

ESET Server Security for Linux V9

機能紹介資料

第2版

2023年1月24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 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 V8.1 (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

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 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	

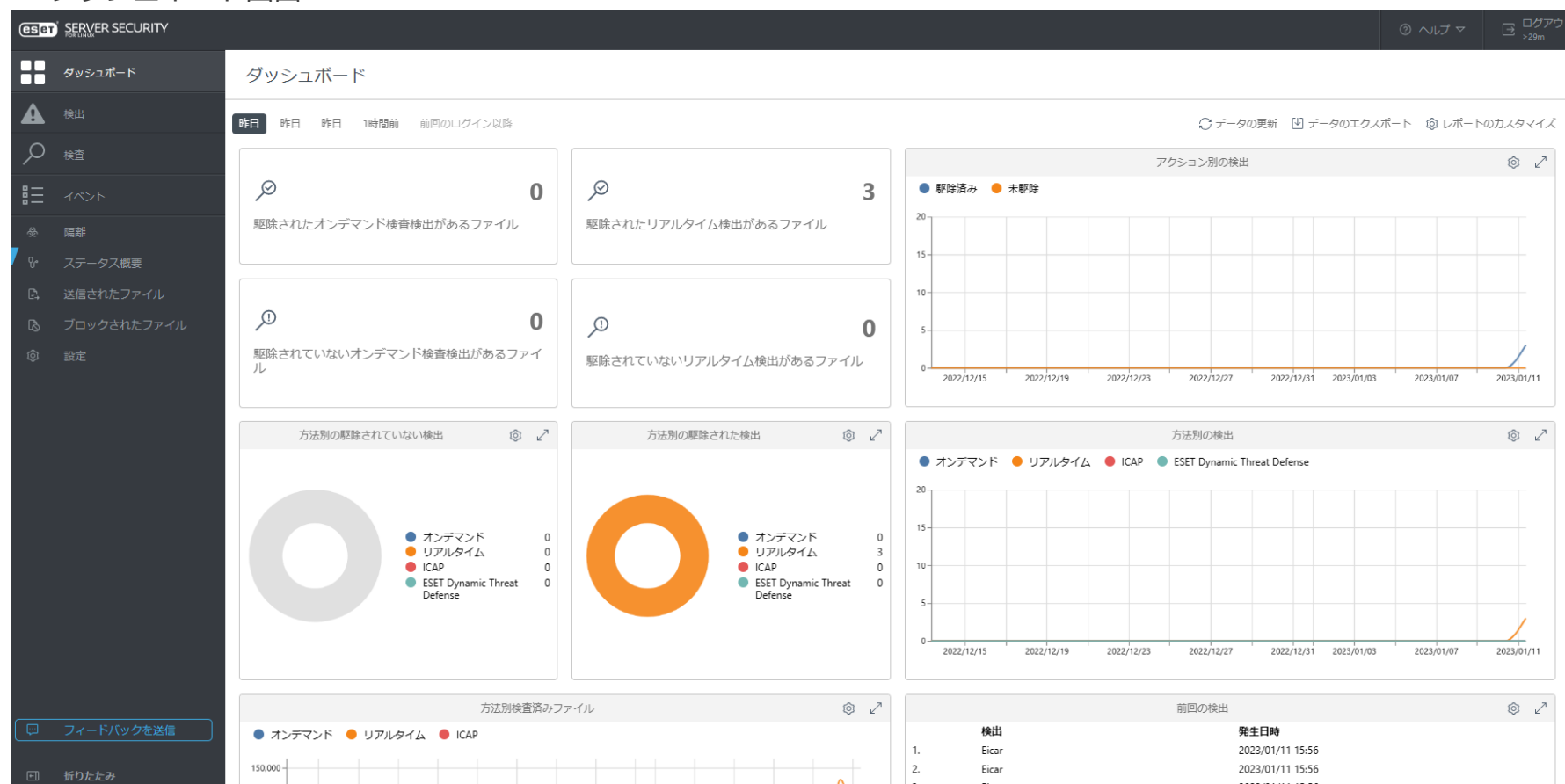
Webインターフェースについて

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

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	ハッシュ
2022年4月15日 13:09	⚠	リアルタイムファイルシステム保護	file:	テストファイル	削除によって駆除されました	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。	3395856CE81F287
2022年4月15日 10:54	⚠	リアルタイムファイルシステム保護	file:	テストファイル	削除によって駆除されました	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。	3395856CE81F287

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						
2022年4月15日 12:55	完了	47,005	1	1	10 秒	root
2022年4月15日 11:14	完了	47,005	0	0	10 秒	root
2022年4月15日 10:42	完了	48,626	0	0	22 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: 2022年4月15日 12:55
完了時刻: 2022年4月15日 12:55
時間: 10 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
未検出: 0
検査済み: 47,005

■ 検査の詳細画面②

検出された時刻	重大度	オブジェクトID	検出	検出タイプ	アクション	ハッシュ
2022年4月15日 12:55	中	file\\root\\scan.com	検出	スクリプトファイル	削除によって駆除されました	339585ACB81F287382DE8726027F888427147402

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 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



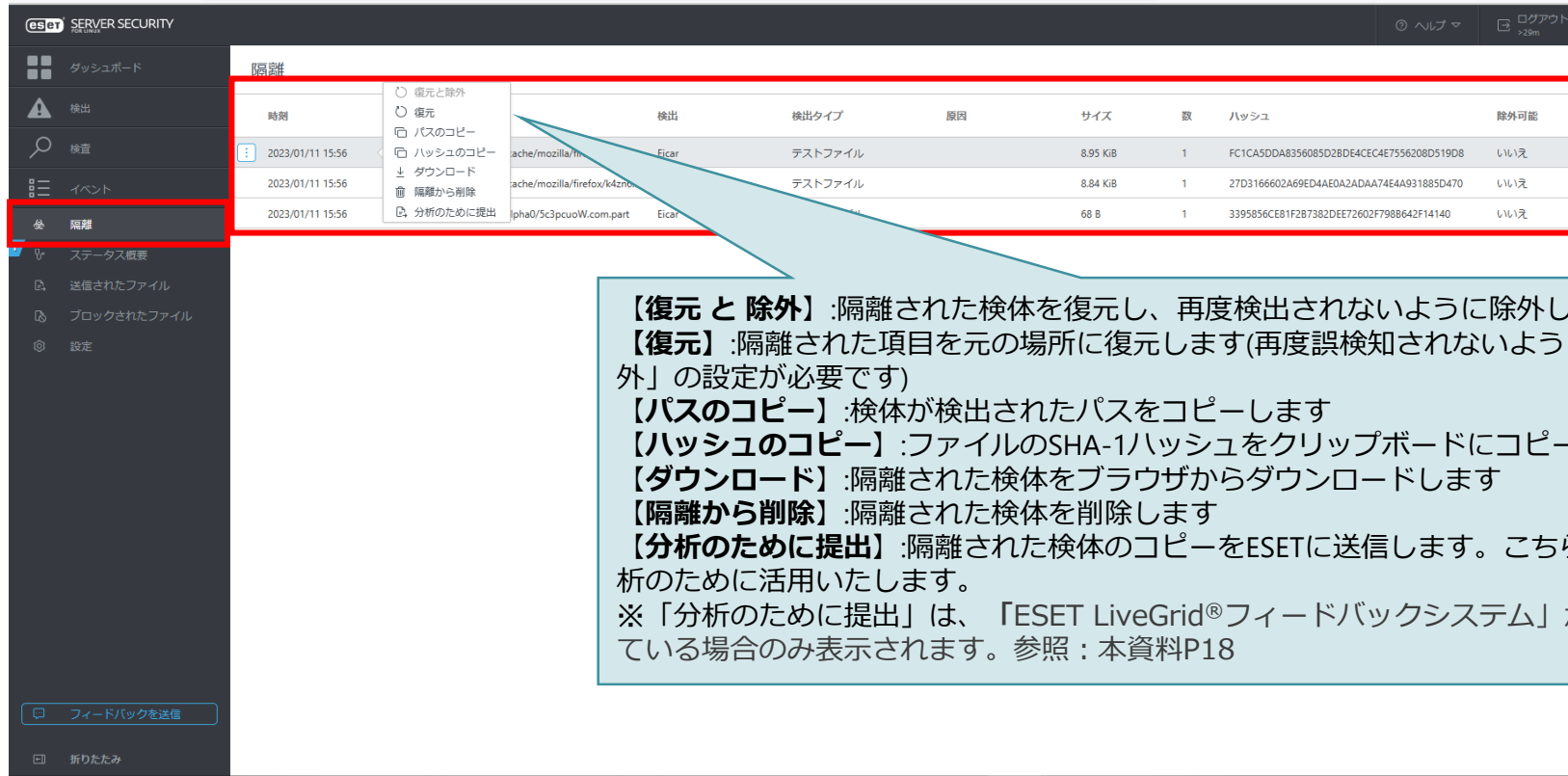
時刻	コンポーネント	イベント	ユーザー
2022年4月15日 09:45	更新サービス	検出エンジンが正常にバージョン25109 (20220414)にアップデートされました。	eset-efs-updated
2022年4月14日 17:35	リアルタイムファイルシステム保...	アクセス中の検査のシステムハンドラーの初期化が失敗しました。OSを更新して、コンピューターを再起動してから、システムログを確認してください。	root
2022年4月14日 17:35	リアルタイムファイルシステム保...	UEKカーネルを実行している場合は、必ずkernel-uek-develがインストールされていることを確認してください。	root
2022年4月14日 17:35	リアルタイムファイルシステム保...	ファイル/lib/modules/3.10.0-1160.el7.x86_64/eset/efs/eset_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
2022年4月14日 17:18	リアルタイムファイルシステム保...	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、システムログを確認してください。	root
2022年4月14日 17:18	リアルタイムファイルシステム保...	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
2022年4月14日 17:18	リアルタイムファイルシステム保...	ファイル/lib/modules/3.10.0-1160.el7.x86_64/eset/efs/eset_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
2022年4月14日 17:18	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
2022年4月14日 17:18	サービスを開始しています	SELinuxが有効ですが、サポートするには、「selinux-policy-devel」パッケージが必要です。インストールして、製品を再起動してください。	root
2022年4月14日 17:07	更新サービス	検出エンジンが正常にバージョン25104 (20220414)にアップデートされました。	eset-efs-updated
2022年4月14日 17:04	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
2022年4月14日 16:12	認証サービス	無効な資格情報	eset-efs-authd
2022年4月14日 15:49	リアルタイムファイルシステム保...	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、システムログを確認してください。	root
2022年4月14日 15:49	リアルタイムファイルシステム保...	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
2022年4月14日 15:49	リアルタイムファイルシステム保...	ファイル/lib/modules/3.10.0-1160.el7.x86_64/eset/efs/eset_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
2022年4月14日 15:49	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
2022年4月14日 15:49	サービスを開始しています	SELinuxが有効ですが、サポートするには、「selinux-policy-devel」パッケージが必要です。インストールして、製品を再起動してください。	root
2022年4月14日 15:32	リアルタイムファイルシステム保...	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、システムログを確認してください。	root
2022年4月14日 15:32	リアルタイムファイルシステム保...	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
2022年4月14日 15:32	リアルタイムファイルシステム保...	ファイル/lib/modules/3.10.0-1160.el7.x86_64/eset/efs/eset_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
2022年4月14日 15:32	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
2022年4月14日 15:32	サービスを開始しています	SELinuxが有効ですが、サポートするには、「selinux-policy-devel」パッケージが必要です。インストールして、製品を再起動してください。	root

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



隔離画面

時刻	検出	検出タイプ	原因	サイズ	数	ハッシュ	除外可能
2023/01/11 15:56	ache/mozilla/...	Eicar	テストファイル	8.95 KiB	1	FC1CA5DDA8356085D28DE4CEC4E7556208D519D8	いいえ
2023/01/11 15:56	ache/mozilla/firefox/k4zm...	テストファイル		8.84 KiB	1	27D3166602A69ED4AE0A2ADA74E4A931885D470	いいえ
2023/01/11 15:56	pha0/5c3pcuoW.com.part	Eicar		68 B	1	3395856CE81F2B7382DEE72602F798B642F14140	いいえ

【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

statuses overview screen

statuses overview

modules update
 ✓ all modules are up to date

product update
 ✓ product is up to date

licenses
 ✓ license is valid

real-time scan
 ✓ current status: running
 ✓ scan service: running

on-demand scan
 ✓ scan service: running

other functions
 ✓ ESET LiveGrid® Reputation System: effective
 i ESET LiveGrid® Feedback System: ineffective
 i Unlikely application detection: ineffective
 i Remote Scan - ICAP: ineffective
 ✓ Watchdog: effective

ウォッチドッグ機能により、ステータスを確認できます。

ウォッチドッグ機能により、ステータスを確認できます。

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



eset SERVER SECURITY FOR LINUX

ヘルプ ログアウト >29m

ダッシュボード

検出

検査

イベント

隔離

1 ステータス概要

送信されたファイル

ブロックされたファイル

設定

フィードバックを送信

折りたたみ

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 ここには、ブロックされたファイルのリストが表示されます。ファイルがブロックされていないが、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、現在データが表示されていません。								

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)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】

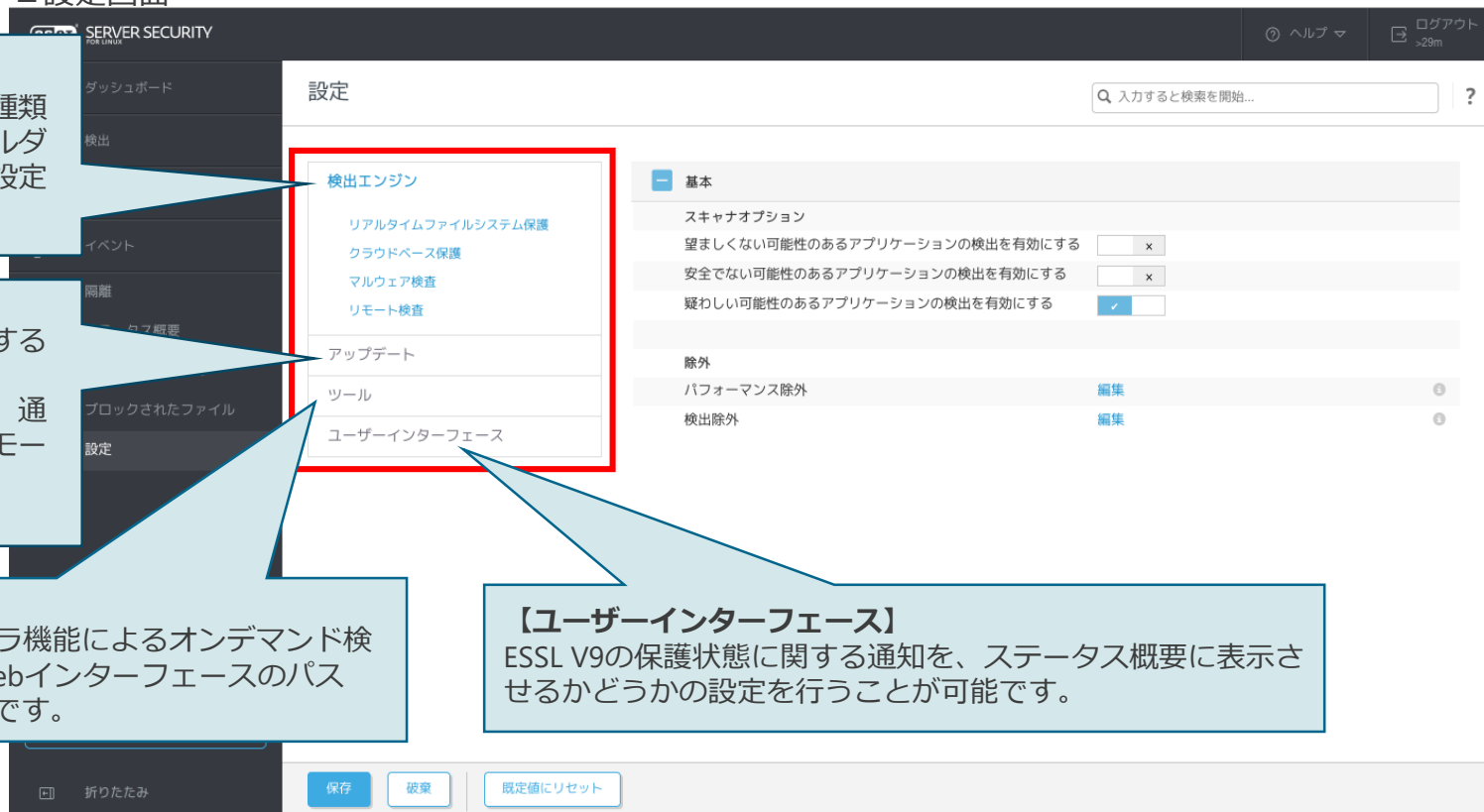
アップデートの項目では、検出エンジンの取得先を変更することなどが可能です。アップデートモードは通常のアップデートモードのほか、通常の検出エンジンの配信より少し早く配信されるテストモードや、逆に通常配信後12時間経過してから配布される遅延アップデートを選ぶことが可能です。

【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

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

検出除外

編集

編集

「望ましくない可能性の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の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。

「疑わしい可能性の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 Q 入力すると検索を開始...

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 ☐ x

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 ☐ x

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

検出除外

編集

編集

「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

「検出除外」

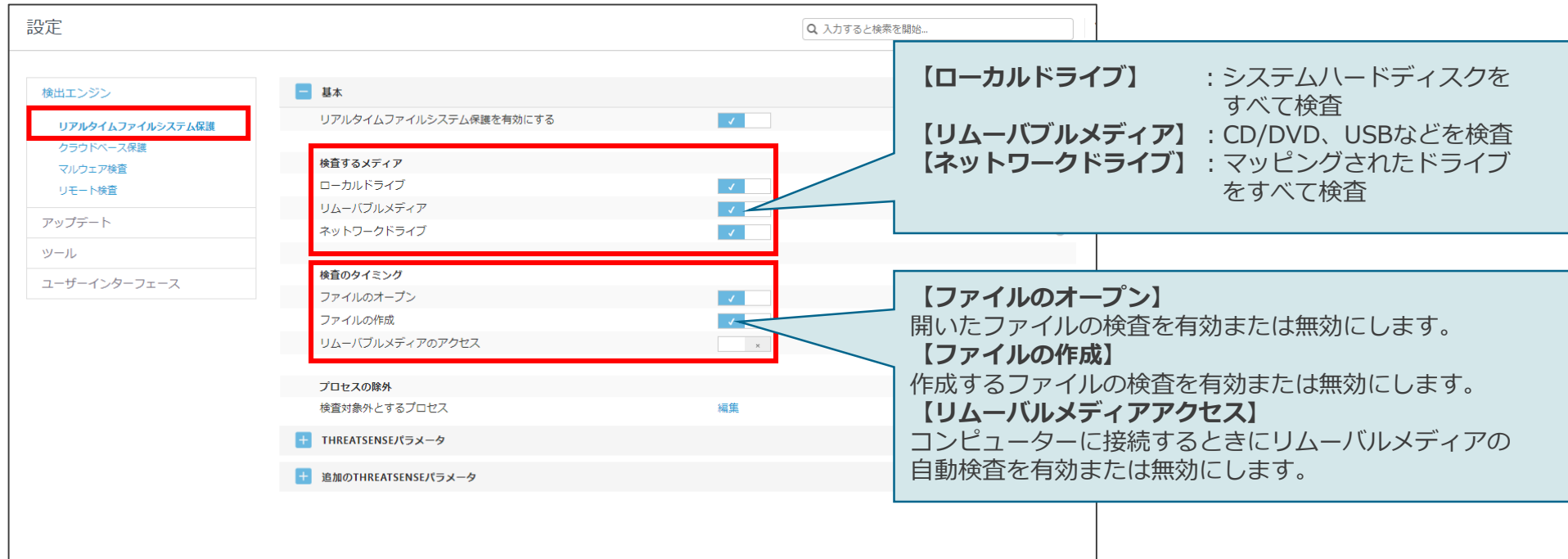
指定したパスの検査は行いますが、ルールに定められたオブジェクトやハッシュを検出から除外します。指定したパスの検査は行いますが、ルールに定められたオブジェクトやハッシュを検出から除外します。

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



【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。

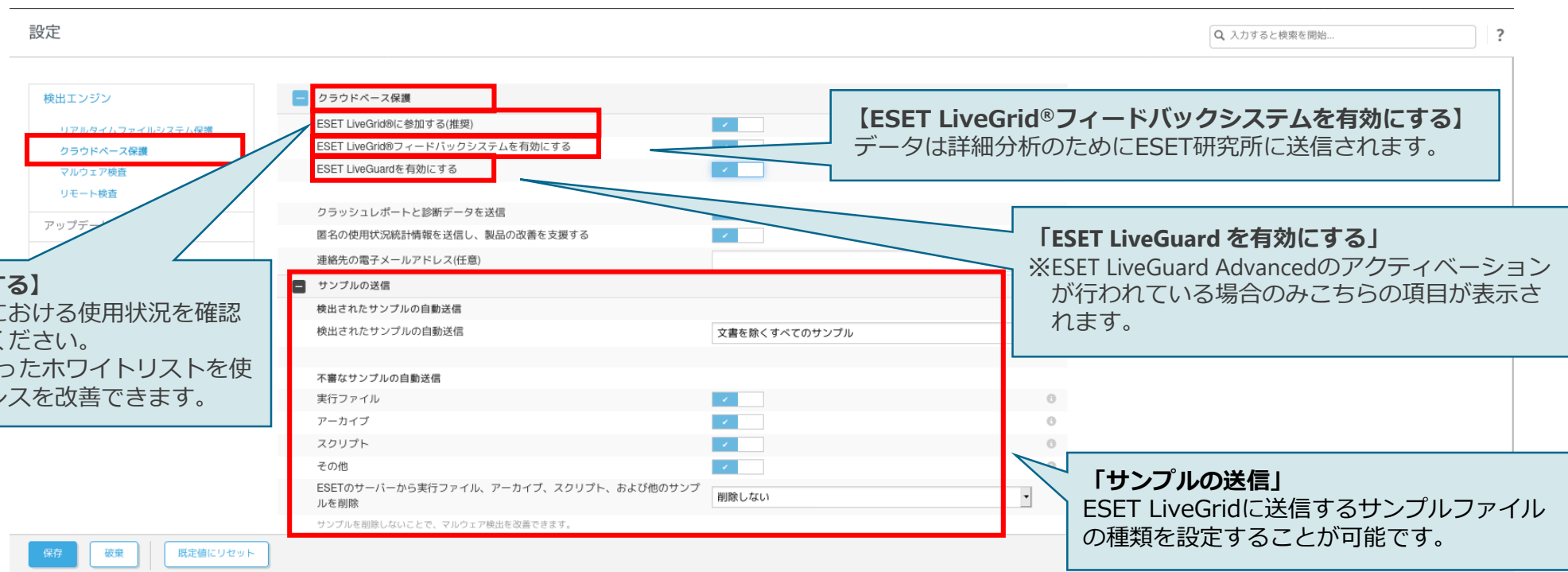
■ RHEL / CentOS / Amazon Linux2の場合 : Kernel, kernel-devel, kernel-headers ■ SUSEの場合 : kernel-default, kernel-default-devel, kernel-devel, kernel-macros

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



設定

検索 入力すると検索を開始...

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
- アップデイト

クラウドベース保護

- ESET LiveGrid®に参加する(推奨) ☒
- ESET LiveGrid®フィードバックシステムを有効にする ☒
- ESET LiveGuardを有効にする ☒

クラッシュレポートと診断データを送信 ☒
匿名の使用状況統計情報を送信し、製品の改善を支援する

連絡先の電子メールアドレス(任意)

サンプルの送信

検出されたサンプルの自動送信 ☒ 文書を除くすべてのサンプル

検出されたサンプルの自動送信 ☒

不審なサンプルの自動送信

実行ファイル ☒

アーカイブ ☒

スクリプト ☒

その他 ☒

ESETのサーバーから実行ファイル、アーカイブ、スクリプト、および他のサンプルを削除 ☒ 削除しない

サンプルを削除しないことで、マルウェア検出を改善できます。

保存 破棄 既定値にリセット

【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

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) link; '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 '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) checked; '駆除' (Removal) with '駆除レベル' (Removal level) set to '厳密な駆除' (Thorough removal); and '除外' (Exclusions) with a red box around '検査対象外とするファイル拡張子' (File extensions to exclude from inspection).

【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-インターフェイス

スケジュール

タスク

ウォッチドッグ

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ル設定画面①

オンデマンド検査スケジュール

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

コンピューターがオフの場合、コンピューター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。

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。

■ オンデマンド検査スケジュール設定画面②

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

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



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。

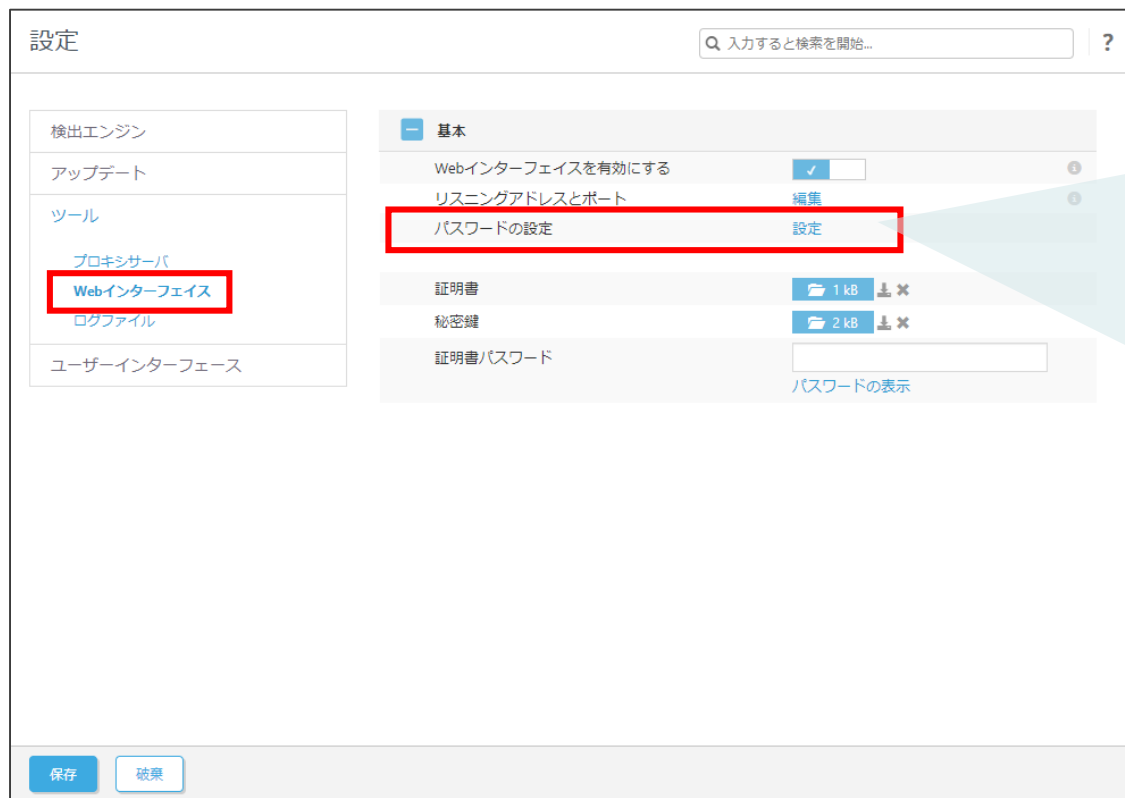
プロキシサーバで認証が必要な場合は、**【プロキシサーバは認証が必要】**にチェックを付け、有効なユーザー名とパスワードを入力します。

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

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

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

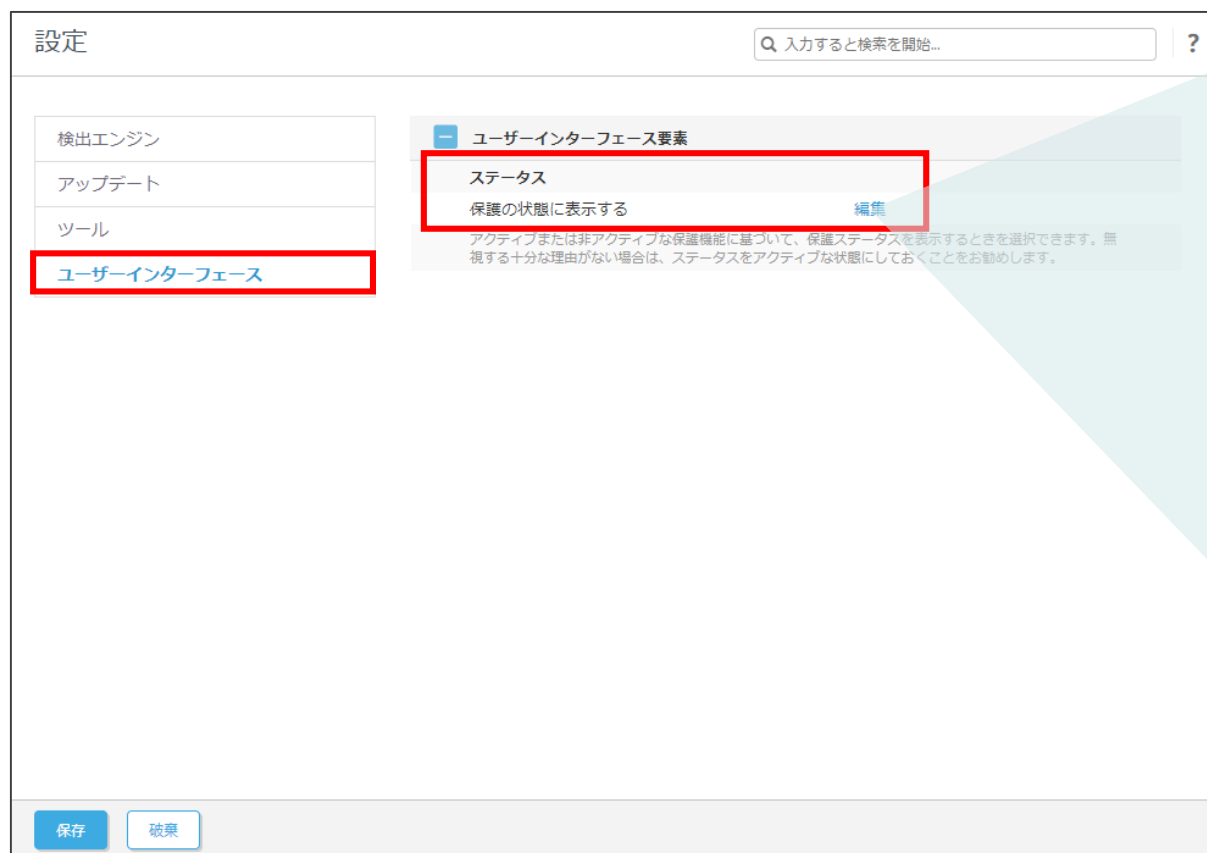
- 【重大な警告】** : 重大なエラー(ウイルス対策の起動に失敗したなど)が含まれます。
- 【エラー】** : 「ファイルのダウンロード中にエラーが発生しました」といったエラーや重大な警告が記録されます。
- 【警告】** : 重大なエラーと警告メッセージとエラーが記録されます。
- 【情報レコード】** : アップデートの成功メッセージを含むすべての情報メッセージと上記のすべてのレコードが記録されます。
- 【診断レコード】** : プログラムおよび上記のすべてのレコードを微調整するのに必要な情報が含まれます。

3. 詳細設定について

(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



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 LIVEGUARD

ESET LiveGuardが有効ですが、アクティベーションされていません ☒

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 ☐

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 ☒

ESET LiveGrid® レビューシステムが無効です ☒

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が無効です ☒

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 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/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=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

- 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。

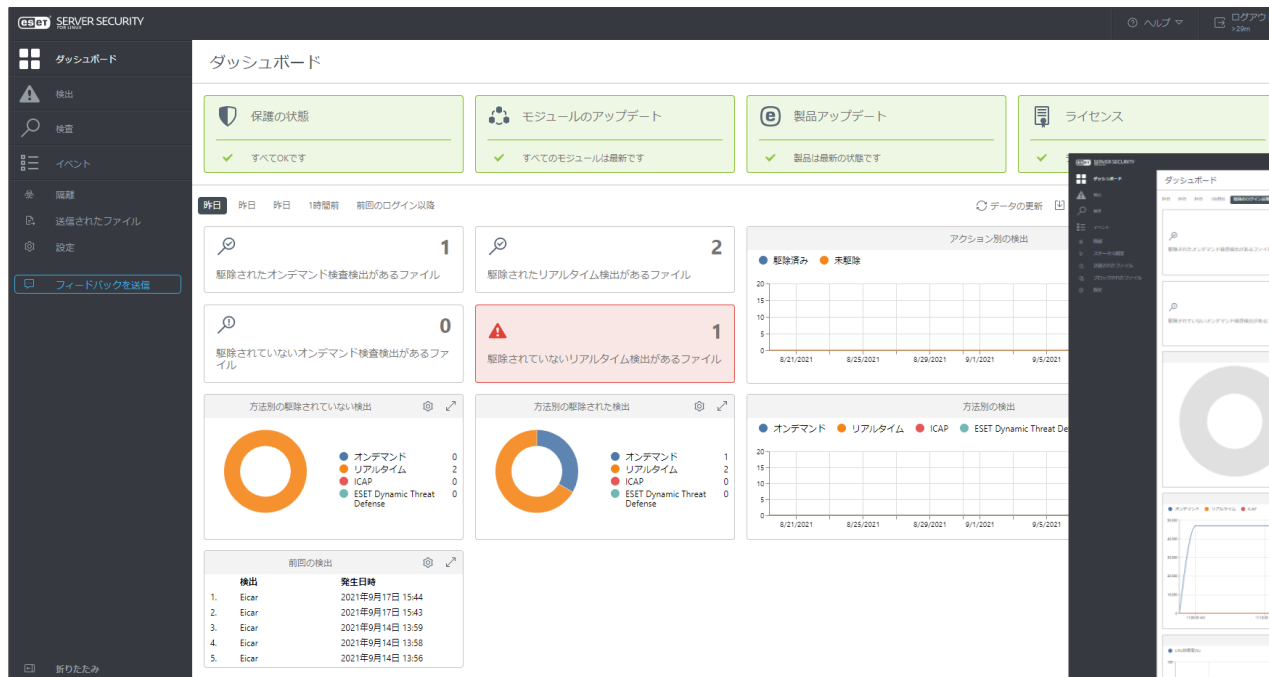
※インストールにはroot権限(スーパーユーザー)が必要です。

4. ESSLの仕様について

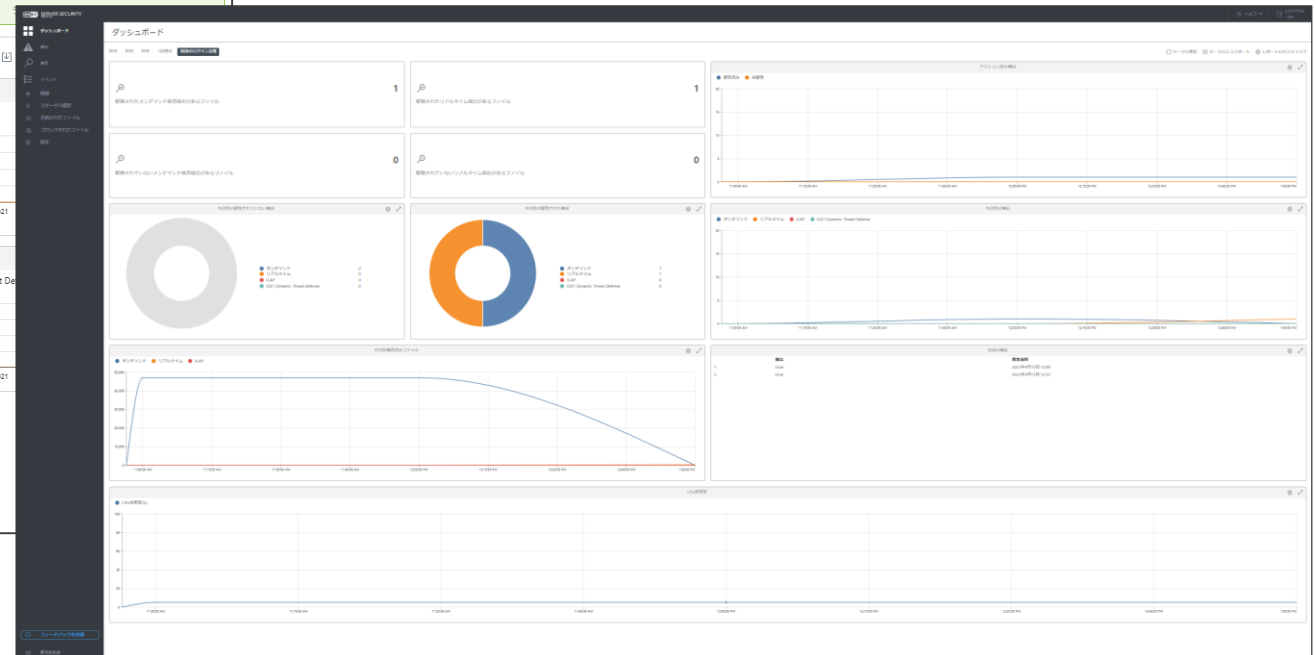
(2)ダッシュボードについて

- ESSL 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

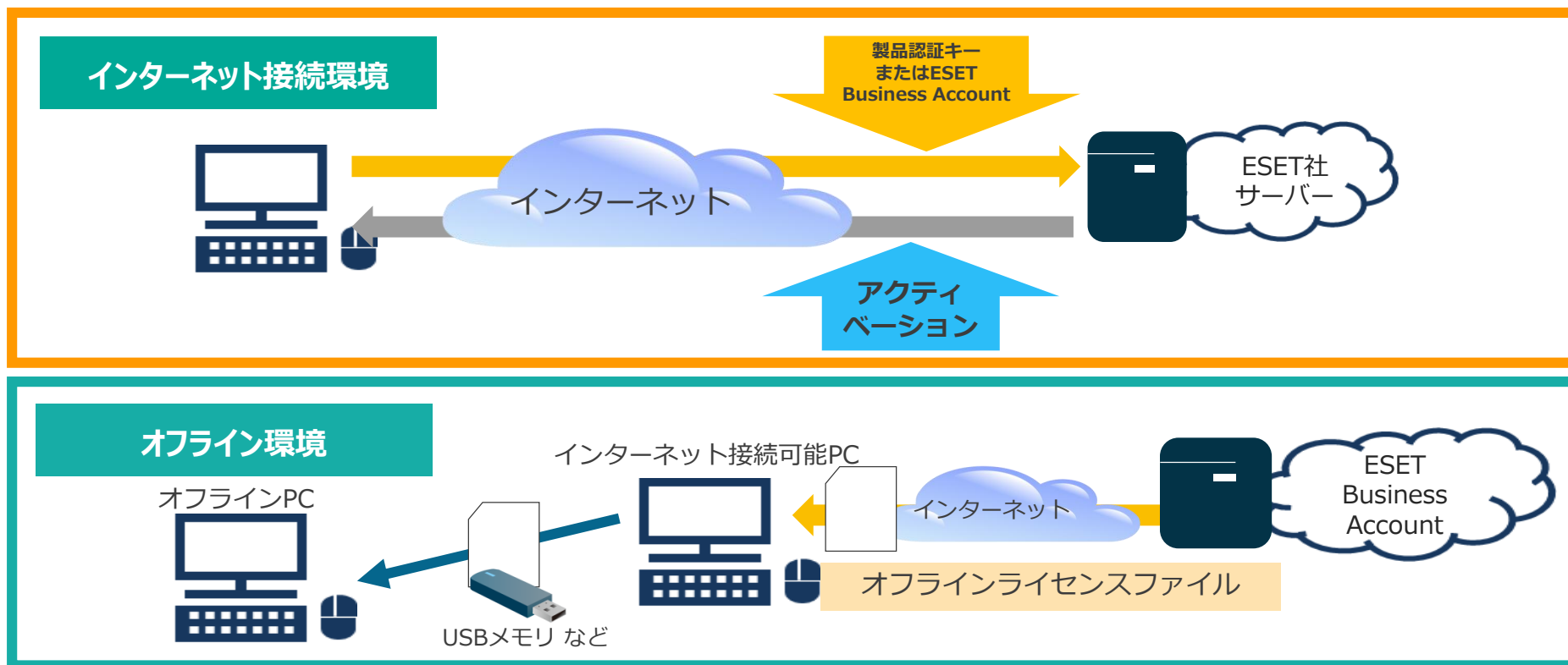


※デフォルトでは非表示です。

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



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)

ESET Business Account
ESET Business Accountからライセンスをアクティベーションします。セキュリティ管理専用情報も入力できます。

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。

「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限: 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。