ESET Endpoint 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 Endpoint 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遭わず、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 ESET Endpoint Security8 1
1.1 このバージョンの新機能? 2
1.2 システム要件 3
1.2 サポートされている言語 4
1.3 セキュリティの考え方 5
1.4 ヘルプページ 6
2 リモート管理されたエンドポイントのドキュメント 7
2.1 ESET PROTECTの概要 8
2.2 ESET PROTECT Cloudの概要 10
2.3 設定をパスワードで保護する 10
2.4 ポリシーの概要 11
2.4 ポリシーのマージ 11
2.5 フラグの仕組み 12
3 単独でのESET Endpoint Securityの使用 13
3.1 インストール方法 13
3.1 ESET AV Removerでインストール 14
3.1 ESET AV Remover 15
3.1 ESET AV Removerによるアンインストールがエラーで終了した場合 17
3.1 インストール (.exe) 18
3.1 インストールフォルダの変更(.exe) 20
3.1 インストール (.msi) 21
3.1 詳細インストール (.msi) 23
3.1 コマンドラインインストール 25
3.1 GPOまたはSCCMを使用した展開 30
3.1 最新バージョンへのアップグレード 30
3.1 レガシー製品自動アップグレード 31
3.1 セキュリティと安定性のアップデート 32
3.1 一般的なインストールの問題 32
3.1 アクティベーションに失敗 32
3.2 製品のアクティベーション 33
3.3 コンピュータの検査 33
3.4 初心者向けガイド 33
3.4 ユーザーインターフェイス 33
3.4 アップデートの設定 37
3.4 ゾーンの設定 38
3.4 Webコントロールツール 39
4 ESET Endpoint Securityの使用方法 39
4.1 コンピュータ 42
4.1 検出エンジン 43
4.1 検出エンジンの詳細オプション 48
4.1 侵入物が検出された 48
4.1 共有ローカルキャッシュ 50
4.1 リアルタイムファイルシステム保護 50
4.1 リアルタイム保護の確認 52
4.1 リアルタイム保護の設定の変更 52
4.1 リアルタイム保護が機能しない場合の解決方法 52
4.1 コンピュータの検査 53
4.1 カスタム検査起動ツール 55
4.1 検査の進行状況 57
4.1 コンピューター検査ログ 58

4.1 マルウェア検査 58
4.1 アイドル状態検査 59
4.1 検査プロファイル 59
4.1 検査の対象 60
4.1 詳細検査オプション 61
4.1 デバイスコントロール 61
4.1 デバイスコントロールルールエディタ 62
4.1 検出されたデバイス 63
4.1 デバイスグループ 64
4.1 デバイスコントロールルールの追加 65
4.1 ホストベースの侵入防止システム(HIPS) 67
4.1 HIPSインタラクティブウィンドウ 69
4.1 潜在的なランサムウェア動作の検出 70
4.1 HIPSルール管理 71
4.1 HIPSルール設定 72
4.1 HIPS詳細設定 74
4.1 ドライバは常にロードできます 75
4.1 プレゼンテーションモード 75
4.1 スタートアップ検査の設定 76
4.1 自動スタートアップファイルのチェック 76
4.1 ドキュメント保護 77
4.1 除外 77
4.1 パフォーマンス除外 78
4.1 パフォーマンス除外の追加または編集 79
4.1 パス除外形式 80
4.1 検出除外 81
4.1 検出除外の追加または編集 83
4.1 検出除外の作成ウィザード 85
4.1 除外(7.1以下) 86
4.1 プロセスの除外 86
4.1 プロセス除外の追加または編集 87
4.1 HIPS除外 87
4.1 ThreatSense パラメータ 87
4.1 駆除レベル 91
4.1 検査対象外とするファイル拡張子 92
4.1 追加のThreatSenseパラメータ 93
4.2 ネットワーク 93
4.2 ネットワーク 94
4.2 学習モード 96
4.2 ネットワーク攻撃保護 97
4.2 詳細フィルタリングオプション 98
4.2 IDSルール 100
4.2 不審な脅威がブロックされました 102
4.2 ネットワーク保護トラブルシューティング 102
4.2 ネットワーク名 103
4.2 既知のネットワーク 103
4.2 既知のネットワークエディタ 104
4.2 ネットワーク認証 – サーバー構成 107
4.2 ファイアウォールプロファイル 107
4.2 ネットワークアダプタに割り当てられたプロファイル 108
4.2 アプリケーションの変更の検出 108

4.2 変更の検出から除外されたアプリケーション 109
4.2 ルールの設定と使用 109
4.2 ファイアウォールルールリスト 109
4.2 ファイアウォールルールの追加または編集 111
4.2 ファイアウォールルール - ローカル 112
4.2 ファイアウォールルール - リモート 113
4.2 一時IPアドレスブラックリスト 114
4.2 信頼ゾーン 114
4.2 ゾーンの設定 115
4.2 ファイアウォールゾーン 115
4.2 ファイアウォールログ 115
4.2 接続の確立 - 検出 116
4.2 ESETファイアウォールの問題の解決 117
4.2 トラブルシューティングウィザード 118
4.2 ロギングとログからのルールまたは例外の作成 118
4.2 ログからルールを作成 118
4.2 ファイアウォール通知からの例外の作成 119
4.2 ネットワーク保護詳細ログ 119
4.2 プロトコルフィルタリングの問題の解決 119
4.3 Webとメール 120
4.3 プロトコル フィルタリング 122
4.3 対象外のアプリケーション 122
4.3 対象外のIPアドレス 123
4.3 SSL/TLS 124
4.3 証明書 125
4.3 暗号化されたネットワークトラフィック 125
4.3 既知の証明書のリスト 126
4.3 SSL/TLSフィルタリングされたアプリケーションのリスト 127
4.3 電子メールクライアント保護 127
4.3 電子メールプロトコル 129
4.3 電子メールアラートと通知 130
4.3 メールクライアントとの統合 131
4.3 Microsoft Outlookツールバー 131
4.3 Outlook ExpressおよびWindowsメールツールバー 131
4.3 確認ダイアログ 132
4.3 メッセージの再検査 132
4.3 迷惑メール対策機能 133
4.3 迷惑メール対策アドレス帳 134
4.3 ブラックリスト/ホワイトリスト/除外リスト 135
4.3 ブラックリスト/ホワイトリスト/例外アドレスの追加/編集 136
4.3 Webアクセス保護 136
4.3 Webアクセス保護詳細設定 139
4.3 Webプロトコル 139
4.3 URLアドレス管理 140
4.3 URLアドレスリスト 141
4.3 新しいURLアドレスリストの作成 142
4.3 URLマスクを追加する方法 143
4.3 フィッシング対策機能 143
4.3 安全なブラウザー詳細設定 145
4.3 保護されたWebサイト 145
4.4 Webコントロール 146

4.4 Webコントロールルール 147
4.4 Webコントロールルールの追加 148
4.4 分類グループ 150
4.4 URLグループ 151
4.4 ブロックされたWebページメッセージのカスタマイズ 152
4.5 アップデート 154
4.5 アップデートの設定 158
4.5 アップデートのロールバック 161
4.5 プログラムコンポーネントのアップデート 163
4.5 接続オプション 163
4.5 配布用アップデート 165
4.5 ミラーのHTTPサーバーとSSL 167
4.5 ミラーからのアップデート 167
4.5 ミラーアップデートの問題のトラブルシューティング 169
4.5 アップデートタスクの作成方法 170
4.6 ツール 170
4.6 ログファイル 171
4.6 ログのフィルタリング 174
4.6 ログ設定 175
4.6 監査ログ 176
4.6 スケジューラー 177
4.6 アクティビティの確認 180
4.6 ESET SysInspector 181
4.6 クラウドベース保護 182
4.6 クラウドベース保護の除外フィルター 185
4.6 実行中のプロセス 185
4.6 セキュリティレポート 187
4.6 ネットワーク接続 189
4.6 ESET SysRescue Live 190
4.6 分析用サンプルの提出 190
4.6 分析のためにサンプルを提出 – 不審なファイル 191
4.6 分析のためにサンプルを提出 – 不審なサイト 192
4.6 分析のためにサンプルを提出 – 誤検出ファイル 192
4.6 分析のためにサンプルを提出 – 誤検出サイト 192
4.6 分析のためにサンプルを提出 – その他 193
4.6 通知 193
4.6 アプリケーション通知 194
4.6 デスクトップ通知 195
4.6 電子メール通知 195
4.6 通知のカスタマイズ 198
4.6 隔離 198
4.6 プロキシサーバーの設定 200
4.6 タイムスロット 201
4.6 Microsoft Windows Update 202
4.6 ライセンス間隔チェック 203
4.7 ユーザーインターフェイス 203
4.7 ユーザーインタフェース要素 203
4.7 アプリケーションステータス 205
4.7 アクセス設定 206
4.7 詳細設定のパスワード 207
4.7 アラートとメッセージボックス 207

4.7 対話アラート ... 209
4.7 確認メッセージ ... 210
4.7 詳細設定競合エラー ... 211
4.7 リムーバブルメディア ... 211
4.7 再起動する必要があります ... 213
4.7 再起動が推奨されます ... 214
4.7 システムトレイアイコン ... 216
4.7 コンテキストメニュー ... 217
4.7 ヘルプとサポート ... 217
4.7 ESET Endpoint Securityの概要 ... 218
4.7 システム構成データの送信 ... 219
4.7 テクニカルサポート ... 219
4.7 プロファイルマネージャ ... 220
4.7 キーボードショートカット ... 221
4.7 診断 ... 221
4.7 コマンドラインスキャナー ... 222
4.7 ESET CMD ... 225
4.7 アイドル状態検知 ... 227
4.7 設定をインポートおよびエクスポートする ... 227
4.7 すべての設定を既定値に戻す ... 228
4.7 現在のセクションのすべての設定を元に戻す ... 228
4.7 設定の保存中のエラー ... 228
4.7 リモート監視と管理 ... 229
4.7 ERMMコマンドライン ... 230
4.7 ERMM JSONコマンドのリスト ... 231
4.7 保護ステータスの取得 ... 232
4.7 アプリケーション情報の取得 ... 233
4.7 ライセンス情報の取得 ... 235
4.7 ログの取得 ... 235
4.7 アクティベーションステータスの取得 ... 236
4.7 検査情報の取得 ... 237
4.7 設定の取得 ... 238
4.7 アップデートステータスの取得 ... 239
4.7 検査の開始 ... 240
4.7 アクティベーションの開始 ... 240
4.7 アクティベーション解除の開始 ... 241
4.7 アップデートの開始 ... 242
4.7 構成の設定 ... 242
5 よくある質問 ... 243
5.1 ESET Endpoint Securityをアップデートする方法 ... 244
5.2 ESET Endpoint Securityをアクティベートする方法 ... 244
5.2 アクティベーション中の製品認証キーの入力 ... 245
5.2 ESET Business Accountへのログイン ... 245
5.2 レガシーライセンス認証情報を使用して、新しいESETエンドポイント製品をアクティベーションする方法 ... 246
5.3 PCからウイルスを取り除く方法 ... 246
5.4 アプリケーションに通信を許可する方法 ... 246
5.5 スケジューラで新しいタスクを作成する方法 ... 247
5.5 週次コンピューター検査をスケジュールする方法 ... 248
5.6 ESET Endpoint SecurityをESET PROTECTに接続する方法 ... 249
5.6 上書きモードを使用する方法 ... 249
5.6 ESET Endpoint Securityの推奨されたポリシーを適用する方法 ... 251

5.7 ミラーを構成する方法 254
5.8 ESET Endpoint Securityがインストールされた状態でWindows 10にアップグレードする方法 254
5.9 リモート監視と管理をアクティブ化する方法 255
5.10 インターネットから特定のファイルタイプのダウンロードをブロックする方法 257
5.11 ESET Endpoint Securityユーザーインターフェースを最小化する方法 258
5.12 「安全なブラウザーを要求されたWebページにリダイレクトできませんでした」を解決する方法 259
6 エンドユーザーライセンス契約 260
7 プライバシーポリシー 266

ESET Endpoint Security8

ESET Endpoint Security 8では、コンピュータのセキュリティに新しいアプローチで取り組んでいます。最新バージョンのThreatSense 検査エンジンは、ファイアウォールおよび迷惑メール対策機能を備え、ご使用中のコンピュータを高い精度と速度をもって安全に保ちます。 その結果、このシステムでは、コンピュータにとって脅威となる攻撃とマルウェアを常に警戒します。

ESET Endpoint Security 8は、弊社の長期にわたる取り組みによって保護機能の最大化とシステムフットプリントの最小化を実現した完全なセキュリティソリューションです。人工知能に基づく高度な技術は、システムのパフォーマンスを低下させたり、コンピュータを中断させることなく、ウイルス、スパイウェア、トロイの木馬、ワーム、アドウェア、ルートキット、およびその他のインターネット経由の攻撃の侵入を強力に阻止します。

ESET Endpoint Security 8は主に小規模事業環境のワークステーションで使用するために設計されています。

ESETEndpointSecurityを単独での使用するセクションでは、ダウンロード⍰インストール⍰アクティベーションなど、ヘルプトピックが複数の章と節に分類され、位置付けやコンテキストがわかりやすくなっています。

エンタープライズ環境でESET Endpoint SecurityをESET PROTECTとともに使用することにより、ネットワークに接続されたのどのコンピュータからクライアントワークステーションをいくつでも簡単に管理し、ポリシーとルールの適用、検出の監視、クライアントのリモート設定が可能になります。

よくある質問の章では、よくある質問と問題をいくつか説明します。

機能と利点

ユーザーインターフェイスの再設計	このバージョンでは、ユーザーインターフェイスが大幅に再設計され、ユーザビリティテストの結果に基づいて簡略化されています。 すべての GUI 用語と通知は慎重にレビューされ、インターフェースは現在ヘブライ語やアラビア語など右から左に記述する言語もサポートしています。 オンラインヘルプはESET Endpoint Securityに統合され、ダイナミックにアップデートされたサポートコンテンツを提供します。
ウイルス・スパイウェア対策	従来よりもさらに多くの既知および未知のウイルス、ワーム⍰トロイの木馬、そしてルートキットを早期に検出し駆除します。 アドバンスドヒューリスティックにより、これまで見られなかったようなマルウェアも検出して未知の脅威からユーザーを保護し、損害をもたらす前にそれらを無効化します⍰[Webアクセス保護]と[フィッシング対策]は、Webブラウザとリモートサーバー間の通信(SSLを含む)を監視することで保護します。[電子メールクライアント保護]では、POP3(S)とIMAP(S)プロトコルで受信したメール通信を検査します。
通常アップデート	検出エンジン(以前はウィルス定義データベースという名称)とプログラムモジュールを定期的にアップデートすることは、コンピューターのセキュリティを最大限に確保するのに最良の方法です。
ESET LiveGrid®(クラウドによる評価)	ユーザーは、ESET Endpoint Securityから、稼働中のプロセスやファイルの評価を直接チェックできます。

リモート管理	ESET PROTECTまたはESET Security Management Centerでは、1つの集中管理された場所から、ネットワーク環境におけるワークステーション、サーバー、モバイルデバイス上のESET製品を管理できます。ESET Security Management Center Webコンソール(ESMC Webコンソール)を使用すると、ESETソリューションを展開し、タスクを管理し、セキュリティポリシーを施行し、システムステータスを監視して、リモートコンピュータの問題または脅威にすばやく対応します。
ネットワーク攻撃保護	ネットワークトラフィックの内容を分析し、ネットワーク攻撃から保護します。有害だと見なされるすべてのトラフィックがブロックされます。
Webコントロール(ESET Endpoint Securityのみ)	[Webコントロール]セクションでは、対象ユーザーに対して適切でない内容を掲載していると考えられるWebページをブロックします。さらに、企業やシステム管理者は、事前に定義された27以上のカテゴリと140以上のサブカテゴリへのアクセスを禁止できます。

このバージョンの新機能?

ESET Endpoint Security 8がリリースされ、ダウンロードできます

セキュアブラウザー

- コンピューターで実行中の他のプロセスからWebブラウザーを保護します。
- ゼロトラストアプローチであり、コンピューターまたはその保護機能が危険にさらされている、または不十分であるという前提でブラウザーのメモリ空間や結果的にブラウザーウィンドウの内容が改ざんされることを防止します。
- 既定では、管理者がセキュリティポリシーの機能を活用する十分な時間を確保できるように、この機能は無効になっています。

WMIと詳細レジストリ検査

- レジストリまたはWMIリポジトリのどこかで悪意のある参照または危険なコンテンツを検出および排除できるレジストリ検査の改善
- 検査には時間がかかる場合があります。これらの検査対象は、「詳細」検査プロファイルの場合でも、すべてのオンデマンド検査で選択する必要があります

マイクロプログラムコンポーネントアップデート(機能アップデート)

- ESET Endpoint Securityの保守を最小限に抑えるためのスマートソリューション
- MicroPCUは再起動を数週間待機することができます
- 設定転送を含む、プロセス中のシステムからの登録解除など、すべての問題のある製品は再インストールされません
- ダウンロードするデータが少なくなります(差分アップデート)
- ユーザーのための簡易または完全に抑制可能なの事前通知があり、管理されたネットワークに対応し

ています

セキュリティと安定性のアップデート

- セキュリティおよび安定性アップデートは、サポートされているバージョン(7.x以降)に自動的に配布されます。サポートされているバージョンには、重要な変更のみが含まれており、変更ログて文書化されます。

このリリースには、さまざまなバグ修正とパフォーマンスの改善が含まれています。

ESET Endpoint Securityの新機能の詳細とスクリーンショットについては、次のESETナレッジベース記事をお読みください。

- ESET Endpoint Security8の新機能

システム要件

ESET Endpoint Securityをシームレスに動作させるために、システムは、次のようなハードウェアおよびソフトウェア要件を満たしている必要があります(既定の製品設定)。

サポート対象のプロセッサ

IntelまたはAMDのSSE2命令セットの32ビット(x86)プロセッサーまたは64ビット(x64)プロセッサ1 GHz以上

OS

Microsoft® Windows® 10
Microsoft® Windows® 8.1
Microsoft® Windows® 8

Microsoft® Windows® 7 SP1と最新のWindowsアップデート(KB4474419およびKB4490628以上)

Windows XPとWindows Vistaはサポートされません

常にオペレーティングシステムを最新の状態に保つようにしてください。

その他

- コンピューターにインストールされているオペレーティングシステムと他のソフトウェアのシステム要件が満たされていること
- 0.3 GBの空きシステムメモリ(注記1を参照)
- 1 GBの空きディスク領域(注記2を参照)
- 最低ディスプレイ解像度1024x768

• 製品アップデートのソース(注記3を参照)へのインターネット接続またはローカルエリアネットワーク接続

• 1台のデバイスで同時に実行されている2つのウイルス対策プログラムにより、システムの速度が低下して動作不能になるなど、必然的にシステムリソースの競合が発生します。

これらの要件を満たさないシステムで製品をインストールおよび実行できる場合がありますが、パフォーマンス要件に基づいて事前の使用テストを実行することをお勧めします。

(1): 感染による損傷が多いコンピューターでメモリが使用されない場合、または大量のデータリストが製品にインポートされているとき(URLホワイトリストなど)には、製品は追加のメモリを使用する可能性があります。
(2): インストーラーをダウンロード、製品をインストール、ロールバック機能をサポートするためにプログラムデータのインストールパッケージと製品アップデートのバックアップのコピーを保存するために必要なディスク領域。別の設定が使用される(追加の製品アップデートバックアップバージョンが保存されるときにメモリダンプまたは大量のログレコードのリストが保持されるなど)場合、または感染したコンピューター(隔離機能のためなど)では、追加のディスク領域が使用される場合があります。オペレーティングシステムのアップデートとESET製品アップデートをサポートするために、十分な空きディスク領域を確保することをお勧めします。
(3): 製品はリムーバブルメディアから手動でアップデートできます(非推奨)。

サポートされている言語

ESET Endpoint Securityは、次の言語でインストールおよびダウンロードできます。

言語	言語コード	LCID
英語(米国)	en-US	1033
アラビア語(エジプト)	ar-EG	3073
ブルガリア語	bg-BG	1026
簡体中国語	zh-CN	2052
繁体中国語	zh-TW	1028
クロアチア語	hr-HR	1050
チェコ語	cs-CZ	1029
エストニア語	et-EE	1061
フィンランド語	fi-FI	1035
フランス語(フランス)	fr-FR	1036
フランス語(カナダ)	fr-CA	3084
ドイツ語(ドイツ)	de-DE	1031
ギリシャ語	el-GR	1032
*ヘブライ語	he-IL	1037
ハンガリー語	hu-HU	1038
*インドネシア語	id-ID	1057
イタリア語	it-IT	1040
日本語	ja-JP	1041
カザフスタン語	kk-KZ	1087
韓国語	ko-KR	1042

言語	言語コード	LCID
*ラトビア語	lv-LV	1062
リトアニア語	lt-LT	1063
オランダ語	nl-NL	1043
ノルウェー語	nn-NO	1044
ポーランド゛語	pl-PL	1045
ポルトガル語(ブラジル)	pt-BR	1046
ルーマニア語	ro-RO	1048
ロシア語	ru-RU	1049
スペイン語(チリ)	es-CL	13322
スペイン語(スペイン)	es-ES	3082
スウェーデン語(スウェーデン)	sv-SE	1053
スロバキア語	sk-SK	1051
スロヴェニア語	sl-SI	1060
タイ語	th-TH	1054
トルコ語	tr-TR	1055
ウクライナ語(ウクライナ)	uk-UA	1058
*ベトナム語	vi-VN	1066

* ESET Endpoint Securityはこの言語で提供されていますが、オンラインユーザーガイドは提供されていません(英語版にリダイレクトされます)。

このオンラインユーザーガイドの言語を変更するには、言語選択ボックスを確認してください(右上端).

セキュリティの考え方

コンピュータを使用するとき、特にインターネットを利用する場合には、攻撃や検出とリモート攻撃の危険を完全に排除できるウイルス対策システムは存在しないということを忘れないでください。最大限の保護と利便性を提供するには、ウイルス対策ソリューションを正しく試用し、複数の役立つルールに従うことが重要です。

定期的にアップデートする

ESET LiveGrid®の統計データによると、既存のセキュリティ手段をすり抜けマルウェアの作成者に利益をもたらすために、毎日数千種類のマルウェアが新たに作成されています。この利益は、他のユーザーの犠牲の上に成り立っています。ESETのウイルスラボの担当者は、ユーザーの保護レベルを改善するために、これらのウイルスを毎日解析し、更新ファイルを作成してリリースしています。これらの最新版の効果を最大限生かすためには、システムのアップデートを正しく設定することが重要です。アップデートの設定方法の詳細は、「アップデートの設定」の章を参照してください。

セキュリティパッチをダウンロードする

多くの場合、悪意のあるソフトウェアの作成者はシステムのさまざまな脆弱性を悪用します。それは、悪意のあるコードを効率的に蔓延させるためです。これを念頭に、ソフトウェアベンダ各社は、アプリケーションの脆弱性が表面化しないかどうかを注意深く見守り、潜在的な脅威を排除するためにセキュリティ更新ファイル(セキュリティパッチ)を定期的にリリースします。これらのセキュリティ更新ファ

イルは、リリースされたらすぐにダウンロードすることが重要です。例えばMicrosoft Windows やInternet ExplorerなどのWebブラウザは、更新ファイルが定期的にリリースされています。

重要なデータをバックアップする

マルウェアの作成者がユーザーに配慮することは、ほとんどありません。悪意のあるプログラムが、オペレーティングシステムの誤作動を引き起こし、重要なデータを喪失させることがよくあります。重要なデータや機密データは、DVDや外付けハードディスクなどの外部メディアに定期的にバックアップすることが重要です。これにより、システム障害が発生したときでもデータを簡単にすばやく復旧できます。

コンピュータにウイルスがいないか定期的にスキャンする

既知や未知のウイルス、ワーム、トロイの木馬、およびルートキットは、リアルタイムファイルシステム保護機能によって処理されます。これにより、ファイルにアクセスするかファイルを開くたびに、マルウェアの活動を検査します。ただし、マルウェアのシグネチャは変化することがあり、検出エンジンは毎日更新されるため、少なくとも1か月に1回はコンピュータの完全な検査を実行することをお勧めします。

基本的なセキュリティルールに従う

常に用心することこそ、あらゆるルールの中で最も有益で効果的なルールです。今日の多くのマルウェアは、ユーザーが操作しないと、実行されず蔓延しません。新しいファイルを開くときに注意すれば、感染した場合にマルウェアを駆除するために多大な時間と労力を費やさずに済みます。次に、いくつかの有益なガイドラインを示します。

- ポップアップや点滅する広告がいくつも表示される、怪しいWebサイトにはアクセスしない。
- フリーウェアやコーデックパックのインストール時には注意する。安全なプログラムだけ使用し、安全なWebサイトにだけアクセスする。
- メールの添付ファイルを開くときに注意する。特に、大量に送信されたメッセージや知らない送信者からのメッセージの添付ファイルに注意する。
- 日々の作業では、コンピュータの管理者アカウントを使用しない。

ヘルプページ

ESET Endpoint Securityヘルプへようこそ。ここに示された情報を参照することで、製品の理解を深めることができ、コンピュータの安全性を高めることができます。

はじめに

ESET Endpoint Securityを使用する前に、この製品はESET Security Management Center経由での接続または単独で使用できることにご留意ください。また、コンピューターの使用時に発生する可能性がある、さまざまなタイプの侵入とリモート攻撃について、十分に理解することをお勧めします。

このバージョンのESET Endpoint Securityに導入された機能の詳細については、「新機能」を参照してください。ESET Endpoint Securityの基本設定とカスタマイズに便利なガイドもご用意しました。

ESET Endpoint Securityヘルプページの使用方法

ヘルプトピックは、位置付けやコンテキストをわかりやすくするために、複数の章と節に分割されています。関連する情報は、ヘルプページ構造を見るだけで見つけることができます。

プログラムで表示されるウィンドウについての説明を見るには、**F1**キーを押してください。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。

ヘルプページを検索するには、キーワードを使用するか、単語またはフレーズを入力します。キーワード検索では、その特定のキーワードが本文中に出てこないヘルプページでも、論理的に関連付けられている場合表示されます。語句による検索では、すべてのページの内容が検索され、その語句が出てくるページだけが表示されます。

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 Endpoint 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。

目を通すことが推奨される注意が必要な項目です。 通常は、重大ではないものの、重要な情報が記載されています。

一層の注意が必要な情報です。 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。

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。

表記規則	意味
太字	ボックスやオプションボタンなどのインターフェイス項目の名前。
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。
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にインストールされたプログラムが保存されるWindowsシステムディレクトリ。

オンラインヘルプはヘルプコンテンツの主なソースです。 インターネットに接続している場合には、最新バージョンのオンラインヘルプが自動的に表示されます。

リモート管理されたエンドポイントのドキュメント

ESETビジネス製品およびESET Endpoint Securityは、1つの集中管理された場所から、ネットワーク接続環境におけるクライアントワークステーション、サーバー、およびモバイルデバイスで、リモート管理できます。10台以上のクライアントワークステーションを管理するシステム管理者は、ESETリモート管理ツールのいずれかを展開すると、1つの集中管理された場所からESETソリューションの展開、タスクの管理、セキュリティポリシーの施行、システムステータスの監視、およびリモートコンピューターでの問題や脅威に対する迅速な対応が可能です。

ESETリモート管理ツール

ESET Endpoint Securityは、ESET Security Management CenterまたはESET Cloud Administratorでリモート管理できます。

- ESET PROTECTの概要
- ESET PROTECT Cloudの概要

サードパーティーのリモート管理ツール

- リモート監視と管理 (RMM)

ベストプラクティス

- ESET Endpoint Securityを使用してすべてのエンドポイントをESET PROTECTに接続する
- 接続されたクライアントコンピューターで、詳細設定を保護し、不正な修正を防止する
- 推奨されたポリシーを適用して、使用可能なセキュリティ機能を施行する
- ユーザーインターフェースを最小化する。ユーザーによるESET Endpoint Securityの操作を制限する。

ガイド

- 上書きモードを使用する方法
- GPOまたはSCCMを使用してESET Endpoint Securityを展開する方法

ESET PROTECTの概要

ESET PROTECTで、ネットワーク接続環境におけるワークステーション、サーバー、モバイルデバイス上のESET製品を1つの集中管理された場所から管理できます。

ESET PROTECT Webコンソールを使用するとESETソリューションの展開、タスクの管理、セキュリティポリシーの施行、システムステータスの監視、リモートコンピューターでの問題や検出への迅速な対応ができます。ESET PROTECTアーキテクチャおよびインフラストラクチャ要素の概要ESET PROTECT Webコンソールの基本サポートされているデスクトッププロビジョニング環境を参照してください。

ESET PROTECTは次のコンポーネントで構成されています。

- ESET PROTECT サーバー - ESET PROTECTサーバーはWindowsとLinuxにインストールでき、仮想アプライアンスとして付属しています。エージェントとの通信を処理し、アプリケーションデータを収集し、データベースに保存します。

- ESET PROTECT Webコンソール - ESET PROTECT Webコンソールは、環境内のクライアントコンピューターを管理できるメインのインターフェースです。ネットワーク上のクライアントについてステータスの概要を表示し、管理対象外のコンピューターにリモートでESETソリューションを展開できますESET PROTECTサーバーをインストールすればWebブラウザーを使用してWebコンソールにアクセスできますWebサーバーをインターネット上で公開すると、インターネットに接続されているすべての場所とデバイスからESET PROTECTを使用できます。

- ESET Managementエージェント - ESET Managementエージェントは、ESET PROTECTサーバーとクライアントコンピューターの間の通信を容易にします。コンピューターとESET PROTECTサーバーの間の通信を確立するには、エージェントをクライアントコンピューターにインストールする必要があります。そうすれば、クライアントコンピューター上のESET Managementエージェントを使用することになって複数のセキュリティシナリオを保存できるため、新しい検出への対応時間が大幅に短くなります。ESET PROTECTWebコンソールを使用すると、Active DirectoryまたはESET RD Sensorで特定された管理対象外のコンピューターに、ESET Managementエージェントを展開できます。また、必要に応じて、クライアントコンピューターに、ESET Managementエージェントを手動でインストールできます。

- Rogue Detection Sensor - ESET PROTECT Rogue Detection (RD) Sensorは、ネットワークに存在する管理されていないコンピュータを検出し、その情報をESET PROTECTサーバーに送信します。これにより、新しいクライアントコンピュータを保護されたネットワークに容易に追加できます。RD Sensorは検出されたコンピュータを記憶し、同じ情報を2回送信しません。

- Apache HTTP Proxy - ESET PROTECTと組み合わせて使用できるサービスで、

  oクライアントコンピュータにアップデートを配布し、ESET Managementエージェントにインストールパッケージを配布します。

  oESET Managementエージェントから ESET PROTECTサーバーに通信を転送します。

- モバイルデバイスコネクター - ESET PROTECTでモバイルデバイス管理を可能にするコンポーネントであり、モバイルデバイス(AndroidおよびiOS)を管理し、ESET Endpoint Security for Androidを管理できます。

- ESET PROTECT仮想アプライアンス - ESET PROTECT VAは、仮想環境でESET PROTECTを実行したいユーザを対象にしています。。

- ESET PROTECT仮想エージェントホスト - ESET PROTECTのコンポーネントであり、エージェントレス仮想マシンの管理ができるように、エージェントエンティティを仮想化します。このソリューションにより、自動化、動的グループの利用、物理コンピューターのESET Managementエージェントと同じレベルのタスク管理が可能になります。仮想エージェントは仮想マシンから情報を収集し、ESET PROTECTサーバーに送信します。

- ミラーツール – ミラーツールは、オフラインモジュールアップデートで必要です。クライアントコンピュータがインターネットに接続しない場合、ミラーツールを使用してESETアップデートサーバーからアップデートファイルをダウンロードし、ローカルに保存できます。

- ESET Remote Deployment Tool – このツールでは<%PRODUCT%>ESET_PROTECT Webコンソールで作成されたオールインワンパッケージを展開できます。ネットワーク上のコンピュータでESET Managementエージェントと ESET製品を配布するための便利な方法です。

- ESET Business Account - ESETビジネス製品向けの新しいライセンスポータルでは、ライセンスを管理できます。製品をアクティベーションする手順については、このドキュメントのESET Business Accountセクションを参照してください。ESET Business Accountの使用の詳細については、ESET Business Accountユーザーガイドを参照してください。すでにESETが発行したユーザー名とパスワードがあり、製品認証キーに変換する場合には、「レガシーライセンス資格情報の変換」セクションを参照してください。

- ESET Enterprise Inspector – 包括的なエンドポイント検出および応答システムであり、インシデント検出、インシデント管理と応答、データ収集、危険検出の指標、特異性の検出、動作検出、ポリシー違反などの機能があります。

ESET PROTECT Webコンソールを使用してESETソリューションの展開、タスクの管理、セキュリティポリシーの施行、システムステータスの監視、リモートコンピューターでの問題や脅威に対する迅速な対

応ができます。

詳細については、ESET PROTECTオンラインユーザーガイドをご覧ください。

ESET PROTECT Cloudの概要

ESET PROTECT CloudではESET PROTECTやESMCなどの物理または仮想サーバーを必要とせずに、ネットワーク環境におけるワークステーションおよびサーバー上のESET製品を、集中管理された1つの場所から管理できますESET PROTECT Cloud Webコンソールを使用すればESETソリューションの展開、タスクの管理、セキュリティポリシーの施行、システムステータスの監視、リモートコンピューターでの問題や脅威への迅速な対応が可能です。

- ESET PROTECT Cloudオンラインユーザーガイドをお読みください

設定をパスワードで保護する

システムのセキュリティを最大化するにはESET Endpoint Securityを正しく設定する必要があります。適正ではない変更や設定は、クライアントセキュリティや保護レベルの低下につながるおそれがあります。詳細設定へのユーザーアクセスを制限するために、管理者は、設定をパスワードで保護することができます。

管理者は、接続されたクライアントコンピューターのESET Endpoint Securityの詳細設定をパスワードで保護するためのポリシーを作成できます。新しいポリシーを作成するには、次の手順に従います。

1. ESET PROTECT WebコンソールまたはESMC Webコンソールで、左側のメインメニューで**ポリシー**をクリックします。

2. **新しいポリシー**をクリックします。

3. 新しいポリシーの名前を指定し、任意で簡単な説明を指定します。**続行**ボタンをクリックします。

4. 製品のリストから、**ESET Endpoint for Windows**を選択します。

5. 設定リストの**ユーザーインターフェース**をクリックし、**アクセス設定**を展開します。

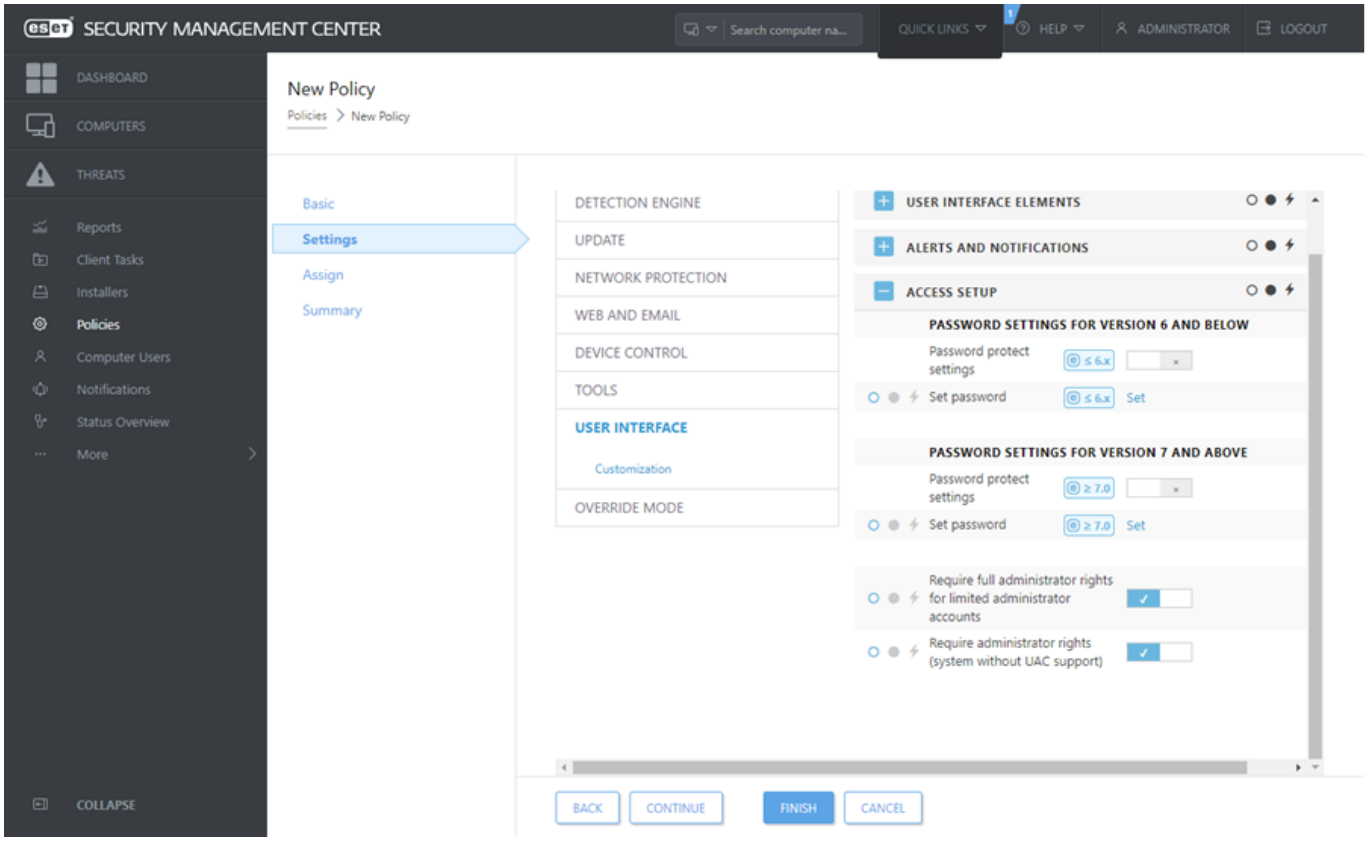
6. ESET Endpoint Securityのバージョンに従い、サイドバーをクリックして、**設定を保護するパスワード**を有効にしますESETEndpoint製品バージョン7では、保護が強化されています。バージョン7とバージョン6 の両方のEndpoint製品をネットワークで使用している場合は、各バージョンに別のパスワードを使用して2つの別のポリシーを作成することをお勧めします。

7. ポップアップウィンドウで、新しいパスワードを作成し、確認して、**OK**をクリックします。**続行**をクリックします。

8. ポリシーをクライアントに割り当てます。**割り当て**をクリックし、パスワードで保護するコンピュータまたはコンピュータのグループを選択します。**OK**をクリックして確認します。

9.すべての目的のクライアントコンピュータがターゲットリストにあることを確認し、**続行**をクリックします。

10. サマリーでポリシー設定を確認し、**完了**をクリックして、新しいポリシーを保存します。



ポリシーの概要

管理者は、ESET PROTECT WebコンソールまたはESMC Webコンソールから、ポリシーを使用して、クライアントコンピューターで実行されるESET製品に特定の設定をプッシュすることができます。ポリシーは、直接個別のコンピューターやコンピューターのグループに適用できます。また、複数のポリシーをコンピューターまたはグループに割り当てることができます。

ユーザーが新しいポリシーを作成するには、次の権限が必要です。**読み取り**権限は、ポリシーのリストを読み取ります。**使用**権限は、ポリシーをターゲットコンピュータに割り当てます。**書き込み**権限は、ポリシーを作成、修正、または編集します。

ポリシーは、静的グループの配置順に適用されます。これは、ポリシーが最初に子動的グループに適用される、動的グループには当てはまりません。これにより、より大きい影響度でポリシーをグループツリーの最上位に適用し、より固有のポリシーをサブグループに適用できます。フラグを使用すると、ツリーの上位にあるグループにアクセスできるESETEndpointSecurityユーザーは、下位のグループのポリシーを上書きできます。このアルゴリズムについては、ESETPROTECTオンラインヘルプを参照してください。

i グループツリーの上位にあるグループには、より汎用的なポリシー(アップデートサーバーポリシーなど)を割り当てることをお勧めします。より特定のポリシー(デバイスコントロール設定など)はグループツリーの下位に割り当てられます。通常、マージ時に下位のポリシーが上位の設定を上書きします(ポリシーフラグで定義されている場合を除く)。

ポリシーのマージ

通常、クライアントに適用されたポリシーは、複数のポリシーが1つの最終ポリシーにマージされたものです。ポリシーは1つずつマージされます。ポリシーをマージするときの原則は、後のポリシーによって、前のポリシーで構成された設定が必ず置換されるということです。この動作を変更するには、ポリシーフラグ(各設定で使用可能)を使用できます。

ポリシーを作成するときには、一部の設定には設定できる追加ルール(置換/後に追加/前に追加)があります。

- **置換** – リスト全体が置換され、新しい値が追加されて、すべての以前の値が削除されます。
- **後に追加** – 項目は現在適用されているリストの最後に追加されます(別のポリシーである必要があります。ローカルリストは常に上書きされます)。
- **前に追加** – 項目はリストの先頭に追加されます(ローカルリストは上書きされます)。

ESET Endpoint Securityは、新しい方法でリモートポリシーとローカル設定のマージをサポートします。設定がリスト(ブロックされたWebサイトのリストなど)で、ポリシーが既存のローカル設定と競合している場合、リモートポリシーが優先されます。ローカルリストとリモートリストを結合する方法を選択するには、別のマージルールを選択します。

- リモートポリシーの設定のマージ。
- リモートおよびローカルポリシーのマージ – ローカル設定を結果のリモートポリシーでマージ。

ポリシーのマージの詳細については、ESET PROTECTオンラインユーザーガイドに従い、例を参照してください。

フラグの仕組み

通常、クライアントコンピュータに適用されるポリシーは、1つの最終ポリシーにマージされる複数のポリシーの結果です。ポリシーをマージするときには、適用されるポリシーの順序のため、ポリシーフラグを使用して、最終ポリシーの想定される動作を調整できます。フラグは、ポリシーが特定の設定を処理する方法を定義します。

各設定に対して、次のフラグのいずれかを選択できます。

未適用	このフラグの設定はポリシーによって設定されていません。設定はポリシーによって設定されていないため、後から適用される他のポリシーで変更できます。
適用	**適用**フラグが付いた設定は、クライアントコンピューターに適用されます。ただし、ポリシーをマージするときには、後から適用される他のポリシーによって上書きされることがあります。このフラグが付いた設定を含むクライアントコンピューターにポリシーが送信されるときには、これらの設定により、クライアントコンピューターのローカル設定が変更されます。設定は強制ではないため、後から適用される他のポリシーによって変更されることがあります。
強制	**強制**フラグが付いた設定は優先度があり、(**強制**フラグがある場合でも)後から適用されるどのポリシーによっても上書きされることはありません。これにより、後から適用される他のポリシーがマージ中にこの設定を変更できないことが保証されます。このフラグが付いた設定を含むクライアントコンピューターにポリシーが送信されるときには、これらの設定により、クライアントコンピューターのローカル設定が変更されます。

シナリオ:管理者はユーザー*John*がホームグループのポリシーを作成または編集し、 強制フラグが付いたポリシーを含む、管理者が作成したすべてのポリシーを表示できるようにします。管理者は、*John*がすべてのポリシーを表示できるようにしますが、管理者が作成した既存のポリシーの編集は許可しません。*John*は、ホームグループSan Diego内でのみ、ポリシーを作成または編集できます。

解決策: 管理者は次の手順に従います。

カスタム静的グループと権限設定の作成

1. 新しい静的グループの*San Diego*を作成します。
2. 静的グループすべてへのアクセスと**ポリシー**の**読み取り**権限がある新しい権限設定の*Policy - All John*を作成します。
3. 静的グループ*San Diego*へのアクセスと**グループとコンピュータ**と**ポリシー**の**書き込み**権限がある新しい権限設定の*Policy John*を作成します。この権限設定により、*John*は、ホームグループ*San Diego*でポリシーを作成または編集できます。
4. 新しいユーザー*John*を作成し、 **権限**設定セクションで、*Policy - All John*と*Policy John*を選択します。

ポリシーの作成

5. 新しいポリシー*All- Enable Firewall*を作成し、 **設定**セクションを展開し、**ESET Endpoint for Windows**を選択して、**ネットワーク保護 > 基本**に移動して、 強制フラグですべての設定を適用します。 **割り当て**セクションを展開し、静的グループ*All*を選択します。
6. 新しいポリシー*John Group- Enable Firewall*を作成し、**設定**セクションを展開し、**ESET Endpoint for Windows**を選択して、**パーソナルファイアウォール > 基本**に移動して、 適用フラグですべての設定を適用します。**割り当て**セクションを展開し、静的グループ*San Diego*を選択します。

結果

強制フラグがポリシー設定に適用されたため、管理者が作成したポリシーは最初に適用されます。強制フラグが適用された設定は優先度があり、後から適用される別のポリシーで上書きできません。ユーザー*John*が作成したポリシーは、管理者が作成したポリシーの後に適用されます。最終ポリシー順序を確認するには、**詳細 > グループ > San Diego**に移動します。コンピュータを選択して、**詳細の表**示を選択します。**設定**セクションで、**適用されたポリシー**をクリックします。

単独でのESET Endpoint Securityの使用

ユーザーガイドのこのセクションとESET Endpoint Securityの操作セクションは、ESET PROTECTESET Security Management CenterまたはESET PROTECT CloudESET Endpoint Securityを使用せずにESET Endpoint Securityを使用するユーザー向けです。ユーザーのアカウント権限に応じてESET Endpoint Securityのすべての機能を使用できます。

インストール方法

ESET PROTECTESET Security Management CenterまたはESET PROTECT CloudESET Endpoint Securityをリモートでクライアントワークステーションに展開していないかぎり、クライアントワークステーションではESET Endpoint Securityバージョン8.xをインストールするための複数の方法があります。

- バージョン6.6.xへのESET Endpoint Securityのインストールまたはアップグレード

検査方法	目的	ダウンロードリンク

検査方法	目的	ダウンロードリンク
ESET AV Removerでインストール	ESET AV Removerヘルプツールを使用すると、インストールを続行する前に、以前にシステムにインストールしたほぼすべてのウイルス対策ソフトウェアを削除できます。	64ビットのダウンロード 32ビットのダウンロード
*** インストール (.exe)	ESET AV Removerを使用しないインストール処理	N/A
インストール (.msi)	ビジネス環境では.msiインストーラーが推奨されるインストールパッケージです。これは、主に、オフラインおよびリモート展開がESET Security Management Centerなどのさまざまなツールを使用するためです。	64ビットのダウンロード 32ビットのダウンロード
コマンドラインインストール	ESET Endpoint Securityは、コマンドラインでローカルにインストールするかESET PROTECTまたはESET Security Management Centerからのクライアントタスクを使用してリモートでインストールできます。	N/A
GPOまたはSCCMを使用した展開	GPOやSCCMなどの管理ツールを使用してESET Management AgentおよびESET Endpoint Securityをクライアントワークステーションに展開します。	N/A
RMMツールを使用した展開	Remote Management and Monitoring (RMM)ツール向けのESET DEMプラグインではESET Endpoint Securityをクライアントワークステーションに展開できます。	N/A

ESET Endpoint Securityは30種類以上の言語で提供されています。

ESET AV Removerでインストール

インストール処理を続行する前に、コンピュータ上の既存のセキュリティアプリケーションをアンインストールすることが重要です。**ESET AV Removerを使用して不要なセキュリティ製品をアンインストールする**の横のチェックボックスを選択し、ESETAVRemoverでシステムを検査し、サポートされているセキュリティアプリケーションを削除します。チェックボックスをオフにして、**続行**をクリックするとESET AV Removerを実行せずにESET Endpoint Securityをインストールします。



ESET AV Remover

ESET AV Removerツールを使用すると、以前にシステムにインストールしたほぼすべてのウイルス対策ソフトウェアを削除できます。次の手順に従い、ESET AV Removerを使用して既存のウイルス対策プログラムを削除します。

1. ESET AV Removerで削除できるウイルス対策ソフトウェアの一覧については、ESETナレッジベース記事を参照してください。

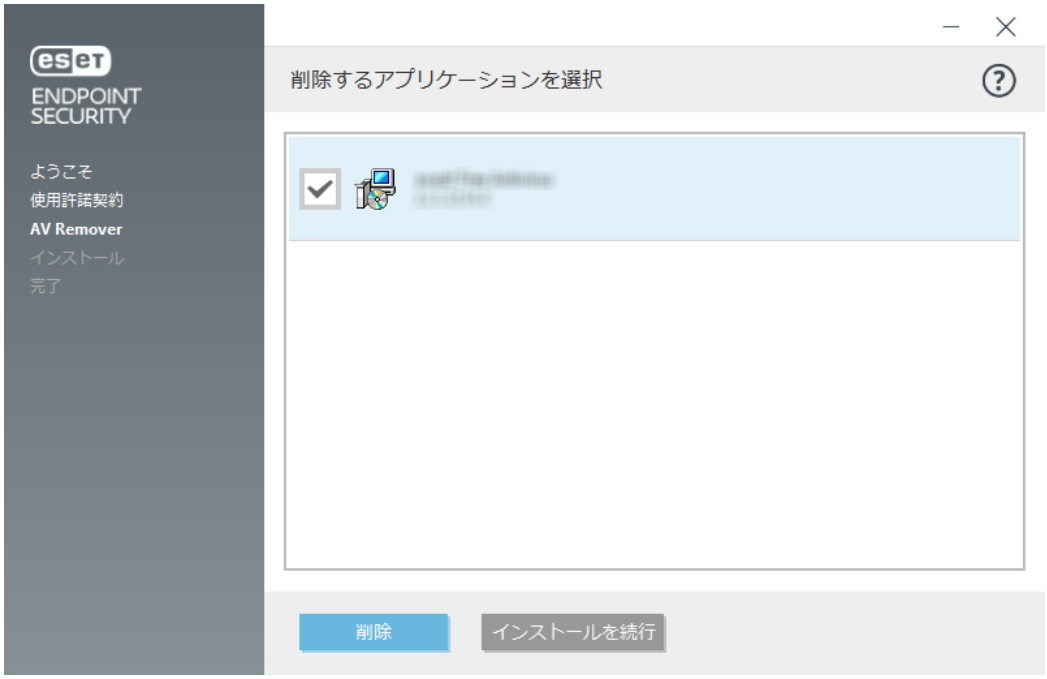
2. エンドユーザーライセンス契約を読んで[**同意する**]をクリックし、承諾することを確認します。[**同意しない**]をクリックすると、コンピュータ上の既存のセキュリティアプリケーションを削除せずにESET Endpoint Securityのインストールを続行します。



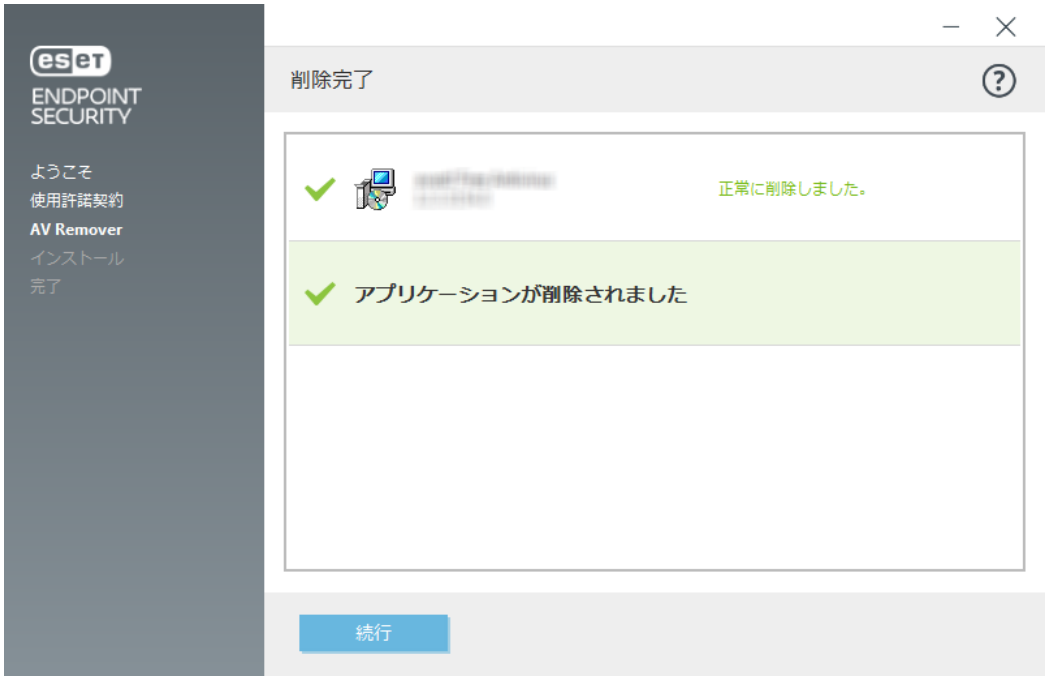
3. ESET AV Removerがシステムのウイルス対策ソフトウェアを検索し始めます。



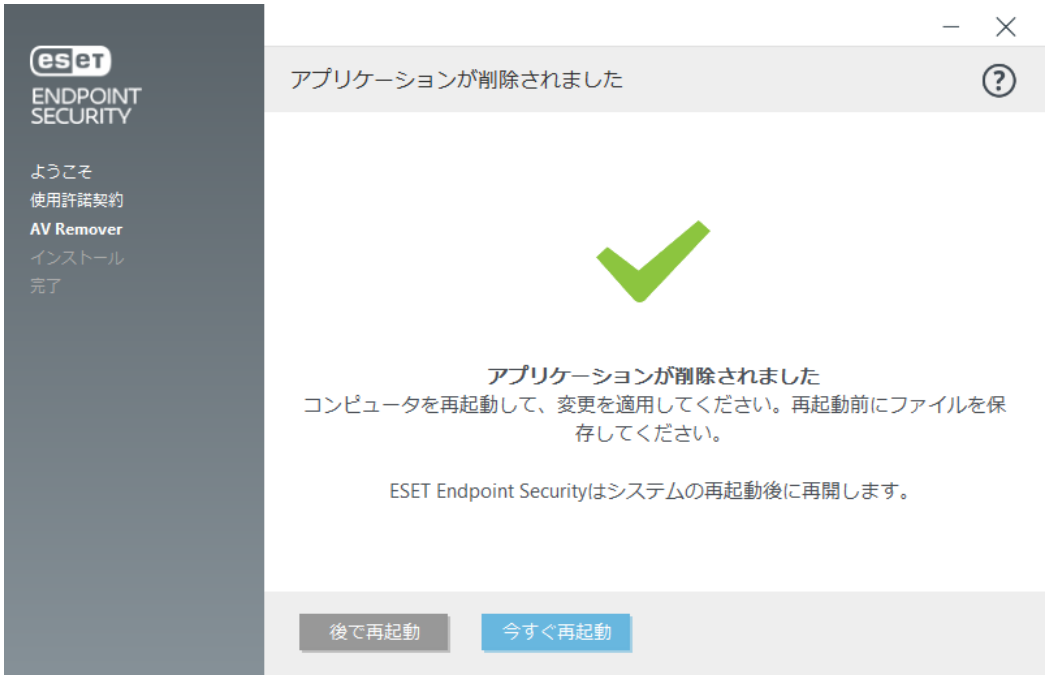
4. 一覧のウイルス対策アプリケーションを選択し、[**削除**]をクリックします。削除にはしばらくかかる場合があります。



5. 削除が成功したら、[**続行**]をクリックします。



6. コンピュータを再起動して変更を適用し、ESET Endpoint Securityのインストールを続行します。アンインストールが失敗した場合は、このガイドの「ESET AV Removerによるアンインストールがエラーで終了した場合」を参照してください。



ESET AV Removerによるアンインストールがエラーで終了した場合

ESET AV Removerを使用してウイルス対策プログラムを削除できない場合は、削除しようとしているアプリケーションがESET AV Removerによってサポートされていない可能性があるという通知が表示されます。ESETナレッジベースのサポートされている製品の一覧または一般的なWindowsウイルス対策ソフトウェアのアンインストーラを参照して、この特定のプログラムを削除できるかどうかを確認してください。

セキュリティ製品のアンインストールが失敗した場合や、コンポーネントの一部が部分的にアンインス

トールされなかった場合は、**再起動して再検査**するように指示されます。起動後にUACを確認し、検査とアンインストール処理を続行します。

必要に応じて、ESETテクニカルサポートに連絡してサポート申請を行い、**AppRemover.log**ファイルを提出してESET技術者を支援します。**AppRemover.log**ファイルは**eset**フォルダにあります。Windowsエクスプローラで*%TEMP%*を参照し、このフォルダにアクセスします。ESETテクニカルサポートはできるかぎり速やかに対応し、問題の解決をお手伝いします。

インストール (.exe)

インストーラーを起動すると.exeインストールウィザードが表示されるので、その案内に従ってインストール処理を行ってください。

コンピュータに他のウイルス対策プログラムがインストールされていないことを確認します。2つ以上のウイルス対策が1台のコンピュータにインストールされている場合、互いに競合する場合があります。システムから他のウイルス対策プログラムをアンインストールすることをお勧めします。一般的なウイルス対策ソフトウェアのアンインストーラツール(英語および他のいくつかの各国語のもの)のリストは、ナレッジベースの記事を参照してください。



1. エンドユーザーライセンス契約を読み、[**同意する**]をクリックし、エンドユーザーライセンス契約を承諾することを確認します。契約に同意したら[**次へ**]をクリックし、インストールを続行します。



2. ESET LiveGrid®を有効にするかどうかを選択しますESET LiveGrid®は、ESETが新しい侵入情報について継続的に即時通知を受けることを保証します。これによって、ユーザーの保護を強化できますESETウイルスラボに新しい脅威を提出するようにし、そこでこれらが解析および処理され、検出エンジンに追加されます。

3. インストールプロセスの次のステップでは、望ましくない可能性があるアプリケーションの検出を設定します。 詳細は、「望ましくない可能性があるアプリケーション」の章を参照してください。

4. 最後の手順は、**インストール**をクリックして、インストールを確認しますESET Endpoint Securityを特定のフォルダーにインストールするには、**インストールフォルダーの変更**をクリックします。インストールが完了した後、ESET Endpoint Securityをアクティベーションするように指示されます。



インストールフォルダの変更(.exe)

望ましくない可能性のあるアプリケーションの検出設定を選択し、**インストールフォルダの変更**をクリックするとESET Endpoint Securityのインストールフォルダを選択するように指示されます。既定では、プログラムは以下のディレクトリにインストールされます。

C:\Program Files\ESET\ESET Security

プログラムモジュールとデータの場所を指定できます。既定では、プログラムは以下のディレクトリにそれぞれインストールされます。

C:\Program Files\ESET\ESET Security\Modules
C:\ProgramData\ESET\ESET Security

場所を変更するには、[**参照**]をクリックします(推奨しません)。



[続行]⍰**[インストール]**の順にクリックすると、インストールを開始します。

インストール (.msi)

.msiインストーラーを起動すると、インストールウィザードが表示されるので、その案内に従ってインストール処理を行ってください。

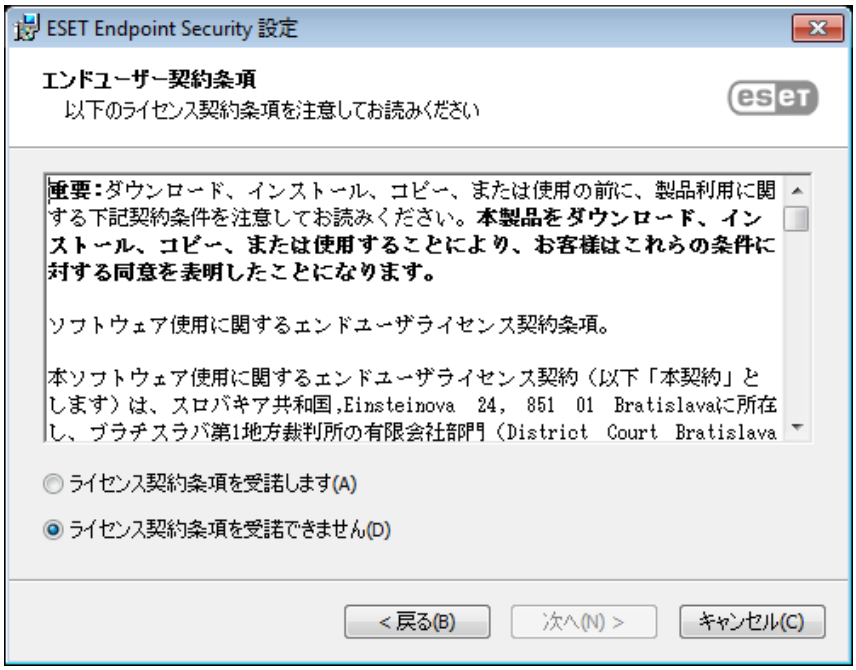
ビジネス環境では⍰.msiインストーラーが推奨されるインストールパッケージです。これは、主に、オフラインおよびリモート展開がESET Security Management Centerなどのさまざまなツールを使用するためです。

コンピュータに他のウイルス対策プログラムがインストールされていないことを確認します。2つ以上のウイルス対策が1台のコンピュータにインストールされている場合、互いに競合する場合があります。システムから他のウイルス対策プログラムをアンインストールすることをお勧めします。一般的なウイルス対策ソフトウェアのアンインストーラツール(英語および他のいくつかの各国語のもの)のリストは、ナレッジベースの記事を参照してください。

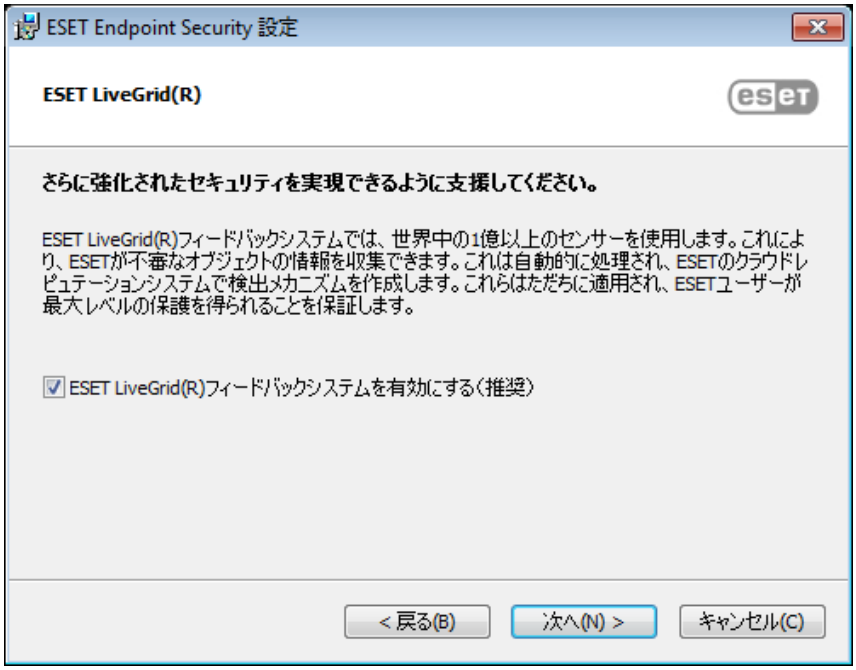
1. 任意の言語を選択し、**次へ**をクリックします。



2. エンドユーザーライセンス契約を読み、[**ライセンス契約条項を受諾します**]をクリックし、エンドユーザーライセンス契約を承諾することを確認します。契約に同意したら[**次へ**]をクリックし、インストールを続行します。

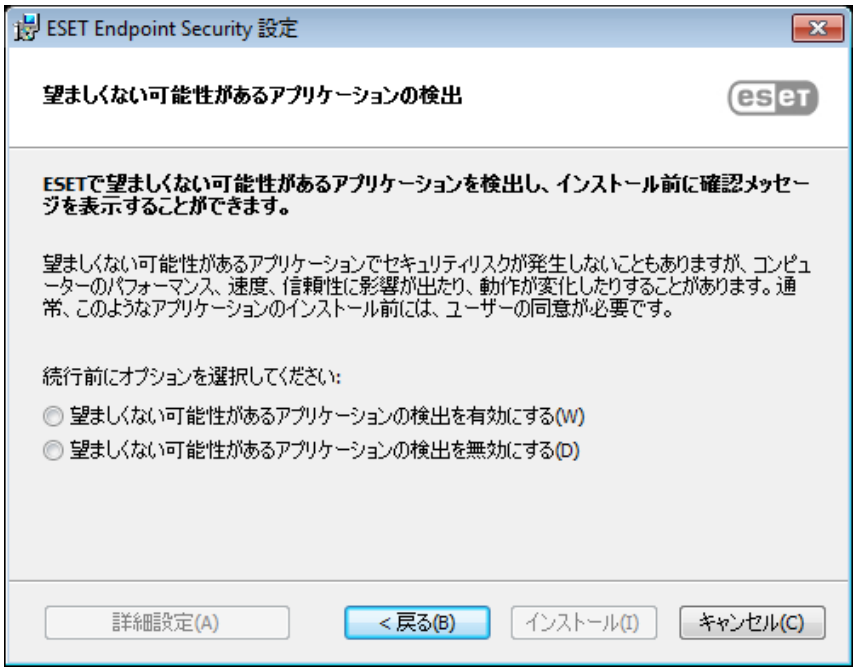


3. ESET LiveGrid®フィードバックシステムの設定を選択します。ESET LiveGrid®は、ESETが新しい侵入情報について継続的に即時通知を受けることを保証します。これによって、ユーザーの保護を強化できます。ESETウイルスラボに新しい脅威を提出するようにし、そこでこれらが解析および処理され、検出エンジンに追加されます。



4. インストールプロセスの次のステップでは、望ましくない可能性があるアプリケーションの検出を設定します。 詳細は、「望ましくない可能性があるアプリケーション」の章を参照してください。

詳細インストール(.msi)を続行する場合は、**詳細設定**をクリックします。



5. 最後の手順は、[**インストール**]をクリックして、インストールを確認します。インストールが完了した後、ESET Endpoint Securityをアクティベーションするように指示されます。

詳細インストール (.msi)

詳細インストールでは、標準インストールでは使用できないさまざまなインストールパラメータをカスタマイズできます。

5. 不審なアプリケーションの検出設定を選択し、[**詳細設定**]をクリックするとESET Endpoint Securityのインストールフォルダーを選択するように指示されます。既定では、プログラムは以下のディレク

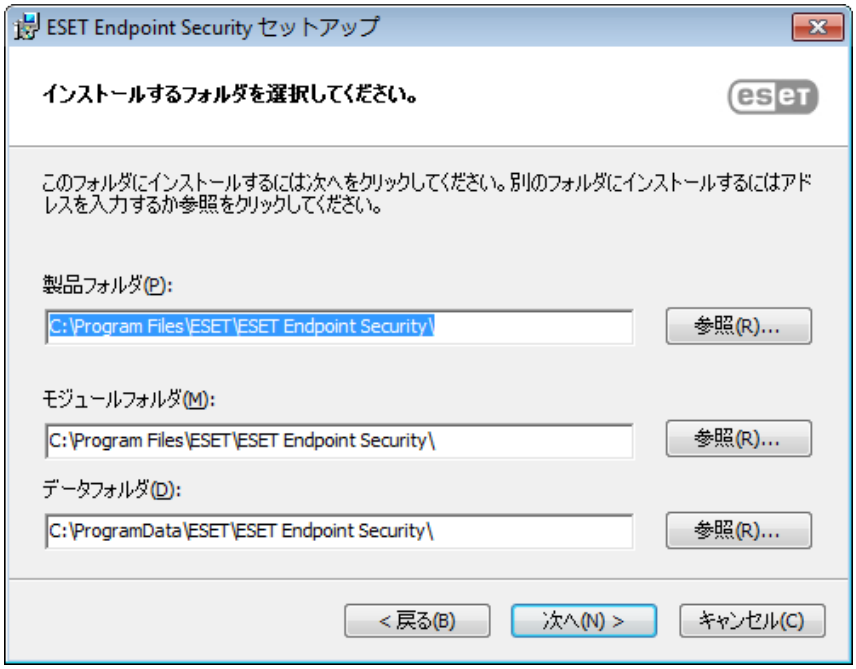
トリにインストールされます。

C:\Program Files\ESET\ESET Security

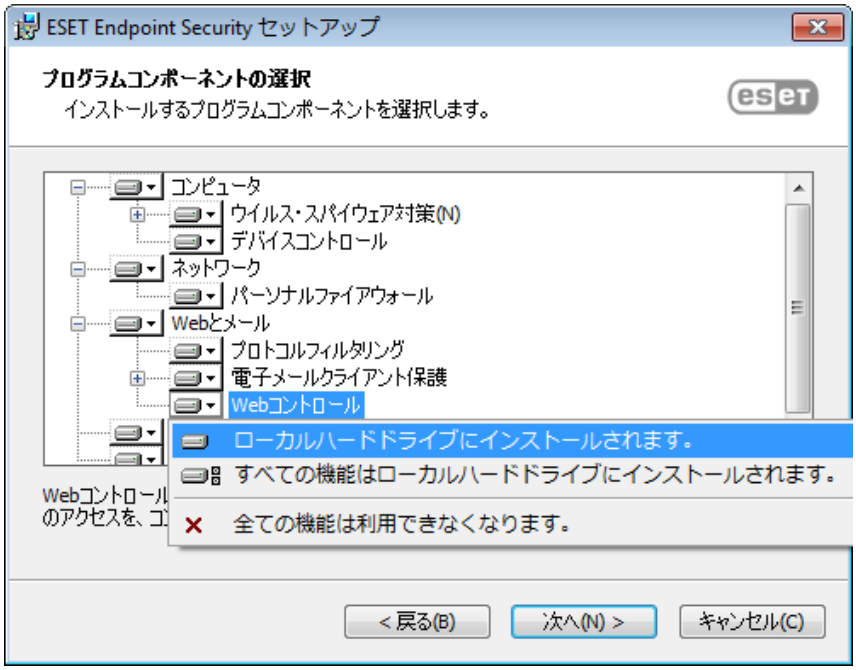
プログラムモジュールとデータの場所を指定できます。既定では、プログラムは以下のディレクトリにそれぞれインストールされます。

C:\Program Files\ESET\ESET Security\Modules
C:\ProgramData\ESET\ESET Security

場所を変更するには、[**参照**]をクリックします(推奨しません)。



6. インストールされる製品コンポーネントを選択します。コンピューターセクションの製品コンポーネントには、リアルタイムファイルシステム保護、コンピューターの検査、ドキュメント保護、およびデバイスコントロールがあります。最初の2つのコンポーネントはセキュリティソリューションの動作のために必要です。ネットワークセクションにはESETファイアウォールをインストールするオプションがあります。これは、すべての送受信トラフィックを監視し、個別のネットワーク接続のルールを適用します。ファイアウォールには、リモートコンピューターからの攻撃に対する保護機能もあります。ネットワーク攻撃保護(IDS)は、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。Webとメールセクションのコンポーネントは、インターネットの閲覧とメール経由での通信中に保護を行います。アップデートミラーコンポーネントは、ネットワークの他のコンピューターをアップデートするために使用できます。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によってアクセスできるローカルで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を監視および制御するプロセスです。



7. 最後の手順では、[**インストール**]をクリックしてインストールを確認します。

コマンドラインインストール

コマンドラインを使用してローカルでESET Endpoint Securityをインストールするか、ESET PROTECTまたはESET Security Management Centerからクライアントタスクを使用してリモートでインストールできます。

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。

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パッケージでの使用方法: `ees_nt64_ENU.msi /qn ADDLOCAL=<list>`

• **ADDLOCAL**プロパティの詳細については、http://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspxを参照してください。

ADDEXCLUDE= <list>

• 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のリストであり、古いREMOVEに代わるものです。

• インストールしない機能を選択するときには、パス全体(すべてのサブ機能など)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パッケージでの使用方法: `ees_nt64_enu.msi /qn ADDEXCLUDE=Firewall,Network`

ADDEXCLUDEは**ADDLOCAL**とともに使用できません。

適切な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、ドキュメントを参照してください。

ルール

• **ADDLOCAL**リストは、インストールされるすべての機能名のカンマ区切り値リストです。

• インストールする機能を選択するときには、パス全体(すべての親機能)が明示的にリストに含まれる必要があります。

• 正しい使用方法については、追加ルールを参照してください。

コンポーネントと機能

ADDLOCAL/ADDEXCLUDEパラメーターを使用したコンポーネントインストールは、ESET Endpoint Antivirusで動作しません。

機能は4つのカテゴリに分類されます。

• **必須** – 機能は常にインストールされます。

• **オプション** – 機能の選択を解除して、インストールされないようにすることができます。

• **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。

• **プレースホルダ** – 製品には影響がない機能。ただし、サブ機能とともにリストに含まれます。

ESET Endpoint Securityの機能セットは次とおりです。

説明	機能名	機能親	存在
基本プログラムコンポーネント	Computer		プレースホルダ
検出エンジン	Antivirus	Computer	必須
検出エンジン/マルウェア検査	Scan	Computer	必須
検出エンジン/リアルタイムファイルシステム保護	RealtimeProtection	Computer	必須

説明	機能名	機能親	存在
検出エンジン/マルウェア検査/ドキュメント保護	DocumentProtection	Antivirus	任意
デバイスコントロール	DeviceControl	Computer	任意
ネットワーク保護	Network		プレースホルダ
ネットワーク保護/ファイアウォール	Firewall	Network	任意
ネットワーク保護/ネットワーク攻撃保護/...	IdsAndBotnetProtection	Network	任意
安全なブラウザー	OnlinePaymentProtection	WebAndEmail	任意
Webとメール	WebAndEmail		プレースホルダ
Webと電子メール/プロトコルフィルタリング	ProtocolFiltering	WebAndEmail	非表示
Webと電子メール/Webアクセス保護	WebAccessProtection	WebAndEmail	任意
Webと電子メール/電子メールクライアント保護	EmailClientProtection	WebAndEmail	任意
Webと電子メール/電子メールクライアント保護/電子メールクライアント	MailPlugins	EmailClientProtection	非表示
Webと電子メール/電子メールクライアント保護/迷惑メール対策保護	Antispam	EmailClientProtection	任意
Webと電子メール/Webコントロール	WebControl	WebAndEmail	任意
ツール/ESET RMM	Rmm		任意
アップデート/プロファイル/アップデートミラー	UpdateMirror		任意
ESET Enterprise Inspectorプラグイン	EnterpriseInspector		非表示

グループ機能セット:

説明	機能名	機能の存在
すべての必須機能	_Base	非表示
すべての使用可能な機能	ALL	非表示

追加ルール

- **WebAndEmail**機能がインストールに選択されている場合、非表示の**ProtocolFiltering**機能をリストに含める必要があります。

- すべての機能の名前は大文字と小文字を区別します。たとえば、UpdateMirrorはUPDATEMIRRORと同じではありません。

構成プロパティのリスト

プロパティ	値	機能
CFG_POTENTIALLYUNWANTED_ENABLED=	0 – 無効 1 – 有効	PUA検出
CFG_LIVEGRID_ENABLED=	以下を参照	以下のLiveGridプロパティを参照
FIRSTSCAN_ENABLE=	0 – 無効 1 – 有効	インストール後にコンピューターの検査をスケジュールして実行
CFG_PROXY_ENABLED=	0 – 無効 1 – 有効	プロキシサーバーの設定
CFG_PROXY_ADDRESS=	<ip>	プロキシサーバのIPアドレス
CFG_PROXY_PORT=	<port>	プロキシサーバーポート番号
CFG_PROXY_USERNAME=	<username>	認証用のユーザー名
CFG_PROXY_PASSWORD=	<password>	認証のパスワード。
ACTIVATION_DATA=	以下を参照	製品のアクティベーション、製品認証キー、またはオフラインライセンスファイル
ACTIVATION_DLG_SUPPRESS=	0 – 無効 1 – 有効	「1」に設定すると、製品のアクティベーションダイアログが最初の起動後に表示されません
ADMINCFG=	<path>	エクスポートされたXML構成へのパス (既定値*cfg.xml*)

ESET Endpoint Securityでのみの設定プロパティ

CFG_EPFW_MODE=	0 – 自動(既定) 1 – 対話モード 2 – ポリシーに基づく 3 – 学習	ファイアウォールフィルタリングモード
CFG_EPFW_LEARNINGMODE_ENDTIME=	<timestamp>	Unixタイムスタンプとしての学習モードの終了日

LiveGrid®プロパティ

ESET Endpoint Securityと CFG_LIVEGRID_ENABLEDをインストールすると、インストール後の製品の動作は次のようになります。

機能	CFG_LIVEGRID_ENABLED=0	CFG_LIVEGRID_ENABLED=1
ESET LiveGrid®レピュテーションシステム	オン	オン
ESET LiveGrid®フィードバックシステム	オフ	オン
匿名で統計情報を送付する	オフ	オン

ACTIVATION_DATAプロパティ

書式	検査方法
ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE	ESET製品認証キーを使用したアクティベーション(インターネット接続が必要)

書式	検査方法
ACTIVATION_DATA=offline:C:\ProgramData\ESET\ESET Security\license.lf	オフラインライセンスファイルを使用したアクティベーション

言語プロパティ

ESET Endpoint Security言語(両方のプロパティを指定する必要があります)

プロパティ	値
PRODUCT_LANG=	LCID10進数(ロケールID)例: 1033は英語(米国。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は英語 – 米国。言語コードの一覧を参照してください。

コマンドラインインストールの例

インストールを実行する前に、エンドユーザーライセンス契約を読んで、管理者権限があることを確認してください。

NetworkProtectionセクションをインストールから除外する(すべての子機能を指定する必要があります):
```
msiexec /qn /i ees_nt64.msi ADDEXCLUDE=Network,Firewall,IdsAndBotnetProtection
```

インストール後にESET Endpoint Securityを自動的に設定する場合は、インストールコマンド内で基本設定パラメーターを指定できます。
ESET LiveGrid®を有効にしてESET Endpoint Securityをインストールする:
```
msiexec /qn /i ees_nt64.msi CFG_LIVEGRID_ENABLED=1
```

既定以外のアプリケーションインストールディレクトリにインストールします。
```
msiexec /qn /i ees_nt64_enu.msi APPDIR=C:\ESET\
```

ESET製品認証キーを使用してESET Endpoint Securityをインストールしてアクティベーションします。
```
msiexec /qn /i ees_nt64_enu.msi ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE
```

詳細ロギング(トラブルシューティングで有用)でサイレントインストール、必須のコンポーネントでのみRMM:
```
msiexec /qn /i ees_nt64.msi /l*xv msi.log ADDLOCAL=_Base,Rmm
```

指定された言語でサイレント完全インストールを強制する。
```
msiexec /qn /i ees_nt64.msi ADDLOCAL=ALL PRODUCT_LANG=1033 PRODUCT_LANG_CODE=en-us
```

インストール後のコマンドラインオプション

- ESETCMD –.xml設定ファイルをインポートするか、セキュリティ機能をオン/オフにします
- コマンドラインスキャナー – コマンドラインからコンピューターの検査を実行します

GPOまたはSCCMを使用した展開

クライアントワークステーションに直接ESET Endpoint Securityをインストールするか、ESMCでサーバータスクを使用してリモート展開する他に、グループポリシーオブジェクト(GPO)ソフトウェアセンター構成マネージャ(SCCM)Symantec Altirisまたは Puppetなどの管理ツールを使用してインストールすることもできます。

管理対象(推奨)

管理されたコンピューターの場合、最初にESET Managementエージェントをインストールしてから ESET Security Management Center (ESMC)経由でESET Endpoint Securityを展開しますESMCはネットワークにインストールする必要があります。

1. ESET Managementエージェント向けのスタンドアロンインストーラーをダウンロードします。

2. GPO/SCCMリモート展開スクリプトを準備します。

3. GPOまたはSCCMを使用してESET Managementエージェントを展開します。

4. クライアントコンピューターがESMCに追加されたことを確認します。

5. ESET Endpoint Securityをコンピューターに展開してアクティベーションします。

次のESETナレッジベース記事は、英語でのみ提供されている場合があります。
- SCCMまたはGPO経由でESET Management Agentを展開する
- グループポリシーオブジェクト(GPO)を使用してESET Management Agentを展開する

最新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 Endpoint Securityの新バージョンが提供されています。

最新バージョンへのアップグレードには、いくつかの方法があります。

1. 自動的にアップグレードしますESET PROTECTESET Security Management Center (ESMC)またはESET PROTECT Cloud. ESET Endpoint Securityバージョン8の使用は、ESET Remote Administratorによって管理できません。

2. 自動的にアップグレードします。GPOまたはSCCMを使用します。

3. 自動で、プログラムアップデートを利用する方法。
プログラムのアップデートはすべてのユーザーに配布されますが、システム設定によっては影響を受ける可能性があります。従って、考えられるどのようなシステム設定でも確実に動作するように、長期間のテストを経て発行されます。 リリース直後の新バージョンにアップグレードする必要がある場合、以下の方法の1つを使用します。
詳細設定(F5) > **アップデート** > **プロファイル** > **プログラムコンポーネントのアップデート**で**アップデートモード**を有効にしたことを確認してください。

4. 手動で、最新バージョンをダウンロードしおよびインストールし、以前のバージョンに上書きイン

ストールします。

推奨アップグレードシナリオ

ESET 製品をリモートで管理する、管理したい

10台を超えるESET Endpoint製品を管理する場合は、ESET PROTECT、ESET PROTECT Cloud、ESMCを使用してアップグレードを処理することを検討してください。

次のドキュメントを参照してください。

- ESET PROTECT | クライアントタスクを使用してESETソフトウェアをアップグレードする
- ESET PROTECT | 最大250のWindows ESET エンドポイント製品を管理する小規模から中規模の企業向けガイド
- ESET PROTECT Cloudの概要

クライアントコンピューターで手動によりアップグレードする

バージョン4.xの上にバージョン8をインストールしないでください。古い/機能しないESET Endpoint Securityバージョン5.xまたは6.x.がある場合にも、バージョン8をインストールしないでください。

個別のクライアントワークステーションで手動によりアップグレードする計画の場合は。

1. オペレーティングシステムがサポートされていることを確認します(Windows VistaおよびWindows XPはこのバージョンでサポートされていません)。

2. 以前のバージョンよりも新しいバージョンをダウンロードしてインストールします。

> 最新バージョン8.xへのアップグレードを正常に実行する可能性を最大化する場合は、次のバージョンのESET Endpoint Securityからアップグレードしてください。
> - 5.0.2272.x
> - 6.5.2132.x
> - 7.3.2044.x
>
> そうでない場合は、最初にESET Endpoint Securityをアンインストールします。クライアントワークステーションでのESET Endpoint Securityのアップグレードの詳細については、次のESETナレッジベース記事をお読みください。

レガシー製品自動アップグレード

ESET製品バージョンはサポートされておらず、製品は最新バージョンにアップグレードされました。

⚠ 一般的なインストールの問題

> ESET製品の新しいバージョンごとに、多くのバグ修正と改良が行われます。ESET製品の有効なライセンスをお持ちのお客様は、同じ製品の最新バージョンに無料でアップグレードできます。

インストールを完了するには:

1. **同意して続行**をクリックして、エンドユーザーライセンス契約に同意し、プライバシーポリシーを確認します。エンドユーザーライセンス契約に同意しない場合は、**アンインストール**をクリックします。以前のバージョンに戻す方法はありません。

2. **すべて許可して続行**をクリックして、ESET LiveGrid®フィードバックシステムを許可するか、参加しない場合は**続行**をクリックします。

3. 製品認証キーを使用して新しいESET製品をアクティベーションすると、ホームページが表示されます。ライセンス情報が見つからない場合は、新しい試用ライセンスで続行します。前の製品で使用されているライセンスが無効な場合は、ESET製品をアクティベーションしてください。

4. インストールを完了するには、デバイスの再起動が必要です。

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 Endpoint Securityのアップデートが必要です。各新しいバージョンのESET Endpoint Securityには、多数の改良やバグ修正が導入されていますESET Endpoint 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 Endpoint 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 Endpoint 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。

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。

一般的なインストールの問題

インストール中に問題が発生した場合、一般的なインストールエラーと解決方法で問題の解決方法を探してください。

アクティベーションに失敗

ESET Endpoint Securityのアクティベーションが失敗した場合、最も一般的な考えられるシナリオは次のとおりです。

- すでに使用されたライセンス
- 無効なライセンスキー。製品のアクティベーションフォームエラーです
- アクティベーションに必要な追加情報がないか無効です
- アクティベーションデータベースとの通信に失敗しました。15分以内にもう一度アクティベーションを試みてください
- ESETアクティベーションサーバーへの接続がないか無効です

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、アクティベーションを再試行してください。

アクティベーションできない場合は、ウェルカムパッケージがアクティベーションとライセンスに関する一般的な質問、エラー、問題について説明します(英語および複数の他の言語で提供されています)。

- ESET製品のアクティベーションのトラブルシューティングを開始

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。

ESETEndpointSecurity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。詳細については、「ESET Endpoint Securityのアクティベーション方法」を参照してください。

コンピュータの検査

定期コンピューターの検査を実行するか、定期検査をスケジュールして、脅威を確認することをお勧めします。メインプログラムウィンドウから[**コンピュータの検査**]をクリックし、[**スマート検査**]をクリックします。コンピュータの検査の詳細は、「コンピュータの検査」セクションを参照してください。



初心者向けガイド

この章ではESET Endpoint Securityの概要とその基本設定について説明します。

ユーザーインターフェイス

ESET Endpoint Securityのメインウィンドウは、2つのセクションに分かれています。右のプライマリウィンドウには、左のメインメニューで選択したオプションに対応する情報が表示されます。

次に、メインメニューにあるオプションについて説明します。

現在の状況 - ESET Endpoint Securityの保護の状態に関する情報が表示されます。

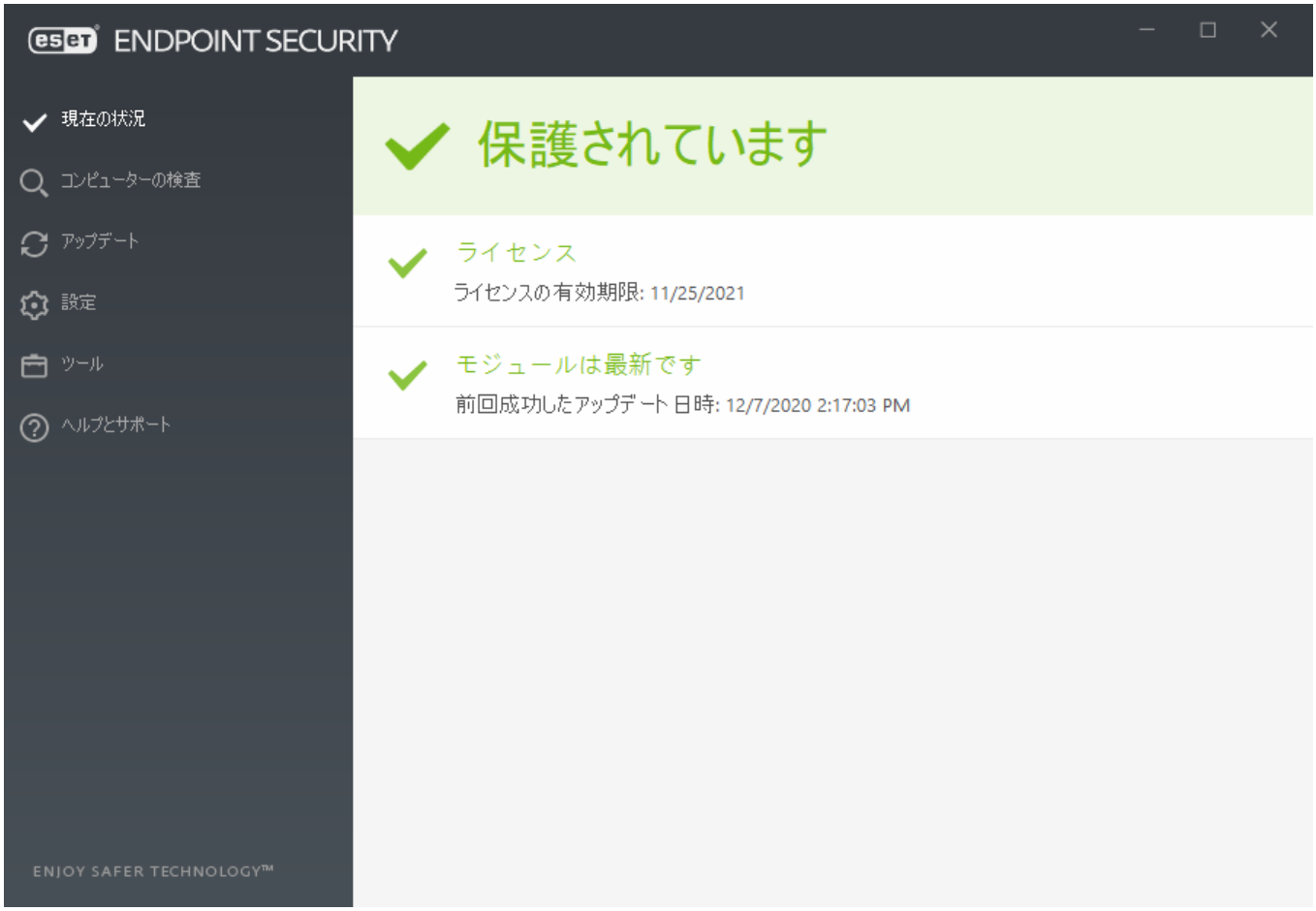
コンピュータの検査 – このオプションを使用すると、スマート検査、カスタム検査、リムーバブルメディア検査の設定や起動を行うことができます。最後に実行された検査を繰り返すこともできます。

アップデート – 検出エンジンについての情報を表示し、手動でアップデートを確認できます。

設定 – このオプションを選択すると、コンピュータ、ネットワーク、Webとメールセキュリティ設定を調整します。

ツール – [ログファイル]、[セキュリティレポート]、[アクティビティの確認]、[実行中のプロセス]、[スケジューラ]、[隔離]、[ネットワーク接続], ESET SysInspectorおよびレスキューCDを作成するためのESET SysRescueにアクセスできます。分析のためにサンプルを送信することもできます。

ヘルプとサポート – ヘルプファイル、ESETナレッジベース、およびESET企業Webサイトにアクセスできます。また、テクニカルサポート依頼、サポートツール、および製品アクティベーション情報へのリンクもあります。



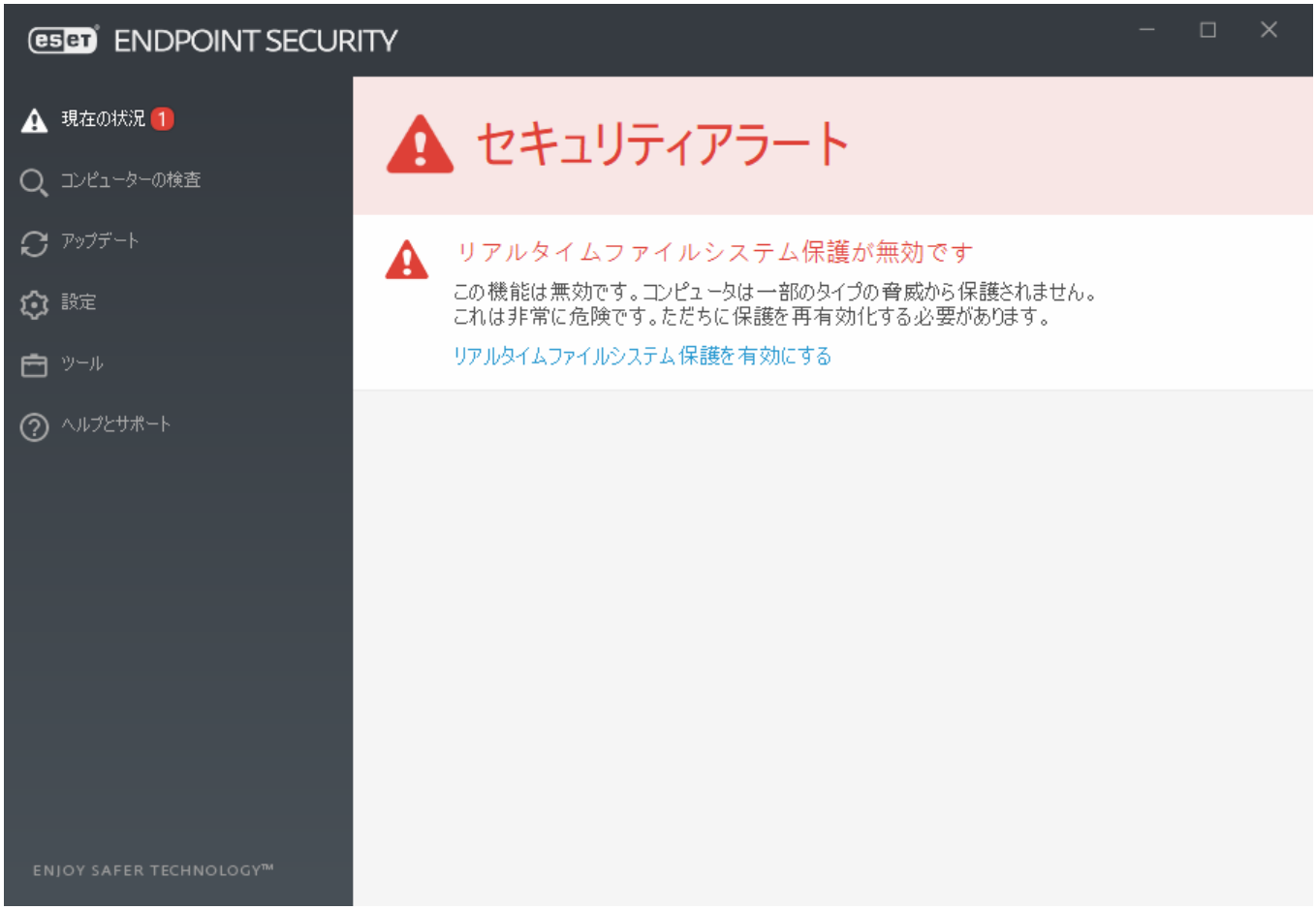
[**現在の状況**]画面で、お使いのコンピュータのセキュリティと現在の保護レベルを知ることができます。緑の保護の状態アイコンは、**最も高い保護**の状態が確保されていることを示します。

ステータスウィンドウにはESET Endpoint Securityで頻繁に使用される機能と前回のアップデート情報へのクイックリンクも表示されます。

プログラムが正しく動作しない場合の解決方法

緑色のチェックマークは、完全に機能するすべてのプログラムモジュールの横に表示されます。赤の「！」マークやオレンジの通知アイコンは、モジュールに注意する必要がある場合に表示されます。完

全な機能を復元する方法に関する推奨事項を含む、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。



赤い感嘆符(!)アイコンはコンピューターの最大の保護が保証されていないことを示します。このタイプの通知は次のシナリオで表示される場合があります。

- **ウイルス・スパイウェア対策は一時停止しています** - [**すべてのウイルス対策をスパイウェア対策モジュールを起動**]をクリックすると、メインプログラムウィンドウの[**現在の状況**]ペインまたは[**設定**]ペインの[**ウイルス対策とスパイウェア対策保護を有効にする**]でウイルス対策とスパイウェア対策保護を再有効化します。

- ウイルス対策機能が機能していません – ウィルススキャナーの初期化が失敗しました。ほとんどのESET Endpoint Securityモジュールは正常に機能しません。

- **フィッシング対策機能が機能していません**– この機能は機能していません。他の必要なプログラムモジュールがアクティブではありません。

- **ESETファイアウォールが無効になっています** – この問題は赤いアイコンで示され、[**ネットワーク**]項目の隣にセキュリティ通知が表示されます。[**フィルタリングモードを有効にする**]をクリックすると、ネットワーク保護を再有効化します。

- **ファイアウォール初期化が失敗しました** – システム統合の問題により、ファイアウォールが無効です。可能なかぎりコンピューターを再起動してください。

- **検出エンジンが最新ではありません** – このエラーは、検出エンジン(旧称「ウイルス定義データベース」)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。

• **製品がアクティベーションされていません**または**ライセンスは有効期限を過ぎています** – 赤色の保護の状態アイコンで示されます。ライセンスの期限が過ぎると、このプログラムではアップデートできなくなります。ライセンスを更新するには、警告ウィンドウの指示に従ってください。

• **ホスト侵入防止システム(HIPS)が無効です** – この問題は、HIPSが詳細設定から無効にされたときに発生します。コンピューターは一部のタイプの脅威から保護されていません。保護を再有効化するには、**[HIPSを有効にする]**をクリックしてください。

• **ESET LiveGrid®が無効です** – この問題は、ESET LiveGrid®が詳細設定で無効にされたときに発生します。

• **定期アップデートがスケジュールされていません** – アップデートタスクをスケジュールしないとESET Endpoint Securityは重要なアップデートを確認または受信しません。

• **アンチステルスは無効です** - **[アンチステルスを有効にする]**をクリックし、この機能を再有効化します。

• **ネットワークアクセスがブロックされました** – ESMCからのこのワークステーションの**コンピューターをネットワークから隔離する**クライアントタスクがトリガーされたときに表示されます。詳細については、システム管理者に連絡してください。

• **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** – リアルタイム保護はユーザーによって無効にされました。コンピューターは脅威から保護されていません。[リアルタイム保護を有効にする]をクリックし、この機能を再有効化します。


オレンジの「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。理由はいくつか考えられます。

• **Webアクセス保護は無効になっています** - Webアクセス保護を再有効化するには、セキュリティ通知をクリックしてから、**[Webアクセス保護を有効にする]**をクリックします。

• **ライセンスの有効期限がまもなく切れます** – これは保護の状態アイコンで示され、エクスクラメーションマークが表示されます。ライセンスの期限が切れたら、プログラムの更新はできなくなり、保護の状態アイコンは赤に変わります。

• **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、この機能を再有効化します。

• **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、この機能を再有効化します。

• **迷惑メール対策保護が一時停止しています** - **[迷惑メール対策保護を有効にする]**をクリックし、この機能を再有効化します。

• **Webコントロールが一時停止しています** - **[Webコントロール有効にする]をクリックし、この機能を再有効化します。**

• **ポリシー上書きアクティブ** – 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。許可されたユーザーのみがポリシー設定を上書きできます。詳細情報については、上書きモードを使用する方法を参照してください。

• **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有効にする]**をクリックし、

この機能を再有効化します。

ESET Endpoint Securityの最初のウィンドウで表示の製品内ステータスを調整するには、アプリケーションステータスを参照してください。

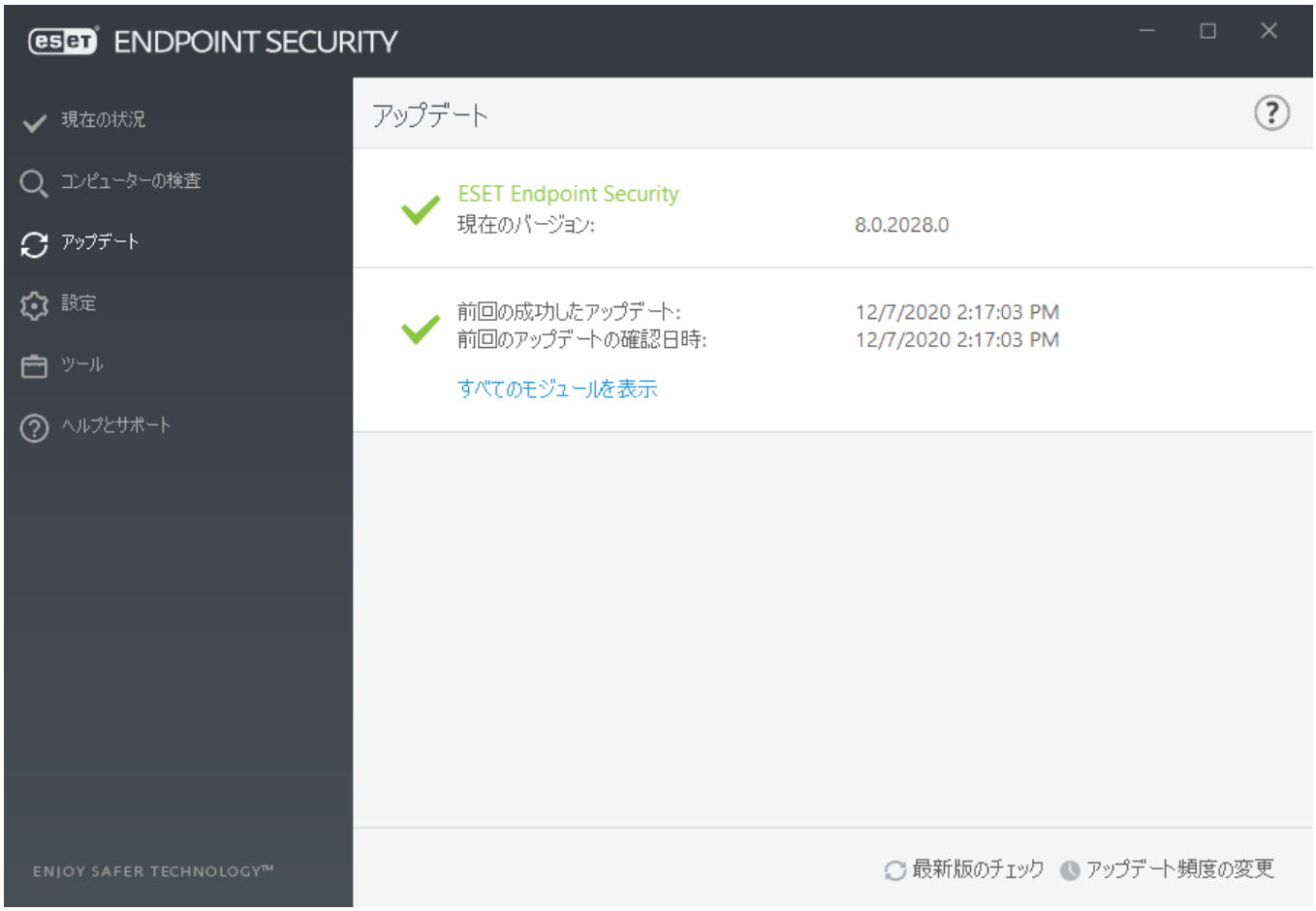
提示された解決策を使用して問題を解決できない場合は、**[ヘルプとサポート]**をクリックしてヘルプにアクセスするか、あるいはESETナレッジベースを検索してください。 問題が解決されない場合は、サポート要求を送信してください。 いただいたご質問にはESETテクニカルサポートが迅速に対応し、解決のお手伝いをいたします。

ステータスがESMCまたはESET PROTECTポリシーによってブロックされる機能に属する場合、リンクをクリックできません。

アップデートの設定

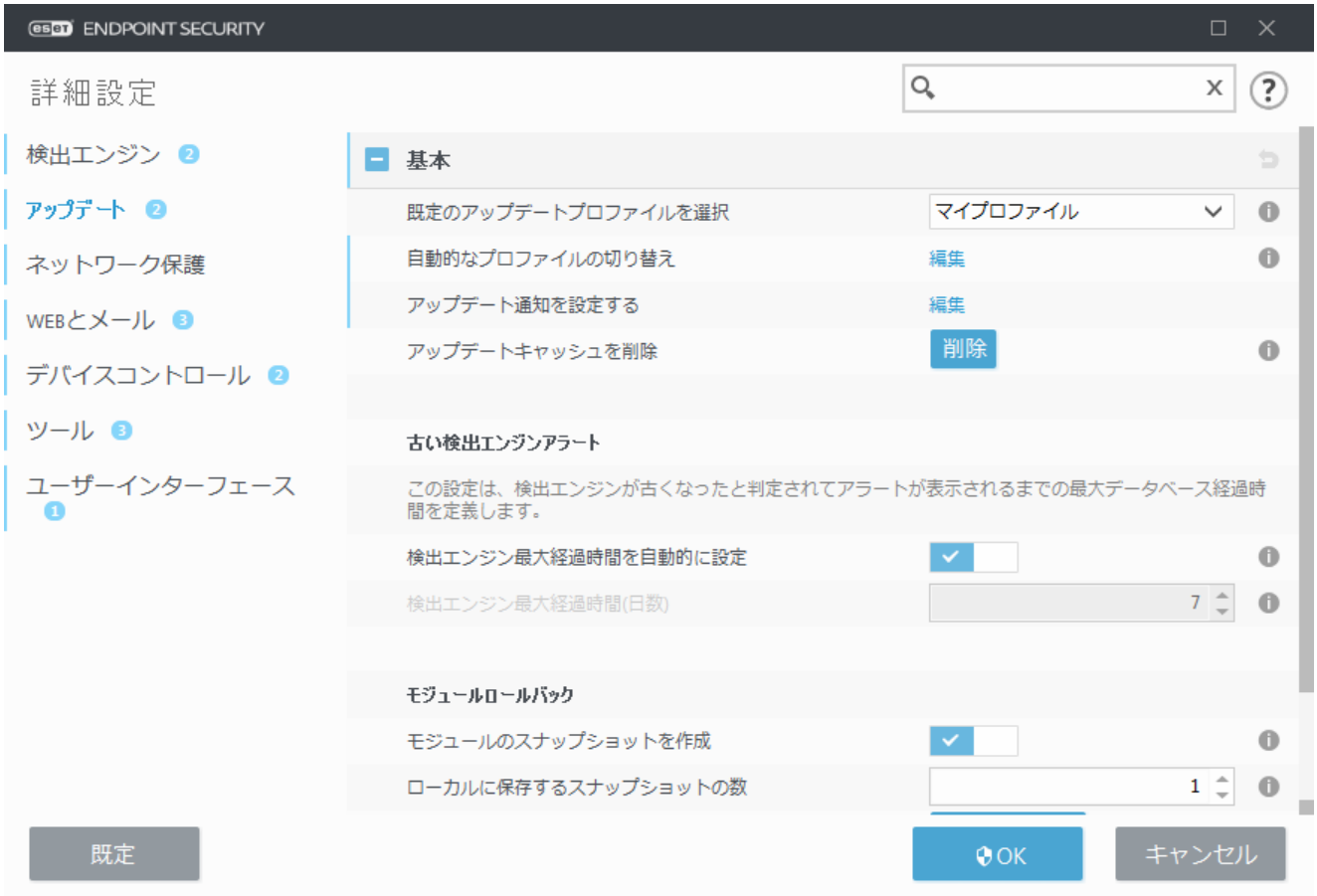
モジュールのアップデートは、悪意のあるコードから完全な保護を管理するうえで重要な部分です。構成と処理のアップデートには特に注意してください。メインメニューから[**アップデート**] > [**最新版のチェック**]を選択して、モジュールの新しいアップデートを確認します。

ライセンスキーを入力していない場合は、新しいアップデートを受信できず、製品をアクティベートするように指示されます。



[詳細設定]ウィンドウ(メインメニューの[**設定**] > [**詳細設定**]をクリックするか、またはキーボードの**F5**キーを押す)に、追加のアップデートオプションが含まれます。アップデートモード、プロキシサーバーアクセスLAN接続、検出エンジンコピー作成設定などの詳細アップデートオプションを構成するには、詳細設定ツリーで**アップデート**をクリックします。

• アップデートで問題が発生した場合は、**クリア**をクリックして、一時アップデートキャッシュをクリアします。



• **プロファイル > アップデート > モジュールアップデート**の**自動的に選択**オプションは既定で有効です。ESETアップデートサーバーを使用してアップデートを受信する場合、これをそのままにすることをお勧めします。

• 画面の右端下に成功した場合のアップデートシステムトレイ通知を表示したくない場合は、**プロファイル > アップデート**を展開し、**受信したアップデート通知を選択**の横の**編集**をクリックしてから、**検出エンジンが正常にアップデートされました**通知のチェックボックスを調整します。

最適な動作を確保するには、プログラムが自動的にアップデートされることが重要です。この操作は、**[ヘルプとサポート]>[製品のアクティベーション]**から正しい**ライセンスキー**を入力した場合にのみ可能です。

インストール後に**ライセンスキー**を入力していない場合は、いつでも入力できます。アクティベーションの詳細については、「ESET Endpoint Securityのアクティベーション方法」を参照し、ESETセキュリティ製品の認証情報を以下の**[ライセンス詳細]**ウィンドウに入力してください。

ゾーンの設定

ネットワーク環境でコンピューターを保護するには、信頼ゾーンを設定する必要があります。信頼ゾーンを設定して共有を許可すると、他のユーザーに自分のコンピュータへのアクセスを許可できます。**[詳細設定]**(F5) > **[ネットワーク保護]** >**[ファイアウォール]** > **[詳細]** > **[ゾーン]**の順にクリックして信頼ゾーンの設定を表示します。

信頼ゾーンの検出は、ESET Endpoint Securityのインストール後、およびコンピュータが新しいネットワー

クに接続されるたびに実行されます。そのため、通常は信頼ゾーンを定義する必要はありません。既定では、新しいゾーンの検出時に、そのゾーンの保護レベルを設定するダイアログウィンドウが表示されます。



信頼済みゾーンを誤って設定すると、コンピュータにセキュリティ上のリスクが生じることがあります。

既定では、信頼済みゾーン内のワークステーションは共有ファイルおよびプリンターへのアクセスを許可されており、受信RPC通信が有効です。さらに、リモートデスクトップの共有も使用可能です。

この新機能の詳細については、次のESETナレッジベース記事をお読みください。

- 新しいネットワークが検出されました ESET Endpoint Security

Webコントロールツール

既にWebコントロールをESET Endpoint Securityで有効化してある場合は、Webコントロール機能が正しく機能するように、指定されたユーザーアカウントにもWebコントロールを設定する必要があります。クライアントワークステーションで特定の制限を作成し、攻撃の可能性から保護する方法については、「Webコントロール」の章を参照してください。

ESET Endpoint Securityの使用方法

ESET Endpoint Securityの設定オプションを使用すると、コンピュータ、Web、メール、ネットワークの保護レベルを調整することができます。

ESET PROTECTWebコンソールまたはESET Security Management Center Webコンソールからポリシーを作成するときに、各設定のフラグを選択できます。強制フラグの設定には優先度があり、後のポリシーに強制フラグがある場合でも、後のポリシーによって上書きすることはできません。こうすると、この設定が変更されない(たとえばユーザーによって、またはマージ中に後のポリシーによって)ことが保証されます。詳細情報については、ESET PROTECTオンラインヘルプのフラグを参照してください。



[**設定**]メニューには次のセクションがあります。

- **コンピュータ**
- **ネットワーク**
- **Webとメール**

コンピューターセクションでは、次の項目について、保護の設定を有効または無効にできます。

- **リアルタイムファイルシステム保護** – ファイルは全て、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。

- **デバイスコントロール** – 自動デバイスコントロール(CD/DVD/USBなど)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。

- **Host Intrusion Prevention System (HIPS)** - HIPS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。

- **詳細メモリ検査**はエクスプロイトブロックとともに動作し、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** - 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クが有効です。 この保護の詳細については、「用語集」を参照してください。

- **ランサムウェア保護**- HIPS機能の一部として動作する保護の別のレイヤーです。 ランサムウェア保護を実行するにはESET LiveGrid®レピュテーションシステムを有効にする必要があります。この保護の詳細を参照してください

- **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。

[**ネットワーク保護**]セクションでは、ファイアウォール、ネットワーク攻撃保護(IDS)およびボットネット保護を設定できます。

[**Webとメールの保護の設定**]セクションでは、次のコンポーネントを有効または無効にすることができます。

- **セキュアブラウザー** – オンラインでの閲覧中に機密データを保護します(オンライン取引中の金融データなど)。

- **Webコントロール** – 不快な内容を掲載していると考えられるWebページをブロックします。また、システム管理者は27個の定義済みWebサイト分類のアクセス設定を指定できます。

- **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**]ではPOP3とIMAPプロトコルで受信した通信が監視されます。

- **迷惑メール対策機能** – 受信者側が送信を要求していないメール(迷惑メール)を検査します。

- **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、任意のモジュールの横にある緑色のスイッチをクリックします。これにより、コンピュータのセキュリティ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、赤色のスイッチをクリックして、コンポーネントを有効状態に戻します。

ESET PROTECT/ESMCポリシーが適用されるときには、特定のコンポーネントの横にロックアイコンが表示されますESET Security Management CenterまたはESET PROTECTによって適用されたポリシーは、ログインユーザー(管理者など)による認証の後にローカルで上書きできます。詳細情報については、ESET PROTECTオンラインヘルプを参照してください。

> この方法で無効にされたすべての保護対策は、コンピュータの再起動後に再有効化されます。

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(コンポーネントの横)をクリックします。

設定ウィンドウの下部に追加オプションがあります。*.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たりするには、[**設定のインポートおよびエクスポート**]のリンクをクリックします。 詳細については、「設定のインポートおよびエクスポート」を参照してください。

詳細オプションについては、[**詳細設定**]をクリックするか、**F5**キーを押してください。

コンピュータ

コンピュータモジュールは、[**設定**] > [**コンピュータ**]にあります。前の章で説明した保護モジュールの概要が表示されます。このセクションでは、次の設定を使用できます。

リアルタイムファイルシステム保護の横の歯車⚙をクリックし、**除外の編集**をクリックして除外設定ウィンドウを開くと、ファイルとフォルダーを検査対象外にできます。**リアルタイムファイルシステム保護**詳細設定を開くには、**設定**をクリックします。



コンピューターセクションでは、次の項目について、保護の設定を有効または無効にできます。

• **リアルタイムファイルシステム保護** – ファイルは全て、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検査されます。

• **デバイスコントロール** – 自動デバイスコントロール(CD/DVD/USBなど)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。

• **Host Intrusion Prevention System (HIPS)** - HIPS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。

• **詳細メモリ検査**はエクスプロイトブロックとともに動作し、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** - 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クが有効です。 この保護の詳細については、「用語集」を参照してください。

• **ランサムウェア保護**- HIPS機能の一部として動作する保護の別のレイヤーです。 ランサムウェア保護を実行するにはESET LiveGrid®レピュテーションシステムを有効にする必要があります。この保護の詳細を参照してください

• **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・スパイウェア対策保護を一時停止する – 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て、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。

検出エンジン

検出エンジンは、ファイル、電子メール、インターネット接続を制御することで、悪意のあるシステム攻撃から保護します。たとえば、マルウェアに分類されたオブジェクトが検出された場合、修復が開始します。検出エンジンは、最初にブロックし、その後に駆除、削除、または隔離に移動して、マルウェアを排除できます。

検出エンジン設定を詳細に設定するには、**[詳細設定]**をクリックするか、**F5**を押します。

このセクションの内容:

- リアルタイム保護および機械学習保護カテゴリ
- マルウェア検査
- 報告設定
- 保護設定
- ベストプラクティス

バージョン7.2以降では、バージョン7.1以下のときにあった検出エンジンセクションのオン/オフスイッチがありません。オン/オフボタンは、強、バランス、注意、およびオフのしきい値に代わりました。

リアルタイム保護および機械学習保護カテゴリ

すべての保護モジュールの**リアルタイム保護および機械学習保護**(リアルタイムファイルシステム保護Webアクセス保護など)では、次のカテゴリのレポートおよび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、よく間違って使用されます。「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て実行されます。
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。

• **望ましくない可能性のあるアプリケーション** - グレイウェアまたは望ましくない可能性があるアプリケーション(PUA)は、ウイルスまたはトロイの木馬などの他のタイプのマルウェアほどはっきりとした意図がない幅広いソフトウェアのカテゴリです。 ただし、追加の不審なソフトウェアをインストールし、デジタルデバイスの動作または設定を変更し、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する可能性があります。
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。

• **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。安全ではない可能性のあるアプリケーション(PUA)の例には、リモートアクセスツール、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)が含まれます。
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。

• **疑わしい可能性があるアプリケーション**には、圧縮形式またはプロテクタで圧縮されたプログラムが含まれます。この種類の防御は、多くの場合、マルウェアの作成者が検知されるのを逃れるために利用します。



詳細機械学習は高度な保護であり、機械学習に基づいて検出を改善する高度なレイヤーとして検出エンジンの一部になっています。このタイプの保護の詳細については、用語集をお読みください。

マルウェア検査

スキャナー設定は、リアルタイムスキャナーとオンデマンドスキャナーで設定できます。既定では、リ

アルタイムファイルシステム保護設定を使用が有効です。有効なときには、関連するオンデマンド検査設定が**リアルタイムおよび機械学習保護**セクションから継承されます。

報告設定

検出が発生するとき(例: 脅威が見つかり、マルウェアとして分類される)に、情報が検出ログに記録され、ESET Endpoint Securityで設定されている場合はデスクトップ通知が発生します。

報告しきい値は、カテゴリごとに設定されます。

1. マルウェア

2. 望ましくない可能性のあるアプリケーション

3. 安全ではない可能性があるアプリケーション

4. 疑わしい可能性のあるアプリケーション

機械学習コンポーネントを含む検出エンジンでレポートが実行されます。現在の保護しきい値よりも高い報告しきい値を設定できます。これらのレポート設定は、オブジェクトのブロック、駆除、または削除に影響しません。

CATEGORY報告のしきい値(またはレベル)を修正する前に、次の点をお読みください。

しきい値	説明
最大	CATEGORY報告は最大感度に設定されています。より多くの検出が報告されます。**最大**設定では、オブジェクトが誤ってCATEGORYとして特定される場合があります。
標準	CATEGORY報告は標準に設定されています。この設定は、検出率のパフォーマンスおよび精度と、誤った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	CATEGORY報告は、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、CATEGORYの動作と一致するときにのみ、オブジェクトが報告されます。
オフ	カテゴリの報告は有効ではありません。このタイプの検出は見つからないか、報告されないか、駆除されません。このため、この設定では、この検出タイプからの保護が無効になります。 マルウェア報告ではオフを使用できません。これは、安全でない可能性があるアプリケーションの既定値です。

ESET Endpoint Security保護モジュールの使用可否

選択したカテゴリしきい値の保護モジュールの使用可否(有効または無効)は次のとおりです。

	最大	標準	最小	オフ**
高度な機械学習モジュール*	✔ (強モード)	✔ (低モード)	X	X
検出エンジンモジュール	✔	✔	✔	X
他の保護モジュール	✔	✔	✔	X

* ESET Endpoint Securityバージョン7.2以降で提供されています。
** 非推奨

製品バージョン、プログラムモジュール、ビルド日を確認します

1. **ヘルプとサポート** > **ESET Endpoint Securityについて**をクリックします。

2. **バージョン情報**画面で、テキストの最初の行にはESET製品のバージョン番号が表示されます。

3. **インストールされたコンポーネント**をクリックすると、特定のモジュールに関する情報が表示されます。

基本事項

環境に適切なしきい値を設定するときの複数の基本事項:

- **標準**しきい値は、ほとんどの設定で推奨されます。

- **最小**しきい値は、前のバージョンのESET Endpoint Security (7.1以下)からの保護の比較可能なレベルを表します。これは、セキュリティソフトウェアにオブジェクトの誤検出を最小化することが優先される環境で推奨されます。

- 報告しきい値が高いほど、検出率が上がりますが、オブジェクトの誤検出の確率も上がります。

- 実際の観点からは、100%の検出率の保証はなく、マルウェアとしてのクリーンなオブジェクトの誤った分類を回避する可能性は0%です。

- ESET Endpoint Securityとモジュールを最新に保つことで、パフォーマンスと検出率の正確性、および誤検出のオブジェクト数の間でバランスを最大化します。

保護設定

カテゴリに分類されたオブジェクトが報告されると、そのオブジェクトがブロックされ、その後に駆除、削除、または隔離に移動されます。

カテゴリ保護のしきい値(またはレベル)を修正する前に、次の点をお読みください。

しきい値	説明
最大	報告されたアグレッシブ(以下)レベルの検出はブロックされ、自動修復(たとえば駆除)が開始します。すべてのエンドポイントがアグレッシブ設定で検査され、誤って報告されたオブジェクトが検出除外に追加されたときには、この設定が推奨されます。
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。自動修復(駆除)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。自動修復(駆除)が開始します。
オフ	誤って報告されたオブジェクトを特定して除外する際に便利です。 マルウェア保護ではオフを使用できません。これは、安全でない可能性があるアプリケーションの既定値です。

ESET Endpoint Security 7.1以下のESET PROTECTポリシー変換表

スキャナー設定のESET PROTECTポリシーエディターのように、各CATEGORYにはON/OFFスイッチがありません。次の表は、ESET Endpoint Security 7.1以下の保護しきい値と最終状態の変換に関する概要を示します。

CATEGORYしきい値状態	最大	標準	最小	オフ
適用されるCATEGORYスイッチ	✓	✓	✓	✗

バージョン7.1以下からバージョン7.2以降にアップグレードするときには、新しいしきい値状態は次のようになります。

アップグレード前のカテゴリスイッチ	✓	✗
アップグレード後の新しいカテゴリしきい値	標準	オフ

ベストプラクティス

管理対象外(個別のクライアントワークステーション)

既定の推奨値をそのまま使用してください。

管理された環境

通常、これらの設定は、ポリシー経由でワークステーションに適用されます。

1. 初期フェーズ

このフェーズは最大で1週間かかる場合があります。

- すべての**報告**しきい値を**標準**に設定します。
注記: 必要に応じて、**最大**に設定します。
- マルウェアの**保護**を**標準**に設定するか、保持します。
- 他のCATEGORIESの**保護**を**最小**に設定します。
備考: このフェーズでは、**保護**しきい値を**最大**に設定することは推奨されません。誤検出を含むすべての検出が修復されるためです。
- 検出ログから誤検出のオブジェクトを特定し、まず検出除外に追加します。

2. 移行フェーズ

- 「本番フェーズ」をテストとして一部のワークステーションに実装します(ネットワークのすべてのワークステーションではない)。

3. 本番フェーズ

- すべての**保護**しきい値を**標準**に設定します。
- リモートで管理するときにはESET Endpoint Securityの該当するウイルス対策定義済みポリシーを使用します。

- **最大**保護しきい値は、最高の検出率が必要で、オブジェクトの誤検出が許容される場合に設定できます。
- 検出ログまたはESET PROTECTレポートに見つかっていない検出があるかどうかを確認してください。

検出エンジンの詳細オプション

アンチステルス技術とは、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、通常の検査技術を使用して検出することはできません。

AMSIによる詳細検査を有効にする - Microsoft Antimalware Scan Interfaceツールで、アプリケーション開発者は新しいマルウェアを防御できます(Windows 10のみ)。

マルウェアが検出された

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、電子メールや、コンピューターのリムーバブルデバイス(USB外付けハードディスクCDDVDなど)など、さまざまです。

標準的な動作

ESET Endpoint 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。

- リアルタイム検査
- 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。検出/駆除されたオブジェクトの詳細については、「ログファイル」を参照してください。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**]または[**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、まず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)。

隔離フォルダーからの復元

隔離にはESET Endpoint Securityのメインプログラムウィンドウから**ツール** > **隔離**をクリックしてアクセスできます。

隔離されたファイルは元の場所に復元することもできます。

- この目的のために**復元**機能を使用するには、隔離内の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を使用します。
- ファイルが望ましくない可能性のあるアプリケーションに設定されている場合、**検査から復元して除外**オプションが有効になります。「除外」も参照してください。
- 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、削除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。
- 復元機能は、読み取り専用のネットワーク共有上にあるファイルなど、使用できない場合があります。

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。

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。

使用しているコンピュータが、マルウェアに感染している気配(処理速度が遅くなる、頻繁にフリーズするなど)がある場合、次の処置を取ることをお勧めします。

- ESET Endpoint Securityを開き、[コンピュータの検査]をクリックする
- [**スマート検査**]をクリックする(詳細については、「コンピュータ検査」を参照)
- スキャン終了後、ログでスキャン済みファイル、感染ファイル、および駆除済みファイルの件数をそれぞれ確認する

ディスクの特定の部分だけを検査するには、[**カスタム検査**]をクリックし、ウイルスを検査する対象を選択します。

共有ローカルキャッシュ

共有ローカルキャッシュは、ネットワークで重複する検査をなくし、分離された環境(仮想マシンなど)でパフォーマンスを高めることができます。これにより、各ファイルが1度だけ検査され、共有キャッシュに保存されることが保証されます。

最初に、ESET Shared Local Cacheをインストールして設定する必要があります。

- ESET Shared Local Cacheをダウンロードします。
- 詳細については、ESET Shared Local Cacheオンラインヘルプを参照してください。

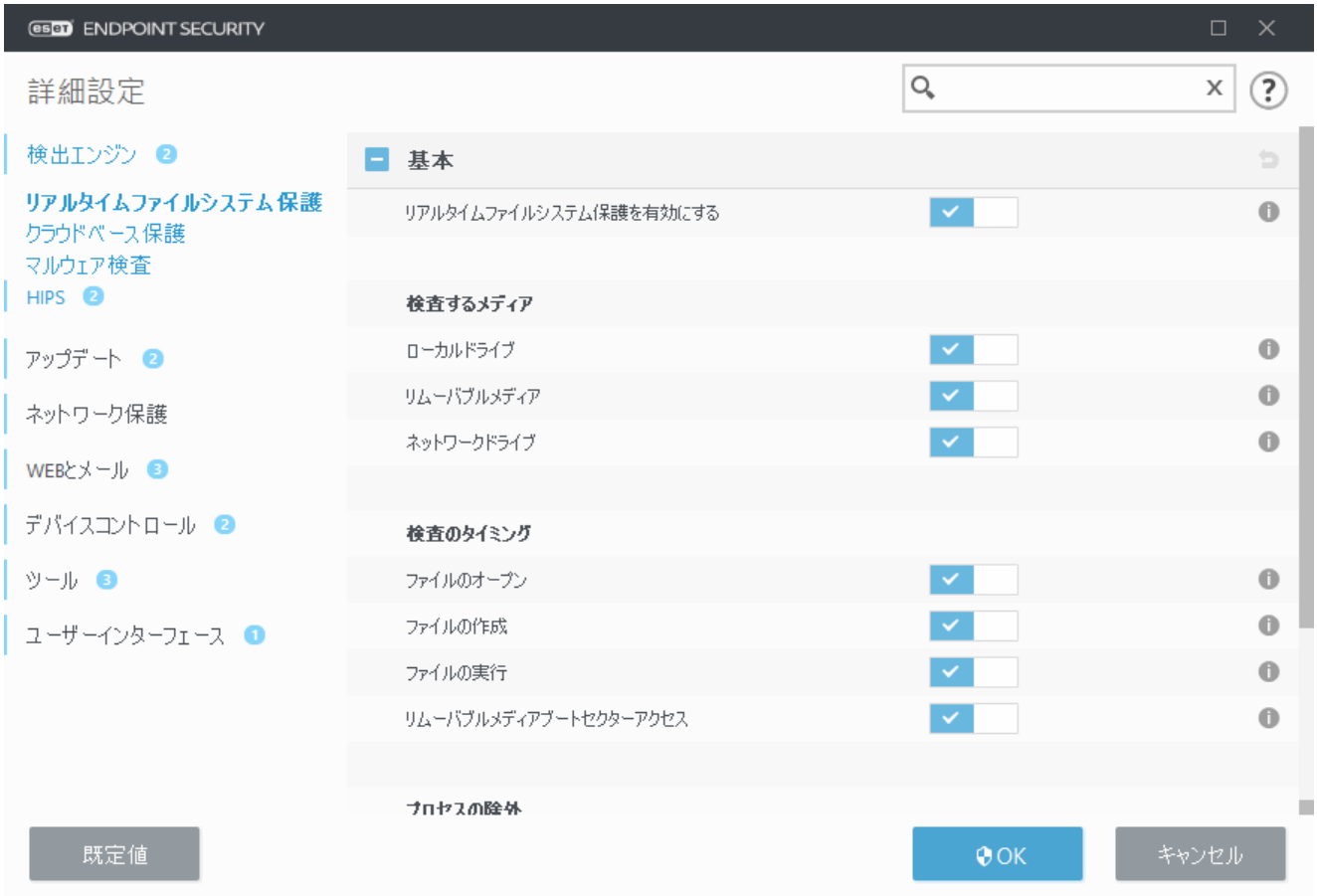
キャッシュオプションスイッチをオンにすると、ネットワークのファイルとフォルダーの検査情報がESET Shared Local Cacheに保存されます。新しい検査を実行する場合は、ESET Endpoint SecurityがESET Shared Local Cacheの検査済みファイルを検索します。ファイルが一致する場合、検査から除外されます。

キャッシュサーバーの設定は次のとおりです。

- **ホスト名** – ESET Shared Local Cacheがあるコンピューターのホスト名またはIPアドレス。
- **ポート** – 通信で使用されるポート番号(ESET Shared Local Cacheで設定されたものと同じ)。
- **パスワード** – 必要に応じて、ESET Shared Local Cacheのパスワードを指定します。

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は、ファイルを開く、作成、実行操作が行われたときに、システムのすべてのファイルを悪意のあるコードから保護します。



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。**[詳細設定]**から**[検出エンジン] > [リアルタイム検査] > [基本]**で**[リアルタイムファイルシステム保護を有効にする]**を無効にしないことをお勧めします。

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** – すべてのシステムと固定ハードドライブを検査します(例: *C:*、*D:*)
- **リムーバブルメディア** – CD/DVD、USBストレージ、メモリカードなどを検査します。
- **ネットワークドライブ** – すべてのマッピングされたネットワークドライブ(例: *\\store04*としての*H:*)または直接アクセスネットワークドライブ(例: *\\store08*)を検査します。

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** – ファイルを開くときに検査します。
- **ファイルの作成** – 作成または修正されたファイルを検査します。
- **ファイルの実行** – **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ブートセクターアクセス** – ブートセクタ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検査は有効になりません。リムーバブルメディアファイル検査は、**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ブートセクターアクセス**が正常に動作するには?ThreatSenseパラメーターで**ブートセクタ?/UEFI**を有効にする必要があります。

検査から除外するプロセス - このタイプの除外については、「プロセスの除外」の章を参照してください。

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、ThreatSenseテクノロジの検出方法(「ThreatSenseエンジンのパラメーターの設定」セクションに説明があります)を使用しており、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。各検出エンジンがアップデートされると、直ちにファイルが再検査されます。この動作は[**スマート最適化**]を使用して設定します。この**スマート最適化**が無効の場合、すべ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**を押して詳細設定を開き、**[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**]ボタンをクリックし、[**スマート最適化を有効にする**]オプションを選択または選択解除します。

リアルタイム保護の確認

リアルタイムファイルシステム保護が機能していてウイルスが検出されることを確認するには?eicar.comのテストファイルを使用します。このテストファイルは、あらゆるウイルス対策プログラムが検出できる無害のファイルです。このファイルは、EICAR(European Institute for Computer Antivirus Research)が、ウイルス対策プログラムの機能をテストする目的で作成しました。

このファイルはhttp://www.eicar.org/download/eicar.comでダウンロードできます。
ブラウザーにこのURLを入力した後、脅威が削除されたというメッセージが表示されます。

リアルタイム保護の設定の変更

リアルタイムファイルシステム保護は、安全なシステムを維持するために最も必要不可欠な要素です。パラメーターを変更する際には注意してください。特定の状況に限ってパラメーターを変更することをお勧めします。

ESET Endpoint Securityのインストール後は、最大レベルのシステムセキュリティをユーザーに提供するように全ての設定が最適化されています。 既定の設定を復元するには、ウィンドウの各タブの横にある ↩ をクリックします(**[詳細設定] > [検出エンジン] > [リアルタイム検査]**)?

リアルタイム保護が機能しない場合の解決方法

この章では、リアルタイム保護使用時に発生することがあるトラブル、およびその解決方法について説明します。

リアルタイム保護が無効である

ユーザーが不注意にリアルタイムファイルシステム保護を無効にしてしまった場合、機能を再アクティベーションする必要があります。 リアルタイムファイルシステム保護を再開するには、メインプログラムウィンドウの**設定**に移動し、**コンピューターの保護] > リアルタイムファイルシステム保護**を有効にします。

リアルタイムファイルシステム保護がシステムの起動時に開始しない場合は[**リアルタイムファイルシステム保護を有効にする**]が無効になっている場合が考えられます。 このオプションを有効にするには、**[詳細設定] (F5)**に移動し、**検出エンジン > 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**をクリックします。

リアルタイム保護がマルウェアの検出と駆除を行わない場合

コンピュータに他のウイルス対策プログラムがインストールされていないことを確認します。 2つのウィルス対策ソフトが同時にインストールされていると、互いに競合することがありますESETをインストールする前に、システムから他のウイルス対策プログラムをアンインストールすることをお勧めします。

リアルタイム保護が開始されない

リアルタイムファイルシステム保護を有効にするが有効であるにもかかわらず、リアルタイムファイルシステム保護がシステム起動時に開始しない場合、他のプログラムとの競合が原因である可能性があります。 この問題を解決するためのサポートについてはESETテクニカルサポートにお問い合わせください。分析用のSysInspectorログを作成し、ESETテクニカルサポートに送信すると、問題の解決に役立ちます。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。

コンピュータの検査

オンデマンドスキャナはESET Endpoint Securityの重要な部分です。コンピューター上のファイルやフォルダーのスキャンを実行するために使用されます。セキュリティの観点からは、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実行(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特定の時点で無効であった場合、検出エンジンが古い場合、またはファイルがディスクに保存されたときにウイルスとして検出されなかった場合に発生することがあります。



2種類の**コンピューターの検査**が利用できます。**コンピューターの検査検査**では、検査パラメータを追加で設定することなく、簡単にシステムを検査します。**カスタム検査**では、あらかじめ定義した検査プロファイルの選択や、特定の検査対象を定義できます。

検査プロセスの詳細については、「検査の進行状況」を参照してください。

コンピューターの検査

スマート検査を使用すると、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。スマート検査の利点は、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。スマート検査では、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。

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、パラメータ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。

検査の対象を選択するには、[**コンピュータの検査**] > [**カスタム検査**]を選択し、[**検査の対象**]ドロップダウンメニューからオプションを選択するか、またはツリー構造から個別の対象を選択します。対象にするフォルダーまたはファイルのパスを入力して、検査対象を指定することもできます。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。検査を実行する時には、**設定** > **ThreatSense パラメータ** > **駆除**をクリックして、4つの駆除レベルから選択できます。

カスタム検査でコンピューターの検査を実行する方法は、ウイルス対策プログラムを以前に使用した経験のある上級ユーザー向けです。

また[**ドラッグアンドドロップ機能**]を使ってファイルまたはフォルダーをクリックすると、マウスボタンを押したままマウスポインターをマークした箇所に移動してからリリースしながら、そのファイルやフォルダーを手動で検査します。 その後、アプリケーションが前面に移動します。

リムーバブルメディア検査

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

前回の検査の再実行

前回実行した検査と同じ設定を使用して、すばやく起動します。

アクションなし/**シャットダウン**/**再起動**/**必要な場合は再起動**を**検査後のアクション**ドロップダウンメニューから選択できます。**スリープ**および**休止**アクションは、コンピューターの電源およびスリープに関するオペレーティングシステムの設定またはコンピューター/ノートブック機能に基づいて提供されます。選択したアクションは、実行中のすべての検査が完了した後に開始します。**シャットダウン**が選択されると、シャットダウン確認ダイアログウィンドウに30秒のカウントダウンが表示されます(**キャンセル**をクリックすると、要求されたシャットダウンが無効になります)。詳細については、詳細検査オプションを参照してください。

> 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。[**ツール**] > [**スケジューラ**]で、検査をスケジュールされたタスクとして設定できます。週次コンピューター検査をスケジュールする方法

カスタム検査起動ツール

個別の対象のみを検査する場合は、カスタム検査ツールを使用できます。そのためには、[**コンピュータの検査**] > [**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オプションを選択するか、フォルダ(ツリー)構造から個別の対象を選択します。

[検査対象]ウィンドウでは、侵入物がないかどうかを検査する対象(メモリ、ドライブ、セクター、ファイルとフォルダー)を定義することができます。

[**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。
- **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。
- **カスタム選択** – 以前の選択をすべてキャンセルします。

フォルダー(ツリー)構造には、特定の検査対象も含まれています。

- **オペレーティングメモリ** – 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にマルウェアが存在するかどうかを検査します。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、および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。検出を駆除するときには、重要なデータが失われないように、レジストリに参照が残ります。

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の空白のフィールドに対象ディレクトリを入力します。



Infected items are not cleaned automatically. Scanning without cleaning can be used to obtain an overview of the current protection status. Furthermore, you can choose from three cleaning levels by clicking **Advanced setup** > **Detection engine** > **On-demand scan** > **ThreatSense parameters** > **Cleaning**. If you are only interested in scanning the system without additional cleaning actions, select **Scan without cleaning**. Scan history is saved to the scan log.

除外を無視を選択すると、以前スキャンから除外された拡張子を持つファイルも、例外なくスキャンされます。

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、**コンテキストメニューの検査**/**詳細検査**/**コンピューターの検査**という3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パラメーターを使用します。使用可能なオプションについては、**詳細設定** > **検出エンジン** > **マルウェア検査** > **オンデマンド検査** > ThreatSenseパラメーターで説明します。

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。

[**管理者として検査**]を使用すると、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。

[ログを表示]をクリックすると、検査が完了したときにコンピューター検査ログを表示できます。

検査の進行状況

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。



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。

検査の進行状況 – まだ検査されていない対象に対する、すでに検査された対象の状況が進捗状況バーに表示されます。検査の進行状況は、検査中に含まれるオブジェクトの総数から求められます。

対象 – 現在検査されている対象の名前と場所。

検出された脅威 – 検査中に検出された脅威の総数を表示します。

中断 – 検査を中断します。

再開 – このオプションは、検査を中断した場合に表示されます。[**再開**]をクリックして検査を続行します。

中止 – 検査を終了します。

ログをスクロールする – オンにすると、新しいエントリーが追加されるときに検査ログが自動的にスクロールされて、最新のエントリーが表示されます。



コンピューター検査ログ

コンピューター検査ログには、次のような検査に関する一般情報が記録されています。

- 検査の日時
- 検査したディスク、フォルダ、ファイル:
- 検査したファイルの数
- 検出された脅威の数
- 完了時間
- 検査に要した時間

マルウェア検査

マルウェア検査セクションには、詳細設定メニューからアクセスできます。**F5**キーを押して、**検出エンジン > マルウェア検査**をクリックし、検査パラメーターを選択するオプションを指定します。このセクションには、次のオプションがあります。

- **選択したプロファイル** – オンデマンドスキャナーによって使用される特定のパラメーターのセッ

ト。
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クリックします。詳細については、検査プロファイルを参照してください。
• **オンデマンド保護および機械学習保護** – 検出エンジン(7.2以降)を参照してください。
• **検査対象** – 特定の対象のみを検査する場合は、**[検査の対象]**の横の**[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。詳細については、検査対象を参照してください。
• **ThreatSense**パラメーター – 検査するファイルの拡張子や使用する検出方法などの詳細設定オプションは、このセクションにあります。クリックすると、詳細スキャナオプションが表示されたタブが開きます。

アイドル状態検査

詳細設定の**検出エンジン > マルウェア検査 > アイドル状態検査**でアイドル状態スキャナーを有効にできます。

アイドル状態検査

[アイドル状態検査を有効にする]の横のチェックボックスを**オン**にすると、この機能を有効にします。コンピュータ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の検査がサイレントに実行されます。

既定では、アイドル状態検出はコンピュータ(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。この設定を変更するには、詳細設定で[**コンピュータがバッテリー電源で作動している場合にも実行する**]の横のスイッチをオンにします。

ログファイルにコンピュータ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[**ツール**] > **[ログファイル**]をクリックし、[**ログ**]ドロップダウンメニューから**[コンピュータの検査**]を選択します)。

アイドル状態検知

アイドル状態スキャナーをトリガーするために満たす必要がある条件の一覧については、アイドル状態検出トリガーを参照してください。

[ThreatSenseエンジン設定]をクリックすると、アイドル状態検査の検査パラメータ(検出方法など)を修正できます。

検査プロファイル

ESET Endpoint Securityには、次の4つの定義済み検査プロファイルがあります。

• **スマート検査**: これは既定の詳細検査プロファイルです。スマート検査プロファイルは、Smart Optimization技術を使用しており、前回の検査で感染していないことが判明したファイルのうち、その検査以降変更されていないファイルを除外します。これにより、検査時間を短縮でき、システムセキュリティへの影響を最小限に抑えることができます。

• **コンテキストメニュー検査**: コンテキストメニューから、任意のファイルのオンデマンド検査を開始できます。コンテキストメニュー検査プロファイルでは、この方法で検査をトリガーするときに使用される検査構成を定義できます。

- **詳細検査**: 既定では、詳細検査プロファイルはSmart optimizationを使用しないため、このプロファイルを使用して検査から除外されるファイルはありません。

- **コンピューターの検査** : これは標準コンピューターの検査で使用される既定のプロファイルです。

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。

新しいプロファイルを作成するには、[詳細設定]ウィンドウ(F5)を開き、[**検出エンジン**] > [**マルウェア検査**] > [**オンデマンド検査**] > [**プロファイルのリスト**]をクリックします。 [**プロファイルマネージャ**]ウィンドウには、既存の検査プロファイルと、新しいプロパティを作成するためのオプションを表示する[**選択したプロファイル**]ドロップダウンメニューがあります。 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。

> 既にある[**コンピューターの検査**]の設定は部分的にしか自分のニーズを満たさないので、独自の検査プロファイルを作成する必要があると仮定します。たとえば、ランタイム圧縮形式と安全でない可能性があるアプリケーションは、検査しません。また、[**厳密な駆除**]を適用することにします。 [**プロファイルマネージャ**]ウィンドウで新しいプロファイルの名前を入力し、[**追加**]をクリックします[**選択したプロファイル**]ドロップダウンメニューから新しいプロファイルを選択し、要件に合わせて残りのパラメータを調整し、**[OK]**をクリックして新しいプロファイルを保存します。

検査対象

[検査対象]ウィンドウでは、侵入物がないかどうかを検査する対象(メモリ、ドライブ、セクター、ファイルとフォルダー)を定義することができます。

[**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。
- **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。
- **カスタム選択** – 以前の選択をすべてキャンセルします。

フォルダー(ツリー)構造には、特定の検査対象も含まれています。

- **オペレーティングメモリ** – 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。
- **ブートセクター/UEFI** – ブートセクターとUEFIにマルウェアが存在するかどうかを検査します。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、および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。検出を駆除するときには、重要なデータが失われないように、レジストリに参照が残ります。

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の空白のフィールドに対象ディレクトリを入力します。

詳細検査オプション

このウィンドウで、スケジュールしたコンピュータ検査タスクの詳細オプションを指定できます。ドロップダウンメニューを使用して、検査の完了後に自動的に実行されるアクションを設定できます。

- **シャットダウン** – 検査完了後にコンピュータがオフになります。
- **再起動** – 検査完了後に、開いているプログラムをすべて終了し、コンピュータを再起動します。
- **必要に応じて再起動** – 検査で必要な場合、すべての開いているプログラムを閉じて、コンピューターを再起動します。
- **スリープ** – セッションを保存し、コンピュータを低電力モードにするため、作業を迅速に再開できます。
- **休止** - RAMで実行中のものをすべて取り込み、ハードディスクの特定のファイルに移動します。コンピュータはシャットダウンしますが、次回の起動時に元の状態から再開されます。
- **アクションなし** – 検査が完了しても、アクションは実行されません。

コンピュータをスリープにしても、コンピュータは動作しています。基本機能は実行され続け、コンピュータがバッテリで動作している場合は、電力を使用します。バッテリの持続時間を長くするために、オフィス外での移動中などには、休止オプションを使用することをお勧めします。

[アクションのキャンセルを許可しない]を選択すると、権限がないユーザーは、検査語に実行されたアクションを停止できません。

一部のユーザーが指定した期間にコンピュータ検査を一時停止できるようにする場合は、**ユーザーによる検査停止可能時間**オプションを選択します。

検査の進行状況の章も参照してください。

デバイスコントロール

ESET Endpoint Securityは、自動デバイスコントロール(CD/DVD/USBなど)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。

サポートされている外部デバイス:

- ディスクストレージ(HDD、USBリムーバブルディスク)
- CD/DVD
- USB プリンター

- FireWire ストレージ
- Bluetoothデバイス
- スマートカードリーダー
- イメージングデバイス
- モデム
- LPT/COMポート
- ポータブルデバイス
- すべてのデバイスタイプ

デバイスコントロール設定オプションは、[**詳細設定**] (F5) > [**デバイスコントロール**]で変更できます。

デバイスコントロールを有効にするの横のチェックボックスを選択するとESET Endpoint Securityのデバイスコントロール機能が起動します。この変更を有効にするには、コンピューターを再起動する必要があります。デバイスコントロールが有効になると、**ルール**が有効になり、ルールエディターウィンドウを開けるようになります。

既存のルールでブロックされているデバイスが挿入されると、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。

デバイスコントロールルールエディタ

デバイスコントロールルールエディタウィンドウには既存のルールが表示されます。このウィンドウを使用すると、ユーザーがコンピューターに接続する外付けデバイスを細かくコントロールすることができます。デバイスコントロールルールの追加も参照してください。

次のESETナレッジベース記事は、英語でのみ提供されている場合があります。
- ESETエンドポイント製品を使用してデバイスコントロールルールを追加および変更する



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。ルール一覧には、外部デバイスの名前と種類、コンピュータに外部デバイスを接続した後に実行するアクション、およびログの重大度などのルールの記述がいくつか示されます。

[**追加**]または[**編集**]をクリックしてルールを管理します。ルールの横の**有効**チェックボックスをオフにすると、今後使用するときまで無効になります。1つ以上のルールを選択し、[**削除**]をクリックすると、ルールが完全に削除されます。

コピー – 別の選択済みルールで使用されている事前定義オプションを備えた新しいルールを作成します。

コンピュータに接続されているデバイスのリムーバブルメディアデバイスパラメータを自動的に入力するには、[**入力**]をクリックします。

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近くに表示されます。

最上位/上/下/最下位**をクリックすると、ルールを移動し、個別またはグループで移動できます。**

デバイスコントロールログは、デバイスコントロールがトリガーされるすべての状況を記録します。ログエントリは、ESET Endpoint Securityのメインプログラムウィンドウの[**ツール**] > [ログファイル]から表示できます。

検出されたデバイス

[**入力**]ボタンを使用すると、現在接続されているすべてのデバイスの概要が表示されます。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、定義済み情報が表示されたルールエディタウィンドウが表示されます(すべての設定は調整できます)。

デバイスグループ

⚠ コンピュータに接続されたデバイスは、セキュリティリスクになる可能性があります。

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、作成されたグループが表示されます。右側のペインに表示するデバイスの一覧とグループを選択します。

デバイスグループウィンドウを開き、グループを選択すると、一覧からデバイスを追加または削除します。また、ファイルからインポートして、グループにデバイスを追加することもできます。あるいは、[**入力**]ボタンをクリックすると、コンピュータに接続されたすべてのデバイスが[**検出されたデバイス**]ウィンドウに一覧表示されます。入力されたリストからデバイスを選択し、**[OK]**をクリックしてグループに追加します。

コントロール要素

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追加するか、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 – 選択したグループまたはデバイスのパラメータ(ベンダー、モデル、シリアル番号)の名前を変更できます。

削除 – ボタンをクリックしたウィンドウの部分によって、選択したグループまたはデバイスを削除します。

インポート – テキストファイルからデバイスのリストをインポートします。テキストファイルからデバイスをインポートするには、正しい形式でなければなりません。

- 1行に1つのデバイスを記述します。
- 各デバイスの**ベンダー⍰モデル⍰シリアル**は必須であり、カンマで区切る必要があります。

✓ テキストファイルの内容の例を次に示します。

```
Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101
```

エクスポート – デバイスのリストをファイルにエクスポートします。

[**入力**]ボタンを使用すると、現在接続されているすべてのデバイスの概要が表示されます。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。

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。

i 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**アクションがあるルールが適用される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、コンピューターに接続したときに、デバイスコントロールによって認識されていないデバイスがブロックされます。

デバイスのタイプによっては、適用されないアクション(権限)もあります。記憶装置タイプのデバイスの場合、4つのアクションすべてを使用できます。記憶装置以外のデバイスでは、これらのうち3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)。

デバイスコントロールルールの追加

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。



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 - 特定の期間に作成されたルールを適用できます。ドロップダウンメニューから、時間スロットを選択します。詳細については、時間スロットを参照してください。

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。デバイスタイプ情報は、オペレーティングシステムから収集されます。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リカ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の例としては、スキャナやカメラが挙げられます。これらのデバイスはアクションに関する情報だけを提供し、ユーザーに関する情報は提供しないため、グローバルにのみブロックできます。

> ユーザー一覧機能はモデムデバイスタイプで使用できません。ルールはすべてのユーザーに適用され、現在のユーザー一覧は削除されます。

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のいずれかです。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。

デバイスのタイプによっては、適用されないアクション(権限)もあります。記憶装置タイプのデバイスの場合、4つのアクションすべてを使用できます。記憶装置以外のデバイスでは、これらのうち3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)。

条件タイプ

デバイスグループまたは**デバイス**を選択します。

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。

> これらのパラメータが未定義の場合、ルールは照合時にこれらのフィールドを無視します。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。

> デバイス情報を表示するには、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。

ログ記録の重大度

- **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、ERA Serverに送信します。
- **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。

- **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。

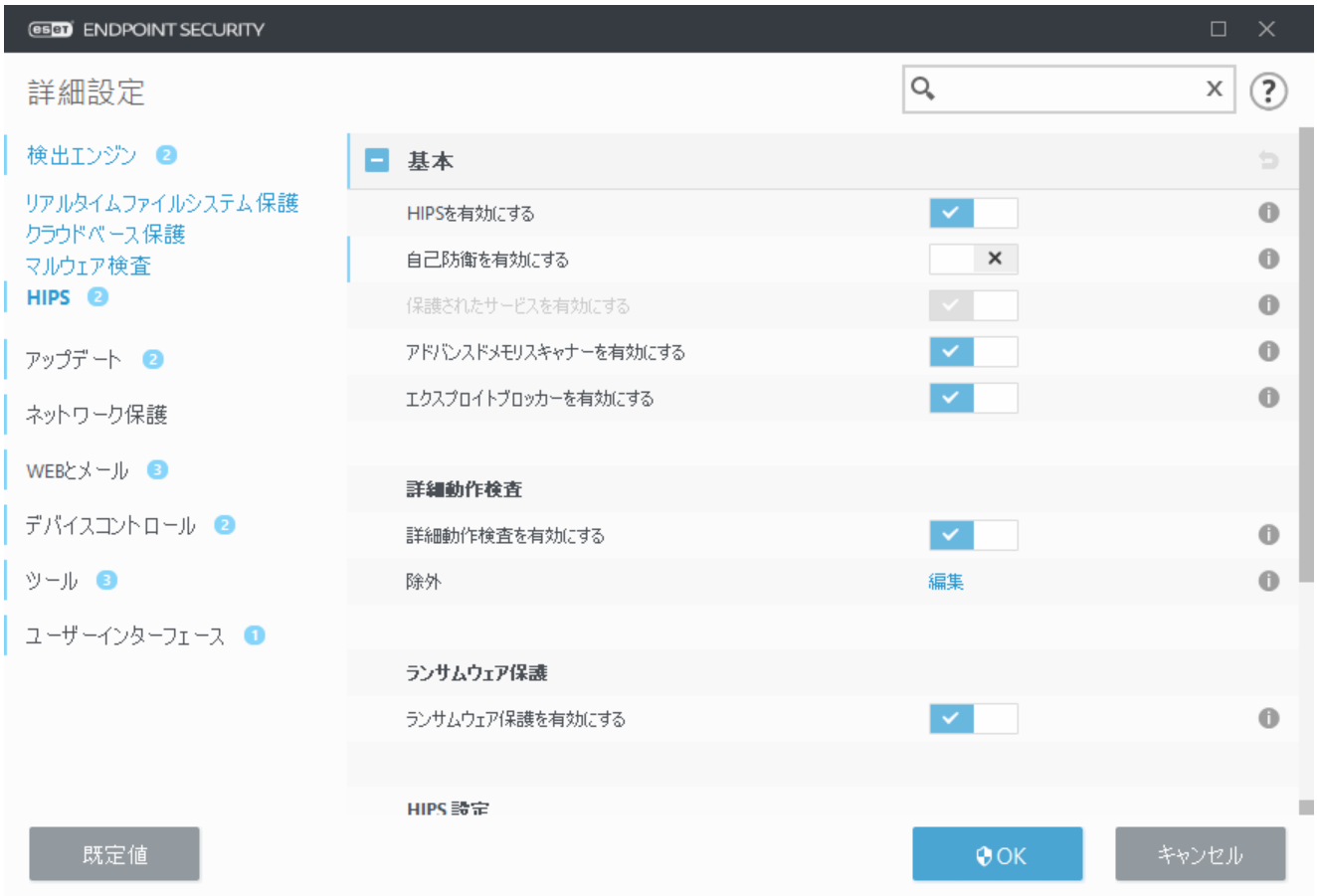
> 一部のデバイスをユーザールールでフィルタリングできません(たとえば、イメージングデバイスではユーザーに関する情報は提供されず、アクションに関する情報だけが提供されます)。

ホストベースの侵入防止システム(HIPS)

> 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。

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。

HIPSは、[**詳細設定**] (F5) > [**検出エンジン**] > [**HIPS**]> [**基本**]をクリックすると見つけられます。HIPS状態(有効/無効)は、ESET Endpoint Securityメインウィンドウの[**設定**] > [**コンピュータ**]に表示されます。



基本

HIPSを有効にする - ESET Endpoint Securityでは既定でHIPSが有効です。HIPSをオフにすると、エクスプロイトブロッカーなどのHIPS関連機能が無効になります。

自己防衛を有効にする - ESET Endpoint Securityには、悪意のあるソフトウェアによってウイルス・スパイウェア対策の保護機能が破損されたり無効化されたりしないようにする**自己防衛**技術がHIPSの一部として組み込まれています。 自己防衛は、重要なシステムおよびESETのプロセス、レジストリキー、およびファイルを改ざんから防止します。インストール時にはESET Managementエージェントも保護されます。

保護されたサービスを有効にする – ESET Service (ekrn.exe)の保護を有効にします。有効にすると、サービスは保護されたWindowsプロセスとして起動し、マルウェアによる攻撃を防御します。このオプションは、Windows 8.1およびWindows 10で使用できます。

詳細メモリ検査を有効にするはエクスプロイトブロックとともに動作し、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クが有効です。 この保護の詳細については、「用語集」を参照してください。

詳細動作検査

詳細動作検査を有効にするは、HIPS機能の一部として動作する別のレイヤーの保護です。このHIPSの拡張は、コンピューターで実行中のすべてのプログラムの動作を分析し、プロセスの動作に悪意がある場合はユーザーに警告します。

詳細動作検査のHIPS除外では、プロセスをスキャンから除外することができます。 すべてのプロセスで脅威の可能性がスキャンされるように、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。

ランサムウェアシールド

ランサムウェアシールドを有効にする - HIPS機能の一部として動作する保護の別のレイヤーです。 ランサムウェアシールドを実行するにはESET LiveGrid®レピュテーションシステムを有効にする必要があります。 この保護の詳細を参照してください

監査モードを有効にする – ランサムウェア保護で検出されたすべての項目は自動的にブロックされませんが、重要度警告でログに出力され、「監査モード」フラグ付きで管理コンソールに送信されます。管理者は、このような検出を除外して、さらなる検出を防止するか、有効な状態を保つ(監査モードが終了した後にブロックされ、削除されます)かどうかを決定できます。監査モードを有効//無効にするとESET Endpoint Securityのログに記録されます。このオプションは、ESET PROTECTまたはESMCポリシー設定エディターでのみ使用できます。

HIPS 設定

フィルタリングモードは、次のモードのいずれかで実行できます。

フィルタリングモード	説明
ルール付き自動モード	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。
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。
ポリシーベースモード	許可する特定のルールで定義されていない、すべての処理をブロックします。
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、**HIPSルール**エディターで表示できますが、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。**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。

学習モードの期限が終了した後にモードを設定する – 学習モードの期限が終了した後に使用されるフィルタリングモードを選択します。期限切れの後は、**ユーザーに確認**オプションでHIPSフィルタリングモードに変更するには、管理者権限が必要です。

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、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。**ルール**の横の[**編集**]をクリックして、**HIPSルール**エディターを開きます。HIPSルールウィンドウでは、ルールを選択、追加、編集、または削除できます。ルール作成とHIPS処理の詳細は、HIPSルールの編集を参照してください。

HIPSインタラクティブウィンドウ

HIPS通知ウィンドウではHIPSが検出する新しいアクションに基づいてルールを作成し、そのアクションを許可または拒否する条件を定義できます。

通知ウィンドウ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ます。通知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。詳細については、HIPSルールの優先度を参照してください。

ルールの既定のアクションを**毎回確認**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[**拒否**]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。

[**アプリケーションが終了するまで記憶**]では、ルールまたはフィルタリングモードの変更HIPSモジュールの更新、またはシステムの再起動まで、アクション(**許可/拒否**)が使用されます。 これら3つのアクションのいずれかが実行された後は、一時的なルールは削除されます。

ルールを作成し、永久に記憶オプションは、HIPSルール管理セクション(管理者権限が必要)で後から変更できる、新しいHIPSルールを作成します。

下部で**詳細**をクリックすると、処理をトリガーするアプリケーション、ファイルのレピュテーション、または許可または拒否するように求められる操作の種類を確認します。

詳細ルールパラメーターの設定は、**詳細オプション**をクリックして、アクセスできます。以下のオプショ

ンは、**ルールを作成し、永久に記憶**を選択した場合にアクセスできます。

- **このアプリケーションでのみ有効なルールを作成する** – このチェックボックスをオフにすると、すべてのソースアプリケーションのルールが作成されます。
- **処理のみ** – ルールファイル/アプリケーション/レジストリ処理を選択します。すべてのHIPS処理の説明をご参照ください。
- **ターゲットのみ** – ルールファイル/アプリケーション/レジストリターゲットを選択します。

通知の表示を停止するには、**詳細設定 (F5) > 検出エンジン > HIPS > 基本**で、フィルタリングモードを**自動モード**変更します。



潜在的なランサムウェア動作の検出

このインタラクティブウィンドウは、潜在的なランサムウェア動作が検出されたときに表示されます。操作を[**拒否**]または[**許可**]することもできます。



詳細をクリックすると、特定の検出パラメーターが表示されます。このダイアログウィンドウでは、**分析のために送信**するか、**検出から除外**することができます。

ランサムウェア保護が正しく動作するにはESET LiveGrid®を有効にする必要があります。

HIPSルール管理

これはHIPSで、ユーザーが定義したルールと自動追加されたルールのリストです。ルール作成とHIPS処理の詳細については、HIPSルール設定の章を参照してください。HIPSの一般原理も参照してください。

列

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オプションをオフにします。

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のあるアクション、つまり[**許可**][**ブロック**]、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。

対象– 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。

ログ記録の重大度 – 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通知が右下隅に表示されます。

コントロール要素

追加 – 新しいルールを作成します。

編集 – 選択したエントリーを編集します。

削除 – 選択したエントリーを削除します。

HIPSルールの優先度

上下ボタンを使用して HIPSルールの優先度レベルを調整するオプションはありません。(ファイアウォールルールでは、ルールは最上位から最下位へと実行されます).

- 作成するすべてのルールの優先度は同じです
- ルールが具体的になるほど、優先度が上がります(たとえば、特定のアプリケーションのルールはすべてのアプリケーションを対象としたルールよりも優先度が高くなります)
- 内部的には HIPSには、ユーザーがアクセスできない高優先度ルールが実装されています(たとえば、自己防衛が定義したルールは上書きできません)
- オペレーティングシステムをフリーズさせる可能性があるルールを作成した場合は、適用されません(優先度が最低になります)

HIPSルール設定

HIPSルール管理を参照してください。

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。

有効 – ルールをリスト内に置いたまま、適用しない場合にこのチェックボックスをオフにします。

ログ記録の重大度 – 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。

ユーザーに通知する – 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。

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。

ターゲットファイル– 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**すべてのファイル**を選択してすべてのファイルを追加します。

アプリケーション– 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。

レジストリエントリ– 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**特定のエントリ**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**すべてのエントリ**を選択してすべてのエントリを追加します。

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。

パスを指定するとC:\exampleはフォルダー自体のアクションに影響し、C:\example*.*はフォルダーのファイルに影響します。

アプリケーション動作

- **別のアプリケーションのデバッグ** – 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 ペインから直接アクセス可能)。

- **新規アプリケーションの開始** – 新しい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。

64ビットバージョンのWindows XP上のプロセス操作をインターセプトすることはできません。

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。

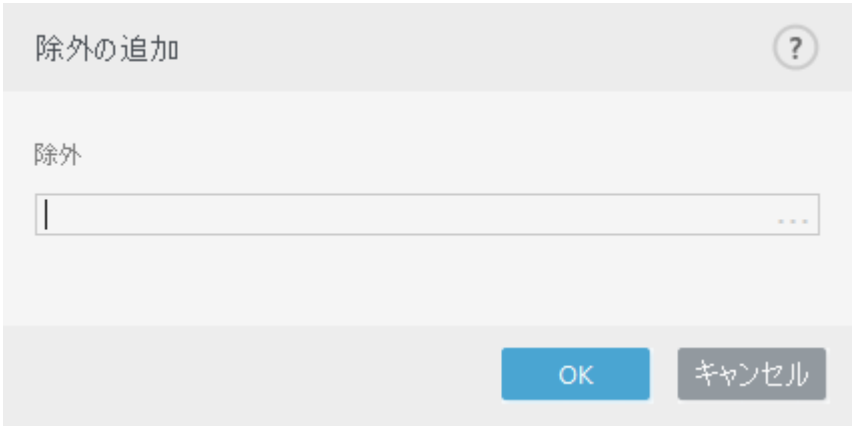
ルールでのワイルドカードの使用
ルールのアスタリスクは、HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet*\Startのように、特定のキーを代入する目的でのみ使用できます。他のワイルドカードの使用方法はサポートされていません。

HKEY_CURRENT_USERキーを対象にしたルールの作成
このキーは、SID (セキュアID)で識別されたユーザー固有のHKEY_USERSの適切なサブキーへのリンクにすぎません。現在のユーザーのルールのみを作成するにはHKEY_CURRENT_USERへのパスを使用する代わりにHKEY_USERS\%SID%を参照するパスを使用します。アスタリスクをSIDとして使用し、ルールをすべてのユーザーに適用することができます。

⚠ 非常に一般的なルールを作成すると、このタイプのルールに関する警告が表示されます。

次の例では、特定のアプリケーションの不要な動作を制限する方法を説明します。

1.ルールに名前を付けて、[**アクション**]ドロップダウンメニューから[**ブロック**](後から選択する場合)**確認**を選択します。
2.[**ユーザーに通知**]チェックボックスをチェックすると、ルールが適用されたときはいつでも通知が表示されます。
3.ルールが適用される1つ以上の処理を、**影響する処理**セクションで選択します。
4.**次へ**をクリックします。
5.**ソースアプリケーション**ウィンドウで、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、指定したアプリケーションに対して選択したアプリケーション処理のいずれかを実行しようとするすべてのアプリケーションに、新しいルールを適用します。
6.**追加**をクリックして、**...**をクリックし、特定のアプリケーションへのパスを選択してから、**OK**を押します。必要に応じて、その他のアプリケーションを追加します。
例: *C:\Program Files (x86)\Untrusted application\application.exe*
7.**ファイルへの書き込み**処理を選択します。
8.ドロップダウンメニューから**すべてのファイル**を選択します。これにより、前の手順で選択したアプリケーションがファイルに書き込む試みをブロックします。
9.[**完了**]をクリックして新規ルールを保存します。



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ー – 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。

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。

ドライバは常にロードできます

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。

追加 – 新しいドライバを追加します。

編集 – 選択したドライバを編集します。

削除 – ドライバをリストから削除します。

リセット – システムドライバのセットをリロードします。

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。

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、ウイルス対策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。

[設定] > [コンピュータ]をクリックしてから、**[プレゼンテーションモード]の横にあるチェックボックスをクリックし、プレゼンテーションモードを手動で有効にします。**[詳細設定] (F5)で、**[ツール] > [プレゼンテーションモード]**をクリックしてから、**[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]の横のチェックボックスをクリックし、全画面アプリケーションの実行時にESET Endpoint Security**を自動的にプレゼンテーションモードにします。プレゼンテーションモードを有効にすると、潜在的なセキュリティリスクが発生するため、タスクバーの保護の状態アイコンがオレンジになり、警告が表示されます。この警告はプログラムのメインウィンドウでも確認でき、[**プレゼンテーションモードが有効です**]がオレンジで表示されます。

[アプリケーションが全画面モードで実行中の場合自動的にプレゼンテーションモードを有効にする]を選択すると、アプリケーションを全画面モードで起動するたびに、プレゼンテーションモードが自動的に開始し、アプリケーションが終了すると自動的に停止します。この機能は特に、ゲーム開始直後、アプリケーションを全画面で開いた直後、またはプレゼンテーションの開始直後にプレゼンテーションモードを開始する場合に便利です。

また、**[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]**を選択し、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。

ファイアウォールが対話モードの場合に、プレゼンテーションモードを有効にすると、インターネットとの接続時に問題が発生することがあります。これは、インターネットに接続するアプリケーションを開始するときに問題となります。通常、そのようなときには確認が求められます(通信のルールや例外が定義されてない場合を除く)が、プレゼンテーションモードではユーザーの操作は無効になっています。この問題を解決するには、この動作と矛盾する可能性のあるアプリケーションごとに通信ルールを定義するか、ファイアウォールで別のフィルタリングモードを使用します。プレゼンテーションモードが有効な場合に、セキュリティ上の潜在的なリスクが存在するWebページまたはアプリケーションにアクセスすると、ブロックされるにもかかわらず、ユーザーとの対話処理が無効なため説明や警告が表示されないことに、注意してください。

スタートアップ検査の設定

既定では、システムの起動時およびモジュールのアップデート時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依存します。

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**]▯[**編集...**]の順にクリックします。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]ウィンドウが表示されます(詳細については、次の章を参照してください)。

スケジューラタスクの作成と管理の詳細については、「新しいタスクの作成」を参照してください。

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ル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。

検査対象ドロップダウンメニューでは、秘密の高度なアルゴリズムに基づくシステムの起動時のファイルの検査レベルを指定します。ファイルは次の基準に従って降順で整理されます。

- **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**
- **一般的に使用されるファイル**
- **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つの検査レベルグループも含まれます。

- **ユーザーのログオン前に実行されるファイル** – 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)。
- **ユーザーのログオン後に実行されるファイル** – 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。

- **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。
- **最低** – システム負荷が可能なかぎり低い場合
- **低** – システム負荷は低い
- **通常** – システム負荷は平均的

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。

文書保護を有効にするには、**詳細設定**ウィンドウ(**F5**) > **検出エンジン** > **マルウェア検査** > **ドキュメント保護**を開き、**ドキュメント保護を有効にする**スイッチをクリックします。

> 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。

除外

除外では、オブジェクトを検出エンジンから除外することができます。すべての対象で検査されるように、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、検査中にコンピュータ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。

パフォーマンス除外では、ファイルと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、ファイルレベルでのゲームアプリケーションの検査を除外したり、異常なシステム動作やパフォーマンスが増加したときに便利です。

検出除外では、検出名、パス、またはハッシュを使用して、オブジェクトを駆除から除外できます。検出除外は、パフォーマンス除外と違い、ファイルとフォルダーを検査から除外しません。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。

バージョン7.1以下の除外では、パフォーマンス除外と検出除外の両方が1つに統合されています。

他の種類の除外と混同しないでください。

- プロセス除外 – 除外されたすべてのアプリケーションプロセスに関連するすべてのファイル操作が検査から除外されます(バックアップ速度とサービスの可用性を向上させるために必要になる場合があります)。
- 除外されたファイル拡張子
- HIPS除外

- クラウドベース保護の除外フィルター

パフォーマンス除外

パフォーマンス除外では、ファイルとフォルダーを検査から除外できます。

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。 しかし、対象を除外する必要がある場合もあります。たとえば、検査中にコンピュータ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。

詳細設定(F5) > 検出エンジン > 除外 > パフォーマンス除外 > 編集で、検査から除外するファイルとフォルダーを除外のリストに追加できます。

オブジェクト(パス：ファイルまたはフォルダ)を検査から除外するには、**追加**をクリックして、アプリケーションパスを入力するか、ツリー構造でパスを選択します。



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。

コントロール要素

- **追加** – オブジェクトを検査から除外する新しいエントリを追加します。
- **編集** – 選択したエントリーを編集します。
- **削除** – 選択したエントリを削除します(CTRLを押しながらクリックすると、複数のエントリを選択できます)。
- **インポート/エクスポート** – パフォーマンス除外のインポートとエクスポートは、後で使用するための現在の除外をバックアップする必要がある場合に便利です。エクスポート設定オプションは、管理サーバで管理されていない環境で任意の除外設定を複数のシステムに対して適用する場合にも便利です。.txtファイルを簡単にインポートして、設定を展開できます。
  インポート/エクスポートファイル形式の例を表示する

```
# {"product":"endpoint","version":"7.2.2055","path":"plugins.01000600.settings.Perfo
rmanceExclusions","columns":["Path","Description"]}

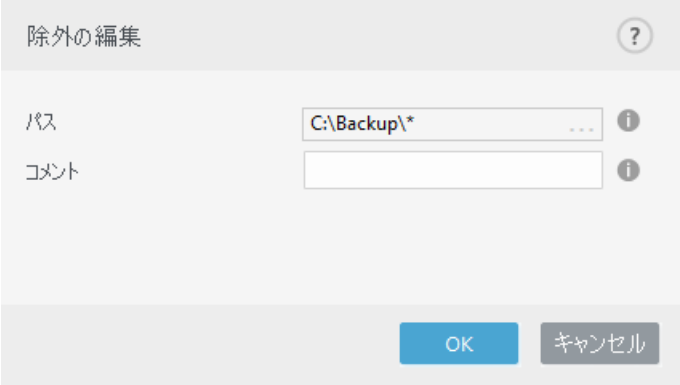
C:\Backup\*,custom comment

C:\pagefile.sys
```

パフォーマンス除外の追加または編集

このダイアログウィンドウは、このコンピューターの特定のパス(ファイルまたはディレクトリ)を除外します。

該当するパスを選択するには、**パス**フィールドで**...**をクリックします。
手動で入力するときには、以下の除外形式の例を参照してください。



ワイルドカードを使用すると、複数のファイルを除外することができます。疑問符(*?*)は1つの文字を表し、アスタリスク(*)は0文字以上の文字列を表します。

- フォルダー内のすべてのファイルとサブフォルダーを除外する場合は、フォルダーのパスを入力し、*のようにワイルドカードを使用します。
- docファイルのみを除外する場合は、マスク**.doc*のようにワイルドカードを使用します。
- 実行可能ファイルの名前に特定数の文字が使用されており(それぞれの文字は異なります)、最初の文字(たとえば"D")のみが明らかな場合は、次の形式を使用します。
D????.exe(疑問符は、不足している文字または不明な文字の代わりに使用されます)

例:

- *C:\Tools** – パスの最後にはバックスラッシュ(\)とアスタリスク(*)を指定して、フォルダーとフォルダーの内容すべて(ファイルとサブフォルダー)が除外されることを示す必要があります。
- *C:\Tools*.*- C:\Tools**と同じ動作
- *C:\Tools* – *Tools*フォルダーは除外されません。スキャナーの観点から、*Tools*をファイル名にすることもできます。
- *C:\Tools*.dat* – これは、*Tools*フォルダーの.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

*%PROGRAMFILES%*などのシステム変数を使用して、検査除外を定義できます。
• 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、除外に追加するときに、パス*%PROGRAMFILES%**(必ずパスの最後にバックスラッシュとアスタリスクを追加すること)を使用します。
• *%PROGRAMFILES%*サブディレクトリのすべてのファイルとフォルダーを除外するには、パス*%PROGRAMFILES%\Excluded_Directory**を使用します。
サポートされるシステム変数のリストを展開する
次の変数は、パス除外形式で使用できます。
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*
ユーザー固有のシステム変数(*%TEMP%*または*%USERPROFILE%*など)、あるいは環境変数(*%PATH%*など)はサポートされていません。

パフォーマンス除外で正式にサポートされていないため、パスの中間でワイルドカードを使用する(例: *C:\Tools*\Data\file.dat*)と、正常に動作しない場合があります。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。
検出除外を使用するときには、パスの中央でワイルドカードを使用することに関する制限はありません。

除外の順序:
• 上下ボタンを使用して、 除外の優先度レベルを調整するオプションはありません。 (ファイアウォールルールでは、ルールは最上位から最下位へと実行されます).
• スキャナーによって最初に適用されるルールが一致すると、2番目に適用されるルールは評価されません。
• ルールが少ないほど、検査のパフォーマンスが向上します。
• 同時ルールの作成を避ける。

パス除外形式

ワイルドカードを使用すると、複数のファイルを除外することができます。疑問符(*?*)は1つの文字を表し、アスタリスク(*)は0文字以上の文字列を表します。

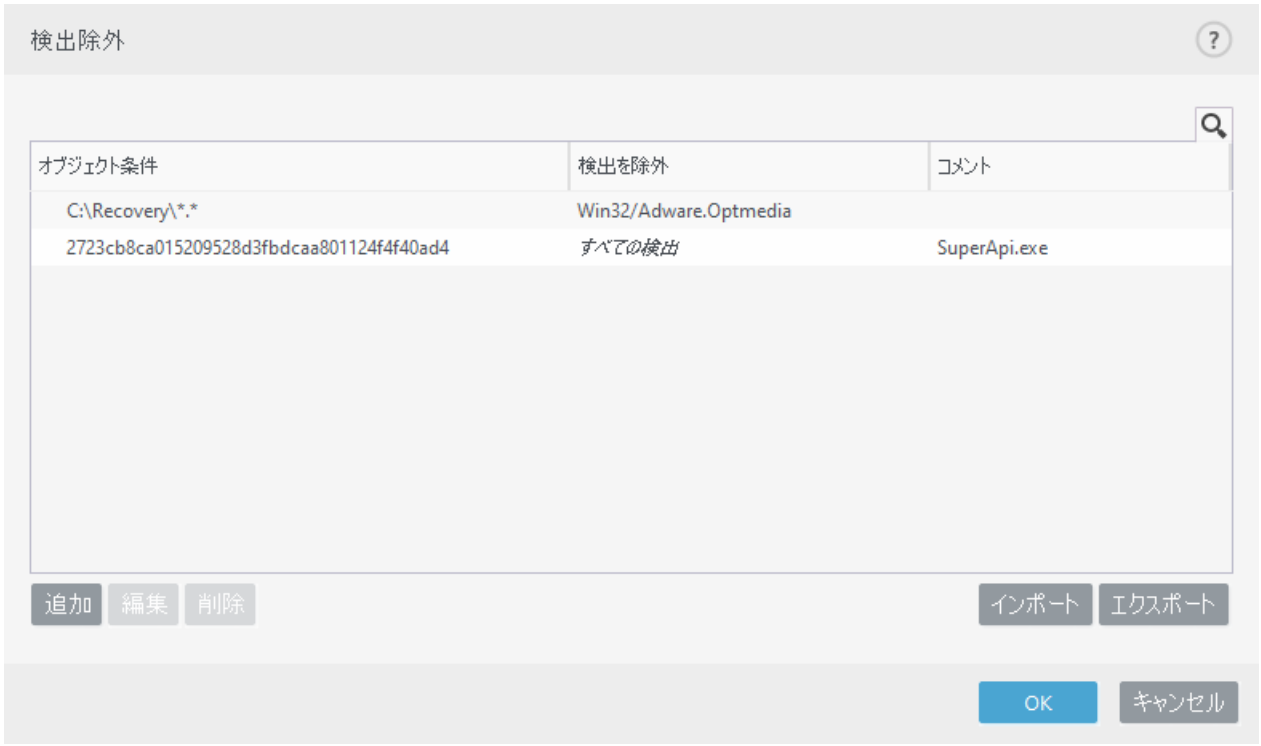
• フォルダー内のすべてのファイルとサブフォルダーを除外する場合は、フォルダーのパスを入力し、*のようにワイルドカードを使用します。
• docファイルのみを除外する場合は、マスク*.docのようにワイルドカードを使用します。
• 実行可能ファイルの名前に特定数の文字が使用されており(それぞれの文字は異なります)、最初の文字(たとえば"D")のみが明らかな場合は、次の形式を使用します。
D????.exe（疑問符は、不足している文字または不明な文字の代わりに使用されます）
例:
• *C:\Tools** – パスの最後にはバックスラッシュ(\)とアスタリスク(*)を指定して、フォルダーとフォルダーの内容すべて(ファイルとサブフォルダー)が除外されることを示す必要があります。
• *C:\Tools*.** - *C:\Tools**と同じ動作
• *C:\Tools* – *Tools*フォルダーは除外されません。スキャナーの観点から、*Tools*をファイル名にすることもできます。
• *C:\Tools*.dat* – これは、*Tools*フォルダーの.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

*%PROGRAMFILES%*などのシステム変数を使用して、検査除外を定義できます。
• 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、除外に追加するときに、パス*%PROGRAMFILES%**(必ずパスの最後にバックスラッシュとアスタリスクを追加すること)を使用します。
• *%PROGRAMFILES%*サブディレクトリのすべてのファイルとフォルダーを除外するには、パス*%PROGRAMFILES%\Excluded_Directory**を使用します。
サポートされるシステム変数のリストを展開する
次の変数は、パス除外形式で使用できます。
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*
ユーザー固有のシステム変数(*%TEMP%*または*%USERPROFILE%*など)、あるいは環境変数(*%PATH%*など)はサポートされていません。

検出除外

検出除外では、検出名、オブジェクトパス、またはハッシュをフィルタリングして、オブジェクトを駆除から除外できます。

検出除外は、パフォーマンス除外と違い、ファイルとフォルダーを検査から除外しません。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。
たとえば(以下の画像の最初の行を参照)、オブジェクトがWin32/Adware.Optmediaとして検出され、検出されたファイルが*C:\Recovery\file.exe*のときです。2番目の行では、適切なSHA-1ハッシュがある各ファイルは、検出名に関係なく、常に除外されます。



すべての脅威を確実に検出するために、絶対に必要なときにのみ検出除外を作成することをお勧めします。

ファイルとフォルダーを除外リストに追加するには、**詳細設定(F5) > 検出エンジン > 除外 > 検出除外 > 編集**で行います。

駆除から(検出名またはハッシュで)オブジェクトを除外するには、**追加**をクリックします。

望ましくない可能性があるアプリケーションと安全でない可能性があるアプリケーションの場合、次の方法で、検出名による除外も作成できます。

- 検出を報告するアラートウィンドウで**詳細オプションを表示**をクリックし、**検出から除外を選択**します。
- 検出除外の作成ウィザードを使用するログファイルコンテキストメニュー。
- **ツール > 隔離**をクリックし、隔離されたファイルを右クリックし、コンテキストメニューから**検査からの復元と除外**を選択して作成できます。

検出除外オブジェクト条件

- **パス** – 指定されたパス(またはすべて)の検出除外を制限します。
- **検出名** – 除外されるファイルの横に検出の名前がある場合、ファイルは特定の検出に対してのみ除外され、完全には除外されません。このファイルが後で他のマルウェアに感染した場合は検出されます。
- **ハッシュ** – ファイルタイプ、場所、名前、拡張子に関係なく、指定されたハッシュSHA-1に基づいて、ファイルを除外します。

コントロール要素

- **追加** – オブジェクトを駆除から除外する新しいエントリを追加します。

- **編集** – 選択したエントリーを編集します。
- **削除** – 選択したエントリを削除します(CTRLを押しながらクリックすると、複数のエントリを選択できます)。
- **インポート/エクスポート** – 検出除外のインポートとエクスポートは、後で使用するための現在の除外をバックアップする必要がある場合に便利です。エクスポート設定オプションは、管理されていない環境で任意の基本設定を複数のシステムに対して使用する場合にも便利です。.txtファイルを簡単にインポートして、設定を転送できます。
  インポート/エクスポートファイル形式の例を表示する

```
# {"product":"endpoint","version":"7.2.2055","path":"Settings.ExclusionsManagement.DetectionExclusions","columns":["Id","Path","ThreatName","Description","FileHash"]}

4c59cd02-357c-4b20-a0ac-ca8400000001,,,SuperApi.exe,00117F70C86ADB0F979021391A8AEAA497C2C8DF

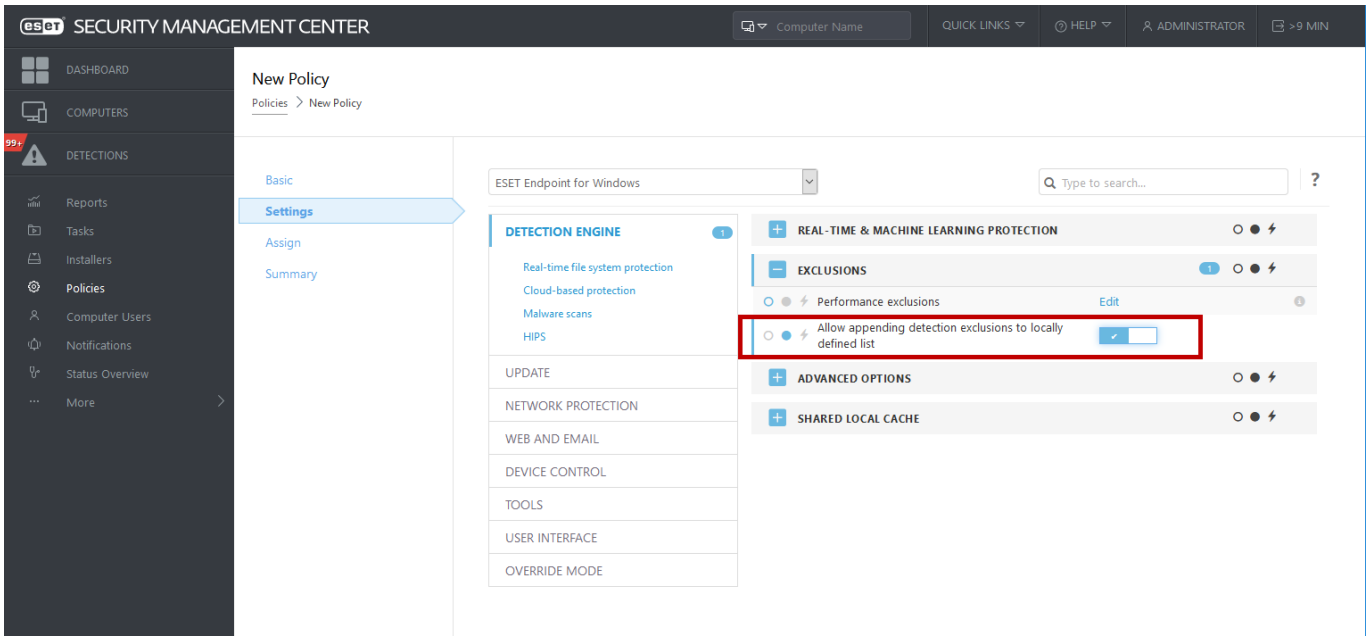
2c362ac8-a630-496e-9665-c76d00000001,C:\Recovery\*.*,Win32/Adware.Optmedia,,
```

ESET PROTECTでの検出除外設定

ESMC 7.1およびESET PROTECT 8.0には、検出除外管理のための新しいウィザードがあり、検出除外を作成し、別のコンピューターまたはグループに適用できます。

ESET PROTECTから検出除外が上書きされる可能性

検出除外ローカルリストが既に存在しているときには、管理者は、**検出除外をローカル定義リストの最後に追加することを許可**によってポリシーを適用する必要があります。その後に、想定どおりESET PROTECTから検出除外を最後に追加できるようになります。

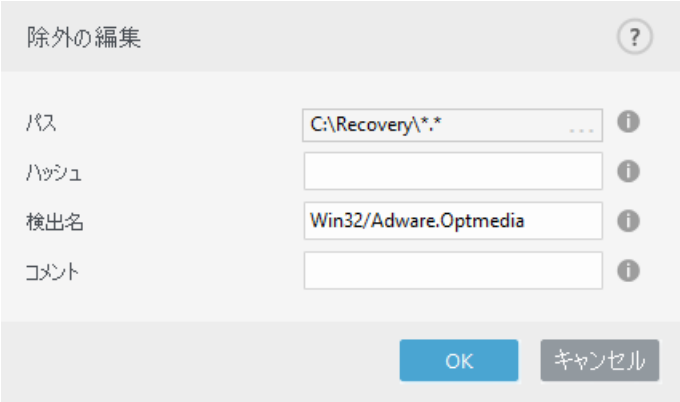


検出除外の追加または編集

検出を除外

有効なESET検出名を指定してください。有効な検出名については、ログファイルを参照し、ログファイルドロップダウンメニューから**検出**を選択します。これは、誤検出サンプルがESET Endpoint Securityで検出されているときに役立ちます。実際の侵入の例外は非常に危険です。**パスマスク**フィールドで**...**をクリックして、影響を受けるファイル/ディレクトリのみを除外するか、一時的に限って除外することを検討してください。除外は、望ましくない可能性のあるアプリケーション、安全でない可能性があるアプリケーション、不審なアプリケーションにも適用されます。

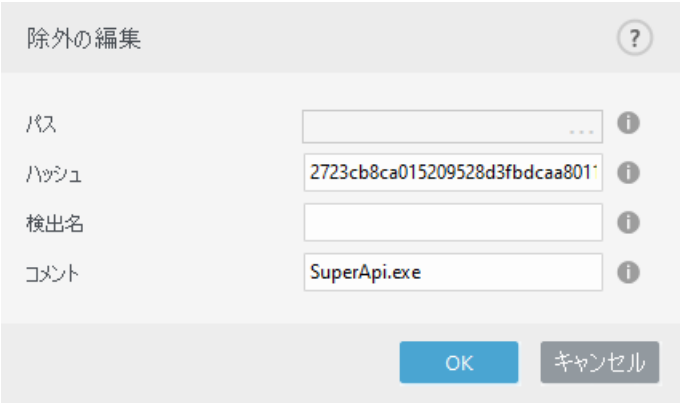
パス除外形式を参照してください。



以下の検出除外の例を参照してください。

ハッシュを除外

ファイルタイプ、場所、名前、拡張子に関係なく、指定されたハッシュSHA-1に基づいて、ファイルを除外します。



特定の検出を名前で除外する場合は、有効な検出名を入力します。
Win32/Adware.Optmedia
ESET Endpoint Securityアラートウィンドウから検出を除外するときには、次の形式を使用することもできます。
@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
@NAME=Win32/Bagle.D@TYPE=worm

コントロール要素

- **追加** – オブジェクトを検出対象外にします。
- **編集** – 選択したエントリーを編集します。
- **削除** – 選択したエントリを削除します(CTRLを押しながらクリックすると、複数のエントリを選択できます)。

検出除外の作成ウィザード

検出除外は、ログファイルコンテキストメニューからも作成できます(マルウェア検出では使用できません)。

1. メインプログラムウィンドウで、**ツール > ログファイル**をクリックします。
2. **検出ログ**で検出を右クリックします。
3. **除外の作成**をクリックします。

除外条件に基づいて1つ以上の検出を除外するには、**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** – 検出名で各ファイルを除外します。
- **パス + 検出** – ファイル名(*file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*など)を含む検出名とパスで各ファイルを除外します。

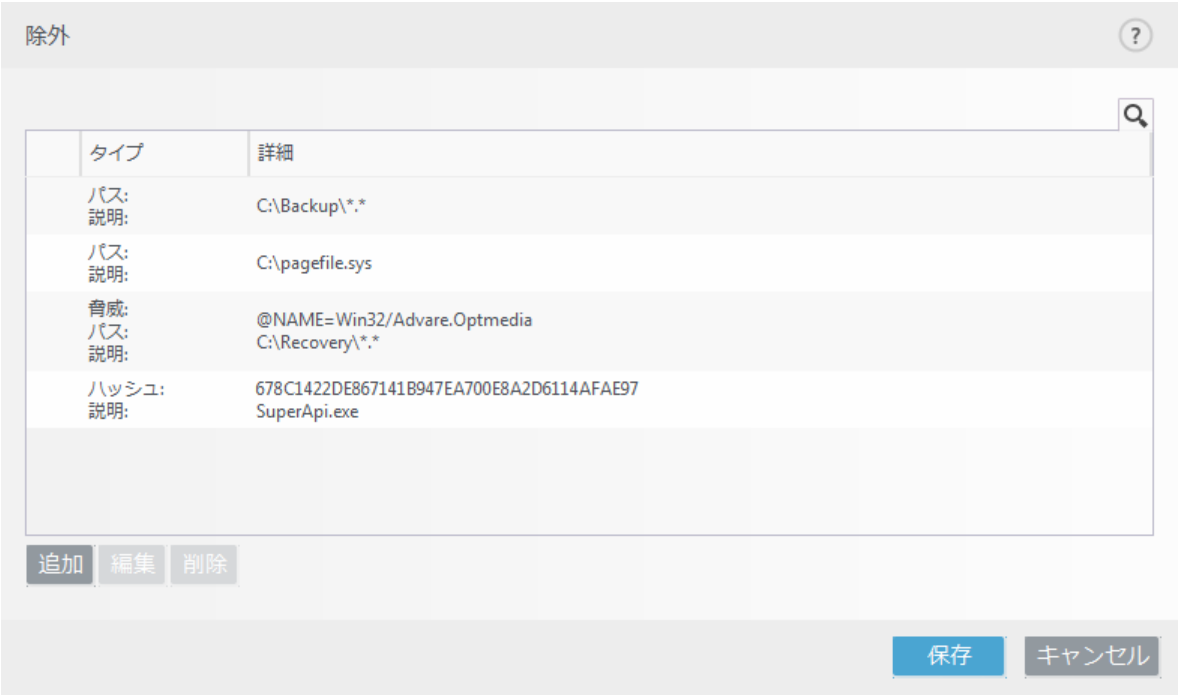
推奨オプションは、検出タイプに基づいてあらかじめ選択されています。

任意で、**除外の作成**をクリックする前に、**コメント**を追加できます。



除外(7.1以下)

バージョン7.1以下の除外では、パフォーマンス除外と検出除外の両方が1つに統合されています。



プロセスの除外

プロセス除外機能では、リアルタイムファイルシステム保護からアプリケーションプロセスを除外できます。バックアップ速度、プロセス整合性、サービス可用性を改善するために、ファイルレベルのマルウェア保護と競合することが確認されている一部の技術がバックアップ中に使用されます。類似したプログラムが、仮想マシンのライブマイグレーションを試行するときに発生することがあります。両方の状況を回避するための効率的な方法は、マルウェア対策ソフトウェアを無効にすることだけです。特定のプロセス(バックアップソリューションなど)を除外すると、このような除外されたプロセスに関連する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、バックアッププロセスへの干渉が最小化されます。除外を作成するときには、注意することをお勧めします。除外されたバックアップツールは、除外された権限がリアルタイム保護モジュールでのみ許可された拡張権限である、アラートをトリガーせずに、感染したファイルにアクセスできます。

プロセス除外は、潜在的な競合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。これにより、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影響を及ぼします。プロセス/アプリケーションの除外は、実行ファイルの除外です(*.exe*)

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** > **プロセス除外**を使用して、実行ファイルを除外されたプロセスのリストに追加できます。

この機能は、バックアップツールを除外するために設計されています。バックアップツールのプロセスを検査から除外すると、システムの安定を保証するだけではなく、実行中にバックアップ速度が低下しないため、バックアップパフォーマンスにも影響しません。

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。ここでは、除外を追加し、検査から除外される実行ファイル(*Backup-tool.exe*など)を参照できます。

✓ *.exe*ファイルが除外に追加されるとすぐに、このプロセスのアクティビティがESET Endpoint Securityによって監視され、このプロセスで実行されるすべてのファイル処理で検査が実行されません。

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、実行ファイルの完全パスを手動で入力する必要があります。そうしないと、除外が正常に動作せず、HIPSがエラーを報告する場合があります。

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。

Webアクセス保護は、この除外を考慮しません。このためWebブラウザーの実行ファイルを除外する場合、ダウンロードされたファイルがまだ検査されます。このようにして、侵入を検出できます。このシナリオは、例ですWebブラウザーの除外は作成しないことをお勧めします。

プロセス除外の追加または編集

このダイアログウィンドウでは、検出エンジンから除外されるプロセスを**追加**できます。プロセス除外は、潜在的な競合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。これにより、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影響を及ぼします。プロセス/アプリケーションの除外は、実行ファイルの除外です(*.exe*)

...(*C:\Program Files\Firefox\Firefox.exe*など)をクリックして、想定されたアプリケーションのファイルパスを選択します。アプリケーション名は入力しないでください。
*.exe*ファイルが除外に追加されるとすぐに、このプロセスのアクティビティがESET Endpoint Securityによって監視され、このプロセスで実行されるすべてのファイル処理で検査が実行されません。

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、実行ファイルの完全パスを手動で入力する必要があります。そうしないと、除外が正常に動作せず、HIPSがエラーを報告する場合があります。

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。

HIPS除外

除外によって、プロセスをHIPS詳細動作検査から除外できます。

オブジェクトを除外するには、**追加**をクリックして、オブジェクトのパスを入力するか、あるいは下のツリー構造でパスを選択します。選択したエントリを**編集**または**削除**することもできます。

除外の章を参照してください。

ThreatSense パラメータ

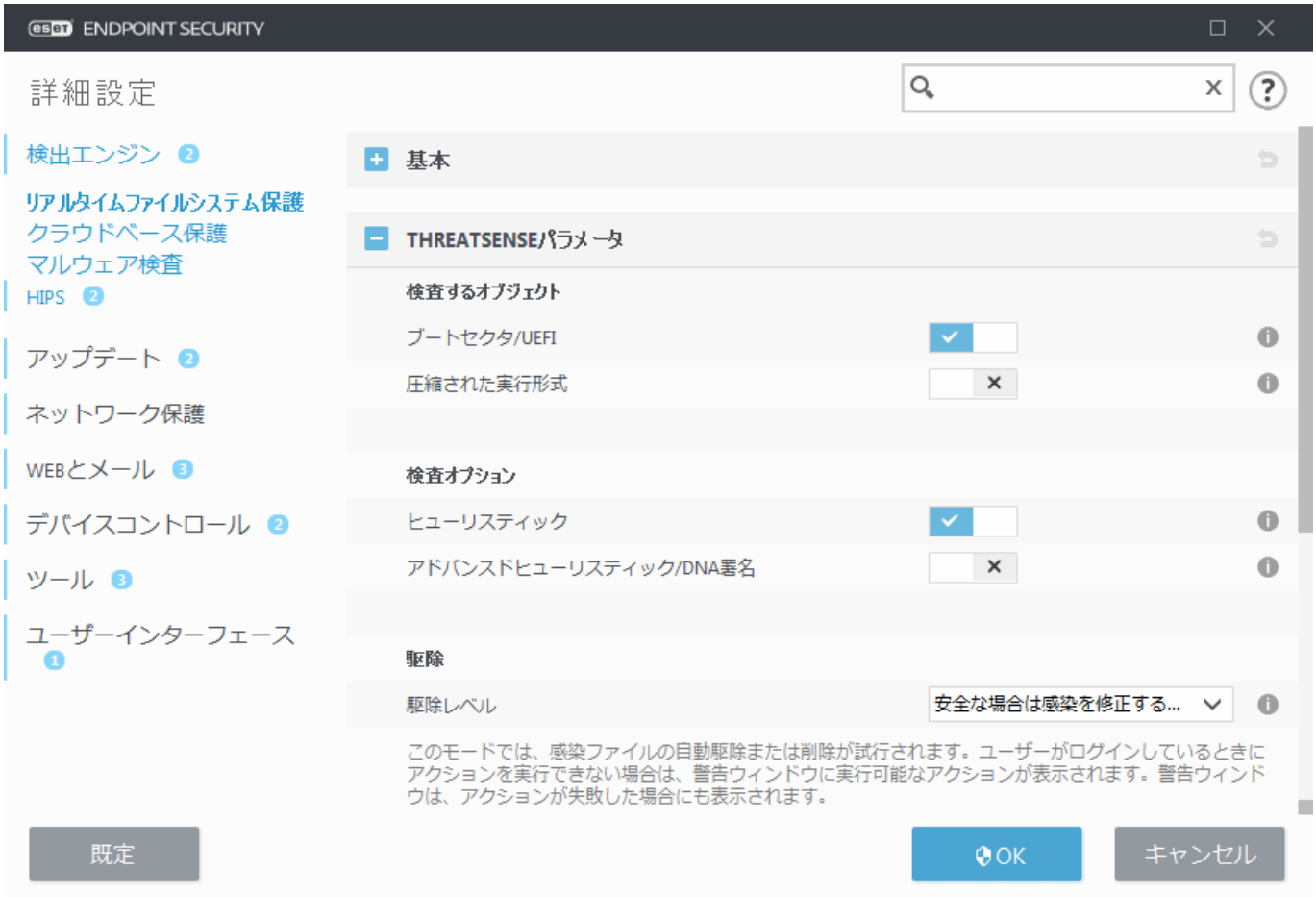
ThreatSenseは、ウイルスを検出する多数の複雑な方法から構成される技術です。 この技術は事前対応型なので、新しいウイルスが広がる初期の段階でも保護することができます。 この技術では、システムのセキュリティを大幅に強化するために連携して動作するコード分析、コードエミュレーション、汎用シグネチャ、ウイルスシグネチャを組み合わせて使用します。 検査エンジンは、複数のデータストリームを同時に検査して、最大限の効率および検出率を確保することができます。 またThreatSense技術によってルートキットを除去することもできます。

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)の詳細設定ウィンドウにある**[ThreatSenseパラメータ]**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。

- リアルタイム検査
- アイドル状態検査
- スタートアップ検査の設定
- 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
- コンピュータの検査



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するか、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)。 コンピューター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。

システムメモリ – システムメモリー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 – ブートセクターのマスターブートレコードにおけるマルウェアの存在を検査します。用語集のUEFIの詳細をお読みください

電子メールファイル – プログラムは以下の拡張子をサポートしますDBX (Outlook Express)およびEML

アーカイブ – 拡張子ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACEなどがサポートされます。

自己解凍アーカイブ – 自己解凍アーカイブ(SFX)は自分自身を展開できるアーカイブです。

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(UPX, yoda, ASPack, FSG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のバージョ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。欠点は、非常に少ないとはいえ、誤検出の可能性がある点です。

アドバンスドヒューリスティック/DNAシグネチャ – 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

駆除設定は、オブジェクト駆除中のESET Endpoint Securityの動作を決定します。

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。このThreatSenseパラメーター設定のセクションでは、スキャンするファイルの種類を指定する方法を説明します。

その他

オンデマンドコンピューターの検査で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で検査 – 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 – 検査ログには、自己解凍アーカイブで、感染していないファイルも含め、すべての検査されたファイルが表示されます(大量の検査ログデータが生成され、検査ログファイルのサイズが大きくなることがあります)。

スマート最適化を有効にする – スマート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。スマート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検査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。

オブジェクトの設定

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、ウイルス対策機能では、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

オブジェクトの最長検査時間(秒) – コンテナーオブジェクト(RAR/ZIPアーカイブや複数の添付ファイルを含む電子メールなど)のファイルを検査する最大時間の値を定義します。この設定は、スタンドアロンファイルには適用されません。ユーザー定義の値が入力され、その時間が経過すると、コンテナーオブジェクトの各ファイルの検査が完了したかどうかに関係なく、検査が可能な限りすぐに停止します。

大きなファイルを含むアーカイブの場合、検査はアーカイブからファイルが展開された時点で停止します(たとえば、ユーザー定義変数が3秒で、ファイルの展開には5秒かかる場合)。アーカイブ内の残りのファイルは、その時間が経過した時点で検査されません。
大きなアーカイブを含む検査時間を制限するには、**最大オブジェクトサイズ**と**アーカイブ内の最大ファイルサイズを**使用します(セキュリティ上のリスクがあるため推奨されません)。
既定値:無制限

アーカイブ検査の設定

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.

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

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。

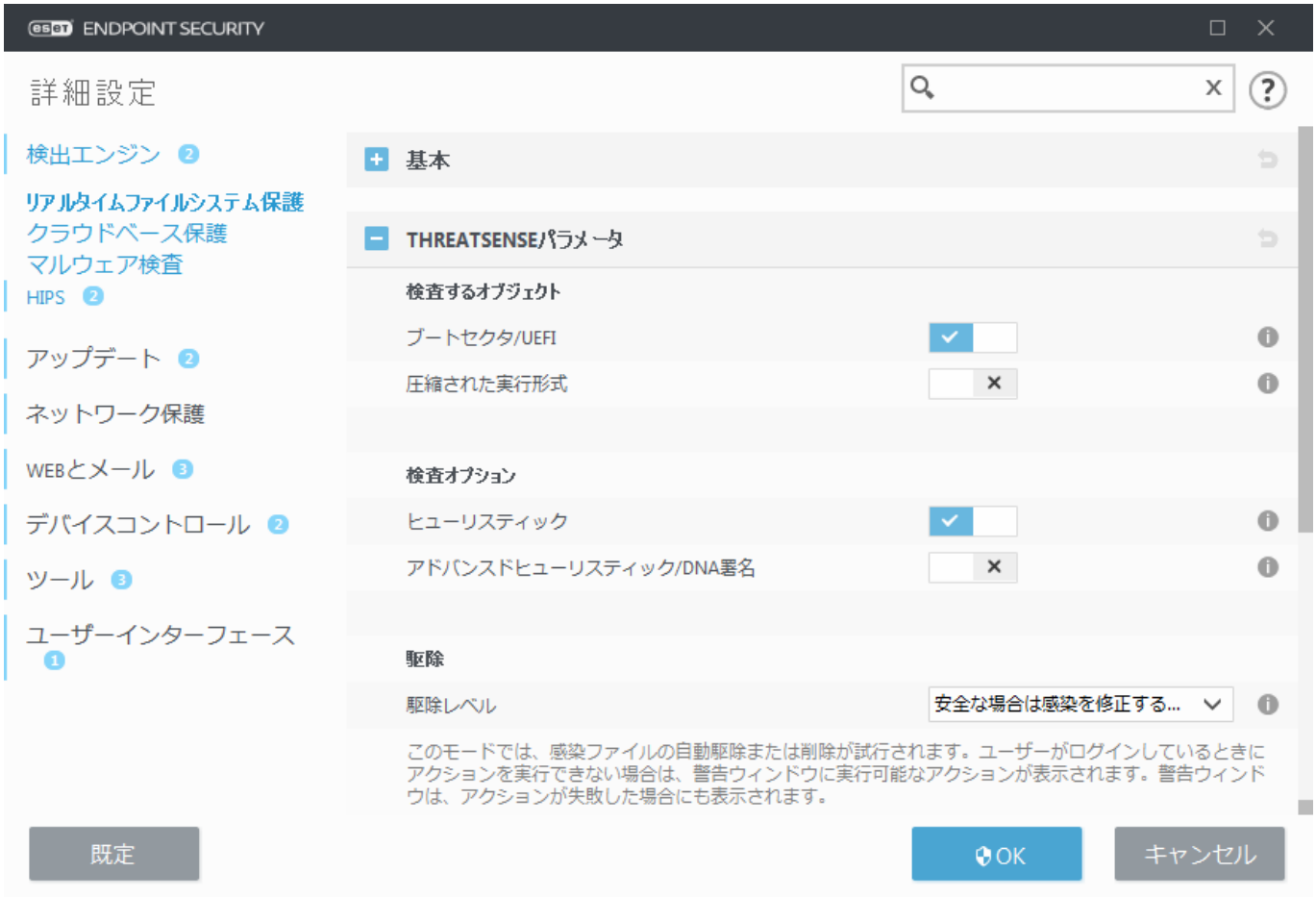
駆除レベル

目的の保護モジュールの駆除レベル設定にアクセスするには、**ThreatSenseパラメーター(リアルタイムファイルシステム保護**など）を展開し、**駆除**をクリックします。

リアルタイムファイルシステム保護および他の保護モジュールには、次の修復(駆除など)レベルがあります。

ESET Endpoint Security8での修復

駆除レベル	説明
常に検出を修正する	オブジェクトの駆除中に検出の修復を試みます。ユーザー操作はありません。ごく一部の場合(システムファイルなど)で、検出を修正できない場合は、報告されたオブジェクトは元の場所に残されます。**常に検出を修正する**は、管理された環境で推奨される既定の設定です。
安全な場合に検出を修正する。安全でない場合は保持する	ユーザー操作なしで、オブジェクトの駆除中に検出の修復を試みます。一部の場合(システムファイルや、感染していないファイルと感染したファイルの両方を含むアーカイブなど)で、検出を修正できない場合は、報告されたオブジェクトは元の場所に残されます。
安全な場合は検出を修正する。安全でない場合は確認する	オブジェクトの駆除中に検出の修復を試みます。一部の場合で、アクションを実行できない場合は、エンドユーザーにインタラクティブアラートが表示され、エンドユーザーが修復アクション(削除または無視など)を選択する必要があります。ほとんどの場合、この設定が推奨されます。
常にエンドユーザーに確認する	エンドユーザーは、オブジェクトの駆除中に対話型ウィンドウが表示され、修復アクション(削除または無視など)を選択する必要があります。このレベルは、検出された場合に実行する手順を理解している上級ユーザー向けに設計されています。



検査対象外とするファイル拡張子

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。このThreatSenseパラメーター設定のセクションでは、スキャンするファイルの種類を指定する方法を説明します。

ⓘ 他の種類の除外と混同しないでください。

既定では、すべてのファイルが検査されます。 スキャンから除外するファイルの一覧には、どの拡張子でも追加できます。

特定の種類のファイルをスキャンすると、特定の拡張子を使用するプログラムが適切に動作しなくなる場合は、ファイルの除外が必要になることがあります。たとえばMS Exchange Serverを使用しているときには、拡張子.edb、.eml、および.tmpを除外すると良いでしょう。

✓ 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。空のフィールドに拡張子を(tmpなど)を入力して、**[OK]**をクリックします。 **[複数の値を入力]**を選択すると、線、カンマ、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、区切り文字として、ドロップダウンから**セミコロン**を選択し、edb;eml;tmpを入力します)。
特殊記号?(疑問符)を使用できます。疑問符は任意の記号を表します(たとえば、?db).

ⓘ Windowsオペレーティングシステムでファイルの拡張子(ある場合)を正確に表示するには、**[コントロールパネル]**>**[フォルダオプション]**>**[表示]**(タブ)の**[既知のファイルタイプの拡張子を表示しない]**をオフにして、この変更を適用する必要があります。

追加のThreatSenseパラメータ

新規作成または変更されたファイルに適用する追加のThreatSenseパラメーター – 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、検出エンジンのアップデートの公開前でも新しいウイルスを検出できます。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)および圧縮された実行形式(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。

圧縮された実行形式、自己解凍形式、およびアドバンスドヒューリスティックの詳細については、ThreatSenseエンジンパラメータ設定を参照してください。

実行したファイルに適用する追加のThreatSenseパラメーター–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。

ネットワーク

ネットワークセクションでは、**詳細設定**の次のコンポーネントまたは設定にすばやくアクセスできます。

- **ファイアウォール** – ここでは、ESETファイアウォールのフィルタリングモードを調整できます。また、詳細設定にアクセスするには、**ファイアウォール**の横の歯車⚙ > [**設定**]をクリックするか、**F5**キーを押して**詳細設定**を表示します。

- **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。有害であると見なされるすべてのトラフィックはブロックされます。保護されていないワイヤレスネットワークや保護が弱いネットワークに接続するとESET Endpoint Securityによって通知されます。

- **ボットネット保護** – システム上のマルウェアを迅速かつ正確に特定します。 をクリックすると、特定の期間の間、ボットネット保護を無効にできます(非推奨)。

- **接続されたネットワーク** – ネットワークアダプタが接続されているネットワークを表示します。歯車をクリックした後、ネットワークアダプタ経由で接続しているネットワークの保護タイプを選択するように指示されます。このウィンドウでは、右下端に**ネットワークアダプタ**を表示することもできます。各ネットワークアダプタと割り当てられたファイアウォールプロファイルと信頼できるゾーンを表示することができます。詳細については、ネットワークアダプタを参照してください。

- **ブロックIPアドレスリスト** – 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。詳細については、このオプションをクリックしてF1を押してください。

- **トラブルシューティングウィザード** - ESETファイアウォールが原因の接続の問題を解決できます。詳細については、「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。



ファイアウォールの横の歯車クリックすると、次の設定が表示されます。

• **設定**– 詳細設定でファイアウォールウィンドウを開きます。ここでは、ファイアウォールでネットワーク通信を処理する方法を定義できます。

• **すべてのトラフィックをブロック** – すべての内向きおよび外向きの通信は、ファイアウォールによってブロックされます。このオプションは、セキュリティ上の重大なリスクの疑いがあってシステムをネットワークから切断する必要がある場合にのみ使用してください。ネットワークトラフィックフィルタリングが**すべてのトラフィックをブロック**モードのときに、**[すべてのトラフィックのブロックを停止]**をクリックすると、ファイアウォールを標準の動作に復元します。

• **ファイアウォールを一時停止(すべてのトラフィックを許可)** – すべてのネットワークトラフィックをブロックするオプションの逆です。 このオプションを選択すると、ファイアウォールのすべてのフィルタリングオプションが無効になり、すべての着信および発信が許可されます。 ネットワークトラフィックフィルタリングがこのモードのときに、**[ファイアウォールを有効にする]**をクリックして、ファイアウォールを再有効化します。

• **自動モード** – (別のフィルタリングモードが有効な場合) – クリックすると、フィルタリングモードを自動フィルタリングモードに変更します(ユーザー定義ルールを使用)。

• **対話モード** – (別のフィルタリングモードが有効な場合) – クリックすると、フィルタリングモードを対話フィルタリングモードに変更します。

ファイアウォール

ファイアウォールはシステムで送受信されるすべてのネットワークトラフィックを制御します。 指定したフィルタリングルールに基づいて個々のネットワーク接続が許可または拒否されます。 パーソナ

ルファイアウォールを使用することで、リモートコンピュータによる攻撃から保護したり、潜在的に危険なサービスをブロックしたりすることができます。

基本

ファイアウォールを有効にする

システムのセキュリティを保証するために、この機能を有効にすることをお勧めします。 ファイアウォールを有効にすると、ネットワークトラフィックは双方向にスキャンされます。

Windowsファイアウォールのルールも評価

自動モードではESETルールで明示的にブロックされていないかぎりWindowsファイアウォールのルールで許可された受信トラフィックも許可します。

グループポリシ(GPO)を使用して設定されたWindowsファイアウォールのルールは評価されません。

Filtering mode

ファイアウォールの動作は、フィルタリングモードによって異なります。フィルタリングモードは、必要なユーザー操作のレベルにも影響します。

ESET Endpoint Security ファイアウォールでは次のフィルタリングが利用できます。

フィルタリングモード	説明
ルール付き自動モード	既定のモードです。 このモードは、ルールを定義する必要なく、ファイアウォールを容易かつ簡便に使用したいユーザーに適しています。 カスタムのユーザー定義ルールを作成できますが、**自動モード**では必須ではありません。 ルール付き自動モードでは、付与されたシステムのすべての送信トラフィックが許可され、ほとんどの応答(IDSと詳細オプション/許可されたサービスで指定された信頼ゾーンからの一部のトラフィックを除く)がブロックされます。
対話モード	ファイアウォールのカスタム設定を作成できます。 通信が検出された際、その通信に適用されるルールがなければ、不明な接続を報告するダイアログウィンドウが表示されます。 このダイアログウィンドウでは、通信を許可するか拒否するかを選択できます。さらに、許可するか拒否するかの決定を、ファイアウォールの新規ルールとして保存することもできます。ユーザーが新しいルールを作成するように選択すると、それ以降、その種類の全ての接続がルールに従って許可または拒否されます。
ポリシーベースモード	接続を許可する特定のルールによって定義されていない全ての接続がブロックされます。 経験豊富なユーザーは、このモードを使用することで、必要かつ安全な接続のみを許可するルールを定義することができます。 その他の不明な接続は、ファイアウォールによってブロックされます。
学習モード	ルールを自動的に作成して保存します。このモードはファイアウォールの初期設定で最適ですが、長時間オンにしないでください。 事前定義されたパラメーターに従い、ESET Endpoint Securityによってルールが保存されるため、ユーザーによる操作は必要ありません。 学習モードではセキュリティに対するリスクを回避するために、必要な通信の全てのルールが完成するまでの間のみ使用してください。

プロファイルを使用すると、さまざまな状況で異なる複数のルールを指定してESET Endpoint Securityファイアウォールの動作をカスタマイズできます。

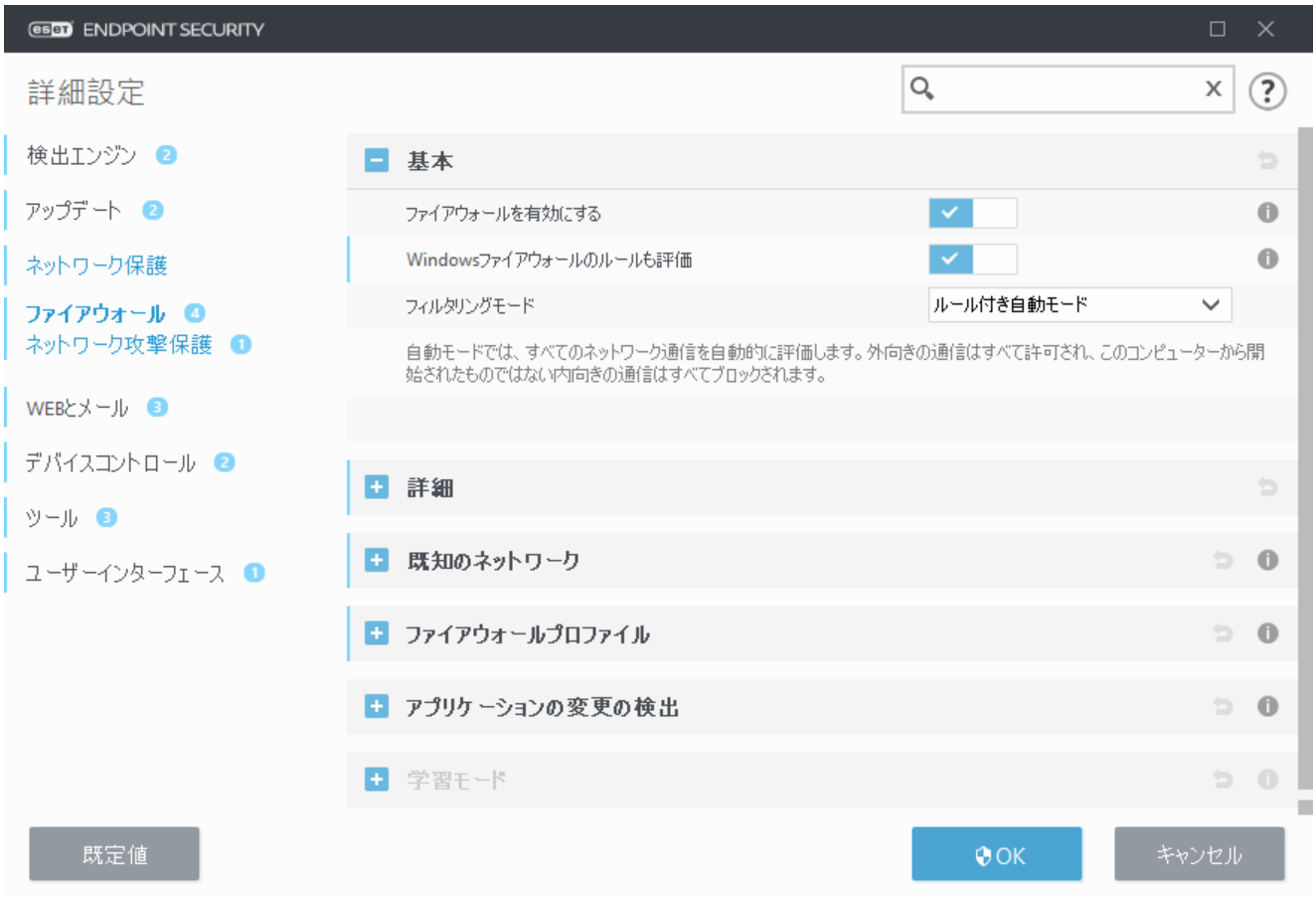
詳細

ルール

[ルールの設定]では、信頼済みゾーンおよびインターネット内で個々のアプリケーションによって生成されるトラフィックに適用されたすべてのルールを表示することができます。

ゾーン

ゾーンは、1つの論理グループを作成するネットワークアドレスの集合を表します。



ボットネットがコンピューターを攻撃するときにIDSルールを作成できます。 例外は、 **編集**をクリックして、**詳細設定** (F5)> **ネットワーク保護** > **ネットワーク攻撃保護** > **IDSルール**から修正できます。

学習モード

学習モードでは、システムで確立した各通信のルールを自動的に作成または保存します。事前定義されたパラメーターに従い、ESET Endpoint Securityによってルールが保存されるため、ユーザーによる操作は必要ありません。

このモードはシステムをリスクにさらす可能性があるため、ファイアウォールの初期設定時にのみ推奨されます。

詳細設定(F5) > **ファイアウォール** > **基本** > **フィルタリングモード**のドロップダウンメニューから**学習モー**

ドを選択し、**学習モードオプション**を有効にします。 このセクションには、次の項目があります。

学習モードでは、ファイアウォールでの通信のフィルタリングが行われません。全ての通信の送受信が許可されます。このモードでは、コンピュータはファイアウォールにより完全に保護されている状態ではなくなります。

学習モードの期限切れの後に設定されたモード – 学習モードの期間が終了した後に、ESET Endpoint Securityファイアウォールが戻るフィルタリングモードを定義します。詳細については、フィルタリングモードをお読みください。期限切れになった後は、ユーザーに確認オプションでファイアウォールフィルタリングモードに変更するには、管理者権限が必要です。

通信タイプ – 通信の各タイプに対して特定のルール作成パラメータを選択します。通信のタイプには、4種類あります。

信頼ゾーンからの受信トラフィック – 信頼ゾーン内の受信接続の例には、コンピュータで実行されているローカルアプリケーションとの通信を確立しようとしている、信頼ゾーン内のリモートコンピュータがあります。

信頼ゾーンへの送信トラフィック – ローカルネットワーク内または信頼ゾーンのネットワーク内の別のコンピュータとの接続を確立しようとしている、ローカルアプリケーション。

受信インターネットトラフィック – コンピュータで実行されているアプリケーションと通信しようとしているリモートコンピュータ。

送信インターネットトラフィック – 別のコンピュータとの接続を確立しようとするローカルアプリケーション。

各セクションでは、新しく作成したルールに追加するパラメータを定義できます。

ローカルポートの追加 – ネットワーク通信のローカルポート番号が含まれます。送信通信の場合、一般的にはランダムな番号が生成されます。そのため、このオプションは受信通信のみに有効にすることをお勧めします。

アプリケーションの追加 – ローカルアプリケーションの名前が含まれます。このオプションは、将来のアプリケーションレベルのルール(アプリケーション全体の通信を定義するルール)に最適です。たとえばWebブラウザまたはメールクライアントのみに通信を有効にすることができます。

リモートポートの追加 – ネットワーク通信のリモートポート番号が含まれます。たとえば、標準的なポート番号(HTTP - 80POP3 - 110など)に関連付けられた特定のサービスを許可または拒否できます。

リモートIPアドレス/信頼済みゾーンの追加 – ローカルシステムとそのリモートアドレス/ゾーン間の全てのネットワーク接続を定義する新しいルールに、リモートIPアドレスまたはゾーンをパラメーターとして使用できます。このオプションは、特定のコンピュータまたはコンピュータネットワークのグループに対するアクションを定義する場合に最適です。

アプリケーションに対する異なるルールの最大数 – アプリケーションがさまざまなポートを介してさまざまなIPアドレスと通信する場合などに、学習モードのファイアウォールはこのアプリケーションに対して適切な数のルールを作成します。このオプションにより、1つのアプリケーションに対して作成できるルールの数を制限できます。

ネットワーク攻撃保護

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。有害だと見なされるすべてのトラフィックがブロックされます。

ボットネット保護を有効にする – コンピュータが感染した場合や、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の通信およびコントロールサーバーを検出してブロックします。用語集のボットネット保護をお読みください

IDSルール – このオプションでは、コンピュータ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を検出する、詳細なフィルタオプションを設定できます。

詳細フィルタリングオプション

ファイアウォールおよびネットワーク攻撃保護セクションでは、詳細フィルタリングオプションを設定し、コンピューターに対して実行される可能性があるさまざまな種類の攻撃および脆弱性を検出できます。

ブロックされた通信についての脅威の通知を受け取らないことがあります。ファイアウォールログでブロックされたすべての通信を表示する手順については、「ロギングとログからのルールまたは例外の作成」を参照してください。

詳細設定(**F5**) > **ネットワーク保護** > **ファイアウォール**および詳細設定(**F5**) > **ネットワーク保護** > **ネットワーク攻撃保護**で使用可能な特定のオプションは、ファイアウォールモジュールのタイプとバージョン、およびオペレーティングシステムのバージョンによって異なる場合があります。

許可するサービス

このグループの設定は、信頼ゾーンからこのコンピュータのサービスにアクセスするための構成を簡素化するためのものです。ほとんどが定義済みファイアウォールルールを有効または無効にします。

- **信頼ゾーンでファイルとプリンタの共有を許可** – 信頼済みゾーン内のリモートコンピュータに共有ファイルおよび共有プリンタへのアクセスを許可します。
- **信頼ゾーンでのシステムサービスに対するUPNPを許可** – システムサービスに関して受信および送信されるUPnPプロトコルの要求を許可しますUPnP(ユニバーサルプラグアンドプレイMicrosoft Network Discoveryとも呼びます)はWindows Vista以降のオペレーティングシステムで使用されています。
- **信頼ゾーンでの内向きのRPC通信を許可** – 信頼ゾーンからのTCP接続を有効にしてMS RPC PortmapperおよびRPC/DCOMサービスへのアクセスを許可します。
- **信頼ゾーンでのリモートデスクトップを許可** - Microsoft Remote Desktop Protocol (RDP)プロトコル経由の接続を有効にしRDPを利用するプログラム(リモートデスクトップ接続など)を信頼ゾーン内のコンピューターで使用して、お使いのコンピューターにアクセスすることを許可します。信頼できるゾーン外データベースRDP接続を許可する方法も参照してください。
- **IGMP経由でのマルチキャストグループへのログインの有効化** - IGMPプロトコル(インターネットグループ管理プロトコル)を使用するプログラムによって生成されたビデオストリーミングなど、内向きおよび外向きのIGMPおよび内向きUDPマルチキャストストリームを許可します。
- **ブリッジ接続の通信を許可する** – ブリッジ接続を終了しないようにするには、このオプションを選択します。ブリッジされたネットワークは、ホストコンピューターのイーサネットアダプターを使用して、ネットワークに仮想マシンを接続します。ブリッジされたネットワークを使用すると、仮想マシンは、ネットワーク上の物理コンピューターであるかのように、ネットワーク上の他のデバイスにアクセスでき、その逆も可能です。
- **信頼ゾーンでのシステムサービスに対する自動Webサービス探索(WSD)を許可** – 信頼ゾーンからファイアウォールを通じてWebサービス探索要求の送受信を行うことを許可しますWSDは、ローカルネットワーク上でサービスを見つけるために使用されるプロトコルです。

- **信頼ゾーンでマルチキャストアドレスの解決を許可(LLMNR)** - LLMNR(リンクローカルマルチキャスト名前解決)とはDNSサーバーやDNSクライアントを設定しなくてもIPv4とIPv6の両方のホストで同じロー

カルリンク上のホストの名前解決が可能な、DNSパケットベースのプロトコルです。このオプションでは、信頼ゾーンからファイアウォールを通じたDNS要求の受信が許可されます。
• **Windows 7ホームグループサポート** - Windows 7以降のオペレーティングシステムのホームグループサポートを有効にします。ホームグループは、ホームネットワーク上のファイルやプリンタを共有できます。ホームグループを構成するには、[**スタート**] > [**コントロール パネル**] > [**ネットワークとインターネット**] > [**ホームグループ**]に移動します。

侵入検出

• **[プロトコル SMB]**- SMBプロトコルの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。

• **不正サーバーチャレンジ攻撃認証を検出** – 認証の際にユーザー認証を取得しようとして不正なチャレンジを使用する攻撃から保護します。

• **名前付きパイプを開くときのIDS回避を検出** - SMBプロトコルでMSRPC名前付きパイプを開くために使用される既知の回避方法を検出します。

• **CVE検出** (Common Vulnerabilities and Exposures) - SMBプロトコルでのさまざまな攻撃、フォーム、セキュリティホール、悪用に関する実装済みの検出方法です。CVE識別子(CVEs)に関する詳細については、cve.mitre.orgのCVE Webサイトを参照してください。

• **プロトコルRPC** - 分散コンピューティング環境(DCE)のために開発されたリモートプロシージャコールシステムでの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(前記を参照)。

• **ARPポイズニング攻撃を検出** – 中間者攻撃によるARPポイズニング攻撃の検出、またはネットワークスイッチにおける盗聴の検出。ARP(アドレス解決プロトコル)は、Ethernetアドレスを決定するためにネットワークアプリケーションまたはデバイスによって使用されます。

• **TCPポートスキャニング攻撃を検出** – ポートスキャニングソフトウェア、すなわち、アクティブなポートを見つけてサービスの脆弱性を悪用することを目的として、広い範囲のポートアドレスにクライアント要求を送信し、ホストの開いているポートを調べるように設計されたソフトウェアによる攻撃を検出します。この攻撃の詳細については、「用語集」を参照してください。

• **攻撃を検出したら安全ではないアドレスを遮断** – 攻撃の元であると検出されたIPアドレスは、一定の時間、接続を遮断するためにブラックリストに追加されます。

• **攻撃の検出後に通知を表示** – 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。

• **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や、脅威によってこの方法でシステムに侵入する試みが行わ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用共有への内向き接続を許可** – 管理用共有は、既定のネットワーク共有で、システム内のハードドライブのパーティション(*C$*、*D$*、...)をシステムフォルダ(*ADMIN$*)と共有します。管理用要求への接続を無効にすると、多くのセキュリティリスクが低下します。たとえば、Conficker ワームは管理用共有に接続するためにディクショナリアタックを行います。

• **古い(サポート対象外) SMBダイアレクトを遮断** - IDSによって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セッションを遮断します。最近の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を確保するために、古いSMBダ

イアレクトをサポートしています。攻撃者は、SMBセッションで古いダイアレクトで使用することにより、トラフィック検査を逃れることができます。お使いのコンピュータで古いバージョンのWindowsを搭載したコンピュータとファイルを共有する必要がない場合は(または通常のSMB通信を使用)、古いSMBダイアレクトを遮断してください。

- **拡張セキュリティのないSMBセキュリティを遮断** - SMBセッションネゴシエーションの際、LAN Managerチャレンジ/レスポンス(LM)認証よりも安全な認証メカニズムを提供するために、拡張セキュリティを使用できますLMスキームは、脆弱であると考えられ、使用は推奨されません。

- **SMBプロトコルで信頼ゾーンの外部にあるサーバ上の実行可能ファイルをオープンすることを遮断** – ファイアウォールの信頼ゾーンに属していないサーバー上の共有フォルダにある実行可能ファイル(.exe.dll)を開こうとすると、接続がドロップされます。信頼できるソースから実行ファイルをコピーすることは合法ですが、この検出によって不審なファイルが悪意のあるサーバーで開かれるリスクを低減します(共有された悪意のある実行ファイルへのハイパーリンクをクリックして開くファイルなど)。

- **信頼ゾーン内にあるサーバーへの接続に対するSMBプロトコルでのNTLM認証を遮断** - NTLM (両方のバージョン)認証スキームを使用するプロトコルは、資格情報転送攻撃(SMBプロトコルではSMBリレー)攻撃の対象になります。信頼ゾーンの外側にあるサーバーでのNTLM認証を遮断すると、信頼ゾーンの外側にある悪意のあるサーバーによって資格情報が転送されるリスクが軽減されます。同様に、信頼ゾーン内のサーバーによるNTLM認証を遮断することも考えられます。

- **セキュリティアカウントマネージャ(SAM)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(LSA)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]と[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** - MSRPCは、MicrosoftによるDCE RPCメカニズムの実装です。またMSRPCでは、転送(ncacn_np転送)のためにSMB(ネットワークファイル共有)プロトコルで名前付きパイプを使用できますMSRPCサービスにはWindowsシステムをリモートからアクセスして管理するためのインタフェースが用意されていますWindows MSRPCシステムに関しては、いくつかのセキュリティ上の脆弱性が発見、悪用されてきました(ConficklerワームSasserワームなど)。多くのセキュリティリスク(リモートコード実行、サービス拒否攻撃など)低下させるために、提供する必要がないMSRPCサービスとの通信は無効にしてください。

IDSルール

一部の状況では、Intrusion Detection Service (IDS)によって、ルーターまたは他の内部ネットワークデバイスとの間の通信が攻撃の可能性として検出される場合があります。たとえば、確認済みの安全なアドレスをIDSゾーンから除外されたアドレスに追加してIDSによる検出を回避することができます。

次のESETナレッジベース記事は、英語でのみ提供されている場合があります。
- クライアントワークステーションでESET Endpoint Security (8.x)のIDSルールを作成する
- クライアントワークステーションでESET PROTECT (8 .x)のIDSルールを作成

列

- **検出** – 検出のタイプ。

- **アプリケーション** - ...(*C:\Program Files\Firefox\Firefox.exe*など)をクリックして、想定されたアプリケーションのファイルパスを選択します。アプリケーション名は入力しないでください。

- **リモートIP** – リモートIPv4またはIPv6アドレス/範囲/サブネットのリスト。複数のアドレスはコンマで区切る必要があります。

- **ブロック** – すべてのシステムプロセスには独自の既定の動作があり、アクション(ブロックまたは許可)が割り当てられています。ESET Endpoint Securityの既定の動作を無効にするには、ドロップダウンメニューを使用して、動作をブロックするか許可するかどうかを選択できます。

- **通知** – はいを選択すると、コンピューターでデスクトップ通知を表示します。デスクトップ通知を表示しない場合は、いいえを選択します。既定/はい/いいえの値を使用できます。

- **ログ** – **はい**を選択すると、 ESET Endpoint Securityログファイルにイベントを記録します。イベントを記録しない場合は、**いいえ**を選択します。**既定/はい/いいえ**の値を使用できます。

管理者がESET PROTECT Webコンソールで IDS除外を作成する場合は、タブ除外が表示されます。IDS除外には許可ルールのみが含まれ、IDSルールの前に評価されます。

IDSルールの管理

- **追加** – クリックすると、新しいIDSルールを作成します。
- **編集** – クリックすると、既存のIDSルールを編集します。

- **削除** - IDSルールのリストから既存の例外を削除する場合は、選択してクリックします。

-  **最上位/上/下/最下位** – ルールの優先度レベルを調整できます(例外は最上位から最下位へと評価されます)。

イベントが発生するたびに、通知を表示して、ログを記録する。
1.**追加**をクリックして、新しいIDSルールを追加します。
2.**検出**ドロップダウンメニューから特定の検出を選択します。
3.**...**をクリックし、通知を適用する特定のアプリケーションのファイルパスを入力します。
4.**ブロック**ドロップダウンメニューで**既定**を選択したままにしますESET Endpoint Securityで適用された既定のアクションが継承されます。
5.**通知**と**ログ**ドロップダウンメニューを、**はい**に設定します。
6.**OK**をクリックしてこの通知を保存します。

脅威と見なさない検出のタイプに関する繰り返し通知を削除する。
1.**追加**をクリックして、新しいIDS例外を追加します。
2.**検出**ドロップダウンメニューから特定の検出を選択します。例：**セキュリティ拡張なしSMBセッション TCPポートスキャニング攻撃**.
3.受信通信の場合は、ドロップダウンメニューで**受信**を選択します。
4.**通知**ドロップダウンメニューを**いいえ**に設定します。
5.**ログ**ドロップダウンメニューを**はい**に設定します。
6.**アプリケーション**を空白のままにします。
7.通信から特定のIPからではない場合、**リモートIPアドレス**を空白にします。
8.**OK**をクリックしてこの通知を保存します。

不審な脅威がブロックされました

この状況は、コンピュータのアプリケーションがネットワーク上の別のコンピュータに悪意のあるトラフィックを送信し、セキュリティホールを利用しようとしている場合や別のユーザーがネットワーク上のポートを検査しようとしている場合に発生することがあります。

脅威 – 脅威の名前。

ソース – ソースネットワークアドレス。

ターゲット – ターゲットネットワークアドレス。

ブロックを中止– 不審な脅威について通信を許可する設定のIDSルールを作成します。

ブロックを続ける– 検出された脅威をブロックします。この脅威について通信をブロックする設定のIDSルールを作成するには、**次回以降通知しない**を選択します。

検出された脅威のタイプによっては、通知ウィンドウに表示される情報が異なる場合があります。脅威と他の関連用語の詳細については、リモート攻撃のタイプまたは検出のタイプを参照してください。

ネットワーク保護トラブルシューティング

トラブルシューティングウィザードではESETファイアウォールが原因の接続の問題を解決できます。ドロップダウンメニューから、通信がブロックされた期間を選択します。 最近ブロックされた通信のリストで、アプリケーションやデバイスの種類、評判とその期間中にブロックされたアプリケーションとデバイスの合計数についての概要の説明を確認できます。 ブロックされた通信の詳細については、**詳細**をクリックします。 次のステップは、接続の問題が発生したアプリケーションやデバイスのブロックの解除です。

[ブロック解除]をクリックすると以前ブロックされた通信が許可されます。 それ以降もアプリケーションで問題が発生する場合、またはデバイスが期待どおりに動作しない場合は、**[アプリケーションが動作しません]**をクリックすると、以前にそのデバイスでブロックされたすべての通信が許可されます。問題が解決しない場合は、コンピューターを再起動します。

変更の表示をクリックすると、ウィザードによって作成されたルールが表示されます。 また、**詳細設定 > ネットワーク保護 > ファイアウォール > 詳細 > ルール**から作成されたルールを確認することができます。

別のブロックを解除で、異なるデバイスやアプリケーションとの通信の問題をトラブルシューティングできます。

ネットワーク名

接続されたネットワークセクションは、ESET Endpoint Securityのメインプログラムウィンドウから、**設定** > **ネットワーク** > **接続されたネットワーク**をクリックしてアクセスできます。

どのネットワークアダプタに接続されているかを示すものです。 ネットワーク名の下のリンクをクリックした後、ネットワークアダプタ経由で接続しているネットワークの保護タイプ(徹底的な保護モードか、許容モード)を選択するように指示されます。または歯車⚙をクリックして**詳細設定**で選択を変更できます。 – この設定は、お使いのコンピュータをネットワーク上の他のコンピュータからどれだけアクセスしやすくするかを設定します。

3つのネットワークロケーションタイプに接続できます。

- **パブリックネットワーク** – このタイプのネットワークロケーションは公共の場所用であり、信頼できません。デバイスはネットワークに表示されません。ネットワーク上の他のデバイスは表示されません。パブリックネットワークでは、ネットワーク検出は既定で無効です。

- **自宅または職場ネットワーク** – パブリックネットワークとは異なり、リソースをプライベートネットワークのLANにある他のコンピューターと共有できます。ネットワーク上のデバイスを把握していて、信頼できる場合は、**自宅または職場ネットワーク**を選択します。

- **ドメインネットワーク** – ネットワーク管理者がこのタイプのネットワークロケーションを制御しています。ユーザーはこのタイプのネットワークを選択または変更できません。ドメインネットワークロケーションタイプは、ローカルコンピューターがActive Directory Domain Servicesのメンバーのときに検出されます。ローカルコンピューターは、ネットワーク接続経由で、そのドメインのドメインコントローラーで認証できます。

ネットワークロケーションを選択すると、コンピューターが常に適切なセキュリティレベルに設定されることを保証できます。

ウィンドウの下部の**ネットワークアダプタ**をクリックすることにより、 各ネットワークアダプタ、割り当てられたファイアウォールプロファイル、および信頼ゾーンを表示できます。 詳細については、「ネットワークアダプタ」を参照してください。

Windows設定を使用するを選択すると、ウィンドウが表示されず、接続されたネットワークはWindows設定に従って自動的に設定されます。この設定により、新しいネットワークから、特定の機能(ファイル共有やリモートデスクトップなど)にアクセスできるようになります。

既知のネットワーク

パブリックネットワークや標準の企業ネットワーク外のネットワークに頻繁に接続するコンピュータを使用している場合は、接続先の新しいネットワークの信頼性を検証することをお勧めします。ネットワークが定義されると、**ネットワークID**で設定されたさまざまなネットワークパラメータを使用してESET Endpoint Securityは信頼できる(ホーム/オフィス)ネットワークを認識できます。コンピュータは、信頼されるネットワークで使用されているIPアドレスに類似したIPアドレスを使用して、ネットワークに接続することがよくあります。このような場合ESET Endpoint Securityは不明なネットワークを信頼できる(ホーム/オフィス)ネットワークと見なすことがあります。**ネットワーク認証**を使用して、このような状況を回避することをお勧めします。

ネットワークアダプタがネットワークに接続されたり、ネットワーク設定が構成されたりするとESET Endpoint Securityは既知のネットワークリストから新しいネットワークと一致するレコードを検索します。**[ネットワークID]**と**[ネットワーク認証]**(オプション)が一致する場合、このインターフェイスでネッ

トワークが接続済みに設定されます。不明なネットワークが見つかった場合、ネットワーク識別設定により、新しいネットワーク接続が作成され、次回接続するときにそのネットワークが特定されます。既定では、新しいネットワーク接続は**パブリックネットワーク**保護タイプを使用します。**[新しいネットワークが検出されました]**ダイアログウィンドウでは、**パブリックネットワーク**または**ホーム/会社ネットワーク**、または**Windows設定を使用する**保護タイプのいずれかを選択するように指示されます。ネットワークアダプタが既知のネットワークに接続され、ネットワークが**ホーム/会社ネットワーク**に設定されると、アダプタのローカルサブネットが信頼ゾーンに追加されます。

新しいネットワークの保護タイプ – 次のオプションから選択しますWindows設定を使用する、ユーザーに確認する、またはパブリックに設定するは、新しいネットワークで既定で使用されます。

> **Windows設定を使用する**を選択すると、ダイアログが表示されず、接続されたネットワークはWindows設定に従って自動的に設定されます。このため、新しいネットワークから、特定の機能(ファイル共有やリモートデスクトップなど)にアクセスできるようになります。

[既知のネットワークエディタ]ウィンドウでは、既知のネットワークを手動で編集できます。

既知のネットワークエディタ

[詳細設定] > [ネットワーク保護] > [ファイアウォール] > [既知のネットワーク] で**既知のネットワーク**の横の**[編集]**をクリックすると、既知のネットワークを手動で変更できます。

列

名前 – 既知のネットワークの名前。

保護タイプ – ネットワークが**ホームまたはオフィスネットワーク**パブリック、または**Windows設定を使用する**のいずれに設定されているのかを示します。

ファイアウォールプロファイル - **[次のプロファイルで使用するルールを表示する]**ドロップダウンメニューからプロファイルを選択し、プロファイルのルールフィルタを表示します。

プロファイルのアップデート – このネットワークに接続するときに、作成されたアップデートプロファイルを適用できます。

コントロール要素

追加 – 新しい既知のネットワークを作成します。

編集 – クリックすると、既存の既知のネットワークを編集します。

削除 – ネットワークを選択し、**[削除]**をクリックすると、既知のネットワークのリストから削除されます。

 **最上位/上/下/最下位** – 既知のネットワークの優先度レベルを調整できます(ネットワークは最上位から最下位へと評価されます)。

ネットワーク構成設定は、次のタブに分類されます。

ネットワーク

ここでは、**ネットワーク名**を定義し、ネットワークの**保護タイプ**([パブリックネットワーク]、[ホームまたはオフィスネットワーク]、または[Windows設定を使用する])を選択します。**[ファイアウォールプロファイル]**ドロップダウンメニューを使用し、このネットワークのプロファイルを選択します。ネットワークが**ホームまたはオフィスネットワーク**保護タイプを使用する場合は、すべての直接接続された

ネットワークサブネットは信頼できると見なされます。例えば、ネットワークアダプタがIPアドレス192.168.1.5とサブネットマスク255.255.255.0を使用してこのネットワークに接続する場合、サブネット192.168.1.0/24がアダプタの信頼ゾーンに追加されます。アダプタにその他のアドレス/サブネットがある場合は、既知のネットワークの**ネットワークID**設定に関係なく、すべてが信頼されます。

また、**[追加の信頼できるアドレス]**で追加されたアドレスは、ネットワークの保護タイプに関係なく、このネットワークに接続されたアダプタの信頼ゾーンに常に追加されます。

弱いWi-Fi暗号化を警告する – ESET Endpoint Securityは、保護されていないワイヤレスネットワークまたは保護が弱いネットワークに接続するときに通知します。

ファイアウォールプロファイル – このネットワークに接続するときに使用されるファイアウォールプロファイルを選択します。

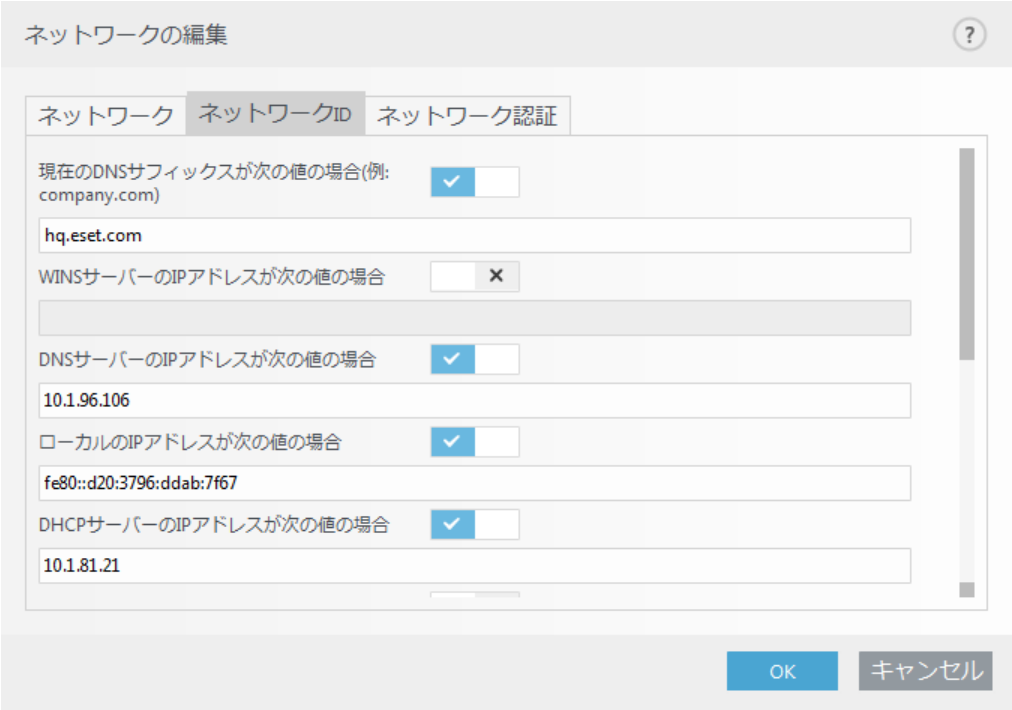
アップデートプロファイル – このネットワークに接続するときに使用されるアップデートプロファイルを選択します。

接続されたネットワークのリストで接続に設定されているネットワークの場合、次の条件が満たされる必要があります。

- **ネットワークID** – すべての入力済みパラメータはアクティブな接続パラメータと一致する必要があります。
- **ネットワーク認証** – 認証サーバーが選択されている場合、ESET Authentication Serverとの認証が正常に実行される必要があります。

ネットワークID

ネットワークIDは、ローカルのネットワークアダプタのパラメータに基づいて実行されます。すべての選択されたパラメータは、アクティブなネットワーク接続の実際のパラメータに対して比較されます。IPv4およびIPv6アドレスはいずれも許可されます。



ネットワーク認証

ネットワーク認証によってネットワーク内の特定のサーバーが検索され、非対称暗号化(RSA)を使用してそのサーバーが認証されます。認証中のネットワークの名前が、認証サーバー設定で指定されたゾーン名と一致する必要があります。名前は大文字と小文字を区別します。サーバー名、サーバーリスニングポート、およびサーバーの秘密鍵に対応する公開鍵を指定します(「ネットワーク認証 – サーバーの設定」を参照)。サーバー名はIPアドレス、DNS、またはNetBios名の形式で入力でき、後ろにサーバーの鍵の場所を指定するパスを続けることができます(例: server_name_/directory1/directory2/authentication)。後ろにパスを付け、セミコロンで区切ると、代替サーバーを指定できます。

ESET認証サーバーをダウンロード

公開鍵は、次のいずれかの種類のファイルを使用してインポートできます。

- PEM暗号化公開鍵(.pem)。この鍵は、ESET認証サーバーを使用して生成できます(「ネットワーク認証 – サーバーの設定」を参照)。
- 暗号化公開鍵
- パブリックキー証明書(.crt)



[テスト]をクリックして設定をテストします。認証が成功すると、[サーバーの認証に成功しました]が表示されます。認証が正常に設定されないと、次のいずれかのエラーメッセージが表示されます。

サーバーの認証に失敗しました。署名が無効であるか、一致しません。
サーバー署名が入力された公開鍵と一致しません。

サーバーの認証に失敗しました。ネットワーク名が一致しません。
設定されているネットワーク名が、認証サーバーゾーン名と一致していません。両方の名前を確認し、同じであることを確かめてください。

サーバーの認証に失敗しました。 サーバーからの応答が無効か、応答がありません。
サーバーが実行中ではないか、アクセスできない場合、応答を受信しません。 別のHTTPサーバーが指定されたアドレスで実行されていると、無効な応答が受信される場合があります。

無効な公開鍵が入力されました。
入力された公開鍵ファイルが破損していないことを確認します。

ネットワーク認証 – サーバー構成

認証プロセスは、認証対象のネットワークに接続されている任意のコンピューター/サーバーによって実行できます。クライアントがネットワークに接続しようとする場合に常に認証のためにアクセスできるコンピューター/サーバーに、ESET認証サーバーアプリケーションをインストールする必要があります。ESET認証サーバーアプリケーションのインストールファイルは、ESET製品のWebサイトからダウンロードできます。

ESET認証サーバーアプリケーションをインストールすると、ダイアログウィンドウが表示されます([**スタート**] > [**プログラム**] > [**ESET**] > [**ESET認証サーバ**]をクリックしてこのアプリケーションにアクセスできます)。

認証サーバーを設定するには、認証ネットワーク名、サーバーリスニングポート(既定値は80)、および公開鍵と秘密鍵のペアを保管する場所を入力します。次に、認証プロセスで使用する公開鍵と秘密鍵を生成します。秘密鍵はサーバー上に設定されたままですが、公開鍵は、クライアント側でファイアウォール設定でネットワークを設定するときに、[ネットワーク認証]セクションにインポートする必要があります。

ファイアウォールプロファイル

グローバル既定プロファイル – ネットワークまたはネットワークアダプタ設定からのプロファイルがない場合、グローバル既定プロファイルが使用されます。

プロファイルのリスト – プロファイルを使用してESET Endpoint Securityファイアウォールの動作を制御できます。ファイアウォールルールの作成時または編集時に、そのルールを特定のプロファイルに割り当てることもすべてのプロファイルに適用することもできます。ネットワークインターフェイスでプロファイルがアクティブな場合、グローバルルール(プロファイルの指定がないルール)と選択したプロファイルに割り当てられているルールのみが適用されます。複数のプロファイルを作成し、異なるルールをネットワークアダプタまたはネットワークに割り当てると、ファイアウォールの動作を簡単に変更できます。

ネットワークアダプタに割り当てられたプロファイル – ネットワークアダプタを設定し、そのネットワークに接続したときに、特定のネットワークに設定されたプロファイルを使用できます。

また、[**詳細設定**] (F5) > [**ファイアウォール**] > [**既知のネットワーク**]の特定のネットワーク上で使用する特定のプロファイルを割り当てることができます。**既知のネットワーク**のリストからネットワークを選択し、[**編集**]をクリックし、[**ファイアウォール**]ドロップダウンメニューから特定のネットワークにファイアウォールプロファイルを割り当てます。ネットワークにプロファイルが割り当てられていない場合、アダプタの既定のプロファイルが使用されます。ネットワークプロファイルを使用するようにアダプタが設定されていない場合は、接続先のネットワークに関係なく、既定のプロファイルが使用されます。ネットワークまたはアダプタ設定のプロファイルがない場合、既定のグローバルプロファイルが使用されます。ネットワークアダプタにプロファイルを割り当てるには、ネットワークアダプタを選択し、[**ネットワークアダプタに割り当てられたプロファイル**]の横にある[**編集**]をクリックします。[**既定のファイアウォールプロファイル**]ドロップダウンメニューからプロファイルを選択してから、**[OK]**をクリックします。

ファイアウォールが他のプロファイルに切り替わった場合、右下に通知が表示されます。

ネットワークアダプタに割り当てられたプロファイ

ル

プロファイルを切り替えると、ファイアウォール動作の複数の変更を簡単に確立できます。特定のプロファイルに対して、カスタムルールを設定し、適用できます。コンピュータに存在するすべてのアダプタのネットワークアダプタエントリは、自動的に[**ネットワークアダプタ**]リストに追加されます。

列

名前 – ネットワークアダプタの名前。

既定のファイアウォールプロファイル – 接続先のネットワークでプロファイルが設定されていないか、ネットワークアダプタがネットワークプロファイルを使用するように設定されていない場合は、既定のプロファイルが使用されます。

ネットワークのプロファイルを優先 – ネットワークアダプタは接続された既知のネットワークに設定されたファイアウォールプロファイルを使用できます。ネットワークのプロファイルが設定されていないか、ネットワークアダプタがネットワークのプロファイルを使用するように設定されていない場合、アダプタの既定のプロファイルが使用されます。

コントロール要素

追加 – 新しいネットワークアダプターを追加します。

編集 – クリックすると、既存のネットワークアダプタを編集します。

削除 – リストからネットワークアダプタを削除する場合は、ネットワークアダプタを選択してクリックします。

OK/キャンセル – 変更を保存する場合は**[OK]**をクリックします。変更せずに終了する場合は[**キャンセル**]をクリックします。

アプリケーションの変更の検出

ファイアウォールルールが設定されているアプリケーションが変更され、接続を確立しようとすると、アプリケーションの変更検出機能によって通知が表示されます。これは、別のアプリケーションによってアプリケーションに対して構成されたルールの悪用を防止するうえで有効です。元のアプリケーションの実行ファイルが一時的または永久に別のアプリケーション実行ファイルで置換されたり、元のアプリケーションの実行ファイルが悪意のある方法で変更されて悪用されることがあります。

この機能は、一般的にアプリケーションの変更を検出するためのものではありません。既存のファイアウォールルールの悪用を防止するものであり、特定のファイアウォールルールが存在するアプリケーションだけが監視されます。

アプリケーションの変更の検出を有効にする – 選択すると、アプリケーションに対する変更(更新、感染、その他の変更)が監視されます。変更されたアプリケーションが接続を確立しようとすると、ファイアウォールによって通知されます。

署名された(信頼された)アプリケーションの変更を許可する – 変更の前後でアプリケーションに同じ有効なデジタル署名がある場合は通知しません。

確認から除外されたアプリケーションのリスト – 通知なく修正が許可されている個別のアプリケーションを追加または削除できます。

変更の検出から除外されたアプリケーション

ESET Endpoint Securityのファイアウォールは、ルールが存在するアプリケーションの変更を検出します(「アプリケーションの変更の検出」を参照)。

しかし、特定のアプリケーションではこの機能を使用せず、ファイアウォールによる検査から除外したいと思うこともあるかもしれません。

追加 – ウィンドウが開き、変更の検出から除外されるアプリケーションのリストに追加するアプリケーションを追加できます。オープンネットワーク通信で実行中のアプリケーションの一覧から選択できます。このようなアプリケーションではファイアウォールルールが存在するか、特定のアプリケーションを追加します。

編集 – ウィンドウが開き、変更の検出から除外されるアプリケーションのリストにあるアプリケーションを追加できます。オープンネットワーク通信で実行中のアプリケーションの一覧から選択できます。このようなアプリケーションではファイアウォールルールが存在するか、手動で場所を変更します。

削除 – 変更の検出から除外されるアプリケーションのリストからエントリを削除します。

ルールの設定と使用

ルールは、全てのネットワーク接続をテストするために使用される条件およびそれらの条件に割り当てられた全てのアクションのセットを表します。ファイアウォールルールを使用すると、各種ネットワーク接続が確立されるときに実行されるアクションを定義できます。ルールフィルタリング設定にアクセスするには、**詳細設定** (F5) > **ネットワーク保護** > [**ファイアウォール**] > **詳細**に移動します。一部の定義済みルールは**許可されたサービス**(IDSと詳細オプション)のチェックボックスに関連付けられ、直接オフにすることはできません。オフにする場合は、関連付けられたチェックボックスを使用します。

以前のバージョンのESETEndpointSecurityとは異なり、ルールは上から下に評価されます。評価中の各ネットワーク接続に対して、最初に一致するルールのアクションが使用されます。これは、以前のバージョンからの重要な動作上の変更点です。以前のバージョンでは、ルールの優先度が自動的に決定され、一般的なルールよりも具体的なルールになるほど優先度が高くなっていました。

接続は着信と発信に分けることができます。着信は、ローカルシステムとの接続を確立しようとしているリモートコンピューターによって開始されます。送信接続は反対方向に動作し、ローカルシステムがリモートコンピュータにアクセスします。

不明な通信が新たに検出された場合は、その接続を許可するか拒否するかを慎重に検討してください。受信者側が送信を要求していない接続、安全でない接続、または不明な接続は、システムにセキュリティ上のリスクをもたらします。このような接続が確立された場合は、コンピューターに接続しようとしているリモートコンピューターおよびアプリケーションに特に注意することをお勧めします。個人データを取得して送信しようとしたり、他の悪意のあるアプリケーションをホストワークステーションにダウンロードしようとしたりするマルウェアが多数あります。ファイアウォールを使用すると、ユーザーはこのような接続を検出し、切断することができます。

ファイアウォールルールリスト

ファイアウォールルールリストは、**詳細設定**(F5) > **ネットワーク保護** > **Firewall** > **基本**にあります。これは、**ルール**の横の**編集**をクリックすると表示されます。

列

名前 – ルールの名前。

有効 – ルールが有効か無効かを示します。ルールを有効にするには、対応するチェックボックスを選択する必要があります。

プロトコル – このルールが有効なプロトコルを示します。

プロファイル – このルールが有効なファイアウォールプロファイルを示します。

アクション – 通信のステータス(ブロック/許可/確認)を表示します。

方向 – 通信の方向(受信/送信/双方向)。

ローカル – ローカルコンピューターのリモートIPv4またはIPv6アドレス/範囲/サブネットおよびポート。

リモート – リモートコンピューターのリモートIPv4またはIPv6アドレス/範囲/サブネットおよびポート。

アプリケーション – ルールの適用先のアプリケーション。



コントロール要素

追加 - 新しいルールを作成します

編集 – 既存のルールを変更します。

削除 – 既存のルールを削除します。

コピー – 選択したルールのコピーを作成します。

すべてのルール(定義済み)を表示 – 特定の通信を許可または遮断するESET Endpoint Securityによって定義されたルール。これらのルールを無効にできますが、定義済みルールは削除できません。

最上位/上/下/最下位 – ルールの優先度レベルを調整できます(ルールは最上位から最下位へと実行されます)。

右上の検索アイコン🔍をクリックし、名前、プロトコル、またはポートでルールを検索します。

ファイアウォールルールの追加または編集

監視するパラメータが変更されるたびに、ルールを変更する必要があります。ルールが条件を満たせず、指定したアクションが適用できないような変更が行われた場合、指定された接続が拒否されることがあります。これによって、ルールの影響を受けるアプリケーションの動作で問題が生じる場合があります。一例として、リモート側のネットワークアドレスやポート番号の変更があります。

次のESETナレッジベース記事は、英語でのみ提供されている場合があります。
- ESET Endpoint Securityでのファイアウォールルールの作成または編集
- ESET Security Management Centerでのクライアントワークステーション用のファイアウォールルールの作成または編集

ウィンドウの上部には、次の3つのタブがあります。

- **一般** – ルール名、接続の方向、アクション(**許可**⍰**拒否**⍰**確認**)、プロトコル、およびルールが適用するプロファイルを指定します。

- **ローカル** – 接続のローカル側に関する情報が表示されます。この情報には、ローカルポートまたはポート範囲の番号および通信するアプリケーションの名前などがあります。[**追加**]をクリックして、ここでIPアドレスの範囲を指定し、定義済みまたは作成したゾーンを追加することもできます。

- **リモート** – リモートポート(ポート範囲)に関する情報が表示されます。ユーザーはこのタブを使用して、指定したルールのリモートIPアドレスまたはゾーンのリストを定義することができます。[**追加**]をクリックして、ここでIPアドレスの範囲を指定し、定義済みまたは作成したゾーンを追加することもできます。

新しいルールを作成するときは、ルールの名前を[**名前**]フィールドに入力する必要があります。[**方向**]ドロップダウンメニューからルールが適用される方向を選択し、[**アクション**]ドロップダウンメニューから通信がルールを満たすときに実行するアクションを選択します。

プロトコル– ルールに使用される転送プロトコル。ドロップダウンメニューから、特定のルールで使用するプロトコルを選択します。

ICMPタイプ/コードは、番号で識別されるICPMメッセージを表します(例: 0は「エコー応答」)。

既定では、**すべてのプロファイル**に対してすべてのルールが有効です。あるいは、[**プロファイル**]ドロップダウンメニューを使用して、作成したファイアウォールプロファイルを選択します。

[**ログ記録の重大度**]をオンにすると、ルールに関連付けられているアクティビティがログに記録されます。[ユーザーに通知する]を選択すると、ルールが適用されたときに通知が表示されます。



警告ステータスのファイアウォールログは、ESET Security Management Centerによって収集できます

次に、新しいルールを作成してFirefox Webブラウザーアプリケーションがインターネット/ローカルネットワークWebサイトにアクセスできるようします。この例では、次を設定する必要があります。
1.[**一般**]タブではTCPおよびUDPプロトコルを介した送信通信を有効にします。
2.**ローカル**タブをクリックします。
3.**...**をクリックして、使用するWebブラウザーのファイルパスを選択します(たとえば、*C:\Program Files\Firefox\Firefox.exe*)。アプリケーションの名前は入力しないでください。
4.標準のインターネット閲覧を許可する場合、[**リモート**]タブでポート番号80および443を有効にします。

定義済みルールは限られた方法でしか修正できません。

ファイアウォールルール - ローカル

ルールが適用されるローカルアプリケーションおよびローカルポートの名前を指定します。

ポート - ローカルポート番号。番号を指定しなかった場合、全てのポートにルールが適用されます。1つの通信ポートまたは通信ポートの範囲を追加します。

IP - ルールが適用されるリモートアドレス、アドレス範囲、またはサブネットを追加します。値を指定しなかった場合、全ての通信にルールが適用されます。

ゾーン - 追加されたゾーンのリスト。

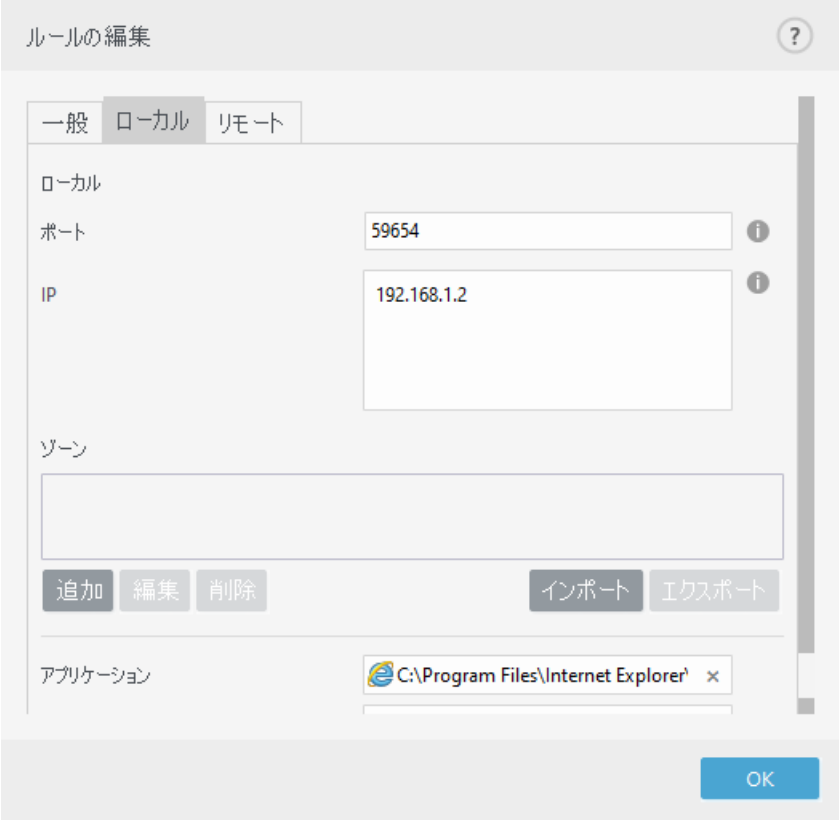
追加 - 作成したゾーンをドロップダウンメニューから追加します。ゾーンを作成するには、[ゾーンの設定]タブを使用します。

削除 - リストからゾーンを削除します。

アプリケーション – ルールの適用先のアプリケーションの名前。ルールが適用されるアプリケーションの場所を追加します。

サービス – ドロップダウンメニューには、システムサービスが表示されます。

ドロップダウンメニューの通信でEHttpSrv サービスを使用して、ポート2221経由でアップデートを提供するミラー用のルールを作成できます。



ファイアウォールルール – リモート

ポート – リモートポート番号。番号を指定しなかった場合、全てのポートにルールが適用されます。1つの通信ポートまたは通信ポートの範囲を追加します。

IP – リモートアドレス、アドレス範囲、またはサブネットを追加します。ルールが適用されるアドレス、範囲、サブネットまたはリモートゾーン。値を指定しなかった場合、通信全体にルールが適用されます。

ゾーン – 追加されたゾーンのリスト。

追加 – ドロップダウンメニューから選択してゾーンを追加します。ゾーンを作成するには、[ゾーンの設定]タブを使用します。

削除 – リストからゾーンを削除します。



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たIPアドレスを表示するには、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ます。ESET Endpoint Securityから、**設定 > ネットワーク保護 > 一時IPアドレスブラックリスト**に移動します。一時的にブロックされたIPアドレスは1時間ブロックされます。

列

IPアドレス – ブロックされているIPアドレスを示します。

ブロックの理由 – このアドレスで防御された攻撃の種類(TCPポートスキャニング攻撃など)を選択してください。

タイムアウト – アドレスがブラックリストから有効期限切れになる日時を示します。

コントロール要素

削除 – クリックすると、有効期限切れになる前にアドレスがブラックリストから削除されます。

すべて削除 – クリックすると、すべてのアドレスがただちにブラックリストから削除されます。

例外を追加 – クリックするとIDSフィルタリングにファイアウォール例外が追加されます。

信頼ゾーン

信頼ゾーンは、ファイアウォールが既定の設定を使用して受信トラフィックを許可するネットワークアドレスのグループです。信頼ゾーン内のファイル共有やリモートデスクトップなどの機能の設定は、許可されたサービスと詳細オプションで決定されます。

実際の信頼ゾーンは、コンピュータが現在接続しているネットワークに基づいて、各ネットワークアダプタに対して動的に個別に計算されます。ゾーンエディタで信頼ゾーン内に定義されたアドレスは常に信頼されます。ネットワークアダプタが既知のネットワークに接続している場合、そのネットワークに設定された**[追加の信頼できるアドレス]**が、アダプタの信頼ゾーンに追加されます。ネットワークの保護タイプがホーム/オフィスの場合、すべての直接接続されたサブネットは信頼ゾーンに含まれます。各ネットワークアダプタの実際の信頼ゾーンは、**[ネットワーク] > [ネットワークアダプタ]**の下の**[設定]**ウィンドウに表示されます。

ゾーンの設定

1つのゾーンは、1つの論理グループを構成するネットワークアドレスのコレクションを表します。アドレスのグループであり、複数のルールで同じグループのアドレスを再利用する必要があるときに有効です。特定のグループ内の各アドレスには、グループ全体について集中的に定義された同様なルールが割り当てられています。このようなグループの一例として、**信頼ゾーン**があります。信頼ゾーンは、ファイアウォールによってブロックされることがないネットワークアドレスのグループです。ゾーンは**詳細設定 > ネットワーク保護 > ファイアウォール>詳細**で、**ゾーン**の横の**編集**をクリックして設定できます。新しいゾーンを追加するには、**追加**をクリックし、ゾーンの**名前**と**説明**を入力し、**リモートコンピューターアドレス(IPv4/IPv6、範囲、マスク)**フィールドにリモートIPアドレスを追加します。ファイアウォールゾーンも参照してください。

ファイアウォールゾーン

ゾーンについての詳細は、ゾーンの設定のセクションを参照してください。

列

名前 – リモートコンピューターのグループの名前。

IP アドレス – ゾーンに属するリモート IP アドレス。

コントロール要素

ゾーンを**[追加]** または **[編集]**する場合、次のフィールドを使用できます:

名前 – リモートコンピューターのグループの名前。

説明 – グループの一般的な説明。

リモートコンピュータアドレス(IPv4、IPv6、範囲、マスク) – リモートアドレス、アドレス範囲、またはサブネットを追加します。

削除 – リストからゾーンを削除します。

事前に定義されたゾーンは削除できません。

ファイアウォールログ

ESET Endpoint Securityファイアウォール では、すべての重要なイベントがログファイルに保存されます。このログファイルはメインメニューから直接表示することができます。**ツール > ログファイル**をクリックし、**ログ**ドロップダウンメニューから**ネットワーク保護**を選択します。ファイアウォールを有効にするには、**詳細設定 > ツール > ログファイル**に移動し、最低ログ詳細レベルを**診断**に設定します。すべての拒否された接続が記録されます。

ログファイルは、エラーを検知し、システムへの侵入を明らかにするために使用できますESET ファイアウォールのログには以下のデータが含まれます。

- **時刻** – イベントの日時。
- **イベント** – イベントの名前。
- **ソース** – ソースネットワークアドレス。
- **ターゲット** – ターゲットネットワークアドレス。
- **プロトコル** – ネットワーク通信プロトコル。
- **ルール/ワーム名** – 適用されたルールまたはワームの名前(識別された場合)。
- **アプリケーション** – 影響するアプリケーション。
- **ユーザー** – 侵入が検出されたときにログインしていたユーザーの名前。

このデータを詳しく分析することで、システムのセキュリティを侵害しようとする行為を検出することができます。次のような他の多くの要素は潜在的なセキュリティリスクがあることを示唆しており、その影響を最小限にとどめることができます。例えば、潜在的な脅威の兆候には、不明な場所からの頻繁な接続、接続を確立しようとする多数の試行、不明なアプリケーションの通信、通常と異なるポート番号の使用があります。

> 実際の悪用が発生する前に、悪用の試みが検出され、ネットワークレベルでブロックされているため、特定の脆弱性が既に修正されている場合でも、セキュリティ脆弱性の悪用のメッセージをログに記録します。

接続の確立 – 検出

ファイアウォールでは、新しく確立された各ネットワーク接続が検出されます。有効なファイアウォールモードによって、新しい接続に対して実行されるアクションが決まります。[**自動モード**]または[**ポリシーベースモード**]を有効にする場合、ファイアウォールはあらかじめ定義されたアクションをユーザーの操作なしで実行します。

対話モードでは、新しいネットワーク接続の検出を報告する情報ウィンドウが表示されます。このウィンドウには、接続に関する詳細情報も表示されます。接続を許可するか拒否するかを選択することができます。ダイアログウィンドウで同じ接続を繰り返し許可する場合は、その接続の新しいルールを作成することをお勧めします。そのためには、[**アクションを記録する(ルールを作成する)**]チェックボックスをチェックし、ファイアウォールの新しいルールとしてそのアクションを保存します。その後、ファイアウォールで同じ接続が認識されると、ユーザー対話を必要としないで既存のルールが適用されます。

[**このプロセスに対するアクションを一時的に記憶する**]では、アプリケーションの再起動、ルールまたはフィルタリングモードの変更、ファイアウォールモジュールの更新、またはシステムの再起動まで、アクション(**許可/拒否**)が使用されます。これらのアクションのいずれかが実行された後は、一時的なルールは削除されます。



新しいルールを作成する際は、慎重に、安全であることがわかっている接続だけを許可してください。すべての接続が許可されると、ファイアウォールはその目的を達成することができません。接続に関する重要なパラメーターは次のとおりです。

- **アプリケーション** – 不明なアプリケーションやプロセスの接続を許可することはお勧めしません。
- **リモートコンピュータ** – 信頼された既知のアドレスへの接続のみを許可します。
- **ローカルポート** – 通常の状況では、共通ポート(ポート番号80のWebトラフィックなど)を許可する必要があります。

コンピューターへのマルウェアは多くの場合、インターネットや表示されない接続を使用してリモートシステムに感染して増殖します。ルールが正しく設定されていれば、ファイアウォールは、悪意のあるコードによるさまざまな攻撃から保護するための有効なツールとなります。

ESETファイアウォールの問題の解決

ESET Endpoint Securityがインストールされた状態で接続の問題がある場合は、複数の方法で、ESETファイアウォールが原因になっているかどうかを判断できます。さらにESETファイアウォールを使用すると、接続の問題を解決するための新しいルールまたは例外を作成できます。

ESETファイアウォールの問題を解決するには、次のトピックを参照してください。

- トラブルシューティングウィザード

- ロギングとログからのルールまたは例外の作成
- ファイアウォール通知からの例外の作成
- ネットワーク保護詳細ログ
- プロトコルフィルタリングの問題の解決

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では、すべてのブロックされた接続をバックグラウンドで監視し、特定のアプリケーションまたはデバイスのファイアウォールの問題を修正するトラブルシューティング処理を案内します。次に、承認した場合、ウィザードは適用される新しいルールのグループを提案します。**トラブルシューティングウィザード**は、**[設定]** > **[ネットワーク]**の下のメインメニューにあります。

次のESETナレッジベース記事は、英語でのみ提供されている場合があります。
- トラブルシューティングウィザードを使用してファイアウォール例外を追加する

ロギングとログからのルールまたは例外の作成

既定では🅴ESETファイアウォールは、ブロックされたすべての接続を記録するわけではありません。ファイアウォールでブロックされた項目を確認するには、**ツール** > **診断**の下の**詳細設定**の**診断**セクションで、ネットワーク保護詳細ログを有効にします。 ファイアウォールでブロックしたくない項目がログにある場合は、項目を右クリックして、**今後、同様のイベントをブロックしない**を選択すると、ルールまたはIDSルールを作成できます。ブロックされたすべての接続のログには、多数の項目が含まれることがあり、このログで特定の接続が見つかりにくい可能性があります。 問題が解決したら、ロギングをオフにできます。

ログの詳細については、「ログファイル」を参照してください。

ロギングを使用して、ファイアウォールが特定の接続をブロックする順序を確認できます。さらに、ログからルールを作成すると、目的のルールを正確に作成できます。

ログからルールを作成

新しいバージョンのESET Endpoint Securityでは、ログからルールを作成できます。メインメニューで、**[ツール]** > **[ログファイル]**をクリックします。ドロップダウンメニューから[**ネットワーク保護**]を選択し、目的のログエントリを右クリックして、コンテキストメニューから[**今後、同様のイベントをブロックしない**]を選択します。通知ウィンドウに新しいルールが表示されます。

ログから新しいルールを作成するには、次の設定でESET Endpoint Securityを構成する必要があります。

- **[詳細設定]** (F5) > **[ツール]** > **[ログファイル]**で、ログの最低詳細レベルを**診断**に設定します。
- **セキュリティホールに対する受信攻撃の通知も表示**を、**詳細設定**(F5) > **ネットワーク保護** > **ネットワーク攻撃保護** > **詳細オプション** > **侵入検出**で有効にします。

ファイアウォール通知からの例外の作成

ESETファイアウォールが悪意のあるネットワークアクティビティを検出すると、イベントを説明する通知ウィンドウが表示されます。この通知にはリンクがあり、イベントの詳細を確認し、必要に応じてこのイベントの例外を設定できます。

ネットワークアプリケーションまたはデバイスがネットワーク規格を正しく実装していない場合、ファイアウォールIDS通知が繰り返しトリガーされる可能性があります。通知から直接例外を作成し、ESETファイアウォールがこのアプリケーションまたはデバイスを検出しないようにできます。

ネットワーク保護詳細ログ

この機能は、ESETテクニカルサポートにより複雑なログファイルを提供するためのものです。ESETテクニカルサポートから要請があった場合にのみこの機能を使用してください。大量のログファイルが生成され、コンピューターの速度が低下するおそれがあります。

1. **詳細設定** > **ツール** > **診断**に移動し、**ネットワーク保護詳細ログを有効にする**を有効にします。
2. 発生している問題を再現してみます。
3. ネットワーク保護詳細ログを無効にします。
4. ネットワーク保護詳細ログで作成されるPCAPログファイルは、診断メモリダンプが生成されるディレクトリ(*C:\ProgramData\ESET\ESET Endpoint Security\Diagnostics*)にあります。

プロトコルフィルタリングの問題の解決

ブラウザまたは電子メールクライアントで問題が発生した場合は、まず、プロトコルフィルタリングに問題がないかを確認します。このためには、詳細設定で一時的にアプリケーションプロトコルフィルタリングを無効にします(完了したら必ずオンに戻してください。ブラウザとメールクライアントが保護されなくなります)。オフにして問題が解決したら、次の一般的な問題の一覧を確認して、問題を解決してください。

アップデートまたは安全な接続の問題

アプリケーションで更新できない場合や、通信チャネルが安全ではないというエラーが表示される場合:

- SSLプロトコルフィルタリングが有効な場合、一時的にオフにしてください。問題が解決する場合は、問題がある通信を除外するとSSLフィルタリングをし続け、アップデートを動作させることができます。
SSLプロトコルフィルタリングモードを非アクティブに切り替えます。アップデートに戻ります。暗号化されたネットワークトラフィックについて通知するダイアログが表示されます。このアプリケーションが問題を解決したアプリケーションと一致し、証明書がアップデート元のサーバーから発行されていることを確認します。次に、この証明書のアクションを保存することを選択し、[無視]をクリックします。これ以上ダイアログが表示されない場合は、フィルタリングモードを自動に戻すことができます。問題は解決されます。

- 問題のアプリケーションがブラウザまたは電子メールクライアントではない場合、プロトコルフィルタリングから完全に除外できます(ブラウザまたは電子メールクライアントでこの操作を実行すると、危険にさらされます)。過去に通信をフィルタリングしたアプリケーションは、例外を追加した

ときに既にリストに登録されています。このため、手動で追加する必要はありません。

ネットワーク上のデバイスにアクセスする問題

ネットワーク上のデバイスの機能を使用できない場合(WebカメラのWebページを開けない、ホームメディアプレイヤーで動画を再生できない場合など)はIPv4およびIPv6アドレスを除外されたアドレスのリストに追加します。

特定のWebサイトの問題

URLアドレス管理を使用すると、プロトコルフィルタリングから特定のWebサイトを除外できます。例えば、https://www.gmail.com/intl/en/mail/help/about.htmlにアクセスできない場合は、除外されたアドレスのリストに*gmail.com*を追加します。

エラー「ルート証明書をインポートできない一部のアプリケーションがまだ実行中です」

SSLプロトコルフィルタリングを有効にするとESET Endpoint Securityは、インストールされたアプリケーションの証明書ストアに証明書をインポートしてSSLプロトコルをフィルタリングする方法をアプリケーションが信頼することを確認します。一部のアプリケーションでは、実行中にこの処理ができません。これにはFirefoxOperaがあります。これらのいずれも実行中ではないことを確認(最も簡単な方法では、タスクマネージャを開き、[プロセス]タブにfirefox.exeopera.exeが表示されていないことを確認)し、再試行をクリックします。

信頼できない発行元または無効なシグネチャに関するエラー

一般的に、前述のインポートが失敗したことを意味します。まず、前述のアプリケーションのいずれも実行されていないことを確認します。次に、SSLプロトコルフィルタリングを無効にし、もう一度オンにします。これでインポートが再実行されます。

Webとメール

Webとメールの設定は、**[設定] > [Webとメール]**にあります。このウィンドウから、プログラムのさらに詳細な設定にアクセスすることができます。



セキュアブラウザー – オンラインでの閲覧中に機密データを保護します。

Webコントロールモジュールでは、管理者が自動ツールを使うための設定を構成して、ワークステーションを保護し、インターネット閲覧の制限を設定できるようにしますWebコントロール機能の目的は、不適切または有害なコンテンツを含むページへのアクセスを防止することです。詳細については、「Webコントロール」を参照してください。

インターネット接続は、パーソナルコンピューターの標準機能です。 しかし残念ながら、インターネットは悪意のある迷惑なコードを転送する主要な方法にもなっています。 そのため、**Webアクセス保護**設定を入念に検討することが不可欠です。

[電子メールクライアント保護]ではPOP3(S)とIMAP(S)プロトコルで受信したメール通信が検査されますESET Endpoint Securityでは、メールクライアントのプラグインプログラムを使用して、メールクライアントからのすべての通信を検査できるようにしています。

[迷惑メール対策機能]は、迷惑メールメッセージをフィルタリングします。

歯車 (迷惑メール対策保護の横)をクリックすると、次のオプションを使用できます。

設定 – 電子メールクライアント迷惑メール対策保護の詳細設定を開きます。

ユーザーのホワイトリスト/ブラックリスト/例外リスト – 安全または危険であると見なされた電子メールアドレスを追加、編集、または削除するダイアログウィンドウを開きます。ここで定義されたルールに従い、これらのアドレスから送信されたメールは検査されず、迷惑メールとして処理されません。ユーザーの例外リストをクリックすると、成りすましが行われている可能性のある電子メールアドレスを追加、編集、または削除するダイアログを開きます。例外リストに登録されているアドレスから送信されたメールに対しては、迷惑メールの検査を常に行います。

フィッシング対策保護は、もう1つの保護レイヤーであり、パスワードやその他の機密情報を取得しよ

うと試みる非合法なWebサイトに対する防御を強化します。フィッシング対策保護は、Webとメールの下の[設定]ペインにあります。詳細については、「フィッシング対策保護」を参照してください。

Web/電子メール/フィッシング対策/迷惑メール対策 保護モジュールは、をクリックして一時的に無効にすることも可能です。

プロトコル フィルタリング

ThreatSenseの検出エンジンには、アプリケーションプロトコルに対するウイルス対策があり、そこではすべての高度なマルウェア検査技術がシームレスに統合されています。 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ー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。暗号化された(SSL)設定を編集するには、**詳細設定**(F5) > **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ために使用できます。ほとんどのESET Endpoint 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Webコントロール)はこれを利用しており、この機能がないと動作しません。

対象外のアプリケーション – 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できます。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。

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。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。

IPv4アドレスとマスク:
- *192.168.0.10* – ルールが適用される各コンピューターのIPアドレスを追加します。
- *192.168.0.1*–*192.168.0.99* – 最初と最後のIPアドレスを入力して、ルールが適用される複数のコンピューターのIP範囲を指定します。
- IPアドレスとマスクで定義されたサブネット(コンピューターのグループ)。たとえば、*255.255.255.0*は、*192.168.1.0/24*プレフィックスのネットワークマスクです。これは、アドレス範囲が*192.168.1.1*–192.168.1.254であることを意味します。

IPv6アドレスとマスク:
- *2001:718:1c01:16:214:22ff:fec9:ca5* – ルールが適用される各コンピューターのIPv6アドレスを追加します。
- *2002:c0a8:6301:1::1/64* – IPv6アドレスと、64ビットのプレフィックス長。*2002:c0a8:6301:0001:0000:0000:0000:0000*–*2002:c0a8:6301:0001:ffff:ffff:ffff:ffff*

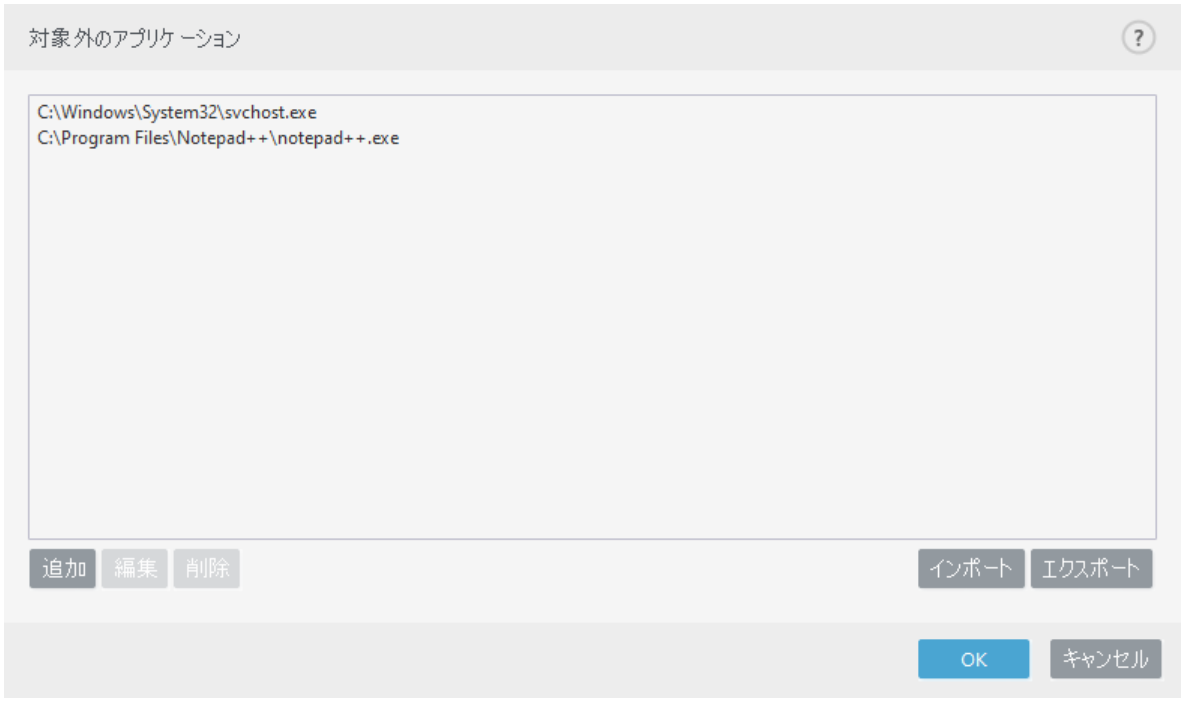
対象外のアプリケーション

特定のネットワーク対応アプリケーションの通信をプロトコルフィルタリングから除外するには、リストでそのアプリケーションを追加します。選択したアプリケーションのHTTP/POP3/IMAP通信のマルウェアは検査されません。プロトコルフィルタリングを有効にしてアプリケーションが正しく機能しない場合にのみ、この方法を使用することをお勧めします。

プロトコルフィルタリングの影響を受けているアプリケーションとサービスは、**[追加]**をクリックすると自動的に表示されます。

編集 – リストから選択したエントリを編集します。

削除 – 選択したエントリーをリストから削除します。



対象外のIPアドレス

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。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。

追加 – クリックすると、ルールが適用されるリモートポイントのIPアドレス/アドレス範囲/サブネットを追加することができます。

編集 – リストから選択したエントリを編集します。

削除 – 選択したエントリーをリストから削除します。



SSL/TLS

ESET Endpoint SecurityはSSL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は既定で有効です。**詳細設定** > **Webとメール** > **SSL/TLS**またはポリシーを使用してSSL/TLSプロトコルフィルタリングを無効にできます。プロトコルフィルタリングが無効な場合、SSL経由の通信は検査されません。

SSL/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。

フィルタリングモード	説明
ルール付き自動モード	既定モードではWebブラウザまたは電子メールクライアントとなど適切なアプリケーションのみをスキャンします。 通信をスキャンするためのアプリケーションを選択することにより、それを優先させることができます。
対話モード	新しいSSL-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証明書/アプリケーションのリストを作成できます。
ポリシーベースモード	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。

SSL/TLS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してESET Endpoint Securityの特定のアプリケーションに対する動作をカスタマイズできます。

既知の証明書のリストでは、特定のSSL証明書に対するESET Endpoint Security動作をカスタマイズできます。

信頼できるドメインとの通信を除外 – 有効にすると、信頼できるドメインとの通信は確認されません。ドメインの信頼性はビルトインのホワイトリストによって決定されます。

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。

信頼できるドメインとの通信を除外する設定が有効で、ドメインが信頼できると見なされる場合には、アドレスがフィルタリングされません。

ルート証明書

ルート証明書 – ブラウザや電子メールクライアントでSSL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ー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、証明書をブラウザーに手動でインポートします。

証明書の有効性

TRCA証明書信頼ストアを確立できない場合 – 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(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ブラウザに委ねます。**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か、破損し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**を選択することをお勧めします。**証明書の有効期間を確認**を選択した場合は、暗号化された通信が確立されたときに実行するアクションを選択するように指示されます。

次のESETナレッジベース記事は、英語でのみ提供されている場合があります。
- ESET製品の証明書通知
- Webページにアクセスすると、「暗号化されたネットワークトラフィック: 信頼できない証明書」が表示されます

証明書

ブラウザーや電子メールクライアントでSSL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(OperaFirefox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ーに、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ー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、証明書をブラウザーに手動でインポートします。

場合によっては、信頼できるルート認証局ストア(VeriSignなど)を使用して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(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。 アクションを選択するダイアログが表示され、ユーザーはその証明書を信頼するか除外するかを決定してマークを付けます。 証明書がTRCAリストに含まれていない場合、ウィンドウは赤になります。 証明書がTRCAリストに含まれている場合、ウィンドウは緑になります。

[**証明書を使用する通信をブロックする**]を選択して、未検証の証明書を使用するサイトとの暗号化通信をいつでも切断できます。

証明書が無効な場合、または破損している場合は、証明書の有効期限が切れているか、不正に自己署名されています。 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。

暗号化されたネットワークトラフィック

SSLプロトコル検査を使用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 Endpoint 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。証明書がTrusted Root Certification Authorities store (TRCA)にない場合、信頼できないと見なされます。

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 Endpoint 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。

次のESETナレッジベース記事は、英語でのみ提供されている場合があります。
- ESET製品の証明書通知
- Webページにアクセスすると、「暗号化されたネットワークトラフィック：信頼できない証明書」が表示されます

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。

既知の証明書のリスト

既知の証明書のリストを使用すると、特定のSSL証明書に対するESET Endpoint Securityの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。[**詳細設定**] (F5) > **[Webとメール]** > **[SSL/TLS]** > [**既知の証明書のリスト**]で、このリストを表示および編集できます。

[**既知の証明書のリスト**]ウィンドウには次の項目があります。

列

名前 – 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 - **許可**または**拒否**を**アクセスアクション**として指定し、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。**自動**を選択すると、信頼できる証明書を許可し、信頼できない証明書については確認します。**確認する**を選択すると、常に処理方法をユーザーに確認します。

検査 - **検査**または**無視**を**検査アクション**として選択すると、この証明書で保護された通信を検査または無視します。**自動**を選択すると、自動モードでは検査し、対話モードでは確認します。**確認する**を選択すると、常に処理方法をユーザーに確認します。

コントロール要素

追加 - *.cer*.*crt*.*pem*拡張子のファイルとして、証明書を手動で読み込めます。[**ファイル**]をクリックしてローカル証明書を読み込むか、**[URL]**をクリックして証明書のオンラインの場所を指定します。

編集 – 設定する証明書を選択し、[**編集**]をクリックします。

削除 – 削除する証明書を選択し、[**削除**]をクリックします。

OK/キャンセル – 変更を保存する場合は**[OK]**をクリックします。変更せずに終了する場合は[**キャン**

セル]をクリックします。

SSL/TLSフィルタリングされたアプリケーションのリスト

SSL/TLS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 Endpoint 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。[**詳細設定**] (F5) > [**Webとメール**] > [**SSL/TLS**] >[**SSL/TLSフィルタリングされたアプリケーションのリスト**]で、このリストを表示および編集できます。

SSL/TLSフィルタリングされたアプリケーションのリストウィンドウは以下で構成されています:

列

アプリケーション – アプリケーションの名前。

スキャン操作 - **スキャン** または **無視**を選択して通信をスキャンまたは無視します。 **自動**を選択すると、自動モードでは検査し、対話モードでは確認します。**確認する**を選択すると、常に処理方法をユーザーに確認します。

コントロール要素

追加 – フィルタリングされたアプリケーションを追加。

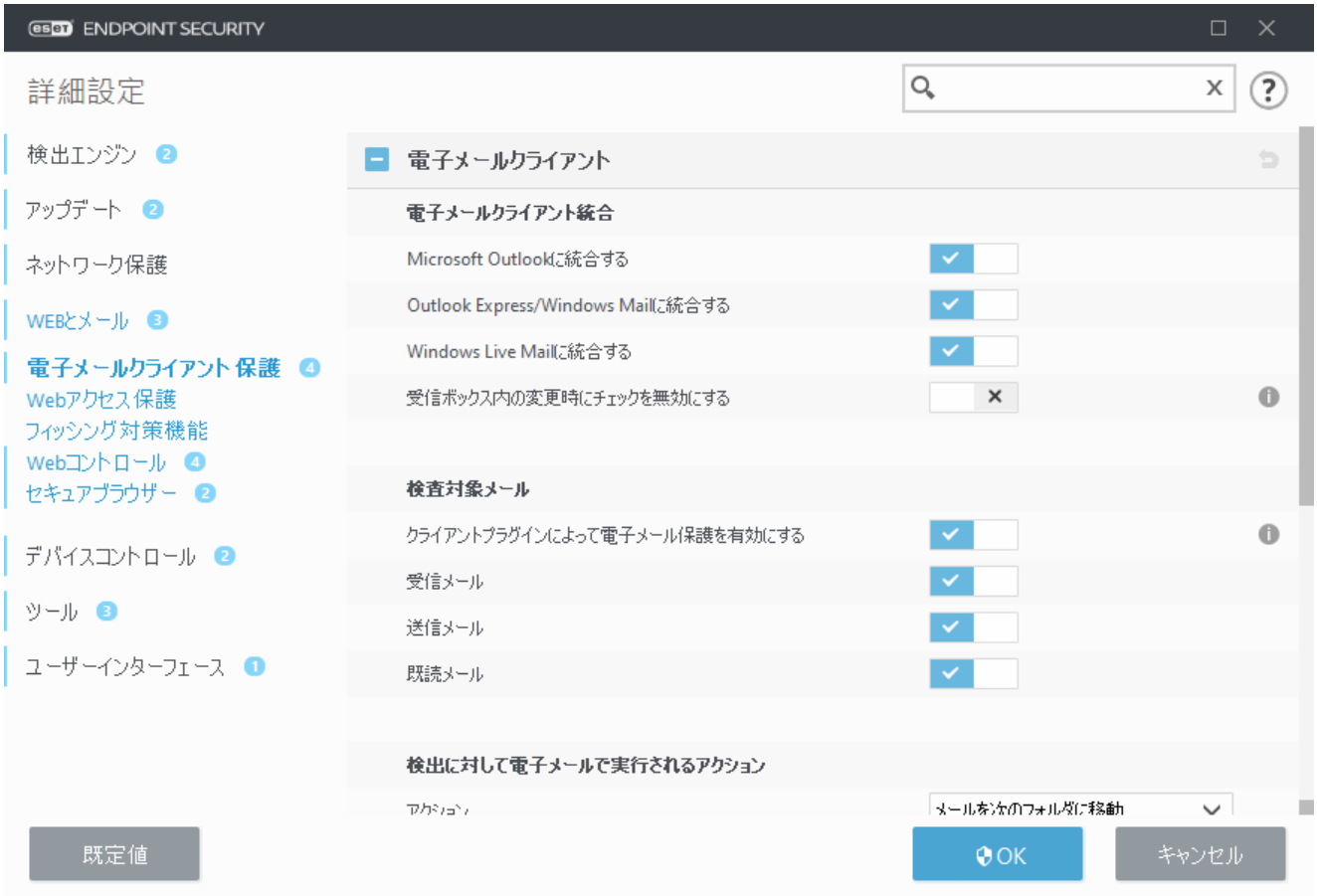
編集 – 設定する証明書を選択し、[**編集**]をクリックします。

削除 – 削除する証明書を選択し、[**削除**]をクリックします。

OK/キャンセル - **変更を保存する場合は**[OK]**をクリックします。保存せずに終了する場合は**[キャンセル]をクリックします。

電子メールクライアント保護

ESET Endpoint 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 Endpoint Securityで有効にできます。統合が有効な場合、ESET Endpoint 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、電子メール保護を効率化できます。統合設定は、[**設定**] > [**詳細設定**] > [**Webとメール**] > [**電子メールクライアント保護**] > [**電子メールクライアント**]の下にあります。



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。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、ESETナレッジベースを参照してください。

電子メールを取得するときに、システムの速度が低下する場合は、**受信ボックスの内容の変更時に確認を無効にする**オンにします。

検査対象メール

クライアントプラグインによる電子メール保護を有効にする – 無効にすると電子メールクライアントプラグインによる保護がオフなります。

受信電子メール – 有効にすると、受信した電子メールメッセージを確認します。

送信電子メール – 有効にすると、送信した電子メールメッセージを確認します。

既読電子メール – 有効にすると、既読の電子メールメッセージを確認します。

クライアントプラグインによる電子メール保護を有効にするを有効にすることをお勧めします。統合が無効である場合や機能していない場合でも、電子メール通信がプロトコルフィルタリング(IMAP/IMAPSおよびPOP3/POP3S)で保護されます。

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。

メールを次のフォルダに移動(既定のアクション) – 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検査 – 有効にすると、検出エンジンアップデートの後に、感染した電子メールを再検査します。

ほかの機能の検査結果を受け入れる – 電子メール検出モジュールは、再検査を実行せずに、他の保護モジュールから受信した検査結果を使用することができます。

電子メールプロトコル

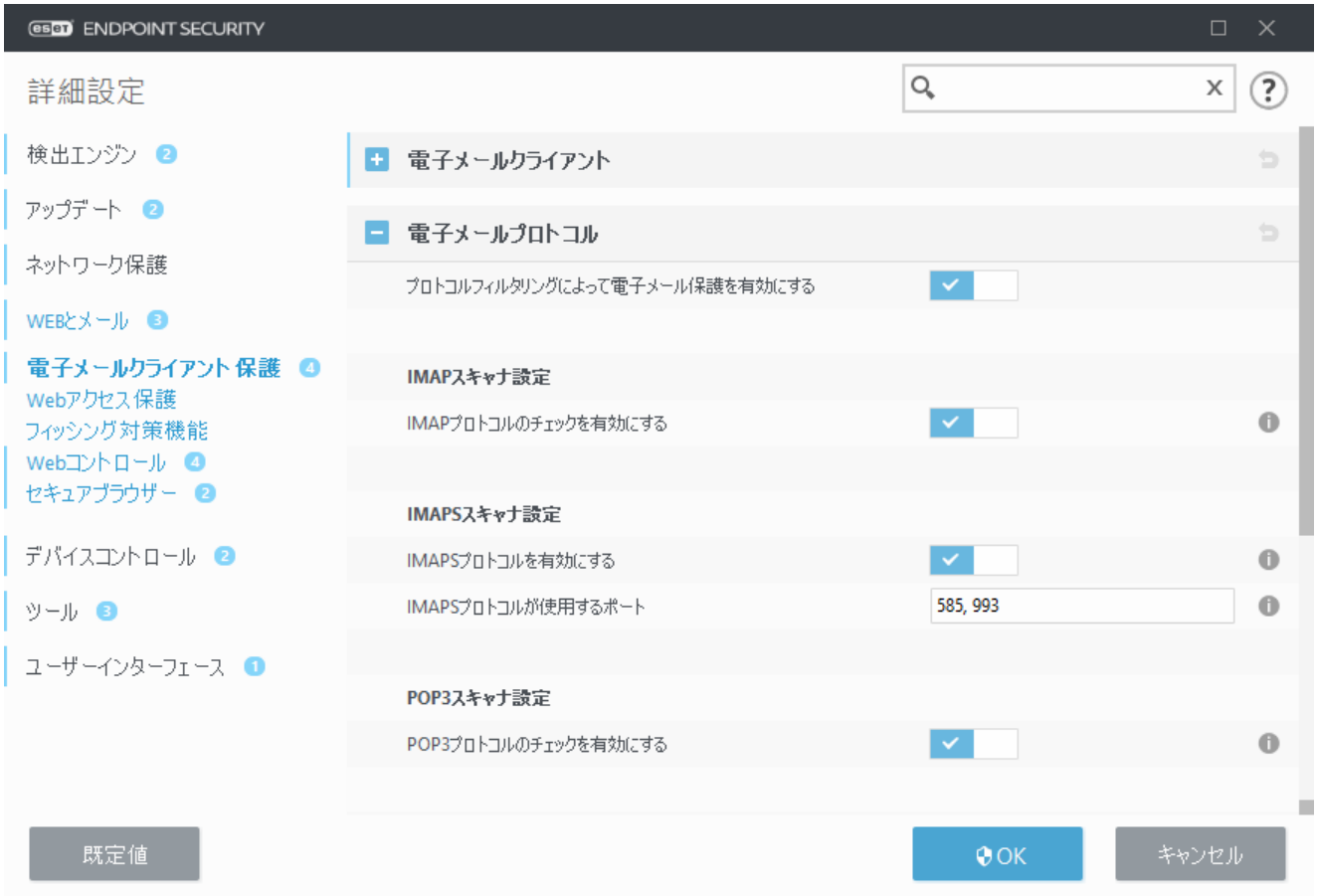
IMAPとPOP3プロトコルは、メールクライアントアプリケーションでの電子メール通信の受信に最もよく使用されているプロトコルです。IMAP(インターネットメッセージアクセスプロトコル)はメール受信のためのもう1つのプロトコルです。IMAPはPOP3よりも優れている点があります。たとえばIMAPでは、複数のクライアントが同時に同じメールボックスに接続して、メッセージが既読か、返信済みか、削除されたかなどの状態の情報を保持できます。このコントロールを提供する保護モジュールは、システムの起動時に自動的に初期化され、メモリ内でアクティブになります。

ESET Endpoint 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。電子メールクライアントの再設定は不要です。既定では、既定のPOP3/IMAPポート番号に関係なくPOP3およびIMAPプロトコルのすべての通信が検査されます。
MAPIプロトコルは検査されません。ただしMicrosoft Exchangeサーバーとの通信は、Microsoft Outlookなどの電子メールクライアントの統合モジュールによって検査できます。

プロトコルフィルタリングによる電子メール保護を有効にするを有効にすることをお勧めしますIMAP/IMAPSおよびPOP3/POP3Sプロトコル確認を設定するには、**詳細設定 > Webとメール > 電子メールクライアント保護 > 電子メールプロトコル**に移動します。

ESET Endpoint SecurityではIMAPS (585993)およびPOP3S (995)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 Endpoint 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。必要に応じて、他の通信ポートを追加できます。複数のポート番号はカンマで区切る必要があります。

暗号化された通信は、既定で検査されます。 スキャナー設定を表示するには、詳細設定セクションの[SSL/TLS]に移動し、[**Webとメール**] > [**SSL/TLS**]に移動し、[**SSL/TLSプロトコルフィルタリングを有効にする**]オプションを有効にします。



電子メールアラートと通知

この機能のオプションは、[**詳細設定] > [Webとメール] > [電子メールクライアント保護] > [警告と通知**]にあります。

電子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**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。
- **検出が発生したとき** – 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)。
- **検査時にすべての電子メール** – 検査された全てのメールに検査通知が追加されます。

送信した電子メールの件名を更新 – 電子メールの保護で、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、感染している電子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(電子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、特定の電子メールまたは送信者の脅威レベルについての貴重な情報を得ることができます。

検出された電子メールの件名に追加するテキスト – 感染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、"[detection %DETECTIONNAME%] Hello"で置き換えられます。変数の%DETECTIONNAME%は検出を表し

ます。

メールクライアントとの統合

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。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、ESETナレッジベースを参照してください。

Microsoft 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 Endpoint Securityのインストール後、ウイルス保護/迷惑メール対策 機能オプションがMicrosoft Outlookに追加されます。

迷惑メール – 選択したメールを迷惑メールとしてマークします。マークすると、迷惑メールのシグネチャを格納するセントラルサーバにメールの"フィンガープリント"が送信されます。複数のユーザーからさらに別の似通った"フィンガープリント"がサーバに送信されると、そのメールは迷惑メールとして分類されます。

信頼メール – 選択したメールを信頼メールとしてマークします。

迷惑メールアドレス(迷惑メールアドレスのリストであるブラックリスト) – 新しい送信元アドレスをブラックリストに追加します。ブラックリスト内のアドレスから受信したメッセージはすべて、自動的に迷惑メールとして分類されます。

> ⚠ スプーフィングに注意してください。スプーフィングとは、メールの送信元アドレスを偽造し、メールの受信者を騙してメールを読ませ、返信させるものです。

信頼アドレス(信頼アドレスのリストであるホワイトリスト) – 新しい送信元アドレスをホワイトリストに追加します。ホワイトリスト内のアドレスから受信したメッセージはすべて、自動的に迷惑メールとして分類されることはありません。

ESET Endpoint Security – アイコンをクリックするとESET Endpoint 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。

迷惑メール対策のセットアップ - [迷惑メール対策機能]設定オプションを表示します。

アドレス帳 – [迷惑メール対策機能]ウィンドウが開きます。このウィンドウから、除外アドレス、信頼アドレス、および迷惑メールアドレスのリストにアクセスできます。

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、プラグイン機能として動作します。ESET Endpoint Securityのインストール後、ウイルス保護/迷惑メール対策 機能オプションを備えたツールバー

がOutlook ExpressまたはWindows Mailに追加されます。

迷惑メール – 選択したメールを迷惑メールとしてマークします。マークすると、迷惑メールのシグネチャを格納するセントラルサーバにメールの"フィンガープリント"が送信されます。複数のユーザーからさらに別の似通った"フィンガープリント"がサーバに送信されると、そのメールは迷惑メールとして分類されます。

信頼メール – 選択したメールを信頼メールとしてマークします。

迷惑メールアドレス – 新しい送信元アドレスをブラックリストに追加します。ブラックリスト内のアドレスから受信したメッセージはすべて、自動的に迷惑メールとして分類されます。

スプーフィングに注意してください。スプーフィングとは、メールの送信元アドレスを偽造し、メールの受信者を騙してメールを読ませ、返信させるものです。

信頼アドレス – 新しい送信元アドレスをホワイトリストに追加します。ホワイトリスト内のアドレスから受信したメッセージはすべて、自動的に迷惑メールとして分類されることはありません。

ESET Endpoint Security – アイコンをクリックするとESET Endpoint 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。

迷惑メール対策のセットアップ - [迷惑メール対策機能]設定オプションを表示します。

ユーザーインターフェイス

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ーとは独立して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。

一方、ダイアログにはこの確認を行わないオプションも用意されています。

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ESETEndpointSecurity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。

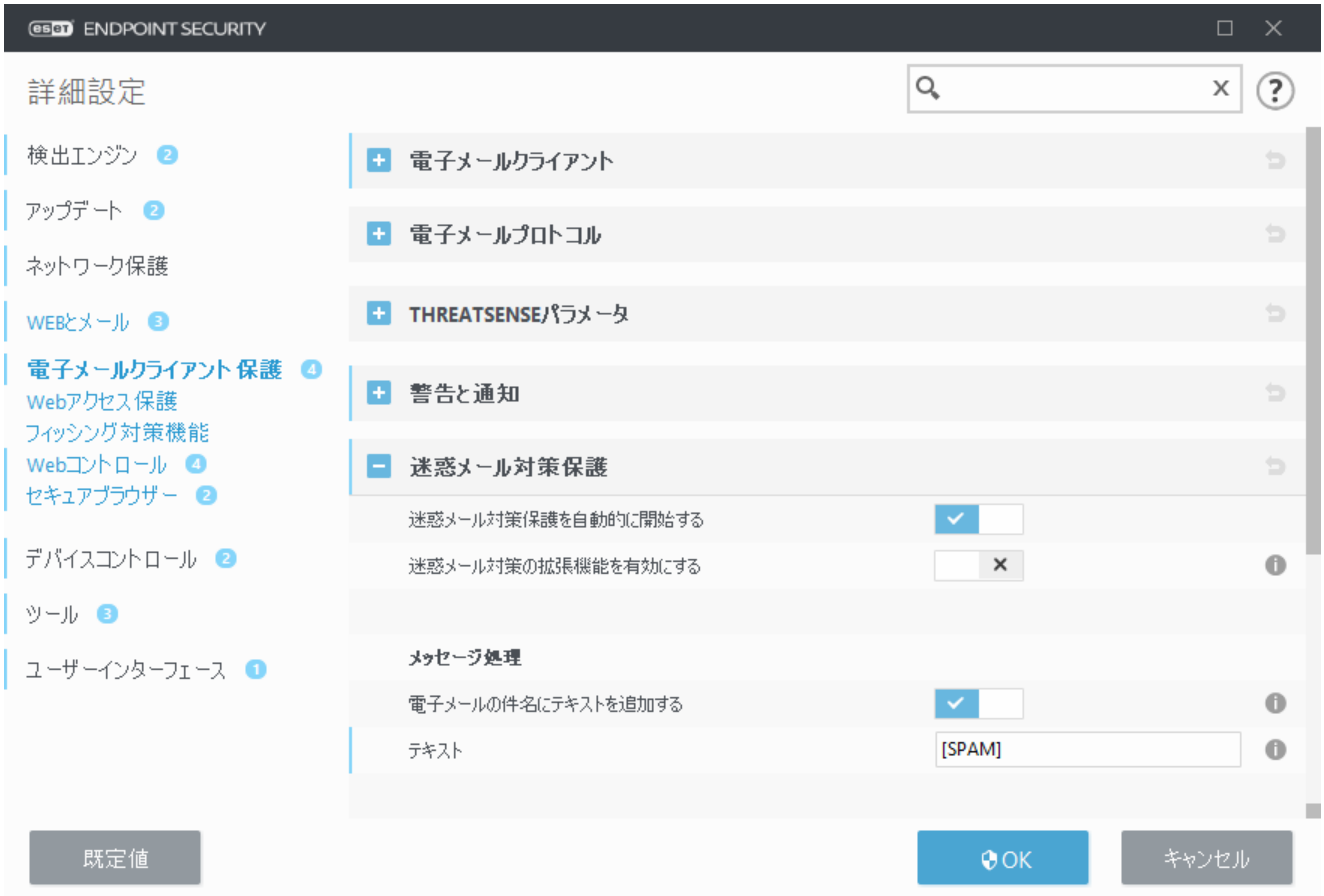
現在のフォルダ内にあるすべてのメッセージ – 現在表示されているフォルダ内にあるメッセージを検査します。

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**]チェックボックスをオンにすると、事前に検査されているメッセージを再度検査できます。

迷惑メール対策保護

受信者側が送信を要求していないメールつまり迷惑メールは、電子通信分野における最大の問題の一つとなっています。迷惑メールは全メール通信の実に50%も占めています。この問題に対処するための機能が、迷惑メールからの保護機能です。メールセキュリティの複数の原則を組み合わせることにより、迷惑メール対策機能のフィルタリング機能は強化されて、受信ボックスは常にクリーンな状態が保持されます。



迷惑メール検出における1つの重要な原理は、あらかじめ定義された信頼済みのアドレスの(ホワイトリスト)と迷惑メールアドレス(ブラックリスト)に基づいて、受信者側が送信を要求していないメールを認識する能力です。連絡先リストから抽出した全てのアドレスが、自動的にホワイトリストに追加されます。さらに、ユーザーが安全とマークしたその他のアドレスも全て、ホワイトリストに追加されます。

迷惑メール検出に使用される主な方法は、メールメッセージのプロパティのスキャンです。受信メッセージは、基本的な迷惑メール対策基準(メッセージ定義、統計ヒューリスティック、認識アルゴリズムやその他の固有の方法)に基づいてスキャンされます。そして、結果として生成されるインデックス値により、あるメッセージが迷惑メールかどうかが判定されます。

迷惑メール対策機能を自動的に開始する – 有効の場合、システムの起動時に迷惑メール対策が自動的

に起動されます。

迷惑メール対策の拡張機能を有効にする – 追加の迷惑メール対策データが定期的にダウンロードされ、迷惑メール対策能力が向上し、より望ましい結果が得られます。

ESET Endpoint Securityの迷惑メールからの保護では、メーリングストで使用するさまざまなパラメーターを設定できます。次のオプションがあります。

メッセージ処理

件名にテキストを追加する: – 迷惑メールとして分類されたメールの表題にカスタムのプリフィクス文字列を追加することができます。既定の文字列は"[SPAM]"です。

メッセージを迷惑メールフォルダに移動する– 有効にすると、迷惑メールメッセージが既定の迷惑メールフォルダに移動され、迷惑メールではないメールとして再分類されたメッセージが受信トレイに移動されます。電子メールメッセージを右クリックし、コンテキストメニューからESET Endpoint Securityを選択すると、該当するオプションを選択できます。

フォルダーを使用 – 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ーを指定します。

迷惑メールを既読としてマークする – 迷惑メールが自動的に既読に設定されます。これによって、"正当"なメールに集中できます。

分類し直したメールを未読としてマークする – 最初に迷惑メールとして分類され、後で"正当"であるとマークされたメールが未読として表示されます。

迷惑メールスコアのログ記録 - ESET Endpoint Securityの迷惑メール対策用エンジンでは、全ての検査済みメッセージに迷惑メールスコアが割り当てられます。このメッセージは、迷惑メール対策ログに記録されます([**ESET Endpoint Security**] > [**ツール**] > [**ログファイル**] > [**迷惑メール対策機能**])

- **書き込まない** – 迷惑メール検査のスコアは記録されません。
- **再分類して迷惑メールに設定**– 迷惑メールとしてマークされたメッセージに迷惑メールスコアを記録する場合、これを選択します。
- **すべて**– ログに迷惑メールスコア付きで全てのメッセージが記録されます。

> 迷惑メールフォルダのメッセージをクリックし、[**選択したメッセージを迷惑メールではないメールに再分類**]を選択すると、メッセージが受信トレイに移動されます。受信トレイにある迷惑メールだと考えられるメッセージをクリックし、[**メッセージを迷惑メールに再分類**]を選択すると、メッセージが迷惑メールフォルダに移動されます。複数のメッセージを選択して、同時にすべてのメッセージ対してアクションを実行できます。

> ESET Endpoint Securityでは、Microsoft Outlook、Outlook Express、Windows Mail、Windows Live Mailの迷惑メールからの保護がサポートされます。

迷惑メール対策アドレス帳

ESET Endpoint Securityの迷惑メール対策機能により、アドレス帳にさまざまなパラメーターを設定できます。

アドレス帳

ユーザーのアドレス帳を利用する – ユーザーがユーザー自身のメールクライアントで作成したアドレス帳を有効にするには、このオプションを有効にします。

グローバルアドレス帳を許可する – このワークステーション全てのユーザー、電子メールシステムのディレクトリサービスで共有されるグローバルアドレス帳を有効にする場合、このオプションを有効にしますGAL(グローバルアドレス帳)には、全てのメールユーザー、配布グループ、リソースの情報が入っています。

ユーザーのホワイトリスト – 連絡先のリスト。安全であると見なされ、メッセージを受信したいアドレスを追加、編集、削除できます。

ユーザーのブラックリスト – 連絡先のリスト。危険であると見なされ、メッセージを受信したくないアドレスを追加、編集、削除できます。

ユーザーの除外リスト – このリストには、偽装されている可能性がある電子メールアドレスと迷惑メールの送信に使用されている可能性がある電子メールアドレスが含まれます。「除外リスト」も参照してください。

グローバルホワイトリスト/ブラックリスト/例外リスト – これらのリストはこのワークステーションでESET Endpoint Securityを使用する全ユーザーに迷惑メール対策ポリシーを適用するために使用しますESET Endpoint Securityがリモートで管理される場合ESET PROTECT/ESMC/ECAポリシーがすべての割り当てられたワークステーションに適用されます。

ユーザーのホワイトリストに自動的に追加する

アドレス帳からアドレスを追加する – 連絡先リストのアドレスをホワイトリストに追加できます。

送信メールの送信先メールアドレスを追加する – 送信メールの受信者アドレスをホワイトリストに追加します。

再分類した信頼メールのアドレスを追加する – 迷惑メールでないとして再分類したメールの送信元アドレスをホワイトリストに追加します。

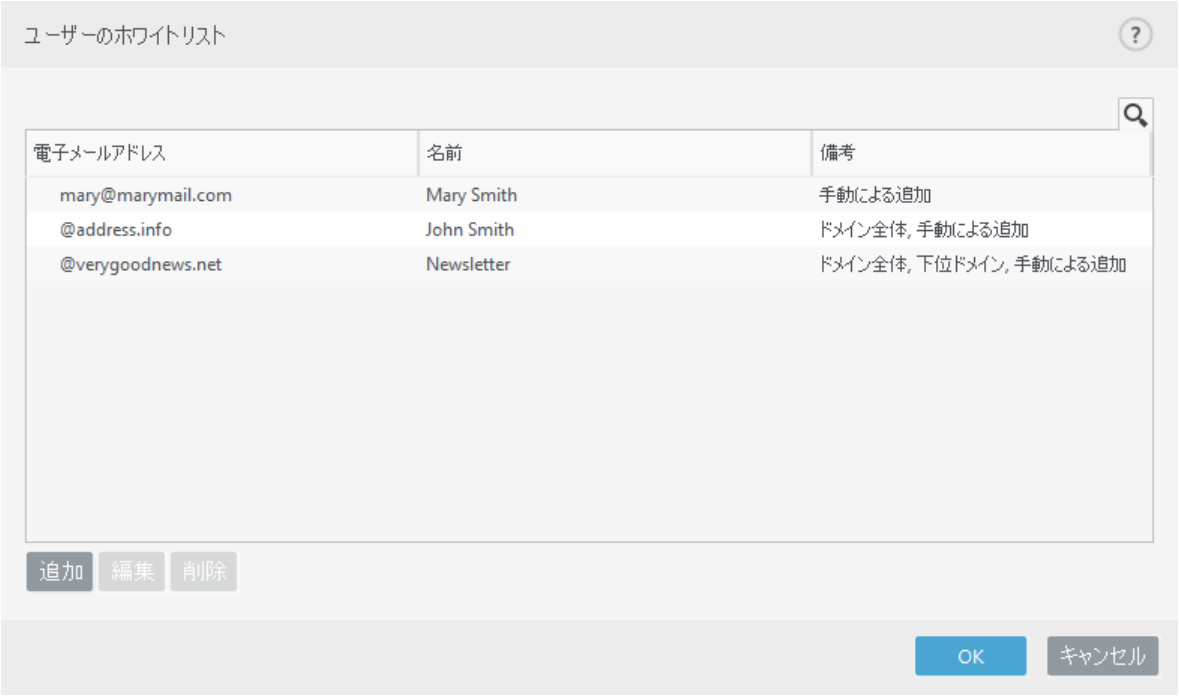
ユーザーの例外リストに自動的に追加する

独自のアカウントからアドレスを追加する – ユーザーの既存のメールクライアントアカウントからアドレスを除外リストに追加します。

ブラックリスト/ホワイトリスト/除外リスト

受信者側が送信を要求していないメールからの保護を実現するためにESET Endpoint Securityでは電子メールアドレスを専用のリストに分類することができます。ホワイトリストには安全と見なされた電子メールアドレスが格納されます。ホワイトリストにあるユーザーからのメールは、常に受信メールフォルダで参照することができます。ブラックリストには、迷惑メールとして分類された電子メールアドレスが格納され、ブラックリストにある送信元からのメッセージはすべて、迷惑メールとしてマークされます。除外リストには、常に迷惑メールかどうかのチェックの対象となる電子メールアドレスが格納されますが、迷惑メールではないように偽装した未承諾メールメッセージのアドレスが格納されることもあります。

すべてのリストは、各リストのダイアログウィンドウにある**追加**/**編集**/**削除**ボタンを使用してESET Endpoint Securityのメインウィンドウの**詳細設定** > **Webとメール** > **電子メールクライアント保護** > **迷惑メール対策アドレス帳**、または歯車(**迷惑メール対策保護**の横)をクリックした後に**設定** > **Webとメール**から編集できます。



既定ではESET Endpoint Securityで、サポートされる電子メールクライアントのアドレス帳のすべてのアドレスがホワイトリストに追加されます。既定では、ブラックリストは空です。既定では、ユーザー自身の電子メールアドレスだけが除外リストに格納されます。

ブラックリスト/ホワイトリスト/例外アドレスの追加/編集

このウィンドウでは、ホワイトリストまたはブラックリストのエントリの追加または編集を行えます。**詳細設定 > Webとメール > 電子メールクライアント保護 > 迷惑メール対策アドレス帳**の順に選択し、ESET Endpoint Securityのメインプログラムウィンドウを開きます。

電子メールアドレス – 追加/編集する電子メールアドレス。

名前 – エントリの名前。

ドメイン全体 – 連絡先のドメイン全体([電子メールアドレス]フィールドに指定したアドレスだけでなく、*address.info*ドメインのすべての電子メールアドレス)にエントリを適用する場合に、このオプションを選択します。

下位ドメイン – 連絡先の下位ドメイン(*address.info*はドメインを表し、*my.address.info*はサブドメインを表す)にエントリを適用する場合に、このオプションを選択します。

Webアクセス保護

インターネット接続は、パーソナルコンピュータの標準機能です。 残念ながら、悪意のあるコードを転送する主要な方法にもなっています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、HTTP (Hypertext Transfer Protocol)およびHTTPS (暗号化通信)のルールに準拠します。

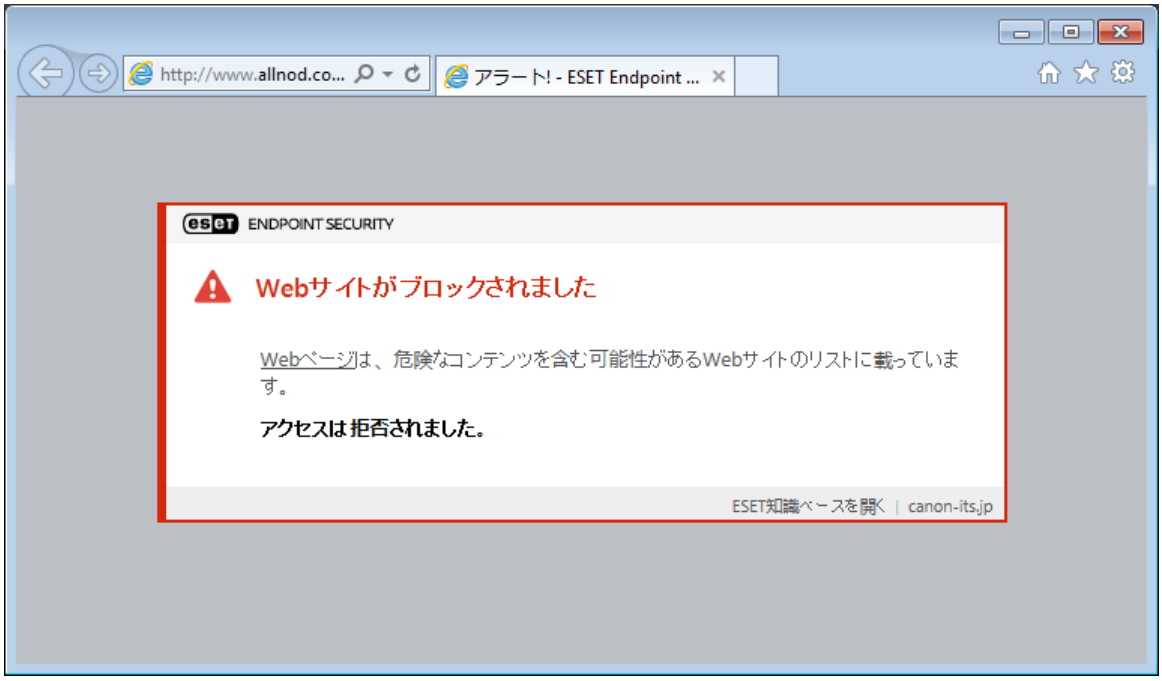
コンテンツをダウンロードする前に、悪意のあるコンテンツが含まれていることがわかっているWebページへのアクセスをブロックします。 その他のすべてのWebページは、読み込み時にThreatSenseスキャ

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。

Webアクセス保護を有効にすることを強くお勧めします。 このオプションは、ESET Endpoint Securityのメインウィンドウから、**[設定] > [インターネットオプション保護] > [Webアクセス保護]**に移動してアクセスできます。



Webアクセス保護は、Webサイトがブロックされたときに、ブラウザーに次のメッセージが表示されます。

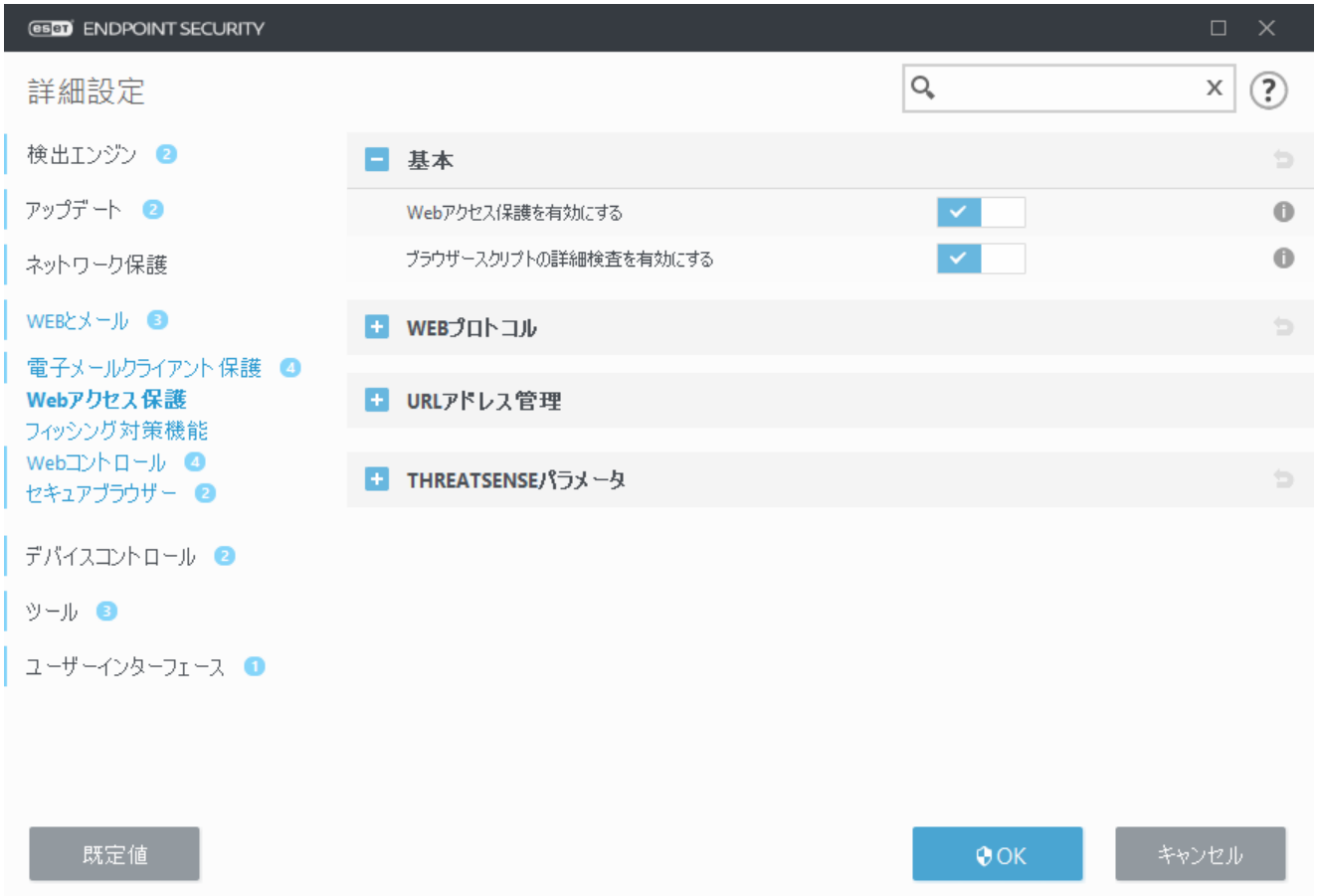


次のESETナレッジベース記事は、英語でのみ提供されている場合があります。

- ESET Endpoint Securityで個別のワークステーションの安全なWebサイトをブロック解除する
- ESET Security Management Centerを使用してエンドポイントで安全なWebサイトをブロック解除する

次のオプションは、[**詳細設定**] (F5) > [**Webとメール**] > [**Webアクセス保護**]から使用できます。

- **基本** – 詳細設定からこの機能を有効または無効にします。
- **Webプロトコル** – ほとんどのインターネットブラウザで使用されるこれらの標準プロトコルの監視を設定できます。
- **URLアドレス管理** – ブロック、許可、またはチェックから除外するURLアドレスを指定できます。
- **ThreatSenseパラメータ** – 詳細ウイルススキャナ設定 – スキャン対象の種類(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。



Webアクセス保護詳細設定

次のオプションは、**詳細設定** (F5) > **Webとメール** > **Webアクセス保護** > **基本**から使用できます。

Webアクセス保護を有効にする – この機能が無効になると、Webアクセス保護とフィッシング対策機能は実行されません。

ブラウザースクリプトの詳細検査を有効にする – 有効にすると、インターネットブラウザーで実行されるすべてのJavaScriptプログラムが検査されます。

Webアクセス保護を有効にすることを強くお勧めします。

Webプロトコル

既定ではESET Endpoint Securityは、大半のインターネットブラウザで使用されるHTTPプロトコルを監視するように設定されています。

HTTPスキャナ設定

HTTPトラフィックは、すべてのアプリケーションのすべてのポートで常に監視されます。

HTTPSスキャナ設定

ESET Endpoint 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 Endpoint 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(443、0–65535)上のトラフィックだけを検査します。

暗号化された通信は、既定で検査されます。 スキャナー設定を表示するには、詳細設定セクションの[SSL/TLS]に移動し、[**Webとメール**] > [**SSL/TLS**]に移動し、[**SSL/TLSプロトコルフィルタリングを有効にする**]オプションを有効にします。

URLアドレス管理

URLアドレス管理セクションでは、ブロック、許可、またはコンテンツ検査から除外するHTTPアドレスを指定できます。

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]**を選択する必要があります。 そうしないとアクセスした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限り、アクセスできません。**コンテンツ検査から除外するアドレスのリスト**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。

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。

特殊記号の*(アスタリスク)および?(疑問符)も各アドレスリストで使用できます。 アスタリスクは0文字以上の任意の文字列を、疑問符は任意の1文字をそれぞれ表します。 除外するアドレスを指定する際は、特に注意する必要があります。このリストには信頼できる安全なアドレスのみを含める必要があるためです。 同様に、記号の*および?を各アドレスリスト内で正しく使用してください。 すべてのサブドメインを含むドメイン全体が安全に照合される方法については、「HTTPアドレス/ドメインのマスクの追加」を参照してください。 アドレスリストを有効にするには、**[アクティブのリスト]**をクリックします。 現在の一覧からアドレスを入力するときに通知が必要な場合は、**[適用時に通知]**を選択します。

URLアドレス管理でも、インターネットの閲覧中に特定の種類のファイルをブロックするか、開くこと許可することができます。 例えば、実行可能なファイルを開くように指定したくない場合、ドロップダウンメニューからこれらのファイルをブロックしたい一覧を選択し "**.exe"の形式でプログラム名を入力します。

Webとメール > **SSL/TLS** > **信頼できるドメインとの通信を除外する**設定が有効で、ドメインが信頼できると見なされる場合には、アドレスがフィルタリングされません。



コントロール要素

追加 – 定義済みのリストの他に、新しい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。 例えば、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。これにより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 – 既存のリストを修正します。 これを使用して、アドレスを追加・削除します。

削除 – 既存のリストを削除します。 **追加**で作成したリストのみを削除できます。既定は削除できません。

URLアドレスリスト

このセクションでは、ブロック、許可、またはチェックから除外するHTTPアドレスのリストを指定できます。

既定では、次の3つのリストを使用できます。

- **コンテンツ検査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でも、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。

新しいリストを作成するには、[**追加**]をクリックします。 選択したリストを削除するには、[**削除**]をクリックします。



次のESETナレッジベース記事は、英語でのみ提供されている場合があります。
- ESET Endpoint Securityで個別のワークステーションの安全なWebサイトをブロック解除する
- ESET Security Management Centerを使用してエンドポイントで安全なWebサイトをブロック解除する

詳細については、「URLアドレス管理」を参照してください。

新しいURLアドレスリストの作成

このセクションでは、ブロック、許可、またはチェックから除外するURLアドレス/マスクのリストを指定できます。

新しいリストを作成するときには、次のオプションを設定できます。

アドレスリストのタイプ – 3種類のリストがあります。

- **チェックから除外** – 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。
- **ブロック** – 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。
- **許可** – この機能を使用するようにポリシーが設定され、ワイルドカード(*)値がこのリストに追加されている場合は、これらのアドレスがブロックされたリストにある場合でも、このリストのアドレスにアクセスできます。

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、このフィールドは使用できません。

リスト説明 – リストの説明を入力します(任意)。このフィールドは、3つの定義済みリストのいずれかを編集している場合は使用できません。

リストのアクティブ化 – スライダーバーを選択すると、リストをアクティブ化します。

適用するときに通知する – 特定のリストがアクセスしたHTTPサイトの評価で使用されているときに通知する場合に選択します。例えば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Webサイトを指定するリストの名前が表示されます。

ログの重要度 – ドロップダウンメニューから重要度を選択します。警告詳細レベルのレコードは、ESMCまたはESET PROTECTによって収集できます。

コントロール要素

追加 – 新しいURLアドレスをリストに追加します(複数の値は区切り文字を使用して入力)。

編集 – リストの既存のアドレスを修正します。**[追加]**を使用して作成したアドレスでのみ使用できます。

削除 – リストの既存のアドレスを削除します。 **[追加]**を使用して作成したアドレスでのみ使用できます。

インポート - URLアドレスを含むファイルをインポートします(たとえば、エンコードUTF-8を使用した* .txtなど、値を改行で区切ります)。

URLマスクを追加する方法

希望のアドレス/ドメインマスクを入力する前に、このダイアログの指示を参照してください。

ESET Endpoint 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。

たとえば、*.c?mは最後の部分がcで始まってmで終わり、その間に任意の記号が 1 つ入るアドレス全て(.comや. camなど)を表します。

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(「/」)とは一致しません。これは、例えば、マスク*.domain.comが*http://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*http://domain.com*にも一致します。**domain.com*の使用は、*http://anotherdomain.com*にも一致するため、正しくありません。

フィッシング対策機能

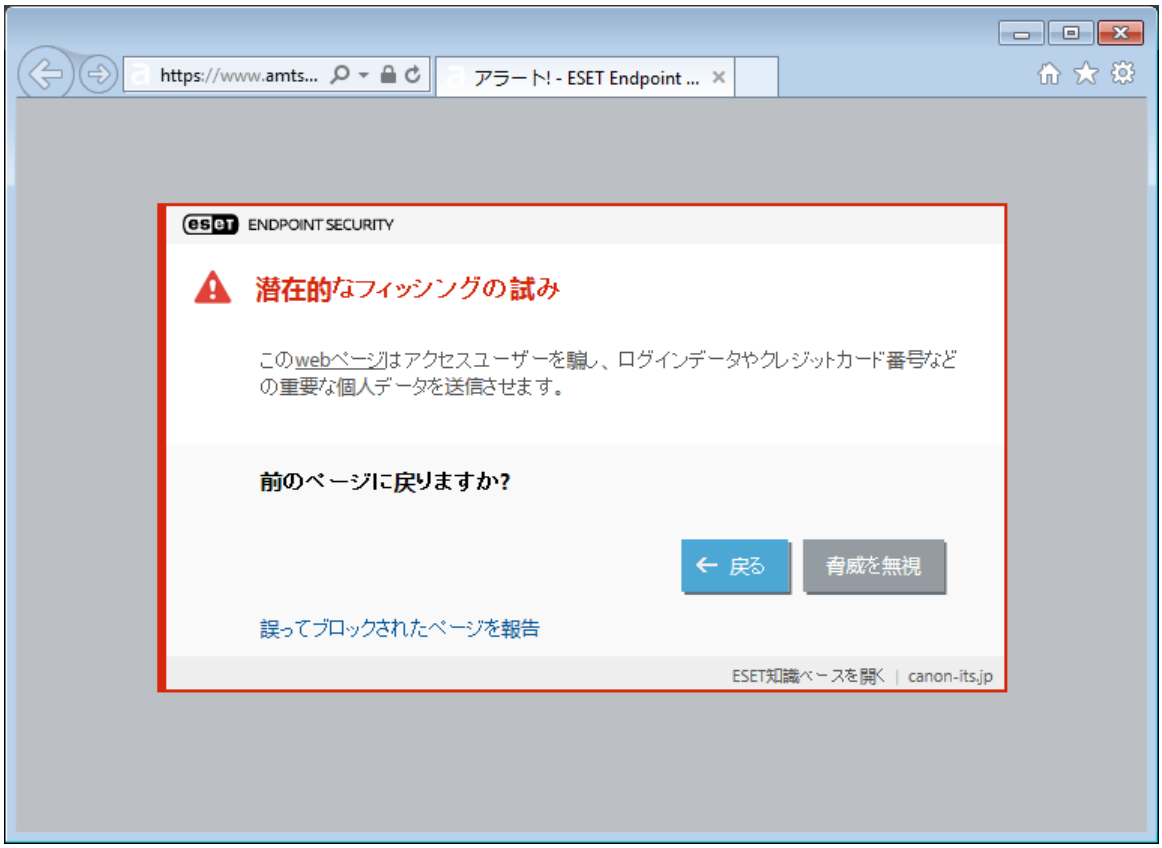
フィッシングとは、ソーシャルエンジニアリング(機密情報を入手するために、ユーザーを操ること)を用いる犯罪行為を指します。フィッシングは、銀行の口座番号やPINコードなどの機密データを入手するためによく使用されます。この活動の詳細については、「用語集」を参照してくださいESET Endpoint Securityはフィッシング対策機能を提供し、このようなコンテンツを配布することが知られているWebページをブロックできます。

ESET Endpoint Securityでフィッシング対策を有効にすることを強くお勧めします。このためには、[**詳細設定**] (F5)を開き、[**Webとメール**] > [**フィッシング対策**]に移動します。

ESET Endpoint 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。

フィッシングWebサイトにアクセスする

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、[**サイトに移動**](推奨されません)をクリックします。



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。[**詳細設定**] (F5)から、[**Webとメール**] > [**Webアクセス保護**] > [**URLアドレス管理**] > [**アドレスリスト**]をクリックし、[**編集**]をクリックして、編集するWebサイトをリストに追加します。

フィッシングサイトの報告

[報告]リンクを使用すると、フィッシングWebサイト/悪意のあるWebサイトを分析のためにESETに報告することができます。

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。

セキュアブラウザー詳細設定

この設定は、[詳細設定] (F5) > [Webとメール] > [セキュアブラウザー]から使用できます。

基本

セキュアブラウザーを有効にする – 有効にすると、保護ウェブサイトの一覧がアクティブになり、保護されたWebサイトウィンドウを開くことができるようになります。

Webサイトリダイレクト

保護されたWebサイトリダイレクトを有効にする – 有効にすると、保護されたWebサイトリストと内部インターネットバンキングリストのWebサイトがセキュアブラウザーにリダイレクトされます。

保護されたWebサイト – どのブラウザを開くか（通常またはセキュアモードで）を選択できるウェブサイト一覧。 ブラウザのフレームに表示されるESETのロゴは、安全なブラウジングがアクティブであることを意味します。

オンラインバンキングおよび決済ページを保護 – 既定では無効です。保護されたWebサイトのリストとESETの内部リストに登録されたWebサイトは、ESETによってセキュアブラウザーにリダイレクトされます。ESETで特定されたWebサイトは定期的に更新されます。

セキュアブラウザ

拡張メモリ保護を有効にする – 有効にすると、セキュアブラウザーのメモリが他のプロセスによって検査から保護されます。

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

セキュアブラウザーの対話型アラートを設定 - 対話型アラートウィンドウを開くことができます。

保護されたWebサイト

ESET Endpoint Securityには保護されたブラウザが開くように事前定義されたウェブサイトのビルトインリストが含まれています。 ウェブサイトを追加したり、製品のコンフィグレーションでウェブサイトのリストを編集したりできます。

保護されたWebサイトリストは、[詳細設定] (F5) > [Webとメール] > [セキュアブラウザー] > [基本] > [保護されたWebサイト] > [編集]から使用できます。

ウィンドウは次の内容で構成されています。

列

Web サイト – 保護されたWebサイト。

セキュアなブラウザ - ESETのロゴが、セキュアに閲覧している時にブラウザの境界線の周囲に表示されます。

標準のブラウザー – このオプションを選択すると、既定のWebブラウザーで続行します(オンラインバンキングトランザクションなど)。

コントロール要素

追加 – 既知の Webサイトとして、一覧に追加できます。

編集 – 選択したエントリーを編集することができます。

削除 – 選択したエントリーを削除します。

Webコントロール

Webコントロールセクションでは、法的責任のリスクから会社を保護する設定を構成できますWebコントロールは、知的財産権に抵触するWebサイトへのアクセスを規制できます。この機能の目的も、作業生産性に悪影響を与える可能性のある不適切または有害なコンテンツやページに従業員がアクセスしないようにすることにあります。

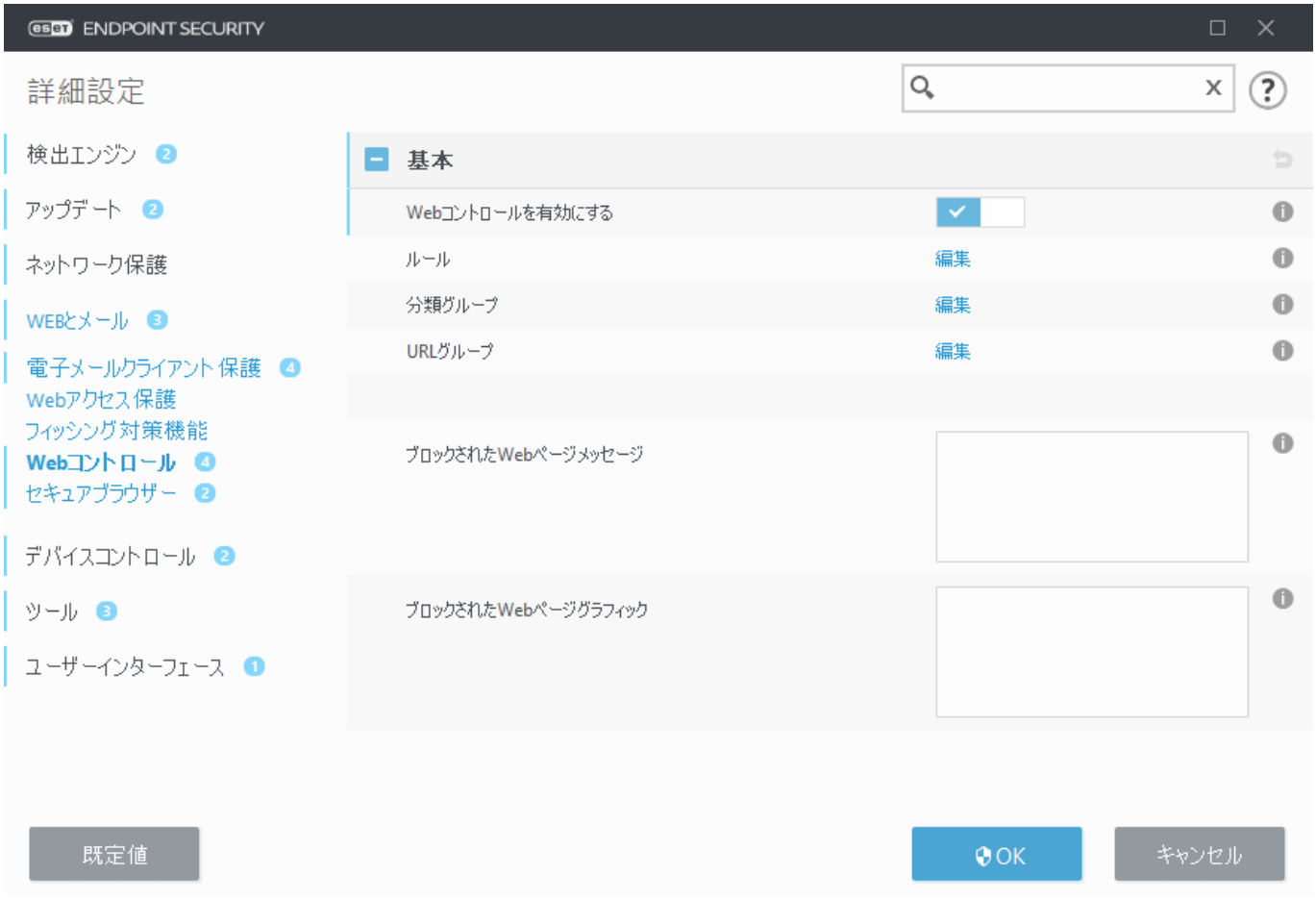
[Webコントロール]セクションでは、対象ユーザーに対して適切でない内容を掲載していると考えられるWebページをブロックします。さらに、企業やシステム管理者は、事前に定義された27以上のカテゴリと140以上のサブカテゴリへのアクセスを禁止できます。

既定ではWebコントロールは無効ですWebコントロールを有効にするには、次の手順を実行します。

1.**F5**を押して、**詳細設定**を表示し、**Webとメール > Webコントロール**を展開します。

2.**Webコントロールを有効にする**を選択してESET Endpoint SecurityでWebコントロールを有効にします。

3.特定のWebページへのアクセスを設定するには、**ルール**の横の**編集**をクリックして、Webコントロールルールエディターウィンドウを開きます。



ブロックされたWebページメッセージと**ブロックされたWebページグラフィック**フィールドではWebサイトがブロックされたときに表示されるメッセージを簡単にカスタマイズできます。

> すべてのWebページをブロックし、特定の項目のみを利用可能にする場合は、URLアドレス管理を使用します。

Webコントロールルール

ルールエディタウィンドウには、既存のURLベースまたはカテゴリベースのルールが表示されます。



このルール一覧には、名前、ブロックのタイプ、Webコントロールルールの照合後に実行するアクション、ログの重大度などのいくつかのルールの説明が含まれます。

[**追加**]または[**編集**]をクリックしてルールを管理します。[**コピー**]をクリックして、別の選択済みルールで使用されている事前定義オプションを備えた新しいルールを作成します。**Ctrl**キーを押しながらクリックすると、複数のルールを選択し、選択したルールをすべて削除できます。[**有効**]チェックボックスでは、ルールを無効または有効にできます。これは、将来使用するつもりのルールを永続的に削除したくない場合に便利です。

ルールは優先度を決定する順序で並べ替えられます。優先度が高いルールが先頭になります。ルールの優先度を変更するには、ルールを選択し、矢印ボタンをクリックして、ルールの優先度を上下します。二重矢印をクリックすると、ルールをリストの一番上または一番下に移動します。

ルールの作成に関する詳細をお読みください。

Webコントロールルールの追加

Webコントロールルールウィンドウでは、Webコントロールの既存フィルタリングルールを手動で作成または変更できます。

名前

特定しやすいように、ルールの説明を**名前**フィールドに入力します。

有効

[**有効**]をクリックすると、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。

アクション

URLに基づくアクションまたは**カテゴリに基づくアクション**を選択します。

URLに基づくアクション

特定のWebサイトへのアクセスを制御するルールの場合、**[URL]**フィールドにURLを入力します。

特殊記号の*(アスタリスク)および?(疑問符)はURLアドレスリストで使用できません。複数の上位レベルドメイン(TLD)があるWebサイトを含むURLグループを作成する場合は、各TLDを個別に追加する必要があります。グループにドメインを追加するときは、このドメインとすべてのサブドメイン(*sub.examplepage.com*など)にあるすべてのコンテンツがURLに基づくアクションに従ってブロックまたは許可されます。

URLまたは**URLグループを使用**- URLリンクまたはリンクのURLグループを使用して、これらのURLのいずれかが検出されたときに、許可、ブロック、またはユーザーへの警告の表示を行います。



分類に基づくアクション

選択すると、ドロップダウンメニューを使用してアクションのWebサイトカテゴリを設定します。

URLカテゴリまたは**グループを使用**-Webサイトカテゴリまたはカテゴリのカテゴリグループを使用して、これらのグループのいずれかが検出されたときに、許可、ブロック、またはユーザーへの警告の表示を行います。

アクセス権

- **許可**- URLアドレス/分類へのアクセスが認可されます。
- **警告** - URLアドレス/分類に関する警告が表示されます。
- **常に警告** - URLアドレス/分類に関する警告が表示されますWebサイトにアクセスできますが、管理者に通知されます。
- **ブロック** - URLアドレス/分類がブロックされます。

適用期間

特定の期間に作成されたルールを適用できます。ドロップダウンメニューから、時間スロットを選択します。

- 時間スロットの詳細

ログ記録の重大度

- **常に記録する** – すべてのオンライン通信を記録します。
- **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** – ログは作成されません。

ログの重要度はルールごとに個別に設定できます。**警告**ステータスのログは、ESET Security Management Centerによって収集できます。

ユーザー一覧

- **追加** - **[ユーザーまたはグループの選択]**ダイアログウィンドウが開き、目的のユーザーを選択できます。ユーザーを入力しないと、ルールはすべてのユーザーに適用されます。
- **削除** – 選択されたユーザーをフィルタから削除します。

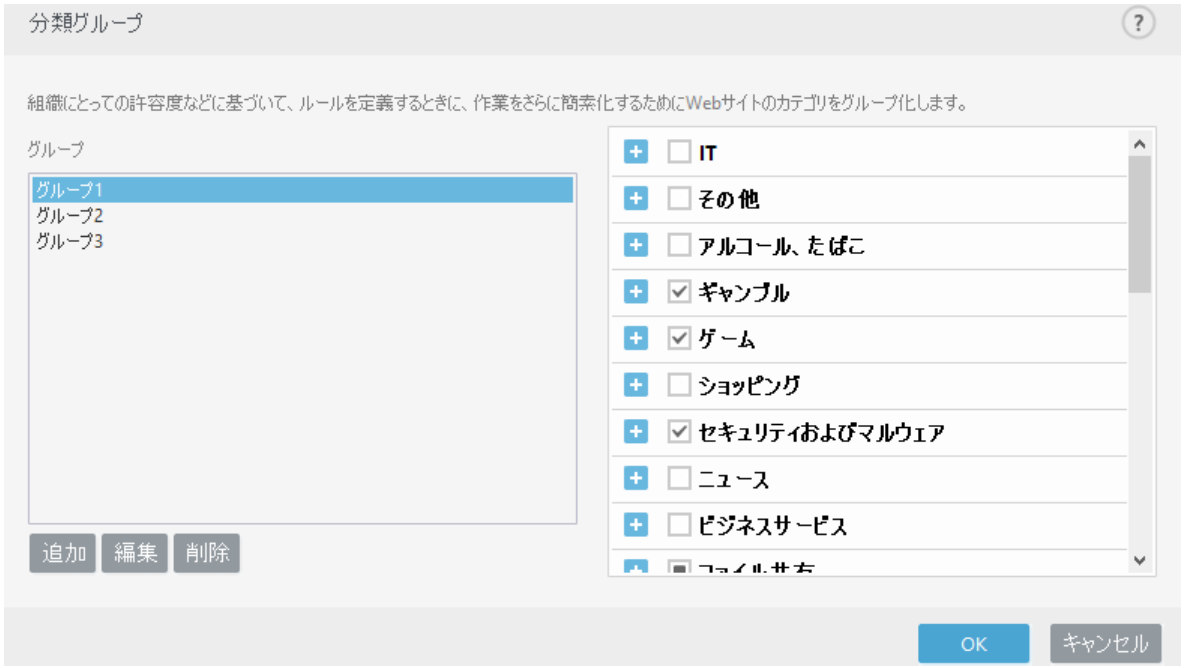
分類グループ

分類グループウィンドウは、2つの部分に分かれます。このウィンドウの左側の部分には、カテゴリグループの一覧が表示されます。

- **追加** – クリックすると、新しいカテゴリグループを作成します。
- **編集** – クリックすると、既存のカテゴリグループを編集します。
- **削除** – カテゴリグループのリストから既存のカテゴリグループを削除する場合は、選択してクリックします。

ウィンドウの右側にはカテゴリとサブカテゴリの一覧が表示されます。カテゴリリストでカテゴリを選択すると、サブカテゴリが表示されます。各グループには、成人向けまたは一般的に不適切なサブカテゴリ、および一般的に問題がないと見なされるカテゴリが含まれます。[分類グループ]ウィンドウを開き、最初のグループをクリックすると、カテゴリまたはサブカテゴリを適切なグループのリストに追加したり、そこから削除したりできます(暴力や武器など)。不適切なコンテンツのWebページはブロックできます。あるいは、定義済みアクションを使用したルールが作成された後に、ユーザーに通知できます。

チェックボックスを選択し、特定のグループにサブカテゴリを追加したり、そこから削除したりします。



ユーザーに知られていない可能性があるカテゴリの例を次に示します。

その他 – 通常は、イントラネット、192.168.0.0/16などのプライベート(ローカル)IPアドレスです。403または404エラーコードが表示された場合、そのWebサイトはこの分類にも一致します。

未解決 – この分類にはWebコントロールデータベースエンジンへの接続時のエラーによって解決されなかったWebページが含まれます。

未分類 – まだWebコントロールデータベースにない未知のWebページです。

プロキシ – 通常はWebコントロールフィルタによって禁止されているWebページに(匿名)アクセスするために、アノニマイザ、リダイレクタ、パブリックプロキシサーバなどのWebページを使用できます。

ファイル共有 – これらのWebページには、写真や画像、電子書籍などの大量のデータが含まれています。これらのサイトには、不快な内容や成人向けコンテンツが含まれている危険性があります。

> サブカテゴリは任意のグループに所属することができます。サブ分類によっては、事前定義のグループ(たとえばゲーム)に所属しないものもありますWebコントロールフィルタを使用して目的のサブ分類を突き合わせるには、それを目的のグループに追加します。

URLグループ

URLグループエディタを使用すると、ルールを作成する複数のURLリンクを含むグループを作成できます(特定のWebサイトを許可/禁止)。

新しいURLグループの作成

新しいURLグループを作成するには、**追加**をクリックして、新しいURLグループの名前を入力します。

管理者がより多くのWebページのルールを作成するときにはURLグループの使用が役立ちます(選択に応じてブロックまたは許可されます)。

URLアドレスをURLグループリストに追加 – 手動

新しいアドレスをリストに追加するにはURLグループを選択し、ウィンドウの右下で**追加**をクリックします。

特殊記号*（アスタリスク）および?（疑問符）はURLアドレスリストで使用できません。

http://またはhttps://で、ドメインの完全名を入力する必要はありません。

ドメインをグループに追加する場合は、このドメインとすべてのサブドメインにあるすべてのコンテンツ（たとえば、*sub.examplepage.com*）がURLに基づくアクションの選択に応じて、ブロックまたは許可されます。

最初のルールがドメインをブロックし、2番目のルールが同じドメインを許可するというような、2つのルール間で競合がある場合は、特定のドメインまたはIPアドレスがブロックされます。ルールの作成の詳細については、URLに基づくアクションを参照してください。

URLアドレスをURLグループリストに追加 – .txtファイルを使用したインポート

インポートをクリックしてURLアドレスのリストのファイルをインポートします（例えばUTF-8エンコーディングされた.txt等を使用しURLアドレスが複数ある場合は改行で区切ることができます）。特殊記号*（アスタリスク）および?（疑問符）はURLアドレスリストで使用できません。

Webコントロールでの URLグループの使用

特定のURLグループで実行されるようにアクションを設定するには、Webコントロールルールエディターを開き、ドロップダウンメニューを使用してURLグループを選択し、他のパラメーターを調整してから、**OK**をクリックします。

> 特定のWebページをブロックするか許可するほうが、1つの分類のWebページ全体をブロックまたは許可するより、精度が高くなることがあります。これらの設定を変更したり、分類やWebページをリストに追加する場合は注意してください。

ブロックされたWebページメッセージのカスタマイズ

ブロックされたWebページメッセージと**ブロックされたWebページグラフィック**フィールドではWebサイトがブロックされたときに表示されるメッセージを簡単にカスタマイズできます。

これは、ユーザーがブロックされたWebサイトにアクセスしようとするときのブラウザー内通知の既定のメッセージおよび設計です。

使用状況

「兵器」のWebサイトカテゴリをブロックします。

ブロックされたWebサイトメッセージの例:

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

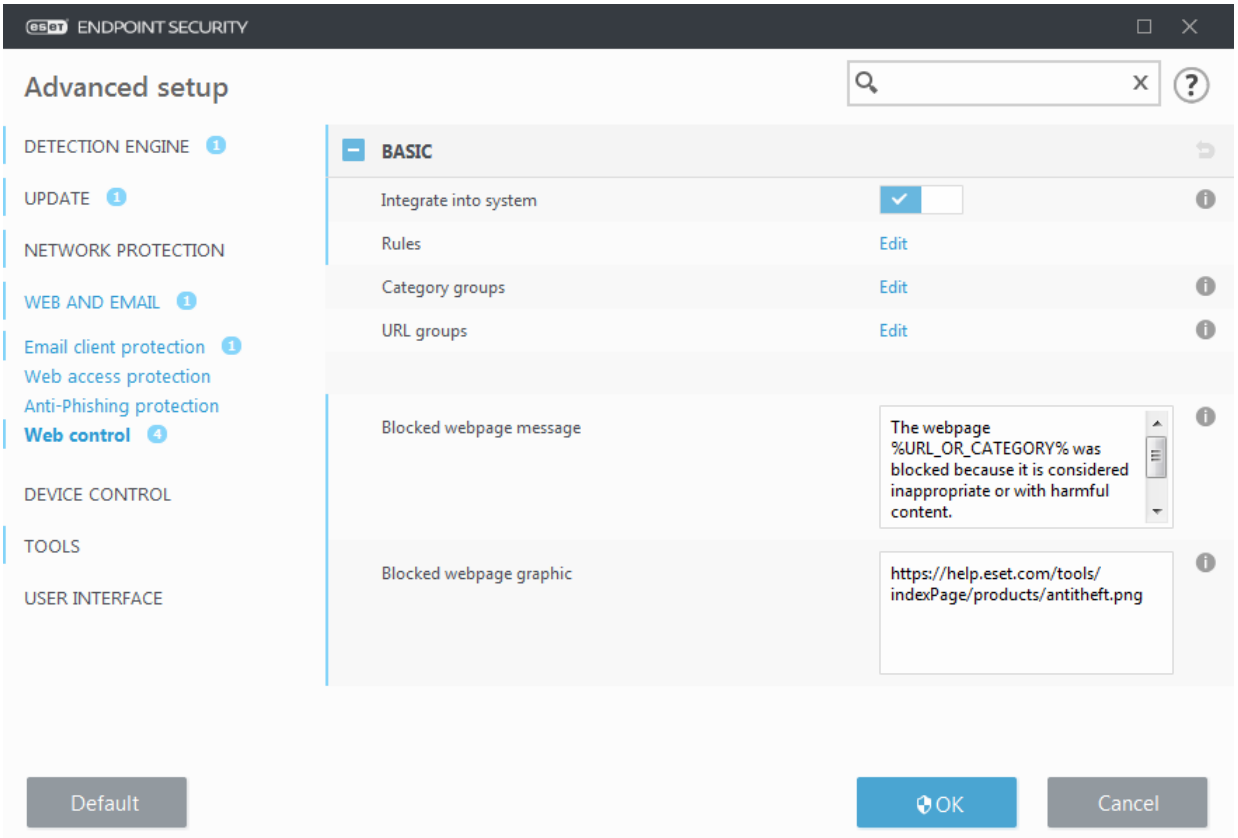
変数	説明
%CATEGORY%	ブロックされたWebコントロールカテゴリ。
%URL_OR_CATEGORY%	ブロックされたWebコントロールWebサイトまたはカテゴリ(Webコントロールブロックルールによる)。
%STR_GOBACK%	[戻る]ボタンの値。
%product_name%	ESET製品の名前(ESET Endpoint Security)
%product_version%	ESET製品のバージョン。

ブロックされたWebページグラフィックスの例:

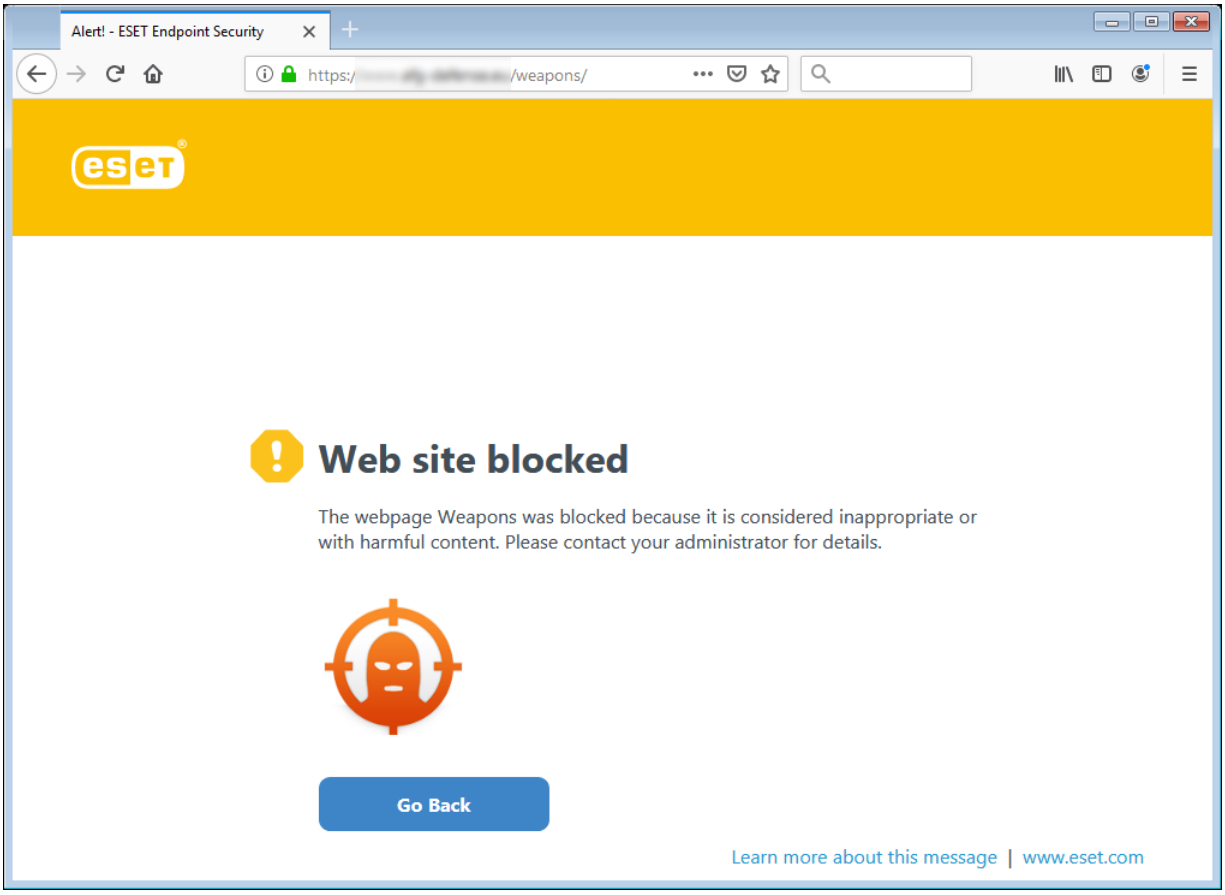
```
https://help.eset.com/tools/indexPage/products/antitheft.png
```

サイズが高すぎる場合は、画像サイズ(幅/高さ)は自動的に調整されます。

ESET Endpoint Securityの設定は次のようになります。



ユーザーがブロックされたWebサイトにアクセスしようとしたときのブラウザー内のカスタム通知は次のようになります。



アップデート

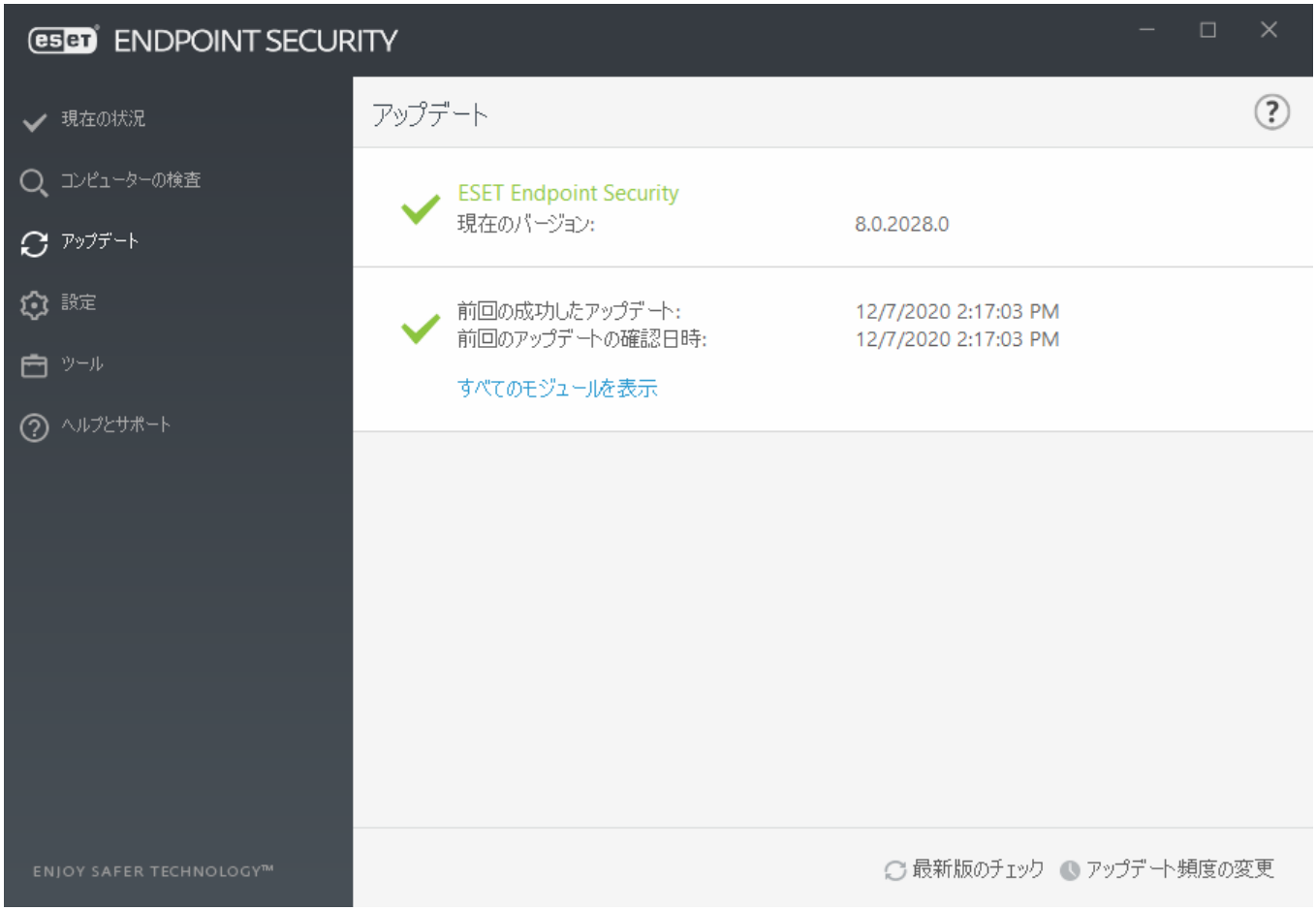
コンピューターのセキュリティを最大限確保するためにはESET Endpoint Securityを定期的にアップデートするのが最善の方法です。アップデートモジュールにより、プログラムは検出エンジンのアップデートとシステムコンポーネントのアップデートという2つの方法で、常に最新の状態に保たれます。プログラムがアクティベーションされるときに、既定では、アップデートは自動的に行われます。

メインプログラムウィンドウの[**アップデート**]をクリックすると、前回成功したアップデートの日時、アップデートが必要かどうかなど、現在のアップデートの状態を確認できます。**すべてのモジュールを表示**リンクをクリックして、インストールされたモジュールのリストを開き、モジュールのバージョンと最後のアップデートを確認します。

さらに、アップデートプロセスを手動で開始する[**最新版のチェック**]も使用できます。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、悪意のあるコードからの完全な保護を維持するための重要な部分です。この部分の設定や操作には注意してください。インストール中にライセンスの詳細を入力しなかった場合は、更新時に[**製品のアクティベート**]をクリックして、ライセンスキーを入力するとESETのアップデートサーバーにアクセスすることができます。

ユーザー名とパスワードを使用せずに、オフラインライセンスファイルを使用してESET Endpoint Securityをアクティベーションする場合は、赤色の情報**モジュールアップデートが失敗しました**が表示され、ミラーからのみアップデートをダウンロードできることを示します。

ESET Endpoint Securityの購入後、ライセンスキーがESETから提供されます。



現在のバージョン - ESET Endpoint Securityのビルド番号。

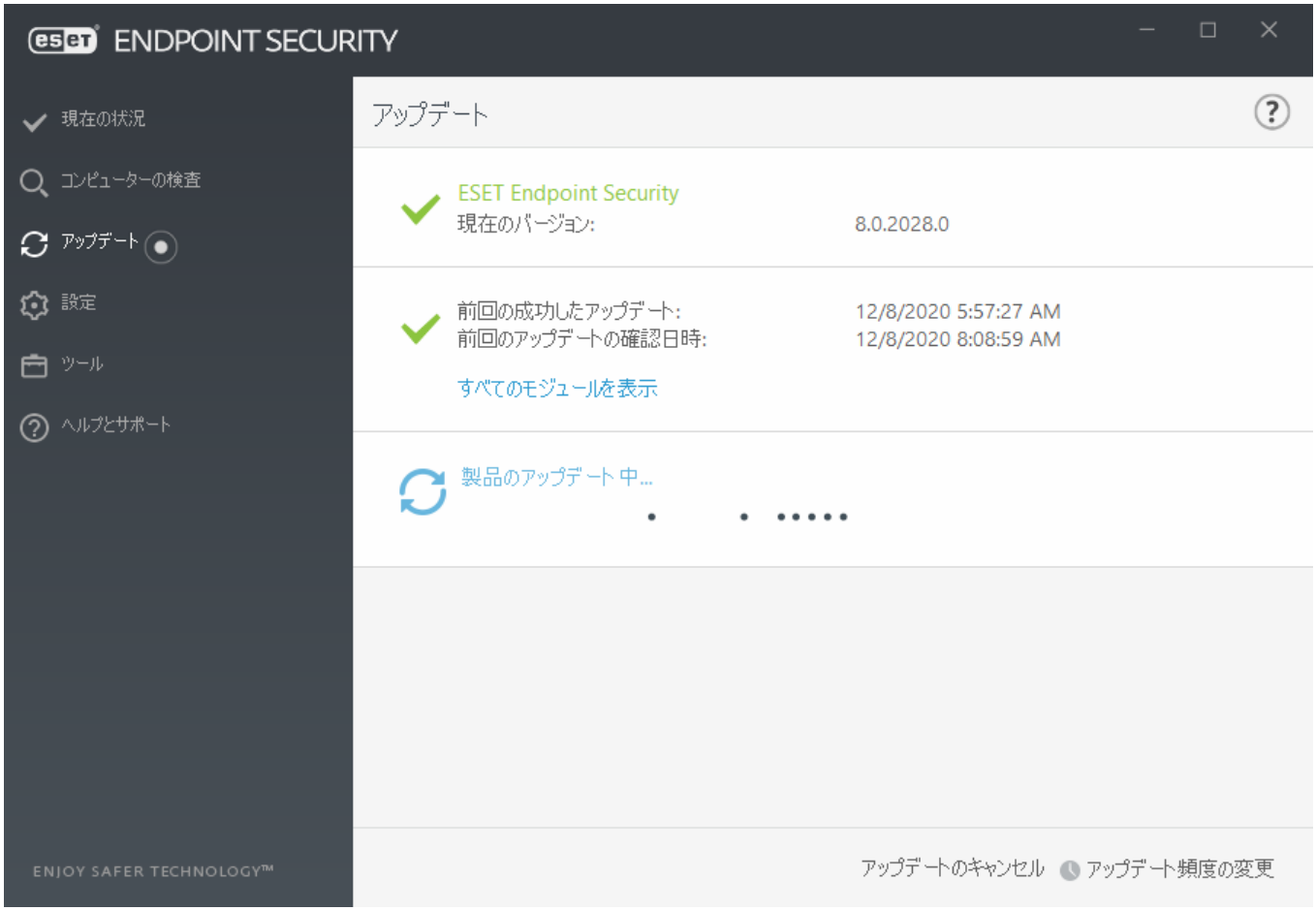
最終成功アップデート – 最終成功アップデートの日時です。検出エンジンが最新、つまり最近の日付になっていることを確認します。

アップデートの最終成功チェック – モジュールのアップデートを最後に試行して成功した日時。

すべてのモジュールを表示 – クリックすると、インストールされたモジュールのリストを開き、モジュールのバージョンと最後のアップデートを確認します。

アップデートプロセス

[**アップデートの確認**]をクリックすると、ダウンロードが始まります。ダウンロードの進行状況バーとダウンロードにかかる残り時間が表示されます。アップデートを中断するには、[**アップデートのキャンセル**]をクリックします。

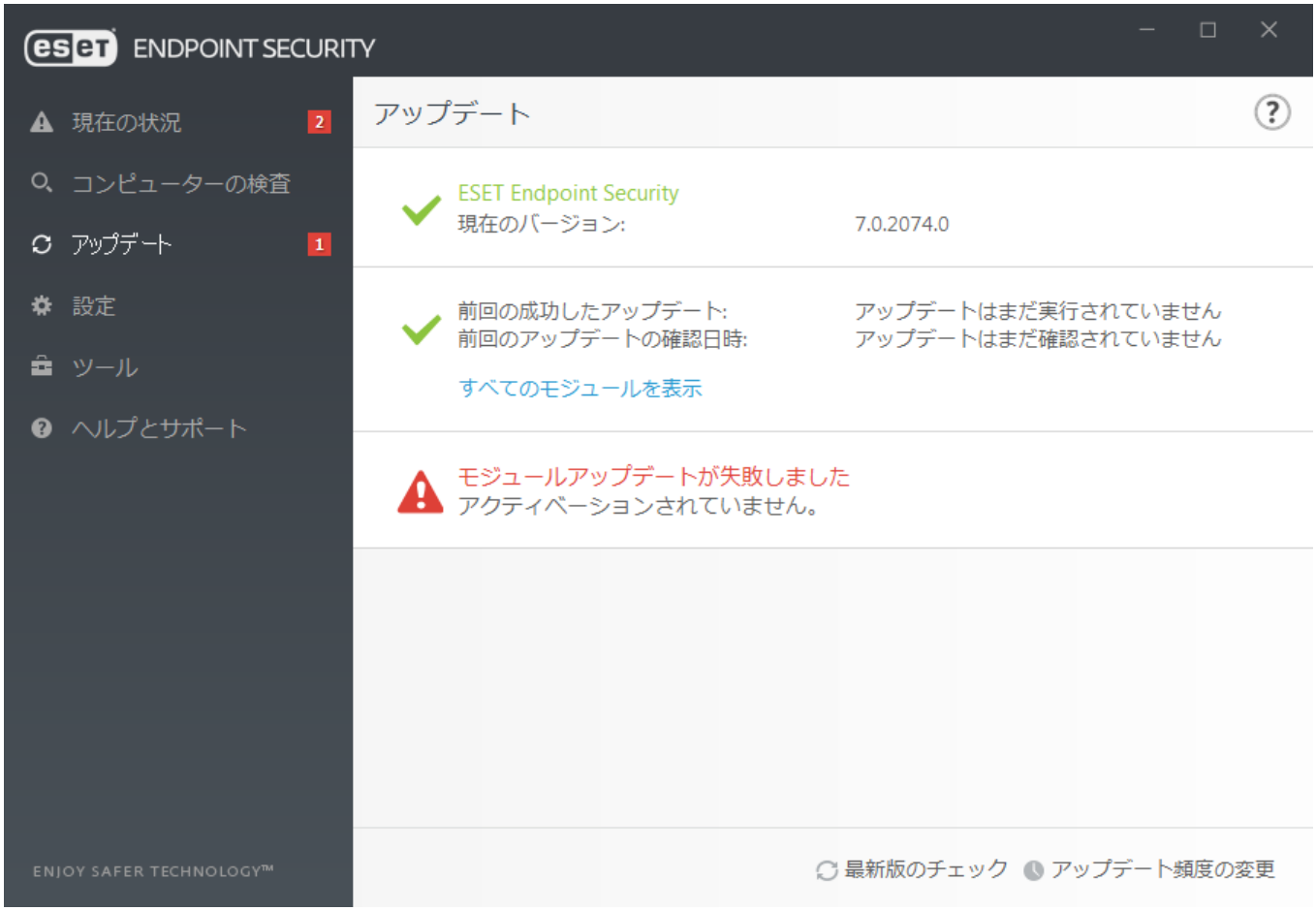


通常は、モジュールは1日に数回アップデートされます。そうでない場合は、プログラムが古くなっており、感染しやすくなっているということです。モジュールはできるだけ早くアップデートしてください。

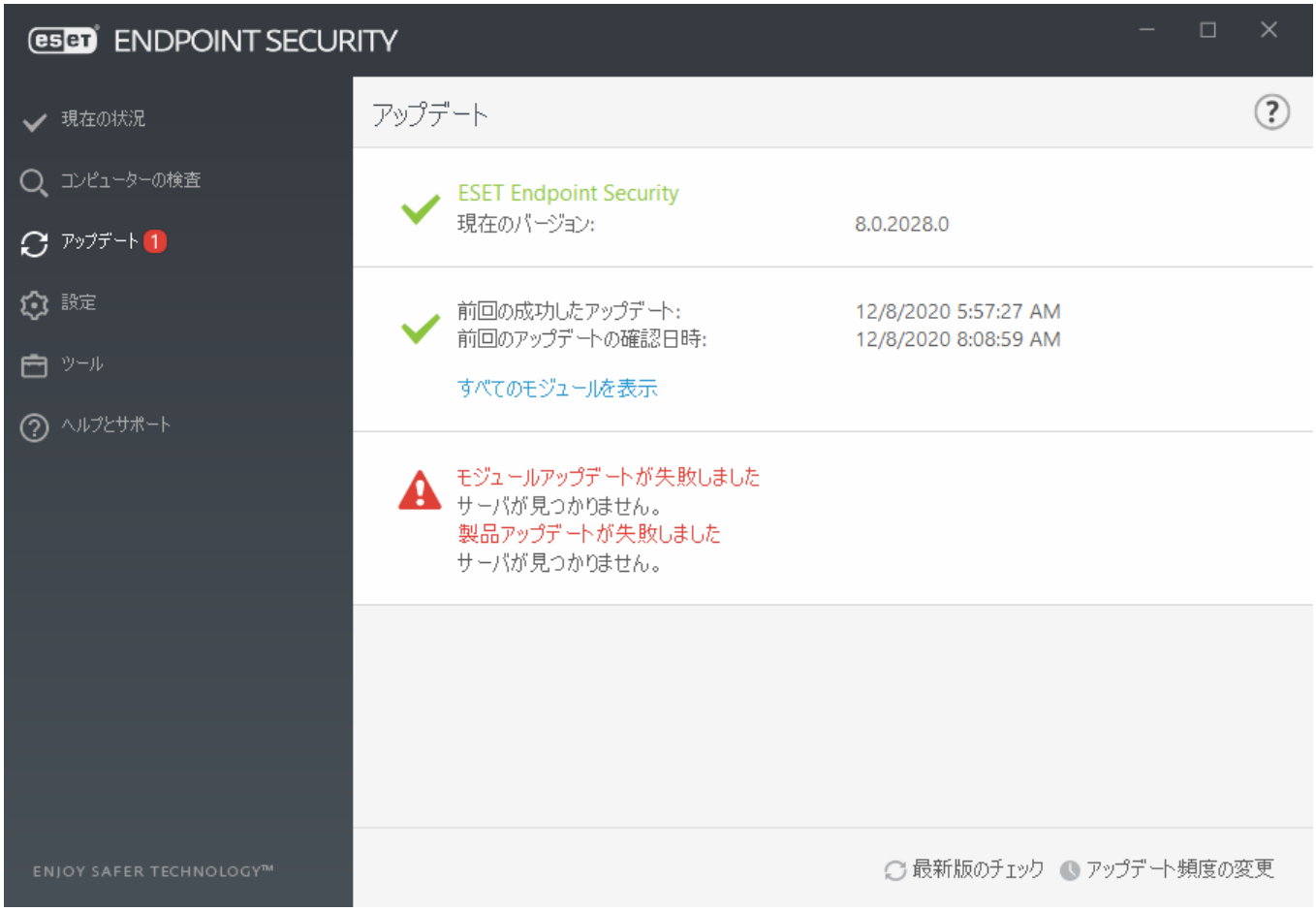
検出エンジンは最新ではありません – このエラーは、モジュールをアップデートしようとして何回か失敗すると表示されます。アップデートの設定をチェックすることをお勧めします。このエラーが起こる原因として最も多いのは、認証データが正しく入力されていない、または 接続設定が適切ではないことです。

上記の通知は、アップデートの失敗に関する次の2つのメッセージ(**モジュールのアップデートが失敗しました**)に関連します。

1. **無効なライセンス** – 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]ウィンドウ(メインメニューで[**設定**]をクリックして、[**詳細設定**]をクリックするか、またはキーボードのF5キーを押す)に、追加のアップデートオプションが示されています。 メインメニューで[**ヘルプとサポート**]>[**ライセンスの変更**]をクリックして、新しい製品認証キーを入力します。



2. **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** – このエラーはインターネット接続の設定が正しくないことが原因のことがあります。インターネット接続を確認することをお勧めします(Webブラウザーで任意の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、コンピューター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。



詳細については、ESETナレッジベース記事を参照してください。

アップデートの設定

アップデートの設定オプションは、[**アップデート**]の下の[**詳細設定**]ツリー(F5キー)から使用できます。このセクションでは、アップデートサーバやそれらのサーバの認証データなど、アップデート用の設定情報を指定します。

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(HTTPS通信)を許可されていることを確認してください。

基本

現在使用中のアップデートプロファイルは、**既定のアップデートプロファイルを選択**ドロップダウンメニューに表示されます。

新しいプロファイルを作成するには、プロファイルセクションを参照してください。

プロファイルの自動切り替え – ファイアウォールの既知のネットワークに従って更新プロファイルを割り当てます。自動プロファイル切り替えは、スケジューラの設定に応じて、特定のネットワークのプロファイルを変更することができます。詳細については、ヘルプページを確認してください。

アップデート通知を設定する – 編集をクリックすると、表示されるアプリケーション通知を選択できます。通知がデスクトップに表示されるか、電子メールで送信されるかどうかを選択できます。

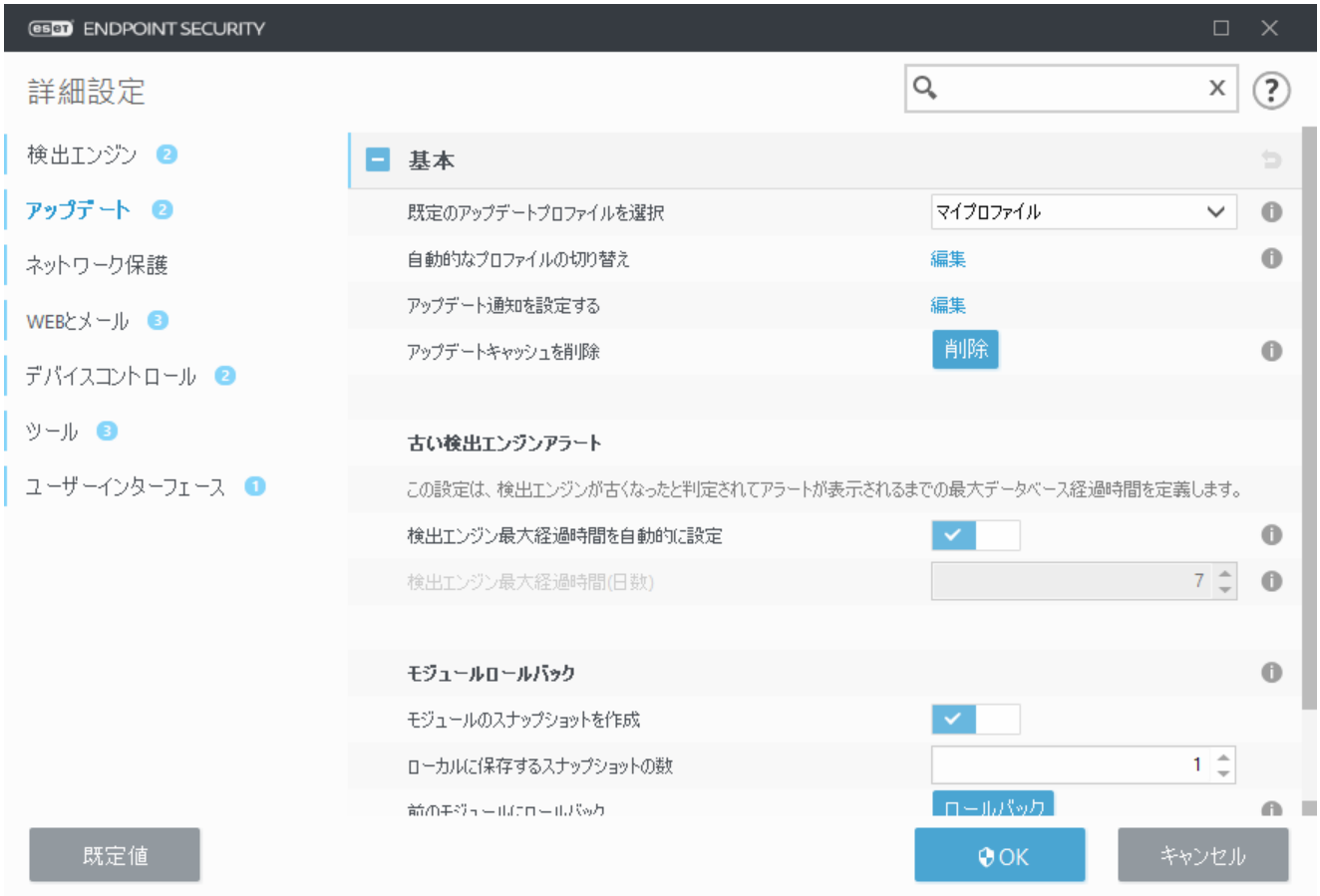
モジュールアップデートを試行するときに問題が発生した場合は、**アップデートキャッシュをクリア**の横の**クリア**をクリックして、一時アップデートファイルとキャッシュを消去します。

古い検出エンジンアラート

最大検出エンジン経過時間を自動的に設定 – 検出エンジンが期限切れに設定されるまでの最大時間(日数)を設定できます。**最大検出エンジン経過時間(日数)**の既定値は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。



プロファイル

さまざまなアップデートの設定用およびアップデートタスク用のアップデート プロファイルを作成できます。アップデートプロファイルを作成することは、常時変わるインターネット接続のプロパティに合わせて代替プロファイルが必要なモバイルユーザーにとって特に便利です。

[**編集するプロファイルを選択**]ドロップダウンメニューには、現在選択されているプロファイルが表示されます。これは、既定では[**マイプロファイル**]に設定されます。

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**]をクリックし、[**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。

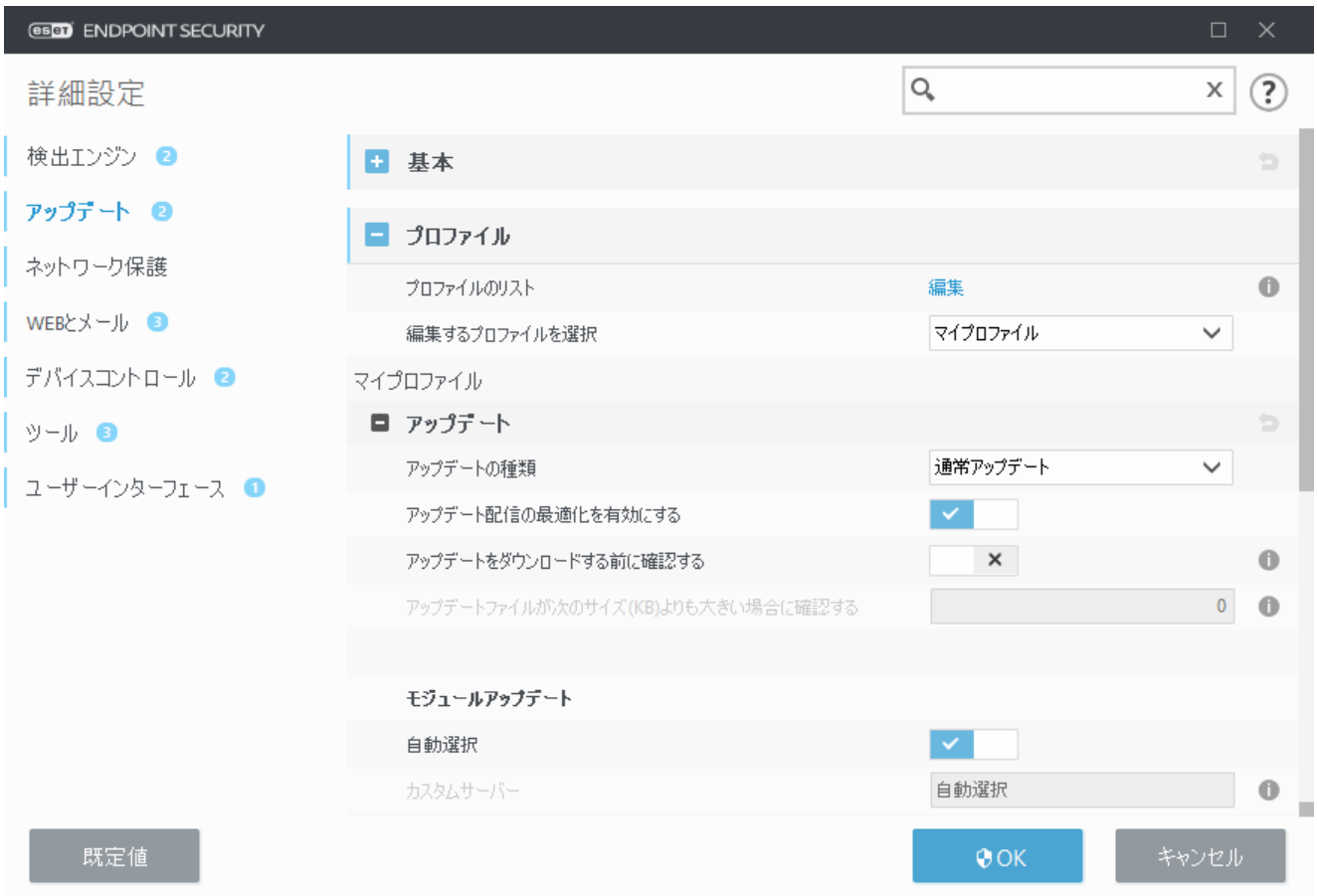
更新

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。テストモードの更新データ([テストモード]オプション)は、徹底的な内部テストを経てリリースされ、近いうちに一般に公開されるアップデートです。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]を使用すると、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。

アップデート配信最適化を有効にする – 有効にするとCDN (コンテンツ配信ネットワーク)からアップデートファイルをダウンロードできます。この設定を無効にすると、専用ESETアップデートサーバーが過負荷状態になったときに、ダウンロードが中断され、速度が低下する場合があります。ファイアウォールによってESETアップデートサーバIPアドレスへのアクセスのみに制限されているときやCDNサービスへの接続が動作していないときに無効にすると役立ちます。

アップデートをダウンロードする前に確認する – アップデートファイルのダウンロードを確認または拒否できる通知が表示されます。アップデートファイルのサイズがアップデートファイルが次のサイズより大きい場合確認する(kB)フィールドに指定した値より大きい場合、確認ダイアログが表示されます。アップデートファイルのサイズが0 KBの場合は、常に確認ダイアログが表示されます。



モジュールアップデート

自動選択オプションが既定で有効です。**カスタムサーバー**オプションは、アップデートファイルが保存される場所ですESETアップデート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。

検出定義のより頻繁なアップデートを有効にする – 検出定義のアップデート間隔が短くなります。この設定を無効にすると、検出率に悪影響を及ぼす場合があります。

リムーバブルメディアからモジュールの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。

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://*コンピューター名または*IP*アドレス: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://*コンピューター名または*IP*アドレス: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。\\コンピューター名または*IP*アドレス\共有フォルダー

上記の例で指定されたHTTPサーバーポート番号は、HTTP/HTTPSサーバーがリスニングするポートによって異なります。

プログラムコンポーネントのアップデート

プログラムコンポーネントのアップデートを参照してください。

接続オプション

接続オプションを参照してください。

配布用アップデート

アップデートミラーを参照してください。

アップデートのロールバック

新しい検出エンジンアップデートやプログラムモジュールのアップデートが不安定であったり破損している疑いがある場合、前のバージョンにロールバックし、一時的に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 Endpoint Securityは、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。 ウイルスデータベース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。**モジュールのスナップショットを作成する**を有効にすると、最初のアップデート中に最初のスナップショットが作成されます。次のスナップショットは48時間後に作成されます。**ローカルに保存するスナップショットの数**フィールドにより、保存されている検出エンジンスナップショットの数が定義されます。

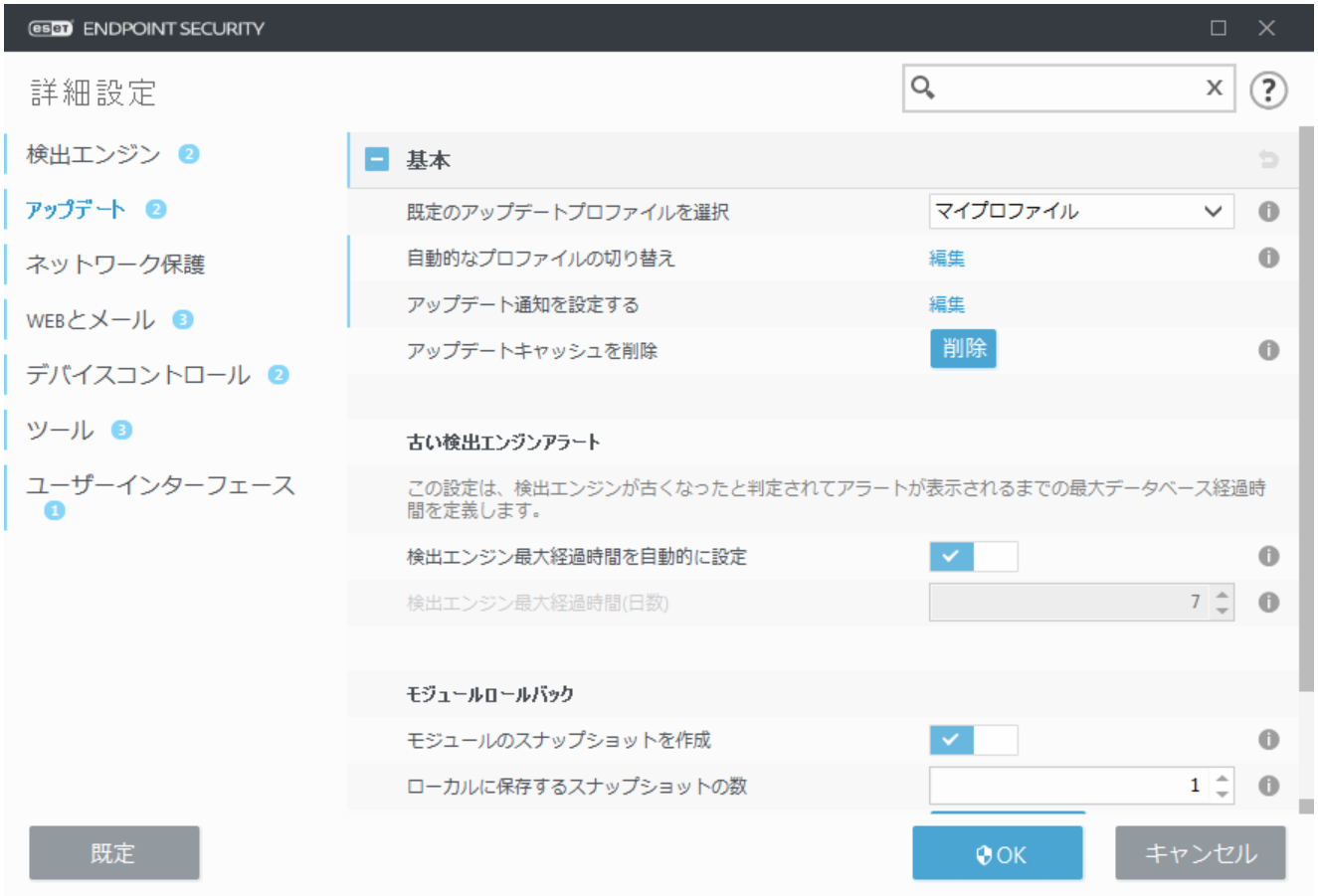
最大スナップショット数(例: 3つ)に達すると、最も古いスナップショットが48時間ごとに新しいスナップショットに置換されますESET Endpoint Securityは検出エンジンとプログラムモジュールのアップデートバージョンを最も古いスナップショットにロールバックします。

ロールバック(詳細設定(F5) > アップデート > 基本 > モジュールロールバック)をクリックする場合は、**期間**ドロップダウンメニューから時間間隔を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。

ロールバックを実行すると、**ロールバック**ボタンは**アップデートを許可**に変わります。**アップデートの一時停止**]ドロップダウンメニューで選択した期間中は、アップデートは許可されません。 検出エンジンのバージョンは最も古い使用可能なバージョン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。



検出エンジンの最新のバージョンが22700であると仮定します。検出エンジンのスナップショットとして、22698と22696が保存されているとします。22697は利用できません。この例では、22697のアップデート中にコンピューターがオフになっていて、22697がダウンロードされるよりも前により新しいアップデートが利用できるようになっています。**ローカルに保存するスナップショットの数**フィールドを2に設定して、**ロールバック**をクリックすると、検出エンジン(プログラムモジュールを含む)はバージョン番号22696に復元されます。このプロセスには少々時間がかかることがあります。アップデートセクションで検出エンジンのバージョンがダウングレードされたかどうかを確認してください。

プログラムコンポーネントのアップデート

プログラムコンポーネントのアップデートセクションには、プログラムコンポーネントのアップデートに関連するオプションがあります。このプログラムでは、プログラムコンポーネントの新しいアップデートファイルが使用可能になったときの動作を事前に定義することができます。

プログラムコンポーネントのアップデートによって、新しい機能が提供されたり、これまでのバージョンの既存の機能が変更されたりします。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。プログラムコンポーネントのアップデートファイルをインストールした後、再起動が必要になることがあります。

アップデートモードドロップダウンメニューには3つのオプションがあります。

- **アップデートする前に確認する** – 管理されていないエンドポイントの既定のオプションです。プログラムコンポーネントのアップデートが利用可能になったとき、インストールするか拒否するかの確認を求められます。
- **自動アップデート** – プログラムコンポーネントのアップデートファイルが自動的にダウンロードされてインストールされます。コンピューターの再起動が必要になることがあるので注意してください。
- **アップデートしない** – プログラムコンポーネントのアップデートは実行されません。このオプションは、サーバーインストールに適しています。サーバーは通常、保守中にしか再起動できないためです。

既定では、プログラムコンポーネントのアップデートはESETリポジトリサーバーからダウンロードされます。大規模な環境やオフライン環境では、トラフィックを分散し、プログラムコンポーネントファイルの内部キャッシュを有効にすることができます。

プログラムコンポーネントのアップデートのカスタムサーバーの定義

1.**カスタムサーバー**フィールドでプログラムコンポーネントのアップデートへのパスを定義します。HTTP(S)リンク、SMBネットワーク共有パス、ローカルディスクドライブ、またはリムーバブルメディアパスにすることができます。ネットワークドライブの場合、マッピングされたドライブ文字の代わりに、UNCパスを使用できます。

2.必要ではない場合、**ユーザー名**と**パスワード**を空欄にします。
必要に応じて、カスタムWebサーバーのHTTP認証について、該当する資格情報をここで定義します。

3.変更を確認し、標準のESET Endpoint Securityアップデートを使用して、プログラムコンポーネントのアップデートの存在をテストします。

最適なオプションの選択方法は、設定が適用されるワークステーションによって異なります。ワークステーションとサーバーとでは異なる点に注意してください。たとえば、プログラムのアップデート後にサーバーを自動的に再起動すると、重大な損害が生じることがあります。

接続オプション

指定されたアップデートプロファイルのプロキシサーバー設定オプションにアクセスするには、**[詳細設定]**ツリー(F5)の[**アップデート**]をクリックしてから、[**プロファイル**] > [**アップデート**] > [**接続オプション**]ボタンをクリックします。

プロキシサーバー

[**プロキシモード**]ドロップダウンメニューをクリックし、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
- プロキシサーバを使用して接続する
- プロキシサーバのグローバル設定を使用する

[**グローバルプロキシサーバ設定を使用する**]を選択すると、[詳細設定]ツリーの[**ツール**]>[**プロキシサーバー**]ブランチで既に指定されているプロキシサーバ設定オプションが使用されます。

[**プロキシサーバを使用しない**]を選択するとESET Endpoint Securityのアップデートにプロキシサーバーを使用しないように指定されます。

[**プロキシサーバを使用して接続する**]オプションは、次の場合に選択する必要があります。

- [ツール] > [**プロキシサーバー**]で定義されている以外のプロキシサーバーはESET Endpoint Securityをアップデートするために使用されます。 この設定では、必要に応じて、[**プロキシサーバー**]の下で、そのプロキシサーバーのアドレス、**ポート**(既定は3128)、**ユーザー名**と**パスワード**を指定する必要があります。
- プロキシサーバー設定はグローバルには設定されませんがESET Endpoint Securityはアップデートを取得するためにプロキシサーバーに接続する場合。
- コンピュータがプロキシサーバー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、変更されている(ISPを変更するなど)場合、このウィンドウから一覧の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ーに接続できません。

プロキシサーバーの既定の設定は、[**プロキシサーバのグローバル設定を使用する**]です。

プロキシが使用できない場合は直接接続を使用する –接続できない場合はアップデート中にプロキシをバイパスします。

Windows共有

Windows NTオペレーティングシステムのバージョンでローカルサーバーからアップデートする場合は、既定で、ネットワーク接続ごとに認証が必要です。

このようなアカウントを構成するには、ドロップダウンメニューから**LANに接続するアカウント**を選択します。

- **システムアカウント(既定)**
- **現在のユーザー**
- **指定したユーザー**

システムアカウントを認証に使用するには、[**システムアカウント(既定)**]を選択します。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するには、[**現在のユーザー**]を選択します。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。

特定のユーザーアカウントが認証に使用されるようにするには、[**指定されたユーザー**]を選択します。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、ローカルサーバー上のアップデートファイルディレクトリー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。

ユーザー名と**パスワード**は任意です。

[**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。

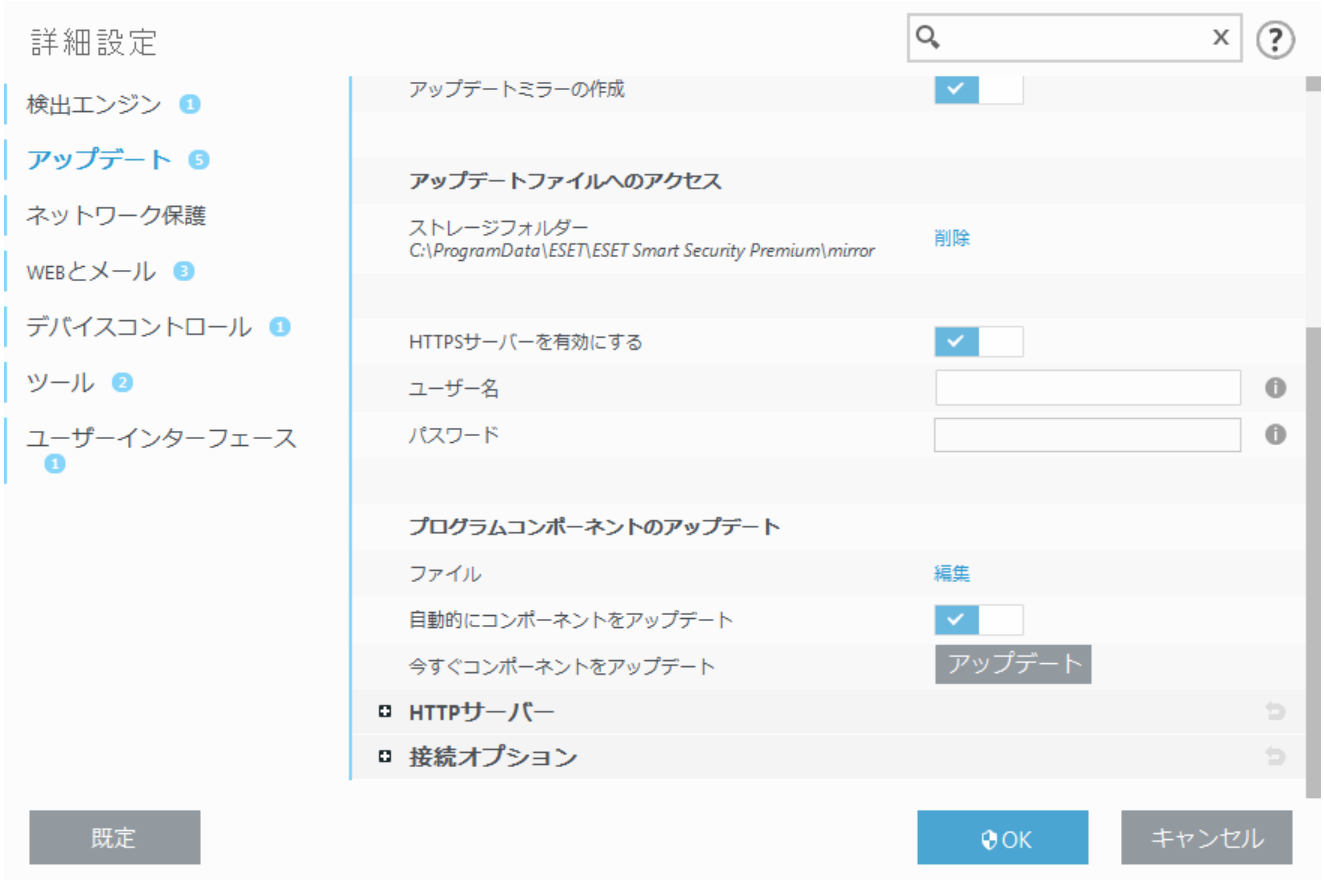
アップデートファイルのダウンロード後もサーバーとの接続がアクティブなままになる場合は、[アップデート終了後にサーバから**切断**する]を選択して強制的に切断します。

配布用アップデート

ESET Endpoint 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。

多数のクライアントを管理するためにESET PROTECTが使用されるネットワークのインターネットトラフィックを最小化するために、クライアントをミラーとして設定するのではなくApache HTTPプロキシを使用することをお勧めしますApache HTTPプロキシは、オールインワンインストーラーを使用してESET PROTECTとともにインストールするか、スタンドアロンコンポーネントとしてインストールできますApache HTTPプロキシ、ミラーツール、および直接接続の詳細と違いについては、ESET PROTECTオンラインヘルプページを参照してください。

[**アップデート**]の下の[詳細設定]フォルダで、ローカルミラーサーバーの設定オプションを使用できます。このセクションにアクセスするには、**F5**を押し、[**アップデート**] > [**プロファイル**]をクリックし、[**アップデートミラー**]タブを選択します。



クライアントワークステーションでミラーを作成するには、**[アップデートミラーを作成]**を有効にします。このチェックボックスをチェックすると、アップデートファイルへのアクセス方法やミラー化されたファイルへのパスなど、他のミラー設定オプションがアクティブになります。

アップデートファイルへのアクセス

HTTPサーバーを有効にする – このチェックボックスをチェックすると、HTTP経由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。認証情報は必要ありません。

ミラーサーバーへのアクセス方法の詳細については、「ミラーからのアップデート」を参照してください。ミラーにアクセスする基本的な方法は2つあります。アップデートファイルを含むフォルダが共有ネットワークフォルダとして表示するか、クライアントがHTTPサーバー上にあるミラーにアクセスする方法です。

ミラーのアップデートファイルを保存するために使用するフォルダーは、[**ストレージフォルダ**]で定義します。別のフォルダーを選択するには、**[クリア]**をクリックして、定義済みフォルダーの*C:\ProgramData\ESET\ESET Endpoint Security\mirror*を削除し、**[編集]**をクリックして、ローカルフォルダ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、<ドメイン>/<ユーザー>または<ワークグループ>/<ユーザー>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。プログラムコンポーネントのアップデートファイルをインストールした後、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。

ミラーのHTTPサーバーとSSL

ミラータブの**HTTPサーバー**セクションで、HTTPサーバーがリスニングする**サーバーポート**、およびHTTPサーバーで使用される**認証**のタイプを指定できます。既定では、サーバーポートは**2221**に設定されています。

[**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**]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。

> **ユーザー名**と**パスワード**が必要な場合のみ入力してください。ミラーHTTPサーバーへのアクセスにのみ使用されます。

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ASNPEMPFX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**オプションは、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。

> **HTTPSミラーの自己署名証明書**
> HTTPSミラーサーバーを使用している場合は、その証明書をすべてのクライアントコンピューターの信頼できるルートストアにインポートする必要がありますWindowsでの信頼できるルート証明書のインストールを参照してください。

ミラーからのアップデート

ミラーを構成するには、2つの基本方法があります。ミラーは、基本的に、クライアントがアップデートファイルをダウンロードできるリポジトリです。アップデートファイルがあるフォルダは、共有ネットワークフォルダまたはHTTPサーバーとして表示されます。

内蔵のHTTPサーバーを使用したミラーへのアクセス

これは、事前定義されたプログラム設定で指定される、既定の設定ですHTTPサーバを使用してミラーにアクセスできるようにするには、[**詳細設定**] > [**アップデート**]> [**プロファイル**]> [**アップデートミラー**]タブ)に移動して、[**更新ミラーの作成**]オプションを選択します。

ミラータブの**HTTPサーバー**セクションで、HTTPサーバーがリスニングする**サーバーポート**、およびHTTPサーバーで使用される**認証**のタイプを指定できます。既定では、サーバーポートは**2221**に設定されてい

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**]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。

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 Endpoint 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。

ミラーからのアップデートが数回失敗すると、メインメニューの[アップデート]ペインに、**無効なユーザー名またはパスワード**エラーが表示されます。**詳細設定>アップデート>プロファイル > アップデートミラー**に移動し、ユーザー名とパスワードを確認することをお勧めします。このエラーの最も一般的な原因は、入力した認証データが正しくないことです。

ミラーサーバーの設定後、クライアントワークステーション上に新しいアップデートサーバーを追加する必要があります。手順は次のとおりです。

- **詳細設定**(F5) を開き、**アップデート > プロファイル > アップデート > モジュールのアップデート**をクリックします。
- **自動選択**をオフにし、次のいずれかの形式で、**アップデートサーバー**フィールドに新しいサーバーを追加します。
  http://<サーバの*IP*アドレス>:2221
  https://<サーバーの*IP*アドレス>:2221 (SSLを使用する場合)

システム共有を使用したミラーへのアクセス

まず、ローカルデバイスまたはネットワークデバイスに共有フォルダーを作成する必要があります。ミラーのフォルダーを作成する際には、フォルダーにアップデートファイルを保存するユーザーに"書き込み"アクセス権を与え、ミラーフォルダーからESET Endpoint Securityをアップデートするすべてのユーザーに"読み取り"アクセス権を与える必要があります。

次に、**詳細設定 > アップデート > プロファイル > アップデートミラー**タブで、**HTTPサーバーを有効にする**チェックボックスのチェックを外して、ミラーへのアクセスを設定します。プログラムのインストールパッケージでは、このチェックボックスは既定でチェックされています。

共有フォルダーがネットワーク内の別のコンピューターにある場合は、そのコンピューターへのアクセスに使用する認証データを入力する必要があります。認証データを入力するには⍰ESET Endpoint Security **の詳細設定**(F5)を開いて、**アップデート > プロファイル > アップデートミラー > 接続オプション > アップデートサーバ接続アカウントの設定** をクリックします。この設定は、「アップデートサーバーへの接続に使用するユーザーアカウント」セクションで説明されているアップデートの設定と同じです。

ミラーフォルダにアクセスするには、ミラーが作成されたコンピュータにログインするために使用されたアカウントでこの操作を実行する必要があります。コンピュータがドメインの場合、「ドメイン\ユーザー」ユーザー名を使用してください。コンピュータがドメインにない場合は、「サーバーのIPアドレス\ユーザー」または「ホスト名\ユーザー」を使用してください。

ミラーの設定が完了したら、次の手順で、クライアントワークステーションで、アップデートサーバーとして*\\UNC\PATH*を設定します。

1.[ESET Endpoint Security**詳細設定**]を開き、[**アップデート**]>[**プロファイル**]>[**アップデート**]をクリックします。

2.**モジュールのアップデート**の横の**自動選択**をオフにし、**アップデートサーバー**フィールドに新しいサーバーを追加します(*\\UNC\PATH*形式)。

アップデートが正しく動作するには、ミラーフォルダのパスをUNCパスとして指定する必要があります。マップされたドライブからのアップデートは動作しない場合があります。

ミラーツールを使用したミラーの作成
ミラーツールは、Endpointミラーが作成するフォルダーとは別のフォルダー構造を作成します。各フォルダーには、製品のグループのアップデートファイルが格納されます。ミラーを使用する製品のアップデート設定で、正しいフォルダーへの完全パスを指定する必要があります。
たとえば、ミラーからESET PROTECTをアップデートするには、アップデートサーバーを(HTTPサーバーのルートの場所に応じて)次のように設定します。
`http://your_server_address/mirror/eset_upd/era6`

最後のセクションでは、プログラムコンポーネント(PCU)を制御します。既定では、ダウンロードされたプログラムコンポーネントは、ローカルのミラーにコピーできるようになっています。[**プログラムコンポーネントアップデート**]が選択されている場合、ファイルが使用可能な状態になると、自動的にローカルミラーにコピーされるため、[**アップデート**]をクリックする必要はありません。プログラムコンポーネントのアップデートの詳細については、「アップデートモード」を参照してください。

ミラーアップデートの問題のトラブルシューティング

一般的に、ミラーサーバーからのアップデート中の問題は、次の1つ以上の原因が該当します。ミラーフォルダオプションの指定が正しくない、ミラーフォルダへの認証データが正しくない、ミラーからアップデートファイルのダウンロードを試行するローカルワークステーションの設定が正しくない、これらの理由の組み合わせ。以下に、ミラーからのアップデート時に発生する可能性のあるよくある問題の概要を紹介します。

ESET Endpoint Securityミラーサーバへの接続エラーが報告される – 原因として、ローカルワークステーションが更新をダウンロードするアップデートサーバー(ミラーフォルダーのネットワークパス)が正しく指定されていないことが考えられます。フォルダーを確認するにはWindowsの[**スタート**]ボタンをクリックし、[**ファイル名を指定して実行**]をクリックします。次に、フォルダー名を入力し、[**OK**]をクリックします。フォルダーの内容が表示されます。

ESET Endpoint Securityでユーザー名とパスワードが要求される – 原因として、アップデートセクションで認証データ(ユーザー名とパスワード)が正しく入力されていないことが考えられます。ユーザー名とパスワードは、プログラムが自身を更新するアップデートサーバーへのアクセスを許可するために使用されます。認証データが適切な形式で正しく入力されていることを確認してください。たとえば、<ドメイン>/<ユーザー名>または<ワークグループ>/<ユーザー名>とそれに対応するパスワードを入力します。"全てのユーザー"がミラーサーバにアクセス可能であっても、全てのユーザーがアクセスを許可されているわけではありません。"全てのユーザー"とは、全ての認証されていないユーザーを意味するのではなく、全てのドメインユーザーがフォルダにアクセスできることを意味します。つまり、"全てのユーザー"がフォルダにアクセス可能な場合でも、アップデートの設定セクションでドメインユーザー名とパスワードを入力する必要があります。

ESET Endpoint Securityミラーサーバーへの接続エラーが報告される – ミラーのHTTPサーバーへのアクセスについて定義されているポート上の通信がブロックされています。

ESET Endpoint Securityがアップデートファイルのダウンロード中にエラーを報告する – 原因として、ローカルワークステーションのアップデートファイルのダウンロード元であるアップデートサーバー(ミラーフォルダーのネットワークパス)が正しく指定されていないことが考えられます。

アップデートタスクの作成方法

アップデートを手動で開始するには、メインメニューの[**アップデート**]をクリックした後で、[**最新版のチェック**]をクリックします。

アップデートはスケジュールされたタスクとしても実行できます。スケジュールされたタスクを設定するには、[**ツール**] > [**スケジューラ**]をクリックしますESET Endpoint Securityでは、次のタスクが既定で登録されています。

- **定期的に自動アップデート**
- **ダイヤ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**

各アップデートタスクは、ユーザーのニーズに合わせて変更することができます。ユーザーは、既定のアップデートタスクとは別に、ユーザー定義の設定で新しいアップデートタスクを作成することができます。アップデートタスクの作成と設定の詳細については、「スケジューラ」を参照してください。

ツール

[**ツール**]メニューには、プログラム管理を容易にし、また上級ユーザー向けの追加オプションを備えたモジュールが用意されています。

このメニューには、次のツールが含まれています。

- ログファイル
- セキュリティレポート(管理されていないエンドポイントの場合)
- 実行中のプロセス (ESET Endpoint SecurityでESET LiveGrid®が有効になっている場合)
- アクティビティの確認
- スケジューラ
- ネットワーク接続 (ファイアウォール が有効にされている場合 ESET Endpoint Security)
- 安全なブラウザー(既定ではESET Endpoint Securityで無効)
- ESET SysInspector
- ESET SysRescue Live- ESET SysRescue Live Webサイトに移動します。ここではMicrosoft Windowsオペレーティングシステム用のESET SysRescue Live.isoCD/DVD画像をダウンロードできます。
- 隔離
- 分析のためにサンプルを提出 – 分析のため、不審なファイルをESET研究所に提出できます(ESET LiveGrid®の構成によっては使用できない場合があります)。



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、検出されたウイルス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 Endpoint Securityから直接テキストメッセージとログを表示できます。ログファイルのアーカイブもできます。

ログファイルにアクセスするには、メインプログラムウィンドウで[**ツール**] > [**ログファイル**]をクリックします。[**ログ**]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。使用可能なログは次のとおりです。

- **検出** – このログにはESET Endpoint Securityにより検知された検出と侵入についての詳細情報が記録されています。 ログ情報には、検出時刻、検出の名前、場所、実行されたアクション、マルウェア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。 ログエントリー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。駆除されていない侵入は、常に、明るい赤色の背景に赤色のテキストで表示されます。駆除された侵入は、白色の背景に黄色のテキストで表示されます。駆除されていないPUAまたは安全でない可能性があるアプリケーションは、白色の背景に黄色のテキストで表示されます。

- **イベント** – イベントログにはESET Endpoint 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、ここで見つかる情報は、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

ンピューター制御に対応します。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。

• **ブロックされたファイル** – ESET Enterprise Inspectorに接続したときに、ブロックされ、アクセスできなかったファイルのレコードを含みます。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。詳細については、ESET Enterprise Inspectorオンラインユーザーガイドを参照してください。

• **送信されたファイル** - ESET LiveGrid®またはESET Dynamic Threat Defenseに分析のために送信されたファイルのレコード。

• **監査ログ** – 各ログには、変更が実行された日時、変更のタイプ、説明、ソース、およびユーザーの情報が含まれます。詳細については、監査ログを参照してください。

• **HIPS** – 記録対象としてマークされた特定のルールのレコードが示されます。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。

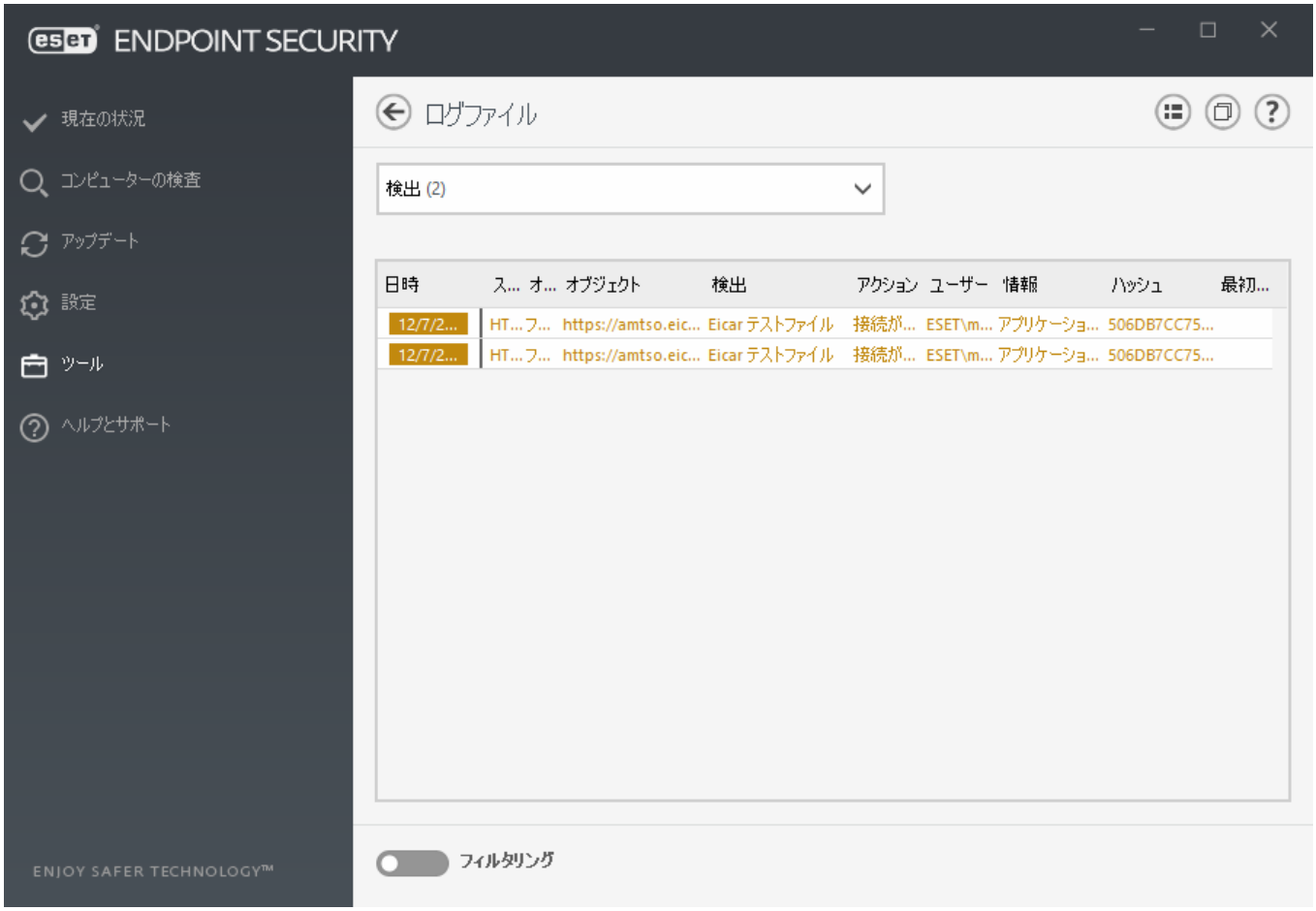
• **ネットワーク保護** – ファイアウォールログには、ネットワーク攻撃保護またはファイアウォールで検出されたすべてのリモート攻撃が表示されます。 ここでは、コンピューターに対するすべての攻撃についての情報が見つかります。[イベント]列には検出された攻撃が表示されます。[ソース]列には、攻撃者の詳細が表示されます。[プロトコル]列には、攻撃に使用された通信プロトコルが表示されます。ファイアウォールのログを解析することにより、システムへ侵入しようとする試みを検知し、不正なアクセスの防止に役立つ場合があります。特定のネットワークの攻撃の詳細については、「IDSと詳細オプション」を参照してください。

• **フィルタリングされたWebサイト** – このリストは、Webアクセス保護またはWebコントロールによってブロックされたWebサイトの一覧を表示する場合に便利です。 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。

• **迷惑メール対策機能** – 迷惑メールとマークされたメールメッセージと関連するレコードが示されます。

• **Webコントロール** – ブロックまたは許可されたURLアドレスとその分類方法の詳細が表示されます。実行したアクションの列には、フィルタリングルールがどのように適用されたかが示されます。

• **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。



ログの内容を選択し、Ctrl + C**を押してクリップボードにコピーします。**Ctrl + Shiftを押して、複数のエントリを選択できます。

フィルタリングをクリックすると、フィルタリング条件を定義することができる ログフィルタリング ウィンドウが開きます。

特定のレコードを右クリックすると、コンテキストメニューが開きます。 以下のオプションがコンテキストメニューに用意されています。

- **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。
- **同じレコードをフィルタ表示** – このフィルターをアクティブにすると、同じタイプのレコード(診断、警告、など)だけが表示されます。
- **フィルタ** – このオプションをクリックすると、ログフィルタリングウィンドウで、特定のログエントリのフィルタリング条件を定義できます。
- **フィルタを有効にする** – フィルタ設定を有効にします。
- **フィルタをクリア** – フィルターのすべての設定(上記)をクリアします。
- **コピー/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/すべて削除** – 選択されたレコードまたは表示されてい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** – レコードに関する情報をXML形式でエクスポートします。

• **すべてエクスポート** – レコードに関する情報をXML形式でエクスポートします。

• **検索/次を検索/前を検索** – このオプションをクリックした後、ログフィルタリングウィンドウで、フィルタリング条件を定義し、特定のエントリをハイライトすることができます。

• **除外の作成** – ウィザードを使用して新しい検出除外を作成します(マルウェア検出では使用できません)。

ログのフィルタリング

ツール > ログファイルで**フィルタリング**をクリックして、フィルタリング条件を定義します。

ログフィルタリング機能では、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。特定のイベントのタイプ、ステータス、期間を検索する場合などに、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す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して、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。**完全一致のみ**または**大文字と小文字を区別する**などの詳細検索オプションも使用できます。

テキスト検索

文字列(単語、特定の単語)を入力します。この文字列に含まれるレコードのみが表示されます。他のレコードは省略されます。

列を検索

検索時に考慮される列を選択します。検索で使用する列を1つ以上チェックできます。

レコードの種類

ドロップダウンメニューからログレコードの種類を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(ウイルス対策保護の開始エラー)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) – 期間で検索せず、ログ全体を検索します。
• **昨日**
• **先週**
• **先月**
• **期間** – 正確な期間(開始日と終了日)を指定して、特定の期間のレコードのみをフィルタリングできます。

完全一致のみ

より正確な結果を得るために完全一致のみで検索する場合に、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

フィルタリング時に大文字または小文字を使用することが重要な場合、このオプションを**有効**にします。フィルタリング/検索オプションを設定した後、**OK**をクリックして、フィルタリングされたログレコードを表示するか、検索で検索を開始します。ログファイルは、現在の位置(ハイライトされたレコード)から、上から下に検索されます。最初の一致するレコードが見つかると、検索が停止します。**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。

ログ設定

ESET Endpoint Securityのログの設定には、プログラムのメインウィンドウからアクセスできます。[**設定**] > [**詳細設定**] > [**ツール**] > [**ログファイル**]をクリックします。[ログ]セクションでは、ログの管理方法を定義することができます。ハード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。ログファイルの次のオプションを指定することができます。

ログに記録する最小レベル – ログに記録するイベントの最低詳細レベルを指定します。

- **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(ウイルス対策保護の開始エラー、ビルトインのファイアウォールなど)。

診断の詳細レベルを選択すると、すべてのブロックされた接続が記録されます。

[**次の日数が経過したエントリを自動的に削除**]フィールドに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。

ログファイルを自動的に最適化する – チェックすると、[**使用されていないエントリの割合が次の値よりも大きくなったら最適化**]フィールドに指定した断片化の割合を超えると、ログファイルは自動的に最適化されます。

[**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**]をオンにすると、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。

- **保存先のフォルダ** – ログファイルが保存されるディレクトリを選択します(テキスト/CSVのみ)。パスをコピーするか、[**クリア**]をクリックして別のディレクトリを選択します。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。

• **タイプ - 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)。

• **全てのログファイルを削除** - [**タイプ**]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。ログ削除の成功に関する通知が表示されます。

監査ログでの構成変更の追跡を有効にする – 各構成変更について通知します。詳細については、監査ログを参照してください。

問題をより迅速に解決できるように、コンピューター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、ESETナレッジベース記事を参照してください。

監査ログ

エンタープライズ環境では、通常、エンドポイントを設定するためのアクセス権が定義された複数のユーザーが存在します。製品設定の修正は製品の動作方法に大きく影響する可能性があるため、管理者がユーザーが行った変更を追跡し、問題をすばやく特定および解決し、詳細に同じまたは同様の問題が発生することを防止できるようにすることが重要です。

監査ログは、ESET Endpoint Securityバージョン7.1からの新しいタイプのログであり、問題の根本を特定するためのソリューションです。監査ログは、設定または保護状態の変更を追跡し、後から参照するためにスナップショットを記録します。

監査ログを表示するには、メインメニューで**ツール**をクリックしてから、**ログファイル**をクリックして、ドロップダウンメニューから**監査ログ**を選択します。

監査ログには次の情報が含まれます。

• 時間– 変更が実行された日時

• タイプ – 変更された設定または機能の種類

• 説明 – 正確な変更の内容、変更された設定の部分、および変更された設定の数

• ソース – 変更の場所

• ユーザー – 変更を行ったユーザー



ログファイルウィンドウで監査ログの**設定変更**タイプを右クリックし、コンテキストメニューから**変更を表示**を選択して、実行された変更に関する詳細情報を表示します。さらに、コンテキストメニューから**復元**をクリックすると、設定変更を復元できます(ESMCまたはESET PROTECTで管理されている製品では使用不可)。コンテキストメニューから**すべて削除**を選択すると、このアクションに関する情報のログが作成されます。

詳細設定 > **ツール** > **ログファイル**で**自動的にログファイルを最適化**を有効にする場合、監査ログは自動的に他のログとして分断されます。

詳細設定 > **ツール** > **ログファイル次の日数が経過したエントリを自動的に削除**を有効にすると、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。

スケジューラ

スケジューラーでは、スケジュールされたタスクが、あらかじめ定義された設定やプロパティと共に管理され、開始されます。

スケジューラーにはESET Endpoint Securityのメインプログラムウィンドウから[**ツール**] > [**スケジューラ**]をクリックしてアクセスできます。**スケジューラー**には、スケジュール済みのすべてのタスクと設定プロパティ(あらかじめ定義した日付、時刻、使用する検査プロファイルなど)の一覧が表示されます。

スケジューラーは次のタスクのスケジュールを行います。検出エンジンアップデート、検査タスク、システムの起動時におけるファイルの検査、およびログの保守。スケジューラーのメインウィンドウから直接、タスクの追加または削除を行うことができます(下部にある[**タスクの追加**]または[**削除**]をクリックします)。[スケジューラ]ウィンドウ内で右クリックすると、次のアクションを実行できます。詳細情報の表示、タスクの即時実行、新しいタスクの追加、および既存のタスクの削除。タスクをアクティブ/非アクティブにするには、各エントリーの最初にあるチェックボックスを使用します。

既定では、次のスケジュールされたタスクが**スケジューラ**に表示されます。

- **ログの保守**
- **定期的に自動アップデート**
- **ダイヤ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**（モジュールの正常なアップデート後）

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)の設定を編集するには、タスクを右クリックして[**編集**]をクリックするか、あるいは変更するタスクを選択して[**編集**]ボタンをクリックします。



新しいタスクの追加

1. ウィンドウの一番下にある[**タスクの追加**]をクリックします。
2. タスク名を入力します。
3. ドロップダウンメニューから目的のタスクを選択します。

- **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。

• **コンピュータの状態のスナップショットを作成する** – ドライバー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。

• **コンピュータの検査** – コンピュータ上のファイルやフォルダに関するコンピュータ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。

4. タスクを有効にする場合(スケジュールされたタスクのリストでチェックボックスをオン/オフにして後から操作できます)は、**[有効]**をオンにし、**[次へ]**をクリックして、タイミングオプションのいずれかを選択します。

• **1回** – あらかじめ定義した日時にタスクが実行されます。

• **繰り返し** – 指定した間隔でタスクが実行されます。

• **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** – 選択した曜日と時刻にタスクが実行されます。

• **イベントごと** – 指定したイベントの発生時にタスクが実行されます。

5. **[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]**を選択すると、ノートブックコンピュータのバッテリ電源での実行中に、システムリソースを最小化できます。タスクは、**[タスク実行]**フィールドで指定された日時に実行されます。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、タスクを再度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まで待機**

• **実行可能になり次第実行する**

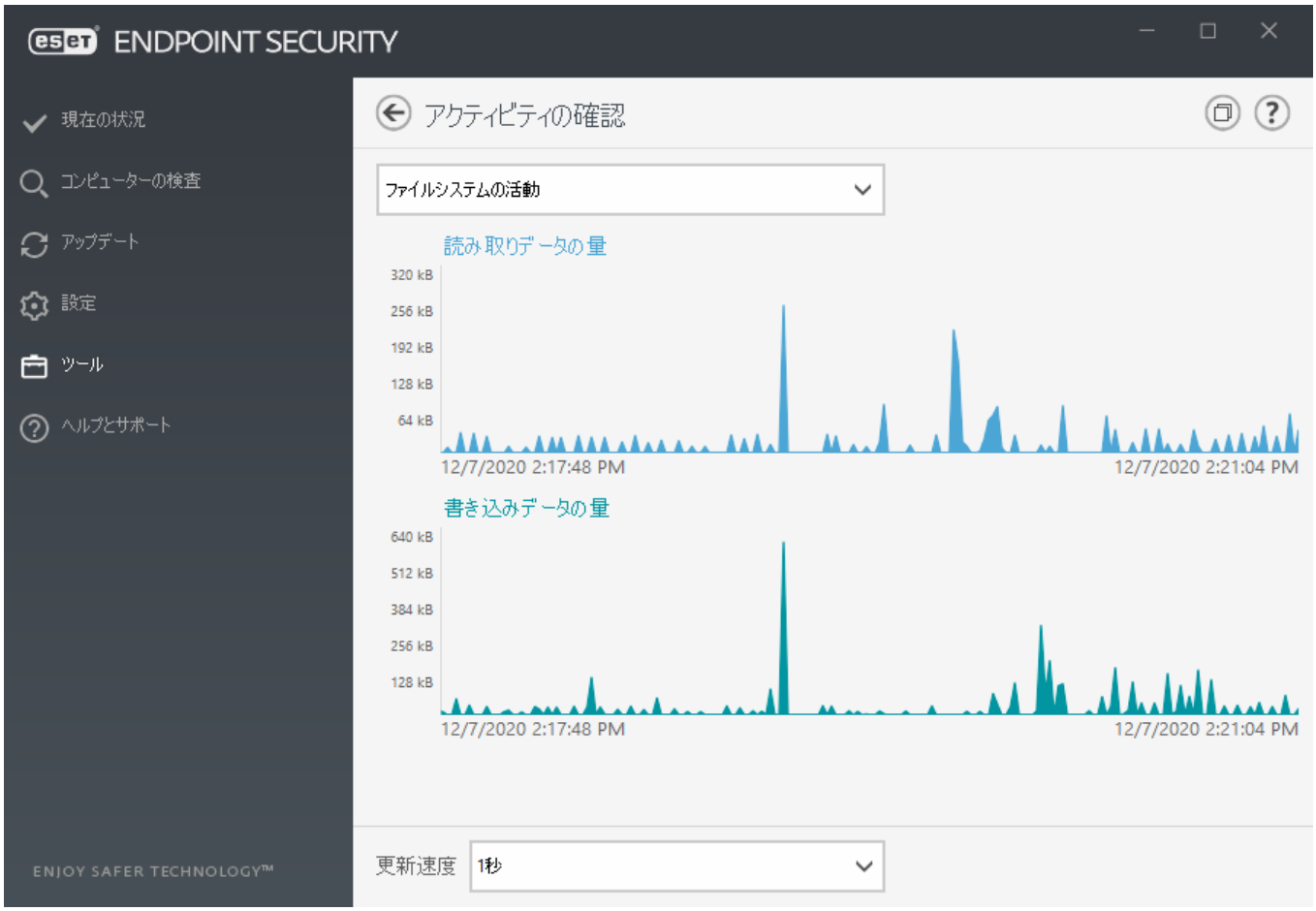
• **すぐに、前回の実行からの時間が指定した値を超えた場合は (前回実行からの時間** スクロールボックスを使用して間隔を定義できます)

[タスクの詳細を表示]を右クリックしてクリックすると、スケジュールされたタスクを確認できます。



アクティビティの確認

現在の**ファイルシステムアクティビティ**をグラフ形式で表示するには、[**ツール**] > [**アクティビティーの確認**]をクリックします。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。時間間隔を変更するには、 **リフレッシュレート** のドロップダウンメニューから選択します。



使用可能なオプションは次のとおりです。

- **ステップ: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。

- **ステップ: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。

- **ステップ: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。

- **ステップ:1時間(選択した月)** – グラフは1時間おきに更新され、時系列は選択した直近X ヶ月間を示します。

ファイルシステムの活動のグラフの縦軸は、読み込みデータ(青)と書き込みデータ(ターコイズ)の量を表します。両方の値はKB(キロバイト)/MB/GBで表されます。グラフの下の凡例の読み込みデータまたは書き込みデータの上にカーソルを置くと、そのアクティビティタイプのデータのみが表示されます。

ドロップダウンメニューから[**ネットワークアクティビティ**]を選択することもできます。[**ファイルシステムアクティビティ**]と[**ネットワークアクティビティ**]のグラフ表示およびオプションは、ネットワークアクティビティでは受信データ(青)と送信データ(ターコイズ)の量を表示することを除いて同じです。

ESET SysInspector

ESET SysInspectorは、コンピューターを徹底的に検査し、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ー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。ESET SysInspectorのオンラインユーザーガイドも参照してください

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、特定のログファイルを右クリックして、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ESET SysInspectorが完了する(ログステータスが「**作成**」として表示される)まで待機してから、ログにアクセスしてください。

- **削除** – 選択したログをリストから削除します。

次の項目は、1つ以上のログファイルが選択されたときに、コンテキストメニューから使用できます。

- **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ESET SysInspectorが完了する(ログステータスが「**作成**」として表示される)まで待機してから、ログにアクセスしてください。

- **削除** – 選択したログを削除します。
- **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。

クラウドベース保護

ESET LiveGrid®高度早期警告システム上に構築されたESETThreatSense.Netはユーザーが世界中で提出したデータを収集し、ESETのリサーチラボに送信します。 世界中の不審なサンプルとメタデータを提供することでESET LiveGrid®によって、お客様のニーズに即時に対応し、最新の脅威に対するESETの対応力を確保できます。

次の3つのオプションがあります。

オプション1:ESET LiveGrid®レピュテーション システムを有効にする

ESET LiveGrid®レピュテーションシステムは、クラウドベースのホワイトリストとブラックリストを提供します。

直接的にはこのプログラムのインタ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、実行中のプロセスやファイルの評価をチェックします。

オプション2:ESET LiveGrid®フィードバック システムを有効にする

ESET LiveGrid®レピュテーションシステムとESET LiveGrid®フィードバックシステムは、新しく検出された脅威に関連して、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 Endpoint Securityは、疑わしいファイルを詳しく解析するためにESETのウイルスラボに送信するように設定されています。*.doc*または*.xls*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。

オプション3: ESET LiveGrid®を有効にしないことを選択する

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 LiveGrid® が有効になっている場合ESET Endpoint Securityは検出エンジンアップデートよりも速く新しい脅威に対応できることがあります。

> 用語集でESET LiveGrid®を参照してください。
> ESET Endpoint SecurityでESET LiveGrid®を有効または無効にする方法については、英語および他の複数の言語で提供されている図解手順を参照してください。

詳細設定でクラウドベース保護を設定する

ESET LiveGrid®設定にアクセスするには、**F5**を押して、詳細設定に移動し、**検出エンジン > クラウドベースの保護**を展開します。

ESET LiveGrid®評価システムを有効にする(推奨) - ESET LiveGrid®評価システムは、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。

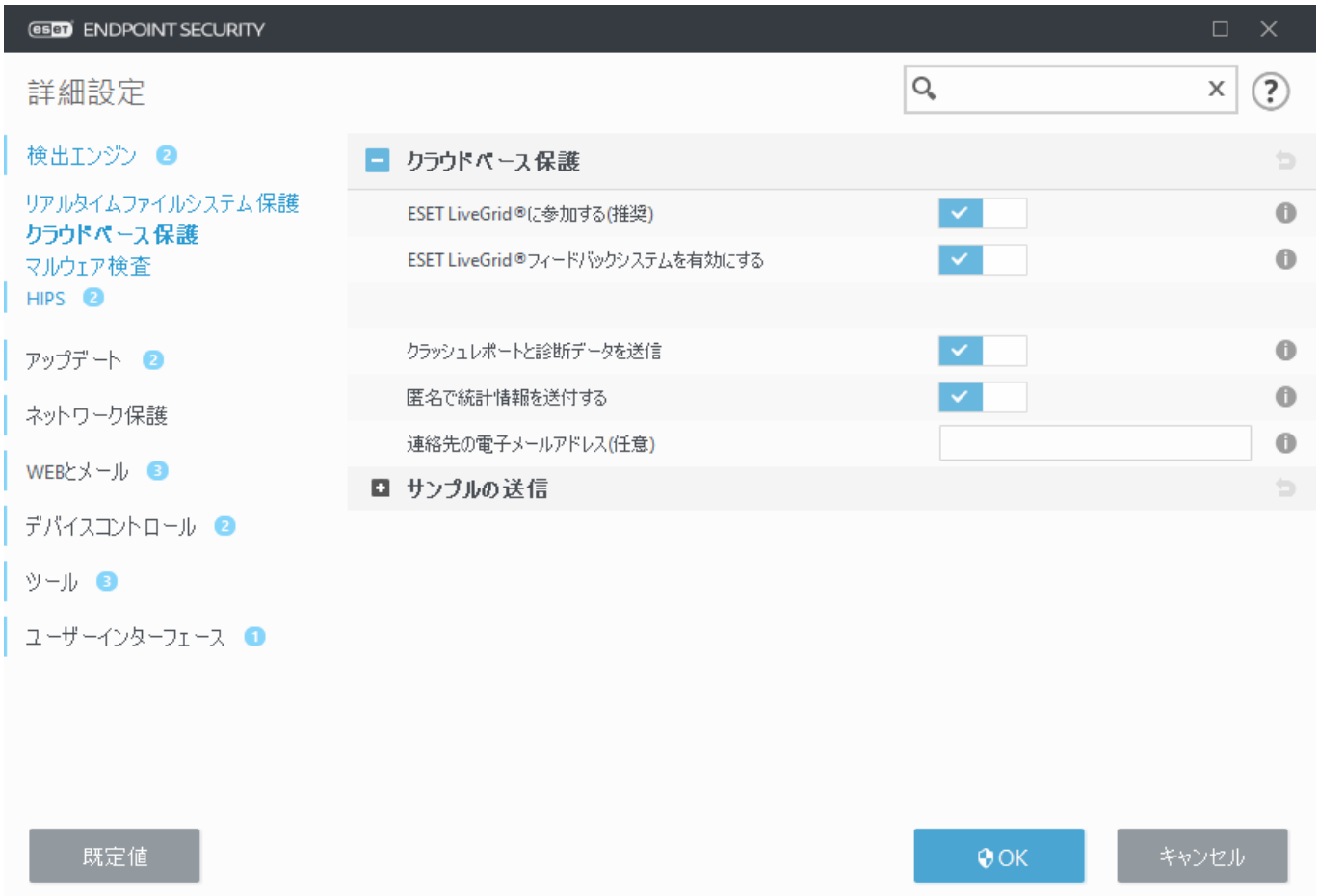
ESET LiveGrid®フィードバックシステムを有効にする – 関連する送信データ(以下の**サンプルの送信**セクションを参照)、クラッシュレポート、統計情報をさらに分析するためESET研究所に送信します。

ESET Dynamic Threat Defenseを有効にする(ESET Endpoint Securityで表示されない) – ESET Dynamic Threat DefenseはESET が提供する有料サービスです。その目的は、発生中の新しい脅威を軽減するために特別に設計された保護層を追加することです。不審なファイルは自動的にESETクラウドに送信されます。クラウドでは、脅威が高度なマルウェア検出エンジンによって分析されます。サンプルを提供したユーザーは、観察されたサンプルの動作の概要を示す動作レポートを受け取ります。

クラッシュレポートと診断データを送信する – クラッシュレポートやモジュールメモリダンプなどのESET LiveGrid®関連の診断データを送信します。このオプションを有効にしESETによる問題の診断、製品の改善、確実なエンドユーザー保護の強化を支援することをお勧めします

匿名の統計情報を送信 – 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に関する情報をESETが収集することを許可します。

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

サンプルの手動送信 – このオプションを有効にすると、コンテキストメニューの隔離またはツール > 分析にサンプルを送信から手動でサンプルをESETに送信します。

検出され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、ESETに送信されるサンプルの種類を選択します。次のオプションを使用できます。

- **すべての検出されたサンプル** – 検出エンジンによって検出されたすべての検出されたオブジェクト(スキャナー設定で有効になっている場合は望ましくない可能性のあるアプリケーションを含む)。
- **文書を除くすべてのサンプル** – **文書**を除くすべての検出されたオブジェクト(以下を参照)。
- **送信しない** – 検出されたオブジェクトはESETに送信されません。

不審なサンプルの自動送信

検出エンジンで検出されなかった場合にも、これらのサンプルがESETに送信されます。たとえば、検出されなかったサンプルや、ESET Endpoint Security保護モジュールのいずれかが不審であると見なしたサンプル、不明瞭な動作のサンプルなどです。

- **実行ファイル** - .exe, .dll, .sysなどのファイルが含まれます。
- **アーカイブ** - .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cabなどのファイルタイプが含まれます。
- **スクリプト** - .bat, .cmd, .hta, .js, .vbs, .ps1などのファイルタイプが含まれます。
- **その他** - .jar, .reg, .msi, .sfw, .lnkなどのファイルタイプを含みます。
- **考えられる迷惑メール** – これにより、詳細な分析のため、添付ファイル付きの迷惑メールの可能性があるメールの一部または全部をESETに送信できます。このオプションを有効にすると、将来の迷惑メール検出の改良などの迷惑メールのグローバル検出が改善されます。
- **文書** – アクティブなコンテンツの有無に関係なくMicrosoft OfficeまたはPDF文書が含まれます。

すべての含まれる文書ファイルタイプの一覧を展開する

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

除外

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なことがあります)。 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、除外するファイルは追加できます。

download.domain.comからダウンロードされたファイルを除外するには、**詳細設定 > クラウドベース保護 > サンプル除外の送信 > 除外**に移動して、.download.domain.comの除外を追加します。

ESET Dynamic Threat Defense

ESET Dynamic Threat Defense Webコンソールを使用してクライアントコンピューターでESET PROTECTサービスを有効にするにはESET Endpoint SecurityのEDTD構成を参照してください。

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。

クラウドベース保護の除外フィルター

除外フィルターを使用すると、特定のファイルやフォルダーをサンプル提出から除外することができます。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。既定では、一般的なファイルタイプ(.docなど)が除外されます。

ドキュメントやスプレッドシートなど、機密情報が含まれているファイルを除外すると便利です。

download.domain.comからダウンロードされたファイルを除外するには、**詳細設定** > **クラウドベース保護** > **サンプル除外の送信** > **除外**に移動して、.download.domain.comの除外を追加します。

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、新規のウイルスを即座にESETに通知し、その通知を継続しますESET Endpoint 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。



レピュテーション – 多くの場合ESET Endpoint SecurityおよびESET LiveGrid®技術では、各オブジェクトの特性を検証して悪意のあるアクティビティである可能性に重み付け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(ファイル、プロセス、レジストリキーなど)に危険レベルが割り当てられます。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9 – 良好(緑)0 – 危険(赤)のリスク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

> 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。

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。

初回発見日 - ESET LiveGrid®技術によってアプリケーションが検出された日付。

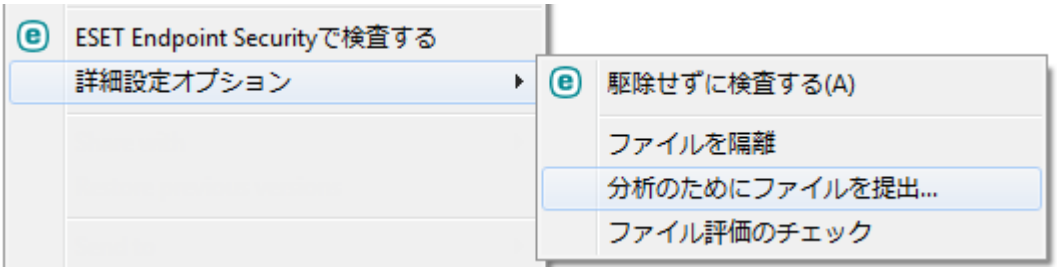
アプリケーションが不明(オレンジ)のセキュリティレベルのマークを付けられていても、必ずしも悪意のあるソフトウェアというわけではありません。通常は、単に新しいアプリケーションというだけです。ファイルについて不明点がある場合は、分析のためにファイルを提出機能を使用してESETのウイルスラボにファイルを送信できます。そのファイルが悪意のあるアプリケーションであることが判明すると、それ以降のいずれかの検出エンジンアップデートファイルにその検出が追加されます。

アプリケーション名 – プログラムまたはプロセスの特定の名前。

下部の特定のアプリケーションをクリックすることにより、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。

評価は、実行中のプログラム/プロセスとして動作しないファイルに対してもチェックできます – チェックするファイルをマークして右クリックし、コンテキストメニューから[**詳細オプション**] > [**ESET LiveGrid®を使用したファイル評価のチェック**]を選択します。



セキュリティレポート

この機能は、次のカテゴリの統計情報の概要を示します。

ブロックされたWebページ – ブロックされたWebページ数を表示します(PUA、フィッシング、ハッキングされたルータ、IPまたは証明書のブラックリストに登録されたURL)。

検出された感染した電子メールオブジェクト – 検出された感染した電子メールオブジェクト数を表示します。

Webコントロールでブロックされた Webページ - Webコントロールでブロックされた Webページ数を表示します。

検出されたPUA – 検出された望ましくない可能性のあるアプリケーション(PUA)数を表示します。

検出された迷惑メール – 検出された迷惑メール数を表示します。

チェックされた文書 – 検査された文書オブジェクト数を表示します。

検査されたアプリケーション – 検査された実行可能なオブジェクト数を表示します。

検査された他のオブジェクト – 他の検査されたオブジェクト数を表示します。

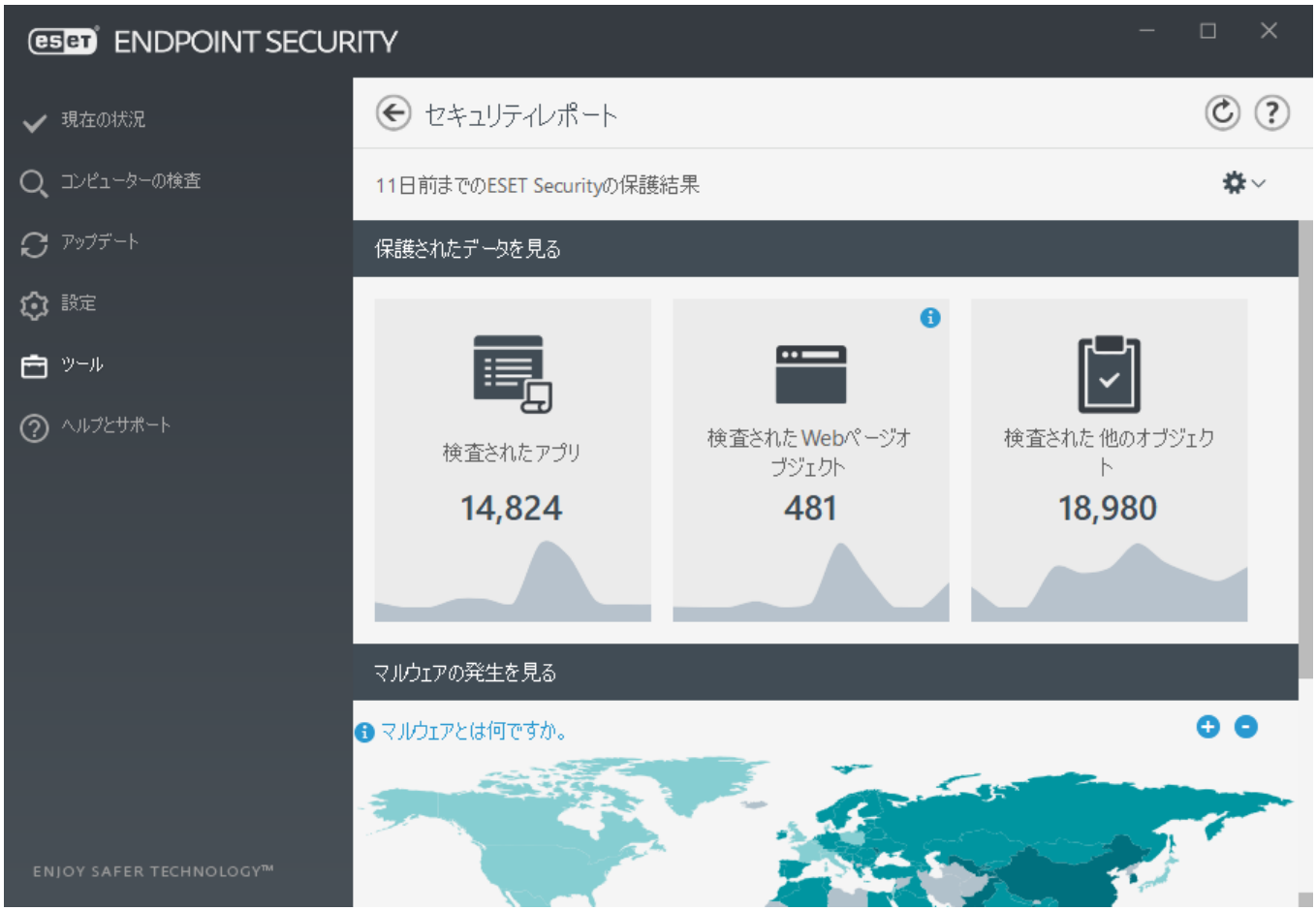
検査されたWebページオブジェクト – 検査されたWebページオブジェクト数を表示します。

検査された電子メールオブジェクト – 検査された電子メールオブジェクト数を表示します。

これらのカテゴリは、降順の数値に基づいています。ゼロ値のカテゴリは表示されません。**[詳細]**をクリックすると、非表示のカテゴリを展開して表示します。

カテゴリの下には、実際のウイルス状況と世界地図が表示されます。各国のウイルスの存在は色で示されます(色が濃いほど、数が多いことを示します)。データがない国は灰色で表示されます。国の上にマウスカーソルを置くと、選択した国のデータが表示されます。特定の大陸を選択すると、自動的に拡大されます。

右上端で歯車をクリックすると、**セキュリティレポート通知を有効/無効にする**か、過去30日間のデータが表示されるか、製品がアクティベーションされた時点以降のデータが表示されるかどうかを選択します。ESET Endpoint Securityのインストール期間が30日未満の場合、インストール日数のみを選択できます。30日間の期間は既定で設定されます。



データのリセットは、すべての統計情報をクリアし、セキュリティレポートの既存のデータを削除します。**詳細設定 > ユーザーインターフェース > アラートとメッセージボックス > 確認メッセージ**で**統計情**

報をリセットする前に確認するオプションをオフにした場合を除き、このアクションを確認する必要があります。

ネットワーク接続

[ネットワーク接続]セクションには、アクティブな接続と保留中の接続のリストが表示されます。このリストは、発信接続を確立しているすべてのアプリケーションを管理するために有用です。



最初の行には、アプリケーションの名前とデータ転送速度が表示されます。アプリケーションによって確立されている接続のリスト(および詳細情報)を表示するには、[+]をクリックします。

列

アプリケーション/ローカルIP – アプリケーションの名前、ローカルIPアドレス、および通信ポート。

リモートIP – 特定のリモートコンピューターのIPアドレスとポート番号。

プロトコル – 使用されている転送プロトコル。

上り速度/下り速度 – 送信データおよび受信データの現在の速度。

送信/受信 – 接続内で交換されるデータの量。

詳細を表示 – このオプションを選択すると、選択した接続に関する詳細情報が表示されます。

ネットワーク接続画面でアプリケーションまたはIPアドレスを選択し、右クリックすると、次の構造でコンテキストメニューが表示されます。

ホスト名を解決 – 可能な場合、全てのネットワークアドレスが、数字によるIPアドレス形式ではな

くDNS形式で表示されます。

TCP接続のみを表示する – リストにはTCPプロトコルスイートに属する接続のみが表示されます。

リスニング接続を表示する – このオプションを選択すると、現時点では通信が確立されていない接続のうち、システムがポートを開いており、接続を待機しているもののみが表示されます。

コンピュータ内部の接続を表示する – このオプションを選択すると、リモート側がローカルシステム(つまり、ローカルホスト)の接続のみが表示されます。

次の追加オプションを表示するには、接続を右クリックします。

指定した接続の通信を拒否 – 確立した通信を切断します。このオプションは、アクティブな接続をクリックしないと使用できません。

更新間隔 – アクティブな接続を更新する頻度を選択します。

最新の情報に更新 – [ネットワーク接続]ウィンドウを読み込み直します。

以下のオプションは、アクティブな接続ではなく、アプリケーションまたはプロセスをクリックしないと使用できません。

指定したプロセスの通信を一時的に拒否 – 指定したアプリケーションの現在の接続を拒否します。新しい接続が確立される場合、ファイアウォールではあらかじめ定義されたルールが使用されます。設定の説明は、[ルールとゾーン]セクションで参照することができます。

指定したプロセスの通信を一時的に許可 – 指定したアプリケーションの現在の接続を許可します。新しい接続が確立される場合、ファイアウォールではあらかじめ定義されたルールが使用されます。設定の説明は、[ルールとゾーン]セクションで参照することができます。

ESET SysRescue Live

ESET SysRescue Liveは無料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。感染したコンピューターをレスキューメディアから起動し、マルウェアを検査して、感染したファイルを駆除できます。

ESET SysRescue Liveの主な利点は、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)通常の動作状況では削除できない脅威に効果を発揮します。

- ESET SysRescue Liveのオンラインヘルプ

分析用サンプルの提出

コンピューター上の疑わしいファイル、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のリサーチラボに提出して解析を受けることができます(ESET LiveGrid®の構成によっては使用できない場合があります)。

次の条件の1つ以上を満たさないかぎり、サンプルを送信しないでください。
- このサンプルがESET製品でまったく検出されない
- サンプルが誤ってウイルスとして検出される
- (ESETでのマルウェア検査を希望する)個人のファイルはサンプルとして許可されません(ESETリサーチラボはユーザーのオンデマンド検査を実行しません)
- わかりやすい件名にし、ファイルに関する情報(ダウンロード元のスクリーンショットやWebサイトなど)をできるだけ多く記載してください。

サンプル送信では、次の方法のいずれかを使用して、分析のためにファイルまたはサイトをESETに送信できます。

1. サンプル送信の使用は、**ツール > 分析のためにサンプルを提出**にあります。

2. また、メールでファイルを提出することもできます。この方法を希望する場合は、WinRAR/ZIPを使用してファイルを圧縮し、アーカイブを"infected"というパスワードで保護し、samples@eset.comに送信してください。

3. 迷惑メールまたは迷惑メールの誤検出、またはWebコントロールモジュールによって誤って分類されたWebサイトを報告するにはESETナレッジベース記事を参照してください。

分析のためのサンプルを選択を開き、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(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。

連絡先のメールアドレス – 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。**匿名で送信**を選択すると、空欄になります。

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。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。
サンプ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ESETアップデートファイルにその検出が追加されます。

分析のためにサンプルを提出 – 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。

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。

分析のためにサンプルを提出 – 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。

- [**感染している**] – 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**] – 簡単にお金を手に入れることを主な目的とした、詐欺または偽装Webサイト。
- 送信するサイトに上記のオプションが該当しない場合は、[**その他**]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。

分析のためにサンプルを提出 – 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、ウイルス対策およびフィッシング対策の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。

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、不審なファイルを処理する際に役立つ追加情報または説明を入力できます。

> 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。

分析のためにサンプルを提出 – 誤検出サイト

感染、詐欺、またはフィッシングと検出され、実際には感染していないサイトは、送信してくださるようお願いします。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。ウイルス対策およびフィッシング対策の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Webサイトを処理する際に役立つ追加情報または説明を入力できます。

分析のためにサンプルを提出 – 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。

ファイルの送信理由 – 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。

通知

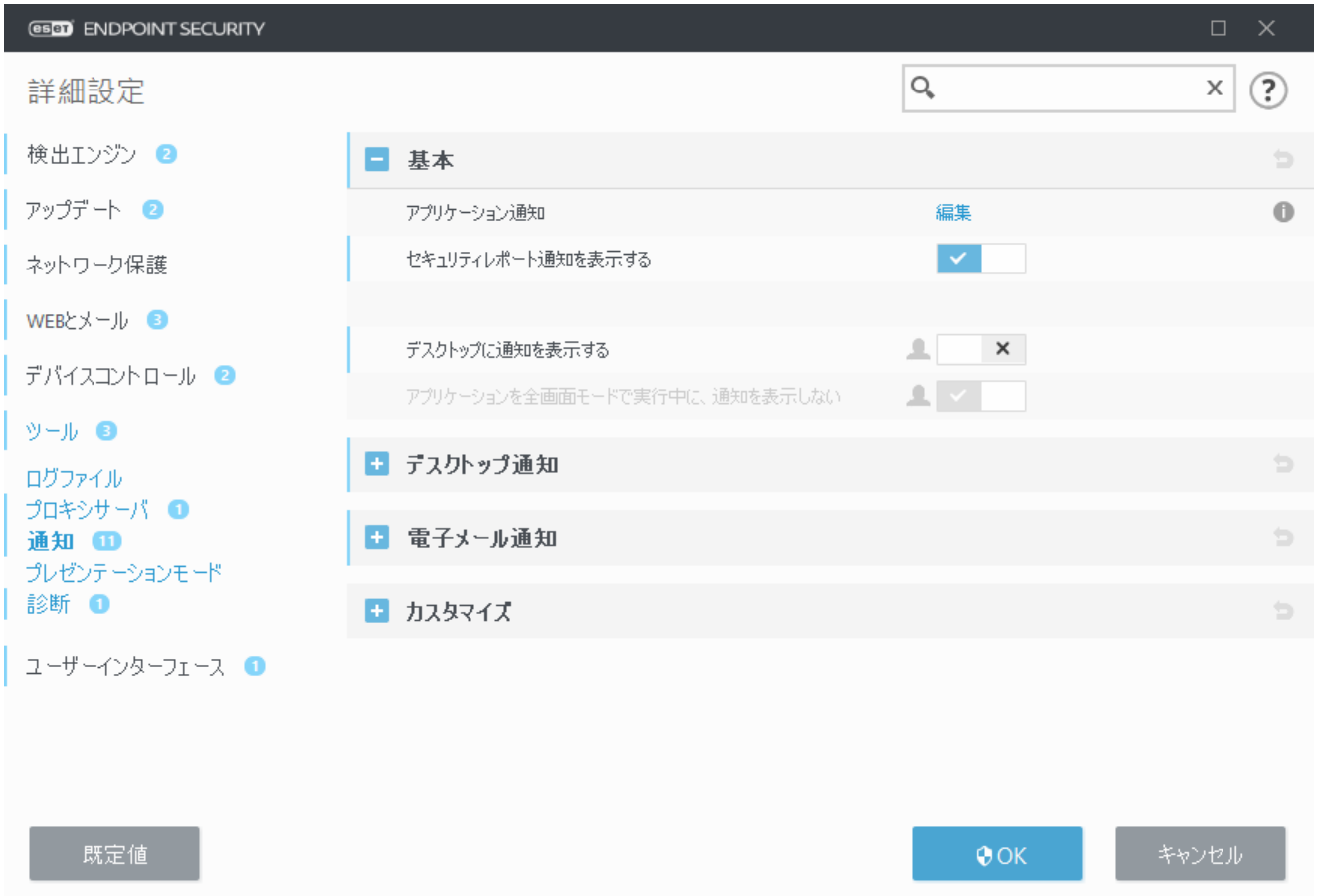
ESET Endpoint Securityがイベントをユーザーに通知する方法を管理するには、**詳細設定**(F5) > **ツール** > **通知**に移動します。この設定ウィンドウでは、次のタイプの通知を設定できます。

- アプリケーション通知 - プログラムのメインウィンドウに直接表示されます。
- デスクトップ通知 – システムタスクバーの横の小さいポップアップウィンドウとして表示されるデスクトップ通知。
- 電子メール通知 - 電子メール通知は指定された電子メールアドレスに送信されます。
- 通知のカスタマイズ – デスクトップ通知などにカスタム通知を追加します。

基本セクションで、対応するスイッチを使用して、次の項目を調整します。

スイッチ	既定値	説明
デスクトップに通知を表示する	✓	無効にすると、システムタスクバーの横のポップアップ通知を非表示にします。このオプションは有効にし、新しいイベントが発生したときに製品が通知を発行できるようにすることをお勧めします。
...のときに通知を表示しない	✓	**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**を有効にすると、すべての非インタラクティブ通知を抑制します。
セキュリティレポート通知を表示する	×	有効にすると、新しいバージョンのセキュリティレポートが生成されたときに通知を表示します(ESET Security Management Centerで管理されていない場合にのみ使用可能)。
成功したアップデートに関する通知を表示する	×	有効にすると、製品がコンポーネントと検出エンジンモジュールをアップデートするときに通知を表示します。
イベント通知をメールで送信する	×	有効にすると、電子メール通知を有効にします。

特定のアプリケーション通知を有効または無効にするには、**アプリケーション通知**の横の**編集**をクリックします。



アプリケーション通知

アプリケーション通知(画面右下に表示)の表示を調整するにはESET Endpoint Security詳細設定ツリーの**ツール > 通知 > 基本 > アプリケーション通知**に移動します。

通知のリストは3つの列に分割されます。通知名は最初の列にカテゴリ別で並べ替えられます。製品が新しいアプリケーションイベントを通知する方法を変更するには、対応する列の**デスクトップに表示**および**電子メールで送信**のチェックボックスをオンにします。



メッセージが表示される時間や、表示するイベントの詳細レベルといったデスクトップ通知の一般設定を設定するには、**詳細設定 > ツール > 通知**のデスクトップ通知を参照してください。

メッセージ形式を設定し、SMTPサーバー設定を設定するには、**詳細設定 > ツール > 通知**の電子メール通知を参照してください。

ESET Dynamic Threat Defenseの使用中に**ファイルが分析されました**および**ファイルが分析されていません**通知を設定する場合は、プロアクティブ保護を**分析結果を受信するまで実行をブロックする**に設定する必要があります。

デスクトップ通知

デスクトップ通知はシステムタスクバーの横の小さいポップアップウィンドウで表示されます。既定では、10秒間表示され、ゆっくりと消えるように設定されています。これはESET Endpoint Securityが製品のアップデートの成功、新しい接続されたデバイス、ウイルス検査タスクの完了、または新しい脅威の検出についてユーザーに通知する主な手段です。

デスクトップ通知セクションでは、ポップアップ通知の動作をカスタマイズできます。次の属性を設定できます。

期間 - 通知メッセージが表示される期間を設定します。値は3～30秒でなければなりません。

透明度 - 通知メッセージの透明度を割合で設定します。サポートされている範囲は0（透明ではない）から80（非常に高い透明度）です。

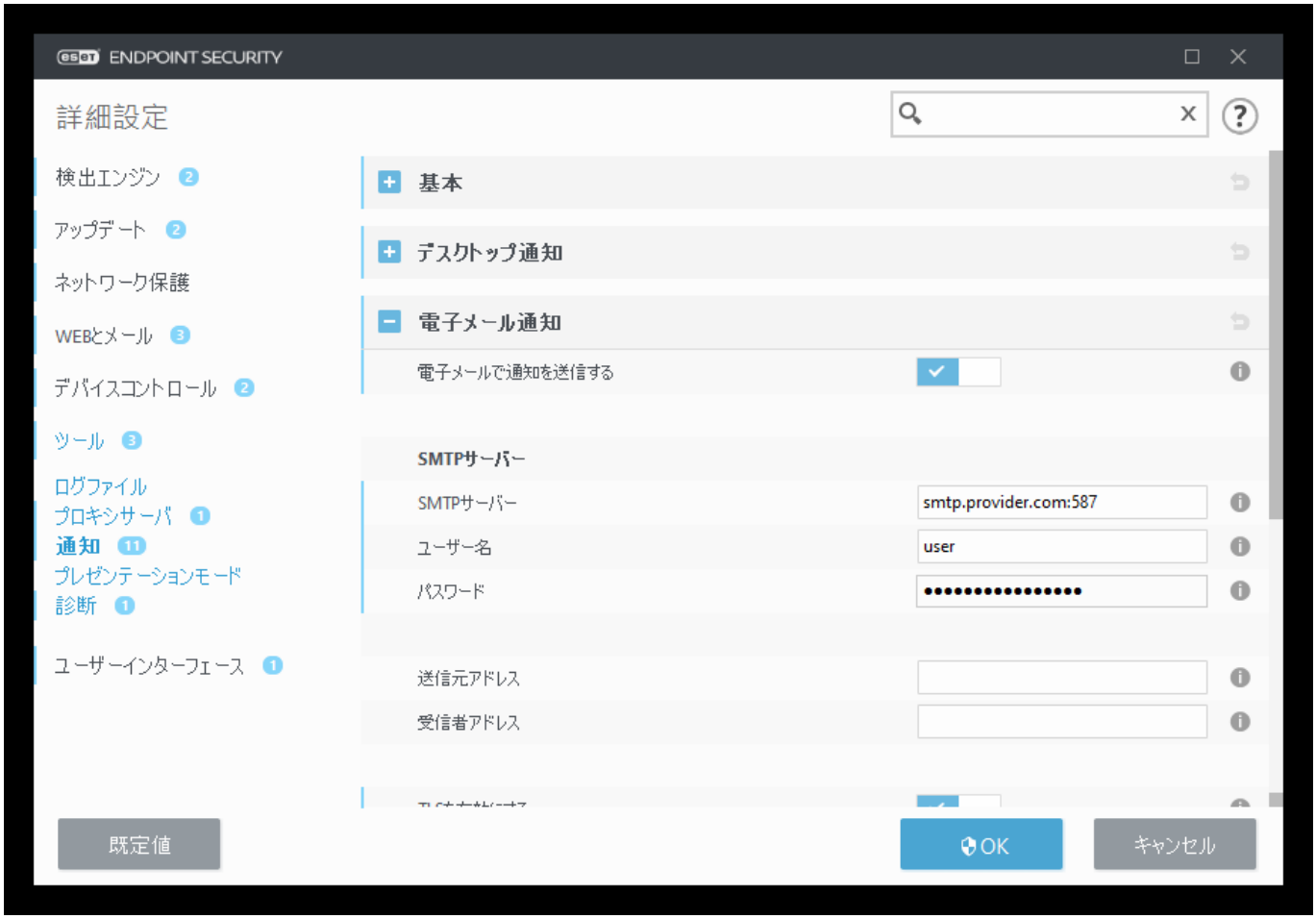
表示イベントの最低詳細レベル - ドロップダウンメニューから、表示する通知の最低重要度を選択できます。

- **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** - 標準以外のネットワークイベントなどの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**- 重大なエラーと警告メッセージを記録します（アンチステルスが正しく実行されていないか、アップデートが失敗しました）。
- **エラー** - エラー（ドキュメント保護が起動していません）や重大なエラーを記録します。
- **重大** - 重大なエラー（ウイルス対策保護の開始エラーや感染したシステム）のみを記録します。

マルチユーザーシステムで、このユーザーの画面に通知を表示する - デスクトップ通知を受信できるユーザーの完全なアカウント名を入力します。たとえば、管理者アカウント以外を使用してコンピューターを使用し、新しい製品イベントの通知を受信し続けたい場合などです。

電子メール通知

ESET Endpoint 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。基本セクションで、**[電子メールで通知を送信する]**をオンにして、電子メール通知を有効にします。



SMTPサーバー

SMTPサーバー – 通知を送信するために使用されるSMTPサーバー(例:*smtp.provider.com:587*、事前定義されたポートは25)。

TLS暗号化機能を備えたSMTPサーバーは、ESET Endpoint Securityでサポートされます。

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。

送信者アドレス – 通知メールのヘッダーに表示される送信者アドレスをこのフィールドに指定します。

受信者アドレス – 通知メールのヘッダーに表示される受信者アドレスをこのフィールドに指定します。セミコロン「;」を使用して、複数の電子メールアドレスを区切ります。

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の送信を有効にします。

電子メール設定

[**通知の最低レベル**]ドロップダウンメニューで、送信する通知の開始重要度を選択できます。

- **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** – 標準以外のネットワークイベントなどの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**– 重大なエラーと警告メッセージを記録します(アンチステルスが正しく実行されていないか、アップデートが失敗しました)。

- **エラー** – エラー(ドキュメント保護が起動していません)や重大なエラーを記録します。
- **重大** – 重大なエラー(ウイルス対策保護の開始エラーや感染したシステム)のみを記録します。

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。

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)。この値を0に設定すると、通知がただちに送信されます。

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。

文字セット – Windows地域設定(windows-1250Unicode (UTF-8)ACSII 7-bit日本語(ISO-2022-JP)など)に基づいて、電子メールメッセージをANSI文字エンコーディングに変換します。結果として"á"は˝a"に変換され、不明な記号は˝?˝に変換されます。

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。

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
- **%Action%** – 侵入に対する処理
- **%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。

通知のカスタマイズ

このウィンドウでは、通知で使用されるメッセージをカスタマイズできます。

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。

検出

[検出通知を自動的に閉じない]を有効にすると、手動で閉じるまでマルウェア通知が画面に表示されます。

既定の通知メッセージを無効にし、**検出の通知メッセージ**フィールドに独自のメッセージを入力すると、カスタム通知メッセージが使用されます。

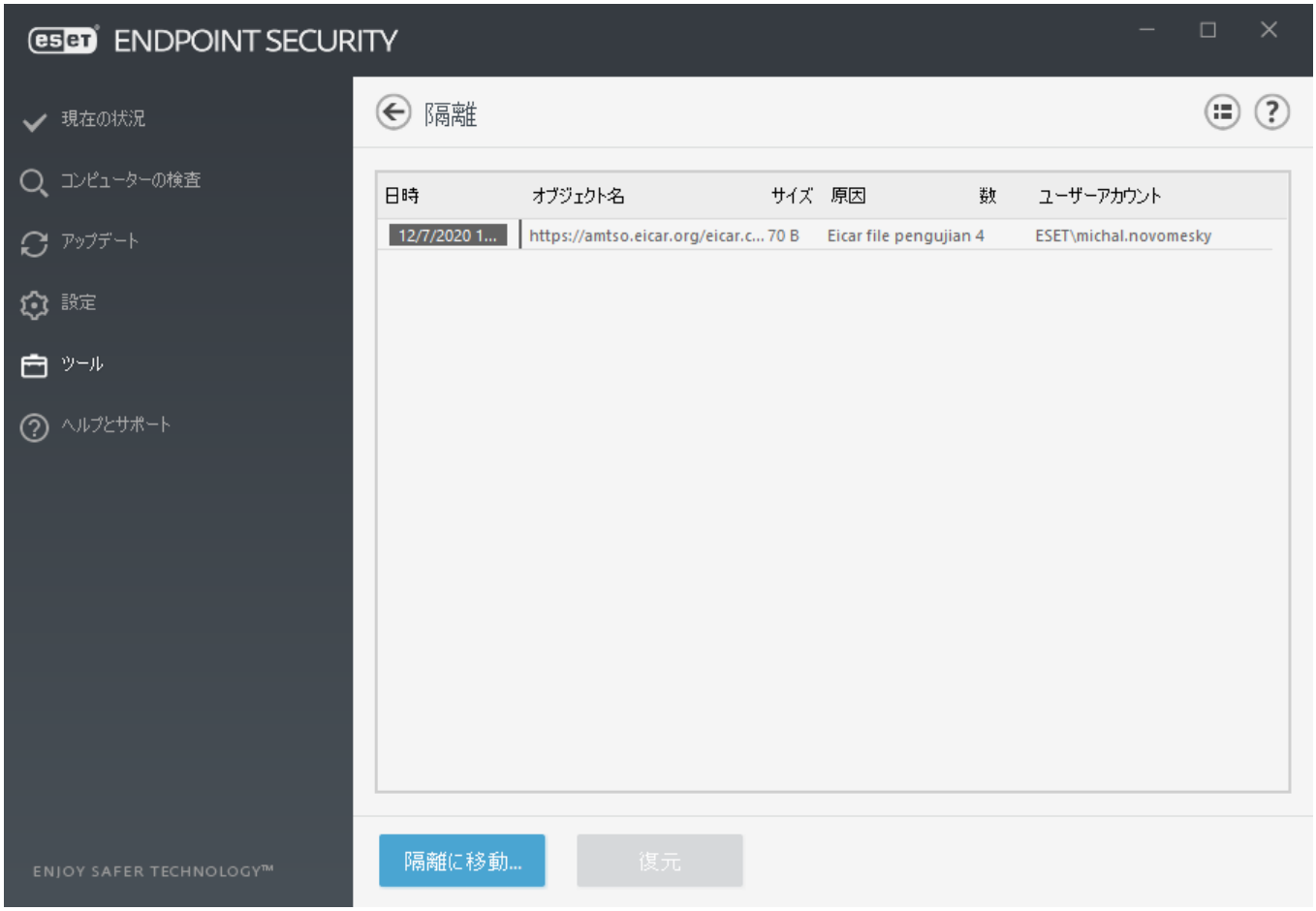
隔離

隔離の主な機能は、報告されたオブジェクト(マルウェア、感染したファイル、望ましくない可能性のあるアプリケーションなど)を安全な方法で保存することです。

隔離にはESET Endpoint Securityのメインプログラムウィンドウから**ツール** > **隔離**をクリックしてアクセスできます。

隔離フォルダーに保存されているファイルについては、表形式で次の情報が表示されます。

- 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(ユーザーが追加したオブジェクトなど)、
- 検出数(同じファイルの重複した検出、複数の侵入を含むアーカイブの場合)。
- リモートでクライアントワークステーションの隔離を管理する



ファイルの隔離

ESET Endpoint Securityは削除されたファイル(アラートウィンドウでこのオプションをキャンセルしていない場合)を自動的に隔離します。

次の場合は、追加のファイルを隔離することをお勧めします。

a.駆除できない

b.安全でないか、削除することが推奨される

c.ESET Endpoint Securityによって誤って検出された場合

d.ファイルが不審な動作をしているが、スキャナーで検出されない

ファイルを隔離するには、次の複数のオプションがあります。

a.ドラッグアンドドロップ機能を使って、ファイルをクリックすると、マウスボタンを押したままマウスポインターをマークした箇所に移動してからマウスボタンを放すと、そのファイルやフォルダーを手動で隔離します。 その後、アプリケーションが前面に移動します。

b.メイン プログラムウィンドウで**隔離に移動...**をクリックします。

c.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。

隔離フォルダーからの復元

隔離されたファイルは元の場所に復元することもできます。

- この目的のために**復元**機能を使用するには、隔離内の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を使用します。
- ファイルが望ましくない可能性のあるアプリケーションに設定されている場合、**検査から復元して除外**オプションが有効になります。 「除外」も参照してください。
- 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、削除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。
- 復元機能は、読み取り専用のネットワーク共有上にあるファイルなど、使用できない場合があります。

隔離から削除する

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。複数の項目を選択して、一度に削除することもできます。削除された項目は完全にデバイスと隔離から削除されます。

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、分析するためサンプルをESET研究所に送信してください。 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。

次のESETナレッジベース記事は、英語でのみ提供されている場合があります。
- ESET PROTECT (8 .x)で隔離を管理する
- ESET製品で検出が通知されました。何をすればよいですか。

プロキシサーバーの設定

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と通信している場合があります。この構成を使用する場合は、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アップデートされませんESET Endpoint Securityでは、[詳細設定]ツリーの2つのセクションでプロキシサーバーを設定できます。

まず、プロキシサーバーは[**詳細設定**]の[**ツール**] > [**プロキシサーバー**]から設定できます。プロキシサーバーをこのレベルで指定するとESET Endpoint Securityの全ての全体的なプロキシサーバー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、インターネットへの接続を必要とする全てのモジュールで使用されます。

プロキシサーバー設定をこのレベルで指定するには、[**プロキシサーバーを使用する**]を選択し、プロキシサーバーのアドレスを[**プロキシサーバー**]フィールドに入力し、プロキシサーバーの[**ポート**]番号を指定します。

プロキシサーバーとの通信に認証が必要な場合、[**プロキシサーバーは認証が必要**]をオンにし、有効な**ユーザー名**と**パスワード**をそれぞれのフィールドに入力します。 [**プロキシサーバーの検出**]をクリックすると、自動的にプロキシサーバー設定が検出されて取り込まれますInternet ExplorerまたはGoogle

Chromeのインターネットオプションで指定したパラメーターがコピーされます。

プロキシサーバー設定には、手動でユーザー名とパスワードを入力する必要があります。

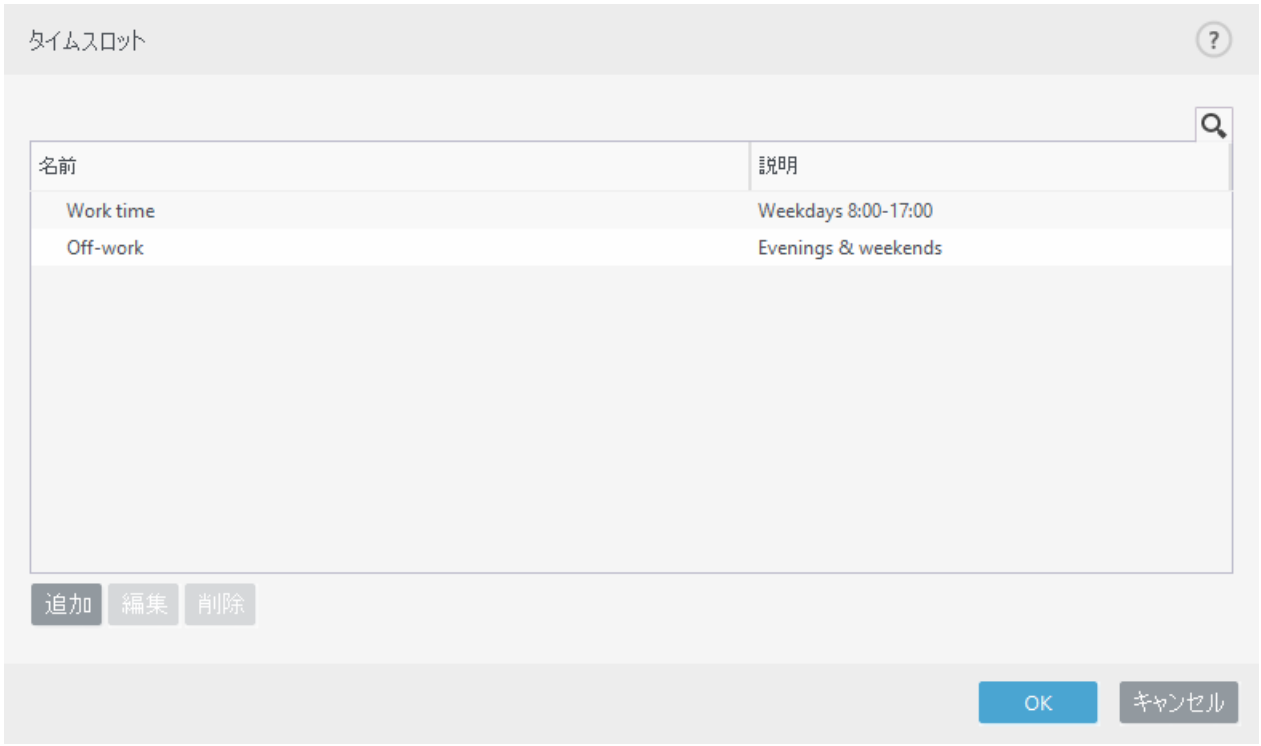
プロキシが使用できない場合は直接接続を使用する - ESET Endpoint Securityがプロキシを使用して接続するように設定され、プロキシに接続できない場合は、ESET Endpoint Securityはプロキシをバイパスし、直接ESETサーバーと通信します。

プロキシサーバー設定は詳細アップデート設定内でも定義できます(**[詳細設定]** > **[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]**の**[プロキシモード]**ドロップダウンメニューから**[プロキシサーバーを使用して接続する]**を選択する)。 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。検出エンジンアップデートをリモートロケーションから受信するノート型コンピューターをお勧めします。 この設定の詳細については「詳細なアップデート設定」を参照してください。



タイムスロット

タイムスロットを作成し、**デバイスコントロール**と **Webコントロール**のルールに割り当てることができます。**タイムスロット**設定は、**詳細設定** > **ツール**にあります。これにより、一般的に使用されるタイムスロット(例: 作業時間、週末など) を定義し、すべてのルールの時間範囲を再定義せずに、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ルールの関連するタイプに適用できます。



タイムスロットを作成するには、次の手順を実行します。

1.**編集** > **追加**をクリックします。

2.タイムスロットの名前と**説明**を入力し、**追加**をクリックします。

3.タイムスロットの曜日と開始/終了時刻を指定するか、**終日**を選択します。

4.**OK**をクリックして確認します。

1つのタイムスロットは、曜日と時刻に基づいて、1つ以上の時間範囲とともに定義できます。タイムスロットが作成されると、デバイスコントロールルールエディタウィンドウ または Web コントロールルールエディタウィンドウの[適用期間]ドロップダウンメニューに表示されます。.

Microsoft Windows Update

Windowsアップデート機能は、悪意のあるソフトウェアからユーザーを保護する重要なコンポーネントです。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 Endpoint 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。

- **アップデートしない** – 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ー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。そのため、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。

ライセンス間隔チェック

ESET Endpoint Securityは自動的にESETサーバーに接続する必要があります。この設定を変更するには、**詳細設定(F5) > ツール > ライセンス**に移動します。既定では、**間隔チェック**は**自動**に設定されています。ESETライセンスサーバーは1時間に数回製品を確認します。ネットワークトラフィックが増大した場合には、設定を**制限**に変更すると、負荷が低減されます。**制限**が選択されるとESET Endpoint Securityは1日に1回またはコンピューターが再起動するときにのみライセンスサーバーを確認します。

間隔チェック設定が**制限**に設定されている場合は、ESET Business Account/ESET MSP Administrator経由で実行されたすべてのライセンス関連の変更がESET Endpoint Securityに適用されるまでに最大で1日かかる場合があります。

ユーザーインターフェイス

[**ユーザーインタフェース**]セクションでは、プログラム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。

[ユーザーインタフェース要素]ツールを使用すると、プログラムの表示状態や使用されているエフェクトを調整できます。

セキュリティソフトウェアのセキュリティを最大限に高めるには、アクセス設定ツールを使用して不正な変更を防止できます。

アラートとメッセージボックスと通知を設定すると、検出アラートとシステム通知の動作を変更できます。これらは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[**ユーザーインターフェイス要素**] > [**アプリケーションステータス**]に表示されます。ここでは、ステータスを確認するか、これらの通知を表示しないようにできます。

選択したオブジェクトを右クリックすると、コンテキストメニュー統合が表示されます。コンテキストメニューに、ESET Endpoint Securityのコントロール要素を組み込むには、このツールを使用します。

アプリケーションでの作業中に、ポップアップウィンドウ、スケジュールされたタスク、およびプロセッサやRAMに負荷を与えるコンポーネントなどによって中断されたくないユーザーにとっては、プレゼンテーションモードが便利です。

ESET Endpoint Securityユーザーインターフェースを最小化する方法も参照してください(管理された環境で有用です)。

ユーザーインタフェース要素

ESET Endpoint Securityのユーザーインターフェースの設定オプションを使用すると、各自のニーズに合わせて作業環境を調整することができます。これらの設定オプションにはESET Endpoint Securityの[詳細設定]ツリーの[**ユーザーインタフェース**] > [**ユーザーインタフェース要素**]ブランチからアクセスします。

[ユーザーインタフェース要素]セクションでは、作業環境を調整できます。**[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。

完全メモリダンプ – 完全なGUIが表示されます。

最低 - GUIが実行中ですが、通知のみがユーザーに表示されます。

手動 – GUIはログオン時に自動的に起動しません。ユーザーは手動で起動できます。

サイレント – 通知またはアラートは表示されません。GUIは管理者のみが起動できます。このモードは、管理された環境またはシステムリソースを節約する必要がある場合に有効です。

> 最低GUI起動モードを選択してコンピューターが再起動すると、通知が表示されますがGUIは表示されません。完全GUIモードに戻すには、管理者としてスタートメニューの**[すべてのプログラム]** > **[ESET]** > ESET Endpoint Securityの下にあるGUIを実行するか、ポリシーを使用してESET Security Management Center経由で実行します。

ESET Endpoint Securityのスプラッシュウィンドウが表示されないようにするには、**[起動時にスプラッシュウィンドウを表示する]**のチェックを外します。

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 Endpoint Securityがサウンドを再生するようにするには、**[サウンドシグナルを使用する]**を選択します。

コンテキストメニューに統合する - ESET Endpoint Securityのコントロール要素をコンテキストメニューに統合します。

ステータス

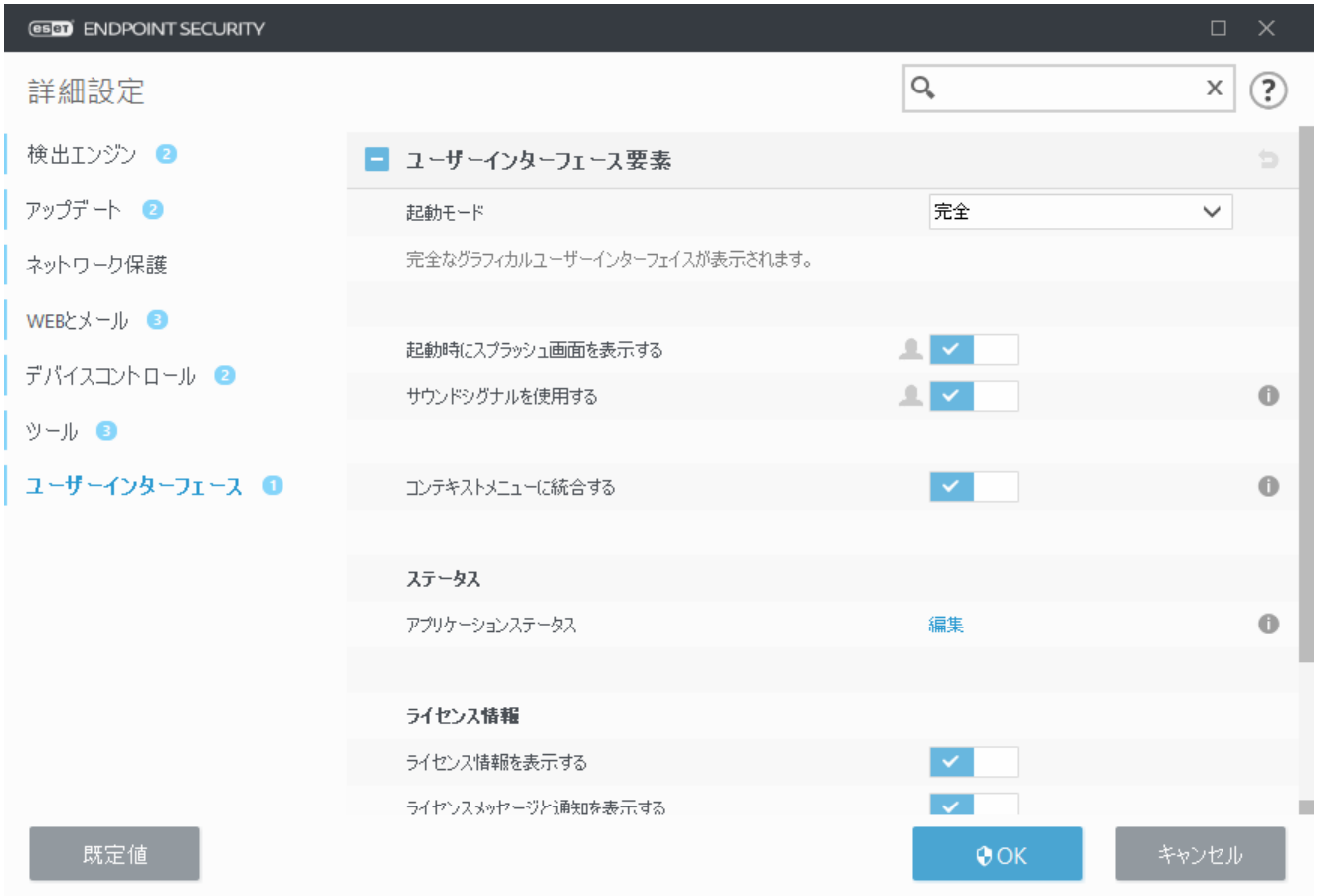
アプリケーションステータス - **[編集]**ボタンをクリックして、メインメニューの**[保護ステータス]**ペインに表示されるステータスを管理(無効)します。

ライセンス情報

ライセンス情報を表示する – 無効にすると、**[保護ステータス]**および**[ヘルプとサポート]**画面のライセンス有効期限が非表示になります。

ライセンスメッセージと通知を表示する – 無効にすると、ライセンスが期限切れの場合にのみ、通知とメッセージが表示されます。

> ライセンス情報設定は適用されますがMSPライセンスでアクティベーションされたESET Endpoint Securityでのみアクセスできます。



アプリケーションステータス

ESET Endpoint Securityの最初のパネルで製品内ステータスを調整するには⊡ESET Endpoint Security詳細設定ツリーの**ユーザーインターフェース > ユーザーインターフェース要素 > アプリケーションステータス**に移動します。



表示欄のチェックを有効/無効にすることで、該当のアプリケーションステータスの表示を有効/無効に

します。たとえば、ウイルス・スパイウェア対策保護を一時停止するときや、プレゼンテーションモードを有効にするときです。また、製品がアクティベーションされていない場合や、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。この設定は、ESET Security Management Centerポリシーから変更できます。

アクセス設定

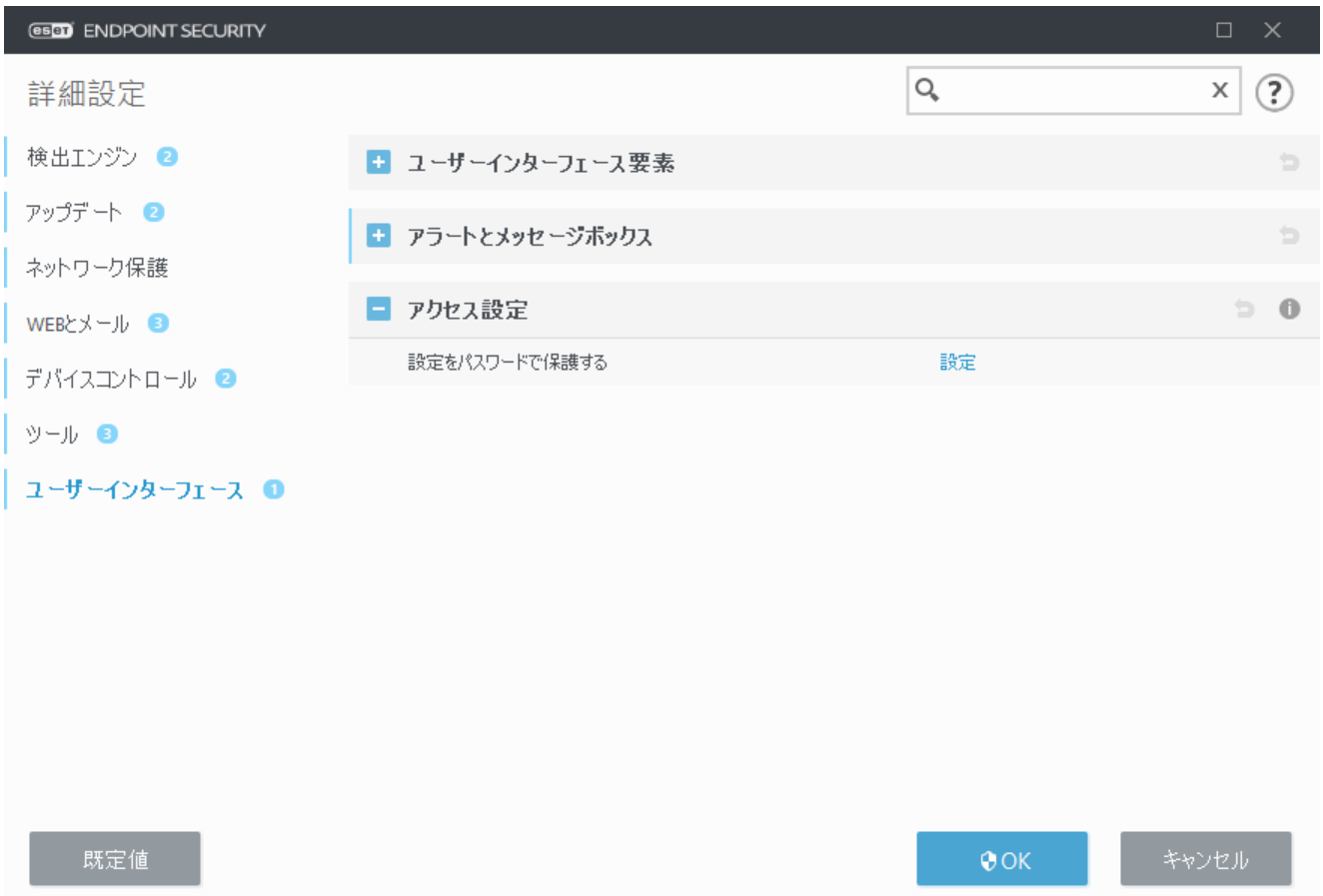
システムのセキュリティを最大限に確保するにはESET Endpoint Securityを正しく設定することが重要です。資格のないユーザーによって変更が行われた場合、重要なデータが失われることがあります。認証されていないユーザーによる変更を防ぐためにESET Endpoint Securityの設定パラメーターをパスワードで保護することができます。

管理された環境

管理者は、接続されたクライアントコンピューターのESET Endpoint Securityの設定をパスワードで保護するためのポリシーを作成できます。新しいポリシーを作成するには、パスワード保護設定を参照してください。

管理対象外

パスワード保護の構成設定は、**ユーザーインターフェース > アクセス設定**の下の**詳細設定(F5)**にあります。



パスワード保護設定 – パスワードの設定。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、[**設定**]をクリックします。

詳細設定のパスワード

不正な修正を防止する目的でESET Endpoint Securityの設定パラメーターを保護するには、新しいパスワードを設定する必要があります。

管理された環境

管理者は、接続されたクライアントコンピューターのESET Endpoint Securityの設定をパスワードで保護するためのポリシーを作成できます。新しいポリシーを作成するには、パスワード保護設定を参照してください。

管理対象外

既存のパスワードを変更したいとき:

1. **古いパスワード**フィールドに古いパスワードを入力します。
2. **新しいパスワード**と**パスワードの確認**に新しいパスワードを入力します。
3. **OK**をクリックします。

ESET Endpoint Securityを将来修正するには、このパスワードが必要です。

パスワードを忘れた場合は、詳細設定へのアクセスを復元できます。

- 「パスワードの復元」方法を使用して復元する(バージョン7.1以上)
- ESET Unlock Toolを使用して復元する(バージョン7.0以下)

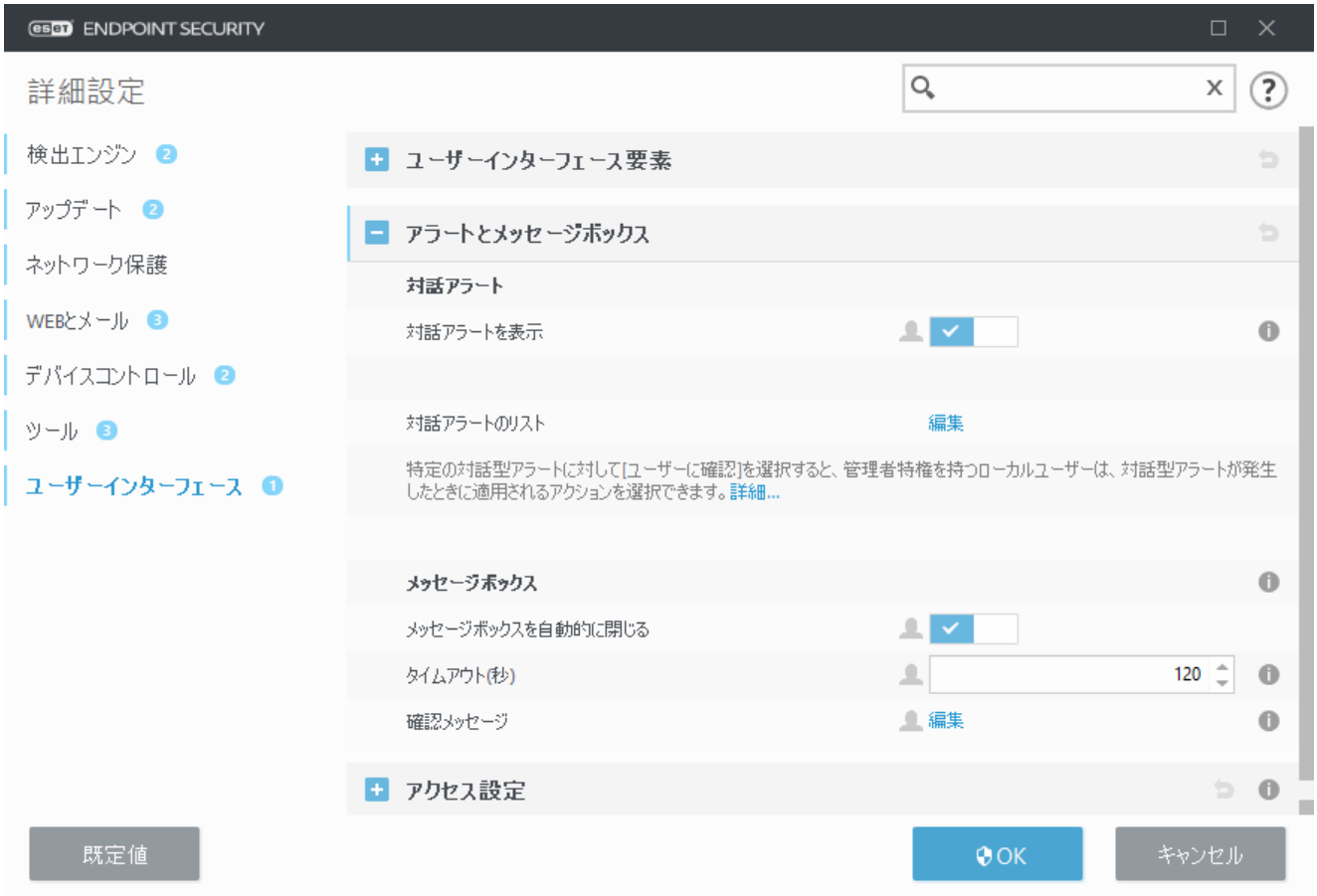
ESETが発行した製品認証キー、ライセンスの有効期限、またはESET Endpoint Securityの他のライセンス情報を忘れた場合は詳細をお読みください

アラートとメッセージボックス

共通のアラートと通知に関する情報

- マルウェアが検出されました
- アドレスがブロックされました
- アクティベーションされていません
- アップデートを利用できます
- アップデート情報に矛盾があります。
- 「モジュールアップデート失敗」メッセージのトラブルシューティング
- 「ファイルが破損しています」または「ファイルの名前を変更できませんでした」
- Webサイト証明書が取り消されました
- ネットワークの脅威がブロックされました

ユーザーインターフェースの下の**アラートとメッセージボックス**セクションでは、ユーザーによる決定が必要な場合(フィッシングWebサイトの可能性など)にESET Endpoint Securityで検出が処理される方法を設定できます。



対話アラート

検出があった場合、またはユーザーの介入が必要な場合には、インタラクティブなアラートウィンドウが表示されます。

対話アラートを表示

ESET Endpoint Securityバージョン7.2以降:

- 管理者権限のないユーザーの場合、このオプションは既定の設定のまま(有効)にすることをお勧めします。
- 管理者権限のあるユーザーの場合、この設定を有効にし、対話アラートのリストでユーザーの定義済みアクションを選択します。

対話アラートを表示を無効にすると、すべてのアラートウィンドウとブラウザー内のダイアログが非表示になります。定義済みの既定のアクションが自動的に選択されます(例:「フィッシングWebサイトの可能性」はブロックされます)。

ESET Endpoint Securityバージョン7.1以下:

この設定の名前は**アラートを表示**です。特定の対話アラートウィンドウの定義済みアクションをカスタマイズすることはできません。

デスクトップ通知

デスクトップの通知とバルーンヒントは情報を表示するだけであり、ユーザー操作は必要ありません。**デスクトップ通知**セクションは、詳細設定の**ツール > 通知**に移動しました(バージョン7.1以降)。

メッセージボックス

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るには、[**自動的にメッセージボックスを閉じる**]を選択します。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。

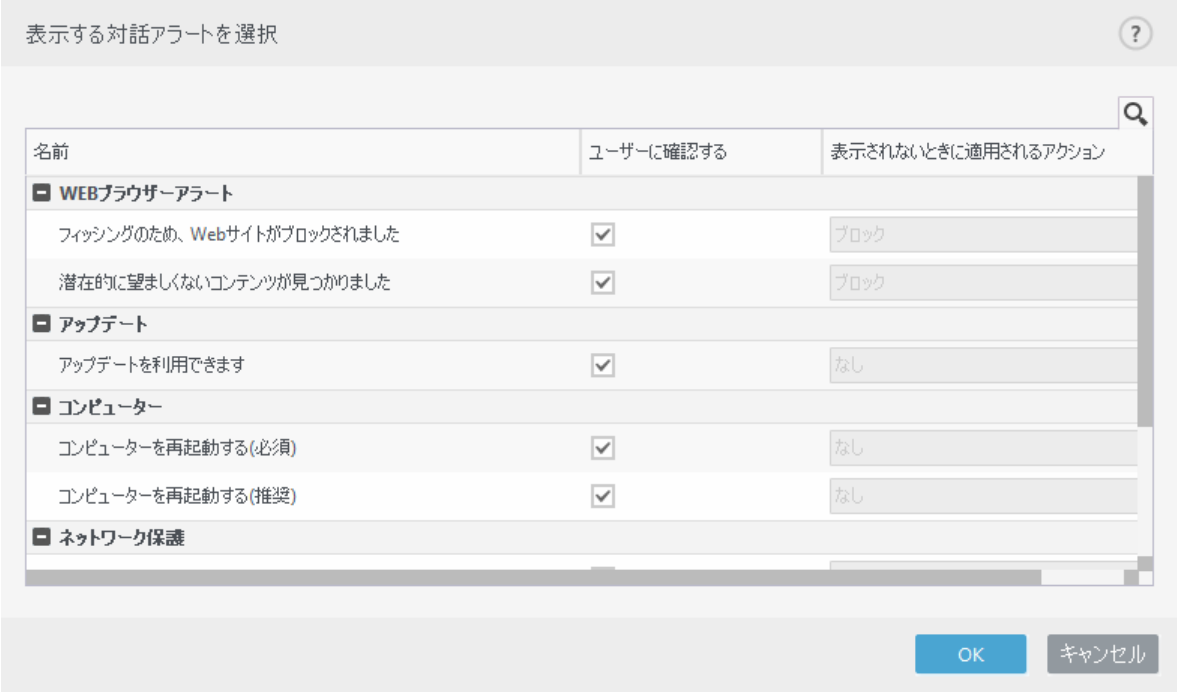
確認メッセージ – 表示または非表示にする確認メッセージを選択できるリストが表示されます。

対話アラート

このセクションでは、アクションが実行される前に、ESETEndpointSecurityで表示される複数の対話アラートウィンドウについて説明します。

設定可能な対話アラートの動作を調整するにはESET Endpoint Security詳細設定ツリーの**ユーザーインターフェース > アラートとメッセージボックス > 対話アラートのリスト**に移動し、**編集**をクリックします。

> 管理者が幾つもの「**ユーザーに確認**」を選択解除したり、対話アラートウィンドウが表示された時に適用される定義済みのアクションを選択しておけるので、管理された環境で役立ちます。製品内のアプリケーションステータスも参照してください。



特定の対話アラートウィンドウについては、他のヘルプセクションを確認してください。

リムーバブルメディア

- 新しいデバイスが選択されました

安全なブラウザー

- 既定のブラウザーで続行することを許可する

ネットワーク保護

- ネットワークアクセスがブロックされましたは、ESET PROTECTからのこのワークステーションのコ

ンピューターをネットワークから隔離するクライアントタスクがトリガーされたときに表示されます。

- ネットワーク通信がブロックされました
- ネットワークの脅威がブロックされました

Webブラウザーアラート

- 望ましくない可能性があるコンテンツが見つかりました
- フィッシングのためWebサイトがブロックされました

コンピュータ

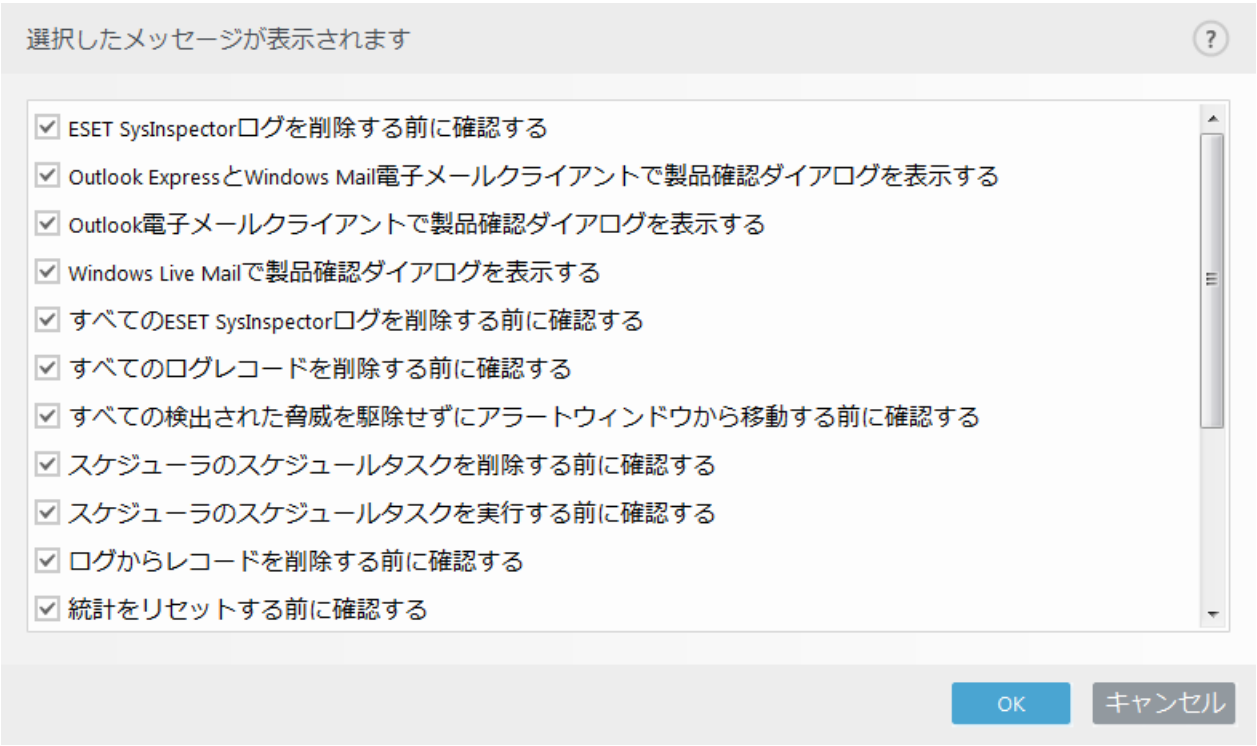
これらのアラートが発生していると、ユーザーインターフェースが次のオレンジ色に変わります。

- コンピューターを再起動する(必須)
- コンピューターを再起動する(推奨)

> 対話アラートには、検出エンジンHIPSファイアウォールの対話ウィンドウは含まれません。これらの動作は、特定の機能で個別に設定することができます。

確認メッセージ

確認メッセージを調整するにはESET Endpoint Security詳細設定ツリーの**ユーザーインターフェース > アラートおよびメッセージボックス > 確認メッセージ**に移動し、**編集**をクリックします。



このダイアログウィンドウには、アクションが実行される前に、ESET Endpoint Securityで表示される確認メッセージが表示されます。各確認メッセージの横のチェックボックスをオンまたはオフにすると、メッセージを許可または無効にします。

確認メッセージに関連した特定の機能の詳細:

- ESET SysInspectorログを削除する前に確認する
- すべてのESET SysInspectorログを削除する前に確認する
- 隔離フォルダのオブジェクトを削除する前に確認する
- 詳細設定の設定を破棄する前に確認する
- すべての検出された脅威を駆除せずにアラートウィンドウから移動する前に確認する
- ログからレコードを削除する前に確認する
- スケジューラのスケジュールタスクを削除する前に確認する
- すべてのログレコードを削除する前に確認する
- 統計をリセットする前に確認する
- 隔離フォルダからオブジェクトを復元する前に確認する
- 隔離フォルダからオブジェクトを復元して検査から除外する前に確認する
- スケジューラのスケジュールタスクを実行する前に確認する
- 迷惑メール対策処理結果通知を表示する
- 電子メールクライアントの迷惑メール対策処理結果通知を表示する
- Outlook ExpressとWindows Mail電子メールクライアントで製品確認ダイアログを表示する
- Windows Live Mailで製品確認ダイアログを表示する
- Outlook電子メールクライアントで製品確認ダイアログを表示する

詳細設定競合エラー

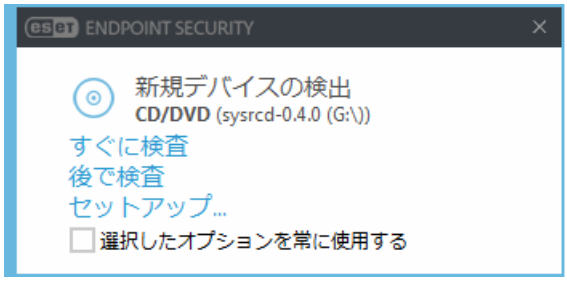
一部のコンポーネント(例: HIPS またはファイアウォール)とユーザーが同時にインタラクティブまたは学習モードでルールを作成するときに発生する場合があります。

独自のルールを作成する場合は、フィルタリングモードを既定の**自動モード**に変更することをお勧めします。 詳細については、ESETファイアウォール学習モードをお読みください。 詳細については、HIPSおよびHIPSフィルタリングモードをお読みください。

リムーバブルメディア

ESET Endpoint Securityには、リムーバブルメディア(CD/DVD/USBなど)をコンピューターに挿入したときに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ー管理者にとって便利です。

リムーバブルメディアを挿入し、ESET Endpoint Securityで**検査オプションを表示**ダイアログが設定されると、次のダイアログが表示されます。



このダイアログのオプション:

- **今すぐスキャン** – リムーバブルメディアのスキャンを開始します。
- **後でスキャン** – リムーバブルメディアのスキャンが延期されます。
- **設定 – 詳細設定**セクションを開きます。
- **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 Endpoint 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機能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。

ESET Endpoint Security 7.2以降

リムーバブルメディア検査の設定にアクセスするには、詳細設定(**F5**) > **ユーザーインターフェイス** > **アラートおよびメッセージボックス** > **対話型アラート** > **対話型アラートのリスト** > **編集** > **検出された新しいデバイス**を開きます。

ユーザーに確認するが選択されていない場合は、リムーバブルメディアをコンピューターに挿入する際のアクションを選択します。

- **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**ウィンドウは開きません。
- **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ーの検査が実行されます。
- **検査オプションを表示 – 対話型アラートの設定**セクションを開きます。

ESET Endpoint Security 7.1以下

リムーバブルメディア検査の設定を表示するには、詳細設定(**F5**) > **検出エンジン** > **マルウェア検査** > **リムーバブルメディア**を開きます。

リムーバブルメディアの挿入後に実行するアクション – コンピューターにリムーバブルメディアデバイス(CD、DVD、USB)が挿入されたときに実行する既定のアクションを選択します。リムーバブルメディアをコンピューターに挿入したときに実行するアクションを選択します。

- **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**ウィンドウは開きません。
- **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ー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。

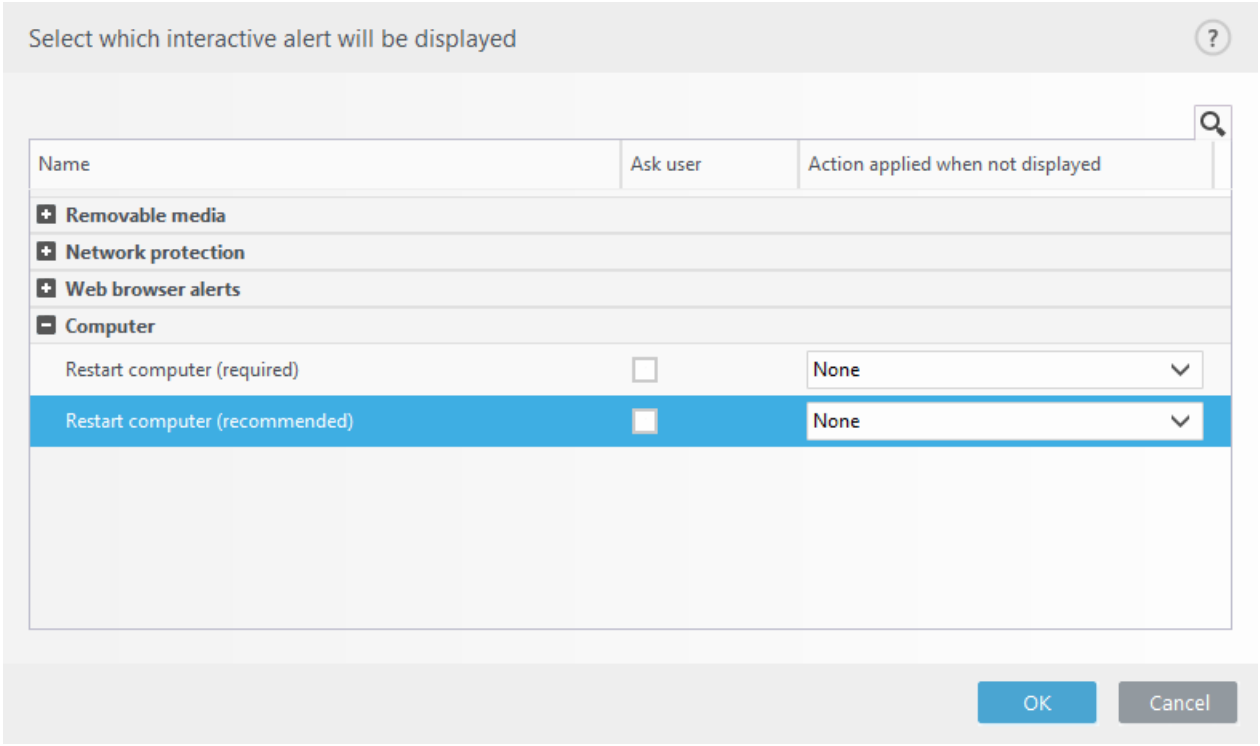
再起動する必要があります

エンドポイントコンピューターが「再起動が必要」の赤色アラートを受信した場合、アラートの表示を無効にすることができます。

「再起動が必要」または「再起動推奨」アラートを無効にするには、次の手順に従います。

1. **F5**キーを押して詳細設定にアクセスし、**アラートとメッセージボックス**セクションを展開します。

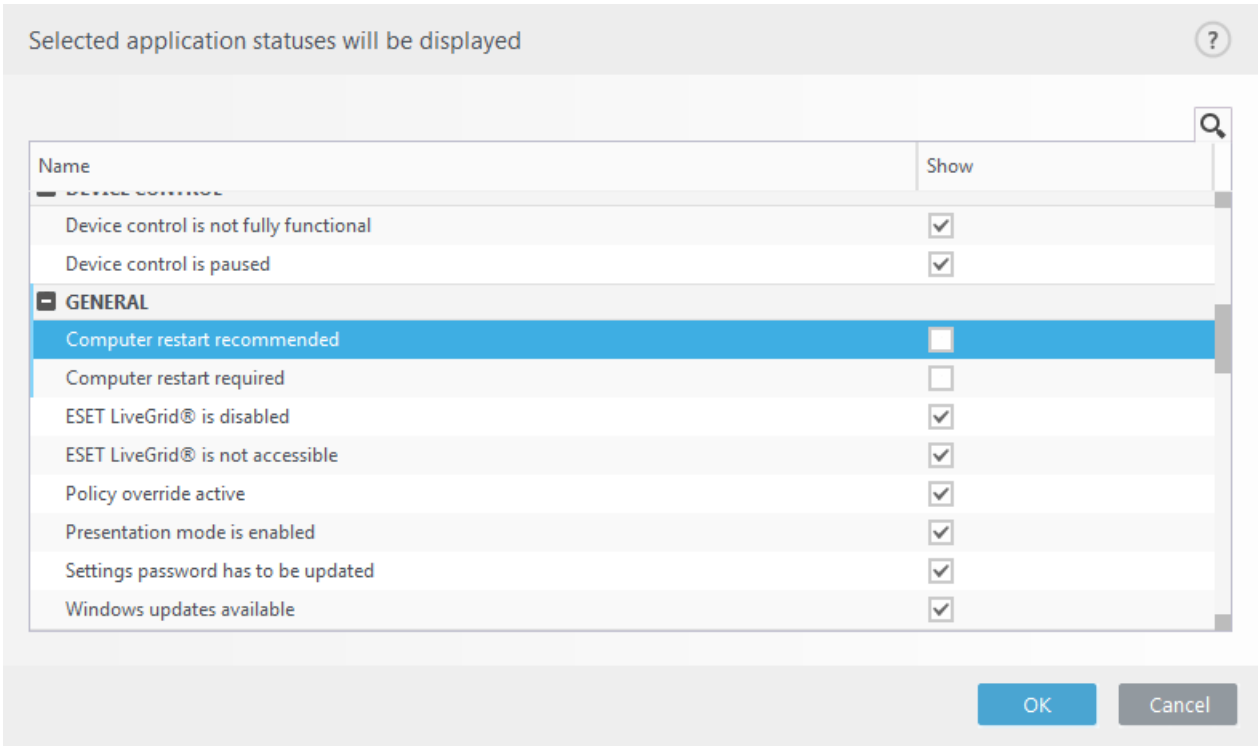
2**対話アラートのリスト**の横にある**編集**をクリックします。**コンピューター**セクションで、**コンピューターを再起動する(必須)**と**コンピューターを再起動する(推奨)**の横のチェックボックスをオフにします。



3. **OK**をクリックすると、両方の開いているウィンドウで変更を保存できます。

4. アラートは、エンドポイントコンピューターに表示されません。

5. (任意)ESET Endpoint Securityのメインプログラムウィンドウでアプリケーションステータスを無効にするには、アプリケーションステータスウィンドウで、**コンピューターの再起動が必要です**と**コンピューターの再起動が推奨されます**の横のチェックボックスをオフにします。



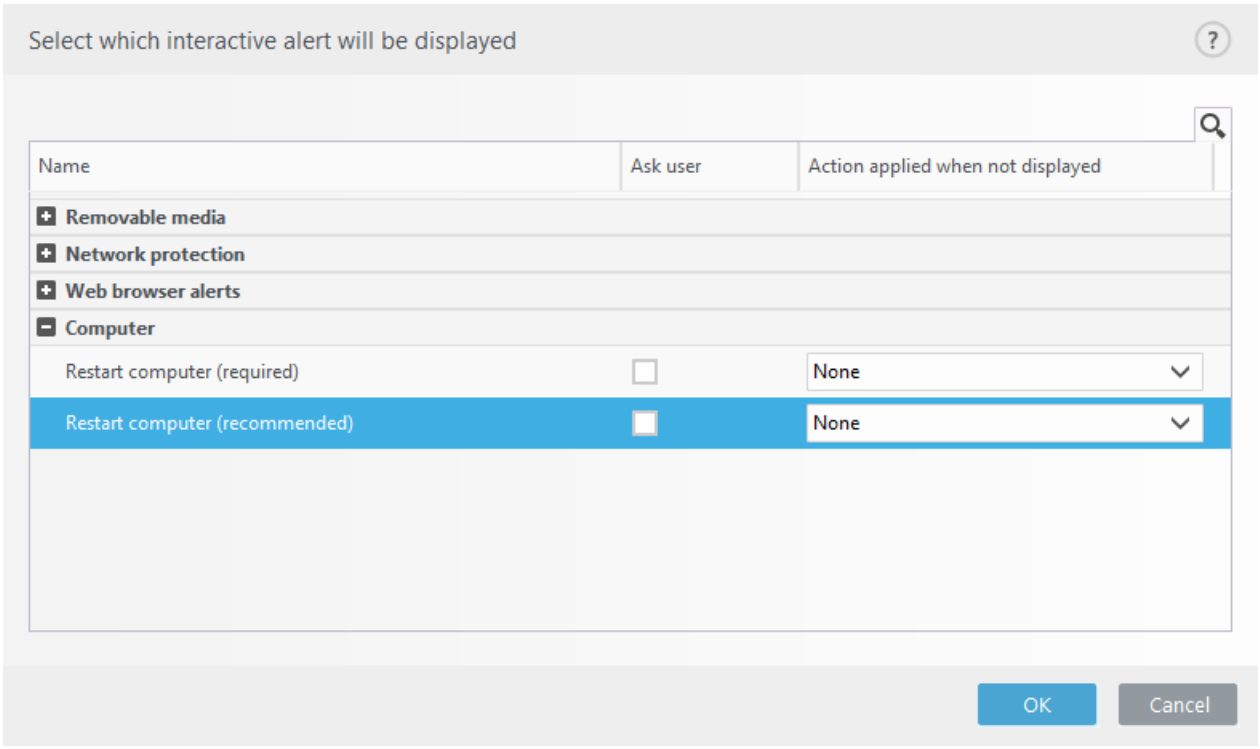
再起動が推奨されます

エンドポイントコンピューターが「再起動推奨」の黄色アラートを受信した場合、アラートの表示を無効にすることができます。

「再起動が必要」または「再起動推奨」アラートを無効にするには、次の手順に従います。

1. **F5**キーを押して詳細設定にアクセスし、**アラートとメッセージボックス**セクションを展開します。

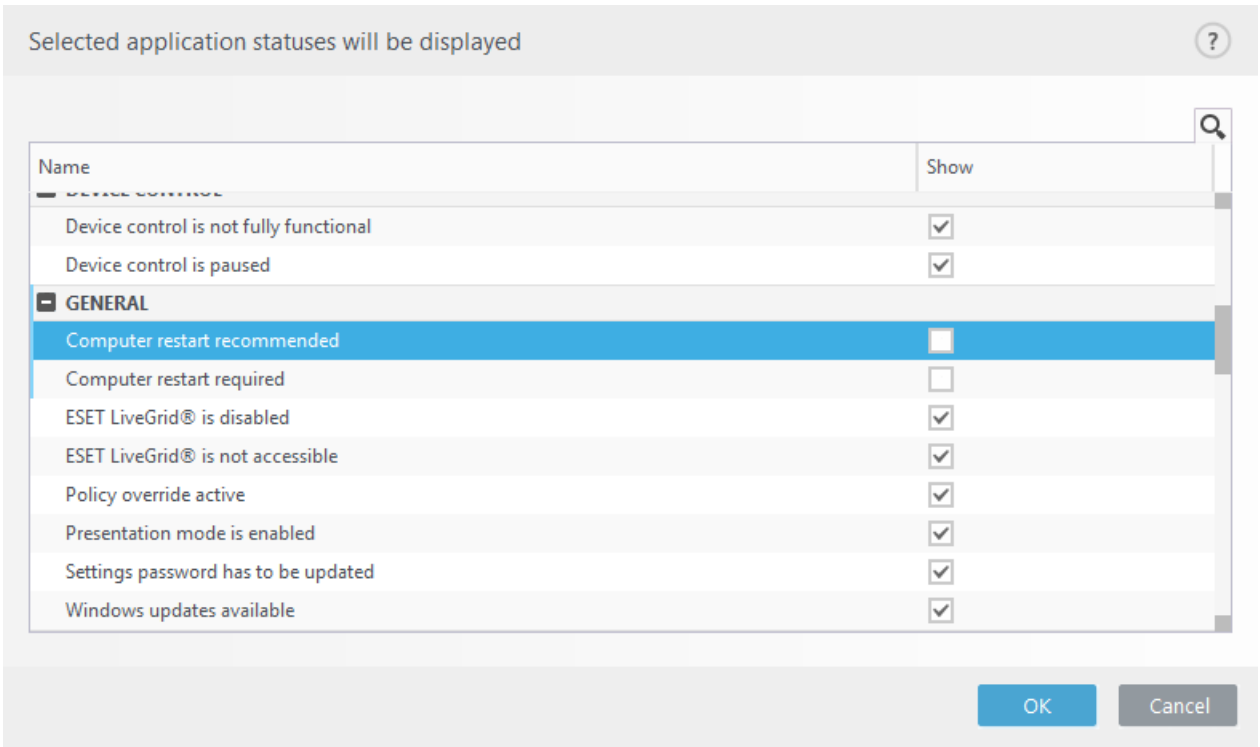
2**対話アラートのリスト**の横にある**編集**をクリックします。**コンピューター**セクションで、**コンピューターを再起動する(必須)**と**コンピューターを再起動する(推奨)**の横のチェックボックスをオフにします。



3. **OK**をクリックすると、両方の開いているウィンドウで変更を保存できます。

4. アラートは、エンドポイントコンピューターに表示されません。

5. (任意)ESET Endpoint Securityのメインプログラムウィンドウでアプリケーションステータスを無効にするには、アプリケーションステータスウィンドウで、**コンピューターの再起動が必要です**と**コンピューターの再起動が推奨されます**の横のチェックボックスをオフにします。



システムトレイアイコン

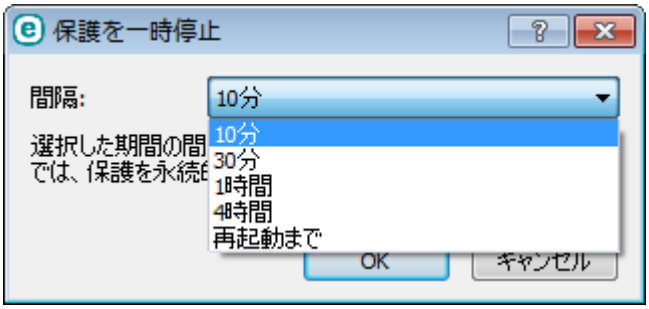
最も重要な設定オプションと機能の一部は、システムトレイアイコンを右クリックすると使用できます。

システムトレイアイコンメニューにアクセスするには、ユーザーインターフェース要素の起動モードが完全に設定されていることを確認してください。



保護を一時停止する – 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、検出エンジン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。

[**間隔**]ドロップダウンメニューは、すべての保護機能を無効にする期間を示します。



ファイアウォールを一時停止する(すべてのトラフィックを許可) – ファイアウォールを無効状態に切り替えます。詳細については、「ネットワーク」を参照してください。

すべてのネットワークをブロックする – 送信/着信のネットワークとインターネットの全トラフィックがファイアウォールによってブロックされます。再有効化するには、[**すべてのネットワークトラフィックのブロックを停止**]をクリックします。

詳細設定 - [**詳細設定**]ツリーを表示する場合にこのオプションを選択します。詳細設定にアクセスするにはF5キーを押すか、[**設定**] > [**詳細設定**]に移動することもできます。

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、検出の概要が表示されます。

ESET Endpoint Securityを開く – トレイアイコンからESET Endpoint Securityメインプログラムウィンドウを開きます。

ウィンドウレイアウトを初期状態に戻す - ESET Endpoint 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 – プログラム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。

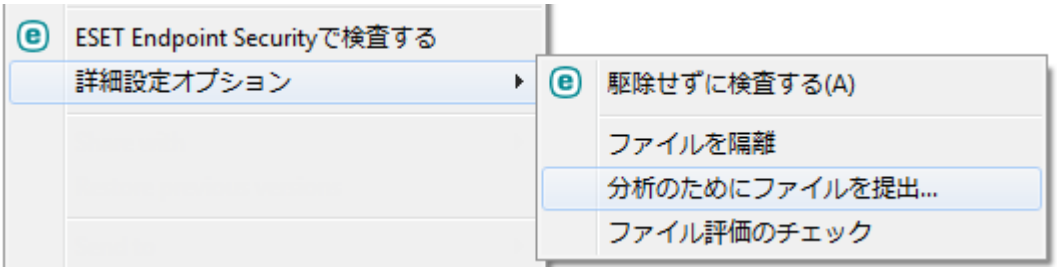
バージョン情報 – システム情報、インストールされているESET Endpoint Securityのバージョンに関する詳細、インストールされているプログラムモジュール、およびライセンスの有効期限が表示されます。オペレーティングシステムとシステムリソース情報は、ページの下部に表示されます。

コンテキストメニュー

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。

ESETEndpointSecurityのコントロール要素をコンテキストメニューに統合できます。詳細設定ツリー([**ユーザーインターフェイス**] > [**ユーザーインターフェイス要素**])に、この機能に対する設定オプションがあります。

コンテキストメニューに統合する - ESET Endpoint Securityのコントロール要素をコンテキストメニューに統合します。



ヘルプとサポート

ESET Endpoint 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ます。

インストールされている製品

- **ESET Endpoint Security** について – ESET Endpoint Securityに関する情報が表示されます。
- 製品のトラブルシューティング – 最もよくある問題の解決策を見つけるには、このリンクをクリックします。
- ライセンスのトラブルシューティング – このリンクをクリックすると、アクティベーションまたはライセンス変更の問題の解決策を検索します。
- ライセンスの変更 – クリックすると、[アクティベーション]ウィンドウが起動し、製品をアクティ

ベーションします。

**ヘルプページ** – このリンクをクリックするとESET Endpoint Securityヘルプページが開きます。

テクニカルサポート

• **サポートを依頼** – 問題の回答が見つからない場合ESETのWebサイトにあるこのフォームを使用して、テクニカルサポート部門に簡単に問い合わせることができますWeb フォームを入力する前に、設定に基づいて、システム構成データの送信ウィンドウが表示されます。

• **テクニカルサポートの詳細** – メッセージが表示された場合、情報をコピーしてESETテクニカルサポートに送信できます（製品名、製品バージョン、オペレーティングシステム、プロセットの種類など）。

• **ESET Log Collector** - ESETナレッジベース記事へのリンク。問題をより迅速に解決するためにコンピュータから情報とログを自動的に収集するアプリケーションである ESET Log Collector ユーティリティをダウンロードできます。 詳細については、 ESET Log Collectorここ をクリックしてください。

• 詳細ログを有効にすると、開発者が問題を診断および解決するために、すべての使用可能な機能の詳細ログを作成できます。 最小ログ詳細レベルは、診断に設定されています。 詳細ログの停止をクリックして停止しない場合、詳細ログは、2時間後に自動的に無効にされます。 すべてのログが作成されるときには、通知ウィンドウが表示され、診断フォルダーと作成されたログに直接アクセスできます。

**ナレッジベース** - 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、さまざまな問題を解決するための最も強力なツールです。

ESET Endpoint Securityの概要

このウィンドウには、インストールされたESET Endpoint Securityのバージョン、オペレーティングシステム、およびシステムリソースの詳細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をクリックすると、インストールされたプログラムモジュールとバージョンの一覧が表示されます。[**コピー**]をクリックして、モジュールに関する情報をクリップボードにコピーできます。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。



システム構成データの送信

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 Endpoint 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。ESETはお客様に技術支援を提供するためにのみこのデータを使用します。

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。 データを送信せずにフォームを送信する場合は、**[データを送信しない]**をクリックし、オンラインサポートフォームを使用してESETテクニカルサポートに連絡できます。

この設定は、**[詳細設定]** > **[ツール]** > **[診断]** > **[テクニカルサポート]**で構成できます。

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。

テクニカルサポート

テクニカルサポートに問い合わせる

サポートを依頼 – 問題の回答が見つからない場合、ESETのWebサイトにあるこのフォームを使用してESETテクニカルサポート部門に簡単に問い合わせることができます。Web フォームを入力する前に、設定に基づいて、システム構成データの送信ウィンドウが表示されます。

テクニカルサポート情報

テクニカルサポートの詳細 – メッセージが表示された場合、情報をコピーしてESETテクニカルサポートに送信できます（ライセンス詳細情報、製品名、製品バージョン、オペレーティングシステム、コンピューター情報など）。

ESET Log Collector - ESETナレッジベース記事へのリンク。問題をより迅速に解決するためにコンピュータから情報とログを自動的に収集するアプリケーションであるESET Log Collectorユーティリティをダウンロードできます。 詳細については、 ESET Log Collectorここ をクリックしてください。

詳細ログを有効にすると、開発者が問題を診断および解決するために、すべての使用可能な機能の詳細ログを作成できます。 最小ログ詳細レベルは、**診断**に設定されています。 **詳細ログの停止**をクリックして停止しない場合、詳細ログは、2時間後に自動的に無効にされます。 すべてのログが作成されるときには、通知ウィンドウが表示され、診断フォルダーと作成されたログに直接アクセスできます。

プロファイルマネージャ

プロファイルマネージャは、ESET Endpoint Security内の2ヶ所、つまり[**コンピュータの検査**]セクションと[**アップデート**]セクションで使用します。

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。

To create a new profile, open the Advanced setup window (F5) and click **Antivirus** > **On-demand computer scan** and then **Edit** next to **List of profiles**. The **Update profile** drop-down menu that lists existing scan profiles. To help you create a scan profile to fit your needs, see the ThreatSense engine parameters setup section for a description of each parameter of the scan setup.

既にある[**コンピューターの検査**]の設定は部分的にしか自分のニーズを満たさないので、独自の検査プロファイルを作成する必要があると仮定します。たとえば、ランタイム圧縮形式と安全でない可能性があるアプリケーションは、検査しません。また、[**厳密な駆除**]を適用することにします。 [**プロファイルマネージャ**]ウィンドウで新しいプロファイルの名前を入力し、[**追加**]をクリックします[**選択したプロファイル**]ドロップダウンメニューから新しいプロファイルを選択し、要件に合わせて残りのパラメータを調整し、[**OK**]をクリックして新しいプロファイルを保存します。

アップデート

[アップデート]-[プロファイル]の部分にあるプロファイルを使用すると、新しいプロファイルを作成できます。ユーザー独自のカスタムプロファイル(つまり、既定の[**マイプロファイル**]以外)を作成して使用するのは、コンピュータからアップデートサーバーへの接続方法が複数ある場合だけにしてください。

例えば、通常はローカルネットワーク内のローカルサーバー、つまりミラーに接続しますが、出張などでこのローカルネットワークに接続していないときには、更新ファイルをESETのアップデートサーバから直接ダウンロードします。これによりノートPCは、2つのプロファイルを使用することができます。1つ目のプロファイルではローカルサーバに接続し、2つ目ではESETのサーバに接続します。プロファイルを設定したら、[**ツール**]>[**スケジューラ**]に移動し、アップデートタスクのパラメーターを編集します。一方のプロファイルをプライマリ、他方をセカンダリに指定します。

アップデートプロファイル – 現在使用されている更新プロファイル。変更するには、ドロップダウンメニューからプロファイルを選択します。

プロファイルのリスト – 新しいアップデートプロファイルを作成するか、既存のアップデートプロファイルを削除します。

ショートカットキー

ESET Endpoint Securityでの操作をより容易にするには、次のキーボードショートカットを使用します。

キーボードショートカット	実行されたアクション
F1	ヘルプページを開きます
F5	詳細設定を開きます
Up/Down	製品の項目間を移動します
TAB	ウィンドウ内のカーソルを移動します
Esc	アクティブなダイアログウィンドウを閉じます
Ctrl+U	ESETライセンスとコンピューターの情報を表示します(テクニカルサポートの詳細)
Ctrl+R	製品ウィンドウを既定のサイズ・既定の位置に戻します

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 Endpoint 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**]をクリックすると、この機能を無効にします。

- **ミニ**(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のに役立つ最低限の有用な情報を記録します。 この種類のダンプファイルは、領域が限られているときに便利です。ただし、含まれ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。

対象ディレクトリ – クラッシュ時、ダンプが作成されるディレクトリーです。

ダンプファイルの保存フォルダを開く – このディレクトリーを新しい *Windows Explorer* ウィンドウで開く場合は、[**開く**]をクリックします。

診断ダンプを作成する - [**作成**]をクリックすると、[**ターゲットディレクトリ**]に診断ダンプを作成します。

詳細ログ

迷惑メール対策エンジン詳細ロギングを有効にする – 迷惑メール対策検査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ESET迷惑メール対策エンジンに関連する問題を診断および修正できます。

コンピュータースキャナー詳細ログを有効にする – 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によるファイルとフォルダーの検査中に発生するすべてのイベントを記録します。

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ます。 これにより、開発者はデバイスコントロールに関連する問題を診断および修正できます。

ドキュメント保護詳細ログを有効にする – ドキュメント保護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。

カーネル詳細ロギングを有効にする-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、問題の診断と解決を許可します(バージョン7.2以降で使用可能)。

ライセンス詳細ロギングを有効にする – ESETアクティベーションおよびESET Business Accountサーバーとのすべての製品の通信を記録します。

メモリ追跡を有効にする – 開発者がメモリリークを診断できるようにすべてのイベントを記録します。

ネットワーク保護詳細ロギングを有効にする- PCAP形式でファイアウォール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、開発者はファイアウォール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。これにより、開発者は、オペレーティングシステムで実行中のESET製品に関連する問題を診断および修正できます。

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。

リアルタイムファイルシステム保護詳細ログを有効にする – リアルタイムファイルシステム保護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。

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。

Webコントロール詳細ログを有効にする – Webコントロールで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Webコントロールに関連する問題を診断および修正できます。

ログファイルの場所

C:\ProgramData\ESET\ESET Endpoint Security\Diagnostics

コマンドラインスキャナー

ESET Endpoint Securityの保護モジュールは、コマンドラインから手動で起動することも("ecls"コマンドを使用します)、バッチ("bat")ファイルを使用して起動することもできますecls.exeは、既定値で

は[C:\Prog]に格納されています。

ESETコマンドラインスキャナーの使用方法:

```
ecls [OPTIONS..] FILES..
```

コマンドラインからオンデマンドスキャナーを実行する際には、次のパラメーターおよびスイッチを使用することができます。

オプション

/base-dir=移動先のフォルダ	FOLDERからモジュールをロードします
/quar-dir=移動先のフォルダ	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	サブフォルダーを検査します(既定)
/no-subdir	サブフォルダーを検査しません
/max-subdir-level=LEVEL	スキャン対象に含めるサブフォルダー階層の下限レベル
/symlink	シンボリックリンクを辿ります(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=ファイル	ログをFILEに出力します
/log-rewrite	出力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)
/aind	アクティビティインジケーターを表示します
/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

スキャナーオプション

/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	メモリーを検査します
/boots	ブートセクターを検査します
/no-boots	ブートセクターを検査しません(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	受信箱を検査します(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	安全でない可能性があるアプリケーションを検査します
/no-unsafe	安全でない可能性が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する(既定)
/no-suspicious	不審なアプリケーションを検査しない
/pattern	シグネチャーを使用します(既定)
/no-pattern	シグネチャーを使用しません
/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	コロンで区切られたEXTENSIONSファイルを検査対象から除外します
/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 - ファイルの内容に関係なく□ecls.exeは駆除を試行せずにファイルを削除します。 • delete - ecls.exeは駆除を試行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	感染ファイルを隔離フォルダーにコピーします (駆除中に実行したアクションの補足)
/no-quarantine	感染ファイルを隔離フォルダーにコピーしません

一般的なオプション

/help	ヘルプの表示と終了を実行します
/version	バージョン情報の表示と終了を実行します
/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	マルウェアが検出されました
100	エラー

100を超える終了コードは、ファイルがスキャンされなかったため、感染している可能性があることを意味します。

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。 これまでは、GUIのみを使用して設定をエクスポート及びインポートすることが可能でしたESET Endpoint 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(*.xml*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、*.xml*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 Endpoint 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。

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**を使用してWindowsコマンドプロンプト(cmd)を開く必要があります。 さもなければ、「**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。

高度なecmdコマンドはローカルでのみ実行できますESET PROTECTまたはESMC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。

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
```

*.xml*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。

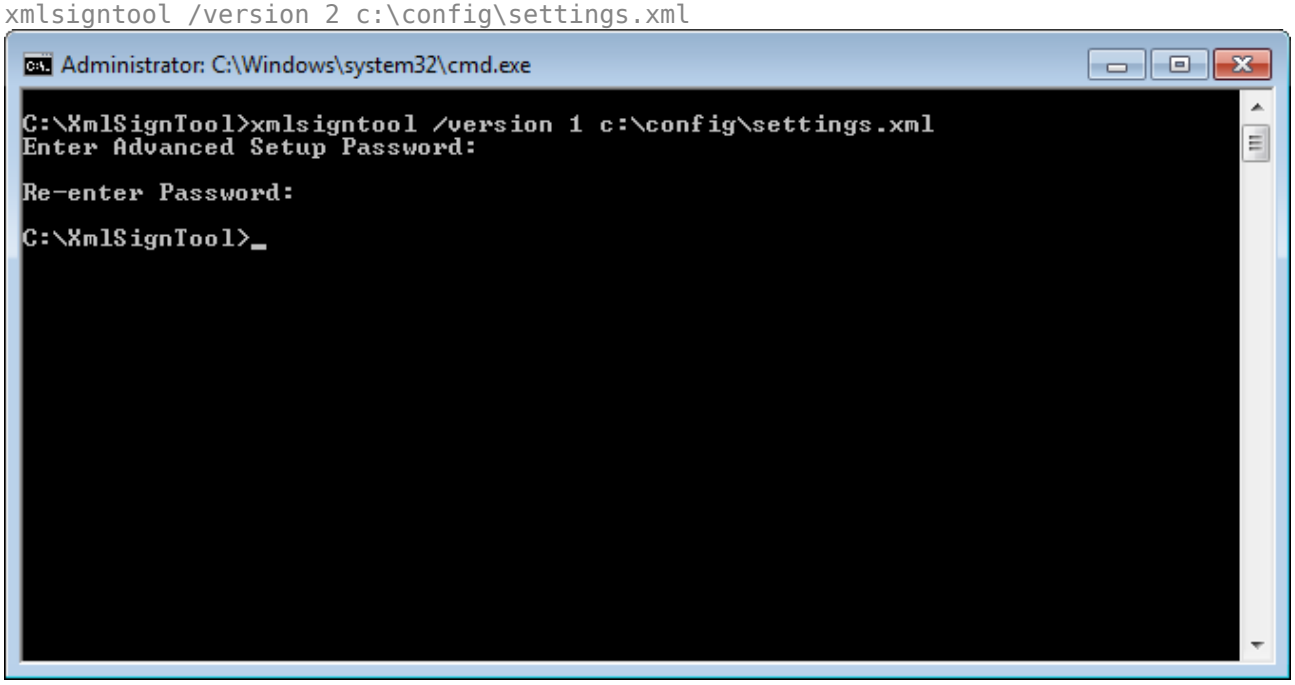
3. `xmlsigntool.exe`の保存場所に移動します。

4. コマンドを実行し、*.xml*設定ファイルに署名します。使用方法: `xmlsigntool /version 1|2 <xml_file_path>`

`/version`パラメーターの値は、ESET Endpoint Securityのバージョンによって異なります。バージョン7以降では、`/version 2`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ます。 *.xml*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 Endpoint 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。

エクスポートされた設定ファイルの署名コマンド:
`xmlsigntool /version 2 c:\config\settings.xml`



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する必要があります。 これにより、インポート前にESET Endpoint 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。

認証なしでESET CMDを有効にすることは推奨されません。これにより、署名されていない設定のインポートが可能になります。**[詳細設定] > [ユーザーインターフェイス] > [アクセス設定]**でパスワードを設定し、ユーザーによる無許可の修正を防止します。

ecmdコマンドのリスト

個別のセキュリティ機能は、ESET PROTECTクライアントタスク実行コマンドで有効にしたり、一時的に無効にしたりできます。コマンドはポリシー設定を上書きせず、一時停止した設定は、コマンドの実行後またはデバイスの再起動後に元の状態に戻されます。この機能を利用するには、同じ名前のフィールドで実行するコマンドラインを指定します。

以下の各セキュリティ機能のコマンドのリストを確認してください。

セキュリティ機能	Temporary Pauseコマンド	Enableコマンド
リアルタイムファイルシステム保護	ecmd /setfeature onaccess pause	ecmd /setfeature onaccess enable
ドキュメント保護	ecmd /setfeature document pause	ecmd /setfeature document enable
デバイスコントロール	ecmd /setfeature devcontrol pause	ecmd /setfeature devcontrol enable
プレゼンテーションモード	ecmd /setfeature presentation pause	ecmd /setfeature presentation enable
アンチステルス技術	ecmd /setfeature antistealth pause	ecmd /setfeature antistealth enable
パーソナルファイアウォール	ecmd /setfeature firewall pause	ecmd /setfeature firewall enable
ネットワーク攻撃保護(IDS)	ecmd /setfeature ids pause	ecmd /setfeature ids enable
ボットネット保護	ecmd /setfeature botnet pause	ecmd /setfeature botnet enable
Webコントロール	ecmd /setfeature webcontrol pause	ecmd /setfeature webcontrol enable
Webアクセス保護	ecmd /setfeature webaccess pause	ecmd /setfeature webaccess enable
電子メールクライアント保護	ecmd /setfeature email pause	ecmd /setfeature email enable
迷惑メール対策保護	ecmd /setfeature antispam pause	ecmd /setfeature antispam enable
フィッシング対策機能	ecmd /setfeature antiphishing pause	ecmd /setfeature antiphishing enable

アイドル状態検知

アイドル状態検知設定は、**詳細設定**の**検出エンジン > マルウェア検査 > アイドル状態検査 > アイドル状態検知**で設定できます。この設定により、次の場合にアイドル状態検査のトリガが指定されます。

- スクリーンセーバが実行されている
- コンピュータがロックされている
- ユーザーがログオフする

それぞれの状態についてチェックボックスを使用して、アイドル状態の検出トリガを有効または無効にします。

設定のインポート/エクスポート

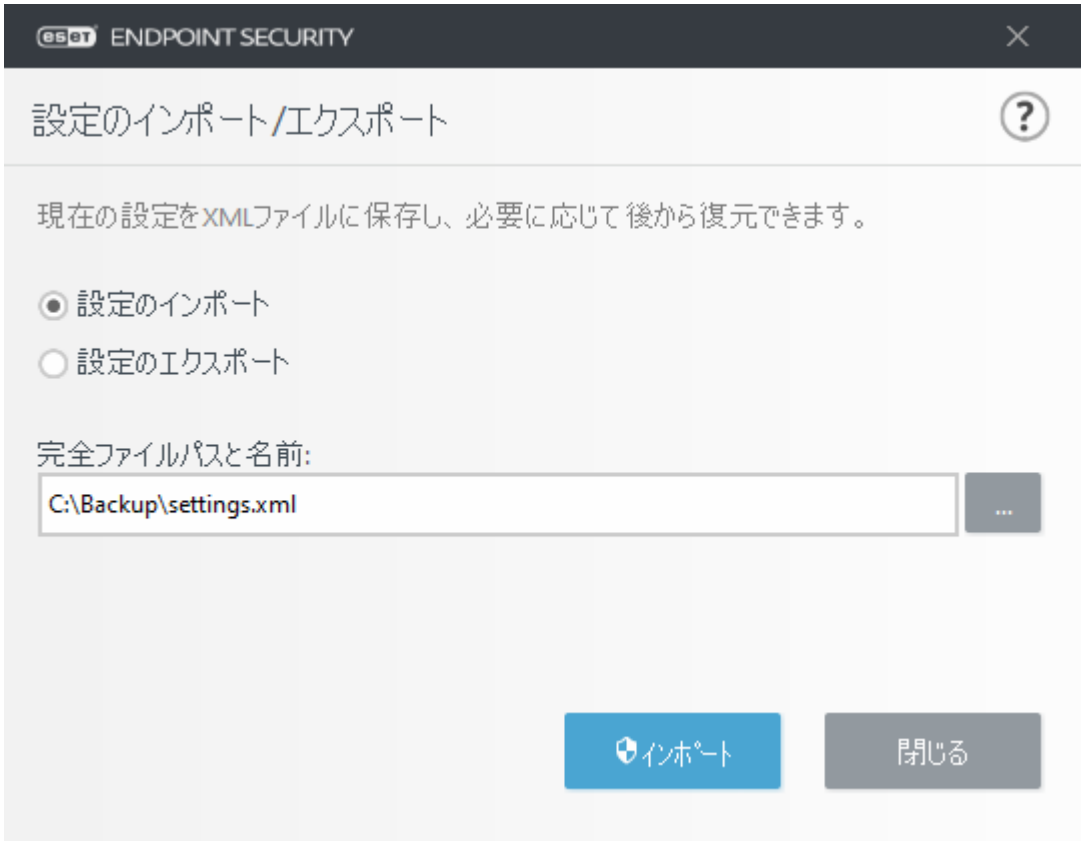
[**設定**]メニューから、カスタマイズしたESET Endpoint Securityの設定ファイル（.xml形式）をインポートまたはエクスポートできます。

設定ファイルのインポートとエクスポートは、後で使用するためにESET Endpoint Securityの現在の設定をバックアップする必要がある場合に便利です。エクスポート設定オプションは、好みの基本設定を複数のシステムに対して使用する場合にも便利です。.xmlファイルを簡単にインポートして、設定を展開できます。

設定のインポートは、非常に簡単です。メインプログラムウィンドウで[**設定**] > [**設定のインポート/エクスポート**]をクリックし、[**設定のインポート**]を選択します。設定ファイルのファイル名を入力するか、あるいは[**...**]ボタンをクリックして、インポートする設定ファイルを参照します。

設定をエクスポートする手順は、ほとんど同じです。メインプログラムウィンドウで[**設定**] > [**設定のインポート/エクスポート**]をクリックします。[**設定のエクスポート**]を選択し、設定ファイルのファイル名（*export.xml*など）を入力します。エクスプローラーを使用して、設定ファイルの保存先を選択します。

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。



すべての設定を既定値に戻す

詳細設定(F5)で**既定**をクリックすると、すべてのモジュールのすべてのプログラム設定を元に戻します。これで、すべてのモジュールのすべてのプログラム設定が新規インストール時の状態にリセットされます。

設定をインポートおよびエクスポートするを参照してください。

現在のセクションのすべての設定を元に戻す

カーブした矢印↶をクリックすると、現在のセクションのすべての設定がESETで定義した既定の設定に戻ります。

既定に戻すをクリックすると、行われたすべての変更が失われます。

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。

設定をインポートおよびエクスポートするを参照してください。

設定の保存中のエラー

このエラーメッセージは、エラーが発生したため設定が正しく保存されなかったことを示しています。

通常、これは、プログラムパラメーターを修正しようとしたユーザーが次の状態であることを意味します。

- アクセス権が不十分であるか、設定ファイルとシステムレジストリを修正するために必要なオペレーティングシステム権限がないことを意味します。
  > 目的の修正を実行するには、システム管理者がログインする必要があります。

- 最近HIPSまたはファイアウォールで学習モードを有効にし、詳細設定を変更しようとしました。
  > 設定を保存し、設定の競合を回避するには、保存せずに詳細設定を閉じ、目的の変更をもう一度試してください。

2番目に一般的な原因としては、プログラムが壊れて正しく動作しなくなり、再インストールが必要になったことが考えられます。

リモート監視と管理

リモート監視と管理(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を監視および制御するプロセスです。

ERMM - RMM向けのESETプラグイン

- 既定のESET Endpoint Securityインストールには、次のディレクトリ内のEndpointアプリケーションにあるermm.exeファイルが含まれます。
  C:\Program Files\ESET\ESET Security\ermm.exe

- ermm.exeは、エンドポイント製品の管理とRMMプラグインとの通信を容易にするために設計されたコマンドラインユーティリティです。

- ermm.exeはRMMプラグインとデータを交換します。これはRMMサーバーにリンクされたRMMエージェントと通信します。既定ではESET RMMツールは無効です。

その他のリソース

- ERMMコマンドライン

- ERMM JSONコマンドのリスト

- リモート監視と管理をアクティブ化する方法ESET Endpoint Security

サードパーティRMMソリューション向けのESET Direct Endpoint Managementプラグイン

サードパーティーのサーバーではRMMサーバーは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プラグイン(ConnectWise Automate版)

- ESET Direct Endpoint Managementプラグイン(DattoRMM版)
- ESET Direct Endpoint Managementプラグイン(Solarwinds N-Central版)
- ESET Direct Endpoint Management (NinjaRMM版)

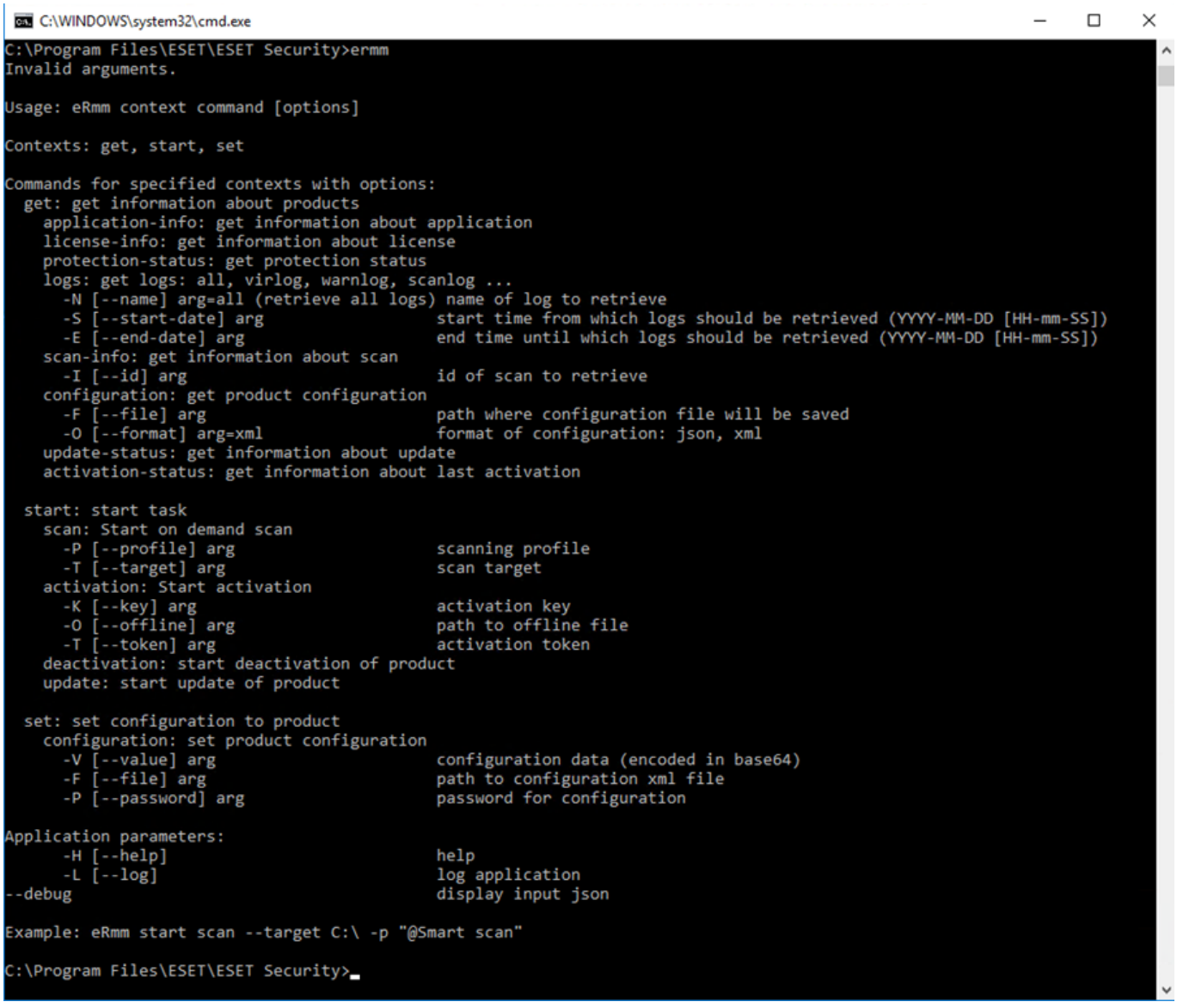
ERMMコマンドライン

Remote monitoring management is run using the command line interface. The default ESET Endpoint Security installation contains the file ermm.exe located in the Endpoint application within the directory *c:\Program Files\ESET\ESET Security*.

Run the Command Prompt (cmd.exe) as an Administrator and navigate to the mentioned path. (To open Command Prompt, press Windows button + R on your keyboard, type a cmd.exe into the Run window and press Enter.)

The command syntax is: `ermm context command [options]`

Also note that the log parameters are case sensitive.



ermm.exe uses three basic contexts: Get, Start and Set. In the table below you can find examples of commands syntax. Click the link in the Command column to see the further options, parameters, and usage examples. After successful execution of command, the output part (result) will be displayed. To see an input part, add parameter `--debug` at the of the command.

Context	Command	Description
get		**Get information about products**
	アプリケーション情報	Get information about product
	ライセンス情報	Get information about license
	保護の状態	Get protection status
	ログ	Get logs
	検査情報	Get information about running scan
	コンフィグレーション	Get product configuration
	アップデートステータス	Get information about update
	アクティベーションステータス	Get information about last activation
start		**Start task**
	スキャンする/走査する	Start on demand scan
	アクティベーション	Start activation of product
	アクティベーション解除	Start deactivation of product
	アップデート	Start update of product
set		**Set options for product**
	コンフィグレーション	Set configuration to product

In the output result of every command, the first information displayed is result ID. To understand better the result information, check the table of IDs below.

Error ID	Error	Description
0	Success	
1	Command node not present	"Command" node not present in input json
2	Command not supported	Particular command is not supported
3	General error executing the command	Error during execution of command
4	Task already running	Requested task is already running and has not been started
5	Invalid parameter for command	Bad user input
6	Command not executed because it's disabled	RMM isn't enabled in advanced settings or isn't started as an administrator

ERMM JSONコマンドのリスト

- 保護ステータスの取得
- アプリケーション情報の取得
- ライセンス情報の取得

- ログの取得
- アクティベーションステータスの取得
- 検査情報の取得
- 設定の取得
- アップデートステータスの取得
- 検査の開始
- アクティベーションの開始
- アクティベーション解除の開始
- アップデートの開始
- 構成の設定

get protection-status

Get the list of application statuses and the global application status

Command line

```
ermm.exe get protection-status
```

Parameters

None

Example

call

```
{
"command":"get_protection_status",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"statuses":[{
"id":"EkrnNotActivated",
"status":2,
"priority":768,
"description":"Product not activated"
}],
"status":2,
"description":"Security alert"
},
"error":null
}
```


get application-info

Get information about the installed application

Command line

```
ermm.exe get application-info
```

Parameters

None

Example

call


```
{
"command":"get_application_info",
"id":1,
"version":"1"
}
```


result

```
{
"id":1,
"result":{
"description":"ESET Endpoint Antivirus",
"version":"6.6.2018.0",
"product":"eea",
"lang_id":1033,
"modules":[{
"id":"SCANNER32",
"description":"Detection engine",
"version":"15117",
"date":"2017-03-20"
},{
"id":"PEGASUS32",
"description":"Rapid Response module",
"version":"9734",
"date":"2017-03-20"
},{
"id":"LOADER32",
"description":"Update module",
"version":"1009",
"date":"2016-12-05"
},{
"id":"PERSEUS32",
"description":"Antivirus and antispyware scanner module",
"version":"1513",
"date":"2017-03-06"
},{
"id":"ADVHEUR32",
"description":"Advanced heuristics module",
"version":"1176",
"date":"2017-01-16"
},{
"id":"ARCHIVER32",
"description":"Archive support module",
"version":"1261",
"date":"2017-02-22"
},{
"id":"CLEANER32",
"description":"Cleaner module",
"version":"1132",
"date":"2017-03-15"
},{
"id":"ANTISTEALTH32",
"description":"Anti-Stealth support module",
"version":"1106",
"date":"2016-10-17"
},{
"id":"SYSTEMSTATUS32",
"description":"ESET SysInspector module",
"version":"1266",
"date":"2016-12-22"
},{
"id":"TRANSLATOR32",
"description":"Translation support module",
"version":"1588B",
"date":"2017-03-01"
},{
"id":"HIPS32",
"description":"HIPS support module",
"version":"1267",
"date":"2017-02-16"
},{
"id":"PROTOSCAN32",
"description":"Internet protection module",
"version":"1300",
"date":"2017-03-03"
},{
"id":"DBLITE32",
"description":"Database module",
"version":"1088",
"date":"2017-01-05"
},{
"id":"CONFENG32",
"description":"Configuration module (33)",
"version":"1496B",
"date":"2017-03-17"
},{
"id":"IRIS32",
"description":"LiveGrid communication module",
"version":"1022",
"date":"2016-04-01"
},{
"id":"SAURON32",
"description":"Rootkit detection and cleaning module",
"version":"1006",
"date":"2016-07-15"
},{
"id":"SSL32",
"description":"Cryptographic protocol support module",
"version":"1009",
"date":"2016-12-02"
}
},
"error":null
}
}
```

get license-info

Get information about the license of the product

Command line

```
ermm.exe get license-info
```

Parameters

None

Example

call

```
{
"command":"get_license_info",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"type":"NFR",
"expiration_date":"2020-12-31",
"expiration_state":"ok",
"public_id":"3XX-7ED-7XF",
"seat_id":"6f726793-ae95-4e04-8ac3-e6a20bc620bf",
"seat_name":"M"
},
"error":null
}
```

get logs

Get logs of the product

Command line

```
ermm.exe get logs --name warnlog --start-date "2017-04-04 06-00-00" --end-
date "2017-04-04 12-00-00"
```

Parameters

Name	Value
name	{ all, virlog, warnlog, scanlog, blocked, hipslog, urllog, devctrllog } : log to retrieve
start-date	start date from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
end-date	end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])

Example

call

```
{
"command":"get_logs",
"id":1,
"version":"1",
"params":{
"name":"warnlog",
"start_date":"2017-04-04 06-00-00",
"end_date":"2017-04-04 12-00-00"
}
}
```

result

```
{
"id":1,
"result":{
"warnlog":{
"display_name":"Events",
"logs":[{
"Time":"2017-04-04 06-05-59",
"Severity":"Info",
"PluginId":"ESET Kernel",
"Code":"Malware database was successfully updated to version 15198 (20170404).",
"UserData":""
},{
"Time":"2017-04-04 11-12-59",
"Severity":"Info",
"PluginId":"ESET Kernel",
"Code":"Malware database was successfully updated to version 15199 (20170404).",
"UserData":""
}]
}
},
"error":null
}
```

get activation-status

Get information about the last activation. Result of status can be {

success, error }

Command line

```
ermm.exe get activation-status
```

Parameters

None

Example

call

```
{
"command":"get_activation_status",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"status":"success"
},
"error":null
}
```

get scan-info

Get information about running scan.

Command line

```
ermm.exe get scan-info
```

Parameters

None

Example

call

```
{
"command":"get_scan_info",
"id":1,
"version":"1"
}
```

result


```
{
"id":1,
"result":{
"scan-info":{
"scans":[{
"scan_id":65536,
"timestamp":272,
"state":"finished",
"pause_scheduled_allowed":false,
"pause_time_remain":0,
"start_time":"2017-06-20T12:20:33Z",
"elapsed_tickcount":328,
"exit_code":0,
"progress_filename":"Operating memory",
"progress_arch_filename":"",
"total_object_count":268,
"infected_object_count":0,
"cleaned_object_count":0,
"log_timestamp":268,
"log_count":0,
"log_path":"C:\\ProgramData\\ESET\\ESET Security\\Logs\\eScan\\ndl31494.dat",
"username":"test-PC\\test",
"process_id":3616,
"thread_id":3992,
"task_type":2
}],
"pause_scheduled_active":false
}
},
"error":null
}
```


get configuration

Get the product configuration. Result of status may be { success, error }

Command line

```
ermm.exe get configuration --file C:\tmp\conf.xml --format xml
```

Parameters

Name	Value
file	the path where the configuration file will be saved
format	format of configuration: json, xml. Default format is xml

Example

call

```
{
"command":"get_configuration",
"id":1,
"version":"1",
"params":{
"format":"xml",
"file":"C:\\tmp\\conf.xml"
}
}
```

result

```
{
"id":1,
"result":{
"configuration":"PD94bWwgdmVyc2lvbj0iMS4w=="
},
"error":null
}
```

get update-status

Get information about the update. Result of status may be { success, error }

Command line

```
ermm.exe get update-status
```

Parameters

None

Example

call

```
{
"command":"get_update_status",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"last_update_time":"2017-06-20 13-21-37",
"last_update_result":"error",
"last_successful_update_time":"2017-06-20 11-21-45"
},
"error":null
}
```

start scan

Start scan with the product

Command line

```
ermm.exe start scan --profile "profile name" --target "path"
```

Parameters

Name	Value
profile	Profile name of On-demand computer scan defined in product
target	Path to be scanned

Example

call

```
{
"command":"start_scan",
"id":1,
"version":"1",
"params":{
"profile":"Smart scan",
"target":"c:\\"
}
}
```

result

```
{
"id":1,
"result":{
"task_id":458752
},
"error":null
}
```

start activation

Start activation of product

Command line

```
ermm.exe start activation --key "activation key" | --offline "path to offline file"
```

Parameters

Name	Value

key	Activation key
offline	Path to offline file

Example

call

```
{
"command":"start_activation"
"id":1,
"version":"1",
"params":{
"key":"XXXX-XXXX-XXXX-XXXX-XXXX"
}
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

start deactivation

Start deactivation of the product

Command line

```
ermm.exe start deactivation
```

Parameters

None

Example

call

```
{
"command":"start_deactivation",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

start update

Start update of the product. Only one update may be running in the product so in case the update is already running, "Task already running" error code is returned

Command line

```
ermm.exe start update
```

Parameters

None

Example

call

```
{
"command":"start_update",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
},
"error":{
"id":4,
"text":"Task already running."
}
}
```

set configuration

Set configuration to the product. Result of status may be { success, error }

Command line

```
ermm.exe set configuration --file C:\tmp\conf.xml --format xml --password pass
```

Parameters

Name	Value
file	the path where the configuration file will be saved

password	password for configuration
value	configuration data from the argument (encoded in base64)

Example

call

```
{
"command":"set_configuration",
"id":1,
"version":"1",
"params":{
"format":"xml",
"file":"C:\\tmp\\conf.xml",
"password": "pass"
}
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

よくある質問

この章では、よくある質問と問題をいくつか説明します。問題の解決方法を調べるには、該当するトピックをクリックしてください。

- ESET Endpoint Securityをアップデートする方法
- ESET Endpoint Securityをアクティベートする方法
- 現在の認証情報を使用して新しい製品をアクティベートする方法
- PCからウイルスを取り除く方法
- アプリケーションに通信を許可する方法
- スケジューラで新しいタスクを作成する方法
- 週次コンピューター検査をスケジュールする方法
- 製品をESET Security Management Centerに接続する方法
上書きモードを使用する方法
- ESET Endpoint Securityの推奨されたポリシーを適用する方法
- ミラーを構成する方法
- ESET Endpoint Securityがインストールされた状態でWindows 10にアップグレードする方法
- リモート監視と管理をアクティブ化する方法

- インターネットから特定のファイルタイプのダウンロードをブロックする方法
- ESET Endpoint Securityユーザーインターフェースを最小化する方法

上記ヘルプページのリストに含まれていない問題の場合は、問題をよく表現しているキーワードまたは語句を使用してESET Endpoint Securityヘルプページ内を検索してみてください。

ヘルプページで問題や疑問への解決策が見つからない場合は、ESETナレッジベースにアクセスし、一般的な問題や質問への回答を検索します。

- ファイルコーダー(ランサムウェア)マルウェアから保護するためのベストプラクティス
- ESET Endpoint SecurityおよびESET Endpoint Antivirus FAQ
- ESMCでのRDP接続を許可するファイアウォールルールを作成または編集します
- ESET製品の完全な機能を許可するためには、他社製のファイアウォールでどのアドレスとポートを開く必要がありますか。

必要に応じて、問題/質問について当社のオンラインテクニカルサポートセンターまでお問い合わせいただくこともできます。オンラインお問い合わせフォームへのリンクは、メインプログラムウィンドウの**[ヘルプとサポート]**ページにあります。

ESET Endpoint Securityをアップデートする方法

ESET Endpoint Securityは、手動または自動で更新できます。 更新を開始するには、メインプログラムウィンドウの[**アップデート**]をクリックしてから、[**アップデートの確認**]をクリックします。

既定のインストール設定では、1時間ごとに実行される自動更新タスクが作成されます。間隔を変更するには、**ツール > スケジューラー**に移動します(スケジューラーの詳細を参照)。

ESET Endpoint Securityをアクティベートする方法

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。

製品のアクティベーションには、いくつかの方法があります。[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(ESET Webページ、インストーラータイプ .msi または .exe など)によって異なります。

プログラムから直接ESET Endpoint Securityのコピーをアクティベーションするには、ESET Endpoint Securityメインプログラムウィンドウを開き、メインメニューで**ヘルプとサポート > 製品のアクティベーション**または**保護の状態 > 製品のアクティベーション**を選択します。

ESET Endpoint 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。

- **購入した製品認証キーを使用** - 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** – 認証情報(電子メールアドレスとパスワード)を使用して、ESET Business Accountポータルで作成されたアカウント。この方法では、1つの場所から複数のライセンスを管理できます。

- **オフラインライセンス** – 自動生成されたファイルをESET製品に転送され、ライセンス情報を提供します。ライセンスによってオフラインライセンスファイル(.lf)をダウンロードできる場合は、このファイルを使用してオフラインアクティベーションを実行できます。オフラインライセンス数は、使用可能な合計ライセンス数から減算されます。オフラインファイルの生成の詳細については、ESET Business Accountユーザーガイドを参照してください。

コンピュータが管理対象ネットワークのメンバーで、管理者がESET Security Management Center経由でリモートアクティベーションを実行する場合は、**[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。

ユーザー名とパスワードが古いESET製品のアクティベーションで使用されるESET Endpoint Securityをアクティベーションする方法がわからない場合、レガシー資格情報を製品認証キーに変換します。

製品のアクティベーションが失敗した場合

製品ライセンスはいつでも変更できます。変更するには、メインプログラムウィンドウで**[ヘルプとサポート] > [ライセンスの変更]**をクリックしますESETサポートへのライセンスを識別するための公開ライセンス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 Security Management Center 7.2またはESET PROTECT 8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ーをアクティベーションできます。手順については、『ESET PROTECTオンラインヘルプ』を参照してください。

アクティベーション中の製品認証キーの入力

自動アップデートはセキュリティのために重要ですESET Endpoint Securityは、**ライセンスキー**を使用してアクティベーションが完了した後にのみアップデートを受信します。

インストール後に製品認証キーを入力していない場合は、製品がアクティベーションされません。メインプログラムウィンドウでライセンスを変更できます。 このためには、**ヘルプとサポート > ライセンスのアクティベーション**をクリックし、受け取ったESETセキュリティ製品のライセンスデータを[製品のアクティベーション]ウィンドウに入力します。

[製品認証キー]は、書かれている通りに入力する必要があります。

- ライセンスキーは、XXXX-XXXX-XXXX-XXXX-XXXXの形式の一意の文字列です。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。

正確性を保つためにも、登録メールからコピーしてペーストすることを強くお勧めします。

ESET Business Accountへのログイン

セキュリティ管理アカウントは、**電子メールアドレス**と**パスワード**を使用してESET Business Accountポータルで作成されたアカウントです。このアカウントでは、すべてのシート権限を見ることができます。セキュリティ管理アカウントでは、複数のライセンスを管理できます。セキュリティ管理アカウントがない場合は、**[アカウントの作成]**をクリックし、ESET Business Account ポータルに移動すると、認証情報を登録できます。

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 Business Accountポータルに移動します。電子メールアドレスを入力し、**サインイン**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。

レガシーライセンス認証情報を使用して、新しいESETエンドポイント製品をアクティベーションする方法

ユーザー名とパスワードがあり、ライセンスキーを受け取りたい場合は、ESET Business Accountポータルにアクセスし、認証情報を新しいライセンスキーに変換できます。

PCからウイルスを取り除く方法

使用しているコンピュータが、マルウェアに感染している兆候(処理速度が遅くなる、頻繁にフリーズするなど)を示している場合、次の処置を取ることをお勧めします。

1. プログラムのメインウィンドウで、[**コンピュータの検査**]をクリックします。

2. [**スマート検査**]をクリックし、システムの検査を開始します。

3. スキャンが完了したら、スキャンされたファイル、感染しているファイル、および駆除されたファイルの数をログで確認します。

4. ディスクの一部のみをスキャンするには、[**カスタム検査**]をクリックし、ウイルスをスキャンする対象を選択します。

詳細については、定期的に更新されるESETナレッジベース記事を参照してください。

アプリケーションに通信を許可する方法

対話モードで新しい接続が検出された場合、適合するルールがなければ、接続を許可するか拒否するかを決定する必要があります。ESET Endpoint Securityで、アプリケーションが接続を確立しようとするたびに同じアクションを実行するには、[**アクションを記憶する(ルールを作成する)**]チェックボックスをチェックします。



ESET Endpoint Securityで検出される前に、ファイアウォール設定ウィンドウでアプリケーション用の新しいファイアウォールルールを作成できます。メインプログラムウィンドウ > **設定 > ネットワーク > ファイアウォール** > 歯車をクリック > **設定 > 詳細 > ルール**を開き、**編集**をクリックします。

[追加]をクリックしてルールを追加します。[**一般**]タブで、ルールの名前、方向、および通信プロトコルを入力します。このウィンドウでは、ルールが適用されたときに実行するアクションを定義することができます。

[**ローカル**]タブで、アプリケーションの実行可能ファイルのパスとローカルの通信ポートを入力します。[**リモート**]タブをクリックして、リモードアドレスとリモートポートを入力します(該当する場合)。アプリケーションが再度通信しようとするとすぐに、新しく作成したルールが適用されます。

スケジューラで新しいタスクを作成する方法

[**ツール**]>[**スケジューラ**]で新しいタスクを作成するには、[**追加...**]をクリックするか、または右クリックしてコンテキストメニューから[**追加**]を選択します。次の5種類のスケジュールされたタスクが使用可能です。

- **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。

- **コンピュータの状態のスナップショットを作成する** – ドライバー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。

- **コンピュータの検査** – コンピュータ上のファイルやフォルダに関するコンピュータの検査を実行します。

- **アップデート**– 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。

スケジュールされたタスクの中で[**アップデート**]が最もよく使用されるので、新しいアップデートタスクを追加する方法を説明します。

[**スケジュールタスク**]ドロップダウンメニューから[**アップデート**]を選択します。[**タスク名**]フィールドにタスクの名前を入力し、[**次へ**]をクリックします。タスクの頻度を選択します。使用可能なオプションは次のとおりです。**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]**を選択すると、ノートブックコンピュータのバッテリ電源での実行中に、システムリソースを最小化できます。タスクは、**[タスク実行]**フィールドで指定された日時に実行されます。次に、スケジュールされた時刻にタスクを実行できない場合や完了できない場合に実行するアクションを定義します。使用可能なオプションは次のとおりです。

- **次のスケジュール設定日時まで待機**

- **実行可能になり次第実行する**

- **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**スクロールボックスを使用して間隔を定義できます)

次のステップでは、現在のスケジュールされたタスクに関する情報が含まれる概要ウィンドウが表示されます。変更が完了したら、**[完了]**をクリックします。

ダイアログウィンドウが表示され、スケジュールされたタスクに使用するプロファイルを選択することができます。ここでは、プライマリプロファイルと代替プロファイルを設定できます。プライマリプロファイルを使用してタスクを完了できない場合は、代替プロファイルが使用されます。**[完了]**をクリックして確認し、新しくスケジュールされたタスクが、現在スケジュールされているタスクのリストに追加されます。

週次コンピューター検査をスケジュールする方法

定期的なタスクをスケジュールするには、プログラムのメインウィンドウを開き、[**ツール**]>[**スケジューラ**]をクリックします。 タスクをスケジュールする手順は次のとおりです。このタスクによって、ローカルドライブの検査が毎週実行されます。 詳細な説明については、ナレッジベース記事を参照してください。

スキャンタスクをスケジュールするには:

1. スケジューラのメイン画面で[**追加**]をクリックします。

2. ドロップダウンメニューから[**コンピュータの検査**]を選択します。

3. タスクの名前を入力し**タスクの頻度に[毎週]**を選択します。

4. タスクを実行する日時を設定します。

5. スケジュールされたタスクの実行が何らかの理由で実行しない場合(コンピューターがオフの場合など)は、**[実行可能になりしだい実行する]**を選択して、後からタスクを実行します。

6. スケジュールされたタスクの概要を確認し、[**完了**]をクリックします。

7. [**対象**]ドロップダウンメニューから[**ローカルドライブ**]を選択します。

8. [**完了**]をクリックすると、タスクが適用されます。

ESET Endpoint SecurityをESET PROTECTに接続する方法

コンピューターにESET Endpoint Securityをインストールし、ESET PROTECT経由で接続するときには、必ず、クライアントワークステーション上にESET Managementエージェントもインストールしたことを確認してください。これはESMCサーバーと通信するすべてのクライアントソリューションの不可欠の要素です。

- クライアントワークステーションにESET Managementエージェントをインストールまたは展開する

参照:

- リモート管理されたエンドポイントのドキュメント
- 上書きモードを使用する方法
- ESET Endpoint Securityの推奨されたポリシーを適用する方法

上書きモードを使用する方法

ESET Endpoint製品 for Windowsバージョン6.5以上)がコンピューターにインストールされている場合は、上書き機能を使用できます。上書きモードでは、設定が適用されたポリシーがある場合でも、クライアントコンピューターレベルで、インストールされたESET製品の設定を変更できます。上書きモードは、特定のADユーザーで有効にするか、パスワードで保護できます。この機能は、1回で4時間を超えると有効にできません。

- 上書きモードを1度有効にするとESMC Webコンソールから停止できます。上書き期間が終了すると、上書きモードは自動的に無効化されます。クライアントコンピューターでオフにすることもできます。
- 上書きモードを使用しているユーザーも、Windows管理者権限が必要です。それ以外の場合、ユーザーはESET Endpoint Securityの設定で変更を保存できません。
- Active Directoryグループ認証は、ESET Endpoint Securityバージョン7.0.2100.4以降でサポートされています。

上書きモードを設定するには

1. **ポリシー > 新しいポリシー**に移動します。

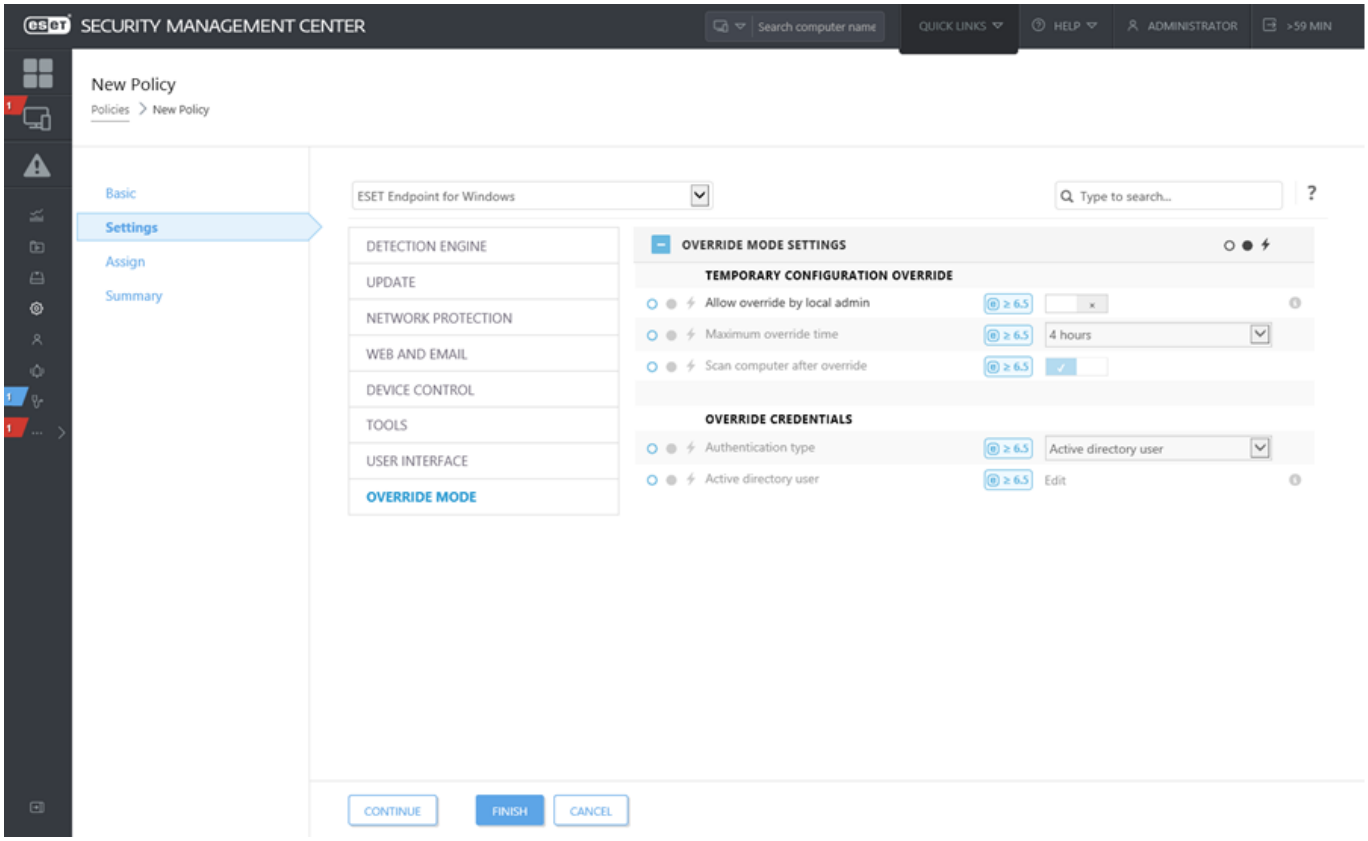
2. [**基本**]セクションに、このポリシーの**名前**と**説明**を入力します。

3. [**設定**]画面で、**[ESET Endpoint for Windows]**を選択します。

4. [**上書きモード**]をクリックし、上書きモードのルールを設定します。

5.[**割り当て**]セクションで、このポリシーが適用されるコンピューターまたはコンピューターのグループを選択します。

6. [**サマリー**]セクションで、[**完了**]をクリックしてポリシーを適用します。



*John*のエンドポイント設定に問題があり、一部の重要な機能またはWebアクセスがコンピューターでブロックされる場合、管理者は*John*が既存のエンドポイントポリシーを上書きし、コンピューターで手動で設定を調整できるようにすることができます。後から、これらの新しい設定はESMCで要求されるため、管理者はそこから新しいポリシーを作成できます。
手順は次のとおりです。
1.**ポリシー > 新しいポリシー**に移動します。
2.**名前**および**説明**フィールドを入力します。[**設定**]画面で、**[ESET Endpoint for Windows]**を選択します。
3.[**上書きモード**]をクリックし、1時間上書きモードを有効にしADユーザーとして*John*を選択します。
4.*John*のコンピューターにポリシーを割り当て、[**完了**]をクリックしてポリシーを保存します。
5.*John*はESETエンドポイントで**上書きモード**を有効にし、コンピューターで手動で設定を変更する必要があります。
6.ESMC Webコンソールで、[**コンピューター**]に移動し、 *John*のコンピューターをクリックして、[**詳細を表示**]をクリックします。
7.[**設定**]セクションで、[**設定の要求**]をクリックして、クライアントタスクをスケジュールして、クライアントから設定をすぐに取得します。
8.少したった後、新しい設定が表示されます。設定を保存する製品をクリックし、[**設定を開く**]をクリックします。
9.設定を確認し、[**ポリシーに変換**]をクリックできます。
10.**名前**および**説明**フィールドを入力します。
11.[**設定**]セクションでは、必要に応じて設定を変更できます。
12.[**割り当て**]セクションで、このポリシーを*John*のコンピューター(またはその他)に割り当てることができます。
13.[**完了**]をクリックして設定保存します。
14.必ず、必要がなくなった時点で、上書きポリシーを削除してください。

ESET Endpoint Securityの推奨されたポリシーを適用する方法

ESET Endpoint SecurityをESET Security Management Centerに接続した後のベストプラクティスは、推奨されたポリシーを適用するか、カスタムポリシーを適用することです。

ESET Endpoint Securityには複数の定義済みポリシーがあります。

ポリシー	説明
ウイルス対策 – バランス重視	ほとんどの設定に推奨されるセキュリティ設定。
ウイルス対策 – 最大限のセキュリティ	機械学習、詳細動作検査SSLフィルタリングを活用します。安全では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、不審な可能性があるアプリケーションの検出に影響します。
クラウドベースのレピュテーションおよびフィードバックシステム	ESET LiveGrid®クラウドベースのレピュテーションおよびフィードバックシステムは、最新の脅威の検出を向上し、悪意あるまたは未知の脅威を分析するのに役立ちます。
デバイスコントロール – 最大限のセキュリティ	すべてのデバイスがブロックされます。デバイスを接続する場合は、管理者によって許可される必要があります。
デバイスコントロール – 読み取り専用	すべてのデバイスが読み取り専用です。書き込みはできません。

ポリシー	説明
ファイアウェール - ESMC & EEI接続を除くすべてのトラフィックをブロック	ESET Security Management CenterおよびESET Enterprise Inspector Server (ESET Endpoint Securityのみ)への接続を除くすべてのトラフィックをブロックします。
ログ – 完全診断ログ	このテンプレートは、必要な場合に、管理者が使用可能なすべてのログを取得できることを保証しますHIPSとThreatsenseパラメーター、ファイアウォールを含む最小の詳細レベルからすべてが記録されます。90日が経過すると、ログは自動的に削除されます。
ログ – 重要なイベントのみを出力	ポリシーは、警告、エラー、重大なイベントが記録されることを保証します。ログは90日を経過すると自動的に削除されます。
表示 – バランス重視	詳細レベルの既定の設定。ステータスと通知が無効です。
表示 – 非表示モード	通知、アラート、GUIのコンテキストメニューとの統合が無効です。egui.exeは実行されません。ESET PROTECT Cloudのみからの管理に適しています。
表示 – ユーザーの操作を減らす	ステータスと通知が無効で、GUIは表示されます。

ワークステーションにインストールされたESET Endpoint Security向けに51個以上の推奨設定を施行する**ウイルス対策 – 最大限のセキュリティ**のポリシーを設定するには、次の手順に従います。

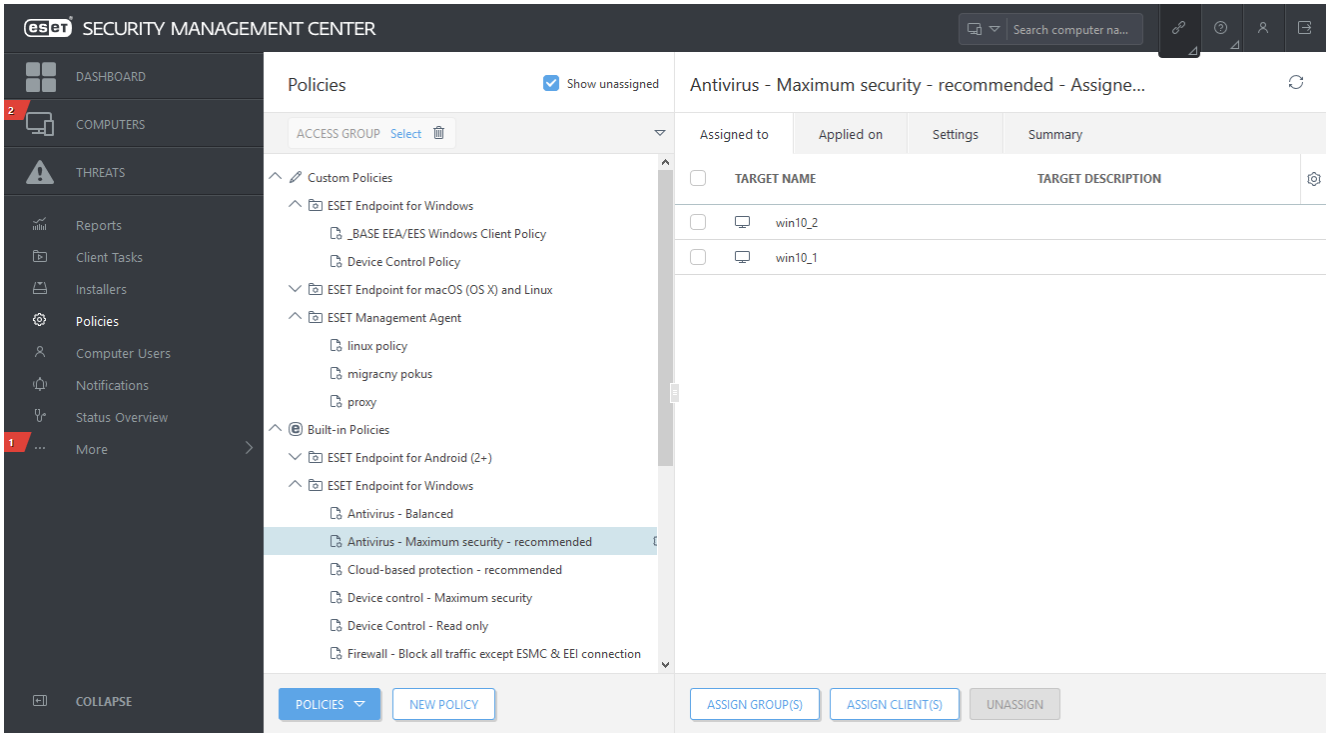
次のESETナレッジベース記事は、英語でのみ提供されている場合があります。
- ESMCを使用してESET Endpoint Securityの推奨または定義済みポリシーを適用する

1. ESMC Webコンソールを開きます。

2. **ポリシー**に移動して、**ビルトインポリシー** > **ESET Endpoint for Windows**を展開します。

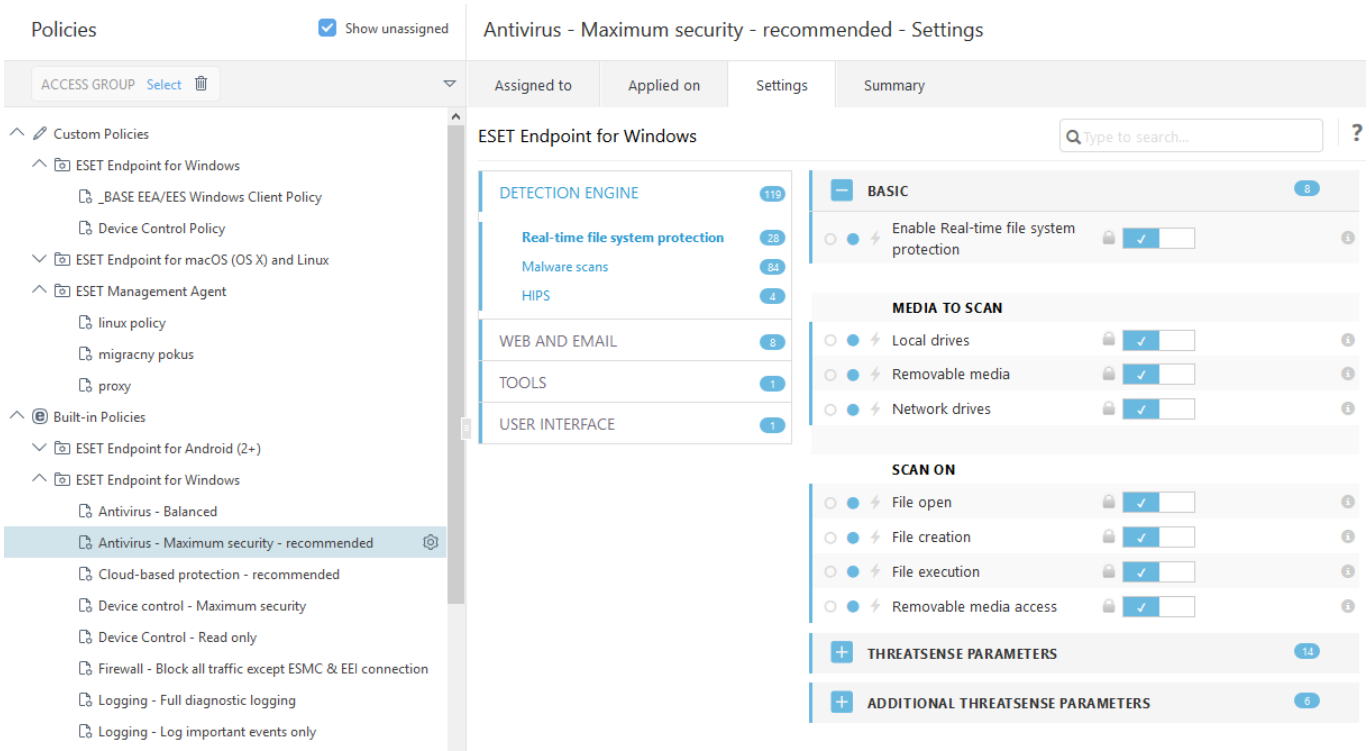
3. **ウイルス対策 – 最大限のセキュリティ – 推奨**をクリックします。

4**割り当て先**タブで、**クライアントの割り当て**または**グループの割り当て**をクリックし、このポリシーを適用する適切なコンピューターを選択します。



このポリシーに適用される設定を確認するには、**設定**タブをクリックして、詳細設定ツリーを展開します。

- 青色の点は、このポリシーの変更された設定を表します。
- 青色の枠の中の数字は、このポリシーによって変更された設定数を表します。
- ESMCポリシーの詳細



ミラーを構成する方法

ESET Endpoint Securityはウイルスアップデートファイルのコピーを保存し、ESET Endpoint SecurityまたはESET Endpoint Antivirusを実行している他のワークステーションにアップデートを配布するように構成できます。

ESET Endpoint Securityをミラーとして構成し、内部HTTPサーバー経由でアップデートを配布する

1. **F5**を押して、詳細設定にアクセスし、**アップデート > プロファイル > アップデートミラー**を展開します。

2. **アップデート**を展開し、**モジュールアップデート**の**自動的に選択**オプションが有効になっていることを確認します。

3. **アップデートミラー**を展開し、**アップデートミラーを作成する**と**HTTPサーバーを有効にする**を有効にします。

詳細については、「アップデートミラー」を参照してください。

共有ネットワークフォルダ経由でアップデートを配布するようにミラーサーバーを構成する

1. ローカルまたはネットワークドライブで共有フォルダを作成します。このフォルダはESETセキュリティソリューションを実行するすべてのユーザーによって読み取られ、ローカルSYSTEMアカウントから書き込み可能でなければなりません。

2. **詳細設定 > アップデート > プロファイル > アップデートミラー**の下で、**アップデートミラーを作成する**を有効にします。

3. **クリア**→**編集**の順にクリックして、該当する**保存フォルダー**を選択します。作成された共有フォルダーを選択します。

> 内部HTTPサーバー経由でモジュールのアップデートを提供しない場合は、**アップデートミラーを作成する**を無効にします。

ESET Endpoint Securityがインストールされた状態でWindows 10にアップグレードする方法

> 最新バージョンのESET製品にアップグレードしてから、最新のモジュールアップデートをダウンロードした後に、Windows 10にアップグレードすることを強くお勧めします。 これにより、最大の保護が保証されWindows 10へのアップグレード中にプログラム設定とライセンス情報が保持されます。

バージョン7.x:

Microsoft Windows 10にアップグレードする準備をするために、以下の該当するリンクをクリックして、最新バージョンをダウンロードおよびインストールしてください。

ESET Endpoint Security 7 32ビットのダウンロード ESET Endpoint Antivirus 7 32ビットのダウンロード

ESET Endpoint Security 7 64ビットのダウンロード ESET Endpoint Antivirus 7 64ビットのダウンロード

バージョン5.x:

バージョン5のESET Endpoint製品は、現在、サポートが終了しています。つまり、ビルドはダウンロード用に公開されていません。最新バージョンのESET Endpoint製品にアップグレードすることを強くお勧めします。

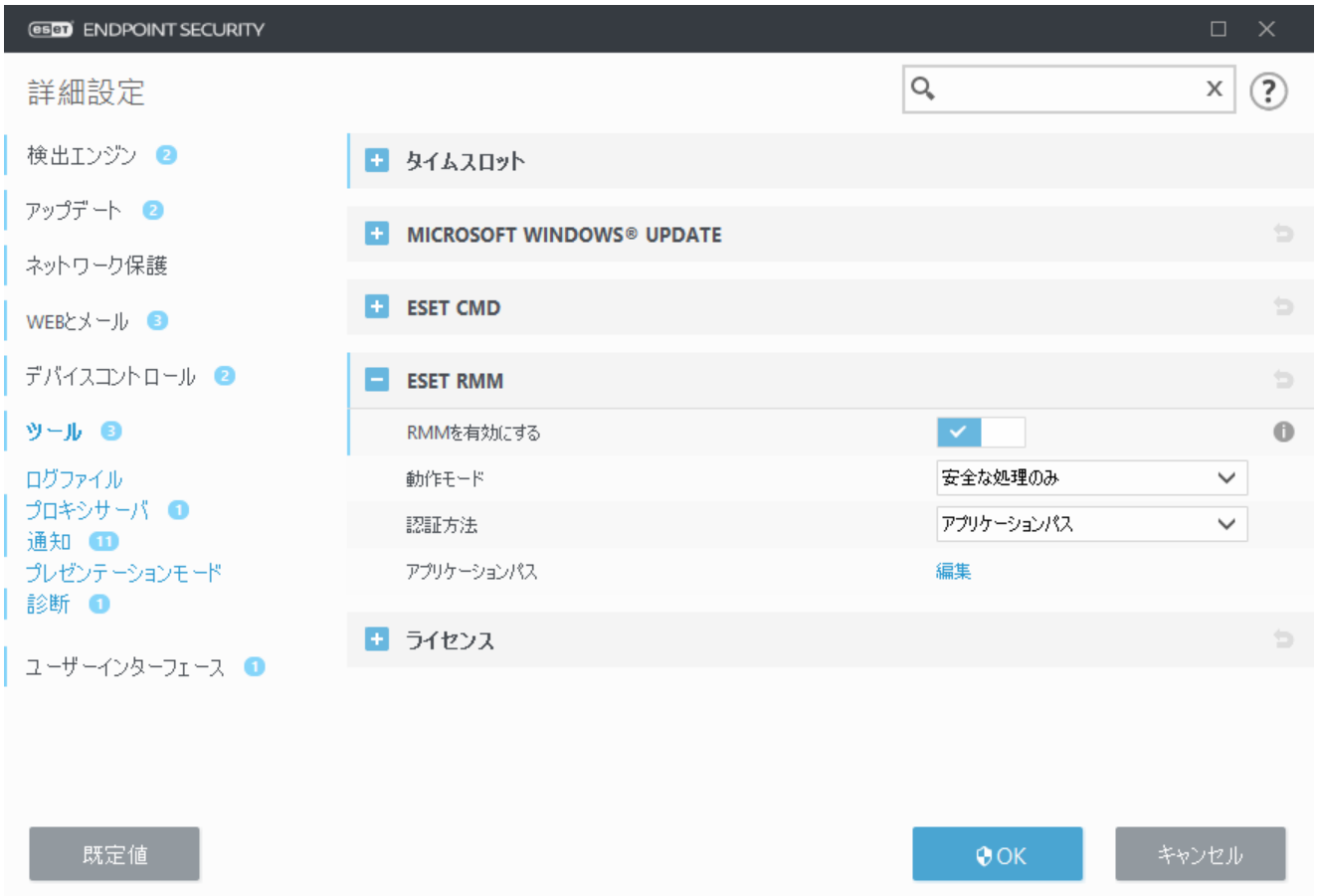
その他の言語バージョン:

別の言語バージョンのESETエンドポイント製品を探している場合は、ESETのダウンロードページをご覧ください

ESETビジネス製品とWindows 10の互換性に関する情報

リモート監視と管理をアクティブ化する方法

リモート監視と管理(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、モバイルデバイスにインストールされたシステムなど)を監視および制御するプロセスですESETEndpointSecurityは、バージョン6.6.2028.0からRMMで管理できます。



既定ではESET RMMは無効ですESET RMMを有効にするには、**F5**を押して詳細設定にアクセスし、**ツール**をクリックして、**ESET RMM**を展開し、**RMMを有効にする**の横のスイッチをオンにします。

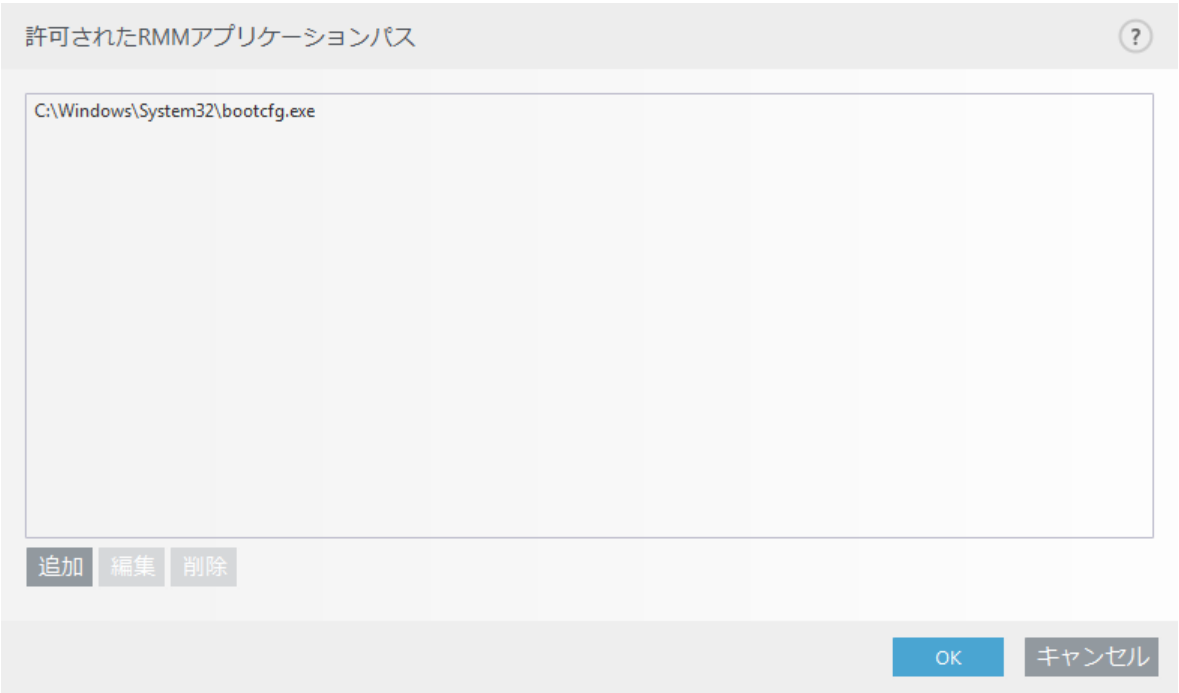
動作モード – 安全な読み取り専用操作用にRMMインターフェースを有効にする場合は、**安全な操作のみ**を選択します。すべての操作でRMMインターフェースを有効にする場合は、**すべての操作**を選択します。

処理	モード安全な操作のみ	モードすべての操作
アプリケーション情報の取得	✔	✔
設定の取得	✔	✔
ライセンス情報の取得	✔	✔
ログの取得	✔	✔
保護の状態の取得	✔	✔
アップデート状態の取得	✔	✔
構成の設定		✔
アクティベーションの開始		✔
検査の開始	✔	✔
アップデートの開始	✔	✔

認証方法 – RMM認証方法を設定します。認証を使用するには、ドロップダウンメニューから**[アプリケーションパス]**を選択するか、**[なし]**を選択します。

RMMは常に認証を使用し、悪意のあるソフトウェアがESETエンドポイント保護を無効化または回避できないようにする必要があります。

アプリケーションパス – RMMを実行できる特定のアプリケーション。認証方法として**アプリケーションパス**を選択した場合は、**編集**をクリックして、**許可されたRMMアプリケーションパス**設定ウィンドウを開きます。



追加 – 新しい許可されたRMMアプリケーションパスを作成します。パスを入力するか、**...**ボタンをクリックして実行ファイルを選択します。

[編集] – 既存の許可されたパスを変更します。実行ファイルの場所が別のフォルダーに変更された場合は、**[編集]**を使用します。

[**削除**] – 既存の許可されたパスを削除します。

既定のESET Endpoint Securityインストールには□Endpointアプリケーションディレクトリ(既定のパスC:*Program Files**ESET**ESET Security*)にあるermm.exeファイルがあります□ermm.exeはRMMエージェントと通信し、RMMサーバーにリンクされたRMMプラグインとデータを交換します。

- ermm.exe – ESETによって開発されたコマンドラインユーティリティで、Endpoint製品の管理とRMMプラグインとの通信ができます。
- RMMプラグインはEndpoint Windowsシステムでローカルで実行される他社のアプリケーションです。このプラグインは、特定のRMMエージェント(Kaseyaのみなど)とermm.exeと通信するために設計されました。
- RMMエージェントはEndpoint Windowsシステムでローカルで実行される他社のアプリケーションです。エージェントはRMMプラグインとRMMサーバーと通信します。

インターネットから特定のファイルタイプのダウンロードをブロックする方法

インターネットから特定のファイルタイプ(exe□pdf□zipなど)のダウンロードを許可しない場合は、URLアドレス管理とワイルドカードを組み合わせて使用します□F5キーを押すと、**詳細設定**が表示されます。**[Webとメール]** > **[Webアクセス保護]**をクリックし、**[URLアドレス管理]**を展開します。**アドレスリスト**の横の[**編集**]をクリックします。

アドレスリストウィンドウで、**ブロックされたアドレスのリスト**を選択し、**編集**をクリックするか、**追加**をクリックして、新しいリストを作成します。新しいウィンドウが開きます。新しいリストを作成している場合は、**アドレスリストタイプ**ドロップダウンメニューから**ブロック**を選択し、リスト名を指定します。現在のリストからファイルタイプにアクセスするときに通知する場合は、**適用するときに通知**サイドバーを有効にします。ドロップダウンメニューから**ログの重要度**を選択します□Remote Administratorは、レコードと**警告**の詳細レベルを収集できます。



[追加]をクリックすると、ダウンロードをブロックするファイルタイプを指定するマスクを入力できます。特定のWebサイトからの特定のファイルのダウンロードをブロックする場合は、完全なURL (例: *http://example.com/file.exe*) を入力します。ワイルドカードを使用すると、複数のファイルを指定することができます。疑問符 (?) は1つの可変文字を表し、アスタリスク (*) は0文字以上の可変文字列を表します。たとえば、マスク **/*.zip*は、すべてのzip圧縮されたファイルのダウンロードをブロックします。

ファイル拡張子がファイルURLの一部であるときに、この方法を使用して、特定のファイルタイプのダウンロードのみをブロックできますWebページでファイルダウンロードURLを使用する場合 (例: *www.example.com/download.php?fileid=42*)、このリンクにあるすべてのファイルは、拡張子をブロックした場合でも、ダウンロードされます。

ESET Endpoint Securityユーザーインターフェースを最小化する方法

リモートで管理するときには、「表示」定義済みポリシーを適用できます。

そうでない場合は、手動で次の手順を実行します。

1. **F5**キーを押して詳細設定を開き、**ユーザーインターフェース > ユーザーインターフェース要素**を展開します。

2. **起動モード**を必要な値に設定します。起動モードの詳細について

3. **起動時にスプラッシュ画面を表示**と**サウンド信号を使用**を無効にします。

4. 通知を設定します。

5. アプリケーションステータスを設定します。

6. 確認メッセージを設定します。

7. アラートとメッセージボックスを設定します。

「安全なブラウザーを要求されたWebページにリダイレクトできませんでした」を解決する方法

このエラーを解決するには、次の手順に従います。

各手順を完了した後、安全なブラウザーが動作しているかどうかを確認します。
ブラウザーウィンドウが動作していない場合、動作するまで、次の手順を完了します。

1. ESET製品のメインプログラムウィンドウが開きます。

2. **ツール** > **安全なブラウザー**をクリックします。安全なブラウザーウィンドウが開くので、次の手順に進みます。



3. ブラウザーキャッシュを消去します。自分のブラウザーで Firefoxキャッシュ または Google Chrome キャッシュ を消去する方法

4. 最新バージョンのWindowsオペレーティングシステムとESET Windowsビジネス製品を使用していることを確認します。最新バージョンのESETビジネス製品を確認します。

5. 安全なブラウザーを無効に し、コンピューターを再起動します。安全なブラウザーを再度有効にし、安全なブラウザーウィンドウを開くことを試みます。

6. 既定のブラウザーが**詳細設定 > Webとメール > プロトコルフィルタリング > 除外されたアプリケーション**で除外されていないことを確認します。

7. サードパーティセキュリティソフトウェアまたはファイアウォールと競合する場合があります。プログラムの追加と削除ウィンドウで、このサードパーティソフトウェアを確認してアンインストールすることを検討してください。

8. 前の手順でESET製品をアップグレードしていない場合、ESET製品をアンインストールして再度インストールします。コンピューターの再起動後、安全なブラウザーを無効にしてから、もう一度有効にします。

安全なブラウザーは、オンライン処理中に金融データを保護するための強化された保護レイヤーです。

ほとんどの場合、安全なブラウザーは、既知のバンキングサイトにアクセスした後で既定のブラウザーで起動します。保護されたブラウザーに直接アクセスするにはESET Endpoint Securityの**ツール**をクリックしてから、**安全なブラウザー**をクリックします。

安全なブラウザーの詳細については、次のESETナレッジベース記事(英語およびその他の言語)をお読みください。

- ESET安全なブラウザーを使用する方法
- 特定のWebサイトでESETインターネットバンキング保護を有効または無効にする
- ESET Windowsホーム製品でインターネットバンキング保護を一時停止または無効にする
- ESETインターネットバンキング保護 – 一般的なエラー
- ESET用語集 | インターネットバンキング保護

問題を解決できない場合は、ESETテクニカルサポートサポートまで電子メールで問い合わせてください。

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, 851 01 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(i) 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NFR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いかぎり、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URLIP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も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、賃借、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ろうと、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、(i) 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。(i)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, 851 01 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でのみ、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、IPパケット、URL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。

ESETは、処理するすべての情報が重要であり、お客様へのサービスおよび製品の提供という正当な利益のために必要であると考えています。

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