

ESET Endpoint アンチウイルス for Linux V11.X 機能紹介資料

第2版

2024年10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 V11.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を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v9.1以降で管理することができます。
- ・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

1. サポート環境
2. インターフェースについて
3. 詳細設定について

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)	※V11.1は対象外
CPU	Intel,AMD(64bit)	
ハードディスク	700MB以上	
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 (GNOME 3.28.2以降、KDE、XFCE、MATE)	
SELinux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	
	サポートしている言語は日本のみ	
	管理ツールで管理する場合の要件は以下の通りです。 ・セキュリティ管理ツール ： ESET PROTECT、ESET PROTECT On-PremV9.1以降※ ・管理エージェント ： ESET Management Agent V10.0以降※	※ESET PROTECT On-Prem V9.1を使用する場合は、ESET Management Agent V10.1以降が必要

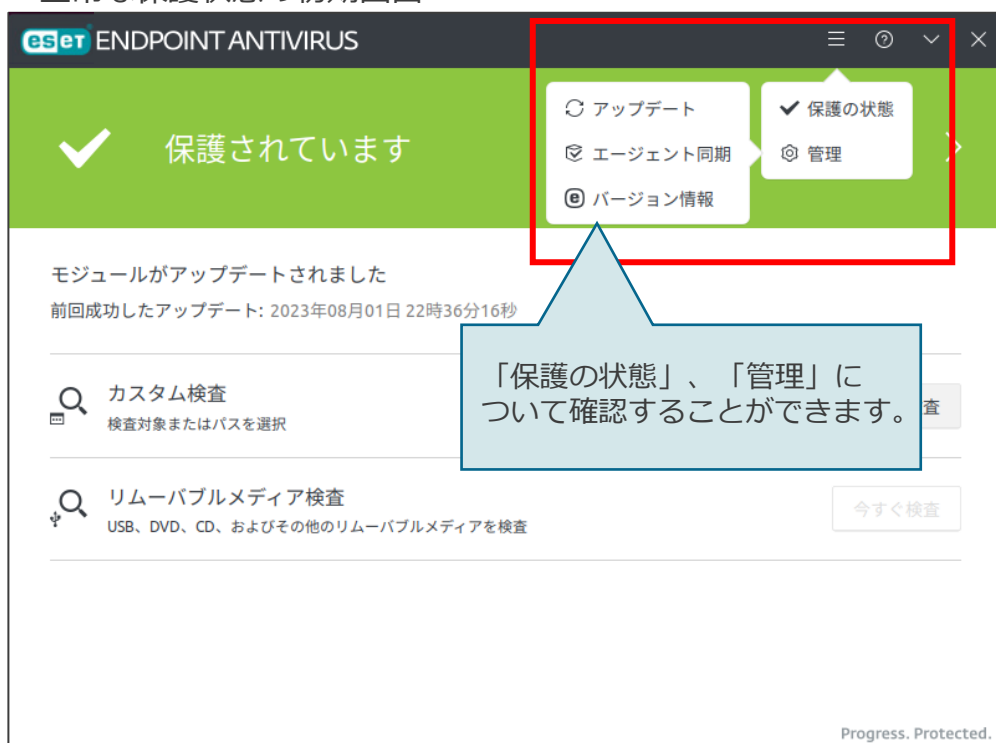
インターフェースについて

2. インターフェースについて

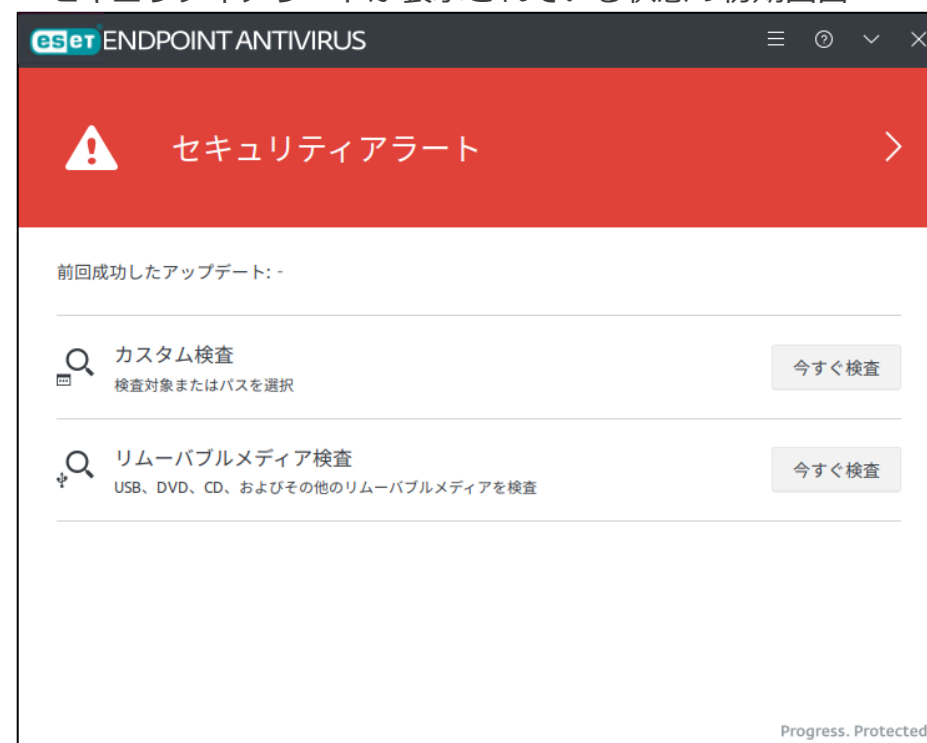
(1) 初期画面

- 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

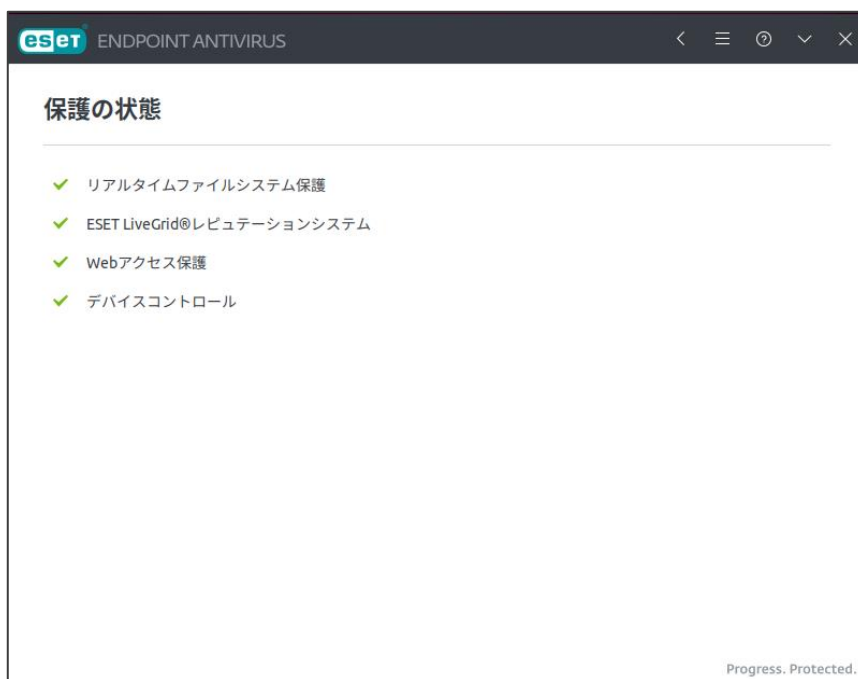


2. インターフェースについて

(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 V11.Xの設定方法に関して

- EEAL V11.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

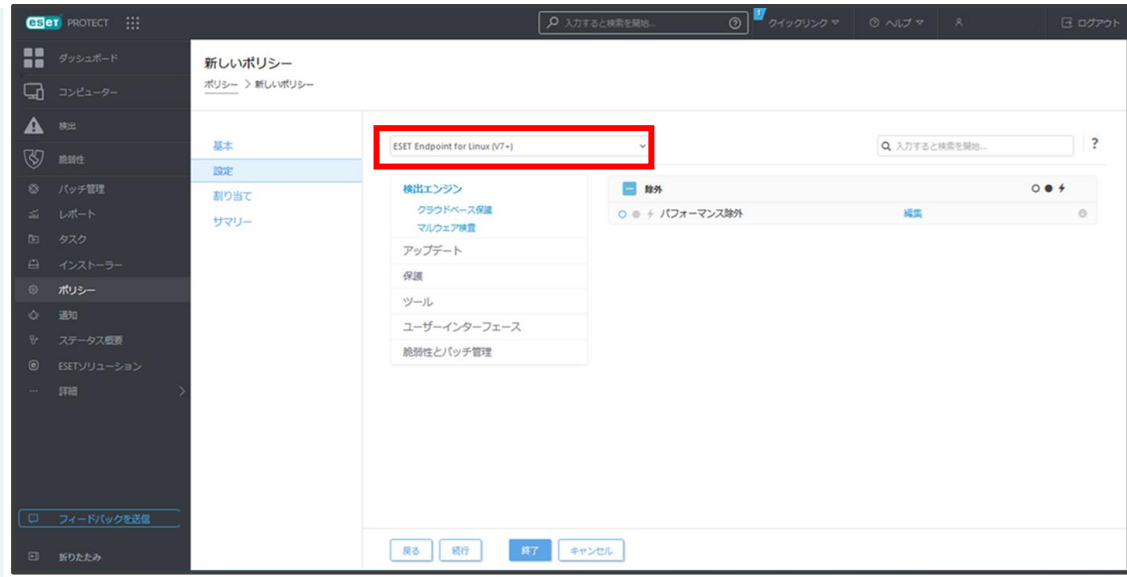
ポリシー

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



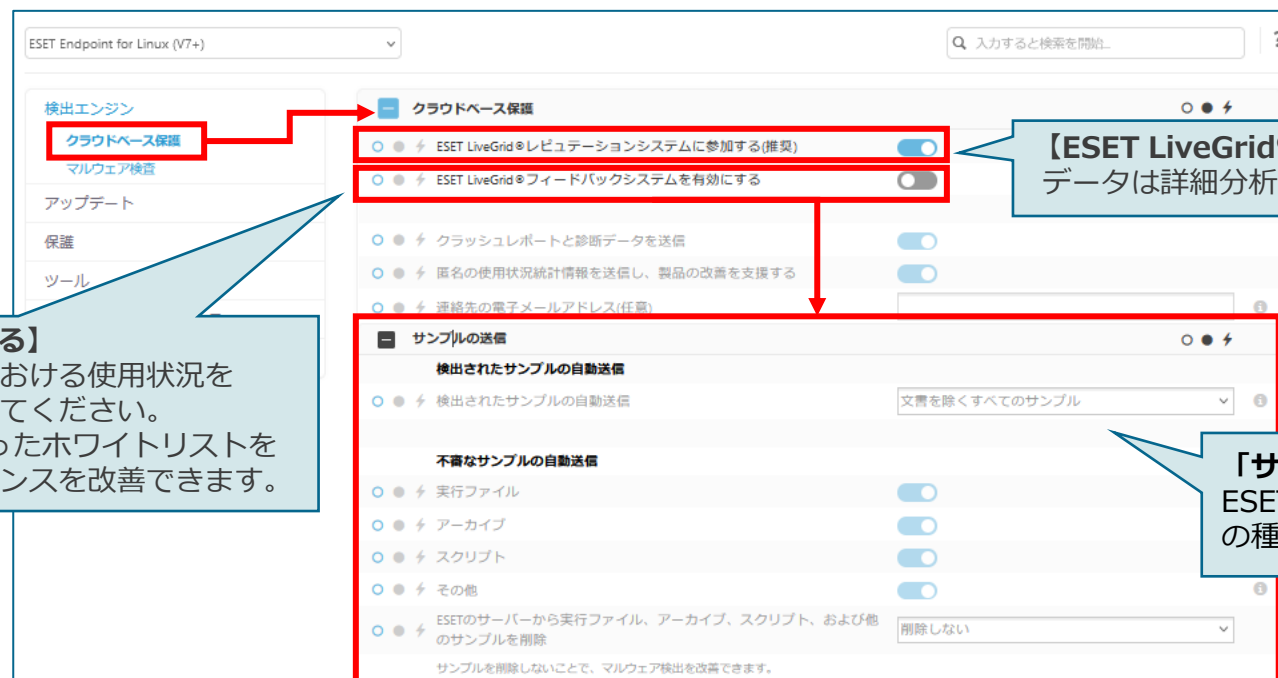
※セキュリティ管理ツールを使用した検出の除外方法は本資料P26をご確認ください。

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

(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

(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世代分のスナップショットを保存します。

【自動アップデート】
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

検出エンジン	検出応答	最大	標準	最小	オフ
マルウェア検出(機械学習を利用)	報告	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
	保護	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
望ましくない可能性があるアプリケーション	報告	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
	保護	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
疑わしい可能性があるアプリケーション	報告	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
	保護	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
安全ではない可能性があるアプリケーション	報告	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
	保護	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

「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。

【プロセス除外】
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

除外の追加
 プロセス実行ファイルを選択し(path/to/executableの形式)
 ファイルパスを指定
 保存 キャンセル

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



ESET Endpoint for Linux (V7+)

検出エンジン

アップデート

保護

- リアルタイムファイルシステム保護
- Webアクセス保護**
- ネットワークアクセス保護
- デバイスコントロール

ツール

ユーザーインターフェース

脆弱性とパッチ管理

WEBアクセス保護

- Webアクセス保護を有効にする
- 対象外のアプリケーション [編集](#)
- 除外されたIP [編集](#)
- +** URLアドレス管理 Ⓜ ≥ 10.0 ⚡
- +** HTTPSトラフィック検査 Ⓜ ≥ 10.0 ⚡
- +** THREATSENSEパラメータ Ⓜ ≥ 10.0 ⚡

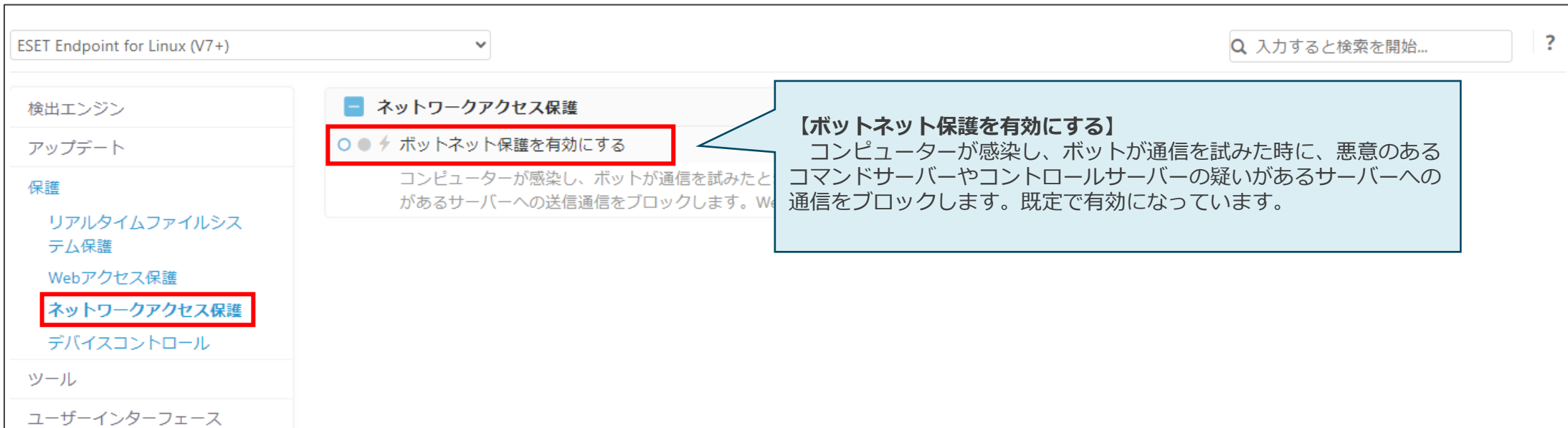
【Webアクセス保護を有効にする】
Webブラウザとリモートサーバー間のHTTPおよびHTTPS通信を監視します。既定で有効になっています。Webアクセス保護を有効にすることを強くお勧めします。

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



ESET Endpoint for Linux (V7+)

ネットワークアクセス保護

⚡ ボットネット保護を有効にする

コンピューターが感染し、ボットが通信を試みたとき、悪意のあるサーバーへの送信通信をブロックします。Webアクセス保護を有効にする必要があります。

【ボットネット保護を有効にする】
 コンピューターが感染し、ボットが通信を試みた時に、悪意のあるコマンドサーバーやコントロールサーバーの疑いがあるサーバーへの通信をブロックします。既定で有効になっています。

検出エンジン
 アップデート
 保護
 リアルタイムファイルシステム保護
 Webアクセス保護
ネットワークアクセス保護
 デバイスコントロール
 ツール
 ユーザーインターフェース

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。※SDカードには対応していません。

■ 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		
	許可	ブロック	書き込みブロック
すべてのデバイスタイプ	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ディスクストレージ	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
CD/DVD	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

■ デバイスコントロール設定

ルールの追加

名前: 無題

有効:

デバイスタイプ: すべてのデバイスタイプ

アクション: 許可

条件: デバイス

ベンダー

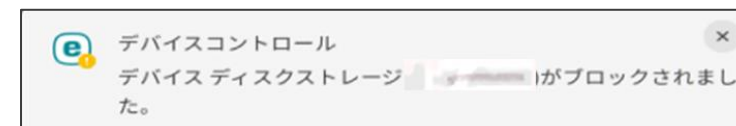
モデル

シリアル番号

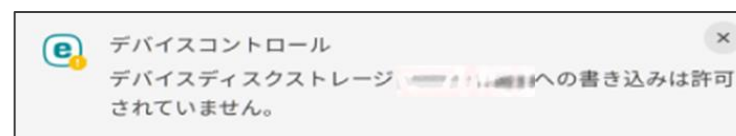
ベンダー、モデル(型番)、シリアルを入力することで詳細な制御が可能です。

OK

(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「書き込みブロック」メッセージ



■ デバイスコントロール設定画面



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



ESET Endpoint for Linux (V7+)

検出エンジン
 アップデート
 保護
 ツール
プロキシサーバ
 ログファイル
 ユーザーインターフェース
 脆弱性とパッチ管理

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
- HTTPプロキシが使用できない場合は直接接続を使用する

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



ESET Endpoint for Linux (V7+) 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

プロキシサーバ

ログファイル

ユーザーインターフェース

脆弱性とパッチ管理

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 ON

○ ● ⚡

○ ● ⚡ ログファイルを自動的に

○ ● ⚡ 使用されていないエントリ

○ ● ⚡ なったら最適化

○ ● ⚡ Syslogファシリティ

- 【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



ESET Endpoint for Linux (V7+)

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
脆弱性とパッチ管理

ユーザーインターフェース要素

通知

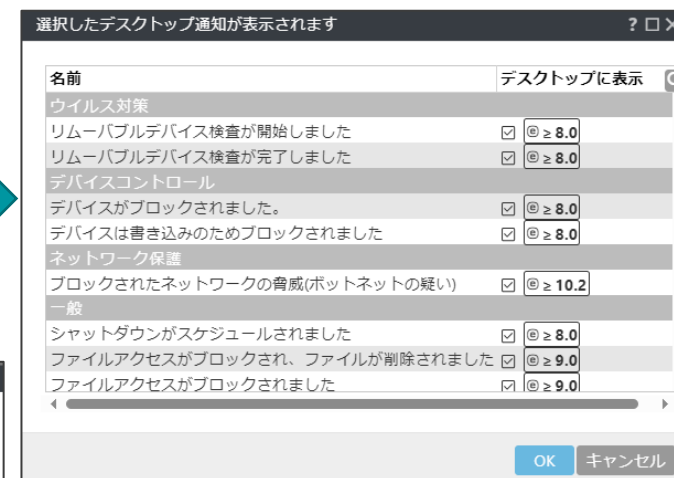
○ ● ⚡ デスクトップに通知を表示する

○ ● ⚡ **アプリケーション通知** @ ≥ 8.0 編集

ステータス

○ ● ⚡ **アプリケーションステータス**

■ アプリケーション通知設定画面



選択したデスクトップ通知が表示されます

名前	デスクトップに表示	バージョン
ウイルス対策		
リムーバブルデバイス検査が開始しました	<input checked="" type="checkbox"/>	@ ≥ 8.0
リムーバブルデバイス検査が完了しました	<input checked="" type="checkbox"/>	@ ≥ 8.0
デバイスコントロール		
デバイスがブロックされました。	<input checked="" type="checkbox"/>	@ ≥ 8.0
デバイスは書き込みのためブロックされました	<input checked="" type="checkbox"/>	@ ≥ 8.0
ネットワーク保護		
ブロックされたネットワークの脅威(ボットネットの疑い)	<input checked="" type="checkbox"/>	@ ≥ 10.2
一般		
シャットダウンがスケジュールされました	<input checked="" type="checkbox"/>	@ ≥ 8.0
ファイルアクセスがブロックされ、ファイルが削除されました	<input checked="" type="checkbox"/>	@ ≥ 9.0
ファイルアクセスがブロックされました	<input checked="" type="checkbox"/>	@ ≥ 9.0

OK キャンセル

■ ステータス設定画面



選択したアプリケーションステータスが表示されます

名前	エンドポイントに表示	管理コンソールに表示
ESET LIVEGUARD		
ESET LiveGuardサーバーに接続できません	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ESET LiveGuardはクラウド接続が制限されています	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ESET LiveGuardライセンスが有効期限切れです	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ライセンスの問題のため、ESET LiveGuardが動作していません	<input type="checkbox"/>	<input checked="" type="checkbox"/>
WEB		
Webアクセス保護が機能していません	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Webアクセス保護が無効になっています	<input type="checkbox"/>	<input checked="" type="checkbox"/>
アップデート		
モジュールアップデートは一時的に停止されました	<input type="checkbox"/>	<input checked="" type="checkbox"/>
古い検出エンジン	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
最新のアップデートの試みが失敗しました	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

OK キャンセル

3. 詳細設定について

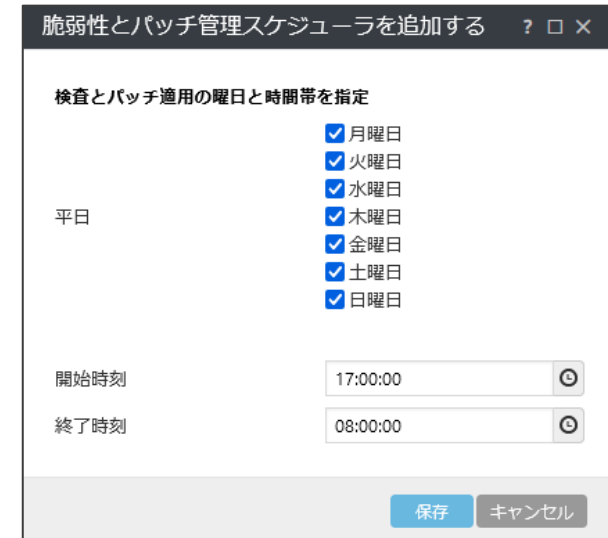
(13) 脆弱性とパッチ管理

- 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。スケジュール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。
 ※パッチ管理は未サポートとなります。(2024年9月現在)

■ 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

- 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/lsllog [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

※詳細に関しては下記URLをご確認ください。

https://help.eset.com/eeau/11/ja-JP/?using_eset_security_product.html

【コマンド例】

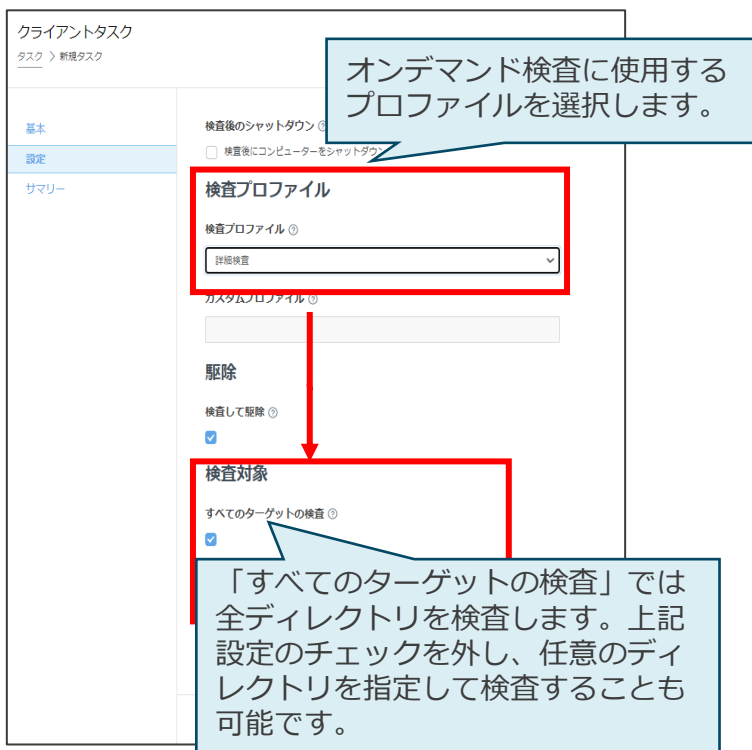
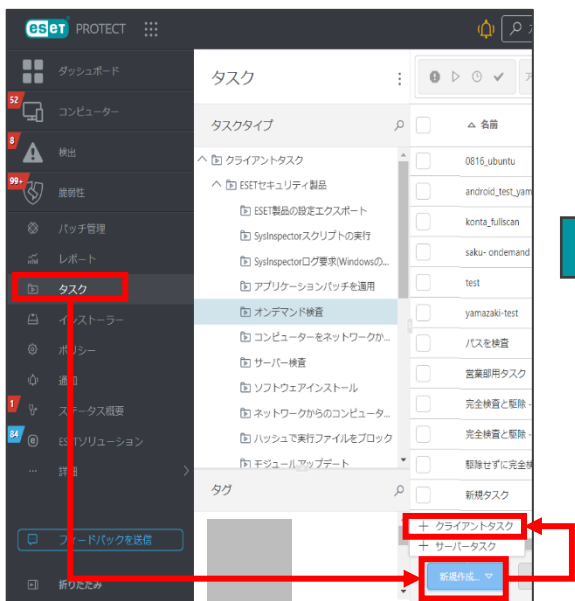
- ・ 複数の対象に関して“@Smart scan”検査プロファイルを使用して検査を実行
/opt/eset/eea/bin/odscan --scan --profile="@Smart scan" /root/* /tmp/*
- ・ モジュールのロールバック
/opt/eset/eea/bin/upd --update --rollback="時間"
- ・ “隔離ファイルのID” を“復元先のパス”へ復元する
/opt/eset/eea/bin/quar -e “隔離ファイルのID” --restore-path="復元先のパス"
- ・ すべてのイベントログを出力する
/opt/eset/eea/sbin/lsllog -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/lsllog --scans

3. 詳細設定について

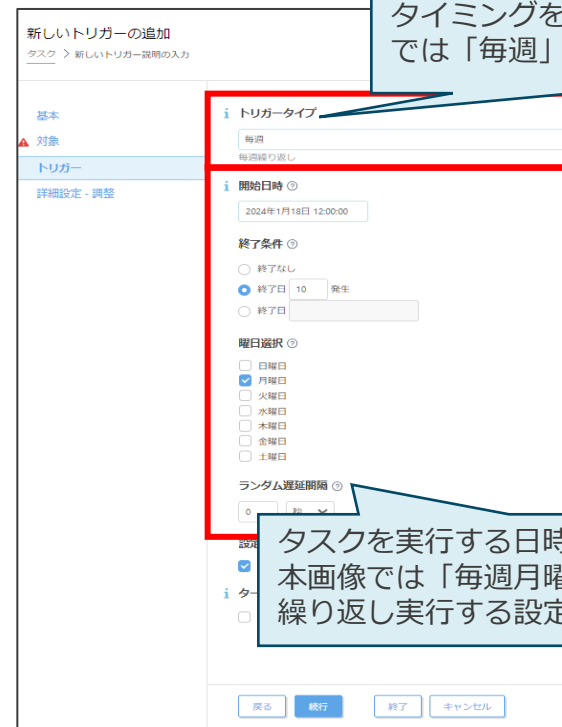
(参考) 定期的なオンデマンド検査

- セキュリティ管理ツールを使用してEEAL V11.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



■ トリガー設定画面



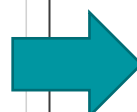
◆クライアントに対して定期的にファイルの検査をさせるには？
https://eset-support.canon-its.jp/faq/show/100?site_domain=business

3. 詳細設定について

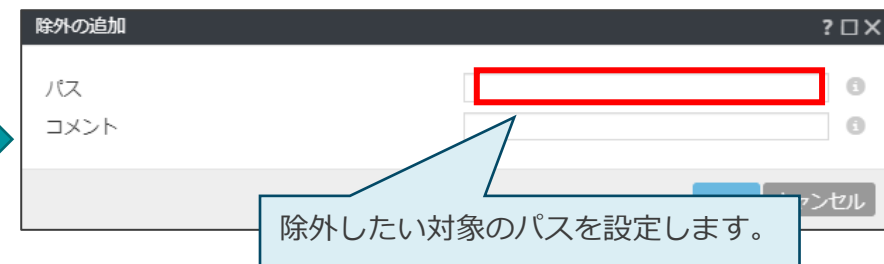
(参考) 検出除外の設定方法

- EEAL V11.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ポリシーより任意のファイル/フォルダを設定します。

■ 除外設定画面



■ 除外の追加画面



※詳細に関しては下記URLをご確認ください。

https://eset-support.canon-its.jp/faq/show/11133?site_domain=business