

■ 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 V11.0
(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/11.0/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、V11 用ミラーツール (ep11 フォルダ)を使用するか、ESET Endpoint Security V11、ESET Endpoint アンチウイルス V11、ESET Server Security for Microsoft Windows Server V11 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。

□ 本製品をミラーサーバーとして使用する場合について

本製品をミラーサーバーとして使用する場合、アップデートが可能な製品バージョンは、V11 のみとなります。

□ 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。

□ 自動アップデート機能について

本製品は、自動アップデート機能が既定で有効となっています。

自動アップデートを無効にしたい場合、以下より設定を無効化してください。※

[アップデート]-[基本]-[製品のアップデート]-[自動アップデート]

※リモート管理製品（ESET PROTECT または ESET PROTECT on-prem）で本製品を管理している場合は、管理製品でポリシーを用いて無効化設定を行う必要があります。

□ 「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 V7.3 から本製品への上書きインストール時に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

[Web とメール]-[SSL/TLS]

・SSL/TLS プロトコルフィルタリングを有効にする

[診断]-[診断]-[詳細ログ]

- ・オペレーティングシステム詳細ログを有効にする
- ・メモリ追跡を有効にする

- ESET Server Security for Microsoft Windows Server V8.0 から本製品への上書きインストール時に引き継がれない項目について

ESET Server Security for Microsoft Windows Server V8.0 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。

[Web とメール]-[SSL/TLS]

- ・SSL/TLS プロトコルフィルタリングを有効にする

[診断]-[診断]-[詳細ログ]

- ・オペレーティングシステム詳細ログを有効にする
- ・メモリ追跡を有効にする

[アップデート]-[プロファイル]-[製品のアップデート]

- ・アップデートモード※

※製品の[アップデート]-[基本]-[自動アップデート]に設定が引き継がれません。

- ESET Server Security for Microsoft Windows Server V9.0 から本製品への上書きインストール時に引き継がれない項目について

ESET Server Security for Microsoft Windows Server V9.0 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。

[診断]-[診断]-[詳細ログ]

- ・オペレーティングシステム詳細ログを有効にする
- ・メモリ追跡を有効にする

- 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

て

旧バージョンから本製品への上書きインストール後に、「デバイスを再起動する必要があります」とアラートが表示され、リアルタイムファイルシステム保護等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。

□ 脆弱性パッチ適用時のサーバー再起動について

本製品に付帯する「脆弱性とパッチ管理」機能でサーバーの再起動設定はできません。

リモート管理製品（ESET PROTECT または ESET PROTECT on-prem）のポリシー設定画面には「コンピューターの再起動オプション」が表示されますが、本オプションは無効です。

コンピューターの再起動は手動で実施してください。

□ ESET Inspect コネクターのアクティベーションについて

リモート管理製品（CT または ESET PROTECT on-prem）で管理された環境に本製品と ESET Inspect コネクターをインストールし、ESET Inspect コネクターのアクティベーションタスクを実行した際、管理コンソール画面のタスク履歴に「セキュリティ製品：タスクが失敗しました」と表示される場合があります。

このメッセージが表示された場合であっても、ESET Inspect コネクターのアクティベーションが成功することを確認しています。

タスク履歴に「セキュリティ製品：タスクが失敗しました」と表示された場合は、管理コンソール画面で「製品及びライセンス」欄に本製品と ESET Inspect コネクターが反映されていることを確認してください。

■ 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。

- 「変更された電子メール」機能が単独で動作しない現象について

電子メールクライアント保護の検査対象メールのうち、「変更された電子メール」を単独で有効にしても、検査が正常に動作しない現象を確認しています。

検査対象メールの項目は、すべて有効の状態でご使用ください。

- サーバーコア環境における除外パスの設定について

サーバーコア環境で本製品の検出除外およびパフォーマンス除外の対象となるパスを設定する際、フォルダ・ファイル選択のダイアログボックスが機能しない事象を確認しています。

除外パスを設定する際は、目的のパスをテキストボックスに直接入力してください。

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/11.0/ja-JP/>