

ESET PROTECTソリューション

ESET Endpoint Security for macOS V8

機能紹介資料

第1版

2024年8月7日

Canon

キヤノンマーケティングジャパン株式会社

もくじ

1. はじめに
 - 1-1. 本資料について

2. ESET Endpoint Security for macOS V8の機能紹介
 - 2-1. 保護機能について
 - 2-2. その他機能について

1. はじめに

1-1. 本資料について (1/2)

本資料はMacクライアント用プログラムの機能を紹介した資料です。

プログラム名	種別
ESET Endpoint Security for macOS V8 (略称表記：EESM)	Mac クライアント用 総合セキュリティプログラム

- 本資料で使用している画面イメージは、主にESET Endpoint Security for macOS V8より取得しておりますが、使用するバージョンやOSにより異なる場合があります。また、今後画面イメージや文言が変更される可能性があります。
- V8より、ESET Endpoint Security for OS X と ESET Endpoint アンチウイルス for OS X の表記による区別はなくなり、ESET Endpoint Security for macOSの表記に統一されました。
ただし、表記はESET Endpoint Security for macOS であっても機能はこれまでのESET Endpoint Security for OS X と ESET Endpoint アンチウイルス for OS X のように保有ライセンス種別により区別されます。
- オフラインライセンスファイルにてアクティベーションした場合は「リアルタイム保護」のみ機能します。
- セキュリティ管理ツール(ESET PROTECT ※以降EP、ESET PROTECT on-prem ※以降EP on-prem)で管理が可能です。
セキュリティ管理ツールで管理可能なプログラムや対応OSにつきましては下記をご参照ください。
■セキュリティ管理ツールで管理可能なクライアント用プログラムは？
https://eset-support.canon-its.jp/faq/show/143?site_domain=business
- ESET PROTECTソリューションではWindows、Linux、Android OS向けのプログラムもご使用いただけます。各プログラムやセキュリティ管理ツールの機能紹介は別資料をご用意しています。

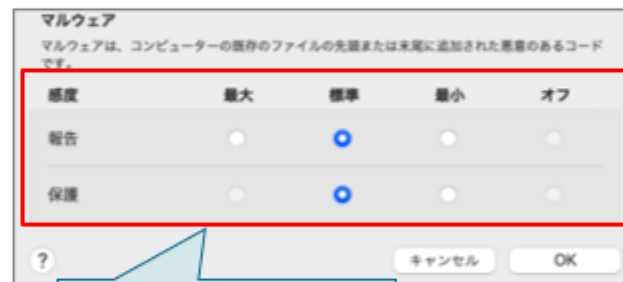
1-1. 本資料について (2/2)

機能名を記載して
おります。

2-1-1. エンジン感度

エンジン感度では、コンピューターのパフォーマンスを低下させる恐れのあるアプリケーションや不正利用される可能性のあるアプリケーションを検出させるかどうかを設定することなどが可能です。

詳細設定 (エンジン感度機能)



機能についての説明と
機能に関する画像を
掲載しております。

マルウェア	コンピューターの既存のファイルに含まれる悪意のあるコードを検出します。
不審なアプリケーション	圧縮されたプログラムが含まれます。マルウェアの作成者が検知をのぼれるために使用する手法です。
疑わしい可能性があるアプリケーション	必ずしも悪意があるとは限りませんが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があるアプリケーションを指します。
安全ではない可能性があるアプリケーション	リモートアクセスツールやパスワード解析ツールなど適正なアプリケーションではあるものの悪用される可能性もあるアプリケーションを検出します。

2. ESET Endpoint Security for macOS V8

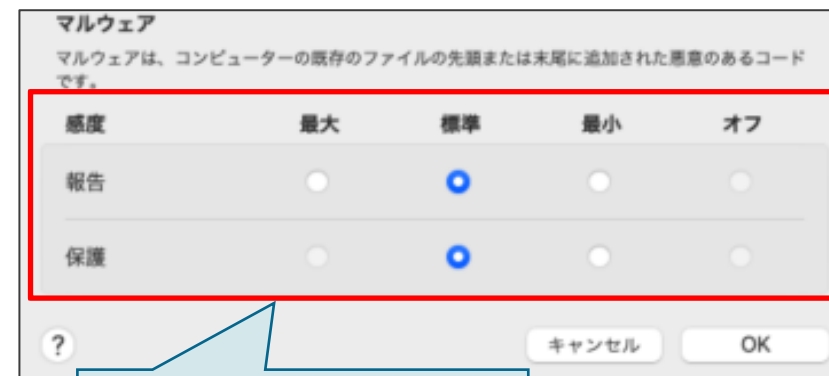
機能紹介

2-1. 保護機能について

2-1-1. エンジン感度

エンジン感度では、コンピューターのパフォーマンスを低下させる恐れのあるアプリケーションや不正利用される可能性のあるアプリケーションを検出させるかどうか設定することなどが可能です。

詳細設定 (エンジン感度機能)



項目ごとにエンジン感度を任意に設定することができます。

マルウェア	コンピューターの既存のファイルに含まれる悪意のあるコードを検出します。
不審なアプリケーション	圧縮されたプログラムが含まれます。マルウェアの作成者が検知から逃れるために使用する方法です。
疑わしい可能性があるアプリケーション	必ずしも悪意があるとは限りませんが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があるアプリケーションを指します。
安全ではない可能性があるアプリケーション	リモートアクセスツールやパスワード解析ツールなど適正なアプリケーションではあるものの悪用される可能性もあるアプリケーションを検出します。

2-1-2. ファイルシステム保護

リアルタイムファイルシステム保護は、ファイルとオブジェクトを悪意のあるコードから保護します。検査するメディア、検査タイミングについて任意の設定をすることができます。

詳細設定（ファイルシステム保護機能）



リアルタイムファイルシステム保護
リアルタイムファイルシステム保護は、ファイルとオブジェクトを悪意のあるコードから保護します。

検査するメディア

- ローカルドライブ
- リムーバブルメディア
- ネットワークメディア

検査のタイミング

- ファイルのオープン
- ファイルの作成
- リムーバブルメディアのアクセス

プロセスの除外

検査対象外とするプロセス >

ThreatSenseパラメータ
これらは検査エンジンの詳細設定です。上級ユーザーの場合にのみ、変更してください。最適な保護とパフォーマンスのためには、既定値を変更しないでください。

検査するメディアを設定できます。検査するメディアは「ローカルドライブ」「リムーバブルメディア」「ネットワークメディア」より指定します。

検査タイミングを設定できます。検査タイミングは「ファイルのオープン」「ファイルの作成」「リムーバブルメディアのアクセス」より指定します。

詳細設定（ThreatSense保護パラメータ）



駆除レベル 厳密な駆除

このモードでは、システムファイルを除く感染したファイルが自動的に駆除または削除されます。

検査オプション >

検査対象外とするファイル拡張子 >

キャンセル OK

検査レベルを設定できます。検査タレベルは「駆除なし」「標準駆除」「厳格な駆除」「完全な駆除」「駆除」より指定します。

2-1-3. Webアクセス保護

Webアクセス保護はHTTP経由のすべての通信トラフィックの検査を行います。悪意のあるコンテンツが含まれるWebサイトへのアクセスをブロックします。

また、Webサイトの読み込み時に悪意のあるコンテンツを検出するとアクセスをブロックします。任意のURLを登録することでWebサイトへの接続を許可/ブロックすることも可能です。

詳細設定 (Webアクセス保護機能)

Webアクセス保護

Webアクセス保護では、ThreatSense検査技術を利用して、HTTPアプリケーションプロトコル経由で移行されたデータをフィルタリングできます。

Webプロトコル

HTTPプロトコルのチェック

HTTPプロトコルが使用するポート

URLアドレス管理

URLアドレス/マスクリストを使用すると、ブロック、許可、またはコンテンツ検査から除外するアドレスを指定できます(他のフィルタリングは通常通り実行されます)。特定のリストはタイプ別にグループ化されます。

- 許可されたアドレス >
- ブロックされたアドレス >
- 除外されたIPアドレス >

ThreatSenseパラメータ

これらは検査エンジンの詳細設定です。上級ユーザーの場合にのみ、変更のためには、既定値を変更しないでください。

通信中の検査を行う場合は、チェックを入れます。
※既定値は有効です。

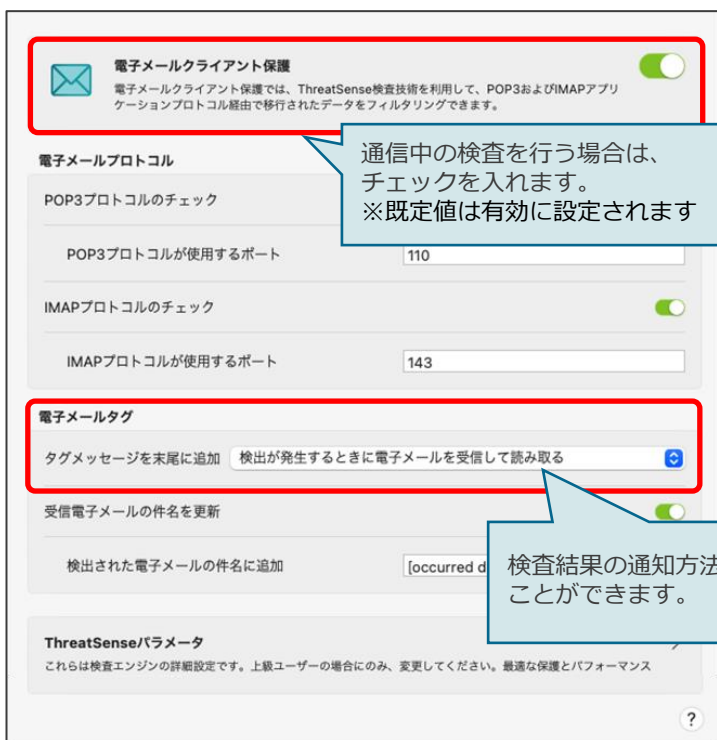
アドレスリスト	動作
許可されたアドレス	URLアドレス/マスクリストを使用して、プロトコルコンテンツフィルタリングを許可するアドレスを指定できます。
ブロックされたアドレス	URLアドレス/マスクリストを使用して、プロトコルコンテンツフィルタリングを拒否するURLのリストを指定します。
除外されたIPアドレス	URLアドレス/マスクリストを使用して、マルウェア検査から除外するアドレスを指定できます。

許可/ブロック/除外するアドレスを設定することができます。

2-1-4. 電子メールクライアント保護

電子メールクライアント保護では、POP3/IMAP プロトコルで受信したメール通信を検査します。検査後、検査結果をメール本文の最後(フットノート)にメッセージを追加したり、感染メールの件名に注釈を追加することが可能です。

詳細設定 (電子メールクライアント保護機能)



電子メールクライアント保護

電子メールクライアント保護では、ThreatSense検査技術を利用して、POP3およびIMAPアプリケーションプロトコル経由で移行されたデータをフィルタリングできます。

電子メールプロトコル

POP3プロトコルのチェック

POP3プロトコルが使用するポート: 110

IMAPプロトコルのチェック

IMAPプロトコルが使用するポート: 143

電子メールタグ

タグメッセージを末尾に追加 検出が発生するときに電子メールを受信して読み取る

受信電子メールの件名を更新

検出された電子メールの件名に追加 [occurred d

ThreatSenseパラメータ

これらは検査エンジンの詳細設定です。上級ユーザーの場合にのみ、変更してください。最適な保護とパフォーマンス

通信中の検査を行う場合は、チェックを入れます。
※既定値は有効に設定されます

検査結果の通知方法を選択することができます。

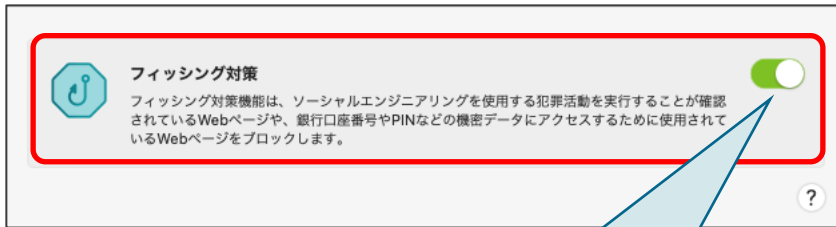
電子メールタグ	動作
しない	検査通知を追加しません。
検出が発生するときに電子メールを受信して読み取る	有害なソフトウェアなどを含むメールのみに検査結果を追加します。
検査時にすべての電子メール	検査したすべてのメールに検査通知を追加します。

※HTMLメールやメール本文自体がマルウェアで偽装されている場合、検査メッセージが追加されないことがあります。

2-1-5. フィッシング対策保護

フィッシング対策機能を有効にすることでフィッシングサイトへのアクセスをブロックできます。フィッシングとは、ソーシャルエンジニアリング（機密情報を入手するためにユーザーを操ること）を用いる犯罪行為です。フィッシングは銀行の口座番号やPIN コードなどの機密データを入手するためによく使用されます。

詳細設定（フィッシング対策）



フィッシング対策を行う場合は、
チェックを入れます。
※既定値は有効に設定されます。

フィッシングサイトの疑いのあるページを検出した場合警告画面



推奨はいたしません、[警告を無視]
をクリックすることでWebサイトへ接続
が可能です。

※フィッシング

実在する会員制のインターネットサービスなどを装い、利用者からIDやパスワード、クレジットカード情報、暗証番号などの個人情報を窃取する不正行為を意味します。詳細はマルウェア情報局 キーワード辞典を参照ください。 http://canon-its.jp/eset/malware_info/term/ha/002.html


2-1-6. ファイアウォール

ファイアウォールは、システムで送受信されるすべての通信トラフィックを検査し指定したフィルタリングルールに基づいて個々のネットワーク接続を許可またはブロックします。

※ファイアウォール設定は、ESET PROTECT On-PremまたはESET PROTECTを使用してリモートで管理されているエンドポイントに対してのみ使用可能です。

※本機能は旧ラインアップであるEssentialライセンスをご利用の場合、お使いいただけません。

設定 (ファイアウォール)



ファイアウォール

ファイアウォールは、システムとの間のすべてのネットワークトラフィックを制御します。これは、指定されたフィルタリングルールに基づいて個々のネットワーク接続を許可または拒否することによって実現されます。

詳細設定 (ファイアウォール)

ESET PROTECT On-PremまたはESET PROTECTのポリシーにより、ファイアウォールを詳細に設定できます。

Common features

アップデート

ネットワークアクセス保護

 接続
 子管理

ネットワークアクセス保護

- ネットワーク接続プロファイルの割り当て 自動
- ネットワーク接続プロファイル 編集
- IPセット 編集

ファイアウォール

- ファイアウォールを有効にする [トグル]
- ルール 編集
- Windowsファイアウォールのルールも評価 [トグル]
- フィルタリングモード ルール付き自動モード
- 自動モードでは、すべてのネットワーク通信を自動的に評価します。外向きの通信はすべて許可され、このコンピューターから開始されたものではない内向きの通信はすべてブロックされます。
- 学習モードの終了時刻 1970 1月 1 09:00:00
- 学習モードの期限切れの後に設定されるモード ユーザーに確認する
- 学習モード設定 編集

製品共通のポリシー「Common features」の「ネットワークアクセス保護」で行う。

2-2. その他機能について

2-2-1. アプリケーションステータス

ESETアプリケーションに表示されるアプリケーションステータスを設定できます。設定をおこなうことで、必要な情報だけ表示させることができます。

アプリケーションステータス(詳細画面)

アプリケーションステータス

ESETセキュリティ製品に表示されるアプリケーションステータスを選択します。特定のアプリケーションステータスを有効または無効にし、最も重要な情報だけを表示できます。

- ライセンス >
- macOS統合 >
- アップデート >
- 検出エンジン >
- 保護 >

表示させたいアプリケーションステータスを設定することができます。



保護状態

ESETセキュリティ製品に表示されるアプリケーションステータスを選択します。[エンドポイントに表示]がオフになっている問題が表示されると、ESETセキュリティ製品は緑色の「OK」ステータスを保持します。

ステータスの表示

- フィッシング対策機能が無効です
- 電子メール保護は無効です
- 電子メール保護が機能していません
- Webアクセス保護が無効になっています
- Webアクセス保護が機能していません
- ファイアウォールが無効です
- ネットワークアクセス保護が機能していません

2-2-2. 製品のアップデート

製品のアップデートは、自動的に新しいバージョンの製品をインストールする機能です。
こちらの設定が有効な場合、製品のアップデートは次回再起動時に自動的におこなわれます。

詳細設定 (製品のアップデート設定)

製品のアップデート
製品のアップデートは、常に最新の製品バージョンを使用していることを保証します。自動更新設定を有効にしておくと、最新の機能に常にアクセスでき、最高レベルの保護が適用されます。

自動アップデート 
自動アップデートが有効な場合、製品のアップデートは次回の再起動時に自動的にインストールされます。

カスタムサーバー

ユーザー名

パスワード
[パスワードを表示](#)

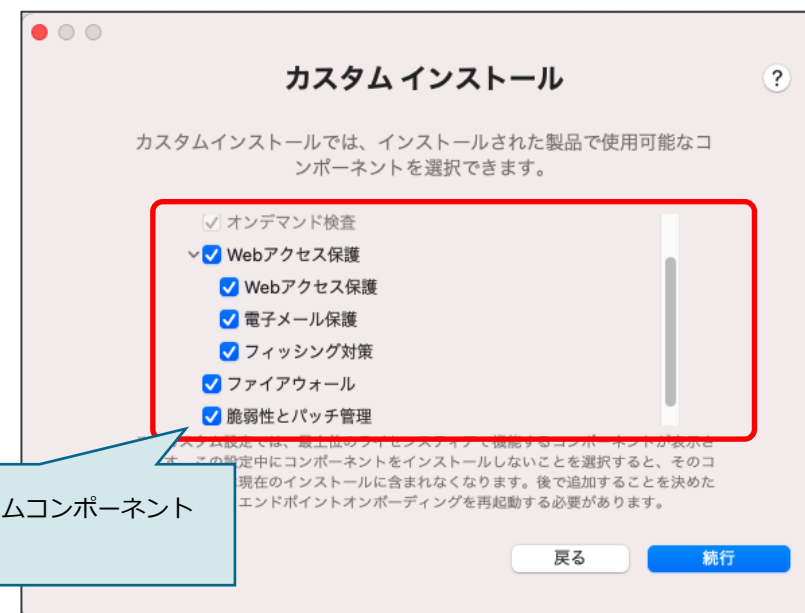
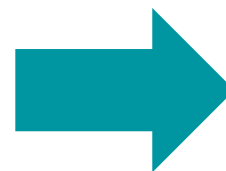
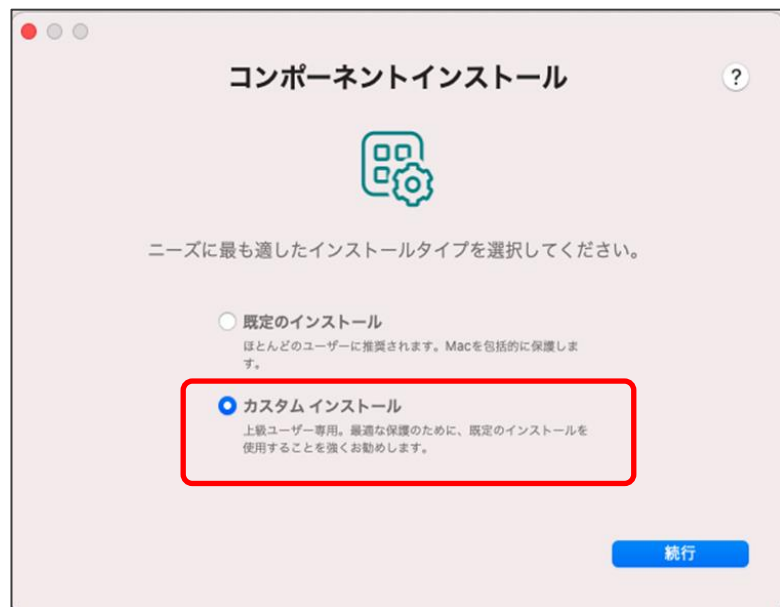


製品のアップデートの可否を設定することができます。

2-2-3. コンポーネントを指定したインストール

インストール時に有効にするプログラムのコンポーネントを指定してインストールすることができます。特に指定がない場合は「既定のインストール」を選択して、インストールしてください。

コンポーネントインストール(プログラムコンポーネントの選択)



有効にするプログラムコンポーネントを選択できます。

2-2-4. ロールバック機能

検出エンジン、および、プログラムモジュールを以前のバージョンへロールバックすることができます。スナップショットを作成することができ、ローカルに保存された一番古いバージョンに戻すことができます。また、管理者によって、セキュリティ管理ツールから任意のコンピューター（複数可）に対して、ロールバックさせたり、コンピューターのアップデートを止めておくことができます。

詳細設定（アップデート設定）

モジュールロールバック

モジュールのアップデートの問題が発生した場合は、前のスナップショットに戻すことができます。モジュールロールバックによって、モジュールが最も古いスナップショットで置換され、サーバーからのモジュールのアップデートのダウンロードが一時停止されます。

モジュールのスナップショットを作成

ロールバック機能で使用する検出エンジンとプログラムモジュールのスナップショットを記録します。

ローカルに保存するスナップショットの数 ↑ ↓

ロールバック 履歴で最も古いバージョンにロールバック

許可 アップデートサーバーからアップデート中

ローカルに保存するスナップショットの数を指定します。

2-2-5. 遅延アップデート

検出エンジンのアップデート方法に、最新の検出エンジンにアップデートする「通常アップデート」以外に、最新から12時間遅れの検出エンジンを配信する特別なアップデートサーバーを、利用できます。

詳細設定 (アップデート設定)

モジュールアップデート

モジュールのアップデートは、利用可能な最も高いセキュリティに常にアクセスできます。モジュールは定期的に自動的にアップデートされます。また、いつでも手動でアップデートできます。

- 更新タイプ
- 通常アップデート
 - リリース前アップデート
 - 遅延アップデート
- モジュール

最新から12時間遅れでアップデートする場合には、アップデートの種類から「遅延アップデート」を選択します。

モジュールのアップデートの問題が発生した場合は、前のスナップショットに戻ることができます。モジュールロールバックによって、モジュールが最も古いスナップショットで置換され、サーバーからのモジュールのアップデートのダウンロードが一時停止されます。