ESET Endpoint アンチウイルス for Linux V10.X
機能紹介資料

第4版

2024年6月25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クライアント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 Endpoint アンチウイルス for Linux　V10.X （略称表記：EEAL）	Linux クライアント用　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ウド型セキュリティ管理ツールESET PROTECT、オンプレミス型セキュリティ管理ツール ESET PROTECT on-prem※にて管理が可能です。また、各セキュリティ管理ツールの機能紹介は別資料でご用意しております。
　※オンプレミス型セキュリティ管理ツールはv9.0以降で管理することができます。
　※オンプレミスセキュリティ管理ツールはバージョンによって以下の通り名称が異なります。
　　v10.X以前はESET PROTECT
　　v11.X以降はESET PROTECT on-prem

・ セキュリティ管理ツールは、「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サーバーOS向けのプログラムもご使用いただけます。

目次

サポート環境

1. サポート環境

項目	条件	備考
OS	Ubuntu 18.04 LTS（64bit） Ubuntu 20.04 LTS（64bit） Ubuntu 22.04 LTS（64bit） Ubuntu 24.04 LTS（64bit） ※	※ EEAL v10.3以降対応
CPU	Intel,AMD(64bit)	
ハードディスク	700MB以上	
必要ソフトウェア	3.10.0 以降のLinux OS カーネルバージョン glibc 2.12 または それ以上のバージョン	
AppArmorへの対応	非対応	既定で有効になっている AppArmor は、無効、またはアンインストールしてください ※ AppArmorが有効の場合、正常に動作しない場合があります。
セキュアブートへの対応	対応	
サポートデスクトップへの対応	対応（GNONE 3.28.2以降、KDE、XFCE、MATE)	
SELiniuxへの対応	非対応	
その他	Open SSL 1.1.1以降	Open SSL 1.1.1以降がインストールされていない場合、コマンド実行が失敗し正常に機能しません。
	UTF-8エンコーディングを使用する任意のロケール	

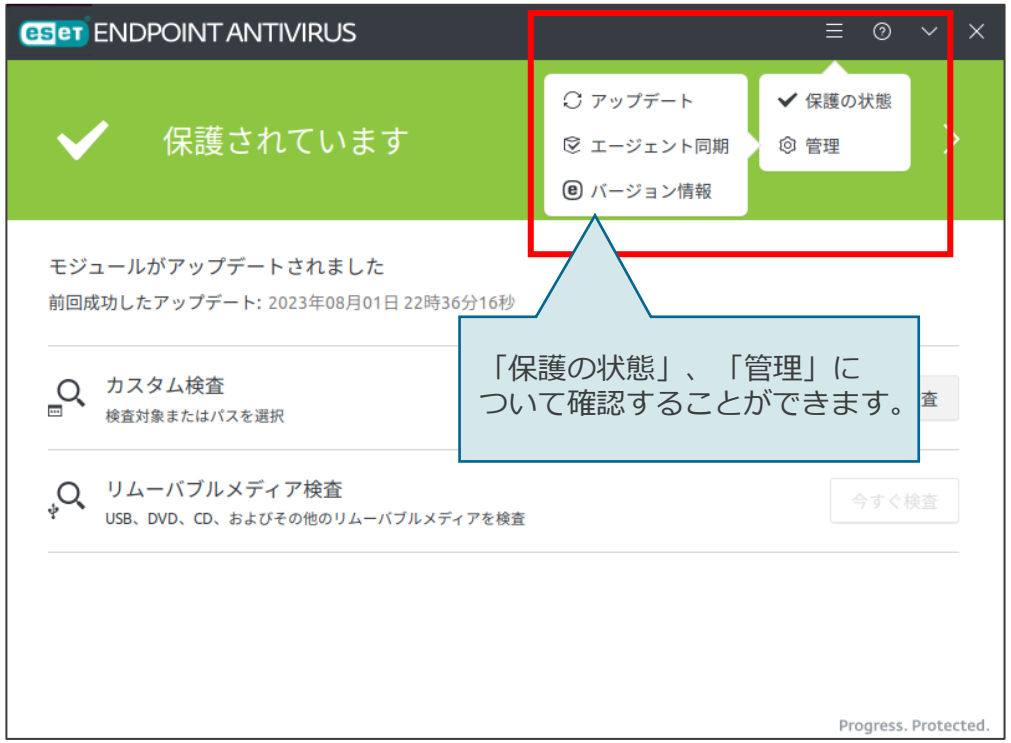
インターフェースについて

2. インターフェースについて

（1）初期画面

- インターフェースは、端末のデスクトップメニュー内のESETアイコンから起動することができます。
  すべて問題なく動作している場合、保護の状態は緑色で表示されます。システムの保護の状態を改善するオプションがある場合、または保護の状態が不十分な場合は、赤色で表示されます。

■正常な保護状態の初期画面



■セキュリティアラートが表示されている状態の初期画面

2. インターフェースについて

（2）保護の状態

- 「保護の状態」では機能している保護機能や検出エンジンなどに関するアラートを表示します。

■保護の状態

2. インターフェースについて

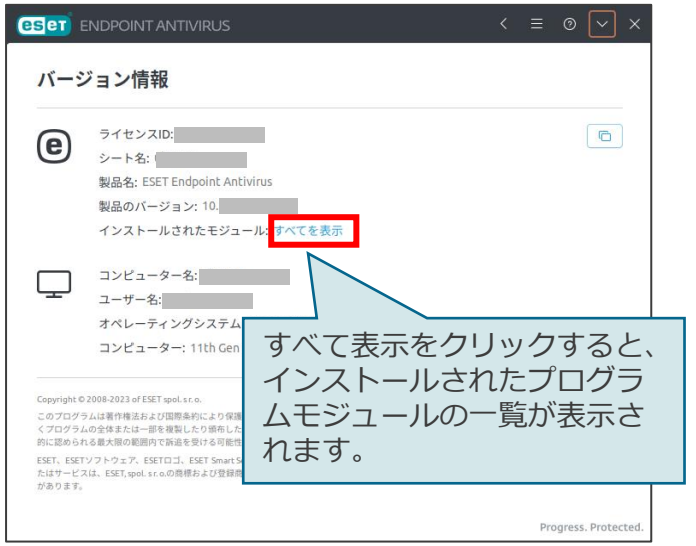
（3）管理

- 「管理」では以下の項目を確認することができます。
  - ・アップデート　　：アップデート状況やモジュール情報が表示されます
  - ・エージェント同期：セキュリティ管理ツールで管理する場合にその通信情報が表示されます
  - ・バージョン情報　：ライセンス情報やインストールされた製品のバージョン、OSなどの情報が表示されます

■アップデート

■エージェント同期

■バージョン情報

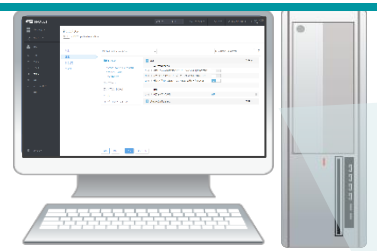


詳細設定について

3. 詳細設定について

EEAL V10.Xの設定方法に関して

- EEAL V10.Xでは、クライアント端末上のインターフェースやコマンドラインから設定を行うことはできません。
  設定を行う場合は、セキュリティ管理ツールのポリシー機能を使用します。
  ※クライアント端末にはESET Management エージェントがインストールされ、セキュリティ管理ツールで管理されている必要があります。



セキュリティ管理ツール

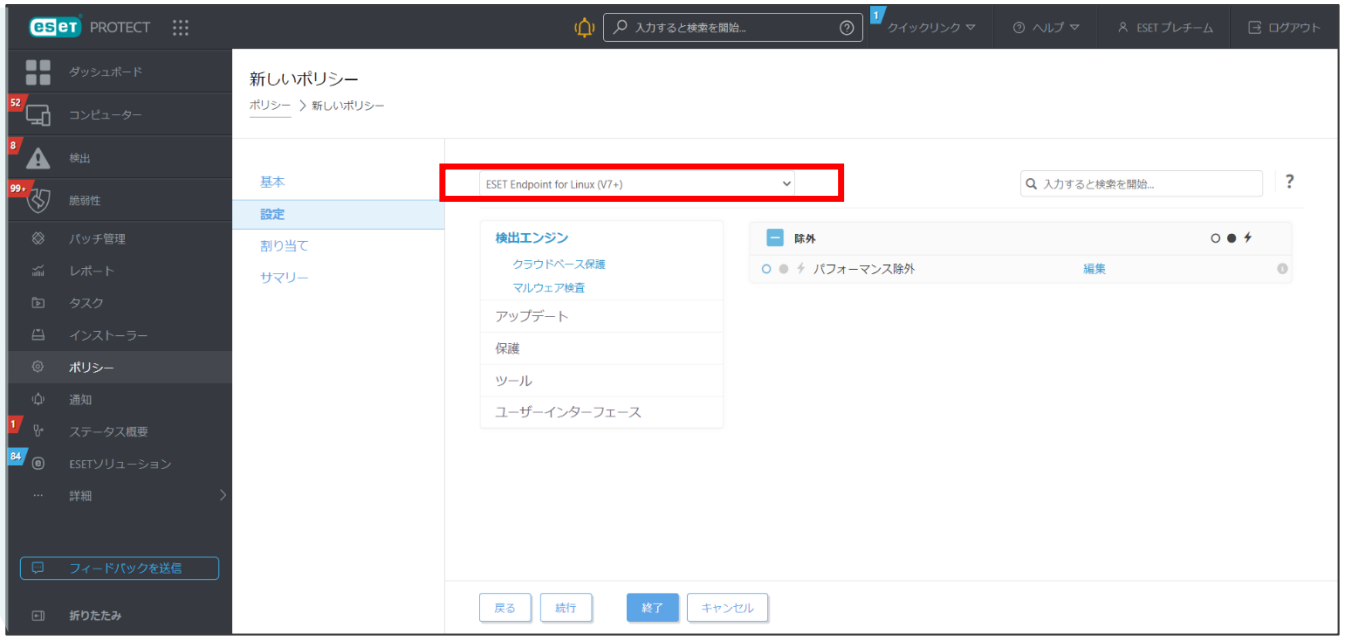
ポリシー

クライアント端末

ESET Management エージェント

ESET Endpoint Antivirus for Linux

■ポリシー作成画面 ※ポリシー作成時の製品名はESET Endpoint for Linux (V7+)を選択します。



◆クラウド型セキュリティ管理ツールを利用して、新しいポリシーを作成する手順
https://eset-support.canon-its.jp/faq/show/21747?site_domain=business

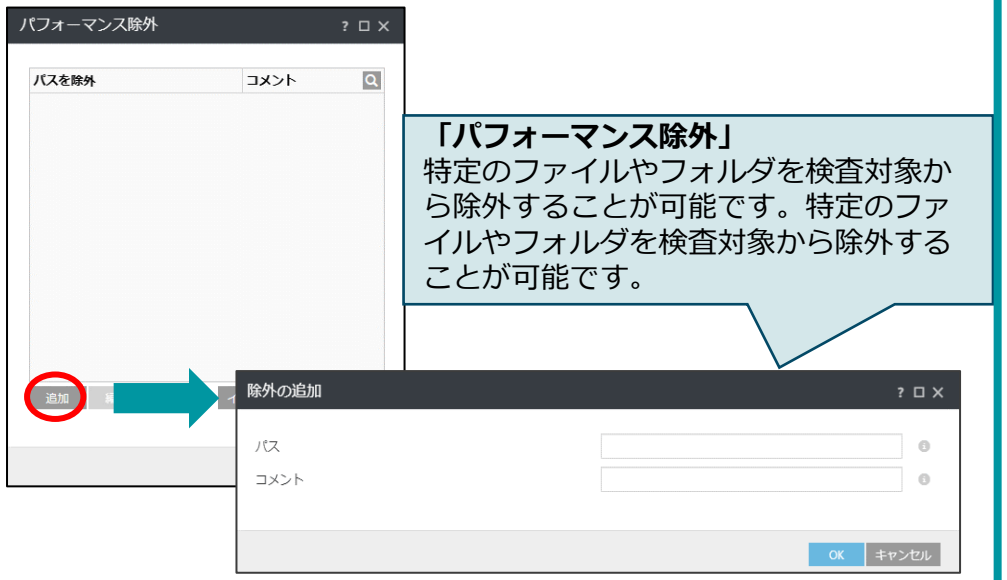
3. 詳細設定について

（1）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



※セキュリティ管理ツールを使用した検出の除外方法は本資料P23をご確認ください。

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。

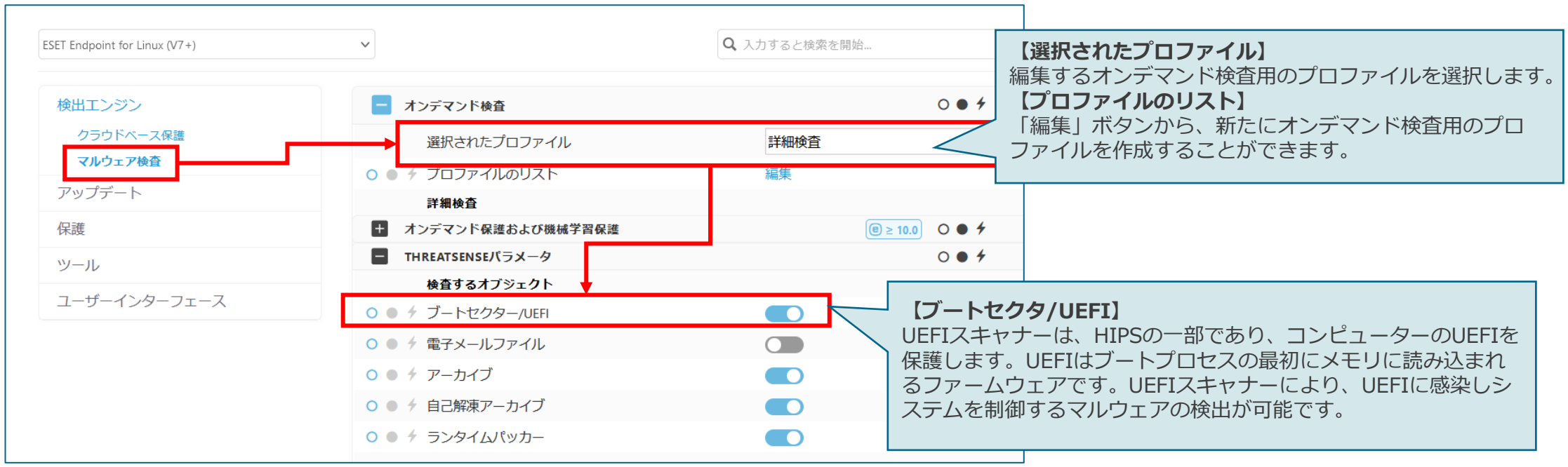
「サンプルの送信」
ESET LiveGrid ®に送信するサンプルファイルの種類を設定することが可能です。

3. 詳細設定について

（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



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

【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。

■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

※セキュリティ管理ツールからモジュールロールバックを行う場合は、「モジュールアップデートロールバック」タスクを使用します。
https://help.eset.com/protect_cloud/ja-JP/client_tasks_database_update_rollback.html

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。

■保護設定画面

「マルウェア検出（機械学習を利用）」
検出エンジンモジュールと機械学習コンポーネントを組み合わせて実行されます。

「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。

「疑わしい可能性があるアプリケーション」
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。

「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。

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

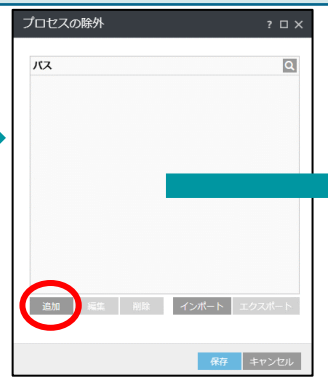
- リアルタイムファイルシステム保護を使用すると、ファイルのオープン時や作成時、また実行時に検査を行うことが可能です。リアルタイムファイルシステム保護はシステム起動時に開始され、中断することなく常に端末を保護します。

■リアルタイムファイルシステム保護設定画面

【ローカルドライブ】　：システムハードディスクと固定ハードドライブをすべて検査
【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ルメディアの自動検査を有効または無効にします。

【プロセス除外】(V8.1以降のみ利用可能)
除外されたアプリケーションプロセスに起因するすべてのファイル操作は検査から除外されます。バックアップツールを使用する際のバックアップ速度改善などに有効です。



■プロセス除外設定画面

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。

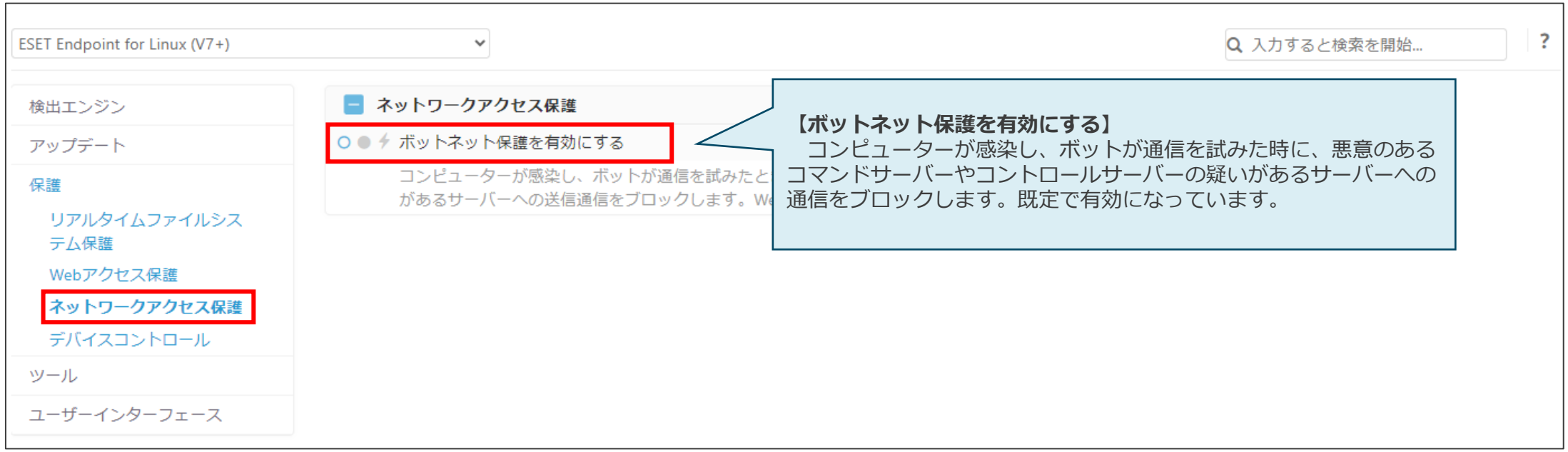
■Webアクセス保護設定画面

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。※EEAL V10.2以降で使用できる機能です

■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

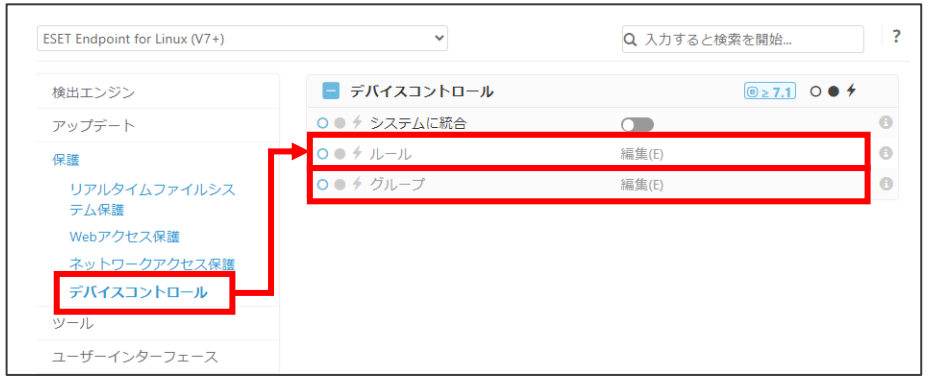
（9）デバイスコントロール

- デバイスコントロール機能を使用することで、CD/DVDドライブ、USB接続のストレージデバイスの利用を制御することが可能です。望ましくないコンテンツを収めたデバイスをユーザーが使用することを防止したい場合や、機密情報を含むファイルなどを持ち出されることを防ぐことが可能です。

■設定可能なデバイスのタイプとアクション

デバイスタイプ	アクション		
	読み込み/書き込み	読み取り専用	ブロック
すべてのデバイスタイプ	○	○	○
ディスクストレージ	○	○	○
CD/DVD	○	○	○

■デバイスコントロール設定画面



■デバイスコントロール設定

(例)デバイスコントロールブロックメッセージ

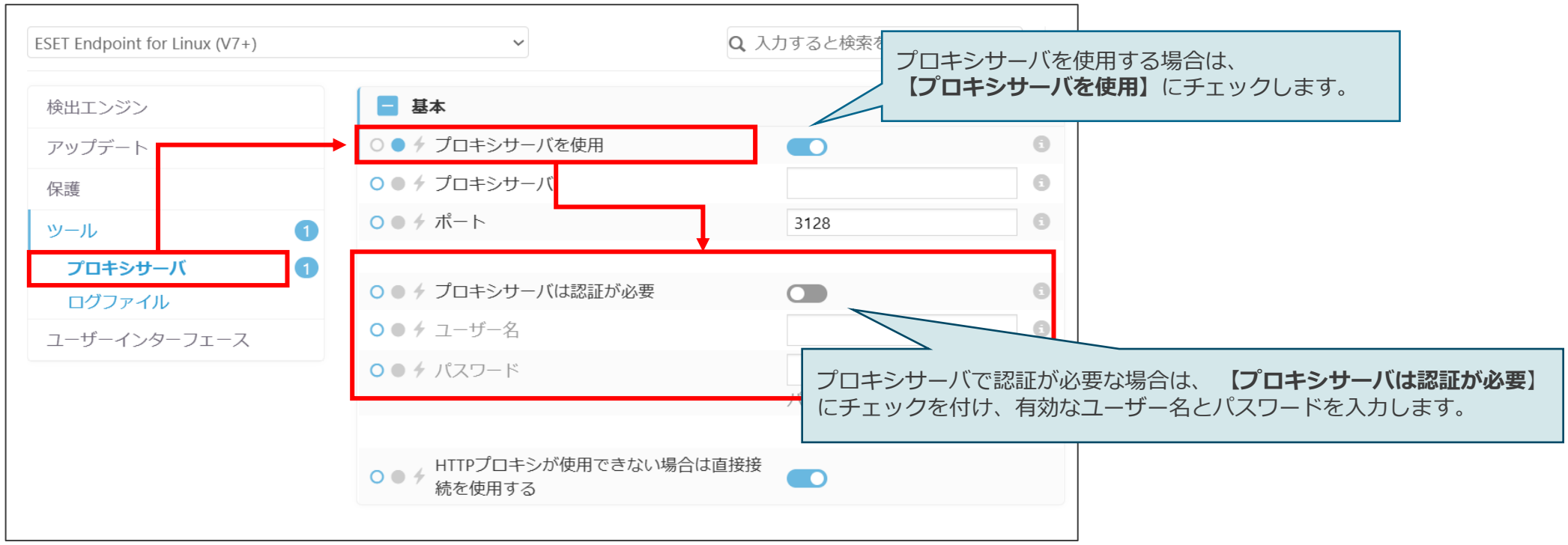
(例)デバイスコントロール読み取り専用メッセージ

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

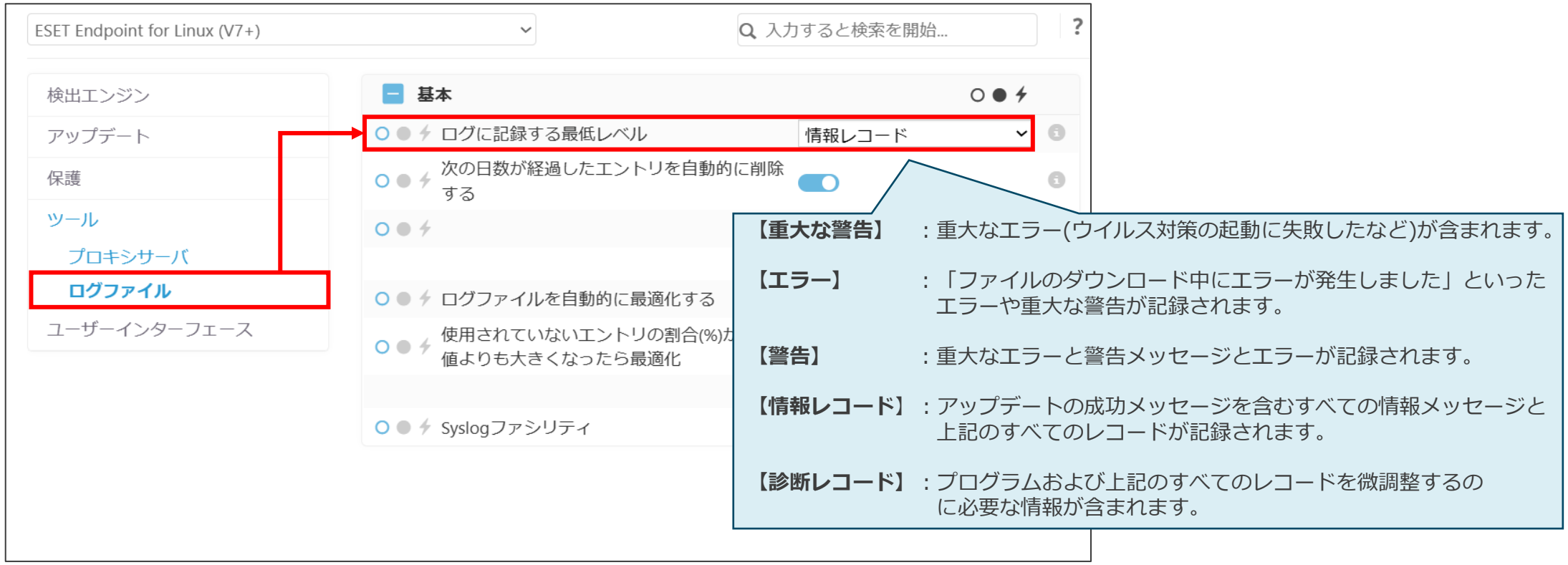


3. 詳細設定について

（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



【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

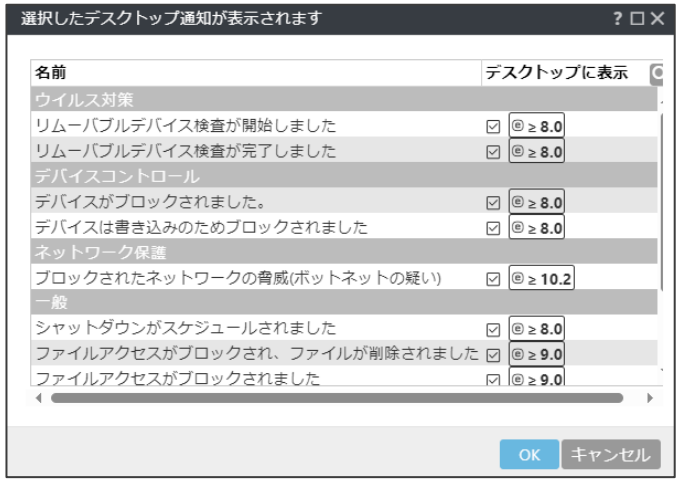
（12）ユーザーインターフェース

- ユーザーインターフェースでは、保護状態に関する通知をデスクトップや管理コンソール上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

■アプリケーション通知設定画面



3. 詳細設定について

（参考）コマンドラインベースの操作

- 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/eea/bin/odscan [OPTIONS]

・**製品モジュールをアップデート**
/opt/eset/eea/bin/upd [OPTIONS]

・**隔離された項目の管理**
/opt/eset/eea/bin/quar [OPTIONS]

・**イベント画面の内容を表示**
/opt/eset/eea/sbin/lslog [OPTIONS]

・**設定のエクスポート**
/opt/eset/eea/lib/cfg --export-xml=/tmp/export.xml

・**設定のインポート**
/opt/eset/eea/lib/cfg --import-xml=/tmp/export.xml

【コマンド例】
・複数の対象に関して“@Smart scan”検査プロファイルを使用して検査を実行
/opt/eset/eea/bin/odscan --scan --profile=“@Smart scan” /root/* /tmp/*

・モジュールのロールバック
/opt/eset/eea/bin/upd --update --rollback=“時間“

・ターミナルウィンドウから隔離ファイルを検出除外する
/opt/eset/eea/bin/quar -e “隔離ファイルのID” --restore-path=“復元先のパス”

・すべてのイベントログを出力する
/opt/eset/eea/sbin/lslog -e

・オンデマンド検査ログのリストを出力します
/opt/eset/eea/sbin/lslog --scans

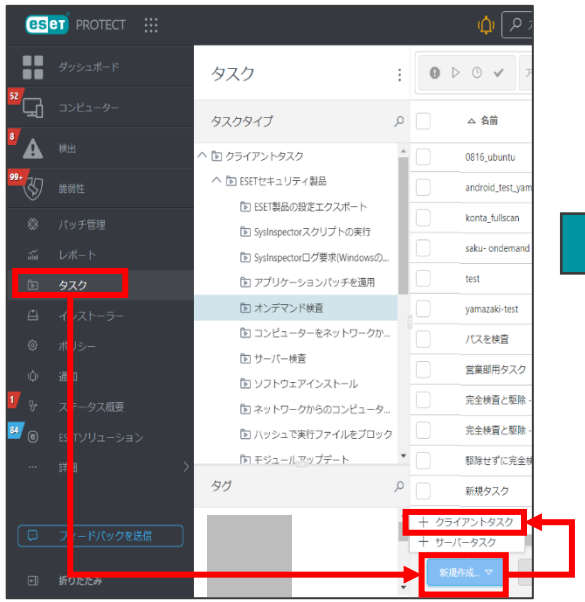
※詳細に関しては以下のURLをご確認ください。
https://help.eset.com/eeau/10/ja-JP/gui.html?using_eset_security_product.html

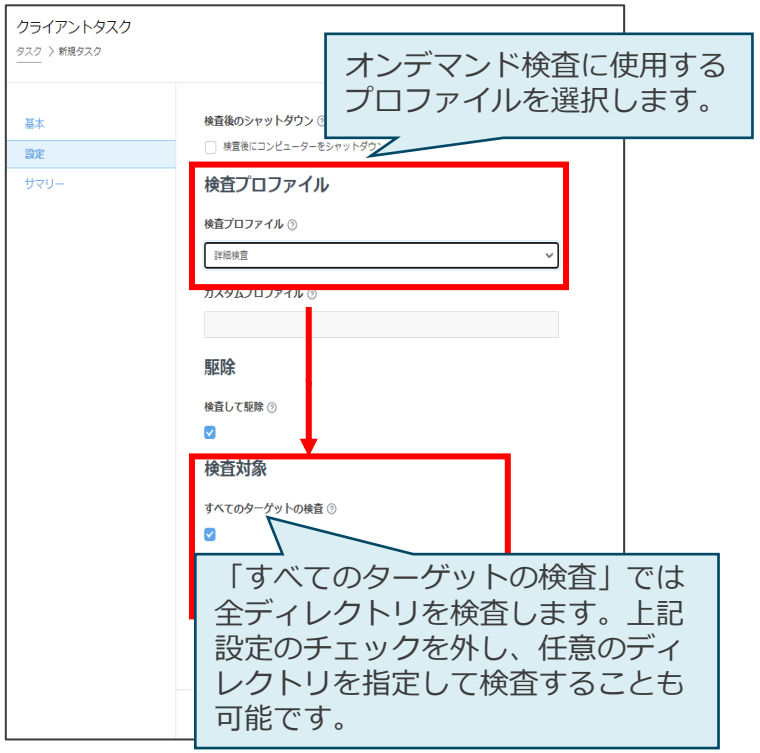
3. 詳細設定について

（参考）定期的なオンデマンド検査

- セキュリティ管理ツールを使用してEEAL V10.Xで定期的にファイルの検査をさせるには、クライアント端末にスケジュール検査をタスクで配布します。

■オンデマンド検査タスク設定画面

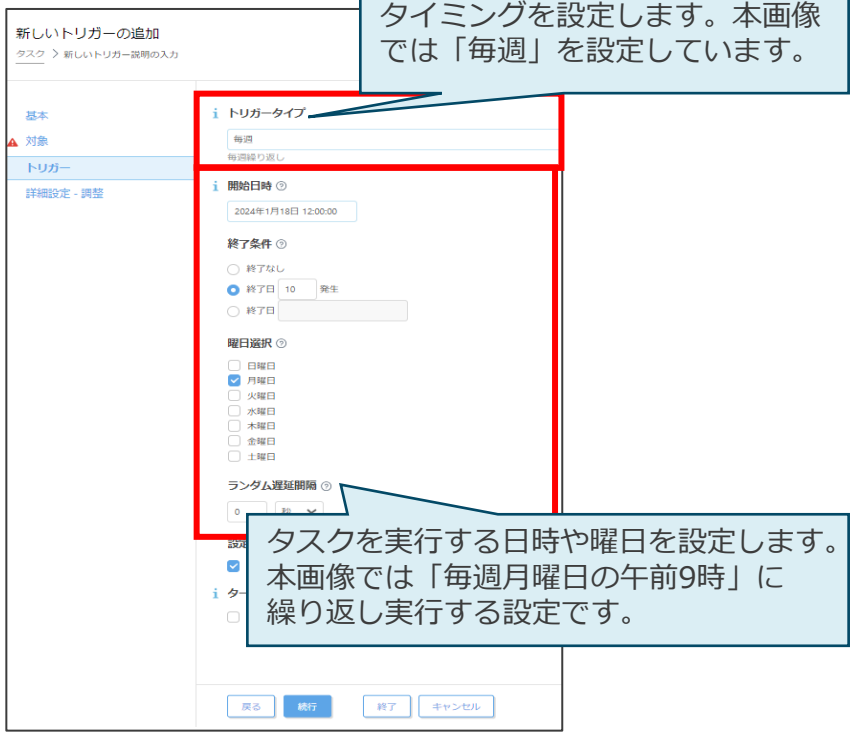




オンデマンド検査に使用するプロファイルを選択します。

「すべてのターゲットの検査」では全ディレクトリを検査します。上記設定のチェックを外し、任意のディレクトリを指定して検査することも可能です。

■トリガー設定画面



トリガータイプではタスクの実行タイミングを設定します。本画像では「毎週」を設定しています。

タスクを実行する日時や曜日を設定します。本画像では「毎週月曜日の午前9時」に繰り返し実行する設定です。

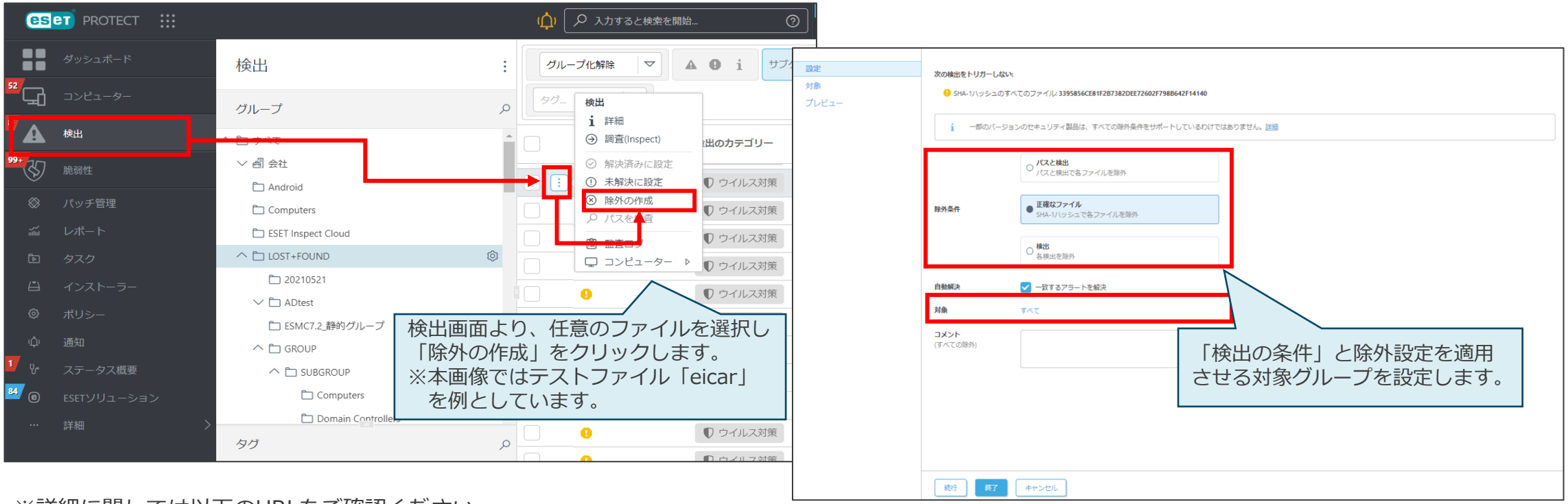
◆クライアントに対して定期的にファイルの検査をさせるには？
https://eset-support.canon-its.jp/faq/show/100?site_domain=business

3. 詳細設定について

（参考）検出除外の設定方法

- EEAL V10.Xで検出されたファイルを次回の検査から除外したい場合は、セキュリティ管理ツールの検出一覧から任意のファイルを選択し「検出の除外」を実施します。

■除外設定画面



※詳細に関しては以下のURLをご確認ください。
https://help.eset.com/protect_cloud/ja-JP/?create_exclusion.html