ESET Server Security for Linux

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 Server Security for Linux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: 2024年/4月/12日

概要

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LinuxのすべてのサーバーでESET Server Security for Linux (ESSL)が最適な選択肢となります。

主要な機能には、オンデマンドスキャナーとオンアクセススキャナーがあります(リアルタイムファイルシステム保護)

オンデマンドスキャナーは、コマンドラインインターフェイスWebインターフェイス、また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)を使用して起動できます。オンデマンドという用語は、ユーザーまたはシステムの要求にょって検査されるファイルシステムオブジェクトを指します。

オンアクセススキャナーは、ユーザーまたはオペレーティングシステムがファイルシステムオブジェクトにアクセスを試みるたびに実行されます。検査はファイルシステムオブジェクトにアクセスする試みによってトリガーされます。

システムの主要な機能

- 自動製品アップデート
- システムの管理を容易にし、セキュリティの概要を示すために再設計されたWebインターフェイス
- ESETの軽量カーネル内モジュールによるアクセス中の検査
- 包括的な検査ログ
- 検索バーが導入された、再設計された使いやすい設定ページ
- 隔離
- ESET PROTECTで管理可能
- クラウドベース保護
- Webアクセス保護
- コンテナーセキュリティ
- ESET Inspectサポート

リリースノート

システム要件

クイックリンク: サポートされているオペレーティングシステムサポートされているブラウザーサポートされているファイルシステム

ハードウェア要件

ハードウェア要件はサーバーロールによって異なります。インストールには、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 x64：2コア
- 2GBのRAM
- 700MBのハードディスク空き領域
- glibc 2.17以降
- Linux OSカーネルバージョン3. 10. 0以降
- 任意のUTF-8エンコーディングロケール

サポート対象のオペレーティングシステム

ESET Server Security for Linux (ESSL)は一覧のオペレーティングシステムの最新のマイナーリリースでテストされ、サポートされています：ESSLのインストール前にオペレーティングシステムを更新してください。

64ビットオペレーティングシステム	セキュアブートがサポートされています	注意
RedHat Enterprise Linux (RHEL) 7	✔	
RedHat Enterprise Linux (RHEL) 8	✔	
RedHat Enterprise Linux (RHEL) 9	✔	
CentOS 7	✔	
Ubuntu Server 18.04 LTS	✔	
Ubuntu Server 20.04 LTS	✔	
Ubuntu Server 22.04 LTS	✔	
Debian 10	✔	
Debian 11	✔	
Debian 12	✔	
SUSE Linux Enterprise Server (SLES) 15	✔	
Alma Linux 8	✔	
Alma Linux 9	✔	
Rocky Linux 8	✔	
Rocky Linux 9	✔	
Oracle Linux 8	✔（ストックカーネルのみ）	Unbreakable Enterprise Kernelが使用されている場合は、kernel-uek-develパッケージを手動でインストールする必要があります。この場合、セキュアブートはサポートされていません。
Amazon Linux 2		

上記の一覧のハードウェア要件が満たされ、使用されているLinuxディストリビューションで不足しているソフトウェア依存関係がないかぎりESSLは最も一般的に使用されている、最新のオープンソースLinuxディストリビューションで動作します。

ELREPOカーネルと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。
「汎用オペレーティングシステムの保護プロファイル(OSPP)のRHELはサポートされていません。

ESET PROTECTでのリモート管理

サポートされているブラウザー

ESSL Webインターフェイスは次のブラウザーのデスクトップバージョンでのみ動作します。

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Safari

ESSLWeb インターフェイスで問題が表示される場合は、上記の最新バージョンのブラウザーを使用してください。

サポートされているファイルシステム

ESET Server Security for Linux (ESSL)は、次のファイルシステムでテストされ、サポートされています。

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 (snapappimage)	✔		

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
tmpfs	✔		
NFSクライアント(バージョン3、バージョン4)			✔
SMB (GVfs, CIFS)			✔
SSHFS			✔

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Webアクセス保護を使用するにはESET Server Security for Linux (ESSL)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ESSL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/efs/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。パスワードは覚えておいてください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/efs/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/efs/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ESSL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/efs/eset_rtp`および`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 Server Security 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 efs
```

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。

インストール

ESET Server Security for Linux (ESSL)はバイナリファイル(*.bin*)として配布されます。

コンピュータに他のウイルス対策プログラムがインストールされていないことを確認します。2つ以上のアンチウイルス溶液が単一のコンピューターにインストールされている場合、それらは互いに競合する可能性があります。システム上の他のウイルス対策プログラムをアンインストールすることをお勧めします。

OSをアップデート
ESET Server Security 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。

不要なモジュールのないインストーラー
バージョン10以降ESET Server Security for Linuxインストールパッケージには必須モジュールのみが含まれており、そのサイズは元のサイズの15%に削減されています。この変更によりESET Server Security for Linuxはインストール後に部分的にしか機能しません。
製品を完全に機能させるには、次のいずれかを行う必要があります。
- インストーラーをパラメーター`-m MIRROR`と使用すると、インストール中に*MIRROR*ディレクトリからモジュールがコピーされます(たとえば、MirrorToolによって作成されたもの)
- ESET Server Security for Linuxをアクティベーションし、不足しているモジュールをダウンロードします

以前のバージョンがアクティベーションされ、すべてのモジュールがある場合、アップグレード後に製品は完全に機能します。

ターミナルを使用してインストールする

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。

- `./efs.x86_64.bin`
- `sh ./efs.x86_64.bin`

使用可能なコマンドライン引数を参照してください

ESET Server Security 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。

```
bash ./efs.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しない
-y	--accept-license	ライセンスを表示しない。ライセンスは承諾済み
-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
-g	--no-gui	インストール後にGUIを設定/起動しない
-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
-m		MIRRORディレクトリからモジュールnupsをコピーする

> **.debまたは.rpmインストールパッケージを入手する**
> OSに適した.debまたは.rpm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 ./efs.x86_64.bin -n
> ```
> または
> ```
> sudo sh ./efs.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すると、インストールが完了し、Webインターフェイスログイン詳細情報が表示されます。

インストーラーは依存関係の問題について通知します。

ESET PROTECTを使用してインストールする

ESET Server Security 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。

必要に応じて、Webインターフェースをリモートで有効にします。

ESET Server Security 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 Server Security 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 Server Security 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/efs/doc/modules_notice/*にある*NOTICE_mode*ファイルを参照してください。

再インストール

インストールが何らかの理由で破損した場合は、インストーラーを再実行してください。設定は変更されません。

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 efs`
- `dpkg remove efs`

Red Hatベースのディストリビューション:

- `yum remove efs`
- `dnf remove efs`
- `rpm -e efs`

SUSEベースのディストリビューション:

- `zypper remove efs`
- `rpm -e efs`

一括展開

このトピックでは、PuppetChefAnsible経由でのESET Server Security 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には、パッケージをインストールする方法について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 Server Security 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 Server Security 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/efs-8.0.1081.0.x86_64.bin":
           mode => "0700",
           owner => "root",
           group => "root",
           source => "puppet:///modules/efs/efs-8.0.1081.0.x86_64.bin"
         }
    exec {"Execute bin package installation":
           command => '/tmp/efs-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/efs-8.0.1081.0.x86_64.deb":
               mode => "0700",
               owner => "root",
               group => "root",
               source => "puppet:///modules/efs/efs-8.0.1081.0.x86_64.deb"
             }
        package {"efs":
               ensure => "installed",
               provider => 'dpkg',
               source => "/tmp/efs-8.0.1081.0.x86_64.deb"
             }
}
if $osfamily == 'RedHat' {

        file {"/tmp/efs-8.0.1081.0.x86_64.rpm":
               mode => "0700",
               owner => "root",
               group => "root",
               source => "puppet:///modules/efs/efs-8.0.1081.0.x86_64.rpm"
             }

        package {"efs":
               ensure => "installed",
               provider => 'rpm',
               source => "/tmp/efs-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/efs-8.0.1084.0.x86_64.bin' do
        source 'efs-7.0.1084.0.x86_64.bin'
        owner 'root'
        group 'root'
        mode '0700'
        action :create
end

execute 'package_install' do
        command '/tmp/efs-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/efs-8.0.1084.0.x86_64.deb' do
        source 'efs-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/efs-8.0.1084.0.x86_64.rpm' do
                source 'efs-8.0.1084.0.x86_64.rpm'
                owner 'root'
                group 'root'
                mode '0700'
                action :create
                only_if { node['platform_family'] == 'rhel'}

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

rpm_package 'efsu' do
        source '/tmp/efs-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: efs-8.0.1084.0.x86_64.bin
    dest: /home/ansible/

- name : "Install product bin package"
  shell: bash ./efs-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: ./efs-8.0.1085.0.x86_64.deb
          dest: /home/ansible/efs-8.0.1085.0.x86_64.deb
          owner: ansible
          mode: a+r
        when:
          - ansible_os_family == "Debian"

      - name: "Copy rpm package to VM"
        copy:
          src: ./efs-8.0.1085.0.x86_64.rpm
          dest: /home/ansible/efs-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/efs-8.0.1085.0.x86_64.deb
          state: present
        when:
          - ansible_os_family == "Debian"

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

ESET Server Security 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 Server Security for Linux (ESSL)をアクティベーションします。

Webインターフェイスを使用してアクティベーションする

1. Webインターフェイスにログインする。
2. **ステータス概要** > **ライセンス**をクリックします。
3. 任意のアクティベーション方法を選択します。

• 製品認証キーでアクティベーションする - ESET Server Security for Linux製品認証キーを購入したユーザー向けです。

• **アカウント** – ESET Server Security for Linuxライセンスをアカウントにインポートした、登録済みのESET Business Account (EBA)またはESET MSP Administrator (EMA)、またはESET PROTECT HUBユーザーの場合はEBAまたはEMAまたはESET PROTECT HUBユーザー名およびパスワードが必要です。

• オフラインライセンス - ESET Server Security for Linuxがインターネットに接続できない場合に、こ

のオプションを使用します。ESSLはオフライン環境で使用されます。

- ESET管理コンソール

ライセンスが期限切れの場合は、同じ場所でライセンスを別のライセンスに変更できます。

EBA、EMA、またはESET PROTECT HUBログイン資格情報を使用してESSLをアクティベーションする

1. Webインターフェイスにログインする。
2. **ステータス概要** > **ライセンス**をクリックし、**アカウント**を選択します。
3. EBA、EMA、またはESET PROTECT HUBログイン資格情報を入力します。
4. 特定のライセンスまたはサイト(ライセンスプール)を選択してESSLをアクティベーションします。
5. **アクティベーション**をクリックします。

ターミナルを使用してアクティベーションする

`/opt/eset/efs/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 Server Security for Linuxをアクティベーションします。

Syntax: `/opt/eset/efs/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てアクティベーション

```
/opt/eset/efs/sbin/lic -k XXXX-XXXX-XXXX-XXXX-XXXX
```

または

```
/opt/eset/efs/sbin/lic --key XXXX-XXXX-XXXX-XXXX-XXXX
```

`XXXX-XXXX-XXXX-XXXX-XXXX`はESET Server Security 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/efs/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ESSL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/efs/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/efs/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/efs/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/efs/sbin/lic -f offline_license.lf
```

または

```
/opt/eset/efs/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。

アクティベーションが完了したら、Webインターフェイスにアクセスし、システムの最初の検査を起動するかESET Server Security for Linuxを設定します。

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。

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/efs/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/efs/sbin/lic -s`
または
`/opt/eset/efs/sbin/lic --status`

製品がアクティベーションされたときの出力内容:
```
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 Server Security 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。

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

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

アップデートとアップグレード

モジュールの更新

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。

手動で検出モジュールをアップデートするには、**モジュールのアップデート > 確認してアップデート**をクリックします。

ESET Server Security 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。**ステータス概要 > モジュールのアップデート > モジュールロールバック**をクリックし、任意の期間を選択して、**今すぐロールバック**をクリックします。

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/efs/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
-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
-l	--list-modules	製品モジュールのリストを表示する
	--check-app-update	リポジトリの新しい製品バージョンの利用可能状況を確認
	--perform-app-update	利用可能な場合は新しい製品バージョンをダウンロードしてインストール
	--accept-license	ライセンスの変更を許可

updの制限
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。

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/efs/bin/upd --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/efs/bin/upd --resume`
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/efs/bin/upd --update --server=192.168.1.2:2221`

ESET Server Security for Linuxを新しいバージョンにアップグレードする

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 Server Security for Linuxの新バージョンが提供されています。

インストールされている製品バージョンを決定する

ESET Server Security for Linuxの製品バージョンは、次の2つの方法で判別することができます。

- Webインターフェースで**ヘルプ > バージョン情報**をクリックします。

- ターミナルウィンドウで、`/opt/eset/efs/sbin/setgui -v`を実行します。

ESET Server Security for Linuxローカルアップグレード

- インストールセクションに従い、OS関連のインストールパッケージを実行します。
- Webインターフェイスで、**ステータス概要 > 製品のアップデート > アップデートの確認**をクリックします。
- `--perform-app-update`パラメーターでupdユーティリティを使用します。
- 自動アップデート/アップグレードの設定

ESET Server Security for Linuxリモートアップグレード

ESET PROTECTを使用してESET Server Security for Linuxを管理している場合は、次の方法でアップグレードを開始できます。

- ソフトウェアインストールタスク。
- Webインターフェイスで、**ダッシュボード > ESETアプリケーション**に移動し、Server SecurityESETをクリックします、**インストールされているESET製品を更新します**
- 自動アップデート/アップグレードの設定

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、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ために使用できるアップデートファイルのコピーを作成することができます。「ミラーサーバーの作成」の使用 - LAN環境でアップデートファイルのコピーを作成すると、ベンダのアップデートサーバーからワークステーションごとに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、インターネット接続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 Server Security for Linuxを設定する

1. Webインターフェイスで、**設定 > アップデート > プライマリサーバー**に移動します。
2. **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。
3. **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。
   a. `http://<IP>:<port>/<path_to_update_folder>`
   b. `http://<hostname>:<port>/<path_to_update_folder>`
4. 該当するユーザー名とパスワードを入力します。

5. **[保存]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。

> **ローカルディレクトリからアップデート**
> */updates/eset*などのローカルディレクトリからアップデートするには、**アップデートサーバー**フィールドを入力します。
> *file:///updates/eset/*

自動製品のアップデート

バージョン9.1以降では、既定でESET Server Security for Linux (ESSL)の自動製品アップデートが有効です。この設定を有効にして、新しいアップデートが利用可能になるときにESSLで最新の製品アップデートがが必ず適用されるようにすることをお勧めします。

ESSLバージョン9.1以降で自動製品製品アップデートを編集するには

1. Webインターフェースで、**設定 > アップデート**をクリックします。
2. **製品のアップデート**セクションで、**自動アップデート**の横のスライダーをクリックします。
3. 製品アップデートでカスタムアップデートサーバーを使用する場合:
   a.**カスタムサーバー**フィールドでサーバーアドレスを定義します。
   b.該当するフィールドに**ユーザー名**と**パスワード**を入力します。
4. **[保存]をクリックします**

ESSLバージョン9.0以前で自動製品アップデートを有効にするには

1. Webインターフェースで、**設定 > アップデート**をクリックします。
2. **製品アップデート**セクションで、**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。
3. 製品アップデートでカスタムアップデートサーバーを使用する場合:
   a.**カスタムサーバー**フィールドでサーバーアドレスを定義します。
   b.該当するフィールドに**ユーザー名**と**パスワード**を入力します。
4. **[保存]をクリックします**

ESET PROTECTを使用してESET Server Security for Linuxを管理する場合は、ポリシーを使用して上記の自動アップデートを設定します。

ESET Server Security 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 Server/File Security 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. [**完了**]をクリックします。

> **再起動が推奨されます**
> リモート管理されたコンピューターで自動アップデートが有効で、新しいパッケージが自動的にダウンロードされる場合、ESET PROTECTの保護の状態が**再起動が推奨されます**になります。

自動アップデート(バージョン9.1以降)

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。

アップデートモード(バージョン9.0以前)

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**ステータス概要**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。

コマンドと ESET Server Security for Linux

Webインターフェイスにアクセスする

インストールが完了した場合は、インストーラーで表示されているURLアドレスとログイン資格情報を使用してWebインターフェイスにログインします。

Webインターフェイスは次の言語で提供されています。

- 英語
- フランス語
- スペイン語
- スペイン語(ラテンアメリカ)
- ドイツ語
- 日本語
- Ukrainian
- ポーランド語

SSL証明書

ESET Server Security for Linux Webインターフェイス証明書

ESET Server Security for Linux Webインターフェイスは自己署名証明書を使用します。初めてWebインターフェイスにアクセスすると、へを追加しないかぎり、証明書の問題というメッセージが表示されます証明書の例外.

- Mozilla Firefoxで証明書の例外を追加します。

1. **詳細** > **例外の追加**をクリックします。
2. **セキュリティ例外の追加**ウィンドウで、**この例外を永久的に保存する**を選択していることを確認します。
3. **セキュリティ例外の確認をクリックします**

- Google Chromeで証明書の例外を追加します。

1. **詳細**をクリックします。
2. **<web address of ESSL WebインターフェイスのWebアドレスに進む（危険）**
3. この時点で、Google Chromeが例外を記憶します。

Webインターフェイスからカスタム SSL証明書を使用するには、証明書を生成してESET Server Security for Linuxにインポートします。

1. SSL証明書を生成する：

```
openssl req -newkey rsa:2048 -new -nodes -x509 -days 3650 -keyout privatekey.pem -
out certificate.pem
```

2. SSL証明書をESET Server Security for Linuxにインポートする：

```
sudo /opt/eset/efs/sbin/setgui -c certificate.pem -k privatekey.pem -e
```

Webインターフェイスをリモートで有効にする

ESET PROTECTを使用してリモートでESET Server Security for Linuxのインストールを実行した場合は、Webインターフェイスが有効になりません。
特定のコンピューターでWebインターフェイスにアクセスする場合は、ターミナルウィンドウから次のコマンドを実行します。
```
sudo /opt/eset/efs/sbin/setgui -gre
```
最終出力は、WebインターフェイスのURLアドレスとアクセス資格情報を示します。
10.1.184.230:9999などのカスタムIPアドレスとポートでWebインターフェイスを使用可能にする場合は、ターミナルウィンドウから次のコマンドを実行します。
```
sudo /opt/eset/efs/sbin/setgui -i 10.1.184.230:9999
```

ESET PROTECT経由でWebインターフェースを有効にするには、コマンドの実行タスクを使用して、次のコマンドを実行します。
```
/opt/eset/efs/sbin/setgui -re --password=<password>
```
<password>はユーザーが定義した任意のパスワードを表します。

setguiコマンドの使用可能なオプション

オプション – 短縮型	オプション – 標準型	説明
-g	--gen-password	Webインターフェイスにアクセスするための新しいパスワードを生成します
-p	--password=パスワード	Webインターフェイスにアクセスするための新しいパスワードを定義します
-f	--passfile=ファイル	Webインターフェイスにアクセスするために、ファイルから読み込まれた新しいパスワードを設定します
-r	--gen-cert	新しい秘密鍵と証明書を生成します
-a	--cert-password=パスワード	証明書パスワードを設定します
-l	--cert-passfile=ファイル	ファイルから読み込まれた証明書パスワードを設定します
-i	--ip-address=IP:PORT	サーバーアドレス(IPとポート番号)
-c	--cert=ファイル	証明書のインポート
-k	--key=ファイル	秘密鍵をインポートします
-d	--disable	Webインターフェイスを無効にします
-e	--enable	Webインターフェイスを有効にします

Webインターフェイスによるパスワードの変更

1.ログアウトボタンの横にあるユーザープロファイルをクリックします。

2.**パスワードの変更**をクリックします。

3.古いパスワードと新しいパスワードを入力します。新しいパスワードは、画面に表示される基準を満たしている必要があります。

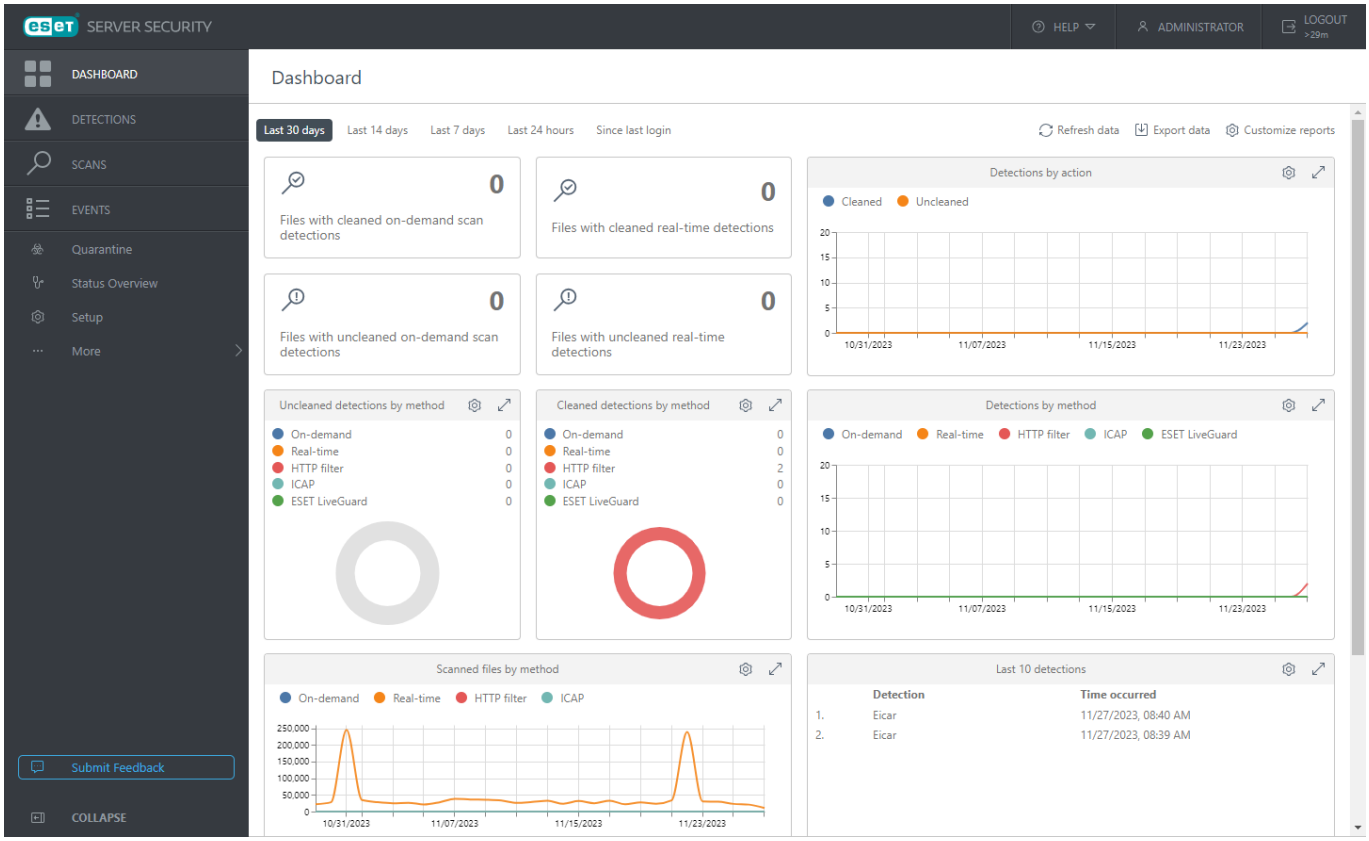
4.**[保存]をクリックします**

製品アクティベーションと最初の検査

ESET Server Security for Linuxのインスタンスをアクティベーションした場合は、検出モジュールをアップデート(**ステータス概要 > モジュールのアップデート > 確認してアップデート**をクリック)し、ファイルシステムの最初の検査を実行します。

ダッシュボード

ダッシュボードには、簡易検査統計情報が表示されます。



検査統計情報

ESET Server Security for Linuxでは、簡易検査統計情報をグラフまたは表で示します。

- アクション別の検出
- 方法別の検出
- 方法別の駆除されていない検出
- 方法別の駆除された検出
- 方法別検査済みファイル *
- 過去10件の検出
- 最もアクセス時の検出が多い上位10ユーザー
- 過去10件のオンデマンド検査と検出
- CPU利用率 *

- **メモリおよびスワップ利用率 ***

タイルの形式でも次の情報が示されます。

- **駆除されたオンデマンド検査の検出があるファイル**
- **駆除されたリアルタイム検出があるファイル**
- **駆除されていないオンデマンド検査の検出があるファイル**
- **駆除されていないリアルタイム検出があるファイル**

> i *が付いた統計は100%正確ではありません。値は15分間隔でサンプルされ、表示前にさらに処理されます。

統計タイルまたはグラフをクリックし、検査または検出画面に移動します。期間プリセットを使用して、統計をフィルタリングします。

駆除されていない検出数が1件以上ある場合は、背景の「未駆除」統計の色が赤に変わります。

表示する統計

1. **レポートのカスタマイズ**をクリックします。
2. 任意の統計を選択/選択解除します。
3. **[保存]をクリックします**

1つの統計を削除するには、設定ボタンをクリックし、**削除**を選択します。

ブラウザーキャッシュを削除しない場合、統計の設定は変更されません。

検査統計のダウンロード

選択した期間のすべての検査統計情報を*.zip*アーカイブファイルとしてダウンロードするには、**データのエクスポート**をクリックします。*.zip*アーカイブファイルには、*.csv*ファイルの統計が含まれます。

特定の検査統計情報をダウンロードするには、設定ボタンをクリックし、**ダウンロード**をクリックしてから**CSV**、または**PDF**を選択します。

検出

アクセス中の検査によって検出されたすべての脅威とそれに対して実行されたアクションは、**検出**画面に記録されます。

オンデマンドスキャナーによって検出された脅威と実行されたアクションは、**検査** > 完了した検査を選択 > **詳細 > 検出**に記録されます。

脅威が検出されていない場合は、行全体が赤色でハイライトされます。

使用可能なセクション

- 検出された悪意があるファイルの駆除を試行するには、特定の行をクリックし、**駆除して再検査**を

選択します。

- 悪意があるファイルとして検出され、まだ削除されていないファイルを探すには、**パスをコピー**を選択し、ファイルブラウザーを使用してファイルを検索します。
- SHA-1ハッシュに基づいて手動で検出除外を作成するには、**ハッシュのコピー**を選択します。
- 除外ウィザードを開始するには、**除外の作成**を選択します。

駆除して再検査または**除外の作成**アクションを一度に複数の検出に適用する:

1. 関連する検出のチェックボックスを選択します。
2. [アクション]をクリックし、任意のアクションを選択します。

検査

検査 > 新規検査 > すべてのローカルドライブを検査から、手動ですべてのローカルドライブの新しい検査を実行します。

カスタム検査を選択します。ここでは、検査プロファイルを選択し、検査する場所を定義できます。**検査して駆除**を選択する場合、選択した検査プロファイルの各駆除レベルが検出された脅威に適用されます。設定された除外を含むすべての項目を検査するには、**検査除外**を選択します。

カスタム検査対象

- ローカルドライブ
- ネットワークドライブ
- リムーバブルメディア
- ブートセクター — すべてのマウントされたドライブ/メディアのブートセクターが検査されます。
- カスタム対象—任意の検査対象パスを入力し、キーボードのTABキーを押します。

各実行済みの検査は、検出および駆除された脅威数情報を含め、**検査**画面に記録されます。**駆除**列が赤色でハイライトされている場合は、一部の感染したファイルが駆除/削除されませんでした。エントリの詳細を表示するには、**詳細を表示**をクリックします。

検査の詳細画面には、次の3つのタブがあります。

- **概要**- **検査**画面に表示されるのと同じ情報に、検査されたディスクの数を加えた情報が表示されます。
- 検出 – 検出された侵入の詳細とそれに対して実行されたアクションが表示されます。
- **検査されていないファイル** – 検査できなかったファイルの詳細と理由が表示されます。

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。

新しいプロファイルを作成するには、**設定 > 検出エンジン > マルウェア検査 > オンデマンド検査 > プロパティのリスト**をクリックします。

ターミナルを使用したオンデマンド検査

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には、/opt/eset/efs/bin/odscanコマンドを使用します。

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

構文: `/opt/eset/efs/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一時停止します
-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(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

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

終了コード	意味
0	マルウェアは検出されませんでした
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

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/efs/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/efs/bin/odscan --scan --profile="@Smart scan" /root/ /tmp/ /home/
```

すべての実行中の検査のリストを出力します

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

除外

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、オンデマンド検査、リモート検査で設定できます。

1. Webインターフェイスで、**設定**をクリックします。
2. 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**をクリックして、リアルタイムファイルシステム保護に関連する除外を変更します。
   - **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**をクリックして、オンデマンド検査(カスタム検査)に関連する除外を変更します。
   - **検出エンジン > リモート検査 > Threatsenseパラメーター**を使用して、リモート検査に関連する除外を変更します。
3. **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。
4. **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。
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. **保存**をクリックして、変更を保存します。

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. Webインターフェイスで、**設定 > 検出エンジン**をクリックします。
2. **パフォーマンスの除外**の横にある**編集**をクリックします。
3. **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。
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. **保存**をクリックして、変更を保存します。

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
システムインフラストラクチャの要件がある場合以外は、パスの中央でワイルドカードを使用しないことをお勧めします(例: */home/user/*/data/file.dat*)。詳細については、次のナレッジベース記事を参照してください。
検出除外を使用するときには、パスの中央でワイルドカードを使用することに関する制限はありません。

検出除外条件

- **パス** – 指定されたパス(または空の場合はすべてのパス)の検出除外

- **検出名** – 検出されたオブジェクトは、定義済みの検出名と一致する場合に除外されます。ファイルが後で他のマルウェアに感染した場合、検出名が変更されます。このような場合、そのファイルは侵入として検出され、適切なアクションが実行されます。**パス**が定義されている場合、そのパスにあり、**検出名**と一致するファイルのみが検出から除外されます。このような検出を除外リストに追加するには、検出除外ウィザードを使用します。あるいは、**隔離**に移動し、隔離されたファイルをクリックして、**復元して除外**を選択します。このオプションは、検出エンジンによって検出対象として評価された項目でのみ表示されます。

- **ハッシュ** – ファイルタイプ、場所、名前、拡張子に関係なく、指定されたハッシュ(SHA1またはSHA256)に基づいて、ファイルを除外します

イベント

ESET Server Security for Linux Webインターフェイスで実行される重要なアクション(Webへのログインの失敗、ターミナルから実行されるESET Server Security for Linux関連のコマンド、および一部のその他の情報は**イベント**画面に出力されます。

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**イベント**画面の内容を表示するには、`lslog`コマンドラインツールを使用します。

Syntax: `/opt/eset/efs/bin/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
`-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

オプション – 短縮型	オプション – 標準型	説明
	--ods-details=ログ名	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=ログ名	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=ログ名	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=ログ名	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のログレコードを一覧表示します

例

すべてのイベントログを出力する:

```
/opt/eset/efs/bin/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/efs/bin/lslog -ec > /home/$USER/Documents/eventlogs.csv
```

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 Server Security 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。任意のファイルを選択して隔離することができます。これは、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にお勧めします。隔離したファイルは、ESETのウイルスラボに提出して分析を受けることができます。

Webインターフェイスで隔離された項目を管理する

隔離画面には、隔離フォルダーに格納されたファイルの一覧が表示されます。この一覧には次の項目が表示されます。

- 隔離の日時、
- 隔離されたファイルの元の場所へのパス
- 検出名(手動で隔離された項目の場合は空)
- ファイルを隔離に移動する理由(手動で隔離された項目の場合は空)

- 脅威の数(複数の侵入を含むアーカイブの場合など)
- 隔離された項目のサイズとハッシュ

隔離された項目をクリックすると、使用可能なアクションが表示されます。

- **復元** – 隔離された項目を元の場所に復元します。
- **復元 と 除外** – 隔離された項目を元の場所に復元し、パスと検出名に一致する検出除外を作成します。
- **パスのコピー** – ファイルの元のパスをクリップボードにコピーします。
- **ハッシュのコピー** —ファイルのSHA-1ハッシュをクリップボードにコピーします。
- **ダウンロード**—隔離された項目をハードドライブにダウンロードします
- **隔離から削除**— 隔離された項目を完全に削除します。
- **分析のために提出**—分析のために隔離された項目のコピーをESETに送信します。

復元して除外オプションは、検出エンジンが除外対象と評価した項目に対してのみ表示されます。

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

分析のために隔離されたファイルを送信する:

1. 項目を選択して、**分析のために送信**を選択します。
2. 適切な**サンプル送信の理由**を選択します。
   - **不審なファイル**: 検査中にファイルを駆除できないファイル、または通常と異なる特性を持つファイル。
   - **誤検出ファイル**: マルウェアとして誤って特定されたファイル
   - **その他**
3. 電子メールアドレスを入力するか、**匿名で送信**を選択します。
4. [**次へ**]をクリックします。
5. 詳細情報を入力します。
6. **送信**をクリックします。

ターミナルを使用した隔離された項目の管理

Syntax: `/opt/eset/efs/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

オプション – 短縮型	オプション – 標準型	説明
-r	--restore=id	idで識別された隔離された項目を--restore-pathによって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新しいパス
-h	--help	ヘルプを表示します
-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「0123456789」の隔離された項目を削除する:

```
/opt/eset/efs/bin/quar -d 0123456789
```

または

```
/opt/eset/efs/bin/quar --delete=0123456789
```

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

または

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

または

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

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/efs/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/efs/bin/quar --restore=ID_OF_OBJECT_TO_RESTORE --restore-
path=/final/path/of/restored/file
```

ステータス概要

ステータス概要は、モジュールと製品のアップデート、ライセンス情報、および製品のアクティベーションオプションを示し、他の製品のステータスを表示します。

すべてが問題なく動作しているときには、タイルが緑色です。システムの保護の状態を改善することが可能な場合、または保護の状態が不十分であることが検出された場合、タイルの色が変わり、詳細情報が表示されます。 タイルをクリックすると、詳細が表示されます。

> **ステータスアラートをミュートまたはミュート解除する**
> 緑以外の各ステータスアラートは、**このアラートをミュート**をクリックしてミュートできます。ステータスが灰色に変わり、関連するタイルがリストの関連する項目の横に🔇が表示されます。**このアラートのミュートを解除**をクリックして、ステータス通知をオンに戻します。
> ESET PROTECTでステータスが無効にされている場合は、**このアラートのミュートを解除**も**有効にする**も**ステータス概要**で使用できません。

モジュールアップデート

すべてのモジュールが最新の場合は、**モジュールのアップデート**タイルが緑色です。モジュールのアップデートが一時的に停止している場合は、タイルがオレンジ色になります。アップデートが失敗した場合は、タイルの色が赤色に変わります。 タイルをクリックすると、詳細が表示されます。

手動で検出モジュールのアップデートを起動するには、**モジュールのアップデート**>**確認してアップデート**をクリックし、アップデートが完了するまで待ちます。

製品のアップデート

すべての製品コンポーネントが最新の場合は、**製品のアップデート**タイルが緑色です。タイルをクリックすると、現在のバージョンの詳細と前回のアップデートの確認が表示されます。

新しいバージョンの製品が利用可能な場合は、タイルが明るい青です。変更ログを表示するか、新しいバージョンにアップグレードするには、**製品アップデート**をクリックしてから、**変更ログを表示**をクリックするか、**今すぐ同意してアップデート**をクリックします。

新しいアップデートの利用可能状況を手動で確認するには、**製品のアップデート**>**アップデートを確認**をクリックします。

自動製品アップデートの設定の詳細を参照してください。

ライセンス

ライセンスがまもなく期限切れの場合、**ライセンス**タイルがオレンジ色になります。ライセンスが期限切れの場合は、タイルが赤色になります。タイルをクリックすると、ライセンスを変更する使用可能なオプションが表示されます。

リアルタイム検査

リアルタイムファイルシステム保護が無効な場合、タイルは赤色です。タイルをクリックし、**保護の状態**通知をミュートにすると、タイルが緑色になります。さらに、が項目の横に表示され、**保護の状態：無効**の横にが表示されます。

> リアルタイムファイルシステム保護が無効で、有効にすると、検査サービスを復元するには最大で1分かかる場合があります。その後、**検査サービス：無効**がタイルに表示されなくなります。**オンデマンド検査**タイルは、ウォッチドッグサービスが有効な場合にのみ表示されます。

その他の機能（以前は他のサービス）

システムの全体的なセキュリティを改善する他の機能およびサービスのグループ。 タイルをクリックすると、詳細が表示されます。

送信されたファイル

ESET Server Security for Linuxバージョン8. 1以降では、分析のためにESET LiveGrid®またはESET LiveGuard Advancedに送信されたファイルの概要を説明しています。

不審なファイルは分析のために自動的にESET LiveGrid®に送信されますESET LiveGuard Advancedを有効にした場合、分析のために手動で送信されたファイルはESET LiveGuard Advancedにのみ送信されます。ただし、一部の自動的に送信されたファイルはESET LiveGrid®にも送信される場合があります。

また、不審なファイルやサイトを分析のために手動で送信することもできます。手動で送信されたファイルがリストに表示されるには数分かかります。

分析のために送信されたファイルのリストを表示するには、Webインターフェイスにログインし、**送信されたファイル**をクリックします。あるいは、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のいずれかを実行します。

```
/opt/eset/efs/bin/lslog -n
```

または

```
/opt/eset/efs/bin/lslog --sent-files
```

分析に送信されたファイルの一時検出除外を作成する場合は、ファイルをクリックして、パスまたはハッシュをコピーします。

分析のためにサンプルを提出

コンピューター上の疑わしいファイル、またはインターネット上の疑わしいサイト見つかった場合は、ESETのリサーチラボに提出して解析を受けることができます。

> **ESET LiveGrid®フィードバックシステムを有効にする必要があります**
> 1. Webインターフェイスで、**設定** > **検出エンジン** > **クラウドベース保護**をクリックします。
> 2. **ESET LiveGrid®フィードバックシステムを有効**にし、**保存**をクリックします。

分析のためにサンプルを提出する:

1. **ヘルプ** > **送信されたファイル**をクリックしてから、**分析のためにサンプルを提出**をクリックします。
2. **サンプル送信の理由**を選択します。
   - **不審なファイル**: 検査中にファイルを駆除できないファイル、または通常と異なる特性を持つファイル。
   - **不審なサイト**:（マルウェアに感染しているWebサイト）
   - **誤検出サイト** : マルウェアに感染していると誤って特定されたWebサイト
   - **誤検出ファイル**: マルウェアとして誤って特定されたファイル
   - **その他**
3. サイトアドレスまたはファイルパスを追加します。
4. 電子メールアドレスを入力するか、**匿名で送信**を選択します。
5. [**次へ**]をクリックします。
6. 詳細情報を入力します。
7. **送信**をクリックします。

分析のために隔離されたファイルを送信することもできます。

ブロックされたファイル

ESET Server Security for Linux (ESSL)がESET Inspectと統合されている場合、ESET Inspectによってブロックされたファイルは**ブロックされたファイル**に表示されます。

ESSLをESET Inspectと統合するには、ESSLで保護されたコンピューターにESET Inspectコネクターを展開します。

ESET Inspectコネクターは自動的にESSLとの通信を開始します。

フィルタリングされたWebサイト

フィルタリングされたWebサイトセクションには、URLアドレスリストで定義された条件に一致するURLへのアクセス試行が表示されます。検出のリストが表示されます。

- 検出日時
- トリガーされた検出のオブジェクトURI
- アイテムが検出された理由
- 検出をトリガーしたアプリのパス
- 検出をトリガーしたユーザー
- 検出をトリガーしたIPアドレス
- 検出によって実行されたアクション
- 検出をトリガーしたリストの重大度

次の条件が満たされた場合、検出リストが表示されます。

- Webアクセス保護が有効になっています
- URLリスト管理からのリストがアクティブである
- リストのログの重大度が**なし**に設定されていない
- リストにURIアドレスが含まれている(*などのワイルドカードを使用できます)
- Webサイトはサーバーからアクセスされる(たとえば、wgetまたはWebブラウザー経由)

検出をクリックして、使用可能なアクションを表示します。

- **アプリケーションのコピー** – アプリのパスをクリップボードにコピーします。
- **URIのコピー** - URIアドレスをクリップボードにコピーします。
- **IPのコピー** - IPv4またはIPv6アドレスをクリップボードにコピーします。
- **除外の作成**—除外条件に基づいて除外を作成します。**IPアドレス**は、検出をトリガーした除外されたIPアドレスのリストにIPアドレスを追加します。**アプリケーション**は、検出をトリガーした除外されたアプリケーションのリストにアプリのパスを追加します。

URLリストの変更

- **許可されたURLリストに追加**—URIアドレスを許可されたアドレスの有効なリストに追加しますURIアドレスが既に許可されたアドレスの有効なリストに追加されている場合は、このオプションは使用できません。
- **許可されたURLリストから削除**—URIアドレスを許可されたアドレスの有効なリストから削除します。このオプションは、許可されたアドレスのアクティブなリストにURIアドレスが含まれていない場合、またはURIアドレスにワイルドカードが含まれている場合は使用できません。
- **ブロックされたURLリストから削除**—URIアドレスをブロックされたアドレスの有効なリストから削除します。このオプションは、ブロックされたアドレスのアクティブなリストにURIアドレスが含まれていない場合、またはURIアドレスにワイルドカードが含まれている場合は使用できません。

ネットワーク保護

ネットワーク保護セクションには、ネットワーク攻撃から保護されたトラフィックが表示されます。現在、ボットネット保護のみがサポートされています。

設定

ESET Server Security for Linuxの既定の設定を変更するには、**設定**画面に移動します。検出動作を調整したり、製品のアップデートおよび接続設定を変更したり、Webインターフェイスのパスワードと証明書を変更したりすることができます。変更を適用するには、**設定**画面で**保存**をクリックします。

要件に従ってESET Server Security for Linuxを設定し、後から使用するために設定を保存する場合(またはESET Server Security for Linuxの別のインスタンスで使用する場合)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/efs/sbin/cfg --export-xml=/tmp/export.xml
```

設定のインポート

```
/opt/eset/efs/sbin/cfg --import-xml=/tmp/export.xml
```

使用可能なオプション

短縮型	標準型	説明
	`--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
  - o検出除外
- クラウドベース保護
- マルウェア検査
- リモート検査(ICAP検査)

除外

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、オンデマンド検査、リモート検査で設定できます。

1. Webインターフェイスで、**設定**をクリックします。
2. 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**をクリックして、リアルタイムファイルシステム保護に関連する除外を変更します。
   - **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**をクリックして、オンデマンド検査(カスタム検査)に関連する除外を変更します。
   - **検出エンジン > リモート検査 > Threatsenseパラメーター**を使用して、リモート検査に関連する除外を変更します。
3. **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。
4. **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。
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. **保存**をクリックして、変更を保存します。

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. Webインターフェイスで、**設定 > 検出エンジン**をクリックします。
2. **パフォーマンスの除外**の横にある**編集**をクリックします。
3. **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。
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. **保存**をクリックして、変更を保存します。

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

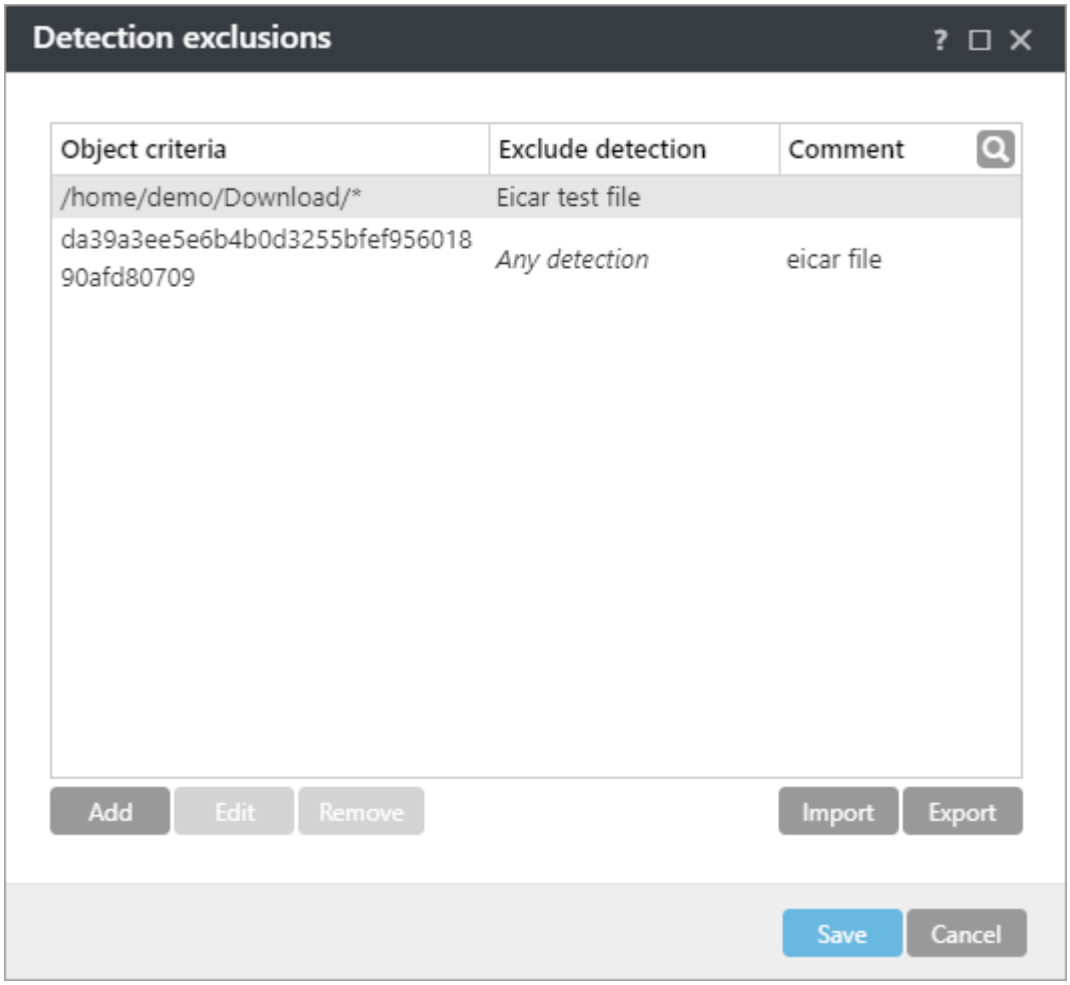
システムインフラストラクチャの要件がある場合以外は、パスの中央でワイルドカードを使用しないことをお勧めします(例: */home/user/*/data/file.dat*)。詳細については、次のナレッジベース記事を参照してください。
検出除外を使用するときには、パスの中央でワイルドカードを使用することに関する制限はありません。

検出除外

検出除外では、検出名、オブジェクトパス、またはハッシュをフィルタリングして、オブジェクトを駆除(削除または隔離への移動)から除外できます。

検出除外の仕組み

検出除外は、**パフォーマンス除外**と違い、ファイルとフォルダーを検査から除外しません。検出除外は、検出エンジンで検出され、適切なルールが除外リストにあるときにのみ、オブジェクトが隔離または削除されないように、除外します。
以下の図のサンプルルールを参照してください。最初の行のルールは、*Eicar test file*として検出され、*/home/demo/Download/some.file*にあるオブジェクトを除外します。2行目のルールは、検出名に関係なく、対応するSHA-1ハッシュを持つ検出されたすべてのオブジェクトを除外します。



検出除外オブジェクト条件

- **パス** – 指定されたパス(または空の場合はすべてのパス)の検出除外
- **検出名** – 検出されたオブジェクトは、定義済みの検出名と一致する場合に除外されます。ファイ

ルが後で他のマルウェアに感染した場合、検出名が変更されます。このような場合、そのファイルは侵入として検出され、適切なアクションが実行されます。**パス**が定義されている場合、そのパスにあり、**検出名**と一致するファイルのみが検出から除外されます。このような検出を除外リストに追加するには、検出除外ウィザードを使用します。あるいは、**隔離**に移動し、隔離されたファイルをクリックして、**復元して除外**を選択します。このオプションは、検出エンジンによって検出対象として評価された項目でのみ表示されます。

- **ハッシュ** – ファイルタイプ、場所、名前、拡張子に関係なく、指定されたハッシュ(SHA1またはSHA256)に基づいて、ファイルを除外します

検出除外の追加または編集

検出除外を手動で定義

1. **設定** > **検出エンジン**をクリックします。

2. **検出除外**の横の**編集**をクリックし、**追加**をクリックします。

3. 除外条件を定義します。

- **パス** – 指定されたパス(または空の場合はすべてのパス)の検出除外

- **検出名** – 検出されたオブジェクトは、定義済みの検出名と一致する場合に除外されます。ファイルが後で他のマルウェアに感染した場合、検出名が変更されます。このような場合、そのファイルは侵入として検出され、適切なアクションが実行されます。**パス**が定義されている場合、そのパスにあり、**検出名**と一致するファイルのみが検出から除外されます。このような検出を除外リストに追加するには、検出除外ウィザードを使用します。あるいは、**隔離**に移動し、隔離されたファイルをクリックして、**復元して除外**を選択します。このオプションは、検出エンジンによって検出対象として評価された項目でのみ表示されます。

- **ハッシュ** – ファイルタイプ、場所、名前、拡張子に関係なく、指定されたハッシュ(SHA1またはSHA256)に基づいて、ファイルを除外します

4. **OK**をクリックしてから、**保存**をクリックします。

5. **設定**画面で**保存**をクリックします。

検出除外ウィザードの使用

1. 検出を選択して、**除外の作成**を選択します。

2. 適切な除外条件を選択します。

   - **正確なファイル** – SHA-1ハッシュでファイルを除外

   - **検出** –検出名でファイルを除外

   - **パス + 検出** – パスと検出名に一致するファイルを除外

3. 必要に応じてコメントを入力します。**設定** > **検出エンジン**に検出除外の一覧が表示されます。**検出除外**の横の**編集**をクリックします。

4. **除外の作成**をクリックします。

検出除外を編集または削除する

1. **設定** > **検出エンジン**をクリックします。
2. **検出除外**の横の**編集**をクリックします。
3. 除外を選択し、**編集**または**削除**をクリックします。
4. 変更を保存します。

検出除外のエクスポート/インポート

設定された検出除外をリモートで管理されていない別のESET Server Security for Linuxインスタンスと共有するには、設定をエクスポートします。

1. **設定** > **検出エンジン**をクリックします。
2. **検出除外**の横の**編集**をクリックし、**エクスポート**をクリックします。
3. **エクスポートされたデータのダウンロード**の横のダウンロードアイコン  をクリックします。
4. ブラウザーでファイルを開くまたは保存するように指示された場合は、**保存**を選択します。

エクスポートされた検出除外ファイルをインポートする:

1. **設定** > **検出エンジン**をクリックします。
2. **検出除外**の横の**編集**をクリックし、**インポート**をクリックします。
3. 参照アイコン  をクリックして、エクスポートされたファイルを参照し、**開く**をクリックします。
4. **インポート** > **OK** > **保存**をクリックします。
5. **設定**画面で**保存**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。

既定ではESET Server Security for Linux(ESSL)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。

設定 > **検出エンジン** > **クラウドベース保護**で設定を変更します。

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。

ESET LiveGuard Advancedを有効にする

ESET Server Security for Linuxバージョン8.1から利用可能です。データはESET LiveGuard Advanced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。

- すべての検出されたサンプル
- 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 – すべてのPE形式ファイル(例: *.exe, .dll, .sys*)とELF ファイル(例: *.axf, .bin, .elf*)が含まれますxフラグ(実行ファイル)のテキストファイルも含めます
- 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, .sh, .py, .pl*

• 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 Office、Libre 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 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。

サービス名の変更

2022年3月23日、ESET Dynamic Threat Defenseのブランド名称がESET LiveGuard Advancedに変更されました。ESETビジネス製品では、ESET LiveGuardとしても表示されます。いずれの名前も同じサービスを参照します。

> **使用可否**
> ESET Server Security 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。使用する前にESET LiveGuard Advancedをアクティベーションします。
> 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。

ESSL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/efs/sbin/cloud -l
```

または

```
/opt/eset/efs/sbin/cloud --liveguard-status
```

ESSLでサービスを有効にするには

1. ESET LiveGuard Advancedをアクティベーションします。
2. Webインターフェイスで、**設定 > 検出エンジン > クラウドベース保護**をクリックします。
3. **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**を有効にしてから、**ESET LiveGuardを有効にする**を有効にします。

4. 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。

5. **[保存]をクリックします**。

ESET PROTECTを使用してリモートでESET LiveGuard Advancedを有効にする手順

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 Server/File Security 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**を有効にしてから、**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. **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。

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、スケジュールされている停止、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。

監視チームは潜在的な問題を内部で検証し、確認されたインシデントは手動で投稿および更新して、高い信頼性と正確性を維持します。そのため、ステータスポータルには若干遅れて表示されます。期間の短いインシデントは、手動で確認される前に解決された場合、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。既定では、**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設定が**検出対応**セクションから継承されます。

リモート検査(ICAP検査)

外部ICAP対応デバイス/ソフトウェアをリモートで保護するには、**リモート検査**を有効にして設定します。

1. Webインターフェイスで、**設定** > **検出エンジン** > **リモート検査**に移動します。
2. **ICAPサービスを使用してリモート検査を有効にする**の横のトグルキーをオンにします。
3. **リスニングアドレスとポート**の横の**編集**をクリックし、**追加**をクリックしてICAPサーバーのアドレスとポートを定義します。**OK**をクリックしてから、**保存**をクリックします。
4. 任意で、ThreatSenseパラメーターを確認して調整します。
5. [**保存**]をクリックします

ICAPサーバーとEMC Isilonとの統合方法を参照してください

サポートされているICAPクライアント

- Dell EMC Isilon
- Citrix ShareFile
- EFT Enterprise
- Nutanix

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 Server Security 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。**ステータス概要** > **モジュールのアップデート** > **モジュールロールバック**をクリックし、任意の期間を選択して、**今すぐロールバック**をクリックします。

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

バージョン9. 1以降では、既定でESET Server Security for Linux (ESSL)の自動製品アップデートが有効です。この設定を有効にして、新しいアップデートが利用可能になるときにESSLで最新の製品アップデートがが必ず適用されるようにすることをお勧めします。

バージョン9.0以前で、自動更新を有効にするには、**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。

自動アップデート(バージョン9.1以降)

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。

アップデートモード(バージョン9.0以前)

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**ステータス概要**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ESSL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で、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。しかし、追加の望ましくない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可能性があります。
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。

- **疑わしいアプリケーション** - 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出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** – 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があるアプリケーション(PUA)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、環境や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、または削除に影響しません。

攻撃的	報告は最大感度に設定されています。より多くの検出が報告されます。**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。

攻撃的	報告されたアグレッシブ(以下)レベルの検出はブロックされ、自動修正(駆除)が開始します。すべてのエンドポイントがアグレッシブ設定で検査され、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。

ローカルでマウントされたNFS共有フォルダーのリモートアクセス中の検査はサポートされていません

ESET Server Security for Linux (ESSL)で保護されているコンピューターにNFSカーネルサーバーがインストールされているとします。共有フォルダーがリモートコンピューターにローカルでマウントされ、ESSLで保護されていない場合、ESSLのオンアクセススキャナーは動作しません。

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. **設定** > **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。
2. **リアルタイムファイルシステム保護**を無効にします。

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、すべての種類のメディアをチェックし、ファイルへのアクセスなどのさまざまなシステムイベントによってトリガーされます。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、

1. Webインターフェイスで**設定** > **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。

2. **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。

3. [**保存**]をクリックします。

除外を処理する

プロセス除外機能では、アプリケーションプロセスをリアルタイムファイルシステム保護から除外できます。

バックアップソリューションは、速度、プロセス整合性、およびサービスの可用性を改善することに努めています。そのために、通常、ファイルレベルのマルウェア保護と競合すると認識されている手法を使用しています。同様の問題は、仮想マシンのライブ移行を完了しようとするときにも発生する可能性があります。通常、このような状況を回避する唯一の効果的な方法は、マルウェア対策ソフトウェアを無効にすることです。

特定のプロセス(バックアップソリューションのプロセスなど)を除外することで、このような除外されたプロセスに関連するすべてのファイル処理が無視され、安全であると見なされます。これにより、バックアッププロセスへの妨害が最小限に抑えられます。除外を作成するときには十分に注意することをお勧めします。除外されたバックアップツールは警告を発行せずに感染したファイルにアクセスすることができます。このため、リアルタイムファイルシステム保護モジュールでアクセス権の拡大が許可されてしまいます。

この機能は、バックアップツールを除外することを目的としています。バックアップツールの検査プロセスを除外すると、システムの安定性が保証されます。またバックアップの実行中に速度が低下しないため、バックアップのパフォーマンスに影響しません。最終的に、競合の可能性のリスクが最小限に抑えられます。

除外されたプロセスのリストにバイナリを追加する

1. **設定** > **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。

2. **リアルタイムファイルシステム保護** > **プロセス除外**セクションで、**検査から除外するプロセス**の横の**編集**をクリックします。

3. [**追加**]をクリックします。

4. バイナリの絶対パスを入力します。

5. **保存**を2回クリックします。

6. **設定**画面で**保存**をクリックします。

バイナリが除外に追加され次第、ESET Server Security for Linuxはアクティビティの監視を停止します。そのバイナリによって実行されるファイル処理には検査が実行されません。

既存のプロセスを**編集**するか、除外から**削除**することもできます。

検出除外のエクスポート/インポート

設定されたプロセス除外をリモートで管理されていない別のESET Server Security for Linuxインスタンスと共有するには、設定をエクスポートします。

1. **設定** > **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。

2. **リアルタイムファイルシステム保護** > **プロセス除外**セクションで、**検査から除外するプロセス**の横の**編集**をクリックします。

3. [**エクスポート**]をクリックします。

4. **エクスポートされたデータのダウンロード**の横のダウンロードアイコン  をクリックします。

5. ブラウザーでファイルを開くまたは保存するように指示された場合は、**保存**を選択します。

エクスポートされたプロセス除外ファイルをインポートする:

1. **設定** > **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。

2. **リアルタイムファイルシステム保護** > **プロセス除外**セクションで、**検査から除外するプロセス**の横の**編集**をクリックします。

3. **インポート**をクリックしてから、参照アイコン  をクリックして、エクスポートされたファイルを参照し、**開く**をクリックします。

4. **インポート** > **OK** > **保存**をクリックします。

5. **設定**画面で**保存**をクリックします。

ThreatSenseパラメーター

ThreatSenseは、多くの複雑な脅威検出方法で構成されています。 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の排除にも成功しています。

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

設定ウィンドウにアクセスするには、**設定** > **検出エンジン**または**保護**をクリックし、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、ファイル名の一部であり、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

を指定できます。

その他

オンデマンド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修正するには、**既定のアーカイブ検査の設定**をオフにします。

- **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。

駆除レベル

- **駆除なし** – 感染しているファイルは自動的に駆除されません。検出された脅威数は、**発生した検出**列で赤でハイライト表示されます。**駆除**列が赤色でハイライト表示されますが、0が表示されます。
- **標準駆除** – 感染したファイルと未感染のファイルが混在しているアーカイブファイルなど有用なデータの損失を引き起こすものを除き、感染したファイルを自動的に駆除または削除しようとします。このようなアーカイブファイルで検出されたファイル数は、**発生した検出**としてカウントされ、 **駆除**列は赤色でハイライトされます。
- **厳密な駆除** – 全ての感染ファイルが駆除または削除されます。ただし、システムファイルは除きます。
- **厳密駆除** – 例外なく、感染したすべてのファイルを駆除または削除します。
- **削除** – 例外なく、感染したすべてのファイルを削除します。

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検査によって検査され、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。既定では有効になっていますが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。

- OpenVPN
- PulseSecure
- Wireguard
- ProtonVPN

現在Webアクセス保護は、ESET Server Security 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。システムおよび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**アドレスのリストにあるWebサイトは、**許可**アドレスのリストにも登録されていないかぎり、アクセスできません。**検出されたマルウェアが無視される**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されます。

アクティブな**許可された**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は、特殊記号の*（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置き換え、疑問符は任意の記号を置き換えます。

リストには信頼できる安全なアドレスのみを含める必要があるため、除外アドレスを指定する際には注意してください。同様に、このリストでは記号の*と?が正しく使われていることを確認してください。

リストを有効化するには、**リスト有効**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トラフィック検査では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。さまざまな検査モードを使用して、信頼できる証明書、不明な証明書、またはSSLで保護された通信検査から除外された証明書を使用してSSLで保護された通信を検査できます。プログラムは、**HTTPSプロトコルで使用される**ポートで定義されたポート(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

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するために使用します。選択したアプリケーションのHTTP 通信は、脅威の検査を行いません。この手法は、プロトコルフィルタリングを有効にして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. Webインターフェイスで、**設定**をクリックします。
2. **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。
3. **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。
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. **保存**をクリックして、変更を保存します。

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**
> システムインフラストラクチャの要件がある場合以外は、パスの中央でワイルドカードを使用しないことをお勧めします(例: */home/user/*/data/file.dat*)。詳細については、次のナレッジベース記事を参照してください。
> 検出除外を使用するときには、パスの中央でワイルドカードを使用することに関する制限はありません。

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ために使用します。選択したIPアドレスとの間のHTTP通信は、脅威の有無をチェックしません。このオプションは、信頼できることがわかっているアドレスに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. Webインターフェイスで、**設定**をクリックします。
2. **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**をクリックして、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. **保存**をクリックして、変更を保存します。

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。

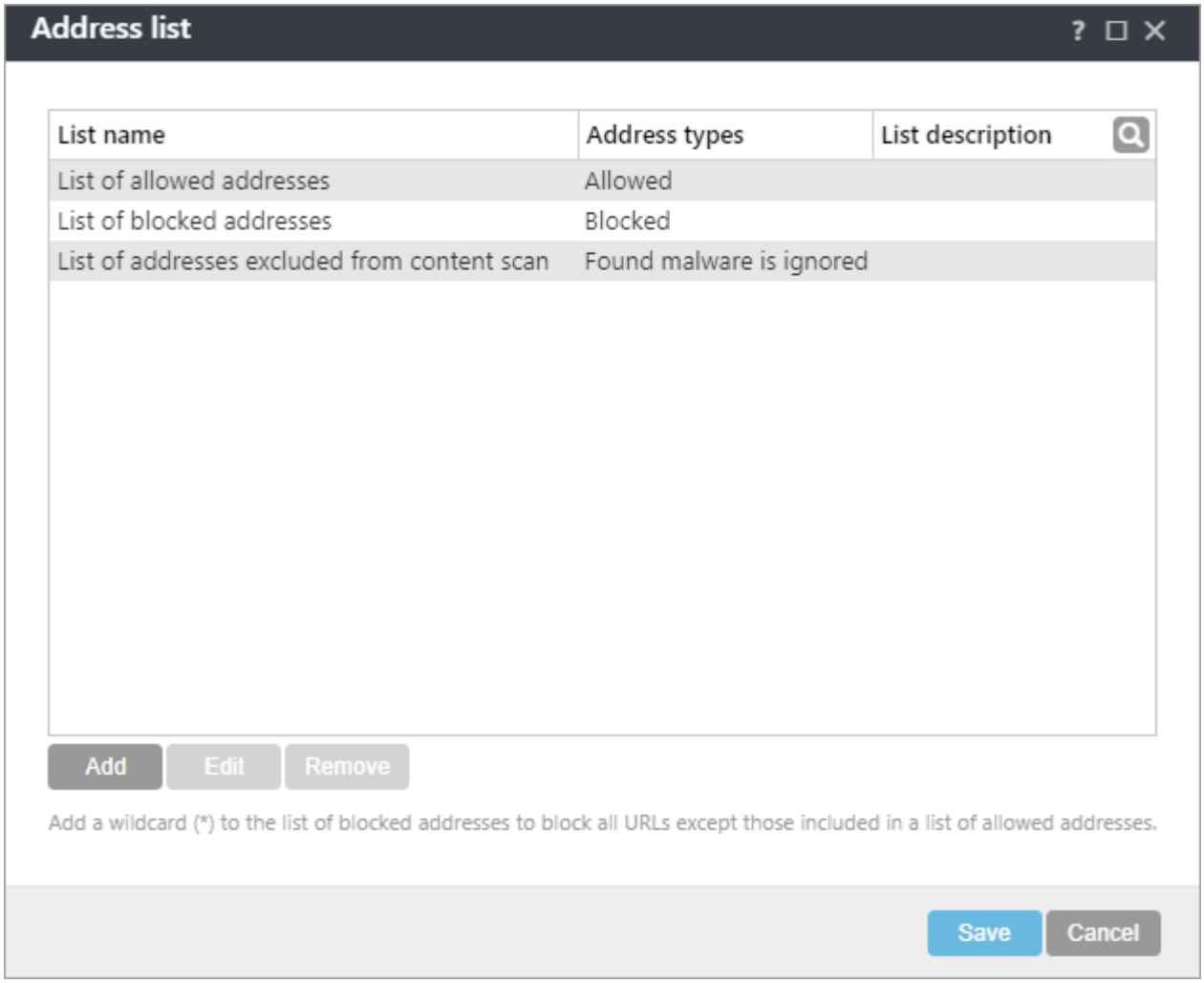
IPv6アドレス:

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。

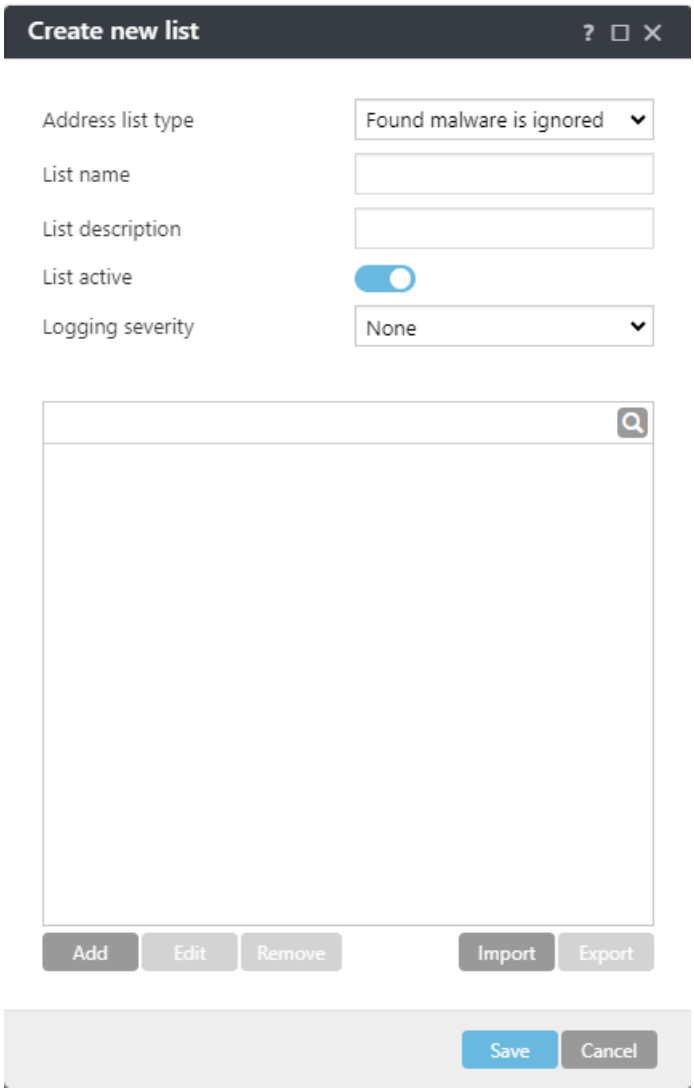
- **ブロックされたアドレスのリスト** – このリストで指定されたアドレスへのアクセスは、アドレスが許可されたアドレスのリストに含まれない限り許可されません。

- **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が許可されます。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。このフィールドは定義済み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。あらかじめ定義されたリストでは、このフィールドを変更できません。

リストアクティブの横のトグルをクリックして、このリストを有効/無効にします。これは、リストを永続的に削除したくない場合に便利です。

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ます。リモートで管理されている場合は、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ます。リモートで管理されている場合は、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、?および*記号が含まれます。

• 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。

ドメイン全体と一致させるには、*.domain.com/*の形式で入力します。マスクで*http://□https://*プレフィックスを指定することは任意です。

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 Server Security for Linux 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。さまざまな検査モードを使用して、信頼できる証明書、不明な証明書、またはSSLで保護された通信検査から除外された証明書を使用して□SSLで保護された通信を検査できます。プログラムは、**HTTPSプロトコルで使用される**ポートで定義されたポート(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 Server Security 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 Server Security 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ビルトインのホワイトリストで決定されます。

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プロトコルで使用されるポート—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カンマで区切ってください。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にはESETのルート証明書を既知のルート証明書(発行元)のリストに追加する必要があります。**ESETルート証明書をサポートされているアプリケーションに統合**を有効にしてください。

サポートされているブラウザーにESETルート証明書を自動的に追加するには、このオプションを選択します。

証明書の有効性

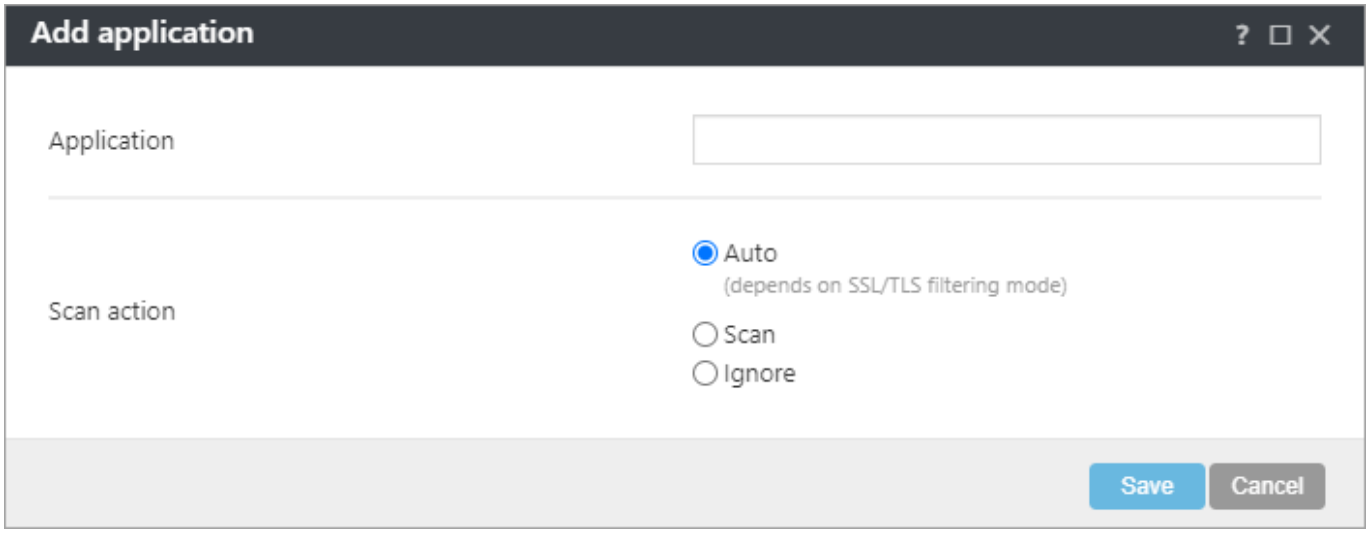
証明書の信頼が確立できない場合—場合によってはTrusted Root Certification Authorities (TRCA)ストアを使用してWebサイト証明書を検証できないことがあります。これは、証明書が他のユーザ(Webサーバーまたは中小企業の管理者)によって自己署名されていて、この証明書を信頼できるとみなしても必ずしもリスクにはならないことを意味します。多くの大企業(銀行など)はTRCAによって署名されている証明書を使用します。**証明書の有効性について確認**が選択されている場合(既定では選択されています)、暗号化された通信が確立されると、ユーザー はアクションを選択するよう指示されます。**証明書を使用する通信をブロック**を選択すると、検証されていない証明書を使用するサイトへの暗号化された接続を常に終了することができます。

証明書が破損している場合—これは、証明書が正しく署名されていないか、破損していることを意味します。この場合、**証明書を使用する通信をブロック**を選択したままにすることをお勧めします。**証明書の有効性について確認**を選択した場合、暗号化通信が確立されたときに実行するアクションを選択するプロンプト が表示されます。

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 Server Security 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**ウィンドウには次の項目が表示されます。



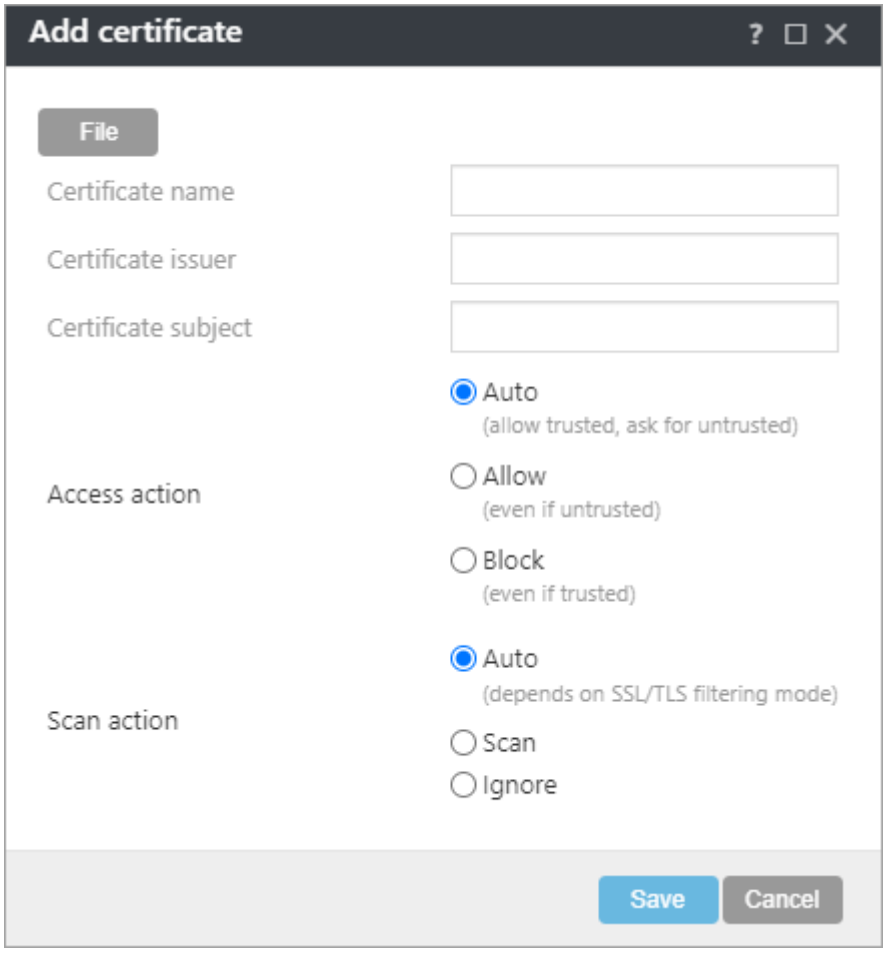
アプリケーション – アプリケーションへの正確なパスを入力します。

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 Server Security for Linux動作をカスタマイズできます。



証明書の追加ウィンドウで、**ファイル**をクリックし、証明書ファイルを指定するか、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 Server Security 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、用語集をお読みください。

ツール

ESET Server Security for LinuxWebインターフェイスの**設定 > ツール**セクションで、ESET Server Security for Linuxの一般設定を修正できます。

- 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
- Webインターフェイスのパスワード/証明書を変更する
- ログファイルの処理方法を設定する
- ウォッチドッグサービスの有効化/無効化

オンデマンド検査をスケジュールすることもできます。

ウォッチドッグ

ウォッチドッグサービスは検査デーモンのステータスを確認し続けます。サービスが有効な場合、**オンデマンド検査**と**リアルタイム検査**タイルの**ステータス概要**に検査サービスのステータスが表示されます。

ウォッチドッグサービスが無効な場合、**オンデマンド検査**タイルは**ステータス概要**で非表示になります。

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 Server Security for Linuxを設定します。パラメーターを調整するには、**設定 > ツール > プロキシサーバー**をクリックします。

Webインタフェース

ESET Server Security for Linux WebインターフェイスのIPアドレスとポートを変更するかWebインターフェイスが使用可能である別のアドレスを追加するには、**リスニングアドレスとポート**の横の**編集**をクリックします。**追加**をクリックし、適切なアドレスとポートを入力し、**OK**をクリックしてから、**保存**をクリックします。**設定**画面で**保存**をクリックします。

新しい証明書と対応する秘密鍵をインポートするには、**証明書**および**秘密鍵**ボタンを使用します。証明書がパスワードで保護されている場合は、**証明書パスワード**フィールドにパスワードを入力します。**設定**画面で**保存**をクリックします。

Webインターフェイスを無効にして有効にする

Webインターフェイスを有効にするの横にあるトグルを切り替え、設定画面で**保存**をクリックすると、ただちにWebインターフェイスからログアウトし、Webインターフェイスを使用できなくなります。

ターミナルウィンドウからもう一度Webインターフェイスを有効にすることができます。

ESET PROTECTを使用してリモートでESET Server Security for Linuxのインストールを実行した場合は、Webインターフェイスが有効になりません。
特定のコンピューターでWebインターフェイスにアクセスする場合は、ターミナルウィンドウから次のコマンドを実行します。

```
sudo /opt/eset/efs/sbin/setgui -gre
```

最終出力は、WebインターフェイスのURLアドレスとアクセス資格情報を示します。
10.1.184.230:9999などのカスタムIPアドレスとポートでWebインターフェイスを使用可能にする場合は、ターミナルウィンドウから次のコマンドを実行します。

```
sudo /opt/eset/efs/sbin/setgui -i 10.1.184.230:9999
```

ESET PROTECT経由でWebインターフェースを有効にするには、コマンドの実行タスクを使用して、次のコマンドを実行します。

```
/opt/eset/efs/sbin/setgui -re --password=<password>
```

<password>はユーザーが定義した任意のパスワードを表します。

setguiコマンドの使用可能なオプション

オプション – 短縮型	オプション – 標準型	説明
-g	--gen-password	Webインターフェイスにアクセスするための新しいパスワードを生成します
-p	--password=パスワード	Webインターフェイスにアクセスするための新しいパスワードを定義します
-f	--passfile=ファイル	Webインターフェイスにアクセスするために、ファイルから読み込まれた新しいパスワードを設定します
-r	--gen-cert	新しい秘密鍵と証明書を生成します
-a	--cert-password=パスワード	証明書パスワードを設定します
-l	--cert-passfile=ファイル	ファイルから読み込まれた証明書パスワードを設定します
-i	--ip-address=IP:PORT	サーバーアドレス(IPとポート番号)
-c	--cert=ファイル	証明書のインポート
-k	--key=ファイル	秘密鍵をインポートします
-d	--disable	Webインターフェイスを無効にします
-e	--enable	Webインターフェイスを有効にします

リスニングアドレスとポート

ESET Server Security for Linuxでは、Webインターフェイスと ICAPサーバーの両方でカスタムIPアドレスとポートを設定できます。

ログファイル

ESET Server Security 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 Server Security 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**イベント**>**検出**、または**送信されたファイル**画面またはログリスト(`lslog`)で非表示にする:

1. **次の日数が経過したエントリを自動的に削除する**をオンにします。
2. 非表示にするファイルの年齢を指定する日を調整します。
3. **[保存]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**使用されていないレコードの割合(%)が次の値よりも大きく場合**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。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)は、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、まだログのフィルタリングで使用できます。

スケジューラ

ESET Server Security for Linuxバージョン8以降では、定義された曜日と時間に、定期的な毎週のカスタム検査を実行できます。

検査のスケジュール設定

1. Webインターフェイスで、**設定** > **ツール** > **スケジューラ**をクリックします。
2. **タスク**の横の**編集**をクリックします。
3. [**追加**]をクリックします。
4. スケジュールに名前を付け、時刻を設定し、カスタム検査が自動的にトリガーされる曜日を選択します。**次へ**をクリックします。
5. 検査プロファイルを選択します。
6. **検査対象**または定義されたカスタム対象を改行で区切って選択します。
7. 使用可能な**オプション**(検査して駆除 検査除外)を選択/選択解除します。
8. **完了**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。
9. **保存**をクリックして、すべての変更を保存します。

スケジュールされたタスクを変更するには、上記の手順3で特定のタスクを選択し、**編集**をクリックします。残りの手順を続行します。

スケジュールされたタスクを削除するには、上記の手順3で特定のタスクを選択し、**削除**をクリックします。手順8とに進みます。

> **スケジュールされたタスクの実行**
> スケジューラはcronを使用し、該当するコンピューターが実行されている場合に実行されます。コンピューターがオフの場合、タスクは、コンピューターがオンになっている次回のスケジュールされた時刻に実行されます。

ユーザーインタフェース

ステータス概要に表示される通知を設定するには

1. Webインターフェースで**設定** > **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**をクリックします。
2. **保護の状態に表示**の横の**編集**をクリックします。
3. 該当する状態を選択します。
4. **OK**をクリックしてから、**保存**をクリックします。

> 選択されていない状態はステータス概要でミュートされています。すべての変更はローカルでのみ適用されます。

リモートでESET Server Security for Linuxを管理する場合は、ESET PROTECTに状態を表示を参照してください。

ステータス

関連するモジュールが無効になっているか、機能しないか、見つからない場合、**ステータス概要**には、**設定 > 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 > 保護の状態に表示する > 編集**で選択した各状態の通知が表示されます。

> 選択されていない状態はステータス概要でミュートされています。すべての変更はローカルでのみ適用されます。

ESET PROTECTでステータスを表示する

ESET Server Security for Linuxをリモートで管理するときにESET PROTECTに状態を表示する:

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 Server/File Security for Linux (V7+)**を選択します。
3. **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**をクリックします。
4. **ESET管理コンソールに送信**の横の**編集**をクリックします。
5. 該当する状態を選択し、**OK**をクリックします。
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。

リモート管理

ESET Server Security for Linuxをリモートで管理するにはESETセキュリティ製品をホストするコンピューターをESET PROTECTに接続します。

1. ESET Management Agentを展開します
2. コンピューターをに追加ESET PROTECTします。

以降は、ESET Server Security for Linuxに関する該当するクライアントタスクを実行できます。

ESSLバージョン8.1以降では、ポリシーのローカルリストとリモートリストのマージをサポートしています。

コンテナーセキュリティ

多くの場合Linuxサーバーは、Dockerコンテナーと Dockerツールを実行するための基本です。コンテナーセキュリティ機能は、ESET Server Security for Linux (ESSL)のリアルタイムファイルシステム保護の一部で

す。

ESSLは、コンテナーの脅威または不審なアクティビティを検出し、ブロックできますが、排除することはできません。つまり、不審なスクリプトの実行はブロックされますが、削除されません。このようなスクリプトは手動で削除できます。

ESETのリアルタイムファイルシステム保護は次のフェーズでコンテナーを検査できます。

- コンテナイメージの作成プロセス
- ESSLで保護されたコンピューターにコンテナーイメージを展開する

コンテナー内のアクティビティもリアルタイムで不審な動作の検査が行われます。

ESETはDockerCE (Community Edition)バージョン20. 10. 7をテストしました。

使用例

この章ではESET Server Security for Linuxの一般的な使用例について説明します。

- stunnel TLSプロキシを使用したセキュリティで保護されたICAP
- ICAPサーバーとEMC Isilonとの統合
- モジュール情報の取得
- 検査のスケジュール

stunnel TLSプロキシを使用したセキュリティで保護されたICAP

stunnelサービスを使用してICAP検査の暗号化された接続を管理し、セキュリティを強化できます。

1. ESET Server Security for Linuxをインストールして、アクティベーションします。
2. ICAP検査を有効にするには、**設定 > 検出エンジン > リモート検査 > ICAPサービスを使用してリモート検査を有効にする**の横のトグルをクリックします。
3. パッケージマネージャーでstunnelをインストールしますUbuntu 20.04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。

```
sudo apt install stunnel
```

4. stunnelによる通信を暗号化するための秘密鍵と公開鍵を、アクセスが制限されたファイルに格納します。この証明書は、このセキュリティで保護された接続を使用してESSLに接続するICAPクライアントによって信頼される必要があります。キ鍵を保存してアクセス許可を設定する方法の例:

```
sudo cat private_key.pem ca_key.pem >> /etc/pki/tls/private/stunnel.pem
```

```
sudo chmod 400 /etc/pki/tls/private/stunnel.pem
```

5. root (chmod 0600)だけが読み取り可能な、次の行を含む設定ファイル*/etc/stunnel/stunnel.conf*を作成します。

```
[efs_icap]

accept = 0.0.0.0:11344

connect = 0.0.0.0:1344

cert = /etc/pki/tls/private/stunnel.pem
```

- **efs_icap** – 次の行で設定するサービス名。Stunnelは次の複数の接続をサポートします。
- **accept**—ICAPS接続を許可するIPアドレスとポート。この例ではlocalhostとポート11344です。
- **connect**—ESSLがICAP要求を待機するIPアドレスとポート。この例では、同じコンピューターと既定のポート1344です。

> Stunnelは専用サーバーで実行できchrootを使用してESSL複数のコンピューターに接続したりchrootでサンドボックス化したりすることもできます。すべてのstunnelオプションについては、マニュアルを参照してください。

6. systemdによってstunnelを起動し、システム起動後に自動的に実行できるようにします。

```
sudo systemctl start stunnel

sudo systemctl enable stunnel
```

7. ファイアウォールでICAPSポートのポートを開きますUbuntu 20.04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。

```
sudo ufw allow 11344/tcp
sudo ufw reload
```

8. ガイドに従ってICAPクライアント(ストレージなど)を設定し、ESSLがstunnelで実行され、使用されている証明書を信頼するポート11344に接続します。その後、eicarサンプルなどのウイルス対策接続が動作するかどうかをテストします。

ICAPサーバーとEMC Isilonとの統合

概要

Internet Content Adaptation Protocol (ICAP)経由でESET Server Security for Linux (ESSL)を統合するとIsilonクラスタに保存したファイルのコンピューターウイルス、マルウェア、およびその他のセキュリティ脅威を検査できます。

前提条件

1. ESSLがインストールされ、Webインターフェイスが有効になっていること。
2. Isilonがインストールされていること。

ESSLでICAPサーバーを有効にする

この例ではICAPサーバーはIPアドレス10.1.169.28、ポート1344でリスニングします。

1. **設定** > **検出エンジン** > **リモート検査**をクリックし、**ICAPサーバーを使用したリモート検査を有効にする**と**Dell EMC Isilon互換**の両方をオンにします。
2. **リスニングアドレスとポート**の横の**編集**をクリックします。
3. [**追加**]をクリックします。
4. 該当するIPアドレスとポートを入力します。この例ではIPアドレス10.1.168.28、ポート1344です。
5. **[保存]をクリックします**。

OneFSでICAPサーバーを有効にする

1. OneFS管理パネルにログインし、**データ保護** > **ウイルス対策** > **ICAPサーバー** > **ICAPサーバーの追加**をクリックします。
2. [ICAPサーバーを有効にする]を選択し、次のパターンでICAPサーバーのURLアドレスを**ICAPサーバURL**フィールドに入力します。`icap://<IP_ADDRESS>:<PORT>/scan`
   例: `icap://10.1.168.28:1344/scan`
3. **サーバーの追加**をクリックします。
4. **設定**をクリックし、**ウイルス対策サービスを有効にする**を選択します。
5. 検査するパスを**パスプレフィックス**に入力します。すべてのパスを検査するには、`/ifs`と入力します(引用符なし)。
6. **変更の保存**をクリックします。

EMC Isilonでの検査関連の設定

- ファイルサイズ、ファイル名、またはファイル拡張子制限
- アクセス中の検査またはポリシーによるオンデマンド検査
- 脅威対応設定

仕組み

ファイルがEMC Isilonクラスタに書き込まれる(またはアクセスされる)ときにOneFSが検査対象のファイルを照会し、そのファイルをOneFSとESSLの両方で設定されたICAPサーバーに送信しますESSLはファイルを検査し、検査されたファイルに対するフィードバックをEMC Isilonに提供しますOneFSは、脅威対応

設定に基づいて、検査されたファイルを処理する方法を決定します。

設定のテスト

設定をテストするには、サポートされているプロトコル経由で、コンピューターからOneFSクラスタにアクセスする必要があります。この例ではNFSプロトコルを使用します。

1. NFSの設定:

   a.OneFS管理パネルにログインし、**プロトコル > UNIX共有(NFS) > エクスポートの作成**をクリックします。

   b.既定の設定を使用します。パスが`/ifs`であることを確認し、**保存**をクリックします。

2. LinuxコンピューターでNFS共有をマウントする:

```
mkdir isilon

sudo mount -t nfs <IP address of OneFS cluster>:/ifs isilon
```

3. テスト検査を完了します。

   a.www.eicar.orgからeicarウイルス対策テストファイルを取得し、IsilonのNFS共有にコピーして、その内容を読み取ろうとします。

```
wget www.eicar.org/download/eicar.com

cp eicar.com isilon

cat isilon/eicar.com
```

   b.OneFSウイルス対策設定に基づいて、結果はそのファイルでアクセス権が拒否される(既定)か、ファイルが切り捨てられ、削除されます。例:

```
cat: isilon/eicar.com:権限が拒否されました
```

   c.検出された脅威を確認するにはOneFS管理パネルにログインし、**データ保護 > ウイルス対策**をクリックします。

一般的なICAP応答コード

終了コード	意味
100	ICAPプレビューの後で続行します。

終了コード	意味
101	プロトコルをクライアントが要求したプロトコルに切り替える準備ができました。
200	要求は成功しました。返される情報は、メソッドによって異なります。
201	作成されました。新しいリソースが作成されます。URIは本文で指定されます。
202	許可されます。要求は許可されますが、処理は完了していません。
204	変更は必要ありません。
400	正しくない要求。
404	ICAPサービスが見つかりません。
405	サービスで許可されていないメソッド(例えば、REQMODのみをサポートするサービスに対してRESPMODが要求されました)。
408	要求のタイムアウト。ICAPサーバーがICAPクライアントからの要求の待機を停止しました。
500	サーバーエラー。ICAPサーバーのエラー(「ディスク容量不足」など)。
501	メソッドが実装されていません。OPTIONSの実装は必須であるため、この応答はOPTIONS要求に対しては無効です。
502	ゲートウェイが正しくありません。これはICAPプロキシであり、プロキシでエラーが発生しました。
503	サービスが過負荷になっています。ICAPサーバーは、このサービスに関連付けられている最大接続制限を超えました。ICAPクライアントは、今後この制限を超えないようにする必要があります。
505	ICAPバージョンがサーバーでサポートされていません。

モジュール情報の取得

ターミナルウィンドウで`upd`パラメーターを指定して`-l`ユーティリティを使用し、すべてのモジュールとそのバージョンを一覧表示します。

```
/opt/eset/efs/bin/upd -l
```

検査のスケジュール

ESET Server Security for Linux v8にはビルトインのスケジューラがあり、定義した日時に定期カスタム検査を実行できます。ビルトインのスケジューラを使用せずに定期カスタム検査を設定するには、次の手順に従います。

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cron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/efs/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/efs/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。

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 Server Security 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 Server Security 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/efs/lib
```

キャッシュディレクトリ

ESET Server Security 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/efs/cache
```

バイナリファイルディレクトリ

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

```
/opt/eset/efs/bin
```

次のユーティリティがあります。

- lslog — ESET Server Security for Linuxで収集したログ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 Server Security 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/efs/sbin
```

次のユーティリティがあります。

- cfg— ESET Server Security for Linux設定のインポート/エクスポートで使用します。
- cloud— ESET LiveGuard Advanced状態を確認するために使用します。
- 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。
- lic — 購入した製品認証キーでESET Server Security 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。
- setgui — ESET Server Security for Linux Webインターフェイスを有効/無効にし、関連する処理を管理するために使用します。
- startd — 停止した場合ESET Server Security for Linuxデーモンを手動で開始するために使用します。

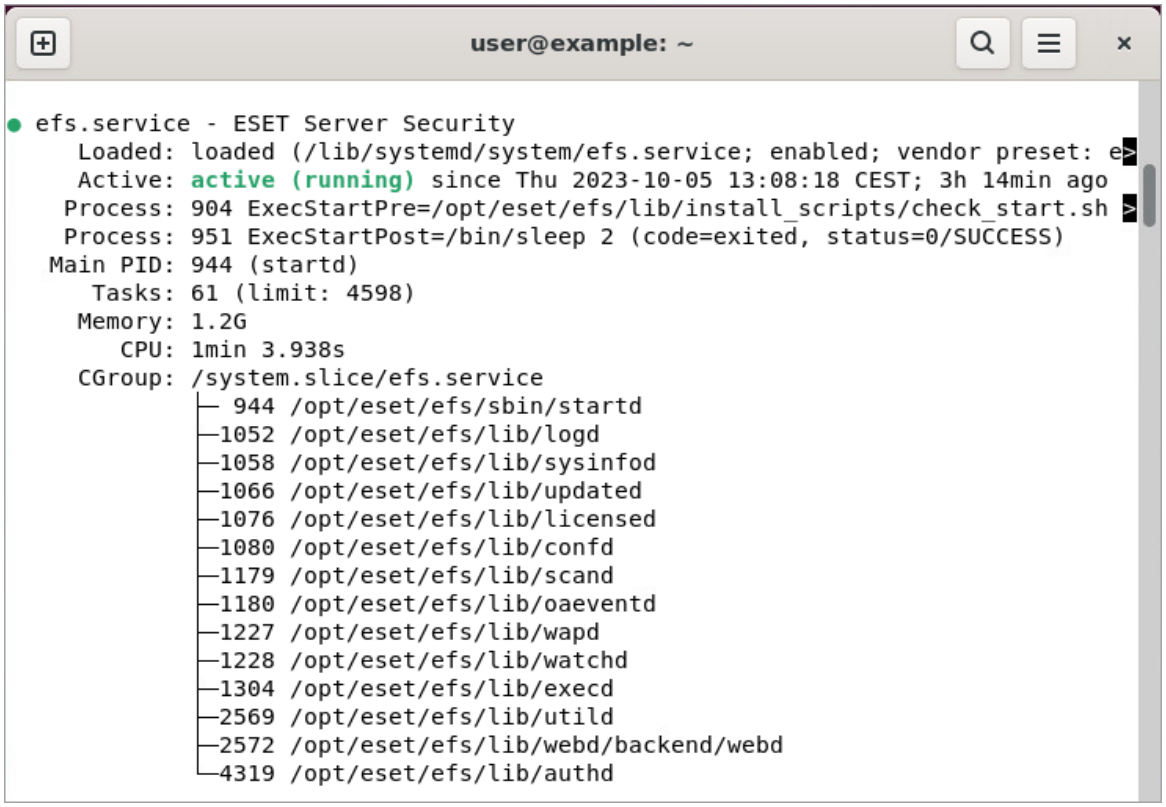
ESET Server Security for Linuxサービスがアクティブであるかどうかを確認するには、ルート権限で、ターミナルウィンドウから次のコマンドを実行します。

```
systemctl status efs.service
```

または

```
/etc/init.d/efs status
```

`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+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/icapd – NASTY検査用のICAPサービス

- lib/webd – httpsサーバーおよびWebインターフェイス
- 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

- bin/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
- sbin/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
- sbin/setgui – 基本Webインターフェイス設定
- sbin/collect_logs.sh – ESETカスタマーサポートから要求された場合にアーカイブファイルとして重要なログを生成するスクリプトです

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
- パスワードを忘れた場合
- アップデート失敗
- noexecフラグの使用
- リアルタイム保護を開始できない
- 起動時にリアルタイムファイルシステム保護を無効にする
- SMBプロトコル用の古いcurlライブラリ
- カスタムTMPDIR
- NFSマウントが失敗する
- WireGuardとWebアクセス保護の使用
- Webアクセス保護とiptables

ログの収集

ESETテクニカルサポートがESET Server Security for Linuxのログを要求する場合は、*collect_logs.sh*にある/opt/eset/efs/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/efs/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。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行うためにESETテクニカルサポートが関連するログの提出を求める場合があります。

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/efs/sbin/ecp_logging.sh -e
```

または

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

または

```
sudo /opt/eset/efs/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。

パスワードを忘れた場合

WebインターフェイスのパスワードをリセットするにはESET Server Security for Linuxがインストールされているコンピューターでターミナルウィンドウを開きます。

- 新しいパスワードを生成するには、ルート権限で次のコマンドを実行します。
  `/opt/eset/efs/sbin/setgui -g`
- 新しいパスワードを定義するには、ルート権限で次のコマンドを実行します。
  `/opt/eset/efs/sbin/setgui --password=PASSWORD`
  PASSWORDは任意のパスワードで置換されます。

最終出力は、WebインターフェイスのURLアドレスとアクセス資格情報を示します。

アップデート失敗

何らかの理由で製品モジュールをアップデートできない場合、ダッシュボードに情報が表示されます。

最近のアップデート試行の失敗 - ESET Server Security for Linuxは最近アップデートサーバーに接続して、最新のウイルス定義アップデートを確認できていません。ネットワーク接続を確認してから、**確認してアップデート**をクリックしてもう一度モジュールをアップデートしてください。

検出エンジンが古くなっています – 検出エンジンはしばらくの間アップデートされていません。ネットワーク接続を確認してから、**確認してアップデート**をクリックしてもう一度モジュールをアップデートしてください。

noexecフラグの使用

*/var*および*/tmp*パスを`noexec`フラグでマウントし、*/opt*の書き込みが制限されている場合は、ESET Server Security for Linuxのインストールが失敗し、次のエラーメッセージが表示されます。

```
環境変数MODMAPDIRの値が無効です。モジュールを読み込めません。
```

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/efs drwxrwxr-x. root eset-efs-daemons
```

2. 次のコマンドを実行します:

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

3. */opt/eset/lib/modules*をsymlinkで置き換えます。

```
# rmdir /opt/eset/lib/modules
# ln -s /opt/eset/lib/modules /usr/lib/efs
```

4. 基本モジュールをコンパイルする:

```
# /opt/eset/efs/bin/upd --compile-nups
```

5. efsサービスを再起動する:

```
# systemctl restart efs
```

標準の権限がないユーザーがefsユーティリティを実行する場合、ユーザーのホームディレクトリがnoexecにマウントされていると同じエラーが表示されます。

回避策

1. 他のユーザーが*/opt/eset/lib/modules*を使用することを許可します

```
# chmod o+rwx /opt/eset/lib/modules
```

2a. または、特定のユーザーのexecが有効になっているフォルダーを作成します。

```
# mkdir /usr/lib/efs-user
# chown <user>:<user_group> /usr/lib/efs-user
# chmod 770 /usr/lib/efs-user
```

2b. あるいは、指定したMODMAPDIR変数でユーティリティを実行します。例:

```
# MODMAPDIR=/usr/lib/efs-user /opt/eset/efs/bin/lslog -s
```

リアルタイム保護を開始できない

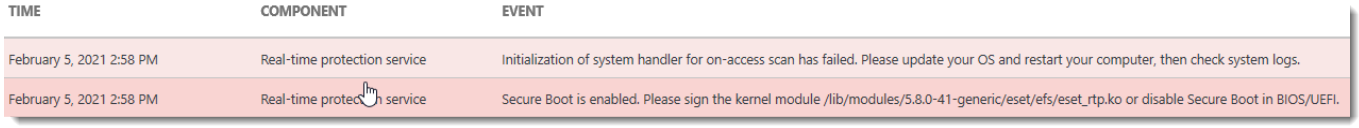
問題

カーネルファイルが見つからないか、セキュアブートを有効にしているため、リアルタイムファイルシステム保護を開始できません。

ESET Server Security for Linux (ESSL)のWebインターフェースの**イベント**画面にエラーメッセージが表示されます。

TIME	COMPONENT	EVENT
November 30, 2020 3:47 PM	Real-time protection service	Initialization of system handler for on-access scan has failed. Please update your OS and restart your computer, then check system logs.
November 30, 2020 3:47 PM	Real-time protection service	If you are running UEK kernel, make sure you have kernel-uek-devel installed
November 30, 2020 3:47 PM	Real-time protection service	Cannot open file /lib/modules/5.4.17-2036.100.6.1.el8uek.x86_64/eset/efs/eset_rtp.ko: No such file or directory

カーネルファイルが不足している



TIME	COMPONENT	EVENT
February 5, 2021 2:58 PM	Real-time protection service	Initialization of system handler for on-access scan has failed. Please update your OS and restart your computer, then check system logs.
February 5, 2021 2:58 PM	Real-time protection service	Secure Boot is enabled. Please sign the kernel module /lib/modules/5.8.0-41-generic/eset/efs/eset_rtp.ko or disable Secure Boot in BIOS/UEFI.

セキュアブートが有効

システムログに、対応するエラーメッセージが表示されます:

```
Nov 30 15:47:02 localhost.localdomain efs[373639]: ESET File Security error: cannot
find kernel sources directory for kernel version 5.4.17-2036.100.6.1.el8uek.x86_64

Nov 30 15:47:02 localhost.localdomain efs[373641]: ESET File Security error: please
check if kernel-devel (or linux-
headers) package version matches the current kernel version

Nov 30 15:47:04 localhost.localdomain oaeventd[373656]: ESET File Security Error: Ca
nnot open file /lib/modules/5.4.17-2036.100.6.1.el8uek.x86_64/eset/efs/eset_rtp.ko:
No such file or directory

Nov 30 15:47:04 localhost.localdomain oaeventd[373656]: ESET File Security Warning:
If you are running UEK kernel, make sure you have kernel-uek-devel installed

Nov 30 15:47:04 localhost.localdomain oaeventd[373656]: ESET File Security Error: In
itialization of system handler for on-
access scan has failed. Please update your OS and restart your computer, then check
system logs.
```

カーネルファイルが不足している

```
Feb 05 14:58:47 ubuntu2004 efs[52262]: ESET File Security Error: Secure Boot require
s signed kernel modules. Please run "/opt/eset/efs/lib/install_scripts/sign_modules.
sh" to sign our modules.

Feb 05 14:58:50 ubuntu2004 oaeventd[52303]: ESET File Security Error: Secure Boot is
 enabled. Please sign the kernel module /lib/modules/5.8.0-41-
generic/eset/efs/eset_rtp.ko or disable Secure Boot in BIOS/UEFI.

Feb 05 14:58:50 ubuntu2004 oaeventd[52303]: ESET File Security Error: Initialization
 of system handler for on-
access scan has failed. Please update your OS and restart your computer, then check
system logs.
```

セキュアブートが有効

解決策

ESSLがインストールされているコンピューターでセキュアブートが有効な場合は、セキュアブートセクションを参照してください。

方法1 – オペレーティングシステムの再起動が必要

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。CentOS 7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。

```
yum 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. 最新のkernel-develモジュール(RPMベースのLinuxディストリビューション)または最新のlinux-headers(DEBベースのLinuxディストリビューション)をインストールします。UbuntuLinux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 install linux-headers-`uname -r`
```

2. ESSLサービスを再起動します。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。

```
systemctl restart efs
```

方法3 - Unbreakable Enterprise Kernelを使用したOS

Unbreakable Enterprise Kernelが使用されている場合は、kernel-uek-develパッケージを手動でインストールする必要があります。

1. Oracle Linuxで、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。

```
yum install kernel-uek-devel-`uname -r` kernel-headers
```

2. ESSLサービスを再起動します。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。

```
systemctl restart efs
```

起動時にリアルタイムファイルシステム保護を無効にする

ESET Server Security for Linuxで保護されているコンピューターの応答が遅く、CPUが常時過負荷状態になっている場合は、トラブルシューティング目的で、起動時にリアルタイム保護を無効にすることができます。

1. コンピューターを起動し、GRUBメニューが表示されるまで待ちます。
2. 使用するカーネルをハイライトし、Eキーを押します。
3. `linux`で始まる行に移動し、行の終わりに`eset_rtp=0`パラメーターを追加します。

4. CTRL + Xを押して起動します。

> **注意**
> 一部のLinuxディストリビューションではGRUBの変更が若干異なる場合があります。

SMBプロトコル用の古いcurlライブラリ

ESET PROTECTを使用して隔離ファイルをアップロードしようとすると、次のエラーメッセージが表示されることがあります。

TIME	COMPONENT	EVENT
11/30/2022, 06:21 AM	Scanning service	File 'MyFile' upload to SMB server 'MyServer' failed: CURL: This version of libcurl does not support SMB protocol
11/30/2022, 06:17 AM	Scanning service	File 'MyFile' upload to SMB server 'MyServer' failed: CURL: This version of libcurl does not support SMB protocol

- この機能を使用するには、curlバージョン7.40.0以降がマシンにインストールされていることを確認してください。

カスタムTMPDIR

ESET Server Security for Linuxの既定の一時ディレクトリ*/tmp*を変更するには

1. `eset-efs-daemons`の読み取りおよび書き込み権限を持つカスタムディレクトリ*/efs-tmp*を作成します。ターミナルウィンドウから特権ユーザーとして次のコマンドを実行します。

```
sudo mkdir /efs-tmp

sudo chmod g+rw /efs-tmp

sudo chgrp eset-efs-daemons /efs-tmp/
```

結果は次のようになります。

```
ls -l /

drwxrwxr-x. 1 root eset-efs-daemons 0 Jan 15 15:56 efs-tmp
```

2. 環境変数を設定ファイルに設定します。

```
sudo echo TMPDIR=/efs-tmp >> /opt/eset/efs/etc/systemd/environment
```

3. 製品を再起動します。

```
sudo systemctl restart efs
```

NFSマウントが失敗する

問題

Webアクセス保護を支える技術は、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、クライアントは1025以下のポート（ルートにアクセス可能）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以上のランダムなポートから接続しようとするため、サーバーが拒否する結果となります。

回避策

NFSマウントサーバーの設定を危険に変更することで、拒否を回避できます。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することができます。

1. NFSサーバーコンピューターで、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安全でないに設定し、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。特権ユーザーとして次のコマンドを実行します。

```
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wg-quickを使用するか、サービスとして使用してWebアクセス保護(WAP)がWireGuardと併用されているとします。この場合WAPインターフェースとWireGuardインターフェー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ことがあります。これはインターフェー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発生します。インターフェースがwg0で、IPアドレスが*10.10.10.2*だとします。ルールは*wg-quick-wg0*テーブルに追加され、チェーンプレビューは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、セキュリティで保護されたシステムでは、このnftablesルールは必要ありません。そのルールをそのままにしないように設定wg-quickすると、接続の問題が解決します。たとえば、影響を受けるインターフェースの設定ファイルを編集し、*[Interface]*セクションに次のPostUpアクションを追加できます。

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

wg-quick-wg0名は*“wg0”*インターフェースにのみ適用され、他のインターフェースの場合はそれに応じて変更する必要があります。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'
```

インターフェースが″wg0"でない場合は、"wg0"に関するすべての記述を更新する必要があることに注意してください。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アクセス保護とiptables

問題

Webアクセス保護は、nftablesを使用して、送信接続をスキャナーにリダイレクトし、そこでHTTPトラフィックを検査します。

一部のお客様においてCentOS 7などのカーネル4.18より前のディストリビューションでWAPがiptables NATルールに干渉する場合に問題が発生しました。この問題は、iptablesとnftablesの両方で同時NATルールをサポートしていない以前のLinuxカーネルのバグが原因で発生します。NATの非互換性を参照してください。

> Centos 7は2024年6月にサポート終了になります。

回避策1

カーネル4.18以降のLinuxディストリビューション(Rocky Linux 8 など)を使用します。

回避策2

iptablesルールをnftablesに変換します。iptablesからnftablesへの移行の記事を参照してくださいNAT出力チェーンが発信接続に最初に適用されるようにするにはWAP出力NATチェーンの優先度が「-101」であるため、「-102」以下の優先度番号を使用することをお勧めします。

回避策がない場合は、Webアクセス保護を無効にしてiptables NATを機能させる必要があります(推奨されません)。

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。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。特定のイベントまたは条件の発生によって有効化されます。

ESET用語集のその他の用語を参照

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-ROMDVD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(EOLポリシー」)が適用される場合があります。https://go.eset.com/eol_home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URLIP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ー、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。

契約書の補遺

ネットワーク接続デバイスセキュリティ評価。ネットワーク接続デバイスセキュリティ評価には、次のように追加の条項が適用されます。

本ソフトウェアには、ネットワーク接続デバイスセキュリティ評価の一部としてライセンス情報に関連する、ローカルネットワークのデバイスの存在、タイプ、名前、IPアドレス、およびMACアドレスなど、ローカルネットワークのデバイスに関する情報とローカルネットワーク名が必要な、エンドユーザーのセキュリティとローカルネットワークのデバイスのセキュリティを確認する機能があります。これらの情報には、ルーターデバイスのワイヤレスセキュリティタイプとワイヤレス暗号化タイプも含まれます。この機能は、ローカルネットワークのデバイスを保護するためのセキュリティソフトウェアソリューションの利用状況に関する情報も提供する場合があります。

データの悪用に対するAnti-Theftの保護。データの悪用に備える保護対策には、次のように追加の条項が適用されます。

本ソフトウェアには、コンピューターの窃盗と直接関連して、重要なデータの損失または悪用を防止する機能が含まれています。この機能は、本ソフトウェアの既定の設定でオフにされています。アクティベーションするにはESET HOMEアカウントを作成する必要があります。 これによって、コンピューターの窃盗の際に、データ収集が有効になります。本ソフトウェアのこの機能を有効にする場合は、盗まれたコンピューターに関するデータが収集され、供給者に送信されます。これには、コンピューターのネットワーク位置情報データ、コンピューター画面に表示された内容のデータ、コンピューターの構成のデータ、およびコンピューターに接続されたカメラによって記録されたデータ(「データ」)が含まれることがあります。エンドユーザーは、コンピューターの窃盗が原因の問題を修正する目的でのみ、この機能

で取得されESET HOMEアカウントに送信されたデータを使用する資格があります。この機能の目的に限り、供給者は、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、データを処理します。供給者は、データが取得された目的を達成するために必要な期間の間、エンドユーザーがデータにアクセスすることを許可するものとします。ただし、この期間は、プライバシーポリシーで規定された保持期間を超えないものとします。データの悪用に対する保護は、エンドユーザーが合法的にアクセスできるコンピューターおよびアカウントでのみ使用されるものとします。不法使用は管轄当局に報告されます。供給者は関連する法律を遵守し、悪用の場合には法執行機関を支援します。お客様は、自身がESET HOMEアカウントにアクセスするためのパスワードを保護する責任を有することを認め、パスワードをいかなる第三者にも開示しないことに同意します。エンドユーザーは、許可の有無を問わず、データの悪用保護機能ESET HOME アカウントを使用したすべての活動に責任を負いますESET HOMEアカウントが危険にさらされた場合は、ただちに供給者に通知してください。データの悪用に備える保護対策の追加条項はESET Internet SecurityおよびESET Smart Security Premiumエンドユーザーにのみ適用されるものとします。

ESET Secure DataESET Secure Dataには、次のように追加の条項が適用されます。

1. 定義ESET Secure Dataのこれらの追加条項では、次の単語には次の対応する意味があります。

a) 情報」本ソフトウェアを使用して暗号化または復号化される情報またはデータ。

b) 製品ESET Secure Dataソフトウェアおよびマニュアル;

c) ESET Secure Data電子データの暗号化および復号化で使用されるソフトウェア。

複数形のすべての参照には、単数形が含まれるものとします。男性形のすべての参照には、女性形および中性形が含まれるものとします。また逆も同様とします。特定の定義がない単語については、本契約で規定された定義に従って使用されるものとします

2. 追加のエンドユーザー宣言。お客様は次のことを認め、同意するものとします。

a) 情報を保護、管理、およびバックアップするのはお客様の責任です。

b) ESET Secure Dataをインストールする前に、コンピューターのすべての情報およびデータ(重要な情報とデータを含むがこれらに限定されない)を完全にバックアップしてください。

c) お客様は、ESET Secure Dataのセットアップおよび利用に必要なすべてのパスワードまたはその他の情報を安全に記録しておく必要があります。また、すべての暗号化キー、ライセンスコード、鍵ファイル、およびその他のデータのコピーを別のストレージメディアにバックアップする必要があります。

d) お客様は製品の使用について責任を負うものとします。供給者は、情報またはデータの保存場所または保存方法に関係なく、情報またはデータ(情報を含むがこれに限定されない)の不正または誤った暗号化または復号化の結果として生じる一切の損失、請求、または損害について責任を負わないものとします。

e) 供給者はあらゆる合理的な手順を講じ、ESET Secure Dataの完全性およびセキュリティを保証することに努めていますが、セキュリティのフェールセーフレベルに依存する領域、あるいは核施設、航空機ナビゲーション、制御、または通信システム、兵器および防衛システム、生命維持または生命監視システムを含む(ただしこれらに限定されない)有害または危険の可能性がある領域において、製品(またはそのいずれか)を使用することは禁止されています。

f) 本製品によって提供されたセキュリティと暗号化のレベルが要件に適していることを確認することはお客様の責任です。

g) お客様は、このような使用がスロバキア共和国または製品が使用される他の国、地域、州などにおけるすべての適用される法律および規制に準拠することの保証を含め(ただしこれに限定されない)、製

品(またはそのいずれか)を使用する責任を負うものとします。お客様は、製品を使用する前に、あらゆる政府(スロバキア共和国または他国)の禁止措置に抵触しないことを保証する必要があります。

h) ESET Secure Dataは時々供給者のサーバーに接続し、ライセンス情報、使用可能なパッチ、サービスパック、およびESET Secure Dataの動作を改善、維持、修正、または強化できるその他のアップデートを確認し、プライバシーポリシーに準拠した方法で機能に関連する一般システム情報を送信する場合があります。

i) 供給者は本ソフトウェアの使用中に生成または保存されたパスワード、設定情報、暗号化キー、ライセンスアクティベーションコード、およびその他のデータの損失、窃盗、悪用、破損、損害、または破壊から生じる一切の損失、損害、費用、または請求については責任を負わないものとします。

ESET Secure Dataの追加条項はESET Smart Security Premiumエンドユーザーにのみ適用されるものとします。

Password Managerソフトウェア。Password Managerソフトウェアには、次のように追加の条項が適用されます。

1. 追加のエンドユーザー宣言。添付文書1はESET Smart Security Premiumエンドユーザーにのみ適用されるものとします。

a) Password Managerソフトウェアを使用して、人間の生命または財産が危険にさらされる可能性がある重要なアプリケーションを運用すること。お客様は、Password Managerソフトウェアがこのような目的では設計されておらず、このような場合における障害は、供給者が責任を負わない死亡、人身傷害、または重大な財産または環境への損害につながる可能性があることを理解するものとします。

PASSWORD MANAGERソフトウェアは、核施設、航空機ナビゲーションまたは通信システム、航空交通管制、および生命維持または兵器システムの設計、開発、保守、または運用を含む(ただしこれらに限定されない)、フェールセーフ制御が必要な危険な環境で使用することを目的としておらず、そのような目的で設計またはライセンス供与されていません。供給者はこのような目的への適合性の明示的または暗示的な保証を具体的に放棄します。

b) 本契約あるいはスロバキア共和国または管轄地域の法律に抵触する方法でPassword Managerソフトウェアを使用すること。特に、Password Managerソフトウェアを使用して、有害なコンテンツ、あるいはストレージ(Password Managerソフトウェアの追加条項では、「ストレージ」は供給者または供給者以外の第三者、およびユーザーデータ の同期とバックアップを有効するためにユーザーが管理するデータストレージ領域を意味します)のアカウント、または他のPassword Managerソフトウェアまたはストレージユーザーのアカウントとデータへのアクセスを取得する試みを含む(ただしこれらに限定されない)、不法行為で使用される可能性があるコンテンツ、または何らかの方法で法律または第三者の権利(知的財産権を含む)を侵害するコンテンツを含む、不法行為を実施または促進することは禁止されています。これらの規定に違反した場合、供給者はただちに本契約を解除し、必要な救済策の費用をお客様に課し、返金の可能性を排除してお客様がPassword Managerソフトウェアを使用できないようにするために必要な手順を講じる資格があります。

2. 責任の制限PASSWORD MANAGERソフトウェアは「現状有姿」で提供されます。一切の明示的または暗示的な保証はありません。本ソフトウェアはお客様の責任で使用するものとします。開発者は、データ同期およびバックアップ目的でPASSWORDMANAGERソフトウェアから外部ストレージに送信されたデータを含む、データの損失、損害、サービス可用性の制限については責任を負いませんPASSWORD MANAGERを使用してデータを暗号化することによって、供給者はそのデータのセキュリティに関する一切の責任を課されないものとします。お客様は、PASSWORD MANAGERソフトウェアを使用して取得、使用、暗号化、保存、同期、または送信されたデータが第三者のサーバーに保存されることがあるということにも明示的に同意するものとします(同期およびバックアップサービスが有効な場合のPASSWORD MANAGERソフトウェアの使用にのみ適用)。供給者がその独自の裁量においてこのような第三者のストレージWebサイトWebポータル、サーバー、またはサービスを使用することを選択した場合、供給者はこのような第三者のサービスの品質、セキュリティ、または可用性について責任を負わないものとし

ます。また、いかなる範囲においても、供給者はお客様に対して第三者の契約または法的義務違反、あるいは本ソフトウェアの使用中に発生した損害、利益の損失、財務的または非財務的損害、またはいかなる他の種類の損失について責任を負わないものとします。供給者はPASSWORD MANAGERソフトウェアを使用して取得、使用、暗号化、保存、同期、または送信されたデータあるいはストレージのデータの内容について責任を負いません。お客様は、供給者が保存されたデータの内容にアクセスできず、データの監視ができず、法的に有害なコンテンツを削除できないことを確認するものとします。

このような改良が何らかの形式でお客様から提出されたフィードバック、アイデア、または提案に基づいて作成された場合においても、供給者はPassword MANAGERソフトウェアに関連する改良、アップグレード、および修正(「改良」)に対するすべての権限を有します。お客様は、このような改良の使用許諾料を含む一切の補償を受け取る権利がないものとします。

供給者企業およびライセンサーは、たとえこのような請求および責任が法的または衡平法上の理論に基づいていたとしても、いかなる方法においても、お客様または第三者によるソフトウェアの使用、

いかなる仲介企業または代理店の使用または不使用、あるいはセキュリティの販売または購入に起因して生じるもしくはそれに関連する一切の種類の請求および義務に対する責任を負わないものとします。供給者企業およびライセンサーは、このような損害請求が法律または衡平法の理論に基づいているかどうかにかかわらず、お客様に対して、第三者のソフトウェア PASSWORD MANAGERソフトウェアを使用してアクセスされるデータ、お客様がPASSWORD MANAGERを使用すること、使用またはアクセスできないこと、あるいはPASSWORD MANAGER経由で提供されたデータから生じるかそれに関連する一切の直接的、付随的、特殊的、間接的、または結果的な損害の責任を負わないものとします。本条項から除外される損害には、事業利益の損失、個人または財産に対する損害、事業の中断、事業または個人情報の損失(ただしこれらに限定されない)があります。 管轄地域によって、付随的または結果的損害の制限が認められない場合があるため、本制限事項がお客様には適用されない場合があります。このような場合、供給者の責任の範囲は適用される法律の下で認められた最低限になります。

株価、分析、市場情報、ニュース、財務データを含むソフトウェア経由で提供される情報には遅延や不正確性、または瑕疵や省略がある可能性があります。供給者企業およびライセンサーはこのような点に関して責任を負わないものとします。供給者は、いかなる時点においても、お客様への事前の通知なく PASSWORD MANAGERソフトウェアの何らかの要素または機能、あるいはPASSWORD MANAGERソフトウェアのすべてまたは一部の機能または技術の使用を変更または終了する場合があります。

本項の条項が何らかの理由により無効になった場合、または適用される法の下で供給者が損失、損害などに対する責任を負うと見なされる場合、両当事者は、お客様に対する供給者の責任はお客様が支払ったライセンス料金の合計金額を上限とすることに同意するものとします。

お客様は、あらゆる第三者(その権限がPASSWORD MANAGERソフトウェアまたはストレージで使用されるデータによって影響されたデバイスの所有者または当事者を含む)の請求、責任、損害、コスト、費用、このような当事者がお客様によるPASSWORD MANAGERソフトウェアの使用の結果として発生しうる料金に対して、供給者およびその従業員、子会社、関係会社、再ブランディング、および他のパートナーを補償、保護、および無害に保つことに同意するものとします。

3.Password Managerソフトウェアのデータ。特に明示的に明記されていないかぎり、お客様が選択してPassword Managerソフトウェアデータベースに保存されるすべてのデータはコンピューターまたはお客様が定義した他のストレージデバイス上に暗号化された形式で保存されます。お客様は、Password Managerソフトウェアデータベースまたは他のファイルの削除または損害が発生した場合には、そこに保存されているすべてのデータが不可逆的に失われることを理解し、このような損失のリスクを理解および承諾するものとします。お客様の個人データがコンピューターに暗号化された形式で保存されるということは、マスターパスワードを知り得た人物が情報を窃盗または悪用したり、データベースを開く目的でお客様が定義したアクティベーションデバイスにアクセスできないことを意味するものではありません。お客様は、すべてのアクセス方法のセキュリティを管理する責任を負うものとします

4. 供給者またはストレージへの個人データの転送。そのように選択した場合、タイムリーなデータ同期およびバックアップを保証する目的でのみPassword Managerソフトウェアは Password Managerソフトウェ

アデータベースからパスワード、ログイン情報、アカウント、およびIDなどの個人データをインターネット経由でストレージに転送または送信します。データは暗号化された形式でのみ転送されます。パスワード、ログイン情報、または他のデータをオンラインフォームに入力する目的でPassword Managerソフトウェアを使用する場合、お客様が指定したWebサイトにインターネット経由で情報を送信する必要があります。このデータ転送はPassword Managerソフトウェアによって開始されないため、供給者は各種供給者によってサポートされるWebサイトとのこのような連携のセキュリティについては責任を負いかねます。インターネット上のあらゆる処理は、Password Managerソフトウェアと連動しているかどうかにかかわらず、お客様独自の裁量およびリスクで行われ、このような素材またはサービスのダウンロードまたは使用から生じるコンピューターシステムへの損害またはデータの損失についてはお客様が単独で責任を負うものとします。価値のあるデータの損失リスクを最小化するために、供給者は、お客様がデータベースおよび他の重要なファイルを定期的に外部デバイスにバックアップすることをお勧めします。供給者は損失または破損したデータの復元については一切の支援を提供いたしかねます。ユーザPCのファイルの破損または削除の場合に供給者がユーザーデータベースファイルのバックアップサービスを提供する場合、このようなバックアップサービスには一切の保証がなく、供給者はいかなる場合でも責任を負わないものとします。

PasswordManagerソフトウェアを使用することによって、お客様は、本ソフトウェアが時々供給者のサーバーに接続し、ライセンス情報、使用可能なパッチ、サービスパック、およびPassword Managerソフトウェアの動作の改良、メンテナンス、修正、または機能強化につながる可能性がある他のアップデートを確認することに同意するものとします。本ソフトウェアは、プライバシーポリシーに準拠し、Password Managerソフトウェアの機能に関連する一般システム情報を送信する場合があります。

5. アンインストール情報および手順。データベースに保持するすべての情報は、Password Managerソフトウェアをアンインストールする前にエクスポートする必要があります。

Password Managerソフトウェアの追加条項はESET Smart Security Premiumエンドユーザーにのみ適用されるものとします。

ESET LiveGuard.ESET LiveGuardには、次のように追加の条項が適用されます。

本ソフトウェアには、エンドユーザーによって送信されたファイルの追加の分析機能が含まれています。供給者は、エンドユーザーが提出したファイル、ならびにプライバシーポリシーおよび関連する法規制に準拠した分析結果のみを使用するものとします。

ESET LiveGuardの追加条項はESET Smart Security Premiumエンドユーザーにのみ適用されるものとします。

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

プライバシーポリシー

個人データの保護は、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: 31333532) (ESETまたは「当社」)にとって特に重要ですESETは、EU一般データ保護規制(GDPR)の下で法的に規定された透明性要件に準拠します。この目標を達成するためにESETは、データ主体としてのお客様(「エンドユーザー」または「お客様」)に次の個人データ保護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。

- 個人データの処理の法的根拠
- データ共有と機密保持
- データセキュリティ

- データ主体としての権利
- 個人データの処理
- 連絡先情報。

個人データの処理の法的根拠

ESETが個人データの保護に関連する該当する法的フレームワークに従って使用するデータ処理には、ほとんど法的根拠がありません。ESETにおける個人データの処理は、主に、エンドユーザーとの エンドユーザー使用許諾契約 (以下EULA)の履行(GDPR第6 (1) (b)条)に必要です。これは、明示的な記載がないかぎり、ESETの製品またはサービスの提供に適用されます。例:

- 正当な利益という法的根拠(GDPR第6 (1) (f)条)。これにより、お客様がサービスを使用する方法、ならびにESETが提供できる最高の保護、サポート、およびエクスペリエンスに対するお客様の満足度に関するデータを処理できます。適用される法律では、マーケティングも正当な利益と認識されているため、通常はお客様とのコミュニケーションで使用されるCookieについては、この概念を適用します。
- 同意(GDPR第6 (1) (a)条)。ESETがこの法的根拠を最も適切な根拠であると見なすとき、または法律で義務付けられている場合には、特定の状況において、ESETがお客様の同意を求める場合があります。
- 電子通信、請求または課金文書の保持に関する要件の規定など、法的義務の遵守(GDPR第6 (1) (c)条)。

データ共有と機密保持

ESETがお客様のデータを第三者と共有することはありません。ただし、ESETは、販売、サービス、および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を通して、世界中で事業を展開する企業です。ESETが処理するライセンス、請求、テクニカルサポート情報は、サービスやサポートの提供といったエンドユーザーライセンス契約の履行の目的で、関連会社またはパートナーとの間で転送される場合があります。

基本的に、ESETは、欧州連合(EU)でデータを処理します。ただし、お客様の居住国(EU外での製品またはサービスの利用)またはお客様が選択するサービスによっては、EU外の国にお客様データを転送しなければならない場合があります。たとえば、ESETは、クラウドコンピューティングに関連してサードパーティサービスを使用しています。このような場合、ESETはサービスプロバイダーを厳選し、契約、技術、組織的な対策を導入して、適切なレベルのデータ保護を保証します。原則として、ESETは、EUの標準契約条項と補足契約規制(必要な場合)に同意します。

英国やスイスなどのEU外の一部の国については、EUが既に同等のデータ保護を決定しています。同等のデータ保護が規定されているため、このような国へのデータ転送には特別な認可または同意が必要ありません。

データセキュリティ

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、すぐに該当する監督当局とデータ主体として影響を受けるエンドユーザーに通知します。

データの主体の権利

すべてのエンドユーザーの権利は重要です。ESETは、すべてのエンドユーザ(EU加盟国およびEU非加盟国)が次の権利について保証されていることを通知します。データ主体の権利を行使するには、サポー

トフォームまたは電子メール(dpo@eset.sk)でお問い合わせください。本人確認目的で、次の情報をご提示ください。お名前、電子メールアドレス、製品認証キー(該当する場合)、お客様番号、会社名。生年月日などの他の個人データは送信しないでください。また ESETは、お客様の依頼を処理し、本人確認を行うために、お客様の個人データを処理します。

同意を取り消す権利。同意のみに基づく処理の場合、同意を取り消す権利が適用されます ESETがお客様の同意に基づいてお客様の個人データを処理する場合、お客様は、理由を提供せずに、いつでも同意を取り消す権利があります。同意の取り消しは将来に対してのみ有効であり、取り消し前に処理されたデータの合法性には影響しません。

異議を申し立てる権利。同意のみに基づく処理の場合、同意を取り消す権利が適用されます ESETが合法的な利益を保護するために、お客様の個人データを処理する場合、データ主体としてのお客様は、いつでもESETが指名した合法的な利益および個人データの処理に対して異議を申し立てる権利があります。異議申し立ては将来に対してのみ有効であり、異議申し立て前に処理されたデータの合法性には影響しません ESETがダイレクトマーケティング目的で個人データを処理している場合、お客様の異議申し立ての理由を提出する必要はありません。これは、このようなダイレクトマーケティングに関連しているかぎり、プロファイリングにも該当します。他のすべての場合において、お客様は、ESETが個人データを処理する正当な利益に対する苦情について簡潔に通知することが求められます。

場合によっては、お客様が同意を取り消したにもかかわらず ESETは、契約の履行など、別の法的根拠に基づいて個人データを引き続き処理する資格があります。

アクセスの権利。お客様は、データ主体として、いつでも無料で、ESETによって保存されたデータに関する情報を取得する権利があります。

修正する権利。ESETがお客様に関する誤った個人データを間違って処理した場合、お客様はこれを修正する権利があります。

消去する権利および処理を制限する権利。データ主体として、お客様は、個人データの削除または制限を要求する権利があります。お客様の同意を得た場合など ESETがお客様の個人データを処理し、お客様がその同意を取り消し、それ以上の法的根拠(契約など)が存在しない場合 ESETはただちにお客様の個人データを削除します。お客様の個人データは、保持期間の終了に指定された目的で必要とされなくなった時点ですみやかに削除されます。

ESETが直接マーケティングの目的でのみお客様の個人データを使用し、お客様が同意を取り消したか、根拠となるESETの合法的な利益に対して異議を申し立てた場合 ESETは、未承諾の連絡を回避する目的でお客様の連絡先データを社内ブラックリストに追加する範囲で、お客様の個人データの処理を制限します。そうでない場合、お客様の個人データは削除されます。

ESETは、立法当局または監督当局によって発行された保持義務および期間が終了するまで、お客様のデータを保存することが義務付けられている場合があります。保持義務と期間は、スロバキアの法律によっても生じ得る場合があります。その後、該当するデータは日常的に削除されます。

データ移植性の権利。ESETは、データ主体としてのお客様に対して ESETが処理する個人データをxls形式で提供いたします。

苦情を申し立てる権利。データ主体として、お客様は、いつでも監督当局に苦情を申し立てる権利を有します 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。該当するデータ監督当局は、スロバキア共和国個人データ保護局(Hraničná 12, 82007 Bratislava 27, Slovak Republic)です。

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、エンドユーザーライセンス契約および製品 ドキュメントをご覧ください。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。

ライセンスおよび請求データ。名前、電子メールアドレス、製品認証キー、(該当する場合)住所、会社名、決済データは、適用法またはお客様の同意に従って、ライセンスのアクティベーション、製品認証キーの提供、有効期限のリマインダー、サポート依頼、ライセンスが本物であることの検証、サービスの提供、および他の通知(マーケティングメッセージを含む)を支援する目的で、ESETによって収集および処理されます。ESETは、10年間請求情報を保持する法的義務を負っています。ただし、ライセンス情報は、遅くともライセンスの有効期限から12か月間経過した後に匿名化されます。

アップデートおよび他の統計情報。処理される情報には、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が含まれます。これらの情報は、アップデートおよびアップグレードサービスの提供、ならびにESETバックエンドインフラストラクチャのメンテナンス、セキュリティ、改善の目的で処理されます。

この情報はエンドユーザーを特定する必要がないため、ライセンスおよび請求目的で必要な個人を識別する情報とは別に保持されます。保持期間は最大4年間です。

ESET LiveGrid®レピュテーションシステム。侵入に関連する単方向ハッシュは、検査されたファイルを、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することで、マルウェア対策ソリューションを効率化するESET LiveGrid®レピュテーションシステムの目的で処理されます。この処理中にエンドユーザーが特定されることはありません。

ESET LiveGrid®フィードバックシステム。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

- 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

- IP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

- 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。

ESET LiveGrid®フィードバックシステム経由で取得および処理されるすべての情報は、エンドユーザーを特定せずに使用されます。

ネットワーク接続デバイスセキュリティ評価。セキュリティ評価機能を提供するために。ESETは、ライセンス情報に関連する、ローカルネットワークのデバイスの存在、タイプ、名前。IPアドレス、およびMACアドレスなど、ローカルネットワークのデバイスに関する情報とローカルネットワーク名を処理します。これらの情報には、ルーターデバイスのワイヤレスセキュリティタイプとワイヤレス暗号化タイプも含まれます。エンドユーザーを識別するライセンス情報は、ライセンスの有効期限から最大12か

月間匿名化されます。

テクニカルサポート。サポート要求に含まれる連絡先・ライセンス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。テクニカルサポートで処理されたデータは4年間保管されます。

データの悪用に対するAnti-Theftの保護。https://home.eset.comでESET HOMEアカウントを作成し、コンピューターの盗難に対処してエンドユーザーがこの機能を有効にした場合は、次の情報が収集および処理されます。位置情報データ、スクリーンショット、コンピューターの構成に関するデータ、コンピューターのカメラによって記録されたデータ。収集されたデータは、3か月間の保持期間の間、ESETのサーバーまたはESETのサービスプロバイダーのサーバーに保管されます。

Password Manager Password Managerの機能を有効にした場合、ログイン詳細情報に関するデータは暗号化された形式でお客様のコンピューターまたは他の指定されたデバイスに保存されます。同期サービスを有効にすると、暗号化データはESETサーバーまたはサービスプロバイダーのサーバーに保存され、このようなサービスが保証されますESETもサービスプロバイダーも、暗号化されたデータにはアクセスできません。お客様のみがデータを復号化するための鍵を保有しています。 この機能を無効にすると、データが削除されます。

ESET LiveGuard.ESET LiveGuard機能を有効にする場合は、エンドユーザーがあらかじめ定義および選択したファイルなどのサンプルを送信する必要があります。リモート分析に選択したサンプルは、ESETサービスにアップロードされ、分析の結果がコンピューターに送信されます。不審なサンプルは、ESET LiveGrid®フィードバックシステムによって収集される情報の方法で処理されます。

カスタマーエクスペリエンス改善プログラム。お客様が カスタマーエクスペリエンス改善プログラムのアクティベーションを選択した場合、お客様の同意に基づき、当社の製品の使用に関連する匿名のテレメトリー情報が収集され、使用されます。

ESETの製品およびサービスを使用する個人が製品またはサービスを購入したエンドユーザーではなくESETとエンドユーザーライセンス契約を締結していない場合(例：エンドユーザーの従業員、家族、エンドユーザーライセンス契約に従ってエンドユーザーから製品またはサービスの使用を許可された人)GDPR第6(1)f)条の解釈に従い、ESETの合法的な利益において、データの処理が実行され、エンドユーザーが許可したユーザーはエンドユーザーライセンス契約に従ってESETが提供する製品およびサービスを使用できるものとします。

連絡先情報

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