ESET Server Security for Linux V10.3 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

（2024 年 9 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 V10.3（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。
- 本製品はセキュア OS の AppArmor には対応しておりません。
- 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。
- kernel 3.10.0-327/kernel 4.18.0-553/ kernel 5.14.0-427 にて実施
- AWS kernel の場合、kernel 5.10.220-209 にて実施
- SUSE Linux の場合、Kernel 5.14.0-42731 にて実施
- glibc 2.17 以降のバージョン
- elfutils-libelf-devel
（RHEL8/9, Amazon Linux2, AlmaLinux, Rocky Linux に必要）
- libselinux
（RHEL, CentOS, Amazon Linux2, AlmaLinux, Rocky Linux に必要。
最新パッケージをご利用ください）
- 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。
RHEL, CentOS, SUSE Linux, Amazon Linux2, AlmaLinux, Rocky Linux に
必要とされるパッケージ
- openssl
- kernel-devel
- gcc
- perl
- nftables
- nss-tools（SUSE Linux の場合「mozilla-nss-tools」）
- sqlite（SUSE Linux の場合「sqlite3」）
RHEL, CentOS, Amazon Linux2, AlmaLinux, Rocky Linux に
必要とされるパッケージ
- kernel-headers
SUSE Linux に必要とされるパッケージ
- kernel-default-devel
- kernel-macros
- linux-glibc-devel

※ 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/index_fs.html

オンラインヘルプ
https://help.eset.com/essl/10.3/ja-JP/

■ 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, CentOS, Amazon Linux2, AlmaLinux, Rocky Linux
- kernel, kernel-devel, kernel-headers

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

□ 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。

□　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、RHEL7/CentOS7 は「yum install glibc-common」、RHEL8/9/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/10.3/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。

□ 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

□ iptables を利用している環境で Web アクセス保護を無効にする必要性について

本製品の Web アクセス保護は iptables をサポートしておらず、iptables を利用している環境で Web アクセス保護が有効の場合、導入環境内部で稼働する Docker や内部システム等の通信を切断してしまう可能性があります。
Firewall が有効な CentOS7/RHEL7 環境は既定で iptables を利用しており影響を受ける可能性が高いです。

iptables を利用している OS では Web アクセス保護は無効に設定してください。

□ 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。

■ 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製品ホームページの Q&A をご確認ください。

ESET 製品 Q&A ページ：
https://eset-info.canon-its.jp/support/

プログラムの変更点について
https://eset-support.canon-its.jp/faq/show/27022?site_domain=server

□ 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。

■ 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://eset-info.canon-its.jp/business/

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

オンラインヘルプ
https://help.eset.com/essl/10.3/ja-JP/