# Avira AntiVir Server
ユーザー マニュアル

AVIRA

# 商標と著作権

## 商標

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

## 著作権情報

Avira AntiVir Server 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 Server ヘルプの第三者ライセンスの下の.を参照してください。

# 目次

# 1 はじめに

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

このマニュアルでは、プログラムのインストールと操作について説明します。

詳細なオプションについては、次の弊社 Web サイトを参照してください。

http://www.avira.jp

Avira Web サイトでは、次のことが可能です。

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

Avira チーム

# 2 アイコンと強調表示

次のアイコンが使用されています。

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

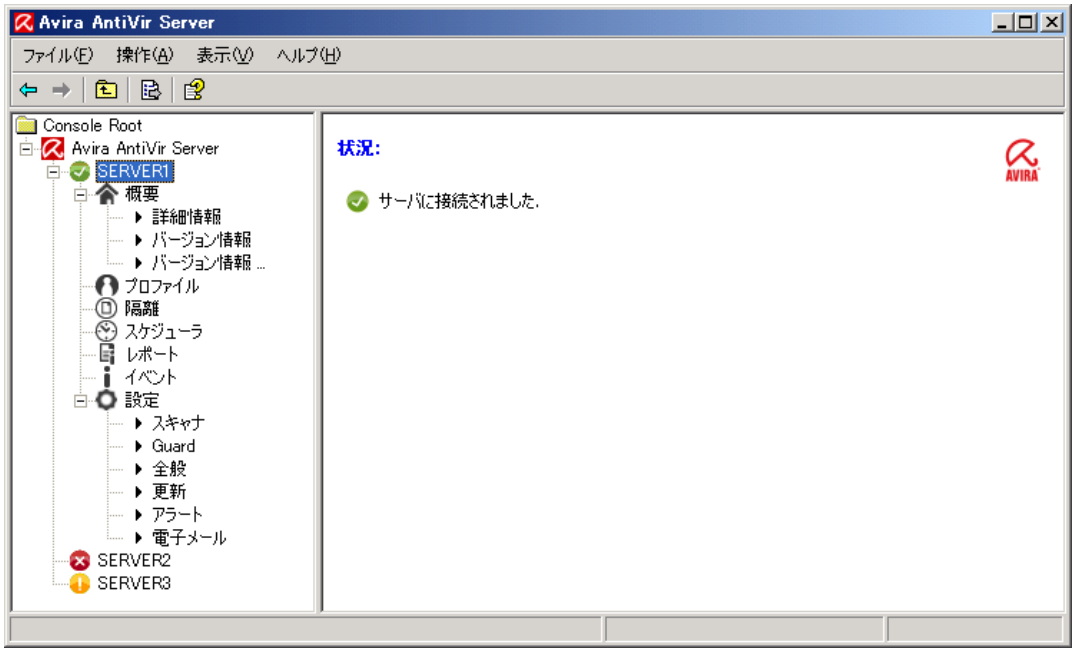
次の強調表示が使用されています。

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

# 3 製品情報

## 3.1 機能

Avira AntiVir Server 保護パッケージには、Avira AntiVir Server サービスおよび AntiVir Server コンソールが含まれています。Avira AntiVir Server サービスは、Windows サーバーをウイルスとマルウェアから保護します。AntiVir Server コンソールは、保護対象のサーバーまたは保護対象のサーバー上の AntiVir サービスを管理、制御、および監視するために使用します。AntiVir Server コンソールを介して、任意の数のサーバーにアクセスできます。




### Avira AntiVir Server サービス

サーバーをウイルスおよびマルウェアから保護します。ネットワーク内で保護するすべての Windows サーバーにこのサービスをインストールします。

AntiVir Server サービスは、システムを保護するための包括的な機能を 1 つのパッケージで提供します。このパッケージには、複数のプログラム コンポーネントとヘルプ プログラムが含まれています。主要コンポーネントの概要:

- **スキャナ**は、コンピュータ システムをスキャンして、ウイルスおよび不要プログラムを検出します (オンデマンド スキャン)。感染したファイルは、設定に従って、削除、修復、または [隔離] に移動されます。スキャナによるスキャンは自動的に実行されます。スキャンの間隔と範囲を設定できます。

- **Guard** はバックグラウンドで実行されます。ファイルを開く、書き込む、コピーなどの操作中にリアルタイムで監視を行い、必要に応じてファイルを修復します。
- **Scheduler** は、インターネットまたはイントラネットを介したスキャンや更新など、定期的なタスクの計画をサポートします。
- **アップデータ**は、インターネットまたはイントラネット接続を介してプログラムを最新状態に保ちます。
- **隔離**は、[隔離] に保管されたファイルを管理および監視します。

#### AntiVir Server コンソール

AntiVir Server サービスを制御、設定、および監視するためのデスクトップを提供します。AntiVir Server コンソールは、保護対象のサーバーにネットワーク経由で接続されている 1 台以上のコンピュータにインストールする必要があります。AntiVir Server コンソールは、保護対象のサーバーにインストールすることもできます。

AntiVir Server コンソールは、保護対象の任意の数のサーバーに接続でき、コンポーネント、レポート、イベントのアクセスや、接続されている AntiVir Server サービスの設定へのアクセスを提供します。

## 3.2 提供範囲

**主要機能:**

- プログラム全体を監視、管理、制御するコンソール
- 単純なキーワード ベースの設定: 統合ウィザードおよび状況依存型のヘルプによる設定のサポート
- 他のコンピュータからの設定および操作が可能: AntiVir サーバー サービスとは別個にユーザー インターフェイス (AntiVir Server コンソール) をインストール可能
- Avira Security Management Center (SMC) を介したネットワーク管理
- すべての既知のウイルスおよびマルウェアの種類に対して、プロファイル制御および設定可能なスキャンを提供するスキャナ (オンデマンド スキャン)
- すべてのファイル アクセスの常時監視を提供する常駐型ウイルス ガード (リアルタイム スキャンまたはオンアクセス スキャン)
- 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
- 革新的な AHeAD (Advanced Heuristic Analysis and Detection) テクノロジに基づく既知の攻撃者または短時間に変化する攻撃者の検出により実現される予防的なセキュリティ
- ネストされたアーカイブの検出や、スマートなファイル タイプの判別による検出など、従来型のあらゆるアーカイブ タイプの検出
- 包括的なフィルタ機能およびファイル キャッシングによる高速なスキャン

- "マルチスレッド機能":複数ファイルの同時高速スキャン
- 設定可能な検出時の動作: プログラムまたはファイルの修復、削除、[隔離] ディレクトリへの移動、ブロック、名前の変更、隔離。ウイルスおよびマルウェアの自動削除
- 隔離: [隔離] ディレクトリ内での感染したファイルの削除、検出場所での復元
- 更新やスキャンなど、1 回限りまたは定期的なジョブを計画するための統合スケジューラ
- インターネットを介した自動更新またはネットワーク全体への配布 (システムの中断なし)
- 管理者のための包括的なログ機能、警告およびメッセージング機能: Windows ネットワーク内で電子メール (SMTP) を介した警告の送信、SMTP 認証が可能
- 強力なセルフテストによる、プログラム ファイルの改変の保護
- 拡張ターミナル サーバー サポート
- ルートキット対策は、Windows XP 64 ビット、Windows 2003 64 ビット、Windows Server 2003 64 ビットでは使用できません。
- Windows Management Instrumentation のサポート

## 3.3 システム要件

Avira AntiVir Server サービスおよび AntiVir Server コンソールを使用するための Avira AntiVir Server の要件を次に示します。

- コンピュータ : Pentium 以上、最低 266 MHz
- オペレーティング システム
- Windows XP SP2 (32 ビットまたは 64 ビット)、または
- Windows Vista (32 ビットまたは 64 ビット、SP 1 推奨) または
- Windows 7 (32 ビットまたは 64 ビット) 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)、または
- Windows Server 2008 R2 (64 ビットのみ)
- 150 MB 以上のハード ディスク空き容量 (隔離機能を使用する場合は、さらに空き容量が必要です)
- 512 MB 以上の RAM (Windows Server 2003 の場合)
- 1024 MB 以上の RAM (Windows Vista、Windows 7、Windows Server 2008、Windows Server 2008 R2 の場合)
- Avira AntiVir Server のインストールの場合:管理者権限

**インターネット アクセス**

定期的な更新を行うために、ネットワークのサーバーはインターネットにアクセスできる必要があります。イントラネット内のファイル サーバーまたは HTTP サーバーから更新プログラムをダウンロードすることもできます。詳細については、「更新」を参照してください。

## 3.4 使用許諾

Avira AntiVir Server を使用するには、ライセンスが必要です。Avira AntiVir Server のライセンスをアクティブ化するには、ライセンス ファイル *hbedv.key* を使用します。このライセンス ファイルは、Avira GmbH から電子メールで送信されます。ライセンス ファイルには、1 つの注文プロセスで注文したすべての製品のライセンスが含まれています。お客様は、ライセンス条件を受け入れる必要があります。

### 3.4.1 ライセンス モデル

次のライセンス モデルにおいて、Avira AntiVir Server の多くの機能をご利用いただけます。

- 評価バージョン: 全機能、30 日間有効のライセンス。
- フル バージョン

使用許諾は、すべてのプラットフォームの使用許諾を表し、Avira AntiVir Server によって保護するネットワーク内のユーザーの数に依存します。ライセンス バージョンとオプションのサポートの詳細については、弊社の以下の Web サイトを参照してください。

http://www.avira.jp

フル バージョンの提供範囲:

- AntiVir バージョンのインターネットからのダウンロード
- インストールのサポート (購入日から 4 週間以内)
- ニュースレター サービス (電子メールによる配信)
- インターネット経由の更新サービス

# 4 インストールとアンインストール

## 4.1 インストール

Avira AntiVir Server をインストールするにあたっては、所定の条件が満たされている必要があります。

- システム要件が満たされていること (「システム要件」を参照)、および使用する Windows Server が実行されていることを確認します。
- 管理者または管理者権限を持つユーザーとしてログインしていることを確認します。
- Avira AntiVir Server を更新するためのダウンロード サーバーへのインターネット接続またはネットワーク接続が存在することを確認します。ファイル サーバーを使用している場合は、サーバーにログインするためのユーザー名とパスワードが必要になります。
- フル バージョンをインストールする場合: 有効なライセンス ファイル *hbedv.key* がサーバーのローカル ディレクトリに格納されていることを確認します。
- Avira AntiVir Server サービスをインストールする場合: AntiVir Server コンソールを使用して保護対象のサーバーにリモート接続する場合は、次のポートが開かれていることを確認します。
  139 (NetBIOS SSN)
  137 (NetBIOS NS)
  138 (NetBIOS DGM)

**インストールの種類**

インストール中、インストール ウィザードで、セットアップの種類を選択できます。

エクスプレス

- Avira AntiVir Server は、Avira AntiVir Server サービス、AntiVir Server コンソール、および推奨のすべてのプログラム コンポーネントと共にインストールされます。
- プログラム ファイルのインストール先フォルダを選択することはできません。

ユーザー定義

- Avira AntiVir Server サービスおよび AntiVir Server コンソールをインストールするかどうかを選択できます。
- Avira AntiVir Server サービスの追加の機能を選択してインストールするオプションがあります。

**AntiVir ルートキット対策**: この機能にはルートキット スキャン プロファイルが含まれており、これを使用して、隠れているマルウェアを探すことができます。

**VMware オフライン スキャナ**: この機能には VMware イメージ スキャン プロファイルが含まれており、これを使用して、ウイルスや不要プログラムに対する VMware のオフライン スキャンを実行できます。

**シェル拡張**:この機能により、ウイルスや不要プログラムに関してディレクトリのスキャンに使用できる、Windows エクスプローラのコンテキスト メニューのエントリを生成できます。

**AntiVir Systray ツール**: この機能により、保護対象のサーバーの通知領域に、Avira AntiVir Server のトレイ アイコンが生成されます。これにより、Avira AntiVir Server の状況を監視し、Avira AntiVir Server の他の機能にアクセスできます。この機能はエクスプレス インストールに含まれていて、ユーザー定義インストールを実行する場合は選択を解除できます。

– 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。

### インストールの実行

Avira AntiVir Server のインストール:

– インターネットでダウンロードしたインストール ファイルをダブルクリックするか、プログラム CD を挿入して、セットアップを開始します。インストール ウィザードが開きます。
– インストール ウィザードの指示に従います。次のインストール手順を実行します。
– 必要に応じて、Microsoft Visual C++ 2008 - Redistributable Kit をインストールします (このキットをまだインストールしていない場合)。

**注意**
Avira AntiVir Server は、Microsoft Visual C++ 2008 - Redistributable Kit のランタイム ライブラリを使用します。したがって、Avira AntiVir Server を使用するには、Microsoft Visual C++ 2008 - Redistributable Kit がインストールされている必要があります。

– 使用許諾契約の確認
– セットアップの種類の選択 (エクスプレス インストールまたはユーザー定義インストール)
– Avira AntiVir Server の使用許諾:ライセンス ファイルの読み込みまたは 30 日間有効のテスト ライセンスの選択
– Avira AntiVir Server サービスおよび AntiVir Server コンソールのインストール

Avira AntiVir Server サービスをインストールした場合、インストールの完了後に設定ウィザードが起動されます。インストールされた Avira AntiVir Server サービスの最も重要な設定を行うことができます。

– **AHeAD (Advanced Heuristic Analysis and Detection) テクノロジ設定の定義。**設定は、スキャナおよび Guard に対して定義されます。
– **脅威カテゴリ (詳細) の選択:** Avira AntiVir Server による検出およびレポートの対象となる他の拡張脅威カテゴリを選択することで、Avira AntiVir Server の保護機能をニーズに対応させることができます。

- **除外する製品の選択 (Guard):** Guard の監視対象から除外するソフトウェア製品を選択できます (オンアクセス スキャナ)。その結果、Guard が原因となるパフォーマンスの低下を回避することができます。
- **電子メールの設定の選択:** 電子メールを送信するためのサーバー設定を定義できます。Avira AntiVir Server では、SMPT を使用して、電子メールの送信および Avira AntiVir Server 管理者への電子メール アラートの送信を行う場合に、SMPT が使用されます。

**注意**
インストール後は、AntiVir Server サービスがインストールされていなくても、AntiVir Server コンソール (ローカル ホスト/127.0.0.1) によって、使用中のシステムが保護対象サーバーとして自動的に追加されます。

**注意**
現在の Avira AntiVir Server インストールのプログラム コンポーネントを追加または削除するには、Avira AntiVir Server のセットアップを使用します。

## 4.2 アンインストール

オペレーティング システムのコントロール パネルまたは AntiVir プログラムのセットアップから、アンインストールを実行します。

アンインストール処理中、AntiVir サービスは停止し、すべてのレポート ファイルおよび ([隔離] 内の) 感染したファイルは削除されます。

アンインストールの際に、レポート ファイルが保存されているディレクトリおよび [隔離] が削除されないように指定することもできます。

## 4.3 ネットワーク上でのインストールとアンインストール

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

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

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

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

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

ネットワーク上でのインストールとアンインストールに関する詳細:

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

### 4.3.1 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)

▶ インストールおよび更新の変更

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

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

管理者権限が必要です (バッチ モードでも必要)。

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

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

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

### 4.3.2 ネットワーク上でのアンインストール

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

管理者権限が必要です (バッチ モードでも必要)。

▶ アンインストールをパラメータ `/inf` および `/AVUNINSTALL` を使用して開始するか、サーバーのログイン スクリプトにパラメータを統合します。

### 4.3.3 セットアップ プログラムのコマンド ライン パラメータ

次のパラメータは、インストールおよびアンインストールに使用します。

- `/INF=<`スクリプト名とパス`>`

  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。

インストール: `PRESETUP.EXE /INF=e:\disks\setup.inf`

アンインストール: `PRESETUP.EXE /INF=e:\disks\setup.inf /AVUNINSTALL`

– /SILENT

セットアップ スクリプトは、ユーザーの関与なしで、完全に停止します。

### 4.3.4 setup.inf ファイルのパラメータ

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

– `InstallPath`

Avira AntiVir Server 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。環境変数は使用できません。

例: InstallPath="%PROGRAMFILES%\Avira\AntiVir Server\"

– `LicenseFile=<`ライセンス ファイルのパスとファイル名`>`

Avira AntiVir Server は、ライセンスと共にインストールされます。ファイル名のみを入力すると、ライセンス ファイルはセットアップのソース フォルダでのみ検索されます。

例: `LicenseFile="A:\hbedv.key"`

– `RestartWindows= 0 | 1`

インストール後にシステムの再起動が必要な場合、これは自動的に実行されるか (標準)、メッセージ ボックスが表示されます。

`0`:無効にする (メッセージ ボックスで再起動)

`1`:有効にする (自動的に再起動)

– `DeleteFolderOnUninstall=1`

アンインストール中に設定を削除します。

– `Guard= 0 | 1`

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

1:AntiVir Guard をインストールする (既定)

0:AntiVir Guard をインストールしない

– `RootKit= 0 | 1`

AntiVir ルートキット対策モジュールをインストールします。システム内に隠れているマルウェアを検出します。

1:AntiVir ルートキット対策をインストールする

0:AntiVir ルートキット対策をインストールしない (既定)

– `VMWare= 0 | 1`

VMWare オフライン スキャナをインストールします。このモジュールは、VMWare イメージに対してウイルスとマルウェアのオフライン スキャンを実行します。

1:VMWare オフライン スキャナをインストールする

0:VMWare オフライン スキャナをインストールしない (既定)

– `ShellExtension= 0 | 1`

シェル拡張をインストールします。Windows エクスプローラのコンテキスト メニューのエントリを使用して、ディレクトリに対して直接ウイルスと不要プログラムのスキャンを実行できます。

1:シェル拡張をインストールする (既定)

0:シェル拡張をインストールしない

– `Systray= 0 | 1`

Systray ツールをインストールします。保護対象のサーバーの通知領域に、Avira AntiVir Server のトレイ アイコンが表示されます。このトレイ アイコンにより、Avira AntiVir Server の状況を監視し、Avira AntiVir Server の他の機能にアクセスできます。

1:Systray ツールをインストールする (既定)

0:Systray ツールをインストールしない

– `GUI= 0 | 1`

AntiVir サーバー コンソールのユーザー インターフェイスをインストールします。これにより、保護対象のサーバー上で実行されている AntiVir サーバー サービスをリモートに管理および設定できます。

1:AntiVir サーバー コンソールをインストールする (既定)

0:AntiVir サーバー コンソールをインストールしない

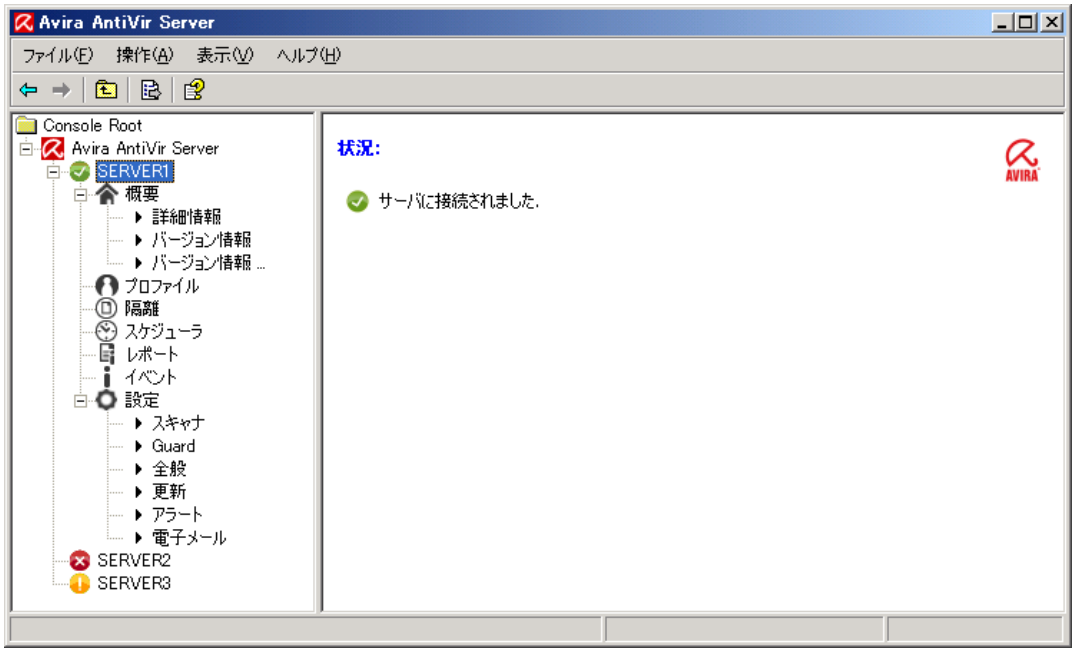
[フィードバック]セクションで、セットアップはエラー コードとセットアップによって報告されたエラー テストを入力します。

例: `ErrCode=0`
`ErrMsg=`製品は正常にインストールされました

# 5 ユーザー インターフェイスと操作

## 5.1 ユーザー インターフェイス: AntiVir Server コンソール

保護対象のサーバーにインストールした Avira AntiVir Server サービスは、**AntiVir Server コンソール**を使用して管理します。AntiVir Server コンソールは、Microsoft 管理コンソール (MMC) のスナップインです。AntiVir Server コンソール上でサーバーを設定および監視するために、保護する任意の数のサーバーを AntiVir Server コンソール上で作成できます。




**注意**
このヘルプでは、AntiVir Server コンソール独自の要素のみについて説明しています。MMC の説明やスナップインを手動で統合する方法については、オペレーティング システムのユーザー マニュアルまたはオンライン ヘルプを参照してください。

### AntiVir Server コンソールの開始と終了

Windows の [スタート] メニューまたは **[すべてのプログラム]** の **[Avira AntiVir Server ユーザー インターフェイス]** リンクを使用して、AntiVir Server コンソールを起動します。AntiVir Server コンソールは MMC で直接読み込むこともできます。事前に設定された AntiVir Server コンソールは、AntiVir Server コンソールのインストール先ディレクトリにあります。AntiVir Server コンソールを閉じるには、MMC を閉じる必要があります。

### 操作

- MMC の左側のウィンドウでコンソール構造内を移動します。ナビゲーション要素は、MMC の右側の詳細ウィンドウにもオブジェクトとして表示されます。これらのオブジェクトをダブルクリックすると、詳細ウィンドウに内容が表示されます。設定は、**[設定]** ノードの下にあります。詳細ウィンドウでは、さまざまな設定セクションを選択できます。選択したセクションを設定できる **[設定]** ウィンドウが開きます。
- 詳細ウィンドウのアイコンに加え、個々のコンソール ノードまたは詳細ウィンドウのオブジェクトのコンテキスト メニューを利用して、さまざまなコマンドおよびアクションを実行できます。
- サーバーの設定において新しい設定を有効にするには、**[設定]** ウィンドウの **[OK]** ボタンまたは **[確認]** ボタンを使用して情報を確定する必要があります。設定をキャンセルするには、**[キャンセル]** ボタンを使用します。

### AntiVir Server コンソールの概要

**Avira AntiVir Server**

- 作成されたサーバーと接続状態の表示
- アクション: サーバーの追加

**注意**
ローカル AntiVir サーバーおよび登録ユーザーによって追加されたすべての AntiVir サーバーが AntiVir Server コンソールに表示されます。

**サーバー**

- サーバーの状態の表示
- アクション: 製品の更新の開始、ライセンス ファイルの更新、設定の再読み込み、レポート ファイルの表示、サーバー名の変更、サーバーの切断、サーバーの接続、サーバーの削除

**概要**

以下の項目の概要

- システムの状態 (最終システム テスト、最終更新、ライセンス)
- Guard のオンアクセス スキャンおよびスキャナのオンデマンド スキャンの統計データ
- プログラムのバージョン
- 問い合わせ先およびサポート連絡先

**プロファイル**

- 既定のプロファイルおよびオンデマンド スキャン用に作成されたプロファイルの表示
- アクション: プロファイルの新規作成、プロファイル名の変更、プロファイルの削除

**隔離**

- [隔離] 内のオブジェクトの表示
- アクション: オブジェクト プロパティの表示、オブジェクトの復元、隔離へのファイルの追加、Avira マルウェア研究センターへのオブジェクトの送信、オブジェクトの削除

**Scheduler**

- 作成されたすべてのスキャン ジョブおよび更新ジョブの表示
- アクション: 新しいジョブの挿入、ジョブ プロパティの表示、ジョブの編集、ジョブの削除

レポート

- オンデマンド スキャンのスキャンおよび更新のレポートの表示
- レポートの表示、レポート ファイルの表示、レポートの印刷、レポートの削除

イベント

- 保護対象のサーバー上の Avira AntiVir Server サービスでのすべてのイベントの表示
- アクション: イベントの表示、イベントのエクスポート、イベントの削除

設定

- 保護対象のサーバー上の Avira AntiVir Server サービスの設定
  設定セクション:
- **スキャナ**: オンデマンド スキャンの設定
- **Guard**: オンアクセス スキャンの設定
- **全般**: オンデマンド スキャンおよびオンアクセス スキャンのための拡張リスク カテゴリ、Avira AntiVir コンソール上のサーバーのパスワード保護、古い Avira AntiVir サーバーに対するセキュリティ アラート、使用するディレクトリ、レポートおよびイベント ログの制限
- **更新**: Web サーバーまたはファイル サーバー経由のダウンロード、製品の更新、ダウンロード サーバーへの接続の設定
- **アラート**: Guard およびスキャナのネットワーク アラートの設定
- **電子メール**: Guard、スキャナ、アップデータ モジュールから SMTP 経由の電子メール アラートの設定

## 5.2 ユーザー インターフェイス: トレイ アイコン

Avira AntiVir Server サービスがインストールされると、保護対象のサーバーの通知領域に Avira AntiVir サーバー トレイ アイコンが表示されます。トレイ アイコンは、AntiVir Guard サービスの状況を表示します。

| アイコン | 説明 |
|---|---|
|  | AntiVir Guard が有効になっています。 |
|  | AntiVir Guard が無効になっています。 |

トレイ アイコンのコンテキスト メニューから機能にアクセスできます。コンテキスト メニューを開くには、トレイ アイコンを右マウス ボタンでクリックします。

- *AntiVir の起動*: 接続されている AntiVir Server を管理するための AntiVir Server コンソールを開きます。このオプションは、AntiVir Server コンソールがコンピュータにローカルにインストールされている場合、および管理者権限でコンピュータにログオンしている場合にのみ使用できます。

- *'マイ ドキュメント' をチェック:* スキャナのスキャン プロファイル "マイ ドキュメント" を開始します。ログインしているユーザーの既定の "マイ ファイル" の場所に対して、ウイルスと不要プログラムのスキャンが実行されます。
- *ヘルプ*: オンライン ヘルプを開きます。
- *インターネット上の Avira*: Avira Web ポータルを開きます。

**注意**
AntiVir Server コンソールは、トレイ アイコンをダブルクリックして開くこともできます。

## 5.3 クイック スタート

Avira AntiVir Server を初めて使用する場合は、次の手順を実行してください。

**1.インストール**

ウイルスや不要プログラムから保護する必要のあるサーバーに Avira AntiVir Server サービスをインストールします。ネットワーク上の 1 台以上のコンピュータに AntiVir Server コンソールをインストールします。
「インストール」の章を参照。

**2.AntiVir Server コンソールの管理**

サーバーの追加

AntiVir Server コンソール上で管理するすべてのサーバーを、AntiVir Server コンソールに追加します。
「AntiVir Server コンソール」の章を参照してください。

追加したサーバーごとに、次の手順を実行します。

設定

保護対象のサーバー上の Avira AntiVir Server サービスを設定します。AntiVir Server コンソール上のサーバーのパスワードを割り当てます。
設定および設定::全般::パスワードの章を参照してください。

更新およびシステム スキャンの実行

最初に、更新を 1 回実行します。そのためには、**Scheduler** で更新ジョブを作成します。開始時間として [即時] を選択します。完全システム スキャンを実行します。そのためには、**Scheduler** でスキャン ジョブを作成します。スキャン ジョブのプロファイルとして [ローカル ハード ディスク] を選択し、開始時間として [即時] を選択します。
「Scheduler」の章を参照してください。

スキャンおよび更新ジョブの定義

スキャンおよび更新ジョブを定義します。スキャナのスキャンを設定するには、最初に、必要に応じて **[Scheduler]** の下でユーザー定義プロファイルを作成します。次に、スキャンを作成し、**[Scheduler]** の下でジョブを更新します。
「スキャン」および「Scheduler」の章を参照してください。

# 6 スキャナ

## 6.1 スキャナ

スキャナ コンポーネントを使用すると、ウイルスと不要プログラムに対する対象を絞ったスキャン (オンデマンド スキャン) を実行できます。ファイルの感染を調べるスキャンでは、次のオプションを使用できます。

- **Scheduler 内のスキャン (リモートおよびローカル)**
  Scheduler には、保護対象のサーバーでスキャン ジョブを実行する時間をスケジュールするオプションがあります。
- **プロファイルによるスキャン (リモートおよびローカル)**
  プロファイルを使用すると、定義および設定されたスキャン プロファイルを保護対象のサーバーで開始できます。
- **シェル拡張: Windows エクスプローラのコンテキスト メニューからスキャン (ローカルのみ)**
  スキャンするディレクトリのコンテキスト メニューの [**選択したファイルを AntiVir でスキャン**] エントリを使用して、そのディレクトリに対してウイルスと不要プログラムをスキャンするオプションがあります。[**シェル拡張**] 機能は、ユーザー定義のインストール中に選択された場合のみ使用できる、追加のコンポーネントです。
- **トレイ アイコンのコンテキスト メニューを使用した独自のドキュメントのスキャン (ローカルのみ)**

トレイ アイコンのコンテキスト メニューの **[マイ ドキュメント]** エントリを選択すると、保護対象のサーバーにある Windows の [マイ ファイル] ユーザー ディレクトリに対して、ウイルスと不要プログラムのスキャンを開始できます。

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

- *[ルートキットおよびアクティブなマルウェアに対するスキャン]* スキャン プロファイルにより、ルートキットをスキャンします。
- **[アクティブなプロセス]** スキャン プロファイルを使用してアクティブなプロセスをスキャンします。
- **[設定]::[スキャナ]::[スキャン]::[その他の設定]** の対応するオプションを有効にして、すべてのスキャン プロファイルのブート セクタ ウイルスをスキャンします。

# 7 更新

アンチウイルス ソフトウェアの有効性は、スキャン エンジンと、最新のウイルス定義が使用されているかどうかに依存します。したがって、Avira AntiVir Server の更新プログラムをダウンロード サーバーから定期的にダウンロードする必要があります。定期的な更新を実行するために、アップデータ コンポーネントは Avira AntiVir Server に統合されています。アップデータ コンポーネントは、次のプログラム コンポーネントを更新します。

- ウイルス定義ファイル
- スキャン エンジン
- プログラム ファイル (製品の更新プログラム)

AntiVir サーバー コンソール上の Scheduler 機能により、指定した間隔で AntiVir アップデータによって実行される更新ジョブを作成できます。AntiVir サーバーのインストール後に、既定では 60 分 の間隔で実行される更新ジョブが作成されます。

更新オーダーごとに、ウイルス定義ファイルおよびスキャン エンジンの状態がチェックされ、必要に応じて更新されます。必要な場合は、設定に合わせて製品の更新が実行されます。AntiVir サーバー コンソール上のサーバー ノードにあるコンテキスト メニューから、手動による製品の更新を開始できます。製品が更新された場合にのみ、更新後にシステムの再起動が必要になります。

更新プログラムは、次の方法で入手できます。

- **Avira GmbH の Web サーバー**を介して**インターネット**から直接入手する。
- **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**から入手する。これらのサーバーは、マスタ サーバーとしてインターネットから更新ファイルをダウンロードし、他のサーバーに配信します。これは、Avira AntiVir Server をネットワーク上の複数のコンピュータで更新する場合に便利です。イントラネット上のダウンロード サーバーを使用すると、最低限のリソースで、保護対象のコンピュータの Avira AntiVir Server を最新状態にすることができます。イントラネット上で機能するダウンロード サーバーを設定するには、Avira AntiVir Server の更新構造と互換性のあるサーバーが必要です。

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。更新は AntiVir Server コンソール上で設定されます。

**注意**
AntiVir Internet Update Manager (Windows のファイル サーバーまたは Web サーバー) を、イントラネット上の Web サーバーまたはファイル サーバーとして使用できます。AntiVir Internet Update Manager は、Avira AntiVir 製品 (Avira AntiVir Server 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 (Avira Web サイト) から入手できます。
http://www.avira.jp

# 8　ウイルスなど

## 8.1 ウイルスとその他のマルウェア

**アドウェア**

アドウェアとは、コンピュータ画面にバナー広告やポップアップ ウィンドウを表示させるソフトウェアです。このような広告は、通常は削除できず、常に表示されたままになります。接続データから、ユーザーの行動に関する多数の情報が得られることになり、データ セキュリティの点で問題があります。

**バックドア**

バックドアは、コンピュータ アクセスのセキュリティ メカニズムをバイパスし、コンピュータへのアクセスを取得します。

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

**ブート ウイルス**

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

**ボットネット**

ボットネットとは、互いに通信するボットで構成された、インターネット上の PC のリモート ネットワークと定義されます。ボットネットは、共通のコマンドと制御インフラストラクチャの下で、通常、ワームやトロイの木馬などと呼ばれるプログラムを実行する、クラックされたコンピュータで構成されます。ボットネットは、サービス拒否攻撃など、通常は感染した PC のユーザーの気付かないところでさまざまな目的に使用されます。ボットネットの主な潜在リスクは、ネットワークを通して数千台ものコンピュータを一括して操作できるため、それらのコンピュータがアクセスする際に発生するデータ転送量の合計が爆発的に増大するということです。

**エクスプロイト**

エクスプロイト (セキュリティ ギャップ) とは、コンピュータ システムのバグ、誤作動、脆弱性、特権の昇格、サービス拒否などを利用したコンピュータ プログラム、またはスクリプトです。たとえば、悪用の 1 つの形態として、操作されたデータ パッケージを使用したインターネットからの攻撃が考えられます。より高レベルのアクセス権を取得するために、エクスプロイトを利用してシステムにプログラムが侵入する場合もあります。

### デマウイルス

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

### ハニーポット

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

### マクロ ウイルス

マクロ ウイルスとは、WinWord 6.0 の WordBasic など、アプリケーションのマクロ言語で記述された小さなプログラムで、通常、そのアプリケーションの文書内でのみ広がります。このため、文書ウイルスとも呼ばれます。マクロ ウイルスがアクティブになるには、対応するアプリケーションがアクティブ化されていて、感染したマクロのいずれかが実行される必要があります。"通常の" ウイルスとは異なり、マクロ ウイルスは実行ファイルの攻撃は行いませんが、対応するホスト アプリケーションの文書を攻撃します。

### ファーミング

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

### フィッシング

フィッシングとは、インターネット ユーザーの個人データを釣るという意味です。フィッシング詐欺師は、通常、電子メールなどで一見正式に思われるレターをユーザーに送信し、送信元を信用させて、ユーザー名とパスワード、オンライン バンキング口座の PIN や TAN などの機密情報を提供させるようにしむけます。フィッシング詐欺師は、盗んだアクセスの詳細情報を使用してユーザーを装い、その名前で取引を実行します。銀行や保険会社が、クレジット カード番号、PIN、TAN、その他アクセスの詳細を電子メール、SMS、または電話で問い合わせることはあり得ません。

### ポリモフィック ウイルス

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

### プログラム ウイルス

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

### ルートキット

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

### スクリプト ウイルスとワーム

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

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

ワームとは、それ自体が増殖するプログラムですが、ホストに感染することはありません。このため、ワームが他のプログラム シーケンスの一部を構成することはありません。セキュリティ対策が限られたシステムで、唯一、あらゆる種類のプログラムに侵入して損傷を与える可能性を持つのがワームです。

### スパイウェア

スパイウェアとは、スパイ プログラムのことで、ユーザーによる同意なく、コンピュータの操作を妨害したり一部を制御します。スパイウェアは、感染したコンピュータを利用して商業的な利益を得るために設計されています。

### トロイの木馬

トロイの木馬は、現在では非常によく見られます。トロイの木馬とは、特定の機能を持つように見せかけて、実行後に正体を表し、多くの場合、破壊的な機能を実行するプログラムです。トロイの木馬は自ら増殖できないところが、ウイルスやワームとは異なります。ユーザーがトロイの木馬を開始するようにしむけるため、大多数には興味をそそるような名前 (SEX.EXE、STARTME.EXE など) が付いています。実行すると、直ちにアクティブになり、ハードディスクをフォーマットする場合もあります。埋め込み型とは、ウイルスを "埋め込む" トロイの木馬の特殊な形態で、コンピュータ システムにウイルスを埋め込みます。

### ゾンビ

ゾンビ PC とは、マルウェア プログラムに感染して、ハッカーがリモート コントロールで犯罪目的に利用できるコンピュータです。コマンドを受けると、感染した PC はスパムやフィッシング電子メールの送信などのサービス拒否 (DoS) 攻撃を開始します。

## 8.2 脅威カテゴリ (拡張)

### ダイヤラ (DIALER)

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

電話の請求書を介したオンライン コンテンツの販売は合法で、ユーザーにとっても有益な場合があります。正規のダイヤラは、間違いなくユーザーが意図的に使用するものです。ユーザーの同意により、ユーザーのコンピュータにインストールされるだけであり、これは完全に明白ではっきりとわかるラベル、またはリクエストを介して行われる必要があります。正規のダイヤラのダイアルアップ プロセスは明確に表示されます。また、正規のダイヤラによって発生した費用は正確に間違いなく伝達されます。

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

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

AntiVir プログラムは、よく使用されるダイヤラを既定で検出します。

[脅威カテゴリ (拡張)] の設定でチェック マークをオンにして **[ダイヤラ]** オプションを有効にすると、ダイヤラが検出されたときに、対応するアラートが送信されます。不要な 0190/0900 ダイヤラである可能性のあるダイヤラは簡単に削除できます。必要なダイアルアップ プログラムである場合は、例外的なファイルであることを宣言すると、その後、そのファイルはスキャンされなくなります。

### ゲーム (GAMES)

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

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

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

### ジョーク (JOKES)

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

ただし、注意してください。ジョーク プログラムのあらゆる現象は、ウイルスやトロイの木馬が原因となっている可能性もあります。少なくとも、自分自身が本当に被害を被ったとなれば、大きなショックを受けパニックになるでしょう。

スキャンと識別ルーチンの拡張により、AntiVir プログラムはジョーク プログラムを検出し、必要に応じて、これらのファイルを不要プログラムとして排除できます。[脅威カテゴリ] の設定にチェック マークを入れて **[ジョーク]** オプションを有効にすると、ジョーク プログラムが検出された場合に対応するアラートが送信されます。

### セキュリティ プライバシ リスク (SPR)

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

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

### バックドア クライアント (BDC)

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

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

### アドウェア/スパイウェア (ADSPY)

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

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

### 通常とは異なるランタイム圧縮 (PCK)

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

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

### 二重の拡張子ファイル (HEUR-DBLEXT)

実際のファイル拡張子を不審な方法で非表示にしている実行ファイルです。このカムフラージュ方法は、マルウェアによく使用されます。

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

### フィッシング

フィッシングは、*ブランドスプーフィング*とも呼ばれ、インターネット サービス プロバイダ、銀行、オンライン バンキング サービス、登録認定機関などの顧客や潜在顧客のデータを巧妙な手段で盗み出すものです。
インターネットで電子メール アドレスを送信、オンライン フォームに入力、ニュースグループや Web サイトにアクセスすると、データがインターネットをクロールするスパイダによって盗まれ、許可なく詐欺やその他の犯罪に使用される可能性があります。

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

### アプリケーション (APPL)

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

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

# 9 情報とサービス

この章には、弊社への連絡方法に関する情報が含まれています。

「連絡先住所」の章を参照。

「テクニカル サポート」の章を参照。

「疑わしいファイル」の章を参照。

「誤検出レポート」の章を参照。

「フィードバックの送付」の章を参照。

## 9.1 テクニカル サポート

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

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

http://www.avira.jp/support

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

- **ライセンス情報**。この情報は、ヘルプ::Avira AntiVir Server バージョン情報::ライセンス情報の下のプログラム インターフェイスで確認できます。
- **バージョン情報**。この情報は、ヘルプ::Avira AntiVir Server バージョン情報::バージョン情報の下のプログラム インターフェイスで確認できます。
- **オペレーティング システムのバージョン**およびインストールされているサービス パック。
- **インストールされているソフトウェア パッケージ** (例: 他のベンダのアンチウイルス ソフトウェア)
- プログラムまたはレポート ファイルの**正確なメッセージ**。

## 9.2 疑わしいファイル

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

- AntiVir Server コンソールの[隔離] でファイルを確認し、コンテキスト メニューまたは対応するボタンを使用して、項目 [ファイルの送信] を選択します。

- ファイルは圧縮して (WinZIP、PKZip、Arj など) 電子メールの添付ファイルとして以下のアドレスにお送りください。
  virus@avira.jp
  電子メール ゲートウェイの一部はアンチウイルス ソフトウェアと連携しているため、パスワードとファイルを提供していただく必要もあります (必ずパスワードを提供してください)。

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

## 9.3 誤検出レポート

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

- virus@avira.jp

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

## 9.4 フィードバックの送付

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

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

vulnerabilities@avira.jp

# 10 参照: 設定オプション

設定の参考資料には、使用可能なすべての設定オプションが文書化されています。

## 10.1 スキャナ

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

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

**ファイル**

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

**すべてのファイル**

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

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

**スマートなファイル タイプ判別**

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

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

**ファイル拡張子リストを使用**

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

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

**ファイル拡張子**

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

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

### その他の設定

**選択したドライブのブート セクタをスキャン**

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

**マスタ ブート セクタをスキャン**

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

**オフライン ファイルを無視**

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

**最適化されたスキャン**

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

**注意**
このオプションは、マルチ プロセッサ システムでのみ利用できますが、設定では常に表示され、有効にすることができます。管理対象のサーバーに、複数のプロセッサが搭載されていない場合、スキャナ オプションは使用されません。

**シンボリック リンクのリンク先をスキャンする**

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

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

スキャン前にルートキットを検索

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

重要
このルートキットは、Windows XP 64 ビット、Windows 2003 64 ビット、および Windows Server 2003 64 ビットでは使用できません。

**重要**
ルートキット スキャンは、リモートで実行されません。

レジストリをスキャン

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

ネットワーク ドライブ上のファイルまたはパスをスキャンしない

**スキャン プロセス**

スキャナの優先度

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

*低*

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

*中*

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

*高*

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

## 10.1.1 検出時のアクション

**検出時のアクション**

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

隔離にバックアップ

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

***プライマリ アクション***

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

**注意**

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

***修復***

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

**注意**

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

***削除***

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

***上書きおよび削除***

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

***名前の変更***

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

***無視***

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

**警告**

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

***隔離***

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

***セカンダリ アクション***

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

***削除***

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

***上書きおよび削除***

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

***名前の変更***

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

***無視***

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

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

***隔離***

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

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

## 10.1.2 その他のアクション

**検出の後にプログラムを起動**

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

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

***プログラム名***

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

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

引数

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

**イベント ログ**

イベント ログの使用

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

## 10.1.3 アーカイブ

## 10.1.4 アーカイブ

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

アーカイブをスキャン

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

すべてのアーカイブ タイプ

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

スマートなファイル タイプ判別

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

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

再帰の深さ

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

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

**最大の再帰レベル**

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

**既定値**

このボタンは、スキャン アーカイブに対する事前に設定済みの値を復元します。

**アーカイブ**

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

## 10.1.5 例外

**スキャナのスキャン対象から除外するファイル オブジェクト**

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

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

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

**警告**
これらのファイルはスキャンに含まれません。

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

**入力ボックス**

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

...

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

追加

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

削除

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

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

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

### 10.1.6 ヒューリスティック

この設定セクションには、スキャン エンジンのヒューリスティック スキャン機能に対する設定が含まれます。

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

**マクロウイルス ヒューリスティック**

マクロウイルス ヒューリスティック

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

**高度なヒューリスティック分析と検出 (AHeAD)**

**AHeAD を有効にする**

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

**低検出レベル**

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

**中検出レベル**

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

**高検出レベル**

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

## 10.1.7 レポート

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

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

**レポート**

**オフ**

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

**既定**

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

**詳細**

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

完了

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

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

## 10.2 Guard

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

### スキャン モード

ここで、ファイルをいつスキャンするかを定義します。

読み取り時にスキャン

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

書き込み時にスキャン

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

読み取り時と書き込み時にスキャン

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

### ファイル

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

すべてのファイル

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

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

スマートなファイル タイプ判別

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

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

**ファイル拡張子リストを使用**

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

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

**ファイル拡張子**

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

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

### アーカイブ

**アーカイブをスキャン**

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

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

***最大の再帰レベル***

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

***最大ファイル数***

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

***最大サイズ (KB)***

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

**ドライブ**

**ローカル ドライブ**

このオプションをアクティブ化すると、HDU、CD、フロッピー ドライブ、MO および ZIP ドライブなどのローカル ドライブのファイルのみが監視されます。このオプションは初期状態で有効に設定されています (推奨の設定)。

**ネットワーク ドライブ**

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

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

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

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

**キャッシュを有効にする**

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

## 10.2.1 検出時のアクション

**検出時のアクション**

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

**拡張ターミナル サーバー サポート**

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、オンアクセス スキャン中にダイアログ ボックスが表示され、関連するファイルをどう処理するかを選択できます。

***修復***

Guard は、可能な場合、感染したファイルを修復します。

***名前の変更***

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

***隔離***

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

***削除***

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

***無視***

ファイルへのアクセスは許可され、ファイルは無視されます。

***上書きおよび削除***

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

**既定**

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

**注意**
**修復**アクションを既定のアクションとして選択することはできません。

**自動**

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

**隔離にバックアップ**

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

**検出アラートを表示**

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

***プライマリ アクション***

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

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

***修復***

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

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

***削除***

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

***上書きおよび削除***

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

***名前の変更***

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

***無視***

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

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

***アクセスの拒否***

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

***隔離***

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

***セカンダリ アクション***

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

***削除***

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

***上書きおよび削除***

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

***名前の変更***

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

***無視***

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

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

***アクセスの拒否***

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

***隔離***

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

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

## 10.2.2 その他のアクション

**通知**

**イベント ログ**

**イベント ログの使用**

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

## 10.2.3 例外

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

**Guard がスキャン対象から除外するプロセス**

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

入力ボックス

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

**注意**
プロセスは最大 128 件まで入力できます。

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

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

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

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

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

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

このボタンでウィンドウが開き、実行可能ファイルを選択できます。

**追加**

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

**削除**

このボタンを使用すると、選択したプロセスを表示ウィンドウから削除できます。

### Guard がスキャン対象から除外するファイル オブジェクト

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

**入力ボックス**

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

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

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

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

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

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

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

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


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

**追加**

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

**削除**

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

除外を指定する場合について、さらに以下のことに注意してください。

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

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

例:

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

このエントリは有効ではありません。例外として処理できません。

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

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

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

除外するプロセスの例:

- application.exe

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

- C:\Program Files1\Application.exe

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

- C:\Program Files1*.exe

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

除外対象ファイルの例:

- *.mdb

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

- *.xls*

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

- C:\Directory*.log

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

– \\Computer name\Shared1\

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

– \\1.0.0.0\Shared1*.mdb

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

-

## 10.2.4 製品

**Guard でスキップする製品**

この表示ボックスで、Guard のスキャン対象から除外する製品を選択できます。選択した製品のすべてのアプリケーション、サービス、またはデータベースは、Guard の監視対象から除外されます。

## 10.2.5 ヒューリスティック

この設定セクションには、スキャン エンジンのヒューリスティック スキャン機能に対する設定が含まれます。

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

**マクロウイルス ヒューリスティック**

マクロウイルス ヒューリスティック

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

#### 高度なヒューリスティック分析と検出 (AHeAD)

**AHeAD** を有効にする

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

低検出レベル

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

中検出レベル

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

高検出レベル

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

### 10.2.6 レポート

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

#### レポート

このグループを使用すると、レポート ファイルの内容を指定できます。

オフ

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

既定

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

詳細

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

完了

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

#### レポート ファイルの制限

サイズを **n** **MB** に制限

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

**短縮前にレポート ファイルをバックアップ**

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

**設定をレポート ファイルに書き込む**

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

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

# 10.3 全般

## 10.3.1 脅威カテゴリ

**脅威カテゴリの選択**

AntiVir 製品によってコンピュータ ウイルスから保護されます。

また、次の脅威カテゴリ (拡張) に従ってスキャンできます。

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

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

**すべて選択**

このオプションを有効にすると、すべてのタイプが有効になります。

既定値

このボタンは事前に設定済みの既定値を復元します。

**注意**

タイプを無効にすると、関連するプログラム タイプで認識されていたファイルは認識されなくなります。レポート ファイルにエントリは書き込まれません。

## 10.3.2 パスワード

パスワードを使用して、AntiVir Server コンソールで保護するサーバーへのアクセスを保護できます。サーバーのパスワードは、サーバーへの接続を行うときに必ず入力する必要があります。パスワードで保護されたサーバーへの接続は、AntiVir Server コンソールを閉じるとすぐに終了します。

**パスワード**

パスワードの入力

パスワードをここに入力します。セキュリティ上の理由から、このスペースに実際に入力する文字は、アスタリスク (*) に置換されます。パスワードは、最大 20 文字です。パスワードが設定されると、正しくないパスワードを入力した場合、プログラムはアクセスを拒否します。空のボックスは "パスワードが未設定" であること意味します。

パスワードの確認

上で入力したパスワードをここに再度入力します。セキュリティ上の理由から、このスペースに実際に入力する文字は、アスタリスク (*) に置換されます。

**注意**

パスワードでは、大文字と小文字が区別されます!

## 10.3.3 セキュリティ

**更新**

最終更新日が次の日数より古い場合、アラートを表示

このボックスに、最終更新から許容される最大経過日数を入力できます。この日数を経過した場合は、[概要] の [状況] に赤いアイコンが表示され、更新の状況が示されます。

ウイルス定義ファイルが古い場合に注意を表示

このオプションを有効にすると、ウイルス定義ファイルが最新でない場合に、アラートが送信されます。アラート オプションを使用すると、最終更新から何日以上経過した場合にアラートが送信されるかを時間間隔で設定できます。

## 10.3.4 WMI

### Windows Management Instrumentation のサポート

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

**WMI のサポートを有効にする**

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

**サービスの有効化/無効化の操作を許可**

このオプションを有効にすると、WMI を介してプログラム サービスを有効/無効にすることができます。

## 10.3.5 イベント

### イベント データベース サイズの制限

**イベントの最大数を n エントリに制限**

このオプションを有効にすると、イベント データベースに列挙されるイベントの最大数を特定のサイズに制限できます。可能な値: 100 ～ 10000 エントリ。入力したエントリ数を超えると、最も古いエントリが削除されます。

**n 日より古いイベントを削除**

このオプションを有効にすると、イベント データベースに列挙されるイベントは、特定の期間後に削除されます。可能な値: 1 ～ 90 日。このオプションは初期状態で有効に設定されていて、既定値は 30 日です。

**イベント データベース サイズを制限しない (イベントを手動で削除)**

このオプションを有効にすると、イベント データベースのサイズが制限されなくなります。ただし、[イベント] の下のプログラム インターフェイスでは、最大 20,000 エントリが表示されます。

## 10.3.6 レポート

レポート数を制限

**数を n 個に制限**

このオプションを有効にすると、レポートの最大数が指定した量に制限されます。許容される値は 1 ～ 300 です。指定した数字を超えると、その時点で最も古いレポートが削除されます。

**n 日より古いすべてのレポートを削除**

このオプションを有効にすると、特定の日数の後、レポートは自動的に削除されます。許容される値: 1 ～ 90 日。このオプションは初期状態で有効に設定されていて、既定値は 30 日です。

**レポート数を制限しない (レポートを手動で削除)**

このオプションを有効にすると、レポートの数が制限されなくなります。

## 10.3.7 ディレクトリ

**一時フォルダ パス**

この入力ボックスに、プログラムが一時ファイルを格納するパスを入力します。

**既定のシステム設定を使用**

このオプションを有効にすると、一時ファイルの処理にシステムの設定が使用されます。

**以下のディレクトリを使用**

このオプションを有効にすると、入力ボックスに表示されるパスが使用されます。

このボタンをクリックするとウィンドウが開き、必要な一時パスを選択できます。

**既定**

このボタンは、一時パスに対する事前に設定済みのディレクトリを復元します。

**レポート ディレクトリ**

この入力ボックスには、レポート ファイルへのパスが含まれています。

このボタンでウィンドウが開き、必要なディレクトリを選択できます。

**既定**

このボタンは、レポート ディレクトリに対する事前定義のパスを復元します。

**[隔離] ディレクトリ**

このボックスには、[隔離] ディレクトリへのパスが含まれています。

このボタンでウィンドウが開き、必要なディレクトリを選択できます。

**既定**

このボタンは、[隔離] ディレクトリへの事前定義のパスを復元します。

# 10.4 更新

## 10.4.1 更新

ダウンロード サーバーへの接続は *[更新]* セクションで設定します。

**ダウンロード**

**Web サーバーを経由**

更新は HTTP 接続を使用して Web サーバー経由で実行されます。インターネット上の専用の Web サーバーを使用するか、イントラネット上の Web サーバーを使用できます。後者の場合、イントラネット上の Web サーバーがインターネット上の専用のダウンロード サーバーから更新プログラムを取得します。

**注意**
このオプションを有効にすると、Web サーバー、および必要に応じてプロキシ サーバーを設定できます。

**ファイル サーバー/共有フォルダを経由**

インターネット上の専用のダウンロード サーバーから更新プログラムを取得する、イントラネット上のファイル サーバー経由で、更新が実行されます。

**注意**
このオプションを有効にすると、使用するファイル サーバーを設定できます。

**[製品の更新]** の下で、製品の更新プログラムをどのように処理するか、利用可能な更新プログラムの通知をどのように処理するかを設定します。

**製品の更新**

**製品の更新プログラムをダウンロードして、自動的にインストールする**

このオプションを有効にすると、製品更新の時間を定義できます。製品を更新する日時を指定してください。製品の更新プログラムを利用できる場合は、この時間に製品の更新が実行されます。ウイルス定義ファイルとスキャン エンジンへの更新は、この設定とは無関係に実行されます。このオプションの条件: すべてのアップデート設定が完了しており、ダウンロード サーバーへの接続が利用可能である必要があります。製品の更新が実行されると、保護対象のサーバーを管理するために使用された AntiVir Server コンソールでアラートが表示されます。

**製品の更新プログラムをダウンロードする。再起動が必要な場合は、システムの再起動後に更新プログラムをインストールします。再起動が必要ない場合は、すぐに更新プログラムをインストールします。**

このオプションを有効にすると、製品の更新プログラムが利用可能になると直ぐにダウンロードされます。再起動が必要でない場合、更新プログラムはダウンロード後に自動的にインストールされます。製品の更新にコンピュータの再起動が必要な場合、更新プログラムはダウンロード直後ではなく、ユーザーによる次回のシステムの再起動時に実行されます。これには、ユーザーがコンピュータで作業中は再起動が実行されないという利点があります。ウイルス定義ファイルとスキャン エンジンへの更新は、この設定とは無関係に実行されます。このオプションの条件: すべてのアップデート設定が完了しており、ダウンロード サーバーへの接続が利用可能である必要があります。

**製品の新しい更新プログラムが使用可能になったら通知**

このオプションを有効にすると、製品の新しい更新プログラムが利用可能になると電子メールで通知されます。ウイルス定義ファイルとスキャン エンジンへの更新は、この設定とは無関係に実行されます。このオプションの条件: すべてのアップデート設定が完了しており、ダウンロード サーバーへの接続が利用可能である必要があります。電子メール通知を設定すると、AntiVir Server コンソールと電子メールによる通知が行われます。

**次の期間経過後に再度通知**

製品の更新プログラムが最初の通知後にインストールされなかった場合に、製品の更新プログラムが利用可能であると再通知されるまでに経過する日数を、このボックスに入力します。

**製品の更新プログラムをダウンロードしない**

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

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

アップデートは、インターネット上で直接 Web サーバーを介して、またはイントラネットで実行されます。

### ダウンロード

**標準のサーバー**

更新プログラムおよびその必須の更新ディレクトリ 'update' を読み込む予定の Web サーバーのアドレス (URL) を入力します。Web サーバーのアドレスの形式は次のとおりです。http://<Web サーバーのアドレス>[:Port]/update。ポートを指定しない場合は、ポート 80 が使用されます。既定では、アクセス可能な Avira GmbH Web サーバーが更新用に指定されます。ただし、企業イントラネットの独自の Web サーバーを使用することもできます。複数の Web サーバーを指定する場合は、それぞれをカンマで区切ります。

**既定**

このボタンは事前に設定済みのアドレスを復元します。

**優先するサーバー**

このフィールドに、更新プログラムを提供するように最初に要求される Web サーバーの update ディレクトリおよび URL を入力します。このサーバーが到達不可能な場合は、表示された標準サーバーが使用されます。Web サーバーのアドレスの形式は次のとおりです。http://<address of web server>[:Port]/update。ポートを指定しない場合は、ポート 80 が使用されます。

## 10.4.2 ファイル サーバー

ネットワークに複数のワークステーションがある場合、AntiVir では、イントラネット上のファイル サーバーから更新プログラムをダウンロードできます。このファイル サーバーがインターネット上の専用のダウンロード サーバーから更新ファイルを取得します。これにより、すべてのワークステーションで AntiVir プログラムが最新であることが確認されます。

**注意**
設定の見出しは、 設定::更新::更新で、**[ファイル サーバー/共有フォルダを経由]** オプションが選択されている場合にのみ有効になります。

**ダウンロード**

AntiVir プログラムの更新プログラムおよびその必須のディレクトリ '/release/update/' があるファイル サーバーの名前を入力します。次の情報を指定する必要があります。file:// <ファイル サーバーの IP アドレス>/release/update/。'release' ディレクトリは、すべてのユーザーがアクセスできるディレクトリであることが必要です。


このボタンをクリックするとウィンドウが開き、必要なダウンロード ディレクトリを選択できます。

**サーバー ログイン**

ログイン名

サーバーにログインするためのユーザー名をここに入力します。サーバー上で使用されている共有フォルダに対してアクセス権限のあるユーザー アカウントを使用します。

ログイン パスワード

ユーザー アカウントのパスワードを入力します。入力した文字は * として表示されます。

**注意**
サーバー ログイン セクションでデータを指定しない場合は、ファイル サーバーへのアクセス時に認証は実行されません。この場合、ユーザーはファイル サーバーに対して十分な権限を持つことが必要です。

### 10.4.3 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。

**警告**

認証を必要とするプロキシ サーバーを使用している場合、*[このプロキシサーバーを使用]* オプションで必要なすべてのデータを入力します。*[Windows システム設定を使用]* オプションは、認証を利用しないプロキシ サーバーでのみ使用できます。

**このプロキシ サーバーを使用(U)**

Web サーバーの接続がプロキシ サーバーを介してセットアップされている場合は、関連する情報をここに入力できます。

**アドレス**

Web サーバーに接続するために使用するプロキシ サーバーのコンピュータ名または IP アドレスを入力します。

**ポート**

Web サーバーへの接続に使用するプロキシ サーバーのポート番号を入力してください。

**ログイン名**

プロキシ サーバーにログインするためのユーザー名をここに入力します。

**ログイン パスワード**

プロキシ サーバーへのログインに関連するパスワードをここに入力します。セキュリティ上の理由から、このスペースに実際に入力する文字は、アスタリスク (*) に置換されます。

*例:*

| | | | |
|---|---|---|---|
| アドレス: | proxy.domain.com | ポート: | 8080 |
| アドレス: | 192.168.1.100 | ポート: | 3128 |

## 10.5 警告

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

**注意**

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

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

**メッセージの送信先**

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

**注意**
コンピュータは、このリストに 1 回だけ入力できます。

**挿入**

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


このボタンをクリックするとウィンドウが開き、代わりに自分のコンピュータ環境から直接コンピュータを選択することもできます。

**削除**

このボタンを使用すると、現在選択しているエントリをリストから削除できます。

## 10.5.1 Guard

**ネットワーク アラート**

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

**注意**
このオプションを有効にするには、全般::アラート::ネットワークの下に、最低 1 人受信者を入力する必要があります。

**送信メッセージ**

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

メッセージの書式設定には、次のキーの組み合わせを使用できます。

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

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

次のワイルドカードを使用できます。

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

**既定**

このボタンは、アラートに対する事前に設定済みの既定のテキストを復元します。

## 10.5.2 スキャナ

**ネットワーク アラートの有効化**

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

**注意**

このオプションを有効にするには、全般::アラート::ネットワークの下に、最低 1 人受信者を入力する必要があります。

**送信メッセージ**

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

メッセージの書式設定には、次のキーの組み合わせを使用できます。

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

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

次のワイルドカードを使用できます。

| | |
|---|---|
| %VIRUS% | 検出されたウイルスまたは不要プログラムの名前が格納されます。 |
| %NAME% | スキャナを使用するログインしたユーザーの名前が格納されます。 |

既定

このボタンは、アラートに対する事前に設定済みの既定のテキストを復元します。

### 10.5.3 音声によるアラート

**音声によるアラート**

Guard によるスキャン中、ウイルスが検出されたことを通知する音声によるアラートをアクティブまたは非アクティブにすることができます。音声によるアラートは、"*拡張ターミナル サーバー サポート*"のアクション モードでのみ再生されます。音声によるアラートとして、別の Wave ファイルを選択することもできます。

**注意**
Guard のアクション モードは、次の場所で設定します。
設定::Guard::検出に対するアクション

音声によるアラートを行わない

このオプションを有効にすると、Guard によってウイルスが検出されても音声によるアラートは再生されません。

**PC のスピーカで再生 (拡張ターミナル サーバー サポート モードのみ)**

このオプションを有効にすると、Guard によってウイルスが検出されたときの音声によるアラートとして、既定のシグナルが使用されます。音声のアラートが PC の内蔵スピーカーで再生されます。

**次の WAV ファイルを使用 (拡張ターミナル サーバー サポート モードのみ)**

このオプションを有効にすると、Guard によってウイルスが検出されたときの音声によるアラートとして、選択した Wave ファイルが使用されます。選択した Wave ファイルが、外部接続のスピーカで再生されます。

**Wave ファイル**

この入力ボックスに、選択したオーディオ ファイルの名前と関連するパスを入力できます。標準として、プログラムの既定の音声によるシグナルが入力されます。


このボタンをクリックするとウィンドウが開き、ファイル エクスプローラを使用して、必要なファイルを選択できます。

テスト

このボタンは、選択した Wave ファイルのテストに使用します。

## 10.6 電子メール

### 10.6.1 電子メール

特定のイベントで AntiVir プログラムは、1 人以上の受信者に電子メールでアラートとメッセージを送信できます。これは Simple Message Transfer Protocol (SMTP) を使用して行います。

メッセージは、さまざまなイベントによってトリガされます。電子メールの送信をサポートするコンポーネントは以下のとおりです。

- Guard:送信通知
- スキャナ: 送信通知
- アップデータ: 送信通知
- 隔離: Avira マルウェア研究センターへの不審ファイルの送信

**注意**
ESMTP はサポートされていないので注意してください。TLS (Transport Layer Security) または SSL (Secure Sockets Layer) を使用した暗号化された転送も現在は行えません。

**電子メール メッセージ**

**SMTP サーバー**

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

*例:*

192.168.1.100 または mail.samplecompany.com。

**送信者のアドレス**

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

**認証**

一部のメール サーバーでは、電子メールの送信前に、プログラムによるサーバーに対する検証 (ログイン) が必要です。アラートは、SMTP サーバーに対する認証を使用して電子メールで送信できます。

**認証を使用**

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

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

**テスト電子メールの送信**

このボタンをクリックすると、プログラムは入力されたデータの確認のため、送信者のアドレスにテスト電子メールの送信を試みます。

## 10.6.2 Guard

AntiVir Guard では、特定のイベントについて 1 人以上の受信者に電子メールでアラートを送信できます。

### Guard

電子メール アラート

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

以下のイベント向けの電子メール メッセージ

オンアクセス スキャンでウイルスや不要なプログラムを検出。

このオプションを有効にすると、オンアクセス スキャンでウイルスや不要プログラムが検出された場合、ウイルスまたは不要プログラムの名前と感染したファイルの名前が記載された電子メールが送信されます。

編集

"*[編集]*" ボタンをクリックすると、"オンアクセス検出" イベントに対する通知を設定できる "*[電子メール テンプレート]*" ウィンドウが開きます。電子メールの件名行および本文にテキストを挿入するオプションがあります。この目的で変数を使用することもできます (設定::全般::電子メール::アラート::電子メール テンプレートを参照)。

Guard で重大なエラーが発生。

このオプションを有効にすると、重大な内部エラーが検出された場合に電子メールを受信します。

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

編集

*[編集]* ボタンをクリックすると、"Guard で重大なエラーが発生" イベントに対する通知を設定できる *[電子メール テンプレート]* ウィンドウが開きます。電子メールの件名行および本文にテキストを挿入するオプションがあります。この目的で変数を使用することもできます (設定::全般::電子メール::アラート::電子メール テンプレートを参照)。

受信者

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

### 10.6.3 スキャナ

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

**スキャナ**

**電子メール アラートの有効化**

このオプションを有効にすると、特定のイベントが発生した場合、プログラムによって最も重要な情報が記載された電子メール メッセージが送信されます。このオプションは初期状態で無効に設定されています。

**以下のイベント向けの電子メール メッセージ**

**オンデマンド スキャンによりウイルスまたは不要なプログラムを検出**

このオプションを有効にすると、オンデマンド スキャンでウイルスや不要プログラムが検出されると必ず、ウイルスまたは不要プログラムと感染したファイルの名前が記載された電子メールが送信されます。

**編集**

*[編集]* ボタンをクリックすると、"スキャン検出" イベントに対する通知を設定できる *[電子メール テンプレート]* ウィンドウが開きます。電子メールの件名行および本文にテキストを挿入するオプションがあります。この目的で変数を使用することもできます (設定::全般::電子メール::アラート::電子メール テンプレートを参照)。

**スケジュールされたスキャンの終了**

このオプションを有効にすると、スキャン ジョブが終了したときに、電子メールが送信されます。電子メールには、スキャン ジョブの時刻と期間、スキャンされたフォルダとファイル、および検出されたウイルスと警告が含まれます。

**編集**

*[編集]* ボタンをクリックすると、"スキャンの終了" イベントに対する通知を設定できる *[電子メール テンプレート]* ウィンドウが開きます。電子メールの件名行および本文にテキストを挿入するオプションがあります。この目的で変数を使用することもできます (設定::全般::電子メール::アラート::電子メール テンプレートを参照)。

**レポート ファイルを添付ファイルとして追加**

このオプションを有効にすると、スキャナ通知を送信するとき、スキャナ コンポーネントの現在のレポート ファイルが添付ファイルとして電子メールに追加されます。

**受信者のアドレス**

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

### 10.6.4 アップデータ

アップデータ コンポーネントでは、特定のイベントについて 1 人以上の受信者に電子メールで通知を送信できます。

アップデータ

電子メール アラート

このオプションを有効にすると、特定のイベントが発生した場合、アップデータ コンポーネントによって最も重要なデータが記載された電子メール メッセージが送信されます。このオプションは初期状態で無効に設定されています。

以下のイベント向けの電子メール メッセージ

**更新は不要です。プログラムは最新の状態です。**

このオプションを有効にすると、アップデータが正常にダウンロード サーバーに接続したが、サーバー上で使用できる新しいファイルがない場合に電子メールが送信されます。これは、AntiVir プログラムが最新の状態であることを意味します。

**編集**

*[編集]* ボタンをクリックすると、"更新は不要" イベントに対する通知を設定できる *[電子メール テンプレート]* ウィンドウが開きます。電子メールの件名行および本文にテキストを挿入するオプションがあります。この目的で変数を使用することもできます (設定::全般::電子メール::アラート::電子メール テンプレートを参照)。

**更新は正常に終了しました。新しいファイルがインストールされています。**

このオプションを有効にすると、実行されたすべての更新について電子メールが送信されます。 たとえば、製品の更新、ウイルス定義ファイルやスキャン エンジンの更新の場合です。

**編集**

*[編集]* ボタンをクリックすると、"更新の正常終了 – 新しいファイルがインストールされた" イベントに対する通知を設定できる *[電子メール テンプレート]* ウィンドウが開きます。電子メールの件名行および本文にテキストを挿入するオプションがあります。この目的で変数を使用することもできます (設定::全般::電子メール::アラート::電子メール テンプレートを参照)。

**更新は正常に終了しました。新しい製品の更新プログラムを使用できます。**

このオプションを有効にすると、製品の更新プログラムを使用できるが更新を実行せずに、スキャン エンジンまたはウイルス定義ファイルの更新を実行した場合にのみ、電子メールが送信されます。

**編集**

*[編集]* ボタンをクリックすると、"更新の正常終了 - 製品の更新プログラムが利用可能" イベントに対する通知を設定できる *[電子メール テンプレート]* ウィンドウが開きます。電子メールの件名行および本文にテキストを挿入するオプションがあります。この目的で変数を使用することもできます (設定::全般::電子メール::アラート::電子メール テンプレートを参照)。

**更新できませんでした。**

このオプションを有効にすると、エラーにより更新を実行できなかった場合に、電子メールが送信されます。

**編集**

*[編集]* ボタンをクリックすると、"更新の失敗" イベントに対する通知を設定できる *[電子メール テンプレート]* ウィンドウが開きます。電子メールの件名行および本文にテキストを挿入するオプションがあります。この目的で変数を使用することもできます (設定::全般::電子メール::アラート::電子メール テンプレートを参照)。

レポート ファイルを添付ファイルとして追加

このオプションを有効にすると、アップデータ通知を送信するとき、アップデータ コンポーネントの現在のレポート ファイルが添付ファイルとして電子メールに追加されます。

**受信者**

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

**注意**
アップデータ通知用の SMTP サーバーおよび受信者アドレスが設定されている場合は、次のイベントに対するアラートが電子メールで常に送信されます。
プログラムの今後のすべての更新プログラムを使用するには、製品の更新が必要です。
製品の更新が必要なため、スキャン エンジン、またはウイルス定義ファイルの更新を実行できませんでした。

これらのアラートは、アップデータ コンポーネントの電子メール警告の設定にかかわらず送信されます。

## 10.6.5 電子メール テンプレート

*[電子メール テンプレート]* ウィンドウで、有効になっているイベントに対する電子メール通知をコンポーネントごとに設定できます。件名行に最大 128 文字、メッセージ フィールドに最大 1024 文字のテキストを挿入できます。

以下の変数を電子メールの件名およびメッセージで使用できます。

**グローバル変数**

| 変数 | 値 |
|---|---|
| Windows 環境変数 | 電子メール通知コンポーネントはすべての Windows 環境変数をサポートしています。 |
| %SYSTEM_IP% | コンピュータの IP アドレス |
| %FQDN% | 完全修飾ドメイン名 |
| %TIMESTAMP% | イベントのタイム スタンプ: オペレーティング システムの言語設定に従った時間および日付の形式 |
| %COMPUTERNAME% | NetBIOS コンピュータ名 |
| %USERNAME% | コンポーネントにアクセスするユーザーの名前 |
| %PRODUCTVER% | 製品バージョン |
| %PRODUCTNAME% | 製品名 |
| %MODULENAME% | 電子メールを送信するコンポーネントの名前 |
| %MODULEVER% | 電子メールを送信するコンポーネントのバージ |

| | |
|---|---|
| | ョン |

### 固有のコンポーネント変数

| 変数 | 値 | コンポーネント電子メール |
|---|---|---|
| %ENGINEVER% | 使用するスキャン エンジンのバージョン | Guard<br>スキャナ |
| %VDFVER% | 使用するウイルス定義ファイルのバージョン | Guard<br>スキャナ |
| %SOURCE% | 完全修飾ファイル名 | Guard |
| %VIRUSNAME% | ウイルスまたは不要プログラムの名前 | Guard |
| %ACTION% | 検出後に実行するアクション | Guard |
| %MACADDR% | 最初に登録したネットワーク カードの MAC アドレス | Guard |
| %UPDFILESLIST% | 更新するファイルのリスト | アップデータ |
| %UPDATETYPE% | 更新のタイプ: スキャン エンジンおよびウイルス定義ファイルの更新、またはスキャン エンジンおよびウイルス定義ファイルの更新による製品の更新 | アップデータ |
| %UPDATEURL% | 更新に使用するダウンロード サーバーの URL | アップデータ |
| %UPDATE_ERROR% | 更新エラー (ワード単位) | アップデータ |
| %DIRCOUNT% | スキャンされたディレクトリの数 | スキャナ |
| %FILECOUNT% | スキャンされたファイルの数 | スキャナ |
| %MALWARECOUNT% | 検出されたウイルスまたは不要プログラムの数 | スキャナ |
| %REPAIREDCOUNT% | 修復された、感染し | スキャナ |

| | | |
|---|---|---|
| | たファイルの数 | |
| %RENAMEDCOUNT% | 名前を変更された、感染したファイルの数 | スキャナ |
| %DELETEDCOUNT% | 削除された、感染したファイルの数 | スキャナ |
| %WIPECOUNT% | 上書きおよび削除された、感染したファイルの数 | スキャナ |
| %MOVEDCOUNT% | 隔離に移動された、感染したファイルの数 | スキャナ |
| %WARNINGCOUNT% | 警告数 | スキャナ |
| %ENDTYPE% | スキャンのステータス: 終了/正常完了 | スキャナ |
| %START_TIME% | スキャンの開始時刻:<br>更新の開始時刻 | スキャナ<br>アップデータ |
| %END_TIME% | スキャンの終了<br>更新の終了 | スキャナ<br>アップデータ |
| %TIME_TAKEN% | スキャンの期間 (分単位)<br>更新の期間 (分単位) | スキャナ<br>アップデータ |
| %LOGFILEPATH% | レポート ファイルのパスおよびファイル名 | スキャナ<br>アップデータ |

AVIRA

live free.™

日本
株式会社アビラ
〒107-0061 ¦ 東京都港区北青山一丁目4番5号ロジェ青山
メール: info@avira.jp
ホームページ : http://www.avira.jp