

Avira AntiVir Premium

ユーザー マニュアル

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、それぞれの所有者の商標または登録商標です。

このマニュアルでは商標を保護するマークは使用していませんが、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 Premium 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 Premium 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.....	1
2	アイコンと強調表示.....	2
3	製品情報.....	3
3.1	提供範囲.....	3
3.2	システム要件.....	4
3.3	ライセンスとアップグレード.....	4
4	インストールとアンインストール.....	6
4.1	インストール.....	6
4.2	インストールの変更.....	12
4.3	インストールモジュール.....	12
4.4	アンインストール.....	13
5	AntiVir Premium の概要.....	15
5.1	ユーザーインターフェイスと操作.....	15
5.1.1	コントロールセンター.....	15
5.1.2	設定.....	18
5.1.3	トレイアイコン.....	21
5.2	方法.....	21
5.2.1	製品をアクティブ化.....	21
5.2.2	自動更新の実行.....	22
5.2.3	手動更新の開始.....	24
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.....	24
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.....	26
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.....	27
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.....	27
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.....	28
5.2.9	検出されたウイルスとマルウェアへの対処.....	29
5.2.10	隔離::隔離されたファイルの処理 (*.qua).....	33
5.2.11	隔離::[隔離]内のファイルの復元.....	35
5.2.12	隔離::疑わしいファイルを [隔離] に移動.....	36
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.....	36
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.....	37
5.2.15	イベント::フィルタイベント.....	37
5.2.16	MailGuard::電子メールアドレスをスキャン対象から除外.....	38

6	スキャナ.....	41
7	更新.....	42
8	FAQ、ヒント	43
8.1	問題が発生した場合のヘルプ.....	43
8.2	ショートカット.....	46
8.2.1	ダイアログボックス内.....	46
8.2.2	ヘルプ内.....	47
8.2.3	コントロールセンター内.....	47
8.3	Windows セキュリティセンター.....	49
8.3.1	全般.....	49
8.3.2	Windows セキュリティセンターと AntiVir プログラム.....	49
9	ウイルスなど	52
9.1	脅威カテゴリ (拡張).....	52
9.2	ウイルスとその他のマルウェア.....	55
10	情報とサービス	59
10.1	連絡先情報.....	59
10.2	テクニカルサポート.....	59
10.3	疑わしいファイル.....	60
10.4	誤検出レポート.....	60
10.5	フィードバックの送付.....	60
11	参照: 設定オプション	61
11.1	スキャナ.....	61
11.1.1	スキャン.....	61
11.1.1.1	検出時のアクション.....	64
11.1.1.2	例外.....	67
11.1.1.3	ヒューリスティック.....	68
11.1.2	レポート.....	69
11.2	Guard.....	70
11.2.1	スキャン.....	70
11.2.1.1	検出時のアクション.....	72
11.2.1.2	その他のアクション.....	74
11.2.1.3	例外.....	75
11.2.1.4	ヒューリスティック.....	78
11.2.2	ProActiv.....	80
11.2.2.1	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.....	81
11.2.2.2	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.....	82
11.2.3	レポート.....	83
11.3	MailGuard.....	84
11.3.1	スキャン.....	84
11.3.1.1	検出時のアクション.....	85
11.3.1.2	その他のアクション.....	86
11.3.1.3	ヒューリスティック.....	87
11.3.2	全般.....	88
11.3.2.1	例外.....	88
11.3.2.2	キャッシュ.....	89

11.3.3	レポート	89
11.4	WebGuard	90
11.4.1	スキャン	91
11.4.1.1.	検出時のアクション	92
11.4.1.2.	ロックする要求	93
11.4.1.3.	例外	94
11.4.1.4.	ヒューリスティック	97
11.4.2	レポート	98
11.5	更新	99
11.5.1	製品の更新を開始	100
11.5.2	設定を再起動する	101
11.6	全般	102
11.6.1	脅威カテゴリ	102
11.6.2	パスワード	103
11.6.3	セキュリティ	105
11.6.4	WMI	106
11.6.5	プロキシ	106
11.6.6	ディレクトリ	107
11.6.7	イベント	108
11.6.8	レポートの制限	108
11.6.9	音声によるアラート	109
11.6.10	警告	109

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。
- 「ライセンスマネージャ」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ー (スキャンエンジン) に基づく、非常に高いウイルスとマルウェアの検出率
- ネストされたアーカイブの検出や、スマート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)

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、アクティブ化キーの形態で提供されます。アクティブ化キーは、AntiVir 製品を購入した後に受け取る文字および数字から成るコードです。アクティブ化キーには、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。

AntiVir プログラムをインターネットで購入された場合、アクティブ化キーは電子メールで送信されます。または製品パッケージに含まれています。

プログラムのライセンス許諾を受けるには、プログラムをアクティブ化するアクティブ化キーを入力してください。製品のアクティブ化操作は、インストール時に実行することもできますが、ライセンス マネージャの [ヘルプ]::[ライセンス管理] で、インストール後に AntiVir プログラムをアクティブ化することもできます。

ライセンス マネージャでは、AntiVir デスクトップ製品ファミリから製品のアップグレードを起動するオプションがあります。古い製品の手動のアンインストールと、新しい製品の手動のインストールは必要ありません。ライセンス マネージャからアップグレードする場合は、[ライセンス マネージャ] 入力ボックスに、アップグレードする製品のアクティブ化コードを入力します。新しい製品が自動的にインストールされます。

次の製品のアップグレードは、ライセンス マネージャを介して自動的に実行できます。

- Avira AntiVir Personal から Avira AntiVir Premium へのアップグレード
- Avira AntiVir Personal から Avira Premium Security Suite へのアップグレード
- Avira AntiVir Premium から Avira Premium Security Suite へのアップグレード

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。
- 「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

- 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なになります。
- ▶ 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)
- ▶ プログラムをアクティブ化するとき
- ▶ 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ときに **AntiVir** プログラムのライセンスキーを便利に使いたいとき

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。

注意

AntiVir プログラムは、製品をアクティブ化するときに **Avira GmbH** サーバーと通信するため、**HTTP** プロトコルとポート **80** (Web 通信) および **SSL** 暗号化プロトコルとポート **443** を使用します。ファイアウォールを使用している場合、必要な接続や受信または送信データがファイアウォールでブロックされていないことを確認してください。

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:

- ▶ 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 Premium 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。
- ▶ 次のセクション「[エクスプレス インストール](#)」はスキップします。

エクスプレス インストール

[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。

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 ウィザードが開きます。

プログラムをアクティブ化するには、次のオプションがあります。

- アクティブ化キーを入力します。
アクティブ化キーを入力すると、ライセンスを使用して AntiVir プログラムがアクティブになります。
- **[製品のテスト]** オプションを選択します。

[製品のテスト] を選択すると、アクティブ化プロセス中に評価ライセンスが生成され、このライセンスによりプログラムがアクティブ化されます。AntiVir プログラムの完全な機能を一定期間テストすることができます。

注意

[利用できる有効な hbedv.key ライセンス ファイル] オプションを使用すると、有効なライセンス ファイルを読み込むことができます。有効なアクティブ化キーを使用した製品のアクティブ化中に、ライセンス キーが生成され、AntiVir プログラムのディレクトリに保存されます。既に製品をアクティブ化し、AntiVir プログラムを再インストールする場合は、このオプションを使用します。

注意

AntiVir 製品の一部の販売バージョンでは、アクティブ化キーが既に製品に含まれています。このため、アクティブ化キーの入力は必要ありません。必要に応じて、アクティブ化キーはライセンス ウィザードに表示されます。

注意

プログラムをアクティブ化するために、Avira GmbH サーバーへの接続が確立されます。**[プロキシ設定]**の下で、プロキシサーバーによるインターネットリンクを設定できます。

- ▶ アクティブ化プロセスを選択し、**[次へ]** をクリックして確認します。

製品のアクティブ化

ダイアログ ボックスが開き、個人データを入力できます。

- ▶ データを入力し、**[次へ]** をクリックします。

データが Avira GmbH サーバーに送信され、スキャンされます。AntiVir プログラムがライセンスによりアクティブ化されます。

ライセンス データが、次のウィンドウに表示されます。

- ▶ **[次へ]** をクリックします。
- ▶ 次の章「**[利用できる有効な hbedv.key]** オプションの選択によるアクティブ化」はスキップします。

[利用できる有効な hbedv.key] オプションを選択します。

ライセンス ファイルを読み込むためのボックスが開きます。

- ▶ プログラムのライセンス データを含むライセンス ファイル hbedv.key を選択し、**[開く]** をクリックします。

ライセンス データが、次のウィンドウに表示されます。

- ▶ **[次へ]** をクリックします。

アクティブ化の完了またはライセンス ファイルの読み込み後の続行

プログラムの機能がインストールされます。インストールの進行状況がダイアログ ボックスに表示されます。

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 テクノロジー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 テクノロジー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 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。

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クリーンを実行します。

- ▶ **[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。プログラムのようにダイアログで、**[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 Premium**

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。

- **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。

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。

5 AntiVir Premium 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、リストを並べ替えられます。

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。

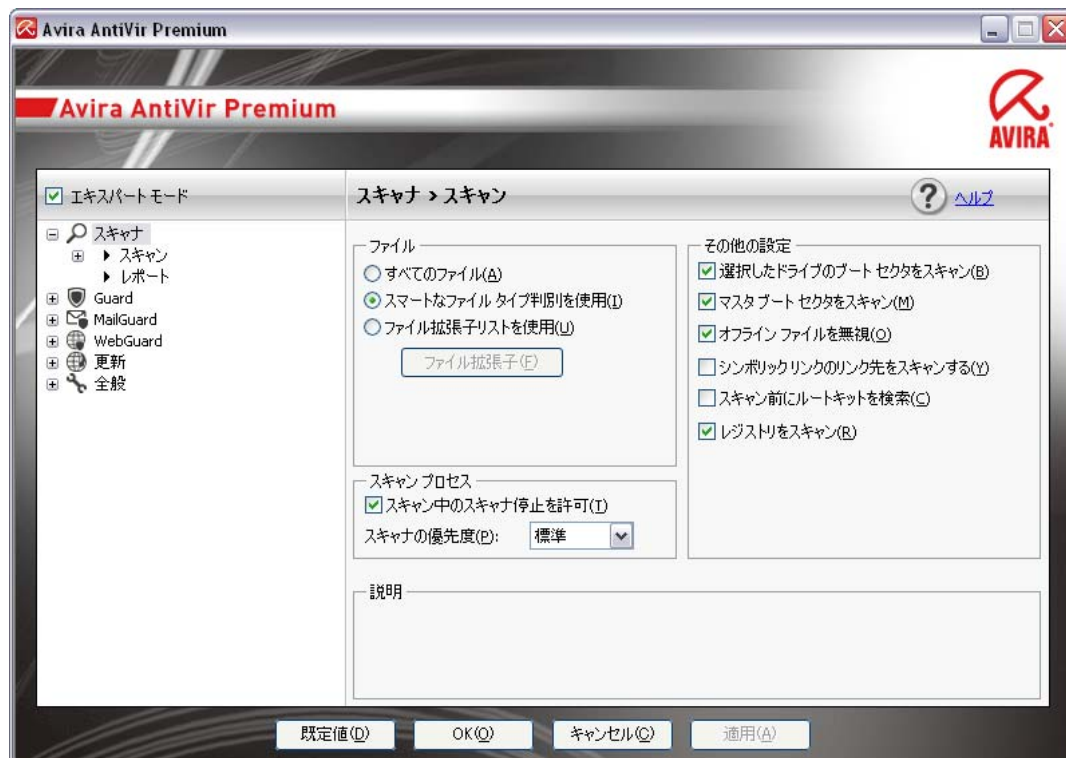
- ▶ 詳細ウィンドウの上部バーで適切なボタンをクリックして、オブジェクトを編集します。

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。
- **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

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

– **全般:**

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、製品の更新のセットアップ

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、
	AntiVir Guard が無効になり、

トレイ アイコンは、Guard 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。
- **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。
- **ヘルプ**: オンライン ヘルプを開きます。
- **バージョン情報 AntiVir Premium**: 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 製品をアクティブ化

AntiVir 製品をアクティブ化するには、以下のオプションがあります。

- 有効なフルライセンスによるアクティブ化
プログラムをフルライセンスでアクティブ化するには、購入したライセンスのデータが保存された有効なアクティブ化キーが必要です。アクティブ化キーは電子メールで送信されているか、製品パッケージに印刷されています。
- 評価ライセンスでのアクティブ化

AntiVir プログラムは、自動生成された評価ライセンスでアクティブ化されます。評価ライセンスを使用すると、AntiVir プログラムの完全な機能を一定期間テストすることができます。

注意

製品のアクティブ化やテスト ライセンスには、アクティブなインターネット接続が必要です。

Avira GmbH のサーバーへの接続が確立できない場合は、使用しているファイアウォールの設定を確認してください。製品のアクティブ化には、HTTP プロトコルとポート 80 を介した通信 (Web 通信) および SSL 暗号化プロトコルとポート 443 を介した通信が使用されます。ファイアウォールで受信データや送信データがブロックされていないことを確認してください。まず、Web ブラウザで Web ページにアクセスできるかどうかを確認してください。

以下に、AntiVir プログラムをアクティブ化する方法を示します。

AntiVir プログラムをインストールしていない場合:

- ▶ AntiVir プログラムをインストールします。
 - インストール中に、アクティブ化オプションの選択が要求されます。
 - **製品をアクティブ化**
= 有効なフル ライセンスでのアクティブ化
 - **製品のテスト**
= 評価ライセンスでのアクティブ化
- ▶ フル ライセンスでのアクティブ化には、アクティブ化キーを入力します。
- ▶ **[次へ]** をクリックして、アクティブ化手順の選択を確認します。
- ▶ 必要に応じて、登録用の個人データを入力し、**[次へ]** をクリックして確認します。

ライセンス データが、次のウィンドウに表示されます。これで、AntiVir プログラムが有効になりました。

- ▶ インストールを続行します。


AntiVir プログラムをまだインストールしていない場合:

- ▶ コントロールセンターで、メニュー項目 **[ヘルプ]::[ライセンス管理]** を選択します。

ライセンス ウィザードが開きます。ここでアクティブ化オプションを選択できます。製品のアクティブ化の次のステップは、上述の手順と同じです。

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 24 時間です。

- ▶ 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。
 [アップデート] 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。
 [アップデート] 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。
 [アップデート] 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 24 時間です。

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。

[Luce 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を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。

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。

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。

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: 感染したディスク 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 ウィ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た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。

– メールを送信をブロック (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/sample_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进行处理するには:

- ▶ 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

一度に 1 ファイルずつアップロードできます。


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
- 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まれ、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。

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をチェックされ、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せん。

更新は、24 時間 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、インターネットでメーカーの **Web** サーバーから取得できます。既存のネットワーク接続が、**Avira GmbH** のダウンロードサーバーの既定の接続です。この既定の設定は、全般::更新の下の設定で変更できます。

8 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。

8.1 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。
- 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。「」

更新を開始しようとする、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。

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)。

8.2 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。

8.2.1 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。

8.2.2 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。

8.2.3 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

[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

8.3 Windows セキュリティ センター

- Windows XP Service Pack 2 以降 -

8.3.1 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。

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

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。

ウイルス対策 見つかりません

このコンピュータでウイルス対策ソフトウェアが検出されませんでした。ウイルス対策ソフトウェアは、ウイルスやその他のセキュリティの脅威からコンピュータを保護するのに役立ちます。実行できる操作を表示するには、[推奨される対策案](#)をクリックしてください。[ウイルス対策ソフトウェアによるコンピュータの保護の詳細について表示します。](#)

注意: ウイルス対策ソフトウェアが Windows で検出されない場合もあります。

[推奨される対策案\(E\)...](#)

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。

ウイルス対策 最新の状態ではありません

ウイルス対策ソフトウェアが最新の状態に保たれていない可能性があります。実行できる操作を表示するには、[推奨される対策案](#)をクリックしてください。[ウイルス対策ソフトウェアによるコンピュータの保護の詳細について表示します。](#)

注意: ウイルス対策ソフトウェアが Windows で検出されない場合もあります。

インストールされているソフトウェア: AntiVir Desktop

[推奨される対策案\(E\)...](#)

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。

ウイルス対策 有効



ウイルス対策ソフトウェアは最新の状態に保たれ、ウイルス スキャンは有効になっています。ウイルス対策ソフトウェアは、ウイルスやその他のセキュリティの脅威からコンピュータを保護するのに役立ちます。[ウイルス対策ソフトウェアによるコンピュータの保護の詳細を表示します。](#)

インストールされているソフトウェア: AntiVir Desktop

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。

 ウイルス対策
無効 

ウイルス対策ソフトウェアは無効になっています。ウイルス対策ソフトウェアはウイルスやその他のセキュリティの脅威からコンピュータを保護するのに役立ちます。実行できる操作を表示するには、[推奨される対策案]をクリックしてください。[ウイルス対策ソフトウェアによるコンピュータの保護の詳細について表示します。](#)

注意: ウイルス対策ソフトウェアが Windows で検出されない場合もあります。

インストールされているソフトウェア: AntiVir Desktop

推奨される対策案(E)...

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、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。

 ウイルス対策
監視していません 

ユーザーが自分で管理するウイルス対策ソフトウェアを使用していることが指定されました。ウイルスやその他のセキュリティの脅威からコンピュータを保護するために役立てるため、ウイルス対策ソフトウェアが有効になっていて、最新の状態であることを確認してください。[ウイルス対策ソフトウェアによるコンピュータの保護の詳細を表示します。](#)

推奨される対策案(E)...

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となります。

9 ウイルスなど

9.1 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きます。

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ーを損害する、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。

9.2 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となります。バックドアによってユーザーの個人データが見つげ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点です。

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があります。

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

ファージングとは、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とらす操作です。従来のフィッシングがさらに発展したものです。ファージング詐欺師は、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。ファージングは、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があります。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。

10 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。

10.1 連絡先情報

Avira 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 Premium バージョン情報を参照してください。

10.2 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/premium-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 Premium 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 Premium 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。**

10.3 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-pe@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/sample_upload

10.4 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-pe@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)。

10.5 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-pe@avira.jp

11 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。

11.1 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。

11.1.1 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変更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。変更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。

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。

シンボリック リnk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nk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nk (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。

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。

11.1.1.1. 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

スキャナの通知では、既定で '[隔離] に移動' アクションがあらかじめ選択されます。その他のアクションは、コンテキストメニューを介して選択できます。

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。

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。こ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。こ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。

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。

11.1.1.2. 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ヤ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ヤ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ヤ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: スキヤン対象から除外するファイル オブジェクト: D:\ = D:\file.txt は、スキヤナのスキヤン対象から除外されますが、D:\folder\file.txt はスキヤン対象から除外されません。

11.1.1.3. ヒューリスティック

この設定セクションには、スキヤン エンジンのヒューリスティック スキヤ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 スキヤ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。スキヤ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 スキヤ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 テクノロジー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。

11.1.2 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。

11.2 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。

11.2.1 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。

11.2.1.1. 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。

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。

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。

11.2.1.2. 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。

11.2.1.3. 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。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、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

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

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。

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らず、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。

11.2.1.4. 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 テクノロジー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。

11.2.2 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け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。

11.2.2.1. 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せんを参照)。

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。

11.2.2.2. 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。

11.2.3 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。

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。

11.3 MailGuard

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

11.3.1 スキャン

受信電子メールのウイルス、マルウェア、のスクキャンには、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 でスクキャンできます。

スクキャン

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ク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クキャンされます。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。

受信メールのスクキャン

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、マルウェアのスク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。

11.3.1.1. 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。

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。

11.3.1.2. 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。

11.3.1.3. 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。

11.3.2 全般

11.3.2.1. 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せん。

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。

11.3.2.2. 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。

11.3.3 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正積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。

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。

11.4 WebGuard

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

11.4.1 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-Frame 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。

11.4.1.1. 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。

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。

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。

11.4.1.2. 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。

11.4.1.3. 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。

11.4.1.4. 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 テクノロジー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。

11.4.2 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せん。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。

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。

11.5 更新

[更新] セクションで、更新の自動受信を設定できます。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。

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。

11.5.1 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、アップデート 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。再起動が不要な場合は、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ち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ト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、アップデート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。

11.5.2 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::製品の更新の下で設定で、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。

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、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。

アップデートにより、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ト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。

11.6 全般

11.6.1 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)
- ダイアラ (DIALER)
- ゲーム (GAMES)
- ジョーク (JOKES)

- セキュリティプライバシーリスク (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。

11.6.2 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	機能
----------------	----

いる領域	
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。
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。
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。

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。
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。
インストーラ/アンインストーラ	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。

11.6.3 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) が変更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。

11.6.4 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

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。

11.6.5 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

11.6.6 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。

11.6.7 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。

11.6.8 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。

11.6.9 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。

11.6.10 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。

そのすべてのブランド名および製品名は、それぞれの所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.



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>