F-Secure Anti-Virus 2013

目次

第 1 章：インストール.....5

インストールする前に.....6
製品をインストールする.....6
アプリケーションのインストールとアップグレード.....6
ヘルプ/サポート.....7

第 2 章：製品を使用するには.....9

自動更新について.....10
更新ステータスを確認する.....10
インターネットの接続設定を変更する.....10
ディープガード ネットワークのステータスを確認する.....11
統計情報を確認する.....11
通知履歴を表示する.....11
通知の設定を変更する.....12
ディープガード ネットワーク.....12
ディープガード ネットワークについて.....12
ディープガード ネットワークのメリット.....13
提供するデータ.....13
個人情報の保護.....14
ディープガード ネットワークにデータ提供する.....14
ディープガード ネットワークに関するお問い合わせ.....15
ライセンスを確認する.....15
アクション センター.....16
ライセンスを認証する.....16

第 3 章：はじめに.....17

全体の保護ステータスを表示する.....18
製品の統計情報を表示する.....18
製品のアップデート.....19
パターン ファイルのバージョンを表示する.....19
モバイル プロバイダの設定を変更する.....19
ウイルスとマルウェアについて.....20
ウイルス.....20
スパイウェア.....21
ルートキット.....21

リスクウェア.....21

第 4 章 : コンピュータをマルウェアから保護する.....23

コンピュータをスキャンする.....24

ファイルを自動的にスキャンする.....24

ファイルを手動でスキャンする.....26

メールをスキャンする.....29

スキャンの結果を表示する.....30

スキャンからファイルを除外する.....30

特定のファイルを除外する.....31

特定の場所にあるファイルを除外する.....31

除外したアプリケーションを表示する.....32

隔離保存フォルダを使用する.....33

隔離保存したアイテムを表示する.....33

隔離保存したアイテムを復元する.....33

ディープガードについて.....34

ディープガードを有効/無効にする.....34

ディープガードがブロックしたアプリケーションを許可する.....35

ディープガードを互換性モードで使用する.....35

不審な動作に関する警告.....35

第

1

章

インストール

トピック：

- *インストールする前に*
- *製品をインストールする*
- *アプリケーションのインストールとアップグレード*
- *ヘルプ/サポート*

インストールする前に

エフセキュアをお選びいただき誠にありがとうございます。

本製品をインストールするには次が必要となります。

- インストール CD またはインストール パッケージ。コンピュータに CD ドライブがない場合、*www.f-secure.com/netbook* からインストール パッケージをダウンロードできます。
- ライセンス キーコード
- インターネットの接続

他社のセキュリティ製品をコンピュータにインストールしている場合、製品が自動的に削除されます。削除されない場合、手動でアンインストールしてください。

注: コンピュータで複数のアカウントを使用している場合、管理者権限のあるアカウントでインストールを実行してください。

製品をインストールする

ここでは、本製品をインストールする方法について説明します。

次の方法で、本製品をインストールをできます。

1. CD をドライブに挿入します。またはダウンロードしたインストーラを実行します。
   インストール ウィザードが自動的に立ち上がります。立ち上がらない場合、Windows エクスプローラから CD-ROM アイコンをダブルクリックし、インストール ファイルを実行します。
2. 画面の指示に従って本製品をインストールします。
   - 本製品のパッケージ版を購入した場合、ライセンス キー コードはクイック インストール ガイドの表紙に表記されています。
   - 本製品をエフセキュアのオンライン ショップから購入した場合、ライセンス キーコードは発注書の確認メールに表記されています。

   ライセンスの認証と更新ファイルのダウンロードを行う前にコンピュータを再起動する必要があるかもしれません。CD からインストールを行なっている場合、ドライブから CD を取り外してください。

アプリケーションのインストールとアップグレード

ここでは、ライセンスを認証する方法について説明します。

次の方法で、ライセンスの認証またはランチャーから新しいアプリケーションをインストールできます。

注: ランチャーは Windows のシステム トレイにあります。

1. ランチャーの一番右にあるアイコンを右クリックします。
   ポップアップ メニューが表示されます。
2. [ライセンス] を選択します。

3. 「マイ ライセンス」から「ライセンス ステータス」ページを開いて、[ライセンスを認証] をクリックします。
   「ライセンスを認証」ウィンドウが開きます。
4. アプリケーションのライセンス キーコードを入力し、[**OK**] をクリックします。
5. ライセンスの認証が完了したら、[閉じる] をクリックします。
6. 「マイ ライセンス」から「インストール ステータス」ページを開きます。インストール ウィザードが立ち上がらない場合、次の手順を実行します。
   a) [インストール] をクリックします。
      インストール ウィンドウが開きます。
   b) [次へ] をクリックします。
      アプリケーションがダウンロードされ、インストールが開始します。
   c) インストールが完了したら、[閉じる] をクリックします。

ライセンスが認証されます。

ヘルプ/サポート

本製品のオンライン ヘルプを表示するには、ヘルプ アイコンまたはユーザ インターフェースで F1 を押してください。

ライセンスを登録したら、無料のアップデートやサポートなどの追加サービスを受けられます。以下の Web ページにアクセスして、ライセンスを登録できます。*www.f-secure.com/register*

第
2
章

製品を使用するには

トピック：

- *自動更新について*
- *統計情報を確認する*
- *ディープガード ネットワーク*
- *ライセンスを確認する*

本製品をすぐに使い始めるための情報。

ここでは、ランチャーを通じて本製品の共通設定とライセンスの管理を行う方法について説明します。

ランチャーの共通設定は、ランチャーにインストールされている各プログラムの設定に適用されます。この機能を利用することで、プログラムの設定を個別に変更する必要はなく、設定を一括で変更できます。

ランチャーの共通設定

- ダウンロード - ダウンロードした更新/アップデートを表示します。新しい更新があるか手動で確認することもできます。
- 接続設定 - コンピュータがインターネットに接続する方法を変更できます。
- 通知 - 発生した通知を確認できます。また、通知の設定を変更することもできます。
- プライバシーの設定 - ディープガード ネットワークに接続できるか指定できます。

ランチャーから各プログラムのライセンスを管理することができます。

自動更新について

自動更新はコンピュータの保護を更新します。

本製品は、コンピュータがインターネットに接続している際に最新の更新をダウンロードします。回線が遅いネットワークでも、インターネット回線の帯域を圧迫することなく最新の更新を受信することが可能です。

更新ステータスを確認する

更新を最後に受信した日付と時間を確認できます。

自動更新が有効の場合、本製品はコンピュータがインターネットに接続しているときに最新の更新をダウンロードします。

最新の更新を受信しているかどうか確認するには

1. ランチャーの一番右にあるアイコンを右クリックします。
   ポップアップ メニューが表示されます。
2. [共通設定を開く] を選択します。
3. 自動更新 > ダウンロード の順にクリックします。
4. [今すぐ更新] をクリックします。
   本製品がインターネットに接続して、最新の更新をチェックします。セキュリティが最新ではない場合、最新の更新がダウンロードされます。

   注: ダイヤルアップまたは ISDN でインターネットに接続する場合、更新を確認するにはインターネットに接続している必要があります。

インターネットの接続設定を変更する

サーバがインターネットに接続する方法を設定することができます。通常、デフォルトの設定を変更する必要はありません。

インターネットの接続設定を変更するには

1. ランチャーの一番右にあるアイコンを右クリックします。
   ポップアップ メニューが表示されます。
2. [共通設定を開く] を選択します。
3. 自動更新 > 接続仕様 の順にクリックします。
4. インターネット接続からインターネットに接続する方法を選択します。
   - インターネットに常時接続している場合、[常に接続済みと想定] を選択します。

     注: コンピュータがインターネットに常時接続されていない環境で、必要時にダイヤルアップ接続をするように設定されている場合、[常に接続済みと想定] を選択することで複数のダイアルアップが開始される可能性があります。

   - ネットワークに接続されている場合にのみ更新を確認する場合、[接続を検出] を選択します。
   - ネットワーク トラフィックが検出された場合にのみ更新を確認する場合、[トラフィックを検出] を選択します。

ヒント: [接続を検出] を選択しネットワークに接続されていない状態でも接続していると判断されてしまう場合、[トラフィックを検出] を代わりに選択します。

5. **HTTP** プロキシで、コンピュータがプロキシ サーバを使用してインターネットに接続するか選択します。
   - コンピュータがインターネットに直接接続している場合、[**HTTP** プロキシを使用しない] を選択します。
   - **HTTP** プロキシを手動で設定するには、[*HTTP プロキシを手動で設定する*] 選択します。
   - ブラウザの **HTTP** プロキシを使用する を選択したら、Web ブラウザの *HTTP* プロキシ設定が適用されます。

ディープガード ネットワークのステータスを確認する

本製品の機能の多くは、ディープガード ネットワークの設定によって動作が異なります。

ネットワークに問題がある場合やファイアウォールがディープガード ネットワークをブロックしている場合、ステータスは「切断中」になります。ディープガード ネットワークへのアクセスを必要とする機能がインストールされていない場合、ステータスは「未使用」になります。

ステータスを確認するには

1. ランチャーの一番右にあるアイコンを右クリックします。
   ポップアップ メニューが表示されます。
2. [共通設定を開く] を選択します。
3. 自動更新 > 接続仕様 の順にクリックします。

「ディープガード ネットワーク」で、ディープガード ネットワークのステータスを確認できます。

統計情報を確認する

「通知」画面では、本製品が行った処理を確認することができます。

特定な動作/処理が行われたときに (ウイルスがブロックされるときなど) 本製品は通知を表示します。新しいサービスが利用できるときなど、プロバイダに送られる通知もあります。

通知履歴を表示する

本製品が表示した通知をすべて確認することができます。

通知履歴を表示するには

1. ランチャーの一番右にあるアイコンを右クリックします。
   ポップアップ メニューが表示されます。
2. [共通設定を開く] を選択します。
3. その他 > 通知 の順にクリックします。
4. [通知履歴] をクリックします。
   通知履歴の一覧が表示されます。

通知の設定を変更する

本製品が表示する通知の設定を変更できます。

通知の設定を変更するには

1. ランチャーの一番右にあるアイコンを右クリックします。
   ポップアップ メニューが表示されます。
2. [共通設定を開く] を選択します。
3. その他 > 通知 の順にクリックします。
4. [プログラムからのメッセージを表示する] をクリックすると、プログラムからのメッセージを有効/無効にします。

   設定を有効にすると、インストールされているプログラムからの通知が表示されるようになります。
5. [広告メッセージを表示する] をクリックすると、広告メッセージを有効/無効にします。
6. [**OK**] をクリックします。

ディープガード ネットワーク

ここでは、F-Secure の安全なアプリケーションと Web サイトを識別し、マルウェアや Web サイトの脆弱性をブロックする「ディープガード ネットワーク」について説明します。

ディープガード ネットワークについて

F-Secure の「ディープガード ネットワーク」は、最新のインターネット脅威に対して高速なセキュリティ対策を提供します。

ディープガード ネットワークにデータを提供すると、最新の脅威に対する保護が強化されます。ディープガードネットワークは、未知、悪質、かつ不審なアプリケーションに関するデータを収集します。このデータは、F-Secure が分析できるように匿名な状態で F-Secure へ提供されます。分析した情報をもとに最新の脅威とマルウェアに対するセキュリティが改善されるようになります。

ディープガード ネットワークの仕組み

ディープガード ネットワークに参加すると、不明なアプリケーションや Web サイト、マルウェア、Web サイトの脆弱性などに関する情報をディープガード ネットワークに提供できます。ディープガード ネットワークは、Web の行動 (アクセスしたサイトなど) を記録しません。また、すでに分析された Web サイトでは情報を収集しません。コンピュータでインストールされている安全なアプリケーションに関する情報も収集しません。

ディープガード ネットワークにデータを提供しない場合、ディープガード ネットワークはインストールされているアプリケーションや Web サイトに関する情報を収集しません。ただし、アプリケーション、Web サイト、メッセージ、および他のオブジェクトに対する評価を調べるために F-Secure のサーバにアクセスする必要があります。該当するオブジェクトは F-Secure に送信されず、チェックサムを使用した上で暗号化されます。ユーザ別にデータは記録されず、問題のあるファイル/Web サイトに対するデータが計上される仕組みです。

ディープガード ネットワークは本製品の保護を提供する上で不可欠な機能を提供するため、ディープガード ネットワークに関連するネットワーク トラフィックを完全に停止することはできません。

ディープガード ネットワークのメリット

ディープガード ネットワークを利用すると、最新の脅威に対してより速くかつ精度の高い保護を受けられます。また、悪質ではない不審なアプリケーションの検出による警告も発生しません。

ディープガード ネットワークにデータを提供することで未知のマルウェアの検出や誤検出の修正が可能になります。

ディープガード ネットワークに情報を提供しているユーザはデータの共有によりディープガード ネットワークを相互的に向上します。ディープガード ネットワークがデバイス上で不審なアプリケーションを検出すると、他のデバイスでそのアプリケーションがすでに検出されている場合に分析情報がすぐに参照できるようになります。また、デバイスにインストールされているセキュリティ製品はディープガード ネットワークがすでに分析し安全とみなしたアプリケーションをスキャンする必要がないため、ディープガード ネットワークはデバイスのパフォーマンスも向上します。悪質な Web サイトやジャンク メールなどの情報もディープガード ネットワークで共有されるため、ディープガード ネットワークは Web サイトの脆弱性やスパム対策も提供します。

ディープガード ネットワークは、データを提供するユーザが多いほど効率性が上がります。

提供するデータ

デバイスに保存されているアプリケーションとアクセスした Web サイトに関する情報がディープガード ネットワークに提供されます。この情報をもとに、ディープガード ネットワークは最新のマルウェアおよび不審な Web サイトに対するセキュリティを提供できるようになります。

ファイル評価の分析

ディープガード ネットワークは評価されていない不明なアプリケーション、および不審なファイルあるいはマルウェアに関する情報を収集します。

ディープガード ネットワークはデバイス上の安全および不審なアプリケーションに関する匿名データを収集します。収集されるファイルのデータは、実行可能ファイル (.cpl、.exe、.dll、.ocx、.sys、.scr、.drv 形式の Windows 上のポータブル実行可能ファイルなど) に限られます。

収集される情報

- アプリケーションのファイル パス
- ファイルのサイズと作成日/変更日
- ファイルの属性と権利
- ファイルの署名情報
- ファイルのバージョンと作成した会社名
- ファイルのソースまたは ダウンロード URL
- エフセキュア ディープガードとアンチウイルスがスキャンしたファイルの分析結果
- その他の関連情報

ディープガード ネットワークは感染した情報を除いて、個人情報を収集しません。マルウェアを検出した場合、感染の名前とファイルの駆除ステータスが収集されます。

ディープガードを使用して、不審なアプリケーションを F-Secure へ分析用に提供することができます。サンプルとして提供できるファイルはポータブル実行可能ファイルに限ります。ディープガード ネットワークは個人情報を収集しません。また、分析用にアップロードされることは一切ありません。

ファイルを分析用に提供する

ディープガードネットワークを使用すると、不審なアプリケーションを分析用に提供することができます。

不審なアプリケーションはメッセージが表示されたときにのみ手動で提供できます。提供できるファイルは実行可能ファイルに限ります。ディープガード ネットワークは個人情報を収集しません。

Web サイトの評価を分析する

ディープガード ネットワークは、Web の行動 (アクセスしたサイトなど) を記録しません。また、すでに分析された Web サイトでは情報を収集しません。ユーザがアクセスする Web サイトが安全であることを確認します。ディープガード ネットワークは「不審」または「危険」と評価された Web サイトをユーザに通知します。

アクセスする Web サイトが悪質/不審コンテンツまたは脆弱性を含めている場合、ディープガード ネットワークはするために Web ページのコンテンツを分析するためにサイトの全体 URL を収集します。

評価されていないページにアクセスすると、ディープガード ネットワークはドメインとサブドメインの名前を収集します。場合により、サイトの分析と評価を行うためにアクセスしたページのパスも収集されます。個人情報と関連付けできる URL のパラメータはすべて削除されます。

注: ディープガード ネットワークはプライベート ネットワークにある Web ページを評価または分析しません。そのことにより、プライベート IP ネットワーク アドレス (イントラネットなど) の情報は収集されません。

システム情報の分析

ディープガード ネットワークはオペレーティング システムの名前とバージョン、インターネットの接続環境、およびディープガード ネットワークの使用に関する統計 (Web サイトの評価サービスを利用した回数や結果の表示にかかった平均時間など) を収集し、サービスの監視と改善を行います。

個人情報の保護

ディープガード ネットワークに関するデータは保護された状態で転送され、データに含まれる個人情報は自動的に取り除かれます。

F-Secure にデータが送信される前に、ディープガード ネットワークはユーザを特定できるようなデータを削除し、残りのデータを不正なアクセスから保護するために暗号化します。収集されるデータは個別に処理されず、他のディープガード ネットワークのユーザから提供されたデータと一緒に処理されます。また、データはすべて統計的および匿名で分析されるため、データを特定のユーザに関連付けることはできません。

F-Secure に提供されるデータには個人を特定できるようなデータは含まれません。ディープガード ネットワークは、プライベート IP アドレスやメールアドレス、ユーザ名、パスワードなどの個人情報を収集しません。万が一個人を特定できるようなデータを削除できなかった場合、F-Secure はそのデータを個人を特定するために利用することはありません。

提供されたデータは転送時、保存時、および処理時に徹底的に保護されます。データは、F-Secure のデータ センターまたは関連会社にあるセキュア サーバで保管され、F-Secure により管理されます。

F-Secure は、収集されたデータを関連会社、ベンダー、再販業者、パートナーと共有することがありますが、データは常に匿名の状態で共有されます。

ディープガード ネットワークにデータ提供する

悪質なプログラムと Web サイトに関する情報をディープガード ネットワークに提供することでディープガード ネットワークの精度を改善することができます。

インストール中にディープガード ネットワークに情報を提供するか選択できます。デフォルトでは、情報の提供は有効です。この設定は後から変更することができます。

ディープガード ネットワークの設定を変更するには

1. ランチャーの一番右にあるアイコンを右クリックします。
   ポップアップ メニューが表示されます。
2. [共通設定を開く] を選択します。
3. その他 > 個人情報保護 の順にクリックします。
4. 該当するチェックボックスをクリックしてディープガード ネットワークの情報提供を有効にします。

ディープガード ネットワークに関するお問い合わせ

ディープガード ネットワークに関するお問い合わせ。

ディープガード ネットワークについてご質問などありしたら、次の連絡先までお問い合わせください。

F-Secure Corporation

Tammasaarenkatu 7

PL 24

00181 Helsinki

Finland

http://www.f-secure.com/en/web/home_global/support/contact

ディープガード ネットワークに関する最新情報は、F-Secure の Web サイトで確認できます。

ライセンスを確認する

「ライセンス ステータス」画面では、ライセンスのタイプとステータスを確認することができます。

ライセンスの有効期限が迫っている場合、またはすでに過ぎている場合、ランチャーで該当するプログラムの保護ステータスが変更されます。

ライセンスの状況を確認する

1. ランチャーの一番右にあるアイコンを右クリックします。
   ポップアップ メニューが表示されます。
2. [ライセンス] を選択します。
3. [ライセンスのステータス] をクリックすると、インストールされているプログラムのライセンスに関する情報を確認できます。
4. [インストール ステータス] をクリックすると、インストールできるプログラムを確認できます。

ライセンスのステータスと有効期限は、「統計情報」画面でも表示されます。ライセンスの有効期限が過ぎている場合、製品を使用し続けるためにライセンスを更新する必要があります。

注: ライセンスが切れている場合、システム トレイのステータス アイコンが点滅します。

アクション センター

アクション センターでは、本製品に関連する重要な通知が表示されます。

ライセンスの有効期限が過ぎた、または近づいている場合、アクション センターで通知が表示されます。ライセンスのタイプとステータスにより、メッセージの背景色とコンテンツが異なります。

- ライセンスの有効期限が近づいている状態で使用できるライセンスがある場合、白い背景色のメッセージと [認証] ボタンが表示されます。
- ライセンスの有効期限が近づいている状態で使用できるライセンスがない場合、黄色い背景色のメッセージと [購入] および [ライセンスの入力] ボタンが表示されます。ライセンスを購入した場合、[ライセンスの入力] をクリックしてライセンスを認証できます。
- ライセンスの有効期限が過ぎた状態で使用できるライセンスがある場合、赤い背景色のメッセージと [認証] ボタンが表示されます。
- ライセンスの有効期限が過ぎた状態で使用できるライセンスがない場合、赤い背景色のメッセージと [購入] および [ライセンスの入力] ボタンが表示されます。ライセンスを購入した場合、[ライセンスの入力] をクリックしてライセンスを認証できます。

注: アクション センターにある [通知履歴を表示] をクリックすると、製品がこれまで表示した通知を確認できます。

ライセンスを認証する

ライセンス キーコード/キャンペーン コードをお持ちの場合、コードを認証することで製品を利用できます。

ライセンスを認証するには

1. ランチャーの一番右にあるアイコンを右クリックします。
   ポップアップ メニューが表示されます。
2. [ライセンス] を選択します。
3. 次のいずれかを選択します。
   - [ライセンスを認証] をクリックします。
   - [キャンペーン コードを認証] をクリックします。
4. 開くウィンドウでライセンス キーコードまたはキャンペーン コードを入力して、[**OK**] をクリックします。

   ヒント: ライセンス キーコードをメールで受け取った場合、キーコードをコピー・アンド・ペーストでフィールドにコピーできます。

「ライセンスの状況」画面で指定したライセンス キーコード/キャンペーン コードと有効期限が表示されるようになります。

第
3
章

はじめに

トピック：

- *全体の保護ステータスを表示する*
- *製品の統計情報を表示する*
- *製品のアップデート*
- *ウイルスとマルウェアについて*

本製品は、コンピュータをウイルスや危険なアプリケーションから保護します。

本製品は、アプリケーションの分析とソフトウェアの自動更新を行います。ユーザによる特別な操作は必要ありません。

全体の保護ステータスを表示する

「ステータス」画面では、インストールされている機能とそのステータスを確認できます。

「ステータス」画面を開くには

ユーザ インターフェースで [ステータス] を選択します。

「ステータス」画面が開きます。

各機能の横にあるアイコンからプログラムのステータスと関連のコンポーネントを確認できます。

ステータス アイコン	ステータス	説明
	OK	コンピュータが保護されています。機能が有効になっており、正常に動作していることを示します。
	情報	特定の機能で特別なステータスが発生していることを示します。 たとえば、機能がアップデートしている場合など。
	警告	コンピュータが保護されていないことを示します。 たとえば、パターン ファイルがしばらく更新されていない場合や特定の機能に問題がある場合など。
	エラー	コンピュータが保護されていないことを示します。 たとえば、ライセンスが切れた場合や重要な機能が無効の場合など
	オフ	機能が無効になっていることを示します。

製品の統計情報を表示する

「統計情報」画面では、本製品がインストールされてから行った処理を確認できます。

「統計情報」画面を開くには

ユーザ インターフェースで [統計情報] をクリックします。

「統計情報」画面が開きます。

- 更新を最後に確認した日時 - 前回の更新がいつ行われたかを表示します。
- ウイルスとスパイウェア スキャン - 本製品がスキャンおよび駆除したファイルの数を表示します。
- アプリケーション - ディープガードが許可またはブロックしたアプリケーションの数を表示します。
- ファイアウォールの接続数 - 許可/ブロックした接続の数を表示します。
- スパム/フィッシング フィルタ - 正常およびスパムとして認識したメールの数を示します。

製品のアップデート

本製品は最新の保護を提供するためにソフトウェアを自動的に更新します。

パターン ファイルのバージョンを表示する

「パターン ファイルの更新」画面でパターン ファイルが最後に更新された時間とバージョン番号を確認できます。

「パターン ファイルの更新」画面を開くには

1. ユーザ インターフェースで [設定] をクリックします。

   注: 設定を変更するには管理者の権限が必要です。

2. その他の設定 > データベースのバージョン の順に選択します。

「パターン ファイルの更新」画面で、ウイルスとスパイウェアのパターン ファイル、ディープガード、スパムとフィッシング フィルタが最後に更新された日付とそのバージョン番号が表示されます。

モバイル プロバイダの設定を変更する

モバイルのプロバイダに使用しているときをセキュリティの更新をダウンロードできるようにするか指定できます。

注: この機能はオペレーティング システムが Microsoft Windows 7 である場合に限り有効です。

デフォルトでは、ホーム (通常の) プロバイダに接続しているときにセキュリティの更新が自動的にダウンロードされ、モバイルのプロバイダでインターネットに接続しているときには更新がダウンロードされないようになっています。これは、通常とは違うプロバイダを使用していることで接続に対する料金が発生することを防ぐための仕様です。更新のダウンロードを停止することでインターネットの使用量とコストを抑えることが可能です。

注: また、この設定はモバイル プロバイダのネットワークに接続したときにのみ有効となります。ワイヤレスまたは有線のネットワークに接続した場合には、更新が通常のように自動でダウンロードされます。

設定を変更するには

1. ユーザ インターフェースで [設定] をクリックします。

   注: 設定を変更するには管理者の権限が必要です。

2. その他の設定 > モバイル プロバイダ > セキュリティ更新をダウンロードする の順に選択します。
3. モバイル接続に対するセキュリティ更新のオプションを選択します。

- ホーム ネットワークのみ

  ホーム ネットワークに接続しているときには更新を自動でダウンロードします。モバイルのネットワークを使用すると更新が停止します。推奨のオプションです。
- -

  モバイル プロバイダを使用している場合、更新はダウンロードされません。
- 常に使用

  接続しているプロバイダ/ネットワークに関係なく、更新を常にダウンロードします。コンピュータのセキュリティを常に最新の状態にしたい場合に適切なオプションです。

4. ホーム ネットワークから切断するときに更新をダウンロードするか毎回選ぶ場合、[ホーム プロバイダのネットワークから切断するときに選択] を選択します。

セキュリティ更新の停止

通常のプロバイダではなく、モバイルのプロバイダなどでインターネットに接続している場合、セキュリティの更新が停止している可能性があります。

その場合、「停止中」を知らせる通知が画面の右下に表示されます。通常とは違うプロバイダを使用していることで接続料金が発生している可能性があるため、セキュリティの更新は停止されます。[変更] をクリックすると、モバイルのプロバイダを使用しているときでも更新をダウンロードできるように設定できます。

注:

この機能はオペレーティング システムが Microsoft Windows 7 である場合に限り有効です。

ウイルスとマルウェアについて

マルウェアは、コンピュータの破壊、悪用、情報の搾取を目的とするプログラムです。

マルウェアは次の害を及ぼす可能性があります。

- Web ブラウザの操作
- 検索内容のリダイレクト
- 不要な広告の表示
- アクセスした Web サイトの記録
- 銀行情報などの個人情報の盗難
- ご利用のコンピュータからのスパムの送信
- ご利用のコンピュータからの他のコンピュータの攻撃

また、コンピュータの動作を遅くしたり不安定にすることもあります。コンピュータの動作が急に遅くなったり、頻繁にクラッシュするようになった場合、コンピュータがマルウェアに感染している可能性が高くなります。

ウイルス

ウイルスは、ファイルに感染して繰り返し自己増殖するプログラムです。他のファイルの内容を変更したり置換したりして、コンピュータに害を及ぼします。

ウイルスは、一般に、ユーザの知らないうちにコンピュータにインストールされるプログラムです。インストールされたウイルスは自己増殖を試みます。ウイルスによって、次のような問題が引き起こされます。

- システム リソースの使用
- コンピュータ上のファイルの変更や破損
- コンピュータを利用して別のコンピュータを感染する試み
- 不正目的でのコンピュータの利用

スパイウェア

スパイウェアは、キーボード入力・履歴・パスワード・個人情報などの機密情報をインターネットを通じて記録したり送付したりする悪意のあるプログラムです。

スパイウェアは次のような個人情報を収集する可能性があります。

- 閲覧したインターネット サイト
- ご利用のコンピュータ上のメール アドレス
- パスワード
- クレジットカード番号

スパイウェアは、ユーザの明示的な許可なしでインストールされることが多くあります。よくある仕組みで、有用なプログラムと一緒にインストールされるスパイウェアがあります。また、ブラウザのポップアップ ウィンドウのオプションをクリックすることで意図せずにインストールされるものもあります。

ルートキット

ルートキットとは、他のマルウェアの検出を困難にするプログラムです。

ルートキットは、ファイルやプロセスを隠します。一般に、コンピュータに実行する有害な処理をユーザから隠すことために利用されます。ルートキットがマルウェアを隠している場合、コンピュータがそのマルウェアを検出するのは困難になります。

本製品にはルートキットを具体的に調べるルートキット スキャナがあるので、マルウェアが自分自身を隠すことは容易ではありません。

リスクウェア

リスクウェアは意図的にコンピュータに害を与えるものではありませんが、悪用された場合にコンピュータに害を及ぼす可能性があります。

リスクウェアは厳密にマルウェアではありません。リスクウェアとして見なされているプログラムの多くは便利ですが、使用によって危険性があるものもあります。

リスクウェアの例：

- インスタント メッセージ用のプログラム (IRC、MSN メッセンジャーなど)
- コンピュータ間のファイル転送をインターネットで行うためのプログラム
- インターネット電話プログラム (*VoIP (Voice Over Internet Protocol)*)
- リモート アクセス ソフトウェア (VNC など)
- スケアウェアなどの偽セキュリティ ツール
- CD のチェックやコピー ガードを解除するソフトウェア

プログラムを明示的にインストールし、正しく設定した場合、危険性は低くなります。

リスクウェアが知らないうちにインストールされている場合、悪意でイントールされている可能性が高いので削除してください。

第
4
章

コンピュータをマルウェアから保護する

トピック：

- *コンピュータをスキャンする*
- *スキャンからファイルを除外する*
- *隔離保存フォルダを使用する*
- *ディープガードについて*

ウイルスとスパイウェアの防御機能は、サーバの破壊、個人情報の盗難、コンピュータの不正使用といった問題を引き起こす可能性のあるプログラムからユーザを保護します。

デフォルトでは、マルウェアは検出時にすぐに処理され、コンピュータに害を及ぼせないになります。

ウイルスとスパイウェアのスキャンはデフォルトでローカルのハードディスク、リムーバブル メディア (ポータブル ドライブやコンパクトディスクなど)、およびダウンロードされたコンテンツを自動的にスキャンします。メールのスキャンを自動で行うように設定することも可能です。

ウイルスとスパイウェア防御は、マルウェアの存在を示す可能性のある変更がないかコンピュータを常に監視します。重要なシステム プロセスを変更するシステム設定やその試みなど、問題を引き起こす可能性のあるシステムの変更が見つかった場合、マルウェアが存在している可能性が高いため、ディープガードによってプログラムの実行が停止されます。

コンピュータをスキャンする

ウイルスとスパイウェア スキャンが有効の場合、コンピュータ上に危険なファイルがあるか自動的にスキャンされます。スキャンを手動で実行したり、特定の日付/時間で実行するようにしたりすることも可能です。

ウイルスとスパイウェア スキャンを常に有効にすることを推奨します。必要に応じてマニュアル スキャンで危険なファイルがないことを確認したり、除外したファイルをスキャンしたりできます。

スケジュール スキャンは、ウイルスとスパイウェア スキャンを設定した日時に実行します。

ファイルを自動的にスキャンする

リアルタイム スキャンは、ファイルがアクセスされたときにスキャンを実行し、マルウェアを含むファイルが検出された場合、そのファイルへのアクセスをブロックしてコンピュータを保護します。

コンピュータがファイルをアクセスする前にリアルタイム スキャンがファイルに悪質なファイルがあるかスキャンします。危険なコンテンツが検出された場合、ファイルが害を及ぼせないように隔離保存されます。

リアルタイム スキャンとシステムの処理速度

通常、スキャンは短時間で終わり、使用するシステム リソースも少ないため、ユーザがその処理を意識することはありません。リアルタイム スキャンに必要な時間とシステムの負荷は、ファイルの内容、場所、種類などによって異なります。

次のようなファイルはスキャンが通常より長くかかります。

- CD、DVD、USB ドライブなどのリムーバブル ドライブにあるファイル。
- 圧縮ファイル (*.zip* など)

  注: 圧縮されたファイルはデフォルトではスキャンされません。

次のような場合、リアルタイム スキャンはコンピュータの動作を低下する可能性があります。

- コンピュータがシステム要件に満たない場合
- 多数のファイルを同時にアクセスする場合。たとえば、スキャン対象のファイルが多く格納されているディレクトリを開いた場合など。

リアルタイム スキャンを有効/無効にする

リアルタイム スキャンを有効にすると、マルウェアがコンピュータに害を与えることができないようできます。

リアルタイム スキャンを有効/無効にするには

1. ユーザ インターフェースで [ステータス] を選択します。
2. [ページの設定を変更する] をクリックします。

   注: セキュリティ機能を無効にするには管理者の権限が必要です。

3. [ウイルスとスパイウェア スキャン] を有効または無効にします。
4. [閉じる] を選択します。

危険なファイルを自動的に処理する

リアルタイム スキャンは危険なファイルを自動的に処理することができます。

リアルタイム スキャンが危険なファイルを自動的に処理するには

1. ユーザ インターフェースで [設定] をクリックします。

   注: 設定を変更するには管理者の権限が必要です。

2. コンピュータ セキュリティ > ウイルスとスパイウェア スキャン の順にクリックします。
3. [危険なファイルを自動的に処理する] を選択します。

危険なファイルを自動的に処理しない場合、危険なファイルの検出時に処理を確認するメッセージが表示されます。

スパイウェアを処理する

ウイルスとスパイウェア スキャンは、スパイウェアの実行を阻止することができます。

スパイウェアが実行される前に本製品がスパイウェアをブロックし、処理をユーザに訪ねます。

スパイウェアの処理

処理	スパイウェアに実行する処理
自動	検出されたスパイウェアに対して本製品が適切な処理を行います。
スパイウェアを隔離保存する	スパイウェアを隔離保存し、害を及ぼせないようにします。
スパイウェアを削除する	スパイウェアをコンピュータから削除します。
スパイウェアをブロックする	スパイウェアをコンピュータに残し、アクセスをブロックします。
スパイウェアをスキャンから除外する	スパイウェアの実行を許可し、今後のスキャンから除外します。

リスクウェアを処理する

ウイルスとスパイウェア スキャンは、リスクウェアの実行を阻止することができます。

リスクウェアが実行される前に本製品がスパイウェアをブロックし、処理をユーザに訪ねます。

リスクウェアの処理

処理	リスクウェアに実行する処理
リスクウェアをブロックする	リスクウェアをコンピュータに残し、アクセスをブロックします。
リスクウェアを隔離保存する	リスクウェアを隔離保存し、害を及ぼせないようにします。
リスクウェアを削除する	リスクウェアをコンピュータから削除します。
リスクウェアをスキャンから除外する	リスクウェアの実行を許可し、今後のスキャンから除外します。

追跡 Cookie を自動的に削除する

追跡 Cookie を削除すると、Web サイトがアクセスしたサイトを記録できないようになります。

追跡 Cookie は、アクセスした Web サイトの記録を保存する小さなファイルです。次の方法で、追跡 Cookie をコンピュータから削除できます。

1. ユーザ インターフェースで [設定] をクリックします。

   注: 設定を変更するには管理者の権限が必要です。

2. コンピュータ セキュリティ > ウイルスとスパイウェア スキャン の順にクリックします。
3. [追跡 Cookie を削除する] を選択します。
4. [OK] をクリックします。

ファイルを手動でスキャンする

ファイルを手動でスキャンすることができます。たとえば、外部のデバイスをコンピュータに接続するときにデバイスにスキャンを実行できます。

マニュアル スキャンを開始する

コンピュータ全体、あるいは特定のドライブやフォルダをスキャンできます。また、特定のマルウェアをスキャンすることも可能です。

特定のマルウェアに感染している疑いがある場合、コンピュータがそのマルウェアに感染しているか確認できます。コンピュータ上の特定の場所 (フォルダ・ドライブなど) に感染の疑いがある場合、その場所のみスキャンすることが可能です。このような特定のファイルや場所に対するマニュアル スキャンは、コンピュータ全体を対象とするスキャンと比べ、短時間で完了します。

マニュアル スキャンを開始するには

1. ユーザ インターフェースで、[スキャン] の下にある矢印をクリックします。

   スキャンのオプションが表示されます。

2. スキャンの種類を選択します。

   [スキャンの設定] を選択すると、マニュアル スキャンの設定を変更できます。

3. [スキャンするオブジェクトを指定] を選択した場合、設定を指定できる別のウィンドウが開きます。[スキャン ウィザード] が開きます。

スキャンの種類

コンピュータ全体か特定の場所をスキャン対象としたり、特定のマルウェアをスキャンしたりすることができます。

スキャンの種類

スキャンの種類	スキャンの対象	用途
ウイルスとスパイウェア スキャン	コンピュータの一部に対してウイルス、スパイウェア、リスクウェアをスキャンします	完全スキャンより短時間で完了します。インストールされているプログラム ファイルなどが主に格納されているフォルダにのみスキャンを実行します。このスキャンは、コンピュータの安全性をすぐに確認したい場合に適切です。

スキャンの種類	スキャンの対象	用途
完全スキャン	コンピュータ全体(内蔵型および外付けハード ドライブすべて) に対してウイルス、スパイウェア、リスクウェアをスキャンします	コンピュータにマルウェアやリスクウェアが一切存在しないことを確認したい場合。マルウェアスキャンとハードディスクスキャンを両方行なうため最も長く時間がかかります。また、ルートキットによって隠されているアイテムもチェックします。
スキャンするオブジェクトを指定...	特定のファイル、フォルダ、またはドライブに対してウイルス、スパイウェア、リスクウェアをスキャンします	コンピュータ上の特定の場所にマルウェアの存在が疑われる場合。たとえば、その場所で不審な活動が見られる場合や、ピア ツー ピア ファイル共有ネットワークなどの有害の可能性のあるソースからダウンロードしたファイルがある場合など。スキャン時間は対象のファイルサイズによります。たとえば、数ファイルしかないフォルダを対象にした場合、スキャンは早く終わります。
ルートキットをスキャン	セキュリティ問題を示す可能性があるような、システムの重要な場所に隠れているファイル、フォルダ、ドライブ、プロセスをスキャンします。	ルートキットがコンピュータに潜んでいる疑いがある場合。たとえば、マルウェアが最近検出された場合などにマルウェアがルートキットをインストールしなかったことを確認したい場合に適切です。

Windows Explorer でスキャンを実行する

Windows エクスプローラからディスク、フォルダ、およびファイルに対して、ウイルス、スパイウェア、およびリスクウェアのスキャンを実行することができます。

ディスク、フォルダ、またはファイルをスキャンする

1. スキャンするディスク、フォルダ、またはファイルにマウス ポインタを合わせ、右クリックします。
2. 右クリック メニューから [フォルダをウイルス スキャン] を選択します (メニューの表示はエクスプローラで選択されている項目 (ファイル、フォルダなど) によって異なります)。
   [スキャン ウィザード] が開き、スキャンが開始します。

ウイルスまたはスパイウェアが検出された場合、スキャン ウィザードに従って駆除の手順を進めます。

スキャンするファイルを選択する

マニュアル スキャンとスケジュール スキャンで、ウイルスやスパイウェアスキャンの対象となるファイルを選択できます。

1. ユーザ インターフェースで [設定] をクリックします。

   注: 設定を変更するには管理者の権限が必要です。

2. その他の設定 > マニュアル スキャン の順に選択します。
3. 「スキャン オプション」で次のいずれかを選択します。

指定ファイルのみス	実行可能ファイルなど、特定の形式のファイルのみスキャンするようにします。このオプションを選択する。す:.ani、.asp、.ax、.bat、.bin、.boo、.chm、.cmd、.com、.cpl、.dll、.doc、.dot、.drv、

キャン	
圧縮ファイルの中をスキャンする	圧縮ファイルの中にあるファイルとフォルダをスキャンします。
ヒューリスティックスを使用する	ヒューリスティックをすべて使用して、最新/未知のマルウェアに対する検出機能を向上します。 注: このオプションを有効にすると、スキャンが完了するまでの時間が長くなり、誤検知が増える可能

4. [OK] をクリックします。

注: 除外リストにあるファイルは指定されてもスキャンの対象にはなりません。

危険なファイルを処理する

危険なファイルの検出時にファイルを処理する方法を選択できます。

危険なコンテンツを処理するには (マニュアル スキャン検出時)

1. ユーザ インターフェースで [設定] をクリックします。

   注: 設定を変更するには管理者の権限が必要です。

2. その他の設定 > マニュアル スキャン の順に選択します。
3. [ウイルスまたはスパイウェア検出時に] で次のいずれかのオプションを選択できます。

オプション	説明
処理を選択する (デフォルト)	処理を選択します。
ファイルを駆除する	感染ファイルを駆除します (できない場合があります)。 注: 感染したファイルを駆除できない場合、ファイルを隔離保存します (ファイルがネットワークまたはリムーバブル ドライブにある場合を除いて)。
ファイルを隔離保存する	危険なファイルを隔離保存フォルダに移動し、コンピュータに害を与えることができないようにします。
自動的に削除	危険なファイルを削除します。
レポートのみ	危険なファイルに対して処理を行いません。危険なファイルの検出はスキャン レポートに記録されます。 注: リアルタイム スキャンが無効の状況でこのオプションを選択すると、コンピュータがマルウェアに感染する危険性があります。

注: スケジュール スキャンで検出された危険ファイルは自動的に駆除されます。

スケジュール スキャンを設定する

スケジュール スキャンを設定すると、コンピュータを使用していない時間にスキャンが自動的に開始するようにしたり、特定の時間にスキャンを定期的に実行するようにしたりできます。

スケジュール スキャンを設定するには

1. ユーザ インターフェースで [設定] をクリックします。

   注: 設定を変更するには管理者の権限が必要です。

2. その他の設定 > スケジュール スキャン の順に選択します。
3. [スケジュール スキャンを有効にする] を有効にします。
4. スキャンを開始する日時を選択します。

オプション	説明
日単位	スキャンを毎日実行します。
週単位	スキャンを毎週指定の日に実行します。リストから日を選択します。
月単位	スキャンを毎月指定の日に実行します。リストから日を選択します。 1. [日] オプションを1つ選択します。 2. リストから日付を選択します。

5. スキャンを実行する時間を指定します。

オプション	説明
開始時刻	指定した時間にスキャンを開始します。
指定アイドル時間が経過した場合	コンピュータを指定した時間以上操作していない場合にスキャンを開始します。

スケジュール スキャンはマニュアル スキャンの設定を使用します。ただし、圧縮ファイルはすべてスキャンの対象となり、危険なファイルは検出時に自動的に駆除されます。

メールをスキャンする

メール スキャンは、システムがメールを通じて危険なファイルに感染することを保護します。

メール スキャンを使用するにはウイルスとスパイウェア スキャンが有効になっている必要があります。

メール スキャンを有効にするには

1. ユーザ インターフェースで [設定] をクリックします。

   注: 設定を変更するには管理者の権限が必要です。

2. コンピュータ セキュリティ > ウイルスとスパイウェア スキャン の順にクリックします。
3. [危険な添付ファイルを削除する] を選択します。
4. [**OK**] をクリックします。

メールと添付ファイルのスキャン

ウイルスとスパイウェア スキャンは、メールから危険なコンテンツを取り除くことができます。

ウイルスとスパイウェア スキャンは、Microsoft Outlook、Outlook Express、Microsoft Mail、Mozilla Thunderbird などのメール プログラムを通じて受信する危険なメールを取り除くことができます。POP3 プロトコルを利用してメール サーバから送られているメール (暗号化されていないもの) と添付ファイル (ある場合) をスキャンできます。

ウイルスとスパイウェア スキャンは Hotmail、Yahoo! mail、Gmail などの Web ブラウザ上で動作するメール プログラムのメール (添付ファイルを含む) をスキャンすることはできません。Web メールを通じて危険な添付ファイルをダウンロードしても、リアルタイム スキャンが危険なファイルを検出できるため、システムはウイルスから保護されます。

注: リアルタイム スキャンはシステムを保護できますが、友人や家族まで保護することはできません。リアルタイム スキャンは添付ファイルを開かない限りスキャンを実行しないため、Web メールで添付ファイルをスキャンせずに転送することが可能です。これは、ウイルスを知らないまま転送できることを意味します。

スキャンの結果を表示する

ウイルスとスパイウェアの履歴から検出した危険なファイルを確認することができます。

場合により、製品が危険なファイルに対して指定した処理を実行できないことがあります。たとえば、ファイルを駆除できない場合、ファイルが隔離保存されます。このような情報をウイルスとスパイウェアの履歴から確認できます。

履歴を確認するには

1. ユーザ インターフェースで [設定] をクリックします。

   注: 設定を変更するには管理者の権限が必要です。

2. コンピュータ セキュリティ > ウイルスとスパイウェア スキャン の順にクリックします。
3. [削除したファイルの履歴を表示する] をクリックします。

ウイルスとスパイウェアの履歴では次の情報が表示されます。

- マルウェア (危険なファイル) が検出された日時
- マルウェアの名前とコンピュータで検出された場所/パス
- マルウェアに対して実行された処理

スキャンからファイルを除外する

スキャンから特定のファイルを除外することができます。除外リストに追加されたアイテムはスキャンされません。

注: 除外リストは、リアルタイム スキャンとマニュアル スキャンでは別です。たとえば、リアルタイム スキャンから特定のファイルを除外した場合、マニュアル スキャンに対してもそのファイルを除外していない限り、ファイルがマニュアル スキャンの対象となります。

特定のファイルを除外する

ファイルの種類でファイルをスキャンから除外した場合、指定した拡張子を持つすべてのファイルがスキャンから除外されます。

特定のファイルの種類をスキャンから除外するには

1. ユーザ インターフェースで [設定] をクリックします。

   注: 設定を変更するには管理者の権限が必要です。

2. ファイルの種類をリアルタイム スキャンまたはマニュアル スキャンから除外するか選択します。
   - コンピュータ セキュリティ > ウイルスとスパイウェア スキャン の順に選択すると、ファイルの種類をリアルタイム スキャンから除外できます。
   - その他 > マニュアル スキャン の順に選択すると、ファイルの種類をリアルタイム スキャンから除外できます。
3. [スキャンからファイルを除外する] をクリックします。
4. 特定のファイルを除外するには
   a) 「ファイルの種類」タブをクリックします。
   b) [次の拡張子のファイルはスキャンしない] を選択します。
   c) [追加] ボタンの横にあるフィールドにスキャンから除外するファイルの拡張子を入力します。

      '.' を入力することで拡張子のないファイルを指定できます。1つの文字 '?' または文字数不定 '*' のワイルドカードも利用できます。

      たとえば、実行ファイルを除外する場合、[exe] をフィールドに入力します。
   d) [追加] をクリックします。
5. 他の拡張子を除外する場合、上記の手順を繰り返します。
6. [**OK**] をクリックして、「スキャン対象から除外」ウィンドウで表示されます。
7. [**OK**] をクリックして、新しい設定を適用します。

指定したファイルの種類がスキャンから除外されます。

特定の場所にあるファイルを除外する

特定の場所/パス (特定のドライブやフォルダなど) にあるファイルをスキャンから除外できます。

スキャンから除外する場所を追加/削除するには

1. ユーザ インターフェースで [設定] をクリックします。

   注: 設定を変更するには管理者の権限が必要です。

2. 場所/パスをリアルタイム スキャンまたはマニュアル スキャンから除外するか選択します。
   - コンピュータ > ウイルスとスパイウェア スキャン の順に選択すると、場所/パスをリアルタイム スキャンから除外できます。
   - コンピュータ > マニュアル スキャン の順に選択すると、場所/パスをマニュアル スキャンから除外できます。
3. [スキャンからファイルを除外する] をクリックします。
4. ファイル/ドライブ/フォルダを除外するには、次の手順を実行します。

a) 「オブジェクト」タブを選択します。
b) [オブジェクトを除外 (ファイル、フォルダ...)] を選択します。
c) [追加] をクリックします。
d) ウイルス スキャンから除外するファイル、フォルダ、ドライブを選択します。

注: ドライブの中には、CD ドライブ、DVD ドライブなどのリムーバブル ドライブやネットワーク ドライブもあります。ネットワーク ドライブと空のリムーバブル ドライブは除外できません。

e) [OK] をクリックします。

5. ウイルス スキャンから他のファイル、フォルダ、ドライブを除外する場合、上記の手順を繰り返します。
6. [OK] をクリックして、「スキャン対象から除外」ウィンドウで表示されます。
7. [OK] をクリックして、新しい設定を適用します。

指定したドライブ/フォルダがスキャンから除外されます。

除外したアプリケーションを表示する

スキャンの対象から除外したアプリケーションを除外リストから削除することで、スキャンの対象に含むことができます。

リアルタイム スキャンまたはマニュアル スキャンがスパイウェア/リスクウェアとして識別したアプリケーションを安全と断定できる場合、そのアプリケーションをスキャンから除外することができます。

注: ウイルスまたは悪質なソフトウェアとして動作するアプリケーションを除外することはできません。

アプリケーションをスキャンから直接除外することはできません。スキャン中に除外したアプリケーションが除外リストに表示されます。

スキャンの対象から除外されているアプリケーションを表示するには

1. ユーザ インターフェースで [設定] をクリックします。

   注: 設定を変更するには管理者の権限が必要です。

2. リアルタイム スキャンまたはマニュアル スキャンから除外したアプリケーションを表示するか選択します。
   - コンピュータ > ウイルスとスパイウェア スキャン の順に選択すると、リアルタイム スキャンから除外したアプリケーションを確認できます。
   - コンピュータ > マニュアル スキャン の順に選択すると、マニュアル スキャンから除外したアプリケーションを確認できます。
3. [スキャンからファイルを除外する] をクリックします。
4. 「アプリケーション」タブをクリックします。

   注: 除外できるアプリケーションはスパイウェアとリスクウェアに限ります。ウイルスは除外できません。

5. 除外したアプリケーションをもう一度スキャンしたい場合
   a) スキャンの対象に含むアプリケーションを選択します。
   b) [削除] をクリックします。

6. [OK] をクリックして「スキャン対象から除外」ウィンドウを閉じます。
7. [OK] をクリックします。

隔離保存フォルダを使用する

隔離保存フォルダには、有害な可能性のあるファイルが格納されています。

隔離保存したファイルは蔓延したり、コンピュータに害を及ぼしたりすることはできません。

マルウェア、スパイウェア、およびリスクウェアを隔離保存して、脅威をさらせないようにすることができます。隔離保存したアプリケーションやファイルが必要な場合、隔離保存フォルダから復元することが可能です。

隔離保存したファイル/アプリケーションが不要な場合、削除してもかまいません。削除すると、ファイル/アプリケーションはコンピュータから完全に削除されます。

- 隔離保存したマルウェアは削除してもコンピュータの動作に影響することはほとんどありません。
- 隔離保存したスパイウェアもマルウェアと同様、大抵の場合削除しても問題はありません。ただし、隔離保存したスパイウェアが正規のプログラムの一部の場合、削除することによりそのプログラムが正しく動作しなくなる可能性があります。正規のプログラムをコンピュータ上で実行するにはスパイウェアを隔離保存フォルダから復元してください。
- 隔離保存したリスクウェアは正規のプログラムである可能性があります。プログラムを自分でインストールおよび設定した場合、プログラムを隔離保存フォルダから復元することができます。リスクウェアが知らないうちにインストールされた場合、悪意でイントールされた可能性が高いので削除してください。

隔離保存したアイテムを表示する

隔離保存したアイテムの詳細を確認できます。

隔離保存したアイテムの詳細を表示するには

1. ユーザ インターフェースで [設定] をクリックします。

   注: 設定を変更するには管理者の権限が必要です。

2. コンピュータ セキュリティ > ウイルスとスパイウェア スキャン の順にクリックします。
3. [隔離保存したファイルを表示する] をクリックします。
   「隔離保存」画面では、隔離保存したアイテムの数を確認することができます。
4. [詳細] をクリックすると、隔離保存したアイテムの詳細を表示できます。
   隔離保存したアイテムはマルウェアの名前またはファイルのパス別に並び替えできます。
   最初の100アイテムのタイプ、名前、パスが表示されます。
5. [状態]列の横にある アイコンをクリックすると、隔離保存したアイテムの追加情報を確認できます。

隔離保存したアイテムを復元する

隔離保存したアイテムを復元することができます。

必要に応じて、隔離保存フォルダからアプリケーションやファイルを復元することができます。隔離保存フォルダからアイテムを復元するとアイテムに対する保護は無効になりますので、注意が必要です。復元したアイテムはコンピュータ上の元の場所に戻ります。

隔離保存したアイテムを復元するには

1. ユーザ インターフェースで [設定] をクリックします。

   注: 設定を変更するには管理者の権限が必要です。

2. コンピュータ セキュリティ > ウイルスとスパイウェア スキャン の順にクリックします。
3. [隔離保存したファイルを表示する] をクリックします。
4. 復元するアイテムを選択します。
5. [復元] をクリックします。

ディープガードについて

ディープガードは、ファイルのコンテンツとアプリケーションの動作を分析した上で危険と判断したアプリケーションを監視します。

ディープガードは、ウイルス、ワーム、および他の危険なアプリケーションの検出とブロックを行い、不審なアプリケーションがインターネットに接続することを阻止します。

ディープガードが危険性のあるアプリケーションを検出した場合、セーフゾーンでアプリケーションの実行が許可されます。セーフゾーンでは、アプリケーションがコンピュータに害を与えることはできません。ディープガードはアプリケーションを分析し、アプリケーションがマルウェア (悪質なソフトウェア) である可能性を判断します。マルウェアの可能性である可能性が高い場合、アプリケーションがブロックされます。

ディープガードは次のようなシステムの変更を検出できます。

- システム設定 (Windows レジストリ) の変更
- 重要なシステム プログラム (本製品のようなセキュリティ プログラムなど) を無効にしようとする試み
- 重要なシステム ファイルを編集しようとする試み

ディープガードを有効/無効にする

ディープガードを有効にすると、不審なアプリケーションがシステムの設定を変更することを阻止できます。

Windows XP を使用している場合、ディープガードを有効にする前に Service Pack 2 がインストールされていることを確認してください。

ディープガードを有効/無効にするには

1. ユーザ インターフェースで [ステータス] を選択します。
2. [ページの設定を変更する] をクリックします。

   注: セキュリティ機能を無効にするには管理者の権限が必要です。

3. [ディープガードを有効にする] を有効または無効にします。
4. [閉じる] を選択します。

ディープガードがブロックしたアプリケーションを許可する

ディープガードが許可/ブロックするアプリケーションを設定できます。

ディープガードはまれに安全なアプリケーションの動作をブロックすることもあります。これは、アプリケーションがシステムを変更する可能性があり、危険性があると判断されることで起こります。また、ディープガードのポップアップが表示されたときに、ユーザがアプリケーションを誤ってブロックした可能性もあります。

ディープガードがブロックしたアプリケーションを許可するには

1. ユーザ インターフェースで [ツール] をクリックします。
2. [アプリケーション] をクリックします。
   「監視しているアプリケーション」リストが表示されます。
3. 対象のアプリケーションを見つけます。

   注: 列のタイトルをクリックすると、リストをソースできます。たとえば、[権限] 列をクリックすると、アプリケーションを許可/ブロックした順に並び替えできます。

4. [権限] 列にある [許可] を選択します。
5. [閉じる] を選択します。

ディープガードがアプリケーションを許可します。

ディープガードを互換性モードで使用する

最高の保護を提供するために、ディープガードは実行されているプログラムを一時的に変更します。オンライン ゲームなど、プログラムの中にはファイルが変更されていないか確認するものがあります。それらのプログラムでディープガードを利用するには互換性モードを有効にする必要があります。

互換性モードを有効にするには

1. ユーザ インターフェースで [設定] をクリックします。

   注: 設定を変更するには管理者の権限が必要です。

2. コンピュータ セキュリティ > ディープガード の順にクリックします。
3. [互換性モードを使用する] を選択します。
4. [**OK**] をクリックします。

不審な動作に関する警告

ディープガードは、危険なアプリケーションを監視します。監視されているアプリケーションがインターネットに接続しようとしたり、システムを変更しようとしたり、不審な動作を実行したりする場合、アプリケーションがブロックされます。

ディープガードの [不審な動作を警告する] 設定を有効にした場合、危険性のあるアプリケーションの検出時、または評価が不明なアプリケーションを起動したときに通知が表示されるようになります。

ディープガードがブロックしたアプリケーションの処理を選択するには

1. [詳細] をクリックするとプログラムの詳細情報を確認できます。
   表示される詳細情報
   - アプリケーションの場所/パス

- アプリケーションに対するディープガード ネットワークの評価
- アプリケーションの普及率/知名度

2. ディープガードがブロックしたアプリケーションを信頼できるか選択します。

- アプリケーションをブロックしない場合、[アプリケーションを信頼しています。アプリケーションの実行を許可します。] を選択します。

  次のような場合、アプリケーションが安全である傾向があります。

  - ディープガードがユーザの操作によってアプリケーションをブロックした
  - アプリケーションに見覚えがある
  - 信頼できるソースからアプリケーションを入手した

- アプリケーションをブロックする場合、[アプリケーションを信頼していません。アプリケーションを拒否します。] をクリックします。

  次のような場合、アプリケーションが危険である傾向があります。

  - アプリケーションが一般的にあまり知られていない
  - アプリケーションの評価が不明
  - アプリケーションに見覚えがない

3. 不審なアプリケーションに対して F-Secure に分析を依頼するには

a) [このアプリケーションを **F-Secure** に報告する] をクリックします。
アプリケーションの分析に関する確認メッセージが表示されます。

b) 条件に同意し、サンプルを提供する場合、[同意する] をクリックします。

次のような場合、サンプルを提供することを推奨します。

- ディープガードが安全と断定できるアプリケーションをブロックした場合
- アプリケーションがマルウェアである可能性が高い場合