



「ESET Endpoint Protection シリーズ」  
「ESET File Security for Linux/Windows Server」  
**ESET File Security for Linux V7.2 機能紹介資料**

第2版

2021年2月10日

**Canon**

キヤノンマーケティングジャパン株式会社

# はじめに（本資料について）

本資料は「ESET Endpoint Protection シリーズ」「ESET File Security for Linux / Windows Server」のLinuxサーバーOS向けプログラムの機能を紹介した資料です。

| プログラム名                                       | 種別                             |
|--|--------------------------------|
| ESET File Security for Linux V7.2（略称表記：EFSL） | Linux サーバー用 ウイルス・スパイウェア対策プログラム |

- ・本資料で使用している画面イメージは使用するOSにより異なる場合があります。また、今後画面イメージや文言が変更される可能性がございます。
- ・上記のプログラムはクライアント管理用プログラムである ESET Security Management Center V7.1（略称表記：ESMC）以降、または ESET PROTECT V8.X（略称表記：EP）で管理が可能です。ESMCとEPの機能紹介は、別資料をご用意しております。
- ・ESMCとEPは、法人向けサーバー・クライアント用製品「ESET Endpoint Protection シリーズ」をご契約のお客さまのみ利用可能です。
- ・「ESET Endpoint Protection シリーズ」ではWindows、Mac、Android OS向けのプログラムもご使用いただけます。また、LinuxクライアントOS向けのプログラムもご使用いただけます。  
「ESET File Security for Linux / Windows Server」では、Windows Server OS向けのプログラムもご使用いただけます。各プログラムの機能紹介は別資料をご用意しています。

# 目次

1. サポート環境
2. Webインターフェースについて
3. 詳細設定について
4. ESET File Security for Linux4.5との違い
  - (1) インストールについて
  - (2) Webインターフェース
  - (3) アクティベーション
5. EFSL V4.5との機能比較



# サポート環境

**Canon**

キヤノンマーケティングジャパン株式会社

# 1. サポート環境



| 項目                  | 条件   | 備考  |
|---------------------|--|---|
| OS                  | Red Hat Enterprise Linux 6.X (64bit)<br>Red Hat Enterprise Linux 7.X (64bit)<br>Red Hat Enterprise Linux 8.X (64bit)<br>SUSE Linux Enterprise 12 SP1まで (64bit)<br>SUSE Linux Enterprise 15 SP1まで (64bit)<br>CentOS 6.X (64bit)<br>CentOS 7.X (64bit)<br>CentOS 8.X (64bit) | Red Hat Enterprise Linux (以降、RHEL)<br>SUSE Linux Enterprise (以降、SUSE) |
| 仮想環境                | VMware ESX/ESXi 4.0/4.1<br>VMware ESX/ESXi 5.0以降<br>Citrix XenServer 5.6<br>Windows Server 2008 R2 Hyper-V<br>Windows Server 2012 Hyper-V<br>Windows Server 2012 R2 Hyper-V<br>Windows Server 2016 Hyper-V<br>Windows Server 2019 Hyper-V                                  | 仮想化ソフトウェアがOSをサポートしていること   |
| クラウド<br>コンピューティング環境 | Amazon Web Services  |   |
| CPU                 | Intel,AMD(64bit)   |   |
| メモリ                 | 256MB以上  |   |
| ハードディスク             | 700MB以上  |   |
| 必要ソフトウェア            | kernelバージョン 2.6.32 または それ以上のバージョン<br>glibc 2.12 または それ以上のバージョン   |   |
| その他                 | UTF-8エンコーディングを使用する任意のロケール  |   |



# Webインターフェースについて

**Canon**

キヤノンマーケティングジャパン株式会社

# 2. Webインターフェースについて

## (1) ダッシュボード

- ダッシュボードから保護状況の確認が可能です。また、検出エンジンの手動アップデートやロールバック、アクティベーションなどを行うことが可能です。

■ ダッシュボード画面（例：保護の状態）



■ ダッシュボード画面（例：モジュールのアップデート）



## 2. Webインターフェースについて

### (2) 検出

- 検出されたすべての脅威とそれらに対して実行されたアクションは、検出画面に記録されます。脅威が検出され、駆除されていない場合は、行全体が赤色でハイライトされます。検出された悪意があるファイルの駆除を試行するには、特定の行をクリックし、「駆除して再検査」を選択します。

#### ■ 検出結果画面

| 検出された時間           | 重大度 | スキャナー       | オブジェクトURI             | 検出    | 検出タイプ   | アクション       | ユーザー | アプリケーション      | 状況                             |
|-------------------|-----|-------------|-----------------------|-------|---------|-------------|------|---------------|--------------------------------|
| 2020年11月11日 09:57 | 🟡   | リアルタイムファ... | file:///tmp/eicar.com | Eicar | テストファイル | 削除によって駆除... | root | /usr/bin/bash | ファイルにアクセスしようとしたときにイベントが発生しました。 |
| 2020年11月11日 09:46 | 🔴   | リアルタイムファ... | file:///tmp/eicar.com | Eicar | テストファイル | 駆除できません     | root | /usr/bin/scp  | 新規作成されたファイルでイベントが発生しました。       |
| 2020年11月11日 09:44 | 🟡   | リアルタイムファ... | file:///tmp/eicar.com | Eicar | テストファイル | 削除によって駆除... | root | /usr/bin/scp  | 新規作成されたファイルでイベントが発生しました。       |

スケジューラー設定に基づいて古いデータが削除された可能性があります。



## 2. Webインターフェースについて

### (3) 検査

- 手動でのオンデマンド検査が可能です。「すべてのローカルドライブを検査」と「カスタム検査」が選択可能で、「カスタム検査」では、事前に作成したプロファイルに基づいた検査や検査対象を指定した検査が可能です。また、検査結果をクリックすることで詳細情報が確認可能です。

#### ■ 検査画面

| 開始時刻             | 進行状況 | 検査済み   | 駆除済み | 検出されました | 時間  | トリガー |
|------------------|------|--------|------|---------|-----|------|
| 完了               |      |        |      |         |     |      |
| 2020年11月5日 17:08 | 完了   | 49,935 | 1    | 1       | 16分 | root |

スケジューラ設定に基づいて古いデータが削除された可能性があります。

#### ■ 検査の詳細画面①

| 基本情報 |                  | 検査設定               | オブジェクト           |
|------|------------------|--------------------|------------------|
| 開始時刻 | 2020年11月5日 17:08 | 検査したディスク、フォルダ、ファイル | 検出されました <b>1</b> |
| 終了時刻 | 2020年11月5日 17:23 |                    | 駆除済み 1           |
| 時間   | 16分              |                    | 未検出 0            |
|      |                  |                    | 検査済み 49,935      |

#### ■ 検査の詳細画面②

| 検出された時刻       | 重大度 | オブジェクトURI          | 検出    | 検出タイプ   | アクション          |
|---------------|-----|--------------------|-------|---------|----------------|
| 2020年11月5日... | ... | file:///etc/passwd | Eicar | テストファイル | 削除によって駆除されま... |

## 2. Webインターフェースについて

### (4) イベント

- EFSL V7.2のWebインターフェースで実行される重要なアクション、Webインターフェースへのログインの失敗、ターミナルから実行されるEFSL V7.2関連のコマンド、および一部のその他の情報はイベント画面に出力されます。

#### ■ イベント画面

| 時刻               | コンポーネント      | イベント  | ユーザー              |
|------------------|--------------|---|-------------------|
| 2020年11月5日 17:09 | 認証サービス       | 無効な資格情報   | eset-efs-authd    |
| 2020年11月5日 16:15 | 更新サービス       | モジュールが正常にアップデートされました。   | eset-efs-updated  |
| 2020年11月5日 15:15 | 更新サービス       | モジュールが正常にアップデートされました。   | eset-efs-updated  |
| 2020年11月5日 15:09 | サービスを開始しています | ソケットから読み取れません: ピアによって接続がリセットされました   | root              |
| 2020年11月5日 15:09 | 構成サービス       | ソケットに書き込めません: 破損したパイプ   | eset-efs-confd    |
| 2020年11月5日 15:09 | 構成サービス       | ソケットに書き込めません: 破損したパイプ   | eset-efs-confd    |
| 2020年11月5日 15:09 | ログサービス       | ソケットに書き込めません: 破損したパイプ   | eset-efs-logd     |
| 2020年11月5日 15:04 | 更新サービス       | モジュールが正常にアップデートされました。   | eset-efs-updated  |
| 2020年11月5日 14:59 | リアルタイム保護サービス | アクセス中の検査のシステムハンドラーの初期化が失敗しました。OSを更新して、コンピューターを再起動してから...                                  | root              |
| 2020年11月5日 14:59 | リアルタイム保護サービス | ファイル/lib/modules/3.10.0-957.el7.x86_64/efset/efs/efset_rtp.koを開けません: ファイルまたはディレクトリがありま... | root              |
| 2020年11月5日 14:57 | 更新サービス       | 検出エンジンが正常にバージョン22268 (20201105)にアップデートされました。  | eset-efs-updated  |
| 2020年11月5日 14:56 | ライセンスサービス    | 同じ名前のコンピューターがこのアカウントに存在します。   | eset-efs-licensed |
| 2020年9月2日 14:20  | リアルタイム保護サービス | アクセス中の検査のシステムハンドラーの初期化が失敗しました。OSを更新して、コンピューターを再起動してから...                                  | root              |
| 2020年9月2日 14:20  | リアルタイム保護サービス | ファイル/lib/modules/3.10.0-957.el7.x86_64/efset/efs/efset_rtp.koを開けません: ファイルまたはディレクトリがありま... | root              |
| 2020年9月2日 14:19  | 認証サービス       | 無効な資格情報   | eset-efs-authd    |

## 2. Webインターフェースについて

### (5) 隔離

- EFSL V7.2によって隔離されたファイルを表示します。隔離された時間やファイルのパス、理由などの確認ができます。隔離されたファイルをクリックすることで、以下のアクションが可能です。

■ 隔離画面

| TIME     | OBJECT                | REASON        | SIZE | COUNT |
|----------|-----------------------|---------------|------|-------|
| 2020年11月 | /etc/eicar.com        | Eicar テストファイル | 68 B | 1     |
| 2020年11月 | /etc/kernel/eicar.com | Eicar テストファイル | 68 B | 2     |

**【復元】** : 隔離された検体を復元します  
(再度誤検知されないように「検出除外」の設定が必要です)

**【パスのコピー】** : 検体が検出されたパスをコピーします

**【ダウンロード】** : 隔離された検体をブラウザからダウンロードします

**【隔離から削除】** : 隔離された検体を削除します

## 2. Webインターフェースについて

### (6) 設定

- 検出エンジン、アップデート、ツールについて設定の確認や変更を行うことが可能です。また、業務を行ううえで一時的にESETの保護機能を変更させたい場合は、Webインターフェースから設定を一時的に有効や無効にすることが可能です。

#### ■ 設定画面

#### 【検出エンジン】

検出エンジンの項目では、検出するアプリケーションの種類を定義するスキャナオプションや特定のファイルやフォルダをウイルス検査の対象から外す除外、各保護機能の詳細設定が可能です。

#### 【アップデート】

アップデートの項目では、検出エンジンの取得先を変更することなどが可能です。  
アップデートモードは通常のアップデートモードのほか、通常検出エンジンの配信より少し早く配信されるテストモードや、逆に通常配信後12時間経過してから配布される遅延アップデートを選ぶことが可能です。

#### 【ツール】

ツールの項目では、スケジューラ機能によるオンデマンド検査やプロキシサーバの設定、Webインターフェースのパスワード/SSL証明書の変更が可能です。

設定

検出エンジン

- リアルタイムファイルシステム保護
- クラウドベース保護
- マルウェア検査
- リモート検査

アップデート

ツール

基本

スキャナオプション

- 望ましくない可能性のあるアプリケーションの検出を有効にする
- 安全でない可能性のあるアプリケーションの検出を有効にする
- 疑わしい可能性のあるアプリケーションの検出を有効にする

除外

- パフォーマンス除外 [編集](#)
- 検出除外 [編集](#)

共有ローカルキャッシュ

保存 破棄



# 詳細設定について

**Canon**

キヤノンマーケティングジャパン株式会社

# 3. 詳細設定について

## (1) 検出エンジン

- 検出エンジンの項目では、コンピューターのパフォーマンスを低下させる恐れのあるアプリケーションや不正利用される可能性のあるアプリケーションを検出させるかどうかを設定することなどが可能です。

■ 検出エンジン設定画面

The screenshot shows the 'Detection Engine' settings page. On the left, a sidebar lists various settings, with 'Detection Engine' highlighted. The main area is titled '基本' (Basic) and contains several options under 'スキャナオプション' (Scanner Options). Three options are highlighted with red boxes and linked to callout boxes:

- 「望ましくない可能性があるアプリケーション」** (Applications with undesirable possibilities): This option is checked. The callout explains that it detects applications like adware or toolbars that negatively impact computer performance.
- 「安全でない可能性があるアプリケーション」** (Applications with unsafe possibilities): This option is unchecked. The callout explains that it detects applications like remote access tools or password analyzers that have the potential for misuse.
- 「疑わしい可能性があるアプリケーション」** (Applications with suspicious possibilities): This option is checked. The callout explains that it detects compressed files like zip files or programs compressed with Proton, which malware creators use to evade detection.

# 3. 詳細設定について

## (2) 除外

- 除外の設定を行うことで、特定のファイルやフォルダをウイルス検査の対象から外すことが可能です。パス、ハッシュ値、検出名で除外設定を行えます。独自開発したアプリケーションやデータベースなどを除外の対象とすることで、誤検知やデータベースなどを検査した際のCPU使用率の上昇を防ぐことが可能です。

### ■ 検出エンジン設定画面

**「パフォーマンス除外」**  
特定のファイルやフォルダを検査対象から除外することが可能です。特定のファイルやフォルダを検査対象から除外することが可能です。

**「検出除外」**  
指定したパスの検査は行いますが、ルールに定められたオブジェクトやハッシュを検出から除外します。指定したパスの検査は行いますが、ルールに定められたオブジェクトやハッシュを検出から除外します。

### ■ パフォーマンス除外設定画面

### ■ 検出除外設定画面

# 3. 詳細設定について

## (3) リアルタイムファイルシステム保護

- リアルタイムファイルシステム保護を使用すると、ファイルのオープン時や作成時、また実行時に検査を行うことが可能です。リアルタイムファイルシステム保護はシステム起動時に開始され、中断することなく常に端末を保護します。

■ リアルタイムファイルシステム保護設定画面



【ローカルドライブ】 : システムハードディスクをすべて検査  
 【リムーバブルメディア】 : CD/DVD、USBなどを検査  
 【ネットワークドライブ】 : マッピングされたドライブをすべて検査

【ファイルのオープン】  
 開いたファイルの検査を有効または無効にします。  
 【ファイルの作成】  
 作成するファイルの検査を有効または無効にします。  
 【リムーバブルメディアアクセス】  
 コンピューターに接続するときにリムーバブルメディアの自動検査を有効または無効にします。

※以下のKernelのバージョンが揃っていない場合、リアルタイムファイルシステム保護は有効にできません。

■ RHEL / CentOSの場合 : Kernel, kernel-devel, kernel-headers    ■ SUSEの場合 : kernel-default, kernel-default-devel, kernel-devel, kernel-macros



# 3. 詳細設定について

## (4) クラウドベース保護

- ESET LiveGrid®に参加すると、クラウドシステムにより実行中のプロセスの全世界における使用状況が共有されます。これにより実行中のプロセスのリスクレベルを確認できます。ESET LiveGrid®に不審なファイルを送付すると、送付されたファイルはESET LiveGrid®により解析されます。これは新たな脅威からESETユーザーを守ることに繋がります。

■ クラウドベース保護設定画面



**【ESET LiveGrid®に参加する】**  
 実行中のプロセスの全世界における使用状況を確認するにはチェックを付けてください。ESET LiveGrid®から受け取ったホワイトリストを使用してスキャンパフォーマンスを改善できます。

**【ESET LiveGrid®フィードバックシステムを有効にする】**  
 データは詳細分析のためにESET研究所に送信されます。

**「サンプルの送信」**  
 ESET LiveGrid®に送信するサンプルファイルの種類を設定することが可能です。

# 3. 詳細設定について

## (5) マルウェア検査

- マルウェア検査では、オンデマンド検査の詳細設定を行うことが可能です。検査の対象やウイルス発見時のアクションを設定できます。オンデマンド検査に使用するプロファイルの作成や、システム起動時に実施されるスタートアップ検査の設定が可能です。

■ マルウェア検査設定画面

設定

検索エンジン

- リアルタイムファイルシステム保護
- クラウドベース保護
- マルウェア検査**
- リモート検査

アップデート

ツール

オンデマンド検査

- 選択されたプロファイル: スマート検査
- プロファイルのリスト: 編集
- スマート検査

THREATSENSEパラメータ

検査するオブジェクト

- ブートセクタ/UEFI**
- 電子メールファイル
- アーカイブ
- 自己修復アーカイブ
- 圧縮された実行形式

検査オプション

- ヒューリスティック
- アドバンスドヒューリスティック/DNA署名

駆除

駆除レベル: 厳密な駆除

このモードでは、システムファイルを除く感染したファイルが自動的に駆除または削除されようとしています。

保存 破棄

**【選択されたプロファイル】**  
編集するオンデマンド検査用のプロファイルを選択します。  
**【プロファイルのリスト】**  
「編集」ボタンから、新たにオンデマンド検査用のプロファイルを作成することができます。

**【ブートセクタ/UEFI】**  
UEFIスキャナーは、HIPSの一部であり、コンピューターのUEFIを保護します。UEFIはブートプロセスの最初にメモリに読み込まれるファームウェアです。UEFIスキャナーにより、UEFIに感染しシステムを制御するマルウェアの検出が可能です。

# 3. 詳細設定について

## (6) アップデート

- アップデートでは、検出エンジンの取得先を変更することなどが可能です。アップデート先としてプライマリサーバー、セカンダリサーバーを設定することによってアップデート先の冗長化が可能です。

■ アップデート詳細設定画面

設定

検出エンジン

**アップデート**

プライマリサーバー  
セカンダリサーバー

ツール

基本

アップデートの種類

モジュールロールバック

モジュールのスナップショットを作成

ローカルに保存するスナップショットの数

プログラムのアップデート

**【モジュールロールバック】**  
検出エンジンのアップデートにより問題が起きた場合にロールバックすることができます。既定では、1つ分のスナップショットを保存します。

保存 破棄

■ プライマリサーバー設定画面

設定

検出エンジン

アップデート

**プライマリサーバー**

セカンダリサーバー

ツール

基本

自動選択

**アップデートサーバー**

ミラーサーバーからアップデート

ユーザー名

パスワード

任意のアップデートサーバーを設定可能です。  
 ・自動選択 : オフ  
 (オンの場合はESET社のサーバーからアップデートを行います)  
 ・アップデートサーバー : (例) http://1.1.1.1:2221

保存 破棄

# 3. 詳細設定について

## (7) ツール

- スケジューラ機能により、定期的なオンデマンド検査が可能です。オンデマンド検査に用いる検査プロファイルは、事前に作成した任意のプロファイルを使用することが可能です。また、検査の対象やウイルス検知時のアクションなども設定可能です。

### ■ ツール設定画面



### ■ タスク追加画面



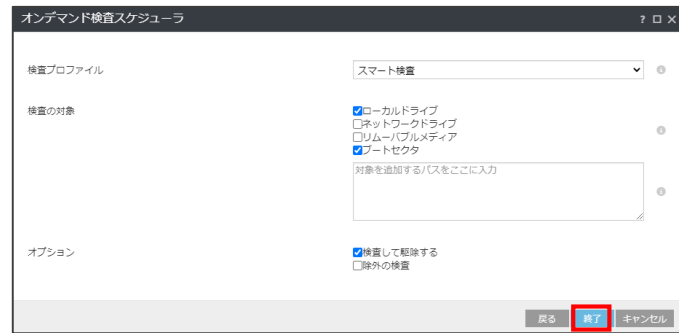
### ■ オンデマンド検査スケジューラ設定画面①



任意のタスク名と時刻を設定し、オンデマンド検査が自動的にトリガーされる曜日を選択します。

- ・ 任意の検査プロファイル
- ・ 検査の対象、
- ・ オプション(検査して駆除、検査除外)を選択して、「完了」ボタンをクリックします。

### ■ オンデマンド検査スケジューラ設定画面②



# 3. 詳細設定について

## (8) プロキシサーバ

- 検出エンジンのアップデートやESETのウイルス対策プログラムのアクティベーション（認証）をインターネット経由で行う場合、インターネットに接続する際にプロキシサーバを経由している環境では、プロキシサーバの設定を行う必要があります。

### ■ プロキシサーバ設定画面

プロキシサーバを使用する場合は、**【プロキシサーバを使用】**にチェックします。

プロキシサーバで認証が必要な場合は、**【プロキシサーバは認証が必要】**にチェックを付け、有効なユーザー名とパスワードを入力します。

# 3. 詳細設定について

## (9) Webインターフェース

- WebインターフェースではEFSL V7.2のインストール直後に自動生成されたWebインターフェースのログインパスワードから任意のパスワードに変更できます。また、WebインターフェースのSSL証明書の設定が可能です。

### ■ Webインターフェース設定画面

### ■ パスワード設定画面

【パスワードの設定】を選択し、新しいパスワードを入力して「OK」ボタンをクリックします。

# 3. 詳細設定について

## (10) ログファイル

- ログに記録する最低レベルやログローテーションの設定、Syslogにログを出力する場合はSyslogファシリティの設定が可能です。

### ■ ログファイル設定画面

設定 Q 入力すると検索を開始... ?

検出エンジン

アップデート

ツール

プロキシサーバ

Webインターフェイス

ログファイル

**基本**

ログに記録する最低レベル 情報レコード ▼

次の日数が経過したエントリを自動的に削除する  90

ログファイルを自動的に最適化する

使用されていないエントリの割合(%)が次の値よりも大きくなったら最適化 25

Syslogファシリティ デーモン

保存
破棄

- 【重大な警告】** : 重大なエラー(ウイルス対策の起動に失敗したなど)が含まれます。
- 【エラー】** : 「ファイルのダウンロード中にエラーが発生しました」といったエラーや重大な警告が記録されます。
- 【警告】** : 重大なエラーと警告メッセージとエラーが記録されます。
- 【情報レコード】** : アップデートの成功メッセージを含むすべての情報メッセージと上記のすべてのレコードが記録されます。
- 【診断レコード】** : プログラムおよび上記のすべてのレコードを微調整するのに必要な情報が含まれます。

## 3. 詳細設定について

### (参考) コマンドラインベースの操作

- EFSL V7.2では、ターミナルウィンドウからも以下の操作が可能です。各オプションの詳細については、以下のコマンド内の[OPTIONS]部分に「-h」を入力することで確認可能です。

- ・ **オンデマンド検査**

/opt/eset/efs/bin/odscan [OPTIONS]

- ・ **製品モジュールをアップデート**

/opt/eset/efs/bin/upd [OPTIONS]

- ・ **隔離された項目の管理**

/opt/eset/efs/bin/quar [OPTIONS]

- ・ **イベント画面の内容を表示**

/opt/eset/efs/bin/lolog [OPTIONS]

- ・ **設定のエクスポート**

/opt/eset/efs/sbin/cfg --export-xml=/tmp/export.xml

- ・ **設定のインポート**

/opt/eset/efs/sbin/cfg --import-xml=/tmp/export.xml

#### 【コマンド例】

- ・ ディレクトリ「/root/exc\_dir」を除外してオンデマンド検査を実行  
/opt/eset/efs/bin/odscan --scan --exclude=/root/exc\_dir

- ・ 任意のミラーサーバーからのアップデート  
/opt/eset/efs/bin/upd --update --server=192.168.1.2:2221

- ・ 隔離された項目を一覧表示  
/opt/eset/efs/bin/quar -l

- ・ すべてのイベントログを出力する  
/opt/eset/efs/bin/lolog -e





# EFSL V4.5との違い

**Canon**

キヤノンマーケティングジャパン株式会社

## 4. ESET File Security for Linux V4.5との違い

### (1) インストールについて

- EFSL V7.2ではインストールの際、OSのオンラインリポジトリに接続できる場合は、EFSL V7.2インストール時に不足パッケージを同時に導入する仕様になっています。
- すでにEFSL V4.5がインストールされている場合は、EFSL V4.5をアンインストール後にEFSL V7.2をインストールします。上書きインストールによるバージョンアップはできません。
- EFSL V7.2では以下のディストリビューションでSELinuxがサポートされています。SELinuxを有効にした状態でEFSL V7.2を使用するには、「selinux-policy-devel」パッケージをインストールする必要があります。
  - **Red Hat Enterprise Linux 6.X (64bit)**
  - **Red Hat Enterprise Linux 7.X (64bit)**
  - **Red Hat Enterprise Linux 8.X (64bit)**
  - **CentOS 6.X (64bit)**
  - **CentOS 7.X (64bit)**
  - **CentOS 8.X (64bit)**

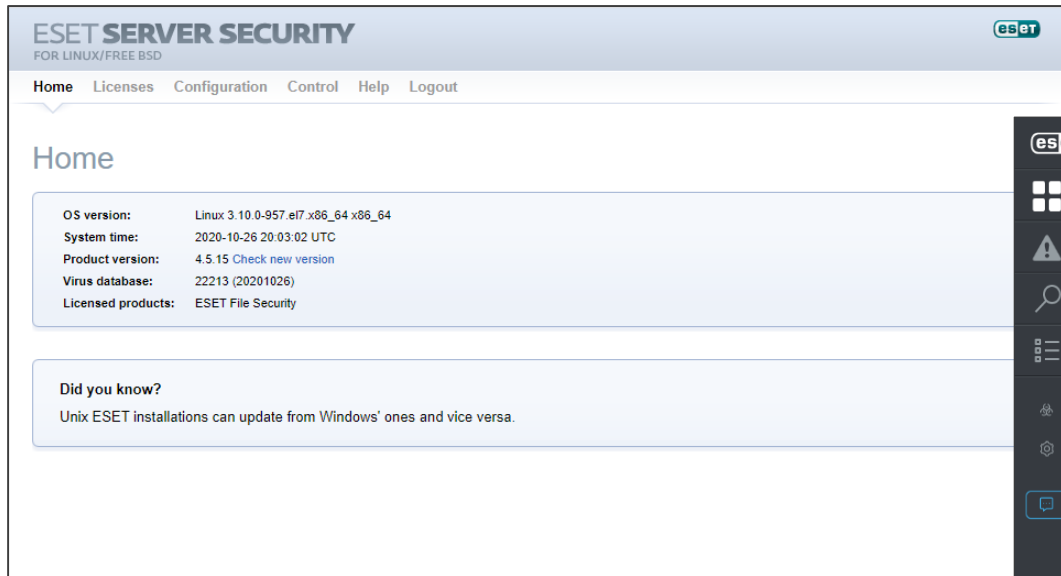
※インストールにはroot権限（スーパーユーザー）が必要です。

# 4. ESET File Security for Linux V4.5との違い

## (2) Webインターフェース

- EFSL V7.2 はEFSL V4.5と同様にWebブラウザを使用したWebインターフェースが利用可能です。EFSL V7.2のユーザーインターフェースは日本語対応しています。

### ■ EFSL V4.5のWebインターフェース



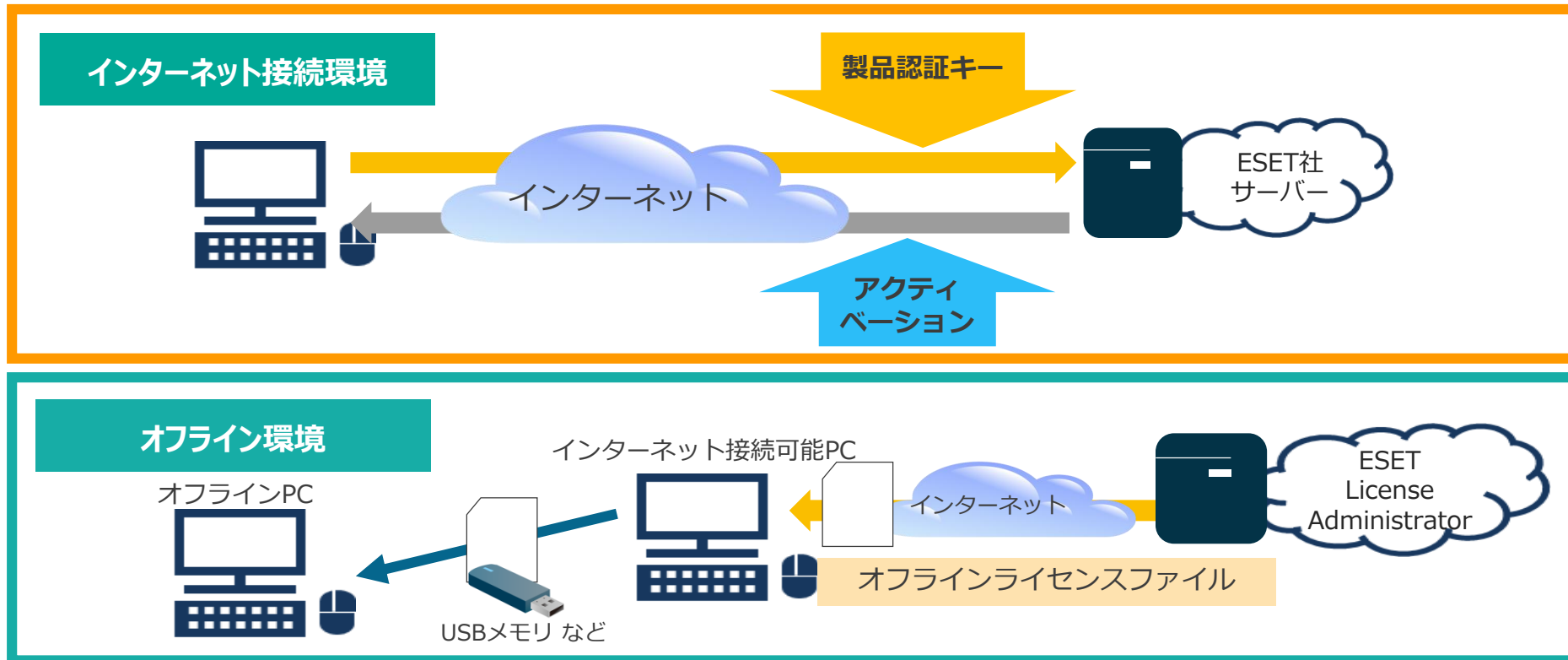
### ■ EFSL V7.2のWebインターフェース



# 4. ESET File Security for Linux V4.5との違い

## (3) アクティベーション①

- アクティベーションとは、製品を利用するために必要な認証作業です。ライセンスキーファイルを使用してプログラムを認証していたEFSL V4.5とは異なり、EFSL V7.2では**製品認証キー**または**オフラインライセンスファイル**を使用したアクティベーション（認証）作業が必要となります。



# 4. ESET File Security for Linux V4.5との違い

## (3) アクティベーション②

- Webインターフェースの「ダッシュボード」からアクティベーションが可能です。「ESET Endpoint Protection シリーズ」の管理用プログラムであるESMCでEFSL V7.2の管理を行っている場合は、ESMCからタスクを使用してアクティベーションを行うことが可能です。

### ■ アクティベーション前のアラート画面

ダッシュボード

ライセンス

▲ 製品がアクティベーションされていません

製品をアクティベーションするオプション:

製品認証キーでアクティベーション  
製品認証キーを使用してアクティベーションを行う (推奨)

オフラインライセンス  
クライアントがネットワークに接続していない場合は、オフラインライセンスファイルを使用します。

「製品認証キー」または「オフラインライセンスファイル」を使用しアクティベーションを行います。

※アクティベーションを行わないと、  
**検出エンジンのアップデートができない問題が発生してしまいます。**

### ■ アクティベーション完了後の画面

ダッシュボード

ライセンス

✓ ライセンスは有効です

ライセンスの有効期限: [redacted]  
パブリックID: [redacted]  
+ ライセンスを変更するオプションを表示

アクティベーションが完了すると、「ライセンスは有効です」と表示されます。



# EFSL V4.5との機能比較

**Canon**

キヤノンマーケティングジャパン株式会社

# 5. EFSL V4.5との機能比較

## 機能比較表①

| ウイルス・スパイウェア対策        |           |           |
|----------------------|-----------|-----------|
| 機能名                  | EFSL V4.5 | EFSL V7.2 |
| オンデマンド検査             | ○         | ○         |
| リアルタイム検査             | ○         | ○         |
| UEFIスキャナー            | ×         | ○         |
| 除外機能                 | ○         | ○         |
| 共有ローカルキャッシュ          | ×         | ○         |
| ESET LiveGrid        | ○         | ○         |
| 検出エンジンの更新およびミラーサーバ機能 |           |           |
| 機能名                  | EFSL V4.5 | EFSL V7.2 |
| 検出エンジンのアップデート        | ○         | ○         |
| 検出エンジンの遅延アップデート      | ○         | ○         |
| 検出エンジンのロールバック機能      | ×         | ○         |
| ミラーサーバ機能             | ○         | ○         |
| アップデート先の冗長化          | ×         | ○         |

# 5. EFSL V4.5との機能比較

## 機能比較表②

| 運用関連機能           |           |           |
|------------------|-----------|-----------|
| 機能名              | EFSL V4.5 | EFSL V7.2 |
| Syslogへの出力       | ○         | ○         |
| コマンドラインインターフェース  | ○         | ○         |
| 設定のインポート、エクスポート  | ○         | ○         |
| Webインターフェースでの設定  | ○         | ○         |
| ESMC V7.Xとの連携    | ○         | ○※        |
| EP V8.Xとの連携      | ×         | ○         |
| 統計表示（検出状況など）     | ○         | ○         |
| その他の機能           |           |           |
| 機能名              | EFSL V4.5 | EFSL V7.2 |
| リムーバブルメディアの検査    | ×         | ○         |
| スケジューラ機能         | ○         | ○         |
| アクティベーションの必要性の有無 | ×         | ○         |
| SELinuxのサポート     | ×         | ○         |

※EFSL V7.2はESMC V7.1以降でのみ管理可能です。