

ESET Server Security for Linux V12.X

機能紹介資料

第1版

2025年10月7日



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 V12.X」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 V12.X(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。
- 本資料で使用している画面イメージはESET Server Security for Linux V12.0で取得しております。使用するOSやバージョン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。
- 「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。

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

サポート環境

1. サポート環境

項目	条件	備考
OS	Red Hat Enterprise Linux 8.X (64bit) ※1 Red Hat Enterprise Linux 9.X (64bit) ※1 Red Hat Enterprise Linux 10.X (64bit) ※1 ※4 SUSE Linux Enterprise 15 (64bit) ※2 Amazon Linux 2023 ※3 Alma Linux 8 ※4 Alma Linux 9 ※5 Alma Linux 10 ※4 Rocky Linux 8 ※5 Rocky Linux 9 ※5 Rocky Linux 10 ※4 Ubuntu Server 20.04LTS Ubuntu Server 22.04LTS ※6 Ubuntu Server 24.04LTS ※7 Debian 11 Debian 12 ※5 Oracle Linux 8 Oracle Linux 9 ※4	※1 Red Hat Enterprise Linux (以降、RHEL) ※2 SUSE Linux Enterprise (以降、SUSE) ※3 ESET Management エージェント V11.2 以降で管理可能 ※4 セキュリティ管理ツールでの管理は未サポート ※5 セキュリティ管理ツール V10.1以降で管理 可能 ※6 カーネル モジュールのコンパイルにgcc-12 が必要 ※7 ESET Management エージェント V11.0 以降で管理可能
CPU	Intel,AMD(64bit)	
メモリ	2GB	
ハードディスク	700MB以上	
必要パッケージ	OSによって必要なパッケージは異なります。下記よりご参照ください。 ▼オンラインヘルプ補足資料 https://eset-info.canon-its.jp/files/user/pdf/manual/v120_users_manual_essl.pdf	
SecureBootへの対応	対応可能 ※8	※8 Oracle Linuxはストックカーネルのみ
その他	en_US.UTF-8エンコーディングを使用する任意のロケール	

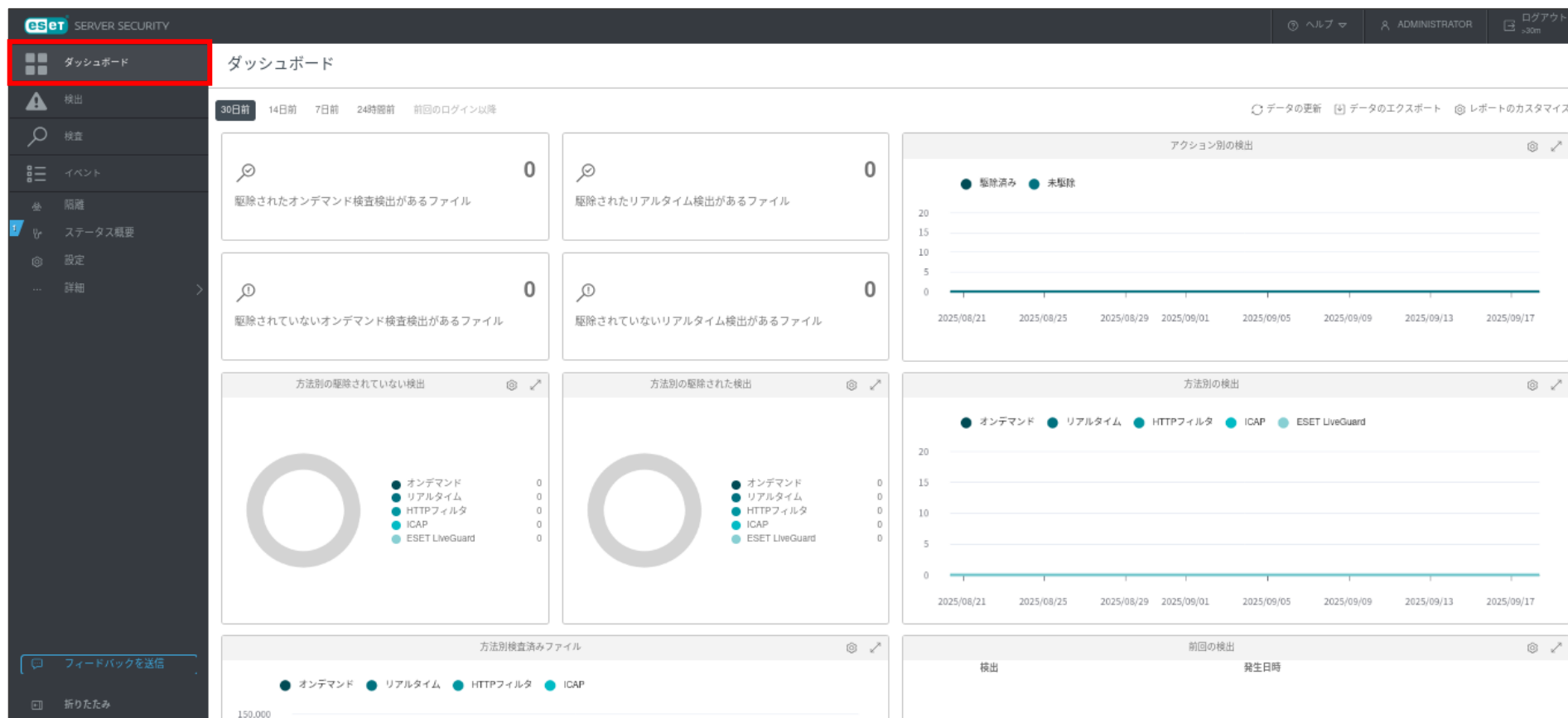
Webインターフェースについて

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。

■ダッシュボード画面



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	オブジェクト	検出タイプ	アクション	ユーザー	アプリケーション	状況
☒	2025/09/18 15:06	!	リアルタイム	file:///hor...	テストファ...	削除によって駆除...	test	/usr/bin/gedit	新規作
☐	2025/09/18 15:04	!	HTTPフィ...	https://se...	テストファ...	接続が切断されま...	test	/usr/lib64/fi...	Webに

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						
2023/11/22 09:53	完了	45,971	1	1	14 秒	root
2023/11/22 09:48	完了	4	0	0	0 秒	root
2023/11/22 09:46	完了	47,493	0	0	21 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。

■ 検査の詳細画面①

基本情報

開始時刻: 2023/08/03 14:49
完了時刻: 2023/08/03 14:49
時間: 20 秒

検査設定

検査対象: 2

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: 48,786

■ 検査の詳細画面②

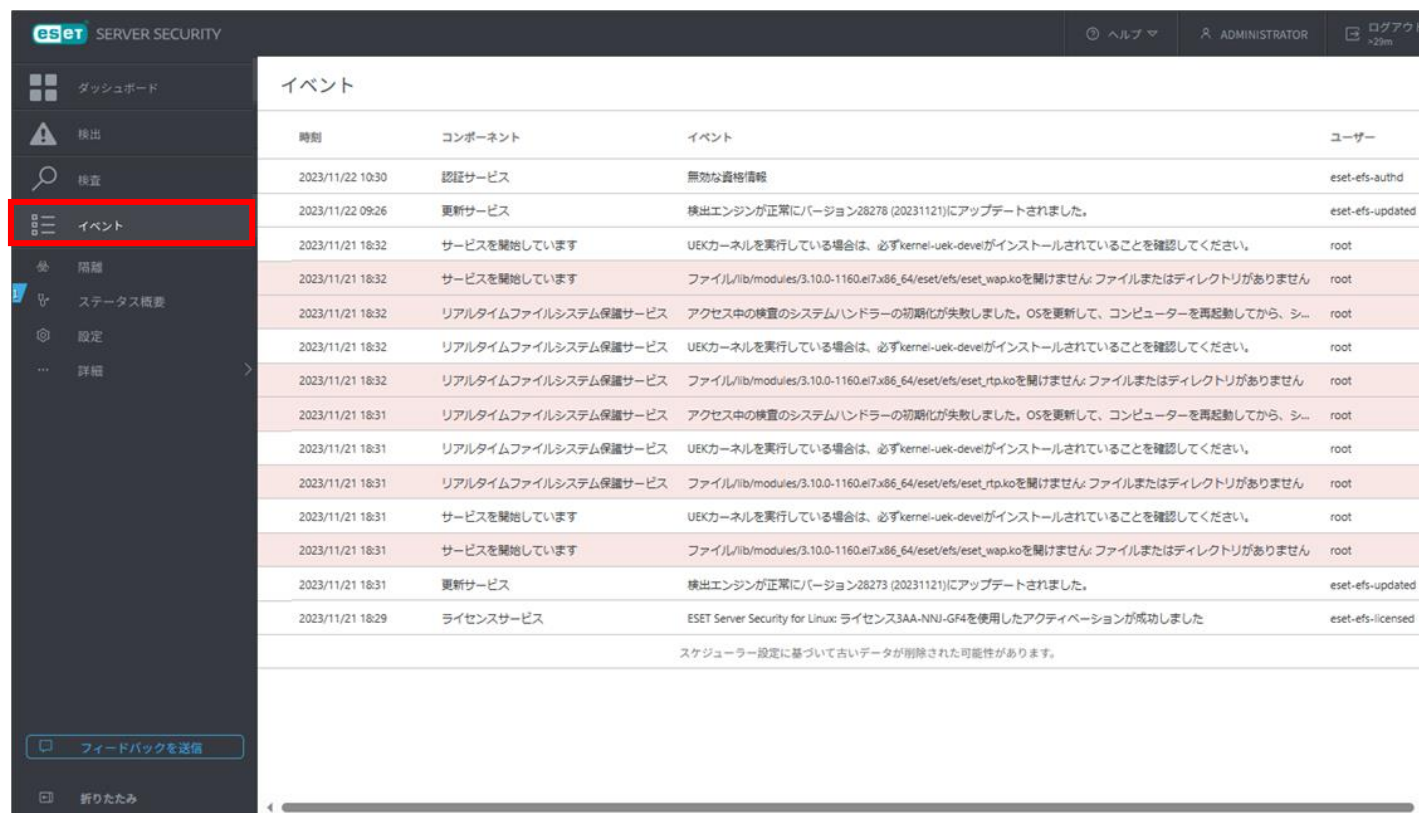
検出された時刻	重大度	オブジェクトURI	検出	検出タイプ	アクション	ハッシュ
2023/08/03 14:49	1	file:///root/.icar.com	Eicar	テストファイル	削除によって駆除されました	3395856CE81F287382DEE72602F798B6...

2. Webインターフェースについて

(4) イベント

- ESSL V12.X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 V12.X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
2023/11/22 10:30	認証サービス	無効な資格情報	eset-efs-authd
2023/11/22 09:26	更新サービス	検出エンジンが正常にバージョン28278 (20231121)にアップデートされました。	eset-efs-updated
2023/11/21 18:32	サービスを開始しています	UEKカーネルを実行している場合は、必ずkernel-uek-develがインストールされていることを確認してください。	root
2023/11/21 18:32	サービスを開始しています	ファイル/lib/modules/3.10.0-1160.el7.x86_64/efi/efi_wap.koを開けません。ファイルまたはディレクトリがありません	root
2023/11/21 18:32	リアルタイムファイルシステム保護サービス	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、コンピュータを再起動してから、シ...	root
2023/11/21 18:32	リアルタイムファイルシステム保護サービス	UEKカーネルを実行している場合は、必ずkernel-uek-develがインストールされていることを確認してください。	root
2023/11/21 18:32	リアルタイムファイルシステム保護サービス	ファイル/lib/modules/3.10.0-1160.el7.x86_64/efi/efi_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せん	root
2023/11/21 18:31	リアルタイムファイルシステム保護サービス	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、コンピュータを再起動してから、シ...	root
2023/11/21 18:31	リアルタイムファイルシステム保護サービス	UEKカーネルを実行している場合は、必ずkernel-uek-develがインストールされていることを確認してください。	root
2023/11/21 18:31	リアルタイムファイルシステム保護サービス	ファイル/lib/modules/3.10.0-1160.el7.x86_64/efi/efi_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せん	root
2023/11/21 18:31	サービスを開始しています	UEKカーネルを実行している場合は、必ずkernel-uek-develがインストールされていることを確認してください。	root
2023/11/21 18:31	サービスを開始しています	ファイル/lib/modules/3.10.0-1160.el7.x86_64/efi/efi_wap.koを開けません。ファイルまたはディレクトリがありません	root
2023/11/21 18:31	更新サービス	検出エンジンが正常にバージョン28273 (20231121)にアップデートされました。	eset-efs-updated
2023/11/21 18:29	ライセンスサービス	ESET Server Security for Linux: 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
		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

(5) 隔離

- ESSL V12.X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

隔離画面のスクリーンショット。左側のナビゲーションメニューには「ダッシュボード」、「検出」、「検査」、「イベント」、「隔離」、「ステータス概要」、「設定」、「詳細」があります。「隔離」が選択されています。中央の「隔離」タブには、隔離されたファイルのリストが表示されています。

時刻	検出	検出タイプ	原因	サイズ	数	ハッシュ	除外可能
2023/11/22 09:53	Eicar	テストファイル		68 B	3	3395856CE81F287382DEE7...	いいえ

右側のコンテキストメニューには以下のアクションがあります：

- 復元と除外
- 復元
- パスのコピー
- ハッシュのコピー
- ↓ ダウンロード
- 🗑️ 隔離から削除
- 📤 分析のために提出

【復元 と 除外】：隔離された検体を復元し、再度検出されないように除外します

【復元】：隔離された項目を元の場所に復元します(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】：隔離された検体のコピーをESETに送信します。提出された検体は分析のために活用いたします。

※「分析のために提出」は「ESET LiveGrid®フィードバックシステム」が有効になっている場合にのみ表示されます。参照：本資料P19

2. Webインターフェースについて

(6)ステータス概要

- 保護状況やアップデート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。

■ステータス概要画面

The screenshot displays the ESET Server Security Web Interface. The sidebar on the left contains navigation links: ダッシュボード (Dashboard), 検出 (Detection), 検索 (Search), イベント (Events), 隔離 (Isolation), **ステータス概要** (Status Overview - highlighted with a red box), 設定 (Settings), and 詳細 (Details). The main content area is titled 'ステータス概要' (Status Overview) and features several status cards:

- モジュールのアップデート** (Module Updates): すべてのモジュールは最新です (All modules are up to date).
- 製品アップデート** (Product Updates): 製品は最新の状態です (Product is up to date).
- ライセンス** (Licenses): ライセンスは有効です (License is valid).
- リアルタイム検査** (Real-time Check): 現在の状況: 実行中 (Current status: Running), 検査サービス: 実行中 (Check service: Running) - highlighted with a red box.
- オンデマンド検査** (On-demand Check): 検査サービス: 実行中 (Check service: Running) - highlighted with a red box.
- Webアクセス保護** (Web Access Protection): 現在の状況: 実行中 (Current status: Running), 検査サービス: 実行中 (Check service: Running).

At the bottom right, a section titled 'その他の機能' (Other features) lists additional capabilities: ESET LiveGrid®レビューエンジン (ESET LiveGrid® Review engine), ESET LiveGrid®フィードバック (ESET LiveGrid® Feedback), 望ましくない可能性があるアプリケーションの検出: 無効 (Detection of applications with potential undesired behavior: Disabled), リモート検査 - ICAP: 無効 (Remote check - ICAP: Disabled), and ウォッチドッグ: 有効 (Watchdog: Enabled). Two callout boxes point to the 'リアルタイム検査' and 'オンデマンド検査' sections, stating: 'ウォッチドック機能により、ステータスを確認できます。' (Thanks to the watchdog function, you can check the status.)

2. Webインターフェースについて

(7)ブロックされたファイル

- ESET Inspectと連携され、ESET Inspectからブロックされたファイルを確認できます。

■ブロックされたファイル画面

ブロックされたファイル

時刻	ファイル	ソース	原因	アクション	アプリケーション	ユーザー	ハッシュ	最初の表示時刻
i ブロックされたファイルなし は、ブロックされたファイルのリストが表示されます。ファイルが								

ESET Inspect連携され、ESET Inspectからブロックされたファイルがこちらに記録されます。

2. Webインターフェースについて

(8)フィルタリングされたWebサイト

- フィルタリングされたWebサイトを確認できます。

■ フィルタリングされたWebサイト画面

eset SERVER SECURITY ヘルプ ADMINISTRATOR ログアウト >29m

詳細ログ
送信されたファイル
ブロックされたファイル
フィルタリングされたWebサイト
ネットワーク保護

フィルタリングされたWebサイト

時刻	オブジェクトURI	原因	アプリケーション	ユーザー	IPアドレス	アクション	重大度
----	-----------	----	----------	------	--------	-------	-----

i
フィルタリングされたWebサイトはありません

ここには、Webアクセス保護によってフィルタリングされたWebサイトのリストが表示されます。Webサイトがフィルタリングされていないか、ログファイルの設定に基づいてデータが削除されたため、現在データが表示

フィルタリングされたWebサイトがこちらに記録されます。

CLOSE アクション ▾

2. Webインターフェースについて

(9) ネットワーク保護

- ボットネット保護に関するログが表示され、確認できます。

■ ネットワーク保護画面

eset SERVER SECURITY

ヘルプ ADMINISTRATOR ログアウト >30m

詳細ログ
送信されたファイル
ブロックされたファイル
フィルタリングされたWebサイト
ネットワーク保護

ネットワーク保護

時刻	イベント	アクション	ソース	ターゲット	プロトコル	方向	ルール/脅威名	アプリケーシ...	ハッシュ	ユーザー
----	------	-------	-----	-------	-------	----	---------	-----------	------	------

i
ブロックされたネットワーク通信はありません

ここには、ネットワークアクセス保護によってブロックされるネットワークアクティビティの一覧が表示されます。ネットワークアクセス保護に

ボットネット保護に関するログがこちらに記録されます。

CLOSE

2. Webインターフェースについて

(10)設定

- 検出エンジン、アップデート、保護、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一時的に設定変更(有効/無効)をすることが可能です。

■ 設定画面

【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。

【検出エンジン】
検出エンジンの項目では、特定のファイルやフォルダをウイルス検査の対象からの除外、クラウドベース保護機能、各検査の詳細設定が可能です。

【保護】
保護の項目では、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各保護機能の詳細設定が可能です。

【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】
保護状態に関する通知を、ステータス概要に表示させるかどうかの設定を行うことが可能です。

2. Webインターフェースについて

(11)GUIパスワード変更

- ESSL V12.X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は、任意のパスワードに変更することができます。

■ GUIパスワード変更画面

クリックするとプロファイル画面が表示されます。

■ パスワード設定画面

パスワード変更

パスワード

新しいパスワード

パスワードの確認

最小文字数:14
小文字1文字
大文字1文字
1つの数字
1文字の特殊文字

保存 キャンセル

「パスワード変更」をクリックし、新しいパスワードを入力して「保存」ボタンをクリックします。

詳細設定について

3. 詳細設定について

(1) 検出エンジン — 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。

■ 検出除外設定画面



「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については検出から除外します。

3. 詳細設定について

(2) 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

The screenshot shows the ESET settings window with the 'Cloud-based Protection' (クラウドベース保護) section selected. The 'ESET LIVEGRID®' section is expanded, showing options to participate in the reputation system and feedback system, both of which are enabled. The 'Sample Submission' (サンプルの送信) section is also expanded, showing options for automatic submission of detected samples and suspicious samples. The 'ESET LIVEGUARD' section is also expanded, showing options for detection threshold, action after detection, and automatic submission of suspicious samples. The 'Detection threshold' (検出しきい値) is set to 'Very Suspicious' (非常に不審). The 'Action after detection' (検出後のアクション) is set to 'Stop execution and remove' (実行中の処理を停止して駆除). The 'Automatic submission of suspicious samples' (不審なサンプルの自動送信) is enabled, and the 'ESET server to delete files from' (ESETのサーバーから文書を削除) is set to '30 days later' (30日後).

【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。

【ESET LiveGrid®レピュテーションシステムに参加する】
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。

【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。

「ESET LiveGuard を有効にする」
※ESET LiveGuard Advancedのアクティベーションが行われている場合のみこちらの項目が表示されます。サンプルの送信内容及び、分析で脅威と検出された場合の動作を指定できます。

3. 詳細設定について

(3)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

【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

(4)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
保護
ツール
ユーザーインターフェース

基本
アップデートの種類

【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。

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 1

製品アップデート
自動アップデート ☒
更新タイミング 段階的な更新のロールアウト
ESETによってタイミングが決定される安定性のための段階的なアップデートを選択するか、リリース直後にインストールされる即時アップデートを選択して、迅速な展開を実現します。 [自動アップデートの詳細](#)
カスタムサーバー 自動選択
ユーザー名
パスワード

【製品アップデート】
自動アップデート機能を使用して、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

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
保護
ツール
ユーザーインターフェース

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://192.168.1.1:2221

3. 詳細設定について

(5)保護

- 保護の項目では、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 window. On the left, a sidebar lists 'Detection Engine', 'Updates', 'Protection' (highlighted with a red box), 'Real-time file system protection', 'Web access protection', 'Network access protection', 'Tools', and 'User interface'. The main area is titled 'Detection response' and contains three sections, each with 'Report' and 'Protect' options:

- 望ましくない可能性があるアプリケーション** (Applications with a possibility of being undesirable): This section is highlighted with a red box. A callout explains that it detects applications like adware or toolbars that negatively impact computer performance.
- 疑わしい可能性があるアプリケーション** (Applications with a suspicious possibility): This section is highlighted with a red box. A callout explains that it detects applications like zip files or programs compressed with protectors, which malware creators use to evade detection.
- 安全ではない可能性があるアプリケーション** (Applications with a possibility of being unsafe): This section is highlighted with a red box. A callout explains that it detects applications like remote access tools or password cracking tools, which are legitimate but can be misused.

At the bottom of the settings window, there is a progress indicator with five circles, where the second circle (corresponding to the 'Suspicious' level) is currently selected.

3. 詳細設定について

(6)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。

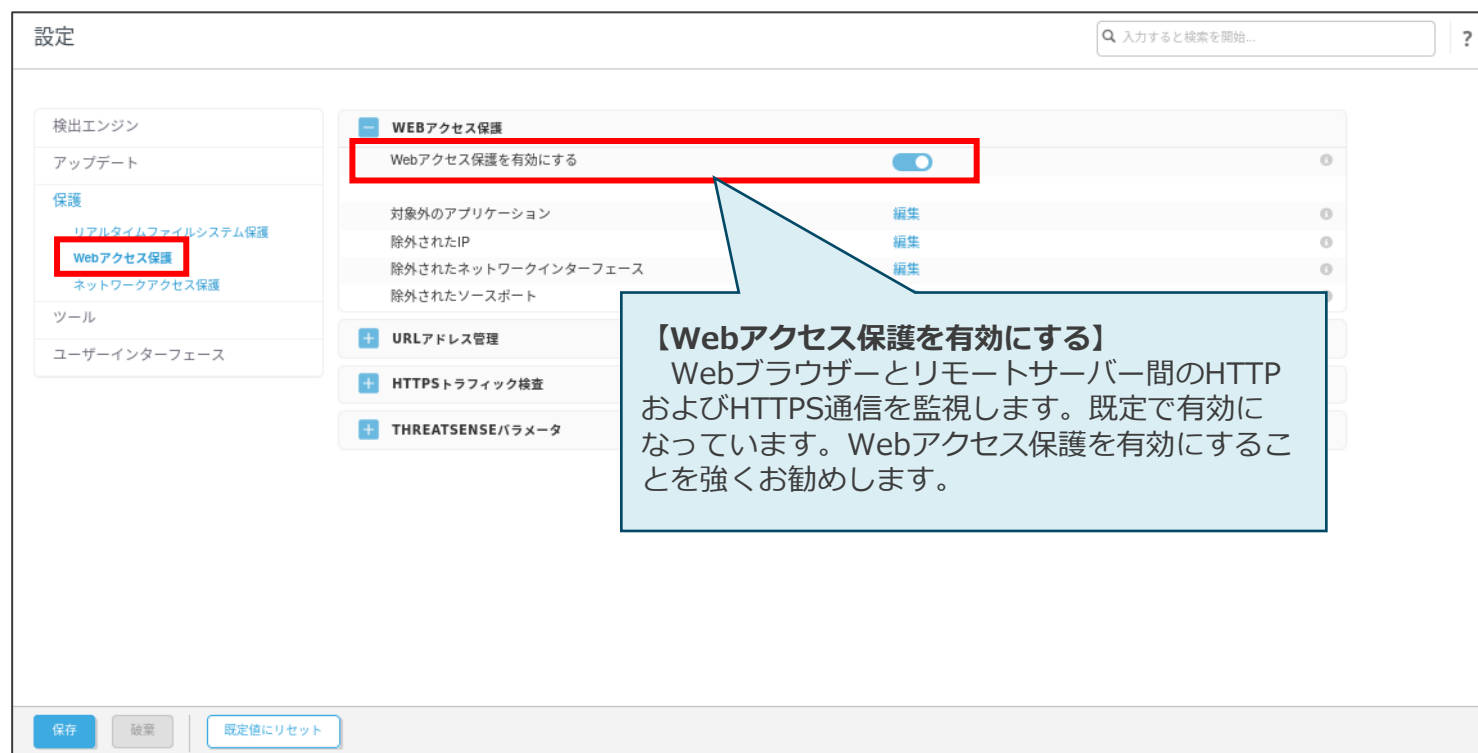
- RHEL / Amazon Linux2023/ AlmaLinux / Rocky Linux / Oracle Linux の場合 : kernel, kernel-devel, kernel-headers
- Ubuntu / Debian の場合 : linux-headers-generic, linux-headers-generic-hwe
- SUSEの場合 : kernel-default, kernel-default-devel, kernel-devel, kernel-macros

3. 詳細設定について

(7)Webアクセス保護

- コンテンツをダウンロードする前に、悪意のあるコンテンツが含まれていることがわかっているWebページへのアクセスをブロックします。その他のすべてのWebページは、読み込み時にThreatSenseスキャンによって検査され、悪意のあるコンテンツの検出時にブロックされます。

■ Webアクセス保護設定画面



3. 詳細設定について

(8) ネットワークアクセス保護

- 通信を解析し、リモートからのアクセスを検知して、迅速にボットを検出します。不正サーバーへの送信となる不審な通信やアドレスを検知して遮断することで、標的型攻撃を防ぎます。この機能を利用するにはWebアクセス保護を有効にする必要があります。

■ ネットワークアクセス保護設定画面



3. 詳細設定について

(9) 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

検出エンジン

アップデート

保護

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

スケジュール

タスク

編集

ウォッチドッグサービス

■ タスク追加画面

有効	名前	トリガー	タスク
☒	Daily computer scan for vulnerabilities and patches	Task will be run at 12:00:00 on the following days : Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday	Vulnerability & Patch Management computer scan

追加 削除 利用

保存 破棄 既定値にリセット

■ オンデマンド検査スケジュール設定画面①

タスク詳細

タスク名

タスクの種類

有効

オンデマンドコンピューターの検査

脆弱性とパッチ管理コンピューターの検査

次へ キャンセル

任意のタスク名とタスクの種類：「オンデマンドコンピューターの検査」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、除外の検査)
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ル設定画面②

タスク詳細

日時

15:35

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

実行されます。

キャンセル

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。

■ オンデマンド検査スケジュール設定画面③

オンデマンド検査スケジュール

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
☒ ブートセクター

対象を追加するパスをここに入力

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

(10)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

保護

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

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 既定値にリセット

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

(11)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

検出エンジン

アップデート

保護

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

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 既定値にリセット

- 【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

(12)ユーザーインターフェース

- ESSL V12.Xの保護状態に関する通知を、ステータス概要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

Q 入力すると検索を開始...

検出エンジン

アップデート

保護

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、保護の状態を表示するを選択できます。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 既定値にリセット

■ 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

ステータス	
ESET LIVEGUARD	
ESET LiveGuardサーバーに接続できません	☐
ESET LiveGuardはクラウド接続が制限されています	☐
ESET LiveGuardは無効ですが、アクティベーションされています	☒
ESET LiveGuardライセンスが有効期限切れです	☐
ライセンスの問題のため、ESET LiveGuardが動作していません	☒
WEBアクセス	
Webアクセス保護が機能していません	☒
Webアクセス保護が無効になっています	☒
その他	
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。	☒
ウォッチドッグサービスが無効です	☒
ウイルス対策	
ESET LiveGrid®フィードバックシステムが無効です	☒

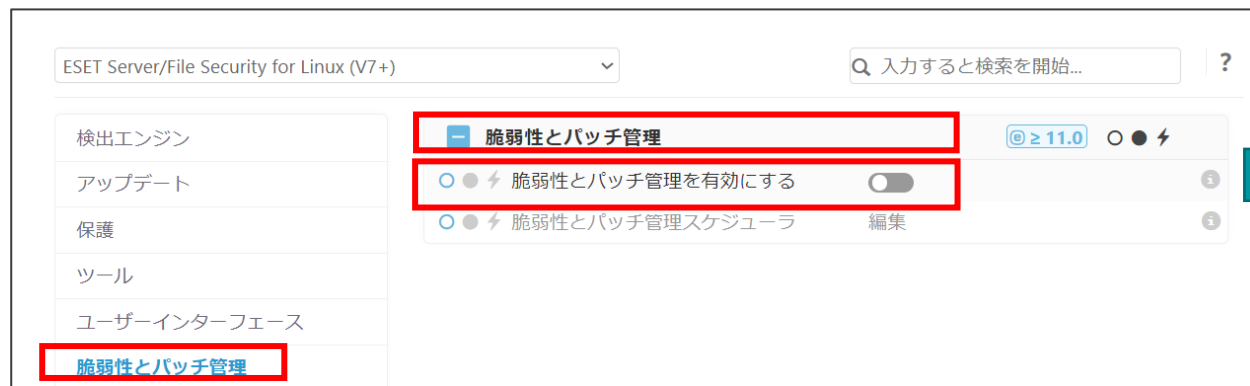
OK キャンセル

3. 詳細設定について

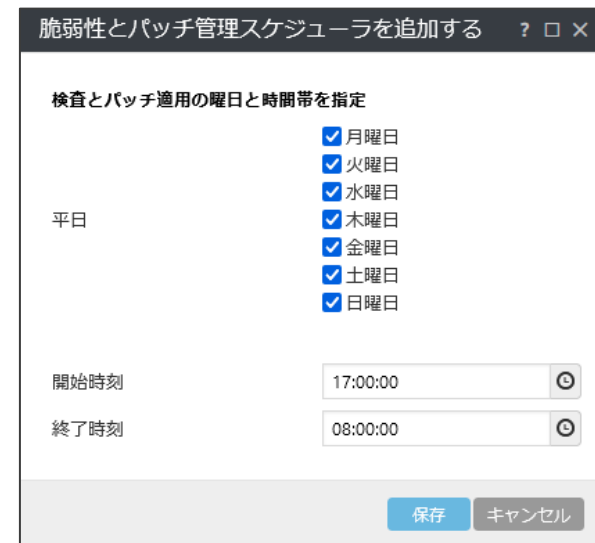
(13)脆弱性とパッチ管理

- 脆弱性とパッチ管理では、アプリケーションの脆弱性状況の検出状況を管理することができます。
スケジューラにて任意のタイミングで実施させることができます。
- ※クラウド型セキュリティ管理ツールESET PROTECTで管理している場合にのみご利用いただけます。
(オンプレミス型セキュリティ管理ツール ESET PROTECT on-premではご利用いただけません。)
- ※「ESET PROTECT Elite」または「ESET PROTECT Complete」ライセンスの場合にのみご利用いただける機能です。

■脆弱性とパッチ管理設定画面



■スケジューラ画面



※脆弱性とパッチ管理(ESET Vulnerability & Patch Management)の詳細は下記よりご確認ください。
https://eset-info.canon-its.jp/files/user/pdf/download/business/request/vapm_function.pdf

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 V12.X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 --profile="@In-depth 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=http://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

4. ESSLの仕様について

(1)インストールについて

※インストールにはroot権限(スーパーユーザー)が必要です。

- ESSL V12.X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。
- 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いません。
- オペレーティングシステム保護プロファイル(OSPP)のRHELはサポートされていません。
- ESSL V9.X以降をご利用の場合は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。
詳細は下記サポートサイトをご参照ください
 - Linux Server向けクライアント用プログラムをバージョンアップしたい
https://eset-support.canon-its.jp/faq/show/3234?site_domain=default

- ESSL V12.XのダッシュボードはESSL V8.1と比較して、CPU利用率/メモリ利用率※/方法別検査済みファイルのグラフ表示ができます。

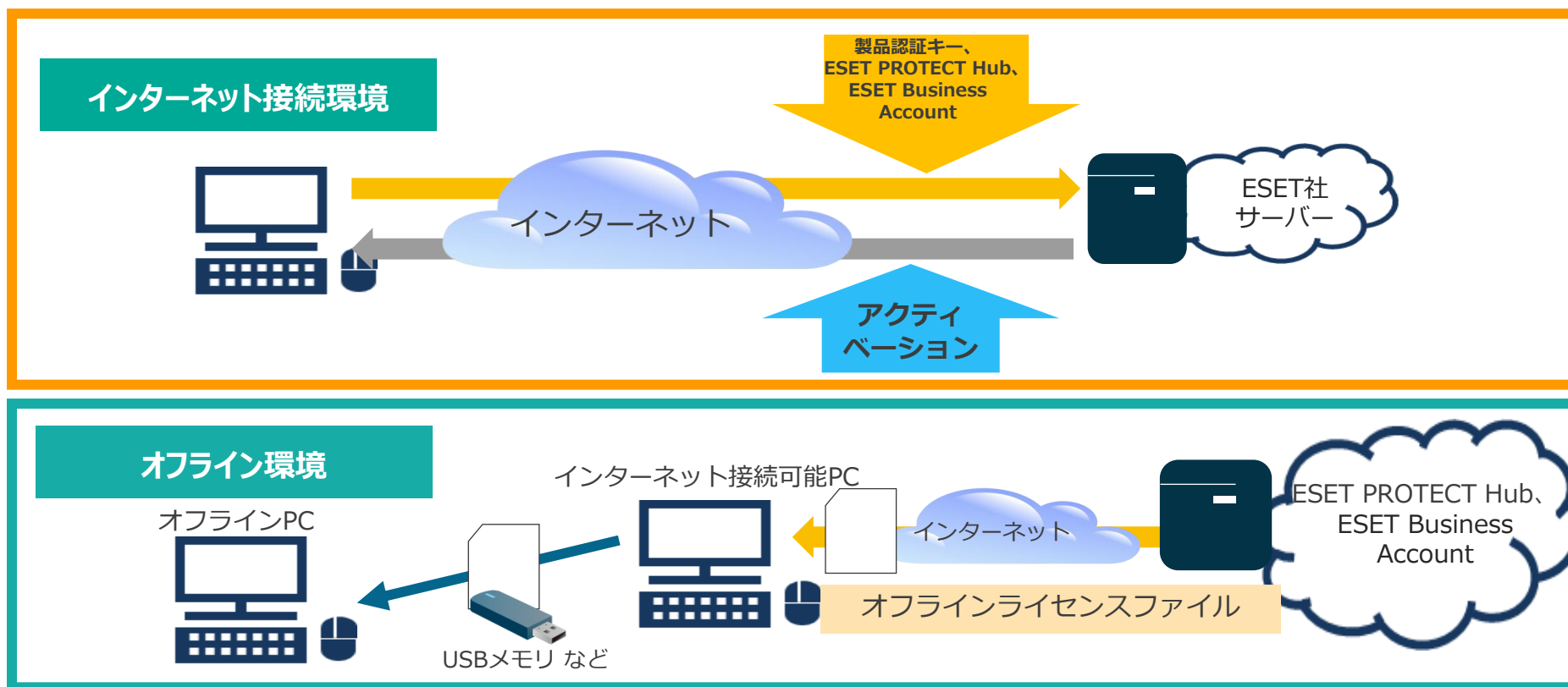
■ESSL V12のダッシュボード



4. ESSLの仕様について

(3)アクティベーションについて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 V12.Xインストール後に**製品認証キー**や**ESET PROTECT Hub/ESET Business Account**、**オフラインライセンスファイル** いずれかを使用してアクティベーション(認証)作業を行っていただく必要があります。



4. ESSLの仕様について

(3) アクティベーションについて②

- Webインターフェースの「ステータス概要」からアクティベーションが可能です。
「ESET PROTECTソリューション」の管理用プログラムであるEPやEP on-premのセキュリティ管理ツールでESSL V12.X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

ステータス概要

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)

アカウント
ESET PROTECT Hubアカウント、ESET Business Account、またはESET MSP Administratorアカウントのライセンスでアクティベーションします。

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。

ESET管理コンソール
ESET管理コンソールを使用して、アクティベーションします。

製品認証キー、ESET PROTECT Hub アカウント/ESET Business Account アカウントまたは、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

ステータス概要

ライセンス

ライセンスは有効です
ライセンスの有効期間: 2026/02/01
ライセンスID: 3AA-NNJ-GF4
+ 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。

※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。