ESET Server Security for Microsoft Windows Server V13.1 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

（2026 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 Microsoft Windows Server V13.1（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/13.1/ja-JP/

■ 旧バージョン（V13.0）からの変更点ついて
以下の機能が追加されました。

□ ランサムウェア修復のバックアップ管理

ランサムウェア保護によりバックアップされたファイルが本製品から確認可能となり、復元や削除が実行できるようになりました。

□ ランサムウェア修復のボリューム単位のバックアップ

ランサムウェア保護によりバックアップされるフォルダがドライブ単位で自動生成されるようになりました。

□ 検査プロファイルの UUID 利用をサポート

検査プロファイルに割り当てられている UUID を利用して、検査プロファイルを指定可能になりました。UUID は eShell から確認可能です。

□ eShell のスケジュールされたタスクに新規レコード追加

eShell のスケジューラーに登録されているタスクに「次回の実行」のレコードが追加されました。

□ 新しいインストールタイプの追加

上書きインストール時に「現在」というインストールタイプが選択できるようになりました。これにより、旧バージョンで導入されているコンポーネントが上書きインストール後も保持できるようになりました。

以下の機能が変更されました。

□ イベントログの履歴出力

隔離ファイルを手動で復元時に、イベントログへ履歴が出力されるようになりました。

□　デフォルトのハッシュアルゴリズムの変更

デフォルトのハッシュアルゴリズムとして SHA256 が採用されました。
これにより検出ログなどに出力されるハッシュ情報も SHA256 のものに変更されます。

□　インストールコンポーネントツリーの再編成

カスタムインストール時に表示されるプログラムコンポーネントの構成が変更されました。

■　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。

□　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、V13 用ミラーツール(ep13 フォルダ)を使用するか、ESET Endpoint Security V13、ESET Endpoint アンチウイルス V13、ESET Server Security for Microsoft Windows Server V13 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、V13 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 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

[通知]- [アプリケーションステータス]- [WEB とメール]
・Web アクセス保護が無効になっています

□ 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
・フィッシング対策機能が機能していません（ネットワークトラフィックスキャナーが無効）

[通知]- [アプリケーションステータス]- [WEB とメール]
・Web アクセス保護が無効になっています

□ 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

[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機能していません（ネットワークトラフィックスキャナーが無効)

□ ESET Server Security for Microsoft Windows Server V12.0 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 V12.0 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機能していません（ネットワークトラフィックスキャナーが無効)

□ ESET Server Security for Microsoft Windows Server V12.1 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 V12.1 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

[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機能していません（ネットワークトラフィックスキャナーが無効)

□ ESET Server Security for Microsoft Windows Server V13.0 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 V13.0 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

□ 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。

□　利用規約への同意について

本製品を旧バージョンからアップデートする場合、利用規約への同意が必要となります。必ず同意いただいてからアップデートを実施してください。

□　脆弱性とパッチ管理機能を有効化時の一時的なアラート

脆弱性とパッチ管理機能を有効化すると、「脆弱性管理機能が動作していません」とアラートが発生します。アラートは数分後に解消され、その後の動作に問題ないことを確認しております。

□　ランサムウェア修復機能について

ランサムウェア修復機能は、Windows Server 2019 以降の OS で動作します。
また、ランサムウェア修復が機能するためには、ESET PROTECT Advanced 以上のライセンスと、EM エージェントを本製品が認識する必要があります。本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、再アクティベーション行ってください。

■　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 FAQ サイトのご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

□ 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。

□ PAC ファイルを指定したプロキシ通信について

[接続]-[プロキシサーバ]-[PAC ファイルの URL] にて PAC ファイルを指定したプロキシ通信を実施した場合、検出エンジンのアップデートが実施できない現象を確認しています。
本製品でプロキシ通信を実施する際は、[プロキシ設定モード]を「手動」に設定して使用してください。

■ 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://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/efsw/13.1/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