ESET PROTECTソリューション
ESET Endpoint Security for OS X V6 /
ESET Endpoint アンチウイルス for OS X V7
機能紹介資料

第14版

2023年10月20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 OS X V6/ESET Endpoint アンチウイルス OS X V7の機能紹介

2-1. ユーザーインターフェースについて

2-2. 保護技術・保護機能について

2-3. 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	アイコン
ESET Endpoint Security for OS X V6 (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	EESM
ESET Endpoint アンチウイルス for OS X V7 (略称表記：EEAM)	Mac クライアント用 ウイルス・スパイウェア対策プログラム	EEAM

・本資料で使用している画面イメージは、主にESET Endpoint アンチウイルス for OS X V7.4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ございます。

・セキュリティ管理ツール(ESET PROTECT Cloud ※以降EPC、ESET PROTECT ※以降EP)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でご用意しています。

1-1. 本資料について (2/2)

機能名を記載しております。

紹介されている機能がどちらのプログラムに搭載されているか示しております。

2-2-1. Webアクセス保護

EESM
EEAM

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）

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。

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。

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。

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。

2. ESET Endpoint Security for OS X V6 / ESET Endpoint アンチウイルス OS X V7 機能紹介

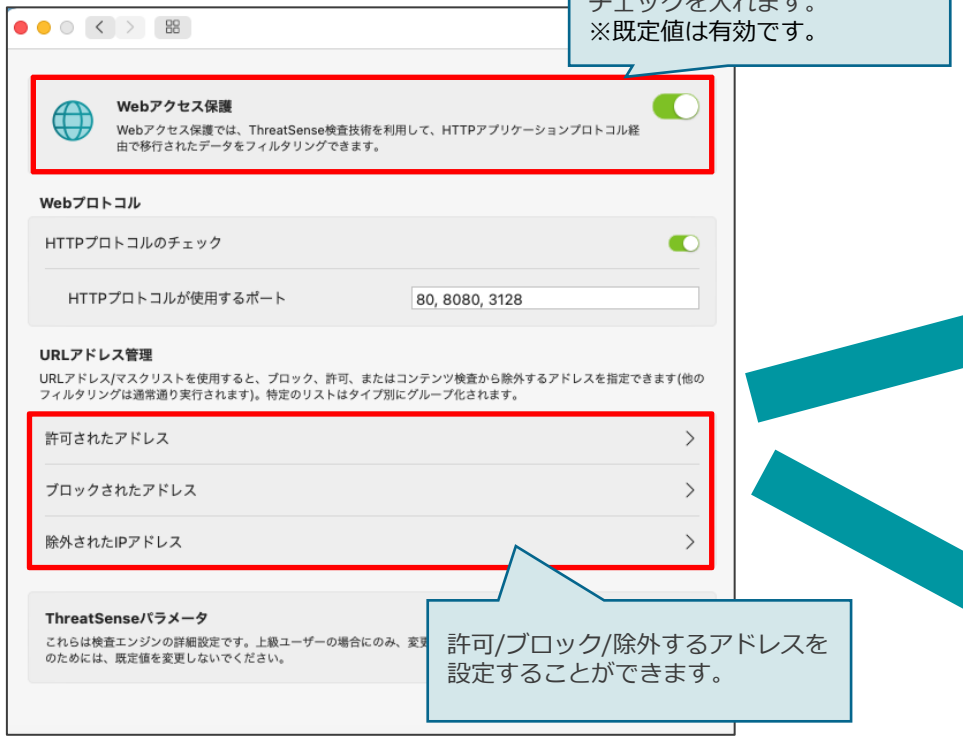
2-1. 保護技術・保護機能

2-1-1. Webアクセス保護

EESM
EEAM

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）



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。

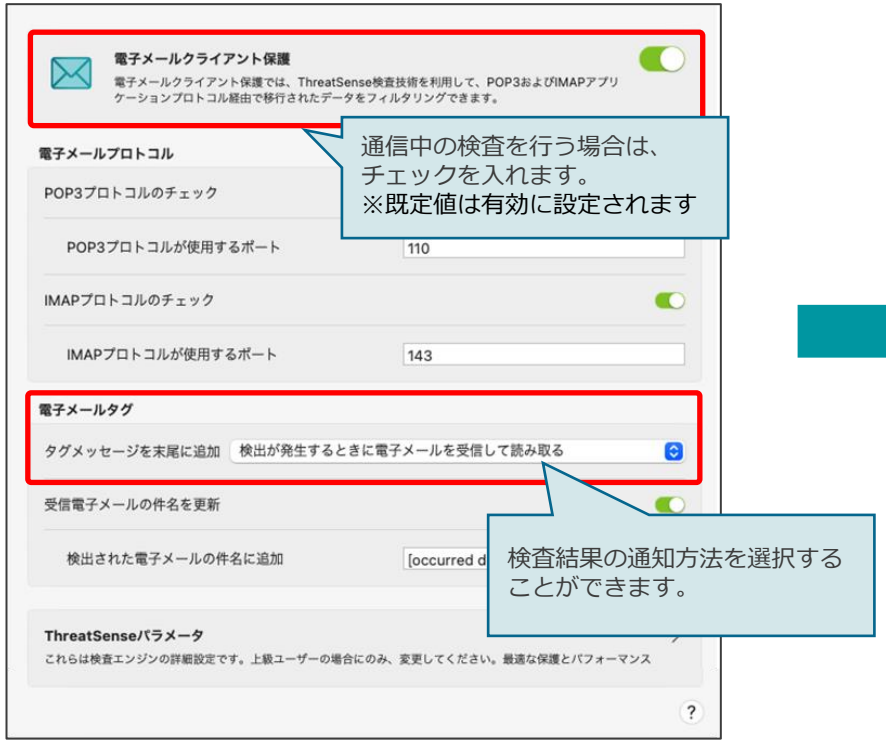
2-1-2. 電子メールクライアント保護

EESM
EEAM

Digital Security
Progress. Protected.

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。

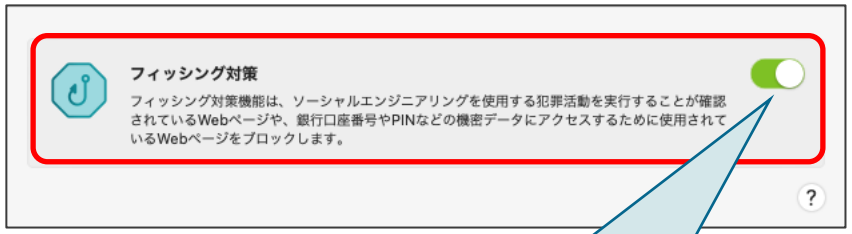
2-1-3. フィッシング対策保護

EESM
EEAM

Digital Security
Progress. Protected.

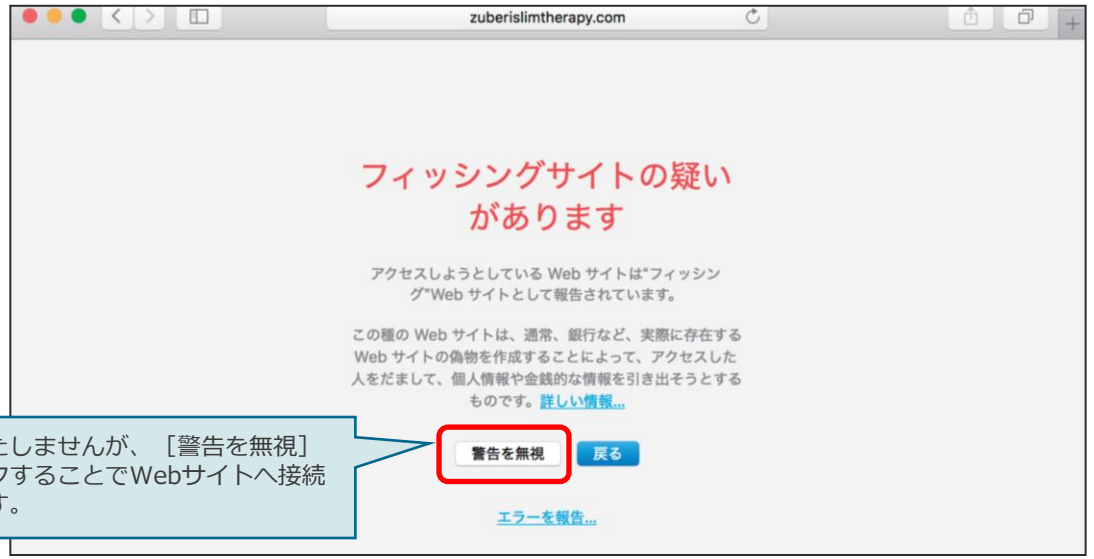
フィッシングとは、ソーシャルエンジニアリング（機密情報を入手するためにユーザーを操ること）を用いる犯罪行為です。
フィッシングは銀行の口座番号やPIN コードなどの機密データを入手するためによく使用されます。
フィッシング対策機能を有効にすることでフィッシングサイトへのアクセスをブロックできます。

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が、［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

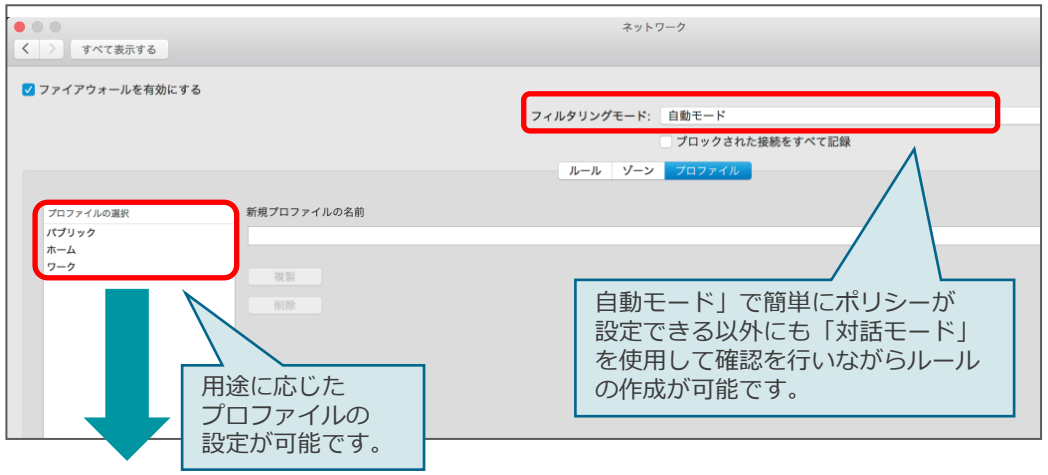
2-1-4. パーソナルファイアウォール

EESM

Digital Security
Progress. Protected.

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。

詳細設定（ファイアウォール）



フィルタリングモード	動作
すべての通信をブロック	すべての通信をブロックします。
自動モード（既定値）	全ての送信トラフィックを許可します。リモート側から開始された接続をブロックします。
対話モード	通信が検出された際に、該当するルールが無い場合はダイアログボックスを表示して通信の可否を選択します。選択結果を自動登録することが可能です。

プロファイル	動作
パブリック	全ての外向き通信を許可しますが、内向き通信は限定します。
ホーム	自宅で利用するのに適した設定を行い、全てのローカルサブネット通信は許可します。
ワーク	職場に利用するのに適した設定を行い、全てのローカルサブネット通信は許可します。

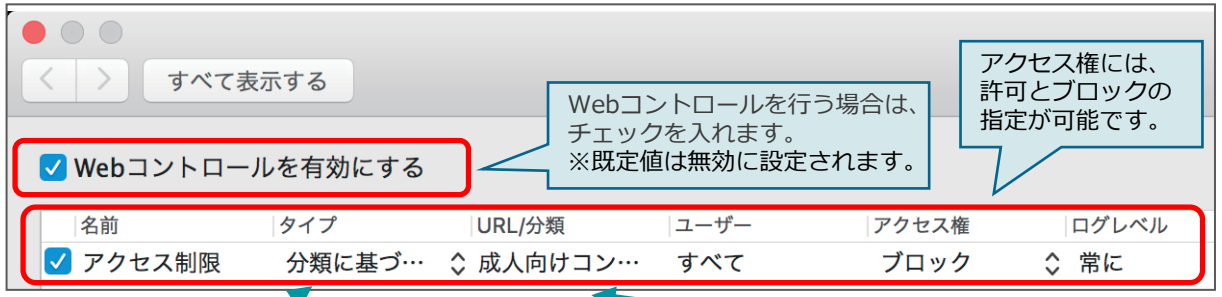
※プロファイルには、ファイアウォールのルールを登録する他に、プロファイルを適用する条件を設定することが可能です。
　プロファイルの条件には、IPアドレスやネットワーク インターフェースなどを条件として使用することが可能です。
⇒本機能を活用し、社内、外出先などの複数のプロファイルを予め作成し自動的に切替させることで、環境毎にクライアントに適切なルールを自動的に
　適用することが可能です。

2-1-5. Webコントロール

EESM

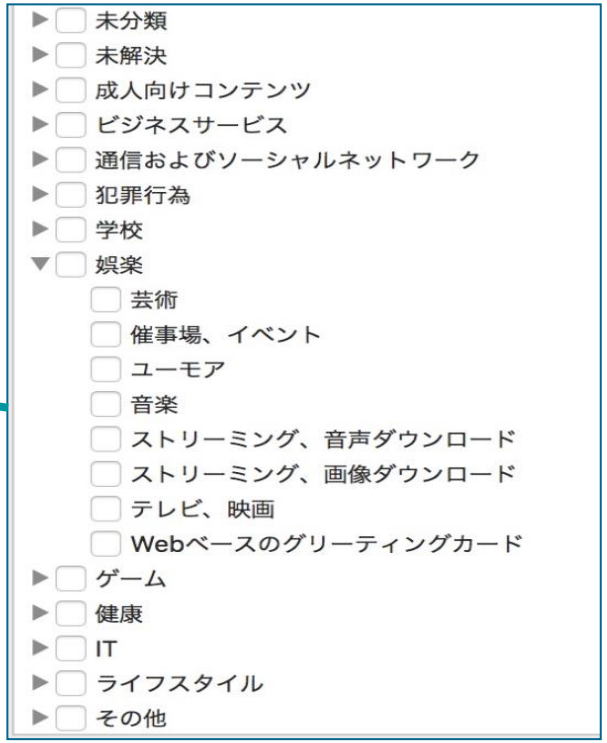
不適切または有害なコンテンツを含む、Web サイトへのアクセスをブロックします。
特定のWebサイトに対してURLを指定したアクセスの制御が実施できる以外に、Web サイトカテゴリを
使用してアクセスをコントロールできます。カテゴリーは27以上のカテゴリと140以上のサブカテゴリから選択可能です。

詳細設定（Webコントロール）



タイプ	動作
URL に基づくアクション	特定のWeb サイトへのアクセスを制御するルールの場合に選択します。「URL」フィールドに入力したURL にアクセスする際に、「アクセス権」で選択したアクションが実行されます。
分類に基づくアクション	あらかじめ用意されているカテゴリでWeb サイトへのアクセスを制御するルールの場合に選択します。指定したカテゴリのWeb サイトにアクセスする際に「アクセス権」で選択したアクションが実行されます。

選択可能なカテゴリ

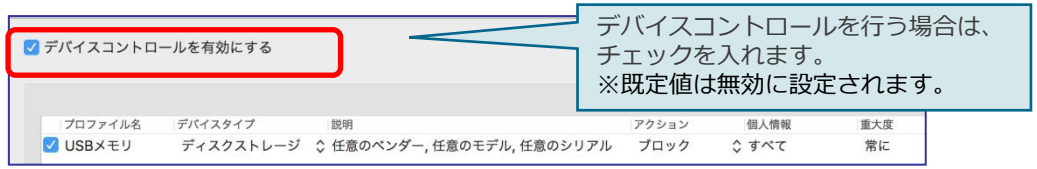


2-1-6. デバイスコントロール

EESM

コンピューター上で利用できるデバイスを指定することができます。
ベンダー名、モデル、シリアル番号を指定することで特定のデバイスだけを接続させることが可能です。
これにより、各端末上で利用できるデバイスを制限し、機密情報を含むファイルなどの持ち出しを防ぐことが可能です。

詳細設定（デバイスコントロール）



設定可能なデバイスのタイプとアクション

デバイスタイプ	アクション		
	読み込み/書き込み	読み取り専用	ブロック
ディスクストレージ	○	○	○
CD/DVD	○	○	○
USBプリンタ	○	ー	○
イメージングデバイス	○	-	○
シリアル	○	-	○
ネットワーク	○	-	○
ポータブルデバイス	○	-	○
すべてのデバイスタイプ	○	○	○

デバイスコントロール設定

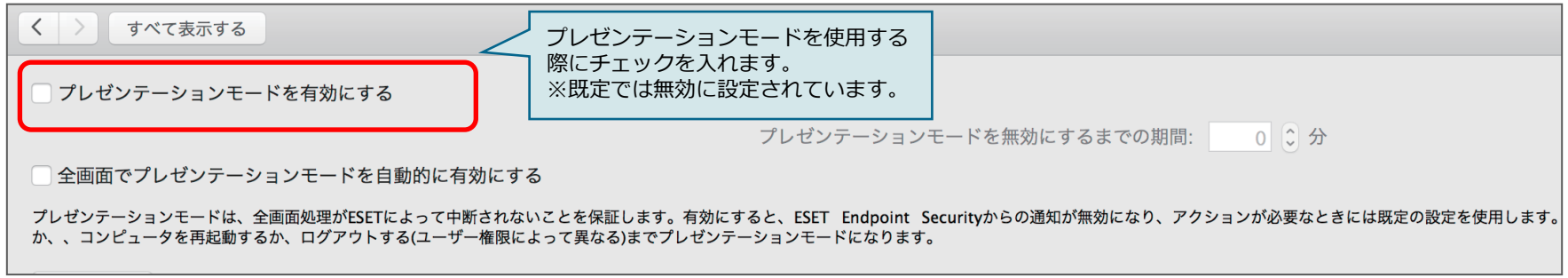
2-2. その他機能

2-2-1. プレゼンテーションモード

EESM

プレゼンテーション中のポップアップ通知、スケジュールタスクなどを一時的に停止することができます。
プレゼンテーションモードを有効にすると、潜在的なセキュリティリスクが存在するため、
メイン画面がオレンジ色になり、警告が表示されます。

設定（プレゼンテーションモード）



設定	動作
プレゼンテーション モードを有効にする	プレゼンテーションモードが有効になります。また指定した時間が経過した際にプレゼンテーションモードを自動的に無効にする［プレゼンテーションモードを無効にするまでの時間］を分単位で設定できます。 既定値は、「0 分」が設定されており、自動的にプレゼンテーションモードが無効にならないように設定されています。
全画面でプレゼンテーション モードを自動的に有効にする	アプリケーションが全画面で実行された際にプレゼンテーションモードを自動的に有効にします。 この機能を有効にすると、全画面でアプリケーションを開始するたびにプレゼンテーションモードが有効になり、アプリケーションを終了すると、自動的に無効になります。 この機能は、プレゼンテーションを開始する場合に便利です。

2-2-2. OSアップデート通知

EESM
EEAM

Digital Security
Progress. Protected.

OSが最新にアップデートされているか確認を行い、OSが最新でない場合に通知を行い、
コンピューターにアップデートを促すことが可能です。

OSアップデート通知画面

クリックすると、アップデート利用可能なソフトウェアの一覧を表示することができます。

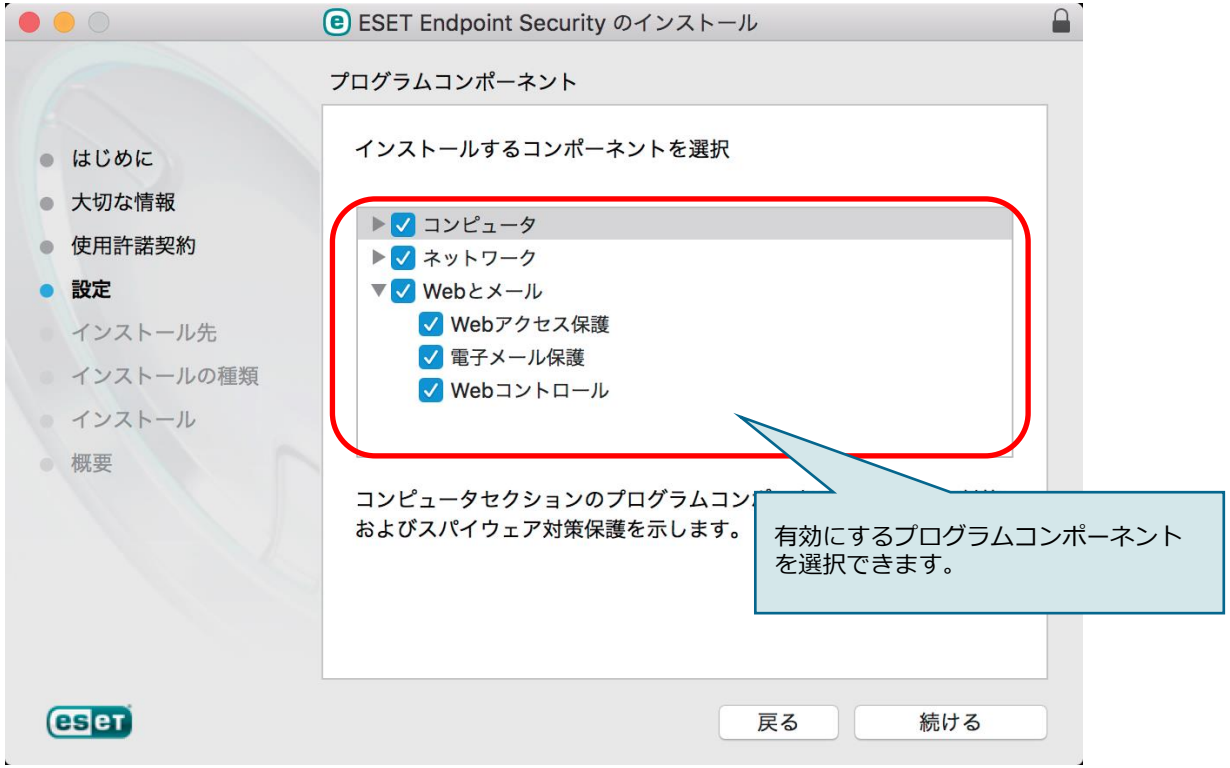
2-2-3. コンポーネントを指定したインストール

EESM
EEAM

Digital Security
Progress. Protected.

インストールするプログラムを選択できます。いくつかのコンポーネントは必須ですが、それ以外は
オプションで機能を利用できなくすることができます。

カスタムセットアップ(プログラムコンポーネントの選択)

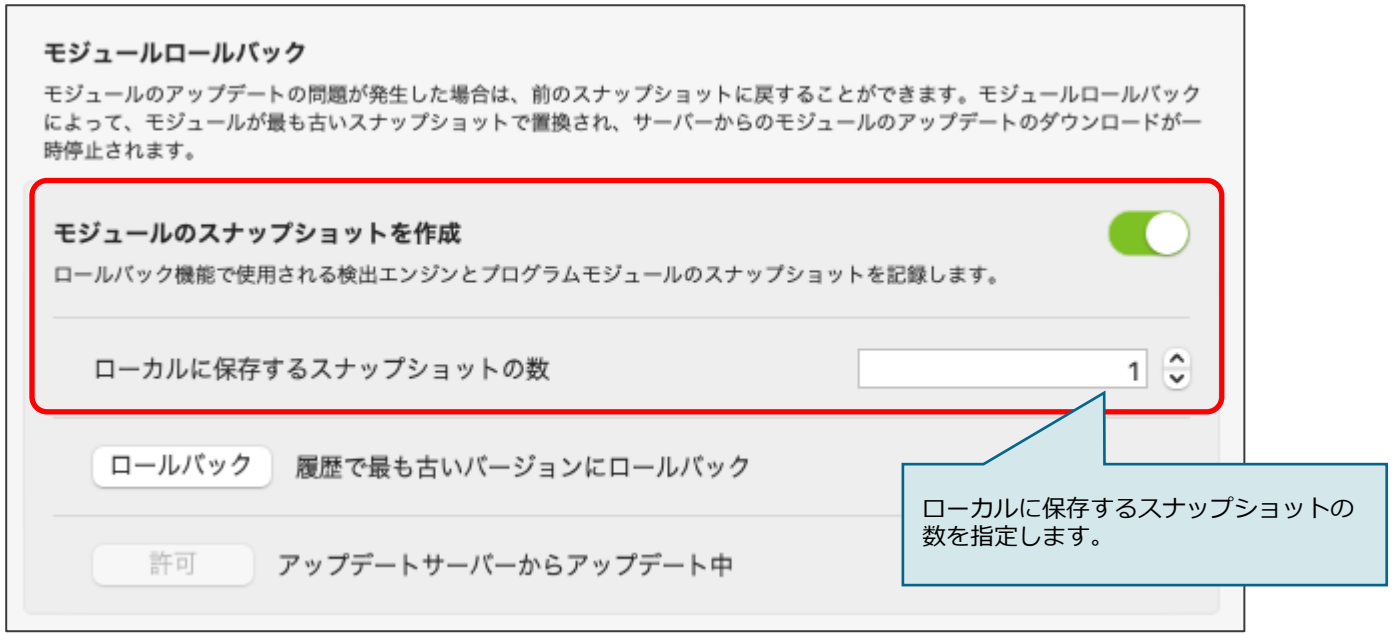


2-2-4. ロールバック機能

EESM
EEAM

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）



2-2-5. 遅延アップデート

EESM
EEAM

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、利用できるようになりました。

詳細設定（アップデート設定）