ESET Server Security for Linux V9
機能紹介資料

第2版

2023年1月24日

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 V9」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 V9(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。)

・本資料はESET Server Security for Linux V9.1を想定して作成しております。

・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ございます。

・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 V8.1 (略称表記：EP) 以降で管理が可能です。EPC / EPの機能紹介は、別資料でご用意しております。

・ EPC / EP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、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

サポート環境

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) Red Hat Enterprise Linux 9.X (64bit) SUSE Linux Enterprise 12 (64bit) SUSE Linux Enterprise 15 (64bit) CentOS 7.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 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	・elfutils-libelf-devel（RHEL8, Amazon Linux2のみ必要） ・libselinux（RHEL, CentOS, Amazon Linux2のみ必要。最新パッケージを利用） ・selinux-policy-devel（SELinux有効で利用）
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	

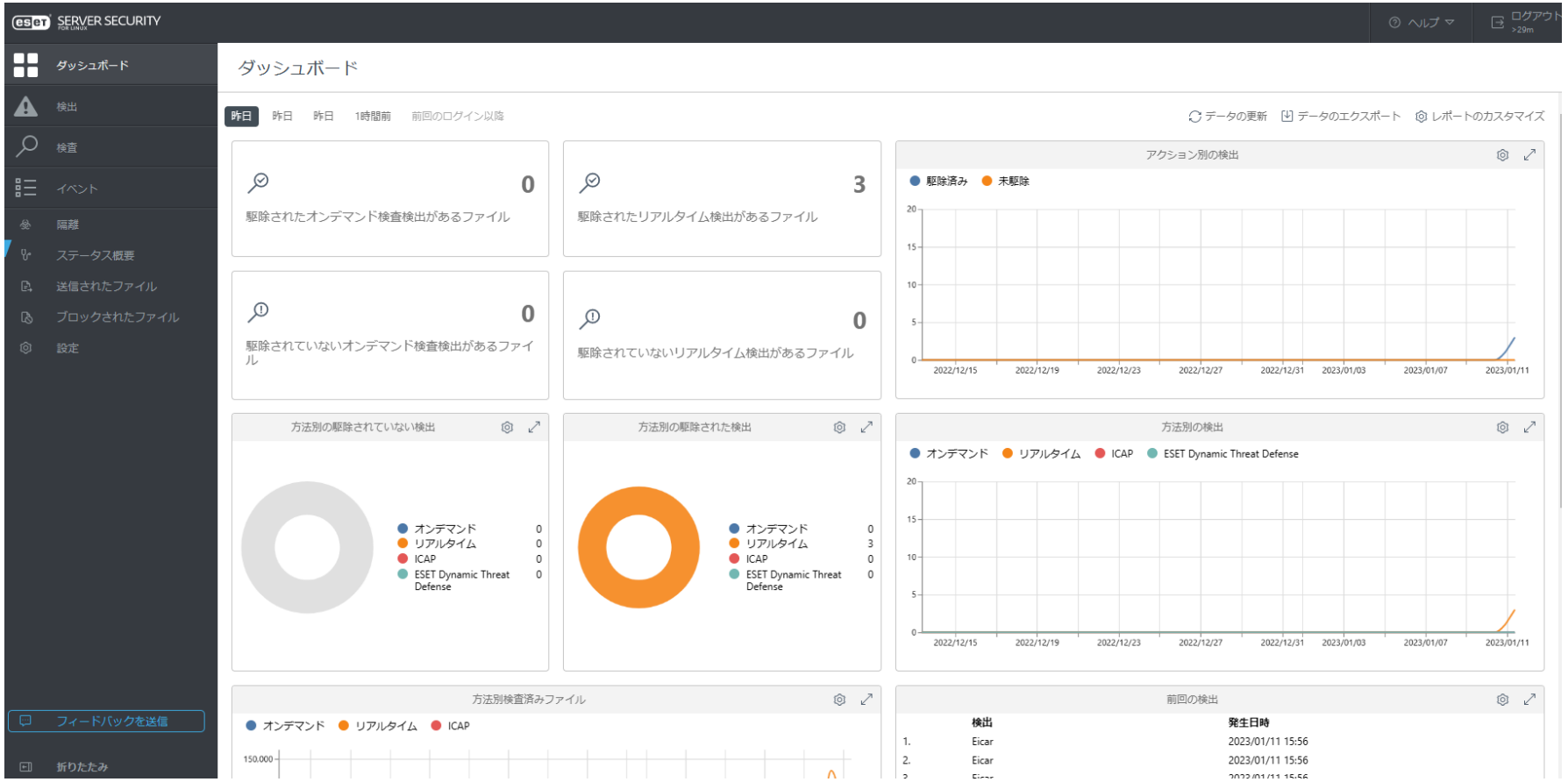
Webインターフェースについて

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

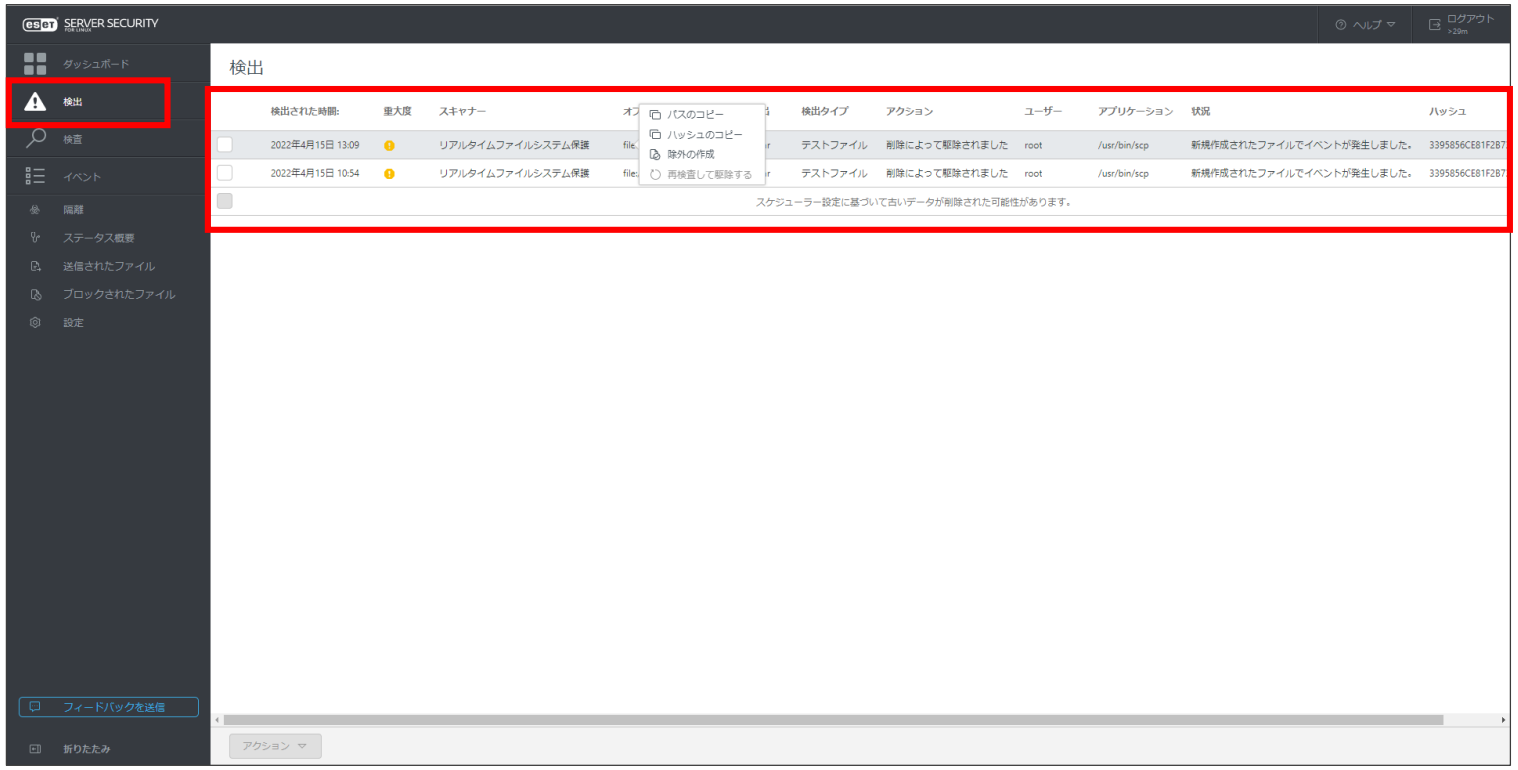


2. Webインターフェースについて

(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

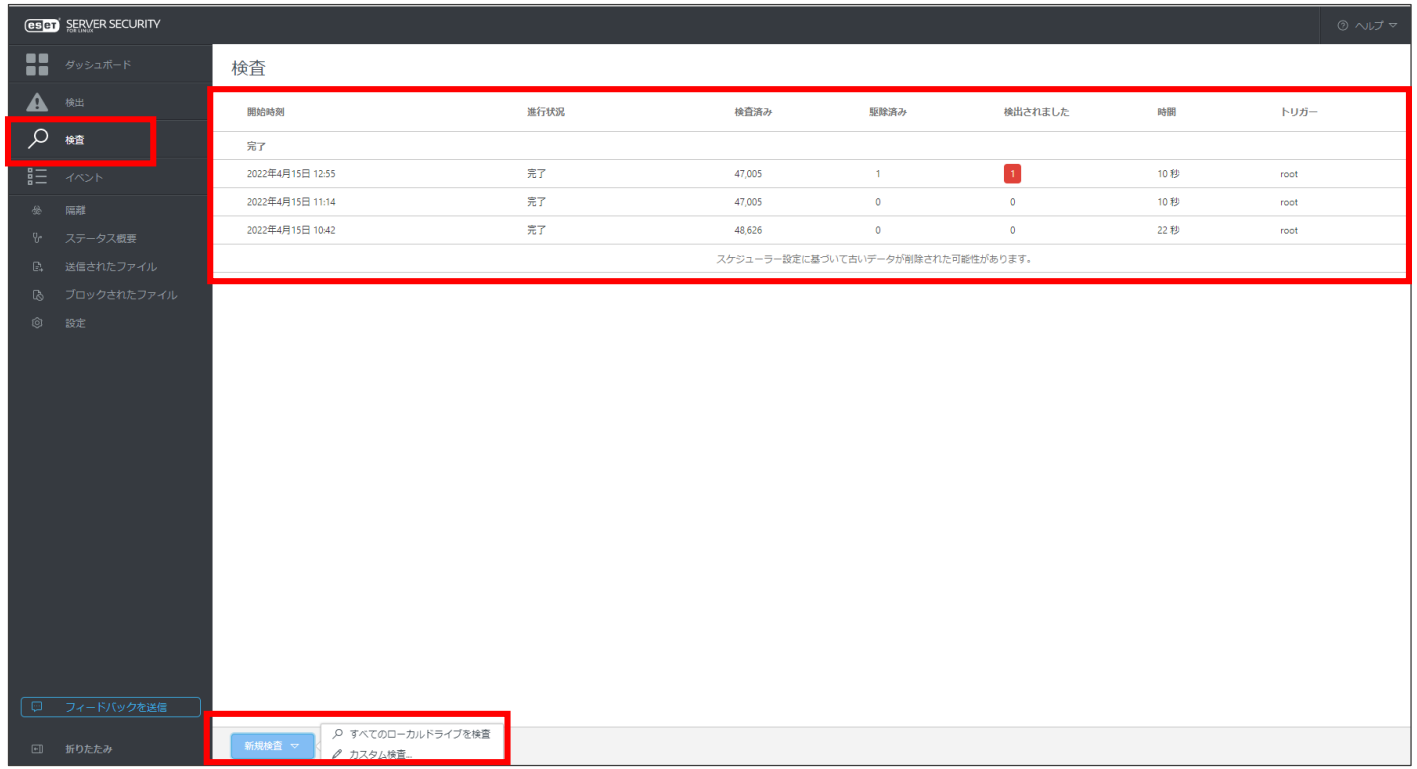


2. Webインターフェースについて

(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



■検査の詳細画面①

■検査の詳細画面②

2. Webインターフェースについて

(4)イベント

- ESSL V9.XのWebインターフェイ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 V9.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。

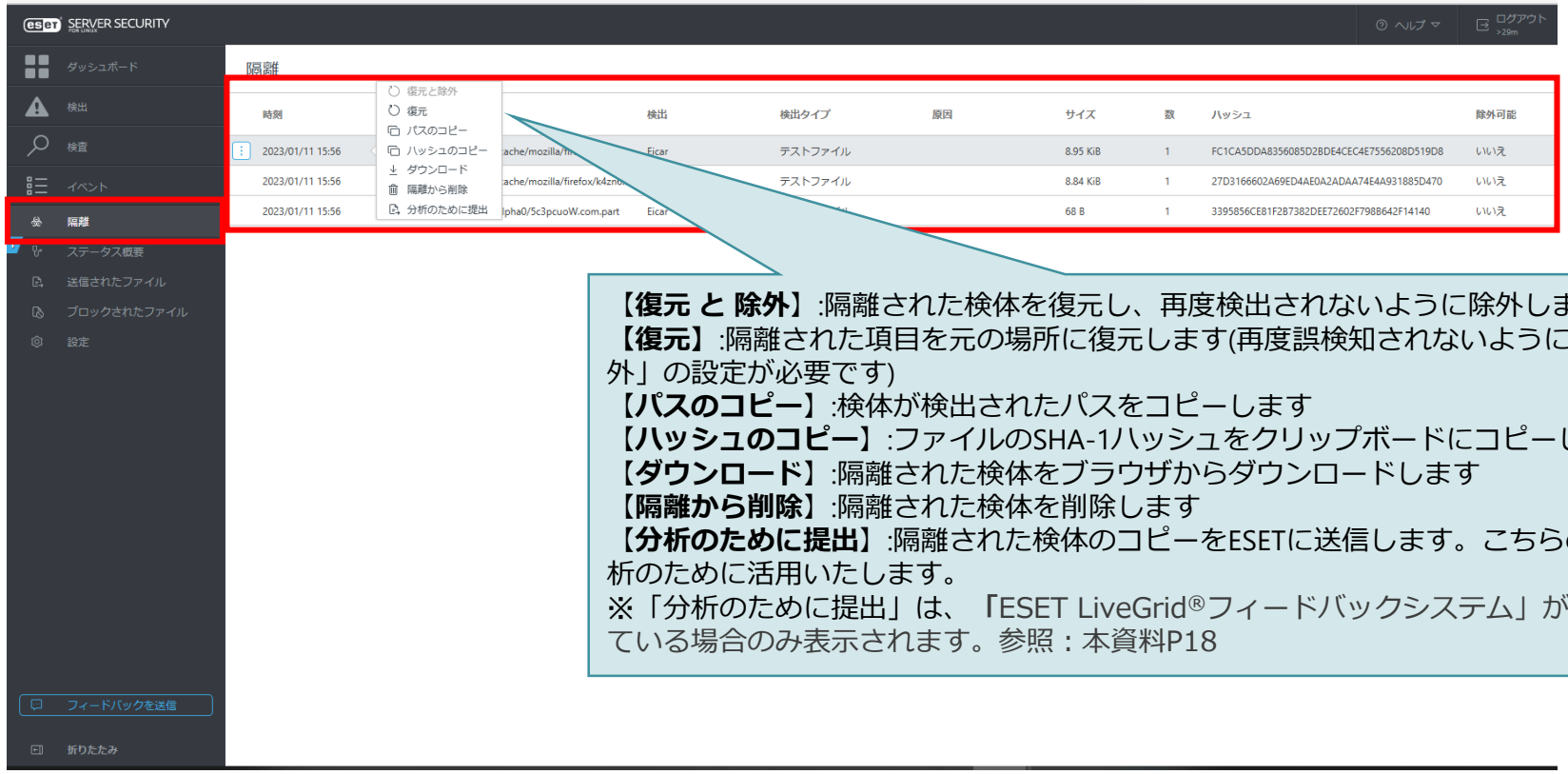
■イベント画面

2. Webインターフェースについて

(5)隔離

- ESSL V9.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



【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。こちらの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のみ表示されます。参照：本資料P18

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

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ができます。

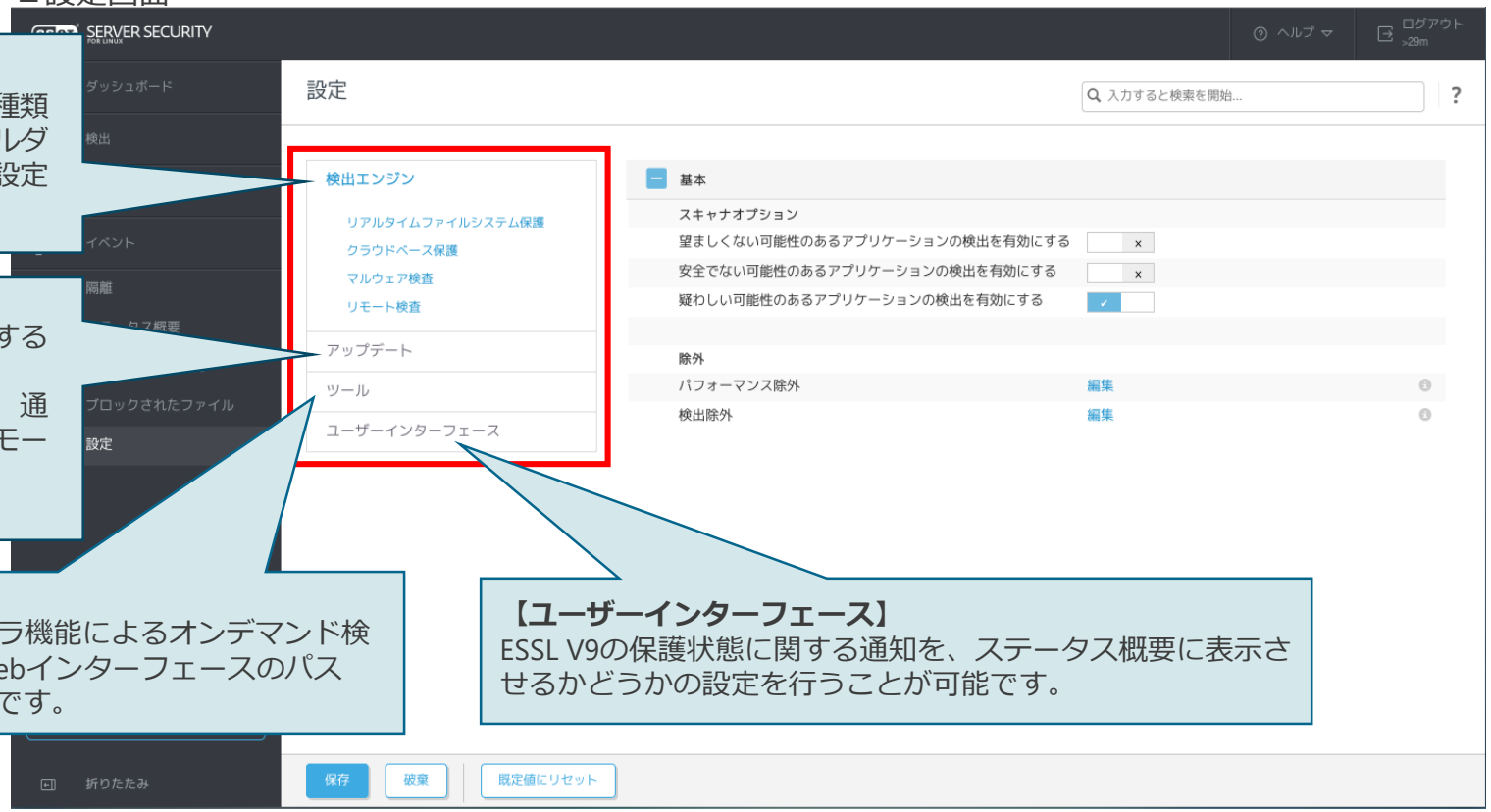
■ブロックされたファイル画面

2. Webインターフェースについて

(8)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 V9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。

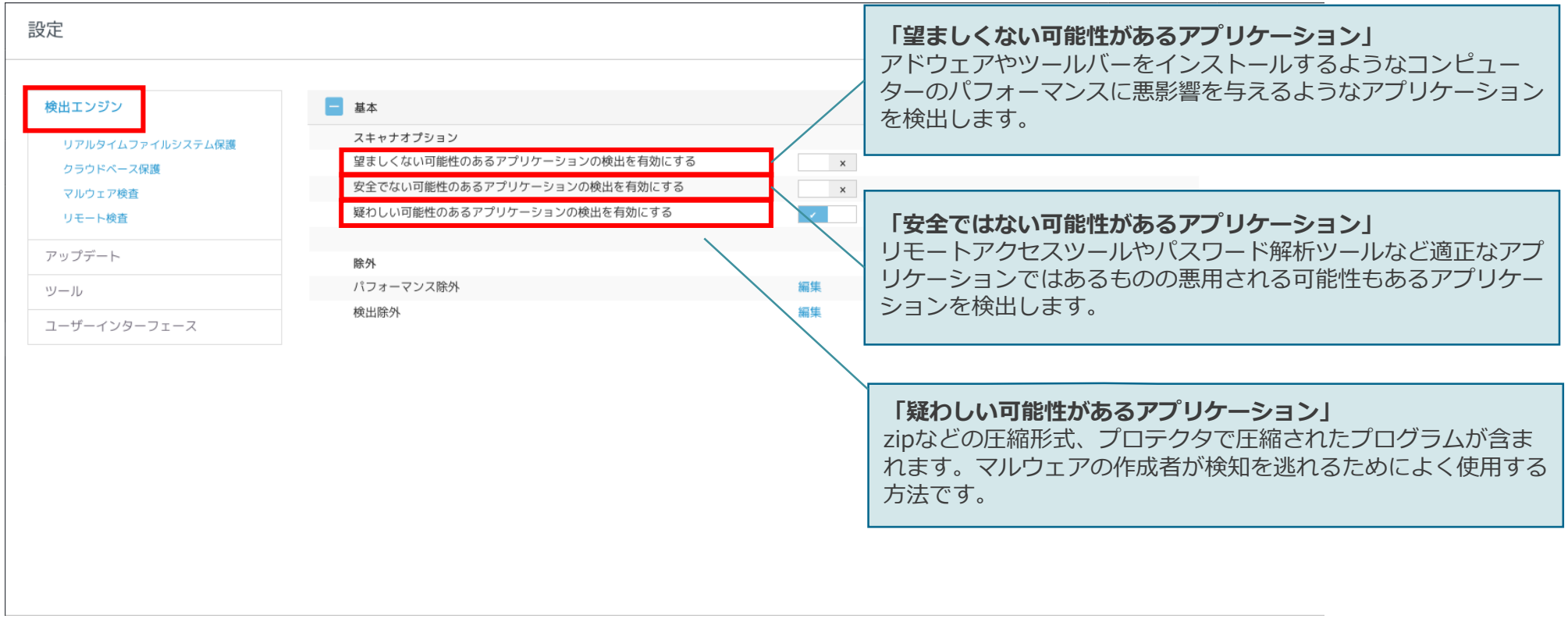
詳細設定について

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



「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。

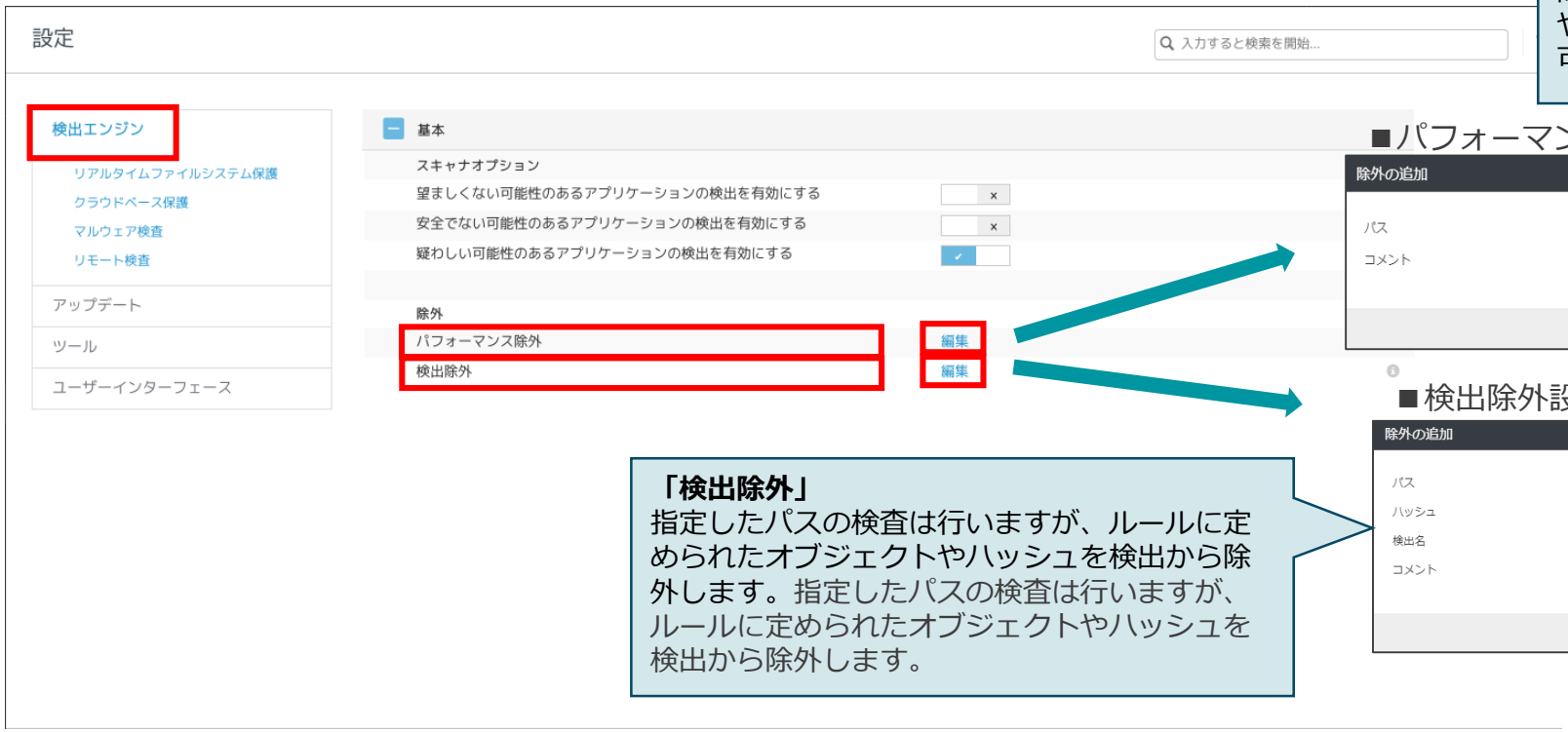
「疑わしい可能性があるアプリケーション」
zipなどの圧縮形式、プロテクタで圧縮されたプログラムが含まれます。マルウェアの作成者が検知を逃れるためによく使用する方法です。

3. 詳細設定について

(2)除外

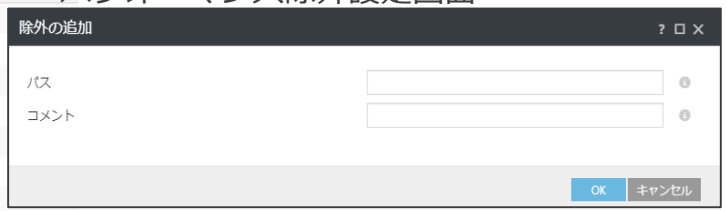
- 除外の設定を行うことで、特定のファイルやフォルダをウイルス検査の対象から外すことが可能です。パス、ハッシュ値、検出名で除外設定を行えます。独自開発したアプリケーションやデータベースなどを除外の対象とすることで、誤検知やデータベースなどを検査した際のCPU使用率の上昇を防ぐことが可能です。

■検出エンジン設定画面

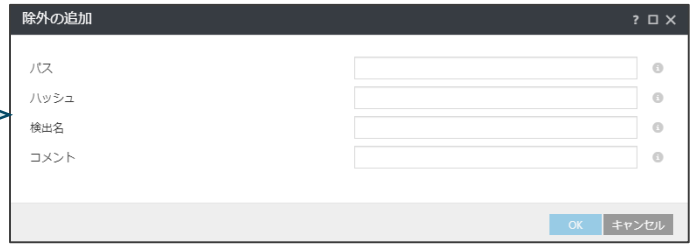


「パフォーマンス除外」
特定のファイルやフォルダを検査対象から除外することが可能です。特定のファイルやフォルダを検査対象から除外することが可能です。

■パフォーマンス除外設定画面



■検出除外設定画面



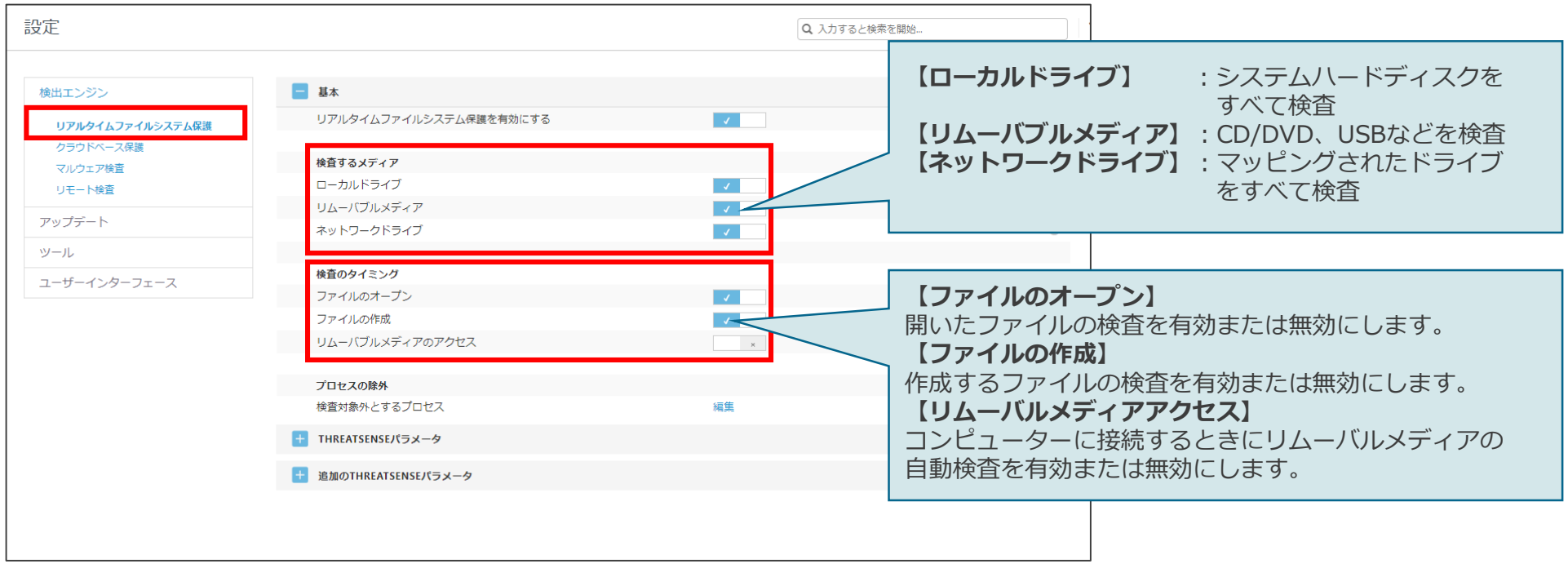
「検出除外」
指定したパスの検査は行いますが、ルールに定められたオブジェクトやハッシュを検出から除外します。指定したパスの検査は行いますが、ルールに定められたオブジェクトやハッシュを検出から除外します。

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。

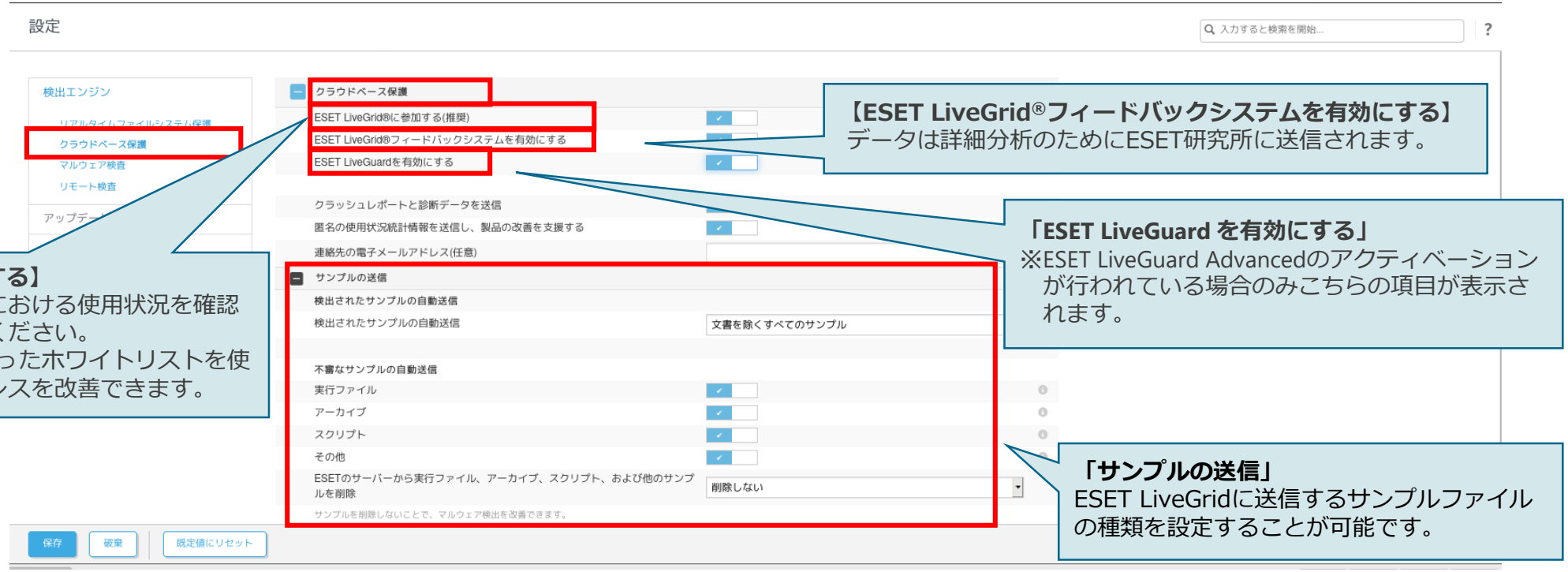
■RHEL / CentOS / Amazon Linux2の場合：Kernel, kernel-devel, kernel-headers　■SUSEの場合：kernel-default, kernel-default-devel, kernel-devel, kernel-macros

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つながります。

■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。

「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」
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

【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

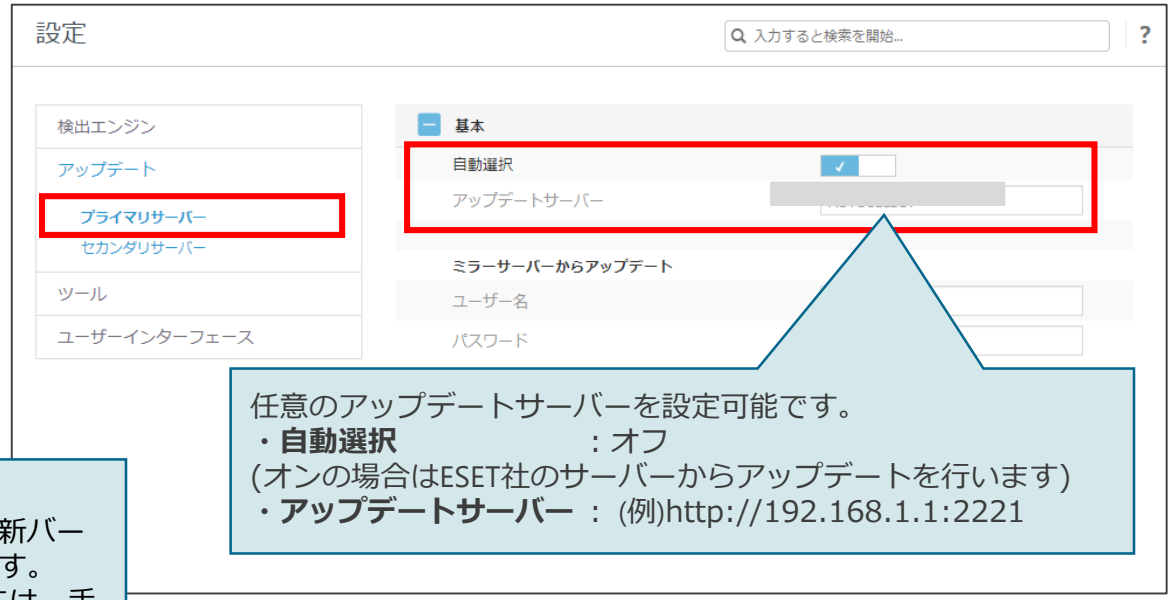
- アップデートでは、検出エンジンの取得先を変更することなどが可能です。アップデート先としてプライマリサーバー、セカンダリサーバーを設定することによってアップデート先の冗長化が可能です。

■アップデート詳細設定画面

【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】
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。
※V9.1より既定で自動アップデート機能が有効になりました。

■プライマリーサーバー設定画面



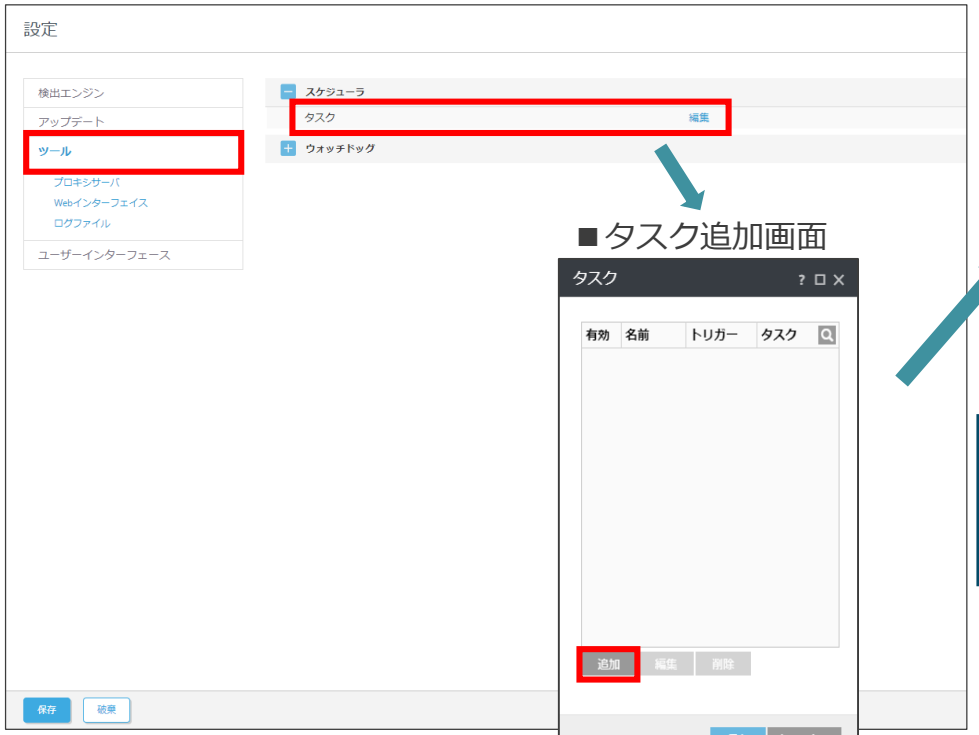
任意のアップデートサーバーを設定可能です。
・**自動選択**　　：オフ
(オンの場合はESET社のサーバーからアップデートを行います)
・**アップデートサーバー**：(例)http://192.168.1.1:2221

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



■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、 除外の検査)
を選択して、「完了」ボタンをクリックします。

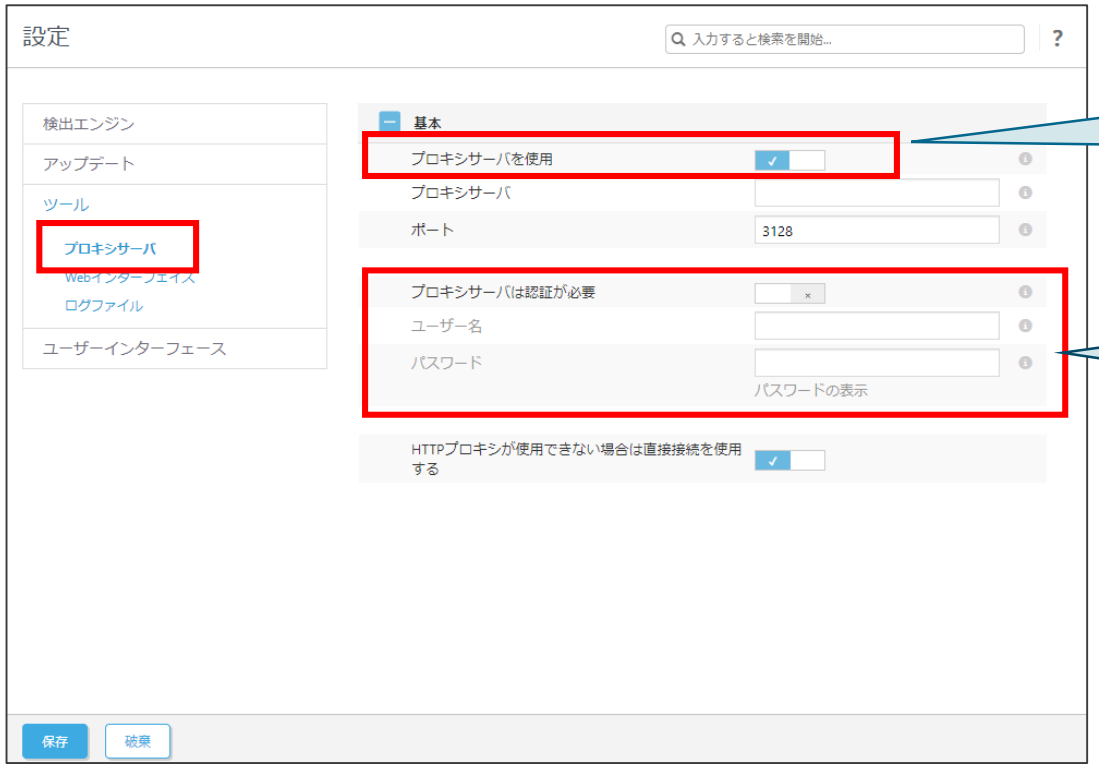
■オンデマンド検査スケジューラ設定画面②

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。

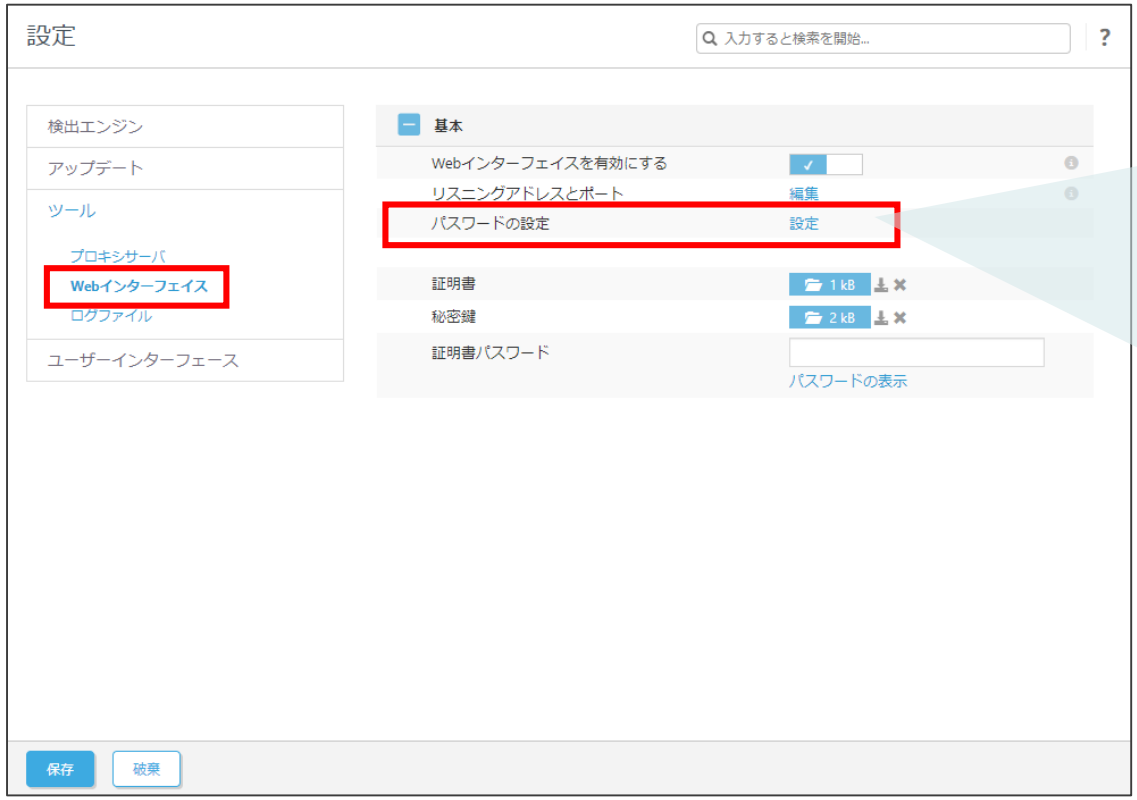
プロキシサーバで認証が必要な場合は、**【プロキシサーバは認証が必要】**にチェックを付け、有効なユーザー名とパスワードを入力します。

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ESSL V9.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

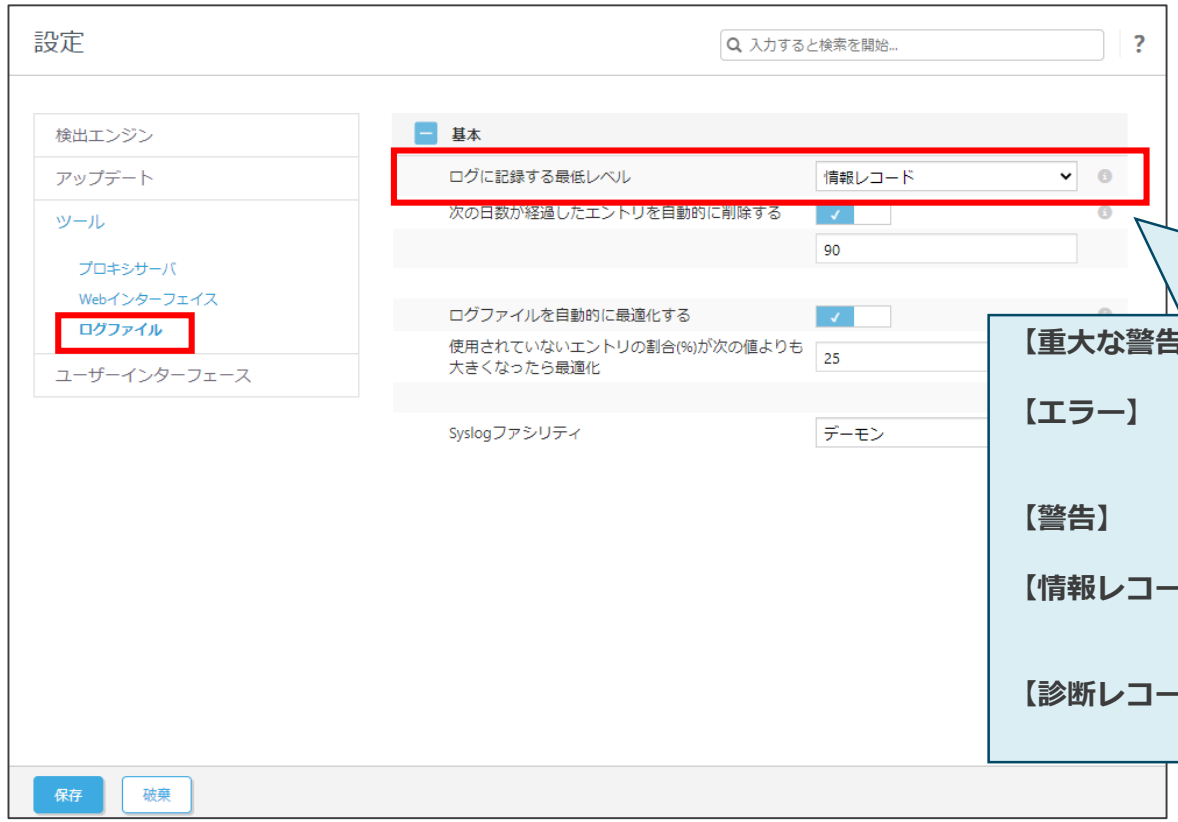
【パスワードの設定】を選択し、新しいパスワードを入力して「OK」ボタンをクリックします。

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



【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。

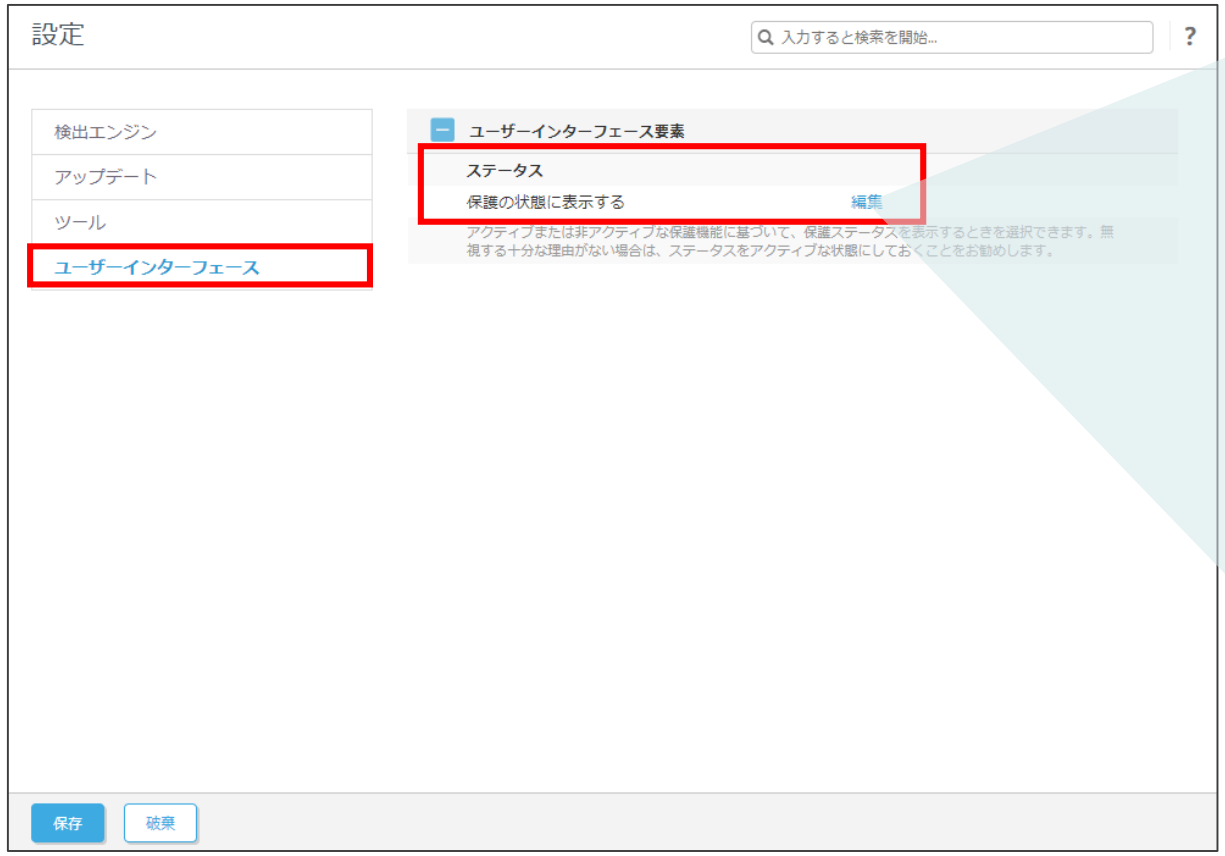
【診断レコード】 ：プログラムおよび上記のすべてのレコードを微調整するのに必要な情報が含まれます。

3. 詳細設定について

(11)ユーザーインターフェース

- ESSL V9.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



■ステータス設定画面

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 V9.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/lslog [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=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/lslog -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

- ESSL V9.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。
- 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 V9.X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、ESSL V8.1/9.0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 V9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 V9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)**
  - **・Red Hat Enterprise Linux 9.X (64bit)**
  - **・CentOS 7.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りません。

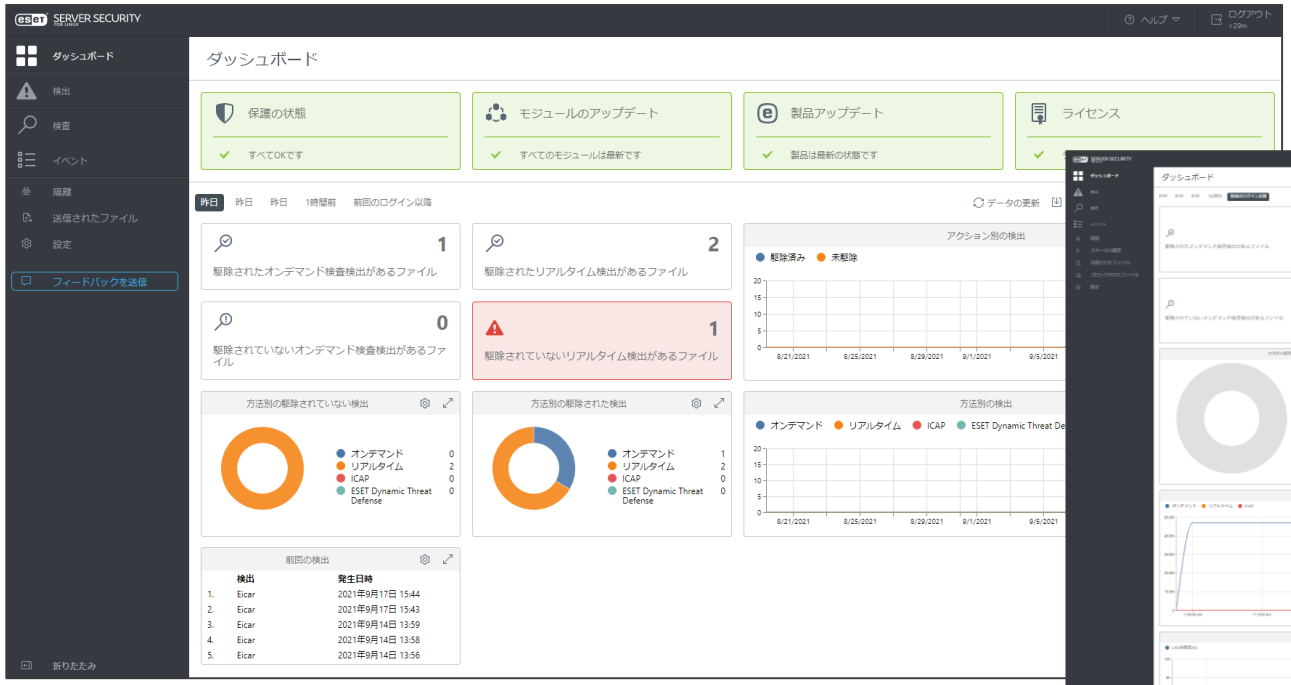
※インストールにはroot権限(スーパーユーザー)が必要です。

4. ESSLの仕様について

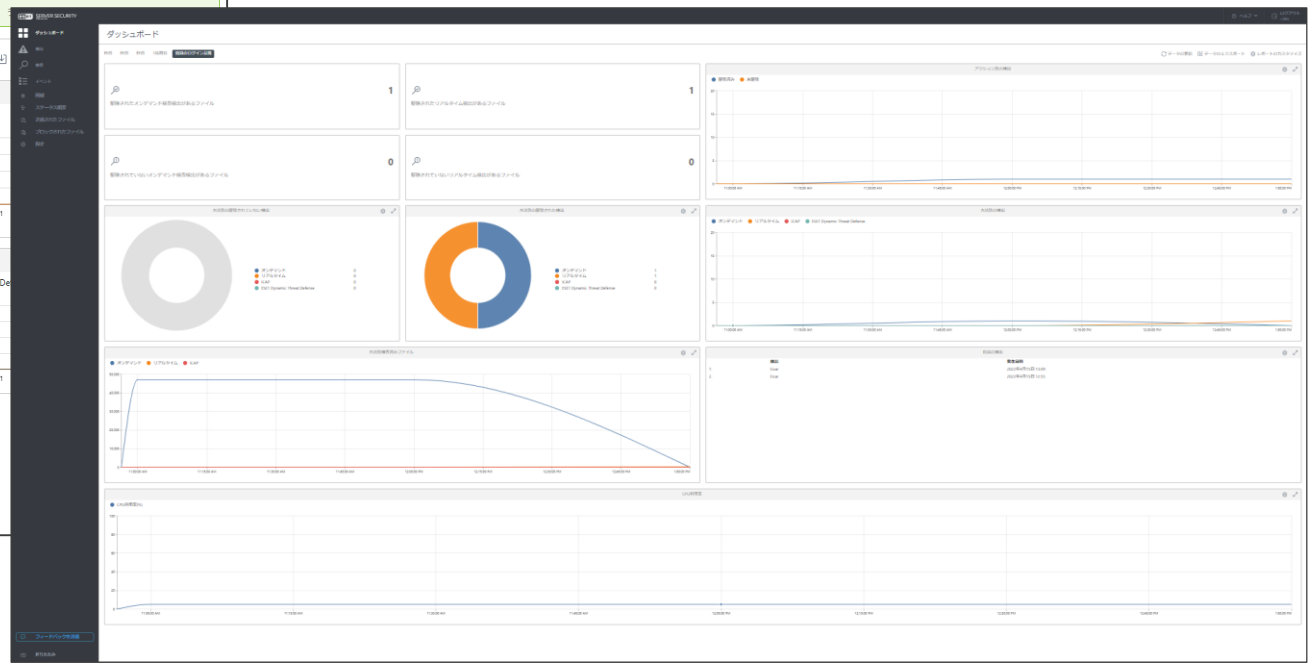
(2)ダッシュボードについて

- ESSL V9.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るようになりました。

■ESSL V8.1のダッシュボード



■ESSL V9のダッシュボード

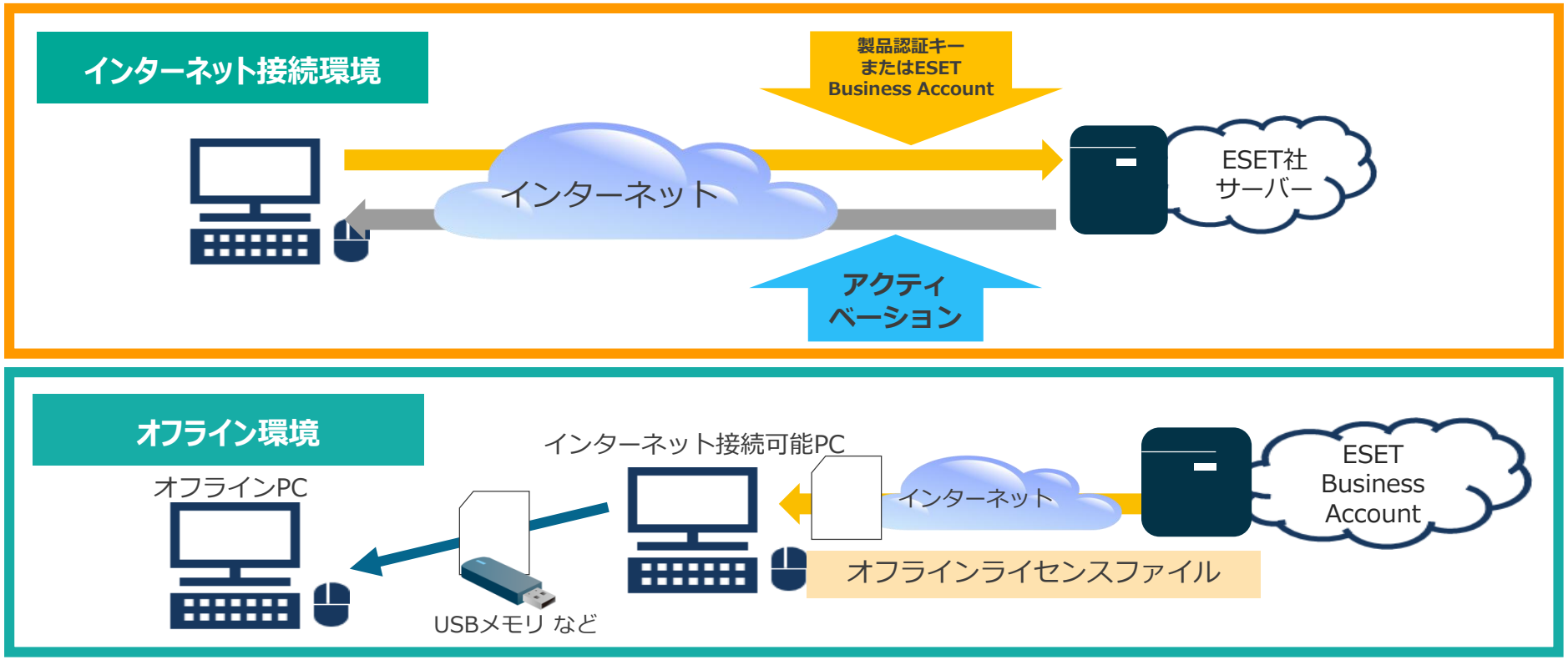


※デフォルトでは非表示です。

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 V9.Xインストール後に**製品認証キー**、**ESET Business Account**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。



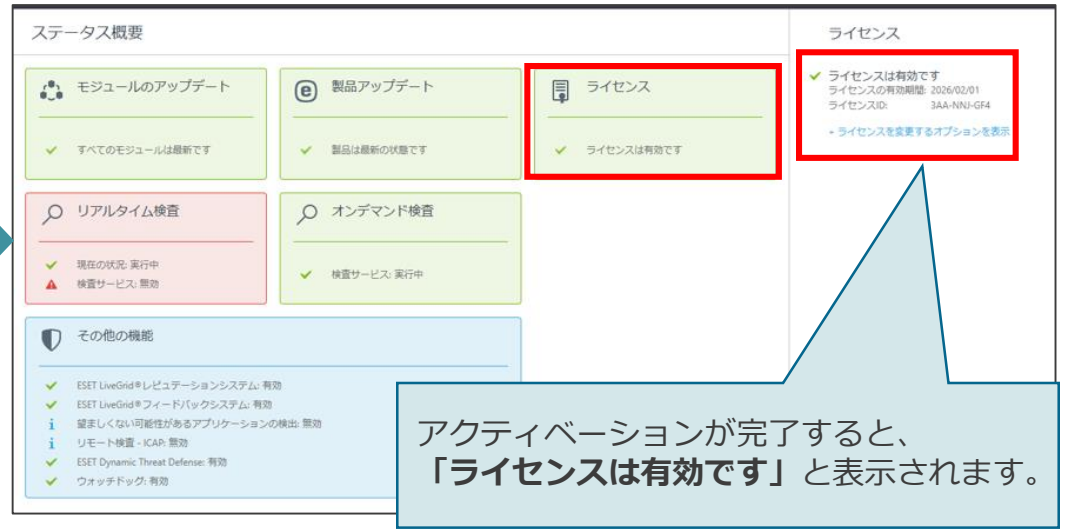
4. ESSLの仕様について

(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EPCやEPのセキュリティ管理ツールでESSL V9.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

■アクティベーション完了後の画面



※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。