

ESET Server Security

ユーザー ガイド

[この文書のオンラインバージョンを表示するにはこちらをクリックしてください。](#)



Copyright ©2023 by ESET, spol. s r.o.

ESET Server SecurityはESET, spol. s r.o.によって開発されています

詳細については<https://www.eset.com>をご覧ください。

All rights reserved.本ドキュメントのいかなる部分も、作成者の書面による許可がない場合、電子的、機械的、複写、記録、スキャンなど、方法または手段の如何をと問わず、複製、検索システムへの保存、または転送が禁じられています。

ESET, spol. s r.o.は、事前の通知なしに、説明されたアプリケーションソフトウェアを変更する権利を有します。

テクニカルサポート: <https://support.eset.com>

改訂: 2023年/3月/19日

1 序文	1
2 概要	2
2.1 主要な機能	2
2.2 新機能	3
2.3 保護の種類	3
3 インストールの準備	4
3.1 システム要件	5
3.2 SHA-2は互換性が必要	6
3.3 ESET Server Securityのインストール手順	7
3.3 既存のインストールの修正	11
3.4 サイレント / 無人インストール	12
3.4 コマンドラインインストール	13
3.5 製品のアクティベーション	16
3.5 ESET Business Account	17
3.5 アクティベーションは正常に実行されました	18
3.5 アクティベーションに失敗しました	18
3.5 ライセンス	18
3.6 新しいバージョンへのアップグレード	18
3.6 ESET PROTECT経由でのアップグレード	19
3.6 ESET Cluster経由でのアップグレード	21
3.7 クラスター環境でのインストール	24
3.8 ターミナルサーバ	24
3.9 セキュリティと安定性のアップデート	24
4 はじめに	25
4.1 ESET PROTECTを使用した管理	25
4.2 監視	26
4.2 状態	27
4.2 Windows Updateが利用可能です	29
4.2 ネットワーク隔離	29
5 コマンドと ESET Server Security	30
5.1 検査	31
5.1 検査ウィンドウと検査ログ	33
5.2 ログファイル	35
5.2 ログのフィルタ	38
5.3 アップデート	40
5.4 設定	42
5.4 サーバー	43
5.4 コンピューター	44
5.4 ネットワーク	45
5.4 ネットワークトラブルシューティングウィザード	46
5.4 Webとメール	46
5.4 ツール - 診断ロギング	47
5.4 設定のインポート/エクスポート	48
5.5 ツール	49
5.5 実行中のプロセス	49
5.5 アクティビティの確認	51
5.5 保護統計	52
5.5 クラスター	53
5.5 クラスターウィザード - ノードの選択	55
5.5 クラスターウィザード - クラスター設定	57

5.5 クラスターウィザード - クラスターセットアップ設定	57
5.5 クラスターウィザード - ノードチェック	58
5.5 クラスターウィザード - ノードインストール	59
5.5 ESET Shell	62
5.5 使用状況	64
5.5 コマンド	69
5.5 バッチファイル/スクリプト	72
5.5 ESET SysInspector	73
5.5 ESET SysRescue Live	74
5.5 スケジューラ	74
5.5 スケジューラー - タスクの追加	75
5.5 タスクの種類	77
5.5 タスクの実行	78
5.5 トリガーされたイベント	78
5.5 アプリケーションの実行	79
5.5 タスクが実行されなかった場合	79
5.5 スケジュールタスクの概要	79
5.5 分析のためにファイルを提出	79
5.5 不審なファイル	80
5.5 不審なサイト	80
5.5 誤検出ファイル	81
5.5 誤検出サイト	81
5.5 その他	82
5.5 隔離	82
5.6 OneDrive検査の設定	83
5.6 ESET OneDrive スキャナーの登録	86
5.6 ESET OneDrive スキャナーの登録解除	90
6 一般設定	94
6.1 検出エンジン	95
6.1 機械学習による検出	97
6.1 除外	99
6.1 パフォーマンスの除外	99
6.1 検出除外	100
6.1 除外の作成ウィザード	102
6.1 詳細設定オプション	103
6.1 自動除外	103
6.1 共有ローカルキャッシュ	103
6.1 侵入が検出された	104
6.1 リアルタイムファイルシステム保護	105
6.1 ThreatSense パラメータ	106
6.1 追加の ThreatSense パラメータ	110
6.1 検査対象外とするファイル拡張子	110
6.1 除外を処理する	111
6.1 クラウドベース保護	112
6.1 除外フィルタ	114
6.1 マルウェア検査	114
6.1 プロファイルマネージャ	116
6.1 プロファイルターゲット	116
6.1 検査の対象	118
6.1 アイドル状態検査	120
6.1 スタートアップ検査	120

6.1 自動スタートアップファイルのチェック	120
6.1 リムーバブルメディア	121
6.1 ドキュメント保護	122
6.1 Hyper-V検査	122
6.1 OneDrive検査	124
6.1 HIPS	125
6.1 HIPSルール設定	127
6.1 HIPS詳細設定	130
6.2 アップデートの設定	130
6.2 アップデートのロールバック	134
6.2 スケジュールタスク - アップデート	134
6.2 ミラーでの更新	135
6.3 ネットワーク保護	137
6.3 IDSの例外	139
6.3 一時IPアドレスブラックリスト	139
6.4 Webとメール	139
6.4 プロトコルフィルタリング	140
6.4 Webと電子メールのクライアント	141
6.4 SSL/TLS	141
6.4 既知の証明書のリスト	142
6.4 暗号化されたSSL通信	143
6.4 電子メールクライアント保護	144
6.4 電子メールプロトコル	145
6.4 警告と通知	146
6.4 MS Outlookツールバー	146
6.4 Outlook ExpressおよびWindowsメールツールバー	147
6.4 確認ダイアログ	147
6.4 メッセージの再検査	147
6.4 Webアクセス保護	148
6.4 URLアドレス管理	149
6.4 新規リストの作成	150
6.4 フィッシング対策Web保護	152
6.5 デバイスコントロール検査	153
6.5 デバイスルール	154
6.5 デバイスグループ	156
6.6 ツール設定	157
6.6 タイムスロット	157
6.6 Microsoft Windows Update	157
6.6 コマンドラインスキャナー	158
6.6 ESET CMD	160
6.6 ESET RMM	162
6.6 ライセンス	163
6.6 WMIプロバイダ	163
6.6 提供されたデータ	164
6.6 提供されたデータへのアクセス	171
6.6 ESET PROTECT検査の対象	172
6.6 上書きモード	172
6.6 ログファイル	176
6.6 プロキシサーバ	177
6.6 通知	178
6.6 アプリケーション通知	178

6.6 デスクトップ通知	179
6.6 電子メール通知	179
6.6 カスタマイズ	181
6.6 プレゼンテーションモード	182
6.6 診断	182
6.6 テクニカルサポート	183
6.6 クラスタ	183
6.7 ユーザーインターフェース	185
6.7 アラートとメッセージボックス	186
6.7 アクセス設定	186
6.7 ESET Shell	187
6.7 ターミナルサーバでのGUIの無効化	188
6.7 無効にされたメッセージとステータス	188
6.7 アプリケーションステータス設定	188
6.7 システムトレイアイコン	189
6.8 デフォルト設定に戻す	190
6.9 ヘルプとサポート	191
6.9 サポート要求の送信	192
6.9 ESET Server Securityについて	193
6.10 用語集	193
7 エンドユーザーライセンス契約	193
8 プライバシーポリシー	199

序文

このガイドは、ESET Server Securityを最大限に活用することを目的としています。プログラムの各ウィンドウの詳細については、特定のウィンドウが開いている状態でキーボードの **F1** を押します。現在表示しているウィンドウに関連するヘルプページが、表示されます。

一貫性と混乱を防止するため、このガイドで使用される用語はESET Server Securityパラメーター名に基づいています。また、統一された記号を使用して、特定の関心または重要性があるトピックを強調しています。

注意

注意は簡単な説明です。省略できますが、特定の機能や一部の関連トピックへのリンクといった有益な情報が含まれていることがあります。

重要

注意が必要であり、省略しないことをお勧めします。重要な注意には、重大ではない重要な情報が含まれます。

警告

十分に注意して目を通すべき重大な情報です。特に、有害な間違いを防止するために警告が書かれています。警告の括弧内にある文を読んで理解してください。十分な注意が必要なシステム設定やリスクがある設定について説明されています。

例

これは使用例または実際の例であり、特定の機能を使用する方法を理解できるようにすることを目的としています。

ヘルプページの右上端に次の要素が表示される場合は、ESET Server Securityのグラフィカルユーザーインターフェース(GUI)のウィンドウにおけるナビゲーションを示しています。この手順に従えば、該当するヘルプページで説明されているウィンドウに移動します。


ESET Server Securityを開く

設定 > サーバ > OneDrive検査設定 > 登録をクリックする



書式規則:

表記規則	意味
太字	セクション見出し、機能名、ボタンなどのユーザーインターフェイス項目。
斜体	ユーザーが入力する情報のプレースホルダー。たとえば、ファイル名やパスは、ユーザーが実際のパスまたはファイル名を入力することを意味します。
Courier New	コードサンプルまたはコマンド

表記規則	意味
ハイパーリンク 	相互参照されたトピックまたは外部Webサイトへのすばやく簡単なアクセスを提供します。ハイパーリンクは青字でハイライトされ、下線も付いている場合があります。
%ProgramFiles%	Windowsなどのインストール済みプログラムを格納するWindowsシステムディレクトリ。



ESET Server Securityオンラインヘルプページは、複数の章と下位章に分割されています。関連する情報を検索するには、ヘルプページの目次を参照します。あるいは、単語または語句を入力して、全文検索を使用できます。

概要

ESET Server Securityは、特にMicrosoft Windows Server環境向けの統合ソリューションです。ESET Server Securityは、さまざまな種類のマルウェアに対する効果的かつ堅牢な保護を備えており、マルウェア対策保護とスパイウェア対策保護という2種類の保護を提供しています。

主要な機能

次の表は、ESET Server Securityで使用可能な機能の一覧を示します。ESET Server Securityは、スタンドアロンおよびクラスタ環境で、Microsoft Windows Server 2008 R2 SP1、2012、2016、2019のほとんどのエディションをサポートします。大規模なネットワークでは、ESET PROTECTを使用してリモートでESET Server Securityを管理できます。

真の64ビット製品コア	製品のコアコンポーネントにより高いパフォーマンスと安定性を追加。
マルウェア対策	受賞経験のある  と革新的なマルウェアに対する防御を実現する、この最先端技術  は攻撃を防止し、ウイルス、ランサムウェア、ルートキット、ワーム、スパイウェアを含むすべての種類の脅威を排除します。クラウドベースの検査を使用するため、さらに検出率が高くなっています。軽量でシステムリソースの負荷が少ないため、パフォーマンスを犠牲にしません。階層型のセキュリティモデルが使用されます。各階層またはフェーズではさまざまなコア技術が使用されています。実行前フェーズでは、UEFIスキャナー、ネットワーク攻撃保護、レピュテーションおよびキャッシュ、製品内サンドボックス、DNA検出などの技術が使用されます。実行フェーズでは、エクスプロイトブロッカー、ランサムウェア保護、アドバンスドメモリスキャナー、スクリプトスキャナ(AMSI)が使用されます。実行後フェーズでは、ボットネット保護、クラウドマルウェア保護システム、サンドボックスが使用されます。この機能が豊富なコア技術により、比類ないレベルの保護が実現されます。
OneDrive検査	これはOneDriveクラウドストレージにあるファイルを検査できる追加された新機能です。Office 365ビジネスアカウント用。
Hyper-V検査	Microsoft Hyper-V Server上の仮想マシン(VM)ディスクの検査を実行できる新しい技術です。特定のVM上で「エージェント」は不要です。
ESET Dynamic Threat Defense (EDTD)	ESETクラウドベースサービスESET Server Securityが不審なコードまたはコードを検出するとESET Dynamic Threat Defense隔離に一時的に配置することで、さらなる脅威アクティビティを防止します。不審なサンプルは自動的にESET Dynamic Threat Defenseサーバーに送信され、最先端のマルウェア検出エンジンで分析されます。ESET Server Securityは、その後分析の結果を受信します。不審なファイルは結果に応じて処理されます。

真の64ビット製品コア	製品のコアコンポーネントにより高いパフォーマンスと安定性を追加。
ESET Cluster	ESET Clusterでは単一の場所から複数のサーバーを管理できます。ワークステーションをノードに結合すると、すべてのクラスタメンバーで1つの構成ポリシーを配布できるため、管理がさらに自動化されます。クラスタ自体の作成は、インストールされたノードで実行できます。これはすべてのノードをリモートでインストールおよび開始できます。ESETサーバー製品によりESETサーバー製品はそれぞれ通信し、構成や通知などのデータを交換するだけでなく、製品インスタンスのグループ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。クラスタ全体で製品の構成は同じです。Windows Failover ClusterおよびNetwork Load Balancing (NLB) ClusterはESET Server Securityによってサポートされます。またESET Clusterメンバーを手動で追加できます。特定のWindows Clusterは必要ありません。ESET Clusterはドメインとワークグループ環境の両方で動作します。
自動除外	動作とパフォーマンスをスムーズにするために、重要なアプリケーションとサーバーファイルを自動的に検出して除外します。
除外を処理する	特定のプロセスをマルウェア対策のアクセス中の検査から除外します。マルウェア対策のアクセス中の検査では、バックアッププロセスや仮想マシンのライブ移行といった特定の状況で競合が発生する可能性があります。プロセス除外では、競合の可能性のリスクを最小化し、除外されたアプリケーションのパフォーマンスを改善します。このようにして、システムの全体的なパフォーマンスと安定性に好ましい効果を及ぼします。プロセス/アプリケーションの除外は、実行ファイル(.exe)の除外です。
eShell ESET Shell	eShell 2.0は、経験豊富なユーザーと管理者向けにESETサーバー製品を管理するための総合的なオプションを提供する、新しいコマンドラインインタフェースです。
ESET PROTECT	オンデマンド検査 をスケジュールする機能を含む、ESET PROTECTとの統合の強化。詳細についてはESET PROTECT オンラインヘルプ を参照してください。
コンポーネントベースのインストール	インストールをカスタマイズし、製品の選択したコンポーネントのみを含めることができます。

新機能

ESET Server Securityの新機能と機能強化:

- 真の64ビット製品コア
- [OneDrive検査](#)
- [ESET Dynamic Threat Defense \(EDTD\)](#)
- [ESET Enterprise Inspector](#) サポート
- [ESET RMM](#)
- [ネットワーク隔離](#)
- [機械学習による検出](#)
- [監査ログ](#)
- [マイクロプログラムコンポーネントのアップデート](#)

保護の種類

保護には、2種類あります。

- マルウェア対策保護
- スパイウェア対策保護

マルウェア対策の保護機能は、ESET Server Security製品の基本機能の1つです。この保護機能は、ファイル、電子メール、およびインターネット通信を検査することにより、悪意のあるシステム攻撃から保護します。脅威が検出されると、検出モジュールがブロックし、次に駆除・削除、または移動して隔離することにより、ウイルスを排除できます。

インストールの準備

製品インストールの準備のために、以下の手順が推奨されています。

- ESET Server Securityの購入後、[ESETのWebサイト](#)から.msiインストールパッケージをダウンロードします。
- ESET Server Securityをインストールするサーバーが[システム要件](#)を満たしていることを確認します。
- を管理者アカウントを使用してサーバーにログインします。

注意

ビルトイン管理者アカウントまたはドメイン管理者アカウント(ローカル管理者アカウントが無効な場合)でインストーラーを実行する必要があります。その他のユーザーには、管理者グループのメンバーでない限り、十分なアクセス権が与えられません。したがって、ビルトインの管理者アカウントを使用する必要があります。ローカルまたはドメイン管理者以外のユーザーアカウントでは、インストールを正常に完了することができません。

- ESET Server Securityの既存のインストールから[アップグレード](#)する場合は、[設定のエクスポート](#)機能を使用して現在の設定をバックアップすることをお勧めします。
- 該当する場合は、システムからサードパーティーのウイルス対策ソフトウェアを削除またはアンインストールします。[ESET AV Remover](#)を使用することをお勧めします。ESET AV Removerを使用して削除できる他社製のウイルス対策ソフトウェアの一覧については、この[KB記事](#)を参照してください。
- Windows Server 2016にESET Server Securityをインストールしている場合は、Microsoftは、Windows Defender機能を[アンインストール](#)し、Windows Defender ATP登録を解除して、複数のウイルス対策製品がコンピューターにインストールすることが原因で発生する問題を回避することを[推奨](#)しています。
- Windows Server 2019, Microsoft Windows Server 2022でESET Server Securityをインストールしている場合Microsoftは、Windows Defender機能を[パッシブモード](#)にして、複数のウイルス対策製品がコンピューターにインストールすることが原因で発生する問題を回避することを[推奨](#)しています。

ESET Server Securityインストーラーは次の2つのモードで実行できます。

- [グラフィカルユーザーインターフェイス\(GUI\)](#)

これは推奨されるインストールウィザードを使用したインストールの種類です。

- [サイレント / 無人インストール](#)

インストールウィザードの他に、コマンドラインからサイレントでESET Server Securityをインストールできます。

重要

可能であれば、新規にインストールして設定したOSにESET Server Securityをインストールするよう強くお勧めします。既存のシステムにインストールする必要がある場合は、以前のバージョンのESET Server Securityをアンインストールし、サーバーを再起動してから新しくESET Server Securityをインストールすることをお勧めします。

- [新しいバージョンへのアップグレード](#)

古いバージョンのESET Server Securityを使用している場合は、適切なアップグレード方法を選択できます。

ESET Server Securityを正常にインストールまたはアップグレードした後は、次の作業を実行します。

- [製品のアクティベーション](#)

[アクティベーション]ウィンドウ内の特定のアクティベーションシナリオを使用できるかどうかは、国、および配布方法によって異なります。

- [一般設定](#)

ESET Server Securityを微調整するには、ニーズに合わせて、各機能の詳細設定を修正します。

システム要件

サポートされるオペレーティングシステム:

- Microsoft Windows Server 2022 (Server Core and Desktop Experience)
- Microsoft Windows Server 2019 (Server Core and Desktop Experience)
- Microsoft Windows Server 2016 (Server Core and Desktop Experience)
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- [KB4474419](#) および [KB4490628](#) がインストールされているMicrosoft Windows Server 2008 R2 SP1 ([SHA-2必須の互換性](#)をお読みください)
- [Server Core \(Microsoft Windows Server 2008 R2 SP1, 2012, 2012 R2, 2016\)](#)

注意

Windows Server 2008 R2 SP1では、**ネットワーク保護**コンポーネントのインストールは既定で無効です(標準インストール)。カスタムインストールを使用して、このコンポーネントをインストールします。

Storage®Small BusinessおよびMultiPointサーバー

- Microsoft Windows Storage Server 2016
- Microsoft Windows Storage Server 2012 R2
- Microsoft Windows Storage Server 2012
- Microsoft Windows Server 2019 Essentials
- Microsoft Windows Server 2016 Essentials
- Microsoft Windows Server 2012 R2 Essentials
- Microsoft Windows Server 2012 Essentials
- Microsoft Windows Server 2012 Foundation

- [KB4474419](#) および [KB4490628](#) がインストールされている Microsoft Windows Small Business Server 2011 SP1 (x64)

- Microsoft Windows MultiPoint Server 2012
- Microsoft Windows MultiPoint Server 2011
- Microsoft Windows MultiPoint Server 2010

Hyper-Vロールでサポートされているホストオペレーティングシステム:

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- [Microsoft Windows Server 2008 R2 SP1](#) - 仮想マシンはオフライン中にのみ検査できます。

ハードウェア要件は、使用するオペレーティングシステムのバージョンによって異なります。ハードウェア要件の詳細については [Microsoft Windows Server](#) 製品のマニュアルを参照することをお勧めします。

注意

Microsoft Server オペレーティングシステムとサーバーアプリケーションの最新のサービスパックをインストールしてから ESET セキュリティ製品をインストールすることを強くお勧めします。また、最新の Windows アップデートとホットフィックスが利用可能なときには必ずインストールすることをお勧めします。

最低ハードウェア要件:

コンポーネント	要件
プロセッサ	Intel または AMD シングルコア x64
メモリー	256 MB の空きメモリー
ハードドライブ	700 MB の空きディスク領域
スクリーン解像度	800 x 600 ピクセル以上

SHA-2は互換性が必要

Microsoft は 2019 年前半に Secure Hash Algorithm 1 (SHA-1) の廃止予定を発表し、SHA-2 への移行を開始しました。このため SHA-1 アルゴリズムで署名されたすべての証明書は認識されなくなり、セキュリティアラートが表示されます。残念ながら、アルゴリズムに弱点が見つかり、プロセッサのパフォーマンスが向上し、クラウドコンピューティングが登場したため SHA-1 ハッシュアルゴリズムのセキュリティは時間の経過とともに安全性が低下しています。

そこで SHA-2 ハッシュアルゴリズム (SHA-1 の後継として) が SSL のセキュリティの持続性を保証する推奨される方法になりました。詳細については、[ハッシュと署名アルゴリズム](#) に関する Microsoft Docs の記事をご覧ください。

注意

この変更によりSHA-2をサポートしないオペレーティングシステムでは、ご使用のESETセキュリティソリューションが検出エンジンを含むモジュールを更新できなくなり、最終的にはESET Server Securityが完全に機能せず、十分な保護を提供できなくなります。

Microsoft Windows Server 2008 R2 SP1または**Microsoft Windows Small Business Server 2011 SP1**を実行している場合は、システムがSHA-2と互換性があることを確認してください。次のように特定のオペレーティングシステムのバージョンに従ってパッチを適用します。

- **Microsoft Windows Server 2008 R2 SP1** — [KB4474419](#) または [KB4490628](#) を適用します (追加のシステム再起動が必要になる場合があります)
- **Microsoft Windows Small Business Server 2011 SP1 (x64)** — [KB4474419](#) および [KB4490628](#) を適用します (追加のシステム再起動が必要になる場合があります)

重要

アップデートをインストールしてシステムを再起動したらESET Server SecurityのGUIを開いてステータスを確認します。ステータスがオレンジ色の場合は、もう一度システムを再起動します。ステータスが最大の保護を示す緑色になります。

注意

Microsoft Serverオペレーティングシステムとサーバーアプリケーションの最新のサービスパックをインストールすることを強くお勧めします。また、最新のWindowsアップデートとホットフィックスが利用可能なときには必ずインストールすることをお勧めします。

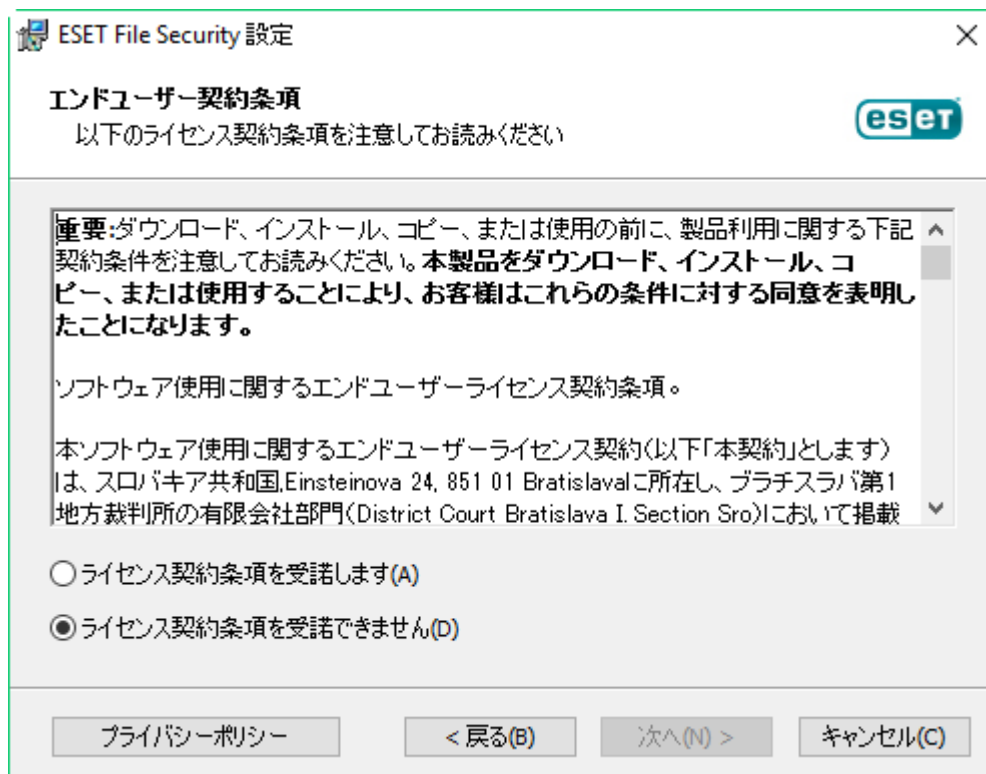
ESET Server Securityのインストール手順

これは、標準のGUIインストールウィザードです。.msiパッケージをダブルクリックし、手順に従ってESET Server Securityをインストールします。

1. **次へ**をクリックして続行するか、インストールを終了する場合は**キャンセル**をクリックします。
2. インストールウィザードは、オペレーティングシステムの**地域 > ロケーション**の**ホームロケーション**で指定される言語で実行されます (または古いシステムでは**地域と言語 > ロケーションの現在のロケーション**設定)。ドロップダウンメニューを使用してESET Server Securityがインストールされる**製品言語**を選択しますESET Server Security用に選択された言語は、インストールウィザードに表示される言語とは関係ありません。



3.次へをクリックすると、エンドユーザーライセンス契約が表示されます。エンドユーザー使用許諾契約(EULA)とプライバシーポリシーに同意したことを確認した後、次へをクリックします。

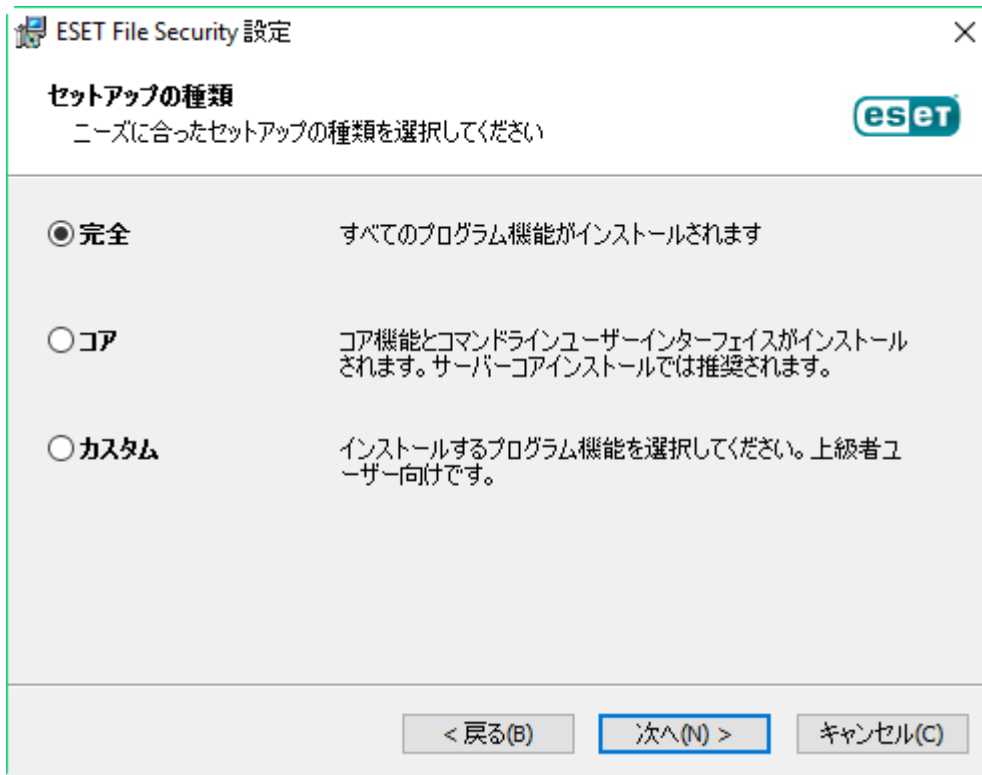


4.使用可能なインストールの種類からいずれかを選択します(選択できるインストールタイプは、オペレーティングシステムによって異なります)。

完了

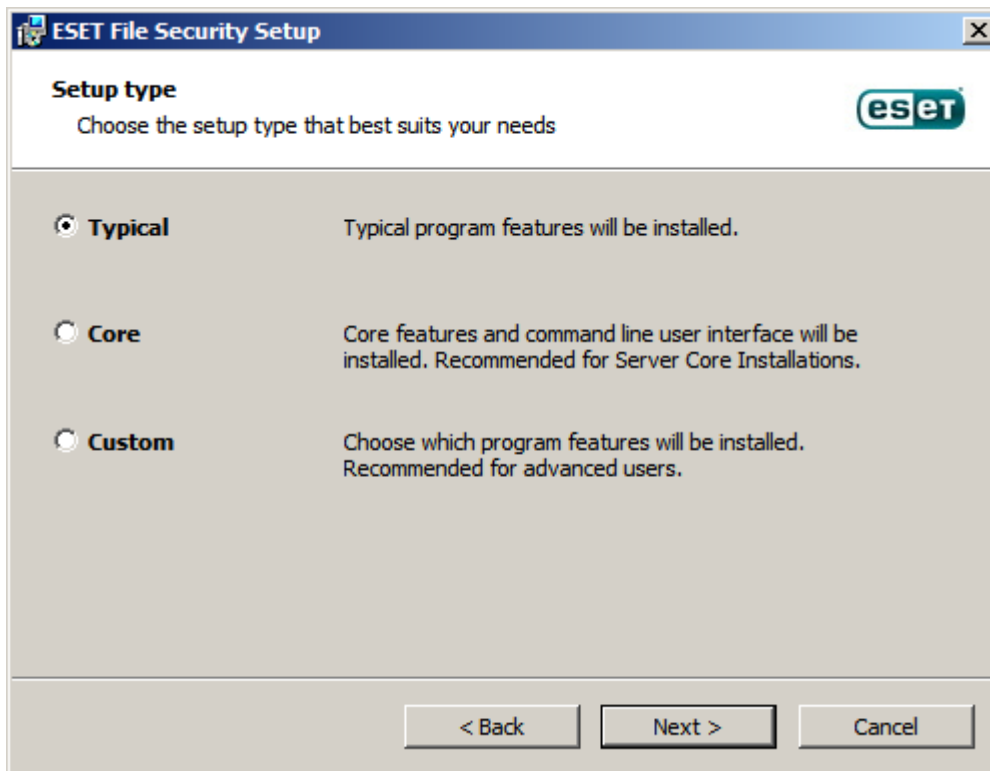
すべてのESET Server Security機能をインストールします。完全インストールとも呼ばれます。これは、推奨されるインストールの種類です。Windows Server 2012®2012 R2®2016®2019®Windows Server 2012

Essentials[®]2012 R2 Essentials[®]2016 Essentials[®]2019 Essentialsで使用できます。



標準

推奨ESET Server Security機能をインストールします。 [2008 R2 SP1](#) および2011で使用できます。



コア

このタイプのインストールは、Windows Server Coreエディション用です。インストール手順は、完全インストールと同じですが、コア機能とコマンドラインユーザーインターフェイスのみがインス

トールされます。コアインストールは主にWindows Server Coreのユーザー向けですが、任意で標準のWindows Serverにもインストールできます。コアインストールでインストールされるESETセキュリティ製品にはGUIがありません。これはESET Server Securityで作業しているときには、コマンドラインユーザーインターフェイスのみ使用できることを意味しています。詳細および他の特殊パラメーターについては、[コマンドラインインストール](#)セクションを参照してください。

例

コマンドライン経由でコアインストールを実行するには、次のサンプルコマンドを使用します。
msiexec /qn /i efsw_nt64.msi ADDLOCAL=_Base

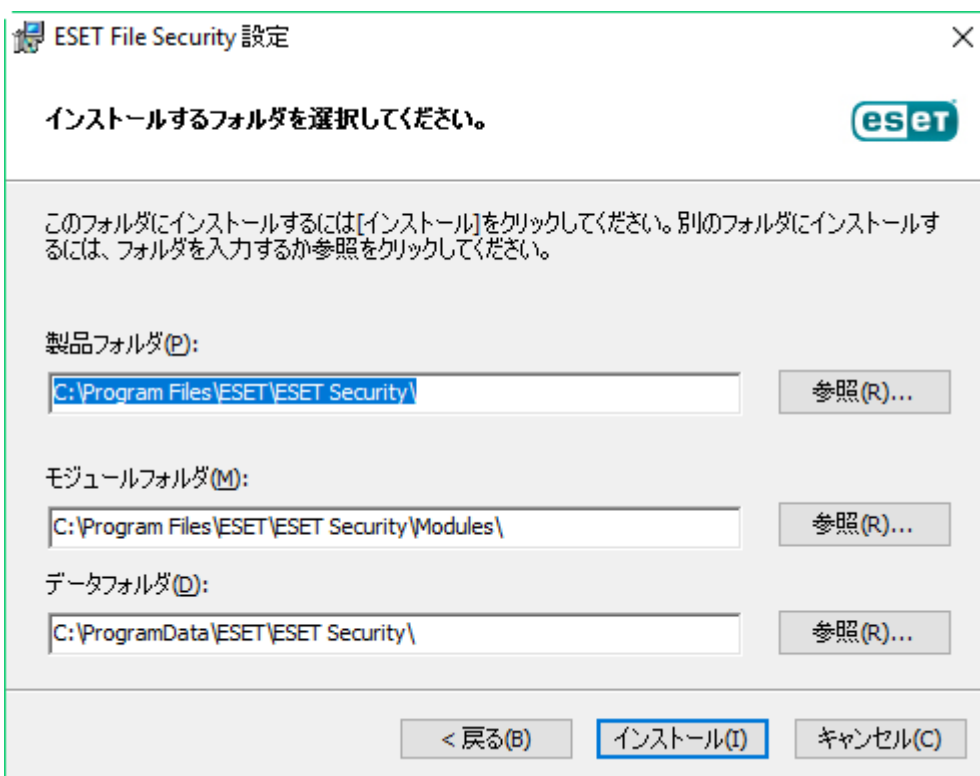
カスタム


システムにインストールされるESET Server Securityの機能を選択できます。インストールを開始する前に、製品モジュールおよび機能の一覧が表示されます。必要なコンポーネントのみを使用してESET Server Securityをカスタマイズするときには有効です。

注意

Windows Server 2008 R2 SP1では、**ネットワーク保護**コンポーネントのインストールは既定で無効です(標準インストール)。このコンポーネントをインストールする場合は、**カスタムインストール**の種類を選択します。

5.ESET Server Securityのインストール先を選択する必要があります。既定では、プログラムは、C:\Program Files\ESET\ESET Server Securityにインストールされます。**参照**をクリックすると、この場所が変更されます(非推奨)。



6.インストールをクリックすると、インストールが開始します。インストールが完了するとESET GUIが起動し、[トレイアイコン](#)が通知領域(システムトレイ)に表示されます。

既存のインストールの修正

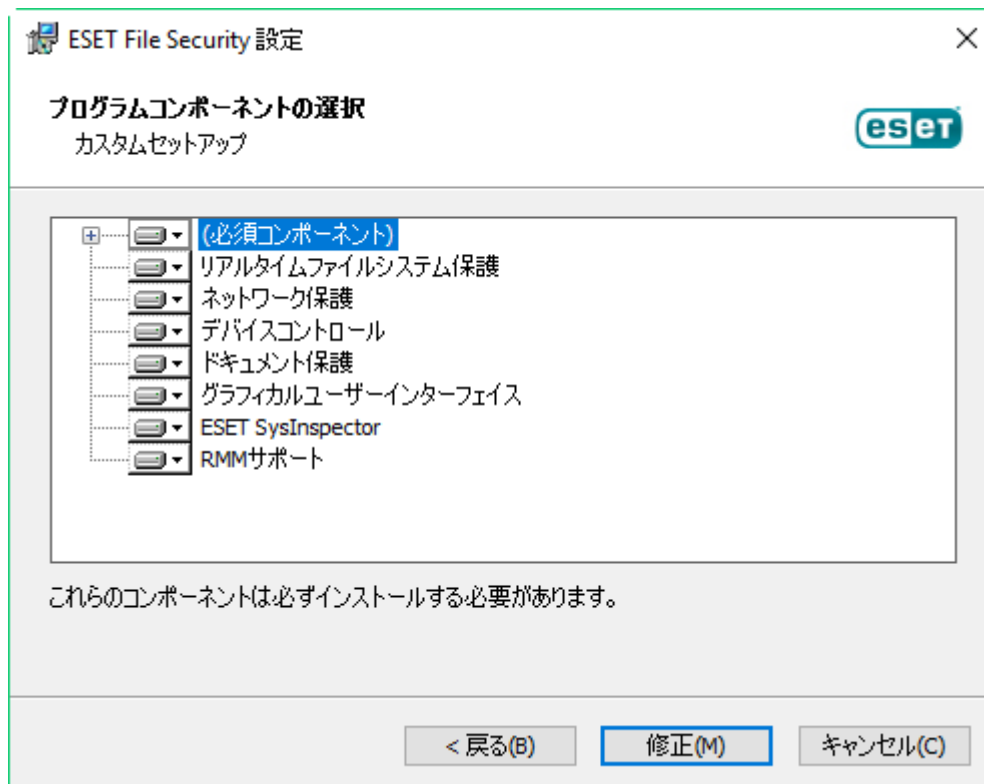
インストールされたコンポーネントを追加するか、削除できます。このためには、初期インストール中に使用した.msiインストーラパッケージを実行するか、[プログラムと機能] (Windowsコントロールパネルからアクセス可能) に移動します。ESET Server Security を右クリックし、**変更**を選択します。次の手順に従い、コンポーネントを追加または削除します。

3つのオプションがあります。インストールされているコンポーネントの**修正** ESET Server Securityのインストールの**修復**または完全に**削除** (アンインストール) ができます。



修正を選択した場合、利用可能なプログラムコンポーネントの一覧が表示されます。

追加または削除するコンポーネントを選択します。複数のコンポーネントの追加/削除を同時に行うことができます。コンポーネントをクリックして、ドロップダウンメニューからオプションを選択します。



オプションを選択したら、**[変更]**をクリックして、修正を実行します。

注意

インストーラを実行すると、インストール済みのコンポーネントをいつでも変更できます。ほとんどのコンポーネントで、変更を適用するためのサーバーの再起動は不要です。GUIが再起動し、インストールすることを選択したコンポーネントだけが表示されます。サーバーの再起動が必要なコンポーネントの場合、Windowsインストーラによって再起動するように指示されます。サーバーがもう一度オンラインになると、新しいコンポーネントが使用可能になります。

サイレント / 無人インストール

次のコマンドを実行し、コマンドライン経由でインストールを完了します。 `msiexec /i <packagename> /qn /l*xv msi.log`

注意

Windows Server 2008 R2 SP1では、**ネットワーク保護**機能がインストールされません。

インストールが成功したことを確認するため、またはインストールで問題が発生した場合には、Windows イベントビューアを使用して、**アプリケーションログ**を確認します(ソースからのレコードを検索: MsIInstaller)。

例

64ビットシステムでの完全インストール:

```
msiexec /i efsw_nt64.msi /qn /l*xv msi.log ADDLOCAL=NetworkProtection,RealtimeProtection,^
DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,SysInspector,SysRescue,Rmm,eula
```

インストールが完了すると、ESET GUIが起動し、**トレイアイコン**  が通知領域(システムトレイ)に表示されます。

例

指定された言語(ドイツ語)での製品のインストール:

```
msiexec /i efsw_nt64.msi /qn ADDLOCAL=NetworkProtection,RealtimeProtection,^
DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,^
SysInspector,SysRescue,Rmm,eula PRODUCT_LANG=1031 PRODUCT_LANG_CODE=de-de
```

詳細および言語コードの一覧については、[コマンドラインインストール](#)の言語パラメーターを参照してください。

重要

REINSTALLパラメーターの値を指定するときには、ADDLOCALまたはREMOVEパラメーターの値として使用されない残りの機能をリストする必要があります。コマンドラインインストールを正常に実行するには、REINSTALL、ADDLOCAL、およびREMOVEパラメーターの値としてすべての機能をリストする必要があります。REINSTALLパラメーターを使用しない場合は、追加または削除が失敗する場合があります。

機能の一覧については、[コマンドラインインストール](#)セクションを参照してください。

例

64ビットシステムからの完全削除(アンインストール):

```
msiexec /x efsw_nt64.msi /qn /l*xv msi.log
```

注意

アンインストールが成功すると、サーバーが自動的に再起動します。

コマンドラインインストール

次の設定は、ユーザーインターフェースの簡易、基本およびなしレベルで使用されるものです。該当するコマンドラインスイッチで使用されるmsiexecバージョンについては、[マニュアル](#)を参照してください。

サポートされているパラメータ:

APPDIR=<path>

- path - 有効なディレクトリパス
- アプリケーションインストールディレクトリ
- 例: efsw_nt64.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection

APPDATADIR=<path>

- path - 有効なディレクトリパス
- アプリケーションデータインストールディレクトリ

MODULEDIR=<path>

- path - 有効なディレクトリパス
- モジュールインストールディレクトリ

ADDLOCAL=<list>

- コンポーネントインストール - ローカルでインストールされる必須以外の機能のリスト。
- ESET .msiパッケージで使用: efsw_nt64.msi /qn ADDLOCAL=<list>

- ADDLOCALプロパティの詳細について

は、<https://docs.microsoft.com/en-gb/windows/desktop/Msi/addlocal> を参照してください。

- ADDLOCALリストは、インストールされるすべての機能のカンマ区切り値リストです。
- インストールする機能を選択するときには、完全パス(すべての親機能を含む)を明示的にリストに含める必要があります。

REMOVE=<list>

- コンポーネントインストール - ローカルインストールしない親 機能
- ESET .msiパッケージで使用: `efsw_nt64.msi /qn REMOVE=<list>`
- REMOVEプロパティの詳細について

は、<https://docs.microsoft.com/en-gb/windows/desktop/Msi/addlocal> を参照してください。

- REMOVEリストは、インストールされない(または既存のインストールの場合に削除される)親機能のカンマ区切りのリストです。
- 親機能のみを指定するだけで十分です。すべての子機能を明示的にリストに追加する必要はありません。

ADDEXCLUDE=<リスト>

- ADDEXCLUDEリストはインストールされないすべての機能名のカンマ区切り値リストです。
- インストールしない機能を選択するときには、パス全体(すべてのサブ機能を含む)と関連する非表示の機能を明示的にリストに含める必要があります。
- ESET .msiパッケージで使用: `efsw_nt64.msi /qn ADDEXCLUDE=<list>`

注意

ADDEXCLUDEはADDLOCALと併用できません。

機能の存在

- 必須 - 機能は常にインストールされます。
- 任意 - 機能のインストールを解除できます。
- 非表示 - 他の機能が正常に動作するために必要な論理機能。

ESET Server Security証明書のリスト

重要

すべての機能名は大文字と小文字を区別します。たとえば、RealtimeProtectionとREALTIMEPROTECTIONは同じではありません

機能名	機能の存在
SERVER	必須
RealtimeProtection	必須
WMIPProvider	必須
HIPS	必須
Updater	必須
eShell	必須
UpdateMirror	必須
DeviceControl	任意
DocumentProtection	任意

機能名	機能の存在
WebAndEmail	任意
ProtocolFiltering	非表示
NetworkProtection	任意
IdsAndBotnetProtection	任意
Rmm	任意
WebAccessProtection	任意
EmailClientProtection	任意
MailPlugins	非表示
Cluster	任意
_Base	必須
eula	必須
ShellExt	任意
_FeaturesCore	必須
GraphicUserInterface	任意
SysInspector	任意
SysRescue	任意
EnterpriseInspector	任意

次の機能のいずれかを削除する場合は、グループに属するすべての機能を指定して、グループ全体を削除する必要があります。そうしないと、この機能は削除されません。ここには2つのグループがあります（各行が1つのグループを表す）。

GraphicUserInterface, ShellExt

NetworkProtection, WebAccessProtection, IdsAndBotnetProtection, ProtocolFiltering, MailPlugins, EmailClientProtection

例

REMOVEパラメーターを使用し、親機能のみを指定して、**ネットワーク保護**セクション(子機能を含む)をインストールから除外します。

```
msiexec /i efsw_nt64.msi /qn ADDLOCAL=ALL REMOVE=NetworkProtection
```

あるいは、ADDEXCLUDEパラメーターを使用できますが、すべての子機能を指定する必要があります。

```
msiexec /i efsw_nt64.msi /qn ADDEXCLUDE=NetworkProtection,WebAccessProtection,IdsAndBotnetProtection,^ProtocolFiltering,MailPlugins,EmailClientProtection
```

例

コアインストールの例:

```
msiexec /qn /i efsw_nt64.msi /l*xv msi.log ADDLOCAL=RealtimeProtection,Rmm
```

インストール後にESET Server Securityを自動的に構成する場合は、インストールコマンド内の基本構成パラメーターを指定できます。

例

ESET Server Security をインストールし、ESET LiveGrid®を無効にする:

```
msiexec /qn /i efsw_nt64.msi ADDLOCAL=RealtimeProtection,Rmm,GraphicUserInterface CFG_LIVEGRID_ENABLED=0
```

すべての構成プロパティのリスト:

スイッチ	値
CFG_POTENTIALLYUNWANTED_ENABLED=1/0	0 - 無効、1 - 有効
CFG_LIVEGRID_ENABLED=1/0	0 - 無効、1 - 有効
FIRSTSCAN_ENABLE=1/0	0 - 無効、1 - 有効
CFG_PROXY_ENABLED=0/1	0 - 無効、1 - 有効
CFG_PROXY_ADDRESS=<ip>	プロキシIPアドレス。
CFG_PROXY_PORT=<port>	プロキシポート番号。
CFG_PROXY_USERNAME=<user>	認証用のユーザー名
CFG_PROXY_PASSWORD=<pass>	認証のパスワード

言語パラメーター：製品言語(両方のパラメーターを指定する必要があります)

スイッチ	値
PRODUCT_LANG=	LCID数値(ロケールID)例：1033 (<i>English - United States</i>) 言語コードの一覧 を参照してください。
PRODUCT_LANG_CODE=	小文字のLCID文字列(言語カルチャー名)。例：en-us (<i>English - United States</i>) 言語コードの一覧 を参照してください。

製品のアクティベーション

インストール完了後、製品のアクティベーションが求められます。




ESET Server Securityをアクティベーションするには、次の方法を使用できます。

ライセンスキーを入力

XXXX-XXXX-XXXX-XXXX-XXXXの形式の一意の文字列。ライセンス所有者を識別し、ライセンスをアクティベーションするために使用されます。


ESET Business Account

登録済みでESET Server Securityライセンスがインポートされた[ESET Business Account \(EBA\)](#) がある場合は、このオプションを使用します。[ESET License Administratorポータル](#) で使用するセキュリティ管理者資格情報も入力できます

オフラインライセンスファイル

自動生成されたファイルESET製品に転送され、ライセンス情報を提供します。オフラインライセンスファイルはライセンスポータルから生成され、アプリケーションがライセンス機関に接続できない環境で使用されます。

コンピューターが管理対象ネットワークのメンバーで、管理者が[ESET PROTECT](#)経由でリモートアクティベーションを実行する場合は、ESET PROTECTで[**後からアクティベーション**]をクリックします。後からこのクライアントをアクティベートする場合は、このオプションを使用することもできます。

メインプログラムウィンドウで[ヘルプとサポート]>[ライセンスの管理]を選択すると、いつでもライセンス情報を管理できますESETが製品を識別し、ライセンスを特定するために使用される公開ライセンスIDが表示されます。コンピュータが登録されるときに使用されるユーザー名は、システムトレイアイコン  を右クリックすると表示される[バージョン情報](#) セクションに保存されます。

ESET Server Securityのアクティベーションが成功したら、メインプログラムウィンドウが開き、[監視](#) ページに現在のステータスが表示されます。最初は何らかの注意が必要な場合があります。例えばESET LiveGrid®に参加するかどうかを確認する必要があります。

メインプログラムウィンドウには、システムアップデート(Windows Updates)や検出エンジンアップデートなどの他の項目に関する通知も表示されます。注意が必要なすべての項目が解決されると、監視ステータスが緑色になり、ステータス「**保護されています**」が表示されます。

また、メインメニューから製品をアクティベーションするには、[ヘルプとサポート]>[製品のアクティベーション]または[監視]ステータス > [製品がアクティベーションされていません]を選択します。

注意

ESET PROTECTは、管理者が使用可能にしたライセンスを使用してバックグラウンドでクライアントコンピュータをアクティベーションできます。

ESET Business Account

ESET Business Accountでは複数のライセンスを管理できますESET Business Accountがない場合は、**アカウントの作成**をクリックし、ESETBusinessAccountポータルに移動すると、登録処理を行うことができます。

注意

詳細については、[ESET Business Account \(EBA\)](#)  ユーザーガイドを参照してください。

セキュリティ管理者資格情報を使用して、パスワードを忘れた場合は、**パスワードを忘れた場合**をクリックするとESET License Administratorポータルに移動します。電子メールアドレスを入力し、**送信**をクリックして確認します。その後に、パスワードリセット手順が記載されたメッセージが送信されます。

アクティベーションは正常に実行されました

アクティベーションは正常に実行され、ESET Server Securityが有効になりました。これでESET Server Securityは定期アップデートを受信して、最新の脅威を特定し、コンピュータを安全に保ち続けることができます。製品のアクティベーションを完了するには、[完了]をクリックします。

アクティベーションに失敗しました

ESET Server Securityのアクティベーションが失敗しました。正しい製品認証キーを入力したか、オフラインライセンスを添付したことを確認してください。別のオフラインライセンスがある場合は、再入力してください。入力したライセンスキーを確認するには、ライセンスキーの再確認をクリックするか、別のライセンスを入力します。

アクティベーションできない場合は、[アクティベーショントラブルシューティングウィザード](#)を参照してください。

ライセンス

ESET Server Securityで使用するアカウントに関連付けられたライセンスを選択するように指示されます。続行をクリックすると、アクティベーションを続行します。

新しいバージョンへのアップグレード

プログラムモジュールの自動更新では解決できない問題の修正や改良を行うためにESET Server Securityの新バージョンが提供されています。

アップグレード方法:

- **アンインストール/インストール** - 新しいバージョンのインストールの前に古いバージョンを削除します。最新バージョンのESET Server Securityをダウンロードします。設定を保持する場合は、既存のESET Server Securityから[設定をエクスポート](#)します。ESET Server Securityをアンインストールして、サーバーを再起動します。ダウンロードしたインストーラーを使用して、[新規インストール](#)を実行します。[設定をインポート](#)し、設定を読み込みます。単一のサーバーでESET Server Securityを実行している場合は、この手順が推奨されます。
- **インプレース** - 既存のバージョンを削除せずに、新しいESET Server Securityを上書きインストールするアップグレード方法。

重要

サーバーに**保留中のWindows Updatesがないこと**と**Windows Updates**または他の理由による**保留中の再起動がない状態**でなければなりません。インプレースアップグレードを実行し、Windows Updatesまたは再起動が保留中である場合は、既存のバージョンのESET Server Securityが正常に削除されない可能性があります。また、後から手動で古いバージョンのESET Server Securityを削除すると、問題が発生します。

注意

ESET Server Securityのアップグレード中にはサーバーの再起動が必要です。

- **リモート** - ESET PROTECTを使用して管理される大規模ネットワーク環境。基本的にクリーンアップ

プグレードですが、リモートで実行されます。ESET Server Securityを実行する複数のサーバーがある場合に、この方法が有用です。

- [ESET Clusterウィザード](#) – アップグレード方法として使用できます。ESET Server Securityのサーバーが2台以上の場合に、この方法を推奨します。基本的にインプレースアップグレードですがESET Cluster経由で実行されます。アップグレードが完了すると、[ESET Cluster](#)を使用し続け、機能を利用できます。

注意

ESET Server Securityをアップグレードした時点で、すべての設定を確かめ、ニーズに合わせて正しく構成されていることを確認することをお勧めします。

ESET PROTECT経由でのアップグレード

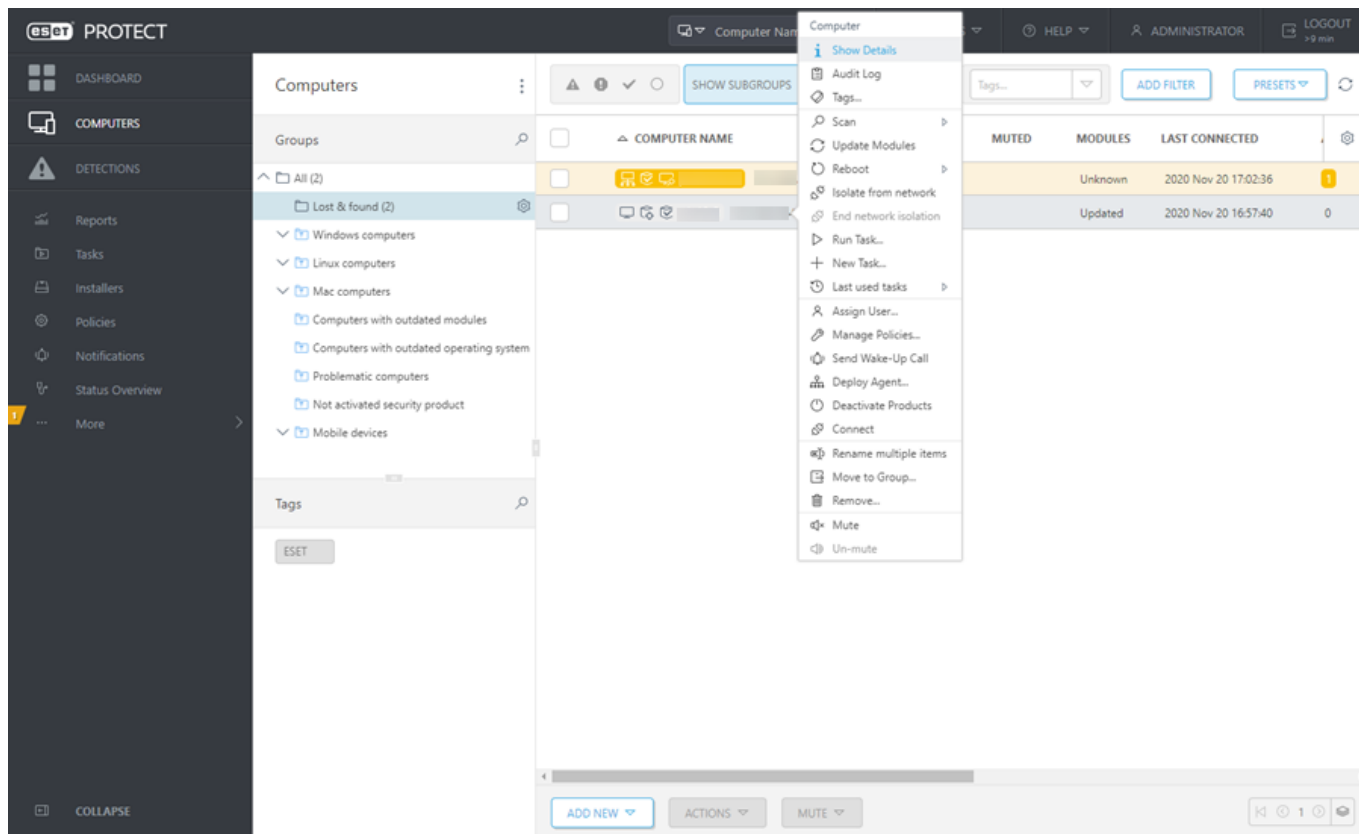
[ESET PROTECT](#)では、古いバージョンのESET Server Securityを実行している複数のサーバーをアップグレードできます。この方法には、各ESET Server Securityが同じ設定になっていることを確認(必要な場合)しながら、同時に多数のサーバーをアップグレードするという利点があります。

手順には次の段階があります。

- 最新バージョンのESET Server Securityを既存のバージョンの上にインストールし、手動で**最初のサーバーをアップグレード**すると、ルール、各種ホワイトリストおよびブラックリストを含む、すべての設定を保持できます。このフェーズは、ESET Server Securityを実行するサーバーでローカルで実行されます。
- 新しくバージョン7.xにアップグレードされたESET Server Securityの**設定を要求**し、ESET PROTECTで**ポリシーに変換**します。このポリシーは後からすべてのアップグレードされたサーバーに適用されます。このフェーズは、ESET PROTECTおよび次のフェーズを使用して、リモートで実行されます。
- 古いバージョンのESET Server Securityを実行するすべてのサーバーで**ソフトウェアのアンインストールタスクを実行**します。
- 最新バージョンのESET Server Securityを実行するすべてのサーバーで**ソフトウェアのアンインストールタスクを実行**します。
- 最新バージョンのESET Server Securityを実行するすべてのサーバーに**設定ポリシーを割り当て**ます。

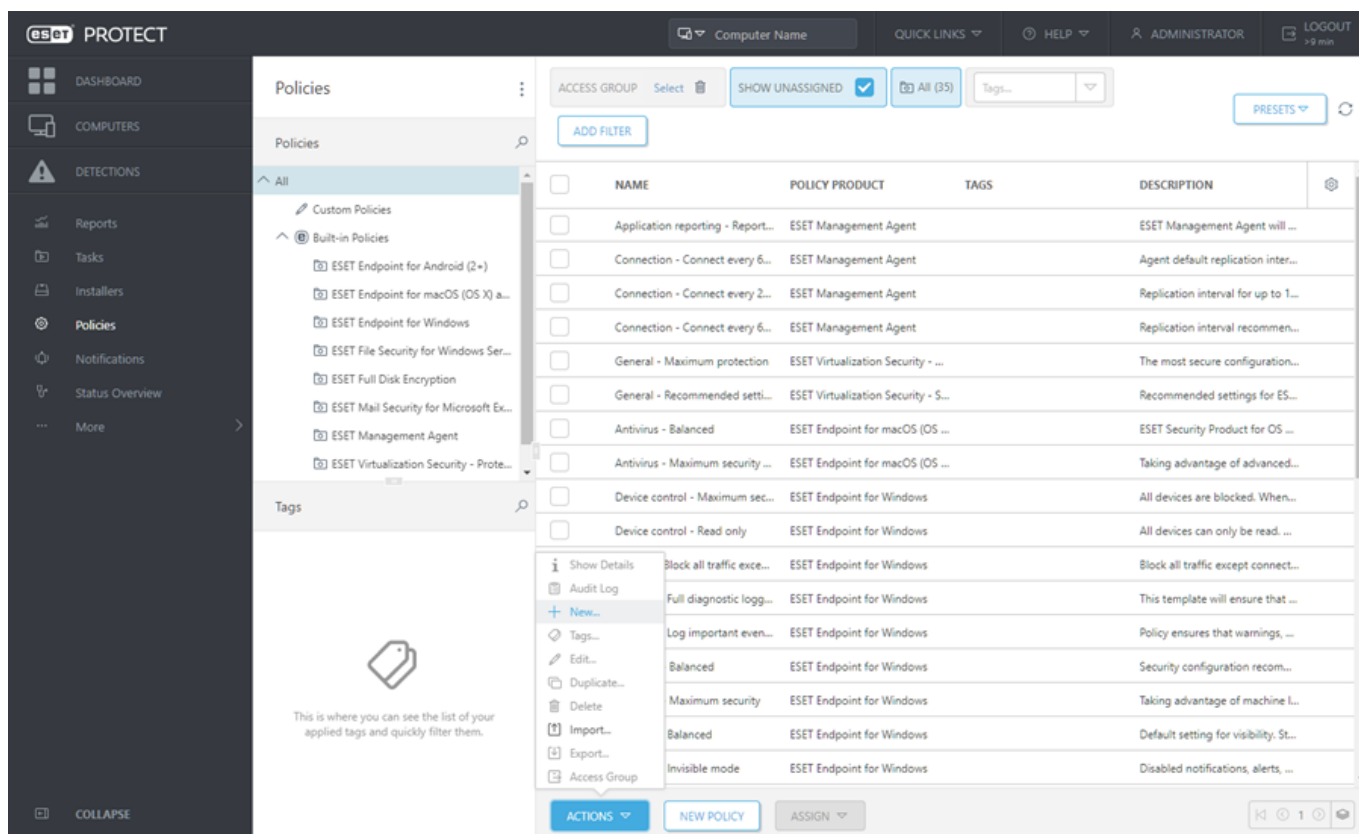
段階的な手順:

- 1.ESET Server Securityを実行するサーバーのいずれかにログオンし、最新バージョンをダウンロードして既存のバージョンの上にインストールして、アップグレードします。[標準のインストール手順](#)に従います。古いESET Server Securityのすべての元の設定は、インストール中に保持されます。
- 2.ESET PROTECT Web Consoleを開き、静的または動的グループからクライアントコンピューターを選択し、**詳細の表示**を選択します。



3. **設定** タブに移動し、**[設定の要求]** ボタンをクリックして、管理されている製品のすべての設定を収集します。設定を取得するには、少し時間がかかります。最新の設定が一覧に表示されたら、**[セキュリティ製品]** をクリックし、**[設定を開く]** を選択します。

4. **[ポリシーに変換]** ボタンをクリックして、設定ポリシーを作成します。新しいポリシーの**名前**を入力し、**[完了]** をクリックします。



5. クライアントタスクを選択し、[ソフトウェアのアンインストール](#)タスクを選択します。アンインストールタスクを作成するときには、[必要な場合には自動的に再起動する]チェックボックスをオンにし、アンインストール後にサーバーを再起動することをお勧めします。タスクが作成されたら、アンインストールするすべての任意の対象コンピューターを追加します。
6. すべての対象からESET Server Securityがアンインストールされたことを確認します。
7. [ソフトウェアのインストール](#)タスクを作成し、最新バージョンのESET Server Securityをすべての任意の対象にインストールします。
8. ESET Server Securityを実行するすべてのサーバー(理想的にはグループ)に**設定ポリシー**を割り当てます。

ESET Cluster経由でのアップグレード

[ESET Cluster](#)を作成すると、古いバージョンのESET Server Securityを実行する複数のサーバーをアップグレードできます。[ESET PROTECTアップグレード](#)の代替策です。環境内にESET Server Securityがあるサーバーが2つ以上ある場合ESET Clusterを使用することをお勧めします。このアップグレードのもう一つの利点は、[ESET Cluster](#)を使用し続け、ESET Server Security設定をすべてのメンバーノードと同期できることです。

次の手順に従い、この方法でアップグレードします。

1. ESET Server Securityを実行するサーバーのいずれかにログオンし、最新バージョンをダウンロードして既存のバージョンの上にインストールして、アップグレードします。[標準のインストール手順](#)に従います。古いESET Server Securityのすべての元の設定は、インストール中に保持されます。
2. [ESET Clusterウィザード](#)を実行し、クラスターノード(ESET Server Securityをアップグレードするサーバー)を追加します。必要に応じて、まだESET Server Securityを実行していない他のサーバーを追加できます(インストールが実行されます)。[クラスター名とインストールの種類](#)を指定する際には、既定の設定を使用することをお勧めします(必ず[製品をアクティベーションせずにライセンスをノードにプッシュする]をオンにします)。
3. [ノードチェックログ]画面を確認します。古い製品バージョンを含み、製品が再インストールされるサーバーが一覧表示されますESET Server Securityは、現在インストールされていない追加されたサーバーにもインストールされます。



Node check log

[13:39:36] Node check started
[13:39:36] PING test:
[13:39:36] OK
[13:39:36] Administration share access test:
[13:39:36] OK
[13:39:36] Service manager access test:
[13:39:39] OK
[13:39:39] Checking installed product version and features:
[13:39:42] -2003-SHAREPOINT_2: Older version of the product detected. Product will be reinstalled.
[13:39:43] -2003-CLEAN: Install will be performed.
[13:39:45] OK
[13:39:45]
[13:39:45] Warning: The product needs to be reinstalled on some machines before creating the cluster. This may cause those machines to be automatically restarted.

Check

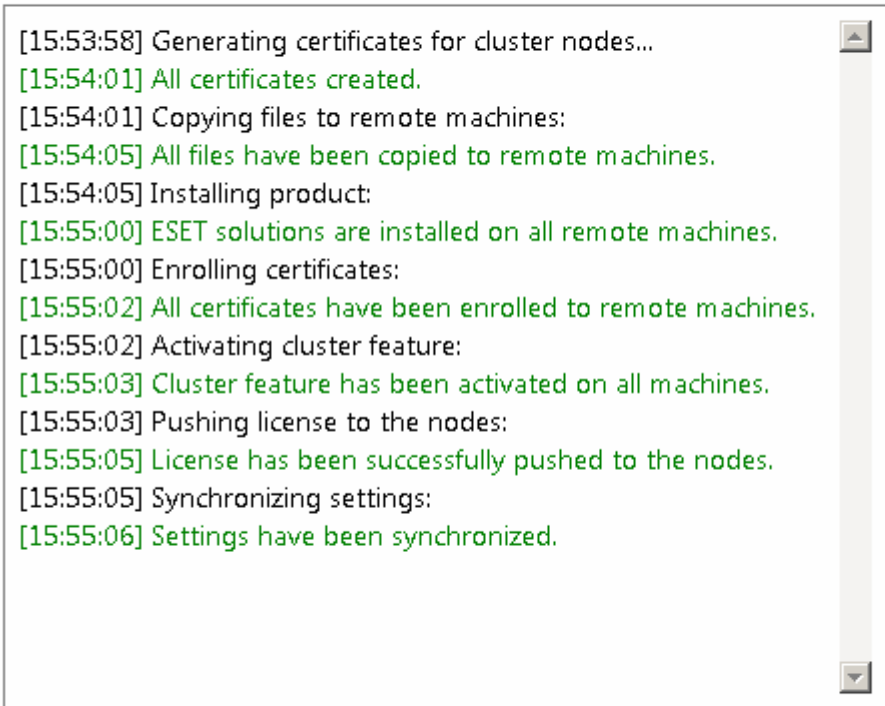
< Previous

Next >

Cancel

4. [ノードインストールとクラスターアクティベーション] 画面にはインストールの進行状況が表示されます。インストールが正常に完了すると、次のような結果で終了します。

Product install log



[15:53:58] Generating certificates for cluster nodes...
[15:54:01] All certificates created.
[15:54:01] Copying files to remote machines:
[15:54:05] All files have been copied to remote machines.
[15:54:05] Installing product:
[15:55:00] ESET solutions are installed on all remote machines.
[15:55:00] Enrolling certificates:
[15:55:02] All certificates have been enrolled to remote machines.
[15:55:02] Activating cluster feature:
[15:55:03] Cluster feature has been activated on all machines.
[15:55:03] Pushing license to the nodes:
[15:55:05] License has been successfully pushed to the nodes.
[15:55:05] Synchronizing settings:
[15:55:06] Settings have been synchronized.

Install

< Previous

Finish

Cancel

ネットワークまたはDNSが正しく設定されていない場合、サーバーからアクティベーショントークンを取得できませんでしたというエラーメッセージが表示されることがあります。[ESET Clusterウィザード](#)をもう一度実行してください。クラスターが破壊され、新しく作成されます(製品は再インストールされません)。アクティベーションはこの時点で正常に完了します。問題が解決しない場合は、ネットワークとDNS設定を確認してください。



Product install log

```
[18:06:59] Generating certificates for cluster nodes...
[18:07:01] All certificates created.
[18:07:01] Copying files to remote machines:
[18:07:01] All files have been copied to remote machines.
[18:07:01] Enrolling certificates:
[18:07:03] All certificates have been enrolled to remote machines.
[18:07:03] Activating cluster feature:
[18:07:04] Cluster feature has been activated on all machines.
[18:07:04] Pushing license to the nodes:
[18:07:04] Failed to obtain activation token from the server.
[18:07:04] There were errors pushing license to the nodes.
[18:07:04] Synchronizing settings:
[18:07:05] There were errors synchronizing settings in the cluster.
```

Install

< Previous

Finish

Cancel

クラスター環境でのインストール

クラスター環境でESET Server Securityを展開できます(フェールオーバークラスターなど)。アクティブなノードでESET Server Securityをインストールし、ESET Server Securityの[ESET Cluster](#)機能を使用して、パッシブノードにインストールを再配布することをお勧めします。インストールとは別に、ESET ClusterはESET Server Security構成のレプリケーションとして機能し、正常な動作に必要なクラスターノード間での整合性を保証します。

ターミナルサーバ

ターミナルサーバとして動作するWindows ServerにESET Server Securityをインストールしている場合に、ユーザーのログインのたびにESET Server SecurityのGUIが起動しないようにすることができます。GUIを無効にする具体的な手順については、[ターミナルサーバでのGUIの無効化](#)を参照してください。

セキュリティと安定性のアップデート

悪意のあるコードに対する完全な保護を維持するための基本的な作業としてESET Server Securityのアップデートが必要です。各新しいバージョンのESET Server Securityには、多数の改良やバグ修正が導入されています。ESET Server Securityを定期的にアップデートして、セキュリティの脆弱性や脅威を防止することを強くお勧めします。ESET Server Securityは、他のESET製品のように製品ライフサイクルの特定の段階

に適合します。[サポート終了ポリシー\(ビジネス製品\)](#) の詳細をお読みください。

ESET Server Securityの変更の詳細については、次の[ESETナレッジベース記事](#)をお読みください。

重要

自動アップデートは、製品の最大限のセキュリティと安定性を保証します。セキュリティアップデートと安定性アップデートを無効にすることはできません。

はじめに

次の部分ではESET Server Securityの基本について説明します。

監視

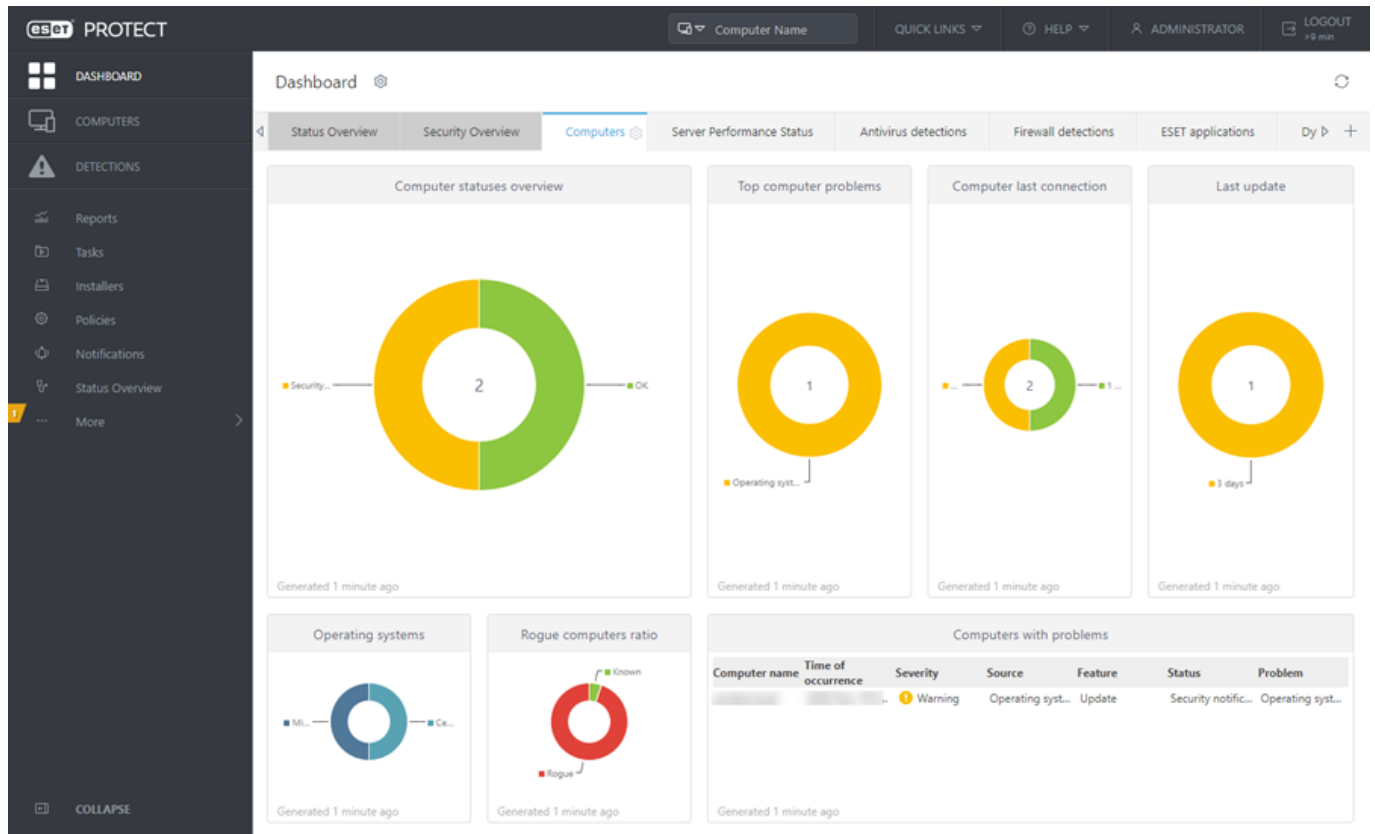
ESET Server Securityの現在のステータスの即時概要を表示します。注意が必要な問題があるかどうかを一目で確認できます。

ESET PROTECTを使用した管理

ESET PROTECTを使用するとESET Server Securityをリモートで管理できます。

ESET PROTECTを使用した管理

ESET PROTECTは、1つの中央の場所からネットワーク環境にあるESET製品を管理できるアプリケーションです。ESET PROTECTタスク管理システムではESETセキュリティソリューションをリモートコンピューターでインストールし、新たな問題や脅威に迅速に対応することができます。ESET PROTECTでは、悪意のあるコードに対しての保護は提供せず、各クライアントのESETセキュリティソリューションに依存しています。ESETセキュリティソリューションは、複数のタイプのプラットフォームを含むネットワークをサポートします。ネットワークには、現在のMicrosoft LinuxおよびMac OSモバイルオペレーティングシステムを含めることができます。



ESET PROTECTの詳細については、[ESET PROTECTオンラインヘルプ](#)を参照してください。

監視

監視セクションに表示される保護の状態は、コンピューターの現在の保護レベルを示します。プライマリウィンドウには ESET Server Security モジュールの動作状態の概要が表示されます。

✓ 緑の保護されています状態は、最も高い保護の状態が確保されていることを示します。

⚠ 赤いアイコンは保護に重大な問題があることを示しています。つまり、コンピュータにはリスクがあります。保護の状態の一覧については、[状態](#)セクションを参照してください。

⚠ オレンジのアイコンは、緊急ではない問題に関する注意が必要であることを示します。

正しく動作するモジュールには緑色のチェックマークが付きます。完全に機能していないモジュールには赤色の感嘆符またはオレンジ色の通知アイコンが表示されます。モジュールに関する追加情報がウィンドウの上部に表示されます。モジュールを修正するための推奨される解決策も表示されます。各モジュールのステータスを変更するには、メインメニューの[\[設定\]](#)をクリックし、必要なモジュールをクリックします。


[監視]ページには、次のようなシステム情報も表示されます。

- **製品バージョン** - ESET Server Securityのバージョン番号。
- **サーバー名** - コンピューターホスト名またはFQDN
- **システム** - オペレーティングシステム詳細。
- **コンピュータ** - ハードウェア詳細。
- **サーバー起動時間** - システムが起動および実行中の時間を示します。基本的にはダウンタイムの反対です。



提示された解決策を使用して問題を解決できない場合は、[\[ヘルプとサポート\]](#)をクリックしてヘルプにアクセスするか、あるいは[ESETナレッジベース](#)を検索してください。ヘルプが必要な場合は、[サポート依頼](#)を送信できます。いただいたご質問にはESETテクニカルサポートが迅速に対応し、解決のお手伝いをいたします。

状態

ESET Server Securityの状態概要には、システムに関する詳細情報がメインウィンドウに表示されます。通常、すべてが問題なく機能しているときには、保護の状態が 緑色です。ただし、保護の状態は特定の状況において変わる可能性があります。次のいずれかが発生する場合、保護の状態が オレンジま

たは  赤に変わり、警告メッセージが表示されます。

警告メッセージ	警告メッセージ詳細
不審なアプリケーションの検出が設定されていません 	望ましくない可能性があるアプリケーション(PUA)は、アドウェアを含んだり、ツールバーをインストールしたり、その他の不明確なオブジェクトを含んだりするプログラムです。望ましくない可能性があるアプリケーションの利点がリスクを上回るとユーザーが感じる場合もあります。
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	リアルタイム保護を有効にする を監視タブで有効にするか、リアルタイムファイルシステム保護をメインプログラムウィンドウの 設定 タブで再有効化します。
フィッシング対策機能が機能していません	他の必要なプログラムモジュールがアクティブではないため、この機能は機能していません。
ESET LiveGrid®が無効です	詳細設定で ESET LiveGrid® が無効なときに、この問題が表示されます。
プロトコルフィルタリングが無効です	プロトコルフィルタリングを有効にする をクリックして、この機能を再有効化します。
オペレーティングシステムは最新ではありません	システムアップデートウィンドウには、ダウンロードおよびインストールが可能なアップデートのリストが表示されます。
まもなくデバイスは保護されなくなります	Microsoft Windowsのバージョンを更新する方法の詳細については、 オプションを表示 をクリックします。Microsoft Windows Server 2008 R2 SP1またはMicrosoft Windows Small Business Server 2011 SP1を実行している場合は、システムがSHA-2と互換性があることを確認してください。特定のオペレーティングシステムのバージョンに従ってパッチを適用します。
プレゼンテーションモードは有効です	ポップアップウィンドウはすべて表示されなくなり、スケジュールされたタスクは一時停止します。
ネットワーク攻撃保護(IDS)が一時停止しています	ネットワーク攻撃保護(IDS)を有効にする をクリックして、この機能を再有効化します。
ボットネット保護が一時停止しています	ボットネット保護を有効にする をクリックして、この機能を再有効化します。
Webアクセス保護が一時停止しています	Webアクセス保護を有効にする を監視タブで有効にするか、Webアクセス保護をメインプログラムウィンドウの 設定 ペインで再有効化します。
デバイスコントロールが一時停止しています	デバイスコントロールを有効にする をクリックして、この機能を再有効化します。
製品がアクティブーションされていないか、ライセンスが期限切れです	これは保護の状態が赤に変わったアイコンで示されます。ライセンスの期限が過ぎたら、このプログラムはアップデートできません。ライセンスをアップデートするには、警告ウィンドウの指示に従ってください。
ポリシーの上書きが有効です	おそらくトラブルシューティングが完了するまで、ポリシーによる設定は一時的に上書きされます。ESET PROTECTを使用してESET Server Securityを管理し、 ポリシー  が割り当てられている場合は、ポリシーに属する機能によっては、ステータスリンクがロック(灰色表示)されます。
コンピューターを再起動する必要があります	このメッセージは、プログラムコンポーネントのアップデート(PCU)およびマイクロプログラムコンポーネントのアップデート(μPCU)が適用された後に表示される場合があります。PCU およびμPCUの詳細については、 アップデート設定 を参照してください。

提示された解決策を使用して問題を解決できない場合は、[ESETナレッジベース](#) を検索してください。ヘルプが必要な場合は、[サポート依頼](#) を送信できます。いただいたご質問にはESETテクニカルサポートが迅速に対応し、解決のお手伝いをいたします。

Windows Updateが利用可能です

[システムのアップデート]ウィンドウには、ダウンロードおよびインストールが可能なアップデートのリストが表示されます。アップデートの優先レベルは、アップデートの名前の横に表示されます。アップデート行を右クリックして、**詳細**をクリックすると、詳細情報のポップアップウィンドウが表示されます。

System updates

Total number of available updates: 7

Name	Type
2019-02 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB4487000)	Critical
2018-12 Cumulative Security Update for Internet Explorer 11 for Windows Server 2012 R2 for x64-based systems (KB4...	Important
Update for Microsoft Silverlight (KB4481252)	Important
Windows Malicious Software Removal Tool x64 - February 2019 (KB890830)	Important
2019-02 Security and Quality Rollup for .NET Framework 3.5, 4.5.2, 4.6, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.2 for Windows 8.1 a...	Important
Update for Windows Server 2012 R2 (KB4033428)	Recommended
Microsoft .NET Framework 4.7.2 for Windows Server 2012 R2 for x64 (KB4054566)	Recommended

Run system update

Cancel

システムアップデートの実行をクリックすると、**WindowsUpdate**ウィンドウが開き、システムアップデートが続行されます。

ネットワーク隔離

ESET Server Securityはネットワーク隔離というサーバーのネットワーク接続をブロックするオプションを提供します。一部の極端なシナリオでは、予防策としてサーバーをネットワークから分離したい場合があります。たとえば、サーバーがマルウェアに感染しているか、またはコンピューターが侵害されている場合などです。

ネットワークの分離を有効化すると、次を除くすべてのネットワークトラフィックがブロックされます。

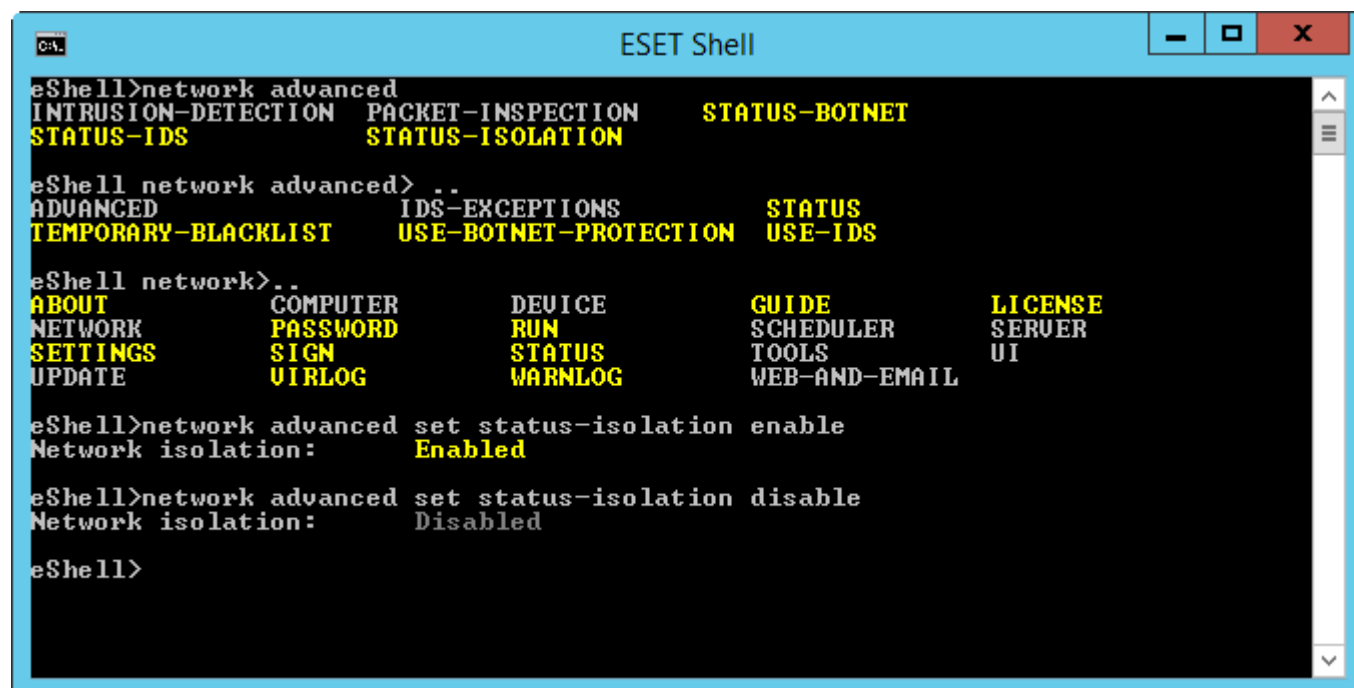
- ドメインコントローラーへの接続は維持されます
- ESET Server Securityはまだ通信が可能です
- ESET Management AgentとESET Enterprise Inspectorエージェントはネットワーク経由で通信できます (存在する場合)

ネットワークの分離を有効化または無効化するには、[eShell](#) コマンドまたは [ESET PROTECT](#) クライアントタスクを使用します。

eShell

対話モード:

- ネットワーク分離を有効にする: `network advanced set status-isolation enable`
- ネットワーク分離を無効にする: `network advanced set status-isolation disable`



```
eShell>network advanced
INTRUSION-DETECTION  PACKET-INSPECTION  STATUS-BOTNET
STATUS-IDS           STATUS-ISOLATION

eShell network advanced> ..
ADVANCED             IDS-EXCEPTIONS      STATUS
TEMPORARY-BLACKLIST  USE-BOTNET-PROTECTION  USE-IDS

eShell network>..
ABOUT              COMPUTER      DEVICE          GUIDE           LICENSE
NETWORK            PASSWORD     RUN             SCHEDULER       SERVER
SETTINGS           SIGN        STATUS          TOOLS           UI
UPDATE             VIRLOG      WARNLOG         WEB-AND-EMAIL

eShell>network advanced set status-isolation enable
Network isolation:    Enabled

eShell>network advanced set status-isolation disable
Network isolation:    Disabled

eShell>
```

または、[バッチ/スクリプトモード](#)を使用してバッチファイルを作成して実行することもできます。

ESET PROTECT

- [クライアントタスク](#)を使用してネットワーク分離を有効にします。
- [クライアントタスク](#)を使用してネットワーク分離を無効にします。

ネットワーク分離が有効化されるとESET Server Securityの状態が赤に変わり、ネットワークアクセスがブロックされましたというメッセージが表示されます。

コマンドと ESET Server Security

この部分では、プログラムのユーザーインターフェイスを詳細に説明し、ESET Server Securityの使用方法を説明します。

ユーザーインターフェイスでは、一般的に使用される機能にすばやくアクセスできます。

- [監視](#)
- [ログファイル](#)
- [検査](#)
- [アップデート](#)
- [設定](#)

検査

オンデマンドスキャナはESET Server Securityの重要な部分です。コンピュータ上のファイルやフォルダのスキャンを実行するために使用されます。ネットワークセキュリティを保証するには、感染が疑われるときだけコンピュータのスキャンを実行するのではなく、通常のセキュリティ手段の一環として定期的に実行することが重要です。システムの詳細検査を定期的に行う(1か月に1回など)し、[リアルタイムファイルシステム保護](#)で検出されないウイルスを検出することをお勧めします。これは、リアルタイムファイルシステム保護が無効なときに脅威が侵入した場合、検出エンジンがアップデートされていない場合、または最初にディスクに保存されたときにファイルが検出されなかった場合に発生する可能性があります。

ESET Server Securityで使用可能なオンデマンド検査を選択します。

ストレージ検査

ローカルサーバー上のすべての共有フォルダを検査します。ストレージ検査が利用できない場合、サーバー上に共有フォルダがないことを意味しています。

コンピュータの検査

コンピュータの検査をすぐに開始して、ユーザーが操作しなくても感染しているファイルからウイルスを駆除できます。コンピュータ検査の利点は、操作が簡単で、詳細な検査設定を必要としないことにあります。検査では、ローカルドライブにあるすべてのファイルが検査されます。検出されたマルウェアがあれば、自動的に駆除または削除されます。駆除のレベルは自動的に既定値に設定されます。駆除の種類の詳細については、「[駆除](#)」を参照してください。

注意

コンピュータの検査を最低でも月に1回は実行することをお勧めします。検査を[スケジュールされたタスク](#)として設定できます。

カスタム検査

カスタム検査は、スキャン対象やスキャン方法などのスキャンパラメーターを自分で指定したい場合に最適なソリューションです。カスタム検査の利点は、検査パラメーターを詳細に設定できることです。設定はユーザー定義の検査プロファイルに保存できます。これは、同じパラメータで検査を繰り返し実行する場合に便利です。

リムーバブルメディア検査

スマート検査と同じように、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。これはUSBフラッシュドライブをコンピュータに接続し、マルウェアや他の潜在的な脅威についてそのコンテンツを検査する場合に便利です。この検査は、[[カスタム検査](#)]をクリックし、[[検査の対象](#)]ドロップダウンメニューから[[リムーバブルメディア](#)]を選択して、[[検査](#)]をクリックして開始することもできます。

Hyper-V検査

このオプションは、ESET Server Securityを実行するサーバーにHyper-V Managerがインストールされている場合にメニューに表示されます。Hyper-V検査では、[Microsoft Hyper-V Server](#)上の仮想マシン(VM)ディスクを検査できます。特定のVMにエージェントをインストールする必要はありません。

OneDrive検査

OneDriveクラウドストレージにあるユーザーのファイルを検査できます。

前回検査の繰り返し

正確に同じ設定を使用し、前回の検査処理を繰り返します。

注意

オンデマンドデータベース検査が存在する場合は、前回の検査を繰り返し機能は使用できません。



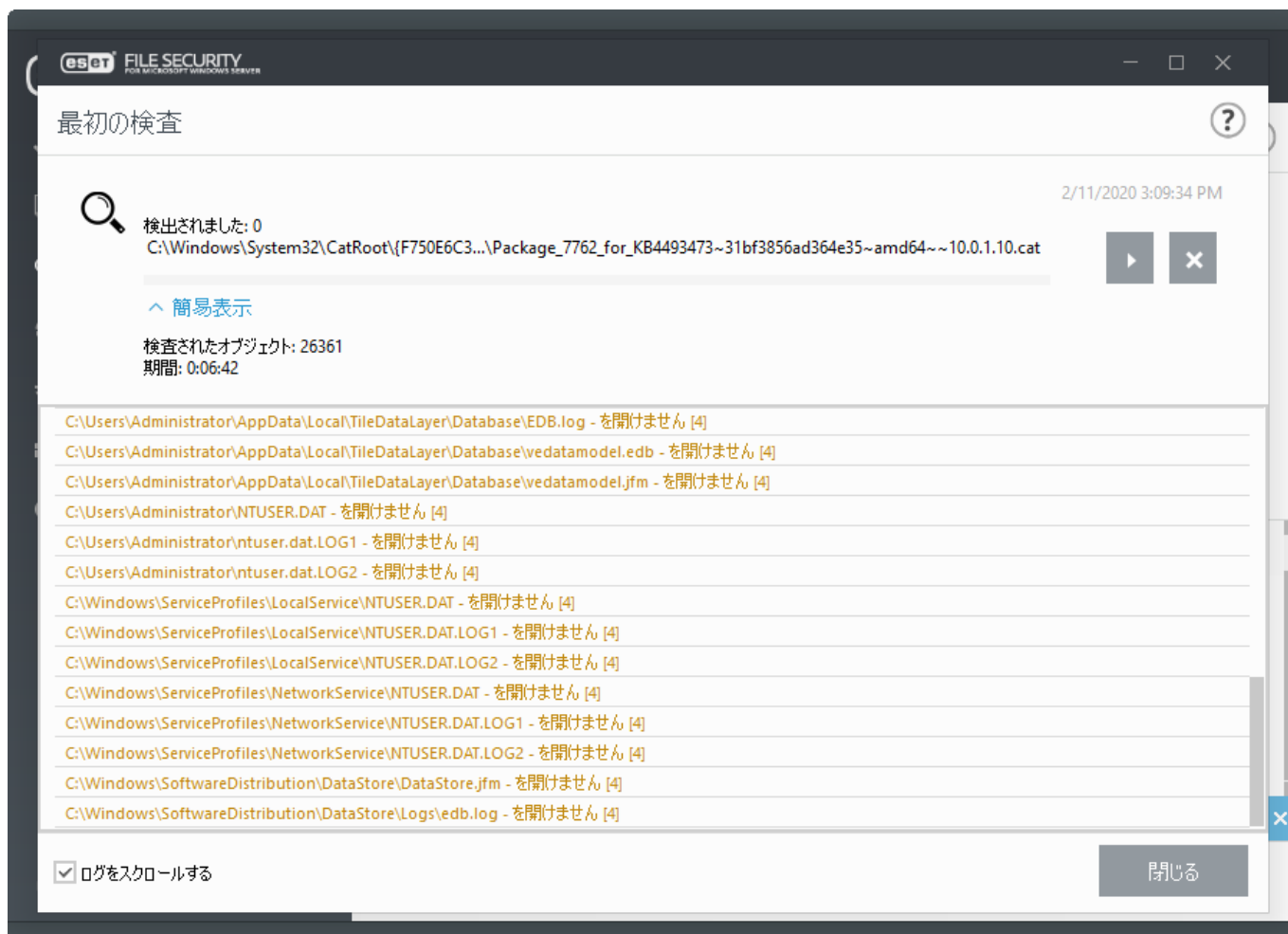
オプションを使用して、検査ステータスに関する詳細を表示します。

ファイルのドラッグアンドドロップ	ファイルをESET Server Security検査ウィンドウにドラッグアンドドロップすることもできます。これらのファイルはすぐにウイルス検査されます。
消去/すべて消去	指定されたメッセージを消去します。
検査ステータス	初期検査のステータスを示します。このスキャンは完了したか、ユーザーによって中断されました。
ログを表示する	詳細情報を表示します。
詳細	検査実行中に、検査を実行したユーザー、さまざまな検査されたオブジェクト、検査時間などの詳細を表示できます。
検査ウィンドウを開く	検査の進行状況ウィンドウには、検査の現状および悪意のあるコードが含むファイルの数に関する情報が表示されます。

検査ウィンドウと検査ログ

検査ウィンドウは、場所、見つかった脅威数(該当する場合)、検査済みオブジェクト数、検査時間を含む、現在検査されているオブジェクトを示します。ウィンドウの下部は検査ログであり、検出エンジンのバージョン番号、検査が開始した日時、対象選択が表示されます。

検査中のときに、検査を一時的に中断する場合は、**一時停止**をクリックします。**再開**オプションは、検査が一時停止しているときに使用できます。



検査ログをスクロールする


古いログを自動スクロールし、アクティブなログを[ログファイル]ウィンドウで表示する場合は、このオプションをオンにしておきます。

注意

パスワード保護されたファイルやシステム専用ファイル(一般的な例としては、*pagefile.sys*や特定のログファイル)など一部のファイルは、検査できなくても正常です。

検査が完了した後、特定の検査に関連するすべての関連する情報の検査ログが表示されます。



スイッチアイコン  **フィルタリング** をクリックし、[ログフィルタリング](#) ウィンドウを開きます。フィルタリングまたは検索条件を定義できます。コンテキストメニューを表示するには、特定のログエントリを右クリックします。

アクション	使用方法	ショートカット	参照
同じレコードのフィルタリング	これは、選択したものと同じタイプのレコードのみを表示する、ログフィルタリングをアクティブ化します。	Ctrl + Shift + F	
フィルタ...	このオプションをクリックすると、ログのフィルタリング ウィンドウでは、特定のログエントリのフィルタ条件を定義することができます。		ログのフィルタ
フィルタを有効にする	フィルタ設定を有効にします。最初にフィルタリングをアクティブ化するときには、設定を定義する必要があります。		
フィルタを無効にする	フィルタリングをオフにします(下にあるスイッチのクリックと同じ)。		
コピー	選択/強調表示されたレコードに関する情報をクリップボードにコピーします。	Ctrl + C	
すべてコピー	ウィンドウにあるすべてのレコードに関する情報をコピーします。		
エクスポート...	選択/強調表示されたレコードに関する情報をXMLファイルにエクスポートします。		
すべてエクスポート...	ウィンドウのすべての情報をXMLファイルにエクスポートします。		

ログファイル

ログファイルには、発生したすべての重要なプログラムイベントに関する情報が格納され、検査結果や検出された脅威などの概要が表示されます。ログは、システムの分析、ウイルスの検出、およびトラブルシューティングで重要なツールとして使用されます。ログへの記録はバックグラウンドでアクティブに実行され、ユーザーの操作を必要としません。情報は、ログの詳細レベルに関する現在の設定に基づいて記録されます。ESET Server Securityから直接テキストメッセージとログを表示できます。

ドロップダウンメニューから目的のログタイプを選択します。次のログを使用できます。

検出

検出ログにはESET Server Securityのモジュールにより検知されたマルウェアについての詳細情報が記録されています。この情報には、検出時刻、侵入物の名前、場所、実行されたアクション、侵入物の検出時にログインしていたユーザーの名前が含まれます。ログエントリをダブルクリックすると、その詳細が別のウィンドウに表示されます。必要に応じて、[検出除外](#)を作成できます。ログレコード(検出)を右クリックして、[除外の作成](#)をクリックします。[除外ウィザード](#)と定義された条件が開きます。除外されたファイルの横に検出の名前が表示されている場合は、特定の検出でのみファイルが除外されることを意味します。そのファイルが後から他のマルウェアで感染した場合は、検出されます。

イベント

イベントログにはESET Server Securityによって実行されたすべての重要なアクションが記録されます。イベントログには、プログラムで発生したイベントやエラーに関する情報が格納されます。システム管理者およびユーザーが問題を解決するように設計されています。多くの場合、ここで見た情報は、プログラムで発生した問題の解決法の検出に役立ちます。

コンピューターの検査

すべての検査結果はこのウィンドウに表示されます。各行は、個々のコンピュータ制御に対応します。エントリをダブルクリックすると、それぞれの検査結果の詳細が表示されます。

ブロックされたファイル

ブロックされ、アクセスできないファイルのレコードが含まれます。このプロトコルは、ファイルをブロックした理由とソースモジュール、ファイルを実行したアプリケーションとユーザーを示します。

送信されたファイル

ファイルクラウドベース保護ESET Dynamic Threat DefenseおよびESET LiveGrid®のレコードが含まれます。

監査ログ

設定および保護状態に変更の記録を含め、後から参照できるようにスナップショットを作成します。設定変更の任意のレコードを右クリックし、コンテキストメニューから[表示](#)をクリックすると、実行された変更に関する詳細情報が表示されます。前の設定に戻すには、[復元](#)を選択します。[すべて削除](#)をクリックすると、ログレコードを削除できます。監査ログを有効にする場合は、[詳細設定](#) > ツール > ログファイル > [監査ログ](#)に移動します。

HIPS

記録対象としてマークされた特定のルールが示されます。このプロトコルは、操作を呼

び出したアプリケーション、結果(ルールが許可されたのか禁止されたのか)、および作成されたルール名を表示します。

ネットワーク保護

ボットネット保護およびIDS(ネットワーク攻撃保護)によってブロックされたファイルの記録が含まれます。

フィルタリングされたWebサイト

[Webアクセス保護](#)。これらのログでは、特定のWebサイトへの接続を開いた時間、URL、ユーザー、およびアプリケーションを確認できます。

デバイスコントロール

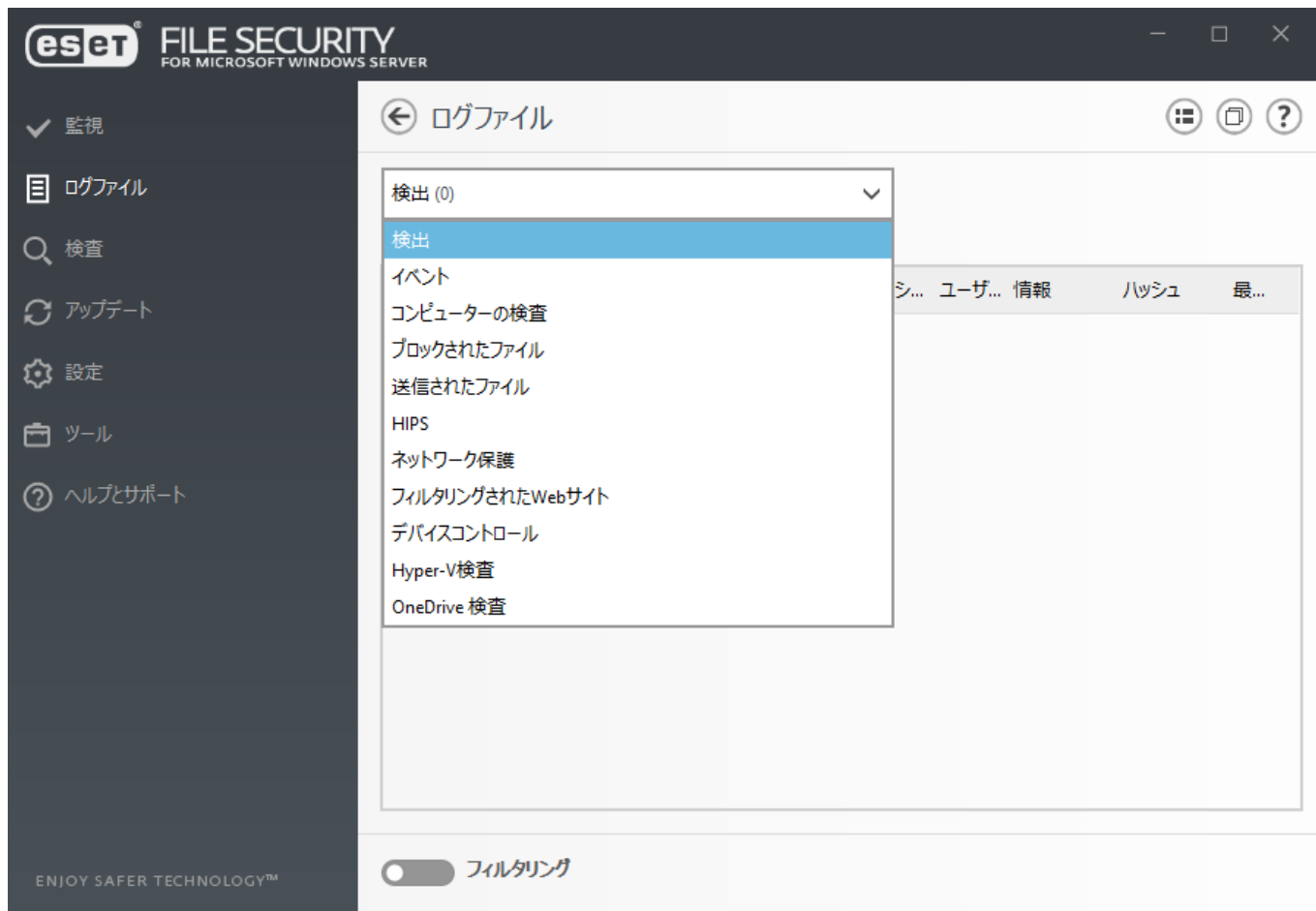
コンピュータに接続されたリムーバブルメディアまたはデバイスの記録が含まれます。個別のデバイスコントロールルールが設定されているデバイスのみがログファイルに記録されます。接続されているデバイスとルールが一致しない場合には、接続されているデバイスのログエントリは作成されません。ここで、デバイスタイプ、シリアル番号、ベンダー名、メディアのサイズ(ある場合)などの詳細情報も確認できます。

Hyper-V検査

Hyper-V検査結果のリストが含まれます。エントリーをダブルクリックすると、それぞれの検査結果の詳細が表示されます。

OneDrive検査

OneDrive検査結果のリストが含まれます。



コンテキストメニュー(右クリック)では、選択したログレコードに対する処理を選択できます。

アクション	使用方法	ショートカット	参照
表示	新しいウィンドウで選択したログに関する詳細を表示します(ダブルクリックと同じ)。		
同じレコードのフィルタリング	これは、選択したものと同じタイプのレコードのみを表示する、ログフィルタリングをアクティブ化します。	Ctrl + Shift + F	
フィルタ...	このオプションをクリックすると、 ログのフィルタリング ウィンドウでは、特定のログエントリのフィルタ条件を定義することができます。		ログのフィルタ
フィルタを有効にする	フィルタ設定を有効にします。最初にフィルタリングをアクティブ化する際には、設定を定義する必要があります。		
フィルタを無効にする	フィルタリングをオフにします(下にあるスイッチのクリックと同じ)。		
コピー	選択/強調表示されたレコードに関する情報をクリップボードにコピーします。	Ctrl + C	
すべてコピー	ウィンドウにあるすべてのレコードに関する情報をコピーします。		
削除	選択/強調表示されたレコードを削除します。このアクションには、管理者権限が必要です。	Del	
すべて削除	ウィンドウにあるすべてのレコードを削除します。このアクションには、管理者権限が必要です。		
エクスポート...	選択/強調表示されたレコードに関する情報をXMLファイルにエクスポートします。		

アクション	使用方法	ショートカット	参照
すべてエクスポート...	ウィンドウのすべての情報をXMLファイルにエクスポートします。		
検索...	ログを検索 ウィンドウを開き、検索条件を定義することができます。検索機能を使用し、フィルタリングがオンのときにも特定のレコードを検索できます。	Ctrl + F	ログ内検索
次を検索	定義した検索の次の出現を検索します。	F3	
前を検索	以前の出現を検索します。	Shift + F3	
除外の作成	検出名、パス、ハッシュを使用してオブジェクトを駆除から除外します。		除外の作成

ログのフィルタ

ログフィルタリング機能は、特に、多数のレコードがあるときに、検索している情報を見つけることができます。たとえば、特定のタイプのイベント、ステータス、または期間を検索している場合、ログレコードを絞り込むことができます。ログレコードをフィルタリングするには、特定の検索オプションを指定します。(検索オプションに従って)関連するレコードのみが、ログファイルウィンドウに表示されます。

テキストの**検索**フィールドに検索しているキーワードを入力します。**列を検索**ドロップダウンメニューを使用すると、検索を絞り込みます。**レコードログタイプ**ドロップダウンメニューから、1つ以上のレコードを選択します。結果を表示する**期間**を定義します。また**完全一致のみ**や**大文字と小文字を区別する**などの別の検索オプションを使用することもできます。

eset FILE SECURITY
FOR MICROSOFT WINDOWS SERVER

— ×

ログのフィルタ?

テキスト検索:

列を検索:
日時; 機能; イベント; ユーザー

レコードの種類:
診断; 情報; 警告; エラー; 重大

期間:
未指定

開始: 12/11/2018 10:00:00

終了: 13/11/2018 10:00:00

検索オプション
☐ 完全一致のみ
☐ 大文字と小文字を区別する

既定値 OK 閉じる

テキスト検索

文字列を入力します(単語または単語の一部)。この文字列を含むレコードのみが検索されます。その他のレコードは省略されます。

列を検索

検索の対象にする列を選択します。検索に使用する1つ以上のカラムをチェックできます。

レコードの種類

ドロップダウンメニューからレコードログの種類を1つ以上選択します。

- **診断** - プログラムおよび上記のすべてのレコードを微調整するのに必要な情報をログに記録します。
- **情報** - アップデートの成功メッセージを含むすべての情報メッセージと上記のすべてのレコードを記録します。
- **警告** - 重大なエラー、エラー、および警告メッセージを記録します。
- **エラー** - 「ファイルのダウンロード中にエラーが発生しました」といったエラーや重大なエラーを記録します。
- **重大** - 重大なエラーのみをログに記録します。

期間

結果を表示する期間を指定します。

- **未指定**(既定) – 期間内で検索するのではなく、ログ全体を検索します
- **昨日**
- **先週**
- **先月**
- **期間** – 正確な期間(開始:と終了:)を指定して、指定した期間のレコードだけを検索できます。

完全一致のみ(W)

完全一致を検索して結果の精度を高める場合に、このチェックボックスをオンにします。

大文字と小文字を区別する

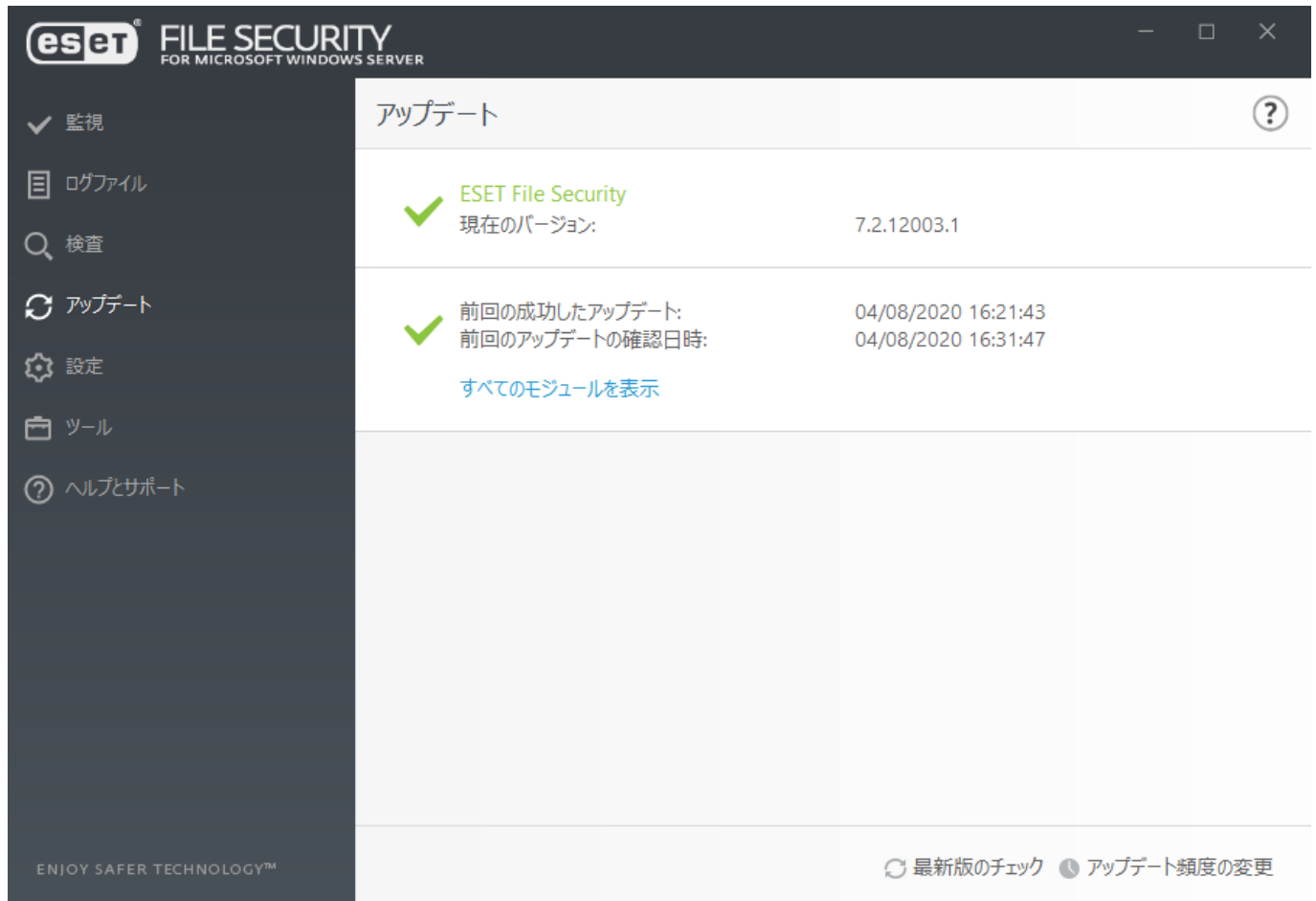
フィルタリングで大文字または小文字を使用することが重要な場合にこのオプションをオンにします。フィルタリング/検索オプションを設定した後に、**OK**をクリックすると、フィルタリングされたログレコードが表示されます。**検索**をクリックすると、検索が開始します。ログファイルは上から下に、現在の位置(ハイライトされたレコード)から開始します。検索は、一致する最初のレコードが見つかった時点で停止されます。**F3**を押すと、次のレコードを検索します。右クリックして**検索**を選択すると、検索オプションを絞り込みます。

アップデート

アップデートセクションには、前回のアップデート成功日時を含む、ESET Server Securityの最新のアップデートステータスが表示されます。サーバーのセキュリティを最大限確保するためにはESET Server Securityを定期的にアップデートするのが最善の方法です。アップデートモジュールにより、プログラムは検出のアップデートとシステムコンポーネントのアップデートという2つの方法で、常に最新の状態に保たれます。検出エンジンとプログラムコンポーネントのアップデートは、悪意のあるコードに対する完全な保護を実現するうえで重要な事項です。

注意

[製品認証キー](#)を入力していない場合は、アップデートを受信できず、製品をアクティベーションするように指示されます。このためには、**ヘルプとサポート > 製品のアクティベーション**に移動します。



現在のバージョン

ESET Server Securityビルドバージョン。

前回の成功したアップデート

最終更新日です。モジュールが最新、つまり最近の日付になっていることを確認します。

前回のアップデートの確認日時

モジュールアップデートの前回の試行日時。

すべてのモジュールを表示

インストールされているモジュールのリストを開きます。

最新版のチェック

モジュールのアップデートは、悪意のあるコードからの完全な保護を維持するための重要な部分です。

アップデート頻度の変更

スケジューラタスク [定期自動アップデート](#) のタスクのタイミングを編集できます。

できるかぎりすぐにアップデートを確認しない場合は、次のいずれかのメッセージが表示されます。

エラーメッセージ	説明
モジュールアップデートは古くなっています	このエラーは、モジュールをアップデートしようとして何回か失敗すると表示されます。アップデートの設定をチェックすることをお勧めします。このエラーが起こる原因として最も多いのは、認証データが正しく入力されていない、または 接続設定 が適切ではないことです。
モジュールのアップデートが失敗しました。製品はアクティベーションされていません	アップデート設定でライセンスキーが正しく入力されていません。認証データを確認することをお勧めします。 詳細設定 (F5を押す) にはその他のアップデートオプションがあります。メインメニューで[ヘルプとサポート]> [ライセンスの管理] をクリックして、新しいライセンスキーを入力します。
アップデートファイルのダウンロード中にエラーが発生しました	インターネット接続設定 によるものです。インターネット接続を確認することをお勧めします(Webブラウザで任意のWebサイトを開いてみます)Webサイトが開かない場合、インターネット接続が確立されていないか、コンピュータの接続に問題がある可能性があります。ご利用のインターネットサービスプロバイダ(ISP)に、有効なインターネット接続があるかどうか確認してください。
モジュールアップデートが失敗しました エラー0073	アップデート>アップデートの確認 をクリックします。詳細については、 ナレッジベース記事 を参照してください。

注意


アップデートプロファイルごとにプロキシサーバのオプションが異なる場合があります。その場合は、**詳細設定 (F5)**の**アップデート>プロファイル**で異なるプロファイルを設定できます。


設定


[設定]メニューウィンドウには次のセクションがあります。

- [サーバー](#)
- [コンピュータ](#)
- [ネットワーク](#)
- [Webとメール](#)
- [ツール - 診断ログイン](#)



個別のモジュールを一時的に無効にするには、該当するモジュールの横にある緑色のスライダーバー  をクリックします。これにより、コンピュータの保護レベルが低下する可能性があります。

無効なセキュリティコンポーネントの保護を再有効化するには、該当するモジュールの横にある赤色のスライダーバー  をクリックして、コンポーネントを有効状態に戻します。

特定のセキュリティコンポーネントの詳細設定にアクセスするには、歯車  をクリックします。



[設定のインポート/エクスポート](#)

.xml設定ファイルを使用して設定パラメーターをロードしたり、現在の設定パラメーターを設定ファイルに保存します。

[詳細設定](#)

各自のニーズにあった設定とオプションを、詳細設定ウィンドウで指定します。詳細設定画面にアクセスするには、プログラムの任意の場所で、**F5**を押します。

サーバー

スライダーバー  を使用して有効/無効にできるコンポーネントが一覧表示されます。特定の項目の設定を構成するには、歯車  をクリックします。

[自動除外](#)


重要なサーバーアプリケーションとサーバーのオペレーティングシステムファイルを識別して、[除外](#)リストに自動的に追加します。この機能によって、脅威検出ソフトウェアを実行する場合に潜在する競合のリスクが最小化されて、サーバーの全体的なパフォーマンスが向上されます。


[クラスタ](#)


ESET Clusterを設定し、有効にします。

[OneDrive検査の設定](#)

ESET OneDrive スキャナーアプリケーションをMicrosoft OneDriveに登録/登録解除できます。

個別のモジュールを一時的に無効にするには、該当するモジュールの横にある緑色のスライダーバー  をクリックします。これにより、コンピュータの保護レベルが低下する可能性があります。

無効なセキュリティコンポーネントの保護を再有効化するには、該当するモジュールの横にある赤色のスライダーバー  をクリックして、コンポーネントを有効状態に戻します。

特定のセキュリティコンポーネントの詳細設定にアクセスするには、歯車  をクリックします。

[設定のインポート/エクスポート](#)

.xml設定ファイルを使用して設定パラメーターをロードしたり、現在の設定パラメーターを設定ファイルに保存します。

[詳細設定](#)

各自のニーズにあった設定とオプションを、詳細設定ウィンドウで指定します。詳細設定画面にアクセスするには、プログラムの任意の場所で、**F5**を押します。

コンピューター

ESETServerSecurityには、コンピューターとしてサーバーの重要な保護を保証するすべての必要なコンポーネントがあります。このモジュールでは、次のコンポーネントを有効/無効にし、構成できます。

[リアルタイムファイルシステム保護](#)

全てのファイルは、コンピューター上で開くとき、作成するとき、または実行するときに、悪意のあるコードがないか検査されます。リアルタイムファイルシステム保護の場合、**設定**または**除外の編集**オプションがあります。これを使用すると、[除外](#)設定ウィンドウが開き、ファイルとフォルダを検査から除外できます。

[デバイスコントロール](#)

このモジュールを使用すると、拡張フィルタ/権限を検査、ブロック、または調整して、ユーザーからの指定デバイスへのアクセス方法やその作業方法を定義できます。

[ホスト侵入防止システム\(HIPS\)](#)

システムは、オペレーティングシステム内のイベントを監視し、カスタマイズされた一連のルールに従って動作します。

- [Advanced memory scanner](#) 


- [エクスプロイトブロック](#)
- [ランサムウェアシールド](#)


[プレゼンテーションモード](#)

ソフトウェアを中断なしに使用できることを要望し、ポップアップウィンドウの邪魔が入ることを望まずCPUの使用量を最小化したいと思っているユーザー向けの機能です。警告メッセージ(潜在的なセキュリティリスク)を受け取った後、プレゼンテーションモードを有効にするとメインプログラムウィンドウがオレンジに変わります。

ウイルス対策およびスパイウェア保護を一時停止

ウイルス・スパイウェア対策保護を一時的に無効にする場合は、ドロップダウンメニューを使用し、選択したコンポーネントを無効にする時間を選択してから、**[適用]**をクリックすると、セキュリティコンポーネントを無効にできます。保護を再有効化するには、**[ウイルス・スパイウェア対策を有効にする]**をクリックします。

個別のモジュールを一時的に無効にするには、該当するモジュールの横にある緑色のスライダーバーをクリックします。これにより、コンピュータの保護レベルが低下する可能性があります。

無効なセキュリティコンポーネントの保護を再有効化するには、該当するモジュールの横にある赤色のスライダーバーをクリックして、コンポーネントを有効状態に戻します。

特定のセキュリティコンポーネントの詳細設定にアクセスするには、歯車をクリックします。

[設定のインポート/エクスポート](#)

.xm設定ファイルを使用して設定パラメーターをロードしたり、現在の設定パラメーターを設定ファイルに保存します。

[詳細設定](#)

各自のニーズにあった設定とオプションを、詳細設定ウィンドウで指定します。詳細設定画面にアクセスするには、プログラムの任意の場所で、**F5**を押します。

ネットワーク


このためには、フィルタリングルールに基づいて、個別のネットワーク接続を許可または拒否します。リモートコンピューターからの攻撃から保護され、一部の危険な可能性があるサービスをブロックします。

[ネットワーク]モジュールでは、次のコンポーネントを有効/無効にし、構成できます。

[ネットワーク攻撃保護\(IDS\)](#)

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。有害と見なされるトラフィックはブロックされます。

[ボットネット保護](#)


[ボットネット](#)  通信の検出と遮断。システムのマルウェアをすばやく正確に特定します。


[一時IPアドレスブラックリスト\(ブロックされたアドレス\)](#)


攻撃の元であると検出され、一定の時間、接続をブロックするためにブラックリストに追加されたIPアドレスの一覧を表示します。

トラブルシューティングウィザード(最近ブロックされたアプリケーションまたはデバイス)

ネットワーク攻撃保護が原因の接続の問題を解決できます。

個別のモジュールを一時的に無効にするには、該当するモジュールの横にある緑色のスライダーバーをクリックします。これにより、コンピュータの保護レベルが低下する可能性があります。

無効なセキュリティコンポーネントの保護を再有効化するには、該当するモジュールの横にある赤色のスライダーバーをクリックして、コンポーネントを有効状態に戻します。

特定のセキュリティコンポーネントの詳細設定にアクセスするには、歯車をクリックします。

設定のインポート/エクスポート

.xm設定ファイルを使用して設定パラメーターをロードしたり、現在の設定パラメーターを設定ファイルに保存します。

詳細設定

各自のニーズにあった設定とオプションを、詳細設定ウィンドウで指定します。詳細設定画面にアクセスするには、プログラムの任意の場所で、**F5**を押します。

ネットワークトラブルシューティングウィザード

トラブルシューティングウィザードは、すべてのブロックされた接続を監視し、特定のアプリケーションまたはデバイスのネットワーク攻撃保護の問題を修正するためのトラブルシューティング手順を案内します。次に、ウィザードは、承認した場合に適用される新しいルールのセットを提案します。

Webとメール

Webとメールでは、次のコンポーネントを有効/無効にし、構成できます。

Webアクセス保護


これを有効にするとHTTPまたはHTTPS経由のすべてのトラフィックを検査して悪意のあるソフトウェアが検出されます。


電子メールクライアント保護


POP3とIMAPプロトコルで受信した通信が監視されます。

フィッシング対策保護

合法的なサイトに偽装した非合法のWebサイトによるパスワード、金融データ、およびその他の機密データの取得の試みから保護します。

個別のモジュールを一時的に無効にするには、該当するモジュールの横にある緑色のスライダーバーをクリックします。これにより、コンピュータの保護レベルが低下する可能性があります。

無効なセキュリティコンポーネントの保護を再有効化するには、該当するモジュールの横にある赤色のスライダーバーをクリックして、コンポーネントを有効状態に戻します。

特定のセキュリティコンポーネントの詳細設定にアクセスするには、歯車をクリックします。


[設定のインポート/エクスポート](#)

.xml設定ファイルを使用して設定パラメーターをロードしたり、現在の設定パラメーターを設定ファイルに保存します。

[詳細設定](#)


各自のニーズにあった設定とオプションを、詳細設定ウィンドウで指定します。詳細設定画面にアクセスするには、プログラムの任意の場所で、**F5**を押します。


ツール – 診断ロギング


特定のESET Server Security機能の動作に関する情報が必要なときには、[診断ログ](#)を有効にします(例: トラブルシューティングの場合)。歯車アイコンをクリックすると、診断ログを収集する[機能](#)を設定できます。

ログが有効になる時間(10分、30分、1時間、4時間、24時間、次回のサーバーの再起動まで、または永久)を選択できます。診断ログをオンにするとESET Server Securityは、有効な機能に従って、詳細ログを収集します。



個別のモジュールを一時的に無効にするには、該当するモジュールの横にある緑色のスライダーバーをクリックします。これにより、コンピュータの保護レベルが低下する可能性があります。

無効なセキュリティコンポーネントの保護を再有効化するには、該当するモジュールの横にある赤色のスライダーバーをクリックして、コンポーネントを有効状態に戻します。

特定のセキュリティコンポーネントの詳細設定にアクセスするには、歯車をクリックします。

設定のインポート/エクスポート

.xml設定ファイルを使用して設定パラメーターをロードしたり、現在の設定パラメーターを設定ファイルに保存します。

詳細設定

各自のニーズにあった設定とオプションを、詳細設定ウィンドウで指定します。**詳細設定**画面にアクセスするには、プログラムの任意の場所で、**F5**を押します。

設定のインポート/エクスポート

ESET Server Securityの現在の設定をバックアップする必要がある場合は、設定のインポート/エクスポート機能が役立ちます。また、インポート機能を使用して、同じ設定をESET Server Securityがインストールされた他のサーバーに配布/適用することができます。設定は、.xmlファイルにエクスポートされます。



注意

エクスポートしたファイルを指定したディレクトリに書き込むための十分な権限を持たない場合、設定のエクスポート中に、エラーが表示されることがあります。

ツール

次の機能は、ESET Server Security管理で使用できます。

- [実行中のプロセス](#)
- [アクティビティの確認](#)
- [保護統計](#)
- [クラスタ](#)
- [ESET Shell](#)
- [ESET Dynamic Threat Defense](#)
- [ESET SysInspector](#)
- [ESET SysRescue Live](#)
- [スケジューラ](#)
- [分析のためにサンプルを提出](#)
- [隔離](#)



実行中のプロセス

実行中のプロセスは、コンピューター上で実行中のプログラムまたはプロセスを表示し、新規のウィルスを即座にESETに通知し、その通知を継続します。ESET Server Securityは実行中のプロセスについて詳細

な情報を提供し、[ESET LiveGrid®](#)技術を有効にしてユーザーを保護します。

 **FILE SECURITY**
FOR MICROSOFT WINDOWS SERVER

✓ 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

← 実行中のプロセス

⌵ ↺ ?

このウィンドウには、実行中のプロセスとESET LiveGrid®からの追加情報のリストが表示されます。それぞれの評価とユーザー数、初回発見時間が示されます。

評価	プロセス	PID	ユーザー数	初回発見日	アプリケーション名
●●●●●●●●	smss.exe	208	●●●●●●●●	5年前	Microsoft® Windows® Op...
●●●●●●●●	csrss.exe	312	●●●●●●●●	5年前	Microsoft® Windows® Op...
●●●●●●●●	wininit.exe	388	●●●●●●●●	2年前	Microsoft® Windows® Op...
●●●●●●●●	winlogon.exe	416	●●●●●●●●	2年前	Microsoft® Windows® Op...
●●●●●●●●	services.exe	480	●●●●●●●●	5年前	Microsoft® Windows® Op...
●●●●●●●●	lsass.exe	488	●●●●●●●●	5年前	Microsoft® Windows® Op...
●●●●●●●●	svchost.exe	544	●●●●●●●●	5年前	Microsoft® Windows® Op...
●●●●●●●●	logonui.exe	668	●●●●●●●●	5年前	Microsoft® Windows® Op...
●●●●●●●●	dwm.exe	676	●●●●●●●●	5年前	Microsoft® Windows® Op...
●●●●●●●●	ekrn.exe	696	●●●●●●●●	1ヶ月前	ESET Security
●●●●●●●●	spoolsv.exe	904	●●●●●●●●	5年前	Microsoft® Windows® Op...
●●●●●●●●	vgauthservice.exe	1104	●●●●●●●●	1年前	VMware Guest Authenticati...
●●●●●●●●	vmtoolsd.exe	1188	●●●●●●●●	1年前	VMware Tools
●●●●●●●●	vmtoolsd.exe	1488	●●●●●●●●	2年前	Microsoft® Windows® Op...
●●●●●●●●	dllhost.exe	296	●●●●●●●●	5年前	Microsoft® Windows® Op...
●●●●●●●●	msdtc.exe	1940	●●●●●●●●	5年前	Microsoft® Windows® Op...

へ 詳細を表示

注意

最高(緑)のマークの付いた既知のアプリケーションは、感染していないことが判明しており(ホワイトリストに記載)、検査から除外されます。これは、コンピューターでの[コンピューターの検査]または[リアルタイムファイルシステム保護]の検査速度を向上させるための仕組みです。

評価	ほとんどの場合ESET Server SecurityおよびESET LiveGrid®技術は、各オブジェクト(ファイル、プロセス、レジストリキーなど)の特性を検査してから、悪意のあるアクティビティの可能性を重み付け評価する一連のヒューリスティックルールを使用して、オブジェクトのレピュテーションを決定します。これらのヒューリスティックに基づいて、オブジェクトには、9(最高レピュテーション(緑))~0(最低レピュテーション(赤))のレピュテーションレベルが割り当てられます。
プロセス	コンピューターで現在実行中のプログラムまたはプロセスのイメージ名。Windowsタスク マネージャを使用して、コンピューターで動作中のプロセスすべてを表示することもできます。タスクマネージャを開くには、タスクバーの何もない領域で右クリックしてから[タスクマネージャ]をクリックするか、またはキーボードでCtrl+Shift+Escを押します。
PID	Windowsオペレーティングシステムで実行中のプロセスのID
ユーザー数	指定されたアプリケーションを使用するユーザーの数。この情報は、ESET LiveGrid®技術によって収集されます。
動作期間	ESET LiveGrid®技術によってアプリケーションが検出された日付。
アプリケーション名	このプロセスに属するプログラムの特定の名前

注意

アプリケーションが不明(オレンジ)のマークを付けられていても、必ずしも悪意のあるソフトウェアというわけではありません。通常は、単に新しいアプリケーションというだけです。ファイルについて不明点がある場合は、[分析のためにファイルを提出](#)機能を使用してESETのウイルスラボにファイルを送信できます。そのファイルが悪意のあるアプリケーションであることが判明すると、それ以降のいずれかの検出エンジンアップデートファイルにその検出が追加されます。

詳細を表示

次の情報がウィンドウ下部に表示されます。

- **ファイルパス** - コンピューター上のアプリケーションの場所。
- **サイズ** - ファイルサイズがKB(キロバイト単位)またはMB(メガバイト単位)のいずれか。
- **説明** - オペレーティングシステムからの情報に基づくファイル特性。
- **会社** - ベンダーまたはアプリケーションプロセスの名前。
- **バージョン** - アプリケーション発行元からの情報。
- **製品** - アプリケーション名および/または商号。
- **作成日** - アプリケーションが作成された日時。
- **変更日** - アプリケーションが最後に変更された日時。

プロセス除外に追加

[実行中のプロセス]ウィンドウでプロセスを右クリックすると、検査から除外されます。パスは、[プロセス除外](#)のリストに追加されます。

アクティビティの確認

アクティビティを監視するには、アクティビティをグラフに含め、ドロップダウンメニューから次のアクティビティを選択します。

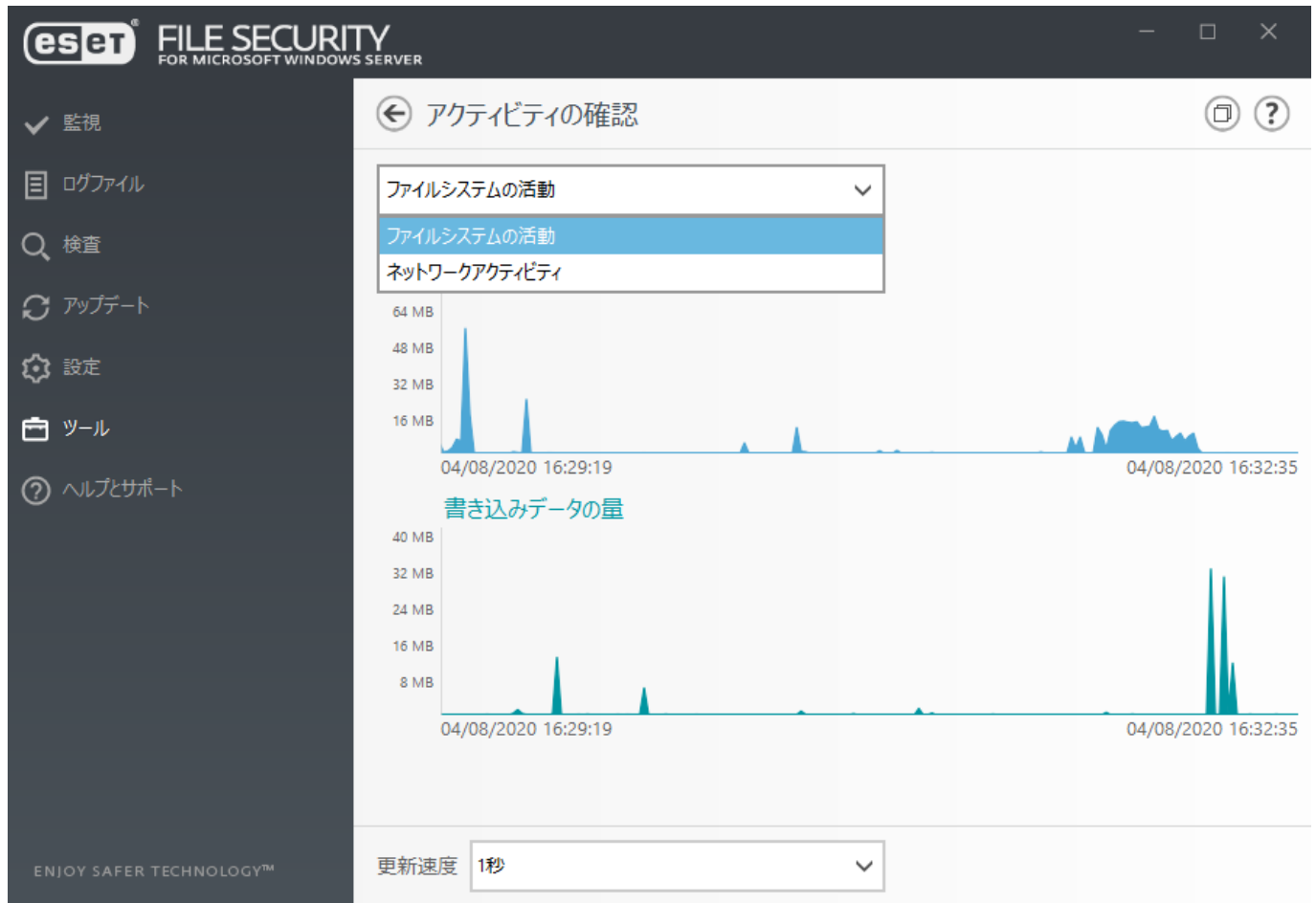
ファイルシステムの活動

読み取りまたは書き込まれたデータの量。グラフの縦軸は、読み取られたデータ(青)および書き込まれたデータ(緑)を示します。

ネットワークアクティビティ

送受信データの量。グラフの縦軸は、受信データ(青)および送信データ(緑)を示します。

グラフの最下部は、ファイルシステムアクティビティを選択された期間に基づいてリアルタイムで示す時系列です。[リフレッシュレート]ドロップダウンメニューを使用して、アップデートの頻度を変更します。

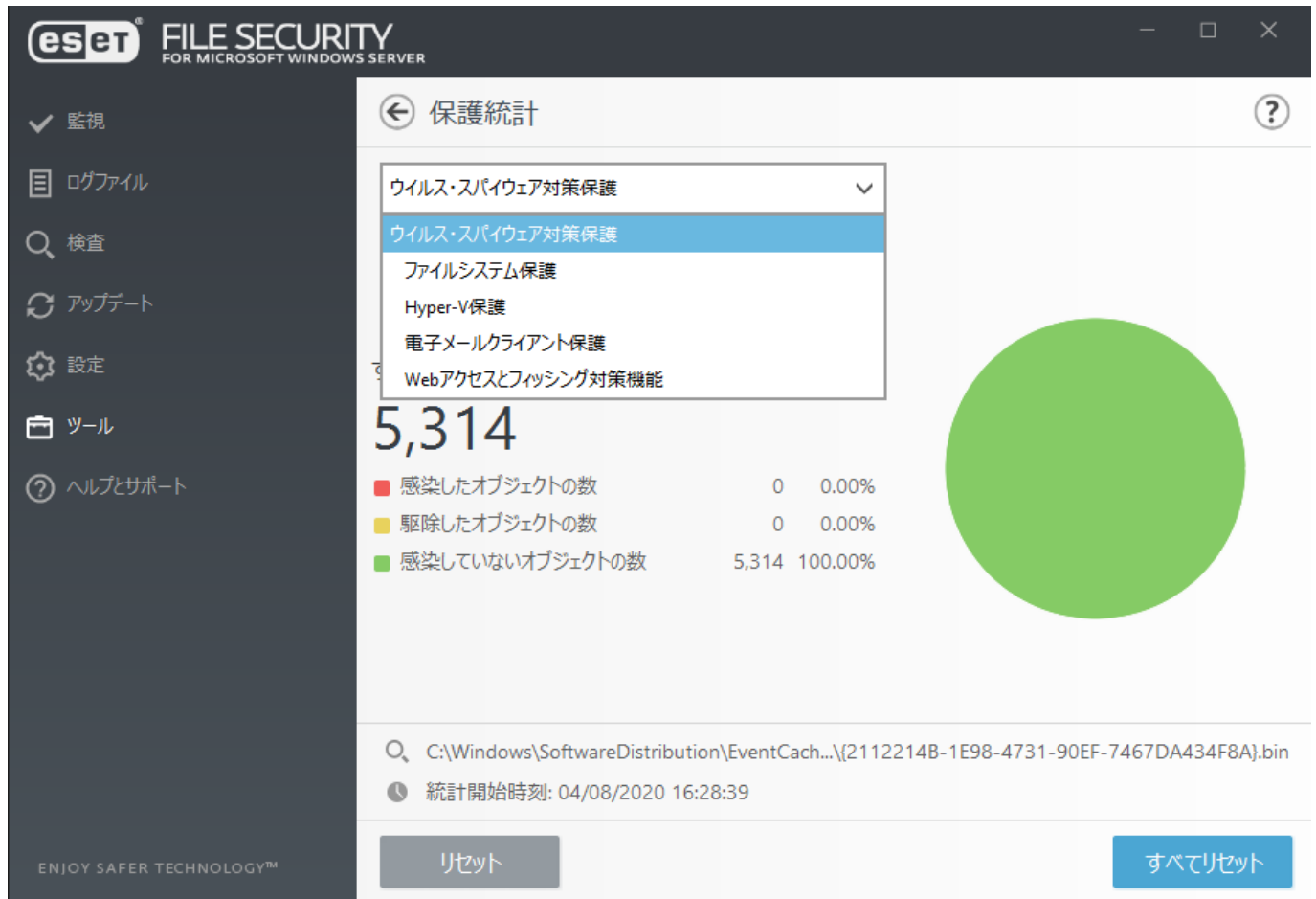


使用可能なオプションは次のとおりです。

1秒	グラフは1秒おきに更新され、時系列は直近10分間を表示します。
1分(直前の24時間)	グラフは1分おきに更新され、時系列は直近24時間を示します。
1時間(先月)	グラフは1時間おきに更新され、時系列は直近1ヶ月間を示します。
1時間(選択した月)	グラフは1時間おきに更新され、時系列は選択した月を示します。ドロップダウンメニューから月(および年)を選択し、アクティビティを表示します。 変更 をクリックします。

保護統計

ESET Server Securityの保護モジュールに関連する統計データを表示するには、ドロップダウンメニューから該当する保護モジュールを選択します。統計の横には、すべての検査済みオブジェクト数、感染オブジェクト数、駆除済みオブジェクト数、および未感染のオブジェクト数が表示されます。**[リセット]**をクリックして統計情報をクリアするか、**[すべてリセット]**をクリックしてすべての既存データを削除します。



ESET Server Securityで使用可能な統計グラフは次のとおりです。

ウイルス・スパイウェア対策保護

感染オブジェクトおよび駆除済みオブジェクトの総数を表示します。

ファイルシステム保護

ファイルシステムにのみ読み込みまたは書き込みされたオブジェクトを表示します。

Hyper-V保護

感染オブジェクトおよび駆除済みオブジェクトの総数を表示します(Hyper-Vのシステムのみ)。

電子メールクライアント保護

電子メールクライアントのみだけに送受信されたオブジェクトを表示します。

Webアクセスとフィッシング対策機能

Webブラウザ だけ でダウンロードした オブジェクトを表示します。

クラスタ

[ESET Cluster]はMicrosoft Windows Server製品のESETラインのP2P通信インフラストラクチャです。

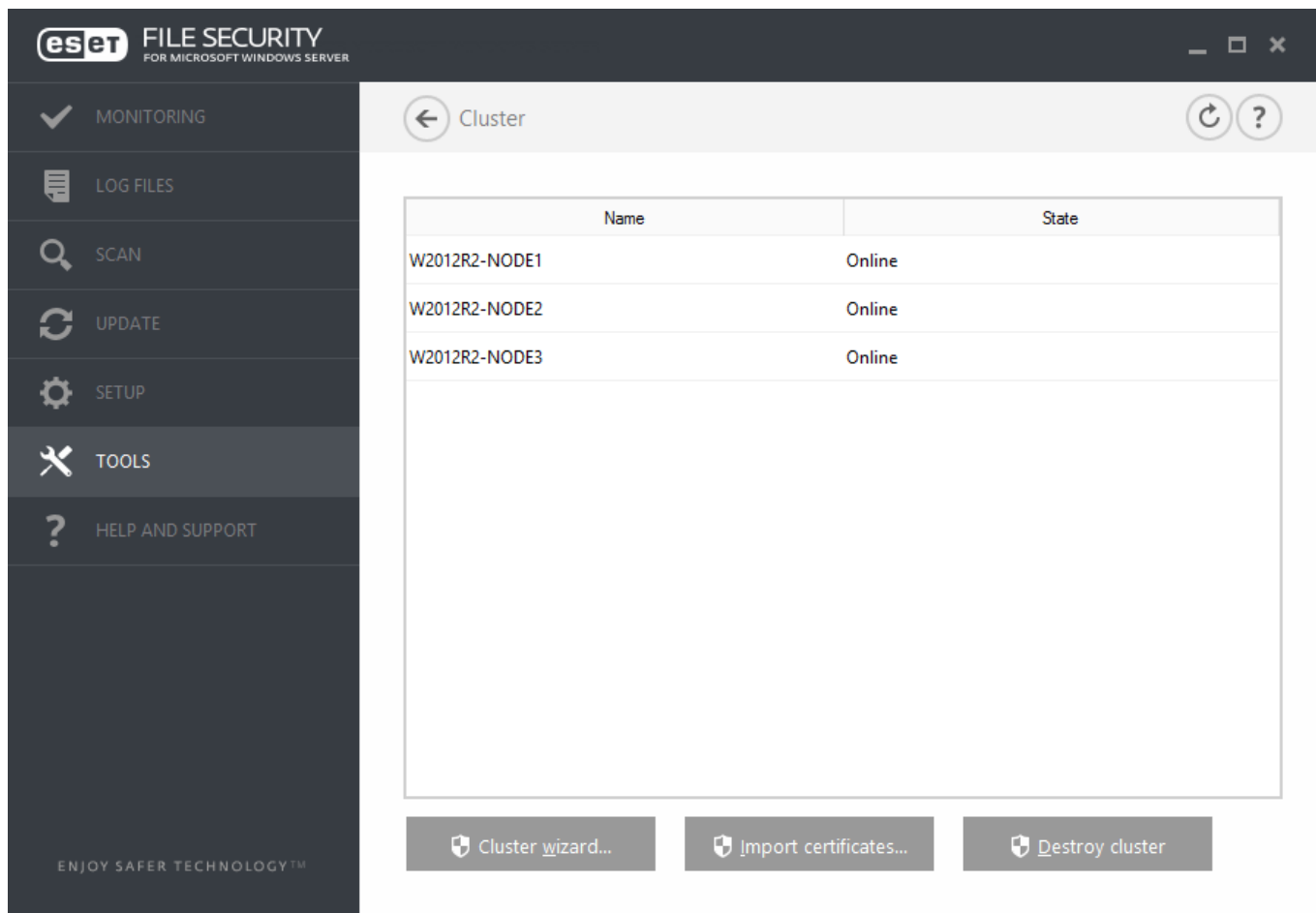
このインフラストラクチャによりESETサーバー製品は相互に通信し、設定や通知などのデータを交換

できます。し、製品インスタンスのグループの正常な動作に必要なデータを同期できます。このようなグループの例は、クラスタ全体に渡って製品の同じ構成を持つ必要がある場所にESET製品がインストールされているWindowsフェールオーバークラスタまたはネットワーク負荷分散(NLB)クラスタ内のノードのグループになります。ESET Clusterでは、インスタンス間でこの整合性を保証します。

注意

[ユーザーインターフェース](#)と[スケジュールされたタスク](#)の設定は、ESET Clusterノード間で同期されません。これは意図された動作です。

ESET Clusterステータスページにアクセスするには、メインメニューの[ツール]>[クラスタ]を選択します。正しく設定されていると、ステータスページは次のように表示されます。



注意

ESET Server SecurityとLinux用のESETファイルセキュリティ間ではESET Clusterの作成がサポートされていません。

ESET Clusterを設定する際、ノードを追加する方法は2つあります。

自動検出

既存のWindows Failover Cluster/NLB Clusterがある場合、自動検出は、メンバーノードを自動的にESET Clusterに追加します。

参照

サーバー名(同じワークグループのメンバーまたは同じドメインのメンバーのいずれか)を入力してノードを手動で追加することができます。

注意

サーバーは、ESET Cluster機能を使用するためにWindows Failover Cluster / NLB Clusterのメンバーである必要はありません。ESET Clusterを使用するにはWindows Failover ClusterまたはNLB Clusterは環境内で必要ありません。

ESETにノードを追加した後、各ノード上に ESET Server Security をインストールします。これはESET Cluster設定中に自動的に行われます。他のクラスタノード上の ESET Server Securityのリモートインストールに必要な資格情報：

ドメインシナリオ

ドメイン管理者の資格情報

ワークグループシナリオ

すべてのノードが同じローカル管理者アカウントの資格情報を使用していることを確認する必要があります。

ESET Clusterでは、既存のWindows Failover Cluster / NLB Clusterのメンバーとして自動で追加したノードと手動で追加したノードの組み合わせを使用することもできます(同じドメインにある場合)。

重要

ドメインノードとワークグループノードを組み合わせることはできません。

ESET Clusterを使用するための他の要件は、ESET Clusterノード上にESET Server Securityのインストールをプッシュする前に、Windowsファイアウォールで**ファイルとプリンタの共有**を有効にする必要があります。

新たなノードを既存のESET Clusterに追加するには、[\[クラスタウィザード\]](#)を実行します。

証明書のインポート

証明書は、HTTPSが使用されるときに、強力なコンピューター間認証を提供するために使用されます。各ESET Clusterには、独立した証明書階層があります。階層には、1つのルート証明書と、ルート証明書によって署名されたノード証明書のセットがあります。ルート証明書の秘密鍵は、すべてのノード証明書が作成された後に破棄されます。新子位ノードをクラスタに追加すると、新しい証明書階層が作成されます。証明書を含む(クラスタウィザード中に作成された)フォルダーに移動します。証明書ファイルを選択し、**開く**をクリックします。

クラスタの無効化

ESET Clusterを破棄することができます。各ノードは、破棄したESET Clusterに関してのイベントログに記録を書き込みます。その後、すべてのESETのファイアウォールルールはWindows Firewallから削除されます。元のノードは以前の状態になり、必要に応じて他のESET Clusterで再度使用することができます。

クラスタウィザード - ノードの選択

ESET Clusterを設定する最初のステップはノードの追加です。[\[自動検出\]](#) オプションまたは [\[参照\]](#) のいずれかを使用してノードを追加します。または、テキストボックスにサーバー名を入力して、[\[追加\]](#) ボタンをクリックします。

自動検出

既存のWindows Failover Cluster / Network Load Balancing (NLB) Clusterから自動的にノードを追加します。ESET Clusterを作成するために使用するサーバーは、ノードを自動追加するためにWindows Failover Cluster / NLB Clusterのメンバーである必要があります。NLB ClusterにはESET Clusterがノードを正しく検出するためにクラスタのプロパティで有効になる[リモート制御許可]機能が必要です。新しく追加されたノードのリストがある場合は、不要なノードを削除できます。

参照

DomainまたはWorkgroup内のコンピューターを検索し選択します。これで、ノードをESET Clusterに手動追加できます。ノードを追加する別の方法は、追加するサーバーのホスト名を入力して、追加をクリックします。

読み込み

ファイルからノードのリストをインポートするには。

The screenshot shows a 'Select nodes' dialog box. It features a text input field for adding a machine to the cluster nodes list, with an 'Add' button. Below this is a list of existing cluster nodes, currently showing 'ESFW_NODE1', 'ESFW_NODE2', and 'ESFW_NODE3'. To the right of the list are buttons for 'Remove', 'Remove all', 'Autodetect', 'Browse...', and 'Load...'. At the bottom right, there are 'Next' and 'Cancel' buttons.

リスト内の[クラスタノード]を変更するには、削除するノードを選択し[削除]をクリックするか、リストを完全に消去するには [すべて削除]をクリックします。

既存のESETクラスタがすでにある場合は、いつでも新しいノードを追加できます。手順は上記と同じです。

注意

リストに残っているすべてのノードはオンラインで到達可能である必要があります。ローカルホストはクラスタノードに既定で追加されます。

クラスターウィザード – クラスター設定

クラスター名、およびネットワーク詳細情報(必要な場合)を定義します。

クラスター

クラスターの名前を入力し、**次へ**をクリックします。

リスニング ポート – (既定ポートは9777です)

ネットワーク環境で既にポート9777が使用されている場合は、使用中ではない他のポート番号を指定します。

Windowsファイアウォールでポートを開く

ルールを確認する時にWindowsファイアウォールで作成されます。

クラスターウィザード – クラスターセットアップ設定

証明書配布モードおよび他のノードに製品をインストールするかどうかを定義します。

証明書配付

- **自動** リモート - 証明書が自動的にインストールされます。
- **手動 - 生成** をクリックし、証明書の保存先ホルダーを選択します。ルート証明書と、ESET Clusterを設定しているノード(ローカルマシン)を含む各ノードの証明書が作成されます。**はい**をクリックして、ローカルマシン証明書を登録することもできます。ここで説明するように、後で証明書を手動でインポートする必要があります。

他のノードへの 製品インストール

- **自動** リモート - ESET Server Security は、各ノードに自動的にインストールされます(提供のオペレーティングシステムは 同じアーキテクチャです)。
- **手動** - ESET Server Security を手動でインストールします(たとえば複数のノードに異なるOSアーキテクチャがある場合)。

アクティベートされた製品がないノードにライセンスをプッシュ

ESET Securityは自動的に、ライセンスがないノードにインストールされているESETソリューションをアクティベーションします。

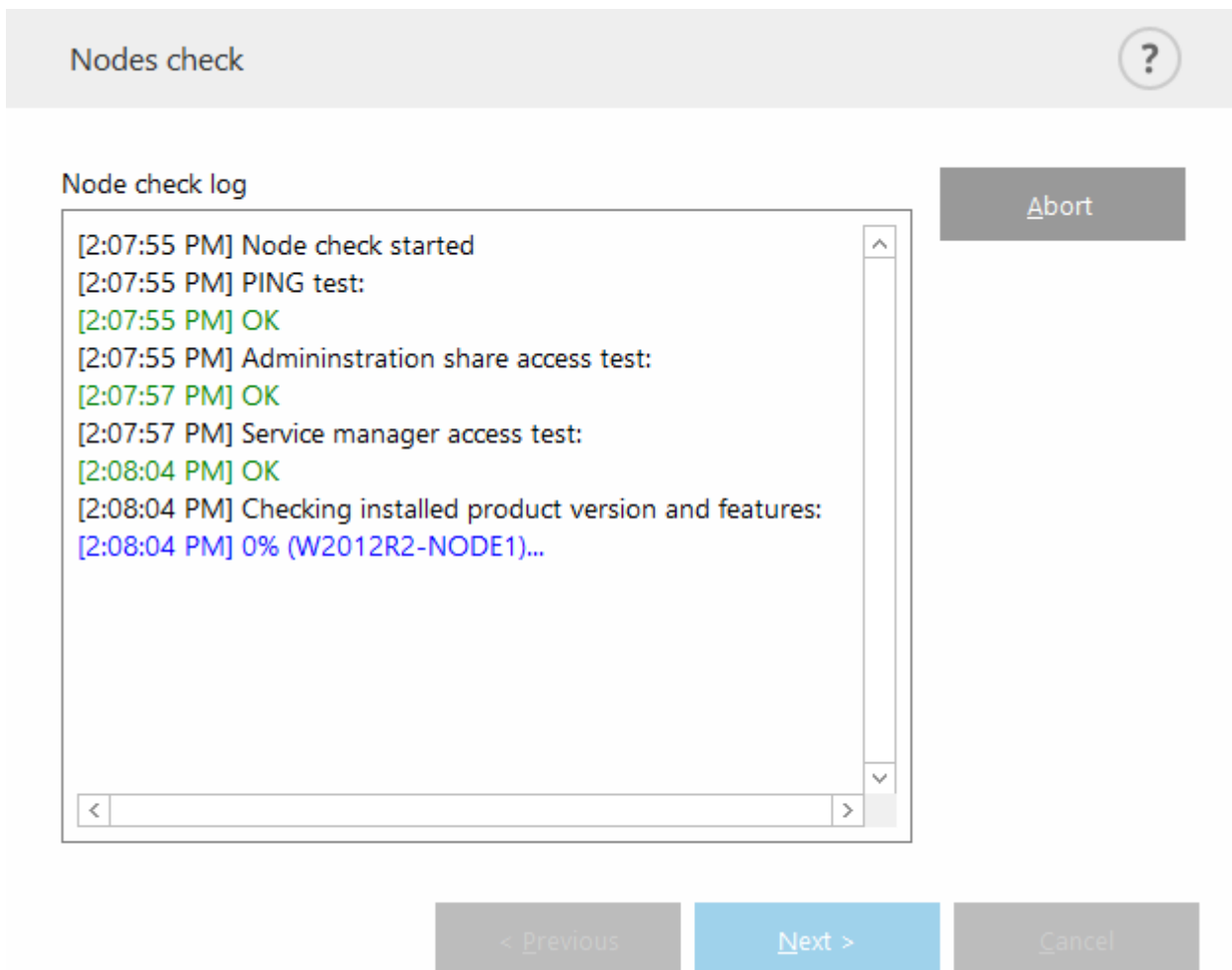
注意

混在オペレーティングシステムアーキテクチャ(32ビットおよび64ビット)でESET Clusterを作成するには、**ESET Server Security**を手動でインストールします。使用中のオペレーティングシステムは、次のステップ中に検出され、ログウィンドウでこの情報を参照することができます。

クラスタウィザード – ノードチェック

インストールの詳細を指定した後、ノードチェックが実行されます。ノードチェックログに次の情報が表示されます。

- 既存のノードがオンラインであることを確認
- 新しいノードがアクセス可能であることを確認
- ノードがオンラインである
- 管理者共有がアクセス可能である
- リモート実行が可能である
- 正しい製品バージョンがインストールされている（または製品がインストールされていない）
- 新規証明書の存在確認



ノードチェックが完了するとレポートが表示されます。

Node check log

[2:07:55 PM] Node check started
[2:07:55 PM] PING test:
[2:07:55 PM] OK
[2:07:55 PM] Administration share access test:
[2:07:57 PM] OK
[2:07:57 PM] Service manager access test:
[2:08:04 PM] OK
[2:08:04 PM] Checking installed product version and features:
[2:08:06 PM] W2012R2-NODE3: Remote machine has different
set of ESET product features installed. Product will be reinstalled.
[2:08:07 PM] W2012R2-NODE2: Install will be performed.
[2:08:08 PM] OK

Check

< Previous

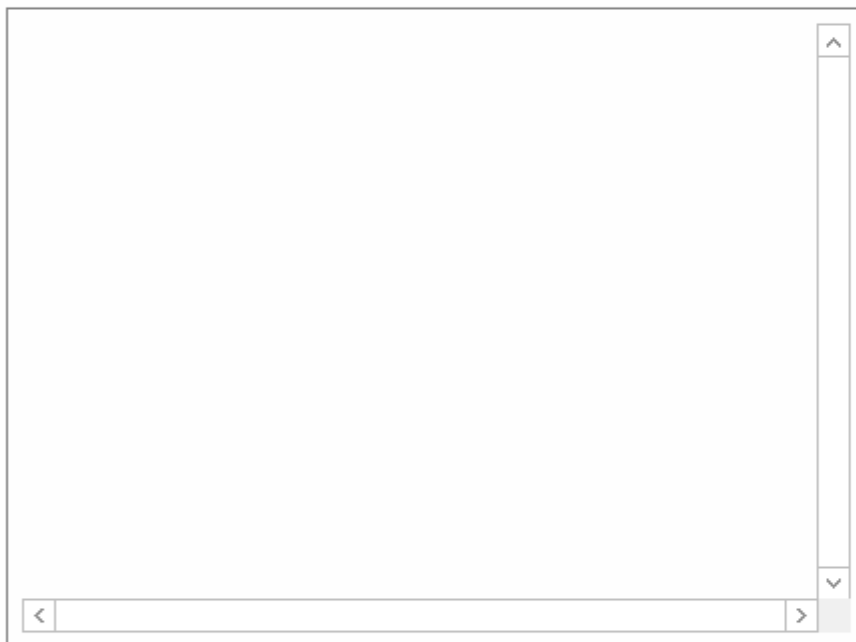
Next >

Cancel

クラスタウィザード - ノードインストール

ESET Clusterの初期化中にリモートマシンで製品をインストールする場合、インストーラーは`%ProgramData%\ESET\ESET Security\Installer`ディレクトリで検索されます。インストーラーパッケージが検索されない場合、ユーザーはインストーラーファイルを検索する必要があります。

Product install log

[Install](#)

< Previous

Finish

Cancel

注意

異なるアーキテクチャ(32ビット対64ビット)を持つノードの自動リモートインストールを使用しようとする、これが検出されるので、手動でインストールする必要があります。

Product install log

[12:56:34 PM] Generating certificates for cluster nodes...
[12:56:36 PM] All certificates created.
[12:56:36 PM] Copying files to remote machines:
[12:56:41 PM] All files have been copied to remote machines.
[12:56:41 PM] Installing product:
[12:56:42 PM] Number of installers started: 2
[12:59:35 PM] ESET product is installed on all remote machines.
[12:59:35 PM] Enrolling certificates:
[12:59:38 PM] All certificates have been enrolled to remote machines.
[12:59:38 PM] Activating cluster feature:
[12:59:40 PM] ESET cluster feature has been activated on all machines.

[Install](#)

< Previous

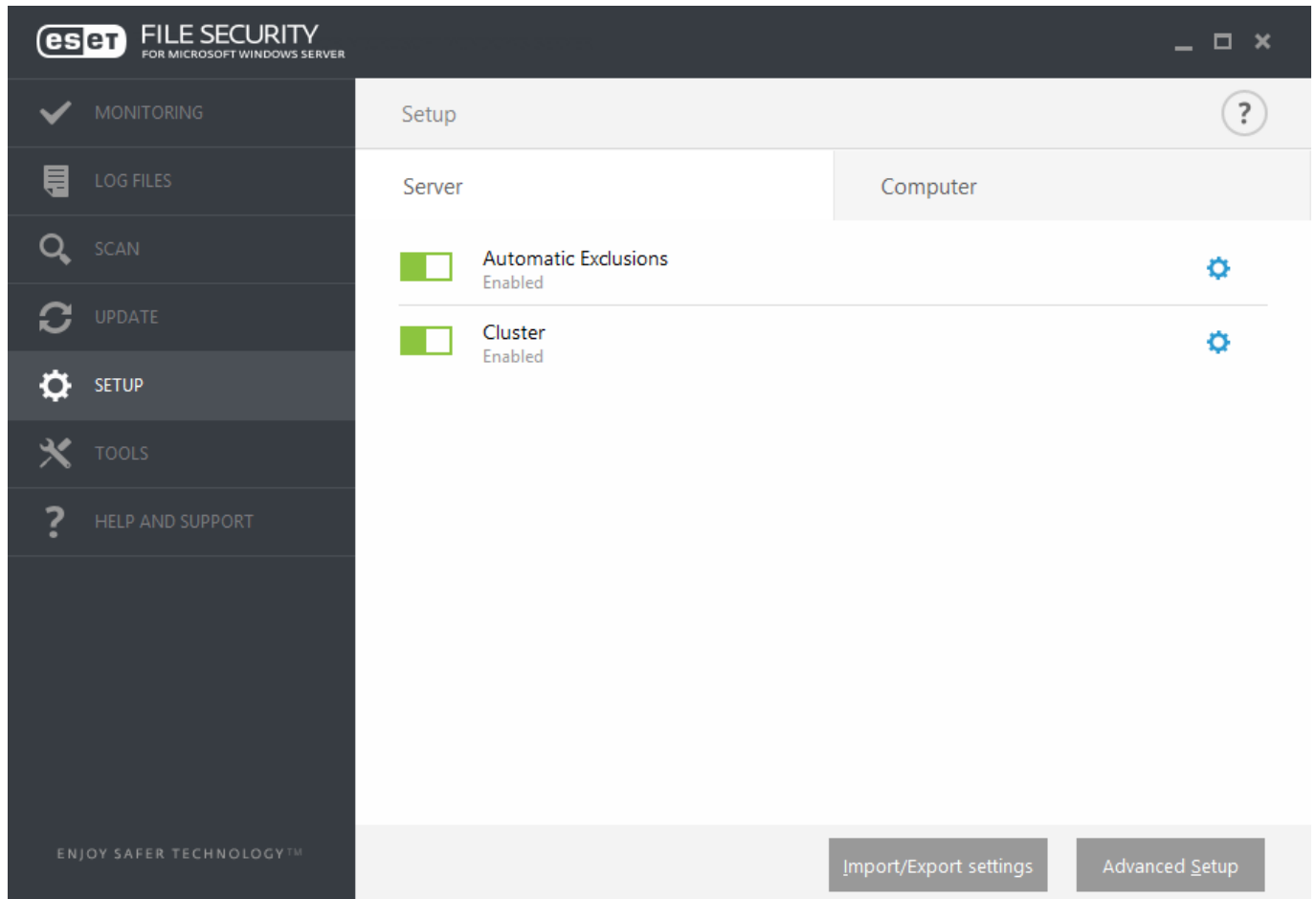
Finish

Cancel

ESET Clusterを正しく構成すると、**設定 > サーバー**ページで有効になります。

注意

古いバージョンのESET Server Securityが既に一部のノードにインストールされている場合は、最新のバージョンがこれらのコンピューターで必要であることが通知されます。ESET Server Securityをアップデートすると、コンピューターが自動的に再起動する場合があります。



また、クラスタのステータスページで現在のステータスを確認することができます（ツール>クラスタ）[図](#)

ESET Shell

eShell (ESET Shell)は、ESET Server Securityのコマンドラインインタフェースです。eShellではグラフィカルユーザーインターフェイス(GUI)の代用として、GUIに通常備わっているほぼすべての機能とオプションを使用でき、eShellでプログラム全体の設定と管理を行うことができます。

GUIで使用可能なすべての機能のほかに、スクリプトを実行して、設定、設定の変更、またはアクションの実行を自動化するオプションがあります。eShellは、GUIよりもコマンドラインのほうが使いやすいユーザーにとっても有用です。

注意

完全な機能を実現するために、管理者として実行を使用してeShellを開くことをお勧めします。Windows コマンドプロンプト(cmd)を使用して1つのコマンドを実行するときにも同じことが当てはまります。管理者として実行を使用してプロンプトを開きます。管理者としてコマンドプロンプトを実行できない場合は、権限不足によりコマンドの実行ができません。

eShellを実行するモードには対話モードと単一コマンド/バッチモードの2つがあります。

1. **対話モード** - 単一のコマンドを実行するだけでなく、設定の変更や、ログの表示などのタスクでeShellを操作する場合に有用です。対話モードは、まだ慣れていないコマンドがある場合にも使用できます。対話モードではeShellを検索しやすくなります。特定のコンテキストで使用できる、有効なコマンドも表示されます。
2. **単一コマンド/バッチモード** - eShellの対話モードを入力せずにコマンドを実行する必要がある

場合のみ、このモードを使用することができます。適切なパラメーターを使用して **eshell** と入力して **Windows** コマンドプロンプトから行うことができます。

例

```
eshell get statusまたはeshell computer set real-time status disabled 1h
```

バッチ/スクリプトモードで特定のコマンド(上記の2番目の例など)を実行するには、まず、数個の設定を構成する必要があります。そうでないと、**アクセスが拒否されました**というメッセージが表示されます。これはセキュリティの理由のためです。

注意

Windows コマンドプロンプトから **eShell** コマンドを使用できるようにするには、設定変更が必要です。バッチファイルの実行の詳細については、[ここ](#)をクリックしてください。

eShell では2つの方法でインタラクティブモードを実行できます。

1. **Windows** の [スタート] メニューから [スタート] > [すべてのプログラム] > [ESET] > [ESET File Security] > ESET Shell

2. **Windows** コマンドプロンプトから **eshell** と入力し、Enter キーを押します

重要

エラー '**eshell**' is not recognized as an internal or external command がある場合は、**ESET Server Security** のインストールの後にシステムによって新しい環境変数が読み込まれていないためです。新しいコマンドプロンプトを開き、もう一度 **eShell** を起動します。エラーが解決しないか **ESET Server Security** の [コアインストール](#) がある場合は、"%PROGRAMFILES%\ESET\ESET File Security\eshell.exe" などの絶対パスで **eShell** を起動します(コマンドを実行するには、"" を使用する必要があります)。

eShell の初回起動時(ガイド)には、初期画面が表示されます。

注意

今後、初回実行画面を表示する場合は、**guide** コマンドを入力します。この画面には **eShell** のいくつかの基本的な使用例と、構文、プリフィクス、コマンドパス、省略形、エイリアスなどが表示されます。

次回 **eShell** を実行すると、次の画面が表示されます。

```
ESET Shell
ESET Shell 2.0 (6.5.12009.1)
Copyright (c) 1992-2017 ESET, spol. s r.o. All rights reserved.

Maximum protection

License validity:      12/30/2021
Last successful update: N/A

Automatic exclusions:      Enabled
Anti-Stealth protection:   Enabled
Document protection:       Disabled
HIPS:                      Enabled
Real-time file system protection: Enabled
Device control:           Disabled
ESET Cluster:              Disabled
Diagnostic logging:        Disabled
Presentation mode:         Paused
Anti-Phishing protection:  Enabled
Email client protection:   Enabled
Web access protection:     Enabled

ABOUT      ANTI VIRUS    DEVICE      GUIDE      LICENSE
PASSWORD    RUN            SCHEDULER  SETTINGS  SIGN
STATUS      TOOLS           UI          UPDATE    VIRLOG
WARNLOG     WEB-AND-EMAIL

eShell>_
```

注意

コマンドは大文字と小文字を区別しません。大文字と小文字のいずれも使用でき、コマンドは区別なく実行されます。

eShellのカスタマイズ

eShellはui eshellコンテキストでカスタマイズできます。[スクリプト](#)のエイリアス、色、言語、実行ポリシー、非表示のコマンドの設定などを構成できます。

使用方法

構文

コマンドが機能するには正しい構文形式が必要です。コマンドはプレフィックス、コンテキスト、引数、オプションなどで構成できます。これはeShell全体で使用する一般的な構文になります。

[<prefix>] [<command path>] <command> [<arguments>]

例(ドキュメント保護の有効化):

SET COMPUTER SCANS DOCUMENT REGISTER ENABLED

SET - プレフィックス

COMPUTER SCANS DOCUMENT - 特定のコマンドのパス、つまり、このコマンドのコンテキスト

REGISTER - コマンド本体

ENABLED - コマンドのパラメータ

?を引数として使用すると、その特定のコマンドの構文が表示されます。たとえば、STATUS ? にはSTATUSコマンドの構文が表示されます。

構文:

[get] status

操作:

get - すべての保護モジュールのステータスを表示

お気付きのように、[get]は括弧で囲まれています。これはプレフィックスgetがstatusコマンドの既定であることを指定します。つまり、プレフィックスを指定せずに、statusを実行するときに、実際には既定のプレフィックス(この場合はget status)を使用します。getがほとんどのコマンドの既定のプレフィックスですが、個々のコマンドについて既定のプレフィックスが何であるかと、実際に所定通りの操作が実行されるのかをあらかじめ確認してください。

注意

コマンドの大文字と小文字は区別されません。大文字と小文字のいずれも使用でき、コマンドは区別なく実行されます。

プレフィックス/操作

プレフィックスは処理です。GETプレフィックスではESET Server Securityの特定の機能の設定内容が表示されるか、または状態が表示されます(たとえば、GET COMPUTER REAL-TIME STATUSは現在の保護の状態を示します)。SETプレフィックスは機能を設定したり、状態を変更したりします(SET COMPUTER REAL-TIME STATUS ENABLEDは保護を有効にします)。

これらはEshellで利用できるプレフィックスです。コマンドでは、以下のプレフィックスがサポートされる場合とそうでない場合があります。

GET	現在の設定/状態を返す
SET	値/状態を設定
SELECT	項目の選択
ADD	項目の追加
REMOVE	項目の削除
CLEAR	すべての項目/ファイルを削除
START	アクションを開始する
STOP	アクションを停止する
PAUSE	アクションを中断する
RESUME	アクションを再開する
RESTORE	既定の設定/オブジェクト/ファイルを復元
SEND	オブジェクト/ファイルを送信する
IMPORT	ファイルからインポートする
EXPORT	ファイルにエクスポートする

注意

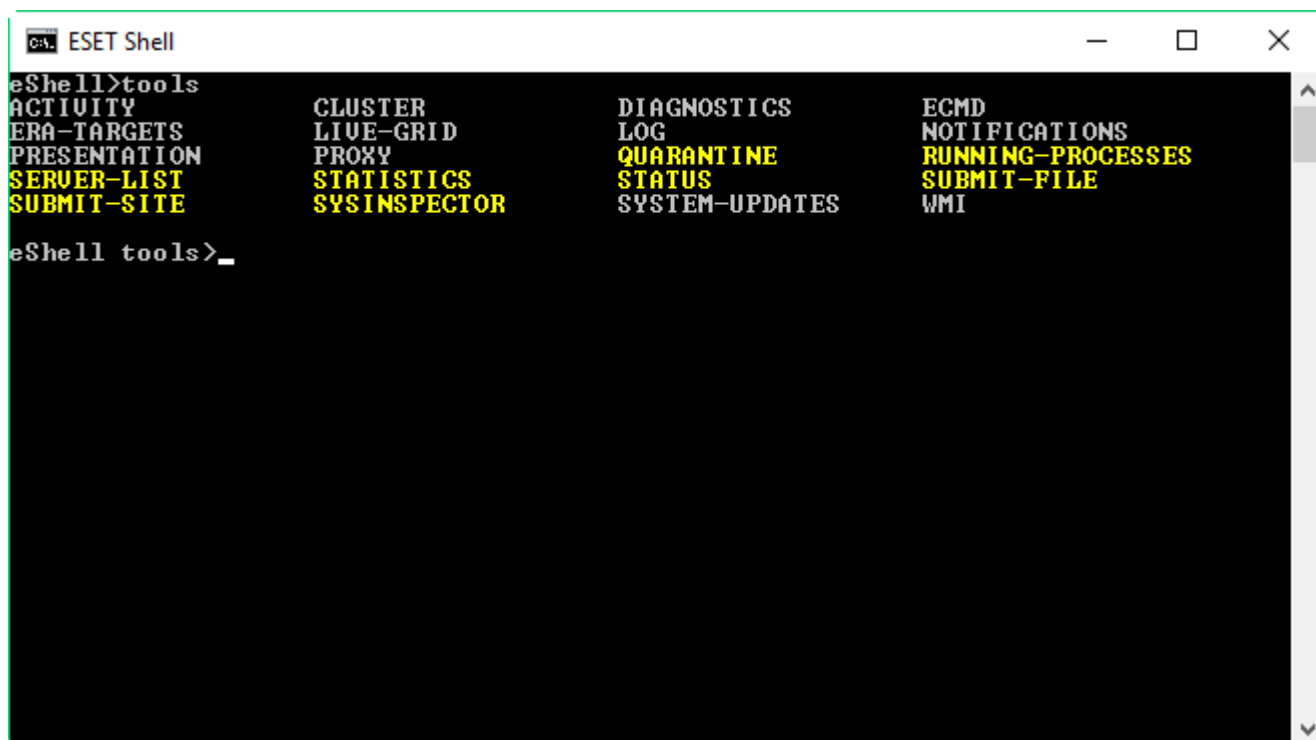
GETやSETなどのプレフィックスは、多くのコマンドで使用されますが、一部(EXITなど)にはプレフィックスを使用しないものもあります。

コマンドパス/コンテキスト

コマンドは、ツリー構造を形成するコンテキスト内で使用されます。ツリーの最上位はルートで、eShellを実行した時点では、ルートレベルになっています。

eShell>

そのままコマンドを実行することもできれば、コンテキスト名を入力してツリー内を移動することもできます。たとえば、TOOLSコンテキストを入力すると、ここで使用可能なすべてのコマンドとサブコンテキストが一覧表示されます。



黄色で示された項目は実行できるコマンド、灰色で示された項目は開始できるサブコンテキストです。サブコンテキストには、コマンドがさらに含まれています。

上のレベルに戻る必要がある場合は、.. (2つのドット)を使用します。

例

次の場所にいるとします。

```
eShell computer real-time>
```

..と入力すると、1つ上のレベルに移動します。

```
eShell computer>
```

eShell computer real-time> (ルートの2レベル下)からルートに戻る場合は、.. ..を入力します(2つのドットと2つのドットはスペースで区切る)。このようにすると、2レベル上がり、この場合のルートになります。バックスラッシュ\を使用すると、現在のコンテキストツリー内の階層に関係なく、あらゆるレベルから直接ルートに戻ります。上位のレベルの特定のコンテキストに移動する場合は、必要に応じて該当する数の.. コマンドを使用(スペース区切り)して、任意のレベルに移動します。たとえば、3つ上位に移動するには、..を使用します

パスは、現在のコンテキストからの相対パスです。現在のコンテキストに入っているコマンドの場合は、パスを入力しません。たとえば、GET COMPUTER REAL-TIME STATUSを実行するには、次のように入力します。

GET COMPUTER STATUS - ルートコンテキスト(コマンドラインは eShell>

GET STATUS - コンテキストCOMPUTER(コマンドラインは eShell computer>)の場合

.. GET STATUS - コンテキストCOMPUTER REAL-TIME(コマンドラインは eShell computer real-time>)の場合

2つのドット..ではなく1つのドット.を使用できます。1つのドットは2つのドットの略語です。

例

. GET STATUS - コンテキストCOMPUTER REAL-TIME(コマンドラインは eShell computer real-time>)の場合

パラメータ

特定のコマンドに対して実行するアクションの引数です。たとえば、コマンドCLEAN-LEVEL (COMPUTER REAL-TIME ENGINEにあります)は次の引数で使用できます。

rigorous - 常に検出を修正する
safe - 安全な場合は検出を修正する、そうでない場合は保持する
normal - 安全な場合は検出を修正する、そうでない場合は確認する
none - 常にエンドユーザーに確認する

別の例として、引数ENABLEDまたはDISABLEDがあります。これらのパラメータは、特定の機能を有効または無効にする場合に使用します。

省略形/簡略化されたコマンド

eShellでは、コンテキスト、コマンド、およびパラメータを簡略化できます(パラメータはスイッチまたは代替オプションの場合に限る)。数値、名前、パスなどの具体的な値を持つパラメータやプレフィックスは簡略化できません。enabledおよびdisabled引数の代わりに、数値1 および 0を使用できます。

例

```
computer set real-time status enabled    =>  com set real stat 1
computer set real-time status disabled    =>  com set real stat 0
```

簡略形式の例:

例

```
computer set real-time status enabled    =>  com set real stat en
computer exclusions add detection-excludes object C:\path\file.ext    =>  com
excl add det obj C:\path\file.ext
computer exclusions remove detection-excludes 1    =>  com excl rem det 1
```

2つのコマンドまたはコンテキストが同じ文字で開始する(ADVANCEDやAUTO-EXCLUSIONSなどで、短縮コマンドとしてAを入力する)場合eShellでは、この2つのコマンドのいずれを実行するのかを特定できません。エラーメッセージおよび"A"で開始されているコマンドの一覧が表示されます。この一覧からコマンドを選択できます。

eShell>a

The following command is not unique: a

COMPUTERコンテキストで使用可能なサブコンテキストは次のとおりです。

ADVANCED

1文字以上追加(たとえば、AではなくAD)すると、現在一意であるためeShellはADVANCEDサブコンテキストを実行します。同じことが省略コマンドにも当てはまります。

注意

コマンドを要求どおりに確実に実行するには、コマンドやパラメータを省略形にせず、完全な形式を使用することをお勧めします。それによりeShellでコマンドが要求どおりに実行されて、無用な失敗がなくなります。このことは、バッチファイル/スクリプトで特に当てはまります。

自動入力

eShell 2.0 で導入されたこの新機能は、Windows コマンドプロンプトの自動補完によく似ています。Windows コマンドプロンプトではファイルパスが補完されますがeShellでは、コマンド、コンテキスト、および処理名も補完されます。引数の補完はサポートされていません。コマンドを入力するときにはTabキーを押すと使用可能なコマンドが補完されるか、使用可能な次のコマンド候補が表示されます。Shift + Tabを押すと、前のコマンドに戻ります。省略形と自動補完を併用することはできません。いずれかを使用してください。たとえば、computer real-time additionalと入力してTabを押しても、何も実行されません。かわりに、comと入力してTabを押すとcomputerが補完され、そのままreal + Tabadd + Tabと入力をしてEnterを押します。on + Tabを入力してEnterを押し続けると、on-execute-ahon-execute-ah-removableon-write-ahon-write-archive-defaultなどのすべての使用可能なバージョンを順番に表示されます。

エイリアス

エイリアスは、コマンドの実行に使用できる代替名です(コマンドにエイリアスが割り当てられている場合)。既定のエイリアスとして、次のものがあります。

```
(global) close - exit
(global) quit - exit
(global) bye - exit
warnlog - tools log events
virlog - tools log detections
```

(global)は、現在のコンテキストに関係なく、任意の場所でコマンドを使用できることを意味します。1つのコマンドには複数のエイリアスを割り当てることができます。たとえば、コマンドEXITには、エイリアスCLOSEQUITBYEがあります。eShellを終了するときには、EXITコマンド自体または任意のエイリアスを使用できます。エイリアスVIRLOGはコマンドDETECTIONSのエイリアスであり、TOOLS LOGコンテキストにあります。このように、検出コマンドはROOTコンテキストで使用でき、簡単にアクセスできます(TOOLSを入力して、LOGコンテキストに移動する必要がなく、ROOTから直接実行できます)。

eShellでは、独自のエイリアスを定義できます。コマンドALIASはUI ESHELLコンテキストにあります。

パスワードで保護された設定

ESET Server Security設定はパスワードで保護できます。[GUIでパスワード](#)を設定するか、set ui access lock-passwordを使用してeShellで実行できます。この後、特定のコマンドでこのパスワードを対話的に入力する必要があります(設定またはデータを変更するコマンドなど)。eShellを長期間使用する計画があり、パスワードを繰り返し入力したくない場合は、set passwordコマンド(rootから実行)を使用してeShellでパスワードを記憶できます。これで、パスワードが必要なコマンドを実行するたびに、パスワードが自動入力されます。これはeShellを終了するまで記憶されます。つまり、新しいセッションを開始し、eShellでパスワードを記憶するときには、set passwordをもう一度使用する必要があります。

Guide / Help

GUIDEまたはHELPコマンドを入力するとeShellの使用方法を説明する初期画面が表示されます。このコマンドは、ROOTコンテキスト(eShell>)からのみ使用できます。

コマンド履歴

eShellでは、前に実行したコマンドの履歴を保持しています。履歴の保持は、現在のeShell対話セッションにのみ適用されます。eShellを終了すれば、コマンド履歴は削除されます。履歴内の移動には、キーボードの上矢印キーおよび下矢印キーを使用します。目的のコマンドが見つかった場合は、それを再度実行することも、最初から全体を入力し直さないで変更することもできます。

CLS/画面の消去

CLSコマンドを使用すると画面を消去できます。Windowsのコマンドプロンプトや同じようなコマンドラインインタフェースの場合と同様の機能です。

EXIT / CLOSE / QUIT / BYE

eShellを閉じる、つまり終了する場合、この任意のコマンドを使用できます(EXITCLOSEQUITBYE)。

コマンド

このセクションではeShellのいくつかの基本的なコマンドと説明を示します。

注意

コマンドの大文字と小文字は区別されません。大文字と小文字のいずれも使用でき、コマンドは区別なく実行されます。

ROOTコンテキストに用意されているコマンドの例:

ABOUT

プログラムに関する情報が表示されます。次のような情報が表示されます。

- インストールされているESETセキュリティ製品の名前とバージョン番号。
- オペレーティングシステムと基本ハードウェア情報。
- ユーザー名(ドメインを含む)、完全コンピューター名(サーバーがドメインのメンバーの場合FQDN)シート名。
- 各コンポーネントのバージョン番号を含む、ESETセキュリティ製品のインストール済みコンポーネント。

コンテキストパス:

```
root
```

PASSWORD

パスワードで保護されたコマンドを実行する場合、通常は、セキュリティ上の理由でパスワードの入力を求められます。これは、保護を無効にするコマンドや、ESET Server Securityの設定に影響する可能性のあるコマンドに適用されます。このようなコマンドは、実行ごとにパスワードを要求します。毎回パス

ワードを入力しないために、パスワードをセットすることができます。セットしたパスワードは、eShellに記録されます。パスワードで保護されたコマンドを実行するときに、セットされたパスワードが自動的に使用されるため

注意

パスワードは、現在のeShell対話セッションに限って有効です。セットしたパスワードは、eShellを終了すると削除されます。eShellを再度開始した場合は、パスワードを再度セットする必要があります。

定義されたパスワードは、未署名のバッチファイル/スクリプトを実行するときにも使用できます。未署名のバッチファイルを実行するときには、必ず、[ESET Shell実行ポリシー](#)をフルアクセスに設定してください。下記に、パスワードのセットを含むバッチファイルの例を示します。

```
eshell set password plain <yourpassword> "&" computer set real-time status disabled
```

上記の連結されたコマンドは、パスワードを定義し、保護を無効にします。

重要

可能なかぎり、署名されたバッチファイルを使用することをお勧めします。このように、バッチファイルにプレーンテキストパスワードが含まれません(上記の方法を使用する場合)。詳細については、[バッチファイル/スクリプト](#) (署名されたバッチファイルセクションを参照してください)。

コンテキストパス:

root

構文:

```
[get] | restore password
```

```
set password [plain <password>]
```

操作:

get - パスワードを表示する

set - パスワードを設定または削除する

restore - パスワードをクリアする

引数:

plain - パラメータとしてパスワードを入力する方式に切り替える

password - パスワード

例:

set password plain <yourpassword> - パスワードで保護されたコマンドに使用するパスワードを設定する

restore password - パスワードをクリアする

例:

get password - パスワードが設定されているかどうかを確認する場合に使用します(アスタリス

ク"*"を表示するだけでパスワード自体は表示しません)。アスタリスクが表示されない場合は、パスワードは設定されていません。

`set password plain <パスワード>` - 定義したパスワードを設定する場合に使用します。

`restore password` - このコマンドは、定義したパスワードをクリアします。

STATUS

GUI同様、現時点におけるESET Server Securityのリアルタイムファイルシステム保護の状態に関する情報を表示します。また、保護の一時停止/再開もできます。

コンテキストパス:

```
computer real-time
```

構文:

```
[get] status
```

```
set status enabled | disabled [ 10m | 30m | 1h | 4h | temporary ]
```

```
restore status
```

操作:

`get` - 現在の設定/状態を表示する

`set` - 値/状態を設定する

`restore` - 既定の設定/オブジェクト/ファイルを復元

引数:

`enabled` - サーバー保護/機能の有効化

`disabled` - サーバー保護/機能の無効化

`10m` - 10分間無効にする

`30m` - 30分間無効にする

`1h` - 1時間無効にする

`4h` - 4時間無効にする

`temporary` - 再起動まで無効にする

注意

1つのコマンドですべての保護機能を無効にすることはできません。`status`コマンドを使用して、保護機能とモジュールを1つずつ管理できます。各保護機能またはモジュールには独自の`status`コマンドがあります。

`status`コマンドを使用して機能の一覧を表示します。

機能	コンテキストとコマンド
自動除外	COMPUTER AUTO-EXCLUSIONS STATUS
ホスト侵入防止システム(HIPS)	COMPUTER HIPS STATUS
リアルタイムファイルシステム保護	COMPUTER REAL-TIME STATUS
デバイスコントロール検査	DEVICE STATUS
ボットネット保護	NETWORK ADVANCED STATUS-BOTNET
ネットワーク攻撃保護(IDS)	NETWORK ADVANCED STATUS-IDS
ネットワーク隔離	NETWORK ADVANCED STATUS-ISOLATION
ESET Cluster	TOOLS CLUSTER STATUS
診断ロギング	TOOLS DIAGNOSTICS STATUS
プレゼンテーションモード	TOOLS PRESENTATION STATUS
フィッシング対策保護	WEB-AND-EMAIL ANTIPHISHING STATUS
電子メールクライアント保護	WEB-AND-EMAIL MAIL-CLIENT STATUS
Webアクセス保護	WEB-AND-EMAIL WEB-ACCESS STATUS

VIRLOG

これはDETECTIONSコマンドのエイリアスです。検出された侵入物に関する情報を表示する必要がある場合に有用です。

WARNLOG

これはEVENTSコマンドのエイリアスです。さまざまなイベントに関する情報を表示する必要がある場合に有用です。

バッチファイル/スクリプト

自動化用の強力なスクリプトツールとしてeShellを使用できます。eShellでバッチファイルを使用するには、バッチファイルを作成し、eShellとコマンドを記述します。

例
eshell get computer real-time status

コマンドを連鎖することもできます。これは必要な場合があります。例えば、特定のスケジュールタスクのタイプを取得する場合は、次のように入力します。

```
eshell select scheduler task 4 "&" get scheduler action
```

通常、項目の選択(この場合はタスク番号4)は、現在実行中のeShellのインスタンスにのみ適用されます。これらの2つのコマンドを順次実行すると、2番目のコマンドが失敗し、「タスクが選択されていないか、選択されたタスクが存在しません」というエラーが発生します。

セキュリティの理由のため、既定では、[実行ポリシー](#)は[制限されたスクリプト]に設定されています。これによりeShellを監視ツールとして使用できますが、スクリプトを実行してもESET Server Securityの構成を変更できません。保護の無効化などのセキュリティに影響する可能性があるコマンドでスクリプトを実行する場合は、**アクセスが拒否されました**というメッセージが表示されます。構成を変更するコマンドを実行するには、署名されたバッチファイルを使用することをお勧めします。

Windowsコマンドプロンプトで手動で入力した1つのコマンドを使用して設定を変更するにはeShellフルアクセスを付与する必要があります(非推奨)。フルアクセスを付与するにはeShell自体のインタラクティ

ブモードまたは**詳細設定 (F5)> ユーザーインターフェース > ESET Shell**のGUIで、`ui eshell shell-execution-policy`を使用します。

署名されたバッチファイル

eShellでは、署名を使用して、一般的なバッチファイル(*.bat)を保護できます。スクリプトは、設定保護で 사용되는ものと同じパスワードで署名されます。スクリプトに署名するには、まず、**設定保護**を有効にする必要があります。この操作は、GUIを使用するかeShell内から`set ui access lock-password`コマンドを使用して実行します。設定保護パスワードが設定されると、バッチファイルの署名を開始できます。

注意

設定保護パスワードを変更する場合は、すべてのスクリプトにもう一度署名する必要があります。そうでない場合、パスワードを変更した後から、スクリプトを実行できなくなります。スクリプトに署名するときに入力されたパスワードは、ターゲットシステムの設定保護パスワードと一致する必要があります。

バッチファイルを署名するにはeShellのルートコンテキストから`sign <script.bat>`を実行します。**script.bat**は、署名するスクリプトへのパスです。署名で使用するパスワードを入力して確認します。このパスワードは、設定保護パスワードと一致する必要があります。署名は、コメントの形式でバッチファイルの最後に配置されます。このスクリプトが以前に署名されている場合は、署名が新しい署名で置換されます。

注意

以前に署名されたバッチファイルを修正する場合は、もう一度署名する必要があります。

Windowsコマンドプロンプトから署名されたバッチファイルを実行するか、スケジュールタスクとして実行するには、次のコマンドを使用します。

```
eshell run <script.bat>
```

script.batはバッチファイルへのパスです。

例

```
eshell run d:\myeshellscript.bat
```

ESET SysInspector

ESET SysInspectorは、コンピュータを徹底的に検査し、インストールされているドライバーやアプリケーション、ネットワーク接続、重要なレジストリーエントリなどのシステムコンポーネントについて詳細な情報を収集し、コンポーネントごとのリスクレベルを評価するアプリケーションです。この情報で、ソフトウェアやハードウェアの互換性の問題やマルウェア感染が原因と思われる疑わしいシステム動作を判別することができます。

作成をクリックし、作成するログについての簡単な**コメント**を入力してESET SysInspectorログが生成される(作成済みの状態)までお待ちください。ハードウェア構成とシステムデータによっては、ログの作成に時間がかかる場合があります。

ESET SysInspectorウィンドウには作成されたログに関する次の情報が表示されます。

- **日時** – ログ作成時刻。
- **コメント** – 短いコメント。
- **ユーザー** – ログを作成したユーザーの名前。
- **状態** – ログ作成の状態。

使用できるアクションは次のとおりです。

- **表示** – 作成したログを開きます。また、ログを右クリックして、メニューから[表示]を選択できます。
- **比較** – 既存の2つのログを比較します。
- **作成** – 新しいログを作成します。作成するログを説明する簡潔なコメントを入力し、[作成]をクリックします。ESET SysInspectorログが終了する(作成済みの[状態])までお待ちください。
- **削除** – 選択したログをリストから削除します。

選択した1つ以上のログを右クリックすると、コンテキストメニューから次の追加オプションを使用できます。

- **表示** - ESET SysInspectorで選択したログを開きます(ログをダブルクリックするのと同じ機能)。
- **比較** – 既存の2つのログを比較します。
- **作成** – 新しいログを作成します。作成するログを説明する簡潔なコメントを入力し、[作成]をクリックします。ESET SysInspectorログが終了する(作成済みの[状態])までお待ちください。
- **削除** – 選択したログをリストから削除します。
- **すべて削除** – すべてのログを削除します。
- **エクスポート** - .xmlファイルまたは圧縮された.xmlにログをエクスポートします。

ESET SysRescue Live

[ESET SysRescue Live](#) は無償のユーティリティであり、ブータブルレスキューCD/DVDまたはUSBドライブを作成できます。レスキューメディアから感染したコンピューターを起動した後に、マルウェアを検査し、感染したファイルを駆除できます。

ESET SysRescue Liveの主な利点は、ESETセキュリティソリューションがホストオペレーティングシステムから独立して稼動し、ディスクおよびファイルシステムに直接アクセスできることにあります。本機能は、たとえばオペレーティングシステムの実行中など、通常は削除できない脅威を削除することができます。

スケジューラ

スケジューラーは、定義されたパラメーターに従って、スケジュールされたタスクを管理および起動します。スケジューラーには、タスクタイプ、タスク名、起動時刻、前回実行日時などのパラメーターを示す表形式ですべてのスケジュールされたタスクが一覧表示されます。また、新しいスケジュールされたタスクを作成するには、[タスクの追加](#)をクリックします。既存のスケジュールされたタスクの設定を編集するには、**編集**ボタンをクリックします。スケジュールされたタスクのリストを既定の設定に戻し、**既定**に既定に戻すをクリックします。行われたすべての変更は失われ、元に戻せません。

定義済みの既定のタスクのセットを示します。

- ログの保守
- 定期自動アップデート(このタスクを使用して、[頻度をアップデート](#))
- ダイアルアップ接続後に自動アップデート
- ユーザーログオン後に自動アップデート

- 自動スタートアップファイルのチェック（ユーザーのログオン後）
- 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後）

注意

該当するチェックボックスを選択して、タスクを有効/無効にします。



次のアクションを実行するには、タスクを右クリックします。

タスクの詳細を表示	スケジュールされたタスクをダブルクリックまたは右クリックするときに、スケジュールされたタスクに関する詳細を表示します。
今すぐ実行	選択したスケジューラータスクを実行し、タスクをだちに実行します。
追加...	スケジューラータスクの作成 を支援するウィザードが起動します。
編集...	既存のスケジュールされたタスク(既定のタスクおよびユーザー定義のタスク)の設定を編集します。
削除	既存のタスクを削除します。

スケジューラー – タスクの追加

新しいスケジュールタスクを作成する

1. **タスクの追加**をクリックします。
2. **タスク名**を入力し、カスタムスケジュールされたタスクを設定します。
3. **タスクタイプ** – ドロップダウンメニューから、該当する**タスクタイプ**を選択します。

スケジューラ - ESET File Security

タスク詳細

タスク名

タスクの種類 外部アプリケーションの実行

有効 ☒

戻る 次へ キャンセル

注意

タスクを無効にするには、**有効**の横のスライダーをクリックします。[スケジューラービュー](#)のチェックボックスをクリックします。

4. [タスクのタイミング](#) - タスクを実行するタイミングを定義するオプションのいずれかを選択します。選択内容によって、特定の時刻、曜日、間隔、またはイベントを選択する必要があります。

スケジューラ - ESET File Security

タスクタイミング

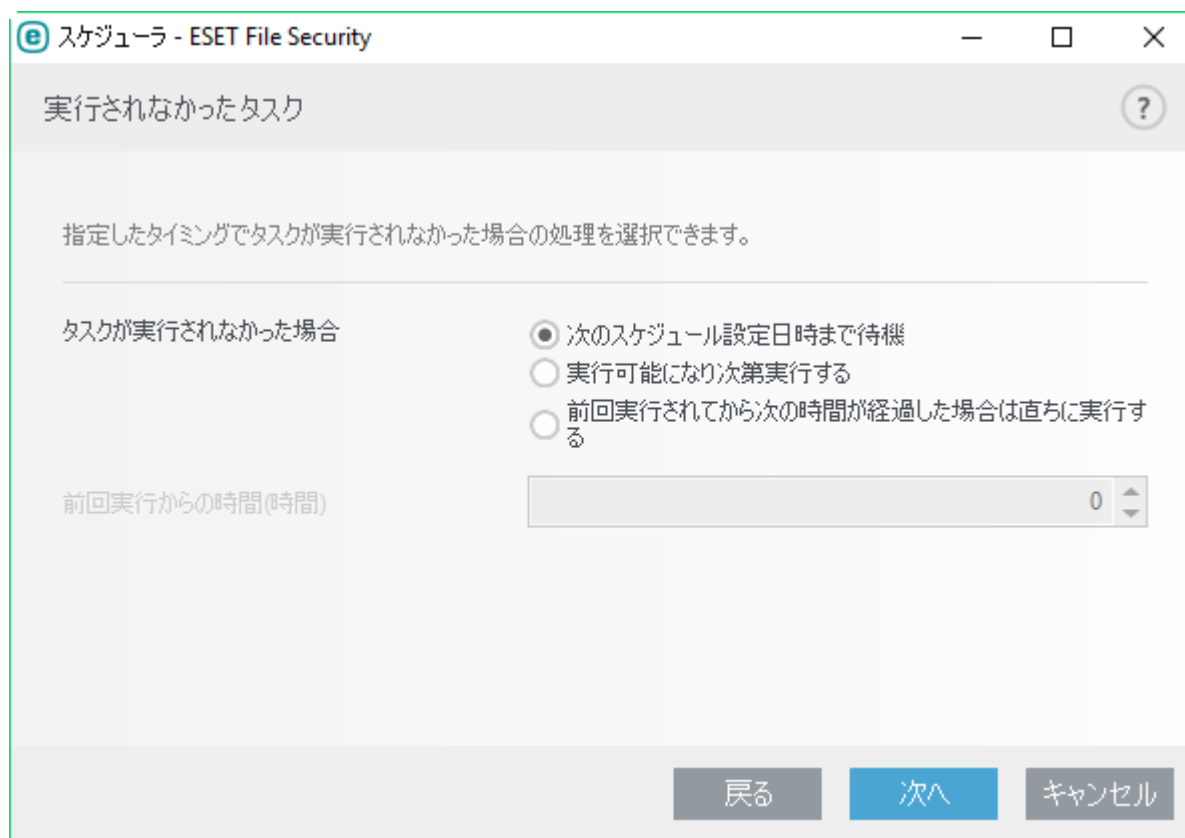
実行するスケジュールタスク

☒ 1回
☐ 繰り返し
☐ 毎日
☐ 毎週
☐ イベントごと

コンピューターがバッテリーで動作している場合は実行しない ☐

戻る 次へ キャンセル

5. [スキップされたタスク](#) - あらかじめ定義した時刻にタスクが実行されなかった場合、[タスクを実行する時期を指定](#)することができます。



6. [アプリケーションの実行](#) - タスクが外部アプリケーションを実行するようにスケジュールされている場合、ディレクトリツリーから実行ファイルを選択します。

7. 変更する必要がある場合は、**戻る**をクリックして、前の手順に戻り、パラメーターを修正します。

8. **完了**をクリックすると、タスクを作成するか、変更を適用します。

新しいスケジュールされたタスクが[スケジューラー](#)ビューに表示されます。

タスクの種類

設定ウィザードは、スケジュールされたタスクの[タスクタイプ](#)によって異なります。**タスク名**を入力し、ドロップダウンメニューから任意の**タスクタイプ**を選択します。

- **外部アプリケーションの実行** - 外部アプリケーションの実行をスケジュールします。
- **ログの保守** - ログファイルには削除されたレコードの痕跡も収められています。このタスクは、効率的に運用するためにログファイル内のレコードを定期的に最適化します。
- **システムスタートアップファイルのチェック** - システムの起動時またはログインに実行されるファイルを検査します。
- **コンピューターのステータススナップショットを作成する** - ドライバやアプリケーションなどのシステムコンポーネントについての情報を収集し、各コンポーネントのリスクレベルを評価するcreates an ESET SysInspector コンピュータスナップショットを作成します。
- **コンピューターの検査** - コンピューター上のファイルやフォルダに関するコンピューターの検

査を実行します。

- **アップデート** - 検出エンジンおよびプログラムモジュールをアップデートすることにより、アップデートタスクをスケジュールします。
- **Hyper-V検査** - [Hyper-V](#)内の仮想ディスクの検査をスケジュールします。
- **OneDrive検査** - [OneDrive](#)に格納された検査ファイルをスケジュールします。

作成された時点でタスクを無効にするには、**有効**の横のスイッチをクリックします。[スケジューラー](#)ビューのチェックボックスをクリックすると、後からタスクを有効にできます。**[次へ]**をクリックして、[次の手順](#)に進みます。

タスクの実行

次のタイミングオプションのいずれかを選択します。

- **1回のみ** - 指定された日時に1回だけタスクが実行されます。**タスク実行**で1回かぎりの開始日時を指定します。
- **繰り返し** - 指定した間隔(分)でタスクが実行されます。**タスク実行**で、毎日タスクが実行される時刻を指定します。
- **毎日** - 毎日、指定した時刻に繰り返しタスクが実行されます。
- **毎週** - 1週間に1回以上、選択した曜日と時刻にタスクが実行されます。指定された日時から開始する、特定の曜日にのみ繰り返しタスクを実行します。タスク実行の時刻に開始時刻を指定します。タスクが実行される曜日(複数可)を選択します。
- [トリガーされたイベント](#) - 指定したイベントが発生すると、タスクが実行されます。

コンピューターがバッテリーで動作している場合は**実行しない**を有効にすると、タスクの実行時にコンピューターがバッテリーで動作している場合は、タスクが開始されません。これはUPSなどで実行されるコンピューターに適用されます。

トリガーされたイベント

イベントによって開始されるタスクをスケジュールする際には、タスクを実行する最短間隔を指定することができます。

次のイベントのいずれかによってタスクを開始できます。

- **コンピュータの起動時**
- **その日の最初のコンピュータ起動時**
- **インターネット/VPNへのダイヤルアップ接続**
- **モジュールアップデートが成功しました。**
- **製品アップデート成功**
- **ユーザーログオン** - このタスクは、ユーザーがシステムにログオンするときに展開されます。1日に複数回、コンピューターにログオンする場合、その日および翌日の初回ログオン時にのみ

タスクを実行するには、24時間を選択します。

- ウイルス検出

アプリケーションの実行

このタスクでは、外部アプリケーションの実行をスケジュールすることができます。

- **実行可能ファイル-参照(...)**をクリックするか手動でパスを入力して、ディレクトリツリーから実行可能ファイルを選択します。
- **作業フォルダ** – 外部アプリケーションの作業ディレクトリを指定します。選択した[**実行可能ファイル**]のすべての一時的なファイルは、このディレクトリに作成されます。
- **パラメーター** – アプリケーションのコマンドラインパラメーター(任意)。

タスクが実行されなかった場合

あらかじめ定義した時刻にタスクが実行されなかった場合、タスクを実行する時期を指定することができます。

- **次のスケジュール設定日時** – タスクは、指定された時刻に実行されます(24時間後など)。
- **実行可能になり次第実行する** – タスクは、タスクの実行を阻んでいるアクションが無効になりしだい実行されます。
- **前回実行されてから次の時間が経過した場合は直ちに実行する** – **前回実行からの時間(時間)** – このオプションを選択した場合は、指定した時間(時間単位)が経過するとタスクが必ず反復されます。

スケジュールタスクの概要

スケジューラービューでタスクをダブルクリックするか、スケジュールされたタスクを右クリックして**タスク詳細を表示する**を選択すると、このダイアログウィンドウには、スケジュールされたタスクの詳細が表示されます。

分析のためにファイルを提出

ファイルの提出ダイアログから、ファイルまたはサイトをESETに送信できます。コンピュータ上の動作が疑わしいファイル、またはインターネット上の疑わしいサイト見つかった場合は、ESETのウイルスラボに提出して解析を受けることができます。そのファイルが悪意のあるアプリケーションやWebサイトであることが判明すると、その後のアップデートファイルにその検出が追加されます。

メールでファイルを提出することもできます。WinRARまたはWinZipなどのプログラムを使用してファイルを圧縮し、「*infected*」というパスワードでアーカイブを保護して、samples@eset.comに送信します。わかりやすい件名にし、ファイルに関する情報(ダウンロード元のWebサイトなど)をできるだけ多く記載してください。

ESETにサンプルを提出する前に、次の基準の1つ以上を満たしていることを確認してください。

- ファイルまたはWebサイトがまったく検出されない

- ファイルまたはWebサイトが誤って脅威として検出される

上記の要件の少なくとも1つが満たされていない場合、詳細が提供されるまで回答を受信しません。

以下の[サンプル提出の理由]ドロップダウンメニューから、お客様が伝えたい内容に最も近いものを選択します。

- [不審なファイル](#)
- [不審なウェブサイト](#) (何らかのマルウェアに感染しているWebサイト)
- [誤検出ファイル](#) (感染と検出されたが未感染であるファイル)
- [誤検出サイト](#)
- [その他](#)

ファイル/サイト

提出するファイルその他Webサイトへのパスを入力します。

連絡先の電子メール

不審なファイルと共に連絡先のメールアドレスをESETに送信します。解析のために詳しい情報が必要な場合、このメールアドレスに連絡がある場合があります。メールアドレスの入力は任意です。詳しい情報が必要でない限り、ESETから連絡することはありません。毎日、何万ものファイルがサーバーに送られてくるので、すべての提出に返信することはできません。

匿名で送信する

匿名で送信するチェックボックスを使用し、自分の電子メールアドレスを入力せずに、不審なファイルやWebサイトを送信します。

不審なファイル

観察されたマルウェア感染の兆候および症状

コンピューター上にある不審なファイルの動作の説明を入力します。

ファイルの入手元(URLアドレスまたはベンダ)

ファイルの入手元(ソース)と、このファイルを入手方法のメモを入力してください。

備考および補足情報

ここには、不審なファイルの判別処理の助けとなる追加情報または説明を入力します。

注意

1つ目のパラメーターである[観察されたマルウェア感染の兆候および症状]は必須ですが、補足情報もご提供いただくと、研究所でのサンプルの特定および処理に非常に役立ちます。

不審なサイト

[サイトの問題点]ドロップダウンメニューで以下のうち1つを選択してください。

感染

ウイルス、またはさまざまな方法で配布される他のマルウェアが含まれるWebサイト。

フィッシング

銀行の口座番号やPINコードなどの機密データを入手するためによく使用されます。この攻撃の詳細については、「[用語集](#)」を参照してください。

詐欺

不正または詐欺Webサイト。

その他

上記のオプションのいずれも送信するサイトに該当しない場合は、このオプションを選択します。

備考および補足情報

ここには、不審なWebサイトを分析するときの助けとなる追加情報または説明を入力します。

誤検出ファイル

感染していると検出され、実際には感染していないファイルは、検出エンジンの向上と他のお客様の保護のために、送信してくださるようお願いいたします。ファイルのパターンが検出エンジンのパターンと一致する場合、誤検出(FP)が発生する場合があります。

注意

指定 3つのパラメーターは、アプリケーションが正当なものであるかどうかを識別し、悪意のあるコードと区別するために必要です。補足情報をご提供いただくと、研究所でのサンプルの特定および処理の際に大いに役立ちます。

アプリケーション名およびバージョン

プログラム名とバージョン(番号、エイリアスまたはコード名など)。

ファイルの入手元(URLアドレスまたはベンダ)

ファイルの入手元(ソース)と、このファイルを入手方法のメモを入力してください。

アプリケーションの目的

アプリケーションの概要、アプリケーションの種類(ブラウザ、メディアプレーヤなど)、その機能などを入力します。

備考および補足情報

ここには、不審なファイル进行处理する際に役立つ追加情報または説明を入力できます。

誤検出サイト

感染、詐欺、またはフィッシングサイトと検出され、実際には感染していないサイトは、送信することをお勧めします。サイトのパターンが検出エンジンのパターンと一致する場合、誤検出(FP)が発生する

場合があります。検出エンジンの向上と他のお客様の保護のために、そのようなWebサイトはご報告ください。

備考および補足情報

ここには、不審なファイル进行处理の際に役立つ追加情報または説明を入力できます。

その他

ファイルを[不審なファイル]または[誤検出]に分類できない場合は、このフォームを使用します。

ファイル提出の理由

ファイル送信に関する詳細な説明と送信理由を入力します。

隔離

隔離の主な機能は、感染ファイルを安全に保存することにあります。ファイルを駆除できない場合、ファイルの削除が安全でもなければ推奨もされない場合ESET Server Securityによって誤検出される場合、ファイルを隔離する必要があります。任意のファイルを選択して隔離することができます。これは、ファイルの動作が疑わしいにもかかわらず、マルウェア対策スキャナーによって検出されない場合にお勧めします。隔離したファイルは、ESETのウイルスラボに提出して分析を受けることができます。



日時	オブジェクト名	サイズ	原因	数	ユーザーアカウント
01/02/2019 ...	http://2016.eicar.org/...				KRC-EFSW\Administrator
01/02/2019 ...	http://2016.eicar.org/...				KRC-EFSW\Administrator
01/02/2019 ...	http://2016.eicar.org/...				KRC-EFSW\Administrator
01/02/2019 ...	C:\Users\ADMINI~1\...				KRC-EFSW\Administrator
01/02/2019 ...	C:\Users\Administra...				KRC-EFSW\Administrator
01/02/2019 ...	C:\Users\ADMINI~1\...				KRC-EFSW\Administrator
01/02/2019 ...	C:\Users\Administra...				KRC-EFSW\Administrator
01/06/2018 ...	http://www.eicar.org/downlo...	308 B	Eicar test file	1	NT AUTHORITY\SYSTEM
01/06/2018 ...	C:\Users\Administrator\AppData...	8.0 kB	Eicar test file	1	KRC-EFSW\Administrator
01/06/2018 ...	C:\Users\ADMINI~1\AppData\...	184 B	Eicar test file	1	KRC-EFSW\Administrator
01/06/2018 ...	http://www.eicar.org/downlo...	68 B	Eicar test file	1	NT AUTHORITY\SYSTEM

隔離フォルダーに保存されているファイルは、隔離の日時、感染ファイルの元の場所のパス、ファイルサイズ(バイト単位)、理由("ユーザーによって追加されました"など)、およびウイルスの数(複数のマルウェアが紛れ込んだアーカイブの場合など)が表示されるテーブルで参照することができます。

電子メールメッセージオブジェクトがファイル隔離に隔離される場合は、メールボックス/フォルダー/ファイル名へのパスが表示されます。

ファイルの隔離

ウイルス検出によって削除されたファイルは、ESET Server Securityにより自動的に隔離されます(警告ウィンドウでユーザーがこのオプションを無効にしなかった場合)。**[隔離]** ボタンをクリックして不審なファイルを手動で隔離することができます。隔離されているファイルを、元の場所から削除できます。この操作にはコンテキストメニューも使用することができます。**[隔離]** ウィンドウ内で右クリックし、**[隔離]** を選択します。

隔離フォルダからの復元

隔離されているファイルを、元の場所に復元することもできます。**[復元]** 機能を使用すると、**[隔離]** ウィンドウで特定のファイルを右クリックして、コンテキストメニューから選択することができます。ファイルが[望ましくない可能性があるアプリケーション](#)に設定されている場合、**[復元して検査から除外]** オプションも使用できます。コンテキストメニューには、**[復元先を指定...]** オプションもあります。このオプションを使用すると、隔離される前の場所とは異なる場所にファイルを復元することができます。

注意

害のないファイルが誤って隔離された場合は、そのファイルを復元した後で[検査から除外](#)し、ESET カスタマーサポートに送信してください。

隔離からのファイルの提出

プログラムによって検出されなかった疑わしいファイルを隔離した場合や、ファイルが(コードのヒューリスティック分析などによって)感染していると誤って評価されて隔離された場合は、そのファイルをESETのウイルスラボに送信してください。隔離フォルダーからファイルを提出するには、ファイルを右クリックし、コンテキストメニューから[分析のためにファイルを提出](#)を選択します。

隔離フォルダからの削除

特定の項目を右クリックし、**[隔離から削除]** を選択するか、削除する項目を選択し、キーボードの **Delete** を押します。

OneDrive検査の設定

ESET Server Securityを開く

設定 > サーバ > **OneDrive検査設定** をクリックする



この機能により、[Microsoft OneDrive for Business](#) クラウドストレージに保存されたファイルを検査できます。ESET Server Security OneDrive検査でファイルとフォルダーのみを処理する必要があります。電子メール、SharePointファイル、連絡先、予定表などの他の種類のデータは検査されません。

クイックリンク

[ESET OneDrive スキャナーの登録](#)

[ESET OneDrive スキャナーの登録解除](#)

ESET Server Security OneDrive検査を使用し始めるには、[ESET OneDrive スキャナー](#) アプリケーションをMicrosoft OneDrive / Microsoft Office 365 / Microsoft Azureに登録します。OneDrive検査設定ページには、登録状況(既に登録されている場合)、登録詳細(テナントID、アプリケーションID、オブジェクトID)および

び証明書サムプリント)が表示されます。ESET OneDrive スキャナーを登録または登録解除できます。



登録の成功後、フォルダー構造でユーザーと、検査対象として選択できるファイルの一覧を表示する [検査](#) メニューで、OneDrive 検査を使用できるようになります。ESET Server Security OneDrive 検査は、OneDrive for Business のユーザーによって並べ替えられた任意のファイルを検査できます。

注意

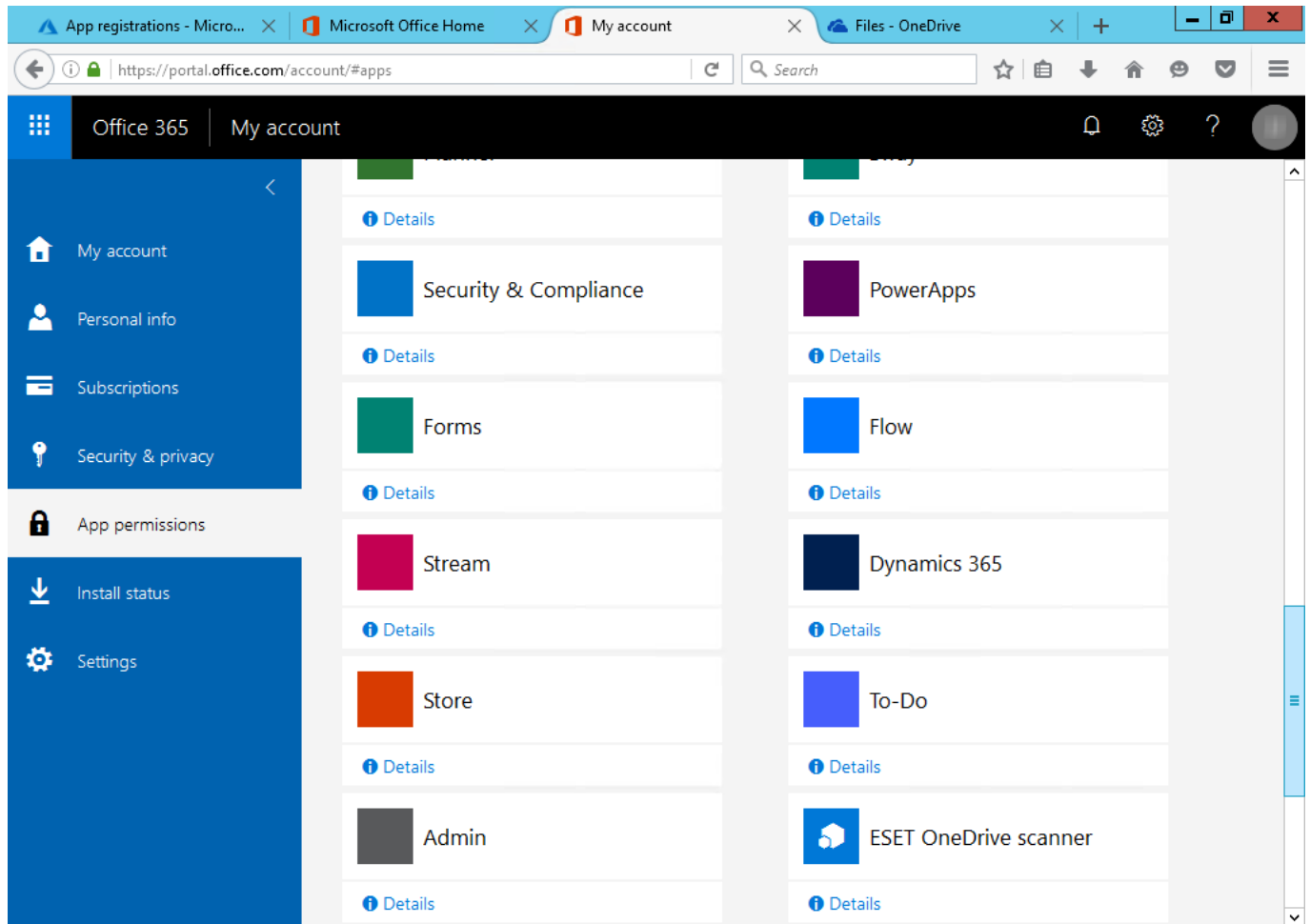
ESET Server Security OneDrive 検査は、OneDrive for Business クラウドストレージからファイルをダウンロードし、ローカルで検査を実行します。検査が完了すると、ダウンロードされたファイルは削除されます。OneDrive から大量のデータをダウンロードすると、ネットワークトラフィックに影響します。

注意

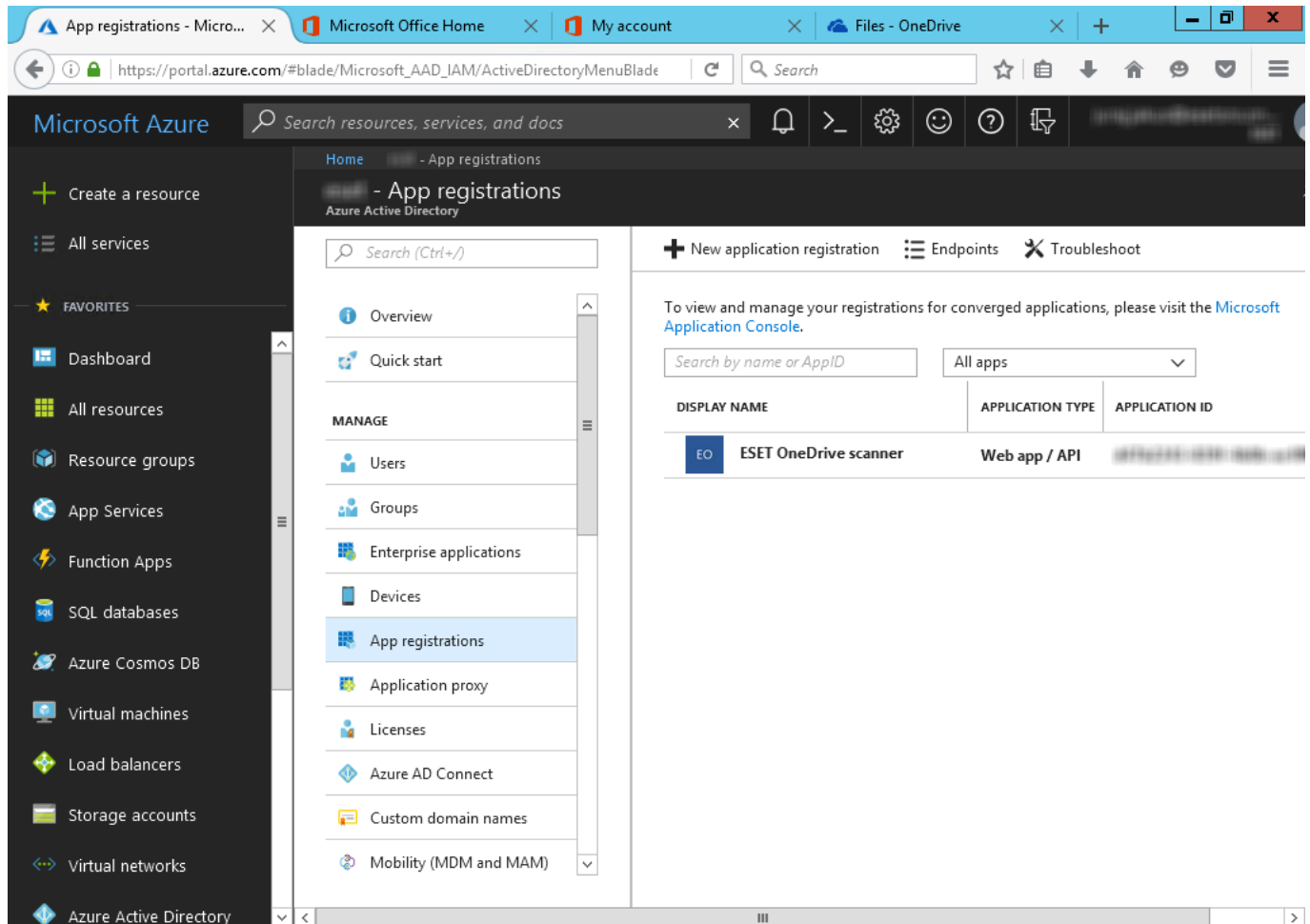
別のアカウントで再登録します。ESET Server Security OneDrive スキャナーを新しい Microsoft OneDrive for Business / Office 365 アカウントに登録する場合は、以前のアカウントを使用していた [ESET OneDrive スキャナーを登録解除](#) し、新しい Microsoft OneDrive for Business / Office 365 管理者アカウントで [登録](#) する必要があります。

Office 365 および Azure でアプリケーションとして登録された ESET OneDrive スキャナーを見つけることができます。

[Office 365 ポータル](#) - [マイアカウント] ページで [アプリ権限](#) をクリックすると ESET OneDrive スキャナー アプリが一覧表示されます。



[Azure](#) - **Azure Active Directory** > **アプリの登録**に移動し、**すべてのアプリケーションを表示**をクリックするとESET OneDriveスキャナーアプリが一覧に表示されます。アプリをクリックすると、詳細が表示されます。



ESET OneDrive スキャナーの登録

ESET Server Securityを開く

設定 > サーバ > OneDrive 検査設定 > 登録をクリックする



次に、Microsoft OneDrive / Office 365 / AzureでのESET OneDriveスキャナーアプリの登録処理を示します。

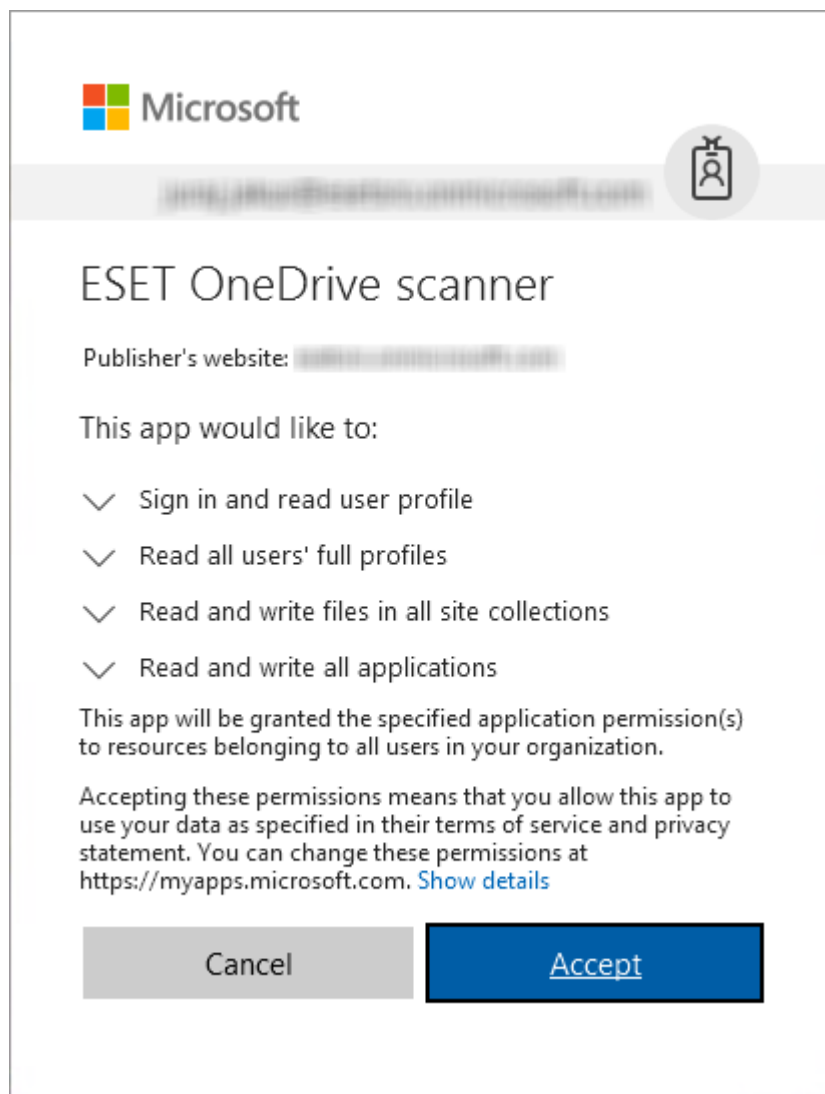
- **登録**をクリックし、ESET OneDriveスキャナー登録処理を開始します。登録ウィザードが開きます。



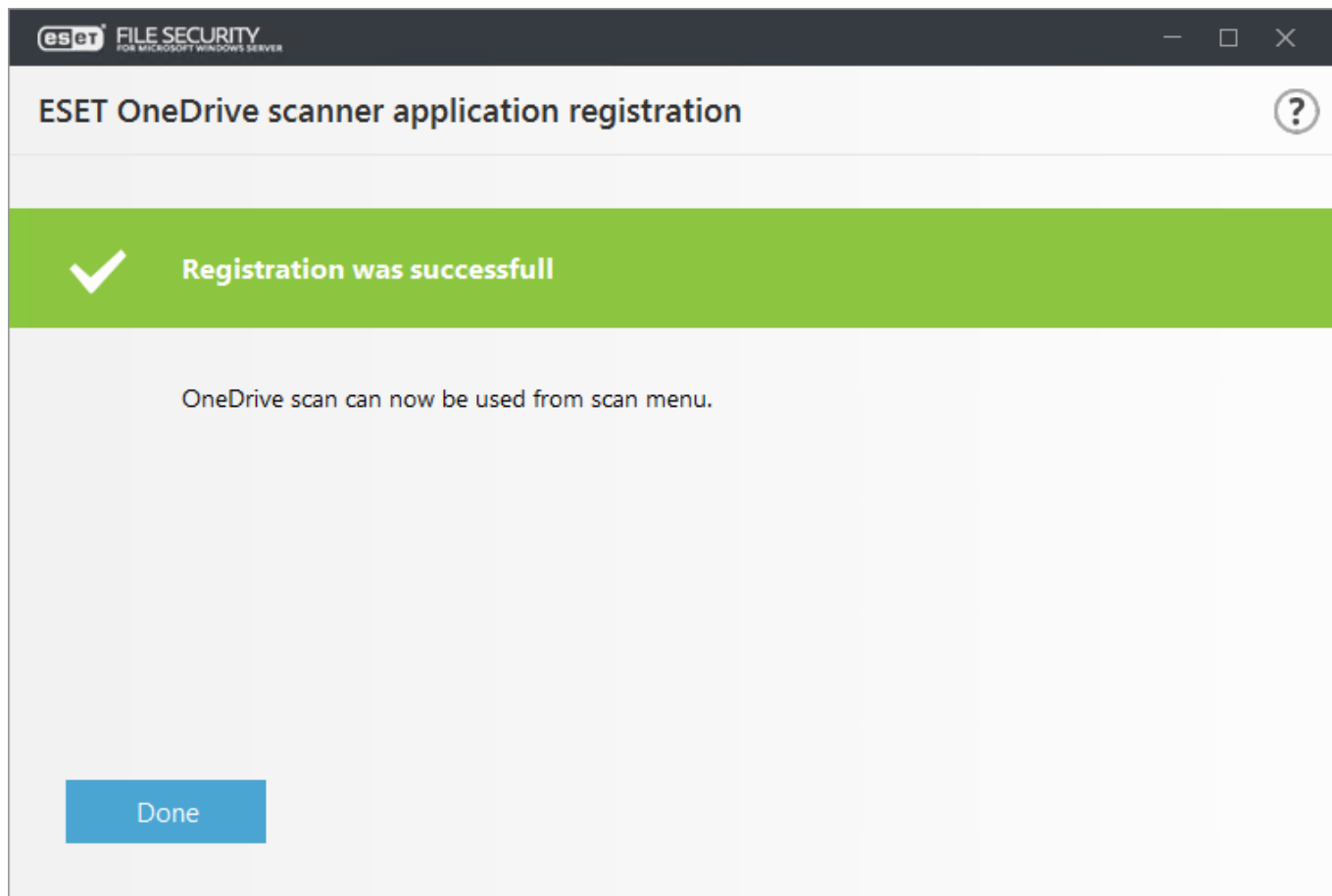
- Microsoft OneDrive / Office 365 管理者アカウント資格情報を入力します。Microsoft OneDrive へのアプリケーション登録が完了するまで待機します。



- Webブラウザで、Microsoftの**アカウントの選択**ページが開きます。使用しているアカウントをクリック(該当する場合)するか**Microsoft OneDrive / Office 365管理者アカウント資格情報**を入力し、**サインイン**をクリックします。
- ESET OneDrive スキャナーアプリでは、許可メッセージに一覧表示される4種類の権限が必要です。**許可**をクリックすると**ESET Server Security OneDrive スキャナー**は、**OneDrive クラウドストレージ**にあるデータにアクセスできます。



- Webブラウザでこの情報を送信するように指示された場合は、**続行**をクリックします(ESET Server Securityがアプリケーション登録が成功したことを認識できるようにlocalhostにのみ送信されます)。
- Webブラウザを閉じると**ESET OneDrive スキャナー登録ウィザード**で、登録が成功しましたというメッセージが表示されます。**完了**をクリックします。



注意

ESET OneDrive スキャナー登録処理は、Microsoft のポータル (OneDrive、Office 365、Azure など) にログインしているかによって、特定の状況で異なる場合があります。登録ウィザードウィンドウの画面の指示およびメッセージに従ってください。

ESET OneDrive スキャナー登録中に次のエラーメッセージが発生する場合は、提案された想定されたソリューションについて、エラーメッセージ詳細を参照してください。

エラーメッセージ	エラーメッセージ詳細
予期しないエラーが発生しました。	ESET Server Security で問題が発生した可能性があります。しばらくたってから ESET OneDrive スキャナー登録を再試行してください。問題が解決しない場合は、ESET テクニカルサポートに連絡してください。
インターネット接続がありません。	ネットワーク/インターネット接続を確認し、ESET OneDrive スキャナー登録を再実行してください。
Microsoft OneDrive で予期しないエラーが発生しました。	HTTP 4xx エラーが返され、エラーメッセージ応答に応答がありません。この問題が解決しない場合は、ESET テクニカルサポートに連絡してください。
Microsoft OneDrive で次のエラーが発生しました。	Microsoft OneDrive サーバーは、特定のエラーコード/名前エラーを返しました。 エラーを表示 をクリックしてください。
セットアップタスクはタイムアウトしました。	ESET OneDrive スキャナー登録設定タスクに時間がかかりすぎています。しばらくたってから ESET OneDrive スキャナー登録を再試行してください。
セットアップタスクはキャンセルされました。	実行中の登録タスクをキャンセルしました。登録を完了する場合は、ESET OneDrive スキャナー登録を再試行してください。
別のセットアップタスクがすでに実行中です。	登録タスクは既に実行中です。最初の登録処理が完了するまでお待ちください。

ESET OneDrive スキャナーの登録解除

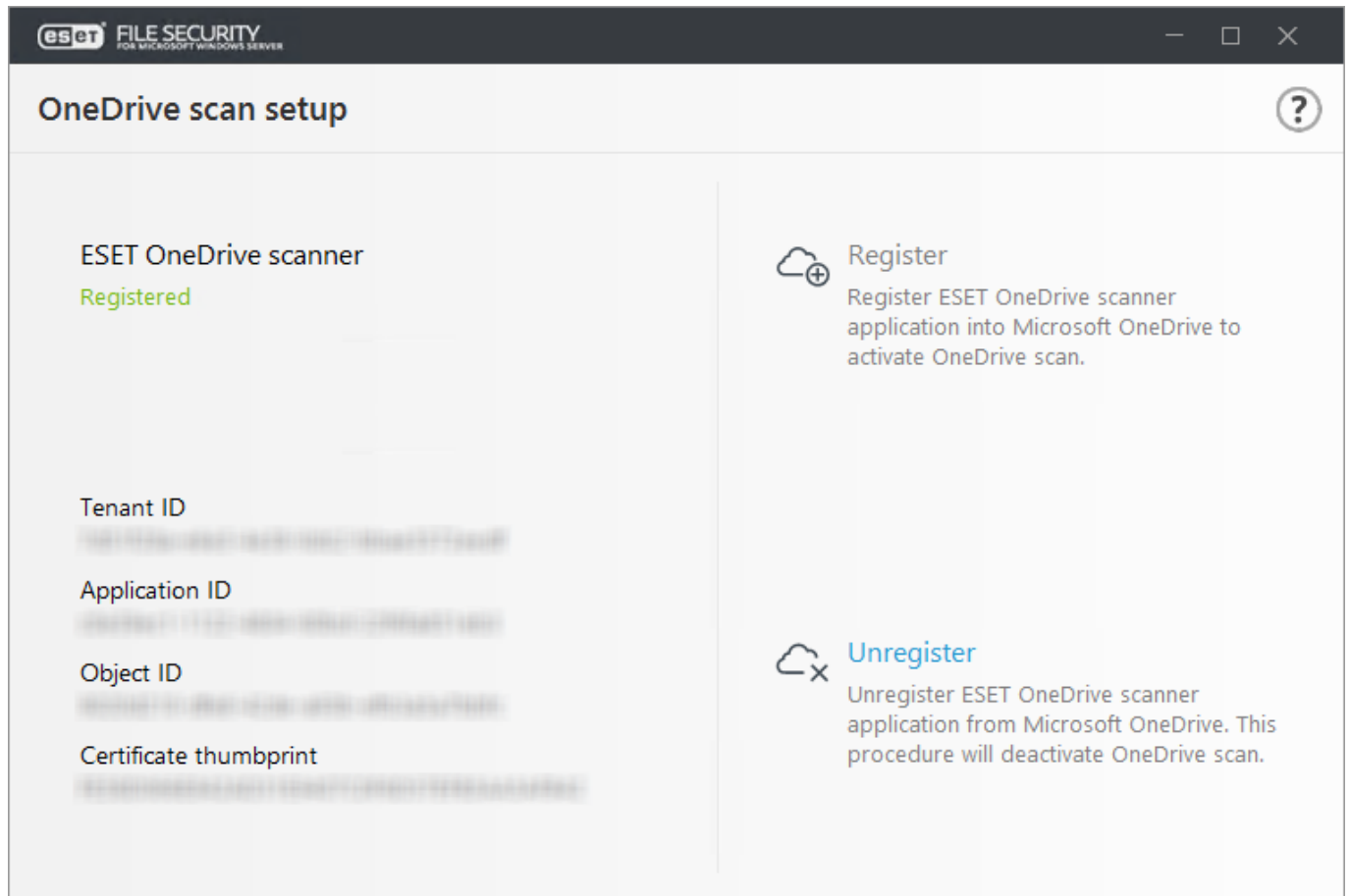
ESET Server Securityを開く

設定 > サーバ > OneDrive 検査設定 > 登録解除をクリックする

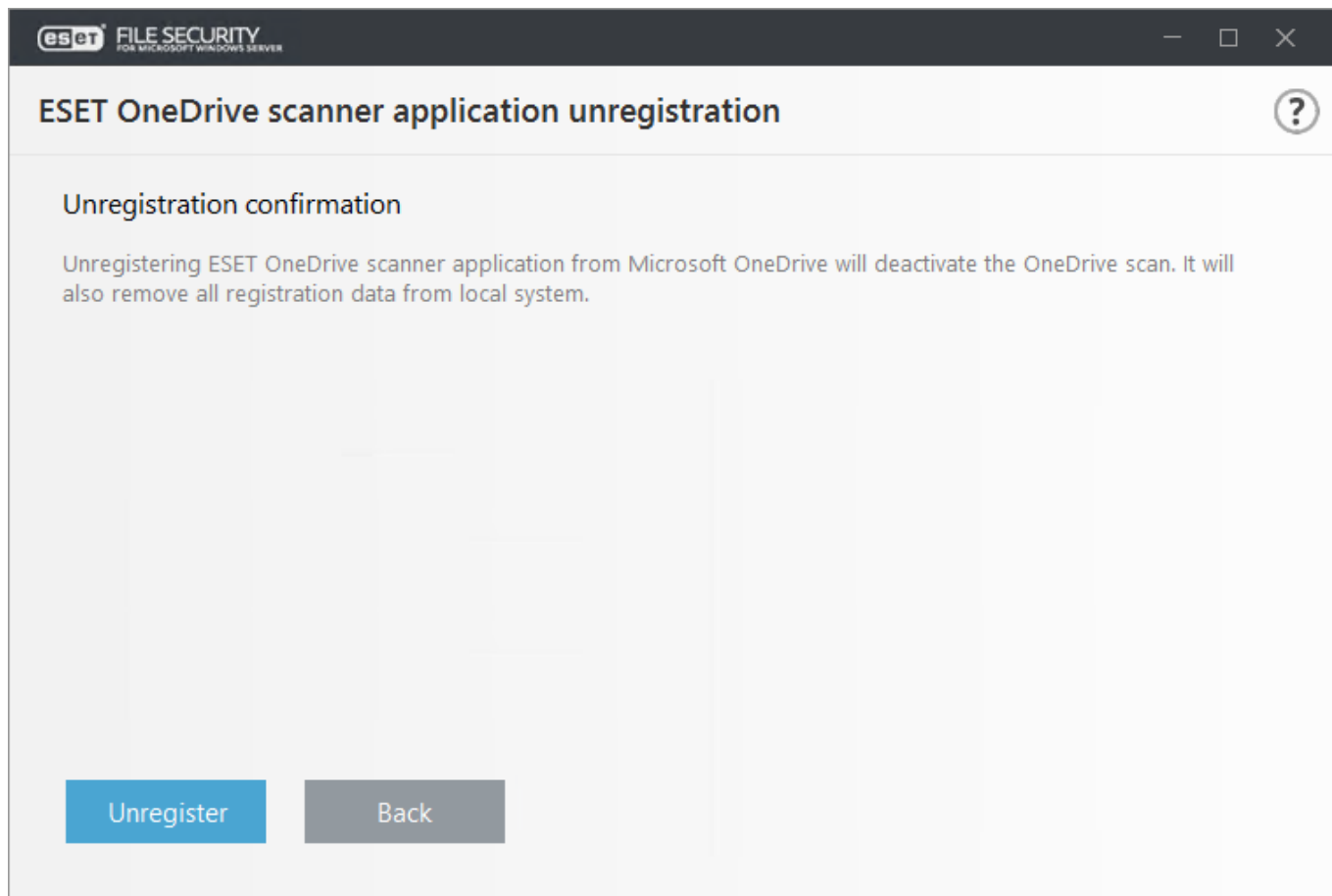


登録解除処理ではMicrosoft OneDrive / Office 365 / Azureから証明書とESET OneDrive スキャナーアプリを削除できます。この処理では、ローカル依存関係を削除し、登録オプションをもう一度使用可能にします。

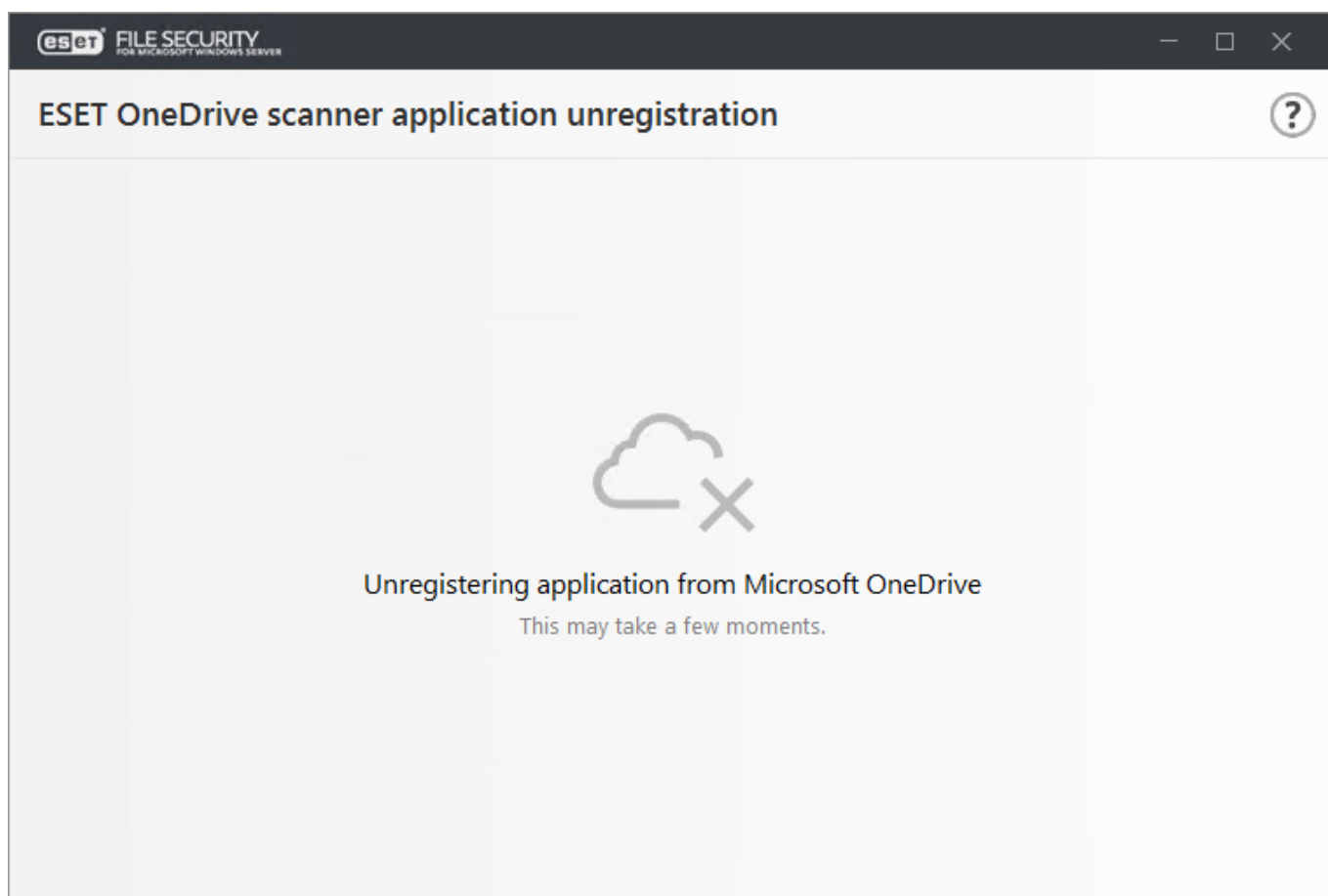
- **登録解除**をクリックし、ESET OneDrive スキャナー登録解除/削除処理を開始します。登録解除ウィザードが開きます。



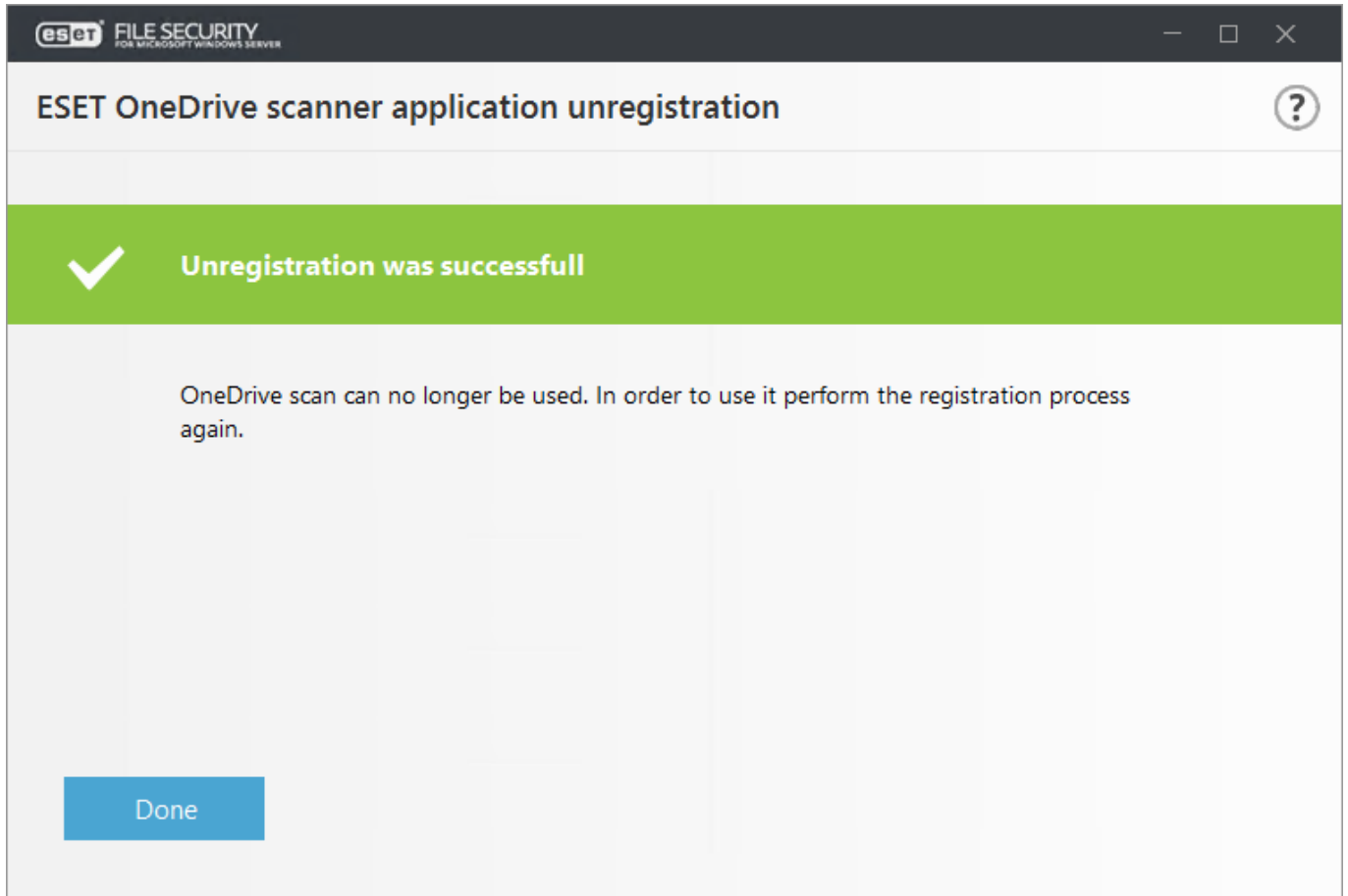
- **登録解除**をクリックし、ESET OneDrive スキャナーを削除することを確認します。



- Microsoft OneDriveからの登録解除が完了するまで待機します。



- 登録解除処理が正常に完了した場合は、登録解除ウィザードで該当するメッセージが表示されます。

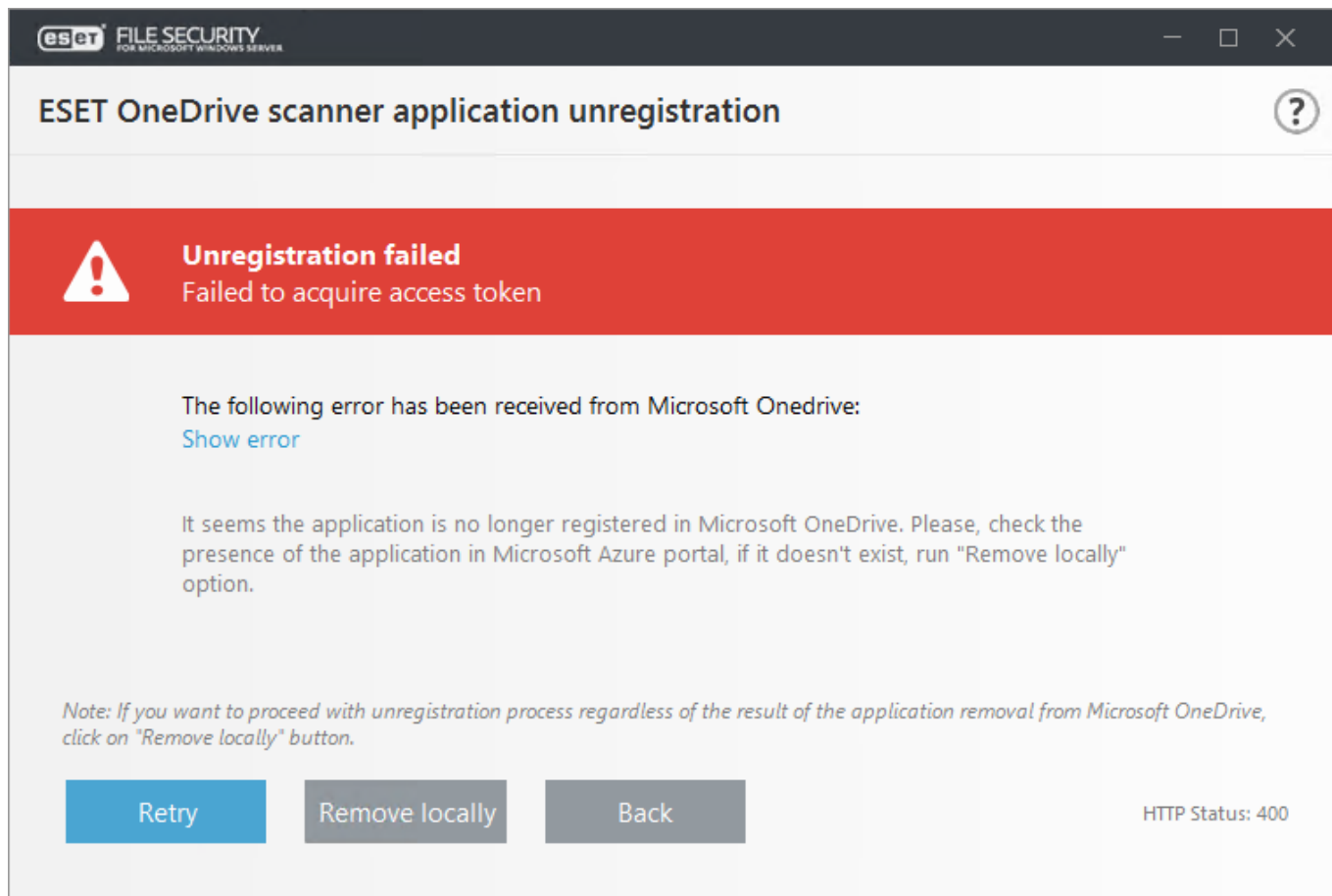


注意

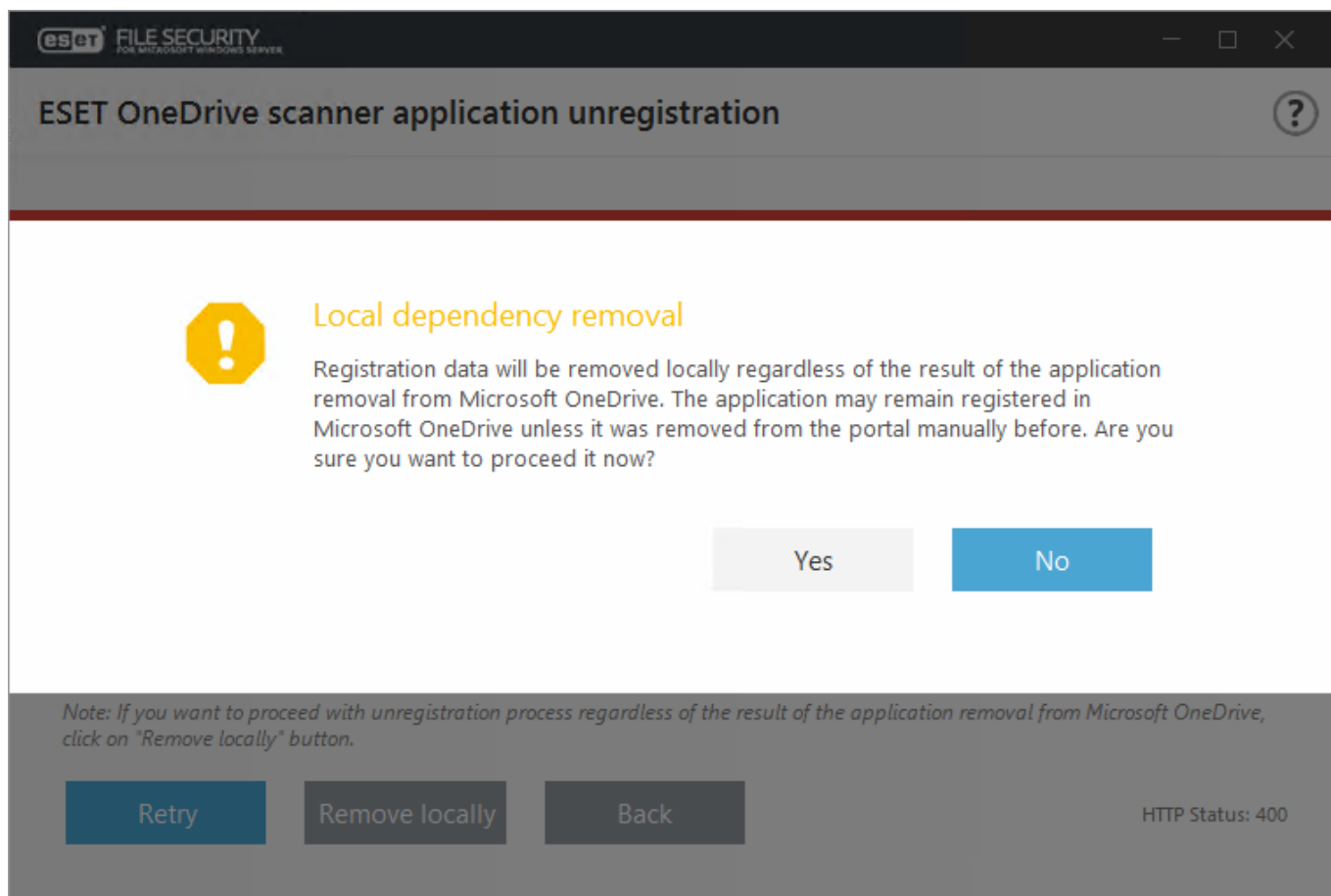
登録解除失敗などのエラーメッセージが表示される場合は、Microsoft OneDriveサーバーとの一般的なネットワークまたはインターネット接続の問題や、ESET OneDriveスキャナーがMicrosoft OneDriveに登録されていないなど、さまざまな理由が考えられます。エラーメッセージの一覧と対処方法については、以下の表を参照してください。

一部のエラーメッセージでは、ローカル依存関係(接続の問題でMicrosoft OneDriveに存在しないアプリなど)を削除するオプションがあります。ESET OneDriveスキャナーをローカルで削除するには、次の手順を実行します。

- **再試行** ボタンが動作せず、問題が解決しない場合は、**ローカルで削除** をクリックし、ESET OneDriveスキャナーローカル依存関係を削除する登録解除処理を進めます。



- はいをクリックしてESET OneDriveスキャナーのローカル削除を続行しますESET OneDrive検査は使用できなくなります。再登録を実行する必要があります。



重要

ローカル依存関係を削除してもAzureポータルでのアプリ登録は変更されずOffice 365ポータルでのアプリ権限も変更されません。Microsoft OneDriveサーバーとのネットワークまたは接続の問題のためESET OneDriveスキャナーをローカルで削除した場合は、手動でAzureのアプリ登録からESET OneDriveスキャナーアプリを削除する必要があります。Azureポータルで手動でESET OneDriveスキャナーを検索して削除する方法については、[OneDrive検査設定](#)を参照してください。

ESET OneDriveスキャナー登録解除中に次のエラーメッセージが発生する場合は、提案された想定されたソリューションについて、エラーメッセージ詳細を参照してください。

エラーメッセージ	エラーメッセージ詳細
Azureアプリケーションへの接続が失敗しました。インターネット接続がありません。	ネットワーク/インターネット接続を確認し、もう一度登録解除を実行します。Microsoft OneDriveからのESET OneDriveスキャナーアプリ削除なしで、登録解除処理を続行する場合は、 ローカルで削除 をクリックします。
アクセストークンを取得できませんでした。Microsoft OneDriveで予期しないエラーが発生しました。	ESET OneDriveスキャナーアプリがMicrosoft OneDriveに登録されていない可能性があります。ESET OneDriveスキャナーアプリは、Azureポータルで手動で削除された可能性があります。ESET OneDriveスキャナーアプリがMicrosoft OneDriveまたはAzureポータルにあることを確認してください。アプリが一覧にない場合は、 ローカルで削除 をクリックして、登録解除処理を続行します。
アクセストークンを取得できませんでした。Microsoft OneDriveでサーバーエラーが発生しました。	Microsoft OneDriveはHTTP 5xxエラーを返しました。現在、登録解除タスクを完了できません。しばらくたってから登録解除を再試行してください。
Microsoft OneDriveで次のエラーが発生しました。	Microsoft OneDriveサーバーは、特定のエラーコード/名前のエラーを返しました。 エラーを表示 をクリックしてください。
別のセットアップタスクがすでに実行中です。	登録解除タスクは既に実行中です。最初の登録解除処理が完了するまでお待ちください。

一般設定

各自のニーズにあった一般設定とオプションを指定できます。左側のメニューには次のカテゴリがあります。

[検出エンジン](#)

望ましくない可能性がある、危険な可能性がある、不審なアプリケーションの検出とアンチステルス保護を有効または無効にします。プロセスまたはファイルとフォルダーの除外を指定します。リアルタイムファイルシステム保護ThreatSenseパラメーター、クラウドベース保護(ESET LiveGrid®)マルウェア検査(オンデマンドコンピューター検査および他の検査オプション)Hyper-V検査およびHIPSを設定します。

[アップデート](#)

プロファイル、検出エンジン経過時間、モジュールロールバックのスナップショット、アップデートタイプ、カスタムアップデートサーバー、接続/プロキシサーバー、アップデートミラー、アップデートファイルへのアクセスHTTPサーバー、ネットワーク接続のユーザーアカウント詳細などのアップデートオプションを設定します。

[Webとメール](#)

プロトコルフィルタリングおよび除外(除外されたアプリケーションおよびIPアドレス)②SSL/TLSプロトコルフィルタリングオプション、電子メールクライアント保護(統合、電子メールプロトコル、アラートおよび通知)②Webアクセス保護(HTTP/HTTPS WebプロトコルおよびURLアドレス管理)および電子メールクライアントフィッシング対策機能を設定できます。

デバイスコントロール

統合を有効にし、デバイスコントロールルールおよびグループを設定します。

ツール設定

ESET CMD②ESET RMM②WMIプロバイダ②ESET PROTECT検査対象②Windows Update通知、ログファイル、プロキシサーバー、電子メール通知、診断、クラスターなどのツールをカスタマイズできます。

ユーザーインタフェース

プログラムのGUI④状態、ライセンス情報、アラートと通知、パスワード保護④eShell実行ポリシーなどの動作を設定します。

検出エンジン

検出エンジンは、ファイル、電子メール、ネットワーク通信を検査して、悪意のあるシステム攻撃から保護します。マルウェアに分類されたオブジェクトが検出されると、修復が開始します。検出エンジンはまずオブジェクトをブロックし、駆除、削除、隔離への移動といったアクションを実行します。

リアルタイム保護および機械学習保護

高度な保護レイヤーとして検出エンジンの一部として、高度な機械学習が追加されました。これにより、機械学習に基づいて検出が改善されます。この種類の保護の詳細については、[用語集](#)を参照してください。次のカテゴリのレポートレベルと保護レベルを設定できます。

マルウェア

コンピューターウイルスは、コンピューターの既存のファイルの前後に追加される悪意のあるコードです。ただし、「ウイルス」という用語は、よく間違っ使用されます。「マルウェア」(悪意のあるソフトウェア)がより正確な用語です。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で実行されます。このような種類のアプリケーションについては、[用語集](#)をご覧ください。

望ましくない可能性があるアプリケーション

望ましくない可能性があるアプリケーションは、明確な悪意がある目的のソフトウェアではありませんが、追加の望ましくないアプリケーションをインストールしたり、デジタルデバイスの動作を変更したり、ユーザーによって承認または想定されていないアクティビティを実行したり、他の不明確な目的を持っていたりする可能性があります。

このカテゴリには、広告表示ソフトウェア、ダウンロードラッパー、各種ブラウザーツールバー、誤解を招く動作のソフトウェア、バンドルウェア、トラックウェアなどがあります。

この種のアプリケーションの詳細については、「[用語集](#)」を参照してください。

不審な可能性があるアプリケーション

リバースエンジニアリングを阻止または実行ファイルの内容を曖昧にする(マルウェアの存在を隠すなど)ために、圧縮または暗号化の独占的な方法によって頻繁に使用される[パッカー](#)またはプロテクターで圧縮されたソフトウェアです。

このカテゴリには、マルウェアを圧縮するために頻繁に使用されるパッカーまたはプロテクターで

圧縮されたすべての不明なアプリケーションが含まれます。

安全ではない可能性があるアプリケーション

この分類は、悪意のある目的で悪用される可能性がある商業的、合法的なソフトウェアです。安全ではない可能性があるアプリケーションは、不正な目的で悪用される可能性のある、市販の適正なソフトウェアです。

このカテゴリは、クラッキングツール、ライセンスキー生成、ハッシュツール、リモートアクセスまたはコントロールツール、パスワード解析アプリケーション、キーロガー(ユーザーが入力した各キーストロークを記録するプログラム)などが含まれます。このオプションは、既定では無効になっています。

この種のアプリケーションの詳細については、「[用語集](#)」を参照してください。

カテゴリレポートまたは保護のしきい値(またはレベル)を変更する前に、次をお読みください。

▼ [報告](#)

レポートは、検出エンジンと機械学習コンポーネントによって実行されます。レポートのしきい値は、環境やニーズに合わせて設定できます。正しい設定は1つではありません。したがって、環境内の動作を監視し、別のレポート設定がより適しているかどうかを判断することをお勧めします。

レポートはオブジェクトに対してアクションを実行せず、それぞれの保護レイヤーに情報を渡し、それに応じて保護レイヤーがアクションを実行します。

攻撃的	最大の感度に構成されたレポート。報告される検出数が多くなります。強レベルの設定は最も安全に見える場合もありますが、敏感すぎることで多く、逆効果になる可能性もあります。
	<div>注意 強レベルの設定では、オブジェクトが悪意のあるオブジェクトとして誤って識別される場合があります、そのようなオブジェクトに対してアクションが実行されます(保護の設定に応じて)。</div>
標準	この設定は、検出率のパフォーマンスおよび精度と、誤って報告されるオブジェクト数の間でバランスを保つように最適化されています。
最小	レポートは、誤って特定されるオブジェクトの数を最小限に抑えながら、効率的なレベルの保護を維持するように設定されています。確率が明らかであり、マルウェアの動作と一致するときのみ、オブジェクトが報告されます。
オフ	レポートがアクティブではありません。検出は見つからないか、報告されないか、駆除されません。
	<div>注意 マルウェアレポートは非アクティブ化できないため、オフ設定をマルウェアで使用できません。</div>

このセクションの設定を既定値に戻す場合は、セクションヘッダーの横にあるUターン矢印をクリックします。このセクションで行った変更はすべて失われます。

▼ [保護](#)

上記の設定と機械学習結果に基づいてオブジェクトが報告されると、そのオブジェクトはブロックされ、アクションが実行されます(駆除、削除、または隔離に移動)。

攻撃的	報告された強(以下の)レベルの検出はブロックされ、自動修復(駆除など)が開始します。
標準	報告されたバランス(以下)レベルの検出はブロックされます。自動修正(駆除)が開始します。

攻撃的	報告された強(以下の)レベルの検出はブロックされ、自動修復(駆除など)が開始します。
最小	報告された注意レベルの検出はブロックされます。自動修正(駆除)が開始します。
オフ	レポートがアクティブではありません。検出は見つからないか、報告されないか、駆除されません。
注意 マルウェアレポートを非アクティブ化できないため、オフ設定をマルウェアで使用できません。	

このセクションの設定を既定値に**戻す**場合は、セクションヘッダーの横にあるUターン矢印をクリックします。このセクションで行った変更はすべて失われます。

注意

既定では、上記の機械学習保護設定は、オンデマンドのコンピューター検査にも適用されます。必要に応じて、**オンデマンドおよび機械学習の保護設定**を個別に構成できます。スイッチアイコンをクリックして**リアルタイムファイルシステム保護設定**を使用を無効にし、設定を続行します。

機械学習による検出

検出エンジンは、ファイル、電子メール、ネットワーク通信を検査して、悪意のあるシステム攻撃から保護します。マルウェアに分類されたオブジェクトが検出されると、修復が開始します。検出エンジンはまずオブジェクトをブロックし、駆除、削除、隔離への移動といったアクションを実行します。

リアルタイム保護および機械学習保護

高度な保護レイヤーとして検出エンジンの一部として、高度な機械学習が追加されました。これにより、機械学習に基づいて検出が改善されます。この種類の保護の詳細については、[用語集](#)を参照してください。次のカテゴリのレポートレベルと保護レベルを設定できます。

マルウェア

コンピューターウイルスは、コンピューターの既存のファイルの前後に追加される悪意のあるコードです。ただし、「ウイルス」という用語は、よく間違っ使用されます。「マルウェア」(悪意のあるソフトウェア)がより正確な用語です。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で実行されます。このような種類のアプリケーションについては、[用語集](#)をご覧ください。

望ましくない可能性があるアプリケーション

望ましくない可能性があるアプリケーションは、明確な悪意がある目的のソフトウェアではありませんが、追加の望ましくないアプリケーションをインストールしたり、デジタルデバイスの動作を変更したり、ユーザーによって承認または想定されていないアクティビティを実行したり、他の不明確な目的を持っていたりする可能性があります。

このカテゴリには、広告表示ソフトウェア、ダウンロードラッパー、各種ブラウザーツールバー、誤解を招く動作のソフトウェア、バンドルウェア、トラックウェアなどがあります。

この種のアプリケーションの詳細については、「[用語集](#)」を参照してください。

不審な可能性があるアプリケーション

リバースエンジニアリングを阻止または実行ファイルの内容を曖昧にする(マルウェアの存在を隠すなど)ために、圧縮または暗号化の独占的な方法によって頻繁に使用される[パッカー](#)またはプロテクターで圧縮されたソフトウェアです。

このカテゴリには、マルウェアを圧縮するために頻繁に使用されるパッカーまたはプロテクターで圧縮されたすべての不明なアプリケーションが含まれます。

安全ではない可能性があるアプリケーション

この分類は、悪意のある目的で悪用される可能性がある商業的、合法的なソフトウェアです。安全ではない可能性があるアプリケーションは、不正な目的で悪用される可能性のある、市販の適正なソフトウェアです。

このカテゴリは、クラッキングツール、ライセンスキー生成、ハッシュツール、リモートアクセスまたはコントロールツール、パスワード解析アプリケーション、キーロガー(ユーザーが入力した各キーストロークを記録するプログラム)などが含まれます。このオプションは、既定では無効になっています。

この種のアプリケーションの詳細については、「[用語集](#)」を参照してください。

カテゴリレポートまたは保護のしきい値(またはレベル)を変更する前に、次をお読みください。

▼ [報告](#)

レポートは、検出エンジンと機械学習コンポーネントによって実行されます。レポートのしきい値は、環境やニーズに合わせて設定できます。正しい設定は1つではありません。したがって、環境内の動作を監視し、別のレポート設定がより適しているかどうかを判断することをお勧めします。

レポートはオブジェクトに対してアクションを実行せず、それぞれの保護レイヤーに情報を渡し、それに応じて保護レイヤーがアクションを実行します。

攻撃的	最大の感度に構成されたレポート。報告される検出数が多くなります。強レベルの設定は最も安全に見える場合もありますが、敏感すぎることが多く、逆効果になる可能性もあります。
	<div>注意 強レベルの設定では、オブジェクトが悪意のあるオブジェクトとして誤って識別される場合があります、そのようなオブジェクトに対してアクションが実行されます(保護の設定に応じて)。</div>
標準	この設定は、検出率のパフォーマンスおよび精度と、誤って報告されるオブジェクト数の間でバランスを保つように最適化されています。
最小	レポートは、誤って特定されるオブジェクトの数を最小限に抑えながら、効率的なレベルの保護を維持するように設定されています。確率が明らかであり、マルウェアの動作と一致するときのみ、オブジェクトが報告されます。
オフ	レポートがアクティブではありません。検出は見つからないか、報告されないか、駆除されません。
	<div>注意 マルウェアレポートは非アクティブ化できないため、オフ設定をマルウェアで使用できません。</div>

このセクションの設定を既定値に[戻す](#)場合は、セクションヘッダーの横にあるUターン矢印をクリックします。このセクションで行った変更はすべて失われます。

▼ [OneDriveおよび機械学習保護](#)

レポート

検出エンジンと機械学習コンポーネントによって実行されます。レポートはオブジェクトに対してアクションを実行しません(これは該当する保護レイヤーによって実行されます)。

保護

[OneDrive](#) セクションで、報告されたオブジェクトに対して実行されるアクションに影響を与えるパラメーターを設定します。

このセクションの設定を既定値に[戻す](#)場合は、セクションヘッダーの横にあるUターン矢印をクリックします。このセクションで行った変更はすべて失われます。

eShellを使用して、機械学習保護を設定します。eShellのコンテキスト名は**MLP**です。対話モードでeShellを開き、MLPに移動します。

```
computer onedrive mlp
```

不審なアプリケーションの現在のレポート設定を確認してください。

```
get suspicious-reporting
```

レポートの厳密さを下げる場合は、設定を最小に変更します。

```
set suspicious-reporting cautious
```

除外

除外では、ファイルやフォルダーを検査から除外することができます。すべての対象で脅威が検査されるように、絶対に必要な場合を除いては、除外を作成しないことをお勧めします。対象を除外する必要がある場合もあります。たとえば、検査中にサーバーの速度を低下させる恐れのある大きなデータベースエントリーや、検査と競合するソフトウェアなどです(バックアップソフトウェアなど)。

警告

[除外された拡張子](#)と[プロセス除外](#)、または[除外フィルター](#)と混同しないでください。

注意

ファイルがスキャンからの除外基準に適合すると、リアルタイムファイルシステム保護モジュールまたはコンピューターの検査モジュールはファイル内の脅威を検出しません。

除外の種類を選択し、**編集**をクリックして新しい除外を追加するか、既存の除外を変更します。

- [パフォーマンスの除外](#) – ファイルとフォルダーを検査から除外します。
- [検出除外](#) – 特定の条件(パス、ファイルハッシュ、または検出名)を使用して、オブジェクトを検査から除外します。

パフォーマンスの除外

この機能を使用すると、ファイルやフォルダーを検査から除外できます。パフォーマンス除外は、基幹アプリケーションのファイルレベルの検査を除外する場合や、検査によってシステムの異常な動作が発生したりパフォーマンスが低下したりする場合に役立ちます。

パス

このコンピューターで特定のパス(ファイルまたはディレクトリ)を除外します。パスの中央では、ワイルドカード – アスタリスク(*)を使用しないでください。詳細については、次の[ナレッジベー](#)

[ス記事](#)を参照してください。

注意

フォルダーの内容を除外する場合は、必ずパスの最後にアスタリスク(*)を追加してください(`C:\Tools*`)。C:\Toolsは除外されません。検査の観点から、Toolsもファイル名になっている可能性があるからです。

コメント

後からでも除外を簡単に識別できるように、任意のコメントを追加します。

例

アスタリスクを使用したパスの除外:

`C:\Tools*` - パスの末尾は、(\)とアスタリスク(*)にし、フォルダーとすべてのフォルダーの内容(ファイルとサブフォルダー)が実行されることを指定する必要があります。

`C:\Tools*. *` - `C:\Tools*`と同じ動作です。つまり、再帰的に動作します。

`C:\Tools*.dat` - ツールバーのdatファイルを除外します

`C:\Tools\sg.dat` - 正確なパスにあるこの特定のファイルを除外します

例

フォルダーのすべてのファイルを除外するには、フォルダーへのパスを入力し、マスク`*.*`を使用します。

- Docファイルのみを除外するには、マスク`*.doc`を使用します。

- 実行ファイルの名前に特定の文字数があり、文字が異なり、最初の1文字のみが分かっている場合(???.exeなど)、次の形式を使用します。

`D?????.exe`(疑問符は見つからないか不明な文字を置換します)

例

%PROGRAMFILES%などのシステム変数を使用して、検査除外を定義します。

- このシステム変数を使用してProgram Filesフォルダーを除外するには、パス`%PROGRAMFILES%\`を使用します(除外を追加するときには、必ずパスの最後にバックスラッシュを追加します)。

- %HOMEDRIVE%サブディレクトリのすべてのファイルを除外するには、パス`%HOMEDRIVE%\Excluded_Directory*.*`を使用します。

次の変数はパス除外形式で使用できます。

`%ALLUSERSPROFILE%`

`%COMMONPROGRAMFILES%`

`%COMMONPROGRAMFILES(X86)%`

`%COMSPEC%`

`%HOMEDRIVE%`

`%HOMEPATH%`

`%PROGRAMFILES%`

`%PROGRAMFILES(X86)%`

`%SystemDrive%`

`%SystemRoot%`

`%WINDIR%`

`%PUBLIC%`

ユーザー固有の変数(`%TEMP%`や`%USERPROFILE%`など)または環境変数(`%PATH%`など)はサポートされません。

検出除外

これは、検出名、パス、ハッシュを使用して、オブジェクトを検査から除外する別の方法です。検出除

外は、ファイルとフォルダーを検査から除外しません([パフォーマンス除外](#)など)。検出除外は、検出エンジンで検出され、適切なルールが除外リストにあるときにのみ、オブジェクトを除外します。

検出ベースの除外を作成する最も簡単な方法は、**ログファイル** > [検出](#)から既存の検出を使用することです。ログレコード(検出)を右クリックし、**除外の作成**をクリックします。これにより、事前に定義された条件を使用して[除外ウィザード](#)が開きます。

検出除外を手動で作成するには、**編集** > **追加**(既存の除外を修正する場合は**編集**)をクリックし、次の条件を1つ以上指定します(組み合わせることができます)。

パス

特定のパス(ファイルまたはディレクトリ)を除外します。特定の場所/ファイルを参照するか、手動で文字列を入力できます。パスの途中に、ワイルドカード - アスタリスク(*)を使用しないでください。詳細については、次の[ナレッジベース記事](#)を参照してください。

注意

フォルダーの内容を除外する場合は、必ずパスの最後にアスタリスク(*)を追加してください(C:\Tools*)。C:\Toolsは除外されません。検査の観点から、Toolsもファイル名になっている可能性があるからです。

ハッシュ

ファイルタイプ、場所、名前、または拡張子に関係なく、指定されたハッシュ(SHA1)に基づいてファイルを除外します。

検出名

有効な検出(脅威)名を入力します。検出名だけに基づいて除外を作成すると、セキュリティ上のリスクが生じる可能性があります。検出名とパスを組み合わせることをお勧めします。この除外条件は、特定の種類の検出にのみ使用できます。

コメント

後からでも除外を簡単に識別できるように、任意のコメントを追加します。

ESETPROTECTには[検出除外管理](#)が含まれており、検出除外を作成して、その他のコンピューター/グループに適用できます。

ワイルドカードを使用すると、類似した複数のファイルを指定することができます。疑問符(?)は任意の1文字を表し、アスタリスク(*)は任意の0文字以上を表します。

例

アスタリスクを使用したパスの除外:

C:\Tools* - パスの末尾は、(\)とアスタリスク(*)にし、フォルダーとすべてのフォルダーの内容(ファイルとサブフォルダー)が実行されることを指定する必要があります。

C:\Tools*. *- C:\Tools*と同じ動作です。つまり、再帰的に動作します。

C:\Tools*.dat - ツールバーのdatファイルを除外します

C:\Tools\sg.dat - 正確なパスにあるこの特定のファイルを除外します

例

脅威を除外するには、次の形式で有効な検出名を入力します。

@NAME=Win32/Adware.Optmedia

@NAME=Win32/TrojanDownloader.Delf.QQI

@NAME=Win32/Bagle.D

例

フォルダーのすべてのファイルを除外するには、フォルダーへのパスを入力し、マスク*.*を使用します。

- Docファイルのみを除外するには、マスク*.docを使用します。

- 実行ファイルの名前に特定の文字数があり、文字が異なり、最初の1文字のみが分かっている場合(DDなど)、次の形式を使用します。

D????.exe(疑問符は見つからないか不明な文字を置換します)

例

%PROGRAMFILES%などのシステム変数を使用して、検査除外を定義します。

- このシステム変数を使用してProgram Filesフォルダーを除外するには、パス%PROGRAMFILES%\を使用します(除外を追加するときには、必ずパスの最後にバックスラッシュを追加します)。

- %HOMEDRIVE%サブディレクトリのすべてのファイルを除外するには、パス%HOMEDRIVE%\Excluded_Directory*.*を使用します。

次の変数はパス除外形式で使用できます。

%ALLUSERSPROFILE%

%COMMONPROGRAMFILES%

%COMMONPROGRAMFILES(X86)%

%COMSPEC%

%HOMEDRIVE%

%HOMEPATH%

%PROGRAMFILES%

%PROGRAMFILES(X86)%

%SystemDrive%

%SystemRoot%

%WINDIR%

%PUBLIC%

ユーザー固有の変数(%TEMP%や%USERPROFILE%など)または環境変数(%PATH%など)はサポートされません。

除外の作成ウィザード

推奨される除外は検出タイプに基づいて事前を選択されていますが、検出の除外条件をさらに指定できます。**条件の変更**をクリックします。

- **正確なファイル** - SHA-1ハッシュで各ファイルを除外します。
- **検出** - 検出名を指定して、そのような検出を含む各ファイルを除外します。
- **パス + 検出** - 検出名とパス(ファイル名を含む)を指定して、指定した場所で検出された各ファイルを除外します。

後からでも除外を簡単に識別できるように、任意の**コメント**を追加します。

詳細設定オプション

アンチステルス技術

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、危険なプログラムを検出する高度なシステムです。そのため、通常のテスト技術を使用して検出することはできません。

AMSI

Microsoft マルウェア対策検査インターフェイス (AMSI) を使用して Windows スクリプトホストによって実行された Powershell スクリプトを検査します。

自動除外

サーバーアプリケーションやオペレーティングシステムの開発者は、開発する大部分の製品の重要な作業ファイルおよびフォルダーをマルウェアの検査の対象外にすることを推奨しています。これはマルウェア検査が、サーバーのパフォーマンスに悪影響を与えたり、競合を起こしたりするおそれがあり、一部のアプリケーションをサーバーで実行できなくするおそれさえあるためです。除外機能は、マルウェア対策ソフトウェアを実行する場合に潜在する競合のリスクを最小化し、サーバーの全体的なパフォーマンスを向上するために有効です。ESET サーバー製品の検査から[除外されたファイルの一覧](#)を参照してください。

ESET Server Security は、重要なサーバーアプリケーションとサーバーのオペレーティングシステムファイルを識別して、[除外](#)リストに自動的に追加します。すべての自動除外は既定で有効です。各サーバーアプリケーション除外を有効/無効にするには、次の結果があるスライダーバーをクリックします。

- 有効にすると、すべての重要なファイルおよびフォルダーは、検査から除外するファイルのリストに追加されます。サーバーを再起動するたびに除外の自動チェックが実行されて、システムまたはアプリケーションの変更がある場合はリストが更新されます (新しいサーバーアプリケーションがインストールされた場合など)。自動除外を必ず常に適用する場合は、この設定をお勧めします。
- 無効にすると、自動的に除外されたファイルとフォルダーはリストから削除されます。手動で入力されたユーザー定義の除外は影響を受けません。

自動除外を特定して生成するために ESET Server Security では、インストールフォルダーにある専用のアプリケーション `eAutoExclusions.exe` が使用されます。自分で操作する必要はありませんが、コマンドラインを使用すると、`eAutoExclusions.exe -servers` を実行することで、システムで検出されたサーバーアプリケーションを一覧表示できます。完全な構文を表示するには、`eAutoExclusions.exe -?` を使用します。

共有ローカルキャッシュ

ESET 共有ローカルキャッシュを使用すると、ネットワークで重複した検査がなくなり、仮想環境のパフォーマンスが向上します。これにより、各ファイルが 1 回だけ検査され、共有キャッシュに保存されます。**[共有ローカルキャッシュ]** をオンにすると、ネットワーク上のファイルとフォルダーの検査情報がローカルキャッシュに保存されます。新しい検査を実行する場合は、ESET Server Security がキャッシュにある検査済みファイルを検索します。ファイルが一致すると、検査から除外されます。

キャッシュサーバー設定には次の内容があります。

- **ホスト名** - キャッシュがあるコンピュータの名前またはIPアドレス。
- **ポート** - 通信で使用するポート番号(共有ローカルキャッシュと同じ)。
- **パスワード** - 必要に応じて、共有ローカルキャッシュのパスワードを指定します。

侵入が検出された

マルウェアがシステムに侵入する経路は、Webページ、共有フォルダ、メールや、コンピュータのリムーバブルデバイス(USB[®]外付けハードディスク[®]CD[®]DVD[®]フロッピーディスクなど)など、さまざまです。

標準的な動作

ESET Server Securityは、一般的に以下を使用してマルウェアを検出して処理します。

- [リアルタイムファイルシステム保護](#)
- [Webアクセス保護](#)
- [電子メールクライアント保護](#)
- [コンピュータの検査](#)

各機能は、標準的な駆除レベルを使用し、ファイルを駆除して、[隔離](#)に移動するか、接続を終了しようとしします。通知ウィンドウは、画面の右下にある通知領域に表示されます。駆除レベルと動作の詳細については、「[駆除](#)」を参照してください。

駆除と削除

リアルタイムファイルシステム保護にあらかじめ指定されたアクションがない場合は、警告ウィンドウが表示され、オプションを選択するよう求められます。選択できるオプションは通常、**[駆除]****[削除]**、および**[何もしない]**のいずれかです。**[何もしない]**を選択すると、感染ファイルが駆除されないまま残されるので、推奨されません。唯一の例外は、そのファイルが「無害なのに誤って感染が検出された」と確信できる場合です。

ウイルスの攻撃によって悪意のあるコードがファイルに添付された場合に、駆除を行います。この場合、元の状態に戻すため、駆除前に感染しているファイルからのウイルスの駆除を試みます。ファイルが悪意のあるコードでのみ構成されている場合には、全体が削除されます。

感染しているファイルが、システムプロセスによって“ロック”または使用されている場合、通常は開放後でなければ削除できません(通常は再起動後)。

複数の脅威

コンピュータの検査中に駆除されなかった感染ファイルがある場合(または[駆除レベル](#)が**[駆除なし]**に設定されていた場合)、警告ウィンドウが開き、これらのファイルに対するアクションを選択するよう求められます。リストの各脅威に対して個別にアクションを選択するか、**[すべてのリストの脅威に対してアクションを選択]**を使用して、リストのすべての脅威に対して実行する1つのアクションを選択してから、**[完了]**をクリックします。

アーカイブのファイルの削除

既定の駆除モードでは、感染していないファイルがなく、感染ファイルのみある場合に限り、アーカイブファイル全体が削除されます。つまり、感染していない無害なファイルも含まれている場合には、アーカイブは削除されません。厳密な駆除スキャンを実行する際には注意が必要です。厳密な駆除を有効にした状態では、アーカイブに感染ファイルが1つでも含まれていれば、アーカイブ内の他のファイルの状態に関係なく、そのアーカイブは削除されます。

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では、システムで発生する、マルウェア関連のイベントをすべてコントロールします。ファイルはすべて、コンピューター上で開くとき、作成するとき、または実行するときに、悪意のあるコードがないかどうか検査されます。既定では、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起動し、中断なしに検査を行います。特殊な場合(別のリアルタイムスキャナーと競合する場合など)は、**リアルタイムファイルシステム保護 > 基本**の下**の詳細設定(F5のリアルタイムファイルシステム保護を自動的に開始するオプションの選択を解除すると、リアルタイム保護を無効にできます。**

ESET Server Securityはクラウド階層が有効なAzure File Syncエージェントを使用するコンピューターと互換性があります。ESET Server Securityは属性FILE_ATTRIBUTE_RECALL_ON_DATA_ACCESSのファイルを認識します。

検査するメディア

既定では、あらゆる種類のメディアに対して潜在的な脅威が検査されます。

- **ローカルドライブ** – システムハードディスクをすべて検査します。
- **リムーバブルメディア** - CD/DVD、USB記憶装置、Bluetoothデバイスなどを検査します。
- **ネットワークドライブ** – マッピングされたドライブをすべて検査します。

既定の設定を変更するのは、あるメディアの検査によりデータ転送が極端に遅くなるときなど、特別な場合だけにすることをお勧めします。

検査のタイミング

既定では、ファイルを開いたり、作成したり、実行したりするときに、すべてのファイルが検査されます。既定の設定ではコンピュータが最大限のレベルでリアルタイムに保護されるので、既定の設定を変更しないことをお勧めします。

- **ファイルを開くとき** – ファイルを開いたとき/ファイルにアクセスしたときに検査します。
- **ファイルを作成するとき** – ファイルを作成/修正したときに検査します。
- **ファイルを実行するとき** – ファイルを実行するときに検査します。
- **リムーバブルメディアアクセス** – リムーバブルストレージにアクセスするときに検査を実行します。ブートセクターを含むリムーバブルメディアがデバイスに挿入されると、ブートセクターがただちに検査されます。このオプションでは、リムーバブルメディアファイルの検査は有効になっていません。リムーバブルメディアファイルの検査は、**検査するメディア > リムーバブルメディア**にあります。リムーバブルメディアのブートセクターのアクセスが正しく機能するように、ThreatSenseパラメーターで**ブートセクタ/UEFIを有効**にしてください。

除外を処理する

特定のプロセスを除外できます。たとえば、バックアップソリューションのプロセスの場合、このような除外されたプロセスに基づくすべてのファイル処理が無視され、安全であると見なされるため、バックアップ処理の中断を最小限に抑えることができます。

ThreatSense パラメータ

リアルタイムファイルシステム保護は、ファイルアクセスなど、さまざまなシステムイベントごとにトリガされ、すべての種類のメディアを確認します。リアルタイムファイルシステム保護は、新しく作成されたファイルを既存のファイルと異なる方法で扱うように設定できます。たとえば、新しく作成されたファイルを今までよりも細かく監視するように、リアルタイムファイルシステム保護を設定できます。

システムの使用領域を最小化するために、リアルタイム保護の使用時、すでに検査されたファイルは(変更がない限り)繰り返し検査されません。ファイルは、各検出エンジンデータベースアップデートの直後にもう一度検査されます。なおこの動作は[スマート最適化]を使用して設定します。スマート最適化が無効の場合、全てのファイルがアクセスのたびに検査されます。この設定を変更するには、**F5**を押し、**詳細設定**を開いて、**検出エンジン > リアルタイムファイルシステム保護**を展開します。**ThreatSenseパラメーター > その他**をクリックし、**スマート最適化を有効にする**を選択または選択解除します。

[追加の ThreatSense パラメータ](#)

新しく作成および変更されたファイルに適用する追加のThreatSenseファイルまたは除外されたファイルの追加のThreatSenseパラメーターの詳細オプションを修正できます。

ThreatSense パラメータ

ThreatSenseは、ウイルスを検出する多数の複雑な方法から構成される技術です。この技術は事前対応型なので、新しいウイルスが広がる初期の段階でも保護することができます。この技術では、システムのセキュリティを大幅に強化するために連携して動作するコード分析、コードエミュレーション、汎用シグネチャ、ウイルスシグネチャを組み合わせで使用します。検査エンジンは、複数のデータストリームを同時に検査して、最大限の効率および検出率を確保することができます。またThreatSense技術によってルートキットを除去することもできます。

注意

自動スタートアップファイルチェックの詳細については、「[スタートアップ検査](#)」を参照してください。

ThreatSenseエンジンの設定オプションを使用すると、ユーザーはさまざまな検査パラメーターを指定することができます。

- 検査するファイルの種類および拡張子
- さまざまな検出方法の組み合わせ
- 駆除のレベルなど

設定ウィンドウにアクセスするにはThreatSense技術を使用する任意の機能(下記を参照)の**詳細設定(F5)**ウィンドウにある**ThreatSenseエンジンパラメータ設定**をクリックします。セキュリティシナリオごとに異なる設定が必要になることがあります。これを念頭に、ThreatSenseは、次の保護モジュールについて個々に設定することができます。

- [Hyper-V検査](#)
- [OneDrive検査](#)
- [リアルタイムファイルシステム保護](#)
- [マルウェア検査](#)
- [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](#)
- [電子メールクライアント保護](#)
- [Webアクセス保護](#)

ThreatSenseのパラメーターは機能ごとに高度に最適化されているので、パラメーターを変更すると、システムの動作に大きく影響することがあります。たとえば、常にランタイム圧縮形式をスキャンするようにパラメーターを変更したり、リアルタイムファイル保護機能のアドバンスドヒューリスティックを

有効にすると、システムの処理速度が低下することがあります(通常は、新しく作成されたファイルのみがこれらの方法を使用してスキャンされます)。コンピュータの検査を除く全ての機能についてThreatSenseの既定のパラメーターを変更しないことをお勧めします。

■ [検査するオブジェクト](#)

このセクションでは、感染を検査するコンピュータのコンポーネントおよびファイルを定義できます。

メモリ

システムメモリを攻撃対象とするマルウェアを検査します。

ブートセクタ/UEFI

MBR(マスターブートレコード)にウイルスがないかどうかブートセクタを検査しますHyper-V仮想マシンの場合、ディスクMBRは読み取り専用モードで検査されます。

電子メールファイル

拡張子DBX (Outlook Express)およびEMLがサポートされます。

アーカイブ

プログラムは以下の拡張子をサポートしますARJBZ2CABCHMDBXGZIPISO/BIN/NRGLHAMIME NSISRARSSISTARTNEFUUEWISEZIPACEおよびその他多数。

自己解凍アーカイブ

自己解凍形式(SFX)とは、解凍に特殊なプログラム(アーカイブ)を必要としないアーカイブです。

圧縮された実行形式

圧縮された実行形式(標準の解凍形式とは異なる)は、実行後メモリー内で解凍されます。スキャナでは、コードのエミュレーションによって、標準の静的圧縮形式(UPXyodaASPackFSGなど)のほかにも多数の圧縮形式を認識できます。

■ [検査オプション](#)

システムの侵入を検査するときに使用する方法を選択します。 使用可能なオプションは次のとおりです。

ヒューリスティック

ヒューリスティックは、悪意のあるプログラムの活動を分析するアルゴリズムです。この技術の主な利点は、前には存在しなかったり、これまでの検出エンジンで特定されていなかったりした悪意のあるソフトウェアを特定できる点です。

アドバンスドヒューリスティック/DNA署名

アドバンスドヒューリスティックは、ESETが開発した独自のヒューリスティックアルゴリズムで構成されます。このアルゴリズムは、コンピューターワームやトロイの木馬を検出するために最適化

され、高度なプログラミング言語で記述されています。アドバンスドヒューリスティックを使用するとESET製品の脅威検出機能が大幅に高まります。シグネチャは確実にウイルスを検出し、特定することができます。自動アップデートシステムを利用することにより、新しいシグネチャを使用するためのウイルス検出時間を短縮できます。シグネチャの欠点は、既知のウイルス(またはこれらのウイルスの多少の変更が加えられたバージョン)しか検出しない点です。

☐ 駆除

駆除設定により、感染ファイルからウイルスを駆除するときのスキャナーの動作が決まります。駆除には、3つのレベルがあります。

駆除なし

感染しているファイルが自動的に駆除されることはありません。警告ウィンドウが表示され、ユーザーがアクションを選択することができます。このレベルは、侵入が発生したときに実行する必要のあるステップを理解している経験豊富なユーザー向けです。

標準駆除

プログラムは、事前定義されたアクション(マルウェアの種類によって異なります)に基づいて、感染ファイルの駆除または削除を自動的に試行します。感染しているファイルの検出と削除は、画面右下隅の通知によって表示されます。適切なアクションを自動的に選択できなかった場合は、ユーザーがその後のアクションを選択することができます。あらかじめ定義されているアクションを実行できなかった場合も同様です。

厳密な駆除

全ての感染ファイルが駆除または削除されます。ただし、システムファイルは除きます。ファイルを駆除できない場合は、実行するアクションの種類を選択する必要があります。

警告

感染しているファイルがアーカイブに含まれている場合、アーカイブの処理方法が2つあります。既定のモード(**標準的な駆除**)では、アーカイブに含まれているすべてのファイルが感染ファイルである場合のみ、アーカイブ全体が削除されます。[**厳密な駆除**]モードでは、アーカイブに感染ファイルが1つ以上含まれている場合、アーカイブ内の他のファイルのステータスに関係なく、アーカイブが削除されます。

重要

Hyper-VホストがWindows Server 2008 R2 SP2で実行されている場合は、**標準の駆除**と**厳密の駆除**はサポートされません。仮想マシンディスクの検査は読み取り専用モードです。駆除しないで実行されます。駆除レベルの選択に関係なく、検査は常に読み取り専用モードで実行されます。

☐ 除外

拡張子は、ファイル名の一部であり、ピリオドで区切られています。拡張子は、ファイルの種類と内容を規定します。ThreatSenseパラメーター設定のこのセクションでは、[検査から除外するファイル](#)の種類を指定できます。

その他

オンデマンドコンピュータの検査でThreatSenseエンジンパラメータ設定を設定する場合は、[その他]セクションの次のオプションも設定できます

代替データストリーム(ADS)を検査

NTFSファイルシステムによって使用される代替データストリームは、通常の検査技術では検出できないファイルとフォルダの関連付けです。多くのマルウェアが、自らを代替データストリームに見せかけることによって、検出を逃れようとします。

低優先でバックグラウンド検査

検査が行われるたびに、一定の量のシステムリソースが使用されます。システムリソースにかなりの負荷がかかるプログラムを使用している場合、優先度が低い検査をバックグラウンドで実行することによって、アプリケーションのためにリソースを節約することができます。

すべてのオブジェクトをログに記録する

このオプションを選択すると、検査済みのファイルをすべて記録します。

スマート最適化を有効にする

SMART最適化を有効にすると、スキャンの速度を最高に保ちながら最も効率的なスキャンレベルが確保されるように、最適な設定が使用されます。さまざまな保護モジュールで高度に検査を行い、それぞれで異なる検査方法を使用して、それらを特定のファイルタイプに適用します。SMART最適化を無効にすると、特定のモジュールのThreatSenseコアのユーザー定義設定のみがスキャンの実行時に適用されます。

最終アクセスのタイムスタンプを保持

データバックアップシステムでの利用などを考慮して、検査済みファイルへのアクセス日時を更新せずに元のまま保持するには、このオプションを選択します。

制限

[制限]セクションでは、検査対象のオブジェクトの最大サイズおよびネストされたアーカイブのレベルを指定できます。

既定のオブジェクトの設定

有効にすると、既定の設定を使用します(制限なし)。ESET Server Securityはカスタム設定を無視します。

オブジェクトの最大サイズ

検査対象のオブジェクトの最大サイズを定義します。これにより、特定の保護モジュールでは、指定した値より小さいサイズのオブジェクトのみが検査されます。上級ユーザーが大きいオブジェクトを検査から除外する必要がある場合のみ、このオプションを変更してください。既定値:無制限

オブジェクトの最大検査時間(秒)

オブジェクトの検査の最長時間の値を定義します。ここでユーザー定義の値が入力されていると、検査が終わっているかどうかにかかわらず、その時間が経過すると保護モジュールは検査を停止します。既定値:無制限

アーカイブ検査の設定

アーカイブ検査設定を修正するには、既定のアーカイブ検査の設定をオフにします。

スキャン対象の下限ネストレベル

アーカイブの検査の最大レベルを指定します。既定値:10。メールボックス転送保護で検出されたオブジェクトの場合、実際のネストレベルが+1です。電子メールのアーカイブ添付ファイルは最初のレベルと見なされるためです。

例

ネストレベルが3に設定されている場合、ネストレベル3のアーカイブファイルは実際のレベル2までトランスポート層でのみ検査されます。このため、レベル3までのメールボックス転送保護によってアーカイブを検査する場合は、**アーカイブネストレベル**の値を4に設定します。

スキャン対象ファイルの最大サイズ

このオプションでは、検査対象のアーカイブ(抽出された場合)に含まれているファイルの最大サイズを指定できます。既定値: 無制限

注意

一般的な環境では既定値を変更する理由はないので、その値を変更しないことをお勧めします。

追加の ThreatSense パラメータ

新しく作成および変更されたファイルに適用する追加のThreatSenseパラメータ

新規に作成したファイルや修正したファイルは、感染の可能性が既存ファイルより高くなっています。そのため、それらのファイルは、検査パラメーターを追加して検査します。一般的なウイルス定義ベースの検査方法とともに、アドバンスドヒューリスティックが使用されます。これにより、モジュールのアップデートの公開前でも新しい脅威を検出できます。新規に作成したファイル以外に、自己解凍形式のファイル(SFX)およびランタイムパッカー(内部圧縮された実行可能ファイル)も検査されます。既定では、アーカイブは最大で10番目のネストレベルまで検査され、実際のサイズにかかわらず検査されます。アーカイブ検査設定を変更するには、**[既定のアーカイブスキャンの設定]**オプションを選択解除します。

実行したファイルに適用する追加のThreatSenseパラメータ

既定では、**アドバンスドヒューリスティック検査**はファイル実行時には使用されません。有効にするときには、**スマート最適化**とESET LiveGrid®を有効にし、システムパフォーマンスへの影響を低減することを強くお勧めします。

検査対象外とするファイル拡張子

拡張子はピリオドで区切られるファイル名の一部です。拡張子はファイルのタイプを定義します。ただし、特定の拡張子のファイルを除外する必要がある場合には**ThreatSense**パラメーター設定によって、拡張子に基づく検査からファイルを除外できます。特定のファイルタイプの検査によってアプリケーションが正常に実行されない場合は、除外が有効な場合があります。

例

新しい拡張子をリストに追加するには、**[追加]**をクリックします。拡張子をテキストフィールドに入力します(tmpなど)。**[OK]**をクリックします。**複数の値を入力する**を選択すると、線、カンマ、またはセミコロンで区切られた複数のファイル拡張子を追加できます(たとえば、ドロップダウンメニューから区切り文字として**セミコロン**を選択し、edb;eml;tmpと入力します)。特殊記号?(疑問符)を使用できます。疑問符は任意の記号(?dbなど)を表します。

注意

Windowsオペレーティングシステムのすべてのファイルの拡張子(ファイルタイプ)を表示するには、コントロールパネル>フォルダーオプション>表示の下の既知のファイルタイプの拡張子を表示しないをオフにします。

除外を処理する

プロセス除外機能では、マルウェア対策オンアクセス検査からのみ、アプリケーションプロセスを除外できます。専用サーバー(アプリケーションサーバー、ストレージサーバーなど)の重要なロールのため、あらゆる種類のインシデントからのタイムリーな回復を保証するために定期的なバックアップが欠かせません。バックアップ速度、プロセス整合性、サービスの可用性を改善するために、ファイルレベルのウイルス対策保護と競合すると見なされる一部の手法がバックアップ中に使用されます。同様の問題は、仮想マシンのライブ移行中にも発生する可能性があります。両方の状況を回避する唯一の効果的な方法は、ウイルス対策ソフトウェアを無効にすることです。たとえば、バックアップソリューションのプロセスの場合、このような除外されたプロセスに基づくすべてのファイル処理が無視され、安全であると見なされるため、バックアップ処理の中断を最小限に抑えることができます。除外を作成するときには注意してください。除外されたバックアップツールは、アラートをトリガーせずに感染ファイルにアクセスできます。このため、拡張権限がリアルタイムファイルシステム保護モジュールでのみ許可されています。

プロセス除外では、競合の可能性のリスクを最小化し、除外されたアプリケーションのパフォーマンスを改善します。このようにして、オペレーティングシステムの全体的なパフォーマンスと安定性に好ましい効果を及ぼします。プロセス/アプリケーションの除外は、実行ファイル(.exe)の除外です。

詳細設定 (F5) > 検出エンジン > リアルタイムファイルシステム保護 > 基本 > プロセス除外を使用するか、メインメニューのツール > 実行中のプロセスから実行中のプロセスのリストを使用して、除外されたプロセスのリストに実行ファイルを追加することができます。

この機能は、バックアップツールを除外することを目的としています。バックアップツールのプロセスを検査から除外すると、システムの安定性が保証されるだけでなく、バックアップの実行中に速度が低下しないため、バックアップのパフォーマンスにも影響しません。

例

編集をクリックして、**プロセス除外**管理ウィンドウを開きます。除外を追加し、検査から除外される実行ファイルを参照できます(*Backup-tool.exe*など)。

.exeファイルが除外に追加されても、すぐにはこのプロセスのアクティビティはESET Server Securityによって監視されません。プロセスによって実行されるファイル処理には検査が実行されません。

重要

プロセス実行ファイルを選択するときに、参照機能を使用しない場合は、手動で実行ファイルの完全パスを入力する必要があります。そうでない場合、除外は正しく動作せず、[HIPS](#)はエラーを報告する場合があります。

Add exclusion



Select process executable (*.exe):

C:\Program Files\Backup Tool\Backup-tool.exe

OK

Cancel

既存のプロセスを編集するか、除外から削除することもできます。

注意

Webアクセス保護はこの除外を考慮しません。Webブラウザの実行ファイルを除外しても、ダウンロードされたファイルは検査されます。このため、侵入を検出することができます。このシナリオは例として説明しています。Webブラウザの除外を作成することはお勧めしません。

クラウドベース保護

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。レピュテーションに基づいて新しく発生する脅威を検出し、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。新しい脅威情報はリアルタイムでクラウドに送信されるためESET Malware Research Labはタイムリーに対応し、常に一貫した保護を提供できます。ユーザーは、直接的にはこのプログラムのインターフェースやコンテキストメニューを用いるか、あるいはESET LiveGrid®に用意されている追加情報を読んで、稼働中のプロセスやファイルの評価をチェックすることができます。

ESET Server Securityをインストールするときには、次のオプションのいずれかを選択します。

- ESET LiveGrid®を有効にしないこともできます。ソフトウェアの機能は一切失われませんが、場合によってはESET Server Securityの新しい脅威への対応が、検出エンジンデータベースアップデートよりも遅くなることがあります。
- 新しいウイルスと新しい危険なコードが検出された場所に関する匿名の情報を提出するようにESET LiveGrid®を設定することができます。このファイルをESETに送信して詳しい解析を受けることができます。これらのウイルスを調査することでESETはウイルス検出機能を最新のものにすることができます。

ESET LiveGrid®は、新しく検出されたウイルスに関連して、コンピューターに関する情報を収集します。この情報には、ウイルスが検出されたファイルのサンプルまたはコピー、そのファイルのパス、ファイル名、日時、ウイルスがコンピューターに侵入したプロセス、およびコンピューターのオペレーティングシステムについての情報が含まれます。

既定ではESET Server Securityは、疑わしいファイルを解析するためにESETのウイルスラボに送信するように設定されています。.docxまたは.xlsxなど、特定の拡張子の付いたファイルは、常に除外されます。お客様やお客様の組織で送信したくない特定のファイルがあれば、他の拡張子を追加することもできます。

ESET LiveGrid®レピュテーションシステムを有効にする (推奨)

ESET LiveGrid®レピュテーションシステムは、検査済みファイルをクラウドのホワイトリストおよび

ブラックリスト項目のデータベースと比較し、ESETマルウェア対策ソリューションの効率化を図ります。

ESET LiveGrid®フィードバックシステムを有効にする

データは詳細分析のためESET研究所に送信されます。

クラッシュレポートと診断データを送信

クラッシュレポート、モジュール、またはメモリダンプなどのデータを送信します。

匿名で統計情報を送付する

脅威名、脅威の日時、検出方法、関連付けられたメタデータ、製品バージョンと設定(システム情報を含む)などの新しく検出された脅威、検査されたファイル(ハッシュ、ファイル名、ファイルの作成元、テレメトリー)、ブロックされたURL、不審なURLに関する情報を収集します。

連絡先の電子メールアドレス(任意)

不審なファイルに連絡先の電子メールアドレスを添付することができます。この電子メールアドレスは、分析のために詳しい情報が必要な場合の連絡先として使用されます。詳しい情報が必要でない限り、ESETから連絡することはありません。

☐ サンプルの送信

感染したサンプルの自動送信

分析および将来の検出を改善する目的で、すべての感染したサンプルをESETに送信します。

- すべての感染したサンプル
- 文書を除くすべてのサンプル
- 送信しない

不審なサンプルの自動送信

脅威に似た疑わしいサンプル、異常な特性や動作を持つサンプルは、分析のためにESETに送信されます。

- **実行ファイル** – 次の実行ファイルタイプが含まれます。*.exe, .dll, .sys*
- **アーカイブ** – 次のアーカイブファイルタイプが含まれます。*.zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab*
- **スクリプト** – 次のスクリプトファイルタイプが含まれます。*.bat, .cmd, .hta, .js, .vbs, .js, .ps1*
- **その他** – 次のファイルタイプが含まれます。*.jar, .reg, .msi, .swf, .lnk*
- **考えられる迷惑メール** – 迷惑メールのグローバル検出を改善します。
- **文書** – アクティブなコンテンツがあるMicrosoft Office文書やPDFが含まれます。

除外



ESET LiveGrid®の除外の横の[編集](#)オプションをクリックすると、分析を受けるためにESETのウイル

スラボに不審なファイルを提出する方法を設定することができます。

サンプルの最大サイズ(MB)

検査対象のサンプルの最大サイズを定義します。


ESET Dynamic Threat Defense

ESET PROTECT Webコンソールを使用しているクライアントコンピューターで[ESET Dynamic Threat Defense](#)  サービスを有効にします。ESET PROTECT Webコンソールで、[新しいポリシーを作成](#)  するか、既存のポリシーを編集してESET Dynamic Threat Defenseを使用するコンピューターに割り当てます。

除外フィルタ

除外フィルタを使用すると、特定のファイルまたはフォルダを送信から除外できます(例: ドキュメントやスプレッドシートなど、機密情報が含まれる可能性があるファイルを除外する場合に便利があります)。このリスト内のファイルは、疑わしいコードを含んでいても、解析のためにESETのラボに送信されることはありません。最も一般的なファイルの種類(.doc.docなど)は、既定で除外されます。必要に応じて、除外するファイルの一覧に追加することもできます。

以前にESETLiveGrid®を使用したことがあり、その後で無効にした場合、送信するデータパッケージが残っていることがあります。無効にした後でも、このようなパッケージはESETに送信されます。すべての最新情報が送信されると、パッケージはこれ以上作成されません。

Add exclusion

Enter a path name and mask that defines the files you want to exclude.
An asterisk '*' denotes any number of any characters whereas '?' denotes a single character. e.g., *.TXT means you are selecting all text files of any name.

Folder...

File...

Enter multiple values

OK

Cancel

不審なファイルがある場合は、ESETのウイルスラボに提出して分析を受けることができます。そのファイルが悪意のあるアプリケーションであることが判明すると、以降の検出モジュールのアップデートで反映されます。

マルウェア検査

このセクションには、検査パラメーターを選択するオプションがあります。

注意

この検査プロファイルセクターは、オンデマンド検査、[Hyper-V検査](#)、および[OneDrive検査](#)に適用されます。

選択されたプロファイル

オンデマンドスキャナーで使用する特定のパラメーターのセット、定義済みの検査プロファイルのいずれかを使用するか、新しいプロファイルを作成できます。検査プロファイルは、さまざまな [ThreatSense エンジンパラメーターを使用できます。](#)

プロファイルのリスト

新しいプロファイルを作成するには、**[編集]** をクリックします。プロファイル名を入力し、**追加** をクリックします。新しいプロファイルは、既存の検査プロファイルが一覧表示される **選択されたプロファイル** ドロップダウンメニューに表示されます。

検査の対象

特定の対象を検査する場合は、**編集** をクリックし、ドロップダウンメニューからオプションを選択するか、フォルダ(ツリー)構造から特定の対象を選択します。

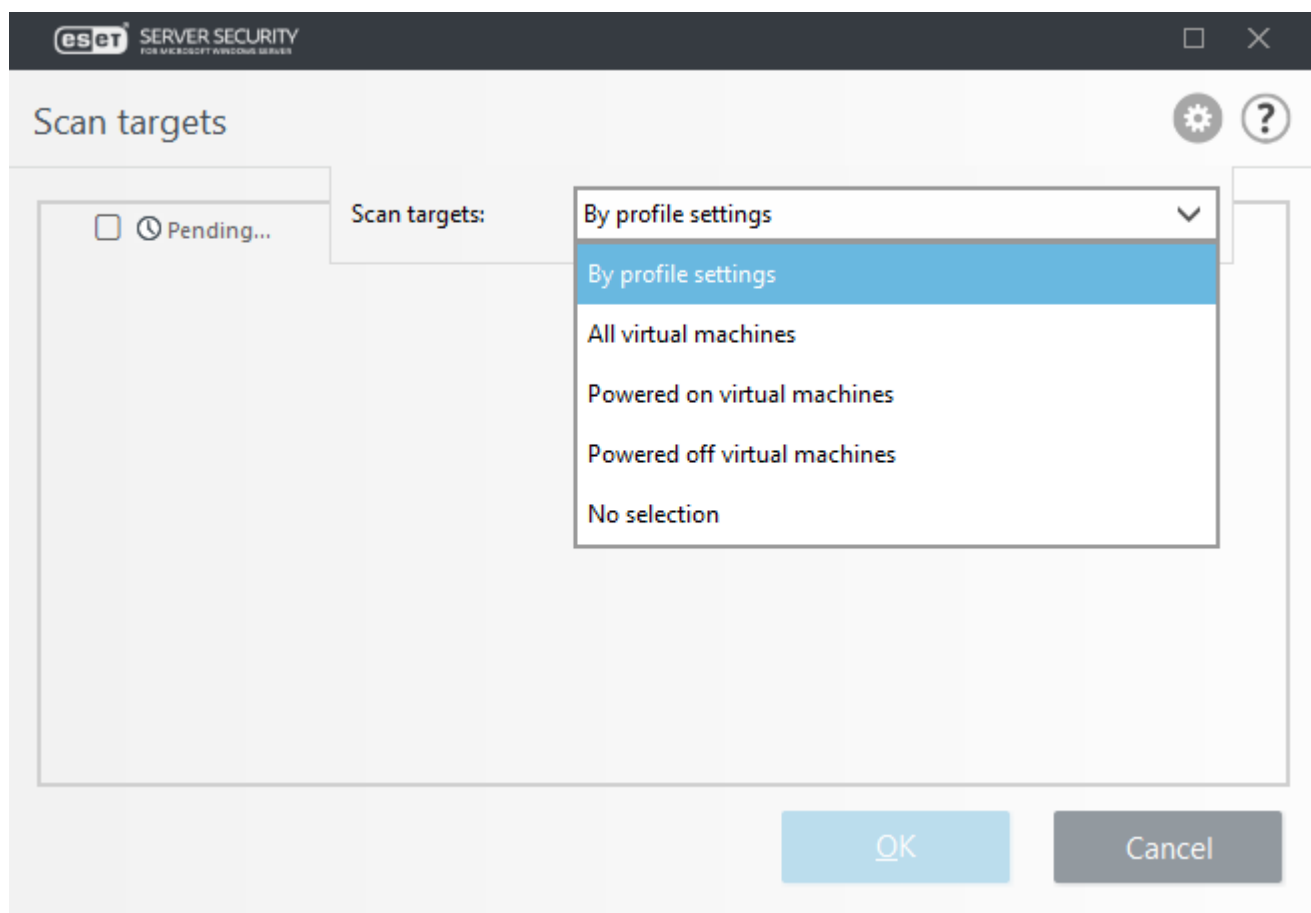
ThreatSense パラメータ

オンデマンドコンピュートースキャナーの検査パラメータを修正します。

オンデマンド保護および機械学習保護

レポートは、検出エンジンと機械学習コンポーネントによって実行されます。

Hyper-V検査 ポップアップウィンドウ:



[Hyper-V検査の対象] ドロップダウンメニューでは、事前定義されている次の検査対象を選択できます。

プロファイル設定によって	選択された検査プロファイルに設定されている対象を選択します。
すべての仮想マシン	すべての仮想マシンを選択します。

プロファイル設定によって	選択された検査プロファイルに設定されている対象を選択します。
電源が入っている仮想マシン	すべてのオンラインの仮想マシンを選択します。
電源が入っていない仮想マシン	すべてのオフラインの仮想マシンを選択します。
選択肢なし	すべての選択をクリアします。

設定したカスタムパラメータを使用して検査を実行するには、[検査]をクリックします。すべての検査が完了した後に、ログファイル > [Hyper-V検査](#) をチェックします。

プロファイルマネージャ

[検査プロファイル] ドロップダウンメニューでは、事前定義されている次の検査プロファイルを選択できます。

- スマート検査
- コンテキストメニューの検査
- 詳細検査
- マイプロファイル([Hyper-V検査](#) [プロファイルのアップデート](#) および [OneDrive検査](#) に適用)

各自のニーズに合った検査プロファイルを作成するための参考情報として、「[ThreatSense エンジンのパラメーターの設定](#)」にある検査設定の各パラメーターの説明を参照してください。

プロファイルマネージャは、ESET Server Securityの3つの場所で使用されます。

コンピュータの検査

目的の検査パラメーターを保存して、後で検査を行う際に使用できます。さまざまな検査対象、検査方法、およびその他のパラメーターについて、定期的に行う検査ごとにプロファイルを作成することをお勧めします。

[アップデート](#)

プロファイルエディタを使用すると、新しい最新のプロファイルを作成できます。コンピューターが複数の手段を使用して、アップデートサーバーに接続する場合にのみ、カスタムアップデートプロファイルを作成する必要があります。



[Hyper-V検査](#)

新しいプロファイルを作成するには、[プロファイルのリスト]の横の[編集]を選択し、新しいプロファイルは、既存の検査プロファイルが一覧表示される**選択されたプロファイル**ドロップダウンメニューに表示されます。

[OneDrive検査](#)

新しいプロファイルを作成するには、[プロファイルのリスト]の横の[編集]を選択し、新しいプロファイルは、既存の検査プロファイルが一覧表示される**選択されたプロファイル**ドロップダウンメニューに表示されます。

プロファイルターゲット

侵入の検査対象を指定できます。システムのすべての使用可能な対象を一覧で示すツリー構造からオブジェクトを選択します(メモリ、ブートセクタ  UEFI  ドライブ、ファイル、フォルダー、ネットワーク)。左上の歯車アイコンをクリックすると、**検査対象**と**検査プロファイル**ドロップダウンメニューが開きま

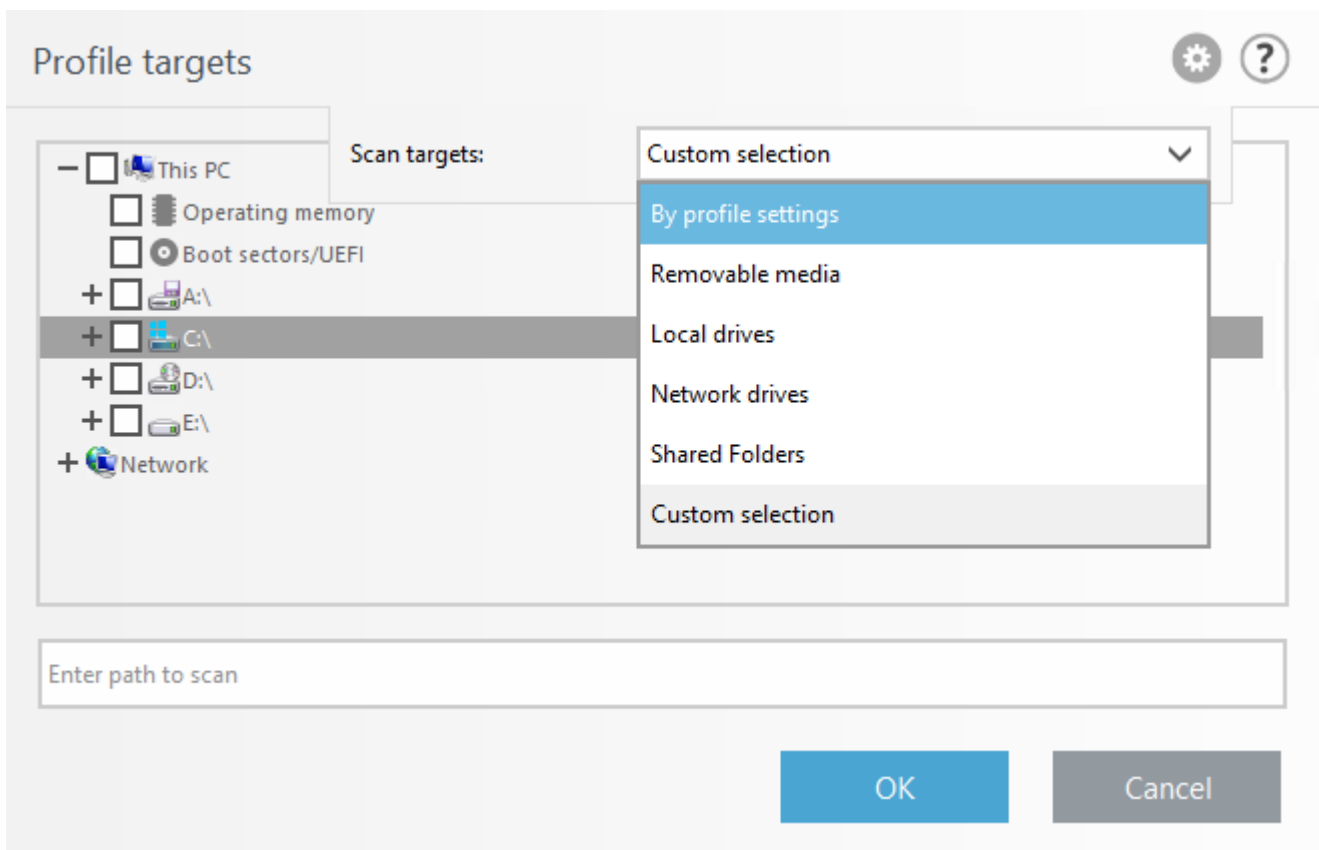
す。

注意

この検査プロファイルセクターは、オンデマンド検査、[Hyper-V検査](#)、および[OneDrive検査](#)に適用されます。

メモリ	現在オペレーティングメモリで使用されているすべてのプロセスとデータを検査します。
ブートセクタ/UEFI	ブートセクターとUEFIのマルウェア検査を実行します。 用語集 のUEFIスキャナーの詳細をお読みください。
WMIデータベース	Windows Management Instrumentation (WMI)データベース全体、すべての名前空間、すべてのクラスインスタンス、すべてのプロパティを検査します。データとして埋め込まれた感染ファイルまたはマルウェアへの参照を検索します。
システムレジストリ	システムレジストリ全体、すべてのキー、およびサブキーを検査します。データとして埋め込まれた感染ファイルまたはマルウェアへの参照を検索します。検出を駆除する際には、レジストリに参照が残り、重要なデータが失われないのを確認できます。

検査対象にすばやく移動したり、対象のフォルダーまたはファイルを追加するには、フォルダーリストの下空白のフィールドに対象ディレクトリを入力します。



[検査の対象] ドロップダウンメニューでは、事前定義されている次の検査対象を選択できます。

プロファイル設定によって	選択された検査プロファイルに設定されている対象を選択します。
リムーバブルメディア	フロッピーディスク、USB記憶装置、CD/DVDを選択します。
ローカルドライブ	システムハードディスクをすべて選択します。
ネットワークドライブ	マッピングされたネットワークドライブをすべて選択します。
共有フォルダー	共有されるローカルサーバー上のすべてのフォルダを選択します。
カスタム選択	すべての選択をクリアします。クリアすると、カスタム選択を行えます。

検査に含めるために、検査対象(ファイルまたはフォルダー)にすばやく移動するには、パスをツリー構造の下テキストフィールドに入力します。パスエントリは大文字と小文字を区別します。

[**検査プロファイル**] ドロップダウンメニューでは、事前定義されている次の検査プロファイルを選択できます。

- **スマート検査**
- **コンテキストメニューの検査**
- **詳細検査**

これらの検査プロファイルは、異なる [ThreatSense エンジンパラメーター](#) を使用します。

駆除せずに検査する

システムの検査で追加の駆除アクションを実行する必要がない場合は、[**駆除せずに検査する**]を選択します。感染している項目があり、これらの感染に関する詳細を取得するか(該当する場合)どうかに関する概要のみを取得する場合に有用です。**設定 > ThreatSense パラメータ > 駆除**をクリックして、3つの駆除レベルから選択できます。検査に関する情報は、検査ログに保存されます。

除外を無視

[**除外を無視する**]を選択すると、通常は適用される [除外](#) を無視して検査を実行できます。

検査の対象

特定の対象のみを検査する場合は、[**カスタム検査**]を使用し、**検査対象**ドロップダウンメニューからオプションを選択するか、フォルダ(ツリー)構造から特定の対象を選択します。

検査対象プロファイルセレクトは次の項目に適用されます。

- [オンデマンド検査](#)
- [Hyper-V検査](#)
- [OneDrive検査](#)

検査対象にすばやく移動したり、新しい対象ファイルまたはフォルダーを追加するには、フォルダリストの下空白のフィールドに対象を入力します。これが可能なのは、ツリー構造内で対象を選択しておらず、[**検査の対象**]メニューに[**選択肢なし**]が設定されている場合のみです。

メモリ	現在オペレーティングメモリで使用されているすべてのプロセスとデータを検査します。
ブートセクタ/UEFI	ブートセクタとUEFIのマルウェア検査を実行します。 用語集 のUEFIスキャナーの詳細をお読みください。
WMIデータベース	Windows Management Instrumentation (WMI)データベース全体、すべての名前空間、すべてのクラスインスタンス、すべてのプロパティを検査します。データとして埋め込まれた感染ファイルまたはマルウェアへの参照を検索します。
システムレジストリ	システムレジストリ全体、すべてのキー、およびサブキーを検査します。データとして埋め込まれた感染ファイルまたはマルウェアへの参照を検索します。検出を駆除する際には、レジストリに参照が残る、重要なデータが失われないのを確認できます。

[**検査の対象**] ドロップダウンメニューでは、事前定義されている次の検査対象を選択できます。

プロファイル設定によって	選択された検査プロファイルに設定されている対象を選択します。
リムーバブルメディア	フロッピーディスク、USB記憶装置、CD/DVDを選択します。
ローカルドライブ	システムハードディスクをすべて選択します。

プロファイル設定によって	選択された検査プロファイルに設定されている対象を選択します。
ネットワークドライブ	マッピングされたネットワークドライブをすべて選択します。
共有フォルダー	共有されるローカルサーバー上のすべてのフォルダを選択します。
カスタム選択	すべての選択をクリアします。クリアすると、カスタム選択を行えます。

選択した対象の検査に使用するプロファイルを、[\[検査プロファイル\]](#)ドロップダウンメニューから選択できます。既定のプロファイルは[\[スマート検査\]](#)です。さらに、[\[詳細検査\]](#)および[\[コンテキストメニュー検査\]](#)という2つの事前定義された検査プロファイルがあります。これらの検査プロファイルでは、さまざまな[ThreatSenseエンジンパラメーター](#)を使用します。

カスタム検査ポップアップウィンドウ:

駆除せずに検査する

システムの検査で追加の駆除アクションを実行する必要がない場合は、[\[駆除せずに検査する\]](#)を選択します。感染している項目があり、これらの感染に関する詳細を取得するか(該当する場合)どうかに関する概要のみを取得する場合に有用です。[設定 > ThreatSenseパラメータ > 駆除](#)をクリックして、3つの駆除レベルから選択できます。検査に関する情報は、検査ログに保存されます。

除外を無視

通常は適用される[除外](#)を無視して検査を実行できます。

検査

設定したカスタムパラメータを使用して検査を実行します。

管理者として検査

管理者アカウントで検査を実行できます。検査対象のファイルにアクセスするための権限がないユー

ザーでログインしている場合は、これをクリックします。現在ログインしているユーザーが管理者としてユーザーアカウント制御を呼び出せない場合、このボタンは使用できません。

アイドル状態検査

コンピューターがアイドル状態になると、すべてのローカルドライブでコンピューターの検査がサイレントに実行されます。コンピューターが次の状態のときに、**アイドル状態検出**が実行されます。

- 画面またはスクリーンセーバーをオフにしました
- コンピュータのロック
- ユーザー ログオフ

コンピューターがバッテリー電源で動作している場合にも実行する

既定では、アイドル状態検出はコンピューター(ノートパソコン)がバッテリー電源で動作しているときは実行されません。

ログを有効にする

[ログファイル](#)にコンピューターの検査の結果を記録するには、詳細設定の[ログを有効にする]を選択します(プログラムのメインウィンドウで[ログファイル]をクリックし、ドロップダウンメニューから[コンピューターの検査]を選択します)。

[ThreatSense パラメータ](#)

アイドル状態スキャナの検査パラメータを変更します。

スタートアップ検査

既定では、システムの起動(ユーザーログオン)時およびモジュールアップデートの成功後に自動起動ファイルの検査が実行されます。この検査は、[スケジューラの設定およびタスク](#)によって制御されます。

スタートアップ検査の設定は、[システムのスタートアップファイルのチェック]のスケジューラタスクに含まれます。

スタートアップ検査設定を修正するには、[ツール]>[\[スケジューラ\]](#)と移動し、[\[自動スタートアップファイルのチェック\]](#) (ユーザーログオンまたはモジュールアップデート)、[\[編集...\]](#)の順にクリックします。ウィザードの残りでクリックすると、最後のステップでは、[\[自動スタートアップファイルのチェック\]](#)の詳細オプションを修正できます。

自動スタートアップファイルのチェック

システム起動時のファイルチェックスケジューラタスクを作成するときに、次のパラメータを調整するいくつかのオプションがあります。

検査対象 - システム起動時に実行されるファイルの検査のレベルを指定します。ファイルは次の基準に従って昇順で整理されます。

- すべての登録ファイル (検査対象のファイル数は最多)
- 使用頻度が低いファイル
- 検査レベル

- 使用頻度が高いファイル
- 最も使用頻度が高いファイルのみ（検査対象のファイル数は最小）

次の2つの検査対象グループも含まれます。

ユーザーログオン前のファイル実行

ユーザーがログオンしていない状態でアクセスできる場所のファイルが含まれます(サービス、ブラウザヘルパーオブジェクト、Winlogon通知、Windowsスケジューラのエントリ、既知のdllといったスタートアップの場所にあるすべてのファイル)。

ユーザーログオン後のファイル実行

ユーザーがログオンした後にのみアクセスできる場所にあるファイル(特定のユーザーだけが実行するファイル、通常は `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` にあるファイル)が含まれます。

検査対象のファイルのリストは、上記の各グループごとに固定されます。

検査の優先度

以下のとおりの、検査をいつ開始するかを決定するために使用する優先度レベル。

- 通常 – システム負荷は平均的
- 低 – システム負荷は低い
- ミニダンプ – システム負荷が可能なかぎり低い場合
- アイドル時 – システムのアイドル時にのみタスクが実行されます。

リムーバブルメディア

ESET Server Securityにはリムーバブルメディア(CD/DVD/USB)を自動的に検査する機能があります。このモジュールを使用すると、挿入したメディアを検査できます。この機能は、ユーザーが求めたものでないコンテンツを収めたリムーバブルメディアのユーザーによる使用を防止したいコンピュータ管理者にとって便利です。

リムーバブルメディアの挿入後に行うアクション

リムーバブルメディアデバイスがコンピュータに挿入されたときに実行するアクションを選択します(CD/DVD/USB)

- 検査しない – アクションは実行されず、[新規デバイスの検出]ウィンドウが閉じられます。
- 自動デバイス検査 – 挿入したリムーバブルメディアに対してコンピュータの検査が実行されます。
- 検査オプションを表示する – [リムーバブルメディア]設定セクションが開きます。

リムーバブルメディアを挿入すると、次のダイアログが表示されます。

- 今すぐ検査 – リムーバブルメディアの検査を開始します。
- 後で検査 – リムーバブルメディアの検査が延期されます。
- 設定 – 詳細設定を開きます。
- 選択したオプションを常に使用する – これを選択すると、リムーバブルメディアが別の時間に挿入されたときに同じアクションが実行されます。

またESET Server Securityは、所定のコンピューター上で外部デバイスを使用するためのルールを定義す

ることができるデバイスコントロールの役割も果たします。デバイスコントロールの詳細については、「[デバイスコントロール](#)」セクションで参照することができます。

ドキュメント保護

ドキュメントの保護機能により、Microsoft Officeドキュメントの検査(開く前に実行)、およびInternet Explorerにより自動的にダウンロードされたファイル(Microsoft ActiveX要素など)の検査が行われます。ドキュメントの保護により、リアルタイムファイルシステム保護に加えてさらに別段の保護が提供されますが、大量のMicrosoft Officeドキュメントを扱わないシステムでは、パフォーマンスを向上させるためにこれを無効にすることができます。

システムに統合

このオプションはMicrosoft Office文書の保護を強化します(通常の状態では必要ありません)。

ThreatSense パラメータ

ドキュメント保護のパラメーターを修正します。

注意

この機能は、Microsoft Antivirus API (Microsoft Office 2000以上、Microsoft Internet Explorer 5.0以上など)を使用するアプリケーションで有効化されます。

Hyper-V検査

現在のバージョンのHyper-V検査は、Hyper-Vのオンラインまたはオフライン仮想システムの検査をサポートします。ホストされたWindows Hyper-Vシステムおよび仮想システムの状態に従って検査のサポートされた種類が以下に示されます。

Hyper-V機能がある仮想システム	Windows Server 2008 R2 SP1 Hyper-V	Windows Server 2012 Hyper-V	Windows Server 2012 R2 Hyper-V	Windows Server 2016 Hyper-V	Windows Server 2019 Hyper-V	Windows Server 2022 Hyper-V
オンラインVM	検査なし	読取専用	読取専用	読取専用	読取専用	読取専用
オフラインVM	読み取り専用/駆除	読み取り専用/駆除	読み取り専用/駆除	読み取り専用/駆除	読み取り専用/駆除	読み取り専用/駆除

ハードウェア要件

サーバーには、仮想マシンを実行する際のパフォーマンスの問題がありません。検査アクティビティは、主に、CPUリソースを使用します。オンラインVMの検査では空きディスク領域が必要です。ディスク領域は、チェックポイントスナップショットと仮想ディスクで使用する領域の2倍以上でなければなりません。

固有の制限事項

- RAIDストレージ、スパンボリューム、および[動的ディスク](#)での検査は、動的ディスクの性質によりサポートされていません。このため、可能なかぎりVMで動的ディスクタイプを使用しないことをお勧めします。
- 検査は常に現在のVMで実行され、チェックポイントまたはスナップショットには影響しません。

- クラスタのホストで実行されているHyper-Vは現在ESET Server Securityによってサポートされていません。
- Windows Server 2008 R2 SP1で実行されているHyper-Vホストの仮想マシンは[ThreatSenseパラメーター](#) (駆除しない) で選択された駆除レベルに関係なく、読み取り専用モードでのみ検査できます。

注意

ESET Securityは仮想ディスクMBRの検査をサポートしますが、これらの対象の読み取り専用検査のみがサポートされます。この設定は、[詳細設定] (F5) > 検出エンジン > [Hyper-V検査] > [\[ThreatSenseパラメーター\]](#) > [ブートセクター] で変更できます。

検査対象の仮想マシンがオフライン - オフ状態に切り替わりました

ESET Server Securityは Hyper-V Managementを使用して、仮想ディスクを検出して接続します。このようにESET Server Securityには、汎用ドライブのデータとファイルにアクセスする場合のように、仮想ディスクの内容にアクセスできます。

検査対象の仮想マシンがオンライン - 実行中、一時停止、保存状態

ESET Server Securityは Hyper-V Managementを使用して、仮想ディスクを検出します。これらのディスクへの実際の接続はできません。このためESET Server Securityは仮想マシンのチェックポイント/スナップショットを作成してから、チェックポイント/スナップショットに接続します。検査が完了したら、チェックポイント/スナップショットは削除されます。つまり、読み取り専用検査は、実行中の仮想マシンが検査アクティビティの影響を受けないため、実行できます。

ESET Server Securityが検査中にスナップショットまたはチェックポイントを作成するには最大1分かかります。多数の仮想マシンでHyper-V検査を実行するときには、この点を考慮してください。

命名規則

Hyper-V検査のモジュールは次の命名規則に従います。

VirtualMachineName\DiskX\VolumeY

Xはディスク数、Yはボリューム数です。例:

Computer\Disk0\Volume1

数字のサフィックスは、VMのディスクマネージャに表示される順序と同じ検出順で、追加されます。この命名規則は、検査対象のツリー構造リスト、進行状況バー、ログファイルで使用されます。

検査の実行

- [オンデマンド - Hyper-V 検査](#) をクリックすると、検査可能な仮想マシンおよびボリュームのリストが表示されます。検査する仮想マシン、ディスク、またはボリュームを選択し、**検査** をクリックします。
- [スケジューラタスクを作成する](#)
- [サーバー検査](#) ☒ クライアントタスクとして ESET PROTECT を使用
- Hyper-V検査は、[eShell](#) 経由で管理および開始できます。

複数のHyper-V検査を同時に実行できます。検査が完了したときには、ログファイルへのリンクが付いた通知を受信します。

想定される問題

- オンライン仮想マシンの検査を実行するときには、特定の仮想マシンのチェックポイント/スナップショットを作成する必要があります。チェックポイント/スナップショットの作成中には、仮想マシンの一部の汎用処理が制限または無効化される場合があります。
- オフライン仮想マシンの検査中には、検査が完了するまでオフにできません。
- Hyper-V Managerでは、2つの異なる仮想マシンに同じ名前を指定できるため、検査ログの確認中にコンピュータを識別できない場合があります。

OneDrive検査

基本

アクションと隔離を設定できます

ファイルが感染している場合に実行するアクション

- **アクションなし** – ファイルの変更は適用されません。
- **削除 - 隔離** – ファイルは隔離に移動し、OneDriveのファイルを削除します。ただし、ファイルは、OneDriveごみ箱にあります。

感染ファイルの隔離

有効にすると、削除に設定されたファイルは隔離に移動されます。この設定を解除すると、隔離が無効になるため、ファイルは隔離に保存されません。

詳細

この部分にはOneDrive検査登録に関する情報(アプリケーションID、AzureポータルオブジェクトID、証明書サムプリント)が含まれます。タイムアウトと同時ダウンロード制限を設定できます。

プロファイル

新しいプロファイルを作成するには、[プロファイルのリスト]の横の[編集]を選択し、[プロファイル名]フィールドに自分の名前を入力して、[追加]をクリックします。新しいプロファイルは、既存の検査プロファイルが一覧表示される**選択されたプロファイル**ドロップダウンメニューに表示されます。

[検査の対象] ドロップダウンメニューでは、事前定義されている次の検査対象を選択できます。

- **プロファイルに依存** – 選択された検査プロファイルに設定されている対象を選択します。
- **すべてのユーザー** – すべてのユーザーを選択します。
- **選択なし** – 現在の選択をクリアします。

設定したカスタムパラメータを使用して検査を実行するには、[検査]をクリックします。すべての検査が完了した後に、ログファイル > [OneDrive検査](#) をチェックします。

ThreatSense パラメータ

OneDrive スキャナーの検査パラメータを変更します。

レポートは、検出エンジンと機械学習コンポーネントによって実行されます。

HIPS

Host-based Intrusion Prevention System (HIPS)により、コンピュータ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はリアルタイムファイルシステム保護とは異なります。ファイアウォールでもありません。

警告

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

ESET Server Securityには、悪意のあるソフトウェアによってマルウェア保護機能が破損されたり無効化されたりしないようにする、自己防衛技術が組み込まれているため、システムが常時確実に保護されます。HIPSを有効にする]設定と[自己防衛を有効にする]設定の変更内容は、Windowsオペレーティングシステムの再起動後に有効になります。HIPSシステム全体を無効にする場合にも、コンピュータの再起動が必要になります。

保護されたサービスを有効にする

Microsoftは、Microsoft Windows Server 2012 R2で保護されたサービスの概念を導入しました。これにより、マルウェア攻撃に対するサービスが防止されます。ESET Server Securityのカーネルは既定で保護されたサービスとして実行されます。この機能は、Microsoft Windows Server 2012 R2以降のサーバーオペレーティングシステムで利用できます。

有効にする Advanced Memory Scanner

エクスプロイトブロッカーとともに動作し、難読化または暗号化を使用することで、マルウェア対策製品の検出を回避するように設計されたマルウェアに対する保護を強化します。既定では、詳細メモリ検査が有効です。この保護の詳細については、「[用語集](#)」を参照してください。

エクスプロイトブロックを有効にする

Webブラウザ、PDFリーダー、電子メールクライアント、MS Officeコンポーネントなどの一般的に利用されるアプリケーションタイプの保護を強化するための機能です。既定では、エクスプロイトブロッカーが有効です。この保護の詳細については、「[用語集](#)」を参照してください。

ランサムウェアシールドを有効にする

この機能を使用するには、HIPSおよびESET Live Gridを有効にします。[用語集](#)のランサムウェアをお読みください。

フィルタリングモード

次のフィルタリングモードのいずれかを選択します。

- **自動モード** – 操作は、システムを保護する事前定義ルールでブロックされる操作を除いて有効

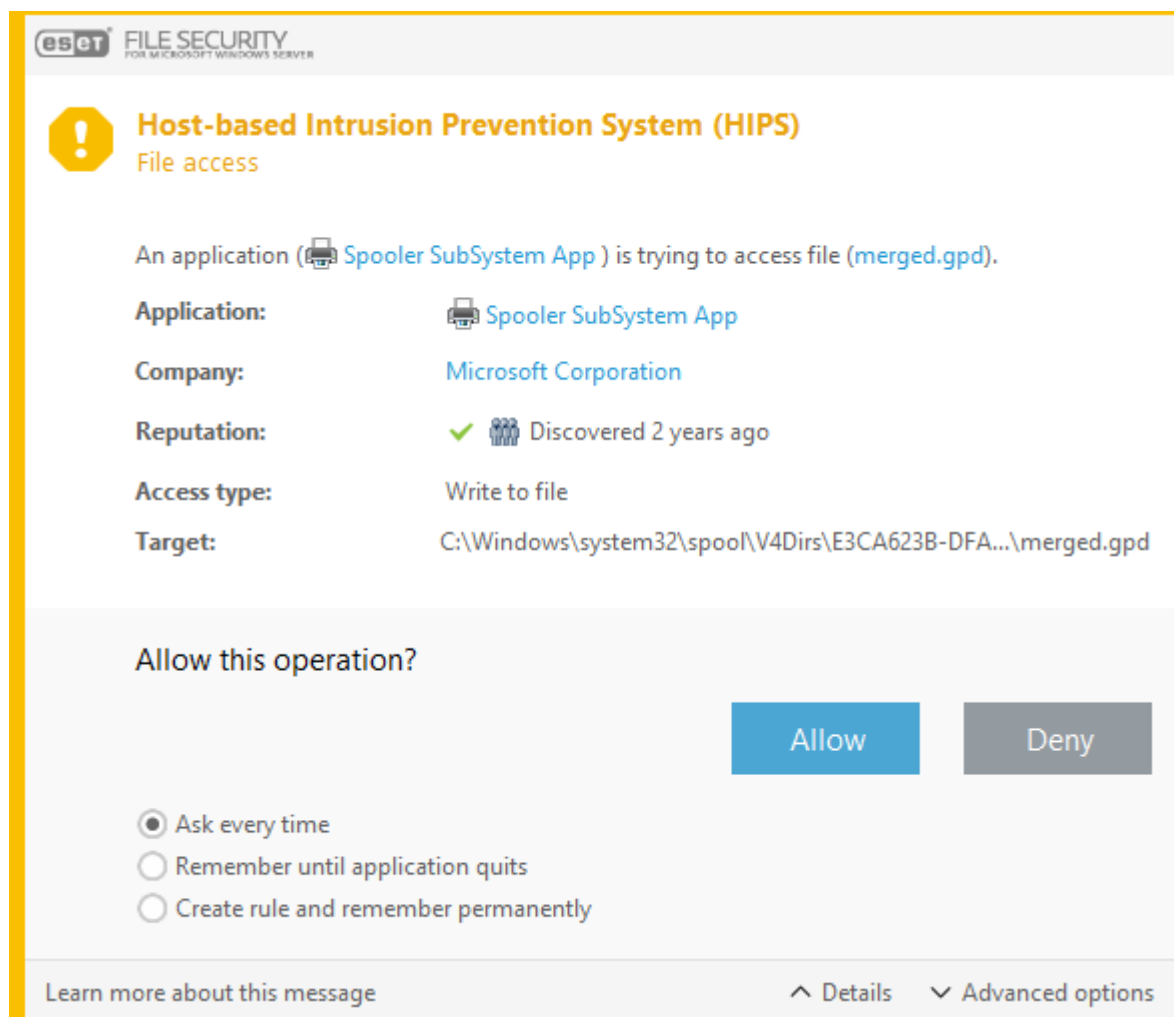
です。ルールで拒否されたアクションを除くすべてが許可されます。

- **スマートモード** – 非常に不審なイベントに関する通知だけが表示されます。
- **対話モード** – ユーザーは操作を確定するよう要求されます。アクセスを許可/拒否、ルールを作成、このアクションを一時的に記憶することができます。
- **ポリシーベースモード** – 操作はブロックされます。ユーザー/定義済みルールのみを許可します。
- **学習モード** – 操作は有効で、各操作の後にルールが作成されます。このモードで作成されたルールは、ルールエディタで表示できますが、手動で作成したルールや、自動モードで作成されるルールより優先度は低くなります。HIPSフィルタリングモードドロップダウンメニューで**学習モード**を選択すると、**[学習モードが終了]**設定が使用できるようになります。学習モードを有効にする期間を選択します。最大期間は14日です。指定した期間が過ぎると、学習モード中にHIPSで作成されたルールを編集するように指示されます。別のフィルタリングモードを選択するか、決定を延期し、学習モードを使用し続けることもできます。

ルール

ルールは、アプリケーションがアクセスを許可されるファイル、レジストリの一部、他のアプリケーションを決定します。HIPSシステムはオペレーティングシステム内部のイベントを監視し、パーソナルファイアウォールで使用されるルールに似たルールに基づいて対応します。[\[編集\]](#)をクリックしてHIPSルール管理ウィンドウを開きます。ルールの既定のアクションを確認に設定した場合、ルールがトリガーされるたびにダイアログウィンドウが表示されます。操作を**[ブロック]**または**[許可]**することもできます。指定された時間内にアクションを選択しなかった場合は、ルールに基づいて新しいアクションが選択されます。

このダイアログウィンドウではHIPSが検出した新しいアクションを基にルールを作成し、そのアクションを**許可**または**ブロック**する条件を定義できます。詳細を表示するには、**[詳細]**をクリックしてアクセスできます。この方法で作成したルールは手動で作成したルールと同等であるとみなされるため、ダイアログウィンドウから作成したルールは、そのダイアログウィンドウをトリガしたルールより汎用的にすることができます。つまり、そのようなルールを作成した場合、同じ操作で同じウィンドウをトリガできます。



毎回確認します

ルールがトリガーされるたびに、ダイアログウィンドウが表示されます。処理の**拒否**または**許可**を選択できます。

アプリケーションが終了するまで記憶

拒否または**許可**処理を選択すると、該当するアプリケーションが終了するまで使用される一時HIPSルールが作成されます。また、フィルタリングモードを変更するか、ルールを変更するかHIPSモジュールが更新され、システムを再起動する場合は、一時ルールが削除されます。

ルールを作成し、永久に記憶

新しいHIPSルールを作成します。後からHIPSルール管理セクションでこのルールを変更できます。

HIPSルール設定

このウィンドウには、既存のHIPSルールの概要が表示されます。

ルール	ユーザーが定義したか、または自動選択されたルール名。
有効	ルールをリスト内に置いたまま、使用しない場合にこのチェックボックスをオフにします。
アクション	ルールは、条件が一致した場合に実行する必要があるアクション、つまり[許可][拒否]、または[確認]を指定します。
ソース	ルールは、このアプリケーションによってイベントが起動された場合のみ使用されます。

ルール	ユーザーが定義したか、または自動選択されたルール名。
ターゲット	操作が特定のファイル、アプリケーション、レジストリエントリに関連付けられている場合にのみ、このルールが使用されます。
ログ重大度	このオプションをオンにすると、このルールに関する情報が HIPSログ に書き込まれます。
通知	イベントが起動された場合に、小さいポップアップウィンドウが右下隅に表示されます。

新しいルールを作成し、**新しいHIPSルールの追加**または**選択したエントリの編集**をクリックします。

ルール名

ユーザーが定義したか、または自動選択されたルール名。

アクション

ルールは、条件が一致した場合に実行する必要のあるアクション、つまり[許可]、[拒否]、または[確認]を指定します。

動作影響

ルールが適用される処理のタイプを選択する必要があります。ルールは、選択された[ターゲット]に対するこのタイプの操作に限り使用されます。ルールは、このルールの使用をトリガする条件を記述した部分で構成されます。

ソースアプリケーション

ルールは、このアプリケーションによってイベントが起動された場合のみ使用されます。ドロップダウンメニューから**特定のアプリケーション**を選択し、[追加]をクリックして、新しいファイルまたはフォルダを選択します。あるいは、ドロップダウンメニューからすべてのアプリケーションを選択して**すべてのアプリケーション**を追加します。

注意

HIPSで事前定義された特定のルールの操作にはブロックできないものがあり、既定で許可されています。さらに、システムの動作すべてがHIPSにより監視されているわけではありません。HIPSは、危険性があると考えられる動作を監視しています。

主要な操作の説明

ファイルの操作:

ファイルの削除	アプリケーションはターゲットファイルを削除する許可を求めています。
ファイルへの書き込み	アプリケーションはターゲットファイルに書き込む許可を求めています。
ディスクへの直接アクセス	アプリケーションは標準的でない方法でディスクからの読み出しまたは書き込みを行おうとしており、通常のWindowsの手順をたどりません。この結果、対応するルールの適用なしにファイルが変更される場合があります。この動作は、マルウェアが検知されるのを逃れようとしていたり、バックアップソフトウェアがディスクの正確なコピーを作成しようとしていたり、またはパーティションマネージャがディスクボリュームを認識しようとしていたりすることで引き起こされる場合があります。
グローバルフックのインストール	MSDNライブラリからのSetWindowsHookEx関数の呼び出しを指します。

ファイルの削除	アプリケーションはターゲットファイルを削除する許可を求めています。
ドライバの読み込み	システムへのドライバのインストールと読み込み。

ルールは、操作がこのターゲットと関連する場合に限り使用されます。ドロップダウンメニューから**特定のファイル**を選択し、**[追加]**をクリックして、新しいファイルまたはフォルダーを追加します。または、ドロップダウンメニューから**すべてのファイル**を選択してすべてのアプリケーションを追加します。

アプリケーション動作:

別のアプリケーションをデバッグ	デバッガをプロセスにアタッチします。アプリケーションのデバッグ中にそのアプリケーションの動作のさまざまな詳細を表示して変更し、そのデータにアクセスできます。
別のアプリケーションからのイベントの取得	ソースアプリケーションは、特定のアプリケーションを対象としたイベントを取得しようとしています(キーロガーがブラウザのイベントのキャプチャを試みるなど)。
別のアプリケーションの終了/中断	プロセスの中断、再開、終了(Process ExplorerまたはProcessesウィンドウから直接アクセス可能)。
新規アプリケーションの開始	新規のアプリケーションまたはプロセスの開始。
別のアプリケーションの状態を変更	ソースアプリケーションは、ターゲットアプリケーションのメモリに書き込もうとしているか、または代行でコードを実行しようとしています。この機能は、この動作の使用をブロックするルール中で、重要なアプリケーションをターゲットアプリケーションとして設定することによって保護するのに役立ちます。

ルールは、操作がこのターゲットと関連する場合に限り使用されます。ドロップダウンメニューから**特定のアプリケーション**を選択し、**[追加]**をクリックして、新しいファイルまたはフォルダーを追加します。または、ドロップダウンメニューから**すべてのアプリケーション**を選択してすべてのアプリケーションを追加します。

レジストリの操作:

スタートアップ設定の変更	設定(Windows起動時に実行するアプリケーションの定義)の変更。これらは、たとえばWindowsレジストリのRunのキーを検索することによって見つけられます。
レジストリからの削除	レジストリキーまたはその値の削除。
レジストリキー名の変更	レジストリキーの名前の変更。
レジストリの変更	レジストリキーの新しい値の作成、既存の値の変更、データベース ツリー内のデータの移動、またはレジストリキーのユーザー権限またはグループ権限の設定。

ルールは、操作がこのターゲットと関連する場合に限り使用されます。ドロップダウンメニューから**特定のエン트리**を選択し、**[追加]**をクリックして、新しいファイルまたはフォルダーを追加します。または、ドロップダウンメニューから**すべてのエン트리**を選択してすべてのアプリケーションを追加します。

注意

ターゲットの入力では、一定の制限付きでワイルドカードを使用できます。レジストリのパス内では、特定のキーの代わりに *(アスタリスク) 記号を使用できます。たとえば、`HKEY_USERS*\software can mean` `HKEY_USER\default\softwareHKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\default\software`とは一致しません。 `HKEY_LOCAL_MACHINE\system\ControlSet*`は、有効なレジストリキーパスではありません。|*のあったレジストリキーのパスは、「このパスまたはこの記号の後の任意のレベルの任意のパス」を意味します。ファイルターゲットに対してワイルドカードを使用する方法はこの方法だけです。最初に、パスの特定の部分が評価された後、ワイルドカード記号(*)に続くパスが評価されます。

警告

明らかな汎用ルールを作成する場合は、通知を受信することがあります。

HIPS詳細設定

次のオプションは、アプリケーションの動作をデバッグおよび分析するときに役立ちます。

使用するデバイスドライバ

ユーザールールで明示的にブロックされないかぎり、設定されたフィルタリングモードに関係なく、選択したドライバは常にロードされます。明示的にユーザールールでブロックされている場合を除き、このリストに表示されるドライバは、HIPSフィルタリングモードに関係なく、常にロードできます。新しいドライバーを追加したり、リストから選択したドライバーを編集または削除したりできます。

注意

手動で追加したドライバを含める場合は、[リセット]をクリックします。これは、複数のドライバを追加し、手動でリストから削除できない場合に有効です。

ブロックされた操作をすべて記録

ブロックされたすべての操作がHIPSログに書き込まれます。

スタートアップアプリケーションに変更があったとき通知する

アプリケーションがシステムスタートアップに追加、またはスタートアップから削除されるたびに、デスクトップ通知を表示します。

アップデートの設定

このセクションでは、使用されるアップデートサーバーやこれらのサーバーの認証データなどのアップデートソース情報を指定します。

注意

アップデートファイルを正しくダウンロードするには、全てのアップデートパラメータを正しく入力することが重要です。ファイアウォールを使用している場合は、ESETプログラムがインターネットとの通信(HTTP通信)を許可されていることを確認してください。

■ 基本

既定のアップデートプロファイルを選択

既定でアップデートに適用される既存のポリシーを選択するか、新しいプロファイルを作成します。

アップデートキャッシュを削除

更新時に問題が発生した場合、[クリア]をクリックすると一時アップデートキャッシュが削除されます。

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)

検出エンジンが範囲外として報告されるまでの最大日数を設定できます。既定値は7です。

モジュールロールバック

検出エンジン/プログラムモジュールの新規アップデートが不安定であったり破損している疑いのある場合、前のバージョンにロールバックし、設定した期間中のアップデートを無効にできます。あるいは、無期限に延期した場合、前に無効にしたアップデートを有効にすることもできます。ESET Server Securityは、[アップデートロールバック](#)機能を使用するため、検出エンジンとプログラムモジュールのスナップショットを記録します。検出エンジンのスナップショットを作成するには、[モジュールのスナップショットを作成する]を有効にしておきます。

ローカルに保存するスナップショットの数

前に保存されたモジュールスナップショット数を定義します。

■ [プロファイル](#)

カスタムアップデートプロファイルを作成するには、[プロファイルのリスト]の横の[編集]を選択し、[プロファイル名]を入力して、[追加]をクリックします。編集するプロファイルを選択し、モジュールアップデートタイプのパラメーターを修正するか、アップデートミラーを作成します。

■ [更新](#)

ドロップダウンメニューからアップデートタイプを選択します。

- **[通常アップデート]** – 既定では、[アップデートの種類]が[定期アップデート]に設定され、最低限のネットワークトラフィックでアップデートファイルがESETサーバーから自動的にダウンロードされます。
- **[リリース前アップデート]** – リリース前アップデートは社内テスト済みで、まもなく一般に公開される予定のものです。テストモードを有効にすることで、最新の保護機能や修正プログラムを利用することができます。ただし、テストモードは常に安定しているとは限りません。最大限の可用性と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。
- **遅延アップデート** – 12時間以上の遅延のある最新バージョンのウイルスデータベース(つまり、実際の環境でテスト済みであって、そのため安定しているとみなされるデータベース)を提供する特別なサーバーからアップデートできます。

アップデートをダウンロードする前に確認する

新しいアップデートが利用可能になると、ダウンロード前に確認が表示されます。

アップデートファイルが次のサイズ(KB)よりも大きい場合に確認する

アップデートファイルのサイズがフィールドで指定した値より大きい場合、通知が表示されます。

成功したアップデートについての通知を無効にする

画面の右下にあるシステムトレイ通知が無効になります。全画面のアプリケーションが実行されている場合、このオプションを選択すると便利です。プレゼンテーションモードではすべての通知が

オフになることに注意してください。

モジュールアップデート

モジュールアップデートには、既定では**[自動選択]**が設定されています。アップデートサーバーは、アップデートファイルが保存される場所です。ESETサーバーを使用するときには、既定のオプションを選択することをお勧めします。

ローカルのHTTPサーバー、つまりミラーを使用する場合は、アップデートサーバーを
`http://computer_name_or_its_IP_address:2221`

SSLを使用するローカルのHTTPサーバーを使用する場合は、アップデートサーバーを
`https://computer_name_or_its_IP_address:2221`

ローカル共有フォルダを使用する場合は、アップデートサーバーを次のように設定してください。
`\\computer_name_or_its_IP_address\shared_folder`

検出シグネチャの高頻度なアップデートを有効にする

検出エンジンはより短い間隔でアップデートされます。この設定を無効にすると、検出率に悪影響を及ぼす可能性があります。

リムーバブルメディアからのモジュールアップデートを許可する

作成されたミラーが含まれる場合は、リムーバブルメディアからアップデートできます。**[自動]**が選択されている場合、アップデートはバックグラウンドで実行されます。アップデートダイアログを表示する場合は、**[常に確認する]**を選択します。

プログラムコンポーネントのアップデート

アップデートモードドロップダウンメニューを使用して、新しいアップデートが利用可能なときにESET Server Securityプログラムコンポーネントのアップデート(PCU)およびマイクロプログラムコンポーネントのアップデート(μPCU)の適用方法を選択します。コンポーネントアップデートは、通常、既存の機能を修正しますが、新しい機能や修正が含まれる場合もあります。選択したアップデートモードによっては、介入や確認なしで、コンポーネントアップデートを自動的に実行できます(再起動が必要な場合は確認が表示されます)。あるいは、アップデートがインストールされる前に通知を送信するように選択できます。

注意

一部の場合では、コンポーネントアップデート後に、サーバーの再起動が必要な場合があります。

使用可能なアップデートモードは次のとおりです。

- **アップデートする前に確認する** – 製品アップデートが利用可能になったとき、確認または拒否を確認するメッセージが表示されます。これは既定のオプションです。コンポーネントアップデート後に、サーバーの再起動が必要な場合があります。
- **自動アップデート** – コンポーネントアップデートが自動的にダウンロードおよびインストールされます。サーバーの再起動が必要な場合があります。
- **アップデートしない** – コンポーネントアップデートはまったく実行されません。手動でコンポーネントアップデートを実行でき、スケジュールされたメンテナンス期間にサーバーを再起動できます。

重要

自動アップデートモードは、コンポーネントアップデートが完了した後に、サーバーを自動的に再起動します。

☐ 接続オプション

プロキシサーバ

特定のアップデートプロファイルのプロキシサーバ設定オプションにアクセスするには。[プロキシモード]タブをクリックし、次の3つのオプションのいずれかを選択します。

- **プロキシサーバを使用しない** - アップデートの実行時に、ESET Server Securityによってプロキシサーバが使用されません。
- **グローバルプロキシサーバ設定を使用する** - [詳細設定](F5) > [ツール] > [プロキシサーバ]で指定されたプロキシサーバ設定を使用します。
- **プロキシサーバを使用して接続する** - 次の場合に、このオプションを使用します。

グローバル設定([ツール] > [プロキシサーバ])で指定したものと異なるプロキシサーバを使用してESET Server Securityをアップデートする場合。この場合は、ここで設定を指定する必要があります。必要に応じて、プロキシサーバの[プロキシサーバ]アドレス、通信[ポート] (既定は3128)、および[ユーザー名]と[パスワード]を指定します。

プロキシサーバ設定はグローバルには設定されませんがESET Server Securityはアップデートを取得するためにプロキシサーバに接続する場合。

コンピュータがプロキシサーバを介してインターネットに接続される場合。設定はプログラムのインストール時にInternet Explorerから取得されますが、その後変更されている(ISPを変更するなど)場合、このウィンドウに表示されているHTTPプロキシ設定が正しいことを確認します。しなかった場合、プログラムはアップデートサーバに接続できません。

注意

[ユーザー名]と[パスワード]などの認証データは、プロキシサーバへのアクセスに使用されます。これらのフィールドには、ユーザー名とパスワードが必要な場合にのみ入力してください。これらのフィールドは、ESET Server Securityのユーザー名とパスワードを入力するためのものではありません。プロキシサーバ経由でインターネットにアクセスするためにパスワードが必要であることがわかっている場合にのみ入力してください。

プロキシが使用できない場合は直接接続を使用する

製品がHTTPプロキシを使用するように構成され、プロキシに接続できない場合は、プロキシをバイパスし、直接ESETサーバと通信します。

Windows共有

Windowsを実行しているローカルサーバからタイプドロップダウンメニューから次のオプションのいずれかを選択します。

アップデートサーバ接続アカウントの設定

アカウントを設定するには、次のオプションのいずれかを選択します。

- **システムアカウント(既定)** - システムアカウントを認証に使用します。一般に、アップデートの設定のメインセクションで認証データが指定されていない場合、認証プロセスは実行されません。
- **現在のユーザー** - このオプションを選択すると、現在ログインしているユーザーアカウントを使用して認証が行われるようになります。この方法の欠点は、ログインしているユーザーがいない場合、プログラムがアップデートサーバに接続できない点です。

- **指定されたユーザー** – このオプションを選択すると、認証用の特定のユーザーアカウントを使用します。この方法は、既定のシステムアカウント接続に失敗した場合に使用してください。指定されたユーザーのアカウントは、ローカルサーバ上のアップデートファイルディレクトリにアクセスできなければなりません。アクセスできない場合は、接続を確立して、アップデートファイルをダウンロードすることができません。

警告

[現在のユーザー]または[指定されたユーザー]オプションが有効になっている場合、プログラムのIDを目的のユーザーに変更すると、エラーが発生することがあります。そのため、アップデートの設定のメインセクションでLANの認証データを入力することをお勧めします。このアップデート設定セクションでは、認証データは次のように入力する必要があります。**domain_name\user**（これがワークグループの場合は**workgroup_name\name**と入力します）およびパスワード。ローカルサーバのHTTPミラーからアップデートする場合、認証は不要です。

アップデート後にサーバから切断

アップデートファイルのダウンロード後もサーバとの接続がアクティブなままになる場合は、強制的に切断します。

☐ [ミラーでの更新](#)

ローカルミラーサーバの設定オプションは、[アップデート] > [プロファイル] > [アップデートミラー]タブの下の[\[詳細設定\]](#)(F5)にあります。

アップデートのロールバック

[ロールバック]をクリックする場合、検出エンジンデータベースおよびプログラムモジュールアップデートを一時停止する期間を指定する時間間隔をドロップダウンメニューから選択する必要があります。

アップデート機能を手動で復元するまで、定期アップデートを無期限に延期するには、[取り消しまで]を選択します。これには潜在的なセキュリティリスクがあるため、このオプションの選択はお勧めしません。

検出エンジンデータベースのバージョンは最も古いものにダウングレードされて、ローカルのコンピューターファイルシステムにスナップショットとして保存されます。

スケジュールタスク – アップデート

2つのアップデートサーバからプログラムをアップデートする場合、2つの異なるアップデート用プロファイルを作成する必要があります。最初のサーバでアップデートファイルのダウンロードに失敗すると、自動的に次のサーバに切り替えられます。これは、通常はローカルLANのアップデートサーバからアップデートを行っているが、別のネットワークからインターネットに接続すること多いノートパソコンなどに最適です。その場合、最初のプロファイルが失敗すると、次のプロファイルが自動的にESETのアップデートサーバからアップデートファイルをダウンロードします。

例

以下の手順は、既存の**定期自動アップデート**を編集するためのタスクを説明します。

1. メインの**スケジューラ**画面で、名前が**定期自動アップデート**の**アップデート**タスクを選択し、**編集**をクリックすると、設定ウィザードが開きます。
2. 実行するスケジューラタスクを設定し、次の**タイミングオプション**のいずれかを選択して、スケジュールされたタスクを実行するタイミングを定義します。
3. システムがバッテリー(UPSなど)で実行中のときにタスクが実行されないようにする場合は、**バッテリー電源で実行中のときにタスクをスキップする**の横のスイッチをクリックします。
4. アップデートで使用する**アップデートプロファイル**を選択します。スケジュールされたタスクを何らかの理由で実行できなかった場合に実行する**アクション**を選択します。
5. **[完了]**をクリックすると、タスクが適用されます。

ミラーでの更新

ESET Server Securityを開く

F5>アップデート > プロファイル > アップデートミラーをクリックします



ESET Server Securityでは、ネットワーク内の他のワークステーションをアップデートするために使用できるアップデートファイルのコピーを作成することができます。「ミラーサーバーの作成」の使用 - LAN環境でアップデートファイルのコピーを作成すると、ベンダのアップデートサーバーからワークステーションごとに繰り返しアップデートファイルをダウンロードしなくて済むので便利です。アップデートがローカルのミラーサーバーにダウンロードされ、すべてのワークステーションに配信されるため、ネットワークトラフィックが過負荷状態になる危険性を回避することができます。ミラーからクライアントワークステーションをアップデートすると、ネットワークの負荷分散が最適化されると共に、インターネット接続の帯域幅が節約されます。

☐ ミラーでの更新

アップデートミラーの作成

ミラー設定オプションを有効にします。

ストレージフォルダー

ミラーリングされたファイル `C:\ProgramData\ESET\ESET Security\mirror` を保存するために定義済みの既定のフォルダーを変更する場合は、[クリア]をクリックします。[編集]をクリックすると、ローカルコンピューターまたは共有ネットワークフォルダーのフォルダーを参照します。指定したフォルダーの認証が必要な場合は、[ユーザー名]フィールドと[パスワード]フィールドで認証データを指定する必要があります。選択した保存先フォルダーが、Windows NT/2000/XPオペレーティングシステムを実行するネットワークディスクにある場合、選択したフォルダーに対する書き込み権限があるユーザー名とパスワードを指定する必要があります。

ユーザー名は、*Domain/User*または*Workgroup/User*という形式で入力する必要があります。対応するパスワードを必ず指定してください。

プログラムコンポーネントのアップデート

ファイル

ミラーを構成するときには、ダウンロードするアップデートの言語バージョンを指定できます。選択した言語は、ユーザーが構成したミラーサーバーによってサポートされている必要があります。

自動的にコンポーネントをアップデート

新しい機能のインストールと、既存の機能の更新ができます。ユーザーが操作を行わずに自動的にアップデートが実行されるようにすることも、アップデートするかどうかをユーザーが決定できるようにすることもできます。製品のアップデートファイルをインストールした後、コンピュータの再起動が必要になることがあります。

今すぐコンポーネントをアップデート

プログラムコンポーネントを最新バージョンにアップデートします。

☐ [HTTPサーバー](#)

サーバーポート

既定のポートは2221に設定されています。別のポートを使用している場合は、この値を変更します。

認証

アップデートファイルにアクセスするために使用される認証方法を定義します。使用可能なオプションは次のとおりです。[なし]☑[基本]☑[NTLM]☑

- **基本**のユーザー名およびパスワード認証でbase64エンコードを使用する場合は、[基本]を選択してください。
- [NTLM]オプションを選択すると、安全なエンコード方法でエンコードされます。認証については、アップデートファイルを共有するワークステーション上で作成されたユーザーが使用されます。
- 既定の設定は[なし]で、認証なしでアップデートファイルにアクセスすることができます。

警告

HTTPサーバー経由によるアップデートファイルへのアクセスを許可する場合、ミラーフォルダーは、ミラーフォルダーを作成するESET Server Securityのインスタンスと同じコンピューターに置かれている必要があります。

HTTPサーバーのSSL

HTTPS(SSL)サポートを使ったHTTPサーバーを実行する場合、**証明書チェーンファイル**を追加するか、自己署名証明書を生成します。以下の証明書タイプを使用できます☑PEM☑PFX☑およびASN☑セキュリティの強化のため☑HTTPSプロトコルを使用してアップデートファイルをダウンロードできます。このプロトコルを使用してデータ転送やログイン資格情報を追跡するのはほぼ不可能です。

秘密鍵タイプは、既定で**統合**に設定されています。このため、秘密鍵ファイルオプションは既定で無効です。つまり、秘密鍵は選択した証明書チェーンファイルの一部です。

☐ [接続オプション](#)

Windows共有

Windowsを実行しているローカルサーバーからタイプドロップダウンメニューから次のオプションのいずれかを選択します。

アップデートサーバー接続アカウントの設定

アカウントを設定するには、次のオプションのいずれかを選択します。

- **システムアカウント(既定)** – システムアカウントを認証に使用します。一般に、アップデート

の設定のメインセクションで認証データが指定されていない場合、認証プロセスは実行されません。

- **現在のユーザー** – これを選択すると、現在ログインしているユーザーアカウントを使用して認証が行われるようにします。この方法の欠点は、ログインしているユーザーがいない場合、プログラムがアップデートサーバーに接続できない点です。
- **指定されたユーザー** – これを選択すると、認証用の特定のユーザーアカウントを使用します。この方法は、既定のシステムアカウント接続に失敗した場合に使用してください。指定されたユーザーのアカウントは、ローカルサーバ上のアップデートファイルディレクトリにアクセスできなければなりません。アクセスできない場合は、接続を確立して、アップデートファイルをダウンロードすることができません。

警告

[現在のユーザー]または[指定されたユーザー]オプションが有効になっている場合、プログラムのIDを目的のユーザーに変更すると、エラーが発生することがあります。そのため、アップデートの設定のメインセクションでLANの認証データを入力することをお勧めします。このアップデート設定セクションでは、認証データは次のように入力する必要があります。`domain_name\user`（これがワークグループの場合は `workgroup_name\name` と入力します）およびパスワード。ローカルサーバーのHTTPミラーからアップデートする場合、認証は不要です。

アップデート後にサーバーから切断

アップデートファイルのダウンロード後もサーバーとの接続がアクティブなままになる場合は、強制的に切断します。

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

信頼できるゾーンからのコンピューターで実行中のサービスの一部へのアクセスを設定し、コンピューターに害をもたらす可能性があるさまざまな攻撃およびエクスプロイトの検出を有効/無効にできます。

ボットネット保護を有効にする

コンピューターが感染し、ボットが通信を試みているときに、一般的なパターンに基づいて、悪意のあるコマンドとコントロールサーバーとの通信を検出してブロックします。

IDSの例外

侵入検出システム(IDS)例外は、ネットワーク保護ルールと考えることができます。[編集](#)をクリックするとIDS例外を定義します。

注意

高速ネットワーク(10GbE以上)を実行している環境の場合は、[ネットワーク速度のパフォーマンス](#)とESET Server Securityの詳細についてKB記事をお読みください。

総当たり攻撃保護

ESET Server Security ネットワークトラフィックの内容を検査し、パスワード推測攻撃の試みをブロックします。

詳細設定オプション

高度なフィルタリングオプションを設定して、コンピューターに対して実行できるさまざまな種類の攻撃や脆弱性を検出します。

侵入検出:

プロトコルSMB - SMBプロトコルでさまざまなセキュリティの問題を検出してブロックします。

プロトコルRPC - 分散コンピューティング環境(DCE)向けに開発されたリモートプロシージャコールシステムで、さまざまなCVEを検出してブロックします。

プロトコルRDP - RDPプロトコルでさまざまなCVEを検出してブロックします(上記を参照)。

攻撃の検出後に安全ではないアドレスをブロック - 攻撃のソースとして検出されたIPアドレスはブラックリストに追加され、特定の期間の間接続が遮断されます。

攻撃の検出後に通知を表示 - 画面の右下端のシステムトレイ通知をオンにします。

セキュリティホールに対する受信攻撃の通知も表示 - セキュリティホールに対する攻撃が検出された場合、またはこの方法でシステムに侵入する試みが脅威によって実行された場合に、通知します。

パケットのチェック:

SMBプロトコルでの管理共有への受信接続を許可 - 管理共有は既定のネットワーク共有で、システムのハードドライブパーティション(C\$, D\$, ...)をシステムフォルダ(ADMIN\$)と共有します。管理共有への接続を無効にすると、多数のセキュリティリスクを緩和します。たとえばConfickerワームは、管理共有に接続するためにディクショナリ攻撃を実行します。

古い(サポート対象外) SMBダイアレクトを拒否 - IDSでサポートされていない古いSMBダイアレクトを使用するSMBセッションを拒否します。最新のWindowsオペレーティングシステムは、Windows 95などの古いオペレーティングシステムとの後方互換性のために、古いSMBダイアレクトをサポートします。攻撃者は、トラフィック検査を回避するためにSMBセッションで古いダイアレクトを使用することがあります。コンピューターが古いバージョンのWindowsがインストールされたコンピューターとファイルを共有(または一般的にSMB通信を使用)する必要がない場合は、古いSMBダイアレクトを拒否します。

セキュリティ拡張のないSMBセッションを拒否 - 拡張セキュリティは、LAN Manager Challenge/Response (LM)認証よりも安全な認証メカニズムを提供するためにSMBセッションネゴシエーション中に使用できます。LMスキームは脆弱であると考えられ、使用することは推奨されません。

セキュリティアカウントマネージャーサービスとの通信を許可 - このサービスの詳細については、[\[MS-SAMR\]](#)を参照してください。

ローカルセキュリティ機関サービスとの通信を許可 - このサービスの詳細については、[\[MS-LSAD\]](#)および[\[MS-LSAT\]](#)を参照してください。

リモートレジストリサービスとの通信を許可 - このサービスの詳細については、[\[MS-RRP\]](#)を参照してください。

サービスコントロールマネージャーサービスとの通信を許可 - このサービスの詳細については、[\[MS-SCMR\]](#)を参照してください。

サーバーサービスとの通信を許可 - このサービスの詳細については、[\[MS-SRVS\]](#)を参照してください。

他のサービスとの通信を許可 - 他のMSRPCサービス

IDSの例外

侵入検出システム(IDS)例外は基本的にネットワーク保護ルールです。例外は上から下に評価されます。IDS例外エディターでは、さまざまなIDS例外のネットワーク保護動作をカスタマイズできます。各アクションタイプ(ブロック、通知、ログ)の最初に一致する例外が個別に適用されます。**Top/Up/Down/Bottom**では、例外の優先度レベルを調整できます。新しいIDS例外を作成するには、**追加**をクリックします。**編集**をクリックすると、既存のIDS例外を修正できます。**削除**をクリックすると、削除できます。

ドロップダウンメニューから**アラートタイプ**を選択します。**脅威名**と**方向**を指定します。例外を作成する**アプリケーション**を参照します。IPアドレス(IPv4またはIPv6)またはサブネットのリストを指定します。複数のエントリでは、カンマを区切り文字として使用します。

ドロップダウンメニュー(**既定**はいいいえ)からオプションのいずれかを選択してIDS例外の**アクション**を設定します。各アクションタイプ(**ブロック**、**通知**、**ログ**)でこの手順を実行します。

例

IDS例外アラートの場合に通知を表示し、イベントの時刻を記録する場合は、**ブロック**アクションタイプを**既定**にします。他の2つのアクションタイプ(**通知**および**ログ**)については、ドロップダウンメニューでは**はい**を選択します。

一時IPアドレスブラックリスト

攻撃の元であると検出され、一定の時間、接続をブロックするためにブラックリストに追加されたIPアドレスの一覧を表示します。ロックされた**IPアドレス**を表示します。

ブロック理由

アドレスから遮断される攻撃のタイプを示します(TCPポートスキャン攻撃など)。

タイムアウト

アドレスがブラックリストで期限切れになる日時を示します。

削除/すべて削除

期限切れになる前に一時ブラックリストから選択したIPアドレスを削除するか、すべてのアドレスをすぐにブラックリストから削除します。

例外の追加

選択したIPアドレスのファイアウォール除外をIDSフィルタリングに追加します。

Webとメール

プロトコルフィルタリング、電子メールクライアント保護、Webアクセス保護、フィッシング対策を設定し、インターネット通信中にサーバーを保護します。

[電子メールクライアント保護](#)

全てのメール通信の制御、悪意のあるコードからの保護、感染検出時のアクションの選択を行います。

Webアクセス保護

HTTPとHTTPSのルールに準拠してWebブラウザとリモートサーバ間の通信を監視します。この機能からは、特定の[URLアドレス](#)のブロック、許可、除外も可能になります。

プロトコルフィルタリング

アプリケーションプロトコルをより詳細に保護するためにThreatSenseスキャンエンジンによって提供されますWebブラウザまたはメールクライアントのいずれかが使用されると、この制御は自動的に実行されます。暗号化([SSL/TLS](#))通信にも機能します。

フィッシング対策保護

フィッシングコンテンツを配信していることが確認されているWebページをブロックできます。

プロトコルフィルタリング

ThreatSenseの検査エンジンには、アプリケーションプロトコルに対するマルウェア対策保護があり、ここでは複数の高度なマルウェアスキャン技術が統合されています。プロトコルフィルタリングは、使用しているインターネットブラウザや電子メールクライアントに関係なく、自動的に動作します。プロトコルフィルタリングが有効な場合ESET Server SecurityはSSL/TLSプロトコルを使用する通信を確認します。**Webとメール** > [SSL/TLS](#)に移動します。

アプリケーションプロトコルフィルタリングを有効にする

プロトコルフィルタリングを無効にすると、ほとんどのESET Server Securityコンポーネント(**Webアクセス保護**、**電子メールプロトコル保護**、**フィッシング対策**)はこれを利用しており、一部の機能が動作しません。

対象外のアプリケーション

特定のネットワーク対応アプリケーションによる通信をコンテンツフィルタリングの対象から除外するには、リストでそのアプリケーションを選択します。選択したアプリケーションのHTTP通信、POP3通信に対してはウイルス検査が行われません。特定のアプリケーションをプロトコルフィルタリングから除外することができます。**編集**と**追加**をクリックして、アプリケーションのリストから実行ファイルを選択し、プロトコルフィルタリングから除外します。

重要

通信を検査すると正常に機能しないアプリケーションに限って、このオプションを使用することをお勧めします。

対象外のIPアドレス

特定のリモートアドレスをプロトコルフィルタリングから除外できます。このリストのIPアドレスはプロトコルコンテンツフィルタリングから除外されます。選択したアドレスに対する送受信のHTTP/POP3/IMAP通信のマルウェアは検査されません。

重要

このオプションは信頼できるとわかっているアドレスに対してのみ使用することをお勧めします。

編集および**追加**をクリックして、除外が適用されるIPアドレス、アドレス範囲、サブネットを指定します。**[複数の値を入力]**を選択すると、改行、カンマ、セミコロンで区切られた複数のIPアドレスを追加できます。複数のセミコロンが有効な場合、アドレスが除外されたIPアドレスリストに表示されます。

注意

例外は、プロトコルフィルタリングで互換性の問題があるときに有効です。

Webと電子メールのクライアント

悪意のある多数のコードがインターネットを通じて広まっているので、コンピュータを保護するには、安全にインターネットを参照できることが非常に重要です。悪意のあるコードは、Webブラウザの脆弱性や不正なリンクを利用して、気付かれずにシステムに侵入します。そのためESET Server SecurityではWebブラウザのセキュリティに重点が置かれています。ネットワークにアクセスする各アプリケーションをインターネットブラウザとして指定することができます。選択したパスから通信またはアプリケーションで既にプロトコルを使用しているアプリケーションを、Webとメールクライアントのリストに追加できます。

SSL/TLS

ESET Server SecurityはSSL/TLSプロトコルを使用する通信で脅威を検査できます。

SSLで保護された通信には、信頼できる証明書、不明な証明書SSLで保護された通信の検査対象から除外された証明書を使用する、さまざまな検査モードがあります。

SSL/TLSプロトコルフィルタリングを有効にする

プロトコルフィルタリングが無効な場合SSL/TLS経由の通信は検査されませんSecure Sockets Layer (SSL) / Transport Layer Security (TLS)プロトコルフィルタリングモードは、次のオプションで使用できます。

- **自動モード** – 検査対象から除外された証明書に保護されている通信以外のSSL/TLSで保護された全通信を検査するには、このオプションを選択します。不明な署名付き証明書を使用した新しい通信が確立された場合、ユーザに通知されず、通信は自動的にフィルタリングされます。信頼しているとマークされている(信頼できる証明書に追加済み)信頼されない証明書を使用してサーバーにアクセスすると、そのサーバーへの通信は許可され、通信チャネルのコンテンツがフィルタリングされます。
- **対話モード** – 新しいSSL/TLSで保護されたサイト(不明な証明書を使用)にアクセスする場合、アクション選択ダイアログが表示されます。このモードでは、検査から除外するSSL/TLS証明書のリストを作成できます。
- **ポリシーモード** – では、構成された例外を除き、すべてのSSL/TLS接続がフィルタリングされます。

SSL/TLSフィルタリングされたアプリケーションのリスト

フィルタリングアプリケーションと検査アクションのいずれかを設定しますSSL/TLSでフィルタリングされたアプリケーションのリストを使用すると、特定のアプリケーションに対するESET Server Security動作をカスタマイズし、対話モードがSSL/TLSプロトコルフィルタリングモードで選択された

場合に選択されたアクションを記憶できます。

既知の証明書のリスト

特定のSSL証明書に対するESET Server Security動作をカスタマイズできます。このリストを表示および管理するには、**既知の証明書のリスト**の横の[編集](#)をクリックします。

信頼できるドメインとの通信を除外

拡張検証証明書を使用する通信をプロトコルチェックから除外します(インターネットバンキング)。

古いプロトコルSSL v2を使用した暗号化通信をブロックする

SSLプロトコルの従来のバージョンを使用した通信は、自動的にブロックされます。

ルート証明書

ブラウザや電子メールクライアントでSSL/TLS通信を正しく機能させるにはESETのルート証明書を既知のルート証明書(発行元)のリストに追加する必要があります。[ルート証明書を既知のブラウザに追加する]を有効にする必要があります。このオプションを選択するとESETルート証明書が既知のブラウザ(Opera、Firefoxなど)に自動的に追加されます。システム証明書の保存先を使用するブラウザに、証明書が自動的に追加されます(Internet Explorerなど)。

サポートされないブラウザに証明書を適用するには、[証明書の表示]>[詳細]>[ファイルにコピー...]をクリックして、証明書をブラウザに手動でインポートします。

証明書の有効性

信頼できるルート認証局ストアを使用して証明書を検証できない場合

場合によっては、**Trusted Root Certification Authorities (TRCA)**ストアを使用してWebサイト証明書を検証できないことがあります。これは、証明書が他のユーザー(Webサーバーまたは中小企業の管理者)によって自己署名されていて、この証明書を信頼できるとみなしても必ずしもリスクにはならないことを意味します。多くの大企業(銀行など)はTRCAによって署名されている証明書を使用します。[証明書の有効性を確認する](既定で選択)が選択されていると、ユーザーは暗号化通信の確立時に取るアクションを選択するよう求められます。[証明書を使用する通信をブロックする]を選択すると、未検証の証明書を使用したサイトへの暗号化接続を常に終了できます。

証明書が無効または破損している場合

その証明書は期限切れであるか、あるいは不正に自己署名されていることを意味します。この場合は、この証明書を使用する通信をブロックすることをお勧めします。

既知の証明書のリスト

特定のSockets Layer (SSL) / Transport Layer Security (TLS)証明書のESET Server Security動作をカスタマイズし、**対話モード**がSSL/TLSプロトコルフィルタリングモードで選択されている場合に選択したアクションを記憶します。選択した証明書を設定するかURLまたはファイルから証明書を追加できます。[証明書の追加]ウィンドウで、[URL]または[ファイル]をクリックし、証明書URLを指定するか、証明書ファイルを参照します。証明書のデータを使用して自動的に入力されるフィールド:

- **証明書名** – 証明書の名前。
- **証明書の発行者** – 証明書の作成者名。
- **証明書の件名** – 件名フィールドは、件名パブリックキーフィールドに保存されたパブリックキー

に関連付けられたエンティティを指定します。

アクセスアクション

- **自動** – 信頼できる証明書を許可し、信頼できない証明書を確認します。
- **許可またはブロック** – 信頼性に関係なく、この証明書で保護された通信を許可またはブロックします。
- **確認** – 特定の証明書が見つかったときに確認メッセージが表示されます。

検査アクション

- **自動** – 自動モードで検査し、対話モードで確認します。
- **検査または無視** – この証明書で保護された通信を検査または無視します。
- **確認** – 特定の証明書が見つかったときに確認メッセージが表示されます。

暗号化されたSSL通信

SSLプロトコル検査をしようするようにシステムが構成されている場合、次の2つの状況でアクションを選択するように指示するダイアログが表示されます。

まずWebサイトが検証不可能または無効な証明書を使用し、このような場合にESET Server Securityがユーザーに確認するように設定されている(検証不可能な証明書の既定は[はい]、無効な証明書の既定は[いいえ])場合、接続を**許可**するか**拒否**するかを確認するダイアログボックスが表示されます。

次に、**SSLプロトコルフィルタリングモード**が**対話モード**に設定されている場合、各Webサイトのダイアログボックスが表示され、トラフィックを**検査**するか**無視**するかどうかを確認します。一部のアプリケーションは、SSLトラフィックが誰かによって修正または検査されていないことを確認します。このような場合ESET Server Securityはトラフィックを**無視**し、アプリケーションを動作させ続ける必要があります。



Encrypted network traffic

Trusted certificate

An application on this computer is trying to communicate over encrypted channel.

Application: Internet Explorer (2568)

Company: Querying

Reputation: Discovered 5 years ago

Certificate: *.google.com

Scan this communication?

Scan

Ignore

☐ Remember action for this certificate

いずれの場合も、ユーザーは選択したアクションを記憶するように選択できます。保存されたアクションは[\[既知の証明書のリスト\]](#)に保存されます。

電子メールクライアント保護

ESET Server Securityをメールクライアントと統合すると、メールメッセージにおいて悪意のあるコードから積極的に保護するレベルが向上します。メールクライアントがサポートされている場合、統合をESET Server Securityで有効にできます。統合が有効な場合ESET Server Securityツールバーが直接電子メールクライアントに挿入され(新しいバージョンのWindows Live Mailのツールバーは挿入されません)、より効率的な電子メール保護が可能です。

電子メールクライアント統合

現在、メールクライアントとしてMicrosoft Outlook®Outlook Express®Windows Mail®Windows Live Mailがサポートされています。メールの保護は、これらのプログラムのプラグインとして機能します。プラグインの主な利点は、使用されるプロトコルに依存しない点です。暗号化されたメールをメールクライアントが受信した場合、メールは解読されてウイルススキャナーに送信されます。統合が有効になっていない場合でも、電子メールクライアント保護モジュール(POP3®IMAP)によってメール通信は保護されます。サポートされている電子メールクライアントとそのバージョンの総合リストは、[ナレッジベース](#)を参照してください。

受信ボックス内の変更時にチェックを無効にする

メールクライアントでの作業時にシステムの速度が低下する場合は、[受信ボックス内の変更時にチェックを無効にする]オプションを選択します(MS Outlookのみ)®Kerio Outlook Connector Storeからメールを取得するときなどに、この状況が発生する場合があります。

クライアントプラグインによって電子メール保護を有効にする

電子メールクライアントとの統合を削除せずに、電子メールクライアント保護を無効にできます。すべてのプラグインを一度に無効にするか、次のように選択して無効にできます。

- **受信メール** – 受信メールを検査対象にする。
- **送信メール** – 送信メールを検査対象にする。
- **既読メール** – 既読メールを検査対象にする。

感染メールに対して実行するアクション

- **何もしない** – これを有効にすると、感染している添付ファイルは特定されますが、メールに対してはいずれのアクションも実行されずそのまま残ります。
- **メールを削除する** – 侵入がユーザーに通知され、メールは削除されます。
- **メールを削除済みフォルダに移動する** – 感染しているメールを自動的に[削除済み]フォルダに移動します。
- **メールをフォルダに移動する** – 感染しているメールを自動的に指定したフォルダに移動します。
- **フォルダ** – 検出に感染した電子メールを移動するカスタムフォルダを指定します。

アップデート後に再度検査を行う

検出エンジンアップデート後の再検査を切り替えます。

ほかの機能の検査結果を受け入れる

選択すると、メールの保護機能でほかの保護機能の検査結果が受け入れられます(POP3とIMAPプロトコル検査)。

電子メールプロトコル

プロトコルフィルタリングによって電子メール保護を有効にする

IMAPとPOP3プロトコルは、電子メールクライアントアプリケーションでのメールの受信に最もよく使用されているプロトコルです。ESET Server Securityでは、使用される電子メールクライアントに関係なく、このプロトコルに対する保護機能を備えています。

ESET Server SecurityではIMAPSおよびPOP3Sプロトコルの検査もサポートします。この場合、暗号化チャネルを使用して、サーバーとクライアント間で情報を送受信します。ESET Server Securityは、SSL (Secure Socket Layer)およびTLS (Transport Layer Security)プロトコルを使用して通信を検査します。このプログラムは、オペレーティングシステムのバージョンに関係なく、**IMAPS/POP3Sプロトコル**で使用されるポートで定義されたポート上のトラフィックだけを検査します。

IMAPS/POP3Sスキャナの設定

既定の設定が使用中のときには、暗号化された通信は検査されません。暗号化された通信の検査を有効にするには、[SSL/TLSプロトコル確認](#)に移動します。

ポート番号はポートの種類を識別します。既定の電子メールポートは以下のとおりです。

ポート名	ポート番号	説明
POP3	110	既定のPOP3非暗号化ポート。
IMAP	143	既定のIMAP非暗号化ポート。

ポート名	ポート番号	説明
セキュアIMAP (IMAP4-SSL)	585	SSL/TLSプロトコルフィルタリングを有効にします。複数のポート番号は、コンマで区切る必要があります。
IMAP4 over SSL (IMAPS)	993	SSL/TLSプロトコルフィルタリングを有効にします。複数のポート番号は、コンマで区切る必要があります。
セキュアPOP3 (SSL-POP)	995	SSL/TLSプロトコルフィルタリングを有効にします。複数のポート番号は、コンマで区切る必要があります。

警告と通知

電子メールクライアント保護では、POP3プロトコルおよびIMAPプロトコルで受信したメール通信が検査されます。ESET Server Securityは、Microsoft Outlook用のプラグインおよびその他のメールクライアントを使用して、メールクライアントからの全通信(POP3、IMAP、IMAP、HTTP)を検査します。受信メッセージを検査するときには、ThreatSenseスキャンエンジンに含まれている詳細なスキャン方法がすべて使用されます。そのため、ウイルス検出データベースと突き合わせて一致する前であっても、悪意のあるプログラムの検出が可能です。POP3プロトコルとIMAPプロトコルの通信のスキャンは、使用されるメールクライアントからは独立しています。

メールが検査された後、スキャン結果を記載した通知をメールに追加することができます。[受信メールと既読メールにタグメッセージを追加]、[受信した感染メールと既読の感染メールの件名に注釈を追加]、または[送信メールにタグメッセージを追加]を選択できます。まれに、問題のあるHTMLメッセージの場合やメッセージがマルウェアによって偽造された場合は、タグメッセージが存在しないことがあることに注意してください。タグメッセージは、受信/既読メールまたは送信メール(あるいはその両方)に追加することができます。使用可能なオプションは次のとおりです。

- **追加しない** – 検査通知は追加されません。
- **感染メールのみ** – 悪意のあるソフトウェアをもった検査通知のみに検査済みのマークが付けられます(既定)。
- **すべてのメール** – スキャンされた全てのメールに検査通知が追加されます。

送信した感染メールの件名にタグを追加

メールの保護で、感染しているメールの件名にウイルス警告を追加しない場合は無効にします。この機能は、感染しているメールを件名に基づいて単純にフィルタリングする場合に有効です(メールプログラムでサポートされている場合)。また、受信者の信頼を高めることができ、マルウェアが検出された場合、特定のメールまたは送信者のマルウェアについての貴重な情報を得ることができます。

感染メールの件名に追加する目印のテンプレート

感染した電子メールの件名のプレフィックス形式を変更する場合はこのテンプレートを編集します。この機能を実行すると、メッセージの件名Helloが、プレフィックス値[virus]([virus] Helloの形式)で置き換えられます。変数 %VIRUSNAME%は検出された脅威を表します。

MS Outlook ツールバー

Microsoft Outlookの保護機能はプラグインとして動作します。ESET Server Securityをインストールすると、マルウェア対策機能オプションを備えた次のツールバーが、Microsoft Outlookに追加されます。

ESET Server Security

アイコンをクリックするとESET Server Securityのメインプログラムウィンドウが開きます。

メッセージの再検査

電子メールのチェックを手動で開始できます。チェックするメッセージを指定して、受信メールの再検査を有効にできます。詳しくは、「[電子メールクライアントの保護](#)」を参照してください。

スキャナの設定

[\[電子メールクライアント保護\]](#)設定オプションを表示します。

Outlook ExpressおよびWindowsメールツールバー

Outlook ExpressおよびWindows Mailの保護機能は、プラグインモジュールとして動作しますESET Server Securityをインストールすると、マルウェア対策機能オプションを備えた次のツールバーが、Outlook ExpressまたはWindowsメールに追加されます。

ESET Server Security

アイコンをクリックするとESET Server Securityのメインプログラムウィンドウが開きます。

メッセージの再検査

電子メールのチェックを手動で開始できます。チェックするメッセージを指定して、受信メールの再検査を有効にできます。詳しくは、「[電子メールクライアントの保護](#)」を参照してください。

スキャナの設定

[\[電子メールクライアント保護\]](#)設定オプションを表示します。

表示のカスタマイズ

ツールバーの表示を、メールクライアントに合わせて変更できます。メールのプログラムパラメータに依存しないように表示をカスタマイズするには、オプションのチェックを外します。

- **テキストの表示** – アイコンの説明が表示されます。
- **右揃え** – オプションの説明がアイコンの下から右側へ移動します。
- **大きいアイコン** – メニューオプションの大きいアイコンを表示します。

確認ダイアログ

この通知は、選択したアクションの実行を確認する意味で表示されるので、誤った操作を防止する効果があります。ダイアログには、確認を無効にするオプションもあります。

メッセージの再検査

メールクライアントに組み込まれたESET Server Securityのツールバーでは、メール検査に関するオプションをいくつか指定できます。[\[メッセージの再検査\]](#)オプションでは次の2つのスキャンモードを選択できます。

- **現在のフォルダ内にあるすべてのメッセージ** – 現在表示されているフォルダ内にあるメッセージを検査します。

- **選択したメッセージのみ** – ユーザーがマークしたメッセージのみを検査します。
- **検査済みのメッセージも含む** – オンにすると、事前に検査されているメッセージを再度検査できます。

Webアクセス保護

Webアクセス保護は、Webブラウザとリモートサーバとの通信を監視することによって機能して、オンライン脅威から保護し、HTTP (Hypertext Transfer Protocol) およびHTTPS (暗号化通信) のルールに準拠します。

コンテンツをダウンロードする前に、悪意のあるコンテンツが含まれていることがわかっているWebページへのアクセスをブロックします。その他のすべてのWebページは、読み込み時にThreatSenseスキャンによって検査され、悪意のあるコンテンツの検出時にブロックされます。Webアクセス保護には、ブラックリストによるブロックとコンテンツによるブロックの2つのレベルがあります。

■ [基本](#)

Webアクセス保護を有効にすることを強くお勧めします。また、このオプションは、ESET Server Securityのメインプログラムウィンドウから、**[設定] > [Webとメール] > [Webアクセス保護]**に移動してアクセスできます。

ブラウザスクリプトの詳細検査を有効にする

既定ではWebブラウザによって実行されるすべてのJavaScriptプログラムが検出エンジンによってチェックされます。

■ [Webプロトコル](#)

ほとんどのインターネットブラウザで 사용되는これらの標準プロトコルの監視を構成できます。既定ではESET Server Securityは、大半のインターネットブラウザで 사용되는HTTPプロトコルを監視するように設定されています。

ESET Server SecurityはHTTPSプロトコルのチェックもサポートします。HTTPS通信では、暗号化チャンネルを使用して、サーバーとクライアント間で情報を送受信します。ESET Server Securityは、SSL (Secure Socket Layer) およびTLS (Transport Layer Security) プロトコルを使用した通信を検査します。このプログラムは、オペレーティングシステムのバージョンに関係なく、**HTTPSプロトコルで使用されるポート**で定義されたポート上のトラフィックだけを検査します。

既定の設定が使用されている場合は、暗号化された接続は検査されません。暗号化された通信の検査を有効にするには、**詳細設定 (F5) > Webとメール > [SSL/TLS](#)**を選択します。

[ThreatSense パラメータ](#)

検査対象の種類(電子メール、アーカイブなど)Webアクセス保護の検出方法などの設定を構成できます。

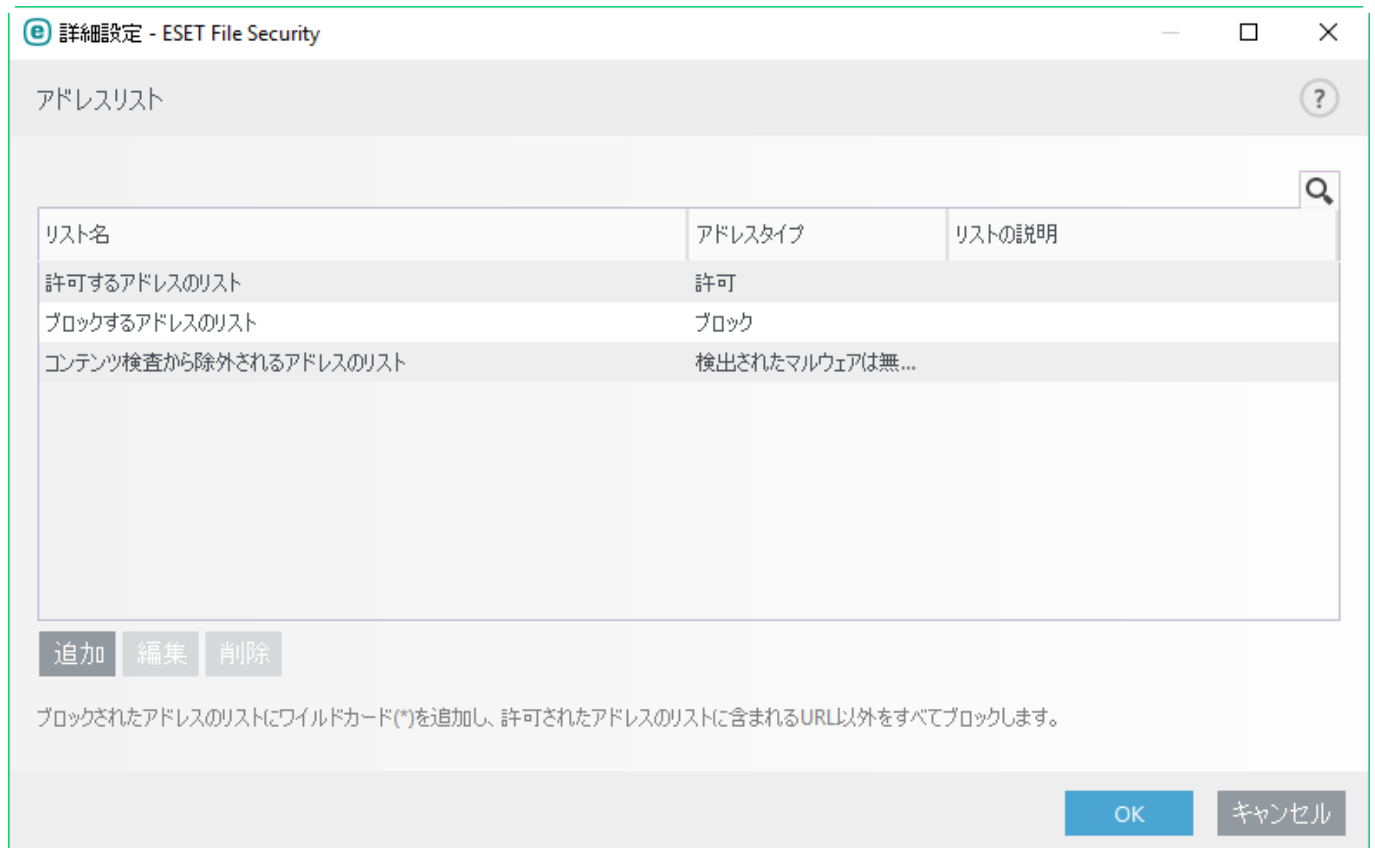
URLアドレス管理

URLアドレス管理では、ブロック、許可、またはチェックから除外するHTTPアドレスを指定できます。ブロックされたアドレスのリストのWebサイトは、許可されたアドレスのリストにも登録されていない場合は、アクセスできません。検査対象外のアドレスのリストのWebサイトは、アクセス時に悪意のあるコードがあるかどうかの検査が行われません。HTTP Webページの他に、HTTPSアドレスをフィルタリングする場合は、[\[SSL/TLSプロトコルフィルタリング\]](#)を有効にする必要があります。それ以外の場合、アクセスしたHTTPSサイトのドメインのみが追加され、完全なURLは追加されません。

ブロックされたアドレスの1つのリストには、一部の外部パブリックブラックリストのアドレスを登録し、もう1つのブロックされたアドレスのリストには独自のブラックリストを登録できます。これによって、自分のブラックリストを修正せずに、外部リストを簡単に更新できます。

編集および**追加**をクリックすると、定義済みのリストの他に、[新しいアドレスリストを作成](#)します。さまざまなグループのアドレスを論理的に分割する場合に便利です。既定では、次の3つのリストを使用できます。

- **フィルタリング対象外とするアドレスのリスト** – アドレスをリストに追加すると、悪意のあるコードのチェックは実行されません。
- **許可するアドレスのリスト** – [許可されたアドレスのリスト内のHTTPアドレスのみにアクセスを許可する]が有効で、ブロックされたアドレスのリストに*(すべてと一致)が含まれる場合、ユーザーはこのリストで指定されたアドレスのみにアクセスできます。このリストのアドレスは、ブロックされたアドレスのリストに含まれる場合にも、許可されます。
- **ブロックされるアドレスのリスト** – 許可されたアドレスにリストにある場合でも、ユーザーは、このリストで指定されたアドレスにはアクセスできません。



新しいURLアドレスをリストに**追加**できます。区切り文字を使用して複数の値を入力することもできま

す。**編集**をクリックすると、リストの既存のアドレスを修正します。**削除**をクリックすると、削除します。**追加**を使用して作成されたアドレスのみを削除できます。インポートされたアドレスは削除できません。

どのリストでも、特殊記号の*(アスタリスク)および?(疑問符)を使用できます。アスタリスクは任意の数字または文字を表します。疑問符は任意の1文字を表します。除外アドレスを指定する際には、細心の注意を払ってください。その一覧には信頼できる安全なアドレスだけを掲載すべきだからです。同様に、記号の*および?を一覧内で正しく使用してください。

注意

アクティブな許可されたアドレスのリストにあるアドレスを除き、すべてのHTTPアドレスをブロックする場合は、アクティブなブロックするアドレスのリストに*を追加します。

新規リストの作成

このリストには、ブロック、許可、または確認から除外される任意のURLアドレス/ドメインマスクが含まれます。新しいリストを作成するときには、次の内容を指定します。

- **アドレスリストタイプ** – ドロップダウンリストからタイプ(確認から除外、ブロック、または許可)を選択します。
- **リスト名** – リストの名前を指定します。3つの定義済みリストのいずれかを編集するときには、このフィールドが灰色で表示されます。
- **リストの説明** – リストの短い説明を入力します(オプション)。3つの定義済みリストのいずれかを編集するときには灰色で表示されます。
- **リストのアクティブ化** – スイッチを使用し、リストを非アクティブ化します。必要に応じて、後からリストをアクティブ化できます。
- **適用するときに通知する** – アクセスしたHTTP/HTTPSサイトの評価で特定のリストが使用されるときに通知を表示します。Webサイトがブロックまたは許可されたアドレスのリストにあるため、ブロックまたは許可された場合、通知が発行されます。通知には、指定されたWebサイトを含むリストの名前があります。
- **ログの重要度** – ドロップダウンリストから、ログの重要度(なし、診断、情報、警告)を選択します。**警告**レベルのレコードは、ESET PROTECTによって収集できます。

ESET Server Securityでは、指定したWebサイトへのアクセスを遮断して、インターネットブラウザにそのコンテンツを表示させないようにすることができます。さらに、検査から除外するアドレスを指定することもできます。リモートサーバの完全な名前が不明であるか、またはリモートサーバのグループ全体を指定する場合には、いわゆるマスクを使用して、そのようなグループを特定できます。

マスクには、記号の?と*があります。

- 記号1つを表すには、“??”を使用します。
- 文字列1つを表すには、*を使用します。

例

*.c?mは、最後の部分が文字cで始まって文字mで終わり、その間に任意のシンボルが入る(.com.camなど)すべてのアドレスに当てはまります。

先頭の「*.」シーケンスは、ドメイン名の先頭で使用されると、特殊な方法で処理されます。まず、こ

の場合、*ワイルドカードはスラッシュ文字('/')を表すことができません。これは、例えば、マスク *.domain.comが <https://anydomain.com/anypath#.domain.com> と一致しないように(このようなサフィックスはダウンロードに影響せずにURLの最後に付加できます)、マスクの迂回を回避するためです。次に、この特殊な場合では、「*。」は空の文字列にも一致します。これは、1つのマスクを使用したサブドメインを含むドメイン全体と一致できるようにするためです。例えば、マスク *.domain.com は <https://domain.com> にも一致します。*.domain.comの使用は <https://anotherdomain.com> にも一致するため、正しくありません。



複数の値を入力

改行、カンマ、セミコロンで区切られた複数のURLアドレスを追加できます。複数のセミコロンが有効な場合、アドレスがリストに表示されます。

インポート

インポートするURLアドレスが記述されたテキスト(値は改行で区切ります。例: UTF-8エンコードを使用した*.txt

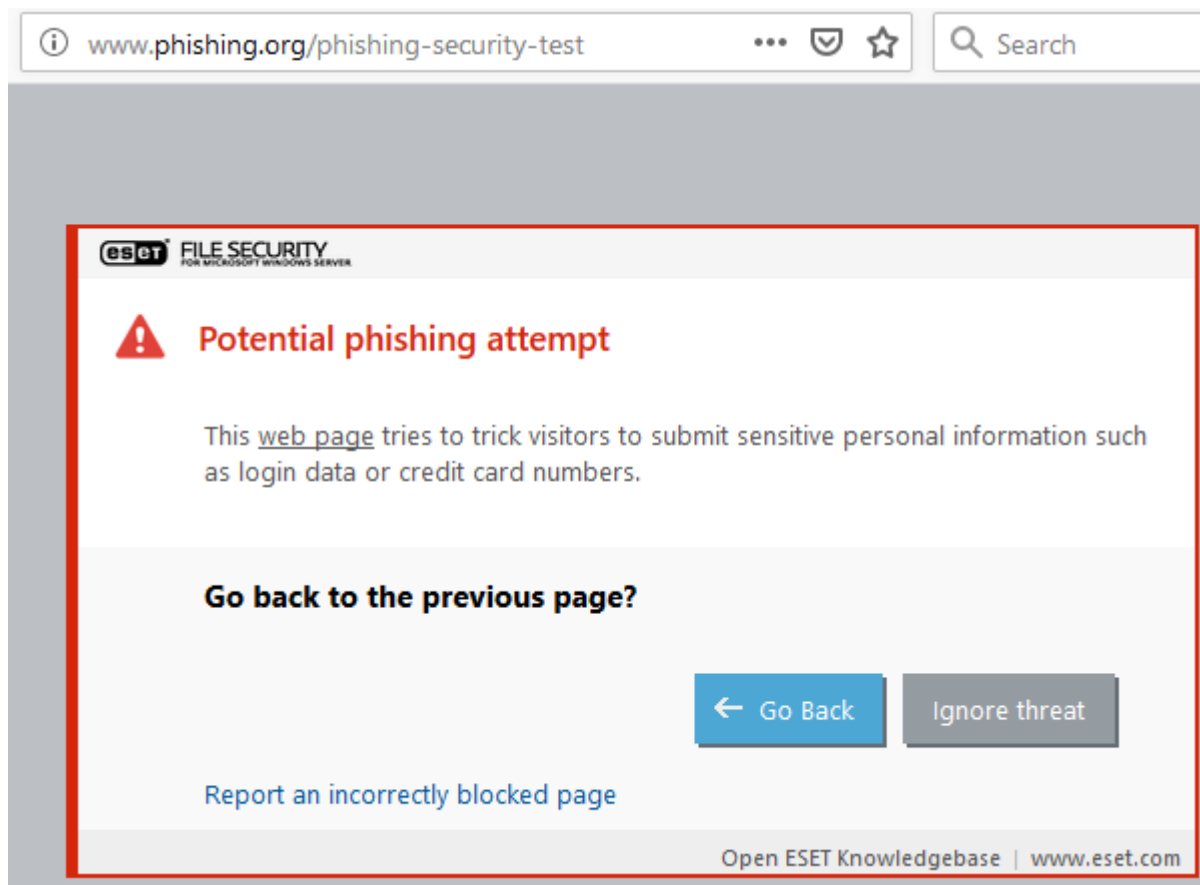


フィッシング対策Web保護

フィッシングとは、ソーシャルエンジニアリング（機密情報を入手するために、ユーザーを操ることを用いる犯罪行為を指します。フィッシングは、銀行の口座番号やPINコードなどの機密データを入手するためによく使用されます。

ESET Server Securityはフィッシング対策機能を提供し、このようなコンテンツを配布することが知られているWebページをブロックできます。ESET Server Securityでフィッシング対策機能を有効にすることを強くお勧めします。ESET Server Securityのフィッシング対策保護の詳細については、[ナレッジベース記事](#)を参照してください。

認識されているフィッシングWebサイトにアクセスすると、次のダイアログがWebブラウザに表示されます。それでもWebサイトにアクセスする場合は、**[脅威を無視]**（推奨されません）をクリックします。



注意

ホワイトリストに入れられた潜在的なフィッシングWebサイトは、既定では数時間後に有効期限が切れます。Webサイトを永続的に許可するには、[URLアドレス管理](#)ツールを使用します。

[フィッシングサイトを報告する](#)

フィッシングまたは他の悪意があるように考えられる不審なWebサイトを見つけた場合は、分析のためにESETに報告できます。ESETにWebサイトを提出する前に、次の基準の1つ以上を満たしていることを確認してください。

- Webサイトがまったく検出されない
- Webサイトが誤ってウイルスとして検出されるこの場合は、[誤検出されたフィッシングサイトを報告](#)できます。

また、メールでWebサイトを提出することもできます。メールはsamples@eset.comに送信してください。わかりやすい件名にし、Webサイトに関する情報(参照元のWebサイト、このWebサイトを知った経緯など)をできるだけ多く記載してください。

デバイスコントロール

ESET Server Securityは、自動デバイスコントロール(CD/DVD/USB)を備えています。このモジュールを使用すると、拡張フィルタ/権限を検査、ブロック、または調整して、ユーザーからの指定デバイスへのアクセス方法やその作業方法を定義できます。この機能は、望ましくないコンテンツを収めたデバイスをユーザーが使用することを防止したいコンピュータ管理者にとって便利です。

注意

システムに統合スイッチを使用して、デバイスコントロールを有効にするとESET Server Securityのデバイスコントロール機能が有効になります。ただし、この変更を有効にするには、システムの再起動が必要です。

デバイスコントロールが有効になり、設定を編集できます。既存のルールでブロックされているデバイスが検出されると、通知ウィンドウが表示され、デバイスへのアクセス権は付与されません。

ルール

デバイスコントロールルールでは、ルール基準に適合するデバイスがコンピュータに接続されたときに実行されるアクションを定義します。

グループ

編集をクリックすると、デバイスグループを管理できます。新しいデバイスグループを作成するか、既存のグループを選択し、リストに追加または削除できます。

注意

ログファイルにデバイスコントロールログエントリを表示できます。

デバイスルール

特定のデバイスについては、ユーザー単位またはユーザーグループ単位で、および複数の追加パラメータに基づいて許可またはブロックできます。これは、ルール設定で指定できます。ルールのリストは名前、外部デバイスのタイプ、デバイスが検出されるときに実行されるアクション、ログの重大性等の複数の詳細説明を含みます。

新しいルールを追加するか、既存のルールの設定を修正できます。識別しやすいように、ルールの説明を[名前]フィールドに入力します。[ルール有効]の隣のチェックボックスを選択すると、このルールは無効または有効になります。これは、ルールを永続的に削除したくない場合に便利です。

適用期間

時間スロットを使用してルールを制限できます。まず時間スロットを作成すると、ドロップダウンメニューに表示されます。

デバイスのタイプ

外部デバイスタイプをドロップダウンメニュー(ディスクストレージ/ポータブルデバイス/Bluetooth/FireWire/...)から選択します。デバイスタイプは、オペレーティングシステムから継承されます。デバイスタイプは、デバイスがコンピュータに接続されていれば、そのシステムのデバイスマネージャで確認できます。記憶装置にはUSBまたはFireWireから接続できる外付けハードディスクや標準的なメモ리카ードリーダーが含まれます。スマートカードリーダーとはSIMカード、認証カードなど、集積回路が埋め込まれているスマートカードを読み取るリーダーのことです。イメージングデバイスは、スキャナやカメラなどです。これらのデバイスはユーザーに関する情報は提供せず、そのアクションだけを提供します。したがって、イメージングデバイスをブロックする場合は全体としてブロックする必要があります。

アクション

記憶装置以外へのアクセスは、許可またはブロックすることができます。それに対して、記憶装置のルールについては、次のいずれかの権限設定を選択できます。

- **読み込み/書き込み** – デバイスへの完全アクセスが許可されます。
- **拒否** – デバイスへのアクセスはブロックされます。
- **読み込み専用** – デバイスからの読み込みアクセスだけが許可されます。
- **警告** – デバイスに接続するたびに、許可またはブロックするかが通知され、ログエントリが作成されます。デバイスは記憶されません。同じデバイスに後から接続する場合にも、通知が表示されます。

注意

デバイスのタイプによっては、適用されない権限(許可されないアクション)もあります。記憶領域を持つデバイスでは、上記の4つのアクションのいずれも選択できます。記憶装置以外のデバイスでは、これらのうち2つだけが適用可能です(たとえばBluetoothの場合、**[読み込み専用]**アクションは適用できないので、許可かブロックだけになります)。

追加パラメータは、ルールを微調整したりデバイスに合わせて変更するのに使用できます。いずれのパラメーターでも大文字と小文字は区別されません。

- **ベンダー** – ベンダー名またはIDによるフィルタリング。
- **モデル** – デバイスに付けられている名前。
- **シリアル** – 外部デバイスには通常独自のシリアル番号が付いています。CD/DVDの場合は、CDドライブではなく、そのメディアのシリアル番号があります。

注意

上記の3つの記述が空の場合、ルールでは突き合せ時にこれらのフィールドは無視されます。すべてのテキストフィールドのフィルタリングパラメータは、大文字と小文字が区別されず、ワイルドカード(*, ?)はサポートされません。

デバイスのパラメータを確認するには、デバイスのタイプのルールを作成し、デバイスをコンピュータに接続してから、[デバイスコントロールログ](#)でデバイス詳細を確認します。

ドロップダウンリストから**ログの重要度**を選択します。

- **常時** – すべてのイベントをログに記録します。
- **診断** – プログラムを微調整するのに必要な情報をログに記録します。
- **情報** – アップデートの成功メッセージを含むすべての情報メッセージと上記のすべてのレコードを記録します。
- **警告** – 重大なエラー、エラー、および警告メッセージを記録します。
- **なし** – ログは記録されません。

ルールを特定のユーザーまたはユーザーグループに限定する場合は、次のようにして該当するユーザーまたはユーザーグループを**[ユーザー一覧]**に追加します。**編集**をクリックすると、ユーザーリストを管理できます。

- **追加** - **[オブジェクトの種類: ユーザーまたはグループ]**ダイアログウィンドウを開きます。このウィンドウで目的のユーザーを選択できます。
- **削除** – 選択されたユーザーをフィルタから削除します。

注意

すべてのデバイスをユーザールールでフィルタリングできます(たとえば、イメージングデバイスではユーザーに関する情報は提供されず、実行されたアクションに関する情報だけが提供されます)。

使用可能な機能は次のとおりです。

編集

選択したルールの名前またはグループに含まれるデバイスのパラメータ(ベンダー、モデル、シリアル番号)を変更できます。

コピー

選択したルールのパラメータに基づいて新しいルールを作成します。

削除

選択したルールを削除します。あるいは、特定のルールの横のチェックボックスを使用して、無効にできます。今後使用する可能性があり、ルールを完全に削除したくない場合に便利です。

入力

現在接続されているすべてのデバイスの概要と次の情報が表示されます。この情報には、デバイスタイプ、デバイスの製造元、モデル、シリアル番号(ある場合)などがあります。検出されたデバイスのリストからデバイスを選択し、**[OK]**をクリックすると、ルールエディタが開き、定義済みの情報が表示されます(すべての設定を調整できます)。

ルールは優先度順に一覧表示されます。最も優先度が高いルールが最上位に表示されます。削除や**最上位/上/下/最下位**(矢印ボタン)をクリックしたリスト内での上下移動など、複数のルールを選択して、アクションを適用できます。

デバイスグループ

デバイスグループウィンドウは、2つの部分に分かれます。ウィンドウの右側には、該当するグループに属するデバイスが一覧表示されます。ウィンドウの左側には、既存のグループのリストが表示されます。右側のペインに表示するデバイスを含むグループを選択します。

異なるルールが適用されるさまざまなデバイスのグループを作成できます。また、**読み書き**または**読み取り専用**に設定されたデバイスのグループは、1つだけ作成できます。これにより、コンピュータに接続したときに、認識されていないデバイスがデバイスコントロールによってブロックされます。

警告

コンピュータに接続された外部デバイスは、セキュリティリスクになる可能性があります。

使用可能な機能は次のとおりです。

追加

追加- ボタンをクリックしたウィンドウの部分に応じて、名前を入力してグループを作成するか、デバイスを既存のグループに追加できます(任意で、ベンダー名、モデル、シリアル番号などの詳細を指定できます)。

編集

選択したグループの名前またはグループに含まれるデバイスのパラメータ(ベンダー、モデル、シリアル番号)を変更できます。

削除

クリックしたウィンドウの場所に応じて、選択したグループまたはデバイスを削除します。あるいは、特定のルールの横のチェックボックスを使用して、無効にできます。今後使用する可能性があり、ルールを完全に削除したくない場合に便利です。

インポート

ファイルからデバイスのシリアル番号のリストをインポートします。

入力

現在接続されているすべてのデバイスの概要と次の情報が表示されます。この情報には、デバイスタイプ、デバイスの製造元、モデル、シリアル番号(ある場合)などがあります。検出されたデバイスのリストからデバイスを選択し、**[OK]**をクリックすると、ルールエディタが開き、定義済みの情報が表示されます(すべての設定を調整できます)。

カスタマイズが完了したら、**[OK]**をクリックします。変更を保存せずに**[デバイスグループ]**を終了する場合は、**[編集]**をクリックします。

注意

デバイスのタイプによっては、適用されない権限(許可されないアクション)もあります。記憶領域を持つデバイスでは、上記の4つのアクションのいずれも選択できます。記憶装置以外のデバイスでは、これらのうち2つだけが適用可能です(たとえばBluetoothの場合、[読み込み専用]アクションは適用できないので、許可がブロックだけになります)。

ツール設定

次の詳細設定をカスタマイズできます。

- [タイムスロット](#)
- [ESET PROTECT検査の対象](#)
- [上書きモード](#)
- [ESET CMD](#)
- [ESET RMM](#)
- [ライセンス](#)
- [WMIプロバイダ](#)
- [ログファイル](#)
- [プロキシサーバ](#)
- [電子メール通知](#)
- [プレゼンテーションモード](#)
- [診断](#)
- [クラスタ](#)

タイムスロット

タイムスロットは、[デバイスコントロールルール](#)で使用され、適用されるときにルールを制限します。タイムスロットを作成し、新しいルールを追加するか、既存のルールを編集するタイミングを選択します(**適用期間**パラメーター)。これにより、一般的に使用されるタイムスロット(業務時間、週末など)を定義し、ルールごとに時間範囲を再定義することなく、簡単に再利用できます。タイムスロットは、時間ベースの制御をサポートするすべての該当するルールのタイプに適用できます。

Microsoft Windows Update

Windowsupdateは、潜在的に危険な脆弱性に対する重要な修正を提供し、コンピュータの一般的なセキュリティレベルを高めます。そのためMicrosoft Windowsアップデートが使用可能になったら即座にイン

ストールすることが欠かせません。ESET Server Securityは、指定されたレベルに従って、欠落したアップデートがあるとユーザーにそれを通知します。使用可能なレベルは次のとおりです。

- **通知しない** – 提示されるシステムアップデートはありません。
- **オプションのアップデート** – 低優先度以上とマークされているアップデートがダウンロード用として提示されます。
- **推奨されるアップデート** – 通常優先度以上とマークされているアップデートがダウンロード用として提示されます。
- **重要なアップデート** – 重要優先度以上とマークされているアップデートがダウンロード用として提示されます。
- **緊急のアップデート** – 緊急のアップデートのみがダウンロード用として提示されます。

変更内容を保存するには、[OK]をクリックします。アップデートサーバでステータスの検証を行った後、[システムのアップデート]ウィンドウが表示されます。システムアップデートの情報は、変更を保存した後、即座に使用できない場合があります。

コマンドラインスキャナー

[eShell](#)の代わりに、インストールフォルダーにあるecls.exeを使用して、コマンドラインからESET Server Securityオンデマンドスキャナーを実行できます。

次に、パラメーターとスイッチの一覧を示します。

オプション:

/base-dir=FOLDER	FOLDERから機能をロードします
/quar-dir=FOLDER	FOLDERを隔離します
/exclude=MASK	MASKと一致するファイルをスキャン対象から除外します
/subdir	サブフォルダを検査します(既定)
/no-subdir	サブフォルダを検査しません
/max-subdir-level=LEVEL	スキャン対象に含めるサブフォルダ階層の下限レベル
/symlink	シンボリックリンクをたどります(既定)
/no-symlink	シンボリックリンクをスキップします
/ads	ADSを検査します(既定)
/no-ads	ADSを検査しません
/log-file=FILE	ログをFILEに出力します
/log-rewrite	ログファイルを上書きします(既定 - append)
/log-console	ログをコンソールに出力します(既定)
/no-log-console	ログをコンソールに出力しません
/log-all	感染していないファイルも記録します
/no-log-all	感染していないファイルは記録しません(既定)
/auid	アクティビティインジケータを表示します
/auto	すべてのローカルディスクを検査し、自動的に駆除します

スキャナオプション:

/files	ファイルを検査します(既定)
/no-files	ファイルを検査しません
/memory	メモリを検査します
/boots	ブートセクタを検査します
/no-boots	ブートセクタを検査しません(既定)
/arch	アーカイブを検査します(既定)
/no-arch	アーカイブを検査しません
/max-obj-size=SIZE	SIZEメガバイト未満のファイルのみスキャンします(既定0 = 制限なし)
/max-arch-level=LEVEL	スキャン対象に含めるアーカイブ内の上限ネストレベル
/scan-timeout=LIMIT	最大でLIMIT秒間アーカイブを検査します
/max-arch-size=SIZE	アーカイブのうちSIZEメガバイト未満のファイルのみスキャンします(既定0 = 制限なし)
/max-sfx-size=SIZE	自己解凍アーカイブのうちSIZEメガバイト未満のファイルのみスキャンします(既定0 = 制限なし)
/mail	電子メールファイルをスキャンします(既定)
/no-mail	電子メールファイルをスキャンしません
/mailbox	メールボックスの検査(既定)
/no-mailbox	受信箱を検査しません
/sfx	自己解凍アーカイブを検査します(既定)
/no-sfx	自己解凍アーカイブを検査しません
/rtp	ランタイム圧縮形式を検査します(既定)
/no-rtp	ランタイム圧縮形式を検査しません
/unsafe	潜在的に危険性のあるアプリケーションを検査します
/no-unsafe	潜在的に危険性のあるアプリケーションを検査しません(既定)
/unwanted	潜在的に不要なアプリケーションを検査します
/no-unwanted	潜在的に不要なアプリケーションを検査しません(既定)
/suspicious	不審なアプリケーションを検査します(既定)
/no-suspicious	不審なアプリケーションを検査しません
/pattern	シグネチャを使用します(既定)
/no-pattern	シグネチャを使用しません
/heur	ヒューリスティックを有効にします(既定)
/no-heur	ヒューリスティックを無効にします
/adv-heur	アドバンスドヒューリスティックを有効にします(既定)
/no-adv-heur	アドバンスドヒューリスティックを無効にします
/ext-exclude=EXTENSIONS	コロン区切りのファイル拡張子を検査から除外します。

/clean-mode=MODE	感染したオブジェクトに対して駆除モードを使用します。 使用可能なオプションは次のとおりです。 • none（既定） - 自動駆除を実行しません。 • standard - ecls.exeは感染したファイルを自動的に駆除または削除しようとしています。 • strict - ecls.exeはユーザー操作を要求せずに感染したファイルを自動的に駆除または削除しようとしています(ファイルが駆除される前の確認メッセージは表示されません)。 • rigorous - ファイルの種類に関係なくecls.exeは駆除せずにファイルを削除します。 • delete - ecls.exeは駆除せずにファイルを削除しますがWindowsシステムファイルなどの重要なファイルは削除しません。
/quarantine	(駆除された場合)感染ファイルを隔離フォルダにコピーします(駆除中に実行されたアクションの補完)。
/no-quarantine	感染ファイルを隔離フォルダにコピーしません

一般的なオプション:

/help	ヘルプを表示して終了します
/version	バージョン情報を表示して終了します
/preserve-time	最終アクセスのタイムスタンプを保持

終了コード:

0	マルウェアは検出されませんでした
1	マルウェアが検出され、駆除されました
10	一部のファイルはスキャンできません(マルウェアの可能性あり)
50	検出された脅威
100	エラー(100を超える終了コードは、ファイルが検査されていないため未感染であると見なせないことを意味します)

ESET CMD

これは高度なecmdコマンドを有効にする機能です。コマンドライン(ecmd.exe)を使用して、設定をインポートおよびエクスポートできます。これまで、[GUI](#)のみを使用して設定をエクスポートできませんでした。ESET Server Security設定を.xmlファイルにエクスポートできます。

ESET CMDを有効にすると、2つの認証方法を使用できます。

- なし - 認証なし。潜在的なリスクとなる未署名の設定のインポートが許可されるため、この方法は推奨されません。
- [詳細設定パスワード] - .xmlファイルから設定をインポートするときには、パスワードが必要です。このファイルを署名する必要があります(.xm設定ファイルの署名を参照してください)。[アクセス設定](#)で指定されたパスワードを、新しい設定をインポートする前に指定する必要があります。アクセス設定パスワードが有効ではないか、パスワードが一致しないか、.xm設定ファイルが署名されていない場合は、設定はインポートされません。

ESET CMDを有効にするとESET Server Security設定のエクスポート/インポートでコマンドラインを使用できます。手動で実行するか、自動化用のスクリプトを作成できます。

重要

高度なecmdコマンドを使用するには、管理者権限で実行するか、**管理者として実行**を使用し、Windowsコマンドプロンプト(cmd)を開く必要があります。そうでないと、**Error executing command.**というメッセージが表示されます。また、設定のインポート時には、インポート先フォルダーが存在する必要があります。エクスポートコマンドは、ESET CMD設定がオフでも動作します。

例

設定のエクスポートコマンド:
ecmd /getcfg c:\config\settings.xml

設定のインポートコマンド:
ecmd /setcfg c:\config\settings.xml

注意

高度なecmdコマンドはローカルでのみ実行できます。ESET PROTECTを使用したクライアントタスクの**コマンドの実行**は動作しません。

.xm設定ファイルの署名:

1. [XmlSignTool](#)実行ファイルをダウンロードします。
2. **管理者として実行**を使用してWindowsコマンドプロンプト(cmd)を開きます。
3. xmlsigntool.exeのロケーションに移動します。
4. .xm設定ファイルを署名するコマンドを実行します。使用方法: `xmlsigntool /version 1|2 <xml_file_path>`

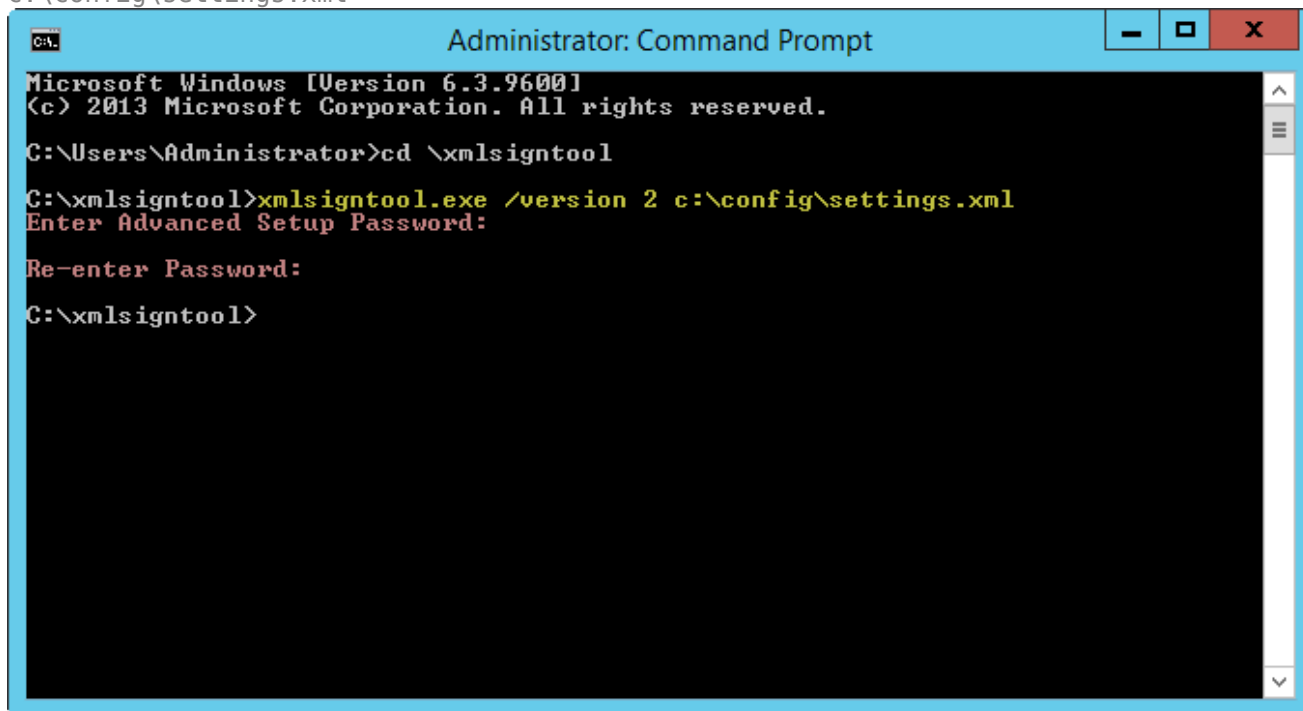
重要

パラメーター/versionの値は、ESET Server Securityバージョンによって異なります。 /version 2 for ESET Server Security 7以降を使用します。

5. XmlSignToolで要求されたら、[詳細設定](#) パスワードを入力して再入力します。.xm設定ファイルが署名されます。パスワード認証方法によってESET CMDを使用してESET Server Securityの別のインスタンスでインポートするために使用できます。

例

エクスポートされた設定ファイルの署名コマンド: `xmldsigntool /version 2 c:\config\settings.xml`



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd \xmldsigntool
C:\xmldsigntool>xmldsigntool.exe /version 2 c:\config\settings.xml
Enter Advanced Setup Password:
Re-enter Password:
C:\xmldsigntool>
```

注意

[アクセス設定](#) パスワードを変更し、古いパスワードで以前に署名された設定ファイルをインポートする場合は、現在のパスワードで、*.xml*設定ファイルをもう一度署名できます。これにより、インポート前にESET Server Securityを実行する他のコンピューターでエクスポートせずに、古い設定ファイルを使用できます。

ESET RMM

リモート監視および管理(RMM)は、管理サービスプロバイダーがアクセスできるローカルにインストールされたエージェントを使用して、ソフトウェアシステム(デスクトップ、サーバー、モバイルデバイスのソフトウェアなど)を監視および制御するプロセスです。

RMMを有効にする

リモート監視と管理コマンドが機能しています。RMMユーティリティを使用するには、管理者権限が必要です。

動作モード

ドロップダウンメニューからRMMの動作モードを選択します。

- **安全な分離のみ** - 安全な読み取り専用の操作に対してRMMインターフェイスを有効にする場合
- **すべての操作** - すべての操作に対してRMMインターフェイスを有効にする場合

認証方法

ドロップダウンメニューからRMM認証方法を設定します。

- **なし** - アプリケーションパスチェックは実行されません。*ermm.exe*を任意のアプリケーション

から実行できます

- **アプリケーションパス** - *ermm.exe*を実行できるアプリケーションを指定します。

既定のESET Endpoint SecurityインストールにはESET Server Securityにある*ermm.exe*ファイル(既定のパスはc:\Program Files\ESET\ESET Server Security)が含まれますRMMエージェントと通信するRMMプラグインとの*ermm.exe*交換データは、RMMサーバーにリンクされます。

- *ermm.exe* - ESETが開発したコマンドラインユーティリティであり、エンドポイント製品とRMMプラグインとの通信を管理できます。
- RMMプラグイン - Endpoint Windowsシステムでローカル実行されるサードパーティアプリケーション。このプラグインは、特定のRMMエージェント(例: Kaseyaのみ)および*ermm.exe*と通信するために設計されています。
- RMMエージェント - Endpoint Windowsシステムでローカル実行されるサードパーティアプリケーション(例: Kaseya)エージェントは、RMMプラグインおよびRMMサーバーと通信します。
- RMMサーバー - サードパーティサーバーのサービスとして実行されます。サポートされているRMMは、Kaseya、Labtech、Autotask、Max Focus、Solarwinds N-ableです。

ESET Server SecurityのESET RMMの詳細については、[ナレッジベース記事](#)を参照してください。

サードパーティのRMMソリューション用ESET Direct Endpoint Managementプラグイン

RMMサーバーは、サードパーティのサーバーでサービスとして実行されています。詳細については、次のESET Direct Endpoint Managementオンラインユーザーガイドを参照してください。

- [ESET Direct Endpoint Management Plug-in for ConnectWise Automate](#)
- [ESET Direct Endpoint Management Plugin for DattoRMM](#)
- [ESET Direct Endpoint Management for Solarwinds N-Central](#)
- [ESET Direct Endpoint Management for NinjaRMM](#)

ライセンス

ESET Server Securityは1時間に数回ESETライセンスサーバーに接続し、チェックを実行します。**間隔チェック**パラメーターは、既定で**[自動]**に設定されています。ライセンスチェックによって発生するネットワークトラフィックを減らしたい場合は、間隔チェックを**制限**に変更すると、ライセンスチェックが1日に1回だけ(サーバーの再起動後に)行われます。

間隔チェックを**制限**に設定するとESET Business AccountとESET MSP管理者経由でESET Server Securityに対して行われたすべてのライセンス関連の変更が適用されるまでに最大で1日かかる場合があります。

WMIプロバイダ

Windows Management Instrumentation (WMI)は、エンタープライズ環境で管理情報にアクセスするための標準技術を開発するための業界の取り組みであるWeb-Based Enterprise Management (WBEM)のMicrosoft実装です。

WMIの詳細については、[http://msdn.microsoft.com/en-us/library/windows/desktop/aa384642\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa384642(v=vs.85).aspx)を参照してください。

ESET WMIプロバイダ

ESET WMIプロバイダの目的は、ESET固有のソフトウェアまたはツールを必要とせずに、エンタープライズ環境でESET製品のリモート監視ができるようにすることです。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。

現在の実装では、基本製品情報、インストール済み機能と保護状態、個別スキャナの統計、および製品ログファイルに読み取りアクセスできます。

WMIプロバイダによって、標準のWindows WMIインフラストラクチャおよびツールの使用と、製品と製品ログの状態の読み取りが可能です。

提供されたデータ

ESET製品に関連付けられたすべてのWMIクラスは「root\ESET」ネームスペースにあります。この後に詳細に説明する次のクラスが現在実装されています。

一般

- **ESET_Product**
- **ESET_Features**
- **ESET_Statistics**

ログ

- **ESET_ThreatLog**
- **ESET_EventLog**
- **ESET_ODFileScanLogs**
- **ESET_ODFileScanLogRecords**
- **ESET_ODServerScanLogs**
- **ESET_ODServerScanLogRecords**
- **ESET_HIPSLog**
- **ESET_URLLog**
- **ESET_DevCtrlLog**
- **ESET_GreylistLog**
- **ESET_MailServeg**
- **ESET_HyperVScanLogs**
- **ESET_HyperVScanLogRecords**

ESET_Product クラス

ESET_Productクラスには1つのインスタンスだけがあります。このクラスのプロパティは、インストール済みのESET製品の基本情報を参照します。

- **ID** - emsなどの製品タイプID
- **Name** - ESET Mail Securityなどの製品名
- **FullName** - ESET Mail Security for IBM Dominoなどの製品名
- **Version** - 「6. 5. 14003. 0」などの製品バージョン
- **VirusDBVersion** - 「14533 (20161201)」などのウイルスデータベースのバージョン
- **VirusDBLastUpdate** - ウイルスデータベースの最終更新日時のタイムスタンプ。この文字列にはWMI日時形式のタイムスタンプが含まれます。例えば、「20161201095245+060」です。

- **LicenseExpiration** – ライセンスの有効期限。この文字列にはWMI日時形式のタイムスタンプが含まれます。
- **KernelRunning** - ekrnサービスがコンピューターで実行中かどうかを示すブール値。例: "TRUE"
- **StatusCode** – 製品の保護ステータスを示す数字。0 – 緑(OK) 1 - 黄(警告)、2 – 赤(エラー)
- **StatusText** – ゼロ以外のステータスコードの理由を説明するメッセージ。ない場合は空です。

ESET_Featuresクラス

ESET_Featuresクラスには、製品機能数に応じて、複数のインスタンスがあります。各インスタンスの内容:

- **Name** – 機能名(名前のリストは以下に示します)
- **ステータス** – 機能のステータス。0 – 非アクティブ、1 – 無効、2 – 有効

現在認識されている製品機能を示す文字列のリスト

- **CLIENT_FILE_AV** – リアルタイムファイルシステムウイルス対策保護
- **CLIENT_WEB_AV** – クライアントWebウイルス対策保護
- **CLIENT_DOC_AV** – クライアントドキュメントウイルス対策保護
- **CLIENT_NET_FW** – クライアントパーソナルファイアウォール
- **CLIENT_EMAIL_AV** – クライアント電子メールウイルス対策保護
- **CLIENT_EMAIL_AS** – クライアント電子メール迷惑メール対策保護
- **SERVER_FILE_AV** – 保護されたファイルサーバー製品のファイルのリアルタイムウイルス対策保護。例えばESET Server Securityの場合に、SharePointのコンテンツデータベースにあるファイルです。
- **SERVER_EMAIL_AV** – 保護されたサーバー製品の電子メールのウイルス対策保護。例えばExchangeまたはIBM Dominoの電子メールです。
- **SERVER_EMAIL_AS** – 保護されたサーバー製品の電子メールの迷惑メール対策保護。例えばExchangeまたはIBM Dominoの電子メールです。
- **SERVER_GATEWAY_AV** – ゲートウェイ上の保護されたネットワークプロトコルのウイルス対策保護
- **SERVER_GATEWAY_AS** – ゲートウェイ上の保護されたネットワークプロトコルの迷惑メール対策保護

ESET_Statisticsクラス

ESET_Statisticクラスには、製品のスキャナ数に応じて、複数のインスタンスがあります。各インスタンスの内容:

- **Scanner** – 特定のスキャナの文字列コード。例えばCLIENT_FILEです。
- **Total** – 検査されたファイルの合計数
- **Infected** – 検出された感染ファイル数
- **Cleaned** – 駆除されたファイル数
- **Timestamp** – この統計が最後に変更されたタイムスタンプWMI日時形式。例えば、「20130118115511.000000+060」です。
- **ResetTime** – 統計カウンタが最後にリセットされたタイムスタンプWMI日時形式。例えば、「20130118115511.000000+060」です。

現在認識されているスキャナを示す文字列のリスト

- **CLIENT_FILE**
- **CLIENT_EMAIL**

- **CLIENT_WEB**
- **SERVER_FILE**
- **SERVER_EMAIL**
- **SERVER_WEB**

ESET_ThreatLog クラス

ESET_ThreatLog クラスには複数のインスタンスがあり、それぞれのインスタンスが「Detected threats」ログのログレコードを表します。各インスタンスの内容:

- **ID** - この検査ログレコードの一意のID
- **Timestamp** - ログの作成タイムスタンプ(WMI日時形式)
- **LogLevel** - [0-8]の数字で表されるログレコードの重要度。値は次の名前付きレベルに対応します: Debug、Info、Footnote、Info、Info-Important、Warning、Error、SecurityWarning、Error-Critical、SecurityWarning-Critical
- **Scanner** - このログイベントを作成したスキャナの名前
- **ObjectType** - このログイベントを作成したオブジェクトのタイプ
- **ObjectName** - このログイベントを作成したオブジェクトの名前
- **Threat** - ObjectName および ObjectType プロパティで記述されたオブジェクトで検出された脅威名
- **Action** - 脅威が特定された後に実行されたアクション
- **User** - このログイベントを作成したユーザーアカウント
- **Information** - イベントの詳細情報
- **Hash** - このログイベントを作成したオブジェクトのハッシュ

ESET_EventLog

ESET_EventLog クラスには複数のインスタンスがあり、それぞれのインスタンスが「Events」ログのログレコードを表します。各インスタンスの内容:

- **ID** - この検査ログレコードの一意のID
- **Timestamp** - ログの作成タイムスタンプ(WMI日時形式)
- **LogLevel** - [0-8]の数字で表されるログレコードの重要度。値は次の名前付きレベルに対応します: Debug、Info、Footnote、Info、Info-Important、Warning、Error、SecurityWarning、Error-Critical、SecurityWarning-Critical
- **Module** - このログイベントを作成したモジュールの名前
- **Event** - イベントの説明。
- **User** - このログイベントを作成したユーザーアカウント

ESET_ODFileScanLogs

ESET_ODFileScanLogs クラスには複数のインスタンスがあり、各インスタンスはオンデマンドファイル検査レコードを表します。これは、ログのGUI「On-demand computer scan」リストに対応します。各インスタンスの内容:

- **ID** - この検査ログレコードの一意のID
- **Timestamp** - ログの作成タイムスタンプ(WMI日時形式)
- **Targets** - スキャンの対象フォルダ/オブジェクト
- **TotalScanned** - 検査されたオブジェクトの合計数
- **Infected** - 検出された感染オブジェクト数
- **Cleaned** - 駆除されたオブジェクト数
- **Status** - 検査処理のステータス

ESET_ODFileScanLogRecords

ESET_ODFileScanLogRecordsクラスには複数のインスタンスがあり、各インスタンスは、ESET_ODFileScanLogsクラスのインスタンスで表される検査ログのいずれかにあるログレコードを表します。このクラスのインスタンスは、すべてのオンデマンド検査/ログのログレコードを提供します。特定の検査ログのインスタンスだけがが必要な場合、LogIDプロパティでフィルタリングする必要があります。各クラスインスタンスの内容:

- **LogID** - このレコードが属する検査ログのID (ESET_ODFileScanLogsクラスのインスタンスのいずれかのID)
- **ID** - この検査ログレコードの一意のID
- **Timestamp** - ログの作成タイムスタンプ(WMI日時形式)
- **LogLevel** - [0-8]の数字で表されるログレコードの重要度。値は次の名前付きレベルに対応します: Debug、Info-Footnote、Info、Info-Important、Warning、Error、SecurityWarning、Error-Critical、SecurityWarning-Critical
- **Log** - 実際のログメッセージ

ESET_ODServerScanLogs

ESET_ODServerScanLogsクラスには複数のインスタンスがあり、各インスタンスはオンデマンドサーバー検査の実行を表します。各インスタンスの内容:

- **ID** - この検査ログレコードの一意のID
- **Timestamp** - ログの作成タイムスタンプ(WMI日時形式)
- **Targets** - スキャンの対象フォルダ/オブジェクト
- **TotalScanned** - 検査されたオブジェクトの合計数
- **Infected** - 検出された感染オブジェクト数
- **Cleaned** - 駆除されたオブジェクト数
- **RuleHits** - ルールヒットの合計数
- **Status** - 検査処理のステータス

ESET_ODServerScanLogRecords

ESET_ODServerScanLogRecordsクラスには複数のインスタンスがあり、各インスタンスは、ESET_ODServerScanLogsクラスのインスタンスで表される検査ログのいずれかにあるログレコードを表します。このクラスのインスタンスは、すべてのオンデマンド検査/ログのログレコードを提供します。特定の検査ログのインスタンスだけがが必要な場合、LogIDプロパティでフィルタリングする必要があります。各クラスインスタンスの内容:

- **LogID** - このレコードが属する検査ログのID (ESET_ODServerScanLogsクラスのインスタンスのいずれかのID)
- **ID** - この検査ログレコードの一意のID
- **Timestamp** - ログレコードの作成タイムスタンプ(WMI日時形式)
- **LogLevel** - [0-8]の数字で表されるログレコードの重要度。値は次の名前付きレベルに対応します: Debug、Info-Footnote、Info、Info-Important、Warning、Error、SecurityWarning、Error-Critical、SecurityWarning-Critical
- **Log** - 実際のログメッセージ

ESET_SmtpProtectionLog

ESET_SmtpProtectionLogクラスには複数のインスタンスがあり、それぞれのインスタンスが「Smtp protection」ログのログレコードを表します。各インスタンスの内容:

- **ID** - この検査ログレコードの一意のID
- **Timestamp** - ログレコードの作成タイムスタンプ(WMI日時形式)
- **LogLevel** - [0-8]の数字で表されるログレコードの重要度。値は次の名前付きレベルに対応します
 DebugInfo-FootnoteInfoInfo-ImportantWarningErrorSecurityWarningError-CriticalSecurityWarning-Critical
- **HELODomain** - HELOドメインの名前
- **IP** - ソースIPアドレス
- **Sender** - 電子メール送信者
- **Recipient** - 電子メール受信者
- **ProtectionType** - 使用される保護の種類
- **Action** - 実行されたアクション
- **Reason** - アクションの理由
- **TimeToAccept** - 電子メールが許可されるまでの分数

ESET_HIPSLog

ESET_HyperVScanLogRecordsクラスには複数のインスタンスがあり、それぞれのインスタンスが「HIPSログのログレコードを表します。各インスタンスの内容:

- **ID** - このログレコードの一意のID
- **Timestamp** - ログレコードの作成タイムスタンプ(WMI日時形式)
- **LogLevel** - [0-8]の数字で表されるログレコードの重要度。値は次の名前付きレベルに対応します
 DebugInfo-FootnoteInfoInfo-ImportantWarningErrorSecurityWarningError-CriticalSecurityWarning-Critical
- **Application** - ソースアプリケーション
- **Target** - 処理のタイプ
- **Action** - HIPSが実行するアクション。例: 許可、拒否
- **Rule** - アクションを実行するルールの名前
- **AdditionalInfo**

ESET_URLLog

ESET_URLLogクラスには複数のインスタンスがあり、それぞれのインスタンスが「フィルタリングされたWebサイト」ログのログレコードを表します。各インスタンスの内容:

- **ID** - このログレコードの一意のID
- **Timestamp** - ログレコードの作成タイムスタンプ(WMI日時形式)
- **LogLevel** - [0-8]の数字で表されるログレコードの重要度。値は次の名前付きレベルに対応します
 DebugInfo-FootnoteInfoInfo-ImportantWarningErrorSecurityWarningError-CriticalSecurityWarning-Critical
- **URL** - URL
- **Status** - URLで発生した処理。例: Webコントロールによりブロック
- **Application** - URLにアクセスしようとしたアプリケーション
- **User** - アプリケーションを実行したユーザーアカウント

ESET_DevCtrlLog

ESET_DevCtrlLogクラスには複数のインスタンスがあり、それぞれのインスタンスが「デバイスコントロール」ログのログレコードを表します。各インスタンスの内容:

- **ID** - このログレコードの一意のID

- **Timestamp** – ログレコードの作成タイムスタンプ(WMI日時形式)
- **LogLevel** – [0-8]の数字で表されるログレコードの重要度。値は次の名前付きレベルに対応します
DebugInfo-FootnoteInfoInfo-ImportantWarningErrorSecurityWarningError-CriticalSecurityWarning-Critical
- **Device** – デバイス名
- **User** – ユーザーアカウント名
- **UserSID** – ユーザーアカウントSID
- **Group** – ユーザーグループ名
- **GroupSID** – ユーザーグループSID
- **Status** – デバイスで発生した処理。例: 書き込みブロック
- **DeviceDetails** – デバイスの詳細情報
- **EventDetails** – イベントに関する詳細情報

ESET_MailServerLog

ESET_MailServerLogクラスには複数のインスタンスがあり、それぞれのインスタンスが「Mail server」ログのログレコードを表します。各インスタンスの内容:

- **ID** – このログレコードの一意のID
- **Timestamp** – ログレコードの作成タイムスタンプ(WMI日時形式)
- **LogLevel** – [0-8]の数字で表されるログレコードの重要度。値は次の名前付きレベルに対応します
DebugInfo-FootnoteInfoInfo-ImportantWarningErrorSecurityWarningError-CriticalSecurityWarning-Critical
- **IPAddr** – ソースIPアドレス
- **HELODomain** – HELOドメインの名前
- **Sender** – 電子メール送信者
- **Recipient** – 電子メール受信者
- **Subject** – 電子メールの件名
- **ProtectionType** – 現在のログレコードに記述されたアクションを実行した保護タイプ。例: マルウェア対策、迷惑メール対策、ルール
- **Action** – 実行されたアクション
- **Reason** – 特定のProtectionTypeによって、アクションがオブジェクトで実行された理由

ESET_HyperVScanLogs

ESET_HyperVScanLogsクラスには複数のインスタンスがあり、各インスタンスはHyper-Vファイル検査実行を表します。これは、ログのGUI「Hyper-V」リストに対応します。各インスタンスの内容:

- **ID** – このログレコードの一意のID
- **Timestamp** – ログレコードの作成タイムスタンプ(WMI日時形式)
- **Targets** – 検査のターゲットコンピューター/ディスク/ボリューム
- **TotalScanned** – 検査されたオブジェクトの合計数
- **Infected** – 検出された感染オブジェクト数
- **Cleaned** – 駆除されたオブジェクト数
- **Status** – 検査処理のステータス

ESET_HyperVScanLogRecords

ESET_HyperVScanLogRecordsクラスには複数のインスタンスがあり、各インスタンスは、ESET_HyperVScanLogsクラスのインスタンスで表される検査ログのいずれかにあるログレコードを表します。このクラスのインスタンスは、すべてのHyper-V検査/ログのログレコードを提供します。特定

の検査ログのインスタンスだけが必要な場合、LogIDプロパティでフィルタリングする必要があります。
各クラスインスタンスの内容:

- **LogID** – このレコードが属する検査ログのID(ESET_HyperVScanLogsクラスのインスタンスのいずれかのID)
- **ID** – このログレコードの一意のID
- **Timestamp** – ログレコードの作成タイムスタンプ(WMI日時形式)
- **LogLevel** – [0-8]の数字で表されるログレコードの重要度。値は次の名前付きレベルに対応します: Debug、Info-Footnote、Info、Info-Important、Warning、Error、SecurityWarning、Error-Critical、SecurityWarning-Critical
- **Log** – 実際のログメッセージ

ESET_NetworkProtectionLog

ESET_NetworkProtectionLogクラスには複数のインスタンスがあり、それぞれのインスタンスが「Network protection」ログのログレコードを表します。各インスタンスの内容:

- **ID** – このログレコードの一意のID
- **Timestamp** – ログレコードの作成タイムスタンプ(WMI日時形式)
- **LogLevel** – [0-8]の数字で表されるログレコードの重要度。値は次の名前付きレベルに対応します: Debug、Info-Footnote、Info、Info-Important、Warning、Error、SecurityWarning、Error-Critical、SecurityWarning-Critical
- **Event** – ネットワーク保護アクションをトリガーするイベント
- **Action** – ネットワーク保護で実行されたアクション
- **Source** – ネットワークデバイスのソースアドレス
- **Target** – ネットワークデバイスの宛先アドレス
- **Protocol** – ネットワーク通信保護
- **RuleOrWormName** – イベントに関連するルールまたはワーム名
- **Application** – ネットワーク通信を開始したアプリケーション
- **User** – このログイベントを作成したユーザーアカウント

ESET_SentFilesLog

ESET_SentFilesLogクラスには複数のインスタンスがあり、それぞれのインスタンスが「Sent files」ログのログレコードを表します。各インスタンスの内容:

- **ID** – このログレコードの一意のID
- **Timestamp** – ログレコードの作成タイムスタンプ(WMI日時形式)
- **LogLevel** – [0-8]の数字で表されるログレコードの重要度。値は次の名前付きレベルに対応します: Debug、Info-Footnote、Info、Info-Important、Warning、Error、SecurityWarning、Error-Critical、SecurityWarning-Critical
- **Sha1** – 送信されたファイルのSHA-1ハッシュ
- **File** – 送信されたファイル
- **Size** – 送信されたファイルのサイズ
- **Category** – 送信されたファイルのカテゴリ
- **Reason** – ファイルを送信する理由
- **SentTo** – ファイルが送信されたESET部門
- **User** – このログイベントを作成したユーザーアカウント

ESET_OneDriveScanLogs

ESET_OneDriveScanLogsクラスには複数のインスタンスがあり、各インスタンスはOneDrive検査実行を表します。これは、ログのGUIのOneDriveリストに対応します。各インスタンスの内容:

- **ID** – このOneDriveログの一意のID
- **Timestamp** – ログの作成タイムスタンプ(WMI日時形式)
- **Targets** – スキャンの対象フォルダ/オブジェクト
- **TotalScanned** – 検査されたオブジェクトの合計数
- **Infected** – 検出された感染オブジェクト数
- **Cleaned** – 駆除されたオブジェクト数
- **Status** – 検査処理のステータス

ESET_OneDriveScanLogRecords

ESET_OneDriveScanLogRecordsクラスには複数のインスタンスがあり、各インスタンスは、ESET_OneDriveScanLogsクラスのインスタンスで表される検査ログのいずれかにあるログレコードを表します。このクラスのインスタンスは、すべてのOneDrive検査/ログのログレコードを提供します。特定の検査ログのインスタンスだけがが必要な場合、LogIDプロパティでフィルタリングする必要があります。各インスタンスの内容:

- **LogID** – このレコードが属する検査ログのID(ESET_OneDriveScanLogsクラスのインスタンスのいずれかのID)
- **ID** – このOneDriveログの一意のID
- **Timestamp** – ログの作成タイムスタンプ(WMI日時形式)
- **LogLevel** – [0-8]の数字で表されるログレコードの重要度。値は次の名前付きレベルに対応します: Debug、Info、Footnote、Info、Info-Important、Warning、Error、SecurityWarning、Error-Critical、SecurityWarning-Critical
- **Log** – 実際のログメッセージ

提供されたデータへのアクセス

WindowsコマンドラインとPowerShellからESET WMIデータにアクセスする方法の一部の例は、次のとおりです。これは、すべての最新のWindowsオペレーティングシステムで動作します。ただし、他のスクリプト言語とツールからデータにアクセスする別の方法もあります。

スクリプトを使用しないコマンドライン

wmicコマンドラインツールは、さまざまな定義済みまたは任意のカスタムWMIクラスにアクセスするために使用できます。

ローカルコンピュータの製品に関する詳細情報を表示する

```
wmic /namespace:\\root\ESET Path ESET_Product
```

ローカルコンピュータの製品の製品バージョン番号だけを表示する

```
wmic /namespace:\\root\ESET Path ESET_Product Get Version
```

IP 10.1.118.180のリモートコンピュータの製品に関する詳細情報を表示する

```
wmic /namespace:\\root\ESET /node:10.1.118.180 /user:Administrator Path ESET_Product
```

PowerShell

ローカルコンピュータの製品に関する詳細情報を取得して表示する

```
Get-WmiObject ESET_Product -namespace 'root\ESET'
```

IP 10.1.118.180のリモートコンピュータの製品に関する詳細情報を取得して表示する

```
$cred = Get-Credential # ユーザーに認証情報を入力させ変数に格納する
Get-WmiObject ESET_Product -namespace 'root\ESET' -computename '10.1.118.180' -cred $cred
```

ESET PROTECT検査の対象

この機能ではESET Server Securityがインストールされているサーバー上で、**サーバー検査**クライアントタスクを実行するときに、[ESET PROTECT](#)がオンデマンドメールボックスデータベース検査および[Hyper-V検査](#)の検査対象を使用できますESET Management Agentがインストールされている場合にのみESET PROTECT検査対象設定を使用できます。それ以外は灰色で表示されます。


対象リストの生成を使用するとESET Server Securityは使用可能な検査対象のリストを作成します。このリストは、**アップデート期間**に従い、定期的に生成されます。

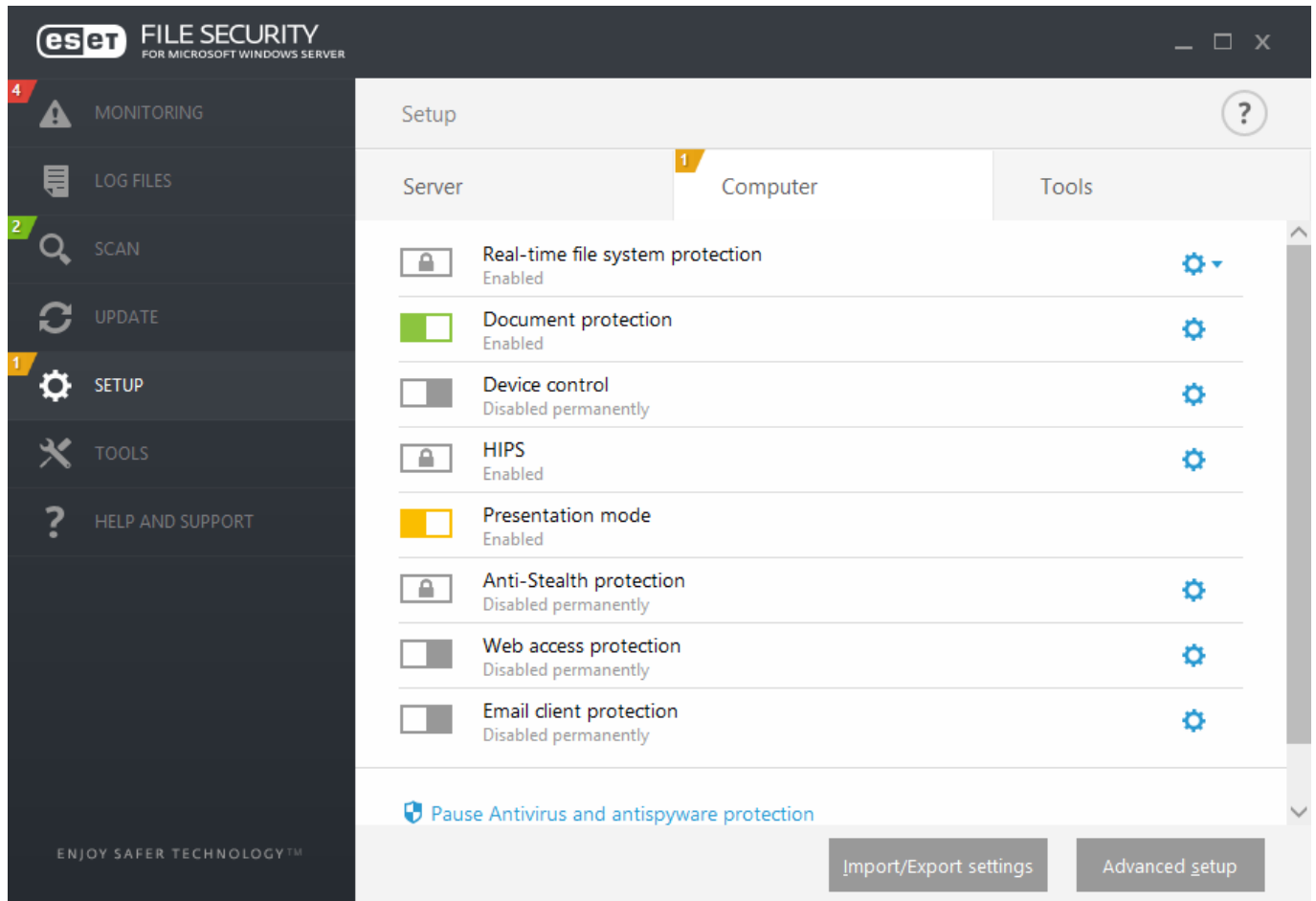
注意

対象リストを生成するを初めて有効にするとESET PROTECTで取得されるまでに、指定した**アップデート期間**の約半分の時間がかかります。このため、**アップデート期間**を60分に設定するとESET PROTECTが検査対象のリストを受信するまでに約30分かかります。これよりも早くESET PROTECTでリストを収集する必要がある場合は、アップデート期間の値を小さく設定します。後からいつでも値を大きくできます。

サーバー検査クライアントタスクを実行する必要がある場合はESET PROTECTはリストを収集し、その特定のサーバーで[Hyper-V検査](#)の検査対象を選択する必要があります。

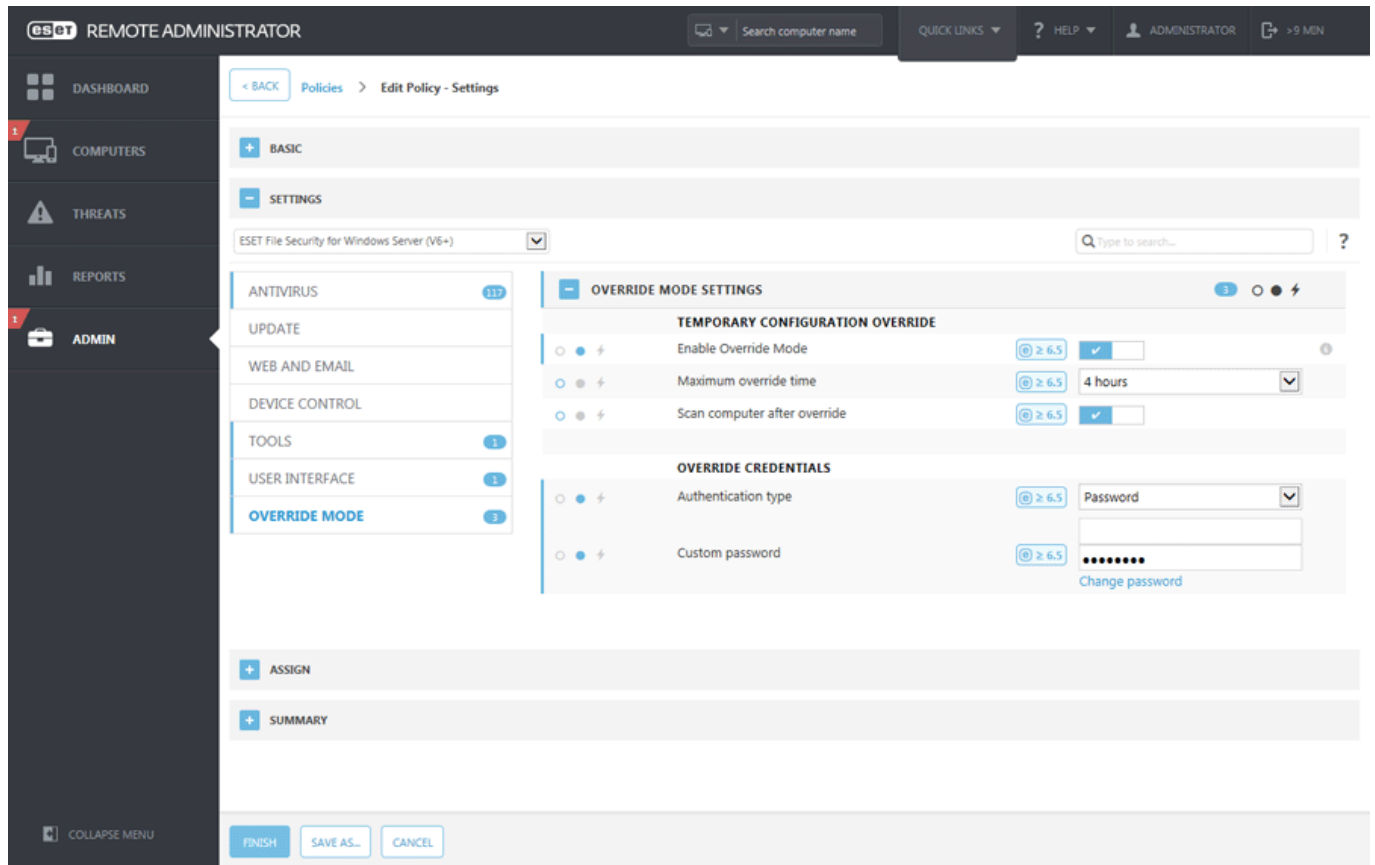
上書きモード

ESET PROTECTポリシーがESET Server Securityに適用されている場合、[設定ページ](#)の有効/無効スイッチと**詳細設定**ウィンドウのスイッチの横のアイコンの代わりに、ロックアイコンが表示されます。

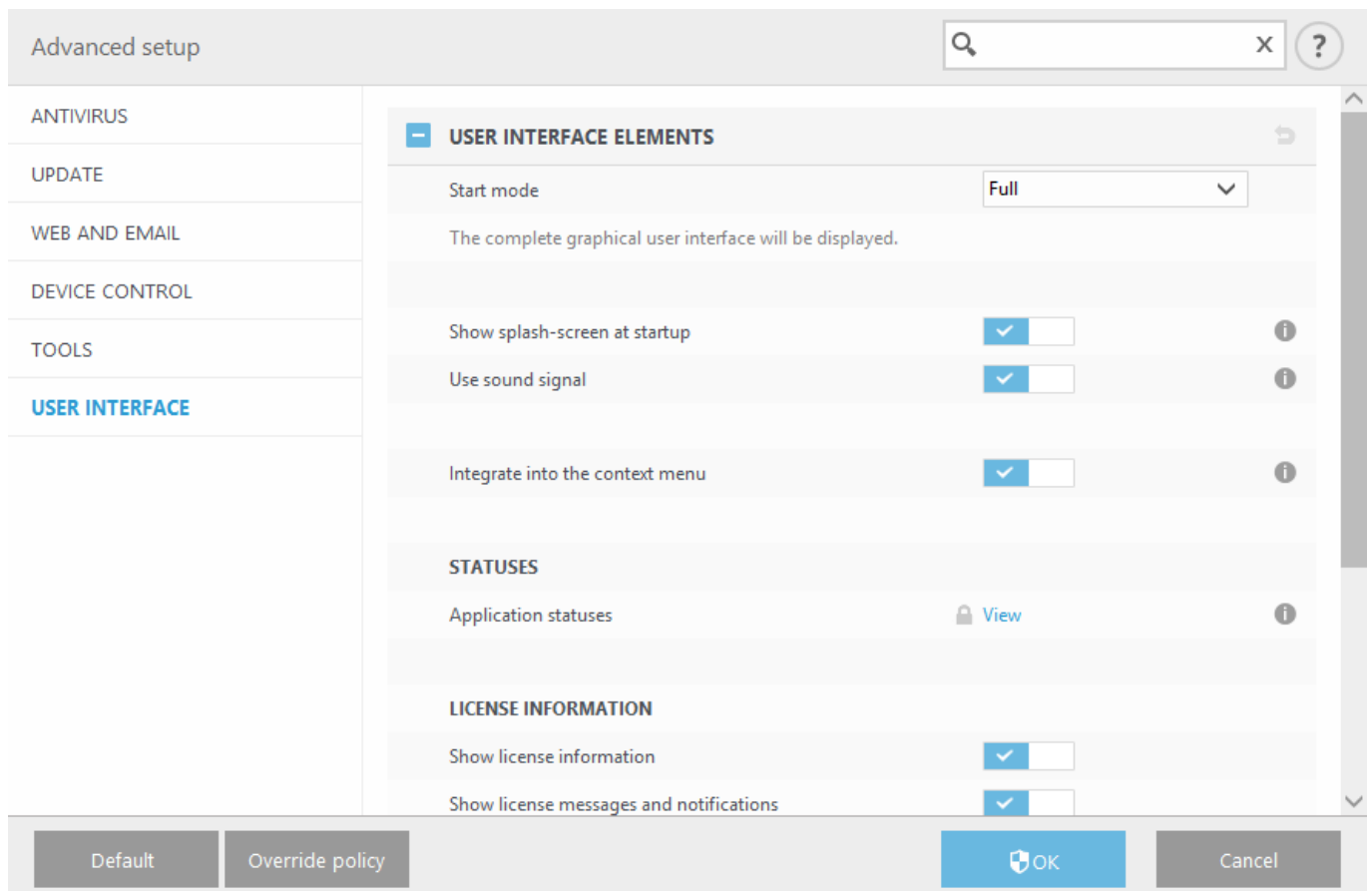


通常ESET PROTECTポリシー経由で構成された設定は修正できません。上書きモードでは、これらの設定を一時的にロック解除できます。ただしESET PROTECTポリシーを使用して上書きモードを有効にする必要があります。

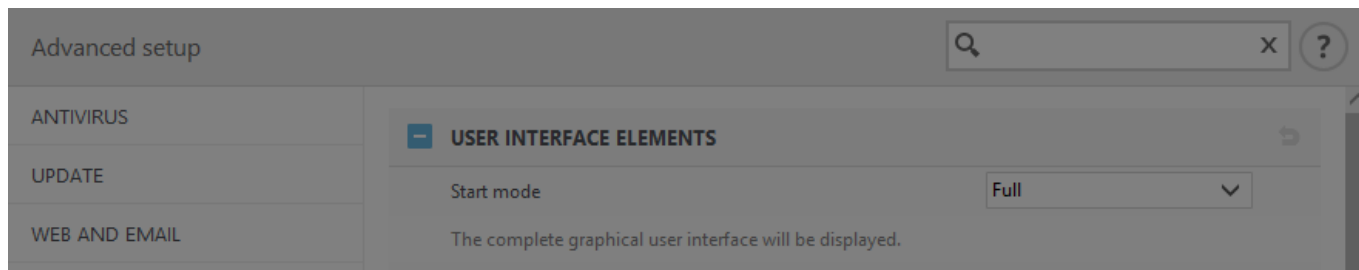
[ESET PROTECT Webコンソール](#) にログインし、[ポリシー]に移動してESET Server Securityに適用される既存のポリシーを選択して編集するか、新しく作成します。[設定]で、[上書きモード]をクリックし、有効にして、認証タイプ (**Active directory**ユーザーまたはパスワード)を含む設定の残りを設定します。



ポリシーが修正されたか、新しいポリシーがESET Server Securityに適用されたら、[ポリシーの無効化]ボタンが[詳細設定]ウィンドウに表示されます。



[ポリシーの無効化]ボタンをクリックし、期間を設定して、[適用]をクリックします。



Temporary policy override

Set the duration for which the policy settings can be overridden. After this duration the configuration will revert to the policy.

Override duration

4 hours ▼

10 min

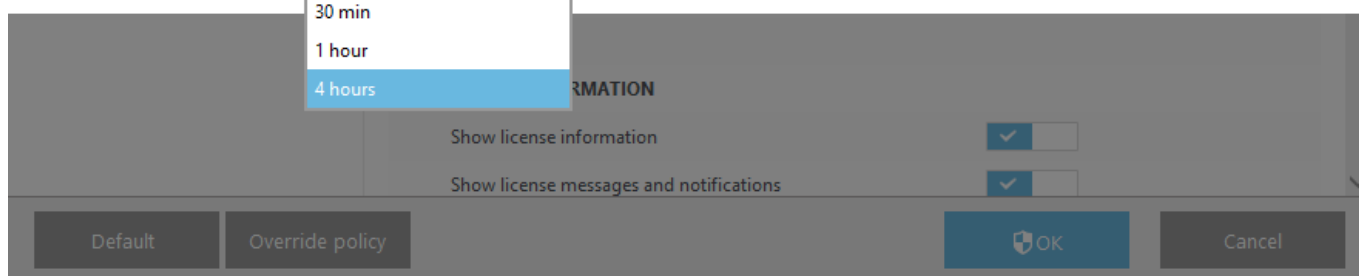
30 min

1 hour

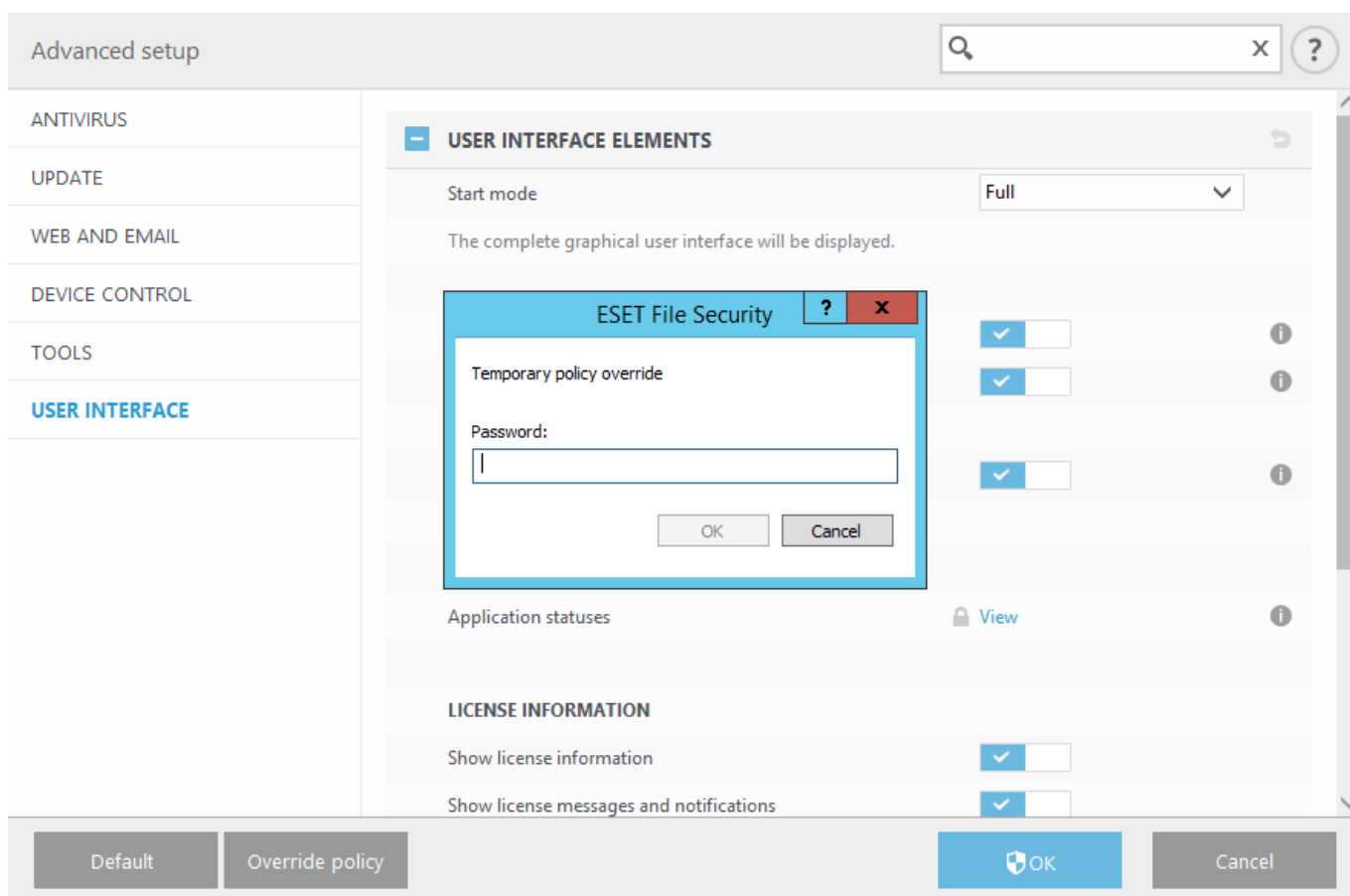
4 hours

Apply

Cancel



認証タイプとしてパスワードを選択した場合は、ポリシー上書きパスワードを入力します。



上書きモードが終了したら、行ったすべて設定変更が元のESET PROTECTポリシー設定に戻ります。上書きが終了する前に通知が表示されます。

[監視ページ](#)または[詳細設定](#)ウィンドウで期限切れになる前に、**上書きモードを終了**できます。

ログファイル

このセクションではESET Server Securityログギングの構成を修正できます。

☐ [ログフィルタ](#)

大量のデータを生成します。すべてのログオプションが既定で有効になっているためです。有用性が低いコンポーネントや問題に関係ないコンポーネントのログを選択して無効にすることをお勧めします。

注意

実際のログギングを開始するには、メインメニューの[設定]>[\[ツール\]](#)で、製品レベルで一般的な**診断ログギング**を有効にする必要があります。ログギング自体をオンにするとESET Server Securityはこのセクションで有効な機能に従い詳細ログを収集します。

スイッチを使用して、特定の機能を有効または無効にできます。このオプションは、ESET Server Securityの個別のコンポーネントの可用性によっては、組み合わせることもできます。

- **[クラスタ診断ログギング]** – クラスタログギングは、一般的な診断ログに含まれます。

☐ [ログファイル](#)

ログの管理方法を定義します。これは、過剰なディスクの使用を防止するのに最も重要です。既定の設定では、ディスクの容量を節約するために、古いログは自動的に削除されます。

次の日数が経過したエントリを自動的に削除する

指定された日数を経過したログエントリは自動的に削除されます。

ログサイズが超過した場合は古いレコードを自動的に削除

ログファイルサイズが**[最大ログサイズ [MB]]**を超過すると、**[縮小されたログサイズ [MB]]**になるまで古いログレコードが削除されます。

自動的に削除されたレコードをバックアップ

自動的に削除されたログレコードとファイルは指定されたディレクトリにバックアップされ、任意でZIPファイルに圧縮されます。

診断ログをバックアップ

削除された診断ログを自動的にバックアップします。有効ではない場合、診断ログレコードはバックアップされません。

バックアップフォルダ

ログバックアップが保存されるフォルダZIPを使用して圧縮されたログバックアップを有効にできます。

ログファイルを自動的に最適化する

有効にすると、断片化の割合が**使用されていないレコードの割合(%)**が次の値よりも大きく場合フィールドの値を超えた場合に、ログファイルは自動的にデフラグされます。**[最適化]**をクリックすると、ログファイルの最適化が開始します。すべての空のログエントリが削除され、パフォーマンスとログ処理速度が改善します。この向上は、特にログに多数のエントリが含まれている場合に顕著に見られます。

テキスト方式を有効にする

[ログファイル](#)とは別のファイル形式でログを保存できます。

- **ターゲットディレクトリ** - ログファイルが保存されるディレクトリ(テキスト/CSVのみ)。各ログセクションには定義済みのファイル名を使用した独自のファイル(例: プレーンテキストファイル形式でログを保存する場合は、ログファイルの検出された脅威セクションは *virlog.txt*)があります。
- **種類** - テキストファイル形式を選択する場合は、ログがテキストファイルに保存されます。データはタブ区切りです。同じことがカンマ区切りの**CSV**ファイル形式にも当てはまります。イベントを選択すると、ファイルではなく**Windows**イベントログに、ログが保存されます(コントロールパネルのイベントビューアで表示できます)。
- **すべてのログファイルを削除** - **[種類]** ドロップダウンメニューで現在選択されているすべての保存済みログが消去されます。

注意

ESETテクニカルサポートが問題をより迅速に解決できるように、コンピュータからログを提供するように依頼される場合があります。[ESET Log Collector](#)を使用すると、必要な情報を簡単に収集できます。ESET Log Collectorの詳細については、[ナレッジベース記事](#)を参照してください。

監査ログ

構成または保護の変更を追跡します。製品構成の修正は、製品の動作に大きく影響する可能性があるため、監査目的で変更の追跡が必要になることがあります。**ログファイル > [監査ログ](#)** セクションには、変更のログレコードが表示されます。

プロキシサーバ

大規模なLANネットワークでは、コンピュータがプロキシサーバを介してインターネットに接続されている場合があります。この場合は、次の設定を定義する必要があります。定義しなかった場合、プログラムは自動的に更新されません。ESET Server Securityでは、**[詳細設定]** ウィンドウ (**F5**) の2つのセクションでプロキシサーバを設定できます。

1. **詳細設定 (F5) > アップデート > プロファイル > アップデート > 接続オプション > [HTTPプロキシ](#)**
この設定は、特定のアップデートプロファイルに適用されます。モジュールをさまざまな場所から受信するノート型コンピューターにお勧めします。
2. **詳細設定 (F5) > ツール > プロキシサーバ**
プロキシサーバをこのレベルで指定するとESET Server Securityの全ての全体的なプロキシサーバ設定が指定されることになります。ここで設定するパラメータは、インターネットへ接続する全てのモジュールで使用されます。

プロキシサーバ設定をこのレベルで指定するには、**[プロキシサーバを使用する]** チェックボックスを選択し、プロキシサーバのアドレスを**[プロキシサーバ]** フィールドに入力し、プロキシサーバの**[ポート]** 番号を指定します。

プロキシサーバは認証が必要

プロキシサーバ経由のネットワーク通信で認証が必要な場合は、このオプションを有効にし、ユーザー名とパスワードを指定します。

プロキシサーバの検出

[検出]をクリックすると、自動的にプロキシサーバの設定が検出されて取り込まれます。Internet Explorerで指定したパラメータがコピーされます。

注意

この機能では、認証データ(ユーザー名とパスワード)は取り出されないため、ユーザーが入力する必要があります。

プロキシが使用できない場合は直接接続を使用する

製品がHTTPプロキシを使用するように構成され、プロキシに接続できない場合は、プロキシをバイパスし、直接ESETサーバーと通信します。

通知

デスクトップ通知とバルーンヒントに表示される情報は情報を提供するのみのもので、ユーザー操作は不要です。これらは、画面の右下にある通知領域に表示されます。次のように、通知の表示時間やウィンドウの透明度などの詳細なオプションを変更することができます。[アプリケーションを全画面モードで実行中に、通知を表示しない]をオンにすると、すべての非対話通知を抑制します。

成功したアップデートについての通知を表示する

アップデートが成功すると、ポップアップ通知が表示されます。

イベント通知をメールで送信する

電子メール通知を有効にします。

アプリケーション通知

[編集](#)をクリックすると、表示アプリケーション通知を有効または無効にできます。

アプリケーション通知

デスクトップに表示したり、電子メールで送信されるESET Server Security通知を設定できます。

注意

電子メール通知の場合は、**基本セクションの電子メールでイベント通知を送信**を有効にしたことを確認してから、[SMTPサーバー](#)と必要に応じて他の詳細情報を設定します。



デスクトップ通知

脅威アラートとシステム通知(成功したアップデートメッセージ)がESET Server Securityによって処理される方法を設定できます。たとえば、表示時間の**期間**とシステムトレイ通知**透明度**を設定できます(これは、システムトレイ通知をサポートするシステムにのみ適用されます)。

[表示イベントの最低詳細レベル] ドロップダウンメニューからは、警告および通知を表示する最初の重大度レベルを選択できます。使用可能なオプションは次のとおりです。

- **診断** - プログラムおよび上記のすべてのレコードを微調整するのに必要な情報をログに記録します。
- **情報** - アップデートの成功メッセージを含むすべての情報メッセージと上記のすべてのレコードを記録します。
- **警告** - 重大なエラー、エラー、および警告メッセージを記録します。
- **エラー** - 「ファイルのダウンロード中にエラーが発生しました」といったエラーや重大なエラーを記録します。
- **重大** - 重大なエラーのみをログに記録します。

[マルチユーザーシステムの場合、以下のユーザーの画面に通知を表示する] フィールドでは、複数のユーザーが同時に接続できるシステムで、システム通知やその他の通知を受け取るユーザーを指定します。通常は、システム管理者またはネットワーク管理者です。このオプションは、全てのシステム通知が管理者に送信される場合、ターミナルサーバーに特に便利です。

電子メール通知

ESET Server Securityは、選択されている詳細レベルのイベントの発生時に、自動的に通知メールを送信できます。

注意

TLS暗号化機能を備えたSMTPサーバーは、ESET Server Securityでサポートされます。

SMTPサーバー

アラートと通知の送信で使用するSMTPサーバーの名前。一般的には「Microsoft Exchange Server」の名前です。

ユーザー名とパスワード

SMTPサーバで認証を要求する場合、有効なユーザー名とパスワードをフィールドに入力して「SMTPサーバへのアクセスを許可する必要があります。

送信元アドレス

通知電子メールのヘッダーに表示される送信者のアドレスを入力します。これは受信者側の**From**フィールドに表示されます。

受信者アドレス

通知が送信される受信者の電子メールアドレス**To**を指定します。

TLSを有効にする

TLS暗号化でサポートされる警告と通知メッセージを有効にします。

電子メール設定

通知の最低レベル

送信する通知の最低詳細レベルを指定します。

新しい通知メールが送信される間隔(分)

新しい通知が電子メールに送信されるまでの間隔(分)。通知をただちに送信する場合は、この値を0に設定します。

各通知を別のメールで送信

有効にすると、受信者は、各個別の通知に関する新しい電子メールを受信します。このため、短期間で大量の電子メールを受信する場合があります。

メッセージの書式

プログラムとリモートユーザーまたはシステム管理者間の通信は、メールまたはLANメッセージ(Windowsメッセージングサービスを使用)によって行われます。警告メッセージおよび通知の既定のフォーマットは、ほとんどの状況に適しています。ただし、場合によっては、イベントメッセージのフォーマットを変更しなければならないことがあります。

イベントメッセージの書式

リモートコンピュータで表示されるイベントメッセージの形式。

脅威警告メッセージの書式

脅威警告と通知メッセージには定義済みの既定の形式があります。この書式は変更しないようお勧めします。ただし、状況によっては(自動メール処理システムを使用している場合など)、メッセージの書式を変更しなければならないことがあります。

メッセージでは、指定されている実際の情報でキーワード(%記号で区切られた文字列)が置き換えられます。使用可能なキーワードは次のとおりです。

- **%TimeStamp%** - イベントの日時
- **%Scanner%** - 関連するモジュール
- **%ComputerName%** - 警告が発生したコンピュータの名前
- **%ProgramName%** - 警告を生成したプログラム
- **%InfectedObject%** - 感染しているファイルやメールなどの名前
- **%VirusName%** - ウイルスのID
- **%ErrorDescription%** - ウイルス以外のイベントの説明

キーワード**%InfectedObject%**および**%VirusName%**はマルウェア警告メッセージのみで使用され、**%ErrorDescription%**はイベントメッセージのみで使用されます。

文字セット

ドロップダウンメニューからエンコーディングを選択できます。電子メールメッセージは、選択した文字エンコーディングに従って変換されます。

Quoted-printableエンコーディングを使用

電子メールメッセージのソースはQuoted-printable (QP)書式でエンコードされます。この書式は、ASCII文字を使用し、特殊な各国語文字を8ビット書式(áéíóú)の電子メールで正確に送信できます。

カスタマイズ

このメッセージはすべての選択された通知のフッターに表示されます。

既定の通知メッセージ

通知のフッターに表示される既定のメッセージ。

脅威

マルウェア通知を自動的に閉じない

手動で閉じるまで、マルウェア通知を画面に表示し続けることができます。

既定のメッセージを使用

既定のメッセージをオフにし、脅威がブロックされたときに表示されるカスタム通知メッセージの処理を指定できます。

脅威通知メッセージ

脅威がブロックされたときに表示するカスタムメッセージを入力します。

プレゼンテーションモード

プレゼンテーションモードは、ソフトウェアを中断なしに使用できることを要望し、ポップアップウィンドウの邪魔が入ることを望まずCPUの使用量を最小化したいと思っているユーザー向けの機能です。プレゼンテーションモードは、ESET Server Securityのアクティビティによって中断されてはならないプレゼンテーション中に使用することもできます。有効にすると、すべてのポップアップウィンドウが無効になり、スケジュールされたタスクは実行されません。システムの保護は引き続きバックグラウンドで実行されますが、ユーザーの操作を必要としません。

全画面モードでのアプリケーションの実行中に自動的にプレゼンテーションモードを有効にする

全画面アプリケーションを実行するたびに、プレゼンテーションモードが自動的に有効になります。プレゼンテーションモードの実行中にはESET Server Securityの通知または[ステータス変更](#)は表示されません。

次の時間が経過した後にプレゼンテーションモードを自動的に無効にする

プレゼンテーションモードが自動的に無効になる時間を分で定義できます。

診断

診断はESETプロセスのアプリケーションクラッシュダンプ(*ekrn*など)を提供します。アプリケーションがクラッシュすると、ダンプが生成されます。これを使用して、開発者は各種ESET Server Securityの問題をデバッグおよび修正できます。

ダンプタイプの横のドロップダウンメニューをクリックし、3つの使用可能なオプションのいずれかを選択します。

- **無効** – この機能を無効にします。
- **ミニダンプ** – (既定)アプリケーションが不意にクラッシュした理由を特定する助けとなる最低限の有用な情報が記録されます。容量が限られているときは、この種のダンプファイルは便利です。しかし、収容できる情報が限られるため、問題の発生時に実行されていたスレッドがエラーの直接の原因ではない場合、ファイルを解析しても原因を判別できない場合があります。
- **完全** – アプリケーションが不意に停止した場合に、システムメモリの全内容が記録されます。完全なメモリーダンプには、メモリーダンプが収集されたときに実行されていたプロセスのデータが含まれます。

保存先のフォルダ

クラッシュ時、ダンプが作成されるディレクトリです。

ダンプファイルの保存フォルダを開く

このディレクトリを新しい *Windows Explorer* ウィンドウで開く場合は、**[開く]** をクリックします。

診断ダンプの作成

作成 をクリックして、ターゲットディレクトリに診断ダンプファイルを作成します。

☐ [詳細ログ](#)

デバイスコントロール詳細ロギングを有効にする

デバイスコントロールで発生するすべてのイベントを記録し、診断と問題解決ができます。

カーネル詳細ログを有効にする

ESETカーネルサービス(ekrn)で発生するすべてのイベントを記録し、診断と問題の解決を可能にします。

ライセンス詳細ロギングを有効にする

ライセンスサーバーとのすべての通信を記録します。

ネットワーク保護詳細ロギングを有効にする

PCAP形式でネットワーク保護経由のすべてのネットワークデータ転送を記録します。これによって、開発者はネットワーク保護関連の問題を診断および修正できます。

オペレーティングシステム詳細ログを有効にする

実行中のプロセス、CPUアクティビティ、ディスク処理などのオペレーティングシステムに関する追加情報が収集されます。

プロトコルフィルタリング詳細ロギングを有効にする

PCAP形式でプロトコルフィルタリング経由のすべてのプロトコルフィルタリングデータ転送を記録します。これによって、開発者はプロトコルフィルタリング関連の問題を診断および修正できます。

アップデートエンジン詳細ロギングを有効にする

アップデート処理中に発生するすべてのイベントを記録します。これにより、開発者はアップデートエンジンに関連する問題を診断および修正できます。

テクニカルサポート

システム構成データの送信

常に送信を選択すると、ESET Server Security設定データをカスタマーサポートに送信する前に確認しません。あるいは、送信前に確認するを使用します。

クラスタ

[クラスタを有効にする]は、ESET Clusterが構成されるときに自動的に有効になります。詳細設定(F5)ウィンドウでスイッチアイコンをクリックして手動で無効にすることができます(ESET Cluster内の他のノードに影響を与えずに構成を変更する必要がある場合など)。このスイッチはESET Cluster機能を有効または無効にするのみになります。クラスタを設定または無効にするには、ツール >メインプログラムウィンドウの[クラスタ]セクションにある[クラスタウィザード](#)または[無効化]を使用します。

ESET Clusterが構成されておらず無効です。

Advanced setup Q X ?

SERVER1

COMPUTER

UPDATE

WEB AND EMAIL

DEVICE CONTROL1

TOOLS

Log files

Proxy server

Email notifications1

Presentation mode

Diagnostics

Cluster

USER INTERFACE

CLUSTER

Settings below are enabled only when the cluster is active.

Open port in Windows firewall ✓ i

Status refresh interval [sec] 10 i

Synchronize product settings ✓ i

CONFIGURATION INFORMATION

Settings below can be changed by the cluster wizard only.

Cluster name

Listening port 9777

List of cluster nodes

Default

OK

Cancel

ESET Clusterが詳細とオプションで正しく構成されています。

Advanced setup Q X ?

SERVER

COMPUTER

UPDATE

WEB AND EMAIL

DEVICE CONTROL

TOOLS

Log files

Proxy server

Email notifications

Presentation mode

Diagnostics

Cluster

USER INTERFACE

CLUSTER

Settings below are enabled only when the cluster is active.

Open port in Windows firewall ✓ i

Status refresh interval [sec] 10 i

Synchronize product settings ✓ i

CONFIGURATION INFORMATION

Settings below can be changed by the cluster wizard only.

Cluster name termix

Listening port 9777

List of cluster nodes W2012R2-NODE1;W2012R2-NODE2;W2012R2-NODE3;WIN-JDLB8CEUR5

Default

OK

Cancel

ユーザーインターフェース

ESET Server Securityのグラフィカルユーザーインターフェース(GUI)の動作を設定できます。プログラムの視覚表示と効果を調整できます。

☐ [ユーザーインターフェース要素](#)

[GUI起動モード] ドロップダウンメニューを使用して、次のGUI起動モードを選択します。

- **完全** – 完全なGUIが表示されます。
- **ターミナル** – 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。グラフィカル要素によってコンピュータのパフォーマンスが低下したり、別の問題が発生したりする場合は、ユーザーインターフェイスをターミナルに設定してください。ターミナルサーバーでGUIをオフにすることもできます。ターミナルサーバーにインストールされたESET Server Securityの詳細については、「[ターミナルサーバーでのGUIの無効化](#)」トピックを参照してください。

起動時にスプラッシュ画面を表示する

システムへのログイン時などESET Server SecurityのGUIが起動するときに、スプラッシュ画面を表示しない場合は、このオプションを無効にします。


サウンドシグナルを使用する

スキャン中に脅威が発見されたりスキャンが終了したなどの重要なイベントが発生したときESET Server Securityがサウンドを再生するようにするには、これを選択します。

コンテキストメニューに統合する

有効にするとESET Server Securityコントロール要素は、コンテキストメニューに統合されます。オブジェクト(ファイル)を右クリックすると、コンテキストメニューが表示されます。このメニューには、オブジェクトに対して実行できるすべてのアクションが一覧表示されます。

アプリケーションステータス

[編集](#)をクリックすると、[監視](#)ウィンドウに表示されるステータスを選択します。あるいは、[ESET PROTECTポリシー](#) を使用して、アプリケーションステータスを設定できます。アプリケーションステータスは、製品がアクティベーションされていないか、ライセンスが期限切れの場合にも表示されます。

ライセンス情報/ライセンス情報を表示する

有効にすると、ライセンスに関するメッセージと通知が表示されます。

[アラートとメッセージボックス](#)

[警告と通知]の設定により、検出されたマルウェアについての警告およびシステム通知の動作を変更できます。これらは、ご自身のニーズに合わせてカスタマイズできます。一部の通知を表示しないように選択した場合、これらの通知は「[無効にされたメッセージとステータス](#)」領域に表示されます。ここでは、ステータスの確認、詳細の表示、またはこのウィンドウからの詳細の削除を実行できます。

[アクセス設定](#)

アクセス設定ツールを使用して権限がない変更を防止し、高いセキュリティを保証します。

ESET Shell

eShellを使用して、製品設定、機能、データへのアクセス権を設定するにはESETシェル実行ポリシーを変更します。

システムトレイアイコン

[このセクションのすべての設定を元に戻す](#)

アラートとメッセージボックス

脅威アラートとシステム通知(成功したアップデートメッセージ)がESET Server Securityによって処理される方法を設定できます。たとえば、表示時間の**期間**とシステムトレイ通知**透明度**を設定できます(これは、システムトレイ通知をサポートするシステムにのみ適用されます)。

対話アラートを表示

Windows通知領域にESET Server Securityのアラートを表示しない場合は、この機能を無効にします。

対話アラートのリスト

自動化に役立ちます。自動化する項目の**ユーザーに確認**をオフにし、アラートウィンドウで操作を待機するかわりに実行するアクションを選択します。

メッセージボックスは、短いテキストメッセージや質問を表示する場合に使用されます。

メッセージボックスを自動的に閉じる

特定の時間が経過した後で自動的にポップアップウィンドウを閉じます。警告ウィンドウを手動で閉じないと、指定した時間が経過すると、ウィンドウは自動的に閉じられます。

確認メッセージ

編集をクリックすると、ポップアップウィンドウが開き、アクションが実行される前に、ESET Server Securityで表示される確認メッセージの一覧が表示されます。チェックボックスを使用して、確認メッセージの設定をカスタマイズできます。

アクセス設定

システムの最大のセキュリティのためESET Server Securityが正しく設定されていることは基本です。許可のない修正を行うと、問題が生じたり、重要なデータが失われるおそれがあります。許可のない修正を回避するためにESET Server Security設定をパスワードで保護できます。

重要

設定へのアクセスをパスワードで保護しているときにESET Server Securityをアンインストールする場合は、パスワードを入力する必要があります。入力しないとESET Server Securityをアンインストールできません。

設定をパスワードで保護する

プログラムの設定パラメーターをロック/ロック解除します。クリックすると、**パスワード設定**ウィ

ンドウが開きます。

パスワードの設定

パスワードを設定または変更して設定パラメーターを保護するには、[パスワードの設定]をクリックします。ESET Server Securityの設定パラメータを保護し、不正な修正を防止するには、新しいパスワードを設定する必要があります。既存のパスワードを変更するときには、[古いパスワード]フィールドに古いパスワードを入力し、[新しいパスワード]フィールドと[パスワードの確認]フィールドに新しいパスワードを入力して、[OK]をクリックします。このパスワードは今後ESET Server Securityを変更する場合に必要になります。

制限された管理者アカウントの場合、完全な管理者権限が必要

このオプションを選択すると、保護モジュールの無効化など、特定のシステムパラメータの変更時に、管理者アカウントの資格情報を入力するように現在のユーザーに求めます。

注意

アクセス設定パスワードを変更し、ESET CMD コマンドラインを使用して既存の.xml設定ファイル(パスワード変更前に署名)をインポートする場合は、必ず現在のパスワードでもう一度サインインします。これにより、インポート前にESET Server Securityを実行する他のコンピューターでエクスポートせずに、古い設定ファイルを使用できます。

ESET Shell

eShellを使用して、製品設定、機能、データへのアクセス権を設定するには、ESETシェル実行ポリシーを変更します。既定の設定は[制限されたスクリプト]ですが、必要に応じて、無効、読み取り専用、またはフルアクセスに制限できます。

無効

eShellはまったく使用できません。eShellの構成は、ui eshellコンテキストでだけ許可されます。eShellの表示はカスタマイズできますが、製品の設定またはデータにはアクセスできません。

読み取り専用

eShellは監視ツールとして使用できます。インタラクティブモードとバッチモードの両方ですべての設定を表示できますが、設定、機能、またはデータは修正できません。

制限されたスクリプト

インタラクティブモードでは、すべての設定、機能、およびデータを表示して修正できます。バッチモードではeShellは、読み取り専用モードのように動作しますが、署名済みバッチファイルを使用する場合は、設定を編集してデータを修正できます。

フルアクセス

インタラクティブモードとバッチモードの両方で、すべての設定に無制限にアクセスできます(バッチファイルを実行するとき)。すべての設定を表示して修正できます。フルアクセスでeShellを実行するには、管理者アカウントを使用する必要があります。UACが有効な場合、昇格も必要です。

ターミナルサーバでのGUIの無効化

この章ではWindowsターミナルサーバで稼動しているESET Server SecurityのGUIを、ユーザーセッションで無効にする方法を説明します。

通常ESET Server SecurityのGUIは、リモートユーザーがサーバにログオンして、端末セッションを作成するたびに開始されます。ターミナルサーバでは、この動作は一般に望ましくありません。ターミナルセッションのGUIをオフにする場合は、[eShell](#)で`set ui ui gui-start-mode none`コマンドを実行します。これによりGUIがターミナルモードになります。GUIスタートアップでは2つのモードがあります。

```
set ui ui gui-start-mode full
set ui ui gui-start-mode none
```

現在のモードを確認するには、`get ui ui gui-start-mode`コマンドを実行します。

注意

CitrixサーバーにESET Server Securityをインストールしている場合は、[ナレッジベース記事](#) の設定を使用することをお勧めします。

無効にされたメッセージとステータス

確認メッセージ

表示または非表示にする確認メッセージを選択できるリストが表示されます。

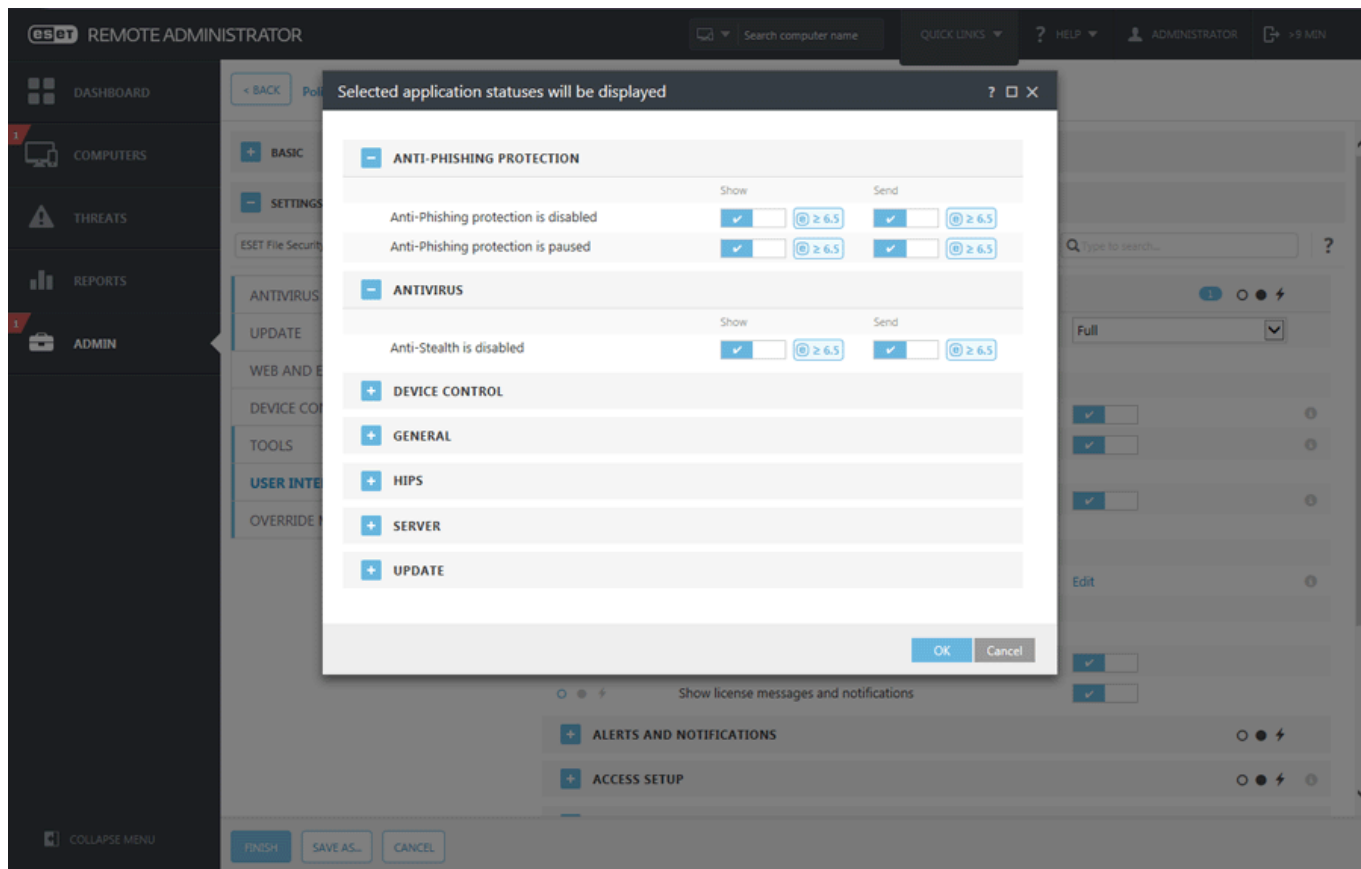
アプリケーションステータス設定

メインメニューの[監視](#)ページで表示ステータスを有効または無効にできます。


アプリケーションステータス設定

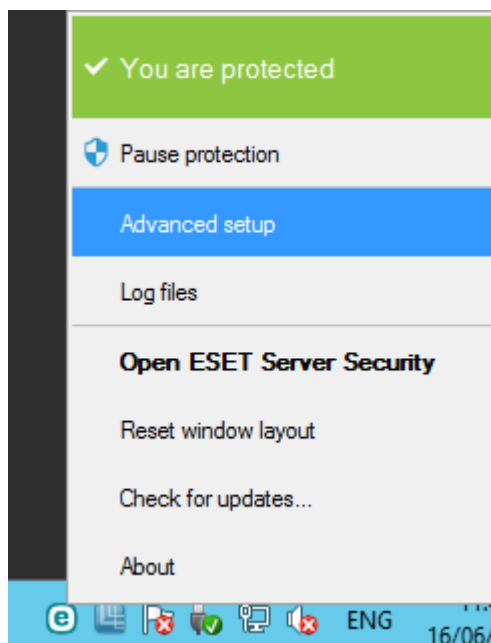
このダイアログウィンドウでは、表示または非表示にするアプリケーションステータスを選択または選択解除できます。たとえば、ウイルス対策およびスパイウェア対策保護を一時停止すると、保護ステータスが変わり、[監視](#)ページに表示されます。また、保護が有効ではない場合や、ライセンスが期限切れの場合にも、アプリケーションステータスが表示されます。

アプリケーションステータスは、[ESET PROTECTポリシー](#) から管理できます。カテゴリとステータスは、2つのオプション**表示**と**送信**ステータスとともにリストに表示されます。アプリケーションステータスの送信裂は、[ESET PROTECTポリシー](#) 設定にのみ表示されます。ESET Server Securityには設定とロックアイコンが表示されます。[上書きモード](#)を使用して、一時的にアプリケーションステータスを変更できます。



システムトレイアイコン


ESET Server Securityの頻繁に使用される項目と機能へのクイックアクセスを提供します。最も重要な設定オプションと機能の一部は、システムトレイアイコンを右クリックすると使用できます。



詳細情報

[監視](#) ページを開き、現在の保護ステータスとメッセージを表示します。

保護を一時停止

ファイルWebおよびメール通信を制御することによって攻撃から保護する、[ウイルス・スパイウェア対策](#)を無効にするための確認ダイアログボックスを表示します。システムトレイアイコンを使用して、ウイルス対策とスパイウェア対策を一時的に無効にするたびに[保護を無効にする]ダイアログボックスが表示されます。これで、選択した期間の間マルウェア関連保護を無効にします(保護を永久に無効にするには、[詳細設定](#)を使用する必要があります)。使用するときには注意してください。保護を無効にすると、システムが脅威にさらされる可能性があります。

詳細設定

このオプションを使用して、[詳細設定](#)を入力します。

ログファイル

発生したすべての重要なプログラムイベントに関する情報が格納され、検出されたマルウェアの概要が表示されます。

ESET Server Securityを非表示にする

画面にESET Server Securityウィンドウを表示しません。

ウィンドウレイアウトのリセット

ESET Server Securityのウィンドウを既定のサイズと画面上の位置にリセットします。

アップデートのチェック

モジュールのアップデートを開始し、悪意のあるコードに対する保護レベルを保証します。

バージョン情報

システム情報、インストールされているESET Server Securityのバージョンに関する詳細、インストールされているプログラムモジュール、およびライセンスの有効期限が表示されます。オペレーティングシステムとシステムリソース情報は、ページの下部に表示されます。

デフォルト設定に戻す

[詳細設定](#)で、設定を既定値に復元できます。2つのオプションがあります。すべてを既定値に戻すか、特定のセクションの設定のみを戻すことができます(他のセクションの設定は変更されません)。

すべての設定に戻す

詳細設定のすべてのセクションのすべての設定が、ESET Server Securityをインストールした後の状態に戻されます。出荷時既定値のリセットと考えることができます。

注意

既定値に戻すをクリックすると、すべての変更が失われます。このアクションは元に戻せません。

このセクションのすべての設定を元に戻す

選択したセクションのモジュール設定を値に戻します。このセクションのすべての変更は失われます。



テーブルの内容を戻す

有効にすると、手動または自動で追加されたルール、タスク、プロファイルが失われます。

ヘルプとサポート

ESET Server Securityには、トラブルシューティングツール、および発生する可能性のある問題の解決に役立つサポート情報が含まれています。

ヘルプ

[ESETナレッジベースの検索](#)

ESETナレッジベースには、最もよくある質問への回答や、さまざまな問題に対する一般的な解決策が登録されています。ESETのテクニカルスペシャリストが定期的に更新しているので、このナレッジベースは、さまざまな種類の問題を解決するための最も強力なツールです。

ヘルプを開く

ESET Server Securityのオンラインヘルプページを起動します。

[解決方法を探す](#)

最もよくある問題の解決策を見つけるには、これを選択します。テクニカルサポートにお問い合わせいただく前に、このセクションを確認することをお勧めします。

テクニカルサポート

[サポート要求の送信](#)

問題の回答を見つけれなかった場合、お問い合わせから当社のテクニカルサポート部門に速やかに連絡することもできます。

[テクニカルサポート詳細](#)

テクニカルサポート用の詳細情報(製品名、製品バージョンなど)を表示します。

サポートツール

[脅威情報](#)

さまざまなタイプのマルウェアの危険と徴候に関する情報を含むESETの脅威に関する情報へのリンクです。

[ESET Log Collector](#)

ESET Log Collector[ダウンロードページ](#)へのリンクESET Log Collectorは、問題をより迅速に解決するために構成やログなどの情報およびログをサーバーから自動的に収集するアプリケーションです。

[検出エンジンの更新履歴](#)

ESETウイルスレーダーへのリンクESET検出モジュールのバージョン情報が含まれます。

[ESET Specialized Cleaner](#)

ESET専用駆除アプリケーションは、ConfickerSirefefNecursなどの一般的なマルウェア感染を駆除するツールです。

製品およびライセンス情報

[製品のアクティベーション / ライセンスの変更](#)

製品のアクティベーションウィンドウを起動するをクリックしますESET Server Securityのアクティベーションで使用可能な方法のいずれかを選択します。

[ESET Server Securityについて](#)

ESET Server Securityのコピーに関する情報が表示されます。

サポート要求の送信

できるかぎり迅速かつ正確にサポートを提供するためにESETは、ESET Server Security構成、詳細なシステム情報、実行中のプロセス([ESET SysInspector ログファイル](#))、およびレジストリデータに関する情報を必要としています。このデータを使用する目的は、お客様に技術するサポートを提供することだけです。この設定は、**詳細設定 (F5) > ツール > 診断 > テクニカルサポート**で設定することもできます。

注意

システムデータを送信する場合は、Webフォームを入力して送信する必要があります。それ以外の場合は、チケットが作成されず、システムデータは失われます。

Webフォームを送信すると、システム構成データもESETに送信されます。この処理を記憶する場合は、**[常にこの情報を送信]**を選択します。

[データを送信しない](#)

データを送信せずにフォームを送信する場合は、このオプションを使用しますESETテクニカルサポートWebページに移動します。

ESET Server Securityについて

このウィンドウには、インストールされたESET Server Securityのバージョンの詳細情報が表示されます。ウィンドウの上部には、オペレーティングシステムおよびシステムリソースと、現在のユーザーおよび完全なコンピューター名の情報が表示されます。

インストールされたコンポーネント

モジュールの情報が表示され、インストールされたコンポーネントのリストと詳細が表示されます。[コピー]をクリックすると、リストをクリップボードにコピーします。この機能は、トラブルシューティングを行う場合、またはテクニカルサポートに問い合わせる場合に便利です。

用語集

技術用語、脅威、およびインターネットセキュリティの詳細については、[用語集](#)をご覧ください。

エンドユーザーライセンス契約

重要:ダウンロード、インストール、コピー、または使用の前に、製品利用に関する下記契約条件を注意してお読みください。本製品をダウンロード、インストール、コピー、または使用することにより、お客様はこれらの条件に対する同意を表明し、次の項目に同意したことになります[プライバシーポリシー](#)

エンドユーザー使用許諾契約

本エンドユーザーライセンス契約（以下「本契約」とします）はEinsteinova 24, 85101 Bratislava, Slovak Republicに所在し、ブラチスラバ第1地方裁判所の有限会社部門District Court Bratislava I. Section Sroにおいて掲載番号3586/B, 31333532として商業登記されているESET, spol. s r. o.またはESETグループ内の別企業（以下ESETまたは「供給者」とします）と、自然人または法人であるお客様（以下「お客様」または「エンドユーザー」とします）との間で締結され、お客様に本契約の第1条で定義する本ソフトウェアを使用する権利を付与するものです。本契約の第1条で定義する本ソフトウェアは、データ記憶媒体への格納、電子メールでの送付、インターネットからのダウンロード、供給者のサーバーからのダウンロード、または後述の条件および状況下におけるその他の供給者からの取得が行えます。

本契約は購入に関する契約ではなく、エンドユーザーの権利に関する合意事項を定めるものです。供給者は、本ソフトウェアのコピー、これが商業包装にて供給される物理的媒体、および本契約に基づきエンドユーザーが権利を付与される本ソフトウェアのすべてのコピーの、所有者であり続けます。

本ソフトウェアのインストール時、ダウンロード時、コピー時または使用時に、[同意します]オプションをクリックすることにより、本契約の条件に明示的に同意するものとします。本契約の規定に同意しない場合は、直ちに[同意しない]オプションをクリックし、インストールまたはダウンロードを取り消すか、本ソフトウェア、インストールメディア、付属ドキュメント、および購入時の領収書を破棄するかESETまたは本ソフトウェアの入手元にそれを返却してください。

お客様は、本ソフトウェアを使用することにより、お客様が本契約を読了かつ理解し、本契約条項による拘束に同意したことになります。

1.ソフトウェア。(i) 本契約およびすべてのコンポーネントに付属するコンピュータープログラム(ii) データ媒体、電子メール、またはインターネット経由でのダウンロードで提供される本ソフトウェアのオブジェクトコードの形式を含む、本契約で提供されるディスクCD-ROMDVD電子メール、添付ファイル、その他の媒体のすべての内容(iii) 本ソフトウェアに関連する書面の説明資料、その他の文書、特に本ソフトウェア、その仕様のすべての説明、本ソフトウェアの属性または動作の説明、本ソフトウェアが

使用される動作環境の説明、本ソフトウェアの使用またはインストール手順、本ソフトウェアの使用方法の説明(「ドキュメント」)(iv)本契約の第3条に従い供給者からお客様にライセンス供与された本ソフトウェアのコピー、本ソフトウェアに不具合があった場合のパッチ、本ソフトウェアへの追加機能、本ソフトウェアの拡張機能、本ソフトウェアの修正バージョン、ソフトウェアコンポーネントのアップデート(該当する場合)を意味します。本ソフトウェアは実行可能なオブジェクトコードの形態でのみ提供されるものとします。

2.インストール、コンピューター、およびライセンスキー。データキャリアで供給、電子メールで送信、インターネットからダウンロード、供給者のサーバーからダウンロード、または他のソースから取得されたソフトウェアにはインストールが必要です。お客様は、本ソフトウェアを正しく設定されたコンピューターにインストールし、少なくともドキュメントで規定された要件に準拠する必要があります。インストール方法はドキュメントで説明されています。本ソフトウェアをインストールするコンピューターに、本ソフトウェアに悪影響を及ぼす可能性があるコンピュータープログラムやハードウェアをインストールすることはできません。コンピューターとは、本ソフトウェアがインストールまたは使用される、パーソナルコンピューター、ノートブック、ワークステーション、パームトップコンピューター、スマートフォン、ハンドヘルド電子機器、または本ソフトウェアの対象として設計されている他の電子機器を含む(ただしこれらに限定されない)を意味します。ライセンスキーとは、本契約に準拠して、本ソフトウェア、特定のバージョン、またはライセンス条項の拡張の法的な使用を許可するために、エンドユーザーに提供される一意の連続する記号、文字、数字、または特殊記号を意味します。

3.ライセンス。お客様が本契約に同意しており、ライセンス料を支払い期日までに支払い、本契約に定められているすべての契約条項に従うことを前提として、供給者はお客様に対し、以下の権利を付与します(以下「ライセンス」とします)。

a) インストールおよび使用。お客様には、コンピューターのハードディスクまたはその他のデータ永久記憶媒体にデータを格納するために本ソフトウェアをインストールし、コンピューターシステムのメモリへ本ソフトウェアをインストールおよび格納し、コンピューターシステム上で本ソフトウェアを実装、格納および表示する、非独占的かつ譲渡禁止の権利が付与されます。

b) ライセンス数の規定。本ソフトウェアを使用する権利は、エンドユーザー数によって制限されます。1人のエンドユーザーとは(ii)本ソフトウェアがインストールされている1台のコンピューターを意味します(ii)ライセンス数がメールボックスを単位として決定される場合、エンドユーザーはメールユーザーエージェント(以下「MUA」とします)を介して電子メールを受信する1人のコンピューターユーザーを意味します。電子メールがMUAで受信後、複数のユーザーに自動的に配信される場合、エンドユーザーの数は、その電子メールが配信されるユーザーの実際の数によって決まります。メールサーバーがメールゲートの役割を果たす場合、エンドユーザーの数は、そのゲートがサービスを提供するメールサーバーユーザーの数と同じになります。(エイリアスなどを使用して)1人のユーザーに不特定多数の電子メールアドレスが送信され、それらが受け付けられる場合、クライアント側で多数のユーザーにそのメールが自動的に配信されるのでなければ、ライセンスは1台のコンピューターに必要です。同じライセンスは、同時に複数のコンピューターで使用できません。エンドユーザーは、供給者によって付与されたライセンス数に基づく制限に従い、本ソフトウェアを使用する権限が与えられている範囲においてのみ、本ソフトウェアのライセンスキーを入力する資格があります。このライセンスキーは機密情報であると見なされます。本契約または供給者によって許可されている場合を除き、お客様はライセンスを第三者と共有すること、または第三者がライセンスを使用することを許可することが禁止されています。ライセンスキーが危険にさらされた場合は、速やかに供給者に通知してください。

c) Business Edition本ソフトウェアをメールサーバー、メール中継、メールゲートウェイ、インターネットゲートウェイで使用する場合は、本ソフトウェアのBusiness Editionバージョンを入手する必要があります。

d) ライセンス契約の期間。お客様は、本ソフトウェアを期限付きで使用する権利があります。

e) OEMソフトウェア。OEMソフトウェアの使用は、それがプリインストールされていたコンピューターに制限されます。別のコンピューターにインストールすることはできません。

f) **NFRまたは試用ソフトウェア**。再販不可品^①NFR^②または試用版に分類されるソフトウェアは、対価を求めて譲渡することはできず、ソフトウェア機能のデモまたはテスト目的のみで使用されるものとします。

g) **ライセンスの契約解除**。ライセンス契約は、その期間の満了により契約が自動的に解除されます。供給者は、お客様が本契約のいずれかの条項に違反したときは、供給者が持つ他の権利および法的救済手段に影響を与えることなく、本契約を解約することができます。本ライセンスを取り消す場合、お客様は、本ソフトウェアおよびバックアップコピーを直ちにすべて削除、破棄するか、自費でESETまたはソフトウェアの入手元にそれを返却する必要があります。ライセンスの終了時には、供給者は、エンドユーザーが、供給者のサーバーまたはサードパーティのサーバーに接続する必要がある本ソフトウェアの機能を使用する権利を取り消す権利があるものとします。

4. **データ収集機能およびインターネット接続要件**。本ソフトウェアの正常な動作には、インターネット接続が必要であり、プライバシーポリシーに従い、定期的に供給者のサーバーまたは第三者のサーバーおよび該当するデータ収集に定期的に接続する必要があります。インターネットへの接続およびデータ収集は、次のソフトウェア機能で必要です。

a) **ソフトウェアのアップデート**。供給者には、本ソフトウェアのアップデート（以下「アップデート」とします）を適時発行する権利がありますが、アップデートを提供する義務はありません。この機能は、ソフトウェアの標準の設定から有効にできます。エンドユーザーがアップデートの自動インストールを無効にしていなかったり、アップデートは自動的にインストールされます。アップデートを提供するために、プライバシーポリシーに準拠し、本ソフトウェアがインストールされているコンピューターまたはプラットフォームに関する情報を含む、ライセンスの正当性を検証する必要があります。

b) **供給者への侵入物および情報の転送**。本ソフトウェアには、コンピューターウイルスおよびその他の悪意のあるプログラム、ファイル^③URL^④IPパケット、イーサネットフレームなどの不審、問題、潜在的に望ましくない、または潜在的に危険なオブジェクト（「侵入」）のサンプルを収集する機能が含まれ、インストール処理、コンピューター、ソフトウェアがインストールされているプラットフォームの情報、本ソフトウェアの操作および機能の情報（「情報」）を含む（ただしこれらに限定されない）、これらのオブジェクトを供給者に送信します。情報および侵入には、エンドユーザーまたは本ソフトウェアがインストールされているコンピューターの他のユーザーのデータ（ランダムまたは誤って取得された個人データを含む）、関連付けられたメタデータによる侵入の影響を受けるファイルが含まれる場合があります。

情報および侵入は次のソフトウェア機能によって収集される場合があります。

i. **LiveGridレピュテーションシステム機能**には、侵入に関する単方向ハッシュの収集と供給者への送信が含まれます。この機能は、ソフトウェアの標準設定で有効です。

ii. **LiveGridフィードバックシステム機能**には、侵入を収集し、関連付けられたメタデータおよび情報とともに供給者に送信する機能が含まれます。この機能は、本ソフトウェアのインストール処理中に、エンドユーザーがアクティブ化することができます。

供給者は、侵入の分析と研究、ソフトウェアの改良、およびライセンスの正当性の検証の目的でのみ、受け取った情報および侵入を使用するものとし、適切な対策を講じて、受け取った侵入および情報が安全であることを保証するものとします。本機能をアクティブ化することで、プライバシーポリシーの規定に従い、関連する法規制に準拠して、侵入および情報は供給者によって収集および処理される場合があります。この機能はいつでも無効にすることができます。

本契約の目的のために、プライバシーポリシーに従い、供給者がお客様を特定できるようにするデータを収集、処理、および保存する必要があります。お客様は、供給者が独自の手段によって、お客様が本契約の規定に従って本ソフトウェアを使用しているかどうかを確認することに同意します。お客様は、本契約の目的でのみ、本ソフトウェアと供給者のコンピューターシステムまたは供給者の販売およびサポートネットワークの一部としての供給者のビジネスパートナーのコンピューターシステムとの間の通信中に、お客様のデータを転送し、本ソフトウェアの機能および本ソフトウェアの使用許可を保証し、供給者の権利を守る必要があることを承諾します。

本契約の締結後、供給者および供給者の販売およびサポートネットワークの一部としての供給者のビジネスパートナーは、請求目的、本契約の履行、およびお客様のコンピューターでの通知の送信のために、お客様を特定できる基本データを転送、処理、および保管する権利を有するものとします。お客様は、マーケティング情報を含む(ただしこれに限定されない)通知およびメッセージを受信することに同意します。

データ主体としてのプライバシー、個人データ保護、およびお客様の権利の詳細については、供給者のWebサイトまたはインストール処理で直接アクセスできるプライバシーポリシーを参照してください。お客様は、ソフトウェアのヘルプセクションからアクセスすることもできます。

5.エンドユーザの権利行使。お客様は、エンドユーザーの権利を、直接またはお客様の従業員を通じて行使する必要があります。お客様は、自らの活動を確実なものとするためにのみ、およびお客様がライセンスを取得したコンピューターシステムを保護するためにのみ、本ソフトウェアを使用できます。

6.権利の制限。お客様は本ソフトウェアのコピー、配布、部品の分離、または派生バージョンの作成を行ってはなりません。本ソフトウェアの使用時には、下記の制限事項に従う必要があります。

a) お客様は、データの永久記憶用媒体上に本ソフトウェアのコピーを1つ、バックアップコピーとして作成できます。ただし、この保管用のバックアップコピーは、他のいかなるコンピュータにもインストールしたり、または使用したりすることができません。これ以外に本ソフトウェアのコピーを作成することは、本契約に対する違反となります。

b) 本契約に規定されている以外のいかなる態様でも、本ソフトウェアまたは本ソフトウェアのコピーの使用、改変、複製、または使用権の譲渡を行ってはなりません。

c) 本ソフトウェアの売却、サブライセンス付与、他人への賃貸もしくは他人からの賃借、借用、または商業サービスの提供目的での本ソフトウェアの使用は禁じられています。

d) 本ソフトウェアのリバースエンジニアリング、逆コンパイル、またはソフトウェアの逆アセンブルを行ったり、ソースコードを取得しようとしたりしてはなりません。ただし、そのような制限を設けることが法律によって明示的に禁止されている範囲内においては、この限りではありません。

e) お客様は、著作権法およびその他の知的財産権から生じる、適用可能な制限など、本ソフトウェアを使用する際の法律におけるすべての適用可能な法的規制に従う態様においてのみ、本ソフトウェアを使用できます。

f) お客様は、本ソフトウェアおよびその機能を、他のエンドユーザーがそれらのサービスにアクセスする可能性を制限しない方法でのみ使用することに同意するものとします。供給者は、可能な限り多くのエンドユーザーがサービスを利用できるようにするために、個別のエンドユーザーに提供されるサービスの範囲を制限する権利を留保します。サービスの範囲を制限することにより、本ソフトウェアのすべての機能を使用することもできなくなり、本ソフトウェアの特定の機能に関連する供給者のサーバー上またはサードパーティのサーバー上のデータおよび情報が削除されることとします。

g) お客様は、本契約の条項に反して、ライセンスキーの使用に関する活動、または何らかの形式での使用済みまたは未使用のライセンスキーの譲渡、不正複製、複製または生成されたライセンスキーの配布、あるいは供給者以外から入手したライセンスキーを使用したソフトウェアの利用など、本ソフトウェアの使用の資格がない個人にライセンスキーを提供する行為を実施しないことに同意します。

7.著作権。本ソフトウェア、および所有権や知的所有権を含む一切の権利は、ESETおよび/またはESETのライセンス供給者の財産です。これらは、国際条約の規定と本ソフトウェアが使用される国のその他のすべての準拠法によって保護されます。本ソフトウェアの構造、編成、およびコードは、ESETおよび/またはESETのライセンス供給者の重要な企業秘密であり機密情報です。お客様は、第6条(a)に当てはまる場合を除いて、本ソフトウェアをコピーすることはできません。本契約に基づき、お客様が作成するコピーはすべて、本ソフトウェア上に示されるものと同じ著作権表示および所有権表示を含んでいなければなりません。お客様がリバースエンジニアリング、逆コンパイル、逆アセンブルを行ったり、本

契約の規定に違反する方法でソースコードを取得しようとした場合、それによって得られたいかなる情報も、それが発生した瞬間からすべて、本契約の違反に関連する供給者の権利にかかわらず、自動的にかつ取り消しできない形で供給者に譲渡され、供給者の所有であるとみなされます。

8.権利の留保。本ソフトウェアに対する権利は、本契約において本ソフトウェアのエンドユーザーとしてお客様に明示的に与えられた権利を除き、すべて供給者自身が留保します。

9.複数言語対応バージョン、デュアルメディアソフトウェア、複数コピー。本ソフトウェアが複数のプラットフォームまたは言語をサポートしているか、お客様が本ソフトウェアのコピーを複数入手した場合、お客様はライセンスを取得したバージョンのコンピューターシステム数でのみ本ソフトウェアを使用できます。使用していない本ソフトウェアのバージョンやコピーを、他者に売却、賃貸、質借、サブライセンス付与、貸与、または譲渡することはできません。

10.本契約の開始と解除。本契約は、お客様が本契約に同意した日から有効となります。本契約は、お客様が本契約に同意した日から有効となります。お客様は、供給者またはそのビジネスパートナーから入手した本ソフトウェア、すべてのバックアップコピー、および関連するすべての資料を、永久的に削除、破棄、または自費で返却することにより、本契約を解除することができます。本契約の終了の態様に関係なく、第7条、第8条、第11条、第13条、第19条、および第21条の規定は、無期限に有効であり続けるものとします。

11.エンドユーザーの表明。お客様はエンドユーザーとして、明示または暗黙のいかなる種類の保証も伴わず、該当の法律によって許可される範囲において、本ソフトウェアが「現状有姿」のまま提供されていることを認めるものとします。供給者、そのライセンス供給者、関係者、および著作権保有者のいずれも、本ソフトウェアの特定の目的に対する商品性または適合性、および第三者の特許、著作権、商標、またはその他の権利に対する侵害の不存在について、明示または黙示を問わず、一切の表明または保証を行いません。供給者もその他の関係者も、本ソフトウェアに含まれている機能がおお客様の要求に沿うこと、または本ソフトウェアが円滑で問題なく動作するということの保証を行いません。お客様は、意図する結果に到達するための本ソフトウェアの選択、および本ソフトウェアのインストール、使用、および本ソフトウェアで達成される結果について、完全に責任とリスクを負います。

12.さらなる義務の否定。本契約で具体的に列挙される義務以外に、本契約が供給者およびそのライセンサーに対して課す義務はありません。

13.責任の制限。準拠法によって許可される最大限の範囲において、いかなる場合も、供給者、その被雇用者、ライセンス供給者は、どのような態様で発生したものであるかと、契約、違法行為、怠慢、または責任の発生を定めるその他の事実のいずれに起因するものであるかを問わず、本ソフトウェアを使用したことにより、または本ソフトウェアが使用できないことにより発生した、利益、収益、または売上の損失、データの喪失、補用品またはサービスの購入にかかった費用、物的損害、人的損害、事業の中断、企業情報の喪失、特別損害、直接損害、間接損害、偶発的損害、経済的損害、補填損害、懲罰的損害、特別または派生的損害に対し、一切責任を負わないものとします。これは、たとえ供給者、そのライセンス供給者、または関係者がそのような損害の可能性について通知を受けていた場合であっても同様です。一部の国および法律では、免責を認めず、しかし限定された範囲の責任を負うことは許可しています。その場合、供給者、その被雇用者、ライセンス供給者、または関係者の責任は、お客様がライセンスの対価として支払った金額を限度とします。

14. 本契約に含まれるものは何も、それに反する場合であっても、消費者として取引するすべての当事者の法的権利を損なうものではありません。

15.テクニカルサポート。テクニカルサポートは、ESETまたはESETの依頼を受けた第三者の独自の判断により提供され、いかなる種類の保証も表明も伴わないものとします。エンドユーザーは、テクニカルサポートの提供の前に、存在するすべてのデータ、ソフトウェア、プログラム機能をバックアップする必要があります。ESETおよび / または ESETの依頼を受けた第三者は、テクニカルサポートの提供によりお客様に生じたデータ、資産、ソフトウェアまたはハードウェアの損害または損失、もしくは利益の喪失について、いかなる責任も負いません。ESETおよび / または ESETの依頼を受けた第三者は、問題をテクニカルサポートで解決できないと判断する権利があります。ESETは、独自の判断により、テクニカルサポー

トの提供を拒否、中断、終了する権利があります。ライセンス情報、情報、およびプライバシーポリシーに準拠した他のデータは、技術サポートを提供するために必要になる場合があります。

16. ライセンスの譲渡。 本契約の条件に違反しないかぎり、あるコンピューターにインストールされていた本ソフトウェアを別のコンピューターシステムにインストールすることができます。エンドユーザーは、本契約の条件に違反しない場合のみ、供給者の同意の元、本契約から派生するライセンスおよびすべての権利を、別のエンドユーザーに永久に譲渡する権利があります。その場合(ii) 元のエンドユーザーは、ソフトウェアのコピーを保持しておらず(ii) 元のエンドユーザーから新しいエンドユーザーへ直接権利が譲渡され(iii) 新しいエンドユーザーが元のエンドユーザーに課せられた本契約に基づくすべての権利および義務を負い、(iv) 元のエンドユーザーが新しいエンドユーザーに、第17条で規定するソフトウェアが正規のものであることを証明するドキュメントを提供するものとします。

17. 正規ソフトウェアの証明。 エンドユーザーのソフトウェアの使用資格は、次のいずれかの方法で証明できます(ii) 供給者または供給者が指定した第三者が発行するライセンス証明書(ii) 締結されている場合、書面によるライセンス契約(iii) アップデートを有効にするライセンスの詳細（ユーザ名およびパスワード）が記載された供給者に送信された電子メールの提出。ライセンス情報およびプライバシーポリシーに準拠したエンドユーザー識別データは、ソフトウェアの純正を検証するために必要になる場合があります。

18. 公共団体および米国政府に対するライセンス。 米国政府を含む公共団体に対する本ソフトウェアのライセンスは、本契約に明記しているライセンス権利および制限に基づいて提供されます。

19. 輸出管理規制

a) お客様は、直接的または間接的に、ESETまたはESETの持ち株会社ESETの子会社、持ち株会社の子会社、持ち株会社が管理する事業体（「関連会社」）による次のような輸出貿易管理法の違反または輸出貿易管理法の下で否定的な結果につながる一切の個人に対して本ソフトウェアを輸出、再輸出、移転、または提供せず、そのような方法でソフトウェアを使用せず、そのような行為に関与したりしないものとします。

i. 米国、シンガポール、英国、欧州連合またはその加盟国、本契約の義務が履行される国、あるいはESETまたはその関連会社が登録または事業を行う国の政府、州、規制当局が発行または採用した、商品、ソフトウェア、技術、サービスの輸出、再輸出、または移転を統制、制限、またはライセンス要件を課すすべての法律（「輸出貿易管理法」）。

ii. 米国、シンガポール、英国、欧州連合またはその加盟国、本契約の義務が履行される国、あるいはESETまたはその関連会社が登録または事業を行う国の政府、州、規制当局が課した経済、金融、貿易、制裁、制限、禁止、輸出入禁止、資金または資産の移転の禁止、サービス提供の禁止、あるいは同等の対策（「制裁法」）。

b) ESETは、次の場合において、本契約の義務を即時停止または解除する権利を有するものとします。

i. ESETが、合理的な意見において、ユーザーが本契約の第19.a条の条項に違反したか違反する可能性が高いと判断した

ii. エンドユーザーまたは本ソフトウェアに輸出貿易管理法が適用され、その結果としてESETが、合理的な意見において、本契約の義務の継続的な履行によってESETまたはその関連会社が輸出貿易管理法に違反するか、輸出貿易管理法の下で否定的な影響を受ける可能性があると判断した

c) いずれの当事者も、適用される輸出貿易管理法に準拠しないか、輸出貿易管理法の下で罰則を受けるか、禁止される行為または不作為（あるいは行為または不作為に同意すること）を勧誘または義務付けられるように、本契約のいずれの条項も意図せず、何もそのように解釈または理解されない

20. 通知。 すべての通知、返却される本ソフトウェアおよび本件ドキュメントは、スロバキア共和国, ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic

21. 準拠法。本契約は、スロバキア共和国の法律に準拠し、これに従って解釈されるものとします。エンドユーザーおよび供給者は、準拠法および国際物品売買契約に関する国際連合条約の矛盾する規定については、適用されないことに同意するものとします。お客様は、本契約に関するいかなるクレームもしくは供給者との紛争、または本ソフトウェアをお客様が使用することによるいかなる紛争またはクレームも、ブラチスラバ第1地方裁判所で解決し、さらに、ブラチスラバ第1地方裁判所での管轄権の行使に同意し、明示的にこれを承諾するものとします。

22. 一般条項。本契約の条項のいずれかが無効または履行不能である場合、これが本契約のその他の条項の有効性に影響を及ぼすことはないものとします。これらその他の条項は、本契約に定める条件に基づき、引き続き有効かつ履行可能であるものとします。本契約の翻訳版の間で不一致がある場合には、英語版が優先されるものとします。本契約に対するいかなる修正も、書面によってしか行うことができず、当該修正は、供給者の正式な代表者か、委任状の条項でこの役割を果たすことが明示的に認められた代理人によって署名されなければなりません。

本契約は、本ソフトウェアに関するお客様および供給者間の合意事項をすべて網羅しており、本ソフトウェアに関する従前のいかなる表明、議論、約束、情報交換、または広告にも取って代わります。

EULA ID: BUS-STANDARD-20-01

プライバシーポリシー

データ管理者としてのESET, spol. s r. o. (登録事業所所在地: Einsteinova 24, 851 01 Bratislava, Slovak Republic) 商業登記: ブラチスラバ第1地方裁判所、有限会社部門、登録番号3586/B 事業登記番号: ブラチスラバ第1地方裁判所、有限会社部門、登録番号3586/B 事業登記番号: 31333532) (ESETまたは「当社」)は、お客様の個人データとプライバシーの処理に関して透明でありたいと考えています。この目標を達成するために、当社は、お客様(「エンドユーザー」または「お客様」)に次の事項を通知する目的のみ、本プライバシーポリシーを発行しています。

- 個人データの処理、
- データの機密保持、
- データの主体の権利。

個人データの処理

製品に実装されたESETが提供するサービスは、エンドユーザーライセンス契約(EULA)の条項に従って提供されますが、項目によっては特定の注意が必要になる場合がありますESETは、サービスの提供に関連するデータ収集の詳細について、お客様に説明しますESETは、アップデート/アップグレードサービスESET LiveGrid®データの悪用に対する保護、サポートなど、エンドユーザーライセンス契約および製品資料に記載されているさまざまなサービスを提供します。すべてを機能させるためにESETは次の情報を収集する必要があります。

- 製品がインストールされているプラットフォームを含むインストール処理とコンピューターに関する情報、およびオペレーティングシステム、ハードウェア情報、インストールID、ライセンスID、IPアドレス、MACアドレス、製品の構成設定といった製品の動作と機能に関する情報を含むアップデートおよび統計情報。
- ESET LiveGrid®レピュテーションシステムの一部として侵入に関連する単方向ハッシュ。これは、検査済みファイルをクラウドのホワイトリストおよびブラックリスト項目のデータベースと比較し、ESETマルウェア対策ソリューションの効率化を図ります。
- ESET LiveGrid®フィードバックシステムの一部として世界から収集した不審なサンプルおよびメタデータ。これによりESETは、エンドユーザーのニーズに迅速に対応し、最新の脅威に反応し続けることができますESETはお客様がESETに送信する次の情報を必要としています

oウイルスおよび他の悪意のあるプログラム、ならびにお客様によって迷惑メールとして報告されたか、製品によって警告された実行ファイル、電子メールメッセージなどの不審であるか、問題があるか、望ましくない可能性があるか、危険の可能性があるオブジェクトの潜在的なサンプルといった侵入情報

oデバイスの種類、ベンダー、モデル、名前などのローカルネットワークのデバイスに関する情報

oIPアドレスおよび地理情報oIPパケットoURLおよびイーサネットフレームなどのインターネットの使用に関する情報

o含まれるクラッシュダンプファイルと情報

当社は、この範囲外でデータを収集する意志はありませんが、場合によってはそれが防止できないことがあります。誤って収集されたデータは、マルウェア自体に含まれる場合があります。当社は、本プライバシーポリシーで規定された目的において、そのようなデータを当社のシステムまたはプロセスに取り込む意図はありません。

- ライセンスIDなどのライセンス情報、および名前、姓、住所、電子メールアドレスなどの個人データは、課金、ライセンスの真正の検証、サービスの提供のために必要です。
- サポート要求に含まれる連絡先情報およびデータは、サポートのサービスで必要になる場合があります。選択した連絡方法に基づき、当社は、電子メールアドレス、電話番号、ライセンス情報、製品詳細、およびサポートケースの説明を収集する場合があります。サポートのサービスを進めるために、他の情報の提供を求められる場合があります。

データの機密保持

ESETは、販売、サービス、サポートネットワークの一部として、関連会社またはパートナー経由で、世界中で事業を展開している会社です。ESETによって処理された情報は、サービスの提供、サポート、または請求などのEULAの履行のため、関連会社またはパートナー企業との間で転送される場合があります。選択した位置情報およびサービスに基づき、欧州委員会の適切な決定権がない国にお客様のデータを転送する必要がある場合があります。この場合でも、情報を転送するたびに、データ保護法の規制が適用され、必要な場合にのみ実行されます。標準契約条項、拘束的企業準則、または他の適切な安全保護対策を例外なく確立する必要があります。

ESETは、エンドユーザーライセンス契約に従って、サービスを提供している間、必要最低限の期間にのみデータが保存されるように最善の努力を講じます。ESETの保持期間は、お客様が簡単かつスムーズな更新が行える時間的余裕を用意するために、ライセンスの有効期間よりも少し長くなる場合があります。ESET LiveGrid®からの最小化および仮名化された統計情報および他のデータが統計目的で処理される場合があります。

ESETは、適切な技術的および組織的な対策を導入し、潜在的なリスクに適したレベルのセキュリティを保証します。当社は最善を尽くし、処理システムおよびサービスに関する、継続中の機密性、完全性、可用性、および障害回復力を保証します。ただし、お客様の権利と自由を脅かす結果になるデータ違反の場合には、すぐに監督当局とデータ主体に通知します。データ主体として、お客様は、監督当局に苦情を申し立てる権利を有します。

データの主体の権利

ESETはスロバキア法の規制に準拠し、欧州連合の一部としてデータ保護法によって拘束されます。適用されるデータ保護法で規定された条件が適用されます。お客様は、データ主体として、次の権利を有しています。

- ESETに対してお客様の個人データへのアクセスを要求する権利、
- 不正確な個人データを修正する権利(不完全な個人データを完全にする権利もあります)

- 個人データの消去を要求する権利、
- 個人データの処理の制限を要求する権利
- 処理に異議を申し立てる権利
- 苦情を申し立てる権利および
- データ移植性の権利。

データ主体として権利を行使する場合、またはご質問や懸念をお持ちの場合は、以下の宛先までご連絡ください。

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk