ESET Endpoint Antivirus for Linux 11.1

ユーザー ガイド

この文書のオンラインバージョンを表示するにはこちらをクリックしてください。

Digital Security
Progress. Protected.

ESET Endpoint Antivirus for Linux 11.1はESET, spol. s r.o.によって開発されています

詳細についてはhttps://www.eset.comをご覧ください。

ESET, spol. s r.o.は、事前の通知なしに、説明されたアプリケーションソフトウェアを変更する権利を有します。

テクニカルサポート: https://support.eset.com

改訂: 2025年/5月/6日

概要

ESET Endpoint Antivirus for Linuxは、Linuxデスクトップ環境用に設計された統合ソリューションですESETの最先端の検出エンジンは、優れた検査速度と検出率を実現します。さらに、リソース消費量が非常に少ないため、どのLinuxデスクトップでもESET Endpoint Antivirus for Linuxが最適な選択肢となります。お使いのシステムがシステム要件を満たしていることを確認します。

ESET Endpoint Antivirus for Linuxは、オンデマンドスキャナーとオンアクセススキャナーを使用して、効果的かつ堅牢な保護を提供します。

コマンドESET PROTECT、またはESET PROTECT On-Premを使用してターミナルからオンデマンド検査を開始できます。あるいは、オペレーティングシステムの自動スケジューリングツール(cronなど)を使用することもできます。オンデマンド検査は、ユーザーまたはシステムの要求によってトリガーされると、ファイルシステムオブジェクトを検査します。

オンアクセススキャナーは、ファイルシステムオブジェクトにアクセスしようとすると呼び出されます。

システムの主要な機能

- ESETの軽量カーネル内モジュールによるオンアクセススキャン
- 包括的な検査ログ
- 再設計された、使いやすい設定
- 自動製品アップデート
- 隔離
- デスクトップ通知
- ESET PROTECTで管理可能
- クラウドベース保護
- Webアクセス保護
- デバイスコントロール
- ESET Inspectサポート

リリースノート

リモートでESET Endpoint Antivirus for Linuxを管理

ESETリモート管理ツール

ESET PROTECT On-Prem

ESETサーバー製品を1か所で管理します。ESET PROTECT On-Prem Webコンソールを使用してESET製品の展開、タスクの管理、セキュリティポリシーの適用、システムステータスの監視、リモートコンピューター上の問題や検出への迅速な対応を行うことができます。

- ESET Endpoint Antivirus for Linuxを実行しているコンピューターでESET Management Agentを展開します。
- コンピューターをESET PROTECTに追加します
- これでESET Endpoint Antivirus for Linuxで適用可能なクライアントタスクを実行できるようになりました。

ESET PROTECT

ESET PROTECT On-Premとは異なり、ネットワーク環境内のサーバー上のESET製品を、物理サーバーや仮想サーバーを必要とせずに、1つの中央の場所から管理できます。

ESET PROTECT Hub

ESET PROTECT統合セキュリティプラットフォームへの中央ゲートウェイです。すべてのESETプラットフォームモジュールのIDサブスクリプション、およびユーザー管理を一元化します。

ESET Business Account

ESETビジネス製品のライセンス管理ポータル。

その他のセキュリティ製品

ESET Inspectまたは**ESET Inspect On-Prem**

オンプレミス版の強力な機能をすべて備えており、クラウド配信サービスを簡単に展開でき、メンテナンス要件がほとんどありません。これはESETエンドポイント検出テクノロジーとノウハウを積み重ねたものです。

仕様

ESET Endpoint Antivirus for Linuxの参照技術仕様:

- システム要件
- セキュアブート

システム要件

ハードウェア要件

ESET Endpoint Antivirus for Linuxが正常に動作するには、インストール処理を実行する前に、次の最低ハードウェア要件を満たす必要があります。

- プロセッサIntel/AMD x64
- 700MBのハードディスク空き領域

ソフトウェア要件

次の64ビットアーキテクチャのオペレーティングシステムが正式にサポートおよびテストされています。

- Ubuntu Desktop 20.04 LTS
- Ubuntu Desktop 22.04 LTS
- Ubuntu Desktop 24.04 LTS
- サポートされているデスクトップ環境がインストールされているRed Hat Enterprise Linux 8, 9
- Linux Mint 20, 21, 22

Ubuntu Desktop 22.04 LTS/Linux Mint 21の最新のLinuxカーネルでは、カーネルモジュールのコンパイルにgcc-12が必要です。この問題の詳細については、ナレッジベースの記事を参照してください。

AWSカーネル
AWS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いません。

サポートされているディスプレイサーバー

- X11
- Wayland

サポートされているデスクトップ環境:

- Cinnamon 5.0以降
- GNOME 3.28.2以降
- KDE
- MATE
- XFCE

UTF-8エンコーディングを使用する任意のロケール

ターミナルウィンドウのユーザーインターフェースとコマンドリストは次の言語で提供されています。

- 英語
- ドイツ語
- スペイン語
- スペイン語(ラテンアメリカ)

- フランス語
- ポーランド語
- Ukrainian
- 日本語

ホストOSがサポートされていない言語を使用する場合、既定では英語が使用されます。

ネットワークの前提条件

ESET Endpoint Antivirus for Linuxの適切な機能を確保するには、ナレッジベースの記事に記載されているネットワークの前提条件を許可します。

サポートされているファイルシステム

次のファイルシステムが正式にサポートおよびテストされています。

ファイルシステム	ローカルデバイス	リムーバブルデバイス	ネットワーク
Btrfs	✔		
FAT		✔	
VFAT	✔	✔	
exFAT	✔	✔	
F2FS		✔	
ext4 (バージョン2、バージョン3)	✔	✔	
JFS	✔		
NTFS	✔	✔	
UDF		✔	
XFS	✔		
ZFS	✔		
EncFS	✔		
FUSE (snap□appimage)	✔		
tmpfs	✔		
NFSクライアント(バージョン3、バージョン4)			✔
SMB (GVfs, CIFS)			✔
SSHFS			✔
davfs			✔

セキュアブート

セキュアブートが有効なコンピューターでリアルタイムファイルシステム保護とアクセス保護を使用するにはESET Endpoint Antivirus for Linux カーネルモジュールを秘密鍵で署名する必要があります。また、対応する公開鍵をUEFIにインポートする必要がありますESET Endpoint Antivirus for Linuxにはビルトインの署名スクリプトが付属しています。このスクリプトは対話モードまたは非対話モードで動作します。

mokutilユーティリティを使用して、コンピューターでセキュアブートが有効であることを確認します。特権ユーザーで、ターミナルウィンドウから次のコマンドを実行します。

```
mokutil --sb-state
```

対話モード

カーネルモジュールに署名する公開鍵と秘密鍵がない場合、対話モードは新しい鍵を生成し、カーネルモジュールに署名できます。また、生成された鍵をUEFIで登録できます。

1. 特権ユーザーで、ターミナルウィンドウから次のコマンドを実行します。

```
/opt/eset/eea/lib/install_scripts/sign_modules.sh
```

2. スクリプトでキーを入力するように指示されたら、Nを入力してから、**Enter**キーを押します。

3. 新しいキーを生成するように指示されたら、Yと入力してから、**Enter**キーを押します。スクリプトは、生成された秘密鍵でカーネルモジュールに署名します。

4. 生成された公開鍵を自動的にUEFIに登録するには、Yと入力してから、**Enter**を押します。登録を手動で完了するには、Nと入力し、**Enter**キーを押して、画面の手順に従います。

5. メッセージが表示されたら、選択したパスワードを入力しますUEFIでの登録が完了(新しいコンピューターの所有者鍵[MOK]の承認)したときに、パスワードが必要になります。

6. 生成されたキーを後で使用するためにハードドライブに保存するには、Yと入力し、ディレクトリへのパスを入力して、**Enter**キーを押します。

7. UEFIを再起動してアクセスするには、メッセージが表示されたらYと入力し、**Enter**キーを押します。

8. UEFIにアクセスするように指示されたら、10秒以内に任意のキーを押します。

9. **MOKの登録**を選択し、**Enter**キーを押します。

10. **続行**を選択し、**Enter**キーを押します。

11. **はい**を選択し、**Enter**キーを押します。

12. 登録を完了し、コンピューターを再起動するには、手順5のパスワードを入力し、**Enter**キーを押します。

非対話モード:

ターゲットコンピューターで公開鍵と秘密鍵を使用できる場合は、このモードを使用します。

Syntax: `/opt/eset/eea/lib/install_scripts/sign_modules.sh[オプション]`

オプション – 短縮型	オプション – 標準型	説明
`-d`	`--public-key`	署名で使用するDER形式の公開鍵へのパスを設定
`-p`	`--private-key`	署名で使用する秘密鍵へのパスを設定
`-k`	`--kernel`	モジュールが署名される必要があるカーネルの名前を設定します。指定されていない場合、既定で現在のカーネルが選択されます
`-a`	`--kernel-all`	ヘッダーを含むすべての既存のカーネルでカーネルモジュールを署名(およびビルド)する
`-h`	`--help`	ヘルプを表示します

1. 特権ユーザーで、ターミナルウィンドウから次のコマンドを実行します。

```
/opt/eset/eea/lib/install_scripts/sign_modules.sh -p <path_to_private_key> -
d <path_to_public_key>
```

`<path_to_private_key>`と`<path_to_public_key>`をそれぞれ秘密鍵と公開鍵へのパスで置き換えます。

2. 指定された公開鍵がUEFIに登録されていない場合は、特権ユーザーで次のコマンドを実行します。

```
mokutil --import <path_to_public_key>
```

`<path_to_public_key>`は指定された公開鍵を表します。

3. コンピューターを再起動し、UEFIにアクセスし、**MOKの登録 > 続行 > はい**を選択します。

複数のデバイスの管理

同じLinuxカーネルを使用し、同じ公開鍵がUEFIに登録されている複数のコンピューターを管理するとします。この場合、秘密鍵を含むコンピューターの1つでESET Endpoint Antivirus for Linuxカーネルモジュールを署名し、署名されたカーネルモジュールを他のコンピューターに転送できます。署名が完了したら、次の手順を実行します。

1. `/lib/modules/<kernel-version>/eset/eea/eset_rtp`, `eset_wap`の署名されたカーネルモジュールをコピーして、ターゲットコンピューターの同じ場所に貼り付けます。

2. ターゲットコンピューターで`depmod <kernel-version>` を呼び出します。

3. ターゲットコンピューターでESET Endpoint Antivirus for Linuxを再起動し、モジュールテーブルを更新します。次のコマンドを特権ユーザーで実行します。

```
systemctl restart eea
```

すべての場合において、カーネルバージョン<kernel-version>を対応するカーネルバージョンで置換します。

ファイルおよびフォルダー構造

このトピックではESETテクニカルサポートがトラブルシューティングのためにファイルへのアクセスを要求した場合に備えてESET Endpoint Antivirus for Linuxのファイルおよびフォルダー構造について詳細に説明します。以下では、デーモンおよびコマンドラインユーティリティ一覧を示します。

基本ディレクトリ

ウイルス定義データベースを含むESET Endpoint Antivirus for Linuxの読み込み可能なモジュールが格納されるディレクトリ。

```
/var/opt/eset/eea/lib
```

キャッシュディレクトリ

ESET Endpoint Antivirus for Linuxのキャッシュおよび一時ファイル(隔離ファイルやレポートなど)が格納されるディレクトリ。

```
/var/opt/eset/eea/cache
```

バイナリファイルディレクトリ

関連するESET Endpoint Antivirus for Linuxバイナリファイルが格納されるディレクトリ。

```
/opt/eset/eea/bin
```

次のユーティリティがあります。

- lsdev — コンピューターに接続されたデバイスの属性のリストを表示するために使用します
- odscan — ターミナルウィンドウからオンデマンド検査を実行するために使用します
- quar — 隔離されたアイテムを管理するために使用します
- upd — モジュールのアップデートを管理したり、アップデート設定を修正するために使用します

システムバイナリファイルディレクトリ

関連するESET Endpoint Antivirus for Linuxシステムバイナリファイルが格納されるディレクトリ。

/opt/eset/eea/sbin

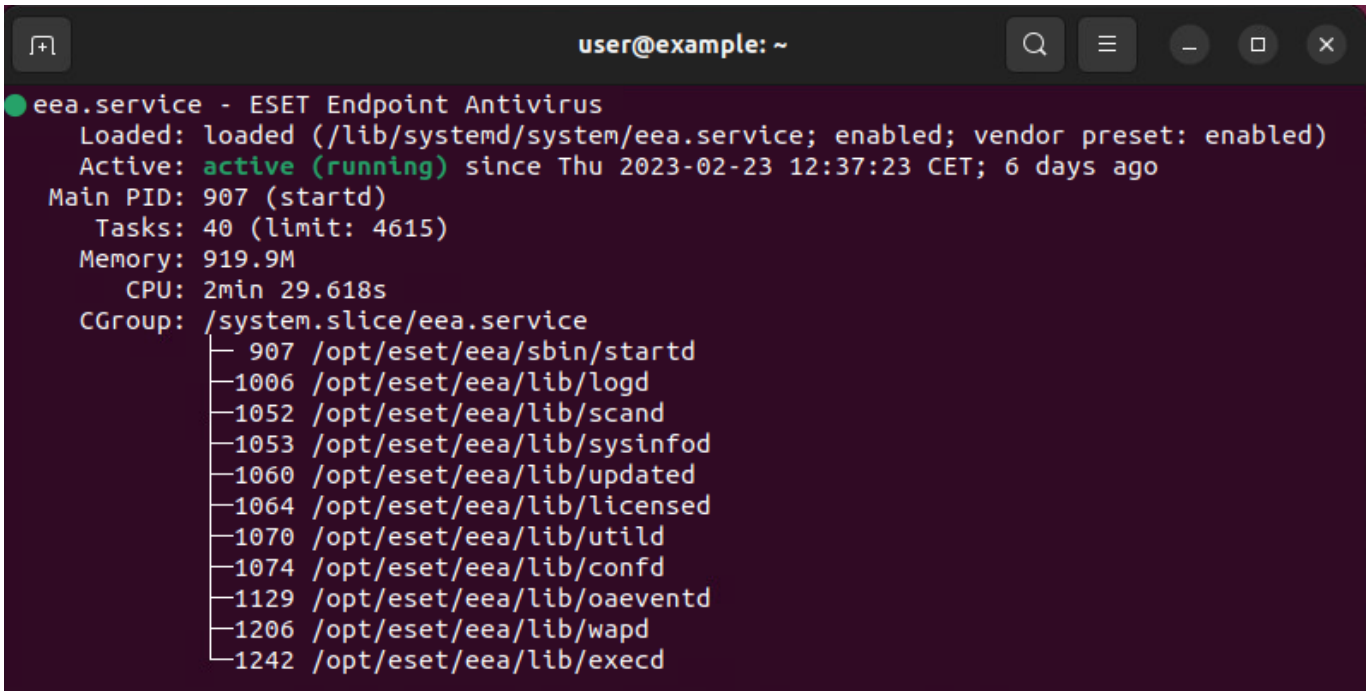
次のユーティリティがあります。

- collect_logs.sh — すべての必要なログをアーカイブファイルとして、ログインユーザーのホームフォルダーに生成するために使用します
- ecp_logging.sh — 製品アクティベーションに関連するログを生成するために使用します
- lic — 購入した製品認証キーでESET Endpoint Antivirus for Linuxアクティベーションするか、アクティベーション状態とライセンスの有効期間を確認するために使用します。
- lslog — ESET Endpoint Antivirus for Linuxで収集したログを表示するために使用します
- startd — 停止した場合ESET Endpoint Antivirus for Linuxデーモンを手動で開始するために使用します。

ESET Endpoint Antivirus for Linuxサービスがアクティブであるかどうかを確認するには、ルート権限で、ターミナルウィンドウから次のコマンドを実行します。

```
systemctl status eea.service
```

systemctlからのサンプル出力:



デーモン

- sbin/startd – メインデーモン、他のデーモンの開始と管理

- lib/scand – 検査デーモン
- lib/oaeventd – オンアクセスイベント傍受サービス(eset_rtpカーネルモジュールを使用)
- lib/confd – 設定管理サービス
- lib/logd – ログ管理サービス
- lib/licensed – アクティベーションおよびライセンスサービス
- lib/updated – モジュールのアップデートサービス
- lib/execd + lib/odfeeder – オンデマンド検査ヘルパー
- lib/utild – ユーティリティサービス
- lib/sysinfod – OSおよびメディア検出サービス
- lib/wapd - Webアクセス保護サービス

コマンドラインユーティリティ

- sbin/lslog – ログリスト出力ユーティリティ
- bin/odscan – オンデマンドスキャナー
- lib/cfg – 設定ユーティリティ
- sbin/lic – ライセンスユーティリティ
- bin/upd – モジュールのアップデートユーティリティ
- bin/quar – 隔離管理ユーティリティ

インストール/アップグレード

以下は、製品のインストール、アップグレード、およびその他の関連情報の詳細です。

- ESET Endpoint Antivirus for Linuxのインストール手順
- 一括展開
- アンインストール

ESET Endpoint Antivirus for Linuxのインストール手順

ESET Endpoint Antivirus for Linuxはバイナリファイル(`.bin`)として配布されます。

一部の他のセキュリティ製品がシステムにインストールされ、実行中の場合は、ESET Endpoint Antivirus for Linuxが正常に動作しない可能性があります。
(不明な)問題が発生した場合は、他のセキュリティまたはサードパーティ製品を使用せずに、クリーンなコンピューターにESET Endpoint Antivirus for Linuxをインストールしてください。

OSをアップデート
ESET Endpoint Antivirus for Linuxのインストール前に、OSに最新のアップデートがインストールされていることを確認してください。

ESET PROTECTを使用してインストールする

ESET Endpoint Antivirus for Linuxをコンピューターにリモート展開するには、ESET PROTECTソフトウェアインストールオンラインヘルプセクションを参照してください。

ターミナルを使用してインストールする

以下のコマンドは、ターミナルウィンドウで前述のファイルの場所にいる場合に有効です。

製品をインストールまたはアップグレードするには、ご使用の適切なOSディストリビューションのルート権限で、ESET配布スクリプトを実行します。

```
./eeau_x86_64.bin
```

```
sh ./eeau_x86_64.bin
```

使用可能なコマンドライン引数を見る

ESET Endpoint Antivirus for Linuxバイナリファイルの使用可能なパラメーター(引数)を表示するには、ターミナルウィンドウから次のコマンドを実行します。
`./eeau_x86_64.bin -h`

使用可能なパラメーター

短縮型	標準型	説明
-h	--help	コマンドライン引数を表示
-n	--no-install	解凍後にインストールを実行しない
-y	--accept-license	製品ライセンス契約に同意し、表示しない
-f	--force-install	確認せずにパッケージマネージャーで強制インストール
-u	--unpack-ertp-sources	「ESETリアルタイムファイルシステム保護カーネルモジュール」ソースを解凍する。インストールは実行しない

.debインストールパッケージを取得する
OSに適した.debまたはインストールパッケージを取得するには、-nコマンドライン引数を使用してESET配布スクリプトを実行します。
`sudo ./eeau_x86_64.bin -n`
または
`sudo sh ./eeau_x86_64.bin -n`

インストールパッケージの依存関係を表示するには、次のコマンドのいずれかを実行します。

```
dpkg -I <deb package>
```

```
rpm -qRp <rpm package>
```

画面の手順に従います。製品ライセンス契約に同意してインストールを完了します。

インストーラーは依存関係の問題について通知します。

> **コンピューターをESET PROTECT On-PremまたはESET PROTECTに追加する**
> インストール後、コンピューターをESET PROTECT On-PremまたはESET PROTECTに追加してESET Endpoint Antivirus for Linux設定を変更できるようにすることを強くお勧めします。リモートでESET Endpoint Antivirus for Linuxを管理で説明されている手順に従います。

ESET Endpoint Antivirus for Linuxのアクティベーション

検出モジュールの定期的な更新を有効にするには、ESET Endpoint Antivirus for Linuxをアクティベーションします。

> **サードパーティーアプリ**
> ESET Endpoint Antivirus for Linuxで使用されるサードパーティーアプリの概要は、`/opt/eset/eea/doc/modules_notice/`にある`NOTICE_mode`ファイルを参照してください。

一括展開

このトピックではPuppetChefAnsible経由でのESET Endpoint Antivirus for Linuxの一括展開について概要を説明します。以下のコードブロックでは、パッケージインストールの基本的な例のみを示していますLinuxディストリビューションによっては異なる場合があります。

パッケージ選択

ESET Endpoint Antivirus for Linuxの一括展開を開始する前に、使用するパッケージを決定する必要がありますESET Endpoint Antivirus for Linuxは`.bin`パッケージとして配布されます。ただし、「`-n`」コマンドライン引数を使用するとESET配布を実行して、deb/rpmパッケージを取得できます。

Puppet

前提条件

- binまたはdeb/rpmパッケージがpuppet-masterで使用可能
- puppet-agentがpuppet-masterに接続されている

Binパッケージ

展開手順:

- binインストールパッケージを任意のコンピューターにコピーします
- binインストールパッケージを実行します

Puppetマニフェストサンプル

```
node default {
    file {"/tmp/eea-8.0.1081.0.x86_64.bin":
           mode => "0700",
           owner => "root",
           group => "root",
           source => "puppet:///modules/eea/eea-8.0.1081.0.x86_64.bin"
         }
    exec {"Execute bin package installation":
           command => '/tmp/eea-8.0.1081.0.x86_64.bin -y -f'
         }
}
```

Deb/rpmパッケージ

展開手順:

- ディストリビューションファミリーに従ってdeb/rpmインストールパッケージを任意のコンピューターにコピーします
- deb/rpmインストールパッケージを実行します

> **依存関係**
> インストールを開始する前に、依存関係を解決する必要があります

Puppetマニフェストサンプル

```
node default {
if $osfamily == 'Debian' {
        file {"/tmp/eea-8.0.1081.0.x86_64.deb":
               mode => "0700",
               owner => "root",
               group => "root",
               source => "puppet:///modules/eea/eea-8.0.1081.0.x86_64.deb"
             }
        package {"eea":
               ensure => "installed",
               provider => 'dpkg',
               source => "/tmp/eea-8.0.1081.0.x86_64.deb"
             }
}
if $osfamily == RedHat {
        file {"/tmp/eea-8.0.1081.0.x86_64.rpm":
               mode => "0700",
               owner => "root",
               group => "root",
               source => "puppet:///modules/eea/eea-8.0.1081.0.x86_64.rpm"
             }
        package {"eea":
               ensure => "installed",
               provider => 'rpm',
               source => "/tmp/eea-8.0.1081.0.x86_64.rpm"
             }
 }
}
```

Chef

前提条件

- binまたはdeb/rpmパッケージがChefサーバーで使用可能
- Chefクライアントが Chefサーバーに接続されている

Binパッケージ

展開手順:

- binインストールパッケージを任意のコンピューターにコピーします
- binインストールパッケージを実行します

Chefレシピサンプル

```
cookbook_file '/tmp/eea-8.0.1084.0.x86_64.bin' do
        source 'eea-8.0.1084.0.x86_64.bin'
        owner 'root'
        group 'root'
        mode '0700'
        action :create
end

execute 'package_install' do
        command '/tmp/eea-8.0.1084.0.x86_64.bin -y -f'
end
```

Deb/rpmパッケージ

展開手順:

- ディストリビューションファミリーに従って deb/rpmインストールパッケージを任意のコンピューターにコピーします
- deb/rpmインストールパッケージを実行します

依存関係
インストールを開始する前に、依存関係を解決する必要があります

Chefレシピサンプル

```
cookbook_file '/tmp/eea-8.0.1084.0.x86_64.deb' do
        source 'eea-8.0.1084.0.x86_64.deb'
        owner 'root'
        group 'root'
        mode '0700'
        action :create
        only_if { node['platform_family'] == 'debian'}
end

cookbook_file '/tmp/eea-8.0.1084.0.x86_64.rpm' do
                source 'eea-8.0.1084.0.x86_64.rpm'
                owner 'root'
                group 'root'
                mode '0700'
                action :create
                only_if { node['platform_family'] == 'rhel'}

dpkg_package 'eea' do
        source '/tmp/eea-8.0.1084.0.x86_64.deb'
        action :install
        only_if { node['platform_family'] == 'debian'}
end

rpm_package 'eea' do
        source '/tmp/eea-8.0.1084.0.x86_64.rpm'
        action :install
        only_if { node['platform_family'] == 'rhel'}
end
```

Ansible

前提条件

- binまたはdeb/rpmパッケージがAnsibleサーバーで使用可能
- ターゲットコンピューターへのsshアクセス

Binパッケージ

展開手順:

- binインストールパッケージを任意のコンピューターにコピーします
- binインストールパッケージを実行します

Playbookタスクサンプル

```
....
- name: "INSTALL: Copy configuration json files"
  copy:
    src: eea-8.0.1084.0.x86_64.bin
    dest: /home/ansible/

- name : "Install product bin package"
  shell: bash ./eea-8.0.1084.0.x86_64.bin -y -f -g
.....
```

Deb/rpmパッケージ

展開手順:

- ディストリビューションファミリーに従ってdeb/rpmインストールパッケージを任意のコンピューターにコピーします
- deb/rpmインストールパッケージを実行します

Playbookタスクサンプル

```
....
      - name: "Copy deb package to VM"
        copy:
          src: ./eea-8.0.1085.0.x86_64.deb
          dest: /home/ansible/eea-8.0.1085.0.x86_64.deb
          owner: ansible
          mode: a+r
        when:
          - ansible_os_family == "Debian"

      - name: "Copy rom package to VM"
        copy:
          src: ./eea-8.0.1085.0.x86_64.rpm
          dest: /home/ansible/eea-8.0.1085.0.x86_64.rpm
          owner: ansible
          mode: a+r
        when:
          - ansible_os_family == "RedHat"

      - name: "Install deb package"
        apt:
          deb: /home/ansible/eea-8.0.1085.0.x86_64.deb
          state: present
        when:
          - ansible_os_family == "Debian"

      - name: "Install rpm package"
        apt:
          deb: /home/ansible/eea-8.0.1085.0.x86_64.rpm
          state: present
        when:
          - ansible_os_family == "RedHat"
....
```

最新バージョンへのアップグレード

プログラムモジュールの自動更新では解決できない問題の修正や改良を行うためにESET Endpoint Antivirus for Linuxの新バージョンが提供されています。

現在インストールされている製品バージョン

EEAUの製品バージョンを判定するには、2つの方法があります。

1. ターミナルウィンドウで、`/opt/eset/eea/lib/egui -v`を実行します。
2. コンピューターセクションでESET PROTECTをチェックインします。

アップグレードする方法は？

最新のバージョンにアップグレードするには、インストールセクションの説明に従い、OS関連のインストールパッケージを実行します。

ESET PROTECTでESET Endpoint Antivirus for Linuxを管理している場合は、ソフトウェアインストールタスクまたは**ダッシュボード** > **ESETアプリケーション** > ESET Endpoint Antivirusをクリック > **インストールされたESET製品のアップデート**から、アップグレードを開始します。

モジュールアップデート

検出モジュールを含む製品モジュールは自動的にアップデートされます。

検出モジュールのアップデートを手動で起動するには、ターミナルウィンドウでアップデートコマンドを実行するか、ESET PROTECTを使用してアップデートします。

ESET Endpoint Antivirus for Linuxアップデートが安定していない場合は、モジュールのアップデートを前の状態にロールバックします。ターミナルウィンドウから該当するコマンドを実行するか、ESET PROTECTを使用してロールバックします。

ターミナルウィンドからすべての製品モジュールをアップデートするには、次のコマンドを実行します。

```
/opt/eset/eea/bin/upd -u
```

ターミナルでのアップデートとロールバック

オプション – 短縮型	オプション – 標準型	説明
-u	--update	モジュールの更新
-c	--cancel	モジュールのダウンロードをキャンセルします
-e	--resume	アップデートのブロックを解除する
-l	--list-modules	使用されているモジュールのバージョンを表示
-r	--rollback=値	スキャナーモジュールの最も古いスナップショットにロールバックし、VALUEに設定した時間のすべてのアップデートをブロックします

updユーティリティを使用して、製品構成を変更することはできません。

例

アップデートを48時間停止し、スキャナーモジュールの最も古いスナップショットにロールバックするには、特権ユーザーで次のコマンドを実行します。

```
sudo /opt/eset/eea/bin/upd --update --rollback=48
```

スキャナーモジュールの自動アップデートを再開するには、特権ユーザーで次のコマンドを実行します。

```
sudo /opt/eset/eea/bin/upd --update --cancel
```

IPアドレス「192.168.1.2」とポート「2221」で使用可能なミラーサーバーからアップデートするには、特権ユーザーで次のコマンドを実行します。

```
sudo /opt/eset/eea/bin/upd --update --server=192.168.1.2:2221
```

配布用アップデート

ESETセキュリティ製品(ESET PROTECTESET Endpoint Antivirusなど)では、アップデートファイルのコピーを作成しネットワーク内の他のワークステーションをアップデートすることができます。ミラーを使用すると各ワークステーションでベンダのアップデートサーバーから繰り返しアップデートファイルをダウンロードしなくて済むので便利です。アップデートがローカルのミラーサーバーにダウンロードされ、すべてのワークステーションに配信されるため、ネットワークトラフィックが過負荷状態になる危険性を回避することができます。ミラーからクライアントワークステーションをアップデートすると、ネットワークの負荷分散が最適化されると共に、インターネットの帯域幅が節約されます。

アップデートミラーを使用するようにESET Endpoint Antivirus for Linuxを設定する

1. ESET PROTECTで、**ポリシー**>**新しいポリシー**をクリックし、ポリシーの名前を入力します。
2. **設定**をクリックし、ドロップダウンメニューから**ESET Endpoint for Linux (V7+)**を選択します。
3. **アップデート**>**プライマリサーバー**をクリックします。
4. **基本**セクションで、**自動的に選択する**の横のトグルをオフにします。
5. **アップデートサーバー**フィールドで、次の形式のいずれかを使用して、ミラーサーバーのURLアドレスを入力します。
   - `http://<IP>:<port>/<path_to_update_folder>`
   - `http://<hostname>:<port>/<path_to_update_folder>`
6. 該当するユーザー名とパスワードを入力します。
7. **設定**>**割り当て**をクリックします。ポリシーが適用されるコンピューターの任意のグループを選択します。
8. **OK**をクリックしてから、**完了**をクリックします。

ネットワークにその他のミラーサーバーがある場合は、上記の手順を繰り返して、セカンダリアップデートサーバーを設定します。

ESET Endpoint Antivirus for Linuxのアクティベーショ

ン

ESET販売店から入手したライセンスを使用してESET Endpoint Antivirus for Linuxをアクティベーションします。

ターミナルを使用してアクティベーションする

/opt/eset/eea/sbin/licユーティリティを特権ユーザーで使用して、ターミナルウィンドウからESET Endpoint Antivirus for Linuxをアクティベーションします。

Syntax: /opt/eset/eea/sbin/lic[オプション]

例
以下のコマンドは、特権ユーザーで実行する必要があります。
製品認証キーを使用したアクティベーション
/opt/eset/eea/sbin/lic -k XXXX-XXXX-XXXX-XXXX-XXXX
または
/opt/eset/eea/sbin/lic --key XXXX-XXXX-XXXX-XXXX-XXXX
XXXX-XXXX-XXXX-XXXX-XXXXはESET Endpoint Antivirus for Linux製品認証キーを表します。
EBA□EMA□またはESET PROTECT Hubアカウントを使用したアクティベーション
1. 次のコマンドを実行します。
/opt/eset/eea/sbin/lic -u your@username
ここで□your@usernameはEBA□EMA□またはESET PROTECT Hubアカウントのユーザー名を表します。
2. パスワードを入力し、**Enter**キーを押します。
3. 使用可能なESET Endpoint Antivirus for Linuxライセンスとサイト(ライセンスプール)の一覧が表示されます。
4. 次のコマンドのいずれかを実行します。
/opt/eset/eea/sbin/lic -u your@username -i site_ID -p XXX-XXX-XXX
XXX-XXX-XXXは、前に表示されたリストの各ライセンスの横にある角括弧で囲まれた公開ライセンスIDを表します。一方、site_IDは、前に表示された各サイトの横にある角括弧で囲まれた英数字文字列を表します。
/opt/eset/eea/sbin/lic -u your@username -i site_ID
site_IDは、前の手順で表示した一覧の各サイトの横にある角括弧で囲まれた英数字の文字列を表します。
5. パスワードを入力し、**Enter**キーを押します。
ユーザー名、パスワード、および公開ライセンスIDがpassword.txtファイルに保存されている場合は、特権ユーザーで次の手順を実行します。
cat password.txt | /opt/eset/eea/sbin/lic -u your@username -p XXX-XXX-XXX --stdin-pass
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
/opt/eset/eea/sbin/lic -f offline_license.lf
または
/opt/eset/eea/sbin/lic -FILE=offline_license.lf

ESET PROTECTを使用してアクティベーションする

ESET PROTECT Webインターフェイスにログインし、**クライアントタスク > 製品のアクティベーション**に移動して、製品のアクティベーション手順に従います。

ライセンスの場所

ライセンスを購入した場合は、ESETから2つの電子メールが届きます。最初の電子メールには□ESET Business Accountポータルに関する情報が記載されています。2つ目の電子メールには、製品認証キー(XXXXX-XXXXX-XXXXX-XXXXX-XXXXX)またはユーザー名(EAV-xxxxxxxxxx)とパスワード(該当する場合)、公開ライセンスID(xxx-xxx-xxx)□製品名(または製品の一覧)、数量に関する詳細情報が記載されています。

無料の試用ライセンスについては、ESET Business Accountの無料の試用ライセンスを参照してください。

ESET PROTECT Hubアカウント

ESET PROTECT Hubは、ESET PROTECT統合セキュリティプラットフォームへの中央ゲートウェイです。すべてのESETプラットフォームモジュールのIDサブスクリプション、およびユーザー管理を一元化しますESET PROTECT Hubを使用すると、次のことができます。

- セキュリティサブスクリプションの概要を表示
- サブスクライブされたサービスの使用状況とステータスを確認
- 各ESETプラットフォームへの細かいアクセスを割り当て、制御する
- すべてのリンクされた、アクセス可能なESETプラットフォームに対するシングルサインイン

登録済みのESET PROTECT Hubアカウントをお持ちでない場合は、新しいアカウントを作成し、**電子メールアドレス**と**パスワード**でログインしてください。

アクティベーションの状態を確認する

アクティベーションの状態とライセンスの有効期間を確認するには、licユーティリティを実行します。特権ユーザーで次のコマンドを実行します。

Syntax: `/opt/eset/eea/sbin/lic[オプション]`

以下のコマンドは、特権ユーザーで実行する必要があります。
`/opt/eset/eea/sbin/lic -s`
または
`/opt/eset/eea/sbin/lic --status`

製品がアクティベーションされたときの出力例:
```
Status: Activated
Public Id: ABC-123-DEF
License Validity: 2020-03-29
```

製品がアクティベーションされていないときの出力内容:
```
Status: Not activated
```

ESET Endpoint Antivirus for Linuxの特定のインスタンスでESET LiveGuard Advancedがアクティベーションされた場合、出力には関連するライセンス詳細情報が表示されます。

バージョン8.1以降ではESETカスタマーサポートから要求された場合にシートIDを表示するには、次のコマンドを実行します。

```
/opt/eset/eea/sbin/lic -s --with-details
```

コマンドと ESET Endpoint Antivirus for Linux

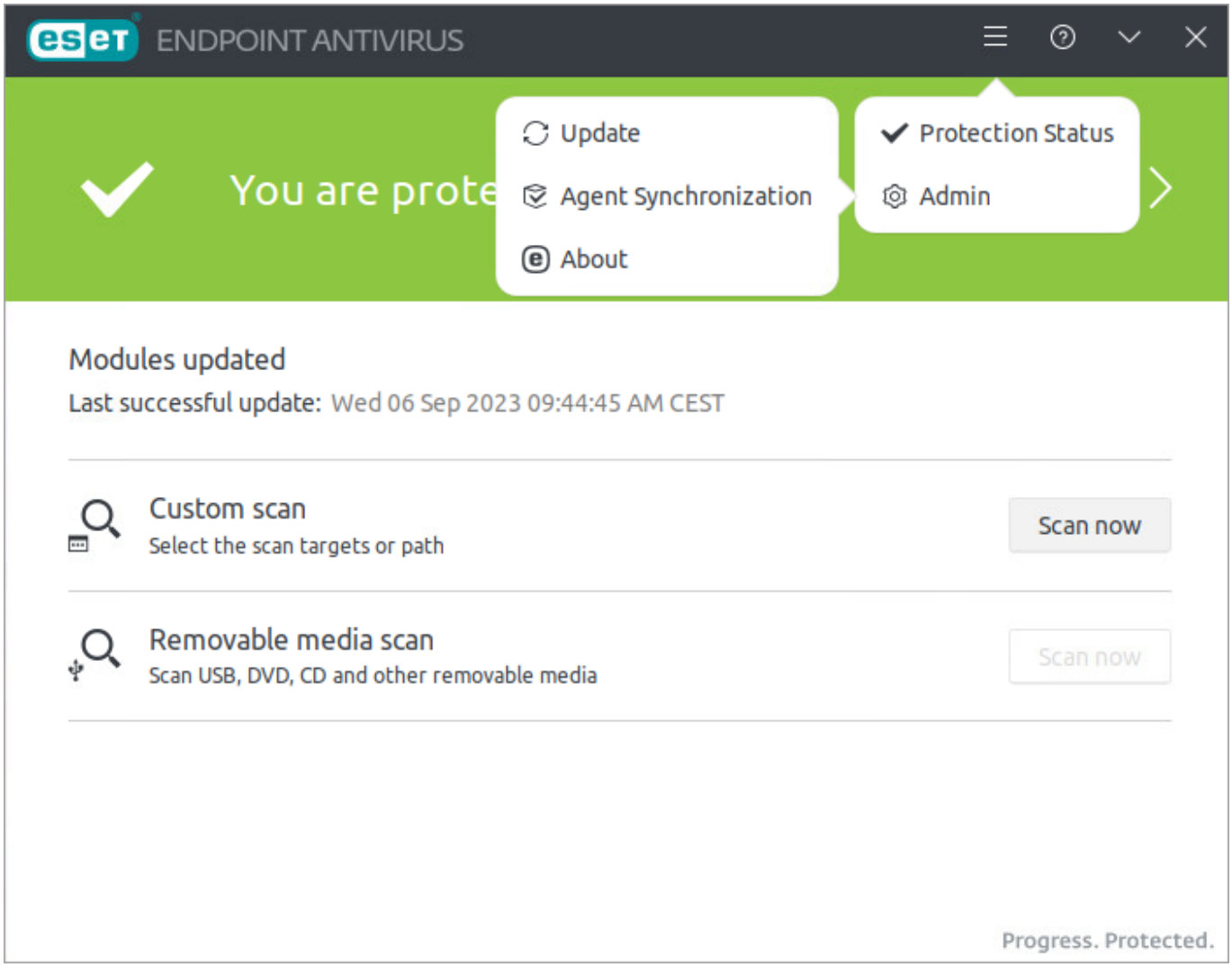
インストール後、ターミナルとESET PROTECTを使用してESET Endpoint Antivirus for Linuxを操作します。

- ターミナル – 日常的なアクティビティ、検査の実行、隔離ログ通知の管理に役立ちます。
- ESET PROTECTまたはESET PROTECT On-Prem - ESET Endpoint Antivirus for Linux設定を変更するために使用します。ターミナルを介して行われる上記のアクティビティに代わる方法でもあります。

ユーザーインターフェイスでは、一部のアクションの実行も有効にできます。

ユーザーインタフェース

ESET Endpoint Antivirus for Linuxには最小限のグラフィカルユーザーインターフェースが導入されています。



ホーム画面には、保護の状態、警告、通知の概要が表示されます。

検査

カスタムパスを検査するには

1. **カスタム検査**セクションで**今すぐ検査**をクリックします。
2. 検査するファイルパスを入力
3. **検査**をクリックします。

リムーバブルメディアデバイスが認識されるとESET Endpoint Antivirus for Linuxは検査を実行できます。**リムーバブルメディア検査**をクリックし、ESET Endpoint Antivirus for Linuxをクリックすると、認識されたすべてのリムーバブルメディアが検査されます。

検査が完了すると、特定された検出と駆除された脅威の簡潔な概要が表示されます。詳細を表示するには、**検査詳細を表示**をクリックします。

メニュー

メニューから任意の画面に移動する場合は、戻るボタンをクリックして、ホーム画面に戻ります。

現在の状況

すべてが問題なく動作している場合、保護の状態(ホーム画面)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。

保護の状態の詳細を表示するには、メニューアイコン > **保護の状態**をクリックします。

アップデート

モジュールのアップデートを手動で実行するには、メニューアイコン > **管理** > **アップデート**をクリックします。画面には、前回の成功したアップデートと前回のアップデートの確認が表示されます。

インストールされたモジュール

インストールされたモジュールを一覧表示するには、次の2つの方法があります。

1. メニューアイコン > **管理** > **アップデート** > **すべてのモジュールを表示**をクリックします。
2. メニューアイコン > **管理** > **バージョン情報** > **すべてを表示**をクリックします。

エージェント同期

リモートでESET Endpoint Antivirus for Linuxを管理する場合は、メニュー > **管理** > **エージェント同期**にManagement Agentの詳細が表示されます。

詳細は次のとおりです。

- インストールされているバージョン – 現在インストールされているリモート管理エージェントのバージョン
- 前回のレプリケーション – リモート管理エージェントとESET PROTECT間の同期の最後の試行が表示されます。

- 前回の成功したレプリケーション
- 前回ステータスログ生成日 – 前回Management Agentがステータスログを生成した日時。ログファイルは */var/log/eset/RemoteAdministrator/Agent/status.html*にあります。

バージョン情報

[バージョン情報]画面には、インストールされたESET Endpoint Antivirus for Linuxのバージョン、オペレーティングシステム、およびシステムリソースの詳細情報が表示されます。

すべてを表示をクリックすると、インストールされたプログラムモジュールの一覧が表示されます。

検査

クイックリンク検査プロファイル

ターミナルウィンドウからオンデマンド検査を実行する

Syntax: `/opt/eset/eea/bin/odscan[オプション]`

オプション – 短縮型	オプション – 標準型	説明
`-l`	`--list`	現在実行中の検査を表示する
	`--list-profiles`	使用可能なすべての検査プロファイルを表示します
	`--all`	他のユーザーが実行した検査も表示します(ルート権限が必要)
`-r`	`--resume=session_id`	`session_id`で特定された、一時停止中の検査を再開します
`-p`	`--pause=session_id`	`session_id`で特定された検査を停止します
`-t`	`--stop=session_id`	`session_id`で特定された検査を停止します
`-s`	`--scan`	検査の開始
	`--show-scan-info`	開始した検査に関する基本情報(`session_id`log_nameを含む)が表示されます。
	`--profile=プロファイル`	選択されたプロファイルを使用して検査します
	`--profile-priority=優先度`	タスクは指定された優先度で実行されます。 優先度は、`normal`lower`lowest`idle`です。
	`--readonly`	駆除せずに検査する
	`--local`	ローカルドライブを検査します
	`--network`	ネットワークドライブを検査します
	`--removable`	リムーバブルメディアを検査します
	`--boot-local`	ローカルドライブのブートセクターを検査します
	`--boot-removable`	リムーバブルメディアのブートセクターを検査します
	`--boot-main`	メインブートセクターを検査します
	`--exclude=ファイル`	選択したファイルまたはディレクトリをスキップします
	`--ignore-exclusions`	除外されたパスと拡張子も検査します

例

バックグラウンドプロセスとして"@Smart scan"検査プロファイルを使用して、再帰的に、*/root/*ディレクトリのオンデマンド検査を実行します。

```
/opt/eset/eea/bin/odscan --scan --profile="@Smart scan" /root/* &
```

複数の対象に関して"@Smart scan"検査プロファイルを使用して、再帰的に、オンデマンド検査を実行します。

```
/opt/eset/eea/bin/odscan --scan --profile="@Smart scan" /root/* /tmp/* /home/*
```

実行中のすべてのスキャンを一覧表示します。

```
/opt/eset/eea/bin/odscan -l
```

session-id "15"の検査を一時停止します。各スキャンには、開始時に生成される独自のセッションIDがあります。

```
/opt/eset/eea/bin/odscan -p 15
```

session-id "15"の検査を停止します。各スキャンには、開始時に生成される独自のセッションIDがあります。

```
/opt/eset/eea/bin/odscan -t 15
```

ディレクトリ*/root/exc_dir*およびファイル*/root/eicar.com*を除外して、オンデマンド検査を実行します。

```
/opt/eset/eea/bin/odscan --scan --profile="@In-depth scan" --
exclude=/root/exc_dir/ --exclude=/root/eicar.com /
```

リムーバブルデバイスのブートセクターを検査します。特権ユーザーで以下のコマンドを実行します:

```
sudo /opt/eset/eea/bin/odscan --scan --profile="@In-depth scan" --boot-removable
```

終了コード

odscanユーティリティは、検査が完了したら、終了コードで終了します。検査が完了したときに、ターミナルウィンドウでecho $?を実行すると、終了コードが表示されます。

終了コード	意味
0	マルウェアは検出されませんでした

終了コード	意味
1	マルウェアが検出され、駆除されました
10	一部のファイルはスキャンできません（マルウェアの可能性あり）
50	マルウェアが検出されました
100	エラー

検査プロファイル

目的の検査パラメーター(Threatsenseパラメーター)を保存して、後で検査を行う際に使用できます。さまざまな検査対象、検査方法、およびその他のパラメーターについて、定期的に行う検査ごとにプロファイルを作成することをお勧めします。

ESET PROTECTを使用して新しいプロファイルを作成する

1. ESET PROTECTで、**ポリシー** > **新しいポリシー**をクリックし、ポリシーの名前を入力します。

2. **設定**をクリックし、ドロップダウンメニューから**ESET Endpoint for Linux (V7+)**を選択します。

3. **検出エンジン** > **マルウェア検査** > **オンデマンド検査**をクリックして、**プロファイルのリスト**の横の**編集**をクリックします。

4. 新しいプロファイルの任意の名前を入力し、**追加**をクリックしてから、**保存**をクリックします。

5**選択したプロファイル**ドロップダウンメニューで、作成した新しいプロファイルを選択し、**マルウェア検査**セクションで検査関連設定を調整します。

6. **割り当て**に移動し、**割り当て**をクリックします。ポリシーが適用されるコンピューターの任意のグループを選択します。

7. **OK**をクリックしてから、**完了**をクリックします。

除外

パフォーマンスの除外

スキャン対象からパス（フォルダー）を除外することで、ファイル システムのマルウェア検査に要する時間を大幅に短縮できます。

1. ESET PROTECTで、**ポリシー** > **新しいポリシー**をクリックし、ポリシーの名前を入力します。

2. **設定**をクリックし、ドロップダウンメニューから**ESET Endpoint for Linux (V7+)**を選択します。

3. **検出エンジン** > **除外**に移動し、**パフォーマンス除外**の横の**編集**をクリックします。

4. **追加**をクリックし、スキャナーでスキップされる**パス**を定義します。任意で、参照用のコメントを追加します。

5. **OK**をクリックしてから、**保存**をクリックして、ダイアログを閉じます。

6. **設定** > **割り当て**をクリックします。ポリシーが適用されるコンピューターの任意のグループを選択します。

7. **OK**をクリックしてから、**完了**をクリックします。

除外パス拡張子

*/root/** - 「*root*」ディレクトリ、およびすべてのサブディレクトリとその内容

/root – /ディレクトリの*root*ファイル

/root/file.txt - *root*ディレクトリのfile.txtのみ

> **パスの途中にあるワイルドカードはサポートされていません**
> パスの途中でワイルドカードを使用しないでください（例：*/home/user/*/data/file.dat*）ESET Endpoint Antivirus for Linuxでサポートされていません。

ファイル拡張子の除外

このタイプの除外は、**リアルタイムファイルシステム保護**と**オンデマンド検査**で設定できます。

1. ESET PROTECTで、**ポリシー** > **新しいポリシー**をクリックし、ポリシーの名前を入力します。

2. **設定**をクリックし、ドロップダウンメニューから**ESET Endpoint for Linux (V7+)**を選択します。

3. 次の場所に移動します。

- **保護** > **リアルタイムファイルシステム保護** > **Threatsenseパラメーター**
- **検出エンジン** > **マルウェア検査** > **オンデマンド検査** > **Threatsenseパラメーター**

4. **検査対象外とするファイル拡張子**の横の**編集**をクリックします。

5. **追加**をクリックして、除外する拡張子を入力します。複数の拡張子を一度に定義するには、**複数の値を入力**をクリックして、任意の拡張子を改行または選択した他の区切り文字で区切って入力します。

6. **OK**をクリックしてから、**保存**をクリックして、ダイアログを閉じます。

7. **設定** > **割り当て**をクリックします。ポリシーが適用されるコンピューターの任意のグループを選択します。

8. **OK**をクリックしてから、**完了**をクリックします。

隔離

隔離の主な機能は、感染ファイルを安全に保存することにあります。ファイルを駆除できない場合、ファイルの削除が安全でもなければ推奨もされない場合、ESET Endpoint Antivirus for Linuxによって誤検出される場合、ファイルを隔離する必要があります。特に、ファイルの動作が疑わしいにもかかわらず、ウイルス対策スキャナーによって検出されない場合は、任意のファイルを選択して隔離することができます。

隔離ディレクトリへのパス：*/var/opt/eset/eea/cache/quarantine/*

隔離ディレクトリは、隔離する項目が最初に存在したときに作成されます。

ターミナルを使用した隔離された項目の管理

Syntax: `/opt/eset/eea/bin/quar[オプション]`

オプション – 短縮型	オプション – 標準型	説明
`-i`	`--import`	ファイルを隔離にインポートします
`-l`	`--list`	隔離ファイルのリストを表示します
`-r`	`--restore=id`	idで特定された隔離された項目を`--restore-path`で定義されたパスに復元します
`-e`	`--restore-exclude=id`	IDで特定され、除外可能列で「x」が設定されている隔離済み項目を復元します
`-d`	`--delete=id`	`id`で特定された隔離済み項目を削除します
	`--restore-path=パス`	隔離された項目を復元するパス
`-h`	`--help`	ヘルプを表示して終了します
`-v`	`--version`	バージョン情報を表示して終了します

> **復元**
> コマンドが特権ユーザーとして実行されない場合は、復元を使用できません。

例

IDが「`09876543210`」の隔離された項目を削除する:

```
/opt/eset/eea/bin/quar -d 09876543210
```

または

```
/opt/eset/eea/bin/quar --delete=09876543210
```

ログインしたユーザーの`Download`フォルダーにID「`9876543210`」の隔離されたアイテムを復元し、名前を`restoredFile.test`に変更します。

```
/opt/eset/eea/bin/quar -r 9876543210 --restore-
path=/home/$USER/Download/restoredFile.test
```

または

```
/opt/eset/eea/bin/quar --restore=9876543210 --restore-
path=/home/$USER/Download/restoredFile.test
```

除外可能列で「**x**」が設定されているIDが「9876543210」の隔離された項目をDownloadフォルダーに復元する:

```
/opt/eset/eea/bin/quar -e 9876543210 --restore-path=/home/$USER/Download/
```

または

```
/opt/eset/eea/bin/quar --restore-exclude=9876543210 --restore-
path=/home/$USER/Download/
```

ターミナルを使用した隔離からのファイルの復元

1. 隔離された項目を一覧表示します。

```
/opt/eset/eea/bin/quar -l
```

2. 復元する隔離済みオブジェクトのIDと名前を検索し、次のコマンドを実行します。

```
/opt/eset/eea/bin/quar --restore=ID_OF_OBJECT_TO_RESTORE --restore-
path=/final/path/of/restored/file
```

ログ

ESET Endpoint Antivirus for Linux ターミナルから実行されるコマンド、および一部のその他のイベントがEEAUによってログに出力されます。

各記録されるアクションには、イベントが発生した日時、コンポーネント(該当する場合)、イベント、ユーザーがあります。

ターミナルからイベントを表示する

ターミナルウィンドウから記録された**ログ**の内容を表示するには、特権ユーザーとしてlslogコマンドラインツールを使用します。

Syntax: /opt/eset/eea/sbin/lslog[オプション]

オプション – 短縮型	オプション – 標準型	説明
-f	--follow	新しいログを待機し、出力の最後に追加します
-o	--optimize	ログを最適化します
-c	--csv	CSV形式でログを表示します
-e	--events	イベントログのリストを出力します
-u	--urls	URLログのリストを出力します

オプション – 短縮型	オプション – 標準型	説明
-l	--device-control	デバイスコントロールログのリストを出力します
-n	--sent-files	分析のために送信されたファイルのリストを表示します
-s	--scans	オンデマンド検査ログのリストを出力します
	--with-log-name	ログ名列を表示します
	--ods-details=log-name	ログ名で特定されたオンデマンド検査の詳細を表示します
	--ods-detections=log-name	ログ名で特定されたオンデマンド検査の検出を表示します
	--ods-notscanned=log-name	ログ名で特定されたオンデマンド検査の検査されていない項目を表示します
-d	--detections	検出ログレコードのリストを出力します
	--ods-events=log-name	ログ名で特定された、特定のオンデマンド検査中に見つかった検出と検査されていないファイルを印刷します。
-b	--blocked-files	ブロックされたファイルログを一覧表示します。
-t	--network	ネットワークアクセス保護ログのリストを出力します
	--va-scans	脆弱性評価の検査ログのリストを表示します。

例

すべてのイベントログを出力する:

```
/opt/eset/eea/sbin/lslog -e
```

現在のユーザーの*Documents*ディレクトリのファイルにCSV形式ですべてのイベントログを保存する:

```
/opt/eset/eea/sbin/lslog -ec > /home/$USER/Documents/eventlogs.csv
```

検出されたすべての脅威とそれに対するアクションを表示する:

```
/opt/eset/eea/sbin/lslog -d
```

通知

EEAUにはアクティビティまたは必要なアクションを通知するさまざまな通知が表示されます。一部の通知は有効または無効にできます

通知は次の情報に関連します。

- オンデマンド検査 –たとえば、リムーバブルデバイスの検査が開始または完了しました。

- デバイスコントロール – デバイスがブロックされたか、デバイスへのデータの書き込みが許可されていません。
- 検出— たとえば、脅威が検出または削除されたか、ファイルが駆除されました。
- Webアクセス保護— たとえば、脅威が検出または削除されたか、ファイルが駆除されました。
- ネットワークアクセス保護 – たとえば、脅威が検出され、ブロックされた場合などです。
- オペレーティングシステム – 再起動が必要か、シャットダウンがスケジュールされています。
- EEAUバージョン8.1以降のESET LiveGuard Advanced – たとえば、ファイルが分析中であるため、一時的に開くことができません。
- EEAUバージョン9.0以降のESET Inspect - たとえば、ファイルアクセスがブロックされているか、セキュリティの理由のためファイルが削除されています。

使用例

この章ではESET Endpoint Antivirus for Linuxの一般的な使用例について説明します:

- モジュール情報の取得
- 検査のスケジュール

モジュール情報の取得

すべてのESET Endpoint Antivirus for Linuxモジュールとバージョンのリストを表示するには、ターミナルウィンドウから次のコマンドを実行します。

```
/opt/eset/eea/bin/upd --list-modules
```

```
/opt/eset/eea/bin/upd --list-modules
出力:
EM000        1074.1 (20190925)       Update module
EM001        1558.2 (20191218)       Antivirus and antispyware scanner module
EM002         20708 (20200121)       Detection engine
EM003          1296 (20191212)       Archive support module
EM004          1197 (20200116)       Advanced heuristics module
EM005          1205 (20191209)       Cleaner module
EM017          1780 (20191217)       Translation support module
EM022          1110 (20190827)       Database module
EM023         15605 (20200121)       Rapid Response module
EM029          1026 (20191107)       Mac/Linux support module
EM037         1833B (20191125)       Configuration module
```

検査のスケジュール

Unixベースのシステムでは、cronを使用して、任意の期間にオンデマンド検査をスケジュールします。

スケジュールされたタスクを設定するには、ターミナルウィンドウからcronテーブル(crontab)を編集します。

初めてクローンテーブルを編集する場合は、対応する番号を押してエディターを選択するオプションが表示されます。使いやすいエディターを選択します(この例では、変更を保存するときに以下のNanoエディターを選択します)

毎週日曜日午前2時に詳細完全ディスク検査をスケジュールする

1. cronテーブルを編集するには、検査対象のフォルダーにアクセスできる特権ユーザーで、ターミナルウィンドウから次のコマンドを実行します。

```
sudo crontab -e
```

2. 矢印キーを使用して、crontabに表示されるテキストの下に移動し、次のコマンドを入力します。

```
0 2 * * 0 /opt/eset/eea/bin/odscan --scan --profile="@In-depth scan" / &>/dev/null
```

3. 変更を保存するには、CTRL + Xを押して、Yと入力して、**Enter**を押します。

毎晩午後11時に特定のフォルダーのスマート検査をスケジュールする

この例では、毎晩*/var/www/download/*フォルダーの検査を実行するようにスケジュールします。

1. cronテーブルを編集するには、検査対象のフォルダーにアクセスできる特権ユーザーで、ターミナルウィンドウから次のコマンドを実行します。

```
sudo crontab -e
```

2. 矢印キーを使用して、crontabに表示されるテキストの下に移動し、次のコマンドを入力します。

```
0 23 * * * /opt/eset/eea/bin/odscan --scan --
profile="@Smart scan" /var/www/download/ &>/dev/null
```

3. 変更を保存するには、CTRL + Xを押して、Yと入力して、**Enter**を押します。

設定

ESET Endpoint Antivirus for Linux設定を変更する場合は、コンピューターがESET PROTECT On-PremまたはESET PROTECTによってリモートで管理されていることを確認してください。

ESET Endpoint Antivirus for Linuxの設定を変更するには:

1. ESET PROTECTで、**ポリシー > 新しいポリシー**をクリックし、ポリシーの名前を入力します。

2. **設定**をクリックし、ドロップダウンメニューから**ESET Endpoint for Linux (V7+)**を選択します。

3. 任意の設定を調整します。

4. **設定 > 割り当て**をクリックします。ポリシーが適用されるコンピューターの任意のグループを選択します。

5. **OK**をクリックしてから、**完了**をクリックします。

> **既存のポリシー設定を調整**
> ESET Endpoint Antivirus for Linuxの既存のポリシー設定を調整するには、ポリシーのリストで変更するポリシーをクリックし、**編集**をクリックします。

検出動作を調整し、製品のアップデートと接続設定を修正することができます。

要件に従ってESET Endpoint Antivirus for Linuxを設定し、後から使用する(またはESET Endpoint Antivirus for Linuxの別のインスタンスで使用する)ために設定を保存するとします。その場合は、*.XML*ファイルにエクスポートできます。

ルート権限で、ターミナルウィンドウから次のコマンドを実行します。

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
```

使用可能なオプション

短縮型	標準型	説明
`-i`	`--json-rpc`	list of json-rpc files
	`--import-xml`	設定をインポートします
	`--export-xml`	設定をエクスポートします
`-h`	`--help`	ヘルプを表示します
`-v`	`--version`	バージョン情報を表示します

検出エンジン

検出エンジンでは、次のオプションを設定できます。

- 除外
- クラウドベース保護
- マルウェア検査

除外

パフォーマンスの除外

スキャン対象からパス（フォルダー）を除外することで、ファイル システムのマルウェア検査に要する時間を大幅に短縮できます。

1. ESET PROTECTで、**ポリシー > 新しいポリシー**をクリックし、ポリシーの名前を入力します。
2. **設定**をクリックし、ドロップダウンメニューから**ESET Endpoint for Linux (V7+)**を選択します。
3. **検出エンジン > 除外**に移動し、**パフォーマンス除外**の横の**編集**をクリックします。
4. **追加**をクリックし、スキャナーでスキップされる**パス**を定義します。任意で、参照用のコメントを追加します。
5. **OK**をクリックしてから、**保存**をクリックして、ダイアログを閉じます。
6. **設定 > 割り当て**をクリックします。ポリシーが適用されるコンピューターの任意のグループを選択します。
7. **OK**をクリックしてから、**完了**をクリックします。

除外パス拡張子

*/root/** - 「*root*」ディレクトリ、およびすべてのサブディレクトリとその内容

/root – /ディレクトリの*root*ファイル

/root/file.txt - *root*ディレクトリのfile.txtのみ

> **パスの途中にあるワイルドカードはサポートされていません**
> パスの途中でワイルドカードを使用しないでください（例：*/home/user/*/data/file.dat*）ESET Endpoint Antivirus for Linuxでサポートされていません。

ファイル拡張子の除外

このタイプの除外は、**リアルタイムファイルシステム保護**と**オンデマンド検査**で設定できます。

1. ESET PROTECTで、**ポリシー > 新しいポリシー**をクリックし、ポリシーの名前を入力します。
2. **設定**をクリックし、ドロップダウンメニューから**ESET Endpoint for Linux (V7+)**を選択します。
3. 次の場所に移動します。

- **保護 > リアルタイムファイルシステム保護 > Threatsenseパラメーター**
- **検出エンジン > マルウェア検査 > オンデマンド検査 > Threatsenseパラメーター**

4. **検査対象外とするファイル拡張子**の横の**編集**をクリックします。
5. **追加**をクリックして、除外する拡張子を入力します。複数の拡張子を一度に定義するには、**複数の**

値を入力をクリックして、任意の拡張子を改行または選択した他の区切り文字で区切って入力します。

6. **OK**をクリックしてから、**保存**をクリックして、ダイアログを閉じます。

7. **設定 > 割り当て**をクリックします。ポリシーが適用されるコンピューターの任意のグループを選択します。

8. **OK**をクリックしてから、**完了**をクリックします。

クラウドベース保護

クイックリンク クラウドベース保護 サンプルの送信 ESET LiveGuard Advanced

ESETLiveGrid®は複数のクラウドベース技術から構成される高度な早期警告システムです。レピュテーションに基づいて新たな脅威を検出し、ホワイトリストを使用して検査パフォーマンスを向上させるのに役立ちます。

ESET PROTECTを介してESET Endpoint Antivirus for Linuxをリモート展開する場合、クラウドベースの保護に関して次のオプションのいずれかを設定することができます。

- ESET LiveGrid®を有効にしないこともできます。ソフトウェアの機能は一切失われませんが、場合によってはESET Endpoint Antivirus for Linuxの新しい脅威への対応が、検出エンジンデータベースアップデートよりも遅くなることがあります。
- 新しいウイルスと新しい危険なコードが検出された場所に関する匿名の情報を提出するようにESET LiveGrid®を設定することができます。このファイルをESETに送信して詳しい解析を受けることができます。これらのウイルスを調査することでESETはウイルス検出機能を最新のものにすることができます。

既定ではESET Endpoint Antivirus for Linuxは、疑わしいファイルを解析するためにESETのウイルスラボに送信するように設定されています。*.doc*または*.xls*など、特定の拡張子の付いたファイルは、常に除外されます。お客様やお客様の組織で送信したくない特定のファイルがあれば、他の拡張子を追加することもできます。

クラウドベース保護

ESET LiveGrid®レピュテーションシステムを有効にする(推奨)

ESETLiveGrid®レピュテーションシステムは、検査済みファイルをクラウドのホワイトリストおよびブラックリスト項目のデータベースと比較し、ESETマルウェア対策ソリューションの効率化を図ります。

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ESET研究所に送信されます。

クラッシュレポートと診断データを送信

クラッシュレポート、モジュール、またはメモリダンプなどのデータを送信します。

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

脅威名、検出日時、検出方法、関連付けられたメタデータ、製品バージョンと設定(システム情報を含む)などの新しく検出された脅威、検査されたファイル(ハッシュ、ファイル名、ファイルの作成元、テ

レメトリー)、ブロックされたURL不審なURLに関する情報を収集します。

連絡先の電子メールアドレス(任意)

不審なファイルに連絡先の電子メールアドレスを添付することができます。この電子メールアドレスは、分析のために詳しい情報が必要な場合の連絡先として使用されます。詳しい情報が必要でない限り、ESETから連絡することはありません。

サンプルの送信

検出されたサンプルの自動送信

選択したオプションに基づいて、分析および将来の検出を改善する目的で、感染したサンプルを ESET に送信できます。

- すべての感染したサンプル
- 文書を除くすべてのサンプル
- 送信しない

不審なサンプルの自動送信

脅威に似た疑わしいサンプル、異常な特性や動作を持つサンプルは、分析のためにESETに送信されます。

- 実行ファイル – 次の実行ファイルタイプが含まれます。*.exe, .dll, .sys*
- アーカイブ – 次のアーカイブファイルタイプが含まれます。*.zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab*
- スクリプト – 次のスクリプトファイルタイプが含まれます。*.bat, .cmd, .hta, .js, .vbs, .ps1*
- その他 – 次のファイルタイプが含まれます。*.jar, .reg, .msi, .swf, .lnk*
- 文書 – アクティブなコンテンツがあるMicrosoft OfficeLibre Officeまたは他のオフィスツールで作成された文書やPDFが含まれます。

除外

除外の横の**編集**オプションをクリックすると、分析を受けるためにESETのウイルスラボに脅威を提出する方法を設定することができます。

サンプルの最大サイズ(MB)

検査対象のサンプルの最大サイズを定義します。

ESET Endpoint Antivirus for Linuxのファイアウォールで以下のネットワーク前提条件が正しく機能するようにします:
- ESET LiveGrid®の正しい操作については、ナレッジベースの記事を参照してください
- ESET LiveGrid®フィードバックシステムの正しい操作(サンプルの提出)については、ナレッジベースの記事を参照してください

ESET LiveGuard Advanced

ESET LiveGuard Advancedは ESETが提供する有料サービスです。世界中の新しい脅威を軽減するために特別に設計された保護のレイヤーを追加することです。

> **使用可否**
> ESET Endpoint Antivirus for Linuxバージョン8.1以降がリモートで管理されている場合にのみ、このサービスを使用できます。
> ESET LiveGuard Advancedのプロアクティブ保護設定によっては、結果が受信されるまで、分析に送信されたファイルの実行がブロックされる場合があります。このようなブロックが実行されると、「操作は許可されていません」などのメッセージが表示されます。

EEAUのインスタンスのESET LiveGuard Advancedサービスのステータスを確認するには、ターミナルウィンドウで特権ユーザーとして次のコマンドのいずれかを実行します。

```
/opt/eset/eea/lib/cloud -l
```

または

```
/opt/eset/eea/lib/cloud --liveguard-status
```

EEAUでサービスを有効にするには

1. ESET PROTECTで、**ポリシー > 新しいポリシー**をクリックし、ポリシーの名前を入力します。
2. **設定**をクリックし、ドロップダウンメニューから**ESET Endpoint for Linux (V7+)**を選択します。
3. **検出エンジン > クラウドベース保護**
4. **ESET LiveGrid®レピュテーションシステムを有効にする(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**を有効にします。
5. 既定のESET LiveGuard Advanced設定を修正するには、ESET LiveGuardをクリックして、使用可能なオプションを調整します。これらのESET LiveGuard設定の詳細については、ESET LiveGuard Advancedドキュメントの見出し「セクション: ESET LiveGuard Advanced」の表を参照してください。
6. **続行 > 割り当て**をクリックします。ポリシーが適用されるコンピューターの任意のグループを選択します。
7. **OK**をクリックしてから、**完了**をクリックします。

ESETステータスポータル

ESETステータスポータルには、ESETクラウドサービスの現在のステータス、スケジュールされた停止、および過去のインシデントが表示されます。サポートされているESETサービスで問題が発生し、ステータスポータルに表示されない場合は、ESETテクニカルサポートにお問い合わせください。

監視チームは、高い信頼性と精度を維持するため、潜在的な問題を内部で検証し、確認されたインシデントを手動で投稿および更新しています。そのため、Status Portalにはわずかに遅れて表示されます。期間が短いインシデントは、手動で確認する前に解決した場合、投稿されない場合があります。

マルウェア検査

このセクションでは、**オンデマンド検査**のスキャンパラメータを選択するためのオプションを提供します。

選択されたプロファイル

オンデマンドスキャナーで使用される特定のパラメーターのセット定義済みの検査プロファイルのいずれかを使用するか、新しいプロファイルを作成できます。検査プロファイルは、さまざまなThreatSenseエンジンパラメーターを使用できます。

プロファイルのリスト

新しいプロファイルを作成するには、[**編集**]をクリックします。プロファイル名を入力し、**追加**をクリックします。新しいプロファイルは、既存の検査プロファイルが一覧表示される**選択されたプロファイル**ドロップダウンメニューに表示されます。

オンデマンド保護および機械学習保護

スキャナー設定は、リアルタイムスキャナーとオンデマンドスキャナーで個別に設定できます。既定で、**リアルタイムファイルシステム保護設定を使用**が有効になっています。有効にすると、関連するオンデマンド検査の設定が**検出応答**セクションから継承されます。

アップデート

既定では、**アップデートの種類**は**通常アップデート**に設定されています。これにより、検出定義データベースと製品モジュールがESETアップデートサーバーから毎日自動的にアップデートされます。

テストモードには、まもなく公開される最新の不具合修正と検出方法が含まれます。ただし、これらは常に安定しているとは限らないため、本番環境での使用は推奨されません。

遅延アップデートにより、特別なアップデートサーバーからの更新が可能になり、新しいバージョンのウイルスデータベースに少なくとも12時間の遅延が発生します（つまり、データベースは実際の環境でテストされ、安定していると見なされます）。

ESET Endpoint Antivirus for Linuxアップデートが安定していない場合は、モジュールのアップデートを前の状態にロールバックします。ターミナルウィンドウから該当するコマンドを実行するか、ESET PROTECTを使用してロールバックします。

最大2つの代替アップデートソース(プライマリとセカンダリサーバー)を定義できます。

既定では、モジュールの1つのスナップショットだけがローカルに保存されます。複数のスナップショットを保存するには、**ローカルに保存するスナップショットの数**を任意の数に増やします。

製品のアップデート

既定では□ESET Endpoint Antivirus for Linux (EEAU)は自動的に製品コンポーネントを更新しません。

EEAUバージョン9. 1以降で自動アップデートを有効にします。

1. ESET PROTECTで、**ポリシー > 新しいポリシー**をクリックし、ポリシーの名前を入力します。

2. **設定**をクリックし、ドロップダウンメニューから**ESET Endpoint for Linux (V7+)**を選択します。

3. **アップデート**をクリックし、**自動アップデート**の横のトグルをクリックします。

4. **設定 > 割り当て**をクリックします。ポリシーが適用されるコンピューターの任意のグループを選択します。

5. **OK**をクリックしてから、**完了**をクリックします。

EEAUバージョン9.0以前で自動アップデートを有効にします。

1. ESET PROTECTで、**ポリシー > 新しいポリシー**をクリックし、ポリシーの名前を入力します。

2. **設定**をクリックし、ドロップダウンメニューから**ESET Endpoint for Linux (V7+)**を選択します。

3. **アップデート**をクリックし、**アップデートモード**リストボックスから**自動アップデート**を選択します。

4. **設定 > 割り当て**をクリックします。ポリシーが適用されるコンピューターの任意のグループを選択します。

5. **OK**をクリックしてから、**完了**をクリックします。

アップデートモード

自動アップデート – 新しいパッケージが自動的にダウンロードされ、次回のOSの再起動時にインストールされます。エンドユーザーライセンス契約のアップデートがある場合、ユーザーは新しいパッケージをダウンロードする前に、更新されたエンドユーザーライセンス契約に同意する必要があります。

アップデートしない – 新しいパッケージはダウンロードされませんが、製品の**ダッシュボード**には新しいパッケージが利用可能であることが表示されます。

カスタムサーバー、ユーザー名、パスワード

複数のEEAUインスタンスを管理し、カスタムロケーションからアップデートする場合は、HTTP(S)サーバー、ローカルドライブ、またはリムーバブルドライブのアドレスと該当するアクセス資格情報を定義します。

保護

保護は、ファイル、デバイス、インターネット通信を制御することにより、悪意のあるシステム攻撃から保護します。たとえば、マルウェアとして分類されたオブジェクトが検出されると、修復が開始します。保護は、マルウェアをブロックしてから、その駆除、削除、または隔離に移動するという処理のいずれかを実行することで、マルウェアを回避できます。

検出応答

次のカテゴリのレポートレベルと保護レベルを設定できます。

- **マルウェア検出(機械学習を利用)** – コンピューターウイルスは、コンピューターの既存のファイルの前後に追加される悪意のあるコードです。ただし、「ウイルス」という用語は、よく間違っ

て使用されます。「マルウェア」(悪意のあるソフトウェア)がより正確な用語です。マルウェアの検出は、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。
このような種類のアプリケーションについては、用語集をご覧ください。

• **望ましくない可能性のあるアプリケーション** – グレイウェアまたは望ましくない可能性のあるアプリケーション(PUA)は、ウイルスやトロイの木馬など、他の種類のマルウェアほど明確に悪意のあるものではない幅広いカテゴリのソフトウェアです。ただし、望ましくない追加のアプリケーションをインストールしたり、デジタルデバイスの動作を変更したり、ユーザーによって承認されていない、または想定されていないアクティビティを実行したりすることがあります。
このような種類のアプリケーションについては、用語集をご覧ください。

• **疑わしい可能性があるアプリケーション**には、圧縮形式またはプロテクタで圧縮されたプログラムが含まれます。この種類の防御は、多くの場合、マルウェアの作成者が検知されるのを逃れるために利用します。

• **安全ではない可能性があるアプリケーション**は、不正な目的で悪用される可能性のある、市販の適正なソフトウェアです。安全ではない可能性のあるアプリケーションの例には、リモートアクセスツール、パスワード解析アプリケーション、キーロガー(ユーザーが入力した各キーストロークを記録するプログラム)が含まれます。
このような種類のアプリケーションについては、用語集をご覧ください。

報告

レポートは、検出エンジンと機械学習コンポーネントによって実行されます。レポートのしきい値は、環境とニーズに合わせてカスタマイズできます。環境内の動作を監視し、別のレポート設定がより適しているかどうかを判断することをお勧めします。これらのレポート設定は、オブジェクトのブロック、駆除、または削除には影響しません。

最大	最大の感度に構成されたレポート。報告される検出数が多くなります。**攻撃的レベルの**設定では、オブジェクトが悪意のあるオブジェクトとして誤って識別される場合があり、そのようなオブジェクトに対してアクションが実行されます(保護の設定に応じて)。
標準	この設定は、検出率のパフォーマンスおよび精度と、誤って報告されるオブジェクト数の間でバランスを保つように最適化されています。
最小	レポートは、誤って特定されるオブジェクトの数を最小限に抑えながら、効率的なレベルの保護を維持するように設定されています。確率が明らかであり、マルウェアの動作と一致するときにのみ、オブジェクトが報告されます。
オフ	レポートがアクティブではありません。検出は見つからないか、報告されないか、駆除されません。 オフはマルウェアレポートには使用できず、望ましくない可能性のある、安全でないアプリケーションの既定値になっています。

保護

オブジェクトが報告されると、プログラムはそのオブジェクトをブロックし、駆除、削除、または隔離に移動します。

最大	報告された最大(以下の)レベルの検出はブロックされ、自動修復(駆除など)が開始します。すべてのエンドポイントが攻撃的設定で検査され、誤って報告されたオブジェクトが検出除外に追加されたときには、この設定が推奨されます。
標準	報告された標準(以下)レベルの検出はブロックされます。自動修正(駆除)が開始します。
最小	報告された最小レベルの検出はブロックされます。自動修正(駆除)が開始します。
オフ	誤って報告されたオブジェクトを特定して除外する際に便利です。 オフはマルウェア保護には使用できず、望ましくない可能性のある、安全でないアプリケーションの既定値になっています。

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は、システム内のすべてのウイルス対策関連のイベントを制御します。すべてのファイルは、コンピューターで開かれたり、作成されたり、実行されたりするときに、悪意のあるコードがないか検査されます。既定では、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、中断のない検索を提供します。

リアルタイムファイルシステム保護では、アーカイブファイルの内容が検査されません。ハードドライブにダウンロードするときに、特定の自己解凍アーカイブの内容が検査されます。

特殊な場合(別のリアルタイムスキャナーと競合する場合など)は、次の方法でリアルタイムファイルシステム保護を無効にできます。

1. ESET PROTECTで、**ポリシー > 新しいポリシー**をクリックし、ポリシーの名前を入力します。
2. **設定**をクリックし、ドロップダウンメニューから**ESET Endpoint for Linux (V7+)**を選択します。
3. **保護 > リアルタイムファイルシステム保護**をクリックします。
4. **リアルタイムファイルシステム保護**を無効にします。
5. **設定 > 割り当て**をクリックします。ポリシーが適用されるコンピューターの任意のグループを選択します。
6. **OK**をクリックしてから、**完了**をクリックします。

検査するメディア

既定では、あらゆる種類のメディアに対して潜在的な脅威が検査されます。

- **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します。
- **リムーバブルメディア** - CD/DVD、USB記憶装置、Bluetoothデバイスなどを検査します。
- **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します。

既定の設定を変更するのは、あるメディアの検査によりデータ転送が極端に遅くなるときなど、特別な場合だけにすることをお勧めします。

検査のタイミング

既定では、ファイルを開いたり、作成したり、実行したりするときに、すべてのファイルが検査されます。既定の設定ではコンピュータが最大限のレベルでリアルタイムに保護されるので、既定の設定を変更しないことをお勧めします。

- **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のアクセス** – 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。

リアルタイムファイルシステム保護は、ファイルアクセスなど、さまざまなシステムイベントごとにト

リガされ、すべての種類のメディアを確認します。リアルタイムファイルシステム保護は、ThreatSenseテクノロジの検出方法(「ThreatSenseパラメータ」セクションに説明があります)を使用しており、新しく作成されたファイルを既存のファイルと異なる方法で扱うように設定できます。たとえば、新しく作成されたファイルを今までよりも細かく監視するように、リアルタイムファイルシステム保護を設定できます。

システムの使用領域を最小化するために、リアルタイム保護の使用時、すでに検査されたファイルは(変更がない限り)繰り返し検査されません。ファイルは、各検出エンジンデータベースアップデートの直後にもう一度検査されます。なおこの動作は**スマート最適化**を使用して設定します。**スマート最適化**が無効の場合、全てのファイルがアクセスのたびに検査されます。この設定を修正するには、ESET PROTECTを使用します。

1. ESET PROTECTで、**ポリシー > 新しいポリシー**をクリックし、ポリシーの名前を入力します。
2. **設定**をクリックし、ドロップダウンメニューから**ESET Endpoint for Linux (V7+)**を選択します。

3. **保護 > リアルタイムファイルシステム保護 > ThreatSenseパラメーター**をクリックします。

4. **スマート最適化を有効にする**をオンまたはオフにします。

5. **設定 > 割り当て**をクリックします。ポリシーが適用されるコンピューターの任意のグループを選択します。

6. **OK**をクリックしてから、**完了**をクリックします。

ThreatSenseパラメーター

ThreatSenseは、ウイルスを検出する多数の複雑な方法から構成される技術です。この技術は事前対応型なので、新しいウイルスが広がる初期の段階でも保護することができます。この技術では、システムのセキュリティを大幅に強化するために連携して動作するコード分析、コードエミュレーション、汎用シグネチャ、ウイルスシグネチャを組み合わせて使用します。検査エンジンは、複数のデータストリームを同時に検査して、最大限の効率および検出率を確保することができます。またThreatSense技術によってルートキットを除去することもできます。

ThreatSenseエンジンの設定オプションを使用すると、ユーザーはさまざまな検査パラメーターを指定することができます。

- 検査するファイルの種類および拡張子
- さまざまな検出方法の組み合わせ
- 駆除のレベルなど

ESET PROTECTを使用して、構成を変更します。以下のモジュールのいずれかを選択して、**ThreatSenseパラメーター**をクリックします。セキュリティシナリオごとに異なる設定が必要になることがあります。これを念頭に、ThreatSenseは、次の保護モジュールについて個々に設定することができます。

- **リアルタイムファイルシステム保護**
- **マルウェア検査**
- **リモート検査**
- **Webアクセス保護**

ThreatSenseのパラメーターは機能ごとに高度に最適化されているので、パラメーターを変更すると、システムの動作に大きく影響することがあります。たとえば、常にランタイム圧縮形式をスキャンするようにパラメーターを変更するか、リアルタイムファイル保護機能のアドバンスドヒューリスティックを有効にすると、システムの処理速度が低下することがあります(通常は、新しく作成されたファイルのみがこれらの方法を使用してスキャンされます)。

検査するオブジェクト

このセクションでは、感染を検査するコンピュータのコンポーネントおよびファイルを定義できます。

- **ブートセクタ/UEFI** – マスターブートレコードにウイルスがいないかブートセクタ/UEFIを検査します
- **電子メールファイル** – プログラムは以下の拡張子をサポートします:DBX (Outlook Express)およびEML
- **アーカイブ** – プログラムは以下の拡張子をサポートします:ARJ、BZ2、CAB、CHM、DBX、GZIP、ISO/BIN/NRG、LHA、MIME、NSIS、RAR、SIS、TAR、TNEF、UUE、WISE、ZIP、ACEおよびその他多数
- **自己解凍アーカイブ** – 自己解凍アーカイブ(SFX)は自分自身を展開できるアーカイブです
- **圧縮された実行形式** – 圧縮された実行形式(標準の解凍形式とは異なる)は、実行後メモリー内で解凍されます。スキャナでは、コードのエミュレーションによって、標準の静的圧縮形式(UPX、yoda、ASPack、FSGなど)のほかにも多数の圧縮形式を認識できます

> リアルタイムファイルシステム保護では、アーカイブファイルの内容が検査されません。ハードドライブにダウンロードするときに、特定の自己解凍アーカイブの内容が検査されます。

検査オプション

システムの侵入を検査するときに使用する方法を選択します。使用可能なオプションは次のとおりです。

- **ヒューリスティック** – ヒューリスティックは、悪意のあるプログラムの活動を分析するアルゴリズムです。 この技術の主な利点は、前には存在しなかったり、これまでのウイルス定義データベースで特定されていなかったりした悪意のあるソフトウェアを特定できる点です。欠点は、非常に少ないとはいえ、誤検出の可能性がある点です
- **アドバンスドヒューリスティック/DNAシグネチャ** – アドバンスドヒューリスティックは、ESETが開発した独自のヒューリスティックアルゴリズムで構成されます。このアルゴリズムは、コンピューターワームやトロイの木馬を検出するために最適化され、高度なプログラミング言語で記述されています。アドバンスドヒューリスティックを使用するとESET製品の脅威検出機能が大幅に高まります。シグネチャは確実にウイルスを検出し、特定することができます。自動アップデートシステムを利用することにより、新しいシグネチャを使用するためのウイルス検出時間を短縮できます。シグネチャの欠点は、既知のウイルス(またはこれらのウイルスの多少の変更が加えられたバージョン)しか検出しない点です。

除外

拡張子は、Filenameの一部であり、ピリオドで区切られています。拡張子は、ファイルの種類と内容を規定しますThreatSenseパラメーター設定のこのセクションでは、検査から除外するファイルの種類を定義できます。

その他

コンピュータの検査でThreatSenseエンジンパラメータ設定を設定する場合は、[**その他**]セクションの次のオプションも設定できます

- **低優先でバックグラウンドで検査** – 検査が行われるたびに、一定の量のシステムリソースが使用されます。システムリソースにかなりの負荷がかかるプログラムを使用している場合、優先度が低い検査をバックグラウンドで実行することによって、アプリケーションのためにリソースを節約することができます

- **スマート最適化を有効にする** – スマート最適化を有効にすると、スキャンの速度を最高に保ちながら最も効率的なスキャンレベルが確保されるように、最適な設定が使用されます。さまざまな保護モジュールで高度に検査を行い、それぞれで異なる検査方法を使用して、それらを特定のファイルタイプに適用します。スマート最適化を無効にすると、特定のモジュールのThreatSenseコアのユーザー定義設定のみが検査の実行時に適用されます。

- **最終アクセスのタイムスタンプを保持** – このオプションを選択すると、スキャンしたファイルを更新するのではなく、元のアクセス時間を保持します。（たとえば、データバックアップシステムで使用する場合）

制限

[**制限**]セクションでは、検査対象のオブジェクトの最大サイズおよびネストされたアーカイブのレベルを指定できます。

オブジェクトの設定

オブジェクト設定を修正するには、**既定のオブジェクト設定**を無効にします。

- **オブジェクトの最大サイズ** – 検査対象のオブジェクトの最大サイズを定義します。これにより、ウイルス対策機能では、指定した値より小さいサイズのオブジェクトのみが検査されます。上級ユーザーが大きいオブジェクトを検査から除外する必要がある場合のみ、このオプションを変更してください。既定値:無制限

- **オブジェクトの最長検査時間(秒)** – オブジェクトの検査の最長時間の値を定義します。ここでユーザー定義の値が入力されていると、検査が終わっているかどうかにかかわらず、その時間が経過するとウイルス対策機能は検査を停止します。既定値:無制限

アーカイブ検査の設定

アーカイブ検査設定を変更するには、**既定のアーカイブ検査の設定**オプションを選択解除します。

- **スキャン対象の下限ネストレベル** – アーカイブの検査の最大レベルを指定します。既定値:10

- **スキャン対象ファイルの最大サイズ** – このオプションでは、検査対象のアーカイブ(抽出された場合)に含まれているファイルの最大サイズを指定できます。既定値:無制限

> **既定値**
> 既定値を変更することはお勧めしません。通常の状況ではそれらを変更する理由はありません。

追加のThreatSenseパラメータ

新しく作成または変更されたファイルでの感染の可能性は、既存ファイルより比較的高くなります。そのため、それらのファイルは、検査パラメーターを追加して検査します。標準のウイルス定義ベースの検査方法とともに、アドバンスドヒューリスティックも使用され、モジュールのアップデートの公開前でも新しい脅威を検出できます。新規に作成したファイル以外に、自己解凍形式のアーカイブ(SFX)およびランタイムパッカー(内部圧縮された実行可能ファイル)も検査されます。

既定では、アーカイブは最大で10番目のネストレベルまで検査され、実際のサイズに関係なく検査されます。アーカイブ検査設定を変更するには、**既定のアーカイブスキャンの設定**オプションを選択解除します。

Webアクセス保護

Webアクセス保護は、Webブラウザーとリモートサーバー間のHTTP (ハイパーテキスト転送プロトコル)およびHTTPS (暗号化通信)通信を検査します。

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アクセス保護には、ブラックリストによるブロックとコンテンツによるブロックの2つのレベルがあります。

Webアクセス保護を有効にする - Webブラウザー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。

除外されたアプリケーション – プロトコルフィルタリングから特定のネットワーク対応アプリケーションの通信を除外するには、編集をクリックします。

除外されたIP – プロトコルコンテンツフィルタリングからIPアドレスを除外するには、編集をクリックします。

Webアクセス保護では、次のVPNがサポートされています。

- Cisco AnyConnect VPN
- OpenVPN
- ProtonVPN
- PulseSecure
- Wireguard

VPNは、NATを使用しないルーティング設定を持つ既定のクライアント設定でサポートされます。

現在、Webアクセス保護は、ESET Endpoint Antivirus for Linuxで明示的に設定されているHTTPプロキシのみをサポートしています。システムプロキシとHTTPSプロキシはサポートされていません。

URLアドレス管理

URLアドレス管理では、ブロック、許可、またはチェックから除外するURLアドレスを指定できます。**ブロックする**アドレスのリストのWebサイトは、**許可する**アドレスのリストにも登録されていない場合は、アクセスできません。**コンテンツ検査から除外される**アドレスのリストにあるWebサイトは、悪意のあるコードを検査せずにアクセスできます。

アクティブな**許可する**アドレスのリストにあるアドレスを除き、すべてのHTTPアドレスをブロックする場合は、アクティブな**ブロックする**アドレスのリストに*を追加します。

アドレスリストを作成するときに、特殊記号「*」(アスタリスク)と「?」(疑問符)を使用できます。アスタリスクは任意の文字列を表し、疑問符は任意の記号を表します。

除外アドレスを指定する際には、細心の注意を払ってください。その一覧には信頼できる安全なアドレスだけを掲載すべきだからです。同様に、記号の*および?をこの一覧で正しく使用してください。

リストをアクティベーションにするには、**リストのアクティブ化**を選択します。現在のリストに含まれるアドレスが入力されたときに通知を受け取る場合は、**適用時に通知**を選択します。詳細については、URLアドレス管理を参照してください。

HTTPSトラフィック検査

HTTPSトラフィック検査を使用するとSSLおよびTLSプロトコルを使用する通信の脅威をチェックできますSSLで保護された通信には、信頼できる証明書、不明な証明書SSLで保護された通信の検査対象から除外された証明書を使用する、さまざまな検査モードがあります。プログラムは、**HTTPSプロトコルで使用されるポート**で定義されているポート(443、0 – 65535)のトラフィックのみを検査します。詳細については、HTTPSトラフィック検査を参照してください。

ThreatSense パラメータ

ThreatSenseパラメーターを使用すると、検査するオブジェクトのタイプ、検査オプションなどWebアクセス保護の設定を設定できます。詳細については、ThreatSenseパラメーターを参照してください。

対象外のアプリケーション

これを使用して、特定のネットワーク対応アプリケーションの通信をプロトコルフィルタリングから除外します。選択したアプリケーションのHTTP/POP3/IMAP通信の脅威は検査されません。この手法は、プロトコルフィルタリングを有効にした状態でアプリケーションが正しく機能しない場合にのみ使用することをお勧めします。

検査からアプリケーションを除外するには、次の手順を実行します。

1. ESET PROTECTで、**ポリシー > 新しいポリシー**をクリックし、ポリシーの名前を入力します。
2. **設定**をクリックし、ドロップダウンメニューから**ESET Endpoint for Linux (V7+)**を選択します。
3. **保護 > Webアクセス保護**に移動し、**対象外のアプリケーション**の横にある**編集**をクリックします。
4. **追加**をクリックし、スキャナーでスキップされる**パス**を定義します。
5. **OK**をクリックしてから、**保存**をクリックして、ダイアログを閉じます。

6. **設定** > **割り当て**をクリックします。ポリシーが適用されるコンピューターの任意のグループを選択します。

7. **OK**をクリックしてから、**完了**をクリックします。

除外パス拡張子

*/root/** - 「*root*」ディレクトリ、およびすべてのサブディレクトリとその内容

/root – /ディレクトリの*root*ファイル

/root/file.txt - *root*ディレクトリのfile.txtのみ

> **パスの途中にあるワイルドカードはサポートされていません**
> パスの途中でワイルドカードを使用しないでください（例：*/home/user/*/data/file.dat*）ESET Endpoint Antivirus for Linuxでサポートされていません。

除外されたIP

これを使用して、プロトコルコンテンツフィルタリングからIPアドレスを除外します。選択したIPアドレスに対する送受信のHTTP/POP3/IMAP通信の脅威は検査されません。このオプションは信頼できるとわかっているアドレスに対してのみ使用することをお勧めします。

検査からIPアドレスを除外するには、次の手順を実行します。

1. ESET PROTECTで、**ポリシー** > **新しいポリシー**をクリックし、ポリシーの名前を入力します。

2. **設定**をクリックし、ドロップダウンメニューから**ESET Endpoint for Linux (V7+)**を選択します。

3. **保護** > **Webアクセス保護**に移動し、**対象外のIPアドレス**の横にある**編集**をクリックします。

3. **追加**をクリックし、除外するIPアドレスを入力します。複数のIPアドレスを一度に定義するには、**複数の値を入力**をクリックして、任意のIPアドレスを改行または選択した他の区切り文字で区切って入力します。

4. **OK**をクリックしてから、**保存**をクリックして、ダイアログを閉じます。

5. **設定** > **割り当て**をクリックします。ポリシーが適用されるコンピューターの任意のグループを選択します。

6. **OK**をクリックしてから、**完了**をクリックします。

IPアドレスの例

IPv4アドレス:

単一のアドレス — 個々のコンピューターのIPアドレス(192.168.1.100 など)を追加します。

アドレス範囲 — 開始IPアドレスと終了IPアドレスを入力して、複数のコンピューターのIP範囲を指定します(例: 192.168.1.1-192.168.1.99)。

サブネット — IPアドレスとマスクで定義されたサブネット(コンピューターのグループ)。たとえば、255.255.255.0は192.168.1.0サブネットのネットワーク マスクであり、192.168.1.0/24のサブネットのタイプ全体を除外します。

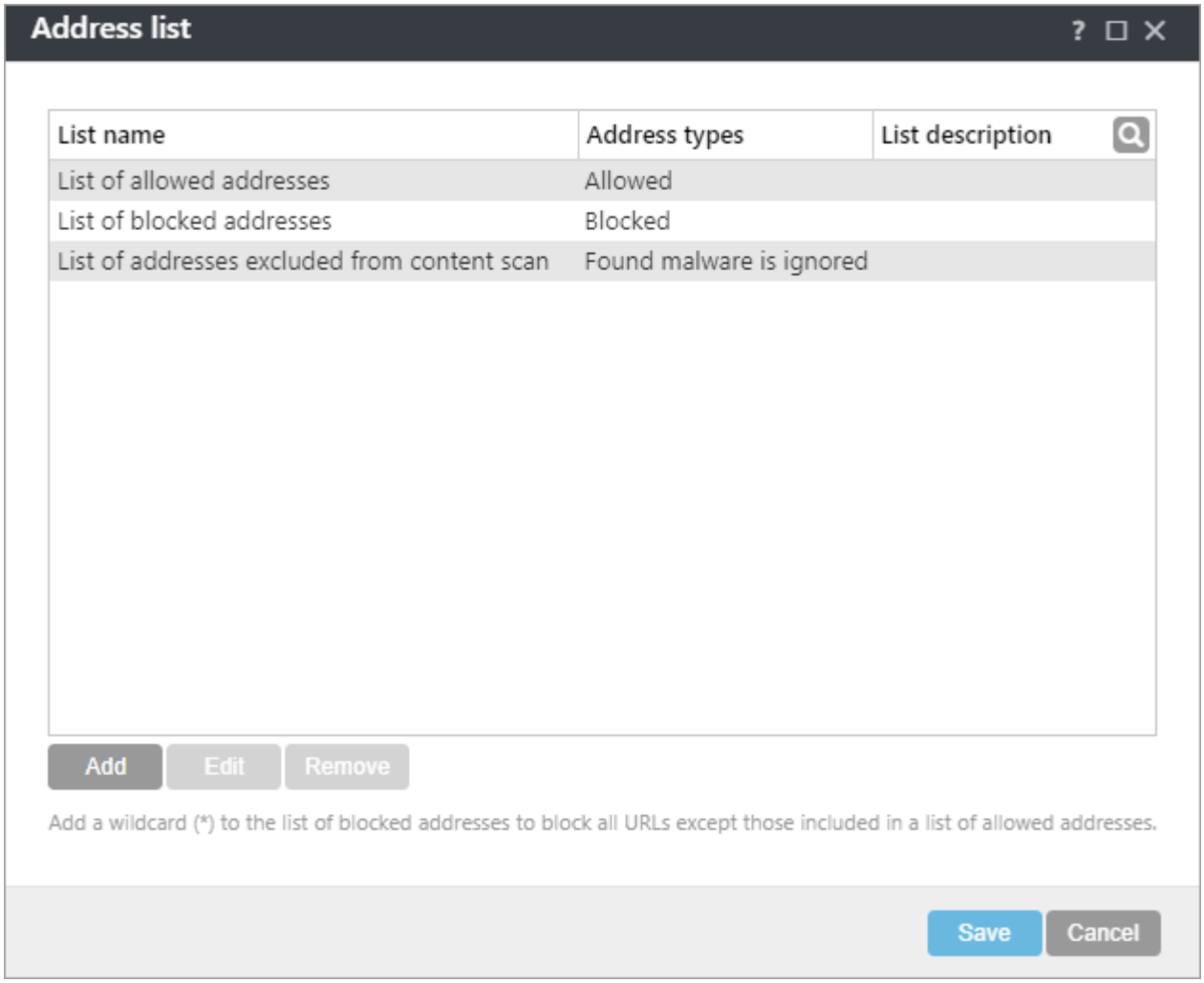
IPv6アドレス:

単一のアドレス — 個々のコンピューターのIPアドレス(::ffff:c0a8:164)を追加します。

サブネット — IPアドレスとマスクで定義されたサブネット(コンピューターのグループ)(::ffff:c0a8:100/64)

URLアドレス管理

このセクションでは、ブロック、許可、またはチェックから除外するHTTPアドレスのリストを指定できます。



既定では、次のリストを使用できます。

- **許可されたアドレスのリスト** – ブロックされたアドレスのリストに* (すべてに一致)が含まれている場合、このリストで指定されたアドレスのみにアクセスできます。

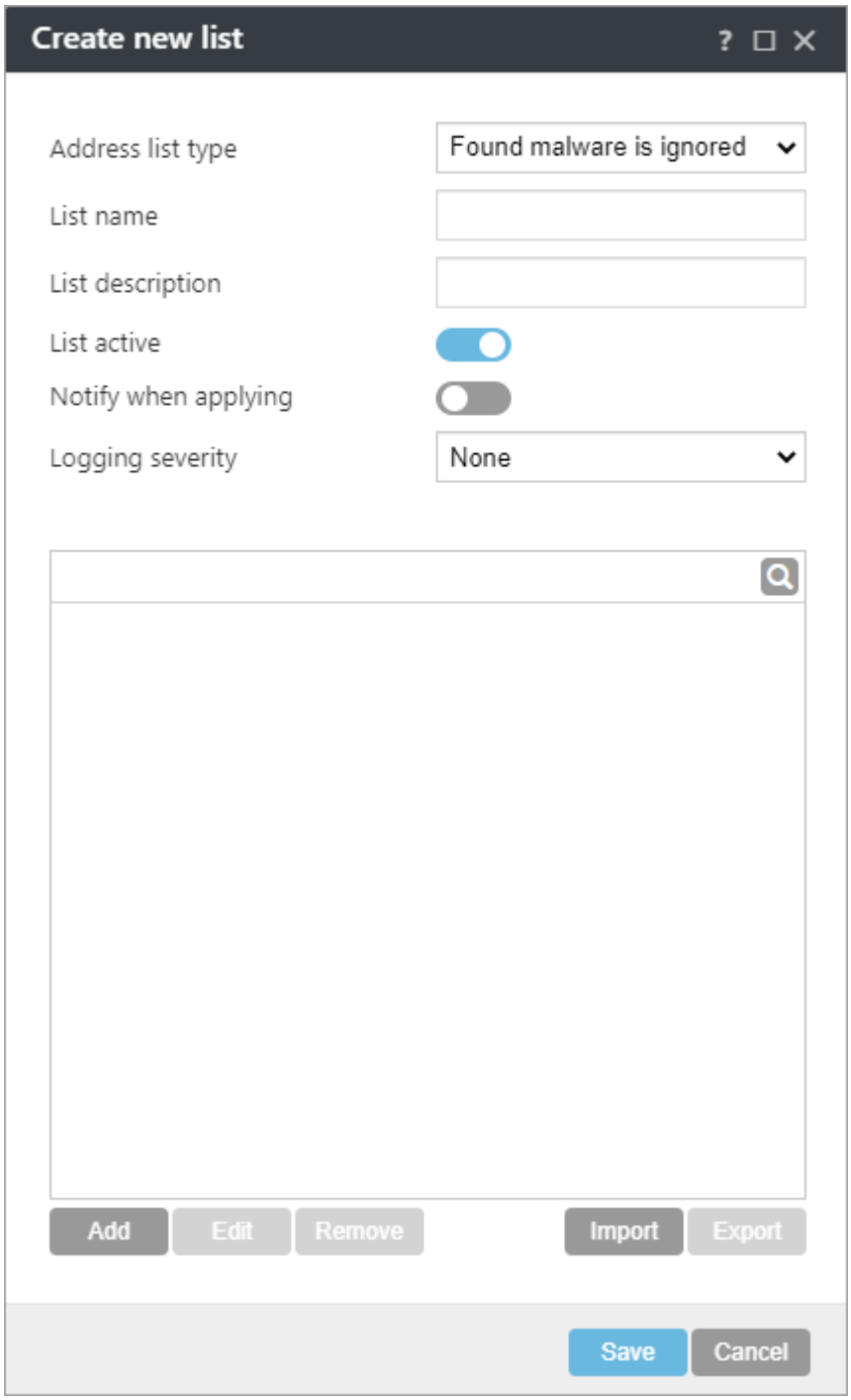
- **ブロックされたアドレスのリスト** – このリストで指定されたアドレスへのアクセスは、アドレスが許可されたアドレスのリストに含まれない限り許可されません。

- **コンテンツ検査から除外されるアドレスのリスト** – 悪意のあるコードがないか検査することなくアドレスにアクセスします。

追加をクリックして、新しいリストを作成します。選択したリストを削除するには、**削除**をクリックします。

新規リストの作成

このダイアログウィンドウでは、ブロック、許可、またはチェックから除外されるURLアドレス/マスクの新規リストを設定できます。



アドレスリストのタイプ

ドロップダウンメニューからアドレスリストの種類を選択します。

- **検出されたマルウェアは無視されます** – アドレスをリストに追加すると、悪意のあるコードのチェックは実行されません。
- **ブロック** – このリストで指定されたアドレスへのアクセスはブロックされます。
- **許可** – このリストで指定されたアドレスへのアクセスは許可されます。このリストのアドレスは、ブロックされたアドレスのリストと一致する場合でも、許可されます。

リスト名 – リストの名前を指定します。このフィールドは、事前定義されたリストでは編集できません。

リストの説明 – 識別しやすいようにリストの説明を入力します。このフィールドは、事前定義されたリストでは編集できません。

リストのアクティブ化の横にあるトグルをクリックして、このリストを無効または有効にします。これは、リストを完全に削除したくない場合に便利です。

適用時に通知の横にあるトグルをクリックしてWebサイトにアクセスするために特定のリストが使用されたときに通知を受け取ります。たとえばWebサイトがブロックまたは許可されたアドレスのリストに含まれており、そのサイトがリストを理由にブロックまたは許可されると、通知を受け取ります。通知には、リストの名前が含まれます。

ログ記録の重大度

ドロップダウンリストからログの重要度を選択します。

- **なし** – メッセージは記録されません。
- **診断** - PIDやパスなどの接続情報を含む、診断メッセージを記録します。
- **情報** – 情報メッセージを記録し、ESET PROTECTに送信します。
- **警告** – 重大なエラー、エラー、および警告メッセージを記録し、ESET PROTECTに送信します。

情報と警告のロギング詳細レベルは、ドメイン内にワイルドカードを持たないコンポーネントが少なくとも2つ含まれているルールでのみ使用できます。例:
- *.domain.com/*
- *www.domain.com/*

コントロール要素

- **追加** – 新しいURLアドレスをリストに追加します。複数のURLアドレスを一度に定義するには、**複数の値を入力**をクリックして、任意のURLアドレスを改行または選択した他の区切り文字で区切って入力します。
- **編集** – リストの既存のアドレスを修正します。
- **削除** – リストの既存のアドレスを削除します。
- **インポート** - URLアドレスを含むテキストファイル(値は改行で区切ります。例: UTF-8エンコード

を使用した*.TXT*)をインポートします。

URLマスク

リモートサーバーの完全な名前が不明な場合、またはリモートサーバーのグループ全体を指定する場合は、マスクを使用できます。マスクには、記号の"?"と"*"があります。

- 記号1つを表すには、"?"を使用します 。
- 文字列1つを表すには、"*"を使用します。

たとえば*.?uは、最後の部分が文字uで終わり、不明な記号(.eu.auなど)が含まれるすべてのアドレスに適用されます。

たとえば*o?は、最後の1文字がoであるアドレスを示します。

ドメイン全体を一致させるには、*.domain.com/*の形式で入力します。マスク内のプロトコルプレフィックス*http://*や*https://*の指定は任意です。

複数のURLマスクを一度に定義するには、**複数の値を入力**をクリックして、任意のURLマスクを改行または選択した他の区切り文字で区切って入力します。

HTTPSトラフィック検査

ESET Endpoint Antivirus for LinuxはSSLおよびTLSプロトコルを使用する通信の脅威を検査できますSSLで保護された通信には、信頼できる証明書、不明な証明書SSLで保護された通信の検査対象から除外された証明書を使用する、さまざまな検査モードがあります。プログラムは、**HTTPSプロトコルで使用されるポート**で定義されているポート(443、0 – 65535)のトラフィックのみを検査します。

SSL/TLSを有効にする - SSL/TLSプロトコルフィルタリングは既定で有効になっています。

SSL/TLSモード – 次の2つのオプションから選択できます。

- **ポリシーモード** – では、構成された例外を除き、すべてのSSL/TLS接続がフィルタリングされます。
- **自動モード** – 設定されている除外を除き、以下でサポートされているSSL/TLS接続のみがフィルタリングされます。

自動モードのSSL/TLSは、次のブラウザーとアプリケーションをサポートしています。

- Edge
- Firefox
- Chrome
- Chromium
- wget
- curl

ブラウザーまたはアプリケーションは、既定の配布パッケージマネージャーでインストールする必要があります。ブラウザーの統合には初期起動が必要です。

アプリケーションス検査ルール - SSL/TLSフィルタリングされたアプリケーションのリストを作成して、特定のアプリケーションのESET Endpoint Antivirus for Linux動作をカスタマイズします。

証明書ルール - 既知の証明書のリストを作成して、特定のSSL証明書のESET Endpoint Antivirus for Linux動作をカスタマイズします。

ESETによって信頼されたドメインのトラフィックを検査しない – 有効にすると、信頼されたドメインとの通信は検査から除外されます。ドメインの信頼性は、組み込みのホワイトリストによって決定されます。

古いSSLで暗号化されたトラフィックをブロックする – 以前のバージョンのSSLプロトコルを使用した通信は自動的にブロックされます。

HTTPSプロトコルで使用するポート – トラフィックを検査するポートを指定します。複数のポート番号は、コンマで区切る必要があります。既定値:443, 0-65535

ルート証明書

サポートされているアプリケーションでSSL/TLS通信を正しく機能させるためにESETのルート証明書は既知のルート証明書(発行元)のリストに自動的に追加されます。

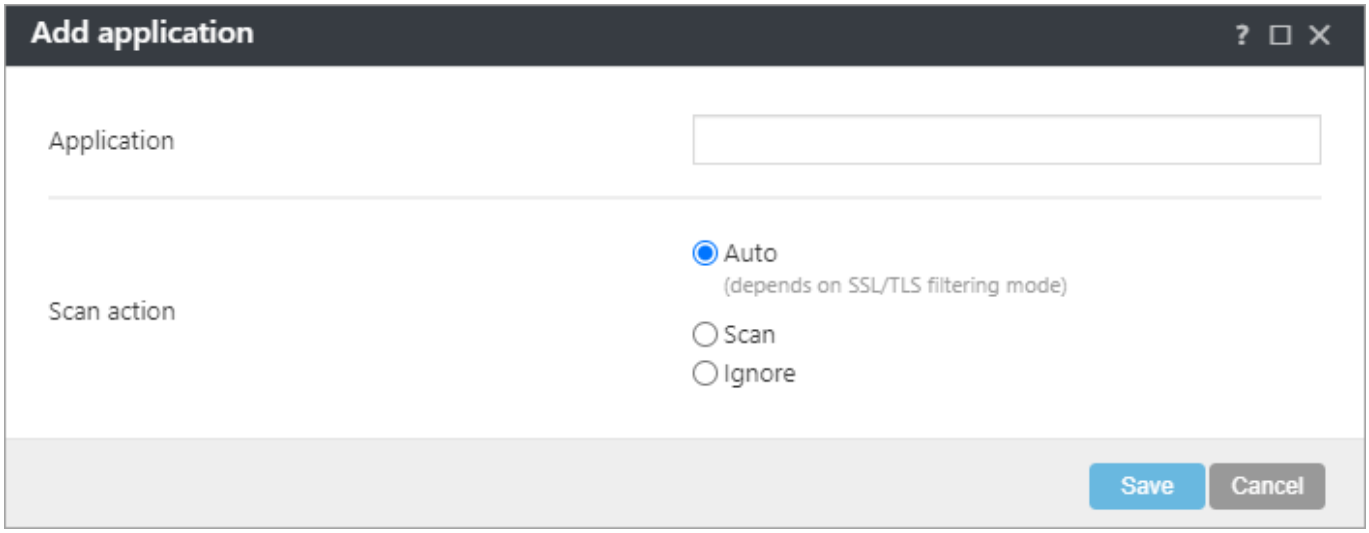
証明書の有効性

証明書の信頼を確立できない場合 – 場合によってはTrusted Root Certification Authorities (TRCA)ストアを使用してWebサイト証明書を検証できないことがあります。これは、証明書が他のユーザ(Webサーバーまたは中小企業の管理者)によって自己署名されていて、この証明書を信頼できるとみなしても必ずしもリスクにはならないことを意味します。多くの大企業(銀行など)はTRCAによって署名されている証明書を使用します。[**証明書の有効性を確認する**](既定で選択)が選択されていると、ユーザーは暗号化通信の確立時に取るアクションを選択するよう求められます。[**証明書を使用する通信をブロックする**]を選択すると、未検証の証明書を使用したサイトへの暗号化接続を常に終了できます。

SSL/TLSフィルタリングされたアプリケーションのリスト

SSL/TLSフィルタリングされたアプリケーションのリストを使用して、特定のアプリケーションのESET Endpoint Antivirus for Linux動作をカスタマイズできます。

追加をクリックして、特定のアプリケーションの動作をカスタマイズします。**アプリケーションの追加**ウィンドウには以下が表示されます。



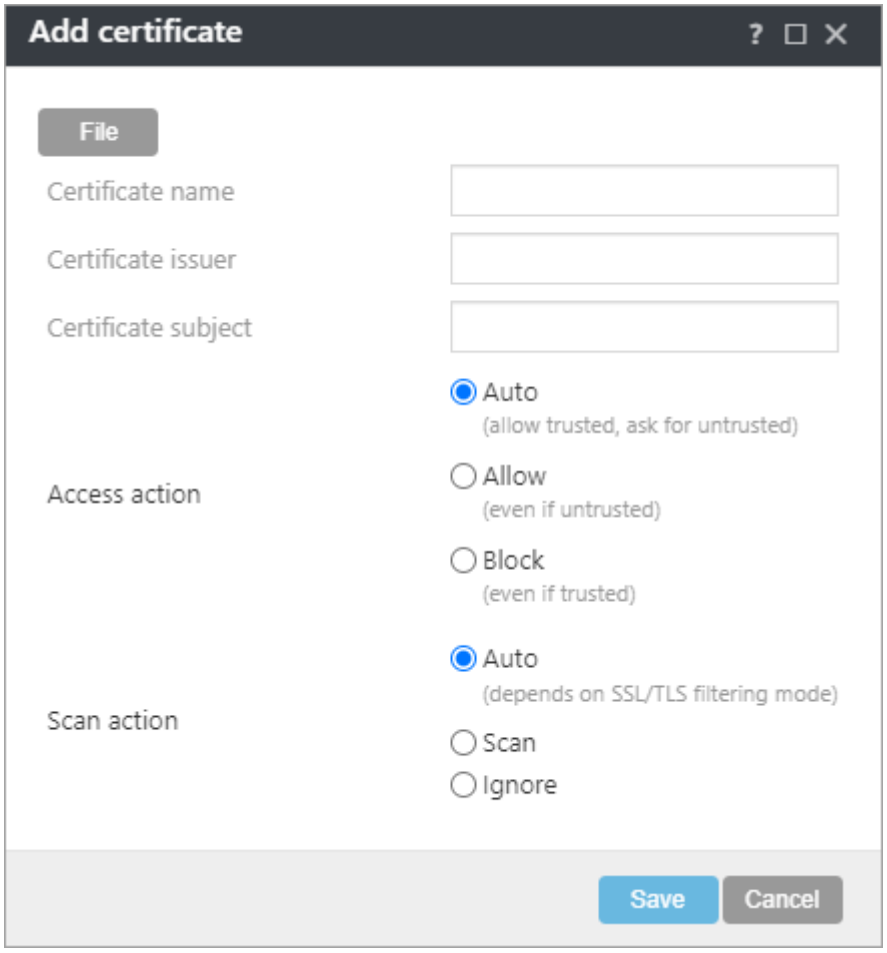
アプリケーション – アプリケーションへの正確なパスを入力します。

検査アクション

- **自動** – 自動モードで検査します。
- **検査または無視** – このアプリケーションによって保護された通信を検査/無視します。

既知の証明書のリスト

既知の証明書のリストを使用して、特定のSSL証明書のESET Endpoint Antivirus for Linux動作をカスタマイズできます。



証明書を追加ウィンドウで、**ファイル**をクリックして証明書ファイルを参照します。証明書のデータを使用して自動的に入力されるフィールド:

- **証明書名** – 証明書の名前。
- **証明書の発行者** – 証明書の作成者名。
- **証明書の件名** – 件名フィールドは、件名パブリックキーフィールドに保存されたパブリックキーに関連付けられたエンティティを指定します。

アクセスアクション

- **自動** – 信頼できる証明書を許可し、信頼できない証明書の場合はユーザーに確認します。
- **許可またはブロック**– 信頼性に関係なく、この証明書で保護された通信を許可またはブロックします。

検査アクション

- **自動** – 自動モードで検査します。
- **検査または無視** – この証明書によって保護された通信を検査/無視します。

検査アクションを**無視**に設定すると、アクセスアクションの**ブロック**が上書きされます。

ネットワークアクセス保護

バージョン10.2以降ESET Endpoint Antivirus for Linuxはボットネット保護をサポートしています。

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ているときに、一般的なパターンに基づいて、悪意のあるコマンドとコントロールサーバーとの通信を検出してブロックします。Webアクセス保護を有効にする必要があります。ボットネット保護の詳細については、ESET用語集を参照してください。

デバイスコントロール

ESET Endpoint Antivirus for Linuxは、自動デバイスコントロール(CD/DVD/USBなど)を備えています。このモジュールを使用すると、拡張フィルター/権限をブロック、または調整して、特定のデバイスにアクセスして操作するユーザーの機能を定義できます。この機能は、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コンピューター管理者にとって便利です。

ファイルシステムの破損の可能性
データの書き込み/読み取り中に、既に接続されているデバイスに対してブロック/読み取り専用アクションを実行するポリシーを適用すると、デバイスが強制的にマウント解除されるため、ファイルシステムが破損する可能性があります。

ポリシーの置換
複数のデバイスコントロールルールポリシーがESET Endpoint Antivirus for Linuxインスタンスに適用される場合、最後に適用されたポリシーは以前のポリシーのルールで置換されます。

サポートされている外部デバイス:

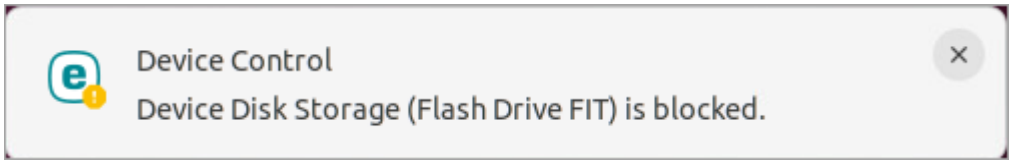
- USB経由で接続されたストレージデバイス
- 内蔵CD/DVDドライブ

デバイスコントロールは、ESET PROTECTのポリシーセクションでオンにして設定できます。

1. ESET PROTECTで、**ポリシー > 新しいポリシー**をクリックし、ポリシーの名前を入力します。
2. **設定**をクリックし、ドロップダウンメニューから**ESET Endpoint for Linux (V7+)**を選択します。
3. **保護 > デバイスコントロール**に移動します。
4. **システムに統合**の横のトグルをクリックします。
5. ルールとグループを設定するには、該当する項目の横の**編集**をクリックします。
6. **割り当て**に移動し、**割り当て**をクリックして、コンピューターの任意のグループを選択します。
7. **OK**をクリックしてから、**完了**をクリックします。

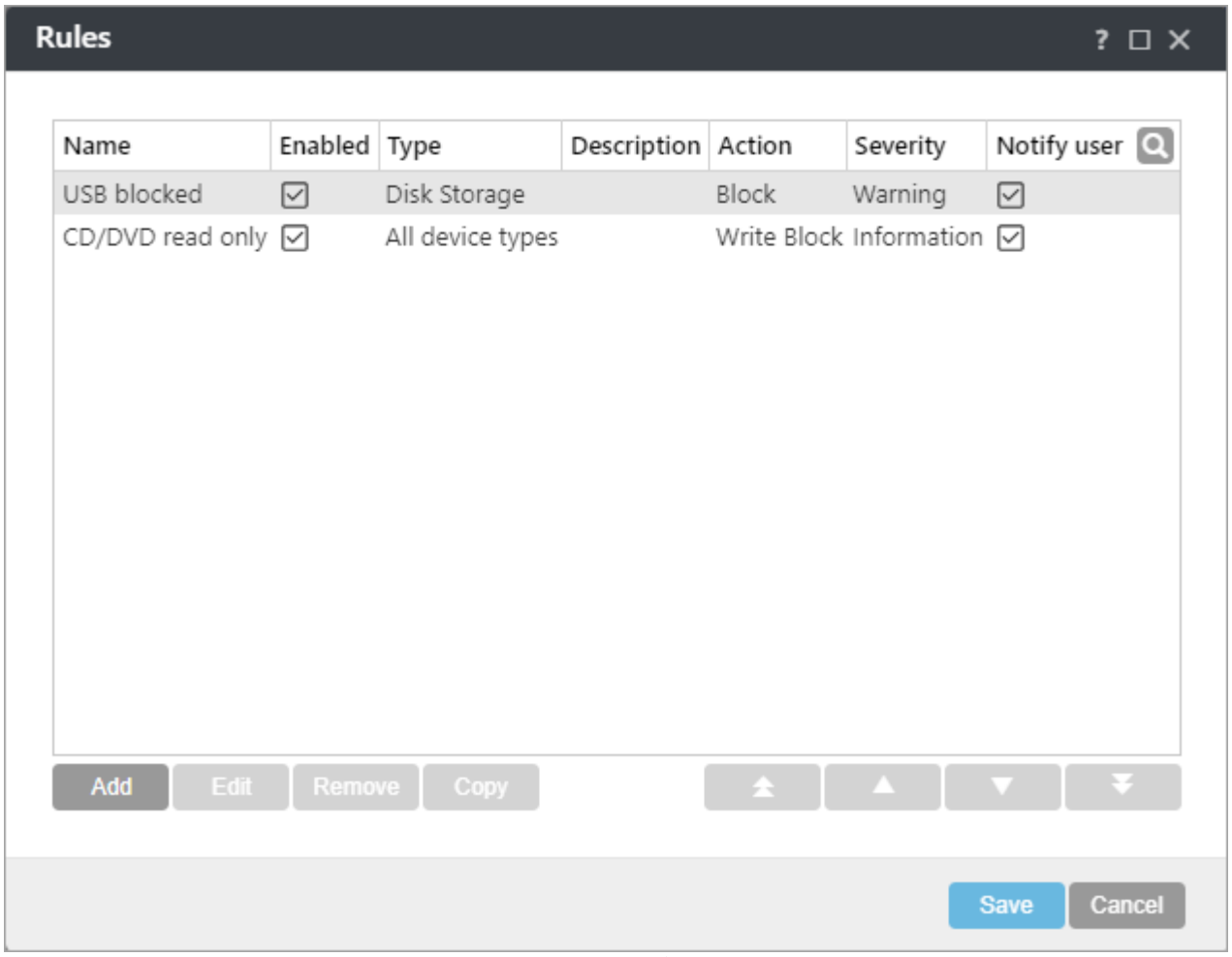
ESET PROTECTからのエンドポイントセキュリティ製品の管理に関する詳細を参照してください。

既存のルールでブロックされているデバイスが接続/挿入されると、通知ウィンドウが表示され、デバイスへのアクセス権は付与されません。



デバイスコントロールルールエディタ

ESET PROTECTの**デバイスコントロールルールエディター**ウィンドウには既存のルールが表示されます。このウィンドウを使用すると、ユーザーがコンピューターに接続するサポート対象の外付けデバイスを細かくコントロールすることができます。



ルール設定で定義されたパラメーターに基づいて、特定のデバイスを許可またはブロックできます。ルール一覧には、外部デバイスの名前と種類、コンピューターに外部デバイスを接続した後に実行するアクションといった、さまざまなルール説明が含まれています。

[**追加**]または[**編集**]をクリックしてルールを管理します。ルールの横の**有効**チェックボックスをオフにすると、今後使用するときまで無効になります。1つ以上のルールを選択し、[**削除**]をクリックすると、ルールが完全に削除されます。

選択したルールのコピーを作成するには、**コピー**をクリックします。

ルールは優先度順に一覧表示されます。ルールを個別に移動したり、グループで移動したりするには、最上位/上へ/下へ/最下位ボタンをクリックします。

デバイスコントロールログは、デバイスコントロールがトリガーされるすべての状況を記録します。

接続されたデバイスの属性

ESET Endpoint Antivirus for Linuxがインストールされているコンピューターに接続しているデバイスの属性のリストを出力するには、ターミナルウィンドウで`lsdev`ユーティリティを使用するか、ESET PROTECTからこのコマンドを実行します。

Syntax: `/opt/eset/eea/bin/lsdev[オプション]`

オプション – 短縮型	オプション – 標準型	説明
`-l`	`--list`	接続されたデバイスのリストを表示します
`-c`	`--csv`	CSV形式を使用して、接続されたデバイスのリストを表示します
`-h`	`--help`	ヘルプの表示と終了を実行します
`-v`	`--version`	バージョン情報を表示して終了します

デバイスグループ

デバイスグループウィンドウは、2つの部分に分かれます。ウィンドウの右側には、該当するグループに属するデバイスのリストが表示されます。ウィンドウの左側には、作成されたグループが表示されます。右側のペインに表示するデバイスのリストを含むグループを選択します。

デバイスグループウィンドウを開いて、グループを選択すると、リストからデバイスを追加または削除できます。グループにデバイスを追加する別の方法は、ファイルからインポートすることです。

コントロール要素

追加 – 名前またはデバイスを既存のグループに入力して、グループを追加できます(任意で、ベンダー名、モデル、シリアル番号などの詳細を指定できます)。

編集 – 選択したグループまたはデバイスのパラメータ(ベンダー、モデル、シリアル番号)の名前を変更します。

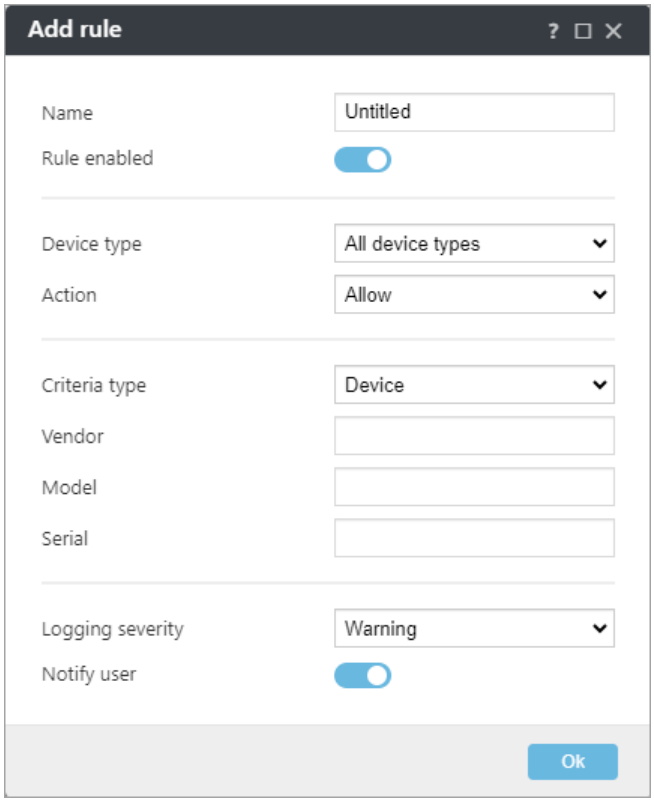
削除 –選択したグループまたはデバイスを削除します。

インポート –ファイルからデバイスのリストをインポートします。

カスタマイズが完了したら、**[OK]**をクリックします。変更を保存せずに[**デバイスグループ**]を終了する場合は、[**編集**]をクリックします。

デバイスコントロールルールの追加

デバイスコントロールルールでは、ルール基準に適合するデバイスがコンピューターに接続されたときに実行されるアクションを定義します。



識別しやすいように、ルールの説明を**名前**フィールドに入力します。これは、ルールを永続的に削除したくない場合に便利です。

デバイスのタイプ

ドロップダウンメニューから外部デバイスタイプを選択します。

- **ディスクストレージ** - USB経由で接続されたすべてのディスクストレージに適用されます(外部CD/DVDドライブと従来のメモリカードリーダーを含む)。
- **CD/DVD** – IDEまたはSATA経由で接続された内蔵のCD/DVDドライブに適用されます。
- **すべてのデバイスタイプ** – 上記のすべてのタイプが含まれます

デバイスタイプ情報は、オペレーティングシステムから収集されます。lsdevユーティリティを使用して、接続されているデバイスとその属性を一覧表示します。

これらのデバイスはアクションに関する情報のみを提供し、ユーザーに関する情報は提供しないため、グローバルにのみブロックできます。

アクション

記憶装置以外へのアクセスは、許可またはブロックすることができます。それに対して、記憶装置のルールについては、次のいずれかの権限設定を選択できます。

- **許可** – デバイスへのフルアクセス
- **ブロック** –デバイスへのアクセスはブロックされます
- **書き込みブロック** – デバイスへの読み取りアクセスのみ

条件タイプで、**デバイス**または**デバイスグループ**を選択します。

追加パラメータは、ルールを微調整したりデバイスに合わせて変更するのに使用できます。いずれのパラメーターでも大文字と小文字は区別されません。

- **ベンダー** – ベンダー名またはIDによるフィルタリング。
- **モデル** – デバイスに付けられている名前。
- **シリアル** – 外部デバイスには通常独自のシリアル番号が付いています。CD/DVDの場合は、CDドライブではなく、そのメディアのシリアル番号があります。

> **未定義のパラメーター**
> これらのパラメーターが未定義の場合、ルールは照合時にこれらのフィールドを無視します。すべてのテキストフィールドのフィルタリングパラメーターは大文字と小文字が区別されず、ワイルドカード(*、?)はサポートされていません。

> **デバイスコントロールログ**
> デバイス情報を表示するには、デバイスのタイプのルールを作成し、デバイスをコンピューターに接続してから、lslogコマンドラインユーティリティで`-l`または`--device-control`パラメーターを使用して、デバイス詳細を確認します。

ログ記録の重大度

- **情報** – 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を記録します。
- **警告** – 重大なエラー、エラー、および警告メッセージを記録し、ESET PROTECTに送信します。

ツール

ツールセクションでESET Endpoint Antivirus for Linux設定を変更するには、ESET PROTECTまたはESET PROTECT On-Premを使用します。

- インターネットに接続するためのプロキシサーバーの詳細を定義する
- ログファイルの処理方法を設定する

プロキシサーバ

プロキシサーバーを使用して、インターネットまたは定義されたアップデートサーバー(ミラー)に接続するようにESET Endpoint Antivirus for Linuxを設定します。**設定 > ツール > プロキシサーバー**セクションでプロキシサーバーパラメーターを調整するには、ESET PROTECTまたはESET PROTECT On-Premを使用します。

ログファイル

ESET Endpoint Antivirus for Linuxログの設定を修正します。

最低ロギング詳細レベル

ロギング詳細レベルは、ログファイルに記録されるESET Endpoint Antivirus for Linuxに関する情報の詳細レベルを定義します。

- **重大な警告** – 重大なエラーのみが含まれます(ウイルス対策の起動に失敗したなど)。
- **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。

次の日数が経過したエントリを自動的に削除する

指定した日数を経過したログエントリをログリスト(`lslog`)で非表示にするには。

1. ESET PROTECTで、**ポリシー > 新しいポリシー**をクリックし、ポリシーの名前を入力します。
2. **設定**をクリックし、ドロップダウンメニューから**ESET Endpoint for Linux (V7+)**を選択します。
3. **ツール > ログファイル**をクリックします。
4. **次の日数が経過したエントリを自動的に削除する**を有効にします。
5. 非表示にするファイルの有効日数を調整します。
6. **設定 > 割り当て**をクリックします。ポリシーが適用されるコンピューターの任意のグループを選択します。
7. **OK**をクリックしてから、**完了**をクリックします。

非表示のログは再表示できません。オンデマンド検査のログエントリはすぐに削除されます。非表示のログの蓄積を防止するには、ログファイルの自動最適化をオンにします。

ログファイルを自動的に最適化する

有効にすると、断片化の割合が**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**フィールドの値を超えた場合に、ログファイルは自動的にデフラグされます。未使用レコードは非表示のログを表します。[**最適化**]をクリックすると、ログファイルの最適化が開始します。すべての空のログエントリが削除され、パフォーマンスとログ処理速度が改善します。この向上は、特にログに多数のエントリが含まれている場合に顕著に見られます。

Syslog機能

Syslog機能はSyslogログパラメーターであり、類似したログメッセージをグループ化するために使用されます。たとえば、デーモンのログ(Syslog機能daemon経由でログを収集)が設定されている場合は、*/var/log/daemon.log*に記録できます。最近のsystemdおよびjournalへの切り替えにより、Syslogは以前

ほど重要ではなくなりましたが、ログのフィルタリングで使用できます。

ユーザーインタフェース

ESET PROTECTのESET Endpoint Antivirus for Linux設定のこのセクションでは、デスクトップ通知を有効/無効にし、通知するアクションとアプリケーションステータスを選択できます。

デスクトップ通知

デスクトップに通知を表示の横のトグルをオン/オフに切り替えると、デスクトップに通知をオン/オフにすることができます。これらは既定で有効です。これらの通知には、ユーザー操作が必要ではない情報が含まれます。

通知されるアクションを設定します。

1. **アプリケーション通知**の横の**編集**をクリックします。
2. 任意のアクションを選択/選択解除します。
3. **OK**をクリックします。

現在の状況

ESET Endpoint Antivirus for Linuxに報告されるアプリケーションステータスを設定します。

1. アプリケーションステータスの横の**編集**をクリックします。
2. **エンドポイントに表示**の下で、通知される任意のアプリケーションステータスを選択します。
3. **OK**をクリックします。

アプリケーションステータス

アプリケーションステータス > 編集 > エンドポイントに表示で選択された各ステータスにはESET Endpoint Antivirus for Linuxの初期画面とメニュー > **保護の状態**に通知が表示されます。

トラブルシューティング

このセクションでは、以下のさまざまな問題に対するトラブルシューティング方法を説明します。

- アクティベーションの問題(英語のみ)
- ログの収集
- noexecフラグの使用
- リアルタイム保護を開始できない
- NFSマウントが失敗する
- WireGuardとWebアクセス保護の使用

- Webアクセス保護を使用しないインストール

ログの収集

ESETテクニカルサポートがESET Endpoint Antivirus for Linuxのログを要求する場合は、*collect_logs.sh*にある*/opt/eset/eea/sbin/*スクリプトを使用して、ログを生成します。

ルート権限で、ターミナルウィンドウからスクリプトを起動します。たとえばUbuntuの場合は、次のコマンドを実行します:

```
sudo /opt/eset/eea/sbin/collect_logs.sh
```

このスクリプトは、必要なすべてのログをアーカイブファイルとしてログインユーザーのホームフォルダーに生成し、パスを表示します。該当する場合は、アクティベーションログも収集します。そのファイルを電子メールでESETテクニカルサポートに送信してください。

アクティベーションログ

製品のアクティベーションに関する問題のトラブルシューティングをサポートするためにESETテクニカルサポートは関連ログをリクエストする場合があります。

1. 次のコマンドを特権ユーザーとして実行して、アクティベーションログサービスを有効にします。

```
sudo /opt/eset/eea/sbin/ecp_logging.sh -e
```

または

```
sudo /opt/eset/eea/sbin/ecp_logging.sh -e -f
```

必要な場合は、確認メッセージを表示せずに、製品を再起動します。

2. アクティベーションプロセスを再試行します。失敗した場合は、特権ユーザーとしてログ収集スクリプトを実行します。

```
sudo /opt/eset/eea/sbin/collect_logs.sh
```

3. 収集したログをESETテクニカルサポートに送信します。

4. 次のコマンドを特権ユーザーとして実行して、アクティベーションログを無効にします。

```
sudo /opt/eset/eea/sbin/ecp_logging.sh -d
```

または

```
sudo /opt/eset/eea/sbin/ecp_logging.sh -d -f
```

必要な場合は、確認メッセージを表示せずに、製品を再起動します。

インストールログ

製品インストールの問題のトラブルシューティングを行うにはESETテクニカルサポートから関連するログおよび情報の送信を求められる場合があります。

1. 実行中のインストーラーのターミナルから出力すべてをコピーします。

2.オペレーティングシステムのバージョンと配布に関する正確な情報をコピーするには、特権ユーザーで、ターミナルウィンドウから次のコマンドを実行します。

```
lsb_release -a
```

または

```
hostnamectl
```

3. カーネルに関する正確な情報をコピーするには、特権ユーザーで、ターミナルウィンドウから次のコマンドを実行します。

```
dmesg | grep Linux
```

または

```
yum list kernel-*
```

4. ハードウェアに関する正確な情報をコピーするには、特権ユーザーで、ターミナルウィンドウから次のコマンドを実行します。

```
lshw
```

5. info_get.commandを使用してログファイルを収集します。

noexecフラグの使用

`noexec`フラグを使用して`/var` と `/tmp`をマウントした場合ESET Endpoint Antivirus for Linuxのインストールが次のエラーメッセージで失敗します。

```
Invalid value of environment variable MODMAPDIR. Modules cannot be loaded.
```

回避策

以下のコマンドはターミナルウィンドウで実行されます。

1. 次の所有者と権限セットを使用して、`exec`が有効なフォルダーを作成します。

```
/usr/lib/eea drwxrwxr-x. root eset-eea-daemons
```

2. 次のコマンドを実行します。

```
# mkdir /usr/lib/eea
# chgrp eset-eea-daemons /usr/lib/eea
# chmod g+w /usr/lib/eea/
```

a.SELinuxが有効な場合、このフォルダーのコンテキストを設定します。

```
# semanage fcontext -a -t tmp_t /usr/lib/eea
# restorecon -v /usr/lib/eea
```

3. 基本モジュールをコンパイルする。

```
# MODMAPDIR=/usr/lib/eea /opt/eset/eea/bin/upd --compile-nups
```

4. `[Service]`ブロックに行を追加して、`/usr/lib/systemd/system/eea.service`で`MODMAPDIR`を設定する:

```
Environment=MODMAPDIR=/usr/lib/eea
```

5. systemdサービス設定を再読み込みする。

```
# systemctl daemon-reload
```

6. eeaサービスを再起動する。

```
# systemctl restart eea
```

リアルタイム保護を開始できない

問題のサンプルがあります。以下の解決策は、Ubuntuで行われています。

問題

カーネルファイルが見つからないため、リアルタイムファイルシステム保護を開始できない。

*/var/log/messages*で、ESET Endpoint Antivirus for Linuxに関するエラーが表示されます。

Oct 15 15:42:30 localhost eea: ESET Endpoint Antivirus error: cannot find kernel sources directory for kernel

version 3.10.0-957.el7.x86_64

Oct 15 15:42:30 localhost eea: ESET Endpoint Antivirus error: please check if kernel-devel (or linux-headers) package version matches the current kernel version

Oct 15 15:42:30 localhost oaeventd[31471]: ESET Endpoint Antivirus Error: Cannot open file /lib/modules/3.10.0-957.el7.x86_64/eset/eea/eset_rtp.ko: No such file or directory

解決策

方法1 – オペレーティングシステムの再起動が必要です

1. オペレーティングシステムのパッケージを最新バージョンにアップグレードします。Ubuntuでは、特権ユーザーで、ターミナルウィンドウから次のコマンドを実行します。

```
apt-get update

apt-get upgrade
```

2. オペレーティングシステムを再起動します。

方法2

1. DEBベースのLinuxディストリビューションに最新のカーネルヘッダーをインストールします。Ubuntuでは、特権ユーザーで、ターミナルウィンドウから次のコマンドを実行します。

```
apt update

apt install linux-headers-$(uname -r)
```

2. EEAサービスを再起動する。

```
systemctl restart eea
```

NFSマウントが失敗する

問題

Webアクセス保護を支えるテクノロジーは、NFSマウントへの接続を切断します。NFSサーバーの既定の設定では、クライアントが1025未満のポート(ルートへアクセス可能)から接続することを想定しています。Webアクセスによって傍受された接続は、1024を超えるランダムなポートから接続を試行し、その結果、サーバーは拒否されます。

回避策

拒否されないようにするには、NFSマウントサーバーの設定をinsecureに変更します。これにより、クライアントはランダムなポートからサーバーに接続できます。

1.NFSサーバーマシンで、特権ユーザーとしてテキストエディターで*/etc/exports*ファイルを開きます。この例では、nanoを使用します。

```
nano /etc/exports
```

2. 共有ディレクトリをinsecureに設定し、変更を保存します。NFS共有ディレクトリの例:

```
/srv/nfs-share  10.10.10.10/24(rw,sync,no_subtree_check,no_root_squash,insecure)
```

3. NFSサーバーを再起動します。次のコマンドを特権ユーザーで実行します。

```
systemctl restart nfs-kernel-server
```

WireGuardとWebアクセス保護の使用

問題

コマンドラインから、またはサービスとしてwg-quickを使用して、Webアクセス保護(WAP)とWireGuardを組み合わせているとします。その場合、WAPとWireGuardインターフェイスの両方が有効になっていると、インターネット接続が失われる可能性があります。これは、インターフェイスが起動したときにwg-quickによってnftablesに追加されるルールが原因です。インターフェイスがwg0で、IPアドレスが10. 10. 10. 2であるとします。ルールはテーブル*wg-quick-wg0*、chain prerawに追加され、次のようになります。

```
iifname != "wg0" ip daddr 10.10.10.2 fib saddr type != local drop
```

このルールの目的は、設定の問題や悪意のあるパケットから守ることです。

回避策

適切に設定された、安全なシステムでは、nftablesルールは必要ありません。そのルールをそのまま残さないようにwg-quickを設定すると、接続の問題が修正されます。たとえば、影響を受けるインターフェイスの設定ファイルを編集し、[インターフェイス]セクションで次のPostUpアクションを追加できます。

```
PostUp = nft flush chain wg-quick-wg0 preraw
```

wg-quick-wg0名前は*"wg0"*インターフェイスにのみ適用され、他のインターフェイスに応じて変更する必要があることに注意してください。それでもある程度の保護が必要な場合は、たとえば次のように、ルールをより弱いルールに置き換えます。

```
PostUp = nft flush chain wg-quick-wg0 preraw; nft 'add rule wg-quick-
wg0 preraw iifname != "wg0" iif != "lo" ip daddr 10.10.10.2 fib saddr type != local
drop'
```

インターフェイスが「wg0」でない場合は、「wg0」に言及しているすべての箇所を更新する必要があることを忘れないでください。また「IP」アドレスが10.10.10.2でない場合は更新する必要があります。

Webアクセス保護を使用しないインストール

Webアクセス保護機能またはその依存関係で問題が発生している場合は、環境変数ESET_DISABLE_WAP=1を使用して、この機能を使用せずに製品をインストールできます。

解決策

Webアクセス保護を使用しないで製品をインストールするには、現在のユーザー権限に応じて以下の手順に従います。

特権ユーザーの場合

特権ユーザーで、ターミナルウィンドウから次のコマンドを実行します。

```
ESET_DISABLE_WAP=1 sudo -E ./eeau_x86_64.bin
```

Rootユーザーの場合

rootユーザーで、ターミナルウィンドウから次のコマンドを実行します。

```
ESET_DISABLE_WAP=1 ./eeau_x86_64.bin
```

- Webアクセス保護を使用しないインストールは永続的なもので、環境変数ESET_DISABLE_WAP=1を使用しないアップグレードでは有効化されず、必要なWebアクセス保護の依存関係のみがインストールされます。
- 製品のアップグレードは、必ず環境変数ESET_DISABLE_WAP=1を使用して行う必要があります。
- Webアクセス保護を使用している製品には、クリーンインストールが必要です。

アンインストール

ESET製品をアンインストールするには、ターミナルウィンドウをスーパーユーザーで起動して「Linux」ディストリビューションに対応するパッケージを削除するコマンドを実行します。

Ubuntu/Debianベースのディストリビューション：

```
apt remove eea
```

```
dpkg --remove eea
```

Red Hatベースのディストリビューション：

```
yum remove eea
```

```
dnf remove eea
```

```
rpm -e eea
```

用語集

- **デーモン**:Unixなどのオペレーティングシステムのプログラムの一種で、バックグラウンドで邪魔にならないように実行されます。これは、特定のイベントまたは条件の発生によってアクティベーションされます。

- ESET用語集のその他の用語を参照。

法的文書

以下は、法的文書一式です。

- エンドユーザーライセンス契約

- プライバシーポリシー

エンドユーザーライセンス契約

発効日：2021年10月19日

重要:ダウンロード、インストール、コピー、または使用の前に、製品利用に関する下記契約条件を注意してお読みください。**本製品をダウンロード、インストール、コピー、または使用することにより、お客様はこれらの条件に対する同意を表明し、**プライバシーポリシー**に同意したことになります。**

エンドユーザー使用許諾契約

本エンドユーザーライセンス契約（「本契約」）は、Einsteinova 24, 85101 Bratislava, Slovak Republicに所在し、ブラチスラバ第1地方裁判所の有限会社部門District Court Bratislava I. Section Sroにおいて掲載番号3586/B, 31333532として商業登記されているESET, spol. s r. o. (ESETまたは「供給者」)と、自然人または法人であるお客様(「お客様」または「エンドユーザー」)との間で締結され、お客様に本契約の第1条で定義する本ソフトウェアを使用する権利を付与するものです。本契約の第1条で定義する本ソフトウェアは、データ記憶媒体への格納、電子メールでの送付、インターネットからのダウンロード、供給者のサーバーからのダウンロード、または後述の条件および状況下におけるその他の供給者からの取得が行えます。

本契約は購入に関する契約ではなく、エンドユーザーの権利に関する合意事項を定めるものです。供給者は、本ソフトウェアのコピー、これが商業包装にて供給される物理的媒体、および本契約に基づきエンドユーザーが権利を付与される本ソフトウェアのすべてのコピーの、所有者であり続けます。

本ソフトウェアのインストール時、ダウンロード時、コピー時または使用時に、[同意します]オプションをクリックすることにより、本契約の条件に明示的に同意し、プライバシーポリシーを承諾するものとします。本契約の規定またはプライバシーポリシーに同意しない場合は、直ちに[同意しない]オプションをクリックし、インストールまたはダウンロードを取り消すか、本ソフトウェア、インストールメディア、付属ドキュメント、および購入時の領収書を破棄するかESETまたは本ソフトウェアの供給者にそれを返却してください。

お客様は、本ソフトウェアを使用することにより、お客様が本契約を読了かつ理解し、本契約条項による拘束に同意したことになります。

1.**ソフトウェア。**(i)本契約およびすべてのコンポーネントに付属するコンピュータープログラム(ii)デー

タ媒体、電子メール、またはインターネット経由でのダウンロードで提供される本ソフトウェアのオブジェクトコードの形式を含む、本契約で提供されるディスク(CD-ROM、DVD、電子メール、添付ファイル、その他の媒体のすべての内容、(iii)本ソフトウェアに関連する書面の説明資料、その他の文書、特に本ソフトウェア、その仕様のすべての説明、 本ソフトウェアの属性または動作の説明、本ソフトウェアが使用される動作環境の説明、本ソフトウェアの使用またはインストール手順、本ソフトウェアの使用方法の説明(「ドキュメント」、(iv)本契約の第3条に従い供給者からお客様にライセンス供与された本ソフトウェアのコピー、本ソフトウェアに不具合があった場合のパッチ、本ソフトウェアへの追加機能、本ソフトウェアの拡張機能、本ソフトウェアの修正バージョン、ソフトウェアコンポーネントのアップデート(該当する場合)を意味します。本ソフトウェアは実行可能なオブジェクトコードの形態でのみ提供されるものとします。

2.**インストール、コンピューター、およびライセンスキー**。データキャリアで供給、電子メールで送信、インターネットからダウンロード、供給者のサーバーからダウンロード、または他のソースから取得されたソフトウェアにはインストールが必要です。お客様は、本ソフトウェアを正しく設定されたコンピューターにインストールし、少なくともドキュメントで規定された要件に準拠する必要があります。インストール方法はドキュメントで説明されています。本ソフトウェアをインストールするコンピューターに、本ソフトウェアに悪影響を及ぼす可能性があるコンピュータープログラムやハードウェアをインストールすることはできません。コンピューターとは、本ソフトウェアがインストールまたは使用される、パーソナルコンピューター、ノートブック、ワークステーション、パームトップコンピューター、スマートフォン、ハンドヘルド電子機器、または本ソフトウェアの対象として設計されている他の電子機器を含む(ただしこれらに限定されない)を意味します。ライセンスキーとは、本契約に準拠して、本ソフトウェア、特定のバージョン、またはライセンス条項の拡張の法的な使用を許可するために、エンドユーザーに提供される一意の連続する記号、文字、数字、または特殊記号を意味します。

3.**ライセンス**。お客様が本契約に同意しており、ライセンス料を支払い期日までに支払い、本契約に定められているすべての契約条項に従うことを前提として、供給者はお客様に対し、以下の権利を付与します（以下「ライセンス」とします）。

a) **インストールおよび使用。**お客様には、コンピューターのハードディスクまたはその他のデータ永久記憶媒体にデータを格納するために本ソフトウェアをインストールし、コンピューターシステムのメモリへ本ソフトウェアをインストールおよび格納し、コンピューターシステム上で本ソフトウェアを実装、格納および表示する、非独占的かつ譲渡禁止の権利が付与されます。

b) **ライセンス数の規定。**本ソフトウェアを使用する権利は、エンドユーザー数によって制限されます。1人のエンドユーザーとは、(i) 本ソフトウェアがインストールされている1台のコンピューターを意味します、(ii)ライセンス数がメールボックスを単位として決定される場合、エンドユーザーはメールユーザーエージェント（以下、MUAとします）を介して電子メールを受信する1人のコンピューターユーザーを意味します。電子メールがMUAで受信後、複数のユーザーに自動的に配信される場合、エンドユーザーの数は、その電子メールが配信されるユーザーの実際の数によって決まります。メールサーバがメールゲートの役割を果たす場合、エンドユーザーの数は、そのゲートがサービスを提供するメールサーバユーザーの数と同じになります。(エイリアスなどを使用して)1人のユーザーに不特定多数の電子メールアドレスが送信され、それらが受け付けられる場合、クライアント側で多数のユーザーにそのメールが自動的に配信されるのでなければ、ライセンスは1台のコンピューターに必要です。同じライセンスは、同時に複数のコンピューターで使用できません。エンドユーザーは、供給者によって付与されたライセンス数に基づく制限に従い、本ソフトウェアを使用する権限が与えられている範囲においてのみ、本ソフトウェアのライセンスキーを入力する資格があります。このライセンスキーは機密情報であると見なされます。本契約または供給者によって許可されている場合を除き、お客様はライセンスを第三者と共有すること、または第三者がライセンスを使用することを許可することが禁止されています。ライセンスキーが危険にさらされた場合は、速やかに供給者に通知してください。

c) **Home/Business Edition**、本ソフトウェアのHome Editionバージョンは、家庭および家族での利用に限定された個人または非商業環境でのみ使用されるものとします。本ソフトウェアを商業環境、またはメールサーバー、メール中継、メールゲートウェイ、インターネットゲートウェイで使用する場合は、本ソフトウェアのBusiness Editionバージョンを入手する必要があります。

d) **ライセンス契約の期間。**お客様は、本ソフトウェアを期限付きで使用する権利があります。

e) **OEMソフトウェア。**OEMに分類されたソフトウェアの使用は、それがプリインストールされていたコンピューターに制限されます。別のコンピューターにインストールすることはできません。

f) **NFRまたは試用ソフトウェア。**再販不可品（NFR）または試用版に分類されるソフトウェアは、対価を求めて譲渡することはできず、ソフトウェア機能のデモまたはテスト目的のみで使用されるものとします。

g) **ライセンスの契約解除。**ライセンス契約は，その期間の満了により契約が自動的に解除されます。供給者は、お客様が本契約のいずれかの条項に違反したときは、供給者が持つ他の権利および法的救済手段に影響を与えることなく、本契約を解約することができます。本ライセンスを取り消す場合、お客様は、本ソフトウェアおよびバックアップコピーを直ちにすべて削除、破棄するか、自費でESETまたはソフトウェアの入手元にそれを返却する必要があります。ライセンスの終了時には、供給者は、エンドユーザーが、供給者のサーバーまたはサードパーティのサーバーに接続する必要がある本ソフトウェアの機能を使用する権利を取り消す権利があるものとします。

4.**データ収集機能およびインターネット接続要件。**本ソフトウェアの正常な動作には、インターネット接続が必要であり、プライバシーポリシーに従い、定期的に供給者のサーバーまたは第三者のサーバーおよび該当するデータ収集に定期的に接続する必要があります。インターネットへの接続およびデータ収集は、次のソフトウェア機能で必要です。

a) **ソフトウェアのアップデート。**供給者には、本ソフトウェアのアップデートまたはアップグレード（「アップデート」）を適時発行する権利がありますが、アップデートを提供する義務はありません。この機能は、ソフトウェアの標準の設定から有効にできます。エンドユーザーがアップデートの自動インストールを無効にしていないかぎり、アップデートは自動的にインストールされます。アップデートを提供するために、プライバシーポリシーに準拠し、本ソフトウェアがインストールされているコンピューターまたはプラットフォームに関する情報を含む、ライセンスの正当性を検証する必要があります。

アップデートの提供には、サービス終了ポリシー（「EOLポリシー」）が適用される場合があります。https://go.eset.com/eol_businessをご覧ください。本ソフトウェアまたは本ソフトウェアの機能がEOLポリシーで定義されているサービス終了日に達した後は、アップデートが提供されません。

b) **供給者への侵入物および情報の転送**。本ソフトウェアには、コンピューターウイルスおよびその他の悪意のあるプログラム、ファイル、URL、IPパケット、イーサネットフレームなどの不審、問題、潜在的に望ましくない、または潜在的に危険なオブジェクト（「侵入」）のサンプルを収集する機能が含まれ、インストール処理、コンピューター、ソフトウェアがインストールされているプラットフォームの情報、本ソフトウェアの操作および機能の情報（「情報」）を含む（ただしこれらに限定されない）、これらのオブジェクトを供給者に送信します。情報および侵入には、エンドユーザーまたは本ソフトウェアがインストールされているコンピューターの他のユーザーのデータ（ランダムまたは誤って取得された個人データを含む）、関連付けられたメタデータによる侵入の影響を受けるファイルが含まれる場合があります。

情報および侵入は次のソフトウェア機能によって収集される場合があります。

i.LiveGridレピュテーションシステム機能には、侵入に関する単方向ハッシュの収集と供給者への送信が含まれます。この機能は、ソフトウェアの標準設定で有効です。

ii.LiveGridフィードバックシステム機能には、侵入を収集し、関連付けられたメタデータおよび情報とともに供給者に送信する機能が含まれます。この機能は、本ソフトウェアのインストール処理中に、エンドユーザーがアクティブ化することができます。

供給者は、侵入の分析と研究、ソフトウェアの改良、およびライセンスの正当性の検証の目的でのみ、受け取った情報および侵入を使用するものとし、適切な対策を講じて、受け取った侵入および情報が安全であることを保証するものとします。本機能をアクティブ化することで、プライバシーポリシーの規定に従い、関連する法規制に準拠して、侵入および情報は供給者によって収集および処理される場合が

あります。この機能はいつでも無効にすることができます。

本契約の目的のために、プライバシーポリシーに従い、供給者がお客様を特定できるようにするデータを収集、処理、および保存する必要があります。お客様は、供給者が独自の手段によって、お客様が本契約の規定に従って本ソフトウェアを使用しているかどうかを確認することに同意します。お客様は、本契約の目的でのみ、本ソフトウェアと供給者のコンピューターシステムまたは供給者の販売およびサポートネットワークの一部としての供給者のビジネスパートナーのコンピューターシステムとの間の通信中に、お客様のデータを転送し、本ソフトウェアの機能および本ソフトウェアの使用許可を保証し、供給者の権利を守る必要があることを承諾します。

本契約の締結後、供給者および供給者の販売およびサポートネットワークの一部としての供給者のビジネスパートナーは、請求目的、本契約の履行、およびお客様のコンピューターでの通知の送信のために、お客様を特定できる基本データを転送、処理、および保管する権利を有するものとします。

データ主体としてのプライバシー、個人データ保護、およびお客様の権利の詳細については、供給者のWebサイトまたはインストール処理で直接アクセスできるプライバシーポリシーを参照してください。お客様は、ソフトウェアのヘルプセクションからアクセスすることもできます。

5.**エンドユーザの権利行使**。お客様は、エンドユーザーの権利を、直接またはお客様の従業員を通じて行使する必要があります。お客様は、自らの活動を確実なものとするためにのみ、およびお客様がライセンスを取得したコンピューターシステムを保護するためにのみ、本ソフトウェアを使用できます。

6.**権利の制限。**お客様は本ソフトウェアのコピー、配布、部品の分離、または派生バージョンの作成を行ってはなりません。本ソフトウェアの使用時には、下記の制限事項に従う必要があります。

a) お客様は、データの永久記憶用媒体上に本ソフトウェアのコピーを1つ、バックアップコピーとして作成できます。ただし、この保管用のバックアップコピーは、他のいかなるコンピュータにもインストールしたり、または使用したりすることができません。これ以外に本ソフトウェアのコピーを作成することは、本契約に対する違反となります。

b) 本契約に規定されている以外のいかなる態様でも、本ソフトウェアまたは本ソフトウェアのコピーの使用、改変、複製、または使用権の譲渡を行ってはなりません。

c) 本ソフトウェアの売却、サブライセンス付与、他人への賃貸もしくは他人からの賃借、借用、または商業サービスの提供目的での本ソフトウェアの使用は禁じられています。

d) 本ソフトウェアのリバースエンジニアリング、逆コンパイル、またはソフトウェアの逆アセンブルを行ったり、ソースコードを取得しようとしたりしてはなりません。ただし、そのような制限を設けることが法律によって明示的に禁止されている範囲内においては、この限りではありません。

e) お客様は、著作権法およびその他の知的財産権から生じる、適用可能な制限など、本ソフトウェアを使用する際の法律におけるすべての適用可能な法的規制に従う態様においてのみ、本ソフトウェアを使用できます。

f) お客様は、本ソフトウェアおよびその機能を、他のエンドユーザーがそれらのサービスにアクセスする可能性を制限しない方法でのみ使用することに同意するものとします。供給者は、可能な限り多くのエンドユーザーがサービスを利用できるようにするために、個別のエンドユーザーに提供されるサービスの範囲を制限する権利を留保します。サービスの範囲を制限することにより、本ソフトウェアのすべての機能を使用することもできなくなり、本ソフトウェアの特定の機能に関連する供給者のサーバー上またはサードパーティのサーバー上のデータおよび情報も削除されることとします。

g) お客様は、本契約の条項に反して、ライセンスキーの使用に関する活動、または何らかの形式での使用済みまたは未使用のライセンスキーの譲渡、不正複製、複製または生成されたライセンスキーの配布、あるいは供給者以外から入手したライセンスキーを使用したソフトウェアの利用など、本ソフトウェアの使用の資格がない個人にライセンスキーを提供する行為を実施しないことに同意します。

7.**著作権**。本ソフトウェア、および所有権や知的所有権を含む一切の権利は、ESETおよび / またはESETのライセンス供給者の財産です。これらは、国際条約の規定と本ソフトウェアが使用される国のその他のすべての準拠法によって保護されます。本ソフトウェアの構造、編成、およびコードは、ESETおよび / またはESETのライセンス供給者の重要な企業秘密であり機密情報です。お客様は、第6条(a)に当てはまる場合を除いて、本ソフトウェアをコピーすることはできません。本契約に基づき、お客様が作成するコピーはすべて、本ソフトウェア上に示されるものと同じ著作権表示および所有権表示を含んでいなければなりません。お客様がリバースエンジニアリング、逆コンパイル、逆アセンブルを行ったり、本契約の規定に違反する方法でソースコードを取得しようとした場合、それによって得られたいかなる情報も、それが発生した瞬間からすべて、本契約の違反に関連する供給者の権利にかかわらず、自動的にかつ取り消しできない形で供給者に譲渡され、供給者の所有であるとみなされます。

8.**権利の留保**。本ソフトウェアに対する権利は、本契約において本ソフトウェアのエンドユーザーとしてお客様に明示的に与えられた権利を除き、すべて供給者自身が留保します。

9.**複数言語対応バージョン、デュアルメディアソフトウェア、複数コピー**。本ソフトウェアが複数のプラットフォームまたは言語をサポートしているか、お客様が本ソフトウェアのコピーを複数入手した場合、お客様はライセンスを取得したバージョンのコンピューターシステム数でのみ本ソフトウェアを使用できます。使用していない本ソフトウェアのバージョンやコピーを、他者に売却、賃貸、賃借、サブライセンス付与、貸与、または譲渡することはできません。

10.**本契約の開始と解除。**本契約は、お客様が本契約に同意した日から有効となります。本契約は、お客様が本契約に同意した日から有効となります。お客様は、供給者またはそのビジネスパートナーから入手した本ソフトウェア、すべてのバックアップコピー、および関連するすべての資料を、永久的に削除、破棄、または自費で返却することにより、本契約を解除することができます。本ソフトウェアおよび本ソフトウェアの機能を使用するお客様の権利にはEOLポリシーが適用される場合があります。本ソフトウェアまたは本ソフトウェアの機能がEOLポリシーで定義されているサービス終了日に達した後は、本ソフトウェアを使用するお客様の権利が失効します。本契約の終了の態様に関係なく、第7条、第8条、第11条、第13条、第19条、および第21条の規定は、無期限に有効であり続けるものとします。

11.**エンドユーザーの表明**。お客様はエンドユーザーとして、明示または暗黙のいかなる種類の保証も伴わず、該当の法律によって許可される範囲において、本ソフトウェアが「現状有姿」のまま提供されていることを認めるものとします。供給者、そのライセンス供給者、関係者、および著作権保有者のいずれも、本ソフトウェアの特定の目的に対する商品性または適合性、および第三者の特許、著作権、商標、またはその他の権利に対する侵害の不存在について、明示または黙示を問わず、一切の表明または保証を行いません。供給者もその他の関係者も、本ソフトウェアに含まれている機能がお客様の要求に沿うこと、または本ソフトウェアが円滑で問題なく動作するということの保証を行いません。お客様は、意図する結果に到達するための本ソフトウェアの選択、および本ソフトウェアのインストール、使用、および本ソフトウェアで達成される結果について、完全に責任とリスクを負います。

12.**さらなる義務の否定**。本契約で具体的に列挙される義務以外に、本契約が供給者およびそのライセンサーに対して課す義務はありません。

13.**責任の制限**。準拠法によって許可される最大限の範囲において、いかなる場合も、供給者、その被雇用者、ライセンス供給者は、どのような態様で発生したものであろうと、契約、違法行為、怠慢、または責任の発生を定めるその他の事実のいずれに起因するものであるかを問わず、本ソフトウェアのインストール、本ソフトウェアの使用、または本ソフトウェアが使用できないことにより発生した、利益、収益、または売上の損失、データの喪失、補用品またはサービスの購入にかかった費用、物的損害、人的損害、事業の中断、企業情報の喪失、特別損害、直接損害、間接損害、偶発的損害、経済的損害、補填損害、懲罰的損害、特別または派生的損害に対し、一切責任を負わないものとします。これは、たとえ供給者、そのライセンス供給者、または関係者がそのような損害の可能性について通知を受けていた場合であっても同様です。一部の国および法律では、免責を認めず、しかし限定された範囲の責任を負うことは許可しています。その場合、供給者、その被雇用者、ライセンス供給者、または関係者の責任は、お客様がライセンスの対価として支払った金額を限度とします。

14. 本契約に含まれるものは何も、それに反する場合であっても、消費者として取引するすべての当事

者の法的権利を損なうものではありません。

15.**テクニカルサポート**。テクニカルサポートは、ESETまたはESETの依頼を受けた第三者の独自の判断により提供され、いかなる種類の保証も表明も伴わないものとします。本ソフトウェアまたは本ソフトウェアの機能がEOLポリシーで定義されているサービス終了日に達した後は、テクニカルサポートが提供されません。エンドユーザーは、テクニカルサポートの提供の前に、存在するすべてのデータ、ソフトウェア、プログラム機能をバックアップする必要があります。ESETおよび／またはESETの依頼を受けた第三者は、テクニカルサポートの提供によりお客様に生じたデータ、資産、ソフトウェアまたはハードウェアの損害または損失、もしくは利益の喪失について、いかなる責任も負いません。ESETおよび／またはESETの依頼を受けた第三者は、問題をテクニカルサポートで解決できないと判断する権利があります。ESETは、独自の判断により、テクニカルサポートの提供を拒否、中断、終了する権利があります。ライセンス情報、情報、およびプライバシーポリシーに準拠した他のデータは、技術サポートを提供するために必要になる場合があります。

16.**ライセンスの譲渡**。本契約の条件に違反しないかぎり、あるコンピューターにインストールされていた本ソフトウェアを別のコンピューターシステムにインストールすることができます。エンドユーザーは、本契約の条件に違反しない場合のみ、供給者の同意の元、本契約から派生するライセンスおよびすべての権利を、別のエンドユーザーに永久に譲渡する権利があります。その場合、(i) 元のエンドユーザーは、ソフトウェアのコピーを保持しておらず、(ii) 元のエンドユーザーから新しいエンドユーザーへ直接権利が譲渡され、(iii) 新しいエンドユーザーが元のエンドユーザーに課せられた本契約に基づくすべての権利および義務を負い、(iv) 元のエンドユーザーが新しいエンドユーザーに、第17条で規定するソフトウェアが正規のものであることを証明するドキュメントを提供するものとします。

17.**正規ソフトウェアの証明。**エンドユーザーのソフトウェアの使用資格は、次のいずれかの方法で証明できます。(i)供給者または供給者が指定した第三者が発行するライセンス証明書、(ii)締結されている場合、書面によるライセンス契約、(iii) アップデートを有効にするライセンスの詳細（ユーザ名およびパスワード）が記載された供給者に送信された電子メールの提出。ライセンス情報およびプライバシーポリシーに準拠したエンドユーザー識別データは、ソフトウェアの純正を検証するために必要になる場合があります。

18.**公共団体および米国政府に対するライセンス**。米国政府を含む公共団体に対する本ソフトウェアのライセンスは、本契約に明記しているライセンス権利および制限に基づいて提供されます。

19.**輸出管理規制**。

a)お客様は、直接的または間接的に、ESETまたはESETの持ち株会社、ESETの子会社、持ち株会社の子会社、持ち株会社が管理する事業体による次のような輸出貿易管理法の違反または輸出貿易管理法の下で否定的な結果につながる一切の個人に対して本ソフトウェアを輸出、再輸出、移転、または提供せず、そのような方法でソフトウェアを使用せず、そのような行為に関与したりしないものとします。

i. 米国、シンガポール、英国、欧州連合またはその加盟国、本契約の義務が履行される国、あるいはESETまたはその関連会社が登録または事業を行う国の政府、州、規制当局が発行または採用した、商品、ソフトウェア、技術、サービスの輸出、再輸出、または移転を統制、制限、またはライセンス要件を課すすべての法律。

ii. 米国、シンガポール、英国、欧州連合またはその加盟国、本契約の義務が履行される国、あるいはESETまたはその関連会社が登録または事業を行う国の政府、州、規制当局が課した経済、金融、貿易、制裁、制限、禁止、輸出入禁止、資金または資産の移転の禁止、サービス提供の禁止、あるいは同等の対策。

（上記第i項および第ii項で参照される法律、ならびに「貿易管理法」）。

b) ESETは、次の場合において、本契約の義務を即時停止または解除する権利を有するものとします。

i.ESETが、合理的な意見において、ユーザーが本契約の第19 a)条の条項に違反したか違反する可能性が

高いと判断した

ii. エンドユーザーまたは本ソフトウェアに輸出貿易管理法が適用され、その結果として□ESETが、合理的な意見において、本契約の義務の継続的な履行によって□ESETまたはその関連会社が輸出貿易管理法に違反するか、輸出貿易管理法の下で否定的な影響を受ける可能性があると判断した

c) いずれの当事者も、適用される輸出貿易管理法に準拠しないか、輸出貿易管理法の下で罰則を受けるか、禁止される行為または不作為(あるいは行為または不作為に同意すること)を勧誘または義務付けられるように、本契約のいずれの条項も意図せず、何もそのように解釈または理解されない

20.**通知**。すべての通知、ならびに本ソフトウェアおよびドキュメントの返却は、本契約の第22条に従い、本契約、プライバシーポリシ□□EOLポリシー、ドキュメントの変更をお客様に通知するESETの権利を損なうことなく□ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic宛てに送付する必要があります□ESETは、電子メールや、本ソフトウェア経由でのアプリ内通知を送信したり□Webサイトにコミュニケーションを投稿したりする場合があります。お客様は、規約、特別な規約、プライバシーポリシーの変更、契約の提案/承諾、またはキャンペーンへの招待、通知または他の法的な通知に関するコミュニケーションを含め、電子的な形式でESETから法的な通知を受信することに同意します。適用される法律で特に別のコミュニケーションの形態が義務付けられている場合を除き、かかる電子的なコミュニケーションは書面を受け取った場合と同義に見なされるものとします。

21.**準拠法**。本契約は、スロバキア共和国の法律に準拠し、これに従って解釈されるものとします。エンドユーザーおよび供給者は、準拠法および国際物品売買契約に関する国際連合条約の矛盾する規定については、適用されないことに同意するものとします。お客様は、本契約に関するいかなるクレームもしくは供給者との紛争、または本ソフトウェアをお客様が使用することによるいかなる紛争またはクレームも、ブラチスラバ第1地方裁判所で解決し、さらに、ブラチスラバ第1地方裁判所での管轄権の行使に同意し、明示的にこれを承諾するものとします。

22.**一般条項**。本契約の条項のいずれかが無効または履行不能である場合、これが本契約のその他の条項の有効性に影響を及ぼすことはないものとします。これらその他の条項は、本契約に定める条件に基づき、引き続き有効かつ履行可能であるものとします。本契約は英語で締結されました。便宜上またはその他の目的で、本契約書の翻訳が用意されている場合、または本契約の翻訳版の間で不一致がある場合には、英語版が優先されるものとします。

ESETは、(i) 本ソフトウェアまたはESETの事業の方法に関する変更を反映する□(ii) 法律、規制、セキュリティの理由から□(iii) 悪用または被害を防止するため、関連するドキュメントを更新することで、いつでも、本ソフトウェアを変更し、本契約、付録、補遺、プライバシーポリシ□□EOLポリシー、ドキュメントまたはその一部を改訂する権利を留保します。これらの条項の改訂は、電子メール、アプリ内通知、または他の電子的な手段で通知されます。お客様が本契約の変更の提案に同意しない場合は、変更の通知を受領してから30日以内にアカウントまたは影響を受ける購入済みのサービスを解約できます。この期限内に本契約を解約しない場合は、提案された変更が承認されたと見なされ、変更の通知を受け取った日時点でお客様側で変更が有効になります。

本契約は、本ソフトウェアに関するお客様および供給者間の合意事項をすべて網羅しており、本ソフトウェアに関する従前のいかなる表明、議論、約束、情報交換、または広告にも取って代わります。

EULAID: EULA-PRODUCT-LG; 3537.0

プライバシーポリシー

データ管理者としてのESET, spol. s r. o. (登録事業所所在地: Einsteinova 24, 851 01 Bratislava, Slovak Republic□商業登記: ブラチスラバ第1地方裁判所、有限会社部門、登録番号3586/B□事業登記番号:ブラチスラバ第1地方裁判所、有限会社部門、登録番号3586/B□事業登記番号:31333532) (□ESET□または「当社」)は、お客様の個人データとプライバシーの処理に関して透明でありたいと考えています。この目標を達成するために、当社は、お客様(「エンドユーザー」または「お客様」)に次の事項を通知する目的でのみ、

本プライバシーポリシーを発行しています。

- 個人データの処理、
- データの機密保持、
- データの主体の権利。

個人データの処理

製品に実装されたESETが提供するサービスは、エンドユーザーライセンス契約(EULA)の条項に従って提供されますが、項目によっては特定の注意が必要になる場合があります。ESETは、サービスの提供に関連するデータ収集の詳細について、お客様に説明します。ESETは、アップデート/アップグレードサービス、ESET LiveGrid®、データの悪用に対する保護、サポートなど、エンドユーザーライセンス契約および製品資料に記載されているさまざまなサービスを提供します。すべてを機能させるために、ESETは次の情報を収集する必要があります。

- 製品がインストールされているプラットフォームを含むインストール処理とコンピューターに関する情報、およびオペレーティングシステム、ハードウェア情報、インストールID、ライセンスID、IPアドレス、MACアドレス、製品の構成設定といった製品の動作と機能に関する情報を含むアップデートおよび統計情報。
- ESET LiveGrid®レピュテーションシステムの一部として侵入に関連する単方向ハッシュ。これは、検査済みファイルをクラウドのホワイトリストおよびブラックリスト項目のデータベースと比較し、ESETマルウェア対策ソリューションの効率化を図ります。
- ESET LiveGrid®フィードバックシステムの一部として世界から収集した不審なサンプルおよびメタデータ。これにより、ESETは、エンドユーザーのニーズに迅速に対応し、最新の脅威に反応し続けることができます。ESETはお客様がESETに送信する次の情報を必要としています
  - oウイルスおよび他の悪意のあるプログラム、ならびにお客様によって迷惑メールとして報告されたか、製品によって警告された実行ファイル、電子メールメッセージなどの不審であるか、問題があるか、望ましくない可能性があるか、危険の可能性があるオブジェクトの潜在的なサンプルといった侵入情報
  - oデバイスの種類、ベンダー、モデル、名前などのローカルネットワークのデバイスに関する情報
  - oIPアドレスおよび地理情報、IPパケット、URLおよびイーサネットフレームなどのインターネットの使用に関する情報
  - o含まれるクラッシュダンプファイルと情報

当社は、この範囲外でデータを収集する意志はありませんが、場合によってはそれが防止できないことがあります。誤って収集されたデータは、マルウェア自体に含まれる場合があります。当社は、本プライバシーポリシーで規定された目的において、そのようなデータを当社のシステムまたはプロセスに取り込む意図はありません。

- ライセンスIDなどのライセンス情報、および名前、姓、住所、電子メールアドレスなどの個人データは、課金、ライセンスの真正の検証、サービスの提供のために必要です。
- サポート要求に含まれる連絡先情報およびデータは、サポートのサービスで必要になる場合があります。選択した連絡方法に基づき、当社は、電子メールアドレス、電話番号、ライセンス情報、製品詳細、およびサポートケースの説明を収集する場合があります。サポートのサービスを進めるために、他の情報の提供を求められる場合があります。

データの機密保持

ESETは、販売、サービス、サポートネットワークの一部として、関連会社またはパートナー経由で、世界中で事業を展開している会社です。ESETによって処理された情報は、サービスの提供、サポート、または請求などのEULAの履行のため、関連会社またはパートナー企業との間で転送される場合があります。選択した位置情報およびサービスに基づき、欧州委員会の適切な決定権がない国にお客様のデータを転送する必要がある場合があります。この場合でも、情報を転送するたびに、データ保護法の規制が適用され、必要な場合にのみ実行されます。標準契約条項、拘束的企業準則、または他の適切な安全保護対策を例外なく確立する必要があります。

ESETは、エンドユーザーライセンス契約に従って、サービスを提供している間、必要最低限の期間にのみデータが保存されるように最善の努力を講じます。ESETの保持期間は、お客様が簡単かつスムーズな更新が行える時間的余裕を用意するために、ライセンスの有効期間よりも少し長くなる場合があります。ESET LiveGrid®からの最小化および仮名化された統計情報および他のデータが統計目的で処理される場合があります。

ESETは、適切な技術的および組織的な対策を導入し、潜在的なリスクに適したレベルのセキュリティを保証します。当社は最善を尽くし、処理システムおよびサービスに関する、継続中の機密性、完全性、可用性、および障害回復力を保証します。ただし、お客様の権利と自由を脅かす結果になるデータ違反の場合には、すぐに監督当局とデータ主体に通知します。データ主体として、お客様は、監督当局に苦情を申し立てる権利を有します。

データの主体の権利

ESETはスロバキア法の規制に準拠し、欧州連合の一部としてデータ保護法によって拘束されます。適用されるデータ保護法で規定された条件が適用されます。お客様は、データ主体として、次の権利を有しています。

- ESETに対してお客様の個人データへのアクセスを要求する権利、
- 不正確な個人データを修正する権利(不完全な個人データを完全にする権利もあります)
- 個人データの消去を要求する権利、
- 個人データの処理の制限を要求する権利
- 処理に異議を申し立てる権利
- 苦情を申し立てる権利および
- データ移植性の権利。

データ主体として権利を行使する場合、またはご質問や懸念をお持ちの場合は、以下の宛先までご連絡ください。

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk