施する必要があります。実行手順については「3.2.2 アップデートの手順」をご参照ください。

3.10 リモート管理

ESET File Security for Linuxは、ESET Remote Administratorを利用することでリモート管理を行えます。ここでは、リモート管理について説明します。

CAUTION

本機能は、サーバー専用ウイルス・スパイウェア対策ソフトESET File Security for Linux / Windows Serverではご利用いただけません。

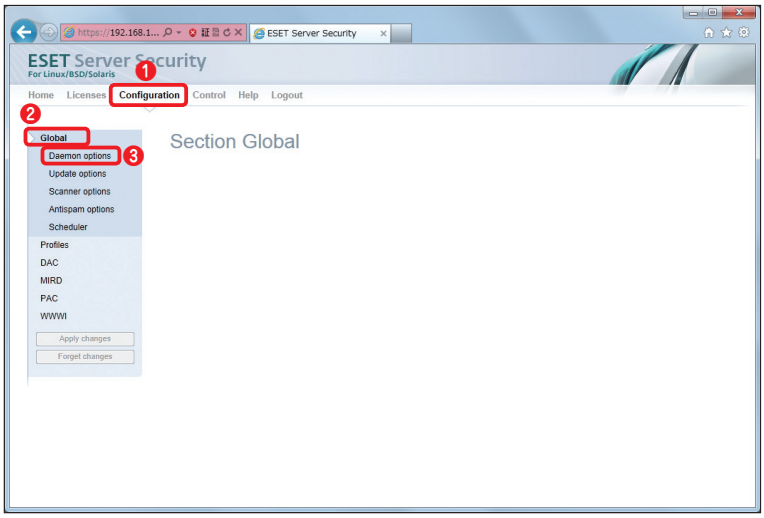
3.10.1 リモート管理の設定

ESET Remote Administrator V5でESET File Security for Linuxをリモート管理するための手順を説明します。

CAUTION

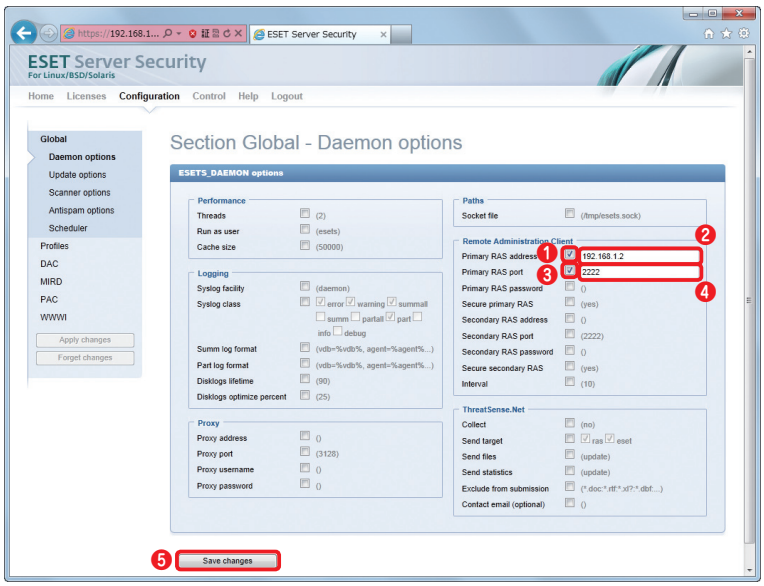
ESET Remote Administrator V6との通信を行うには、「ERAエージェント」のインストールが必要です。「ERAエージェント」のインストールについては『ESET Remote Administrator ユーザーズマニュアル』の「4.2.2 ERAエージェントの展開」を参照してください。
また、ESET Remote Administrator V6で管理できるESET File Security for LinuxはV4.5.3以降です。ERAエージェントをインストール後、手順2の❷のPrimary RAS addressの設定で、IPアドレスに「127.0.0.1」を入力し、❹のPrimary RAS portの設定でポート番号に「2225」を設定してください。

1



Webブラウザーを開き、Webインターフェースのページを開きます。
❶ [Configuration] をクリックし、
❷ [Global] をクリックします。
❸ [Daemon options] をクリックします。

2



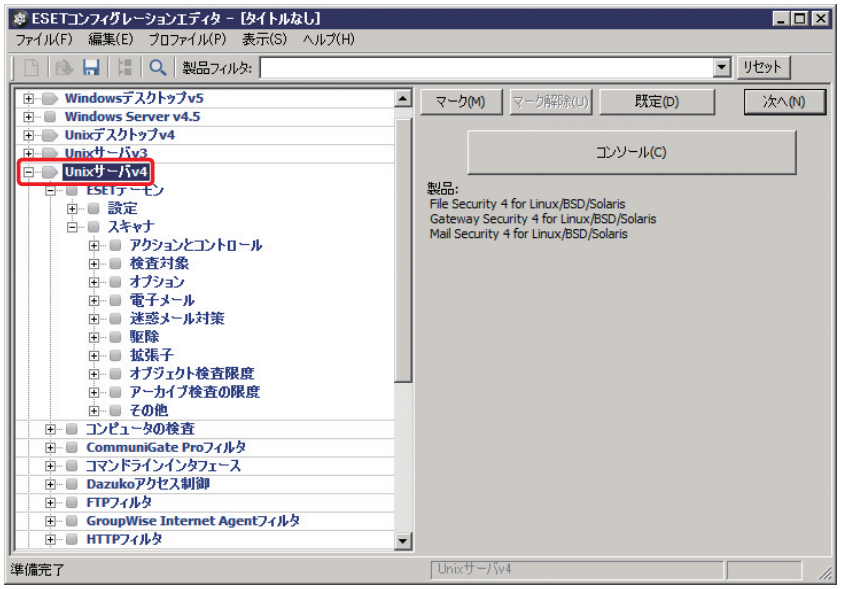
「Remote Administration Client」セクションの設定を行います。❶[Primary RAS address]にチェックを入れ、❷ESET Remote Administratorが動作している管理サーバーのIPアドレスまたはホスト名を入力します。❸[Primary RAS port]にチェックを入れ、❹管理サーバーのポート番号を入力します。❺[Save changes]ボタンをクリックします。

設定を反映させるために、メニューオプションの[Apply changes]ボタンをクリックします。問題がなければメインウィンドウに表示される[Yes]ボタンをクリックします。(参考情報「3.1.2 Webインターフェースでの設定の反映」)

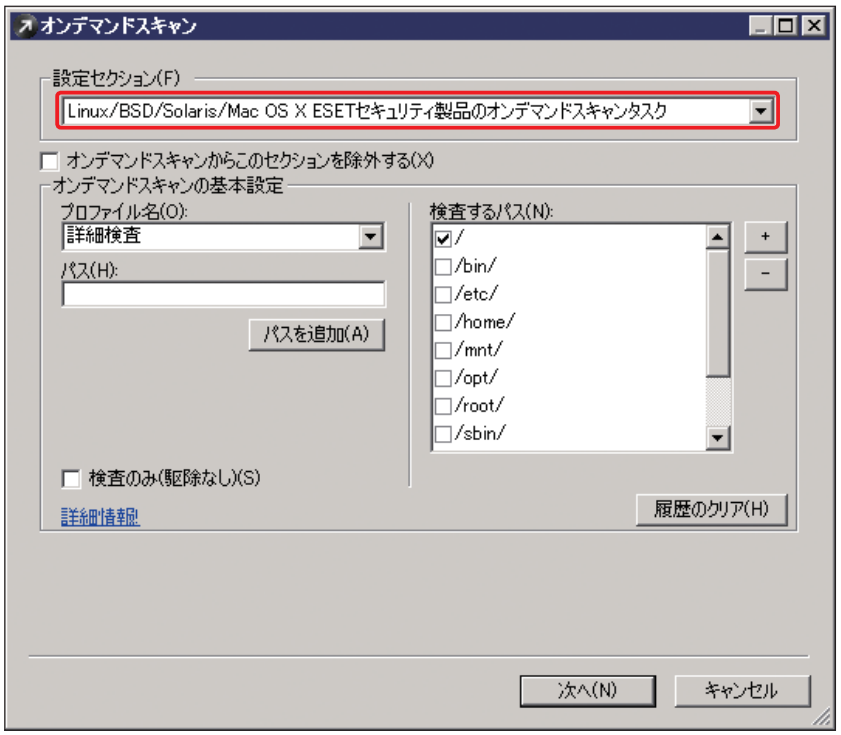
3.10.2 リモート管理について

リモート管理の設定を行うと、ESET File Security for LinuxをESET Remote Administratorでリモート管理を行えます。たとえば、ESET File Security for Linuxの設定をリモートで変更したり、オンデマンドスキャンやウイルス定義データベースのアップデートなどのタスクをリモート操作で実施できます。ESET Remote Administratorを利用したリモート管理の詳細については、ESET Remote Administrator ユーザーズマニュアルをご参照ください。なお、ESET Remote Administrator V5のリモート管理でESET File Security for Linuxの設定の変更を行うときは、ESET コンフィグレーションエディタで「Unixサーバv4」の項目を編集します。また、オンデマンドスキャンやウイルス定義データベースのアップデートなどのタスクの実施する場合は、「Linux/BSD/Solaris/Mac OS X ESETセキュリティ製品」のタスクを選択します。

設定を変更する場合に利用する項目



オンデマンドスキャンなどを行う場合に選択する項目



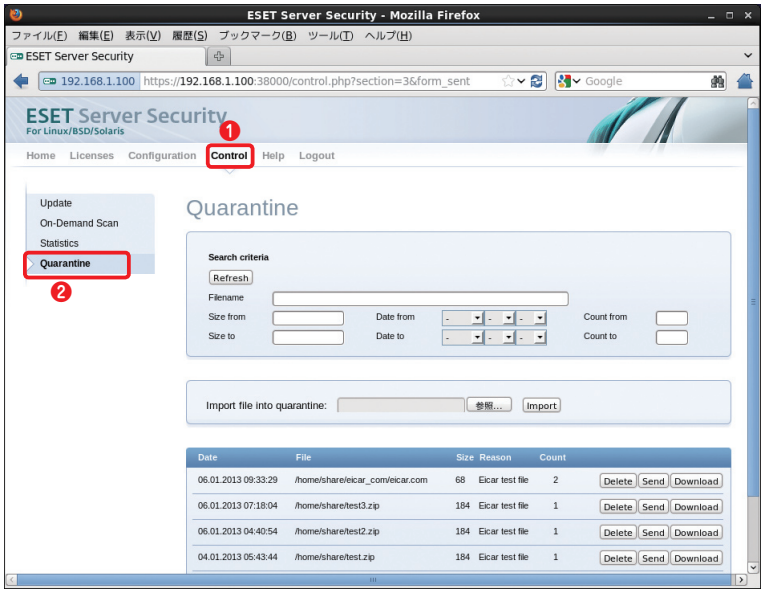
3.11 隔離

隔離の主な役割は、感染ファイルを安全に保存することです。ESET File Security for Linuxでは、「Quarantine（隔離）」を有効にし、「Cleaning mode」に「standard」「strict」「rigorous」「delete」のいずれかを設定すると、感染ファイルを自動的に隔離領域に保存します。ここでは、隔離について説明します。

3.11.1 隔離されたファイルの確認

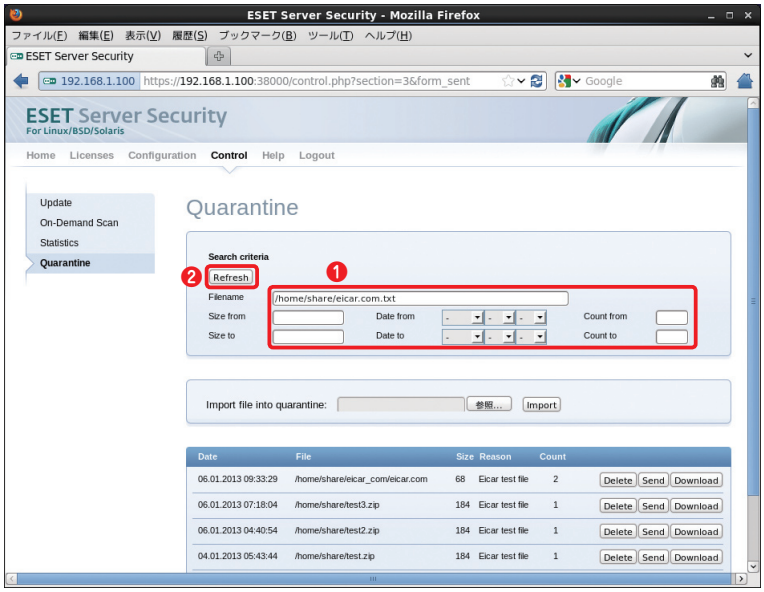
ここでは、隔離されたファイルの確認と検索方法を説明します。

1



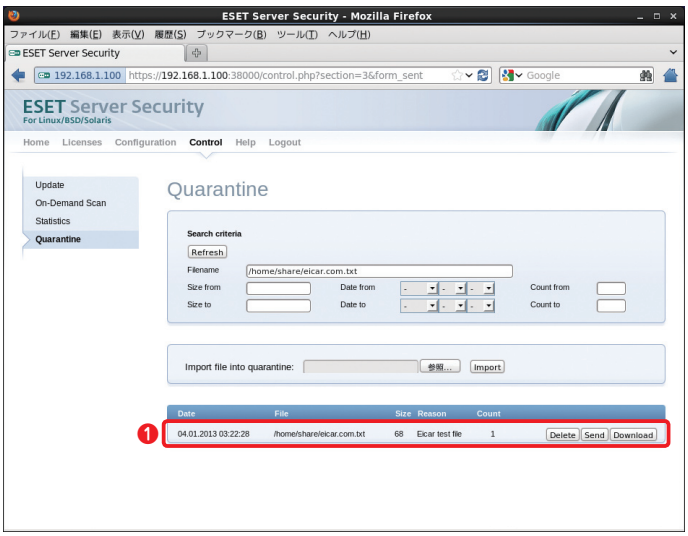
Webブラウザーを開き、Webインターフェースのページを開きます。❶[Control]をクリックし、❷[Quarantine]をクリックします。ここで、隔離されたファイルの一覧が、下の方に表示されます。

2



隔離されたファイルを検索する場合、❶ここに検索したいファイルの条件を入力して、❷[Refresh]ボタンをクリックします。

3



❶検索結果が表示されます。

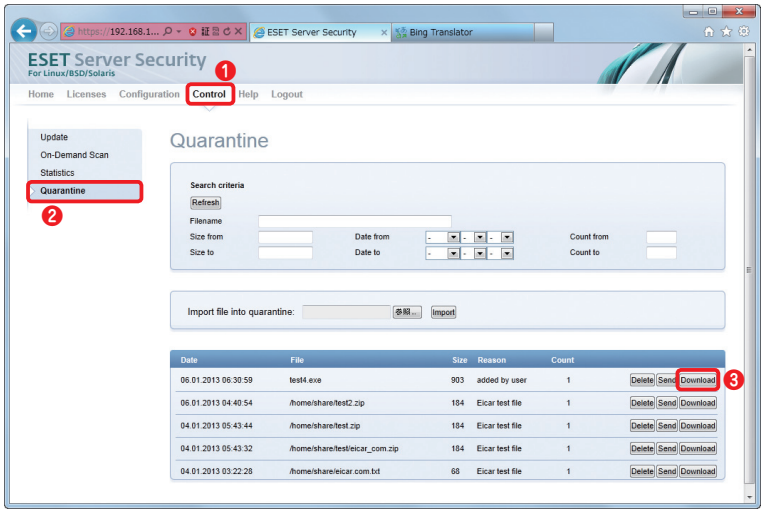
POINT

隔離されたファイルの検索はファイル名、サイズ、隔離された日付などで検索できます。ファイル名はフルパスで入力してください。

3.11.2 隔離されたファイルのダウンロード

隔離されたファイルをダウンロードしたいときは、以下の手順で作業します。

1

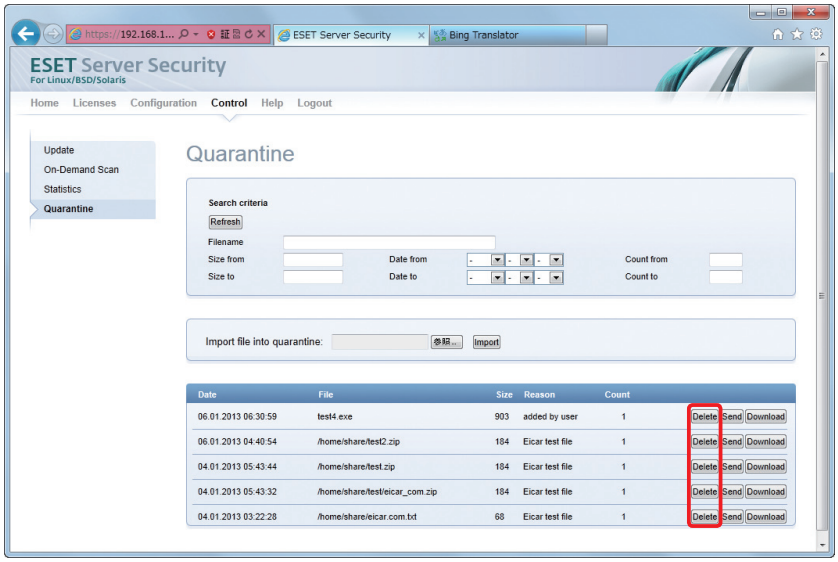


Webブラウザーを開き、Webインターフェースのページを開きます。
❶ [Control] をクリックし、
❷ [Quarantine] をクリックします。ダウンロードしたいファイルの
❸ [Download] ボタンをクリックし、ファイルを保存します。

コラム

隔離されたファイルの削除

隔離されたファイルを削除したいときは、削除したいファイルの[Delete]ボタンをクリックします。

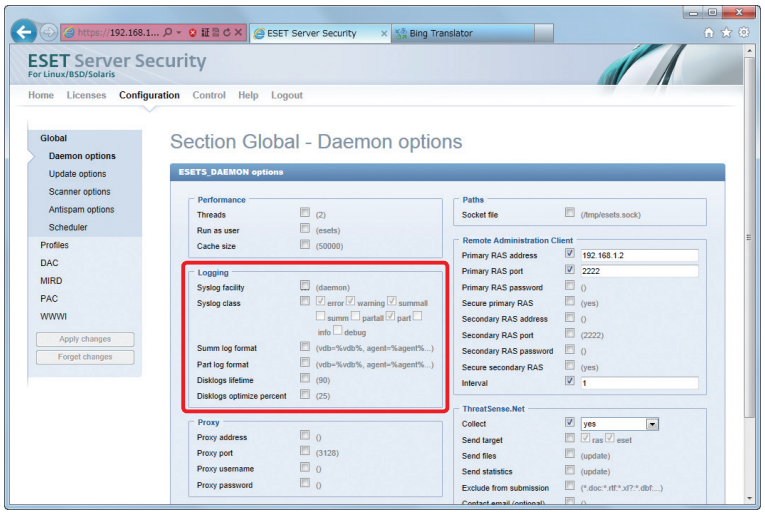


3.12 ログファイル

ESET File Security for Linuxは、syslog経由でさまざまな情報を出力するように設定されています。出力されたログは、システムの分析、ウイルスの検出、およびトラブルシューティングで重要なツールとして利用されます。ここでは、ログの設定について説明します。

3.12.1 syslog経由で出力するログの設定について

ESET File Security for Linuxがsyslog経由で出力するログの設定は、「Configuration」メニューの「Global」セクション内の「Daemon options」で行います。また、以下の項目について設定できます。



POINT

SyslogファシリティとSyslogクラス（項目）についてはESET File Security for Linuxの機能ごとに変更できます。

項目	既定値	概要
Syslog facility	daemon	Syslogファシリティの設定
Syslog class	error,warning,summall,part	Syslog クラス(項目の設定) error:エラーレベルのログ warning:警告レベルのログ summall:検査したすべてのファイルのログ summ:検査したファイルのログ(ウイルスに感染したファイルのみ) partall:検査したすべての特定ファイル(アーカイブファイルなど)のログ part:検査した特定ファイルのログ(ウイルスに感染した特定ファイルのみ) info:情報レベルのログ debug:デバッグレベルのログ
Summ log format	vdb= % vdb % , agent= % agent % , name="% name% ", virus="% virus% ", action="% action% ", info="% info% ", avstatus=" % avstatus % ", hop="% hop% "	通常のファイルの検査ログのフォーマット
Part log format	vdb= % vdb % , agent= % agent % , name="% name% ", virus="% virus% ", action="% action% ", info="% info% "	特定ファイル(アーカイブファイル等)の検査ログのフォーマット
Disklogs lifetime	90	ESET Remote Administratorへ送信するログの有効期限(日数)。これ以前のログを削除する
Disklogs optimize percent	25	ESET Remote Administratorへ送信するログの最適化の設定。使用されていないエントリの割合が設定した値よりも大きくなったら最適化を行う

3.12.2 syslogの詳細設定

ESET File Security for Linuxの既定値では、Syslog facilityに「daemon」が設定されており、各種デーモンのログと同じファイルに本製品のログが出力されます。この設定を変更し、ESET File Security for Linux専用のログファイルにログを出力するには、syslogの設定を変更します。また、オンアクセススキャン（リアルタイムスキャン）のログを非同期で書き込む事によりサーバーのパフォーマンスが向上することがあります。ここでは、syslogの出力先を変更する方法と非同期でログを書き込む方法を紹介します。

設定例

出力先ログファイル：/var/log/eset-syslog.log
Syslog facility：local5

CAUTION

専用のログファイルは自動的にはローテーションされません。Linuxの設定で必要に応じてログファイルをローテーションする設定を行ってください。

CentOS/Red Hat Enterprise Linux 6.3でのsyslog設定例

1 ESET File Security for Linuxのログを出力するファイルを作成します。コマンドラインで以下のように入力します。

```
#touch /var/log/eset-syslog.log
```

2 ログファイルの出力先の設定を行います。設定は、/etc/rsyslog.confにインクルードされるファイル（ここでは、「/etc/rsyslog.d/eset.conf」）に書き込みます。以下の内容のファイルを作成します。

```
local5.*  -/var/log/eset-syslog.log
```

▸▸▸ POINT

rsyslogは、出力先ログファイルのパスの前に-（ハイフン）をつけると非同期でログを書き込みます。

3 Syslog facility「local5」のログを/var/log/messagesに書き込まないように設定します。「/etc/rsyslog.conf」の内容を以下のように書き換えます。

変更前

```
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none                /var/log/messages
```

変更後

```
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none;local5.none                /var/log/messages
```

4 rsyslogを再起動します。コマンドラインで以下のように入力します。

```
#service rsyslog restart
```

SUSE Linux Enterprise10 sp3でのsyslog設定例

1 ESET File Security for Linuxのログを出力するファイルを作成します。コマンドラインで以下のように入力します。

```
#touch /var/log/eset-syslog.log
```

2 ログファイルの出力先の設定を行います。設定は、「/etc/syslog-ng/syslog-ng.conf」に以下の内容を最終行に追記します。

```
filter f_esets { facility(local5); };
destination esets { file("/var/log/eset-syslog.log"); };
log { source(src); filter(f_esets); destination(esets); };
```

››› POINT

syslog-ngは、既定で非同期でログを書き込みます。

3 Syslog facility「local5」のログを/var/log/messagesに書き込まないように、引き続き「/etc/syslog-ng/syslog-ng.conf」の内容を以下のように書き換えます。

変更前

```
filter f_messages { not facility(news, mail) and not filter(f_iptables); };
```

変更後

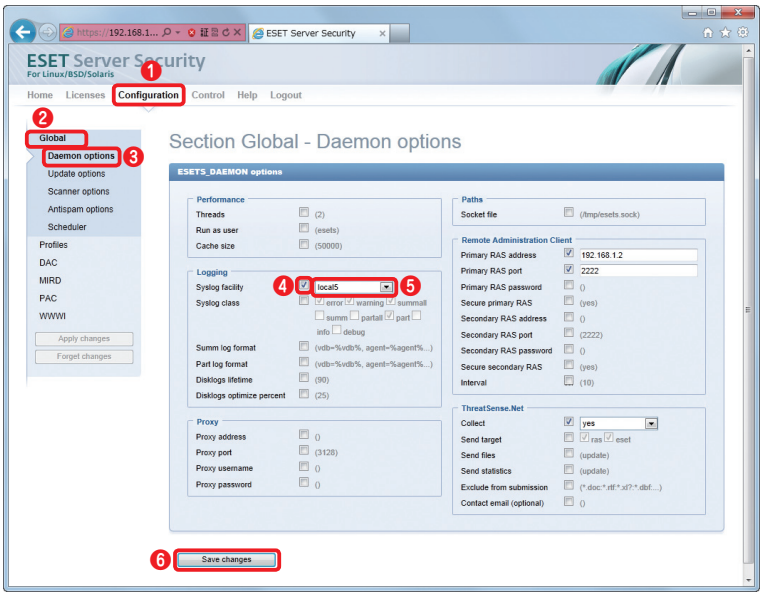
```
filter f_messages { not facility(news, mail, local5) and not filter(f_iptables); };
```

4 syslog-ngを再起動します。コマンドラインで以下のように入力します。

```
#service syslog restart
```

ESET File Security for Linuxのsyslogの設定

1



ESET File Security for Linuxのsyslogの設定を変更します。Webブラウザーを開き、Webインターフェースのページを開きます。❶[Configuration]をクリックし、❷[Global]をクリックします。❸[Daemon options]をクリックし、❹[Syslog facility]にチェックを入れます。❺ドロップダウンリストから[local5]を選択します。❻[Save changes]ボタンをクリックします。

設定を反映させるために、メニューオプションの[Apply changes]ボタンをクリックします。問題がなければメインウィンドウに表示される[Yes]ボタンをクリックします。(参考情報「3.1.2 Webインターフェースでの設定の反映」)

▸▸▸ POINT

出力するログを選択したいときは、[Syslog class]にチェックを入れ、出力したい項目にチェックを入れます。また、[Summ log format]や[Part log format]にチェックを入れると、出力するログのフォーマットを設定できます。

3.12.3 ログの閲覧

ESET File Security for Linuxのログはテキスト形式で出力されますので、ログファイルはLinux上のテキスト閲覧コマンドを利用して閲覧してください。ここでは、検査ログに出力される項目の内容を説明します。

出力項目の内容

項目名	内容
vdb	ウイルス定義データベースのビルドナンバー
vdv	ウイルス定義データベースのバージョン
agent	ESET agentのモジュール名
name	ウイルスが検出されたファイル名
virus	検出されたウイルス名
action	ウイルスを検出したことによって実行したアクション
info	スキャナーから報告された追加情報
avstatus	アンチウィルススキャンステータス
hop	スキャンされたオブジェクトに対して実施されたアクション

3.13 通知スクリプト

リアルタイムスキャン及びスケジューラから実行するオンデマンドスキャン（[On-demand computer scan]）タスクでウイルスを検出した場合に、設定したメールアドレス宛に電子メールで通知します。
このスクリプト（daemon_notification_script）は以下のディレクトリに保存されており、通知する本文内容などを修正する事が可能です。

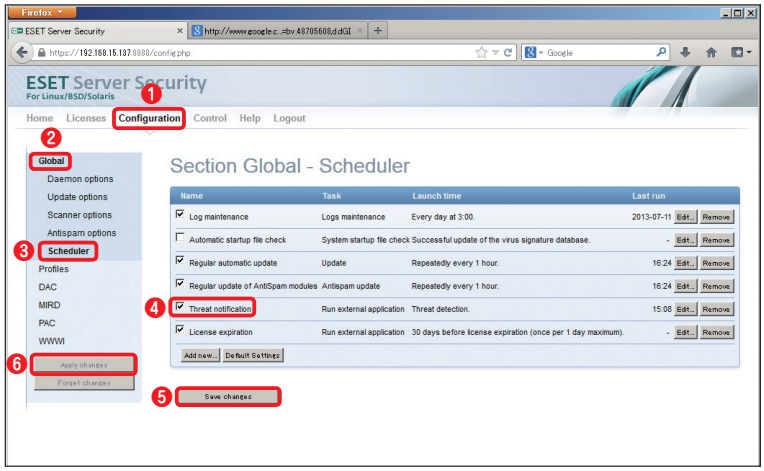
```
/etc/opt/eset/esets/scripts/daemon_notification_script
```

このスクリプトを利用するためには、スケジューラ設定にある「Threat notification」のタスクを有効にする必要があります。ここでは通知を有効にする手順を説明します。

3.13.1 メール通知スクリプトの有効化

Webブラウザーから、ESET File Security for LinuxのWebインターフェースにアクセスします。

1



最初に❶ [Configuration] をクリックし、❷ [Global] をクリックします。
次に❸ [Scheduler] をクリックし、❹ [Threat notification] にチェックを入れて❺ [Save changes] ボタンをクリックします。最後に❻ [Apply changes] をクリック後、[Yes] をクリックし設定を反映させてください。

3.13.2 メール通知スクリプトの編集

初期値のメール通知スクリプトで送信される本文などの設定内容は以下の通りです。
必要に応じて修正することが可能です。設定可能な変数については「ウイルス検出時の通知スクリプトで利用可能な変数」を参照してください。
なお、ESET File Security for Linuxのメール通知スクリプトはsendmailコマンドを利用して通知メールを送信します。

CAUTION

メール通知スクリプトを実行するサーバーがsendmailコマンドを利用して、設定した宛先にメール配信できるように事前にMTAの設定を適切に行ってください。

daemon_notification_script

```
/usr/sbin/sendmail -t -oi << %%
From: esets_daemon
To: root
Subject: notification

  USERSPEC: ${ESETS_USERSPEC}
     MSGID: ${ESETS_MSGID}
    SENDER: ${ESETS_SENDER}
 RECIPIENT: ${ESETS_RECIPIENT}
 AV_STATUS: ${ESETS_AV_STATUS}
    ACTION: ${ESETS_ACTION}
     VIRUS: ${ESETS_VIRUS}
       LOG: ${ESETS_LOG}
%%
```

メール通知スクリプトの変数の内容

NO	パラメータ	説明
1	From	通知メールの送信者アドレス(FROMアドレス)を設定
2	To	通知メールの受信者アドレス(TOアドレス)を設定
3	Subject	通知メールの件名を設定
4	${ESETS_USERSPEC}	ウイルスが検出された作業を行ったユーザー名を出力
5	${ESETS_MSGID}	ウイルスを検出したメールのメッセージIDを出力 ※1
6	${ESETS_SENDER}	ウイルスを検出したメールの送信者アドレスを出力 ※1
7	${ESETS_RECIPIENT}	ウイルスを検出したメールの受信者アドレスを出力 ※1
8	${ESETS_AV_STATUS}	検出されたウイルスファイルに対するスキャン結果を出力 ・clean (deleted) : ウイルスを駆除(削除)されて安全な状態 ・infected : アクセス権や設定によりウイルスファイルを駆除(削除)できなかった状態
9	${ESETS_ACTION}	スキャン後のアクションを出力 ※2
10	${ESETS_VIRUS}	検出されたウイルス名を出力
11	${ESETS_LOG}	ウイルスが検出された時のESETの検査デーモン(esets_daemon)のログ情報を出力 出力されるログの設定は「ESET File Security for Linux マニュアル」のP51 ～ P55を参照してください。

※1 NO5,6,7のパラメータはESET Mail Security for Linuxで使用するため、ESET File Security for Linuxでは出力されません。
※2 NO9のパラメータは主にESET Mail Security for Linuxでウイルス駆除後のメールに対して行ったアクションを表示するために利用されます。そのため、ESET File Security for Linuxでは表示されたアクションは、検出したファイルに影響を与えません。

3.14 コンフィグレーションファイルでの設定

ESET File Security for Linuxの各種設定は、Webインターフェースを利用して行えるほか、コンフィグレーションファイル（/etc/opt/eset/esets/esets.cfg）を直接編集することでも行えます。また、コンフィグレーションファイルを直接編集した場合は、変更した設定を反映するためにESET File Security for Linuxを再起動する必要があります。ESET File Security for Linuxの再起動は、コマンドラインで以下のように入力します。

```
#/etc/init.d/esets restart
```

セクション名	設定内容
[Global]セクション	このセクションでは、ESET File Security for Linuxの全般の設定が行えます。Webインターフェースの[Global]セクションと同じ設定が行えます。
[wwwi]セクション	このセクションでは、Webインターフェースに関する設定が行えます。Webインターフェースの[WWWI]セクションと同じ設定が行えます。
[mird]セクション	このセクションでは、ESET File Security for Linuxが搭載する「Mirror http daemon」を利用してウイルス定義データベースのアップデートを配布する場合の設定が行えます。Webインターフェースの[MIRD]セクションと同じ設定が行えます。
[dac]セクション	このセクションでは、Dazukoと呼ばれるモジュールを利用したオンアクセススキャン（リアルタイムスキャン）の設定を行えます。Webインターフェースの[DAC]セクションと同じ設定が行えます。 ※この機能は、ESET File Security for Linuxではサポート対象外となります。
[pac]セクション	このセクションでは、ESET社が提供するオンアクセススキャン用ライブラリを利用したオンアクセススキャン（リアルタイムスキャン）の設定を行えます。Webインターフェースの[PAC]セクションと同じ設定が行えます。
[scan_deep]セクション	このセクションでは、「deep」プロファイルの設定が行えます。Webインターフェースの[Profiles]セクションの「deep」プロファイルの設定と同じ設定が行えます。
[scan_smart]セクション	このセクションでは、「smart」プロファイルの設定が行えます。Webインターフェースの[Profiles]セクションの「smart」プロファイルの設定と同じ設定が行えます。
[start]セクション	このセクションでは、「start」プロファイルの設定が行えます。Webインターフェースの[Profiles]セクションの「start」プロファイルの設定と同じ設定が行えます。

3.15 コマンドライン操作

ESET File Security for Linuxのオンデマンドスキャンの実行やウイルス定義データベースのアップデート、ライセンス管理、隔離ファイルの管理などはコマンドラインからも行えます。ここでは、コマンドライン操作について説明します。

コマンド	内容
/opt/eset/esets/sbin/esets_scan	オンデマンドスキャンの実行
/opt/eset/esets/sbin/esets_lic	ライセンスの管理
/opt/eset/esets/sbin/esets_update	ウイルス定義データベースのアップデート
/opt/eset/esets/sbin/esets_quar	隔離ファイルの管理

3.15.1 オンデマンドスキャン

コマンドラインでオンデマンドスキャンを実行するときは、以下のように入力します。

```
#/opt/eset/esets/sbin/esets_scan [オプション ..] ディレクトリ ..
```

入力例

「smart」プロファイルを利用し、「/home/share」ディレクトリのオンデマンドスキャンを実施する場合は、以下のように入力します。

```
#/opt/eset/esets/sbin/esets_scan --profile=scan_smart /home/share
```

「deep」プロファイルを利用し、「/usr/local」以下のファイルを除外したすべてのファイルに対してオンデマンドスキャンを実行し、その結果をログファイル「/var/log/esetscan.log」に残す場合は、以下のように入力します。

```
#/opt/eset/esets/sbin/esets_scan –profile=scan_deep –log-file=/var/log/esetscan.log
–exclude=/usr/local/*  /
```

「deep」プロファイルを利用し、すべてのファイルに対してオンデマンドスキャンを実行し、検査を実行したユーザーを「root」で任意のタスク番号を「1」としてESET Remote Administratorへ検査結果のログを送信する場合は、以下のように入力します。

```
#/opt/eset/esets/sbin/esets_scan --profile=scan_deep --scanlog=1:root /
```

esets_scanのオプションの一覧

Options

引数	内容
--exclude=MASK	検査を行わないファイルの設定
--subdir	検査ディレクトリ内のサブディレクトリの検査の実施（default）
--no-subdir	検査ディレクトリ内のサブディレクトリの検査を行わない
--max-subdir-level=level	検査を行うサブディレクトリの最大階層数
-s, --symlink	シンボリックリンク先の検査を行う（default）
--no-symlink	シンボリックリンク先の検査を行わない
--sysexclude	システムコントロールディレクトリの検査を自動的に除外する（default）
--no-sysexclude	システムコントロールディレクトリの検査を行う
--ads	代替データストリームを検査する（default）
--no-ads	代替データストリームを検査しない
-f, --log-file=FILE	指定したファイルに検査ログを出力する
--log-rewrite	検査ログを上書きする（default）
--log-console	コンソールに検査ログを表示する（default）
--no-log-console	コンソールに検査ログを表示しない
-o, --log-all	クリーンファイルのログを出力する
--no-log-all	クリーンファイルのログを出力しない（default）
--scanlog=TASK:USER	任意のタスク番号とユーザー名を使用してESET Remote Administratorへ送信するスキャンログを作成する
--aind	アクティビティインジケータを表示する
--auto	自動的にすべてのローカルディスクの検査を行い、駆除を行う
-p, --profile=PROFILE	検査に利用するプロファイルを指定する

Scanner options

引数	内容
--files	ファイルを検査する（default）
--no-files	ファイルを検査しない
-z, --arch	アーカイブファイルを検査する（default）
--no-arch	アーカイブファイルを検査しない
--max-obj-size=size	検査を行うオブジェクトの最大サイズの設定（MB単位、既定値は、制限なし）
--max-arch-level=level	アーカイブファイルの検査を行う場合の最大階層
--scan-timeout=LIMIT	アーカイブファイルの最大検査時間の設定（秒単位）
--max-arch-size=size	アーカイブファイルの検査を行う場合の解凍後の最大ファイルサイズ
--mail	電子メールの検査を行う（default）
--max-sfx-size=size	自己解凍ファイルの最大ファイルサイズの設定（MB単位）
--no-mail	電子メールの検査を行わない
--mailbox	メールボックスの検査を行う（default）
--no-mailbox	メールボックスの検査を行わない
--sfx	自己解凍形式のファイルの検査を行う（default）
--no-sfx	自己解凍形式のファイルの検査を行わない
--rtp	圧縮された実行形式のファイルの検査を行う（default）
--no-rtp	圧縮された実行形式のファイルの検査を行わない
--adware	Adware/Spyware/Riskwareの検査を行う（default）
--no-adware	Adware/Spyware/Riskwareの検査を行わない
--unsafe	安全でない可能性があるアプリケーションの検出を行う
--no-unsafe	安全でない可能性があるアプリケーションの検出を行わない（default）
--unwanted	望ましくない可能性があるアプリケーションの検出を行う
--no-unwanted	望ましくない可能性があるアプリケーションの検出行わない（default）
--pattern	検査方法にウイルスシグネイチャを使用する（default）
--no-pattern	検査方法にウイルスシグネイチャを使用しない
--heur	検査方法にヒューリスティックを使用する（default）
--no-heur	検査方法にヒューリスティックを使用しない
-w, --adv-heur	検査方法にアドバンスドヒューリスティックを使用する（default）

--no-adv-heur	検査方法にアドバンスドヒューリスティックを使用しない
--ext=EXTENSIONS	「:(コロン)」で区切られたファイルのみを検査する
--ext-exclude=EXTENSIONS	「:(コロン)」で区切られたファイルの検査を行わない
--clean-mode=MODE	駆除レベル(既定値は削除を行わない「standard」)
--quarantine	感染ファイルの隔離を行う
--no-quarantine	感染ファイルの隔離を行わない

General options	
引数	内容
-h, --help	ヘルプを表示する
-v, --version	バージョン情報を表示する
--preserve-time	最終アクセスタイムスタンプを維持する

Exit codes(終了コード)	
終了コード	内容
0	感染ファイルなし
1	感染ファイルを検出し、駆除を行った
10	検査を行えないファイルが存在した。脅威が存在するかもしれません。
50	感染ファイルを検出した
100	エラー

3.15.2 ライセンスの管理

コマンドラインでライセンスを管理するときは、以下のように入力します。

```
#/opt/eset/esets/sbin/esets_lic [オプション ..] [コマンド] [ファイル ..]
```

ESET File Security for Linuxにインポートされている期限切れのライセンスキーファイルを削除する場合は以下のように入力します。

```
#/opt/eset/esets/sbin/esets_lic –remove-expired
```

esets_licのオプションの一覧

引数	内容
--list	登録済みライセンスの一覧を表示
--import=FILE	ライセンスキーファイルのインポート
--remove-expired	期限切れのライセンスキーファイルを削除
--list-fmt=FORMAT	ライセンスリストの表示フォーマットを指定
-h, --help	ヘルプの表示
-v, --version	バージョン情報を表示

3.15.3 ウイルス定義データベースのアップデート

コマンドラインでウイルス定義データベースのアップデートを行うときは、以下のように入力します。

```
#/opt/eset/esets/sbin/esets_update［オプション ..］
```

ESET File Security for Linuxに現在設定されているコンフィグレーションで、ウイルス定義データベースのアップデートを実行する場合は以下のように入力します。

```
#/opt/eset/esets/sbin/esets_update
```

esets_updateのオプションの一覧

引数	内容
--cfg-path=FILE	コンフィグレーションファイル(esets.cfg)のパスの指定
-s, --server=ADDRESS	アップデートサーバーのアドレス
-u, --username=USERNAME	ユーザー名
-p, --password=PASSWORD	パスワード
--prerelease-updates	プレリリースアップデートを有効にする
--proxy-addr=ADDRESS	プロキシサーバーのアドレス
--proxy-port=PORT	プロキシサーバーのポート番号
--proxy-username=USERNAME	プロキシサーバーでユーザー認証を利用している場合のユーザー名
--proxy-password=PASSWORD	プロキシサーバーでユーザー認証を利用している場合のパスワード
--restricted-user=USER	esets_updateはアップデートをダウンロードする前に、ここで指定したユーザーに切り替え、特定のディレクトリの所有権の調整を自動的に行います。
--mirror	ミラーサーバー機能を有効にします。
--mirror-pcu=LIST	プログラムコンポーネントのミラーを作成する場合にダウンロードを行うプログラムコンポーネントのリスト
--verbose	冗長モードでアップデートを実行します。
--silent	サイレントモードでアップデートを実行します。
-h, --help	ヘルプを表示します。
-v, --version	バージョン情報を表示します。

Exit codes(終了コード)	
コード	内容
0	成功
other	エラー

3.15.4 隔離ファイルの管理

コマンドラインで隔離ファイルの管理を行うときは、以下のように入力します。

```
#/opt/eset/esets/sbin/esets_quar コマンド［ルール］［オブジェクト ..］
```

隔離されているファイルを一覧表示する場合は以下のように入力します。

```
# /opt/eset/esets/sbin/esets_quar -l
```

隔離ファイルの一覧表示例

```
id="5834281359974756716", date="17.01.2013 14:11:12", name="./eicar.com", size="68",
reason="Eicar test file", count="1"
id="5834280538916396591", date="17.01.2013 14:07:41", name="/root/testfile.txt", size="61",
reason="added by user", count="1"
```

上記の隔離ファイルの一覧例から「testfile.txt」を「/tmp」ディレクトリに復元する場合は以下のように入力します。なお、復元された後のファイル名は「58342805389163965 91.testfile.txt」のように「ID.元のファイル名」になります。

```
# /opt/eset/esets/sbin/esets_quar -r /tmp –object-name=/root/testfile.txt
```

esets_quarのオプションの一覧

Commands

引数	内容
-i, --import	指定したファイルを隔離します。
-r, --restore=FOLDER	指定したディレクトリに隔離ファイルを復元します。
-l, --list	隔離ファイルの一覧を表示します。
-s, --send	ESETのウイルスラボに指定したファイルを提出します。
-d, --delete	指定したファイルを隔離ディレクトリから削除します。

Rules:

引数	内容
--id=VALUE	オブジェクトの識別番号の指定。
--size-min=VALUE	選択したいオブジェクトの最小サイズの指定。
--size-max=VALUE	選択したいオブジェクトの最大サイズの指定。
--date-min=VALUE	選択したいオブジェクトのタイムスタンプの指定(古い日付)
--date-max=VALUE	選択したいオブジェクトのタイムスタンプの指定(新しい日付)
--object-name=NAME	隔離ファイルのファイル名
--count-min=VALUE	選択したいオブジェクトのエントリー IDの指定(最小)
--count-max=VALUE	選択したいオブジェクトのエントリー IDの指定(最大)

Options:

引数	内容
--list-fmt=FORMAT	隔離ファイル一覧の表示フォーマットの指定

Common options

-h, --help	ヘルプの表示
-v, --version	バージョン情報を表示

3.16 設定リファレンスについて

ESET File Security for Linuxの設定リファレンスについては弊社ホームページ上にて公開していますので、ぜひご活用ください。設定リファレンスは、以下のURLでアクセスできます。

http://canon-its.jp/supp/eset/man/efsl/