



ESET Server Security for Linux V8.1

機能紹介資料

第3版

2021年12月15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LinuxサーバーOS向けプログラム「ESET Server Security for Linux V8.1」の機能を紹介した資料です。

プログラム名	種別
ESET Server Security for Linux V8.1(略称表記：ESSL)	Linux サーバー用 ウイルス・スパイウェア対策プログラム

- ・ ESET File Security for Linuxから名称が変更になりました。(V7.2以下のプログラムはESET File Security for Linuxの名称のままです。)
- ・ 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あります。
- ・ 上記のプログラムはクラウド型セキュリティ管理ツールである**ESET PROTECT Cloud(略称表記：EPC)**、オンプレミス型セキュリティ管理ツールである **ESET PROTECT V8.X (略称表記：EP)** または **ESET Security Management Center V7.1 (略称表記：ESMC)** 以降で**管理が可能です**。EPC / EP / ESMCの機能紹介は、別資料でご用意しております。
- ・ EPC / EP / ESMCは、法人向けサーバー・クライアント用製品「ESET PROTECTソリューション」をご契約のお客さまのみ利用可能です。
- ・ 「ESET PROTECTソリューション」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 Server 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でご用意しています。

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. ESSLの仕様について
 - (1)インストールについて
 - (2)Webインターフェースについて
 - (3)アクティベーションについて
5. 旧バージョンとの機能比較



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 7.X (64bit) Red Hat Enterprise Linux 8.X (64bit) SUSE Linux Enterprise 12 SP1まで (64bit) SUSE Linux Enterprise 15 SP1まで (64bit) CentOS 7.X (64bit) CentOS 8.X (64bit) Amazon Linux 2	Red Hat Enterprise Linux (以降、RHEL) SUSE Linux Enterprise (以降、SUSE)
仮想環境	VMware ESX/ESXi 4.0/4.1 VMware ESX/ESXi 5.0以降 Citrix XenServer 5.6 Windows Server 2008 R2 Hyper-V Windows Server 2012 Hyper-V Windows Server 2012 R2 Hyper-V Windows Server 2016 Hyper-V 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 3.10.0-514 以降または kernel 4.18.0-80 以降のバージョンが導入されていること ・ AWS kernelの場合、kernel 4.14.231-173.361 以降のバージョンが導入されていること ・ glibc 2.17 以降のバージョンが導入されていること ・ elfutils-libelf-devel が導入されていること	・ libselinux (RHEL, CentOSのみ必要。最新パッケージをご利用ください) ・ selinux-policy-devel (SELinux有効で利用される場合) ・ elfutils-libelf-devel (RHEL8, CentOS8 のみ必要)
SecureBootへの対応	対応可能	Amazon Linux 2は非対応
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

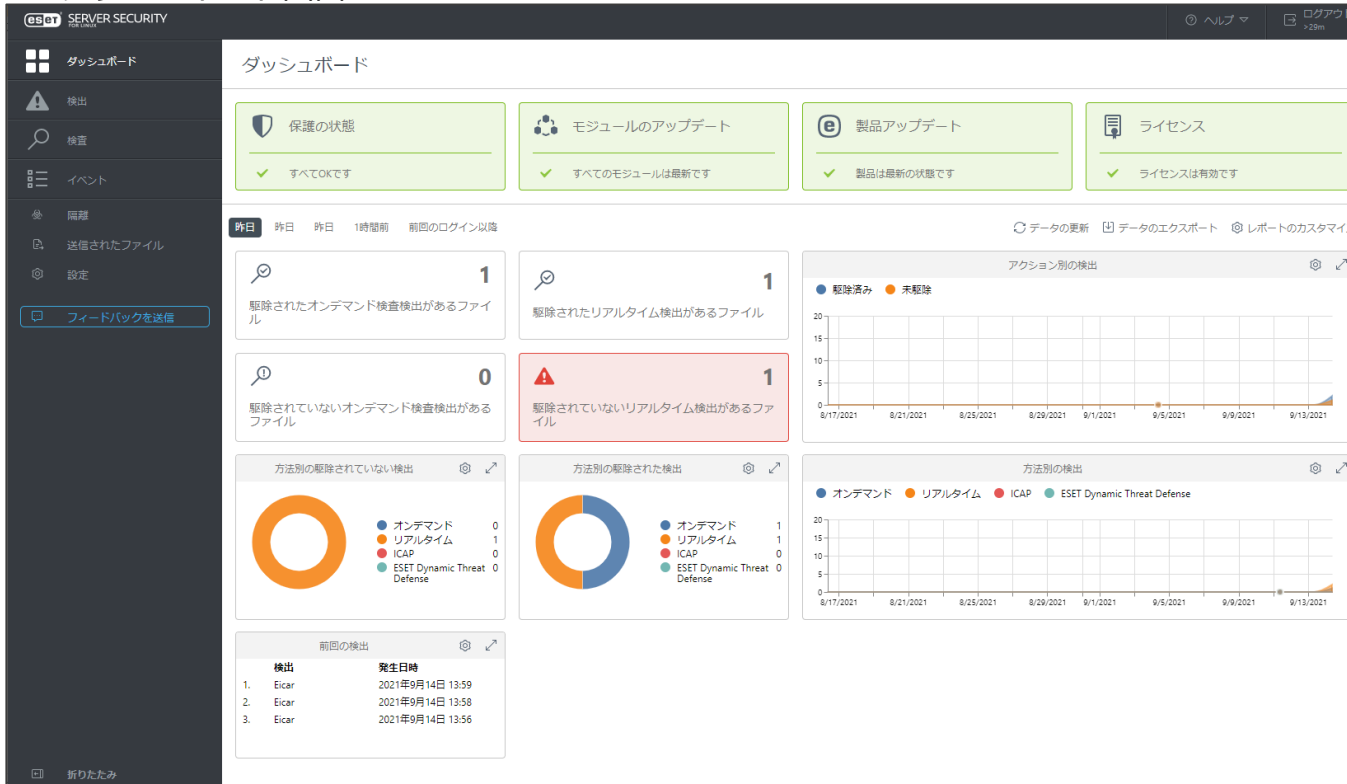
キヤノンマーケティングジャパン株式会社

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や検出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



■ 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、「再検査して駆除する」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	検出タイプ	アクション	ユーザー	アプリケーション	状況	ハッシュ
2021年9月14日 13:59	高	リアルタイムファ...	デストファイル	Cleaned by deleting	root	/usr/bin/scp	新規作成されたフ...	3395856CE811
2021年9月14日 13:56	中	リアルタイムファ...	デストファイル	Cleaned by deleting	root	/usr/bin/scp	新規作成されたフ...	3395856CE811

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						
2021年9月14日 13:58	Completed	3	1	1	0 秒	root
2021年8月19日 17:00	完了	261	0	0	6 秒	root
2021年8月19日 16:53	完了	2	0	0	0 秒	root
2021年8月19日 16:50	完了	2	0	0	0 秒	root

スケジュール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。

新規検査 ▼

- すべてのローカルドライブを検査
- カスタム検査...

■ 検査の詳細画面①

検査の詳細

概要 検出 検査済みファイルではありません

基本情報

開始時刻: 2021年9月14日 13:58
完了時刻: 2021年9月14日 13:58
時間: 0 秒

検査設定

検査したディスク、フ /tmp
オルダ、ファイル

オブジェクト

検出されました: 1
駆除済み: 1
未検査: 0
検査済み: 3

■ 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	ハッシュ
2021年9月14日 13:58	1	file:///tmp/eicar.com	Eicar	テストファイル	Cleaned by deleting	3395856CE81F2B7382DEE72602...

2. Webインターフェースについて

(4) イベント

- ESSL V8.1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ESSL V8.1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
2021年9月14日 13:27	更新サービス	検出エンジンが正常にバージョン23958 (20210914)にアップデートされました。	eset-efs-updated
2021年9月14日 13:26	ライセンスサービス	ESET Server Security: ライセンス3AA-NNJ-GF4を使用したアクティベーションが成功しました	eset-efs-licensed
2021年9月14日 13:23	検査サービス	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	eset-efs-scan
2021年9月14日 13:23	検査サービス	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	eset-efs-scan
2021年9月14日 13:23	ログサービス	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	eset-efs-logd
2021年9月10日 12:20	更新サービス	ウイルス対策モジュール更新エラー: 認証のアップデートが失敗しました。ライセンスが有効かどうかを確認してください。	eset-efs-updated
2021年9月10日 12:20	更新サービス	ウイルス対策モジュール更新エラー: 認証のアップデートが失敗しました。ライセンスが有効かどうかを確認してください。	eset-efs-updated
2021年8月31日 13:29	更新サービス	検出エンジンが正常にバージョン23882 (20210831)にアップデートされました。	eset-efs-updated
2021年8月25日 11:00	更新サービス	検出エンジンが正常にバージョン23875 (20210829)にアップデートされました。	eset-efs-updated
2021年8月25日 10:00	更新サービス	検出エンジンが正常にバージョン23849 (20210824)にアップデートされました。	eset-efs-updated
2021年8月19日 20:23	更新サービス	検出エンジンが正常にバージョン23824 (20210820)にアップデートされました。	eset-efs-updated
2021年8月19日 17:23	更新サービス	検出エンジンが正常にバージョン23823 (20210819)にアップデートされました。	eset-efs-updated
2021年8月19日 13:23	更新サービス	検出エンジンが正常にバージョン23818 (20210819)にアップデートされました。	eset-efs-updated
2021年8月19日 08:23	更新サービス	検出エンジンが正常にバージョン23817 (20210818)にアップデートされました。	eset-efs-updated
2021年8月19日 04:23	更新サービス	検出エンジンが正常にバージョン23816 (20210818)にアップデートされました。	eset-efs-updated
2021年8月19日 03:23	ログサービス	ログ連携および最適化が完了しました	eset-efs-logd
2021年8月19日 03:23	ログサービス	ログ連携および最適化が開始しました	eset-efs-logd
2021年8月19日 00:23	更新サービス	検出エンジンが正常にバージョン23815 (20210818)にアップデートされました。	eset-efs-updated
2021年8月18日 21:23	更新サービス	検出エンジンが正常にバージョン23814 (20210818)にアップデートされました。	eset-efs-updated
2021年8月18日 18:23	更新サービス	検出エンジンが正常にバージョン23813 (20210818)にアップデートされました。	eset-efs-updated
2021年8月18日 13:23	更新サービス	検出エンジンが正常にバージョン23812 (20210818)にアップデートされました。	eset-efs-updated

2. Webインターフェースについて

(5) 隔離

- ESSL V8.1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



時刻	名前	検出	検出タイプ	原因	サイズ	数	ハッシュ
2021年3月26日 18:11	/root/ei		テストファイル		68 B	2	3395856CE81F287382DEE72602F798B642F141...

隔離画面の機能説明:

- 【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
- 【ハッシュのコピー】: ファイルのSHA-1ハッシュをクリップボードにコピーします
- 【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
- 【分析のために提出】: 分析のために隔離された項目のコピーをESETに送信します

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、ユーザーインターフェース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、通常の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。

【ユーザーインターフェース】

ESSL V8.1の保護状態に関する通知を、ダッシュボードに表示させるかどうかの設定を行うことが可能です。





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 in ESET. On the left, a sidebar lists various security features, with 'Detection Engine' highlighted. The main area is divided into sections: 'Basic' (expanded), 'Exclusions', and 'Shared Local Cache'. Under 'Basic', there are three checkboxes for detecting applications with different levels of risk, all of which are checked. Three callout boxes provide detailed explanations for these categories:

- 「望ましくない可能性があるアプリケーション」**
アドウェアやツールバーをインストールするようなコンピューターのパフォーマンスに悪影響を与えるようなアプリケーションを検出します。
- 「安全ではない可能性があるアプリケーション」**
リモートアクセスツールやパスワード解析ツールなど適正なアプリケーションではあるものの悪用される可能性もあるアプリケーションを検出します。
- 「疑わしい可能性があるアプリケーション」**
zipなどの圧縮形式、プロテクタで圧縮されたプログラムが含まれます。マルウェアの作成者が検知を逃れるためによく使用する方法です。

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

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
ユーザーインターフェース

基本

スキャノプション

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

「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」

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。

■ パフォーマンス除外設定画面

除外の追加

パス

コメント

OK キャンセル

■ 検出除外設定画面

除外の追加

パス

ハッシュ

検出名

コメント

OK キャンセル

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

※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

The screenshot shows the 'Malware Inspection' settings window. On the left is a sidebar with navigation links: '検出エンジン' (Detection Engine), 'リアルタイムファイルシステム保護' (Real-time File System Protection), 'クラウドベース保護' (Cloud-based Protection), 'マルウェア検査' (Malware Inspection - highlighted with a red box), and 'リモート検査' (Remote Inspection). Below these are 'アップデート' (Updates), 'ツール' (Tools), and 'ユーザーインターフェース' (User Interface). The main area is titled '設定' (Settings) and contains several sections: 'オンデマンド検査' (On-demand Inspection) with a red box around '選択されたプロファイル' (Selected profile) set to 'スマート検査' (Smart Scan) and a '編集' (Edit) button; 'スマート検査' (Smart Scan); 'THREATSENSE/パラメータ' (THREATSENSE/Parameters) with a red box around '検査するオブジェクト' (Objects to inspect) where 'ブートセクタ/UEFI' (Boot sector/UEFI) is checked; '検査オプション' (Inspection options) with checkboxes for 'ヒューリスティック' (Heuristic) and 'アドバンスドヒューリスティック/DNA署名' (Advanced heuristic/DNA signature); '駆除' (Removal) with a dropdown set to '厳密な駆除' (Thorough removal); and '除外' (Exclusions) with a '編集' (Edit) button. Two callout boxes provide additional information: the top one explains the 'Selected profile' and the 'Edit' button; the bottom one explains the 'Boot sector/UEFI' option.

【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

【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。

【製品アップデート】
プログラムコンポーネントアップデート(PCU)を使用して、自動で最新バージョンへバージョンアップすることができます。
※ バージョンアップ先のプログラムによっては、手動でのバージョンアップが必要な場合があります。

■ プライマリサーバー設定画面

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://192.168.1.1:2221

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

設定

検索エンジン

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

ユーザーインターフェイス

保存 破棄

スケジュール

タスク **編集**

■ タスク追加画面

タスク

有効	名前	トリガー	タスク
----	----	------	-----

追加 編集 削除

保存 キャンセル

■ オンデマンド検査スケジューラ設定画面①

オンデマンド検査スケジューラ

名前

定期的な検査

日時

10:00

次の間隔で繰り返し

☐ 月曜日

☐ 火曜日

☐ 水曜日

☐ 木曜日

☒ 金曜日

☒ 土曜日

☐ 日曜日

コンピュータがオフの場合、コンピュータがオンになる次のスケジュールされた時刻にタスクが実行されます。

次へ キャンセル

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

オンデマンド検査スケジューラ

検査プロファイル

スマート検査

検査の対象

☒ ローカルドライブ

☐ ネットワークドライブ

☐ リムーバブルメディア

☒ ブートセクタ

対象を追加する/バスをここに入力

オプション

☒ 検査して駆除する

☐ 除外の検査

戻る **完了** キャンセル

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

設定

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

ユーザーインターフェース

基本

プロキシサーバを使用 ☒

プロキシサーバ

ポート 3128

プロキシサーバは認証が必要 ☒

ユーザー名

パスワード

パスワードの表示

HTTPプロキシが使用できない場合は直接接続を使用する ☒

保存 破棄

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ESSL 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

設定

検索エンジン

アップデート

ツール

プロキシサーバ

Webインターフェース

ログファイル

ユーザーインターフェース

基本

Webインターフェースを有効にする ☒

リスニングアドレスとポート 編集

パスワードの設定 設定

証明書 1 kB 上 ×

秘密鍵 2 kB 上 ×

証明書パスワード

パスワードの表示

保存 破棄

■ パスワード設定画面

パスワードの設定

新しいパスワード

パスワードの表示

新しいパスワードの確認

パスワードの表示

OK キャンセル

【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

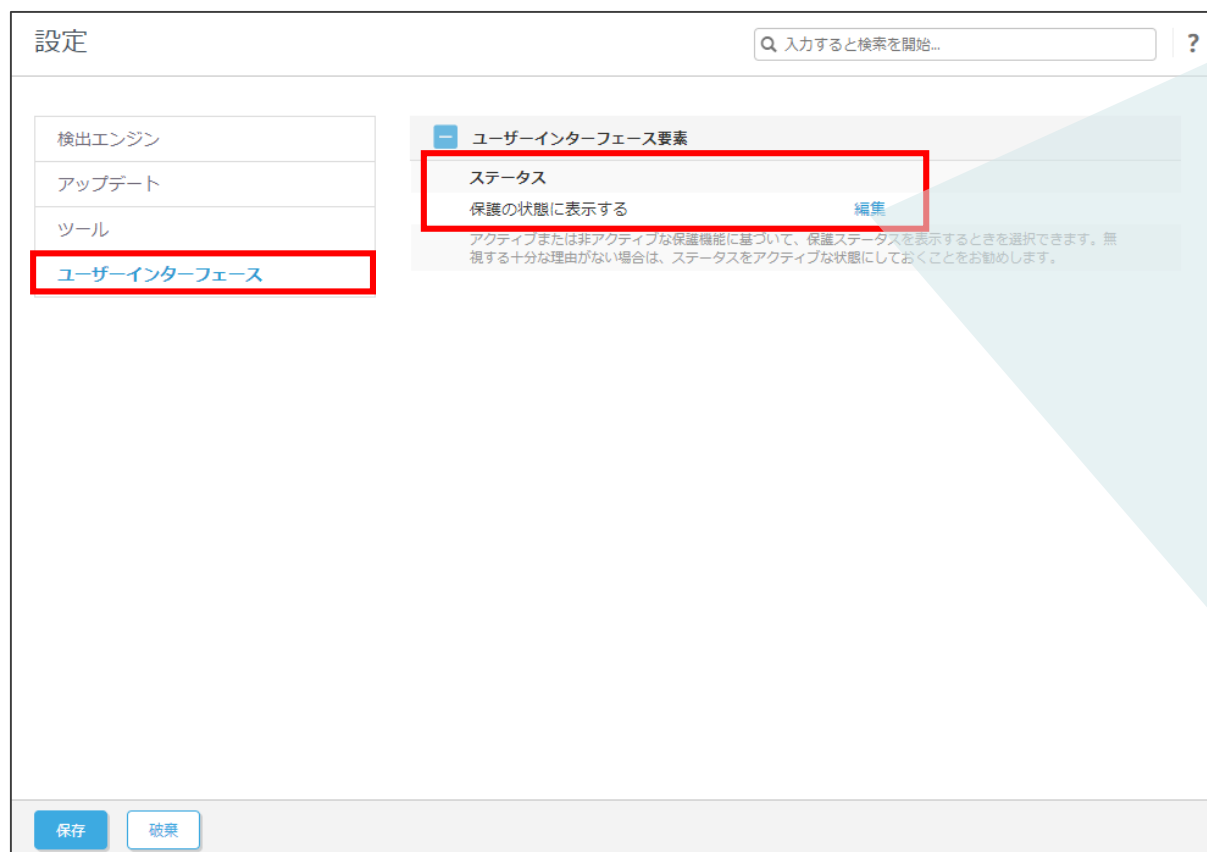
- 【重大な警告】** : 重大なエラー(ウイルス対策の起動に失敗したなど)が含まれます。
- 【エラー】** : 「ファイルのダウンロード中にエラーが発生しました」といったエラーや重大な警告が記録されます。
- 【警告】** : 重大なエラーと警告メッセージとエラーが記録されます。
- 【情報レコード】** : アップデートの成功メッセージを含むすべての情報メッセージと上記のすべてのレコードが記録されます。
- 【診断レコード】** : プログラムおよび上記のすべてのレコードを微調整するのに必要な情報が含まれます。

3. 詳細設定について

(11) ユーザーインターフェース

- ESSL V8.1の保護状態に関する通知を、ダッシュボードに表示させるかどうかの設定を行うことが可能です。

■ ユーザーインターフェース要素画面



設定

検索エンジン
アップデート
ツール
ユーザーインターフェース

ユーザーインターフェース要素

ステータス
保護の状態に表示する [編集](#)

アクティブまたは非アクティブな保護機能に基づいて、保護ステータスを表示する時を選択できます。無視する十分な理由がない場合は、ステータスをアクティブな状態にしておくことをお勧めします。

保存 破棄

■ ステータス設定画面



ステータス

保護の状態に表示するステータスを選択:

ステータス

- ☒ ESET LiveGrid®レピュテーションシステムが無効です
- ☒ ESET LiveGrid®フィードバックシステムが無効です
- ☒ 望ましくない可能性があるアプリケーションの検出が無効です
- ☒ リアルタイムファイルシステム保護が無効です
- ☒ リアルタイムファイルシステム保護は機能していません
- ☒ リモート検査ICAPが無効です
- ☒ SELinuxが有効ですが、サポートするには、「selinux-policy-devel」パッケージも必要です。インストールして、製品を再起動してください。

OK キャンセル

3. 詳細設定について

(参考)コマンドラインベースの操作

- ESSL V8.1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



ESSLの仕様について

Canon

キヤノンマーケティングジャパン株式会社

4. ESSLの仕様について

(1)インストールについて

- ESSL V8.1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ESSL V8.1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からの上書きインストールによるバージョンアップは可能です。
- ESSL V8.1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ESSL V8.1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 7.X (64bit)**
 - **Red Hat Enterprise Linux 8.X (64bit)**
 - **CentOS 7.X (64bit)**
 - **CentOS 8.X (64bit)**
- ELREPOカーネルを使用したLinuxディストリビューションはサポートされておられません。

※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. ESSLの仕様について

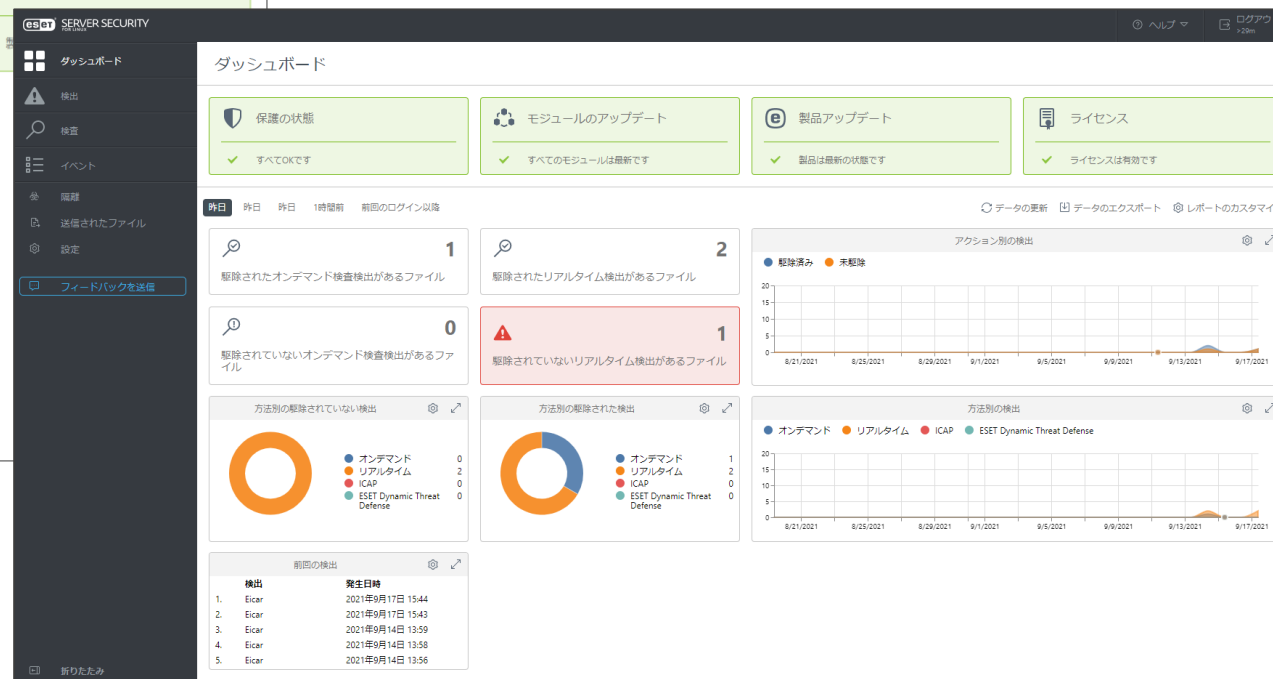
(2)ダッシュボードについて

- ESSL V8.1のダッシュボードはEFSL V7.2と比較して、脅威の検出情報が表示できるようになりました。

■ EFSL V7.2のダッシュボード



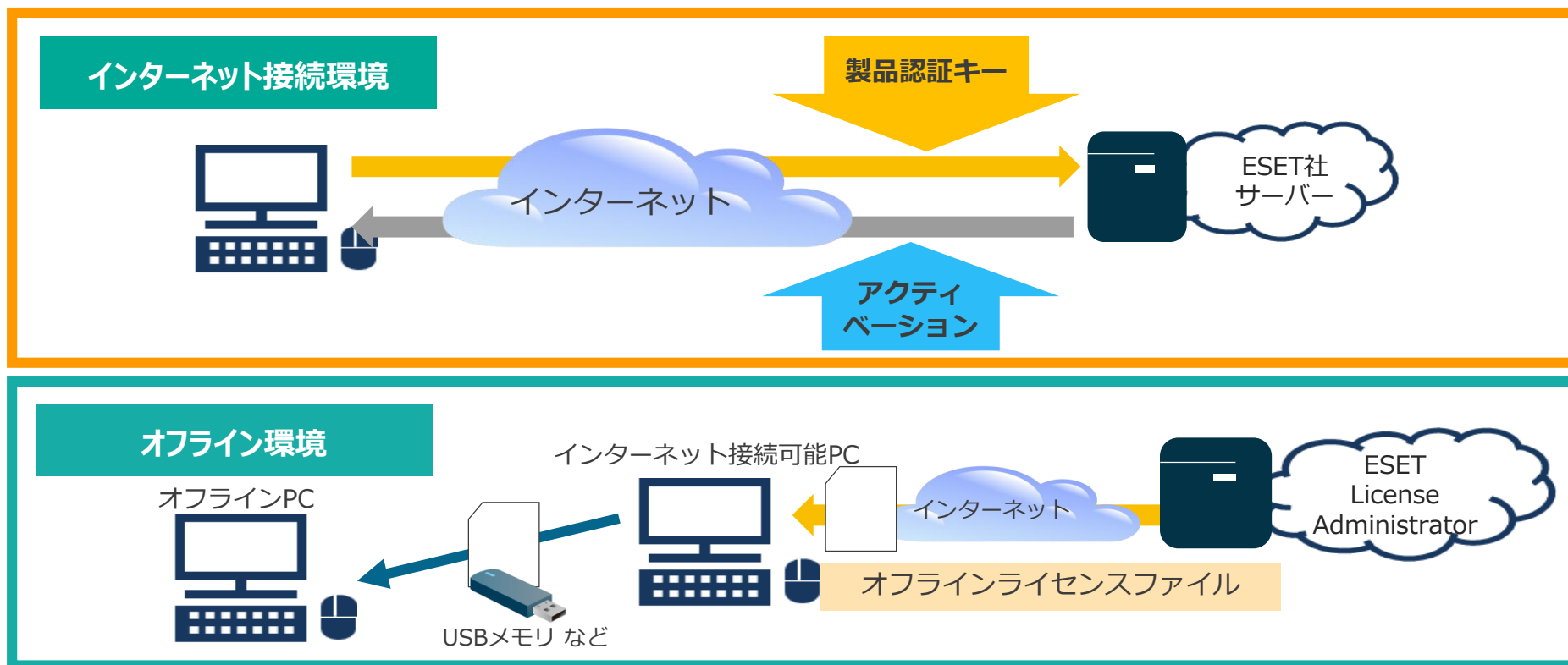
■ ESSL V8.1のダッシュボード



4. ESSLの仕様について

(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。ESSL V8.1インストール後に**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. ESSLの仕様について

(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EPCやEP、ESMCなどのセキュリティ管理ツールでESSL V8.1の管理を行っている場合は、セキュリティ管理ツールの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



「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完了後の画面



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。

※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ません。



旧バージョンとの機能比較

Canon

キヤノンマーケティングジャパン株式会社

5. 旧バージョンとの機能比較

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	ESSL V8.1
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	ESSL V8.1
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. 旧バージョンとの機能比較

機能比較表②

運用関連機能			
機能名	EFSL V4.5	EFSL V7.2	ESSL V8.1
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	○	○	○
ダッシュボードのステータス表示設定	×	×	○
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	ESSL V8.1
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	×	○	○

※ESMC V7.1以降でのみ管理可能です。