AVIRA
More Than Security

ユーザー マニュアル

Avira AntiVir Server | Windows

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

Avira GmbH の Avira AntiVir Server 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 Server マニュアルのダウンロード、Avira AntiVir Server 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 Server 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。

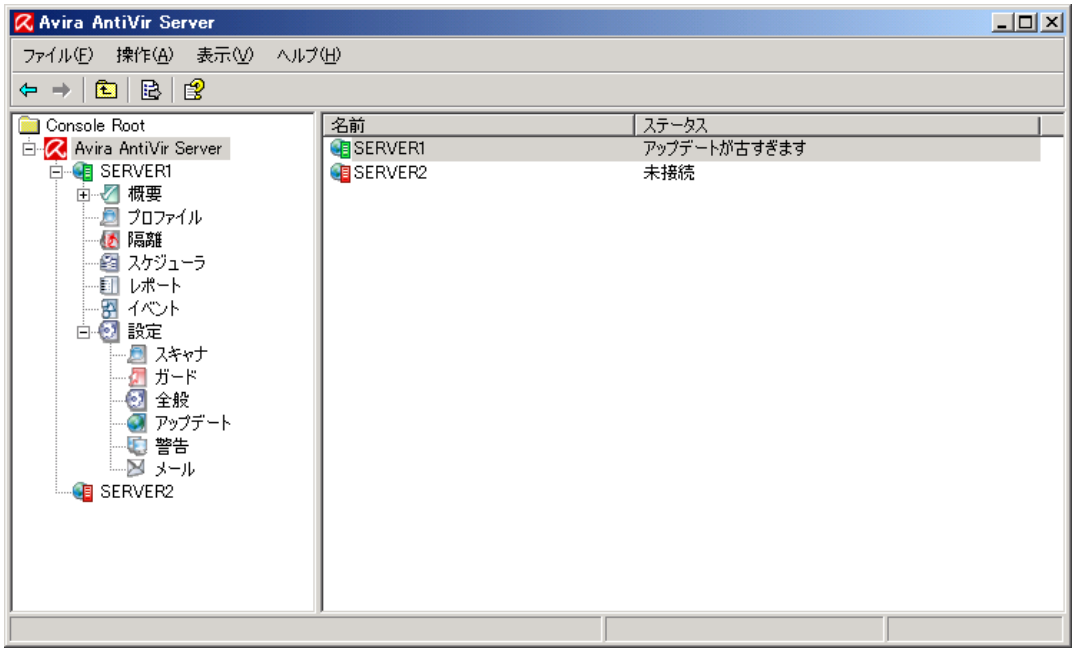
次の強調表示が使用されています。

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

3.1 機能

Avira AntiVir Server 保護パッケージは、Avira AntiVir Server サービスと AntiVir Server Console から構成されます。 Avira AntiVir Server サービスは、Windows サーバーをウイルスおよびマルウェアから保護します。AntiVir Server Console 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 Console 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な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、構成に従って、削除、修復、または Quarantine 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構成できます。
- **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。

- **スケジューラ** 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。
- **AntiVir 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。
- **Quarantine Manager** は、Quarantine に保管されたファイルを管理および監視します。

AntiVir Server Console

AntiVir Server サービスを制御、構成、および監視するためのデスクトップを提供します。 AntiVir Server Console 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 Console 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 Console は、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 AntiVir Server の構成 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 ベースの構成 : 統合アシスタントおよび状況依存型のヘルプによる構成のサポート
- 他のコンピュータからの構成および操作が可能 : AntiVir Server サービスとは別個にデスクトップ (AntiVir Server Console) 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構成可能なスキャンを提供する スキャナ (ダイレクト スキャンまたはオンデマンド 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アタッカまたは短時間に変化するアタッカの検出により実現されるプロアクティブなセキュリティ
- 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
- 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
- 構成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、Quarantine 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

- Quarantine Manager : Quarantine 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
- Microsoft Windows Server 2003 x64 Edition の 32 ビット モードで動作可能 (オンアクセス スキャンおよびオンアクセス スキャンを含む)
- 拡張ターミナル サーバー サポート

3.3 システム要件

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

- 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)
- 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 Server または XP の場合)
- - 512 MB 以上の RAM (Windows Vista、Windows Server 2003、Windows Server 2008 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 Web サイト http://www.avira.jp を参照してください。

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。
- 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 Console を使用して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)
  139 (NetBIOS SSN)
  138 (NetBIOS DGM)

使用タイプ

使用タイプの詳細については、「使用許諾の概念」を参照してください。

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 Server は、Avira AntiVir Server および AntiVir Server Console コンソール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 Console 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。 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

AntiVir Server 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、セットアップを開始します。インストール アシスタントが開きます。
- インストール アシスタントの指示に従います。 次のインストール手順を実行します。
- Microsoft Visual C++ 2008 - Redistributable Kit のインストール (このキットをまだインストールしていない場合)

注
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、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 (完全インストールまたはカスタム インストール)
- 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 日間有効の評価ライセンスの選択
- Avira AntiVir Server サービスおよび AntiVir Server Console 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構成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構成することができます。

- **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。
- **脅威カテゴリの拡張の選択 :** AntiVir Server による検出および報告の対象となる他の拡張脅威カテゴリを選択することで、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 による監視の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の設定を定義できます。AntiVir Server では、電子メールの送信 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
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 Console (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
現在の 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、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 Server 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 (Quarantine 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 Quarantine 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 Avira AntiVir Server のインストールを簡素化するため、Avira AntiVir Server 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 Server 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 Server 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 Server 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 Server 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。

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)

▶ 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 Server 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 Server 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"`

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 Avira AntiVir Server 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 Server の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、[データ] フィールドの次のパラメータを設定して、Avira AntiVir Server 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`>`

AntiVir Server は、ライセンスを使用して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構成を削除します。

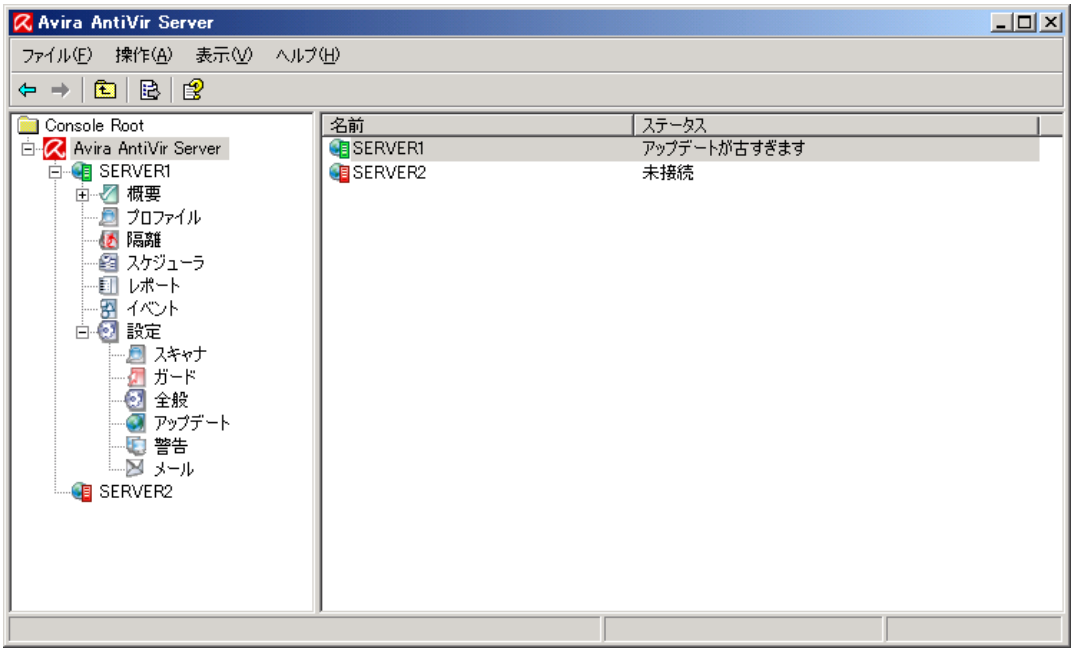
[フィードバック] セクションで、セットアップはエラー コードとセットアップによって報告されたエラー テストを入力します。

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 Console

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 Console** を使用して管理します。 AntiVir Server Console は、Microsoft 管理コンソール (MMC) のスナップインです。 AntiVir Server Console 上で保護対象のサーバーを任意の数だけ作成し、AntiVir Server Console で構成および監視できます。



注
このヘルプでは、AntiVir Server Console 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 Console の開始と終了

Windows の [スタート] メニューまたは **[プログラム]** の **[Avira AntiVir Server Remote Control = Avira AntiVir Server Remote Control]** を使用して、AntiVir Server Console を起動します。 AntiVir Server Console を直接 MMC に読み込むこともできます。 AntiVir Server Console のインストール ディレクトリには、事前に構成された AntiVir Server Console が格納されています。 AntiVir Server Console を終了するには、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。 AntiVir Server の構成 は、**[設定]** ノードの下にあります。 詳細ウィンドウで任意の構成セクションを選択すると、**[設定]** ウィンドウが開き、選択したセクションを構成できます。
- 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 メニューを介して、さまざまなコマンドおよびアクションを実行できます。
- サーバーの構成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 Console 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
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 Console 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、構成のリロード、レポート ファイルの表示、サーバー名の変更、サーバーの接続解除、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 (前回のシステム テスト、前回の更新、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
- AntiVir Server 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

Quarantine

- Quarantine 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、Quarantine へのファイルの追加、Avira マルウェア リサーチ センター へのオブジェクトの送信、オブジェクトの削除

スケジューラ

- 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 サービスの構成
  構成セクション :
- **スキャナ**: オンデマンド スキャンの構成
- **Guard**: オンアクセス スキャンの構成
- **全般** : ダイレクト 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、AntiVir Server Console 上のサーバーのパスワード保護、古い AntiVir Server 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
- **Update** : 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、ダウンロード サーバーへの接続の構成
- **アラート** : Guard および スキャナ のネットワーク アラートの構成
- **電子メール** : Guard、スキャナ、および AntiVir アップデータ の各モジュールの SMTP 経由による電子メール アラートの構成

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 Server 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 が有効です
	AntiVir Guard が無効です

トレイ アイコンのコンテキスト メニューから AntiVir Server の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 アイコンをマウスの右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 Console を開きます。 このオプションは、AntiVir Server Console 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。
- *ヘルプ*: AntiVir Server のオンライン ヘルプを開きます。

– *インターネット上の Avira*: AntiVir Server の Web ポータルを開きます。

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

ウイルスや不要なプログラムから保護するサーバーに 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 Console をインストールします。
「インストール」の章参照。

2. AntiVir Server Console 上での管理

サーバーの追加

AntiVir Server Console で管理するすべてのサーバーを AntiVir Server Console に追加します。
「AntiVir Server Console」の章参照。

追加したサーバーごとに、次の手順を実行します。

構成

保護対象のサーバー上の Avira AntiVir Server サービスを構成します。 AntiVir Server Console 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」の章参照。

更新およびシステム スキャンの実行

最初に、AntiVir Server の更新を 1 回実行します。 そのためには、**スケジューラ** 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、**スケジューラ** 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。
「スケジューラ」の章参照。

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 のスキャンを構成するには、まず必要に応じて **プロファイル** でユーザー定義のプロファイルを作成します。 次に、**スケジューラ** でスキャンおよび更新ジョブを作成します。
「プロファイル」および「スケジューラ」の章参照。

6 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、AntiVir Server の更新をダウンロード 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。 定期的な更新を行うために、AntiVir アップデータ コンポーネントが AntiVir Server に統合されています。 AntiVir アップデータ 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 (製品更新)

AntiVir Server Console の スケジューラ で、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。 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、構成に合わせて製品の更新が実行されます。 AntiVir Server Console では、サーバー ノードのコンテキスト メニューを使用して手動で製品の更新を開始することができます。 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。
- **イントラネット内の 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、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。 マスタ サーバーを設定することで、リソースを節約しながら、保護対象のサーバー上の AntiVir Server が最新状態に保たれます。

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。 更新の構成は AntiVir Server Console で行います。

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、AntiVir 製品 (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 (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、保護対象のサーバー上で AntiVir Server を更新することもできます。

7　ウイルスなど

7.1 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。

7.2 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 Server 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 Server 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 Server 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 Server 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 Server 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 Server 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 Server 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 Server 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 Server 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 Server 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 Server 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 Server 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 Server 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 Server 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 Server 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 Server 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 Server 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 Server 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。

8 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。

8.1 連絡先住所

Avira AntiVir Server 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、AntiVir Server Console の 「ヘルプ :: Avira AntiVir Server バージョン情報」を参照してください。

8.2 テクニカル サポート

Avira AntiVir Server 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 Server AntiVir Server Console のメニュー項目 [ヘルプ] :: [AntiVir Server 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 Server AntiVir Server Console のメニュー項目 [ヘルプ] :: [AntiVir Server 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**。

8.3 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、AntiVir Server Console 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。

8.4 誤検出報告

Avira AntiVir Server 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)。

8.5 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。

9 参照：構成オプション

構成の参考資料には、Avira AntiVir Server 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。

9.1 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、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 Server によって自動的に行われます。これは、Avira AntiVir Server 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が、構成上は常に表示され、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 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。

9.1.1 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。

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。

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。

9.1.2 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。

9.1.3 アーカイブ

9.1.4 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。

9.1.5 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。

9.1.6 ヒューリスティック

この構成セクションには、Avira AntiVir Server 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 Server 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 Server 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 Server 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 Server 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 Server 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。

9.1.7 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。

9.2 Guard

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 Server によって自動的に行われます。これは、Avira AntiVir Server 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

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。このオプションは既定で有効に設定されている推奨設定です。

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)。

9.2.1 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。

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、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。。

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。

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。

9.2.2 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。

9.2.3 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。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、AntiVir Server Console 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
```

9.2.4 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 による監視から除外されます。

9.2.5 ヒューリスティック

この構成セクションには、Avira AntiVir Server 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 Server 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 Server 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 Server 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 Server 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 Server 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。

9.2.6 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。

9.3 全般

9.3.1 脅威カテゴリの拡張

脅威カテゴリの拡張の選択

Avira AntiVir Server 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。

9.3.2 パスワード

パスワードを使用して、AntiVir Server Console 内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 Console を閉じると終了します。

注

SMC を介して AntiVir Server 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 Server 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!

9.3.3 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 Server 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

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。この領域では、AntiVir Server Console 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。

9.3.4 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 AntiVir Server Console では、最大 20,000 エントリが表示されます。

9.3.5 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。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。

9.3.6 ディレクトリ

一時パス

この入力ボックスに、Avira AntiVir Server 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。

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 Server 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 Server 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。

9.4 更新

AntiVir Server の構成 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 Server 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、および必要に応じてプロキシ サーバーを構成できます。

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 サーバー構成セクションで使用しているファイル サーバーを構成できます。

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、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が利用できる場合は、この時間に更新処理が実行されます。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。製品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 Console でアラートが表示されます。

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。AntiVir Server Console の 電子メール通知を設定すると、AntiVir Server Console と電子メールによる通知が行われます。

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)。

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。

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 Server 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。

9.4.1 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 Server 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 Server 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、[更新設定] :: [更新] :: [更新] 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 Server 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。

9.4.2 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

9.5 警告

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
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。

9.5.1 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。

9.5.2 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。

9.5.3 音声のアラート

音声のアラート

Guard のスキャン中、ウイルスが検出されたことを通知する音声のアラートをアクティブ化または非アクティブ化することができます。音声のアラートは、*拡張 ターミナル サーバー サポート*のアクション モードでのみ発せられます。音声のアラートとして、別の Wave ファイルを選択することもできます。

注
Guard のアクション モードは、次の場所で設定します。
[設定]::[Guard]::[懸念のあるファイルに対するアクション]

警告なし

このオプションをアクティブ化すると、Guard によってウイルスが検出されても音声のアラートは再生されません。

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

このオプションをアクティブ化すると、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 (拡張ターミナル サーバー サポート モードのみ)

このオプションをアクティブ化すると、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 WAVE 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 Server 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。

9.6 電子メール

9.6.1 電子メール

特定のイベントについて、Avira AntiVir Server 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 Server 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 Server 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。

9.6.2 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 Server 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。

9.6.3 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、Avira AntiVir Server 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。

9.6.4 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 Server 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。 が構成されました。
AntiVir Server 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。

AVIRA
More Than Security

Avira AntiVir Server | Windows

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

2009 年第二四半期 発行