



ESET Endpoint Security V7 /
ESET Endpoint アンチウイルス V7 /
ESET File Security for Microsoft Windows Server V7
機能紹介資料

第6版

作成：2021年7月1日

Canon

キヤノンマーケティングジャパン株式会社



1. はじめに
 - (1)本資料について
 - (2)本プログラムの特徴
2. ESET Endpoint Security V7/ESET Endpoint アンチウイルス V7/
ESET File Security for Microsoft Windows Server V7の機能紹介
 - (1)ユーザーインターフェースについて
 - (2)詳細設定について
3. プログラム別の機能比較



本資料はWindowsクライアント用プログラムとサーバー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 V7 (略称表記 : EES)	Windows クライアント用 総合セキュリティプログラム	EES
ESET Endpoint アンチウイルス V7 (略称表記 : EEA)	Windows クライアント用 ウイルス・スパイウェア対策プログラム	EEA
ESET File Security for Microsoft Windows Server V7 (略称表記 : EFSW)	Windows サーバー用 ウイルス・スパイウェア対策プログラム	EFSW

- ・本資料で使用している画面イメージは使用するバージョン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。
- ・上記のプログラムはオンプレミス型セキュリティ管理ツールである、ESET Security Management Center V7 (※以降ESMC)とESET PROTECT(※以降EP)とクラウド型セキュリティ管理ツールであるESET PROTECT Cloud(※以降EPC)で管理が可能です。ESMCとEP、EPCの機能紹介は別資料でご用意しています。
- ・ESET PROTECTソリューションではMac、Linux、Android OS向けのプログラムもご使用いただけます。
各プログラムの機能紹介は別資料でご用意しています。
- ・ESET、NOD32、ThreatSense、LiveGrid、ESET Endpoint Protection、ESET Endpoint Security、ESET Endpoint アンチウイルス、ESET File Security、ESET NOD32 アンチウイルス、ESET Security Management Center、ESET PROTECTは、ESET, spol. s. r. o.の商標です。
- ・Windows、Windows Server、Microsoft Edge、Internet Explorerは、米国 Microsoft Corporation の米国、日本およびその他の国における商標登録または商標です。

※ESMC V7.1/V7.2とEPとEPCではEES/EEA/EFSW V6.5以下を管理することはできません。



機能名が記載されております。

V7から搭載された機能であることを表しております。

紹介されている機能がどのプログラムに搭載されているかをアイコンで表しております。

2

NEW

ランサムウェア保護

EES

EEA

EFSW

ランサムウェア保護は、データを修正しようとするアプリケーションとプロセスの動作を監視します。悪意のあるアプリケーションの動作が発見された場合や、ESET LiveGridからの情報によって不審なアプリケーションであると示された場合、そのアプリケーションを、自動的にブロックすることなどが可能です。

※この機能を正しく動作させるには、ESET LiveGridを有効にする必要があります。

詳細設定(HIPS画面)

詳細設定

検出エンジン

リアルタイムファイルシステム保護

クラウドベース保護

マルウェア検査

HIPS

アップデート

ネットワーク保護

WEBとメール

デバイスコントロール

詳細動作検査

詳細動作検査を有効にする ☒

除外 編集

ランサムウェア保護

ランサムウェア保護を有効にする ☒

HIPS 設定

※ ランサムウェア
 ファイルを暗号化するなどの被害を意図的に発生させ、その解決のための身代金を要求するマルウェアのことです。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。
https://eset-info.canon-its.jp/malware_info/term/detail/00104.html

機能についての説明と機能に関する画像が記載されております。

説明中に出てくる単語についての解説が記載されております。



ESETでは、エンドポイントでの多層防御を実装しております。これにより新種の脅威からの防御を強化しております。各防御機能の紹介は以降のページをご参照ください。

巧妙化する脅威から守る「多層防御」

高度化・巧妙化する脅威に対抗するため、マルウェアの起動時だけではなく、その前後も含めた複数のタイミングで攻撃の手法に合わせた方法で検査を行います。新バージョンで新たに加わった高度な機械学習機能は、従来ESET社のクラウド環境でおこなっていた機械学習による解析をユーザーのローカル環境で実施し、より迅速にマルウェアかどうか判定できるようになりました。





(1)ユーザーインターフェースについて



ユーザーインターフェースの左側の各メニューを選択することで、現在の保護状態の確認やコンピューターの検査、ESET製品の設定変更を行うことが可能です。

ユーザーインターフェース(現在の状況)

正常に動作をしている場合は、緑色で表示されます。



以下の6つのメニューがあります。

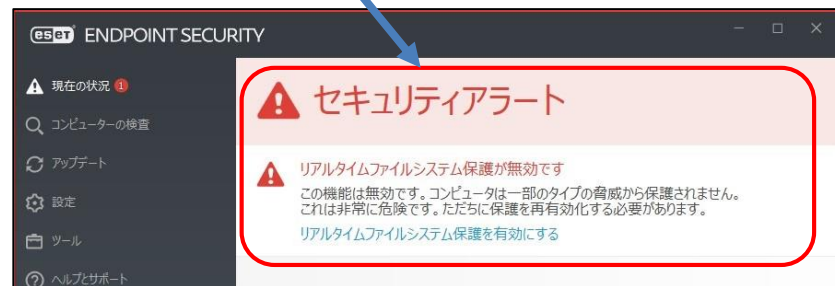
- ・現在の状況 ※
- ・コンピューターの検査 ※
- ・アップデート
- ・設定
- ・ツール
- ・ヘルプとサポート

※ESET File Security for Microsoft Windows Serverでは「現在の状況」は「監視」、「コンピューターの検査」は「検査」となっております。

また、上記のメニューに加え、「ログファイル」のメニューがあります。

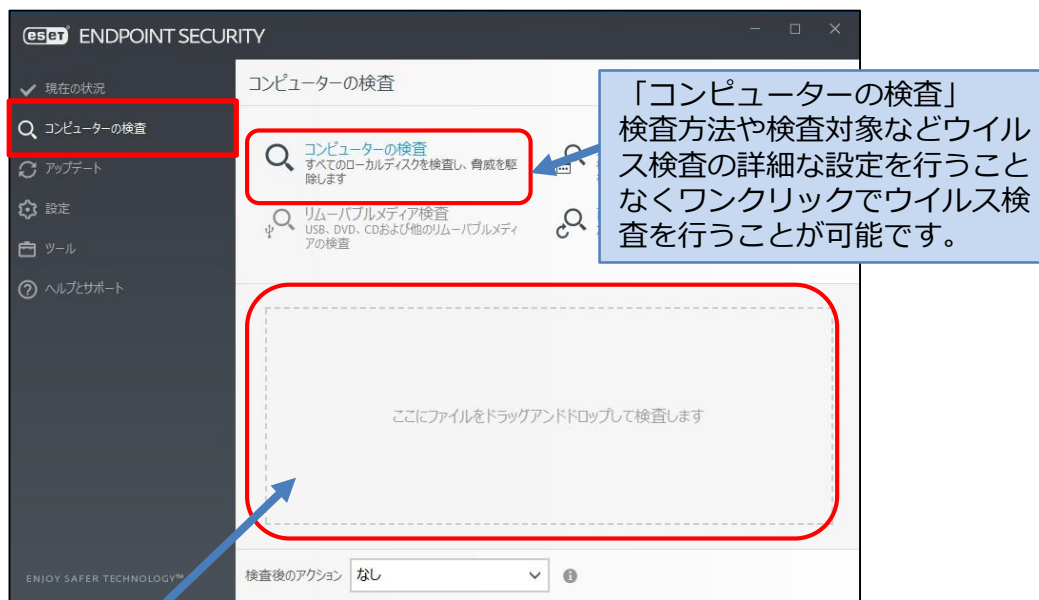


注意が必要な場合は黄色
重大な問題がある場合は赤色
で表示されます。



コンピューターの検査では、コンピューターのウイルス検査を実施し、コンピューター内部に潜んでいるウイルスを検知して、駆除することが可能です。定期的にウイルス検査を実施することで、セキュリティレベルを保つことが可能です。

ユーザーインターフェース(コンピューターの検査)



NEW 「ドラッグアンドドロップ機能」
検査を行いたいファイルやフォルダをユーザーインターフェース上にドラッグアンドドロップすることで検査が可能です。

ウイルス検査中の画面



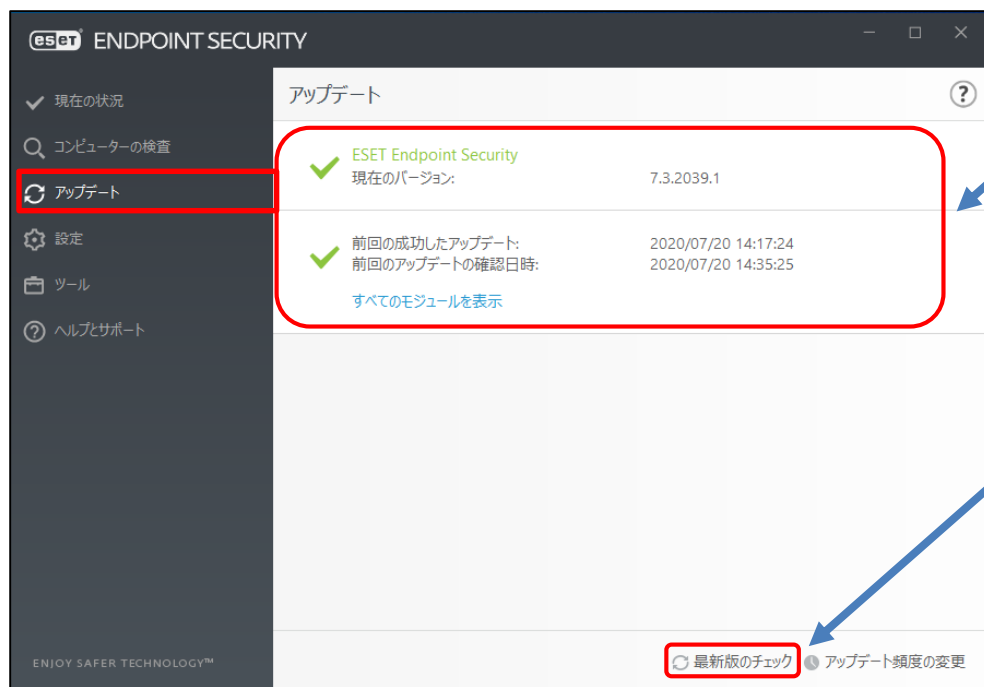
ウイルス検査完了の画面





アップデートでは、ウイルス検査で使用する検出エンジンのアップデートを行うことが可能です。新しいウイルスが日々発生しているため、検出エンジンを常に最新にしておくことで、新たな脅威からコンピューターを保護することが可能です。

ユーザーインターフェース(アップデート)



現在のプログラムのバージョンやアップデートを行った時間を確認することが可能です。

「最新版のチェック」をクリックすることで検出エンジンのアップデートを行うことが可能です。

※検出エンジン

ESET特有の表現方法で、ウイルスを検知するための過去に発見された各ウイルスに関する情報をまとめたデータベースのことを意味します。一般的にはウイルスパターンファイルやウイルス定義ファイル、シグネチャファイルなどと呼ばれております。

2 設定

ENDPOINT SECURITY FOR ENDPOINT ANTIVIRUS

EES

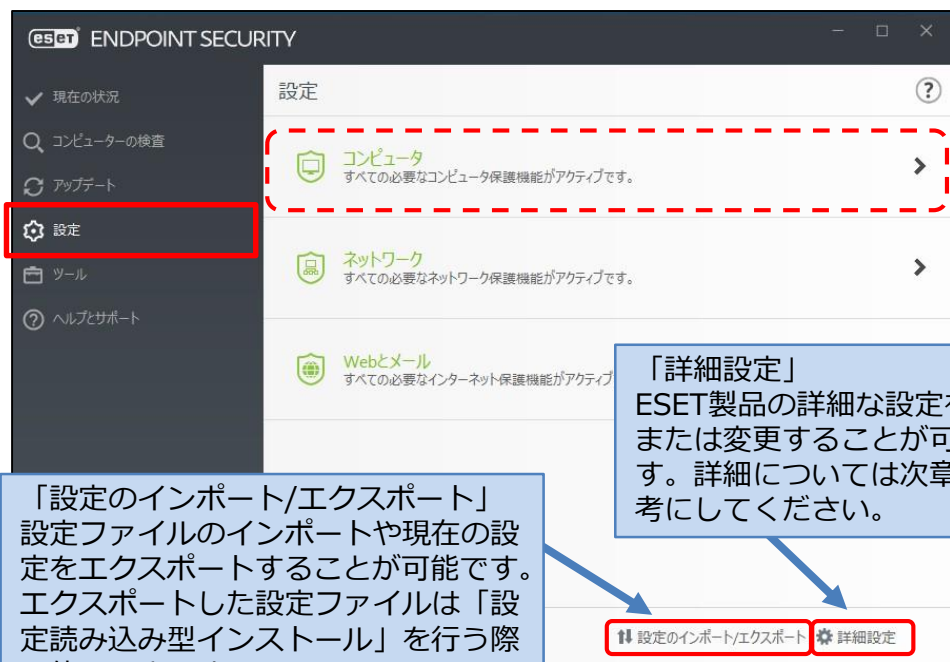
EEA

EFSW



ESETのウイルス・スパイウェア対策プログラムの設定の確認と変更をすることが可能です。また業務を行う上で一時的にESETの保護機能を変更させたい場合はユーザーインターフェースから設定を一時的に有効や無効にすることが可能です。

ユーザーインターフェース(設定)

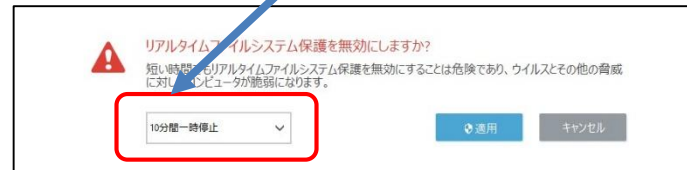


「設定のインポート/エクスポート」
設定ファイルのインポートや現在の設定をエクスポートすることが可能です。エクスポートした設定ファイルは「設定読み込み型インストール」を行う際に使用できます。

「詳細設定」
ESET製品の詳細な設定を確認または変更することが可能です。詳細については次章を参考にしてください。



ウイルス対策機能を一時的に無効にすることが可能です。また、一時停止する時間も指定することが可能です。



※設定読み込み型インストール

インストールを行う過程でエクスポートした設定ファイルを読み込みながらインストールを行います。詳しい手順については、下記サポートページをご覧ください。
https://eset-support.canon-its.jp/faq/show/20?site_domain=business



ツールのスケジューラを使用することで、検出エンジンのアップデートやコンピュータの検査を定期的に行うことが可能です。これにより、自動的にアップデートや検査が実施されるため、ユーザーが意識することなく、セキュリティをより強固にすることが可能です。

ユーザーインターフェース(ツール)

検出された脅威のログや検査を行ったオブジェクトの統計を確認することが可能です。



スケジューラ画面

スケジューラの機能を使用することで定期的に検出エンジンのアップデートを行うことやコンピュータの検査を実施することが可能です。



新たにスケジュールを追加する際は「タスクの追加」をクリックします。



(2)詳細設定について

検出エンジンの項目では、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(検出エンジン画面)



「疑わしい可能性のあるアプリケーション」
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逃れるためによく使用する方法です。

「安全ではない可能性の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。

「望ましくない可能性のあるアプリケーション」
アドウェアやツールバーをインストールするようなコンピューターのパフォーマンスに悪影響を与えるようなアプリケーションを検出します。

「アンチステルス技術を有効にする」
オペレーティングシステムから自らを見えなくするルートキットなどの危険なプログラムを検出します。
※詳細設定オプション内で設定可能です。

機械学習保護は、リアルタイムスキャンやオンデマンドスキャンでの検出に利用できます。ESET独自の機械学習アルゴリズムを利用して、ESET社のクラウド環境に接続することなくローカル内で機械学習による、より高度な解析を実現します。

※EES / EEA V7.3、EFSW V7.2より利用可能です。

詳細設定(検出エンジン画面)

検出エンジン
リアルタイムファイルシステム保護

高度な機械学習モジュールを利用して、以下の検出の閾値を設定可能です。

- ・マルウェア
- ・望ましくない可能性があるアプリケーション
- ・疑わしい可能性があるアプリケーション
- ・安全ではない可能性があるアプリケーション

「報告」では、検出時にログへの出力とデスクトップへの通知における閾値を設定できます。

「保護」は、検出時のブロックレベルの閾値になります。

既定値

リアルタイム保護および機械学習保護		最大	標準	最小	オフ
マルウェア	報告	☐	☒	☐	☐
	保護	☐	☒	☐	☐
望ましくない可能性があるアプリケーション	報告	☐	☒	☐	☐
	保護	☐	☒	☐	☐
疑わしい可能性があるアプリケーション	報告	☐	☒	☐	☐
	保護	☐	☒	☐	☐
安全ではない可能性があるアプリケーション	報告	☐	☒	☐	☐
	保護	☐	☒	☐	☐

除外

詳細設定オプション

閾値は「最大」「標準」「最小」「オフ」の4段階に設定できます。

報告と保護で閾値を分けることが可能なため、報告のみ「高度な機械学習モジュール」を利用するなど、誤検知のリスクを減らしながら運用することも可能です。

※保護の閾値を報告の閾値より大きい値に設定することはできません。

2 Antimalware Scan Interface(AMSI)保護

EES

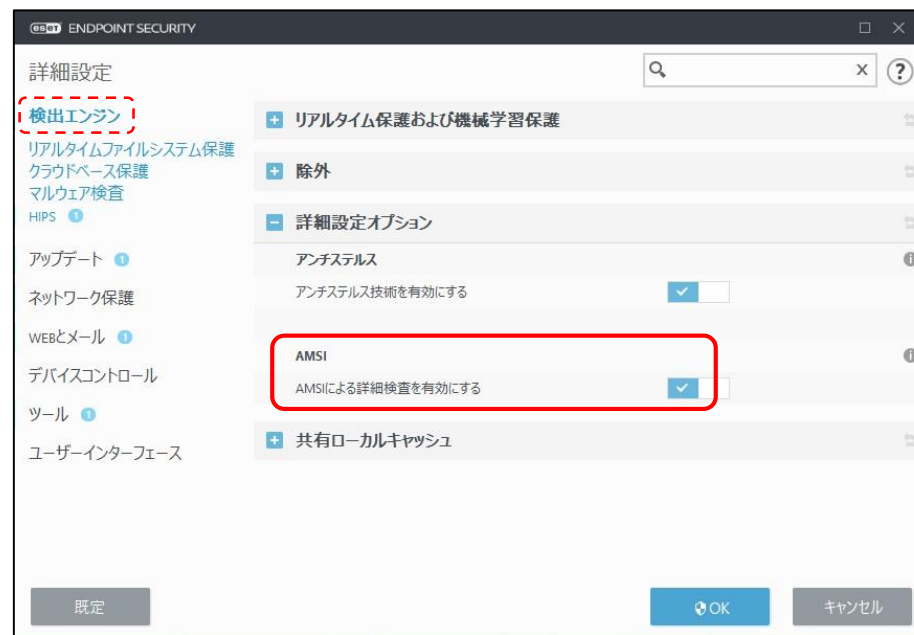
EEA

EFSW

WindowsのAntimalware Scan Interface(AMSI)との連携が可能です。AMSI保護を有効にすることでPowerShellでスクリプトが実行される前にESETで検査し、安全である場合のみ実行が可能となります。これにより、悪意のあるプログラムのインストールを行わないファイルレスマルウェア攻撃の検出が可能です。

※AMSI保護はWindows 10、Windows Server 2016、Windows Server 2019でのみ利用可能です。

詳細設定(検出エンジン画面)



※Antimalware Scan Interface(AMSI)

AMSIはWindows 10から導入されたWindowsのマルウェア防御技術です。

AMSIはアンチマルウェアプログラムと連携して、PowerShellなどのスクリプト攻撃に対処します。詳しくはMicrosoft社にご確認ください。

除外の設定を行うことで、特定のファイルやフォルダをウイルス検査の対象から外すことが可能です。パス、ハッシュ値、検出名で除外設定を行えます。独自開発したアプリケーションやデータベースなどを除外の対象とすることで、誤検知やデータベースなどを検査した際のCPU使用率の上昇を防ぐことが可能です。

※EES/EEA/EFSW 7.1以下では、パフォーマンス除外と検出除外は「検出エンジン」内の「除外」にて1か所で設定を行います。

詳細設定(検出エンジン画面)

詳細設定

検出エンジン

リアルタイムファイルシステム保護

クラウドベース保護

マルウェア検査

HIPS

アップデート

ネットワーク保護

WEBとメール

デバイスコントロール

ツール

ユーザーインターフェース

リアルタイム保護および機械学習保護

除外

パフォーマンス除外

検出除外

詳細設定オプション

共有ローカルキャッシュ

既定

除外の追加

パス

コメント

OK

キャンセル

除外の追加

パス

ハッシュ

検出名

コメント

OK

キャンセル

「検出除外」では、指定したパスの検査は行いますが、ルールに定められたオブジェクトやハッシュを検出から除外します。

「パフォーマンス除外」では、特定のファイルやフォルダを検査対象から除外することが可能です。

※画像はEES/EEA 7.3の設定画面です。

ESET File Security for Microsoft Windows Serverではサーバーアプリケーションやデータベースなどのファイルを自動的にウイルス検査の対象から除外することが可能です。これにより、手動でウイルス検査の対象から除外する設定をすることなく、サーバーの全体的なパフォーマンスを向上することが可能です。

詳細設定(検出エンジン画面)

詳細設定(検出エンジン画面)

検出エンジン

リアルタイムファイルシステム保護
クラウドベース保護
マルウェア検査
Hyper-V検査
OneDrive 検査
HIPS

アップデート
ネットワーク保護
WEBとメール
デバイスコントロール
ツール
ユーザーインターフェース

リアルタイム保護および機械学習保護

除外

詳細設定オプション

自動除外

自動除外を有効にする ☒

自動除外を有効にするアプリケーション/サーバー

Microsoft Windows Server ☒

Microsoft Lync/Skype for Business Server/ファイル共有 ☒

ファイル共有監視 ☒

共有ローカルキャッシュ

既定 OK

パフォーマンス除外

パスを除外 コメント

C:\pagefile.sys
C:\Windows\Security\Database*.chk
C:\Windows\Security\Database*.cmx
C:\Windows\Security\Database*.csv
C:\Windows\Security\Database*.edb
C:\Windows\Security\Database*.jrs
C:\Windows\Security\Database*.log
C:\Windows\Security\Database*.sdb
C:\Windows\Security\Database*.xml
C:\Windows\SoftwareDistribution\Datastore\Datastore.edb

インポート エクスポート

OK キャンセル

サーバーにインストールされている自動除外対象製品を検出し、ウイルス検査の除外対象とするリストに自動的に加えます。

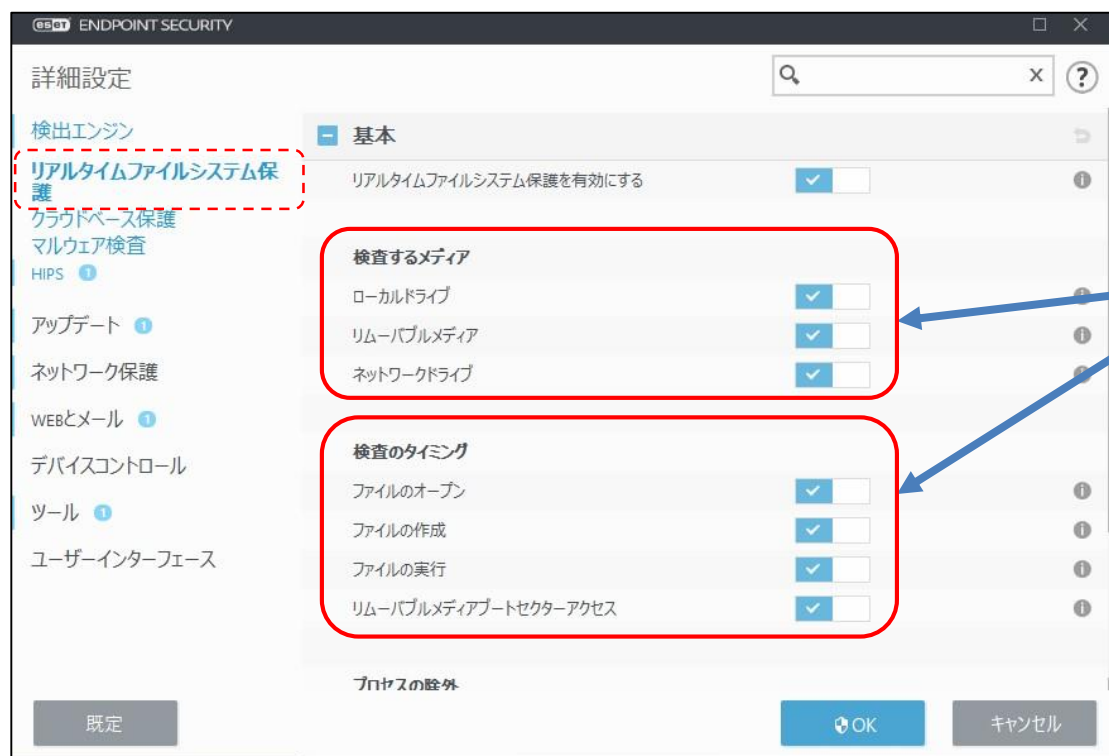
【自動除外対象製品】

- ・ Microsoft Windows Server
- ・ Microsoft SQL Server
- ・ Microsoft Exchange Server
- ・ Microsoft ISA Server
- ・ Microsoft Fore Front Threat Management Gateway
- ・ Microsoft Internet Information Server
- ・ Microsoft Hyper-V
- ・ IBM Lotus Domino Server
- ・ Kerio Connect
- ・ Kerio Control
- ・ ESET Remote Administrator サーバー
- ・ ESET Security Management Center サーバー
- ・ Microsoft Lync Server
- ・ Microsoft Skype for Business Server
- ・ Microsoft SharePoint Server



リアルタイムファイルシステム保護を使用すると、ファイルを開くときや作成するとき、実行するときに検査を行うことが可能です。リアルタイムファイルシステム保護は、システム起動時に開始され、中断することなく常に端末を保護します。

詳細設定(リアルタイムファイルシステム保護画面)



リアルタイムファイルシステム保護を有効にするメディアや、検査を行うタイミングを設定できます。



UEFIスキャナーは、HIPSの一部であり、コンピューターのUEFIを保護します。UEFIはブートプロセスの最初にメモリに読み込まれるファームウェアです。UEFIスキャナーにより、UEFIに感染しシステムを制御するマルウェアの検出が可能です。

詳細設定(リアルタイムファイルシステム保護画面)

詳細設定

検出エンジン

リアルタイムファイルシステム保護

クラウドベース保護

マルウェア検査

Hyper-V検査

OneDrive 検査

HIPS

+ 基本

- THREATSENSEパラメータ

検査するオブジェクト

ブートセクタ/UEFI

圧縮された実行形式

検索

X

?

✓

X

i

i



ESET LiveGrid®に参加すると、クラウドシステムにより実行中のプロセスの全世界における使用状況が共有されます。これにより実行中のプロセスのリスクレベルを確認できます。ESET LiveGrid®に不審なファイルを送付すると、送付されたファイルはESET LiveGrid®により解析されます。これは、新たな脅威からESETユーザーを守ることに繋がります。

詳細設定(クラウドベース保護画面)



「ESET LiveGrid®に参加する」
実行中のプロセスの全世界における使用状況を確認するにはチェックを付けてください。ESET LiveGrid®から受け取ったホワイトリストを使用してスキャンパフォーマンスを改善できます。

「サンプルの送信」
ESET LiveGrid®に送信するサンプルファイルの種類を設定することが可能です。

※ESET LiveGrid®

ESET LiveGrid®は複数のクラウド技術から構成される高度な早期警告システムです
詳細は下記マルウェア情報局のWebページを参照ください。

https://eset-info.canon-its.jp/malware_info/technology/detail/141119_1.html

マルウェア検査では、コンピューターの検査の際の詳細設定を行うことが可能です。検査の対象やウイルス発見時の動作、機械学習保護機能を利用した報告・保護レベルも設定できます。また、アイドル状態時の検査についての設定も可能です。

詳細設定(マルウェア検査画面)



「アイドル状態検査」
コンピューターのアイドル状態(スクリーンセーバーの起動時、コンピューターのロック、ユーザーのログオフ)の間を利用して、コンピューター全体の検査をサイレントに実行する機能です。

「オンデマンド保護および機械学習保護」
オンデマンド検査時の機械学習保護機能のレベルを設定できます。
※EES / EEA V7.3、EFSW V7.2より利用可能です。
※アイドル状態検査、スタートアップ検査、ドキュメント保護では、機械学習保護機能は利用できません。

2

Hyper-V検査

EFSW

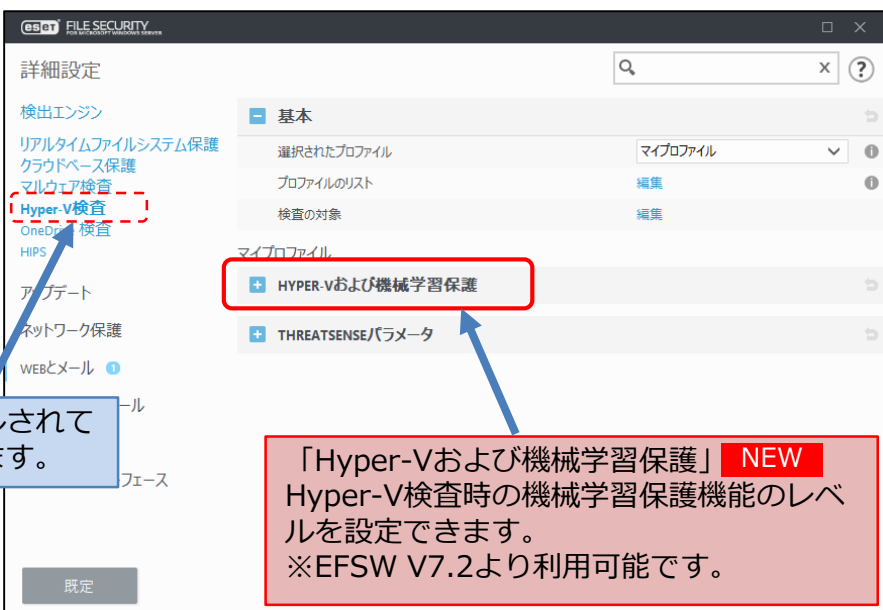
Hyper-V検査により、Microsoft Hyper-V Server上の仮想マシンディスクを検査することができます。ただし、脅威を駆除できるのは仮想マシンが起動していない場合のみです。仮想マシンが起動している場合、仮想マシンのスナップショットが作成され、作成されたスナップショットに対し読み取り専用モードで検査が実行されるため駆除は行われません。

ユーザーインターフェース(検査)



Hyper-Vがインストールされている場合のみ表示されます。

詳細設定(Hyper-V検査画面)



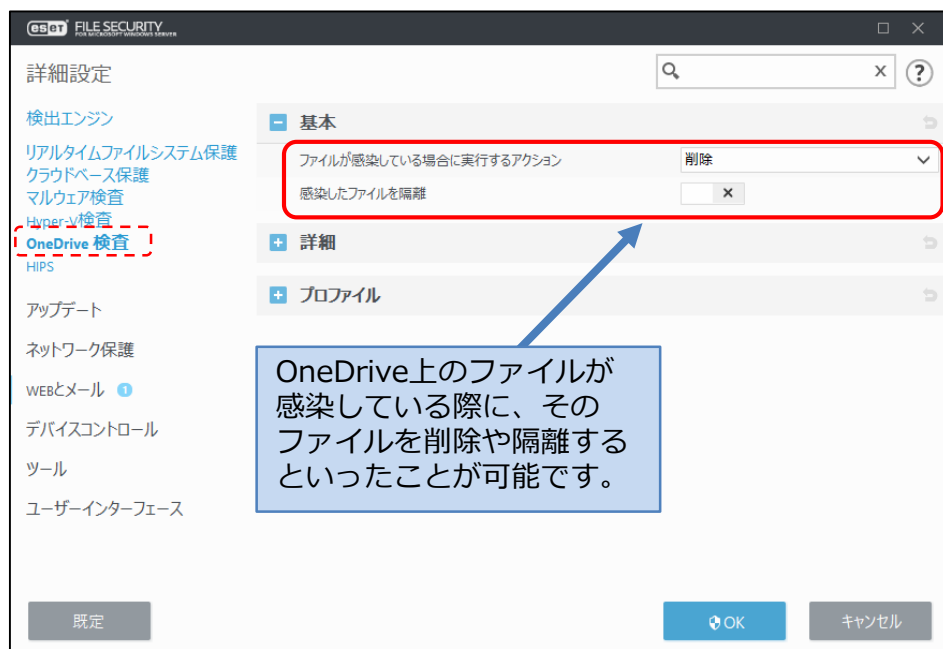
「Hyper-Vおよび機械学習保護」 NEW
Hyper-V検査時の機械学習保護機能のレベルを設定できます。
※EFSW V7.2より利用可能です。

※Hyper-V検査がサポートされるOSは下記となります。

Windows Server 2008 R2(仮想マシンがオフラインのときのみ検査可能)、Windows Server 2012、Windows Server 2012R2、Windows Server 2016、Windows Server 2019

OneDrive検査により、Microsoft OneDrive for Businessクラウドストレージに保存されているファイルやフォルダーを検査することが可能です。なお、本機能を使用する場合は、Microsoft OneDrive/Office365管理者アカウントの資格情報を登録する必要があります。

詳細設定(OneDrive検査画面)



ユーザーインターフェース(OneDrive検査の設定画面)

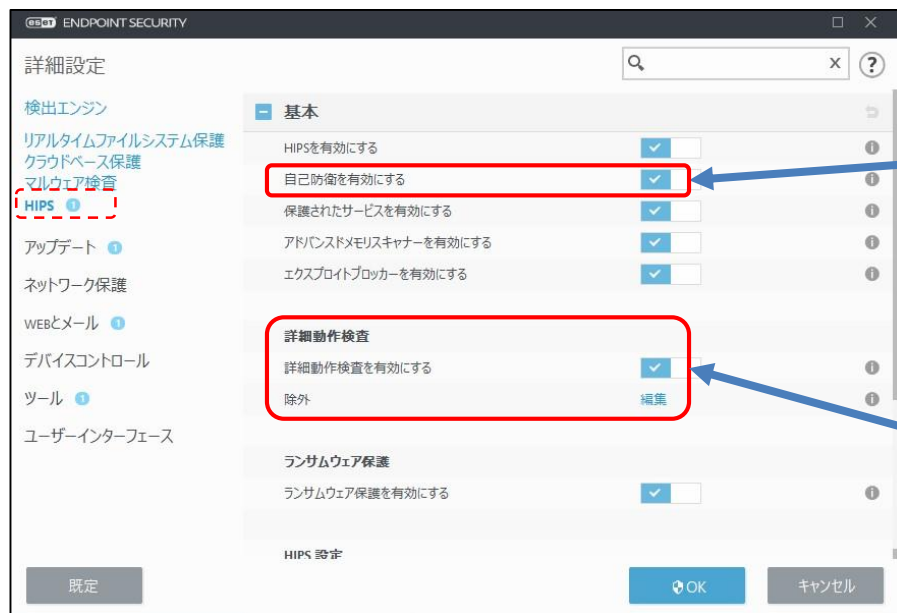




HIPS(Host-based Intrusion Prevention System)により、コンピューターのセキュリティに悪影響を与えようとする望ましくない活動およびマルウェアからシステムが保護されます。HIPSは、高度な動作分析とネットワークフィルタリングの検出機能を連携して、実行中のプロセス、ファイル、およびレジストリキーを監視します。

※HIPS設定の変更は、経験豊富なユーザーだけが行ってください。HIPSの設定が正しくないと、システムが不安定になる可能性があります。

詳細設定(HIPS画面)



「自己防衛」

自己防衛は悪意のあるソフトウェアによって、重要なシステムおよびESETのプロセス、レジストリキー、およびファイルを改ざんから防止し、スパイウェア対策の保護機能が破損されたり、無効化されたりしないようにしています。

「詳細動作検査」

端末で実行中のすべてのプログラムの動作を分析し、プロセスの動作に悪意があるかどうかを検査します。検査から除外するプロセスを設定することも可能です。

※EES/EEA V7.3より利用可能です。



実行中のメモリの詳細な検査を実施し、難読化や巧妙な手法で偽装されたウイルスの検出が可能です。これにより、シグネチャ検査やヒューリスティック検査でも検出が難しい難読化・暗号化されたウイルスについても検出します。

詳細設定(HIPS画面)



※ヒューリスティック

ウイルス検出の手法の一種で、プログラムの挙動を分析して悪意あるプログラムかを判定する技術を意味します。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。

https://eset-info.canon-its.jp/malware_info/term/detail/00092.html

また、『ヒューリスティック「基礎編」未知のウイルスも検出して駆除するESETのヒューリスティック機能』にも詳しい解説が記載されております。

https://eset-info.canon-its.jp/malware_info/technology/detail/140626_3.html



ブラウザー、メールソフトウェア、PDFリーダー、JAVAなどのアプリケーションの脆弱性を悪用するウイルスからコンピューターを保護することが可能です。疑わしい振る舞いを検出したら、直ちに動作をブロックします。これにより脆弱性を悪用して個人情報やFTPアカウントなどを盗もうとするウイルスを検知することが可能です。

詳細設定(HIPS画面)



※エクスプロイト

ソフトウェアの脆弱性を暴く行為、またはそのための検証コードを意味します。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。
https://eset-info.canon-its.jp/malware_info/term/detail/00048.html

※脆弱性(バリエナビリティ)

コンピューター関連のプログラムに潜む欠点や盲点、弱点のことで、「セキュリティ・ホール」とも呼ばれます。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。
https://eset-info.canon-its.jp/malware_info/term/detail/00068.html



ランサムウェア保護は、データを修正しようとするアプリケーションとプロセスの動作を監視します。悪意のあるアプリケーションの動作が発見された場合や、ESET LiveGridからの情報によって不審なアプリケーションであると示された場合、そのアプリケーションを、自動的にブロックすることなどが可能です。

※この機能を正しく動作させるには、ESET LiveGridを有効にする必要があります。

詳細設定(HIPS画面)



※ ランサムウェア

ファイルを暗号化するなどの障害を意図的に発生させ、その解決のための身代金を要求するマルウェアのことです。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。

https://eset-info.canon-its.jp/malware_info/term/detail/00104.html

アップデートの項目では、検出エンジンの取得先を変更することなどが可能です。ミラーサーバーより検出エンジンの取得をする場合は、こちらの項目より設定してください。また、アップデートサーバーは通常のアップデートサーバーのほか、通常の検出エンジンの配信より少し早く配信されるテストモードや、逆に通常配信後12時間経過してから配布される遅延アップデートを選ぶことが可能です。

※テストモードはESET社内部テストを経てリリースされますが、常に安定しているわけではありません。

高い可用性や安定性が必要な実働サーバーやワークステーションでは決して使用しないでください

詳細設定(アップデート画面)

詳細設定

検出エンジン

アップデート

ネットワーク保護

アップデート通知を設定する

アップデートキャッシュを削除

古い検出エンジンアラート

この設定は、検出エンジンが古くなったと判定されてアラートが表示されるまでの最大データベース経過時間を定義します。

検出エンジン最大経過時間を自動的に設定

検出エンジン最大経過時間(日数)

7

モジュールロールバック

モジュールのスナップショットを作成

ローカルに保存するスナップショットの数

1

前のモジュールにロールバック

ロールバック

プロファイル

既定

OK

キャンセル

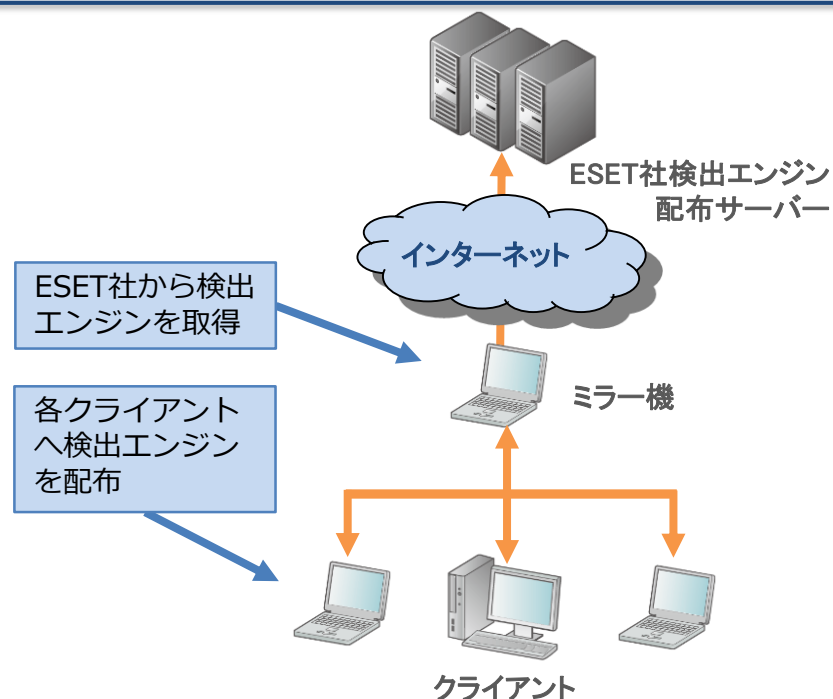
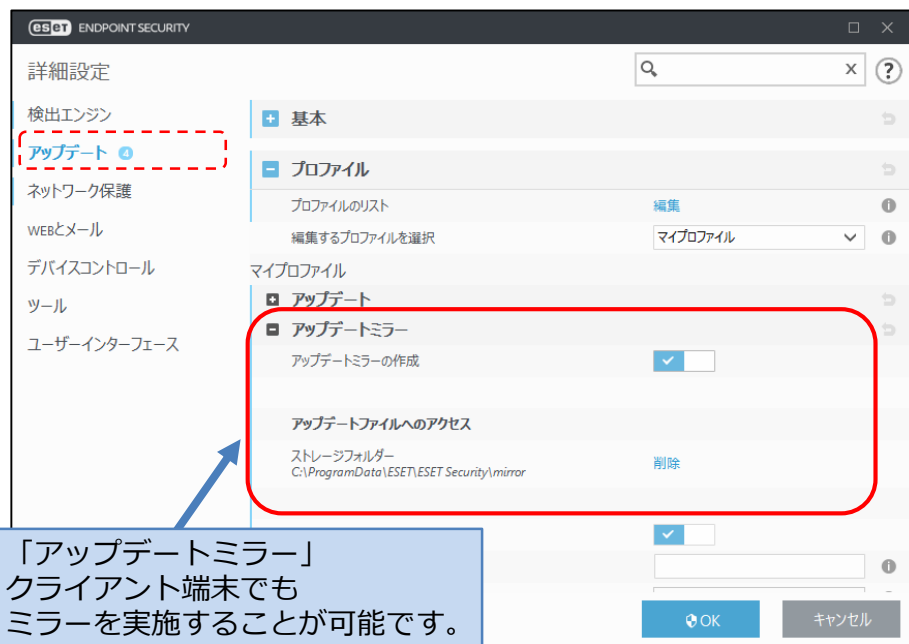
「モジュールロールバック」
検出エンジンのアップデートにより問題が起きた場合にロールバックすることができます。既定では、1つ分のスナップショットを保存します。



ミラー機能とは、ESET社から配布される検出エンジンなどのアップデートファイルをミラーリングし、クライアントに配布する機能です。これにより、検出エンジンのアップデートに伴うインターネット負荷が軽減されます。

また、ESET Endpoint Security / ESET Endpoint アンチウイルスにもミラー機能が搭載されているので、サーバーをご用意いただくなくても、ミラー環境を構築することが可能です。

詳細設定(アップデートミラー画面)





不正侵入対策(パーソナルファイアウォール)によって、ネットワークトラフィックを確認し、ルールに基づいた接続の許可や拒否の設定を行うことが可能です。

プロトコル、ポート、アプリケーションなどの指定によるルール作成が可能です。

※ファイアウォール機能はESET Endpoint Security でのみご使用いただけます。

詳細設定(ファイアウォール画面)

詳細設定(ファイアウォール画面)

詳細設定 - ESET Endpoint Security

ファイアウォールルール

ルールはファイアウォールが送受信するネットワーク接続の処理方法を定義します。ルールは上から下に評価されます。ルールと一致する最初のアクションが適用されます。

名前	有効	プロトコル	プロファイル	アクション	方向	ローカル	リモート	アプリケ...

追加

すべてのルール(定義済み)を表示

詳細設定 - ESET Endpoint Security

ルールの追加

一般 ローカル リモート

名前 無題

有効 ☒

方向 内向き

アクション 遮断

プロトコル TCPおよびUDP

ICMPタイプ/コード 0

プロファイル 任意のプロファイル

ログ記録の重大度 診断

ユーザーに通知 ☒

OK

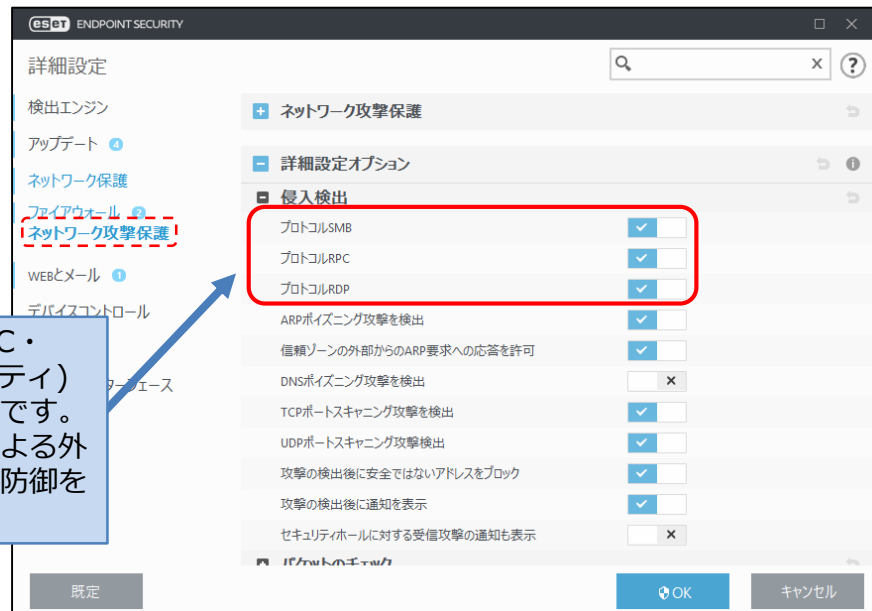
ネットワークトラフィックの内容を分析し、ネットワーク攻撃から保護します。有害だと見なされるすべてのトラフィックがブロックされます。これによりワーム攻撃、DoS攻撃、ポートスキャン攻撃、などを検出することが可能です。

詳細設定(ネットワーク攻撃保護画面)



ネットワークプロトコル(SMB・RPC・RDP)の既知の脆弱性(バグ)の悪用に対して保護することが可能です。これにより脆弱性やリモート操作による外部からのネットワーク攻撃に対する防御を行っています。

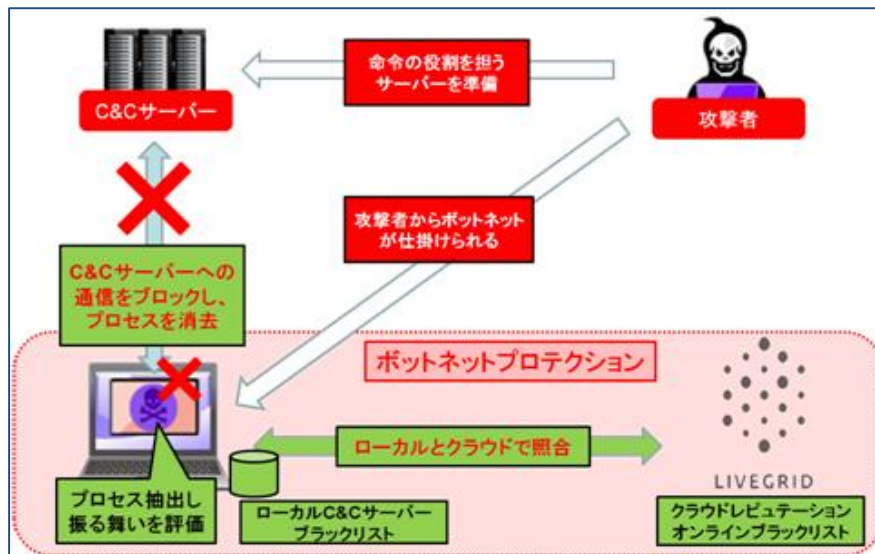
詳細設定(侵入検出画面)



「侵入検出」
コンピュータに被害を与えるために使用されるおそれがある、さまざまなタイプの脅威の検出を有効または無効にできます。

通信を解析し、リモートからのアクセスを検知して、迅速にボットを検出します。多層防御における防御層のひとつとして、不正サーバーへの送信となる不審な通信やアドレスを検知して遮断することで、標的型攻撃を防ぎます。

ボットネット攻撃例



ユーザーインターフェース(ネットワーク設定画面)



※ボットネット

第三者の指示通りに動く操り人形(ロボット)にしてしまう悪意のあるプログラムが「ボット」、ボットをいくつも集めてネットワーク化したものがボットネットと呼ばれます。

※下記マルウェア情報局のWebページ『ボットネットとは何か? どうやって防ぐのか?』も参照ください。

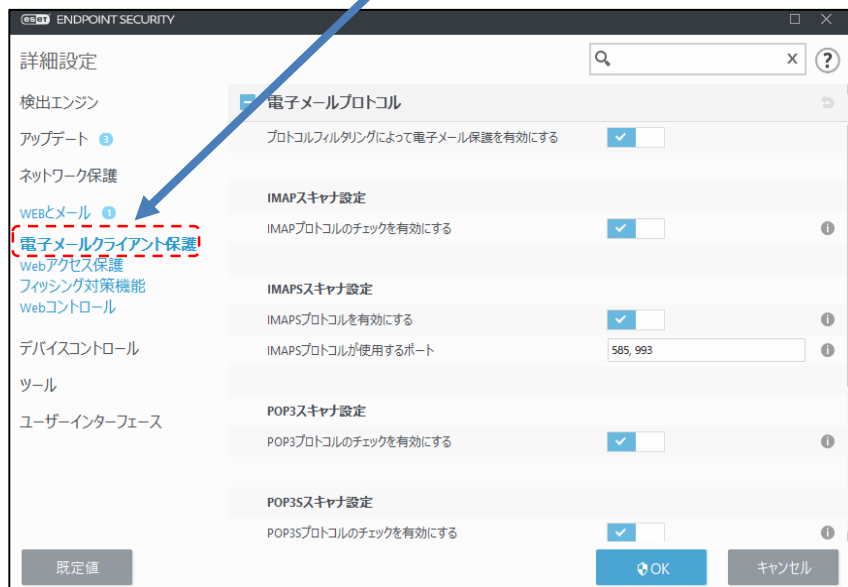
https://eset-info.canon-its.jp/malware_info/trend/detail/150120_3.html



プロトコルフィルタリングの機能により、使用しているインターネットブラウザやメールクライアントに関係なく、HTTP(S)、POP3(S)、IMAP(S)トフィックの検査を行い、ウイルスを検出することが可能です。これによりWebブラウザやメールの添付ファイルに潜むウイルスを検知することが可能です。

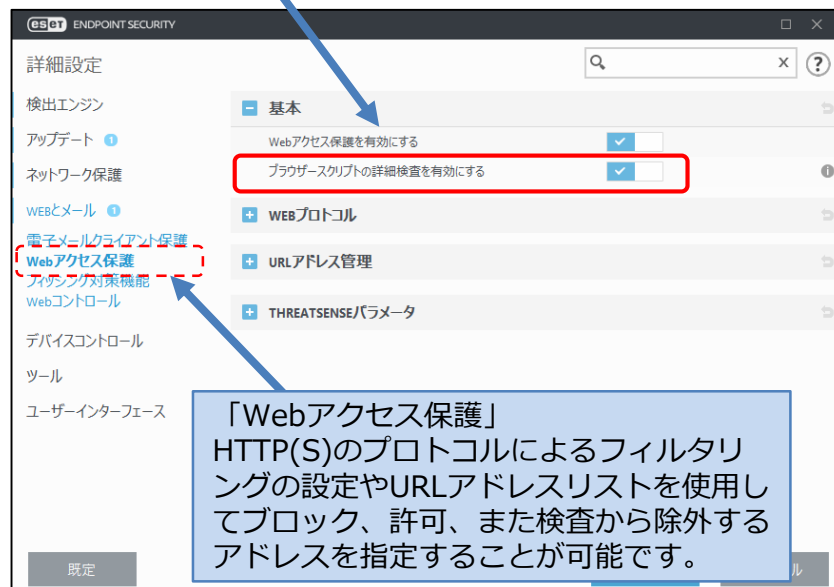
詳細設定(電子メールクライアント保護画面)

「電子メールクライアント保護」
POP3(S)とIMAP(S)のプロトコルによる
フィルタリングの設定や迷惑メール対策の
設定を行うことが可能です。



詳細設定(Webアクセス保護画面)

「ブラウザスクリプトの詳細検査を有効にする」
インターネットブラウザで使用されるJavaScriptプログラムの
検査を行うことが可能です。



「Webアクセス保護」
HTTP(S)のプロトコルによるフィルタリ
ングの設定やURLアドレスリストを使用し
てブロック、許可、また検査から除外する
アドレスを指定することが可能です。

2 フィッシング対策

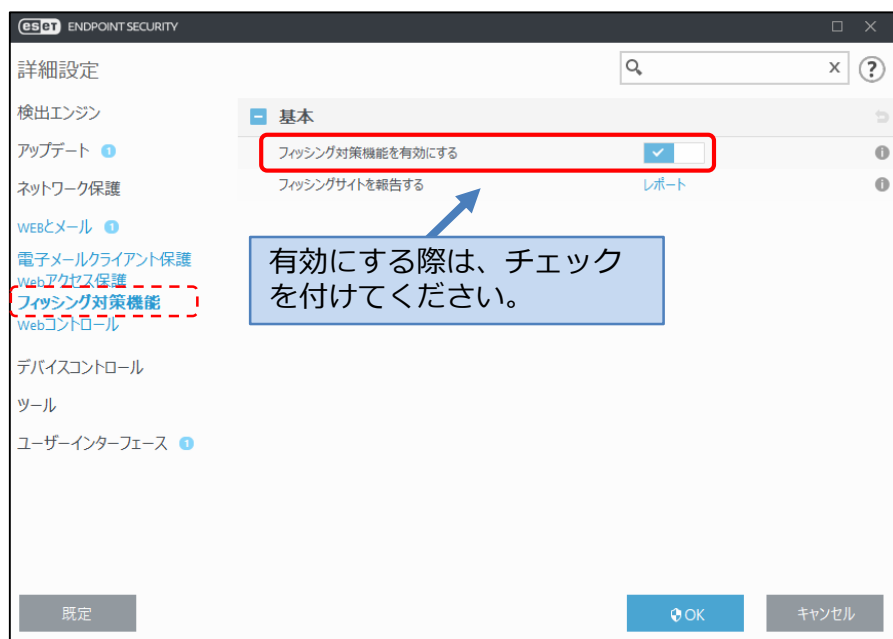
EES

EEA

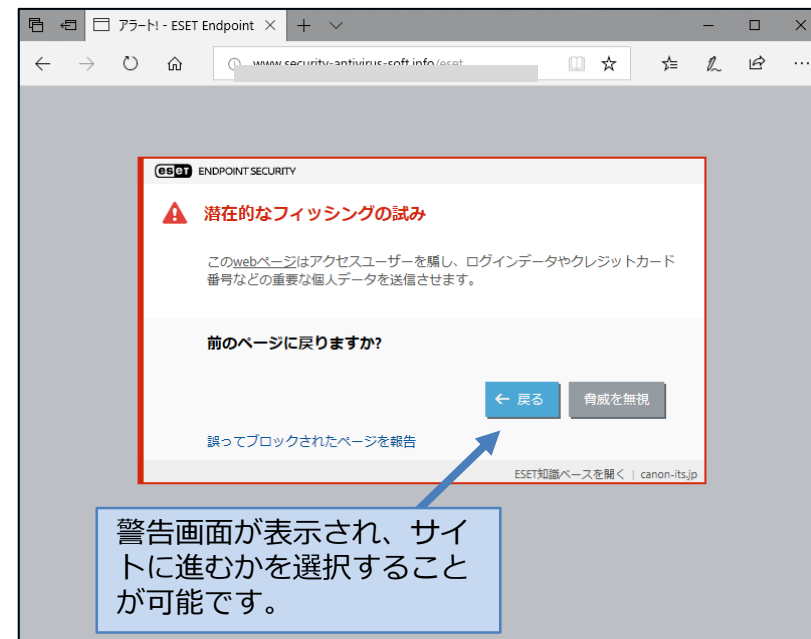
EFSW

フィッシングサイトのリスト、シグネチャと照合・検査を行います。フィッシングページへアクセスするとアクセスを抑止するダイアログが表示されます。また、フィッシングページと思われるURLをユーザーが開発元ESET社へ報告することも可能です。

詳細設定(フィッシング対策機能画面)



潜在的なフィッシングの脅威検出画面



※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



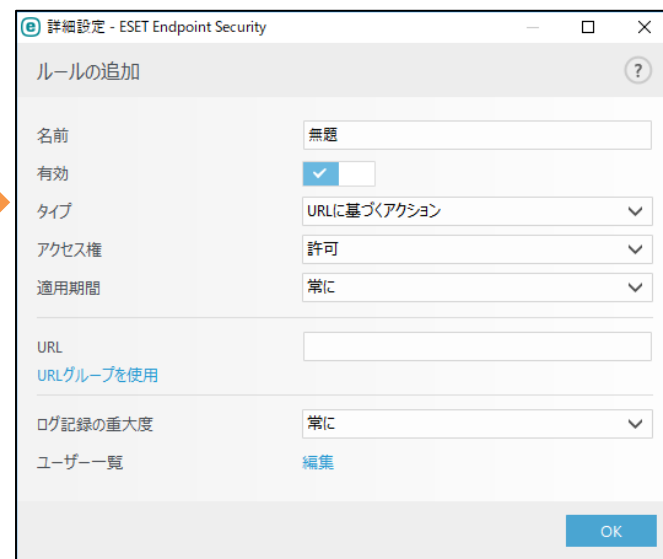
Webコントロール機能によって、WebサイトをURLやカテゴリごとに接続の許可や拒否の設定を行うことが可能です。これにより、ユーザーの生産性を低下させたり、悪影響を与えたりする可能性のある不適切または有害なコンテンツやページにアクセスすることを防ぐことが可能です。

※Webコントロール機能はESET Endpoint Security でのみご使用いただけます。

詳細設定(Webコントロール画面)



Webコントロールルール作成画面



「Webコントロールルール作成」
URLやカテゴリを指定して、ルールを作成することが可能です。



デバイスコントロール機能を使用することで、CD/DVDドライブ、USB接続のストレージデバイスなどの利用を制御することが可能です。これにより、各端末上で利用できるデバイスを制限し、USBメモリやスマートフォンなどで機密情報を含むファイルなどを持ち出されることを防ぐことが可能です。

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	警告
ディスクストレージ	○	○	○	○
CD/DVD	○	○	○	○
USBプリンタ	○	—	○	○
FireWireストレージ	○	○	○	○
Bluetoothデバイス	○	—	○	○
スマートカードリーダー	○	—	○	○
イメージングデバイス	○	—	○	○
モデム	○	—	○	○
LPT/COMポート	○	—	○	○
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

デバイスタイプ: ディスクストレージ

アクション: 読み込み/書き込み

条件: デバイス

ベンダー:

モデル:

シリアル番号:

ログ記録の重大度:

ユーザー一覧:

ベンダー、モデル(型番)、シリアルを入力することで詳細な制御が可能です。

デバイスコントロール警告メッセージ画面

ESet ENDPOINT SECURITY

⚠ デバイスアクセス制限

現在のデバイスコントロールポリシーは接続されたデバイスへのアクセスを制限します。
デバイスにアクセスする場合は、インシデントがセキュリティログに記録されます。

デバイスへのアクセスをブロックしますか?

アクセス制御

このメッセージの詳細を見る ▼ 詳細

事前に「タイムスロット」の設定にて期間を作成しておくことで、Webコントロールルールとデバイスコントロールルールを作成する際に、ルールを適用する時間帯や曜日を指定することが可能です。

これにより、業務時間中のみ特定のWebサイトへのアクセスを制限するなどお客様の運用に合わせて柔軟な運用が可能です。

※Webコントロールのルール作成はESET Endpoint Security のみご使用いただけます。

詳細設定 (タイムスロット画面)

名前	説明
月～金9:00～12:00まで適用	午前の業務時間
月～金13:00～17:30まで適用	午後の業務時間

事前にタイムスロットの設定で曜日と時間を設定しておくことで「Webコントロール」や「デバイスコントロール」のルール設定において、適用期間の設定項目として選択が可能になります。

2 プロキシサーバ

EES

EEA

EFSW

検出エンジンのアップデートやESETのウイルス・スパイウェア対策プログラムのアクティベーション(認証)を、インターネット経由で行う場合、インターネットに接続する際にプロキシサーバを経由する環境では、ESETのウイルス・スパイウェア対策プログラムにプロキシサーバの設定を行う必要があります。

詳細設定(プロキシサーバ画面)

プロキシサーバを設定する際はチェックを付けてください。

プロキシサーバで認証が必要な場合は、チェックを付け有効なユーザー名とパスワードを入力してください。



電子メール通知を使用することで、各端末で「ウイルスを検出した」などのイベントが発生した際に、管理者にメールで通知することが可能です。これにより、ウイルス感染などの問題が発生した際に、素早く対処に取り掛かることが可能です。

詳細設定(通知画面)

詳細設定

検出エンジン

アップデート

ネットワーク保護

WEBとメール

デバイスコントロール

ツール

ログファイル

プロキシサーバ

通知

プレゼンテーションモード

診断

ユーザーインターフェース

電子メール通知

電子メールで通知を送信する

SMTPサーバー

SMTPサーバー

ユーザー名

パスワード

送信元アドレス

受信者アドレス

TLSを有効にする

SMTP接続のテスト

電子メール設定

通知の最低レベル

各通知を別のメールで送信

新しい通知メールが送信される間隔(分)

既定値

OK

キャンセル

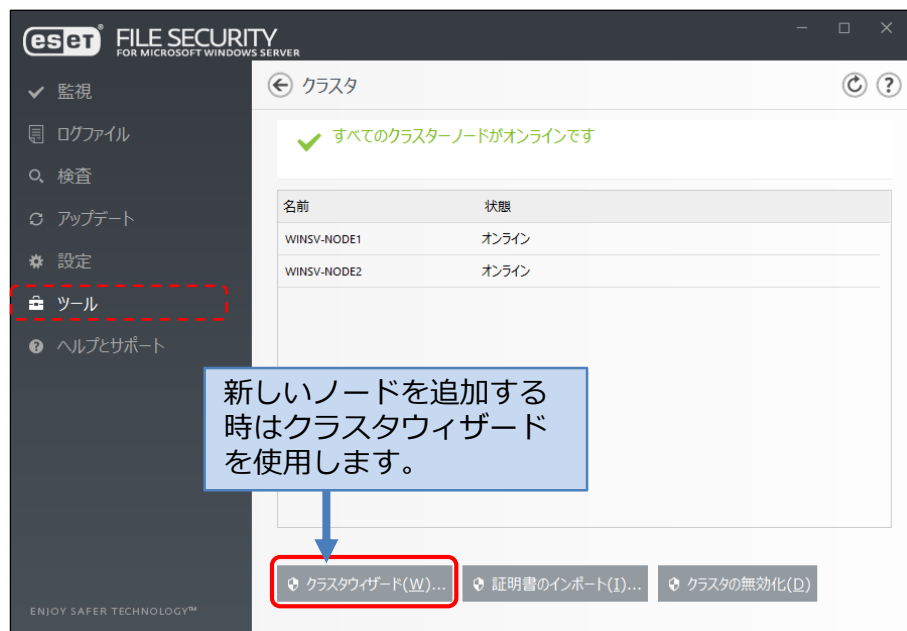
電子メール通知機能を使用する場合はチェックを付けてください。

使用するSMTPサーバー名を入力します。また、「SMTPサーバー名:ポート番号」と入力することでポートを指定することが可能です。
※既定では25番ポートを使用します。

送信する通知のログレベルを設定します。また、メールが送信される間隔も設定でき、間隔を「0」に設定することでリアルタイムでメールを受信できます。

クラスタを構築した場合、サーバー同士が通信を行い ESET File Security for Microsoft Windows Server をインストールさせたり、設定情報などを同期させたりすることが可能です。クラスタを構築するためにはクラスタウィザードを使用します。クラスタウィザードを使用することで、新たなノードの追加やクラスタ名などを設定することが可能です。

ユーザーインターフェース(クラスタ)

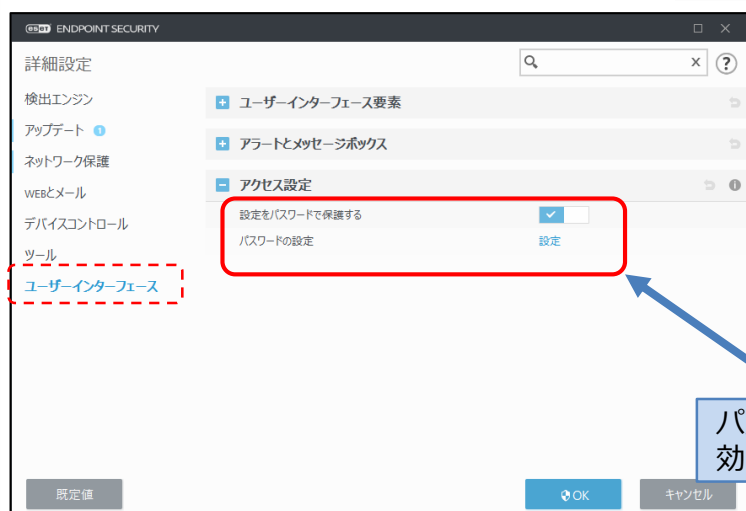


詳細設定(クラスタ画面)



設定をパスワードで保護することにより、ユーザーに設定を変更されたり、ESETのウイルス・スパイウェア対策プログラムをアンインストールされることを防止することが可能です。

詳細設定(ユーザーインターフェース画面)



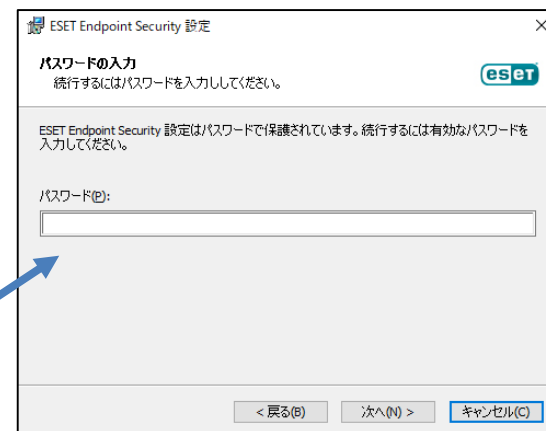
パスワードを設定する場合は有効にしてください。

パスワード入力画面(詳細設定を確認する場合)



詳細設定を確認する際やアンインストール時にパスワード入力を求められます。

パスワード入力画面(アンインストールする場合)





プログラム別の機能比較

3

プログラム別の機能比較



機能名	EES		EEA		EFSW	
	V6	V7	V6	V7	V6	V7
ウイルス・スパイウェア対策機能						
コンピューターの検査	○	○	○	○	○	○
ユーザーインターフェースからのドラッグアンドドロップ検査 NEW	×	○	×	○	×	○
スクリプトに基づく攻撃保護	○ ※1	○ ※1	○ ※1	○ ※1	×	○ ※1
リアルタイムファイルシステム保護	○	○	○	○	○	○
機械学習保護 NEW	×	○ ※2	×	○ ※2	×	○ ※2
UEFIスキャナー NEW	×	○	×	○	×	○
ESET LiveGrid	○	○	○	○	○	○
アイドル状態検査	○	○	○	○	○	○
OneDrive検査 NEW	×	×	×	×	×	○
Hyper-V検査	×	×	×	×	○ ※3	○
ホスト侵入防止システム(HIPS)	○	○	○	○	○	○
自己防衛機能	○	○	○	○	○	○
アドバンスドメモリスキャナー	○	○	○	○	○	○
エクスプロイトブロッカー	○	○	○	○	○	○
ランサムウェア保護 NEW	×	○	×	○	×	○

※1 AMSIによるスクリプト保護はOSがWindows10、Windows Server 2016、Windows Server 2019 の場合のみ使用することが可能です。

また、EES/EEAのV6.6から搭載されております。

※2 EES/EEAのV7.3、EFSWのV7.2から搭載されております。

※3 EFSWのV6.3から搭載されております。

3

プログラム別の機能比較

ESENT ANTIVIRUS



機能名	EES		EEA		EFSW	
	V6	V7	V6	V7	V6	V7
ウイルス・スパイウェア対策機能						
電子メール保護	○	○	○	○	○	○
Webアクセス保護	○	○	○	○	○	○
暗号化通信の検査 (HTTPS・POPS・IMAPSの検査)	○	○	○	○	○	○
フィッシング対策機能	○	○	○	○	○	○
ネットワーク通信関連機能						
ファイアウォール	○	○	×	×	×	×
迷惑メール対策	○	○	×	×	×	×
Webコントロール	○	○	×	×	×	×
バルナラビリティシールド	○	○	×	○	×	○
ボットネット保護	○	○	×	○	×	○
アップデート・ミラーサーバー機能						
検出エンジンのアップデート	○	○	○	○	○	○
オフライン更新機能	○	○	○	○	○	○
検出エンジンのロールバック	○	○	○	○	○	○
ミラー機能	○	○	○	○	○	○

3

プログラム別の機能比較



機能名	EES		EEA		EFSW	
	V6	V7	V6	V7	V6	V7
その他の機能						
設定のインポート・エクスポート	○	○	○	○	○	○
除外設定	○	○	○	○	○	○
自動除外設定	×	×	×	×	○	○
デバイスコントロール	○	○	○	○	○	○
デバイスコントロール グループールの追加	○	○	○	○	○	○
タイムスロット NEW	×	○	×	○	×	○
プロキシサーバの設定	○	○	○	○	○	○
Windowsクラスタ環境のサポート	×	×	×	×	○	○
電子メール通知機能	○	○	○	○	○	○
パスワードによる保護	○	○	○	○	○	○
ESET Security Management Center V7 による管理 ※1	○ ※2	○	○ ※2	○	×	○
ESET PROTECT V8による管理 ※1	×	○	×	○	×	○

※1 セキュリティ管理ツールでクライアントを管理するには各クライアントにESET Managementエージェントの導入が必要です。

※2 ESET Security Management Center V7.1/V7.2ではEES/EEA V6.5以下を管理することができません。