



ESET Endpoint アンチウイルス for Linux V8 機能紹介資料

第3版

2021年9月6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 V8（略称表記：EEAL） ※ESET NOD32アンチウイルス for Linux Desktop （略称表記：EAVL）の後継プログラム	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.X（略称表記：EP）**、または**ESET Security Management Center V7.1（略称表記：ESMC）以降で管理が可能です**。EPとESMCの機能紹介は、別資料でご用意しております。
- ・ EPC、EP、ESMC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
4. EAVL V4.0との違い
 - (1) インストール
 - (2) Webインターフェース
 - (3) アクティベーション
5. EAVL V4.0との機能比較



サポート環境

Canon

キヤノンマーケティングジャパン株式会社

1. サポート環境

項目	条件	備考
OS	Ubuntu 18.04 (64bit) Ubuntu 20.04 (64bit)	
仮想環境	VMware ESX/ESXi Citrix XenServer 5.6 以降 Windows Server 2019 Hyper-V Windows Server 2016 Hyper-V Windows Server 2012 R2 Hyper-V Windows Server 2012 Hyper-V Windows Server 2008 R2 Hyper-V (2.0)	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)	
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	
セキュアブートへの対応	対応	
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、EEAL V8のコマンドが失敗します
	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

Canon

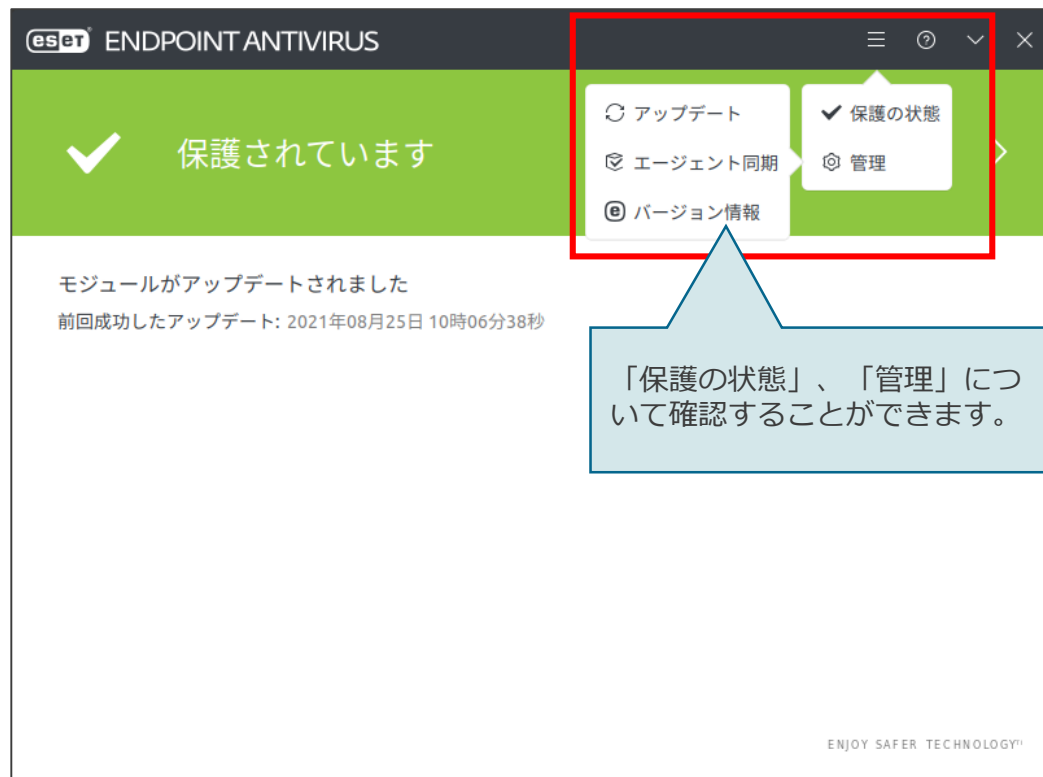
キヤノンマーケティングジャパン株式会社

2. インターフェースについて

(1) 初期画面

- EEAL V8の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。すべてが問題なく動作している場合、保護の状態が緑色です。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、色が赤に変わります。

■ 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



■ 保護の状態



2. インターフェースについて

(3) 管理

- 「管理」には「アップデート」、「エージェント同期」、「バージョン情報」の項目があります。「アップデート」では、EEAL V8のアップデート状況やモジュール情報が確認できます。「エージェント同期」では、セキュリティ管理ツールでEEAL V8を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」では、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、オペレーティングシステム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

Canon

キヤノンマーケティングジャパン株式会社

3. 詳細設定について

EEAL V8の設定方法に関して

- EEAL V8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て設定を行います。

※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。

■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。

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

新しいポリシー

ポリシー > ESET Endpoint Antivirus for Linux

基本

設定

割り当て

サマリー

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

アップデート

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

基本

スキャンオプション

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

共有ローカルキャッシュ

戻る

続行

終了

キャンセル

◆ESET PROTECT V8 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/18287?site_domain=business

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

■ 検出エンジン設定画面

ESET Endpoint for Linux (V7+)

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

アップデート

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

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

共有ローカルキャッシュ

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。

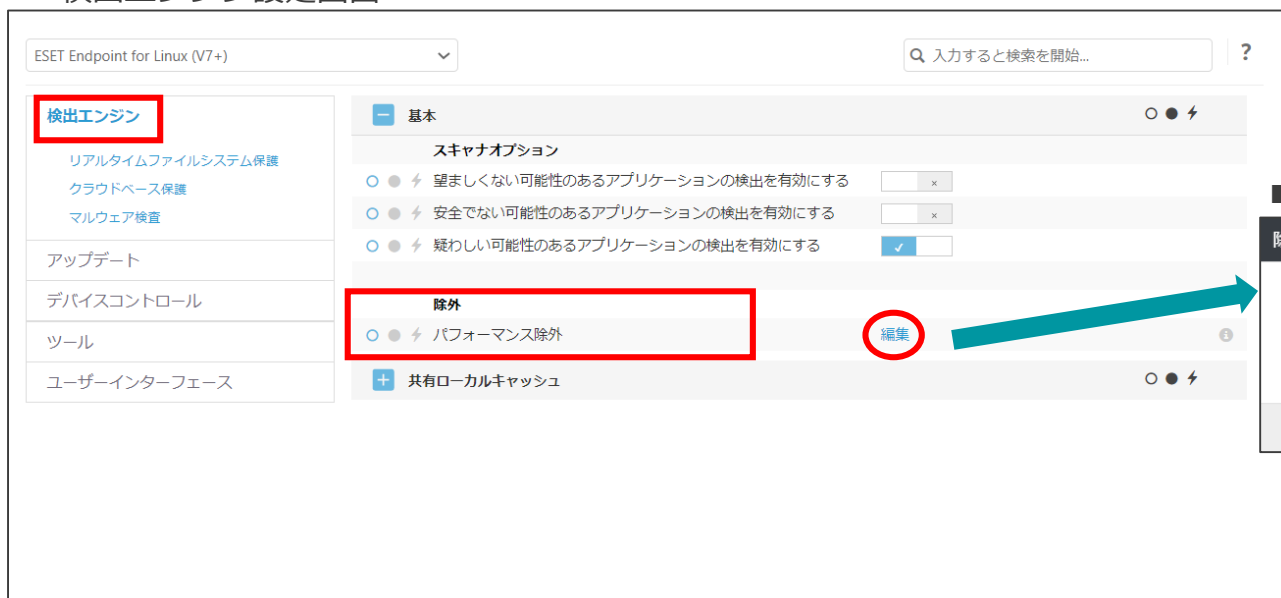
「疑わしい可能性のあるアプリケーション」
圧縮形式、プロテクタで圧縮されたプログラムが含まれます。
マルウェアの作成者が検知を逃れるためによく使用する方法
です。

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。

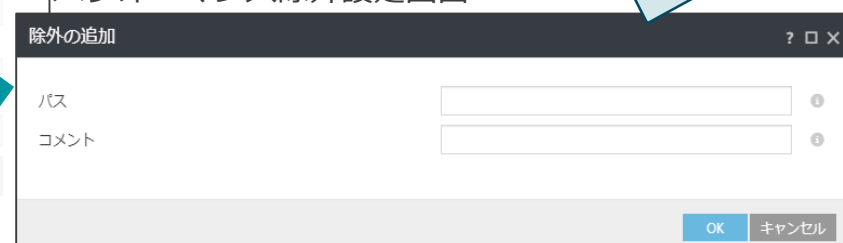
■ 検出エンジン設定画面



「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



※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

(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。

【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

(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 Endpoint for Linux (V7+)

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

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
- ☒ 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

- ☒ 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 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

(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】

Micro PCU（プログラムコンポーネントアップデート）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

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_admin/80/ja-JP/?client_tasks_database_update_rollback.html

3. 詳細設定について

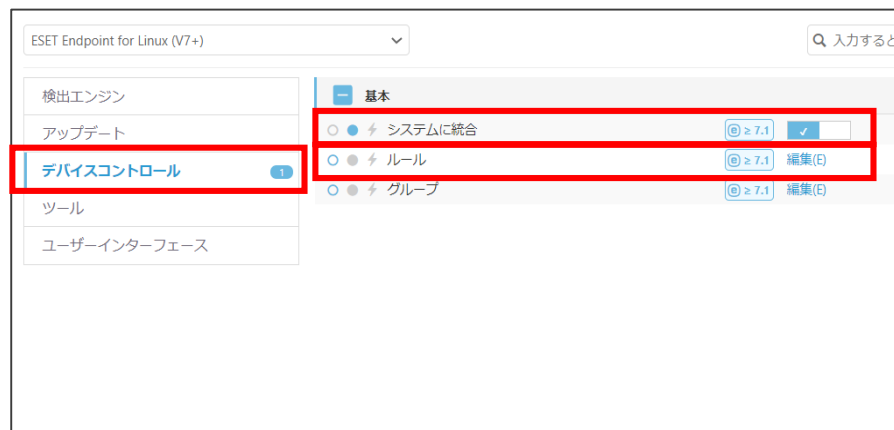
(7) デバイスコントロール

- 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

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: 読み込み/書き込み

条件: デバイス

ベンダー:

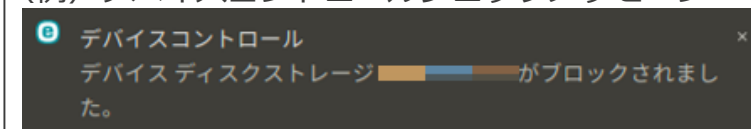
モデル:

シリアル番号:

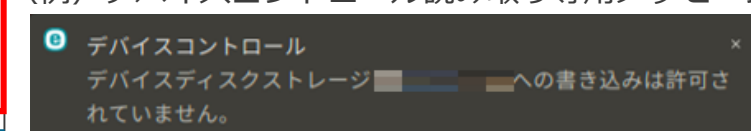
ベンダー、モデル(型番)、シリアルを入力することで詳細な制御が可能です。

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読み取り専用メッセージ



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) 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+)

検出エンジン

アップデート

デバイスコントロール

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

基本

○ ● ⚡ ログに記録する最低レベル

○ ● ⚡ 次の日数が経過したエントリを自動的に削除する

○ ● ⚡

○ ● ⚡ 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
ら最適化

○ ● ⚡ Syslogファシリティ

情報レコード

90

- 【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

(10) ユーザーインターフェース

- EEAL V8の保護状態に関する通知を、デスクトップやユーザーインターフェース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

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

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 ☒ 編集

○ ● ⚡ 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 編集

■ アプリケーション通知設定画面

選択したアプリケーション通知が表示されます

名前	デスクトップに表示
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	☒ @ ≥ 8.0
リムーバブルデバイス検査が完了しました	☒ @ ≥ 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。	☒ @ ≥ 8.0
デバイスは書き込みのためブロックされました	☒ @ ≥ 8.0
一般	
シャットダウンがスケジュールされました	☒ @ ≥ 8.0
再起動が推奨されます	☒ @ ≥ 8.0

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
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	☐ @ ≥ 8.0	☒
古い検出エンジン	☒ @ ≥ 8.0	☒
最近のアップデートの試みが失敗しました	☒ @ ≥ 8.0	☒
ウイルス対策		
リアルタイムファイルシステム保護が無効です	☐ @ ≥ 8.0	☒
リアルタイムファイルシステム保護は機能していません	☒ @ ≥ 8.0	☒
デバイスコントロール		
デバイスコントロールは機能していません	☒ @ ≥ 8.0	☒ @ ≥ 7.1
ライセンス		
ライセンスは間もなく有効期限切れとなります	☐ @ ≥ 8.0	☒
ライセンスは有効期限を過ぎています	☒ @ ≥ 8.0	☒
製品がアクティベーションされていません	☒ @ ≥ 8.0	☒
一般		
ESETは... (不明)	☐ @ ≥ 8.0	☐

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

- EEAL V8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/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/lolog [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/lolog -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/lolog --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/8/ja-JP/?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 V8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

オンデマンド検査タスク設定画面

クライアントタスク
タスク名: オンデマンド検査, EEAL V8

基本
設定
サマリー

検査後のシャットダウン
☐ 検査後にコンピュータをシャットダウン

検査プロファイル
検査プロファイル:

カスタムプロファイル

除外
検査して除外: ☐

検査対象
すべてのターゲットの検査: ☒
ターゲットの追加:
検査対象:
削除: すべて削除:

「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。

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。

■ トリガー設定画面

新しいトリガーの追加
タスク: EEAL, オンデマンド検査

基本
対象
トリガー
詳細設定 - 調整

トリガータイプ
毎週
毎週繰り返し

開始日時
2021 5月 24 09:00:00

終了条件
☒ 終了なし
☐ 終了日 10 発生
☐ 終了日

曜日選択
☐ 日曜日
☒ 月曜日
☐ 火曜日
☐ 水曜日
☐ 木曜日
☐ 金曜日
☐ 土曜日

ランダム遅延間隔
0 秒

設定した時間に実行
☒

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。

トリガータイプではタスクを実行する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。

◆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 V8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。

※詳細に関しては以下のURLをご確認ください。

https://help.eset.com/protect_admin/80/ja-JP/?create_exclusion.html



EAVL V4.0との違い

Canon

キヤノンマーケティングジャパン株式会社

4. EAVL V4.0との違い

(1) インストール

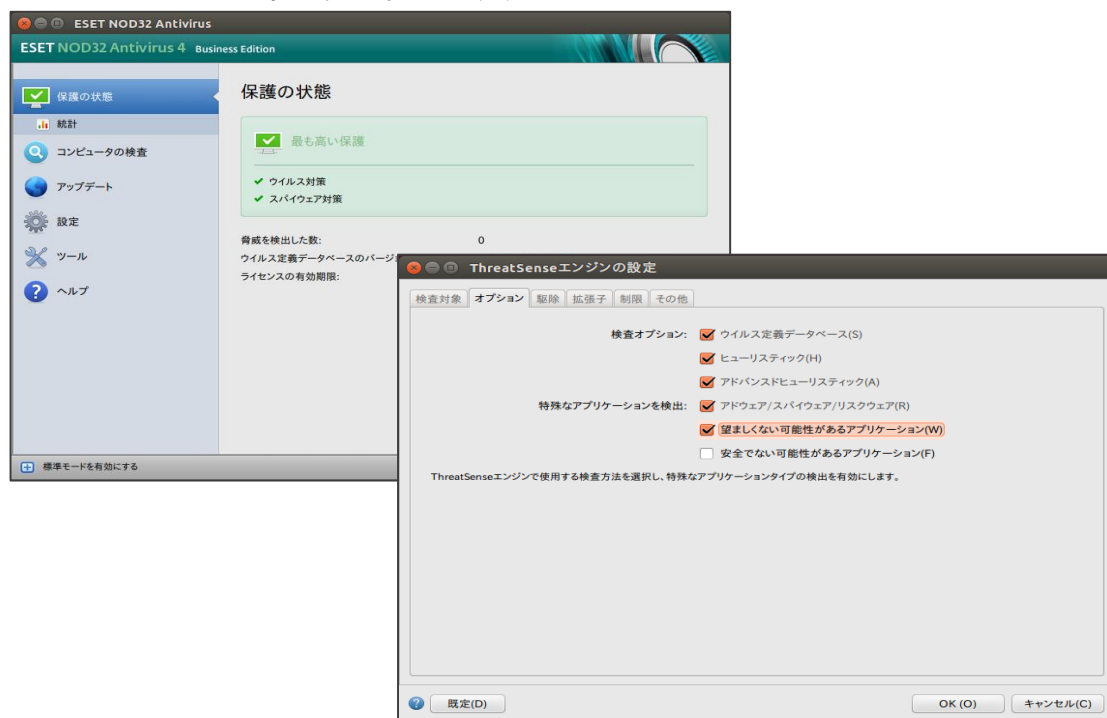
- EEAL V8をインストールの際、OSのオンラインリポジトリに接続できる場合は、EEAL V8インストール時に不足しているプログラムを同時に導入する仕様になっています。
【インストールされるプログラム】
 - gcc
 - make
 - libelf-dev
 - linux-headers-generic
 - linux-headers-generic-hwe
- すでにEAVL V4.0がインストールされている場合は、EAVL V4.0をアンインストール後にEEAL V8をインストールします。上書きインストールによるバージョンアップはできません。
※インストールにはroot権限（スーパーユーザー）が必要です。
- セキュリティ管理ツールのソフトウェアインストールタスクを使用したリモートインストールが可能です。
◆セキュリティ管理ツールに搭載されているソフトウェアインストールタスクを使用して、クライアント用プログラムをリモートインストールするには？
https://eset-support.canon-its.jp/faq/show/5165?site_domain=business

4. EAVL V4.0との違い

(2) インターフェース

- EEAL V8のインターフェースでは端末の保護状況が確認できます。また、EEAL V8ではEAVL V4.0と異なり、インターフェースからの設定が廃止になり、セキュリティ管理ツールのポリシーを使用して設定を行います。

■ EAVL V4.0のインターフェース



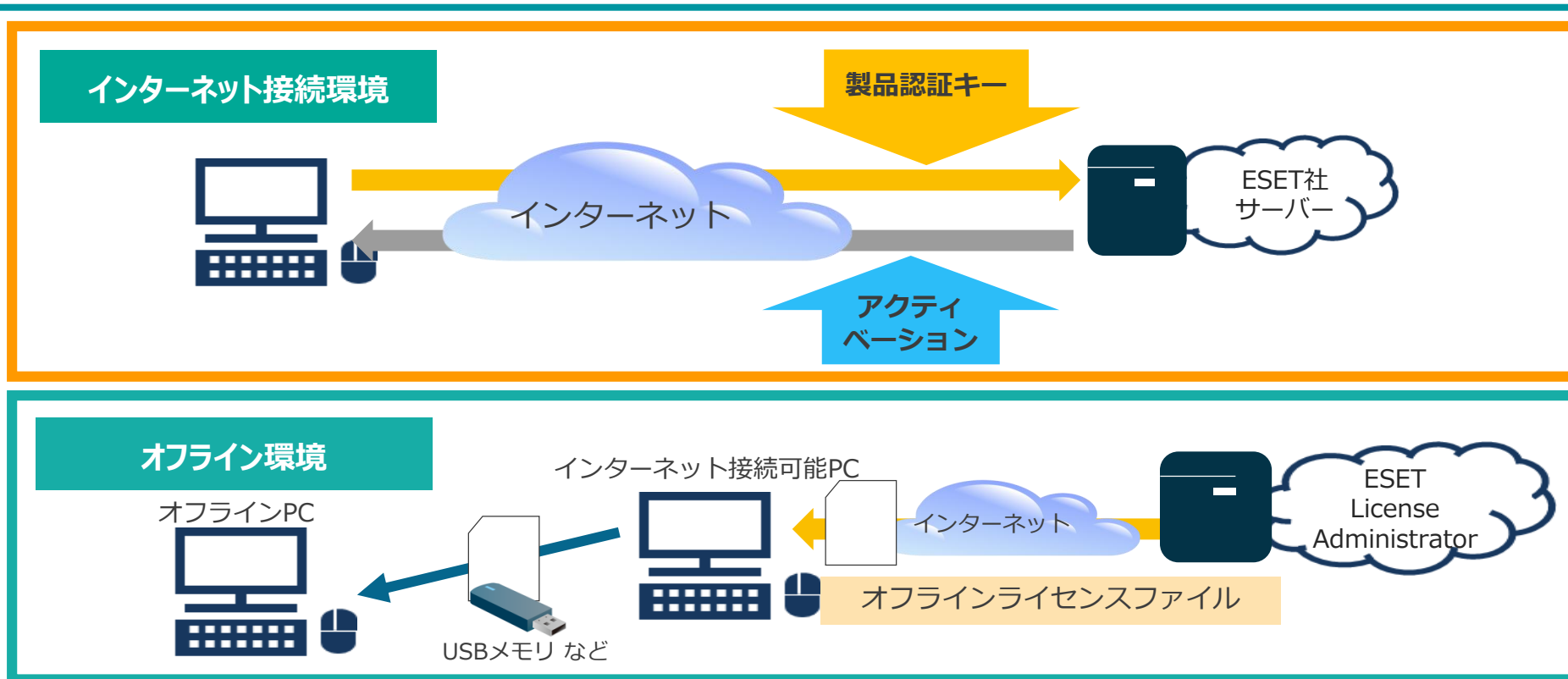
■ EEAL V8のインターフェース



4. EAVL V4.0との違い

(3) アクティベーション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。ライセンスキーファイルを使用してプログラムを認証していたEAVL V4.0とは異なり、EEAL V8では**製品認証キー**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. EAVL V4.0との違い

(3) アクティベーション②

- 端末のターミナルウィンドウ、または「ESET PROTECTソリューション」のセキュリティ管理ツールであるEPまたはESMC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。

ターミナルウィンドウから アクティベーションを行うコマンド例

製品認証キーを使用する場合

`/opt/eset/eea/sbin/lic --key=製品認証キー`

オフラインライセンスファイルを使用する場合

`/opt/eset/eea/sbin/lic -FILE=offline_license.lf`

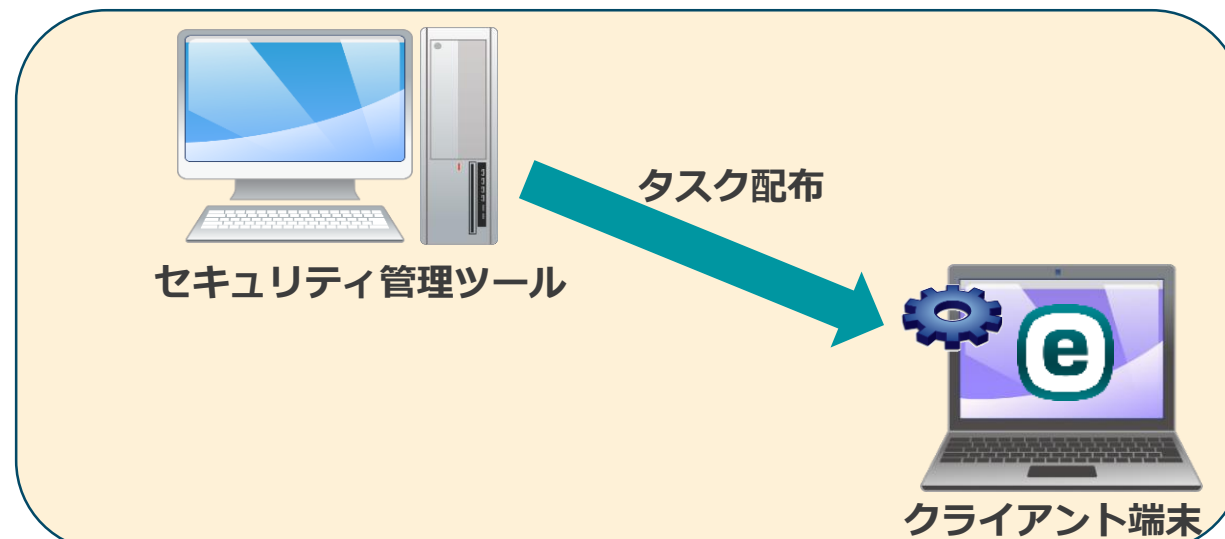
■ターミナルウィンドウからアクティベーションを行う例

```
virtual-machine: ~  
ファイル(F) 編集(E) 表示(V) 検索(S) 端末(T) ヘルプ(H)  
virtual-machine:~$ sudo /opt/eset/eea/sbin/lic --key=  
アクティベーションは正常に実行されました。  
virtual-machine:~$
```

◆オフラインライセンスファイルのダウンロード方法

https://eset-support.canon-its.jp/faq/show/4327?site_domain=business

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場合



◆セキュリティ管理ツールから、クライアント用プログラム / iOS端末 / Mobile Device Connector のアクティベーションをするには？

https://eset-support.canon-its.jp/faq/show/13245?site_domain=business

※アクティベーションを行わないと検出エンジンがアップデートできません。



EAVL V4.0との機能比較

Canon

キヤノンマーケティングジャパン株式会社

5. EAVL V4.0との機能比較

ウイルス・スパイウェア対策		
機能名	EAVL V4.0	EEAL V8
オンデマンド検査	○	○
リアルタイム検査	○	○
除外機能	○	○
リムーバブルメディアの検査	○	○
共有ローカルキャッシュ	×	○
ESET LiveGrid	×	○
検出エンジンの更新およびミラーサーバ機能		
機能名	EAVL V4.0	EEAL V8
検出エンジンのアップデート	○	○
検出エンジンの遅延アップデート	○	○
検出エンジンのロールバック機能	×	○
アップデート先の冗長化	○	○

5. EAVL V4.0との機能比較

運用関連機能		
機能名	EAVL V4.0	EEAL V8
Syslogへの出力	○	○
コマンドラインインターフェース	×	○
設定のインポート、エクスポート	○	○
インターフェースでの設定	○	×
ESMC V7.Xとの連携	○	○※1
EP V8.xとの連携	○	○
その他の機能		
機能名	EAVL V4.0	EEAL V8
リムーバブルメディアの検査	×	○
デバイスコントロール	△※2	○
プロキシの設定	○	○
アクティベーションの必要性の有無	×	○

※1…ESMC V7.1以降でのみ管理可能です。

※2…ブロックのアクションのみ可能です。