ESET Server Security for Linux V12.1 リリースノート

キヤノンマーケティングジャパン株式会社

（2025 年 11 月）

■ はじめに

キヤノンマーケティングジャパン製品をご愛顧いただき誠にありがとうございます。
このリリースノートには、ESET Server Security for Linux V12.1（以降、本製品と記載）を正しくご利用頂くための情報が記載されています。
本製品をインストールする前に必ずお読みください。

■ インストール前の注意事項

本製品をインストールする前に、以下の内容を確認してください。

- 本製品をインストールする前に、すべてのプログラムを必ず終了してください。
- 本製品以外のウイルス対策ソフトウェアがインストールされていないことを確認してください。本製品以外のウイルス対策ソフトウェアがインストールされている場合は、必ずアンインストールしてください。
- 本製品をインストールする場合は、root 権限（スーパーユーザー）でインストールしてください。
- 本製品をインストールするには OS リポジトリに接続できる必要がございます。
- 本製品のインストール時に不足しているパッケージについてはインストール時に合わせて OS リポジトリから取得しインストールされます。
- 本製品のインストールを行う前に、導入されているプログラムをアップデートしてください。

・ 本製品をインストールするコンピューターに前提となるプログラムが導入されていることを確認してください。また、以下記載のパッケージバージョンは予告なく変更する場合がございます。予めご了承ください。
弊社では以下の kernel で動作検証を実施しております。
- Redhat 系の場合、kernel 4.18.0-553/ kernel 5.14.0-570/ kernel 6.12.0-55/ kernel 6.12.0-100 にて実施
- AWS kernel の場合、kernel 6.12.40-63.114 にて実施
- SUSE Linux の場合、kernel 5.14.21-150400.24.100 にて実施
- Ubuntu の場合、kernel 5.4.0-216/ 5.15.0-161/ 6.8.0-87 にて実施
- Debian の場合、kernel 5.10.0-36/ 6.1.0-40/ 6.12.48 にて実施
- glibc 2.28 以降のバージョン
- en-US.UTF-8 エンコーディングロケール

・ 本製品をインストールするコンピューターには、上記のほかに次のプログラムがインストールされます。

共通で必要とされるパッケージ
- openssl
- gcc
- perl
- nftables
- nss-tools（SUSE の場合 mozilla-nss-tools、Debian の場合 libnss3-tools）
- sqlite（SUSE の場合 sqlite3、Debian の場合 libsqlite3）
- tar
- make

RHEL, Amazon Linux, AlmaLinux, Rocky Linux, Oracle Linux に必要とされるパッケージ
- kernel-devel
- kernel-headers

SUSE Linux に必要とされるパッケージ
- kernel-default-devel
- kernel-macros
- linux-glibc-devel

Debian, Ubuntu に必要とされるパッケージ
- linux-headers-generic
- linux-headers-generic-hwe
- libelf-dev

- libudev1
- cron
- anacron
- btrfs-progs
- libcurl

※ 不足している記載パッケージと依存性関連のパッケージが OS リポジトリより取得、導入されます。

■ 製品マニュアルについて

本製品のマニュアルにはオンラインヘルプとオンラインヘルプ補足資料があります。
はじめにオンラインヘルプ補足資料を確認してください。
オンラインヘルプ補足資料は「ユーザーズサイト」よりダウンロードすることが出来ます。

ユーザーズサイト
https://canon-its.jp/product/eset/users/

オンラインヘルプ
https://help.eset.com/essl/12.1/ja-JP/

■ 旧バージョン（V12.0）からの変更点について

以下の機能が追加されました。

□ 検出シグネチャの更新頻度の向上

検出シグネチャの更新頻度が高くなりました。

□ Debian 13 のサポート

Debian 13 に対応しました。

□ Oracle Linux 10 のサポート

Oracle Linux 10 に対応しました。

以下の機能が変更されました。

□　プロキシサーバの設定箇所の変更

プロキシサーバの設定箇所が[ツール]セクションから[接続]セクションに再配置されました。

■　使用上の注意事項について
本製品を使用する前に、以下の内容を確認してください。

□　kernel バージョンについて

本製品のリアルタイムファイルシステム保護は以下記載の kernel バージョンを揃える必要がございます。

RHEL, Amazon Linux, AlmaLinux, Rocky Linux, Oracle Linux
 - kernel, kernel-devel, kernel-headers

SUSE Linux
 - kernel-default, kernel-devel, kernel-default-devel, kernel-macros

Debian, Ubuntu
 - linux-headers-generic-hwe, linux-headers-generic

□　ミラーサーバーを使用したアップデートについて

本製品をミラーサーバー経由でアップデートする場合は、ミラーツールの --updateServer オプションを使用して ESET Server Security for Linux のモジュールを取得したミラーサーバーを作成する必要があります。

詳細については以下のオンラインヘルプを参照ください。
https://help.eset.com/protect_install/12.1/ja-JP/mirror_tool_windows.html

□　パフォーマンス除外の登録について

本製品でWebGUIを開き、「設定>検出エンジン>基本>パフォーマンス除外」から特定のディレクトリ配下にパフォーマンス除外設定を行う際、以下のように設定ください。

設定例）パフォーマンス除外で「/root」配下を除外する場合
パフォーマンス除外設定に「/root/*」と登録する

□ プロセス除外に登録するパスについて

本製品でプロセス除外を行う場合、登録するパスにシンボリックリンクが含まれていると除外されない現象を確認しています。

設定例）プロセス除外設定に「vi」を登録する場合
/bin/vi：「/bin」がシンボリックリンクのためプロセス除外されない
/usr/bin/vi：プロセス除外される

プロセス除外が機能しない場合は登録したパスにシンボリックリンクが含まれているかをご確認ください。

※注意事項
一部のOSでは、/usr/bin/viがバイナリファイルからシェルスクリプトに変更されました。
シェルスクリプトの内部には、/usr/bin/vimを実行するよう記述があります。
その影響により、一部のOSでは/usr/bin/viでなく/usr/bin/vimをプロセス除外に登録しないと動作しないためご注意ください。

□ en-US.UTF-8ロケールについて

本製品をインストールする環境にen-US.UTF-8ロケールが必要です。
en-US.UTF-8ロケールがインストールされていない場合、RHEL/AlmaLinux/Rocky Linuxは「dnf install glibc-langpack-en」にてロケールをインストールすることが可能です。

□ セキュアブート環境でのアップデートについて

セキュアブート環境で本製品のアップデートを行う場合は、アップデート後に再

度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。作業手順についてはオンラインヘルプをご確認ください。

https://help.eset.com/essl/12.1/ja-JP/secure_boot.html

□　アップデート時に表示される警告について

旧バージョンよりアップデートを行う際、コンソールに「警告：ファイル /var/opt/eset/efs/bin/Modules: 削除に失敗しました: そのようなファイルやディレクトリはありません」と警告メッセージが表示される場合があります。

アップデート後の製品動作に問題ありませんのでそのままご利用いただけます。

□　リポジトリへのプログラム公開について

本製品のリポジトリ公開ですが、同世代の ESET PROTECT on-prem 以降で公開される仕様となっています。そのため本製品バージョンより古い ESET PROTECT on-prem をご利用の場合、最新のプログラムが公開されない場合がございますのでご注意ください。

□　Web アクセス保護のアドレスリスト内にある許可するアドレスのリストについて

本製品の[Web アクセス保護] > [URL アドレス管理] > [アドレスリスト]内にある許可するアドレスのリストですが、ブロックするアドレスのリスト内に記録されているアドレスの特定のページのみアクセスされる場合に登録する機能です。本設定に登録した URL が無条件に許可されるわけではないのでご注意ください。

設定例）ブロック登録されているアドレスの特定のページのみ参照させる場合
ブロックされたアドレス：https://BlockURL/*
許可するアドレスのリスト：https://BlockURL/permit

ブロックされたアドレス内の「https://BlockURL/permit」ページのみ参照可能となる

□　NFS サーバーの設定について

Web アクセス保護が有効な場合、Web アクセス保護によって傍受された接続は 1024 番ポートを超えるランダムなポートで NFS サーバーへ接続いたします。
NFS サーバー既定の Secure 設定ですと 1024 より小さいポート番号からのリクエストしか受け付けないため、NFS マウントに失敗します。

NFS サーバマシンで共有ディレクトリ設定を insecure に設定するか、Web アクセス保護を無効にすることで本事象を回避することができます。

詳細については以下のオンラインヘルプを参照ください。
https://help.eset.com/essl/12.1/ja-JP/secure_boot.html?nfs_mount_fails.html

■ 既知の問題について

本製品には、以下の問題と制約があります。
これらの問題については、将来のリリースで修正される可能性があります。
最新の情報につきましては弊社 FAQ サイトの案内をご確認ください。

ESET 製品 FAQ サイト：
https://eset-support.canon-its.jp/?site_domain=business

□ リスニングアドレスを空欄にしてポート番号を変更するとポート変更ができない

本製品の WebUI よりポート変更をする際、リスニングアドレスを空欄にしてポート変更を行うと、変更したポートに変更できず、WebUI にアクセスできない現象を確認しております。

現象が発生してしまった場合、コマンド「/opt/eset/efs/sbin/setgui –i <IP>:<Port>」にてポート番号を変更することが可能です。

□ SELinux が導入されていない環境でアップデートを実行するとコンソールにエラーが表示される

本製品を旧バージョンからアップデートする際、SELinux が導入されていない環境でコンソールに「/var/tmp/rpm-tmp.wARwrm: line 31: semodule: command not found」と表示される現象を確認しています。

アップデート後の製品動作に問題はありませんのでそのままご利用いただけます。

□　隔離から復元した検体が検出されない現象について

本製品で隔離した検体を復元する場合、復元した検体がリアルタイム検査で検出されない現象を確認しております。

■　製品情報

本製品に関する情報は、以下の URL から参照することができます。

ESET 製品ページ：
https://canon.jp/biz/solution/security/it-sec/lineup/eset

ユーザーズサイト：
https://canon-its.jp/product/eset/users/

オンラインヘルプ
https://help.eset.com/essl/12.1/ja-JP/

自動アップデート機能に関するページ：
https://eset-support.canon-its.jp/faq/show/28331?site_domain=business