



ESET PROTECTソリューション
ESET Endpoint Security V6 /
ESET Endpoint アンチウイルス V6/
ESET File Security for Microsoft Windows Server V6
新機能紹介資料

第12版
作成：2021年7月1日



1. はじめに
 - (1)本資料について
 - (2)本プログラムの特徴（多層防御機能で新種の脅威を防御）
2. ESET Endpoint Security V6/ESET Endpoint アンチウイルス V6
 - (1)新機能および改善された機能について
 - ①ユーザーインターフェースの改善
 - ②保護技術・保護機能の追加および改善
 - ③その他機能の追加および改善
 - (2)バージョン別の機能比較について
3. ESET File Security for Microsoft Windows Server V6
 - (1)V5からの新機能および改善された機能について
 - ①ユーザーインターフェースの改善
 - ②保護技術・保護機能の追加および改善
 - ③その他機能の追加および改善
 - (2)バージョン別の機能比較について



本資料は「ESET PROTECTソリューション」で提供されている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新機能と改善された機能を紹介した資料です。

プログラム名	種別
ESET Endpoint Security V6（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 V6（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 File Security for Microsoft Windows Server V6 （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

- ・ 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セキュリティ管理ツール(ESET Security Management Center ※以降ESMC)で管理が可能です。ESET PROTECT Cloud（※以降EPC）、ESET PROTECT（※以降EP）での管理はできません。
- ・ 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。



本プログラムより新たな防御機能が実装され『多層防御』により新種の脅威からクライアントおよびサーバーを防御する機能が向上いたしました。

各防御機能の紹介およびプログラムの実装状況は以降のページをご参照ください。

ESET PROTECTソリューションでの防御の流れ

「標的型攻撃」「脆弱性攻撃」など、高度化、巧妙化が進むサイバー攻撃に対抗する機能は、ヒューリスティックだけではありません。ファイルやプログラムがエンドポイントに侵入、動作するタイミングで、各種プロアクティブ検出機能がデータの中身や振る舞いをチェックし、悪意のあるプログラムによる被害を未然に防ぎます。また、ボットなどによる外部との通信を検出、防御する「出口対策機能」も搭載しています。

#1
ダウンロード開始:



NEW

「バルナラビリティシールド」
ネットワーク通信を検査して
脆弱性への攻撃をブロック

#2
コンテンツ処理:



NEW

「エクスプロイトブロッカー」
ダウンロード処理の不整合を
チェックして脆弱性への攻撃を
ブロック

#3
ファイルアクセス/実行:



「アドバンスド
ヒューリスティック」
DNA検査を実施

#4
ファイル実行中:



NEW

「アドバンスド
メモリスキャナー」
メモリー上で不審な実行
コードを検出

マルウェアによる通信:



NEW

「ボットネット
プロテクション」
マルウェアのC&Cサーバー
との通信を検出



ESET Endpoint Security V6/ ESET Endpoint アンチウイルス V6

(1)新機能および改善された機能について

2 新機能および改善された機能について



ESET Endpoint Security V6/ ESET Endpoint アンチウイルス V6プログラムの新機能および改善された機能の一覧は以下のとおりです。

①ユーザーインターフェースの改善

デザインの変更	ユーザーインターフェースの起動モード	NEW
---------	--------------------	-----

②保護技術・保護機能の追加および改善

アドバンスドメモリスキャナー	NEW	エクスプロイトブロック	NEW	バルナラビリティ シールド (EESのみ)	NEW
ボットネット保護 (EESのみ)	NEW	アイドル状態検査	NEW	共有ローカルキャッシュ	NEW
フィッシング対策		アンチステルス技術		リムーバブルメディア検査	
IDSの除外設定				—	

③その他機能の追加および改善

デバイスコントロール グループ ルールの追加	電子メール通知間隔の選択	Webコントロールブロック メッセージの変更
古い検出エンジン（ウイルス定義データ ベース）アラート	ESET SysRescue Live	ESET Log Collector NEW
ESET特殊駆除ツール NEW	ESET CMD NEW	—

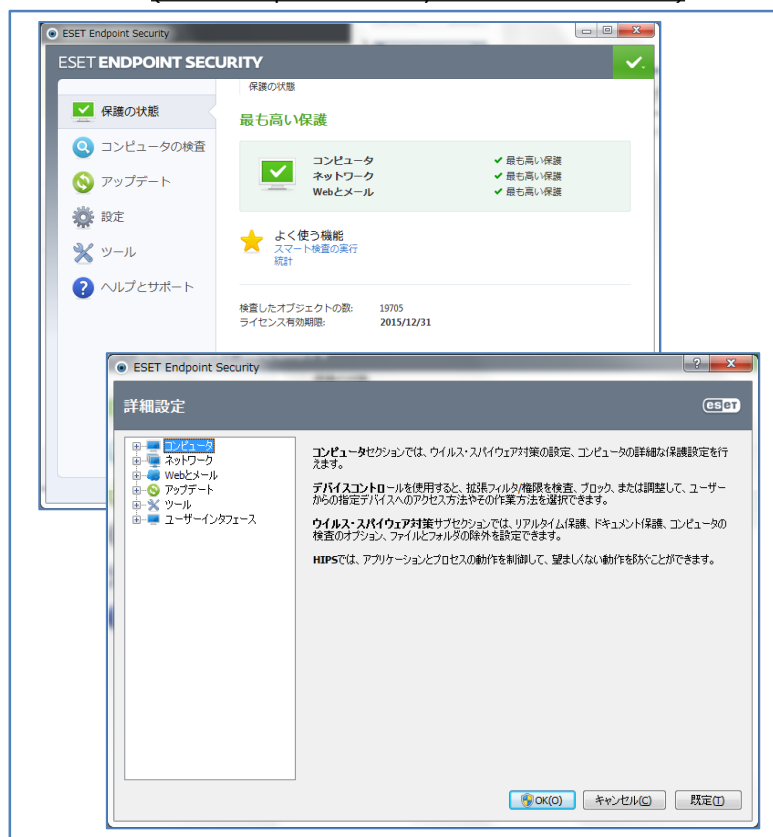


①ユーザーインターフェースの 改善

2 デザインの変更

ユーザーインターフェースが新しいデザインに変更され、より高い可視性とより直感的な操作が可能となりました。

旧バージョン
(ESET Endpoint Security V5.0 プログラム画面)



新バージョン
(ESET Endpoint Security V6 プログラム画面)



2 ユーザーインターフェースの起動モード



ユーザーインターフェースの起動モードを選択することが可能となりました。
クライアントの用途や運用に合わせてユーザーインターフェースの表示を調整することができます。

詳細設定(ユーザーインターフェース画面)

起動モード

完全
完全
最低
手動
サイレント

起動モードを選択できます。
※既定値は「完全」が設定されます。

モード	動作
完全	基本画面、通知、アラートを含むすべてのGUIが表示されます。
最低	通知のみが表示されます。(管理者のみ基本画面を表示可)
手動	GUIは起動せず、通知やアラートは表示されません。
サイレント	GUIは起動せず、通知やアラートは表示されません。(管理者のみGUIを起動可)



②保護技術・保護機能の 追加および改善

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となりました。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)

詳細設定

ウイルス対策

リアルタイムファイルシステム保護

コンピューターの検査

アイドル状態検査

スタートアップ検査

リムーバブルメディア

ドキュメント保護

HIPS ⓘ

基本

HIPSを有効にする



自己防衛を有効にする



保護されたサービスを有効にする



アドバンスドメモリスキャナーを有効にする



エクスプロイトブロックを有効にする



有効にする際には、
チェックを付けてください。
※既定値は有効に設定されます。

※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

※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

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となりました。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に対して検知性能が向上しました。

詳細設定 (HIPS画面)

詳細設定

ウイルス対策

リアルタイムファイルシステム保護

コンピューターの検査

アイドル状態検査

スタートアップ検査

リムーバブルメディア

ドキュメント保護

HIPS

基本

HIPSを有効にする	☒
自己防衛を有効にする	☒
保護されたサービスを有効にする	☒
アドバンスドメモリスキャナーを有効にする	☒
エクスプロイトブロックを有効にする	☒

有効にする際には、チェックを付けてください。
※既定値は有効に設定されます。

※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 (バグ/脆弱性)

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

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となりました。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検出力が向上しました。

※ 本機能はESET Endpoint アンチウイルス V6 には搭載されていません。

詳細設定(IDSと詳細オプション画面)

ツール ①

ユーザーインターフェース

ゾーン

編集

IDSの例外

編集

■ IDSと詳細オプション

▣ 許可するサービス

▣ SMB経由の受信RPC通信

▣ 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

☒

有効にする際には、
チェックを付けてください。
※既定値は有効に設定されます。

※バルナラビリティ（脆弱性）

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

2 ボットネット保護

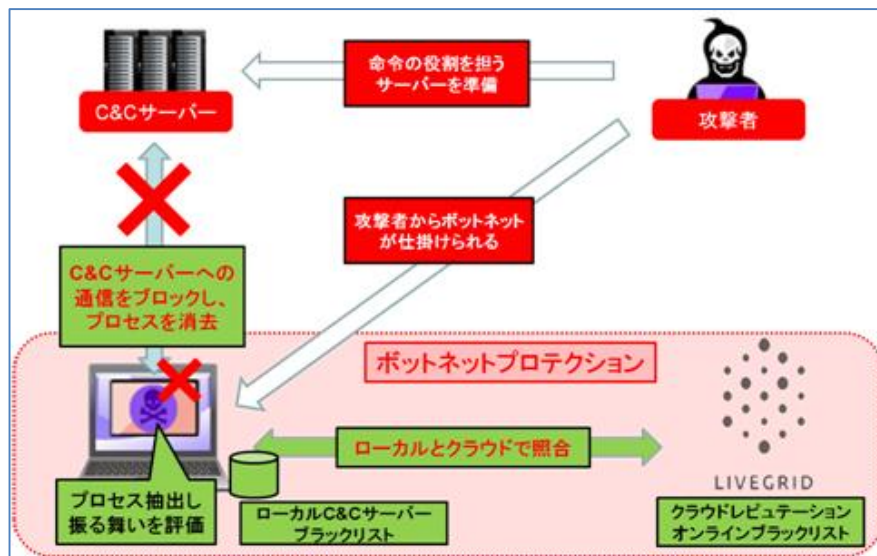
ENDPOINT ANTIVIRUS

NEW

パーソナルファイアウォール機能を利用して通信を解析し、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。これまでのフィルタリング機能に加え、多重防御を行い、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。

※ 本機能はESET Endpoint アンチウイルス V6 には搭載されておりません。

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）」になっ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。

※ボットネットとは何か？ どうやって防ぐのか？

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

コンピュータのアイドル状態(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、コンピュータ全体の検査をサイレントに実行する機能が追加されました。これにより、ユーザーはコンピュータの検査を意識することなく、コンピュータを利用することが可能です。

詳細設定(アイドル状態検査画面)

詳細設定

ウイルス対策

リアルタイムファイルシステム保護

コンピュータの検査

アイドル状態検査 ①

スタートアップ検査

リムーバブルメディア

ドキュメント保護

HIPS ①

アップデート

ファイアウォール ②

WEBとメール

基本

アイドル状態検査を有効にする



コンピュータがバッテリー電源で動作している場合にも実行する



ログを有効にする



アイドル状態検知

ディスプレイの電源を切るもしくはスクリーンセーバー



コンピュータのロック



ユーザーのログオフ



有効にする際には、
チェックを付けてください。
※既定値は無効に設定されます。

どのアイドル状態を利用して
検査を行うか選択してください。

仮想環境において、検査結果を共有する機能が追加されました。これにより重複した検査がなくなり、検査速度や仮想環境のパフォーマンスが向上します。本機能を使用する場合、各クライアントで検査した情報をキャッシュし共有するための、共有ローカルキャッシュサーバー(Linux OSで稼動)を用意する必要があります。

詳細設定(ウイルス対策画面)

詳細設定

ウイルス対策 ①

リアルタイムファイルシステム保護

コンピューターの検査

アイドル状態検査 ①

スタートアップ検査

リムーバブルメディア

ドキュメント保護

HIPS ①

アップデート

ファイアウォール ②

+ 基本

- 共有ローカルキャッシュ

共有ローカルキャッシュを有効にする



キャッシュサーバー

ホスト名



ポート



パスワード



有効にする際にはチェックを付けてください。また、キャッシュサーバーの指定を行ってください。
※既定値は無効に設定されます。

2

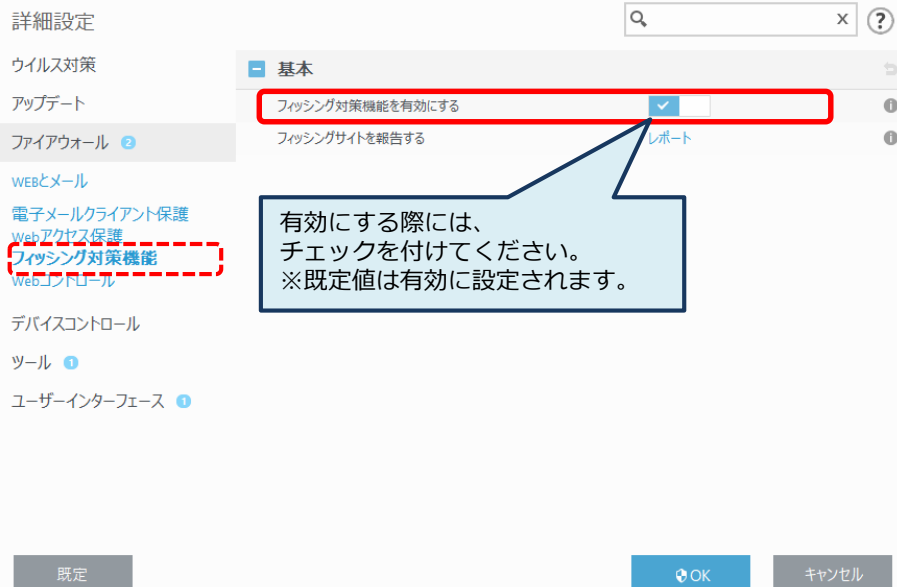
フィッシング対策

ENDPOINT ANTIVIRUS

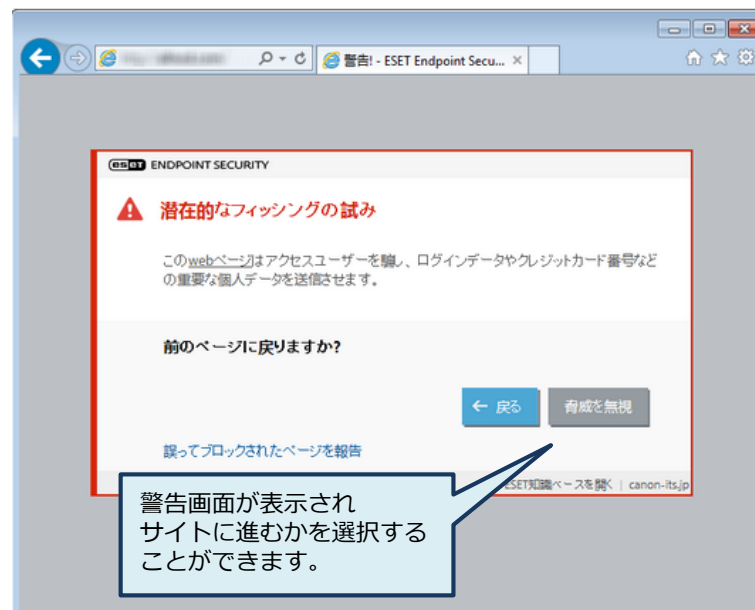


Webアクセス保護に統合されていたフィッシング対策機能が新機能として独立しました。フィッシングページへアクセスするとアクセスを抑止するダイアログが表示されます。また、フィッシングページと思われるURLを開発元ESET社へ報告することも可能となりました。

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

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



アンチステルス技術が改善され、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の検出性能が向上しました。

詳細設定(フィッシング対策画面)

詳細設定

ウイルス対策 ①

リアルタイムファイルシステム保護
コンピューターの検査
アイドル状態検査 ①
スタートアップ検査
リムーバブルメディア
ドキュメント保護
HIPS ①

アップデート

ファイアウォール ②

WEBとメール

基本

スキャナオプション

望ましくない可能性のあるアプリケーションの検出を有効にする ☐ x

安全でない可能性のあるアプリケーションの検出を有効にする ☐ x

疑わしい可能性のあるアプリケーションの検出を有効にする ☒

アンチステルス

アンチステルス技術を有効にする ☒

除外フィルタ

有効にする際には、
チェックを付けてください。
※既定値は有効に設定されます。

※アンチステルス技術

ルートキットなどの自己の存在を隠蔽し、通常のスキャンでは感知 できない悪質な不正プログラムも検出可能にする技術を意味します。

※ルートキット

自己の存在を隠しながら、インターネットからの攻撃者が、システムに無制限にアクセスできるようにする悪意のあるプログラムです。ルートキットは、システムにアクセス(通常はシステムの脆弱性を悪用します)した後、オペレーティングシステムの様々な機能を使用して、ウイルス対策ソフトウェアによる検出を免れようとしています。



コンピュータの検査について従来の「スマート検査」と「カスタム検査」のほか「リムーバブルメディア検査」が新たに追加されました。

「リムーバブルメディア検査」では、現在コンピュータに接続されているリムーバブルメディア(CD/DVD/USBなど)の検査をすばやく開始します。

メインメニュー(コンピュータの検査画面)





パーソナルファイアウォールのIDSの機能にて、例外設定が強化されました。
リモートIPアドレスの例外の追加以外にもアプリケーション単位で例外設定をすることが可能になりました。

※ 本機能はESET Endpoint Securityでご使用いただけます。

詳細設定(パーソナルファイアウォール画面)



詳細設定(IDS例外の追加画面)





③その他機能の追加 および改善

2 デバイスコントロール グループルールの追加

デバイスコントロール機能にて、接続されているデバイスを検出することが、可能となりました。また、複数のデバイスをデバイスグループとしてまとめることが可能となりました。これにより、デバイスコントロールルールの作成が行いやすくなりました。

詳細設定(デバイスコントロール画面)

詳細設定

ウイルス対策

アップデート

ファイアウォール

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

基本

システムに統合

ルールの設定

デバイスグループ

この変更を有効にするには、コンピュータの再起動が必要です。

編集

編集

有効にする際には、チェックを付けてください。
※既定値は無効に設定されます。

既定 OK キャンセル

デバイスグループ

グループ1	ベンダー	モデル	シリアル
	任意のベンダー	RUF2-HSCLT	070007B71C08879E6712
	任意のベンダー	IR5_CENA_X64FRE_VA-JP_DV9	12C1283F

複数のデバイスをグループとしてまとめることが可能になりました。

検出されたデバイス

デバイスタイプ	ベンダー	モデル	シリアル
LPT/COMポート	(標準ポート)	プリンター ポート	
LPT/COMポート	(標準ポート)	通信ポート	
LPT/COMポート	(標準ポート)	通信ポート	
CD/DVD		IR5_CENA_X64FRE_VA-JP_DV9	12C1283F
ディスクストレージ		RUF2-HSCLT	070007B71C08879E6712
ディスクストレージ		RUF2-HSCLT	070007B71C08879E6712

クライアントに接続されたデバイスを検出することができるようになり、ルールの作成が行いやすくなりました。

2

電子メール通知間隔の選択



電子メール通知機能にてイベント発生後やウイルス検出後に電子メールで通知を行うまでの期間を選択することができるようになりました。

これにより即座に管理者へ電子メール通知を行うことが可能となります。

詳細設定(電子メール通知画面)

2 Webコントロールブロックメッセージの変更

Webコントロール機能にてWebサイトへのアクセスをブロックした場合に表示させるメッセージをカスタマイズ可能になりました。

また、表示される画像についてもWebアドレスやネットワークパスを指定することで、任意の画像を表示させることも可能になりました。

詳細設定(Webコントロール画面)

詳細設定

ウイルス対策

アップデート

ファイアウォール 2

WEBとメール

電子メールクライアント保護

Webアクセス保護

フィッシング対策機能

Webコントロール 1

デバイスコントロール

ツール 1

ユーザーインターフェース

既定

OK

キャンセル

基本

システムに統合 ☒

ルール 編集

分類グループ 編集

URLグループ 編集

ブロックされたWebページメッセージ

ブロックされたWebページグラフィック

メッセージおよび表示させる画像の指定が可能です。

Webコントロールメッセージ画面

ENDPOINT SECURITY

Webサイトがブロックされました

このWebページは、不適切または有害なコンテンツであると見なされるため、ブロックされました。詳細については、管理者に連絡してください。

戻る

このメッセージの詳細を見る

2

古い検出エンジンアラート

検出エンジンが古い場合にアラートを表示します。※
任意の日数を設定することができるようになり、社内のポリシーにあわせてアラートを表示させることが可能です。

※検出エンジン=ウイルス定義データベースのこと

詳細設定(アップデート画面)

詳細設定

ウイルス対策

アップデート

ファイアウォール 2

WEBとメール

デバイスコントロール

ツール 1

ユーザーインターフェース 1

一般

アップデートプロファイル マイプロファイル

アップデートキャッシュを削除 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。

隔離フォルダのオブジェクトを削除する前に確認する ☒

検出エンジン最大経過時間(日数) 7

ロールバック

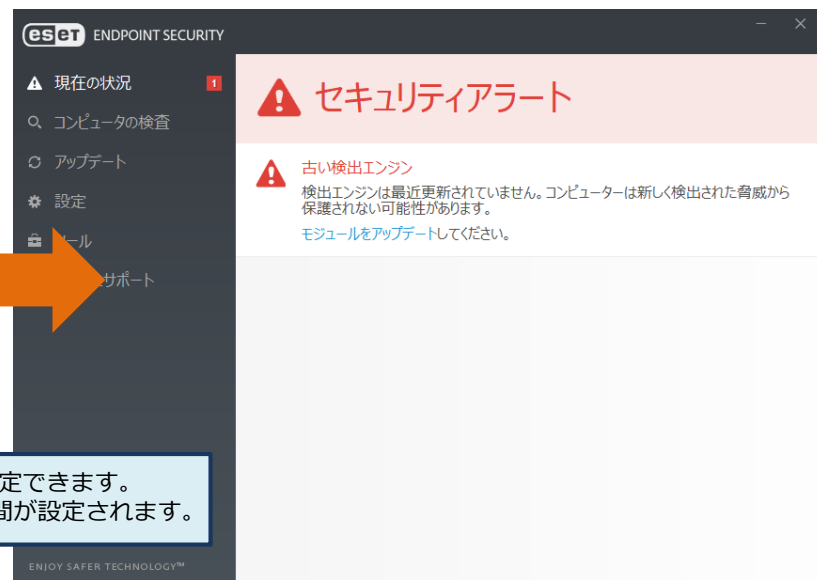
モジュールのスナップショットを作成 ☒

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

プロファイル

既定 OK キャンセル

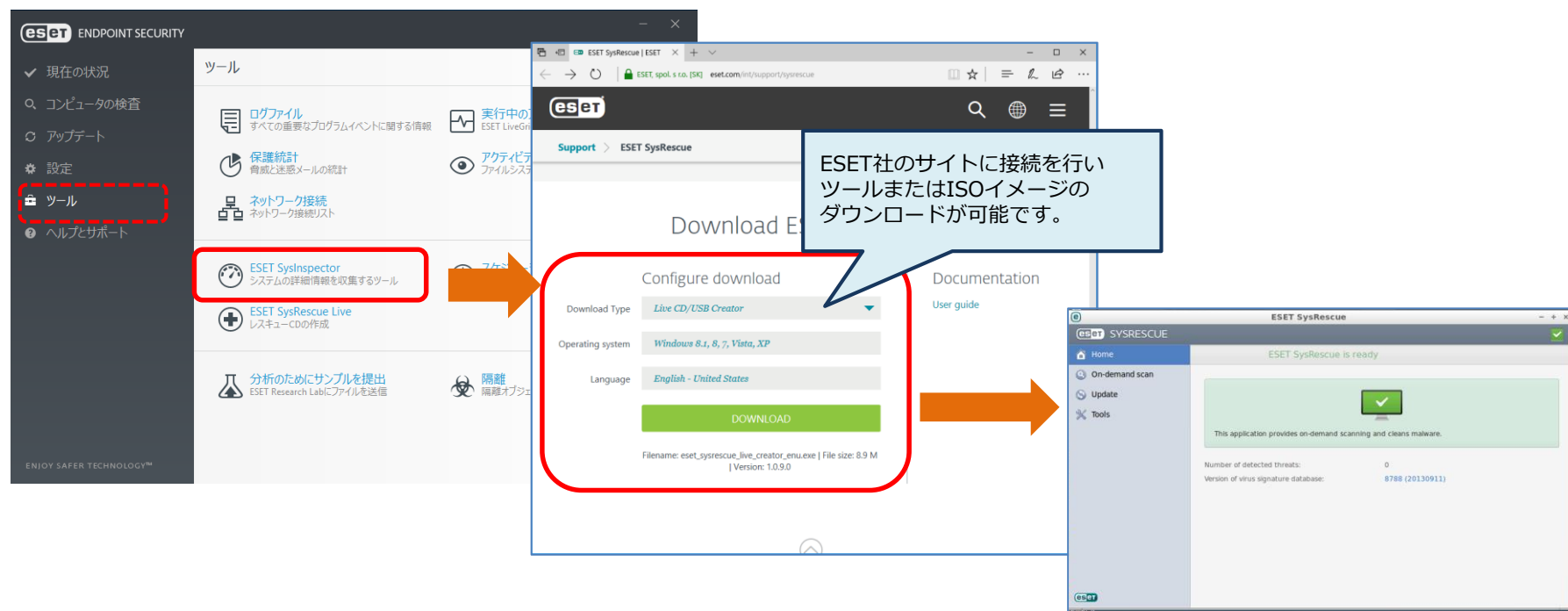


任意の日にちを指定できます。
※既定値では7日間が設定されます。



ESET SysRescue（レスキューCD）の作成方法が刷新され、従来と比べ使いやすくなりました。ESET SysRescue Liveのリンクをクリックすると、専用WebページよりESET SysRescueの作成ツールやESET SysRescueのディスクイメージをダウンロードすることが可能になりました。

ESET SysRescue Live利用の流れ



システム情報やログ情報を収集するツールが新たに追加されました。これにより問題解決するための各種情報を速やかに取得することが可能です。

※本ツールはサポートセンターよりお客様へご案内があった場合にのみご利用ください。

ESET Log Collectorご利用までの流れ

The image shows the ESET Log Collector download process in two parts. On the left, the ESET Endpoint Security application window is displayed. In the left-hand menu, the 'ヘルプとサポート' (Help and Support) option is highlighted with a red dashed box. In the main content area, under the 'サポートツール' (Support Tools) section, the 'ESET Log Collector' link is highlighted with a red rectangle. An orange arrow points from this link to the right. On the right, a web browser window shows the ESET website. The 'DOWNLOAD ESET LOG COLLECTOR' button is highlighted with a red rectangle. A blue speech bubble points to this button with the text: 'ESET社のサイトに接続を行いツールのダウンロードが可能です。' (You can connect to the ESET website and download the tool.)

複数のマルウェアを駆除するツールが新たに追加されました。これによりESETの標準機能では駆除ができないウイルスに対応することが可能です。

※本ツールはサポートセンターよりお客様へご案内があった場合にのみご利用ください。

ESET特殊駆除ツールご利用までの流れ



コマンドラインを利用して設定ファイルをインポートおよびエクスポートできるようになりました。コマンドラインを利用した手動実行や自動化用のスクリプトの作成をすることができます。ECMDコマンドを使用する際には管理者権限で実行するか、管理者として実行を使用してコマンドプロンプトを開く必要があります。

※高度なECMDコマンドはローカルのみで実行できます。ERAを使用したクライアントタスクのコマンド実行では動作しません。

詳細設定(ツール画面)

詳細設定

ウイルス対策

アップデート ①

ファイアウォール ②

WEBとメール

デバイスコントロール

ツール ②

ログファイル

プロキシサーバ

電子メール通知 ②

プレゼンテーションモード

ESET LIVEGRID®

MICROSOFT WINDOWS® アップデート

MICROSOFT NAP

ESET CMD

高度なECMDコマンドを有効にする ☒

認証方法 詳細設定パスワード

パスワード保護の使用が推奨されます。インポートする設定ファイルについて [ユーザーインターフェース] > [アクセス設定] で設定したパスワードと一致するか確認します。インポートするファイルをツールを用いて署名する必要があります。

パスワード認証を使用するには、詳細設定でパスワードを設定する必要があります(ユーザーインターフェース > アクセス設定)。

※本機能はESET Endpoint Security V6.5、ESET Endpoint アンチウイルス V6.5よりご利用いただけます。



ESET Endpoint Security V6/ ESET Endpoint アンチウイルス V6

(2)バージョン別の機能比較について



ウイルス・スパイウェア対策機能		
機能名	V5	V6
オンデマンド検査	○	○
リアルタイム保護	○	○
ドキュメント保護	○	○
Webアクセス保護	○	○
電子メール保護	○	○
暗号化通信の検査 (HTTPS・POP3Sの検査)	○	○
ESET Live Grid (ThreatSense.Net)	○	○
ホスト侵入防止システム (HIPS)	○	○
自己防衛機能	○	○
アイドル状態検査	×	○
アドバンスドメモリースキャナー	×	○
エクスプロイトブロック	×	○

- ※1: ESET Endpoint Securityのみ搭載
 ※2: ESET Endpoint Security V6に搭載
 ※3: ESET Endpoint アンチウイルスのみ搭載

ネットワーク通信関連機能		
機能名	V5	V6
パーソナルファイアウォール	○※1	○※1
迷惑メール対策	○※1	○※1
Webコントロール	○※1	○※1
ネットワーク接続表示	○	○
バルナラビリティシールド	×	○※2
ボットネット保護	×	○※2
アップデート・ミラーサーバー機能		
定義データベースのアップデート	○	○
定義データベースの 遅延アップデート	○	○
オフライン更新機能	○	○
定義データベースのロールバック	○	○
ミラーサーバー機能	○※3	○
ミラーサーバーのSSL対応	○※3	○
ミラーサーバー機能の差分更新 (ナノアップデート)	○※3	○

【略称について】

- V5 : ESET Endpoint Security V5 / ESET Endpoint アンチウイルス V5
 V6 : ESET Endpoint Security V6 / ESET Endpoint アンチウイルス V6



その他の機能 (1)		
機能名	V5	V6
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	×	○
リムーバブルメディアの 自動検査	○	○
Windows更新プログラムの 適用通知	○	○
プレゼンテーションモード	○	○
ユーザーインターフェースの 起動モード選択	×	○
統計表示	○	○
アクティビティの表示	○	○
実行中のプロセス表示	○	○
共有ローカルキャッシュ	×	○

その他の機能 (2)		
機能名	V5	V6
設定のインポート・エクスポート	○	○
ESET CMD	×	○※3
ESET SysInspector機能	○	○
ESET SysRescue機能	○	○
モジュールを指定したインストール	○※1	○※1
サーバーOSへのインストール	×	×
ESET Remote Administrator V5.3による管理	○	×
ESET Remote Administrator V6による管理	○※2	○※2

※1: ESET Endpoint Securityのみ搭載

※2: ESET Remote Administratorでクライアントを管理するには、各クライアントにERAエージェントの導入が必要

※3: ESET Endpoint Security V6.5、ESET Endpoint アンチウイルス V6.5 からの搭載

※ ESET Remote Administratorはサポートを終了いたしました。

【略称について】

V5 : ESET Endpoint Security V5 / ESET Endpoint アンチウイルス V5

V6 : ESET Endpoint Security V6 / ESET Endpoint アンチウイルス V6



3. ESET File Security for Microsoft Windows Server V6

(1)新機能および改善された機能について

3 新機能および改善された機能について



ESET File Security for Microsoft Windows Server V6プログラムの新機能および改善された機能の一覧は以下のとおりです。

(1) ユーザーインターフェースの改善

デザインの変更	ユーザーインターフェースの起動モード	NEW
---------	--------------------	-----

(2) 保護技術・保護機能の追加および改善

アドバンスドメモリスキャナー	NEW	エクスプロイトブロック	NEW	Hyper-V検査	NEW
ストレージ検査	NEW	アイドル状態検査	NEW	共有ローカルキャッシュ	NEW
HIPS	NEW	フィッシング対策		アンチステルス技術	
リムーバブルメディア検査		-			

(3) その他機能の追加および改善

Windowsクラスタ環境へのサポート	NEW	デバイスコントロール	NEW	遅延アップデート	NEW
ウイルス定義データベースのロールバック	NEW	古いウイルス定義データベースアラート		電子メール通知間隔の選択	NEW
WMIプロバイダー	NEW	汎用フォーマットのログオプション	NEW	プログラムコンポーネント別のインストール	NEW
ESET SysRescue Live		ESET特殊駆除ツール	NEW	ESET Log Collector	NEW
ESET CMD	NEW	-		-	



①ユーザーインターフェースの 改善

3 デザインの変更

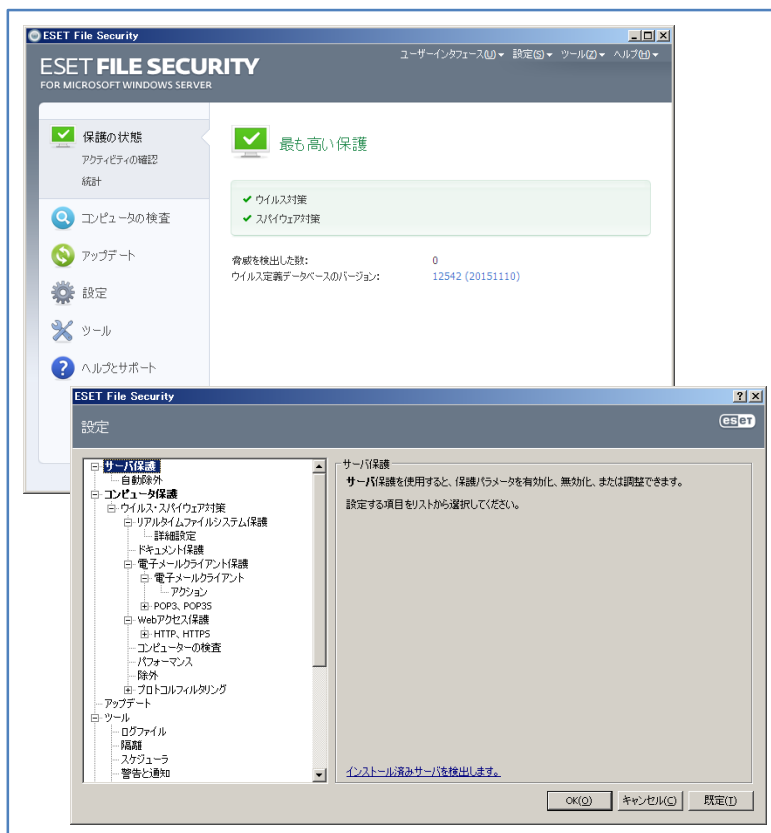
ESET ENDPOINT ANTIVIRUS



ユーザーインターフェースが新しいデザインに変更され、より高い可視性とより直感的な操作が可能となりました。

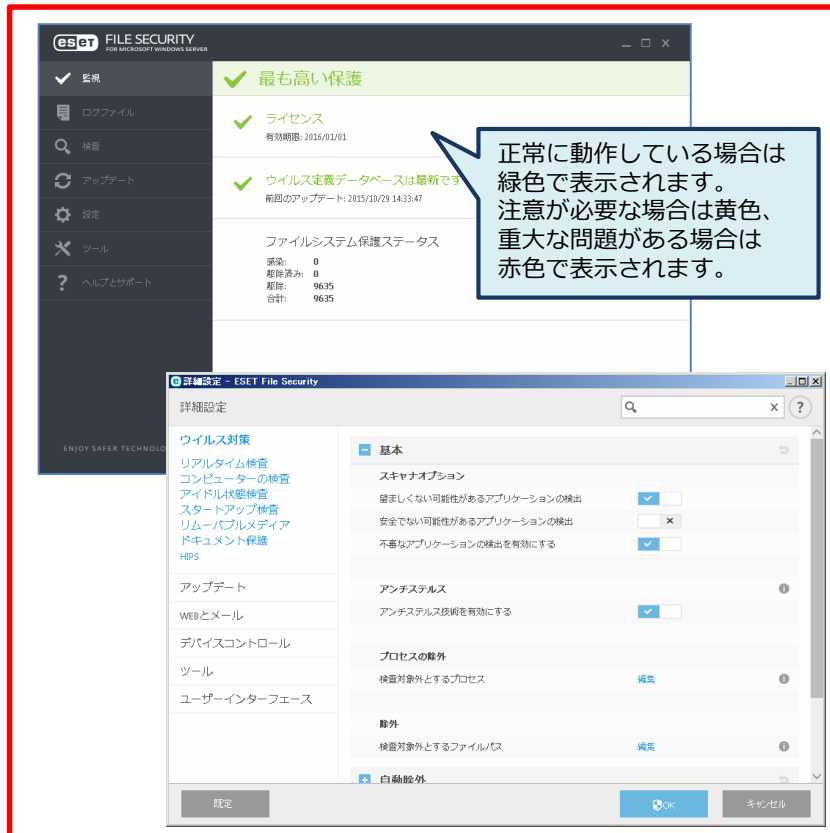
旧バージョン

(ESET File Security for Microsoft Windows Server V4.5
プログラム画面)



新バージョン

(ESET File Security for Microsoft Windows Server V6
プログラム画面)



3 ユーザーインターフェースの起動モード



ユーザーインターフェースの起動モードが選択することが可能となりました。
クライアントの用途や運用に合わせてユーザーインターフェースの表示を調整することができます。

詳細設定(ユーザーインターフェース画面)



起動モード

モード	動作
完全	基本画面、通知、アラートを含むすべてのGUIが表示されます。
ターミナル、端末	通知またはアラートは表示されません。管理者だけがGUIを起動できます。



②保護技術・保護機能の 追加および改善

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を可能となりました。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

※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

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となりました。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に対して検知性能が向上しました。

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 (バルナラビリティ)

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

Microsoft Hyper-V Server上の仮想マシン(VM)ディスクを検査する機能が追加されました。Hyper-V検査は現時点では読み取り専用となり、検査のみを行い駆除を行いません。脅威への駆除機能は将来実装される予定です。

(i)検査対象の仮想マシンがオンラインの場合

仮想マシンのスナップショットを作成し、スナップショット経由で読み取り専用モードでディスクに接続し検査します。

(ii)検査対象の仮想マシンがオフラインの場合

Hyper-V Managementと仮想ディスクのサポートにより、仮想マシンのOSのディスクを検出し検査します。

※ESET File Securityを実行するサーバー上にHyper-V Managerがインストールされている場合に、ESETの検査メニューにHyper-V検査が表示されます。

※サポート対象のOSは下記となります。

- Windows Server 2016
 - Windows Storage Server 2016
 - Windows Server 2012 R2
 - Windows Server 2012
 - Windows Server 2008 R2
- ※本OSを実行する仮想マシンはオフラインの場合のみ検査できます。

※本機能はESET File Security for Microsoft Windows Server V6.3よりご使用いただけます。

ローカルサーバーのすべての共有ファイルを検査します。本機能によりファイルサーバーに保存されたユーザーデータだけを選択して、検査が容易に行えるようになりました。なお、本検査はローカルに共有フォルダがある場合に実行可能です。

メインメニュー（検査）



コンピュータのアイドル状態(スクリーンセーバー、コンピュータのロック、ユーザーのログオフ)の間を利用して、コンピュータ全体の検査をサイレントに実行する機能が追加されました。これにより、ユーザーはコンピュータの検査を意識することなく、コンピュータを利用することが可能です。

詳細設定(アイドル状態検査画面)

詳細設定 - ESET File Security

詳細設定

ウイルス対策

リアルタイム検査

コンピュータの検査

アイドル状態検査 1

スタートアップ検査

リムーバブルメディア

ドキュメント保護

HIPS

アップデート

WEBとメール

デバイスコントロール

基本

アイドル状態検査を有効にする ☒

コンピュータがバッテリー電源を使用している場合にも実行 ☐ x

ログを有効にする ☐ x

アイドル状態検知

スクリーンセーバー ☒

コンピュータのロック ☒

ユーザーのログオフ ☒

有効にする際には、チェックを付けてください。※既定値は無効に設定されます。

どのアイドル状態の間を利用して検査を行うか選択することが可能です。

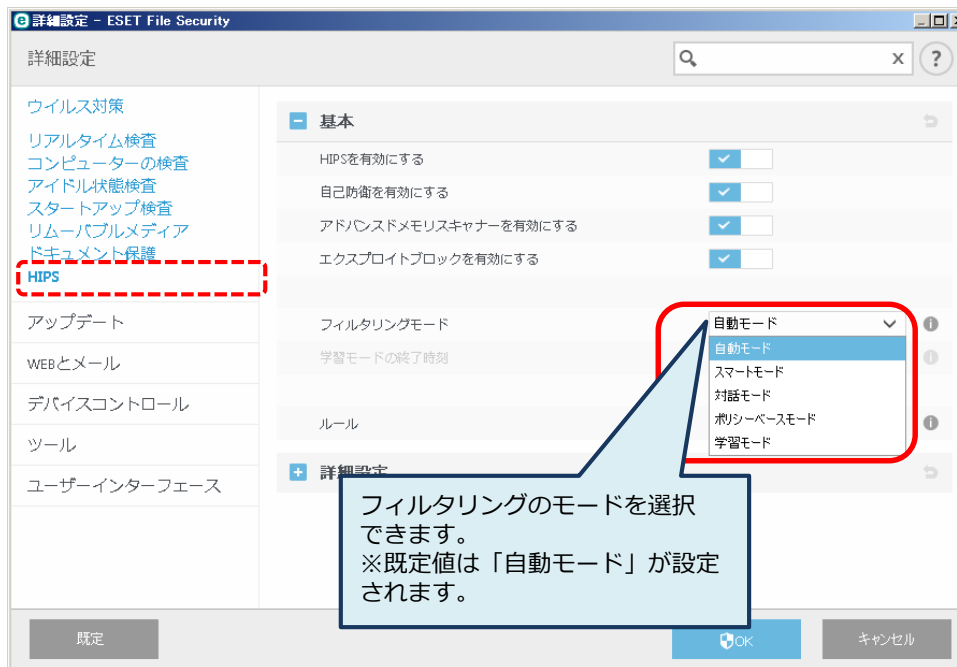
仮想環境において、検査結果を共有する機能が追加されました。これにより重複した検査がなくなり、検査速度や仮想環境のパフォーマンスが向上します。本機能を使用する場合、各クライアントで検査した情報をキャッシュし共有する、共有ローカルキャッシュサーバー(Linux OSで稼動)を用意する必要があります。

詳細設定(ウイルス対策画面)



上級ユーザー向けの機能として、任意のシステムレジストリ/プロセス/アプリケーション/ファイルに対して、変更の可否やモニタリングなどのルールを定義することができます。

詳細設定(HIPS画面)



HIPS警告画面



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。

※本機能はESET Endpoint Security V5/ESET Endpoint アンチウイルス V5以降のプログラムでもご使用いただけます。
(V5製品のサポートは終了いたしました。)

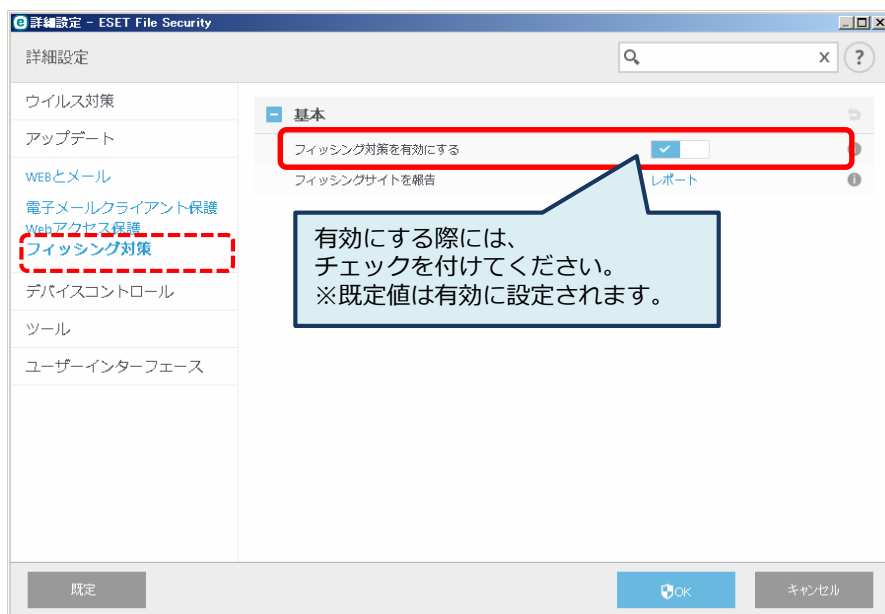
3

フィッシング対策

ENDPOINT ANTIVIRUS

Webアクセス保護に統合されていたフィッシング対策機能が新機能として独立しました。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を開発元ESET社へ報告することも可能となりました。

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

実在する会員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



アンチステルス技術が改善され、オペレーティングシステムから自らを見えなくすることができるルートキットなどの危険なプログラムの検出性能が向上しました。

詳細設定(ウイルス対策画面)



※アンチステルス技術

ルートキットなどの自己の存在を隠蔽し、通常のスキャンでは感知できない悪質な不正プログラムも検出可能にする技術を意味します。

※ルートキット

自己の存在を隠しながら、インターネットからの攻撃者が、システムに無制限にアクセスできるようにする悪意のあるプログラムです。ルートキットは、システムにアクセス(通常はシステムの脆弱性を悪用します)した後、オペレーティングシステムの様々な機能を使用して、ウイルス対策ソフトウェアによる検出を免れようとしています。



コンピュータの検査について従来の「スマート検査」と「カスタム検査」のほか「リムーバブルメディア検査」が新たに追加されました。

「リムーバブルメディア検査」では、現在コンピュータに接続されているリムーバブルメディア(CD/DVD/USBなど)の検査をすばやく開始します。

メインメニュー(コンピュータの検査)



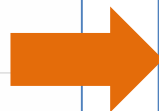


③その他機能の追加 および改善

システム情報やログ情報を収集するツールが新たに追加されました。これにより問題解決のための各種情報を速やかに取得することが可能です。

- 本ツールはサポートセンターよりお客様へご案内があった場合にのみご利用ください。

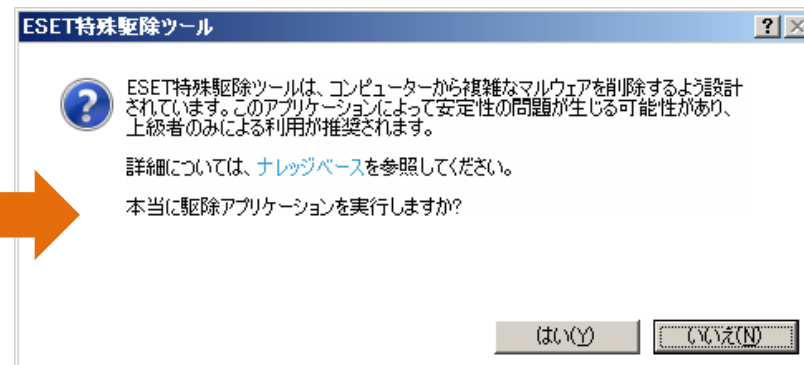
ESET Log Collectorご利用までの流れ



複数のマルウェアを駆除するツールが新たに追加されました。これによりESETの標準機能では駆除ができないウイルスに対応することが可能です。

- 本ツールはサポートセンターよりお客様へご案内があった場合にのみご利用ください。

ESET特殊駆除ツールご利用までの流れ



3

電子メール通知間隔の選択

電子メール通知機能にてイベント発生後やウイルス検出後に電子メールで通知を行うまでの期間を選択することができるようになりました。

これにより即座に管理者へ電子メール通知を行うことが可能となります。

詳細設定(電子メール通知画面)

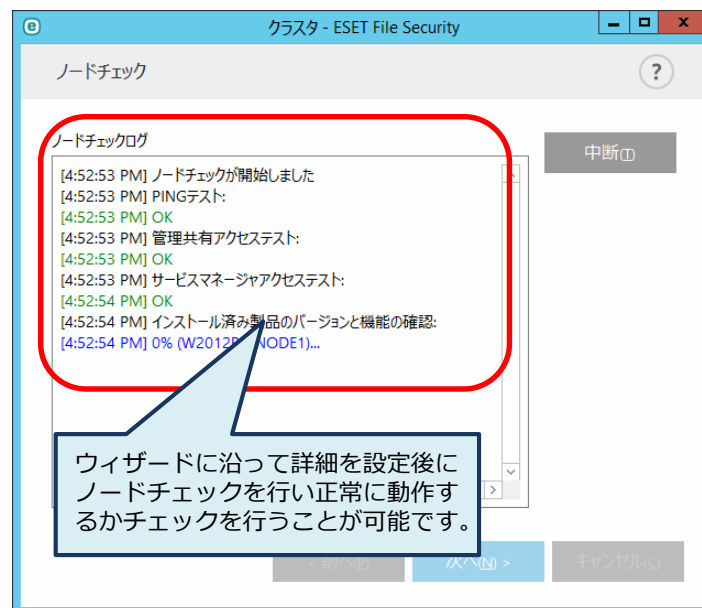
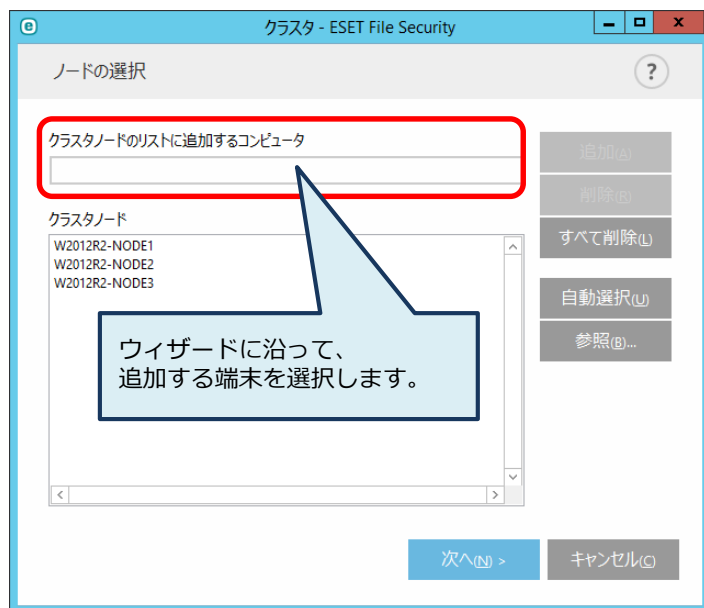
間隔を「0」に指定すると、
即時送信されます。
※既定値は5分が設定されます。

3 Windowsクラスター環境へのサポート



Windowsクラスター環境へのサポートが可能となりました。クラスターを構成した場合にESET製品同士が通信を行い、構成や設定情報、通知などクラスター環境が正しく動作するために必要なデータを同期することができます。本機能はクラスターが構成されている場合に有効となります。クラスターの設定および、ノードの追加はクラスターウィザードを用いることで構成が可能です。

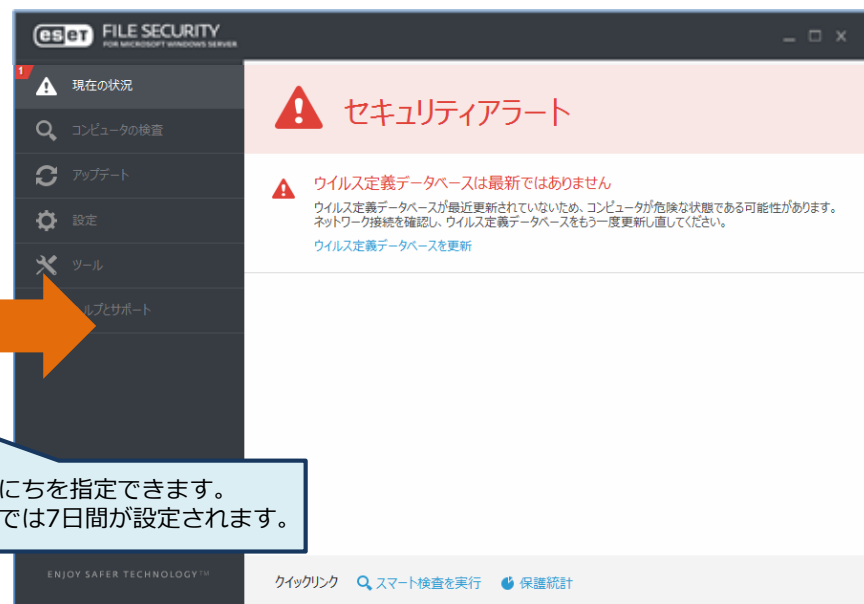
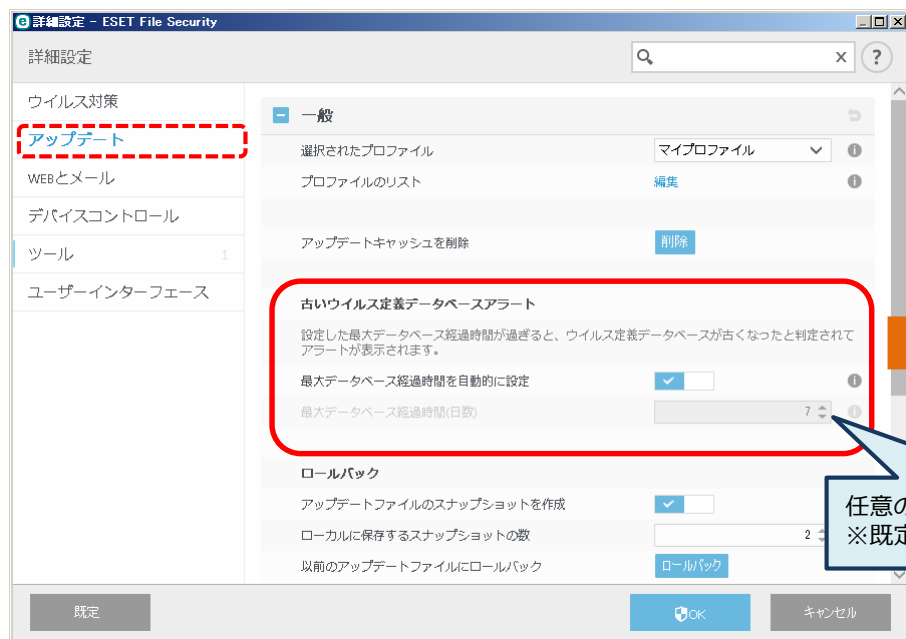
詳細設定（クラスターウィザード画面）



3 古いウイルス定義データベースアラート

ウイルス定義データベースが古い場合にアラートを表示します。
任意の日数を設定することができるようになり、社内のポリシーにあわせてアラートを表示させることが可能です。

詳細設定(アップデート画面)



各エンドポイント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。

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	○	-	○	○
USB プリンタ	○	-	○	○
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	○	○	○	○

※本機能はESET Endpoint Security V5/ESET Endpoint アンチウイルスV5以降のプログラムでもご使用いただけます。
(V5製品のサポートは終了いたしました。)

デバイスコントロール設定

デバイスのタイプ: ディスクストレージ

アクション: 読み込み/書き込み

条件タイプ: デバイス

ベンダー:

モデル:

シリアル:

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。またユーザーの指定も可能です。

デバイスコントロール警告メッセージ画面

FILE SECURITY

⚠ デバイスへのアクセスは拒否されました

デバイスのタイプ(V): CD/DVD

ドライブ: D:\

ベンダ(IN): eset-20150723

モデル(IL): 6C75ABEA

デバイス制御使用ポリシーによって、デバイスへのアクセスが制限されています。このポリシーに
関係なくデバイスにアクセスする場合は[アクセスする]をクリックします。これはセキュリティロ
グに記録されます。

続ける

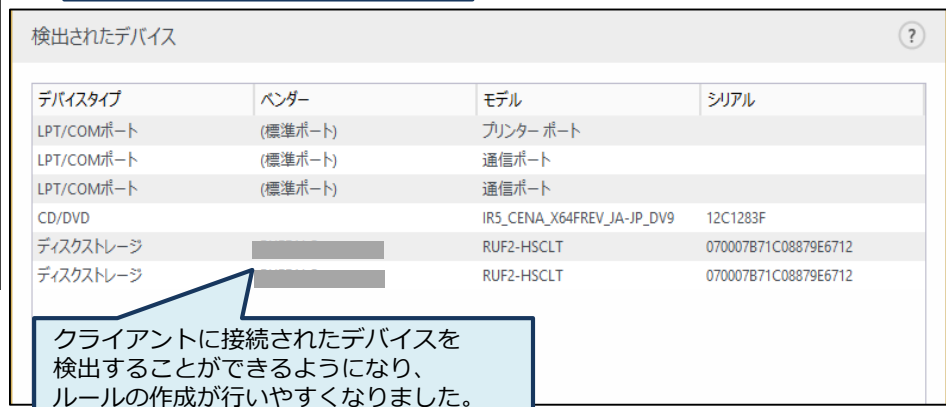
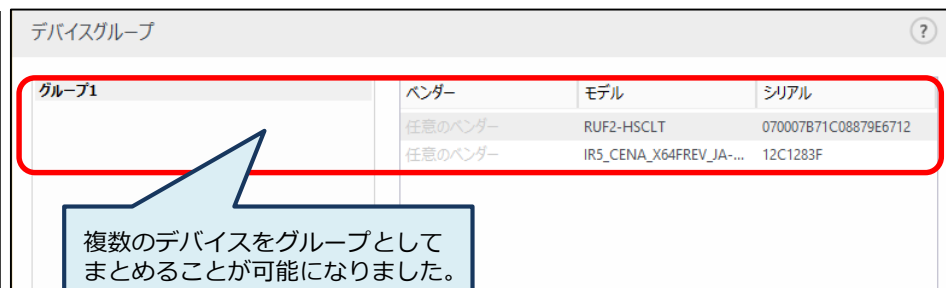
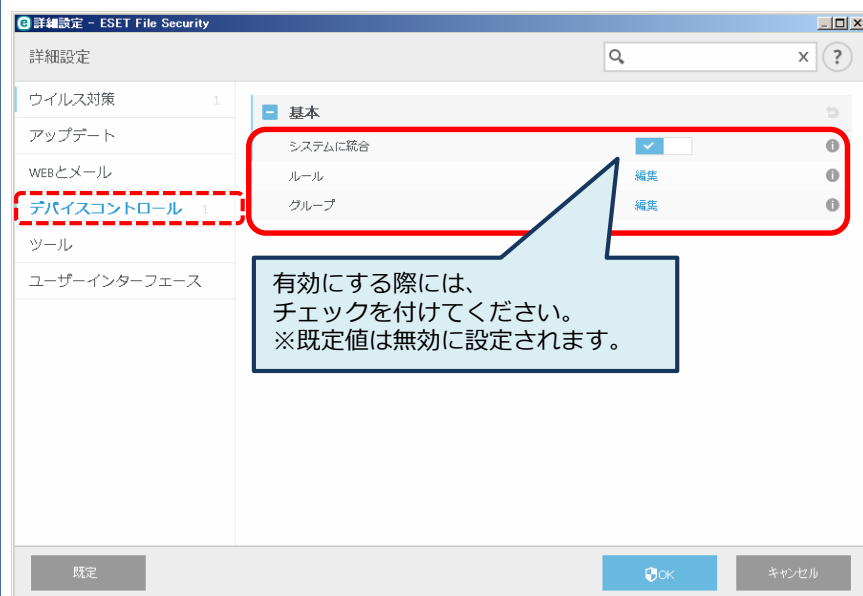
キャンセル

3 デバイスコントロール グループルールの追加

NEW

デバイスコントロール機能にて、接続されているデバイスを検出することが、可能となりました。また、複数のデバイスをデバイスグループとしてまとめることが可能となりました。これにより、デバイスコントロールルールの作成が行いやすくなりました。

詳細設定(デバイスコントロール画面)



3 ウイルス定義データベースのロールバック

NEW

ウイルス定義データベース、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。既定値では、2つまでスナップショットを作成することができ、クライアント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、ESET Remote Administratorから任意のクライアント（複数可）に対して、ロールバックさせたり、指定時間(12, 24, 36, 48時間)、または、手動で取り消すまでの間、クライアント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）

The screenshot shows the 'ESET File Security' settings window. The 'Update' tab is selected in the left sidebar. The 'Rollback' section is highlighted with a red box. It contains the following settings:

- アップデートファイ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: 2
- 以前のアップデートファイルにロールバック:

A callout box explains: 「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。スナップショットの容量は規定の2世代で約120MB程度になります。」

Below the main window, a smaller window titled 'ロールバック' is shown. It has a '時間' (Time) dropdown menu with the following options: 12時間, 128時間, 248時間, 368時間, 488時間, and 取り消しまで. The '12時間' option is selected. A callout box explains: 「ロールバック実施後、次回アップデートを停止する時間を指定します。」

At the bottom left, a note states: 「※本機能はESET Endpoint Security V5/ESET Endpoint アンチウイルス V5以降のプログラムでもご使用いただけます。（V5製品のサポートは終了いたしました。）」

ウイルス定義データベースのアップデート方法に、最新のウイルス定義データベース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時間遅れのウイルス定義データベースを配信する特別なアップデートサーバを、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)



※本機能はESET Endpoint Security V5/ESET Endpoint アンチウイルス V5以降のプログラムでもご使用いただけます。
(V5製品のサポートは終了いたしました。)

WMIプロバイダーは、ESETのセキュリティ管理ツールを必要とせずに、ESET製品のリモート監視を提供するための機能です。

WMI経由で基本製品、ステータス、統計情報を提供し、企業管理者がESET製品を監視する能力を高めています。

管理者はWMIのさまざまなアクセス方法(コマンドライン、スクリプト、他社製のエンタープライズ監視ツール)を利用して、ESET製品の状態を監視できます。

※WMI : Windows Management Instrumentationの略

(コマンドラインを使用した情報の取得例)

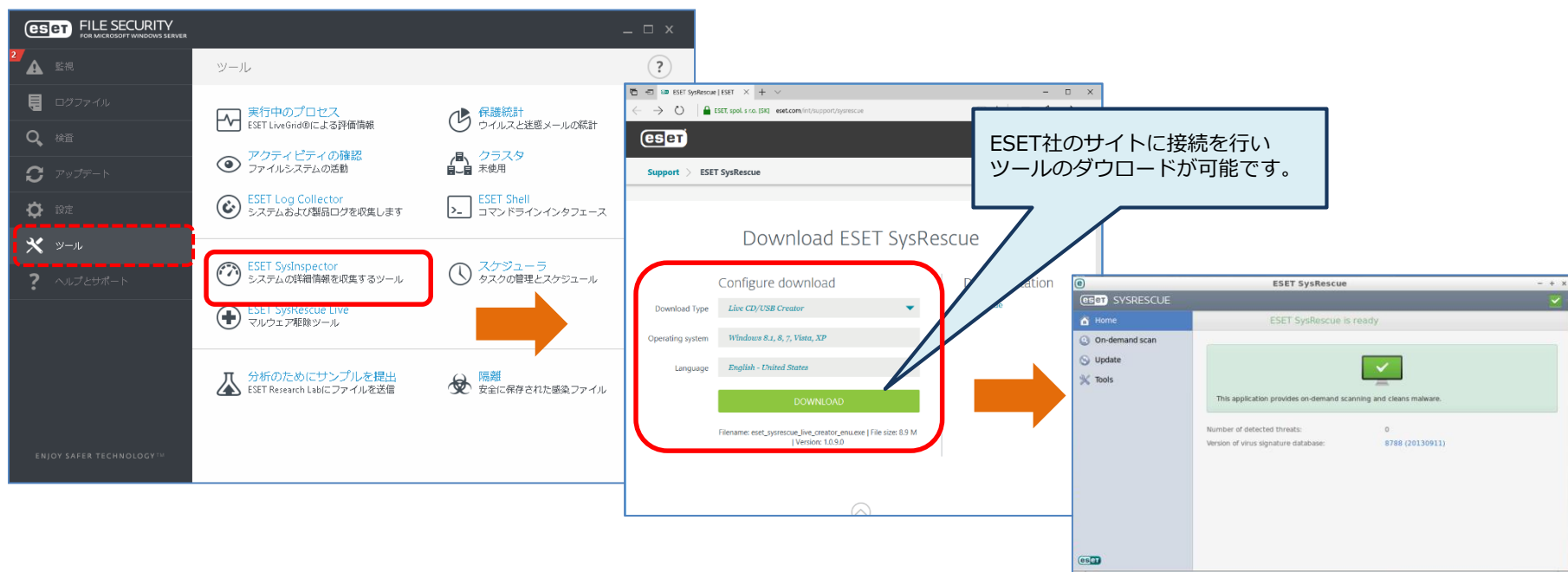
- ・ローカルコンピュータのESET製品の製品バージョン番号を表示する場合

```
C:¥Users¥administrator>wmic /namespace:¥¥root¥ESET Path ESET_Product Get Version  
Version  
6.2.12007.1
```



ESET SysRescue（レスキューCD）の作成方法が刷新され、従来と比べ使いやすくなりました。ESET SysRescue Liveのリンクをクリックすると、専用WebページよりESET SysRescueの作成ツールやESET SysRescueのディスクイメージをダウンロードすることが可能です。

ESET SysRescue Live利用の流れ

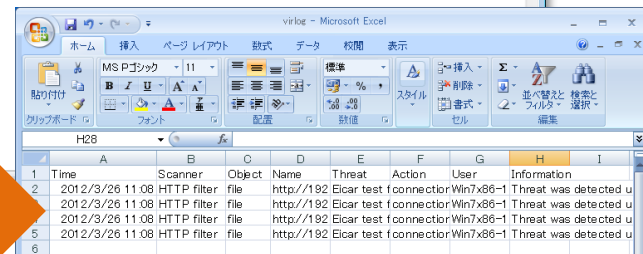
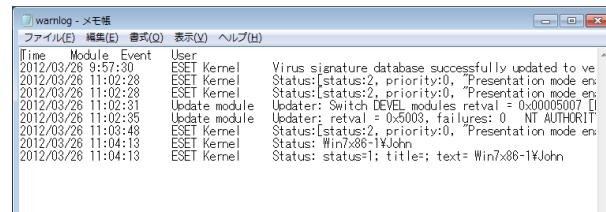
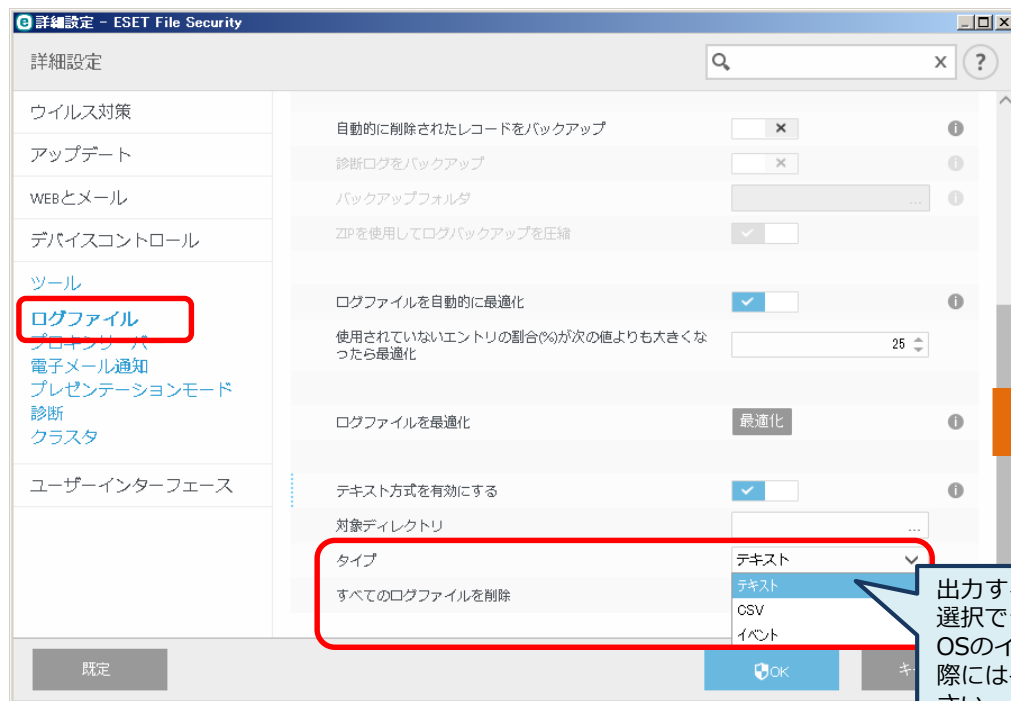


3 汎用フォーマットのログオプション

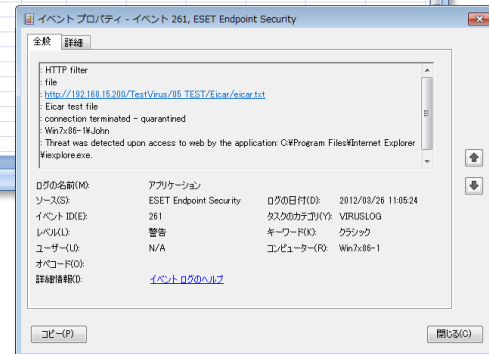
NEW

通常のログに加えて、CSV/プレーンテキストフォーマットを選択してログを作成することができます。本機能によりサードパーティーのログ管理ツールとの連携が可能となります。また、OSイベントログへの記録も行うことができます。

詳細設定（ログファイル設定画面）



出力するログのタイプを選択できます。
OSのイベントログに出力する際にはイベントを選択してください。



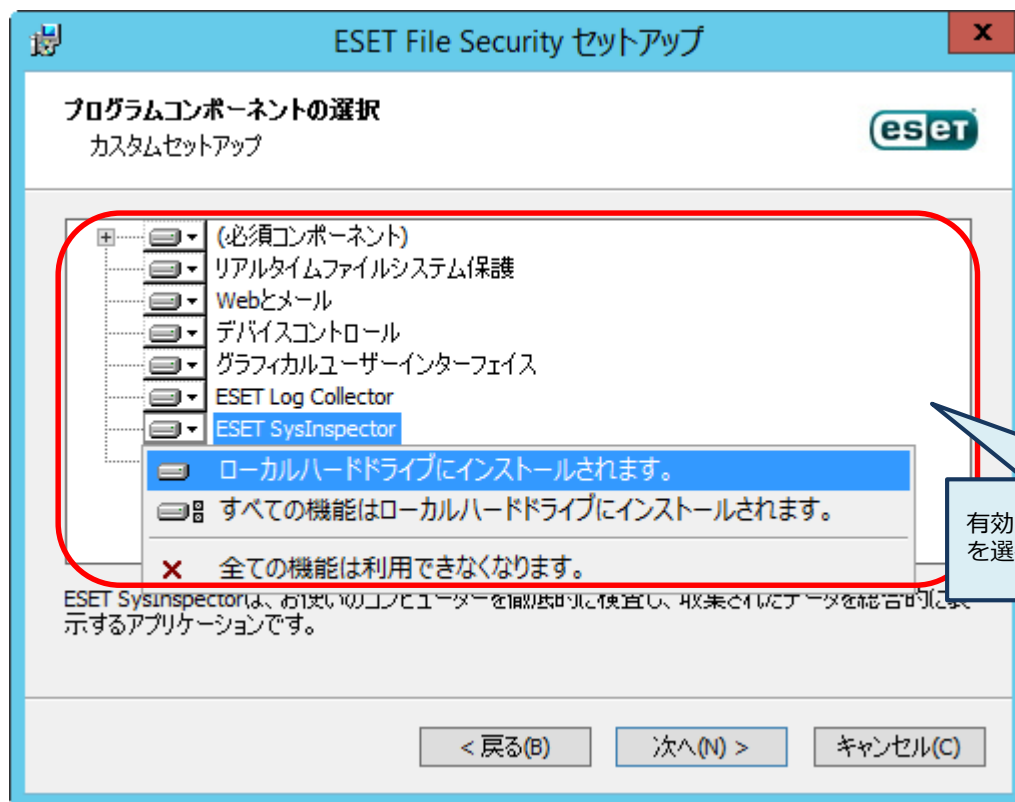
※本機能はESET Endpoint Security V5.0/ESET Endpoint アンチウイルス V5.0以降のプログラムでもご使用いただけます。（V5製品のサポートは終了いたしました。）

3 プログラムコンポーネント別のインストール



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)

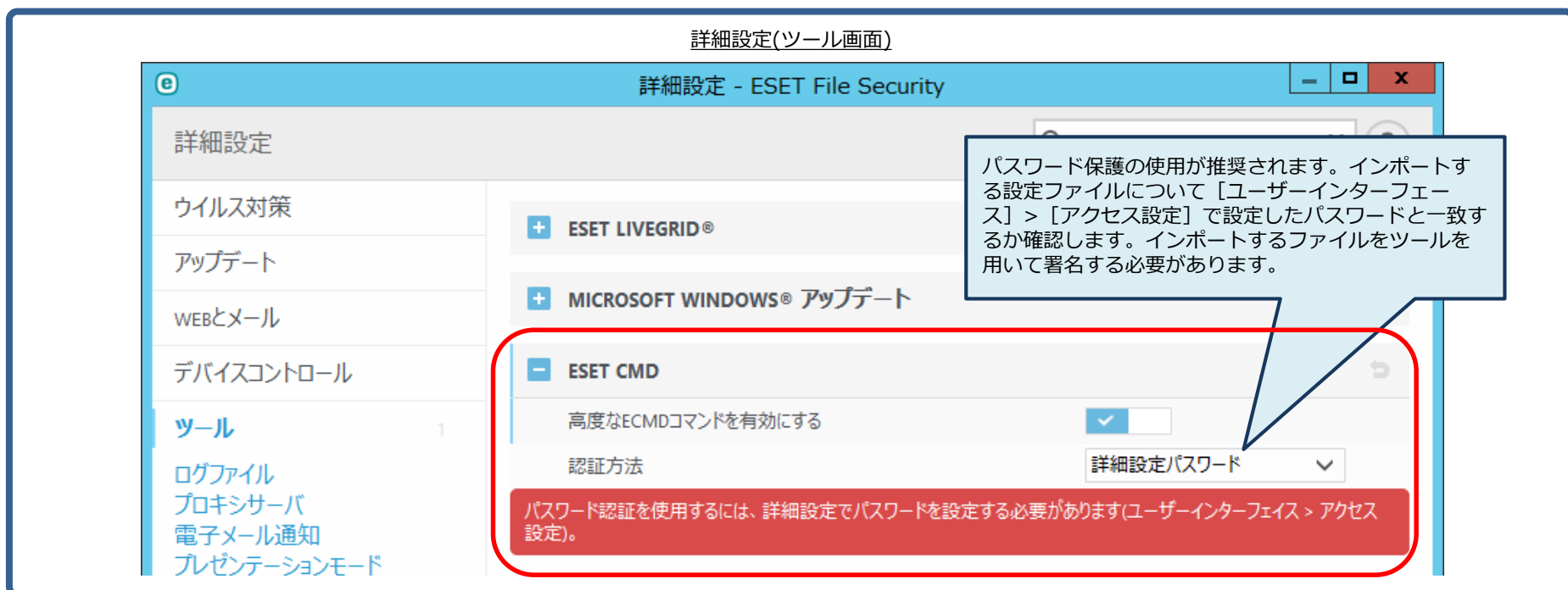


※本機能はESET Endpoint Security V5.0以降のプログラムでもご使用いただけます。
(V5製品のサポートは終了いたしました。)

コマンドラインを利用して設定ファイルをインポートおよびエクスポートできるようになりました。コマンドラインを利用した手動実行や自動化用のスクリプトの作成をすることができます。ECMDコマンドを使用する際には管理者権限で実行するか、管理者として実行を使用してコマンドプロンプトを開く必要があります。

※高度なECMDコマンドはローカルのみで実行できます。

ERAを使用したクライアントタスクのコマンド実行では動作しません。



※本機能はESET File Security for Microsoft Windows Server V6.5よりご利用いただけます。



ESET File Security for Microsoft Windows Server V6

(2)バージョン別の機能比較について



ESET File Security for Microsoft Windows ServerはサーバOS向けに最適化した製品になります。本バージョンよりクライアントOS向けプログラムと同じバージョンとなり、同等の機能を実装しました。

ウイルス・スパイウェア対策機能		
機能名	EFSW V4.5	EFSW V6
オンデマンド検査	○	○
リアルタイム保護	○	○
ドキュメント保護	○	○
Webアクセス保護	○	○
電子メール保護	○	○
暗号化通信の検査 (HTTPS・POP3Sの検査)	○	○
ESET Live Grid (ThreatSense.Net) ※1	○	○
ホスト侵入防止システム (HIPS)	×	○
自己防衛機能	○	○
アイドル状態検査	×	○
アドバンスドメモリースキャナー	×	○
エクスプロイトブロック	×	○

ネットワーク通信関連機能		
機能名	EFSW V4.5	EFSW V6
ネットワーク接続表示	○	○
アップデート・ミラーサーバー機能		
定義データベースのアップデート	○	○
定義データベースの遅延アップデート	×	○
オフライン更新機能	○	○
定義データベースのロールバック	×	○
ミラーサーバー機能	○	○
ミラーサーバー機能の差分更新 (ナノアップデート)	×	○

※1: 「ESET Live Grid」は「ThreatSense.Net」の後継機能

【略称について】

EFSW : ESET File Security for Microsoft Windows Server

3

バージョン別の機能比較(2/2)



その他の機能 (1)		
機能名	EFSW V4.5	EFSW V6
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	×	○
リムーバブルメディアの 自動検査	×	○
Windows更新プログラムの 適用通知	○	○
プレゼンテーションモード	×	○
ユーザーインターフェースの 起動モード選択	×	○
統計表示	○	○
アクティビティの表示	○	○
実行中のプロセス表示	×	○
サーバーの保護機能 (自動除外)	○	○
共有ローカルキャッシュ	×	○
eShell (コマンドラインインターフェース)	○	○

その他の機能 (2)		
機能名	EFSW V4.5	EFSW V6
設定のインポート・エクスポート	○	○
ESET CMD	×	○※2
ESET SysInspector機能	○	○
ESET SysRescue機能	○	○
モジュールを指定したインストール	×	○
サーバーOSへのインストール	○	○
Windowsクラスター環境のサポート	×	○
ESET Remote Administrator V5.3による管理	○	×
ESET Remote Administrator V6による管理	○※1	○※1

※1: ESET Remote Administratorでクライアントを管理するには、
各クライアントにERAエージェントの導入が必要

※2: ESET File Security for Microsoft Windows Server V6.5 からの搭載

※ ESET Remote Administratorのサポートは終了いたしました。

【略称について】

EFSW : ESET File Security for Microsoft Windows Server