AVG Email Server Edition

ユーザー マニュアル

ドキュメント改訂 2013.10 (03/12/2013)

目次

1. はじめに

このユーザー マニュアルは、**AVG Email Server Edition** の包括的なマニュアルです。

AVG Email Server Edition をご購入いただき、ありがとうございます。

AVG Email Server Edition は、サーバーの総合的なセキュリティを提供するように設計された、受賞経験のある AVG 製品の 1 つです。すべての AVG 製品と同様に、AVG の信頼性のあるセキュリティ機能をより分かりやすく、効率的な方法で提供するために、**AVG Email Server Edition** は完全に再設計されました。

AVG は、コンピュータとネットワーク アクティビティの保護を目的として設計、開発されています。AVG による完全な保護をぜひ体感してください。

***注意**: このドキュメントでは、Email Server Edition の特定の機能について説明しています。他の AVG 機能に関する情報が必要な場合は、Internet Security Edition のユーザー ガイドを参照してください。すべての必要な詳細について説明しています。このガイドは、http://www.avg.com からダウンロードできます。*

2. AVG インストール要件

2.1. 対応オペレーティング システム

AVG Email Server Edition は、次のオペレーティング システムで稼動するメール サーバーの保護を目的としています。

- Windows 2012 Server R2 Edition
- Windows 2012 Server Edition (x86 および x64)
- Windows 2008 Server R2 Edition
- Windows 2008 Server Edition (x86 および x64)
- Windows 2003 Server (x86, x64) SP1

2.2. サポートされている電子メール サーバー

次のメール サーバーがサポートされています。

- MS Exchange 2003 Server バージョン
- MS Exchange 2007 Server バージョン
- MS Exchange 2010 Server バージョン
- MS Exchange 2013 Server バージョン
- Kerio MailServer – バージョン 6.7.2 以上

2.3. ハードウェア要件

AVG Email Server Edition の最低ハードウェア要件:

- Intel Pentium CPU 1.5 GHz
- ハードディスク空き容量 500 MB以上 (インストールのため)
- 512 MB の RAM メモリ

AVG Email Server Edition の推奨ハードウェア要件:

- Intel Pentium CPU 1.8 GHz
- ハードディスク空き容量 600 MB以上 (インストールのため)
- 512 MB の RAM メモリ

2.4. 古いバージョンのアンインストール

古いバージョンの AVG Email Server をインストールしている場合は、手動でアンインストールしてから、**AVG Email Server Edition** をインストールする必要があります。標準の Windows 機能を使用して、古いバージョンを手動でインストールできます。

- スタートメニューから[***スタート/設定/コントロールパネル/プログラムの追加と削除***] を選択し、インストール済みソフトウェアのリストから該当するプログラムを選択します (または、メニューから[***スタート/すべてのプログラム/AVG/AVG のアンインストール***] を選択する方が簡単かもしれません)。

- 以前に AVG 8.x 以前のバージョンを使用した場合は、必ず個々のサーバープラグインもアンインストールしてください。

  注意: *アンインストール処理中に、ストアサービスを再起動する必要があります。*

  プラグインの交換 - /uninstall パラメータを使用して、プラグインがインストールされたフォルダから setupes.exe を実行します。

  例] C:\AVG4ES2K\setupes.exe /uninstall

  Lotus Domino/Notes プラグイン - /uninstall パラメータを使用して、プラグインがインストールされたフォルダから setupln.exe を実行します。

  例: C:\AVG4LN\setupln.exe /uninstall

2.5. MS Exchange サービス パック

MS Exchange 2003 Server ではサービス パックは必要ありません。ただし、最高レベルのセキュリティを保証するために、最新のサービス パックとホットフィックスをインストールして、システムを最新の状態に保つことをお勧めします。

MS Exchange 2003 Server のサービス パック (任意):

http://www.microsoft.com/en-us/download/details.aspx?id=9664

セットアップを開始すると、すべてのシステム ライブラリのバージョンがチェックされます。最新のライブラリをインストールする必要がある場合は、インストーラは .delete 拡張子を付けて古いライブラリの名前を変更します。このファイルはシステムの再起動時に削除されます。

MS Exchange 2007 Server のサービス パック (任意):

http://www.microsoft.com/downloads/details.aspx?FamilyID=44c66ad6-f185-4a1d-a9ab-473c1188954c&displaylang=en

MS Exchange 2010 Server のサービス パック (任意):

http://www.microsoft.com/en-us/download/details.aspx?id=28190

3. AVG インストール処理

AVG をコンピュータにインストールするには、最新のインストール ファイルを入手する必要があります。パッケージ版の CD にあるインストール ファイルも使用できますが、このファイルは古い可能性があります。したがって、最新のインストール ファイルをオンラインで入手することをお勧めします。AVG ウェブサイト (http://www.avg.com/download?prd=msw) からファイルをダウンロードできます。

各製品には 32 ビット オペレーティング システム (x86) 用と64 ビット オペレーティング システム (x64) 用の 2 種類のパッケージがあります。必ず使用しているオペレーティング システムに合った正しいインストール パッケージを使用してください。

インストール処理中にはライセンス番号を入力する必要があります。インストールを開始する前にライセンス番号を準備してください。番号は CD のパッケージに記載されています。AVG 製品をオンラインで購入した場合、ライセンス番号は電子メールで送信されます。

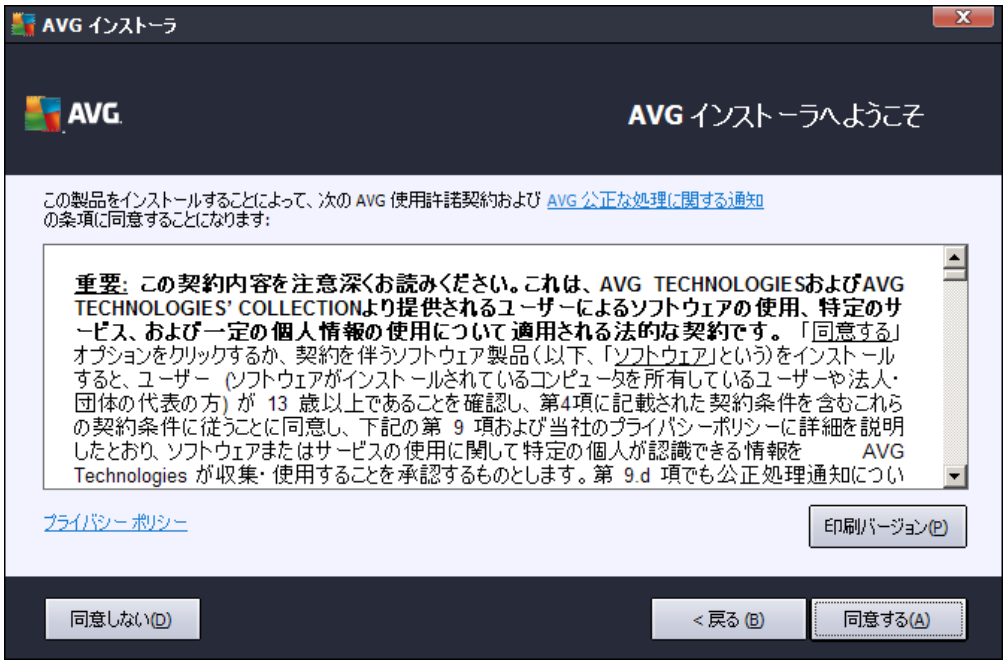
インストールファイルをハードディスクにダウンロードし保存した後、インストールプロセスを実行することができます。インストールは各ステップの操作の概要を案内する一連のダイアログで構成されています。次に、各ダイアログの説明を示します。

3.1. インストールの実行

インストール処理は [**ようこそ**] ウィンドウから始まります。このウィンドウではインストール処理で使用する言語を選択し、[**次へ**] ボタンを押します。

インストール処理の後半で、アプリケーション インターフェースの言語を追加することもできます。

3.2. ライセンス契約



このダイアログでは、ライセンス条件を読むことができます。[***印刷バージョン***] ボタンをクリックすると、新しいウィンドウでライセンス契約が表示されます。[***同意する***] ボタンをクリックして確認し、次のダイアログへ進みます。

3.3. ライセンスのアクティベート

[***ライセンスのアクティベート***] ダイアログではライセンス番号を入力する必要があります。

ライセンス番号を [***ライセンス番号***] テキスト フィールドに入力します。ライセンス番号は、オンラインでの AVG 製品ご購入後に送信された確認メールに記載されています。この番号を記載通り正確に入力する必要があります。デジタル形式のライセンス番号が利用できる場合 (電子メール) は、コピーと貼り付けを使用して入力することをお勧めします。

[***次へ***] ボタンをクリックして、インストール処理を続行します。

3.4. インストール タイプの選択

[***インストール タイプの選択***] ダイアログでは、[***高速インストール***] と[***カスタム インストール***] の 2 つのインストール オプションから選択できます。

ほとんどのユーザーには、[***高速インストール***] を選択し、プログラム ベンダーが事前定義した設定を使用して AVG を自動モードでインストールすることを強くお勧めします。この設定は、最適なリソース消費で最大のセキュリティを実現します。将来的に設定の変更の必要が生じた場合は、いつでも AVG アプリケーションで直接変更できます。

カスタム インストールは、AVG を標準設定でインストールしない合理的な理由がある場合、経験のあるユーザーのみが行ってください (特定のシステム要件への適合など)。

カスタム インストールを選択すると、ダイアログの下部に [***インストール先 フォルダ***] セクションが表示されます。このセクションで、AVG をインストールする場所を指定できます。既定では AVGは C ドライブの program files フォルダにインストールされます。この場所を変更する場合は、[***参照***] ボタンをクリックしてドライブ構成を表示し、対象フォルダを選択します。

3.5. カスタム インストール - カスタム オプション

[***コンポーネント選択***] セクションには、インストール可能なすべての AVG コンポーネントの概要が表示されます。デフォルトの設定が適当でない場合は、個別のコンポーネントを追加または削除できます。

ただし、選択できるコンポーネントは購入した AVG 製品に含まれているコンポーネントのみです。[コンポーネント選択] ダイアログでは、これらのコンポーネントのみをインストール可能です。

- ***遠隔管理*** - AVG を AVG DataCenter (AVG Network Edition) に接続する場合は、このオプションを選択する必要があります。
- ***追加でインストールする言語*** - インストールされる言語を選択できます。[***追加でインストールする言語***] 項目にチェックを付け、該当するメニューから任意の言語を選択します。

個別のサーバー コンポーネントの基本的な概要 ([***サーバー***] の部分)

- ***Anti-Spam Server for MS Exchange***

  すべての受信メールをチェックし、望ましくないメールをスパムとしてマークします。複数の分析手法を使用して各メールを処理し、望ましくない電子メールからの最大限の保護を提供します。

- ***MS Exchange 向けメール スキャナ (転送エージェントのルーティング)***

  MS Exchange HUB ロールを経由するすべての着信、送信、および内部電子メールをチェックします。

- ***MS Exchange 向けメール スキャナ (SMTP 転送エージェント)***

  MS Exchange SMTP インターフェースを経由して着信したすべての電子メールをチェックします (EDGE ロールおよび HUB ロールの両方にインストールできます)。

- ***MS Exchange 向けメール スキャナ (VSAPI)***

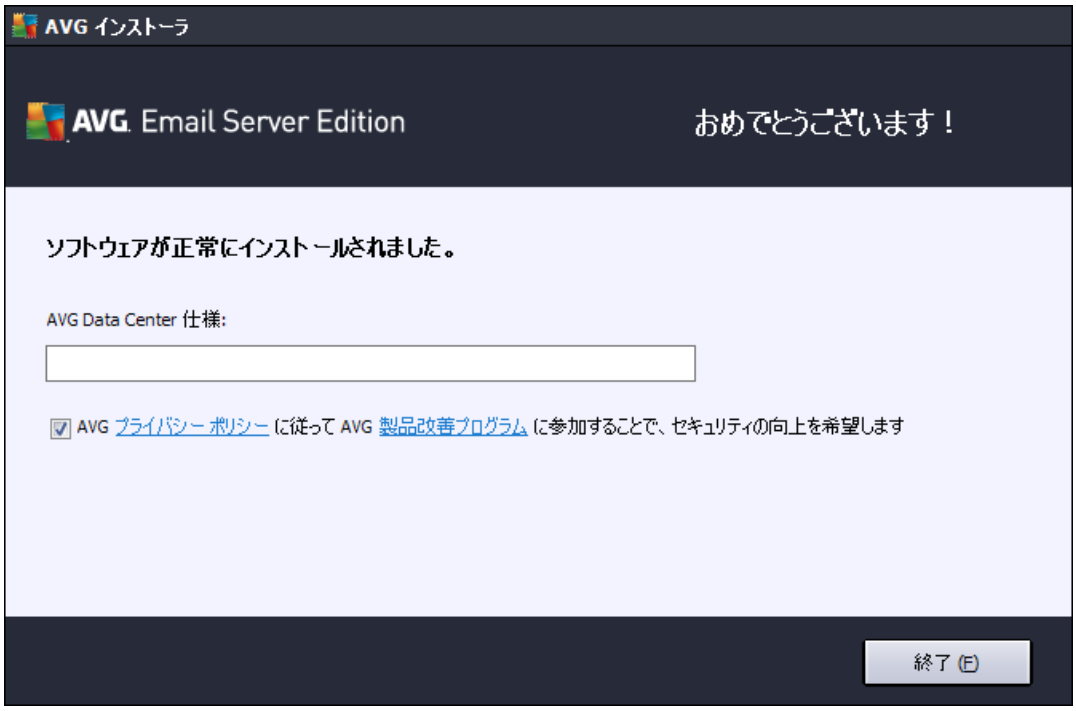
  ユーザーのメールボックスに保存されているすべての電子メールをチェックします。ウイルスを検出すると、ウイルス隔離室に移動するか、完全に削除します。

スパム対策およびメール スキャナ (VSAPI) コンポーネントは、Exchange 2003 のユーザーのみが利用可能です。

[***次へ***] ボタンをクリックして続行します。

3.6. インストール完了

モジュール選択で***遠隔管理*** モジュールを選択した場合は、この最後の画面で AVG DataCenter への接続時に使用する接続文字列を定義できます。



また、このダイアログでは、全体的なインターネット セキュリティレベルを高める目的で、検出された脅威に関する匿名の情報を収集する製品改善プログラムに参加するかどうかも選択できます。この内容に同意する場合は、[***AVG プライバシー ポリシーに準拠した AVG 製品改善プログラムに参加してセキュリティを向上させる***] オプションを選択したままの状態にしてください *(このオプションはデフォルトにより選択されています)*。

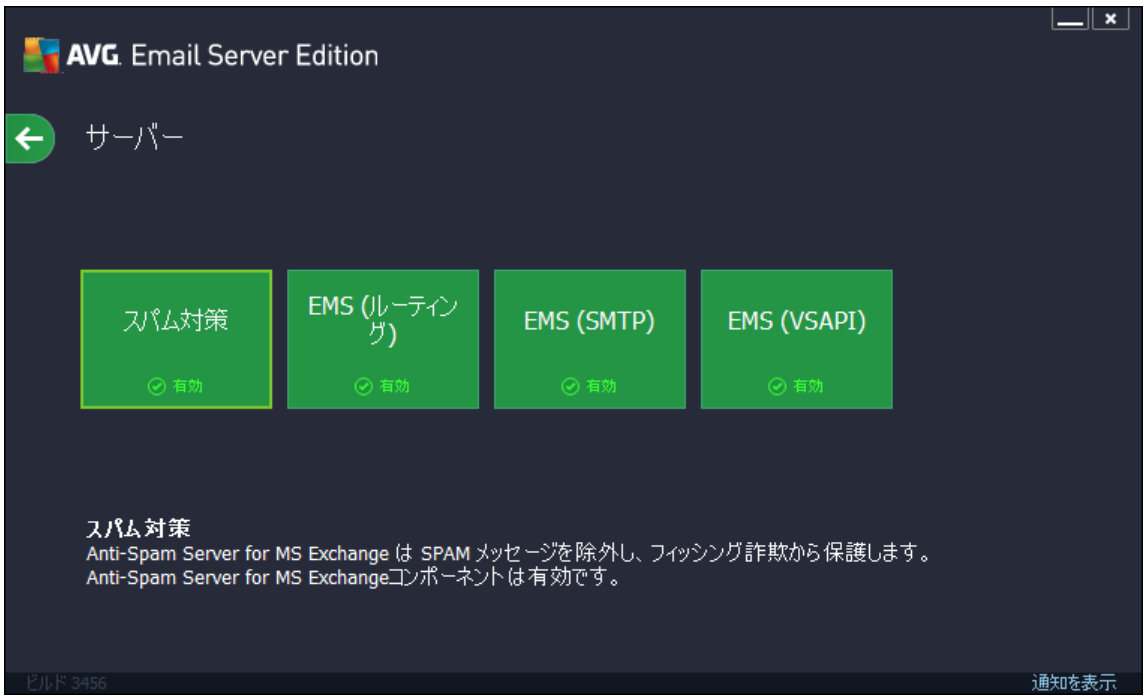
[**完了**] ボタンをクリックして、選択内容を確定します。

AVG はコンピュータにインストールされ、完全に機能しています。プログラムは完全自動モードでバックグラウンドで実行中です。

4. インストール後

インストールが完了するとすぐに、***AVG Email Server Edition*** のメイン画面が表示されます。

このマニュアルでは、***AVG Email Server Edition*** 固有の機能のみについて説明します。他のすべてのコンポーネントや設定については、AVG Desktop マニュアルで説明されています。メイン サーバー コンポーネント ダイアログを開くには、[***サーバー***] ボタンをクリックします。すると、次の画面が開きます。



MS Exchange 2007 以降を使用している場合に限り、すべてのサーバー コンポーネントが利用可能であることにご注意ください (インストールのプロセスで一部のコンポーネントをインストールしない選択を行った場合は当然該当しません)。MS Exchange 2003 は、スパム対策およびメール スキャナ (VSAPI) のコンポーネントのみをサポートしています。

メール サーバーの保護を個別に設定するには、該当する章の説明に従ってください。

- ***MS Exchange 向けメール スキャナ***
- ***Anti-Spam Server for MS Exchange***
- ***AVG for Kerio MailServer***

5. MS Exchange 向けメール スキャナ

5.1. 概要

個別のメール スキャナ サーバー コンポーネントの基本的な概要

- ***EMS (ルーティング) - MS Exchange 向けメール スキャナ (転送エージェントのルーティング)***

  MS Exchange HUB ロールを通過するすべての着信、送信、および内部電子メールをチェックします。

  MS Exchange 2007/2010/2013 で使用でき、HUB ロールのみにインストールできます。

- ***EMS (SMTP) - MS Exchange 向けメール スキャナ (SMTP 転送エージェント)***

  MS Exchange SMTP インターフェース経由で着信したすべての電子メールをチェックします。

  MS Exchange 2007/2010/2013 でのみ使用でき、EDGE ロールおよび HUB ロールの両方にインストールできます。

- ***EMS (VSAPI) - MS Exchange 向けメール スキャナ (VSAPI)***

  ユーザーのメールボックスに保存されているすべての電子メールをチェックします。ウイルスを検出すると、ウイルス隔離室に移動するか、完全に削除します。

必要なコンポーネント アイコンをクリックすると、インターフェースが開きます。すべてのコンポーネントで、以下の操作ボタンとリンクが共通して使用されています。

- ***有効/無効*** - このボタンをクリックすると、選択したコンポーネントのオン/オフが切り替えられます (コンポーネントがオンの場合、ボタンとテキストは緑で表示され、オフの場合は赤で表示されます)。

- ***スキャン結果***

  スキャン結果を確認するための新しいダイアログが開きます。

  このダイアログでは、メッセージが重要度に応じて複数のタブに分かれて表示されます。重要度の変更方法とレポート方法については、各コンポーネントの設定を参照してください。

  デフォルトでは過去 2 日間の結果のみが表示されます。次のオプションを変更することで、表示期間を変更できます。

  - ***次の過去の期間内の結果を表示*** - 任意の日数と時間数を入力します。
  - ***選択した期間の結果を表示*** - カスタム日時間隔を選択します。
  - ***すべて表示*** - 期間全体の結果を表示します。

  [***更新***] ボタンをクリックすると、結果がロードされます。

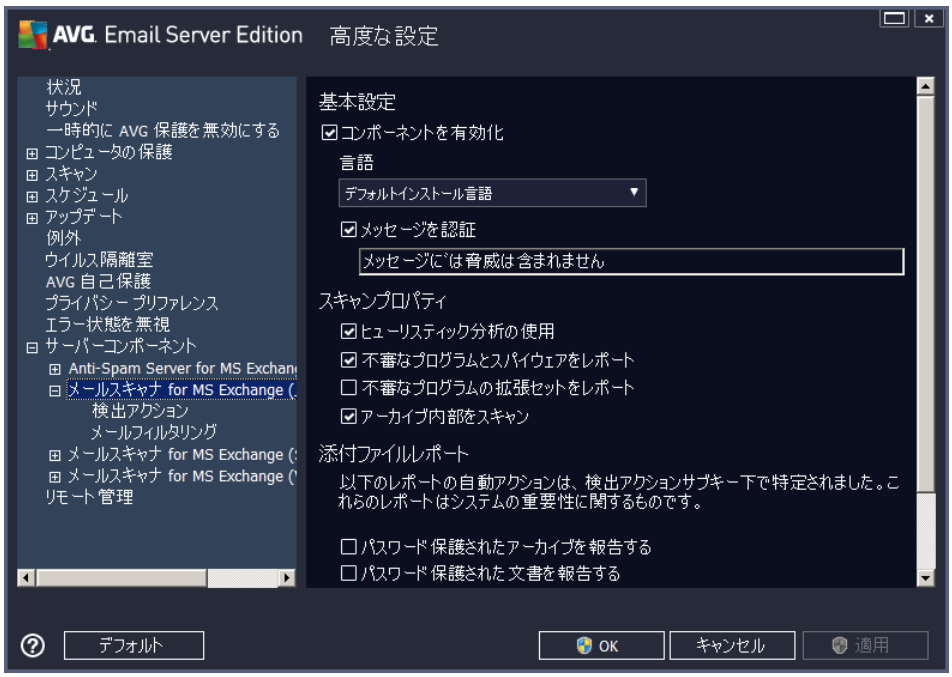
- ***統計値の更新*** - 上記で表示される統計値が更新されます。

[***設定***] 作業ボタンをクリックすると、選択したコンポーネントの高度な設定が開きます (すべてのコンポーネントの個々の設定についての詳細情報は下記の章に記載されています)。

5.2. MS Exchange 向けメール スキャナ (ルーティング TA)

MS Exchange 向けメール スキャナ (ルーティングトランスポートエージェント) の設定を開くには、コンポーネントのインターフェースから [***設定***] ボタンを選択します。

[***サーバー コンポーネント***] リストから、[***MS Exchange 向けメール スキャナ (ルーティング TA)***] を選択します。



[***基本設定***] セクションには次のオプションがあります。

- ***コンポーネントを有効にする*** - チェックを外すと、コンポーネント全体を無効にします。
- ***言語*** - 任意のコンポーネント言語を選択します。
- ***メッセージを認証する*** - すべてのスキャン済みメッセージに認証を追加する場合はこのオプションにチェックを付けます。次のフィールドでメッセージをカスタマイズできます。

[***スキャン プロパティ***] セクション:

- ***ヒューリスティックを使用する*** - スキャン時にヒューリスティック分析方式を有効にするにはこのオプションにチェックを付けます。
- ***不審なプログラムとスパイウェア脅威を報告する*** - このオプションにチェックを付けると、不審なプログラムとスパイウェアの存在を報告します。
- ***不審なプログラムの拡張設定を報告する*** - チェックを付けると、スパイウェアの拡張パッケージを検出します。スパイウェアは、製造元から直接取得する場合には完全に問題がなく無害なプログラムですが、後から悪意のある目的で悪用されるおそれのあるプログラムです。また、常に無害ですが、望ましくないプログラムもあります (各種ツールバーなど)。この機能はコンピュータセキュリティと快適性をさらに高めるための追加的な手段ですが、合法的なプログラムもブロックする可能性があるため、デフォルトではオフになっています。メモ: この検出機能は前のオプションの追加機能です。したがって、基本タイプのスパイウェアに対する保護を適用する場合には、必ず前のボックスにもチェックを付けた状態にしてください。
- ***アーカイブ内部をスキャンする*** - アーカイブファイル内 (zip、rar など) もスキャンする場合は、このオプションにチェックを付けます。

[***電子メール添付ファイルの報告***] セクションでは、スキャン中に報告する項目を選択できます。チェックを付けると、このような項目を含むメールの件名に [INFORMATION] タグが追加されます。これはデフォルトの設定で、[***検出アクション***] セクションの [***情報***] の部分で簡単に修正できます (次を参照)。

次のオプションが利用可能です。

- ***パスワード保護されたアーカイブを報告する***
- ***パスワード保護されたドキュメントを報告する***
- ***マクロを含むファイルを報告する***
- ***非表示の拡張子を報告する***

またツリー構造では次の下位項目も利用できます。

- ***検出アクション***
- ***メールフィルタリング***

5.3. MS Exchange 向けメールスキャナ (SMTP TA)

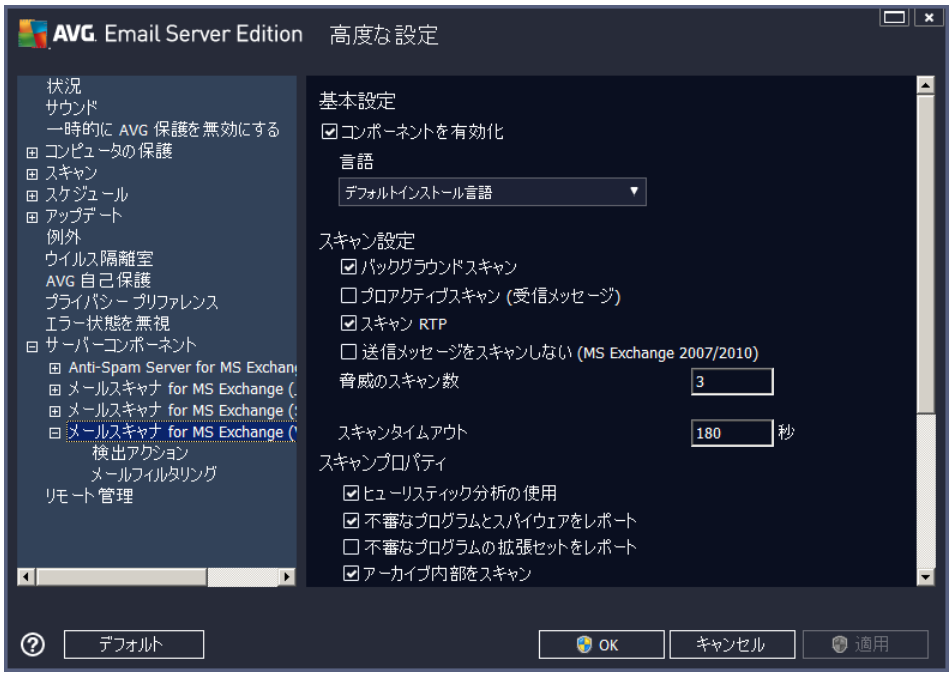
[***MS Exchange (SMTP TA) 向けメールスキャナ***] の設定はトランスポートエージェントのルーティングと全く同じです。詳細については、前述の「***MS Exchange (ルーティング TA) 向けメールスキャナ***」の章をご覧ください。

またツリー構造では次の下位項目も利用できます。

- ***検出アクション***
- ***メールフィルタリング***

5.4. MS Exchange 向けメールスキャナ (VSAPI)

この項目には ***MS Exchange (VSAPI) 向けメールスキャナ***の設定が含まれます。



[***基本設定***] セクションには次のオプションがあります。

- ***コンポーネントを有効にする*** - チェックを外すと、コンポーネント全体が無効になります。
- ***言語*** - 任意のコンポーネント言語を選択します。

[***スキャン設定***] セクション:

- ***バックグラウンド スキャン*** - ここでバックグラウンド スキャン処理を有効/無効にできます。バックグラウンド スキャンは VSAPI 2.0/2.5 アプリケーション インターフェース機能の 1 つです。Exchange Messaging Database のスレッド化されたスキャンを提供します。最新の AVG ウイルス ベース更新でスキャンされなかったアイテムがユーザーのメールボックス フォルダに入った場合は、AVG for Exchange Server に送信されてスキャンされます。検査されていないオブジェクトのスキャンと検索は並行して実行されます。

  特定の低優先度スレッドは各データベースで使用されます。これにより、他のタスク (Microsoft Exchange データベースの電子メール メッセージ ストレージなど) が常に優先的に実行されることが保証されます。

- ***プロアクティブ スキャン (受信メッセージ)***

  ここで VSAPI 2.0/2.5 のプロアクティブ スキャン機能を有効/無効にできます。アイテムがフォルダに配信された後、クライアントによる要求がない場合に、このスキャンが実行されます。

  メッセージが Exchage 保管庫に送信されるとすぐに、低優先度 (最大 30 アイテム) でグローバル スキャンの待ち行列に入ります。先入れ先出し (FIFO) ベースでスキャンされます。待ち行列にあるアイテムがアクセスされると、高優先度に変更されます。

オーバーフローしたメッセージはスキャンされない状態で保存されます。

[バックグラウンド スキャン] と ***[プロアクティブ スキャン]*** オプションの両方を無効にしても、MS Outlook クライアントでメッセージをダウンロードする場合は、オン アクセス スキャナが有効になります。

- ***RTF のスキャン*** - ここで RTF ファイル タイプをスキャンするかどうかを指定できます。
- ***送信メッセージをスキャンしない (MS Exchange 2007/2010/2013)*** - VSAPI とルーティング転送エージェント (ルーティング TA) サーバー コンポーネントの両方がインストールされていると (1 台のサーバーを使用しているか、2 台のサーバーを別々に使用しているかにかかわらず)、送信メールが 2 回スキャンされる場合があります。最初のスキャンは VSAPI オンアクセス スキャナによって実行され、次のスキャンはルーティング転送エージェントによって実行されます。これにより、特定のサーバーの速度が低下し、電子メール送信で多少の遅延が発生する場合があります。両方のサーバー コンポーネントが確実にインストールされ、アクティブになっている場合は、このボックスにチェックを付け、VSAPI オンアクセス スキャナを無効にすることで、この送信メール スキャンを回避できます。
- ***スキャン スレッド数*** - *デフォルトではスキャン処理はスレッド化され、一定レベルの並列性によりスキャン パフォーマンス全体が向上します。*ここでスレッド数を変更できます。

  デフォルトのスレッド数は「プロセッサ数」の 2倍 + 1 です。

  スレッドの最小数は「プロセッサ数」+1 を 2 で割った数です。

  スレッドの最大数は「プロセッサ数」の 5 倍 +1 です。

値が最小値以下の場合または最大値以上の場合は、デフォルト値が使用されます。

- ***スキャン タイムアウト*** - 1 つのスレッドがスキャン中のメッセージにアクセスする最大継続間隔 (秒数) です (デフォルト値は 180 秒)。

[***スキャン プロパティ***] セクション:

- ***ヒューリスティックを使用する*** - スキャン時にヒューリスティック分析方式を有効にするには、このボックスにチェックを付けます。
- ***不審なプログラムとスパイウェア脅威を報告する*** - このオプションにチェックを付けると、不審なプログラムとスパイウェアの存在を報告します。
- ***不審なプログラムの拡張設定を報告する*** - チェックを付けると、スパイウェアの拡張パッケージを検出します。スパイウェアは、製造元から直接取得する場合には完全に問題がなく無害なプログラムですが、後から悪意のある目的で悪用されるおそれのあるプログラムです。また、常に無害ですが、望ましくないプログラムもあります (各種ツールバーなど)。この機能はコンピュータセキュリティと快適性をさらに高めるための追加的な手段ですが、合法的なプログラムもブロックする可能性があるため、デフォルトではオフになっています。メモ: この検出機能は前のオプションの追加機能です。したがって、基本タイプのスパイウェアに対する保護を適用する場合には、必ず前のボックスにもチェックを付けた状態にしてください。
- ***アーカイブ内部をスキャンする*** - アーカイブ ファイル内 (zip、rar など) もスキャンする場合は、このオプションにチェックを付けます。

[***電子メール添付ファイルの報告***] セクションでは、スキャン中に報告する項目を選択できます。デフォルトの設定は [***検出アクション***] セクションの [***情報***] の部分で簡単に修正できます (下記を参照)。

次のオプションが利用可能です。

- ***パスワード保護されたアーカイブを報告する***
- ***パスワード保護されたドキュメントを報告する***
- ***マクロを含むファイルを報告する***
- ***非表示の拡張子を報告する***

一般的に、これらの機能の一部は Microsoft VSAPI 2.0/2.5 アプリケーション インターフェース サービスのユーザー拡張です。VSAPI 2.0/2.5 の詳細については、次のリンクと参照リンクからアクセスできるリンクを確認してください。

- http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k - Exchange とウイルス対策ソフトウェア連携に関する情報
- http://support.microsoft.com/default.aspx?scid=kb;en-us;823166 Exchange 2003 Server アプリケーションでの追加 VSAPI 2.5 機能に関する情報

またツリー構造では次の下位項目も利用できます。

- ***検出アクション***
- ***メール フィルタリング***

5.5. 検出アクション

[***検出アクション***] サブアイテムでは、スキャン処理中の自動アクションを選択できます。

このアクションは以下のアイテムで利用可能です。

- ***高い重要度の検出*** – 自分自身をコピーして拡大させる悪意のあるコード。多くの場合、被害が発生するまで気付きません。
- ***中程度の重要度の検出*** - 一般的にこの種のプログラムには、明らかに深刻なものからプライバシーに潜在的な脅威を与えるものまであります。
- ***重要度の検出情報*** - 検出されたすべての潜在的な脅威のうち、上記のいずれのカテゴリにも分類できない項目が表示されます。

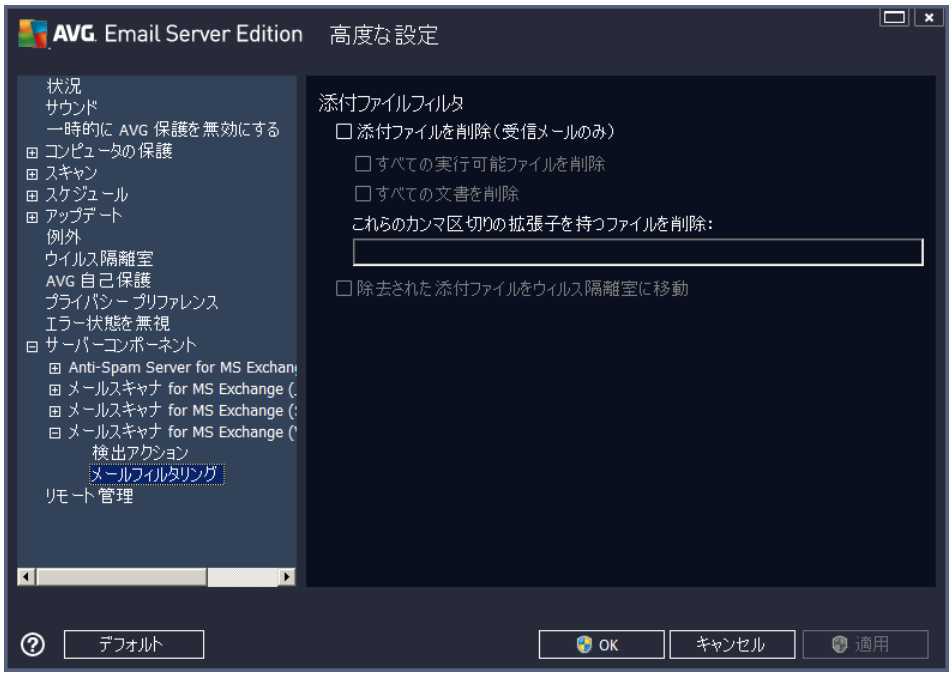
ロールダウンメニューを使い、各アイテムのアクションを選択します。

- ***なし*** - アクションは行われません。
- ***ウイルス隔離室に移動*** - 既知の脅威はウイルス隔離室に移動します。
- ***削除*** - 既知の脅威は削除されます。

既知のアイテムや脅威を含むメッセージの件名文を選択する場合は、[***...を含む件名をマークする***] ボックスのチェックをオンにし、希望の値を入力します。

MS Exchange VSAPI 向け電子メールスキャナでは、上記の機能のうち、最後の機能は利用できません。

5.6. メール フィルタリング



[***メール フィルタリング***] サブアイテムでは、自動的に削除する添付ファイル（ある場合）を選択できます。次のオプションが利用可能です。

- ***添付ファイルを削除*** - このボックスをオンにして、機能を有効にします。
- ***すべての実行可能ファイルを削除*** - すべての実行可能ファイルが削除されます。
- ***すべてのドキュメントを削除*** - すべてのドキュメントファイルが削除されます。
- ***コンマで区切られた拡張子でファイルを削除*** - 自動的に削除するボックスをファイル拡張子で埋めます。拡張子をコンマで区切ります。
- ***除外された添付ファイルをウイルス隔離室に移動する*** - 除外された添付ファイルを完全に削除しない場合にはチェックを付けます。このボックスを選択すると、ダイアログで選択されたすべての添付ファイルが自動的にウイルス隔離室環境に移動されます。ウイルス隔離室は潜在的に悪意のあるファイルを保存するための安全な場所です。システムに危害を及ぼさずにファイルの確認と調査ができます。ウイルス隔離室は **AVG Email Server Edition** メインインターフェースの上部のメニューからアクセスできます。***オプション***の項目をクリックし、ドロップダウンメニューから***ウイルス隔離室***を選択します。

6. MS Exchange 向けスパム対策サーバー

6.1. スパム対策基本

スパムとは未承諾電子メールのことです。ほとんどが製品やサービスの広告メールで、大量のメールアドレスに一度に送信され、受信者のメールボックスを満杯にします。消費者が受信に同意した合法的な商業上のメールは、スパムではありません。スパムは単に迷惑なだけではなく、しばしば詐欺、ウイルス、不快な内容を含んでいます。

スパム対策は、すべての受信メールをチェックし、望ましくないメールをスパムとしてマークします。複数の分析手法を使用して各メールを処理し、望ましくない電子メールからの最大限の保護を提供します。

6.2. スパム対策インターフェース

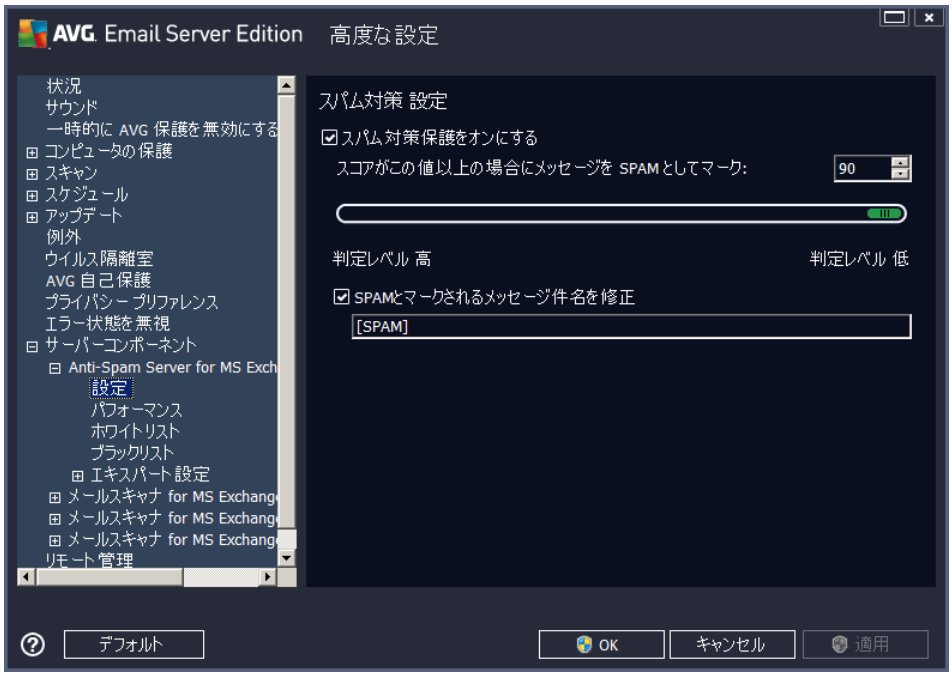
このダイアログには、サーバーコンポーネントの機能に関する概要情報、その現在のステータス (*有効/無効*)、およびいくつかの統計値が表示されます。

利用可能なボタンとリンク

- ***有効/無効*** - このボタンをクリックすると、選択したコンポーネントのオン/オフが切り替えられます (コンポーネントがオンの場合、ボタンとテキストは緑で表示され、オフの場合は赤で表示されます)。
- ***統計値の更新*** - 上記で表示される統計値が更新されます。
- ***設定*** – [スパム対策設定] を開くには、このボタンを使用します。

6.3. スパム対策設定

6.3.1. 設定



このダイアログでは [***スパム対策保護をオンにする***] チェックボックスを使用して、電子メール通信のスパム対策スキャンを許可/禁止できます。

このダイアログでは、スコアの判定レベルを選択することもできます。[***スパム対策***] フィルタは、複数の動的スキャン技術に基づいて、各メッセージにスコアを割り当てます (*メッセージの内容とSPAM メッセージとの類似性など*)。値 (*50 ～ 90*) を入力するか、スライダを左右に動かして、[***スコアが次の値以上の場合はメッセージをスパムと見なす***] 設定を調整できます。

次に、スコアのしきい値の概要を示します。

- ***値 90*** - 大部分の受信電子メールは通常通りに (スパムとしてマークされずに) 配信されます。最も容易に特定できるスパムは除外されますが、かなりの数のスパムが配信される可能性があります。
- ***値 80 ～ 89*** - スパムの可能性が高い電子メールは除外されます。一部の非スパムメッセージも誤って除外される可能性があります。
- ***値 60 ～ 79*** - かなり積極的な設定です。スパムの可能性のある電子メールは除外されます。スパムではないメールも同様に除外される場合があります。
- ***値 50 ～ 59*** - 非常に積極的な設定です。スパムではないメールが、本物のスパムメールと同様に除去される可能性が高くなります。通常、この値は推奨されません。

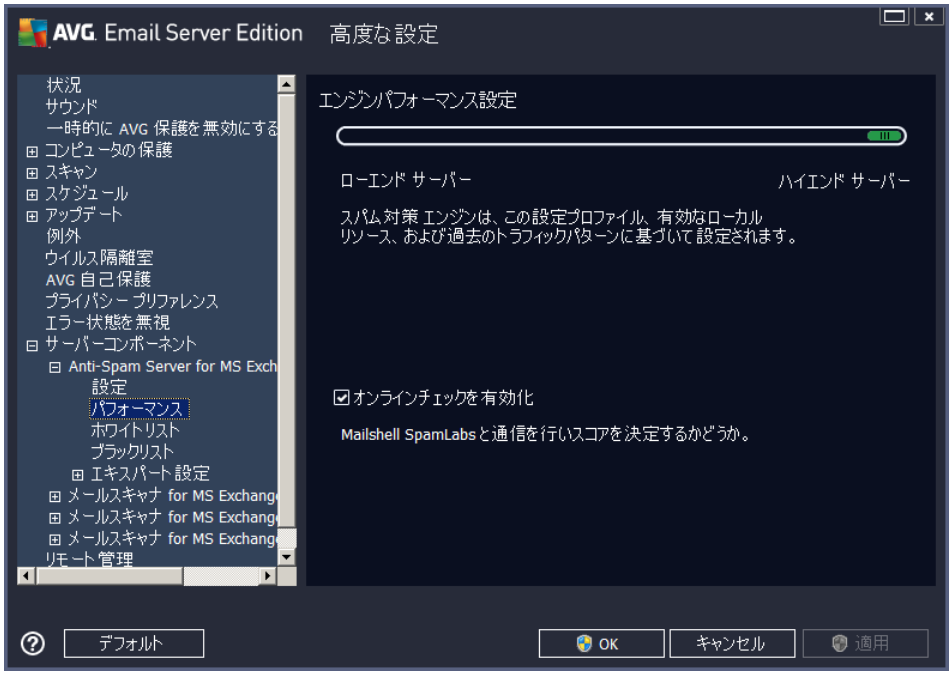
さらに、検出したスパムメールを処理する方法を定義できます。

- ***スパムとしてマークされたメッセージの件名を修正*** - スパムとして検出されたすべてのメールの件名フィー

ルドに特定の単語や文字を追加してマークする場合は、このチェックボックスにチェックを付けます。希望するテキストは、有効化されたテキスト フィールドに入力できます。

- ***誤検出を報告する前に確認する*** - インストール処理中に製品改善プログラムへの参加に同意し、検出された脅威の AVG への報告を許可した場合に指定できます。この製品改善プログラムは、最新の脅威に関する情報を全世界の参加者から収集することで、全ユーザーのために製品の保護機能を改善します。報告は自動的に実行されます。ただし、このチェックボックスにチェックを付けると、検出されたスパムを AVG に送信する前にダイアログ ボックスを表示し、そのメッセージをスパムとして分類する必要があるかどうか確認できます。

6.3.2. パフォーマンス



[***エンジン パフォーマンス設定***] ダイアログ (*左側のナビゲーションの [**パフォーマンス**] からリンク*) では、***スパム対策*** コンポーネントのパフォーマンスを設定できます。スライダを左右に動かして、***低メモリ消費*** モードと***高パフォーマンス*** モードの間でスキャン パフォーマンス レベルを変更します。

- ***低メモリ消費*** - スキャン処理でスパムを判定するときに、ルールは使用されません。学習データのみが判定に使用されます。コンピュータ ハードウェア性能が著しく低い場合などをのぞき、このモードは一般の利用には推奨されません。

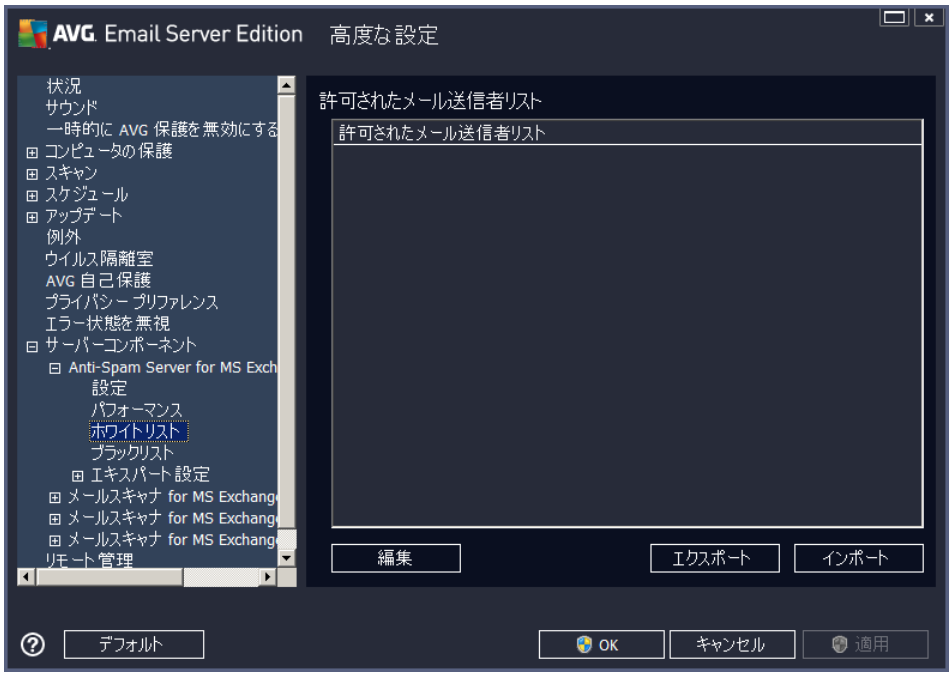
- ***高パフォーマンス*** - このモードでは大量のメモリを消費します。スパム スキャン中には、ルールとスパム データベース キャッシュ、基本ルール、高度なルール、スパム送信者 IP アドレス、スパム送信者データベース機能が使用されます。

[***オンライン チェックを有効にする***] は既定でオンとなっています。これにより、Mailshell サーバーとの通信によってスキャン データが Mailshell データベースとオンラインで比較されるため、より正確なスパム検出が実行されます。

通常、やむを得ない理由がある場合を除き、既定の設定を保持することをお勧めします。この設定の変更は上級者ユーザーのみが行ってください。

6.3.3. ホワイトリスト

[***ホワイトリスト***] をクリックすると、スパム送信者として判定されない承認済みの送信者メールアドレスとドメイン名のグローバルリストが表示されるダイアログが開きます。



編集インターフェースでは、望ましくないメッセージ (スパム) を送信しない送信者のリストを編集できます。また、スパムメッセージが生成されないことがわかっているドメイン名 (*avg.com など*) のリストを編集できます。

スパム送信者やドメイン名のリストがすでにある場合は、各メールアドレスを直接入力するか、一度にアドレスのリスト全体をインポートすることでリストを入力できます。次のコントロールボタンを利用できます。

- ***編集*** - このボタンをクリックするとダイアログが開きます。このダイアログでは、手動でアドレスのリストを入力できます (*コピーと貼り付け*も使用できます)。各行に 1 項目 (送信者、ドメイン名) を入力します。
- ***インポート*** - このボタンをクリックすると、既存の電子メールアドレスをインポートできます。テキストファイル (各行にアドレスまたはドメイン名の 1 項目のみを記載したプレーンテキスト形式) または WAB ファイルを入力できます。あるいは、Windows アドレス帳または Microsoft Office Outlook からインポートできます。
- ***エクスポート*** - 何らかの目的でレコードをエクスポートする場合は、このボタンをクリックします。すべてのレコードがプレーンテキスト形式で保存されます。

6.3.4. ブラックリスト

[***ブラックリスト***] 項目は、常にスパム送信者としてブロックするメール アドレスとドメイン名のグローバル リストが表示されるダイアログを開きます。

編集インターフェースでは、望ましくないメッセージ (スパム) を送信すると思われる送信者のリストを編集できます。また、スパム メッセージを送信するドメイン名リスト (*spammingcompany.com* など) も編集できます。リスト中のアドレスとドメインからのメールは、すべてスパムとして判定されます。

スパム送信者やドメイン名のリストがすでにある場合は、各メールアドレスを直接入力するか、一度にアドレスのリスト全体をインポートすることでリストを入力できます。次のコントロール ボタンを利用できます。

- ***編集*** - *このボタンをクリックするとダイアログが開きます。このダイアログでは、手動でアドレスのリストを入力できます (コピーと貼り付けも使用できます)*。各行に 1 項目 (送信者、ドメイン名) を入力します。
- ***インポート*** - このボタンをクリックすると、既存の電子メール アドレスをインポートできます。テキスト ファイル (各行にアドレスまたはドメイン名の 1 項目のみを記載したプレーン テキスト形式) または WAB ファイルを入力できます。あるいは、Windows アドレス帳または Microsoft Office Outlook からインポートできます。
- ***エクスポート*** - 何らかの目的でレコードをエクスポートする場合は、このボタンをクリックします。すべてのレコードがプレーン テキスト形式で保存されます。

6.3.5. エキスパート設定

この部分には、スパム対策コンポーネントに関するさまざまな設定オプションが表示されます。これらの設定は、メール サーバーを最大限に保護するために詳細なスパム対策設定を行う必要があるネットワーク管理者などの、経験あるユーザー専用です。このため、個々のダイアログに関する詳細なヘルプは提供されていません。各オプションの簡単な説明については、ユーザー インターフェース上に直接表示されます。

Spamcatcher (MailShell Inc.) の高度な設定に精通している場合を除いて、設定変更を行わないことを強くお勧めします。ファイルが不適切に変更された場合は、パフォーマンスの悪化やコンポーネント機能の不正動作につながるおそれがあります。

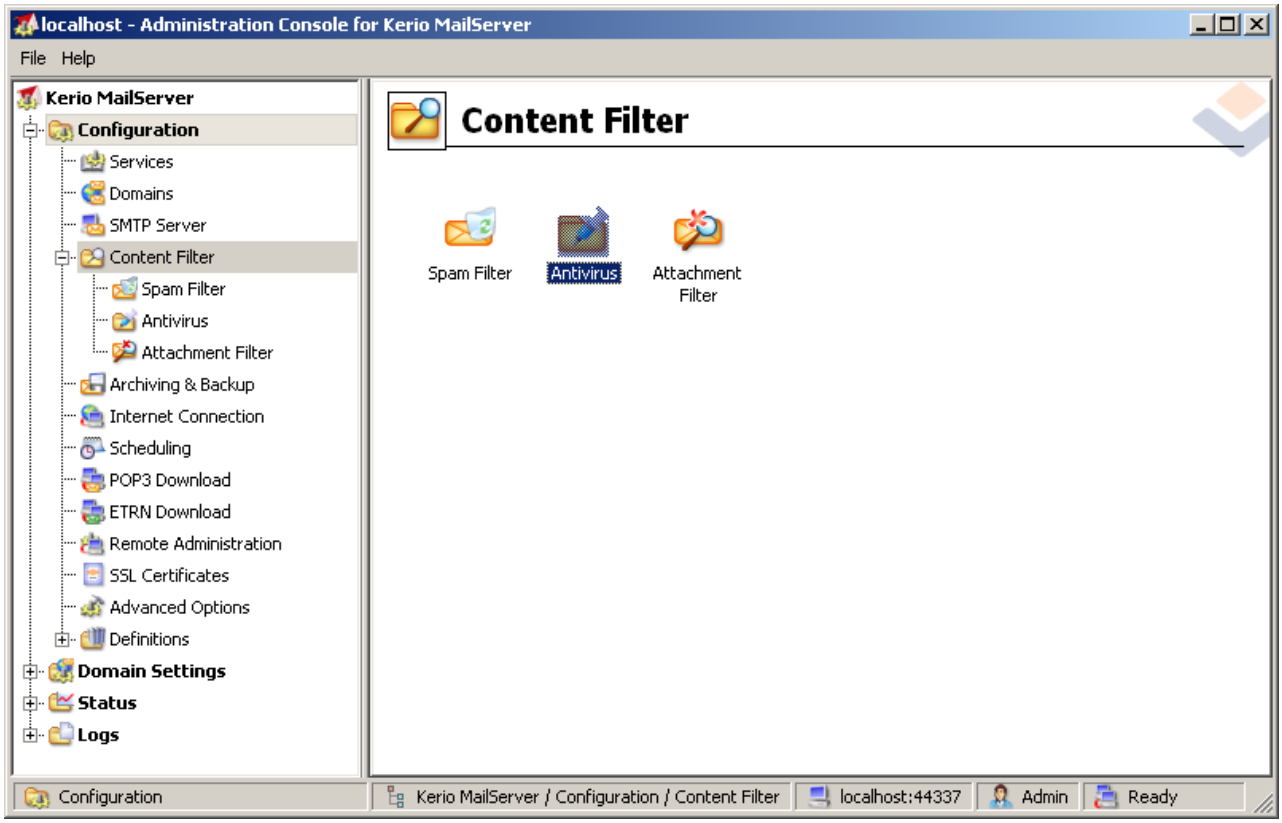
非常に高度なレベルでスパム対策設定を変更する必要がある場合は、ユーザー インターフェースに直接表示される指示に従ってください。通常、各ダイアログで変更できるのは、1 つの特定の機能のみです。その説明は常にダイアログ内に表示されます。

- ***フィルタリング*** - 言語リスト、国リスト、許可された IP、ブロックする IP、ブロックする国、ブロックする文字セット、スプーフィング送信者
- ***RBL*** - RBL サーバー、マルチヒット、しきい値、タイムアウト、最大 IP
- ***インターネット接続*** - タイムアウト、プロキシサーバー、プロキシ認証

7. AVG for Kerio MailServer

7.1. 構成

ウィルス対策保護メカニズムは Kerio MailServer アプリケーションと直接統合されています。AVG スキャン エンジンによる Kerio MailServer の電子メール保護を有効化するには、Kerio Administration Console アプリケーションを起動します。アプリケーションウィンドウの左側のコントロールツリーで、[Configuration] ブランチの [Content Filter] サブブランチを選択します。

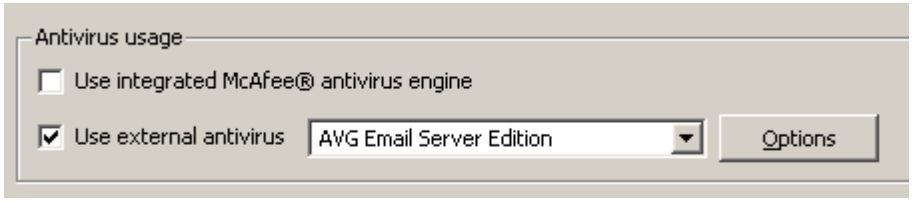


[Content Filter] 項目をクリックすると、3 つの項目が含まれるダイアログが表示されます。

- ***Spam Filter***
- ***Antivirus*** (***ウイルス対策***の項を参照)
- ***Attachment Filter*** (***添付ファイルフィルタ***の項を参照)

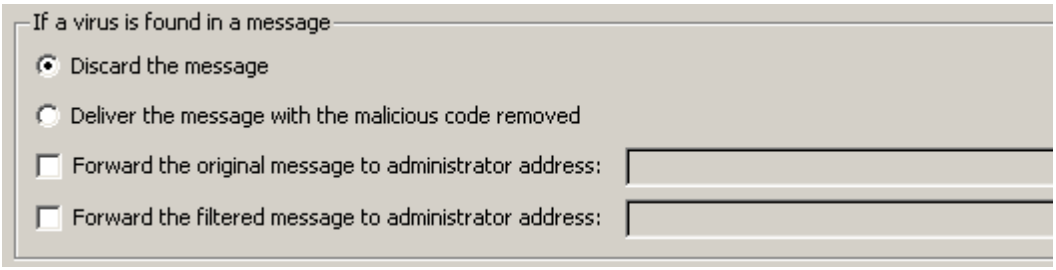
7.1.1. ウィルス対策

AVG for Kerio MailServer を有効化するには、[外部ウイルス対策を使用] チェックボックスを選択し、コンフィグレーション ウィンドウの [ウイルス対策使用] フレームの [外部ソフトウェア] メニューから [AVG Email Server Edition] 項目を選択します。



次のセクションでは、感染したメッセージまたはフィルタリングされたメッセージの処理方法を指定できます。

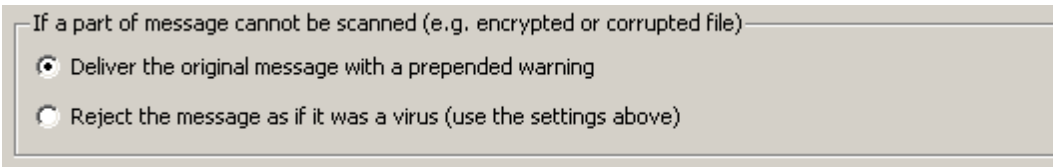
- ***メッセージでウイルスが検出された場合***



このフレームでは、メッセージでウィルスが検出された場合や、添付ファイル フィルタでメッセージが除外された場合に実行するアクションを指定します。

  - ***メッセージを廃棄*** - 選択すると、感染またはフィルタリングされたメッセージは削除されます。
  - ***悪意のあるコードを除去してメッセージを配信*** - 選択すると、メッセージは受信者に配信されますが、有害な可能性のある添付ファイルは除去されます。
  - ***元のメッセージを管理者のアドレスに転送*** - 選択すると、ウイルスに感染したメッセージは、[アドレス] テキスト フィールドで指定したアドレスに転送されます。
  - ***フィルタリングされたメッセージを管理者のアドレスに転送*** - 選択すると、フィルタリングされたメッセージは、[アドレス] テキスト フィールドで指定したアドレスに転送されます。

- ***メッセージの一部をスキャンできない場合 (暗号化ファイルや破損したファイルなど)***

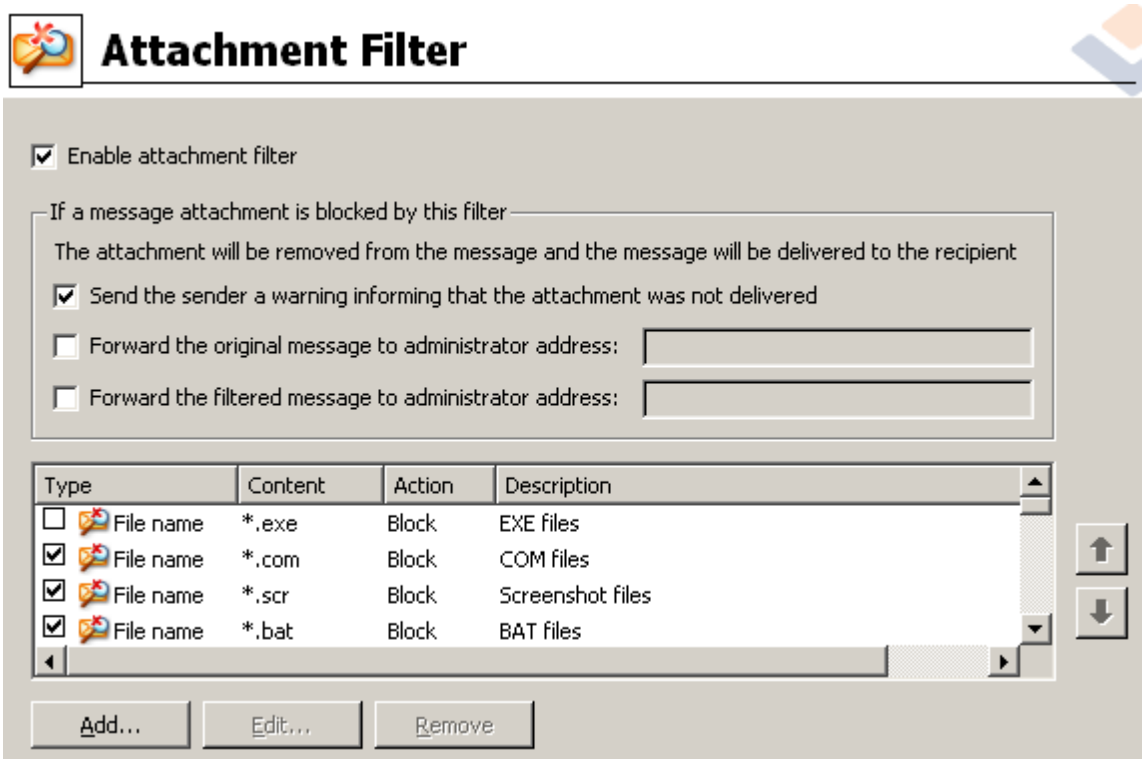


このフレームでは、メッセージや添付ファイルの一部をスキャンできない場合のアクションを指定します。

  - ***元のメッセージを警告とともに配信*** - メッセージまたは添付ファイルはチェックせずに配信されます。ユーザーはウイルスが含まれている可能性があるというメッセージ警告を受信します。
  - ***ウイルスの場合と同様にメッセージを拒否*** - システムはウイルスが検出された場合と同じ処理を実行します。つまり、メッセージは添付ファイルを削除してから配信されるか、拒否されます。このオプションは安全ですが、パスワード保護したアーカイブの送信は事実上不可能です。

7.1.2. 添付ファイル フィルタ

[添付ファイルフィルタ] メニューには、さまざまな添付ファイル定義のリストがあります。



[添付ファイルフィルタを有効にする] チェックボックスを選択すると、電子メール添付ファイルのフィルタリングの有効化/無効化を切り替えられます。任意で、次の設定を変更できます。

- ***添付ファイルが配信されなかったという警告を送信者に送信***

  送信者は、Kerio MailServer から、ウイルスまたはブロックされた添付ファイルを含むメッセージを送信したことを示す警告を受信します。

- ***元のメッセージを管理者のアドレスに転送***

  メッセージは、ローカルアドレスまたは外部アドレスに関係なく、定義した電子メールアドレスに転送されます (感染や禁止された添付ファイルが含まれたままの状態で)。

- ***フィルタリングされたメッセージを管理者のアドレスに転送***

  感染や禁止された添付ファイルが含まれないメッセージが指定された電子メール アドレスに転送されます (下記で選択したアクションは除く)。これは、ウイルス対策または添付ファイルフィルタ、あるいはその両方が正しく機能していることを検証するために使用できます。

拡張子のリストでは、各アイテムに 4 つのフィールドがあります。

- ***種類*** - [コンテンツ] フィールドで指定された拡張子で判断される添付ファイルの種類を指定。選択できる種類は、ファイル名または MIME タイプです。このフィールドの該当するボックスを選択すると、添付ファイルフィルタにアイテムを追加/除外できます。

- ***コンテンツ*** - ここでフィルタリングする拡張子を指定できます。ここでは、オペレーティングシステムのワイルドカードを使用できます (例えば、文字列 *.doc.* ’は、.doc 拡張子のすべてのファイルとそれに続くすべての拡張子を示します)。

- ***アクション*** - 特定の添付ファイルに対して実行するアクションを定義します。許可 (添付ファイルを許可)、ブロック (先に無効な添付ファイルのリストとして定義されたとおりに処理されます) のいずれかのアクションを実行できます。

- ***説明*** - このフィールドでは添付ファイルの説明を定義します。

[削除] ボタンをクリックすると、リストからアイテムが削除されます。[***追加...***] ボタンをクリックすると、リストに別のアイテムを追加できます。あるいは、[***編集...***] ボタンをクリックすると、既存のレコードを編集できます。次のウィンドウが表示されます。

- [説明] フィールドには、フィルタリングする添付ファイルの概要説明を入力できます。

- [電子メールメッセージに添付ファイルが含まれる場合] フィールドでは、添付ファイルの種類 (ファイル名または MIME タイプ) を選択できます。表示される拡張子リストから特定の拡張子も選択できます。あるいは、拡張子ワイルドカードを直接入力できます。

[次の処理] フィールドでは、定義された添付ファイルを許可するか、ブロックするかを決定できます。

8. FAQ およびテクニカル サポート

AVG に関する問題がある場合、購入に関する問題、技術的問題にかかわらず、AVG Web サイト (***http://www.avg.com***) の FAQ を参照してください。

この方法でヘルプが見つからない場合は、電子メールでテクニカルサポート部門までお問い合わせください。システム メニューの***ヘルプ/オンライン ヘルプ***より、お問い合わせフォームをご利用ください。