

ESET Server Security for Microsoft Windows Server V12 機能紹介資料

第1版

2025年2月19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
 - 1-2. 本プログラムの特徴

2. ESET Server Security for Microsoft Windows Server V12.x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. はじめに（本資料について）

本資料はWindows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
ESET Server Security for Microsoft Windows Server V12.x (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の後継プログラムです。
- ESET Server Security for Linux / Microsoft Windows Serverでは、Linux Server OS向けのプログラムもご使用いただけます。Linux Server OS向けの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 Server Security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. はじめに (本資料について)

- 本資料の画面構成は以下になります。

機能名を記載しております。

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などを検出することが可能です。

「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。

「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。

ネットワークプロトコル(SMB・RPC・RDP)の既知の脆弱性(バグ/脆弱性)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。

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。

1-2. はじめに（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 Server Security for Microsoft Windows

Server V12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。



The screenshot displays the ESET Server Security user interface. On the left, a dark sidebar contains a menu with icons and labels: 監視 (Monitoring), ログファイル (Log Files), 検査 (Check), アップデート (Update), 設定 (Settings), ツール (Tools), and ヘルプとサポート (Help and Support). The main content area is divided into sections. The top section, highlighted with a green header, shows a green checkmark and the text '保護されています' (Protected). Below this, it states 'モジュールは最新です' (Modules are up to date) with the last successful update date: '2023/03/22 6:24:06'. The next section, titled 'ファイルシステム保護ステータス' (File System Protection Status), shows statistics: '感染: 0' (Infections: 0), '駆除済み: 0' (Quarantined: 0), '未感染: 141,890' (Not infected: 141,890), and '合計: 141,890' (Total: 141,890). At the bottom, system information is visible: 'Standard 64-bit (10.0.17763)' and '(M) i7-11700 @ 2.50GHz (2496 MHz), 2047 MB RAM'. On the right, two alert panels are shown. The top one has a yellow header and says '注意が必要です' (Attention required), with a warning icon and the text 'デバイスコントロールが完全に機能していません' (Device control is not fully functioning). The bottom one has a red header and says 'セキュリティアラート (必須設定残り: 2)' (Security Alert (2 required settings remaining)), with a warning icon and the text '不審な可能性があるアプリケーションの検出が設定されていません' (Detection of suspicious applications is not configured). A sidebar menu on the right also lists: 監視 (Monitoring), ログファイル (Log Files), 検査 (Check), アップデート (Update), and 設定 (Settings).

正常に動作をしている場合は、緑色で表示されます。

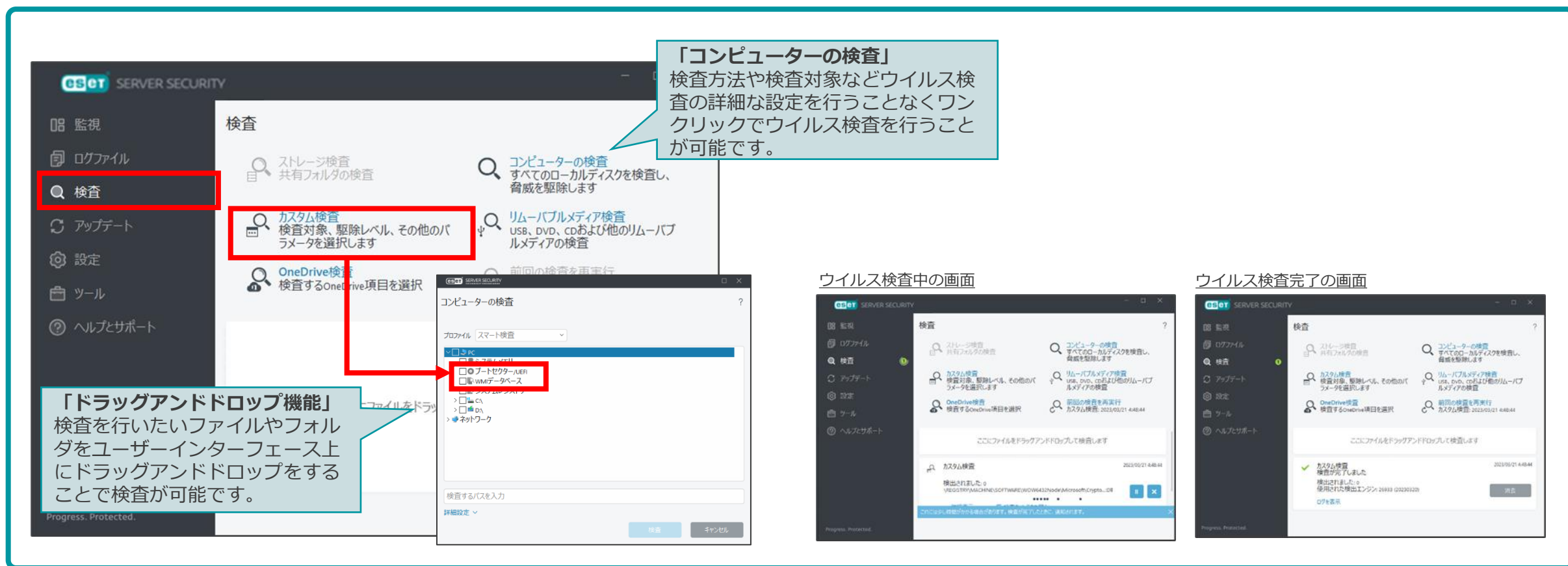
注意が必要な場合は黄色
重大な問題がある場合は赤色
で表示されます。

以下の7つのメニューがあります。

- ・ 監視
- ・ ログファイル
- ・ 検査
- ・ アップデート
- ・ 設定
- ・ ツール
- ・ ヘルプとサポート

2-1-2. 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。また、WMIデータベースやシステムレジストリを検査する機能もご利用いただけます。



「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。

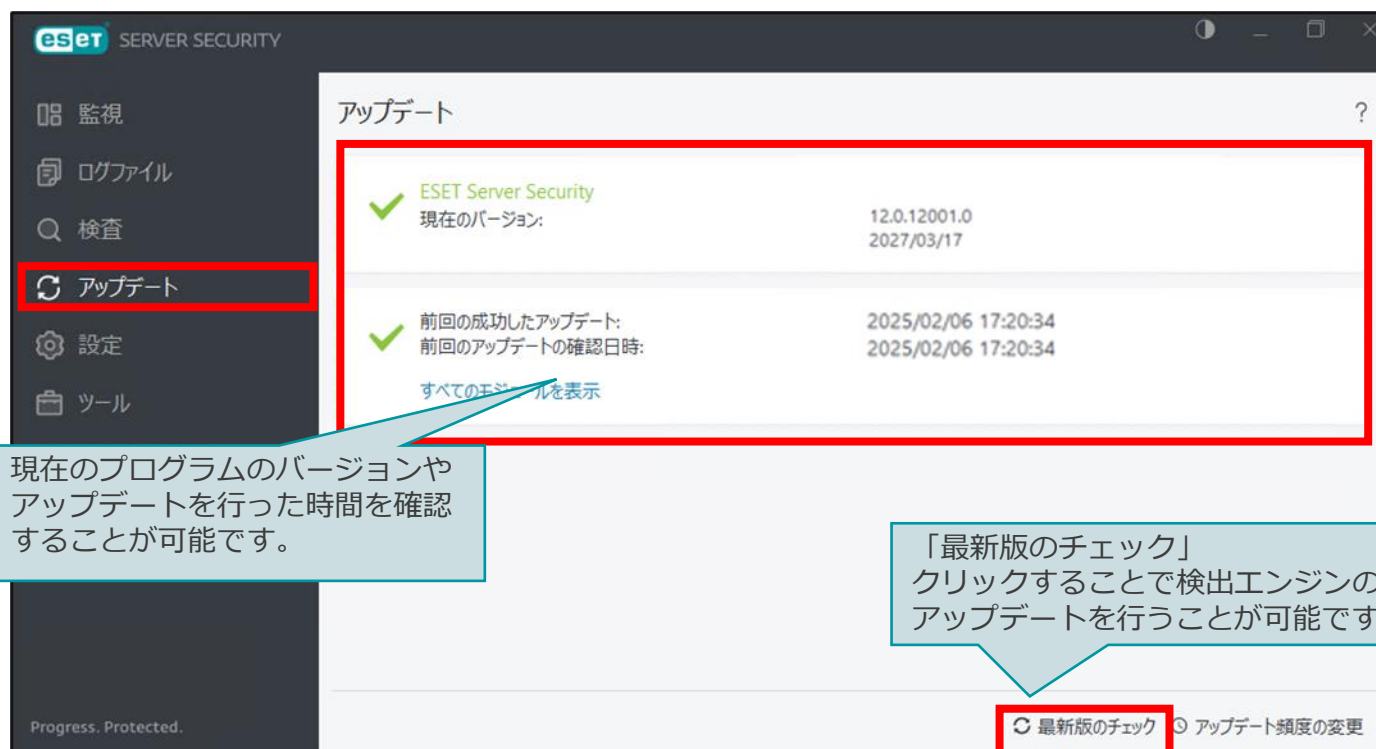
「ドラッグアンドドロップ機能」
検査を行いたいファイルやフォルダをユーザーインターフェース上にドラッグアンドドロップすることで検査が可能です。

ウイルス検査中の画面

ウイルス検査完了の画面

2-1-3. アップデート

- 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。



The screenshot shows the 'アップデート' (Update) window in ESET Server Security. The left sidebar has 'アップデート' highlighted with a red box. The main content area, also outlined in red, shows the current version (12.0.12001.0) and the last successful update (2025/02/06 17:20:34). At the bottom right, the '最新版のチェック' (Check for updates) button is highlighted with a red box.

項目	値
現在のバージョン:	12.0.12001.0 2027/03/17
前回の成功したアップデート:	2025/02/06 17:20:34
前回のアップデートの確認日時:	2025/02/06 17:20:34

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。

2-1-4. 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。



「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。

※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

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
- HIPS
 - 有効: アプリケーションからの望ましくない動作の検出と防止
- アドバンスドメモリスキャナー
 - 有効: メモリで直接隠蔽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

ウイルス対策およびスパイウェア保護を一時停止

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

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。

2-1-5. 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。



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ー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。

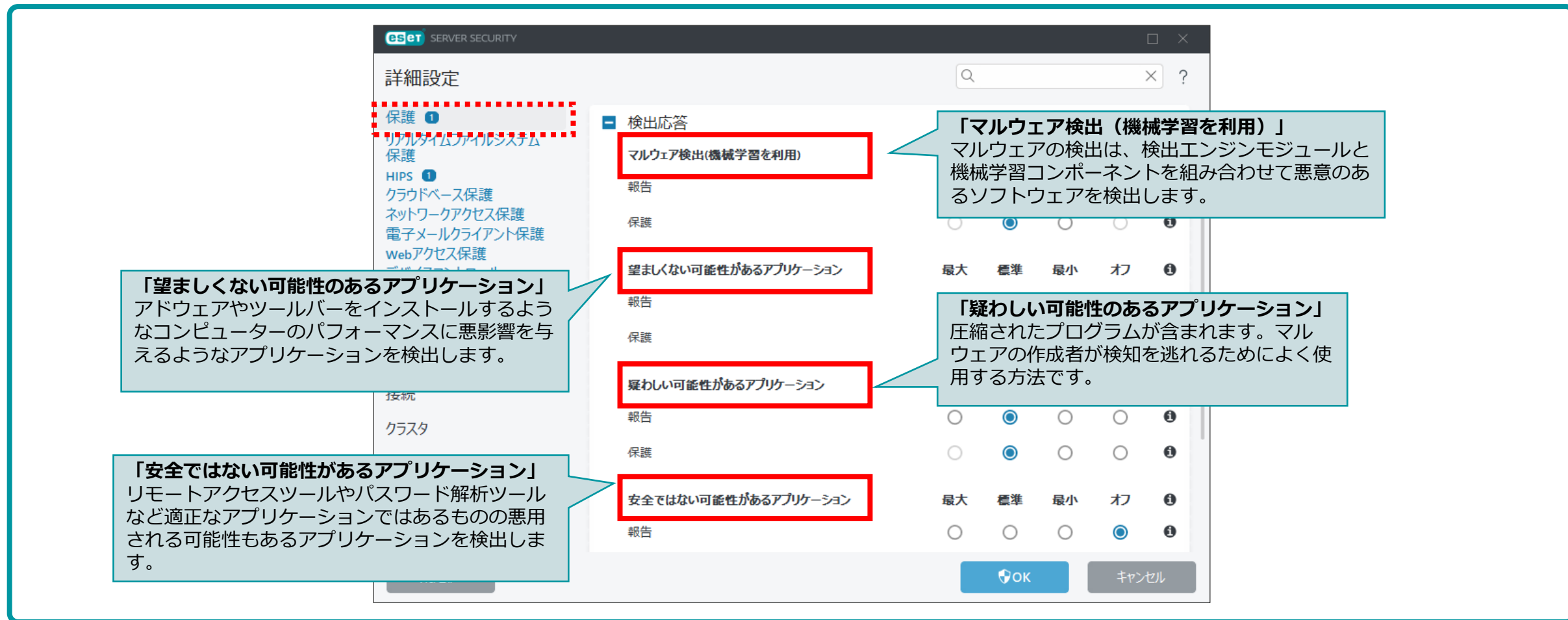
タスク	トリガー	次回の実行	前回の実行
<input checked="" type="checkbox"/> ログの保守 ログの保守	タスクは毎日2:00:00に実行さ...	2025/02/08 2:00:00	2025/02/07 2:00:44
<input checked="" type="checkbox"/> アップデート 定期的に自動アップデート	タスクは60分ごとに繰り返...	2025/02/08 0:34:43	2025/02/07 23:34:43
<input type="checkbox"/> アップデート ユーザーログイン後に自動アップデート	ユーザーログイン(最多で時...	イベントごと	
<input checked="" type="checkbox"/> システムのスタートアップファイルのチェック 自動スタートアップファイルのチェック	ユーザーログイン このタスクは...	イベントごと	2025/02/06 16:45:45
<input checked="" type="checkbox"/> システムのスタートアップファイルのチェック 自動スタートアップファイルのチェック	モジュールアップデートの成功...	イベントごと	2025/02/07 23:34:58
<input checked="" type="checkbox"/> 脆弱性とパッチ管理コンピューターの検査 脆弱性とパッチの日次コンピューターの検査	タスクは毎日12:00:00に実行...	2025/02/08 0:31:55	

2. ESET Server Security for Microsoft Windows Server V12の機能紹介

2-2. 詳細設定について

2-2-1. 保護

- 保護の項目では、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。



The screenshot shows the 'eSET SERVER SECURITY' interface with the '詳細設定' (Detailed Settings) window open. The '保護' (Protection) section is highlighted with a red dashed box. The '検出応答' (Detection Response) section is highlighted with a red solid box and contains three items:

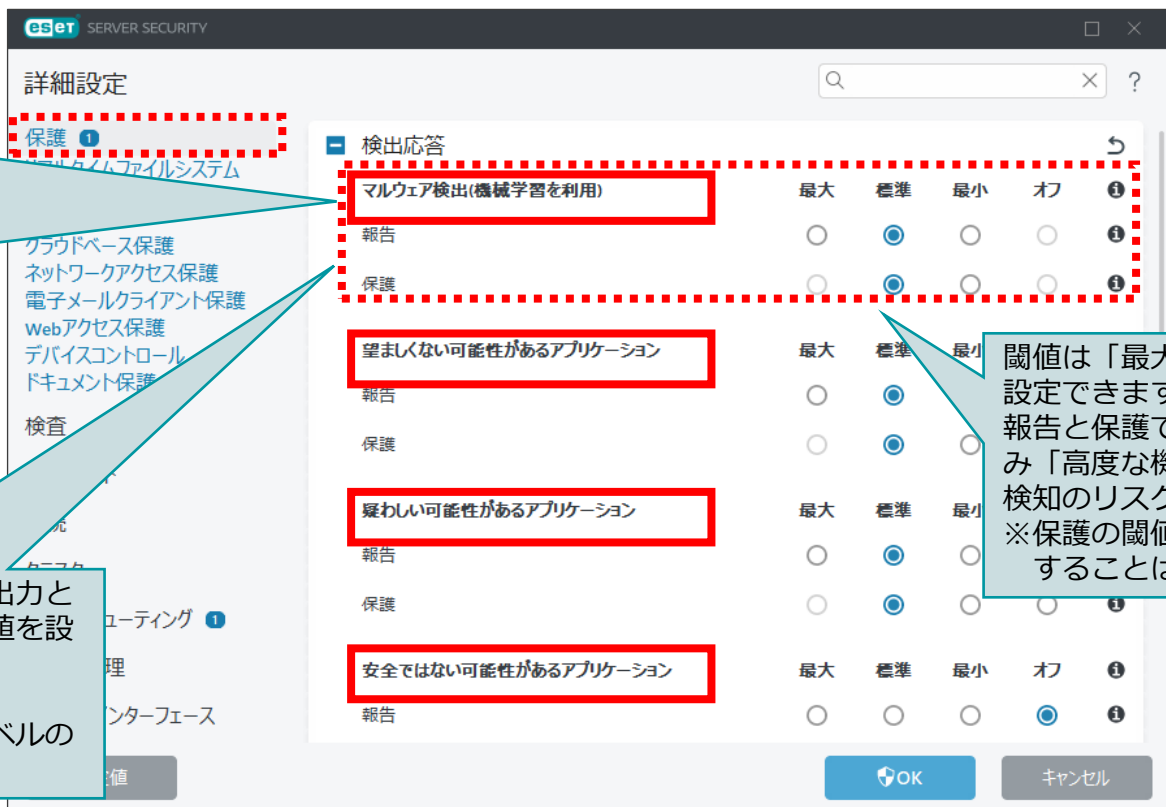
- マルウェア検出(機械学習を利用)** (Malware detection using machine learning)
- 望ましくない可能性のあるアプリケーション** (Applications with undesirable possibilities)
- 疑わしい可能性のあるアプリケーション** (Applications with suspicious possibilities)
- 安全ではない可能性のあるアプリケーション** (Applications with unsafe possibilities)

Callout boxes provide detailed explanations for these categories:

- 「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。
- 「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。
- 「マルウェア検出(機械学習を利用)」**
マルウェアの検出は、検出エンジンモジュールと機械学習コンポーネントを組み合わせることで悪意のあるソフトウェアを検出します。
- 「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。

2-2-2. 検出応答

- 検出応答は、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。

- ・マルウェア検出（機械学習を利用）
- ・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。

検出項目	報告	保護
マルウェア検出(機械学習を利用)	最大	標準
望ましくない可能性があるアプリケーション	最大	標準
疑わしい可能性があるアプリケーション	最大	標準
安全ではない可能性があるアプリケーション	最大	標準

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. 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、デバイスコントロールルールやWeb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デバイスの利用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コントロールはESSW V12.0より追加された機能です。



タイムスロット詳細設定

詳細設定

- 保護 3
- リアルタイムウイルスシステム保護
- HIPS 1
- クラウドベース保護
- ネットワークアクセス保護 1
- 電子メールクライアント保護
- Webアクセス保護
- デバイスコントロール 1
- ドキュメント保護

検出応答

SSL/TLS

タイムスロット

タイムスロット 編集

タイムスロット

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

タイムスロットの追加

名前

説明

平日 時刻

時間範囲の追加

平日

- 日曜日
- 月曜日
- 火曜日
- 水曜日
- 木曜日
- 金曜日
- 土曜日

終日

開始時刻 9:00:00

終了時刻 17:00:00

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、「デバイスコントロール」および「Web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。

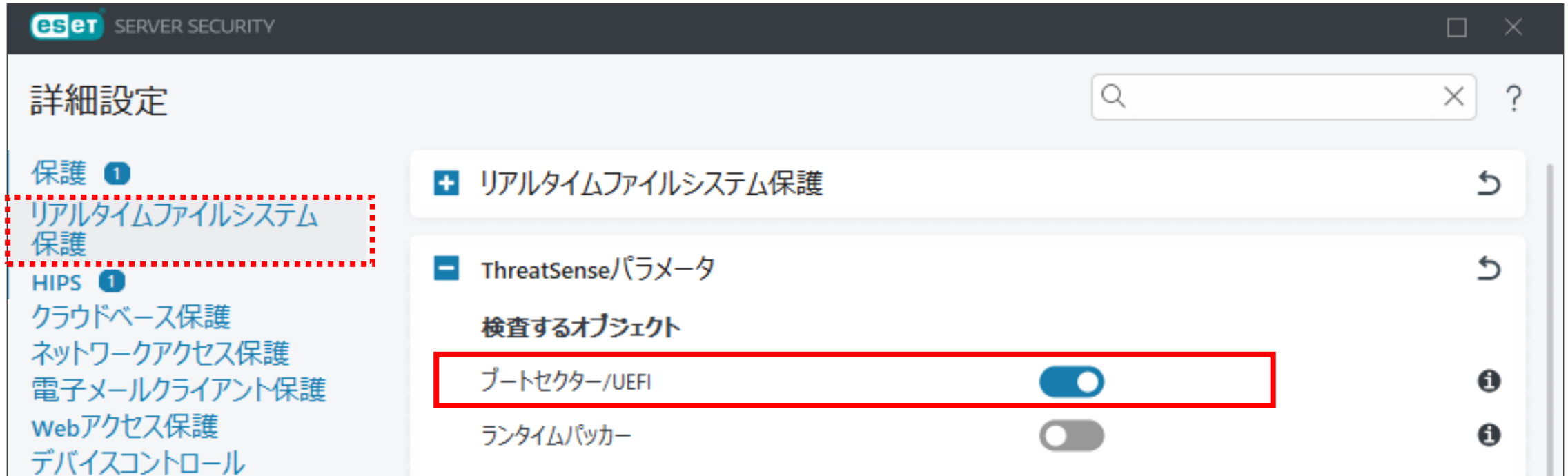
2-2-4. リアルタイムファイルシステム保護

- 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。



2-2-5. 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。



2-2-6. 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。



「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。

2-2-7. 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。



※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

また、下記Webページもご参照ください。
<https://canon.jp/business/solution/it-sec/lineup/eset/feature/antivirus>

2-2-8. エクスプロイトブロッカー

- 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。



※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

※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

2-2-9. 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。

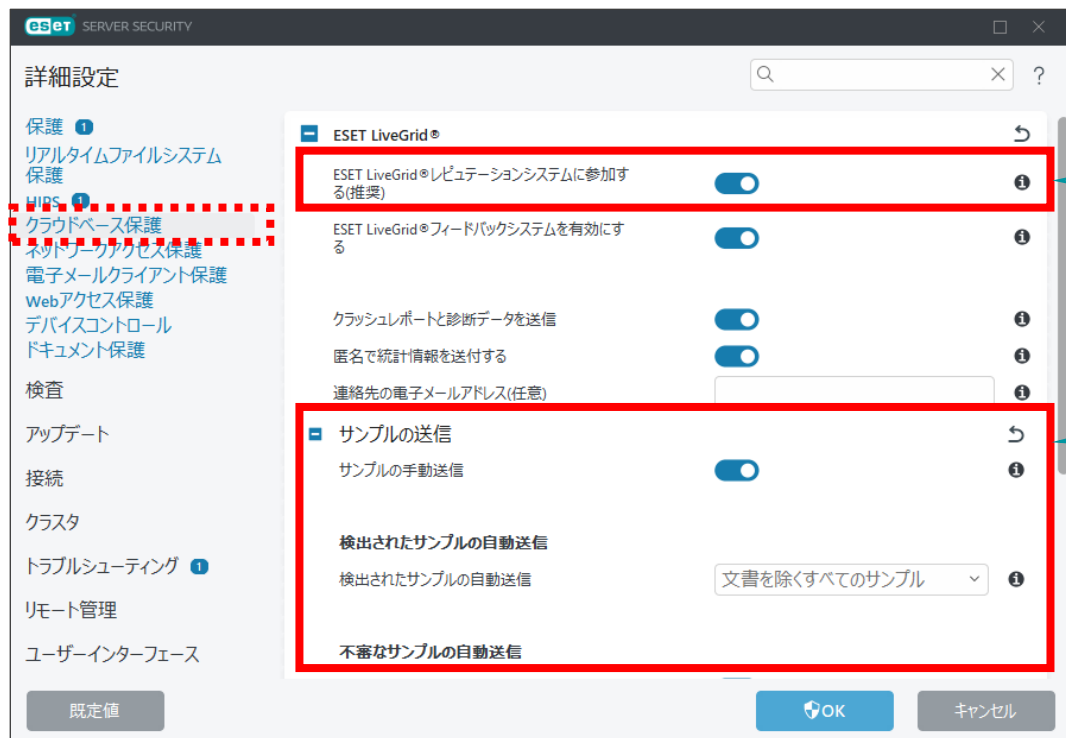
※この機能を正しく動作させるには、ESET LiveGridを有効にする必要があります。



※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

2-2-10. 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。



「ESET LiveGrid®レピュテーションシステムに参加する」
 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。

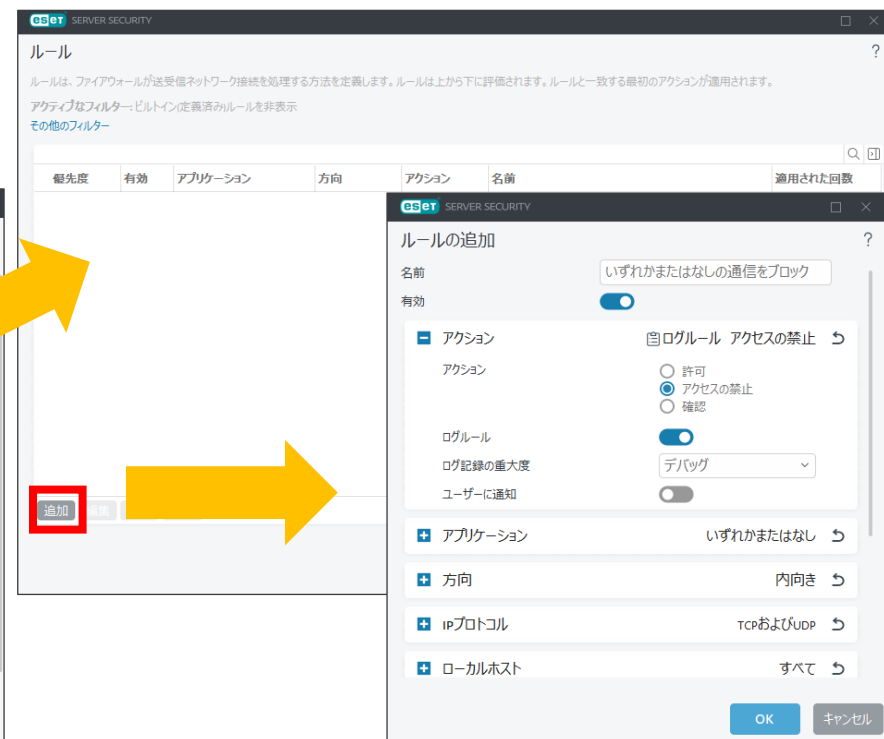
「サンプルの送信」
 ESET LiveGrid®に送信するサンプルファイルの種類を設定することが可能です。

※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://canon.jp/business/solution/it-sec/lineup/eset/feature/cloud-sandbox>

2-2-12. 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。
 ※ESSW V11.0より追加された機能です。

詳細設定(ネットワークアクセス保護画面)



「Windowsグループポリシーファイアウォールルールの評価」
 GPOを介して配布されるファイアウォールルールもESETのファイアウォールルールで使えます。
 ※EESW V12.0より追加された機能です。

2-2-11. 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などを検出することが可能です。



「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。

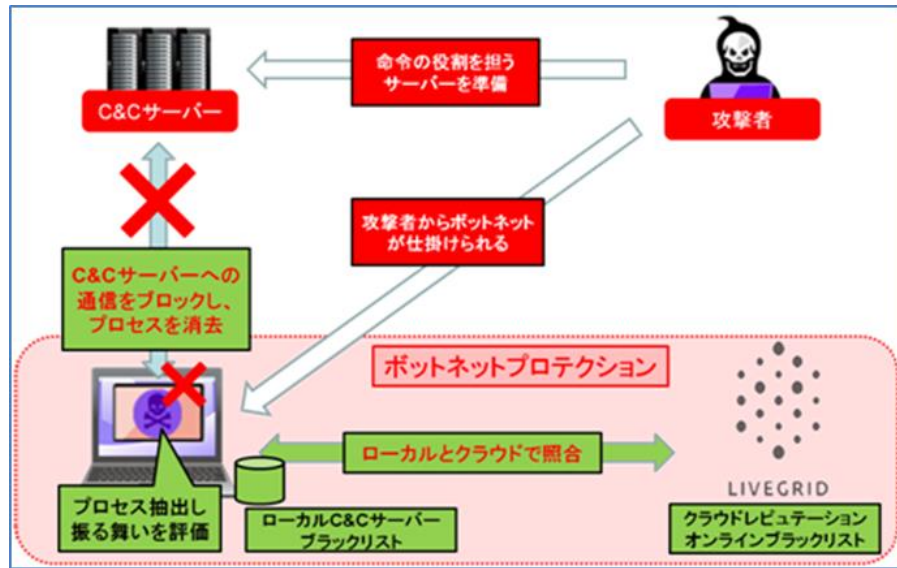
「侵入検出」
コンピュータに被害を与えるために使用されるおそれがある、さまざまなタイプの脅威の検出を有効または無効にできます。

ネットワークプロトコル(SMB・RPC・RDP)の既知の脆弱性(バルナラビリティ)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。

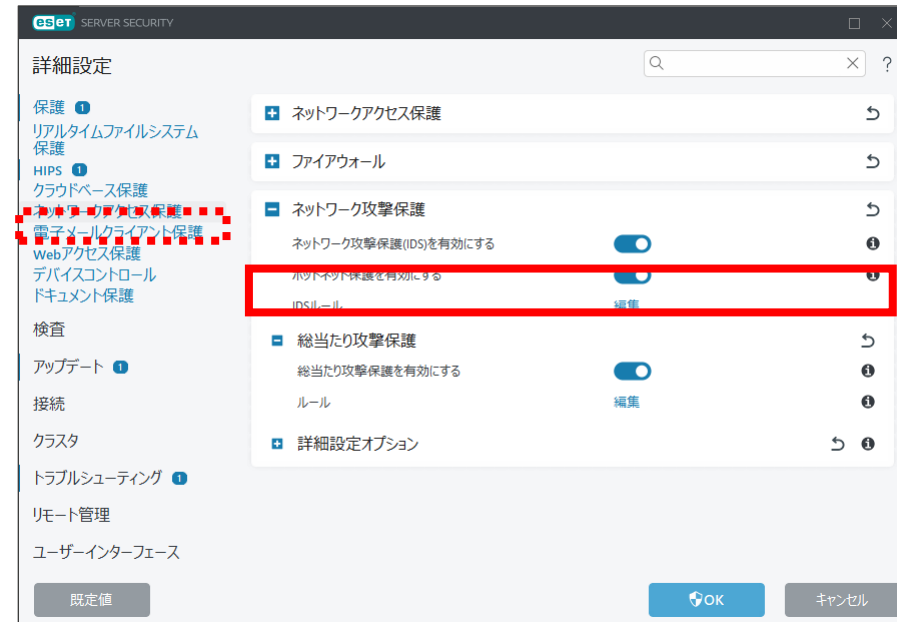
2-2-13. ボットネット保護

- 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。多重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



基本設定(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

2-2-14. 電子メールクライアント保護

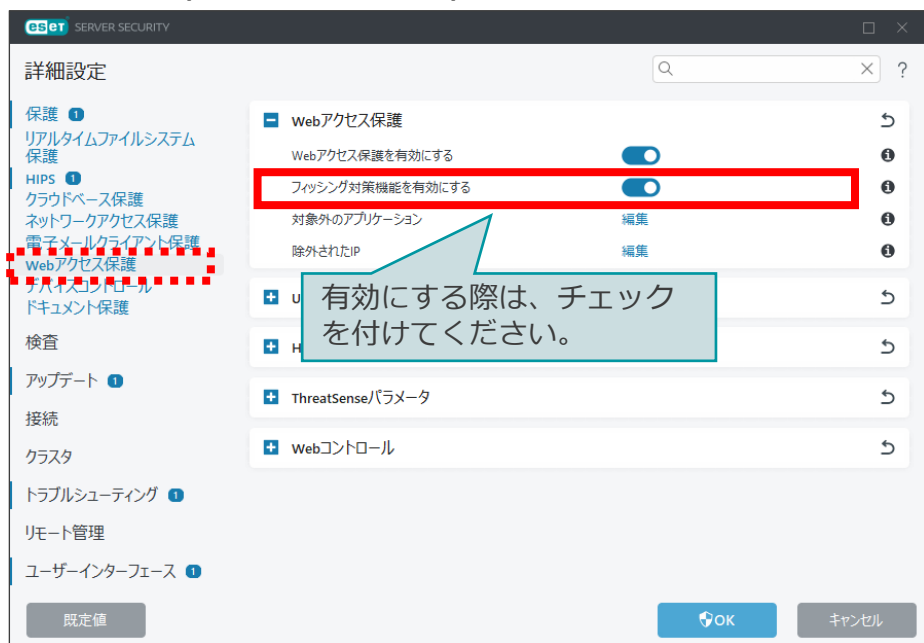
- プロトコルフィルタリングの機能により、使用しているインターネットブラウザやメールクライアントに関係なく、HTTP(S)、POP3(S)、IMAP(S)トラフィックの検査を行い、ウイルスを検出することが可能です。これによりWebブラウザやメールの添付ファイルに潜むウイルスを検知することが可能です。



2-2-15. 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制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)



潜在的なフィッシングの脅威検出画面



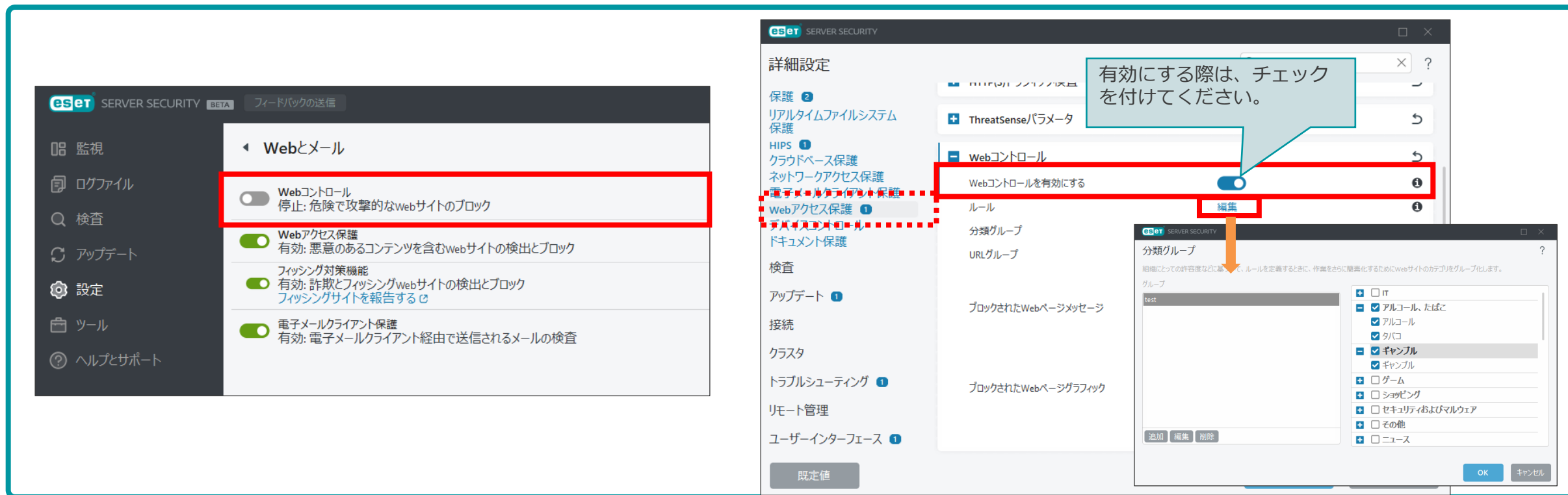
※フィッシング詐欺

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

2-2-16. Webコントロール

- Webコントロールを使うと、不快な内容を含むWebページをブロックできます。27のカテゴリと140以上のサブカテゴリへのアクセスを制限可能です。ブロックされたときのメッセージとグラフィックもカスタマイズできます。特定のWebページを除くすべてのページをブロックするには、URLリスト管理機能を使用します。

※ESSW V12.0より追加された機能です。



有効にする際は、チェックを付けてください。

Webコントロールを有効にする

編集

分類グループ

グループ

test

- IT
- アルコール、たばこ
- アルコール
- タバコ
- ギャンブル
- ギャンブル
- ゲーム
- ショッピング
- セキュリティおよびマルウェア
- その他
- ニュース

追加 編集 削除

OK キャンセル

2-2-17. 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	<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ストレージ	<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

ルールの追加

名前: 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

ユーザー一覧: 編集

ユーザーに通知:

OK

デバイスコントロール警告メッセージ画面

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。

アクセス制御

ブロック

このメッセージの詳細を見る

2-2-18. 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。



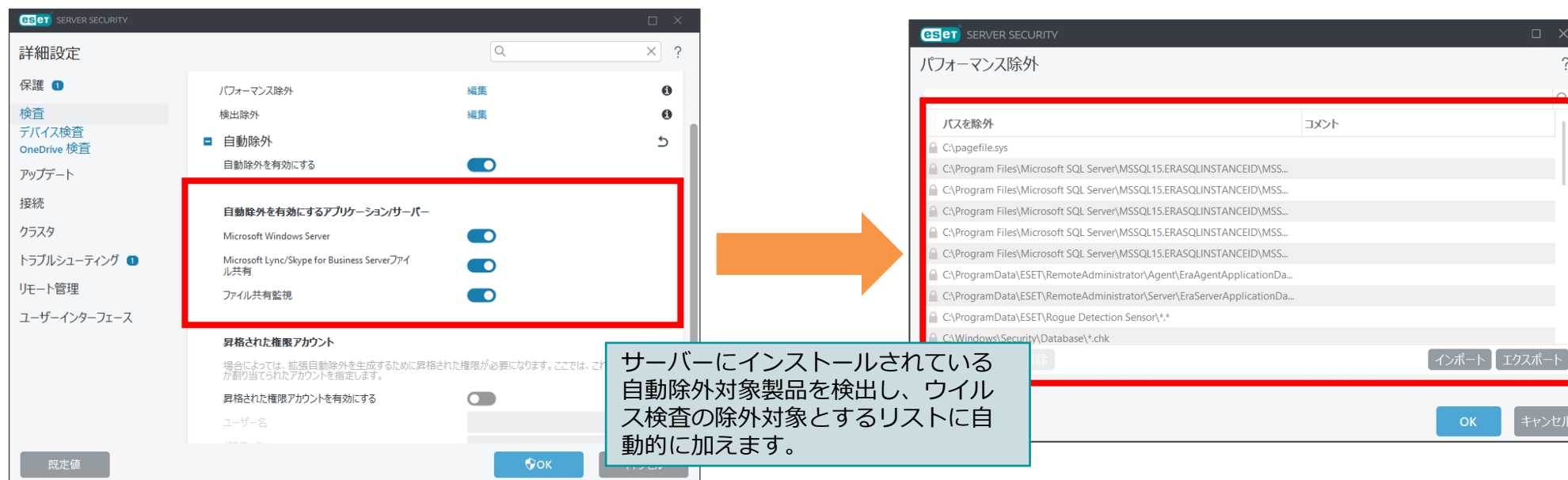
The image shows the ESET Server Security interface with the '除外' (Exclusions) section highlighted. Two options, 'パフォーマンス除外' (Performance Exclusion) and '検出除外' (Detection Exclusion), are highlighted with red boxes. Arrows point from these boxes to their respective configuration dialog boxes.

「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。

2-2-19. 自動除外

- 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。



The image shows two screenshots from the ESET Server Security console. The left screenshot shows the '詳細設定' (Detailed Settings) window with the '自動除外' (Automatic Exclusion) section highlighted in red. The right screenshot shows the 'パフォーマンス除外' (Performance Exclusion) window, also with a red box around the list of excluded paths. An orange arrow points from the left window to the right window. A text box at the bottom explains the process.

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。

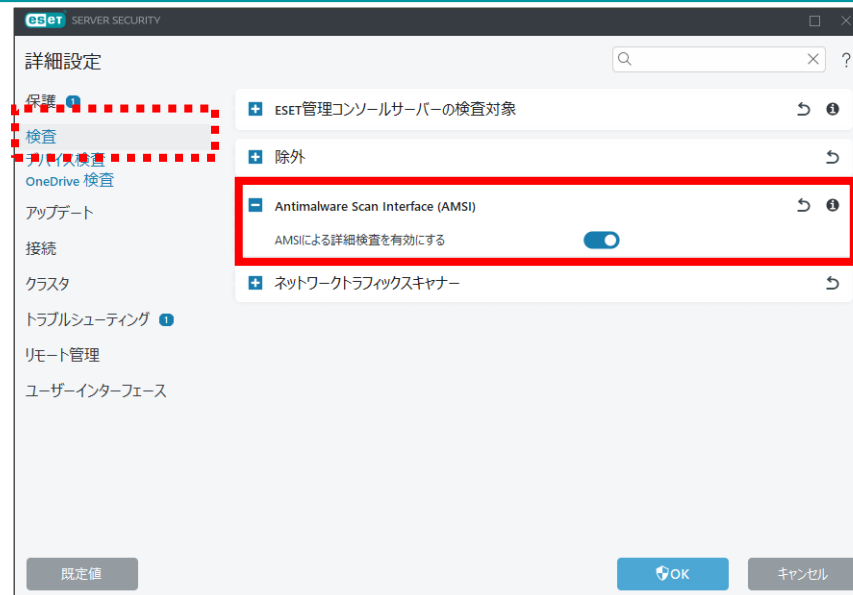
【自動除外対象製品】

- 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

2-2-20. 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Windows Server 2016 / 2019 / 2022 / 2025でのみ利用可能です。



※Antimalware Scan Interface(AMSI)
AMSIはWindows Server 2016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。

2-2-21. デバイス検査

- デバイス検査では、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。



「アイドル状態検査」

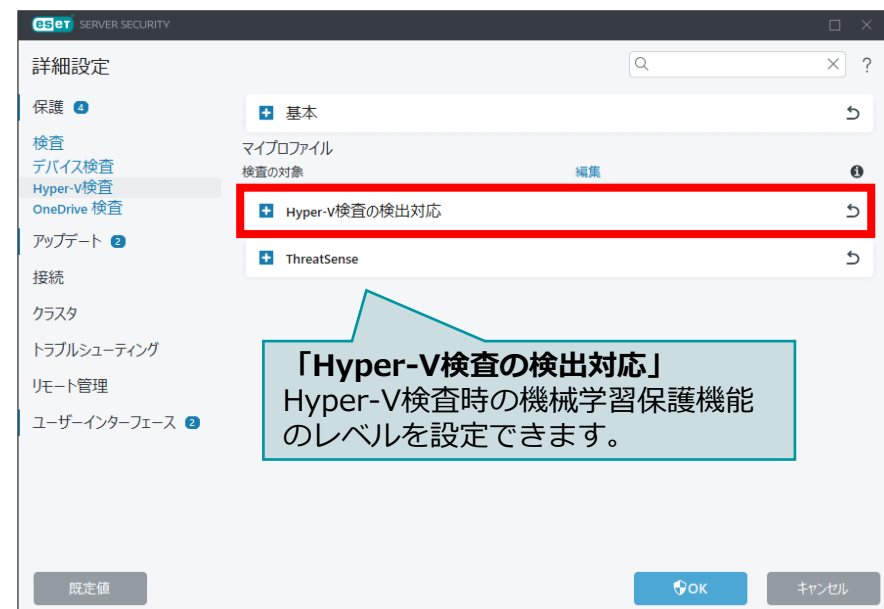
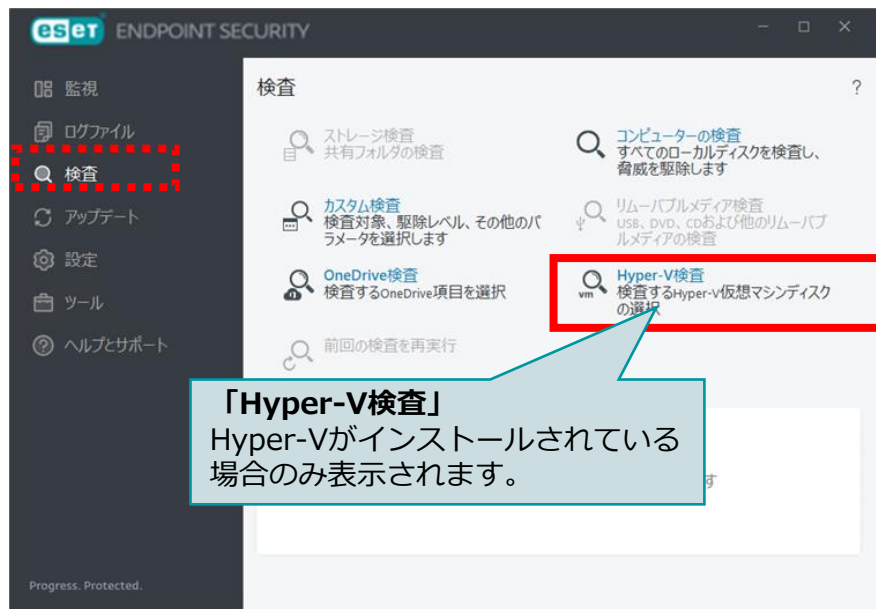
コンピューターのアイドル状態(スクリーンセーバーの起動時、コンピューターのロック、ユーザーのログオフ)の間を利用して、コンピューター全体の検査をサイレントに実行する機能です。

「オンデマンド検査の検出対応」

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。

2-2-22. Hyper-V検査

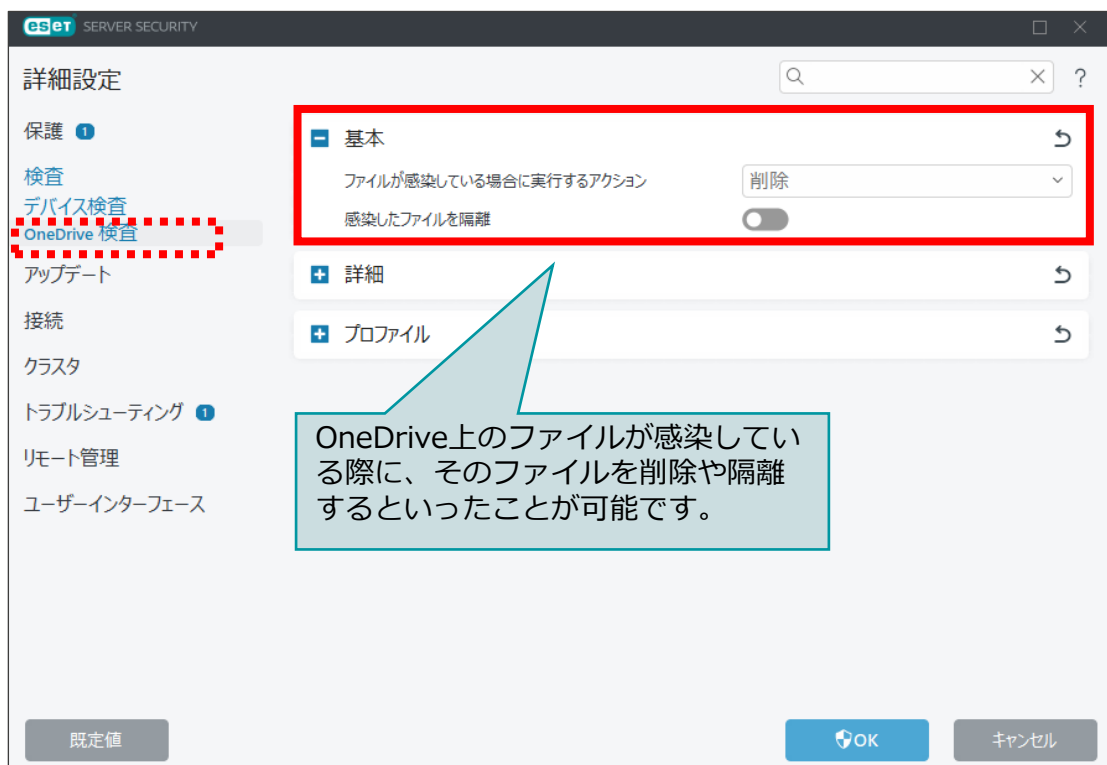
- Hyper-V検査により、Microsoft Hyper-V Server上の仮想マシンディスクを検査することができます。ただし、脅威を駆除できるのは仮想マシンが起動していない場合のみです。仮想マシンが起動している場合、仮想マシンのスナップショットが作成され、作成されたスナップショットに対し読み取り専用モードで検査が実行されるため駆除は行われません。



※Hyper-V検査がサポートされるOSは下記となります。
Windows Server 2012、Windows Server 2012R2、Windows Server 2016、Windows Server 2019、Windows Server 2022、Windows Server 2025

2-2-23. OneDrive検査

- 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。



2-2-24. 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。



「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。
デフォルト設定では有効になっています。
※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。
※旧バージョンのPCU設定値は引き継がれません。

「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。

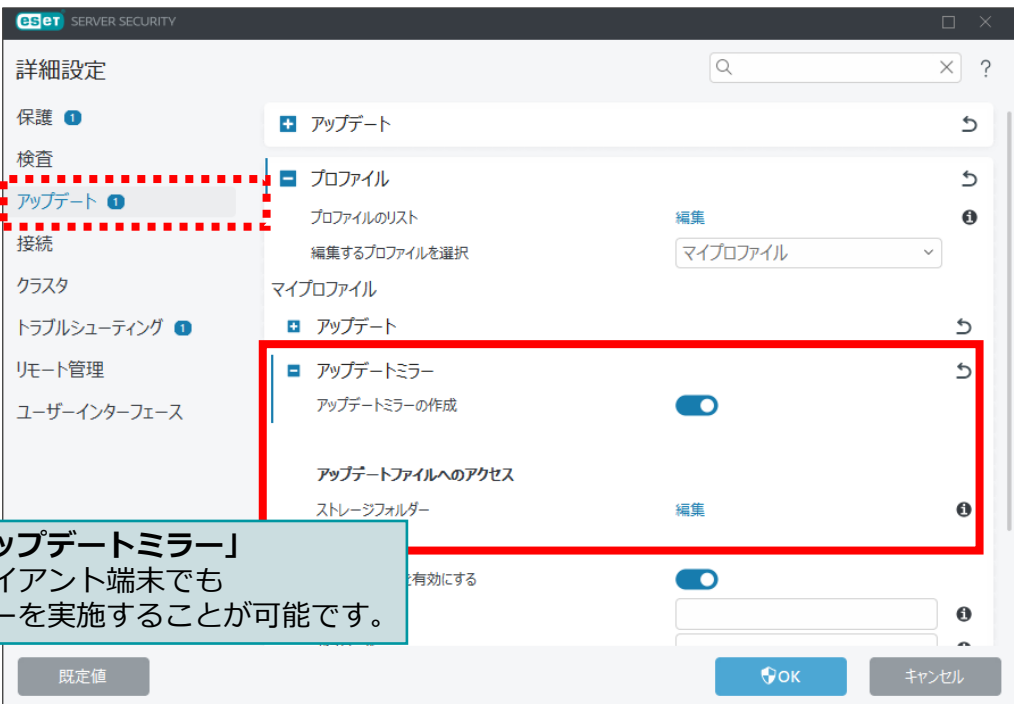
モジュールロールバック
モジュールのスナップショットを作成
ローカルに保存するスナップショットの数
前のモジュールにロールバック

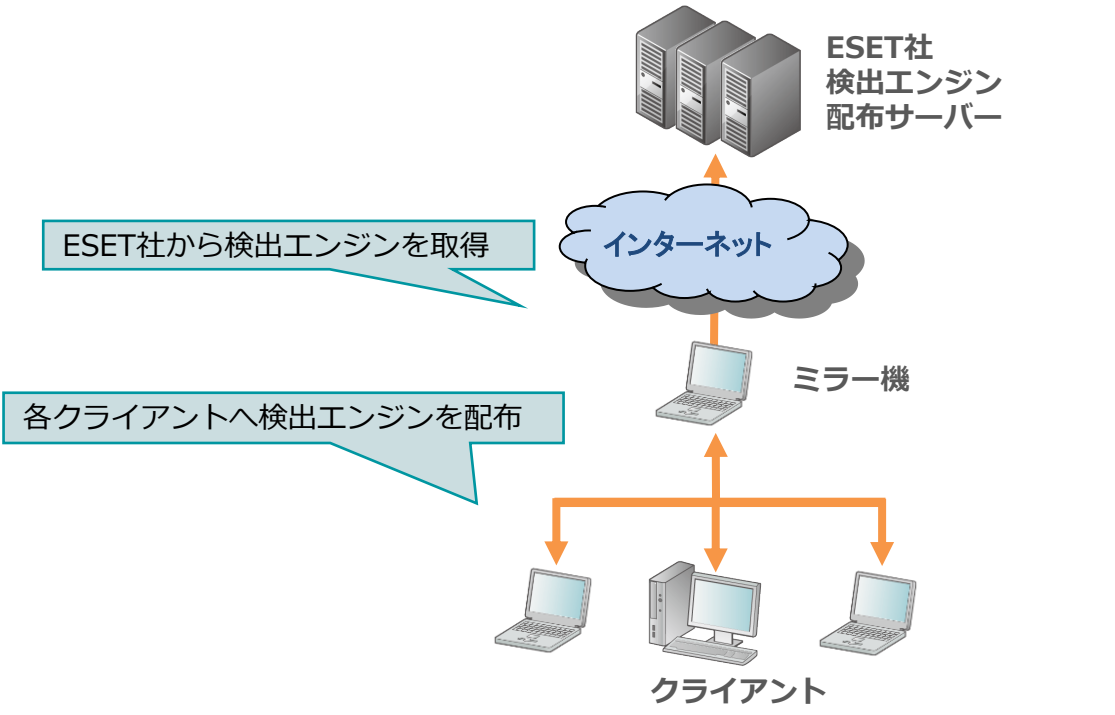
製品のアップデート
自動アップデート
アップデートが無効になっている場合でも、サポートされているバージョンへの1回限りの緊急アップデートが実行され、保護が維持されます。

2-2-25. 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かなくても、ミラー環境を構築することが可能です。





2-2-26. 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。

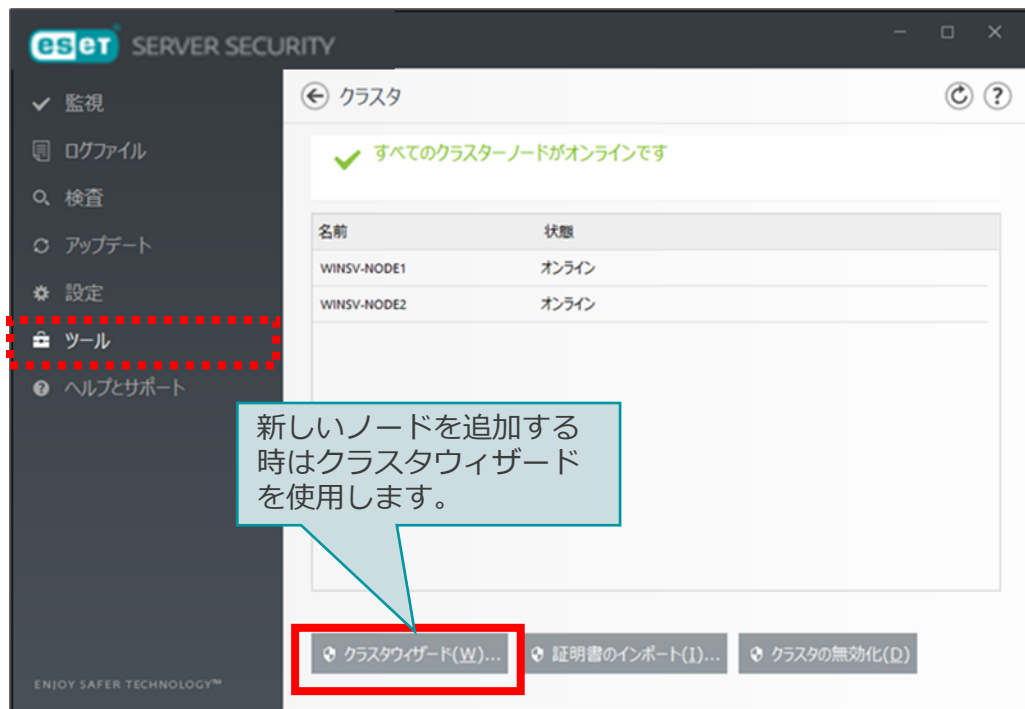


プロキシサーバを設定する際はチェックを付けてください。

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。

2-2-27. クラスタ

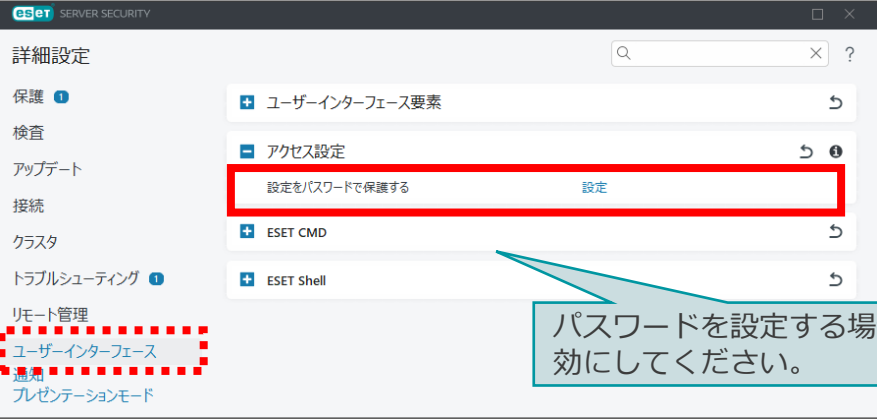
- クラスタを構築した場合、サーバー同士が通信を行い ESET Server Security for Microsoft Windows Server をインストールさせたり、設定情報などを同期させたりすることが可能です。クラスタを構築するためにはクラスタウィザードを使用します。クラスタウィザードを使用することで、新たなノードの追加やクラスタ名などを設定することが可能です。



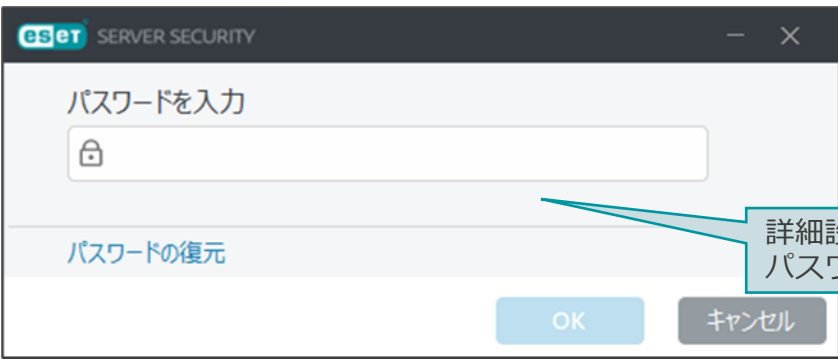
2-2-28. パスワード保護

- 設定をパスワードで保護することにより、ユーザーによる設定変更や、ESETのウイルス・スパイウェア対策プログラムのアンインストールを防止することが可能です。

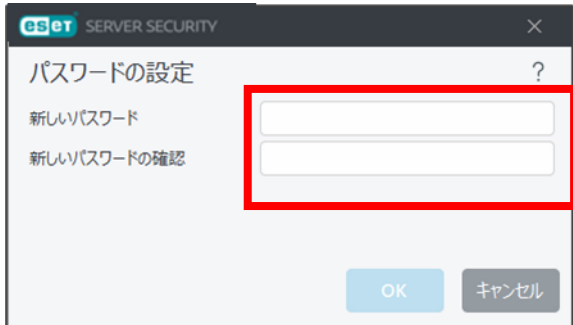
パスワード設定画面




パスワード入力画面(詳細設定を確認する場合)



パスワードの設定



パスワード入力画面(アンインストールする場合)



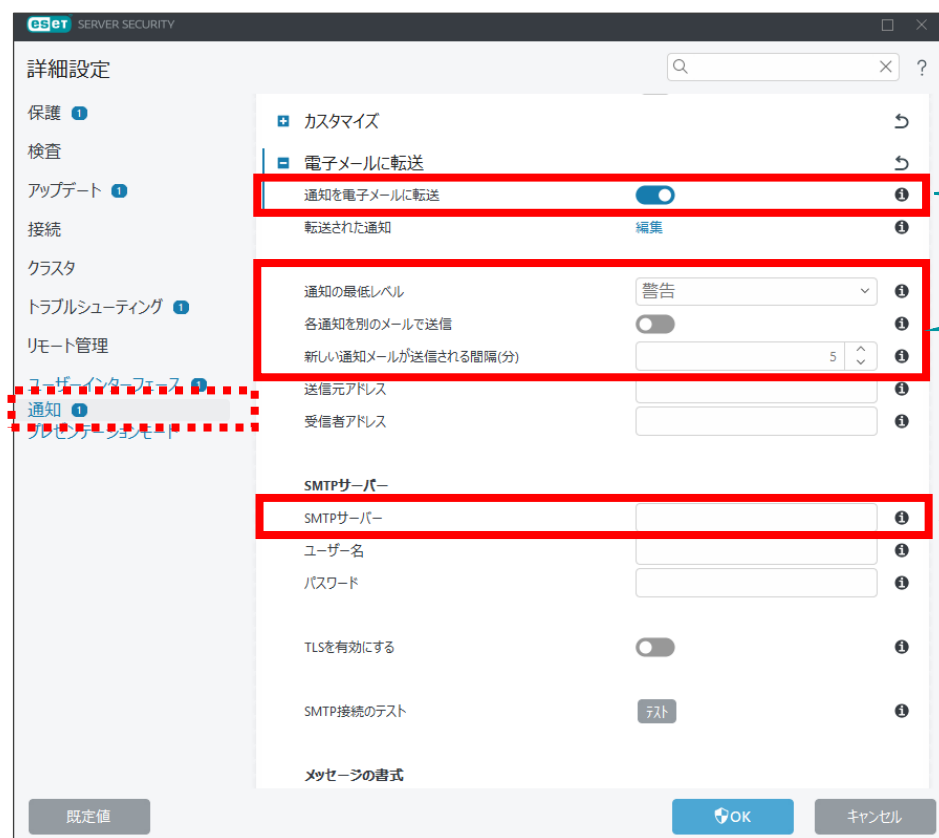
パスワードを設定する場合は有効にしてください。

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。



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。

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。

2-2-30. 脆弱性とパッチ管理

- 脆弱性とパッチ管理では、アプリケーションの脆弱性状況の検出状況を管理することができます。スケジュールにて任意のタイミングで実施させることができます。

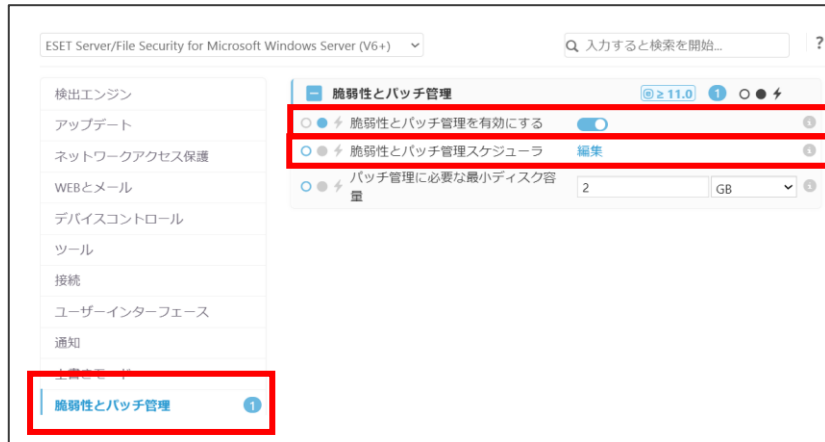
※クラウド型セキュリティ管理ツールESET PROTECTで管理している場合にのみご利用いただけます。

(オンプレミス型セキュリティ管理ツール ESET PROTECT on-premではご利用いただけません。)

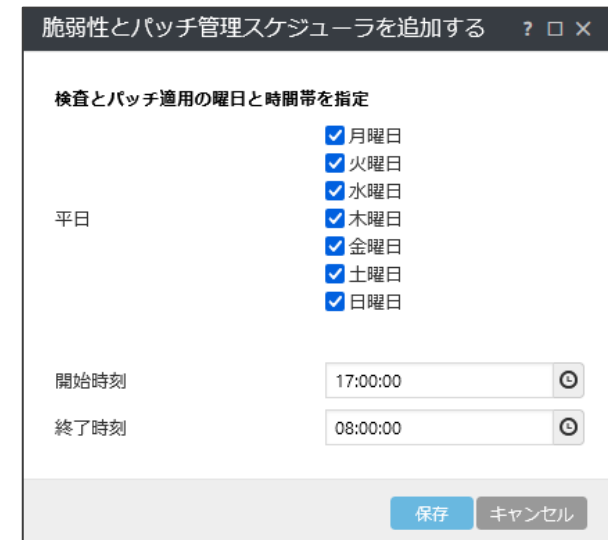
※「ESET PROTECT Elite」または「ESET PROTECT Complete」ライセンスの場合にのみご利用いただける機能です。

※パッチの自動適用は未サポートとなります。(2025年2月現在)

脆弱性とパッチ管理設定画面



スケジュール画面



※脆弱性とパッチ管理(ESET Vulnerability & Patch Management)の詳細は下記よりご確認ください。
https://eset-info.canon-its.jp/files/user/pdf/download/business/request/vapm_function.pdf

3. プログラム別の機能比較

3. プログラム別の機能比較 (1/2)

機能名	ESSW				
	V8.X	V9.X	V10.X	V11.X	V12.X
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	○	○	○	○	○
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спロイトブロッカー	○	○	○	○	○
ランサムウェア保護	○	○	○	○	○

機能名	ESSW				
	V8.X	V9.X	V10.X	V11.X	V12.X
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	○	○	○	○	○
Webコントロール機能	×	×	×	×	○
ネットワーク通信関連機能					
バルナラビリティシールド	○	○	○	○	○
ボットネット保護	○	○	○	○	○
ファイアウォール	×	×	×	○※1	○※1
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	○	○	○	○	○
製品の自動アップデート	○※2	○	○	○	○
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	○	○	○	○	○

※1 Essentialライセンスの場合、ご利用いただけません。
 ※2 V8ではPCU(プログラムコンポーネントアップデート)という名称です。

3. プログラム別の機能比較 (2/2)

機能名	ESSW				
	V8.X	V9.X	V10.X	V11.X	V12.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ルールの追加	○	○	○	○	○
タイムスロット	○	○	○	○	○
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	○	○	○	○	○