ESET Endpoint Security for macOS V9.0 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 10 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 Endpoint Security for macOS V9.0
（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。
- 本製品をインストールする場合は、管理者アカウントでインストールしてください。
- 本製品をインストールできる OS は、macOS 11 以降です。しかし、本製品のサポートは、macOS 26 にインストールした場合に限られます。
- インストール時にインターネットに接続している必要があります。

■ 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できます。

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/ees_mac/9/ja-JP/

■ 旧バージョン（V8.1）からの変更点について

以下の機能が追加されました。

□ デバイスコントロール

デバイスコントロール機能が追加されました。[設定]>[保護]>[デバイスコントロール]の設定画面で設定が可能です。

□ HTTPS トラフィックのスキャン

HTTPS トラフィックのスキャンができるようになりました。
[設定]>[検出エンジン]>[セキュアなトランスポートプロトコル]の設定画面で設定が可能です。

□ macOS 26 のサポート

macOS 26 に対応しました。

□ より頻繁な検出シグネチャの更新

高頻度のアップデートを可能にする設定が追加されました。既定値は有効で、管理ツールのポリシーでのみ設定が可能です。

以下の機能が変更されました。

□ 脆弱性およびパッチ管理スケジューラの再設計

管理ツールのポリシーで行う脆弱性およびパッチ管理のスケジューラの設定画面が新しくなり、より詳細な設定が可能になりました。

□ ネットワークからの隔離機能で除外設定が可能

ESET PROTECT または、ESET PROTECT on-prem v11,1 以降で利用可能なネットワークからの隔離機能で除外設定が可能になりました。

以下の不具合が修正されました。

□　フィッシング対策の警告画面が英語で表示される

フィッシング対策の警告画面が英語で表示される不具合が修正され、日本語で表示されるようになりました。

□　URL アドレス管理によるブロック時のポップアップが英語で表示される

URL アドレス管理によるブロック時のポップアップが英語で表示される不具合が修正され、日本語で表示されるようになりました。

□　arm の環境で、chrome を使用した場合、フィッシング対策保護が機能しない

arm の環境で、chrome を使用した場合、フィッシング対策保護が機能しない不具合が修正されました。

□　macOS 15 で拡張子が「.com」や「.dex」のファイルを隔離から復元したときに、ファイル名の後ろに「.c」が付加される

macOS 15 で拡張子が「.com」や「.dex」のファイルを隔離から復元したときに、ファイル名の後ろに「.c」が付加される事象が修正されました。

□　設定画面に「ネットワークプロファイル」が表示される

設定画面に、使用できない機能である「ネットワークプロファイル」が表示される事象が修正されました。

□　設定画面の「ファイアウォール」の「既定値」のボタンが機能しない

設定画面の「ファイアウォール」の「既定値」のボタンは削除されました。

■　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。

□　プログラムの統合について

従来の 2 つのプログラム（ESET Endpoint アンチウイルス for macOS と ESET Endpoint Security for macOS）が ESET Endpoint Security for macOS に一本化され、アクティベーションに使用する製品の種別によってプログラムに機能が追加されるようになりました。
「ネットワーク保護強化」の機能を使用できる製品でアクティベーションした場合のみ、「ネットワーク保護強化」の機能を使用することができます。
製品ごとの機能差異は、以下をご確認ください。

https://canon.jp/biz/solution/security/it-sec/lineup/eset/product

□　ミラーサーバーからのアップデートについて

以下の製品を使用して構築したミラーサーバーから、検出エンジン（ウイルス定義データベース）のアップデートができません。

・　ESET Endpoint Security
・　ESET Endpoint アンチウイルス
・　ESET File Security for Microsoft Windows Server

ミラーサーバーをご使用の場合は、以下の製品を使用して、ミラーサーバーを構築してください。

・　ミラーツール

本製品から.dylib モジュール用のアップデートファイルを使用します。古いバージョンのミラーツールでは、.dylib モジュール用のアップデートファイルをダウンロードすることができません。2024 年 8 月以降に公開したミラーツールをご利用ください。

□　ミラーツールのアップデート指定先フォルダについて

本製品は、「--updateServer オプション」を用いて、「http://update.eset.com/eset_upd/businessmac」からモジュールを取得してください。アップデートサーバーは、以下のように設定してください。

http://ミラーサーバーのアドレス:ポート/BusinessMac

□　旧バージョンからのバージョンアップ時に一部の設定が引き継がれない

旧バージョンからのバージョンアップ時に一部の設定が引き継がれません。
必要に応じてバージョンアップ後に設定を変更してください。セキュリティ管理ツールを使用して、本製品を管理している場合は、ポリシーを使用することで設定を変更できます。
引き継げない項目の詳細については以下をご確認ください。

https://eset-support.canon-its.jp/faq/show/4299?site_domain=business

□　スケジューラの自動設定について

セキュリティ管理ツールで本製品を管理していない場合、本製品をインストールするとスケジューラに「定期自動検査」という名前のオンデマンド検査が、インストールした数分後の時刻とインストールした曜日で自動設定されます。必要に応じて設定を変更してください。

□　その他のアクティベーションオプションについて

GUI にその他のアクティベーションオプション（ESET Business Account(以降、EBA)、オフラインライセンス）はありません。オフラインライセンスのアクティベーションは、コマンドでの実施および ESET PROTECT(以降、EP)や ESET PROTECT On-Prem (以降、EPO)からのアクティベーションタスクで可能ですが、オフラインライセンスでアクティベーションした場合は、リアルタイムファイルシステム保護だけが機能します。

□　製品の自動アップデートについて

製品の自動アップデートの既定値が有効になっています。自動アップデートが有効だと、新バージョンが出たときに本製品が自動的にバージョンアップされます。
自動でのアップデートを望まない場合は、[設定]>[更新]>[製品のアップデート]の設定画面で、[自動アップデート]の設定を無効にしてください。

□　バージョンアップ後のフルディスクアクセス権の付与について

旧バージョンからバージョンアップした後に、本製品へのフルディスクアクセス権を付与する必要があります。

□　Web コントロール機能について

本製品には Web コントロール機能は実装されておりません。

□　ファイアウォールの設定について

ファイアウォールの詳細な設定は、EP や EPO で「Common features」のポリシーのネットワークアクセス保護の設定を使用して行います。EP や EPO で管理してルールを設定しない場合は、既定のルール（外向きの通信は許可され、自身の PC から開始されたものでない内向きの通信は全てブロック）が適用されます。

□　通知が機能しない場合がある

通知が機能しないことがあります。OS 側の問題に起因しているため、発生した場合は OS の再起動を試してください。

□　コンピュータをネットワークから隔離する機能について

コンピュータをネットワークから隔離する機能は、ファイアウォールの機能を使用するため、「ネットワーク保護強化」の機能を使用できる製品でのアクティベーションが必要です。

□　セキュアなトランスポートプロトコルのフィルタリングモードについて

フィルタリングモードの設定が「自動」の場合、自動で選択されたアプリケーションに対してのみ機能します。すべてのアプリケーションを対象としたい場合は、「ポリシーベース」の設定をご利用ください。

□　デバイスコントロールの既定のルールついて

デバイスコントロールを有効にした場合、すべてのデバイスをブロックするルー

ルが既定のルールとして適用されます。必要に応じて設定を変更してください。

■ 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 FAQ サイトの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

□ Safari を使用した場合に Web アクセス保護の除外が機能しない

Safari を使用した場合に Web アクセス保護の除外が機能しないことを確認しております。Web アクセス保護の除外を使用したい場合は、他のブラウザを、ご使用ください。

□ リムーバルメディアの検査で検出後にファイルが残る事象を確認しております。

ファイルの中身は削除されていますので、同名のファイルが残る以外の影響はありません。

□ Safari に対してファイアウォールルールが適用されない

/Applications/Safari.app に対してアプリケーション固有のファイアウォールルールが正常に機能しない不具合を確認しております。

□ Web アクセス保護と電子メール保護のアクションアラートダイアログが英語で表示される

Web アクセス保護と電子メール保護のアクションアラートダイアログ（駆除レベルを「駆除なし」にして検出した時に対応を選択するダイアログ）が英語で表示されることを確認しています。

□ エンドポイント側の保護状態のアラートに関する設定値がセキュリティ管理ツールのコンソール上に反映されない

エンドポイント側の保護状態のアラートに関する設定値がセキュリティ管理ツールのコンソール上（設定のリクエストで確認できる[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]の「エンドポイントに表示」の列の設定値）に反映されない事象を確認しています。

□ 検査のタイミングで「リムーバルメディアのアクセス」を有効にした場合に実行されるリムーバブルメディアの自動検査で検出がされない

検査のタイミングで「リムーバルメディアのアクセス」を有効にした場合に実行されるリムーバブルメディアの自動検査で検出がされない事象を確認しています。リアルタイム保護やオンデマンド検査での駆除は可能です。ファイルを触る前に検査をしておきたい場合は、手動でのオンデマンドスキャンをご利用ください。

□ エンドポイント側のシステム統合に関する設定値がセキュリティ管理ツールのコンソール上に反映されない

エンドポイント側のシステム統合に関する設定値がセキュリティ管理ツールのコンソール上(設定のリクエストで確認できる[ユーザーインターフェース]配下の以下の設定に反映されない事象を確認しています。

・ユーザーがグラフィカルユーザーインターフェースを開くことを許可する
・メニューバーにアイコンを表示する
・デスクトップに通知を表示する

□ 「脆弱性およびパッチ管理」のスキャンおよびパッチ適用が機能しない

「脆弱性およびパッチ管理」のスキャンおよびパッチ適用が機能しない事象を確認しています。「脆弱性およびパッチ管理」用のライセンスを付与した時点で「機能しない」というエラーが発生します。

■ 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://canon.jp/biz/solution/security/it-sec/lineup/eset

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