

**ESET Endpoint Security V9 /**  
**ESET Endpoint アンチウイルス V9 /**  
**ESET Server Security for Microsoft Windows Server V9**  
**機能紹介資料**

第3版  
2022年9月8日

**Canon**

# もくじ

1. はじめに
  - 1-1. 本資料について
  - 1-2. 本プログラムの特徴
  
2. ESET Endpoint Security V9 / ESET Endpoint アンチウイルス V9 / ESET Server Security for Microsoft Windows Server V9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. 詳細設定について
  
3. プログラム別の機能比較

# 1. はじめに

# 1-1. 本資料について

本資料はWindows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 V9 (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	
ESET Endpoint アンチウイルス V9 (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	
ESET Server Security for Microsoft Windows Server V9 (略称表記：ESSW)	Windows サーバー用 ウイルス・スパイウェア対策プログラム	

- 本資料で使用しているESET製品の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あります。
- ESSWはESET File Security for Microsoft Windows Server(略称表記：EFSW)の後継プログラムです。
- 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(略称表記：ESMC)とESET PROTECT(略称表記：EP)、クラウド型セキュリティ管理ツールであるESET PROTECT Cloud(略称表記：EPC)で管理が可能です。ESMCとEP、EPCの機能紹介は別資料をご用意しています。
- 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をご用意しています。
- 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。

# 1-1. 本資料について

機能名が記載しております。

## 2-2-24. セキュアブラウザ

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示しております。



コンピューターで実行中の他のプロセスからWebブラウザを保護します。ブラウザのメモリ空間やブラウザウィンドウの内容が改ざんされることを防止します。任意のWebサイトやESETのインターネットバンキングリストに登録されているWebサイトをセキュアブラウザにリダイレクトします。  
**※セキュアブラウザはESET Endpoint Security のみご使用いただけます。**

詳細設定(セキュアブラウザ画面)

セキュアブラウザ(例)

「キーボード保護を有効にする」  
 セキュアブラウザにキーボードから入力した情報は他のアプリケーションから隠すことができます。これにより、キーロガーに対する保護が強化されます。

「保護されたWebサイト」(編集画面)  
 セキュアブラウザにリダイレクトさせるWebサイトページを設定できます。

※EES/EEA V9.1以降、緑色のフレームをつけないことも可能です。

機能についての説明と機能に関する画像を記載しております。

# 1-2. 本プログラムの特徴

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。



## **2. ESET Endpoint Security V9 / ESET Endpoint アンチウイルス V9 / ESET Server Security for Microsoft Windows Server V9の機能紹介**

### **2-1. ユーザーインターフェースについて**

# 2-1-1. ユーザーインターフェース



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 Server 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」となっています。

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。

注意が必要です

OSのアップデートが利用可能です  
デバイスで利用可能なosのアップデートがあります。これらをインストールして、保護を保証してください。  
[詳細情報](#)

セキュリティアラート

リアルタイムファイルシステム保護が一時停止しています  
この機能は一時停止しています。コンピューターは一部のタイプの脅威から保護されません。これは非常に危険です。ただちに保護を再有効化する必要があります。  
[リアルタイムファイルシステム保護を有効にする](#)



## 2-1-2. コンピューターの検査



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。ファイルやフォルダ、システムメモリだけでなく、WMIデータベースやシステムレジストリを検査することも可能です。

**ユーザーインターフェース(コンピューターの検査)**

「コンピューターの検査」  
検査方法や検査対象などウイルス検査の詳細な設定を行うことなくワンクリックでウイルス検査を行うことが可能です。

「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。

**コンピューターの検査**

- コンピューターの検査  
すべてのローカルディスクを検査し、脅威を駆除します
- カスタム検査  
検査対象、駆除レベル、その他のパラメータを選択します
- リムーブメディア検査  
USB、DVD、CDおよび他のリムーブメディアの検査
- 前回の検査を再実行

ここにファイルをドラッグアンドドロップして検査します

**カスタム検査の設定画面**

コンピューターの検査

- PC
  - システムメモリ
  - ブートセクタ/UEFI
  - WMIデータベース
  - システムレジストリ
  - +
  - +
  - +
  - ネットワーク

検査するパスを入力

管理者として検査 検査 キャンセル

**コンピューターの検査中の画面**

コンピューターの検査

検索済みの項目: 0  
C:\Recycle.Bin\5-1-5-21-2364088963-42877627-1282289967-1001\85301C1.ms

検索後のアクション: アクションなし

**コンピューターの検査完了の画面**

コンピューターの検査

検索済みの項目: 0  
使用された検出エンジン: 24388 (20211209)

検索後のアクション: アクションなし

## 2-1-2. アップデート



アップデートでは、ウイルス検査で使用され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。

✓ ESET Endpoint Security	現在のバージョン:	9.1.2053.1
✓ 前回の成功したアップデート:	前回のアップデートの確認日時:	2022/07/25 9:40:24

すべてのモジュールを表示

「最新版のチェック」  
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。

最新版のチェック

アップデート中の画面

アップデート

✓ ESET Endpoint Security	現在のバージョン:	9.1.2053.1
✓ 前回の成功したアップデート:	前回のアップデートの確認日時:	2022/07/27 13:50:56

すべてのモジュールを表示

製品のアップデート中...

アップデートのキャンセル

※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。

## 2-1-3. 設定



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。

「コンピュータ」  
リアルタイムファイルシステム保護  
有効: コンピュータ上のマルウェアの即時検出と駆除  
デバイスコントロール  
停止  
アドバンスドメモリスキャナー  
有効: メモリで直接感染されたスレッドの検出。  
エクスプロイトブロック  
有効: アプリケーションのエクスプロイトに対する保護。  
ランサムウェア保護  
有効: ユーザーデータを暗号化し、身代金を要求するマルウェアに対する保護。  
プレゼンテーションモード  
一時停止: ゲームモードとプレゼンテーションのパフォーマンス最適化

リアルタイムファイルシステム保護を無効にしますか?  
短い時間でもリアルタイムファイルシステム保護を無効にすることは危険であり、ウイルスとその他の脅威に対してコンピュータが脆弱になります。

10分間一時停止

適用 キャンセル

※設定読み込み型インストール  
事前にエクスポートした設定ファイルをインストールを行う過程で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](https://eset-support.canon-its.jp/faq/show/20?&site_domain=business)

## 2-1-4. スケジューラ

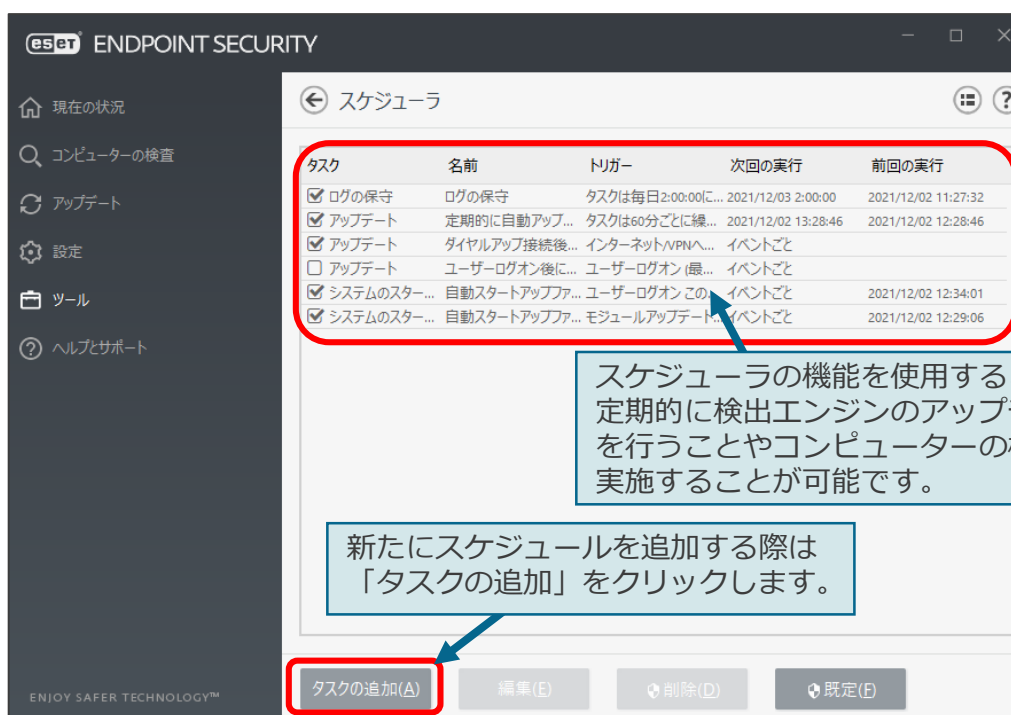


ツールのスケジューラを使用することで、検出エンジンのアップデートやコンピューターの検査を定期的に行うことが可能です。これにより、自動的にアップデートや検査が実施されるため、ユーザーが意識することなく、セキュリティをより強固にすることが可能です。

ユーザーインターフェース(ツール)



スケジューラ画面



## **2. ESET Endpoint Security V9 / ESET Endpoint アンチウイルス V9 / ESET Server Security for Microsoft Windows Server V9の機能紹介**

### **2-2. 詳細設定について**

## 2-2-1. 検出エンジン



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)

The screenshot shows the 'Detection Engine' settings in ESET Endpoint Security. The 'Detection Engine' section is highlighted with a red dashed box. Below it, there are several settings for different types of applications, each with a 'Report' and 'Protection' column. The settings are:

Application Type	Report	Protection
Real-time file system protection	Standard	Off
Malware	Standard	Off
Unwanted applications	Standard	Off
Suspicious applications	Standard	Off
Unsafe applications	Standard	Off

Callouts from the left:

- 「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。

Callouts from the right:

- 「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。

Bottom callout: **「詳細設定オプション」**

## 2-2-2. 機械学習保護



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。

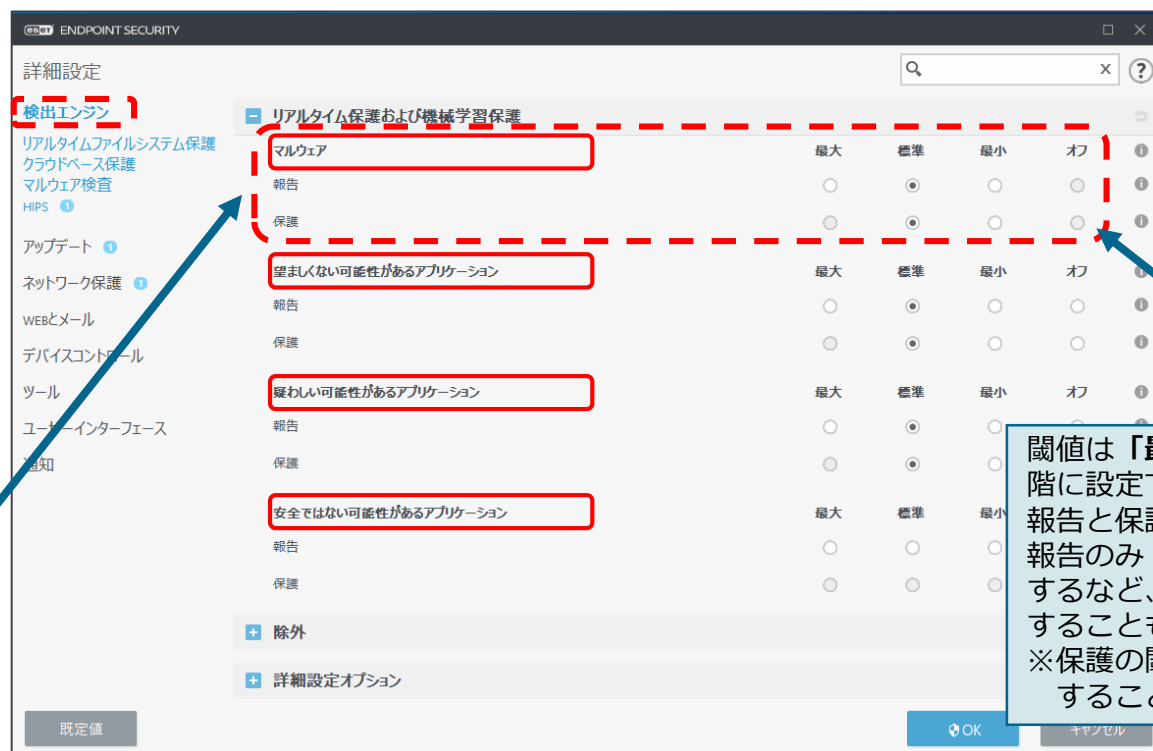
高度な機械学習モジュールを利用して、以下の検出の閾値を設定可能です。

- ・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。

詳細設定(検出エンジン画面)



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。

## 2-2-3. Antimalware Scan Interface(AMSI)保護



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Windows10、Windows11、Windows Server 2016、Windows Server 2019、Windows Server 2022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Windows10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。



## 2-2-4. 除外



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。

詳細設定(検出エンジン画面)

The screenshot shows the ESET Endpoint Security interface. On the left, the '検出エンジン' (Detection Engine) section is expanded, showing 'リアルタイム保護および機械学習保護' (Real-time protection and machine learning protection) and '除外' (Exclusions). Under '除外', 'パフォーマンス除外' (Performance exclusion) and '検出除外' (Detection exclusion) are highlighted with red boxes. A yellow arrow points from 'パフォーマンス除外' to a dialog box titled '除外の追加' (Add Exclusion) with fields for 'パス' (Path) and 'コメント' (Comment). Another yellow arrow points from '検出除外' to a dialog box titled '除外の追加' (Add Exclusion) with fields for 'パス', 'ハッシュ', '検出名', and 'コメント'. A blue arrow points from a text box to the '検出除外' dialog. A second text box points to the 'パフォーマンス除外' dialog.

**「検出除外」**  
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。

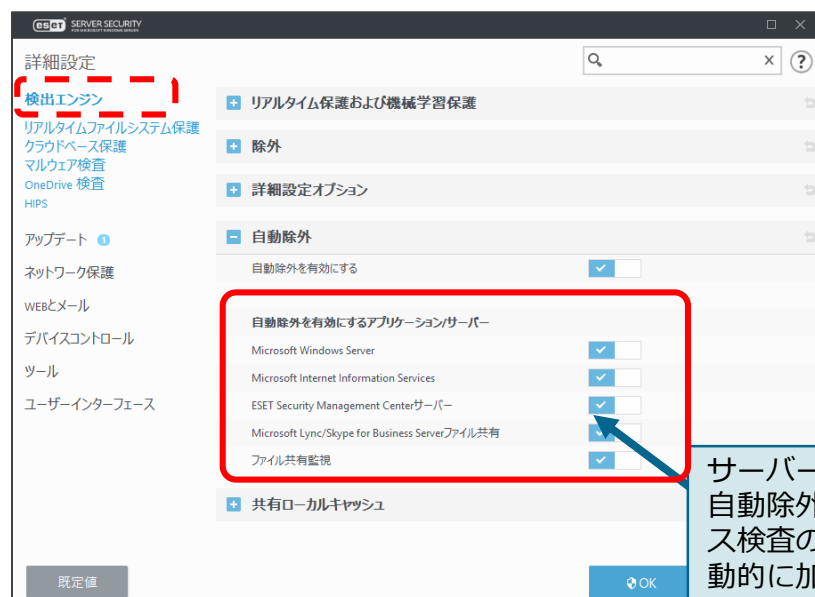
**「パフォーマンス除外」**  
特定のファイルやフォルダを検査対象から除外することが可能です。

## 2-2-5. 自動除外

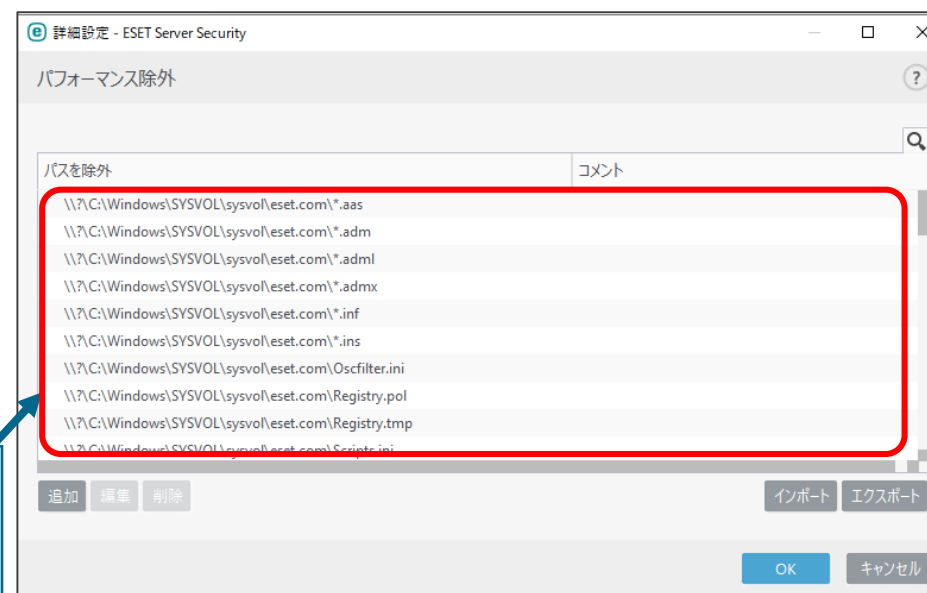
ESSW

ESET Server 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)



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】

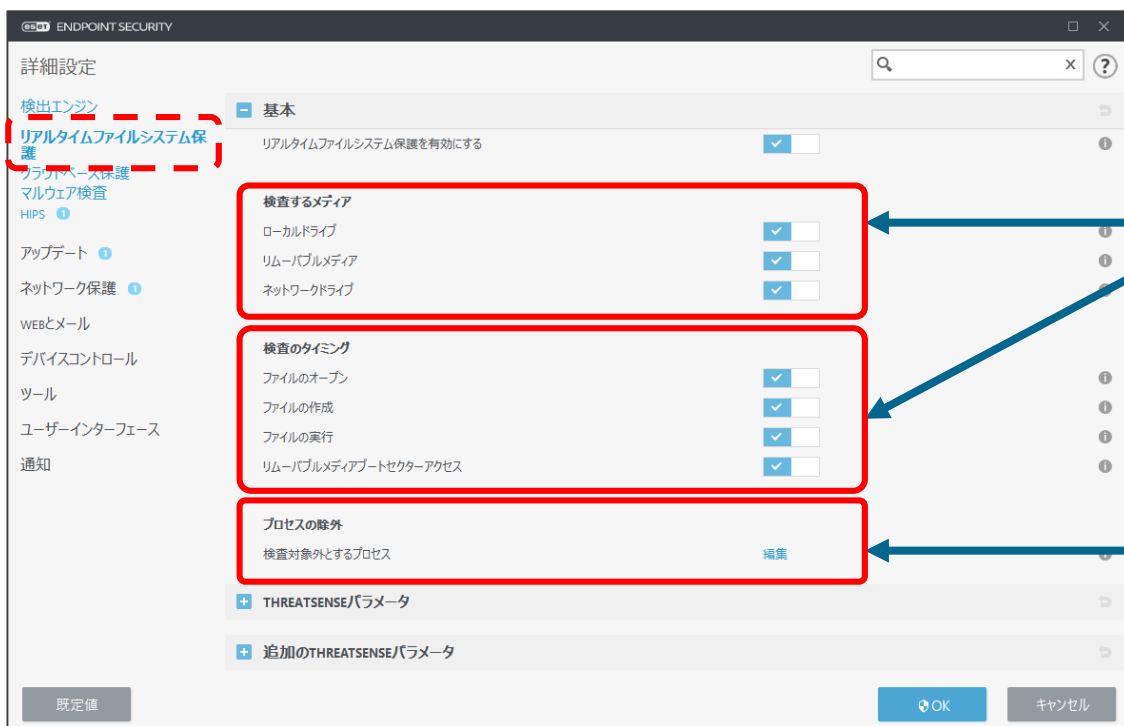
- ・ Microsoft Windows Server
- ・ Microsoft SQL Server
- ・ Microsoft Exchange Server
- ・ Microsoft ISA Server
- ・ Microsoft Fore Front Threat Management Gateway
- ・ Microsoft Internet Information Server
- ・ Microsoft Hyper-V
- ・ IBM Lotus Domino Server
- ・ Kerio Connect
- ・ Kerio Control
- ・ ESET Security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

## 2-2-6. 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、実行するときには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。

**「プロセスの除外」**  
検査から除外される実行ファイルを指定できます。実行ファイルが除外に追加されるとすぐに、そのプロセスのアクティビティがによって監視され、このプロセスで実行されるすべてのファイル処理で検査が実行されません。

## 2-2-7. UEFIスキャナー



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)

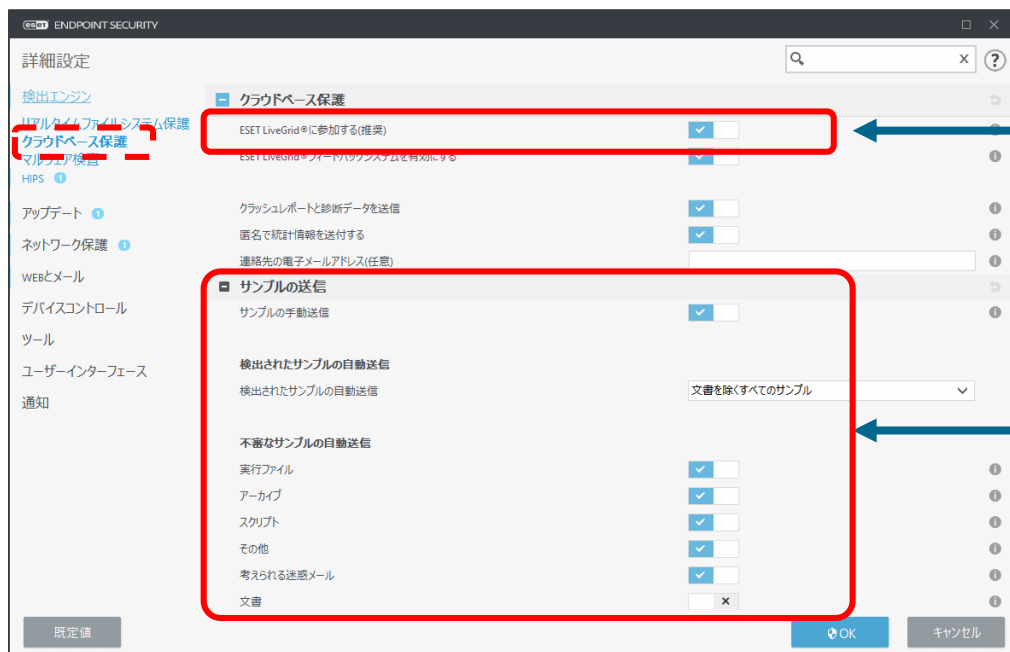


## 2-2-8. クラウドベース保護



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Webページをご参照ください。  
<https://eset-info.canon-its.jp/business/reason/#anc01>

## 2-2-9. マルウェア検査



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。  
※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。

## 2-2-10. Hyper-V検査

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)



詳細設定(Hyper-V検査画面)



## 2-2-11. OneDrive検査

ESSW

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)





## 2-2-12. HIPS

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)



### 「自己防衛を有効にする」

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。

## 2-2-13. アドバンスドメモリスキャナー



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。詳細はサイバーセキュリティ情報局、キーワード辞典をご参照ください。

[https://eset-info.canon-its.jp/malware\\_info/term/detail/00092.html](https://eset-info.canon-its.jp/malware_info/term/detail/00092.html)

また、下記Webページもご参照ください。

<https://eset-info.canon-its.jp/business/reason/#anc01>

## 2-2-14. エクスプロイトブロッカー



ブラウザ、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。



### ※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。詳細はサイバーセキュリティ情報局、キーワード辞典をご参照ください。

[https://eset-info.canon-its.jp/malware\\_info/term/detail/00048.html](https://eset-info.canon-its.jp/malware_info/term/detail/00048.html)

### ※脆弱性(バリエナラビリティ)

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。詳細はサイバーセキュリティ情報局、キーワード辞典をご参照ください。

[https://eset-info.canon-its.jp/malware\\_info/term/detail/00068.html](https://eset-info.canon-its.jp/malware_info/term/detail/00068.html)

## 2-2-15. ランサムウェア保護



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。



※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。詳細はサイバーセキュリティ情報局、キーワード辞典をご参照ください。  
[https://eset-info.canon-its.jp/malware\\_info/term/detail/00104.html](https://eset-info.canon-its.jp/malware_info/term/detail/00104.html)

## 2-2-16. アップデート

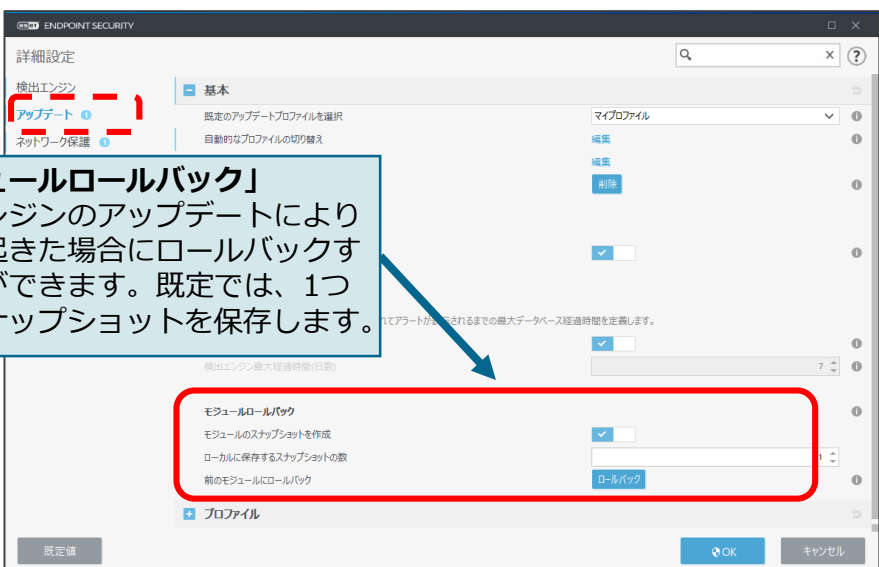


アップデートの項目では、検出エンジンの取得先を変更することなどが可能です。ミラーサーバーより検出エンジンの取得をする場合は、こちらの項目より設定してください。また、アップデートサーバーは通常のアップデートサーバーのほか、通常の検出エンジンの配信より少し早く配信されるテストモードや、逆に通常配信後12時間経過してから配布される遅延アップデートを選ぶことが可能です。

※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。

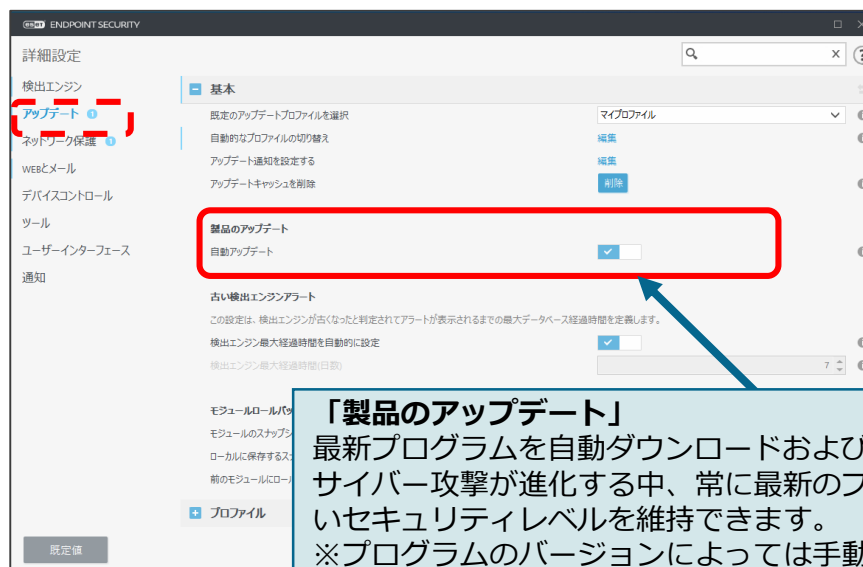
高い可用性や安定性が必要な実働サーバーやワークステーションでは決して使用しないでください

詳細設定(アップデート画面)



**「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。

詳細設定(プログラムコンポーネントのアップデート画面)



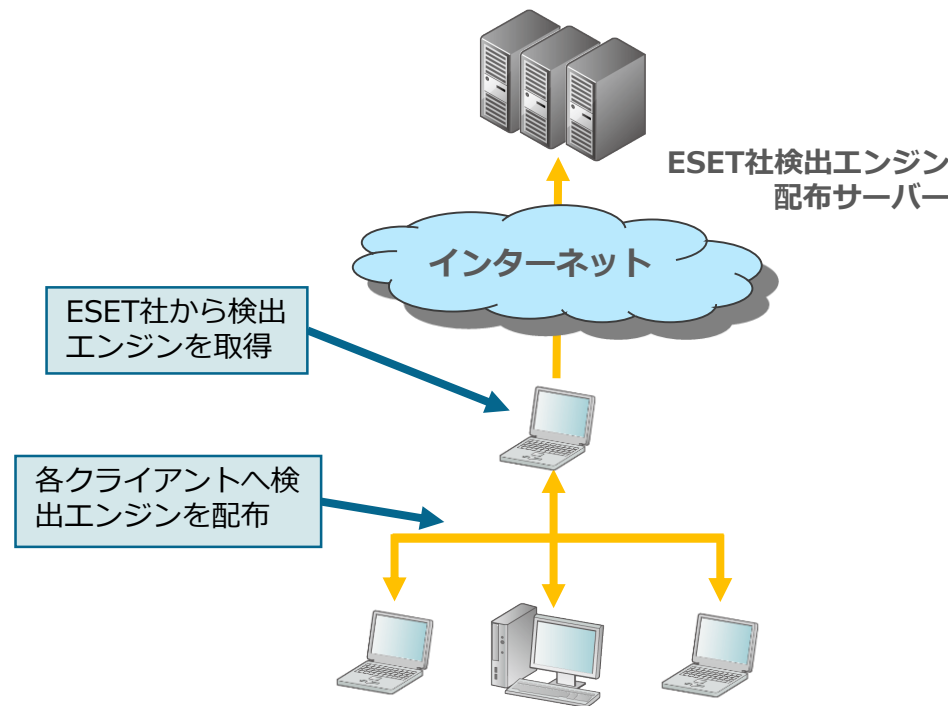
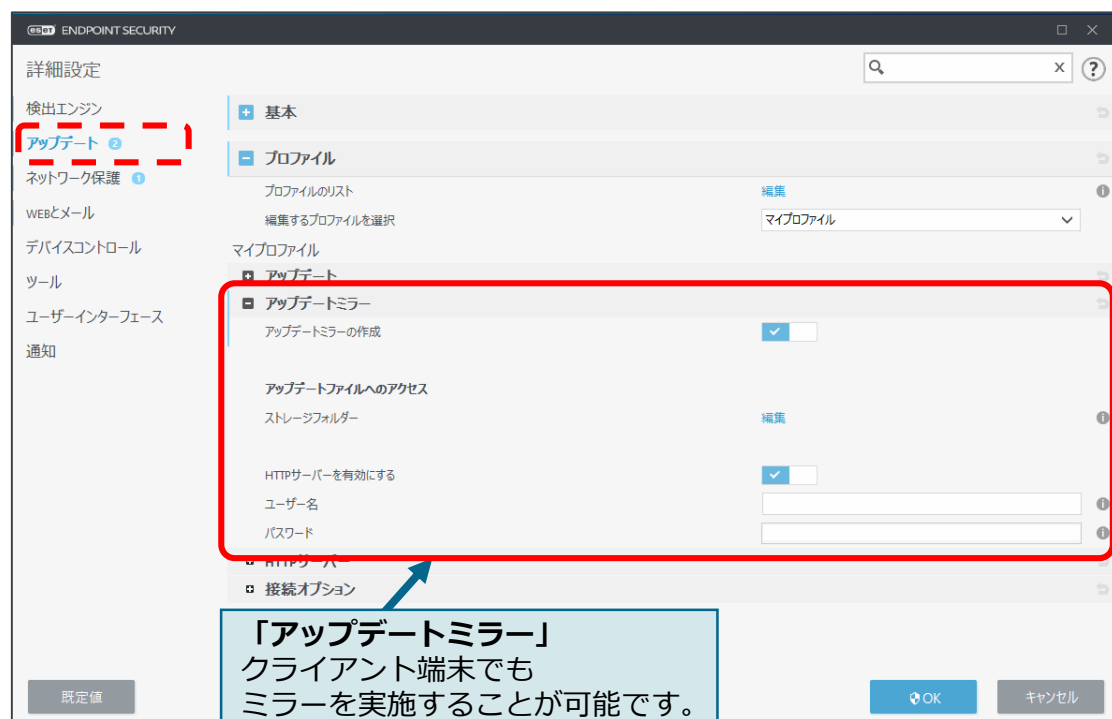
**「製品のアップデート」**  
最新プログラムを自動ダウンロードおよびインストールできる機能です。サイバー攻撃が進化する中、常に最新のプログラムを利用することで高いセキュリティレベルを維持できます。  
※プログラムのバージョンによっては手動でのバージョンアップが必要な場合があります。

## 2-2-17. ミラー機能



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ため、サーバーをご用意いただかなくても、ミラー環境を構築することが可能です。

詳細設定(アップデート画面)



## 2-2-18. ファイアウォール

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)

The image displays three overlapping screenshots from the ESET Endpoint Security interface, illustrating the steps to configure a firewall rule. Yellow arrows indicate the flow from the main settings to the rule list, and then to the rule configuration dialog.

- Left Screenshot (Main Settings):** Shows the '詳細設定' (Detailed Settings) window. The 'ファイアウォール' (Firewall) section is expanded, and the '詳細' (Details) sub-section is selected. A red box highlights the '詳細' button.
- Middle Screenshot (Rule List):** Shows the 'ファイアウォールルール' (Firewall Rules) window. A table lists rules with columns for '名前' (Name), '有効' (Enabled), 'プロトコル' (Protocol), 'プロファイル' (Profile), 'アクション' (Action), '方向' (Direction), 'ローカル' (Local), 'リモート' (Remote), and 'アプリケーション' (Application). A red box highlights the '追加' (Add) button at the bottom left.
- Right Screenshot (Rule Configuration):** Shows the 'ルールの追加' (Add Rule) dialog box. The 'ローカル' (Local) tab is active. Fields include '名前' (Name), '有効' (Enabled), '方向' (Direction), 'アクション' (Action), 'プロトコル' (Protocol), 'ICMPタイプ/コード' (ICMP Type/Code), 'プロファイル' (Profile), 'ログ記録の重大度' (Log Severity), and 'ユーザーに通知' (Notify User).

## 2-2-19. ネットワーク攻撃保護



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、ブルートフォース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)

詳細設定

検出エンジン

ネットワーク攻撃保護

ネットワーク攻撃保護(IDS)を有効にする

ポットネット保護を有効にする

IDSルール

**総当たり攻撃保護**

総当たり攻撃保護を有効にする

ルール

詳細設定オプション

既定値

**「総当たり攻撃保護」**  
SMB・RDPに対する総当たり攻撃から端末を保護します。事前に定義した認証の最大試行回数を超えた場合、一定期間接続をブロックします。  
※EES/EEA V9.0以降のみ対応

詳細設定

検出エンジン

ネットワーク攻撃保護

ネットワーク保護

ファイアウォール

**ネットワーク攻撃保護**

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

通知

詳細設定オプション

**侵入検出**

プロトコルSMB

プロトコルRPC

プロトコルRDP

ARPポイズニング攻撃を検出

TCPポートスキャン攻撃を検出

未知のIPアドレスを検出

IPアドレスをブロック

IPアドレスで通知

受信攻撃に対する受信攻撃を通知

既定値

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。

**「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。

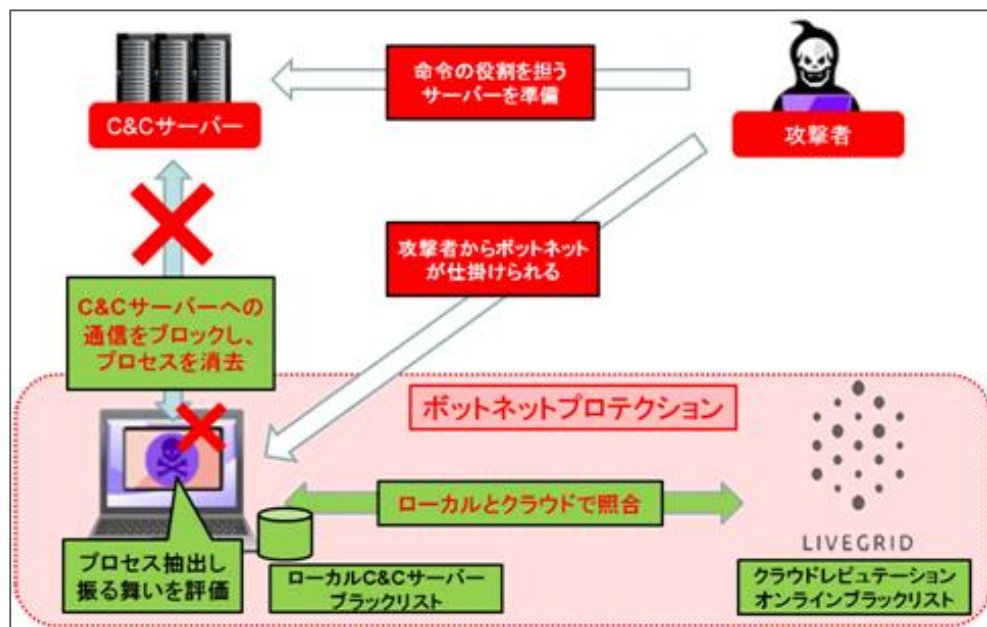


## 2-2-20. ボットネット保護

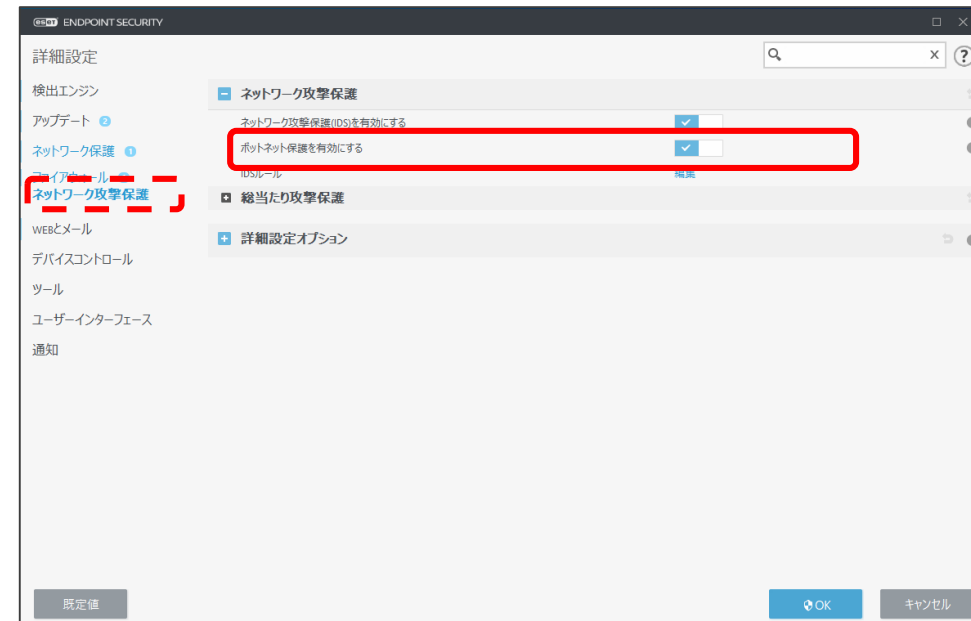


通信を解析し、リモートからのアクセスを検知して、迅速にボットを検出します。多層防御における防御層のひとつとして、不正サーバーへの送信となる不審な通信やアドレスを検知して遮断することで、標的型攻撃を防ぎます。

ボットネット攻撃例



詳細検査(ネットワーク攻撃保護画面)



※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。

※下記サイバーセキュリティ情報局のWebページ『ボットネットとは何か? どうやって防ぐのか?』もご参照ください。

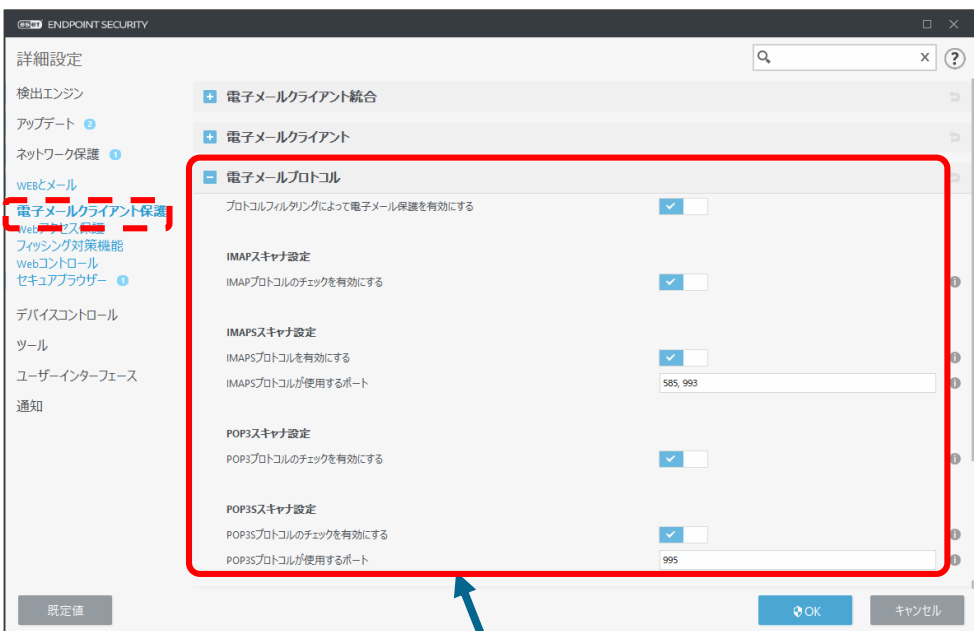
[https://eset-info.canon-its.jp/malware\\_info/trend/detail/150120\\_3.html](https://eset-info.canon-its.jp/malware_info/trend/detail/150120_3.html)

## 2-2-21. WEBとメール



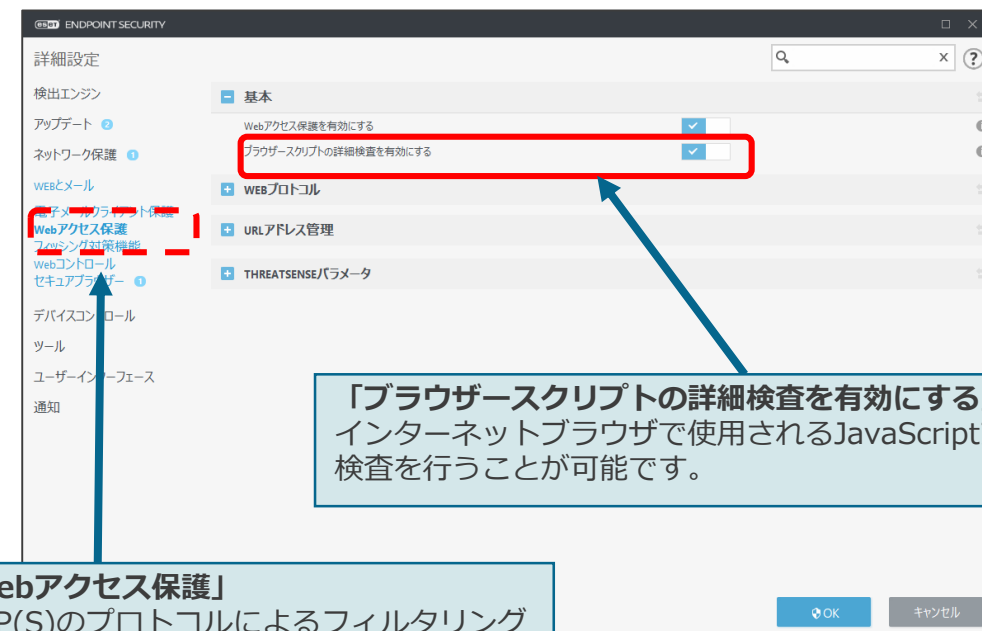
プロトコルフィルタリングの機能により、使用しているインターネットブラウザやメールクライアントに関係なく、HTTP(S)、POP3(S)、IMAP(S)トラフィックの検査を行い、ウイルスを検出することが可能です。これによりWebブラウザやメールの添付ファイルに潜むウイルスを検知することが可能です。

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。

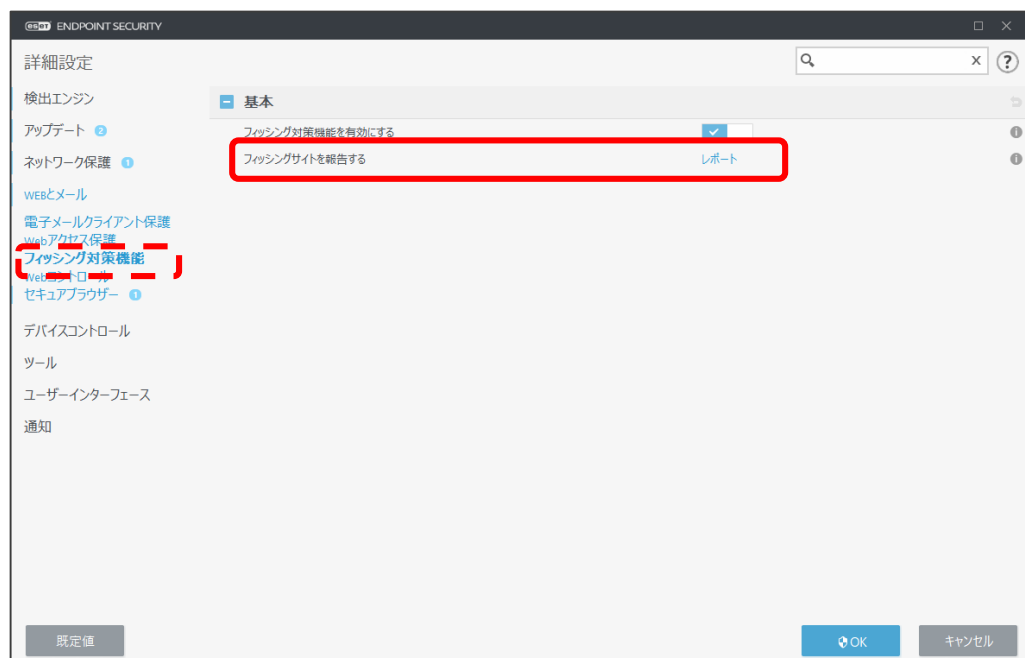
**「Webアクセス保護」**  
HTTP(S)のプロトコルによるフィルタリングの設定やURLアドレスリストを使用してブロック、許可、また検査から除外するアドレスを指定することが可能です。

## 2-2-22. フィッシング対策



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の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



### ※フィッシング詐欺

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。

詳細はサイバーセキュリティ情報局、キーワード辞典をご参照ください。

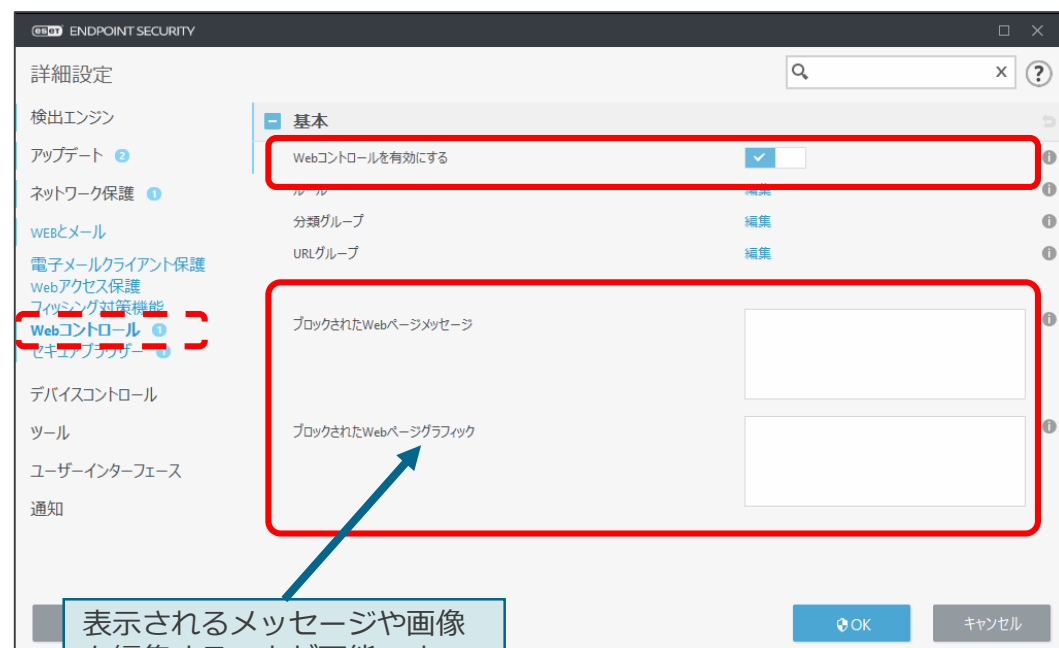
[https://eset-info.canon-its.jp/malware\\_info/term/detail/00128.html](https://eset-info.canon-its.jp/malware_info/term/detail/00128.html)

## 2-2-23. Webコントロール

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



## 2-2-24. セキュアブラウザ

EES

コンピューターで実行中の他のプロセスからWebブラウザを保護します。ブラウザのメモリ空間やブラウザウィンドウの内容が改ざんされることを防止します。任意のWebサイトやESETのインターネットバンキングリストに登録されているWebサイトをセキュアブラウザにリダイレクトします。

※セキュアブラウザはESET Endpoint Security でのみご使用いただけます。

詳細設定(セキュアブラウザ画面)

詳細設定

基本

セキュアブラウザを有効にする

WEBサイトリダイレクト

保護されたWebサイトリダイレクトを有効にする

保護されたWebサイト [編集](#)

安全なオンラインバンキングと決済ページ

セキュアブラウザ

拡張メモリ保護

キーボード保護

ブラウザの緑色のフレーム

セキュアブラウザの対話型アラートを設定 [編集](#)

Webサイトの追加

Webサイトページ

このWebサイトを開く

セキュアブラウザ

標準のブラウザ

OK キャンセル

既定

「キーボード保護を有効にする」  
セキュアブラウザにキーボードから入力した情報は他のアプリケーションから隠すことができます。これにより、キーロガーに対する保護が強化されます。

「保護されたWebサイト」(編集画面)  
セキュアブラウザにリダイレクトさせるWebサイトページを設定できます。

セキュアブラウザ(例)

ESET

ESETを使用してインターネットを安全に閲覧

ESET安全なブラウザを使用して、セキュリティを強化し、オンラインで閲覧しているときにデータを保護します。

※EES/EEA V9.1以降、緑色のフレームを消すことも可能です。

# 2-2-25. デバイスコントロール



デバイスコントロール機能を使用することで、CD/DVDや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			
	許可 (読み込み/ 書き込み)	ブロック	書き込み ブロック (読み取り 専用)	警告
ディスクストレージ	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
CD/DVD	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
USBプリンタ	<input type="radio"/>	<input type="radio"/>	—	<input type="radio"/>
FireWire	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Bluetoothデバイス	<input type="radio"/>	<input type="radio"/>	—	<input type="radio"/>
スマートカードリーダー	<input type="radio"/>	<input type="radio"/>	—	<input type="radio"/>
イメージングデバイス	<input type="radio"/>	<input type="radio"/>	—	<input type="radio"/>
モデム	<input type="radio"/>	<input type="radio"/>	—	<input type="radio"/>
LPT/COMポート	<input type="radio"/>	<input type="radio"/>	—	<input type="radio"/>
ポータブルデバイス	<input type="radio"/>	<input type="radio"/>	—	<input type="radio"/>
すべてのデバイスタイプ	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

デバイスコントロール設定

ルール名: 無題  
 有効:   
 適用期間: 常に  
 デバイスタイプ: ディスクストレージ  
 アクション: 許可  
 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: 常に

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



デバイスコントロールブロックメッセージ画面



## 2-2-26. タイムスロット



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。

## 2-2-27. プロキシサーバ



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。

「検出」をクリックすると、自動的にInternet ExplorerまたはGoogle Chromeのインターネットオプションで指定したパラメーターがコピーされます。

「プロキシが使用できない場合は直接接続を使用する」  
「プロキシサーバを使用する」設定をしている際に、プロキシに接続できない場合は、プロキシをバイパスして通信を行います。



## 2-2-28. パスワード保護

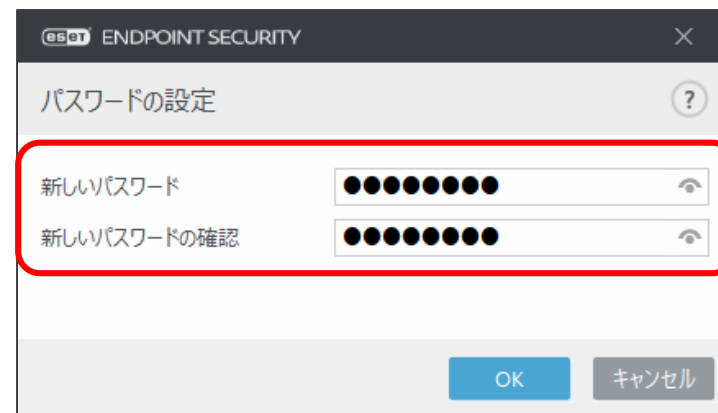


設定をパスワードで保護することにより、ユーザーに設定を変更されたり、ESETのウイルス・スパイウェア対策プログラムをアンインストールされることを防止することが可能です。

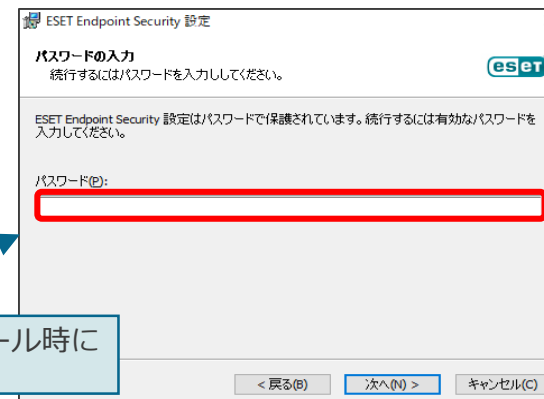
詳細設定(ユーザーインターフェース画面)



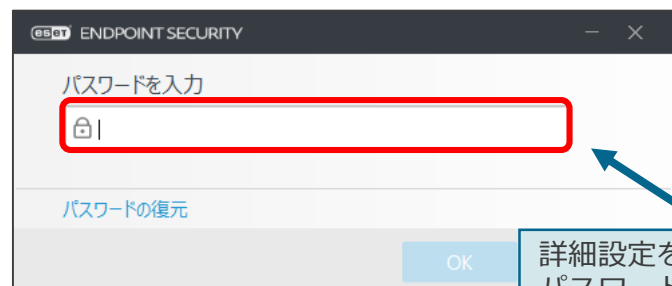
パスワードを設定する場合は有効にしてください。



パスワード入力画面(アンインストールする場合)



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。

## 2-2-29. 電子メール通知



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)

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。

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。

受信者アドレスは「;(セミコロン)」で区切ることで複数登録可能です。

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。

### 3. プログラム別の機能比較

### 3. プログラム別の機能比較 (1/3)

機能名	EES			EEA			ESSW(EFSW)		
	V7.3	V8.X	V9.X	V7.3	V8.X	V9.X	V7.3	V8.X	V9.X
<b>ウイルス・スパイウェア対策機能</b>									
コンピューターの検査	○	○	○	○	○	○	○	○	○
コンピューターの検査 WMIデータベースやシステムレジストリの検査	×	○	○	×	○	○	×	○	○
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	○	○	○	○	○	○	○	○	○
スクリプトに基づく攻撃保護	○	○	○	○	○	○	○	○	○
リアルタイムファイルシステム保護	○	○	○	○	○	○	○	○	○
機械学習保護	○	○	○	○	○	○	○	○	○
UEFIスキャナー	○	○	○	○	○	○	○	○	○
ESET LiveGrid	○	○	○	○	○	○	○	○	○
アイドル状態検査	○	○	○	○	○	○	○	○	○
OneDrive検査	×	×	×	×	×	×	○	○	○
Hyper-V検査	×	×	×	×	×	×	○	○	○
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	○	○	○	○	○	○	○	○	○

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

### 3. プログラム別の機能比較 (2/3)

機能名	EES			EEA			ESSW(EFSW)		
	V7.3	V8.X	V9.X	V7.3	V8.X	V9.X	V7.3	V8.X	V9.X
<b>ウイルス・スパイウェア対策機能</b>									
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	○	○	○	○	○	○	○	○	○
<b>ネットワーク通信関連機能</b>									
ファイアウォール	○	○	○	×	×	×	×	×	×
迷惑メール対策	○	○	○	×	×	×	×	×	×
Webコントロール	○	○	○	×	×	×	×	×	×
セキュアブラウザー	×	○	○	×	×	×	×	×	×
バルナラビリティシールド	○	○	○	○	○	○	○	○	○
ボットネット保護	○	○	○	○	○	○	○	○	○
<b>アップデート・ミラーサーバー機能</b>									
検出エンジンのアップデート	○	○	○	○	○	○	○	○	○
プログラムコンポーネントアップデート(PCU)	×	○	○	×	○	○	×	○	○
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 (3/3)

機能名	EES			EEA			ESSW(EFSW)		
	V7.3	V8.X	V9.X	V7.3	V8.X	V9.X	V7.3	V8.X	V9.X
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	×	×	×	×	×	×	○	○	○
デバイスコントロール	○	○	○	○	○	○	○	○	○
デバイスコントロール - グループルールの追加	○	○	○	○	○	○	○	○	○
タイムスロット	×	○	○	×	○	○	×	○	○
プロキシサーバの設定	○	○	○	○	○	○	○	○	○
電子メール通知機能	○	○	○	○	○	○	○	○	○
パスワードによる保護	○	○	○	○	○	○	○	○	○
ESET Security Management Center V7.2による管理 ※	○	○	○	○	○	○	○	○	○
ESET PROTECT V8による管理 ※	○	○	○	○	○	○	○	○	○
ESET PROTECT V9による管理 ※	○	○	○	○	○	○	○	○	○

※ 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。