Avira Antivirus Premium

ユーザー マニュアル

AVIRA

商標と著作権

商標

Windows は、米国およびその他の国における、米国 Microsoft Corporation の登録商標です。
その他すべてのブランド名および製品名は、その所有者の商標または登録商標です。
このマニュアルでは、商標を保護するマークは使用していません。
しかし、これらの商標を自由に使用できるという意味ではありません。

著作権情報

サードパーティのプロバイダによるコードが、Avira Antivirus Premium に使用されています。
当社がコードを使用することを許諾してくださった著作権所有者の方々に感謝します。
著作権に関する詳細情報については、Avira Antivirus Premium のプログラム ヘルプの「サード パーティ ライセンス」下のを参照してください。

目次

1. はじめに

Avira
製品は、ウィルス、ワーム、トロイの木馬、アドウェア、スパイウェア、その他の危険から、コンピュータを保護します。
これらは、このマニュアルで、ウィルスあるいはマルウェア（有害ソフトウェア）、および不要プログラムとして扱われています。

マニュアルには、プログラムのインストールと操作に関する説明が記載されています。

その他のオプション、情報は、当社のウェブサイトでご覧ください（http://www.avira.jp）。

Avira ウェブサイトでは、次の事が可能です。

- Avira デスクトップ プログラムに関する情報へのアクセス
- 最新 Avira デスクトップ プログラムのダウンロード
- 最新製品のマニュアル（PDF）のダウンロード
- 無料サポート、リペア ツールのダウンロード
- 包括的な知識データベースおよびトラブルシューティングのための FAQ へのアクセス
- 国別サポート連絡先へのアクセス。

Avira チーム一同

1.1 アイコンと強調表示

次のアイコンが使用されています。

アイコン／記号表示	説明
✓	アクションを実行する前に、満たしている必要のある条件の前に配置されています。
▸	ユーザーが実行するアクション ステップの前に配置されています。
↳	前のアクションに続くイベントの前に配置されています。
警告	重大なデータ喪失の発生の警告の前に配置されています。
注意	特に重要な情報、またはAvira製品を使いやすくするためのヒントの前に配置されています。

次の強調表示が使用されています。

強調表示	説明
イタリック体	ファイル名、またはパス データ
	表示されたソフトウェア インターフェイス エレメント（例：ウィンドウ セクションやエラー メッセージ）。
太字	クリックできるソフトウェア インターフェイス エレメント（例：メニュー項目、ナビゲーション エリア、オプション ボックス、ボタン）。

2. 製品情報

この章には、Avira 製品の購入および使用に関する概要が記載されています。

- 参照：章 提供範囲
- 参照：章 システム要件
- 参照：章 使用許諾およびアップグレード
- 参照：章 ライセンス マネージャ

Avira
製品は、ウィルス、マルウェア、不要プログラム、その他の危険からコンピュータを保護する包括的でフレキシブルなツールです。

▸ 以下の情報に注意してください。

警告
貴重なデータの損失は、通常、重大な問題につながります。
どんなに素晴らしいアンチウィルス
プログラムでも、データ損失を完全に回避できる保護を提供することはできません。
安全のためにも、定期的にデータのコピーを作成（バックアップ）してください。

注意
プログラムが最新の状態である場合にのみ、ウィルス、マルウェア、不要プログラム、その他の危険に対する、確実で効率的な保護を提供することができます。 自動更新により、Avira
製品が最新の状態になっていることを確認してください。
必要に応じて、プログラムを設定します。

2.1 提供範囲

Avira製品は以下の機能を装備しています:

- プログラム全体を監視/ 管理/ コントロールするコントロール センター
- わかりやすい標準および上級オプションならびに詳細コンテキスト付きヘルプによるセンター環境設定
- すべての既知のウイルスおよびマルウェアの種類に対して、プロファイル コントロールならびに設定可能なスキャンを提供するSystem Scanner(オンデマンドスキャン)
- Windows Vistaのユーザー アカウント コントロールに統合して、管理者権限を必要とするタスクの実行が可能。
- すべてのファイル アクセスの試行に対する継続的な監視(オンアクセス スキャン)のためのReal-Time Protection機能
- プログラム アクションの恒久的監視を行う ProActiv コンポーネント (32 ビット システムのみ)
- 添付ドキュメントのチェックを含む、メールのウイルスとマルウェアに対する恒久的なチェックを実行するMail Protection(POP3スキャナ、IMAPスキャナおよびSMTPスキャナ)
- ウェブブラウザ内に統合され、高速で便利な検索オプション搭載の検索ツールバーAvira SearchFree Toolbarを提供。 一般に知られたインターネット機能のウィジェットも搭載されています。
- HTTPプロトコル(ポート80, 8080, 3128の監視)使用のインターネットから転送されるデータとファイルの監視用のWeb Protection
- Avira Free Android Security アプリケーションの目的は、盗難対策だけではありません。 アプリケーションは携帯電話をなくした時、あるいは最悪の場合、盗難にあった時の再発見にその有益性を発揮します。 さらにアプリケーションは、受信あるいはSMSをブロッキングします。 Avira Free

Android Security は、Android オペレーティング
システムで作動している携帯電話、スマートフォンを保護します。

- 疑わしいファイルの隔離と処理のための統合隔離管理
- コンピューター
  システムにインストールされた秘匿マルウェア(ルートキット)検出用のRootkits Protection
  (Windows XP 64ビットに使用できません)
- 検出されたウイルスとマルウェアに関する詳細情報へのインターネットによる直接アクセス
- インターネットでのウェブサーバーを介した単一ファイル更新と増分VDF更新、ウイルス定義、および検索エンジンに関する簡単で迅速なプログラム更新
- ライセンス マネージャでのわかりやすい使用承認
- 更新やスキャンに関する1回限りまたは定期的なジョブを計画するための統合スケジューラ
- ヒューリスティック スキャン方式を含む革新的なスキャン テクノロジー(スキャン エンジン)に基づく、非常に高いウイルスとマルウェアの検出率
- ネストされたアーカイブの検出や、スマート拡張子の検出を含む、すべての従来型のアーカイブ タイプの検出
- 高パフォーマンスのマルチスレッド機能(複数ファイルの同時高速スキャン)

2.2 システム要件

システム要件は以下の通りです：

- Pentiumプロセッサー搭載コンピューターあるいはそれ以降(1 GHz以上推薦)
- オペレーティング システム(OS)
  - Windows XP、最新SP (32あるいは64ビット)または
  - Windows 7、最新SP (32あるいは64ビット)または
  - Windows 8、最新SP (32あるいは64ビット)

- 150 MB以上のハード ディスク空き容量
  (隔離機能を使用する場合は、さらに空き容量が必要です)
- Windows XPで512 MB以上のRAM
- Windows Vista、Windows 7で1024 MB以上のRAM。
- インストールには管理者権限が必要
- すべてのインストールにInternet Explorer 6.0以降が必要
- 適切なインターネット接続(インストールを参照)

Avira SearchFree Toolbar

- オペレーティング システム(OS)
  - Windows XP、最新SP (32あるいは64ビット)または
  - Windows 7、最新SP (32あるいは64ビット)または
  - Windows 8、最新SP (32あるいは64ビット)
- ウェブブラウザ
  - Internet Explorer 6.0以降
  - Firefox 3.0以降
  - Chrome 18.0以降

> 注記
> 必要に応じて、Avira SearchFree Toolbarをインストールする前に既存の旧検索ツールバーをアンインストールしてください。 そうしないと、Avira SearchFree Toolbarがインストールできない場合があります。

Windows Vista ユーザーの場合

Windows XP上では多くののユーザーが管理者権限で作業を行います。
しかしながら、このためにウィルスあるいは迷惑プログラムがコンピュータに侵入しやすくなるため、セキュリティの観点からはこれは望ましくありません。

このためにMicrosoftは、Windows Vistaで「ユーザー アカウント
コントロール」を導入しています。
これは管理者としてログインするユーザーに、より多くの保護を提供します。それによって、Windows Vistaでは管理者が通常ユーザーよりも先に特権を受けます。
アクションに対して管理者権限が必要な場合、Windows
Vistaでは情報アイコンによって明確に表示されます。
さらに、ユーザーは必要なアクションを明確に確定する必要があります。
それによって特権が増加するだけで、管理業務は許可の取得後にオペレーティング
システム(OS)によって実行されます。

Avira製品は、Windows Vistaでのいくつかのアクションに管理者権限を必要とします。
これらのアクションには、次の記号が付いています。 
このシンボルがボタン上にも表されている場合、このアクションの実行には管理者権限が必要です。 現在のユーザー アカウントに管理者権限がないと、Windows
Vistaのユーザー アカウント
コントロールのダイアログで、管理者パスワードを入力するように要求されます。
管理者パスワードがないと、このアクションは実行できません。

2.3 ライセンスとアップグレード

2.3.1 使用許諾

Avira を使用するには、ライセンスが必要です。 ライセンス条件を受け入れます。

ライセンスが、アクティベーション コードという形で提供されます。
アクティベーション コードとは、Avira
製品の購入後にユーザーが受け取る、数字とアルファベットで構成されたコードです。

アクティベーション
コードには、プログラムの使用許諾の有効期間に関する正確なデータが含まれています。

Avira 製品を、インターネットで購入した場合、アクティベーション
コードは、電子メールで送信されます。あるいは製品パッケージに表示されています。

プログラムをライセンス化するため、アクティベーション
コードを入力して、プログラムを有効にします。
インストール中に、製品の有効化を実行することができます。
しかし、インストール後、ライセンス マネージャで Avira
製品を有効にすることもできます（**ヘルプ > ライセンス管理**）。

2.3.2 ライセンスの延長

ライセンスの期限切れが近づくと、Avira
から、ライセンスの延長をお知らせするスライドアップが届きます。
これを実行するには、リンクをクリックするだけで、Avira
オンラインショップに移動できます。 しかし、**[ヘルプ] > [ライセンス管理]**
で、ライセンス マネージャで Avira 製品のライセンスを延長することもできます。

Avira のライセンス ポータルで登録された場合、**[ライセンス概要]**
で直接ライセンスを延長するか、ライセンスの自動更新を選択することもできます。

2.3.3 アップグレード

ライセンス マネージャで、Avira
デスクトップ製品シリーズから、製品のアップグレードを起動することもできます。
古い製品の手動アンインストールや新製品の手動インストールは、必要ありません。
ライセンス
マネージャでアップグレードを行う場合、アップグレードする製品のアクティベーション
コードを、ライセンス マネージャの入力ボックスに入力します。
新製品は、自動的にインストールされます。

コンピュータの高い信頼性、安全性を確保するため、Avira
は、システム新バージョンへのアップグレードを通知するポップアップ
アイテムを送信します。 ポップアップ
アイテムの**アップグレード**リンクをクリックすると、製品のアップグレード
サイトにリンクします。

製品のアップグレード、またはより包括的な製品へのアップグレードが可能です。
製品概要ページでは、現在使用しているプログラムの種類が表示され、他の Avira
製品と比較することができます。
製品名の右隣の**情報**アイコンをクリックして、詳細情報をご覧ください。
現在の製品の使用を継続する場合は、**アップグレード**をクリックし、新しいバージョン
のダウンロードを開始してください。
より包括的な製品を入手したい場合は、製品欄の下部にある**購入**ボタンをクリックします
。 製品の注文が可能な Avira オンライン ショップへ、自動的に転送されます。

> 注意
> 製品、オペレーティング
> システムによっては、アップグレードを実行する際に、管理者権限を必要とす
> る場合もあります。
> アップグレードを実行する前に、管理者としてログインします。

2.3.4 ライセンス マネージャ

Avira Antivirus Premium ライセンス マネージャを使用すると、Avira Antivirus
Premium ライセンスを簡単にインストールすることができます。

Avira Antivirus Premium ライセンス マネージャ

ダブルクリックで、ファイル
マネージャ、またはアクティベーション電子メールのライセンス
ファイルを選択し、スクリーンの指示に従ってライセンスをインストールします。

注意

Avira Antivirus Premium
ライセンスマネージャは、関連する製品フォルダに対応するライセンスを自動的にコピーします。 ライセンスが既に存在する場合は、既存のライセンス
ファイルを変更するかどうかを確認するメッセージが表示されます。
この場合、既存のファイルは、新規ライセンス
ファイルにより上書きされます。

3. インストールとアンインストール

この章には、Avira
製品インストールとアンインストールに関する情報が記載されています。

- 参照：章プレ セットアップ要件、インストールのためのコンピュータの準備
- 参照：章エクスプレス インストール：既定の設定による標準インストール
- 参照：章カスタム インストール：設定可能なインストール
- 参照：章テスト製品のインストール
- 参照：章環境設定ウィザード
- 参照：章インストールの変更
- 参照：章インストール モジュール
- 参照：章アンインストール：アンインストール

3.1 インストールの種類

インストール中、インストール
ウィザードで、セットアップの種類を選択することができます。

高速

- *C:¥Program Files* の既定のフォルダに、プログラム ファイルはインストールされます。
- Avira 製品は、既定の設定でインストールされます。
  環境設定ウィザードを使用してカステム設定を定義することができるオプションもあります。

カスタム

- 個々のプログラム
  コンポーネントをインストールするために選択することができます（参照：章インストールとアンインストール > インストール モジュール）。

- プログラム ファイルのインストール先フォルダを選択することができます。
- **スタートメニューで、デスクトップ アイコンの作成とプログラム グループの作成**を無効にすることができます。
- 環境設定ウィザードで、Avira 製品のカスタム設定を定義し、インストール後に自動的に実行されるショートスキャンを開始することができます。

3.2 プレ セットアップ

> 注意
> インストール前に、コンピュータがシステム要件を満たしているかどうか確認してください。 コンピュータが全ての要件を満たしている場合は、Avira 製品をインストールすることができます。

プレ セットアップ

✓ 電子メール プログラムを閉じます。
全ての作動中のアプリケーションを終了することをお勧めします。

✓ 他のアンチウイルス ソリューションがインストールされていないことを確認してください。
様々なセキュリティ ソリューションの自動保護機能が、相互に干渉する可能性があります。

↳ 互換性のないソフトウェアがコンピュータに存在していないかどうか、Avira 製品が検索します。

↳ 互換性がない可能性があるソフトウェアが検出された場合、Avira は、これらのプログラムのリストを生成します。

↳ コンピュータの安定性を確保するためにも、これらのプログラムの削除をお勧めします。

▸ コンピュータから自動的に削除するプログラムのチェックボックスを、リストで選択し、**次へ**をクリックします。

- プログラムのアンインストールを、手動で確定する必要があります。
  プログラムを選択し、**次へ**をクリックします。
  - ↪ 選択したプログラムをアンインストールすると、コンピュータを再起動する必要があります。 再起動後、インストールが続行します。

警告
Avira
製品のインストールが完了するまで、コンピュータは保護されていない状態になります。

インストール

インストール プログラムは、わかりやすいダイアログ モードで実行されます。
全てのウィンドウに、インストール
プロセスを制御するボタンの選択が含まれています。

最も重要なボタンには、次の機能が割り当てられています：

- **OK**：アクションを確定します。
- **中止**：アクションを中止します。
- **次へ**：次の手順に進みます。
- **戻る**：前の手順に戻ります。
  - インターネット接続の確立：次のインストール手順を実行するには、インターネット接続が必要です。
    - インストール プログラムを介した、プログラム ファイル、スキャン エンジン、最新のウイルス定義ファイルのダウンロード（インターネット ベースのインストールの場合）
    - プログラムの有効化
    - インストール完了後のアップデートの実行（必要に応じて）

- プログラムを有効にする時のために、Avira 製品アクティベーション コード、またはライセンス ファイルは、適切に保管してください。

注意

インターネット基盤のインストール：
インターネットを基盤とするプログラムのインストールのために、Avira ウェブサーバーによるインストールの前に、プログラム ファイルを読み込むインストール プログラムが用意されています。最新のウィルス定義ファイルと共に Avira 製品がインストールされることを、このプロセスが保証します。

インストールとインストール パッケージ：
インストール パッケージには、インストール プログラムと全ての必要なプログラム ファイルが含まれています。インストール パッケージを使用したインストールでは、言語を選択することはできません。
インストール完了後に、ウィルス定義ファイルを更新することをお勧めします。

注意

製品の有効化の際、Avira 製品は、Avira サーバーと通信するために、HTTP プロトコルと Port 80（ウェブ通信）、および暗号化プロトコル SSL とポート 443 を使用します。
ファイアウォール(FireWall)を使用している場合、必要な接続や受信または送信データがファイアウォールで制止されていないことを確認してください。

3.3 高速インストール

Avira 製品のインストール：

インターネットでダウンロードしたインストール
ファイルをダブルクリックするか、プログラム CD を挿入してインストール
プログラムを開始します。

インターネット ベースのインストール

↳ **ようこそ** 画面が表示されます。

- **次へ** をクリックし、インストールを続行します。

  ↳ **言語選択** ダイアログが表示されます。

- Avira 製品のインストールに使用する言語を選択し、**次へ**
  をクリックして言語選択を確定します。

  ↳ **ダウンロード** ダイアログ ボックスが表示されます。
  インストールに必要なファイルはすべて Avira ウェブ
  サーバーからダウンロードされます。
  ダウンロードが完了した後で、**ダウンロード** ウィンドウが閉じます。

インストール パッケージを使用したインストール

↳ **インストールの準備** ウィンドウが表示されます。

↳ インストール ファイルが抽出されます。 インストール ルーチンが開始します。

↳ **インストールの種類の選択** ダイアログ ボックスが表示されます。

> 注意
> 既定高速インストールがプレセットされます。
> 環境設定しないであろう全ての標準コンポーネントがインストールされます。
> カスタム インストールを実行する場合は、インストールとアンインストール > カスタム インストールの章を参照してください。

- デフォルトにより、**Avira Proactiv と Protection Cloud を使用して保護を高める** チェックボックス（設定 > 一般 > 高度な保護）が予め設定されています。 Avira Community への参加を希望しない場合は、このボックスのチェックマークを外してください。

  ↳ Avira Community への参加を確定すると、検知された不審なプログラムのデータが Avira により Avira Malware Research Center に送信されます。 このデータは高度なオンライン スキャンおよび検知技術の開発と改善のためにのみ利用されます。 **ProActiv** および **Protection Cloud** のリンクをクリックすると、拡張されたオンライン スキャンおよびクラウド スキャンに関する詳細情報が取得できます。

- **エンドユーザー使用許諾契約**に同意することを確定します。 **エンドユーザー使用許諾契約**の詳細な内容を読むには、リンクをクリックしてください。

  ↳ **ライセンス ウィザード**が開き、製品のアクティベーションをお手伝いします。

  ↳ ここで、プロキシ サーバーを設定することができます。

- 必要に応じて、**プロキシ設定** をクリックして設定を行い、**OK** をクリックして設定を確定します。

- すでにアクティベーション コードを受け取っている場合は、**製品のアクティベーションを行う** を選択し、アクティベーション コードを入力します。

  または

- アクティベーション コードがない場合は、**アクティベーションコードを購入する** リンクをクリックします。

  ↳ Avira の Web サイトに転送されます。

あるいは、**有効なライセンス ファイルをすでに持っている**
リンクをクリックします。

↳ **ファイルを開く ダイアログ**が表示されます。

- お持ちの *.KEY* ライセンス ファイルを選択し、**開く** をクリックします。

  ↳ アクティベーション コードが、ライセンス ウィザードにコピーされます。

- 製品の試用を行う場合は、製品インストールのテストの章をお読みください。
- **次へ** をクリックします。

  ↳ インストールの進行状況は、グリーンのバーで表示されます。

- **次へ** をクリックします。

  ↳ **Avira SearchFree をすでに使用している数百万人の Avira ユーザーの一員となる** ダイアログ ボックスが表示されます。

- Avira SearchFree Toolbarのインストールを希望しない場合は、Avira SearchFree Toolbarと Avira SearchFree
  アップデータの**使用許諾契約書**のチェックボックス、そして**Avira SearchFree（search.avira.com）**をブラウザー
  ホームページに定義するというチェックボックスのマークを外してください。

> 注意
> 必要であれば、Avira SearchFree Toolbarをインストールする前に、以前にインストールした検索ツールバーをアンインストールします。 そうしないと、Avira SearchFree Toolbarがインストールできない場合があります。

- **次へ** をクリックします。

  ↳ Avira SearchFree Toolbar のインストールの進行状況は、グリーンのバーで表示されます。

  ↳ Avira トレイ アイコンは、タスクバーに配置されています。

↳ コンピュータを効率的に保護するために、**アップデータ**が可能な更新を検索します。

↳ **Luke Filewalker** ウィンドウが開き、ショート システム スキャンが実行されます。 スキャンの状況、結果が表示されます。

- スキャン後、再起動を要求するメッセージが表示された場合は、確実にシステムを保護するために、**はい**をクリックしてください。

インストール完了後、コントロール センターのステータスフィールドで、プログラムが最新の状態かどうか、確認することをお勧めします。

- Avira 製品が、コンピュータが危険な状態にあることを示唆するメッセージを表示した場合は、**問題を修正**をクリックします。

  ↳ **保護の復元**というダイアログが開きます。

- 事前設定したオプションを有効にして、システムの安全性を確保します。
- 必要に応じて、その後、完全システム スキャンを実行します。

3.4 カスタム インストール

Avira 製品のインストール：

インターネットでダウンロードしたインストール ファイルをダブルクリックするか、プログラム CD を挿入してインストール プログラムを開始します。

インターネット ベースのインストール

↳ **ようこそ** 画面が表示されます。

- **次へ** をクリックし、インストールを続行します。

  ↳ **言語選択** ダイアログが表示されます。

- Avira 製品のインストールに使用する言語を選択し、**次へ**
  をクリックして言語選択を確定します。

  ↳ **ダウンロード** ダイアログ ボックスが表示されます。
  インストールに必要なファイルはすべて Avira ウェブ
  サーバーからダウンロードされます。
  ダウンロードが完了した後で、**ダウンロード** ウィンドウが閉じます。

インストール パッケージを使用したインストール

↳ **インストールの準備** ウィンドウが表示されます。

↳ インストール ファイルが抽出されます。 インストール ルーチンが開始します。

↳ **インストールの種類の選択** ダイアログ ボックスが表示されます。

> 注意
> 既定高速インストールがプレセットされます。
> 環境設定しないであろう全ての標準コンポーネントがインストールされます。
> 高速インストールの実行を希望する場合は、インストールとアンインストール > 高速インストールを必ず参照してください。

- 個々のプログラム
  コンポーネントをインストールするには、**カスタム**を選択してください。
- **Avira Proactiv と Protection Cloud を使って保護を強化したい**というチェック
  ボックスは、規定でプレセットされています。 Avira
  コミュニティへの参加を希望しない場合は、チェック
  ボックスのマークを外してください。

  ↳ Avira Community
  への参加を確定すると、検知された不審なプログラムのデータが Avira により
  Avira Malware Research Center に送信されます。
  このデータは高度なオンライン
  スキャンおよび検知技術の開発と改善のためにのみ利用されます。 **ProActiv**

および **Protection Cloud** のリンクをクリックすると、拡張されたオンラインスキャンおよびクラウド スキャンに関する詳細情報が取得できます。

- **エンドユーザー使用許諾契約**に同意することを確定します。
  エンドユーザー使用許諾契約の詳細な内容を読むには、リンクをクリックしてください。
- **次へ** をクリックします。
  - ↳ **ターゲット フォルダの選択**ウィンドウが開きます。
  - ↳ 既定フォルダは、*C:¥Program Files¥Avira¥AntiVir Desktop¥* です。
- **次へ**をクリックして、続行します。

  または

  ブラウザボタンで異なるターゲット
  フォルダを選択し、**次へ**をクリックして確定します。
  - ↳ **コンポーネント ダイアログをインストール**と表示されます。
- リストから選択、除外し、**次へ**で確定しプロセスを進めます。
- **Protection Cloud**
  コンポーネントのインストールを選択したものの、クラウドで分析するためにファイルを送信する際、手動での確定を希望する場合は、**Avira への不審ファイル送信時の手動による確定**オプションを有効化します。
- **次へ** をクリックします。
- 次のダイアログ ボックスで、デスクトップ ショートカットやプログラム
  グループを**スタートメニュー**に作成するかどうか、決めることができます。
- **次へ** をクリックします。
  - ↳ **ライセンス ウィザード**が開きます。

プログラムを有効化するには、次のオプションがあります。

- アクティベーション コードを入力します。

↳ ライセンスで有効となる Avira 製品のアクティベーション
コードを入力します。

- アクティベーション コードがない場合は、**アクティベーションコードを購入する**リンクをクリックします。

  ↳ Avira の Web サイトに転送されます。

- オプション**テスト製品**を選択します。

  ↳ **テスト製品**を選択すると、有効化プロセス中に、プログラムを有効にするための評価版ライセンスが生成されます。 Avira
  製品の機能全般を一定期間テストすることができます。 (テスト製品のインストール参照)。

注意

オプション**既に有効なライセンス ファイルを持っている**で、有効なライセンス
ファイルをロードすることができます。 有効なアクティベーション
コードで製品を有効化すると、ライセンス キーが生成され、Avira
製品のプログラム ディレクトリに保存されます。
製品を既に有効化しており、Avira
製品を再インストールしたい場合に、このオプションを使用してください。

注意

Avira 製品の販売バージョンの中には、製品にアクティベーション
コードが含まれているものがあります。
そのため、有効化の入力の必要がありません。
必要な場合は、アクティベーション コードがライセンス
ウィザードに表示されます。

注意
プログラムを有効にするため、Avira サーバーへ接続します。
プロキシ設定で、プロキシ サーバーによるインターネット
リンクを設定することができます。

- 有効化プロセスを選択し、**次へ**をクリックして確定します。
- 有効なライセンス
  ファイルを所有している場合、ディレクトリのチャプター「オプションの選択 *既に有効なライセンスを持っている*」へ移動します。

製品の有効化

→ 個人情報を入力することができるダイアログ ボックスが開きます。

- データを入力し、**次へ**をクリックします。

  → Avira サーバーにデータが転送され、スキャンされます。
  ライセンスにより、Avira 製品が有効化されます。

  → ライセンス データが次のウィンドウで表示されます。

- **次へ** をクリックします。
- 「オプションの選択 *既に有効なライセンスを持っている*」へとスキップします。

オプション「既に有効なライセンスを持っている」を選択します。

→ ライセンス ファイルをロードするためのボックスが開きます。

- キー ライセンス ファイルとプログラムのためのライセンス
  データを選択し、**開く**をクリックします。

  → ライセンス データが次のウィンドウで表示されます。

- **次へ** をクリックします。

有効化完了後、継続、もしくはライセンス ファイルをロードします。

→ **Avira SearchFree をすでに使用している数百万人の Avira ユーザーの一員となる** ダイアログ ボックスが表示されます。

- Avira SearchFree Toolbarのインストールを希望しない場合は、Avira SearchFree Toolbarと Avira SearchFree アップデータの**使用許諾契約書**のチェックボックス、そして**Avira SearchFree（search.avira.com）**をブラウザー ホームページに定義するというチェックボックスのマークを外してください。

> 注意 必要であれば、Avira SearchFree Toolbarをインストールする前に、以前にインストールした検索ツールバーをアンインストールします。 そうしないと、Avira SearchFree Toolbarがインストールできない場合があります。

- **次へ** をクリックします。

→ Avira SearchFree Toolbar のインストールの進行状況は、グリーンのバーで表示されます。

→ **インストール ウィザード**が閉じ、**環境設定ウィザード**が開きます。

3.5 テスト製品のインストール

Avira 製品のインストール：

インターネットでダウンロードしたインストール ファイルをダブルクリックするか、プログラム CD を挿入してインストール プログラムを開始します。

インターネット ベースのインストール

→ **ようこそ** 画面が表示されます。

- **次へ** をクリックし、インストールを続行します。

↳ **言語選択** ダイアログが表示されます。

- Avira 製品のインストールに使用する言語を選択し、**次へ** をクリックして言語選択を確定します。

  ↳ **ダウンロード** ダイアログ ボックスが表示されます。
  インストールに必要なファイルはすべて Avira ウェブ サーバーからダウンロードされます。
  ダウンロードが完了した後で、**ダウンロード** ウィンドウが閉じます。

インストール パッケージを使用したインストール

↳ **インストールの準備** ウィンドウが表示されます。

↳ インストール ファイルが抽出されます。 インストール ルーチンが開始します。

↳ **インストールの種類の選択** ダイアログ ボックスが表示されます。

> 注意
> **既定高速インストール**がプレセットされます。
> 環境設定しないであろう全ての標準コンポーネントがインストールされます。
> カスタム
> インストールの実行を希望する場合は、インストールとアンインストール > カスタム インストールを参照してください。

- デフォルトにより、**Avira Proactiv と Protection Cloud を使用して保護を高める** チェックボックス（設定 > 一般 > 高度な保護）が予め設定されています。 Avira コミュニティへの参加を希望しない場合は、チェック ボックスのマークを外してください。

  ↳ Avira Community への参加を確定すると、検知された不審なプログラムのデータが Avira により Avira Malware Research Center に送信されます。
  このデータは高度なオンライン スキャンおよび検知技術の開発と改善のためにのみ利用されます。 **ProActiv**

および **Protection Cloud** のリンクをクリックすると、拡張されたオンラインスキャンおよびクラウド スキャンに関する詳細情報が取得できます。

- **エンドユーザー使用許諾契約**に同意することを確定します。
  エンドユーザー使用許諾契約の詳細な内容を読むには、リンクをクリックしてください。
- **次へ** をクリックします。
  - ↪ **ライセンス ウィザード**が開き、製品のアクティベーションをお手伝いします。
  - ↪ ここで、**プロキシ サーバー**を設定することができます。
- 環境設定の**プロキシ設定**をクリックし、**OK** で確定します。
- ライセンス
  ウィザードの**テスト製品**というオプションを選択し、**次へ**をクリックします。
- **登録***フィールドの入力必須欄にデータを入力してください。* **Avira Newsletter** の配信を希望するかどうか決定し、**次へ**をクリックします。
  - ↪ インストールの進行状況は、グリーンのバーで表示されます。
  - ↪ **Avira SearchFree Toolbarを使用している Avira ユーザーに参加**というダイアログ ボックスが表示されます。
- Avira SearchFree Toolbarのインストールを希望しない場合は、Avira SearchFree Toolbarと Avira SearchFree アップデータの**使用許諾契約書**のチェックボックス、そして**Avira SearchFree（search.avira.com）**をブラウザー ホームページに定義するというチェックボックスのマークを外してください。

> 注記
> 必要に応じて、Avira SearchFree Toolbarをインストールする前に既存の旧検索ツールバーをアンインストールしてください。 そうしないと、Avira SearchFree Toolbarがインストールできない場合があります。

- **次へ** をクリックします。
  - ↳ Avira SearchFree Toolbar のインストールの進行状況は、グリーンのバーで表示されます。
- Avira を有効にするための、システムの再起動を指示するメッセージが表示されます。**はい**をクリックして、コンピュータを再起動します。
  - ↳ Avira トレイ アイコンは、タスクバーに配置されています。
  - ↳ 評価ライセンスは、31 日間有効です。

3.6 環境設定ウィザード

ユーザー定義インストールの最後に、環境設定ウィザードが開きます。
環境設定ウィザードでは、Avira 製品のカスタム設定を定義することができます。

- 環境設定ウィザードのウェルカム ウィンドウにある**次へ**をクリックして、プログラムの環境設定を開始します。
  - ↳ ダイアログ ボックス **AHeAD の環境設定**で、AHeAD テクノロジの検出レベルを選択することができます。選択した検出レベルは、System Scanner（オンデマンド スキャン）および Real-Time Protection（オンアクセス スキャン）の AHeAD テクノロジ設定に使用されます。
- 検出レベルを選択し、**次へ**をクリックしてインストールを続行します。
  - ↳ 次のダイアログ ボックス **脅威カテゴリ（拡張）の選択**では、Avira 製品の保護機能を、特定の脅威カテゴリに適合させることができます。
- 必要に応じて、他の脅威カテゴリをアクティブにし、**次へ**をクリックしてインストールを続行します。
  - ↳ Avira Real-Time Protection のインストール モジュールを選択した場合、**Real-Time Protection 開始モード**というダイアログ ボックスが表示されます。 Real-Time Protection の開始時間を規定することができます。

コンピュータが再起動される度に、指定した起動モードで Real-Time Protection が起動します。

> 注意
> 指定した Real-Time Protection の起動モードは、レジストリに保存されます。環境設定で変更することはできません。

> 注意
> Real-Time Protection の既定の起動モード（通常スタート）を選択し、スタート アップのログオン プロセスを迅速に実行している場合、スタート アップスで自動開始に設定されているプログラムは、キャンされない可能性があります。これは、Real-Time Protection が完全に開始する前に、プログラムが開始するためです。

- 必要なオプションを有効にし、**次へ**をクリックして設定を続行します。
  - ↳ 次の**システム スキャン** ダイアログ ボックスでは、簡易システム スキャンを有効、無効にすることができます。 簡易システム スキャンは、設定が完了した後からコンピュータが再起動されるまでの間に、実行中のプログラムおよび重要なシステム ファイルを対象にウィルスおよびマルウェアのスキャンを実行します。
- **簡易システム スキャン**
  オプションを有効または無効にし、**次へ**をクリックして設定を続行します。
  - ↳ 次のダイアログ ボックスでは、**終了**をクリックして設定を完了できます。
  - ↳ 指定および選択した設定が受け入れられます。
  - ↳ **簡易システム スキャン** オプションを有効にしている場合、 **Luke Filewalker** ウィンドウが開きます。 Scanner が、簡易システム スキャンを実行します。

- スキャン後の再起動を要求するメッセージが表示された場合は、確実にシステムを保護するために、**はい**をクリックしてください。

インストール完了後、**コントロール センター**
フィールドの**ステータス** で、プログラムが更新されているかどうか、確認することをお勧めします。

- Avira
  製品が、コンピュータが危険な状態にあることを示唆するメッセージを表示した場合は、**問題を修正**をクリックします。
  - ↳ **保護の復元**というダイアログが開きます。
- 事前設定したオプションを有効にして、システムの安全性を確保します。
- 必要に応じて、その後、完全システム スキャンを実行します。

3.7 インストールの変更

現在の Avira 製品インストールの個々のプログラム
コンポーネントを追加、または削除することができるオプションがあります（参照：章 インストールとアンインストール > インストール モジュール）。

現在のインストールにモジュールを追加、またはインストールからモジュールを削除したい場合は、**Windows コントロール**
パネルで、プログラムを**変更／削除**するためのオプション**プログラムの追加と削除**を使用することができます。

該当する Avira 製品を選択し、**変更**をクリックします。 プログラムの**ウェルカム**
ダイアログで、オプション**修正**を選択します。
インストールの変更中は、手順が表示されます。

3.8 インストール モジュール

ユーザー定義のインストール、または変更のインストールでは、次のインストール
モジュールを選択、追加、削除することができます。

- **Avira Antivirus Premium**
  このモジュールには、Avira
  製品の正常なインストールに必要な全てのコンポーネントが含まれています。
- **Real-Time Protection**
  Avira Realtime は、バックグランドで作動します。 オンアクセス
  モードで、開く、書き込む、コピーなどの操作中に、ファイルを監視、必要に応じて修復します。
  ユーザーがファイル操作（文書の読み込み、実行、コピーなど）を実行するたびに、Avira 製品が自動的にファイルをスキャンします。 ファイル名を変更すると、Avira Real-Time Protection のスキャンは実行されません。
- **Mail Protection**
  Mail Protection は、コンピュータと、電子メール プログラム（メール
  クライアント）が電子メールをダウンロードする電子メール
  サーバーの間のインターフェイスです。 Mail Protection は、電子メール
  プログラムと電子メール サーバー間のプロキシとして接続されています。
  全ての受信メールは、このプロキシを経由し、ウィルスと不要プログラムのスキャンが実行されます。そして、それらの受信メールは、電子メール
  プログラムに転送されます。
  環境設定によって、感染した電子メールを、プログラムが自動的に処理するか、あるいは特定のアクションをユーザーに確認します。
- **Rootkits Protection**
  Avira Rootkits Protection は、通常のマルウェア対策では、コンピュータ
  システム侵入後に検出することができないソフトウェアが、コンピュータにインストールされているかどうかを確認します。
- **ProActiv**
  ProActiv
  コンポーネントは、アプリケーションのアクションを監視します。不審な動きがあった場合は、アラートを発し、ユーザーに通知します。
  この動きを認識する機能により、不明なマルウェアに対する保護が可能になります。
  ProActiv コンポーネントは、Avira Real-Time Protection に統合されています。

- **Protection Cloud**
  Protection Cloud コンポーネントは、不明なマルウェアのダイナミック
  オンライン検出のためのモジュールです。
- **Web Protection**
  インターネット サーフィン中、ウェブ
  サーバーからのデータをリクエストするために、ウェブ
  ブラウザが使用されています。 ウェブ サーバーから転送されるデータ（HTML
  ファイル、スクリプトと画像ファイル、Flash
  ファイル、動画と音楽ストリーム等）は、通常、ウェブ
  ブラウザで表示するために、ブラウザのキャッシュに直接移動されます。そのため、A
  vira Real-Time Protection によるオンアクセス
  スキャンを実行することはできません。
  これにより、ウィルスや不要プログラムが、コンピュータ
  システムにアクセスする可能性があります。 Web Protection は、HTTP
  プロキシで、データ転送に使用されるポート（80、8080、3128）を監視し、転送さ
  れたデータをスキャンしてウィルスや不要プログラムを検出します。
  設定によって、プログラムが感染したファイルを自動的に処理するか、ユーザーに特
  定のアクションを実行するよう指示する場合があります。
- **Shell Extension**
  Shell Extension は、Windows エクスプローラのコンテキスト メニュー（右マウス
  ボタン）に、**Avira で選択したファイルをスキャン**というエントリを生成します。
  このエントリで、ファイルまたはディレクトリを、直接スキャンすることができます
  。

3.9 アンインストール

コンピュータから Avira 製品を削除するには、Windows コントロール
パネルでプログラムを**変更／削除**するためのオプション**プログラムの追加と削除**を使用
することができます。

Avira 製品をアンインストールする方法（例：Windows 7）：

- Windows **スタートメニューのコントロール パネル**を開きます。

- **プログラムおよび機能** をダブルクリックします。
- リストから、該当する Avira 製品を選択し、**アンインストール**をクリックします。
  - ↳ プログラムの削除を確認するメッセージが表示されます。
- **はい**をクリックして、確定します。
  - ↳ プログラムの全てのコンポーネントが削除されます。
- **完了**をクリックして、アンインストールを完了します。
  - ↳ コンピュータの再起動を推奨するダイアログボックスが表示される場合もあります。
- **はい**をクリックして、確定します。
  - ↳ Avira 製品がアンインストールされました。コンピュータを再起動した時には、プログラムの全ディレクトリ、ファイル、レジストリのエントリが削除されているはずです。

注意

Avira SearchFree Toolbar は、アンインストールプログラムに含まれていません。そのため、上記の手順に従い、個別にアンインストールしてください。 Firefox でこの操作を行う場合は、Add-On Manager で Avira SearchFree Toolbar を無効にする必要があります。アンインストール後、ウェブ ブラウザに検索バーはありません。

4. Avira Antivirus Premiumの概要

この章には、Avira 製品の機能と操作に関する概要が記載されています。

- 参照：章 ユーザー インターフェイスと操作
- 参照：章 Avira SearchFree Toolbar
- 参照：章 How to...?

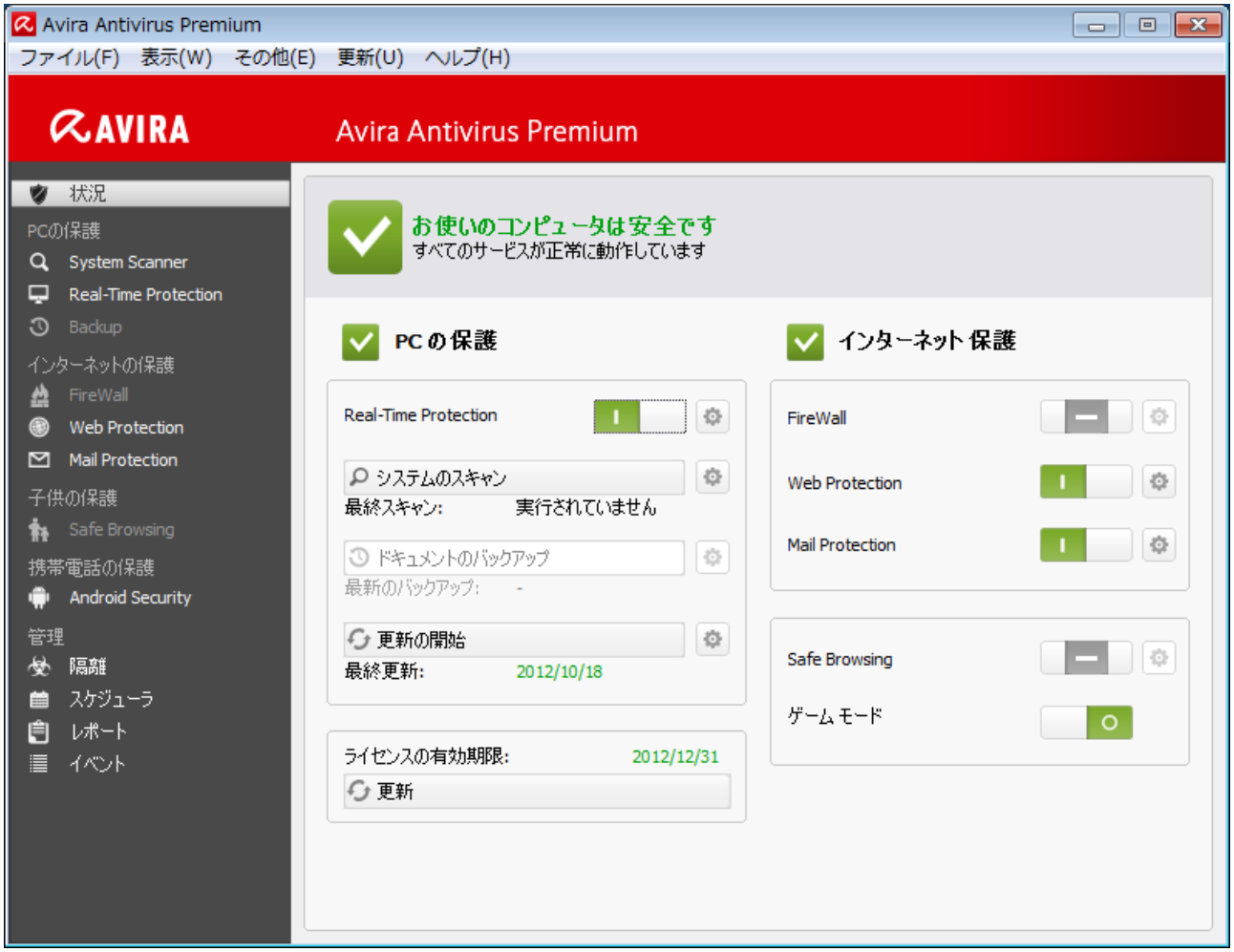
4.1 ユーザー インターフェイスと操作

3 種類のインターフェイス エレメントを介して、Avira 製品を操作します。

- コントロール センター：Avira 製品の監視および制御
- 環境設定：Avira 製品の環境設定
- トレイ アイコン（タスクバーのシステム トレイ）：コントロール センターおよび他の機能の操作

4.1.1 コントロール センター

コントロール センターは、コンピュータ システムの保護ステータスを監視し、Avira 製品の保護コンポーネントと機能を制御および操作するために設計されています。



コントロール センターのウィンドウは、メニュー バー、ナビゲーション エリア、およびステータスの詳細ウィンドウという 3 つの領域に分割されています。

- メニュー バー：コントロール センターのメニュー バーで、一般的なプログラムの機能と情報にアクセスできます。
- ナビゲーション領域：ナビゲーション領域では、コントロール センターの個々のセクションを簡単に切り替えることができます。個々のセクションには、プログラム コンポーネントの情報と機能が含まれており、作業内容ごとにナビゲーション バーに配置されています。 例：作業内容 *PC PROTECTION* - 選択 **Real-Time Protection**.
- ステータス：コントロール センターを開くと、ステータスが表示されます。一目でコンピュータの保護状況を確認することができ、有効なモジュールの概要、バックアップ、システム

スキャンの最終実行日などを見ることができます。
ステータス表示には、機能、操作を開始することができるボタンがあります（例：**Real-Time Protection** のスタート／ストップ）。

コントロール センターの開始と終了

コントロール センターを開始するには、次のオプションがあります。

- デスクトップのプログラム アイコンをダブルクリック
- **スタート > プログラム**プログラムのエントリ
- Avira 製品のトレイ アイコン

ファイルメニューの**閉じる**コマンドでコントロール センターを閉じるか、コントロール センターの「閉じる」タブをクリックします。

コントロール センターの操作

コントロール センターの移動

- ナビゲーション バーで作業内容を選択します。
  - ↪ 作業内容が開き、他のセクションが表示されます。
    作業内容の最初のセクションが選択され、表示されます。
- 必要に応じて別のセクションをクリックして、詳細ウィンドウを表示します。

> 注意
> メニュー バーのキーボード ナビゲーションは、**[Alt]** キーで有効にします。ナビゲーションを有効にすると、**矢印**キーでメニュー内を移動することができます。 **Return**キーで、有効なメニュー項目を起動します。
> コントロール
> センターのメニューの表示／非表示を切り替えたり、メニュー内を移動したりするには、次のようなキーの組み合わせを利用することができます。**[Alt]** +
> メニュー コマンドの下線付きの文字、あるいはメニュー
> コマンドを押してください。 メニュー、メニュー

コマンド、またはサブメニューにアクセスするには、[**Alt**]
キーを押したままにします。

詳細ウィンドウに表示されたデータやオブジェクトの処理：

- 編集するデータ、またはオブジェクトをハイライト表示します。

  複数の要素（列の要素）をハイライト表示するには、**Control** キー、または **Shift** キーを押したままにして、要素を選択します。

- 詳細ウィンドウの上部バーで適切なボタンをクリックして、オブジェクトを編集します。

コントロール センターの概要

- **ステータス**：ステータスバーをクリックすると、製品の機能や性能に関する概要が表示されます（参照ステータス）。
  - **ステータス**セレクションでは、一目で、有効なモジュール、最終の更新に関する情報を見ることができます。
- *PC PROTECTION*：このセクションでは、コンピュータシステムのファイルに存在するウィルスやマルウェアをチェックするコンポーネントを見つけることができます。
  - System Scanner セクションでは、オンデマンドスキャンの設定と開始を簡単に行うことができます。
    事前に設定済みのプロファイルを使用すると、調整済みの既定のオプションでスキャンを実行できます。
    手動による選択（保存されません）またはユーザー定義のプロファイルを作成して、個々の要件に合わせて、ウィルスや不要プログラムに対するスキャンを調整することもできます。
  - Real-Time Protection
    セクションには、スキャンしたファイルに関する情報とその他の統計データが表示されます。これらはいつでもリセットすることができ、またレポートファイルへのアクセスを可能にします。

最後に検出されたウイルスまたは不要プログラムに関する詳細情報は、「ボタンを押す」だけで取得できます。

- *INTERNET PROTECTION*：このセクションでは、コンピュータシステムをインターネットのウィルスやマルウェア、不正なネットワークアクセスから保護するためのコンポーネントが、提供されています。
  - Web Protection セクションには、スキャンされた URL と検出されたウイルスに関する情報、その他の統計データが表示されます。これらはいつでもリセットすることができ、レポートファイルへのアクセスを可能にします。
    最後に検出されたウイルスまたは不要プログラムに関する詳細情報は、「ボタンを押す」だけで取得できます。
  - Mail Protection セクションには、Mail Protection によりスキャンされた電子メール、そのプロパティ、およびその他の統計データが表示されます。
- *CHILD PROTECTION*：このセクションには、子供が安全にインターネットを使用できる環境を確保するためのコンポーネントが用意されています。
- *MOBILE PROTECTION*：このセクションから、Android デバイスへのオンラインアクセスにリダイレクトします。
  - Avira Free Android Security は、全ての Android 基盤デバイスを管理します。
- *管理*：このセクションでは、疑わしいファイルや感染したファイルを分離して管理したり、定期的なタスクの計画を行うためのツールを使用することができます。
  - 隔離セクションには、いわゆる隔離マネージャがあります。すでに隔離に配置されたファイルや、隔離に配置したい疑わしいファイルのための、セントラル ポイントです。 選択したファイルを電子メールで Avira Malware Research Center に送信することもできます。
  - スケジューラセクションでは、スケジュールされたスキャンと更新ジョブの設定、バックアップ ジョブ、および既存のジョブの調整、または削除が可能です。
  - 報告セクションでは、実行されたアクションの結果を表示できます。

- イベントセクションでは、特定のプログラム
  モジュールによって生成されるイベントを表示することができます。

4.1.2 ゲーム モード

コンピュータ システムにて、フル スクリーン
モードでアプリケーションが実行されている場合、ゲーム
モードを有効にすることで、ポップアップ
ウィンドウや製品メッセージなどのデスクトップ通知を、意図的に停止することができます。

ゲームモードおよびその自動モードは、**ON／OFF**
ボタンをクリックして、有効、無効の操作を行います。 既定では、ゲーム
モードは、**自動**に設定されており、グリーンで表示されます。
既定の設定では、自動機能が設定されており、フル スクリーン
モードを必要とするアプリケーションを実行する度に、Avira 製品は自動的にゲーム
モードに切り替わります。

▸ **OFF** ボタンの左隣のボタンで、ゲーム モードを有効にします。

↳ ゲーム モードが有効になり、イエローで表示されます。

> 注意
> ネットワーク
> イベントおよび可能な脅威に関するデスクトップ通知、警告を受信することができないため、フル スクリーン認識モードの既定の設定 **OFF**
> を一時的に変更することをお勧めします。

4.1.3 環境設定

環境設定で、Avira 製品の設定を定義することができます。 インストールされた Avira 製品は、コンピュータ
システムをしっかりと保護するために、標準設定で設定されています。

しかし、コンピュータ システムもしくは Avira
製品の特殊要件に合わせ、プログラムの保護コンポーネントを調整する必要があります。

環境設定のダイアログ ボックスを開きます。**OK** もしくは
適用ボタンで、環境設定を保存することができます。キャンセル
ボタンをクリックすると設定を削除することができます。**既定値**ボタンで、既定の設定を
復元することができます。 個々の環境設定セクションは、左側のナビゲーション
バーで選択できます。

環境設定へのアクセス

環境設定にアクセスするには、複数のオプションがあります。

- Windows コントロール パネル
- Windows セキュリティ センター - Windows XP Service Pack 2 以降
- Avira 製品のトレイ アイコン

- コントロール センターのメニュー項目その他 > 環境設定
- コントロール センターの環境設定ボタン

> 注意
> コントロール センターの**環境設定**ボタンで環境設定にアクセスする場合、コントロール センターで有効になっているセクションの環境設定登録に進みます。個々の環境設定登録を選択するには、**エキスパート モード**を有効にする必要があります。 この場合、エキスパート モードの有効化を確認するダイアログが表示されます。

環境設定操作

Windows エクスプローラと同じように、設定ウィンドウで移動します。

- ツリー構造のエントリをクリックすると、詳細ウィンドウにその環境設定セクションが表示されます。
- エントリの前のプラス記号をクリックすると、設定セクションが展開され、ツリー構造の環境設定サブセクションが表示されます。
- 環境設定サブセクションを非表示にするには、展開された環境設定セクションの前のマイナス記号をクリックします。

> 注意
> 環境設定オプションを有効／無効に切り替えたり、ボタンを使用したりするには、次のキー コンビネーションを使用することができます。**[Alt]** + オプション名またはボタンのラベルの下線付きの文字を押す方法です。

> 注意
> 全ての環境設定セクションは、**エキスパート モード**でのみ表示されます。環境設定セクションを表示するには、**エキスパート**

モードを有効にしてください。
有効化の際に定義するパスワードで、エキスパート
モードが保護されている場合があります。

環境設定を有効にする方法：

- **OK** をクリックします。
  ↳ 環境設定ウィンドウが閉じて、入力した設定が有効になります。

  - または -

- **適用**をクリックします。
  ↳ 設定が適用されます。 環境設定ウィンドウは、開いたままです。

環境設定を確定せずに終了したい場合：

- **キャンセル**をクリックします。
  ↳ 環境設定ウィンドウが閉じて、設定は破棄されます。

全ての環境設定を規定値へと復元したい場合：

- **既定値**をクリックします。
  ↳ すべての環境設定は既定値に復元されます。
  デフォルト設定が保存されると、すべての修正ならびに顧客エントリは消去されます。

環境設定オプションの概要

次の環境設定オプションを使用することができます。

- **System Scanner**：オンデマンド スキャンの環境設定
  - 検出時のアクション
  - アーカイブ スキャン オプション
  - システム スキャンの例外

- システム スキャン ヒューリスティック
- 報告機能設定

- **Real-Time Protection**：オンアクセス スキャンの環境設定
  - スキャン オプション
  - 検出時のアクション
  - その他のアクション
  - オンアクセス スキャンの例外
  - オンアクセス スキャン ヒューリスティック
  - 報告機能設定
- **更新**：更新の環境設定
  - プロキシ設定
- **Web Protection**：Web Protection の環境設定
  - スキャン オプション、Web Protection の有効化／無効化
  - 検出時のアクション
  - ブロックされたアクセス：迷惑ファイル形式と MIME 形式、既に知っている迷惑な URL のための Web フィルター（マルウェア、フィッシング等）
  - Web Protection スキャンの例外：URL、ファイル形式、MIME 形式
  - Web Protection ヒューリスティック
  - 報告機能設定
- **Mail Protection**: Mail Protectionの環境設定
  - スキャン オプション：POP3 アカウント監視の有効化、IMAP アカウント、送信メール（SMTP）
  - 検出時のアクション
  - その他のアクション
  - Mail Protection スキャン ヒューリスティック
  - AntiBot 機能：許可される SMTP サーバー、許可される電子メール送信者
  - Mail Protection スキャンの例外

- キャッシュ、エンプティ キャッシュの環境設定
- アンチスパム学習データベース、エンプティ学習データベースの環境設定
- 報告機能設定

- **全般**:
  - System Scanner と Real-Time Protection の脅威カテゴリ
  - 高度な保護：ProActiv および Protection Cloud 機能を有効にするオプション
  - アプリケーション フィルタ：アプリケーションのブロックあるいは許可
  - コントロール センターおよび環境設定へのアクセスのためのパスワード保護
  - セキュリティ：自動開始機能のブロック、製品の保護、Windows ホスト ファイルの保護
  - WMI：WMI サポートを有効にする
  - イベント ログの環境設定
  - 報告機能の環境設定
  - 使用ディレクトリの設定
  - マルウェア検出時の音響アラートの環境設定

4.1.4 トレイ アイコン

インストール後、タスクバーのシステム トレイにAvira製品のトレイ アイコンが表示されます:

アイコン	説明
	Avira Real-Time Protectionは有効
	Avira Real-Time Protectionは無効

トレイ アイコンには、Real-Time Protectionサービスのステータスが表示されます。

Avira製品の中心的機能は、**トレイ アイコン**のコンテキスト
メニューを通してすばやくアクセスすることができます。 コンテキスト
メニューを開くには、**トレイ アイコン**を右マウス ボタンでクリックします。

コンテキスト メニューのエントリ

- **Real-Time Protectionを有効化**: Avira Real-Time Protectionを有効化/無効化します。
- **Mail Protectionを有効化**: Avira Mail Protectionを有効化/無効化します。
- **Web Protectionを有効化**: Avira Web Protectionを有効化/無効化します。
- **Avira Antivirus Premiumを開始**: コントロール センターを開きます。
- **Avira Antivirus Premiumを設定**: 環境設定を開きます。
- **マイ メッセージ**: Avira製品に関する現在情報付きのスライドアップを開きます。
- **マイ コミュニケーション設定**: 製品メッセージ サブスクリプション センターを開きます。
- **更新開始** 更新をスタートします。
- **ヘルプ** : オンライン ヘルプを開きます。
- **Avira Antivirus Premiumについて:** Avira製品上で情報付き対話ボックスを開きます: 製品情報、バージョン情報、ライセンス情報。
- **インターネット上のAvira** インターネット上でAviraウェブポータルを開きます。 これはインターネットにアクティブに接続されている場合に限られます。

4.2 Avira SearchFree Toolbar

Avira SearchFree Toolbar には2つのメイン コンポネントが含まれています: Avira SearchFree および Toolbarです。

Avira SearchFree Toolbar はアドオンとしてインストールされます。
ブラウザが起動(FirefoxとInternet

Explorer)されるとメッセージが現れて、ツールバーのインストール許可を問い合わせます。 Avira SearchFree Toolbar
の順調なインストールを完結させるために、これを許可します。

Avira
SearchFreeは検索エンジンで、これにはAviraウェブサイトおよびウェブ、イメージならびにビデオ チャンネルへクリックでリンクされるAviraロゴが含まれています。
これはAviraユーザーに安全なインターネット ナビゲーションを提供します。

ウェブブラウザに内蔵のツールバーは、検索ボックス、Aviraウェブサイトへリンクされているロゴ、2つのステータス表示、3つのウィジェットならびに**Toolbar Options** メニューから構成されます。

- 検索ツールバー
  Avira検索エンジンを使用したインターネットの迅速検索用の無料検索ツールバーです。
- ステータス表示
  このステータス表示は、Web
  Protectionのステータス情報およびAvira製品の現在更新ステータスを提供し、PCを保護するために必要なアクションの識別をサポートします。
- ウィジェット
  Aviraは、最も重要なインターネット関連機能へ3つのウィジェットを提供しています。
  ひとつのクリックでフェイスブックとEメールに直接アクセス、あるいは安全なウェブブラウジング(FirefoxおよびInternet Explorerのみ)を保証します。
- オプション
  Toolbar Options メニューは、ツールバー
  オプションのアクセス、履歴の消去、ツールバー
  ヘルプおよび情報の発見に使用する、さらにはAvira SearchFree Toolbar
  を直接のウェブブラウジング (FirefoxおよびInternet Explorer
  のみ)経由でアンインストールすることもできます。

4.2.1 使用方法

Avira SearchFree

Avira SearchFree
を使って、インターネットを閲覧するための用語を、複数定義することができます。

検索ボックスに用語を入力し、**Enter** キーを押すか、**Search**をクリックします。 Avira SearchFree エンジンが、インターネット検索を開始し、検索結果をブラウザーウィンドウに表示します。

Internet Explorer、Firefox、Chrome で Avira SearchFree
をカスタム設定する方法は、**Toolbar Options**でご覧ください。

ステータスの表示

Web Protection
Avira の Web Protection ステータスの情報と、ステータス
メッセージは、左側に表示されます。
アイコンやメッセージを使って、コンピュータを保護するために必要なアクションを定義することもできます。

アイコン	ステータス	説明
	*Web Protection*	アイコンの上にカーソルを移動すると、次のメッセージが表示されます： *Avira Web Protection is active. Your browsing is protected* ▸ 特別なアクションは、必要ありません。
	*Web Protection*	アイコンの上にカーソルを移動すると、次のメッセージが表示されます： *Avira Web Protection is off. Click to find out how to turn it on.* ↳ *A*viraのナレッジ ベース に転送されます。

	*Web Protection* がありません	アイコンの上にカーソルを移動すると、次のメッセージが表示されます： *You do not have Avira Web Protection installed. Click to find out how to protect your browsing.* 正しくインストールされなかった場合、あるいは Avira 製品をアンインストールした場合に、このメッセージは表示されます。 *Web Protection is included for free with Avira Antivirus. Click to find out how to install it.* インストールされなかった場合、あるいは Web Protection 製品をアンインストールした場合に、このメッセージは表示されます。 ↳ Avira 製品をダウンロードすることができるAvira ホームページに転送されます。
	エラー	アイコンの上にカーソルを移動すると、次のメッセージが表示されます： *Avira reported an error. Click to contact Support for help.* ▸ グレーのアイコン、または Avira サポートページに移動というテキストをクリックします。

ウィジェット

Avira SearchFree には、最近のインターネットに必要な機能を有する 3 種類のウィジェットが装備されています（Facebook、電子メール、Browser Security）。

Facebook

この機能を使って、Facebook のメッセージを受信したり、常にアップデートしたりすることができます。

電子メール

ツールバーの電子メール シンボルをクリックすると、ドロップ ダウン
リストが表示されます。 一般的に使用されている電子メール
プロバイダーを選択することができます。

Browser Security

このウィジェットは、日常で必要な全てのインターネット セキュリティ
オプションを、ワン クリックで簡単に提供するために考案されています。
このオプションは Firefox と Internet Explorer でのみ使用することができます。
ブラウザーによって、機能の名称が異なる場合があります：

- *Pop-up Blocker*

このオプションが有効になっていると、ポップアップ ウィンドウがブロックされます。

- *Cookie Blocker*

このオプションが有効になっていると、クッキーがコンピュータに保存されません。

- *Private Browsing（Firefox）／InPrivate Browsing（Internet Explorer）*

インターネット
サーフィン中に、個人情報を一切提供したくない場合に、このオプションを有効にします。 Internet Explorer 7 および 8
では、このオプションを利用することはできません。

- *Clear Recent History (Firefox)／Delete Browsing History（Internet Explorer）*

このオプションで、インターネットでの活動履歴を削除することができます。

Website Safety Advisor

Website Safety Advisor は、ナビゲート中の安全性ランキングを提供します。
閲覧しているウェブサイトの評価にアクセスし、リスクの高さをチェックすることができます。

このウィジェットは、ウェブサイトに関するその他の情報も提供します（ドメイン所有者、ウェブサイトが安全／危険だと分類された理由等）。

Website Safety Advisor のステータスが、様々な Avira トレイアイコンで、ツールバーや検索結果に表示されます：

アイコン	ステータス	説明
	*安全*	ウェブサイトが安全な場合は、グリーンのチェックマークが表示されます。
	*低リスク*	ウェブサイトのリスクが低い場合は、黄色いエクスクラメーションマークが表示されます。
	*高リスク*	ウェブサイトのリスクが高い場合は、赤いストップサインが表示されます。
	*不明*	ステータスが不明な場合は、グレーのクエスチョンマークが表示されます。
	*確認中*	ウェブサイトのステータスを確認している間に、このサインが表示されます。

Browser Tracking Blocker

Browser Tracking Blocker で、インターネットサーフィン中に、ユーザーに関する情報を収集する追跡者をストップすることができます。
このウィジェットでは、ブロックする追跡者と、追跡を許可する追跡者を選択することができます。

追跡グループは、3 種類に分類されます：

- ソーシャル ネットワーク
- アド ネットワーク
- その他のグループ

4.2.2 オプション

Avira SearchFree Toolbar は、Internet Explorer、Firefox、Google Chrome との互換性があり、3 つのウェブ ブラウザーで設定することができます。

- Internet Explorer 設定オプション
- Firefox 設定オプション
- Google Chrome 設定オプション

Internet Explorer

Internet Explorer では、**Toolbar Options**メニューで、Avira SearchFree Toolbar の次の環境設定オプションを使用することができます。

Toolbar Options

Search

Avira Searchエンジン

Select Avira Searchエンジンメニューでは、検索で使用する検索エンジンを選択することができます。
アメリカ、ブラジル、ドイツ、スペイン、ヨーロッパ、フランス、イタリア、オランダ、ロシア、英国で、検索エンジンが使用可能です。

Open searches in

Open searches inオプション
メニューで、検索結果を表示する場所を選択することができます（現在のウィンドウ、新しいウィンドウ、新しいタブ）。

Display recent searches

Display recent searchesオプションを有効にすると、検索ツールバーのエントリボックスに、以前検索した用語を表示することができます。

Auto clear recent search history when I close the browser

以前の検索を保存せず、ブラウザを閉じた時に検索履歴を消去したい場合は、**Auto clear recent search history when I close the browser**オプションを有効にします。

More options

Select toolbar language

Select toolbar languageでは、Avira SearchFree Toolbar
を表示する言語を選択することができます。
ツールバーは、英語、ドイツ語、スペイン語、フランス語、イタリア語、ポルトガル語、オランダ語で使用することができます。

> 注意
> 可能な場合、プログラムの言語が、規定の Avira SearchFree Toolbar
> の言語として設定されています。
> その他の言語の場合、ツールバーの規定の言語は、英語に設定されています。

Show button text labels

Avira SearchFree Toolbar
のアイコンの隣のテキストを非表示にしたい場合は、**Show button text labels**を無効にします。

Clear History

以前の検索の保存を希望せず、履歴をすぐに削除したい場合は、**Clear History**オプションを有効にします。

Help

Helpツールバーに関するよくある質問（FAQs）を含むウェブサイトへアクセスします。

Uninstall

Internet Explorer で、Avira SearchFree Toolbar ディレクトリをアンインストールすることもできます（ウェブブラウザーでアンインストール）。

About

Aboutをクリックして、インストールした Avira SearchFree Toolbar のバージョンを表示します。

Firefox

Firefox のウェブブラウザーでは、**オプション**メニューで、Avira SearchFree Toolbarの次の環境設定オプションを使用することができます。

Toolbar Options

Search

Select Avira search engine

Avira search enigineメニューでは、検索で使用する検索エンジンを選択することができます。アメリカ、ブラジル、ドイツ、スペイン、ヨーロッパ、フランス、イタリア、オランダ、ロシア、英国で、検索エンジンが使用可能です。

Display recent searches

Display recent searchesオプションが有効な場合、検索ツールバーの矢印をクリックすることで、以前の検索用語を表示することができます。
検索結果を表示したい場合は、検索用語を選択します。

Auto clear recent search history when I close the browser

以前の検索を保存せず、ブラウザを閉じた時に検索履歴を消去したい場合は、**ブラウザを閉じた時に最近の検索履歴を自動削除**オプションを有効にします。

Display Avira search results when I type keywords or invalid URLs into the browser address bar

このオプションを有効にすると、キーワードを入力した時、あるいはブラウザーのアドレスに無効な URL を入力した時に、検索が開始され、検索結果が表示されます。

More options

Select toolbar language

Select toolbar languageでは、Avira SearchFree Toolbar を表示する言語を選択することができます。
ツールバーは、英語、ドイツ語、スペイン語、フランス語、イタリア語、ポルトガル語、オランダ語で使用することができます。

> 注意
> 可能な場合、プログラムの言語が、規定の Avira SearchFree Toolbar の言語として設定されています。
> その他の言語の場合、ツールバーの規定の言語は、英語に設定されています。

Show button text labels

Avira SearchFree Toolbar のアイコンの隣のテキストを非表示にしたい場合は、**Show button text lables**を無効にします。

Clear History

以前の検索の保存を希望せず、履歴をすぐに削除したい場合は、**Clear History**オプションを有効にします。

Help

Helpツールバーに関するよくある質問（FAQs）を含むウェブサイトへアクセスします。

Uninstall

直接 Firefox で Avira SearchFree Toolbar をアンインストールすることもできます（ウェブ ブラウザーでアンインストール）。

About

Aboutをクリックして、インストールした Avira SearchFree Toolbar のバージョンを表示します。

Google Chrome

Chrome のウェブ ブラウザーでは、赤い Avira の傘のメニューで、Avira SearchFree Toolbar の次の環境設定オプションを使用することができます。

Help

Helpツールバーに関するよくある質問（FAQs）を含むウェブサイトへアクセスします。

Uninstall instructions

ツールバーをアンインストールするのに必要な情報を含む記事へ、リンクすることができます。

About

Aboutで、インストールした Avira SearchFree Toolbar のバージョンを表示します。

Show/Hide the Avira SearchFree Toolbar

ウェブ ブラウザーで Avira SearchFree Toolbar を表示、または非表示にするには、ここをクリックします。

4.2.3 アンインストール

Avira SearchFree Toolbarをアンインストールするには(たとえばWindows 7):

- Windowsの**スタートメニュー**を経て、**コントロール パネル**を開きます。
- **プログラムおよび機能**上をダブルクリックします。
- **Avira SearchFree Toolbar plus Web Protection**をリスト内で選択し、**アンインストール**をクリックします。
  - ↳ この製品を本当にアンインストールするかどうかの確認の問い合わせがあります。
- 確定には**はい**を押します。
  - ↳ Avira SearchFree Toolbar plus Web Protectionはアンインストールされ、コンピューターを再起動するとAvira SearchFree Toolbar plus Web Protectionのすべてのディレクトリ、ファイルおよびレジストリ エントリーは削除されます。

ウェブブラウザを通したアンインストール

Avira SearchFree Toolbarをブラウザ内で直接アンインストールするオプションもあります。
このオプションは**FirefoxとInternet Explorer**だけに入手可能:

- 検索ツールバー内で**オプション**メニューが開きます。

- アンインストールをクリックします。
  - ↪ ウェブブラウザを開くと、それを閉じる問い合わせがあります。
- ウェブブラウザを閉じるにはOKをクリックします。
  - ↪ Avira SearchFree Toolbar plus Web Protectionはアンインストールされ、コンピューターを再起動するとAvira SearchFree Toolbar plus Web Protectionのすべてのディレクトリ、ファイルおよびレジストリエントリーは削除されます。

> 注記
> Avira SearchFree Toolbar をアンインストールするには、ツールバーがアドオンマネジャー内で有効であることに注意してください。

アドオンでのアンインストール

ツールバーがアドオンとしてインストールされているため、その一部としてだけアンインストールできます:

Firefox

ツール > アドオン > 拡張子。 ここからAviraアドオンを管理することができます:

ツールバーとアンインストールの有効化/無効化。

Internet Explorer

アドオンの管理 > ツールバーと拡張子へ進みます。 ここで、Avira SearchFree Toolbarの有効化/無効化あるいはアンインストールを決めることができます。

Google Chrome

オプション > 拡張子をクリックして、ツールバーを簡単に管理できます:

有効化、無効化あるいはアンインストール。

4.3 ...の仕方?

章「How to...?」 ライセンスと製品の有効化に関する簡単な手引き、および Avira 製品の重要な機能に関する情報が記載されています。 選択した記事は、Avira 製品の機能に関する概要を記載しています。 ヘルプ センターの各セクションの詳細情報を代替するものではありません。

4.3.1 ライセンスの有効化

Avira 製品のライセンスを有効にする方法：

Avira 製品のライセンスは、*.KEY* ライセンス ファイルで有効化します。 ライセンス ファイルは、Avira から電子メールで送信されます。 ライセンス ファイルには、1回の注文プロセスで注文した全製品のライセンスが含まれています。

Avira 製品をまだインストールしていない場合：

- ライセンス ファイルをコンピュータのローカル ディレクトリに保存します。
- Avira 製品をインストールします。
- インストール中に、ライセンス ファイルの保存場所を入力します。

Avira 製品を既にインストールしている場合：

- ファイル マネージャ、またはアクティベーション電子メールのライセンス ファイルをダブルクリックし、ライセンス マネージャが開いたら画面上の指示に従います。

  - または -

  Avira 製品のコントロール センターで、メニュー項目 **ヘルプ > ライセンス管理**を選択します。

注意

Windows Vista では、ユーザー
アカウント制御ダイアログボックスが表示されます。
必要に応じて、管理者としてログインしてください。 **継続**をクリックします。

- ライセンス ファイルをハイライト表示して、**開く**をクリックします。
  - ↳ メッセージが表示されます。
- **OK** をクリックして、確定します。
  - ↳ ライセンスの有効化が完了しました。
- 必要に応じて、システムを再起動してください。

4.3.2 製品のアクティブ化

Avira製品をアクティブ化するには、以下のオプションがあります:

有効なフル ライセンスでのアクティブ化

プログラムをフル ライセンスでアクティブにするには、ご購入いただいたライセンス データを含む有効なアクティベーション キーを必要とします。 アクティベーション キーはEメールで送信されているか、製品パッケージに印刷されています。

評価ライセンスでのアクティブ化

Avira製品は、限定された期間内でAvira製品の機能全般をテストできる、自動生成の評価ライセンスでアクティブ化することができます。

注記

製品のアクティブ化あるいはテスト
ライセンスには、アクティブなインターネット リンクを必要とします。
Aviraのサーバーへの接続が構築できない場合は、ご使用のfirewallの設定を確認してください:
HTTPプロトコルとポート80(ウェブ通信)経由の接続、ならびに暗号化プロト

コルSSLとポート443経由の接続が、製品アクティブ化に使用されます。
firewallで受信データや送信データが制止されていないことを確認してください。
まず、ウェブブラウザでウェブページにアクセスできるかどうかを確認してください。

Avira製品のアクティブ化は以下に説明します:

Avira 製品がまだインストールされていない場合:

- Avira製品をインストールします。
  - ↳ インストール中には、アクティベーション オプションの選択が問われます。
- **製品のアクティブ化**: 有効なフル ライセンスでのアクティブ化
- **製品のテスト**: 評価ライセンスでのアクティブ化
- フル ライセンスでのアクティブ化用のアクティベーション キーを入力します。
- **次へ**をクリックして、アクティベーションの選択を確認してください。
- 必要に応じて、登録用の個人データを入力し、**次へ** をクリックして確認します。
  - ↳ ライセンス データが次のウィンドウで表示されます。
    Avira製品が有効となりました。
- インストールを続行します。

Avira 製品がすでにインストールされている場合:

- コントロール センター内でメニュー項目**ヘルプ >**
  ライセンス管理を選択してください。
  - ↳ *ライセンス ウィザード*が開きます。ここでアクティベーション
    オプションを選択できます。
    製品アクティベーションの次のステップは、前述の手順と同様です。

4.3.3 自動更新の実行

Avira製品を自動的に更新するためのスケジューラによるジョブの作成:

- コントロール センター内で、セクション*ADMINISTRATION* > スケジューラを選択します。
- **新規ジョブの挿入**アイコンをクリックします。
  - ↳ **ジョブの名前と説明**対話ボックスが表示されます。
- ジョブに名前を付け、必要に応じて説明を付けてください。
- **次へ**をクリックします。
  - ↳ **ジョブのタイプ**対話ボックスが表示されます。
- リストから **更新ジョブ**を選択します。
- **次へ**をクリックします。
  - ↳ **ジョブの時間**対話ボックスが表示されます。
- 更新の時間を選択します:

- **即時**
- **毎日**
- **毎週**
- **間隔**
- **単一**
- **ログイン**

> 注意
> 当社では、定期的な自動更新を推奨しています。 推薦される更新間隔: 2 時間.

- 必要に応じて、選択内容に従って日付を指定してください。
- 必要に応じて、追加オプションを選択してください (ジョブタイプによって使用可能):

- **期限切れのジョブの繰り返し**
  コンピュータの電源が入っていなかった場合など、必要な時間に実行されなかった過去のジョブが実行されます。
- **インターネット接続中のジョブの開始 (ダイヤルアップ)**
  定義した頻度だけでなく、インターネット接続が構築される場合にもジョブが実行されます。

▸ **次へ**をクリックします。

↳ **表示モードの選択**対話ボックスが表示されます。

▸ ジョブ ウィンドウの表示モードを選択:

- **非表示**: ジョブ ウィンドウなし
- **最小化**: 進捗バーのみ
- **最大化**: ジョブ ウィンドウ全体

▸ **終了** をクリックします。

↳ 新たに作成したジョブは、*ADMINISTRATION* > **スケジューラ**セクションの開始ページにアクティブ化のステータス(チェックマーク)と共に表示されます。

▸ 必要に応じて、実行されないジョブを非アクティブにします。

次のアイコンを使用して、さらにジョブを定義します:

 ジョブのプロパティを表示

 ジョブの編集

 ジョブの削除

 ジョブの開始

ジョブの停止

4.3.4 手動更新の開始

手動更新を開始するには、様々なオプションがあります。手動で更新を開始すると、常にウィルス定義ファイルとスキャン エンジンが更新されます。

Avira 製品の手動更新を開始する方法：

- 右マウス ボタンで、タスクバーの Avira トレイ アイコンをクリックします。
  - ↳ コンテキスト メニューが表示されます。
- **更新の開始**を選択します。
  - ↳ **アップデータ**のダイアログ ボックスが表示されます。

- または -

- コントロール センターで、**ステータス**を選択します。
- **最終更新**フィールドで、**更新の開始**リンクをクリックします。
  - ↳ アップデータのダイアログ ボックスが表示されます。

- または -

- コントロール センターの**更新**メニューで、メニュー コマンド**更新の開始**を選択します。
  - ↳ アップデータのダイアログ ボックスが表示されます。

> 注意
> 当社では、定期的な自動更新を推奨しています。 推薦される更新間隔: 2 時間.

> 注意
> 直接 Windows セキュリティ センターで、手動更新を実行することもできます。

4.3.5 スキャン プロファイルを使用したウイルスとマルウェアのスキャン

スキャン プロファイルは、スキャンするドライブとディレクトリのセットです。

スキャン プロファイルを介したスキャンでは、次のオプションが使用できます：

事前設定のスキャン プロファイルを使用

事前設定のスキャン プロファイルが要件に一致している場合。

カスタマイズしてスキャン プロファイルを適用(手動による選択)

カスタマイズしたスキャン プロファイルでスキャンする場合。

新しいスキャン プロファイルを作成して適用

独自のスキャン プロファイルを作成する場合。

オペレーティング
システム(OS)によって、スキャンプロファイルの開始に使用できるアイコンが異なります：

- Windows XP:

   このアイコンは、スキャン プロファイルを使用してスキャンを開始します。

- Windows Vista:

  Microsoft Windows Vista
  の場合、コントロールセンターには現在、ディレクトリとファイルへのアクセスなど、制限付きの権限しかありません。
  特別な操作およびファイルへのアクセスは、拡張された管理者権限を使用してのみ、コントロール センターで実行できます。 拡張された管理者権限は、スキャン プロファイルを介した各スキャンの開始時に承認される必要があります。

  -  このアイコンはスキャンプロファイルを使用して、制限されたスキャンを開始します。 Windows Vista
    がアクセス権限を承認したディレクトリとファイルのみがスキャンされます。

-  このアイコンは、拡張された管理者権限を使用してスキャンを開始します。
  確定後、選択したスキャンプロファイルのすべてのディレクトリとファイルがスキャンされます。

スキャン プロファイルを使用したウイルスとマルウェアのスキャン：

- コントロール センターに移動して、セクション*PC PROTECTION* >**System Scanner**を選択します。
  ↪ 事前設定のスキャン プロファイルが表示されます。
- 事前設定のスキャン プロファイルのいずれか1つを選択します。
  -もしくは-
  手動による選択スキャン プロファイルを調整します。
  -もしくは-
  新しいスキャン プロファイルの作成
- アイコンをクリックします(Windows XP の場合は  、Windows Vista の場合は )。
- **Luke Filewalker**ウィンドウが開き、システム スキャンが開始します。
  ↪ スキャンが完了すると、結果が表示されます。

スキャン プロファイルを適用する場合：

- スキャン プロファイルで、**手動による選択**
  ファイルツリーを展開し、スキャンするすべてのドライブとディレクトリを開きます。
- +アイコンをクリックすると、次のディレクトリ レベルが表示されます。
- -アイコンをクリックすると、次のディレクトリ レベルが秘匿されます。
- 適切なディレクトリレベルの関連するボックスをクリックして、スキャンするノードとディレクトリをハイライト表示します：
  ディレクトリの選択には以下のオプションが使用可能：

- サブディレクトリを含むディレクトリ(黒のチェック マーク)
- 1つのディレクトリのサブディレクトリのみ(灰色のチェック マーク、サブディレクトリは黒のチェック マーク)
- ディレクトリなし(チェック マークなし)

新たなスキャン プロファイルを作成する場合：

▸  **新規プロファイルの作成** アイコンをクリックします。

↳ **新規プロファイル**が、旧プロファイルの下に表示されます。

▸ 必要に応じて、 
アイコンをクリックして、スキャンプロファイルに名前を付けます。

▸ それぞれのディレクトリ
レベルのチェックボックスをクリックして、保存するノードとディレクトリをハイライト表示します。

ディレクトリの選択には以下のオプションが使用可能：

- サブディレクトリを含むディレクトリ(黒のチェック マーク)
- 1つのディレクトリのサブディレクトリのみ(灰色のチェックマーク、サブディレクトリは黒のチェック マーク)
- ディレクトリなし(チェック マークなし)

4.3.6 Drag & Drop を使用したウイルスとマルウェアのスキャン

Drag & Drop を使用してウィルスやマルウェアをスキャンする方法：

✓ Avira 製品のコントロール センターを開きます。

▸ スキャンするファイルまたはディレクトリをハイライト表示します。

▸ マウスの左ボタンを使用して、ハイライト表示したファイルまたはディレクトリを**コントロール センター**にドラッグします。

↳ **Luke Filewalker** ウィンドウが表示され、システム スキャンが開始されます。

↳ スキャンが完了すると、結果が表示されます。

4.3.7 コンテキスト メニューを使用したウィルスとマルウェアのスキャン

コンテキスト メニューを使用してウィルスやマルウェアをスキャンする方法：

- スキャンするファイルまたはディレクトリを、右マウス ボタンでクリックします（例：Windowsエクスプローラ、デスクトップ、開いている Windows ディレクトリ）。
  - ↳ Windows エクスプローラのコンテキスト メニューが表示されます。
- コンテキスト メニューで、**Avira で選択したファイルをスキャン**を選択します。
  - ↳ **Luke Filewalker** ウィンドウが表示され、システム スキャンが開始されます。
  - ↳ スキャンが完了すると、結果が表示されます。

4.3.8 ウイルスとマルウェアの自動スキャン

> 注記
> インストール後には、スキャン ジョブ**全システムスキャン**がスケジューラ内に作成されます:
> 全システムスキャンは、推薦される間隔で自動的に実行されます。

ウイルスとマルウェアの自動スキャン用のジョブの作成

- コントロール センター内で、セクション*ADMINISTRATION* > **スケジューラ**を選択します。
- アイコン + をクリックします。
  - ↳ **ジョブの名前と説明**対話ボックスが表示されます。
- ジョブに名前を付け、必要に応じて説明を付けてください。
- **次へ**をクリックします。
  - ↳ **ジョブのタイプ**対話ボックスが表示されます。
- **スキャン ジョブ** を選択します。

▸ **次へ**をクリックします。

↳ **プロファイルの選択** ダイアログ ボックスが表示されます。

▸ スキャンするプロファイルを選択します。

▸ **次へ**をクリックします。

↳ **ジョブの時間**対話ボックスが表示されます。

▸ スキャン時刻を選択します:

- **即時**
- **毎日**
- **毎週**
- **間隔**
- **単一**
- **ログイン**

▸ 必要に応じて、選択内容に従って日付を指定してください。

▸ 必要に応じて、次の追加オプションを選択してください
(ジョブタイプによって使用可能):

- **時間切れにはジョブを繰り返す**

  コンピュータの電源が入っていなかった場合など、必要な時間に実行されなかった過去のジョブが実行されます。

▸ **次へ**をクリックします。

↳ **表示モードの選択** 対話ボックスが表示されます。

▸ ジョブ ウィンドウの表示モードを選択:

- **非表示**: ジョブ ウィンドウなし
- **最小化**: 進捗バーのみ
- **最大化**: ジョブ ウィンドウ全体

▸ スキャン終了後にコンピューターのシャットダウンを自動的に行いたい場合は、**ジョブ終了後にコンピューターの電源を切る**オプションを選択します。

このオプションは、表示モードが最大あるいは最小化されているときだけ使用可能です。

- **終了** をクリックします。
  - ↳ 新たに作成したジョブは、*ADMINISTRATION* > スケジューラセクションの開始ページにアクティブ化のステータス(チェックマーク)と共に表示されます。
- 必要に応じて、実行されないジョブを非アクティブにします。

次のアイコンを使用して、さらにジョブを定義します:

 ジョブのプロパティを表示

 ジョブの編集

 ジョブの削除

 ジョブの開始

ジョブの停止

4.3.9 アクティブなルートキットに対象を絞ったスキャン

アクティブなルーキットをスキャンするには、定義済みのスキャンプロファイル**ルーキットとアクティブなマルウェアに対するスキャン**を使用します。

アクティブなルートキットをスキャンする方法：

- コントロール センターへ移動し、*PC PROTECTION* > **System Scanner** セクションを選択します。
  - ↳ 定義済みのスキャン プロファイルが表示されます。
- 定義済みのスキャンファイル**ルートキットとアクティブなマルウェアに対するスキャン**を選択します。

- 必要に応じて、ディレクトリ レベルのチェック
  ボックスをクリックして、スキャンするその他のノードとディレクトリをハイライト表示します。
- アイコン（Windows XP：  または Windows Vista：
   ）をクリックします。
  - ↳ **Luke Filewalker** ウィンドウが表示され、システム スキャンが開始されます。
  - ↳ スキャンが完了すると、結果が表示されます。

4.3.10 検出されたウィルスやマルウェアへの対応

Avira
製品の個々の保護コンポーネントでは、**検出に対するアクション**セクションの**環境設定**で、Avira 製品にどう対処させるかを定義することができます。

Real-Time Protection の ProActiv
のための設定可能なアクションのオプションは、ありません。検出通知は、常に**Real-Time Protection: 疑わしいアプリケーション ビヘイビア**
ウィンドウに表示されます。

System Scanner の操作オプション：

対話型

対話型アクション モードでは、System Scanner によるスキャン結果がダイアログボックスに表示されます。
このオプションは、初期状態で有効に設定されています（デフォルト設定）。

System Scanner スキャン
の場合、スキャン完了後、感染ファイルのリストを添付したアラートが届きます。
状況依存のメニューを使用して、感染したさまざまなファイルに対して実行するアクションを選択できます。
全ての感染したファイルに対して標準のアクションを実行したり、もしくは、System Scanner をキャンセルすることもできます。

自動

自動アクション
モードの場合、ウィルスまたは不要プログラムが検出されると、この領域で選択されているアクションが、自動的に実行されます。

Real-Time Protection の操作オプション：

対話型

対話型アクション モードの場合、データ
アクセスは拒否され、デスクトップに通知が表示されます。
デスクトップの通知で、マルウェアを除去したり、その他のウィルス管理のための詳細ボタンを使って、マルウェアをSystem Scanner
コンポーネントに転送することができます。 System Scanner は、コンテキストメニューを介して、感染ファイルの様々な管理オプションを記載した、検出通知オプションを含むウィンドウを開きます（検出 > System Scanner）：

自動

ボタンを使って、マルウェアをSystem Scanner
コンポーネントに転送することができます。

Mail Protection、Web Protection の操作オプション：

対話型

対話型アクション
モードでは、ウィルスまたは不要プログラムが検出された場合に、ダイアログボックスが表示され、感染したオブジェクトの処理方法を選択することができます。
このオプションは、初期状態で有効に設定されています（デフォルト設定）。

自動

自動アクション
モードの場合、ウィルスまたは不要プログラムが検出されると、この領域で選択されているアクションが、自動的に実行されます。

対話型アクション
モードでは、検出されたウィルスおよび不要プログラムに対するアクションを選択できます。そのためには、（アラートに表示される）感染したオブジェクトのアクションを選択し**確認**をクリックして選択したアクションを実行します。

感染したオブジェクトを処理するために選択できるアクションを次に示します。

> 注意
> 選択できるアクションは、オペレーティング
> システム、検出した保護コンポーネント（Avira Real-Time
> Protection、Avira System Scanner、Avira Mail Protection、Avira Web
> Protection）、および検出されたマルウェアのタイプにより異なります。

**System Scanner、Real-Time Protection のアクション（ProActiv
検出ではありません）：**

修復

ファイルの修復を行います。

このオプションは、感染したファイルが修復可能な場合にのみ使用できます。

名前の変更

**.vir* 拡張子で、ファイルの名前を変更します。
これらのファイルへ直接アクセスすること（ダブルクリックなど）は、不可能になります。 ファイルは、後で修復して、元の名前に変更することができます。

隔離

ファイルは特殊な形式にパッケージされ（**.qua*）、ハードディスクの隔離ディレクトリ *INFECTED*
に移動されます。その後、これらのファイルに直接アクセスすることは、できません。 このディレクトリのファイルは、後々、隔離内で修復できます。必要に応じて Avira に送信することもできます。

削除

ファイルの削除が行われます。
このプロセスは、**上書きおよび削除**よりはるかに速く実行することができます。
ブート セクタ ウィルスが検出された場合、ブート セクタを削除することでブート セクタ ウィルスを削除できます。 新しいブート セクタが書き込まれます。

無視

特別なアクションは、必要ありません。
感染したファイルは、コンピュータ上で実行可能な状態のままになります。

上書きおよび削除

ファイルは既定のテンプレートで上書きされ、削除されます。
この処理を施したファイルは、復元不能となります。

> **警告**
> データの損失とオペレーティング
> システムへの悪影響につながる可能性があります！ **無視**
> オプションは、例外的な場合にのみ選択するようにしてください。

常に無視

Real-Time Protection 検出の操作オプション：Real-Time Protection
の特別なアクションの必要は、ありません。
ファイルへのアクセスが、許可されます。
このファイルへの全てのアクセスが許可され、コンピュータの再起動、もしくはウィルス定義ファイルの更新まで、通知はありません。

隔離にコピー

ルートキット検出の操作アクション：検出が、隔離にコピーされます。

ブートセクターの修復 | 修復ツールのダウンロード

感染したブートセクターが検出された場合の操作オプション：感染したディスケットドライブを修復するための様々なオプションがあります。 Avira 製品で修復することができない場合、ブートセクターウィルスの検出と除去を行うスペシャルツールをダウンロードすることができます。

> 注意
> プロセス作動中にアクションを実行した場合、問題のプロセスは、アクションが実行される前に終了します。

ProActiv コンポーネントの検出の Real-Time Protection の操作（アプリケーションの疑わしいアクションの通知）：

信頼できるプログラム

アプリケーションは、継続して作動します。 プログラムは、許容アプリケーションリストに追加され、ProActiv コンポーネントによる監視の対象から除外されます。許容アプリケーションリストに追加された場合、監視のタイプは、コンテンツに設定されます。つまり、アプリケーションは、コンテンツが変更されない限り、ProActiv コンポーネントのみの監視から除外されている、というです（アプリケーションフィルタ：許容アプリケーション参照）。

一回だけプログラムをブロックする

例えば、アプリケーションの終了等の場合、アプリケーションがブロックされます。アプリケーションのアクションは、引き続き ProActiv コンポーネントにより監視されます。

常にこのプログラムをブロックする

例えば、アプリケーションの終了等の場合、アプリケーションがブロックされます。プログラムは、ブロックされたアプリケーションのリストに追加され、作動すること

はできません（アプリケーション
フィルタ：ブロックするアプリケーション参照）。

無視

アプリケーションは、作動し続けます。 アプリケーションのアクションは、引き続き ProActiv コンポーネントにより監視されます。

Mail Protection 操作：受信メール

隔離に移動

電子メールは、全て添付ファイルと共に隔離に移されます。
感染した電子メールは、削除されます。
電子メールのテキストの本文と添付ファイルは、既定のテキスト.に置換されます。

メール削除

感染した電子メールは削除されます。
電子メールのテキストの本文と添付ファイルは、既定のテキストに置換されます。

添付ファイルの削除

感染した添付ファイルは、既定のテキストに置換されます。
電子メールのテキストの本文が感染している場合は、削除され、既定のテキストに置換されます。 電子メール自体は配信されます。

添付ファイルを隔離に移動

感染した添付ファイルは、隔離に配置されてから削除されます
（既定のテキストに置換されます)。 電子メールの本文は配信されます。
感染した添付ファイルは、後で 隔離マネージャによって配信されます。

無視

感染した電子メールは配信されます。

警告

ウィルスや不要プログラムが、コンピュータ
システムにアクセスする可能性があります。
無視オプションは、例外的な場合にのみ選択するようにしてください。 メール クライアントのプレビューを無効にして、添付ファイルをダブルクリックで開いたりは、絶対にしないでください！

Mail Protection の操作：送信メール

隔離にメールを移動（送信しない）

電子メールは、すべての添付ファイルと共に隔離にコピーされ、送信されません。 電子メールは、電子メール クライアントの送信トレイに残っています。 電子メール プログラムから、エラーメッセージが届きます。 電子メール
アカウントから送信される、その他すべての電子メールに対して、マルウェアのスキャンが実行されます。

メールの送信をブロック（送信しない）

電子メールは、電子メール クライアントの送信トレイに残っています。 電子メール プログラムから、エラーメッセージが届きます。 電子メール
アカウントから送信される、その他すべての電子メールに対して、マルウェアのスキャンが実行されます。

無視

感染した電子メールが、送信されます。

警告

メールを送信することで、ウィルスや不要プログラムが、メールを受け取った人のコンピュータ システムに、侵入する可能性があります。.

Web Protection の操作：

アクセスの拒否

Web サーバーまたは転送されたデータおよびファイルによって要求された Web サイトは、Web ブラウザには送信されません。
アクセスが拒否されたことを通知するエラー メッセージが、Web ブラウザに表示されます。

隔離に移動

Web サーバーによって要求された Web サイトおよび転送されたデータやファイルは、隔離に移動されます。
情報として価値がある場合、感染ファイルを隔離マネージャから復元することができます。また、必要に応じて Avira マルウェア リサーチ センターに送信することもできます。

無視

Web サーバーによって要求された Web サイト、および転送されたデータやファイルは、Web Protection によって Web ブラウザに送信されます。

警告
ウィルスや不要プログラムが、コンピュータ システムにアクセスする可能性があります。
無視オプションは、例外的な場合にのみ選択するようにしてください。

注意
修復できない疑わしいファイルは、全て隔離に移動することをお勧めします。

注意

ヒューリスティック

スキャン機能で報告されたファイルを分析するため、弊社にお送りいただくことも可能です。

例えば、こういったファイルを、弊社のウェブサイトでアップロードすることもできます：http://www.avira.jp/sample_upload

。ヒューリスティックで報告されたファイルを、名前のプレフィックス記号 *HEUR/* や *HEURISTIC/* などで特定することができます（例：*HEUR/testfile.**）。

4.3.11 隔離されたファイル（*.qua）の処理

隔離されたファイルを処理する方法：

- コントロール センターで、*管理* > **隔離**セクションを選択します。
- 関連するファイルを確認します。必要に応じて、別の場所から元のファイルをコンピュータにリロードすることができます。

ファイルの詳細情報を閲覧したい場合：

- ファイルをハイライト表示して  をクリックします。
  - ↪ ダイアログ ボックス **プロパティ**に、ファイルの情報が表示されます。

ファイルを再度スキャンしたい場合：

Avira

製品のウィルス定義ファイルを更新した上で、誤検出レポートの可能性がある場合は、ファイルをスキャンすることをお勧めします。

この方法で誤検出を確認して、ファイルを復元できます。

- ファイルをハイライト表示して  をクリックします。

↳ システム
スキャンの設定を使用して、ファイルのウィルスとマルウェアのスキャンが実行されます。

↳ スキャン後、**スキャンの統計データ**に、再スキャン前後のファイルのステータスに関する統計データが表示されます。

ファイルを削除する方法：

- ファイルをハイライト表示して  をクリックします。
- 選択は、**はい**で確定します。

分析のために、ファイルを Avira Malware Research Center ウェブサーバーにアップロードする方法：

- アップロードするファイルをハイライト表示します。
-  をクリックします。
  ↳ ダイアログが開き、連絡先データを入力するためのフォームが表示されます。
- 必要なデータを全て入力します。
- 種類を選択します（**疑わしいファイル**または**誤検出の疑い**）。
- 返信のフォーマットを選択します（**HTML**、**Text**、**HTML & Text**）。
- **OKをクリックします。**
  ↳ 圧縮形式で、ファイルが Avira Malware Research Center ウェブサーバーにアップロードされます。

注意
次のケースの場合、Avira Malware Research Center による分析をお勧めします。
ヒューリスティック機能による検出（疑わしいファイル）、スキャンで Avira
製品により疑わしいファイルと分類され隔離に移動されたファイル、Avira

Malware Research Center による分析を推奨するウィルス検知ダイアログボックスやレポートファイルがスキャンにより作成された場合、などです。
疑わしいファイル：スキャンでは、ウィルスやマルウェアが検出されなかったものの、ユーザー自身が、疑わしいと判断し、隔離に移動したファイルです。
誤検出の疑い：ウィルス検出という報告が、誤っているのではないかとユーザーが判断したファイルです。Avira
製品が、ファイルでウィルスを検出したと報告しているものの、そのファイルがマルウェアに感染している可能性が低いという場合です。

注意
アップロードできるファイルのサイズは、未圧縮で 20 MB、圧縮済みで 8 MB までです。

注意
一度にアップロードできるファイル数は、ひとつです。

テキスト ファイルに、隔離オブジェクトのプロパティをエクスポートしたい場合：

- オブジェクトをハイライト表示して、 をクリックします。
  - ↳ 選択した隔離オブジェクトのデータを記載するテキスト ファイル *quarantaene - メモ帳*が開きます。
- テキスト ファイルを保存します。

隔離のファイルを復元することも可能です（参照：章 隔離：隔離されたファイルの復元）。

4.3.12 隔離内のファイルの復元

OSにより、さまざまなアイコンで復元手順が制御されます:

- Windows XP:

-  このアイコンは、元のディレクトリへファイルを復元します。
-  このアイコンは、選択するディレクトリへファイルを復元します。

- Windows Vista:

  Microsoft Windows Vista の場合、コントロール センターには現在、ディレクトリとファイルへのアクセスなど、制限付きの権限しかありません。
  特別な操作およびファイルへのアクセスは、拡張された管理者権限を使用してのみ、コントロール センターで実行できます。 拡張された管理者権限は、スキャン プロファイルを介した各スキャンの開始時に承認される必要があります。

  -  このアイコンは、選択するディレクトリへファイルを復元します。
  -  このアイコンは、元のディレクトリへファイルを復元します。
    このディレクトリへのアクセスに拡張された管理者権限が必要な場合は、対応する要求が表示されます。

隔離内のファイルの復元:

> **警告**
> これはデータの損失とコンピュータのオペレーティング システムの損傷につながる可能性があります！
> **選択したオブジェクトの復元**機能は例外的な場合にのみ使用してください。
> 新たなスキャンで修復できる可能性のあるファイルのみを復元してください。

✓ ファイルは再スキャンされ、修復されます。

▸ コントロール センター内で、セクション*ADMINISTRATION* > **隔離**を選択します。

> 注記
> ファイル拡張子が **.eml*の場合、EメールとEメールの添付ファイルはオプション  によってのみ復元できます。

ファイルを本来の場所へ復元:

- ファイルをマーキングして、次のアイコン(Windows XPの場合は  、Windows Vistaの場合は )をクリックします。

このオプションは、Eメールには使用できません。

> 注記
> ファイル拡張子が
> *.eml*の場合、EメールとEメールの添付ファイルはオプション
>  によってのみ復元できます。

  - ↳ ファイルを復元するかどうかを確認するメッセージが表示されます。
- **はい**をクリックします。
  - ↳ ファイルは、隔離に移動される前に配置されていたディレクトリに復元されます。

ファイルを指定ディレクトリへ復元:

- ファイルをハイライト表示して  をクリックします。
  - ↳ ファイルを復元するかどうかを確認するメッセージが表示されます。
- **はい**をクリックします。
  - ↳ ディレクトリの選択には、Windowsのデフォルトウィンドウ*別名で保存*ウィンドウが表示されます。
- ファイルを復元するディレクトリを選択して確定します。
  - ↳ ファイルは選択したディレクトリに復元されます。

4.3.13 疑わしいファイルを隔離に移動

手動で疑わしいファイルを隔離に移動する方法：

- コントロール センターで、*管理* > **隔離**セクションを選択します。
-  をクリックします。
  - ↪ Windows の既定ファイル選択ウィンドウが表示されます。
- ファイルを選択し、**開く**で確定します。
  - ↪ ファイルが隔離に移されます。

隔離にあるファイルは、Avira System Scanner
でスキャンすることができます。（章： 隔離：隔離されたファイル（*.qua）の処理）。

4.3.14 スキャン プロファイルのファイル タイプの修正または削除

スキャン プロファイルで、追加のファイル
タイプをスキャン対象に規定する方法、またはスキャン対象から除外する方法（手動による選択およびカスタマイズされたスキャン プロファイルの場合にのみ可能）：

✓ コントロール センターで、*PC PROTECTION* > **System Scanner**
セクションに移動します。

- 右マウス ボタンで、編集したいスキャン プロファイルをクリックします。
  - ↪ コンテキスト メニューが表示されます。
- **ファイル フィルタ** を選択します。
- コンテキスト メニューの右側の小さな三角形をクリックして、コンテキスト
メニューを展開します。
  - ↪ エントリ**既定**、**全てのファイルをスキャン**、**ユーザー定義**が表示されます。
- **ユーザー定義**を選択します。
  - ↪ スキャン プロファイルでスキャンする全ファイル
タイプのリストと共に、**ファイル拡張子**ダイアログ ボックスが表示されます。

ファイル タイプをスキャン対象から除外したい場合：

- ファイル タイプをハイライト表示して、**削除**をクリックします。

ファイル タイプをスキャン対象に追加したい場合：

- ファイル タイプをハイライト表示します。
- **挿入**をクリックし、インプット ボックスにファイル タイプのファイル拡張子を入力します。

最大 10 文字入力することができます。先頭にピリオドは入力しないでください。ワイルドカード (* および ?) を使用できます。

4.3.15 スキャン プロファイルのデスクトップ ショートカットの作成

Avira 製品のコントロール センターにアクセスすることなく、スキャン プロファイルのデスクトップ ショートカットを使用して、デスクトップから直接、スキャンを開始することができます。

スキャン プロファイルのデスクトップ ショートカットの作成法：

✓ コントロール センターで、*PC PROTECTION* > **System Scanner** セクションに移動します。

- ショートカットを作成するスキャン プロファイルを選択します。
- アイコン  をクリックします。

  ↪ デスクトップ ショートカットが作成されます。

4.3.16 フィルタ イベント

Avira 製品のプログラム コンポーネントにより生成されたイベントは、*管理* > **イベント** のコントロール センターに表示されます（Windows オペレーティング システムのイベント表示と同様）。 プログラム コンポーネントは、次の通りです（アルファベット順）。

- ヘルプ サービス
- Mail Protection

- Real-Time Protection
- スケジューラ
- System Scanner
- アップデータ
- Web Protection

次のイベントが表示されます。

- *情報*
- *警告*
- *エラー*
- *検出*

表示されたイベントのフィルタリング：

- コントロール センターで、セクション *管理* > **イベント** を選択します。
- 有効なコンポーネントのイベントを表示するプログラム
  コンポーネントのボックスをオンにします。

  - または -

  無効なコンポーネントのイベントを非表示にするプログラム
  コンポーネントのボックスをオフにします。
- これらのイベントを表示するには、イベント タイプのボックスをオンにします。

  - または -

  これらのイベントを非表示にするには、イベント
  タイプのボックスをオフにします。

4.3.17 電子メール アドレスをスキャン対象から除外

Mail Protection スキャン対象外の電子メール アドレス（送信者）の定義法（ホワイト リスト）：

- コントロール センターに移動し、*INTERNET PROTECTION* > **Mail Protection** セクションを選択します。
  - ↪ 受信電子メールがリストに表示されます。
- Mail Protection のスキャン対象から除外する電子メールをハイライト表示します。
- なアイコンをクリックして、Mail Protection のスキャンから電子メールを除外します：
-  選択した電子メール アドレスに対するウィルスと不要プログラムのスキャンは、今後、実行されません。
  - ↪ 送信者の電子メール アドレスは除外リストに含められ、ウィルス、マルウェア、のスキャンは、今後、実行されません。

警告

送信者を完全に信頼できる場合にのみ、電子メール アドレスを Mail Protection のスキャン対象から除外してください。

注意

Mail Protection > 全般 > 例外 の環境設定で、電子メール アドレスを除外リストに追加したり、除外リストから削除することができます。

5. System Scanner

System Scannerを使用すると、ウィルスあるいは迷惑プログラムに対象を絞ったスキャン(オンデマンド スキャン)を実行できます。
以下のオプションは感染ファイルのスキャンに使用できます:

- **コンテキスト メニューを使用したSystem scan**
  コンテキスト メニューを使用したSystem scan(右マウス ボタン - エントリー**Aviraによる選択されたファイルのスキャン**)は、たとえば個々のファイルやディレクトリをスキャンする場合にお勧めします。 他の利点は、コンテキスト メニューを使用したシステム スキャンには最初にコントロール センターを開始する必要がないことです。
- **Drag＆Dropによるシステム スキャン**
  ファイルまたはディレクトリをコントロール センターのプログラム ウィンドウにドラッグすると、System Scannerはファイルまたはディレクトリならびにそれに含まれるすべてのサブディレクトリをスキャンします。
  この手順は、たとえばコンピューターなどに保存してある個々のファイルやディレクトリをスキャンする場合にお勧めします。
- **プロファイルを通したシステム スキャン**
  この手順は、特定のディレクトリとドライブを定期的にスキャンする場合にお勧めします(定期的に新しいファイルを保存する作業ディレクトリやドライブなど)。
  これらのディレクトリやドライブは新たにスキャンするたびに選択する必要はありません。関連するプロファイルを使用して選択するだけです。
  プロファイルを通したシステム スキャンを参照。
- **スケジューラを通したシステム スキャン**
  スケジューラは、時間コントロールのスキャン実行を可能にします。
  スケジューラを通したシステム スキャンを参照。

rootkits、ブート セクタ
ウイルス、ならびにアクティブなプロセスのスキャンには、特別なプロセスが必要です。
以下のオプションが使用可能:

- スキャン
  プロファイルを経由したrootkitsのスキャン**rootkitsおよびアクティブなマルウェアのスキャン**
- スキャン プロファイル**アクティブ プロセス**経由のアクティブ プロセスのスキャン
- メニュー コマンド**ブート レコード スキャン...**、メニュー**その他**内、を通したブート セクタ ウイルスのスキャン

6. 更新

アンチウィルス
ソフトウェアの効率は、プログラム、特にウィルス定義ファイルと検索エンジンが、どれだけ新しいかにより異なります。 定期的に更新を行うため、Avira
製品には、アップデータ コンポーネントが統合されています。 アップデータは、常にAvira 製品を最新の状態に保ち、新たに出現するウィルスに対処します。
アップデータは、次のコンポーネントを更新します：

- ウィルス定義ファイル：

  ウィルス定義ファイルは、有害なプログラムのウィルス
  パターンを含んでいます。Avira 製品は、このウィルス
  パターンを使って、ウィルスやマルウェアのスキャンを行い、感染したオブジェクトを修復します。

- スキャン エンジン：

  スキャンエンジンには、Avira
  製品がウィルスやマルウェアのスキャンに使用するメソッドが含まれています。

- プログラム ファイル（製品更新プログラム）：

  製品の更新パッケージにより、各プログラム
  コンポーネントの追加機能を使用することができるようになります。

更新により、ウィルス定義ファイル、スキャンエンジン、および製品が最新かどうかを確認し、必要に応じて更新を実装します。
製品の更新後、コンピュータを再起動する必要があります。
ウィルス定義ファイルとスキャン
エンジンのみが更新された場合は、コンピュータを再起動する必要はありません。

製品の更新により再起動が必要になる場合は、そのまま更新を続行するか、後で更新について通知させるかを選択できます。
そのまま製品の更新を続行する場合でも、再起動のときに再び選択することができます。

後で更新についての通知を希望する場合はウイルス定義ファイルとスキャンエンジンは更新されますが、製品の更新は行われません。

> 注意
> 製品の更新は、再起動が実行されません、完了しません。
>
> 注意
> セキュリティ上の理由から、コンピュータの Windows ホストファイルが改変されていないか、更新 URL がマルウェアに操作されていないか、アップデータが不要なダウンロードサイトに転送されていないかどうかを、アップデータがチェックします。Windows ホストファイルが操作されている場合は、アップデータのレポートファイルに表示されます。

更新は、次の間隔で実行されます：2 時間。

スケジューラのコントロール
センターで、指定した間隔で、アップデータにより実行される追加の更新ジョブを作成することができます。 手動で更新を開始するオプションもあります：

- コントロールセンターの**更新**メニューおよび**ステータス**セクション
- トレイ アイコンのコンテキスト メニュー

更新プログラムは、メーカーのウェブサーバーを介してインターネットから取得できます。 既存のネットワーク接続は、Avira のダウンロード サーバーの既定の接続です。
環境設定 > 更新の下でこのデフォルト設定を変更できます。

7. FAQ、ヒント

この章には、Avira
製品の使用におけるトラブルシューティングおよびその他のヒントに関する重要な情報が記載されています。

- 参照：章 問題が発生した場合のヘルプ
- 参照：章 ショートカット
- 参照：章 Windows セキュリティ センター（Windows XP、Vista）あるいは Windows アクション センター（Windows 7、Windows 8）

7.1 問題が発生した場合のヘルプ

ここには、発生する可能性のある問題の原因と解決策に関する情報が記載されています。

- エラー メッセージライセンス *ファイルが開けません*が表示されます。
- エラー メッセージ*ファイルのダウンロード中、接続に失敗しました ...*
  が、アップデートを開始しようとすると表示されます。
- ウィルスとマルウェアの移動や削除ができません。
- トレイ アイコンのステータスが無効です。
- データ バックアップを実行すると、コンピュータが極端に遅くなります。
- ファイアウォールが、Avira Real-Time Protection および Avira Mail Protection を、起動後すぐに報告します。
- Avira Mail Protection が機能しません。
- TSL 接続を介して送信した電子メールが、Mail Protection にブロックされました。
- Web チャットができません。チャットのメッセージが表示されません。

エラー メッセージ *ライセンス ファイルが開けません*が表示されます。

原因：ファイルが暗号化されています。

- ライセンスを有効にするために、ファイルを開く必要はありませんが、ファイルをプログラム ディレクトリに必ず保存してください。

エラー メッセージ*ファイルのダウンロード中、接続に失敗しました ...*
が、アップロードを開始すると表示されます。

原因：インターネットに接続されていません。 インターネットの web サーバーに接続することができません。

- WWW や電子メールなど、その他のインターネット サービスが機能しているかどうかテストしてください。機能していない場合、再度インターネット接続を試みてください。

原因：プロキシサーバーに接続できません。

- プロキシサーバーへのログイン情報が変更されていないかを確認し、必要に応じて設定を調整してください。

原因：*update.exe* ファイルに対して、パーソナル ファイアウォールによる完全な承認が行われていません。

- *update.exe* ファイルがパーソナル ファイアウォールで完全に承認されていることを確認してください。

もしくは、

- 環境設定（エキスパート モード）の設定を確認してください（PC Protection > 更新）。

ウィルスとマルウェアの移動や削除ができません。

原因：ファイルが Windows によって読み込まれ、アクティブになっています。

- Avira 製品の更新を実行してください。
- Windows XP を使用している場合は、システムの復元を無効にします。
- コンピュータをセーフ モードで起動します。

- Avira 製品の環境設定を開始します（エキスパート モード）。
- System Scanner > スキャン > ファイル > 全てのファイル の順に選択し、**OK** を押して確定します。
- すべてのローカル ドライブのスキャンを開始します。
- 標準モードでコンピュータを起動します。
- 標準モードでスキャンを実行します。
- 他のウィルスまたはマルウェアが検出されず、使用可能な場合は、システムの復元を有効にします。

トレイ アイコンのステータスが無効です。

原因：Avira Real-Time Protection が無効です。

- コントロールセンターの**ステータス**をクリックして、**PC Protection**エリアの*Real-Time Protection*を有効にします。

-もしくは-

- トレイ アイコンを右クリックして、コンテキスト メニューを開きます。 **Real-Time Protection の有効化**をクリックします。

原因：ファイアウォールにより、Avira Real-Time Protection がブロックされています。

- ファイアウォールの設定で、Avira Real-Time Protection を全般的に承認するように定義してください。 Avira Real-Time Protection は、アドレス 127.0.0.1（ローカルホスト）でのみ機能します。インターネットに接続していません。 Avira Mail Protection も同様です。

もしくは、

- Avira Real-Time Protection サービスのスタートアップ タイプを確認します。必要であれば、タスクバーで**スタート > 設定 > コントロール**

パネルを選択し、サービスを有効にします。
ダブルクリックで、**サービス**環境設定パネルを開始します（Windows XP では、サービス アプレットは、*管理ツール*のサブディレクトリに配置されます）。
エントリ *Avira Real-Time Protection* を検索します。
スタートアップの種類には自動、ステータスには開始と入力する必要があります。
必要に応じて、該当するラインと、**開始**ボタンを選択してサービスを手動で開始します。 エラー メッセージが表示されたら、イベント表示を確認してください。

データ バックアップを実行すると、コンピュータが極端に遅くなります。

原因：バックアップ中、Avira Real-Time Protection が、使用された全ファイルのスキャンを行っています。

- 環境設定で **Real-Time Protection > スキャン > 例外** を選択し、バックアップ ソフトウェアのプロセス名を入力します。

ファイアウォールが、Avira Real-Time Protection および Avira Mail Protection を、起動後すぐに報告します。

原因：Avira Real-Time Protection と Avira Mail Protection のコミュニケーションは、TCP/IP インターネット プロトコルを介して行われます。ファイアウォールは、このプロトコルを介したすべての接続を監視します。

- Avira Real-Time Protection と Avira Mail Protection の一般的な承認を定義してください。 Avira Real-Time Protection は、アドレス 127.0.0.1（ローカルホスト）でのみ機能します。
インターネットに接続していません。 Avira Mail Protection も同様です。

Avira Mail Protection が機能しません。

Avira Mail Protection で問題が発生している場合は、次のチェックリストを使用して、Avira Mail Protection が適切に機能しているかを確認してください。

チェックリスト

- メール クライアントが、Kerberos、APOP、または RPA を介してサーバーにログインしているかどうかを確認してください。これらの検証方法は、現在サポートされていません。
- メール クライアントが、SSL（TLS – Transport Layer Security とも呼ばれる）を通して、サーバーにレポートしているかどうか確認してください。 Avira Mail Protection は、SSL に対応していません。ですから、暗号化された SSL 接続は、全て終了します。 暗号化された SSL 接続を、Mail Protection で保護せずに利用したい場合は、Mail Protection で監視されていないポートを使って接続してください。 Mail Protection で監視するポートは、**Mail Protection > スキャン** で設定することができます。
- Avira Mail Protection サービスは、アクティブですか？必要であれば、タスクバーで**スタート > 設定 > コントロール パネル**を選択し、サービスを有効にします。ダブルクリックで、**サービス**環境設定パネルを開始します（Windows XP では、サービス アプレットは、*管理ツール*のサブディレクトリに配置されます）。エントリ *Avira Mail Protection* を検索します。スタートアップの種類には自動、ステータスには開始と入力する必要があります。必要に応じて、該当するラインと、**開始**ボタンを選択してサービスを手動で開始します。 エラー メッセージが表示されたら、イベント表示を確認してください。うまくいかない場合は、**スタート > 設定 > コントロール パネル > プログラムの追加と削除**で Avira 製品をアンインストールし、Avira 製品を再インストールしてから、コンピュータを再起動する必要があります。

全般

SSL（Secure Sockets Layer、または TLS (Transport Layer Security)）を介した暗号化 POP3 接続は、現在保護することができないため、無視されます。

メール サーバーの検証は、現在パスワードでのみ対応しています。 Kerberos と RPA には、現在対応していません。

Avira 製品は、送信するメールのウィルスや不要プログラムのチェックは行いません。

> 注意
> セキュリティ ギャップをなくすため、定期的に Microsoft の更新プログラムをインストールすることをお勧めします。

TSL 接続を介して送信した電子メールが、Mail Protection にブロックされました。

原因：Transport Layer Security (TLS:インターネット上のデータ転送用暗号化プロトコル) は、現在、Mail Protection ではサポートされていません。
電子メールの送信には、次のオプションを使用することができます。

- SMTP によって使用されるポート 25 以外のポートを使用します。これによって、Mail Protection による監視がバイパスされます。
- 暗号化された TLS 接続をオフにし、電子メール クライアントで TLS サポートを無効にします。
- Mail Protection > スキャンの環境設定で、Mail Protection による送信メールの監視を（一時的に）無効にします。

Web チャットができません。チャットのメッセージが表示されません。データはブラウザに読み込まれています。

この現象は、チャンク転送エンコードを使用したHTTP プロトコル基盤のチャット中に、発生することがあります。

原因：Web Protection は、送信データが Web ブラウザに読み込まれる前に、ウィルスや不要プログラムがないか完全にチェックします

。チャンク転送コードを使用したデータ転送中、Web Protection は、メッセージの長さやデータ容量を判断できません。

- Web チャットの URL を例外として設定に入力します（環境設定参照：**Web Protection > スキャン > 例外**）。

7.2 ショートカット

キーボード コマンド (またはショートカット) - プログラムを通した迅速なナビゲーション、個々のモジュールのすばやい読み出しとアクションの開始を提供します。

以下に使用可能なキーボード コマンドの概要を記載します。
機能に関する詳細は、対応するヘルプの章に記載されています。

7.2.1 ダイアログ ボックス内

ショートカット	説明
Ctrl + Tab **Ctrl + Page down**	コントロール センターでのナビゲーション 次のセクションに移動。
Ctrl + Shift + Tab **Ctrl + Page up**	コントロール センターでのナビゲーション 前のセクションに移動。

←↑→↓	環境設定セクションでのナビゲーション まず、マウスを用いて環境設定セクションを開きます。 マークされたドロップダウン リストのオプション、またはオプション グループ内の複数のオプションの間で切替えます。
Tab	次のオプションまたはオプション グループに切替えます。
Shift + Tab	前のオプション、またはオプション グループに切替えます。
Space	アクティブなオプションがチェック ボックスの場合、チェック ボックスをアクティブまたは非アクティブにします。
Alt + **下線付き文字**	オプションを選択、またはコマンドを開始します。
Alt + ↓ **F4**	選択したドロップダウン リストを開きます。
Esc	選択したドロップダウン リストを閉じます。 コマンドをキャンセルして、ダイアログを閉じます。
Enter	アクティブなオプションまたはボタンに対応するコマンドを開始します。

7.2.2 ヘルプ内

ショートカット	説明
Alt + Space	システム メニューを表示します。
Alt + Tab	ヘルプと開いている他のウィンドウ間を切替えます。
Alt + F4	ヘルプを閉じます。
Shift + F10	ヘルプのコンテキスト メニューを表示します。
Ctrl + Tab	ナビゲーション ウィンドウで次のセクションに移動します。
Ctrl + Shift + Tab	ナビゲーション ウィンドウで前のセクションに移動します。
Page up	コンテンツ、インデックス、または検索結果のリストの上に表示されるテーマを切替えます。
Page down	コンテンツの現在のテーマ、インデックス、または検索結果のリストの下に表示されるテーマを切替えます。

Page up **Page down**	テーマを閲覧します。

7.2.3 コントロール センター内で

全般

ショートカット	説明
F1	ヘルプの表示
Alt + F4	コントロール センターを閉じる
F5	リフレッシュ
F8	環境設定を開く
F9	更新開始

スキャン セクション

ショートカット	説明
F2	選択したプロファイルの名前変更
F3	選択したプロファイルのスキャンを開始

F4	選択したプロファイルのデスクトップリンクの作成
Ins	新規プロファイルの作成
Del	選択したプロファイルの削除

隔離セクション

ショートカット	説明
F2	オブジェクトの再スキャン
F3	オブジェクトの復元
F4	オブジェクトの送信
F6	オブジェクトの復元先
Return	プロパティ
Ins	ファイルの追加

Del	オブジェクトの削除

スケジューラ セクション

ショートカット	説明
F2	ジョブの編集
Return	プロパティ
Ins	新規ジョブの挿入
Del	ジョブの削除

報告セクション

ショートカット	説明
F3	報告ファイルの表示
F4	報告ファイルの印刷
Return	報告の表示
Del	報告の削除

イベント セクション

ショートカット	説明
F3	イベントのエクスポート
Return	イベントの表示
Del	イベントの削除

7.3 Windows セキュリティ センター

- Windows XP Service Pack 2、Windows Vista -

7.3.1 全般

Windows セキュリティ
センターは、重要なセキュリティ観点から、コンピュータの状態をチェックします。

これらの重要点のいずれかで問題が検出されると（古いアンチウィルス
プログラム等）、セキュリティ
センターは、アラートを発して、コンピュータをより適切に保護する方法に関するアドバイスを提供します。

7.3.2 Windows セキュリティ センターおよび Avira 製品

アンチウィルス ソフトウェア／悪意のあるソフトウェアに対する保護

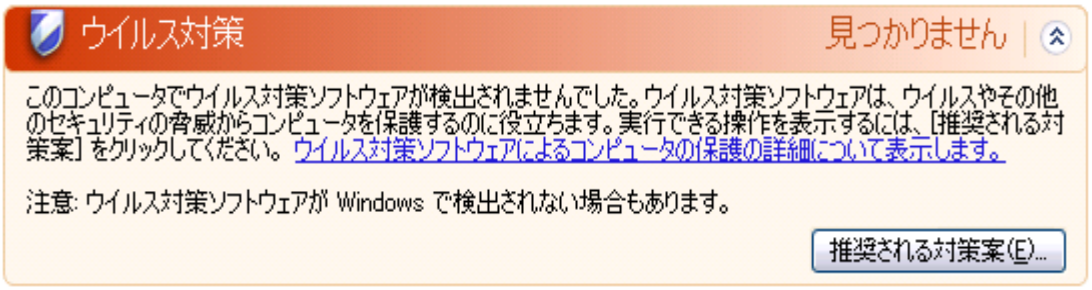
ウィルス対策に関して、Windows セキュリティ
センターから、次のような情報が送信される場合があります：

- ウィルス対策がありません
- ウィルス対策の有効期限が切れています

- ウィルス対策オン
- ウィルス対策オフ
- ウィルス対策が監視されていません

ウィルス対策がありません

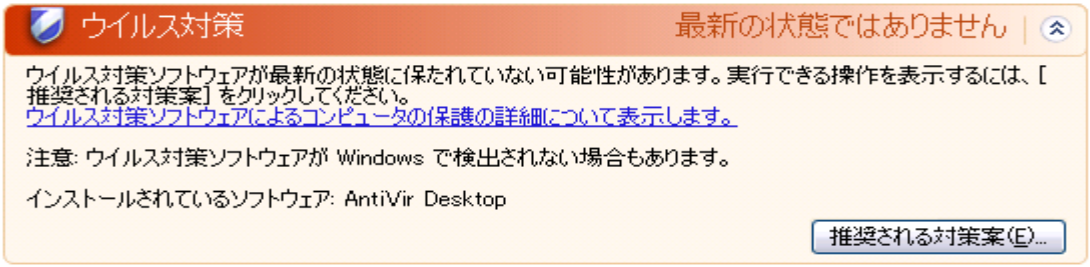
Windows セキュリティ
センターが、コンピュータ上でウィルス対策ソフトウェアを見つけることができなかった場合、このメッセージが表示されます。



> 注意
> Avira
> 製品をインストールして、コンピュータをウィルスやその他の不要プログラムから保護してください！

ウィルス対策の有効期限が切れています

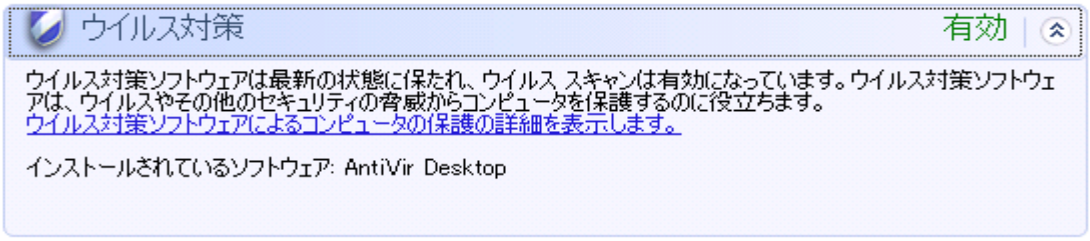
Windows XP Service Pack 2 または Windows Vista
をインストールしているシステムに Avira 製品をインストールしたり、Avira
製品を既にインストールしているシステムに Windows XP Service Pack 2 または Windows Vista をインストールすると、次のメッセージが表示されます：



> 注意
>
> Windows セキュリティ センターに、Avira
> 製品が最新であることを認識させるには、インストール後に更新する必要があります。 更新 を実行して、システムを更新してください。

ウィルス対策オン

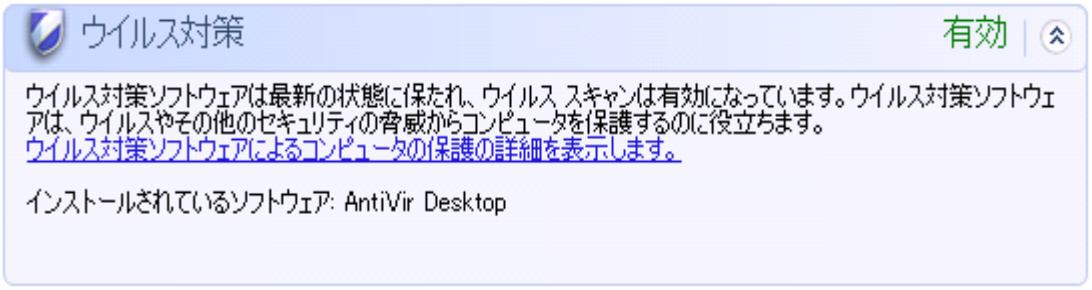
Avira
製品をインストールし、その後の更新手続きを適切に行っている場合、次のようなメッセージが届きます：



Avira 製品は、最新の状態です。Avira Real-Time Protection
は、有効になっています。

ウィルス対策オフ

Avira Real-Time Protection を無効にしたり、Real-Time Protection
サービスを停止すると、次のメッセージが表示されます。

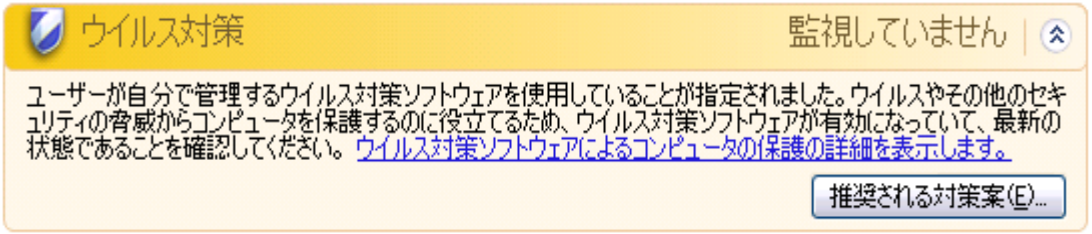


注意

コントロール センターのステータス セクションで、Avira Real-Time Protection を有効化/無効化することができます。 Avira Real-Time Protection
が有効かどうかは、タスクバーの赤い傘が開いているかどうかで確認することができます。

ウィルス対策が監視されていません

アンチウィルス ソフトウェアの監視をユーザー自身が行うことを希望すると、Windows セキュリティ センターから次のメッセージが表示されます。



注意

この機能は、Windows Vista には対応していません。

注意

Avira 製品は、Windows セキュリティ センターに対応しています。
このオプションは、**推奨対策案**ボタンで、いつでも有効にすることができます。

注意
Windows XP Service Pack 2 または Windows Vista
をインストールしていても、ウィルス対策は、必要です。 Windows
は、アンチウィルス
ソフトウェアを監視しますが、アンチウイルス機能を有しているわけではありません。
つまり、追加のウィルス対策ソリューション無しでは、ウィルスやマルウェアからコンピュータを保護することができないのです！

7.4 Windows アクション センター

- Windows 7 および Windows 8 -

7.4.1 全般

注意：
Windows 7 から、**Windows セキュリティ センター**が、新しく**Windows アクション センター**という名前に変更されました。
このセクションでは、全てのセキュリティ
オプションの状況をご覧いただくことができます。

Windows アクション
センターは、重要なセキュリティ観点から、コンピュータの状態をチェックします。
アクセスするには、タスクバーのフラッグをクリックしてください。もしくは、**コントロール パネル > アクション センター**を選択してください。

重要な問題が検出されると（期限切れのアンチウィルス プログラム等）、アクション
センターは、アラートを発して、コンピュータの適切な保護に関するアドバイスを提供します。
つまり、全てが適切に機能している場合、メッセージが送られることはありません。
セキュリティアイテムのWindows アクション

センターで、コンピュータのセキュリティ状態をチェックすることができます。

Windows アクション

センターは、インストールされているプログラムの管理オプションの提供や、適切なプログラムの選択も行います（例：*インストールしたスパイ対策プログラムの表示*）。

アクション

センターの設定変更で、警告メッセージの発信をオフにすることもできます（例：*スパイウェア関連の保護に関するメッセージをオフにする*）。

7.4.2 Windows アクション センターと Avira 製品

ウィルス対策

ウィルス対策に関して、Windows アクション
センターから、次のような情報が送信される場合があります。

- Avira Desktop 報告：最新の状態です。ウィルス スキャンは、オンの状態です。
- Avira Desktop 報告：オフの状態です。
- Avira Desktop 報告：最新の状態ではありません。
- Windows
  は、このコンピュータ上でウィルス対策ソフトウェアを見つけることができませんでした。
- Avira Desktop の有効期限が切れました。

Avira Desktop 報告：最新の状態です。ウィルス スキャンは、オンの状態です。

Avira 製品をインストールし、その後の更新手続きを適切に行っていれば、Windows アクション センターからメッセージが届くことはありません。 **アクション センター > セキュリティ**を開くと、「*Avira Desktop 報告：最新の状態です。ウィルス スキャンは、オンの状態です*」というメッセージが表示されています。 つまり、Avira 製品が、最新の状態であり、Avira Real-Time Protection
が、有効であることを意味しています。

Avira Desktop 報告：オフの状態です。

Avira Real-Time Protection を無効にしたり、Real-Time Protection サービスを停止すると、次のメッセージが表示されます。

注意

Avira コントロール センターのステータスせくしょｎで、Avira Real-Time Protection を有効化／無効化することができます。 Avira Real-Time Protection が有効かどうかは、タスクバーの赤い傘が開いているかどうかで確認することができます。 Windows アクション センター メッセージの「*オンにする*」ボタンをクリックして、Avira 製品を有効にすることもできます。 Avira を実行するかどうか、許可を求める通知が届きます。「*はい、発行元を信頼し、このプログラムを実行します*」をクリックすると、Real-Time Protection が、再び有効になります。

Avira Desktop 報告：最新の状態ではありません。

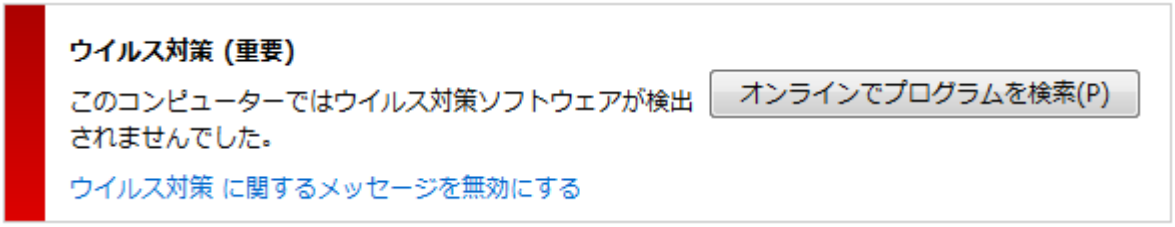
Avira をインストールしたばかりの場合、または何らかの理由により Avira のウイルス定義ファイル、スキャンエンジン、またはプログラムファイルが自動的に更新されない場合 (たとえば、Avira 製品がすでにインストールされている旧版の Windows オペレーティング システムから更新を行った場合) に次のメッセージが表示されます。

注意

Windows アクション センターに、Avira
製品が最新であることを認識させるには、インストール後に更新する必要があります。 更新を実行して、Avira 製品を更新してください。

Windows
は、このコンピュータ上でウィルス対策ソフトウェアを見つけることができませんでした。

Windows アクション
センターが、コンピュータ上でウィルス対策ソフトウェアを見つけることができなかった場合、このメッセージが表示されます。



注意

Windows Defender
にもウイルス保護機能が事前に設定されているため、Windows 8
ではこのオプションは表示されません。

注意

Avira

製品をインストールして、コンピュータをウィルスやその他の不要プログラムから保護してください！

Avira Desktop の有効期限が切れています。

Avira 製品のライセンスが切れると、Windows Action Center のこの情報が表示されます。
サブスクリプションの更新ボタンをクリックと、Avira ウェブサイトが表示され、新規のライセンスを購入できます。

注意
このオプションは、Windows 8でのみ使用できます。

スパイウェアおよび不要ソフトウェアからの保護

ウィルス対策に関して、Windows セキュリティ センターから、次のような情報が届く場合があります。

- Avira Desktop 報告：オンの状態です。
- Windows Defender と Avira Desktop はいずれもオフの状態です。
- Avira Desktop 報告：最新の状態ではありません。
- Windows Defender は、最新の状態ではありません。
- Windows Defender は、オフの状態です。

Avira Desktop 報告：オンの状態です。

Avira 製品をインストールし、その後の更新手続きを適切に行っていれば、Windows アクション センターからメッセージが届くことは、ありません。 **アクション センター > セキュリティ**を開くと、「*Avira Desktop 報告：オンの状態です*」と表示されています。 これは、Avira 製品が最新状態であり、Avira Real-Time Protection が有効であることを意味しています。

Windows Defender と Avira Desktop の報告：いずれもオフの状態です。

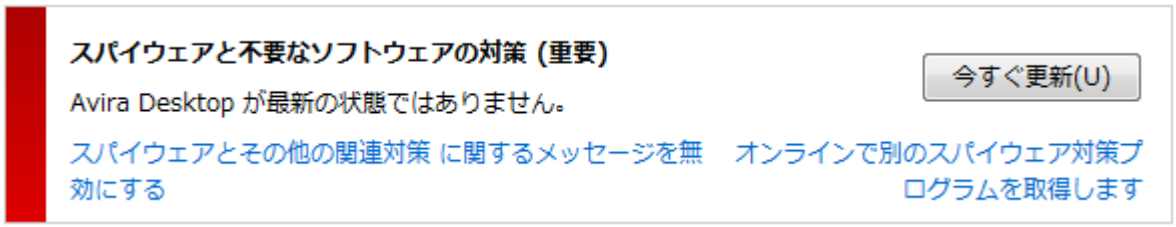
Avira Real-Time Protection を無効にしたり、Real-Time Protection サービスを停止すると、次のメッセージが表示されます。

注意

Avira コントロール センターのステータスせくしょｎで、Avira Real-Time Protection を有効化／無効化することができます。 Avira Real-Time Protection が有効かどうかは、タスクバーの赤い傘が開いているかどうかで確認することができます。 Windows アクション センター メッセージの「*オンにする*」ボタンをクリックして、Avira 製品を有効にすることもできます。 Avira を実行するかどうか、許可を求める通知が届きます。「*はい、発行元を信頼し、このプログラムを実行します*」をクリックすると、Real-Time Protection が、再び有効になります。

Avira Desktop 報告：最新の状態ではありません。

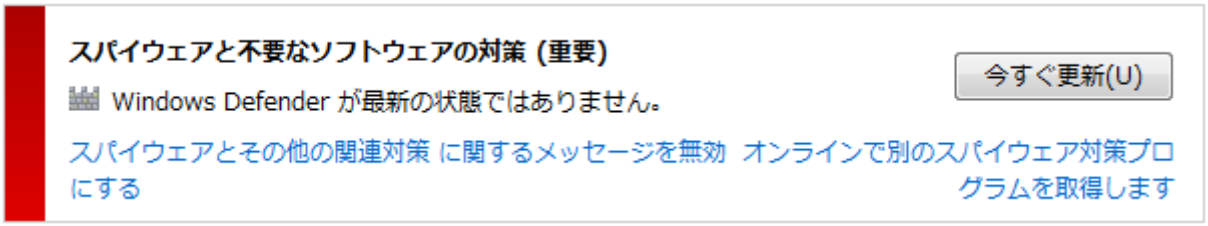
Avira をインストールしたばかりの場合、または何らかの理由により Avira のウイルス定義ファイル、スキャンエンジン、またはプログラムファイルが自動的に更新されない場合 (たとえば、Avira 製品がすでにインストールされている旧版の Windows オペレーティング システムから更新を行った場合) に次のメッセージが表示されます。



> 注意
>
> Windows アクション センターに、Avira 製品が最新であることを認識させるには、インストール後に更新する必要があります。 更新を実行して、Avira 製品を更新してください。

Windows Defender は、最新の状態ではありません

Windows Defender を起動した場合、次のようなメッセージが表示されます。 Avira 製品が既にインストールされている場合、このメッセージは表示されないはずです。インストールがきちんと行われたかどうか、確認してください。

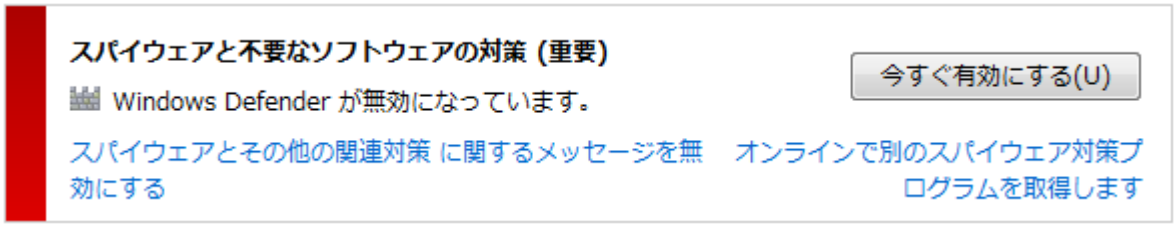


> 注意
>
> Windows Defender は、Windows で事前に設定されたスパイウェア

ソリューションで、Windows
のウイルス保護ソリューションとして提供されます。

Windows Defender は、オフの状態です

Windows アクション センターが、コンピュータ上で、デフォルト装備されている Windows Defender
以外のウィルス対策ソフトウェアを見つけることができなかった場合、このメッセージが表示されます。
以前、コンピュータにウィルス対策ソフトウェアをインストールしていた場合、このアプリケーションは、無効の状態になっています。 Avira
製品を既にインストールしている場合、このメッセージは表示されません。Avira
は、自動的に検知されます。
インストールがきちんと行われたかどうか、確認してください。



8. ウイルスなど

8.1 ウィルスなど

Avira Antivirus Premium
は、ウィルスやマルウェアを検出するだけではなく、その他の危険からコンピュータを保護します。
この章では、様々なマルウェアやその他の危険に関する概要をご覧いただけます。そのバック グラウンド、動き、待ち受けている不快な影響などを記載しています。

関連トピック：

- 脅威カテゴリ
- ウィルスとその他のマルウェア

8.2 脅威カテゴリ

アドウェア

アドウェアとは、コンピュータ画面にバナー広告やポップアップ
ウィンドウを表示するソフトウェアです。
これらの広告は、削除することができず、常に表示された状態にあります。
接続データが、インターネットの使用状況を示唆する情報を発生するため、データの保護という点で、問題のあるソフトウェアです。

Avira の製品は、アドウェアを検出します。
アドウェアオプションを有効にするには、環境設定の脅威カテゴリにチェックマークを入れます。そうすると、Avira
製品が、アドウェアを検出した場合、アラートを送信します。

アドウェア／スパイウェア

広告を表示したり、ユーザーが気付かないうちに、ユーザーの同意なく、個人データを第三者に送信したりする、好ましくないソフトウェアです。

Avira 製品は、「アドウェア／スパイウェア」を認識します。
アドウェア／スパイウェアオプションを有効にするには、環境設定の脅威カテゴリにチェックマークを入れます。そうすると、Avira
製品が、アドウェアもしくはスパイウェアを検知した場合、アラートを送信します。

アプリケーション

APPL
は、使用すると危険なリスクが含まれるアプリケーション、もしくは発信源が不審なアプリケーションを意味しています。

Avira 製品は、「Application (APPL)」を認識します。
アプリケーションオプションを有効にするには、環境設定の脅威カテゴリにチェックマークを入れます。そうすると、Avira
製品が、そのような動きを検出した場合、アラートを送信します。

バックドア クライアント

バックドア サーバー
プログラムは、データの盗難やコンピュータの操作を目的とし、ユーザーが知らない間にシステムに忍び込みます。 インターネットやネットワークを介し、バックドア
コントロール
ソフトウェア（クライアント）を使用することで、第三者が、このプラグラムを制御することが可能になります。

Avira 製品は、「バックドア コントロール ソフトウェア」を認識します。
バックドアオプションを有効にするには、環境設定の脅威カテゴリにチェックマークを入れます。そうすると、Avira
製品が、そのようなソフトウェアを検出した場合、アラートを送信します。

ダイヤラ

インターネットには、一部、有料のサービスがあります。
ドイツでは、そのようなサイトの請求は、0190／0900

というダイヤラ番号で行われます（もしくはオーストリア、スイスのダイヤラ番号 09x0／ドイツでは、中期的に 09x0 へ変更）。
これらのプログラムは、コンピュータに一度インストールされると、高額な支払い請求の原因となる割増料金番号を介した接続を確保し続けます。

電話の請求書を介したオンライン
コンテンツの販売は、合法です。ユーザーにとっても有益な場合があります。
正規のダイヤラは、意識的、意図的に、ユーザーの使用の意思を確認します。
明確に視覚に訴える形での表示、もしくはリクエストを介して得たユーザーの同意のもと、ユーザーのコンピュータにインストールされます。 正規のダイヤラのダイアルアッププロセスは、明確に表示されます。
また、正規のダイヤラは、発生した費用を正確に、間違いなく表示します。

残念ながら、ダイヤラの中には、ユーザーが気がつかないうちに勝手にインストールを実行してしまうものや、不適切な手段、もしくは詐欺的な意図のもとインストールを実行するものもあります。 例えば、このようなダイヤラは、インターネット ユーザーの ISP（インターネット サービス
プロバイダ）の既定データ通信リンクを置き換えます。そして、接続が行われる度に、高額な費用を発生する 0190／0900 番号へダイヤルします。
ユーザーは、コンピュータ上に不要な 0190／0900 ダイヤラ
プログラムが存在し、接続のたびに割り増し料金でダイヤルしていることに、電話料金の請求書が届くまで、気が付きません。その結果、極端に高い請求額を支払わなくてはならないことになります。

このような場合、電話会社に直接連絡し、不要なダイヤラ（0190／0900 ダイヤラ）への対策として、この番号を直ちにブロックするよう依頼することをお勧めします。

Avira 製品は、よく使用されるダイヤラを、規定で検出します。

ダイヤラオプションを有効にするには、環境設定の脅威カテゴリにチェックマークを入れます。そうすると、Avira
製品が、そのようなダイヤラを検出した場合、アラートを送信します。 不要な

0190／0900 ダイヤラを簡単に削除できます。 必要なダイアルアップ
プログラムである場合は、例外的なファイルであることを宣言すると、その後、そのファイルはスキャンされなくなります。

二重の拡張子ファイル

拡張子ファイルを、疑わしい方法で隠している実行ファイルです。
このカムフラージュ方法は、マルウェアによく使用されます。

Avira 製品は、「二重の拡張子ファイル」を認識します。
二重の拡張子ファイルオプションを有効にするには、環境設定の脅威カテゴリにチェックマークを入れます。そうすると、Avira
製品が、そのようなファイルを検出した場合、アラートを送信します。

詐欺的なソフトウェア

「スケアウェア」もしくは「ローグウェア」として知られるこのソフトウェアは、コンピュータがウィルスやマルウェアに感染していることを装う詐欺的なソフトウェアです。
このソフトウェアは、一見、プロフェッショナルなアンチウィルス
ソフトウェアに似ているように見えますが、ユーザーの不安感をあおり、ユーザーに脅威を与えるように構成されています。
（事実ではない）脅威をもって、被害者に恐怖心を与え、その脅威を除去するために、料金を支払わせることが、このソフトウェアの目的です。
中には、攻撃されていると被害者に信じ込ませ、本当に危険な攻撃を引き起こすアクションを、被害者自身が実行するように操作ガイドするケースもあります。

Avira 製品は、スケアウェアを検出します。
詐欺的なソフトウェアオプションを有効にするには、環境設定の脅威カテゴリにチェックマークを入れます。そうすると、Avira
製品が、そのようなファイルを検出した場合、アラートを送信します。

ゲーム

コンピュータ
ゲームは、とても楽しいものです。しかし、仕事中のゲームは、タブーです（昼食時間は、OK かもしれませんが）。
しかし、インターネットからダウンロード可能なゲームが多数あるため、かなり多くの会社員、公務員が、勤務中、マイン スイーパや Patience などのオンライン
ゲームを利用しています。
インターネットからは、様々なゲームがダウンロードできます。 電子メール
ゲームも、人気になりつつあります。シンプルなチェスから、「艦隊ゲーム」（ミサイル攻撃等）まで、様々な種類のゲームが、市場に出回っています。電子メール
プログラムで、パートナーに自分の動きを送信し、パートナーがそれに応答するという形で、ゲームが進められます。

勤務時間中、コンピュータゲームに使用される時間が、経済社会に深刻な影響を与える程の規模に達していることが、様々な調査により判明しています。
そのため、職場のコンピュータでのコンピュータ
ゲームを禁止する方法を考慮する企業が増えているのは、当然のことと言えます。

Avira 製品は、コンピュータ ゲームを認識します。
ゲームオプションを有効にするには、環境設定の脅威カテゴリにチェックマークを入れます。そうすると、Avira 製品が、ゲームを検出した場合、アラートを送信します。
ゲーム削除、つまり本当の意味で、ゲーム終了です。

ジョーク

ジョークとは、損害を与えたり、複製を作成したりするのではなく、ただ誰かを驚かせたり、楽しませることを目的としたプログラムです。 ジョーク
プログラムが読み込まれると、突然音を発生したり、ユニークな物体を画面に表示したりします。 例えば、ジョークには、ディスク
ドライブの洗濯機（DRAIN.COM）やスクリーン
イーター（BUGSRES.COM）などがあります。

しかし、気を付けてください！ ジョーク
プログラムの現象は、ウィルスやトロイの木馬が原因となっている可能性もあります。
自分自身で被害を引き起こしたとなれば、ユーザーは、大きなショックを受け、パニックに陥るはずです。

スキャンと識別ルーチンの拡張により、Avira 製品は、ジョーク
プログラムを検出し、必要に応じて、これらのファイルを不要プログラムとして排除します。
ジョークオプションを有効にするには、環境設定の脅威カテゴリにチェックマークを入れます。そうすると、Avira 製品が、ジョーク
プログラムを検出した場合、アラートを送信します。

フィッシング

フィッシングは、「ブランド スプーフィング」とも呼ばれ、インターネット サービス
プロバイダー、銀行、オンライン バンキング
サービス、登録認定機関などの顧客、顧客予備軍のデータを巧妙に盗む詐欺行為です。
電子メール アドレスの送信、オンライン フォームの入力、ニュースグループや Web
サイトへのアクセスをインターネット上で行うことにより、インターネットをクロールするスパイダによりデータが盗まれ、許可なく詐欺やその他の犯罪に使用される可能性があります。

Avira 製品は、「フィッシング」を認識します。
フィッシングオプションを有効にするには、環境設定の脅威カテゴリにチェックマークを入れます。そうすると、Avira
製品が、そのような動きを検出した場合、アラートを送信します。

個人のプライバシーを侵害するプログラム

システム セキュリティの侵害、不要なプログラム
アクティビティの起動、プライバシーの侵害、ユーザー行動の調査などを行うことができる、不要なソフトウェアです。

Avira 製品は、「セキュリティ プライバシ リスク」ソフトウェアを検出します。
個人のプライバシーを侵害するプログラムオプションを有効にするには、環境設定の脅威カテゴリにチェックマークを入れます。そうすると、Avira
製品が、そのようなソフトウェアを検出した場合、アラートを送信します。

通常とは異なるランタイム圧縮

通常とは異なるランタイム
パッカーで圧縮したため、疑わしいと分類されるファイルです。

Avira 製品は、「通常とは異なるランタイム パッカー」を認識します。
通常とは異なるランタイム圧縮オプションを有効にするには、環境設定の脅威カテゴリにチェックマークを入れます。そうすると Avira
製品が、そのようなパッカーを検出した場合、アラートを送信します。

8.3 ウィルスとその他のマルウェア

アドウェア

アドウェアとは、コンピュータ画面にバナー広告やポップアップ
ウィンドウを表示するソフトウェアです。
これらの広告は、削除することができず、常に表示された状態にあります。
接続データが、インターネットの使用状況を示唆する情報を発生するため、データの保護という点で、問題のあるソフトウェアです。

バックドア

バックドアは、コンピュータ アクセスのセキュリティ
メカニズムをすり抜けて、コンピュータへアクセスすることができます。

通常、バックグラウンドで実行されるプログラムは、攻撃者に無制限の権限を与えることになります。
バックドアにより、ユーザーの個人データが見つけ出される可能性もあります。

しかし、主に、バックドアは、関連システムにコンピュータ
ウィルスやワームをインストールするために使用されます。

ブート ウィルス

主に、ブート セクタ ウィルスが、ハード ディスクのブート、またはマスタ ブート
セクタに感染します。
これらのウィルスは、システム実行に必要な重要情報を上書きします。
最悪の場合、コンピュータ システムが読み込めなくなる場合もあります。

ボットネット

ボットネットとは、互いに通信するボットで構成された、（インターネット上の）PC
のリモート ネットワークと定義されます。
ボットネットは、共通のコマンドと制御インフラストラクチャの下で、（通常、ワームやトロイの木馬等と呼ばれる）プログラムを実行する、クラックされたコンピュータで構成されます。 ボットネットは、Dos
攻撃（サービス拒否攻撃）等を含む様々な用途に利用されます。通常、感染しているコンピュータのユーザーは、そのことに気がつきません。
ボットネットの怖さは、膨大な数のコンピュータで構成されるネットワークに成長する可能性があり、その全体の帯域幅が、通常のインターネット接続の帯域幅を越える場合もあるということです。

エクスプロイト

エクスプロイト（セキュリティ ギャップ）とは、コンピュータ
システムの権限昇格やサービス拒否を引き起こすバグ、誤作動、脆弱性を利用するコンピュータ プログラム、またはスクリプトです。
例えば、エクスプロイトのひとつの形態として、操作されたデータ
パッケージを使用したインターネットからの攻撃があります。
高度なアクセスを取得するため、プログラムに侵入します。

詐欺的なソフトウェア

「スケアウェア」もしくは「ローグウェア」として知られるこのソフトウェアは、コンピュータがウィルスやマルウェアに感染していることを装う詐欺的なソフトウェアです。
このソフトウェアは、一見、プロフェッショナルなアンチウィルス
ソフトウェアに似ているように見えますが、ユーザーの不安感をあおり、ユーザーに脅威を与えるように構成されています。
（事実ではない）脅威をもって、被害者に恐怖心を与え、その脅威を除去するために、料金を支払わせることが、このソフトウェアの目的です。
中には、攻撃されていると被害者に信じ込ませ、本当に危険な攻撃を引き起こすアクションを、被害者自身が実行するように操作ガイドするケースもあります。

デマウィルス

ここ数年、インターネット ユーザー、その他のネットワーク
ユーザーを対象に、電子メールを通じて広がると言う、実在しない、偽のウィルスに関するアラートが送信されています。
こういったアラートには、多くの人が危険に備えることができるように、その電子メールをできる限り多くの同僚や他のユーザーに送信するように、というリクエストが記載されています。そういった電子メールを介して、数多くの人々の間に広まっていきます。

ハニーポット

ハニーポットとは、ネットワークにインストールされているサービス（プログラムまたはサーバー）です。 その機能は、ネットワークやログ攻撃の監視です。
このサービスは、正規のユーザーには、あまり知られていません。そのため、正規のユーザーを対象とはしていませんでした。
攻撃者が、ネットワークのウィークポイントを探し、ハニーポットにより提供されているサービスを使用した場合、ハニーポットは、それを検知し、アラートを発生します。

マクロ ウィルス

マクロ ウィルスは、アプリケーションのマクロ言語（例：WinWord 6. の WordBasic）で書かれた小さなプログラムです。通常、そのアプリケーションのドキュメント（文書）内でのみ、感染を拡大することができます。
このため、文書ウィルスとも呼ばれます。
対応するアプリケーションが起動し、感染したマクロのひとつが実行されると、このウィルスは、アクティブになります。 「通常」のウィルスとは異なり、マクロ
ウィルスは実行ファイルの攻撃は行いませんが、対応するホスト
アプリケーションの文書を攻撃します。

ファーミング

ファーミングとは、Web ブラウザのホストファイルを操作して、Web
サイトの閲覧の問い合わせ処理を、スプーフィングされた偽装 Web
サイトに誘導する不正行為です。 従来のフィッシングを、さらに発展させた手口です。
ファーミング詐欺犯罪者は、偽装 Web サイトが保存されている独自の大型のサーバー
ファームを操作します。 ファーミングは、様々な DNS
攻撃の包括的用語として定着しています。 ホスト
ファイルを操作する場合、システムの具体的な操作は、トロイの木馬やウィルスを使用して行います。 その結果、正しい Web アドレスが入力されても、システムは、偽装 Web サイトにしかアクセスできなくなります。

フィッシング

フィッシングとは、インターネット ユーザーの個人データを釣るという意味です。
フィッシング犯罪者は、公式であることを装った電子メール等の文書を被害者に送付し、個人情報を記入するように仕向けます。特に、オンライン
バンキングのユーザーネーム、パスワード、PIN、TAN などが狙われます。
不正に入手したアクセス情報で、フィッシング犯罪者は、被害者になりすまし、被害者の名義で取引を行います。 銀行や保険会社が、クレジット

カード番号、PIN、TAN、その他のアクセス情報を、電子メール、SMS、または電話で問い合わせることは、絶対にありません。

ポリモフィック ウィルス

ポリモフィック ウィルスは、偽装の達人です。 自らのプログラム
コードを変えるため、検出は非常に困難です。

プログラム ウィルス

コンピュータ
ウィルスとは、実行され、感染を引き起こした後、他のプログラムに付着するプログラムです。 ウィルスは、ロジックボムやトロイの木馬とは異なり、自ら増殖します。
ワームとは対照的に、ウィルスは、ホストとしてのプログラムを必要とします。そこに、悪性コードを預けます。 ホストのプログラム実行は、原則として変更されません。

ルートキット

ルートキットは、コンピューター
システムへの侵入を確保した後、侵入者のログイン、プロセス、記録データを隠すため、つまり侵入者自身を見えない状態にするためのソフトウェア ツールの集合体です。
既にインストールされているスパイウェアの更新や、削除したスパイウェアの再インストールを試みます。

スクリプト ウイルスとワーム

この種のウィルスは、必要な技術さえ持っていれば、簡単に構成し、感染を拡大することができます。電子メールを介して、数時間で世界中に感染が拡大することもあります。

スクリプト ウィルスとワームには、Javascript、VBScript
などのスクリプト言語のいずれかが使用されており、自らを他の新しいスクリプトに挿入したり、オペレーティング システム機能を呼び出して広がっていきます。
これは電子メールやファイル（文書）のやり取りで、よく起こります。

ワームは、ワーム自体の操作を行い、ホストには感染することがないプログラムです。
このため、ワームが、他のプログラム シーケンスの一部を構成することはありません。
ワームは、制限的セキュリティ対策のシステムへの損傷を与えるプログラムを侵入させる唯一の方法として、よく使用されます。

スパイウェア

スパイウェアとは、スパイ
プログラムのことです。このプログラムは、ユーザーによる同意なく、コンピュータの操作を妨害したり、一部を制御したりします。
スパイウェアは、感染したコンピュータを営利目的で利用するために構成されています。

トロイの木馬

トロイの木馬は、現在、非常によく見られます。
トロイの木馬とは、特定の機能を持つように見せかけて、実行後に正体を表し、多くの場合、破壊的な機能を実行するプログラムです。
トロイの木馬は、自ら増殖できません。そこが、ウィルスやワームとは異なります。
多くの場合、ユーザーにトロイの木馬をスタートさせることを狙い、興味を惹きつけるような名前（SEX.EXE や STARTME.EXE）が付けられています。
実行されると直ちにアクティブになり、例えば、ハードディスクを初期化したりします。
ドロッパー型とは、ウイルスを「ドロップ」する、すなわちコンピュータ
システムにウィルスを埋め込み、内包する特殊な形態のトロイの木馬です。

ゾンビ

ゾンビ PC とは、マルウェア プログラムに感染しており、ハッカーが、リモート
コントロールで犯罪目的に利用できるコンピュータです。 感染した PC
は、コマンドに従い、例えば、サービス拒否（DoS）攻撃を開始したり、スパムメールやフィッシングメールを送信したりします。

9. 情報とサービス

この章には、当社への連絡方法に関する情報が記載されています。

- 参照：章 連絡先
- 参照：章 テクニカル サポート
- 参照：章 疑わしいファイル
- 参照：章 誤検出の報告
- 参照：章 フィードバックの送信

9.1 連絡先

Avira
製品ラインに関する質問、要望は、当社までお気軽にお寄せください。喜んでサポートさせていただきます。 **ヘルプ > Avira Antivirus Premium** についてのコントロールセンターに、連絡先が記載されています。ご参照ください。

9.2 テクニカル サポート

Avira サポートは、お客様の質問に対応し、技術的問題を解決します。

サポート サービスに関する必要な情報は、ウェブサイトでご覧いただけます：

http://www.avira.jp/premium-support

迅速で信頼できるサポートを提供するため、お客様には、次の情報を準備していただきます：

- **ライセンス情報** メニュー項目**ヘルプ > Avira Antivirus Premium** について > **ライセンス情報**のプログラム
  インターフェイスで、この情報を確認することができます。 参照 ライセンス情報.

- **バージョン情報**. メニュー項目**ヘルプ > Avira Antivirus Premium について > バージョン情報**のプログラム
  インターフェイスで、この情報を確認することができます。 参照 バージョン情報.
- **オペレーティング システムのバージョン**およびインストールされているサービス パック。
- **インストールされているソフトウェア パッケージ**、他のベンダーのアンチウィルス ソフトウェア。
- プログラム、またはレポート ファイルの**正確なメッセージ**。

9.3 疑わしいファイル

当社の製品によりまだ検出、削除されていないウィルスや疑わしいファイルは、当社宛てに送信してください。 この操作は、様々な方法で行うことができます。

- のコントロール センターの隔離マネージャでファイルを識別し、コンテキスト メニュー、または適切なボタンでアイテム**ファイルの送信**を選択します。
- 必要なファイルを圧縮し（WinZIP、PKZip、Arj 等）、電子メールに添付して、次のアドレスまで送信してください（ virus-premium@avira.jp ）。電子メール ゲートウェイのなかには、アンチウィルス ソフトウェアと連携して機能しているものもあるため、ファイルと共にパスワードを提出していただく必要があります（必ずパスワードを提供してください）。
- 当社のウェブサイトを介して、疑わしいファイルを送信することもできます（http://www.avira.jp/sample_upload）。

9.4 誤検出の報告

Avira
製品が「問題のない」ファイルを感染ファイルとして検出している可能性がある場合、適切な形式に圧縮し（WinZIP、PKZip、Arj,
等）、電子メールに添付して次のアドレスに送信してください：

virus-premium@avira.jp

電子メール ゲートウェイのなかには、アンチウィルス
ソフトウェアと連携して機能しているものもあるため、ファイルと共にパスワードを提出していただく必要があります（必ずパスワードを提供してください）。

9.5 フィードバックの送付

Avira は、お客様のセキュリティを第一に考えています。
そのため、製品をリリースする前に、エキスパート チームが、Avira
ソリューションの品質、安全性をテストしています。しかし、それだけではありません。
当社は、改善可能なセキュリティ関連のギャップについてのご指摘を、大変重要だと考えています。そのようなご指摘には、真剣に対応させていただきます。

当社の製品のセキュリティ
ギャップを検出した場合は、次のアドレスまで電子メールを送信してください：

vulnerabilities-premium@avira.jp

10. リファレンス: 環境設定オプション

環境設定リファレンスはすべての使用可能な環境設定オプションを網羅しています。

10.1 System Scanner

環境設定の**System Scanner**部で、オンデマンド スキャンの環境設定を行います。
(オプションはエキスパート モードでのみ使用可能。)

10.1.1 スキャン

オンデマンド スキャン ルーチンの挙動を決めることができます
(オプションはエキスパート モードでのみ使用可能)。
スキャンする特定のディレクトリを選択する場合、System
Scannerは環境設定に応じてスキャンします:

- 特定のスキャン順位で、
- ブートセクターとメインメモリーも含めて、
- ディレクトリ内のすべてあるいは選択されたファイル、

ファイル

System
Scannerは特定の拡張子(形式)を伴うファイルのスキャン専用にフィルターを使用することができます。

全ファイル

このオプションが有効な場合、コンテンツとファイル拡張子に関係なく全ファイルがウィルスあるいは迷惑プログラムについてスキャンされます。
フィルターは使用されません。

注記

全ファイルが有効な場合、ボタンファイル拡張子は選択できません。

スマート拡張子の使用

このオプションが有効な場合、ウィルスあるいは迷惑プログラムについてスキャンされるファイルはプログラムによって自動的に選択されます。
つまり、Aviraプログラムがファイルのコンテンツに応じてスキャンの実行を決めます。
この方法はファイル拡張子リストの使用よりも幾分遅いですが、ファイル拡張子だけをベースにスキャンするわけではないために、より安全です。
このオプションはデフォルト設定で有効で、推薦されます。

注記

スマート拡張子の使用が有効な場合、ボタンファイル拡張子は選択できません。

ファイル拡張子リストの使用

このオプションが有効な場合、特定の拡張子を伴うファイルだけがスキャンされます。
ウィルスあるいは迷惑プログラムの保有可能なすべてのファイル形式がセットされています。 リストはボタン"**ファイル拡張子**"を用いて手動で編集可能です。

注記

このオプションが有効で、ファイル拡張子を伴うリストからすべてのエントリを削除している場合、これはテキスト "*ファイル拡張子なし*"
で表示されます(ボタンファイル拡張子で)。

ファイル拡張子

このボタンで、**"ファイル拡張子リストの使用"**
モードでスキャンされるすべての拡張子が表示される、対話ボックスが開かれます。

デフォルト
エントリは拡張子のためにセットされていますが、エントリは追加、削除が可能です
。

> 注記
> デフォルトリストはバージョン毎に違うことがありますので注意してください
> 。

追加の設定

選択されたドライブのブートセクターのスキャン

このオプションが有効な場合、System
Scannerはシステムスキャン用に選択されたドライブのブートセクターをスキャンします。 このオプションは、初期状態で有効に設定されています（デフォルト設定）。

マスター ブートセクターのスキャン

このオプションが有効な場合、System
Scannerはシステムで使用されるハードディスクのマスター
ブートセクターをスキャンします。

オフライン ファイルの無視

このオプションが有効な場合、ダイレクトスキャンはスキャン中にいわゆるオフライン ファイルをすべて無視します。
これは、これらのファイルがウィルスあるいは迷惑プログラムのスキャンから免れることを意味します。 オフライン
ファイルは、いわゆる階層型記録管理システム(HSMS)によってハードディスクからたとえばテープへ物理的に移動されたファイルのことです。
このオプションは、初期状態で有効に設定されています（デフォルト設定）。

システムファイルの整合性チェック

このオプションが有効な場合、最も重要なWindowsのシステムファイルは各オンデマンド
スキャンにおいてマルウェアによる改変の特別な安全チェックの対象となります。
改変されたファイルが検出される場合、これは疑惑として報告されます。
この機能は、多くのコンピューター能力を使用します。
そのために、デフォルト設定ではこのオプションは無効となっています。

> 注記
> このオプションはWindows Vista以降でのみ使用可能です。

> 注記
> このオプションは、システムファイルを変更してブートあるいはスタートスクリーンを貴独自の必要条件に適合させる第3者ツールを使用している場合には、使用しないでください。
> そのようなツールの例としては、skinpacks、TuneUp utilities あるいはVista Customizationが挙げられます。

最適化スキャン

このオプションが有効な場合、プロセッサー能力はSystem Scannerスキャン時に最適に活用されます。
パフォーマンス上の理由により、合理化スキャンは標準レベルでのみスタートします。

> 注記
> このオプションは、マルチプロセッサー システム上でのみ使用できます。

シンボル リンクに追従

このオプションが有効な場合、System Scannerはスキャンプロファイル内のすべてのシンボルリンクあるいは選択されたディレクトリに従って、リンクされたファイルをウィルスあるいはマルウェアについてスキャンします。

> 注記
> オプションはショートカットを含めませんが、ファイルシステム内で明白なシンボルリンク(mklink.exeにより生成)あるいはジャンクション ポイント(junction.exeにより生成)だけは許容します。

スキャン前のルートキットの調査

このオプションが有効でスキャンが開始している場合、System ScannerはWindowsシステム ディレクトリをいわゆるショートカット内でアクテイブなルートキットについてスキャンします。
このプロセスは貴コンピューターをアクティブなルートキットについて、スキャンプロファイル"**ルートキットのスキャン**"ほど広範にスキャンしませんが、実行は顕著に高速です。
このオプションは、ユーザーにより作成されたプロファイルの設定を変更します。

> 注記
> ルートキットスキャンはWindows XP 64 bit

レジストリのスキャン

このオプションが有効な場合、レジストリはマルウェア照合についてスキャンされます。
このオプションは、ユーザーにより作成されたプロファイルの設定を変更します。

ネットワーク ドライブ上のファイルとパスの無視

このオプションが有効な場合、コンピューターへ接続されているネットワークドライブはオンデマンド スキャンから除外されます。
このオプションは、サーバーあるいは他のワークステーション自体がアンチウィルスソフトウェアで保護されている場合に推薦されます。
このオプションはデフォルト設定で無効です。

スキャンプロセス

スキャナーの停止を許可

このオプションが有効な場合、ウィルスあるいは迷惑プログラムのスキャンはいつでも"Luke Filewalker"ウィンドウ内のボタン"**停止**"で停止させることができます。
この設定を無効化している場合、"Luke Filewalker"ウィンドウ内の**停止**ボタンは灰色表示されます。 スキャンプロセスの尚早終了は不可能です！
このオプションは、初期状態で有効に設定されています（デフォルト設定）。

スキャナー順位

System Scannerはオンデマンド スキャンの順位レベル間を区別します。
これはワークステーション上で複数のプロセスが同時に進行している場合にだけ有益です。 選択はスキャン速度に影響します。

低

System Scannerは、他のプロセスがコンピューター使用時間を要求しない場合にだけOSからプロセッサー時間を割当てられます。つまりSystem Scannerだけが進行中は、その速度は最大です。
しかしながら、他のプログラムとの作動が理想的です。System Scannerが背景で継続作動している間に他のプログラムがコンピューター使用時間を要求する場合のほうが、コンピューターはよりすばやく反応します。

普通

System Scannerは通常順位で実行されます。
すべてのプロセスは、OSによって同等のプロセッサー時間量を割当てられます。
このオプションはデフォルト設定で有効で、推薦されます。
特定状況の下では、他のアプリケーションとの同時稼動は影響を受けることがあります。

高

System Scannerは最高の順位で稼動します。
他のアプリケーションとの同時稼動はほとんど不可能です。
いずれにしても、System Scannerは完全なスキャンを最大速度で実行します。

検出アクション

ウィルスあるいは迷惑プログラムが検出された場合になすべきアクションを、System Scannerにて決定することができます。 (オプションはエキスパート
モードでのみ使用可能。)

インタラクティブ

このオプションが有効な場合、スキャンの結果は対話ボックスで表示されます。
System
Scannerでスキャンが実行される場合、スキャン後には感染ファイルのリストと共に警告が発動されます。
各種の感染ファイルの処理アクションを選択するためには、コンテンツ繊細メニューを使用することができます。
すべての感染ファイルに標準アクションを実行する、あるいはSystem
Scannerをキャンセルすることもできます。

> 注記
> アクション**隔離**は、System
> Scannerの通知内でデフォルトとして事前選択されています。
> その他のアクションはコンテキスト メニューで選択することができます。

自動

このオプションが有効な場合、対話ボックスはウィルス検出時に表示されません。System
Scannerはこのセクションにおける一次的、二次的アクションとしての設定に基づいて対応します。

アクション前にファイルを隔離へコピー

このオプションが有効な場合、System
Scannerは要求される一次あるいは二次アクションが実行される前にバックアップコピーを作成します。
バックアップコピーは隔離内に保存され、情報価値を含む場合にはそこで復元することができます。 より詳細な調査のために、バックアップコピーをAvira マルウェアリサーチセンターへ送付することもできます。

一次アクション

一次アクションは、System
Scannerがウィルスあるいは迷惑プログラムを検出したときに実行されるアクションです。
オプション"**修復**"が選択されていて、しかし感染ファイルが修復できない場合には、"**二次アクション**"で選択されているアクションが実行されます。

> 注記
> オプション二次アクションは、**修復**設定が一次アクションで選択されている場合だけ、選択することができます。

修復

このオプションが有効な場合、System
Scannerは感染ファイルを自動的に修復します。 System
Scannerが感染ファイルを修復できない場合、二次アクションで選択されているアクションが実行されます。

注記
自動修復が推薦されますが、それはSystem Scannerがファイルをワークステーション上で変更することを意味します。

名称変更

このオプションが有効な場合、System Scannerはファイルを名称変更します。そのために、当ファイルにはもう直接アクセスできません(たとえばダブルクリック等で)。 しかしファイルは後に修復可能で、再び元の名を与えることができます。

隔離

このオプションが有効な場合、System Scannerはファイルを隔離に移動させます。これらのファイルは後に修復する、あるいは必要に応じてAviraマルウェアリサーチセンターに送付して復元させることができます。

削除

このオプションが有効な場合、ファイルは削除されます。このプロセスは、「上書きと削除」よりもはるかに高速です。

無視

このオプションが有効な場合、ファイルへのアクセスが許可され、ファイルはそのままに留まります。

警告
汚染されたファイルはワークステーション上で有効中です!
ワークステーションに重大なダメージを与える恐れがあります！

上書きと削除

このオプションが有効な場合、System Scannerは、ファイルをデフォルト形式で上書きしてから削除します。これはもう復元できません。

二次アクション

オプション"二次アクション"は、修復設定が"一次アクション"で選択されている場合だけ、選択することができます。
このオプションで、感染ファイルが修復できない場合のアクションを決めます。

名称変更

このオプションが有効な場合、System Scannerはファイルを名称変更します。
そのために、当ファイルにはもう直接アクセスできません(たとえばダブルクリック等で)。 しかしファイルは後に修復可能で、再び元の名を与えることができます。

隔離

このオプションが有効な場合、System Scannerはファイルを隔離に移動させます。
これらのファイルは後に修復する、あるいは必要に応じてAviraマルウェアリサーチセンターに送付して復元させることができます。

削除

このオプションが有効な場合、ファイルは削除されます。
このプロセスは、「上書きと削除」よりもはるかに高速です。

無視

このオプションが有効な場合、ファイルへのアクセスが許可され、ファイルはそのままに留まります。

警告
汚染されたファイルはワークステーション上で有効中です!
ワークステーションに重大なダメージを与える恐れがあります！

上書きと削除

このオプションが有効な場合、System Scannerは、ファイルをデフォルト形式で上書きしてから削除(消去)します。
これはもう復元できません。

注記

削除 あるいは **上書きと削除**
を一次あるいは二次アクションとして選択している場合には以下に注意してください:
ヒューリスティクが含まれるケースでは感染ファイルは削除されず、隔離へ移動されます。

アーカイブ

アーカイブをスキャンする場合、System Scannerは再帰的なスキャンを使用します。アーカイブ内のドキュメントは開梱されてウィルスあるいは迷惑プログラムのスキャンを実行されます。
ファイルはスキャンされ、解凍され、そして再びスキャンされます。
(オプションはエキスパート モードでのみ使用可能。)

アーカイブのスキャン

このオプションが有効な場合、アーカイブリスト内の選択されたアーカイブはスキャンされます。 このオプションはデフォルト設定で有効です。

全アーカイブ形式

このオプションが有効な場合、アーカイブリスト内の全アーカイブ形式が選択されてスキャンされます。

スマート拡張子

このオプションが有効な場合、System Scannerはファイルが梱包されたファイル形式(アーカイブ)かどうか、ファイル拡張子が通常の拡張子と異なるかどうかを検出して、アーカイブをスキャンします。
いずれにしても各ファイルはこのために開梱する必要があり、これはスキャン速度を減速します。 例: *.zipアーカイブがファイル拡張子 *.xyzを持っている場合、System Scannerはこのアーカイブも開梱してスキャンします。
このオプションはデフォルト設定で有効です。

注記
アーカイブリストにマークされているアーカイブ形式だけがサポートされます。

再帰深さの制限

再帰アーカイブの開梱およびスキャンは、コンピューターに多大な時間とリソースに負担をかけます。
このオプションが有効な場合、スキャンの深さをマルチ梱包アーカイブから特定の梱包レベル数へ制限することができます(最大再帰深さ)。
これは時間ならびにコンピューターのリソース(メモリー)の負担を軽減します。

注記
アーカイブでのウィルス等の検出のために、System Scannerはウィルスあるいは迷惑プログラムの存在する再帰レベルまでスキャンしなければなりません。

最大再帰深さ

最大再帰深さを得るには、オプション再帰深さの制限を有効化する必要があります。
要求する再帰深さを直接記入する、あるいはエントリー欄上で右矢印キーを用いて記入します。 許可されるバリューは1 ～ 99です。
推薦される標準バリューは20です。

デフォルト バリュー

このボタンは、アーカイブ スキャン用のデフォルト バリューを決めます。

アーカイブ

この表示領域では、System Scannerがスキャンするべきアーカイブをセットすることができます。
そのためには、関連エントリーを選択してください。

除外

System Scannerを省略されるファイル オブジェクト (オプションはエキスパートモードでのみ使用可能。)

このウィンドウ内のリストは、System Scannerによるウィルスあるいは迷惑プログラムのスキャンに含まないファイルとそのパスを収納しています。

ここではできる限り除外を少なく、理由の如何に関わらず通常スキャンに含めないファイルだけを記入してください。
これらのファイルをこのリストに含める前に、これらには常にウィルスあるいは迷惑プログラムのスキャンを実行することを推薦します！

> 注記
> リスト内のエントリーは総計で6000文字を超えないこと。

> **警告**
> これらのファイルはスキャンに含まれていません！

> 注記
> このリストに含まれるファイルは、報告ファイル内に記録されます。
> ここに除外した理由がもうない、スキャンされていないファイルがないか、時々報告ファイルをチェックしてください。
> このような場合、このファイルの名をリストから削除してください。

入力ボックス

この入力ボックスには、オンデマンド スキャンに含まれていないファイル オブジェクトの名称を記入することができます。 デフォルト設定ではファイル オブジェクトは記入されません。

...

ボタンは、要求されるファイルあるいはパスが選択できるウィンドウを開きます。
ファイル名とその完全なパスを入力すると、このファイルだけがスキャンを免れます。
パスなしでファイル名を入力すると、パスあるいはドライブに関わりなくこの名のすべてのファイルがスキャンされません。

追加

このボタンで、入力ボックスに記入されたファイル
オブジェクトを表示ウィンドウへ追加することができます。

削除

このボタンは選択されたエントリーをリストから削除します。
このボタンはエントリーが選択されていない場合は非作動です。

ヒューリスティク

この環境設定セクションには、スキャンエンジンのヒューリスティク用の設定が含まれます。 (オプションはエキスパート モードでのみ使用可能。)

Avira製品には強力なヒューリスティク機能が含まれており、これによってダメージエレメントに対抗するための特殊ウィルス形跡が確定される前に、またウィルスガードの更新が実行される前に、未知のマルウェアが事前にキャッチされます。
ウィルス検出にはマルウェアの典型的な機能の大規模な解析ならびに感染コードの調査が含まれます。スキャンされたコードがそれらの典型的な特徴を示す場合、それは疑惑として報告されます。これは、必ずしもコードがマルウェアと確定されたわけではありません。時には間違いの陽性反応が発生する可能性があります。コードソースが信頼性のあるものかどうかの、感染コードの処理に関する決定は、ユーザーが自身の知識に基づいて行います。

マクロウィルス ヒューリスティク

マクロウィルス ヒューリスティク

Avira製品には、高性能なマクロウィルス
ヒューリスティク(発見的問題解決法)が含まれています。
このオプションが有効な場合、関連ドキュメント内のすべてのマクロはリペア処理によって削除される、または代替として疑惑ドキュメントとして報告され、警告が発動されます。このオプションはデフォルト設定で有効にすることが推薦されます。

上級ヒューリスティク解析&検出(AHeAD)

AHeADの有効化

Aviraプログラムには、Avira AHeAD
テクノロジーに基づく高性能なヒューリスティク機能が含まれており、これは未知の(新たな)マルウェアも検出します。
このオプションが有効な場合、このヒューリスティクの「積極性」を設定することができます。 このオプションはデフォルト設定で有効です。

低検出レベル

このオプションが有効な場合、未知マルウェアの検出度合いはわずかに減少され、それによって間違い警告のリスクは減少します。

中検出レベル

このオプションは、高検出レベルと間違い警告の低リスクを組み合わせています。
中レベルは、このヒューリスティクの活用が選択される場合にデフォルト設定となります。

高検出レベル

このオプションが有効な場合、未知のマルウェアが著しく検出されます、しかし単なる間違い陽性反応のリスクも多くなります。

10.1.2 報告

System Scannerは広範な報告機能を持っています。 従って、オンデマンドスキャンの結果に関して正確な情報を受け取ることができます。

報告ファイルはシステムのすべてのエントリーならびにオンデマンドスキャンの警告やメッセージを含んでいます。 (オプションはエキスパートモードでのみ使用可能。)

> 注記
> ウィルスあるいは迷惑プログラムの検出時にSystem Scannerが実行したアクションを閲覧するには、報告ファイルをエキスパートモードの環境設定内で有効化する必要があります。

報告

オフ

このオプションが有効な場合、System Scannerはオンデマンドスキャンのアクションならびに結果を報告しません。

デフォルト

このオプションが有効な場合、System Scannerは該当ファイルの名とパスを記録します。
さらに、現在スキャンの環境設定、バージョン情報ならびにライセンス情報が報告ファイル内に記載されます。

拡張

このオプションが有効な場合、System Scannerは警告とヒントをデフォルト情報への追加として記載します。
報告には、Cloud Protectionによる検出の識別のための[クラウド]拡張子も含まれます。

完全

このオプションが有効な場合、System Scannerはすべてのスキャン済みファイルも記録します。

さらに、関連するすべてのファイル、警告ならびにヒントが報告ファイル内に含まれます。

注記
トラブルシューティングのために、報告ファイルをいつでも弊社へご送付ください。なお、報告ファイルはこのモード(完全)で作成願います。

10.2 Real-Time Protection

環境設定の**Real-Time Protection**セクションで、オンアクセス
スキャンの環境設定を行います。 (オプションはエキスパート モードでのみ使用可能。)

10.2.1 スキャン

通常はシステムの一貫した監視が望ましいです。 この終了時にはReal-Time Protection (=オンアクセス System Scanner)を使用します。
このように、"オンザフライ"コンピューターでコピーされ、開かれるすべてのファイルをウィルスあるいは迷惑プログラムについてスキャンすることができます。
(オプションはエキスパート モードでのみ使用可能。)

ファイル

Real-Time
Protectionは、特定の拡張子(形式)を持つそれらのファイル専用のスキャンにフィルターを使用することができます。

全ファイル

このオプションが有効な場合、それらのコンテンツとファイル拡張子に関係なく全ファイルがウィルスあるいは迷惑プログラムについてスキャンされます。

注記
全ファイルが有効な場合、ボタン**ファイル拡張子**は選択できません。

スマート拡張子の使用

このオプションが有効な場合、ウィルスあるいは迷惑プログラムについてスキャンされるファイルはプログラムによって自動的に選択されます。
つまり、プログラムがファイルのコンテンツに応じてスキャンの実行を決めます。
この方法はファイル拡張子リストの使用よりも幾分遅いですが、ファイル拡張子だけをベースにスキャンするわけではないために、より安全です。

注記
スマート拡張子の使用が有効な場合、**ファイル拡張子**ボタンは選択できません。

ファイル拡張子リストの使用

このオプションが有効な場合、特定の拡張子を伴うファイルだけがスキャンされます。
ウィルスあるいは迷惑プログラムの保有可能なすべてのファイル形式がセットされています。
リストはボタン"**ファイル拡張子**"を用いて手動で編集可能です。このオプションはデフォルト設定で有効で、これが推薦されます。

注記
このオプションが有効で、ファイル拡張子を伴うリストからすべてのエントリーを削除している場合、これはボタン**ファイル拡張子**においてテキスト「ファイル拡張子なし」で表示されます。

ファイル拡張子

このボタンで、**"ファイル拡張子リストの使用"**
モードでスキャンされるすべての拡張子が表示される、対話ボックスが開かれます。
デフォルト
エントリーは拡張子のためにセットされていますが、エントリーは追加、削除が可能です。

> 注記
> デフォルトリストはバージョン毎に違うことがありますので注意してください。

スキャン モード

ここでは、ファイルのスキャン時間を定義します。

読取り時にスキャン

このオプションが有効な場合、Real-Time Protectionはファイルの読取り前にあるいはアプリケーションまたはOSで実行される前に、ファイルをスキャンします。

書込み時にスキャン

このオプションが有効な場合、Real-Time Protectionは書込み時にファイルをスキャンします。
このプロセスが完結した後にはじめて、ファイルにアクセスすることができます。

読取り/書込み時にスキャン

このオプションが有効な場合Real-Time Protectionは、開き、読取り、実行の前にそして書込み後にファイルをスキャンします。 このオプションはデフォルト設定で有効で、それが推薦されます。

ドライブ

ネットワーク ドライブの監視

このオプションが有効な場合、サーバー ボリューム、ピアドライブ等のネットワークドライブ(マップドライブ)上のファイルがスキャンされます。

注記

コンピューター性能を落とし過ぎないために、オプション**ネットワークドライブの監視**は例外的ケースにだけ許可してください。

警告

このオプションが無効な場合、ネットワーク ドライブは監視されません。これらはもう、ウィルスあるいは迷惑プログラムに対して保護されません！

注記

ファイルがネットワークドライブ上で実行されるときには、それらは**ネットワークドライブの監視**オプションの設定に関係なくReal-Time Protectionでスキャンされます。 でのいくつかの例では、ネットワークドライブ上のファイルは、**ネットワークドライブの監視**オプションが無効中でも、開かれているときにはスキャンされます。 理由:

これらのファイルは、‘ファイルの実行’権でアクセスされるためです。

これらのファイルを除外したい場合、あるいはネットワークドライブ上の実行済みファイルをReal-Time Protectionスキャンから除外したい場合は、ファイルを除外ファイルオブジェクトのリスト内へ挿入します(Real-Time Protection > スキャン > 除外を参照)。

キャッシュの許可

このオプションが有効な場合、ネットワークドライブ上の監視されるファイルはReal-Time Protectionのキャッシュ内で使用可能になります。

キャッシュ機能なしのネットワークドライブの監視はより確実ですが、キャッシュ付きのネットワークドライブの監視ほど性能は良くはありません。

アーカイブ

アーカイブのスキャン

このオプションが有効な場合、アーカイブはスキャンされます。
圧縮ファイルはスキャンされ、解凍され、そして再びスキャンされます。
このオプションは、デフォルトで無効です。
アーカイブスキャンは、再帰深さ、スキャンされるファイル数ならびにアーカイブ容量に応じて制限されます。
最大再帰深さ、スキャンされるファイル数ならびに最大アーカイブ容量を設定することができます。

> 注記
> このオプションは、プロセスがコンピューターの性能に大きな負担を掛けるため、デフォルトで無効です。 これは通常、アーカイブがオンデマンドスキャンを用いてチェックされる場合に推薦されます。

最大再帰深さ

アーカイブをスキャンする場合、Real-Time Protectionは再帰的なスキャンを使用します。アーカイブ内のドキュメントは開梱されてウィルスあるいは迷惑プログラムのスキャンを実行されます。
再帰深さは定義することができます。
再帰深さのデフォルト値は1で、これが推薦されます:
メインアーカイブ内に直接位置付けされているすべてのファイルはスキャンされます。

最大ファイル数

アーカイブのスキャン時には、スキャンをアーカイブ内の最大ファイル数に制限することができます。
スキャンされる最大ファイル数のデフォルト値は10で、これが推薦されます。

最大容量 (KB)

アーカイブのスキャン時には、スキャンを開梱される最大アーカイブ容量に制限することができます。 1000 KBの標準値が推薦されます。

検出時のアクション

ウィルスあるいは迷惑プログラムが検出された場合になすべきアクションを、Real-Time Protectionにて決定することができます。 (オプションはエキスパート
モードでのみ使用可能。)

インタラクティブ

このオプションが有効な場合、Real-Time
Protectionがウィルスあるいは迷惑プログラムを検出した時にスクリーン通知が現れます。
検出されたマルウェアを削除する、あるいは"**詳細**"ボタンを経由してその他の可能なウィルス処理アクションにアクセスするオプションがあります。
それらのアクションは対話ボックス内に表示されます。
このオプションは、初期状態で有効に設定されています（デフォルト設定）。

許可されたアクション

この表示ボックスには、対話ボックス内でその他のアクションとして使用可能なウィルス管理アクションを指定することができます。
このためには対応オプションを有効化する必要があります。

修復

Real-Time Protectionは可能な限り、感染ファイルを修復します。

名前の変更

Real-Time Protectionはファイルの名称を変更します。
これらのファイルへ直接アクセスすること（ダブルクリックなど）は、不可能になります。 ファイルは、後の時間に再度修復および名称変更をおこなうことができます。

隔離

Real-Time Protectionはファイルを隔離へ移動させます。
ファイルは、情報価値を含む場合、隔離マネジャーによって復元する、あるいは必要に応じてAviraマルウェア リサーチセンターに送付して復元させることができます。
ファイルによっては、その他の選択オプションが隔離マネジャー内で使用可能です。

削除

ファイルの削除が行われます。
このプロセスは**上書きと削除**よりもはるかに高速です(下記を参照)。

無視

ファイルへのアクセスは許可され、ファイルは無視されます。

上書きおよび削除

Real-Time Protectionは、削除する前にファイルをデフォルト形式で上書きします。
この処理を施したファイルは、復元不能になります。

警告
Real-Time Protectionが**書込み時にスキャン**に設定されている場合、感染ファイルは書込みされません。

既定

このボタンによってデフォルトで、ウィルス検出時に対話ボックスでアクションを選択することができます。
デフォルトで有効化されるアクションを選択して、"**デフォルト**"ボタンをクリックします。

注記
アクション**修復**はデフォルト アクションとして選択できません。

詳細情報はここをクリックします。

自動

このオプションが有効な場合、対話ボックスはウィルス検出時に表示されません。
Real-Time
Protectionは、このセクションにおける一次的、二次的アクションとしての設定に基づいて対応します。

アクション前にファイルを隔離へコピー

このオプションが有効な場合、Real-Time
Protectionは要求される一次あるいは二次アクションが実行される前にバックアップコピーを作成します。 バックアップコピーは隔離内に保存されます。
それは情報価値を含む場合、隔離マネジャーを経由して復元することができます。
より詳細な調査のために、バックアップコピーをAvira マルウェア
リサーチセンターへ送付することもできます。
オブジェクトによっては、その他の選択オプションが隔離マネジャー内で使用可能です。

プライマリアクション

プライマリアクションは、Real-Time
Protectionがウィルスあるいは迷惑プログラムを検出したときに実行されるアクションです。
オプション"**修復**"が選択されていて、しかし感染ファイルが修復できない場合には、"**二次アクション**"で選択されているアクションが実行されます。

> 注記
> オプション二次アクションは、修復設定がプライマリアクションで選択されている場合だけ、選択することができます。

修復

このオプションが有効な場合、Real-Time
Protectionは感染ファイルを自動的に修復します。 Real-Time

Protectionが感染ファイルを修復できない場合、二次アクションで選択されているアクションが実行されます。

> 注記
> 自動修復が推薦されますが、それはReal-Time Protectionがファイルをワークステーション上で変更することを意味します。

名前の変更

このオプションが有効な場合、Real-Time Protection はファイル名を変更します。これらのファイルへ直接アクセスすること（ダブルクリックなど）は、不可能になります。 ファイルは、後に修復して、再び元の名に戻すことができます。

隔離

このオプションが有効な場合、Real-Time Protectionはファイルを隔離へ移動させます。
このディレクトリ内のファイルは後に修復する、あるいは必要に応じてAviraマルウェア リサーチセンターに送付して復元させることができます。

削除

このオプションが有効な場合、ファイルは削除されます。
このプロセスは、**上書きと削除**よりもはるかに高速です。

無視

このオプションが有効な場合、ファイルへのアクセスが許可され、ファイルはそのままの状態を保ちます。

> 警告
> 汚染されたファイルは、ワークステーション上で、アクティブな状態を保っています! ワークステーションに重大なダメージを与える恐れがあります！

上書きおよび削除

このオプションが有効な場合、Real-Time Protectionは、ファイルを既定のパターンで上書きしてから、削除します。
この処理を施したファイルは、復元不能になります。

アクセスの拒否

このオプションを有効にすると、レポート機能が有効な場合、Real-Time Protection は、レポート ファイルに検出を書き込みます。
このオプションが有効な場合、Real-Time Protection は、エントリをイベント ログに書き込みます。

警告

Real-Time Protectionが**書込み時にスキャン**に設定されている場合、感染ファイルは書込みされません。

二次アクション

オプション"**二次アクション**"は、"**修復**"オプションが"**プライマリアクション**"で選択されている場合だけ、選択できます。
このオプションで、感染ファイルが修復できない場合のアクションを決めます。

名前の変更

このオプションが有効な場合、Real-Time Protection はファイル名を変更します。これらのファイルへ直接アクセスすること（ダブルクリックなど）は、不可能になります。 ファイルは、後に修復して、再び元の名に戻すことができます。

隔離

このオプションが有効な場合、Real-Time Protectionはファイルを隔離へ移動させます。
これらのファイルは後に修復する、あるいは必要に応じてAviraマルウェア リサーチセンターに送付して復元させることができます。

削除

このオプションが有効な場合、ファイルは削除されます。
このプロセスは、**上書きと削除**よりもはるかに高速です。

無視

このオプションが有効な場合、ファイルへのアクセスが許可され、ファイルはそのままの状態を保ちます。

警告
汚染されたファイルはワークステーション上で有効中です!
ワークステーションに重大なダメージを与える恐れがあります！

上書きおよび削除

このオプションが有効な場合、Real-Time Protectionは、ファイルを既定のパターンで上書きしてから、削除します。
この処理を施したファイルは、復元不能になります。

アクセスの拒否

このオプションが有効な場合、感染ファイルは書込みされません。Real-Time Protectionは、報告機能が有効な時だけレポートファイル内の検出を行います。
このオプションが有効な場合、Real-Time Protection は、エントリをイベントログに書き込みます。

注記
削除 あるいは
上書きと削除を一次あるいは二次アクションとして選択している場合には以下に注意してください:
ヒューリスティックが含まれるケースでは感染ファイルは削除されず、隔離へ移動されます。

その他のアクション

イベントログの使用

このオプションが有効な場合、エントリーは探知のためにWindowsのイベントログに追加されます。
イベントはWindowsのイベントビューアに呼出すことができます。
このオプションはデフォルト設定で有効です。(オプションはエキスパートモードでのみ使用可能。)

例外

これらのオプションで、Real-Time Protectionの除外オブジェクトを設定することができます(オンアクセス スキャン)。関連オブジェクトはその際、オンアクセス スキャンに含まれません。 Real-Time Protectionは、省略プロセスリストを介したオンアクセス中にそれらのオブジェクトへのファイル アクセスを無視することができます。
これはたとえば、データベースあるいはバックアップソリューションとの併用は有益です。 (オプションはエキスパートモードでのみ使用可能。)

省略するプロセスおよびファイルオブジェクトを指定する場合は、以下に注意してください:
リストはトップからボトムへと実行されます。
リストが長いほど、各アクセスに要するリストプロセスのためのプロセッサー時間が長くなります。 そのために、リストは可能な限り短く保持してください。

Real-Time Protectionによる省略プロセス

このリスト内のプロセスへのすべてのファイルアクセスは、Real-Time Protectionによる監視から除外されます。

入力ボックス

この欄には、リアルタイム スキャンにより無視するプロセス名を記入します。
デフォルト設定で入力されているプロセスはありません。

指定するプロセスのパスとファイル名は最大255文字までです。
128個までのプロセスを記入することができます。
リスト内のエントリは総計で6000文字を超えないこと。

プロセスを記入する場合、ユニコード文字が許可されます。
そのために、特殊文字を含むプロセスあるいはディレクトリ名を記入することができます。

ドライブ情報は次のように記入する必要があります: [ドライブの文字]:\

コロン(:)は、ドライブを指定するときだけ使用します。

プロセスを特定する場合はワイルドカード「*」(任意の文字数用) および「?」
(単一文字用)が使用可能です。

```
C:\Program Files\Application\application.exe
C:\Program Files\Application\applicatio?.exe
C:\Program Files\Application\applic*.exe
C:\Program Files\Application\*.exe
```

Real-Time
Protectionによる監視のグローバルな除外プロセスを避けるために、以下の文字だけで構成する除外の指定は無効です。「*」(アステリスク)、「?」
(疑問符)、「/」(フォワードスラッシュ)、「\」(バックスラッシュ)、
「.」(ドット),「:」(コロン)。

完全詳細パスを指定せずにReal-Time
Protectionの監視対象となるプロセスを除外できます。 例: `application.exe`

これは、ハードディスク
ドライブ上で実行可能ファイルのある箇所のプロセスだけを適用します。

完全詳細パスは、たとえばネットワーク
ドライブ等の接続されたドライブ上の、実行可能ファイルある箇所のプロセスに要求

されます。 接続ネットワーク
ドライブ上の除外の注記の一般情報を参照してください。

ダイナミック
ドライブ上の実行可能ファイルがある箇所のプロセスの除外は指定しないでください。 ダイナミック ドライブは、CD、DVD、あるいはUSBメモリー等のリムーバブルドライブに使用されます。

警告
リスト内に記録されたプロセスでアクセスされたすべてのファイルは、ウィルスあるいは迷惑プログラムのスキャンから除外されます。

ボタンは、実行可能ファイルが選択できるウィンドウを開きます。

プロセス

"**プロセス**"ボタンは、実行プロセスが表示される"**プロセス選択**"ウィンドウを開きます。

追加

このボタンで、入力ボックスに記入されたプロセスを表示ウィンドウへ追加することができます。

削除

このボタンで、選択されたプロセスを表示ウィンドウから削除することができます。

Real-Time Protectionによる省略ファイル オブジェクト

このリスト内のオブジェクトへのすべてのファイルアクセスは、Real-Time Protectionによる監視から除外されます。

入力ボックス

この入力ボックスには、オンアクセス スキャンに含まれないファイル オブジェクトの名称を記入することができます。 デフォルト設定ではファイル オブジェクトは記入されません。

リスト内のエントリは総計で6000文字を超えないこと。

省略するファイルオブジェクトを指定する場合は、ワイルドカードとして * (任意の数の文字) と？(1 文字) を指定できます。個々のファイル拡張子は (ワイルドカードも含む) を除外することもできます。

```
C:\Directory\*.mdb
*.mdb
*.md?
*.xls*
C:\Directory\*.log
```

ディレクトリ名はバックフラッシュ「\」で終了すること。

ディレクトリが除外される場合、そのすべてのサブディレクトリも自動的に除外されます。

各ドライブには、完全なパス入力(先頭のドライブ文字からはじめて)で最大20個までの除外を指定できます。 例：

```
C:\Program Files\Application\Name.log
```

完全パスのない場合の最大除外数は64。例：

```
*.log
\computer1\C\directory1
```

他のドライブのディレクトリとして取付けられているダイナミック ドライブの場合、除外リスト内に組み込まれたドライブ用のOSのエイリアスは以下のように使用されます:

```
\Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\
```

マウントポイント自体を使用する場合、たとえば`C:\DynDrive`、ダイナミック ドライブはそれにもかかわらずスキャンされます。
使用されるOSのエイリアスをReal-Time Protectionのレポートファイルから決めることができます。

ボタンは、除外するファイル オブジェクトを選択するウィンドウを開きます。

追加

このボタンで、入力ボックスに記入されたファイル
オブジェクトを表示ウィンドウへ追加することができます。

削除

このボタンで、選択されたファイル
オブジェクトを表示ウィンドウから削除することができます。

除外を特定する場合にはその他の情報も考慮してください:

オブジェクトを除外するためにも、それらが短縮DOSファイル名(DOS命名規約 8.3)でアクセスされる場合、適切な短縮ファイル名もリスト内へ記入してください。

ワイルドカードを含むファイル名は、バックスラッシュで終了できないことがあります。
例:
`C:\Program Files\Application\applic*.exe\`
このエントリは有効ではなく、除外として処理されません！

接続ネットワーク ドライブ上の除外の考慮の下に、以下のことに注意してください:
接続ネットワーク
ドライブのドライブレターを使用する場合、指定されるファイルとフォルダーはReal-Time Protectionスキャンから除外されません。
除外リスト内のUNCパスがネットワークドライブへの接続に使用されるUNCパス(除外リスト内のIPアドレス規格 –
ネットワークドライブへの接続用のコンピューター名称規格)と一致しない場合、指定されるフォルダーとファイルはReal-Time Protectionスキャンから除外されません。
関連UNCパスをReal-Time Protectionのレポートファイルに位置付けます:
`\\<Computer name>\<Enable>\` - あるいは - `\\<IP address>\<Enable>\`

Real-Time Protectionが感染ファイルのスキャンに使用するパスを、Real-Time Protectionレポートファイル内に位置付けすることができます。
まったく同じパスを除外リスト内に表示します。 以下のように続行します: Real-Time Protectionのプロトコル機能を環境設定内で完全に設定します(Real-Time Protection > レポートの下で)。 次に、有効化されたReal-Time Protectionで、ファイル、フォルダー、取付けドライブあるいは接続ネットワークドライブにアクセスします。 使用するパスをReal-Time Protectionの報告ファイルから読取ることができます。
レポートファイルは、コントロールセンターのローカル プロテクション > Real-Time Protectionの下でアクセスすることができます。

ヒューリスティック

この環境設定セクションには、スキャンエンジンのヒューリスティク用の設定が含まれます。 (オプションはエキスパート モードでのみ使用可能。)

Avira製品には強力なヒューリスティック機能が含まれており、これによってダメージエレメントに対抗するための特殊ウィルス形跡が確定される前に、またウィルスガードの更新が実行される前に、未知のマルウェアが事前にキャッチされます。
ウィルス検出にはマルウェアの典型的な機能の大規模な解析ならびに感染コードの調査が含まれます。
スキャンされたコードがそれらの典型的な特徴を示す場合、それは疑惑として報告されます。 これは、必ずしもコードがマルウェアと確定されたわけではありません。
時には間違いの陽性反応が発生する可能性があります。
コードソースが信頼性のあるものかどうかの、感染コードの処理に関する決定は、ユーザーが自身の知識に基づいて行います。

マクロウィルス ヒューリスティック

マクロウィルス ヒューリスティク

Avira製品には、高性能なマクロウィルス ヒューリスティック(発見的問題解決法)が含まれています。
このオプションが有効な場合、関連ドキュメント内のすべてのマクロは修復処理によ

って削除される、または代替として疑惑ドキュメントとして報告され、警告が発動されます。 このオプションはデフォルト設定で有効にすることが推薦されます。

上級ヒューリスティック解析&検出(AHeAD)

AHeADの有効化

Aviraプログラムには、Avira AHeAD
テクノロジーに基づく高性能なヒューリスティック機能が含まれており、これは未知の(新たな)マルウェアも検出します。
このオプションが有効な場合、このヒューリスティックの「積極性」を設定することができます。 このオプションはデフォルト設定で有効です。

低検出レベル

このオプションが有効な場合、未知マルウェアの検出度合いはわずかに減少され、それによって間違い警告のリスクは減少します。

中検出レベル

このオプションは、高検出レベルと間違い警告の低リスクを組み合わせています。
中レベルは、このヒューリスティックの活用が選択される場合にデフォルト設定となります。

高検出レベル

このオプションが有効な場合、未知のマルウェアが著しく検出されます、しかし単なる間違い陽性反応のリスクも多くなります。

10.2.2 報告

Real-Time
Protectionには、検出の形式と仕様に関する正確な注記をユーザーあるいはアドミニストレータに提供するための拡張ログ機能が含まれています。 (オプションはエキスパートモードでのみ使用可能。)

報告

このグループは、報告コンテンツの確定を許可します。

オフ

このオプションが有効な場合、Real-Time Protectionはログを作成しません。
ログ機能は、たとえば複数のウィルスあるいは迷惑プログラムのトライアル実行中のような例外的ケースにだけオフにすることを推薦します。

デフォルト

このオプションが有効な場合、Real-Time Protectionは重要な情報(検出関連、警告とエラー)を記録し、あまり重要でない情報は見易さの改善のために無視されます。
このオプションはデフォルト設定で有効です。

拡張

このオプションが有効な場合、Real-Time Protectionはあまり重要でない情報も報告ファイルに記録します。

完全

このオプションが有効な場合、Real-Time Protectionはファイルサイズ、ファイル形式、日付等も含めて入手可能なすべての情報を報告ファイル内に記録します。

報告ファイルの制限

制限容量は n MB

このオプションが有効な場合、報告ファイルは特定容量に制限されます。
許可される値は1 ～ 100 MBです。
システムリソースの使用量を最小にするための報告ファイルの制限には、約50 kBの特別スペースが許可されます。 ログファイルの容量が表示の容量を50 kB以上超える場合、表示容量より50 kB減少するまで旧エントリーが消去されます。

短縮する前に報告ファイルをバックアップ

このオプションが有効な場合、報告ファイルは短縮する前にバックアップされます。

環境設定を報告ファイルに書き込む

このオプションが有効な場合、オン-アクセス
スキャンの環境設定が報告ファイル内に記録されます。

注記
報告ファイルに何の特定制限も加えない場合は、報告ファイルが100
MBに到達すると新規の報告ファイルが自動的に作成されます。
旧報告ファイルのバックアップが作成されます。
3つまでの旧報告ファイルが保存されます。
最も古いバックアップから順に削除されます。

10.3 更新

更新セクションでは、更新の自動受信。 様々な更新期間。

自動更新

n 日 / 時間 / 分ごと

このボックスでは、自動更新が行われるインターバルを指定できます。
更新インターバルを変えるには、ボックス内で時間オプションをマーキングして入力ボックスの右の矢印キーを用いておこないます。

インターネットへ接続中にジョブをスタート(ダイヤルアップ)

このオプションが有効な場合、更新インターバルに加えて、インターネット接続が構築されるたびに更新ジョブが実行されます。 (オプションはエキスパート
モードでのみ使用可能。)

時間切れにはジョブを繰り返す

このオプションが有効な場合、たとえばコンピューターがスイッチオフだったために指定時間に実行されなかった過去の更新ジョブが実行されます。
(オプションはエキスパート モードでのみ使用可能。)

10.3.1 ウェブサーバー

ウェブサーバー

更新は、インターネットあるいはイントラネットのウェブサーバー経由で直接実行できます。. (オプションはエキスパート モードでのみ使用可能。)

ウェブサーバー接続

既存の接続(ネットワーク)の使用

この設定は、接続がネットワーク経由で使用される場合に表示されます。

以下の接続の使用

この設定は、接続を個々に定義する場合に表示されます。

アップデーターは、どの接続オプションが使用可能かを自動的に検出します。
使用できない接続オプションは灰色表示され、有効化できません。
ダイヤルアップ接続はたとえば、Windows内で電話帳エントリを経由して手動で構築することができます。

ユーザー

選択されたアカウントのユーザー名を記入します。

パスワード

このアカウント用のパスワードを記入します。
安全上の理由から、このスペースに記入する現行文字はアステリスク(*)で置換されます(*)。

注記
既存のインターネット
アカウント名あるいはパスワードを忘れた場合は、インターネット サービス プロバイダーに連絡してください。

注記
いわゆるダイヤルアップ ツール (たとえば SmartSurfer, Olecoその他)を通したアップデーターの自動ダイヤルアップは現在まだ使用できません。

更新用に構築されたダイヤルアップ接続の終了

このオプションが有効な場合、更新用に構築されたダイヤルアップ接続はダウンロードが順調に実行されるとすぐに自動的に中断されます。

注記
このオプションは、Windows XP でのみ使用できます。 Windows XP 以降のOSでは、更新用に開かれているダイヤルアップ接続はダウンロードが終了すると常に即座に終了されます。

プロキシ設定

プロキシ サーバー

プロキシ サーバーを使用しない

このオプションが有効な場合、ウェブサーバーへの接続はプロキシサーバー経由で構築されません。

プロキシ システム設定の使用

このオプションが有効な場合、現在のWindowsシステム設定がプロキシサーバーを経由したウェブサーバーへの接続に使用されます。

プロキシサーバーを使用するためのWindowsシステム設定を**コントロール パネル > インターネット オプション > 接続 > LAN 設定**でおこないます。 インターネットオプションはインターネット
エクスプローラ内のメニュー**その他**でもアクセスできます。

警告
認証を要求するプロキシサーバーを使用している場合、要求されるすべてのデータをオプション**このプロキシサーバーを使用**で記入します。 **プロキシシステム設定の使用**オプションは、認証なしのプロキシサーバーが使用される場合にだけ使用されます。

このプロキシ サーバーの使用

ウェブサーバー接続がプロキシサーバー経由で構築されている場合、ここで関連情報を記入することができます。

アドレス

ウェブサーバーの接続に使用したいプロキシサーバーのIPアドレスあるいはコンピューター名を記入します。

ポート

ウェブサーバーへ接続へ使用したいプロキシサーバーのポート番号を記入します。

ロクイン名

プロキシサーバーへログインするためのユーザー名を記入します。

ログイン パスワード

プロキシサーバーにログインするための重要なパスワードをここに記入します。
安全上の理由から、このスペースに記入する現行文字はアステリスク(*)で置換されます(*)。

例:

アドレス: `proxy.domain.com` ポート: `8080`

アドレス: 192.168.1.100 ポート: 3128

10.4 Web Protection

環境設定 > インターネット保護でのWeb Protection部で、Web Protectionの環境設定を行います。

10.4.1 スキャン

Web Protectionは、インターネットから貴ウェブブラウザ上にロードするウェブページから貴コンピューターに到達するウィルスあるいはマルウェアを駆除します。
スキャンオプションはWeb Protectionコンポネントの動向設定に使用することができます。
(オプションはエキスパート モードでのみ使用可能。)

スキャン

IPv6 サポートの有効化

このオプションが有効な場合、IPv6がWeb Protectionでサポートされます。
このオプションは、Windows 8の新規または更新インストールでは利用できません。

ドライブバイ対策

ドライブバイ対策は、I-Frame(＝インライン フレーム)のブロッキング設定を許可します。 I-FrameはHTMLエレメント、つまりウェブページの領域を制限するインターネット ページのエレメントです。 I-Frameは、各種のウェブコンテンツ(通常は他のURLをブラウザのサブウィンドウ内に非依存のドキュメントとして表示される)のロードと表示に使用することができます。 I-Frameはたいていの場合、バナー宣伝用に投入されます。 いくつかの例では、I-Frameは潜伏マルウェアとして投入されることがあります。 こういった場合、I-Frameの領域は多くのケースにおいてブラウザ内でまったくあるいはほとんど見えませ

ん。 **不審なI-Frameをブロックする** このオプションはI-Frameのロードのチェックとブロッキングを許可します。

不審なI-Frameをブロックする

このオプションが有効な場合、希望するウェブページ上のI-Frameは特定基準に基づいてスキャンされます。 要求されたウェブページ上のI-Frameが疑わしい場合、このI-Frameはブロッキングされます。 エラーメッセージがI-Frame ウィンドウ内に表示されます。

検出アクション

ウィルスあるいは迷惑プログラムが検出された場合になすべきアクションを、Web Protectionにて決定することができます。 (オプションはエキスパートモードでのみ使用可能。)

対話型

このオプションが有効な場合、オンデマンドスキャン中にウィルスあるいは迷惑プログラムが検出された時は対話ボックスが現れ、感染ファイルの処置を選択することができます。
このオプションはデフォルト設定で有効です。

進行状況表示バーの表示

このオプションが有効な場合、ウェブサイト内容のダウンロードに20秒のタイムアウト以上掛かるときにはスクリーン上にダウンロード進行バー付きの通知が表示されます。
このスクリーン通知は特に大きなデータ量を持つウェブサイトのダウンロード用に設定されています。Web Protection、ウェブサイト内容はインターネットブラウザ内で表示される前にウイルス、マルウェアについてスキャンされるため、すぐにダウンロードされません。 このオプションはデフォルト設定で無効です。

詳細はここをクリックしてください。

自動

このオプションが有効な場合、対話ボックスはウィルス検出時に表示されません。Web Protectionは、このセクションにおける一次的、二次的アクションとしての設定に基づいて対応します。

プライマリアクション

アプライマリクションは、Web Protectionがウィルスあるいは迷惑プログラムを検出したときに実行されるアクションです。

アクセスの拒否

ウェブサーバーから要求されるウェブサイトおよび/あるいは伝送されるデータとファイルがウェブブラウザに送られません。
アクセス拒否のエラーメッセージがウェブブラウザに表示されます。
報告機能が有効な場合、Web Protectionは検出を報告ファイルに記録します。

[隔離]に移動

ウィルスあるいはマルウェアが検出された場合、ウェブサーバーから要求されるウェブサイトおよび/あるいは伝送されるデータとファイルは隔離されます。
感染したファイルは、情報価値を含む場合、あるいは必要に応じて、Aviraマルウェア リサーチセンターに送付されて隔離マネジャーによって復元することができます。

無視

ウェブサーバーから要求されるウェブサイトおよび/あるいは伝送されたデータとファイルは、Web Protectionを介してウェブブラウザに送られます。
ファイルへのアクセスは許可され、ファイルは無視されます。

警告
汚染されたファイルはワークステーション上で有効中です!
ワークステーションに重大なダメージを与える恐れがあります！

ブロックする要求

ブロックする要求 では、Web Protectionでのスキャン時にブロッキングするファイル形式とMIME形式(伝送データ用のコンテンツ形式)を特定することができます。 ウェブフィルターは既知のフィッシング / マルウェアURLをブロッキングします。 Web Protectionは、インターネットから貴コンピューターシステムへのデータのダウンロードを予防します。 (オプションはエキスパート モードでのみ使用可能。)

Web Protectionでは次のファイル形式　/　MIMEタイプをブロックします

リスト内のすべてのファイル形式とMIME形式(伝送データ用のコンテンツ形式)はWeb Protectionでブロッキングされます。

入力ボックス

このボックスには、Web Protectionでブロッキングしたいの名称を挿入することができます。 ファイル形式にはたとえばファイル拡張子**.htm**を記入します。 MIME形式には、メディア形式ならびに適用可能な場合はサブ形式も提示します。 ふたつのステートメントはシングルスラッシュでたとえば **video/mpeg** あるいは **audio/x-wav**のように分離します。

注記

すでに貴システムに過渡的インターネット ファイルとしてストアされてWeb Protectionでブロッキングされているファイルは、いずれにしてもローカルで貴コンピューターのインターネット ブラウザでインターネットからダウンロードできます。 過渡的インターネット ファイルは、インターネット ブラウザによって貴コンピューター上にセーブされるファイルで、それによってウェブサイトはより早くアクセスすることができます。

注記

ブロッキングするファイルとMIME形式のリストは、Web Protection > スキャン > 除外の下でファイルとMIME形式がブロッキングリストに挿入される場合は無視されます。

注記

ワイルドカード(* - 複数文字の代わり、あるいは？- 単一文字の代わり)はファイル形式およびMIME形式の記入時に使用できません。

MIME形式: メディア形式の例:

- テキスト = テキストファイル用
- 画像 = 画像ファイル用
- ビデオ = ビデオファイル用
- オーディオ = オーディオファイル用
- アプリケーション = 他のプログラムにリンクされるファイル用

除外されるファイルとMIME形式の見本

- アプリケーション/octet-stream = アプリケーション/octet-stream MIME形式ファイル(実行可能ファイル *.bin, *.exe, *.com, *dll, *.class)はWeb Protectionでブロッキングされます。
- アプリケーション/olescript = アプリケーション/olescript MIME形式ファイル(ActiveX script-files *.axs)はWeb Protectionでブロッキングされます。
- .exe = 拡張子 .exe を伴うすべてのファイル(実行可能ファイル)はWeb Protectionでブロッキングされます。
- .msi = 拡張子 .msi を伴うすべてのファイル(Windows インスターラーファイル)はWeb Protectionでブロッキングされます。

追加

このボタンは、MIMEとファイル形式を記入欄からディスプレイウィンドウへコピーすることを許可します。

削除

このボタンは選択されたエントリーをリストから削除します。
このボタンはエントリーが選択されていない場合は非作動です。

Webフィルター

Webフィルターは、コンテンツに基づいて毎日更新しながらURLを分類する内的データベースを基盤とします。

Webフィルターを有効にする

オプションが有効な場合、Webフィルター
リスト内の選択カテゴリーに一致するすべてのURLはブロッキングされます。

Webフィルター リスト

Webフィルター リストでは、Web
Protectionでブロッキングされるコンテンツ
カテゴリーを選択することができます。

注記
Webフィルターは Web Protection > スキャン > 除外での除外URLリスト内のエントリーを無視します。

注記
スパム URL はスパムメールを伴うURLです。 **ごまかし / 詐欺** カテゴリーには、「購読料期限切れ」のウェブページならびにプロバイダーによって費用を秘匿されているその他の提供内容が含まれます。

例外

このオプションでは、Web
ProtectionでのスキャンのためのMIME形式(伝送データ用のコンテンツ形式)ならびにURL(インターネット
アドレス)用のファイル形式をベースとした除外をセットすることができます。
MIMEとURLの専用形式はWeb
Protectionで無視されます、つまりあなたのコンピュータ
システムにデータが伝送される場合にウィルスとマルウェアのスキャンが実行されません。 (オプションはエキスパート モードでのみ使用可能。)

Web Protectionのスキャン対象から除外するMIMEタイプ

この欄では、Web
Protectionでのスキャン時に無視するMIME形式(伝送データ用のコンテンツ形式)を選択することができます。

*Web
Protectionのスキャン対象から除外するファイルタイプ／MIMEタイプ(ユーザー定義)*

リスト内のすべてのMIME形式(伝送データ用のコンテンツ形式)は、Web
Protectionでのスキャン中に無視されます。

入力ボックス

このボックスには、Web
Protectionでのスキャン時に無視するMIME形式とファイル形式の名称を挿入することができます。 ファイル形式にはたとえばファイル拡張子**.htm**を記入します。
MIME形式には、メディア形式ならびに適用可能な場合はサブ形式も提示します。
ふたつのステートメントはシングルスラッシュでたとえば **video/mpeg** あるいは **audio/x-wav**のように分離します。

注記
ワイルドカード(* - 複数文字の代わり、あるいは？-

単一文字の代わり)はファイル形式およびMIME形式の記入時に使用できません。

警告

除外リスト上のすべてのファイル形式およびコンテンツ形式はブロックする要求(Web Protection > スキャン > ブロックする要求でブロッキングされるファイルとMIME形式のリスト)のスキャンなしでインターネット ブラウザへ、あるいはWeb Protectionを介してダウンロードされます。除外リスト上のすべてのエントリー、ファイルとMIME形式リスト上のブロッキング用エントリーは無視されます。 ウィルスとマルウェアのスキャンは実行されません。

MIME形式: メディア形式の例:

- テキスト = テキストファイル用
- 画像 = 画像ファイル用
- ビデオ = ビデオファイル用
- オーディオ = オーディオファイル用
- アプリケーション = 他のプログラムにリンクされるファイル用

除外されるファイルとMIME形式:

- オーディオ/ = すべてのオーディオメディア形式ファイルはWeb Protectionスキャンから除外されます。
- ビデオ/クイックタイム = すべてのクイックタイム サブ形式ビデオファイル(*.qt, *.mov)はWeb Protectionスキャンから除外されます。
- .pdf = すべてのアドビPDFファイルはWeb Protectionスキャンから除外されます。

追加

このボタンは、MIMEとファイル形式を記入欄からディスプレイウィンドウへコピーすることを許可します。

削除

このボタンは選択されたエントリーをリストから削除します。
このボタンはエントリーが選択されていない場合は非作動です。

Web Protectionのスキャン対象から除外するURL

このリスト内のすべてのURLはWeb Protectionスキャンから除外されます。

入力ボックス

このボックスには、Web Protectionスキャンから除外したいURL(インターネットアドレス)、たとえば `www.domainname.com`を挿入することができます。
すべてのページおよびドメインのすべてのサブドメイン用にドメインレベルを表示させるために、たとえば `.domainname.com`のように文頭あるいは文末にドットを用いてURLの一部を特定することができます。 トップレベルドメインを伴うウェブサイト(`.com` あるいは `.net`)を次のドットで `domainname.`表示します。
文頭あるいは文末にドットのないストリングを表示させる場合、ストリングはたとえば `net` -すべてのNETドメイン(`www.domain.net`)のトップレベルドメインとして解釈されます。

注記

URLを特定する場合はワイルドカード *
を複数の文字用に活用することができます。
文頭あるいは文末でのドットとワイルドカードを組み合わせてドメインレベルを表示させることもできます。

```
.domainname.*
*.domainname.com
```

`.*name*.com` (有効ですが推薦はしません)
ドットなしの仕様、たとえば `*name*`、はトップレベルドメインの一部と解釈されるため、得策ではありません。

警告

除外URLリスト上のすべてのウェブサイトはウェブフィルターあるいはWeb Protectionでのスキャンなしにインターネット
ブラウザへダウンロードされます。除外URLリスト内のすべてのエントリー、ウェブフィルター内のエントリー(Web Protection > スキャン > ブロックする要求を参照) は無視されます。
ウィルスとマルウェアのスキャンは実行されません。
そのために、信頼できるURLだけをWeb Protectionスキャンから除外してください。

追加

このボタンは、記入欄(インターネット アドレス)に挿入されたURLをビューアウィンドウへコピーすることを許可します。

削除

このボタンは選択されたエントリーをリストから削除します。
このボタンはエントリーが選択されていない場合は非作動です。

スキップされるURLの例:

- `www.avira.com` -あるいは- `www.avira.com/*`
  = ドメイン `www.avira.com`を伴うすべてのURLはWeb Protectionスキャンから除外されます、たとえば*www.avira.com/en/pages/index.php*, *www.avira.com/en/support/index.html*, *www.avira.com/en/download/index.html*, など。
  ドメイン `www.avira.de`を伴うURLは、Web Protectionスキャンから除外されません。
- `avira.com` -あるいは- `*.avira.com`
  = 二次あるいはトップレベル ドメイン `avira.com` を含むすべてのURLはWeb Protectionスキャンから除外されます。この仕様は`.avira.com`の存在するすべてのサブドメインを示唆します、たとえば *www.avira.com*, *forum.avira.com*, 等。

- avira. -あるいは- *.avira.*
  = 二次レベル ドメイン avira を伴うすべてのURLは、Web Protectionスキャンから除外されます。この仕様は .avira用に存在するすべてのトップレベル ドメインあるいはサブドメインを示唆します、たとえば *www.avira.com*, *www.avira.de*, *forum.avira.com*, 等。
- .*domain*.*
  ストリング domain を伴う二次レベルドメインを含むすべてのURLはWeb Protectionスキャンから除外されます、たとえば*www.domain.com*, *www.new-domain.de*, *www.sample-domain1.de*, 等。
- net -あるいは- *.net
  = トップレベル ドメインnet を伴うすべてのURLは、Web Protectionスキャンから除外されます、たとえば*www.name1.net*, *www.name2.net*, 等。

警告

Web Protectionスキャンから除外したいURLの記入は可能な限り正確に行ってください。 トップレベル ドメインの包括的なあるいは二次レベルドメインの一部の特定は、マルウェアと迷惑プログラムを配布するインターネット ページのリスクが除外の全体的仕様を通してWeb Protectionスキャンから除外されてしまうため、避けてください。 少なくとも完全な二次レベル ドメインおよびトップレベル ドメインの特定、たとえばdomainname.comを推薦します。

ヒューリスティク

この環境設定セクションには、スキャンエンジンのヒューリスティック用の設定が含まれます。 (オプションはエキスパート モードでのみ使用可能。)

Avira製品には強力なヒューリスティック機能が含まれており、これによってダメージエレメントに対抗するための特殊ウィルス形跡が確定される前に、またウィルスガードの更新が実行される前に、未知のマルウェアが事前にキャッチされます。
ウィルス検出にはマルウェアの典型的な機能の大規模な解析ならびに感染コードの調査が含まれます。
スキャンされたコードがそれらの典型的な特徴を示す場合、それは疑惑として報告されます。 これは、必ずしもコードがマルウェアと確定されたわけではありません。
時には間違いの陽性反応が発生する可能性があります。
コードソースが信頼性のあるものかどうかの、感染コードの処理に関する決定は、ユーザーが自身の知識に基づいて行います。

マクロウィルス ヒューリスティック

Avira製品には、高性能なマクロウィルス
ヒューリスティック(発見的問題解決法)が含まれています。
このオプションが有効な場合、関連ドキュメント内のすべてのマクロは修復処理によって削除される、または代替として疑惑ドキュメントとして報告され、警告が発動されます。 このオプションはデフォルト設定で有効にすることが推薦されます。

高度なヒューリスティック分析と検出(AHeAD)

AHeADを有効にする

Aviraプログラムには、Avira AHeAD
テクノロジーに基づく高性能なヒューリスティック機能が含まれており、これは未知の(新たな)マルウェアも検出します。
このオプションが有効な場合、このヒューリスティックの「積極性」を設定することができます。 このオプションはデフォルト設定で有効です。

低検出レベル

このオプションが有効な場合、未知マルウェアの検出度合いはわずかに減少され、それによって間違い警告のリスクは減少します。

中検出レベル

このオプションは、高検出レベルと間違い警告の低リスクを組み合わせています。
中レベルは、このヒューリスティックの活用が選択される場合にデフォルト設定となります。

高検出レベル

このオプションが有効な場合、未知のマルウェアが著しく検出されます、しかし単なる間違い陽性反応のリスクも多くなります。

10.4.2 レポート

Web Protectionには、検出の形式と仕様に関する正確な注記をユーザーあるいはアドミニストレータに提供するための拡張ログ機能が含まれています。

レポート

このグループは、報告コンテンツの確定を許可します。

オフ

このオプションが有効な場合、Web Protectionはログを作成しません。
ログ機能は、たとえば複数のウィルスあるいは迷惑プログラムのトライアル実行中のような例外的ケースにだけオフにすることを推薦します。

既定

このオプションが有効な場合、Web Protectionは重要な情報(検出関連、警告とエラー)を記録し、あまり重要でない情報は見易さの改善のために無視されます。
このオプションはデフォルト設定で有効です。

拡張

このオプションが有効な場合、Web Protectionはあまり重要でない情報も報告ファイルに記録します。

完全

このオプションが有効な場合、Web Protectionはファイルサイズ、ファイル形式、日付等も含めて入手可能なすべての情報を報告ファイル内に記録します。

レポートファイルの制限

サイズの制限値は n MB

このオプションが有効な場合、報告ファイルは指定容量(n)に制限されます。許容バリューは 1 ～ 100 MB内です。
システムリソースの使用量を最小にするための報告ファイルの制限には、約50 kBの特別スペースが許可されます。 ログファイルの容量が表示の容量を50 kB以上超える場合、表示容量が20 %減少するまで旧エントリーが消去されます。

構成をレポートファイルに書き込む

このオプションが有効な場合、オン-アクセス スキャンの環境設定が報告ファイル内に記録されます。

注記
報告ファイルに何の特定制限も加えない場合は、報告ファイルが100 MBに到達すると旧エントリーは自動的に削除されます。 報告ファイルが80 MBの容量になるまで旧エントリーが削除されます。

10.5 Mail Protection

環境設定の**Mail Protection**部で、Mail Protection環境設定を行います。

10.5.1 スキャン

Mail Protectionは、受信メールをウィルスとマルウェアについてスキャンします。
送信メールも、ウィルスとマルウェアについてMail Protectionでスキャンすることができます。

Mail Protectionの許可

このオプションが有効な場合、メール交信はMail Protectionによって監視されます。 Mail Protectionは、使用するメールサーバーとコンピューター システム上のメール クライエント プログラム間のデータ交信をチェックするプロキシサーバーです: 受信メールはデフォルトでマルウェアについてスキャンされます。
このオプションが無効な場合、Mail Protectionサービスは開始しますがMail Protectionでの監視は無効状態です。

受信メールのスキャン

このオプションが有効な場合、受信メールはウィルスとマルウェアについてスキャンされます。 Mail ProtectionはPOP3およびIMAPプロトコルをサポートします。
メールクライエントからメールを受け取る受信箱アカウントの、Mail Protectionでの監視を許可します。

POP3アカウントの監視

このオプションが有効な場合、POP3アカウントは指定ポート上で監視されます。

監視するポート

この欄には、POP3プロトコルによる受信箱として使用されるポートを記入します。 複数のポートはコンマで分離します。 (オプションはエキスパート モードでのみ使用可能。)

既定値

このボタンは指定ポートをデフォルトのPOP3ポートにリセットします。
(オプションはエキスパート モードでのみ使用可能。)

IMAPアカウントの監視

このオプションが有効な場合、IMAPアカウントは指定ポート上で監視されます。

監視中のポート

この欄には、IMAPプロトコルによる受信箱として使用されるポートを記入します。複数のポートはコンマで分離します。 (オプションはエキスパートモードでのみ使用可能。)

既定値

このボタンは指定ポートをデフォルトのIMAPポートにリセットします。(オプションはエキスパート モードでのみ使用可能。)

送信メールのスキャン(SMTP)

このオプションが有効な場合、送信メールはウィルスとマルウェアについてスキャンされます。

監視中のポート

この欄には、SMTPプロトコルによる送信箱として使用されるポートを記入します。複数のポートはコンマで分離します。 (オプションはエキスパートモードでのみ使用可能。)

既定値

このボタンは指定ポートをデフォルトSMTPポートにリセットします。(オプションはエキスパート モードでのみ使用可能。)

> 注記
> 使用するプロトコルとポートを確認するには、メール クライエントプログラムでメール アカウントのプロパティを呼出します。デフォルトポートはもっとも頻繁に使用されます。

IPv6 サポートの有効化

このオプションが有効な場合、IPv6がMail Protectionでサポートされます。(オプションはエクスパートモードでのみ利用可能です。Windows 8の新規または更新インストールでは利用できません。)

検出時のアクション

この環境設定セクションは、Mail Protectionがメールあるいはアタッチメントにウィルスあるいは迷惑プログラムを検出した場合の対処についての設定を含んでいます。 (オプションはエキスパートモードでのみ使用可能。)

> 注記
> これらのアクションは、受信メールあるいは送信メールのどちらでもウィルスが検出された場合に実行されます。

インタラクティブ

このオプションが有効な場合、メールあるいはアタッチメントにウィルスあるいは迷惑プログラムが検出された時に対話ボックスが現れ、該当するメールあるいはアタッチメントの処置を選択することができます。
このオプションは、初期状態で有効に設定されています（デフォルト設定）。

進行状況表示バーの表示

このオプションが有効な場合、Mail Protectionはメールのダウンロード中に進行バーを表示します。
このオプションは、オプション"インタラクティブ"が選択されているときだけ有効です。

自動

このオプションが有効な場合、ウィルスあるいは迷惑プログラムが検出された時に感染が通知されません。 Mail Protectionは、このセクションで定義した設定に基づいて対応します。

感染メール

"*感染メール*"用に選択されたアクションは、Mail Protectionがメール内にウィルスあるいは迷惑プログラムを検出したときに実行されます。

オプション"**無視**"が選択されている場合でも、"*感染した添付ファイル*"の下で、アタッチメントで検出されたウィルスあるいは迷惑プログラムの処理プロセスを選択することもあり得ます。

削除

このオプションが有効な場合、ウィルスあるいは迷惑プログラムが検出された時は感染メールは自動的に削除されます。
メールの本文は、下記に与えられたデフォルト文で置き換えられます。
同じことが、含まれるすべてのアタッチメントに適用されます。これらもデフォルト文で置き換えられます。

無視

このオプションが有効な場合、感染メールはウィルスあるいは迷惑プログラムが検出されても無視されます。
いずれにしても、感染アタッチメントの処理を決めることができます。

[隔離]に移動

このオプションが有効な場合、ウィルスあるいは迷惑プログラムが検出された時は、感染メールはすべてのアタッチメントを含めて完全に隔離へ移動されます。
それは必要に応じて後に、保存することができます。
感染メール自身は削除されます。
メールの本文は、下記に与えられたデフォルト文で置き換えられます。
同じことが、含まれるすべてのアタッチメントに適用されます。これらもデフォルト文で置き換えられます。

感染した添付ファイル

オプション"*感染した添付ファイル*"は、設定"**無視**"が"*感染メール*"で選択されている場合にだけ選択できます。
このオプションで、アタッチメントにウィルスあるいは迷惑プログラムが検出された時の処置を決定することができます。

削除

このオプションが有効な場合、感染アタッチメントはウィルスあるいは迷惑プログラムが検出されてデフォルト文で置き換えられると削除されます。

無視

このオプションが有効な場合、アタッチメントはウィルスあるいは迷惑プログラムが検出されてかつ送付されても無視されます。

警告
このオプションを選択する場合、Mail Protectionによるウィルスあるいは迷惑プログラムに対する保護がありません。自身のアクションを明確に自覚している場合だけ、この項目を選択してください。メール プログラムでのプレビューが無効な場合、ダブルクリックでアタッチメントを開けません！

[隔離]に移動

このオプションが有効な場合、感染アタッチメントは隔離に移動されて、その後に削除されます(デフォルト文で置換)。
感染アタッチメントは必要に応じて後に、保存することができます。

その他のアクション

この環境設定セクションは、Mail Protectionがメールあるいはアタッチメントにウィルスあるいは迷惑プログラムを検出した場合の対処についてのその他の設定を含んでいます。 (オプションはエキスパートモードでのみ使用可能。)

注記
これらのアクションは、受信箱メールにウィルスが検出された場合だけに実行されます。

電子メールの削除／移動に対する既定テキスト

このボックス内のテキストは、感染メールの代わりにメッセージとしてメール内に挿入されます。 このメッセージは編集できます。 テキストは最大500文字までです。

フォーマットには以下のキーコンビネーションを使用できます:

Ctrl + Enter = ラインブリークの挿入。

既定

ボタンは前提デフォルト文を編集ボックス内に挿入します。

添付ファイルの削除／移動に対する既定テキスト

このボックス内のテキストは、感染アタッチメントの代わりにメッセージとしてメール内に挿入されます。 このメッセージは編集できます。
テキストは最大500文字までです。

フォーマットには以下のキーコンビネーションを使用できます:

Ctrl + Enter = ラインブリークの挿入。

既定値

ボタンは前提デフォルト文を編集ボックス内に挿入します。

ヒューリスティック

この環境設定セクションには、スキャンエンジンのヒューリスティック用の設定が含まれます。 (オプションはエキスパート モードでのみ使用可能。)

Avira製品には強力なヒューリスティック機能が含まれており、これによってダメージエレメントに対抗するための特殊ウィルス形跡が確定される前に、またウィルスガードの更新が実行される前に、未知のマルウェアが事前にキャッチされます。
ウィルス検出にはマルウェアの典型的な機能の大規模な解析ならびに感染コードの調査が含まれます。
スキャンされたコードがそれらの典型的な特徴を示す場合、それは疑惑として報告されます。 これは、必ずしもコードがマルウェアと確定されたわけではありません。
時には間違いの陽性反応が発生する可能性があります。

コードソースが信頼性のあるものかどうかの、感染コードの処理に関する決定は、ユーザーが自身の知識に基づいて行います。

マクロウィルス ヒューリスティック

Avira製品には、高性能なマクロウィルス
ヒューリスティック(発見的問題解決法)が含まれています。
このオプションが有効な場合、関連ドキュメント内のすべてのマクロはリペア処理によって削除される、または代替として疑惑ドキュメントとして報告され、警告が発動されます。 このオプションはデフォルト設定で有効にすることが推薦されます。

高度なヒューリスティック分析と検出(AHeAD)

AHeADを有効にする

Aviraプログラムには、Avira AHeAD
テクノロジーに基づく高性能なヒューリスティック機能が含まれており、これは未知の(新たな)マルウェアも検出します。
このオプションが有効な場合、このヒューリスティックの「積極性」を設定することができます。 このオプションはデフォルト設定で有効です。

低検出レベル

このオプションが有効な場合、未知マルウェアの検出度合いはわずかに減少され、それによって間違い警告のリスクは減少します。

中検出レベル

このオプションは、高検出レベルと間違い警告の低リスクを組み合わせています。
中レベルは、このヒューリスティックの活用が選択される場合にデフォルト設定となります。

高検出レベル

このオプションが有効な場合、未知のマルウェアが著しく検出されます、しかし単なる間違い陽性反応のリスクも多くなります。

10.5.2 全般

例外

スキャン除外

この表は、Mail Protectionのスキャンから除外されるメール
アドレスを示します(ホワイトリスト).

> 注記
> 除外リストは、Mail Protectionで受信メールだけを考慮して使用されます。

スキャンの例外設定

入力ボックス

このボックスには、スキャンしないメール アドレスのリストへ追加したいメール アドレスを記入します。 設定に応じてメール アドレスは今後、Mail Protectionのスキャンから除外されます。

追加

このボタンで、入力ボックスに記入したメール アドレスを、スキャンしないメール アドレスのリストへ追加することができます。

削除

このボタンはマーキングされたメール アドレスをリストから削除します。

電子メール アドレス

もうスキャンされないメール

マルウェア

このオプションが有効な場合、メール
アドレスはマルウェアについてもうスキャンされません。

上 (Up)

このボタンで、マーキングされたメール アドレスを上へ移動させます。
マーキングされたエントリーがない場合あるいはマーキングされたアドレスがすでにリストの最初の位置にある場合は、ボタンは非作動です。

下 (Down)

このボタンで、マーキングされたメール アドレスを下へ移動させます。
マーキングされたエントリーがない場合あるいはマーキングされたアドレスがすでにリストの最後の位置にある場合は、ボタンは非作動です。

キャッシュオプション

Mail Protectionキャッシュには、 **Mail Protection**でのコントロールセンター内に統計データとして表示されるスキャン済みメールを考慮したデータが含まれています。 (オプションはエキスパート モードでのみ使用可能。)

キャッシュ内の電子メールの最大件数

この欄では、Mail Protectionによってキャッシュ内に保存される最大メール数を設定します。
最も古いメールから順に削除されます。

メールを保管する最大日数

メールの最大保存日数をこのボックス内に記入します。
この日数後には、メールはキャッシュから削除されます。

キャッシュを空にする

このボタンを押すと、キャッシュ内に保存中の全メールが削除されます。

10.5.3 レポート

Mail Protectionには、検出の形式と仕様に関する正確な注記をユーザーあるいはアドミニス

トレータに提供するための拡張ログ機能が含まれています。 (オプションはエキスパートモードでのみ使用可能。)

レポート

このグループは、レポートコンテンツの確定を許可します。

オフ

このオプションが有効な場合、Mail Protectionはログを作成しません。
ログ機能は、たとえば複数のウィルスあるいは迷惑プログラムのトライアル実行中のような例外的ケースにだけオフにすることを推薦します。

既定

このオプションが有効な場合、Mail Protectionは重要な情報(検出関連、警告とエラー)を記録し、あまり重要でない情報は見易さの改善のために無視されます。
このオプションはデフォルト設定で有効です。

拡張

このオプションが有効な場合、Mail Protectionはあまり重要でない情報も報告ファイルに記録します。

完全

このオプションが有効な場合、Mail Protectionはあまり重要でない情報もすべて報告ファイルに記録します。

レポートファイルの制限

サイズの制限値は n MB

このオプションが有効な場合、報告ファイルは指定容量(n)に制限されます。許容値は 1 ～ 100
MB内です。システムリソースの使用量を最小にするための報告ファイルの制限には

、約50 kBの特別スペースが許可されます。 ログファイルの容量が表示の容量を50 kB以上超える場合、表示容量より50 kB減少するまで旧エントリーが消去されます。

短縮前にレポートファイルをバックアップ

このオプションが有効な場合、報告ファイルは短縮する前にバックアップされます。

構成をレポートファイルに書き込む

このオプションが有効な場合、Mail Protectionの環境設定が報告ファイル内に記録されます。

注記

報告ファイルに何の特定制限も加えない場合は、報告ファイルが100 MBに到達すると新規の報告ファイルが自動的に作成されます。
旧報告ファイルのバックアップが作成されます。
3つまでの旧報告ファイルが保存されます。
最も古いバックアップから順に削除されます。

10.6 Child Protection

Avira の *CHILD PROTECTION* 機能を使用することで、子供やその他のコンピュータユーザーが安全にインターネットを使用することができる環境を確保することができます。

10.7 Mobile Protection

Avira は、コンピュータシステムをマルウェアやウィルスから保護することだけではなくて、Android オペレーティング システムのスマートフォンも紛失や盗難から守ります。 Avira Free Android Security を使って、着信拒否したい電話番号や受信拒否したい SMS をブロックすることができます。 通話、着信履歴、SMS の履歴から電話番号を選択し、追加するか、手動でブロックしたい連絡先を作成します。

さらに詳しい情報は、当社のウェブサイトでご覧いただけます。

http://www.avira.com/android

10.8 全般

Avira製品は特定の出来事において、メール経由で一人以上の受信者へメッセージを
これはSMTP(Simple Message Transfer Protocol)でおこなわれます。

このメッセージは様々な出来事によって発動されます。
以下のコンポネントはメール送信をサポートします:

> 注記
> ESMTPはサポートされていないので注意してください。 さらに、TLS (Transport Layer Security)あるいはSSL (Secure Sockets Layer)経由の暗号化転送は現在まだできません。

電子メール メッセージ

SMTPサーバー

使用されるホスト名(IPアドレスまたはホスト名を直接)をここに記入します。
ホスト名の最大許容長さは127文字です。

例*:*

`192.168.1.100` あるいは `mail.samplecompany.com`

ポート

使用されるポートをここに記入します。

送信者アドレス

送信者メールアドレスをこの入力ボックスに記入します。 送信者メール
アドレスの最大許容長さは127文字です。

認証

いくらかのメールサーバーは、メールが送られる前にそれを確認するためのプログラム(ログイン)を期待することがあります。
警告は、認証によってメール経由でSMTPサーバーへ送信することができます。

認証の使用

このオプションが有効な場合、ユーザー名とパスワードをログインのために適切なボックス内へ記入します(認証)。

ログイン名:
ここにユーザー名を記入します。

パスワード:
ここに適切なパスワードを記入します。 パスワードは暗号化形式で保存されます。
安全上の理由から、このスペースに記入する現行文字はアステリスク(*)で置換されます。

テスト電子メールの送信

ボタン上をクリックすると、プログラムは記入されたデータのチェックのために送信者アドレスへテスト電子メールを送ります。

10.8.1 脅威カテゴリー

拡張脅威カテゴリーの選択 (オプションはエキスパート モードでのみ使用可能。)

Avira製品はコンピューターをウィルスから保護します。
さらに、以下の拡張脅威カテゴリーに基づいてスキャンすることができます。

- アドウェア
- アドウェア／スパイウェア
- アプリケーション
- バックドア クライアント
- ダイヤラー
- 二重の拡張子ファイル

- 偽ソフトウェア
- ゲーム
- ジョーク
- フィッシング
- 個人のプライバシーを侵害するプログラム
- 通常とは異なるランタイム圧縮ツール

関連ボックスをクリックすると、選択された形式は有効化(チェックを入れる)無効化(チェックなし)されます。

すべて選択

このオプションが有効な場合、すべての形式が有効化されます。

既定値

このボタンは事前設定のデフォルト値を復元します。

> 注記
> 形式が無効化されている場合、関連プログラム形式として認識されていたファイルはもう表示されません。 報告ファイル内にエントリーがありません。

10.8.2 上級保護

ProActiv (オプションはエキスパート モードでのみ使用可能。)

ProActivを有効化

このオプションが有効な場合、システム上のプログラムは監視され、疑惑アクションをチェックされます。
典型的なマルウェア挙動が検出されると、メッセージを受け取ります。
プログラムを制止するか、あるいはプログラムの使用を続行するために"**無視**"を選択します。 監視プロセスは以下を除外します:

信頼可として分類されるプログラム、デフォルトで許可アプリケーション フィルターに含まれている信頼可で署名済みのプログラム、ならびに許可プログラム用のアプリケーション フィルターに追加したすべてのプログラム。

ProActivは、ウィルスあるいはヒューリスティックの定義がまだ使用できない新規で未知の脅威からコンピューターを保護します。 ProActivテクノロジーはReal-Time Protectionコンポネント内に内蔵されており、実行されるプログラムのアクションを監視、解析します。 プログラムの挙動は典型的なマルウェア
アクションの傾向(アクションの形式とアクションの連続性)についてチェックされます。プログラムが典型的なマルウェア挙動を示す場合、これはウィルス検出として処理されます。プログラムをブロックするか、通知を無知してプログラムの使用を続行するかを選択できます。
プログラムを信頼可として分類し、それを許可プログラム用のアプリケーション フィルターに追加することができます。
常に制止コマンドを用いて、プログラムを制止プログラム用のアプリケーション フィルターに追加するオプションがあります。

ProActivコンポネントは、Aviraマルウェア
リサーチセンターで開発された規則セットを疑惑挙動の識別に使用します。
規則セットは、Aviraデータベースによって供給されます。
ProActivは記録用に、各疑惑プログラムの情報をAviraデータベースへ送ります。
Aviraのインストール中に、Aviraデータベースへのデータ送信を無効化するオプションがあります。

> 注記
> ProActivテクノロジーはまだ64 bitシステムに使用できません！

Cloud Protection(オプションはエキスパート モードでのみ使用可能。)

Cloud Protectionの有効化

すべての疑惑ファイルの痕跡は、ダイナミック オフライン
インスペクション用にCloud Protectionへ送られます。
実行ファイルは即座にクリーン、感染あるいは未知に識別されます。

Cloud Protectionはセントラル
ロケーションとして、ユーザーベースを通したサイバー攻撃の監視に貢献します。
コンピューターでアクセスされるファイルは、クラウド内に保存されているファイルの痕跡に対して照合されます。
クラウド内でのスキャンが多く実行されるほど、アンチウィルス
アプリケーションに要求されるプロセスパワーが節約されます。

マルウェアによって頻繁に目標とされるファイル ロケーションのリストは、**クイック システム スキャン**ジョブが実行されると生成されます。
リストには、進行中のプロセス、起動とサービス時に作動するプログラムが含まれます。
各ファイルの痕跡は生成されてCloud
Protectionへ送られ、「クリーン」または「マルウェア」に分類されます。
未知のプログラム ファイルは、解析のためにCloud
Protectionへアップロードされます。

Aviraに疑しいファイルを送信する場合は手動で確認する。

Cloud
Protectionへ送られる疑惑ファイルのリストは閲覧でき、送りたいファイルを選択することができます。

ブロックするアプリケーション

ブロックするアプリケーション では、有害として分類してデフォルトでAvira
ProActivによるブロックを望むアプリケーションを記入します。
追加されたアプリケーションはコンピューター システム上で実行されません。
このプログラムを常に制止オプションを選択して、疑惑挙動プログラムに関するReal-Time Protection通知を経由したブロック用アプリケーション
フィルターへ、プログラムを追加することもできます。。

ブロックするアプリケーション

アプリケーション

このリストには、環境設定を通して記入したあるいはProActivコンポネントの通知により有害として分類したすべてのアプリケーションが含まれます。
リスト上のアプリケーションは、Avira ProActivによって制止され、コンピューターシステム上で実行することができません。
制止されたプログラムが起動すると、OSメッセージが現れます。
制止アプリケーションは、特定パスおよびファイル名をベースとしてAvira ProActivで識別され、それらのコンテンツに関係なくブロックされます。

入力ボックス

制止したいアプリケーションをこのボックス内に記入します。
アプリケーションを識別するには、完全なパス、ファイル名およびファイル拡張子を特定してください。
パスはアプリケーションのあるドライブ、あるいは環境変数でスタートするドライブを表示しなければなりません。

ボタンは、制止アプリケーションを選択するウィンドウを開きます。

追加

"**追加**"ボタンで、入力ボックスで特定したアプリケーションをブロックするアプリケーションリストへ移動させることができます。

> 注記
> OSの本来の操作用に必要なアプリケーションは追加できません。

削除

"**削除**"ボタンで、マーキングされたアプリケーションを制止アプリケーションリストから削除します。

除外するアプリケーション

セクションスキップするアプリケーションは、ProActivコンポネントによる監視から除外されるアプリケーションをリストアップします:
デフォルトでリスト内に信頼可で包含可として分類された署名済みプログラム、アプリケーション フィルターへ信頼可で包含可として分類されたすべてのアプリケーション:
許可済みアプリケーションを環境設定リストへ追加できます。 Real-Time Protection通知内の**信頼可プログラム**オプションを用いて、Real-Time Protection通知経由でアプリケーションを挙動疑惑プログラムへ追加するオプションも使用可能です。

除外するアプリケーション

アプリケーション

リストには、ProActivコンポネントによる監視から除外されるアプリケーションが含まれます。
デフォルトのインストール設定では、リストには信頼可ベンダーからの署名済みアプリケーションが含まれます。 環境設定あるいはReal-Time Protection通知のどちら経由が信頼できるか考慮するアプリケーションを追加するオプションが、使用可能です。
ProActivコンポネントは、パス、ファイル名およびコンテンツを用いてアプリケーションを識別します。
マルウェアは更新等の変更を通してプログラムに添加されるため、コンテンツのチェックを推薦します。 コンテンツチェックが特定**形式**から実行されるかどうかを決定できます:
"コンテンツ"形式には、パスとファイル名で特定されるアプリケーションがProActivコンポネントによる監視から除外される前に、ファイルコンテンツの変更をチェックされます。
ファイルコンテンツが変更されている場合、アプリケーションは再びProActivコンポネントによって監視されます。 "パス"形式には、アプリケーションがReal-Time Protectionによる監視から除外される前はコンテンツチェックが実行されません。
除外形式を変更するには、表示される形式上をクリックします。

警告

例外ケースではパス形式だけを使用してください。
マルコードは更新を通してアプリケーションに追加される可能性があります。
元は罪のないアプリケーションが、マルウェアに変わります。

注記

たとえばAvira製品のすべてのアプリケーション
コンポネントを含めたいくつかの信頼可アプリケーションは、それらがリストに含まれていないにもかかわらず、デフォルトでProActivコンポネントによる監視から除外されます。

入力ボックス

このボックス内には、ProActivコンポネントによる監視から除外されるアプリケーションを記入します。
アプリケーションを識別するには、完全なパス、ファイル名およびファイル拡張子を特定してください。
パスはアプリケーションのあるドライブ、あるいは環境変数でスタートするドライブを表示しなければなりません。

ボタンは、除外するアプリケーションを選択するウィンドウを開きます。

追加

"**追加**"ボタンで、入力ボックスで特定したアプリケーションを除外アプリケーションリストへ移動させることができます。

削除

"**削除**"ボタンで、マーキングされたアプリケーションを除外アプリケーションリストから削除します。

10.8.3 パスワード

パスワードでAvira製品の各領域を保護することができます。
パスワードが設置されると、保護領域を開くときにはいつもパスワードを問われます。

パスワード

パスワードの入力

要求されるパスワードをここに記入します。
安全上の理由から、このスペースに記入する現行文字はアステリスク(*)で置換されます(*)。 パスワードは最大で20文字までです。
パスワードが一度設定されると、間違ったパスワードの入力時にはプログラムはアクセスを拒否します。 空のボックスは「パスワードなし」を意味します。

確認

上欄に記入したパスワードをここに再記入してください。
安全上の理由から、このスペースに記入する現行文字はアステリスク(*)で置換されます(*)。

> 注記
> パスワードは大/小文字を区別します！

パスワード保護されている領域(オプションはエキスパート モードでのみ使用可能。)

Avira製品は、独自の領域をパスワードで保護することができます。
適切なボックスをクリックして、パスワード要求を独自の領域について無効化/有効化することができます。

パスワード保護領域	機能
コントロールセンター	このオプションを有効にすると、コントロールセンターの開始には事前設定のパスワードが要求されます。
Real-Time Protectionの有効化/無効化化	このオプションが有効な場合、Avira Real-Time Protectionの有効化/無効化に事前設定のパスワードが要求されます。
Mail Protectionの有効化/無効化	このオプションが有効な場合、Mail Protectionの有効化/無効化に事前設定のパスワードが要求されます。
Web Protectionの有効化/無効化	このオプションが有効な場合、Web Protectionの有効化/無効化に事前設定のパスワードが要求されます。
隔離	このオプションが有効な場合、隔離マネジャーのすべての領域でパスワード保護が有効化されます。 適切なボックスをクリックして、パスワード照会を独自の領域について無効化/有効化することができます。
感染オブジェクトの復元	このオプションを有効にすると、オブジェクトの復元には事前設定のパスワードが要求されます。

感染オブジェクトの再スキャン	このオプションを有効にすると、オブジェクトの再スキャンには事前設定のパスワードが要求されます。
感染オブジェクト プロパティ	このオプションを有効にすると、オブジェクトのプロパティ表示には事前設定のパスワードが要求されます。
感染オブジェクトの削除	このオプションを有効にすると、オブジェクトの削除には事前設定のパスワードが要求されます。
Aviraに電子メールを送信	このオプションを有効にすると、オブジェクトの送信(Aviraマルウェア リサーチセンターへ検査のため)には事前設定のパスワードが要求されます。
環境設定	このオプションが有効な場合、事前設定パスワードの入力後にはじめてプログラムの環境設定が可能となります。
インストールとアンインストール	このオプションを有効にすると、プログラムのインストール/アンインストールには事前設定のパスワードが要求されます。

10.8.4 セキュリティ

(オプションはエキスパート モードでのみ使用可能。)

自動実行

自動実行機能のブロック

このオプションが有効な場合、USBメモリー、CD/DVDドライブおよびネットワークドライブを含めたすべての接続ドライブ上のWindows自動実行

機能の実行は制止されます。 Windows自動実行
機能によって、データメディアあるいはネットワーク
ドライブ上のファイルはロードあるいは接続時に即座に読取られ、それによってファイルは自動的にスタートしてコピーされます。
マルウェアと迷惑プログラムが自動スタートと共にインストールされることがあるため、この機能は大きな安全上のリスクを伴います。。 自動実行
機能は特にUSBメモリーに関しては、その中のデータがいつでも変わる可能性があるために批判的です。

CDとDVDを除外する

このオプションが有効な場合、CDとDVDドライブ上の自動実行
機能は許可されます。

> **警告**
> 信頼できるデータメディアだけを使用していることが確かな場合にだけ、CDとDVDドライブの自動実行機能を無効化してください。

システムの保護

Windows hostsファイルへの書き込みを防

このオプションが有効な場合、Windows hosts ファイルは書込み保護されます。
変更操作はもうできません。
たとえば、マルウェアによる不要ウェブサイトへの書き換えは不可能です。
このオプションはデフォルト設定で有効です。

製品の保護

> 注記
> 製品保護オプションは、ユーザー定義のインストール
> オプションを使用するReal-Time
> Protectionがインストールされていない場合には、使用できません。

意図しない終了操作からプロセスを保護

このオプションが有効な場合、プログラムのすべてのプロセスはウィルスとマルウェアあるいはユーザーによる、たとえばタスクマネジャーを通した'コントロールのない'無用の終了から保護されます。 このオプションはデフォルト設定で有効です。

高度なプロセス保護

このオプションが有効な場合、プログラムのすべてのプロセスは上級オプションによって無用の終了から保護されます。
上級プロセス保護は、簡易プロセス保護と比較してより多くのコンピューターリソースを必要とします。 このオプションはデフォルト設定で有効化されています。
このオプションの無効化には、コンピューターの再起動が必要です。

注記
パスワード保護はWindows XP 64 bit には使用できません！

注記
プロセス保護が有効な場合、他のソフトウェア製品との競合問題の発生することがあります。 このような場合には、プロセス保護を無効にしてください。

ファイルとレジストリ エントリを外部の操作から保護

このオプションが有効な場合、プログラムのすべてのレジストリエントリーならびにすべてのプログラム
ファイル(バイナリと環境設定ファイル)は変更操作から保護されます。
変更操作に対する保護は必然的に、書込み、削除ならびにいくつかのケースではユーザーあるいは外部プログラムによるレジストリ エントリーあるいはプログラムファイルへの読取りアクセスを予防します。
このオプションの有効化には、コンピューターの再起動が必要です。

警告

このオプションが無効な場合には、特定タイプのマルウェアに感染したコンピューターの修理ができないことがあります。

注記

このオプションが有効な場合、環境設定への変更は、スキャンあるいは更新要求への変更も含めて、ユーザー
インターフェイスを使用してだけ可能なことがあります。

注記

ファイルとレジストレーション エントリーの保護は、Windows XP 64 bit で使用できません。

10.8.5 WMI

(オプションはエキスパート モードでのみ使用可能。)

Windows Management Instrumentation(WMI)のサポート

Windows Management Instrumentation(WMI)は、読取り/書込みのアクセスをローカルとリモートの両方で許可して、Windowsシステム上で設定するための、スクリプトとプログラミング言語を使用するベーシックなWindows管理テクノロジーです。
Avira製品はWMIをサポートしてデータ(ステータス情報、統計的データ、報告、計画リクエストその他)、ならびにインターフェイスを経由したイベントを提供します。
WMIは、プログラムからの操作データのダウンロードおよびプログラム制御のオプションを提供しています。

WMIサポートを有効にする

このオプションが有効な場合、WMI経由でプログラムから操作データをダウンロードすることができます。

10.8.6 イベント

(オプションはエキスパート モードでのみ使用可能。)

イベント データベースサイズの制限

最大サイズの制限値は n エントリー

このオプションが有効な場合、イベント
データベース内に記入されるイベントの最大数は特定の容量に制限することができ、
その可能な数値は100 ～ 10000エントリーです。
記入されるエントリー数が超える場合には、最も古いエントリーが削除されます。

次より古いすべてのイベントを削除 n 日

このオプションが有効な場合、イベント
データベース内に記入されたイベントは、特定の期間後に削除されます。可能な値:
1 ～ 90日です。 このオプションはデフォルト設定で30日有効です。

制限なし

このオプションが有効な場合、イベント データベースのサイズは制限されません。
いずれにしても、「イベント」のプログラム
インターフェイス内では最大で20,000のエントリーが表示されます。

10.8.7 レポート

(オプションはエキスパート モードでのみ使用可能。)

レポートの制限

最大値に数を制限

このオプションが有効な場合、報告最大数は指定数に制限されます。 1 ～ 300の値が使用可能です。
使用可能定数が超えた場合には、その時点で最も古い報告から順に削除されます。

次より古いすべてのレポートを削除 n 日

このオプションが有効な場合、報告は指定日数後に自動的に削除されます。
許容日数は1から90日までです。
このオプションはデフォルト設定で30日有効です。

制限なし

このオプションが有効な場合、報告数は制限されません。

10.8.8 ディレクトリ

(オプションはエキスパート モードでのみ使用可能。)

一時フォルダパス

既定のト システム設定を使用する

このオプションが有効な場合、システムの設定は過渡的ファイルの処理に使用されます。

> 注記
> システムが過渡的ファイルを保存する場所 - たとえばWindows XPは - **スタート > 設定 > コントロール パネル > システム > 索引カード "アドバンスド" ボタン "環境変数"**。
> 現在登録されているユーザー用の過渡的変数(TEMP, TMP)ならびにシステム変数(TEMP, TMP)は、ここでそれらの適切な値で表示されます。

以下のディレクトリを使用

このオプションを有効にすると、入力ボックスに表示されるパスが使用されます。

入力ボックス

この入力ボックスには、プログラムが過渡的ファイルを保管するパスを記入します。

...

このボタンはウィンドウを開き、要求される過渡的パスを選択できます。

既定

このボタンは、過渡的パス用に事前定義されたディレクトリを復元します。

10.8.9 音声によるアラート

(オプションはエキスパート モードでのみ使用可能。)

ウィルスあるいはマルウェアがSystem ScannerあるいはReal-Time Protectionで検出されると、対話型アクション モードで警告が発動します。
音声によるアラート
の有効化/無効化を選択し、警告音用に代わりのWAVEファイルを選ぶことができます。

> 注記
> System Scannerのアクションモードは、System Scanner > スキャン > 検出に対するアクション.で設定されます。 Real-Time Protectionのアクションモードは Real-Time Protection > スキャン > 検出に対するアクションの環境設定内で設定されます。

音声によるアラートを行わない

このオプションが有効な場合、ウィルスあるいはマルウェアがSystem ScannerあるいはReal-Time Protectionで検出されたときにが発動しません。

PCスピーカーを使用する(対話型モードのみ)

このオプションが有効な場合、ウィルスがSystem ScannerあるいはReal-Time Protectionで検出されたときにデフォルト信号でのが発動されます。
はPCの内蔵スピーカーで発せられます。

次のWAVEファイルを使用する(対話型モードのみ)

このオプションが有効な場合、ウィルスがSystem ScannerあるいはReal-Time Protectionで検出されたときに選択されたWAVEファイルによるが発動されます。
選択されたWAVEファイルの音声が、接続された外部スピーカーから発せられます。

WAVEファイル

この入力ボックスでは、選択したい音声ファイルの名称と関連パスを記入します。
プログラムのデフォルト音声信号が標準で記入されています。

...

ボタンは、ファイル
エクスプローラを用いて要求されるファイルが選択できるウィンドウを開きます。

テスト

このボタンは、選択されたWAVEファイルのテストに使用されます。

10.8.10 アラート

Avira製品はいわゆるスライドアップ、更新等のプログラム
シーケンスの成功/不成功についての情報を与える、特別イベント用のスクリーン通知を生成します。
アラートにおいて、特別イベント用の通知を有効化/無効化することができます。

スクリーン通知によって、直接スライドアップ内で通知を無効化するオプションが得られます。 通知は、アラート設定ウィンドウ内で再び有効化することができます。

更新

最終更新日が次の日数より古い場合、アラートを表示する

このボックス内で、最後の更新から経過して良い最大日数を記入することができます。

この日数が経過すると、更新ステータス用の赤いアイコンがステータスのコントロール センター内に表示されます。

ウィルス定義ファイルが古い場合に注意を表示する

このオプションが有効な場合、ウィルス定義ファイルが有効切れになったときに警告が発動します。 警告オプションを用いて、最後の更新がｎ
日を経過した場合の警告用の過渡的インターバルを設定することができます。

以下の状況での警告 / 注意

ダイヤルアップ接続を使用しています

このオプションが有効な場合、ダイヤラーが電話機あるいはISDNネットワーク経由でコンピューターにダイヤルアップ接続を構築すると、スクリーン通知警告が表示されます。
これは、接続が未知の迷惑ダイヤラーによって行われたもので、接続がチャージされるものである危険性があります。 (ウィルスなど > 脅威カテゴリー: ダイアラーを参照)

ファイルが正常に更新されました

このオプションが有効な場合、更新が順調に実行されてファイルが更新されると、スクリーン通知が表示されます。

更新に失敗しました

このオプションが有効な場合、更新に失敗したときはいつもスクリーン通知が表示されます、たとえばダウンロード
サーバーに接続が構築されなかった、あるいは更新ファイルがインストールされなかった場合等です。

更新は不要です

このオプションが有効な場合、更新は開始したがプログラムが最新のためにファイルのインストールが必要なかったときは、いつもスクリーン通知が表示されます。

Issued Q2-2013

AVIRA

live free.™

www.avira.jp

株式会社アビラ
〒150-8512
東京都渋谷区桜丘町
26-1
セルリアンタワー15階