System Center

Endpoint Protection Mac

インストールマニュアルとユーザガイド

Microsoft

目次

System Center Endpoint Protection

Unixベースのオペレーティングシステムを使用するユーザーが増えるにつれて、Macユーザーをターゲットとして作成されるマルウェアの脅威が増大しています。System Center Endpoint Protectionは、そのような新たな脅威に対して強力かつ効率のよい保護を提供します。また、System Center Endpoint ProtectionにはWindowsの脅威を回避する機能も搭載されており、Windowsユーザーとやり取りするMacユーザーを保護します(逆も同様です)。Windowsのマルウェアは、Macの直接の脅威とはなりませんが、Macマシンに感染したマルウェアを無効にすることで、ローカルネットワークまたはインターネットを介して脅威がWindowsベースのコンピューターに拡散しないようにすることができます。

システム要件

System Center Endpoint Protectionのパフォーマンスを最大化するには、システムは、次のようなハードウェアおよびソフトウェア要件を満たしている必要があります。

System Center Endpoint Protection:

	システム要件
プロセッサーのアーキテクチャ	32bit、64bit Intel R
オペレーティングシステム	Mac OS X 10.6以降
メモリ	512 MB
空きディスク容量	100 MB

インストール

インストール処理を開始する前に、コンピュータ上に開いているすべてのプログラムを閉じてください。System Center Endpoint Protectionには、すでにコンピュータにインストールされているその他のウイルス対策プログラムと競合する可能性のあるコンポーネントが含まれています。問題の生じる可能性をなくすため、他のウイルス対策プログラムを削除することを強く推奨します。System Center Endpoint Protectionは、インストールCD/DVDまたは弊社Webページから入手できるファイルを使用してインストールできます。

インストールウィザードを起動するには、次のいずれかを実行します。

- インストールCD/DVDからインストールする場合、CD/DVDをコンピューターに挿入し、デスクトップまたは[Finder]ウィンドウから開き、[**インストール**]アイコンをダブルクリックします。
- ダウンロードしたファイルを使用してインストールする場合は、ダウンロードしたファイルを開き、[**インストール**]アイコンをダブルクリックします。

インストーラーを起動すると、インストールウィザードが表示されるので、その案内に従って基本設定を行ってください。ソフトウェア使用許諾契約書に同意し、プライバシー声明を読んだ後、インストールの種類を以下から選択することができます。

- 標準 4
- カスタム 5

標準インストール

標準インストールモードには、ほとんどのユーザーに適した設定オプションが用意されています。この設定は、最大限のセキュリティと優れたシステムパフォーマンスの組み合わせを実現します。標準インストールは既定のオプションで、固有の設定に対して特定の要件を必要としない限り推奨されます。

[**標準**]インストールモードを選択してから、[**望ましくない可能性があるアプリケーションの検出**]を設定します。望ましくない可能性があるアプリケーションは、必ずしも悪意があるとは限りませんが、オペレーティングシステムの動作に悪影響を及ぼす可能性があります。これらのアプリケーションは、その他のプログラムに組み込まれていることが多く、インストールプロセス時に気付きにくいことがあります。これらのアプリケーションは通常インストール時に通知を表示しますが、同意なしにインストールできるので、ユーザーが安易にインストールしてしまうこともあります。

System Center Endpoint Protectionをインストールした後、悪意あるコードを対象としたコンピューターの検査を実行する必要があります。そのために、メインプログラムウィンドウから[**コンピューターの検査**]をクリックし、[**Smart検査**]をクリックします。コンピューターの検査の詳細については、「コンピューターの検査 11」を参照してください。

カスタムインストール

カスタムインストールモードは、経験豊富なユーザーがインストールプロセス中に詳細な設定を変更できるように設計されています。

[**カスタム**]インストールモードを選択すると、[**プロキシサーバー**]を設定するためのプロンプトが表示されます。プロキシサーバーを使用している場合は、[**プロキシサーバーを使用する**]オプションを選択することによって、パラメーターを定義できます。[**アドレス**]フィールドにプロキシサーバーのIPアドレスまたはURLを入力します。[ポート]フィールドには、プロキシサーバーが接続を受け付けるポートを指定します(既定では3128です)。プロキシサーバーで認証が要求される場合は、有効な[**ユーザー名**]と[**パスワード**]を入力して、プロキシサーバーへのアクセスを可能にする必要があります。プロキシサーバーを使用していないことがわかっている場合は、[**プロキシサーバーを使用しない**]オプションを選択します。不明な場合は、[**システム設定と同じ設定を使用する(推奨)**]を選択すると、現在のシステム設定を使用できます。

次のステップでは、プログラム設定を編集できる[**権限ユーザーの定義**]を設定します。左側のユーザー一覧からユーザーを選択し、[**追加**]をクリックして[**権限ユーザー**]の一覧に追加します。全てのシステムユーザーを表示するには、[**全ユーザーを表示**]オプションを選択します。

インストールプロセスの次のステップでは、[**望ましくない可能性があるアプリケーションの検出**]を設定します。望ましくない可能性があるアプリケーションは、必ずしも悪意があるとは限りませんが、オペレーティングシステムの動作に悪影響を及ぼす可能性があります。これらのアプリケーションは、その他のプログラムに組み込まれていることが多く、インストールプロセス時に気付きにくいことがあります。これらのアプリケーションは通常インストール時に通知を表示しますが、同意なしにインストールできるので、ユーザーが安易にインストールしてしまうこともあります。

System Center Endpoint Protectionをインストールした後、悪意あるコードを対象としたコンピューターの検査を実行する必要があります。そのために、メインプログラムウィンドウから[**コンピューターの検査**]をクリックし、[**Smart検査**]をクリックします。コンピューターの検査の詳細については、「コンピューターの検査 11」を参照してください。

アンインストール

コンピューターからSystem Center Endpoint Protectionをアンインストールする場合、以下を行います。

- コンピューターにSystem Center Endpoint ProtectionインストールCD/DVDを挿入し、これをデスクトップまたは[Finder]ウィンドウから開き、[**アンインストール**]アイコンをダブルクリックします。
- System Center Endpoint Protection インストールファイル(.dmg)を開き、[**アンインストール**]アイコンをダブルクリックするか、
- [Finder]を起動し、ハードドライブにある[**アプリケーション**]フォルダーを開き、Ctrlを押しながらSystem Center Endpoint Protectionアイコンをクリックして、[**パッケージコンテンツを表示**]オプションを選択します。[Contents > Helpers]フォルダーを開き、[Uninstaller]アイコンをダブルクリックします。

初心者向けガイド

この章では、System Center Endpoint Protectionとその基本設定の初期概要について説明します。

ユーザーインターフェイス

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

次に、メインメニューにあるオプションについて説明します。

- [**保護の状態**] - System Center Endpoint Protectionの保護の状態に関する情報が表示されます。[**詳細モード**]を有効にすると、[**統計**]サブメニューが表示されます。
- [**コンピューターの検査**] - このオプションを使用すると、[コンピューターの検査]の設定や起動を行うことができます。
- [**アップデート**] - ウイルス定義データベースのアップデートに関する情報が表示されます。
- [**設定**] – このオプションを選択すると、コンピューターのセキュリティレベルを調整することができます。[**詳細モード**]を有効にすると、[**ウイルス・スパイウェア対策**]サブメニューが表示されます。
- [**ツール**] - [**ログファイル**]? [**隔離**]および[**スケジューラ**]にアクセスできます。このオプションは[**詳細モード**]の場合にのみ表示されます。
- [**ヘルプ**] - プログラム情報とヘルプファイルへのアクセスを提供します。

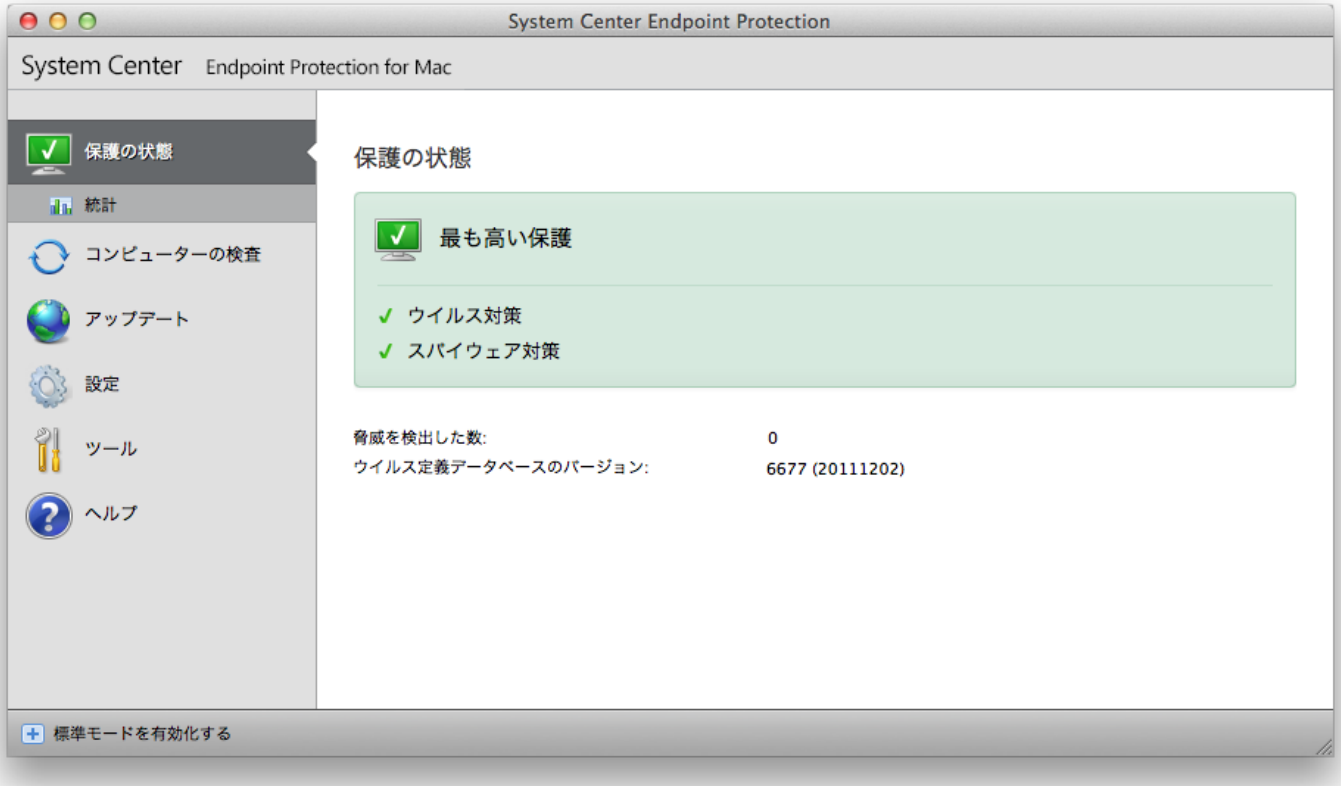
System Center Endpoint Protectionのユーザーインターフェイスでは、標準モードと詳細モードを切り替えることができます。標準モードでは、一般的な操作に必要な機能にアクセスすることができます。詳細設定オプションは表示されません。モードを切り替えるには、メインプログラムウィンドウの左下にある[**詳細モードを有効化する**]/[**標準モードを有効化する**]の横のプラスアイコン(+)をクリックするか、cmd+Mを押します。

詳細モードに切り替えると、[**ツール**]オプションがメインメニューに追加されます。[**ツール**]オプションを使用すると、[**ログファイル**]? [**隔離**]、および[**スケジューラ**]のサブメニューにアクセスできます。

注意: このガイドの残りの説明は、[**詳細モード**]で全て実行されています。

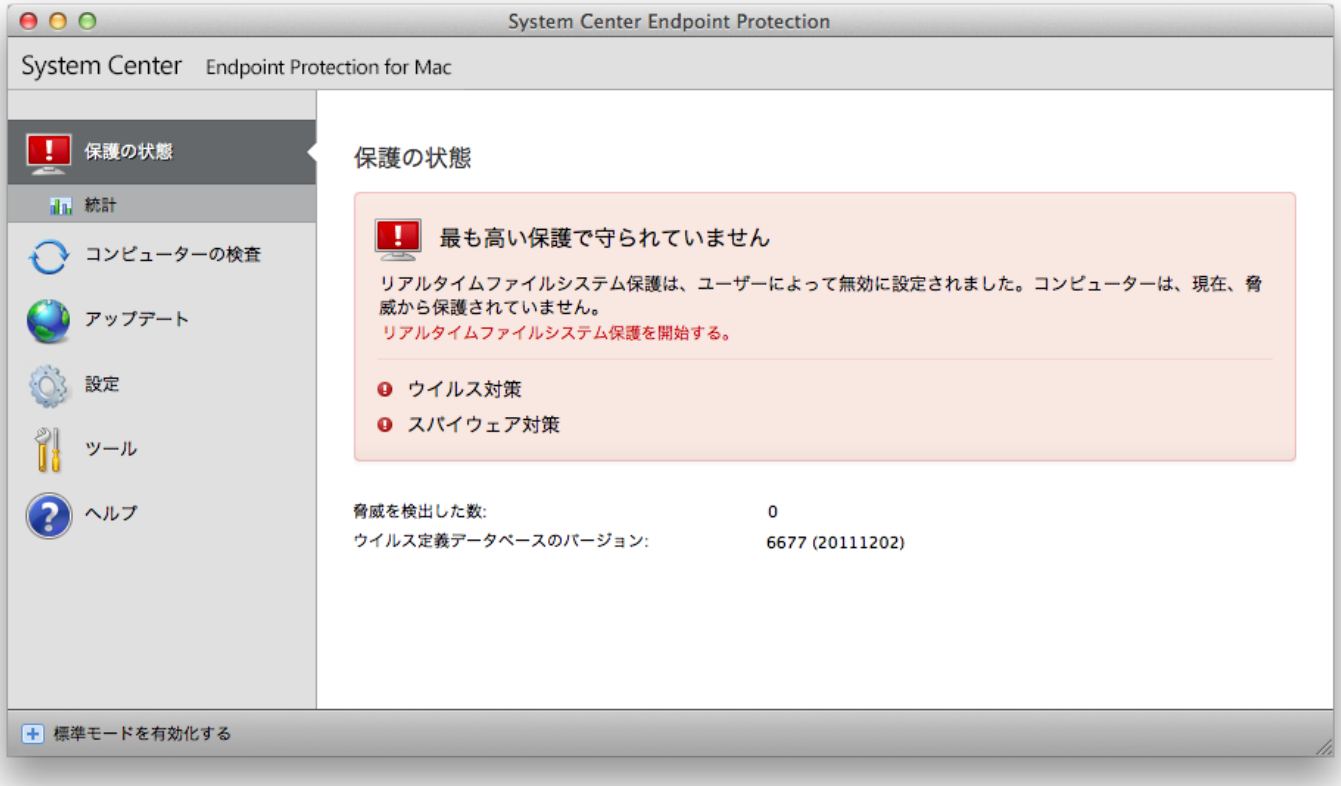
システムの動作の確認

[**保護の状態**]を表示するには、メインメニューの一番上のオプションをクリックします。プライマリウィンドウにはSystem Center Endpoint Protectionの動作状態の概要と[**統計**]などのサブメニューが表示されます。[統計]を選択すると、システムで実行されたコンピューターの検査に関する詳細な情報と統計が表示されます。[統計]ウィンドウは詳細モードの場合にのみ使用できます。



プログラムが正しく動作しない場合の解決方法

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



System Center Endpoint Protectionの操作

ウイルス・スパイウェア対策

ウイルス・スパイウェア対策は、潜在的な脅威を与えるファイルを修正することによって、悪意のあるシステム攻撃を防御する機能です。悪意のあるコードを含む脅威が検出されると、ウイルス対策機能がブロックし、次に駆除、削除、または移動して隔離することにより、ウイルスを排除できます。

リアルタイムファイルシステム保護

リアルタイムファイルシステム保護では、システムで発生する、ウイルス対策に関係するイベントを全て検査します。ファイルはすべて、コンピューター上で開くとき、作成するとき、または実行するときに、悪意のあるコードがないか検査されます。リアルタイムファイルシステム保護は、システム起動時に開始されます。

リアルタイム保護の設定

リアルタイムファイルシステム保護では、あらゆる種類のメディアを調べます。検査は多種多様なイベントによってトリガーされます。リアルタイムファイルシステム保護は、新たに作成されたファイルと既存のファイルとでは異なることがあります。新規作成ファイルの場合、より深いレベルの検査を適用できます。

既定では、リアルタイム保護はシステム起動時に起動し、中断されることなく検査が行われます。他のリアルタイムスキャナーと競合する場合などの特殊な場合は、メニューバー(画面最上部)のSystem Center Endpoint Protectionアイコンをクリックし、[**リアルタイムファイルシステム保護を無効化する**]オプションを選択して、リアルタイム保護を終了することができます。リアルタイム保護はメインウィンドウから終了することもできます([**設定**] > [**ウイルス・スパイウェア対策**] > [**無効化**])。

リアルタイム保護の詳細設定を変更するには、[**設定**] > [**アプリケーション設定を入力する...**]> [**保護**] > [**リアルタイム保護**]に移動して、[**詳細設定オプション**]の横にある[**設定...**]ボタンをクリックします(「詳細検査オプション 9」セクションを参照)。

検査のタイミング(イベント発生時の検査)

既定では、全てのファイルが、**ファイルを開くとき**? **ファイルを作成するとき**、または**ファイルを実行するとき**に検査されます。既定の設定によりコンピューターが最大限のレベルでリアルタイムに保護されるので、既定の設定を変更しないことをお勧めします。

詳細検査オプション

このウィンドウでは、スキャンエンジンで検査するオブジェクトの種類を定義し、[**アドバンスドヒューリスティック**]を有効化/無効化できます。アーカイブおよびファイルキャッシュの設定を変更することもできます。

アーカイブネストの値を大きくするとシステムのパフォーマンスが低下する場合があるため、特定の問題を解決するために必要でない限り、[**既定のアーカイブ設定**]セクションの既定値を変更しないことをお勧めします。

実行済み、作成済み、変更済みのファイルに対してそれぞれ別々にアドバンスドヒューリスティック検査のオンとオフを切り替えることができます。それには、個々のエンジンパラメーターセクションで[**アドバンスドヒューリスティック**]チェックボックスをクリックします。

リアルタイム保護を使用する際に、最適化キャッシュのサイズを定義し、システムフットプリントを最小化することができます。この動作は、[**未感染ファイルをキャッシュ**]オプションが有効の場合にアクティブになります。このオプションが無効の場合、全てのファイルがアクセスのたびに検査されます。定義したキャッシュのサイズに達するまで、キャッシュされたファイルが繰り返し検査されることはありません(ファイルが変更されている場合は除く)。ウイルス定義データベースがアップデートされると、直ちにファイルが再検査されます。

このオプションを有効化/無効化するには、[**未感染ファイルをキャッシュ**]をクリックします。キャッシュされるファイルの容量を設定するには、[**キャッシュサイズ**]の横の入力フィールドに値を入力します。

[**エンジンの設定**]ウィンドウでその他の検査パラメーターを設定できます。リアルタイムファイルシステム保護に関しては、検査対象の**オブジェクト**の種類を**オプション**と**駆除**レベルの組み合わせで定義できます。また、検査対象に課す**制限**を**拡張子**とファイルサイズで定義することもできます。エンジンの設定ウィンドウを表示するには、[詳細設定]ウィンドウで[**エンジン**]の横にある[**設定...**]ボタンをクリックします。エンジンのパラメーターの詳細については、「エンジンのパラメーターの設定 14」を参照してください。

検査からの除外

このセクションでは、特定のファイルやフォルダーを検査から除外することができます。

- **パス** - 除外されるファイルやフォルダーのパスです。
- **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。したがって、このファイルが後で他のマルウェアに感染した場合は、ウイルス対策機能によって検出されます。
- **追加...** - オブジェクトを検出対象外にします。対象のパスを入力するか(ワイルドカード*および?を使用できます)、あるいはツリー構造でフォルダーまたはファイルを選択します。
- **編集...** - 選択したエントリーを編集します。
- **削除** - 選択したエントリーを削除します。
- **既定** - 全ての除外対象を取り消します。

リアルタイム保護の設定の変更

リアルタイム保護は、安全なシステムを維持するために最も必要不可欠な要素です。リアルタイム保護パラメーターを変更する場合は、注意が必要です。特定の状況に限ってパラメーターを変更することをお勧めします。たとえば、特定のアプリケーションや別のウイルス対策プログラムのリアルタイムスキャナーとの競合がある場合などです。

System Center Endpoint Protectionのインストール後は、最大レベルのシステムセキュリティをユーザーに提供するようにすべての設定が最適化されています。既定の設定に戻すには、[**リアルタイム保護**]ウィンドウ([**設定**] > [**アプリケーション設定を入力する...**]> [**保護**] > [**リアルタイム保護**])の左下にある[**既定**]ボタンをクリックします。

リアルタイム保護の確認

リアルタイム保護が機能しており、ウイルスを検出することを確認するため、eicar.comのテストファイルを使用します。このテストファイルは、あらゆるウイルス対策プログラムで検出できる特殊な無害のファイルです。このファイルは、EICAR (European Institute for Computer Antivirus Research)が、ウイルス対策プログラムの機能をテストする目的で作成しました。

リアルタイム保護のステータスを確認するには、**ターミナル**を使用してリモートでクライアントコンピュータに接続し、次のコマンドを発行します。

```
/Applications/.scep/Contents/MacOS/scep_daemon --status
```

リアルタイム検査のステータスは、`RTPStatus=Enabled`または`RTPStatus=Disabled`として表示されます。

ターミナルBASHの出力には次のステータスも含まれます。

- クライアントコンピュータにインストールされたSystem Center Endpoint Protectionのバージョン
- ウイルス署名データベースの日付とバージョン
- 更新サーバーへのパス

注意: ターミナルの使用は上級ユーザーにのみ推奨されます。

リアルタイム保護が機能しない場合の解決方法

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

リアルタイム保護が無効である
ユーザーが不注意にリアルタイム保護を無効にしてしまった場合は、再開する必要があります。リアルタイム保護を再開するには、[**設定**] > [**ウイルス・スパイウェア対策**]に移動し、メインプログラムウィンドウの[**リアルタイムファイルシステム保護を有効化する**]をクリックします。あるいは、[詳細設定]ウィンドウの[**保護**] > [**リアルタイム保護**]で、[**リアルタイムファイルシステム保護を有効化する**]オプションを選択して、リアルタイムファイルシステム保護を有効化することもできます。

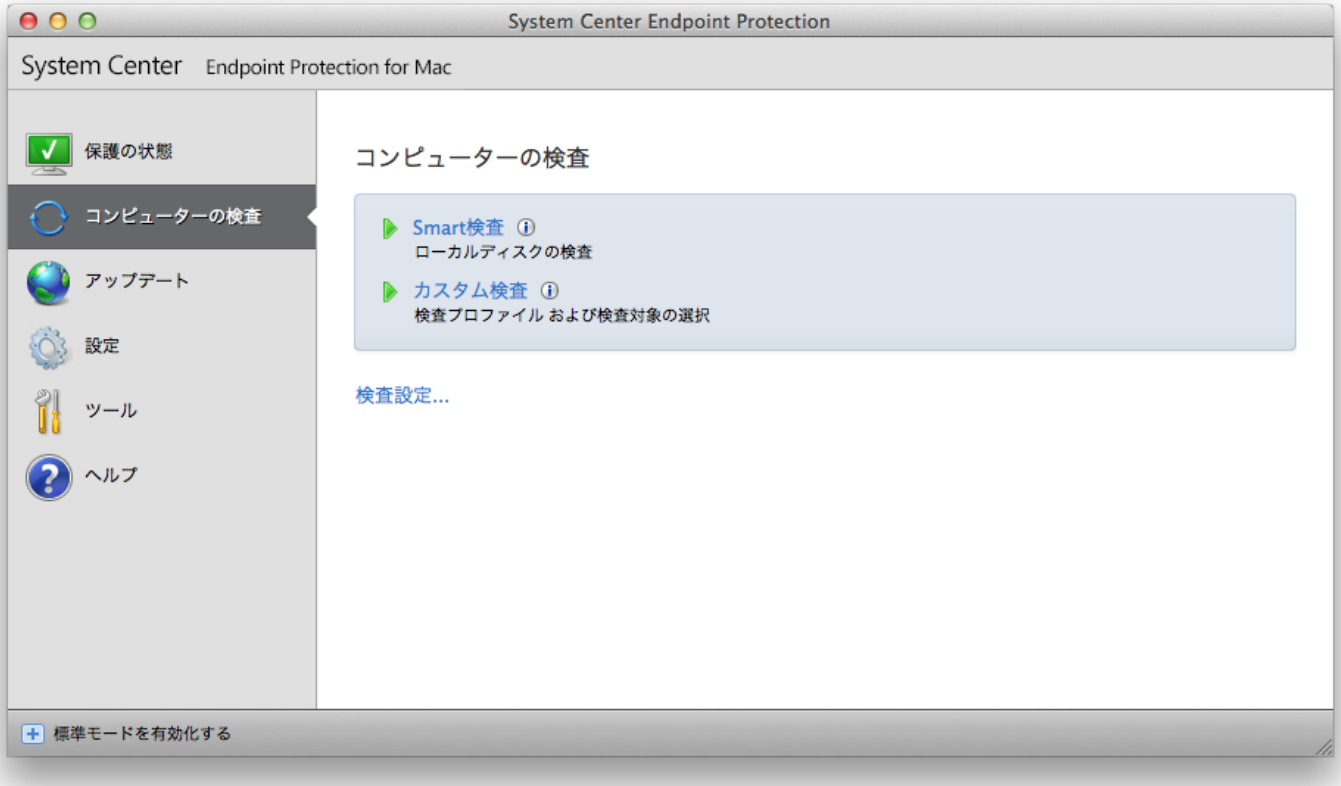
リアルタイム保護が侵入物の検出と駆除を行わない
コンピューターに他のウイルス対策プログラムがインストールされていないことを確認します。2つのリアルタイム保護シールドが同時に有効になっていると、互いに競合することがあります。システムから他のウイルス対策プログラム(インストールされている場合)をアンインストールすることをお勧めします。

リアルタイム保護が開始されない
リアルタイム保護がシステム起動時に開始されない場合、他のプログラムとの競合が原因であることがあります。この場合には、カスタマーサポート担当者までご相談ください。

コンピューターの検査

コンピューターの動作が異常で感染していると思われる場合には、[**コンピューターの検査**] > [**Smart検査**]を実行して、コンピューターに侵入物がいないかどうかを調べます。保護機能の効果を最大化するため、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手段の一環として定期的に実行する必要があります。検査を定期的に行うと、ディスクに保存されたときにリアルタイムスキャナーで検出されなかった侵入物でも、検出できます。リアルタイムスキャナーで検出できないケースとは、感染時にリアルタイムスキャナーが無効に設定されていた場合や、ウイルス定義データベースが最新でない場合などです。

コンピューターの検査を最低でも月に1回は実行することをお勧めします。[**ツール**] > [**スケジューラ**]で、検査をスケジュールされたタスクとして設定できます。



また、選択したファイルおよびフォルダーをデスクトップまたは[Finder]ウィンドウからドラッグし、System Center Endpoint Protectionのメイン画面、ドックアイコン、メニューバーアイコン(画面上部)、またはアプリケーションアイコン(/Applicationsフォルダー内に置かれています)にドロップすることもできます。

検査の種類

コンピューターの検査には次の2種類があります。[**Smart検査**]では、検査パラメーターを追加で設定することなく、簡単にシステムを検査します。[**カスタム検査**]では、あらかじめ定義した検査プロファイルの選択や、特定の検査の対象の選択を行うことができます。

Smart検査

Smart検査を使用すると、コンピューターの検査をすぐに開始して、ユーザーが操作しなくても、感染しているファイルからウイルスを駆除できます。主な利点は、スキャンを詳細に設定しなくても簡単に操作できることにあります。Smart検査では、全てのフォルダーにある全てのファイルが検査されます。検出された侵入物があれば、自動的に駆除または削除されます。駆除レベルは自動的に既定値に設定されます。駆除の種類の詳細については、「駆除 15」のセクションを参照してください。

カスタム検査

カスタム検査は、検査の対象やスキャン方法などの検査パラメーターを自分で指定したい場合に最適です。カスタム検査を実行する利点は、パラメーターを詳細に設定できることです。さまざまな設定をユーザー定義の検査プロファイルとして保存できます。これは、同じパラメーターで検査を繰り返し実行する場合に便利です。

検査の対象を選択するには、[**コンピューターの検査**] > [**カスタム検査**]を選択し、ツリー構造から特定の**検査の対象**を選択します。検査の対象をさらに細かく指定することもできます。そのためには、対象にするフォルダーまたはファイルのパスを入力します。システムの検査で追加の駆除アクションを実行する必要がない場合は、[**駆除せずに検査する**]オプションを選択します。さらに、[**設定...**]> [**駆除**]をクリックして、3種類の駆除レベルから選択できます。

カスタム検査でコンピューターの検査を実行するのは、ウイルス対策プログラムを以前に使用した経験のある上級ユーザーにお勧めします。

検査の対象

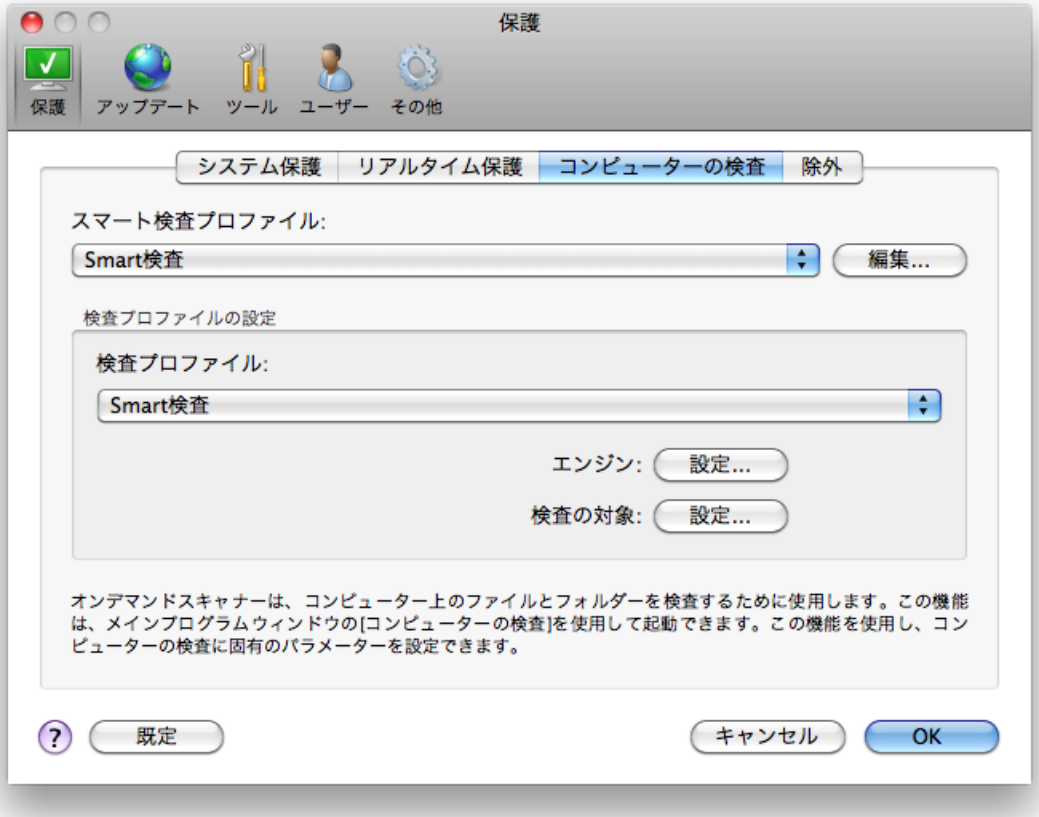
[検査の対象]ツリー構造を使用すると、ウイルスを検査するファイルおよびフォルダーを選択できます。フォルダーはプロファイルの設定に従って選択することもできます。

検査の対象をさらに細かく定義することもできます。そのためには、検査の対象に含めるフォルダーまたはファイルのパスを入力します。コンピューター上で使用できる全てのフォルダーを表示しているツリー構造から対象を選択します。

検査プロファイル

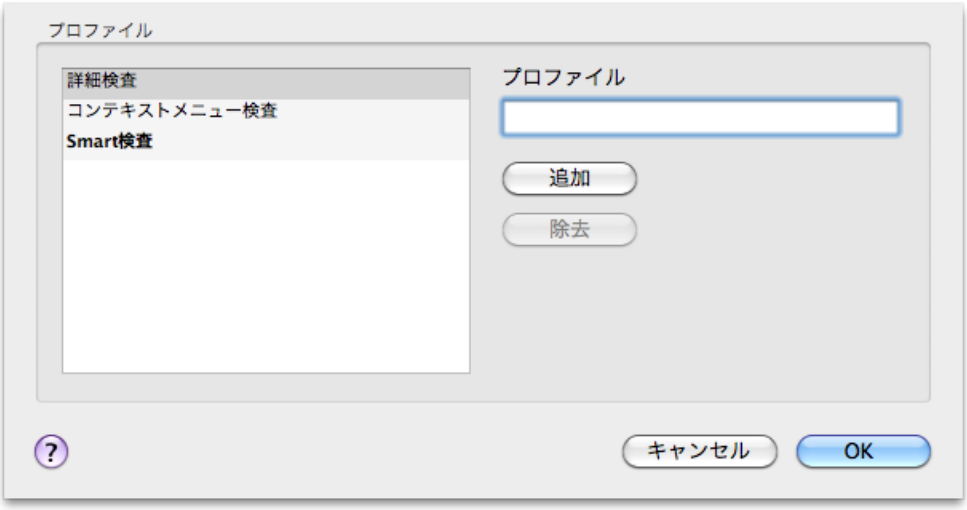
検査について好みの基本設定を保存して、後で検査を行う際に使用できます。さまざまな検査の対象、検査方法、およびその他のパラメーターについて、定期的に行う検査ごとにプロファイルを作成することをお勧めします。

新しいプロファイルを作成するには、[**設定**] > [**アプリケーション設定を入力する...**]> [**保護**] > [**コンピューターの検査**]をクリックし、現在のプロファイルの一覧の横にある[**編集...**]をクリックします。



ニーズに合った検査プロファイルを作成するための参考情報として、「エンジンのパラメーターの設定 14」セクションにある検査設定の各パラメーターの説明を参照してください。

例:既にあるSmart検査の設定は部分的にしか自分のニーズを満たさないので、独自の検査プロファイルを作成する必要があるとします。そこで、圧縮された実行形式と安全でない可能性があるアプリケーションを検査しないよう設定します。また、厳密な駆除を適用することにします。[**オンデマンドスキャナープロファイルリスト**]ウィンドウで、プロファイル名を入力して[**追加**]ボタンをクリックし、[OK]をクリックして確認します。次に、[**エンジン**]および[**検査の対象**]を設定してパラメーターを調整し、自分の要件に合わせます。



エンジンのパラメータ設定

System Center Endpoint Protectionで使用される技術は事前対応型なので、新しい脅威が広がる初期の段階でも保護することができます。この技術では、システムのセキュリティを大幅に強化するために連携して動作するさまざまな方法(コード分析、コードエミュレーション、汎用シグネチャ、ウイルスシグネチャ)の組み合わせが使用されます。スキャンエンジンは、複数のデータストリームを同時に検査して、最大限の効率および検出率を確保することができます。また、この技術によってルートキットを的確に防止することもできます。

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

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

設定ウィンドウにアクセスするには、[**設定**] > [**ウイルス・スパイウェア対策**] > [**ウイルス・スパイウェア対策保護の詳細設定**]をクリックし、次に[**システム保護**]? [**リアルタイム保護**]および[**コンピューターの検査**]の各ワイルドカードの[**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必要になることがあります。これを念頭に、以下の保護モジュールごとにエンジンパラメータを個々に設定できます。

- [**システム保護**] > [自動起動ファイルの検査]
- [**リアルタイム保護**] > [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**] > [コンピューターの検査]

エンジンパラメーターは機能ごとに固有の最適化がされているので、パラメーターを変更すると、システムの動作に大きく影響することがあります。たとえば、常に圧縮された実行形式を検査するように設定を変更したり、リアルタイムファイルシステム保護機能で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。そのため、コンピューターの検査を除く全ての機能について、エンジンの既定のパラメータを変更しないことをお勧めします。

検査対象

[**検査対象**]セクションでは、侵入物を検査するコンピューターのファイルを指定できます。

- **ファイル** - 一般的なファイルの種類(プログラム、画像、音声、動画、データベースファイルなど)を全て検査します。
- **シンボリックリンク** - (オンデマンド検査のみ)オペレーティングシステムによって別のファイルまたはディレクトリへのパスとして解釈され、たどることができるテキスト文字列を含む特殊な種類のファイルを検査します。
- **電子メールファイル** - (リアルタイム保護では使用できません)電子メールメッセージが含まれている特殊なファイルを検査します。
- **メールボックス** - (リアルタイム保護では使用できません)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** - (リアルタイム保護では使用できません)アーカイブ内の圧縮されたファイル(.rar、.zip、.arj、.tarなど)を検査します。
- **自己解凍形式** - (リアルタイム保護では使用できません)自己解凍形式のアーカイブファイルに含まれているファイルを検査します。

- **圧縮された実行形式** – メモリに展開されるランタイム圧縮形式(標準のアーカイブ形式とは異なります)、および標準的な静的圧縮形式(UPX、yoda、ASPack、FGSなど)を検査します。

オプション

[**オプション**]セクションでは、システムの侵入物の検査時に使用される方法を選択できます。使用可能なオプションは、

- **ヒューリスティック** - ヒューリスティックは、悪意のあるプログラムの活動を解析するアルゴリズムを使用します。ヒューリスティック検出法の主な利点は、これまで存在しなかった、またはこれまでのウイルス定義データベースで特定されていなかった、悪意のある新しいソフトウェアを検出できる能力です。
- **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、高級プログラミング言語で作成されたコンピュータワームやトロイの木馬の検出に最適の独自のヒューリスティックアルゴリズムで構成されます。アドバンスドヒューリスティックによって、プログラムの検出能力が大幅に向上します。
- **望ましくない可能性があるアプリケーション** - 望ましくない可能性があるアプリケーションは、必ずしも悪意があるとは限りませんが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があります。通常、このようなアプリケーションをインストールするには同意が必要です。このようなアプリケーションをコンピューターにインストールすると、アプリケーションをインストールする前とは異なる状態でシステムが動作します。最も大きな変化としては、不要なポップアップウィンドウ、隠しプロセスの開始と実行、システムリソースの使用率の増加、検索結果の変更、アプリケーションがリモートサーバと通信することなどがあります。
- **安全ではない可能性があるアプリケーション** - 安全ではない可能性があるアプリケーションとは、そのアプリケーションがインストールされたことをユーザーが知らない場合、アタッカーが悪用する可能性のある、市販の適正なソフトウェアのことを指します。これには、リモートアクセスツールなどのプログラムが含まれます。そのため、既定ではこのオプションは無効に設定されています。

駆除

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

- **駆除なし** - 感染しているファイルが自動的に駆除されることはありません。警告ウィンドウが表示され、アクションを選択することができます。
- **標準的な駆除** - 感染ファイルが自動的に駆除または削除されます。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。あらかじめ指定したアクションを完了できなかった場合にも、その後のアクションの選択が表示されます。
- **厳密な駆除** - 全ての感染ファイルが駆除または削除されます(アーカイブも対象)。ただし、システムファイルは除きます。感染ファイルを駆除できなかった場合は、警告ウィンドウでアクションを選択することができます。

警告: 既定の標準的な駆除モードでは、アーカイブファイル全体が削除されるのは、アーカイブ内の全てのファイルが感染している場合のみです。問題のないファイルが含まれている場合には、アーカイブファイルは削除されません。厳密な駆除モードでは、感染しているアーカイブファイルが検出された場合、感染していないファイルがあっても、アーカイブ全体が削除されます。

拡張子

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

既定では、拡張子に関係なく、全てのファイルが検査されます。検査から除外するファイルの一覧に任意の拡張子を追加できます。[**追加**]および[**削除**]のボタンを使用することで、目的の拡張子のスキャンを有効にしたり禁止したりできます。

特定のファイルタイプを検査するとプログラムが正しく稼動しなくなる場合のように、場合によっては検査からファイルを除外する必要があります。たとえば、.log? .cfg、および.tmp拡張子は除外することをお勧めします。

制限

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

- **最大サイズ**:検査対象のオブジェクトの最大サイズを定義します。これにより、ウイルス対策機能では、指定した値より小さいサイズのオブジェクトのみが検査されます。一般的には既定値を変更する理由はないので、その値を変更しないことをお勧めします。上級ユーザーが大きいオブジェクトを検査から除外する必要がある場合のみ、このオプションを変更してください。
- **最長検査タイム**:オブジェクトの検査に割り当てられた最長時間を定義します。ここでユーザー定義の値が入力されていると、検査が終わっているかどうかにかかわらず、その時間が経過するとウイルス対策機能は検査を停止します。
- **最大のネストレベル**:アーカイブの検査の最大レベルを指定します。一般的な環境では既定値(10)を変更する理由はないので、その値を変更しないことをお勧めします。ネストされたアーカイブ数が原因で検査が途中で終了した場合、アーカイブは未チェックのままになります。
- **最大のファイルサイズ**:このオプションを使用すると、検査対象のアーカイブ(抽出された場合)に含まれるファイルの最大ファイルサイズを指定できます。この制限により検査が途中で終了した場合、アーカイブは未チェックのままになります。

その他

SMART最適化を有効にすると、スキャンの速度を最高に保ちながら最も効率的なスキャンレベルが確保されるように、最適な設定が使用されます。さまざまな保護モジュールで異なるスキャン方法を使用し、それらを特定のファイルタイプに適用して、高度にスキャンを行います。SMART最適化は製品内で厳密に定義されているものではありません。開発チームは新しい変更点を継続的に実装しており、ご使用のSystem Center Endpoint Protectionには、定例のアップデートの際に組み込まれます。SMART最適化を無効にすると、特定のモジュールのエンジンコアのユーザー定義設定のみがスキャンの実行時に適用されます。

[**代替データストリームを検査する**](オンデマンドスキャナーのみ)
ファイルシステムによって使用される代替データストリーム(リソース/データフォーク)は、通常のスキャン技術では検出できないファイルとフォルダの関連付けです。多くのマルウェアが、自らを代替データストリームに見せかけることによって、検出を逃れようとします。

侵入物が検出された

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

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。

1. System Center Endpoint Protectionを開き、[**コンピューターの検査**]をクリックします。
2. [**Smart検査**]をクリックします(詳細については、「Smart検査 12」を参照してください)。
3. 検査終了後、ログで検査済みファイル、感染ファイル、および駆除済みファイルの件数をそれぞれ確認します。

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

System Center Endpoint Protectionでの侵入物の一般的な処理例として、リアルタイムのファイルシステムモニターにより侵入物が検出されたものとして説明します(駆除レベルは既定値)。モニター機能は、ファイルからウイルスを駆除するか、またはファイル自体を削除しようとします。リアルタイム保護モジュールで使用できるあらかじめ指定されたアクションがない場合は、警告ウィンドウが表示され、オプションを選択するよう求められます。選択できるオプションは通常、[**駆除**]? [**削除**]、および[**何もしない**]のいずれかです。[**何もしない**]はお勧めできません。感染しているファイルが、そのままにされるからです。唯一の例外は、そのファイルが「無害なのに誤って感染が検出された」と確信できる場合です。

駆除と削除 - ウイルスが悪意のあるコードをファイルに添付して攻撃している場合に、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、まず感染しているファイルからのウイルスの駆除を試みます。ファイルが悪意のあるコードのみで構成されている場合には、ファイル全体が削除されます。

アーカイブのファイルの削除 - 既定の駆除モードでは、アーカイブファイルに感染ファイルしか含まれていない場合にのみ、アーカイブファイル全体が削除されます。つまり、感染していない無害なファイルも含まれている場合には、アーカイブは削除されません。ただし、**厳密な駆除**スキャンを実行する際には注意が必要です。厳格な駆除では、アーカイブに感染ファイルが1つでも含まれていれば、アーカイブ内の他のファイルの状態に関係なく、アーカイブが削除されます。

プログラムのアップデート

最大レベルのセキュリティを維持するためには、System Center Endpoint Protectionを定期的にアップデートする必要があります。アップデート機能では、最新のウイルス定義データベースのダウンロードにより、プログラムを常に最新の状態に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。アップデートプロセスを手動で開始するには、[**ウイルス定義データベースをアップデートする**]をクリックします。

通常の状況では、更新ファイルが正常にダウンロードされると、[アップデート]ウィンドウに[*アップデートは必要ありません - 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。

[アップデート]ウィンドウには、ウイルス定義データベースのバージョンに関する情報も表示されます。この番号は、個々のアップデートで追加されたすべてのシグネチャの一覧を表示しているWebサイトへのアクティブリンクになっています。

アップデートの設定

テストモードの使用を有効化するには、[**詳細設定オプション**]の横にある[**設定...**]ボタンをクリックし、[**テストモードを有効化する**]チェックボックスをチェックします。アップデートに成功するごとに表示されるシステムトレイの通知を無効化するには、[**成功したアップデートについての通知を表示しない**]チェックボックスをチェックします。

一時的に保存されたアップデートデータを全て削除するには、[**アップデートキャッシュを削除**]の横にある[**削除**]ボタンをクリックします。アップデート中に問題が発生した場合はこのオプションを使用してください。

アップデートタスクの作成方法

アップデートを手動で開始するには、メインメニューの[**アップデート**]をクリックした後に表示されるプライマリウィンドウで、[**ウイルス定義データベースをアップデートする**]をクリックします。

アップデートはスケジュールされたタスクとしても実行できます。スケジュールされたタスクを設定するには、[**ツール**] > [**スケジューラ**]をクリックします。System Center Endpoint Protectionでは、次のタスクが既定で有効になっています。

- **定期的に自動アップデート**
- **ユーザーログオン後に自動アップデート**

アップデートタスクはそれぞれ、ユーザーのニーズに合わせて変更することができます。ユーザーは、既定のアップデートタスクとは別に、ユーザー定義の設定で新しいアップデートタスクを作成することができます。アップデートタスクの作成と設定の詳細については、「スケジューラ 18」セクションを参照してください。

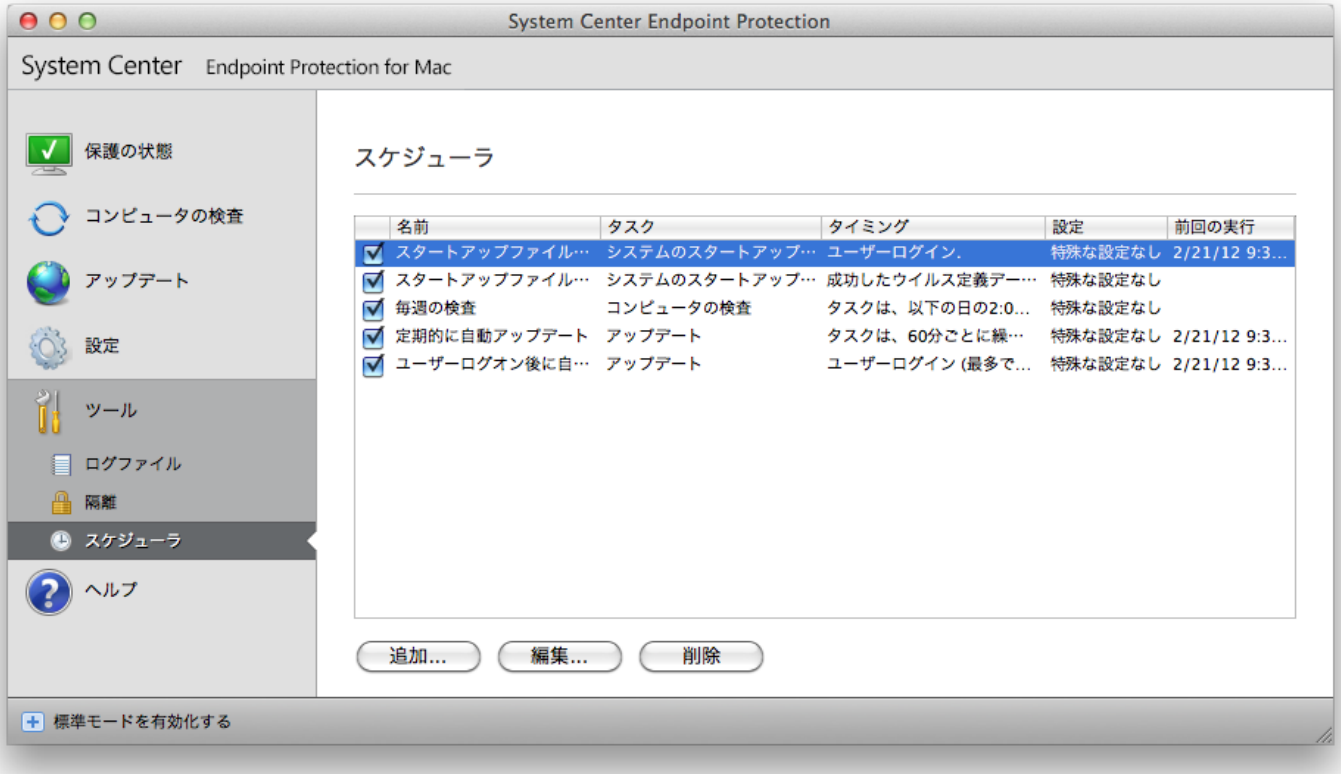
新ビルドへのアップグレード

保護の効果を最大限にするため、System Center Endpoint Protectionの最新ビルドを使用することが重要です。新バージョンの有無を確認するには、左側のメインメニューで[**アップデート**]をクリックします。新しいビルドが提供されている場合、画面の下部に[*利用できる新バージョンの製品があります!*]というメッセージが表示されます。[**詳細を見る...**]をクリックすると、新たなウィンドウに新ビルドのバージョン番号と変更内容が表示されます。

[**ダウンロード**]をクリックすると、最新ビルドをダウンロードできます。後でアップグレードをダウンロードする場合は、[**閉じる**]をクリックしてウィンドウを閉じます。

スケジューラ

System Center Endpoint Protectionの詳細モードが有効になっている場合、**スケジューラ**を使用することができます。スケジューラは、System Center Endpoint Protectionのメインメニューの[**ツール**]にあります。**スケジューラ**には、スケジュール済みの全てのタスクと設定プロパティ(あらかじめ定義した日付、時刻、使用する検査プロファイルなど)の一覧が表示されます。



既定では、次のスケジュールされたタスクがスケジューラに表示されます。

- 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
- 起動ファイルの検査(ユーザーのログオン後)
- 起動ファイルの検査(成功したウイルス定義データベースのアップデート後)
- ログの保守(スケジューラの設定で[**システムタスクを表示する**]オプションを有効にした後)
- 毎週の検査

既存のスケジュールされたタスク(既定のタスクおよびユーザー定義のタスク)の設定を編集するには、Ctrlキーを押して、変更するタスクをクリックし、[**編集...**]を選択するか、あるいはタスクを選択して[**タスクの編集...**]ボタンをクリックします。

タスクをスケジュールする目的

スケジューラでは、スケジュールされたタスクが、あらかじめ定義された設定やプロパティと共に管理され、開始されます。設定およびプロパティには、日時のほか、タスクの実行時に使用される所定のプロファイルなどの情報が含まれます。

新しいタスクの作成

スケジューラで新しいタスクを作成するには、[**タスクの追加...**]ボタンをクリックするか、またはCtrlキーを押してブランクのフィールド内をクリックし、コンテキストメニューから[**追加...**]を選択します。次の5種類のスケジュールされたタスクが使用可能です。

- **アプリケーションの実行**
- **アップデート**
- **ログの保守**
- **コンピューターの検査**
- **システムのスタートアップファイルのチェック**

スケジュールされたタスクの中でアップデートが最もよく使用されるので、新しいアップデートタスクを追加する方法を説明します。

[**スケジュールタスク**]ドロップダウンメニューから[**アップデート**]を選択します。[**タスク名**]フィールドにタスクの名前を

入力します。[**実行タスク**]ドロップダウンメニューからタスクの頻度を選択します。使用可能なオプションは、[**ユーザー定義**]? [**1回**]? [**繰り返し**]? [**毎日**]? [**毎週**]、および[**イベントの発生時**]です。選択された頻度に基づいて、さまざまなアップデートパラメーターが提示されます。

[**ユーザー定義**]を選択すると、cronフォーマットで日付/時刻を指定するためのプロンプトが表示されます（詳細については「ユーザー定義タスクの作成 20」セクションを参照してください）。

次のステップで、スケジュールされた時刻にタスクを実行できない場合や完了できない場合に実行するアクションを定義します。次の3つのオプションが使用可能です。

- **スケジューリングされている次回まで待つ。**
- **可能になり次第タスクを実行する。**
- **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**([**タスクの実行間隔**]オプションで、間隔を定義することができます)。

次のステップでは、現在のスケジュールされたタスクに関する情報の概要のウィンドウが表示されます。[**完了**]ボタンをクリックします。

新しくスケジュールされたタスクが、現在スケジュールされているタスクのリストに追加されます。

システムには、製品を正常に機能させるため、いくつかの重要なタスクがあらかじめスケジュール設定されています。これらのタスクは、不用意に変更されないように既定では非表示にされています。このオプションを変更し、これらのタスクを表示するには、[**設定**] > [**アプリケーション設定を入力する...**]> [**ツール**] > [**スケジューラ**]をクリックし、[**システムタスクを表示する**]オプションを選択します。

ユーザー定義タスクの作成

[**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)で入力する必要があります。
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:
```
30 6 22 3 2012 4
```

cron表現では、以下の特殊文字がサポートされています:
- アスタリスク(*) - 表現はフィールドのすべての値に一致します。例：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(-) - 範囲を指定します。例： `3-9`
- カンマ(,)- リストの項目を区切ります。例： `1,3,7,8`
- スラッシュ(/)- 範囲の増分を定義します。例：`3-28/5` 3つ目のフィールド(月)では、毎月3日および5日ごととなります。

曜日名(Monday-Sunday)と月名(January-December)はサポートされていません。

注意: 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。

隔離

隔離の主な役割は、感染ファイルを安全に保存することです。ファイルを駆除できない場合、ファイルの削除が安全でないまたは推奨されない場合、あるいはSystem Center Endpoint Protectionで誤って検出された場合、ファイルを隔離する必要があります。

任意のファイルを選択して隔離することができます。これは、ファイルの動作が疑わしいにもかかわらず、ウイルス対策スキャナーによって検出されない場合にお勧めします。

隔離フォルダーに保存されているファイルは、隔離の日時、感染ファイルの元の場所のパス、ファイルサイズ(バイト単位)、理由("ユーザーによって追加されました"など)、およびウイルスの数(複数の侵入物を含むアーカイブかどうかなど)を表示するテーブルで見ることができます。隔離ファイルを収容した隔離フォルダー(/Library/Application Support/Microsoft/scep/cache/quarantine)は、System Center Endpoint Protectionをアンインストールした後もシステムに残ります。隔離されたファイルは暗号化された安全な形式で格納されており、System Center Endpoint Protectionのインストール後に再度復元できます。

ファイルの隔離

削除されたファイルは、System Center Endpoint Protectionにより自動的に隔離されます(警告ウィンドウでユーザーがこのオプションをキャンセルしなかった場合)。必要に応じて、[**隔離...**]ボタンをクリックして不審なファイルを手動で隔離することができます。この操作にはコンテキストメニューも使用することができます。Ctrlキーを押し、ブランクのフィールド内をクリックし、[**隔離...**]を選択してから、隔離するファイルを選択し、[**開く**]ボタンをクリックします。

隔離フォルダーからの復元

隔離されているファイルを、元の場所に復元することもできます。この操作には、[**復元**]ボタンを使用します。復元はコンテキストメニューから選択することもできます。それには、[**隔離**]ウィンドウで特定のファイルを右クリックし[**復元**]をクリックします。コンテキストメニューには、[**復元先を指定...**]オプションもあります。このオプションを使用すると、隔離される前の場所とは異なる場所にファイルを復元することができます。

ログファイル

ログファイルには、発生した全ての重要なプログラムイベントに関する情報が格納され、検出された脅威の概要が表示されます。ログは、システムの分析、脅威の検出、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。System Center Endpoint Protection環境から直接、ログをアーカイブするだけでなく、テキストメッセージとログを表示することができます。

ログファイルにアクセスするには、System Center Endpoint Protectionのメインメニューで[**ツール**]? [**ログファイル**]の順にクリックします。ウィンドウの最上部にある[**ログ**]ドロップダウンメニューを使用して、目的のログの種類を選択します。使用可能なログは次のとおりです。

1. **検出された脅威** - このオプションを選択すると、侵入物の検出に関連するイベントに関する全ての情報が表示されます。
2. **イベント** - このオプションは、システム管理者およびユーザーが問題を解決するために使用します。イベントログには、System Center Endpoint Protectionによって実行された全ての重要なアクションが記録されます。
3. **コンピューターの検査** - このウィンドウには、完了した全ての検査結果が表示されます。エントリーをダブルクリックすると、コンピューターの検査結果の詳細がそれぞれ表示されます。

各セクションで、エントリーを選択し、[**コピー**]ボタンをクリックすると、表示されている情報をクリップボードに直接コピーすることができます。

ログの保守

System Center Endpoint Protectionのログの設定には、プログラムのメインウィンドウからアクセスすることができます。[**設定**] > [**アプリケーション設定を入力する...**]> [**ツール**] > [**ログファイル**]の順にクリックします。ログファイルの次のオプションを指定することができます。

- **古いログレコードを自動的に削除する** - 指定した日数より古いログエントリが自動的に削除されます。
- **ログファイルを自動的に最適化する** - 未使用のレコードが指定した割合を超えると、ログファイルが自動的に最適化されます。

グラフィカルユーザーインターフェイスに表示されるすべての関連情報、脅威、およびイベントメッセージは、プレーンテキストやCSV(カンマ区切り値ファイル)などの人間が読み取れるテキスト形式で保存できます。これらのファイルをサードパーティ製のツールを使用して処理できるようにするには、**[テキストファイルへのログ記録を有効化する]**の横のチェックボックスをオンにします。

ログファイルの保存先フォルダを定義するには、**[詳細設定]**の横の**[設定...]**をクリックします。

[テキストログファイル:] [編集]の下で選択したオプションに基づいて、次の書き込まれた情報とともにログを保存できます。

- 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。
- *無効なユーザー名とパスワード*? *ウイルス署名データベースを更新できません*などのイベントは、eventslog.txtファイルに書き込まれます。
- 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。

[**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**]のフィルターを設定するには、このオプションの横の[**編集...**]ボタンをクリックし、必要に応じてログの種類を選択または選択解除します。これらのログタイプの詳細については、この章[22]を参照してください。

ログのフィルタリング

ログには、重要なシステムイベントに関する情報が格納されています。ログフィルタリング機能では、特定の種類のイベントに関するレコードを表示することができます。

最も頻繁に使用されるログの種類は以下のとおりです。

- **重大な警告** - 重大ななシステムエラー(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通知情報。
- **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。

ユーザーインターフェイス

System Center Endpoint Protectionのユーザーインターフェイスの設定オプションを使用すると、各自のニーズに合わせて作業環境を調整することができます。これらの設定オプションには、[**設定**] > [**アプリケーション設定を入力する...**]> [**ユーザー**] > [**インタフェース**]からアクセスします。

このセクションの詳細モードオプションを使用して、詳細モードに切り替えることができます。詳細モードでは、System Center Endpoint Protectionのより詳細な設定と追加コントロールが表示されます。

起動スプラッシュウィンドウ機能を有効化するには、[**起動時にスプラッシュウィンドウを表示する**]オプションを選択します。

[**標準メニューを使用する**]セクションで、[**標準モードで**]または[**詳細モードで**]オプションを選択すると、それぞれの表示モードでプログラムのメインウィンドウの標準メニューを使用できます。

ツールヒントを有効化するには、[**ツールヒントを表示**]オプションを選択します。[**隠しファイルを表示する**]オプションを選択すると、[**コンピューターの検査**]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。

警告と通知

[**警告と通知**]セクションでは、脅威の警告やシステム通知をSystem Center Endpoint Protectionでどのように処理するかを設定することができます。

[**警告ウィンドウを表示**]オプションを無効にすると、全ての警告ウィンドウが表示されなくなります。この設定が適しているのは、特定の限られた状況のみです。ほとんどのユーザーには、既定の設定のままにすることをお勧めします(チェックボックスをオンにします)。

[**デスクトップに通知を表示する**]オプションを選択すると、ユーザーの操作が不要な警告ウィンドウをデスクトップに表示できます(既定では画面の右上角)。通知の表示時間を定義するには、[**次の後に通知を自動的に閉じる**]のX[**秒**]の値を調整します。

警告と通知の詳細設定

ユーザー操作が必要な通知だけ表示する
このオプションを使用すると、ユーザーに操作を要求するメッセージの表示をオンまたはオフにすることができます。

全画面モードでアプリケーションを実行中にユーザーの操作が必要な通知のみ表示する
プレゼンテーションやその他のアクティビティなど、画面全体が必要な操作を行う場合、このオプションを選択すると便利です。

権限

System Center Endpoint Protection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、プログラム設定を編集する権限を持つユーザーを選択できます。

権限ユーザーを指定するには、[**設定**] > [**アプリケーション設定を入力する...**]> [**ユーザー**] > [**権限**]に入力します。

システムのセキュリティを最大限に確保するには、プログラムを正しく設定することが重要です。許可なく変更が行われた場合、重要なデータが失われることがあります。権限ユーザーの一覧を設定するには、左側の[**ユーザー**]一覧からユーザーを選択し、[**追加**]ボタンをクリックします。ユーザーを削除するには、右側の[**権限ユーザー**]一覧でユーザー名を選択し、[**削除**]をクリックします。

注意: 権限ユーザーの一覧が空の場合、システムの全てのユーザーにプログラムの編集権限があります。

コンテキストメニュー

コンテキストメニューの統合を有効にするには、[**設定**] > [**アプリケーション設定を入力する...**]> [**ユーザー**] > [**コンテキストメニュー**]セクションで[**コンテキストメニューに統合する**]チェックボックスをオンにします。

上級ユーザー

設定をインポートおよびエクスポートする

System Center Endpoint Protectionの設定のインポートとエクスポートは、詳細モード時に[**設定**]から行うことができます。

インポートとエクスポートのいずれの場合もアーカイブファイルを使用して設定を保存します。インポートとエクスポートは、後で使用するためにSystem Center Endpoint Protectionの現在の設定をバックアップする必要がある場合に便利です。エクスポート設定オプションは、System Center Endpoint Protectionの好みの基本設定を複数のシステムに対して使用する場合にも便利です。設定ファイルを簡単にインポートして、目的の設定を転送できます。

設定のインポート

設定のインポートは、非常に簡単です。メインメニューで[**設定**] > [**設定をインポートおよびエクスポートする...**]をクリックし、[**設定のインポート**]オプションを選択します。設定ファイルの名前を入力するか、または[**参照...**]ボタンをクリックして、インポートする設定ファイルを参照します。

設定のエクスポート

設定をエクスポートする手順は、ほとんど同じです。メインメニューで[**設定**] > [**設定をインポートおよびエクスポートする...**]をクリックします。[**設定のエクスポート**]オプションを選択し、設定ファイルの名前を入力します。ブラウザを使用して、設定ファイルの保存先を選択します。

プロキシサーバーの設定

プロキシサーバーの設定は、[**その他**] > [**プロキシサーバー**]で行うことができます。プロキシサーバをこのレベルで指定すると、System Center Endpoint Protectionのすべての機能に対するプロキシサーバーのグローバル設定が指定されることになります。ここで設定するパラメーターは、インターネットへの接続を必要とするすべてのモジュールで使用されます。

プロキシサーバー設定をこのレベルで指定するには、[**プロキシサーバーを使用する**]チェックボックスをオンにし、プロキシサーバーのIPアドレスまたはURLを[**プロキシサーバー**]フィールドに入力します。[ポート]フィールドには、プロキシサーバーが接続を受け付けるポートを指定します(既定では3128です)。プロキシサーバーとの通信に認証が必要な場合、[**プロキシサーバーは認証が必要**]チェックボックスをオンにし、有効な**ユーザー名**と**パスワード**をそれぞれのフィールドに入力します。

リムーバブルメディアのブロック

リムーバブルメディア(CD、USBキーなど)に悪意のあるコードが入っていると、コンピューターを危険にさらす可能性があります。リムーバブルメディアをブロックするには、[**リムーバブルメディアの遮断を有効化する**]の横のチェックボックスをオンにします。特定のタイプのメディアへのアクセスを許可するには、許可するメディアタイプの横のチェックボックスをオフにします。

これらの設定をCD、DVD、FireWire、USB以外のメディアタイプに適用する場合は、**[その他]**の横のチェックボックスをオンにします。この設定は、特に、Thunderboltインターフェイス経由でコンピュータに接続するすべての周辺機器に適用されます。

用語集

侵入物の種類

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

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を破損させる侵入物の一種です。ウイルスは生物学上のウイルスにちなんで名付けられました。同じような手法でコンピューター間に蔓延していくからです。

コンピューターーウイルスは、主に実行可能ファイル、スクリプト、およびドキュメントを攻撃します。自己を複製するため、ウイルスは"本体"を標的ファイルの末尾に付着させます。コンピューターウイルスの動作を簡単に説明します。感染したファイルの実行後、ウイルスは(元のアプリケーションよりも前に)自身をアクティブにし、事前定義タスクを実行します。元のアプリケーションが実行できるようになるのは、その後です。ウイルスは、悪意のあるプログラムをユーザーが(偶然または故意に)実行したり開いたりしない限り、コンピューターーに感染することはできません。

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

ウイルスは少なくなっています(トロイの木馬やスパイウェアと比較して)。悪意のあるソフトウェア開発者にとって金銭的に魅力的ではないためです。また、"ウイルス"という用語は、あらゆる種類の侵入物を意味する用語として誤用されることがよくあります。この用法は、新しくより正確な用語"マルウェア" (悪意のあるソフトウェア)へと次第に言い換えられています。

お使いのコンピューターがウイルスに感染した場合は、感染したファイルを元の状態に復元する、つまりウイルス対策プログラムでファイルからウイルスを駆除する必要があります。

ウイルスの例:OneHalf? Tenga、およびYankee Doodle。

ワーム

コンピューターワームとは、感染先のコンピューターを攻撃しネットワークを介して蔓延する、悪意のあるコードを含む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、ワームは自己を複製し、自ら移動できることです。ワームは宿主ファイル(またはブートセクター)に依存しません。ワームはアドレス帳の電子メールアドレスを介して広がるか、またはネットワークアプリケーションのセキュリティ上の脆弱性を悪用します。

したがって、ワームはコンピューターウイルスよりはるかに生存能力が高いプログラムです。インターネットは至る所から利用できるので、リリースしてから数時間以内に世界中に蔓延できます。場合によっては、数分で広まります。自己を単独で急速に複製できる能力があるので、他の種類のマルウェアより危険です。

システム内でワームが活性化されると、迷惑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、他の種類の侵入物の"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、感染ファイルを削除することをお勧めします。悪意のあるコードが含まれている可能性が高いからです。

よく知られているワームの例:Lovsan/Blaster? Stration/Warezov? Bagle、およびNetsky。

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、こうしてユーザーを騙して実行させようとする侵入物の1つのクラスとして定義されてきました。今やトロイの木馬は偽装する必要がなくなりました。トロイの木馬の唯一の目的は、できるだけ簡単に侵入し、悪意のある目標を達成することです。"トロイの木馬"は、極めて一般的な用語になりました。今日では侵入物のどの特定のクラスにも分類されない侵入物なら、すべて該当します。

このカテゴリの範囲は非常に広いので、多くのサブカテゴリに分類されることもよくあります。

- ダウンローダ - インターネットから他の侵入物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 - 弱体化されたコンピューターに他の種類のマルウェアを落とす(ドロップする)トロイの木馬の一種。
- バックドア - リモートの攻撃者と通信して、システムにアクセスし制御できるようにするアプリケーション。
- キーロガー - (キーストロークロガー) - ユーザーが入力した各キーストロークを記録し、リモートの攻撃者にその情報を送信するプログラム。
- ダイアラ - 情報料代理徴収番号に接続するよう設計されたプログラム。新しい接続が作成されたことにユーザーが気づくのは、ほとんど不可能です。ダイアラで被害を被るのは、ダイヤルアップモデムを使用するユーザーのみです。このモデムは今日ではあまり使用されていません。
- 通常、トロイの木馬は実行可能ファイルの形式です。トロイの木馬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、削除することをお勧めします。悪意のあるコードが含まれている可能性が高いからです。

よく知られているトロイの木馬の例:NetBus? Trojandownloader.Small.ZL? Slapper。

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」を省略した用語です。広告を表示するプログラムが、このカテゴリに分類されます。アドウェアアプリケーションは、広告が表示される新しいポップアップウィンドウをインターネットブラウザ内に自動的に開いたり、ブラウザのホームページを変更したりすることがよくあります。アドウェアは、フリーウェアプログラムに同梱されていることが多く、フリーウェアプログラム(通常は便利なアプリケーション)の開発者が、その開発費を賄うことができます。

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

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

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

スパイウェア

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

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

スパイウェアが同梱されている、よく知られているフリーウェア製品の例としては、P2P(ピアツーピア)ネットワークのクライアントアプリケーションがあります。SpyfalconやSpy Sheriffを始めとする多数のプログラムは、スパイウェアの特定のサブカテゴリに属します。これらは一見、スパイウェア対策プログラムに見えますが、実はそれ自体がスパイウェアプログラムなのです。

コンピューター上のファイルがスパイウェアとして検出された場合は、削除することをお勧めします。悪意のあるコードが含まれている可能性が高いからです。

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、少なくありません。ただし、悪意のあるユーザーの手に渡ると、不正な目的で誤用される可能性があります。System Center Endpoint Protectionにはこのような脅威を検出するオプションがあります。

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

コンピューターに、安全ではない可能性があるアプリケーションが存在し、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。

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、必ずしも悪意があるとは限りませんが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があります。通常、このようなアプリケーションをインストールするには同意が必要です。このようなアプリケーションをコンピューターにインストールすると、インストール前とは異なる方法でシステムが動作します。最も大きな違いは次のとおりです。

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