ESET ENDPOINT SECURITY
ユーザーズマニュアル

目次

Chapter 1
ESET Endpoint Security
P.7

1.1 ESET Endpoint Security について …… 8
1.2 セキュリティの考え方 …… 9

Chapter 2
インストール
P.11

2.1 インストーラーの起動 …… 12
2.2 標準インストール …… 14
2.3 カスタムインストール …… 17
2.4 ユーザー名とパスワードの入力 …… 22
2.5 最新バージョンへのアップグレード …… 23
2.6 インストール直後のコンピュータの検査 …… 24

Chapter 3
初心者向けガイド
P.25

3.1 ユーザーインタフェースのデザインの概要 …… 26
3.2 プログラムが正しく動作しない場合の解決方法 …… 27
3.3 アップデートの設定 …… 29
3.4 プロキシサーバーの設定 …… 31
3.5 設定の保護 …… 32
3.6 信頼ゾーンの設定 …… 33

Chapter 4
ESET Endpoint Security
の使用方法
P.35

4.1 ESET Endpoint Security の概要 …… 36
4.2 コンピューター …… 38
4.2.1 ウイルス・スパイウェア対策 …… 39
4.2.1.1 リアルタイムファイルシステム保護 …… 39
4.2.1.2 ドキュメント保護 …… 43
4.2.1.3 コンピュータの検査 …… 43
4.2.1.4 スタートアップ検査 …… 47
4.2.1.5 パスによる除外 …… 48
4.2.1.6 ThreatSense エンジンのパラメーターの設定 …… 49
4.2.1.7 マルウェアが検出されたとき …… 55
4.2.2 リムーバブルメディア …… 57
4.2.3 デバイスコントロール …… 58
4.2.3.1 デバイスコントロールルール …… 58
4.2.3.2 デバイスコントロールルールの追加 …… 59
4.2.4 HIPS（Host-based Intrusion Prevention System） …… 61
4.3 ネットワーク …… 64
4.3.1 フィルタリングモード …… 66
4.3.2 ファイアウォールプロファイル …… 67
4.3.3 ルールの設定と使用 …… 69
4.3.3.1 ルールの設定 …… 70
4.3.3.2 ルールの編集 …… 71
4.3.4 ゾーンの設定 …… 73
4.3.4.1 ネットワーク認証 …… 73
4.3.5 接続の確立 - 検出 …… 77
4.3.6 ログ …… 78
4.3.7 システム統合 …… 78

4.4 Web とメール 79
4.4.1 Web アクセス保護 81
4.4.1.1 HTTP、HTTPS 81
4.4.1.2 URL アドレス管理 83
4.4.2 電子メールクライアント保護 84
4.4.2.1 POP3/POP3S のフィルタ 85
4.4.2.2 IMAP、IMAPS プロトコルの検査 86
4.4.2.3 メールクライアントとの統合 87
4.4.2.4 マルウェアの削除 88
4.4.3 迷惑メール対策機能 89
4.4.3.1 ホワイトリストとブラックリストへのアドレスの追加 90
4.4.3.2 メッセージを迷惑メールとしてマークする 90
4.4.4 プロトコルフィルタリング 91
4.4.4.1 Web と電子メールのクライアント 91
4.4.4.2 対象外のアプリケーション 92
4.4.4.3 除外される IP アドレス 92
4.4.4.4 SSL 通信のチェック 93
4.5 Web コントロール 96
4.5.1 Web コントロールルール 97
4.5.2 Web コントロールルールの追加 98
4.5.3 グループエディター 99
4.6 アップデート 100
4.6.1 アップデートの設定 104
4.6.1.1 アップデートプロファイル 105
4.6.1.2 アップデートの詳細設定 105
4.6.1.3 アップデートのロールバック 108
4.6.2 アップデートタスクの作成方法 110
4.7 ツール 111
4.7.1 ログファイル 113
4.7.1.1 ログの保守 114
4.7.2 スケジューラ 115
4.7.2.1 新しいタスクの作成 117
4.7.3 統計 119
4.7.4 アクティビティの確認 120
4.7.5 ESET SysInspector 121
4.7.6 ESET Live Grid 122
4.7.6.1 不審なファイル 123
4.7.7 実行中のプロセス 124
4.7.8 ネットワーク接続 126
4.7.9 隔離 128
4.7.10 分析用ファイルの提出 130
4.7.11 警告と通知 131
4.7.11.1 メッセージの書式 132
4.7.12 システムのアップデート 133
4.7.13 診断 133
4.7.14 ライセンス 134
4.7.15 リモート管理 135
4.8 ユーザーインタフェース 136
4.8.1 グラフィックス 137
4.8.2 警告と通知 138
4.8.2.1 詳細設定 139
4.8.3 非表示の通知ウィンドウ 140
4.8.4 アクセス設定 140
4.8.5 プログラムメニュー 141
4.8.6 コンテキストメニュー 142
4.8.7 プレゼンテーションモード 143

Chapter 5
上級者向けガイド
P.145

5.1 プロキシサーバーの設定 …… 146
5.2 設定のインポート / エクスポート …… 147
5.2 キーボードショートカット …… 148
5.4 コマンドライン …… 149
5.5 ESET SysInspector …… 152
5.5.1 ESET SysInspector の概要 …… 152
5.5.1.1 ESET SysInspector の起動 …… 152
5.5.2 ユーザーインタフェースとアプリケーションの使用 …… 153
5.5.2.2 ESET SysInspector におけるナビゲーション …… 155
5.5.2.1 プログラムコントロール …… 153
5.5.2.3 ログの比較 …… 158
5.5.3 コマンドラインパラメーター …… 160
5.5.4 サービススクリプト …… 161
5.5.4.1 サービススクリプトの生成 …… 161
5.5.4.2 サービススクリプトの構造 …… 161
5.5.4.3 サービススクリプトの実行 …… 165
5.5.5 FAQ …… 166
5.5.6 ESET Endpoint Security の一部としての ESET SysInspector …… 168
5.6 ESET SysRescue …… 169
5.6.1 レスキュー CD の作成方法 …… 169
5.6.2 対象の選択 …… 169
5.6.3 設定 …… 170
5.6.3.1 フォルダー …… 170
5.6.3.2 ESET アンチウイルス …… 171
5.6.3.3 詳細設定 …… 171
5.6.3.4 インターネットプロトコル …… 172
5.6.3.5 起動可能な USB デバイス …… 172
5.6.3.6 書き込み …… 172
5.6.4 ESET SysRescue の操作 …… 173
5.6.4.1 ESET SysRescue の使用 …… 173

Chapter 6
用語集
P.175

6.1 マルウェアの種類 …… 176
6.1.1 ウイルス …… 176
6.1.2 ワーム …… 177
6.1.3 トロイの木馬 …… 177
6.1.4 ルートキット …… 178
6.1.5 アドウェア …… 178
6.1.6 スパイウェア …… 179
6.1.7 安全ではない可能性があるアプリケーション …… 179
6.1.8 望ましくない可能性があるアプリケーション …… 180
6.2 リモート攻撃の種類 …… 181
6.2.1 DoS 攻撃 …… 181
6.2.2 DNS キャッシュポイズニング …… 181
6.2.3 ワーム攻撃 …… 181
6.2.4 ポートスキャン …… 182
6.2.5 TCP 非同期 …… 182
6.2.6 SMB リレー …… 183
6.2.7 ICMP 攻撃 …… 183

6.3 メール …… 184
6.3.1 広告 …… 184
6.3.2 デマ …… 185
6.3.3 フィッシング …… 185
6.3.4 迷惑メール詐欺の特定 …… 186
6.3.4.1 ルール …… 186
6.3.4.2 ホワイトリスト …… 187
6.3.4.3 ブラックリスト …… 187
6.3.4.4 サーバー側での検査 …… 187

■本書について

○本書は、ESETセキュリティ ソフトウェア シリーズ ライセンス製品の共通ガイドとしてまとめています。

○文中に設けているアイコンは、該当するプログラムを示しています。「ESET Endpoint Security」は アイコン、「ESET Endpoint アンチウイルス」は アイコン、「ESET File Security for Microsoft Windows Server」は アイコン、「ESET NOD32アンチウイルス」は アイコンです。

■お断り

○本書は、本書作成時のソフトウェアおよびハードウェアの情報に基づき作成されています。ソフトウェアのバージョンアップなどにより、記載内容とソフトウェアに搭載されている機能が異なっている場合があります。また本書の内容は、改訂などにより予告なく変更することがあります。

○本製品の一部またはすべてを無断で複写、複製、改変することはその形態を問わず、禁じます。

○本書の著作権は、キヤノンITソリューションズ株式会社に帰属します。ESETセキュリティ ソフトウェア シリーズの各プログラムの著作権は、ESET, spol. s. r. o. に帰属します。

○ESET、ESET Smart Security、NOD32、ESET Remote Administrator、ESET Endpoint Security、ThreatSenseは、ESET, spol.s.r.o. の商標です。

○Microsoft、Windows、Windows Vista、Windows Server、Windows Live、ActiveX、Internet Explorer、Outlookは、米国Microsoft Corporationの米国、日本およびその他の国における登録商標または商標です。

○FireWireは、米国およびその他の国で登録されているApple Inc. の商標です。

[Chapter 1]
ESET Endpoint Security

1.1 ESET Endpoint Security について …… 8
1.2 セキュリティの考え方 …… 9

1.1 ESET Endpoint Securityについて

ESET Endpoint Securityは、コンピュータセキュリティの真の統合への第一歩を踏み出します。最新バージョンのThreatSense®検査エンジンに、パーソナルファイアウォールおよび迷惑メール対策機能が組み合わせると、ご使用のコンピュータを安全に保つために必要な速度および精度が実現されます。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は、ESET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は、主に小規模ビジネス/企業環境のワークステーションでの使用を対象に設計されています。ESET Remote Administratorと接続することにより、ネットワークに接続された任意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、リモート設定が可能になります。

1.2 セキュリティの考え方

コンピュータを操作するとき、特にWebアクセスをするときには、不正侵入とマルウェアが引き起こす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得るには、ウイルス対策システムを正しく使用し、有益な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 Live Gridの統計データによると、毎日数千種類のマルウェアが新たに作成されています。これは、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です。その利益は、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が、これらのウイルスを毎日解析し、アップデートファイルを作成してリリースしています。それは、ウイルス対策プログラムのユーザーの保護レベルを継続的に向上させるためです。アップデートの設定に誤りがあると、ウイルス対策プログラムの効果は低下してしまいます。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

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果的に蔓延させるためです。そこで、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新たに表面化しないかどうかを注意深く見守り、潜在的なマルウェアを排除するセキュリティアップデートファイルを定期的にリリースします。これらのセキュリティアップデートファイルは、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。このようなアプリケーションの例としては、Windowsオペレーティングシステムや広く使用されているインターネットブラウザのInternet Explorerなどがあります。

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のニーズに配慮することは、ほとんどありません。悪意のあるプログラムの活動が、オペレーティングシステムの全面的な誤作動を引き起こし、重要なデータを故意に破壊することがよくあります。重要なデータと機密データをDVDや外付けハードディスクなどの外部ソースに定期的にバックアップすることが重要です。これらの予防対策を講じることにより、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

適切に設定した自動スキャンをコンピュータで定期的に実施することにより、ウイルス定義データベースが古いために見逃されたマルウェアでも削除できます。

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れこそ、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、感染した場合にコンピュータから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。役立つルールのいくつかは、次のとおりです。

●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。

[Chapter 2]
インストール

2.1 インストーラーの起動 …… 12
2.2 標準インストール …… 14
2.3 カスタムインストール …… 17
2.4 ユーザー名とパスワードの入力 …… 22
2.5 最新バージョンへのアップグレード …… 23
2.6 インストール直後のコンピュータの検査 …… 24

2.1 インストーラーの起動

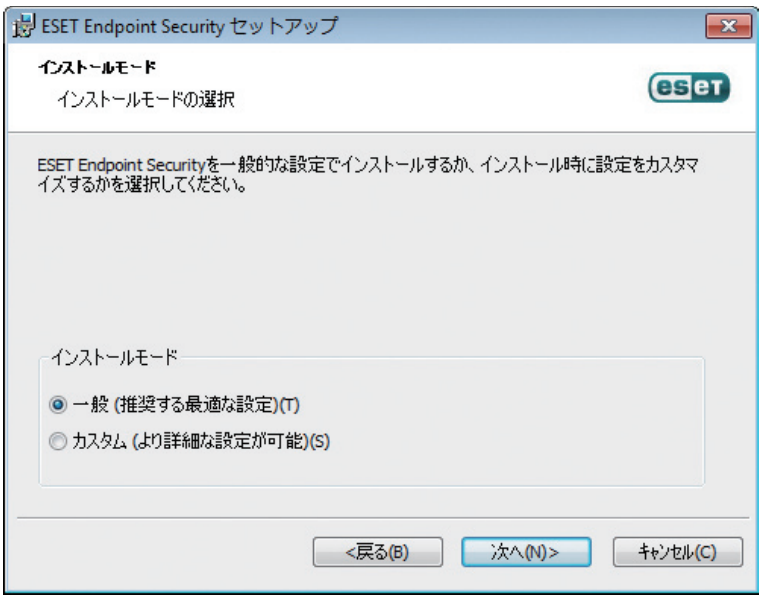
インストーラーを起動すると、インストールウィザードが表示されるので、その案内に従って設定処理を行ってください。

重要

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。

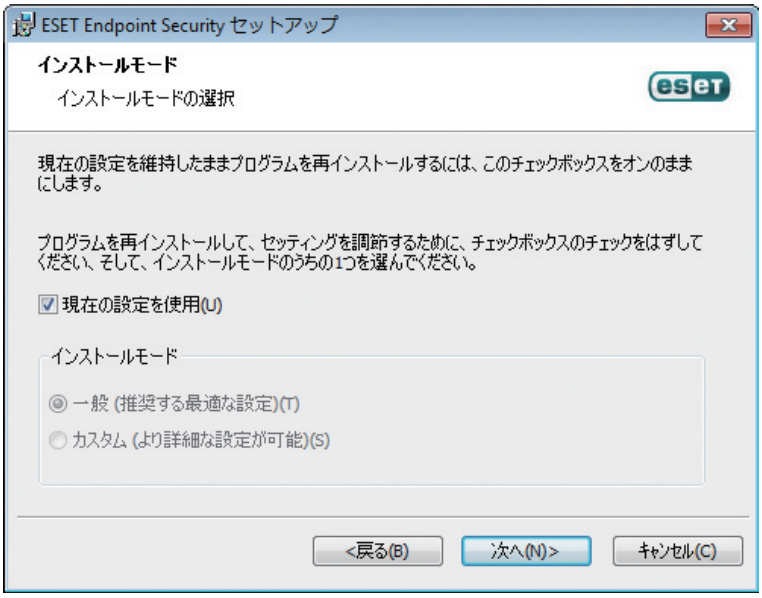
インストーラーを実行すると、エンドユーザーライセンス契約が表示されます。契約を読んで [同意する] をクリックし、エンドユーザーライセンス契約を承諾することを確認します。承諾した後、インストールの続きには2通りのシナリオがあります。

1



ESET Endpoint Securityをコンピュータに初めてインストールする場合、[エンドユーザーライセンス契約] の承諾後、左のウィンドウが表示されます。ここで、標準インストールまたはカスタムインストールを選択でき、選択にしたがって続行します。

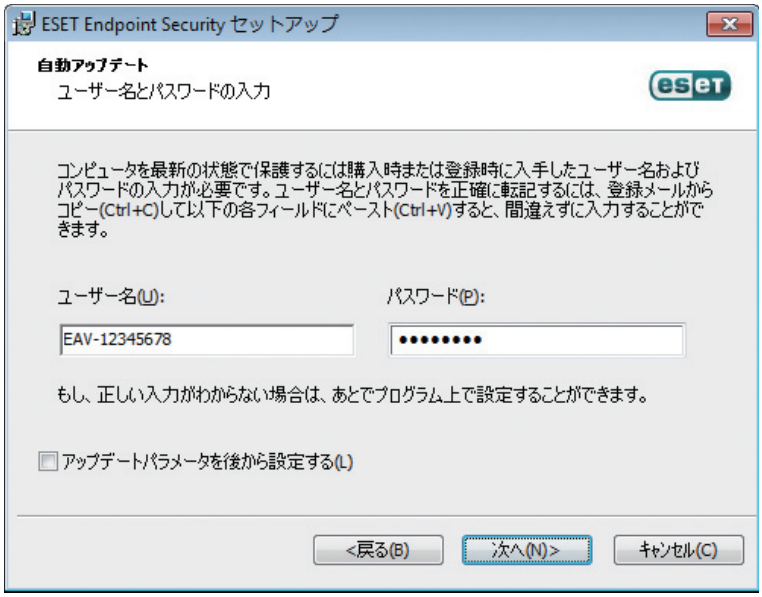
2



前のバージョンのソフトウェアを上書きしてESET Endpoint Securityをインストールする場合、左のウィンドウで、新規インストールに対して現在のプログラム設定を使用することを選択できます。あるいは、[現在の設定を使用] オプションのチェックを外した場合は、上記の2つのインストールモードのいずれかを選択することもできます。

2.2 標準インストール

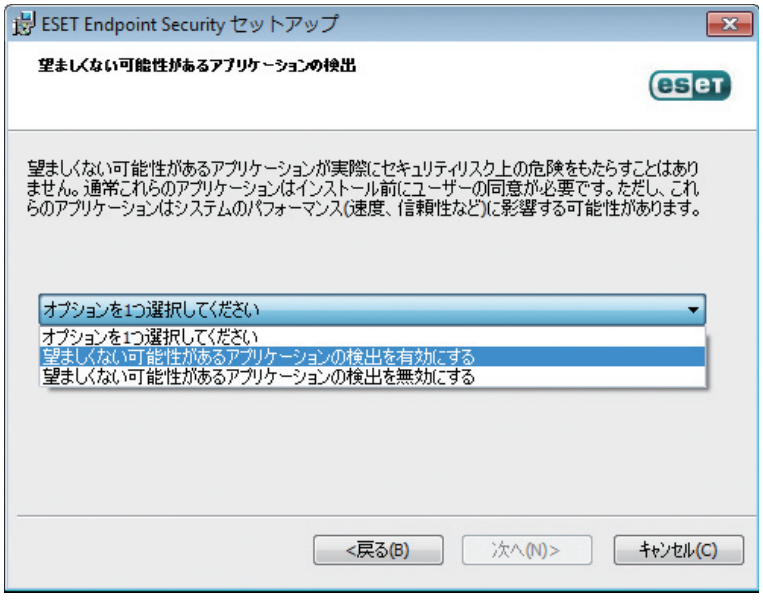
標準インストールには、ほとんどのユーザーに適した設定オプションが用意されています。これらの設定は、優れたセキュリティ、簡単な設定、優れたシステムパフォーマンスを実現します。標準インストールモードは既定のオプションであり、特定の設定に対して特定の要件がない限りこれをご使用ください。
インストールモードを選択して[次へ]をクリックすると、プログラムの自動アップデートのためにユーザー名とパスワードの入力を求められます。プログラムの自動アップデートは、継続してシステムを保護する上で重要な役割を果たします。



[ユーザー名]および[パスワード]フィールドに、製品の購入後または登録後に受け取った認証データを入力します。使用可能なユーザー名とパスワードが現時点で持っていない場合は、[アップデートパラメータを後から設定する]チェックボックスをクリックします。ユーザー名とパスワードを後でプログラムそのものに入力できます。
次の手順ではESET Live Gridを設定します。ESET Live Gridによって、新しいマルウェアが迅速かつ継続的にESETに通知されるので、お客様をすばやく保護することができます。ESETのウイルスラボに新しいマルウェアが提出されると、これらが解析および処理され、ウイルス定義データベースに追加されます。

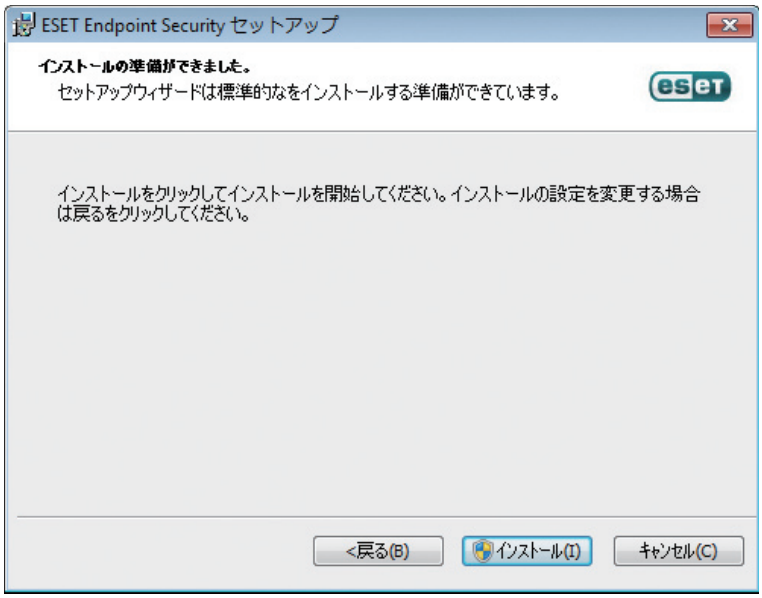
デフォルトでは [ESET Live Gridへの参加に同意する] オプションが選択され、この機能が有効になっています。

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。望ましくない可能性があるアプリケーションは、必ずしも悪意があるとは限りませんが、オペレーティングシステムの動作に悪影響を及ぼす可能性があります。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。



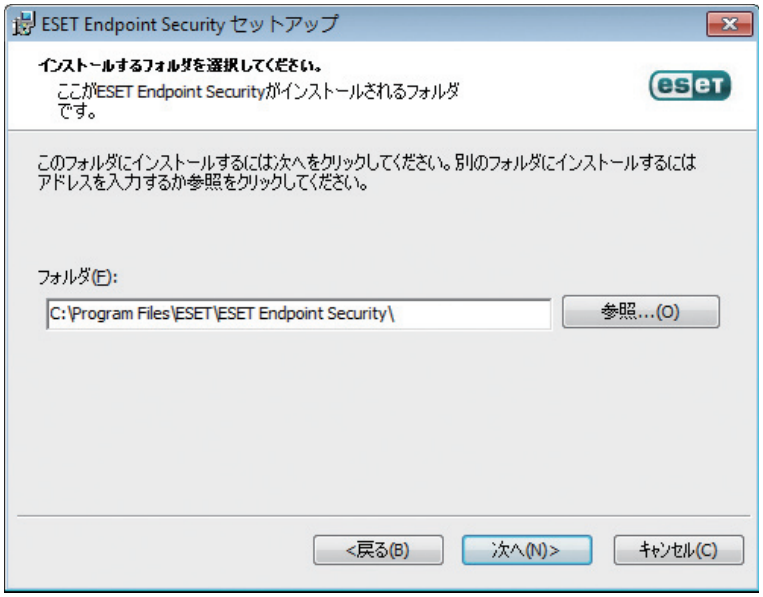
ESET Endpoint Securityでこのようなマルウェアを検出できるようにするには、[望ましくない可能性があるアプリケーションの検出を有効にする] オプションを選択します。

標準インストールモードの最後のステップでは、[インストール] ボタンをクリックしてインストールを確認します。



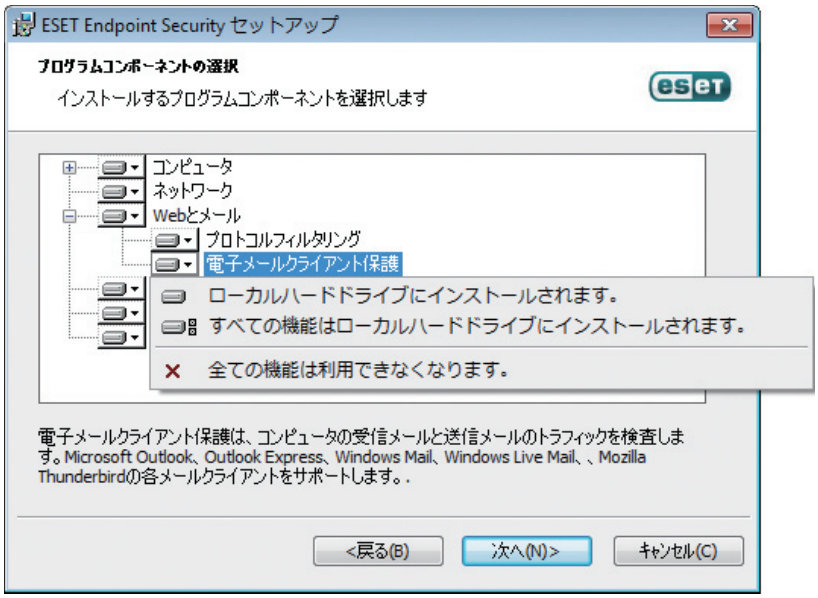
2.3 カスタムインストール

カスタムインストールモードは、プログラムを微調整した経験があるユーザーや、インストール時に詳細設定を変更したいユーザーを対象としています。
このインストールモードを選択して [次へ] をクリックすると、インストール先の場所を選択するように促すプロンプトが表示されます。
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)。



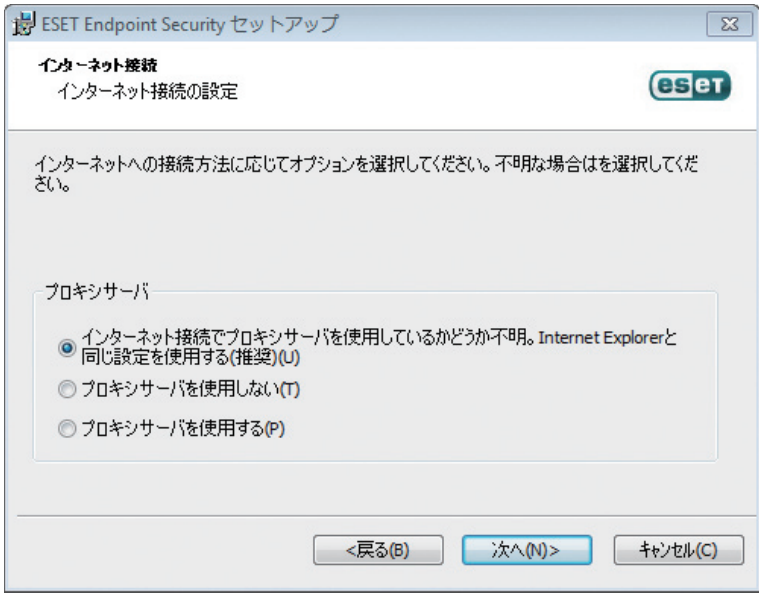
次に、ユーザー名とパスワードを入力します。このステップは、標準インストール（「標準インストール」を参照）と同じです。

インストールプロセスの次のステップでは、インストールするプログラムコンポーネントを選択します。コンポーネントツリーを展開して機能を選択すると、3つのインストールオプションが表示されます。[ローカルハードドライブにインストールされます] オプションは既定で選択されています。[すべての機能はローカルハードドライブにインストールされます] を選択すると、選択済みのツリーの下にすべての機能がインストールされます。機能やコンポーネントを使用したくない場合、[全ての機能は利用できなくなります] を選択します。



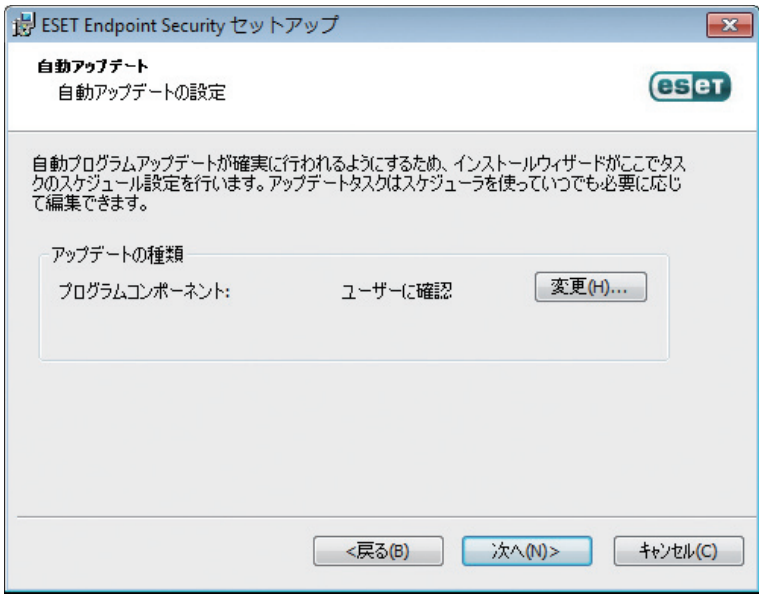
[次へ] をクリックし、インターネット接続の設定に進みます。プロキシサーバーを使用する場合、ウイルス定義アップデートが動作するよう正しく設定されている必要があります。

インターネット接続にプロキシサーバーを使用するかどうかわからない場合は、[インターネット接続でプロキシサーバーを使用しているかどうか不明。Internet Explorerと同じ設定を使用する（推奨）] を選択して、[次へ] をクリックします。プロキシサーバを使用しない場合は、[プロキシサーバーを使用しない] オプションを選択します。

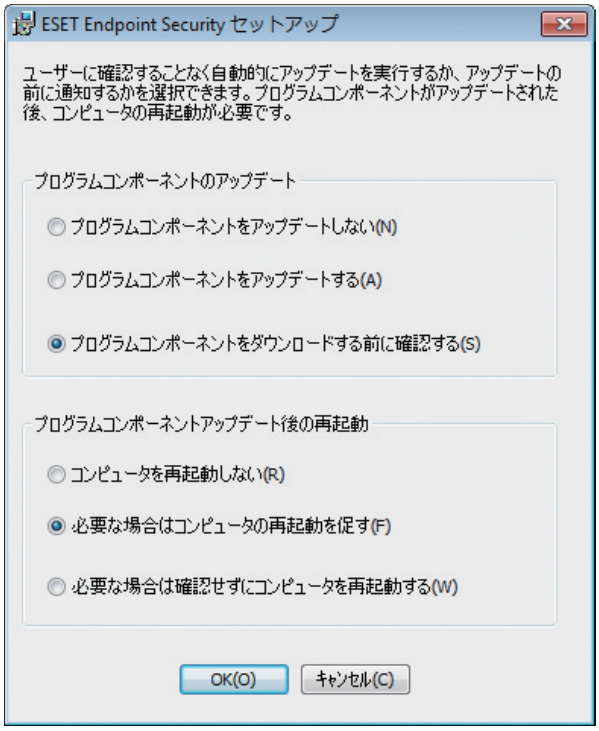


プロキシサーバーの設定を行うには、[プロキシサーバを使用する]を選択し、[次へ]をクリックします。[アドレス]フィールドにプロキシサーバーのIPアドレスまたはURLを入力します。[ポート]フィールドには、プロキシサーバーが接続を受け付けるポートを指定します(既定では3128です)。プロキシサーバーで認証が要求される場合は、有効な[ユーザー名]と[パスワード]を入力して、プロキシサーバーへのアクセスを可能にする必要があります。Internet Explorerからプロキシサーバーの設定をコピーするには、[適用]をクリックし、選択内容を確認します。

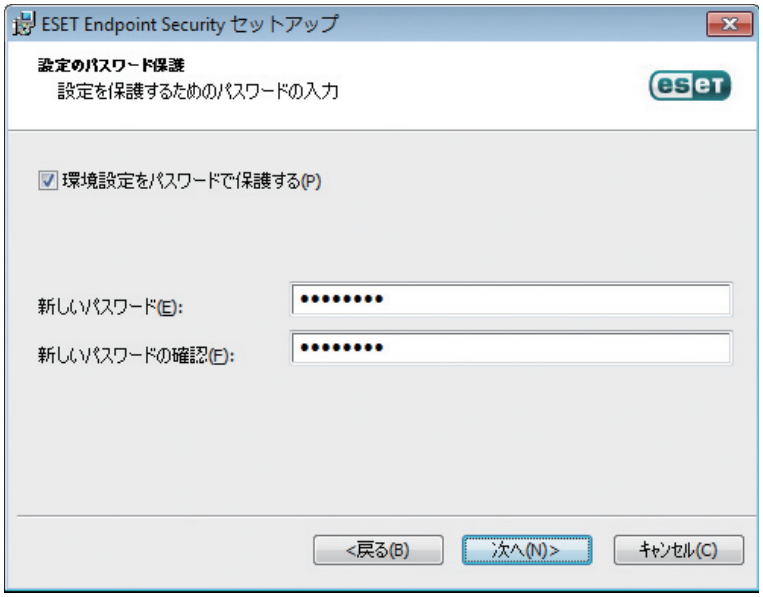
このインストール手順で、システムでの自動プログラムアップデートの扱い方を指定できます。詳細設定にアクセスするには、[変更...]をクリックします。



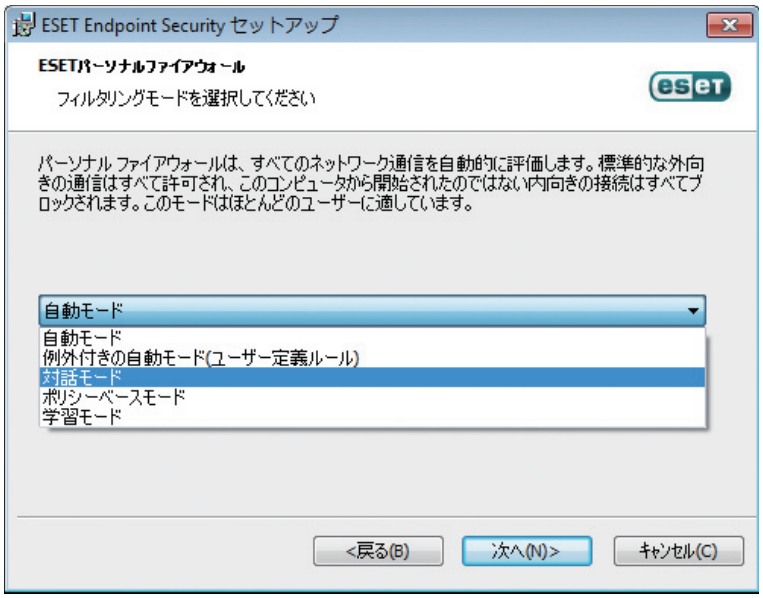
プログラムコンポーネントをアップデートしない場合は、[プログラムコンポーネントをアップデートしない] を選択します。[プログラムコンポーネントをダウンロードする前に確認する] オプションを選択すると、システムがプログラムコンポーネントをダウンロードしようとするたびに確認ウィンドウが表示されます。プログラムコンポーネントのアップデートファイルを自動的にダウンロードするには、[プログラムコンポーネントをアップデートする] オプションをオンにします。



次のインストールウィンドウには、プログラム設定を保護するためのパスワードを設定するオプションがあります。[環境設定をパスワードで保護する] オプションを選択し、パスワードを [新しいパスワード] および [新しいパスワードの確認] フィールドに入力します。このパスワードは、ESET Endpoint Securityの設定の変更やアクセスに必要になります。両方のパスワードフィールドが一致したら、[次へ] をクリックして続行します。



次のインストールステップ [自動アップデート]、[ESET Live Grid]、および [望ましくない可能性があるアプリケーションの検出] は、標準インストールモードの場合と同様に処理されます (「標準インストール」を参照)。
次に、ESETパーソナルファイアウォールのフィルタリングモードを選択します。ESET Endpoint Securityパーソナルファイアウォールには、5つのフィルタリングモードがあります。ファイアウォールの動作は、選択したモードによって異なります。



[インストールの準備ができました] ウィンドウで [インストール] をクリックしてインストールを完了します。

2.4 ユーザー名とパスワードの入力

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。これが可能なのは、アップデートの設定で正しいユーザー名とパスワードを入力した場合のみです。
インストール時にユーザー名とパスワードを入力しなかった場合、ここで入力することができます。メインプログラムウィンドウで、[アップデート] をクリックしてからキーボードの [CTRL+U] を押し、ユーザー名、パスワードを、[ライセンスの詳細] ウィンドウに入力します。

[ユーザー名] および [パスワード] は、書かれている通りに入力する必要があります。

●ユーザー名およびパスワードは、大文字と小文字の区別があり、ユーザー名中で使われているハイフンは必要です。
●パスワードは、10文字の長さで、すべて小文字です。
●パスワードでは、英字のLを使用していません（数字の1を使用してください）。
●大きい'O'は数字のゼロ、小さい'o'は英字のoです。

2.5 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アップデートでは解決できない問題の修正や改良を行うため、ESET Endpoint Security の最新バージョンが発行されます。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。

●手動で、最新バージョンをダウンロードし、以前のバージョンに上書きインストールします。インストールの開始時に、[現在の設定を使用] チェックボックスを選択して、現在のプログラム設定を保存するかどうかを選択できます。

●手動で、ESET Remote Administrator経由のネットワーク環境で自動展開します。

2.6 インストール直後のコンピュータの検査

ESET Endpoint Securityのインストール後、コンピュータの検査を実行することを推奨します。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」を参照してください。

[Chapter 3]
初心者向けガイド

3.1 ユーザーインタフェースのデザインの概要 …… 26
3.2 プログラムが正しく動作しない場合の解決方法 …… 27
3.3 アップデートの設定 …… 29
3.4 プロキシサーバーの設定 …… 31
3.5 設定の保護 …… 32
3.6 信頼ゾーンの設定 …… 33

3.1 ユーザーインタフェースのデザインの概要

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。

保護の状態	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、スマート検査またはカスタム検査の設定や起動を行うことができます。
アップデート	ウイルス定義データベースのアップデートに関する情報が表示されます。
設定	このオプションを選択すると、コンピュータ、Webとメールの設定を確認、または変更できます。
ツール	[ログファイル]、[保護統計]、[監視アクティビティ]、[実行中のプロセス]、[ネットワーク接続]、[スケジューラ]、[隔離]、[ESET SysInspector]、および[ESET SysRescue]にアクセスできます。
ヘルプとサポート	ヘルプファイル、製品ホームページのFAQ、ESETのWebサイトのリンクを利用できます。

[保護の状態] 画面には、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が示されています。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。
[状態] ウィンドウには、ESET Endpoint Securityの頻繁に使用する機能も表示されます。また、プログラムの有効期限も表示されます。

3.2 プログラムが正しく動作しない場合の解決方法

各モジュールが正しく動作している場合は、緑のチェックが表示されます。正しく動作していない場合は、エクスクラメーションマークまたはオレンジの通知アイコンが表示され、モジュールに関する追加情報がウィンドウの上部に表示されます。モジュールを修正するための推奨される解決策も表示されます。各モジュールのステータスを変更するには、メインメニューの [設定] をクリックし、必要なモジュールをクリックします。

赤いアイコンは保護に重大な問題があることを示しています。つまり、コンピュータは最も高い保護で守られていません。理由はいくつか考えられます。

●リアルタイムファイルシステム保護が無効になっている
●パーソナルファイアウォールが無効になっている
●ウイルス定義データベースが失効している
●製品ライセンスの有効期限が切れている

黄色のアイコンは、以下のことを示しています。
●Webアクセスまたは電子メールクライアントの保護が無効にされている
●またはアップデートに関する問題（ウイルス定義データベースが期限切れになっていてアップデートできない）がある
●ライセンスの期限が切れそうである

ウイルス・スパイウェア対策は無効です	この問題があると赤のアイコンが示され、[コンピュータ]項目の隣にセキュリティ通知が表示されます。ウイルス対策保護機能を再度有効にするには、[ウイルス・スパイウェア対策のすべての保護機能を開始する]をクリックします。
Webアクセス保護が無効になっています	この問題は、黄色の"i"アイコンとセキュリティ通知の状態で表示されます。もう一度、Webアクセス保護とを有効にするには、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。
ESETパーソナル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]をクリックして、ネットワークの保護を再度有効にできます。
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、プログラムのアップデートはできなくなり、保護の状態アイコンは赤に変わります。
ライセンスは有効期限を過ぎています	これは保護の状態が赤に変わったアイコンで示されます。ライセンスの期限が過ぎたら、このプログラムはアップデートできません。ライセンスをアップデートするには、警告ウィンドウの指示に従うことをお勧めします。

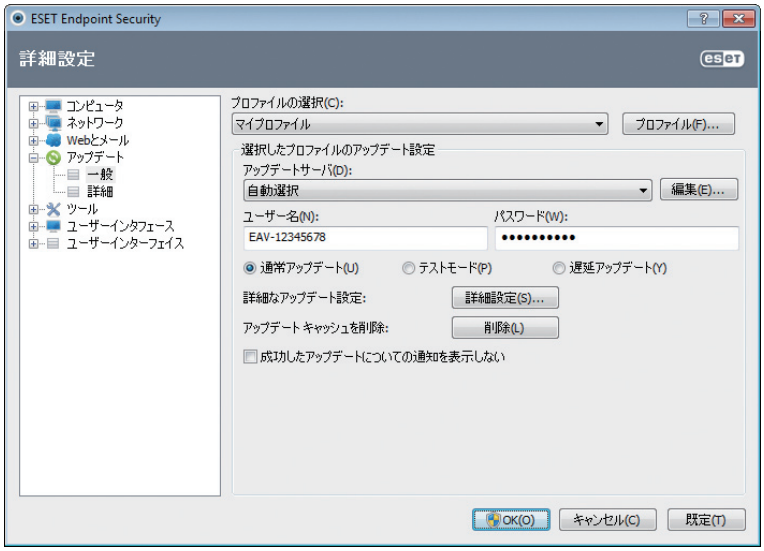
提示された解決策を使用して問題を解決できない場合は、[ヘルプとサポート] をクリックしてヘルプ情報を確認するか、あるいは製品ホームページのFAQをご参照ください。問題が解決されない場合は、サポートセンターにご連絡ください。

製品ホームページ
http://canon-its.jp/product/eset/license/

3.3 アップデートの設定

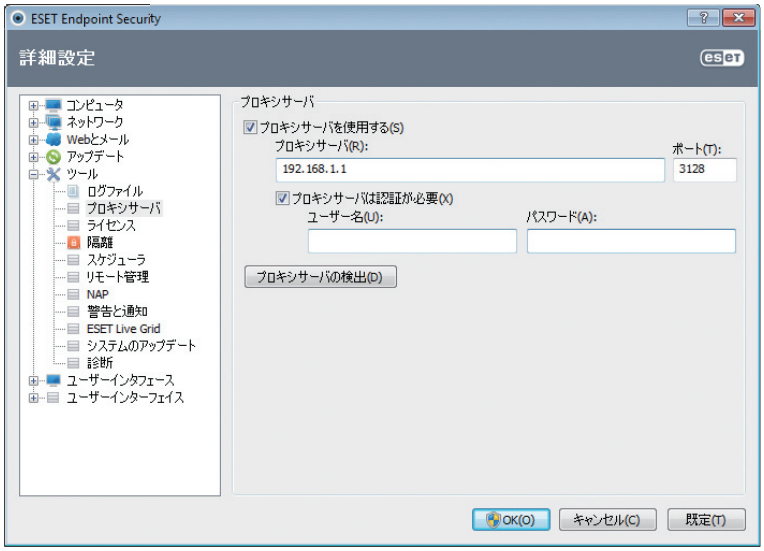
ウイルス定義データベースのアップデートとプログラムコンポーネントのアップデートは、悪意のあるコードから完全に保護するための重要な部分です。この設定や操作には特に注意してください。メインメニューから [アップデート] を選択し、[ウイルス定義データベースのアップデート] をクリックして、データベースの新しいアップデートを確認します。ユーザー名とパスワードの入力を (ESET Endpoint Securityの) インストールプロセス中に行わなかった場合、この時点で行うようプロンプトで指示されます。

[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、[詳細設定を表示する...]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。左の詳細設定ツリーの[アップデート]をクリックします。[アップデートサーバ]ドロップダウンメニューには、既定では[自動選択]が設定されています。アップデートモード、プロキシサーバーアクセス、LAN接続、ウイルス定義コピーの作成など、詳細なアップデートオプションを設定するには、[詳細設定]ボタンをクリックします。



3.4 プロキシサーバーの設定

ESET Endpoint Securityを使用しているシステムでインターネット接続を制御するためにプロキシサーバーを使用する場合は、詳細設定に指定する必要があります。プロキシサーバーの設定ウィンドウにアクセスするには、F5キーを押して[詳細設定]ウィンドウを開き、[詳細設定]ツリーから[ツール]>[プロキシサーバ]をクリックします。[プロキシサーバを使用する]オプションを選択して、[プロキシサーバ](IPアドレス)および[ポート]フィールドに入力します。必要に応じて、[プロキシサーバは認証が必要]オプションを選択して、[ユーザー名]および[パスワード]を入力します。



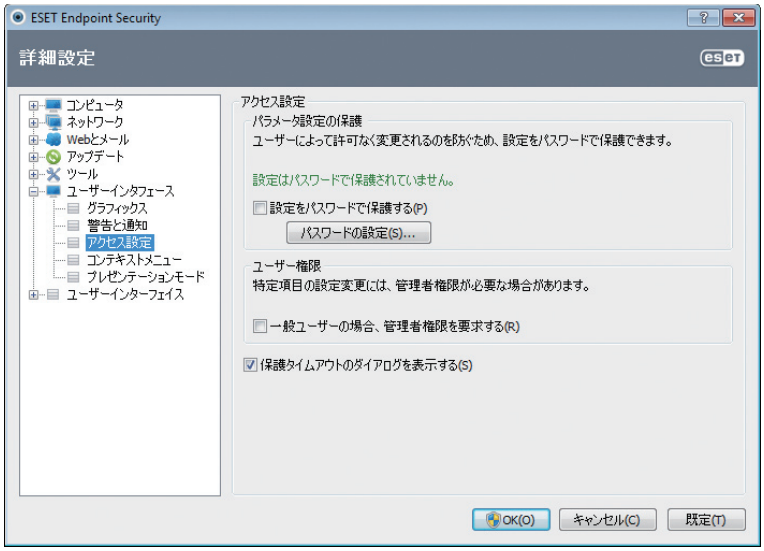
[プロキシサーバの検出]ボタンは、Internet Explorerに設定されているプロキシサーバー設定を呼び出すことができます。

NOTE

アップデートプロファイルごとにプロキシサーバのオプションが異なる場合があります。異なる場合は、詳細設定ツリーから[アップデート]をクリックし、[詳細設定]で別のアップデートプロファイルを設定します。

3.5 設定の保護

ESET Endpoint Securityの設定は、セキュリティポリシーの観点から、非常に重要になることがあります。許可なく変更が行われた場合は、システムの安定性と保護が危険にさらされる可能性があります。セットアップパラメータをパスワードで保護するには、メインメニューで [設定] > [詳細設定を表示する...] > [ユーザーインターフェイス] > [アクセス設定] をクリックし、[設定をパスワードで保護する] オプションを選択して、[パスワードの設定...] ボタンをクリックします。



[新しいパスワード] フィールドと [新しいパスワードの確認] フィールドにパスワードを入力して、[OK] をクリックします。このパスワードは今後、ESET Endpoint Securityの設定を変更する場合に常に必要になります。

3.6 信頼ゾーンの設定

ネットワーク環境でコンピュータを保護するには、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。[設定]>[ネットワーク]>[ネットワークでのコンピュータの保護モードを変更する…] をクリックします。ネットワークコンピュータに設定可能な保護モードのオプションがウィンドウに表示されます。

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。

CAUTION

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。

NOTE

注意: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。

[Chapter 4]
ESET Endpoint Security の使用方法

4.1 ESET Endpoint Security の概要 …… 36
4.2 コンピューター …… 38
4.3 ネットワーク …… 64
4.4 Web とメール …… 79
4.5 Web コントロール …… 96
4.6 アップデート …… 100
4.7 ツール …… 111
4.8 ユーザーインタフェース …… 136

4.1 ESET Endpoint Securityの概要

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

[設定] メニューには次のオプションがあります。

●コンピュータ
●ネットワーク
●Webとメール

いずれかのコンポーネントをクリックすると、対応する保護モジュールの詳細設定を調整することができます。

[コンピュータ] 保護モード設定で、次のコンポーネント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	すべてのファイルを対象に、オープン、作成、実行のイベントが発生するとファイルは検査されます。
ドキュメント保護	ドキュメントの保護機能により、Microsoft Officeドキュメントの検査(開く前に実行)、およびInternet Explorerにより自動的にダウンロードされたファイル(Microsoft ActiveX要素など)の検査が行われます。(※)
デバイスコントロール	このモジュールを使用すると、拡張フィルタ/権限を検査、ブロック、または調整して、ユーザーによる指定デバイス(CD/DVD/USB...)のアクセス方法や作業方法を選択できます。
HIPS	HIPSシステムは、オペレーティングシステム内のイベントを監視し、カスタマイズされた一連のルールに従って対処します。
プレゼンテーションモード	プレゼンテーションモードを有効または無効にします。警告メッセージを受け取った後(潜在的なセキュリティリスク)、プレゼンテーションモードを有効にするとメインウィンドウが黄色に変わります。
アンチステルス保護	ルートキットなどの危険なプログラムを検出する機能です。ルートキットは、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ます。そのため、通常のテスト技術を使用して検出することはできません。

※本機能は既定の設定では、無効になっています。

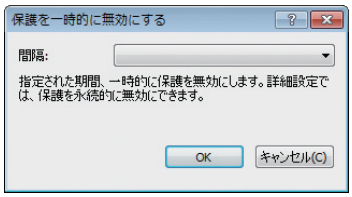
[ネットワーク] セクションでは、[パーソナルファイアウォール] を有効または無効にすることができます。[Webとメールの保護の設定] では、次のコンポーネントを有効または無効にすることができます。

Webアクセス保護	有効にした場合、HTTPまたはHTTPS経由のすべてのトラフィックで悪意のあるソフトウェアが検査されます。
電子メールクライアント保護	POP3とIMAPプロトコルで受信した通信が監視されます。
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、つまり迷惑メールを検査します。
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。さらに、雇用者またはシステム管理者は、最大27までのWebサイトカテゴリを事前定義してアクセスを禁止できます。

NOTE

[詳細設定をする...] (F5) > [コンピュータ] > [ウイルス・スパイウェア対策] > [ドキュメント保護] > [システム統合] でオプションを有効にした後、 ドキュメント保護が表示されます。

[有効] をクリックすると、[保護を一時的に無効にする] ダイアログボックスが表示されます。[OK] をクリックして、選択したセキュリティコンポーネントを無効にします。[間隔] ドロップダウンメニューは、選択したセキュリティコンポーネントを無効にする期間を示します。



無効にしたセキュリティコンポーネントの保護を再度有効にするには、[無効] をクリックします。

NOTE

この方法で保護を無効にした場合は、無効にした保護機能のすべての部分が、コンピュータの再起動後に有効になります。

設定ウィンドウの下部に追加オプションがあります。設定ファイルを使用して設定パラメータをロードしたり、現在の設定パラメータを設定ファイルに保存したりするには、[設定のインポートとエクスポート] を使用します。

4.2 コンピューター

[コンピュータ] メニューは、[設定] ペインで [コンピュータ] のタイトルをクリックすると表示されます。ここには、すべての保護機能の概要が表示されます。個々の機能を一時的に無効にするには、該当する機能の下の [無効] 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が低下する可能性があります。各機能の詳細設定にアクセスするには、[設定...] をクリックします。

[除外の編集...] をクリックすると、[除外] 設定ウィンドウが開き、検査からファイルやフォルダーを除外することができます。

一時的にウイルス・スパイウェア対策を無効にする	ウイルス・スパイウェア対策のすべての保護機能を無効にします。[間隔] ドロップダウンメニューを含む[保護を一時的に無効にする]ダイアログボックスが表示されます。[間隔] ドロップダウンメニューは、保護を無効にする期間を示します。[OK]をクリックして、確定します。
コンピュータの検査の設定	クリックすると、オンデマンドスキャナ(手作業で実行するスキャン)のパラメータを調整できます。

4.2.1 ウイルス・スパイウェア対策

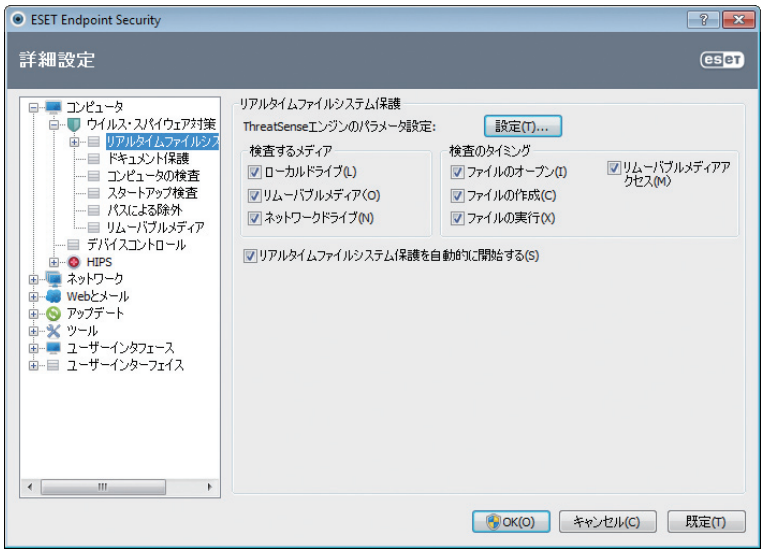
ウイルス・スパイウェア対策機能は、ファイル、メール、およびWeb通信を検査することにより、悪意のあるシステム攻撃から保護します。悪意のあるコードを含むウイルスが検出されると、保護モジュールがまずブロックし、次に駆除、削除、または隔離することにより、ウイルスを排除できます。

4.2.1.1 リアルタイムファイルシステム保護

リアルタイムファイルシステム保護では、システムで発生する、ウイルスが関係するイベントを全て検査します。すべてのファイルを対象に、オープン、作成、実行のイベントが発生するとファイル内に、悪意のあるコードがないかをスキャンします。リアルタイムファイルシステム保護は、システム起動時に開始されます。

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、すべての種類のメディアを確認します。ThreatSenseテクノロジの検出方法（「ThreatSenseエンジンのパラメータの設定」セクションに説明があります）を使用するリアルタイムファイルシステム保護は、新規作成ファイルと既存ファイルで検査方法が異なることがあります。新規作成ファイルの場合、より深いレベルの検査を適用できます。

リアルタイムファイルシステム保護の使用時に、システムへの負荷を最小化するために、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。ウイルス定義データベース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 [SMART最適化] を使用して設定します。このオプションが無効の場合、全てのファイルがアクセスのたびに検査されます。このオプションを変更するには、F5キーを押して、[詳細設定] ウィンドウを開き、[詳細設定] ツリーで [コンピュータ] > [ウイルス・スパイウェア対策] > [リアルタイムファイルシステム保護] をクリックします。次に、[ThreatSenseエンジンのパラメータ設定] の隣にある [設定...] ボタンをクリックして、[その他] をクリックし、[SMART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。
既定では、リアルタイムファイルシステム保護はシステム起動時に起動し、中断なしに検査を行います。特殊な場合（別のリアルタイムスキャナと競合する場合など）は、[リアルタイムファイルシステム保護を自動的に開始する] オプションの選択を解除すると、リアルタイムファイルシステム保護を終了できます。



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マルウェアが検査されます。

ローカルドライブ	システムハードディスクを全て検査します。
リムーバブルメディア	フロッピーディスク、CD/DVD、USB記憶装置などを検査します。
ネットワークドライブ	割り当てられたネットワークドライブを全て検査します。

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

検査のタイミング（イベント発生時の検査）

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。既定の設定により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。

ファイルのオープン	開いたファイルの検査を有効または無効にします。
ファイルの作成	新しく作成したファイルまたは変更したファイルの検査を有効または無効にします。
ファイルの実行	実行されたファイルの検査を有効または無効にします
リムーバブルメディアアクセス	ストレージに空き容量がある特定のリムーバブルメディアを利用することで行われ検査を有効または無効にします。

詳細検査オプション

詳細検査オプションは、[コンピュータ]＞[ウイルス・スパイウェア対策]＞[リアルタイムファイルシステムシステム保護]＞[詳細設定] にあります。

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	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、検査パラメータを追加して検査されます。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。それにより、ウイルス定義データベースのアップデートの公開の前でも新しいウイルスを検出できるので、検出率が大幅に向上します。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。
実行したファイルに適用する追加のThreatSenseパラメータ	既定では、アドバンスドヒューリスティック検査はファイル実行時には使用されません。ただし、場合によっては、このオプションを有効にする（[ファイル実行時のアドバンスドヒューリスティック]オプションをチェックする）ことも可能です。アドバンスドヒューリスティックを使用するとシステム所要量が増大するので、一部のプログラムの実行速度が低下する場合があります。[リムーバブルメディアからのファイル実行時のアドバンスドヒューリスティック]オプションを有効にした場合に、ファイル実行時に一部のリムーバブルメディア（USB）のポートをアドバンスドヒューリスティックの検査対象から除外するには、[例外...]をクリックして、リムーバブルメディアを除外対象にするウィンドウを開きます。ここから、各ポートのチェックボックスを選択は選択解除することによって、設定をカスタマイズできます。

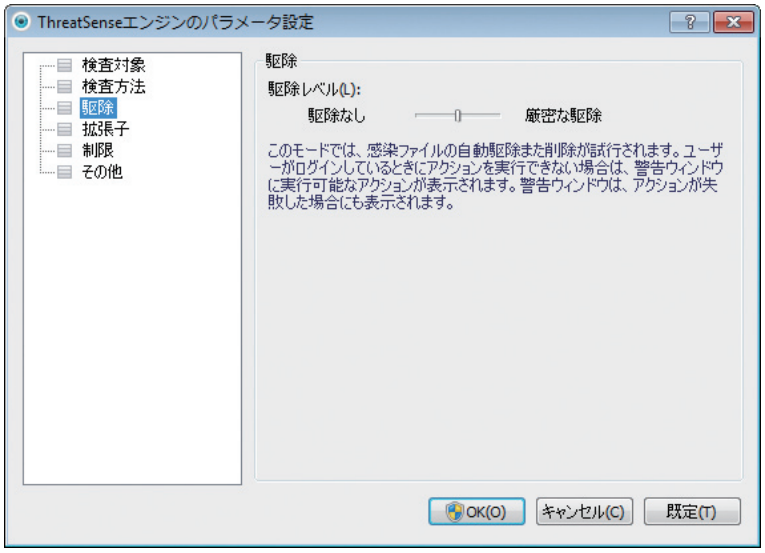
駆除レベル

リアルタイムファイルシステム保護には、3つの駆除レベルがあります（[ファイルシステムのリアルタイム保護] セクションの [設定...] ボタンをクリックしてから、[駆除] をクリックしてアクセス）。

駆除なし	感染しているファイルが自動的に駆除されることはありません。警告ウィンドウが表示され、ユーザーがアクションを選択することができます。このレベルは、ウイルスの侵入が発生したときに実行する必要のあるステップを理解している経験豊富なユーザー向けです。
標準的な駆除	プログラムは、事前定義されたアクション(マルウェアの種類によって異なります)に基づいて、感染ファイルの駆除または削除を自動的に試行します。感染しているファイルの検出と削除は、画面右下隅の情報メッセージによって通知されます。適切なアクションを自動的に選択できなかった場合は、ユーザーがその後のアクションを選択することができます。あらかじめ定義されているアクションを実行できなかった場合も同様です。
厳密な駆除	全ての感染ファイルが駆除または削除されます。ただし、システムファイルは除きます。感染ファイルを駆除できなかった場合は、アクションの選択を促す警告ウィンドウが表示されます。

CAUTION

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



リアルタイムファイルシステ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。たとえば、特定のアプリケーションや別のウイルス対策プログラムのリアルタイムスキャナーとの競合がある場合などです。

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。既定の設定に戻すには、[リアルタイムファイルシステム保護] ウィンドウ（[詳細設定] > [コンピュータ] > [ウイルス·スパイウェア対策] > [リアルタイムファイルシステム保護]）の右下にある [既定をクリックします。

リアルタイムファイルシステム保護の確認

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特殊な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。ファイルeicar.comは、http://www.eicar.org/download/eicar.comからダウンロードできます。

▸▸▸ NOTE

リアルタイム保護の確認を実行する前に、Webアクセス保護にする必要があります。Webアクセス保護が有効になっていると、この機能によってファイルが検出されてしまって、テストファイルをダウンロードできません。

リアルタイムファイルシステム保護が機能しない場合の解決方法

この章では、リアルタイムファイルシステ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。

リアルタイムファイルシステ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、再開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、［リアルタイムファイルシステム保護を有効にする］をクリックします。

システム起動時にリアルタイムファイルシステム保護が開始されない場合、その原因は通常、［リアルタイムファイルシステム保護を自動的に開始する］オプションが選択されていないからです。このオプションを有効にするには、［詳細設定］（F5）に移動し、［詳細設定］ツリーで［コンピュータ］＞［ウイルス･スパイウェア対策］＞［リアルタイムファイルシステム保護］をクリックします。ウィンドウの下部にある［詳細設定］セクションで［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］チェックボックスが選択されていることを確認します。

リアルタイムファイルシステ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つのリアルタイムファイルシステム保護が同時に有効になっていると、互いに競合することがあります。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。

リアルタイムファイルシステ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］オプション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されない場合、他のプログラムとの競合が原因であることがあります。この場合には、サポートセンターにお問い合わせください。

4.2.1.2 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によるファイルのダウンロード時にファイル（Microsoft ActiveX要素など）の検査が行われます。保護システムは、[システム統合] オプションで有効になります。このオプションを変更するには、F5キーを押して、[詳細設定] ウィンドウを開き、[詳細設定] ツリーで [コンピュータ] > [ウイルス・スパイウェア対策] > [ドキュメント保護] をクリックします。ドキュメント保護を有効にすると、ESET Endpoint Securityの [設定] > [コンピュータ] セクションのメインプログラムウィンドウに表示できます。

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。

4.2.1.3 コンピュータの検査

オンデマンドスキャナーはウイルス対策の重要な部分であり、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。そのような状況は、書き込みの時点でリアルタイムファイルシステム保護が無効に設定されていた場合や、ウイルス定義データベースが古い場合、またはファイルをディスクに保存する時点でウイルスとして検出されなかった場合など、ディスクに書き込まれたときに [リアルタイムファイルシステム保護] では捕捉されなかったウイルスを検出するために、システムの徹底的な検査を定期的に実行することをお勧めします。

2種類のコンピュータの検査が利用できます。スマート検査では、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、特定の検査対象の選択を行うことができます。

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。

スキャンの種類

■ スマート検査

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全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

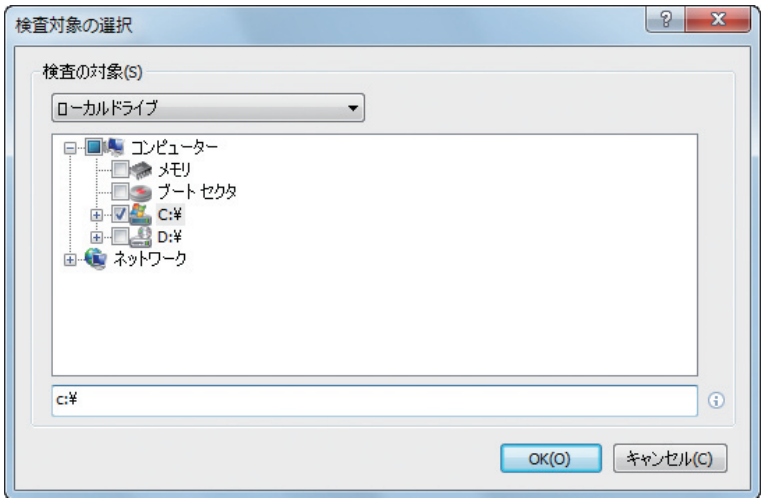
カスタム検査は、スキャン対象やスキャン方法などのスキャンパラメーターを自分で指定したい場合に最適なソリューションです。カスタム検査の利点は、パラメーターを詳細に設定できることです。設定はユーザー定義の検査プロファイルに保存できます。これは、同じパラメーターで検査を繰り返し実行する場合に便利です。
検査の対象を選択するには、[コンピュータの検査] > [カスタム検査] を選択し、[検査の対象] ドロップダウンメニューからオプションを選択するか、またはツリー構造から個別の対象を選択します。対象にするフォルダーまたはファイルのパスを入力して、検査対象を指定することもできます。システムの検査で追加の駆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] オプションを選択します。さらに、[設定...] > [駆除] をクリックして、3種類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。

検査対象

[検査の対象] ウィンドウでは、マルウェアがないかどうかを検査する対象（メモリ、ドライブ、セクタ、ファイルとフォルダ）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―マップされたネットワークドライブをすべて選択します。
●選択肢なし―すべての選択をキャンセルします。

検査に組み込みたい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。コンピューター上で使用できる全てのフォルダーを表示しているツリー構造から対象を選択します。



検査対象にすばやく移動したり、任意の対象を直接追加するには、フォルダーリストの下の空白のフィールドに対象を入力します。これが可能なのは、ツリー構造内で対象を選択しておらず、[検査の対象] メニューに [選択肢なし] が設定されている場合のみです。

検査プロファイル

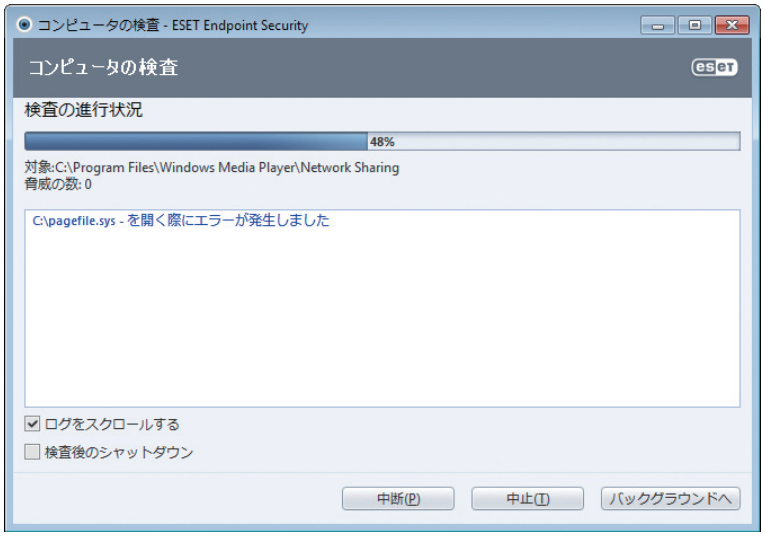
目的の検査パラメーターを保存して、後で検査を行う際に使用できます。さまざまな検査対象、検査方法、およびその他のパラメーターについて、定期的に行う検査ごとにプロファイルを作成することをお勧めします。

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、[コンピュータ] > [ウイルス・スパイウェア対策] > [コンピュータの検査] > [プロファイル...] をクリックします。[設定プロファイル] 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 [プロファイルの選択] 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の設定」にある検査設定の各パラメータの説明を参照してください。

例:既にあるスマート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。例えば、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。[設定プロファイル] ウィンドウで [追加...] ボタンをクリックします。[プロファイル名] フィールドに新しいプロファイルの名前を入力し、[ロファイルの設定をコピー] ドロップダウンメニューから [スマート検査] を選択します。次に、自分の要件に合うように、残りのパラメーターを調整します。

検査の進行状況

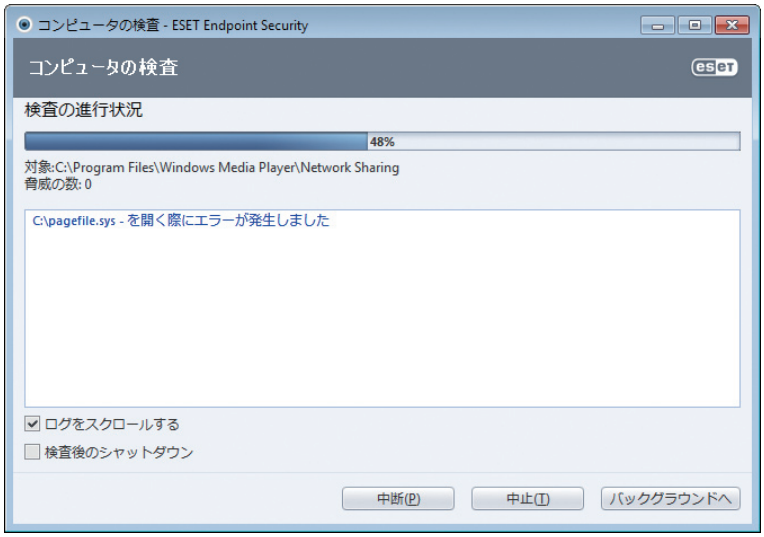
検査の進行状況ウィンドウには、検査の現在の状態および悪意のあるコードが入っているのが見つかったファイルの数に関する情報が表示されます。



NOTE

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	まだスキャンされていない対象に対する、既にスキャンされた対象の割合が進捗状況バーに表示されます。この値は、検査の対象の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。
マルウェアの数	検査中に検出されたウイルス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。
バックグラウンドへ	並行して別の検査を実行できます。実行中の検査は最小化されてバックグラウンドへ移動されます。
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。
検査後のシャットダウン	コンピュータの検査が完了するときのスケジュールされたシャットダウンを有効にします。60秒でタイムアウトするシャットダウン確認ダイアログウィンドウが開きます。要求したシャットダウンを無効にする場合は、[キャンセル]をクリックします。



[バックグラウンドへ] をクリックすると、検査がバックグラウンドに移動し、検査処理に戻ります。

4.2.1.4 スタートアップ検査

システムの起動時または、ウイルス定義データベース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。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...] ボタン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

検査レベル

システム起動時に実行されるファイルの検査のレベルを指定します。ファイルは、次のように、ファイル数に応じて昇順に整理されています。

●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)
●使用頻度が高いファイル
●使用頻度が中程度のファイル
●使用頻度が低いファイル
●すべての登録ファイル (検査対象のファイル数は最多)

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これらのファイルの実行を許可す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実行が許可され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HKCU￥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、各グループごとに固定されます。

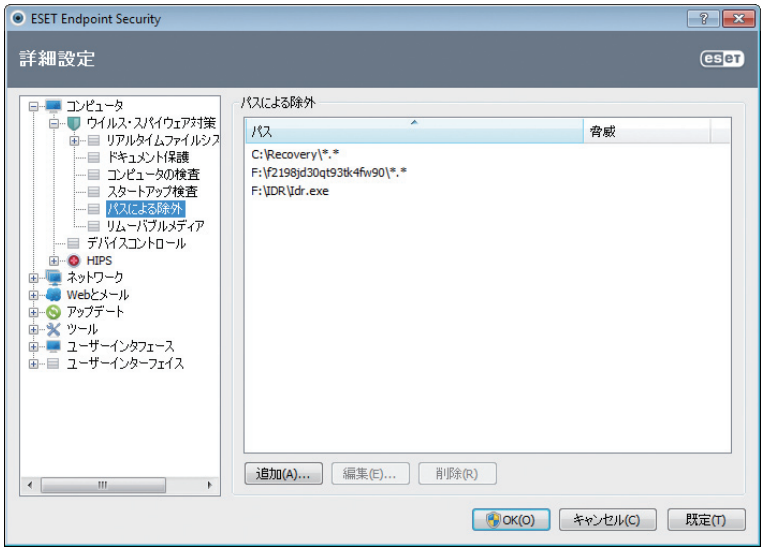
検査の優先度

以下のとおりの、検査で使用する優先度レベル。

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

4.2.1.5 パスによる除外

除外では、ファイルやフォルダーをスキャンから除外することができます。全ての対象でウイルスがスキャンされるように、これらのオプションを変更しないことをお勧めします。ただし、オブジェクトを除外する必要がある場合もあります。たとえば、スキャン時にコンピュータの速度を低下させる恐れのある大規模なデータベースエントリや、スキャンと競合するソフトウェアなどです。



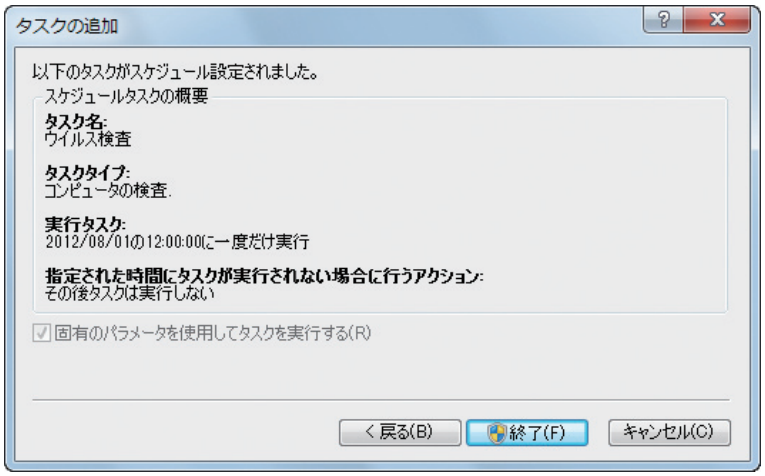
パス	除外されるファイルやフォルダのパスです。
脅威	除外されるファイルの横にマルウェアの名前がある場合、それは特定のマルウェアに対してのみファイルの除外が行われ、完全には行われないことを意味します。したがって、このファイルが後で他のマルウェアに感染した場合は、ウイルス対策機能によって検出されます。このような除外は、一定の種類のマルウェアにのみ使用できます。これは、マルウェアをレポートするマルウェア警告ウィンドウで作成する([設定の表示]をクリックしてから[検出対象外]を選択します)か、隔離するファイルでコンテキストメニューオプション[検出からの復元と除外]を使用して[設定]>[隔離]で作成できます。
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	選択したエントリーを削除します。

スキャンから対象を除外するには:

1 [追加...] をクリックします。

2 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。

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。



例

●フォルダ内のすべてのファイルを除外する場合は、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。

●すべてのファイルとサブフォルダも含めドライブ全体を除外するには、マスク"*"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、"D????.exe"という形式を使用します。疑問符は、不足している（不明な）文字の代わりに使用されます。

4.2.1.6 ThreatSenseエンジンのパラメーターの設定

ThreatSenseは、ウイルスを検出する多数の複雑な方法を備えた技術です。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さまざまな方法（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）の組み合わせが使用されます。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技術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

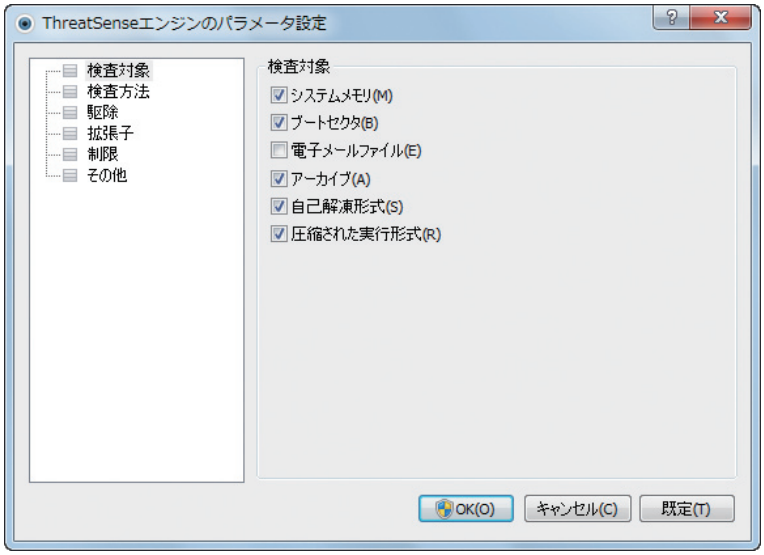
設定ウィンドウにアクセスするには、ThreatSense技術を使用する任意の機能（下記を参照）の設定ウィンドウにある[設定...]ボタンをクリックします。セキュリティシナリオごとに異なる設定が必要になることがあります。これを念頭に、ThreatSenseは、次の保護モジュールについて個々に設定することができます。

●リアルタイムファイルシステム保護
●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のパラメータは機能ごとに高度に最適化されているので、パラメータを変更すると、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を変更したり、リアルタイムファイル保護機能のアドバンスドヒューリスティックを有効にしたりすると、システムの処理速度が低下することがあります(通常は、新しく作成されたファイルのみがこれらの方法を使用してスキャンされます)。コンピュータの検査を除く全ての機能について、ThreatSenseの既定のパラメータを変更しないことをお勧めします。

検査対象

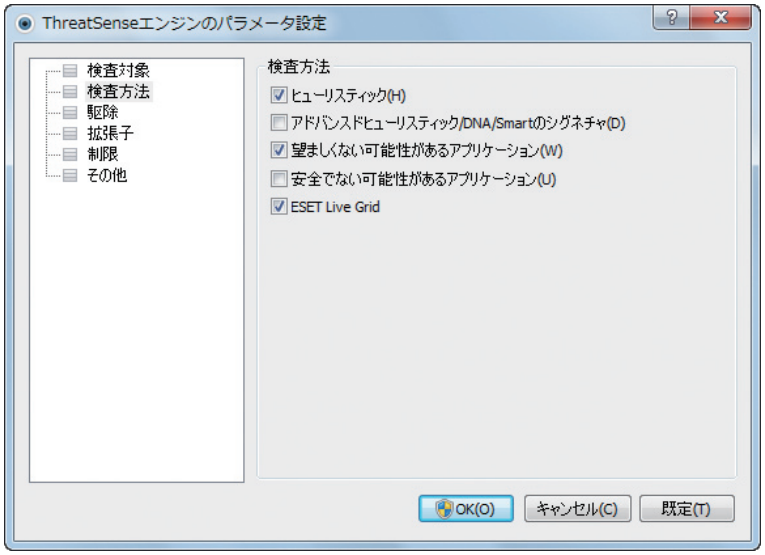
[検査対象] セクションでは、感染を検査するコンピュータのコンポーネントおよびファイルを定義できます。



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	マスターブートレコードにウイルスがいないかブートセクターを検査します。
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	プログラムは以下の拡張子をサポートします。ARJ、BZ2、CAB、CHM、DBX、GZIP、ISO/BIN/NRG、LHA、MIME、NSIS、RAR、SIS、TAR、TNEF、UUE、WISE、ZIP、ACE、およびその他多数。
自己解凍形式	自己解凍形式(SFX)とは、解凍に特殊なプログラム(アーカイブ)を必要としないアーカイブです。
圧縮された実行形式	圧縮された実行形式(標準の解凍形式とは異なる)は、実行後メモリー内で解凍されます。スキャナーでは、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がサポートされます。

検査方法

[検査方法] セクションでは、システムに対する感染をどのように検査するかを選択できます。使用可能なオプションは次のとおりです。



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。主な利点は、前には存在しなかったり、これまでのウイルス定義データベース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

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ています。アドバンスドヒューリスティックによって、プログラムの検出機能が大幅に向上します。

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。自動更新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。

望ましくない可能性があるアプリケーション

望ましくない可能性があるアプリケーション（PUA）は、必ずしも悪意があるとは限りませんが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があります。通常、このようなアプリケーションをインストールするには同意が必要です。このようなアプリケーションをコンピューターにインストールすると、システムはそれ以前とは違う動作をします。最も大きな違いは次のとおりです。

●これまでに表示されたことがない新しいウィンドウ（ポップアップ、広告など）が表示される。
●隠しプロセスがアクティブになり、実行される。
●システムリソースの使用率が高くなる。
●検索結果が異なる。
●アプリケーションがリモートサーバーと通信する。

安全でない可能性があるアプリケーション

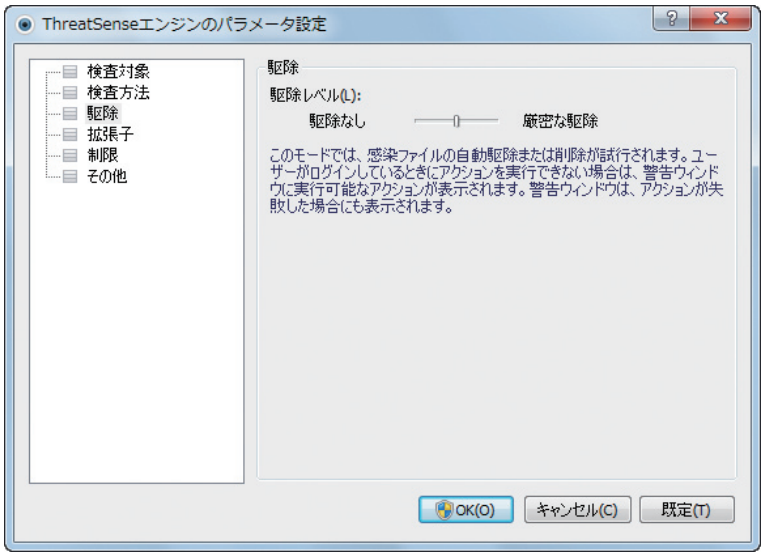
安全でない可能性があるアプリケーションは、市販の適正なソフトウェアに使用される分類です。これには、リモートアクセスツール、パスワード解析アプリケーション、キーロガー（ユーザーが入力した各キーストロークを記録するプログラム）などのプログラムが含まれます。このオプションは、既定では無効になっています。

ESET Live Grid

ESETの評価テクノロジにより、検査されたファイルの情報が、クラウドベースのESET Live Gridのデータに対して検証され、検出速度と検査速度が向上します。

駆除

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



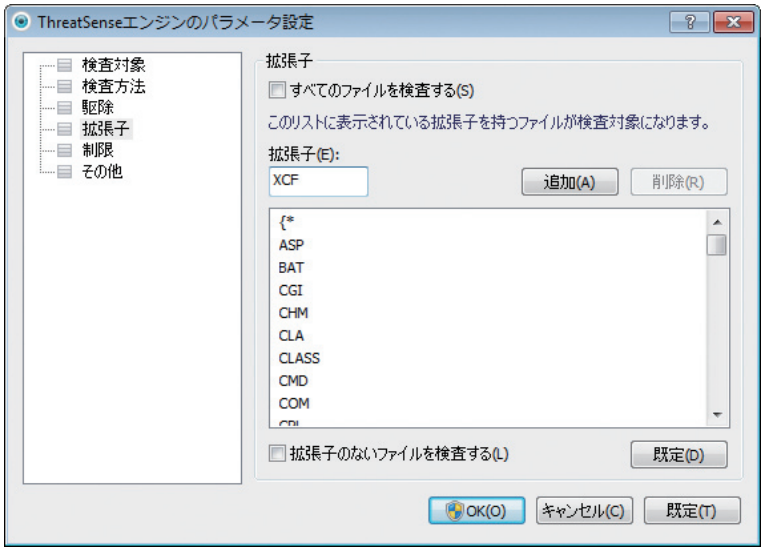
駆除なし	感染しているファイルが自動的に駆除されることはありません。警告ウィンドウが表示され、ユーザーがアクションを選択することができます。このレベルは、ウイルスが発生したときに実行する必要のあるステップを理解している経験豊富なユーザー向けです。
標準的な駆除	プログラムは、事前定義されたアクション（マルウェアの種類によって異なります）に基づいて、感染ファイルの駆除または削除を自動的に試行します。感染しているファイルの検出と削除は、画面右下隅の情報メッセージによって通知されます。適切なアクションを自動的に選択できなかった場合は、ユーザーがその後のアクションを選択することができます。あらかじめ定義されているアクションを実行できなかった場合も同様です。
厳密な駆除	全ての感染ファイルが駆除または削除されます。ただし、システムファイルは除きます。感染ファイルを駆除できなかった場合は、アクションの選択を促す警告ウィンドウが表示されます。

CAUTION

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

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。



既定では、拡張子に関係なく、全てのファイルがスキャンされます。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。[全てのファイルをスキャンする] オプションが選択解除されている場合、一覧が変わり、現在スキャンされる全てのファイル拡張子が表示されます。

拡張子のないファイルのスキャンを有効にするには、[拡張子のないファイルを検査する] オプションをチェックします。[拡張子のないファイルは検査しない] オプションは、[全てのファイルをスキャンする] オプションをチェックすると、有効になります。

特定の種類のファイルをスキャンすると、こ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。

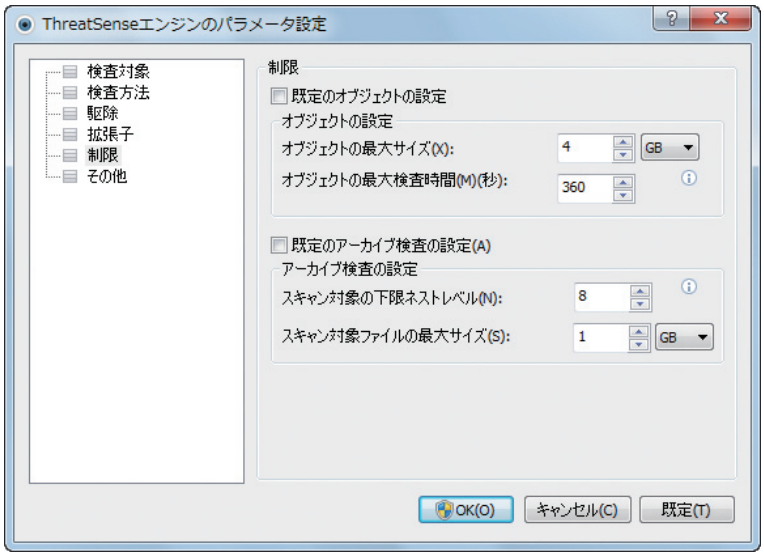
[追加] および [削除] のボタンを使用することで、特定のファイル拡張子のスキャンを有効にしたり禁止したりできます。拡張子を入力すると、[追加] ボタンがアクティブになり、新しい拡張子をリストに追加することができます。リスト内の拡張子を選択し、[削除] ボタンをクリックすると、リストから拡張子が削除されます。

特殊記号の* (アスタリスク) および? (疑問符) を使用できます。アスタリスクは任意の文字列を、疑問符は任意の記号をそれぞれ表します。除外アドレスを指定する際には、細心の注意を払ってください。その一覧には信頼できる安全なアドレスだけを掲載すべきだからです。同様に、記号の*および?を一覧内で正しく使用してください。

既定の拡張子セットのみをスキャンする場合、[既定] ボタンをクリックし、確認を求められたら [はい] をクリックします。

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。



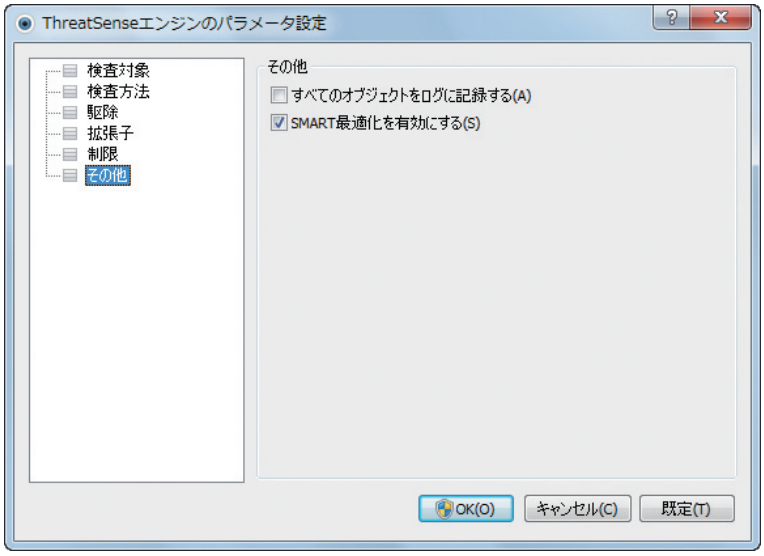
オブジェクトの最大サイズ	検査対象のオブジェクトの最大サイズを定義します。これにより、ウイルス対策機能では、指定した値より小さいサイズのオブジェクトのみが検査されます。上級ユーザーが大きいオブジェクトを検査から除外する必要がある場合のみ、このオプションを変更してください。既定値:無制限
オブジェクトの最長検査時間(秒)	オブジェクトの検査の最長時間の値を定義します。ここでユーザー定義の値が入力されていると、検査が終わっているかどうかにかかわらず、その時間が経過するとウイルス対策機能は検査を停止します。既定値:無制限
スキャン対象の下限ネストレベル	アーカイブの検査の最大レベルを指定します。既定値: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:無制限この条件を満たさないために検査が途中で終了したアーカイブのチェックボックスは、未チェックのままになります。

▸▸▸ NOTE

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。

その他

[その他] のセクションでは、次のオプションを設定できます。



すべてのオブジェクトをログに記録	このチェックボックスをチェックすると、感染していないファイルを含め、スキャンされた全てのファイルがログファイルに表示されます。たとえば、アーカイブ内にマルウェアが見つかった場合は、アーカイブ内の駆除ファイルもリストされます。
SMART最適化を有効にする	SMART最適化を有効にすると、スキャンの速度を最高に保ちながら最も効率的なスキャンレベルが確保されるように、最適な設定が使用されます。さまざまな保護モジュールで高度に検査を行い、それぞれで異なる検査方法を使用して、それらを特定のファイルタイプに適用します。SMART最適化を無効にすると、特定のモジュールのThreatSenseコアのユーザー定義設定のみが検査の実行時に適用されます。

コンピューターの検査でThreatSenseエンジンパラメータを設定する場合は、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および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。
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、このオプションをチェックします。
検査ログをスクロールする	このチェックボックスを使用すると、ログのスクロールを有効/無効にすることができます。チェックボックスをオンにすると、表示ウィンドウ内で情報が上にスクロールされます。

4.2.1.7 マルウェアが検出されたとき

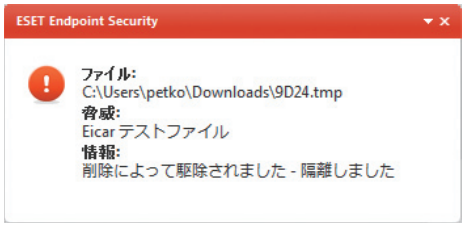
マルウェアがシステムに侵入する経路は、Webページ、共有フォルダー、メールや、コンピューターのリムーバブルデバイス(USBフラッシュメモリー、外付けハードディスク、CD、DVD、フロッピーディスクなど)など、さまざまです。

標準的な動作

ESET 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。

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

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



駆除と削除

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

ウイルスの攻撃によって悪意のあるコードがファイルに添付された場合に、駆除を行います。この場合、元の状態に戻すため、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。

POINT

駆除は、ウイルスに感染したファイルからウイルスだけを取り除き、正常なファイルに戻すことを指します。削除は、感染したファイルそのものを削除することです。ウイルスの種類によっては駆除が難しく、場合によってはファイルを削除しなければなりません。

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）。

アーカイブのファイルの削除

既定の駆除モードでは、検査対象のファイルがすべて感染ファイルである場合に限り、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、アーカイブが削除されます。

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］をクリックします。
●［スマート検査］をクリックします（詳細については、「スマート検査」を参照）。

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。

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

外部デバイスの挿入後に行うアクション	コンピュータにリムーバブルメディアデバイス（CD、DVD、USBフラッシュメモリー）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。[検査オプションの表示]を選択すると、必要なアクションを選択する通知が表示されます。
今すぐ検査	挿入したリムーバブルメディアに対してコンピュータの検査が実行されます。
後で検査	アクションは実行されず、[新規デバイスの検出]ウィンドウが閉じられます。
設定...	[リムーバブルメディア]設定セクションが開きます。

また、ESET Endpoint Securityは、所定のコンピュータ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。

4.2.3 デバイスコントロール

ESET Endpoint Securityでは、自動デバイスコントロール（CD/DVD/USBフラッシュメモリなど）を提供します。このモジュールを使用すると、拡張フィルタ /権限を検査、ブロック、または調整して、ユーザーからの指定デバイスへのアクセス方法やその作業方法を選択できます。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デバイスのユーザーによる使用を防止したいコンピュータ管理者にとって便利です。

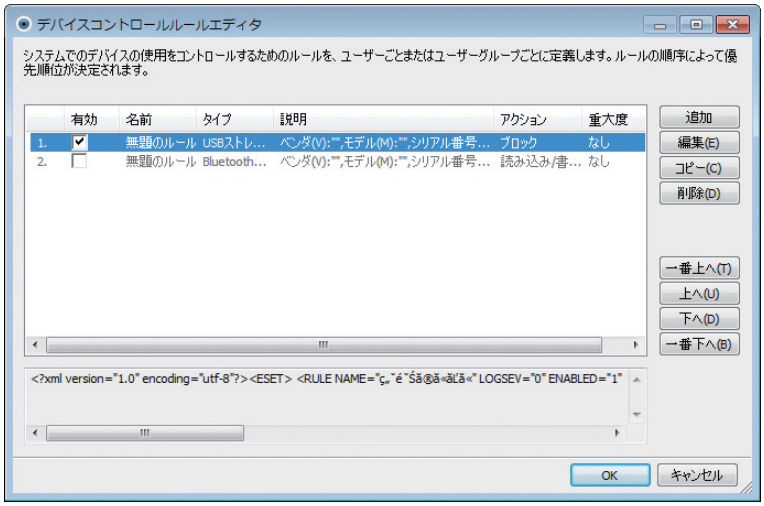
サポートされている外部デバイス
- CD/DVD/Blu-ray
- USBストレージデバイス
- FireWireデバイス
- イメージングデバイス
- USBプリンタ
- Bluetooth
- カードリーダー
- モデム
- LPT/COMポート

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。[システム統合]オプションは、デバイスコントロールをESET Endpoint Securityに統合し、[デバイスコントロールルールエディタ]ウィンドウにアクセスするための [ルールの設定...] ボタンを有効にします。

搭載された外部デバイスが、[ブロック] アクションを実行する既存ルールを適用すると、右下隅に通知ウィンドウが表示されて、そのデバイスへのアクセスは認可されません。

4.2.3.1 デバイスコントロールルール

[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に接続する外付けデバイスを的確にコントロールすることができます。



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、デバイス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。

[新規] または [変更] 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、別の選択済みルールで使用されている事前定義のオプションを備えた新規のルールを作成します。ルールをクリックすると表示されるXMLストリングは、クリップボードにコピーできます。またこれは、システム管理者がそのデータを、たとえばESET Remote Administrator内でエクスポート/インポートしたり、使用したりするのに役立ちます。

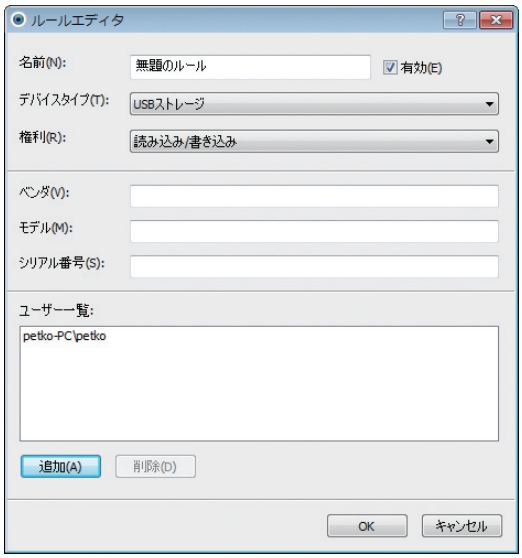
CTRLを押してクリックすれば、複数のルールを選択してアクション（削除やリスト内での上下移動など）をすべての選択済みルールに適用できます。[有効] チェックボックスはルールを無効または有効にします。将来使用するつもりのルールを永続的に削除したくない場合はチェックを外します。

このコントロールは、ルールに従って実行されますが、ルールは優先度の高いものが先頭になっています。

ルールを右クリックして、コンテキストメニューを表示できます。ここで、ルールのログエントリー用の重大度を設定できます。ログエントリーは、ESET Endpoint Securityのメインウィンドウの [ツール] > [ログファイル] から表示できます。

4.2.3.2 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ーに接続されたときに取ら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。[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。

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（USBストレージ/Bluetoothデバイス/FireWireストレージ/...）から選択します。デバイスのタイプは、オペレーティングシステムから継承されます。デバイスのタイプは、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。ドロップダウンメニューの [光学式ドライブ] デバイスは、読み取り用光メディア（CD、DVDなど）へのデータの保管を指します。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。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。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のリーダーのことです。

権限

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になります。それに対し、記憶装置のルールについては、次のいずれかの権限を選択できます。

ブロック	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だけが許可されます。
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。

デバイスのタイプによっては、適用できない権限（許可されないアクション）があります。ストレージに空き容量がある場合は、上記の3つのアクションをすべて選択できます。記憶装置以外の場合、そのうちの2つしか適用できません（たとえば、Bluetoothデバイスの場合、[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）。

次のパラメータは、ルールを微調整したり、実際のデバイスに合わせて調整するのに使用できます。このパラメータはすべて大文字小文字を区別しません。

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。
シリアル番号	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、特定のメディアのシリアル番号があります。

▸▸▸ NOTE

上記の3つの記述が空の場合、ルールでは突き合せ時にこれらのフィールドは無視されます。

ヒント:デバイスのパラメータを理解するために、該当するデバイスのタイプに許可されているルールを作成し、そのデバイスをコンピュータに接続して、デバイスコントロールのログでそのデバイスの詳細をチェックします。
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。

4.2.4 HIPS(Host-based Intrusion Prevention System)

HIPS (Host-based Intrusion Prevention System) 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、そのような活動を積極的にブロックおよび回避します。

HIPSは、[詳細設定] (F5) で [コンピュータ] > [HIPS] をクリックして見つけられます。HIPSの状態 (有効/無効) は、ESET Endpoint Securityメインウィンドウで、[設定] ペインの [コンピュータ] セクションの右側に表示されます。

CAUTION

HIPS設定は、上級ユーザー向けです。

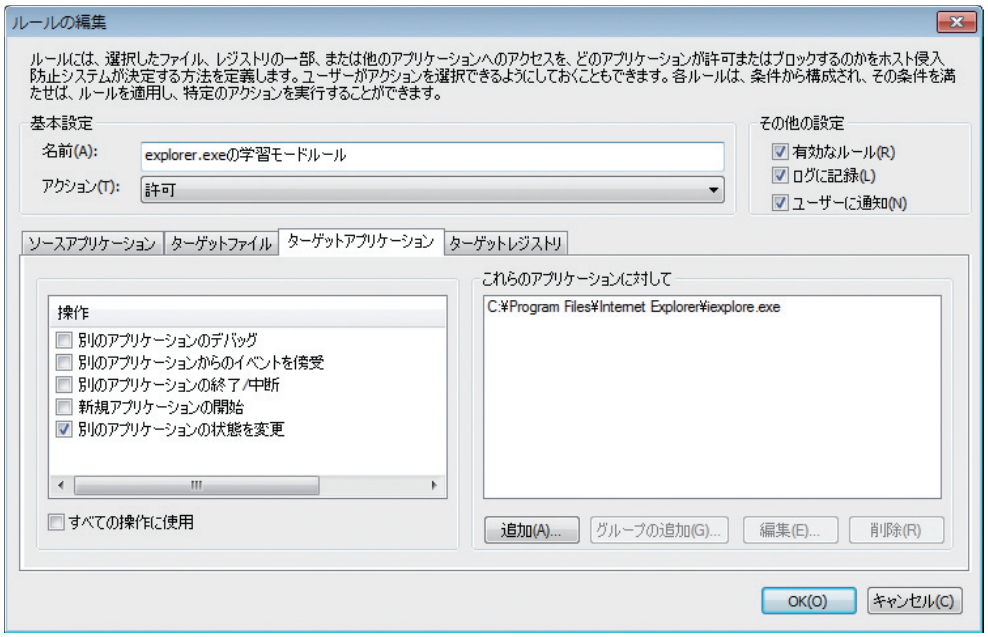
ESET Endpoint Securityには、悪意のあるソフトウェアによってウイルス・スパイウェア対策の保護機能が破損されたり無効化されたりしないようにする、自己防衛技術が組み込まれているため、システムが常時確実に保護されます。[HIPSを有効にする] 設定と [自己防衛を有効にする] 設定の変更内容は、Windowsオペレーティングシステムの再起動後に有効になります。HIPSシステム全体を無効にする場合にも、コンピュータの再起動が必要になります。フィルタリングは、次の4つのモードのいずれかで実行できます。

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を除いて有効です。
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	操作はブロックされます。
学習モード	操作は有効で、各操作の後にルールが作成されます。このモードで作成されたルールは、ルールエディタで表示できますが、手動で作成したルールや、自動モードで作成されるルールより優先度は低くなります。[学習モード]を選択すると、[学習モードの有効期限まであとX日と通知する]オプションが有効になります。この期間が過ぎると、学習モードは再度無効になります。最長期間は14日間です。この期間が過ぎると、ポップアップウィンドウが開き、ルールを編集したり、別のフィルタモードを選択したりできます。
HIPSシステム	オペレーティングシステム内部のイベントを監視し、パーソナルファイアウォールで使用されるルールに似たルールに基づいて対応します。[ルールの設定...]をクリックして、HIPSルール管理ウィンドウを開きます。このウィンドウにルールが保管されており、ここで、ルールを選択、作成、編集、または削除できます。

次の例では、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] を選択します。
2. [ターゲットアプリケーション] タブを開きます。[ソースアプリケーション] タブはブランクのままにして、[対象アプリケーション] リスト内のアプリケーションに対して [操作] リスト中のチェック付きの操作のいずれかを実行しようとしているすべてのアプリケーションに対して、新規ルールを適用します。
3. [別のアプリケーションの状態を変更] を選択します (すべての操作は製品のヘルプに説明されています。以下のイメージと同じウィンドウでF1キーを押します)。
4. 保護する1つまたは複数のアプリケーションを追加します。
5. [ユーザーに通知] オプションを有効にし、ルールが適用されるときは常にユーザーへの通知を表示します。

6 [OK] をクリックして新規ルールを保存します。



[確認] が既定のアクションの場合は、ダイアログウィンドウが毎回表示されます。それにより、ユーザーは、操作を [遮断] するのか [許可] するのかを選択できます。指定された時間内にユーザーがアクションを選択しなかった場合は、ルールに基づいて新しいアクションが選択されます。

このダイアログウィンドウでは、ダイアログウィンドウを起動したアクションと、このアクションの条件を基にルールを作成できます。厳密なパラメータは、[設定の表示] をクリックして設定できます。この方法で作成したルールは手動で作成したルールと同等であるとみなされるため、ダイアログウィンドウから作成したルールは、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。

[このプロセスに対するアクションを一時的に記憶する] オプションでは、このプロセスに対してアクション ([許可] / [遮断]) が記憶され、この操作によってダイアログウィンドウがトリガされるたびに使用されます。これらの設定は、一時的にすぎません。ルールまたはフィルタリングモードを変更してから、HIPS機能をアップデートするかシステムを再起動した場合、それらの変更は削除されます。

4.3 ネットワーク

パーソナルファイアウォールによって、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が検査され、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ーによる攻撃から保護したり、一部のサービスをブロックしたりすることができます。また、HTTP、POP3、およびIMAPプロトコルについてウイルスからの保護を実現することもできます。この機能は、コンピューターのセキュリティにおける非常に重要な要素です。

パーソナルファイアウォールの設定は、[設定] ペインで [ネットワーク] をクリックすると表示されます。ここでは、フィルタリングモード、ルール、および詳細設定を調整することができます。ここから、プログラムのより詳細な設定にアクセスすることもできます。

すべてのネットワークトラフィックを確実にブロックする唯一の方法は、[すべてのネットワーク通信を遮断する:ネットワーク接続をしない] をクリックすることです。すべての内向きおよび外向きの通信は、パーソナル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。

[フィルタリングを無効にする:すべての通信を許可する] オプションは、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とは逆です。このオプションを選択すると、パーソナル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、すべての内向き通信および外向き通信が許可されます。ファイアウォールが存在しないのと同じことになります。ネットワークトラフィックのフィルタリングが [ブロック] 状態の間は、[フィルタリングモードへ切り替え] オプションによりファイアウォールが有効になります。

以下のオプションは、自動フィルタリングモードが有効な場合に使用可能です。

自動フィルタリングモード	フィルタリングモードを変更するには、[対話型フィルタリングモードへ切り替え]オプションをクリックします。

ゾーンの設定...
-信頼済みゾーンの設定オプションが表示されます。
以下のオプションは、対話型フィルタリングモードが有効な場合に使用可能です。

対話型フィルタリングモードへ切り替え	フィルタリングモードを変更するには、現在のフィルタリングモードに応じて、[自動フィルタリングモードへ切り替え]または[例外付きの自動フィルタリングモードへ切り替え]をクリックします。

ルールとゾーンの設定...
-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するための [ゾーンとルールの設定] ウィンドウが開きます。

ネットワークでのコンピュータの保護モードを変更する...
-徹底的な保護モードと許容モードのいずれにするかを選択できます。

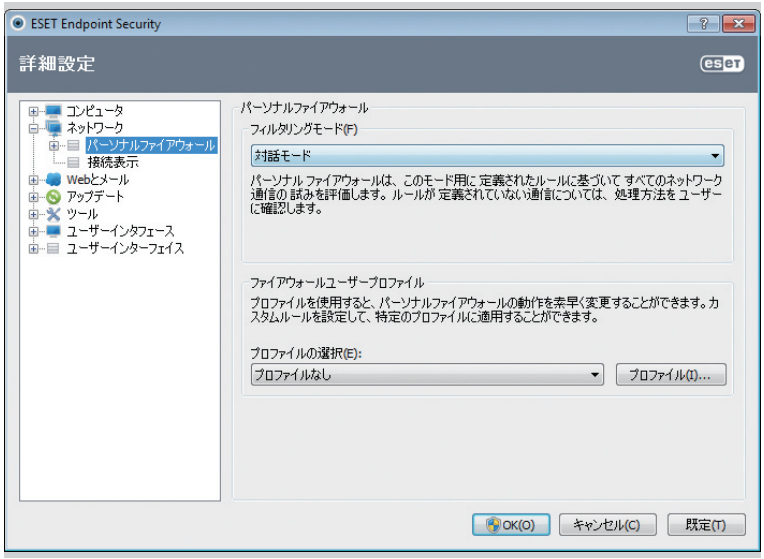
パーソナルファイアウォールの詳細設定...
-ファイアウォールの詳細設定オプションにアクセスすることができます。

4.3.1 フィルタリングモード

ESET Endpoint Securityのパーソナルファイアウォールには、5つのフィルタリングモードがあります。フィルタリングモードは、[ネットワーク]＞[パーソナルファイアウォール]をクリックし、[詳細設定](F5)にあります。ファイアウォールの動作は、選択した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。

フィルタリングは、次の5つのモードのいずれかで実行できます。

自動モード	既定のモードです。このモードは、ルールを定義せずに、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。自動モードでは、指定したシステムについて全ての送信トラフィックを許可し、ネットワーク側から開始された全ての新しい接続をブロックすることができます。
例外(ユーザー定義ルール)のある自動モード	自動モードの他に、カスタムのユーザ定義ルールも追加できます。
対話モード	パーソナル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することができます。さらに、許可するか拒否するかというその決定を、パーソナルファイアウォールの新しいルールとして記録することもできます。ユーザーがこの時点で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、パーソナル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。パーソナルファイアウォールの初期設定に適しています。事前定義されたパラメータに従って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。学習モードでは安全を確保できないため、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。

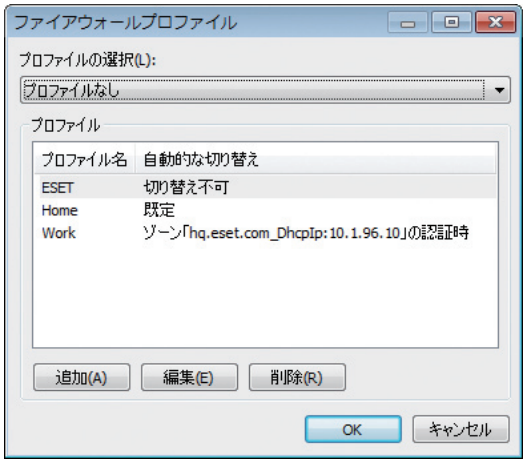


プロファイルは、ESET Endpoint Securityパーソナルファイアウォールの動作を制御するためのツールです。

4.3.2 ファイアウォールプロファイル

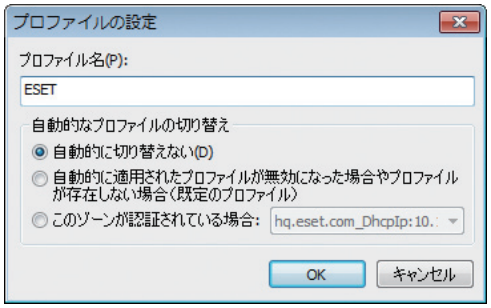
プロファイルを使用して、ESET Endpoint Securityパーソナルファイアウォールの動作を制御できます。パーソナルファイアウォールルールの作成時または編集時に、そのルールを特定のプロファイルに割り当てることもすべてのプロファイルに適用することもできます。1つのプロファイルを選択すると、グローバルルール（プロファイルの指定がないルール）と選択したプロファイルに割り当てられているルールのみが適用されます。パーソナルファイアウォールの動作を簡単に変更できるように、さまざまなルールを割り当てた複数のプロファイルを作成することができます。

[プロファイル...] ボタン（「フィルタリングモード」のセクションの図を参照）をクリックし、[ファイアウォールプロファイル] ウィンドウを開きます。このウィンドウからは、プロファイルを [追加]、[編集] または [削除] できます。ただし、プロファイルを [編集] または [削除] する場合は、[プロファイルの選択] ドロップダウンメニューでプロファイルを選択しないでください。プロファイルを追加または編集する場合、プロファイルが実行される条件を定義することもできます。



プロファイルの作成時には、そのプロファイルを実行するイベントを選択できます。使用可能なオプションは次のとおりです。

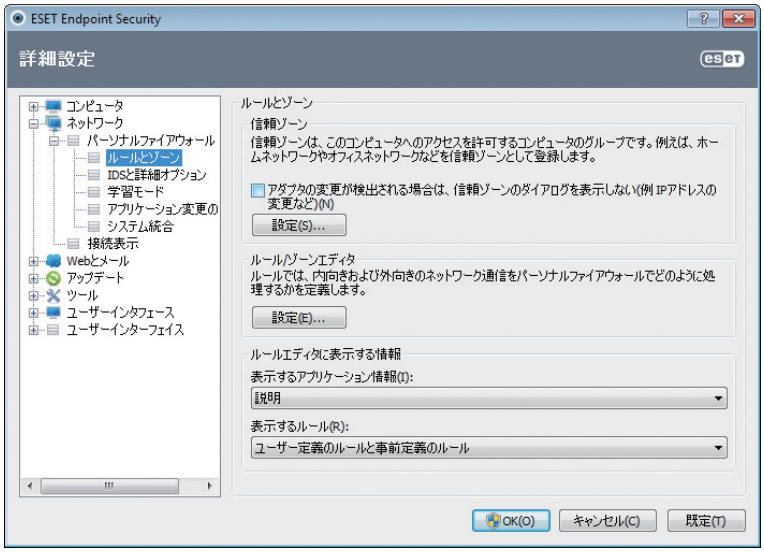
●自動的に切り替えない—自動実行がオフになります（プロファイルを手動で有効にする必要があります）。
●自動的に適用されたプロファイルが無効になった場合やプロファイルが存在しない場合（既定のプロファイル）—自動プロファイルが無効になっており（信頼されないネットワークにコンピュータが接続されている（「ネットワーク認証」のセクションを参照））、他のプロファイルが代わりに有効になっていない（別の信頼されるネットワークにコンピュータが接続されていない）場合、パーソナルファイアウォールはこのプロファイルに切り替えられます。1つのプロファイルのみをこの切り替えに指定できます。
●このゾーンが認証されている場合—指定されたゾーンが認証された場合にこのプロファイルが実行されます（「ネットワーク認証」のセクションを参照）。



パーソナル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。

4.3.3 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効果的に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。パーソナルファイアウォールでは、ルールによって定義された接続が確立された場合に実行するアクションを定義することができます。ルールの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] > [パーソナルファイアウォール] > [ルールとゾーン] に移動します。



[信頼ゾーン] セクションの [設定...] ボタンをクリックし、信頼ゾーンの設定ウィンドウを表示します。[ネットワークアダプタ設定の変更が検出された場合は、信頼ゾーンのダイアログを表示しない] オプションを指定すると、新しいサブネットの存在が検出されるたびに、信頼できるゾーンの設定ウィンドウを無効にできます。現在指定されているゾーン設定が自動的に使用されます。

NOTE

パーソナルファイアウォールが自動モードに設定されている場合、これらの設定の一部は使用できません。

[ルール/ゾーンエディタ] セクションの [設定...] ボタンをクリックすると、[ゾーンとルールの設定] ウィンドウが表示され、ルールまたはゾーンの概要が (現在選択されているタブに応じて) 表示されます。ウィンドウは2つのセクションに分かれています。上部のセクションには、全てのルールが簡略化された形式で表示されます。下部のセクションには、上部のセクションで現在選択しているルールの詳細情報が表示されます。ウィンドウ下部に [新規]、[編集]、および [削除] ボタンが配置されていて、ルールを設定できます。

接続は内向き通信と外向き通信に分けることができます。内向き通信は、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。外向き通信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ーにアクセスします。

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する必要があります。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。パーソナル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。

表示するアプリケーション情報では、ルール一覧でのアプリケーションの表示方法を指定できます。使用可能なオプションは次のとおりです。

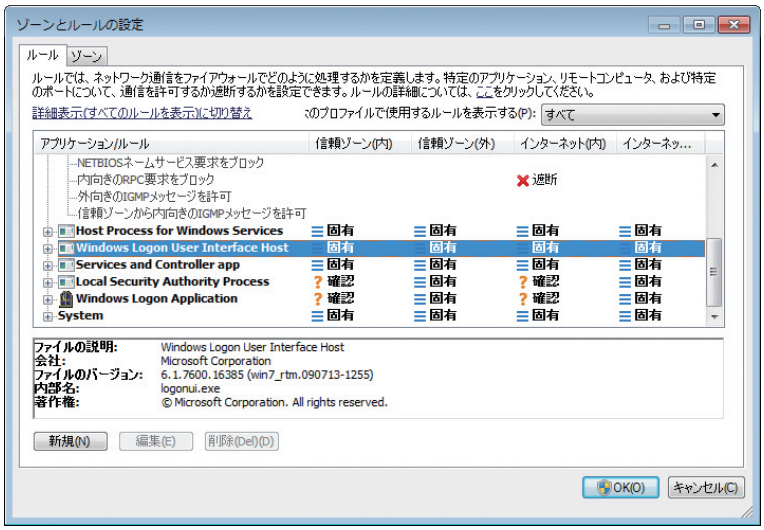
●フルパス—アプリケーションの実行ファイルへのフルパス。
●説明—アプリケーションの説明。
●名前—アプリケーションの実行可能ファイルの名前。

[表示するルール] リストでは、表示するルールのタイプを選択します。

●ユーザー定義のルールのみ—ユーザーによって作成されたルールのみが表示されます。
●ユーザー定義ルールと事前定義ルール—ユーザー定義ルールとあらかじめ定義されている既定のルールが全て表示されます。
●全てのルール（システムを含む）—全てのルールが表示されます。

4.3.3.1 ルールの設定

[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。既定では、新しい通信に対するユーザーの対応に従って、自動的にルールが追加されます。このウィンドウの下部にアプリケーションに関する詳細情報を表示するには、アプリケーションの名前をクリックします。



ルールに関連する各行の最初には、情報の展開/折りたたみに使用するボタン（+/-）があります。[アプリケーション/ルール] 列でアプリケーションの名前をクリックすると、このウィンドウの下部にルールに関する情報が表示されます。コンテキストメニューを使用すると、表示モードを変更することができます。コンテキストメニューは、ルールの追加、編集、および削除にも使用できます。

●信頼済みゾーン内/外—信頼済みゾーン内の受信または送信通信に関連するアクション。
●インターネット内/外—インターネット接続と関係する受信または送信通信のアクション。

通信の種類（方向）ごとに、次のアクションを選択することができます。

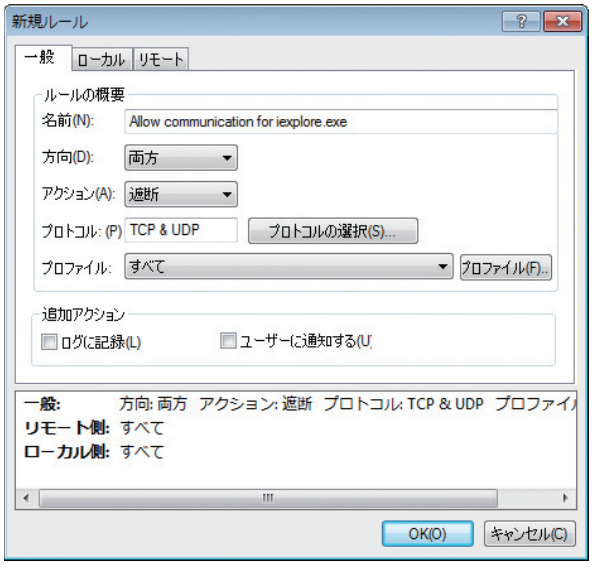
- ✔ 許可—通信を許可する場合に使用します。
- ? 確認—通信を確立するたびに、許可するか遮断するかを確認するよう求められます。
- ✖ 遮断—通信を遮断する場合に使用します。
- ☰ 固有—他のアクションをふまえた分類はできません。たとえば、IPアドレスまたはポートがパーソナルファイアウォールを通過できる場合、関連アプリケーションの着信または発信通信が許可されているかどうかに関係なく、このIPアドレスまたはポートを確実に分類することはできません。

ネットワークにアクセスする新しいアプリケーションをインストールした場合や、既存の接続（リモート側、ポート番号など）を変更する場合は、新しいルールを作成する必要があります。既存のルールを編集する場合は、[ルール] タブが選択されていることを確認し、[編集] ボタンをクリックします。

4.3.3.2 ルールの編集

監視するパラメーターのいずれかが変更されるたびに、ルールを変更する必要があります。このようなときには、ルールが条件を満たさなくなるので、指定したアクションは適用されません。パラメーターが変更されている場合は、指定した接続が拒否され、該当するアプリケーションの動作に問題が生じる場合があります。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。
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、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。
- ●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。また、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。



プロトコル - ルールに使用される転送プロトコル。[プロトコルの選択...] をクリックし、[プロトコルの選択] ウィンドウを開きます。

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...] ボタンを使用して、カスタムファイアウォールプロファイルを選択します。

[ログに記録] をクリックすると、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] オプションを選択すると、ルールが適用されたときに通知が表示されます。

[情報] ボックス内の3つのすべてのタブの下部に、ルールの概要が表示されます。同じ情報は、メインウィンドウでルールをクリックしても表示できます ([ツール] > [ネットワーク接続] を開き、ルールを右クリックして、[詳細を表示] オプションを有効にします (「ネットワーク接続」の章を参照。)

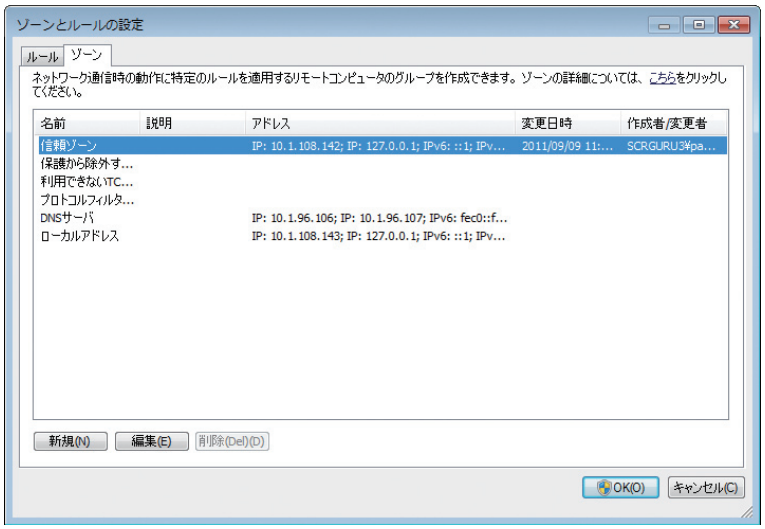
新しいルールを作成するときは、ルールの名前を [名前] フィールドに入力する必要があります。ルールを適用する方向を [方向] ドロップダウンメニューから選択します。通信がルールに適合したときに実行するアクションを [アクション] ドロップダウンメニューで設定します。

新しいルールを追加するわかりやすい例として、インターネットブラウザーにネットワークへのアクセスを許可する場合があります。この場合、次のように設定する必要があります。

- [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。
- ブラウザアプリケーションを表すプロセス (Internet Explorerの場合は iexplore.exe) を [ローカル] タブに追加します。
- 標準のインターネット閲覧アクティビティを許可する場合のみ、[リモート] タブでポート番号80を有効にします。

4.3.4　ゾーンの設定

[ゾーンの設定] ウィンドウでは、ゾーンの名前、説明、ネットワークアドレスのリスト、およびゾーン認証を指定できます（詳細については「ゾーン認証-クライアントの設定」を参照してください）。



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。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、完全に信頼され、パーソナル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。

これらのゾーンを設定するには、[ゾーンおよびルールの設定] ウィンドウの [ゾーン] タブで [編集] ボタンをクリックします。ゾーンの [名前] と [説明] を入力し、[IPv4/IPv6アドレスを追加] ボタンをクリックしてリモートIPアドレスを追加します。

4.3.4.1　ネットワーク認証

モバイルコンピューターの場合は、接続先ネットワークのネットワークの信頼性を確認することをお勧めします。信頼ゾーンは、ネットワークアダプターのローカルIPアドレスによって識別されます。モバイルコンピューターは、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。信頼ゾーンの設定を手動で [厳密に保護] に切り替えないと、パーソナルファイアウォールでは引き続き [共有を許可] モードが使用されます。

このような状況が起きないように、ゾーン認証の使用をお勧めします。

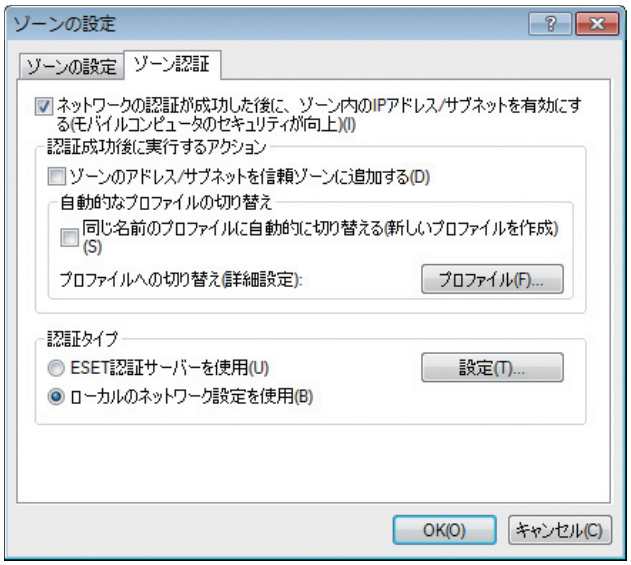
ゾーン認証-クライアントの設定

[ゾーンとルールの設定] ウィンドウの [ゾーン] タブをクリックすると、サーバーによって認証されたゾーンの名前を使用して新しいゾーンを作成できます。次に、[IPv4アドレスを追加] をクリックし、[サブネット] オプションを選択して、認証サーバー含まれるサブネットマスクを追加します。

[ゾーン認証] タブをクリックします。各ゾーンをサーバーに検証されるように設定できます。ゾーン（IPアドレスおよびサブネット）が有効になるのは、ゾーンが正常に認証された後です。たとえば、ファイアウォールのプロファイルに切り替えて、ゾーンのアドレス/サブネットを [信頼ゾーン] に追加するなどのアクションが実行されるのは、認証に成功した後のみです。

[ネットワークのサーバ認証が成功した後に...] オプションを選択して、認証に失敗した場合は無効になるゾーンを作成します。ゾーン認証が成功した後に有効になるパーソナルファイアウォールプロファイルを選択するには、[プロファイル...] ボタンをクリックします。

[ゾーンのアドレス/サブネットを信頼ゾーンに追加する] オプションを選択すると、認証が成功した後にゾーンのアドレス/サブネットが信頼ゾーンに追加されます (推奨)。認証に失敗した場合、アドレスは信頼ゾーンに追加されません。同じ名前のプロファイルに自動的に切り替える (新しいプロファイルを作成) オプションがアクティブな場合、認証に成功した後に新しいプロファイルが作成されます。[プロファイル...] ボタンをクリックし、[ファイアウォールプロファイル] ウィンドウを開きます。



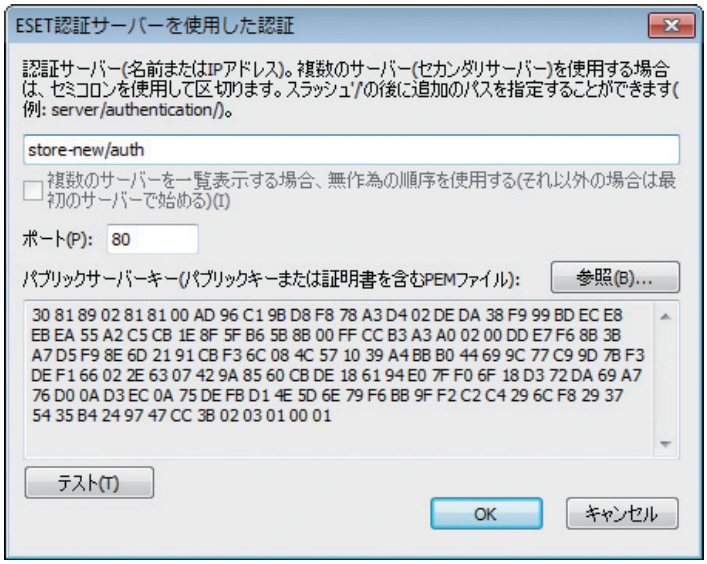
次の種類の認証を使用できます。

1) ESET認証サーバーを使用

ゾーン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。この認証プロセスは、コンピューターの接続先のネットワークごとに繰り返されます。[詳細設定...] をクリックして、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 (「ゾーン認証-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ます。サーバー名に続いて、サーバー上のキーの場所を指定するパスを入力できます (例:<サーバ名>/directory1/directory2/authentication)。最初のサーバーが使用できなくなった場合に代替サーバーとして機能するように、複数のサーバーをセミコロンで区切って入力します。

公開鍵は、次のいずれかの種類のファイルとして指定できます。

●PEM暗号化公開鍵（.pem）
　この鍵は、ESET認証サーバを使用して生成できます（「ゾーン認証-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）



設定をテストするには、[テスト] ボタンをクリックします。認証が成功すると、[サーバーの認証に成功しました] というメッセージが表示されます。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。

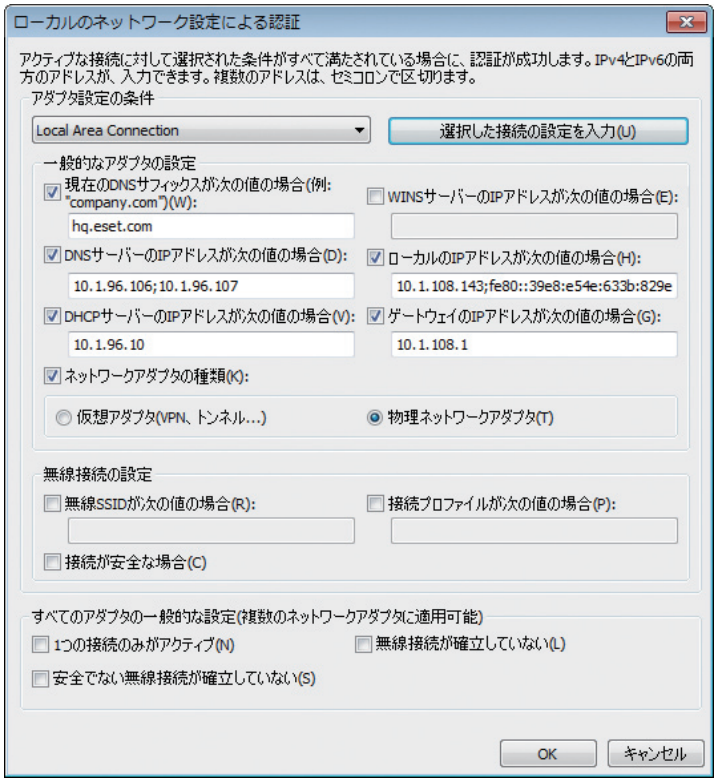
サーバーの認証に失敗しました。認証の最大時間が経過しました。	認証サーバーにアクセスできません。サーバー名/IPアドレスを確認し、クライアントとサーバーセクションのパーソナルファイアウォールの設定を確認してください。
サーバーとの通信中にエラーが発生しました。	認証サーバーが実行されていません。認証サーバーサービスを開始してください（「ゾーン認証-サーバーの設定）」のセクションを参照）。
認証ゾーンの名前がサーバーゾーンと一致していません。	設定されているゾーン名が、認証サーバーゾーンに一致していません。両方のゾーンをチェックして、それらの名前が同一であることを確認してください。
サーバーの認証に失敗しました。サーバーのアドレスが、指定されたゾーンのアドレスのリストに見つかりませんでした。	認証サーバを実行しているコンピュータのIPアドレスが、現在のゾーン設定で定義されているIPアドレス範囲外にあります。
サーバーの認証に失敗しました。無効なパブリックキーが入力された可能性があります。	指定された公開鍵が、サーバーの秘密鍵に対応していることを確認してください。また、公開鍵のファイルが破損していないことを確認してください。

▸▸▸ NOTE

本機能は日本語版ではサポートされていません。

2) ローカルのネットワーク設定を使用

認証は、ローカルのネットワークアダプターのパラメーターに基づいて実行されます。アクティブな接続に対して選択されたパラメーターがすべて有効な場合に、ゾーンは認証されます。



ゾーン認証-サーバーの設定

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、認証ゾーン名、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ゾーンを設定するときに、[ゾーン認証] セクションにインポートする必要があります。

4.3.5 接続の確立-検出

パーソナル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、新しいルール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] を有効にしたパーソナル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、パーソナル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。

新しいルールを作成する際は、慎重に、安全な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、パーソナル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は次のとおりです。

●リモート側—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。
●ポート番号—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、パーソナル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。

4.3.6 ログ

ESET Endpoint Securityのパーソナルファイアウォールでは、重要なすべての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 [パーソナルファイアウォールのログ] を選択します。

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の貴重なツールです。ESETパーソナルファイアウォールのログには次のデータが保存されます。

●イベントの日時
●イベントの名前
●ソース
●宛先のネットワークアドレス
●ネットワーク通信プロトコル
●適用されたルール、ワームの名前（特定された場合）
●関連するアプリケーション
●ユーザー

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。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。

4.3.7システム統合

ESET Endpoint Securityパーソナルファイアウォールは、いくつかのレベルで動作できます。

●すべての機能が有効―パーソナルファイアウォールが完全に統合されて、コンポーネントがアクティブになります（既定のオプション）。コンピュータがより大規模のネットワークやインターネットに接続されている場合は、このオプションを有効のままにすることをお勧めします。このオプションが一番安全で、システムを完全に保護します。
●パーソナルファイアウォールを無効にする―パーソナルファイアウォールはシステムに統合されてネットワーク通信を仲介しますが、マルウェアのチェックは実行しません。
●アプリケーションプロトコルのみ検査する―アプリケーションプロトコル（HTTP、POP3、IMAP、およびそれぞれのセキュアバージョン）の検査を実行するパーソナルファイアウォールのコンポーネントのみが有効になります。アプリケーションプロトコルが検査されない場合、リアルタイムファイルシステム保護機能とコンピューターの検査のレベルで保護されます。
●パーソナルファイアウォールを全く使用しない―パーソナルファイアウォールをシステムから完全に登録解除する場合、このオプションを選択します。検査は実行されません。これはテストの場合に便利です。アプリケーションがブロックされた場合に、ファイアウォールによってブロックされたかどうかをチェックできます。このオプションは安全性においては一番低いので、ファイアウォールを完全に無効にするときには注意してください。

コンピューターが再起動されるまで、パーソナルファイアウォール機能のアップデートを延期する-アップデートはダウンロードのみとなり、コンピューターの再起動時にインストールが実行されます。

4.4 Webとメール

Webとメール設定は、[設定] ペインで [Webとメール] をクリックすると表示されます。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。

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。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。したがって、Webアクセス保護について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とIMAP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たメッセージにも対応しています。

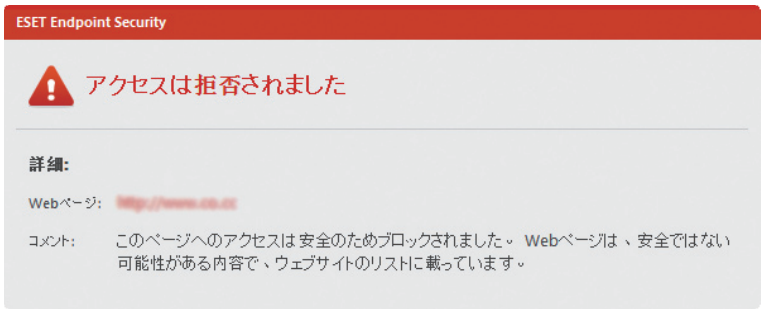
[迷惑メール対策機能] は、迷惑メールメッセージをフィルタリングします。

無効にする	メールクライアントのWeb/メール/迷惑メール対策保護機能を無効にします。
設定...	Web/メール/迷惑メール対策保護機能の詳細設定を開きます。
ユーザーのホワイトリスト	安全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。ホワイトリストにリストされている送信元アドレスを持つメールメッセージに対しては迷惑メールの検査を行いません。
ユーザーのブラックリスト	安全でない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。ブラックリストにリストされている送信元アドレスを持つメールメッセージは、迷惑メールであると見なされます。
ユーザーの除外リスト	スプーフィングされており迷惑メールに使用さ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ウィンドウを開きます。除外リストにリストされている送信元アドレスを持つメールメッセージに対しては常に迷惑メールの検査を行います。既定では、既存メールクライアントのアカウントにある電子メールアドレスは、除外リストに入っています。

4.4.1 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ーの標準機能です。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ブラウザーとリモートサーバーとの間で行われるHTTP（Hypertext Transfer Protocol）および HTTPS（暗号化通信）のルールに準拠した通信を監視することによって機能します。

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）のさまざまな手法を用いる犯罪行為を指します。このアクティビティの詳細は、用語集を参照してください。ESET Endpoint Security はフィッシング対策保護をサポートします。該当する内容の既知のWebページは常にブロックされます。



Webアクセス保護を有効にすることを強くお勧めします。このオプションには、ESET Endpoint Securityのメインウィンドウから [設定] > [Webとメール] > [Webアクセス保護] と移動するとアクセスできます。

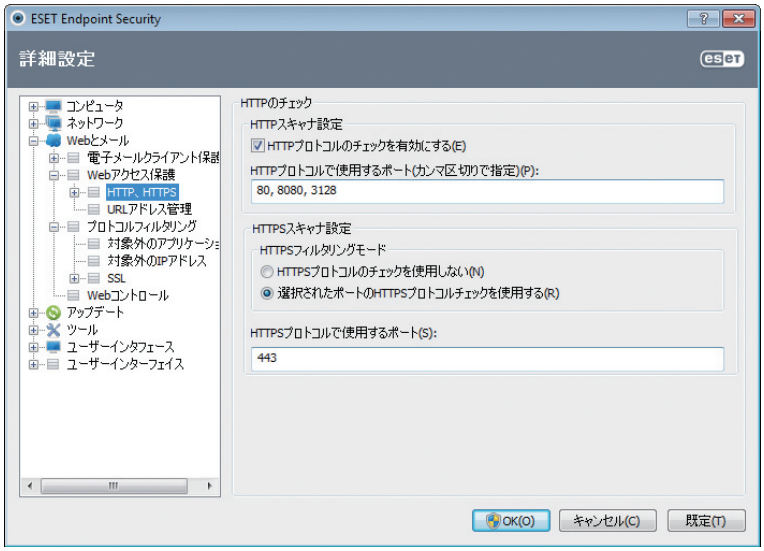
4.4.1.1 HTTP、HTTPS

既定では、ESET Endpoint Securityは、大半のインターネットブラウザーの標準を使用するよう設定されています。HTTPスキャナーの設定オプションは、[詳細設定] (F5) > [Webとメール] > [Webアクセス保護] > [HTTP/HTTPS] で変更できます。[HTTP/HTTPSスキャナ] メインウィンドウで、[HTTPのチェックを有効にする] オプションを選択または選択解除できます。また、HTTP通信に使用するポート番号も指定できます。既定では、ポート番号は80（HTTP）、8080、および3128（プロキシサーバ）が指定されています。

ESET Endpoint SecurityはHTTPSプロトコルのチェックをサポートします。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）の暗号化手法を使用した通信を検査します。HTTPSのチェックは、次のモードで実行できます。

HTTPSプロトコルのチェックを使用しない	暗号化通信はチェックされません。
選択されたポートのHTTPSプロトコルチェックを使用する	[HTTPSプロトコルで使用するポート] で定義されているポートに関してのみHTTPSのチェックを行います。
選択したポートに対してHTTPSプロトコルのチェックを使用する	ブラウザセクションで指定されていて、[HTTPSプロトコルで使用するポート] で定義されているポートを使用するアプリケーションのみをチェックします。既定では、ポート443が設定されます。

既定では、暗号化された通信は検査されません。暗号化された通信の検査とスキャナ設定の表示を有効にするには、[詳細設定] セクションの [SSLプロトコルチェック] に移動し、[Webとメール] > [プロトコルフィルタリング] > [SSL]) に移動し、[SSLプロトコルを常に検査する] オプションを有効にします。



Webブラウザーのアクティブモード

ESET Endpoint Securityには、Webブラウザーの検査モードを定義する [アクティブモード] サブメニューがあります。

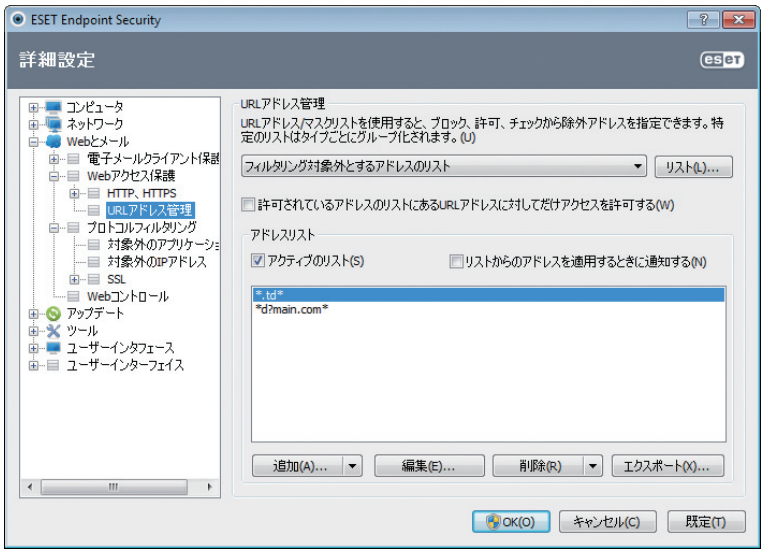
アクティブモードは、Webブラウザーであるかどうかに関係なく、インターネットにアクセスする全てのアプリケーションの転送データを検証するので便利です (詳細については、「Webと電子メールのクライアント」を参照してください。)。アクティブモードを無効にすると、アプリケーションの通信はバッチ処理で段階的に監視されます。これにより、データ確認処理の効果は低下しますが、一覧に列挙されたアプリケーションに対する互換性は向上します。使用中に何も問題が発生しなければ、目的のアプリケーションの隣にあるチェックボックスをチェックして、アクティブ検査モードを有効にすることをお勧めします。アクティブモードは次のように動作します。管理対象のアプリケーションによってデータがダウンロードされると、まず、ESET Endpoint Securityによって作成された一時ファイルにデータが保存されます。この時点では、そのアプリケーションでデータを使用することはできません。ダウンロードが完了すると、悪意のあるコードがないかどうかが検査されます。マルウェアが検出されなければ、元のアプリケーションにデータが送信されます。このプロセスによって、管理対象のアプリケーションによる通信が完全に制御されます。パッシブモードが有効な場合は、タイムアウトを避けるために、データが少しずつ元のアプリケーションに送信されます。

4.4.1.2 URLアドレス管理

URLアドレス管理のセクションでは、ブロック、許可、またはチェックから除外するHTTPアドレスを指定できます。[追加]、[編集]、[削除] および [エクスポート] ボタンを使用して、アドレス一覧を管理します。ブロックされるアドレスの一覧にあるWebサイトにはアクセスできません。除外されるアドレスの一覧にあるWebサイトには、悪意のあるコードがあるかどうかを検査せずにアクセスできます。[許可されているアドレスのリストにあるURLアドレスに対してだけアクセスを許可する] オプションを選択すると、許可するアドレスの一覧にあるアドレスのみにアクセスでき、その他のHTTPアドレスは全てブロックされます。

[フィルタリング対象外とするアドレスのリスト] にURLアドレスを追加すると、そのアドレスは検査から除外されます。また、[許可するアドレスのリスト] または [ブロックするアドレスのリスト] に追加して、特定のアドレスを許可またはブロックできます。[リスト...] ボタンをクリックすると、[HTTPアドレス/マスクリスト] ウィンドウが表示され、アドレスをリストに [追加] または [削除] できます。リストにHTTPS URLアドレスを追加する場合、[SSLプロトコルを常に検査する] を有効にする必要があります。

どのリストでも、特殊記号の* (アスタリスク) および? (疑問符) を使用できます。アスタリスクは任意の文字列を、疑問符は任意の一文字をそれぞれ表します。除外アドレスを指定する際には、細心の注意を払ってください。その一覧には信頼できる安全なアドレスだけを掲載すべきだからです。同様に、記号の*および?を一覧内で正しく使用してください。一覧を有効にするには、[一覧アクティブオプション] を選択します。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、[リストからのアドレスを適用するときに通知する] を選択します。



追加.../ファイルから	手動で([追加])、または単純なテキストファイルから([ファイルから])、アドレスをリストに追加できます。[ファイルから]オプションを使用すると、テキストファイルに保存されている複数のアドレスを追加できます。
編集...	マスク("*"および"?")を追加するなどして、手動でアドレスを編集します。
削除/全て削除	リストから選択したアドレスを削除する場合、[削除]をクリックします。全てのアドレスを削除する場合、[すべて削除]を選択します。
エクスポート...	現在のリストにあるアドレスを単純なテキストファイルに保存します。

4.4.2 電子メールクライアント保護

電子メールクライアント保護では、POP3プロトコルおよびIMAPプロトコルで受信したメール通信が検査されます。ESET Endpoint Securityは、Microsoft Outlook用のプラグインおよびその他のメールクライアントを使用して、メールクライアントからの全通信（POP3、MAPI、IMAP、HTTP）を検査します。受信メッセージを検査するときには、ThreatSenseスキャンエンジンに用意されている詳細なスキャン方法が全て使用されます。そのため、ウイルス定義データベースと突き合わせて一致する前であっても、悪意のあるプログラムの検出が可能です。POP3プロトコルとIMAPプロトコルの通信のスキャンは、使用されるメールクライアントからは独立しています。

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] にあります。

ThreatSenseエンジンのパラメータ設定—ウイルススキャナーの詳細設定では、スキャン対象や検出方法などを設定することができます。[設定...] をクリックすると、ウイルススキャナーの詳細設定ウィンドウが表示されます。

メールが検査された後、スキャン結果を記載した通知をメールに追加することができます。[受信メールと既読メールにタグメッセージを追加] および [送信メールにタグメッセージを追加] を選択できます。ただし、検査通知を完全に信頼することはできません。これは、問題があるHTMLメールで検査通知が表示されなかったり、一部のウイルスによって検査通知が偽造されたりすることがあるためです。検査通知は、受信/既読メールまたは送信メール（あるいはその両方）に追加することができます。使用可能なオプションは次のとおりです。

追加しない	検査通知は追加されません。
感染メールのみ	悪意のあるソフトウェアをもった検査通知のみに検査済みのマークが付けられます（既定）。
すべてのメール	スキャンされた全てのメールに検査通知が追加されます。

受信した感染メールと表示/送信した感染メールの件名に注を追加
-メールの保護で、感染しているメールの件名にウイルス警告を追加する場合はこのチェックボックスをチェックします。この機能は、感染しているメールを件名に基づいて単純にフィルタリングする場合に有効です（メールクライアントでサポートされている場合）。また、受信者の信頼を高めることができ、マルウェアが検出された場合、特定のメールまたは送信者のマルウェアについての貴重な情報を得ることができます。

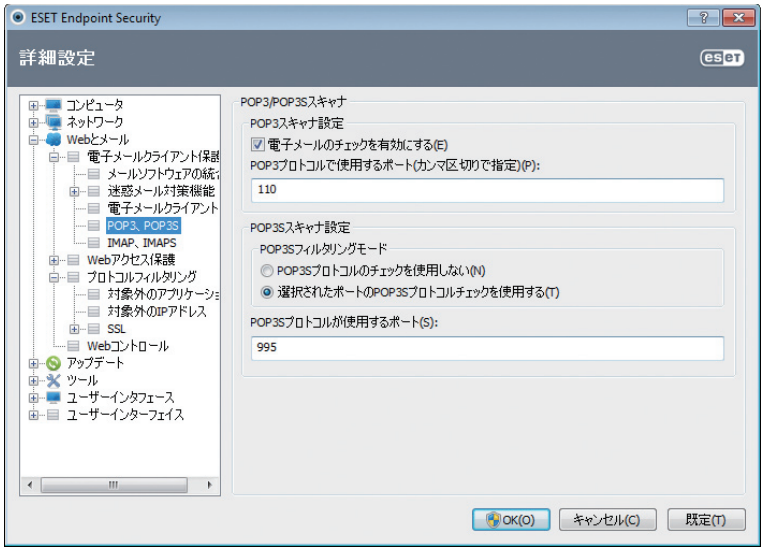
感染メールの件名に追加する目印のテンプレート
-感染メールの件名のプレフィックス形式を変更する場合はこのテンプレートを編集します。この機能を実行すると、メッセージの件名"Hello"が、プリフィクス値"[virus]"（"[virus] Hello"の形式）で置き換えられます。変数の%VIRUSNAME%は検出されたマルウェアです。

4.4.2.1 POP3/POP3Sのフィルタ

POP3プロトコルは、電子メールクライアントアプリケーションでのメール通信の受信の受信に最もよく使用されているプロトコルです。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。

この検査を行う保護モジュールは、システムの起動時に自動的に起動され、次いでメモリーでアクティブになります。モジュールが正常に機能できるように、必ず有効にしてください。POP3プロトコルの検査は、メールクライアントを設定し直さなくても、自動的に実行されます。既定では、ポート110での通信が全てスキャンされますが、他の通信ポートも必要に応じて追加できます。複数のポート番号は、コンマで区切る必要があります。

既定では、暗号化された通信は検査されません。暗号化された通信の検査とスキャナー設定の表示を有効にするには、[詳細設定] セクションの [SSLプロトコルチェック] に移動し、[Webとメール] > [プロトコルフィルタリング] > [SSL]) に移動し、[SSLプロトコルを常に検査する] オプションを有効にします。



このセクションでは、POP3およびPOP3Sプロトコルの検査を設定できます。

電子メールのチェックを有効にする	有効にすると、POP3を使用する全てのトラフィックで悪意のあるソフトウェアが監視されます。
POP3プロトコルで使用するポート	POP3プロトコルによって使用されるポートのリストです(既定では110)。

ESET Endpoint Securityは、POP3Sプロトコルの検査もサポートしています。このタイプの通信では、暗号化チャンネルを使用して、サーバ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) の暗号化手法を使用した通信を検査します。

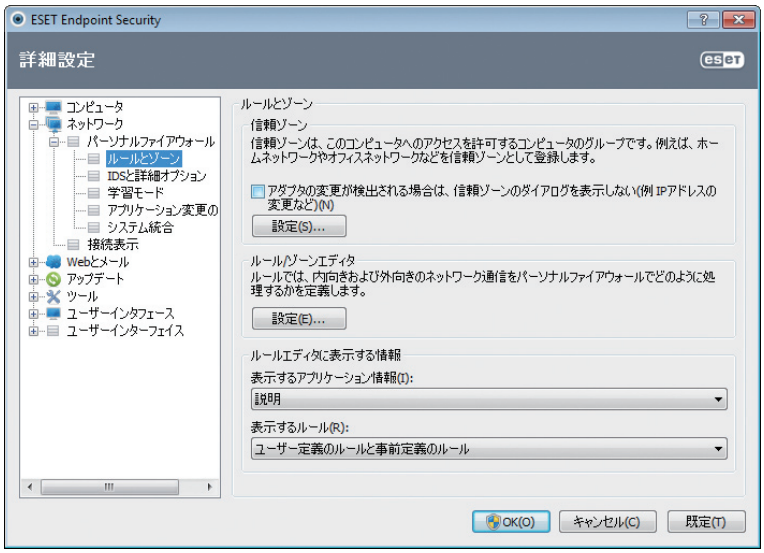
POP3Sプロトコルのチェックを使用しない	暗号化通信はチェックされません。
選択されたポートのPOP3Sプロトコルチェックを使用する	[POP3Sプロトコルで使用するポート]で定義されているポートに関してのみPOP3Sのチェックを有効にする場合は、このオプションを選択します。
POP3Sプロトコルが使用するポート	検査するPOP3Sポートのリストです(既定では995)。

4.4.2.2 IMAP、IMAPSプロトコルの検査

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。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、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維持できます。ESET Endpoint Securityでは、使用しているメールクライアントにかかわらず、このプロトコルが保護されます。

この検査を行う保護モジュールは、システムの起動時に自動的に起動され、次いでメモリーでアクティブになります。モジュールが正常に機能できるように、必ず有効にしてください。IMAPプロトコル検査は、電子メールクライアントを設定し直さなくても、自動的に実行されます。既定では、ポート143での通信が全てスキャンされますが、他の通信ポートも必要に応じて追加できます。複数のポート番号は、コンマで区切る必要があります。

既定では、暗号化された通信は検査されません。暗号化された通信の検査とスキャナー設定の表示を有効にするには、[詳細設定] セクションの [SSLプロトコルチェック] に移動し、[Webとメール] > [プロトコルフィルタリング] > [SSL]）に移動し、[SSLプロトコルを常に検査する] オプションを有効にします。

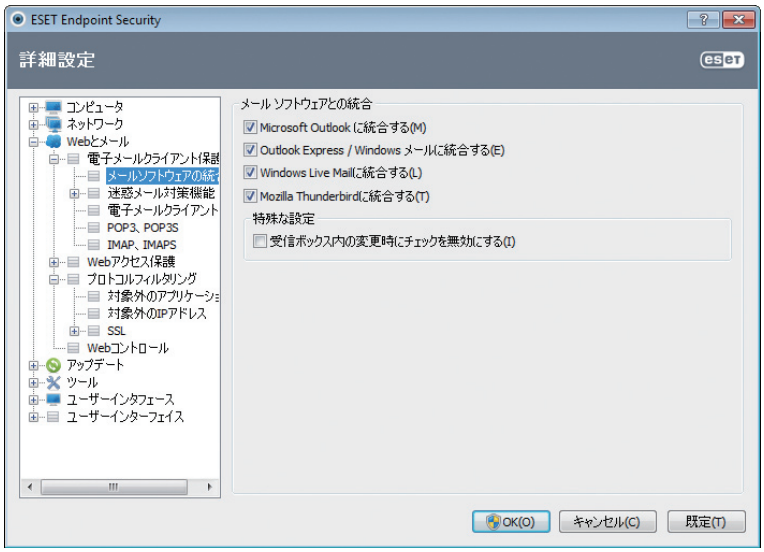


4.4.2.3 メールクライアントとの統合

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、その統合をESET Endpoint Securityで有効にできます。統合が有効な場合、ESET Endpoint Securityツールバーがメールクライアントに直接挿入されるため、メール保護の効率が高まります。統合設定を使用するには、[設定] > [詳細設定を表示する...] >> [Webとメール] > [電子メールクライアント保護] > [メールソフトウェアの統合] を選択します。

現在、メールクライアントとしてMicrosoft Outlook、Outlook Express、Windows Mail、Windows Live Mail、およびMozilla Thunderbirdがサポートされています。

電子メールクライアントでの作業時にシステムの速度が低下する場合は、[受信ボックス内の変更時にチェックを無効にする]の横のチェックボックスを選択します。Kerio Outlook Connector Storeからメールをダウンロードするときに、このような状況が発生する場合があります。



統合が有効になっていない場合でも、メールクライアント保護モジュール（POP3、IMAP）によってメール通信は保護されます。

メールクライアント保護の設定

電子メールクライアントの保護機能では、メールクライアントとしてMicrosoft Outlook、Outlook Express、Windows Mail、Windows Live Mail、およびMozilla Thunderbirdをサポートしています。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。プラグイン制御の主な利点は、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。

検査対象メール

受信メール	検査対象の受信メールを切り替えます。
送信メール	検査対象の送信メールを切り替えます。
既読メール	検査対象を既読メールに切り替えます。

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。
メールをごみ箱に移動する	感染しているメールを自動的に[削除済み]フォルダに移動します。
メールをフォルダに移動する	感染しているメールが検出された場合に、その移動先のカスタムフォルダを指定します。

その他

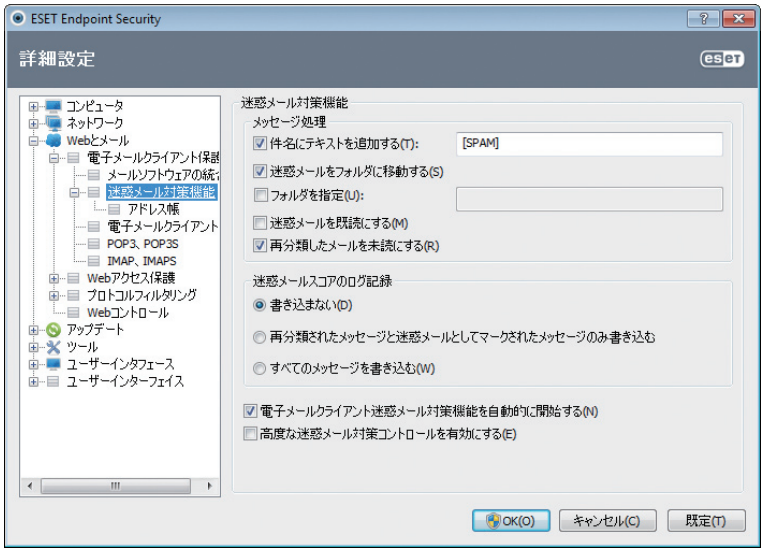
アップデート後に再度検査を行う	ウイルス定義データベースのアップデート後に再検査に切り替えます。
ほかの機能の検査結果を受け入れる	このオプションを選択すると、メールの保護機能でほかの保護機能の検査結果が受け入れられます。

4.4.2.4 マルウェアの削除

ウイルスに感染しているメールを受信した場合、警告ウィンドウが表示されます。警告ウィンドウには、送信者名、メール、およびマルウェアの名前が表示されます。ウィンドウの下部には、検出された対象に使用できる、[駆除]、[削除]、または[スキップ]というオプションがあります。基本的に、[駆除]または[削除]を選択することをお勧めします。特定な状況で、ウイルスに感染しているメールを受信したい場合には、[スキップ]を選択します。[厳密な駆除]が有効の場合、情報を提示するだけで、感染している対象に使用できるオプションは何もない情報ウィンドウが、表示されます。

4.4.3 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 80%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。複数の効率的な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駆除された状態になります。



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（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。

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を設定できます。次のオプションがあります。
電子メールクライアント迷惑メール対策機能を自動的に開始する-電子メールクライアントの保護を有効/無効にします。

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。
迷惑メールをフォルダに移動する	有効にすると、迷惑メールは既定の迷惑メールフォルダーに移動されます。
フォルダを指定	ユーザー定義のフォルダーに迷惑メールを移動します。
迷惑メールを既読にする	迷惑メールが自動的に既読としてマークされます。これによって、"正当"なメールに集中できます。
再分類したメールを未読にする	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―迷惑メール対策ログの [スコア] セルには何も書き込まれません。
●再分類されたメッセージと迷惑メールとしてマークされたメッセージのみ書き込む―迷惑メールのマークが付けられたメッセージに迷惑メールスコアを記録する場合、このオプションを使用します。
●すべてのメッセージを書き込む―すべてのメッセージが迷惑メールスコア付きでログに記録されます。

電子メールクライアント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。
高度な迷惑メール対策コントロールを有効にする	追加の迷惑メール対策データベースがダウンロードされますので、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では、Microsoft Outlook、Outlook Express、Windows Mail、Windows Live Mail、およびMozilla Thunderbirdの迷惑メールからの保護がサポートされます。

4.4.3.1 ホワイトリストとブラックリストへのアドレスの追加

頻繁にやり取りする相手の電子メールアドレスをホワイトリストに追加すると、ホワイトリストにあるアドレスからのメッセージは、決して迷惑メールとして分類されなくなります。既知の迷惑メールアドレスは、ブラックリストに追加して、必ず迷惑メールとして分類させることができます。新しいアドレスをホワイトリストまたはブラックリストに追加するには、電子メールを右クリックして [ESET Endpoint Security]＞[ホワイトリストに追加] または [ブラックリストに追加] を選択するか、または電子メールクライアントのESET Endpoint Security迷惑メール対策ツールバーにある [信頼アドレス] ボタンまたは [迷惑メールアドレス] ボタンをクリックします。

この操作は、迷惑メールのアドレスでも同じです。電子メールアドレスがブラックリストに載せられると、そのアドレスから届く各メッセージは、迷惑メールとして分類されます。

4.4.3.2 メッセージを迷惑メールとしてマークする

メールクライアントに表示されるどのメッセージも、迷惑メールとしてマークできます。そのためには、メッセージを右クリックして、[ESET Endpoint Security]＞[選択したメッセージを迷惑メールとして再分類] をクリックするか、またはメールクライアントの上部にあるESET Endpoint Security迷惑メール対策ツールバーの [迷惑メールアドレス] をクリックします。

再分類されたメッセージは、迷惑メールフォルダーに自動的に移動されますが、送信者の電子メールアドレスは、ブラックリストに追加されません。同様に、メッセージを"迷惑メールでない"として分類することもできます。迷惑メールフォルダーにあるメッセージが、迷惑メールでないとして分類された場合、元のフォルダーに移動されます。迷惑メールでないというマークをメッセージに付けても、その送信者の電子メールアドレスが自動的にホワイトリストに追加されることはありません。

4.4.4 プロトコルフィルタリング

ThreatSenseの検査エンジンには、アプリケーションプロトコルに対するウイルス対策があり、そこでは全ての高度なマルウェアスキャン技術がシームレスに統合されています。この検査は、使用しているインターネットブラウザやメールクライアントに関係なく、自動的に動作します。暗号化（SSL）通信については、[プロトコルフィルタリング]＞[SSL]を参照してください。

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-有効にすると、全ての HTTP（S）、POP3（S）、IMAP（S）トラフィックがウイルス対策スキャナーによって検査されます。

NOTE

Windows Vista Service Pack1、Windows7および Windows Server 2008以降では、ネットワーク通信のチェックに新しいWindowsフィルタリングプラットフォーム(WFP)が使用されます。WFPテクノロジーは特殊な監視技術を使用するので、次のオプションは使用できません。

HTTPおよびPOP3ポート	内部プロキシサーバーへのトラフィックのルーティングを、HTTPおよびPOP3ポートのみに制限します。
Webブラウザまたは電子メールクライアントとしてマークされたアプリケーション	内部プロキシサーバーへのトラフィックのルーティングを、ブラウザおよび電子メールクライアントとマークされたアプリケーションのみに制限します（[Webとメール]＞[プロトコルフィルタリング]＞[Webと電子メールのクライアント]）。
Webブラウザまたは電子メールクライアントとしてマークされたポートとアプリケーション	内部プロキシサーバー上のブラウザーおよび電子メールクライアントと指定されたアプリケーションの全ての通信に加え、HTTPおよびPOP3ポート上の全てのトラフィックのルーティングを有効にします。

4.4.4.1 Webと電子メールのクライアント

NOTE

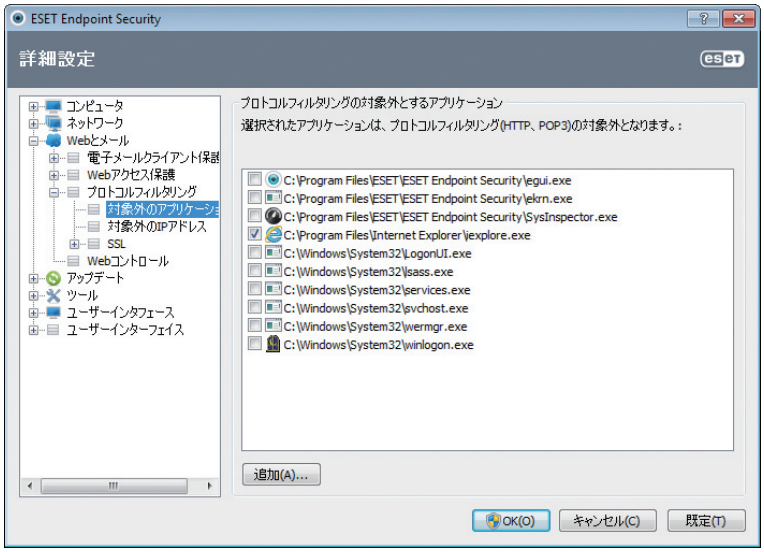
Windows Vista Service Pack 1および Windows Server 2008以降では、ネットワーク通信のチェックに新しいWindowsフィルタリングプラットフォーム(WFP)が使用されます。WFP技術では特殊な監視手法が採用されているため、[Webと電子メールのクライアント]セクションを利用できません。

悪意のある多数のコードがインターネットを通じて広まっているので、コンピュータを保護するには、安全にインターネットを参照できることが非常に重要です。悪意のあるコードは、Webブラウザーの脆弱性や不正なリンクを利用して、気付かれずにシステムに侵入します。そのため、ESET Endpoint SecurityではWebブラウザーのセキュリティに重点が置かれています。ネットワークにアクセスする各アプリケーションをインターネットブラウザーとして指定することができます。チェックボックスには次の2つの状態があります。

チェックマークなし	指定されたポートでのみアプリケーションの通信がフィルタリングされます。
チェックマーク付き	通信は常にフィルタリングされます（別のポートが設定されている場合も同様）。

4.4.4.2 対象外のアプリケーション

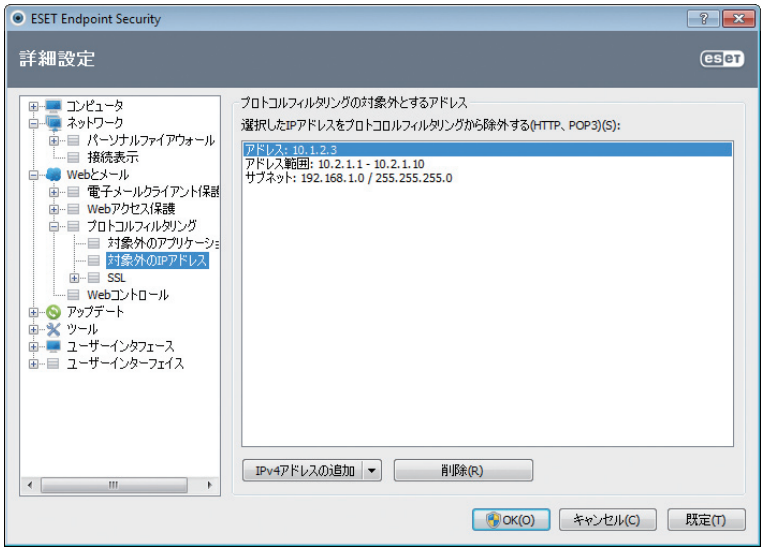
特定のネットワーク対応アプリケーションの通信をコンテンツフィルタリングから除外するには、リストでそのアプリケーションを選択します。選択したアプリケーションのHTTP/POP3/IMAP通信のマルウェアは検査されません。このオプションは、通信の検査を行うと正常に機能しないアプリケーションのみに使用することをお勧めします。
アプリケーションとサービスはここから自動で実行できます。プロトコルフィルタリングの一覧に表示されていないアプリケーションを手動で選択するには、[追加...] ボタンをクリックします。



4.4.4.3 除外されるIPアドレス

アドレスリスト中のエントリーは製品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アドレスに対してのみ使用します。

IPv4/IPv6アドレスの追加	このオプションを使用すると、ルールの適用先の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。
削除	選択したエントリーをリストから削除します。



IPv4アドレスの追加

このオプションを使用すると、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。インターネットプロトコルバージョン4は古いバージョンですが、現在も広く使用されています。

単一のアドレス	192.168.0.10など、ルールが適用される各コンピュータのIPアドレスを追加します。
アドレス範囲	最初と最後のIPアドレスを入力して、192.168.0.1 ～ 192.168.0.99など、ルールが適用される複数のコンピュータのIP範囲を指定します。
サブネット	サブネット(コンピューターのグループ)は、IPアドレスとマスクによって定義されます。

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アドレスの追加

このオプションを使用すると、ルールが適用されるリモートポイントのIPv6アドレス/サブネットを追加することができます。IPv6はインターネットプロトコルの最新バージョンで、前のバージョン4に代わるものです。

単一のアドレス	2001:718:1c01:16:214:22ff:fec9:ca5など、ルールが適用される各コンピュータのIPアドレスを追加します。
サブネット	サブネット(コンピュータのグループ)は、IPアドレスとマスクによって定義されます(例:2002:c0a8:6301:1::1/64)。

4.4.4.4 SSL通信のチェック

ESET Endpoint Securityでは、SSLプロトコルでカプセル化されたプロトコルをチェックできます。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プロトコルを常に検査する	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、ユーザーに通知されず、通信は自動的にフィルタリングされます。ユーザーが信頼しているとマークしている(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。
アクセスしていないサイトについて確認する(除外を設定できます)	SSLで保護された新しいサイトに入る(不明な証明書を使用して)と、動作を選択を求める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証明書のリストを作成できます。
SSLプロトコルを検査しない	これを選択すると、SSLを介した通信は検査されません。
証明書に基づいて作成した例外を適用する	SSL通信の検査で除外証明書および信頼できる証明書で指定された除外の使用を有効にします。このオプションは、[SSLプロトコルを常に検査する]を選択すると有効になります。
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。

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, spol. s r.o.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。したがって、[ルート証明書を既知のブラウザに追加する]オプション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ー（Webサーバーまたは中小企業の管理者）によって自己署名されていて、この証明書を信頼できるとみなしても必ずしもリスクにはならないことを意味します。多くの大企業（銀行など）は、TRCAにより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]オプション（既定）を選択すると、ユーザーは暗号化通信の確立時にと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]オプションを選択して、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。

■信頼できる証明書

ESET Endpoint Securityでは、信頼できる証明書の格納先となる信頼できるルート認証局ストアーが統合されるだけでなく、信頼できる証明書のカスタムリストを作成し、[詳細設定]（F5）＞[Webとメール]＞[プロトコルフィルタリング]＞[SSL]＞[証明書]＞[信頼できる証明書]で表示することもできます。ESET Endpoint Securityでは、このリスト内の証明書を利用して暗号化通信のコンテンツを検査します。

リストから選択したアイテムを削除するには、[削除]ボタンをクリックします。[表示]オプションをクリックすると（または証明書をダブルクリックすると）、選択した証明書に関する情報が表示されます。

■除外される証明書

[除外される証明書]セクションには、安全と見なされている証明書があります。このリストにある証明書を使用する暗号化通信のコンテンツは、マルウェアがあるかどうかを検査されません。安全性が保証されているWeb証明のみを除外することをお勧めします。このような証明書を利用する通信は、検査する必要がありません。リストから選択したアイテムを削除するには、[削除]ボタンをクリックします。[表示]オプションをクリックすると（または証明書をダブルクリックすると）、選択した証明書に関する情報が表示されます。

■暗号化されたSSL通信

コンピューターがSSLプロトコル検査を行うように設定されている場合、(不明な証明書を使用して)暗号化通信が試行されると、アクションの選択を求めるダイアログウィンドウが表示されることがあります。このダイアログウィンドウには、通信を開始したアプリケーション名および使用された証明書名が表示されます。

証明書が信頼されたルート証明機関ストアーにない場合は、信頼できない証明書と見なされます。

証明書で使用できるアクションは、次のとおりです。

はい	現行のセッションに対して、証明書は一時的に信頼できる証明書としてマークされます。次回、証明書を使用する際に警告ウィンドウは表示されません。
はい(常時)	証明書を信頼できる証明書としてマークして、信頼できる証明書リストに追加します。信頼できる証明書に対して警告ウィンドウは表示されません。
いいえ	現行のセッションに対して、証明書を信頼できない証明書としてマークします。次回、証明書を使用する際、警告ウィンドウが表示されます。
除外対象	証明書を除外される証明書のリストに追加します。指定された暗号化チャンネル経由で転送されたデータは、検査されません。

4.5 Webコントロール

[Webコントロール] セクションでは、知的財産権に違反するWebサイトなど、会社が法的責任を負うリスクを防止する設定を行うことができます。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コントロールを使用して、不快な内容を掲載していると考えられるサイトをブロックできます。また、雇用者またはシステム管理者は、最大20までのWebサイトカテゴリと140以上のサブカテゴリを事前定義してアクセスを禁止できます。

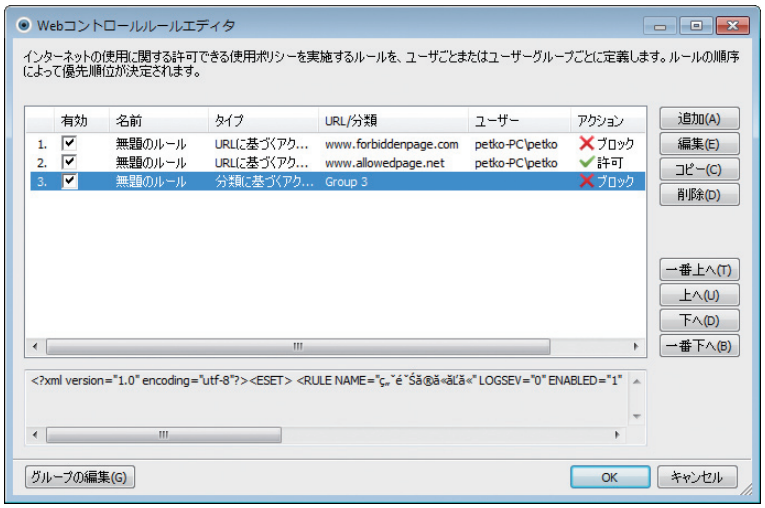
Webコントロール設定オプションは、[詳細設定] (F5) > [Webコントロール] で変更できます。[システム統合] の横にあるチェックボックスを使用すると、WebコントロールをESET Endpoint Securityに統合し、[ルールの設定...] をアクティブにして、[Webコントロールルールエディタ] ウィンドウにアクセスすることです。

▸▸▸ NOTE

Webコントロールが正しく機能するには、[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]、[HTTPプロトコルのチェックを有効にする]、および[パーソナルファイアウォール/システム統合] が有効になっている必要があります。これらの機能はすべて、既定で無効になっています。

4.5.1 Webコントロールルール

[Webコントロールルールエディタ] ウィンドウには、URLのアドレスとWebページという分類の既存ルールが表示されます。



このルール一覧には、Webコントロールルールおよびログ重大度との突き合せの結果として、名前、ブロックのタイプ、実行すべきアクションなどのいくつかのルールの説明が示されます。

[新規] または [変更] 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、別の選択済みルールで使用されている事前定義のオプションを備えた新規のルールを作成します。ルールをクリックすると表示されるXMLストリングは、クリップボードにコピーできます。またこれは、システム管理者がそのデータを、たとえばESET Remote Administrator内でエクスポート/インポートしたり、使用したりするのに役立ちます。

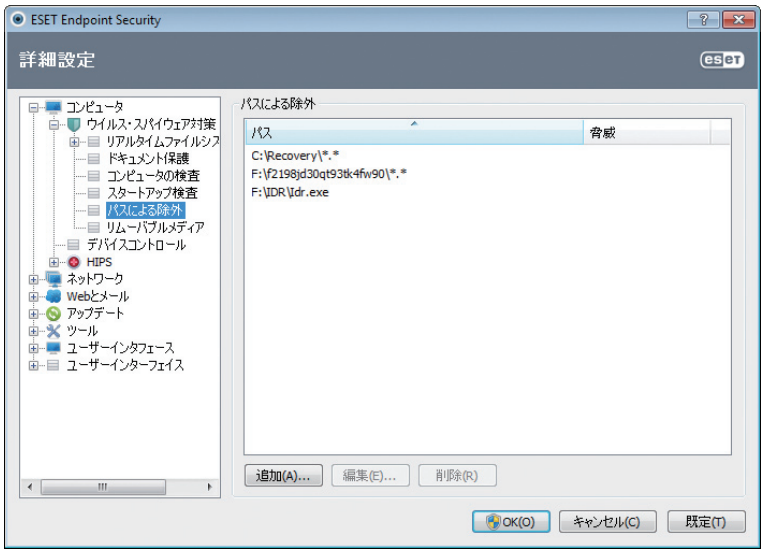
CTRLを押してクリックすれば、複数のルールを選択してアクション（削除やリスト内での上下移動など）をすべての選択済みルールに適用できます。[有効] チェックボックスはルールを無効または有効にします。これは、将来使用するつもりのルールを永続的に削除したくない場合に便利です。

このコントロールは、ルールに従って実行されますが、ルールは優先度の高いものが先頭になっています。ルールを右クリックして、コンテキストメニューを表示できます。ここで、ルールのログエントリ用の重大度を設定できます。ログエントリは、ESET Endpoint Securityのメインウィンドウの [ツール] > [ログファイル] から表示できます。

[グループの編集] をクリックしてグループエディタウィンドウを開きます。そこで、該当するグループに所属する事前定義のカテゴリおよびサブカテゴリの追加や削除を行うことができます。

4.5.2 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。



分かりやすいルールの説明を [名前] フィールドに入力します。チェックボックス [有効] で、このルールを無効または有効にします。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。

アクションのタイプ

●URLに基づくアクション—特定のWebサイトへのアクセス。該当するURLアドレスを [URL] フィールドに入力します。

●分類に基づくアクション—このオプションを選択した場合、次に [分類] ドロップダウンメニューから分類を選択する必要があります。

URLアドレスリストでは、特殊記号の*(アスタリスク)および?(疑問符)は使用できません。たとえば、複数のTLDが含まれるWebページのアドレス(examplepage.com、examplepage.skなど)は手入力する必要があります。.リストにドメインを入力するときは、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。

アクション

●許可—URLアドレス/分類へのアクセスが認可されます。

●ブロック—URLアドレス/分類がブロックされます。

ユーザー一覧

●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。

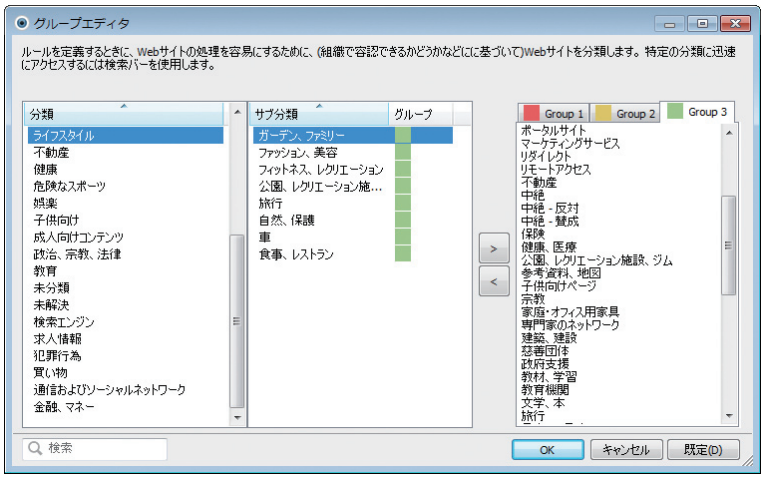
●削除—選択されたユーザーをフィルタから削除します。

4.5.3 グループエディター

[グループエディタ] ウィンドウは、2つの部分に分かれます。このウィンドウの右側の部分には、分類およびサブ分類の一覧が示されます。[分類] リストで分類を選択し、そのサブ分類を表示します。たいていのサブ分類は、彩色されたグループに所属します。

赤色のグループには、成人または一般的に不適切なサブ分類（またはこの両方）が所属します。他方、緑色のグループには、許可できるとみなされるWebページの分類が所属します。

選択したグループに対して選択したサブ分類を追加または削除するには、矢印を使用します。



NOTE

1つのサブ分類は1つのグループにのみ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せるには、それを目的のグループに追加します。追加したサブ分類がすでに別のグループに所属している場合、それは削除されて、選択したグループに追加されます。

グループを検索するには、ウィンドウの左下隅にある [検索] フィールドに検索用語を入力します。

4.6 アップデート

コンピュータ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。アップデート機能により、プログラムはウイルス定義データベース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。

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。プライマリウィンドウには、ウイルス定義データベースのバージョンも表示されます。ウイルス定義ファイルの番号はESETのWebサイトへのアクティブなリンクになっており、このリンクをクリックすると、そのアップデートで追加されたすべての定義の一覧が表示されます。

さらに、アップデートプロセスを手動で開始する［ウイルス定義データベースのアップデート］オプションも使用できます。ウイルス定義データベース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情報（ユーザー名とパスワード）を入力しなかった場合、ESETのアップデートサーバーにアクセスするためのアップデート時にユーザ名とパスワードを入力できます。

NOTE

お客様のユーザー名とパスワードは、ユーザーズサイトより確認できます。ユーザーズサイトへのアクセス手順については「ESETライセンス製品 ご利用の手引」をご参照ください。

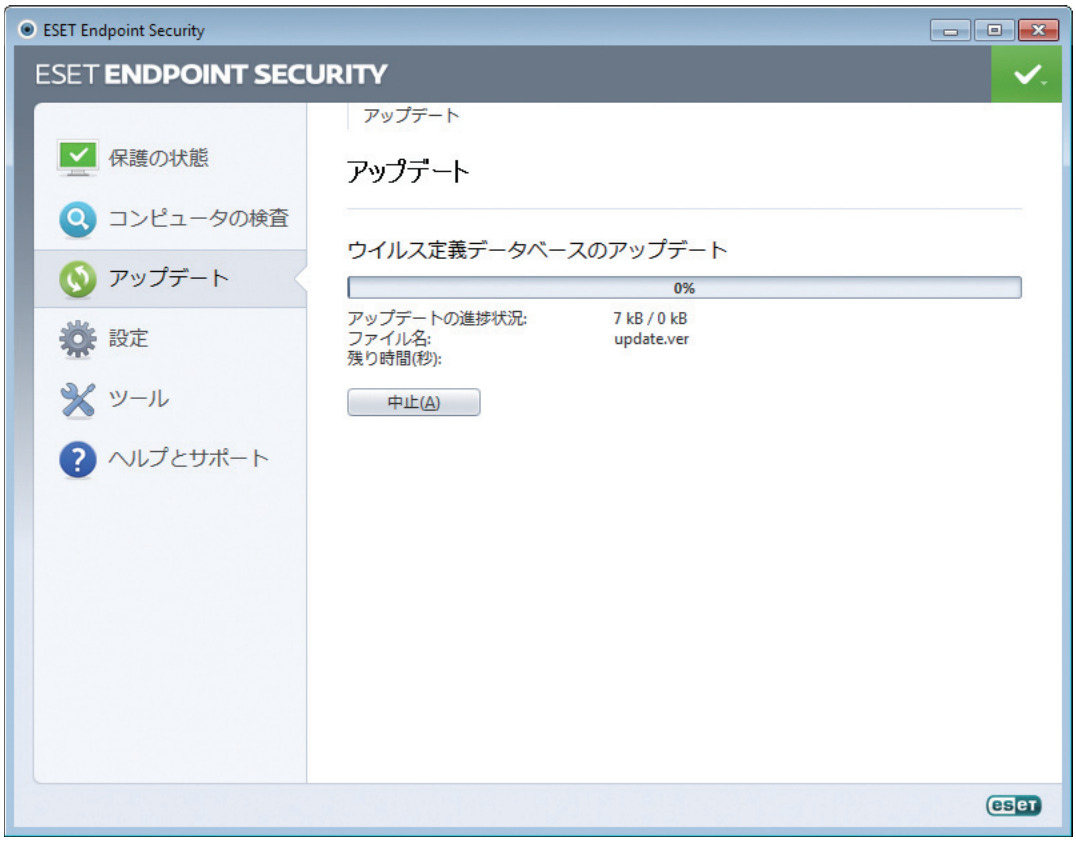
ユーザーズサイト　http://canon-its.jp/product/eset/users/

前回成功したアップデート	最終アップデート日です。ウイルス定義データベースが最新、つまり最近の日付になっていることを確認します。
ウイルス定義データベースのバージョン	ウイルス定義データベースの番号。同時にESETのWebサイトへのアクティブなリンクになっています。クリックすると、所定のアップデートで追加されたウイルス定義がすべてリスト表示されます。

[チェック] をクリックし、使用可能な最新のESET Endpoint Securityを検出します。

更新プロセス

[ウイルス定義データベースをアップデートする] をクリックすると、ダウンロードプロセスが始まります。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、[中止] をクリックします。



重要

通常の状況では、アップデートファイルが正常にダウンロードされると、[アップデート] ウィンドウに[アップデートは必要ありません-ウイルス定義データベースは最新です] というメッセージが表示されます。表示されないということは、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。ウイルス定義データベースはできるだけ早くアップデートしてください。ダウンロードが正常に行われなかった場合は、次のメッセージが表示されます。

ウイルス定義データベースは最新ではありません

このエラーは、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複数回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、認証データの入力の誤り、または接続設定の設定の誤りです。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(ウイルス定義データベースのアップデートが失敗しました)に関連します。

ユーザー名またはパスワード（あるいはその両方）が無効です

アップデート設定でユーザー名とパスワードが誤って入力されました。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、[詳細設定を表示する...] をクリックするか、またはキーボードのF5キーを押す）に、追加の更新オプションが示されています。[詳細設定] ツリーの [アップデート] > [一般] をクリックして、新しいユーザー名とパスワードを入力します。

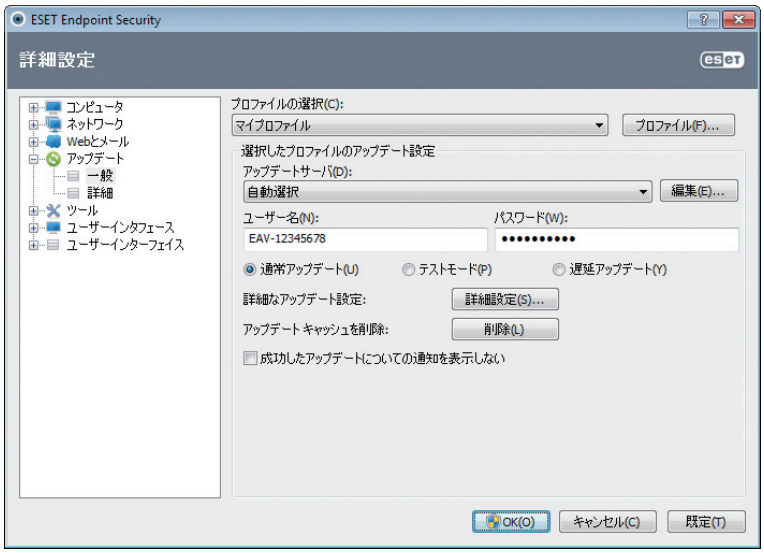
アップデートファイルのダウンロード中にエラーが発生しました

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ブラウザで任意のWebサイトを開いてみます）。Webサイトが開かない場合、インターネット接続が確立されていないか、コンピュータの接続に問題がある可能性があります。ご利用のインターネットサービスプロバイダ（ISP）に、有効なインターネット接続があるかどうか確認してください。

4.6.1 アップデートの設定

アップデート設定セクションでは、アップデートサーバーやそれらのサーバの認証データなど、アップデートファイルの送信元の情報を指定します。既定では、[アップデートサーバ] ドロップダウンメニューは自動的に [自動選択] に設定され、最もネットワークトラフィックが少ないESETサーバからアップデートファイルが自動的にダウンロードされます。アップデートの設定オプションは、詳細設定ツリー（F5キー）の [アップデート] > [一般] をクリックして使用します。

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、プログラムがインターネットとの通信（HTTP通信）を許可されていることを確認してください。



現在使用されているアップデートプロファイルが、[プロファイルの選択] 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...] をクリックします。

使用可能なアップデートサーバのリストにアクセスするには、[アップデートサーバ] ドロップダウンメニューを使用します。アップデートサーバは、アップデートファイルが保存される場所です。ESETサーバを使用する場合は、既定のオプション [自動的に選択する] を選択したままにしてください。新しいアップデートサーバを追加するには、[選択したプロファイルのアップデート設定] セクションの [編集...] をクリックし、[追加] ボタンをクリックします。

ローカルのHTTPサーバ、つまりミラーを使用する場合は、アップデートサーバを
https://<コンピュータ名またはIPアドレス>:2221のように設定する必要があります。

SSLを使用するローカルのHTTPサーバを使用する場合は、アップデートサーバを
https://<コンピュータ名またはIPアドレス>:2221のように設定する必要があります。

アップデートサーバに対する認証は、購入後に生成され、送信されたユーザー名とパスワードを使用して行われます。ローカルのミラーサーバを使用する場合、検証はミラーサーバの設定によって異なります。既定では、検証は必要ないため、[ユーザー名] フィールドと [パスワード] フィールドは空欄のままです。

テストモード（[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、短期間の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。現在のモジュールの一覧は、[ヘルプとサポート] > [ESET Endpoint Securityのバージョン5について] で確認できます。基本ユーザーは、[定期アップデート] を既定で選択されたままにすることをお勧めします。企業ユーザーは [遅延アップデート] オプションを選択すると、一定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）を提供する特別なアップデートサーバからアップデートできます。

[詳細なアップデート設定] の横にある [詳細設定] ボタンをクリックし、詳細なアップデートオプションが示されたウィンドウを表示します。

アップデート時に問題が発生した場合、[削除...] ボタンをクリックするとフォルダの一時的なアップデートファイルが削除されます。

アップデートの成功についての通知を表示しない—画面の右下にあるシステムトレイ通知が無効になります。全画面のアプリケーションまたはゲームが実行されている場合、このオプションを選択すると便利です。プレゼンテーションモードではすべての通知がオフになることに注意してください。

4.6.1.1 アップデートプロファイル

さまざまなアップデートの設定用および更新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の作成は、モバイルユーザーにとって特に便利です。定期的に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を作成できるためです。

[プロファイルの選択] 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] ボタンをクリックし、[追加] ボタンをクリックして、[プロファイル名] フィールドに独自の名前を入力します。新しいプロファイルを作成する際、[プロファイルの設定をコピー] ドロップダウンメニューから既存のプロファイルを選択して、そのプロファイルから設定をコピーすることができます。

プロファイル設定ウィンドウでは、使用可能なサーバのリストからアップデートサーバを指定するか、または新しいサーバを追加することができます。既存のアップデートサーバのリストは、[アップデートサーバ] ドロップダウンメニューに一覧表示されます。新しいアップデートサーバを追加するには、[選択されたプロファイルの更新設定] セクションの [編集...] をクリックし、[追加] ボタンをクリックします。

4.6.1.2 アップデートの詳細設定

[アップデートの詳細設定] を表示するには、[詳細設定] ボタンをクリックします。詳細なアップデート設定オプションには、[アップデートモード]、[HTTPプロキシ]、[LAN] および [ミラー] があります。

アップデートモード

[アップデートモード] タブには、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。[プログラムコンポーネントのアップデート] セクションでは、次の3つのオプションが使用可能です。

プログラムコンポーネントを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、サーバインストールに適しています。サーバは通常、保守中にしか再起動できないためです。
プログラムコンポーネントをアップデートする	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。
プログラムコンポーネントをダウンロードする前に確認する	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、インストールをするか拒否するかの確認を求められます。

プログラムコンポーネントをアップデートしたら、全てのモジュールが完全に機能するようにコンピュータを再起動する必要がある場合があります。[プログラムコンポーネント更新後の再起動] セクションで、次の3つのオプションのいずれかを選択することができます。

コンピュータを再起動しない	再起動が必要な場合でも、再起動を求めるメッセージは表示されません。次に再起動するまでコンピュータが正しく動作しない可能性があるので、このオプションを選択することはお勧めしません。
必要な場合はコンピュータの再起動を促す	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後、ダイアログウィンドウが開き、コンピュータの再起動を求めるメッセージが表示されます。
必要な場合は確認せずにコンピュータを再起動する	プログラムコンポーネントのアップデート後、コンピュータは(必要な場合)再起動されます。

▸▸▸ NOTE

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。

[アップデートをダウンロードする前に確認する] オプションをチェックした場合、新しいアップデートが利用できるようになると、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] に指定した値より大きい場合、プログラムによって通知が表示されます。

プロキシサーバー

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、[詳細なアップデート設定]の右にある[設定...]ボタンをクリックします。[HTTP プロキシ] タブをクリックし、次の3つのオプションのいずれかを選択します。

●プロキシサーバのグローバル設定を使用する
●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] オプションを選択すると、[詳細設定] ツリーの [ツール]、[プロキシサーバ] ブランチで指定された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] オプションを選択すると、ESET Endpoint Securityの更新にプロキシサーバ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。

●グローバル設定 ([ツール] > [プロキシサーバ]) で指定したものと異なるプロキシサーバーを使用してESET Endpoint Securityを更新する場合。この場合は、ここで設定を指定する必要があります。必要に応じて、プロキシサーバーの [プロキシサーバ] アドレス、通信 [ポート]、および [ユーザー名] と [パスワード] を指定します。
●プロキシサーバ設定はグローバルには設定されませんが、ESET Endpoint Securityはアップデートを取得するためにプロキシサーバに接続します。
●コンピュータがプロキシサーバを介してインターネットに接続されます。設定はプログラムのインストール時にInternet Explorerから取得されますが、その後変更されている (ISPを変更するなど) 場合、このウィンドウからHTTPプロキシ設定が正しいことを確認します。しなかった場合、プログラムはアップデートサーバに接続できません。

プロキシサーバの既定の設定は、[プロキシサーバのグローバル設定を使用する] です。

▸▸▸ NOTE

[ユーザー名] と[パスワード] などの認証データは、プロキシサーバへのアクセスに使用されます。これらのフィールドには、ユーザー名とパスワードが必要な場合にのみ入力してください。これらのフィールドは、ESET Endpoint Securityのパスワードとユーザー名を入力するためのものではありません。プロキシサーバ経由でインターネットにアクセスするためにパスワードが必要であることがわかっている場合にのみ入力してください。

LANへの接続

NTベースのオペレーティングシステムを実行しているローカルサーバ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。ほとんどの場合、ローカルシステムアカウントにはミラーフォルダ (アップデートファイルのコピーを格納するフォルダ) にアクセスする十分な権限がありません。この場合は、アップデートの設定セクションでユーザー名とパスワードを入力するか、またはプログラムがアップデートサーバ (ミラー) へのアクセスに使用する既存のアカウントを指定してください。

このようなアカウントを設定するには、[LAN] タブをクリックします。[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] セクションには、[システムアカウント (標準)]、[現在のユーザー]、および [指定されたユーザー] オプションが配置されています。

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、ローカルサーバ上のアップデートファイルディレクトリにアクセスできなければなりません。アクセスできない場合は、接続を確立して、アップデートファイルをダウンロードすることができません。

CAUTION

[現在のユーザー] または[指定されたユーザー] オプションが有効になっている場合、プログラムのIDを目的のユーザーに変更すると、エラーが発生することがあります。そのため、アップデートの設定のメインセクションでLANの認証データを入力することをお勧めします。このアップデート設定セクションでは、認証データは次のように入力する必要があります。domain_name¥user(これがワークグループの場合はworkgroup_name¥nameと入力します) およびパスワード。ローカルサーバのHTTPバージョンからアップデートする場合、認証は不要です。

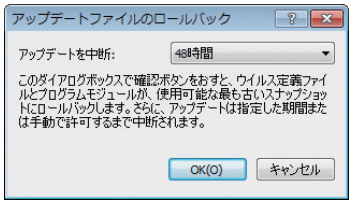
アップデートファイルのダウンロード後もサーバとの接続がアクティブなままになっている場合、[アップデート終了後にサーバから切断する] オプションを選択します。

4.6.1.3 アップデートのロールバック

ウイルスデータベース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、選択した期間中のすべてのアップデートを無効にできます。あるいは、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には、ウイルスデータベースのモジュールのバックアップと復元 (いわゆるロールバック) が備わっています。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、[アップデートファイルのスナップショットを作成する] チェックボックスを選択状態のままにします。[ローカルに保存するスナップショットの数] フィールドは、ローカルのコンピュータファイルシステムに保存されている以前のウイルスデータベーススナップショットの数を定義しています。

[ロールバック] ([詳細設定] (F5) > [アップデート] > [詳細]) をクリックする場合、ウイルス定義データベースおよびプログラムモジュールアップデートを休止する期間を指定する時間間隔を [アップデートを中断] ドロップダウンメニューから選択する必要があります。

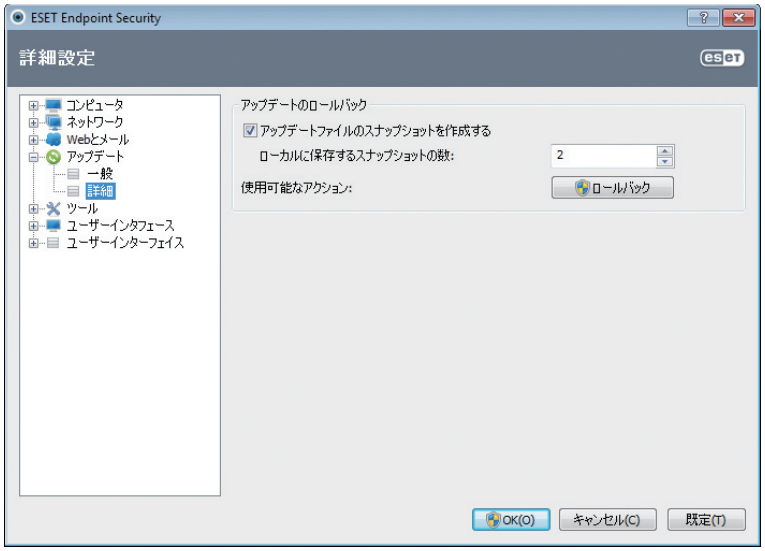


手動で定期アップデートを許可したい場合、[取り消すまで] を選択します。これには潜在的なセキュリティリスクがあるため、このオプションの選択はお勧めしません。

ロールバックを有効にすると、[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。[間隔] 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。ウイルス定義データベースのバージョンは最も古いものにダウングレードされて、ローカルのコンピュータ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。

例:ウイルス定義データベースの最新のバージョンは6871番であると仮定します。ウイルス定義データベースのスナップショットとして、6870と6868が保存されているとします。たとえば、コンピュータがオフになっていたため、6869は使用不可であることに注意してください。[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2を入力して [ロールバック] をクリックすると、ウイルス定義データベースはバージョン番号 6868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。ESET Endpoint Securityのメインプログラムウィンドウの「アップデート」セクションで、ウイルス定義データベース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ます。

ESET Endpoint Securityの [詳細設定] セクションにあるライセンスマネージャーで有効なライセンスキーを追加した後、ローカルミラーサーバーの設定オプションにアクセスできます。ワークステーションをミラーとして使用している場合、アップデートコピーが、最新のエンドユーザー契約条項(EULA)を事前に受諾済みである必要があります。受諾済みであってはじめて、ネットワーク上にある他のワークステーションをアップデートするのに使用されるコピーアップデートファイルとして作成することができます。アップデート時にさらに新しいバージョンのEULAが使用可能であると、その確認のために、60秒のタイムアウトのダイアログウィンドウが表示されます。これを手動で行うには、このウィンドウの [PCUライセンス] セクションの [設定...] をクリックします。



4.6.2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] をクリックした後に表示されるプライマリウィンドウで、[ウイルス定義ファイルのアップデート] 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有効になっています。

●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。

4.7 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。

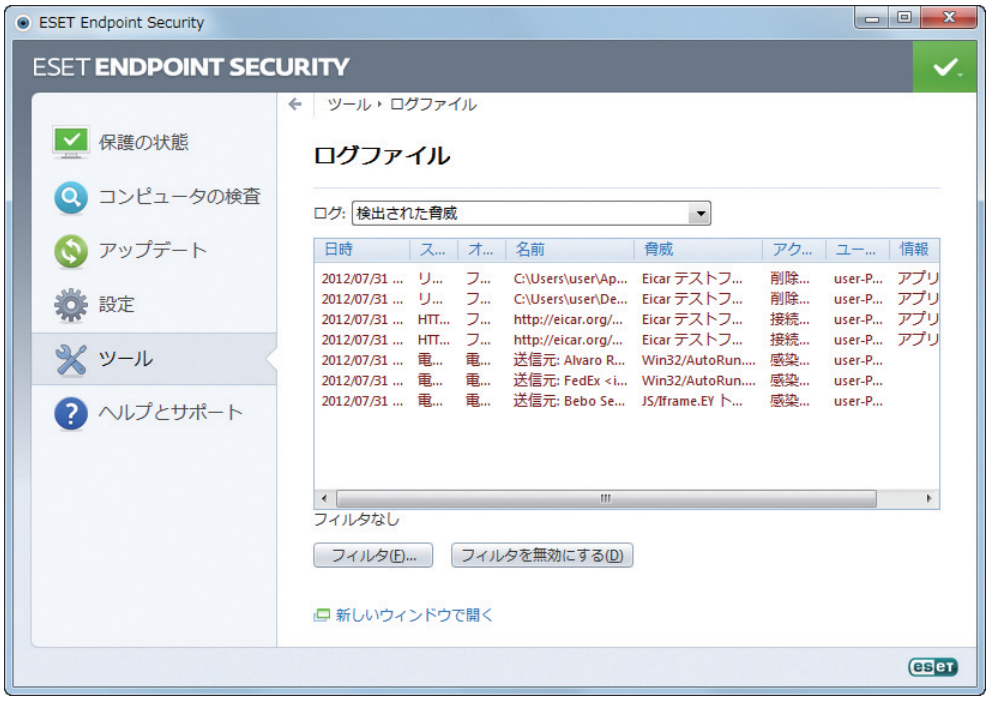
- ログファイル
- 保護統計
- アクティビティの確認
- [実行中のプロセス]
- スケジューラ
- 隔離
- ネットワーク接続
- ESET SysInspector

分析のためにファイルを提出
分析のため、不審なファイルをESETのウイルスラボに提出できます。このオプションをクリックすると表示されるダイアログウィンドウについては、「分析用ファイルの提出」を参照してください。

ESET SysRescue
ESET SysRescue作成ウィザードを起動します。

4.7.1 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環境から直接、ログをアーカイブするだけでなく、テキストメッセージとログを表示することができます。



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。

検出された脅威	ウイルスログには、ESET Endpoint Securityのモジュールにより検知されたウイルスについての詳細情報が記録されています。この情報には、検出時刻、ウイルスの名前、場所、実行されたアクション、ウイルスの検出時にログインしていたユーザーの名前が含まれます。ログエントリをダブルクリックすると、その詳細が別のウィンドウに表示されます。
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。
コンピュータの検査	このウィンドウには、完了した全ての手動またはスケジュールされた検査結果が表示されます。各行は、個々のコンピュータ制御に対応します。エントリ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。
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。
パーソナルファイアウォール	ファイアウォールログには、パーソナルファイアウォールによって検出された全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。
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。

各セクションで、エントリを選択し、[コピー] をクリックすると、表示されている情報をクリップボードに直接コピーすることができます(キーボードショートカットはCtrl+C)。CtrlキーおよびShiftキーを使用して複数エントリを選択できます。

特定のレコードを右クリックしてコンテキストメニューを表示できます。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。

同じ種類のレコードをフィルタ表示	このフィルタ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、[ログのフィルタ]ウィンドウがポップアップして、フィルタ基準を定義できます。
フィルタを無効にする	フィルタのすべての設定(上記)をクリアします。
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/全て削除	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。
ログのスクロール	古いログを自動スクロールし、アクティブなログを[ログファイル]ウィンドウで監視する場合は、このオプションをオンにしておきます。

4.7.1.1 ログの保守

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] > [詳細設定を表示する...] > [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。

エントリを自動的に削除する	[次の日数が経過したエントリを削除]に指定した日数より古い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値を超えると、ログファイルは自動的に最適化されます。

[今すぐ最適化] をクリックすると、ログファイルの最適化が開始します。このプロセスによって空の全てのログエントリが削除され、ログの処理のパフォーマンスおよび速度が向上します。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。

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、パーソナルファイアウォールなど)のエラーを記録します。

[既定のフィルタ...] ボタンをクリックすると、[ログのフィルタ] ウィンドウが開きます。ログに表示するレコードタイプを確認して、[OK] をクリックします。

4.7.2 スケジューラ

スケジューラでは、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。

スケジューラは次のタスクのスケジュールを行います。ウイルス定義データベースのアップデート、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 [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。

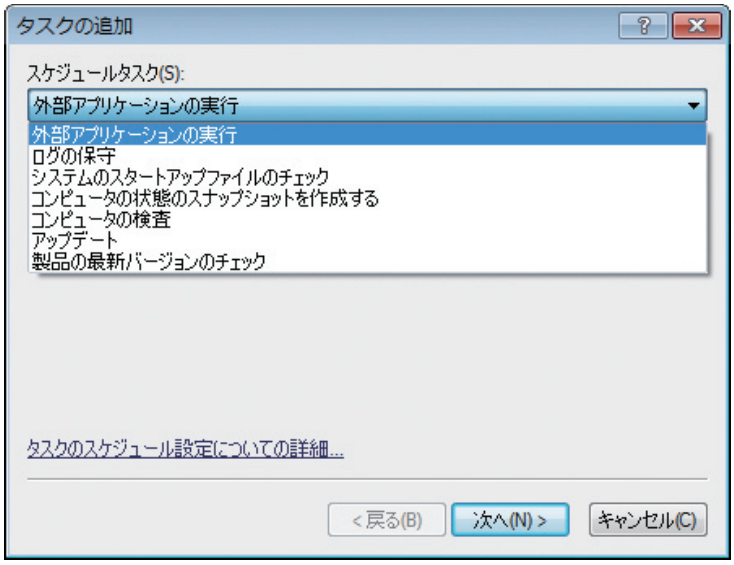
●ログの保守
●定期的に自動アップデート
●ダイヤルアップ接続後に自動アップデート
●ユーザーログオン後に自動アップデート
●自動スタートアップファイルのチェック (ユーザーのログオン後)
●自動起動ファイルの検査 (ウイルス定義データベースの正常なアップデート後)

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

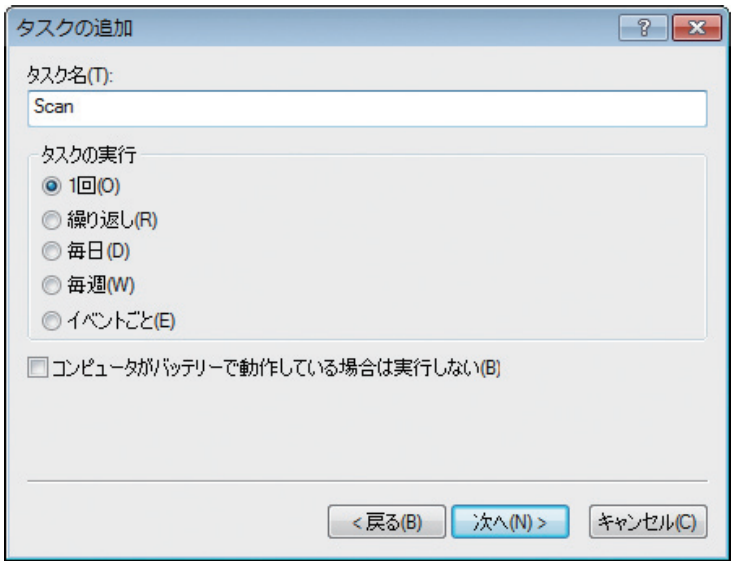
1 ウィンドウの一番下にある [追加...] をクリックします。

2 プルダウンメニューから目的のタスクを選択します。



3 タスクの名前を入力し、次のオプションの中からタスクを実行する時期を選択します。

- ●1回―事前定義した日時にタスクを1回だけ実行します。
- ●繰り返し―指定した間隔（時間単位）でタスクが実行されます。
- ●毎日―毎日、指定した時刻にタスクが実行されます。
- ●毎週―1週間に1回以上、選択した曜日と時刻にタスクが実行されます。
- ●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。



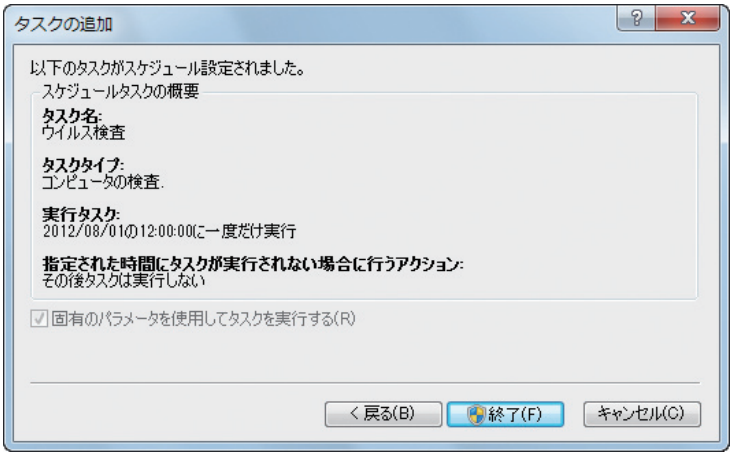
4 前の手順で選択したタイミングオプションに応じて、次のいずれかのダイアログウィンドウが表示されます。

- ●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、指定した時刻にタスクが繰り返し実行されます。
- ●毎週—選択した曜日と時刻にタスクが実行されます。

5 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。

- ●次にスケジュールされた時刻まで待機
- ●実行可能になりしだい実行する
- ●前回実行されてから次の時間が経過した場合直ちに実行する

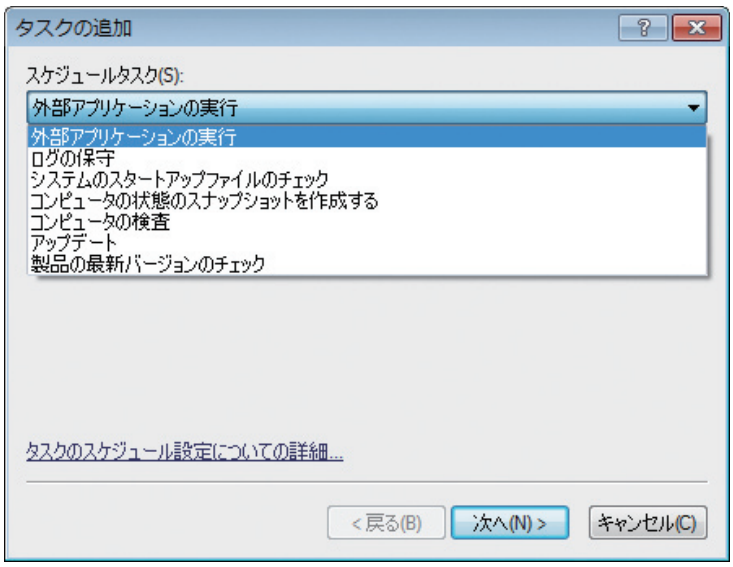
6 最後のステップでは、スケジュールされるタスクを確認することができます。[完了] をクリックすると、タスクが適用されます。



4.7.2.1 新しいタスクの作成

スケジューラで新しいタスクを作成するには、[追加...] ボタンをクリックするか、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の検査を実行します。
アップデート	ウイルス定義データベースのアップデートおよびプログラムモジュールのアップデートを行って、アップデートタスクをスケジュールします。
最新製品バージョンの確認	製品の最新バージョンのチェック



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。[次へ] をクリックして [タスク名] フィールドにタスクの名前を入力します。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]、および [イベントの発生時]。ラップトップコンピュータがバッテリー電源で実行されているときにシステムリソースを最小化するには、[コンピュータがバッテリーで動作している場合は実行しない] オプションを使用します。選択された頻度に基づいて、さまざまな更新パラメータが提示されます。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。次の3つのオプションが使用可能です。

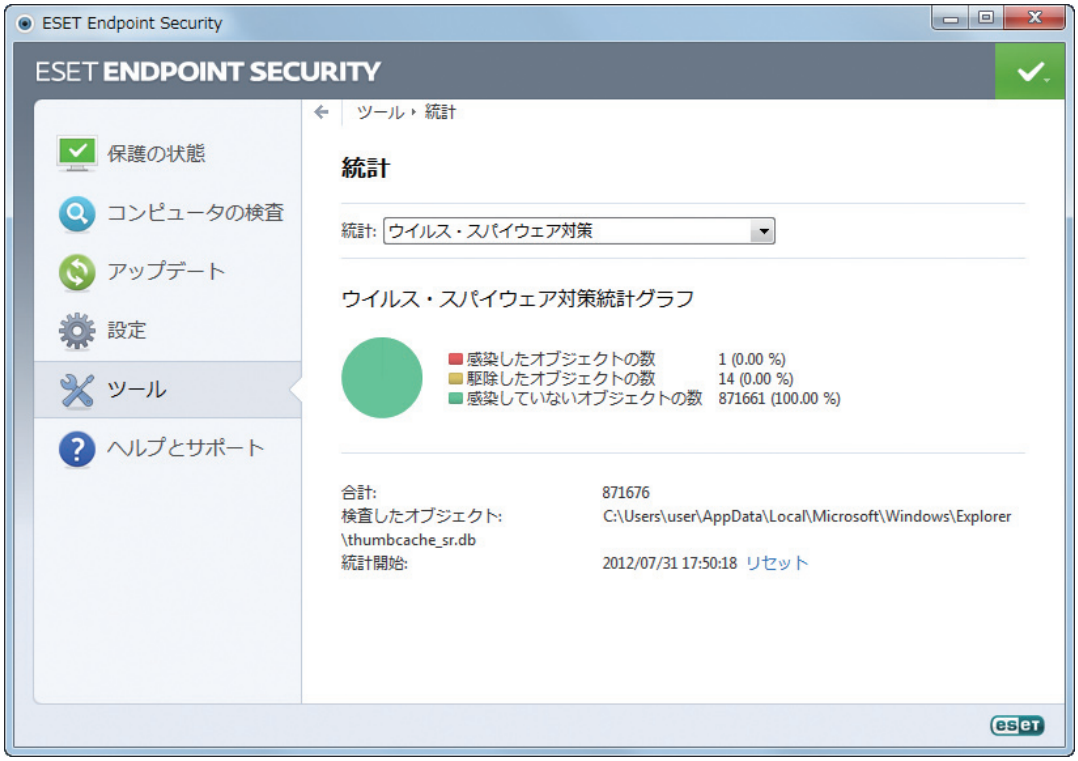
●次にスケジュールされた時刻まで待機
●実行可能になりしだい実行する
●前回実行されてから次の時間が経過した場合直ちに実行する

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の概要が表示されます。[特定のパラメータでタスクを実行する] チェックボックスは自動的にチェックされます。[完了] ボタンをクリックします。

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指定することができます。代替プロファイルは、プライマリプロファイルを使用してタスクを実行できない場合に使用されます。確認画面で [終了] をクリックして確認します。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。

4.7.3 統計

ESET Endpoint Securityの保護機能に関連する統計データのグラフを表示するには、[ツール]＞[保護統計]をクリックします。[統計]ドロップダウンメニューから該当する保護機能を選択して、対応するグラフと凡例を表示します。凡例の項目の上にカーソルを置くと、その項目のデータのみがグラフに表示されます。



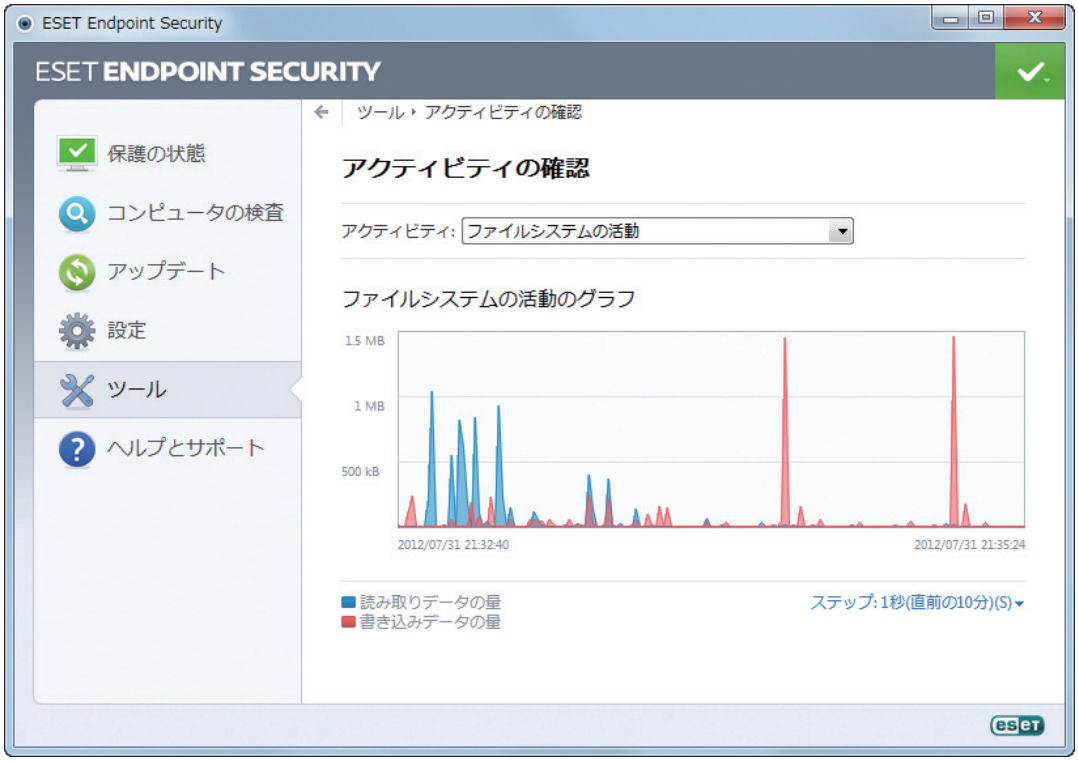
使用可能な統計グラフは次のとおりです。

ウイルス・スパイウェア対策	感染オブジェクトおよび駆除済みオブジェクトの数を表示します。
リアルタイムファイルシステム保護	読み込まれたオブジェクト、またはファイルシステムに書き込まれたオブジェクトのみを表示します。
電子メールクライアント保護	メールクライアントが送信または受信したオブジェクトのみを表示します。
Webアクセス保護	Webブラウザによってダウンロードされたオブジェクトのみを表示します。
電子メールクライアント迷惑メール対策機能	前回の起動以降の迷惑メール統計の履歴を表示します。

統計グラフの下に、検査されたオブジェクトの総数、検査された最新オブジェクト、および統計タイムスタンプが表示されます。すべての統計情報を消去するには、[リセット]をクリックします。

4.7.4 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、選択された期間で、ファイルシステムアクティビティのエントリの時系列をリアルタイムに示します。期間を変更するには、ウィンドウの右下にある [ステップ1...] オプションをクリックします。



使用可能なオプションは次のとおりです。

ステップ1秒(直前の10分)	グラフは1秒おきに更新され、時系列は直近10分間を示します。
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、時系列は過去1カ月間を示します。
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、時系列は選択した過去Xカ月間を示します。

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(赤)と書き込みデータ(青)を表します。どちらもKB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。

[アクティビティ] 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] を表示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(赤)と送信データ(青)を表示することを除いて同じです。

4.7.5 ESET SysInspector

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

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。

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ログが終了する(作成済みの[状態])までお待ちください。
削除	選択したログをリストから削除します。

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

表示	ESET SysInspectorで選択したログを開きます(ログをダブルクリックするのと同じ機能)。
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。

4.7.6 ESET Live Grid

ESET Live Grid（次世代のESET ThreatSense.Net）は、台頭しつつある脅威に対して評価に基づいて対処する先進の警告システムです。ESETウィルスラボは、クラウドから得たウイルス関連情報をリアルタイムで活用することで、常に防御策を最新に保って定常的な保護に努めています。ユーザーは、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 Live Gridに用意されている追加情報を読んで、稼働中のプロセスやファイルの評価をチェックすることができます。2つのオプションがあります。

1.ESET Live Gridを有効にしないこともできます。ソフトウェアの機能は失われず、提供される最高の保護を受けることができます。
2.新しいウイルスと新しい危険なコードが含まれている場所に関する匿名の情報を提出するようにESET Live Gridを設定することができます。このファイルをESETに送信して詳しい解析を受けることができます。これらのウイルスを調査することで、ESETはウイルス検出機能を最新のものにすることができます。

ESET Live Gridは、新しく検出されたウイルスに関連してコンピュータ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に侵入したプロセス、およびコンピュータ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。

ESET Live Gridの設定メニューには、疑わしいファイルや匿名の統計情報をESETのラボに提出するのに使用するESET Live Gridを有効または無効にするためのオプションがいくつかあります。この設定メニューにアクセスするには、[詳細設定] ツリーで [ツール] > [ESET Live Grid] をクリックします。

ESET Live Gridへの参加に同意する（推奨）	疑わしいファイルや匿名の統計情報をESETラボに提出するのに使用するESET Live Gridを有効または無効にします。
統計を提出しない	ご使用のコンピュータに関する匿名情報をESET Live Gridから提出しない場合に選択します。これは、ウイルス名、検出日時情報、ESET Endpoint Securityバージョン、コンピュータのオペレーティングシステムバージョン、場所設定などの、新たに検出された脅威に関する情報です。統計は通常、1日1回または2回、ESETのサーバに配信されます。
ファイルを提出しない	内容または動作から判断してウイルスと思われるファイルが、ESETに提出され、ESET Live Gridテクノロジによる解析を受けます。
詳細設定...	ESET Live Gridの詳細設定を指定するウィンドウを開きます。

以前にESET Live Grid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。無効にした後も、このようなパッケージは次の機会にESETに送信されます。その後、それ以上パッケージが作成されることはありません。

4.7.6.1 不審なファイル

ESET Live Gridの詳細設定の[ファイル]タブでは、分析を受けるためにESETのウイルスラボにウイルスを提出する方法を設定することができます。

不審なファイルは、ESETのウイルスラボに提出して分析を受けることができます。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、次のウイルス定義のアップデートにその検出が追加されます。

除外フィルタ
除外フィルタを使用すると、特定のファイルやフォルダを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。たとえば、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可能性があるファイルを除外するときに便利です。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。

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。

このセクションでは、ESETリモートアドミニストレーターを使用してファイルおよび統計情報を提出するか、または直接ESETに提出するかを選択することもできます。疑わしいファイルおよび統計情報を確実にESETに渡したい場合、[リモート管理者経由または直接ESETへ]オプションを選択します。すると、すべての利用可能な手段を使ってファイルと統計が送信されます。リモート管理者を介して疑わしいファイルを送信すると、ファイルと統計はリモート管理者サーバーに送信され、そこからさらに、ESETのウイルスラボに確実に送信されます。[直接ESETへ]オプションを選択した場合、すべての疑わしいファイルと統計情報は、プログラムからESETのウイルスラボに直接送信されます。

[ログを有効にする]オプションを選択し、ファイルと統計情報の送信を記録するイベントログを作成します。それによって、ファイルまたは統計の送信時のイベントログへのログ記録が可能になります。

4.7.7実行中のプロセス

実行中のプロセスは、コンピュータ上で実行中のプログラムまたはプロセスを表示し、新規の侵入を即座に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 Live Grid技術でユーザーを保護します。

プロセス	コンピュータ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を押して、タスクマネージャを開くことができます。
リスクレベル	多くの場合、ESET Endpoint SecurityおよびESET Live Grid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1-良好(緑) ～ 9-危険(赤)のリスクレベルが割り当てられます。

››› NOTE

良(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 Live Grid技術によって収集されます。
初回発見日	ESET Live Grid技術によってアプリケーションが検出されてからの期間。

››› POINT

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。ファイルに確信が持てない場合、ESETのウイルスラボに分析のためにファイルを提出できます。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更新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。
新しいウィンドウで開く	実行中のプロセスの情報は新規ウィンドウに表示されます。

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。

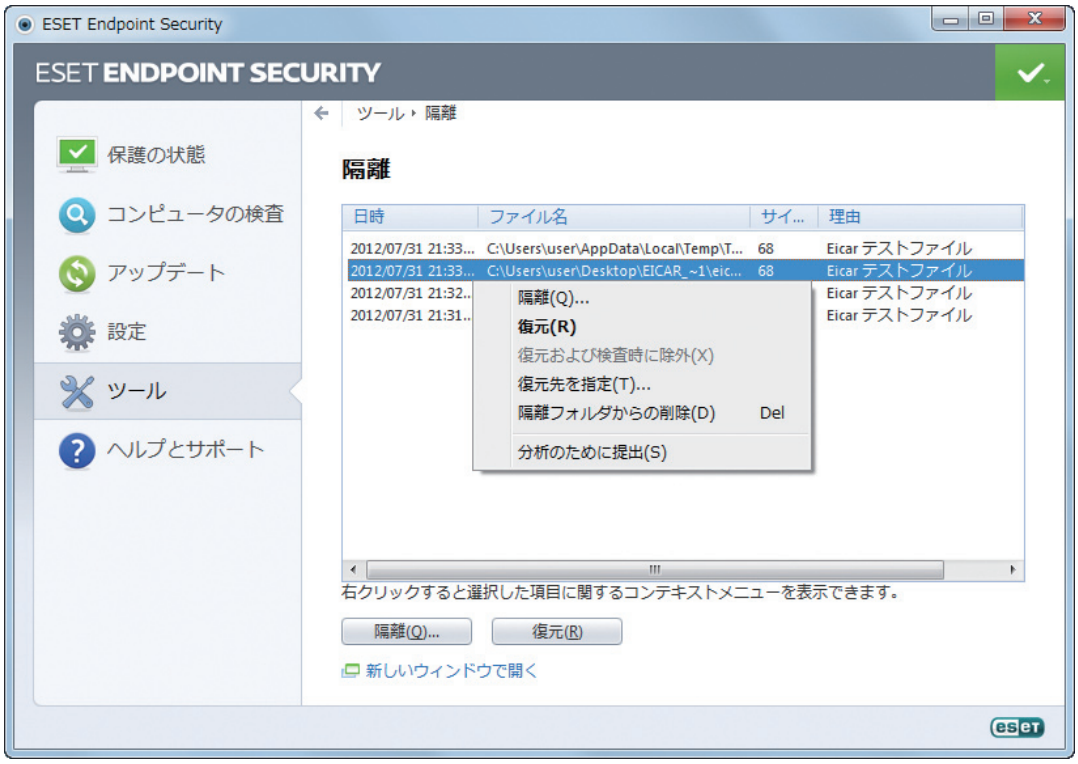
●ファイル―コンピュータ上のアプリケーションの場所。
●ファイルサイズ―ファイルサイズがKB（キロバイト単位）またはMB（メガバイト単位）のいずれか。
●ファイルの説明―オペレーティングシステムからの情報に基づくファイル特性。
●会社名―ベンダまたはアプリケーションプロセスの名前。
●ファイルのバージョン―アプリケーション発行元からの情報。
●製品名―アプリケーション名および/または商号。

▸▸▸ NOTE

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 Live Gridを使用したファイル評価のチェック]を選択します。

4.7.8 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、外向き通信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。

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。
新しいウィンドウで開く	別のウィンドウで情報を表示します。[ネットワーク接続] 画面の [接続表示を設定...] オプションには、詳細設定構造が開き、接続表示オプションを変更するセクションが表示されます。
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プロトコル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。
コンピュータがリッスンしている開いたポートを使用する接続を表示する	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も表示する	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。
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。
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。

4.7.9 隔離

隔離の主な機能は、感染ファイルを安全に保存することにあります。ファイルを駆除できない場合、ファイルの削除が安全でもなければ推奨もされない場合、あるいはESET Endpoint Securityで誤って検出された場合は、ファイルを隔離する必要があります。

任意のファイルを選択して隔離することができます。これは、ファイルの動作が疑わしいにもかかわらず、ウイルス対策スキャナによって検出されない場合にお勧めします。隔離したファイルは、ESETのウイルスラボに提出して分析を受けることができます。

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

ファイルの隔離

削除されたファイルは、ESET Endpoint Securityにより自動的に隔離されます（警告ウィンドウでユーザーがこのオプションをキャンセルしなかった場合）。必要に応じて、[隔離...] ボタンをクリックして不審なファイルを手動で隔離することができます。この場合、元のファイルは元の場所から削除されません。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...] オプションを選択します。

隔離フォルダからの復元

隔離されているファイルを、元の場所に復元することもできます。そのためには、[復元] 機能を使用します。この機能は、隔離ウィンドウで特定のファイルを右クリックして、コンテキストメニューから選択することができます。ファイルに [望ましくない可能性があるアプリケーション] のマークがついている場合、[復元および検査時に除外] オプションが有効になります。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。コンテキストメニューには、[復元先を指定...] オプションもあります。このオプションを使用すると、隔離される前の場所とは異なる場所にファイルを復元することができます。

隔離からのファイルの提出

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

4.7.10 分析用ファイルの提出

[ツール] > [分析のためにファイルを提出] の [ファイルの提出] ダイアログからは、ESETに分析するファイルを送信できます。動作が疑わしいファイルがコンピュータ上で見つかった場合、ESETのウイルスラボにファイルを提出して解析を受けることができます。そのファイルが悪意のあるアプリケーションであることが判明すると、それ以降のいずれかの更新ファイルにその検出が追加されます。

NOTE

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

●ファイルがまったく検出されない
●ファイルが誤ってウイルスとして検出される

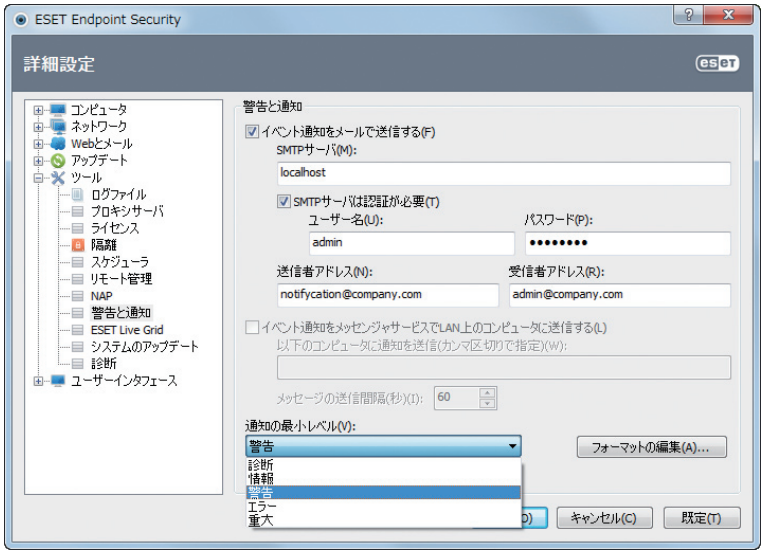
解析のために詳しい情報が必要でない限り、ESETから連絡することはありません。

以下の [ファイル提出の理由] 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
●誤検出（感染と検出されたけれども未感染であるファイル）
●その他

ファイル	提出するファイル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。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に送られてくるので、全ての提出に返信することはできません。

4.7.11 警告と通知

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の電子メールの送信をサポートします。[イベント通知をメールで送信する]チェックボックスをクリックしてこの機能を有効にし、電子メール通知を有効にします。



SMTPサーバー	通知を送信するために使用されるSMTPサーバ。 注意:SSL/TLS暗号化機能を備えたSMTPサーバーは、ESET Endpoint Securityではサポートされません。
SMTPサーバは認証が必要	SMTPサーバーが認証を必要とする場合、SMTPサーバーへのアクセス許可に対して有効なユーザー名とパスワードをフィールドに入力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。
イベント通知をメッセンジャサービスでLAN上のコンピューターに送信する	このチェックボックスを選択し、Windowsメッセージングサービスを介してLANコンピュータにメッセージを送信します。
以下のコンピュータに通知を送信(カンマ区切りで指定)	Windowsメッセージングサービスを使用して通知を受け取るコンピュータの名前を入力します。
メッセージの送信間隔(秒)	LAN経由で送信される通知の間隔を変更する場合、必要な間隔を秒単位で入力します。
通知の最小詳細レベル	送信する通知の最低詳細レベルを指定します。
フォーマットの編集...	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、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-[フォーマットの編集...をクリックします。

4.7.11.1 メッセージの書式

ここで、リモートコンピュータ上に表示されるイベントメッセージの形式を設定できます。

脅威警告メッセージおよび通知メッセージには、既定の書式があらかじめ定義されています。この書式は変更しないようお勧めします。ただし、状況によっては（自動メール処理システムを使用している場合など）、メッセージの書式を変更しなければならないことがあります。

メッセージでは、指定されている実際の情報でキーワード（%記号で区切られた文字列）が置き換えられます。使用可能なキーワードは次のとおりです。

●% TimeStamp %—イベントの日時。
●% Scanner %—関連するモジュール。
●% ComputerName %—警告が発生したコンピュータの名前。
●% ProgramName %—警告を生成したプログラム。
●% InfectedObject %—感染しているファイルや電子メールなどの名前。
●% VirusName %—ウイルスのID。
●% ErrorDescription %—ウイルス以外のイベントの説明。

キーワード% InfectedObject % および % VirusName % は脅威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。

各地域のアルファベット文字を使用	Windowsの地域の設定に基づいて、電子メールメッセージをANSI文字エンコーディング（たとえば windows-1250）に変換します。このオプションのチェックを外すと、メッセージは変換されてACSII 7ビット（たとえば"a"は"a"に変換され、不明の記号は"?"に変換されます）でエンコードされます。
各地域の文字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（aeiou）の電子メールで正確に送信できます。

4.7.12 システムのアップデート

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不可欠です。ESET Endpoint Securityは、指定されたレベルに従って、欠如したアップデートがあるとユーザーにそれを通知します。使用可能なレベルは次のとおりです。

●通知しない—ダウンロードできるシステムアップデートはありません。
●オプションのアップデート—低優先度以上とマークされているアップデートがダウンロード用として提示されます。
●推奨されるアップデート—通常優先度以上とマークされているアップデートがダウンロード用として提示されます。
●重要なアップデート—重要優先度以上とマークされているアップデートがダウンロード用として提示されます。
●緊急のアップデート—緊急のアップデートのみがダウンロード用として提示されます。

変更内容を保存するには、[OK] をクリックします。アップデートサーバでステータスの検証を行った後、[システムのアップデート] ウィンドウが表示されます。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。

4.7.13 診断

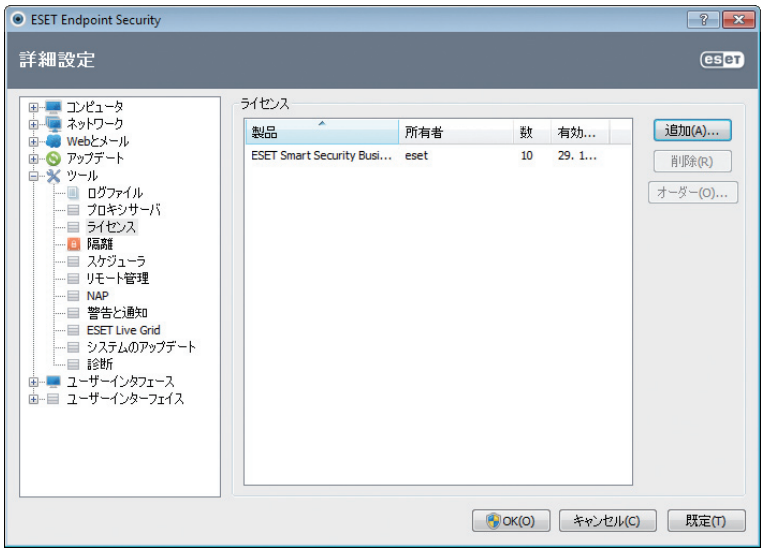
診断では、ESETのプロセス（ekrnなどの）のアプリケーションクラッシュダンプが生成されます。アプリケーションがクラッシュした場合、ダンプが生成されます。開発者はこれを使用し、ESET Endpoint Securityのさまざまな問題をデバッグまたは修正できます。次の2種類のダンプを利用できます。

●完全なメモリダンプ—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。完全なメモリダンプには、メモリ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。
●ミニダンプ—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最低限必要な一連の有用な情報が記録されます。容量が限られているときは、この種のダンプファイルは便利です。しかし、収容できる情報が限られるため、問題の発生時に実行されていたスレッドがエラーの直接の原因ではない場合、ファイルを解析しても原因を判別できない場合があります。
●この機能を無効にするには、[メモリダンプを生成しない]（既定）を選択します。

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です。このディレクトリを新しいWindows Explorer ウィンドウで開く場合は、[フォルダを開く...] をクリックします。

4.7.14 ライセンス

[ライセンス] ブランチを使用すると、ESET Endpoint Securityおよび ESET Remote Administratorなどの他のライセンス製品のライセンスキーを管理できます。製品を購入すると、ユーザー名やパスワードと共にライセンスキーが配布されます。ライセンスキーを追加/削除するには、ライセンスマネージャ (ライセンス) ウィンドウの [追加/削除] ボタンをクリックします。ライセンスマネージャには、詳細設定ツリーの [ツール] > [ライセンス] をクリックしてアクセスすることができます。



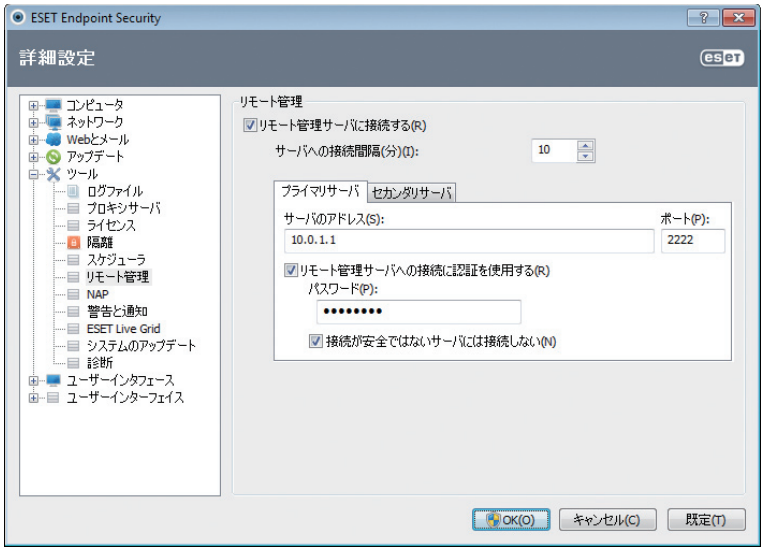
ライセンスキーは、購入した製品に関する情報 (所有者、ライセンス数、および有効期限) を記載したテキストファイルです。

ライセンスマネージャウィンドウでは、[追加...] ボタンを使用して、ライセンスキーの内容をアップロードし、表示することができます。ライセンスファイルをリストから削除するには、選択して [削除] ボタンをクリックします。

4.7.15 リモート管理

ESET Remote Administrator（ERA）は、セキュリティポリシーを管理するため、およびネットワーク内の全体的なセキュリティの概要を取得するために使用する強力なツールです。大規模なネットワークに適用すると、特に効果的です。ERAによってセキュリティレベルが向上するだけでなく、クライアントワークステーションにおけるESET Endpoint Securityの管理が容易になります。インストール、設定、ログの表示、更新タスクやスキャンタスクのスケジュールなどが可能です。ESET Remote Administrator Server（ERAS）とESETセキュリティ製品間の通信には、両方のエンドポイントにおける適切な設定が必要です。

リモート管理の設定オプションには、ESET Endpoint Securityのメインウィンドウからアクセスすることができます。[設定] > [詳細設定を表示する...] >> [ツール] > [リモート管理] をクリックしてください。



リモート管理を有効にするには、[リモート管理サーバーに接続する] オプションを選択します。この操作で、下記のその他のオプションへのアクセスが可能になります。

サーバへの接続間隔（分）	ESETセキュリティ製品がデータを送信するためにERASに接続する頻度を指定します。
プライマリサーバ、セカンダリサーバ	一般的にはプライマリサーバのみを設定する必要があります。複数のERAサーバがネットワーク上で稼働している場合、別のセカンダリERAサーバ接続を追加することもできます。追加した接続はフォールバックソリューションとして機能します。プライマリサーバにアクセスできなくなると、ESETセキュリティソリューションは自動的にセカンダリERAサーバに問い合わせます。同時に、プライマリサーバへの接続の再確立を試行します。この接続が再度有効になると、ESETセキュリティソリューションはプライマリサーバに戻されます。2つのリモート管理サーバープロファイルの設定は、ローカルネットワークおよびネットワーク外部の両方から接続するクライアントをもつモバイルクライアントに最も適しています。
サーバのアドレス	ERASを実行するサーバのDNS名またはIPアドレスを指定します。
ポート	このフィールドには、接続に使用される、あらかじめ定義されたサーバポートが表示されます。既定のポート設定"2222"をそのまま使用することをお勧めします。
サーバへの接続間隔（分）	ESET Endpoint SecurityがERA Serverに接続する頻度を指定します。0に設定されている場合、5秒ごとに情報が送信されます。
リモート管理サーバへの接続に認証を使用する	必要に応じて、ERA Serverへの接続に使用するパスワードを入力することができます。
接続が安全ではないサーバには接続しない	このオプションを選択すると、不正アクセスが有効なERAサーバーとの接続が無効になります（[ERA Console]>[サーバのオプション]>[セキュリティ]>[クライアントの未承認のアクセスを有効にする]を参照）。

[OK] をクリックして変更を確認し、設定を適用します。ESET Endpoint Securityはこれらの設定を使用して、ERA Serverに接続します。

4.8 ユーザーインタフェース

[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フェース (GUI) の動作を設定できます。

[グラフィックス] 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。

[警告と通知] の設定により、検出された脅威についての警告およびシステム通知の動作を変更できます。これらは、ご自身のニーズに合わせてカスタマイズできます。

一部の通知を表示しないように選択した場合、これらの通知は [非表示の通知ウィンドウ] 領域に表示されます。ここでは、ステータスの確認、詳細の表示、またはこのウィンドウからの詳細の削除を実行できます。

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パスワードによる設定の保護を実現し、不正な変更を防止します。

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。

4.8.1 グラフィックス

ESET Endpoint Securityのユーザーインタ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] > [グラフィックス] ブランチからアクセスします。

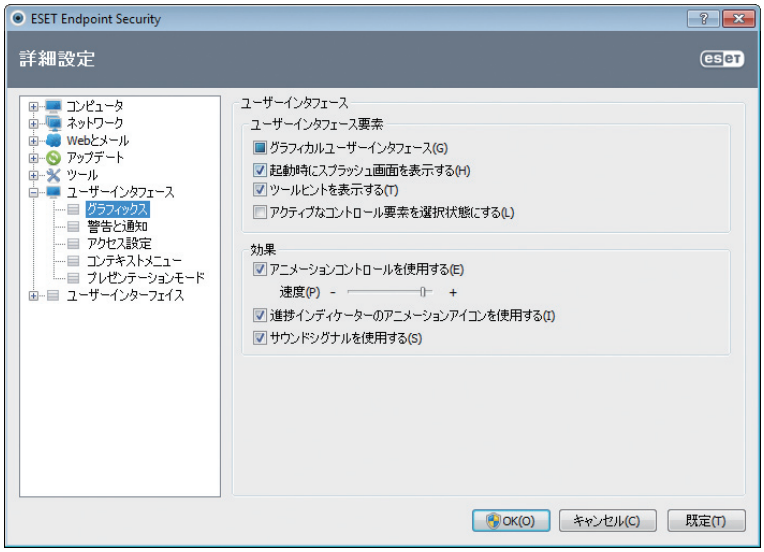
グラフィカル要素によってコンピュータのパフォーマンスが低下低下する場合や、その他の問題が発生する場合は、[ユーザーインタフェース要素] セクションの [グラフィカルユーザーインタフェース] オプションを無効にする必要があります。また、ユーザーが視覚に障害のある場合は、画面に表示されるテキストの読み上げ専用アプリケーションと競合するグラフィカルインタフェースをオフにする必要があります。

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] チェックボックスのチェックを外します。

[ツールヒントを表示する] オプションが有効化されている場合は、オプションの上にカーソルを置くと、そのオプションの簡単な説明が表示されます。[アクティブなコントロール要素を選択する] チェックボックスをチェックすると、現在マウスカーソルのアクティブな領域の下にある要素が強調表示されます。マウスでクリックすると、強調表示された要素がアクティブになります。

アニメーション効果の速度を増減するには、[アニメーションコントロールを使用する] オプションを選択して、[速度] スライダバーを左右に移動します。

さまざまな操作の進捗を示すアニメーションアイコンの使用を有効にするには、[進捗インディケーターのアニメーションアイコンを使用する] オプションを選択します。重要なイベントが発生したときに警告音を鳴らすには、[サウンドシグナルを使用する] オプションを選択します。



4.8.2 警告と通知

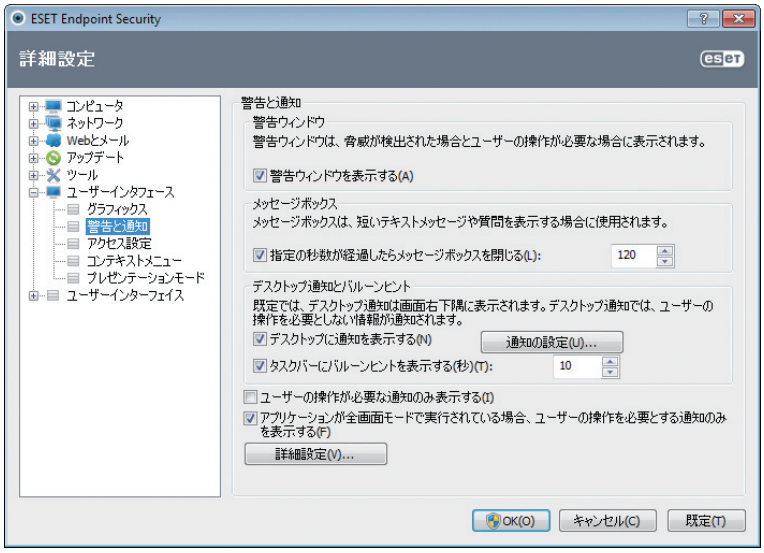
[ユーザーインタフェース] の下にある [警告と通知の設定] を使用すると、ウイルス警告メッセージやシステム通知（アップデートメッセージの成功など）をESET Endpoint Securityでどのように処理するかを設定することができます。また、システムトレイ通知の表示時間と透明度のレベルを設定することもできます（システムトレイ通知をサポートするシステムのみに適用されます）。

最初の項目は [警告を表示する] です。このチェックボックスのチェックを外すと、全ての警告ウィンドウが表示されなくなります。この設定が適しているのは、特定の限られた状況のみです。ほとんどのユーザーには、既定の設定のままにすることをお勧めします（チェックボックスをオンにします）。

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、[指定の秒数が経過したらメッセージボックスを閉じる] チェックボックスを選択します。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。

デスクトップ通知とバルーンヒントに表示される情報は情報を提供するのみのもので、ユーザーには操作を求めていません。これらは、画面の右下にある通知領域に表示されます。デスクトップ通知を有効にするには、[デスクトップに通知を表示する] オプションを選択します。[通知の設定...] ボタンをクリックすると、通知の表示時間やウィンドウの透明度などの詳細なオプションを変更することができます。通知の動作をプレビューするには、[プレビュー] ボタンをクリックします。

バルーンヒントの表示時間を設定するには、[タスクバーにバルーンヒントを表示する（秒）] オプションを参照して、任意の時間間隔を隣接フィールドに入力します。



[ユーザーの操作が必要な通知のみ表示する] オプションを使用すると、ユーザーの操作を必要としない警告や通知をオンまたはオフにすることができます。対話式でないすべての通知が表示されないようにするには、[アプリケーションが全画面モードで実行されている場合、ユーザーが操作を必要とする通知のみを表示する] を選択します。

[詳細設定...] をクリックすると、追加の [警告と通知] 設定オプションが表示されます。

4.8.2.1 詳細設定

警告および通知の表示を開始する重大度を、[表示イベントの最小レベル] ドロップダウンメニューから選択できます。

●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―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、パーソナルファイアウォールなど）のエラーを記録します。

このセクションの最後の機能からは、マルチユーザー環境における通知の送付先を設定できます。[マルチユーザーシステムの場合、以下のユーザーの画面に通知を表示する] フィールドでは、複数のユーザーが同時に接続できるシステムで、システム通知やその他の通知を受け取るユーザーを指定します。通常は、システム管理者またはネットワーク管理者です。このオプションは、全てのシステム通知が管理者に送信される場合、ターミナルサーバに特に便利です。

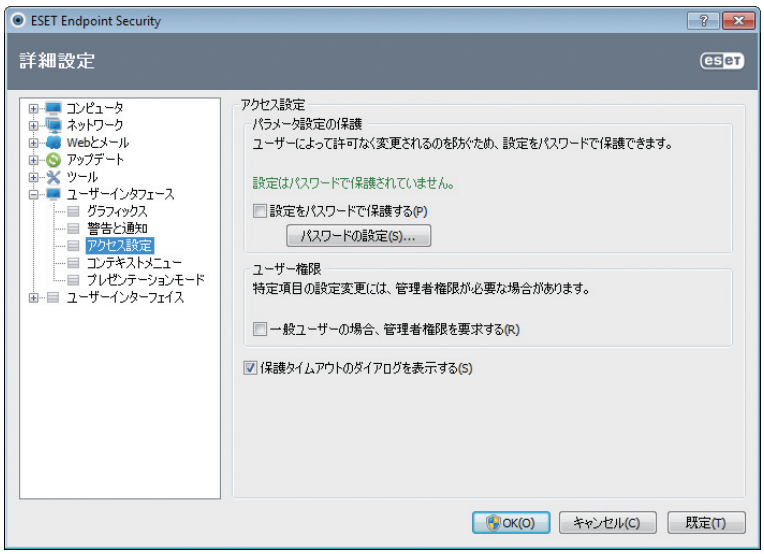
4.8.3 非表示の通知ウィンドウ

以前に表示された任意の通知ウィンドウ（警告）で、[このメッセージを再度表示しない] オプションが選択された場合、非表示の通知ウィンドウのリストにそれが表示されます。現在自動的に実行されるアクションは、[確認] という列に表示されます。

表示	現在表示されないけれども自動処理を設定されている通知ウィンドウのプレビューが表示されます。
削除	[非表示のメッセージボックス]のリストから項目を削除します。リストから削除された通知ウィンドウは全て表示されるようになります。

4.8.4 アクセス設定

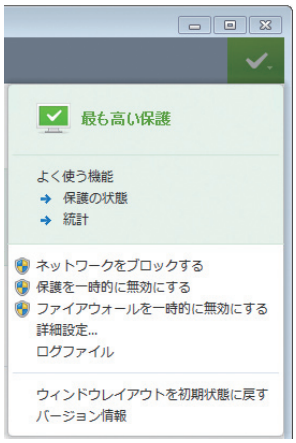
システムのセキュリティを最大限に確保するには、ESET Endpoint Securityを正しく設定することが重要です。資格のないユーザーによって変更が行われた場合、重要なデータが失われることがあります。このオプションは、詳細設定ツリーの[ユーザーインタフェース]の下の[アクセス設定]サブメニューに配置されています。認証されていないユーザーによる変更を防ぐために、ESET Endpoint Securityの設定パラメータをパスワードで保護することができます。



設定をパスワードで保護する	プログラムの設定パラメータをロック/ロック解除します。このチェックボックスをチェックするか、チェックを外すと、[パスワードの設定]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を保護するには、[パスワードの設定...]をクリックします。
一般ユーザーの場合、管理者権限を要求する	特定のシステムパラメータの変更時に、管理者のユーザー名とパスワードを入力する(Windows VistaのUACと同様)よう現在のユーザーに求める場合(このユーザーに管理者権限がない場合)、このオプションを選択します。パラメータの変更には、保護モジュールの無効化やファイアウォールの無効化などが含まれます。
保護タイムアウトのダイアログを表示する	プログラムメニューまたは[ESET Endpoint Security]>[設定]セクションから一時的に保護を無効にしているときに、このオプションを選択すると、指示されます。[保護を一時的に無効にする]ウィンドウの[間隔]ドロップダウンメニューには、選択されている保護が無効になる期間を示します。

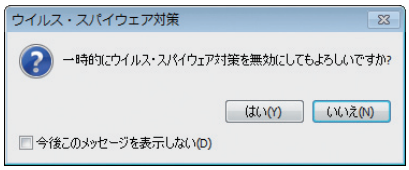
4.8.5 プログラムメニュー

最も重要な設定オプションおよび機能の一部は、メインプログラムメニューにあります。

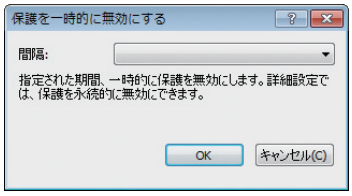


よく使う機能—ESET Endpoint Securityの使用頻度の最も高い部分を表示します。プログラムメニューからこれらに素早くアクセスできます。

保護を一時的に無効にする—ファイル、Web、およびメール通信を制御することによって悪意のあるシステム攻撃から保護する、ウイルス·スパイウェア対策を無効にするための確認ダイアログボックスを表示します。このメッセージを今後表示しないようにするには、[このメッセージを今後表示しない] チェックボックスを選択します。



[間隔] ドロップダウンメニューは、すべてのウイルス·スパイウェア対策保護機能を無効にする期間を示します。



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パーソナルファイアウォールによってブロックされます。
ファイアウォールを一時的に無効にする	ファイアウォールを無効状態に切り替えます。詳しくは、「パーソナルファイアウォールのシステム統合」を参照してください。
詳細設定(D)...	[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。F5キーを押すか、あるいは [設定] > [詳細設定を表示する...] に移動するなど、他の方法によって開くこともできます。
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、検出された脅威の概要が表示されます。
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。
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、およびインストールされているプログラムモジュールが表示されます。また、ライセンスの有効期限も確認できます。一番下には、オペレーティングシステムおよびシステムリソースについての情報が記載されています。

4.8.6 コンテキストメニュー

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が表示されます。このメニューには、そのオブジェクトで実行できるオプションが全て表示されます。

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できます。詳細設定ツリー（[ユーザーインタフェース]＞[コンテキストメニュー]）に、この機能に対する詳細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。

[メニュータイプ] ドロップダウンメニューには、次のオプションがあります。

フル（最初に検査）	すべてのコンテキストメニューオプションを有効にします。メインメニューには、[ESET Endpoint Securityで検査]オプションが表示されます。
フル（最初に駆除）	すべてのコンテキストメニューオプションを有効にします。メインメニューには、[ESET Endpoint Securityで駆除]オプションが表示されます。
スキャンのみ	[ESET Endpoint Securityでスキャン]オプションのみがコンテキストメニューに表示されます。
駆除のみ	[ESET Endpoint Securityで駆除]オプションのみがコンテキストメニューに表示されます。

4.8.7 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する必要があり、ポップアップウィンドウに邪魔されることを望まず、そして CPUの使用量を最小化したいと願う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。この機能を有効にすると、すべてのポップアップウィンドウが無効になり、スケジューラの活動は完全に停止されます。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。

メインプログラムウィンドウの [プレゼンテーションモード] を有効または無効にするには、[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] の下の [有効] をクリックします。あるいは、詳細設定ツリー (F5) で、プレゼンテーションモード [ユーザインタフェース] を展開し、プレゼンテーションモードをクリックして、[プレゼンテーションモードを有効にする.の横にあるチェックボックスをオンにします。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黄色になり、警告が表示されます。また、この警告は、プレゼンテーションモードは有効ですが黄色で表示されている場合にもメインプログラムウィンドウに表示されます。

[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] チェックボックスをチェックすると、アプリケーションを全画面モードで起動した場合にはプレゼンテーションモードが自動的に開始し、そのアプリケーションを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、[プレゼンテーションモードを一定時間後に自動的に無効にする] チェックボックスをチェックし、時間 (既定値は1分) を定義することもできます。これを使用するのは、プレゼンテーションモードをある一定の時間だけ必要とし、その後自動的に無効にしたい場合です。

▸▸▸ NOTE

パーソナル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、インターネットへの接続で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ゲーム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、次のモードではユーザーの操作は無効になっています:プレゼンテーションモード.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、パーソナル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。また、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。

[Chapter 5]
上級者向けガイド

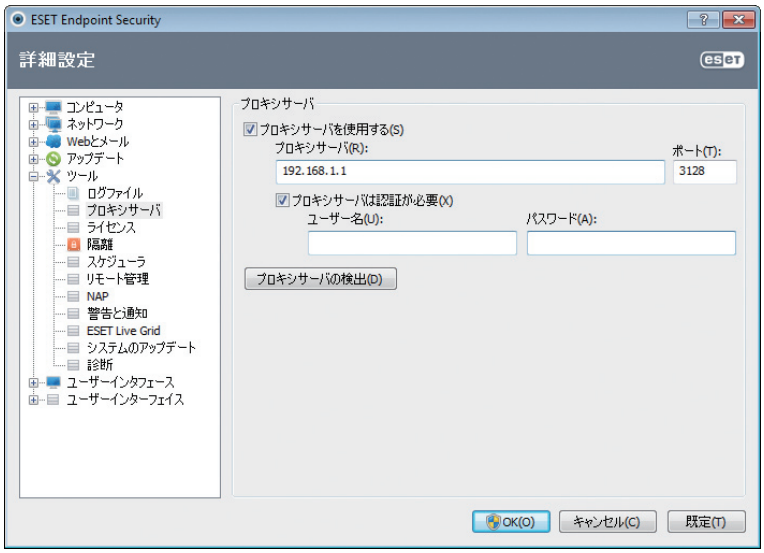
5.1 プロキシサーバーの設定……146
5.2 設定のインポート / エクスポート……147
5.3 キーボードショートカット……148
5.4 コマンドライン……149
5.5 ESET SysInspector……152
5.6 ESET SysRescue……169

5.1 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に接続されている場合があります。この場合は、次の設定を定義する必要があります。定義しなかった場合、プログラムは自動的にアップデーされません。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を設定できます。

まず、プロキシサーバは [詳細設定] の [ツール] > [プロキシサーバ] から設定できます。プロキシサーバ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] チェックボックスを選択し、プロキシサーバのアドレスを [プロキシサーバ] フィールドに入力し、プロキシサーバーの [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] チェックボックスをオンにし、有効なユーザ名とパスワードをそれぞれのフィールドに入力します。[プロキシサーバの検出] ボタンをクリックすると、自動的にプロキシサーバの設定が検出されて取り込まれます。Internet Explorerに指定したパラメータがコピーされます。

NOTE

この機能では、認証データ(ユーザー名とパスワード)は取り出されないので、ユーザーが入力する必要があります。

プロキシサーバの設定は、[詳細なアップデート設定] ([詳細設定] ツリーの [アップデート] ブランチ) から実行することもできます。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。ウイルス定義アップデートをさまざまな場所から受信するノート型コンピュータにお勧めします。この設定の詳細について、「詳細なアップデート設定」のセクションを参照してください。

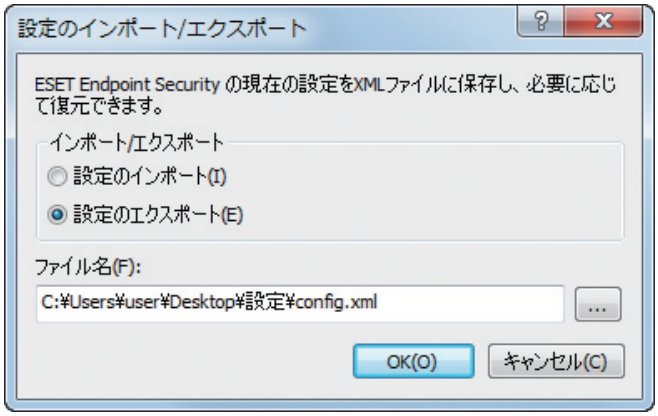
5.2 設定のインポート/エクスポート

ESET Endpoint Securityの設定のインポートとエクスポートは、[設定] から行うことができます。

インポートおよびエクスポートの両方で、.xmlファイルタイプを使用します。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、ESET Endpoint Securityの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、目的の設定を転送できます。

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] オプションを選択します。設定ファイルのパスを入力するか、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] オプションを選択し、設定ファイルのファイル名（つまりexport.xml）を入力します。ブラウザを使用して、設定ファイルの保存先を選択します。



5.3 キーボードショートカット

ESET Endpoint Securityで使用できるショートカットキーは、次のとおりです。

Ctrl+G	製品のGUIを無効にします
Ctrl+I	ESETSysInspectorページを開きます
Ctrl+L	[ログファイル] ページを開きます
Ctrl+S	[スケジューラ] ページを開きます
Ctrl+Q	[隔離] ページを開きます
Ctrl+U	ユーザー名とパスワードを設定するダイアログウィンドウを開きます
Ctrl+R	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

ESETセキュリティ製品での移動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。

F1	ヘルプページを開きます
F5	詳細設定を開きます
上へ/下へ	製品の項目間を移動します
*	詳細設定ツリーノードを展開します
-	詳細設定ツリーノードを折りたたみます
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

5.4 コマンドライン

ESET Endpoint Securityのウイルスから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。ESETコマンドラインスキャナの使用法は、次のとおりです。

ecls [OPTIONS..] FILES..

コマンドラインからオンデマンドスキャナを実行する際には、次のパラメータ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=FOLDER	FOLDERからモジュールをロードします
/quar-dir=FOLDER	FOLDERを隔離します
/exclude=MASK	MASKと一致するファイルをスキャン対象から除外します
/subdir	サブフォルダを検査します(既定)
/no-subdir	サブフォルダ検査しません
/max-subdir-level=LEVELス	キャン対象に含めるサブフォルダ階層の下限レベル
/symlink	シンボリックリンクをたどります(既定)
/no-symlink	シンボリックリンクをスキップします
/ads ADS	を検査します(既定)
/no-ads ADS	を検査しません
/log-file=FILE	ログをFILEに出力します
/log-rewrite	ログファイルを上書きします(既定-append)
/log-console	ログをコンソールに出力します(既定)
/no-log-console	ログをコンソールに出力しません
/log-all	感染していないファイルも記録します
/no-log-all	感染していないファイルは記録しません(既定)
/aind	アクティビティインジケータを表示します
/auto	すべてのローカルディスクを検査し、自動的に駆除します

スキャナオプション

/files	ファイルを検査します（既定）
/no-files	ファイルを検査しません
/memory	メモリを検査します
/boots	ブートセクタを検査します
/no-boots	ブートセクタを検査しません（既定）
/arch	アーカイブを検査します（既定）
/no-arch	アーカイブを検査しません
/max-obj-size=SIZE	SIZEメガバイト未満のファイルのみスキャンします（既定0=制限なし）
/max-arch-level=LEVEL	スキャン対象に含めるアーカイブ内の上限ネストレベル
/scan-timeout=LIMIT	最大でLIMIT秒間アーカイブを検査します
/max-arch-size=SIZE	アーカイブのうち、SIZE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
/adware	アドウェア/スパイウェア/リスクウェアを検査します（既定）
/no-adware	アドウェア/スパイウェア/リスクウェアを検査しません
/unsafe	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）
/pattern	シグネチャを使用します（既定）
/no-pattern	シグネチャを使用しません
/heurヒューリスティック	を有効にします（既定）
/no-heur	ヒューリスティックを無効にします
/adv-heur	アドバンスドヒューリスティックを有効にします（既定）
/no-adv-heur	アドバンスドヒューリスティックを無効にします
/ext=EXTENSIONS	コロンで区切られたEXTENSIONSのみをスキャンします
/ext-exclude=EXTENSIONS	コロンで区切られたEXTENSIONSをスキャン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（MODE）:none、standard（既定）、strict、rigorous、delete
/quarantine	感染ファイルを隔離フォルダにコピーします（駆除中に実行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	脅威は検出されませんでした
1	脅威が検出され、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（脅威の可能性あり）
50	脅威が検出されました
100	エラー

▸▸▸ NOTE

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。

5.5 ESET SysInspector

ESET SysInspectorは、お使いのコンピュータを徹底的に検査し、収集されたデータを総合的に表示するアプリケーションです。インストールされているドライバやアプリケーション、ネットワーク接続、重要なレジストリエントリなどの情報は、疑わしいシステム動作（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によるものなど）の調査に役立てることができます。

5.5.1 ESET SysInspectorの概要

ESET SysInspectorにアクセスする方法は2通りあります。ESET Securityソリューションの統合バージョンを使用するか、またはESETのWebサイトから無償のスタンドアロンバージョン（SysInspector.exe）をダウンロードします。どちらのバージョンも機能的には同じであり、同一のプログラムコントロールをもっています。唯一の相違は、出力の管理の仕方にあります。スタンドアロンバージョンまたは統合バージョンのどちらでも、システムスナップショットを.xmlファイルにエクスポートし、ディスクに保存することができます。ただし、統合バージョンでは、[ツール]>[ESET SysInspector] を使って、システムスナップショットを直接保存することもできます（ESET Remote Administratorを除く）。

ESET SysInspectorによるコンピュータの検査には少々時間がかかります。ご使用のハードウェアの設定、オペレーティングシステム、およびコンピュータにインストールされているアプリケーションの数に応じて、10秒から数分かかると思われます。

5.5.1.1 ESET SysInspectorの起動

ESETのWebサイトからダウンロードしたSysInspector.exe実行可能ファイルを実行するだけで、ESET SysInspectorを起動できます。

アプリケーションがシステムを検査している間、お待ちください。お使いのハードウェアと収集されるデータによって異なりますが、これには数分間かかる可能性があります。

5.5.2 ユーザーインタフェースとアプリケーションの使用

メインウィンドウは、使いやすいように4つの主要セクションに分かれています。プログラムのコントロールはメインウィンドウの上部、ナビゲーションウィンドウは左側、説明ウィンドウは中央右側、詳細ウィンドウはメインウィンドウの下部右側にそれぞれ配置されています。ログ状況のセクションには、ログの基本パラメータ（使用されているフィルタ、フィルタタイプ、ログは比較の結果かどうかなど）が一覧表示されます。

5.5.2.1 プログラムコントロール

ここでは、ESET SysInspectorで使用可能なすべてのプログラムコントロールについて説明します。

ファイル

[ファイル] をクリックすると、後で調査するために現在のシステムステータスを保存したり、以前に保存されたログを開いたりできます。公開を目的としている場合は、[送信に適した形式] でログを生成することをお勧めします。この形式のログでは、機密情報（現在のユーザ名、コンピュータ名、ドメイン名、現在のユーザ特権、環境変数など）は省かれます。

NOTE

以前に保存したESET SysInspectorレポートをメインウィンドウにドラッグアンドドロップするだけで、それらのレポートを開くことができます。

ツリー

すべてのノードを展開したり閉じたりできます。また、選択したセクションをサービススクリプトにエクスポートすることもできます。

リスト
プログラム内でのナビゲーションをより容易にするための機能のほか、オンラインでの情報検索などの他のさまざまな機能が含まれます。

ヘルプ
アプリケーションとその機能に関する情報が含まれます。

詳細
この設定は、メインウィンドウに表示される情報に影響し、情報を処理しやすくなります。"基本"モードでは、システム内の一般的な問題に対する解決策を見つけるための情報にアクセスできます。"中間"モードでは、あまり一般的でない詳細が表示されます。"完全"モードのESET SysInspectorでは、極めて具体的な問題の解決に必要な全ての情報が表示されます。

アイテムのフィルタリング
アイテムのフィルタリングは、システム内の疑わしいファイルまたはレジストリエントリを見つけるために最もよく使用される方法です。スライダを調整することで、リスクレベルによってアイテムをフィルタできます。スライダーを最左端（リスクレベル1）にすると、全ての項目が表示されます。スライダを右に動かすと、現在のリスクレベルより低いリスクレベルのアイテムが除外され、表示されたレベルのアイテムよりも疑わしいアイテムのみが表示されます。スライダーを最右端にすると、既知の有害な項目のみが表示されます。

リスク6～9に分類されている全ての項目には、セキュリティリスクが生じる可能性があります。ESETの何らかのセキュリティソリューションを使用していない場合は、ESET SysInspectorでそのようなアイテムが見つかった後、ESET Online Scannerでシステムを検査することをお勧めします。ESET Online Scannerは無料のサービスです。

▸▸▸ NOTE

注意:項目のリスクレベルは、項目の色とリスクレベルのスライダーの色を比べることにより迅速に判別できます。

検索
[検索] を使用して、特定のアイテムを、その名前または名前の一部によって簡単に見つけることができます。検索要求の結果は、説明ウィンドウに表示されます。

戻る
左矢印または右矢印をクリックすることで、説明ウィンドウ内で前に表示された情報に戻ることができます。左矢印と右矢印をクリックする代わりに、それぞれBackSpaceキーとスペースキーを使用できます。

ステータスセクション
ナビゲーションウィンドウ内の現在のノードを表示します。

重要

赤で表示されているアイテムは、プログラムによって潜在的な危険性があるとマークされた不明アイテムです。項目が赤で表示されている場合でも、ファイルの削除が可能であることを自動的に意味するわけではありません。削除する前に、ファイルが本当に危険かどうか、または不要かどうかを確認してください。

5.5.2.2 ESET SysInspectorにおけるナビゲーション

ESET SysInspectorでは、さまざまな種類の情報が、ノードと呼ばれる複数の基本セクションに分けられています。サブノードがある場合は、各ノードをサブノードに展開して追加情報を確認することができます。ノードの展開/折りたたみを行うには、ノードの名前をダブルクリックするか、またはノードの名前の横にある⊞または⊟をクリックします。ナビゲーションウィンドウでノードおよびサブノードのツリー構造内を参照すると、説明ウィンドウに各ノードのさまざまな詳細情報が表示されます。説明ウィンドウでアイテムを参照すると、各アイテムの追加の詳細情報が詳細ウィンドウに表示されます。

ナビゲーションウィンドウのメインノード、および説明ウィンドウと詳細ウィンドウの関連情報についての説明を次に示します。

実行中のプロセス
このノードには、ログの生成時に実行されていたアプリケーションとプロセスに関する情報が含まれます。説明ウィンドウには、プロセスによって使用されたダイナミックライブラリとシステム内のそれらのライブラリの場所、アプリケーションベンダの名前、ファイルのリスクレベルなど、各プロセスに関する追加の詳細情報が表示されます。詳細ウィンドウには、ファイルサイズやハッシュなど、説明ウィンドウで選択した項目に関する追加情報が表示されます。

››› NOTE

オペレーティングシステムは、複数の重要なカーネルコンポーネントで構成されます。これらのコンポーネントは、毎日24時間稼動し、他のユーザーアプリケーションに対して基本的かつ重要な機能を提供します。場合によっては、ESET SysInspectorツールに表示されるそれらのプロセスのファイルパスが¥??¥で始まることもあります。これらの記号はプロセスの起動前最適化を可能にするもので、システムにとって安全です。

ネットワーク接続
説明ウィンドウには、ナビゲーションウィンドウで選択したプロトコル（TCPまたはUDP）を使用してネットワーク経由で通信するプロセスとアプリケーションのリストが、アプリケーションの接続先となるリモートアドレスと共に表示されます。DNSサーバのIPアドレスをチェックすることもできます。

詳細ウィンドウには、ファイルサイズやハッシュなど、説明ウィンドウで選択した項目に関する追加情報が表示されます。

重要なレジストリエントリ
スタートアッププログラムやブラウザヘルパオブジェクト（BHO）を指定するものなど、システムに関するさまざまな問題に関連することが多い選択されたレジストリエントリのリストが表示されます。
説明ウィンドウには、特定のレジストリエントリにどのファイルが関連しているかが示されます。詳細ウィンドウでは、追加の詳細情報を確認できます。

サービス
説明ウィンドウには、Windowsサービスとして登録されているファイルのリストが表示されます。詳細ウィンドウで、サービスを開始するための設定方法と、ファイルに関する特定の詳細を確認できます。

ドライバ
システムにインストールされているドライバのリストです。

重要なファイル
説明ウィンドウには、Microsoft Windowsオペレーティングシステムに関連する重要なファイルの内容が表示されます。

システムスケジューラタスク
Winodwsタスクスケジューラによって指定の時刻/間隔で起動されるタスクのリストを示します。

システム情報
ハードウェアとソフトウェアに関する詳細情報と、set環境変数、ユーザー権限、およびシステムイベントログに関する情報を表示します。

ファイルの詳細
[プログラムファイル]フォルダ内の重要なシステムファイルおよびファイルのリストです。ファイル固有の追加情報は、説明ウィンドウと詳細ウィンドウに表示されます。

バージョン情報
ESET SysInspectorのバージョンに関する情報とプログラムモジュールのリストです。

キーボードショートカット

ESET SysInspectorで使用できるショートカットキーは、次のとおりです。

[ファイル]

Ctrl+O	既存のログを開きます。
Ctrl+S	作成したログを保存します。

生成

Ctrl+G	コンピュータの標準状態のスナップショットを生成します。
Ctrl+H	機密情報もログ記録できるコンピュータの状態のスナップショットを生成します。

項目のフィルタリング

1,O	良好、リスクレベル1～9の項目が表示されます。
2	良好、リスクレベル2～9の項目が表示されます。
3	良好、リスクレベル3～9の項目が表示されます。
4,U	不明、リスクレベル4～9の項目が表示されます。
5	不明、リスクレベル5～9の項目が表示されます。
6	不明、リスクレベル6～9の項目が表示されます。
7,B	危険、リスクレベル7～9の項目が表示されます。
8	危険、リスクレベル8～9の項目が表示されます。
9	危険、リスクレベル9の項目が表示されます。
-	リスクレベルを下げます。
+	リスクレベルを上げます。
Ctrl+9	フィルタリングモード、同等以上のレベル
Ctrl+0	フィルタリングモード、同等レベルのみ

表示

Ctrl+5	ベンダによる表示、全てのベンダ
Ctrl+6	ベンダによる表示、Microsoftのみ
Ctrl+7	ベンダによる表示、他の全てのベンダ
Ctrl+3	完全な詳細を表示します。
Ctrl+2	中程度の詳細を表示します。
Ctrl+1	基本的な表示です。
BackSpace	1ステップ戻ります。
Space	1ステップ進みます。
Ctrl+W	ツリーを展開します。
Ctrl+Q	ツリーを折りたたみます。

その他のコントロール

Ctrl+T	検索結果で選択した後、項目の元の場所に移動します。
Ctrl+P	項目についての基本情報を表示します。
Ctrl+A	項目についての完全情報を表示します。
Ctrl+C	現在の項目のツリーをコピーします。
Ctrl+X	項目をコピーします。
Ctrl+B	選択したファイルについての情報をインターネット上で検索します。
Ctrl+L	選択したファイルが格納されているフォルダを開きます。
Ctrl+R	該当するエントリをレジストリエディタで開きます。
Ctrl+Z	ファイルまでのパスをコピーします（項目がファイルに関連付けられている場合）。
Ctrl+F	検索フィールドに切り替えます。
Ctrl+D	検索結果を閉じます。
Ctrl+E	サービススクリプトを実行します。

比較

Ctrl+Alt+O	比較元と比較先のログを開きます。
Ctrl+Alt+R	比較を取り消します。
Ctrl+Alt+1	全ての項目を表示します。
Ctrl+Alt+2	追加された項目のみを表示します。ログには現在のログにある項目が表示されます。
Ctrl+Alt+3	削除された項目のみを表示します。ログには前回のログにある項目が表示されます。
Ctrl+Alt+4	置き換えられた項目のみを表示します（ファイルも含まれます）。
Ctrl+Alt+5	ログ間の相違のみを表示します。
Ctrl+Alt+C	比較結果を表示します。
Ctrl+Alt+N	現在のログを表示します。
Ctrl+Alt+P	前回のログを開きます。

その他

F1	ヘルプを表示します。
Alt+F4	プログラムを閉じます。
Alt+Shift+F4	確認せずにプログラムを閉じます。
Ctrl+I	統計をログに記録します。

5.5.2.3 ログの比較

比較機能を使用すると、ユーザーは既存の 2つのログを比較できます。この機能により、両方のログで共通していない一連のアイテムが表示されます。システムの変更を追跡するには、この機能が適しています。これは、悪意のあるコードの活動を検出するのに有用なツールです。

起動後、新しいログが作成され、新しいウィンドウに表示されます。[ファイル] > [ログの保存] に移動して、ログをファイルに保存します。これで、ログファイルを後で開いて表示できるようになります。既存のログを開くには、[ファイル] -> [ログを開く] メニューを使用します。ESET SysInspectorのメインプログラムウィンドウで一度に表示できるログは1つです。

2つのログの比較には、現在アクティブなログと、ファイルに保存されているログを表示できるという利点があります。ログを比較するには、[ファイル] > [ログの比較] オプションを使用し、[ファイルの選択] を選択します。プログラムのメインウィンドウで、選択したログがアクティブなログと比較されます。比較ログには、2つのログの相違のみが表示されます。

NOTE

2つのログファイルを比較する場合は、[ファイル]->[ログの保存] を選択し、ログをZIPファイルとして保存します。これで、両方のファイルが保存されます。後でそのファイルを開くと、保存されているログが自動的に比較されます。

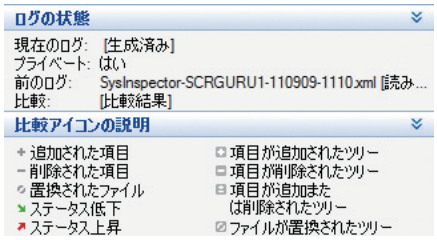
表示されたアイテムの横に、比較対象のログの相違を示す記号がESET SysInspectorによって表示されます。

-のマークの付いた項目はアクティブログのみに見つかり、開かれた比較ログには見つからなかったものです。
+が付いているアイテムは、開かれているログにのみ存在し、アクティブなログには存在しないものです。

項目の横に表示される全ての記号について次に説明します。

- +以前のログには存在しない新しい値
- 新しい値を含むツリー構造セクション
- -以前のログにのみ存在する、削除された値
- 削除された値を含むツリー構造セクション
- 変更されている値/ファイル
- 変更された値/ファイルを含むツリー構造セクション
- リスクレベルが、以前のログよりも低下している
- リスクレベルが、以前のログよりも上昇している

左下隅に表示される説明セクションでは、全ての記号が説明され、比較対象のログの名前も表示されます。



比較ログはいずれもファイルに保存して、後で開くことができます。

例
システムに関する初期情報を記録したログを生成して、previous.xmlという名前のファイルに保存します。システムに変更を行った後、ESET SysInspectorを開いて、新しいログを生成します。current.xmlという名前のファイルにログを保存します。

これら2つのログの相違を追跡するには、[ファイル] > [ログの比較] に移動します。2つのログの相違を示した比較ログが作成されます。

次のコマンドラインオプションを使用した場合も同様の結果が得られます。
SysIsnpector.exe current.xml previous.xml

5.5.3 コマンドラインパラメーター

ESET SysInspectorでは、次のパラメータを使用してコマンドラインからレポートを生成できます。

/gen	GUIを実行せずにコマンドラインから直接ログを生成します。
/privacy	機密情報を除外してログを生成します。
/zip	生成されたログを圧縮ファイルとして直接ディスクに格納します。
/silent	ログ生成の進捗状況バーは表示されません。
/help,/?	コマンドラインパラメータに関する情報を表示します。

例
特定のログを直接ブラウザに読み込むには、次のように指定します。SysInspector.exe "c: ¥clientlog.xml"
ログを現在の場所に生成するには、次のように指定します。SysInspector.exe/gen
ログを特定のフォルダに生成するには、次のように指定します。SysInspector.exe/gen="c: ¥folder¥"
ログを特定のファイル/場所に生成するには、次のように指定します。SysInspector.exe/gen="c:¥folder¥mynewlog.xml"
ログを、機密情報を除外して直接圧縮ファイルとして生成するには、次のように指定します。SysInspector.exe/gen="c:¥mynewlog.zip"/privacy/zip
2つのログを比較するには、次のように指定します。SysInspector.exe"current.xml" "original.xml"

▸▸▸ NOTE

ファイル/フォルダの名前に空白が含まれている場合は、名前を引用符(逆コンマ)で囲む必要があります。

5.5.4 サービススクリプト

サービススクリプトは、ESET SysInspectorを使用するユーザーがシステムから不要なオブジェクトを簡単に削除できるよう手助けをするツールです。

サービススクリプトを使用すると、ユーザーはESET SysInspectorログの全体、または選択した部分をエクスポートできます。エクスポートした後、不要なオブジェクトに削除対象のマークを付けることができます。その後、修正したログを実行して、マークを付けたオブジェクトを削除できます。

サービススクリプトは、過去にシステムの問題を診断した経験のある上級ユーザー向けです。そうではないユーザが変更を行うと、オペレーティングシステムの障害を引き起こす可能性があります。

例
コンピュータが、ご使用のウイルス対策プログラムでは検出されないウイルスに感染している疑いがある場合は、次の手順を実行してください。

- ●ESET SysInspectorを実行して、システムスナップショットを新規に生成します。
- ●ツリー構造の左側のセクションで最初の項目を選択して、Ctrlキーを押しながら最後の項目を選択し、全ての項目をマークします。
- ●選択したオブジェクトを右クリックし、[選択したセクションをサービススクリプトにエクスポート] コンテキストメニューオプションを選択します。
- ●選択したオブジェクトが新しいログにエクスポートされます。
- ●これは、手順全体の中で最も重要なステップです。新しいログを開いて、削除対象のすべてのオブジェクトの-属性を+に変更します。オペレーティングシステムの重要なファイルやオブジェクトにマークが付いていないことを確認してください。
- ●ESET SysInspectorを起動し、[ファイル] > [サービススクリプトの実行] をクリックして、スクリプトへのパスを入力します。
- ● [OK] をクリックしてスクリプトを実行します。

5.5.4.1 サービススクリプトの生成

サービススクリプトを生成するには、ESET SysInspectorのメインウィンドウで、メニューツリー(左ペイン)の任意のアイテムを右クリックします。コンテキストメニューで、[すべてのセクションをサービススクリプトにエクスポート] オプションまたは [選択したセクションをサービススクリプトにエクスポート] オプションを選択します。
注意:2つのログを比較しているときは、サービススクリプトをエクスポートすることはできません。

5.5.4.2 サービススクリプトの構造

スクリプトのヘッダの最初の行には、エンジンバージョン(ev)、GUIバージョン(gv)、およびログバージョン(lv)に関する情報が記載されています。このデータを使用して、スクリプトを生成した.xmlファイル内の変更内容を追跡し、実行中に不整合が発生するのを防ぐことができます。スクリプトのこの部分は変更しないでください。

ファイルの残りの部分は、複数のセクションに分かれており、そこでアイテムを編集する(つまり、アイテムがスクリプトによって処理されることを示す)ことができます。アイテムの前にある"-"記号を"+"記号に置き換えることで、アイテムが処理対象としてマークされます。スクリプト内の各セクションは、空の行によって区切られています。各セクションには、番号とタイトルが付けられています。

01）Running processes（実行中のプロセス）:
このセクションには、システム内で実行されているすべてのプロセスのリストが含まれます。各プロセスは、そのUNCパスと、それに続くアスタリスク（*）で囲まれたCRC16ハッシュコードによって識別されます。

例:
01）Running processes:- ¥SystemRoot ¥System32 ¥smss.exe*4725*
-C: ¥Windows ¥system32 ¥svchost.exe*FD08*
+ C:¥Windows ¥system32 ¥module32.exe*CF8A* [...]
この例では、プロセスmodule32.exeが選択されています（"+"記号でマークされています）。このプロセスは、スクリプトの実行時に終了します。

02）Loaded modules（読み込まれたモジュール）:
このセクションには、現在使用されているシステムモジュールのリストが示されます。

例:
02）Loaded modules:
-c: ¥windows ¥system32 ¥svchost.exe
-c: ¥windows ¥system32 ¥kernel32.dll
+ c: ¥windows ¥system32 ¥khbekhb.dll
-c: ¥windows ¥system32 ¥advapi32.dll [...]
この例では、モジュール khbekhb.dllが"+"でマークされています。スクリプトが実行されると、この特定のモジュールを使用しているプロセスが認識され、それらが終了されます。
03）TCP connections（TCP接続）:

このセクションには、既存のTCP接続に関する情報が含まれます。

例:
03）TCP connections:
-Active connection:127.0.0.1:30606->127.0.0.1:55320, owner:ekrn.exe
-Active connection:127.0.0.1:50007->127.0.0.1:50006,
-Active connection:127.0.0.1:55320->127.0.0.1:30606, owner:OUTLOOK.EXE
-Listening on*, port 135（epmap）, owner: svchost.exe
+ Listening on*, port 2401, owner: fservice.exe Listening on*, port 445（microsoft-ds）, owner:System
[...]

スクリプトを実行すると、マークされたTCP接続内のソケットの所有者が見つけられ、ソケットが停止されて、システムリソースが解放されます。

04) UDP endpoints (UDPエンドポイント):
このセクションには、既存のUDPエンドポイントに関する情報が含まれます。

例:
04) UDP endpoints:-0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
-0.0.0.0, port 4500 (ipsec-msft)
-0.0.0.0, port 500 (isakmp)
[...]

スクリプトが実行されると、マークされたUDPエンドポイントのソケットの所有者が分離され、ソケットが停止されます。

05) DNS server entries (DNSサーバ関連のエントリ):
このセクションには、現在のDNSサーバのコンフィグレーションに関する情報が含まれます。

例:
05) DNS server entries:
+ 204.74.105.85
-172.16.152.2
[...]

スクリプトが実行されると、マークされたDNSサーバエントリが削除されます。

06) Important registry entries (重要なレジストリエントリ):
このセクションには、重要なレジストリエントリに関する情報が含まれます。

例:
06) Important registry entries:
* Category: Standard Autostart (3 items)
HKLM ¥SOFTWARE ¥Microsoft ¥Windows ¥CurrentVersion ¥Run
-HotKeysCmds = C: ¥Windows ¥system32 ¥hkcmd.exe-IgfxTray = C: ¥Windows ¥system32vigfxtray.exe
HKCU¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run-Google Update = "C:¥Users¥antoniak¥AppData¥Local¥Google¥Update¥GoogleUpdate.exe" ¥c
* Category: Internet Explorer (7 items) HKLM¥Software¥Microsoft¥Internet Explorer¥Main
+Default_Page_URL = http://thatcrack.com¥ [...]

スクリプトが実行されると、マークされたエントリが削除されるか、0バイト値に縮小されるか、またはその既定値にリセットされます。特定のエントリに適用されるアクションは、エントリのカテゴリと特定のレジストリのキー値によって異なります。

07) Services (サービス):
このセクションには、システム内の登録済みサービスのリストが示されます。

例:
07) Services:
-Name:Andrea ADI Filters Service, exe path:c:¥windows¥system32¥aeadisrv.exe, state:Running, startup:Automatic
-Name:Application Experience Service, exe path:c:¥windows¥system32¥aelupsvc.dll, state:Running, startup:Automatic
-Name:Application Layer Gateway Service, exe path:c:¥windows¥system32¥alg.exe, state:Stopped, startup:Manual
[...]

スクリプトが実行されると、マークされたサービスとそれらの依存サービスは停止され、アンインストールされます。

08) Drivers (ドライバ):
このセクションには、インストール済みのドライバのリストが示されます。

例:
08) Drivers:
-Name:Microsoft ACPI Driver, exe path: c:¥windows¥system32¥drivers¥acpi.sys, state:Running, startup:Boot
-Name:ADI UAA Function Driver for High Definition Audio Service, exe path:c:¥windows¥system32¥drivers¥adihdaud.sys, state:Running, startup:Manual
[...]

スクリプトを実行すると、選択したドライバは停止します。ドライバによっては、停止するようになっていないことがあります。

09) Critical files (不可欠なファイル):
このセクションには、オペレーティングシステムが正常に機能するために不可欠なファイルに関する情報を記載しています。

例:
09) Critical files:
*File: win.ini
- [fonts]
- [extensions]
- [files]
-MAPI=1
[...]
*File:system.ini
- [386Enh]
-woafont=dosapp.fon
-EGA80WOA.FON=EGA80WOA.FON
[...]
*File: hosts
-127.0.0.1 localhost
-::1 localhost
[...]

選択したアイテムは、削除されるか、またはその元の値にリセットされます。

5.5.4.3 サービススクリプトの実行

目的のアイテムをすべてマークし、スクリプトを保存して閉じます。[ファイル] メニューの [サービススクリプトの実行] オプションを選択して、ESET SysInspectorのメインウィンドウから、編集したスクリプトを直接実行します。スクリプトを起動すると、次のような内容のメッセージが表示されます。「サービススクリプト"% Scriptname % "を実行しますか?」これを確認すると、実行しようとしているサービススクリプトが署名されていないという別の警告が表示される場合があります。[実行] をクリックしてスクリプトを起動します。
ダイアログウィンドウに、スクリプトが正常に実行されたことが示されます。
スクリプトの一部だけが処理された可能性がある場合、次のような内容のメッセージがダイアログウィンドウに表示されます。「サービススクリプトは部分的に実行されました。エラーレポートを表示しますか?」 [はい] を選択して、実行されなかった操作が記載されている複雑なエラーレポートを表示します。
スクリプトが認識されなかった可能性がある場合、次のような内容のメッセージがダイアログウィンドウに表示されます。「選択したサービススクリプトは署名されていません。署名されていない不明なスクリプトを実行すると、コンピュータのデータに深刻なダメージを与えるおそれがあります。スクリプトを実行し、アクションを実行してもよろしいですか?」これは、スクリプト内の不整合 (見出しが損傷している、セクションタイトルが壊れている、セクション間の空の列が失われているなど) によって引き起こされた可能性があります。スクリプトファイルを再度開いてスクリプト内のエラーを修正するか、または新しいサービススクリプトを作成します。

5.5.5 FAQ

01 ESET SysInspectorを実行するには管理者特権が必要ですか？

ESET SysInspectorを実行するには管理者特権は必要ありませんが、収集される情報の中には管理者アカウントからのみアクセスできるものもあります。標準ユーザーまたは制限付きユーザーが実行した場合は、動作環境に関する情報の収集量は少なくなります。

02 ESET SysInspectorではログファイルが作成されますか？

ESET SysInspectorでは、コンピュータの設定のログファイルを作成できます。このログファイルを保存するには、メインメニューの［ファイル］>［ログを保存］を選択します。ログはXML形式で保存されます。既定では、ファイルは% USERPROFILE%¥My Documents¥ディレクトリに保存されます。ファイルの命名規則は、SysInpsector-%COMPUTERNAME%-YYMMDD-HHMM.XMLとなります。ログファイルを保存する前に、そのファイルの場所と名前を、必要に応じて別のものに変更できます。

03 ESET SysInspectorのログファイルを表示するにはどうしたらいいですか？

ESET SysInspectorで作成されたログファイルを表示するには、プログラムを実行し、メインメニューで［ファイル］>［ログを開く］を選択します。ログファイルをESET SysInspectorアプリケーションにドラッグアンドドロップすることもできます。ESET SysInspectorのログファイルを頻繁に表示する必要がある場合は、デスクトップにSYSINSPECTOR.EXEファイルへのショートカットを作成することをお勧めします。こうしておくと、ログファイルをこのショートカットにドラッグアンドドロップして表示することができます。セキュリティ上の理由で、Windows VistaとWindows7では異なるセキュリティアクセス許可を持つウィンドウ間でのドラッグアンドドロップが許可されない場合があります。

04 ログファイル形式の仕様は使用できますか？SDKは使用できますか？

現時点では、プログラムは開発途中であるため、ログファイルの仕様やSDKは使用できません。プログラムのリリース後、カスタマのフィードバックと要望に基づいて提供する可能性があります。

05 ESET SysInspectorでは、特定のオブジェクトによってもたらされるリスクはどのように評価されますか？

多くの場合、ESET SysInspectorは、各オブジェクトの特性を検証して悪意のある活動である可能性を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）にリスクレベルを割り当てます。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1-良好（緑）～9-危険（赤）のリスクレベルが割り当てられます。左側のナビゲーションペインでは、オブジェクトが持つ最大リスクレベルを基にセクションが色分けされます。

06 リスクレベル"6-不明（赤）"は、オブジェクトが危険であることを意味しますか？

ESET SysInspectorの評価により、オブジェクトが悪意のあるものであることが確定されるわけではありません。セキュリティの専門家による判断が必要です。ESET SysInspectorは、セキュリティの専門家が、システムのどのオブジェクトについて動作が異常でないかどうかを詳細に検証する必要があるかを、迅速に判断できるように設計されています。

07 ESET SysInspectorの実行時にインターネットに接続するのはなぜですか？

多くのアプリケーションと同様に、ESET SysInspectorには、このソフトウェアがESETから発行されたものであって、改変されていないことを確認できるよう、"証明書"のデジタル署名が付けられています。証明書を検証するために、オペレーティングシステムは証明機関にソフトウェア発行元を問い合わせて確認します。これは、Microsoft Windows下で動作する全てのデジタル署名プログラムの標準的な動作です。

08 アンチステルス技術とはどのようなものですか？

アンチステルス技術は、ルートキットを効率的に検出するためのものです。
ルートキットとして動作する悪意のあるコードによってシステムが攻撃を受けると、ユーザーはデータの喪失や盗難などの被害を受けます。専用のルートキット対策ツールが無ければ、ルートキットの検出はほとんど不可能です。

09 "MSによって署名済み"としてマークされたファイルが、異なる"会社名"エントリを同時に持つことがあるのはなぜですか？

実行可能ファイルのデジタル署名を識別するときに、ESET SysInspectorは、まずファイルに埋め込まれたデジタル署名をチェックします。デジタル署名が見つかったら、その情報を使ってファイルが検証されます。デジタル署名が見つからない場合、ESIは、処理する実行可能ファイルに関する情報を収めた対応するCATファイル（セキュリティカタログ-% systemroot%¥system32¥catroot）の検索を開始します。該当する CATファイルが見つかると、そのCATファイルのデジタル署名が実行可能ファイルの検証プロセスに適用されます。
"Signed by MS"というマークのあるファイルが、異なる"CompanyName"エントリを持つ場合があるのはこのためです。

例:
Windows 2000では、C:¥Program Files¥Windows NTにハイパーターミナルアプリケーションがあります。このアプリケーションの主要な実行可能ファイルはデジタル署名されていませんが、ESET SysInspectorでは、そのファイルをMicrosoftによって署名されたファイルとマークします。この理由は、C:¥WINNT¥system32¥CatRoot¥{F750E6C3-38EE-11D1-85E5-00C04FC295EE}¥sp4.catにおける参照が C:¥Program Files¥Windows NT¥hypertrm.exe（ハイパーターミナルアプリケーションの主要な実行可能ファイル）をポイントし、sp4.catがMicrosoftによってデジタル署名されているためです。

5.5.6 ESET Endpoint Securityの一部としてのESET SysInspector

ESET SysInspectorセクションをESET Endpoint Securityで開くには、[ツール] > [ESET SysInspector] をクリックします。ESET SysInspectorウィンドウでの管理システムは、コンピュータ検査ログまたはスケジュールされたタスクの管理システムとほぼ同じです。システムのスナップショットを伴う全ての操作（作成、表示、比較、削除、エクスポート）には、1回または2回のクリックでアクセスできます。

ESET SysInspectorウィンドウには、作成時刻、短いコメント、スナップショットを作成したユーザの名前、およびスナップショットの状態など、作成されたスナップショットに関する基本的な情報が表示されます。

スナップショットを比較、作成、または削除するには、ESET SysInspectorのウィンドウでスナップショットのリストの下にある対応するボタンを使用します。これらのオプションはコンテキストメニューでも使用できます。選択したシステムスナップショットを表示するには、[表示] コンテキストメニューオプションを使用します。選択したスナップショットをファイルにエクスポートするには、スナップショットを右クリックして [エクスポート...] を選択します。

次に、使用可能なオプションについて詳しく説明します。

- [比較] ―既存の2つのログを比較できます。現在のログと以前のログの間の変更を追跡するには、これが適切です。このオプションを有効にするには、比較する2つのスナップショットを選択する必要があります。
- [作成...] ―新しいレコードを作成します。この操作を実行するには、まずレコードに関する短いコメントを入力する必要があります。現在生成されているスナップショットの作成の進行状況を確認するには、[状態] 列を参照してください。完了したスナップショットはすべて、[作成済み] の状態になります。
- [削除/すべて削除] ―リストからエントリを削除します。
- [エクスポート...] ―選択したエントリをXMLファイル（または圧縮バージョン）で保存します。

5.6 ESET SysRescue

ESET SysRescueは、ESET Securityソリューションのうちの1つ(ESET NOD32アンチウイルス、ESET Smart Security、またはサーバ指向製品のいずれか)を収めた起動可能ディスクを作成するためのユーティリティです。ESET SysRescueの主な利点は、ESET Securityソリューションがホストオペレーティングシステムから独立して稼動する一方で、ディスクおよびファイルシステム全体に直接アクセスできることにあります。これにより、オペレーティングシステムが実行中の場合など、通常は削除できないウイルスを削除できます。

5.6.1 レスキューCDの作成方法

ESET SysRescueウィザードを開始するには、[スタート]>[プログラム]>[ESET]>[ESET Endpoint Security]>[ESET SysRescue]をクリックします。

まず、Windows AIKとブートメディアの作成に適したデバイスがあるかどうかがチェックされます。コンピュータにWindows AIKがインストールされていない場合(または破損していたり正しくインストールされていない場合)、インストールするオプションまたはWindows AIKフォルダへのパスを入力するオプションがウィザードに表示されます(http://go.eset. eu/AIK)。

NOTE

Windows AIKはサイズが1GBを超えるので、スムーズにダウンロードするには高速インターネット接続が必要です。

次のステップでは、ESET SysRescueを保存する対象のメディアを選択します。

5.6.2 対象の選択

CD/DVD/USBに加えて、ISOファイルにESET SysRescueを保存することもできます。後で、ISOイメージをCD/DVDに書き込んだり、その他の方法で(VMwareやVirtualBoxのような仮想環境などで)使用することができます。

対象メディアにUSBを選択した場合に、特定のコンピュータでブートが行われないことがあります。一部のBIOSバージョンでは、BIOSに関する問題が報告されることがあります。ブートマネージャの通信(Windows Vistaなど)と起動処理が終了し、次のエラーメッセージが表示されます。

ファイル:¥boot¥bcd
状態:0xc000000e
情報:ブート設定データの読み込み時にエラーが発生しました

このメッセージが表示された場合、USBメディアでなくCDを選択することをお勧めします。

5.6.3 設定

ESET SysRescueの作成を開始する前に、インストールウィザードでは、コンパイルパラメータがESET SysRescueウィザードの最終ステップで表示されます。それらのパラメータを変更するには、[変更...] ボタンをクリックします。使用可能なオプションは次のとおりです。

●フォルダ
●ESETアンチウイルス
●詳細
●インターネットプロトコル
●起動可能なUSBデバイス（対象のUSBデバイスの選択時）
●書き込み（対象のCD/DVDドライブの選択時）

MSIインストールパッケージを指定していなかったり、コンピュータにESET Securityソリューションをインストールしていないと、[作成] ボタンは使用できません。インストールパッケージを選択するには、[変更] ボタンをクリックして、[ESETアンチウイルス] タブに移動します。ユーザ名とパスワードを入力しなかった場合も（[変更] > [ESETアンチウイルス]）、[作成] ボタンは無効になります。

5.6.3.1 フォルダー

一時フォルダーは、ESET SysRescueのコンパイル時に必要なファイルの作業ディレクトリです。

ISOフォルダは、コンパイルの完了後に、生成されたISOファイルが保存されるフォルダです。

このタブには、全てのローカルドライブとマッピングされているネットワークドライブ、および使用可能な空き領域がリストされます。表示されているフォルダの一部が、空き領域の不十分なドライブにある場合、十分な空き領域のある別のドライブを選択することをお勧めします。ディスクの空き領域が不足していると、コンパイルが途中で終了する場合があります。

外部アプリケーション—ESET SysRescueメディアから起動後に実行またはインストールする追加プログラムを指定できます。

外部アプリケーションを含める—外部プログラムをESET SysRescueのコンパイルに追加できます。
選択されたフォルダ—ESET SysRescueディスクに追加するプログラムを格納するフォルダです。

5.6.3.2 ESETアンチウイルス

ESET SysRescue CDを作成する際、コンパイラが使用するESETファイルのソースとして、2種類を選択できます

ESS/EAVフォルダ—コンピュータ上のESET Securityソリューションのインストール先フォルダに含まれる既存ファイル。

[MSIファイル]—MSIインストーラに含まれているファイルが使用されます。
次に、選択によっては、(Nup)ファイルの場所を更新できます。通常、既定オプション[ESS/EAVフォルダ/MSIファイル]が設定されているはずです。ウイルス定義データベースの古いバージョンまたは新しいバージョンを使用するためといった場合によっては、カスタムの[アップデートフォルダ]を選択してもかまいません。

ユーザ名とパスワードのソースとして、次の2つのうちのどちらかを使用できます。

インストール済みのESS/EAV—ユーザー名とパスワードは、現在インストールされているESET Securityソリューションからコピーされます。

ユーザー指定—対応するテキストボックスに入力されたユーザー名とパスワードが使用されます。

▸▸▸ NOTE

ESET SysRescue CD上のESET Securityソリューションは、インターネットからか、またはESET SysRescue CDが実行されているコンピュータにインストールされているESET Securityソリューションからアップデートされます。

5.6.3.3 詳細設定

[詳細]タブでは、コンピュータのメモリ容量に従ってESET SysRescue CDを最適化できます。[576MB以上]を選択すると、CDのコンテンツがシステムメモリ(RAM)に書き込まれます。[576MB未満]を選択すると、WinPEが実行されるときに常にRecovery CDにアクセスされます。

[外部ドライバ]セクションでは、特定のハードウェア用のドライバ(通常はネットワークアダプタ)を挿入できます。WinPEは、幅広いハードウェアをサポートするWindows Vista SP1をベースにしていますが、時にはハードウェアが認識されないこともあります。そのようなときは、ドライバを手動で追加する必要があります。ESET SysRescueのコンパイルにドライバを追加するには、手動([追加]ボタン)と自動([自動検索]ボタン)の2つの方法があります。手動で追加する場合は、該当する.infファイルへのパスを選択する必要があります(適用可能な*.sysファイルがそのフォルダ内になければなりません)。自動的に追加する場合は、指定のコンピュータのオペレーティングシステムでドライバが自動的に検索されます。自動追加は、ESET SysRescue CDの作成先コンピュータで使用しているのと同じネットワークアダプタを備えたコンピュータで、ESET SysRescueを使用する場合にのみ使うことをお勧めします。作成時にESET SysRescueドライバがコンパイルに組み込まれるため、ユーザが後で検索する必要はありません。

5.6.3.4 インターネットプロトコル

ここでは、ESET SysRescueの後で、基本ネットワーク情報を設定し、事前定義接続を設定することができます。

IPアドレスをDHCP（動的ホスト構成プロトコル）サーバーから自動的に取得するには、[自動的にIPアドレスを取得する] を選択します。

あるいは、ネットワーク接続で、手動で指定したIPアドレス（静的IPアドレスとも呼ばれる）を使用することもできます。適切なIP設定を構成するには、[カスタム] を選択します。このオプションを選択する場合、[IPアドレス] を指定し、LANおよび高速インターネット接続の場合は [サブネットマスク] を指定する必要があります。[優先DNSサーバー] および [代替DNSサーバー] に、プライマリおよびセカンダリのDNSサーバーアドレスを入力します。

5.6.3.5 起動可能なUSBデバイス

対象のメディアとしてUSBデバイスを選択した場合、[起動可能なUSBデバイス] タブで、使用可能なUSBデバイスのいずれかを選択できます（複数のUSBデバイスがある場合）。

ESET SysRescueのインストール先として適切な対象 [デバイス] を選択します。

CAUTION

選択したUSBデバイスは、ESET SysRescueの作成時にフォーマットされます。デバイス上の全てのデータが削除されます。

[クイックフォーマット] オプションを選択した場合、フォーマットによりすべてのファイルが領域から除去されますが、ディスクの不良セクタは検査されません。USBデバイスが事前にフォーマット済みであって損傷を受けていないことが確実であれば、このオプションを使用します。

5.6.3.6 書き込み

書き込み先メディアとしてCDまたはDVDを選択した場合、[書き込み] タブで書き込みパラメータを追加指定できます。

[ISOファイルを削除する] —ESET SysRescue CDの作成後に一時ISOファイルを削除する場合、このチェックボックスをオンにします。

[削除有効] —高速消去と完全消去を選択できます。

[書き込みデバイス] —書き込みに使用するデバイスを選択します。

CAUTION

これは既定のオプションです。再書き込み可能なCD/DVDを使用した場合、CD/DVD上のすべてのデータが消去されます。

[メディア] セクションには、CD/DVDデバイス内のメディアに関する情報が表示されます。

[書き込み速度] —ドロップダウンメニューから速度を選択します。書き込み速度を選択する際には、書き込みデバイスの処理能力と使用するCD/DVDの種類を考慮に入れる必要があります。

5.6.4　ESET SysRescueの操作

レスキューCD/DVD/USBが効果的に機能するためには、ESET SysRescueブートメディアからコンピュータを起動する必要があります。ブートの優先度はBIOSで変更できます。また、コンピュータの起動時にブートメニューを使用することもできます。通常は、マザーボード/BIOSのバージョンによって、F9～F12のいずれかのキーを使用します。

ブートメディアからのブート後にESET Securityソリューションが起動します。ESET SysRescueが使用されるのは特定の状況に限られているので、標準バージョンのESET Securityソリューションにある保護モジュールやプログラム機能の中には不要なものもあります。それらは、[コンピュータの検査]、[アップデート] および [設定] の一部のセクションのみに絞り込まれます。ウイルス定義データベースをアップデートする機能は、ESET SysRescueの最も重要な機能です。コンピュータ検査を開始する前にこのプログラムをアップデートすることをお勧めします。

5.6.4.1　ESET SysRescueの使用

実行可能（.exe）ファイルを変更するウイルスがネットワーク内のコンピュータに感染したと仮定します。ESET Securityソリューションは、セーフモードでも駆除できないexplorer.exeを除くすべての感染ファイルを駆除できます。それは、explorer.exeがWindowsの基本プロセスの1つであるためにセーフモードでも起動するからです。ESET Securityソリューションは、このファイルに対して何もアクションをとれないので、このファイルは感染したままになります。

この種のシナリオでは、ESET SysRescueを使用して問題を解決できます。ESET SysRescueには、ホストオペレーティングシステムのどのコンポーネントも必要ないので、ディスク上のどのファイルでも処理（駆除や削除）できます。

[Chapter 6]
用語集

6.1 マルウェアの種類……176
6.2 リモート攻撃の種類……181
6.3 メール……184

6.1 マルウェアの種類

マルウェアとは、ユーザーのコンピュータに入り込み、損害を与えようとする悪意があるソフトウェアのことです。

6.1.1 ウイルス

コンピュータウイルスとは、コンピュータ上の既存ファイルに事前にまたは後から追加される悪意あるコードのことです。ウイルスは生物学上のウイルスにちなんで名付けられました。同じような手法でコンピュータ間に蔓延していくからです。「ウイルス」という用語は、あらゆる種類の脅威を意味するかのように誤って使用されることがよくあります。この用法は徐々に敬遠されるようになり、より正確な用語「マルウェア」（悪意のあるソフトウェア）へと次第に言い換えられています。

コンピュータウイルスは、主に実行可能ファイルとドキュメントを攻撃します。コンピュータウイルスの動作を簡単に説明します。ファイルに感染した後で、元のアプリケーションの実行よりも前に、悪意あるコードが呼び出されて実行されます。ウイルスは、現在のユーザーが持つ書き込み許可の対象のすべてのファイルに感染することができます。

コンピュータウイルスの目的と重大度は、さまざまです。ハードディスクからファイルを意図的に削除できるウイルスもあり、このようなウイルスは大変危険です。一方、実質的には被害を及ぼさないウイルスもあります。作成者が単にユーザーを困らせ、自分の技術上の技量を誇示するに過ぎないものもあります。

コンピュータがウイルスに感染し、駆除できない場合、詳しい検査のためにESETラボに送ってください。場合によっては、感染したファイルは、駆除不能のためクリーンなコピーに置き換える必要があるほどに改ざんされていることがあります。

6.1.2 ワーム

コンピュータワームとは、感染先のコンピュータを攻撃しネットワークを介して蔓延する、悪意のあるコードの入ったプログラムを指します。ウイルスとワームの基本的な違いは、ワームは独自に伝播できる点にあります。ワームは宿主ファイル（またはブートセクター）に依存しません。ワームはアドレス帳の電子メールアドレスを介して広がるか、またはネットワークアプリケーションのセキュリティ上の脆弱性を悪用します。

したがって、ワームはコンピュータウイルスよりはるかに実行可能性が高いです。インターネットは広く普及しているため、ワームはリリースから数時間、場合によっては数分で世界中に蔓延することがあります。自己を単独で急速に複製できる能力があるので、他の種類のマルウェアよりはるかに危険です。

システム内でワームが活性化されると、多くの不都合な事態が引き起こされることがあります。ファイルの削除、システムパフォーマンスの低下だけでなく、プログラムが動かなくなることすらあります。コンピュータワームはその本来の性質ゆえに、他の種類のマルウェアの"搬送手段"となります。

コンピュータがワームに感染した場合は、感染ファイルを削除することをお勧めします。悪意のあるコードが含まれている可能性が高いからです。

6.1.3 トロイの木馬

従来、コンピュータ分野でのトロイの木馬は、自己を有益なプログラムに見せかけ、こうしてユーザーを騙して実行させようとするマルウェアの1つのクラスとして定義されてきました。

トロイの木馬の範囲は非常に広いので、多くのサブカテゴリに分類されることもよくあります。

ダウンローダ	インターネットから他のマルウェアをダウンロードする機能を備えた悪意のあるプログラム。
ドロッパ	被害を受けるコンピュータに他の種類のマルウェアを取り込む悪意のあるプログラム。
バックドア	リモートの攻撃者と通信して、コンピュータにアクセスし制御権を乗っ取れるようにする悪意のあるプログラム
キーロガー（キーストロークロガー）	ユーザーが入力した各キーストロークを記録し、リモートの攻撃者にその情報を送信するプログラム。
ダイアラ	ユーザーのインターネットサービスプロバイダではなく有料情報サービスを介して接続するよう設計された悪意あるプログラム。新しい接続が作成されたことにユーザーが気づくのは、ほとんど不可能です。ダイアラで被害を被るのは、ダイヤルアップモデムを使用するユーザーのみです。このモデムは今日ではあまり使用されていません。

コンピュータ上のファイルがトロイの木馬として検出された場合、削除することをお勧めします。悪意のあるコードしか入っていない可能性が高いからです。

6.1.4 ルートキット

ルートキットとは、自己の存在を隠しながら、インターネットからの攻撃者が、システムに無制限にアクセスできるようにする悪意のあるプログラムです。ルートキットは、システムにアクセス（通常はシステムの脆弱性を悪用します）した後、オペレーティングシステムのさまざまな機能を使用して、ウイルス対策ソフトウェアによる検出を免れます。具体的には、プロセス、ファイル、およびWindowsレジストリデータを隠します。そのため、通常のテスト技術を使用して検出することはほとんどできません。

ルートキットから保護するための検出処理には2つのレベルがあります。

1.システムへのアクセスを試みているときには、まだシステム内には存在しないので、活動していません。このレベルなら、たいていのウイルス対策システムはルートキットを排除できます（ウイルス対策システムが、ルートキットに感染しているファイルを実際に検出したと仮定した場合）。

2.通常のテストで検出されない場合、ESET Endpoint Securityのユーザーは、アンチステルス技術を活用できます。これで、活動しているルートキットの検出と排除が可能です。

6.1.5 アドウェア

アドウェアは、広告機能をサポートしているソフトウェアです。広告を表示するプログラムが、このカテゴリに分類されます。アドウェアアプリケーションは、広告が表示される新しいポップアップウィンドウをインターネットブラウザ内に自動的に開いたり、ブラウザのホームページを変更したりすることがよくあります。アドウェアは、フリーウェアプログラムの開発者がその開発費を賄うことができるように、フリーウェアによく添付されています。

アドウェア自体は、危険ではありません。ユーザーは広告に悩まされるだけです。危険は、アドウェアが（スパイウェアと同様に）追跡機能を発揮することもある、という事実にあります。

フリーウェア製品を使用することにした場合には、インストールプログラムに特に注意してください。大半のインストールプログラム（インストーラ）は、アドウェアプログラムを追加でインストールすることをユーザーに通知します。アドウェアのインストールをキャンセルし、アドウェアなしで目的のプログラムをインストールできることが一般的です。

場合によっては、アドウェアをインストールしないと目的のプログラムをインストールできなかったり、機能が制限されてしまうこともあります。これは、そのアドウェアが頻繁にシステムに"合法的に"アクセスする可能性があることを意味します。ユーザーがアドウェアのインストールに同意したからです。この場合、後悔するよりは用心した方が賢明です。アドウェアとして検出されるファイルがコンピュータにある場合は、削除することをお勧めします。悪意のあるコードが含まれている可能性が高いからです。

6.1.6　スパイウェア

このカテゴリには、本人の同意も認識もないまま個人情報を送信するすべてのアプリケーションが該当します。スパイウェアは、追跡機能を使用して、アクセスしたWebサイトの一覧、ユーザーの連絡先リストにある電子メールアドレスや、記録されたキーストロークなどのさまざまな統計データを送信します。

スパイウェアの作成者は、こうした手法はユーザーのニーズと関心に関するデータをさらに見つけ、的を絞った広告を出せるようにすることが目的であると主張します。問題は、有益なアプリケーションと悪意のあるアプリケーションとの間に明確な境界線がなく、しかも、引き出された情報が悪用されることはない、とだれも断言できないことです。スパイウェアが収集したデータには、セキュリティコード、PIN、銀行の口座番号などが含まれていることがあります。スパイウェアはフリーバージョンのプログラムの作成者が、プログラムに同梱していることがよくあります。これは、収益を上げたり、そのプログラムを購入するよう動機を与えるためです。プログラムのインストール中に、スパイウェアが含まれていることをユーザーに知らせることもよくあります。これは、スパイウェアが含まれない有料バージョンにアップグレードするよう促すためです。

スパイウェアが組み入れられている、よく知られているフリーウェア製品の例としては、P2P（ピアツーピア）ネットワークのクライアントアプリケーションがあります。SpyfalconやSpy Sheriffを始めとする多数のプログラムは、スパイウェアの特定のサブカテゴリに属します。これらは一見、スパイウェア対策プログラムに見えますが、実はそれ自体がスパイウェアプログラムなのです。スパイウェアとして検出されるファイルがコンピュータにある場合は、削除することをお勧めします。悪意のあるコードが含まれている可能性が高いからです。

6.1.7　安全ではない可能性があるアプリケーション

ネットワークに接続されたコンピュータの管理を容易にする機能を持つ適正なプログラムはたくさんあります。ただし、悪意のあるユーザーの手に渡ると、不正な目的で悪用される可能性があります。ESET Endpoint Securityにはこのような脅威を検出するオプションがあります。

[安全ではない可能性があるアプリケーション] は、市販の適正なソフトウェアに適用される分類です。これには、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）などのプログラムが含まれます。

安全ではない可能性があるアプリケーションがコンピュータに存在して実行されている（しかも、自分ではインストールしていない）ことに気づいた場合には、ネットワーク管理者まで連絡するか、そのアプリケーションを削除してください。

6.1.8 望ましくない可能性があるアプリケーション

望ましくない可能性があるアプリケーション（PUA）は、必ずしも悪意があるとは限りませんが、コンピュータのパフォーマンスに悪影響を及ぼす可能性があります。通常、このようなアプリケーションをインストールするには同意が必要です。このようなアプリケーションをコンピュータにインストールすると、システムはそれ以前とは違う動作をします。最も大きな違いは次のとおりです。

●これまでに表示されたことがない新しいウィンドウ（ポップアップ、広告など）
●隠しプロセスがアクティブになり、実行される
●システムリソースの使用率が高くなる
●検索結果が異なる
●アプリケーションがリモートサーバと通信する

6.2 リモート攻撃の種類

攻撃者がリモートシステムを弱体化させる特別な手法は、いくつかあります。それらはいくつかのカテゴリに分類できます。

6.2.1 DoS攻撃

DoS（サービス拒否）とは、対象のユーザーがコンピュータやネットワークを使用できないようにする行為です。攻撃を受けるユーザー間の通信は、妨害されるので、正常に機能し続けることはできなくなります。DoS攻撃にさらされたコンピュータは通常、再起動する必要があります。そうしないと、正常に機能しません。
大半の場合、標的とされるのはWebサーバであり、その目的はある程度の期間、それらのサーバをユーザーが使用できなくすることです。

6.2.2 DNSキャッシュポイズニング

DNS（ドメインネームサーバ）侵害を使用すると、ハッカーは任意のコンピュータのDNSサーバを騙し、偽のデータを提供して正規の本物のデータであると信じさせることができます。特定の期間キャッシュされる偽の情報を利用して、攻撃者はDNSからのIPアドレスの返答を書き換えることができてしまいます。その結果、インターネット上のWebサイトにアクセスしようとするユーザーが、本来のコンテンツではなくコンピュータウイルスやワームをダウンロードさせられることがあります。

6.2.3 ワーム攻撃

コンピュータワームとは、感染先のコンピュータを攻撃しネットワークを介して蔓延する、悪意のあるコードの入ったプログラムを指します。ネットワークワームは、さまざまなアプリケーションに存在するセキュリティ上の脆弱性を悪用します。インターネットを使用できるので、ワームはリリースから数時間以内に世界中に蔓延することがあります。場合によっては、数分で広まることもあります。

大半のワーム攻撃（SasserやSqlSlammerなど）は、ファイアウォールの既定のセキュリティ設定を使用するか、または保護されていないポートと未使用のポートをブロックすることにより、防ぐことができます。また、最新のセキュリティパッチでオペレーティングシステムを更新することも重要です。

6.2.4 ポートスキャン

ポートスキャンは、ネットワークホスト上のどのポートが開いているかの特定に使用されます。ポートスキャナは、そのようなポートを見つけるためのソフトウェアです。

ポートとは、受信データと送信データを処理する仮想的な点のことです。これは、セキュリティの観点からは重要です。ネットワークが大規模な場合、ポートスキャナが収集した情報が、潜在的な脆弱性を特定するのに役立つことがあります。このような使用法は、合法です。

ただし、ポートスキャンは、セキュリティを低下させようとするハッカーが悪用することもよくあります。ハッカーが行う最初の手順としては、パケットが各ポートに送信されます。その応答の種類に応じて、使用中のポートを判断することができます。スキャン自体は無害ですが、潜在的な脆弱性をあらわにし、攻撃者がリモートコンピュータを制御できるようにする可能性もあることに注意してください。

ネットワーク管理者は、未使用のポートをすべてブロックし、使用中のポートを無許可のアクセスから保護するよう勧められています。

6.2.5 TCP非同期

TCP非同期とは、TCPハイジャック攻撃で使用される手法です。あるプロセスで受信パケットのシーケンス番号が、所定のものと異なる場合に、トリガされます。所定のものでないシーケンス番号のパケットは、破棄されます（または、現在の通信ウィンドウに存在する場合には、バッファメモリに保存されます）。

非同期処理では、双方の通信端末が、受信パケットを破棄します。リモートの攻撃者はこの部分に侵入して、正しいシーケンス番号を持つパケットを送り込むことができます。通信を操作したり、変更したりすることもできます。

TCPハイジャック攻撃の目的は、サーバ/クライアント通信やピアツーピア通信を妨害することです。多くの攻撃は、各TCPセグメントに認証を使用することで回避できます。また、使用しているネットワークデバイス向けの推奨設定を使用してください。

6.2.6 SMBリレー

SMBRelayとSMBRelay2は、リモートコンピュータに攻撃を仕掛けることができる特殊なプログラムです。このプログラムは、Server Message Blockファイル共有プロトコルを利用します。このプロトコルはNetBIOSの上位層で機能します。LAN内でフォルダやディレクトリを共有する場合、このファイル共有プロトコルを使用するのが一般的です。

ローカルネットワーク通信内では、パスワードハッシュが交換されます。

SMBRelayは、UDPポート139と445で接続を受信し、クライアントとサーバ間で交換されるパケットを中継して、そのパケットを書き換えます。接続して認証した後、クライアントは接続を切断されます。SMBRelayは、新しい仮想のIPアドレスを作成します。新しいアドレスには、コマンド"net use￥￥192.168.1.1"でアクセスできます。これ以降、このアドレスは、Windowsのネットワーク機能で使用できます。SMBRelayはネゴシエーションと認証以外のSMBプロトコル通信を中継します。クライアントコンピュータが接続している限り、リモートの攻撃者はこのIPアドレスを利用できます。

SMBRelay2はSMBRelayと同じ原理で機能しますが、IPアドレスではなくNetBIOS名を使用する点が異なります。どちらも"中間者"攻撃を実行できます。この攻撃では、リモートの攻撃者は、2つの通信端末間で交換されるメッセージの読み取り、挿入、および変更を密かに行えます。このような攻撃にさらされるコンピュータは、応答しなくなるか、突然に再起動することがよくあります。

攻撃を避けるため、認証パスワードか認証鍵の使用をお勧めします。

6.2.7 ICMP攻撃

ICMP（インターネット制御メッセージプロトコル）は、広く使用されている一般的なインターネットプロトコルです。主に、さまざまなエラーメッセージを送信するために、ネットワークに接続されたコンピュータによって使用されます。

リモートアタッカーは、ICMPプロトコルの脆弱性を悪用しようとします。ICMPプロトコルは、認証を必要としない一方向の通信用に設計されています。そのため、リモートアタッカーは、いわゆるDoS（Denial of Service）攻撃、つまりサービス拒否攻撃や、認証されていないユーザーに受信および送信パケットへのアクセス権を与える攻撃を開始することができます。

ICMP攻撃の一般的な例として、pingフラッド、ICMP_ECHOフラッド、および smurf攻撃があります。ICMP攻撃にさらされたコンピュータは処理速度が大幅に低下し（これは、インターネットを使用する全てのアプリケーションに該当します）、インターネットへの接続に関する問題が発生します。

6.3 メール

メール（電子メール）は、多数の利点を備えた最新の通信形態で、柔軟性、速度、直接性があり、1990年代の初めには、インターネットの普及において重要な役割を果たしました。

しかし、匿名性が高いため、メールとインターネットには迷惑メールなどの不正な活動の余地があります。迷惑メールには、受信者側が送信を要求していない広告、デマ、悪意のあるソフトウェア（マルウェア）の拡散があります。送信費が最小限であること、また、迷惑メールの作成者には新しいメールアドレスを入手するさまざまなツールがあることから、ユーザーに対する迷惑行為や危険性は増加しています。さらに、迷惑メールの量や多様性のために、規制することは非常に困難です。メールアドレスを長く使用するほど、迷惑メールエンジンデータベースに登録される可能性が高くなります。回避策をいくつか紹介します。

●可能な場合、インターネットにメールアドレスを公開しない。
●信頼できる個人のみにメールアドレスを知らせる。
●可能な場合、一般的なエイリアスを使用しない。複雑なエイリアスを使用するほど、追跡される可能性が低くなります。
●受信ボックスに届いた迷惑メールに返信しない。
●インターネットフォームに記入する際に注意する。特に、"はい。情報を受信します。"のようなチェックボックスには注意してください。
●ビジネス用、友人との通信用など、"専用の"メールアドレスを使用する。
●メールアドレスをときどき変更する。
●迷惑メール対策ソリューションを使用する。

6.3.1 広告

インターネット広告は、最も急速に普及している広告の一つです。マーケティング上の主な利点は、経費が最小限で済み、直接的にうったえることができること以外に、メッセージがほぼ瞬時に配信されることにあります。多くの企業では、メールをマーケティングツールとして使用して、既存顧客および見込み客と効果的に連絡を取り合っています。

この種の広告は、適正なものです。ユーザーは製品に関する商業上の情報を受け取ることに関心がある可能性があるからです。しかし、多くの企業が、受信者側が送信を要求していない商業メッセージを大量に送っています。このような場合、メール広告は迷惑メールになってしまいます。

受信者側が送信を要求していないメールの量が、実際に問題になっています。鎮まる様子がありません。こうしたメールの作成者はたいてい、迷惑メールを適正なメッセージに見せかけようとします。

6.3.2 デマ

デマは、インターネットを通じて広がる偽情報です。デマは、通常電子メールやICQやSkypeなどの通信ツール経由で送信されます。メッセージ自体はジョークや都市伝説であることがほとんどです。

コンピュータウイルスとしてのデマは、受信者に恐怖、不安、および疑念（FUD）を抱かせ、ファイルの削除およびパスワードの取得や、その他の有害な操作をシステムに対して実行する"検出不可能なウイルス"があると信じ込ませます。

一部のデマは、他のユーザーにメッセージを送信するよう求め、デマを拡散させます。携帯電話によるデマ、援助を求める訴え、海外からの送金の申し出などがあります。ほとんどの場合、作成者の意図を突き止めることは不可能です。

知り合い全員に転送するよう求めるメッセージは、確実にデマであると考えられます。インターネット上には、適正なメールであるかどうかを確認できるWebサイトが多数あります。デマの疑いがあるメッセージを受け取った場合は、転送する前にインターネットで検索してみてください。

6.3.3 フィッシング

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）のさまざまな手法を用いる犯罪行為を指します。その目的は、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ことです。

入手するための一般的な手口は、信頼できる人物や企業（金融機関や保険会社など）を装い、メールを送ることです。このメールは本物そっくりに見えることがあり、成り済ます相手が使用しているグラフィックやインターネットコンテンツが含まれているのが一般的です。データの確認や金融業務を装い、個人データを入力するようユーザーに指示します。たとえば、銀行の口座番号やユーザー名とパスワードなどです。このようなデータは、いったん提出すると、簡単に盗まれ悪用されてしまいます。

銀行、保険会社、およびその他の合法的な企業は、受信者側が送信を要求していないメールでユーザー名とパスワードを入力するよう要求することなど、決して行いません。

6.3.4 迷惑メール詐欺の特定

通常、いくつかの指標を参考にすることで、メールボックス内の迷惑メール（受信者が送信を要求していないメール）を特定することができます。メールが少なくとも次の基準のいくつかを満たしている場合、迷惑メールの可能性があります。

●送信元アドレスが連絡先リスト内の連絡先のものでない。
●多額のお金が提供されるが、最初に少額を提供する必要がある。
●データの確認や金融業務を装い、銀行の口座番号やユーザー名とパスワードなどの個人データを入力するよう求められる。
●外国語で記載されている。
●関心のない製品を購入するよう求められる。購入することにした場合は、メールの送信元が信頼できるベンダであることを確認してください（本来の製品製造元に問い合わせてください）。
●迷惑メールフィルタを騙そうとして、単語のスペルを間違えている。たとえば、"viagra"の代わりに"vaigra"と記載している場合などです。

6.3.4.1 ルール

ウイルス対策ソリューションとメールクライアントに関する限りでは、ルールはメール機能を操作するためのツールとなります。ルールは次の2つの論理的部分で構成されます。

1.条件（たとえば、受信メッセージが、ある特定のアドレスからのものである）
2.アクション（たとえば、メッセージを削除したり、指定フォルダに移動したりする）

ルールの数と組み合わせは、迷惑メール対策ソリューションに応じて異なります。このルールは、迷惑メール（受信者側が送信を要求していないメール）を防ぐための手段となります。よくある例は、次のとおりです。

1.条件:受信メールに、迷惑メールメッセージに特有の語がいくつか含まれる。
2.アクション:メッセージを削除する。

1.条件:受信メールに、拡張子が.exeの添付ファイルが含まれる。
2.アクション:添付ファイルを削除し、メッセージをメールボックスに配信する。

1.条件:雇用者からの受信メッセージである。
2.アクション:メッセージを"仕事"フォルダに移動する。管理し易くし、迷惑メールのフィルタリングの効果を向上させるため、迷惑メール対策プログラムで複数のルールを組み合わせて使用することをお勧めします。

6.3.4.2 ホワイトリスト

一般に、ホワイトリストとは、受け入れられる物や人物、または許可を与えられている物や人物の一覧を指します。"メールホワイトリスト"という用語は、ユーザーがメッセージを受信したいと思う相手の連絡先の一覧を意味します。このようなホワイトリストは、電子メールアドレス、ドメイン名、またはIPアドレスで検索するキーワードに基づきます。

ホワイトリストを"除外モード"で使用すると、一覧にないアドレス、ドメイン、またはIPアドレスからのメッセージは、受信されません。除外モードでない場合には、そのようなメッセージは削除されず、別の仕方でフィルタリングされます。

ホワイトリストは、ブラックリストとは正反対の原則に基づきます。ホワイトリストの保守は、ブラックリストより簡単です。ホワイトリストとブラックリストの両方を使用して、迷惑メールをより効果的にフィルタリングすることをお勧めします。

6.3.4.3 ブラックリスト

一般に、ブラックリストとは、受け入れられないかまたは禁止されている品目や人物の一覧のことです。仮想世界では、そのような一覧に掲載されている全ユーザーからのメッセージを拒否するためのテクニックです。

ブラックリストには、2種類あります。ユーザーが迷惑メール対策ソフトウェアを使用して作成したブラックリストと、定期的に更新される、専門機関が作成したインターネット上にある専門的なブラックリストがあります。

迷惑メールを防ぐには、ブラックリストの使用は不可欠ですが、保守が困難です。ブロックすべき新しい項目が毎日現れるからです。迷惑メールをより効果的にフィルタリングするには、ホワイトリストとブラックリストの両方を使用することをお勧めします。

6.3.4.4 サーバー側での検査

サーバ側での検査とは、受信したメッセージ数とユーザーの反応に基づいて、大量の迷惑メールを特定するための手法のことです。各メッセージは、その内容に基づいて、固有のデジタル"痕跡"を残します。この固有のID番号でメールの内容を知ることはできません。2通のメッセージが、同じであれば痕跡も同じであり、異なれば痕跡も異なります。

あるメッセージが迷惑メールとしてマークされた場合、その痕跡がサーバに送信されます。サーバが同じ痕跡（ある特定の迷惑メールメッセージに対応します）をさらに受信すると、痕跡は迷惑メール痕跡データベースに格納されます。受信メッセージを検査する際に、メッセージの痕跡がサーバに送信されます。サーバはユーザーにより迷惑メールとして既にマークされているメッセージに対応する痕跡に関する情報を返します。