Avira AntiVir Professional

ユーザー マニュアル

AVIRA

商標と著作権

商標

AntiVir は Avira GmbH の登録商標です。
Windows は米国 Microsoft Corporation の米国およびその他の国における登録商標です。
その他すべてのブランド名および製品名は、それぞれの保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が、 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

Avira AntiVir Professional には、第三者により提供されたコードが使用されています。 弊社による使用を許諾した著作権所有者に謝意を表します。 著作権の詳細については、Avira AntiVir Professional ヘルプの第三者ライセンスの下の.を参照してください。

目次

1 はじめに

AntiVir プログラムは、コンピュータをウイルス、ワーム、トロイの木馬、アドウェア、スパイウェア、その他のリスクから保護します。このマニュアルでは、これらをウイルスまたはマルウェア (有害なソフトウェア) および不要なプログラムといいます。

このマニュアルでは、プログラムのインストールと操作について説明します。

詳細なオプションについては、次の弊社 Web サイトを参照してください。

http://www.avira.jp

Avira Web サイトでは、次のことが可能です。

- 他の AntiVir デスクトップ プログラムに関する情報を参照します。
- 最新の AntiVir デスクトップ プログラムをダウンロードします
- PDF 形式で最新の製品マニュアルをダウンロードします
- 無料のサポートおよび修復ツールをダウンロードします
- トラブルシューティングのために、包括的なナレッジ データベースおよび FAQ にアクセスします
- 国固有のサポート アドレスにアクセスします。

Avira チーム

2 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
✓	アクションの実行前に満たしている必要のある条件の前に付けられています。
▸	ユーザーが実行するアクションのステップの前に付けられています。
→	前のアクションに続くイベントの前に付けられています。
警告	重大なデータ損失の危険に対する警告の前に付けられています。
注意	特に重要な情報、または AntiVir プログラムを使いやすくするためのヒントの前に付けられています。

次の強調表示が使用されています。

強調表示	説明
筆記体	ファイル名、またはパス データ。
	表示されるソフトウェアのインターフェイス (ウィンドウの見出し、ウィンドウのフィールド、オプション ボックスなど)。
太字	クリックされるソフトウェアのインターフェイス要素 (メニュー項目、セクション、ボタンなど)。

3 製品情報

この章には、AntiVir 製品の購入と使用に関するあらゆる情報が含まれています。

- 「提供範囲」の章を参照。
- 「システム要件」の章を参照。
- 「使用許諾」の章を参照。
- の章を参照。

AntiVir プログラムは、ウイルス、マルウェア、不要プログラム、およびその他の危険からコンピュータを保護する包括的で、柔軟性と信頼性のあるツールです。

► 以下の情報に注意してください。

注意
貴重なデータの損失は、通常、大きな結果につながります。最高のアンチウイルス プログラムでも、データ損失から 100 パーセントの保護を提供することはできません。セキュリティ上の理由から、データは定期的にコピーを作成 (バックアップ) してください。

注意
プログラムは、最新状態にされている場合に、ウイルス、マルウェア、不要プログラムおよびその他の危険からの信頼性のある効果的な防止対策を提供します。AntiVir プログラムを自動更新により確実に最新に維持します。それに従ってプログラムを設定します。

3.1 提供範囲

AntiVir プログラムには、以下の機能があります。

- プログラム全体を監視、管理および制御するコントロール センター
- 使いやすい標準オプションと詳細オプション、および状況依存のヘルプを使用した中央設定
- 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、プロファイル制御および設定可能なスキャンを提供するスキャナ (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すると、管理者権限を必要とするタスクを実行できます。
- すべてのファイル アクセスの試行に対する Guard (オンアクセス スキャン) の継続的な監視
- プログラムによるアクションの常時監視のための ProActiv コンポーネント (32 ビット システムのみが対象、Windows 2000 では使用できません)
- ウイルスとマルウェアに関して完全な電子メールのチェックを実行する MailGuard (POP3 スキャナ、IMAP スキャナ 、および SMTP スキャナ)。電子メールの添付ファイルのチェックが含まれています。

- HTTP プロトコル (ポート 80、8080、3128 を監視) を使用して、インターネットから転送されるデータおよびファイルを監視する WebGuard
- 疑わしいファイルを分離して処理する統合された [隔離] の管理
- コンピュータ システムにインストールされた非表示のマルウェア (ルートキット) の検出のためのルートキット対策
  (Windows XP 64 ビットでは使用できません)
- 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
- インターネットまたはイントラネットでの Web サーバーを介した単一ファイル更新と増分 VDF 更新によるプログラム、ウイルス定義、および検索エンジンに対する簡単ですばやい更新
- ライセンス マネージャでのわかりやすい使用許諾
- 更新やスキャンなど、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 (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、スマートなファイル タイプの判別による検出など、従来型のあらゆるアーカイブ 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)
- インターネットまたは他のネットワークからの不正アクセス、許可されていないユーザーによるインターネット/ネットワークへの不正アクセスからコンピュータを保護する Avira FireWall

3.2 システム要件

システム要件は、以下のとおりです。

- コンピュータ : Pentium 以上、最低 266 MHz
- オペレーティング システム
- Windows XP SP2 (32 ビットまたは 64 ビット)、または
- Windows Vista (32 または 64 ビット、SP 1)
- Windows 7 (32 ビットまたは 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)
- 256 MB 以上の RAM (Windows XP の場合)
- 1024 MB 以上の RAM (Windows Vista、Windows 7 の場合)
- プログラムのインストールの場合: 管理者権限
- すべてのインストール: Internet Explorer 6.0 以降
- インターネット接続 (必要な場合。「インストール」を参照)

3.3 ライセンスとアップグレード

AntiVir 製品を使用するには、ライセンスが必要です。お客様は、ライセンス条件を受け入れる必要があります。

ライセンスは、hbedv.key というファイルの形態でデジタル ライセンス コードで発行されます。このデジタル ライセンス コードは、ユーザーの個人ライセンスのキーです。どのプログラムに対するライセンスがいつまで提供されているかに関する正確な詳細が含まれています。このため、デジタル ライセンス コードには、複数製品のライセンスが含まれている場合もあります。

AntiVir プログラムをインターネットまたはプログラム CD/DVD で購入された場合、デジタル ライセンス コードは電子メールで送信されます。ライセンス キーは、プログラムのインストール中に読み込んだり、後でライセンス マネージャでインストールできます。

3.3.1 ライセンス マネージャ

Avira AntiVir Professional ライセンス マネージャを使用すると、Avira AntiVir Professional ライセンスを非常に簡単にインストールできます。

Avira AntiVir Professional ライセンス マネージャ

ライセンスは、ファイル マネージャ、またはアクティブ化電子メールでライセンス ファイルを選択してダブルクリックし、画面上の関連する指示に従ってインストールできます。

注意

Avira AntiVir Professional ライセンス マネージャは、対応するライセンスを関連する製品フォルダに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 ファイルを上書き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しいライセンス ファイルにより上書きされます。

4 インストールとアンインストール

この章には、AntiVir プログラムのインストールとアンインストールに関連する情報が含まれています。

- 「インストール::条件、インストールの種類、インストール」の章を参照。
- 「インストール モジュール」の章を参照。
- 「変更のインストール」の章を参照。
- ネットワーク上でのインストールとアンインストール
- 「アンインストール:アンインストール」の章を参照。

4.1 インストール

インストールの前に、コンピュータが最小システム要件を満たしていることを確認してください。お使いのコンピュータがすべての要件を満たしている場合は、AntiVir プログラムをインストールできます。

注意
インストール プロセス中に、復元ポイントを作成することを選択できます。復元ポイントの目的は、オペレーティング システムをインストール前の状況にリセットすることです。このオプションを使用する場合は、オペレーティング システムで復元ポイントの作成が許可されていることを確認してください。
Windows XP: システム プロパティ -> システム復元: オプション **[システム復元の禁止]** を無効にします。
Windows Vista/Windows 7:システム プロパティ -> コンピュータ保護:**[保護設定]** 領域で、システムがインストールされるドライブをハイライト表示し、**[設定]** ボタンをクリックします。**[システム保護]** ウィンドウで、**[システム設定および以前のファイル バージョンの復元]** オプションを有効にします。

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できます。

エクスプレス

- すべてのプログラム コンポーネントがインストールされるわけではありません。次のコンポーネントはインストールされません。

  Avira AntiVir ProActiv

  Avira FireWall

- プログラム ファイルは、`C:\Program Files` の下にある指定された既定のフォルダにインストールされます。
- AntiVir プログラムが、既定の設定でインストールされます。設定ウィザードを使用してカスタム設定を定義するオプションがあります。

ユーザー定義

- 個々のプログラム コンポーネントのインストールを選択できます (インストールとアンインストール::インストール モジュールの章を参照)。
- プログラム ファイルのインストール先フォルダを選択できます。
- デスクトップ アイコンを作成する機能とスタート メニューにプログラム グループを作成する機能を無効にできます。
- 設定ウィザードを使用すると、AntiVir プログラム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短いシステム スキャンを開始できます。

インストール開始前

- ▶ 電子メール プログラムを閉じます。実行されているすべてのアプリケーションを終了することもお勧めします。
- ▶ 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。さまざまなセキュリティ 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。
- ▶ インターネット接続を確立します。インターネット接続は、次のインストール手順を実行するときに必要になります。
- ▶ インストール プログラムを介して最新のプログラム ファイル、スキャン エンジン、ウイルス定義ファイルをダウンロードするとき (インターネット ベースのインストールの場合)
- ▶ インストールの完了後に更新を行うとき (該当する場合)
- ▶ AntiVir プログラムをアクティブ化するためにライセンス ファイル hbedv.key をコンピュータ システムに保存するとき

注意

インターネット ベースのインストール:
インターネット ベースでのプログラムのインストールのために、Avira GmbH Web サーバーによるインストールの前に現在のプログラム ファイルを読み込むインストール プログラムが提供されています。このプロセスにより、AntiVir プログラムが最新のウイルス定義ファイルと共にインストールされることが保証されます。
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 パッケージには、インストール プログラムとすべ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、AntiVir プログラムの言語を選択することはできません。インストールが完了した後に、ウイルス定義ファイルを更新することをお勧めします。

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。すべてのウィンドウに、インストール プロセスを制御する、ボタンによる特定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。

AntiVir プログラムのインストール:

注意
Windows FireWall を停止する次のアクションは、Windows XP オペレーティング システムにのみ適用されます。

▶ 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...] というダイアログ ボックスが表示されます。

▶ **[次へ]** をクリックして、インストールを続行します。

[言語の選択] ダイアログ ボックスが表示されます。

▶ AntiVir プログラム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の選択を確定します。

[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すべてのファイルが Avira GmbH Web 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すると、*[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 ウィザードにより、*Avira AntiVir Professional* をインストールするためのダイアログ ボックスが開きます。

▶ *[同意]* をクリックして、インストールを開始します。

インストール ファイルが展開されます。インストール ルーチンが開始されます。

[ようこそ...] というダイアログ ボックスが表示されます。

▶ **[次へ]** をクリックします。

インターネット ベースのインストールと、インストール パッケージを使用したインストールの継続

ライセンス契約を含むダイアログ ボックスが表示されます。

▶ ライセンス契約への同意を確認し、**[次へ]** をクリックします。

[シリアル番号の生成] ダイアログ ボックスが表示されます。

▶ 必要に応じて、更新中にランダムなシリアル番号が生成され、送信されたことを確認し、**[次へ]** をクリックします。

[インストール タイプの選択] ダイアログ ボックスが表示されます。

▶ **[エクスプレス]** オプションまたは **[ユーザー定義]** オプションを有効にします。復元ポイントを作成する場合は、**[システムの復元ポイントを作成する]** オプションを有効にします。**[次へ]** をクリックして設定を確認します。

ユーザー定義インストール

[ターゲット ディレクトリの選択] ダイアログ ボックスが表示されます。

▶ **[次へ]** をクリックして、指定したターゲット ディレクトリを確認します。

- または -

[参照] ボタンを使用して別のターゲット ディレクトリを選択し、**[次へ]** をクリックして確認します。

[コンポーネントのインストール] ダイアログ ボックスが表示されます。

▶ 必要なコンポーネントを有効または無効にし、**[次へ]** をクリックして確認します。

ProActiv コンポーネントのインストールを選択した場合、*[AntiVir ProActiv コミュニティ]* ウィンドウが表示されます。Avira AntiVir ProActiv コミュニティへの参加を確認するオプションが提示されます。このオプションを有効にした場合、Avira AntiVir ProActiv は ProActiv コンポーネントによって検出された不審なプログラムに関するデータを Avira マルウェア研究センターに送信します。このデータは、高度なオンライン スキャン、検出テクノロジーの進展および改良のためにのみ使用されます。拡張オンライン スキャンの詳細については、「**詳細情報**」のリンクを参照してください。

▶ AntiVir ProActiv コミュニティへの参加を有効または無効にし、**[次へ]** をクリックすることにより確認します。

次のダイアログ ボックスでは、デスクトップ ショートカットや [スタート] メニュー内のプログラム グループを作成するかどうかを決定できます。

▶ **[次へ]** をクリックします。

再開: エクスプレス インストールとユーザー定義インストール

[ライセンスのインストール] ダイアログ ボックスが表示されます。

▶ ライセンス ファイルを保存したディレクトリに移動し、ダイアログ ボックスのメッセージを読み、**[次へ]** をクリックして確定します。

ライセンス ファイルがコピーされ、コンポーネントがインストールおよび開始されます。

次のダイアログ ボックスでは、インストールの完了後に Readme ファイルを開くかどうかと、コンピュータを再起動するかどうかを選択できます。

▶ 必要に応じて同意し、*[終了]* をクリックしてインストールを完了します。

インストール ウィザードが閉じられます。

再開: ユーザー定義インストール
設定ウィザード

ユーザー定義インストールを選択した場合は、次の手順で設定ウィザードが開きます。設定ウィザードでは、AntiVir プログラムのカスタム設定を定義できます。

▶ 設定ウィザードのようこそ画面で **[次へ]** をクリックして、プログラムの設定を開始します。

[AHeAD の設定] ダイアログ ボックスでは、AHeAD テクノロジの検出レベルを選択できます。選択した検出レベルは、スキャナ (オンデマンド スキャン) および Guard (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 *[脅威カテゴリ (拡張) の選択]* ダイアログ ボックスでは、AntiVir プログラムの保護機能を指定した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、さらに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。

AntiVir Firewall インストール モジュールを選択した場合は、*[FireWall のセキュリティ レベル]* ダイアログ ボックスが表示されます。Avira FireWall が、有効になっているリソースおよび信頼済み企業のアプリケーションによるネットワーク アクセスを許可するかどうかを定義できます。

▶ 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。

AntiVir Guard インストール モジュールを選択した場合は、*[Guard 起動モード]* ダイアログ ボックスが表示されます。Guard の開始時間は指定できます。コンピュータが再起動されるごとに、指定した起動モードで Guard が起動されます。

注意
指定した Guard の起動モードはレジストリに保存されます。設定を使用して起動モードを変更することはできません。

▶ 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。

以下の *[電子メールの設定の選択]* ダイアログ ボックスでは、電子メールを送信するためのサーバー設定を定義できます。AntiVir プログラムでは、SMPT を使用して、電子メールの送信電子メール アラートの送信を行う場合に、SMPT が使用されます。

▶ 必要に応じてサーバー設定を調整し、*[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、ショート システム スキャンを有効または無効に設定できます。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イ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。

▶ *[終了]* をクリックして、設定を完了します。

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た場合は、[Luke Filewalker] ウィンドウが開きます。スキャナによって簡易システム スキャンが実行されます。

再開: エクスプレス インストールとユーザー定義インストール

最終的なインストール ウィザードで **[コンピュータを再起動する]** オプションを選択した場合は、コンピュータが再起動されます。

インストール ウィザードで **[Readme.txt の表示]** オプションを選択した場合、コンピュータの再起動後に Readme ファイルが表示されます。

インストールが正常に完了したら、プログラムが最新であることをコントロール センターの *[概要]::[状況]* で確認することをお勧めします。

- ▶ 必要に応じて更新を実行し、最新のウイルス定義ファイルを入手してください。
- ▶ その後で、完全システム スキャンを実行します。

4.2 インストールの変更

現在の AntiVir プログラムのインストールに含まれる個々のプログラム コンポーネントを追加または削除することができます (「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」の章を参照)。

現在のインストールに追加と削除を行う場合は、**Windows のコントロール パネル**の **[プログラムの追加と削除]** の **[プログラムの追加と削除]** オプションを使用します。

AntiVir プログラムを選択して、**[変更]** をクリックします。プログラムのようこそダイアログで、**[変更]** オプションを選択します。インストールの変更に関する案内が提供されます。

4.3 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、または削除できます。

- **AntiVir Professional**
  このモジュールには、AntiVir プログラムの正常なインストールに必要なすべてのコンポーネントが含まれています。
- **AntiVir Guard**
  AntiVir Guard はバックグラウンドで実行されます。オンアクセス モードでの開く、書き込む、コピーなどの操作中に、可能な場合、ファイルは監視および修復されます。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、AntiVir プログラムは自動的にファイルをスキャンします。ファイルの名前を変更しても、AntiVir Guard によるスキャンは起動しません。
- **AntiVir 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、不審なアプリケーションの動作をユーザーに警告します。この動作ベースの認識により、不明なマルウェアからの保護が可能になります。ProActive コンポーネントは AntiVir Guard に統合されています。

- **AntiVir MailGuard**
  MailGuard は、ユーザーのコンピュータと、電子メール プログラム (電子メール クライアント) による電子メールのダウンロード元となる電子メール サーバーの間のインターフェイスです。MailGuard 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ます。すべての受信電子メールに対して、このプロキシを経由してウイルスと不要プログラムのスキャンが実行され、電子メール プログラムに転送されます。設定によって、プログラムは感染した電子メー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かを確認します。
- **AntiVir WebGuard**
  インターネットを閲覧するときは、Web ブラウザを使用して、Web サーバーからのデータを要求します。Web 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など) は、通常、ブラウザのキャッシュに直接移動され、Web ブラウザで表示されるため、AntiVir Guard によるオンアクセス スキャンは実行できません。この方法を使用すると、ウイ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。WebGuard 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イ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かを確認する場合があります。
- **Avira FireWall:**
  Avira FireWall は、コンピュータとの通信を制御します。セキュリティ ポリシーに基づいて、通信を許可または拒否します。
- ***AntiVir ルートキット対策***
  AntiVir ルートキット対策では、従来のマルウェア保護ではコンピュータ システムへの侵入後に検出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ないかが確認されます。
- **シェル拡張**
  シェル拡張により、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、エントリ「選択したファイルを AntiVir でスキャン」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できます。

4.4 アンインストール

コンピュータから AntiVir プログラムを削除するには、Windows のコントロール パネルの **[プログラムの追加と削除]**、**[プログラムの変更と削除]** を選択します。

AntiVir プログラムをアンインストールするには (Windows XP および Windows Vista の場合):

- Windows の **[スタート]** メニューで、**[コントロール パネル]** を開きます。
- **[プログラム]** (Windows XP: **[プログラムの追加と削除]**) をダブルクリックします。

▶ リストで AntiVir プログラムを選択して、**[削除]** 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。

Windows FireWall を再度有効にするかを確認するメッセージが表示されます (Avira FireWall は無効になっています)。

▶ **[はい]** をクリックして確定します。

プログラムのすべ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。

AntiVir プログラムがアンインストールされ、コンピュータを再起動したときに、プログラムのすべてのディレクトリ、ファイル、およびレジストリのエントリが削除されます。

4.5 ネットワーク上でのインストールとアンインストール

システム管理者による、複数クライアント コンピュータのネットワーク上の AntiVir プログラムのインストールを簡略化するため、AntiVir プログラムには最初のインストールとインストール済み設定の変更に特別の手順があります。

セットアップ プログラムは、setup.inf 制御ファイルに従って自動インストールを行います。セットアップ プログラム (presetup.exe) は、プログラムのインストール パッケージに含まれています。インストールは、スクリプトまたはバッチ ファイルで開始し、必要な情報は制御ファイルから取得されます。このため、スクリプト コマンドはインストール中に通常の手動入力に置換されます。

注意
ネットワーク上での最初のインストールには、ライセンス ファイルが必要です。

注意
ネットワークを介したインストールを行うには、AntiVir プログラムのインストール パッケージが必要です。インターネット ベースのインストール用のインストール ファイルは使用できません。

AntiVir プログラムは、サーバー ログイン スクリプト、または SMS を介して、ネットワークで簡単に共有できます。

ネットワーク上でのインストールとアンインストールに関する詳細:

- 「セットアップ プログラムのコマンド ライン パラメータ」の章を参照。
- 「setup.inf ファイルのパラメータ」の章を参照。
- 「ネットワーク上でのインストール」の章を参照。
- 「ネットワーク上でのアンインストール」の章を参照。

注意
AntiVir Security Management Center には、ネットワーク上での AntiVir プログラムのインストールとアンインストールのための簡単な別のオプションが用意されています。AntiVir Security Management Center では、ネットワーク上での AntiVir 製品のリモート インストールとメンテナンスが可能です。詳細については、弊社 Web サイト を参照してください。
http://www.avira.jp

4.5.1 ネットワーク上でのインストール

インストールは、バッチ モードでスクリプト制御が可能です。

セットアップは、次のインストールに適しています。

- ネットワークを介した初めてのインストール (無人セットアップ)
- シングル ユーザー コンポーネントのインストール

▶ インストールおよび更新の変更

注意
インストール ルーチンがネットワークで実装される前に、自動インストールをテストすることをお勧めします。

ネットワーク上で AntiVir プログラムを自動的にインストールするには:

管理者権限が必要です (バッチ モードでも必要)。

▶ *setup.inf* ファイルのパラメータを設定して、ファイルを保存します。

▶ パラメータ /inf を使用してインストールを開始するか、パラメータをサーバーのログイン スクリプトに統合します。

- 例: `presetup.exe /inf="c:\temp\setup.inf"`
  インストールは自動的に開始します。

4.5.2 ネットワーク上でのアンインストール

ネットワーク上で AntiVir プログラムを自動的にアンインストールするには:

管理者権限が必要です (バッチ モードでも必要)。

▶ アンインストールは、パラメータ `/remsilent` または `/remsilentaskreboot` を使用して開始するか、パラメータをサーバーのログイン スクリプトに統合します。

アンインストール ログに対するパラメータを指定することもできます。

- 例: `preetup.exe /remsilent /unsetuplog="c:\logfiles\unsetup.log"`
  アンインストールは自動的に開始します。

注意
アンインストール セットアップ プログラムは、AntiVir プログラムをアンインストールする PC 上で開始する必要があります。ネットワーク ドライブからセットアップ プログラムを開始しないでください。

4.5.3 セットアップ プログラムのコマンド ライン パラメータ

すべてのパス、またはファイル データは "..." に配置する必要があります。

次のパラメータはインストールに使用できます。

– `/inf`

セットアップ プログラムは、指定したスクリプトで開始し、必要なすべてのパラメータを取得します。

例: `presetup.exe /inf="c:\temp\setup.inf"`

次のパラメータは、アンインストールに使用できます。

– `/remove`

セットアップ プログラムは、AntiVir プログラムをアンインストールします。

例: `presetup.exe /remove`

– `/remsilent`

セットアップ プログラムは、ダイアログを表示せずに、AntiVir プログラムをアンインストールします。コンピュータは、アンインストール後に再起動されます。

例: `presetup.exe /remsilent`

– `/remsilentaskreboot`

セットアップ プログラムは、ダイアログを表示せずに AntiVir プログラムをアンインストールし、アンインストール後にコンピュータに再起動を要求します。

例: `presetup.exe /remsilentaskreboot`

次のパラメータは、アンインストール ログに対するオプションとして使用できます。

– `/unsetuplog`

アンインストール中のすべてのアクションが記録されます。

例: `presetup.exe /remsilent /unsetuplog="c:\logfiles\unsetup.log"`

4.5.4 setup.inf ファイルのパラメータ

制御ファイル setup.inf では、[DATA] フィールドの次のパラメータを設定して、AntiVir プログラムを自動でインストールできます。パラメータの順序は重要ではありません。パラメータの設定が欠けていたり間違っていると、セットアップ ルーチンが中止し、エラー メッセージが表示されます。

- `DestinationPath`

  プログラムがインストールされるセットアップ先のパス。スクリプトに含まれている必要があります。セットアップには、会社名と製品名が自動的に含まれることに注意してください。環境変数が使用できます。

  例: DestinationPath=`%PROGRAMFILES%`
  では、インストール先のパス `C:\Programme\Avira\AntiVir Desktop` が作成されます。

- `ProgramGroup`

  Windows のスタート メニューにコンピュータのすべてのユーザーに対するプログラム グループを作成します。

  `1`:プログラム グループを作成する

  `0`:プログラム グループを作成しない

  例: `ProgramGroup=1`

- `DesktopIcon`

  コンピュータのすべてのユーザーに対するショートカット アイコンをデスクトップに作成します。

  `1`:デスクトップにアイコンを作成する

  `0`:デスクトップにアイコンを作成しない

  例: `DesktopIcon=1`

- `ShellExtension`

  シェル拡張をレジストリに登録します。シェル拡張を使用すると、右マウス ボタンのコンテキスト メニューで、ファイルまたはディレクトリのウイルスやマルウェアをスキャンできます。

  `1`:シェル拡張を登録する

  `0`:シェル拡張を登録しない

  例: `ShellExtension=1`

- `Guard`

  AntiVir Guard (オンアクセス スキャナ) をインストールします。

  `1`:AntiVir Guard をインストールする

0:AntiVir Guard をインストールしない

例: Guard=1

– MailScanner

AntiVir MailGuard をインストールします。

1:AntiVir MailGuard をインストールする

0:MailGuard をインストールしない

例: MailScanner=1

– KeyFile

インストール中にコピーされたライセンス ファイルに対するパスを指定します。初回インストールの場合: 必須。ファイル名は完全に指定する必要があります (完全修飾)。(変更インストールの場合: オプション)

例: KeyFile=D:\inst\license\hbedv.key

– ShowReadMe

インストール後に readme.txt ファイルを表示します。

1:ファイルを表示する

0:ファイルを表示しない

例: ShowReadMe=1

– RestartWindows

インストール後にコンピュータを再起動します。このエントリは、ShowRestartMessage より優先度が高くなっています。

1:コンピュータを再起動する

0:コンピュータを再起動しない

例: RestartWindows=1

– ShowRestartMessage

セットアップ中、自動再起動を実行する前に情報を表示します。

0:情報を表示しない

1:情報を表示する

例: ShowRestartMessage=1

– SetupMode

初回インストールには必要ありません。セットアップ プログラムは、初回インストールが実行されているかどうかを認識します。インストールの種類を指定します。インストールが既に使用可能な場合は、SetupMode でこのインストールが更新のみか、変更 (再設定) か、またはアンインストールかを指定する必要があります。

更新: 既存のインストールを更新します。この場合、Guard などの設定パラメータは無視されます。

Modify: 既存のインストールを変更 (再設定) します。プロセスで、ファイルはアンインストール パスにコピーされません。
Remove: AntiVir プログラムをシステムからアンインストールします。

例: `SetupMode=Update`

– `AVWinIni (オプション)`

インストール中にコピーされる可能性のある設定ファイルに対するセットアップ先パスを指定します。ファイル名は完全に指定する必要があります (完全修飾)。

例: `AVWinIni=d:\inst\config\avwin.ini`

– `Password`

このオプションを使用すると、インストール (の変更) とアンインストールについてセットアップ ルーチンに設定されたパスワードを割り当てます。エントリは、パスワードが設定されている場合にのみ、セットアップ ルーチンによってスキャンされます。パスワードが設定されていて、パスワード パラメータが不足していたり間違っていると、セットアップ ルーチンが中止します。

例: `Password=Password123`

– `WebGuard`

AntiVir WebGuard をインストールします。

1:AntiVir WebGuard をインストールする

0:AntiVir WebGuard をインストールしない

例: `WebGuard=1`

– `RootKit`

AntiVir ルートキット対策モジュールをインストールします。AntiVir ルートキット対策がない場合、スキャナはシステム上のルートキットをスキャンできません。

1:AntiVir ルートキット対策をインストールする

0:AntiVir ルートキット対策をインストールしない

例: `RootKit=1`

– HIPS

AntiVir ProActiv コンポーネントをインストールします。AntiVir ProActiv は、未知のマルウェアを検出できるようにするパターン ベースの検出テクノロジです。

1:ProActiv をインストールする

0:ProActiv をインストールしない

例: HIPS=1

– FireWall

Avira FireWall コンポーネントをインストールします。Avira FireWall は、コンピュータ システム上の受信および送信データ トラフィックを監視および制限して、インターネットまたはその他のネットワーク環境から発生する脅威からコンピュータを保護します。

1:ファイアウォールをインストールする

0:ファイアウォールをインストールしない

例: FireWall=1

5 AntiVir Professional の概要

この章には、AntiVir プログラムの機能と操作の概要が含まれています。

- 「ユーザー インターフェイスと操作」の章を参照。
- 「方法」の章を参照。

5.1 ユーザー インターフェイスと操作

AntiVir プログラムは、プログラムの 3 つのインターフェイス要素で操作できます。

- コントロール センター: AntiVir プログラムを監視および制御します
- 設定: AntiVir プログラムを設定します
- タスクバーのシステム トレイのトレイ アイコン: コントロール センターと他の機能を開きます。

5.1.1 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 システムの保護状況を監視し、AntiVir プログラム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] ウィンドウは、次の 3 つの領域から成ります。**メニュー バー**、**ナビゲーション バー**、および詳細ウィンドウ**表示**。

- **メニュー バー:** コントロール センターのメニュー バーで、プログラムの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いて、作業内容によってナビゲーション バーに配置されています。例: 作業内容 *概要* - セクション **ステータス**。
- **表示:** このウィンドウには、ナビゲーション領域で選択したセクションが表示されます。セクションに応じて、詳細ウィンドウの上部のバーに、機能やアクションを実行するボタンが表示されます。データまたはデータ オブジェクトは個々のセクションのリストに表示されます。リストの並べ替え方法を定義するボックスをクリックすると、リストを並べ替えできます。

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、次のオプションを使用できます。

- 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] メニューのプログラム エントリを選択
- AntiVir プログラムのトレイ 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 センター内で移動するには:

▶ 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。

- または -

▶ *[表示]* メニューでセクションを選択します。

注意

メニュー バーのキーボード ナビゲーションは Alt キーを使用してアクティブにできます。ナビゲーションがアクティブになると、矢印キーでメニュー内を移動できます。Return キーを使用して、アクティブなメニュー項目をアクティブにできます。

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方法には、キーの組み合わせを使用して、Alt キーを押しながらメニューまたはメニュー コマンドの下線付きの文字を押す方法もあります。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、またはオブジェクトを処理するには:

▶ 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

– **概要**: **[概要]** には、AntiVir プログラムの機能を監視するすべてのセクションが記載されています。

- **[状況]** セクションでは、アクティブなプログラム モジュールを確認できます。また、最終更新の実行に関する情報も提供されます。有効なライセンスを保有しているかどうかも確認できます。
- [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できます。
- [レポート] 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。

– **ローカル保護**: **[ローカル保護]** では、コンピュータ システムのウイルスやマルウェアについてファイルをチェックするコンポーネントが使用できます。

- [スキャン] 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えます。事前に設定済みのプロファイルを使用すると、調整済みの標準のオプションでスキャンを実行できます。同様に、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イ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。
- [Guard] 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でき、またレポート ファイルへのアクセスも可能です。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な情報は、"ボタンを押す" だけで取得できます。

– **オンライン保護**: **[オンライン保護]** には、インターネットからのウイルスやマルウェア、および不正なネットワーク アクセスからコンピュータ システムを保護するためのコンポーネントが用意されています。

- [MailGuard] セクションには、MailGuard によって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。
- [WebGuard] 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でき、またレポート ファイルへのアクセスも可能です。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な情報は、"ボタンを押す" だけで取得できます。
- [FireWall] セクションでは、Avira FireWall の基本設定を設定できます。また、ネットワーク接続を使用して、現在のデータ転送速度やすべてのアクティブなアプリケーションが表示されます。

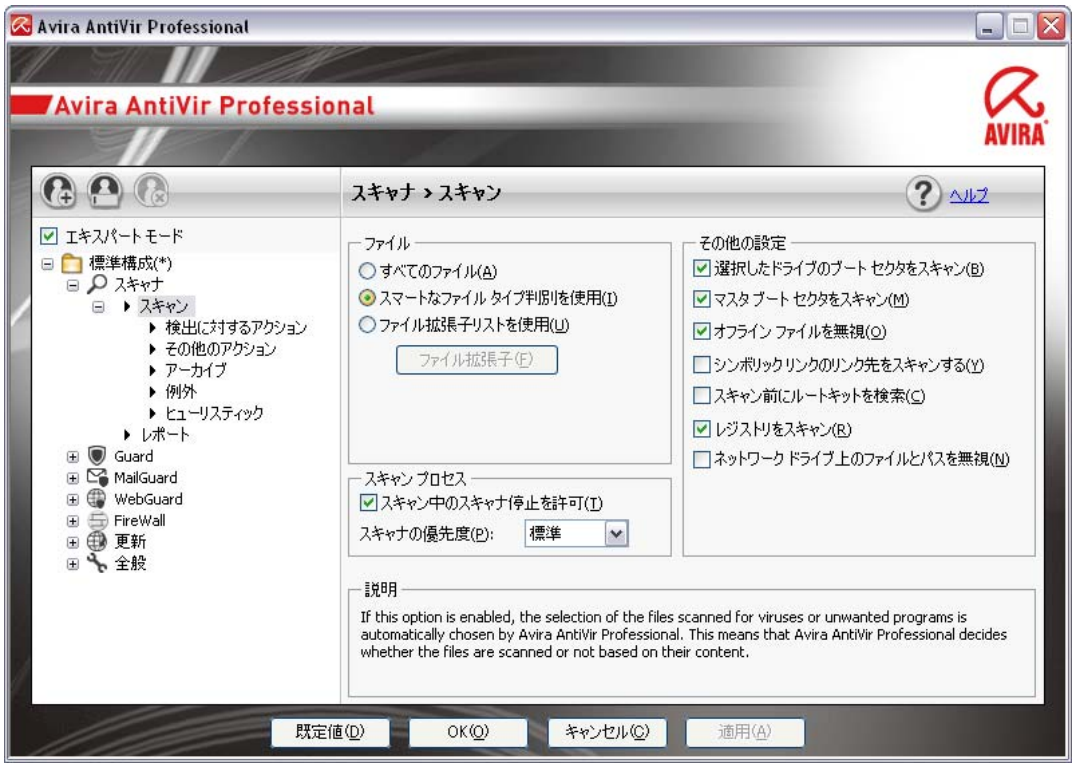
– **管理**:**[管理]** では、疑わしいファイルや感染したファイルを分離して管理したり、定期的なタスクの計画を行うためのツールを使用できます。

- [隔離] セクションには、隔離が含まれています。既に [隔離] に配置されているファイルや疑わしいファイルで [隔離] に配置したいファイルを操作するための一元的な場所です。選択したファイルを電子メールで Avira マルウェア研究センターに送信することもできます。

- [Scheduler] 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、および既存のジョブの調整、または削除が可能です。

5.1.2 設定

設定で、AntiVir プログラムの設定を定義できます。インストール後、AntiVir プログラムは、コンピュータ システムに最適の保護が提供されるように標準設定で設定されます。ただし、ユーザーのコンピュータ システムや AntiVir プログラムに対する固有の要件により、プログラムの保護コンポーネントを調整する必要がある場合があります。



設定により、ダイアログ ボックスが開きます。[OK] ボタンまたは [適用] ボタンをクリックすると、設定を保存できます。[キャンセル] ボタンをクリックすると、設定を削除できます。[既定値] ボタンをクリックすると、既定の設定を復元できます。個々の設定は、左側のナビゲーション バーで選択できます。

設定へのアクセス

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 のセキュリティ センター (Windows XP Service Pack 2 以降)。
- AntiVir プログラムのトレイ アイコン。
- コントロール センターのメニュー項目 [その他] | [設定]。
- コントロール センターの [設定] ボタン。

注意
コントロール センターで **[設定]** ボタンからアクセスしている場合は、コントロール センターでアクティブになっているセクションの設定登録に進みます。個々の設定登録を選択する場合は、エキスパート モードをアクティブにする必要があります。この場合、エキスパート モードのアクティブ化を確認するダイアログが表示されます。

設定の操作

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、ツリー構造に設定サブセクションが表示されます。
- 設定サブセクションを非表示にするには、展開された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
設定のオプションの有効/無効を切り替えたり、ボタンを使用したりする方法には、キーの組み合わせを使用して、Alt キーを押しながら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もあります。

注意
すべての設定セクションは、エキスパート モードでのみ表示できます。すべての設定セクションを表示するには、エキスパート モードをアクティブにしてください。エキスパート モードはパスワードで保護できます。このパスワードはアクティブ化中に定義する必要があります。

設定を有効にするには:

- **[OK]** をクリックします。

  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 -

- **[同意する]** をクリックします。

  入力した設定が有効になります。この場合、ウィンドウは開いたままになります。

設定項目を確定せずに、設定を終了する場合は:

- **[キャンセル]** をクリックします。

  設定ウィンドウが閉じて、設定は破棄されます。

すべての設定を既定値に復元するには:

- **[既定値を復元]** をクリックします。

  すべての設定が既定値に復元されます。既定値に復元すると、すべての変更とカスタム エントリが失われます。

設定プロファイル

設定は設定プロファイルとして保存することができます。設定プロファイルには、すべての設定オプションがグループ別に保存されます。設定は、ナビゲーションバーにノードとして表示されます。既定の設定に他の設定を追加することもできます。特定の設定に切り替えるためのルールを定義することもできます。
ルールベースの手順を使用して設定を切り替える場合、LAN 接続またはインターネット接続 (既定のゲートウェイを介した識別) の使用に設定をリンクできます。このようにして、異なるラップトップ使用シナリオに対して設定プロファイルを作成できます。

- 社内ネットワークでの使用: イントラネット サーバーを介した更新、WebGuard が無効
- 自宅での使用: 既定の Avira GmbH Web サーバーを介した更新、WebGuard が有効

切り替えルールが定義されていない場合、トレイ アイコンのコンテキスト メニューを使用すると、設定を手動で切り替えることができます。設定セクションでは、設定の追加、名前変更、削除、コピー、または復元を行ったり、ナビゲーション バーのボタンまたはコンテキスト メニューのコマンドを使用して設定を切り替えるためのルールを定義したりできます。

注意
Windows 2000 では、別の設定への自動切り替えはサポートされません。Windows 2000 では、設定を切り替えるためのルールを定義できません。

設定オプションの概要

次の設定オプションを使用できます。

- **スキャナ**: オンデマンド スキャンの設定

  スキャン オプション

  検出時のアクション

  ファイル スキャン オプション

  オンデマンド スキャンの例外

  オンデマンド スキャンのヒューリスティック

  レポート機能の設定

- **Guard**: オンアクセス スキャンの設定

  スキャン オプション

  検出時のアクション

  オンアクセス スキャンの例外

  オンアクセス スキャンのヒューリスティック

  レポート機能の設定

- **MailGuard**: MailGuard の設定

  スキャン オプション: POP3 アカウント、IMAP アカウント、送信電子メール (SMTP) の監視を有効にする

  マルウェアに対するアクション

MailGuard スキャンのヒューリスティック

MailGuard スキャンの例外

キャッシュの設定、キャッシュを空にする

送信電子メールのフッターの設定

レポート機能の設定

– **WebGuard**WebGuard の設定

スキャン オプション、WebGuard 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: 不要なファイル タイプおよび MIME タイプ、既知の不要な URL の Web フィルタ (マルウェア、フィッシングなど)

WebGuard スキャンの例外: URL、ファイル タイプ、MIME タイプ

WebGuard ヒューリスティック

レポート機能の設定

– **FireWall**:FireWall の設定

アダプタ ルールの設定

ユーザー定義アプリケーション ルールの設定

信頼済みプロバイダのリスト (アプリケーションによるネットワーク アクセスの例外)

拡張設定: ルールのタイムアウト、Windows Host ファイルのロック、Windows FireWall の停止、通知

ポップアップ設定 (アプリケーションによるネットワーク アクセスのアラート)

– **全般**:

SMTP を使用した電子メールの設定

オンデマンド スキャンおよびオンアクセス スキャンのための拡張リスク カテゴリ

コントロール センターおよび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: 更新の状態表示、完全システム スキャンの状態表示、製品の保護

WMI: WMI のサポートを有効にする

イベント ログの設定

レポート機能の設定

使用するディレクトリの設定

更新: ダウンロード サーバーへの接続の設定、Web サーバーまたはファイル サーバー経由のダウンロード、製品の更新のセットアップ

アラート: 以下のコンポーネントの電子メール アラートの設定:
スキャナ
Guard
アップデータ
以下のコンポーネントのネットワーク アラートの設定: スキャナ, Guard

マルウェア検出時の音声によるアラートの設定

5.1.3 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 AntiVir プログラムのトレイ アイコンが表示されます。

アイコン	説明
	AntiVir Guard が有効になり、FireWall が有効になっています。
	AntiVir Guard が無効になり、FireWall が無効になっています。

トレイ アイコンは、Guard および FireWall サービスの状況を表示します。

AntiVir プログラムの中心機能には、トレイ アイコンのコンテキスト メニューからすばやくアクセスできます。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

- **AntiVir Guard を有効にする**: AntiVir Guard を有効または無効にします。
- **AntiVir MailGuard を有効にする**: AntiVir MailGuard を有効または無効にします。
- **AntiVir WebGuard を有効にする**: AntiVir WebGuard を有効または無効にします。
- **FireWall**:
- FireWall を有効にする: FireWall を有効または無効にします。
- すべてのトラフィックをブロック: 有効: ファイアウォールによって、ホスト コンピュータ システムへの転送以外、すべてのデータ転送がブロックされます (ローカル ホスト/IP 127.0.0.1)。
- ゲーム モードを有効にする: モードを有効または無効にします。
  有効:アクティブにすると、定義されたすべてのアダプタ ルールとアプリケーション ルールが適用されます。ルールの定義されていないアプリケーションは、ネットワーク アクセスを許可され、ポップアップ ウィンドウは表示されません。
- **AntiVir の起動**: コントロール センターを開きます。
- **AntiVir の設定**: 設定を開きます。
- **更新の開始** 更新を開始します。

- **設定の選択**:サブメニューに使用可能な設定プロファイルが表示されます。設定をクリックすると、その設定がアクティブになります。設定の自動切り替えのルールを既に定義している場合、このメニュー コマンドは無効です。
- ヘルプ: オンライン ヘルプを開きます。
- **バージョン情報 AntiVir Professional:** AntiVir プログラムに関する詳細情報のダイアログ ボックスが開きます。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**: インターネット上の Avira Web 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。

5.2 方法...

5.2.1 ライセンスのアクティブ化

AntiVir プログラムのライセンスをアクティブ化するには:

AntiVir 製品のライセンスをアクティブ化するには、ライセンス ファイル hbedv.key を使用します。このライセンス ファイルは、Avira GmbH 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 つの注文プロセスで注文したすべての製品のライセンスが含まれています。

AntiVir プログラムを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。
- AntiVir プログラム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。

AntiVir プログラムをまだインストールしていない場合:

- ファイル マネージャ、またはアクティブ化電子メールでライセンス 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 -

- AntiVir プログラムのコントロール センターで、メニュー項目 [ヘルプ] / [ライセンス ファイル...] 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。 **[続行]** 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させて、**[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。

  ライセンスがアクティブ化されます。

- 必要に応じて、システムを再起動します。

5.2.2 自動更新の実行

AntiVir Scheduler を使用してジョブを作成し、AntiVir プログラムを自動的に更新するには:

- コントロール センターで、**[管理]::[Scheduler]** セクションを選択します。
-  *[ウィザードで新規ジョブを作成]* アイコンをクリックします。

  [ジョブの名前と説明] ダイアログ 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] ダイアログ 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] ダイアログ 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
定期的で頻繁な自動更新をお勧めします。推奨の更新間隔は 60 分です。

- 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)。
  - **ジョブは、インターネット接続が確立されているときに開始してください**

    定義した頻度だけでなく、インターネット接続が設定されている場合にもジョブが実行されます。
  - **時間切れになったらジョブを繰り返す**

    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] ダイアログ 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します。
  - **最小化**: プログレス バーのみ
  - **最大化**: ジョブ ウィンドウ全体
  - **非表示**: ジョブ ウィンドウなし
- **[終了]** をクリックします。

  新たに作成したジョブは、**マネージャ::スキャン** セクションの開始ページ

にアクティブ化のステータスと共に表示されます (チェック マーク)。

► 必要に応じて、実行されてい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

 ジョブの変更

 ジョブの削除

 ジョブの開始

 ジョブの中止

5.2.3 手動更新の開始

更新を手動で開始するには複数のオプションがあります。更新を手動で開始すると、ウイルス定義ファイルとスキャン エンジンが常に更新されます。製品の更新は、**[製品の更新をダウンロードして、自動的にインストールします]** オプションが [全般] ::更新

AntiVir プログラムの更新を手動で開始するには:

► 右マウス ボタンで、タスクバーの AntiVir 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] 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、**[概要]::[状況]** セクションを選択します。

► *[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] 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] ダイアログ ボックスが表示されます。

注意
定期的な自動更新をお勧めします。推奨の更新間隔は 60 分です。

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

5.2.4 オンデマンド スキャン::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 プロファイルとは、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。

– 事前に設定済みのスキャン プロファイルを使用

事前に設定済みのスキャン 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 および 2000 の場合:

 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 の場合:

Microsoft Windows Vista の場合、現在のところ、コントロール センターには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、コントロール センターにおいて実行できます。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てウイルスとマルウェアをスキャンするには:

▶ [コントロール センター] に移動して、**[ローカル保護]::[スキャン]** セクションを選択します。

事前に設定済みのスキャン プロファイルが表示されます。

▶ 事前に設定済みのスキャン プロファイルのいずれか 1 つを選択します。

- または -

▶ *[手動による選択]* スキャン プロファイルを調整します。

- または -

▶ 新しいスキャン プロファイルを作成します。

▶ 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]* ウィンドウが表示され、オンデマンド 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 プロファイルを調整する場合は:

▶ 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します。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します。次のディレクトリ レベルが非表示になります。

▶ 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おいて次のオプションが使用できます:

- 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)
- サブディレクトリを除くディレクトリ (緑のチェック 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)

新しいスキャン プロファイルを作成する場合:

▶  **[新しいプロファイルの作成]** アイコンをクリックします。

[新しいプロファイル] プロファイルが、前に作成した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おいて次のオプションが使用できます:

- 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)
- サブディレクトリを除くディレクトリ (緑のチェック 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)

5.2.5 オンデマンド スキャン::ドラッグ アンド ドロップを使用したウイルスとマルウェアのスキャン

ドラッグ アンド ドロップを使用してウイルスとマルウェアを体系的にスキャンするには:

AntiVir プログラムのコントロール センターが開いています。

- 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、オンデマンド 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。

5.2.6 オンデマンド スキャン::コンテキスト メニューを利用したウイルスとマルウェアのスキャン

コンテキスト メニューを利用してウイルスとマルウェアを体系的にスキャンするには:

- スキャンするファイルまたはディレクトリで、右マウス ボタンをクリックします (Windows エクスプローラではデスクトップ、または開いている Windows のディレクトリ)。

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 メニューの**[選択したファイルを AntiVir でスキャン]** を選択します。

[Luke Filewalker] ウィンドウが表示され、オンデマンド 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。

5.2.7 オンデマンド スキャン::ウイルスとマルウェアの自動スキャン

注意
インストール後に、スキャン ジョブ *[完全システム スキャン]* が Scheduler に作成されます。完全システム スキャンが推奨の間隔で自動的に実行されます。

ウイルスとマルウェアを自動的にスキャンするジョブを作成するには:

- コントロール センターで、**[管理]:: [Scheduler]** セクションを選択します。
-  をクリックします。

[ジョブの名前と説明] ダイアログ 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] ダイアログ 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] ダイアログ ボックスが表示されます。

▶ スキャンを開始する時刻を選択します。

- **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)。

- **時間切れになったらジョブを繰り返す**

  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] ダイアログ 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します。

- **最小化**: プログレス バーのみ
- **最大化**: ジョブ ウィンドウ全体
- **非表示**: ジョブ ウィンドウなし

▶ スキャン終了時にコンピュータが自動的にシャットダウンするようにする場合は、*[コンピュータのシャットダウン]* オプションを選択します。このオプションを利用できるのは、表示モードが最小化または最大化に設定されている場合のみです。

▶ **[終了]** をクリックします。

新たに作成したジョブは、*マネージャ::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と共に表示されます (チェック マーク)。

▶ 必要に応じて、実行されてい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

 ジョブの変更

 ジョブの削除

 ジョブの開始

 ジョブの中止

5.2.8 オンデマンド スキャン::ルートキットおよびアクティブなマルウェアに対象を絞ったスキャン

アクティブなルートキットをスキャンするには、事前に設定済みの *[ルートキットおよびアクティブなマルウェアに対するスキャン]* スキャン プロファイルを選択します。

アクティブなルートキットを体系的にスキャンするには:

- [コントロール センター] に移動して、**[ローカル保護]:: [スキャナ]**セクションを選択します。

  事前に設定済みのスキャン プロファイルが表示されます。
- 事前に設定済みの **[ルートキットおよびアクティブなマルウェアに対するスキャン]** スキャン プロファイルを選択します。
- 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] ウィンドウが表示され、オンデマンド 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。

5.2.9 検出されたウイルスとマルウェアへの対処

AntiVir プログラム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]* セクションの設定で、ウイルスまたは不要プログラムを検出した場合に、どう対処させるかを定義できます。

Guard の ProActiv コンポーネントに関しては、設定可能なアクション オプションはありません。検出の通知は、常に *[Guard]::[不審なアプリケーションの動作]* ウィンドウに表示されます。

スキャナのアクション オプション:

– **対話型**

対話型アクション モードでは、スキャン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。
スキャナのスキャンの場合、スキャンが完了したときに、感染したファイルのリストと共にアラートが表示されます。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。すべ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するか、またはスキャナをキャンセルすることができます。

– **自動**

自動アクション モードでは、ウイ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。*[アラートの表示]* オプションを有効にした場合、ウイルスが検出されるたびに、実行されたアクションを示すアラートが表示されます。

Guard のアクション オプション:

– **対話型**

対話型アクション モードでは、データ アクセスが拒否され、デスクトップ通知が表示されます。デスクトップ通知では、検出されたマルウェアを削除するか、将来のウイルス管理のために [詳細] ボタンを使用してマルウェアをスキャナ コンポーネントに転送できます。検出の通知が含まれたウィンドウが開き、コンテキスト メニューを介して、感染したファイルの管理に関する複数のオプションを利用できます (検出::スキャナを参照)。

– **自動**

自動アクション モードでは、ウイ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。*[アラートの表示]* オプションを有効にした場合、ウイルスが検出されるたびに、デスクトップ通知が表示されます。

MailGuard、WebGuard のアクション オプション:

– **対話型**

対話型アクション モードでは、ウイ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をどう処理するかを選択できます。このオプションは初期状態で有効に設定されています。

– **自動**

自動アクション モードでは、ウイ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。*[アラートの表示]* オプションを有効にした場合、ウイルスが検出されると、アラートが表示されます。このアラートにより、実行するアクションを確認できます。

対話型アクション モードでは、検出されたウイ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 (AntiVir Guard、AntiVir スキャナ、AntiVir MailGuard、AntiVir WebGuard)、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。

スキャナ および Guard のアクション (ProActiv 検出ではない) :

– **修復**

ファイルは修復されます。

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。

– **[隔離] に移動**

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] ディレクトリである *INFECTED* に移動され、直接アクセスすることはできなくなります。 このディレクトリのファイルは、後で [隔離] で修復できます。必要があれば、Avira GmbH に送信することもできます。

– **削除**

ファイルは削除されます。このプロセスは、*[上書きおよび削除]* よりはるかに速くなります。ブート セクタ ウイ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 ウイ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。

– **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。この場合、ファイルは復元できません。

– **名前の変更**

*.*vir* 拡張子を追加して、ファイルの名前が変更されます。これらのファイルへの直接のアクセス (ダブルクリックなど) はできなくなります。ファイルは後で修復して、元の名前に変更できます。

– **無視**

特別な操作は行いません。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。

警告
これは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してください。

– **常に無視**

Guard による検出に対するアクション オプション: Guard によるさらなる操作は行われません。ファイルへのアクセスが許可されます。このファイルに対する以降のすべてのアクセスが許可されます。また、コンピュータを再起動するか、ウイルス定義ファイルを更新するまで、さらなる通知は提示されません。

– **[隔離] にコピー**

[ルートキットの検出に対するアクション] オプション: 検出されたファイルは、[隔離] にコピーされます。

– **ブート セクタを修復 | 修復ツールのダウンロード**

感染したブート セクタが検出されたときのアクション 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に、さまざまなオプションを利用できます。AntiVir プログラムが修復を実行できない場合は、ブート セクタ ウイルスを検出および削除するための特殊なツールをダウンロードできます。

注意
実行中のプロセスでアクションを実行する場合は、問題のプロセスが終了されてからアクションが実行されます。

ProActiv コンポーネントによって行われた検出に対する Guard のアクション (アプリケーションの不審なアクション):

– **信頼済みのプログラム**

アプリケーションは引き続き実行されます。このプログラムは許可されているアプリケーションのリストに追加され、ProActiv コンポーネントによる監視から除外されます。許可されているアプリケーションのリストに追加すると、監視タイプは *[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場合のみ、ProActiv コンポーネントによる監視から除外されます (設定::Guard::ProActiv::アプリケーション フィルタ::許可されるアプリケーションを参照)。

– **1 回のみプログラムをブロック**

アプリケーションはブロックされます (アプリケーションは終了されます)。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って監視されます。

– **このプログラムを常にブロック**

アプリケーションはブロックされます (アプリケーションは終了されます)。このプログラムはブロックされているアプリケーションのリストに追加され、実行されなくなります (設定::Guard::ProActiv::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を参照)。

– **無視**

アプリケーションは引き続き実行されます。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って監視されます。

MailGuard アクション: 受信電子メール

– **[隔離] に移動**

電子メールはすべての添付ファイルと共に [隔離] に移動されます。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。

– **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、既定のテキストで置換されます。電子メールのテキストの本文が感染した場合は、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、Quarantine 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
この方法を使用すると、ウイ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、添付ファイルは絶対にダブルクリックで開かないでください。

MailGuard アクション: 送信電子メール

– **[隔離] にメールを移動 (送信はしない)**

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 プログラムでエラー メッセージを受信します。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 (送信はしない)**

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 プログラムでエラー メッセージを受信します。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は送信されます。

警告
この方法で、ウイルスや不要プログラムがコンピュータ システムに侵入する可能性があります。

WebGuard アクション:

– **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旨のエラー 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/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、感染したファイルは、[隔離] から復元できます。また、必要に応じて Avira マルウェア研究センターに送信できます。

– **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/ファイルは WebGuard によって Web ブラウザに送信されます。

警告
この方法を使用すると、ウイ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してください。

注意
修復できない疑わしいファイルはすべて [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弊社での分析用にお送りいただくこともできます。
たとえば、これらのファイルを弊社の Web サイトにアップロードすることもできます。http://www.avira.jp/support/upload
ヒューリスティック スキャン機能によって報告されたファイルは、*HEUR/* または *HEURISTIC/* がファイル名の前に付いています。例 : *HEUR/testfile.**.

5.2.10 隔離::隔離されたファイルの処理 (*.qua)

隔離されたファイルを処理するには:

- 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再読み込みすることができます。

ファイルに関する詳細情報を表示するには:

- ファイルをハイライト表示して  をクリックします。

  [プロパティ] ダイアログ ボックスにファイルの詳細情報が表示されます。

ファイルを再スキャンするには:

AntiVir プログラムのウイルス定義ファイルが更新されていて、誤検出報告が疑われる場合は、ファイルのスキャンをお勧めします。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。

  ファイルには、オンデマンド スキャンの設定を使用して、ウイルスとマルウェアの検索が実行されます。

  スキャン後、*[スキャンの統計データ]* が表示され、再スキャン前後のファイルの状況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には:

- ファイルをハイライト表示して  をクリックします。

ファイルを分析のために Avira マルウェア研究センター Web サーバーにアップロードする場合:

- 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。
- 必要なデータをすべて入力します。
- タイプの選択: **[不審なファイル]** または **[誤検出]**。
- **[OK]** をクリックします。

ファイルは圧縮形式で Avira マルウェア研究センター Web サーバーにアップロードされます。

注意
次の場合は、Avira マルウェア研究センターによる分析をお勧めします。
ヒューリスティック スキャン機能による検出 (疑わしいファイル): スキャン中、AntiVir プログラムによってファイルが疑わしいと分類され、[隔離] に移動された場合: ウイルス検出ダイアログ ボックス内またはスキャンによって生成されたレポート ファイル内で、Avira マルウェア研究センターでのファイルの分析を行うことが勧告された。
疑わしいファイル: ファイルを疑わしいと判断して [隔離] に移動した後、ウイルスおよびマルウェアについてファイルをスキャンしたが陰性と判定された場合。
誤検出: 誤検出でウイルスが検出されたと思われる場合: AntiVir プログラムによってファイルが検出されたが、マルウェアの感染の可能性はほとんどないと思われる。

注意
アップロードするファイルのサイズ制限は、未圧縮で 20 MB、圧縮済みで 8 MB までです。

注意
複数のファイルを一度にアップロードするには、対象のファイルをすべて選択し、**[オブジェクトの送信]** ボタンをクリックします。

隔離されたオブジェクトを隔離から他のディレクトリに移動する場合:

▶ 隔離オブジェクトをハイライト表示して  をクリックします。

スキャン ダイアログが開き、ディレクトリを選択できます。

▶ 隔離オブジェクトのコピーを保存するディレクトリを選択し、選択を確認します。

選択された隔離オブジェクトが、選択したディレクトリに保存されます。

注意
隔離されたオブジェクトは復元されたファイルと同一ではありません。隔離されたオブジェクトは暗号化され、元の形式で実行または読み取ることができなくなります。

隔離されたオブジェクトのプロパティをテキスト ファイルでエクスポートする場合:

▶ 隔離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からのデータを含むテキスト ファイルが開きます。

▶ テキスト ファイルを保存します。

[隔離] 内のファイルは復元することもできます。

– 隔離: [隔離] 内のファイルの復元の章を参照してください。

5.2.11 隔離::[隔離] 内のファイルの復元

オペレーティング システムにより、さまざまなアイコンで復元手順が制御されます。

– Windows XP および 2000 の場合:

 このアイコンは、元のディレクトリのファイルを復元します。

 このアイコンは、選択したディレクトリのファイルを復元します。

– Windows Vista の場合:

Microsoft Windows Vista の場合、現在のところ、コントロール センターには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、コントロール センターにおいて実行できます。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、選択したディレクトリのファイルを復元します。

 このアイコンは、元のディレクトリの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] 内のファイルを復元するには:

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 センターで、**[管理]::[隔離]** セクションを選択します。

注意
ファイル拡張子が **.eml* の場合、電子メールと電子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。

元の場所のファイルを復元するには:

▶ ファイルをハイライト表示して、次のアイコン (Windows 2000/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、電子メールには使用できません。

注意
ファイル拡張子が **.eml* の場合、電子メールと電子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。

ファイルを指定したディレクトリに復元するには:

▶ 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。

Windows 標準のディレクトリ選択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。

5.2.12 隔離::疑わしいファイルを [隔離] に移動

疑わしいファイルを手動で [隔離] に移動するには:

▶ 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 標準のファイル選択ウィンドウが表示されます。

▶ ファイルを選択して確定します。

ファイルは、[隔離] に移動されます。

[隔離] 内のファイルは、AntiVir スキャナを使用してスキャンできます。

- 隔離: 隔離されたファイル (*.qua) の処理の章を参照してください。

5.2.13 スキャン プロファイル::スキャン プロファイルのファイル タイプの変更または削除

スキャン プロファイルで特定のファイル タイプをスキャン対象に含めるか、スキャン対象から除外するには (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、**[ローカル保護]::***[スキャン]* セクションに移動します。

▶ 右マウス ボタンで、編集するスキャン 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 メニューをさらに展開します。

[既定]、*[すべてのファイルのスキャン]*、および *[ユーザー定義]* というエントリが表示されます。

▶ **[ユーザー定義]** を選択します。

[ファイル拡張子] ダイアログ ボックスが、スキャン プロファイルを使用してスキャンされるすべてのファイル タイプのリストと共に表示されます。

特定のファイル タイプをスキャン対象から除外するには:

▶ 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。

特定のファイル タイプをスキャンに追加するには:

▶ ファイル タイプをハイライト表示します。

▶ **[追加]** をクリックして、入力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 文字を入力できます。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？) を使用することもできます。

5.2.14 スキャン プロファイル::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

オンデマンド スキャンは、AntiVir プログラムのコントロール センターにアクセスせずに、スキャン プロファイルへのデスクトップ ショートカットを使用して、デスクトップから直接開始できます。

スキャン プロファイルへのデスクトップ ショートカットを作成するには:

コントロール センターで、**[ローカル保護]::***[スキャン]* 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。

▶  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。

5.2.15 イベント::フィルタ イベント

AntiVir プログラム コンポーネントによって生成されたイベントは、コントロール センターの **[概要]::[イベント]** 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に似ています)。プログラムのコンポーネントは次のとおりです。

- アップデータ
- Scheduler
- Guard
- MailGuard
- スキャナ
- FireWall
- WebGuard
- ヘルパー サービス
- ProActiv

次のイベント タイプが表示されます。

- 情報
- 警告
- エラー
- 検出

表示されたイベントにフィルタを適用するには:

- コントロール センターで、**[概要]::[イベント]** セクションを選択します。
- アクティブにされた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 -

  非表示の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。

5.2.16 MailGuard::電子メール アドレスをスキャン対象から除外

MailGuard のスキャン対象から除外する電子メール アドレス (送信者) を定義するには (ホワイトリスト):

- [コントロール センター] に移動して、**[オンライン保護]::[MailGuard]** を選択します。

  リストに受信電子メールが表示されます。
- MailGuard 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。
- 適切なアイコンをクリックして、MailGuard のスキャンから電子メールを除外します。

   今後、選択した電子メール アドレスにウイルスと不要プログラムのスキャンを実行しません。

送信者の電子メール アドレスは除外リストに含められ、ウイルス、マルウェア、のスキャンは実行されなくなります。

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 MailGuard のスキャン対象から除外してください。

注意
MailGuard::全般::例外の設定で、他の電子メール 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。

5.2.17 FireWall : FireWall のセキュリティ レベルの選択

セキュリティ レベルには、さまざまな選択肢があります。選択したレベルによって、アダプタ ルールの設定オプションも異なります。

次のセキュリティ レベルが使用できます。

– **低**

- フラッディングとポート スキャンが検出されます。

– **中**

- 疑わしい TCP パッケージと UDP パッケージが破棄されます。
- フラッディングとポート スキャンが禁止されます。

– **高**

- コンピュータはネットワーク上で非表示になります。
- 外部からの接続はブロックされます。
- フラッディングとポート スキャンが禁止されます。

– **ユーザー**

- ユーザー定義ルール: このセキュリティ レベルを選択すると、プログラムはアダプタ ルールが変更されたことを自動的に認識します。

注意
Avira FireWall のすべての事前に設定済みのルールに対する既定のセキュリティ レベル設定は、**[高]** です。

FireWall のセキュリティ レベルを定義するには:

▶ [コントロール センター] に移動して、**[オンライン保護]::[FireWall]** を選択します。

▶ スライダを必要なセキュリティ レベルに移動します。

選択したセキュリティ レベルは、すぐに適用されます。

6 スキャナ

スキャナ コンポーネントを使用すると、ウイルスと不要プログラムに対する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。ファイルの感染を調べるスキャンでは、次のオプションを使用できます。

- **コンテキスト メニューを利用したオンデマンド スキャン**
  コンテキスト メニューを利用したオンデマンド スキャン (右マウス ボタンから **[選択したファイルを AntiVir でスキャン]**) は、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。もう 1 つの利点は、コンテキスト メニューを利用したオンデマンド スキャンでは、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。
- **ドラッグ アンド ドロップを介したオンデマンド 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、スキャナはファイルまたはディレクトリ、および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、デスクトップなどに保存した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。
- プロファイルを介したオンデマンド 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。
- **Scheduler を介したオンデマンド スキャン**
  Scheduler を使用すると、時間制御スキャンを実行できます。

ルートキット、ブート セクタ ウイルス、アクティブ プロセスのスキャンには、特別なプロセスが必要です。次のオプションがあります。

- *[ルートキットおよびアクティブなマルウェアに対するスキャン]* スキャン プロファイルにより、ルートキットをスキャンします。
- **[アクティブなプロセス]** スキャン プロファイルを使用してアクティブなプロセスをスキャンします。
- **[その他]** メニューの **[ブート セクタ ウイルスのスキャン]** メニュー コマンドを使用してブート セクタ ウイルスをスキャンします。

7 更新

アンチウイルス ソフトウェアの有効性は、特にウイルス定義ファイルとスキャン エンジンがどれだけ新しいかによって異なります。定期的な更新を行うために、アップデータ コンポーネントが AntiVir に統合されています。アップデータにより AntiVir プログラムは常に最新状態に保たれ、毎日登場する新しいウイルスに対処できます。アップデータは、次のコンポーネントを更新します。

– ウイルス定義ファイル:

ウイルス定義ファイルには、有害なプログラムのウイルス パターンが含まれています。これは、AntiVir プログラムがウイルスやマルウェアのスキャンや感染したオブジェクトの修復に使用します。

– スキャン エンジン:

スキャン エンジンには、ウイルスとマルウェアのスキャンに AntiVir プログラムが使用する方法が含まれています。

– プログラム ファイル (製品の更新プログラム):

製品の更新パッケージは、個々のプログラム コンポーネントで追加機能を使用可能にします。

更新によって、ウイルス定義ファイルとスキャン エンジンが最新かどうかがチェックされ、必要に応じて更新が実装されます。設定済みの項目に従って、アップデータは製品の更新も実行するか、製品の更新プログラムが利用可能であることを通知します。製品の更新後に、コンピュータ システムの再起動が必要になることがあります。ウイルス定義ファイルとスキャン エンジンのみが更新される場合、コンピュータの再起動は不要です。

注意
セキュリティ上の理由から、アップデータは、コンピュータの Windows Host ファイルが改変され、たとえば、更新 URL がマルウェアに操作され、アップデータが不要なダウンロード サイトに向けられていないかをチェックします。Windows Host ファイルが操作されると、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、60 分 の間隔で自動的に行われます。自動更新は、設定 (設定::更新) を通じて編集または無効にすることができます。

コントロール センターの Scheduler では、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: [状況] セクションの [更新] メニュー
– 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、インターネットで独自の Web サーバーから、またはインターネットから更新ファイルをダウンロードするイントラネットのファイル サーバーから取得して、ネットワーク上の他のコンピュータで使用可能にすることができます。これは、AntiVir プログラムをネットワーク上の複数のコンピュータで更新する場合に便利です。イントラネット上のダウンロード サーバーを使用すると、最低限のリソースで、保護対象のコンピュータの AntiVir プログラムを最新状態にすることができます。イントラネット上で機能するダウンロード サーバーを設定するには、AntiVir プログラムの更新構造と互換性のあるサーバーが必要です。

注意

AntiVir Internet Update Manager (Windows のファイル サーバーまたは Web サーバー) を、イントラネット上の Web サーバーまたはファイル サーバーとして使用できます。AntiVir Internet Update Manager は、Avira AntiVir 製品のダウンロード サーバーをミラーするもので、インターネットの Avira Web サイトから入手できます。
http://www.avira.jp

Web サーバーを使用する場合は、ダウンロードに HTTP プロトコルが使用されます。ファイル サーバーを使用する場合は、ネットワークを介して提供された更新ファイルにアクセスします。Web サーバーまたはファイル サーバーに対する接続は、全般::更新の [設定] で設定できます。既定の設定は、既存のインターネット接続を Avira GmbH Web サーバーへの接続として使用します。

8 Avira FireWall::概要

Avira FireWall は、コンピュータ システム上の受信および送信データ トラフィックを監視および制限して、インターネットからのさまざまな攻撃および脅威からコンピュータを保護します。セキュリティ ガイドラインに基づき、受信/送信データ トラフィックやポートのリッスンが許可または拒否されます。Avira FireWall によってネットワーク アクティビティが拒否され、ネットワーク接続がブロックされた場合は、デスクトップ通知が表示されます。Avira FireWall の設定では、次のオプションを使用できます。

– コントロール センターのセキュリティ レベルの設定

コントロール センターのセキュリティ レベルを定義できます。*[低]*、*[中]*、および *[高]* の各セキュリティ レベルには、パケット フィルタに基づいていくつかの補足的なセキュリティ ルールが含まれています。これらのセキュリティ ルールは、FireWall::アダプタ ルールで事前に設定済みのアダプタ ルールとして設定に保存されます。

– [ネットワーク イベント] ウィンドウ内のアクションを記憶

アプリケーションがネットワーク接続またはインターネット接続を初めて作成しようとすると、*[ネットワーク イベント]* ポップアップ ウィンドウが表示されます。ユーザーは、*[ネットワーク イベント]* ウィンドウを使用して、アプリケーションのネットワーク アクティビティを許可するかまたは拒否するかを選択できます。**[このアプリケーションに対するアクションを記憶]** オプションを有効にしている場合、アクションがアプリケーション ルールとして作成され、[FireWall]::[アプリケーション ルール] の設定に保存されます。アクションを [ネットワーク イベント] ウィンドウに保存することで、アプリケーションのネットワーク アクティビティに対する一式のルールを利用できるようになります。

注意
信頼済みプロバイダからのアプリケーションの場合、アダプタ ルールによって禁止されていない限り、ネットワーク アクセスは既定で許可されます。信頼済みプロバイダのリストからこのプロバイダを削除することもできます。

– 設定でのアダプタおよびアプリケーション ルールの作成

設定では、事前に設定済みのアダプタ ルールを変更したり、新しいアダプタ ルールを作成したりできます。アダプタ ルールの追加または変更を行った場合、FireWall のセキュリティ レベルは自動的に値 *[ユーザー]* に設定されます。
アプリケーション ルールを使用すると、アプリケーションに対して指定された監視ルールを定義できます。
単純なアプリケーション ルールでは、ソフトウェア アプリケーションのすべてのネットワーク アクティビティを拒否/許可するかどうか、または *[ネットワーク イベント]* ポップアップ ウィンドウを使用してその処理方法を決定するかどうかを定義できます。
[アプリケーション ルールの設定] の詳細設定では、アプリケーションに対して別のパケット フィルタを定義できます。このフィルタは、指定されたアプリケーション ルールとして実行されます。

注意
アプリケーション ルールには、*特権*モードと *フィルタ* モードの 2 つの異なるモードがあります。*フィルタ* モードのアプリケーション ルールの場合、該当するアダプタ ルールは優先的に実行されます。つまり、アプリケーション ルールの実行後に、アダプタ ルールが実行されます。したがって、高いセキュリティ レベルまたは対応するアダプタ ルールが原因でネットワーク アクセスが拒否される可能性があります。*特権*モードのアプリケーション ルールの場合、アダプタ ルールは無視されます。*特権*モードでアプリケーションが許可されている場合、アプリケーションは常にネットワーク アクセスを許可されます。

9 FAQ、ヒント

この章には、トラブルシューティングに関する重要な情報およびAntiVirプログラムの使用に関するより詳細なヒントが含まれます。

「トラブルシューティング」の章を参照。

「キーボード コマンド」の章を参照。

「Windows セキュリティ センター」の章参照。

9.1 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。
- AntiVir MailGuard が機能しません。
- Avira FireWall をホスト マシンにインストールし、Avira FireWall のセキュリティ レベルを中、または高に設定した場合に、仮想マシン (VMWare、Virtual PC など) で使用できるネットワーク接続がありません。
- Avira FireWall のセキュリティ レベルが中、または高に設定されていると、Virtual Private Network (VPN) 接続がブロックされます。
- TSL 接続を介して送信した電子メールが MailGuard にブロックされました。
- Webchat が機能しません。チャット 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。

理由: ファイルが暗号化されています。

▶ ライセンスをアクティブ化するためにファイルを開く必要はありませんが、プログラム ディレクトリに保存する必要があります。「ライセンス マネージャ」の章も参照。

更新を開始しようとすると、エラー メッセージ *"ファイルのダウンロード中に接続に失敗しました ..."* が表示されます。

理由: インターネット接続が非アクティブになっています。したがって、インターネットで Web サーバーへの接続は確立できません。

▶ 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。これらのサービスが機能していない場合は、インターネット接続を再確立してください。

理由: 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。

理由: 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。

該当しない場合:

▶ 全般::更新の設定で、設定 (エキスパート モード) をチェックします。

ウイルスとマルウェアの移動や削除ができません。

理由: 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。

▶ AntiVir 製品を更新します。

▶ Windows XP オペレーティング システムを使用している場合は、システムの復元を非アクティブにします。

▶ コンピュータをセーフ モードで起動します。

▶ AntiVir プログラムおよび設定 (エキスパート モード) を起動します。

▶ スキャナ::スキャン::ファイル::すべ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。

▶ 他のウイ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アクティブにします。

トレイ アイコンの状況が無効になっています。

理由: AntiVir Guard が無効になっています。

▶ コントロール センターの概要::状況セクションで、[AntiVir Guard] 領域の **[有効化]** リンクをクリックします。

理由: AntiVir Guard がファイアウォールでブロックされています。

▶ ファイアウォールの設定で、AntiVir Guard を全般的に承認するように定義します。AntiVir Guard は、アドレス 127.0.0.1 (localhost) でのみ機能します。インターネット接続は確立されません。AntiVir MailGuard も同様です。

該当しない場合:

▶ AntiVir Guard サービスのスタートアップの種類を確認してください。必要に応じて、サービスを有効にします。タスクバーで [スタート | 設定 | コントロール パネル] を選択します。ダブルクリックで、[サービス] 設定パネルを開始します (Windows 2000 および 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 AntiVir Guard* を検索します。スタートアップの種類には "自動"、状態には "開始" を指定する必要があります。必要に応じて、該当する行と、[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。

理由: バックアップ プロシージャ中、AntiVir Guard はバックアップ プロシージャによって使用されるすべてのファイルをスキャンします。

▶ 設定 (エキスパート モード) で、Guard::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。

ファイアウォールから、AntiVir Guard と AntiVir MailGuard のレポートをアクティブ化直後に受け取りました。

理由: AntiVir Guard および AntiVir MailGuard との通信が、TCP/IP インターネット プロトコルを介して行われています。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。

▶ AntiVir Guard および AntiVir MailGuard を全般的に承認するように定義します。AntiVir Guard は、アドレス 127.0.0.1 (localhost) でのみ機能します。インターネット接続は確立されません。AntiVir MailGuard も同様です。

AntiVir MailGuard が機能しません。

AntiVir MailGuard 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、AntiVir MailGuard 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 (TSL - Transport Layer Security とも呼ばれる) を介してサーバーに報告しているかどうかを確認してください。AntiVir MailGuard は SSL をサポートしていないので、暗号化されている SSL 接続を終了します。MailGuard で保護せずに、暗号化されている SSL 接続を使用する場合は、接続用に MailGuard によって監視されていないポートを使用する必要があります。MailGuard によって監視されているポートは、MailGuard::スキャンの下で設定できます。

▶ AntiVir MailGuard サービスはアクティブですか。必要に応じて、サービスを有効にします。タスクバーで [スタート | 設定 | コントロール パネル] を選択します。ダブルクリックで、[サービス] 設定パネルを開始します (Windows 2000 および 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 AntiVir MailGuard* を検索します。スタートアップの種類には "自動"、状態には "開始" を指定する必要があります。必要に応じて、該当する行と、[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 AntiVir プログラムをアンインストールし、AntiVir プログラム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) とも呼ばれる) を介した暗号化 POP3 接続には現在保護が行われず、無視されます。

▶ メール サーバーに対する検証は、現在 "パスワード" を介してのみサポートされています。"Kerberos" と "RPA" は現在サポートされていません。

▶ AntiVir プログラムは、送信電子メールのウイルスと不要プログラムはチェックしません。

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。

Avira FireWall をホスト マシンにインストールし、Avira FireWall のセキュリティ レベルを中、または高に設定した場合に、仮想マシン (VMWare、Virtual PC など) で使用できるネットワーク接続がありません。

Avira FireWall がコンピュータにインストールされ、仮想マシン (VMWare、Virtual PC など) が起動していて、Avira FireWall のセキュリティ レベルが中、または高に設定されていると、ファイアウォールは仮想マシンに対するすべてのネットワーク接続をブロックします。セキュリティ レベルが低に設定されている場合、FireWall は予想どおりに機能します。

理由: 仮想マシンがソフトウェアを介して、ネットワーク カードにエミュレートされています。このエミュレーションでは、特殊なパッケージ (UDP パッケージ) でゲスト システムのデータ パッケージがカプセル化され、外部ゲートウェイを介して、ホスト システムに戻るように経路が設定されます。セキュリティ レベルを中で開始すると、Avira FireWall はこれらのパッケージを外部からのパッケージとして拒否します。

この動作を避けるには、以下を実行してください。

▶ [コントロール センター] に移動して、**[オンライン保護]::[FireWall]** を選択します。

▶ **[設定]** リンクをクリックします。

▶ *[設定]* ダイアログ ボックスが表示されます。ここは *[アプリケーション ルール]* 設定セクションです。

▶ **[エキスパート モード]** オプションを有効にします。

▶ **[アダプタ ルール]** 設定セクションを選択します。

▶ **[ルールの追加]** をクリックします。

▶ **[UDP]** を *[着信ルール]* セクションで選択します。

▶ ルールの [セクション名] にルールの**名前**を入力します。

▶ **[OK]** をクリックします。

▶ ルールが、**[すべての IP パケットを拒否]** のすぐ上にあることを確認します。

警告
このルールは、フィルタリングなしで UDP パケットを許可するため、危険な場合があります。仮想マシンでの作業後は、前のセキュリティ レベルに変更してください。

Avira FireWall のセキュリティ レベルが中、または高に設定されていると、Virtual Private Network (VPN) 接続がブロックされます。

理由: この問題は、このルールより上のいずれかのルールに一致しないすべてのパケットを破棄する最後のルール **[すべての IP パケットを拒否]** によって発生しています。VPN ソフトウェア (GRE パケット) によって送信されるパッケージの種類は、他のカテゴリに一致しないため、このルールによってフィルタされます。

[すべての IP パケットを拒否] ルールを TCP パケットと UPD パケットを拒否する、新しい 2 つのルールで置換します。これにより、他のプロトコルのパケットを許可できます。

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

理由: 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、現在では MailGuard でサポートされていません。電子メールの送信には、次のオプションが使用可能です。

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

Webchat が機能しません。チャット 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て、HTTP プロトコルに基づいたチャット中に発生する場合があります。

理由: WebGuard は、送信データが Web ブラウザに読み込まれる前に、ウイ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、WebGuard 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 (設定::WebGuard::例外を参照)。

9.2 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) - 個々のモジュールにすばやく移動し読み出して、プログラムを介したアクションを開始できます。

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、ヘルプの対応する章に記載されています。

9.2.1 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します。
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します。
← ↑ → ↓	設定セクションでのナビゲーション 最初に、マウスを使用して設定セクションにフォーカスを設定します。
Tab	次のオプション、またはオプション グループに変更します。
Shift + Tab	前のオプション、またはオプション グループに変更します。
← ↑ → ↓	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り替えます。
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 + 下線付きで表示された文字	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、またはボタンに対するコマンドを開始します。

9.2.2 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を切り替えます。
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 ウィンドウの次のセクションに移動します。
Ctrl + Shift + Tab	ナビゲーション ウィンドウの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変更します。

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変更します。
Page up Page down	テーマを閲覧します。

9.2.3 コントロール センター内

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	更新
F8	設定を開く
F9	更新の開始

[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 リンクを作成
Insert	新しいプロファイルの作成
Delete	選択したプロファイルの削除

[FireWall] セクション

ショートカット	説明
Return	プロパティ

[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	復元先を指定してオブジェクトを復元...
Return	プロパティ

Insert	ファイルの追加
Delete	オブジェクトの削除

[Scheduler] 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
Insert	新規ジョブの挿入
Delete	ジョブの削除

[レポート] セクション

ショートカット	説明
F3	レポート ファイルの表示
F4	レポート ファイルの印刷
Return	レポートの表示
Delete	レポートの削除

[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
Delete	イベントの削除

9.3 Windows セキュリティ センター

- Windows XP Service Pack 2 以降 -

9.3.1 全般

Windows セキュリティ センターは、重要なセキュリティ面について、コンピュータの状況をチェックします。

これらの重要点のいずれかで問題が検出されると (古いアンチウイルス プログラムなど)、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。

9.3.2 Windows セキュリティ センターと AntiVir プログラム

FireWall

ファイアウォールに関して、セキュリティ センターから次の情報を受け取る場合があります。

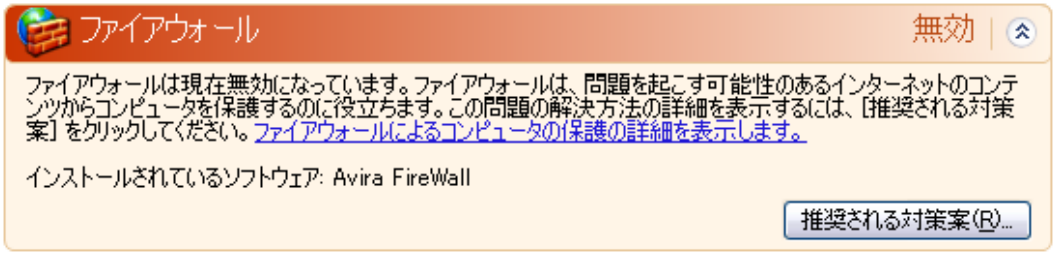
- FireWall: 有効/FireWall: オン
- FireWall: 無効/FireWall: オフ

FireWall: 有効/FireWall: オフ

AntiVir プログラムをインストールし、Windows ファイアウォールをオフにすると、以下のメッセージが表示されます。

FireWall: 無効/FireWall: オフ

Avira FireWall を無効にすると、すぐに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 [状況] タブを介して、Avira FireWall を有効または無効にできます。

警告

Avira FireWall をオフにすると、ネットワークまたはインターネットを介した許可されていないユーザーによるアクセスの取得を防止することができなくなります。

アンチウイルス ソフトウェア/悪意のあるソフトウェアに対する保護

ウイルス対策に関して、Windows セキュリティ センターから、次のような情報を受け取る場合があります。

ウイルス対策: 見つかりません

ウイルス対策: 最新の状態ではありません

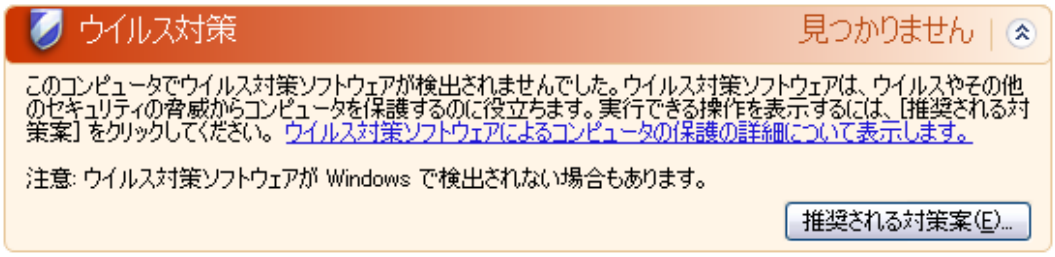
ウイルス対策: 有効

ウイルス対策: 無効

ウイルス対策: 監視していません

ウイルス対策: 見つかりません

コンピュータ上でアンチウイルス ソフトウェアを発見できない場合、Windows セキュリティ センターはこの情報を表示します。



注意

コンピュータに AntiVir プログラムをインストールして、ウイルスやその他の不要プログラムから保護してください。

ウイルス対策: 最新の状態ではありません

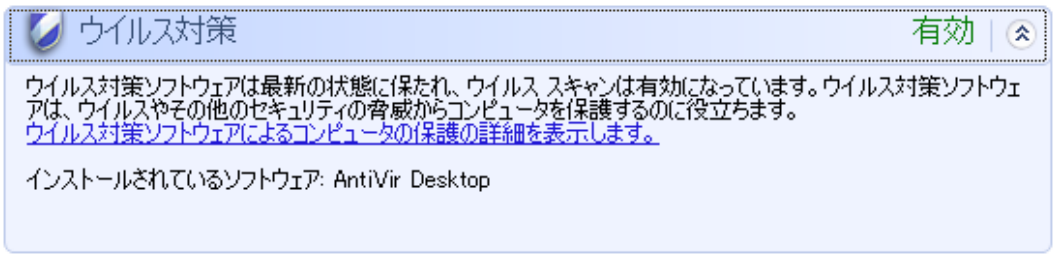
Windows XP Service Pack 2 または Windows Vista をインストールしているシステムに AntiVir プログラムをインストールしたり、AntiVir プログラムが既にインストールされているシステムに Windows XP Service Pack 2 または Windows Vista をインストールすると、次のメッセージが表示されます。

注意

Windows セキュリティ センターに AntiVir プログラム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が必要です。更新を実行して、システムを更新してください。

ウイルス対策: 有効

AntiVir プログラムをインストールして更新すると、次のメッセージが表示されます。



AntiVir プログラムは最新状態になり、AntiVir Guard が有効になっています。

ウイルス対策: 無効

AntiVir Guard を無効にしたり、Guard 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

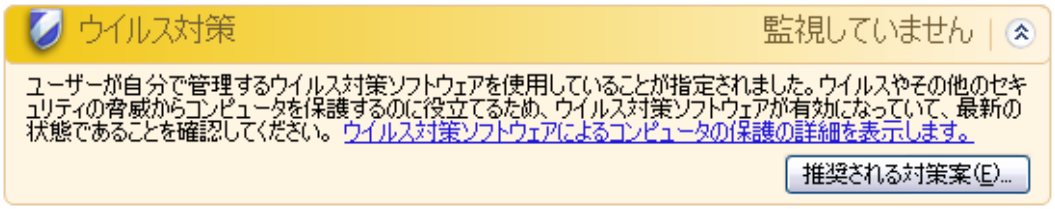
コントロール センターの概要::状況セクションで、AntiVir Guard を有効または無効にできます。AntiVir Guard が有効になっているかどうかは、タスクバーで赤い傘が開いているかどうかでも確認できます。

ウイルス対策: 監視していません

アンチウイルス ソフトウェアの監視を自分で実行しようとすると、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

Windows Vista ではこの機能はサポートされません。



注意

Windows セキュリティ センターは、AntiVir プログラムによりサポートされています。このオプションは [推奨される対策案...] ボタンでいつでも有効にできます。

注意

Windows XP Service Pack 2 または Windows Vista をインストールしていても、ウイルス対策は必要です。Windows XP Service Pack 2 以降は、アンチウイルス ソフトウェアを監視しますが、それ自体がアンチウイルス機能を持っているわけではありません。このため、別のアンチウイルス ソリューションを使用しないと、ウイルスやマルウェアに対して保護されないことになります。

10 ウイルスなど

10.1 脅威カテゴリ (拡張)

ダイヤラ (DIALER)

インターネットには、一部有料のサービスがあります。このようなサービスは、ドイツでは、0190 または 0900 という局番でダイヤラを介して請求されます (オーストリアとスイスでは 09x0。ドイツでは中期的に 09x0 への変更が予定されています)。このようなプログラムがコンピュータにインストールされると、適切な割り増し料金の番号を使用した接続が行われますが、料金の範囲はかなり幅広くなっています。

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、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、間違いなくユーザーが意図的に使用するものです。ユーザーの同意により、ユーザーのコンピュータにインストールされるだけであり、これは完全に明白ではっきりとわかるラベル、またはリクエストを介して行われる必要があります。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、正規のダイヤラによって発生した費用は正確に間違いなく伝達されます。

残念ながら、気付かれずに疑わしい方法や不正な意図でコンピュータにインストールされるダイヤラもあります。たとえば、このようなダイヤラは、ISP (インターネット サービス プロバイダ) へのインターネット ユーザーの既定のデータ通信を置換して、接続が行われるたびに、0190/0900 で始まる有料の番号や極端に高額な費用が発生する番号にダイヤルさせます。影響を受けたユーザーは、コンピュータ上の不要な 0190/0900 ダイヤラ プログラムが接続のたびに割り増し料金でダイヤルしていて、極端に費用が増加していることを、次の電話料金の請求書が届くまで気付かない可能性があります。

このような場合は、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。

AntiVir プログラムは、よく使用されるダイヤラを既定で検出します。

[脅威カテゴリ (拡張)] の設定でチェック マークをオンにして **[ダイヤラ]** オプションを有効にすると、ダイヤラが検出されたときに、対応するアラートが送信されます。不要な 0190/0900 ダイヤラである可能性のあるダイヤラは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。

ゲーム (GAMES)

コンピュータ ゲーム用の場所もありますが、昼休み中などを除き、仕事中には必要ありません。それでも、インターネットからダウンロード可能な多数のゲームがあるため、会社員や公務員もかなりマイン スイーパーや Patience などのゲームをしています。ユーザーはさまざまなゲームをインターネットでダウンロードできます。電子メール ゲームも人気が出てきて、簡単なチェスから、魚雷を使用した戦闘が含まれた "船隊演習" まで、さまざまなゲームが配布されています。ゲームの動きは電子メール プログラムを通じて、パートナーに伝達されるようになっています。

調査によると、コンピュータ ゲームに費やされる労働時間は、経済的にかなりの比率を占めるところまで達しています。このため、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している企業が増えているのも当然のことでしょう。

AntiVir プログラムはコンピュータ ゲームを認識します。[脅威カテゴリ] の設定にチェック マークを入れて、**[ゲーム]** オプションを有効にすると、AntiVir プログラムがゲームを検出した場合に、対応するアラートが送信されます。ゲームは簡単に削除できるので、文字通り「ゲーム オーバー」になります。

ジョーク (JOKES)

ジョークとは、損害を与えたり、複製を作成したりせず、ただ誰かを驚かせたり、楽しませるためのものです。ジョーク プログラムが読み込まれると、どこかで音を出したり、何か変わった物を画面に表示したりします。ジョークの例としては、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) などが挙げられます。

ただし、注意してください。ジョーク プログラムのあらゆる現象は、ウイ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。少なくとも、自分自身が本当に被害を被ったとなれば、大きなショックを受けパニックになるでしょう。

スキャンと識別ルーチンの拡張により、AntiVir プログラムはジョーク 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できます。[脅威カテゴリ] の設定にチェック マークを入れて **[ジョーク]** オプションを有効にすると、ジョーク プログラムが検出された場合に対応するアラートが送信されます。

セキュリティ プライバシ リスク (SPR)

システムのセキュリティに問題を生じさせる、不要プログラムの活動を開始する、ユーザーのプライバシを損害する、ユーザーの操作を探るなど、望ましくないソフトウェアです。

AntiVir プログラムは "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。[脅威カテゴリの拡張] の設定にチェック マークを入れて **[セキュリティ プライバシ リスク]** オプションを有効にすると、AntiVir プログラムが該当するソフトウェアを検出した場合に、対応するアラートが送信されます。

バックドア クライアント (BDC)

バックドア サーバー プログラムは、データを盗んだり、コンピュータを操作するために、ユーザーが知らない間に忍び込みます。このプログラムは、インターネットまたはネットワークを介してバックドア制御ソフトウェア (クライアント) で第三者による制御が可能です。

AntiVir プログラムは "バックドア制御のコンピュータ ゲーム" を認識します。[脅威カテゴリの拡張] の設定にチェック マークを入れて **[バックドア制御ソフトウェア (BDC)]** オプションを有効にすると、AntiVir プログラムが該当するソフトウェアを検出した場合に、対応するアラートが送信されます。

アドウェア/スパイウェア (ADSPY)

広告を表示したり、ユーザーが気付かないうちに同意なしでユーザーの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。

AntiVir プログラムは、"アドウェア/スパイウェア" を認識します。[脅威カテゴリの拡張] の設定にチェック マークを入れて **[アドウェア/スパイウェア (ADSPY)]** オプションを有効にすると、AntiVir プログラムがアドウェアまたはスパイウェアを検出した場合に、対応するアラートが送信されます。

通常とは異なるランタイム圧縮 (PCK)

通常とは異なるランタイム圧縮ツールで圧縮され、不審と分類される可能性のあるファイルです。

AntiVir プログラムは "通常とは異なるランタイム圧縮" を認識します。[脅威カテゴリの拡張] の設定にチェック マークを入れて **[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と、AntiVir プログラムが該当する圧縮を検出した場合に、対応するアラートが送信されます。

二重の拡張子ファイル (HEUR-DBLEXT)

実際のファイル拡張子を不審な方法で非表示に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。

AntiVir プログラムは "二重の拡張子ファイル" を認識します。[脅威カテゴリの拡張] の設定でチェック マークを入れて **[二重の拡張子ファイル]** (HEUR-DBLEXT) オプションを有効にすると、AntiVir プログラムが該当するファイルを検出した場合に、対応するアラートが送信されます。

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、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や潜在顧客のデータを巧妙な手段で盗み出すものです。
インターネットで電子メール アドレスを送信、オンライン フォームに入力、ニュースグループや Web サイトにアクセスすると、データがインターネットをクロールするスパイダによって盗まれ、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。

AntiVir プログラムは "フィッシング" を認識します。[脅威カテゴリの拡張] の設定にチェック マークを入れて **[フィッシング]** オプションを有効にすると、AntiVir プログラムが該当する動作を検出した場合に、対応するアラートが送信されます。

アプリケーション (APPL)

APPL という用語は、提供元に不審な点があるプログラム、または、使用すると有害な影響が生じる可能性のあるプログラムを指します。

AntiVir プログラムは "アプリケーション (APPL)" を認識します。[脅威カテゴリの拡張] の設定にチェック マークを入れて **[アプリケーション (APPL)]** オプションを有効にすると、AntiVir プログラムが該当する動作を検出した場合に、対応するアラートが送信されます。

10.2 ウイ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 ウィンドウを表示させるソフトウェアです。このような広告は、通常は削除できず、常に表示されたままになります。接続データから、ユーザーの行動に関する多数の情報が得られることになり、データ セキュリティの点で問題があります。

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 メカニズムをバイパスし、コンピュータへのアクセスを取得します。

バックグラウンドで実行されるプログラムは、通常、攻撃者に無制限の権限を与えることになります。バックドアによって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が、バックドアは主として関連システムに、コンピュータ ウイルスやワームをさらにインストールするために使用されます。

ブート ウイルス

ハードディスクのブート セクタ、またはマスタ ブート セクタは、主としてブート セクタ ウイルスに感染します。これらのウイルスは、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など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、サービス拒否攻撃など、通常は感染した PC のユーザーの気付かないところでさまざまな目的に使用されます。ボットネットの主な潜在リスクは、ネットワークを通して数千台ものコンピュータを一括して操作できるため、それらのコンピュータがアクセスする際に発生するデータ転送量の合計が爆発的に増大するということです。

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 システムのバグ、誤作動、脆弱性、特権の昇格、サービス拒否などを利用したコンピュータ プログラム、またはスクリプトです。たとえば、悪用の 1 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考えられます。より高レベルのアクセス権を取得するために、エクスプロイトを利用してシステムにプログラムが侵入する場合もあります。

デマウイルス

ここ数年間、インターネット ユーザーおよび他のネットワーク ユーザーは、電子メールを通じて広がると噂されるウイルスに関するアラートを受け取っています。このアラートは、電子メールを通じて広がり、できる限り多くの同僚や他のユーザーに送信して、全員が "危険" に備えるように警告する内容でした。

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るサービス (プログラムまたはサーバー) です。ネットワークやログ攻撃を監視する機能があります。このサービスは、正当なユーザーには未知であるため、ユーザーが対応することはできません。攻撃者がネットワークの弱点を調べ、ハニーポットが提供するサービスを使用した場合、その行為は記録され、アラートが起動されます。

マクロ ウイルス

マクロ ウイルスとは、WinWord 6.0 の WordBasic など、アプリケーションのマクロ言語で記述された小さなプログラムで、通常、そのアプリケーションの文書内でのみ広がります。このため、文書ウイルスとも呼ばれます。マクロ ウイルスがアクティブになるには、対応するアプリケーションがアクティブ化されていて、感染したマクロのいずれかが実行される必要があります。"通常の" ウイルスとは異なり、マクロ ウイ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、照会先を偽装ウェブサイトにそらす操作です。従来のフィッシングがさらに発展したものです。ファーミング詐欺師は、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、さまざまな DNS 攻撃の包括的な用語として確立しています。ホスト ファイルの操作の場合、システムの具体的な操作は、トロイの木馬やウイルスを使用して実行されます。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。フィッシング詐欺師は、通常、電子メールなどで一見正式に思われるレターをユーザーに送信し、送信元を信用させて、ユーザー名とパスワード、オンライン バンキング口座の PIN や TAN などの機密情報を提供させるようにしむけます。フィッシング詐欺師は、盗んだアクセスの詳細情報を使用してユーザーを装い、その名前で取引を実行します。銀行や保険会社が、クレジット カード番号、PIN、TAN、その他アクセスの詳細を電子メール、SMS、または電話で問い合わせることはあり得ません。

ポリモフィック ウイルス

ポリモフィック ウイルスは、偽装の真の達人です。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 ウイルス

コンピュータ ウイルスとは、実行されたり、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。ウイルスは、論理爆弾やトロイの木馬とは異なり、自ら増殖します。ワームとは異なり、ウイルスには伝染力のあるコードを植え付けるホストとしてのプログラムが常に必要です。通常、ホスト自体のプログラムの実行は変更されません。

ルートキット

ルートキットとは、侵入者がコンピュータ システムに侵入した後でインストールされるソフトウェア ツールの集合であり、侵入者のログイン、プロセス、データ記録を隠し、わからないようにします。侵入者は、既にインストールされたスパイ プログラムを更新し、削除されたスパイウェアを再インストールしようと試みます。

スクリプト ウイルスとワーム

このようなウイルスはプログラムの作成も蔓延も極めて簡単で、必要な技術があれば世界全体に数時間で広がります。

スクリプト ウイルスとワームには、Javascript、VBScript などのスクリプト言語のいずれかが使用されていて、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ります。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。

ワームとは、それ自体が増殖するプログラムですが、ホストに感染することはありません。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。セキュリティ対策が限られたシステムで、唯一、あらゆる種類のプログラムに侵入して損傷を与える可能性を持つのがワームです。

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、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ます。スパイウェアは、感染したコンピュータを利用して商業的な利益を得るために設計されています。

トロイの木馬

トロイの木馬は、現在では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ないところが、ウイルスやワームとは異なります。ユーザーがトロイの木馬を開始するようにしむけるため、大多数には興味をそそるような名前 (SEX.EXE、STARTME.EXE など) が付いています。実行すると、直ちにアクティブになり、ハード ディスクをフォーマットする場合もあります。埋め込み型とは、ウイルスを "埋め込む" トロイの木馬の特殊な形態で、コンピュータ システムにウイルスを埋め込みます。

ゾンビ

ゾンビ PC とは、マルウェア プログラムに感染して、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。コマンドを受けると、感染した PC はスパムやフィッシング電子メールの送信などのサービス拒否 (DoS) 攻撃を開始します。

11 情報とサービス

この章には、弊社への連絡方法に関する情報が含まれています。

「連絡先住所」の章を参照。

「テクニカル サポート」の章を参照。

「疑わしいファイル」の章を参照。

「誤検出レポート」の章を参照。

「フィードバックの送付」の章を参照。

11.1 連絡先情報

AntiVir 製品ラインに関するご質問やご要望をぜひお送りください。弊社の連絡先情報については、コントロール センターのヘルプ::Avira AntiVir Professional バージョン情報を参照してください。

11.2 テクニカル サポート

Avira のサポートでは、質問への回答と技術的な問題の解決に信頼性のある支援が提供されます。

弊社の包括的なサポート サービスに関して、必要なあらゆる情報は、弊社 Web サイトから入手可能です。

http://www.avira.jp/support

弊社から迅速に信頼性のある支援を提供できるよう、次の情報を準備していただく必要があります。

- **ライセンス情報**。この情報は、ヘルプ::Avira AntiVir Professional バージョン情報::ライセンス情報の下のプログラム インターフェイスで確認できます。
- **バージョン情報**。この情報は、ヘルプ::Avira AntiVir Professional バージョン情報::バージョン情報の下のプログラム インターフェイスで確認できます。
- **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** (例: 他のベンダのアンチウイルス 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**。

11.3 疑わしいファイル

弊社製品によってまだ検出、あるいは削除されていないウイルスや疑わしいファイルを弊社宛に送信することができます。これにはいくつかの方法があります。

- コントロール センターの [隔離] でファイルを確認し、コンテキスト メニューまたは対応するボタンを使用して、項目 [ファイルの送信] を選択します。
- ファイルは圧縮して (WinZIP、PKZip、Arj など) 電子メールの添付ファイルとして以下のアドレスにお送りください。
  virus@avira.jp
  電子メール ゲートウェイの一部はアンチウイルス ソフトウェアと連携しているため、パスワードとファイルを提供していただく必要もあります (必ずパスワードを提供してください)。

疑わしいファイルは、弊社 Web サイト からお送りいただくことも可能です。http://www.avira.jp/support/upload

11.4 誤検出レポート

クリーンである可能性が最も高いファイルで AntiVir プログラムにより検出がレポートされていると考えられる場合は、関連するファイルを圧縮し (WinZIP、PKZip、Arj など)、電子メールの添付ファイルとして以下のアドレスに送信してください。

- virus@avira.jp

電子メール ゲートウェイの一部はアンチウイルス ソフトウェアと連携しているため、パスワードとファイルを提供していただく必要もあります (必ずパスワードを提供してください)。

11.5 フィードバックの送付

Avira では、お客様のセキュリティが最重要課題です。このために弊社が抱えているのは、製品リリース前に、すべての Avira GmbH ソリューションの品質とセキュリティをテストする社内のエキスパート チームだけではありません。弊社では、改善が可能なセキュリティに関連するギャップに関するご指摘を大変重視しており、真摯に対処いたします。

弊社製品にセキュリティ ギャップが検出された場合は、以下のアドレス宛に電子メールをお送りください。

vulnerabilities@avira.jp

12 参照: 設定オプション

設定の参考資料には、使用可能なすべての設定オプションが文書化されています。

12.1 スキャナ

オンデマンド スキャンの設定には、設定の [スキャナ] セクションを使用します。

12.1.1 スキャン

ここで、オンデマンド スキャンに関するスキャン ルーチンの基本動作を定義します。オンデマンド スキャンで特定のディレクトリを選択してスキャンする場合、設定に従って、スキャナは次のようにスキャンを実行します。

- 特定のスキャン機能を使用する (優先)
- ブート セクタとメイン メモリも対象にする
- 特定のセクタまたはすべてのブート セクタとメイン メモリ
- ディレクトリ内のすべてのファイルまたは選択したファイル

ファイル

スキャナでは、フィルタを使用して、特定の拡張子を持つ (特定のタイプの) ファイルのみがスキャンされるように設定できます。

すべてのファイル

このオプションを有効にすると、内容やファイル拡張子にかかわらず、すべてのファイルに対してウイルスまたは不要プログラムのスキャンが実行されます。フィルタは使用されません。

注意
[すべてのファイル] を有効にすると、**[ファイル拡張子]** ボタンは選択できなくなります。

スマートなファイル タイプ判別

このオプションを有効にすると、ウイルスまたは不要プログラムのスキャンを実行するファイルの選択が、プログラムによって自動的に行われます。これは、AntiVir プログラムが内容に基づいてファイルをスキャンするかどうかを判断することを意味します。この方法は、[ファイル拡張子リストを使用] より若干遅くなりますが、ファイル拡張子のみに基づくスキャンではないため、より確実です。このオプションは初期状態で有効に設定されています (推奨の設定)。

注意
[スマートなファイル タイプ判別] を有効にすると、**[ファイル拡張子]** ボタンは選択できなくなります。

ファイル拡張子リストを使用

このオプションを有効にすると、指定した拡張子のファイルのみがスキャンされます。ウイルスや不要プログラムを含む可能性のあるすべてのファイル タイプが事前に設定されます。リストは "**[ファイル拡張子]**" ボタンを使用して手動で編集できます。

注意
このオプションを有効にして、ファイル拡張子でリストからすべてのエントリを削除すると、**[ファイル拡張子]** ボタンの下に、"ファイル拡張子がありません" と表示されます。

ファイル拡張子

このボタンをクリックするとダイアログ ボックスが開き、"**ファイル拡張子を使用**"モードでスキャンしたすべてのファイル拡張子が表示されます。拡張子に対して、既定のエントリが設定されていますが、エントリは追加または削除できます。

注意
既定のリストは、バージョンにより異なる場合がありますので注意してください。

その他の設定

選択したドライブのブート セクタをスキャン

このオプションを有効にすると、スキャナはオンデマンド スキャンで選択したドライブのブート セクタをスキャンします。このオプションは初期状態で有効に設定されています。

マスタ ブート セクタをスキャン

このオプションを有効にすると、スキャナはシステムで使用されているハード ディスクのマスタ ブート セクタをスキャンします。

オフライン ファイルを無視

このオプションを有効にすると、ダイレクト スキャンではスキャン中にオフライン ファイルが完全に無視されます。これは、これらのファイルに対してウイルスと不要プログラムのスキャンが実行されないことを意味します。オフライン ファイルとは、たとえば、階層ストレージ管理システム (HSMS) によって、ハード ディスクからテープなどに物理的に移動されたファイルです。このオプションは初期状態で有効に設定されています。

システム ファイルの完全性チェック

このオプションを有効にすると、オンデマンド スキャンの際、システム ファイルがマルウェアによって改変されていないかが厳重にチェックされます。Windows の重要なシステム ファイルのほとんどが、このチェックの対象になります。改変されたファイルが検出された場合、疑わしいファイルとして報告されます。この機能は、コンピュータのリソースを大量に消費します。そのため、初期設定では、このオプションが無効に設定されています。

重要
このオプションは Windows Vista 以上でのみ使用できます。SMC の下で AntiVir プログラムを管理している場合、このオプションは使用できません。

注意
システム ファイルを変更して独自の要件に起動または開始画面を合わせるサードパーティ製のツールを使用している場合、このオプションを使用しないでください。そのようなツールの例は、スキンパック、TuneUp ユーティリティ、または Vista Customization です。

最適化されたスキャン

このオプションを有効にすると、スキャナによるスキャン中、プロセッサのリソース利用が最適化されます。パフォーマンス上の理由から、最適化されたスキャンは標準レベルでのみ記録されます。

注意
このオプションは、マルチ プロセッサ システムでのみ利用できます。AntiVir プログラムを SMC で管理している場合、このオプションが常に表示され、有効にすることができます。管理対象のシステムに、複数のプロセッサが搭載されていない場合、スキャナ オプションは使用されません。

シンボリック リンクのリンク先をスキャンする

このオプションを有効にすると、スキャナはスキャン プロファイル、または選択したディレクトリのすべてのシンボリック リンクに従って、リンク先のファイルに対してウイルスとマルウェアのスキャンを実行します。Windows 2000 では、このオプションはサポートされていないため無効になります。

重要
このオプションにショートカットは含まれていませんが、ファイル システムで透過的な、シンボリック リンク (mklink.exe によって生成) または接合ポイント (junction.exe によって生成) のみが参照されます。

スキャン前にルートキットを検索

このオプションを有効にしてスキャンを開始すると、スキャナは、Windows システム ディレクトリでショートカット内のアクティブなルートキットをスキャンします。このプロセスでは、"**[ルートキットをスキャン]**" スキャン プロファイルほど包括的にアクティブなルートキットのスキャンは行われませんが、非常にすばやく実行できます。

重要
このルートキットは、Windows XP 64 ビットでは使用できません。

レジストリをスキャン

このオプションを有効にすると、レジストリに対してマルウェアへの参照のスキャンが実行されます。

ネットワーク ドライブ上のファイルまたはパスをスキャンしない

このオプションを有効にすると、コンピュータに接続されたネットワーク 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、サーバーまたは他のワークステーション自体がアンチウイルス ソフトウェアで保護されている場合にお勧めします。このオプションは初期状態で無効に設定されています。

スキャン プロセス

スキャナの停止を許可

このオプションを有効にすると、"Luke Filewalker" のウィンドウで、**[停止]** ボタンを押して、ウイルスや不要プログラムのスキャンをいつでも終了できます。この設定を無効にすると、[Luke Filewalker] ウィンドウの **[停止]** ボタンの背景が灰色になります。このため、スキャン プロセスを途中で終了させることはできません。このオプションは初期状態で有効に設定されています。

スキャナの優先度

オンデマンド スキャンで、スキャナは優先度のレベルを区別します。これは、複数のプロセスがワークステーションで同時に実行されている場合に効果的です。この選択はスキャン速度に影響を与えます。

低

スキャナにはオペレーティング システムによってのみプロセッサ時間が割り当てられるため、他のプロセスで計算時間が必要でなければ、スキャナが実行されている限り、速度は最大になります。全体として、他のプログラムとの連携が最適化されます。他のプログラムが計算時間を必要とする場合も、コンピュータはよりすばやく応答し、スキャナはバックグラウンドで動作し続けます。このオプションは初期状態で有効に設定されています (推奨の設定)。

中

スキャナは、通常の優先度で実行されます。オペレーティング システムによって、すべてのプロセスに同じ量のプロセッサ時間が割り当てられます。特定の状況下では、他のアプリケーションとの連携に影響を与える可能性があります。

高

スキャナの優先度が最も高くなります。他のアプリケーションとの同時連携は、ほぼ不可能です。スキャナはスキャンを最高速度で完了します。

12.1.1.1. 検出時のアクション

検出時のアクション

ウイルスまたは不要プログラムが検出された場合に、スキャナが実行するアクションを定義できます。

対話型

このオプションを有効にすると、スキャナ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。スキャナによるスキャンの実行時、スキャンが完了したときに、感染したファイルのリストと共にアラートが表示されます。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。すべ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するか、またはスキャナをキャンセルすることができます。

注意
スキャナのダイアログでは、'[隔離] に移動' アクションは既定のアクションとして表示されます。

許可されたアクション

このボックスでは、ウイルス検出時に個別通知モードまたはエキスパート通知モードで選択できるアクションを指定できます。これに対応するオプションを有効にする必要があります。

修復

スキャナは、可能な場合、感染したファイルを修復します。

名前の変更

スキャナは、ファイルの名前を変更します。これらのファイルへの直接のアクセス (ダブルクリックなど) はできなくなります。ファイルは後で修復して、再び名前を変更できます。

隔離

スキャナはファイルを [隔離] に移動します。情報として価値がある場合、ファイルは、隔離から復元できます。また、必要に応じて Avira マルウェア研究センターに送信できます。ファイルによっては、隔離で別の選択オプションも使用できます。

削除

ファイルは削除されます。このプロセスは、[上書きおよび削除] よりはるかに高速に実行されます。

無視

無視するファイル。

上書きおよび削除

スキャナは、既定のパターンに一致するファイルを上書きしてから削除します。この場合、ファイルは復元できません。

既定

このボタンは、検出されたファイルを処理するときのスキャナの既定のアクションを定義するために使用します。アクションをハイライト表示し、**[既定値]** ボタンをクリックします。複合通知モードでは、該当するファイルに対して選択した既定のアクションのみが実行されます。個別通知モードおよびエキスパート通知モードでは、該当ファイルに対して選択された既定のアクションがあらかじめ選択状態になります。

注意
修復アクションを既定のアクションとして選択することはできません。

注意
[削除] または *[上書きおよび削除]* を既定のアクションとして選択したうえで、通知モードを複合通知モードに設定する場合は、次の点に注意してください。ヒューリスティック スキャン機能による検出の場合、感染したファイルは削除されず、[隔離] に移動されます。

詳細については、こちらをクリックしてください。

自動

このオプションが有効である場合、ウイルス検出時にダイアログ ボックスは表示されません。スキャナは、プライマリ アクションおよびセカンダリ アクションとしてこのセクションで事前に定義された設定に従って動作します。

隔離にバックアップ

このオプションを有効にすると、スキャナは、要求されたプライマリ アクション、またはセカンダリ アクションの実行前に、バックアップ コピーを作成します。情報として価値がある場合に、ファイルの復元が可能な、[隔離] にバックアップ コピーが保存されます。さらに調査するため、バックアップ コピーを Avira マルウェア研究センターに送信することもできます。

検出アラートを表示

このオプションをアクティブ化すると、ウイルスまたは不要なプログラムを検出するたびに、実行されるアクションを示すアラートが表示されます。

プライマリ アクション

プライマリ アクションとは、スキャナがウイルスまたは不要なプログラムを検出した場合に実行されるアクションです。**[修復]** オプションが選択されていて、感染したファイルの修復が不可能な場合、**[セカンダリ アクション]** で選択したアクションが実行されます。

注意

[セカンダリ アクション] は、**[修復]** オプションが **[プライマリ アクション]** の下で選択されている場合にのみ選択できます。

修復

このオプションを有効にすると、スキャナは感染したファイルを自動的に修復します。スキャナが感染したファイルを修復できない場合、[セカンダリ アクション] の下で選択したアクションが実行されます。

注意

自動修復をお勧めしますが、これはスキャナがワークステーション上でファイルを変更することを意味します。

削除

このオプションを有効にすると、ファイルは削除されます。このプロセスは、[上書きおよび削除] よりはるかに高速に実行されます。

上書きおよび削除

このオプションを有効にすると、スキャナは、既定のパターンに一致するファイルを上書きしてから削除します。この場合、ファイルは復元できません。

名前の変更

このオプションを有効にすると、スキャナはファイルの名前を変更します。これらのファイルへの直接のアクセス (ダブルクリックなど) はできなくなります。ファイルは後で修復して、再び元の名前に変更できます。

無視

このオプションを有効にすると、ファイルへのアクセスは許可され、ファイルはそのまま残されます。

警告

感染したファイルは、ワークステーションで実行可能な状態のままになります。これはワークステーションに深刻な悪影響を及ぼす可能性があります。

隔離

このオプションを有効にすると、スキャナはファイルを [隔離] に移動します。それらのファイルは後で修復したり、必要に応じて Avira マルウェア研究センターに送信できます。

セカンダリ アクション

[セカンダリ アクション] は、**[修復]** オプションが **[プライマリ アクション]** の下で選択されている場合にのみ選択できます。このオプションを使用すると、感染したファイルを修復できない場合の処理を決定できます。

削除

このオプションを有効にすると、ファイルは削除されます。このプロセスは、[上書きおよび削除] よりはるかに高速に実行されます。

上書きおよび削除

このオプションを有効にすると、スキャナは、既定のパターンに一致するファイルを上書きしてから削除 (ワイプ) します。この場合、ファイルは復元できません。

名前の変更

このオプションを有効にすると、スキャナはファイルの名前を変更します。これらのファイルへの直接のアクセス (ダブルクリックなど) はできなくなります。ファイルは後で修復して、再び元の名前に変更できます。

無視

このオプションを有効にすると、ファイルへのアクセスは許可され、ファイルはそのまま残されます。

警告
感染したファイルは、ワークステーションで実行可能な状態のままになります。これはワークステーションに深刻な悪影響を及ぼす可能性があります。

隔離

このオプションを有効にすると、スキャナはファイルを [隔離] に移動します。それらのファイルは後で修復したり、必要に応じて Avira マルウェア研究センターに送信できます。

注意
[削除] または **[上書きおよび削除]** をプライマリ アクションまたはセカンダリ アクションとして選択した場合は、次の点に注意する必要があります。ヒューリスティック スキャン機能による検出の場合、感染したファイルは削除されず、[隔離] に移動されます。

12.1.1.2. その他のアクション

検出の後にプログラムを起動

オンデマンド スキャンの後、1 つ以上のウイルスまたは不要プログラムが検出された場合、他のユーザーや管理者に連絡できるように、スキャナは選択したファイルやプログラム (たとえば電子メール プログラム) を開くことができます。

注意
セキュリティ上の理由から、ユーザーがコンピュータにログオンしているときで、検出された後でなければプログラムは起動できません。ファイルは、ログオンしているユーザーに適用される権限で開かれます。ログオンしているユーザーがいない場合、このオプションは実行されません。

プログラム名

この入力ボックスで、検出後にスキャナによる起動が必要なプログラムの名前と関連するパスを入力できます。

このボタンでウィンドウが開き、ファイル選択ダイアログを使用して、目的のプログラムを選択できます。

引数

必要に応じて、この入力ボックスに起動するプログラムのコマンド ライン パラメータを入力できます。

イベント ログ

イベント ログの使用

このオプションを有効にすると、スキャナによるスキャンの完了後、イベント レポートとスキャン結果が Windows イベント ログに転送されます。このイベントは、Windows イベント ビューアで表示できます。このオプションは既定で無効に設定されています。

アーカイブをスキャンする場合、スキャナは再帰スキャンを使用します。アーカイブ内のアーカイブも解凍され、ウイルスと不要プログラムのスキャンが実行されます。ファイルはスキャンされ、解凍されて再度スキャンされます。

アーカイブをスキャン

このオプションを有効にすると、アーカイブ リストで選択したアーカイブがスキャンされます。このオプションは初期状態で有効に設定されています。

すべてのアーカイブ タイプ

このオプションを有効にすると、アーカイブ リストのすべてのアーカイブ タイプが選択されスキャンされます。

スマートなファイル タイプ判別

このオプションを有効にすると、スキャナはファイルが圧縮ファイル形式 (アーカイブ) であるかを検出し、ファイル拡張子が通常の拡張子と異なっていても、アーカイブをスキャンします。ただし、すべてのファイルを開く必要があるため、スキャン速度が遅くなります。例: *.zip アーカイブに *.xyz というファイル拡張子が付いていても、スキャナはこのアーカイブを解凍してスキャンします。このオプションは初期状態で有効に設定されています。

注意
サポートされるアーカイブ タイプのみが、アーカイブ リストでマークされます。

再帰の深さ

再帰レベルの深いアーカイブの解凍とスキャンには、コンピュータの CPU 時間とリソースが非常に多く必要になる場合があります。このオプションを有効にすると、複数の圧縮が行われたアーカイブのスキャンの再帰レベルを特定の圧縮レベルに制限します (最大の再帰レベル)。これにより、コンピュータの使用時間とリソースを節約できます。

注意
アーカイブ内のウイルスまたは不要プログラムを検出するには、ウイルスまたは不要プログラムが含まれている再帰レベルまでスキャナがスキャンする必要があります。

最大の再帰レベル

最大の再帰レベルを入力するには、[再帰レベルを制限] を有効にする必要があります。
必要な再帰レベルは直接入力するか、エントリ フィールドの右矢印キーで指定できます。許容される値は 1 ～ 99 です。標準値の 20 をお勧めします。

既定値

このボタンは、スキャン アーカイブに対する事前に設定済みの値を復元します。

アーカイブ

この表示領域で、スキャナがスキャンする必要のあるアーカイブを設定できます。このためには、関連するエントリを選択する必要があります。

12.1.1.3. 例外

スキャナのスキャン対象から除外するファイル オブジェクト

このウィンドウのリストには、スキャナによるウイルスまたは不要プログラムのスキャン対象から除外するファイルとパスが含まれます。

ここに入力する例外は、何らかの理由で通常のスキャンの対象から除外するファイルのみとし、できる限り少なくしてください。このリストにファイルを含める前に、それらのファイルに対して必ずウイルスまたは不要プログラムのスキャンを実行することをお勧めします。

注意
リストのエントリに、合計 6000 文字を超える文字を含めることはできません。

警告
これらのファイルはスキャンに含まれません。

注意
このリストに含まれるファイルは、レポート ファイルに書き込まれます。ファイルを除外すべき理由が既になくなっている場合もあるため、スキャンされていないファイルはレポート ファイルでときどき確認してください。この場合、そのファイルの名前をこのリストから再び削除する必要があります。

入力ボックス

この入力ボックスに、オンデマンド スキャンに含めないファイル オブジェクトの名前を入力できます。既定で入力されているファイル オブジェクトはありません。

このボタンをクリックするとウィンドウが開き、必要なファイルまたはパスを選択できます。
完全なパスとファイル名を入力すると、そのファイルだけが感染のスキャンの対象から除外されます。パスなしでファイル名を入力すると、パスまたはドライブにかかわらずその名前を持つすべてのファイルがスキャンされなくなります。

追加

このボタンを使用すると、入力ボックスに入力したファイル オブジェクトを表示ウィンドウに追加できます。

削除

このボタンは、選択したエントリをリストから削除します。エントリが選択されていないと、このボタンは非アクティブになります。

注意
ファイル オブジェクトのリストにパーティションを追加すると、そのパーティション直下に保存されたファイルのみがスキャン対象から除外されます。そのパーティション上のサブディレクトリ内のファイルは除外されません。
例: スキャン対象から除外するファイル オブジェクト: `D:\` = `D:\file.txt` は、スキャナのスキャン対象から除外されますが、`D:\folder\file.txt` はスキャン対象から除外されません。

注意
SMC で AntiVir プログラムを管理している場合、ファイルの除外のためにパスの詳細で変数を使用できます。変数::Guard および Scanner の除外で、使用可能な変数のリストを参照できます。

12.1.1.4. ヒューリスティック

この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 スキャン機能に対する設定が含まれます。

AntiVir 製品は非常に強力なヒューリスティック スキャン機能を備えており、有害な要素に対応する専用のウイルス シグネチャが作成される前や、アンチウイルス ソフトウェアの更新プログラムが送信される前などに、未知のマルウェアを予防的に検出することができます。ウイルスの検出では、マルウェアの典型的な機能に関して、感染したコードの広範な分析と検査が行われます。スキャンされたコードにこれらに独特の特徴が見られる場合、疑わしいファイルとして報告されます。これは必ずしもそのコードが、実際にマルウェアであるという意味ではありません。誤検出が生じる場合もあります。感染したと疑われるコードの処理に関する決定は、コードのソースが信頼できるかどうかに関する知識などに基づいて、ユーザーが判断する必要があります。

マクロウイルス ヒューリスティック

マクロウイルス ヒューリスティック

AntiVir 製品には、非常に強力なマクロウイルス ヒューリスティック スキャン機能が含まれています。このオプションを有効にすると、修復の場合に関連ドキュメントのすべてのマクロが削除されるか、あるいはアラートの送信などで不審な文書に関するレポートのみが行われます。このオプションは初期状態で有効に設定されています (推奨の設定)。

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

AntiVir プログラムには、AntiVir AheAD テクノロジという非常に強力なヒューリスティック スキャン機能が含まれていて、未知の (新しい) マルウェアも検出できます。このオプションを有効にすると、このヒューリスティック スキャン機能をどの程度 "アグレッシブ" にするかを定義できます。このオプションは初期状態で有効に設定されています。

低検出レベル

このオプションを有効にすると、検出される未知のマルウェアがやや減りますが、誤ったアラートのリスクは低くなります。

中検出レベル

このヒューリスティック スキャン機能の使用を選択すると、このオプションが初期状態で有効になります。

高検出レベル

このオプションを有効にすると、未知のマルウェアをかなり多く検出するようになりますが、より高い確率で誤検出が起こる点にも注意が必要です。

12.1.2 レポート

スキャナには、包括的なレポート機能があります。このため、オンデマンド スキャンの結果に関する正確な情報を取得できます。レポート ファイルには、システムのすべてのエントリとオンデマンド スキャンのアラートおよびメッセージが書き込まれます。

注意
ウイルスまたは不要プログラムが検出されたときにスキャナが実行するアクションを設定できるように、常にレポート ファイルが作成されるようにする必要があります。

レポート

オフ

このオプションを有効にすると、スキャナはオンデマンド スキャンのアクションと結果を報告しません。

既定

このオプションを有効にすると、スキャナは疑わしいファイルの名前とパスを記録します。現在のスキャンの設定、バージョン情報、およびライセンスに関する情報も、レポート ファイルに書き込まれます。

詳細

このオプションを有効にすると、スキャナは既定の情報に加えて、アラートとヒントを記録します。

完了

このオプションを有効にすると、スキャナはすべてのスキャンされたファイルを記録します。関与するすべてのファイル、アラート、およびヒントもレポート ファイルに書き込まれます。

注意
任意でレポート ファイルの送信が必要になった場合は (トラブルシューティング用)、このモードでこのレポート ファイルを作成してください。

12.2 Guard

オンアクセス スキャンの設定には、設定の [Guard] セクションを使用します。

12.2.1 スキャン

通常、管理者もユーザーもシステムを常時監視したいと考えます。このためには、Guard (= オンアクセス スキャナ) を使用します。この方法で、コンピュータ上にコピーされた、または開かれたすべてのファイルを "オンザフライ" でスキャンしてウイルスまたは不要プログラムを検索します。

スキャン モード

ここで、ファイルをいつスキャンするかを定義します。

読み取り時にスキャン

このオプションを有効にすると、Guard はファイルがアプリケーションやオペレーション システムで読み込まれたり実行される前にスキャンします。

書き込み時にスキャン

このオプションを有効にすると、Guard は書き込み時にファイルをスキャンします。このプロセスが完了するまで、ファイルに再びアクセスすることはできません。

読み取り時と書き込み時にスキャン

このオプションを有効にすると、Guard はファイルを開く前、読み取る前、実行する前、および書き込み後にスキャンします。このオプションは初期状態で有効に設定されています (推奨の設定)。

ファイル

Guard では、フィルタを使用して、特定の拡張子を持つ (特定のタイプの) ファイルのみがスキャンされるように設定できます。

すべてのファイル

このオプションを有効にすると、内容やファイル拡張子にかかわらず、すべてのファイルに対してウイルスまたは不要プログラムのスキャンが実行されます。

注意
[すべてのファイル] を有効にすると、**[ファイル拡張子]** ボタンは選択できなくなります。

スマートなファイル タイプ判別

このオプションを有効にすると、ウイルスまたは不要プログラムのスキャンを実行するファイルの選択が、プログラムによって自動的に行われます。これは、プログラムが内容に基づいてファイルをスキャンするかどうかを判断することを意味します。この方法は、[ファイル拡張子リストを使用] より若干遅くなりますが、ファイル拡張子のみに基づくスキャンではないため、より確実です。

注意
[スマートなファイル タイプ判別] を有効にすると、**[ファイル拡張子]** ボタンは選択できなくなります。

ファイル拡張子リストを使用

このオプションを有効にすると、指定した拡張子のファイルのみがスキャンされます。ウイルスや不要プログラムを含む可能性のあるすべてのファイル タイプが事前に設定されます。リストは **[ファイル拡張子]** ボタンを使用して手動で編集できます。このオプションは初期状態で有効に設定されています (推奨の設定)。

注意
このオプションを有効にして、ファイル拡張子でリストからすべてのエントリを削除すると、**[ファイル拡張子]** ボタンの下に、"ファイル拡張子がありません" と表示されます。

ファイル拡張子

このボタンをクリックするとダイアログ ボックスが開き、**"ファイル拡張子を使用"**モードでスキャンしたすべてのファイル拡張子が表示されます。拡張子に対して、既定のエントリが設定されていますが、エントリは追加または削除できます。

注意
ファイル拡張子リストは、バージョンにより異なる場合がありますので注意してください。

アーカイブ

アーカイブをスキャン

このオプションを有効にすると、アーカイブがスキャンされます。圧縮ファイルがスキャンされ、解凍されて再度スキャンされます。このオプションは既定で無効に設定されています。アーカイブのスキャンは、再帰レベル、スキャン対象ファイル数、およびアーカイブのサイズによって制限されます。再帰レベルの最大値、スキャン対象ファイル数、およびアーカイブの最大サイズはユーザーが設定できます。

注意
このプロセスはコンピュータのパフォーマンスへの要求度が高いため、このオプションは既定で無効に設定されています。通常、アーカイブにはオンデマンド スキャンでのチェックをお勧めします。

最大の再帰レベル

アーカイブをスキャンする場合、Guard は再帰スキャンを使用します。アーカイブ内のアーカイブも解凍され、ウイルスと不要プログラムのスキャンが実行されます。再帰レベルを定義できます。再帰レベルの既定値で推奨される値は 1 です。この場合、メイン アーカイブに直接配置されたすべてのアーカイブがスキャンされます。

最大ファイル数

アーカイブをスキャンする場合に、スキャンをアーカイブ内の最大ファイル数に制限できます。スキャン対象の最大ファイル数の既定値は 10 です。通常は、この値をお勧めします。

最大サイズ (KB)

アーカイブをスキャンする場合に、スキャンを解凍可能な最大アーカイブ サイズに制限できます。標準値の 1000 KB をお勧めします。

ドライブ

ネットワーク ドライブ

このオプションを有効にすると、サーバー ボリューム、ピア ドライブなどのネットワーク ドライブ (マップされたドライブ) 上のファイルがスキャンされます。

注意
コンピュータのパフォーマンスの大幅な低下を避けるには、**[ネットワーク ドライブ]** オプションは例外的な場合にのみ有効にする必要があります。

警告
このオプションを無効にすると、ネットワーク ドライブは監視**されません**。ウイルスまたは不要プログラムに対する保護がなくなります!

注意
ネットワーク ドライブ上で実行されるファイルは、*[ネットワーク ドライブ]* オプションの設定に関係なく Guard によってスキャンされます。場合によっては、*[ネットワーク ドライブ]* オプションが無効になっていても、ネットワーク ドライブ上のファイルを開くと、それらのファイルがスキャンされます。理由: これらのファイルにアクセスするには、'ファイルの実行' 権限が必要です。これらのファイル (またはネットワーク ドライブ上で実行されるファイル) を Guard のスキャン対象から除外するには、それらのファイルを除外ファイル オブジェクトのリストに入力します(Guard::スキャン::例外を参照)。

キャッシュを有効にする

このオプションを有効にすると、ネットワーク ドライブ上の監視対象のファイルは Guard のキャッシュで使用可能になります。キャッシュ機能を使用しないネットワーク ドライブの監視はより安全ですが、キャッシュ機能を使用するネットワーク ドライブの監視よりもパフォーマンスは低くなります。

12.2.1.1. 検出時のアクション

検出時のアクション

ウイルスまたは不要プログラムが検出された場合に、Guard が実行するアクションを定義できます。

対話型

このオプションを有効にすると、Guard によってウイルスまたは不要プログラムが検出されると、デスクトップ通知が表示されます。検出されたマルウェアを削除するか、[詳細] ボタンをクリックして他の可能なウイルス処理アクションにアクセスするかを選択できます。それらのアクションはダイアログ ボックスに表示されます。それらのアクションはダイアログ 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。

許可されたアクション

この表示ボックスで、ダイアログ ボックスにその他のアクションとして表示されるウイルス管理アクションを指定できます。これに対応するオプションを有効にする必要があります。

修復

Guard は、可能な場合、感染したファイルを修復します。

名前の変更

Guard は、ファイルの名前を変更します。これらのファイルへの直接のアクセス (ダブルクリックなど) はできなくなります。ファイルは後で修復して、再び名前を変更できます。

隔離

Guard はファイルを [隔離] に移動します。情報として価値がある場合、ファイルは、隔離から復元できます。また、必要に応じて Avira マルウェア研究センターに送信できます。ファイルによっては、隔離で別の選択オプションも使用できます。

削除

ファイルは削除されます。このプロセスは、[上書きおよび削除] よりはるかに高速に実行されます。

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

Guard は、既定のパターンに一致するファイルを上書きしてから削除します。この場合、ファイルは復元できません。

既定

このボタンを使用すると、ウイルスが検出された場合、ダイアログ ボックスで既定でアクティブにするアクションを選択できます。既定でアクティブにするアクションを選択して、"**[既定]**" ボタンをクリックします。

注意
修復アクションを既定のアクションとして選択することはできません。

詳細については、こちらをクリックしてください。

自動

このオプションが有効である場合、ウイルス検出時にダイアログ ボックスは表示されません。Guard は、プライマリ アクションおよびセカンダリ アクションとしてこのセクションで事前に定義された設定に従って動作します。

隔離にバックアップ

このオプションを有効にすると、Guard は、要求されたプライマリ アクション、またはセカンダリ アクションの実行前に、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、隔離に保存されます。情報として価値がある場合は、隔離から復元できます。さらに調査するため、バックアップ コピーを Avira マルウェア研究センターに送信することもできます。オブジェクトによっては、隔離で別の選択オプションも使用できます。

検出アラートを表示

このオプションを有効にすると、ウイルスまたは不要なプログラムを検出するたびに、アラートが表示されます。

プライマリ アクション

プライマリ アクションとは、Guard がウイルスまたは不要なプログラムを検出した場合に実行されるアクションです。**[修復]** オプションが選択されていて、感染したファイルの修復が不可能な場合、**[セカンダリ アクション]** で選択したアクションが実行されます。

注意
[セカンダリ アクション] オプションは、[修復] 設定が [プライマリ アクション] の下で選択されている場合にのみ選択できます。

修復

このオプションを有効にすると、Guard は感染したファイルを自動的に修復します。Guard が感染したファイルを修復できない場合、[セカンダリ アクション] の下で選択したアクションが実行されます。

注意
自動修復をお勧めしますが、これは Guard がワークステーション上でファイルを変更することを意味します。

削除

このオプションを有効にすると、ファイルは削除されます。このプロセスは、[上書きおよび削除] よりはるかに高速に実行されます。

上書きおよび削除

このオプションを有効にすると、Guard は、既定のパターンに一致するファイルを上書きしてから削除します。この場合、ファイルは復元できません。

名前の変更

このオプションを有効にすると、Guard はファイルの名前を変更します。これらのファイルへの直接のアクセス (ダブルクリックなど) はできなくなります。ファイルは後で修復して、再び元の名前に変更できます。

無視

このオプションを有効にすると、ファイルへのアクセスは許可され、ファイルはそのまま残されます。

警告
感染したファイルは、ワークステーションで実行可能な状態のままになります。これはワークステーションに深刻な悪影響を及ぼす可能性があります。

アクセスの拒否

このオプションを有効にすると、レポート機能をアクティブにしている場合、Guard はレポート ファイルに検出されたファイルを書き込みます。また、Guard はイベント ログにもエントリを追加します (該当するオプションを有効にしている場合)。

隔離

このオプションを有効にすると、Guard はファイルを [隔離] に移動します。このディレクトリのファイルは後で修復したり、必要に応じて Avira マルウェア研究センターに送信できます。

セカンダリ アクション

[セカンダリ アクション] オプションは、**[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にのみ選択できます。このオプションを使用すると、感染したファイルを修復できない場合の処理を決定できます。

削除

このオプションを有効にすると、ファイルは削除されます。このプロセスは、[上書きおよび削除] よりはるかに高速に実行されます。

上書きおよび削除

このオプションを有効にすると、Guard は、既定のパターンに一致するファイルを上書きしてから削除します。この場合、ファイルは復元できません。

名前の変更

このオプションを有効にすると、Guard はファイルの名前を変更します。これらのファイルへの直接のアクセス (ダブルクリックなど) はできなくなります。ファイルは後で修復して、再び元の名前に変更できます。

無視

このオプションを有効にすると、ファイルへのアクセスは許可され、ファイルはそのまま残されます。

警告
感染したファイルは、ワークステーションで実行可能な状態のままになります。これはワークステーションに深刻な悪影響を及ぼす可能性があります。

アクセスの拒否

このオプションを有効にすると、レポート機能をアクティブにしている場合、Guard はレポート ファイルに検出されたファイルを書き込みます。また、Guard はイベント ログにもエントリを追加します (該当するオプションを有効にしている場合)。

隔離

このオプションを有効にすると、Guard はファイルを [隔離] に移動します。それらのファイルは後で修復したり、必要に応じて Avira マルウェア研究センターに送信できます。

注意
[削除] または**[上書きおよび削除]** をプライマリ アクションまたはセカンダリ アクションとして選択した場合は、次の点に注意する必要があります。ヒューリスティック スキャン機能による検出の場合、感染したファイルは削除されず、[隔離] に移動されます。

12.2.1.2. その他のアクション

通知

イベント ログ

イベント ログの使用

このオプションを有効にすると、検出されるたびに、Windows イベント ログにエントリが追加されます。 このイベントは、Windows イベント ビューアで表示できます。このオプションは初期状態で有効に設定されています。

自動開始

自動開始機能をブロックする

このオプションを有効にすると、Windows の自動開始機能の実行は、USB スティック、CD および DVD ドライブ、ネットワーク ドライブなど、接続されているすべてのドライブに対してブロックされます。 Windows の自動開始機能を使用している場合、データ メディアまたはネットワーク ドライブ上のファイルは、セットまたは接続直後に読み取られ、ファイルは自動的に起動されたり、コピーされたりします。ただし、この機能には高いセキュリティ リスクがあります。自動開始機能によってマルウェアおよび不要プログラムがインストールされる可能性があるためです。自動開始機能は USB スティックに対して特にリスクが高くなります。スティック上のデータはいつでも変更可能であるためです。

CD と DVD を除外する

このオプションを有効にすると、自動開始機能は CD および DVD ドライブに対して許可されます。

警告
自動開始機能を無効にするのは、CD および DVD ドライブで信頼できるデータ メディアのみを使用することが確かな場合のみにしてください。

12.2.1.3. 例外

これらのオプションを使用すると、Guard に対する例外オブジェクトを設定できます (オンアクセス スキャン)。関連するオブジェクトが、オンライン スキャンに含まれなくなります。スキャン対象から除外するプロセスのリストによって、オンアクセス スキャン中、Guard はこれらのオブジェクトへのファイル アクセスを無視できます。これは、データベースやバックアップ ソリューションなどに便利です。
除外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に、以下のことに注意してください。このリストは、上から下に処理されます。リストが長くなると、各アクセスに対するリストの処理に必要なプロセッサ時間も長くなります。このため、リストはできる限り短くしてください。

Guard がスキャン対象から除外するプロセス

このリストのプロセスのすべてのファイル アクセスは、Guard の監視対象から除外されます。

入力ボックス

このフィールドに、リアルタイム スキャンによって無視されるプロセスの名前を入力します。既定で入力されているプロセスはありません。

注意
プロセスは最大 128 件まで入力できます。

注意
プロセスを入力する場合、Unicode 記号を使用できます。したがって、特殊な記号を含むプロセスまたはディレクトリ名を入力できます。

注意
フル パスの詳細を含めないで、Guard による監視からプロセスを除外できます。
application.exe
ただしこれは、実行可能ファイルがハード ディスク ドライブ上に位置するプロセスにのみ適用されます。
実行可能ファイルがネットワーク ドライブなどの接続ドライブにあるプロセスではフル パスの詳細が必要です。接続されているネットワーク ドライブに関する例外に関する一般的な情報に注意してください。
実行可能ファイルが動的ドライブ上にあるプロセスに対しては除外を指定しないでください。動的ドライブは、CD、DVD、USB スティックなどのリムーバブル ディスクで使用されます。

注意
ドライブ情報は、[ドライブ文字]:\ の形式で入力する必要があります。
コロン記号 (:) は、ドライブを指定するためにのみ使用します。

注意
プロセスを指定する場合、ワイルドカード * (任意の数の文字) および ?? (単一の文字) を使用できます。
C:\Program Files\Application\application.exe
C:\Program Files\Application\applicatio?.exe
C:\Program Files\Application\applic*.exe
C:\Program Files\Application*.exe
Guard による監視からプロセスがグローバルに除外されることを避けるために、文字 * (アスタリスク)、? (疑問符)、/ (スラッシュ)、\ (円記号)、. (ピリオド)、: (コロン) のみを含む指定は無効です。

注意
プロセスのパスおよびファイル名に指定できるのは最大 255 文字です。リストのエントリに、合計 6000 文字を超える文字を含めることはできません。

警告
リストに記録されたプロセスによってアクセスされたすべてのファイルは、ウイルスと不要プログラムのスキャンの対象から除外されますので注意してください。
Windows エクスプローラとオペレーティング システム自体を除外することはできません。リスト内のこれに該当するエントリは無視されます。

このボタンでウィンドウが開き、実行可能ファイルを選択できます。

プロセス

[プロセス] ボタンをクリックすると、*[プロセスの選択]* ウィンドウが開き、実行中のプロセスが表示されます。

追加

このボタンを使用すると、入力ボックスに入力したプロセスを表示ウィンドウに追加できます。

削除

このボタンを使用すると、選択したプロセスを表示ウィンドウから削除できます。

Guard がスキャン対象から除外するファイル オブジェクト

このリストのオブジェクトに対するすべてのファイル アクセスは、Guard の監視対象から除外されます。

入力ボックス

このボックスに、オンアクセス スキャンに含めないファイル オブジェクトの名前を入力できます。既定で入力されているファイル オブジェクトはありません。

注意
監視対象のファイル オブジェクトを指定する場合、ワイルドカード * (任意の数の文字) および ?? (単一の文字) を使用できます。個々のファイル拡張子 (ワイルドカードを含む) を除外することもできます。
C:\Directory*.mdb
*.mdb
*.md?
.xls
C:\Directory*.log

注意
ディレクトリ名の末尾には、円記号 \ を付ける必要があります。それ以外の場合は、ファイル名と見なされます。

注意
リストのエントリに、合計 6000 文字を超える文字を含めることはできません。

注意
ディレクトリを除外すると、そのディレクトリのすべてのサブディレクトリも自動的に除外されます。

注意
各ドライブについて、完全なパス (ドライブ文字で開始) を入力して、最大 20 件の例外を指定できます。
例: C:\Program Files\Application\Name.log

完全なパスを入力しない場合、例外の最大数は 64 件です。
例: *.log
\computer1\C\directory1

注意
別のドライブにディレクトリとして組み込まれている動的ドライブの場合、例外のリスト内では、統合されたドライブに対してオペレーティング システムの別名を使用する必要があります。
例: \Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\
C:\DynDrive のようなマウント ポイント自体を使用する場合は、いずれにしても動的ドライブはスキャンされます。Guard のレポート ファイルからオペレーティング システムの別名が使用されるように指定できます。

このボタンをクリックするとウィンドウが開き、除外するファイル オブジェクトを選択できます。

追加

このボタンを使用すると、入力ボックスに入力したファイル オブジェクトを表示ウィンドウに追加できます。

削除

このボタンを使用すると、選択したファイル オブジェクトを表示ウィンドウから削除できます。

除外を指定する場合について、さらに以下のことに注意してください。

注意
MS-DOS ファイル名 (8.3 形式) でアクセスされるオブジェクトも除外するには、関連する MS-DOS ファイル名もリストに入力する必要があります。

注意
ワイルドカードを含むファイル名の末尾に円記号を使用することはできません。

例:

```
C:\Program Files\Application\applic*.exe\
```

このエントリは有効ではありません。例外として処理できません。

注意
接続ネットワーク ドライブに関する除外について、以下のことに注意してください。接続されているネットワーク ドライブのドライブ文字を使用している場合、指定したファイルとフォルダは Guard のスキャン対象外になりません。例外のリストにある 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 パスと異なる場合 (例外のリストでの IP アドレスの指定 - ネットワーク ドライブへの接続用のコンピュータ名の指定)、指定したフォルダおよびファイルは Guard のスキャン対象外になりません。Guard レポート ファイルで関連する UNC パスを特定します。
\\<コンピュータ名>\<Enable>\ - または - \\<IP アドレス>\<Enable>\

注意
Guard が感染したファイルのスキャンに使用するパスは、Guard のレポート ファイルで確認できます。例外リストには、これとまったく同じようにパスを指定してください。具体的な手順は次のとおりです。Guard::レポートの設定で、Guard のプロトコル機能を **[完全]** に設定します。次に、有効化された Guard で、ファイル、フォルダ、マウント ドライブ、または接続先ネットワーク ドライブにアクセスします。これで、Guard レポート ファイルから使用されたパスを読み取ることができるようになります。レポート ファイルは、コントロール センターのローカル保護::Guard からアクセスできます。

注意
SMC で AntiVir プログラムを管理している場合、プロセスおよびファイルの除外のためにパスの詳細で変数を使用できます。変数::Guard および Scanner の除外で、使用可能な変数のリストを参照できます。

除外するプロセスの例:

- application.exe

  application.exe プロセスは、それが位置するハード ディスク ドライブおよびディレクトリにかかわりなく、Guard スキャンから除外されます。

- C:\Program Files1\Application.exe

  パス C:\Program Files1 にあるファイル application.exe のプロセスは、Guard のスキャンから除外されます。

- C:\Program Files1*.exe

パス C:\Program Files1 の下に位置する実行可能ファイルのすべてのプロセスが Guard スキャンから除外されます。

除外対象ファイルの例:

– *.mdb

拡張子 'mdb' を持つすべてのファイルが Guard スキャンから除外されます。

– *.xls*

ファイル拡張子の先頭が 'xls' であるすべてのファイル (たとえば、拡張子.xls および .xlsx のファイル) が Guard スキャン から除外されます。

– C:\Directory*.log

パス C:\Directory の下にある拡張子 'log' を持つすべてのログ ファイルが Guard スキャンから除外されます。

– \\Computer name\Shared1\

接続 '\\Computer name1\Shared1' によりアクセスされる Guard スキャンからすべてのファイルが除外されます。これは一般に、コンピュータ名 'Computer name1' および共有名 'Shared1' により、共有フォルダで別のコンピュータにアクセスする接続ネットワーク ドライブです。

– \\1.0.0.0\Shared1*.mdb

拡張子 'mdb' を持つすべてのファイルは、接続 '\\1.0.0.0\Shared1' によりアクセスされる Guard スキャンから除外されます。これは一般に、IP アドレス '1.0.0.0' および共有名 'Shared1' により、共有フォルダで別のコンピュータにアクセスする接続ネットワーク ドライブです。

-

12.2.1.4. ヒューリスティック

この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 スキャン機能に対する設定が含まれます。

AntiVir 製品は非常に強力なヒューリスティック スキャン機能を備えており、有害な要素に対応する専用のウイルス シグネチャが作成される前や、アンチウイルス ソフトウェアの更新プログラムが送信される前などに、未知のマルウェアを予防的に検出することができます。ウイルスの検出では、マルウェアの典型的な機能に関して、感染したコードの広範な分析と検査が行われます。スキャンされたコードにこれらに独特の特徴が見られる場合、疑わしいファイルとして報告されます。これは必ずしもそのコードが、実際にマルウェアであるという意味ではありません。誤検出が生じる場合もあります。感染したと疑われるコードの処理に関する決定は、コードのソースが信頼できるかどうかに関する知識などに基づいて、ユーザーが判断する必要があります。

マクロウイルス ヒューリスティック

マクロウイルス ヒューリスティック

AntiVir 製品には、非常に強力なマクロウイルス ヒューリスティック スキャン機能が含まれています。このオプションを有効にすると、修復の場合に関連ドキュメントのすべてのマクロが削除されるか、あるいはアラートの送信などで不審な文書に関するレポートのみが行われます。このオプションは初期状態で有効に設定されています (推奨の設定)。

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

AntiVir プログラムには、AntiVir AheAD テクノロジという非常に強力なヒューリスティック スキャン機能が含まれていて、未知の (新しい) マルウェアも検出できます。このオプションを有効にすると、このヒューリスティック スキャン機能をどの程度 "アグレッシブ" にするかを定義できます。このオプションは初期状態で有効に設定されています。

低検出レベル

このオプションを有効にすると、検出される未知のマルウェアがやや減りますが、誤ったアラートのリスクは低くなります。

中検出レベル

このヒューリスティック スキャン機能の使用を選択すると、このオプションが初期状態で有効になります。

高検出レベル

このオプションを有効にすると、未知のマルウェアをかなり多く検出するようになりますが、より高い確率で誤検出が起こる点にも注意が必要です。

12.2.2 ProActiv

Avira AntiVir ProActiv では、使用可能なウイルス定義またはヒューリスティックスがまだない、新たな不明な脅威からの保護が可能です。ProActiv テクノロジは Guard コンポーネントに統合され、実行されるプログラム アクションを監視および分析します。プログラムの動作は典型的なマルウェアのアクション パターン、つまり、アクションのタイプとアクションの順序に対してチェックされます。プログラムがマルウェアに典型的な動作を示す場合、これはウイルス検出として扱われます。プログラムをブロックするか、通知を無視してプログラムの使用を続行するかを選択できます。プログラムを信頼済みとして分類し、許可するプログラムのアプリケーション フィルタに追加できます。*[常にブロック]* コマンドを使用して、ブロックするプログラムのアプリケーション フィルタにプログラムを追加することもできます。

ProActiv コンポーネントは Avira マルウェア研究センターによって開発されたルール セットを使用して、不審な動作を特定します。ルール セットは Avira GmbH データベースによって提供されます。Avira AntiVir ProActiv は、検出されたあらゆる不審なプログラムに関する情報をログ用に Avira データベースに送信します。Avira データベースへのデータの送信を無効にすることもできます。

注意

ProActiv テクノロジは、64 ビット システムに対してはまだ使用できません。Windows 2000 は ProActiv コンポーネントをサポートしていません。

全般

Avira AntiVir ProActiv を有効にする

このオプションを有効にすると、プログラムがコンピュータ システム上で監視され、不審な動作がチェックされます。典型的なマルウェア動作が検出された場合は、メッセージが表示されます。プログラムをブロックするか、"*[無視]*" を選択してプログラムの使用を続行できます。次のものは監視プロセスの対象外になります。 信頼済みと分類されているプログラム、許可されるアプリケーションのフィルタに既定で含まれている信頼済みかつ署名済みプログラム、許可されるプログラムとしてアプリケーション フィルタに追加したすべてのプログラム。

AntiVir ProActiv コミュニティに参加することで、コンピュータのセキュリティが向上します。

このオプションを有効にした場合、Avira AntiVir ProActiv は高度なオンライン スキャンのために Avira マルウェア研究センターに不審なプログラムに関するデータ、さらに場合によっては不審なプログラム ファイル (実行可能ファイル) を送信します。評価後、これらのデータは ProActiv の動作に関する分析ルール セットに追加されます。このように、Avira ProActiv コミュニティの一員となって、ProActiv セキュリティ テクノロジの継続的な向上および洗練に貢献します。 このオプションを無効にすると、データは送信されません。このオプションにより ProActiv 機能に影響はありません。

詳細については、こちらをクリックしてください。

このリンクでは、高度なオンライン スキャンに関する詳細情報を参照できるインターネット ページが開きます。このインターネット ページには、高度なオンライン スキャン中に送信されたすべてのデータが含まれます。

12.2.2.1. 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

[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] で、有害として分類して Avira AntiVir ProActiv で既定でブロックする必要のあるアプリケーションを入力できます。追加したアプリケーションはコンピュータ システム上で実行できません。Guard による不審なプログラムの動作の通知で、*[このプログラムを常にブロック]* オプションを有効にしても、ブロックするアプリケーションのフィルタにプログラムを追加できますを参照)。

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、設定での入力によりまたは ProActiv コンポーネントへの通知により、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。リスト内のアプリケーションは Avira AntiVir ProActiv によってブロックされ、コンピュータ システム上で実行できません。ブロックされたプログラムの起動時にオペレーティング システム メッセージが表示されます。ブロックするアプリケーションは指定したパスとファイル名に基づいて Avira AntVir ProActiv によって特定され、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

ブロックするアプリケーションをこのボックスに入力します。アプリケーションを特定するために、フル パス、ファイル名、ファイル拡張子を指定する必要があります。パスには、アプリケーションのあるドライブを指定するか、先頭に環境変数を指定する必要があります。

このボタンをクリックすると、ブロックするアプリケーションを選択できるウィンドウが開きます。

追加

[追加] ボタンをクリックすると、ブロックするアプリケーションのリストに、入力ボックスで指定したアプリケーションを追加できます。

注意
オペレーティング システムの正常な動作に必要なアプリケーションは追加できません。

削除

[削除] ボタンをクリックすると、ブロックするアプリケーションのリストから、ハイライト表示したアプリケーションを削除できます。

12.2.2.2. アプリケーション フィルタ::許可されるアプリケーション

[アプリケーション フィルタ]::[許可されるアプリケーション] セクションには、ProActiv コンポーネントの監視対象外のアプリケーションが表示されます。具体的には、信頼済みとして分類され既定でこのリストに追加される署名済みプログラム、信頼済みとして分類されアプリケーション フィルタに追加されるすべてのアプリケーションです。 設定で、許可されるアプリケーションをリストに追加できます。Guard による不審なプログラムの動作の通知で、**[信頼済みのプログラム]** オプションを使用しても、このリストにアプリケーションを追加できます。

除外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、ProActiv コンポーネントの監視対象外のアプリケーションが表示されます。既定のインストール設定で、このリストには信頼済みプロデューサからの署名済みのアプリケーションが含まれています。設定でまたは Guard による通知で信頼済みとするアプリケーションを追加することもできます。ProActiv コンポーネントはパス、ファイル名、コンテンツを使用してアプリケーションを特定します。更新のような変更を通じてプログラムにマルコードが追加される可能性があるため、コンテンツ チェックをお勧めします。指定したタイプによって、コンテンツ チェックが実行されるかどうかが決まります。*"[コンテンツ]"* タイプの場合、パスとファイル名で指定したアプリケーションは、ProActiv コンポーネントの監視対象外になる前に、ファイルのコンテンツに対する変更についてチェックされます。ファイルのコンテンツが変更されている場合、そのアプリケーションは再度 ProActiv コンポーネントの監視対象になります。*"[パス]"* タイプの場合、アプリケーションが Guard の監視対象外になる前に、コンテンツ チェックは実行されません。除外タイプを変更するには、表示されたタイプをクリックします。

警告
特別な場合のみ、*[パス]* タイプを使用します。マルコードは更新を通じてアプリケーションに追加される可能性があります。もともとは無害だったアプリケーションがマルウェアとなっている可能性があります。

注意
一部の信頼済みアプリケーション、たとえば AntiVir プログラムのすべてのアプリケーション コンポーネントは、このリストに含まれていない場合でも、既定で ProActiv コンポーネントの監視対象外になります。

入力ボックス

このボックスに、ProActiv コンポーネントの監視対象外にするアプリケーションを入力します。アプリケーションを特定するために、フル パス、ファイル名、ファイル拡張子を指定する必要があります。パスには、アプリケーションのあるドライブを指定するか、先頭に環境変数を指定する必要があります。

このボタンをクリックすると、監視対象外にするアプリケーションを選択できるウィンドウが開きます。

追加

[追加] ボタンをクリックすると、監視対象外にするアプリケーションのリストに、入力ボックスで指定したアプリケーションを追加できます。

削除

[削除] ボタンをクリックすると、監視対象外にするアプリケーションのリストから、ハイライト表示したアプリケーションを削除できます。

12.2.3 レポート

Guard には、ユーザーおよび管理者に検出のタイプと方法に関する正確な注釈を提供することのできる詳細なログ機能が備えられています。

レポート

このグループを使用すると、レポート ファイルの内容を指定できます。

オフ

このオプションを有効にすると、Guard はログを作成しません。
ログ機能は、複数のウイルスまたは不要プログラムに関するテストの実行など、例外的な場合にのみオフにすることをお勧めします。

既定

このオプションを有効にすると、Guard はレポート ファイルに重要な情報 (ウイルス検出、アラートおよびエラー) を書き込み、レポート ファイルが見やすくなるように重要性の低い情報は無視します。このオプションは初期状態で有効に設定されています。

詳細

このオプションを有効にすると、Guard はレポート ファイルに重要性の低い情報も書き込みます。

完了

このオプションを有効にすると、Guard はレポート ファイルに、ファイル サイズ、ファイル タイプ、日付など、使用可能なすべての情報を書き込みます。

レポート ファイルの制限

サイズを n MB に制限

このオプションを有効にすると、レポート ファイルを特定のサイズに制限できます。可能な値: 許容される値は 1 ～ 100 MB です。レポート ファイルのサイズを制限するとき、システム リソースの使用を最小限に抑えるために、最大 50 キロバイトの予備領域が設定されています。ログ ファイルのサイズが指定したサイズを 50 キロバイト以上超えると、指定したサイズより 50 キロバイト少なくなるまで、古いエントリが削除されます。

短縮前にレポート ファイルをバックアップ

このオプションを有効にすると、レポート ファイルが短縮される前にバックアップされます。保存場所については、設定::全般::ディレクトリ::レポート ディレクトリを参照してください。

設定をレポート ファイルに書き込む

このオプションを有効にすると、オンアクセス スキャンで使用された設定がレポート ファイルに書き込まれます。

注意

レポート ファイルの制限を指定していない場合、レポート ファイルが 100MB に達すると新しいレポート ファイルが自動的に作成されます。古いレポート ファイルのバックアップが作成されます。最大で、古いレポート ファイルの 3 つのバックアップが保存されます。最も古いバックアップが最初に削除されます。

12.3 MailGuard

MailGuard の設定には、設定の [MailGuard] セクションを使用します。

12.3.1 スキャン

受信電子メールのウイルス、マルウェア、のスキャンには、MailGuard を使用します。送信電子メールのウイルスとマルウェアは、MailGuard でスキャンできます。

スキャン

MailGuard を有効にする

このオプションを有効にすると、電子メール トラフィックが MailGuard により監視されます。MailGuard は、使用中の電子メール サーバーとコンピュータ システム上の電子メール クライアント プログラム間のデータ トラフィックをスキャンするプロキシ サーバーです。受信電子メールは、マルウェアについて既定でスキャンされます。 このオプションを無効にすると、MailGuard サービスは開始されますが、MailGuard による監視は無効になります。

受信メールのスキャン

このオプションを有効にすると、受信電子メールに対してウイルス、マルウェアのスキャンが実行されます。MailGuard では、POP3 プロトコルおよび IMAP プロトコルがサポートされます。電子メール クライアントが電子メールの受信に使用する受信トレイ アカウントに対して、MailGuard による監視を有効にします。

POP3 アカウントの監視

このオプションを有効にすると、特定のポートで POP3 アカウントが監視されます。

監視中のポート

このフィールドには、POP3 プロトコルが受信トレイとして使用するポートを入力します。複数のポートを指定する場合は、カンマで区切って指定します。

既定

このボタンは、特定のポートを既定の POP3 ポートにリセットします。

IMAP アカウントの監視

このオプションを有効にすると、特定のポートで IMAP アカウントが監視されます。

監視中のポート

このフィールドには、IMAP プロトコルが受信トレイとして使用するポートを入力します。複数のポートを指定する場合は、カンマで区切って指定します。

既定

このボタンは、特定のポートを既定の IMAP ポートにリセットします。

送信メールのスキャン (SMTP)

このオプションを有効にすると、送信電子メールに対してウイルスおよびマルウェアのスキャンが実行されます。

監視中のポート

このフィールドには、SMTP プロトコルが送信トレイとして使用するポートを入力します。複数のポートを指定する場合は、カンマで区切って指定します。

既定

このボタンは、特定のポートを既定の SMTP ポートにリセットします。

注意

使用されているプロトコルおよびポートを確認するには、電子メール クライアント プログラムで、実際の電子メール アカウントのプロパティを表示してください。通常は、既定のポートが使用されます。

12.3.1.1. 検出時のアクション

この設定セクションには、MailGuard が電子メール、または添付ファイルにウイルスまたは不要プログラムを検出した場合に実行されるアクションに関する設定が含まれています。

注意

これらのアクションは、受信電子メールにウイルスが検出された場合と、送信電子メールにウイルスが検出された場合の両方に実行されます。

検出時のアクション

対話型

このオプションを有効にすると、電子メールまたは添付ファイルにウイ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、疑わしい電子メールまたは添付ファイルをどう処理するかを選択できます。このオプションは初期状態で有効に設定されています。

許可されたアクション

このボックスでは、ウイルス検出時に表示される選択可能なアクションを指定できます。これに対応するオプションを有効にする必要があります。

[隔離] に移動

このオプションを有効にすると、電子メールはすべての添付ファイルを含めて、[隔離] に移動されます。後で、隔離を介して配信することもできます。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。

削除

このオプションを有効にすると、ウイルスまたは不要プログラムが検出された場合、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

このオプションを有効にすると、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。電子メールの本文が感染した場合は、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

このオプションを有効にすると、感染した添付ファイルは、[隔離] に移動されてから削除されます (既定のテキストに置換)。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、後で隔離によって配信されます。

無視

このオプションを有効にすると、感染した電子メールはウイルスまたは不要プログラムが検出されても配信されます。

既定

このボタンを使用すると、ウイルスが検出された場合、ダイアログ ボックスで既定でアクティブにするアクションを選択できます。既定でアクティブにするアクションを選択して、**[既定]** ボタンをクリックします。

プログレス バーの表示

このオプションを有効にすると、電子メールのダウンロード中、MailGuard にプログレス バーが表示されます。このオプションは、**[対話型]** オプションが選択されている場合のみ有効にできます。

自動

このオプションを有効にすると、ウイルスまたは不要プログラムが検出されても、通知されなくなります。MailGuard は、このセクションで定義した設定に従って動作します。

プライマリ アクション

プライマリ アクションとは、MailGuard が電子メールにウイルスまたは不要プログラムを検出した場合に実行されるアクションです。**[電子メールを無視]** オプションを選択すると、**[感染した添付ファイル]** の下で、添付ファイルにウイルスまたは不要プログラムが検出された場合にどう処理するかも選択できます。

電子メールを削除

このオプションを有効にすると、ウイルスまたは不要プログラムが検出された場合、感染した電子メールは自動的に削除されます。電子メールの本文は、以下に指定する既定のテキストに置換されます。これは含まれるすべての添付ファイルにも適用され、既定のテキストに置換されます。

電子メールを分離

このオプションを有効にすると、ウイルスまたは不要プログラムが検出された場合、すべての添付ファイルを含む完全な電子メールが [隔離] に配置されます。必要に応じて、後で復元できます。感染した電子メール自体は削除されます。電子メールの本文は、以下に指定する既定のテキストに置換されます。これは含まれるすべての添付ファイルにも適用され、既定のテキストに置換されます。

電子メールを無視

このオプションを有効にすると、感染した電子メールはウイルスまたは不要プログラムが検出されても配信されます。ただし、感染した添付ファイルをどう処理するかを選択できます。

影響を受ける添付ファイル

[感染した添付ファイル] オプションは、**[電子メールを無視]** の設定が **[プライマリ アクション]** の下で選択されている場合にのみ選択できます。このオプションを使用して、添付ファイルにウイルスまたは不要プログラムが検出された場合にどう処理するかを決定できるようになりました。

削除

このオプションを有効にすると、ウイルスまたは不要プログラムが検出された場合、既定のテキストに置換され、感染した添付ファイルは削除されます。

分離

このオプションを有効にすると、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)。必要に応じて、感染した添付ファイルは後で復元できます。

無視

このオプションを有効にすると、ウイルスまたは不要プログラムが検出されても添付ファイルは無視され、配信されます。

警告

このオプションを有効にすると、MailGuard によるウイルスおよび不要プログラムに対する保護がなくなります。内容を完全に把握している場合にのみ、このオプションを有効にしてください。電子メール プログラムのプレビューを無効にして、添付ファイルは絶対にダブルクリックで開かないでください。

12.3.1.2. その他のアクション

この設定セクションには、MailGuard が電子メール、または添付ファイルにウイルスまたは不要プログラムを検出した場合に実行されるアクションに関するその他の設定が含まれています。

注意

これらのアクションは、受信電子メールにウイルスが検出された場合にのみ実行されます。

電子メールの削除/移動に対する既定テキスト

このボックスのテキストは、感染した電子メールの代わりにメッセージとして電子メールに挿入されます。このメッセージは編集できます。テキストには、最大 500 文字を含めることができます。

書式設定には、次のキーの組み合わせを使用できます。

Strg + Enter　改行を挿入します。

既定

このボタンは、事前に設定済みの既定のテキストを編集ボックスに挿入します。

添付ファイルの削除/移動に対する既定テキスト

このボックスのテキストは、感染した添付ファイルの代わりに、メッセージとして電子メールに挿入されます。このメッセージは編集できます。テキストには、最大 500 文字を含めることができます。

書式設定には、次のキーの組み合わせを使用できます。

Strg + Enter　改行を挿入します。

既定

このボタンは、事前に設定済みの既定のテキストを編集ボックスに挿入します。

12.3.1.3. ヒューリスティック

この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 スキャン機能に対する設定が含まれます。

AntiVir 製品は非常に強力なヒューリスティック スキャン機能を備えており、有害な要素に対応する専用のウイルス シグネチャが作成される前や、アンチウイルス ソフトウェアの更新プログラムが送信される前などに、未知のマルウェアを予防的に検出することができます。ウイルスの検出では、マルウェアの典型的な機能に関して、感染したコードの広範な分析と検査が行われます。スキャンされたコードにこれらに独特の特徴が見られる場合、疑わしいファイルとして報告されます。これは必ずしもそのコードが、実際にマルウェアであるという意味ではありません。誤検出が生じる場合もあります。感染したと疑われるコードの処理に関する決定は、コードのソースが信頼できるかどうかに関する知識などに基づいて、ユーザーが判断する必要があります。

マクロウイルス ヒューリスティック

マクロウイルス ヒューリスティックを有効化

AntiVir 製品には、非常に強力なマクロウイルス ヒューリスティック スキャン機能が含まれています。このオプションを有効にすると、修復の場合に関連ドキュメントのすべてのマクロが削除されるか、あるいはアラートの送信などで不審な文書に関するレポートのみが行われます。このオプションは初期状態で有効に設定されています (推奨の設定)。

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

AntiVir プログラムには、AntiVir AheAD テクノロジという非常に強力なヒューリスティック スキャン機能が含まれていて、未知の (新しい) マルウェアも検出できます。このオプションを有効にすると、このヒューリスティック スキャン機能をどの程度 "アグレッシブ" にするかを定義できます。このオプションは初期状態で有効に設定されています。

低検出レベル

このオプションを有効にすると、検出される未知のマルウェアがやや減りますが、誤ったアラートのリスクは低くなります。

中検出レベル

このヒューリスティック スキャン機能の使用を選択すると、このオプションが初期状態で有効になります。このオプションは初期状態で有効に設定されています (推奨の設定)。

高検出レベル

このオプションを有効にすると、未知のマルウェアをかなり多く検出するようになりますが、より高い確率で誤検出が起こる点にも注意が必要です。

12.3.2 全般

12.3.2.1. 例外

例外のスキャン

この表は、AntiVir MailGuard のスキャン対象から除外される電子メール アドレスのリストです (ホワイト リスト)。

注意
例外のリストは、MailGuard のみによって、受信電子メールに対して使用されます。

状況

アイコン	説明
	この電子メール アドレスに対して、マルウェアのスキャンが実行されなくなります。

電子メール アドレス

スキャンを実行しない電子メール アドレス。

マルウェア

このオプションを有効にすると、その電子メール アドレスに対しては、マルウェアのスキャンが実行されなくなります。

上

このボタンを使用すると、ハイライト表示された電子メール アドレスが上の位置に移動します。ハイライト表示されたエントリがなかったり、ハイライト表示されたアドレスがリストの最初の位置にある場合、このボタンは有効になりません。

下

このボタンを使用すると、ハイライト表示された電子メール アドレスが下の位置に移動します。ハイライト表示されたエントリがなかったり、ハイライト表示されたアドレスがリストの最後の位置にある場合、このボタンは有効になりません。

入力ボックス

このボックスには、スキャンされない電子メール アドレスのリストに追加する電子メール アドレスを入力します。設定により、電子メール アドレスに対して、MailGuard によるスキャンが実行されなくなります。

追加

このボタンを使用すると、入力ボックスに入力した電子メール アドレスをスキャンされない電子メール アドレスのリストに追加できます。

削除

このボタンは、ハイライト表示された電子メール アドレスをリストから削除します。

12.3.2.2. キャッシュ

キャッシュ

MailGuard のキャッシュには、MailGuard の下のコントロール センターで統計データとして表示される、スキャン済み電子メールに関するデータが格納されます。

キャッシュ内の電子メールの最大件数

このフィールドは、MailGuard によってキャッシュに保存される電子メールの最大数の設定に使用します。最も古い電子メールが最初に削除されます。

メールを保管する最大日数

電子メールの最大保存期間をこのボックスに日数で入力します。この日数が経過すると、電子メールはキャッシュから削除されます。

空のキャッシュ

このボタンをクリックすると、電子メールがキャッシュから削除されます。

12.3.2.3. フッター

[フッター] の下で、送信する電子メールに表示される電子メール フッターを設定できます。この機能には、送信電子メールの MailGuard スキャンをアクティブにすることが必要です (*設定::MailGuard::スキャン*の下の [送信メールのスキャン (SMTP)] オプションを参照)。定義した AntiVir MailGuard フッターを使用して、送信電子メールがウイルス対策プログラムによってスキャンされたことを確認できます。ユーザー定義のフッター用のテキストを自分で挿入することもできます。両方のフッター オプションを使用する場合、AntiVir MailGuard フッターがユーザー定義のテキストの前に挿入されます。

送信するメールのフッター

AntiVir MailGuard フッターを添付

このオプションを有効にすると、AntiVir MailGuard フッターが、送信電子メールのメッセージ テキストの下に表示されます。AntiVir MailGuard フッターにより、送信電子メールが AntiVir MailGuardAntiVir MailGuard フッターには次のテキストが含まれます。"AntiVir MailGuard [製品バージョン] [検索エンジンのイニシャルおよびバージョン番号] [ウイルス定義ファイルのイニシャルおよびバージョン番号] によってスキャンされました。"

このフッターを添付

このオプションを有効にすると、入力ボックスに挿入したテキストが送信電子メールのフッターとして表示されます。

入力ボックス

この入力ボックスでは、送信電子メールのフッターとして表示されるテキストを挿入できます。

12.3.3 レポート

MailGuard には、ユーザーおよび管理者に検出のタイプと方法に関する正確な注釈を提供することのできる詳細なログ機能が備えられています。

レポート

このグループを使用すると、レポート ファイルの内容を指定できます。

オフ

このオプションを有効にすると、MailGuard はログを作成しません。
ログ機能は、複数のウイルスまたは不要プログラムに関するテストの実行など、例外的な場合にのみオフにすることをお勧めします。

既定

このオプションを有効にすると、MailGuard はレポート ファイルに重要な情報 (ウイルス検出、アラートおよびエラー) を書き込み、レポート ファイルが見やすくなるように重要性の低い情報は無視します。このオプションは初期状態で有効に設定されています。

詳細

このオプションを有効にすると、MailGuard はレポート ファイルに重要性の低い情報も書き込みます。

完了

このオプションを有効にすると、MailGuard はレポート ファイルにすべての情報を書き込みます。

レポート ファイルの制限

サイズを n MB に制限

このオプションを有効にすると、レポート ファイルを特定のサイズに制限できます。可能な値: 許容される値は 1 ～ 100 MB です。レポート ファイルのサイズを制限するとき、システム リソースの使用を最小限に抑えるために、最大 50 キロバイトの予備領域が設定されています。ログ ファイルのサイズが指定したサイズを 50 キロバイト以上超えると、指定したサイズより 50 キロバイト少なくなるまで、古いエントリが削除されます。

短縮前にレポート ファイルをバックアップ

このオプションを有効にすると、レポート ファイルが短縮される前にバックアップされます。保存場所については、設定::全般::ディレクトリ::レポート ディレクトリを参照してください。

設定をレポート ファイルに書き込む

このオプションを有効にすると、MailGuard の設定がレポート ファイルに書き込まれます。

注意

レポート ファイルの制限を指定していない場合、レポート ファイルが 100MB. に達すると新しいレポート ファイルが自動的に作成されます。古いレポート ファイルのバックアップが作成されます。最大で、古いレポート ファイルの 3 つのバックアップが保存されます。最も古いバックアップが最初に削除されます。

12.4 ファイアウォール

Avira Firewall の設定には、[設定] の [FireWall] セクションを使用します。

12.4.1 アダプタ ルール

Avira FireWall では、アダプタとはソフトウェアでシミュレーションされたハードウェア デバイス (例: ミニポート、ブリッジ接続など) または実際のハードウェア デバイス (例: ネットワーク カード) を指します。

Avira FireWall では、ドライバがインストールされているコンピュータのすべての既存のアダプタのアダプタ ルールが表示されます。

事前に設定済みのアダプタ ルールは、セキュリティ レベルに依存します。セキュリティ レベルを、Avira AntiVir Professional コントロール センター の [オンライン保護] :: [コントロール センターで FireWall の設定を変更できます。独自のアダプタ ルールを定義することもできます。コントロール センターの [FireWall] セクションで、独自のアダプタ ルールを定義している場合、セキュリティ レベルはカスタムに設定されます。

注意
Avira FireWall のすべての事前に設定済みのルールに対する既定のセキュリティ レベル設定は、**[中]** です。

ICMP プロトコル

インターネット制御メッセージ プロトコル (ICMP) は、ネットワーク上でのエラー メッセージや情報メッセージの交換に使用されます。このプロトコルは、ping または tracer のステータス メッセージにも使用されます。
このルールを使用すると、受信および送信ブロック メッセージ タイプ、フラッディングの場合の動作、断片化した ICMP パケットへの対応を定義できます。このルールは、ICMP flood 攻撃の防止に役立ちます。この攻撃を受けたコンピュータはすべてのパケットに応答することになるため、そのコンピュータの CPU の負荷が増大します。

ICMP プロトコルの事前に設定済みのルール

設定: 低	設定: 中	設定: 高
受信ブロック タイプ: **タイプなし**。 送信ブロック タイプ: **タイプなし**。 パケット間の遅延が **50** ミリ秒未満の場合、フラッディングを想定します。 断片化した ICMP パケットを**拒否**します。	これは低レベルと同じルールです。	受信ブロック タイプ: **複数のタイプ** 送信ブロック タイプ: **複数のタイプ** パケット間の遅延が **50** ミリ秒未満の場合、フラッディングを想定します。 断片化した ICMP パケットを**拒否**します。

受信ブロック タイプ: タイプなし/複数のタイプ

このリンクをマウスでクリックすると、ICMP パケット タイプのリストが表示されます。このリストから、ブロックする受信 ICMP メッセージ タイプを指定できます。

送信ブロック タイプ: タイプなし/複数のタイプ

このリンクをマウスでクリックすると、ICMP パケット タイプのリストが表示されます。このリストから、ブロックする送信 ICMP メッセージ タイプを選択できます。

フラディング

このリンクをマウスでクリックすると、ダイアログ ボックスが表示され、最大許容 ICMPA 遅延を入力できます。

断片化した ICMP パケット

このリンクをマウスでクリックすると、断片化した ICMP パケットを拒否するかしないかを選択できます。

TCP ポート スキャン

このルールを使用すると、FireWall によって TCP ポート スキャンが想定される場合、およびその場合に何を実行するかを定義できます。このルールは、TCP ポート スキャン攻撃の防止に役立ちます。この攻撃を受けたコンピュータでは、開いたままの TCP ポートが検出されます。この種の攻撃は、コンピュータの弱点の検索に使用され、その後、さらに危険な攻撃タイプが続く場合もよくあります。

TCP ポート スキャンの事前に設定済みのルール

設定: 低	設定: 中	設定: 高
50 以上のポートが **5,000** ミリ秒でスキャンされた場合、TCP ポート スキャンを想定します。 検出されたとき、攻撃者の IP を**記録**し、攻撃をブロックするルールは**追加しません**。	**50** 以上のポートが **5,000** ミリ秒でスキャンされた場合、TCP ポート スキャンを想定します。 検出されたとき、攻撃者の IP を**ログ**し、攻撃をブロックするルールを**追加**します。	中レベルと同じルール。

ポート

このリンクをマウスでクリックすると、ダイアログ ボックスが表示されます。このダイアログ ボックスに入力したポート数がスキャンされた場合、TCP ポート スキャンを想定します。

ポート スキャン時間枠

このリンクをマウスでクリックすると、ダイアログ ボックスが表示されます。このダイアログ ボックスに入力したポート スキャンの時間枠内に一定数のポート スキャンが実行された場合、TCP ポート スキャンを想定します。

レポート ファイル

このリンクをマウスでクリックすると、攻撃者の IP アドレスを記録するかしないかを選択できます。

ルール

このリンクをマウスでクリックすると、TCP ポート スキャン攻撃をブロックするルールを追加するかしないかを選択できます。

UDP ポート スキャン

このルールを使用すると、FireWall によって UDP ポート スキャンが想定される場合、およびその場合に何を実行するかを定義できます。このルールにより、UDP ポート スキャン攻撃を防止できます。この攻撃を受けると、コンピュータで開いている UDP ポートが検出されます。この種の攻撃は、コンピュータの弱点の検索に使用され、その後、さらに危険な攻撃タイプが続く場合もよくあります。

UDP ポート スキャンの事前に設定済みのルール

設定: 低	設定: 中	設定: 高
50 以上のポートが **5,000** ミリ秒でスキャンされた場合、UDP ポート スキャンを想定します。 検出されたとき、攻撃者の IP を**記録**し、攻撃をブロックするルールは**追加しません**。	**50** 以上のポートが **5,000** ミリ秒でスキャンされた場合、UDP ポート スキャンを想定します。 検出されたとき、攻撃者の IP を**ログ**し、攻撃をブロックするルールを**追加**します。	中レベルと同じルール。

ポート

このリンクをマウスでクリックすると、ダイアログ ボックスが表示されます。このダイアログ ボックスに入力したポート数がスキャンされた場合、UDP ポート スキャンを想定します。

ポート スキャン時間枠

このリンクをマウスでクリックすると、ダイアログ ボックスが表示されます。このダイアログ ボックスに入力したポート スキャンの時間枠内に一定数のポート スキャンが実行された場合、UDP ポート スキャンを想定します。

レポート ファイル

このリンクをマウスでクリックすると、攻撃者の IP アドレスを記録するかしないかを選択できます。

ルール

このリンクをマウスでクリックすると、UDP ポート スキャン攻撃をブロックするルールを追加するかしないかを選択できます。

12.4.1.1. 受信ルール

受信ルールは、Avira FireWall による受信トラフィックの制御のために定義します。

注意
パケットがフィルタされるとき、対応するルールが連続して適用されるため、ルールの順序は非常に重要です。内容を完全に把握している場合にのみ、ルールの順序を変更してください。

TCP データ トラフィック データ モニタの事前に設定済みのルール

設定: 低	設定: 中	設定: 高
Avira FireWall は受信データ トラフィックをブロックしません。	– ポート 135 上の TCP 接続確立を許可 **次の TCP パケットを許可する:** アドレス **0.0.0.0**、マスク **0.0.0.0**、ローカル ポート **{135}**、リモート ポート **{0-65535}**。 **既存の接続のパケット**に適用する。 パケットがルールに一致するときは記録しない。 詳細: 次のパケットを破棄する: **<empty>**、マスク **<empty>**、オフセット **0**。 – 135 の TCP パケットを拒否 次の TCP パケットを拒否する : アドレス **0.0.0.0**、マスク **0.0.0.0**、ローカル ポート **{135}**、リモート ポート **{0-65535}**。 すべてのパケット**に適用する。** パケットがルールに一致するときは記録しない。 詳細: 次のパケットを破棄する:	– 確立された TCP データ トラフィックを監視 **次の TCP パケットを拒否する:** アドレス **0.0.0.0**、マスク **0.0.0.0**、ローカル ポート **{0-65535}**、リモート ポート **{0-65535}**。 **既存の接続のパケット**に適用する。 パケットがルールに一致するときは記録しない。 詳細: 次のパケットを破棄する: **<empty>**、マスク **<empty>**、オフセット **0**。

	<empty>、マスク **<empty>**、オフセット **0**。 – TCP 正常データトラフィックを監視 **次の TCP パケットを拒否する:** アドレス **0.0.0.0**、マスク **0.0.0.0**、ローカル ポート **{0-65535}**、リモート ポート **{0-65535}**。**接続開始と既存接続のパケットに適用する。** パケットがルールに一致するときは記録しない。 詳細: 次のパケットを破棄する: **<empty>**、マスク **<empty>**、オフセット **0**。 – すべての TCP パケットを拒否 次の **TCP パケットを**拒否する: アドレス **0.0.0.0**、マスク **0.0.0.0**、ローカル ポート **{0-65535}**、リモート ポート **{0-65535}**。**すべてのパケットに**適用する。パケットがルールに一致するときは記録しない。	

	詳細: 次のパケットを破棄する: **<empty>**、マスク **<empty>**、オフセット **0**。	

TCP パケットを許可/拒否

このリンクをマウスでクリックすると、特別に定義した受信 TCP パケットを許可するか拒否するかを選択できます。

IP アドレス

このリンクをマウスでクリックすると、ダイアログ ボックスが開き、必要な IP アドレスを入力できます。

IP マスク

このリンクをマウスでクリックすると、ダイアログ ボックスが開き、必要な IP マスクを入力できます。

ローカル ポート

このリンクをマウスでクリックすると、ダイアログ ボックスが表示され、ローカル ポート番号、またはポートの全範囲を定義できます。

リモート ポート

このリンクをマウスでクリックすると、ダイアログ ボックスが表示され、リモート ポート番号、またはポートの全範囲を定義できます。

適用方法

このリンクをマウスでクリックすると、接続開始と既存接続のパケットに対して、既存接続のパケットに対してのみ、またはすべてのパケットに対して、ルールを適用するかを選択できます。

レポート ファイル

このリンクをマウスでクリックすると、パッケージがルールに一致する場合に、レポート ファイルに書き込むかどうかを決定できます。

詳細機能を使用するとコンテンツ フィルタを有効にできます。たとえば、特定のオフセットで特定のデータを含むパケットを拒否できます。このオプションを使用しない場合は、ファイルを選択しないか空のファイルを選択してください。

フィルタ対象のコンテンツ: データ

このリンクをマウスでクリックすると、ダイアログ ボックスが表示され、特定のバッファを含むファイルを選択できます。

フィルタ対象のコンテンツ: マスク

このリンクをマウスでクリックすると、ダイアログ ボックスが表示され、特定のマスクを選択できます。

フィルタ対象のコンテンツ: オフセット

このリンクをマウスでクリックすると、ダイアログ ボックスが表示され、フィルタ対象のコンテンツのオフセットを定義できます。オフセットは、TCP ヘッダーの終了位置から計算されます。

UDP データ トラフィック モニタの事前に設定済みのルール

設定: 低	設定: 中	設定: 高
-	– 許可された UDP データ トラフィックを監視 **次の UDP パケットを許可する:** アドレス **0.0.0.0**、マスク **0.0.0.0**、ローカル ポート **{0- 66535}**、リモート ポート **{0-66535}**。**開いたままのポート**にルールを適用する。パケットがルールに一致するときは記録しない。詳細: 次のパケットを破棄する: **<empty>**、マスク **<empty>**、オフセット **0**。 – すべての UDP パケットを拒否 次の **UDP パケットを**拒否する: アドレス **0.0.0.0**、マスク **0.0.0.0**、ローカル ポート **{0-65535}**、リモート ポート **{0-65535}**。**すべてのポート**に適用する。パケットがルールに一致するときは記録しない。詳細: 次のパケットを破棄する: **<empty>**、マス	確立された UDP トラフィックを監視 次の **UDP パケット**を許可: アドレス **0.0.0.0**、マスク **0.0.0.0** (ローカル ポートの範囲が **{0-65535}** で、リモート ポートの範囲が **{53, 67, 68, 123}** の場合)。**開いたままのポート**にルールを適用する。パケットがルールに一致するときは記録しない。詳細: 次のパケットを破棄する: **<empty>**、マスク **<empty>**、オフセット **0**。

	ク **<empty>**、オフセット **0**。	

UDP パケットを許可/拒否

このリンクをマウスでクリックすると、特別に定義した受信 UDP パケットを許可するか拒否するかを選択できます。

IP アドレス

このリンクをマウスでクリックすると、ダイアログ ボックスが開き、必要な IP アドレスを入力できます。

IP マスク

このリンクをマウスでクリックすると、ダイアログ ボックスが開き、必要な IP マスクを入力できます。

ローカル ポート

このリンクをマウスでクリックすると、ダイアログ ボックスが表示され、ローカル ポート番号、またはポートの全範囲を定義できます。

リモート ポート

このリンクをマウスでクリックすると、ダイアログ ボックスが表示され、リモート ポート番号、またはポートの全範囲を定義できます。

適用方法

このリンクをマウスでクリックすると、このルールをすべてのポートに適用するか、オープンしたすべてのポートに適用するかを選択できます。

レポート ファイル

このリンクをマウスでクリックすると、パッケージがルールに一致する場合に、レポート ファイルに書き込むかどうかを決定できます。

詳細機能を使用するとコンテンツ フィルタを有効にできます。たとえば、特定のオフセットで特定のデータを含むパケットを拒否できます。このオプションを使用しない場合は、ファイルを選択しないか空のファイルを選択してください。

フィルタ対象のコンテンツ: データ

このリンクをマウスでクリックすると、ダイアログ ボックスが表示され、特定のバッファを含むファイルを選択できます。

フィルタ対象のコンテンツ: マスク

このリンクをマウスでクリックすると、ダイアログ ボックスが表示され、特定のマスクを選択できます。

フィルタ対象のコンテンツ: オフセット

このリンクをマウスでクリックすると、ダイアログ ボックスが表示され、フィルタ対象のコンテンツのオフセットを定義できます。オフセットは、UDP ヘッダーの終了位置から計算されます。

ICMP データ トラフィック モニタの事前に設定済みのルール

設定: 低	設定: 中	設定: 高
-	– IP アドレスに基づいて ICMP を破	中レベルと同じルール。

	棄しない **次の ICMP パケットを許可する**: アドレス **0.0.0.0**、マスク **0.0.0.0**。パケットがルールに一致するときは記録しない。 詳細: 次のパケットを破棄する: **<empty>**、マスク **<empty>**、オフセット **0**。	

ICMP パケットを許可/拒否

このリンクをマウスでクリックすると、特別に定義した受信 ICMP パケットを許可するか拒否するかを選択できます。

IP アドレス

このリンクをマウスでクリックすると、ダイアログ ボックスが開き、必要な IP アドレスを入力できます。

IP マスク

このリンクをマウスでクリックすると、ダイアログ ボックスが開き、必要な IP マスクを入力できます。

レポート ファイル

このリンクをマウスでクリックすると、パッケージがルールに一致する場合に、レポート ファイルに書き込むかどうかを決定できます。

詳細機能を使用するとコンテンツ フィルタを有効にできます。たとえば、特定のオフセットで特定のデータを含むパケットを拒否できます。このオプションを使用しない場合は、ファイルを選択しないか空のファイルを選択してください。

フィルタ対象のコンテンツ: データ

このリンクをマウスでクリックすると、ダイアログ ボックスが表示され、特定のバッファを含むファイルを選択できます。

フィルタ対象のコンテンツ: マスク

このリンクをマウスでクリックすると、ダイアログ ボックスが表示され、特定のマスクを選択できます。

フィルタ対象のコンテンツ: オフセット

このリンクをマウスでクリックすると、ダイアログ ボックスが表示され、フィルタ対象のコンテンツのオフセットを定義できます。オフセットは、ICMP ヘッダーの終了位置から計算されます。

IP パケットの事前に設定済みのルール

設定: 低	設定: 中	設定: 高
-	-	すべての IP パケットを拒否 次の **IP パケット**を拒否する: アドレス **0.0.0.0**、マスク **0.0.0.0**。 パケットがルールに一致するときは記録しない。

IP パケットを許可/拒否

このリンクをマウスでクリックすると、特別に定義した IP パッケージを許可するか拒否するかを決定できます。

IP アドレス

このリンクをマウスでクリックすると、ダイアログ ボックスが開き、必要な IP アドレスを入力できます。

IP マスク

このリンクをマウスでクリックすると、ダイアログ ボックスが開き、必要な IP マスクを入力できます。

レポート ファイル

このリンクをマウスでクリックすると、パッケージがルールに一致する場合に、レポート ファイルに書き込むかどうかを決定できます。

IP プロトコルに基づいて IP パッケージを監視するルール

IP パッケージ

このリンクをマウスでクリックすると、特別に定義した IP パッケージを許可するか拒否するかを決定できます。

IP アドレス

このリンクをマウスでクリックすると、ダイアログ ボックスが開き、必要な IP アドレスを入力できます。

IP マスク

このリンクをマウスでクリックすると、ダイアログ ボックスが開き、必要な IP マスクを入力できます。

プロトコル

このリンクをマウスでクリックすると、ダイアログ ボックスが開き、必要な IP プロトコルを入力できます。

レポート ファイル

このリンクをマウスでクリックすると、パッケージがルールに一致する場合に、レポート ファイルに書き込むかどうかを決定できます。

12.4.1.2. 送信ルール

送信ルールは、Avira FireWall による送信データ トラフィックの制御のために定義します。送信ルールは、次のいずれかのプロトコルに対して定義できます: IP、ICMP、UDP、TCP。

注意
パケットがフィルタされるとき、対応するルールが連続して適用されるため、ルールの順序は非常に重要です。内容を完全に把握している場合にのみ、ルールの順序を変更してください。

ボタン

ボタン	説明
追加	新しいルールを追加できます。このボタンを押すと、**[新規ルールの追加]** ダイアログ ボックスが開きます。このダイアログ ボックスで、新しいルールを選択できます。
削除	選択したルールを削除します。
優先度を下げる	選択したルールを 1 行下に移動します (つまり、ルールの優先度が下がります)。
優先度を上げる	選択したルールを 1 行上に移動します (つまり、ルールの優先度が上がります)。
名前の変更	選択したルールに別の名前を付けることができます。

注意
新しいルールは、アダプタごとに、またはコンピュータ上のすべてのアダプタに追加できます。すべてのアダプタにアダプタ ルールを追加するには、表示されているアダプタ階層から、**[コンピュータ]** を選択し、**[追加]** ボタンをクリックします。

注意
マウスでルールを目的の位置にドラッグしても、ルールの位置を変更できます。

12.4.2 アプリケーション ルール

ユーザー向けのアプリケーション ルール

このリストには、システム内のすべてのユーザーが含まれます。管理者としてログインしている場合は、ルールを適用するユーザーを選択できます。特権のあるユーザーでない場合は、現在ログオンしているユーザーしか表示できません。

アプリケーション リスト

このテーブルには、ルールが定義されるアプリケーションのリストが表示されます。アプリケーション リストには、Avira FireWall のインストール以降に実行され、ルールが保存されている各アプリケーションの設定が含まれます。

標準の表示

	説明
アプリケーション	アプリケーション名。
モード	選択したアプリケーション ルールのモードを表示します。**[フィルタ]** モードでは、アプリケーション ルールの実行後に、アダプタ ルールがチェックされ、実行されます。*[特権]* モードでは、アダプタ ルールが無視されます。リンクをクリックすると、異なるモードに切り替わります。
アクション	ネットワークの使用法のタイプにかかわらず、アプリケーションがネットワークを使用しているときに、Avira FireWall が自動的に実行するアクションを示します。このリンクをマウスでクリックすると、別のアクションのタイプに切り替えることができます。アクション タイプは、**[問い合わせ]**、**[許可]**、**[拒否]** のいずれかになります。**[問い合わせ]** が既定のアクションです。

拡張設定

アプリケーションのネットワーク アクセスに個別のルールが必要な場合は、アダプタ ルールの作成と同じように、パケット フィルタに基づくアプリケーション ルールを作成できます。拡張設定のアプリケーション ルールに変更するには、まずエキスパート モードをアクティブにする必要があります。FireWall::設定セクションで、設定するアプリケーション ルールを変更します。**[拡張設定]** オプションを有効にし、**[確認]** または **[OK]** をクリックして設定を保存します。ファイアウォール設定で、**[FireWall]::[アプリケーション ルール]** セクションを選択します。見出し *[フィルタ]* の追加の列、その下のエントリ *[簡易]* がアプリケーション ルールのリストに表示されます。これで、追加の **[フィルタ]::***[詳細] - [アクション]::[ルール] オプションを使用して、拡張設定を選択できます。*

	説明
アプリケーション	アプリケーション名。
モード	選択したアプリケーション ルールのモードを表示します。**[フィルタ]** モードでは、アプリケーション ルールの実行後に、アダプタ ルールがチェックされ、実行されます。*[特権]* モードでは、アダプタ ルールが無視されます。リンクをクリックすると、異なるモードに切り替わります。

アクション	ネットワークの使用法のタイプにかかわらず、アプリケーションがネットワークを使用しているときに、Avira FireWall が自動的に実行するアクションを示します。 *[フィルタ] - [簡易]* を選択した場合は、別のアクション タイプを選択するリンクをクリックできます。値は、**[問い合わせ]**、**[許可]** 、**[拒否]**、*[拡張]* のいずれかになります。 *[フィルタ] - [詳細]* を選択した場合は、*[ルール]* アクション タイプが表示されます。**[ルール]** リンクをクリックすると、**[アプリケーション ルール]** ウィンドウが開きます。このウィンドウで、アプリケーションに固有のルールを入力できます。
[フィルタ]	フィルタのタイプを表示します。このリンクのクリックにより、別のタイプのフィルタを選択できます。 *[簡易]*: 簡易フィルタの場合、ソフトウェア アプリケーションによって実行されたすべてのネットワーク アクティビティに対して、指定したアクションが実行されます。 *[詳細]*: このタイプのフィルタの場合、拡張設定に追加したルールが適用されます。

アプリケーションに固有のルールを 作成する場合は、*[フィルタ]*の下で **[詳細]** エントリを選択します。その後、*[ルール]* エントリが **[アクション]** 列に表示されます。**[ルール]** をクリックして、特定のアプリケーション ルールを作成するためのウィンドウを開きます。

拡張設定で指定したアプリケーション ルール

アプリケーション ルールの指定によって、アプリケーションの特定のデータ トラフィックを許可/拒否したり、個々のポートに対するパッシブなリッスンを許可/拒否したりすることができます。次のオプションがあります。

コード インジェクションを許可または拒否する

コード インジェクションとは、アクションを実行する別のプロセスのアドレス スペースにコードを取り込んで、このプロセスにダイナミック リンク ライブラリ (DLL) を読み込ませる手法です。コード インジェクションは、特に別のプログラムを偽装してコードを実行するマルウェアに使用されます。このような方法で、インターネットへのアクセスを FireWall に対して隠すことが可能です。既定のモードで、コード インジェクションは、すべての署名付きアプリケーションに対して許可されています。

アプリケーションのポートに対するパッシブ リッスンを許可または拒否する

データ トラフィックを許可または拒否する

受信/送信 IP パケットを許可または拒否する

受信/送信 TCP パケットを許可または拒否する

受信/送信 UDP パケットを許可または拒否する

アプリケーション ルールは各アプリケーションに対して必要な数だけ作成できます。 アプリケーション ルールは、表示されている順序で実行されます (詳細については、。

注意
アプリケーション ルールの *[詳細]* フィルタを変更した場合、既に拡張設定で作成されているアプリケーション ルールは非アクティブになるだけで、完全に削除されるわけではありません。*[詳細]* フィルタを再度選択した場合、既存のアプリケーション ルールが再度アクティブになり、アプリケーション ルール ウィンドウの拡張設定に表示されます。

アプリケーションの詳細

このボックスで、アプリケーション リスト ボックスで選択したアプリケーションの詳細を確認できます。

	説明
名前	アプリケーション名。
パス	実行可能ファイルへのフル パスです。

ボタン

ボタン	説明
アプリケーションの追加	新しいアプリケーション ルールを追加できます。このボタンを押すと、ダイアログ ボックスが開きます。ここで新しいルールの作成のために必要なアプリケーションを選択できます。
ルールの削除	選択したアプリケーション ルールを削除します。
再読み込み	アプリケーションのリストを再読み込みし、同時にアプリケーション ルールに対して直前に行われた変更を破棄します。

12.4.3 信頼済みプロバイダ

[信頼済みプロバイダ] には、信頼済みソフトウェア プロデューサのリストが表示されます。リストに対するプロデューサの追加と削除は、*[ネットワーク イベント]* ポップアップ ウィンドウの *[このプロバイダを常に信頼する]* オプションを使用して行うことができます。リストに登録されているプロバイダによって署名されているアプリケーションからのネットワーク アクセスを初期状態で許可するには、**[信頼済みプロバイダからのアプリケーションを自動的に許可する]** オプションを有効にします。

ユーザーに対して信頼済みのベンダ

このリストには、システム内のすべてのユーザーが含まれます。管理者としてログインしている場合は、どのユーザーの信頼済みプロバイダのリストを表示または更新するかを選択できます。特権のあるユーザーでない場合は、ログオンしているの現在ユーザーしか表示できません。

信頼済みベンダによって作成されたアプリケーションを自動的に許可

このオプションを有効にすると、既知の信頼済みプロバイダによって署名されたアプリケーションは、ネットワークへのアクセスが自動的に許可されます。このオプションは初期状態で有効に設定されています。

ベンダ

このリストには、"信頼済み" として分類されたすべてのプロバイダが表示されます。

ボタン

ボタン	説明
削除	ハイライト表示されたエントリを信頼済みプロバイダのリストから削除します。選択したプロバイダをリストから完全に削除するには、設定ウィンドウで **[確認]** または **[OK]** をクリックします。
再読み込み	変更内容が元に戻されます。前回保存したリストが読み込まれます。

注意

リストからプロバイダを削除した後、**[適用]** を選択した場合は、プロバイダがリストから完全に削除されます。*[再読み込み]* で変更を元に戻すことはできません。ただし、*[ネットワーク イベント]* ポップアップ ウィンドウの *[このプロバイダを常に信頼する]* オプションを使用して、信頼済みプロバイダのリストに再度プロバイダを追加することはできます。

注意

FireWall は、信頼済みプロバイダのリストにエントリを追加する前に、アプリケーション ルールの優先順位を付けます。アプリケーション ルールが既に作成されており、アプリケーション プロバイダが信頼済みプロバイダのリストに登録されている場合、そのアプリケーション ルールが実行されます。

12.4.4 設定

詳細オプション

FireWall を有効にする

このオプションを有効にすると、Avira FireWall が有効になり、インターネットおよびその他のネットワークから生じるリスクからコンピュータが保護されます。

起動時に Windows ファイアウォールを停止

このオプションを有効にすると、コンピュータを再起動したときに、Windows ファイアウォールが非アクティブになります。このオプションは初期状態で有効に設定されています。

Windows Host ファイルがロックされていない/ロックされている

このオプションを [ロックされています] に設定すると、Windows ホスト ファイルは書き込み保護されます。このファイルに対する操作は禁止されます。たとえば、マルウェアによる好ましくない Web サイトへのリダイレクトは不可能になります。このオプションは、初期状態で [ロックされていません] に設定されています。

ルールのタイムアウト

無期限にブロック

このオプションを有効にすると、ポート スキャン中などに自動的に作成されたルールが維持されます。

次の時間経過後にルールを削除

このオプションを有効にすると、ポート スキャン中などに自動的に作成されたルールは定義した時間の後、再び削除されます。このオプションは初期状態で有効に設定されています。

通知

[通知] では、どのようなイベントが発生したら、FireWall からデスクトップ通知を受け取るかを定義します。

ポート スキャン

このオプションを有効にすると、FireWall がポート スキャンを検出した場合にデスクトップ通知が表示されます。

フラディング

このオプションを有効にすると、FireWall がフラッド攻撃を検出した場合にデスクトップ通知が表示されます。

ブロックされたアプリケーション

このオプションを有効にすると、FireWall がアプリケーションのネットワーク アクティビティを拒否 (ブロック) した場合に、デスクトップ通知が表示されます。

ブロックされた IP アドレス

このオプションを有効にすると、FireWall が特定の IP アドレスからのデータ トラフィックを拒否 (ブロック) した場合に、デスクトップ通知が表示されます。

アプリケーション ルール

[アプリケーション ルール] オプションは、FireWall::アプリケーション ルール セクションで、アプリケーション ルールに対する設定オプションを設定するために使用されます。

詳細オプション

このオプションを有効にすると、アプリケーションによる各種のネットワーク アクセスを個別に制御できます。

基本設定

このオプションを有効にすると、アプリケーションによる各種のネットワーク アクセスに対し、1 つのアクションのみを設定できます。

12.4.5 ポップアップ設定

ポップアップ設定

プロセス起動スタックの検査

このオプションを有効にすると、プロセス スタック検査でより正確な制御が可能になります。FireWall は、スタック内の信頼できない任意のプロセスは、子プロセスを通じて実際にネットワークにアクセスしている可能性があると想定します。このため、プロセス スタックに信頼できないプロセスがあると、それぞれに対してさまざまなポップアップ ウィンドウが表示されます。このオプションは初期状態で無効に設定されています。

プロセスごとに複数のポップアップを許可

このオプションを有効にすると、アプリケーションがネットワーク接続を行うたびに、ポップアップ ウィンドウが表示されます。または、最初の接続の試行時にのみ通知されるようにできます。このオプションは初期状態で無効に設定されています。

ゲーム モードでのポップアップ通知を自動的に無効化

このオプションを有効にした場合、使用しているコンピュータ システム上で、アプリケーションを全画面表示モードで実行すると、Avira FireWall のゲーム モードが自動的にアクティブになります。ゲーム モードでは、定義されたすべてのアダプタ ルールとアプリケーション ルールが適用されます。"*[許可]*" または "*[拒否]*" のアクションを指定したルールが定義されていないアプリケーションも一時的にネットワークへのアクセスが許可され、対応するネットワーク イベントについて確認するポップアップ ウィンドウは表示されません。

このアプリケーションに対するアクションを記憶

常に有効

このオプションを有効にすると、"**[ネットワーク イベント]**" ダイアログ ボックスの "**[このアプリケーションに対するアクションを記憶]**" オプションは初期状態で有効になります。このオプションは初期状態で有効に設定されています。

常に無効

このオプションを有効にすると、"**[ネットワーク イベント]**" ダイアログ ボックスの "**[このアプリケーションに対するアクションを記憶]**" オプションは初期状態で無効になります。

署名付きアプリケーションを許可

このオプションを有効にすると、"**[ネットワーク イベント]**" ダイアログ ボックスの "**[このアプリケーションに対するアクションを記憶]**" オプションは、署名付きアプリケーションによるネットワーク アクセス中に自動的に有効になります。メーカーは、Microsoft、Mozilla、Opera、Yahoo、Google、Hewlet Packard、Sun、Skype、Adobe、Lexmark、Creative Labs、ATI、nVidia です。

最終使用状況を記憶

このオプションを有効にすると、"**[ネットワーク イベント]**" ダイアログ ボックスの "**[このアプリケーションに対するアクションを記憶]**" オプションは、前のネットワーク イベントに対してと同じく有効になります。"**[このアプリケーションに対するアクションを記憶]**" オプションを有効にすると、次のネットワーク イベントでこのオプションが有効になります。前のネットワーク イベントに対して "**[このアプリケーションに対するアクションを記憶]**" オプションを無効にしていた場合、そのオプションは次のネットワーク イベントに対しても無効になります。

詳細の表示

この設定オプションのグループで、**[ネットワーク イベント]** ウィンドウの詳細情報の表示をセットアップできます。

詳細データの表示 (オンデマンド)

このオプションを有効にすると、詳細情報は要求時のみ、"*[ネットワーク イベント]*" ウィンドウに表示されます。つまり、詳細情報は、"*[ネットワーク イベント]*" ウィンドウで "**[詳細の表示]**" ボタンをクリックしたときのみ表示されます。

詳細データを常に表示

このオプションを有効にすると、詳細情報は常に、"*[ネットワーク イベント]*" ウィンドウに表示されます。

最終使用状況を記憶

このオプションを有効にすると、詳細情報の表示は、前のネットワーク イベントに対してと同じく管理されます。前のネットワーク イベント中に詳細情報を表示するか、詳細情報にアクセスすると、詳細情報は次のネットワーク イベントに対して表示されます。詳細情報を非表示にしていて、前のネットワーク イベント中に表示しなかった場合、次のネットワーク イベントに対して詳細情報は表示されません。

特権を許可

この設定オプションのグループで、**[ネットワーク イベント]** ウィンドウの *[特権を許可]* オプションの状態を定義できます。

常に有効

このオプションを有効にすると、"*[ネットワーク イベント]*" ウィンドウの "*[特権を許可]*" オプションが初期状態で有効になります。

常に無効

このオプションを有効にすると、"*[ネットワーク イベント]*" ウィンドウの "*[特権を許可]*" オプションが初期状態で無効になります。

最終使用状況を記憶

このオプションを有効にすると、"*[特権を許可]*" オプションの状態は "*[ネットワーク イベント]*" ウィンドウ内の前のネットワーク イベントに対してと同じく制御されます。前のネットワーク イベントの実行に対して "*[特権を許可]*" オプションを有効にしている場合、そのオプションは次のネットワーク イベントに対して初期状態で有効になります。前のネットワーク イベントの実行に対して "*[特権を許可]*" オプションを無効にしている場合、そのオプションは次のネットワーク イベントに対して初期状態で無効になります。

12.5 SMC 内のファイアウォール

FireWall を管理に固有の要件を満たすように設定します。この設定は Avira Security Management Center を通じて行います。拡張オプションおよび制限は設定オプションごとに用意されています。

- FireWall 設定はクライアント コンピュータのすべてのユーザーに適用されます。
- アダプタ ルール: 個々のアダプタのセキュリティ レベルはコンテキスト メニューを使用して設定できます。
- アプリケーション ルール : アプリケーションによるネットワーク アクセスを許可するか拒否するかを設定できます。独自のアプリケーション ルールを作成する方法はありません。

AntiVir プログラムを Avira Security Management Center で管理する場合は、クライアント コンピュータ上のコントロール センターで次の FireWall 設定オプションが無効になります。

- FireWall のセキュリティ レベルの設定
- アダプタおよびアプリケーション ルールの設定

12.5.1 全般設定

詳細オプション

Windows ホスト ファイルをロック

このオプションが有効になっている場合、Windows Host ファイルは書き込み保護されます。このファイルに対する操作は禁止されます。たとえば、マルウェアによる好ましくない Web サイトへのリダイレクトは不可能になります。

ゲーム モードを有効にする

このオプションを有効にした場合、使用しているコンピュータ システム上で、アプリケーションを全画面表示モードで実行すると、Avira FireWall のゲーム モードが自動的にアクティブになります。ゲーム モードでは、定義されたすべてのアダプタ ルールとアプリケーション ルールが適用されます。"*[許可]*" または "*[拒否]*" のアクションを指定したルールが定義されていないアプリケーションも一時的にネットワークへのアクセスが許可され、対応するネットワーク イベントについて確認するポップアップ ウィンドウは表示されません。

起動時に Windows FireWall を停止

このオプションを有効にすると、コンピュータを再起動したときに、Windows FireWall が非アクティブになります。このオプションは初期状態で有効に設定されています。

FireWall を有効にする

このオプションを有効にすると、Avira FireWall が有効になり、インターネットおよびその他のネットワークから生じるリスクからコンピュータが保護されます。

ルールのタイムアウト

無期限にブロック

このオプションを有効にすると、ポート スキャン中などに自動的に作成されたルールが維持されます。

次の時間経過後にルールを削除

このオプションを有効にすると、ポート スキャン中などに自動的に作成されたルールは定義した時間の後、再び削除されます。このオプションは初期状態で有効に設定されています。

12.5.2 全般アダプタ ルール

設定済みのネットワーク接続をアダプタに指定できます。アダプタ ルールを以下のクライアント ネットワーク接続について作成できます。

- 既定のアダプタ: LAN または高速インターネット
- ワイヤレス
- ダイヤルアップ接続

アダプタのコンテキスト メニューから、以下の使用可能なアダプタについて、事前に定義済みのアダプタ ルールを指定できます。

- セキュリティ レベル - 高
- セキュリティ レベル - 中
- セキュリティ レベル - 低

独自の要件に合わせて個々のアダプタ ルールを変更するオプションもあります。

注意
Avira FireWall のすべての事前に設定済みのルールに対する既定のセキュリティ レベル設定は、**[中]** です。

ICMP プロトコル

インターネット制御メッセージ プロトコル (ICMP) は、ネットワーク上でのエラー メッセージや情報メッセージの交換に使用されます。このプロトコルは、ping または tracer のステータス メッセージにも使用されます。
このルールを使用すると、受信および送信ブロック メッセージ タイプ、フラッディングの場合の動作、断片化した ICMP パケットへの対応を定義できます。このルールは、ICMP flood 攻撃の防止に役立ちます。この攻撃を受けたコンピュータはすべてのパケットに応答することになるため、そのコンピュータの CPU の負荷が増大します。

ICMP プロトコルの事前に設定済みのルール

設定: 低	設定: 中	設定: 高
受信ブロック タイプ: **タイプなし**。 送信ブロック タイプ: **タイ**	これは低レベルと同じルールです。	受信ブロック タイプ: **複数のタイプ** 送信ブロック タイプ: **複数**

プなし。 パケット間の遅延が **50** ミリ秒未満の場合、フラッディングを想定します。 断片化した ICMP パケットを**拒否**します。		のタイプ パケット間の遅延が **50** ミリ秒未満の場合、フラッディングを想定します。 断片化した ICMP パケットを**拒否**します。

受信ブロック タイプ: タイプなし/複数のタイプ

このリンクをマウスでクリックすると、ICMP パケット タイプのリストが表示されます。このリストから、ブロックする受信 ICMP メッセージ タイプを指定できます。

送信ブロック タイプ: タイプなし/複数のタイプ

このリンクをマウスでクリックすると、ICMP パケット タイプのリストが表示されます。このリストから、ブロックする送信 ICMP メッセージ タイプを選択できます。

フラディング

このリンクをマウスでクリックすると、ダイアログ ボックスが表示され、最大許容 ICMPA 遅延を入力できます。

断片化した ICMP パケット

このリンクをマウスでクリックすると、断片化した ICMP パケットを拒否するかしないかを選択できます。

TCP ポート スキャン

このルールを使用すると、FireWall によって TCP ポート スキャンが想定される場合、およびその場合に何を実行するかを定義できます。このルールは、TCP ポート スキャン攻撃の防止に役立ちます。この攻撃を受けたコンピュータでは、開いたままの TCP ポートが検出されます。この種の攻撃は、コンピュータの弱点の検索に使用され、その後、さらに危険な攻撃タイプが続く場合もよくあります。

TCP ポート スキャンの事前に設定済みのルール

設定: 低	設定: 中	設定: 高
50 以上のポートが **5,000** ミリ秒でスキャンされた場合、TCP ポート スキャンを想定します。 検出されたとき、攻撃者の IP を**記録**し、攻撃をブロックするルールは**追加しません**。	**50** 以上のポートが **5,000** ミリ秒でスキャンされた場合、TCP ポート スキャンを想定します。 検出されたとき、攻撃者の IP を**ログ**し、攻撃をブロックするルールを**追加**します。	中レベルと同じルール。

ポート

このリンクをマウスでクリックすると、ダイアログ ボックスが表示されます。このダイアログ ボックスに入力したポート数がスキャンされた場合、TCP ポート スキャンを想定します。

ポート スキャン時間枠

このリンクをマウスでクリックすると、ダイアログ ボックスが表示されます。このダイアログ ボックスに入力したポート スキャンの時間枠内に一定数のポート スキャンが実行された場合、TCP ポート スキャンを想定します。

レポート ファイル

このリンクをマウスでクリックすると、攻撃者の IP アドレスを記録するかしないかを選択できます。

ルール

このリンクをマウスでクリックすると、TCP ポート スキャン攻撃をブロックするルールを追加するかしないかを選択できます。

UDP ポート スキャン

このルールを使用すると、FireWall によって UDP ポート スキャンが想定される場合、およびその場合に何を実行するかを定義できます。このルールにより、UDP ポート スキャン攻撃を防止できます。この攻撃を受けると、コンピュータで開いている UDP ポートが検出されます。この種の攻撃は、コンピュータの弱点の検索に使用され、その後、さらに危険な攻撃タイプが続く場合もよくあります。

UDP ポート スキャンの事前に設定済みのルール

設定: 低	設定: 中	設定: 高
50 以上のポートが **5,000** ミリ秒でスキャンされた場合、UDP ポート スキャンを想定します。 検出されたとき、攻撃者の IP を**記録**し、攻撃をブロックするルールは**追加しません**。	**50** 以上のポートが **5,000** ミリ秒でスキャンされた場合、UDP ポート スキャンを想定します。 検出されたとき、攻撃者の IP を**ログ**し、攻撃をブロックするルールを**追加**します。	中レベルと同じルール。

ポート

このリンクをマウスでクリックすると、ダイアログ ボックスが表示されます。このダイアログ ボックスに入力したポート数がスキャンされた場合、UDP ポート スキャンを想定します。

ポート スキャン時間枠

このリンクをマウスでクリックすると、ダイアログ ボックスが表示されます。このダイアログ ボックスに入力したポート スキャンの時間枠内に一定数のポート スキャンが実行された場合、UDP ポート スキャンを想定します。

レポート ファイル

このリンクをマウスでクリックすると、攻撃者の IP アドレスを記録するかしないかを選択できます。

ルール

このリンクをマウスでクリックすると、UDP ポート スキャン攻撃をブロックするルールを追加するかしないかを選択できます。

12.5.2.1. 受信ルール

受信ルールは、Avira FireWall による受信トラフィックの制御のために定義します。

注意
パケットがフィルタされるとき、対応するルールが連続して適用されるため、ルールの順序は非常に重要です。内容を完全に把握している場合にのみ、ルールの順序を変更してください。

TCP データ トラフィック データ モニタの事前に設定済みのルール

設定: 低	設定: 中	設定: 高
Avira FireWall は受信データ トラフィックをブロックしません。	– ポート 135 上の TCP 接続確立を許可 **次の TCP パケットを許可する:** アドレス **0.0.0.0**、マスク **0.0.0.0**、ローカル ポート **{135}**、リモート ポート **{0-65535}**。 **既存の接続のパケット**に適用する。 パケットがルールに一致するときは記録しない。 詳細: 次のパケットを破棄する: **<empty>**、マスク **<empty>**、オフセット **0**。 – 135 の TCP パケットを拒否 次の TCP パケットを拒否する : アドレス **0.0.0.0**、マスク **0.0.0.0**、ローカル ポート **{135}**、リモー	– 確立された TCP データ トラフィックを監視 **次の TCP パケットを拒否する:** アドレス **0.0.0.0**、マスク **0.0.0.0**、ローカル ポート **{0-65535}**、リモート ポート **{0-65535}**。 **既存の接続のパケット**に適用する。 パケットがルールに一致するときは記録しない。 詳細: 次のパケットを破棄する: **<empty>**、マスク **<empty>**、オフセット **0**。

	トポート **{0-65535}**。 すべてのパケットに適用する。 パケットがルールに一致するときは記録しない。 詳細: 次のパケットを破棄する: **<empty>**、マスク **<empty>**、オフセット **0**。 – TCP 正常データトラフィックを監視 次の **TCP** パケットを拒否する: アドレス **0.0.0.0**、マスク **0.0.0.0**、ローカルポート **{0-65535}**、リモートポート **{0-65535}**。 接続開始と既存接続のパケットに適用する。 パケットがルールに一致するときは記録しない。 詳細: 次のパケットを破棄する: **<empty>**、マスク **<empty>**、オフセット **0**。 – すべての TCP パケットを拒否 次の **TCP** パケットを拒否する: アドレス **0.0.0.0**、マスク **0.0.0.0**、	

	ローカル ポート **{0-65535}**、リモート ポート **{0-65535}**。 **すべてのパケット**に適用する。 パケットがルールに一致するときは記録しない。 詳細: 次のパケットを破棄する: **<empty>**、マスク **<empty>**、オフセット **0**。	

TCP パケットを許可/拒否

このリンクをマウスでクリックすると、特別に定義した受信 TCP パケットを許可するか拒否するかを選択できます。

IP アドレス

このリンクをマウスでクリックすると、ダイアログ ボックスが開き、必要な IP アドレスを入力できます。

IP マスク

このリンクをマウスでクリックすると、ダイアログ ボックスが開き、必要な IP マスクを入力できます。

ローカル ポート

このリンクをマウスでクリックすると、ダイアログ ボックスが表示され、ローカル ポート番号、またはポートの全範囲を定義できます。

リモート ポート

このリンクをマウスでクリックすると、ダイアログ ボックスが表示され、リモート ポート番号、またはポートの全範囲を定義できます。

適用方法

このリンクをマウスでクリックすると、接続開始と既存接続のパケットに対して、既存接続のパケットに対してのみ、またはすべてのパケットに対して、ルールを適用するかを選択できます。

レポート ファイル

このリンクをマウスでクリックすると、パッケージがルールに一致する場合に、レポート ファイルに書き込むかどうかを決定できます。

詳細機能を使用するとコンテンツ フィルタを有効にできます。たとえば、特定のオフセットで特定のデータを含むパケットを拒否できます。このオプションを使用しない場合は、ファイルを選択しないか空のファイルを選択してください。

フィルタ対象のコンテンツ: データ

このリンクをマウスでクリックすると、ダイアログ ボックスが表示され、特定のバッファを含むファイルを選択できます。

フィルタ対象のコンテンツ: マスク

このリンクをマウスでクリックすると、ダイアログ ボックスが表示され、特定のマスクを選択できます。

フィルタ対象のコンテンツ: オフセット

このリンクをマウスでクリックすると、ダイアログ ボックスが表示され、フィルタ対象のコンテンツのオフセットを定義できます。オフセットは、TCP ヘッダーの終了位置から計算されます。

UDP トラフィック データ モニタの事前に設定済みのルール

設定: 低	設定: 中	設定: 高
-	– 許可された UDP データ トラフィックを監視 **次の UDP パケットを許可する:** アドレス **0.0.0.0**、マスク **0.0.0.0**、ローカル ポート **{0- 66535}**、リモート ポート **{0-66535}**。**開いたままのポート**にルールを適用する。パケットがルールに一致するときは記録しない。詳細: 次のパケットを破棄する: **<empty>**、マスク **<empty>**、オフセット **0**。 – すべての UDP パケットを拒否 次の **UDP パケット**を拒否する: アドレス **0.0.0.0**、マスク **0.0.0.0**、ローカル ポート	確立された UDP トラフィックを監視 次の **UDP パケット**を許可: アドレス **0.0.0.0**、マスク **0.0.0.0** (ローカル ポートの範囲が **{0-65535}** で、リモート ポートの範囲が **{53, 67, 68, 123}** の場合)。**開いたままのポート**にルールを適用する。パケットがルールに一致するときは記録しない。詳細: 次のパケットを破棄する: **<empty>**、マスク **<empty>**、オフセット **0**。

	{0-65535}、リモート ポート **{0-65535}**。 **すべてのポート**に適用する。 パケットがルールに一致するときは記録しない。 詳細: 次のパケットを破棄する: **<empty>**、マスク **<empty>**、オフセット **0**。	

UDP パケットを許可/拒否

このリンクをマウスでクリックすると、特別に定義した受信 UDP パケットを許可するか拒否するかを選択できます。

IP アドレス

このリンクをマウスでクリックすると、ダイアログ ボックスが開き、必要な IP アドレスを入力できます。

IP マスク

このリンクをマウスでクリックすると、ダイアログ ボックスが開き、必要な IP マスクを入力できます。

ローカル ポート

このリンクをマウスでクリックすると、ダイアログ ボックスが表示され、ローカル ポート番号、またはポートの全範囲を定義できます。

リモート ポート

このリンクをマウスでクリックすると、ダイアログ ボックスが表示され、リモート ポート番号、またはポートの全範囲を定義できます。

適用方法

このリンクをマウスでクリックすると、このルールをすべてのポートに適用するか、オープンしたすべてのポートに適用するかを選択できます。

レポート ファイル

このリンクをマウスでクリックすると、パッケージがルールに一致する場合に、レポート ファイルに書き込むかどうかを決定できます。

詳細機能を使用するとコンテンツ フィルタを有効にできます。たとえば、特定のオフセットで特定のデータを含むパケットを拒否できます。このオプションを使用しない場合は、ファイルを選択しないか空のファイルを選択してください。

フィルタ対象のコンテンツ: データ

このリンクをマウスでクリックすると、ダイアログ ボックスが表示され、特定のバッファを含むファイルを選択できます。

フィルタ対象のコンテンツ: マスク

このリンクをマウスでクリックすると、ダイアログ ボックスが表示され、特定のマスクを選択できます。

フィルタ対象のコンテンツ: オフセット

このリンクをマウスでクリックすると、ダイアログ ボックスが表示され、フィルタ対象のコンテンツのオフセットを定義できます。オフセットは、UDP ヘッダーの終了位置から計算されます。

ICMP トラフィック データ モニタの事前に設定済みのルール

設定: 低	設定: 中	設定: 高
-	– IP アドレスに基づいて ICMP を破棄しない **次の ICMP パケットを許可する**: アドレス **0.0.0.0**、マスク **0.0.0.0**。 パケットがルールに一致するときは記録しない。 詳細: 次のパケットを破棄する: **<empty>**、マスク **<empty>**、オフセット **0**。	中レベルと同じルール。

ICMP パケットを許可/拒否

このリンクをマウスでクリックすると、特別に定義した受信 ICMP パケットを許可するか拒否するかを選択できます。

IP アドレス

このリンクをマウスでクリックすると、ダイアログ ボックスが開き、必要な IP アドレスを入力できます。

IP マスク

このリンクをマウスでクリックすると、ダイアログ ボックスが開き、必要な IP マスクを入力できます。

レポート ファイル

このリンクをマウスでクリックすると、パッケージがルールに一致する場合に、レポート ファイルに書き込むかどうかを決定できます。

詳細機能を使用するとコンテンツ フィルタを有効にできます。たとえば、特定のオフセットで特定のデータを含むパケットを拒否できます。このオプションを使用しない場合は、ファイルを選択しないか空のファイルを選択してください。

フィルタ対象のコンテンツ: データ

このリンクをマウスでクリックすると、ダイアログ ボックスが表示され、特定のバッファを含むファイルを選択できます。

フィルタ対象のコンテンツ: マスク

このリンクをマウスでクリックすると、ダイアログ ボックスが表示され、特定のマスクを選択できます。

フィルタ対象のコンテンツ: オフセット

このリンクをマウスでクリックすると、ダイアログ ボックスが表示され、フィルタ対象のコンテンツのオフセットを定義できます。オフセットは、ICMP ヘッダーの終了位置から計算されます。

IP パケットの事前に設定済みのルール

設定: 低	設定: 中	設定: 高
-	-	すべての IP パケットを拒否 次の **IP パケット**を拒否する: アドレス **0.0.0.0**、マスク **0.0.0.0**。 パケットがルールに一致するときは記録しない。

IP パケットを許可/拒否

このリンクをマウスでクリックすると、特別に定義した IP パッケージを許可するか拒否するかを決定できます。

IP アドレス

このリンクをマウスでクリックすると、ダイアログ ボックスが開き、必要な IP アドレスを入力できます。

IP マスク

このリンクをマウスでクリックすると、ダイアログ ボックスが開き、必要な IP マスクを入力できます。

レポート ファイル

このリンクをマウスでクリックすると、パッケージがルールに一致する場合に、レポート ファイルに書き込むかどうかを決定できます。

IP プロトコルに基づいて IP パッケージを監視するルール

IP パッケージ

このリンクをマウスでクリックすると、特別に定義した IP パッケージを許可するか拒否するかを決定できます。

IP アドレス

このリンクをマウスでクリックすると、ダイアログ ボックスが開き、必要な IP アドレスを入力できます。

IP マスク

このリンクをマウスでクリックすると、ダイアログ ボックスが開き、必要な IP マスクを入力できます。

プロトコル

このリンクをマウスでクリックすると、ダイアログ ボックスが開き、必要な IP プロトコルを入力できます。

レポート ファイル

このリンクをマウスでクリックすると、パッケージがルールに一致する場合に、レポート ファイルに書き込むかどうかを決定できます。

12.5.2.2. 送信ルール

送信ルールは、Avira FireWall による送信データ トラフィックの制御のために定義します。送信ルールは、次のいずれかのプロトコルに対して定義できます: IP、ICMP、UDP、TCP。

注意
パケットがフィルタされるとき、対応するルールが連続して適用されるため、ルールの順序は非常に重要です。内容を完全に把握している場合にのみ、ルールの順序を変更してください。

ボタン

ボタン	説明
追加	新しいルールを追加できます。このボタンを押すと、**[新規ルールの追加]** ダイアログ ボックスが開きます。このダイアログ ボックスで、新しいルールを選択できます。
削除	選択したルールを削除します。
優先度を下げる	選択したルールを 1 行下に移動します (つまり、ルールの優先度が下がります)。
優先度を上げる	選択したルールを 1 行上に移動します (つまり、ルールの優先度が上がります)。
名前の変更	選択したルールに別の名前を付けることができます。

注意
新しいルールは、アダプタごとに、またはコンピュータ上のすべてのアダプタに追加できます。すべてのアダプタにアダプタ ルールを追加するには、表示されているアダプタ階層から、**[コンピュータ]** を選択し、**[追加]** ボタンをクリックします。

注意
マウスでルールを目的の位置にドラッグしても、ルールの位置を変更できます。

12.5.3 アプリケーション リスト

アプリケーション リストを使用して、アプリケーションがどのようにネットワークにアクセスするかを指定するルールを作成できます。リストにアプリケーションを追加した後、コンテキスト メニューを使用して、選択したアプリケーションについて *[許可]* と **[ブロック]** のルールを設定できます。

- *[許可]* ルールを設定したアプリケーションによるネットワークへのアクセスは許可されます。
- *[ブロック]* ルールを設定したアプリケーションによるネットワークへのアクセスは拒否されます。

アプリケーションの追加時、*[許可]* ルールを設定します。

アプリケーション リスト

このテーブルには、ルールが定義されるアプリケーションのリストが表示されます。記号は、アプリケーションによるネットワーク アクセスが許可されるか拒否されるかを示します。アプリケーションに関するルールはコンテキスト メニューを使用して変更できます。

ボタン

ボタン	説明
パスを使用して追加	このボタンをクリックすると、アプリケーションを選択できるダイアログ ボックスが開きます。 選択したアプリケーションは、"**ネットワーク アクセスを許可**" ルールを設定したアプリケーション リストに追加されます。"**[パスを使用して追加]**" オプションを使用した場合、追加される FireWall アプリケーションがパスおよびファイル名により識別されます。 追加された実行可能ファイルの内容が更新などにより変更された場合でも、アプリケーションのルールは有効なままであり、FireWall により使用されます。
MD5 を使用して追加	このボタンをクリックすると、アプリケーションを選択できるダイアログ ボックスが開きます。 選択したアプリケーションは、"**ネットワーク アクセスを許可**" ルールを設定したアプリケーション リストに追加されます。オプション ""**[MD5 を使用した追加]**" を使用した場合、追加したすべてのアプリケーションは MD5 チェックサムを使用して一意に識別されます。これにより、FireWall でファイル内容の変更を識別できます。たとえば、更新後にアプリケーションに変更があった場合、そのアプリケーションと該当するルールはアプリケーション リストから自動的に削除されます。変更後、アプリケーションをリストに再度追加する必要があります。その後、必要なルールが再度適用されます。
グルー	このボタンをクリックすると、ディレクトリを選択できるダイ

プの追加	アログ ボックスが開きます。選択したパスにあるすべてのアプリケーションは、"**ネットワーク アクセスの許可**" ルールを設定したアプリケーション リストに追加されます。
削除	選択したアプリケーション ルールが削除されます。
すべての削除	すべてのアプリケーション ルールが削除されます。

12.5.4 信頼済みプロバイダ

[信頼済みプロバイダ] には、信頼済みソフトウェア プロデューサのリストが表示されます。このリストに表示されているソフトウェア メーカーのアプリケーションは、ネットワークへのアクセスを許可されます。リストからメーカーを追加および削除できます。

ベンダ

このリストには、"信頼済み" として分類されたすべてのプロバイダが表示されます。

ボタン

ボタン	説明
追加	このボタンをクリックすると、アプリケーションを選択できるダイアログ ボックスが開きます。 選択したアプリケーションのメーカーは信頼され、信頼済みプロバイダのリストに追加されます。
グループの追加	このボタンをクリックすると、ディレクトリを選択できるダイアログ ボックスが開きます。 選択したパスにあるすべてのアプリケーションのメーカーは信頼され、信頼済みプロバイダのリストに追加されます。
削除	ハイライト表示されたエントリを信頼済みプロバイダのリストから削除します。選択したプロバイダをリストから完全に削除するには、設定ウィンドウで "**[確認]**" または "**[OK]**" をクリックします。
すべての削除	すべてのエントリは信頼済みプロバイダのリストから削除されます。
再読み込み	変更内容が元に戻されます。前回保存したリストが読み込まれます。

注意
リストからプロバイダを削除した後、**[適用]** を選択した場合は、プロバイダがリストから完全に削除されます。*[再読み込み]* で変更を元に戻すことはできません。

注意
FireWall は、信頼済みプロバイダのリストにエントリを追加する前に、アプリケーション ルールの優先順位を付けます。アプリケーション ルールが既に作成されており、アプリケーション プロバイダが信頼済みプロバイダのリストに登録されている場合、そのアプリケーション ルールが実行されます。

12.5.5 その他の設定

通知

[通知] では、どのようなイベントが発生したら、FireWall からデスクトップ通知を受け取るかを定義します。

ポート スキャン

このオプションを有効にすると、FireWall がポート スキャンを検出した場合にデスクトップ通知が表示されます。

フラディング

このオプションを有効にすると、FireWall がフラッド攻撃を検出した場合にデスクトップ通知が表示されます。

ブロックされたアプリケーション

このオプションを有効にすると、FireWall がアプリケーションのネットワーク アクティビティを拒否 (ブロック) した場合に、デスクトップ通知が表示されます。

ブロックされた IP アドレス

このオプションを有効にすると、FireWall が特定の IP アドレスからのデータ トラフィックを拒否 (ブロック) した場合に、デスクトップ通知が表示されます。

ポップアップ設定

プロセス起動スタックの検査

このオプションを有効にすると、プロセス スタック検査でより正確な制御が可能になります。FireWall は、スタック内の信頼できない任意のプロセスは、子プロセスを通じて実際にネットワークにアクセスしている可能性があると想定します。このため、プロセス スタックに信頼できないプロセスがあると、それぞれに対してさまざまなポップアップ ウィンドウが表示されます。このオプションは初期状態で無効に設定されています。

プロセスごとに複数のポップアップを許可

このオプションを有効にすると、アプリケーションがネットワーク接続を行うたびに、ポップアップ ウィンドウが表示されます。または、最初の接続の試行時にのみ通知されるようにできます。このオプションは初期状態で無効に設定されています。

ゲーム モードでのポップアップ通知を自動的に無効化

このオプションを有効にした場合、使用しているコンピュータ システム上で、アプリケーションを全画面表示モードで実行すると、Avira FireWall のゲーム モードが自動的にアクティブになります。ゲーム モードでは、定義されたすべてのアダプタ ルールとアプリケーション ルールが適用されます。"*[許可]*" または "*[拒否]*" のアクションを指定したルールが定義されていないアプリケーションも一時的にネットワークへのアクセスが許可され、対応するネットワーク イベントについて確認するポップアップ ウィンドウは表示されません。

12.5.6 表示設定

このアプリケーションに対するアクションを記憶

常に有効

このオプションを有効にすると、"**[ネットワーク イベント]**" ダイアログ ボックスの "**[このアプリケーションに対するアクションを記憶]**" オプションは初期状態で有効になります。このオプションは初期状態で有効に設定されています。

常に無効

このオプションを有効にすると、"**[ネットワーク イベント]**" ダイアログ ボックスの "**[このアプリケーションに対するアクションを記憶]**" オプションは初期状態で無効になります。

署名付きアプリケーションを許可

このオプションを有効にすると、"**[ネットワーク イベント]**" ダイアログ ボックスの "**[このアプリケーションに対するアクションを記憶]**" オプションは、署名付きアプリケーションによるネットワーク アクセス中に自動的に有効になります。メーカーは、Microsoft、Mozilla、Opera、Yahoo、Google、Hewlet Packard、Sun、Skype、Adobe、Lexmark、Creative Labs、ATI、nVidia です。

最終使用状況を記憶

このオプションを有効にすると、"**[ネットワーク イベント]**" ダイアログ ボックスの "**[このアプリケーションに対するアクションを記憶]**" オプションは、前のネットワーク イベントに対してと同じく有効になります。"**[このアプリケーションに対するアクションを記憶]**" オプションを有効にすると、次のネットワーク イベントでこのオプションが有効になります。前のネットワーク イベントに対して "**[このアプリケーションに対するアクションを記憶]**" オプションを無効にしていた場合、そのオプションは次のネットワーク イベントに対しても無効になります。

詳細の表示

この設定オプションのグループで、**[ネットワーク イベント]** ウィンドウの詳細情報の表示をセットアップできます。

詳細データの表示 (オンデマンド)

このオプションを有効にすると、詳細情報は要求時のみ、"*[ネットワーク イベント]*" ウィンドウに表示されます。つまり、詳細情報は、"*[ネットワーク イベント]*" ウィンドウで "**[詳細の表示]**" ボタンをクリックしたときのみ表示されます。

詳細データを常に表示

このオプションを有効にすると、詳細情報は常に、"*[ネットワーク イベント]*" ウィンドウに表示されます。

最終使用状況を記憶

このオプションを有効にすると、詳細情報の表示は、前のネットワーク イベントに対してと同じく管理されます。前のネットワーク イベント中に詳細情報を表示するか、詳細情報にアクセスすると、詳細情報は次のネットワーク イベントに対して表示されます。詳細情報を非表示にしていて、前のネットワーク イベント中に表示しなかった場合、次のネットワーク イベントに対して詳細情報は表示されません。

特権を許可

この設定オプションのグループで、**[ネットワーク イベント]** ウィンドウの *[特権を許可]* オプションの状態を定義できます。

常に有効

このオプションを有効にすると、"*[ネットワーク イベント]*" ウィンドウの "*[特権を許可]*" オプションが初期状態で有効になります。

常に無効

このオプションを有効にすると、"*[ネットワーク イベント]*" ウィンドウの "*[特権を許可]*" オプションが初期状態で無効になります。

最終使用状況を記憶

このオプションを有効にすると、"*[特権を許可]*" オプションの状態は "*[ネットワーク イベント]*" ウィンドウ内の前のネットワーク イベントに対してと同じく制御されます。前のネットワーク イベントの実行に対して *[特権を許可]* オプションを有効にしている場合、そのオプションは次のネットワーク イベントに対して初期状態で有効になります。前のネットワーク イベントの実行に対して *[特権を許可]* オプションを無効にしている場合、そのオプションは次のネットワーク イベントに対して初期状態で無効になります。

12.6 WebGuard

WebGuard の設定には、設定の [WebGuard] セクションを使用します。

12.6.1 スキャン

WebGuard では、インターネットから Web ブラウザに読み込んだ Web ページに潜むウイルスやマルウェアの攻撃からコンピュータを保護します。*[スキャン]* を使用して、WebGuard コンポーネントの動作を設定できます。

スキャン

WebGuard を有効にする(W)

このオプションを有効にすると、インターネット ブラウザを使用して要求された Web ページに対してウイルスとマルウェアのスキャンが実行されます。
WebGuard は、ポート 80、8080、3128 で HTTP プロトコルを使用してインターネットで転送されるデータを監視します。感染した Web ページが検出されると、その Web ページの読み込みがブロックされます。このオプションを無効にすると、WebGuard サービスは開始されますが、ウイルスおよびマルウェアのスキャンは無効になります。

ドライブバイ対策

ドライブバイ対策により、I-Frame (インライン フレームとも呼ばれます) をブロックするように設定できます。I-Frame は HTML 要素であり、Web ページの領域を区切るインターネット ページの要素です。I-Frame を使用して、さまざまな Web コンテンツ (通常は他の URL) をブラウザのサブウィンドウに独立したドキュメントとして読み込み、表示することができます。I-Frame は、ほとんどの場合はバナー広告に使用されます。ただし、I-Frame がマルウェアを隠すために使用されることがあります。その場合、ブラウザ内で I-Frame の領域は見えないようにされています。[*不審な I-Frame をブロックする*] オプションをオンにすると、I-Frame の読み込みをブロックできます。

不審 I フレームのブロック

このオプションを有効にすると、要求した Web ページの I-Frame が特定の条件に基づいてスキャンされます。要求された Web ページに不審な I-Frame がある場合、I-Frame はブロックされます。I-Frame ウィンドウにエラー メッセージが表示されます。

既定

このオプションを有効にすると、不審なコンテンツを含む I-Frame はブロックされます。

詳細

このオプションを有効にすると、不審なコンテンツを含む I-Frame および不審な方法で使用されている I-Frame はブロックされます。I-Frame の使用が疑わしいと見なされるのは、I-Frame が非常に小さく、そのために非表示になっている場合、または I-Frame が Web ページの通常とは異なる位置に配置されて I-Frame がブラウザ内でほとんど非表示になっている場合です。

12.6.1.1. 検出時のアクション

検出時のアクション

ウイルスまたは不要プログラムが検出された場合に、WebGuard が実行するアクションを定義できます。

対話型

このオプションを有効にすると、オンデマンド スキャン中にダイアログ ボックスが表示され、ウイルスまたは不要プログラムが検出された場合、感染したファイルをどう処理するかを選択できます。このオプションは初期状態で有効に設定されています。

許可されたアクション

このボックスでは、ウイルス検出時に表示される選択可能なアクションを指定できます。これに対応するオプションを有効にする必要があります。

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旨のエラー メッセージが Web ブラウザに表示されます。レポート機能をアクティブにしている場合、WebGuard は検出されたファイルをレポート ファイルに書き込みます。

隔離

ウイルスまたはマルウェアが検出されると、Web サーバーまたは転送されたデータおよびファイルから要求された Web サイトは、[隔離] に移動されます。感染したファイルは、情報として価値がある場合、Quarantine Manager から復元できます。また、必要であれば、Avira マルウェア研究センターに送信できます。

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/ファイルは WebGuard によって Web ブラウザに送信されます。

既定

このボタンを使用すると、ウイルスが検出された場合、ダイアログ ボックスで既定でアクティブにするアクションを選択できます。既定でアクティブにするアクションを選択して、[既定値] ボタンをクリックします。

詳細については、こちらをクリックしてください。

プログレス バーの表示

このオプションを有効にした場合、Web サイト コンテンツのダウンロードで 20 秒のタイムアウト時間を超過すると、ダウンロード プログレス バーと共にデスクトップに通知が表示されます。このデスクトップ通知は、特にデータ ボリュームの大きい Web サイトのダウンロードのために設計されています。WebGuard を使用して Web を閲覧すると、Web サイトのコンテンツはインターネット ブラウザに表示される前にウイルスとマルウェアのスキャンが実行されるため、Web サイトのコンテンツの逐次的なダウンロードは行われません。このオプションは初期状態で無効に設定されています。

自動

このオプションが有効である場合、ウイルス検出時にダイアログ ボックスは表示されません。WebGuard は、プライマリ アクションおよびセカンダリ アクションとしてこのセクションで事前に定義された設定に従って動作します。

検出アラートを表示

このオプションをアクティブ化すると、ウイルスまたは不要なプログラムを検出するたびに、実行されるアクションを示すアラートが表示されます。

プライマリ アクション

プライマリ アクションとは、WebGuard がウイルスまたは不要なプログラムを検出した場合に実行されるアクションです。

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旨のエラー メッセージが Web ブラウザに表示されます。レポート機能をアクティブにしている場合、WebGuard は検出されたファイルをレポート ファイルに書き込みます。

分離

ウイルスまたはマルウェアが検出されると、Web サーバーまたは転送されたデータおよびファイルから要求された Web サイトは、[隔離] に移動されます。感染したファイルは、情報として価値がある場合、Quarantine Manager から復元できます。また、必要であれば、Avira マルウェア研究センターに送信できます。

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/ファイルは WebGuard によって Web ブラウザに送信されます。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

感染したファイルは、ワークステーションで実行可能な状態のままになります。これはワークステーションに深刻な悪影響を及ぼす可能性があります。

12.6.1.2. ロックする要求

[ロックする要求] で、WebGuard によりブロックするファイル タイプと MIME タイプ (転送されたデータのコンテンツ タイプ) を指定できます。Web フィルタを使用して、既知のフィッシングおよびマルウェアの URL をブロックできます。WebGuard は、インターネットからコンピュータ システムへのデータの転送を阻止します。

WebGuard のブロック対象ファイル タイプ/MIME タイプ (ユーザー定義)

リストに登録されているすべてのファイル タイプと MIME タイプ (転送されたデータのコンテンツ タイプ) が WebGuard によってブロックされます。

入力ボックス

このボックスに、WebGuard によりブロックする MIME タイプとファイル タイプの名前を入力します。ファイル タイプには、**.htm** などのファイル拡張子を入力します。MIME タイプには、メディア種別を指定し、必要に応じてサブタイプを入力します。メディア種別を 2 つ指定する場合は、**video/mpeg** や **audio/x-wav** のようにスラッシュで区切ります。

注意

インターネット一時ファイルとしてコンピュータ システムに既に保存されている WebGuard のブロック対象となるファイルは、コンピュータのインターネット ブラウザでインターネットからローカルにダウンロードできます。インターネット一時ファイルとは、Web サイトによりすばやくアクセスできるように、インターネット ブラウザによってコンピュータに保存されたファイルです。

注意

WebGuard::スキャン::例外の下の除外ファイルと MIME タイプのリストに、ブロックされるファイルと MIME タイプを入力すると、それらのファイルと MIME タイプは無視されます。

注意

ワイルドカード (* (任意の数の文字) または ? (単一の文字)) は、ファイル タイプと MIME タイプを入力する場合は使用できません。

MIME タイプ: メディア種別の例:

- `text` = テキスト ファイルの場合

- `image` = グラフィック ファイルの場合
- `video` = ビデオ ファイルの場合
- `audio` = サウンド ファイルの場合
- `application` = 特定のプログラムにリンクされるファイルの場合

例: 除外ファイルと MIME タイプ

- `application/octet-stream` = application/octet-stream MIME タイプ ファイル (実行可能ファイル *.bin、*.exe、*.com、*dll、*.class) は WebGuard によってブロックされます。
- `application/olescript` = application/olescript MIME タイプ ファイル (ActiveX スクリプト ファイル *.axs) は、WebGuard によってブロックされます。
- `.exe` = 拡張子 .exe を持つすべてのファイル (実行可能ファイル) が WebGuard によってブロックされます。
- `.msi` = 拡張子 .msi を持つすべてのファイル (Windows インストーラ ファイル) が WebGuard によってブロックされます。

追加

このボタンを使用すると、入力フィールドから表示ウィンドウに MIME タイプとファイル タイプをコピーできます。

削除

このボタンは、選択したエントリをリストから削除します。エントリが選択されていないと、このボタンは非アクティブになります。

Web フィルタ

Web フィルタは内部データベースに基づいて毎日更新され、コンテンツに従って URL を分類します。

Web フィルタを有効にする

このオプションを有効にすると、Web フィルタ リスト内で選択したカテゴリに一致するすべての URL がブロックされます。

Web フィルタ リスト

[Web フィルタ リスト] では、WebGuard によって URL がブロックされるコンテンツのカテゴリを選択できます。

注意

Web フィルタは、WebGuard::スキャン::例外の下の除外 URL のリストのエントリに対しては無視されます。

注意

スパム URL は、スパム電子メールで送信される URL です。 詐欺や不正のカテゴリには、“登録期間が終了した” Web ページや、提供者が費用を公表していないサービスなどの Web ページが含まれます。

12.6.1.3. 例外

これらのオプションを使用すると、MIME タイプ (転送されたデータのコンテンツ タイプ) と URL のファイル タイプ (インターネット アドレス) に基づいて、WebGuard によるスキャンに対する例外を設定できます。指定した MIME タイプと URL は、WebGuard によって無視されます。このため、データがコンピュータ システムに転送されるときに、ウイルスやマルウェアのスキャンは実行されません。

WebGuard のスキャン対象から除外する MIME タイプ

このフィールドで、WebGuard によるスキャン中に無視される MIME タイプ (転送されたデータのコンテンツ タイプ) を選択できます。

WebGuard 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)

このリストのすべての MIME タイプ (転送されたデータのコンテンツ タイプ) は WebGuard による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、WebGuard によるスキャン中に無視する MIME タイプとファイル タイプの名前を入力できます。ファイル タイプには、**.htm** などのファイル拡張子を入力します。MIME タイプには、メディア種別を指定し、必要に応じてサブタイプを入力します。メディア種別を 2 つ指定する場合は、**video/mpeg** や **audio/x-wav** のようにスラッシュで区切ります。

注意
ワイルドカード (* (任意の数の文字) または ? (単一の文字)) は、ファイル タイプと MIME タイプを入力する場合は使用できません。

警告
除外リストのすべてのファイル タイプとコンテンツ タイプがインターネット ブラウザにダウンロードされます。ただしその後、ブロック対象アクセス (WebGuard::スキャン::ブロック対象アクセス内のブロック対象ファイルと MIME タイプのリスト) のスキャンまたは WebGuard によるスキャンは実行されません。除外リストのすべてのエントリ、ブロック対象ファイルと MIME タイプのリストのエントリは無視されます。ウイルスとマルウェアのスキャンは実行されません。

MIME タイプ: メディア種別の例:

- `text` = テキスト ファイルの場合
- `image` = グラフィック ファイルの場合
- `video` = ビデオ ファイルの場合
- `audio` = サウンド ファイルの場合
- `application` = 特定のプログラムにリンクされるファイルの場合

例: 除外ファイルと MIME タイプ

- `audio/` = すべてのオーディオ メディア タイプのファイルが WebGuard のスキャン対象から除外されます。

- `video/quicktime` = すべての Quicktime サブタイプ ビデオ ファイル (*.qt, *.mov) が WebGuard のスキャン対象から除外されます。
- `.pdf` = すべての Adobe PDF ファイルが WebGuard のスキャン対象から除外されます。

追加

このボタンを使用すると、入力フィールドから表示ウィンドウに MIME タイプとファイル タイプをコピーできます。

削除

このボタンは、選択したエントリをリストから削除します。エントリが選択されていないと、このボタンは非アクティブになります。

WebGuard でスキップされた URL

このリストのすべての URL が WebGuard のスキャン対象から除外されます。

入力ボックス

このボックスに、WebGuard のスキャン対象から除外する URL (インターネット アドレス。例: **www.domainname.com**) を入力できます。URL を部分的に指定し、ドメイン レベルを表すピリオドを先頭またはそれ以降に使用できます。たとえば、「.domainname.com」と指定すると、このドメインのすべてのページおよびすべてのサブドメインが対象となります。Web サイトは、トップレベル ドメイン (.com or .net) と以降のピリオドで、domainname. のように記述します。先頭または末尾のピリオドを使用せずに記述すると、その文字列はトップレベル ドメインと解釈されます (例: **net** は、すべての NET のドメイン、つまり www.ドメイン名.net と解釈されます)。

注意

ワイルドカードの * を使用して任意の数の文字を表すこともできます。先頭または末尾のピリオドとワイルドカードを組み合わせてドメイン レベルを示すこともできます。
.domainname.*
*.domainname.com
.*name*.com (有効ですが推奨されていません)
name のようにピリオドなしで指定すると、トップレベル ドメインの一部として解釈されるので好ましくありません。

警告

除外 URL のリストにあるすべての Web サイトがインターネット ブラウザにダウンロードされます。ただしその後、Web フィルタまたは WebGuard によるスキャンは実行されません。除外 URL のリストのすべてのエントリ、Web フィルタのエントリは無視されます (WebGuard::スキャン::ブロック対象アクセスを参照)。ウイルスとマルウェアのスキャンは実行されません。このため、信頼済み URL のみを WebGuard のスキャン対象から除外する必要があります。

追加

このボタンを使用すると、入力フィールドに入力した URL (インターネット アドレス) をビューア ウィンドウにコピーできます。

削除

このボタンは、選択したエントリをリストから削除します。エントリが選択されていないと、このボタンは非アクティブになります。

例: スキャン対象から除外する URL

– `www.avira.com` -または- `www.avira.com/*`

= ドメイン 'www.avira.com' を含むすべての URL が WebGuard のスキャン対象から除外されます。例: 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' を含む URL は WebGuard のスキャン対象から除外されません。

– `avira.com` -または- `*.avira.com`

= 第 2 レベルおよびトップレベル ドメイン 'avira.com' を含むすべての URL が WebGuard のスキャン対象から除外されます。この指定は '.avira.com' のすべての既存のサブドメインを含んでいます。例: www.avira.com、forum.avira.com など。

– `avira`。-または- `*.avira.*`

= 第 2 レベル ドメイン 'avira' を含むすべての URL が WebGuard のスキャン対象から除外されます。これにより、'.avira' のすべての既存のトップレベル ドメインまたはサブドメインが指定されます。例: www.avira.com、www.avira.de、forum.avira.com など。

– `.*domain*.*`

文字列 'domain' を含む第 2 レベル ドメインを含むすべての URL が WebGuard のスキャン対象から除外されます。例: www.domain.com、www.new-domain.de、www.sample-domain1.de。

– `net` -または- `*.net`

= トップレベル ドメイン 'net' を含むすべての URL が WebGuard のスキャン対象から除外されます。例: www.name1.net、www.name2.net など。

警告
WebGuard のスキャン対象から除外する URL はできるだけ正確に入力してください。除外する URL をグローバルに指定した場合、マルウェアや好ましくないプログラムを配布するインターネット ページが WebGuard のスキャン対象から除外されるおそれがあるので、トップレベル ドメイン全体または第 2 レベル ドメインの一部を指定しないでください。少なくとも、完全な第 2 レベル ドメインおよびトップレベル ドメインを指定することが推奨されています。例: domainname.com。

12.6.1.4. ヒューリスティック

この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 スキャン機能に対する設定が含まれます。

AntiVir 製品は非常に強力なヒューリスティック スキャン機能を備えており、有害な要素に対応する専用のウイルス シグネチャが作成される前や、アンチウイルス ソフトウェアの更新プログラムが送信される前などに、未知のマルウェアを予防的に検出することができます。ウイルスの検出では、マルウェアの典型的な機能に関して、感染したコードの広範な分析と検査が行われます。スキャンされたコードにこれらに独特の特徴が見られる場合、疑わしいファイルとして報告されます。これは必ずしもそのコードが、実際にマルウェアであるという意味ではありません。誤検出が生じる場合もあります。感染したと疑われるコードの処理に関する決定は、コードのソースが信頼できるかどうかに関する知識などに基づいて、ユーザーが判断する必要があります。

マクロウイルス ヒューリスティック

マクロウイルス ヒューリスティック

AntiVir 製品には、非常に強力なマクロウイルス ヒューリスティック スキャン機能が含まれています。このオプションを有効にすると、修復の場合に関連ドキュメントのすべてのマクロが削除されるか、あるいはアラートの送信などで不審な文書に関するレポートのみが行われます。このオプションは初期状態で有効に設定されています (推奨の設定)。

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

AntiVir プログラムには、AntiVir AheAD テクノロジという非常に強力なヒューリスティック スキャン機能が含まれていて、未知の (新しい) マルウェアも検出できます。このオプションを有効にすると、このヒューリスティック スキャン機能をどの程度 "アグレッシブ" にするかを定義できます。このオプションは初期状態で有効に設定されています。

低検出レベル

このオプションを有効にすると、検出される未知のマルウェアがやや減りますが、誤ったアラートのリスクは低くなります。

中検出レベル

このヒューリスティック スキャン機能の使用を選択すると、このオプションが初期状態で有効になります。

高検出レベル

このオプションを有効にすると、未知のマルウェアをかなり多く検出するようになりますが、より高い確率で誤検出が起こる点にも注意が必要です。

12.6.2 レポート

WebGuard には、ユーザーおよび管理者に検出のタイプと方法に関する正確な注釈を提供することのできる詳細なログ機能が備えられています。

レポート

このグループを使用すると、レポート ファイルの内容を指定できます。

オフ

このオプションを有効にすると、WebGuard はログを作成しません。
ログ機能は、複数のウイルスまたは不要プログラムに関するテストの実行など、例外的な場合にのみオフにすることをお勧めします。

既定

このオプションを有効にすると、WebGuard はレポート ファイルに重要な情報 (ウイルス検出、アラートおよびエラー) を書き込み、レポート ファイルが見やすくなるように重要性の低い情報は無視します。このオプションは初期状態で有効に設定されています。

詳細

このオプションを有効にすると、WebGuard はレポート ファイルに重要性の低い情報も書き込みます。

完了

このオプションを有効にすると、WebGuard はレポート ファイルに、ファイル サイズ、ファイル タイプ、日付など、使用可能なすべての情報を書き込みます。

レポート ファイルの制限

サイズを n MB に制限

このオプションを有効にすると、レポート ファイルを特定のサイズに制限できます。可能な値: 許容される値は 1 ～ 100 MB です。レポート ファイルのサイズを制限するとき、システム リソースの使用を最小限に抑えるために、最大 50 キロバイトの予備領域が設定されています。指定したサイズの 20 % を下回ると、指定したサイズより 50 キロバイト少なくなるまで、古いエントリが削除されます。

短縮前にレポート ファイルをバックアップ

このオプションを有効にすると、レポート ファイルが短縮される前にバックアップされます。保存場所については、設定::全般::ディレクトリ::レポート ディレクトリを参照してください。

設定をレポート ファイルに書き込む

このオプションを有効にすると、オンアクセス スキャンで使用された設定がレポート ファイルに書き込まれます。

注意
レポート ファイルの制限を指定していない場合、レポート ファイルが 100MB に達すると古いエントリが自動的に削除されます。レポート ファイルのサイズが 80MB になるまで、エントリが削除されます。

12.7 更新

[更新] セクションで、更新の自動受信およびダウンロード サーバーへの接続を設定できます。 さまざまな更新間隔を指定したり、自動更新を有効または無効にしたりできます。

注意
AntiVir Security Management Center で AntiVir プログラムを設定する場合、自動更新は使用できません。

自動更新

開始する

このオプションを有効にすると、自動更新は有効になっているイベントに対して、指定した間隔で実行されます。

自動更新を n 日/時間/分ごとに実行

このボックスで、自動更新を実行する間隔を指定できます。更新間隔を変更するには、ボックスで時間オプションの１つをハイライト表示し、入力ボックスの右側の矢印キーを使用して間隔を変更します。

インターネットに接続された時にジョブを開始する (ダイヤルアップのみ)

このオプションを有効にすると、指定した更新間隔に加えて、インターネット接続の確立時にも毎回、更新ジョブが実行されます。

時間切れになったらジョブを繰り返す

このオプションを有効にすると、たとえばコンピュータの電源がオフになっていたためなど、指定した時間に実行できなかった過去の更新ジョブが実行されます。

ダウンロード

Web サーバーを経由

更新は HTTP 接続を使用して Web サーバー経由で実行されます。インターネット上の専用の Web サーバーを使用するか、イントラネット上の Web サーバーを使用できます。後者の場合、イントラネット上の Web サーバーがインターネット上の専用のダウンロード サーバーから更新プログラムを取得します。

注意
Web サーバー経由での更新については、次の場所でその他の設定も可能です。設定::全般::更新::Web サーバー。

ファイル サーバー/共有フォルダを経由

インターネット上の専用のダウンロード サーバーから更新プログラムを取得する、イントラネット上のファイル サーバー経由で、更新が実行されます。

注意
ファイル サーバー経由での更新については、次の場所でその他の設定も可能です。設定::全般::更新::ファイル サーバー。

12.7.1 製品の更新を開始

[製品の更新] の下で、製品の更新プログラムをどのように処理するか、利用可能な更新プログラムの通知をどのように処理するかを設定します。

製品の更新

製品の更新プログラムをダウンロードして、自動的にインストールする

このオプションを有効にすると、製品の更新プログラムが利用可能になると直ちにダウンロードされ、アップデータ コンポーネントによって自動的にインストールされます。ウイルス定義ファイルとスキャン エンジンへの更新は、この設定とは無関係に実行されます。このオプションの条件: すべてのアップデート設定が完了しており、ダウンロード サーバーへの接続が利用可能である必要があります。

製品の更新プログラムをダウンロードする。再起動が必要な場合は、システムの再起動後に更新プログラムをインストールします。再起動が必要ない場合は、すぐに更新プログラムをインストールします。

このオプションを有効にすると、製品の更新プログラムが利用可能になると直ぐにダウンロードされます。再起動が必要でない場合、更新プログラムはダウンロード後に自動的にインストールされます。製品の更新にコンピュータの再起動が必要な場合、更新プログラムはダウンロード直後ではなく、ユーザーによる次回のシステムの再起動時に実行されます。これには、ユーザーがコンピュータで作業中は再起動が実行されないという利点があります。ウイルス定義ファイルとスキャン エンジンへの更新は、この設定とは無関係に実行されます。このオプションの条件: すべてのアップデート設定が完了しており、ダウンロード サーバーへの接続が利用可能である必要があります。

製品の新しい更新プログラムが使用可能になったら通知

このオプションを有効にすると、製品の新しい更新プログラムが利用可能になると電子メールで通知されます。ウイルス定義ファイルとスキャン エンジンへの更新は、この設定とは無関係に実行されます。このオプションの条件: すべてのアップデート設定が完了しており、ダウンロード サーバーへの接続が利用可能である必要があります。コントロール センターの [概要]::[イベント] に、デスクトップ ポップアップ ウィンドウ、および警告メッセージを介してアップデータからの通知が表示されます。

次の期間経過後に再度通知

製品の更新プログラムが最初の通知後にインストールされなかった場合に、製品の更新プログラムが利用可能であると再通知されるまでに経過する日数を、このボックスに入力します。

製品の更新プログラムをダウンロードしない

このオプションを有効にすると、アップデータによる自動の製品の更新、または利用できる製品の通知は実行されません。ウイルス定義ファイルと検索エンジンへの更新は、この設定とは無関係に実行されます。

重要

ウイルス定義ファイルと検索エンジンの更新は、製品の更新に対する設定から独立して、すべての更新プロセス中に実行されます (「更新」)。

注意

製品の自動更新のオプションを有効にしている場合は、[設定を再起動する] の下で、再起動のその他の通知およびキャンセル オプションを設定できます。

12.7.2 設定を再起動する

AntiVir プログラムの製品の更新時、コンピュータ システムの再起動が必要になることがあります。全般::更新::製品の更新の下で製品の自動更新を選択している場合は、**[設定を再起動する]** の下で、再起動のその他の通知およびキャンセル オプションを選択できます。

注意
再起動の設定では、全般::更新::製品の更新の下の設定で、コンピュータの再起動が必要な製品の更新の実行について、2 つのオプションのいずれかを選択できることに注意してください。

更新プログラムが利用可能になったら、コンピュータの再起動が必要な製品の更新を自動的に実行する: ユーザーがコンピュータで作業中に更新と再起動が実行されます。このオプションを有効にすると便利なのは、キャンセル オプションまたは通知機能を備えた再起動ルーチンを選択する場合です。

次回のシステムの再起動の後に、コンピュータの再起動が必要な製品の更新を実行する: ユーザーがコンピュータを起動しログインした後、更新および再起動が実行されます。このオプションを有効した場合は、自動再起動ルーチンを使用することをお勧めします。

設定を再起動する

n 秒後にコンピュータを再起動します。

このオプションを有効にすると、製品の更新の実行後に必要になる再起動が、指定した間隔で**自動的**に実行されます。カウントダウン メッセージは表示されますが、コンピュータの再起動をキャンセルするオプションは提供されません。

再起動の通知メッセージを n 秒ごとに表示する

このオプションを有効にすると、製品の更新の実行後に必要になる再起動が自動的に実行**されません**。指定した間隔で、再起動の通知メッセージが表示されますが、キャンセル オプションは提供されません。これらの通知では、コンピュータの再起動を確定するか、**"[もう一度通知]"** オプションを選択することができます。

コンピュータを再起動するかどうかをクエリする

このオプションを有効にすると、製品の更新の実行後に必要になる再起動が自動的に実行**されません**。再起動を直接実行するか、または再起動ルーチンをキャンセルするオプションを提示する 1 つのメッセージのみを受信します。

クエリなしでコンピュータを再起動する

このオプションを有効にすると、製品の更新の実行後に必要になる再起動が**自動的**に実行されます。通知メッセージも表示されません。

12.7.3 ファイル サーバー

ネットワークに複数のワークステーションがある場合、AntiVir では、イントラネット上のファイル サーバーから更新プログラムをダウンロードできます。このファイル サーバーがインターネット上の専用のダウンロード サーバーから更新ファイルを取得します。これにより、すべてのワークステーションで AntiVir プログラムが最新であることが確認されます。

注意
設定の見出しは、設定::全般::製品の更新 で、**[ファイル サーバー/共有フォルダを経由]** オプションが選択されている場合にのみ有効になります。

ダウンロード

AntiVir プログラムの更新プログラムおよびその必須のディレクトリ '/release/update/' があるファイル サーバーの名前を入力します。次の情報を指定する必要があります。file:// <ファイル サーバーの IP アドレス>/release/update/。'release' ディレクトリは、すべてのユーザーがアクセスできるディレクトリであることが必要です。

このボタンをクリックするとウィンドウが開き、必要なダウンロード ディレクトリを選択できます。

サーバー ログイン

ログイン名

サーバーにログインするためのユーザー名をここに入力します。サーバー上で使用されている共有フォルダに対してアクセス権限のあるユーザー アカウントを使用します。

ログイン パスワード

ユーザー アカウントのパスワードを入力します。入力した文字は * として表示されます。

注意
サーバー ログイン セクションでデータを指定しない場合は、ファイル サーバーへのアクセス時に認証は実行されません。この場合、ユーザーはファイル サーバーに対して十分な権限を持つことが必要です。

アップデートは、インターネット上で直接 Web サーバーを介して、またはイントラネットで実行されます。

Web サーバー接続

既存の接続を使用 (ネットワーク)

ネットワークを介した接続を使用している場合は、この設定が表示されます。

次の接続を使用する:

個別に接続を定義している場合は、この設定が表示されます。

アップデータにより、使用可能な接続オプションが自動的に検出されます。使用できない接続オプションは灰色表示になり、有効にすることはできません。Windows の電話帳エントリなどを介して、ダイヤルアップ接続を手動で確立できます。

- **ユーザー:**選択したアカウントのユーザー名を入力します。
- **パスワード:**このアカウントのパスワードを入力します。セキュリティ上の理由から、このスペースに実際に入力する文字は、アスタリスク (*) に置換されます。

注意
既存のインターネット アカウント名またはパスワードを忘れた場合は、インターネット サービス プロバイダにご連絡ください。

注意
ダイヤルアップ ツール (SmartSurfer、Oleco など) を介したアップデータによる自動ダイヤルアップは、現在のところ利用できません。

更新後、確立したダイヤルアップ接続を切断

このオプションを有効にすると、更新のために確立された RDT 接続は、ダウンロードが正常に実行されると、再び自動的に中断します。

注意
このオプションは、Vista では使用できません。Vista では、更新目的で開かれたダイヤルアップ接続は、ダウンロードの実行後に常に切断されます。

ダウンロード

標準のサーバー

更新プログラムおよびその必須の更新ディレクトリ 'update' を読み込む予定の Web サーバーのアドレス (URL) を入力します。Web サーバーのアドレスの形式は次のとおりです。http://<Web サーバーのアドレス>[:Port]/update。ポートを指定しない場合は、ポート 80 が使用されます。既定では、アクセス可能な Avira GmbH Web サーバーが更新用に指定されます。ただし、企業イントラネットの独自の Web サーバーを使用することもできます。複数の Web サーバーを指定する場合は、それぞれをカンマで区切ります。

既定

このボタンは事前に設定済みのアドレスを復元します。

優先するサーバー

このフィールドに、更新プログラムを提供するように最初に要求される Web サーバーの update ディレクトリおよび URL を入力します。このサーバーが到達不可能な場合は、表示された標準サーバーが使用されます。Web サーバーのアドレスの形式は次のとおりです。http://<address of web server>[:Port]/update。ポートを指定しない場合は、ポート 80 が使用されます。

12.8 全般

12.8.1 電子メール

特定のイベントで AntiVir プログラムは、1 人以上の受信者に電子メールでアラートとメッセージを送信できます。これは Simple Message Transfer Protocol (SMTP) を使用して行います。

メッセージは、さまざまなイベントによってトリガされます。電子メールの送信をサポートするコンポーネントは以下のとおりです。

- Guard:送信通知
- スキャナ: 送信通知
- アップデータ: 送信通知

注意
ESMTP はサポートされていないので注意してください。TLS (Transport Layer Security) または SSL (Secure Sockets Layer) を使用した暗号化された転送も現在は行えません。

電子メール メッセージ

SMTP サーバー

ここで使用するホストの名前、IP アドレス、またはダイレクト ホスト名を入力します。
ホスト名は、最大 127 文字です。

例:

192.168.1.100 または mail.samplecompany.com。

送信者のアドレス

この入力ボックスに、送信者の電子メール アドレスを入力します。送信者のアドレスは、最大 127 文字です。

認証

一部のメール サーバーでは、電子メールの送信前に、プログラムによるサーバーに対する検証 (ログイン) が必要です。アラートは、SMTP サーバーに対する認証を使用して電子メールで送信できます。

認証を使用

このオプションを有効にすると、ログインに関連するボックスにユーザー名とパスワードを入力できます (認証)。

- **ユーザー名**: ここにユーザー名を入力してください。
- **パスワード**: 関連するパスワードをここに入力してください。パスワードは暗号化された形式で保存されます。セキュリティ上の理由から、このスペースに実際に入力する文字は、アスタリスク (*) に置換されます。

テスト電子メールの送信

このボタンをクリックすると、プログラムは入力されたデータの確認のため、送信者のアドレスにテスト電子メールの送信を試みます。

12.8.2 脅威カテゴリ

脅威カテゴリの選択

AntiVir 製品によってコンピュータ ウイルスから保護されます。

また、次の脅威カテゴリ (拡張) に従ってスキャンできます。

- バックドア クライアント (BDC)
- ダイヤラ (DIALER)
- ゲーム (GAMES)
- ジョーク (JOKES)
- セキュリティ プライバシ リスク (SPR)
- アドウェア/スパイウェア (ADSPY)
- 通常とは異なるランタイム圧縮 (PCK)
- 二重の拡張子ファイル (HEUR-DBLEXT)
- フィッシング
- アプリケーション (APPL)

関連するボックスをクリックすると、選択したタイプを有効にしたり (チェック マークを設定) または無効にできます (チェック マークなし)。

すべて選択

このオプションを有効にすると、すべてのタイプが有効になります。

既定値

このボタンは事前に設定済みの既定値を復元します。

注意

タイプを無効にすると、関連するプログラム タイプで認識されていたファイルは認識されなくなります。レポート ファイルにエントリは書き込まれません。

12.8.3 パスワード

パスワードを使用して、AntiVir プログラムをさまざまな領域で保護できます。パスワードが発行されると、保護された領域を開くときに、毎回パスワードが要求されます。

パスワード

パスワードの入力

パスワードをここに入力します。セキュリティ上の理由から、このスペースに実際に入力する文字は、アスタリスク (*) に置換されます。パスワードは、最大 20 文字です。パスワードが設定されると、正しくないパスワードを入力した場合、プログラムはアクセスを拒否します。空のボックスは "パスワードが未設定" であること意味します。

パスワードの確認

上で入力したパスワードをここに再度入力します。セキュリティ上の理由から、このスペースに実際に入力する文字は、アスタリスク (*) に置換されます。

注意
パスワードでは、大文字と小文字が区別されます!

パスワード保護される領域

AntiVir プログラムでは、パスワードを使用して個々の領域を保護できます。必要に応じて、関連するボックスをクリックして、個々の領域に対するパスワードの要求を無効にしたり、再度有効にしたりできます。

パスワード保護されている領域	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 センターの開始時に事前に設定済みのパスワードが要求されます。
Guard のアクティブ化 / 非アクティブ化	このオプションを有効にすると、AntiVir Guard の有効化または無効化に、事前に設定済みのパスワードが要求されます。
MailGuard のアクティブ化 / 非アクティブ化	このオプションを有効にすると、MailGuard の有効化/無効化に事前に設定済みのパスワードが要求されます。
FireWall を有効にする / 無効にする	このオプションを有効にすると、FireWall の有効化/無効化に事前に設定済みのパスワードが要求されます。
WebGuard のアクティブ化 / 非アクティブ化	このオプションを有効にすると、WebGuard の有効化/無効化に事前に設定済みのパスワードが要求されます。
レスキュー CD をインターネットからダウンロード	このオプションを有効にすると、Avira レスキュー CD のダウンロード開始時に事前に設定済みのパスワードが要求されます。
隔離	このオプションを有効にすると、隔離のすべての領域でパスワード保護が有効になります。関連するボックスをクリックして、個々の領域に対する要求に応じて、パスワードの問い合わせを無効にしたり、再度有効

	にしたりできます。
影響を受ける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事前に設定済みのパスワードが要求されます。
感染した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事前に設定済みのパスワードが要求されます。
影響を受けるオブジェクトのプロパティ	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の表示に事前に設定済みのパスワードが要求されます。
影響を受ける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事前に設定済み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、オブジェクトを調査のために Avira マルウェア研究センターに送信するために、事前に設定済みのパスワードが要求されます。
感染したオブジェクトをコピーしています	このオプションを有効にすると、感染したオブジェクトのコピーに事前に設定済みのパスワードが要求されます。
ジョブの追加と変更	このオプションを有効にすると、スケジューラでのジョブの追加および変更に事前に設定済みのパスワードが要求されます。
製品の更新を開始	このオプションを有効にすると、更新メニューでの製品更新に事前に設定済みのパスワードが要求されます。
設定	このオプションを有効にすると、事前定義のパスワードを入力した場合にのみ、プログラムを設定できます。
設定を手動で切り替える	このオプションを有効にすると、別の設定プロファイルに手動で切り替えるために、事前に設定済みのパスワードが要求されます。
エキスパート モードを有効にする	このオプションを有効にすると、エキスパート モードの有効化/無効化に事前に設定済みのパスワードが要求されます。

インストール/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またはアンインストールに事前に設定済みのパスワードが要求されます。

12.8.4 セキュリティ

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

このボックスに、最終更新から許容される最大経過日数を入力できます。この日数を経過した場合、コントロール センターで [状況] の下に赤いアイコンが表示され、更新の状況が示されます。

ウイルス定義ファイルが古い場合に注意を表示

このオプションを有効にすると、ウイルス定義ファイルが最新でない場合に、アラートが送信されます。アラート オプションを使用すると、最終更新から何日以上経過した場合にアラートが送信されるかを時間間隔で設定できます。

製品の保護

注意
ユーザー定義のインストール オプションにより Guard がインストールされていない場合、製品の保護オプションは使用できません。

不要な終了からプロセスを保護

このオプションを有効にすると、プログラムのすべてのプロセスはウイルスやマルウェアによる不要な終了や、タスク マネージャによるユーザーに "制御できない" 終了から保護されます。このオプションは初期状態で有効に設定されています。

高度なプロセス保護

このオプションを有効にすると、プログラムのすべてのプロセスは詳細オプションを使用した不要な終了から保護されます。高度なプロセス保護は、簡易保護と比べると、大幅に多くのコンピュータ リソースが必要です。このオプションは初期状態で有効に設定されています。このオプションを無効にするには、コンピュータを再起動する必要があります。

重要
パスワード保護は、Windows XP 64 ビットでは使用できません。

警告
プロセスの保護を有効にした場合、他のソフトウェア製品との対話に問題が生じる可能性があります。その場合は、プロセスの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

このオプションを有効にすると、プログラムのすべてのレジストリ エントリおよびすべてのプログラム ファイル (バイナリおよび設定ファイル) が改変されないように保護されます。ユーザーまたは外部プログラムによるレジストリ エントリまたはプログラム ファイルの書き込みや削除のほか、場合によっては、読み取りアクセスも禁止されます。このオプションを有効にするには、コンピュータを再起動する必要があります。

警告
このオプションを無効にした場合、特定のタイプのマルウェアに感染したコンピュータの修復が失敗する可能性があることに注意してください。

注意
このオプションを有効にすると、スキャン要求や更新要求の変更といった設定の変更が、ユーザー インターフェイス経由でしか行えなくなります。

重要
ファイルとレジストリ エントリの保護は、Windows XP 64 ビットでは使用できません。

12.8.5 WMI

Windows Management Instrumentation のサポート

Windows Management Instrumentation は、Windows システム上の設定にスクリプトとプログラミング言語を使用してアクセスできるようにする、Windows 管理の基本的な手法であり、ローカルまたはリモートから、各種の設定を読み取ったり書き込んだりすることができます。AntiVir プログラムは WMI をサポートしており、データ (ステータス情報、統計データ、レポート、予定した要求など) を提供するほか、インターフェイスでのイベントおよびメソッド (プロセスの開始と停止) を提供します。WMI により、プログラムから動作データをダウンロードし、プログラムを制御できます。 WMI インターフェイスの詳細なリファレンス ガイドについては、製造元にお問い合わせください。秘密保持契約に署名すると、PDF 形式のリファレンス ファイルを入手できます。

WMI のサポートを有効にする

このオプションを有効にすると、プログラムから WMI を介して動作データをダウンロードできます。

サービスの有効化/無効化の操作を許可

このオプションを有効にすると、WMI を介してプログラム サービスを有効/無効にすることができます。

12.8.6 ディレクトリ

一時フォルダ パス

この入力ボックスに、プログラムが一時ファイルを格納するパスを入力します。

既定のシステム設定を使用

このオプションを有効にすると、一時ファイルの処理にシステムの設定が使用されます。

注意

システムがどこに一時ファイルを保存しているかを確認できます。たとえば、Windows XP の場合は、[スタート]、[設定]、[コントロール パネル]、[システム]、[詳細設定]、[環境変数] で確認できます。現在登録されているユーザーに対する一時変数 (TEMP、TMP) およびシステム変数に対する一時変数 (TEMP、TMP) は、ここに関連する値と共に表示されます。

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。

このボタンをクリックするとウィンドウが開き、必要な一時パスを選択できます。

既定

このボタンは、一時パスに対する事前に設定済みのディレクトリを復元します。

レポート ディレクトリ

この入力ボックスには、レポート ファイルへのパスが含まれています。

このボタンでウィンドウが開き、必要なディレクトリを選択できます。

既定

このボタンは、レポート ディレクトリに対する事前定義のパスを復元します。

[隔離] ディレクトリ

このボックスには、[隔離] ディレクトリへのパスが含まれています。

このボタンでウィンドウが開き、必要なディレクトリを選択できます。

既定

このボタンは、[隔離] ディレクトリへの事前定義のパスを復元します。

12.8.7 プロキシ

プロキシ サーバー

プロキシ サーバーを使用しない

このオプションを有効にすると、Web サーバーへの接続はプロキシ サーバーを介さずに実行されます。

Windows システム設定を使用

このオプションを有効にすると、プロキシ サーバーを介した Web サーバーへの接続に現在の Windows システム設定が使用されます。**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、プロキシ サーバーを使用するように Windows システム設定を構成します。また、Internet Explorer の [その他] メニューでインターネット オプションを利用できます。

警告
認証を必要とするプロキシ サーバーを使用している場合、*[このプロキシサーバーを使用]* オプションで必要なすべてのデータを入力します。*[Windows システム設定を使用]* オプションは、認証を利用しないプロキシ サーバーでのみ使用できます。

このプロキシ サーバーを使用(U)

Web サーバーの接続がプロキシ サーバーを介してセットアップされている場合は、関連する情報をここに入力できます。

アドレス

Web サーバーに接続するために使用するプロキシ サーバーのコンピュータ名または IP アドレスを入力します。

ポート

Web サーバーへの接続に使用するプロキシ サーバーのポート番号を入力してください。

ログイン名

プロキシ サーバーにログインするためのユーザー名をここに入力します。

ログイン パスワード

プロキシ サーバーへのログインに関連するパスワードをここに入力します。セキュリティ上の理由から、このスペースに実際に入力する文字は、アスタリスク (*) に置換されます。

例:

アドレス:	proxy.domain.com	ポート:	8080
アドレス:	192.168.1.100	ポート:	3128

12.8.8 警告

12.8.8.1. ネットワーク

個別に設定可能なアラートは、スキャナまたは Guard からネットワーク内の任意のワークステーションに送信できます。

注意
"メッセージ サービス" が開始しているかどうかを確認してください。このサービスは、たとえば Windows XP の場合は、[スタート]、[設定]、[システムコントロール]、[管理]、[サービス] の下にあります。

注意
アラートは特定のユーザーに送信されるのではなく、常にコンピュータに送信されます。

警告
次のオペレーティング システムでは、この機能のサポートは廃止されます。
Windows Server 2008 以上
Windows Vista 以上

メッセージの送信先

このウィンドウのリストには、ウイルスまたは不要プログラムが検出された場合に、メッセージを受信するコンピュータの名前が表示されます。

注意
コンピュータは、このリストに 1 回だけ入力できます。

挿入

このボタンを使用すると、さらにコンピュータを追加できます。ウィンドウが開き、新しいコンピュータの名前を入力できます。コンピュータの名前は、最大 15 文字までです。

このボタンをクリックするとウィンドウが開き、代わりに自分のコンピュータ環境から直接コンピュータを選択することもできます。

削除

このボタンを使用すると、現在選択しているエントリをリストから削除できます。

Guard

ネットワーク アラート

このオプションを有効にすると、ネットワーク アラートが送信されます。このオプションは初期状態で無効に設定されています。

注意
このオプションを有効にするには、全般::アラート::ネットワークの下に、最低 1 人受信者を入力する必要があります。

送信メッセージ

このウィンドウには、ウイルスまたは不要プログラムが検出されたときに、選択したワークステーションに送信されたメッセージが表示されます。このメッセージは編集できます。テキストには、最大 500 文字を含めることができます。

メッセージの書式設定には、次のキーの組み合わせを使用できます。

Strg + Tab	タブを挿入します。現在の行が数文字、右にインデントされます。
Strg + Enter	改行を挿入します。

メッセージには、検索中に発見された情報のためのワイルドカードを含めることができます。これらのワイルドカードは、送信時に実際のテキストに置換されます。

次のワイルドカードを使用できます。

%VIRUS%	検出されたウイルスまたは不要プログラムの名前が格納されます。
%FILE%	感染したファイルのパスとファイル名が格納されます。
%COMPUTER%	Guard を実行しているコンピュータの名前が格納されます。
%NAME%	感染したファイルにアクセスしたユーザーの名前が格納されます。
%ACTION%	ウイルス検出後に実行されたアクションが格納されます。
%MACADDR%	Guard を実行しているコンピュータの MAC アドレスが格納されます。

既定

このボタンは、アラートに対する事前に設定済みの既定のテキストを復元します。

スキャナ

ネットワーク アラートの有効化

このオプションを有効にすると、ネットワーク アラートが送信されます。このオプションは初期状態で無効に設定されています。

注意
このオプションを有効にするには、全般::アラート::ネットワークの下に、最低 1 人受信者を入力する必要があります。

送信メッセージ

このウィンドウには、ウイルスまたは不要プログラムが検出されたときに、選択したワークステーションに送信されたメッセージが表示されます。このメッセージは編集できます。テキストには、最大 500 文字を含めることができます。

メッセージの書式設定には、次のキーの組み合わせを使用できます。

Strg + Tab	タブを挿入します。現在の行が数文字、右にインデントされます。
Strg + Enter	改行を挿入します。

メッセージには、検索中に発見された情報のためのワイルドカードを含めることができます。これらのワイルドカードは、送信時に実際のテキストに置換されます。

次のワイルドカードを使用できます。

%VIRUS%	検出されたウイルスまたは不要プログラムの名前が格納されます。
%NAME%	スキャナを使用するログインしたユーザーの名前が格納されます。

既定

このボタンは、アラートに対する事前に設定済みの既定のテキストを復元します。

12.8.8.2. 電子メール

電子メール

特定のイベントで AntiVir プログラムは、1 人以上の受信者に電子メールでアラートとメッセージを送信できます。これは Simple Message Transfer Protocol (SMTP) を使用して行います。

メッセージは、さまざまなイベントによってトリガされます。電子メールの送信をサポートするコンポーネントは以下のとおりです。

- Guard:送信通知
- スキャナ: 送信通知
- アップデータ: 送信通知

注意

ESMTP はサポートされていないので注意してください。TLS (Transport Layer Security) または SSL (Secure Sockets Layer) を使用した暗号化された転送も現在は行えません。

電子メール メッセージ

SMTP サーバー

ここで使用するホストの名前、IP アドレス、またはダイレクト ホスト名を入力します。
ホスト名は、最大 127 文字です。

例:

192.168.1.100 または mail.samplecompany.com。

送信者のアドレス

この入力ボックスに、送信者の電子メール アドレスを入力します。送信者のアドレスは、最大 127 文字です。

認証

一部のメール サーバーでは、電子メールの送信前に、プログラムによるサーバーに対する検証 (ログイン) が必要です。アラートは、SMTP サーバーに対する認証を使用して電子メールで送信できます。

認証を使用

このオプションを有効にすると、ログインに関連するボックスにユーザー名とパスワードを入力できます (認証)。

- **ユーザー名**: ここにユーザー名を入力してください。

– **パスワード**: 関連するパスワードをここに入力してください。パスワードは暗号化された形式で保存されます。セキュリティ上の理由から、このスペースに実際に入力する文字は、アスタリスク (*) に置換されます。

テスト電子メールの送信

このボタンをクリックすると、プログラムは入力されたデータの確認のため、送信者のアドレスにテスト電子メールの送信を試みます。

Guard

AntiVir Guard では、特定のイベントについて 1 人以上の受信者に電子メールでアラートを送信できます。

Guard

電子メール アラート

このオプションを有効にすると、特定のイベントが発生した場合、AntiVir Guard によって最も重要な情報が記載された電子メール メッセージが送信されます。このオプションは初期状態で無効に設定されています。

以下のイベント向けの電子メール メッセージ

オンアクセス スキャンでウイルスや不要なプログラムを検出。

このオプションを有効にすると、オンアクセス スキャンでウイルスや不要プログラムが検出された場合、ウイルスまたは不要プログラムの名前と感染したファイルの名前が記載された電子メールが送信されます。

編集

"*[編集]*" ボタンをクリックすると、"オンアクセス検出" イベントに対する通知を設定できる "*[電子メール テンプレート]*" ウィンドウが開きます。電子メールの件名行および本文にテキストを挿入するオプションがあります。この目的で変数を使用することもできます (設定::全般::電子メール::アラート::電子メール テンプレートを参照)。

Guard で重大なエラーが発生。

このオプションを有効にすると、重大な内部エラーが検出された場合に電子メールを受信します。

注意
この場合は、電子メールに記載されていたデータを含めて、テクニカル サポートにご連絡ください。調査のため、指定したファイルも送信する必要があります。

編集

[編集] ボタンをクリックすると、"Guard で重大なエラーが発生" イベントに対する通知を設定できる *[電子メール テンプレート]* ウィンドウが開きます。電子メールの件名行および本文にテキストを挿入するオプションがあります。この目的で変数を使用することもできます (設定::全般::電子メール::アラート::電子メール テンプレートを参照)。

受信者

このボックスには、受信者の電子メール アドレスを入力します。アドレスはカンマで区切ってください。すべてのアドレスを合わせた (文字列合計の) 長さは最大 260 文字です。

スキャナ

特定のイベントについては、オンデマンド スキャンを使用して、1 人以上の受信者に電子メールでアラートとメッセージを送信できます。

スキャナ

電子メール アラートの有効化

このオプションを有効にすると、特定のイベントが発生した場合、プログラムによって最も重要な情報が記載された電子メール メッセージが送信されます。このオプションは初期状態で無効に設定されています。

以下のイベント向けの電子メール メッセージ

オンデマンド スキャンによりウイルスまたは不要なプログラムを検出

このオプションを有効にすると、オンデマンド スキャンでウイルスや不要プログラムが検出されると必ず、ウイルスまたは不要プログラムと感染したファイルの名前が記載された電子メールが送信されます。

編集

[編集] ボタンをクリックすると、"スキャン検出" イベントに対する通知を設定できる *[電子メール テンプレート]* ウィンドウが開きます。電子メールの件名行および本文にテキストを挿入するオプションがあります。この目的で変数を使用することもできます (設定::全般::電子メール::アラート::電子メール テンプレートを参照)。

スケジュールされたスキャンの終了

このオプションを有効にすると、スキャン ジョブが終了したときに、電子メールが送信されます。電子メールには、スキャン ジョブの時刻と期間、スキャンされたフォルダとファイル、および検出されたウイルスと警告が含まれます。

編集

[編集] ボタンをクリックすると、"スキャンの終了" イベントに対する通知を設定できる *[電子メール テンプレート]* ウィンドウが開きます。電子メールの件名行および本文にテキストを挿入するオプションがあります。この目的で変数を使用することもできます (設定::全般::電子メール::アラート::電子メール テンプレートを参照)。

レポート ファイルを添付ファイルとして追加

このオプションを有効にすると、スキャナ通知を送信するとき、スキャナ コンポーネントの現在のレポート ファイルが添付ファイルとして電子メールに追加されます。

受信者のアドレス

このボックスには、受信者の電子メール アドレスを入力します。アドレスはカンマで区切ってください。すべてのアドレスを合わせた (文字列合計の) 長さは最大 260 文字です。

アップデータ

アップデータ コンポーネントでは、特定のイベントについて 1 人以上の受信者に電子メールで通知を送信できます。

アップデータ

電子メール アラート

このオプションを有効にすると、特定のイベントが発生した場合、アップデータ コンポーネントによって最も重要なデータが記載された電子メール メッセージが送信されます。このオプションは初期状態で無効に設定されています。

以下のイベント向けの電子メール メッセージ

更新は不要です。プログラムは最新の状態です。

このオプションを有効にすると、アップデータが正常にダウンロード サーバーに接続したが、サーバー上で使用できる新しいファイルがない場合に電子メールが送信されます。これは、AntiVir プログラムが最新の状態であることを意味します。

編集

[編集] ボタンをクリックすると、"更新は不要" イベントに対する通知を設定できる *[電子メール テンプレート]* ウィンドウが開きます。電子メールの件名行および本文にテキストを挿入するオプションがあります。この目的で変数を使用することもできます (設定::全般::電子メール::アラート::電子メール テンプレートを参照)。

更新は正常に終了しました。新しいファイルがインストールされています。

このオプションを有効にすると、実行されたすべての更新について電子メールが送信されます。 たとえば、製品の更新、ウイルス定義ファイルやスキャン エンジンの更新の場合です。

編集

[編集] ボタンをクリックすると、"更新の正常終了 – 新しいファイルがインストールされた" イベントに対する通知を設定できる *[電子メール テンプレート]* ウィンドウが開きます。電子メールの件名行および本文にテキストを挿入するオプションがあります。この目的で変数を使用することもできます (設定::全般::電子メール::アラート::電子メール テンプレートを参照)。

更新は正常に終了しました。新しい製品の更新プログラムを使用できます。

このオプションを有効にすると、製品の更新プログラムを使用できるが更新を実行せずに、スキャン エンジンまたはウイルス定義ファイルの更新を実行した場合にのみ、電子メールが送信されます。

編集

[編集] ボタンをクリックすると、"更新の正常終了 - 製品の更新プログラムが利用可能" イベントに対する通知を設定できる *[電子メール テンプレート]* ウィンドウが開きます。電子メールの件名行および本文にテキストを挿入するオプションがあります。この目的で変数を使用することもできます (設定::全般::電子メール::アラート::電子メール テンプレートを参照)。

更新できませんでした。

このオプションを有効にすると、エラーにより更新を実行できなかった場合に、電子メールが送信されます。

編集

[編集] ボタンをクリックすると、"更新の失敗" イベントに対する通知を設定できる *[電子メール テンプレート]* ウィンドウが開きます。電子メールの件名行および本文にテキストを挿入するオプションがあります。この目的で変数を使用することもできます (設定::全般::電子メール::アラート::電子メール テンプレートを参照) 。

レポート ファイルを添付ファイルとして追加

このオプションを有効にすると、アップデータ通知を送信するとき、アップデータ コンポーネントの現在のレポート ファイルが添付ファイルとして電子メールに追加されます。

受信者

このボックスには、受信者の電子メール アドレスを入力します。アドレスはカンマで区切ってください。すべてのアドレスを合わせた (文字列合計の) 長さは最大 260 文字です。

注意

アップデータ通知用の SMTP サーバーおよび受信者アドレスが設定されている場合は、次のイベントに対するアラートが電子メールで常に送信されます。
プログラムの今後のすべての更新プログラムを使用するには、製品の更新が必要です。
製品の更新が必要なため、スキャン エンジン、またはウイルス定義ファイルの更新を実行できませんでした。

これらのアラートは、アップデータ コンポーネントの電子メール警告の設定にかかわらず送信されます。

電子メール テンプレート

[電子メール テンプレート] ウィンドウで、有効になっているイベントに対する電子メール通知をコンポーネントごとに設定できます。件名行に最大 128 文字、メッセージ フィールドに最大 1024 文字のテキストを挿入できます。

以下の変数を電子メールの件名およびメッセージで使用できます。

グローバル変数

変数	値
Windows 環境変数	電子メール通知コンポーネントはすべての Windows 環境変数をサポートしています。
%SYSTEM_IP%	コンピュータの IP アドレス
%FQDN%	完全修飾ドメイン名
%TIMESTAMP%	イベントのタイム スタンプ: オペレーティング システムの言語設定に従った時間および日付の

	形式
%COMPUTERNAME%	NetBIOS コンピュータ名
%USERNAME%	コンポーネントにアクセスするユーザーの名前
%PRODUCTVER%	製品バージョン
%PRODUCTNAME%	製品名
%MODULENAME%	電子メールを送信するコンポーネントの名前
%MODULEVER%	電子メールを送信するコンポーネントのバージョン

固有のコンポーネント変数

変数	値	コンポーネント電子メール
%ENGINEVER%	使用するスキャン エンジンのバージョン	Guard スキャナ
%VDFVER%	使用するウイルス定義ファイルのバージョン	Guard スキャナ
%SOURCE%	完全修飾ファイル名	Guard
%VIRUSNAME%	ウイルスまたは不要プログラムの名前	Guard
%ACTION%	検出後に実行するアクション	Guard
%MACADDR%	最初に登録したネットワーク カードの MAC アドレス	Guard
%UPDFILESLIST%	更新するファイルのリスト	アップデータ
%UPDATETYPE%	更新のタイプ: スキャン エンジンおよびウイルス定義ファイルの更新、またはスキャン エンジンおよびウイルス定義ファイルの更新による製品の更新	アップデータ
%UPDATEURL%	更新に使用するダウンロード サーバーの URL	アップデータ
%UPDATE_ERROR%	更新エラー (ワード単位)	アップデータ

%DIRCOUNT%	スキャンされたディレクトリの数	スキャナ
%FILECOUNT%	スキャンされたファイルの数	スキャナ
%MALWARECOUNT%	検出されたウイルスまたは不要プログラムの数	スキャナ
%REPAIREDCOUNT%	修復された、感染したファイルの数	スキャナ
%RENAMEDCOUNT%	名前を変更された、感染したファイルの数	スキャナ
%DELETEDCOUNT%	削除された、感染したファイルの数	スキャナ
%WIPECOUNT%	上書きおよび削除された、感染したファイルの数	スキャナ
%MOVEDCOUNT%	隔離に移動された、感染したファイルの数	スキャナ
%WARNINGCOUNT%	警告数	スキャナ
%ENDTYPE%	スキャンのステータス: 終了/正常完了	スキャナ
%START_TIME%	スキャンの開始時刻: 更新の開始時刻	スキャナ アップデータ
%END_TIME%	スキャンの終了 更新の終了	スキャナ アップデータ
%TIME_TAKEN%	スキャンの期間 (分単位) 更新の期間 (分単位)	スキャナ アップデータ
%LOGFILEPATH%	レポート ファイルのパスおよびファイル名	スキャナ アップデータ

12.8.8.3. 音声によるアラート

音声によるアラート

対話型アクション モードでは、スキャナまたは Guard によってウイルスやマルウェアが検出されると、音声によるアラートが再生されます。音声によるアラートをアクティブまたは非アクティブにしたり、音声によるアラートとして別の Wave ファイルを選択したりできます。

注意
スキャナのアクション モードは、スキャナ::スキャン::検出に対するアクションの設定で設定します。Guard のアクション モードは、Guard::スキャン::検出に対するアクションの設定で設定します。

音声によるアラートを行わない

このオプションを有効にすると、スキャナまたは Guard によってウイルスが検出されても音声によるアラートは再生されません。

PC スピーカーを使用 (対話型モードのみ)

このオプションを有効にすると、スキャナまたは Guard によってウイルスが検出されたときの音声によるアラートとして、既定のシグナルが使用されます。音声のアラートが PC の内蔵スピーカーで再生されます。

次の WAV ファイルを使用 (対話型モードのみ)

このオプションを有効にすると、スキャナまたは Guard によってウイルスが検出されたときの音声によるアラートとして、選択した Wave ファイルが使用されます。選択した Wave ファイルが、外部接続のスピーカで再生されます。

Wave ファイル

この入力ボックスに、選択したオーディオ ファイルの名前と関連するパスを入力できます。標準として、プログラムの既定の音声によるシグナルが入力されます。

...

このボタンをクリックするとウィンドウが開き、ファイル エクスプローラを使用して、必要なファイルを選択できます。

テスト

このボタンは、選択した Wave ファイルのテストに使用します。

12.8.8.4. 警告

AntiVir プログラムは、特定のイベントに対するデスクトップ通知 (いわゆるスライドアップ) を生成します。この通知では、更新のようなプログラム シーケンスが成功したか失敗したかに関する情報が提供されます。*[警告]* で、特定のイベントに対する通知を有効または無効にできます。

デスクトップ通知について、スライド アップでの直接表示を無効にすることもできます。*[警告]* で、無効になっている通知を有効にできます。

警告

ダイヤルアップ接続の使用

このオプションを有効にした場合、ダイヤラによって電話または ISDN ネットワーク経由でコンピュータ上にダイヤルアップ接続が作成されると、デスクトップ通知アラートが表示されます。不明や不要なダイヤラによって接続が作成され、その接続が課金される可能性があるという危険があります。(ウイルスなど::脅威カテゴリ::ダイヤラを参照)。

正常に更新されたファイル

このオプションを有効にすると、更新が正常に実行され、ファイルが更新されるたびに、デスクトップ通知が表示されます。

失敗した更新

このオプションを有効にした場合、更新が失敗するたびに、デスクトップ通知が表示されます。ダウンロード サーバーへの接続を作成できないか、更新ファイルをインストールできない可能性があります。

更新が不要

このオプションを有効にすると、更新が開始されたが、プログラムが最新の状態なのでファイルのインストールが必要ないときに、毎回デスクトップ通知が表示されます。

12.8.9 イベント

イベント データベース サイズの制限

イベントの最大数を n エントリに制限

このオプションを有効にすると、イベント データベースに列挙されるイベントの最大数を特定のサイズに制限できます。可能な値: 100 ～ 10000 エントリ。入力したエントリ数を超えると、最も古いエントリが削除されます。

n 日より古いイベントを削除

このオプションを有効にすると、イベント データベースに列挙されるイベントは、特定の期間後に削除されます。可能な値: 1 ～ 90 日。このオプションは初期状態で有効に設定されていて、既定値は 30 日です。

イベント データベース サイズを制限しない (イベントを手動で削除)

このオプションを有効にすると、イベント データベースのサイズが制限されなくなります。ただし、[イベント] の下のプログラム インターフェイスでは、最大 20,000 エントリが表示されます。

12.8.10 レポートの制限

レポート数を制限

数を n 個に制限

このオプションを有効にすると、レポートの最大数が指定した量に制限されます。許容される値は 1 ～ 300 です。指定した数字を超えると、その時点で最も古いレポートが削除されます。

n 日より古いすべてのレポートを削除

このオプションを有効にすると、特定の日数の後、レポートは自動的に削除されます。許容される値: 1 ～ 90 日。このオプションは初期状態で有効に設定されていて、既定値は 30 日です。

レポート数を制限しない (レポートを手動で削除)

このオプションを有効にすると、レポートの数が制限されなくなります。

そのべてのブランド名および製品名は、それぞれの保有者の商標または登録商標です。

このマニュアルは、細心の注意を払って作成されていますが、
設計上のエラーおよびコンテンツのエラーが含まれている可能性があります。

Avira Operations GmbH & Co. KG からの書面による事前の許可なしに、本出版物を複製することは
(たとえ一部であっても)、
どのような形式であれ、禁止されています。
エラーおよび技術情報は、予告なく変更されることがあります。

© 2011 Avira Operations GmbH &Co. KG. All rights reserved.

AVIRA

live free.™

日本
株式会社アビラ
〒107-0061 ¦ 東京都港区北青山一丁目4番5号ロジェ青山
メール: info@avira.jp
ホームページ : http://www.avira.jp