

■ 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 Microsoft Windows Server V8.0
(以降、本製品と記載します) 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。
- ・ 本製品は Windows Server 2016 以降のインストールオプションである [Nano Server] へのインストールは対応していません。

■ 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/efsw/8.0/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。

□ リアルタイムファイルシステム保護のアップデート完了前の動作について

本製品をアクティベーション後、アップデートが完了するまではリアルタイムファイルシステム保護が有効になりません。本製品インストール時、必ずアクティベーションとアップデートを行なってください。

□ 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、V8用ミラーツールを使用するか、ESET Endpoint Security V7/V8、ESET Endpoint アンチウイルス V7/V8、ESET Server Security for Microsoft Windows Server V7/V8 のいずれかでミラーサーバーを作成する必要があります。

□ SSL/TLS プロトコルフィルタリングの「証明書の有効性を確認する」設定の挙動について

SSL/TLS プロトコルフィルタリングの「証明書の有効性」において、「証明書の有効性を確認する」を選択している場合でも、証明書の有効性が確認できない Web サイトへアクセスした際に、確認ダイアログを表示しない仕様に変更になりました。

該当 Web サイトへのアクセス可否につきましては、ブラウザにてご対応ください。

□ IIS を使用して検出エンジンを公開する際の動作について

本製品で自己防衛が有効な状態で、検出エンジンを IIS で公開する場合、既定のストレージフォルダを使用すると MIME の設定で「エラー：アクセス許可がないため構成ファイルを書き込むことができません」とメッセージが表示され IIS での公開ができません。

自己防衛を無効にするか、既定フォルダ以外の任意のフォルダを指定することで本事象を回避できます。

- インストールオプションの「修正」および「修復」について

インストールオプションの「修正」および「修復」は利用できません。実行しようとする「このコンピュータでは、ユーザーによるインストールはポリシーで無効になっています。」というメッセージが表示されます。

- 「Azure Code Signing (ACS)」準拠について

本製品は Azure Code Signing (ACS) で署名されているため、本製品をインストールする際は OS によって事前に対応が必要となります。

詳細は、以下の URL を確認ください。

https://eset-support.canon-its.jp/faq/show/25954?site_domain=business

- ESET File Security for Microsoft Windows Server 旧バージョンから本製品への引き継がれない項目について

ESET File Security for Microsoft Windows Server V7.3 から本製品への上書きインストールにおいて、以下の項目が引き継がれずに、本製品の既定値となる事を確認しています。

[ネットワーク保護]-[ネットワーク攻撃保護]-[IDS ルール]

・「カスタムアラート」のルール

[ユーザーインターフェース]-[アプリケーションステータス]

・ネットワーク攻撃保護 (IDS) が機能していません

- ESET File Security for Microsoft Windows Server 旧バージョンから本製品への上書きインストール時に表示されるアラートについて

ESET File Security for Microsoft Windows Server 旧バージョンから本製品への上書きインストール後に、「再起動する必要があります」とアラートが表示され、HIPS、Web アクセス保護、フィッシング対策保護の機能、ネットワーク攻撃保護 (IDS)、アンチステルスが上書きインストール前に有効の場合に、該当の機能が停止されることがあります。

本アラートはサーバーの再起動を行なうことで解消されます。
上書きインストール後は、必ずサーバーの再起動を行なってください。

■ 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/2293?site_domain=business

- ミラーサーバー機能で、HTTPS 接続のための証明書を指定するとミラーサーバーに接続できない現象について

本製品で HTTPS のミラーサーバーを構築する際、以下の設定項目の「サーバ秘密鍵のタイプ」で「統合」を指定すると、HTTPS ミラーサーバーが起動せず、このミラーサーバーに対して HTTPS 接続を行なうと「サーバーに接続できません」というエラーが表示されます。

[アップデート]-[プロファイル]-[アップデートミラー]-[HTTP サーバー]-[HTTP サーバーの SSL]

本製品で HTTPS のミラーサーバー機能をご利用の際は、「サーバ秘密鍵のタイプ」で「統合」以外のタイプを使用してください。

- Office 365 アカウントに二要素認証が設定されていると OneDrive 検査のアカウント登録に失敗する現象について

二要素認証が設定されている Office 365 アカウントを OneDrive 検査に登録すると、アカウント登録に失敗する現象を確認しています。

□ アンインストール後の再インストールが失敗する現象について

アンインストール後の再インストールが失敗する現象を確認しています。アンインストール時に、アンインストールツールを使用する。もしくは、アンインストール時に残ってしまうデータ「C:\ProgramData\ESET\ESET Security」を手動で削除してください。

□ 本製品の再起動ボタンをクリックしても OS が再起動しない現象について

Windows Server 2019 以降でビルドイン Administrator ではない管理者アカウントを使用している場合、バージョンアップ後等に本製品の再起動ボタンをクリックしても OS が再起動しない場合があります。現象が発生した場合は、OS 側の操作で再起動を行ってください。

■ 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/>

オンラインヘルプ

<https://help.eset.com/efsw/8.0/ja-JP/>