ESET Endpoint アンチウイルス for OS X ユーザーズマニュアル

■お断り

○本マニュアルは、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記載されている機能が異なる場合があります。また、本マニュアルの内容は、改訂などにより予告なく変更することがあります。

改定日：2016 年 2 月 25 日

目　次

Chapter 1 はじめに

1.1 ESET Endpoint アンチウイルス for OS X について

ESET Endpoint アンチウイルス for OS X では、コンピューターのセキュリティに新しいアプローチで取り組んでいます。最新バージョンの ThreatSense 検査エンジンは、高速かつ正確に、コンピューターを安全に保ちます。その結果、コンピューターにとって脅威となる可能性のある攻撃と不正ソフトウェアに対して常に警戒態勢を保ちます。

ESET Endpoint アンチウイルス for OS X は、長期にわたる取り組みによって保護機能の多様化とシステムリソース消費量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、コンピューター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 アンチウイルス for OS X は 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複数のコンピューターを簡単に一元管理し、ポリシーとルールの適用、検出の監視、リモート設定などが可能になります。

1.2 動作環境

ESET Endpoint アンチウイルス for OS X は Mac OS X オペレーティングシステム専用の製品です。動作環境については、弊社ホームページをご参照ください。
http://canon-its.jp/product/eset/license/eep_adv/spec.html#spec1

1.3　ご利用にあたって

ウイルス対策ソフトを導入しているだけでは、不正侵入とマルウェアが引き起こす危険を完全に排除することはできません。最大限の保護と利便性を得るためには、ウイルス対策ソフトを正しく使用し、セキュリティルールを守ることが重要です。

■定期的にアップデートする

毎日数千種類のマルウェアが新たに作成されています。ESET では、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リリースしています。保護レベルを継続的に向上させるために、定期的にアップデートを行ってください。
アップデートの設定方法については「3.3　アップデートの設定」を参照してください。

■セキュリティパッチをダウンロードする

多くのマルウェアは効率的に広めるために、システムの脆弱性を悪用するように作成されています。そのため、ソフトウェアベンダ各社は、システムの脆弱性を悪用されないためにセキュリティアップデートファイル（セキュリティパッチ）を定期的にリリースしています。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。

■重要なデータをバックアップする

マルウェアによってオペレーティングシステムの誤操作が引き起こされ、重要なデータが喪失されることがあります。定期的に DVD や外付けハードディスクなどの外部媒体にバックアップを行ってください。システム障害が発生したときにバックアップされたデータを使用して素早く復旧することができます。

■コンピューターにウイルスがいないか定期的にスキャンする

ウイルス定義データベースは毎日アップデートされています。定期的にコンピューターの完全な検査を実行することをお勧めします。

■基本的なセキュリティルールに従う

多くのマルウェアは、ユーザーが操作を行わないと実行されずに蔓延することはありません。新しいファイルを開くときに注意をすれば、マルウェアの蔓延を防ぐことができます。マルウェアの蔓延を防ぐ有効的な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は注意する。特に、大量に送信されたメールや、知らない送信者からのメールの添付ファイルに注意する。
- 日々の作業では、コンピューター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 インストール手順

インストーラーを利用した手動インストールの手順について記載しています。以下の手順に沿ってインストール作業を実施します。
リモートインストールを行う場合は、『ESET Remote Administrator ユーザーズマニュアル』を参照してください。

STEP 1	ESET Endpoint アンチウイルス for OS X をインストールする	P8 参照
STEP 2	アクティベーションを行う	P18 参照
STEP 3	コンピューターの検査を行う	P21 参照

2.2 標準インストール

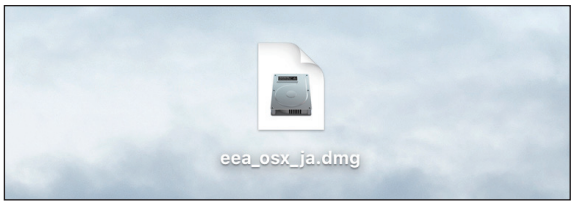
標準インストールには、ほとんどのユーザーに適した設定オプションが用意されています。特定の設定を行わない場合は、標準インストールでインストールを行います。
詳細インストールを行う場合は手順⑦まで操作を行った後「2.3 詳細インストール」に進みます。

! 重 要

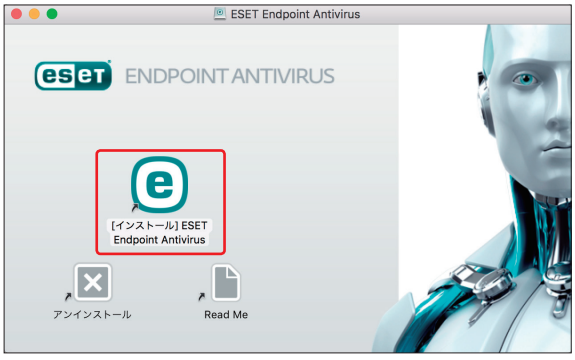
ESET Endpoint アンチウイルス for OS X をインストールする前に、他のウイルス対策ソフトがインストールされていないことを確認してください。2 つ以上のウイルス対策ソフトが 1 台のコンピューターにインストールされていると、互いに競合し重大な問題が発生する場合がありますので、他のウイルス対策ソフトはアンインストールしてください。

操作手順

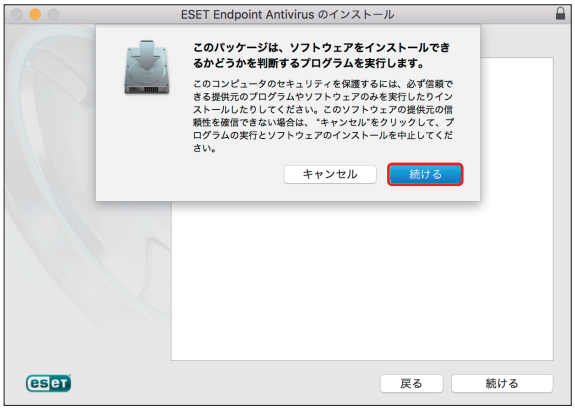
1 ダウンロードしたインストーラーをダブルクリックして起動します。



2 [[インストール] ESET Endpoint Antivirus] ボタンをダブルクリックします。

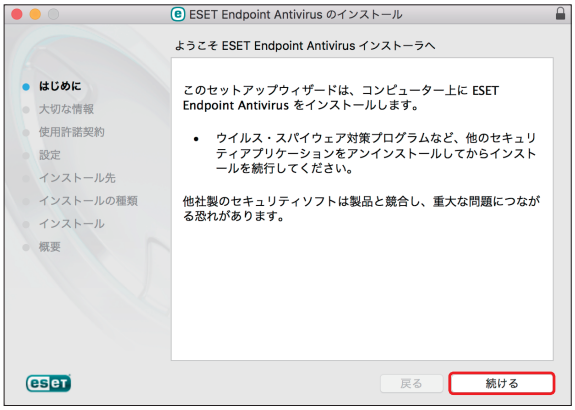


3 [続ける] ボタンをクリックします。

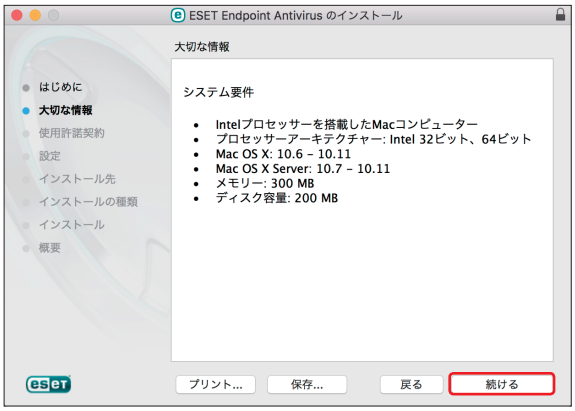


続く

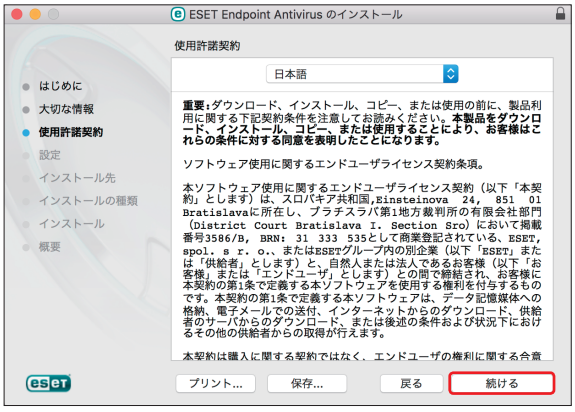
4 [続ける] ボタンをクリックします。



5 [続ける] ボタンをクリックします。

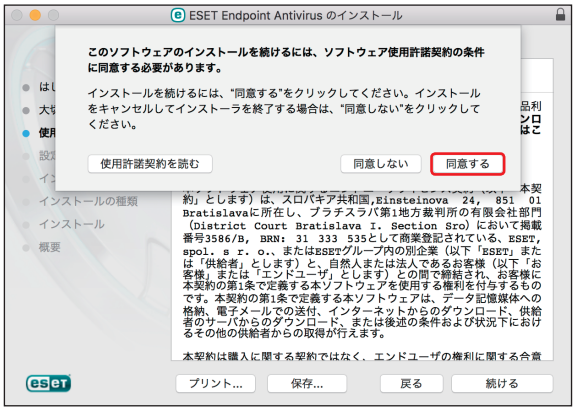


6 使用許諾契約の内容を確認し [続ける] ボタンをクリックします。

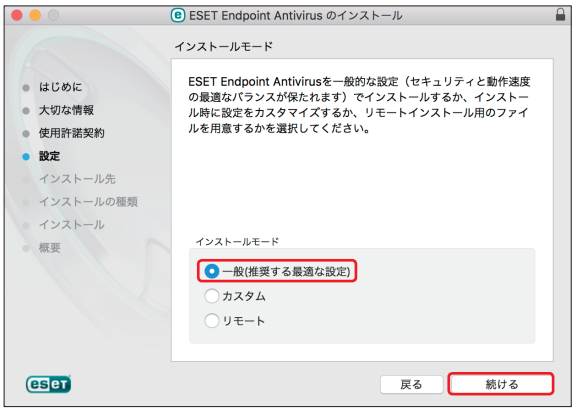


続く

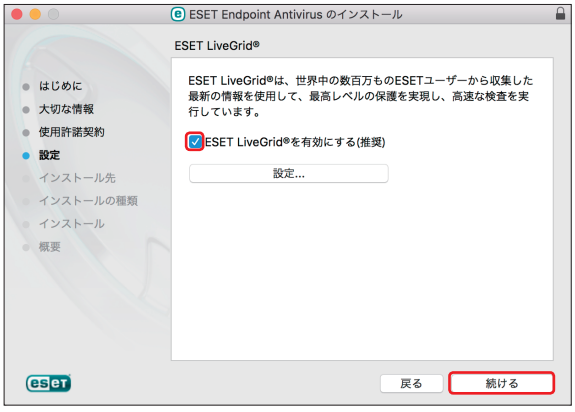
7 ［同意する］ボタンをクリックします。



8 ［一般（推奨する最適な設定）］のチェックを確認して［続ける］ボタンをクリックします。



9 ESET LiveGrid を有効にする場合は、［ESET LiveGrid を有効にする（推奨）］のチェックを確認して［続ける］ボタンをクリックします。

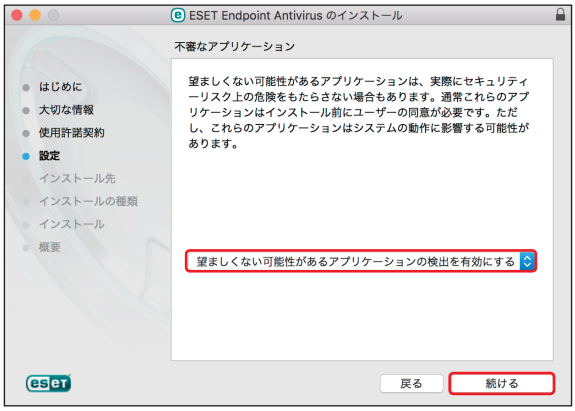


ワンポイント

ESET LiveGrid（早期警告システム）は新しく検出したウイルスの統計情報や、疑わしいファイルが検出された場合に ESET 社へ情報の送信を行います。
ESET 社へ届いた情報が解析および処理され、早く正確にマルウェアを検出することが可能になります。

続く

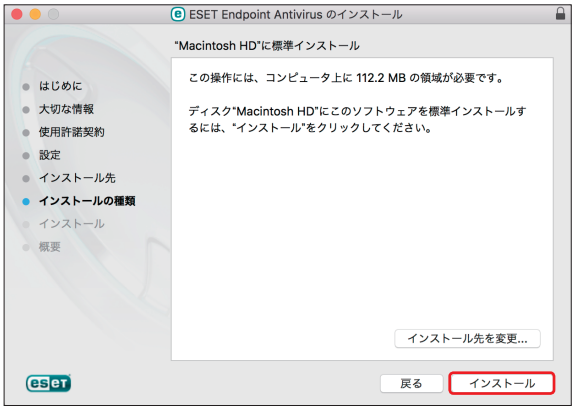
10 望ましくない可能性があるアプリケーションの検出の有無を設定します。ポップアップメニューから［望ましくない可能性があるアプリケーションの検出を有効にする］を選択して、［続ける］ボタンをクリックします。



ワンポイント

望ましくない可能性があるアプリケーションの検出の詳細は「4.6.3 リアルタイムファイルシステム保護」の「●オプション」を参照してください。

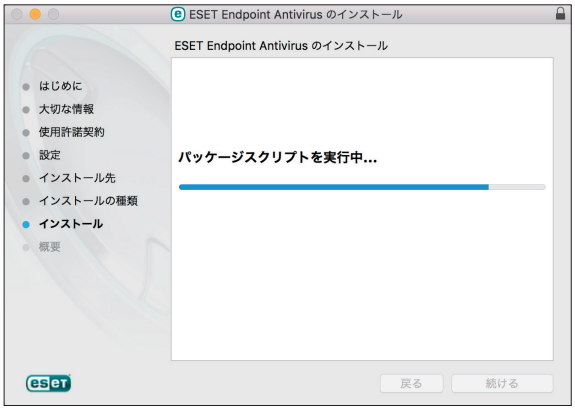
11 ［インストール］ボタンをクリックします。



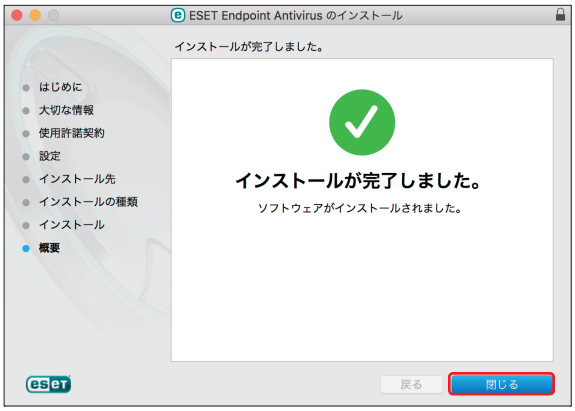
12 管理者アカウントの「ユーザ名」と「パスワード」を入力し、［ソフトウェアをインストール］ボタンをクリックします。

続く

⑬ インストール完了までお待ちください。



⑭ [閉じる] ボタンをクリックします。



ワンポイント

手順⑭の画面の上にアクティベーション画面が表示されたときは、その画面を移動させて、手順⑭の作業を行ってください。

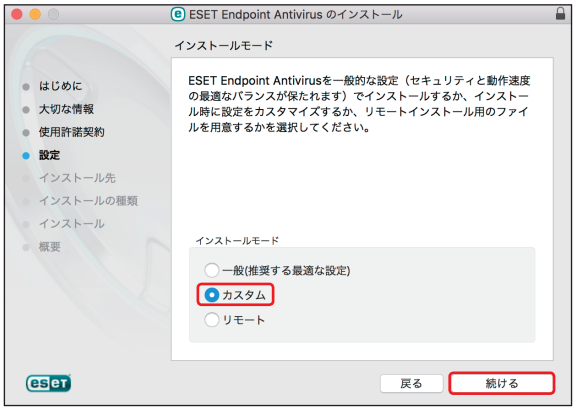
2.3 詳細インストール

詳細インストールは、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。

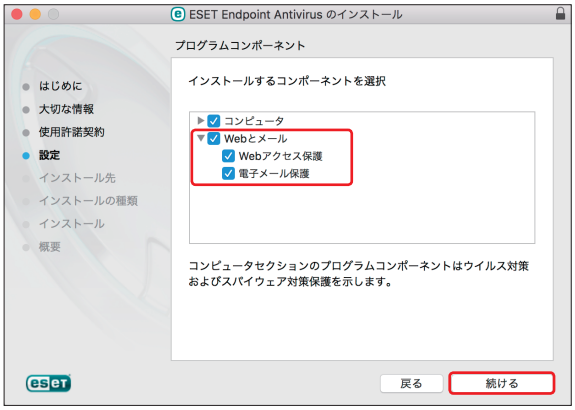
操作手順

「2.2 標準インストール」手順⑦の続き

1 ［カスタム］ボタンをクリックして選択し、［続ける］ボタンをクリックします。



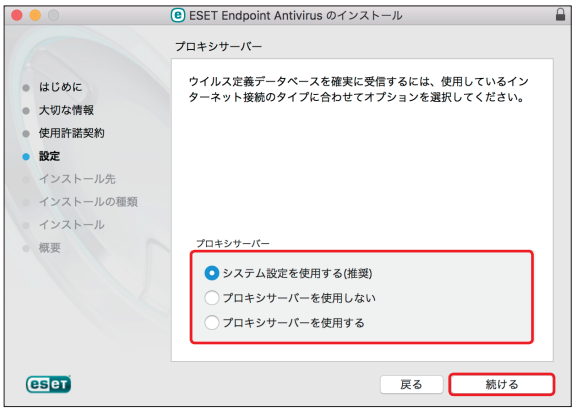
2 インストールするコンポーネントの選択を行い、［続ける］ボタンをクリックします。
チェックを「オン」にするとコンポーネントがインストールされ、オフにするとそのコンポーネントはインストールされません。また、コンポーネントツリーを展開すると、詳細なコンポーネントの選択が行えます。



続く

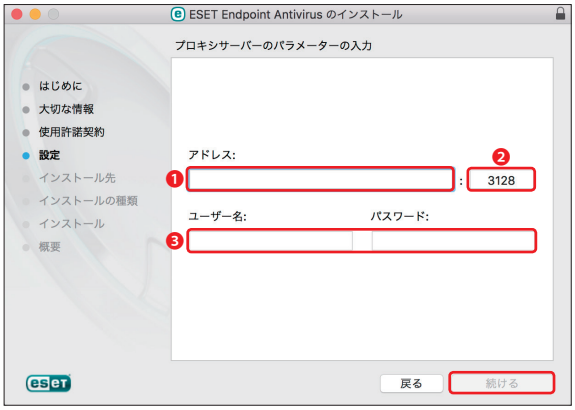
3 インターネット接続時のプロキシサーバーの設定を選択して［続ける］ボタンをクリックします。

- ［システム設定を使用する（推奨）］または［プロキシサーバーを使用しない］を選択して［続ける］ボタンをクリックした場合は、手順⑤へ進みます。
- ［プロキシサーバーを使用する］を選択して、［続ける］ボタンをクリックした場合は、手順④へ進みます。



4 プロキシサーバーのパラメーターを入力して［続ける］ボタンをクリックします。

❶	アドレス	プロキシサーバーの IP アドレスまたは、URL を入力します。
❷	ポート	プロキシサーバーが接続を受け付けるポートを入力します（既定値は 3128）。
❸	ユーザー名とパスワード	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ます。



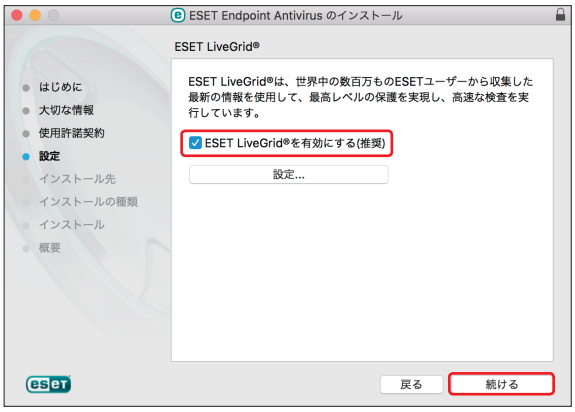
続く

5 権限ユーザーの設定を行います。[ユーザー]グループに登録されているユーザーの中から権限ユーザーに登録したいユーザーをクリックして選択し、[追加]ボタンをクリックします。この作業を繰り返し、権限ユーザーにしたいユーザーをすべて登録します。権限ユーザーへの登録が完了したら、[続ける]ボタンをクリックします。

ワンポイント

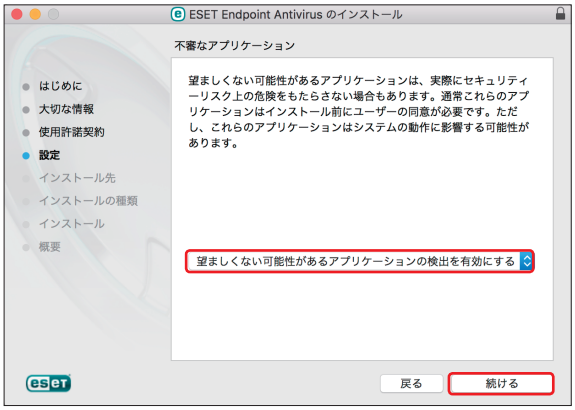
本プログラムの各種設定を変更できるのは、「権限ユーザー」グループに登録されたユーザーアカウントのみです。「権限ユーザー」グループにユーザーアカウントが登録されていない場合は、全てのユーザーに設定変更を行う権限があるとみなされます。この設定は、設定変更を行えるユーザーを限定したいときに行ってください。

6 ESET LiveGrid を有効にする場合は、[ESET LiveGrid を有効にする（推奨）]のチェックを確認して［続ける］ボタンをクリックします。

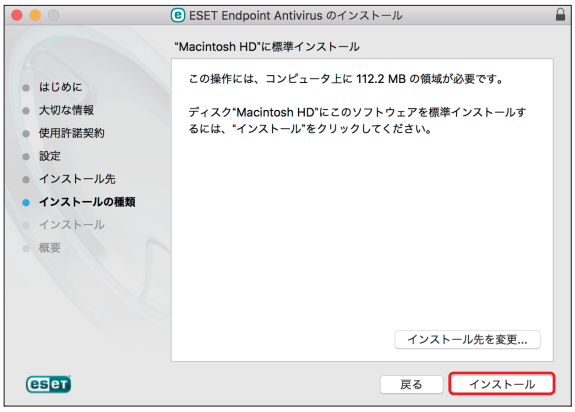


続く

7 望ましくない可能性があるアプリケーションの検出の有無を設定します。ポップアップメニューから［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］を選択して、［続ける］ボタンをクリックします。



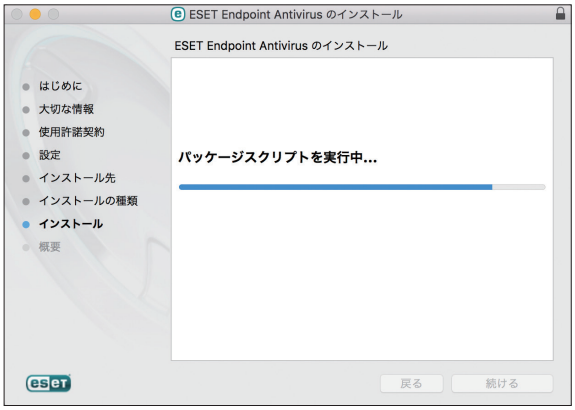
8 ［インストール］ボタンをクリックします。



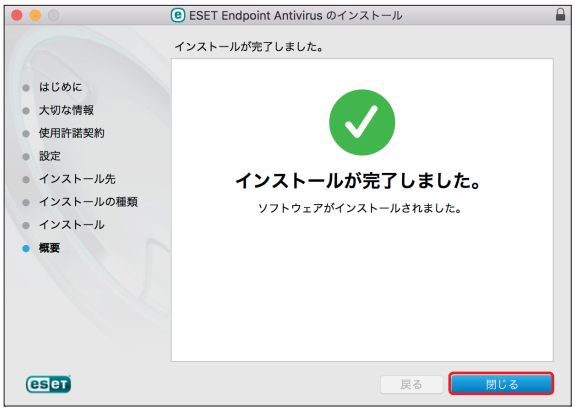
9 管理者アカウントの「ユーザ名」と「パスワード」を入力し、［ソフトウェアをインストール］ボタンをクリックします。

続く

⑩ インストール完了までお待ちください。



⑪ [閉じる] ボタンをクリックします。



ワンポイント

手順⑪の画面の上にアクティベーション画面が表示されたときは、その画面を移動させて、手順⑪の作業を行ってください。

2.4　アクティベーション

インストール完了後に、「製品のアクティベーション」画面が表示されます。
アクティベーションには次の 3 つの方法がありますが、日本では製品認証キーまたはオフラインライセンスを使用してアクティベーションします。

・製品認証キーを使用してアクティベーション：事前に入手した製品認証キーを入力する。
・セキュリティ管理者：日本では使用しません。
・オフラインライセンス：ユーザーズサイトからダウンロードします。

ワンポイント

管理者が ESET Remote Administrator の「製品のアクティベーション」タスクにより、リモートから製品認証キーを ESET Endpoint アンチウイルス for OS X に適用しアクティベーションすることができます。詳細は『ESET Remote Administrator ユーザーズマニュアル』の「6.5.3.1　タスクタイプの設定　■製品のアクティベーション」を参照してください。

! 重　要

製品のアクティベーションを行うことにより、ウイルス定義データベースを最新のバージョンに更新することができます。必ずアクティベーションを実施してください。

! 重　要

オフラインライセンスは、インターネット接続が一切できない端末でアクティベーションを行う場合にご利用ください。

2.4.1　製品認証キーを使用してアクティベーション

! 重　要

製品認証キーを使用して、アクティベーションするためにはコンピューターが ESET 社のライセンスサーバーに HTTPS で接続できる環境が必要です。

操作手順

製品認証キーを入力して［アクティベート］ボタンをクリックします。

製品認証キーを使用してアクティベーションするためには、コンピューターが ESET 社のライセンスサーバーに HTTPS で接続できる環境が必要です。
必要に応じて、プロキシサーバーの設定を行います。
プロキシサーバーの設定手順は「3.4　プロキシサーバーの設定」を参照してください。

2.4.2 オフラインライセンスファイルを使用してアクティベーション

! 重 要

インターネット接続が行えないコンピューターのアクティベーションを行うには、「オフラインライセンスファイル」が必要になります。オフラインライセンスファイルは、ユーザーズサイトからダウンロードできます。ダウンロードしたオフラインライセンスファイルは、アクティベーションを行うコンピューターで読み出せるようにしておいてください。

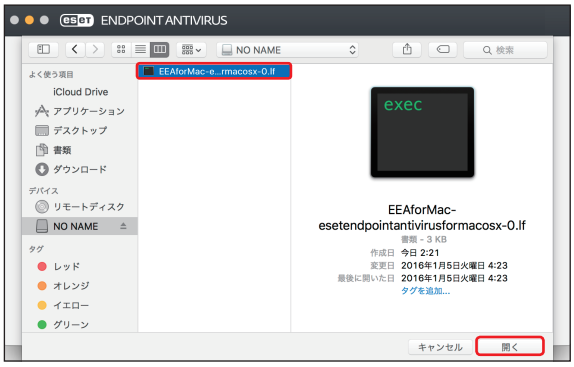
操作手順

1. オフラインライセンスファイルをコンピューターで読み出せる状態にします。
2. ESET Endpoint アンチウイルス for OS X のメイン画面で［ヘルプ］をクリックします。
3. ［製品のアクティベーション］ボタンをクリックします。

4. ［オフラインライセンス］をクリックします。

続く

5 オフラインライセンスファイルをクリックし、［開く］ボタンをクリックします。



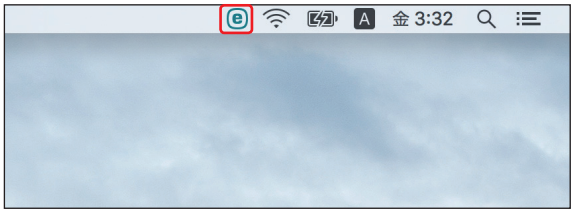
6 自動的にアクティベーションが完了します。［完了］ボタンをクリックします。

2.5 コンピューターの検査

インストール後にスマート検査を実行することを推奨しています。ESET Endpoint アンチウイルス for OS X を起動してスマート検査から検査を行います。

操作手順

1 メニューバーのアイコンをクリックします。



2 [ESET Endpoint Antivirus を開く] をクリックします。

3 [スマート検査] をクリックします。

2.6　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解決できない問題の修正や改良を行うために、ESET Endpoint アンチウイルス for OS X の新バージョンが提供されています。最新バージョンへのアップグレードには、次の 2 つの方法があります。

■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する

最新バージョンのインストーラーをダウンロードして、インストーラーを実行します。詳細な手順については、「2.1　インストール手順」を参照してください。

■ ESET Remote Administrator 経由のネットワーク環境で自動展開する

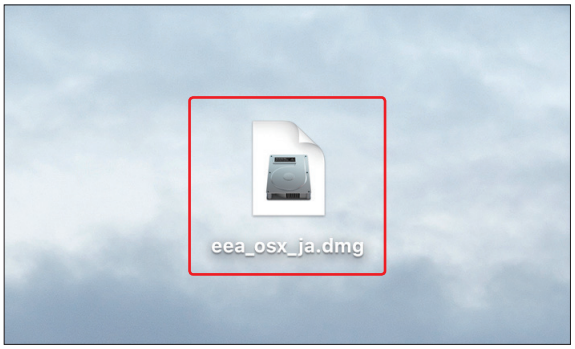
ESET Remote Administrator の「管理」メニューのクライアントタスクにある、「ソフトウェアインストール」を使用して最新バージョンを上書きインストールします。詳細は『ESET Remote Administrator ユーザーズマニュアル』の「6.5.3.1 ESET セキュリティ製品」の「■ソフトウェアインストール」または、「4.2.3　製品インストール」を参照してください。

2.7 アンインストール

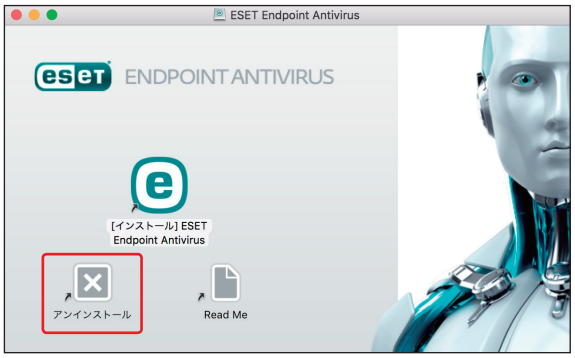
ESET Endpoint アンチウイルス for OS X のアンインストール方法を説明します。

操作手順

1. ダウンロードしたインストーラーをダブルクリックして起動します。



2. ［アンインストール］ボタンをダブルクリックします。

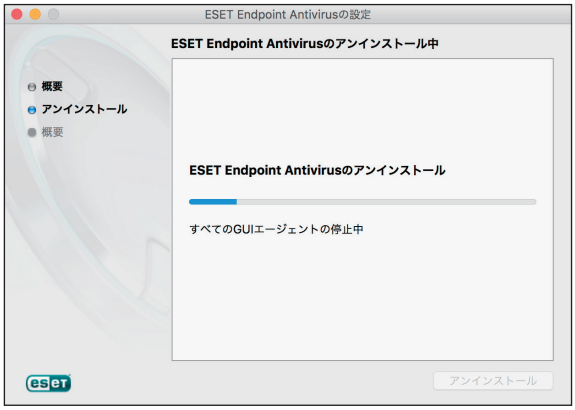


3. アンインストーラーが起動します。［アンインストール］ボタンをクリックします。

続く

4 管理者アカウントの「ユーザ名」と「パスワード」を入力し、[OK] ボタンをクリックします。

5 アンインストール完了までお待ちください。



6 「アンインストールに成功しました。」と表示されたら、アンインストールは完了です。[閉じる] ボタンをクリックします。

Chapter 3 ご利用開始時の確認・設定事項

3.1 画面構成

ESET Endpoint アンチウイルス for OS X のメイン画面は、各メニューが並んでいる「メインメニュー」とメインメニューで選択された機能が表示される「プライマリウインドウ」に分かれています。

■各メニューについて

保護の状態	保護の状態、ライセンス有効期限が確認できます。
コンピュータの検査	スマート検査、カスタム検査、リムーバブルメディア検査、最後に利用した検査の再実行が行えます。
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	コンピューター、Web とメールの設定を確認、変更することができます。
ツール	[ログファイル]、[統計]、[スケジューラー]、[実行中のプロセス]、[隔離] にアクセスできます。分析のためにサンプルを送信することもできます。
ヘルプ	ヘルプファイル、製品ホームページの FAQ のリンクを利用できます。また、サポートツール、製品アクティベーションへのリンクも利用できます。

3.2 保護状態の確認

「保護の状態」画面には、利用しているコンピューターのセキュリティと現在の保護レベルが表示されています。各モジュールが正しく動作している場合は、緑色の表示になります。正しく動作していない場合は、赤色もしくは黄色の表示になり問題、注意の内容が表示されます。モジュールを修正するための推奨される解決策が表示されますので内容を確認してください。各モジュールの設定の変更はメインメニューの［設定］から行えます。

緑色の表示は「最も高い保護」の状態を示しています。各機能が正しく動作しています。

赤色の表示は「保護に重大な問題」があることを示しています。

主な理由

- 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
- Web アクセス保護が無効になっている
- 電子メールクライアント保護が無効になっている
- フィッシング対策機能が無効になっている
- ウイルス定義データベースが最新でない
- 製品のライセンスの有効期限が切れている

■主な解決策

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場合	［設定］メニューの［コンピュータ］より、［リアルタイムファイルシステム保護］をクリックして有効にします。
Web アクセス保護が無効になっている場合	［設定］メニューの［Web とメール］より、［Web アクセス保護］をクリックして有効にします。
電子メールクライアント保護が無効になっている場合	［設定］メニューの［Web とメール］より、［電子メールクライアント保護］をクリックして有効にします（表示は「リアルタイムファイルシステム保護はユーザーによって無効にされています。」となります）。
フィッシング対策機能が無効になっている場合	［設定］メニューの［Web とメール］より、［フィッシング対策保護］をクリックして有効にします。
ライセンスが有効期限を過ぎている場合	ライセンスの有効期限が過ぎると、ウイルス定義データベースのアップデートができません。警告ウインドウの指示に従ってライセンスの更新を行ってください。

黄色の表示は「注意が必要」な状態を示しています。

主な理由
・アップデートに関する問題がある（ウイルス定義データベースが期限切れになっている）
・ライセンスの有効期限がせまっている

■主な解決策

ライセンスの期限が切れました	ライセンスの有効期限が切れると、ウイルス定義データベースのアップデートができなくなります。ライセンスの更新を行ってください。

提示された解決策を使用して問題が解決されない場合は、［ヘルプ］をクリックしてヘルプ情報を確認するか、製品ホームページの FAQ を参照してください。それでも解決されない場合は、サポートセンターへご連絡ください。

製品ホームページの FAQ
http://eset-support.canon-its.jp/?site_domain=business

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は、コンピューターを保護するための重要な作業です。メインメニューから［アップデート］メニューを選択し、［ウイルス定義データベースをアップデートする］をクリックして、最新のウイルス定義データベースを確認します。
ESET Endpoint アンチウイルス for OS X のインストール作業中に、アクティベーションを行わなかった場合、「アクティベート」画面が表示されますのでアクティベーションを行ってください。

アップデートに関する設定は、「詳細設定」画面で確認、変更することができます。

操作手順

1 メインメニューの［設定］メニューから［詳細設定を表示する］をクリックします。

続く

2 ［アップデート］をクリックします。

3 アップデートの設定画面が表示されます。「アップデートサーバー」には、既定では［自動選択］が設定されています。［編集］ボタンをクリックすると、接続先のアップデートサーバーの情報の追加が行えます。追加したアップデートサーバーを利用する場合は、アップデートサーバーへの接続アカウントの設定が行えます。詳細オプションの［設定］ボタンをクリックすると、アップデートモードなど、詳細なアップデートオプションを設定できます。

ワンポイント

アップデートサーバーの設定に「自動選択」を選択している場合、ユーザー名とパスワードの入力は行えません。自動選択では、ユーザー名とパスワードの入力は不要です。

3.4 プロキシサーバーの設定

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している場合は、「詳細設定」画面で「プロキシサーバー」（IP アドレス）と「ポート」の設定をします。

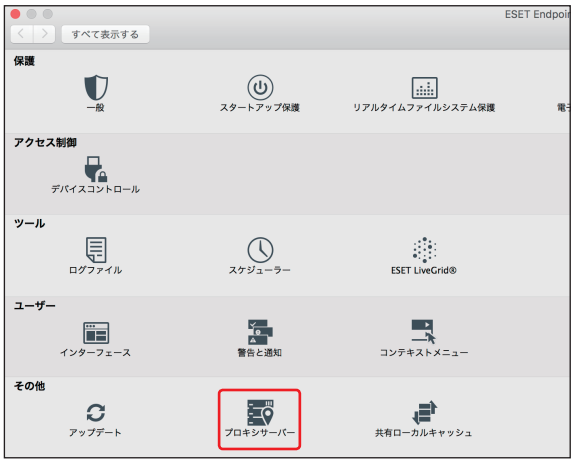
操作手順

1 メインメニューの［設定］メニューから［詳細設定を表示する］をクリックします。

ワンポイント

キーボードの【command】＋【,】キーを押して「詳細設定」画面を表示させることもできます。

2 ［プロキシサーバー］をクリックします。



3 ❶「プロキシサーバーを使用する」のチェックをオンにして、❷「プロキシサーバー」（IP アドレスまたは URL）、❸「ポート」を入力します。

3.5 設定の保護

ESET Endpoint アンチウイルス for OS X の設定は、セキュリティポリシーの観点から、非常に重要であり、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。ESET Endpoint アンチウイルス for OS X では許可なく変更されるのを防ぐために、設定の変更を行える「権限ユーザー」を設定し、権限ユーザー以外のユーザーが設定を変更できないようにすることが可能です。

操作手順

1 メインメニューの［設定］メニューから［詳細設定を表示する］をクリックします。

2 ［権限］をクリックします。

3 ［ユーザー」グループに登録されているユーザーの中から権限ユーザーに登録したいユーザーをクリックして選択し、［追加］ボタンをクリックします。この作業を繰り返し、権限ユーザーにしたいユーザーを登録します。

ワンポイント

上の手順ではユーザーを登録していますが、［グループ］タブをクリックすると、グループを登録することもできます。グループを登録する場合、「nobody」を登録すると、すべてのユーザーが権限ユーザーとなるので注意してください。

3.6 ESET Remote Administrator との接続

ESET Remote Administrator はネットワーク環境にある ESET 製品を管理できるアプリケーションです。ESET Remote Administrator は「ERA エージェント」経由で ESET Endpoint アンチウイルス for OS X との通信を行います。
ESET Remote Administrator との通信を行うには、「ERA エージェント」のインストールが必要です。
「ERA エージェント」のインストールについては『ESET Remote Administrator ユーザーズマニュアル』の「4.2.2　ERA エージェントの展開」を参照してください。

Chapter 4 ESET Endpoint アンチウイルス for OS X の使い方

この章では、コンピューターの検査、ESET Endpoint アンチウイルス for OS X の設定、ツール類の使い方について説明します。

4.1 コンピューターの検査

「コンピュータの検査」はコンピューター上のファイルやフォルダーの検査を実施します。感染が疑われるときだけコンピューターの検査を実行するのではなく、通常のセキュリティ対策の一環として定期的（1 か月に 1 回など）に実行することが重要です。

「コンピュータの検査」を行うと、「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る場合、ウイルス定義データベースが古い場合、ファイルをディスクに保存したときにウイルスが検出されなかった場合など、リアルタイムに検出されなかったウイルスを検出することができます。

「コンピュータの検査」は、スマート検査、カスタム検査、リムーバブルメディア検査の 3 種類の方法があります。リアルタイムファイルシステム保護については「4.3.1 コンピュータ」を参照してください。

! 重 要

コンピューターの検査は最低でも 1 か月に 1 回は実行することをお勧めします。メインメニューの［ツール］>［スケジューラー］で、コンピューターの検査をタスクとして設定できます。設定方法については「4.4.3 スケジューラー」を参照してください。

4.1.1 スマート検査

スマート検査は、コンピューターの検査を行い、感染しているファイルからウイルスを自動的に駆除します。「スマート検査」をクリックするだけで、詳細な検査パラメーターの設定を行うことなく、ローカルドライブにあるすべてのファイル検査が実行されます。駆除レベルは既定で設定されていますが、変更することができます。駆除レベルについては、「4.6.3 リアルタイムファイルシステム保護」の「●駆除」を参照してください。

4.1.2 カスタム検査

カスタム検査は、検査対象や検査方法など検査パラメーターを指定する検査方法です。設定した検査パラメーターは、ユーザー定義の検査プロファイルに保存できます。検査プロファイルに保存しておくと、同じパラメーターで繰り返し検査を実行できます。

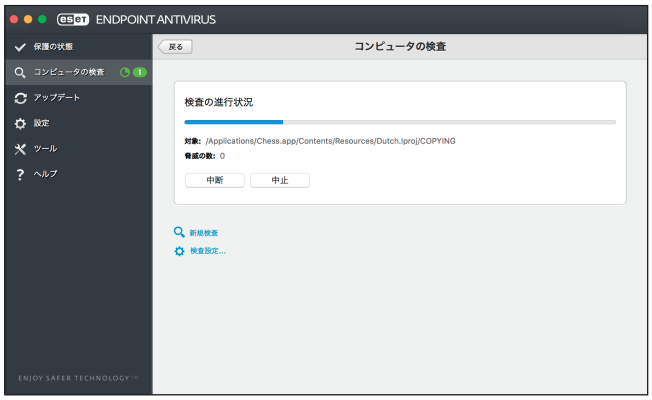
■カスタム検査の設定

［カスタム検査］をクリックすると、「カスタム検査」画面が表示され検査の対象を選択することができます。

❶	**検査プロファイル**	検査で使用するプロファイルを選択できます。既定のプロファイルは［スマート検査］です。さらに、［コンテキストメニューの検査］および［詳細検査］を指定できます。それぞれのプロファイルで、様々な ThreatSense エンジンパラメーターを設定して保存することができます。	
❷	**検査の対象**	あらかじめ定義されている検査対象を選択するか、ツリー構造内から検査対象を選択します。	
		プロファイル設定によって	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 メモリー、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。
		ネットワークメディア	マッピングされたネットワークドライブをすべて選択します。
		選択肢なし	選択した検査対象をキャンセルします。
❸	**設定**	［検査プロファイル］で選択した検査プロファイルの詳細を設定します。「その他」セクションで使用できる機能については、「4.6.3　リアルタイムファイルシステム保護」の「■ ThreatSense エンジン」を参照してください。	
❹	**検査対象の指定**	検査対象として指定するパスを直接入力します。 ツリー構造内で対象を選択しておらず、［検査の対象］ドロップダウンメニューで［選択なし］を選択している場合のみです。	
❺	**駆除せずに検査する**	感染しているファイルやフォルダーが自動的に駆除されず、現在の保護状態の概要が表示されます。感染しているファイルやフォルダーを駆除する必要がない場合は、［駆除せずに検査する］をチェックします。	
❻	**保存**	設定した検査パラメーターを保存すると、後で検査を行うときに使用できます。検査対象や検査方法、その他のパラメーターなど、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。	
❼	**検査後にコンピューターをシャットダウン**	検査が終了したら、パソコンを自動でシャットダウンします。検査完了と同時にパソコンをシャットダウンしたいときは、［検査後にコンピューターをシャットダウン］をチェックします。	
❽	**検査**	設定したカスタムパラメーターを使用して検査を実行します。	

4.1.3 検査の進行状況

「検査の進行状況」画面には、検査の現状および検出したファイル数に関する情報が表示されます。



!重 要

システム専用ファイルなど、一部のファイルは検査できませんが、エラーではありません。

検査の進行状況	すでに検査した対象の割合が進行状況バーに表示されます。検査の進行状況は、検査対象の総数から求められます。
対象	現在検査している対象の名前と保存場所が表示されます。
脅威の数	検出された脅威の総数が表示されます。
中断	検査を中断します。
再開	検査を続行します。［再開］は検査を中断した場合に表示されます。
中止	検査を終了します。

4.1.4 クイックリンク

クイックリンクには、［詳細検査］や［リムーバブルメディア検査］、［最後に使用した検査を実行］、［定期的な検査をスケジュール］などの項目が準備されています。

■詳細検査

［詳細検査］をクリックすると、詳細検査が実行されます。スマート検査では、シンボリックリンクや自己解凍形式、圧縮された実行形式などを対象に検査が実行されますが、詳細検査では、これらに加えて、電子メールファイルやアーカイブなどの検査も行われます。詳細検査は、より詳細な検査を実行したいときに利用します。

■リムーバブルメディア検査

［リムーバブルメディア検査］をクリックすると、USB メモリーや USB 接続の HDD などのリムーバブルメディアを対象にスマート検査と同じように検査が実行されます。この項目は、光学ドライブにディスクがセットされていたり、USB メモリーに接続されていたり場合など、リムーバブルメディアが利用可能な場合にのみ利用できます。
リムーバブルメディア検査は、［カスタム検査］をクリックし、［検査の対象］ドロップダウンメニューから［リムーバブルメディア］を選択して［検査］をクリックして実行することもできます。

■最後に使用した検査を実行

［最後に使用した検査を実行］をクリックすると、最後に使用した検査を実行します。最後に利用した検査をそのままの設定で実行したいときに利用します。

■定期的な検査をスケジュール

［定期的な検査をスケジュール］をクリックすると、「タスクの追加」画面が表示され、特定の曜日や日時などに自動実行する検査を作成できます。設定の詳細のついては、「4.4.3　スケジューラー」をご参照ください。

4.1.5　検査設定

検査プロファイルは、検査について目的の基本設定を保存して、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。検査プロファイルの設定の変更や新規の検査プロファイルの作成は、［検査設定］をクリックすることで行えます。

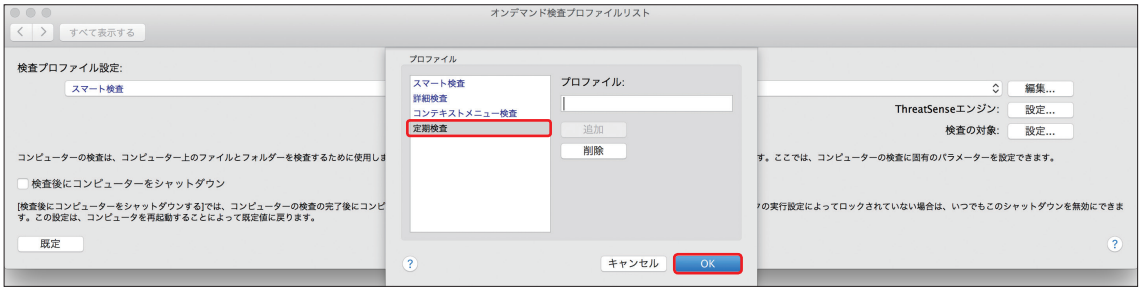
検査プロファイル設定	設定を行うプロファイルを選択できます。
編集	プロファイルの作成や削除などを行えます。既定値では、「スマート検査」「詳細検査」「コンテキストメニュー検査」の 3 つのプロファイルが用意されていますが、それ以外に独自の検査プロファイルを作成したいときに利用します。
ThreatSense エンジンの［設定］	選択した検査プロファイルを利用して、検査を行うときの詳細な設定を行えます。設定されている内容は、プロファイルごとに異なります。設定の詳細については、「4.6.3　リアルタイムファイルシステム保護」の「■ ThreatSense エンジン」を参照してください。
検査の対象の［設定］	選択した検査プロファイルで検査を行うファイルやフォルダーを設定できます。
検査後にコンピューターをシャットダウン	タスクが完了したらコンピューターの電源を自動的にシャットダウンしたいときにチェックを入れます。

■検査プロファイルを作成する

独自の検査プロファイルを作成する手順は、次のとおりです。

操作手順

1. ［検査設定］をクリックします。
2. ［編集］ボタンをクリックします。
3. プロファイルにプロファイル名を入力して、［追加］ボタンをクリックします。
4. プロファイルが追加されます。［OK］ボタンをクリックします。



5. 検査プロファイル設定で作成したプロファイルを選択します。
6. ThreatSense エンジンの［設定］ボタンをクリックし、検査に関する各種設定を行います。設定の詳細については、「4.6.3　リアルタイムファイルシステム保護」の「■ ThreatSense エンジン」を参照してください。
7. 検査の対象の［設定］ボタンをクリックし、検査対象のファイルやフォルダーを設定します。

4.2 アップデート

ESET Endpoint アンチウイルス for OS X はウイルス定義データベースのアップデートで、常に最新の状態を保つことができます。

メインメニューの［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。また、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。ウイルス定義データベースのバージョンは、ESET 製品の Web サイトへのリンクになっており、クリックするとアップデートで追加されたすべてのウイルス定義データベースの一覧が表示されます。
また、［ウイルス定義データベースをアップデートする］をクリックして、アップデートを手動で開始することもできます。

! 重 要

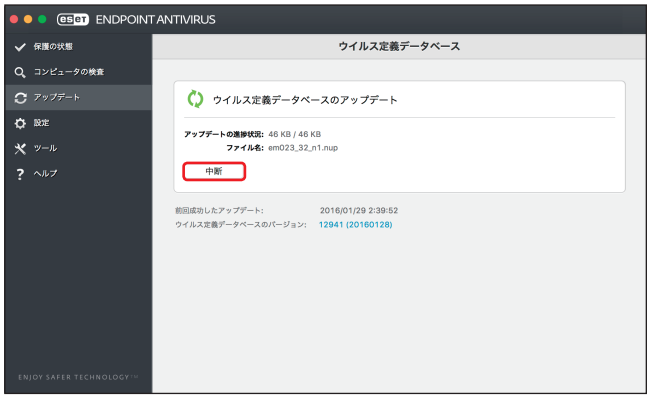
ウイルス定義データベースのアップデートは、悪意のあるコードからコンピューターを保護するための重要な機能です。設定や操作には注意してください。

! 重 要

ESET Endpoint アンチウイルス for OS X のインストール時にアクティベーションしなかった場合は、アップデート時に［製品のアクティベート］をクリックして製品認証キーを入力すると、ESET のアップデートサーバーにアクセスすることができます。

アップデートのプロセス

［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、アップデートが始まります。アップデートを中断するには、［中断］をクリックします。



アップデートの終了

通常の状況では、アップデートが正常に終了すると、「アップデート」画面に「アップデートは必要ありません。インストールされている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。表示されない場合は、ウイルス定義データベースが古い状態のままで、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。

アップデートの失敗

アップデート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。」**

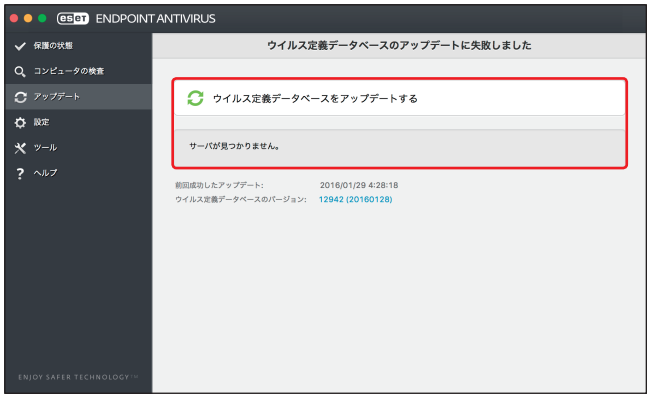
ウイルス定義データベースのアップデートに複数回失敗すると表示されます。アップデートの設定をチェックすることをお勧めします。失敗の原因として最も多いのは、製品認証キーが正しく入力されていない、またはインターネット接続設定が適切ではないことです。
このメッセージは、アップデートの失敗に関する次の 2 つのメッセージ（ウイルス定義データベースのアップデートはエラーのため終了しました）に関連します。

- **「ウイルス定義データベースのアップデートに失敗しました - アクティベーションされていません。」**

アップデート設定で製品認証キーが正しく入力されていないため、ライセンスが無効になっています。製品認証キーを確認して、メニューバーのアイコンをクリックし、［製品のアクティベーション］をクリックして、製品認証キーを入力してください。

- **「ウイルス定義データベースのアップデートに失敗しました - サーバが見つかりません。」**

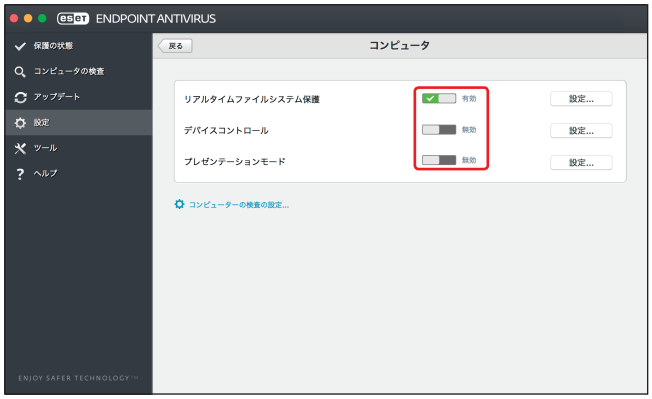
インターネット接続の設定が正しくない可能性があります。Web ブラウザーで任意の Web サイトを表示するなどして、インターネット接続が正しく設定されているか確認してください。Web サイトが表示されない場合は、インターネット接続が確立されていないか、コンピューターの接続に問題がある可能性があります。ご利用のインターネットサービスプロバイダー（ISP）に、有効なインターネット接続があるかどうか確認してください。



4.3 設定

ESET Endpoint アンチウイルス for OS X の設定オプションを使用すると、コンピューター、ネットワーク、Web とメールの保護レベルを調整することができます。それぞれの項目をクリックすると、対応する保護機能の詳細を設定できます。

個別の機能を一時的に無効にするには、機能名の左側にある をクリックします。ただし、無効にすると、コンピューターのセキュリティレベルが低下する可能性がありますので注意してください。
無効な機能を再度有効にするには、 をクリックして に戻します。



4.3.1 コンピュータ

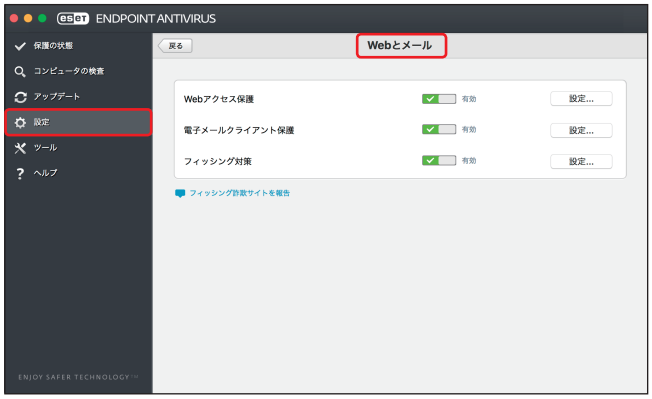
リアルタイムファイルシステム保護	ファイルの読み込み、作成、実行時に、脅威がないか検査します。すべてのファイルが対象になります。
デバイスコントロール	USB メモリーや USB 接続の HDD、光学ドライブ、メモリーカード、イメージングデバイスなどの各種機器の利用を制限したいときに使用します。USB メモリーや USB 接続の HDD、光学ドライブ、メモリーカードなどのストレージ機器では、読み出しのみ許可、読み出し / 書き込みの両方を許可、すべて拒否などの設定が行えます。
プレゼンテーションモード	ソフトウェアを中断したくないとき、ポップアップウインドウを表示させたくないとき、CPU の使用量を最小化したいときなどに使用します。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存在するため、メイン画面がオレンジ色になり、警告が表示されます。

コンピュータの検査の設定

コンピューターの検査（手作業で実行する検査）のパラメーターを調整します。

詳細な設定は、「4.6.7 コンピューターの検査」を参照してください。

4.3.2 Web とメール



Web アクセス保護	HTTP 経由のすべての通信トラフィックで、悪意のあるソフトウェアを検査します。
電子メールクライアント保護	POP3 と IMAP プロトコル経由の通信トラフィックで、悪意のあるソフトウェアの検査を行います。
フィッシング対策	パスワード、金融データ、その他の機密データを収集する目的で偽装した、非合法の Web サイトへのアクセスをブロックします。

フィッシング詐欺サイトを報告

フィッシング詐欺サイトの報告用 Web ページが表示されます。フィッシング詐欺サイトを発見したときは、ここから報告できます。

4.3.3 設定のインポート／エクスポート

xml 形式のファイルを使用して、ESET Endpoint アンチウイルス for OS X の設定をインポートまたはエクスポートできます。設定を後で復元できるように現在の設定をバックアップする場合や、同じ設定内容を複数のコンピューターに適用する場合などに便利です。

■設定のインポート

「設定」画面で［設定のインポート／エクスポート］＞［設定のインポート］を選択します。「ファイル名」フィールドに設定ファイルのファイル名を入力するか、［参照］をクリックしてインポートする設定ファイルを指定して［OK］をクリックします。

■設定のエクスポート

「設定」画面の［インポート／エクスポート］＞［設定のエクスポート］を選択します。「ファイル名」フィールドに設定ファイルの保存場所とファイル名（config など）を入力するか、［参照］をクリックしてファイル名を入力して、保存先のフォルダーを選択し、［OK］をクリックします。

！重　要

エクスポートしたファイルを指定したフォルダーに書き込む権限がない場合は、エクスポート中にエラーが表示されることがあります。

4.3.4 すべての設定を既定値に戻す

ESET Endpoint アンチウイルス for OS X のすべての設定を既定値にすることができます。各種設定を既定値に戻すときは、［設定］画面の［すべての設定を既定値に戻す］をクリックし、ダイアログボックスが表示されたら、［OK］ボタンをクリックします。

4.3.5 詳細設定を表示する

ESET Endpoint アンチウイルス for OS X の各種設定は、［詳細設定］画面から行えます。「詳細設定」画面を表示したいときは、［設定］画面の［詳細設定を表示する］をクリックします。

保護	「保護」セクションでは、コンピューターの保護に関する各種設定が行えます。	
	一般	スキャナオプションなど、すべての保護機能に共通の設定が行えます。詳細については、「4.6.1 一般」を参照してください。
	スタートアップ保護	システム起動時やウイルス定義データベースのアップデート時に実行される検査に関しての設定が行えます。詳細については、「4.6.2 スタートアップ保護」を参照してください。
	リアルタイムファイルシステム保護	リアルタイムファイルシステム保護に関する設定が行えます。詳細については、「4.6.3 リアルタイムファイルシステム保護」を参照してください。
	電子メール保護	電子メール保護に関する設定が行えます。詳細については、「4.6.4 電子メール保護」を参照してください。
	Web アクセス保護	Web アクセス保護に関する設定が行えます。詳細については、「4.6.5 Web アクセス保護」を参照してください。
	フィッシング対策	フィッシング対策に関する設定が行えます。詳細については、「4.6.6 フィッシング対策」を参照してください。
	コンピューターの検査	コンピューターの検査に関する設定が行えます。詳細については、「4.6.7 コンピューターの検査」を参照してください。

アクセス制御	「アクセス制御」セクションでは、USB メモリーなどのデバイスの制御に関する設定が行えます。	
	デバイスコントロール	USB メモリーやメモリーカードなどのデバイスの利用をコントロールするための設定が行えます。詳細については、「4.6.8 デバイスコントロール」を参照してください。
ツール	「ツール」セクションでは、ログファイルやスケジューラー、ESET LiveGrid、権限、プレゼンテーションモードなどに関する設定が行えます。	
	ログファイル	ログファイルの保存期間などの設定が行えます。詳細については、「4.6.9 ログファイル」を参照してください。
	スケジューラー	システムタスクの表示 / 非表示の切り替えを行えます。詳細については、「4.6.10 スケジューラー」を参照してください。
	ESET LiveGrid	ESET LiveGrid に関する設定が行えます。詳細については、「4.6.11 ESET LiveGrid」を参照してください。
	権限	ESET Endpoint アンチウイルス for OS X の各種設定を行える権限ユーザーの追加や削除などが行えます。権限ユーザーの登録方法の詳細については、「3.5 設定の保護」を参照してください。
	プレゼンテーションモード	プレゼンテーションモードに関する設定が行えます。詳細については、「4.6.13 プレゼンテーションモード」を参照してください。
ユーザー	「ユーザー」セクションでは、ユーザーインターフェースや通知、コンテキストメニューなどに関する設定が行えます。	
	インターフェース	ESET Endpoint アンチウイルス for OS X のメイン画面に関する設定が行えます。詳細については、「4.6.14 インターフェース」を参照してください。
	警告と通知	脅威が検出されたときに警告ウインドウを表示したり、デスクトップに通知を表示するかどうかなどの設定が行えます。詳細については、「4.6.15 警告と通知」を参照してください。
	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または右クリックに相当する操作を行ったときに表示されるコンテキストメニューに関する設定を行えます。詳細については、「4.6.16 コンテキストメニュー」を参照してください。
その他	「その他」セクションでは、アップデートやプロキシサーバー、共有ローカルキャッシュなどに関する設定が行えます。	
	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利用するアップデートサーバーに関する設定が行えます。詳細については、「4.6.17 アップデート」を参照してください。
	プロキシサーバー	プロキシサーバーに関する設定が行えます。詳細については、「3.4 プロキシサーバーの設定」を参照してください。
	共有ローカルキャッシュ	共有ローカルキャッシュに関する設定が行えます。詳細については、「4.6.19 共有ローカルキャッシュ」を参照してください。

4.4 ツール

ツールには、ESET Endpoint アンチウイルス for OS X を管理するための機能や上級ユーザー向けのオプション機能などが用意されています。

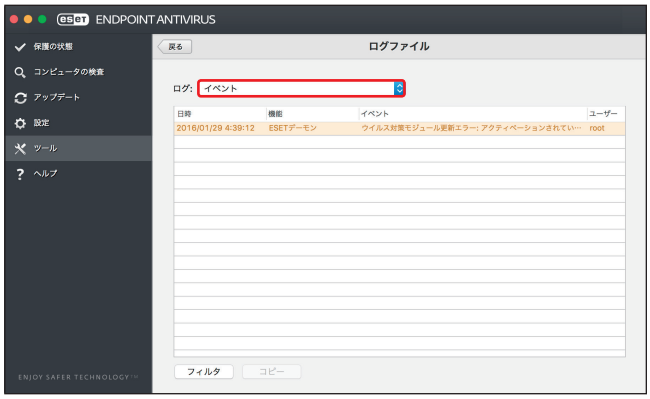
4.4.1 ログファイル

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記録されるため、検出されたウイルスの概要を確認できます。ログは、システムの分析、ウイルスの検出、トラブルシューティングの重要なツールとして使用できます。

ログへの記録はバックグラウンドで実行され、ユーザーの操作を必要としません。

ログに記録された情報は、ESET Endpoint アンチウイルス for OS X で表示できます。また、ログファイルのエクスポートもできます。

■ログファイルの確認



ログファイルを確認するには、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。確認できるログの種類は次のとおりです。

検出された脅威	ESET Endpoint アンチウイルス for OS X で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。記録される情報は、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などです。
イベント	ESET Endpoint アンチウイルス for OS X によって実行された、重要なアクション、発生したイベントや、エラーに関する情報がすべて記録されています。ESET Endpoint アンチウイルス for OS X で問題が発生したときは、「イベントログ」の情報から、問題点を確認できる場合があります。
コンピュータの検査	ESET Endpoint アンチウイルス for OS X によって実行されたクライアントコンピューターの検査結果が記録されています。ログは検査したフォルダーごとに記録されます。ログをダブルクリックすると、詳細が別画面で表示されます。
デバイスコントロール	コンピューターに接続されたリムーバブルメディアなどのデバイスの情報が記録されています。ログに記録されるのは、デバイスコントロールルールに一致するデバイスのみで、一致しない場合は記録されません。記録される情報は、デバイスタイプ、シリアル番号、ベンダー名、メディアのサイズなどです。
フィルタリングされた Web サイト	Web アクセス保護または Web コントロールによってブロックされた Web サイトが記録されています。Web サイトへのアクセスを試みた時刻、URL、ユーザー、アプリケーションを確認できます。

■ログの操作

ログを選択して【command】キーと【C】キーを押すと、画面に表示されている情報をクリップボードにコピーできます。【command】キーまたは【shift】キーを押しながらログをクリックすると、複数のログを選択できます。

［フィルタ］ボタンをクリックすると、フィルタリング条件を定義できる「ログのフィルタ」画面が表示されます。

ログを【control】キーを押しながらクリックするとコンテキストメニューが表示され、次の機能を実行できます。

表示	選択したログの詳細画面が表示されます（一部の種類のログのみ）。
同じタイプのフィルターレコード	同じタイプ（診断、警告など）の情報だけが表示されるようになります。
フィルタ	「ログのフィルタ」画面が表示され、ログのフィルタリング条件を定義できます。
フィルタを無効にする	「ログのフィルタ」画面の設定を無効にします。
フィルタをクリア	「ログのフィルタ」画面の設定をクリアします。
コピー／すべてコピー	選択したログまたはすべてのログ情報をクリップボードにコピーします。
削除／すべて削除	選択したログまたはすべてのログを削除します。ログを削除するには、管理者権限が必要です。
エクスポート／すべてエクスポート	選択したログまたはすべてのログをテキスト形式のファイルにエクスポートします。

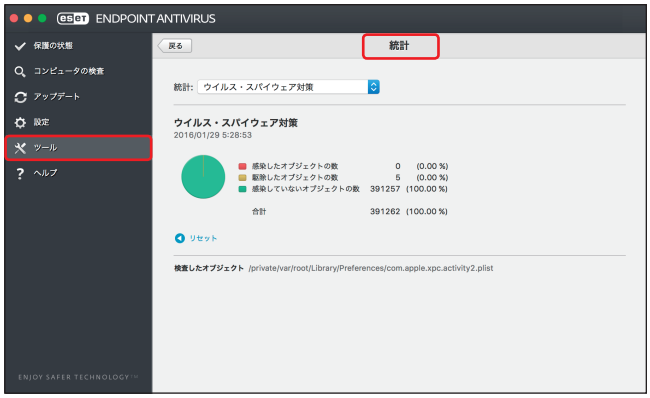
■ログのフィルタ／検索

ログには、重要なシステムイベントに関する情報が記録されます。ログのフィルタ機能では、条件を指定して特定の種類のログのみを絞り込み表示できます。ログのフィルタ機能を使用するには、［フィルタ］ボタンをクリックするか、ログを【control】キーを押しながらクリックし、［フィルタ］をクリックします。

ログのフィルタ

4.4.2 統計

統計では、ESET Endpoint アンチウイルス for OS X の保護機能に関連する統計データをグラフで確認できます。
統計を表示するには、メインメニューの［ツール］>［統計］をクリックします。



ドロップダウンメニューから保護機能を選択すると、選択した保護機能のグラフと凡例が表示されます。凡例の項目にカーソルを合わせると、その項目のデータのみがグラフに表示されます。
グラフを表示できる保護機能は次のとおりです。

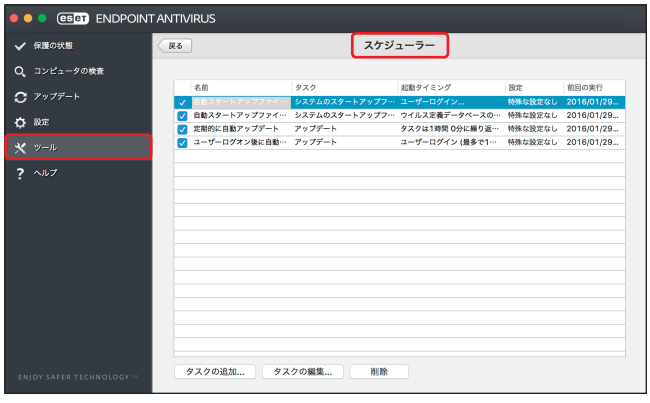
ウイルス・スパイウェア対策	感染したオブジェクト及び駆除したオブジェクトの数や感染していないオブジェクトの数を表示します。ウイルス・スパイウェア対策に表示される情報は、「コンピューターの検査」「リアルタイムファイルシステム保護」「電子メールクライアント保護」「Web アクセス保護」の 4 つの保護機能の全体の統計データとなります。
コンピューターの検査	オンデマンド検査によって検出された感染したオブジェクト及び駆除したオブジェクトの数と感染していないオブジェクトの数を表示します。
リアルタイムファイルシステム保護	読み込まれたオブジェクト、またはファイルシステムに書き込まれたオブジェクトの中で、感染したオブジェクト及び駆除したオブジェクトの数や感染していないオブジェクトの数を表示します。
電子メールクライアント保護	電子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中で感染したオブジェクト及び駆除したオブジェクトの数や感染していないオブジェクトの数を表示します。
Web アクセス保護	Web ブラウザーによってダウンロードされたオブジェクトの中で、感染したオブジェクト及び駆除したオブジェクトの数や感染していないオブジェクトの数を表示します。

統計グラフの横には、検査済みオブジェクト数、感染したオブジェクト数、駆除したオブジェクト数、未感染のオブジェクト数が表示されます。［リセット］をクリックすると、表示中の保護機能の統計情報が削除されます。

4.4.3 スケジューラー

スケジューラーは、実行時間や実行するアクションなどをタスクとして登録し、自動で定期的にタスクを実行する機能です。

スケジューラーを設定するには、メインメニューの［ツール］>［スケジューラー］をクリックします。
スケジューラーには、登録されているタスクの設定内容（タスクのタイプ、名前、実行のタイミングなど）が一覧で表示されます。



［タスクの追加］、［タスクの編集］、［削除］をクリックすると、タスクの追加、編集、削除ができます（「■新しいタスクの追加」参照）。

【control】キーを押しながらタスクをクリックすると、コンテキストメニューが表示され、次の機能を実行できます。

- タスクの詳細を表示（「■タスクの詳細確認」参照）
- 今すぐ実行
- 追加
- 編集
- 削除

タスクの有効／無効を設定するには、各タスクのチェックボックスをオン／オフにします。

既定では、次のタスクが登録されています。

- 定期的に自動アップデート
- ユーザーログオン後に自動アップデート
- 自動スタートアップファイルのチェック（ユーザーのログオン後）
- 自動スタートアップファイルのチェック（ウイルス定義データベースのアップデート後）

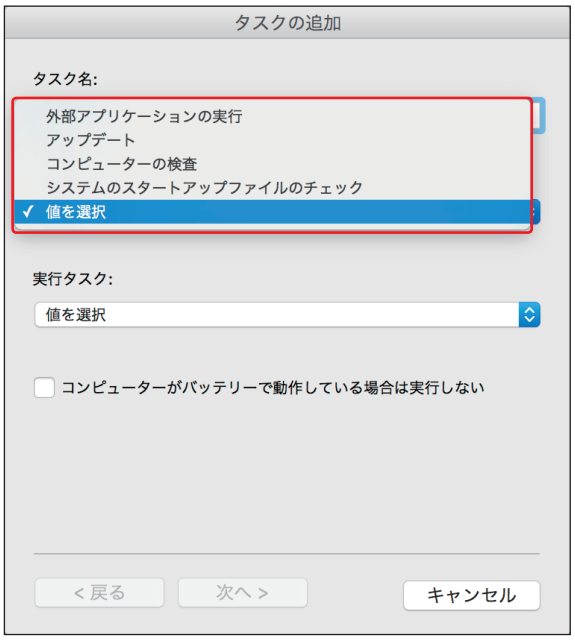
■新しいタスクの追加

次の 4 種類のタスクを追加することができます。

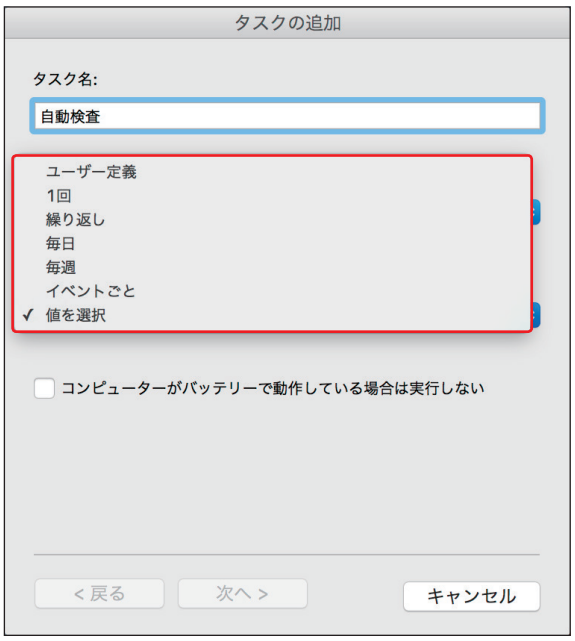
外部アプリケーションの実行	外部アプリケーションを実行します。
アップデート	ウイルス定義データベースおよびプログラムコンポーネントをアップデートします。
コンピューターの検査	コンピューター上のファイルやフォルダーを検査します。
システムスタートアップファイルのチェック	システムの起動時またはログイン時に実行されるファイルを検査します。

操作手順

1. ［タスクの追加］をクリックします。
2. タスク名を入力します。
3. 「タスクの種類」ドロップダウンメニューから目的のタスクを選択します。



4. ドロップダウンメニューからタスクを実行するタイミングを選択します。



続く

ユーザー定義	ユーザーが定義したルールによってタスクを実行します。
1 回	指定した日時にタスクを実行します。
繰り返し	指定した間隔でタスクを繰り返し実行します。
毎日	毎日指定した時刻にタスクを実行します。
毎週	毎週指定した曜日と時刻にタスクを実行します。
イベントごと	次のいずれかのイベントの発生時にタスクを実行します。 • ESET 製品プログラムが起動されるたび • その日に初めて ESET 製品プログラムが起動されるとき • ウイルス定義データベースのアップデート • ユーザーログイン • 脅威の検出 • ファイルが検査されなかったとき 詳細は「■タスク開始のタイミング－イベントのトリガー」を参照してください。

5 バッテリー電源で動作しているノートパソコンなどで、システムリソースを最小化するためにタスクを実行しないようにする場合は、［コンピューターがバッテリーで動作している場合は実行しない］を有効にします。

6 ［次へ］をクリックします。

続く

7 各項目を設定します。表示される項目は、手順❸で選択した「タスクの種類」によって変わります。

- **［外部アプリケーションの実行］を選択した場合**

アプリケーション	実行するアプリケーションをフルパスで入力し、必要に応じてコマンドラインパラメーターも入力します。［参照］ボタンをクリックすると、Finder を利用して実行するアプリケーションを選択できます。
ファイルパッケージをディレクトリとして表示	ファイルパッケージをディレクトリとして表示したいときは、このチェックをオンにします。

- **［コンピューターの検査］を選択した場合**

続く

プロファイルの選択	検査に利用するプロファイルを選択します。[スマート検査] [詳細検査] [コンテキストメニュー検査] の中から選択できます。それぞれのプロファイルで、様々な ThreatSense エンジンパラメーターを設定できます。ThreatSense エンジンパラメーターの詳細については、「4.6.3 リアルタイムファイルシステム保護」の「■ ThreatSense エンジン」を参照してください。
検査の対象	ツリー構造内から検査対象とするフォルダーを選択します。
駆除せずに検査する	感染しているファイルやフォルダーが自動的に駆除されず、現在の保護状態の概要が表示されます。感染しているファイルやフォルダーを駆除する必要がない場合は、[駆除せずに検査する] をチェックします。
タスクの完了時にコンピュータをシャットダウン	タスクが完了したらコンピューターの電源を自動的に切断したいときにチェックを入れます。このオプションにチェックを入れた場合は、[シャットダウンをキャンセルできません] のオプションも選択できます。[シャットダウンをキャンセルできません] にチェックを入れると、シャットダウン処理をキャンセルできなくなります。

8 タスクの実行時刻を指定します。

設定内容は、手順4で設定したタスクのタイミングによって異なります。

9 [次へ] をクリックします。

10 指定した時刻にタスクが実行されなかった場合に、タスクを再度実行するタイミングを選択します。

次のスケジュール設定日時まで待機	次のスケジュール設定日時に実行されます（24 時間後など）。
実行可能になり次第実行する	タスクの実行を妨げている原因が解消され次第実行されます。
前回実行されてから次の時間が経過した場合は直ちに実行する	指定した時間が経過するとタスクが再度実行されます。 「前回実行からの時間（時間）」で時間を設定します。

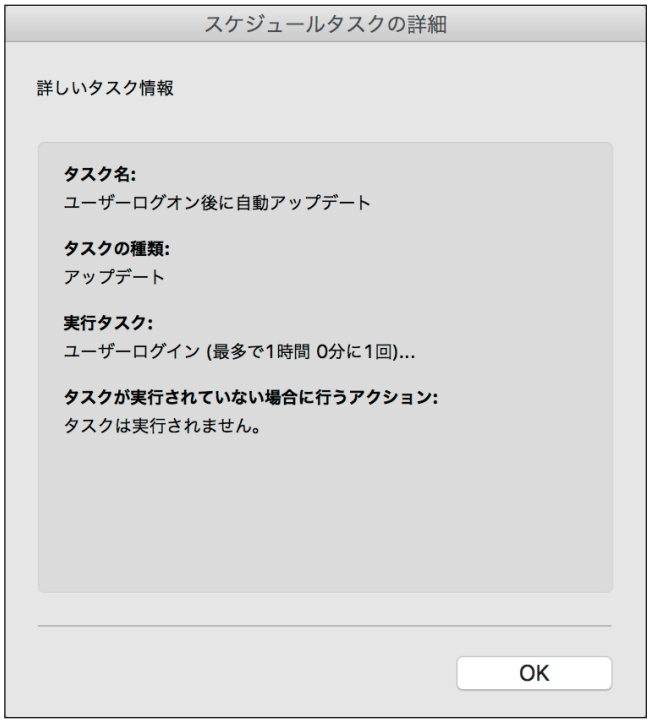
続く

11 タスクの優先度を設定します。この項目は、［システムのスタートアップファイルのチェック］を選択した場合にのみ表示されます。

12 ［終了］をクリックします。

■タスクの詳細確認

タスクをダブルクリックするか【control】キーを押しながら右クリックして［タスクの詳細を表示］をクリックすると、タスクの詳細を確認できます。



■タスク開始のタイミング－イベントのトリガー

手順❹でタスクを実行するタイミングに［イベントごと］を選択したときは、次のいずれかのイベントによってタスクを開始できます。

- ESET 製品プログラムが起動されるたび
- その日に初めて ESET 製品プログラムが起動されるとき
- ウイルス定義データベースのアップデート
- ユーザーログイン
- 脅威の検出
- ファイルが検査されなかったとき

イベントによって開始されるタスクをスケジュールする際には、タスクを実行する最短間隔を指定することができます。例えば、1 日に複数回クライアントコンピューターにログオンする場合、その日および翌日の初回ログオン時にのみタスクを実行するには、「その日に初めて ESET 製品プログラムが起動されるとき」を選択します。

■タスク開始のタイミング－ユーザー定義

手順❹でタスクを実行するタイミングに［ユーザー定義］を選択したときは、以下のフォーマットでユーザーがタイミングを定義できます。

[ユーザー定義タスク] の日付および時刻は、4 桁の西暦での cron フォーマット (スペース区切りの 6 つのフィールドで構成される文字列) で入力します。曜日名（Monday-Sunday）と月名（January-December）はサポートされていません。

分（ 0- 59）時（ 0- 23）日（ 1- 31）月（1- 12）年（ 1970- 2099）曜日（ 0- 7）(日曜 = 0 または 7)

例 :2016 年 3 月 22 日（火曜日）6 時 30 分を指定する場合
30 6 22 3 2016 2

次の特殊文字が cron 式でサポートされています。

- アスタリスク (*) は、フィールドのすべての値に一致します。たとえば、3 つ目のフィールド (日) にアスタリスクがある場合、毎日となります。
- ハイフン (-) は、範囲を指定します。
- カンマ (,) は、リストの項目を区切ります。
- スラッシュ (/) は、範囲の増分を定義します。

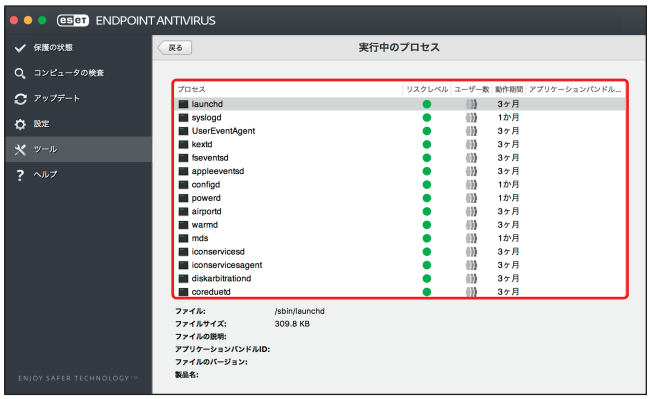
たとえば、3 つ目のフィールド (日) に「3-28/5」と入力すると、毎月 3 ～ 28 日の間で、3 日から 5 日ごとに実行されます。

! 重　要

日および曜日の両方を定義すると、コマンドは両フィールドが一致するときのみに実行されます。

4.4.4 実行中のプロセス

実行中のプロセスは、クライアントコンピューター上で実行中のプログラムまたはプロセスを表示し、新規のウイルスを即座に ESET に通知し、その通知を継続します。ESET Endpoint アンチウイルス for OS X 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 技術でクライアントコンピューターを保護します。
実行中のプロセスを表示するには、メインメニューの［ツール］>［実行中のプロセス］をクリックします。
ESET LiveGrid が無効になっている場合、「実行中のプロセス」は表示されません。
ESET LiveGrid の設定については、「4.6.11 ESET LiveGrid」を参照してください。



「実行中のプロセス」画面には、次の情報が表示されます。

プロセス	クライアントコンピューターで現在実行中のプログラムまたはプロセスのイメージ名が表示されます。
リスクレベル	ESET Endpoint アンチウイルス for OS X および ESET Live Grid 技術が、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をランク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）に危険レベルを割り当てます。危険レベルには「1：良好（緑）」から「9：危険（赤）」のレベルがあります。
ユーザー数	アプリケーションを使用するユーザーの数が表示されます。「ユーザー数」は、ESET Live Grid 技術によって収集されます。
検出の時間	ESET Live Grid 技術によってアプリケーションが発見されてからの期間が表示されます。
アプリケーションハンドル ID	ベンダープログラムまたはアプリケーションプロセスの名前が表示されます。

ワンポイント
「リスクレベル」に「オレンジ」（不明）が表示されていても、必ずしも悪意のあるアプリケーション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、「オレンジ」（不明）が表示されます。

ワンポイント
「リスクレベル」に「緑」（良）のマークが付いた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。検査から除外するのは、「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。

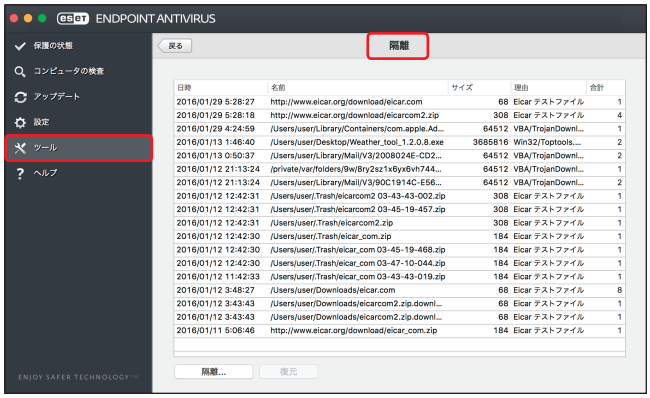
一覧からプロセスをクリックすると、次の情報がウインドウ下部に表示されます。

ファイル	クライアントコンピューター上のアプリケーションの場所が表示されます。
ファイルサイズ	ファイルサイズが KB（キロバイト）または MB（メガバイト）のどちらかの単位で表示されます。
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の特性が表示されます。
アプリケーションハンドル ID	ベンダーまたはアプリケーションプロセスの名前が表示されます。
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に基づくファイルのバージョンが表示されます。
製品名	アプリケーション名および商号が表示されます。

4.4.5 隔離

隔離の主な目的は、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、またはファイルの削除が危険で推奨されない場合は、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。ファイルの動作が疑わしいにもかかわらず、ウイルス対策機能によって検出されない場合は、隔離機能の使用をお勧めします。隔離したファイルは、分析のために ESET のウイルスラボに提出できます。
隔離ファイルの一覧を表示するには、メインメニューの［ツール］>［隔離］をクリックします。



「隔離」画面には、隔離フォルダーに保存されているファイルが一覧で表示されます。一覧には隔離した日時、隔離したファイルの元の場所のパス、ファイルサイズ（バイト単位）、隔離した理由（「ユーザーによって追加」など）、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）が表示されます。

■ファイルの隔離

ウイルス検出によって削除されたファイルは、警告画面でユーザーが隔離を無効にしない限り自動的に隔離されます。[隔離］ボタンをクリックすると、不審なファイルを手動で隔離できます。隔離したファイルは元の場所から削除されます。

■隔離フォルダーからの復元

隔離されているファイルを、元の場所に復元できます。隔離されているファイルを復元するには、一覧でファイルを選択して［復元］ボタンをクリックするか、一覧で【control】キーを押しながらファイルをクリックして［復元］をクリックします。また、一覧で【control】キーを押しながらファイルをクリックして［復元先を指定］をクリックすると、隔離される前の場所とは異なる場所にファイルを復元できます。

！重　要

害のないファイルが誤って隔離された場合は、ファイルを復元した後で検査から除外することができます。除外の設定については、「4.6.1　一般」の「●除外設定」を参照してください。

■隔離フォルダーからの削除

一覧で【control】キーを押しながらファイルをクリックして［削除］をクリックすると、隔離フォルダーから隔離されたファイルを削除できます。複数のファイルを選択して、一度に削除することもできます。

■隔離からのファイルの提出

ウイルス対策機能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、またはファイルが脅威として誤って検出されて隔離された場合は、ファイルを ESET のウイルスラボに送信することができます。隔離フォルダーからファイルを提出するには、【control】キーを押しながらファイルをクリックし、［分析のためにサンプルを提出］をクリックします。

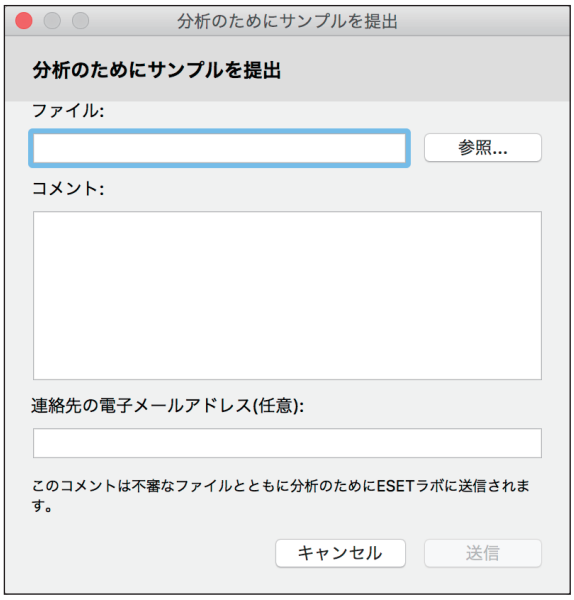
4.4.6　分析のためにサンプルを提出

クライアントコンピューター上での動作が疑わしいファイルや、インターネット上で疑わしいサイトが見つかった場合は、ファイルまたは Web サイトを ESET のウイルスラボに提出して解析を受けることができます。解析の結果、悪意のあるアプリケーションや Web サイトであることが判明すると、以降のウイルス定義データベースに検出結果が追加されます。

分析用ファイルを ESET に提出する手順は、次のとおりです。

操作手順

1. メインメニューの［ツール］>［分析のためにサンプルを提出］をクリックします。
「分析のためにサンプルを提出」画面が表示されます。



続く

2 ［参照 ...］ボタンをクリックして提出したいファイルを選択し、［選択］ボタンをクリックします。

3 「コメント」欄に症状やファイルの動作など詳細説明を入力します。

ワンポイント

コメントは本製品の開発元である ESET 社へ直接送られます。英語以外のコメント内容は ESET 社で確認できない可能性がありますので、あらかじめご了承ください。

4 「連絡先の電子メールアドレス」に連絡先のメールアドレスを入力します。

電子メールアドレスの入力は任意です。解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します。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。

5 ［送信］ボタンをクリックします。

! 重　要

ESET に分析用ファイルを提出する前に、次の基準を 1 つ以上満たしていることを確認してください。
・ファイルまたは Web サイトがまったく検出されない。
・ファイルまたは Web サイトが誤って脅威として検出される。

4.5 ヘルプ

ESET Endpoint アンチウイルス for OS X には、トラブルシューティングツール、および発生する可能性のある問題の解決に役立つサポート情報が含まれています。
「ヘルプとサポート」画面を表示するには、メインメニューの［ヘルプ］をクリックします。

「ヘルプとサポート」画面には次の項目が含まれています。

ヘルプ	P61 参照
サポートツール	P61 参照
製品およびライセンス情報	P61 参照

■ヘルプ

インターネットで調べる	ESET セキュリティ ソフトウェア シリーズのサポート情報が表示されます。FAQ（よくある質問）への回答や、様々な問題に対する一般的な解決策が登録されています。このナレッジベースは、定期的にアップデートされており、様々な種類の問題を解決するための最も有効なツールです。
ヘルプを開く	ESET Endpoint アンチウイルス for OS X のヘルプページを開きます。

■サポートツール

ウイルス情報	様々なタイプのマルウェアの危険と兆候に関する情報を含む、ESET の最新ウイルス情報一覧へのリンクです。
ウイルス定義データベース履歴	ESET ウイルスレーダーへのリンクです。ウイルス定義データベースのバージョン情報が含まれています。

■製品およびライセンス情報

ESET Endpoint Antivirus について	バージョン情報やインストール済のコンポーネントについて確認できます。
ライセンスを管理	製品のアクティベーション画面を開きます。詳細については 2.4 アクティベーション」を参照してください。

4.6 詳細設定

4.6.1 一般

ファイル、メール、および Web 通信を検査することにより、悪意のある攻撃からコンピューターを保護します。悪意のあるコードを含むウイルスが検出されると、まず保護機能がブロックし、次に駆除、削除、隔離のいずれかを行って、ウイルスを排除します。

ウイルス対策機能の詳細を設定するには、メインメニューの［設定］>［詳細設定を表示する］をクリックして、「詳細設定」画面を表示し、［一般］をクリックします。
ウイルス対策画面では、次の設定ができます。

スキャナオプション	望ましくない可能性があるアプリケーション	必ずしも悪意があるとは限らないが、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るウイルスを検出するかどうかを設定します。
	安全でない可能性があるアプリケーション	悪用される可能性がある市販のソフトウェアを検出するかどうかを設定します。安全でない可能性があるアプリケーションの例としては、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を記録するプログラム）などがあります。既定では無効に設定されています。
	疑わしいアプリケーション	圧縮されたプログラムが含まれます。マルウェアの作成者が検知されるのを逃れるためによく使用する方法です。
除外	指定したファイルやフォルダーを検査から除外します。すべてのファイルやフォルダーでウイルスが検出できるように、基本的には除外しないことをお勧めします。コンピューターの処理速度を低下させる恐れのある大きなデータベースエントリーを検査する場合や、検査と競合するソフトウェアがある場合などは、必要に応じて除外を設定してください。除外の設定は、［設定］ボタンをクリックすることで行えます。除外の詳細については、「●除外設定」を参照してください。	

●除外設定

除外設定では、特定のファイルやフォルダー、IP／IPv6アドレスやアプリケーションを検査の対象外に指定できます。ファイルやフォルダーの除外指定は、コンピューターの処理速度を低下させる恐れのある大きなデータベースエントリーを検査する場合や、検査と競合するソフトウェア（バックアップソフトウェア）がインストールされている場合など、特別な場合以外は行わないことをお勧めします。［ファイルシステム］タブをクリックすると、ファイルやフォルダーの除外設定を行えます。［Web とメール］をクリックすると、特定の IP ／ IPv6 アドレスに対して行う通信やアプリケーションが行う通信をプロトコルの検査から除外できます。

■ファイルシステム

パス	検査から除外するファイルやフォルダーのパスが表示されます。
脅威	除外されるファイルの横に脅威の名前がある場合、ファイルは特定の脅威に対してのみ除外され、完全には除外されません。このファイルが後で他のマルウェアに感染した場合は、ウイルス対策機能によって検出されます。
＋	検査から除外するファイルやフォルダーのパスを追加します。
－	選択したパスを削除します。

特定のファイルやフォルダーを検査から除外する手順は、次のとおりです。

操作手順

1. ［ファイルシステム］タブをクリックします。
2. ［＋］ボタンをクリックします。
3. ツリー構造内でファイルかフォルダーを選択するか、除外するファイルやフォルダーのパスを入力します。

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

   例
   - フォルダー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ーを含めたドライブ全体を除外するには、「*」を使用します。
   - doc ファイルのみを除外する場合は、「*.doc」のようにワイルドカードを使用します。

続く

- 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、一部の文字しかわからない場合は、「?」疑問符を使用します。例えば、文字数が 5 文字で、最初の文字が「D」であることのみわかっている場合は、「D????.app」という形式を使用します。疑問符は、不足している（不明な）文字の代わりになります。

! 重 要

除外に設定されていると、リアルタイムファイルシステム保護機能またはコンピューターの検査機能はファイル内の脅威を検出しません。

■ Web とメール

パス	検査から除外する IP/IPv6 アドレスまたはアプリケーションが表示されます。
除外を表示	表示する除外対象を［IP/IPv6 アドレス］または［アプリケーション］の中から選択できます。
＋	検査から除外する IP/IPv6 アドレスまたはアプリケーションを追加します。
－	選択した IP/IPv6 アドレスまたはアプリケーションを削除します。

特定の IP/IPv6 アドレスまたはアプリケーションの通信をプロトコルの検査の対象から除外する手順は、次のとおりです。

操作手順

1. ［Web とメール］をクリックします。
2. ［除外を表示］のドロップダウンメニューから登録したい情報（IP/IPv6 アドレスまたはアプリケーション）を選択します。
3. ［＋］ボタンをクリックします。
4. 手順❷で IP/IPv6 アドレスを選択した場合は、除外したい IP/IPv6 アドレスを入力し、［OK］ボタンをクリックします。手順❷でアプリケーションを選択した場合は、ツリー構造内でアプリケーションを選択するか、除外したいアプリケーションのパスを入力し、［OK］ボタンをクリックします。

●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 サイト、共有フォルダー、メール、リムーバブルデバイス（USB 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、様々です。

標準的な動作

ESET Endpoint アンチウイルス for OS X は、基本的に次の機能で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
- コンピューターの検査

各機能は、標準的な駆除レベルを使用してファイルを駆除し、駆除したファイルを隔離するか、接続を切断します。通知画面は、デスクトップ右上に表示されます。駆除レベルと動作の詳細については、「4.6.3 リアルタイムファイルシステム保護」の「●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、警告画面が表示され、ウイルスに感染したファイルに対するアクションを選択できます。選択できるアクションは通常、[駆除]、[削除]、[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りますので、そのファイルが「無害なのに誤って感染が検出されたことが確実」な場合のみ選択してください。

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、ファイルを元の状態に戻すため、まず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は、ファイルそのものを削除します。

ワンポイント

駆除とは、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です。削除とは、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、通常は解放後でなければ削除できません（通常は再起動後）。

複数の脅威

コンピューターの検査中に駆除されなかった感染ファイルがある場合、または駆除レベルが［駆除なし］に設定されている場合は、警告画面が表示され、感染ファイルに対するアクションを選択できます。

アーカイブファイルの削除

既定の駆除モードでは、アーカイブ内のすべてのファイルが感染ファイルの場合、アーカイブファイルは削除されます。感染していないファイルが含まれている場合、アーカイブは削除されません。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。そのため、厳密な駆除モードを実行する際には注意が必要です。詳細については、「4.6.3　リアルタイムファイルシステム保護」の「●駆除」を参照してください。

使用しているコンピューターの処理速度が遅くなる、頻繁にフリーズするなど、マルウェアに感染している兆候がある場合は、次の処置をお勧めします。

操作手順

1. メインメニューの［コンピュータの検査］をクリックします。
2. ［スマート検査］をクリックします。
   詳細については、「4.1　コンピューターの検査」を参照してください。
3. 検査の終了後、ログで検査済みファイル、感染ファイル、駆除済みファイルの件数をそれぞれ確認します。

ワンポイント

コンピューターの特定の領域だけを検査する場合は、［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。

4.6.2 スタートアップ保護

スタートアップ保護では、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、ファイルの検査を実行します。スタートアップ保護は、[システムのスタートアップファイルのチェック] のスケジューラータスクで起動します。スタートアップ保護の設定を変更するには、メインメニューの [ツール] > [スケジューラー] をクリックし、[システムのスタートアップファイルのチェック] を選択して [タスクの編集] をクリックします。なお、[システムのスタートアップファイルのチェック] には、起動タイミングの違いによって 2 種類の検査が用意されています。1 つが「ユーザーログイン」、もう 1 つが「ウイルス定義データベースのアップデート」です。
スケジューラータスクの作成と管理の詳細については、「4.4.3 スケジューラー」の「■新しいタスクの追加」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

検査の優先度
スタートアップ検査のスケジュールタスクを作成するときに、検査の優先度を指定します。選択できる優先度は次のとおりです。

- アイドル：システムが待機時のみ、スタートアップ検査が実行されます。
- 最低：システム負荷が最低の場合に、スタートアップ検査が実行されます。
- 低め：システム負荷が低い場合に、スタートアップ検査が実行されます。
- 普通：システム負荷が平均的な場合に、スタートアップ検査が実行されます。

■ ThreatSense エンジン

[ThreatSense エンジン] をクリックすると、スタートアップ検査の検査パラメーターを設定できます。詳細については、「4.6.3 リアルタイムファイルシステム保護」の「■ ThreatSense エンジン」を参照してください。

4.6.3 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」ではリアルタイムファイルシステム保護の設定が行えます。
リアルタイムファイルシステム保護は、システム起動時に有効になり、ファイルのオープン、作成、実行などのイベントが発生したとき、ファイル内に悪意のあるコードがないかを検査します。
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必要不可欠な機能です。パラメーターを変更する際には注意してください。パラメーターの変更は、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競合する場合など、特別な場合のみ行うことをお勧めします。

ワンポイント
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、様々なシステムイベントが発生するたびに、すべての種類のメディアを確認します。ThreatSense テクノロジーの検出方法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、より高いレベルの検査を適用します。
ThreatSense テクノロジーの検出方法の詳細については、「4.6.3 リアルタイムファイルシステム保護」の「■ ThreatSense エンジン」を参照してください。

ワンポイント
ESET Endpoint アンチウイルス for OS X の既定の設定は、最大レベルでシステムを保護できるように最適化されています。既定の設定に戻すには、「詳細設定」画面を表示し、[すべての設定を既定値に戻す] をクリックします。

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、常にイベントを検査します。別のリアルタイムスキャナーと競合するなど、リアルタイムファイルシステム保護を無効にしたい場合は、「詳細設定」画面を表示して、［リアルタイムファイルシステム保護］>「リアルタイムファイルシステム保護を有効にする」を無効にします。無効状態では危険なため別のリアルタイムスキャナーとの競合などの問題が解決したら、有効に戻してください。

●検査のタイミング（イベント発生時の検査）

既定では、ファイルを開く、作成する、実行するなどのイベントが発生すると、ファイルを検査します。

ファイルのオープン	ファイルを開いたときに検査を行うかどうかを設定します。
ファイルの作成	ファイルを新しく作成したとき、またはファイルの内容を変更したときに、検査を行うかどうかを設定します。
ファイルの実行	ファイルを実行したときに検査を行うかどうかを設定します。

！重　要

コンピューターが最大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。

■ ThreatSense エンジン

ThreatSense は、ウイルスを検出する高度な技術です。この技術はプロアクティブ（事前対応型）の検出方法なので、新しいウイルスが広がる初期の段階でシステムを保護することができます。ThreatSense は、システムのセキュリティを大幅に強化するために、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などを組み合わせて保護します。検査エンジンは、複数のデータストリームを同時に検査することで、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。

設定できるパラメーター

ThreatSense エンジンの設定オプションを使用すると、様々な検査パラメーターを指定できます。

- 検査するファイルの種類
- 様々な検出方法の組み合わせ
- 駆除のレベル

など

ThreatSense エンジンのパラメーターを設定できる保護機能

ThreatSense エンジンのパラメーターを設定するには、「詳細設定」画面で ThreatSense 技術を使用する機能の［ThreatSense エンジン］の［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できるように、ThreatSense は次の保護機能ごと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
- コンピューターの検査
- スタートアップ検査
- 電子メール保護
- Web アクセス保護

! 重　要

ThreatSense のパラメーターは機能ごとに高度に最適化されているので、パラメーターを変更すると、システムの動作に大きく影響することがあります。例えば、通常は新しく作成されたファイルのみが検査対象となりますが、リアルタイムファイルシステム保護機能で常に圧縮された実行形式を検査するようにパラメーターを変更したり、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。コンピューターの検査以外の機能については、ThreatSense のパラメーターを変更しないことをお勧めします。

●オブジェクト

「オブジェクト」タブでは、検査するコンピューターのオブジェクトのタイプを定義できます。

電子メールファイル	電子メールファイルを検査します。
メールボックス	システム内のユーザーのメールボックスを検査します。このオプションを正しく使用しない場合、電子メールクライアントとの競合が発生することがあります。
アーカイブ	以下の拡張子のアーカイブを検査します。 ARJ、BZ2、CAB、CHM、DBX、GZIP、ISO/BIN/NRG、LHA、MIME、NSIS、RAR、SIS、TAR、TNEF、UUE、WISE、ZIP、ACE、その他多数。
自己解凍形式	解凍に特殊なプログラムを必要としない自己解凍形式（SFX）のアーカイブを検査します。
圧縮された実行形式	標準のアーカイブ形式とは異なり、ランタイム圧縮形式はメモリーに展開されます。このオプションを選択すると、標準的な静的圧縮形式 (たとえば、UPX、yoda、ASPack、FGS) も検査されます。

●オプション

「オプション」タブでは、システムを検査する方法を選択します。使用可能なオプションは次のとおりです。

ヒューリスティック	ヒューリスティックは、悪意のあるプログラムの動きを分析するアルゴリズムです。主な利点は、以前には存在しない、またはこれまでのウイルス定義データベースにない悪意のあるソフトウェアを特定できる点です。欠点は、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ています。このアルゴリズムは、コンピューターワームやトロイの木馬を検出するために最適化され、高度なプログラミング言語で記述されています。アドバンスドヒューリスティックを使用すると、脅威の検出機能が大幅に向上します。

潜在的な脅威が検出された場合

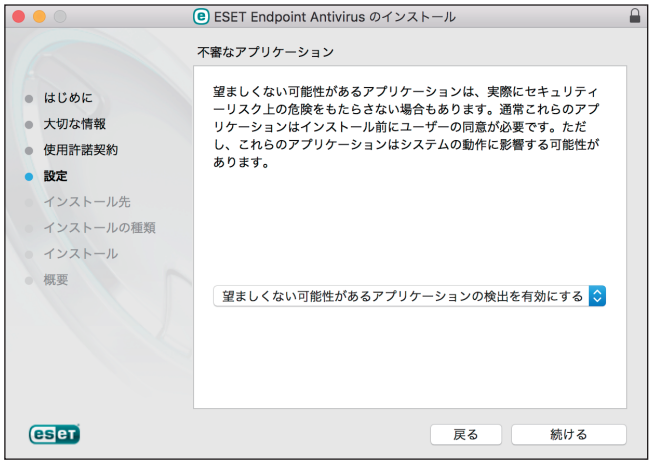
望ましくない可能性があるアプリケーションが検出された場合は、実行するアクションを選択できます。

- 駆除／切断：アクションを終了し、潜在的な脅威がシステムに侵入するのを防ぎます。
- 何もしない：潜在的な脅威がシステムに進入するのを許可します。
- 今後中断せずにコンピューターでアプリケーションを実行できるようにするには、[設定を表示する] をクリックし、[検出対象外] をチェックします。

検出された望ましくない可能性があるアプリケーションを駆除できない場合は、デスクトップの右上に「アドレスはブロックされました」という通知が表示されます。通知の詳細を確認するには、メインメニューの［ツール］>［ログファイル］をクリックし、ドロップダウンメニューから［フィルタリングされた Web サイト］を選択します。

望ましくない可能性があるアプリケーションに関する設定

ESET Endpoint アンチウイルス for OS X をインストールするとき、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かどうかを設定できます。



望ましくないアプリケーションの検出設定は、設定オプションで変更できます。変更するには、次の操作を行います。

操作手順

1. ESET Endpoint アンチウイルス for OS X のメイン画面を開きます。ESET Endpoint アンチウイルス for OS X のメイン画面の開き方については「2.5　コンピューターの検査」の手順❶～❷を参照してください。
2. ［設定］をクリックします。
3. ［詳細設定を表示する］をクリックします。
4. ［一般］をクリックします。
5. 次の各機能を有効または無効にします。
   - 望ましく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
   - 疑わしいアプリケーション

ソフトウェアラッパー

ソフトウェアラッパーは、特殊なタイプの修正アプリケーションで、ファイルホスティング Web サイトの一部で使用されます。ソフトウェアラッパーはサードパーティ製のツールですが、ツールバーやアドウェアなどの追加ソフトウェアもインストールします。追加されたソフトウェアは、Web ブラウザーのホームページや検索設定を変更する場合があります。多くの場合、ファイルホスティング Web サイトはソフトウェアベンダーやダウンロード受信者に、設定が変更されたことを通知しないため、変更を回避することができません。このため、ESET Endpoint アンチウイルス for OS X はソフトウェアラッパーを望ましくない可能性のあるアプリケーションのタイプに分類しています。ユーザーはソフトウェアラッパーをダウンロードするかどうかを設定できます。

●駆除

「駆除」タブでは、感染ファイルからウイルスを駆除するときのレベルを設定します。
感染ファイルからウイルスを駆除するときのレベルには、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は自動的に駆除されず、警告画面でユーザーがアクションを選択することができます。ウイルスの侵入が発生したときに実行しなければならないステップを理解している経験豊富なユーザー向けのレベルです。
標準駆除	あらかじめ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、感染ファイルを自動的に駆除または削除します。感染しているファイルの検出と削除は、デスクトップ右上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	すべての感染ファイルが駆除または削除されます（システムファイルを除く）。感染ファイルを駆除できなかった場合は、アクションを選択する警告画面が表示されます。

! 重　要

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は 2 つあります。「標準駆除」モードでは、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 つでも含まれている場合、アーカイブ内の他のファイルの感染に関係なく、アーカイブが削除されます。

●除外

拡張子は、ファイル名の一部であり、ピリオドで区切られています。既定では、拡張子に関係なく、すべてのファイルが検査されます。「除外」タブでは検査対象外とする拡張子を指定します。「除外」タブで追加した拡張子のファイルは検査対象外となります。

ESET Endpoint アンチウイルス for OS X では、どのような拡張子でも検査対象外に指定できます。ファイルの検査によってプログラムが正常に動作しなくなる場合は、その拡張子を検査から除外する必要があります。

拡張子の管理

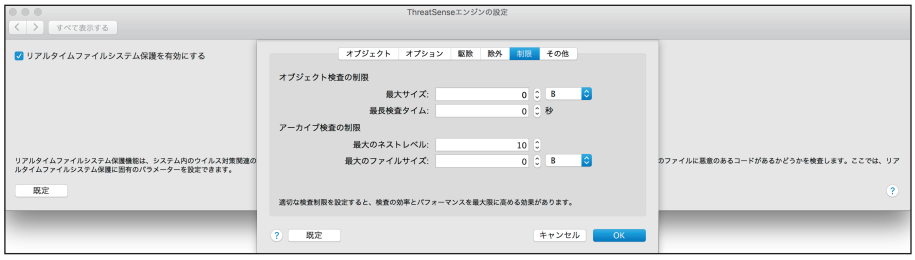
検査対象外となっている拡張子を表示するには、メインメニューの［設定］>［詳細設定を表示する］をクリックして「詳細設定」画面を表示し、各保護機能を開き［ThreatSense エンジン］の［設定］>「除外」をクリックします。
拡張子を追加するには、「除外」画面で［+］をクリックし、拡張子を入力して【return】キーを押します。
登録済みの拡張子を編集するには、「拡張子リストを除外する」画面の拡張子一覧で対象の拡張子をダブルクリックします。
拡張子を削除するには、「拡張子リストを除外する」画面の拡張子一覧で対象の拡張子を選択し、［−］をクリックします。

ワンポイント

拡張子の指定では、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。特殊記号を使って拡張子を指定する際は、正しい形式で入力してください。

●制限

「制限」タブでは、検査対象オブジェクトの最大サイズやアーカイブのネストレベルなどを指定できます。



オブジェクト検査の制限

最大サイズ	検査対象のオブジェクトの最大サイズを設定します。最大サイズを設定すると、指定した値より小さいサイズのオブジェクトのみ検査されます。上級ユーザーがサイズの大きいオブジェクトを検査から除外する場合のみ、設定を変更してください。既定値は無制限です。
最長検査タイム	オブジェクト検査の最長時間を設定します。最長時間を設定すると、検査が終了しているかどうかにかかわらず、設定した時間が経過した時点で検査を停止します。既定値は無制限です。

アーカイブ検査の制限

最大のネストレベル	検査するアーカイブのネストレベルを指定します。既定値は「10」です。
最大のファイルサイズ	検査対象のアーカイブに含まれているファイルの最大サイズを指定します。既定値は無制限です。

!重　要

一般的な環境では既定値を変更しないことをお勧めします。

●その他

「その他」タブでは、TheatSense エンジンのその他のパラメーターの設定を行えます。

SMART 最適化を有効にする	SMART 最適化を有効にすると、検査の速度を最高に保ちながら、最も効率的な検査レベルが確保されるように最適化されます。保護機能に応じた検査方法を使用して、高度な検査を行います。SMART 最適化を無効にすると、ThreatSense コアのユーザー定義設定のみが検査に適用されます。
代替データストリームを検査する	ファイルシステムで使用される代替データストリームは、ファイルとフォルダーに紐付いています。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ため、多くのマルウェアは自らを代替データストリームに見せかけ、検出を逃れようとします。代替データストリームを検査することで、マルウェアを検出できます。
システム制御フォルダーを検査から除外する	システムによって制御されるフォルダーを検査の対象から除外したいときは、「システム制御フォルダーを検査から除外する」にチェックを入れます。

ワンポイント

「スマート最適化」ではリアルタイムファイルシステム保護のシステムへの負荷を最小限にするため、すでに検査されたファイルは変更がない限り、次回、ウイルス定義データベースが変更されるまで検査されません。ウイルス定義データベースがアップデートされた場合は、すぐにファイルが再検査されます。「スマート最適化」が無効の場合、すべてのファイルがアクセスのたびに検査されます。

4.6.4 電子メール保護

電子メール保護では POP3 と IMAP プロトコルで受信したメール通信を制御できます。受信メッセージを検査するときには、ThreatSense エンジンで設定されたスキャン方法がすべて使用されます。これはウイルス定義データベースに対し一致する前に悪意のあるプログラムの検査が行われることを意味します。POP3 と IMAP プロトコル通信の検査は使用される電子メールクライアントから独立しています。電子メール保護を有効にするには、メインメニューの［設定］＞［Web とメール］をクリックし、［電子メールクライアント保護］を有効にするか、メインメニューの［設定］＞［詳細設定を表示する］をクリックして「詳細設定」画面を表示し、［電子メール保護］をクリックして、［電子メールクライアント保護を有効にする］にチェックを入れます。電子メール保護の設定画面は、メインメニューの［設定］＞［Web とメール］をクリックし、［電子メールクライアント保護］の［設定］ボタンをクリックすることでも表示できます。電子メール保護の設定画面では次の設定が行えます。

■電子メールクライアント保護を有効にする

この設定にチェックを入れると、電子メールクライアント保護が有効になります。

■ ThreatSense エンジン

ThreatSense エンジンの［設定］ボタンをクリックすると、電子メールクライアント保護で利用する検査対象や検出方法などを設定できます。詳細については、「4.6.3 リアルタイムファイルシステム保護」の「■ ThreatSense エンジン」を参照してください。

■警告と通知

電子メールクライアント保護では、POP3/IMAP プロトコルで受信したメール通信を検査します。ESET Endpoint アンチウイルス for OS X は、電子メールクライアントからの POP3 や IMAP プロトコルの通信を検査します。受信メッセージは、ThreatSense エンジンパラメーターの設定に従って検査するため、ウイルス定義データベースと照合する前に悪意のあるコードを検出できます。POP3/IMAP プロトコルの通信検査は、電子メールクライアントからは独立しており、次の設定が行えます。

メールのフットノートへタグメッセージを追加	メールが検査された後、検査結果と通知をメールのフットノートに追加します。［無期限］［感染メールのみ］［すべての検査済みメール］の中からタグメッセージを追加する方法を選択できます。［無期限］を設定すると、検査通知を追加しません。［感染メールのみ］を選択すると、有害なソフトウェアを含むメールのみに検査通知を追加します。［すべての検査済みメール］を選択すると、検査した全てのメールに検査通知を追加します。
感染メールの件名に注釈を追加	［感染メールの件名に注釈を追加］にチェックを入れると、「感染メールの件名に追加する注釈のテンプレート」を変更できます。

! 重 要

HTML メールやメール本文自体がマルウェアで偽装されている場合、検査メッセージが追加されないことがあります。

■ POP3

POP3 プロトコルは、電子メールクライアントアプリケーションでのメールの受信に最もよく使用されているプロトコルです。ESET Endpoint アンチウイルス for OS X 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。[POP3 プロトコルのチェックを有効にする] にチェックを入れると、この機能が有効になります。この機能はシステム起動時に、自動的に起動され、メモリーでアクティブになります。POP3 プロトコルチェックは、電子メールクライアントを再構成せずに、自動的に実行されます。既定では、ポート 110 にある全ての通信が検査されますが、他の通信ポートは必要に応じて追加できます。他のポートを追加するときは、ポート番号をカンマで区切って入力します。

■ IMAP

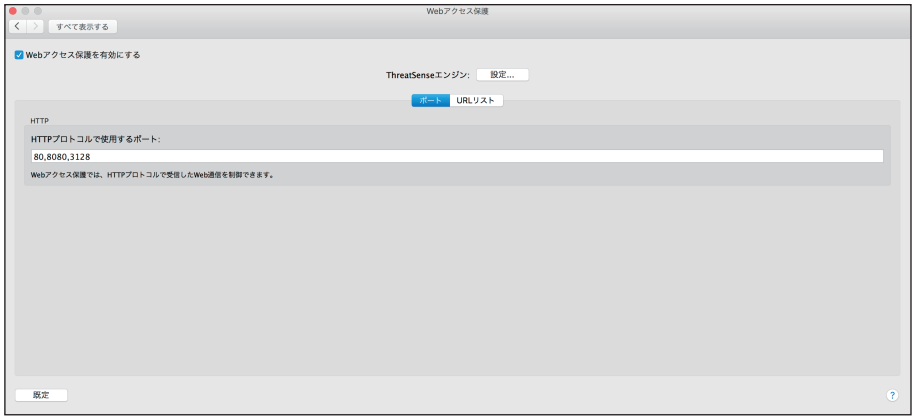
IMAP (Internet Message Access Protocol) は電子メール取得に使われるもう一つのインタネットプロトコルです。IMAP は POP3 よりも優れている点があります。たとえば、IMAP では、複数のクライアントが同時に同じメールボックスに接続して、メッセージが既読か、返信済みか、削除されたかなどの状態の情報を保持できます。ESET Endpoint アンチウイルス for OS X では、使用しているメールクライアントに関係なく、このプロトコルを保護できます。[IMAP プロトコルのチェックを有効にする] にチェックを入れると、この機能が有効になります。この制御を提供する保護機能はシステム起動時に、自動的に起動され、メモリーでアクティブになります。IMAP プロトコルチェックは、電子メールクライアントを再構成せずに、自動的に実行されます。既定では、ポート 143 にある全ての通信が検査されますが、他の通信ポートは必要に応じて追加できます。他のポートを追加するときは、ポート番号をカンマで区切って入力します。

4.6.5 Web アクセス保護

インターネット接続は、コンピューターの標準機能です。しかし、コンピューターによるインターネット接続は、悪意のあるコードを転送する主要な方法になっています。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 のルールに準拠した通信を監視します。

Web アクセス保護によって、悪意のあるコンテンツが含まれている Web サイトへのアクセスをブロックします。悪意のあるコンテンツが含まれているかどうか不明な Web サイトは、読み込み時に ThreatSense スキャンによって検査を行い、悪意のあるコンテンツを検出すると、アクセスをブロックします。

Web アクセス保護の設定を行うには「詳細設定」画面を表示して、[Web アクセス保護] をクリックします。



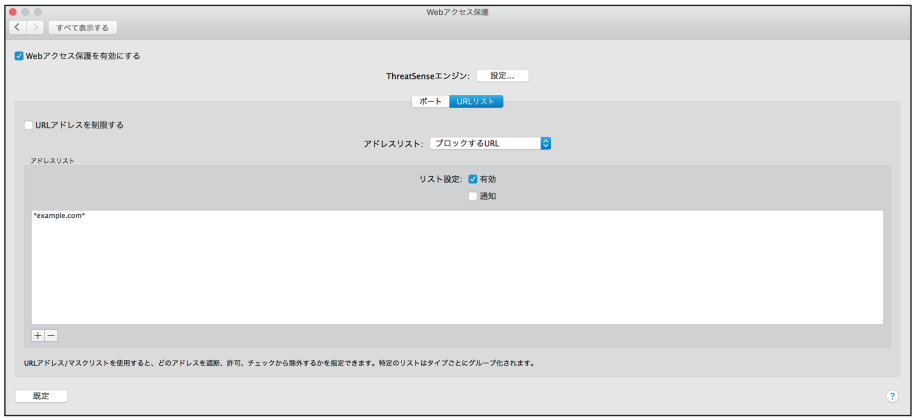
Web アクセス保護を有効にする	Web アクセス保護の有効 / 無効を設定します。

HTTP

Web アクセス保護は、Web ブラウザとリモートサーバー間の通信を監視し、HTTP (Hypertext Transfer Protocol) プロトコルによる通信を検査します。[ポート] タブで HTTP 通信で使用されるポート番号を定義でき、既定ではポート番号 80、8080 および 3128 が事前定義されています。

URL リスト

[URL リスト] タブをクリックすると、特定の HTTP アドレスへの接続を許可またはブロックしたり、検査から除外できます。この機能を利用するには、[URL アドレスを制限する] にチェックを入れる必要があります。URL リストでは次の設定が行えます。



URL アドレスを制限する	［許可する URL］リストの URL へのアクセスのみを許可し、それ以外の URL へのアクセスを全て禁止する場合に有効にします。	
アドレスリスト	アドレスリストでは、許可、ブロック、検査から除外する HTTP アドレスを設定できます。既定では、次の 3 つのリストを利用できます。	
	許可する URL	接続を許可する HTTP アドレス（URL）のリストです。ブロックする URL のリストに「*」（すべてと一致）が含まれる場合、ユーザーは、このリストで指定されたアドレスだけにアクセスできます。このリストのアドレスは、ブロックする URL のリストよりも優先されるため、このリストとブロックするアドレスのリストの両方に登録されている場合にも、アクセスが許可されます。
	ブロックする URL	接続を拒否する HTTP アドレス（URL）のリストです。ユーザーは、基本的にこのリストで指定されたアドレスにはアクセスできません。
	検査から除外する URL	検査を行わない HTTP アドレス（URL）のリストです。このリストに追加すると、悪意のあるコードのチェックが実行されなくなります。
リスト設定	許可する URL やブロックする URL、検査から除外する URL に登録した HTTP アドレス（URL）のリストの有効／無効を設定します。「有効」にチェックを入れると、アドレスリストで選択したリストが有効に設定され、チェックを外すと無効に設定されます。［通知］にチェックを入れると、リストに登録した HTTP アドレス（URL）へのアクセスが発生した場合に、通知が行われます。	
＋	選択中のアドレスリストに HTTP アドレス（URL）を追加します。追加済みのアドレスを編集したいときは、そのアドレスをダブルクリックします。	
－	選択したアドレスを選択中のリストから削除します。	

アドレスリストを有効にするには、アドレスリストで設定を行いたいリストを選択し、リストの設定の「有効」にチェックを入れます。また、アドレスリストの URL にアクセスしたときに通知する場合は、「通知」にチェックを入れます。許可するアドレスリストに登録されているアドレスを除いて、すべての HTTP アドレスをブロックする場合は、ブロックするアドレスリストのアドレスに「*」を追加します。

ワンポイント

すべてのアドレスリストで、特殊記号の「*」（アスタリスク）および「?」（疑問符）を使用できます。アスタリスクは任意の数字または文字を表します。疑問符は任意の 1 文字を表します。検査対象外のアドレスを指定する際は、信頼できる安全なアドレスだけを登録する必要があるため、細心の注意を払って特殊記号を使用してください。

■ThreatSense エンジン

［ThreatSense エンジン］の［設定］をクリックすると、Web アクセス保護の検査パラメーターを設定できます。詳細については、「4.6.3　リアルタイムファイルシステム保護」の「■ ThreatSense エンジン」を参照してください。

4.6.6 フィッシング対策

フィッシングとは、ソーシャルエンジニアリング（機密情報を入手するためにユーザーを操ること）を用いる犯罪行為です。フィッシングは、銀行の口座番号や PIN コードなどの機密データを入手するためによく使用されます。
ESET Endpoint アンチウイルス for OS X はフィッシング対策機能を搭載しており、フィッシングサイトへのアクセスをブロックできます。
「詳細設定」画面で、［フィッシング対策］をクリックします。

フィッシング対策を有効にする	フィッシング対策の有効 / 無効を切り替えます。

フィッシングサイトにアクセスすると、次の警告画面が Web ブラウザーに表示されます。それでも Web サイトにアクセスする場合は、［警告を無視］をクリックします。

! 重 要

［警告を無視］の選択は推奨しません。

! 重 要

ホワイトリストに登録されている潜在的なフィッシングサイトは、既定では数時間後に有効期限が切れます。潜在的なフィッシングサイトを永続的に許可するには、Web アクセス保護の URL リストに、「許可する URL」として登録を行います。URL リストの詳細については、「4.6.5 Web アクセス保護」の「■ URL リスト」を参照してください。

フィッシングサイトの報告

フィッシングサイトおよび悪意のある Web サイトを分析のために ESET に報告したいときは、メインメニューの［設定］>［Web とメール］をクリックし、［フィッシングサイトを報告］をクリックします。詳細については、「4.3.2 Web とメール」の「フィッシング詐欺サイトを報告」を参照してください。

! 重 要

ESET にフィッシングサイトを報告する前に、次の基準を 1 つでも満たしていることを確認してください。

- Web サイトがまったく検出されない
- Web サイトが誤ってウイルスとして検出される（この場合は、誤検出されたフィッシングサイトを報告してください。）

4.6.7 コンピューターの検査

「コンピューターの検査」画面では、検査プロファイルの各種設定や新しい検査プロファイルの作成が行えます。また、各検査プロファイルの設定は、メインメニューの「コンピュータの検査」から行うこともできます。詳細については、「4.1 コンピューターの検査」を参照してください。

検査プロファイル設定	設定を行うプロファイルを選択できます。
編集	プロファイルの作成や削除などを行えます。既定値では、「スマート検査」「詳細検査」「コンテキストメニュー検査」の 3 つのプロファイルが用意されていますが、それ以外に独自の検査プロファイルを作成したいときに利用します。新規プロファイルの作成については、「4.1.5 検査設定」の「■検査プロファイルを作成する」を参照してください。
ThreatSense エンジンの［設定］	選択した検査プロファイルを利用して、検査を行うときの詳細な設定を行えます。設定されている内容は、プロファイルごとに異なります。設定の詳細については、「4.6.3 リアルタイムファイルシステム保護」の「■ ThreatSense エンジン」を参照してください。
検査の対象の［設定］	選択した検査プロファイルで検査を行うファイルやフォルダーを設定できます。
検査後にコンピューターをシャットダウン	タスクが完了したらコンピュータの電源を自動的にシャットダウンしたいときにチェックを入れます。

4.6.8 デバイスコントロール

デバイスコントロール機能は、CD/DVD/USB メモリーなどのデバイスをコンピューターで使用するとき、読み込み／書き込みの許可、ブロック、警告表示など、指定デバイスへのアクセス方法やその作業方法を定義できる機能です。使ってほしくないファイルが格納されているデバイスの使用を防止したいコンピューター管理者にとって便利な機能です。デバイスコントロールは、「デバイスコントロール」画面で設定を行います。「デバイスコントロール」画面は、メインメニューの［設定］＞［詳細設定を表示する］をクリックし、「詳細設定」画面を表示して、［デバイスコントロール］をクリックすることで表示できます。また、メインメニューの［設定］＞［コンピュータ］＞［デバイスコントロール］の［設定］をクリックすることでも「デバイスコントロール」画面を表示できます。

サポートするデバイス

デバイスコントロール機能でサポートするデバイスは次のとおりです。

- ディスクストレージ（HDD、USB メモリー）
- CD/DVD
- USB プリンター
- イメージングデバイス
- ネットワーク
- シリアル
- ポータブルデバイス

デバイスコントロールを有効にする	デバイスコントロール機能の有効 / 無効を設定します。［デバイスコントロールを有効にする］にチェックを入れると、デバイスコントロール機能が有効になり、各種設定が行えます。
「ルールの設定」タブ	「ルールの設定」タブでは、制御に利用するルールの作成や削除、編集を行えます。詳細は、「●ルールの設定」を参照してください
「デバイスグループ」タブ	「デバイスグループ」タブでは、デバイスのグループを作成できます。詳細は、「●デバイスグループ」を参照してください。

●ルールの設定

「ルールの設定」タブでは、デバイスの制御に利用するルールの作成や削除、編集を行えます。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で、アクセスの許可またはブロックを定義することもできます。ルール一覧には、プロファイル名とデバイスタイプ、デバイスのベンダー名などの説明、デバイスにアクセスしたときに実行するアクション、デバイスを利用可能なユーザー、ログの重大度などが表示されます。チェックボックスにチェックを入れるとルールが有効になり、チェックを外すとルールは無効になります。ルールの設定では、次の操作ができます。

＋	新しいルールを追加します。
－	ルールを削除します。
⚙	選択したルールの編集を行ったり、ルールを上や下に移動できます。
入力	コンピューターに接続されている機器のパラメーターを自動的に入力してルールの作成画面を開きます。

！重　要

デバイスの機種やデバイス側の設定によって意図しないタイプで認識される場合があります。確実にデバイスのタイプを確認する場合は、デバイスの接続後に［入力］ボタンをクリックしてデバイスを表示させてください。

●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、コンピューターからデバイスにアクセスしようとしたときに実行するアクションを定義します。

名前	識別しやすいように、ルールの説明を入力します。ここで入力した名前は、プロファイル名として表示されます。	
有効	ルールの有効／無効を設定できます。ルールを削除せずに無効にしたい場合に便利です。	
デバイスタイプ	デバイスタイプ（ディスクストレージ／CD/DVD／USB プリンター／イメージングデバイス、シリアル、ネットワーク、ポータブルデバイスなど）をドロップダウンメニューから選択します。デバイスタイプは、オペレーティングシステムから引き継がれます。 ストレージデバイスには、USB または FireWire から接続できる外付けハードディスクや USB メモリー、標準的なメモリーカードリーダーが含まれます。イメージングデバイスとは、スキャナーやカメラなどのデバイスです。 これらのデバイスはアクションに関する情報だけを提供し、ユーザーに関する情報は提供しないため、汎用的なデバイスを確実にブロックできます。	
アクション	デバイスへのアクセスについて、次のいずれかのアクションを定義できます。 **ワンポイント** デバイスのタイプによっては、選択できないアクションがあります。［すべてのデバイスタイプ］［ディスクストレージ］［CD/DVD］などのデバイスタイプの場合、3 つのアクションすべてを選択できます。それ以外のデバイスタイプでは、［読み込み／書き込み］と［ブロック］の 2 つのアクションを選択できます。例えば、デバイスのタイプが Bluetooth の場合は、［読み込み専用］アクションは選択できません。	
	読み込み／書き込み	デバイスへの完全アクセスを許可します。
	読み込み専用	デバイスからの読み込みアクセスだけを許可します。
	ブロック	デバイスへのアクセスをブロックします。
条件	［デバイスグループ］または［デバイス］を選択します。なお、［デバイスグループ］は、［デバイスグループ］タブでグループの登録を行っている場合のみ選択できます。	

<table>
<tr><td>追加パラメーター</td><td colspan="2">ルールを微調整したり、デバイスに合わせて変更したりするのに使用します。いずれのパラメーターも大文字と小文字は区別しません。追加のパラメーターを入力すると、ベンダー名やモデル、シリアル番号などの追加した情報が一致した場合にのみ作成したルールが適用されます。また、デバイス接続後に［入力］ボタンをクリックし、リストからデバイスを選択して［続行］ボタンをクリックすると、ベンダー名やモデル、シリアル番号などの情報をデバイスから読み取ってルールの作成を行えます。
!重　要
追加パラメーターが定義されていない場合、ルール照合時は追加パラメーターを無視します。
また、追加パラメーターではワイルドカード（*、?）はサポートしていません。</td></tr>
<tr><td rowspan="6">ログ記録の重大度</td><td>ベンダー</td><td>入力したベンダー名または ID によってフィルタリングを行います。</td></tr>
<tr><td>モデル</td><td>デバイスの名前を入力します。</td></tr>
<tr><td>シリアル</td><td>デバイス独自のシリアル番号を入力します。
CD/DVD の場合は、CD ドライブではなく、デバイス独自のシリアル番号があります。</td></tr>
<tr><td>常に</td><td>デバイスコントロールルールのすべてのアクションをログに記録します。</td></tr>
<tr><td>診断</td><td>プログラムを微調整するのに必要な情報をログに記録します。</td></tr>
<tr><td>情報</td><td>アップデート成功のメッセージを含むすべての情報メッセージと、アクション、診断の情報をログに記録します。</td></tr>
<tr><td>警告</td><td>重大なエラー、エラー、警告メッセージをログに記録します。</td></tr>
<tr><td>なし</td><td>ログは記録しません。</td></tr>
<tr><td>ユーザー一覧</td><td colspan="2">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して適用します。ユーザーまたはユーザーグループを指定するには、［編集］ボタンをクリックします。ユーザーまたはグループの登録画面が表示されるので、登録したいユーザーを左のユーザー画面から選択し、［追加］をクリックします。ユーザーまたはユーザーグループを削除するには、選択したユーザー画面から削除したいユーザーを選択し、［削除］をクリックします。</td></tr>
</table>

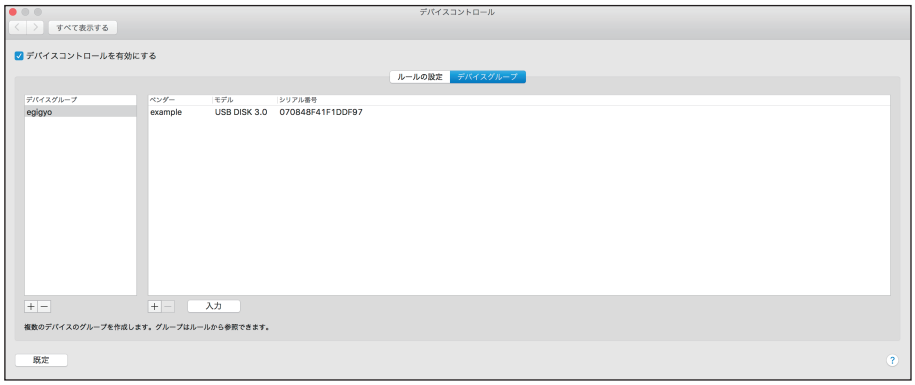
!重　要

［デバイスのタイプ］で次のデバイスを選択した場合、ユーザールールでフィルタリングすることはできません。実行されるアクションに関する項目についてのみフィルタリングできます。

- USB プリンター
- イメージングデバイス
- ネットワーク
- ポータブルデバイス

●デバイスグループ

「デバイスグループ」タブでは、デバイスグループを作成できます。デバイスグループでは、最初にグループを作成し、次にグループで利用するデバイスの登録を行います。作成したデバイスグループは、ルールの作成に利用できます。



左側ペイン	＋	新しいデバイスグループを追加します。
	－	デバイスグループを削除します。
右側ペイン	＋	デバイスグループにデバイスを追加します。ベンダー、モデル、シリアル番号を登録します。
	－	登録されているデバイスを削除します。
	入力	現在接続されているすべてのデバイスのデバイスタイプ、ベンダー名、モデル名、シリアル番号が表示されます。リストからデバイスを選択して、［続行］ボタンをクリックすると、ベンダー名やモデル、シリアル番号などの情報を読み取って、そのデバイスを追加できます。

4.6.9 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。ログの設定は、「ログファイル」画面で行います。「ログファイル」画面は、メインメニューの［設定］＞［詳細設定を表示する］をクリックし、「詳細設定」画面を表示して、［ログファイル］をクリックすることで表示できます。「ログファイル」画面では、次の設定が行えます。

古いログレコードを自動的に削除する	チェックボックスにチェックを入れて有効にすると、指定した日数より古いログエントリーが自動的に削除されます。既定値では、「90 日」が設定されています。	
ログファイルを自動的に最適化	チェックボックスにチェックを入れて有効にすると、未使用のレコードが指定した割合を超えたときにログファイルが自動的に最適化されます。既定値では、「25%」が設定されています。	
テキストファイルでログを記録する	チェックボックスにチェックを入れて有効にすると、ログファイルをテキスト形式で記録でき、次の設定を行えます。	
	タイプのテキストファイルを使用	［TXT］または［CSV］の中から保存形式を選択できます。既定では、「TXT」が設定されています。
	詳細オプション	［設定］ボタンをクリックすると、テキストファイルで保存したログファイルの保存先を設定できます。
	テキストログファイルを削除	このボタンをクリックすると、テキストファイルで保存したログファイルがすべて削除されます。
テキストログファイル	［編集］ボタンをクリックすると、保存するログの内容を選択できます。次のログを選択でき、既定値ではすべてのログが選択されています。	
	イベント	無効なユーザー名とパスワード、ウイルス定義データベースを更新できなかったときなどのイベントは、「eventslog.txt」ファイルに書き込まれます。
	検出された脅威	起動時検査、リアルタイム保護、またはコンピュータ検査によって検出された脅威は「threatslog.txt」ファイルに保存されます。
	コンピュータの検査	すべての完了した検査の結果は、「scanlog. 番号 .txt」の形式で保存されます。
	デバイスコントロール	デバイスコントロールでブロックされたデバイスについては、「devctllog.txt」に記述されています。
コンピューターの検査のログレコードの既定フィルター	［編集］ボタンをクリックすると、表示するログに関する設定が行えます。次のログの中から表示するログを選択できます。既定では、すべてのログが選択されています。	
	重大な警告	致命的なシステムエラー（ウイルス・スパイウェア対策の起動に失敗したなど）。
	エラー	" ファイルのダウンロードエラー " などのエラーメッセージと重大なエラー。
	警告	警告メッセージ。
	情報レコード	アップデートの正常完了や警告などの情報。
	診断レコード	プログラムの微調整に必要な情報および上記の全てのレコード。

4.6.10 スケジューラー

スケジューラーは、実行時間や実行するアクションなどをタスクとして登録し、自動で定期的にタスクを実行する機能です。スケジューラーを表示するには、メインメニューの［ツール］>［スケジューラー］をクリックします。スケジューラーの詳細については、「4.4.3 スケジューラー」を参照してください。
また、スケジューラーには、登録されているタスクの設定内容（タスクのタイプ、名前、実行のタイミングなど）が一覧で表示されますが、既定値ではシステムタスクは表示されません。システムタスクを表示したいときは、スケジューラーの設定画面で設定を行います。メインメニューの［設定］>［詳細設定を表示する］をクリックし、「詳細設定」画面を表示して、［スケジューラー］をクリックするとスケジューラーの設定画面が表示されます。［システムタスクを表示する］のチェックボックスにチェックを入れると、システムタスクがスケジューラーに表示されます。

4.6.11 ESET LiveGrid

ESET LiveGrid は、複数のクラウド技術で構成される高度な早期警告システムです。レピュテーションに基づいて新しく発生する脅威を検出し、ホワイトリストを使用して検査の精度を向上させます。新しい脅威の情報はリアルタイムでクラウドに送信されるため、ESET ウイルスラボでは迅速に対応することが可能となり、常に最大の保護を提供できます。ユーザーは、直接 ESET LiveGrid を操作したり、ESET LiveGrid に用意されている追加情報を閲覧して、稼働中のプロセスやファイルの評価を確認したりすることができます。
ESET Endpoint アンチウイルス for OS X をインストールするときには、次のオプションのいずれかを選択します。

- ESET LiveGrid を無効にします。ESET Endpoint アンチウイルス for OS X の機能は一切失われませんが、場合によっては、新しい脅威への対応がウイルス定義データベースのアップデートよりも遅くなることがあります。
- ESET LiveGrid を有効にします。新しいウイルスと危険なコードが検出された場合、その情報を匿名で ESET に送信して詳しい解析を受けることができます。ESET は送信されたウイルスを解析することで、ウイルス検出機能を最新のものにできます。

ESET LiveGrid は、新しく検出されたウイルスに関連して、クライアントコンピューターに関する情報を収集します。この情報には、ウイルスが検出されたファイルのサンプルまたはコピー、ファイルのパス、ファイル名、日時、ウイルスがコンピューターに侵入したプロセス、コンピューターのオペレーティングシステムについての情報が含まれます。
メインメニューの［設定］>［詳細設定を表示する］をクリックし、「詳細設定」画面を表示して、［ESET LiveGrid］をクリックすると ESET LiveGrid の各種設定を行えます。

ESET LiveGrid に参加する（推奨）	チェックボックスにチェックを入れると、新しいウイルスと危険なコードが検出された場所に関する匿名の情報を ESET のウイルスラボに提出します。ESET LiveGrid 評価システムは、解析済みのウイルスをクラウドのホワイトリストおよびブラックリストのデータベースと比較し、ESET マルウェア対策ソリューションの効率化を図ります。	
詳細オプション	［設定］ボタンをクリックすると、ESET LiveGrid に関する詳細な設定が行えます。	
	ファイルを提出	チェックボックスにチェックを入れると、脅威に似ているファイルや、標準ではない特性や動作を持つ不審なファイルは、分析するために ESET に送信されます。
	匿名の統計情報を送信	チェックボックスにチェックを入れると、脅威名、脅威を検出した日時、検出方法、関連付けられたメタデータ、製品バージョン、設定（システム情報を含む）など、新しく検出された脅威に関する情報を ESET が収集します。
	除外フィルター	このオプションを使用すると、特定のファイルの種類を提出から除外できます。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したいときに利用します。なお、最も一般的なファイルの種類（.doc、.rtf など）は、既定で除外されます。除外するファイルの一覧にないファイルの種類を追加したいときは、マスクに除外したいファイルの拡張子を「*.test」などの形式で入力し、［追加］ボタンをクリックします。
	連絡先の電子メールアドレス（任意）	不審なファイルに添付する連絡先の電子メールアドレスを入力します。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します。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。

ワンポイント

ESET LiveGrid を無効にしても、有効中に収集していたデータが残っている場合は ESET に送信されます。すべてのデータが送信されると、データはそれ以上収集されません。

4.6.12 権限

ESET Endpoint アンチウイルス for OS X の設定は組織のセキュリティポリシーにとって非常に重要です。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。このような問題に備えて、ESET Endpoint アンチウイルス for OS X では、設定を編集する権限を持つユーザー（権限ユーザー）を選択できるように設計されています。権限ユーザーの設定は、メインメニューの［設定］＞［詳細設定を表示する］をクリックし、「詳細設定」画面を表示して、［権限］をクリックすることで行えます。権限ユーザーの設定手順については、「3.5 設定の保護」を参照してください。

4.6.13 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せずに使用したい、ポップアップウインドウを表示させたくない、CPU の使用量を最小化したい、ウイルス検査でプレゼンテーションを中断したくない、などの要望に応えるための機能です。プレゼンテーションモードを有効にすると、すべてのポップアップウインドウが無効になり、ESET Endpoint アンチウイルス for OS X のスケジューラーが停止します。また、システムの保護はバックグラウンドで実行され、ユーザーの操作は必要ありません。

プレゼンテーションモードの詳細を設定するには、「詳細設定」画面を表示して、メインメニューの［設定］＞［詳細設定を表示する］をクリックし、［プレゼンテーションモード］をクリックします。

! 重　要

プレゼンテーションモードが有効なときに、セキュリティ上のリスクが存在する Web サイトまたはアプリケーションにアクセスした場合、ユーザーとの対話処理が無効なため、ブロックの説明や警告が表示されませんので注意してください。

プレゼンテーションモードを有効にする	チェックボックスにチェックを入れると、プレゼンテーションモードが有効になります。また、プレゼンテーションモードを有効にすると、指定した時間が経過した際にプレゼンテーションモードを自動的に無効にする［プレゼンテーションモードを無効にするまでの時間］を分単位で設定できます。既定値は、「0 分」が設定されており、自動的にプレゼンテーションモードが無効にならないように設定されています。
全画面でプレゼンテーションモードを自動的に有効にする	チェックボックスにチェックを入れると、アプリケーションが全画面で実行された際に、プレゼンテーションモードを自動的に有効にします。この機能を有効にすると、全画面でアプリケーションを開始するたびにプレゼンテーションモードが有効になり、アプリケーションを終了すると、自動的に終了します。この機能は、プレゼンテーションを開始する場合に便利です。

4.6.14 インターフェース

インターフェースの設定オプションを使用すると、各自のニーズに合わせて作業環境を調整できます。インターフェースの設定オプションはメインメニューの [設定] > [詳細設定を表示する] をクリックして、「詳細設定」画面を表示し、[インターフェース] をクリックします。ここでは、次の項目について ESET Endpoint アンチウイルス for OS X のグラフィカルユーザーインターフェース（GUI）の設定を行えます。

起動時にスプラッシュ画面を表示する	チェックボックスにチェックを入れると、ESET Endpoint アンチウイルス for OS X 起動時にスプラッシュ画面を表示します。
アプリケーションをドックに表示する	チェックボックスにチェックを入れると、ESET Endpoint アンチウイルス for OS X のアイコンがドックに表示されます。また、【command】キーを押しながら【tab】キーを押すと、起動中のアプリが表示され、ESET Endpoint アンチウイルス for OS X とその他の動作アプリケーションの間で切り替えを行うことができます。設定の変更を行った場合は、ESET Endpoint アンチウイルス for OS X の再起動（通常はコンピューターの再起動によって行います）後に有効になります。
標準メニューを使用	チェックボックスにチェックを入れると、メニューバーに標準メニュー項目（[ユーザーインターフェース]、[設定]、[ツール]）が表示されます。
ツールヒントを表示	チェックボックスにチェックを入れると、特定のオプションの上にマウスポインターを置くとヒントを表示します。
隠しファイルを表示	チェックボックスにチェックを入れると、[コンピュータの検査] の [検査の対象] 設定で隠しファイルを表示して選択することができます。

4.6.15 警告と通知

脅威の警告やシステム通知の設定を変更したいときは、[警告と通知] の設定画面を表示します。[警告と通知] の設定画面は、メインメニューの［設定］＞［詳細設定を表示する］をクリックし、「詳細設定」画面を表示して、［警告と設定］をクリックすることで表示できます。［警告と通知］の設定画面では次の項目について設定できます。

警告を表示	チェックボックスにチェックを入れると、脅威が検出された場合やユーザーの操作が必要な場合に警告ウインドウを表示します。チェックを外すと、警告ウインドウを表示しません。なお、警告を表示しないように設定することが推奨されるのは、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（チェックボックスにチェックが入った状態）で利用されることをお勧めします。また、チェックボックにチェックを入れている場合は、表示を行う警告ウインドウの内容を詳細設定オプションで設定できます。	
	詳細オプション	［設定］ボタンをクリックすると、表示を行う警告ウインドウの内容を設定できます。
デスクトップに通知を表示	チェックボックスにチェックを入れると、ユーザーの操作が不要な警告ウインドウ（通知）をデスクトップに表示できます（既定では画面の右上角に表示します）。この設定を行った場合は、表示した警告ウインドウ（通知）が自動的に消えるまでの時間（秒単位）を設定できます。表示時間の設定は、[次の後に通知を自動的に閉じる] で行います。	

4.6.16 コンテキストメニュー

コンテキストメニューは、【control】キーを押しながらファイルやフォルダーをクリックしたときに表示されるメニューです。OS の設定で右クリックを有効にしている場合は、右クリックでも表示されます。ESET Endpoint アンチウイルス for OS X の機能をコンテキストメニューから利用したいときは、「コンテキストメニュー」の設定画面で行います。「コンテキストメニュー」の設定画面は、メインメニューの［設定］＞［詳細設定を表示する］をクリックし、「詳細設定」画面を表示して、［コンテキストメニュー］をクリックすることで表示できます。コンテキストメニューを利用するときは、[コンテキストメニューに統合] のチェックボックスにチェックを入れます。ログアウトまたはコンピューターの再起動後に、変更が有効になります。また、次のメニュータイプを設定できます。

完全	［完全］を選択すると、コンテキストメニューで利用できるすべての機能を表示します。
検査のみ	［検査のみ］を選択すると、コンテキストメニューに検査機能のみを表示します。
駆除のみ	［駆除のみ］を選択すると、コンテキストメニューに駆除機能のみを表示します。

●コンテキストメニューの表示

コンテキストメニューを表示したいときは、ファイル／フォルダーを【control】キーを押しながらクリックし、［サービス］から利用したい機能を選択します。

4.6.17 アップデート

アップデートの設定を行うには、メインメニューの［設定］>［詳細設定を表示する］をクリックして「詳細設定」画面を表示し、［アップデート］をクリックします。アップデートの設定では、アップデートサーバーやアップデートサーバーの認証データなど、アップデートファイルの送信元の情報を指定します。

「プライマリ」タブ	プライマリのアップデートサーバーの設定を行います。ESET Endpoint アンチウイルス for OS X では、代替またはフェイルオーバーのアップデートサーバーを設定できます。たとえば、プライマリのアップデートサーバーには社内に設置したミラーサーバーを設定し、セカンダリのアップデートサーバーには、標準のアップデートサーバー（自動選択）に設定します。このように設定しておくことで、ESET Endpoint アンチウイルス for OS X で使用する最適なアップデートサーバーを自動選択するフェイルオーバーアップデート機能を利用できます。なお、セカンダリのアップデートサーバーはプライマリのアップデートサーバーとは異なったサーバーである必要があります。同じアップデートサーバーを設定することはできません。
「セカンダリ」タブ	セカンダリのアップデートサーバーの設定を行います。通常は、社内と社外でアップデートサーバーを自動切り替えしたい場合などに設定します。セカンダリで設定するアップデートサーバーは、プライマリのアップデートサーバーとは異なっている必要があります。
アップデートサーバー	利用するアップデートサーバーの選択やアップデートサーバーへの認証情報（ユーザー名やパスワード）の設定を行います。既定値は、［自動選択］が選択されており、ESET 社の提供しているアップデートサーバー利用されます。社内にミラーサーバーが設置されている場合など、特定のアップデートサーバーを利用したい場合は、［編集］ボタンをクリックして、アップデートサーバーの情報の登録を行い、そのサーバーを選択します。アップデートサーバーの情報の登録方法については、「■ミラーサーバーからのアップデート」を参照してください。
詳細オプション	［設定］ボタンをクリックすると、アップデートに関する詳細な設定を行えます。詳細については、「●詳細設定オプション」を参照してください。
アップデートキャッシュを削除	［削除］ボタンをクリックすると、一時アップデートファイルとキャッシュを削除します。ウイルス定義データベースのアップデート時に問題が発生した場合は、［削除］をクリックして、一時アップデートファイルとキャッシュを削除してください。

! 重　要

アップデートファイルを正しくダウンロードするには、すべてのアップデートパラメーターを正しく設定してください。ファイアウォールを使用している場合は、ESET プログラムのインターネットとの通信（HTTP 通信）が許可されていることを確認してください。

●詳細設定オプション

アップデートの設定画面では、「詳細オプション」の［設定］ボタンをクリックすることでアップデートに関する詳細な設定が行えます。詳細オプションでは、次の項目について設定が行えます。

成功したアップデートについての通知を表示しない	チェックボックスにチェックを入れると、アップデートに成功するごとに表示される通知を無効にします。	
アップデートモード	アップデートモードの設定を行います。設定は、次の 3 種類から選択できます。	
	テストモード	テストモードは、テスト中の開発モジュールをダウンロードします。この設定は、ESET Endpoint アンチウイルス for OS X に問題が発生している場合など、製品の問題を解決したい場合に有効な設定です。
	通常アップデート	既定値で選択されているモードです。スケジューラーで設定された間隔でアップデートのチェックを行い、アップデートがある場合は、すぐにアップデートを実施します。正式版のみをダウンロードし、テスト中の開発モジュールは、ダウンロードしません。
	遅延アップデート	遅延アップデートは、正式版のリリースの数時間後にアップデートをダウンロードします。
アップデートのロールバック	ESET Endpoint アンチウイルス for OS X は、アップデートのロールバック機能を利用できるようにするために、ウイルス定義データベースとプログラムモジュールのスナップショットを記録しています。アップデートのロールバックは、ウイルス定義データベース／プログラムコンポーネントの新規アップデートが不安定な場合や、破損している疑いがある場合に、前のバージョンにロールバックすることで、ロールバックより後のアップデートを無効にして問題を解決するための機能です。次の項目について設定を行えます。	
	アップデートファイルのスナップショットを作成	チェックボックスにチェックを入れると、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スナップショットを自動的に作成します。
	スナップショットの数	コンピューターに保存するスナップショットの数を設定します。既定値は「2」に設定されています。
	ロールバックの時間	ロールバックを行いアップデートを一時停止する期間の設定を行えます。設定は、［12］時間、［24］時間、［36］時間、［48］時間、［取り消しまで］の中から選択できます。［取り消しまで］を選択した場合は、［アップデートを再開］ボタンを手動でクリックするまで、標準アップデートは再開されません。
	ロールバック	［ロールバック］ボタンをクリックすると、ロールバックを開始します。ロールバックを実行すると、ウイルス定義データベースのバージョンは使用できる最も古いバージョンにダウングレードされ、ローカルのクライアントコンピューターにスナップショットとして保存されます。
	アップデートを再開	［アップデートを再開］ボタンをクリックすると、ロールバックを行い、一時停止していた標準アップデートを再開します。

古いウィルス定義データベースアラート	ウイルス定義データベースが古くなったことを通知するまでの時間（日数）を設定できます。	
	以下の期間アップデートされていないときに警告する	チェックボックスにチェックを入れると、指定した期間アップデートされていないときに警告ウインドウを表示します。既定値では、7 日が設定されています。

■ミラーサーバーからのアップデート

アップデートサーバーとは、アップデートファイルが保存されている場所です。既定では、「自動選択」が有効になっています。ESET サーバーを使用するときには、既定のままにすることをお勧めします。社内に設置されたミラーサーバーなど、既定以外のアップデートサーバーを使用する場合は、「自動選択」を無効にして、手動でアップデートサーバーを指定します。アップデートサーバーの指定は、次の手順で行います。

操作手順

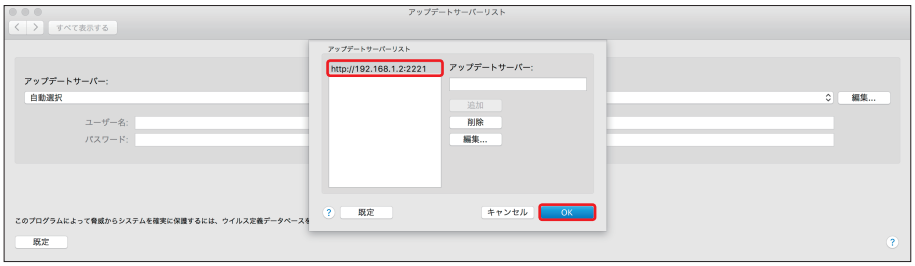
1. メインメニューの［設定］＞［詳細設定を表示する］をクリックし、「詳細設定」画面を表示します。
2. ［アップデート］をクリックします。
3. ［プライマリ］タブが選択されていることを確認し、［編集］ボタンをクリックします。

4. ［アップデートサーバー］にアップデートサーバーの情報を以下の形式で入力し、［追加］ボタンをクリックします。

   - **ローカルの HTTP サーバーを使用する場合**
     ［http://< クライアントコンピューター名または IP アドレス >:2221

   - **SSL を利用するローカルの HTTP サーバーを使用する場合**
     https://< クライアントコンピューター名または IP アドレス >:2221

5. アップデートサーバーリストに入力した情報が登録されます。［OK］ボタンをクリックします。



6 アップデートサーバーに手順4で入力した情報をポップアップメニューから選択します。

7 選択したアップデートサーバーへの接続アカウントが必要になるときは、ユーザー名やパスワードを設定します。

●ミラーサーバーからのアップデートに関するトラブルシューティング

一般的に、ミラーサーバーからのアップデート中に発生する問題の原因は、次のとおりです。

- ミラーサーバーの指定が正しくない
- ミラーサーバーにアクセスするための認証データが正しくない
- ミラーサーバーからアップデートファイルをダウンロードするローカルコンピューターの設定が正しくない
- 上記 3 つのエラーの組み合わせ

ミラーサーバーからのアップデート時に発生する問題の概要を紹介します。

ミラーサーバーへの接続エラーが通知される

原因として、ローカルコンピューターのアップデートファイルのダウンロード元であるアップデートサーバーが正しく指定されていないことが考えられます。ミラーサーバーのアドレスが間違っていないか確認してください。

ESET Endpoint アンチウイルス for OS X でユーザー名とパスワードが要求される

原因として、アップデートサーバーの設定で、認証データ（ユーザー名とパスワード）が正しく設定されていないことが考えられます。ユーザー名とパスワードは、アップデートファイルのダウンロード元であるアップデートサーバーにアクセスするために使用されます。認証データが適切な形式で正しく設定されていることを確認してください。

ミラーサーバーへの接続エラーが通知される

HTTP サーバーを使用したミラーサーバーへのアクセスで定義されているポート上の通信がブロックされています。

! 重 要

OS のファイアウォール機能によって、通信がブロックされていないか確認してください。

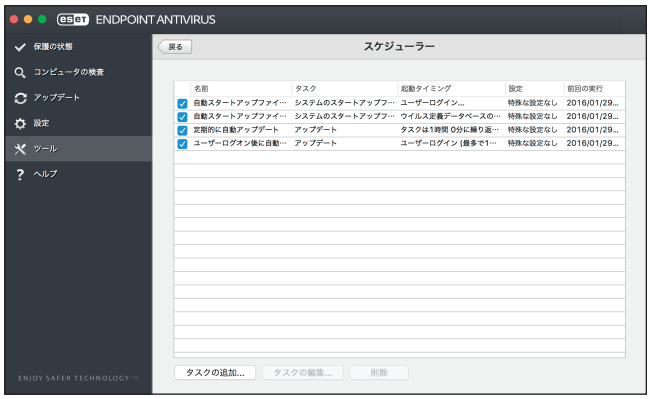
●アップデートタスクの作成

メインメニューの「アップデート」>［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、手動でアップデートすることができますが、スケジューラー機能でアップデートタスクを作成して実行することもできます。

アップデートタスクを作成するには、メインメニューの［ツール］>［スケジューラー］をクリックします。ESET Endpoint アンチウイルス for OS X では、次のタスクが既定で設定されています。

- 定期的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

既定のアップデートタスクは、ニーズに合わせて変更できます。また、既定のアップデートタスクとは別に、新しいアップデートタスクを作成することもできます。アップデートタスク作成の詳細については、「4.4.3　スケジューラー」を参照してください。



●システムアップデート

Mac OS X システム更新機能は、悪意のあるソフトウェアからユーザーを保護するための重要なコンポーネントです。最大限のセキュリティを維持するために、更新が利用可能になった時点でただちにインストールすることをお勧めします。OS のアップデートが行われていない場合、ESET Endpoint アンチウイルス for OS X は重要度レベルに従い、アップデートを通知します。通知が表示されたときは、ただちにインストールを行うことをお勧めします。

4.6.18 プロキシサーバー

大規模な LAN ネットワークでは、コンピューターがプロキシサーバーを介してインターネットに接続している場合があります。ESET Endpoint アンチウイルス for OS X をこのような環境で運用するには、プロキシサーバーを定義する必要があります。
プロキシサーバーの設定は、メインメニューの［設定］＞［詳細設定を表示する］をクリックし、「詳細設定」画面を表示して［プロキシサーバー］をクリックすることで行います。

ワンポイント
インターネットへの接続を必要とするすべての機能は、ここで設定したプロキシサーバーを使用します。

プロキシサーバを使用する	プロキシサーバーの使用を有効にします。
プロキシサーバー	プロキシサーバーのアドレスを設定します。
ポート	プロキシサーバーが使うポートを設定します。既定値は「3128」です。
ユーザー名	プロキシサーバーに認証が設定されている場合、ユーザー名を入力します。
パスワード	プロキシサーバーに認証が設定されている場合、パスワードを入力します。

4.6.19 共有ローカルキャッシュ

共有ローカルキャッシュを使用すると、ファイルとフォルダーの検査情報がキャッシュサーバーの共有キャッシュに保存されます。新しい検査を実行する際は、ESET Endpoint アンチウイルス for OS X がキャッシュサーバーのキャッシュにある検査済みファイル情報を検索し、ファイル情報が一致すれば検査から除外されます。これにより、ネットワーク上での検査の重複がなくなり、仮想環境のパフォーマンスが向上します。
共有ローカルキャッシュの設定は、メインメニューの［設定］＞［詳細設定を表示する］をクリックし、「詳細設定」画面を表示して［共有ローカルキャッシュ］をクリックすることで行います。また、次の設定項目が用意されています。

ESET 共有ローカルキャッシュを使用してキャッシュを有効にする	チェックボックスにチェックを入れると、ESET 共有ローカルキャッシュが有効になります。
サーバのアドレス	キャッシュがあるコンピューターの名前または IP アドレスです。
ポート	通信で使用されるポート番号（共有ローカルキャッシュと同じ）です。制限値は「0」～「65535」です。
パスワード	ESET 共有ローカルキャッシュのパスワードです。必要に応じて設定します。

Chapter 5 用語集

5.1 マルウェアの種類

マルウェアとは、コンピューターに入り込んで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。

5.1.1 ウイルス

コンピューターウイルスとは、コンピューター上の既存のファイルにあらかじめ追加されている、または後から追加される悪意の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。生物学上のウイルスと同じような手法でコンピューター間に蔓延していくからです。「ウイルス」という用語は、あらゆる種類のマルウェア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、より正確な用語である「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るようになっています。

コンピューターウイルスは、主に実行可能ファイルとドキュメントを攻撃します。コンピューターウイルスに感染すると、元のアプリケーションよりも前に悪意のあるコードが呼び出されて実行されます。ウイルスは、ユーザーが書き込み権限を持つすべてのファイルに感染することができます。

コンピューターウイルスの目的と重大さは多種多様です。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、自分の技量を誇示することだけが目的のウイルスもあります。

コンピューターがウイルスに感染して駆除できない場合は、詳しい検査のために感染したファイルを ESET ラボに送ることができます。場合によっては、駆除が不可能であるためクリーンなコピーに置き換える必要があるほど改ざんされていることがあります。

5.1.2 ワーム

コンピューターワームとは、ネットワークを介して感染先のコンピューターを攻撃して蔓延する、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ことです。ワームは宿主のファイル（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ーウイルスよりはるかに危険性が高いです。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。自己増殖する能力があるので、他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すると、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。コンピューターワームはその本来の性質ゆえに、他のマルウェアの「搬送手段」となります。

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

5.1.3 トロイの木馬

従来、コンピューター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、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ーに分類できます。

ダウンローダー	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。
ドロッパー	被害を受けるコンピューターに他のマルウェアを取り込む悪意のあるプログラム。
バックドアー	ネットワークを通じてコンピューターにアクセスし、遠隔操作でき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、ネットワークを通じてその情報を送信するプログラム。
ダイアラー	ユーザーのインターネットサービスプロバイダーではなく、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のあるプログラム。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。ダイアラーで被害を受けるのは、ダイアルアップモデムを使用するユーザーのみです。今日ではあまり使用されていません。

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

5.1.4 ルートキット

ルートキットとは、攻撃者が自己の存在を隠しながら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、Windows レジストリーデータを隠します。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、ルートキットに感染しているファイルを検出できれば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。
2. 通常の検査で検出されない場合は、ESET Endpoint アンチウイルス for OS X のアンチステルス技術を利用して、アクティブなルートキットを検出して駆除できます。

5.1.5 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、このカテゴリーに分類されます。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画面を Web ブラウザー内に自動的に開いたり、Web ブラウザー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。ユーザーが広告に悩まされるだけです。危険なのは、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があるということです。

フリーウェア製品を使用する場合には、インストールプログラムに特に注意してください。ほとんどのインストールプログラム（インストーラー）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、目的のプログラムのみ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ったりすることがあります。このようなプログラムをインストールした場合は、ユーザーがアドウェアのインストールに同意したことになり、アドウェアが頻繁にかつ「合法的に」システムにアクセスする危険性があります。後悔しないように、このようなプログラムはインストールしないほうが賢明です。

アドウェアとして検出されるファイルがコンピューターにある場合は、悪意のあるコードが含まれている可能性が高いため、削除することをお勧めします。

5.1.6 スパイウェア

このカテゴリーには、ユーザー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、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を調査し、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、と誰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プログラムの作成者がプログラムに同梱したり、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がよくあります。これは、スパイウェアが含まれていない有料バージョンにアップグレードするよう促すことで、収益を上げたり、プログラムを購入する動機を与えようとしているためです。

スパイウェアが組み入れられている有名なフリーウェア製品として、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ーに属します。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ーにある場合は、悪意のあるコードが含まれている可能性が高いため、削除することをお勧めします。

5.1.7 圧縮プログラム

圧縮プログラムは、複数のマルウェアを 1 つのパッケージにロールアップするランタイム自己解凍実行可能ファイルです。

最も一般的な圧縮プログラムには、UPX、PE_Compact、PKLite、ASPack があります。別の圧縮プログラムを使用して圧縮した場合、同じマルウェアが異なって検出されることがあります。圧縮プログラムには、シグネチャーを時間の経過と共に変化させ、マルウェアの検出と削除を困難にする機能もあります。

5.1.8 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ー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 アンチウイルス for OS X にはこのようなマルウェア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ーで実行されている（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。

5.1.9 望ましくない可能性があるアプリケーション

望ましくない可能性があるアプリケーションは、アドウェアを含んだり、ツールバーをインストールしたり、その他の不明確なオブジェクトを含んだりするプログラムです。場合によっては、ユーザーが望ましくない可能性があるアプリケーションを使用するリスクよりも利点の方が大きいと感じることがあります。このため、このようなアプリケーションには、トロイの木馬やワームなどのマルウェアと比べて、低いリスクのカテゴリーが割り当てられています。

■望ましくない可能性があるアプリケーションが検出された場合

次の警告画面が表示されます。

ユーザーは実行するアクションを選択できます。

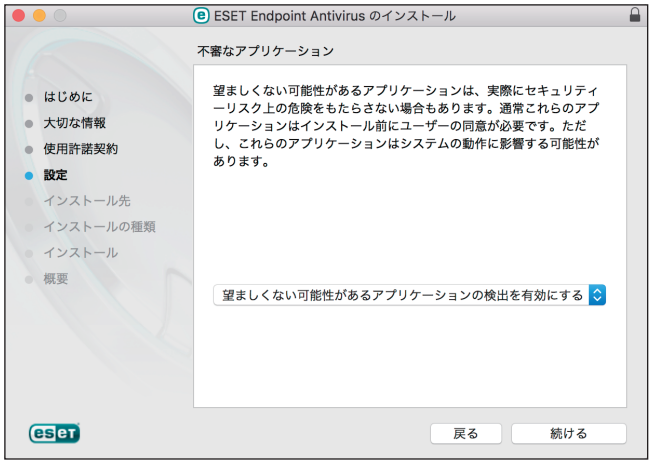
駆除／削除	アクションを終了し、潜在的な脅威がシステムに侵入するのを防ぎます。
何もしない	潜在的な脅威がシステムに侵入するのを許可します。

今後中断せずにコンピューターでアプリケーションを実行できるようにするには、［設定を表示する］をクリックし、［検出対象外］をチェックします。

望ましくない可能性があるアプリケーションが検出され、駆除できない場合は、デスクトップの右下に「アドレスがブロックされました」という通知が表示されます。通知の詳細を確認するには、メインメニューの［ツール］>［ログファイル］をクリックし、ドロップダウンメニューから［フィルタリングされた Web サイト］を選択します。

■望ましくない可能性があるアプリケーションに関する設定

ESET Endpoint アンチウイルス for OS X をインストールするとき、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かどうかを設定できます。



また、望ましくないアプリケーションの検出設定は、設定オプションで変更できます。変更するには、次の操作を行います。

操作手順

1. ESET Endpoint アンチウイルス for OS X を開きます。ESET Endpoint アンチウイルス for OS X の開き方については「2.5　コンピューターの検査」の手順❶～❷を参照してください。
2. ［設定］をクリックします。
3. ［詳細設定を表示する］をクリックします。
4. ［一般］をクリックします。
5. 次の各機能を有効または無効にします。
   - 望ましく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
   - 疑わしいアプリケーション

■ソフトウェアラッパー

ソフトウェアラッパーは特殊なタイプの修正アプリケーションで、ファイルホスティング Web サイトの一部で使用されます。ソフトウェアラッパーはサードパーティー製のツールですが、ツールバーやアドウェアなどの追加ソフトウェアもインストールします。追加されたソフトウェアは、Web ブラウザーのホームページや検索設定を変更する場合があります。多くの場合、ファイルホスティング Web サイトはソフトウェアベンダーやダウンロード受信者に設定が変更されたことを通知しないため、変更を回避することができません。このため、ESET Endpoint アンチウイルス for OS X はソフトウェアラッパーを望ましくない可能性のあるアプリケーションのタイプに分類しています。ユーザーはソフトウェアラッパーをダウンロードするかどうかを設定できます。

5.1.10 ボットネット

ボットまたは Web ロボットは自動マルウェアプログラムであり、ネットワークアドレスのブロックを検査し、脆弱なコンピューターを感染させます。ボットを利用することでハッカーが同時に複数のコンピューターを乗っ取り、コンピューターをボット（ゾンビ）に変えることができます。一般的に、ハッカーはボットを使用して、多数のコンピューターを感染させます。このような大規模な感染コンピューターのグループがボットネットと呼ばれます。コンピューターが感染してボットネットのメンバーになると、分散型サービス拒否攻撃（DDoS）で使用されます。また、ユーザーが知らない間に、インターネット上での自動乗っ取りを実行するためにコンピューターが使用されることもあります（迷惑メール、ウイルスの送信、銀行の認証情報やクレジットカード番号などの個人情報の窃盗など）。

5.2 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、いくつかのカテゴリーに分類できます。

5.2.1 ワーム攻撃

コンピューターワームとは、ネットワークを介して感染先のコンピューターを攻撃して蔓延する、悪意のあるコードが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。インターネットを通じて、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。

ほとんどのワーム攻撃は、ファイアウォールの既定のセキュリティ設定で回避できます。また、パブリックネットワークではパブリックネットワーク保護タイプを選択し、最新のセキュリティパッチを適用して、オペレーティングシステムとプログラムを最新の状態に保つことが重要です。

5.2.2 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ーやネットワークを使用できないようにする行為です。攻撃を受けた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ができなくなります。DoS 攻撃にさらされたコンピューターを正常に機能させるには、通常再起動する必要があります。

ほとんどの場合、標的とされるのは Web サーバーであり、目的はある程度の期間ユーザーがサーバーを使用できなくすることです。

5.2.3 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を特定するのに使用されます。ポートスキャナーは開いている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の出入り口のことです。セキュリティの観点では、ポートは重要な要素です。ネットワークが大規模な場合、ポートスキャナーが収集した情報が、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ー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にすることをお勧めします。

5.2.4 DNS キャッシュポイズニング

DNS（ドメインネームサーバー）キャッシュポイズニングを使用すると、ハッカーは任意のコンピューターの DNS サーバーを騙し、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ー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。

5.2.5 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ことが要因となります。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、現在の通信画面に存在する場合には、バッファメモリーに保存されます）。

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、サーバー／クライアント通信や P2P 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。

5.2.6 SMB リレー

SMBRelay と SMBRelay2 は、リモートコンピューター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 内でフォルダーやディレクトリーを共有する場合、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ー間で交換されるパケットを中継して、パケットを書き換えます。認証後、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ー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。この場合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、変更を密かに行えます。このような攻撃にさらされたコンピューターは、応答しなくなるか、突然再起動することがよくあります。

SMB リレーによる攻撃を避けるため、認証パスワードか認証鍵の使用をお勧めします。

5.2.7 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ーによって使用されます。

リモートの攻撃者は、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、リモートの攻撃者は、いわゆる DoS 攻撃（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、smurf 攻撃があります。ICMP 攻撃にさらされたコンピューター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すべ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。

5.3 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、電子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）を拡散します。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電子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。電子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、インターネットに電子メールアドレスを公開しない。
- 信頼できる個人のみに電子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。
- 仕事専用と友人専用など、用途ごとに異なる電子メールアドレスを使用する。
- 電子メールアドレスを定期的に変更する。
- 迷惑メール対策ソリューションを使用する。

5.3.1 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 1 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、直接的に訴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。

一方的に送信されてくるメールの量が実際に問題になっており、減少する兆しはありません。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。

5.3.2 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、Skype などの通信ツールを経由して送信されます。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。

コンピューター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、ファイルを削除させたり、パスワードを取得させたりします。また、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、援助の訴え、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。デマの疑いがあるメッセージを受け取った場合は、安易に転送などしないよう、注意してください。

5.3.3 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、電子メールを送ることです。この電子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、銀行の口座番号やユーザー名、パスワードなど個人データを入力するようユーザーに指示します。このようなデータは、一度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が、受信者側が送信を要求していない電子メールでユーザー名とパスワードを入力するように要求することは決してありません。

5.3.4 迷惑メール詐欺の特定

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）を特定するためのチェック項目がいくつかあります。受信メールが次のチェック項目のいくつかに該当する場合は、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はない。
- 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、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ー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ーを騙そうとして、単語のスペルを間違えている。
  例えば、「viagra」の代わりに「vaigra」と記載している場合などです。

■サーバー側での検査

サーバー側での検査とは、受信メール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。各電子メールは、その内容に基づいて固有のデジタルな「痕跡」を残します。痕跡で電子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。

ある電子メールが迷惑メールとしてマークされた場合、その痕跡がサーバーに送信されます。サーバーが迷惑メールとしてマークされた電子メールと同じ痕跡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。受信メールを検査する際に、電子メールの痕跡がサーバーに送信されます。サーバーは迷惑メールとして既にマークされている電子メールの痕跡に関する情報を返します。

5.4 ESET 技術

5.4.1 ESET LiveGrid

ThreatSense.Net 高度早期警告システム上に構築された ESET LiveGrid は、ESET ユーザーが世界中で提出したデータを収集し、ESET のウイルスラボに送信します。世界中の不審なサンプルとメタデータを提供することで、ESET LiveGrid は、ユーザーのニーズに即時に対応し、最新の脅威に対する ESET の対応力を確保できます。ESET のマルウェア研究者はこの情報を使用して、脅威の特性と範囲の正確なスナップショットを構築し、適切な目標に集中できるようにします。ESET LiveGrid データは自動処理される機能の中で優先度の高いものです。

また、レピュテーションシステムを導入し、マルウェア対策ソリューションの全体的な効率を改善します。実行ファイルまたはアーカイブがユーザーのシステム上で検査されているときに、まずハッシュタグがホワイトリストおよびブラックリスト項目のデータベースで比較されます。ホワイトリストで検出された場合、検査されたファイルはクリーンとみなされ、今後の検査対象から除外するように設定されます。ブラックリストで検出された場合、脅威の特性に応じて適切なアクションが実行されます。一致するものがない場合、ファイルは徹底的に検査されます。この検査の結果に基づいて、ファイルは脅威または脅威以外に分類されます。このアプローチは、検査のパフォーマンスに対して好ましい影響を及ぼします。

レピュテーションシステムによって、1 日に数回ウイルス定義データベース経由でシグネチャーがユーザーに配信される前に、マルウェアサンプルを効果的に検出できます。

5.5 FAQ

よくある質問と問題をいくつか紹介します。問題の解決方法を調べるには、該当するトピックをクリックしてください。

上記に含まれていない問題や疑問を解決したい場合は、ESET Endpoint アンチウイルス for OS X ヘルプページでキーワードを入力して検索してください。

ESET Endpoint アンチウイルス for OS X をアップデートする方法

ESET Endpoint アンチウイルス for OS X は、手動または自動でアップデートできます。アップデートを開始するには、メインメニューの［アップデート］>［今すぐアップデート］をクリックします。

既定では、1 時間ごとに自動的にアップデートが実行されるタスクが登録されています。間隔を変更するには、メインメニューの［ツール］>［スケジューラー］をクリックします。スケジューラーの詳細については、「4.4.3 スケジューラー」を参照してください。

ESET Endpoint アンチウイルス for OS X をアクティベートする方法

インストール完了後、ESET Endpoint アンチウイルス for OS X のアクティベーションが求められます。

アクティベーションについては、「2.4 アクティベーション」を参照してください。

任意のタイミングで製品ライセンスを変更するには、メインメニューの［ヘルプ］をクリックします。カスタマーサポートに問い合わせる際に、ライセンスを識別するために必要になるライセンス ID が表示されます。

コンピューターからウイルスを取り除く方法

使用しているコンピューターが、マルウェアに感染している兆候（処理速度が遅くなる、頻繁にフリーズするなど）を示している場合、次の処置を取ることをお勧めします。

操作手順

1. メインメニューの［コンピュータの検査］をクリックします。
2. ［スマート検査］をクリックします。

ワンポイント
ディスクの一部のみを検査するには、［カスタム検査］をクリックし、検査する対象を選択します。

3. 検査が完了したら、検査されたファイル、感染しているファイル、駆除されたファイルの数をログで確認します。

詳細については、「4.1　コンピューターの検査」を参照してください。

スケジューラーで新しいタスクを作成する方法

メインメニューの［ツール］>［スケジューラー］をクリックすると、スケジューラー画面が表示されます。［タスクの追加］ボタンをクリックするか、一覧を【control】キーを押しながらクリックし、コンテキストメニューから［追加］をクリックすると、新しいタスクを作成できます。タスクには次の 4 種類があります。

外部アプリケーションの実行	外部アプリケーションを実行します。
アップデート	ウイルス定義データベースおよびプログラムコンポーネントをアップデートします。
コンピュータの検査	コンピューター上のファイルやフォルダーを検査します。
システムの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時に実行されるファイルを検査します。

スケジューラーに登録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ため、ここでは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。

操作手順

1. タスク名を入力します。
2. 「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。
3. ドロップダウンメニューからタスクを実行するタイミング（頻度）を選択します。

- 1 回
- 繰り返し
- 毎日
- 毎週
- イベントごと

ワンポイント
「コンピューターがバッテリーで動作している場合は実行しない」のチェックボックにチェックを入れると、ノートパソコンのバッテリー電源での実行中はタスクを実行せず、システムリソースを最小化できます。

続く

4 ［次へ］をクリックします。

5 タスクの実行時刻を指定します。
設定内容は、手順❸で設定したタスクのタイミングによって異なります。

6 ［次へ］をクリックします。

7 「タスクが実行されなかった場合」で、指定し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選択します。

- 次のスケジュール設定日時まで待機
- 実行可能になり次第実行する
- 前回実行されてから次の時間が経過した場合は直ちに実行する（「タスクの最小間隔（DD:HH:MM）」のスクロールボックスを使用して間隔を指定します）

8 ［次へ］をクリックします。

9 ［終了］ボタンをクリックします。
「スケジューラー」の一覧に作成したタスクが追加されます。

検査を 24 時間ごとに実行するタスクを作成する方法

ローカルディスクの検査を 24 時間ごとに実行するタスクを作成する方法は、次のとおりです。

操作手順

1 メインメニューの［ツール］>［スケジューラー］をクリックします。

2 ［タスクの追加］をクリックするか、一覧を【control】キーを押しながらクリックし、コンテキストメニューから［追加］をクリックします。
「タスクの追加」画面が表示されます。

3 タスク名を入力します。

4 ［スケジュールタスク］ドロップダウンメニューから［コンピュータの検査］を選択します。

5 ドロップダウンメニューからタスクを実行するタイミング（頻度）に［繰り返し］を選択します。

6 ［次へ］をクリックします。

7 ［プロファイルの選択］の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。

8 ［検査の対象］を選択します。ハードディスク（SSD）全体を検査するときは、検査したいドライブ（初期値では「Macintosh HD」）にチェックを入れます。

9 ［次へ］ボタンをクリックします。

続く

10 ［タスクの実行間隔（DD:HH:MM）］に「1：0：0」を設定します。

11 ［次へ］ボタンをクリックします。

12 「タスクが実行されなかった場合」で、指定し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選択します。

13 ［終了］ボタンをクリックします。
「スケジューラー」の一覧にローカルディスクを 24 時間ごとに検査するタスクが追加されます。

ESET Endpoint アンチウイルス for OS X を ESET Remote Administrator に接続する方法

コンピューターに ESET Endpoint アンチウイルス for OS X をインストールし、ESET Remote Administrator 経由で接続する場合、クライアントワークステーションに ERA エージェントがインストールされていることを確認します。ERA エージェントは、ERA サーバーと通信するすべてのクライアントソリューションの基本要素です。ESET Remote Administrator は、ネットワーク上でコンピューターを検索するために RD Sensor ツールを使用します。RD Sensor で検出されるネットワーク上のすべてのコンピューターが Web コンソールに表示されます。

ERA エージェントが展開されたら、クライアントコンピューターで ESET セキュリティ製品のリモートインストールを実行できます。リモートインストールの詳細な手順については、『ESET Remote Administrator ユーザーズマニュアル』を参照してください。