ESET Server Security for Microsoft Windows Server V12.0 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 2 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 Microsoft Windows Server V12.0（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/12.0/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、V12 用ミラーツール(ep12 フォルダ)を使用するか、ESET Endpoint Security V12、ESET Endpoint アンチウイルス V12、ESET Server Security for Microsoft Windows Server V12 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、V12 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現象を回避できます。

□　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 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。

[通知]- [アプリケーションステータス]- [フィッシング対策機能]
・フィッシング対策機能が無効です

□ 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。

[ツール]-[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

[通知]- [アプリケーションステータス]- [フィッシング対策機能]
・フィッシング対策機能が無効です

□ ESET Server Security for Microsoft Windows Server V10.0 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 V10.0 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

[通知]- [アプリケーションステータス]- [フィッシング対策機能]
・フィッシング対策機能が無効です

□ ESET Server Security for Microsoft Windows Server V11.0 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 V11.0 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

[通知]- [アプリケーションステータス]- [フィッシング対策機能]
・フィッシング対策機能が無効です

[ネットワークアクセス保護]- [ネットワーク攻撃保護]- [詳細設定オプション] - [侵入検出]
・ARP ポイズニング攻撃を検出
・TCP ポートスキャニング攻撃を検出
・UDP ポートスキャニング攻撃を検出

□ ESET Server Security for Microsoft Windows Server V11.1 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 V11.1 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

[ネットワークアクセス保護]- [ネットワーク攻撃保護]- [詳細設定オプション] - [侵入検出]
・ARP ポイズニング攻撃を検出
・TCP ポートスキャニング攻撃を検出
・UDP ポートスキャニング攻撃を検出

□ 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

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。コンピューターの再起動は手動で実施してください。

□ リモートデスクトップ接続の接続元を制限する設定について

本製品を新規でインストールし、ファイアウォール機能が使用できないライセンスでアクティベーションした場合、本製品がインストールされている端末に対して、リモートデスクトップ接続の接続元を制限する設定が既定で行われます。

本製品がインストールされている端末に対してリモートデスクトップ接続が必要な場合は、以下項目を適切な値に設定し、必要なリモートデスクトップ接続が遮断されないように設定してください。

[ネットワークアクセス保護]-[ネットワーク攻撃保護]-[総当たり攻撃保護]
・受信 RDP 接続を制限

□ ネットワーク隔離からの除外について

ネットワーク隔離からの除外が機能するためには、ESET Management エージェント（以降、EM エージェント）が本製品を認識する必要があります。ネットワーク隔離からの除外の機能を使用したい場合は、EM エージェントをインストールした後に本製品をインストールしてください。もし本製品を EM エージェントより先にインストールしていた場合は OS を再起動して EM エージェントに本製品を認識させてください。

■ 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。

■ 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/12.0/ja-JP/