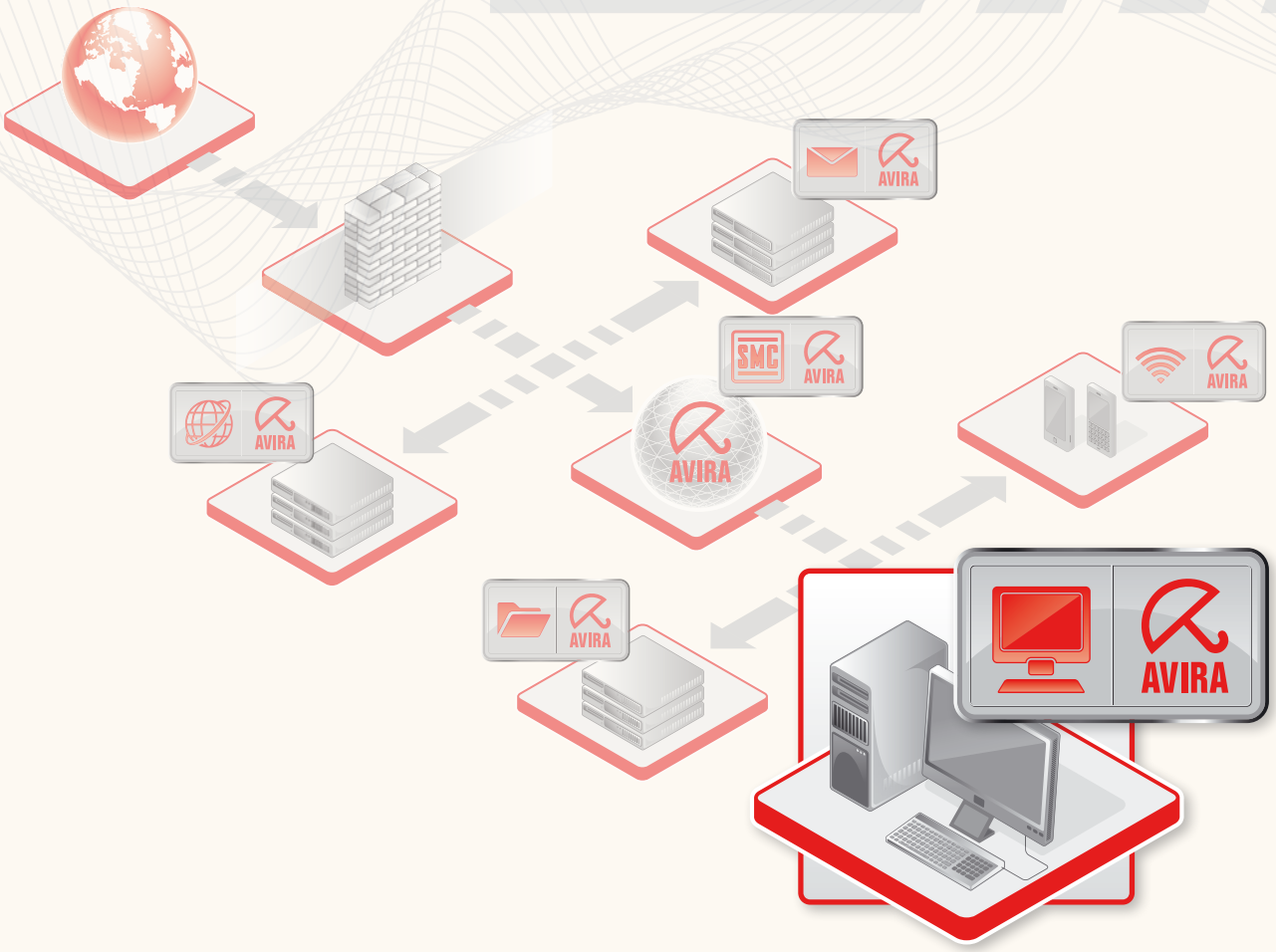
AVIRA
More Than Security

ユーザー マニュアル

Avira AntiVir Professional



www.promark-inc.com

商標と著作権

商標

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

著作権情報

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

目次

1 はじめに

Avira GmbH の Avira AntiVir Professional は、コンピュータをウイルス、マルウェア、アドウェア、スパイウェア、不要なプログラム、およびその他の危険から保護します。 このマニュアルでは、ウイルスとソフトウェアについて簡単に説明します。

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。

弊社 Web サイト http://www.avira.jp にアクセスしてください。 ここでは、PDF 形式の Avira AntiVir Professional マニュアルのダウンロード、Avira AntiVir Professional の更新、またはライセンスの更新が可能です。

弊社 Web サイトでは、テクニカル サポート用の電話番号や弊社ニュースレターの購読方法などの情報も入手できます。

Avira GmbH 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
✓	実装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	特に重要な情報、または Avira AntiVir Professional 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
草書体	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、またはボタンなど)

3 製品情報

この章には、Avira AntiVir Professional 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」の章参照。
- 「システム要件」の章参照。
- 「使用許諾」の章参照。
- 「ライセンス マネージャ」の章参照。

Avira AntiVir Professional は、ウイルス、マルウェア、不要なプログラム、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
貴重なデータの損失は、通常、大きな結果につながります。 最高のウイルス防止プログラムでも、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
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、不要な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。 Avira AntiVir Professional が自動更新で最新になっていることを確認してください。 それに従ってプログラムを構成します。

3.1 提供範囲

Avira AntiVir Professional では、次の機能が提供されます。

- 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高度なオプション、および状況依存のヘルプを使用した中央構成
- 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構成可能な検索を提供する 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
- 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 AntiVir WebGuard
- 疑わしいファイルを隔離して処理する統合された Quarantine 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
  (32 ビット システムに対してのみ)
- 検出されたウイルスとマルウェアに関する詳細情報へのインターネットによる直接アクセス
- インターネットまたはイントラネットでの Web サーバーを介した単一ファイル更新と増分 VDF 更新によるプログラム、ウイルス定義、および検索エンジンに対する簡単ですばやい更新
- ライセンス マネージャでのわかりやすい使用許諾
- 更新やテストの実行など、 1 回限り、または定期的なタスクを計画するための統合された スケジューラ
- ヒューリスティック スキャン方式を含む革新的なスキャン テクノロジ (スキャン エンジン) に基づく、非常に高いウイルスとマルウェアの検出率
- ネストされたアーカイブとスマート拡張の検出など、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

Avira AntiVir Professional が完全に機能するには、コンピュータ システムが次の要件を満たしている必要があります。

- Pentium 以上、最低 266 MHz
- オペレーティング システム
- Windows 2000 SP4 およびロールアップ修正プログラム 1、または
- Windows XP SP2 (32 ビットまたは 64 ビット)、または
- Windows Vista (32 ビットまたは 64 ビット、SP 1 推奨)、または
- Windows 2000 Server SP4 およびロールアップ修正プログラム 1、または
- Windows Server 2003 SP1 (32 ビットまたは 64 ビット)、または
- Windows Server 2008 (32 ビットまたは 64 ビット、SP1 推奨)
- 100 MB 以上のハード ディスク空き容量 (Quarantine 機能を使用する場合は、さらに空き容量が必要です)
- 192 MB 以上の RAM (Windows 2000/XP/ Windows 2000 Server の場合)
- 512 MB 以上の RAM (Windows Vista、Windows Server 2003、Windows Server 2008 の場合)
- Avira AntiVir Professional 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)

Windows Vista ユーザーの場合

Windows 2000 および Windows XP では、多数のユーザーが管理者権限で作業を行います。 ただし、ウイルスや不要なプログラムがコンピュータに侵入しやすくなるため、セキュリティの観点からはこれは望ましくありません。

このため、Microsoft は、Windows Vista では "ユーザー アカウント コントロール" を導入しています。 これは、管理者としてログインしているユーザーにより強い防止策が提供されます。 このため、Windows Vista で管理者は最初は通常のユーザーの権限しか持つことができません。 アクションに対して管理者権限が必要な場合、Windows Vista では情報アイコンによってはっきりと示されます。 さらに、ユーザーは必要なアクションを明示的に確認する必要があります。 単に特権が増加するだけで、管理業務は許可が取得されるとオペレーティング システムによって実行されます。

Avira AntiVir Professional には、Windows Vista の一部のアクションで管理者権限が必要です。 これらのアクションには、次の記号が付いています。 . このシンボルがボタン上にも表されている場合、このアクションの実行には管理者権限が必要です。 現在のユーザー アカウントに管理者権限がないと、Windows Vista のユーザー アカウント コントロールのダイアログで、管理者のパスワードを入力するように要求されます。 管理者パスワードがないと、このアクションは実行できません。

3.3 使用許諾

Avira AntiVir Professional を使用するには、ライセンスが必要です。 その場合、Avira AntiVir Professional のライセンス条件を受け入れる必要があります。

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

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

3.3.1 ライセンス マネージャ

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

Avira AntiVir Professional ライセンス マネージャ

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

注

Avira AntiVir Professional ライセンス マネージャは、対応するライセンスを関連する製品フォルダに自動的にコピーします。 ライセンスが既に存在する場合は、既存のライセンス ファイルを上書きするかどうかを確認するメッセージが表示されます。 その場合、既存のファイルは、hbedv.old という名前に変更されます。

4 インストールとアンインストール

この章には、Avira AntiVir Professional 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」の章参照。
- 「インストール モジュール」の章参照。
- 「変更のインストール」の章参照。
- ネットワーク上でのインストールとアンインストール
- 「アンインストール : アンインストール」の章参照。

4.1 インストール

Avira AntiVir Professional をインストールする前に、コンピュータが最小システム要件を満たしているか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、Avira AntiVir Professional をインストールできます。

注
Windows XP の場合、Avira AntiVir Professional は、Avira AntiVir Professional のインストール前にコンピュータに復元ポイントを生成します。 このため、インストールに失敗しても、安全に Avira AntiVir Professional を削除できます。 このため、[スタート | 設定 | コントロール パネル | システム | システムの復元] で、**[システムの復元を無効にする]** オプションはオンにしないでください。
[スタート | プログラム | アクセサリ | システム ツール | システムの復元] で、システムを前の状態に復元できます。 Avira AntiVir Professional によって生成される復元ポイントは、AntiVir Professional のエントリによって示されます。

インストールの種類

インストール中、インストール アシスタントで、セットアップの種類を選択できます。

フル

AntiVir Professional が、すべてのプログラム コンポーネントと共に完全にインストールされます。 プログラム ファイルは、`C:\Program Files` の下の既定の標準フォルダにインストールされます。

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。

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の終了も推奨されます。
- ▶ 他のウイルス防止ソリューションがインストールされていないことを確認してください。 さまざまなセキュリティ ソリューションの自動保護機能が相互に干渉する可能性があります。
- ▶ インターネット接続を確立します。 インターネット接続は、次のインストール手順を実行するときに必要になります。
- ▶ インストール プログラムを介して最新のプログラム ファイル、検索エンジン、ウイルス定義ファイルをダウンロードするとき (インターネット ベースのインストールの場合)
- ▶ インストールの完了後に AntiVir Professional の更新を行うとき (該当する場合)
- ▶ Avira AntiVir Professional をアクティブ化するためにライセンス ファイル hbedv.key をコンピュータ システムに保存するとき

注
インターネット ベースのインストール :
Avira GmbH では、インストールの前に Avira GmbH Web サーバーを使用して最新のプログラムを読み込む、Avira AntiVir Professional のインターネット ベースのインストールを実現するインストール プログラムを提供しています。 このプロセスにより、AntiVir Professional 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 Professional の言語を選択することはできません。 インストールが完了した後に、ウイルス定義ファイルを更新することをお勧めします。

インストール

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

最も重要なボタンには、次の機能が割り当てられています。

- – **OK:** アクションを確認します。
- – **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 Professional のインストール方法 :

- ▶ 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 Professional のインストールに使用する言語を選択し、**[次へ]** をクリックして言語の選択を確定します。

➔ *[ダウンロード]* ダイアログ ボックスが表示されます。 インストールに必要なすべてのファイルが Avira GmbH Web サーバーからダウンロードされます。ダウンロードが完了すると、*[ダウンロード]* ウィンドウが閉じます。

インストール パッケージを使用したインストール

➔ インストール ウィザードにより、*Avira AntiVir Professional* をインストールするためのダイアログ ボックスが開きます。

▶ *[確認 = 不明UIAHeAD の構成]* ダイアログ ボックスでは、AHeAD テクノロジの検出レベルを選択できます。 選択した検出レベルは、スキャナ (オンデマンド スキャン) および Guard (オンアクセス スキャン) の AHeAD テクノロジ設定に使用されます。

▶ 検出レベルを選択し、**[次へ]** をクリックしてインストールを続行します。

➔ 次の *[脅威カテゴリの拡張の選択]* ダイアログ ボックスでは、AntiVir Professional 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化し、*[次へ]* をクリックしてインストールを続行します。

▶ 必要なオプションを有効にし、*[次へ]* をクリックして構成を続行します。

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

▶ 必要に応じてサーバー設定を調整し、*[次へ]* をクリックして構成を続行します。

➔ 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。 ショート システム スキャンは、構成が完了した後からコンピュータが再起動されるまでの間に、実行中のプログラムおよび重要なシステム ファイルを対象にウイルスおよびマルウェアのスキャンを実行します。

▶ *[ショート 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]* をクリックして構成を続行します。

➔ 次のダイアログ ボックスでは、*[完了]* をクリックして構成を完了できます。

▶ *[完了]* をクリックして、構成を完了します。

➔ 指定および選択した設定が受け入れられます。

➔ *[ショート 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 によってショート システム スキャンが実行されます。

➔ *[インストールを閉じる]* ダイアログ ボックスが表示されます。

➔ Windows XP 上に AntiVir Professional をインストールした後で Windows ファイアウォールを無効にすると、コンピュータの再起動を促すメッセージ ウィンドウが表示されます。

▶ 必要があれば同意し、*[完了]* をクリックしてインストールを完了します。

インストールが正常に完了したら、AntiVir Professional 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 AntiVir Professional を更新して、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、フル 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 Avira AntiVir Professional インストールの個々のプログラム コンポーネントを追加または削除することができます (「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」の章参照)。

実際の Avira AntiVir Professional 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。

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

4.3 インストール モジュール

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

- **AntiVir Professional**
  このモジュールには、Avira AntiVir Professional 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 がバックグラウンドで実行されます。 オンアクセス モードの開く、書き込む、コピーなどの操作中に、必要に応じて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、Avira AntiVir Professional 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 MailGuard**
  MailGuard は、コンピュータと電子メール サーバーとのインターフェイスで、ここから電子メール プログラム (メール クライアント) が電子メールをダウンロードします。 MailGuard は、電子メール プログラムと電子メール サーバーとの間のプロキシとして接続されています。 すべての着信電子メールには、このプロキシを経由してウイルスと不要なプログラムを検索する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。 構成によって、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。 ウイルスや不要なプログラムが、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。AntiVir 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なプログラムを検出します。 構成によって、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 ルートキット検出***
  AntiVir ルートキット検出 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を確認します。
- **シェル拡張**
  Avira AntiVir Professional のシェル拡張は、Windows エクスプローラのコンテキスト メニュー (右マウスボタン) に、AntiVir で選択したファイルをスキャン のエントリを生成します。 このエントリで、ファイルまたはディレクトリを直接スキャンできます。

4.4 アンインストール

コンピュータから Avira AntiVir Professional 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。

Avira AntiVir Professional 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。

▶ **[Avira AntiVir Professional]** 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。

→ 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。

→ Avira AntiVir Professional 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、Avira AntiVir Professional のすべてのディレクトリ、ファイル、お

よびレジストリのエントリが削除されます。

4.5 ネットワーク上でのインストールとアンインストール

システム管理者による、複数クライアント コンピュータのネットワーク上の Avira AntiVir Professional のインストールを簡素化するため、Avira AntiVir Professional には最初のインストールと変更のインストールに特別の手順があります。

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

注
ネットワーク上での最初のインストールには、ライセンス ファイルが必要ですので注意してください。

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

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

ネットワーク上でのインストールとアンインストールに関する詳細 :

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

注
ネットワーク上での Avira AntiVir Professional のインストールとアンインストールには、AntiVir Security Management Center というもう 1 つの簡単なオプションがあります。 AntiVir Security Management Center を使用すると、ネットワーク上での AntiVir 製品 のリモート インストールとメンテナンスが実行できます。 詳細については、弊社 Web サイト http://www.avira.jp を参照してください。

4.5.1 ネットワーク上でのインストール

インストールは、バッチ モードでスクリプト制御が可能です。

セットアップは、次のインストールに適しています。

- ネットワークを介した初めてのインストール (無人セットアップ)

– シングル ユーザー コンポーネントのインストール

► 変更のインストールと更新

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

Avira AntiVir Professional をネットワーク上で自動的にインストールするには :

✓ 管理者権限が必要です (バッチ モードでも必要)

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

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

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

➔ インストールは自動的に開始します。

4.5.2 ネットワーク上でのアンインストール

ネットワーク上で Avira AntiVir Professional を自動的にアンインストールするには :

✓ 管理者権限が必要です (バッチ モードでも必要)

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

アンインストール ログに対するパラメータを指定することもできます。

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

➔ アンインストールは自動的に開始します。

4.5.3 セットアップ プログラムのコマンド ライン パラメータ

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

次のパラメータはインストールに使用できます。

– `/inf`

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

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

次のパラメータは、アンインストールに使用できます。

– `/remove`

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

例 : `presetup.exe /remove`

– `/remsilent`

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

例 : `presetup.exe /remsilent`

– `/remsilentaskreboot`

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

例 : `presetup.exe /remsilentaskreboot`

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

– `/unsetuplog`

アンインストール中のすべてのアクションがログに記録されます。

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

4.5.4 setup.inf ファイルのパラメータ

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

– `DestinationPath`

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

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

– `ProgramGroup`

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

1: プログラム グループを作成する

0: プログラム グループを作成しない

例 : ProgramGroup=1

– DesktopIcon

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

1: デスクトップ アイコンを作成する

0: デスクトップ アイコンを作成しない

例 : DesktopIcon=1

– ShellExtension

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

1: シェル拡張を登録する

0: シェル拡張を登録しない

例 : ShellExtension=1

– Guard

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

1: AntiVir Guard をインストールする

0: AntiVir Guard をインストールしない

例 : Guard=1

– MailScanner

AntiVir MailGuard をインストールします。

1: AntiVir MailGuard をインストールする

0: AntiVir MailGuard をインストールしない

例 : MailScanner=1

– KeyFile

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

例 : KeyFile=D:\inst\license\hbedv.key

– ShowReadMe

インストール後に readme.txt ファイルを表示します。

1: ファイルを表示する

0: ファイルを表示しない

例 : ShowReadMe=1

– RestartWindows

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

1: コンピュータを再起動する

0: コンピュータを再起動しない

例 : RestartWindows=1

– ShowRestartMessage

セットアップ中、自動再起動を実行する前に情報を表示します。

0: 情報を表示しない

1: 情報を表示する

例 : ShowRestartMessage=1

– SetupMode

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

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

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

例 : SetupMode=Update

– AVWinIni (オプション)

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

例 : AVWinIni=d:\inst\config\avwin.ini

– ScanMode

このオプションは、正常なインストール後、すべてのドライブのスキャンをアクティブ化します。

1: スキャンの開始

0: スキャンしない

例 : ScanMode=1

– Password

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

例 : Password=Password123

– WebGuard

AntiVir WebGuard をインストールします。

1: AntiVir WebGuard をインストールする

0: AntiVir WebGuard をインストールしない

例 : WebGuard=1

– RootKit

AntiVir ルートキット検出 モジュールをインストールします。 AntiVir ルートキット検出 を使用しないと、スキャナ は、システム上のルートキットを検索できません。

1: AntiVir ルートキット検出 をインストールする

0: AntiVir ルートキット検出 をインストールしない

例 : RootKit=1

5 AntiVir Professional の概要

この章には、AntiVir Professional 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」の章参照。
- 「方法」の章参照。

5.1 ユーザー インターフェイスと操作

AntiVir Professional 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 Professional の監視と制御
- Avira AntiVir Professional 構成: AntiVir Professional の構成
- 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 Professional の保護コンポーネントと機能を制御および操作するために設計されています。

コントロール センター のウィンドウは、**メニュー バー**、**ナビゲーション バー**、および詳細ウィンドウ**表示**という 3 つの領域に分割されています。

- **メニュー バー :** コントロール センター のメニュー バーで、AntiVir Professional 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られます。 個々のセクションには、AntiVir Professional のプログラム 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 **[状況]**。
- **表示 :** このウィンドウには、ナビゲーション領域で選択されたセクションが表示されます。 セクションに応じて、詳細ウィンドウの上部のバーに、機能やアクションを実行するボタンが表示されます。 データまたはデータ オブジェクトは個々のセクションのリストに表示されます。 リストの並べ替え方法を定義するボックスをクリックすると、リストを並べ替えできます。

コントロール センター の開始と終了

コントロール センター を開始するには、次のオプションが使用できます。

- 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] の AntiVir Professional プログラムのエントリ
- Avira AntiVir Professional 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
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化できます。 ナビゲーションがアクティブ化されると、矢印キーでメニュー内を移動できます。 [戻る] を使用して、アクティブなメニュー項目をアクティブ化できます。
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、Avira AntiVir Professional 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 Avira AntiVir Professional 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。
- The イベント セクションでは、特定の Avira AntiVir Professional 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、Avira AntiVir Professional によって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。
- スキャナ セクションでは、オンデマンド スキャンの構成と開始を簡単に行えます。 事前定義のプロファイルを使用すると、事前定義の既定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な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な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**ではコンピュータ システムをインターネットのウイルスやマルウェア、不正なネットワーク アクセスから保護するためのコンポーネントが提供されています。
- 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。
- AntiVir 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な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。
- Quarantine セクションには、Quarantine Manager が含まれています。 既に Qualantine に配置されているファイルや疑わしいファイルで Quarantine に配置したいファイルの中心点です。 選択したファイルを電子メールで Avira マルウェア リサーチ センター に送信することもできます。
- スケジューラ セクションでは、スケジュールされたスキャンと更新ジョブの構成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 構成

Avira AntiVir Professional 構成 では、AntiVir Professional の設定を実装できます。インストール後、AntiVir Professional は、ユーザーのコンピュータ システムに最適の保護が提供されるように標準設定で構成されますが、ユーザーのコンピュータ システムや AntiVir Professional に対する固有の要件により、AntiVir Professional の保護コンポーネントを調整する必要がある場合があります。

Avira AntiVir Professional 構成 によりダイアログ ボックスが開きます。 [OK] ボタンまたは [確認] ボタンをクリックすると、構成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。[既定値を復元] ボタンをクリックすると、既定の構成設定を復元できます。 個々の構成は、左側のナビゲーション バーで選択できます。

Avira AntiVir Professional 構成 へのアクセス

構成にアクセスするには、複数のオプションがあります。

- Windows のコントロール パネル。
- Windows のセキュリティ センター (Windows XP Service Pack 2 以降)。
- Avira AntiVir Professional のトレイ アイコン。
- Avira AntiVir Professional コントロール センター のメニュー項目 [その他] | [構成]。
- Avira AntiVir Professional コントロール センター の [構成] ボタン。

注
コントロール センター で **[構成]** 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構成登録に進みます。 個々の構成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化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。

Avira AntiVir Professional 構成 の操作

Windows エクスプローラと同じように、構成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構成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、構成セクションが展開され、ツリー構造に構成サブセクションが表示されます。
- 構成サブセクションを非表示にするには、展開された構成セクションの前のマイナス記号をクリックします。

注
Avira AntiVir Professional 構成 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
すべての構成セクションは、エキスパート モードでのみ表示できます。 すべての構成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化してください。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ベーション中に定義する必要があります。

構成の設定を確認するには :

- **[OK]** をクリックします。

→ 構成ウィンドウが閉じて、設定が受け入れられます。

- または -

- **[同意する]** をクリックします。

→ 設定が受け入れられます。 構成ウィンドウは開いたままになります。

設定を確認せずに、構成を終了する場合は :

- **[キャンセル]** をクリックします。

→ 構成ウィンドウが閉じて、設定は破棄されます。

すべての構成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。

→ すべての構成設定が既定値にリセットされます。 既定にリセットすると、すべての変更とカスタム エントリが失われます。

構成プロファイル

構成設定は構成プロファイルとして保存することができます。 構成プロファイルには、すべての構成オプションがグループ別に保存されます。 構成は、ナビゲーション バーにノードとして表示されます。 既定の構成に他の構成を追加することもできます。 トレイ アイコンのコンテキスト メニューを使用すると、複数の構成を手動で切り替えることができます。 特定の構成に切り替えるためのルールを定義することもできます。
ルールベースの手順を使用して構成を切り替える場合、LAN 接続またはインターネット接続 (既定のゲートウェイを介した識別) の使用に構成をリンクできます。 このようにして、異なるラップトップ使用シナリオに対して構成プロファイルを作成できます。

- 社内ネットワークでの使用 : イントラネット サーバーを介した更新、無効化された AntiVir WebGuard
- 家庭での使用 : 既定の Avira GmbH web サーバーを介した更新、有効化された AntiVir WebGuard

構成セクションでは、構成の追加、名前変更、削除、コピー、または復元を行ったり、ナビゲーション バーのボタンまたはコンテキスト メニューのコマンドを使用して構成を切り替えるためのルールを定義したりできます。

注
Windows 2000 では、別の構成への自動切り替えはサポートされません。Windows 2000 では、構成を切り替えるためのルールを定義できません。

構成オプションの概要

次の構成オプションが使用できます。

- **スキャナ**: オンデマンド スキャンの構成

  スキャン オプション

  懸念のあるファイルに対するアクション

  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 スキャンの構成

  スキャン オプション

  懸念のあるファイルに対するアクション

  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 の構成

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

  マルウェア対応アクション

MailGuard スキャン ヒューリスティック

MailGuard スキャンの例外

キャッシュの構成、空のキャッシュ

レポート機能の設定

– **AntiVir WebGuard**: AntiVir WebGuard の構成

スキャン オプション、AntiVir WebGuard の有効化/無効化

懸念のあるファイルに対するアクション

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)

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

AntiVir WebGuard ヒューリスティック

レポート機能の設定

– **全般** :

SMTP を使用した電子メールの構成

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 Avira AntiVir Professional 構成 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、フル システム スキャンの状態表示、製品の保護

WMI : WMI サポートの有効化

イベント ログの構成

レポート機能の構成

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構成、ダウンロード方法 (Web サーバーまたはファイル サーバーを介して)、製品の更新のセットアップ

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

マルウェア検出時の音声アラートの構成

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 Professional のトレイ アイコンが表示されます。

アイコン	説明

	AntiVir Guard が有効化され、
	AntiVir Guard が無効化されるか、

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

Avira AntiVir Professional 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 アイコンをマウスの右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 のアクティブ化**: Avira AntiVir Guard を有効化または無効化します。
- **AntiVir の起動**: Avira AntiVir Professional コントロール センター を開きます。
- **AntiVir の構成**: Avira AntiVir Professional 構成 を開きます。
- **更新の開始**: 更新を開始します。
- **ヘルプ** : このオンライン ヘルプを開きます。
- **インターネット上の Avira**: インターネット上の AntiVir Professional の Web ポータルを開きます。 これはインターネットにアクティブに接続されている場合に限られます。

5.2 方法...

5.2.1 ライセンスのアクティブ化

AntiVir Professional ライセンスをアクティブ化するには :

ライセンス ファイル hbedv.key を使用して、Avira AntiVir Professional のライセンスをアクティブ化します。 Avira GmbH から電子メールでライセンス ファイルが送信されます。 ライセンス ファイルには、1 つの注文プロセスで注文したすべての製品のライセンスが含まれています。

Avira AntiVir Professional をまだインストールしていない場合 :

▶ ライセンス ファイルをコンピュータのローカル ディレクトリに保存します。

▶ Avira AntiVir Professional をインストールします。

▶ インストール中に、ライセンス ファイルの保存場所を入力します。

Avira AntiVir Professional を既にインストールしている場合 :

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

- または -

▶ Avira AntiVir Professional コントロール センター で、メニュー項目 [ヘルプ] / [ライセンス ファイル] にアクセスします。

注
Windows Vista では、[ユーザー アカウント コントロール] ダイアログ ボックスが表示されます。 必要に応じて、管理者としてログインしてください。 **[続行]** をクリックします。

- ▶ ライセンス ファイルをハイライト表示させて、**[開く]** をクリックします。
- → メッセージが表示されます。
- ▶ **[OK]** をクリックして確認します。
- → ライセンスがアクティブ化されます。
- ▶ 必要に応じて、システムを再起動します。

5.2.2 Avira AntiVir Professional の自動更新

注
インターネット接続が利用可能で、インターネット接続が確立されている場合、更新ジョブは、Avira AntiVir Professional を 60 分 ごとに更新するようにプレインストールされています。

AntiVir Scheduler で Avira AntiVir Professional を自動的に更新するジョブを作成するには :

- ▶ コントロール センター で、**[マネージャ] :: [スケジューラ]** 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。
- → *[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。
- → *[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**
  - **ログイン時**

注
Avira AntiVir Professional は定期的かつ頻繁に、たとえば 60 分 ごとに更新することをお勧めします。

- ▶ 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します**

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。

→ *[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

▶ **[完了]** をクリックします。

→ 新たに作成したジョブは、**[マネージャ] :: スキャナ]** セクションの開始ページにアクティブ化の状況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化します。

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

Avira AntiVir Professional の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検索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] の下でアクティブ化されている場合のみ実行されます。

Avira AntiVir Professional の更新を手動で開始するには :

▶ マウスの右ボタンで、タスクバーの Avira AntiVir Professional のトレイ 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。

→ [*Avira AntiVir Professional アップデータ*] ダイアログ ボックスが表示されます。

- または -

▶ コントロール センター で、**[概要] :: [状況]** セクションを選択します。

▶ *[最終更新]* フィールドで、**[更新の開始]** リンクをクリックします。

➔ [Avira AntiVir Professional アップデータ] ダイアログ ボックスが表示されます。

- または -

▶ コントロール センター の **[更新]** メニューで、メニュー コマンド *[更新の開始]* を選択します。

➔ [Avira AntiVir Professional アップデータ] ダイアログ ボックスが表示されます。

注
Avira AntiVir Professional については、60 分 ごとなど、定期的な自動更新を強くお勧めします。

注
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。

– 事前定義のスキャン プロファイルを使用

事前定義のスキャン 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、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。 特定のアクションと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 センターおいてのみ実行できます。 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。 確認後、選択されたスキャン 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 で、**[ローカル保護] :: [スキャナ]** セクションを選択します。

➔ 事前定義のスキャン プロファイルが表示されます。

▶ 事前定義のスキャン 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。

– **[+]** 記号をクリック : 次のディレクトリ レベルが表示されます。

– **[-]** 記号をクリック : 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。

次のオプションが使用できます。 ディレクトリを選択します。

– 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は :

▶  **[新規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。

  次のオプションが使用できます。 ディレクトリを選択します。
  - – 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 : Dragamp;Drop を使用したウイルスとマルウェアのスキャン

Drag&Drop を使用してウイルスとマルウェアを体系的にスキャンするには :

✓ Avira AntiVir Professional の コントロール センター を開きます。

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

➔ *[Luke Filewalker]* ウィンドウが表示され、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 メニューを介したウイルスとマルウェアのスキャン

コンテキスト メニューを介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、マウスの右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 メニューで、**[AntiVir で選択したファイルをスキャン]** を選択します。

➔ *[Luke Filewalker]* ウィンドウが表示され、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

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、**[マネージャ] :: [スケジューラ]** 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。

→ *[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。

→ *[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。

→ *[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**
- **ログイン時**

▶ 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します**

  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。

→ *[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

▶ **[完了]** 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状況 (チェック マーク) と共に表示されます。

▶ 必要に応じて、実行されていないジョブを非アクティブ化します。

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：アクティブなルートキットに対象を絞ったスキャン

アクティブなルートキットをスキャンするには、事前定義の *[ルートキットのスキャン]* 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 で、**[ローカル保護] :: [スキャナ]** セクションを選択します。
- → 事前定義のスキャン プロファイルが表示されます。
- ▶ 事前定義の **[ルートキットのスキャン]** 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 Professional の個々の保護コンポーネントでは、*懸念のあるファイルに対するアクション*セクションの構成で、ウイルスまたは不要なプログラムを検出した場合に、AntiVir Professional にどう対処させるかを定義できます。

スキャナ のオプション：

– **対話式**

対話型アクション モードでは、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。 このオプションは既定で有効に設定されています。

ルートキット、起動セクタ ウイルスのスキャン中、および**アクティブ プロセスのスキャン中**、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。

ファイルのスキャン中、検出されたファイルの処理に関する通知および選択オプションは、選択されている通知モードに依存します。

通知モード：複合

複合通知モードでは、ファイル スキャンの完了時に、検出されたファイルのリストと共にアラートが出力されます。 検出されたファイルを処理するための選択オプションは用意されていません。 すべての感染したファイルに対して スキャナ の既定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。 感染したファイルに対する スキャナ の既定のアクションでは、該当するファイルが Quarantine に移動されます。

通知モード: 複合 (エキスパート)

エキスパート通知モードでは、ファイル スキャンの完了時に、検出されたファイルのリストと共にアラートが出力されます。 コンテンツ依存型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。

通知モード: 個別

個別通知モードでは、ファイル スキャン中に検出されたすべてのウイルスが別のウィンドウにレポートされます。 検出されたファイルの処理方法を選択できます。

– **自動**

自動アクション モードでは、ウイルスまたは不要なプログラムが検出されると、この領域で選択されているアクションが自動的に実行されます。 *[アラートの表示]* オプションを有効にした場合、ウイルスが検出されるたびに、実行されたアクションを示すアラートが表示されます。

Guard、MailGuard、AntiVir WebGuard のオプション :

– **対話式**

対話型アクション モードでは、ウイルスまたは不要な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。 このオプションは既定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なプログラムが検出されると、この領域で選択されているアクションが自動的に実行されます。 *[アラートの表示]* オプションを有効にした場合、ウイルスが検出されるたびに、実行されたアクションを示すアラートが表示されます。

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な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
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 Scanner、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 :

– **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のみ使用できます。

– **Quarantine 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 Quarantine ディレクトリ *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 Quarantine 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が、適切なツールで復元できます (*Avira UnErase* など)。 これにより、ウイルスの署名を復元することができます。 このプロセスは、*上書きと削除*よりはるかに高速です。 起動セクタ ウイルスが検出された場合、起動セクタを削除することで起動セクタ ウイルスを削除できます。 新しい起動セクタが書き込まれます。

– **上書きと削除**

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。 復元はできません。

– **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**

Avira AntiVir Professional は以降のアクションを実行しません。 感染したファイルは、コンピュータ上でアクティブなままになります。

警告
これはデータの損失とオペレーティング システムの損傷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。

– **アクセスの拒否**

Guard による検出に対するアクション オプション : 感染したファイルへのアクセスはブロックされます。 レポート機能が有効な場合、検出されたファイルがレポート ファイルに入力されるだけです。

– **Quarantine 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、Quarantine にコピーされます。

– **プログラムを終了する**

疑わしいプロセスの検出に対するアクション オプション : プロセスを終了します。 ダイアログ ボックスが表示され、実行可能ファイルの処理を選択できます。

MailGuard のアクション : 着信電子メール

– **Quarantine に移動**

電子メールはすべての添付ファイルと共に Quarantine 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 Quarantine 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 Quarantine Manager 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、ウイルスや不要なプログラムが、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 のアクション : 発信電子メール

– **Quarantine 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 Quarantine 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は、マルウェアを検索するスキャンが実行されます。

– **メールの送信をブロック (送信はしない)**

電子メールは電子メール クライアントの送信トレイに残っています。 電子メールプログラムでエラー メッセージを受信します。 電子メール アカウントから送信されるその他すべての電子メールには、マルウェアを検索する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
この方法はウイルスや不要な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。

AntiVir WebGuard のアクション :

– **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。

– **Quarantine 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 Quarantine 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 Quarantine Manager で復元できます。また、必要がある場合は、Avira マルウェア リサーチ 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 AntiVir 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、ウイルスや不要なプログラムが、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
修復できない疑わしいファイルはすべて Quarantine に移動することをお勧めします。

注
ヒューリスティックで報告されたファイルを弊社での分析用にお送りいただくこともできます。
たとえば、これらのファイルを弊社の Web サイトにアップロードすることもできます。http://www.avira.jp/support/upload
ヒューリスティック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 Quarantine: 隔離されたファイルの処理 (*.qua)

隔離されたファイルを処理するには :

- ▶ コントロール センター で、**[マネージャ] :: [Quarantine]** 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 :

Avira AntiVir Professional 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。 .

ファイルを分析用に Avira マルウェア リサーチ センター Web サーバーにアップロードするには :

► 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]**。

► Drücken Sie auf **OK.**

➥ ファイルが圧縮形式で Avira マルウェア リサーチ センター Web サーバーにアップロードされます。

注
次のケースに該当する場合は、Avira マルウェア リサーチ 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によるヒット (不審なファイル) : スキャン中、AntiVir Professional によってファイルが疑わしいと分類され、Quarantine 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 リサーチ センター でのファイルの分析が勧告された。
不審なファイル : ファイルを疑わしいと判断して Quarantine 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 Professional 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
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
複数のファイルを一度にアップロードするには、対象のファイルをすべて選択し、**[オブジェクトの送信]** ボタンをクリックします。

Quarantine のファイルは復元することもできます。

– 「Quarantine : Quarantine 内のファイルの復元」の章参照。

5.2.11 Quarantine: Quarantine 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、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。 特定のアクションと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 センターおいてのみ実行できます。 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。

Quarantine 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、**[マネージャ] :: [Quarantine]** セクションを選択します。

注
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
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、Quarantine 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 既定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認します。

➔ 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 Quarantine: 疑わしいファイルを Quarantine に移動

疑わしいファイルを手動で Quarantine に移動するには :

▶ コントロール センター で、**[マネージャ] :: [Quarantine]** セクションを選択します。

▶  をクリックします。

➔ Windows 既定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認します。

➔ ファイルは、Quarantine に移動されます。

Quarantine 内のファイルは、AntiVir Scanner を使用してスキャンできます。

- 「Quarantine : 隔離されたファイルの処理 (*.qua)」の章参照。

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 タイプをスキャンに追加、または特定のファイル タイプをスキャンから除外するには (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 の場合のみ可能):

✓ コントロール センター で、**[ローカル保護] ::** *[スキャナ]* セクションに移動します。

▶ マウスの右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 文字で、冒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？) は、置換する文字として許可されます。

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、Avira AntiVir Professional 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] ::** *[スキャナ]* 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

コントロール センター では、**[概要] :: イベント]** で、AntiVir Professional 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が表示されます。 (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
– Guard
– MailGuard
– スキャナ
– スケジューラ

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。

▶ アクティブ化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から除外

MailGuard のスキャン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。

→ リストに着信電子メールが表示されます。

▶ MailGuard のスキャン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なプログラムのスキャンを実行しません。

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

警告
送信者を完全に信頼できる場合のみ、電子メール アドレスを MailGuard のスキャンから除外してください。

注
[MailGuard] :: [全般] :: [除外] の構成で、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、ウイルスと不要な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 メニューを介したオンデマンド スキャン**
  コンテキスト メニューを介したオンデマンド スキャン (右のマウスボタンから **[AntiVir で選択したファイルをスキャン]**) 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推奨されます。 もう 1 つの利点は、コンテキスト メニューを介したオンデマンド スキャンでは、最初に Avira AntiVir Professional コントロール センター を開始する必要がないことです。
- **Drag&Drop 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 Avira AntiVir Professional 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推奨されます。
- 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推奨されます (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。
- **スケジューラ を介したオンデマンド スキャン**
  スケジューラ 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、起動セクタ 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。

- *[ルートキットのスキャン]* スキャン プロファイルを使用してルートキットをスキャンする。
- *[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する。
- **[その他]** メニューの **[起動セクタ ウイルスのスキャン]** メニュー コマンドを使用して起動セクタ ウイルスをスキャンする。

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検索エンジンがどれだけ新しいかによって異なります。 更新を行うために、AntiVir アップデータ が AntiVir Professional に統合されています。 AntiVir アップデータ により Avira AntiVir Professional 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。AntiVir 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 Professional 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。

– 検索エンジン :

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

– プログラム ファイル (製品更新):

製品更新の更新パッケージは、個々のプログラム コンポーネントに対して使用できる追加機能を作成します。

更新によって、ウイルス定義ファイルと検索エンジンが最新かどうかがチェックされ、必要に応じて更新が実装されます。 構成の設定により、AntiVir アップデータ は製品更新も実行するか、製品更新が利用可能であることを通知します。 更新後、AntiVir Professional を再起動する必要はありません。

注
セキュリティ上の理由から、Avira AntiVir Professional アップデータ は、コンピュータの Windows ホスト ファイルが改変され、たとえば、Avira AntiVir Professional 更新 URL がマルウェアに操作され、Avira AntiVir Professional 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 のホスト ファイルが操作されると、Avira AntiVir Professional アップデータ のレポート ファイルに表示されます。

スケジューラ の下の コントロール センター で、指定した間隔で AntiVir アップデータ が実行されるよう、更新ジョブを体系化できます。 更新ジョブは、AntiVir Professional のインストール後、既定で作成されます。 手動で更新を開始するオプションもあります。

– コントロール センター の場合 : [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

更新は、インターネットでメーカーの Web サーバーから、またはインターネットから更新ファイルをダウンロードするイントラネットのファイル サーバーから取得して、ネットワーク上の他のコンピュータで使用可能にすることができます。 これは、AntiVir Professional をネットワーク上の複数のコンピュータで更新する場合に便利です。 更新サーバーを使用すると、最低限のリソースで、関連するコンピュータの AntiVir Professional を最新状態にすることができます。

注

AntiVir Internet Update Manager (Windows のファイル サーバーまたは Web サーバー) をイントラネット上の Web サーバーまたはファイル サーバーとして使用できます。AntiVir Internet Update Manager は、Avira AntiVir 製品 (AntiVir Professional を含む) のダウンロード サーバーをミラーするもので、インターネット (http://www.avira.com) から入手できます。 ただし、イントラネットの中央ファイル サーバーを介したカスケードを使用して、ネットワーク上の関連するコンピュータで AntiVir Professional を更新することもできます。

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

8 FAQ、ヒント

この章には、Avira AntiVir Professional に関するさまざまなよくある質問 (FAQ)、トラブルシューティングのセクション、Avira AntiVir Professional を使用する際のヒントとコツが記載されています。

「トラブルシューティング」の章参照。

「キーボード コマンド」の章参照。

「Windows セキュリティ センター」の章参照。

8.1 トラブルシューティング

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、Avira AntiVir Professional のプログラム ディレクトリに保存する必要があります。「Avira AntiVir Professional ライセンス管理」も参照してください。

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

理由 : インターネット接続が非アクティブになっています。 このため、Avira AntiVir Professional は、インターネット上の Web サーバーを検索できません。

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

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が変更されていないかを確認し、必要に応じて構成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] の下で、Avira AntiVir Professional 構成 (エキスパート モード) の設定を確認してください。

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。

▶ Avira AntiVir Professional を更新します。

▶ Windows XP 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。

▶ Avira AntiVir Professional と Avira AntiVir Professional 構成 (エキスパート モード) を開始します。

▶ [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]** を押して確認します。

▶ 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化します。

トレイ アイコンの状況が無効になっています。

理由 : AntiVir Guard が非アクティブになっています。

▶ コントロール センター で、[概要] :: [状況] セクションをクリックし、[AntiVir Guard] フィールドを検索して、**[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構成で、AntiVir Guard を全般的に承認するように定義してください。 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。 これは、AntiVir MailGuard についても同じです。

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] 構成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。

▶ Avira AntiVir Professional 構成 (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 の報告をアクティベーション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 と AntiVir MailGuard を全般的に承認するように定義してください。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。 これは、AntiVir MailGuard についても同じです。

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 IMAP を介してメール サーバーと通信しているかを確認してください。 このプロトコルは、現在サポートされていません。

▶ メール クライアントが Kerberos、APOP、または RPA を介してサーバーにログインしているかどうかを確認してください。 これらの検証方法は、現在サポートされていません。

▶ メール クライアントが SSL (TSL - Transport Layer Security とも呼ばれる) を介してサーバーにログインしているかどうかを確認してください。 AntiVir MailGuard は SSL をサポートしていますが、暗号化された電子メールに対するウイルスや不要なプログラムのスキャンは実行しません。 これは、接続が通常の POP3 ポート 110 ではなく、ポート 995 を介して行われていることが条件です。 このポートはよく "代替ポート" とも呼ばれます。 大多数の電子メール サーバーは、このポートを介した SSL もサポートしています。

▶ AntiVir MailGuard サービスはアクティブになっていますか。 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] 構成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 Avira AntiVir Professional をアンインストールし、Avira AntiVir Professional 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

▶ AntiVir MailGuard は、現在 IMAP (Internet Message Access Protocol) をサポートしていません。 電子メールプログラムがこのプロトコルを使用して電子メール サーバーと通信すると、ウイルスまたは不要なプログラムに対して保護されません。

▶ SSL (Secure Sockets Layer、または TLS (Transport Layer Security) とも呼ばれる) を介した暗号化 POP3 接続には現在保護が行われず、無視されます。

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

▶ Avira AntiVir Professional は、発信電子メールのウイルスと不要なプログラムはチェックしません。

注
セキュリティ ギャップをなくすため、定期的に Microsoft の更新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 MailGuard ではサポートされていません。 電子メールの送信には、次のオプションが使用可能です。

▶ 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] の構成で、MailGuard による発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 : AntiVir WebGuard は、送信データが Web ブラウザに読み込まれる前に、ウイルスや不要な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、AntiVir 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 を例外として構成に入力します (Avira AntiVir Professional 構成: 「AntiVir 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、Avira AntiVir Professional を介したアクションを開始できます。

以下に Avira AntiVir Professional で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	次のセクションに移動します。

Ctrl + Shift + Tab Ctrl + Page up	前のセクションに移動します。
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化または非アクティブ化します。
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。
Shitf + 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。
F6	ナビゲーションとテーマのウィンドウを切り替えます。
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	構成を開く
F9	更新の開始

スキャナ 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の変更
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
Ins	新規プロファイルの作成
Del	選択したプロファイルの削除

Quarantine セクション

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

スケジューラ セクション

ショートカット	説明
F2	ジョブの編集
Return	プロパティ
Ins	新しいジョブを挿入
Del	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
Del	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
Del	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 Avira AntiVir Professional

ウイルス防止ソフトウェア/悪意のあるソフトウェアに対する保護

ウイルス防止に関して、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。

ウイルス対策が見つかりません

ウイルス対策期限切れ

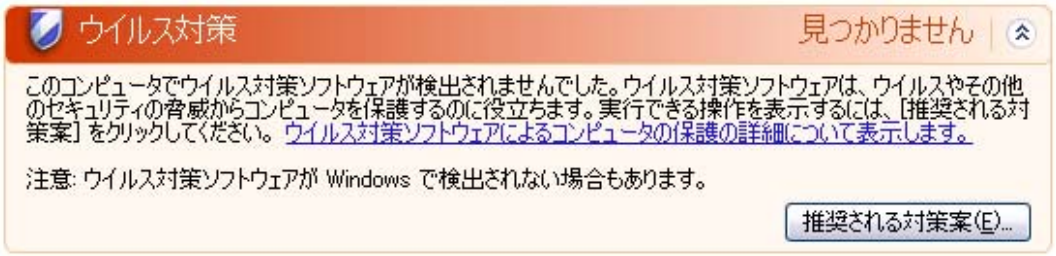
ウイルス対策有効

ウイルス対策無効

ウイルス対策 監視していません

ウイルス対策が見つかりません

コンピュータにアンチウイルス ソフトウェアが見つからないと、Windows セキュリティ センターからこの情報が表示されます。



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

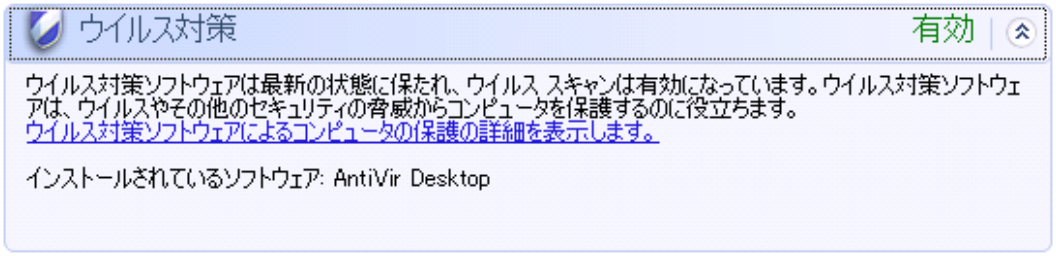
ウイルス対策期限切れ

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

注
Windows セキュリティ センターに Avira AntiVir Professional 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。 Avira AntiVir Professional の更新を実行して、システムを更新してください。

ウイルス対策有効

Avira AntiVir Professional 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。



Avira AntiVir Professional は最新状態になり、AntiVir Guard が有効になっています。

ウイルス対策無効

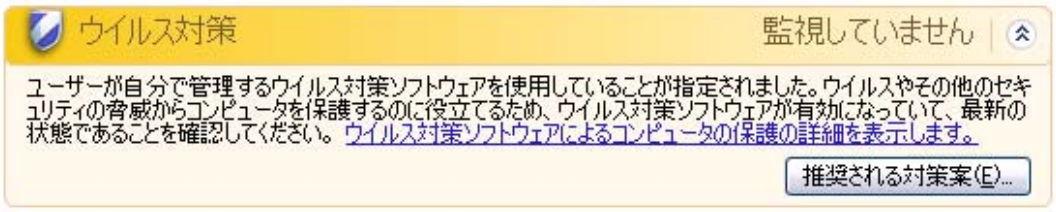
AntiVir Guard を無効にしたり、Guard サービスを停止すると、次のメッセージが表示されます。

注
AntiVir Guard を有効化/無効化するには、[概要] で Avira AntiVir Professional コントロール センター の状態を有効化/無効化します。 AntiVir Guard が有効になっているかどうかは、タスクバーで赤い傘が開いているかどうかでも確認できます。

ウイルス対策 監視していません

アンチウイルス ソフトウェアの監視を自分で実行しようとすると、Windows セキュリティ センターから次のメッセージが表示されます。

注
Windows Vista ではこの機能はサポートされません。



注
Windows セキュリティ センターは Avira AntiVir Professional でサポートされていません。 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
Windows XP Service Pack 2 または Windows Vista をインストールしていても、Avira AntiVir Professional などのウイルス対策は必要です。 Windows XP Service Pack 2 は、アンチウイルス ソフトウェアを監視しますが、それ自体がアンチウイルス機能を持っているわけではありません。 このため、別のアンチウイルス ソリューションを使用しないと、ウイルスやマルウェアに対して保護されないことになります。

9 ウイルスなど

9.1 脅威カテゴリの拡張

ダイヤラ (DIALERS)

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 への変更が設定されています)。 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保証されますが、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。 真正のダイヤラにはユーザーによって意図的に使用される余地はありません。 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。 真正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、真正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、気づかれずに疑わしい方法、または不正な意図で、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 で始まり、極端に高額な費用が発生することの多い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 (0190/0990 ダイヤラ) への対策として、この番号を直ちにブロックするよう依頼することをお勧めします。

Avira AntiVir Professional は、よく使用されるダイヤラを既定で検出します。

[脅威カテゴリの拡張] の構成でチェック 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、昼休み以外、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、会社の従業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まで含まれた "船隊演習" まで、さまざまなゲームが配布されています。 動きは電子メール プログラムを通じて、パートナーに伝達されるようになっています。

研究によると、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。

Avira AntiVir Professional は、コンピュータ ゲームを検出します。 [脅威カテゴリの拡張] の構成にチェック マークを入れて、**[ゲーム]** オプションを有効にすると、Avira AntiVir Professional 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。 簡単に削除できますから、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によるものの可能性もあります。 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、Avira AntiVir Professional 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なプログラムとして排除できます。 [脅威カテゴリの拡張] の構成にチェック 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への問題、不要なプログラムの活動の開始、プライバシへの損害、ユーザー活動の探り出しなどを行い、望ましくない可能性のあるソフトウェア。

Avira AntiVir Professional 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] の構成にチェック 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、Avira AntiVir Professional 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)

データを盗んだり、コンピュータを操作するため、バックドア サーバー プログラムは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 コントロール 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。

Avira AntiVir Professional は "バックドア制御ソフトウェア" を検出します。 [脅威カテゴリの拡張] の構成にチェック マークを入れて **[バックドア クライアント]** オプションを有効にすると、Avira AntiVir Professional 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)

広告を表示するソフトウェアや、ユーザーが気が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するために好ましくないソフトウェア。

Avira AntiVir Professional は "アドウェア/スパイウェア" を検出します。 [脅威カテゴリの拡張] の構成にチェック マークを入れて **[アドウェア/スパイウェア]** オプションを有効にすると、Avira AntiVir Professional 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。

通常とは異なるランタイム圧縮ツール (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。

Avira AntiVir Professional は "通常とは異なるランタイム圧縮ツール" を検出します。 [脅威カテゴリの拡張] の構成にチェック マークを入れて **[通常とは異なるランタイム圧縮ツール]** オプションを有効にすると、Avira AntiVir Professional が該当する圧縮ツール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)

本当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。 このカムフラージュ方法は、マルウェアによく使用されます。

Avira AntiVir Professional は "二重の拡張子ファイル" を検出します。 [脅威カテゴリの拡張] の構成でチェック マークを入れて **[二重の拡張子ファイル]** (HEUR-DBLEXT) を有効にすると、Avira AntiVir Professional 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窃盗を巧妙な手段で行うものです。
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。

Avira AntiVir Professional は、"フィッシング" を検出します。 [脅威カテゴリの拡張] の構成にチェック 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、Avira AntiVir Professional がこのような行為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、使用された場合にリスクが生じる可能性があるか、ソースが疑わしいアプリケーションについて言及される場合に使用されます。

Avira AntiVir Professional は、"アプリケーション (APPL)" を検出します。 [脅威カテゴリの拡張] の構成でチェック 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、Avira AntiVir Professional がこのような行為を検出した場合に、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、使用行動に関する多数の結論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 メカニズムの周辺から、コンピュータへのアクセスを取得します。

バックグラウンドで実行されるプログラムは、通常、攻撃者に無制限の権限を与えることになります。 バックドアによってユーザーの個人データが見つけ出される可能性もありますが、バックドアは主として関連システムに、コンピュータ ウイルスやワームをさらにインストールするために使用されます。 接続データから、使用行動に関する多数の結論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。

ブート ウイルス

ハード ディスクの起動セクタ、またはマスタ起動セクタは、主として起動セクタ 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、一部は感染した PC のユーザーの気づ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能力は、ネットワークが数千台規模のコンピュータをアーカイブできるため、データ転送量の合計が大多数の従来のインターネット アクセスを爆発させるということです。

エクスプロイト

エクスプロイト (セキュリティ ギャップ) とは、コンピュータ システムのバグ、誤作動、脆弱性、特権の昇格、サービス拒否などを利用したコンピュータ プログラム、またはスクリプトです。 たとえば、エクスプロイトの 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。 より高いアクセスを取得するために、プログラムが侵入する場合もあります。

デマウイルス - Scherz、Schabernack、Ulk)

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たサービス (プログラムまたはサーバー) です。 ネットワークやプロトコル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、そのユーザーが特定されることはありません。 攻撃者は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て、ログに記録し、アラートを起動します。

マクロ ウイルス

マクロ ウイルスとは、WinWord 6.0 の場合の 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。 アクティブにするには、対応するアプリケーションがアクティブ化されていて、感染したマクロのいずれかが実行される必要があります。 "通常の" ウイルスとは異なり、マクロ ウイルスは実行ファイルの攻撃は行いませんが、対応するホスト アプリケーションの文書を攻撃します。

ファーミング

ファーミングとは、Web ブラウザのホスト ファイルを操作して、照会を偽装ウェブサイトにそらす操作です。 従来のフィッシングがさらに発展したものです。ファーミング詐欺師は、偽装 Web サイトが保存されている独自の大型のサーバー ファームを操作します。 ファーミングは、さまざまな DNS 攻撃の包括的な用語として確立しています。 ホスト ファイルの操作の場合、システムの具体的な操作は、トロイの木馬やウイルスを使用して実行されます。 その結果、正しい Web アドレスが入力されても、システムは偽装 Web サイトにしかアクセスできなくなります。

フィッシング

フィッシングとは、インターネット ユーザーの個人データを釣るという意味です。 フィッシング詐欺師は、通常、犠牲者に電子メールなどで一見正式に思われるレターを送信し、犯罪者を信用して、特に、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。 盗んだアクセスの詳細から、フィッシング詐欺師は犠牲者の ID を使用して自ら取引を実行します。 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宿主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、侵入者がログインを隠し、プロセスを非表示にし、データを記録し、つまり見えない状態でコンピュータ 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 ツールの集合体です。 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地球全体に数時間で広がります。

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

ワームとは、それ自体が増殖するプログラムですが、宿主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商売上の利益に利用す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、大多数には面白そうな名前 (SEX.EXE、STARTME.EXE など) が付いています。 実行すると直ちに、アクティブ化され、ハード ディスクをフォーマットする場合もあります。 埋め込み型とは、ウイルスを "埋め込む" トロイの木馬の特殊な形態で、コンピュータ システムにウイルスを埋め込みます。

ゾンビ

ゾンビ PC とは、マルウェア プログラムに感染して、ハッカーがリモート コントロールで犯罪目的に利用できるコンピュータです。 コマンドによって、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」の章参照。

「テクニカル サポート」の章参照。

「不審なファイル」の章参照。

「誤検出報告」の章参照。

「フィードバックの送付」の章参照。

10.1 連絡先住所

Avira AntiVir Professional 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。 弊社の連絡先住所については、コントロール センター の 「ヘルプ :: Avira AntiVir Professional バージョン情報」を参照してください。

10.2 テクニカル サポート

Avira AntiVir Professional 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 http://www.avira.jp/support から入手可能です。

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、Avira AntiVir Professional コントロール センター のメニュー項目 [ヘルプ] :: [AntiVir Professional バージョン情報] :: [ライセンス情報] で確認できます。
- **バージョン情報**。 この情報は、Avira AntiVir Professional コントロール センター のメニュー項目 [ヘルプ] :: [AntiVir Professional バージョン情報] :: [バージョン情報] 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 : 他のベンダーのアンチウイルス 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 不審なファイル

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不審な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。

- Quarantine Manager では、コントロール センター ファイルを選択し、コンテキスト メニューを使用するか、対応するボタンを使用して、[ファイルの送信] 選択してください。
- 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 virus@avira.jp 宛にお送りください。 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。

10.4 誤検出報告

Avira AntiVir Professional から "クリーン" だと思われるファイルについて報告を受けた場合、該当するファイルを圧縮して (WinZIP、PKZip、Arj など) 電子メールの添付ファイルとして virus@avira.jp 宛にお送りください。 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

お客様のセキュリティは、Avira にとって大変重要です。 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 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、率直に対処いたします。

弊社製品にセキュリティ ギャップが検出された場合は、vulnerabilities@avira.jp 宛に電子メールをお送りください。

11 参照：構成オプション

構成の参考資料には、Avira AntiVir Professional で使用可能なすべての構成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 スキャンの構成には、Avira AntiVir Professional 構成 の スキャナ セクションが関与しています。

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、構成に従って、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して (優先度)
- 起動セクタとメイン メモリも含めて
- 特定のセクタまたはすべての起動セクタとメイン 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、特定の拡張子 (タイプ) を持つファイルのみをスキャンするフィルタを使用できます。

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ウイルスまたは不要なプログラムを検索するスキャンが実行されます。フィルタは使用できません。

注

[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。

スマート拡張

このオプションを有効にすると、ウイルスまたは不要なプログラムに関するスキャンを実行するファイルの選択が、Avira AntiVir Professional によって自動的に行われます。これは、Avira AntiVir Professional 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。この設定は既定でアクティブ化されている推奨設定です。

注
[スマート拡張] を有効にすると、**[ファイル拡張子]** 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、指定された拡張子を持つファイルのみがスキャンされます。ウイルスや不要な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定義されます。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
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

このボタンでダイアログ ウィンドウが開き、**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
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起動セクタをスキャン

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起動セクタのみをスキャンします。このオプションは既定で有効に設定されています。

マスタ起動セクタをスキャン

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起動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なプログラムを検索する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、 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。このオプションは既定で有効に設定されています。

システム ファイルの完全性チェック

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

最適化スキャン

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により、最適化スキャンのログは、標準レベルでのみ記録されます。

注
このオプションは、マルチ プロセッサ システムでのみ利用できます。AntiVir Professional を SMC で管理している場合、このオプションが常に表示され、有効化できるようになっています。管理対象のシステムに、複数のプロセッサが搭載されていない場合、スキャナ オプションは使用されません。

シンボリック リンクに従う

このオプションを有効にすると、スキャナ はスキャン プロファイル、または選択したディレクトリのすべてのシンボリック リンクに従ってスキャンを実行し、リンクされたファイルにウイルスとマルウェアに関するスキャンを実行します。このオプションは、Windows 2000 ではサポートされていないため非アクティブ化されます。

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 システムにおいて透過的で、シンボリック リンク (mklink.exe によって生成)、または接合ポイント (junction.exe によって生成) のみを参照します。

スキャン前にルートキットをスキャン

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
64 ビット システムでは、ルートキット スキャンはまだ使用できません

ネットワーク ドライブ上のファイルまたはパスをスキャンしない

このオプションを有効にすると、コンピュータに接続されたネットワーク ドライブはオンデマンド スキャンから除外されます。このオプションは、Avira AntiVir Professional が他のワークステーションにインストールされている場合など、サーバーまたは他のワークステーション自体がアンチウイルス ソフトウェアで保護されている場合に推奨されます。このオプションは既定で無効に設定されています。

スキャン プロセス

中止の許可

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、ウイルスや不要なプログラムに関する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。このオプションは既定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します。

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実行が継続します。この設定は既定でアクティブ化されている推奨設定です。

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す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. 懸念のあるファイルに対するアクション

懸念のあるファイルに対するアクション

ウイルスまたは不要な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。

対話式

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。ルートキットのスキャン中、起動セクタ ウイルスのスキャン中、およびアクティブ プロセスのスキャン中、ダイアログ ボックスが表示され、検出されたオブジェクトをどう処理するかを選択できます。ファイルのスキャン中、検出されたファイルの処理に関する通知および選択オプションは、選択されている通知モードに依存します。このオプションは既定で有効に設定されています。

許可されるアクション

この表示ボックスで、個別通知モードまたはエキスパート通知モードでウイルスが検出された場合に、ダイアログ ボックスで選択できるアクションを指定できます。これに対応するオプションをアクティブ化する必要があります。

修復

スキャナ は、可能な場合、感染したファイルを修復します。

名前の変更

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

Quarantine

スキャナ はファイルを Quarantine に移動します。情報として価値がある場合、ファイルは、Quarantine Manager から復元できます。 また、必要がある場合は、Avira マルウェア リサーチ センター に送信できます。ファイルによっては、Quarantine Manager で他の選択オプションも利用可能です。

削除

ファイルは削除されますが、関連するツール (Avira UnErase など) で必要があれば復元できます。ウイルスのパターンは、再度検出可能です。このプロセスは、"上書きと削除" よりはるかに早くなります。

無視

無視するファイル。

上書きと削除

スキャナ はファイルを既定のパターンで上書きしてから削除します。復元はできません。

既定値

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

注
修復アクションを既定のアクションとして選択することはできません。

注
[削除] または *[上書きと削除]* を既定のアクションとして選択したうえで、通知モードを複合通知モードに設定する場合は、次の点に注意する必要があります。ヒューリスティックによるヒットの場合、感染したファイルは削除されず、Quarantine に移動されます。

詳細については、こちらをクリックしてください。

通知モード

通知モードでは、スキャナ によるファイル スキャンでウイルスが検出された場合に、どのような形で報告するかを定義します。通知モードを使用することにより、検出ファイルに適用する処理を、いくつかの選択肢の中から選べるようにすることができます。

複合

複合通知モードでは、ファイル スキャンの完了時に、検出されたファイルのリストと共にアラートが出力されます。検出されたファイルを処理するための選択オプションは用意されていません。すべての感染したファイルに対して スキャナ の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。感染したファイルを処理する スキャナ の既定のアクションでは、該当するファイルが Quarantine に移動されます。

複合 (エキスパート)

エキスパート通知モードでは、ファイル スキャンの完了時に、検出されたファイルのリストと共にアラートが出力されます。コンテンツ依存型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。

個別

個別通知モードでは、ファイル スキャン中に検出されたすべてのウイルスが別のウィンドウにレポートされます。検出されたファイルの処理方法を選択できます。

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なプログラムの検出後、アクションを選択するダイアログ ボックスは表示されません。スキャナ は、このセクションで定義した設定に従って動作します。

アクション前にファイルを Quarantine にコピー

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、Quarantine 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 リサーチ センター に送信することもできます。

警告メッセージの表示

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

プライマリ アクション

プライマリ アクションとは、スキャナ がウイルスまたは不要なプログラムを検出した場合に実行されるアクションです。**[修復]** オプションが選択されていて、関与するファイルの修復が不可能な場合、**[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

[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

自動修復が推奨されますが、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が、必要があれば適切なツール (Avira UnErase など) で復元できます。これはウイルスのパターンが再度検出可能であることを意味します。このプロセスは、[上書きと削除] よりはるかに早くなります。

上書きと削除

このオプションを有効にすると、スキャナ はファイルを既定のパターンで上書きしてから削除します。復元はできません。

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アクティブなままになります。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。

Quarantine

このオプションを有効にすると、スキャナ はファイルを Quarantine に移動します。このファイルは後で復元したり、必要があれば Avira マルウェア リサーチ 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]** が**[プライマリ アクション]** の下で選択されている場合のみ選択できます。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が、必要があれば適切なツール (Avira UnErase など) で復元できます。これはウイルスのパターンが再度検出可能であることを意味します。このプロセスは、[上書きと削除] よりはるかに早くなります。

上書きと削除

このオプションを有効にすると、スキャナ はファイルを既定のパターンで上書きしてから削除 (ワイプ) します。復元はできません。

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アクティブなままになります。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。

Quarantine

このオプションを有効にすると、スキャナ はファイルを Quarantine に移動します。このファイルは後で復元したり、必要があれば Avira マルウェア リサーチ センター に送信できます。

注

[削除] または **[上書きと削除]** 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によるヒットの場合、感染したファイルは削除されず、Quarantine に移動されます。

11.1.1.2. 以降のアクション

検出の後にプログラムを起動

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

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

プログラム名

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

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

引数

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

イベント ログ

イベント ログの使用

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

アーカイブをスキャンする場合、スキャナ は再帰スキャンを使用します。アーカイブ内のアーカイブも解凍され、ウイルスと不要なプログラムを検索する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。このオプションは既定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。

スマート拡張

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

注
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。

再帰の深さを制限

再帰の深いアーカイブの解凍とスキャンには、かなりのコンピュータの使用時間とリソースが必要です。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深さを特定の圧縮レベルに制限します (最大の回帰の深さ)。これにより、コンピュータの使用時間とリソースが節約できます。

注
アーカイブでウイルス、または不要なプログラムを検出するには、スキャナ がウイルスまたは不要なプログラムが配置されている再帰レベルまでスキャンする必要があります。

最大の再帰の深さ

最大の再帰の深さを入力するには、[再帰の深さを制限] を有効にする必要があります。
必要な再帰の深さは直接入力するか、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 が推奨されます。

既定値

このボタンは、スキャン アーカイブに対して事前定義の値を復元します。

アーカイブ リスト

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。

11.1.1.3. 例外

スキャナ で省略するファイル 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なプログラムのスキャンに含める必要のない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に含める必要のないファイルのみとし、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、必ずウイルスまたは不要なプログラムに対するスキャンを実行することをお勧めします。

注
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
このリストに含まれるファイルは、レポート ファイルに入力されます。ファイルを除外した理由が存在し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 ファイルで時々確認してください。この場合、こ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。

このボタンでウィンドウが開き、必要なファイルまたは必要なパスを選択できます。
完全なパスとファイル名を入力すると、そのファイルだけが感染のスキャンから除外されます。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) その名前のすべてのファイルがスキャンされなくなります。

ルールの追加

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
ファイル オブジェクトのリストに完全なパーティションを追加すると、そのパーティションの下で直接保存されたファイルのみがスキャンから除外されます。 これは対応するパーティションに関するサブディレクトリのファイルには適用されません。
例 :省略されるファイル オブジェクト :`D:\` = `D:\file.txt` は、スキャナ のスキャンから除外されますが、`D:\folder\file.txt` はスキャンから除外されません。

11.1.1.4. ヒューリスティック

この構成セクションには、Avira AntiVir Professional 検索エンジンのヒューリスティックに対する設定が含まれます。

Avira AntiVir Professional は非常に強力なヒューリスティックを備えており、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、ウイルス対策ソフトウェアの更新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。

Macrovirus ヒューリスティック

Macrovirus ヒューリスティック

Avira AntiVir Professional には、非常に強力な Macrovirus ヒューリスティックが含まれています。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疑わしい文書に関する報告のみが行われます。このオプションは既定で有効に設定されている推奨設定です。

高度なヒューリスティック分析および検出 (AHeAD)

AHeAD の有効化

Avira AntiVir Professional 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。このオプションをアクティブ化すると、このヒューリスティックをどの程度 "アグレッシブ" にするかを定義できます。このオプションは既定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、Avira AntiVir Professional が検出する未知のマルウェアがいくらか少なくなりますが、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の使用を選択すると、既定でこの設定がアクティブ化されます。

高検出レベル

このオプションを有効にすると、Avira AntiVir Professional はより多くの未知のマルウェアを検出しますが、誤検出が発生する可能性もあります。

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含まれます。

注
ウイルスまたは不要なプログラムが検出されたときに、常にレポート ファイルが作成されるように、スキャナ が実行するアクションを設定できます。

ロギング

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。

既定値

このオプションをアクティブ化すると、スキャナ は懸念のあるファイ ルの名前とパスを記録します。現在のスキャンの構成、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。

拡張

このオプションをアクティブ化すると、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。

フル

このオプションをアクティブ化すると、スキャナ はすべてのスキャン 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 ファイルに含まれます。

注
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 スキャンの構成には、Avira AntiVir Professional 構成 の Guard セクションが関与しています。

11.2.1 スキャン

通常、ユーザーはシステムは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な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 はファイルが読み込まれたり、アプリケーションやオペレーション システムで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 はファイルを開いたり読み込んだり実行する前、および書き込み後にスキャンします。このオプションは既定で有効に設定されている推奨設定です。

ファイル

Guard では、特定の拡張子 (タイプ) を持つファイルのみをスキャンするフィルタを使用できます。

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、すべてのファイルをスキャンしてウイルスまたは不要なプログラムを検索します。つまり、フィルタは使用されません。

注
[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。

スマート拡張

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に関するスキャンを実行するファイルの選択が、Avira AntiVir Professional によって自動的に行われます。これは、Avira AntiVir Professional 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
[スマート拡張]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、指定された拡張子を持つファイルのみがスキャンされます。ウイルスや不要な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定義されます。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。この設定は既定でアクティブ化されている推奨設定です。

注
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

このボタンでダイアログ ウィンドウが開き、**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
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非アクティブに設定されています。アーカイブのスキャンは、再帰の深さ、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。再帰の深さの最大値、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
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非アクティブ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が推奨されます。

最大の再帰の深さ

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、ウイルスと不要なプログラムを検索するスキャンが実行されます。再帰の深さを定義できます。再帰の深さの既定値で推奨される値は 1 です。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は、解凍されスキャンされます。

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、この値を推奨します。

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 が推奨されます。

ドライブ

ネットワーク ドライブ

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

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

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

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

11.2.1.1. 懸念のあるファイルに対するアクション

懸念のあるファイルに対するアクション

ウイルスまたは不要な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。

対話式

このオプションを有効にすると、オンアクセス スキャン中にダイアログ ウィンドウが表示され、ウイルスまたは不要なプログラムが検出された場合、関連するファイルをどう処理するかを選択できます。このオプションは既定で有効に設定されています。

許可されるアクション

この表示ボックスで、ウイルスまたは不要なプログラムが検出された場合に、ダイアログ ボックスに表示されるアクションを指定できます。対応するオプションをアクティブ化する必要があります。

修復

Guard は、可能な場合、感染したファイルを修復します。

名前の変更

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

Quarantine

Guard はファイルを Quarantine に移動します。情報として価値がある場合、ファイルは、Quarantine Manager から復元できます。また、必要がある場合は、Avira マルウェア リサーチ センター に送信できます。ファイルによっては、Quarantine Manager で他の選択オプションも利用可能です。

削除

ファイルは削除されますが、関連するツール (Avira UnErase など) で必要があれば復元できます。ウイルスのパターンは、再度検出可能です。このプロセスは、"上書きと削除" よりはるかに早くなります。

無視

ファイルへのアクセスは許可され、ファイルは無視されます。

上書きと削除

Guard は、削除前にファイルを既定のパターンで上書きします。復元はできません。

アクセスの拒否

ファイルへのアクセスは拒否されます。 レポート機能がアクティブ化されている場合、Guard は検出されたファイルをレポート ファイルに記録します。このオプションを有効にすると、Guard は、イベント ログにもエントリを書き込みます。

既定値

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

注
修復アクションを既定のアクションとして選択することはできません。

詳細については、こちらをクリックしてください。

自動

このオプションを有効にすると、ウイルスまたは不要なプログラムの検出後、アクションを選択するダイアログ ボックスは表示されません。Guard は、このセクションで定義した設定に従って動作します。

アクション前にファイルを Quarantine にコピー

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、Quarantine に保存されます。情報として価値がある場合は、Quarantine Manager から復元できます。バックアップ コピーを Avira マルウェア リサーチ センター に送信することもできます。オブジェクトによっては、Quarantine Manager で別の選択を行うこともできます。

警告メッセージの表示

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

プライマリ アクション

プライマリ アクションとは、Guard がウイルスまたは不要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、関与するファイルの修復が不可能な場合、**[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
[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] の下で選択されている場合のみ選択できます。

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
自動修復が推奨されますが、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が、必要があれば適切なツール (Avira UnErase など) で復元できます。これはウイルスのパターンが再度検出可能であることを意味します。このプロセスは、[上書きと削除] よりはるかに早くなります。

上書きと削除

このオプションを有効にすると、Guard はファイルを既定のパターンで上書きしてから削除します。復元はできません。

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アクティブなままになります。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、Guard はレポート機能が有効にされていた場合、レポート ファイルに検出されたファイルを入力するだけです。このオプションを有効にすると、Guard は、イベント ログにもエントリを書き込みます。

Quarantine

このオプションを有効にすると、Guard はファイルを Quarantine 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、必要があれば Avira マルウェア リサーチ 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]** の下で選択されている場合のみ選択できます。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が、必要があれば適切なツール (Avira UnErase など) で復元できます。これはウイルスのパターンが再度検出可能であることを意味します。このプロセスは、[上書きと削除] よりはるかに早くなります。

上書きと削除

このオプションを有効にすると、Guard はファイルを既定のパターンで上書きしてから削除します。復元はできません。

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アクティブなままになります。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、Guard はレポート機能が有効にされていた場合、レポート ファイルに検出されたファイルを入力するだけです。このオプションを有効にすると、Guard は、イベント ログにもエントリを書き込みます。

Quarantine

このオプションを有効にすると、Guard はファイルを Quarantine に移動します。このファイルは後で修復したり、必要があれば Avira マルウェア リサーチ センター に送信できます。

注
[削除] または **[上書きと削除]** 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によるヒットの場合、感染したファイルは削除されず、Quarantine に移動されます。

11.2.1.2. 以降のアクション

通知

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、イベント ログにエントリが追加されます。管理者は検出されたファイルを識別し、それに従って対応できます。このオプションは既定で有効に設定されています。

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。プロセスを省略するリストによって、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。

Guard によって省略されるプロセス

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 による監視から除外されます。

入力ボックス

このボックスに、オンアクセス スキャンに含めないプロセスの名前を入力できます。既定で入力されているプロセスはありません。個々のプロセスの名前は、タスク マネージャを介して最も簡単に取得できます。タスク マネージャの [プロセス] タブには、現在アクティブなすべてのプロセスの名前が表示されます。[イメージ名] から目的のプロセスを選んでその名前を入力します。

注
プロセスは最大 20 件まで入力できます。

警告 :
プロセス名の最初の 15 文字 (ファイル拡張子を含む) のみが考慮されます。同じ名前で 2 つのプロセスがあると、Guard は両方のプロセスを監視から除外します。

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。リストでこれに該当するエントリは無視されます。

ルールの追加

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 で省略するファイル 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 による監視から除外されます。

注
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。

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。

このボタンでウィンドウが開き、除外するファイル オブジェクトを選択できます。

ルールの追加

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。

次の点に注意してください。

- ファイル名には、ワイルドカード * (任意の数の文字) および ? (単一文字) のみを含めることができます。
- ディレクトリ名の末尾には、バックスラッシュ \ を付ける必要があります。 それ以外の場合は、ファイル名と見なされます。
- このリストは、上から下に処理されます。
- 個々のファイル拡張子を除外することもできます (ワイルドカードを含む)。
- 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。
- 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。
- MS-DOS ファイル名 (8.3 形式) でアクセスされた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。
- 接続先ネットワーク ドライブ上のファイルおよびフォルダを Guard によるスキャンから除外するには、次のように、ネットワーク ドライブの UNC パスを例外リストに指定します。
  \\<コンピュータ名>\<Enable>\ - または - \\<IP アドレス>\<Enable>\

注
ワイルドカードを含むファイル名をバックスラッシュで終わらせ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
接続先ネットワーク ドライブに対する例外については、次の点に注意してください：接続先ネットワーク ドライブのドライブ文字を使用した場合、指定のファイルおよびフォルダが、Guard によるスキャンから除外されません。例外リストの UNC パスが、ネットワーク ドライブへの接続に使用される UNC パスと異なる場合 (例外リストは IP アドレスで指定し、ネットワーク ドライブへの接続にはコンピュータ名を使用するなど)、指定されたフォルダおよびファイルが Guard によるスキャンから除外されません。Guard レポート ファイルで適切な UNC パスを確認してください。

注
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、例外のリストで統合されたドライブに対するオペレーティング システムの別名が使用される必要があります。
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。

注
Guard が感染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] の構成で、Guard のプロトコル機能を **[完了]** に設定します。次に、アクティブ化された Guard で、ファイル、フォルダ、マウント ドライブ、または接続先ネットワーク ドライブにアクセスします。これで、Guard レポート ファイルから使用されたパスを読み取ることができるようになります。レポート ファイルは、コントロール センター の [ローカル保護] :: [Guard] にあります。

例：

```
C:
C:\
C:\*.*
C:\*
*.exe
*.xl?
```

```
*.*
C:\Program Files\Application\application.exe
C:\Program Files\Application\applic*.exe
C:\Program Files\Application\applic*
C:\Program Files\Application\applic?????.e*
C:\Program Files\
C:\Program Files
C:\Program Files\Application\*.mdb
\\コンピュータ名\Enable\
\\1.0.0.0\Enable\application.exe
```

11.2.1.4. ヒューリスティック

この構成セクションには、Avira AntiVir Professional 検索エンジンのヒューリスティックに対する設定が含まれます。

Avira AntiVir Professional は非常に強力なヒューリスティックを備えており、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、ウイルス対策ソフトウェアの更新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。

Macrovirus ヒューリスティック

Macrovirus ヒューリスティック

Avira AntiVir Professional には、非常に強力な Macrovirus ヒューリスティックが含まれています。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疑わしい文書に関する報告のみが行われます。このオプションは既定で有効に設定されている推奨設定です。

高度なヒューリスティック分析および検出 (AHeAD)

AHeAD の有効化

Avira AntiVir Professional 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。このオプションをアクティブ化すると、このヒューリスティックをどの程度 "アグレッシブ" にするかを定義できます。このオプションは既定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、Avira AntiVir Professional が検出する未知のマルウェアがいくらか少なくなりますが、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の使用を選択すると、既定でこの設定がアクティブ化されます。

高検出レベル

このオプションを有効にすると、Avira AntiVir Professional は、未知のマルウェアをよ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という点には注意が必要です。

11.2.2 レポート

Guard には、広範囲にわたるログ機能が含まれていて、ユーザーまたは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します。

ロギング

このグループを使用すると、レポート ファイルの内容を決定できます。

オフ

このオプションを有効にすると、Guard でログは作成されません。
ログ機能は、複数のウイルスまたは不要なプログラムでのテストの実行など、例外的な場合のみオフにすることを推奨します。

既定値

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を記録し (検出されたファイル、アラートおよびエラー)、重要性の低い情報は明快さを向上させるために無視されます。このオプションは既定で有効に設定されています。

拡張

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記録します。

フル

このオプションを有効にすると、Guard は、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レポート ファイルに記録します。

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。このオプションは既定でアクティブに設定されていて、既定値は 1 MB です。

短縮前にレポート ファイルをバックアップ

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

構成をレポート 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構成が、レポート ファイルに書き込まれます。

11.3 MailGuard

Avira AntiVir Professional 構成 の MailGuard セクションは、MailGuard の構成に使用されます。

11.3.1 スキャン

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

スキャン

着信電子メールのスキャン

このオプションを有効にすると、着信電子メールのウイルス、マルウェアを検索するスキャンが実行されます。MailGuard では、POP3 プロトコルおよび IMAP プロトコルがサポートされます。電子メール クライアントが電子メールの受信に使用する受信トレイ アカウントについて、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。

監視対象ポート

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。

既定値

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。

監視対象ポート

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。

既定値

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。

発信電子メールのスキャン (SMTP)

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

監視対象ポート

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。

既定値

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
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. 懸念のあるファイルに対するアクション

この構成セクションには、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
これらのアクションは、着信電子メールにウイルスが検出された場合と、発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。

懸念のあるファイルに対するアクション

対話式

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 ウィンドウが表示され、懸念のある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。このオプションは既定で有効に設定されています。

許可されるアクション

この表示ボックスで、ウイルスまたは不要なプログラムが検出された場合に、ダイアログ ボックスに表示されるアクションを指定できます。対応するオプションをアクティブ化する必要があります。

Quarantine に移動

このオプションをアクティブ化すると、電子メールはすべての添付ファイルを含めて、Quarantine に移動されます。後で、Quarantine Manager によってメールで送信することもできます。感染した電子メールは削除されます。電子メールのテキストの本文と添付ファイルは、標準テキストに置換されます。

削除

このオプションを有効にすると、ウイルスまたは不要プログラムが検出された場合、感染した電子メールは削除されます。電子メールのテキストの本文と添付ファイルは、標準テキストに置換されます。

添付ファイルの削除

このオプションをアクティブ化すると、懸念のある添付ファイルは標準テキストに置換されます。電子メールのテキストの本文が感染した場合は、削除され標準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 Quarantine に移動

このオプションをアクティブ化すると、感染した添付ファイルは、Quarantine に移動された後に削除されます (標準テキストに置換)。電子メールの本文は配信されます。感染した添付ファイルは、後で Quarantine Manager によって配信されます。

無視

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

既定値

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

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、**[対話式]** 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な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、MailGuard が電子メールに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。**[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な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な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な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 Quarantine 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な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。

感染した添付ファイル

[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な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な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、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)。必要に応じて、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な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
このオプションを選択すると、MailGuard によるウイルスおよび不要な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のみ、この項目を選択してください。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

この構成セクションには、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な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
これらのアクションは、着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。

削除/移動した電子メールの既定のテキスト

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。最大 500 文字まで入力できます。

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。

既定値

このボタンは、事前定義の既定のテキストを編集ボックスに挿入します。

削除/移動した電子メールの既定のテキスト

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。最大 500 文字まで入力できます。

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。

既定値

このボタンは、事前定義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

この構成セクションには、Avira AntiVir Professional 検索エンジンのヒューリスティックに対する設定が含まれます。

Avira AntiVir Professional は非常に強力なヒューリスティックを備えており、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、ウイルス対策ソフトウェアの更新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。

Macrovirus ヒューリスティック

Macrovirus ヒューリスティック

Avira AntiVir Professional には、非常に強力な Macrovirus ヒューリスティックが含まれています。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疑わしい文書に関する報告のみが行われます。このオプションは既定で有効に設定されている推奨設定です。

高度なヒューリスティック分析および検出 (AHeAD)

AHeAD の有効化

Avira AntiVir Professional 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。このオプションをアクティブ化すると、このヒューリスティックをどの程度 "アグレッシブ" にするかを定義できます。このオプションは既定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、Avira AntiVir Professional が検出する未知のマルウェアがいくらか少なくなりますが、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の適用を選択すると、既定の設定としてこのオプションが有効になります。このオプションは既定で有効に設定されている推奨設定です。

高検出レベル

このオプションを有効にすると、Avira AntiVir Professional は、未知のマルウェアをよ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という点には注意が必要です。

11.3.2 全般

11.3.2.1. 例外

スキャンされない電子メール アドレス

この表は、AntiVir MailGuard によるスキャン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
例外のリストは、MailGuard のみによって、着信電子メールに対して使用されます。

状況

アイコン	説明
	この電子メール アドレスには、マルウェアを検索する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 アドレスには、マルウェアを検索するスキャンが実行されなくなります。

上方向へ

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。

下方向へ

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。

ルールの追加

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された電子メールに関するデータが含まれます。

キャッシュに保管する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、広範囲にわたるログ機能が含まれていて、ユーザーまたは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します。

ロギング

このグループを使用すると、レポート ファイルの内容を決定できます。

オフ

このオプションを有効にすると、MailGuard でログは作成されません。
ログ機能は、複数のウイルスまたは不要なプログラムでのテストの実行など、例外的な場合のみオフにすることを推奨します。

既定値

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を記録し (検出されたファイル、アラートおよびエラー)、重要性の低い情報は明快さを向上させるために無視されます。このオプションは既定で有効に設定されています。

拡張

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記録します。

フル

このオプションを有効にすると、MailGuard は、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レポート ファイルに記録します。

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。このオプションは既定でアクティブに設定されていて、既定値は 1 MB です。システム リソースの使用を最小限に抑えるため、最大 50 キロバイトの予備領域が許容されています。ログ ファイルのサイズが指定されたサイズを 50 キロバイト以上超えると、指定されたサイズより 50 キロバイト少なくなるまで、古いエントリが削除されます。

短縮前にレポート ファイルをバックアップ

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

構成をレポート ファイルに書き込む

このオプションを有効にすると、MailGuard の構成がレポート ファイルに記録されます。

11.4 AntiVir WebGuard

Avira AntiVir Professional 構成 の AntiVir WebGuard セクションは、AntiVir WebGuard の構成に使用されます。

11.4.1 スキャン

AntiVir WebGuard では、インターネットから Web ブラウザで読み込んだ Web ページでの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、AntiVir WebGuard コンポーネントの動作を設定できます。

スキャン

Webguard の有効化

このオプションが有効になっている場合、インターネット Web ブラウザを使用して要求した Web ページがスキャンされてウイルスやマルウェアが検索されます。AntiVir 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。 このオプションが無効になっている場合、AntiVir 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。

Drive-by (ドライブバイ) 攻撃からの保護

Drive-by (ドライブバイ) 攻撃からの保護により、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 ページの領域を制限しないインターネット 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 の領域がほぼ非表示となっています。 [*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。

不審な I-Frame をブロックする

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 があった場合、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 (HTTP ステータス コード 403) が表示されます。

既定値

このオプションが有効になっている場合、不審なコンテンツを含む I-Frame はブロックされます。

拡張

このオプションが有効になっている場合、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. 懸念のあるファイルに対するアクション

懸念のあるファイルに対するアクション

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

対話式

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 ウィンドウが表示され、ウイルスまたは不要な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。 このオプションは既定で有効に設定されています。

許可されるアクション

この表示ボックスで、ウイルスまたは不要なプログラムが検出された場合に、ダイアログ ボックスに表示されるアクションを指定できます。 これに対応するオプションをアクティブ化する必要があります。

アクセスの拒否

Web サーバーまたは転送されたデータおよびファイルによって要求された Web サイトは Web ブラウザには送信されません。 アクセスが拒否されたことを通知するエラー メッセージが、Web ブラウザに表示されます。 レポート機能 がアクティブ化されている場合、AntiVir WebGuard は検出されたファイルをレポート ファイルに記録します。関連するオプションが有効にされている場合、AntiVir WebGuard はイベント ログにもエントリを追加します。

Quarantine

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、Quarantine 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 Quarantine Manager で復元できます。 また、必要がある場合は、Avira マルウェア リサーチ 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やファイルは AntiVir WebGuard によって Web ブラウザに送信されます。

既定値

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

詳細については、こちらをクリックしてください。

プログレス バーの表示

このオプションを有効にした場合、Web サイト コンテンツのダウンロードで 20 秒のタイムアウト時間を超過すると、ダウンロード プログレス バーと共にデスクトップに通知が表示されます。 このデスクトップ通知は、特にデータ ボリュームの大きい Web サイトのダウンロードのために設計されています。 AntiVir 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を検索するスキャンが実行されるため、Web サイトのコンテンツの増分的なダウンロードは行われません。このオプションは既定で無効に設定されています。

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なプログラムの検出後、アクションを選択するダイアログ ボックスは表示されません。AntiVir WebGuard は、このセクションで定義した設定に従って対応します。

警告メッセージの表示

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

プライマリ アクション

プライマリ アクションとは、AntiVir 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ことを通知するエラー メッセージが、Web ブラウザに表示されます。 レポート機能 がアクティブ化されている場合、AntiVir WebGuard は検出されたファイルをレポート ファイルに記録します。関連するオプションが有効にされている場合、AntiVir WebGuard はイベント ログにもエントリを追加します。

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、Quarantine 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 Quarantine Manager で復元できます。 また、必要がある場合は、Avira マルウェア リサーチ 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やファイルは AntiVir 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アクティブなままになります。 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. ロックされた要求

ロックされた要求で、AntiVir WebGuard によって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とマルウェアの URL をブロックできます。AntiVir 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。

AntiVir WebGuard でブロックされたファイル タイプ/MIME タイプ (ユーザー定義)

リストのすべてのファイル 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 AntiVir 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、AntiVir WebGuard にブロックさせる 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、メディアの種類を指定し、必要に応じてサブタイプを入力します。 2 つ記述する場合は、**video/mpeg** や **audio/x-wav** のようにスラッシュ 1 つで区切ります。

注

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て AntiVir WebGuard にブロックされたファイルは、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で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

[AntiVir WebGuard]::[スキャン]::[例外] の下で除外されるファイルと MIME タイプのリストに入力すると、ブロックされたファイルと MIME タイプのリストは無視されます。

注

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 : メディアの種類の例 :

- `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：除外されたファイルと 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 AntiVir 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、AntiVir 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 AntiVir 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 AntiVir WebGuard によってブロックされます。

ルールの追加

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 フィルタの有効化

オプションが有効になっている場合、Web フィルタ リスト内の選択されたカテゴリに一致するすべての URL はブロックされます。

Web フィルタ リスト

[Web フィルタ リスト] では、AntiVir 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
Web フィルタは、[AntiVir WebGuard]::[スキャン]::[例外] の下の除外 URL のリストのエントリについては無視されます。

注
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、AntiVir WebGuard によるスキャンに対する例外を設定できます。 指定された MIME タイプと URL は、AntiVir 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に対するスキャンは実行されません。

AntiVir WebGuard でスキップされた MIME タイプ

このフィールドで、AntiVir 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。

AntiVir WebGuard でスキップされたファイル タイプ/MIME タイプ (ユーザー定義)

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) が AntiVir 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、AntiVir 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、z.B. **.htm** などのファイル拡張子を入力します。 MIME タイプには、メディアの種類を指定し、必要に応じてサブタイプを入力します。 2 つ記述する場合は、 **video/mpeg** または **audio/x-wav** のようにスラッシュ 1 つで区切ります。

注
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。 ブロックされたアクセス ([AntiVir WebGuard]::[スキャン]::[ブロックされたアクセス] でブロックされたファイルと MIME タイプのリスト) または AntiVir WebGuard によるそれ以上の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、ブロックされたファイルと 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に関するスキャンは実行されません。

MIME タイプ : メディアの種類の例 :

- `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/` = すべての音声メディア タイプのファイルが AntiVir WebGuard のスキャンから除外されます。

- `video/quicktime` = すべての Quicktime サブタイプ ビデオ ファイル (*.qt, *.mov) が AntiVir WebGuard のスキャンから除外されます。
- `.pdf` = すべての Adobe PDF ファイルが AntiVir WebGuard のスキャンから除外されます。

ルールの追加

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。

AntiVir WebGuard でスキップされた URL

このリストのすべての URL が AntiVir WebGuard のスキャンから除外されます。

入力ボックス

このボックスに、AntiVir WebGuard のスキャンから除外する URL (例 : **www.domainname.com**) を入力できます。 冒頭または末尾にドメイン レベルを示すピリオドを使用して、URL を部分的に指定できます。たとえば、.domainname.de は、ドメインのすべてのページおよびサブドメインを表します。Web サイトは、トップレベル ドメイン (.com または .net) と末尾のピリオドで、**domainname.** のように記述します。 冒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、"www.ドメイン名.net" と解釈される)。

注

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

除外された 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、 Web フィルタまたは AntiVir WebGuard によるそれ以上のスキャンは実行されません。 除外された 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 ([AntiVir WebGuard]::[スキャン]::[ブロックされたアクセス] 参照)。 ウイルスとマルウェアに関するスキャンは実行されません。 このため、 信頼できる URL は AntiVir WebGuard のスキャンから除外する必要があります。

ルールの追加

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 : スキップされる 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 AntiVir WebGuard のスキャンから除外されます。例 : www.avira.com/en/pages/index.php、www.avira.com/en/support/index.html、www.avira.com/en/download/index.html。ドメイン 'www.avira.de' を持つ URL は AntiVir WebGuard のスキャン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 AntiVir WebGuard のスキャンから除外されます。 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。

– `avira`。 -または- `*.avira.*`

= 第 2 レベル ドメイン 'avira' を含むすべての URL が AntiVir WebGuard のスキャンから除外されます。 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。

– `.*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 AntiVir WebGuard のスキャンから除外されます。例 : www.domain.com、www.new-domain.de、www.sample-domain1.de。

– `net` -または- `*.net`

= ドップレベル ドメイン 'net' を含むすべての URL が AntiVir WebGuard のスキャンから除外されます。例 : www.name1.net、www.name2.net。

警告

AntiVir WebGuard のスキャンから除外する 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 AntiVir WebGuard のスキャン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

この構成セクションには、Avira AntiVir Professional 検索エンジンのヒューリスティックに対する設定が含まれます。

Avira AntiVir Professional は非常に強力なヒューリスティックを備えており、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、ウイルス対策ソフトウェアの更新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。

Macrovirus ヒューリスティック

Macrovirus ヒューリスティック

Avira AntiVir Professional には、非常に強力な Macrovirus ヒューリスティックが含まれています。 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疑わしい文書に関する報告のみが行われます。 このオプションは既定で有効に設定されている推奨設定です。

高度なヒューリスティック分析および検出 (AHeAD)

AHeAD の有効化

Avira AntiVir Professional 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。 このオプションをアクティブ化すると、このヒューリスティックをどの程度 "アグレッシブ" にするかを定義できます。 このオプションは既定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、Avira AntiVir Professional によって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の使用を選択すると、既定でこの設定がアクティブ化されます。

高検出レベル

このオプションを有効にすると、Avira AntiVir Professional はより多くの未知のマルウェアを検出しますが、誤検出が発生する可能性もあります。

11.4.2 レポート

AntiVir WebGuard には、広範囲にわたるログ機能が含まれていて、ユーザーまたは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します。

ロギング

このグループを使用すると、レポート ファイルの内容を決定できます。

オフ

このオプションを有効にすると、AntiVir WebGuard でログは作成されません。ログ機能は、複数のウイルスまたは不要なプログラムでのテストの実行など、例外的な場合のみオフにすることを推奨します。

既定値

このオプションを有効にすると、AntiVir WebGuard はレポート ファイルに重要な情報を記録し (検出されたファイル、アラートおよびエラー)、重要性の低い情報は明快さを向上させるために無視されます。 このオプションは既定で有効に設定されています。

拡張

このオプションを有効にすると、AntiVir WebGuard はレポート ファイルに重要性の低い情報も記録します。

フル

このオプションを有効にすると、AntiVir WebGuard は、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レポート ファイルに記録します。

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。 このオプションは既定でアクティブに設定されていて、既定値は 1 MB です。 システム リソースの使用を最小限に抑えるため、最大 50 キロバイトの予備領域が許容されています。 ログ ファイルのサイズが指定されたサイズを 50 キロバイト以上超えると、指定されたサイズより 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。

構成をレポート 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構成が、レポート ファイルに書き込まれます。

11.5 全般

11.5.1 構成 ::全般

11.5.1.1. 電子メール

特定のイベントについて、Avira AntiVir Professional では、アラートとメッセージを電子メールで 1 人以上の受信者に送信できます。これは Simple Message Transfer Protocol (SMTP) を使用して行います。

メッセージは、さまざまなイベントでトリガされます。電子メールの伝送は、次のモジュールでサポートされています。

– Guard からの電子メール アラート

– スキャナ からの電子メール アラート
– Avira マルウェア リサーチ センター への不審ファイルの調査の問い合わせ

注
ESMTP はサポートされていませんのでご注意ください。TLS (Transport Layer Security) または SSL (Secure Sockets Layer) を使用した暗号化された転送も、現在はできません。

電子メール メッセージ

SMTP サーバー

ここで使用するホストの名前、IP アドレス、またはダイレクト ホスト名を入力します。
ホスト名は、最大 127 文字にできます。

例：

192.168.1.100 または mail.musterfirma.de

送信者のアドレス

この入力ボックスに、送信者の電子メール アドレスを入力します。送信者のアドレスは、最大 127 文字にできます。

認証

一部のメール サーバーでは、電子メールの送信前に、プログラムによるサーバーに対する検証 (ログイン) が必要です。 Avira AntiVir Professional では、SMTP サーバーに対する認証に関するアラートを電子メールで送信できます。

認証を使用

このオプションを有効にすると、ログインに関連するボックスにユーザー名とパスワードを入力できます (認証)。

– **ユーザー名** :ここにユーザー名を入力してください。
– **パスワード** :関連するパスワードをここに入力してください。パスワードは暗号化された形態で保存されます。セキュリティのため、このスペースに実際に入力する文字は、アスタリスク (*) に置換されます。

テスト電子メールの送信

このボタンをクリックすると、入力されたデータの確認のため、Avira AntiVir Professional により、送信者のアドレスにテスト電子メールが送信されます。

11.5.2 構成 ::全般

11.5.2.1. 脅威カテゴリの拡張

脅威カテゴリの拡張の選択

Avira AntiVir Professional によってコンピュータ ウイルスから保護されます。

また、次の脅威カテゴリの拡張に従ってスキャンできます。

- バックドア クライアント (BDC)
- ダイヤラ (DIALER)
- ゲーム (GAMES)
- ジョーク (JOKES)
- セキュリティ プライバシ リスク (SPR)
- アドウェア/スパイウェア (ADSPY)
- 通常とは異なるランタイム圧縮 (PCK)
- 二重の拡張子ファイル (HEUR-DBLEXT)
- フィッシング
- アプリケーション (APPL)

関連するボックスをクリックすると、選択したタイプを有効にしたり (チェック マークを設定) または無効にできます (チェック マークなし)。

すべて有効化

このオプションを有効化すると、すべてのタイプが有効になります。

既定値

このボタンは事前定義の既定値を復元します。

注
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記載されません。

11.5.3 構成 ::全般

11.5.3.1. パスワード

パスワードを使用して、Avira AntiVir Professional 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。

注
SMC を介して AntiVir Professional を管理する場合、パスワード フィールドは非アクティブ化されます。AntiVir Professional のパスワードは、ローカルでのみ設定できます。

パスワード

パスワードの入力

必要な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。パスワードが発行されると、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 "パスワードがない" ことを意味します。

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。セキュリティのため、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
パスワードでは、大文字と小文字が区別されます!

パスワードで保護されている領域

Avira AntiVir Professional では、個々のエラーをパスワードで保護できます。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、再度アクティブ化することができます。

パスワード保護された領域	機能
コントロール センター	このオプションを有効にすると、コントロール センター の開始にパスワードが要求されます。
Guard の有効化/無効化	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、事前定義のパスワードが要求されます。
MailGuard の有効化/無効化	このオプションを有効にすると、MailGuard の有効化/無効化に事前定義のパスワードが要求されます。
AntiVir WebGuard の有効化/無効化	このオプションを有効にすると、AntiVir WebGuard の有効化/無効化に事前定義のパスワードが要求されます。
ジョブの追加と変更	このオプションを有効にすると、スケジューラ でのジョブの追加と変更にパスワードが要求されます。
製品アップグレードを開始	このオプションを有効にすると、更新メニューでの製品更新にパスワードが要求されます。
レスキュー CD をインターネットからダウンロード	このオプションを有効にすると、Avira Rescue CD のダウンロード開始時にパスワードが要求されます。
Quarantine	このオプションを有効にすると、Quarantine Manager 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、再度有効にすることができます。
感染した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パスワードが要求されます。
感染したオブジェクトの修復	このオプションを有効にするとオブジェクトの復元にパスワードが要求されます。
感染した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パスワードが要求されます。
感染した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パスワードが要求されます。
AntiVir に電子メール	このオプションを有効にすると、調査のための Avira マルウ

を送信	ェア リサーチ センター へのオブジェクトの送信にパスワードが要求されます。
構成	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ないと、Avira AntiVir Professional の構成ができなくなります。
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 モードを有効にするためにパスワードが要求されます。
インストール/アンインストール	このオプションを有効にすると、Avira AntiVir Professional のインストールまたはアンインストールにパスワードが要求されます。

11.5.4 セキュリティ

更新

最終更新から n 日経過した場合にアラート

このボックスに、Avira AntiVir Professional の最終更新から許容される最大経過日数を入力できます。この日数を超えると、スケジューラ に警告が表示されます。

検出パターン付き署名データベース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 メッセージが送信されます。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 メッセージが送信されるかを時間間隔で設定できます。

フル システム スキャン

この領域では、コントロール センター の [概要] :: [状況] に表示されるフル システム スキャンの状態表示を構成できます。

経過日数が n 日を超えた場合 "黄色" 状態

前回の完全システム スキャンからの経過日数が何日を超えたら黄色の状態表示に切り替えるかを入力します。赤色の状態に対して指定する間隔よりも短くする必要があります。標準値の 7 日が推奨されます。

経過日数が n 日を超えた場合 "赤色" 状態

前回の完全システム スキャンからの経過日数が何日を超えたら赤色の状態表示に切り替えるかを入力します。黄色の状態に対して指定する間隔よりも長くする必要があります。標準値の 30 日が推奨されます。

注
両方の間隔に「0」を指定した場合、完全システム スキャンの状態監視は無効になります。常に緑色の記号が表示されます。例外的なケースを除き、この設定は避けてください。どちらか一方の間隔だけを「0」に設定した場合は、無効な指定として破棄されます。

製品の保護

プロセスが終了しないように保護します。

このオプションを有効にすると、AntiVir 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 マネージャーによるユーザーに "制御できない" 終了から保護されます。このオプションは既定で有効に設定されています。

重要
64 ビット システムでは、まだ保護は使用できません。

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。

ファイルおよびレジストリ エントリを改変から保護する

このオプションを有効にすると、AntiVir Professional 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 (バイナリおよび構成ファイル) が改変されないように保護されます。ユーザーまたは外部プログラムによるレジストリ エントリまたはプログラム ファイルの書き込みや削除のほか、場合によっては、読み取りアクセスも禁止されます。

注
このオプションをアクティブ化すると、スキャン要求や更新要求の変更といった構成の変更が、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
現在、64 ビット システムでは、ファイルおよびレジストリ エントリの保護は利用できません。

11.5.5 WMI

Windows Management Instrumentation のサポート

Windows Management Instrumentation は、Windows システム上の設定にスクリプトとプログラミング言語を使用してアクセスできるようにする、Windows 管理の基本的な手法であり、ローカルまたはリモートから、各種の設定を読み取ったり書き込んだりすることができます。AntiVir Professional は WMI をサポートしており、データ (状態情報、統計データ、レポート、予定された要求など) を提供するほか、インターフェイスでのイベントおよびメソッド (プロセスの開始と停止) を提供します。WMI を使用することにより、AntiVir Professional から動作データをダウンロードしたり、AntiVir Professional を制御したりすることができます。WMI インターフェイスの詳細なリファレンス ガイドについては、AntiVir Professional の製造元にお問い合わせください。秘密保持契約に署名すると、PDF 形式のリファレンス ファイルを入手できます。

WMI サポートの有効化

このオプションを有効にすると、AntiVir Professional から WMI を介して動作データをダウンロードできます。

サービスを有効/無効にできるようにする

このオプションを有効にすると、AntiVir Professional から WMI を介してサービスを有効/無効にすることができます。

11.5.6 ディレクトリ

一時パス

この入力ボックスに、Avira AntiVir Professional と連動する一時パスを入力します。

既定のシステム設定の使用

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
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] タブ | [環境変数] ボタンです。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。

このボタンでウィンドウが開き、必要な一時パスを選択できます。

既定値

このボタンは、一時パスに対して事前定義のディレクトリを復元します。

レポート ディレクトリ

この入力ボックスには、Avira AntiVir Professional のレポート ファイルへのパスが含まれています。

このボタンでウィンドウが開き、必要なディレクトリを選択できます。

既定値

このボタンは、レポート ディレクトリに対する事前定義のパスを復元します。

Quarantine ディレクトリ

このボックスには、 Avira AntiVir Professional の quarantine ディレクトリへのパスが含まれています。

このボタンでウィンドウが開き、必要なディレクトリを選択できます。

既定値

このボタンは、quarantine ディレクトリへの事前定義のパスを復元します。

11.5.7 更新

Avira AntiVir Professional 構成 の**更新** セクションは、アップデータ の構成に関与しています。Web サーバーまたはファイル サーバー/共有で更新を実行できます。

ダウンロード

Web サーバーを介して

Avira AntiVir Professional アップデータ は、セントラル サーバーを使用して、インターネットまたはイントラネットから更新を取得します。

注
このオプションを有効にすると、Web サーバー経由での更新を [構成] :: [全般] :: [更新] :: [Web サーバー] で必要に応じて設定することができます。

ファイル サーバー/共有を介して

更新は、ファイル サーバーまたは共有を介して実行されます。

注
このオプションを有効にすると、ファイル サーバー経由での更新を [構成] :: [全般] :: [更新] :: [ファイル サーバー] で必要に応じて設定することができます。

製品の更新

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。

このオプションを有効にすると、更新が利用可能になると直ちに、製品の更新がダウンロードされ、AntiVir アップデータ 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。このオプションの条件は、更新の完全な構成とダウンロード サーバーへの開かれた接続です。

新製品の更新が使用可能な場合に通知

このオプションを有効にすると、新製品の更新が使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。このオプションの条件は、更新の完全な構成とダウンロード サーバーへの開かれた接続です。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 AntiVir アップデータ からの通知が表示されます。

製品の更新をダウンロードしない

このオプションを有効にすると、AntiVir アップデータ による自動の製品の更新、または利用できる製品の通知は実行されません。ウイルス定義ファイルと検索エンジンへの更新は、この設定とは無関係に実行されます。

重要
ウイルス定義ファイルと検索エンジンの更新は、製品の更新に対する設定から独立して、すべての更新プロセス中に実行されます (「更新」の章を参照)。

11.5.7.1. ファイル サーバー

ネットワークに複数のワークステーションがある場合、Avira AntiVir Professional では、イントラネットのサーバーから更新をダウンロードできます。 イントラネットのサーバーは、順番にインターネットから更新ファイルを取得します。このようにして、Avira AntiVir Professional はすべてのワークステーションで最新の状態になります。

注
構成の見出しは、[構成] :: [全般] :: で **[ファイル サーバー/共有を介して]** オプションが選択されている場合にのみ有効になります。

ダウンロード

サーバー上で Avira AntiVir Professional の現在のファイルが置かれている場所のパスをここに入力します。

このボタンでウィンドウが開き、必要なダウンロード ディレクトリを選択できます。

サーバー ログイン

ログイン名

サーバーへのログイン名をここに入力します。

ログイン パスワード

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。セキュリティのため、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
サーバー ログイン セクションにデータを入力しないと、アクセス中にファイル サーバーに関する認証が完了しません。この場合、適切なユーザー権限をファイル サーバーに保存する必要があります。

11.5.7.2. Web サーバー

更新はインターネット上で直接 Web サーバーを介して、またはイントラネットで実行できます。

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。

Avira AntiVir Professional アップデータ により、使用可能な接続オプションが自動的に検出されます。使用できない接続オプションは灰色表示になり、アクティブ化できません。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。セキュリティのため、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
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
ダイヤルアップ ツール (SmartSurfer、Oleco など) を介したアップデータによる自動ダイヤルアップは、現在 Avira AntiVir Professional では利用できません。

更新にセットアップされたダイヤルアップ接続を終了

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
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必ず切断されます。

ダウンロード

Standard-Server

更新をダウンロードする Web サーバーのアドレス (URL) をここに入力します。Web サーバーには、インターネットまたはイントラネット上のサーバーを設定できます。複数のアドレスを入力できます。AntiVir Professional の更新でアクセス可能な Web サーバーが既定で入力されます。

既定値

このボタンは、事前定義のアドレスを復元します。

優先度サーバー

このフィールドには、更新中に最初のサーバーとしてアクセスする Web サーバーのアドレス (URL) を入力します。このサーバーにアクセスできない場合、標準サーバーとして示されるサーバーが使用されます。

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。

次のプロキシ サーバーを使用

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 サーバーへの接続に使用するプロキシ サーバーの URL 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 サーバーへのログイン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。セキュリティのため、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：	proyx.domain.com	ポート：	8080
アドレス：	192.168.1.100	ポート：	3128

11.5.8 警告

11.5.8.1. ネットワーク

個別に構成可能なアラートは、スキャナ または Guard からネットワーク内の任意のワークステーションに送信できます。

注
"メッセージ サービス" が開始しているかどうかを確認してください。このサービスは、(Windows XP など) "スタート | 設定 | System control | Administration | Services" の下にあります。

注
アラートは特定のユーザーに送信されるのではなく、常にコンピュータに送信されます。

警告
次のオペレーティング システムでは、この機能のサポートは廃止されます。
Windows Server 2008 以上
Windows Vista 以上

メッセージの送信先

このウィンドウのリストには、ウイルスまたは不要なプログラムが検出された場合に、メッセージを受信するコンピュータの名前が表示されます。

注
コンピュータは、このリストに 1 回だけ入力できます。

追加

このボタンを使用すると、別のコンピュータを追加できます。ウィンドウが開き、新しいコンピュータの名前を入力できます。コンピュータの名前は、最大 15 文字にできます。

このボタンを使用するとウィンドウが開き、代わりにネットワーク環境から直接コンピュータを選択することもできます。

削除

このボタンを使用すると、現在選択しているエントリをリストから削除できます。

Guard

ネットワーク アラート

このオプションを有効にすると、ネットワーク アラートが送信されます。このオプションは既定で無効に設定されています。

注
このオプションをアクティブ化するには、[全般] :: [アラート] :: [ネットワーク] の下に、最低 1 人受信者を入力する必要があります。

送信されるメッセージ

このウィンドウには、ウイルスまたは不要なプログラムが検出されたときに、選択したワークステーションに送信されたメッセージが表示されます。このメッセージは編集できます。テキストには、最大 500 文字含めることができます。

メッセージの書式設定には、次のキーの組み合わせを使用できます。

Strg + Tab	タブを挿入します。現在の行が、数文字右にインデントされます。
Strg + Enter	改行を挿入します。

メッセージには、検索中に発見された情報のためのワイルドカードを含めることができます。これらのワイルドカードは、送信時に実際のテキストに置換されます。

次のワイルドカードが使用できます。

%VIRUS%	検出されたウイルスまたは不要なプログラムの名前が含まれます。
%FILE%	感染したファイルのパスとファイル名が含まれます。
%COMPUTER%	Guard を実行しているコンピュータの名前が含まれます。
%NAME%	感染したファイルにアクセスしたユーザーの名前が含まれます。
%ACTION%	ウイルス検出後に実行されたアクションが含まれます。
%MACADDR%	Guard を実行しているコンピュータの MAC アドレスが含まれます。

既定値

このボタンは、アラートに対する事前定義の既定のテキストを復元します。

スキャナ

ネットワーク アラートの有効化

このオプションを有効にすると、ネットワーク アラートが送信されます。このオプションは既定で無効に設定されています。

注
このオプションをアクティブ化するには、[全般] :: [アラート] :: [ネットワーク] の下に、最低 1 人受信者を入力する必要があります。

送信されるメッセージ

このウィンドウには、ウイルスまたは不要なプログラムが検出されたときに、選択したワークステーションに送信されたメッセージが表示されます。このメッセージは編集できます。テキストには、最大 500 文字含めることができます。

メッセージの書式設定には、次のキーの組み合わせを使用できます。

Strg + Tab	タブを挿入します。現在の行が、数文字右にインデントされます。
Strg + Enter	改行を挿入します。

メッセージには、検索中に発見された情報のためのワイルドカードを含めることができます。これらのワイルドカードは、送信時に実際のテキストに置換されます。

次のワイルドカードが使用できます。

%VIRUS%	検出されたウイルスまたは不要なプログラムの名前が含まれます。
%NAME%	スキャナ を実行するログインしたユーザーの名前が含まれます。

既定値

このボタンは、アラートに対する事前定義の既定のテキストを復元します。

11.5.8.2. 電子メール

Guard

AntiVir Guard を使用すると、特定のイベントに対して、1 人以上の受信者に電子メールでアラートを送信できます。

Guard

電子メール アラート

このオプションを有効にすると、特定のイベントが発生した場合、AntiVir Guard によって最も重要な情報を記載した電子メール メッセージが送信されます。このオプションは既定で無効に設定されています。

以下のイベントを伴う電子メール通知

– **オンデマンド スキャンでウイルスや不要なプログラムを検出**
このオプションを有効にすると、オンアクセス スキャンでウイルスや不要なプログラムを検出した場合、ウイルスまたは不要なプログラムの名前と感染したファイルの名前が記載された電子メールを受信します。
– **Guard で重大なエラーが発生**
このオプションを有効にすると、Avira AntiVir Professional が重大な内部エラーを検出した場合に電子メールが送信されます。

注
この場合は、電子メールに記載されていたデータを含めて、テクニカル サポートにご連絡ください。調査のため、指定されたファイルも送信する必要があります。

受信者

このボックスには、受信者の電子メール アドレスを入力します。アドレスはカンマで区切ってください。すべてのアドレスを合わせた (文字列合計の) 長さは最大 260 文字です。

スキャナ

特定のイベントについては、オンデマンド スキャンを使用して、1 人以上の受信者に電子メールでアラートとメッセージを送信できます。

スキャナ

電子メール アラートの有効化

このオプションを有効にすると、特定のイベントが発生した場合、Avira AntiVir Professional によって最も重要な情報を記載した電子メール メッセージが送信されます。このオプションは既定で無効に設定されています。

以下のイベントを伴う電子メール通知

– **オンデマンド スキャンでウイルスや不要なプログラムを検出**
このオプションを有効にすると、オンデマンド スキャンでウイルスや不要なプログラムを検出すると必ず、ウイルスまたは不要なプログラムと感染したファイルの名前が記載された電子メールが送信されます。
– **予定したスキャンの終了**
このオプションをアクティブ化すると、スキャン ジョブが実行されたときに、電子メールが送信されます。電子メールには、スキャン ジョブの時刻と期間、スキャンされたフォルダとファイル、および検出されたウイルスと警告が含まれます。

受信者のアドレス

このボックスには、受信者の電子メール アドレスを入力します。アドレスはカンマで区切ってください。すべてのアドレスを合わせた (文字列合計の) 長さは最大 260 文字です。

AntiVir アップデータ

AntiVir アップデータ を使用すると、特定のイベントに対して、1 人以上の受信者に電子メールで通知を送信できます。

AntiVir アップデータ

電子メール アラート

このオプションを有効にすると、特定のイベントが発生した場合、AntiVir アップデータ によって最も重要なデータを記載した電子メール メッセージが送信されます。このオプションは既定で無効に設定されています。

以下のイベント向けの電子メール メッセージ

- **更新は不要です。プログラムは最新です。**
  このオプションを有効にすると、AntiVir アップデータ が正常にダウンロード サーバーに接続したが、サーバー上で利用できる新しいファイルがない場合に電子メールが送信されます。これは、AntiVir Professional が最新であることを意味します。
- **更新が正常に完了しました。新しいファイルがインストールされました。**
  このオプションを有効にすると、実行されたすべての更新に対して電子メールが送信されます。 これは、製品更新の場合、またはウイルス定義ファイルやスキャン エンジンの更新の場合があります。
- **更新が正常に完了しました。新しい製品の更新が使用できます。**
  このオプションを有効にすると、製品更新なしでスキャン エンジンまたはウイルス定義ファイルの更新が実行され、製品更新が利用できない場合のみに、電子メールが送信されます。
- **更新できませんでした。**
  このオプションを有効にすると、エラーにより更新が実行できなかった場合に、電子メールが送信されます。

受信者

このボックスには、受信者の電子メール アドレスを入力します。アドレスはカンマで区切ってください。すべてのアドレスを合わせた (文字列合計の) 長さは最大 260 文字です。

注

以下で電子メール通知が構成されている場合、次のイベントにより、電子メールの警告メッセージが送信されます。 [構成]::[全般]::[電子メール] が構成されました。
AntiVir Professional の今後のすべての更新を利用するには、製品更新が必要です。
製品更新が必要なため、スキャン エンジン、またはウイルス定義ファイルの更新が実行できませんでした。

これらの警告メッセージは、AntiVir アップデータ の電子メール警告の設定にかかわらず送信されます。

11.5.8.3. 音声のアラート

音声のアラート

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、音声のアラートが鳴ります。音声のアラートをアクティブ化または非アクティブ化したり、音声の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
スキャナ のアクション モードは、[スキャナ]::[スキャン]::[懸念のあるファイルに対するアクション] の構成で設定します。Guard のアクション モードは、[Guard]::[スキャン]::[懸念のあるファイルに対するアクション] の構成で設定します。

警告なし

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、音声のアラートは生成されません。

PC のスピーカーで再生 (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のアラートとして既定の信号が使用されます。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のアラートとして、選択された WAV ファイルが使用されます。選択された WAV ファイルが、外部接続のスピーカーで再生されます。

WAVE ファイル

この入力ボックスに、選択した音声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 AntiVir Professional の既定の音声信号が入力されます。

このボタンでウィンドウが開き、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。

11.5.9 イベント

イベント データベースの制限サイズ

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 データベースに一覧表示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 ～ 10 000 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 データベースに一覧表示されるイベントは、特定の期間後に削除されます。 可能な値 :1 ～ 90 日。このオプションは既定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)

このオプションをアクティブ化すると、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 コントロール センター では、最大 20,000 エントリが表示されます。

11.5.10 レポートの制限

レポート数を制限

数を n 個に制限

このオプションを有効にすると、レポートの最大数が指定した量に制限されます。1 から 300 までの値が許容されます。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

このレポートを削除すると、特定の日数の後、レポートは自動的に削除されます。許容される値は 1 ～ 90 日です。このオプションは既定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。

11.5.11 音声のアラート

音声のアラート

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、音声のアラートが鳴ります。音声のアラートをアクティブ化または非アクティブ化したり、音声の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

スキャナ のアクション モードは、[スキャナ]::[スキャン]::[懸念のあるファイルに対するアクション] の構成で設定します。Guard のアクション モードは、[Guard]::[スキャン]::[懸念のあるファイルに対するアクション] の構成で設定します。

警告なし

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、音声のアラートは生成されません。

PC のスピーカーで再生 (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のアラートとして既定の信号が使用されます。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のアラートとして、選択された WAV ファイルが使用されます。選択された WAV ファイルが、外部接続のスピーカーで再生されます。

WAVE ファイル

この入力ボックスに、選択した音声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 AntiVir Professional の既定の音声信号が入力されます。

このボタンでウィンドウが開き、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。

AVIRA
More Than Security

Avira AntiVir Professional

Promark, Inc.

〒157-0076 東京都世田谷区
岡本3丁目20番18号、302

電話番号：03-3417-4630
ファックス：03-3417-4698

インターネット：http://www.promark-inc.com