ESET Endpoint Security for macOS V8.0 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

（2024 年 8 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 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 v11 以降です。
- 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/8/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。

□ 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。

製品ラインアップ｜ESET セキュリティソリューションシリーズ｜キヤノン(canon.jp)

□ 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 月に公開した新しい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。

□　デバイスコントロール機能について

本製品にはデバイスコントロール機能は実装されておりません。

□　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が、デフォルトで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、[環境設定]>[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]の設定をオフにしてください。

□　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。

□　v6 から v8 へバージョンアップした時のファイアウォールの設定ついて

v6 のファイアウォールの設定は、v8 へのバージョンアップ時に引き継ぐことができますが、設定を引き継ぐためには条件があります。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/29875?site_domain=business

□ v6 と異なるファイアウォールの仕様について

v6 と異なり、ファイアウォールの設定はアクティブな接続に対しても有効です。

□ v6 と異なる Web アクセス保護の URL アドレス管理の仕様について

v6 と異なり、Web アクセス保護の URL アドレス管理でホワイトリストのような設定（許可する URL を設定するだけで、許可した URL 以外の URL にアクセスできないようにすること）はできません。ブロックしたい URL と許可したい URL を組み合わせて設定してください。

□ 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。

□ 設定組み込み済みインストーラー（リモートインストールパッケージ）について

v6 と異なり、設定組み込み済みインストーラー（リモートインストールパッケージ）の作成はできません。リモートインストールについては、EP や EPO のソフトウェアインストールタスクなどの利用をご検討ください。

□ 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。

■ 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

□ MacOS13 以降で、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

MacOS13 以降で、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。MacOS13 以降で 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。

□ macOS13 以前の OS で、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。

□ OS 再起動後に、Licensing service に関するエラーログが記録される

OS 再起動後に、Licensing service に関するエラーログが記録されることを確認しております。
確認できているイベントメッセージは以下の通りです。

・ サーバーからデータを受信できません：ネットワークに到達できません

保護機能への影響はございませんので、このイベントログは無視してご利用いただけます。

□ v6 から本製品へバージョンアップした時に、本製品にフルディスクアクセスの許可が必要になるが、macOS11 の場合、一度 OS を再起動しないと許可することができない。

v6 から本製品へバージョンアップした時に、本製品にフルディスクアクセスの許可が必要になりますが、macOS11 の場合、一度 OS を再起動しないと許可することができないことを確認しています。macOS11 で本製品を利用する場合は、OS を再起動してからで本製品にフルディスクアクセスの許可を設定してください。

□　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ことを確認しています。

□　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ことを確認しています。

□　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。

□　macOS13 だとインストーラーの画面で、システム要件の個所が真っ白で表示されない

macOS13 だとインストーラーの画面で、システム要件の個所が真っ白で表示されないことを確認しております。白い部分をクリックすると内容が表示されるので内容を確認したい場合は、白い部分をクリックしてください。

□　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

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を確認しております。

□　EP のコンソール上で脆弱性とパッチ管理（以降、V&PM）で検出した脆弱性の詳細をコンテキストメニューで確認しようとするとエラーが発生する

EP のコンソール上で V&PM で検出した脆弱性の詳細をコンテキストメニューで確認しようとするとエラーが発生する不具合を確認しております。

□　EBA アカウントを使用したアクティベーションができない

EBA アカウントを使用したアクティベーションができない不具合を確認しており

ます。

□ ESET Inspect（以降、EI）と連携すると EI のコンソールの「ネットワーク隔離」がグレーアウトされて EI からのネットワーク隔離が使用できない

ESET Inspect（以降、EI）と連携すると EI のコンソールの「ネットワーク隔離」がグレーアウトされて EI からのネットワーク隔離が使用でき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。

■ 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/