AVG Email Server Edition 2012

ユーザー マニュアル

ドキュメント改訂 2012.06 (2/ 28/ 2012)

目次

1. はじめに 4

2. AVG インストール要件 5

2.1 対応オペレーティング システム 5
2.2 対応電子メール サーバー 5
2.3 ハードウェア要件 5
2.4 古いバージョンのインストール 5
2.5 MS Exchange サービス パック 6

3. AVG インストール処理 7

3.1 インストールの実行 7
3.2 ライセンスのアクティベート 8
3.3 インストール タイプの選択 9
3.4 カスタム インストール - カスタム オプション 10
3.5 インストール完了 11

4. MS Exchange Server 2007/ 2010 向けメール スキャナ 13

4.1 概要 13
4.2 MS Exchange 向けメール スキャナ (ルーティング TA) 16
4.3 MS Exchange 向けメール スキャナ (SMTP TA) 17
4.4 MS Exchange 向けメール スキャナ (VSAPI) 18
4.5 検出アクション 21
4.6 メール フィルタリング 22

5. MS Exchange Server 2003 向けメールスキャナ 24

5.1 概要 24
5.2 MS Exchange 向けメール スキャナ (VSAPI) 27
5.3 検出アクション 30
5.4 メール フィルタリング 31

6. AVG for Kerio MailServer 32

6.1 構成 32
6.1.1 ウィルス対策 32
6.1.2 添付ファイル フィルタ 32

7. スパム対策設定 36

7.1 スパム対策インターフェース 36

7.2 スパム対策の原理 38
7.3 スパム対策設定 38
7.3.1 スパム対策学習ウィザード *38*
7.3.2 メッセージのあるフォルダを選択 *38*
7.3.3 メッセージ フィルタリング オプション *38*
7.4 パフォーマンス 43
7.5 RBL 44
7.6 ホワイトリスト 45
7.7 ブラックリスト 46
7.8 エキスパート設定 47

8. AVG 設定マネージャ 48

9. FAQ およびテクニカル サポート 51

1. はじめに

このユーザー マニュアルは、**AVG Email Server Edition 2012** の包括的なマニュアルです。

AVG Email Server Edition 2012 をご購入いただき、どうもありがとうございます。

AVG Email Server Edition 2012 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 2012** 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、特定の電子メールサーバー版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、ユーザーガイドの Internet Security 版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 2012 は、次のオペレーティング システムで稼動する電子メール サーバーの保護を目的としています。

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

2.2. 対応電子メール サーバー

次の電子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
- 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 2012 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 2012 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 2012** 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/exchange/evaluation/sp2/overview.mspx

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

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 Web 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。

メモ: *各製品には 32 ビット オペレーティング システム (x86) 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/セール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 をオンラインで購入した場合は、ライセンス番号が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て保存すると、インストール処理を実行できます。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、ライセンス条件に目を通します。[***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。

メモ: *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 AVG をオンラインで購入した後に送信される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継続します。

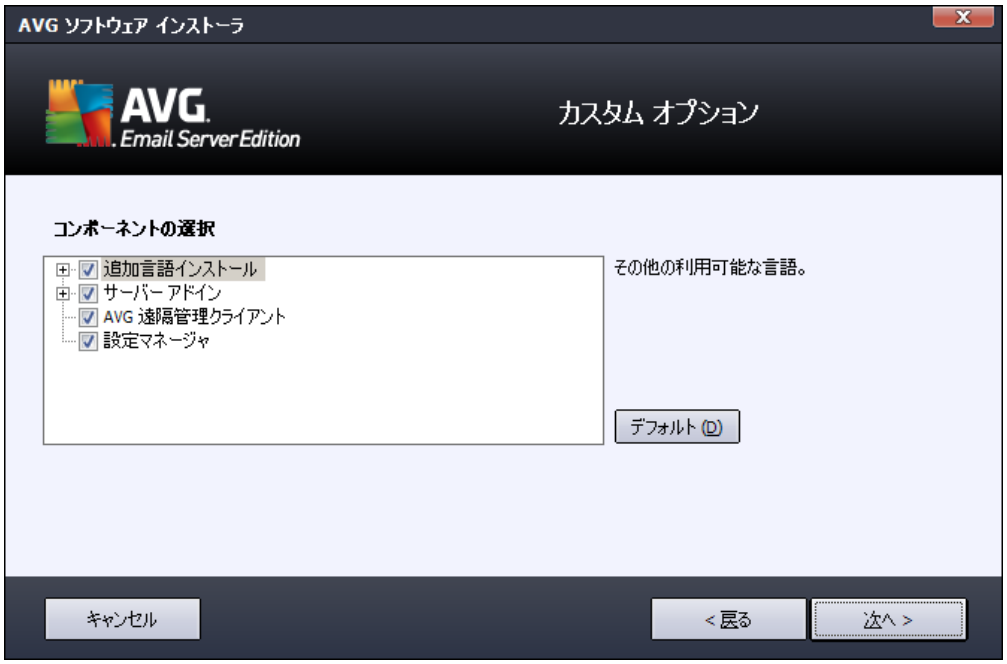
3.3. インストール タイプの選択

[***インストール タイプの選択***] ダイアログでは、[***クイック 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。

通常ユーザーの場合は、[***クイック 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が強く推奨されます。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)。

3.4. カスタム インストール - カスタム オプション



[***インストール先 フォルダ***] ダイアログでは、AVG をインストールする場所を指定します。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。

[***コンポーネント選択***] ダイアログでは、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。既定の設定が適当でない場合は、特定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。

- ***AVG 遠隔管理クライアント*** - 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。
- ***設定マネージャ*** - 主にネットワーク管理者向けのツールで、AVG 設定のコピー、編集、配布ができます。設定をポータブル デバイス (USB フラッシュ ドライバなど) に保存して、手動またはその他の方法で選択したステーションに適用できます。
- ***追加のインストール言語*** - AVG のインストールで使用する言語を定義できます。[***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 アドイン***):

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

  すべての受信電子メールをチェックし、望ましくないメールを SPAM と見なします。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 メッセージに対する最大限の保護を提供します。

- ***E-mail Scanner for MS Exchange (ルーティング転送エージェント)***

  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 メッセージがチェックされます。

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

- ***E-mail Scanner for MS Exchange (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 メッセージをチェックします。

  MS Exchange 2007/2010 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。

- ***E-mail Scanner for MS Exchange (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 メッセージをチェックします。ウィルスが検出されると、ウイルス隔離室に移動されるか、完全に削除されます。

メモ: *MS Exchange のバージョンによって利用可能なオプションが異なります。*

[***次へ***] ボタンをクリックして続行します。

3.5. インストール完了

モジュール選択で***遠隔管理コンポーネント***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。

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。

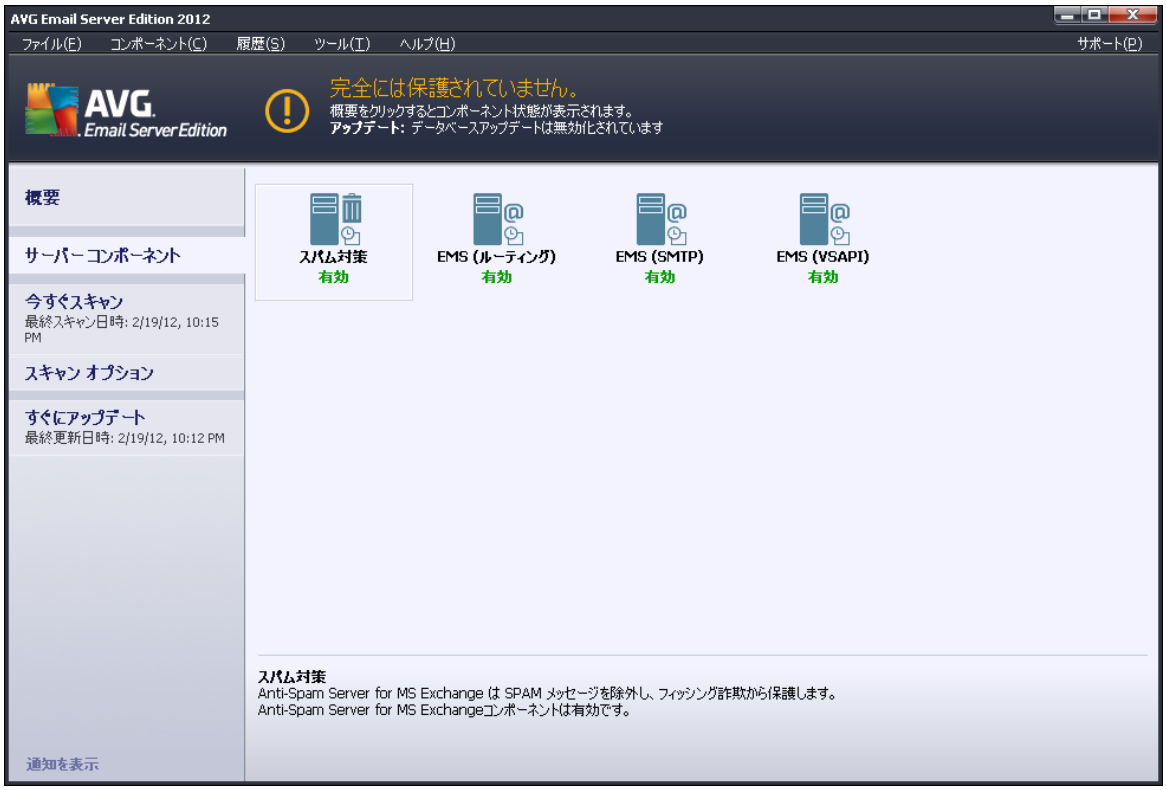
電子メール サーバーの保護を個々に設定する場合は、該当する章に記載されている手順に従ってください。

- *MS Exchange Server 2007/2010 向けメール スキャナ*
- *MS Exchange Server 2003 向けメール スキャナ*
- *AVG for Kerio MailServer*

4. MS Exchange Server 2007/ 2010 向けメール スキャナ

4.1. 概要

AVG for MS Exchange Server 2007/2010 構成オプションはサーバー コンポーネントとして AVG Email Server Edition 2012 と完全に統合されています。



各サーバー コンポーネントの基本概要

- ***スパム対策 - MS Exchange 向けスパム対策サーバー***

  すべての受信電子メールをチェックし、望ましくないメールを SPAM と見なします。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 メッセージに対する最大限の保護を提供します。

- ***EMS (ルーティング) - MS Exchange 向け電子メール スキャナ (ルーティング転送エージェント)***

  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 メッセージがチェックされます。

  MS Exchange 2007/2010 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 向け電子メール 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 メッセージをチェックします。

MS Exchange 2007/2010 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 向け電子メール スキャナ (VSAPI)***

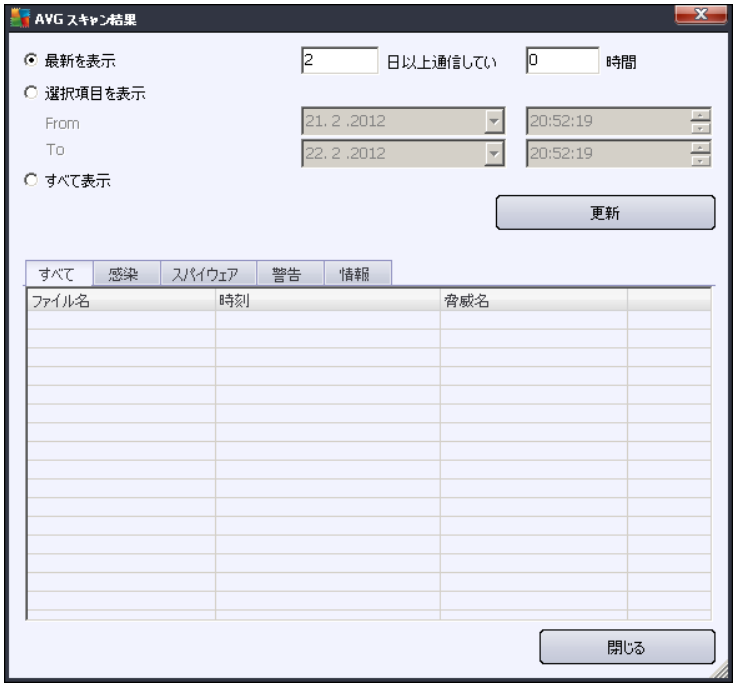
  ユーザーのメールボックスに保存されているすべての電子メール メッセージをチェックします。ウィルスが検出されると、ウイルス隔離室に移動されるか、完全に削除されます。

重要な注意事項: *Hub Exchange ロールでルーティング転送エージェントとともに VSAPI をインストールして使用する場合は、電子メール メッセージが 2 度スキャンされます。これを回避するため、VSAPI 設定の [**送信メッセージをスキャンしない (MS Exchange 2007/2010)**] ボックスをチェックしてください (こちら をクリックすると詳細を表示します)。*

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。スパム対策を除くすべてのコンポーネントで次のコントロール ボタンとリンクを利用できます。

- ***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。

既定では過去 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。
- ***統計値のリセット*** - すべての統計値をゼロにリセットします。

次の操作ボタンを利用できます。

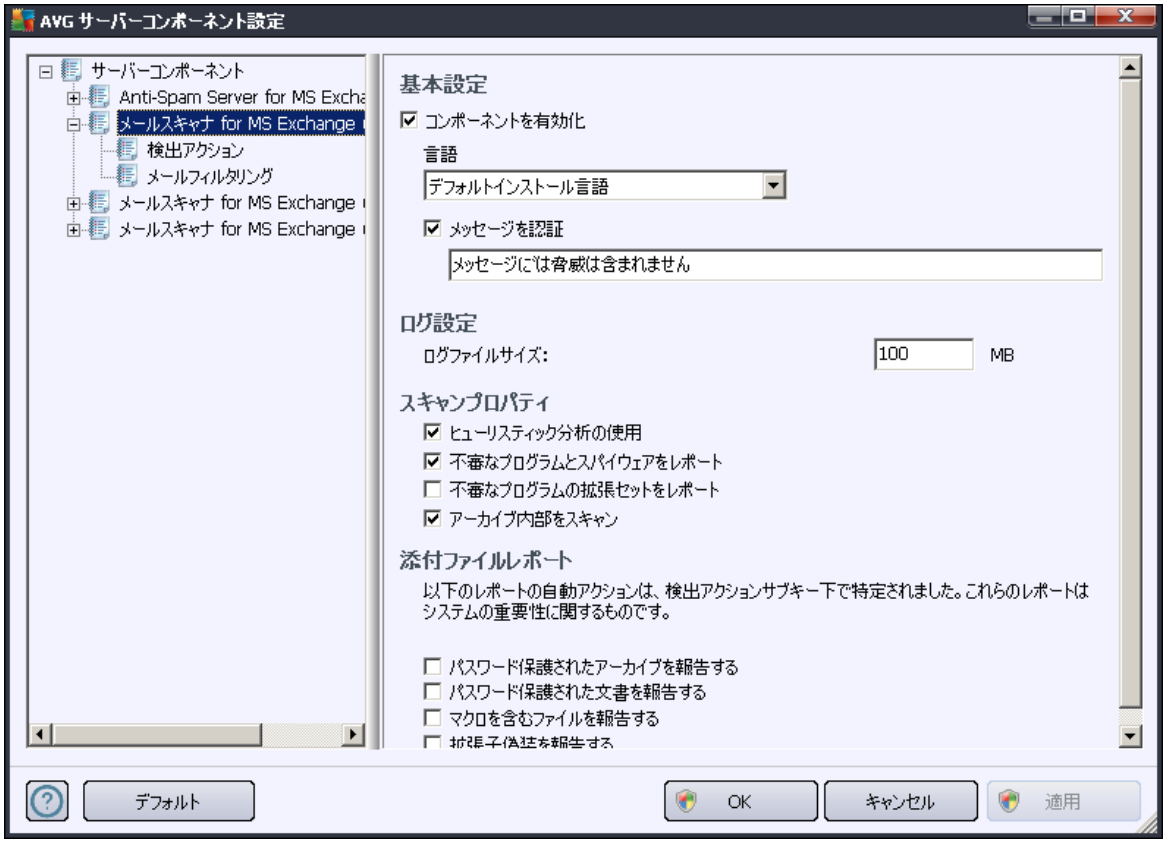
- ***設定*** - このボタンをクリックすると、コンポーネントの設定が開きます。
- ***戻る*** – このボタンをクリックすると、サーバー コンポーネント概要

各コンポーネント固有の設定の詳細については、次の章を参照してください。

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

E-mail Scanner for MS Exchange (ルーティング転送エージェント) 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)***] 項目を選択します。



[***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チェックをオンにします。次のフィールドでメッセージをカスタマイズできます。

[***ログ設定***] セクション:

- ***ログ ファイル サイズ*** - 任意のログファイルサイズを選択します。既定値は 100 MB です。

[***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

チェックをオンにします。

- ***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、既定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のチェックをオンにします。

[***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] が追加されます。この既定の設定は [***検出アクション***] セクションの [***情報***] 部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***

4.3. MS Exchange 向けメールスキャナ (SMTP TA)

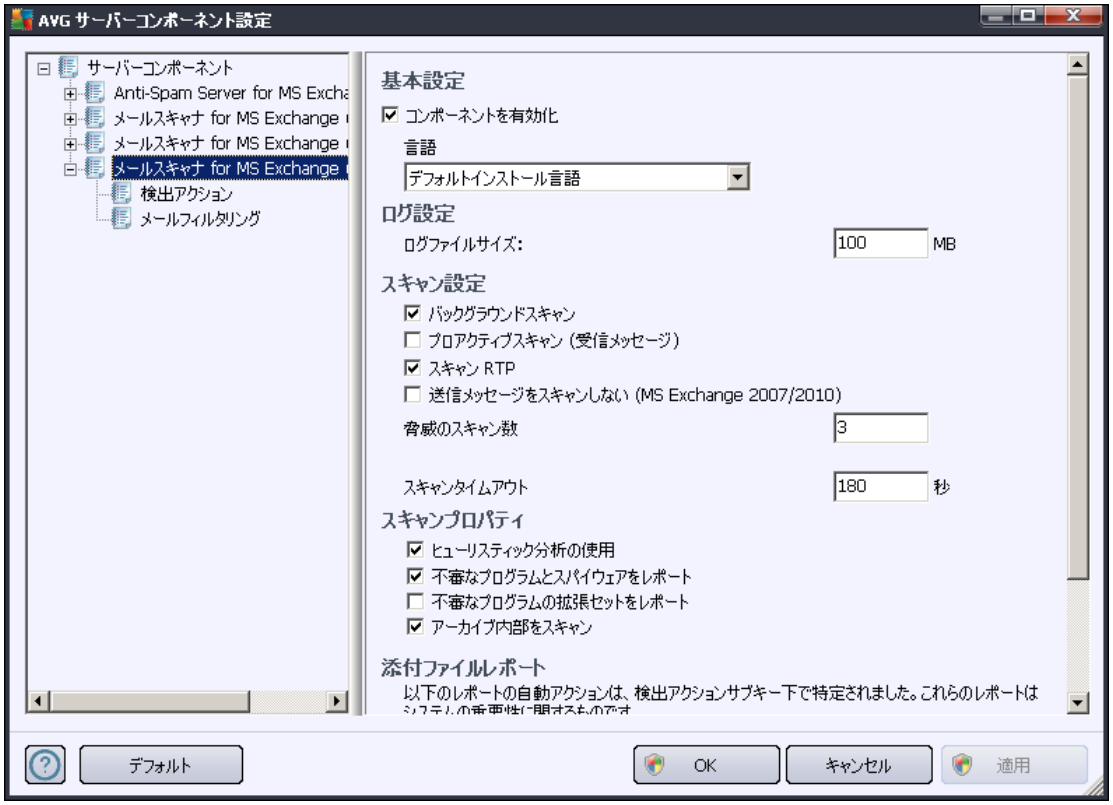
[***MS Exchange (SMTP TA) 向けメールスキャナ***] 設定はトランスポートエージェントのルーティングと全く同じです。詳細については、前述の ***MS Exchange (ルーティング TA) 向けメールスキャナ***の章をご覧ください。

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***

4.4. MS Exchange 向けメール スキャナ (VSAPI)

この項目には ***E-mail Scanner for MS Exchange (VSAPI)*** 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。

[***ログ設定***] セクション:

- ***ログ ファイル サイズ*** - 任意のログファイルサイズを選択します。既定値は 100 MB です。

[***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 ウィルス 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列で実行されます。

  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 (E-mail Scanner for MS Exchange データベースの電子メール 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 ストア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。

  メモ: *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。*

メモ: [バックグラウンド スキャン] *と* ***[プロアクティブ スキャン]*** *オプションを無効にしても、ユーザーが MS Outlook クライアントでメッセージをダウンロードするときには、オンアクセス スキャナが有効になっています。*

- ***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)*** - 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 (1 台のサーバーを使用しているか、別々で 2 台のサーバーを使用しているかは関係ありません) と、送信メールが 2 度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、電子メール送信である程度の遅延が発生する場合があります両方のサーバー コンポーネントがインストールされ、アクティブになっているかどうかがわからない場合は、このボックスをチェックし、VSAPI オンアクセス スキャナーを無効にすることで、この二重の送信メール スキャンを回避できます。
- ***スキャン スレッド数*** - *既定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。

  既定のスレッド数は「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、既定値が使用されます。

- ***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 (既定値は 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チェックをオンにします。
- ***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、既定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のチェックをオンにします。

[***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。既定の設定は [***検出アクション***] セクションの [***情報***] 部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***

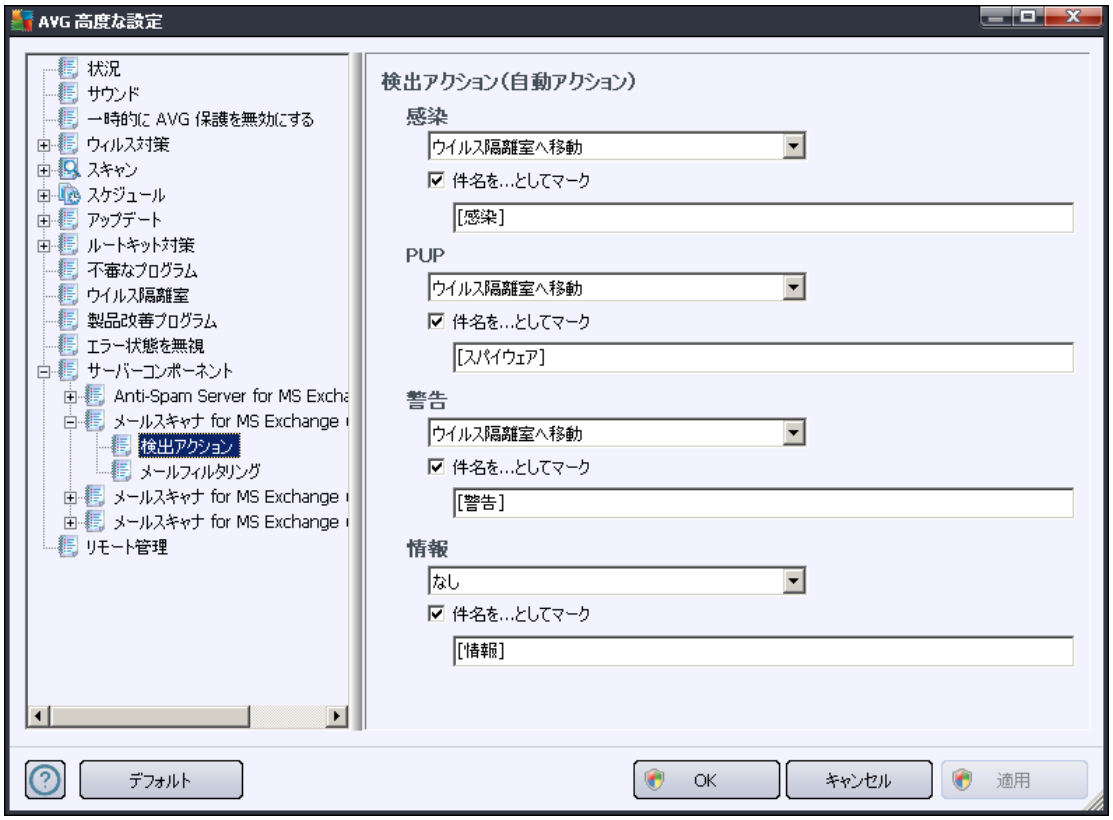
一般的に、これらの機能の一部は Microsoft VSAPI 2.0/2.5 アプリケーション インターフェース サービスのユーザー拡張です。VSAPI 2.0/2.5 の詳細については、次のリンクと参照リンクからアクセスできるリンクを確認してください。

- http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k - Exchange とウィルス対策ソフトウェア連携の情報
- 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 機能の情報

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***

4.5. 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。

- ***感染***
- ***PUP (不審なプログラム)***
- ***警告***
- ***情報***

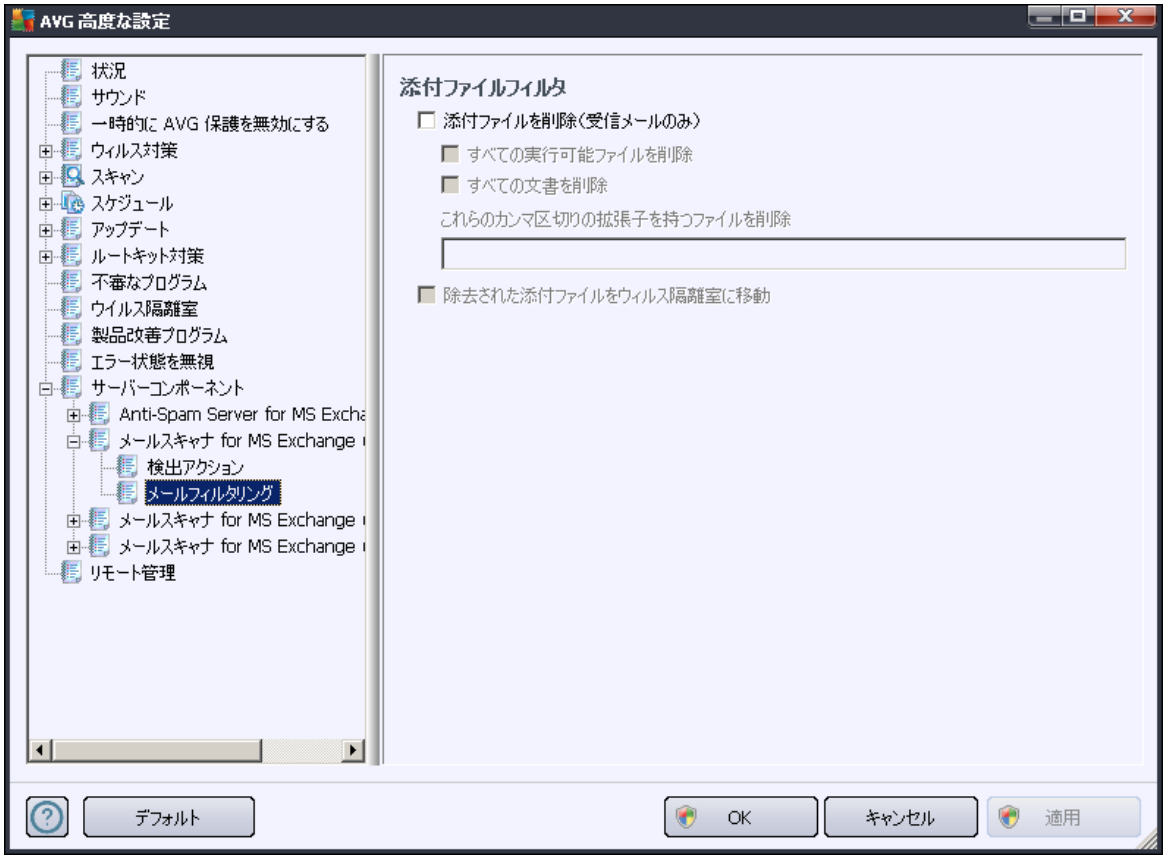
ロールダウンメニューを使い、各アイテムのアクションを選択します。

- ***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。

***注意**: 最後に説明されている機能は、MS Exchange VSAPI 向け電子メールスキャナでは利用できません。*

4.6. 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。

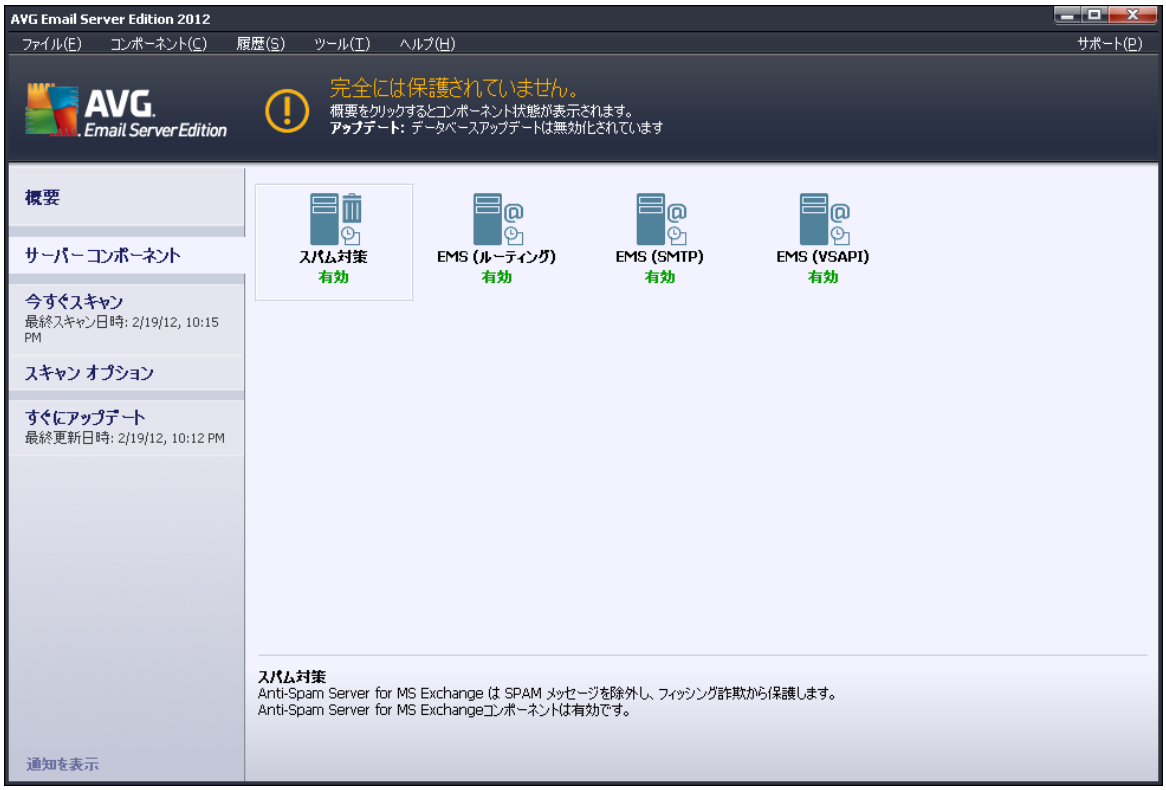
- ***添付ファイルを削除*** - このボックスをオンにして、機能を有効にします。
- ***すべての実行可能ファイルを削除*** - すべての実行可能ファイルが削除されます。
- ***すべてのドキュメントを削除*** - すべてのドキュメントファイルが削除されます。
- ***コンマで区切られた拡張子でファイルを削除*** - 自動的に削除するボックスをファイル拡張子で埋めます。拡張子をコンマで区切ります。
- ***除外された添付ファイルをウィルス隔離室に移動する*** - 除外された添付ファイルを完全に削除しない場合にはチェックを付けます。このボックスを選択すると、ダイアログで選択されたすべての添付ファイルが自動的にウィルス隔離室環境に移動されます。ウィ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。ウィルス隔離室は **AVG Email Server Edition 2012** 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。[***履歴***] 項目をクリックするだけで、ドロップダウン メニュー

から[***ウィルス隔離室***] 項目を選択できます。

5. MS Exchange Server 2003 向けメールスキャナ

5.1. 概要

E-mail Scanner for MS Exchange Server 2003 構成オプションは、完全にサーバー コンポーネントとして AVG Email Server Edition 2012 と統合されています。



サーバー コンポーネントには次が含まれます。

各サーバー コンポーネントの基本概要

- ***スパム対策 - MS Exchange 向けスパム対策サーバー***

  すべての受信電子メールをチェックし、望ましくないメールを SPAM と見なします。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 メッセージに対する最大限の保護を提供します。

- ***EMS (VSAPI) - MS Exchange 向け電子メール スキャナ (VSAPI)***

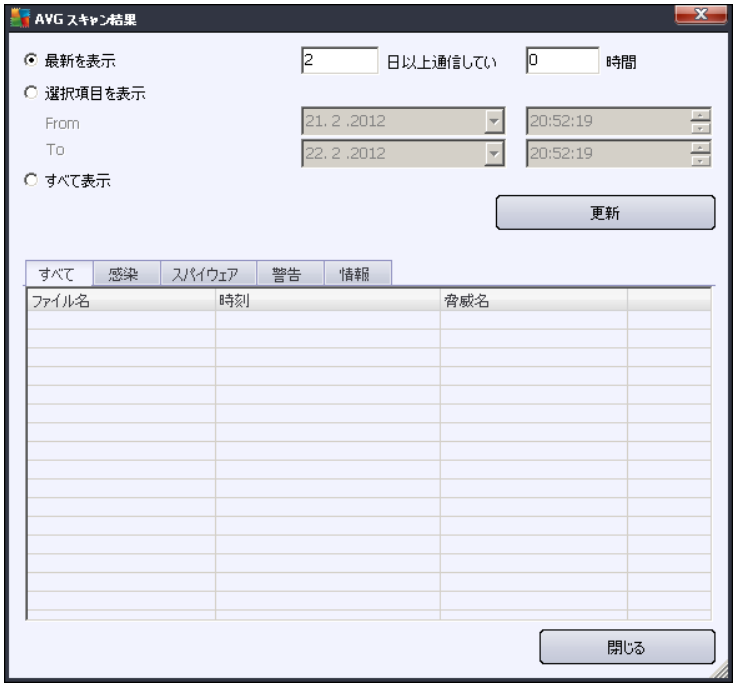
  ユーザーのメールボックスに保存されているすべての電子メール メッセージをチェックします。ウィルスが検出されると、ウイルス隔離室に移動されるか、完全に削除されます。

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。***スパム対策 コンポーネント***の独自の画面については、個別の章を参照してください。***E-mail Scanner for MS Exchange***

(VSAPI) インターフェースには次 のコントロール ボタンとリンクがあります。

- ***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。

既定では過去 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。
- ***統計値のリセット*** - すべての統計値をゼロにリセットします。

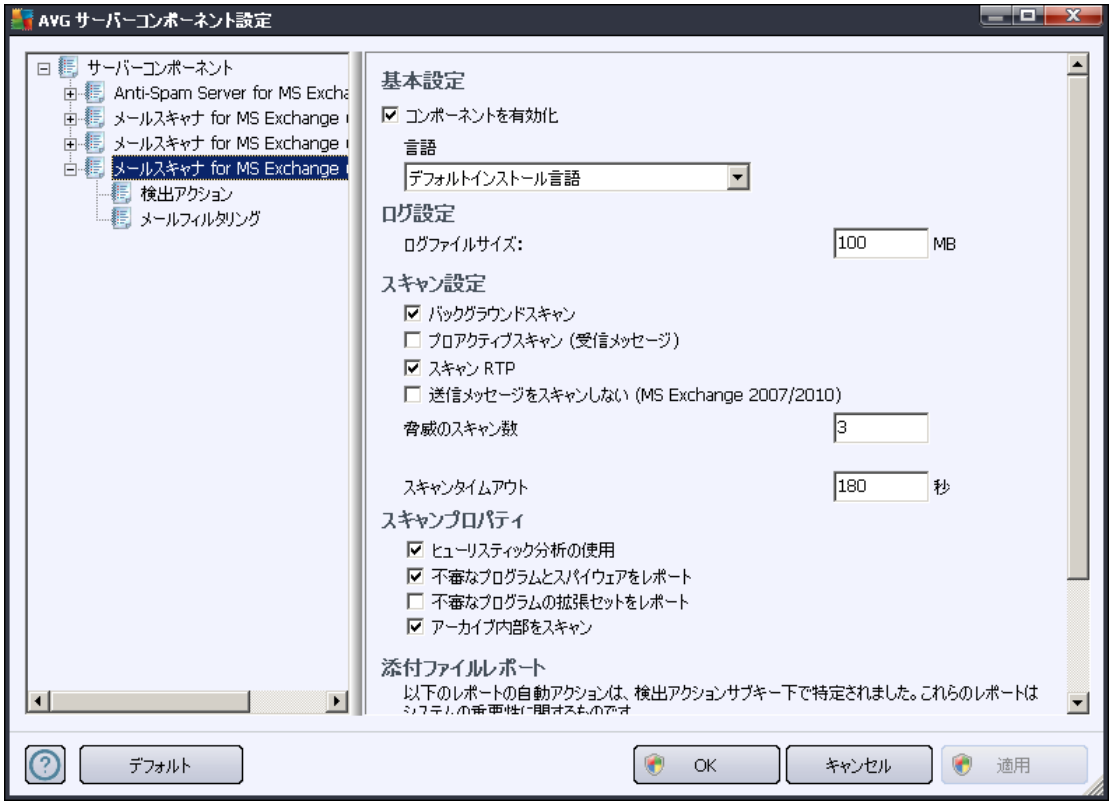
次の操作ボタンを利用できます。

- ***設定*** - このボタンをクリックすると、コンポーネントの設定が開きます。
- ***戻る*** – このボタンをクリックすると、サーバー コンポーネント概要

各コンポーネント固有の設定の詳細については、次の章を参照してください。

5.2. MS Exchange 向けメール スキャナ (VSAPI)

この項目には ***E-mail Scanner for MS Exchange (VSAPI)*** 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。

[***ログ設定***] セクション:

- ***ログ ファイル サイズ*** - 任意のログファイルサイズを選択します。既定値は 100 MB です。

[***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 ウィルス 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列で実行されます。

  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 (E-mail Scanner for MS Exchange データベースの電子メール 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 ストア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。

  メモ: *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。*

メモ: [バックグラウンド スキャン] *と* ***[プロアクティブ スキャン]*** *オプションを無効にしても、ユーザーが MS Outlook クライアントでメッセージをダウンロードするときには、オンアクセス スキャナが有効になっています。*

- ***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。
- ***スキャン スレッド数*** - *既定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。

  既定のスレッド数は「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、既定値が使用されます。

- ***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 (既定値は 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チェックをオンにします。
- ***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、既定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のチェックをオンにします。

[***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。既定の設定は [***検出アクション***] セクションの [***情報***] 部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***

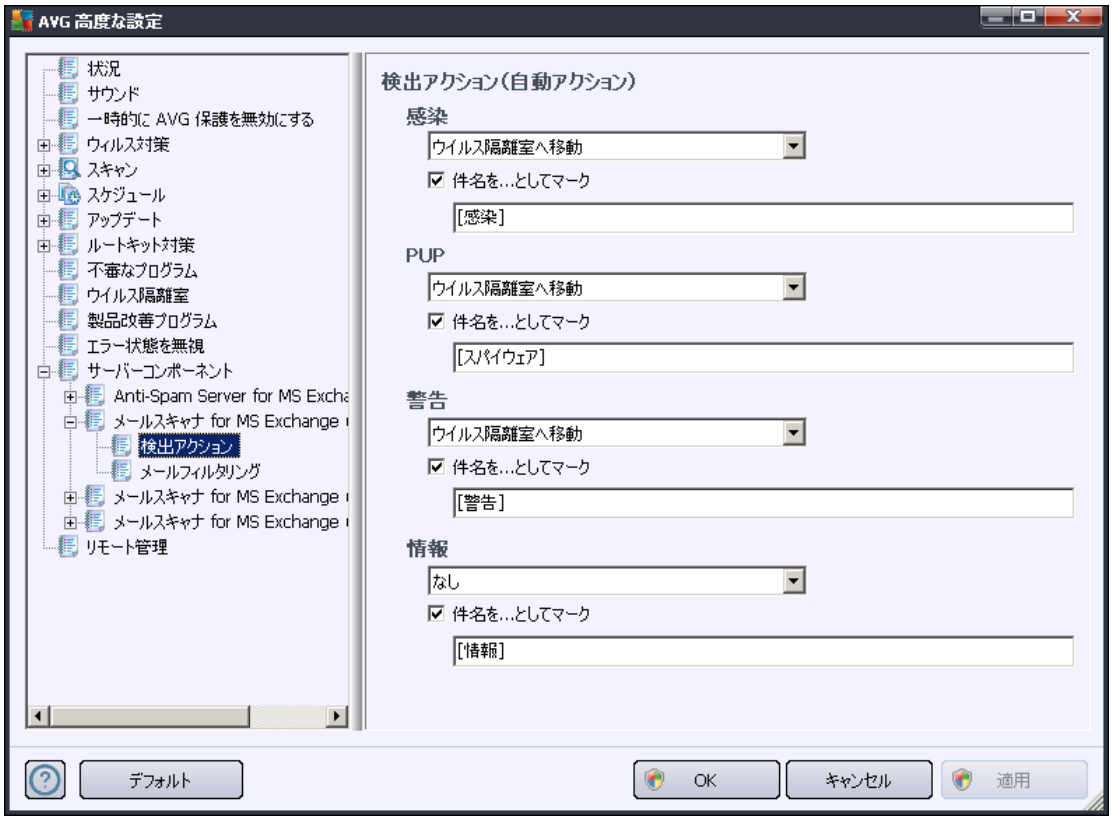
一般的に、これらの機能はすべて Microsoft VSAPI 2.0/2.5 アプリケーション インターフェース サービスのユーザー拡張です。VSAPI 2.0/2.5 の詳細については、次のリンクと参照リンクからアクセスできるリンクを確認してください。

- http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k - Exchange とウィルス対策ソフトウェア連携の情報
- 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 機能の情報

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***

5.3. 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。

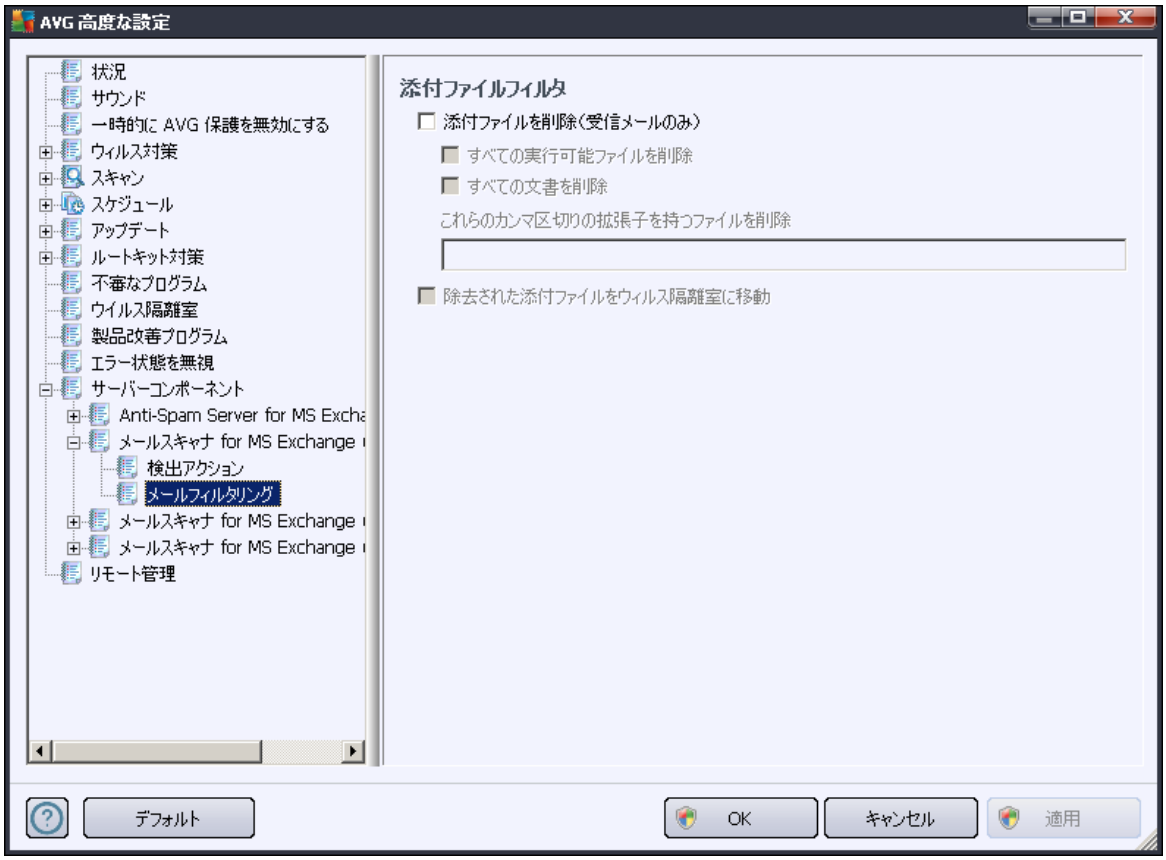
このアクションは以下のアイテムで利用可能です。

- ***感染***
- ***PUP (不審なプログラム)***
- ***警告***
- ***情報***

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。

5.4. メール フィルタリング



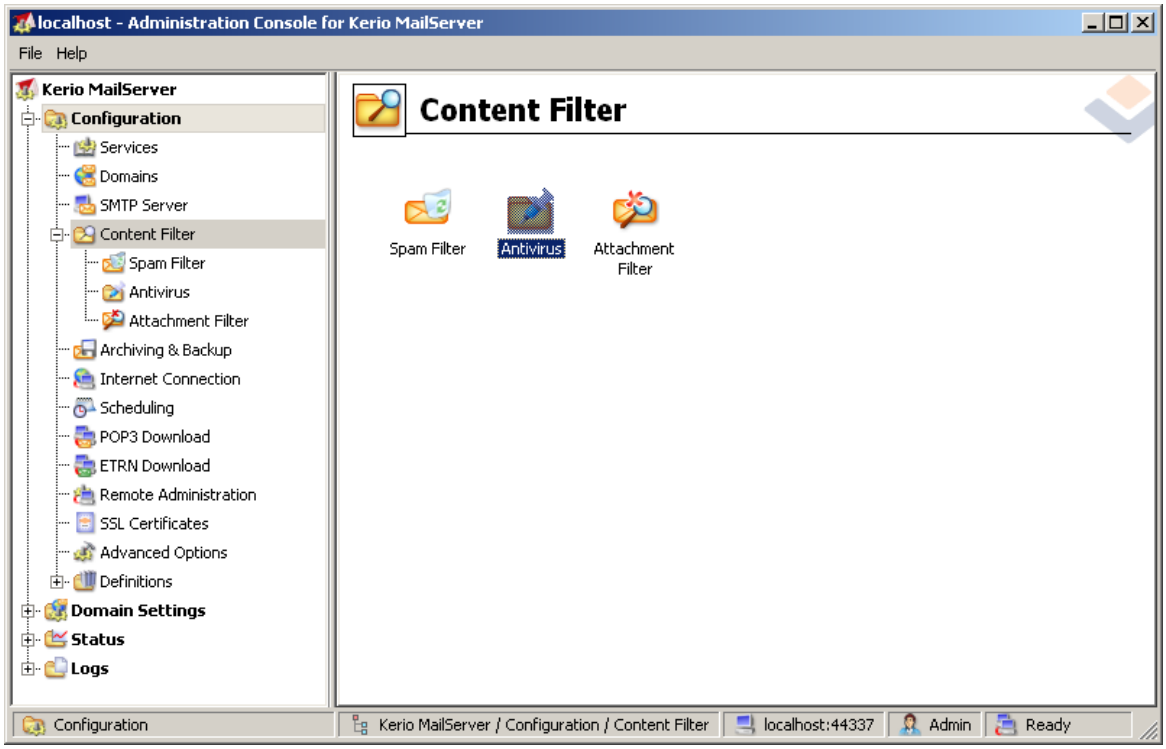
[***メールフィルタリング***] サブアイテムでは、自動的に削除する添付ファイル（ある場合）を選択できます。次のオプションが利用可能です。

- ***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ィ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ィルス隔離室環境に移動されます。ウィ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にアクセスできます。ウィルス隔離室は **AVG Email Server Edition 2012** 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。[***履歴***] 項目をクリックするだけで、ドロップダウンメニューから[***ウィルス隔離室***] 項目を選択できます。

6. AVG for Kerio MailServer

6.1. 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 スキャンエンジンで 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。

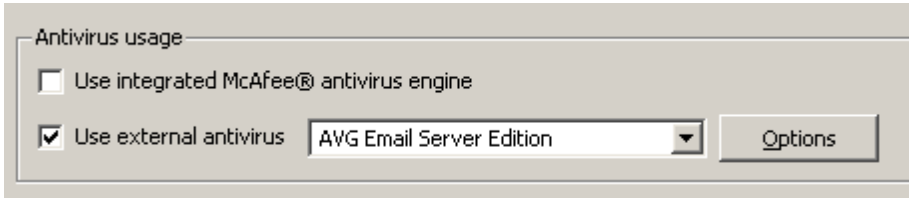


[Content Filter] 項目をクリックすると、3 つの項目が含まれるダイアログが表示されます。

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

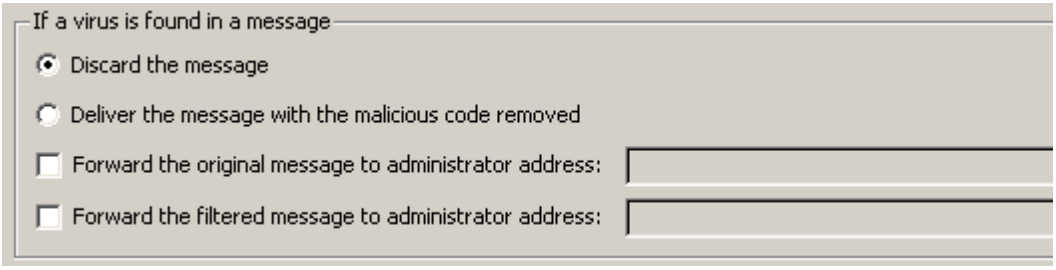
6.1.1. ウィルス対策

AVG for Kerio MailServer を有効化するには、[外部ウィルス対策を使用] 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 [ウィルス対策使用] 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。

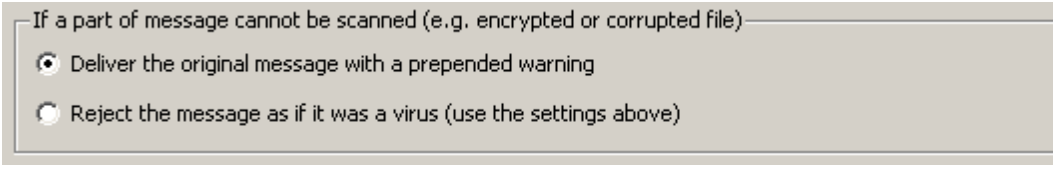
- ***メッセージでウィルスが検出された場合***



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、ウィ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)***



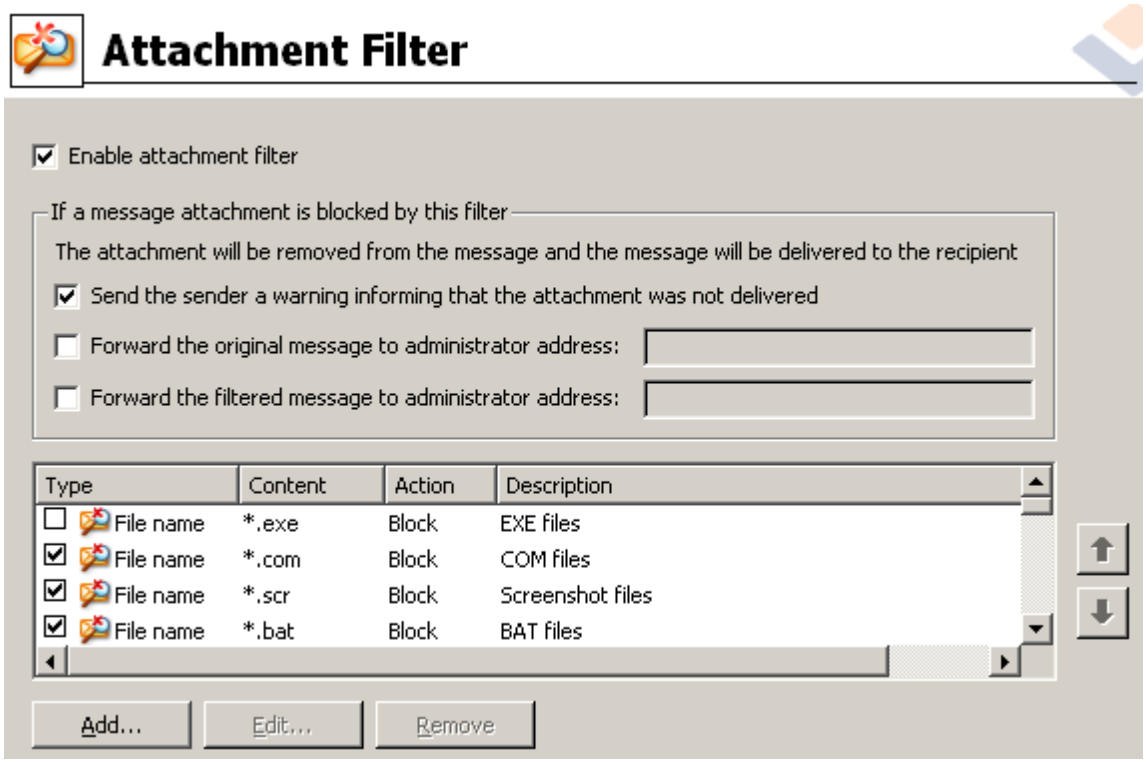
このフレームでは、メッセージや添付ファイルの一部をスキャンできない場合のアクションを指定します。

  - ***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。ユーザーはウィ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。

- ***ウィルスの場合と同様にメッセージを拒否*** - システムはウィ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。

6.1.2. 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、ウィ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 (であるため、感染や禁止された添付ファイルが含まれます)。

- ***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***

  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 (次に選択したアクションは除く)。これは、ウィ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。

7. スパム対策設定

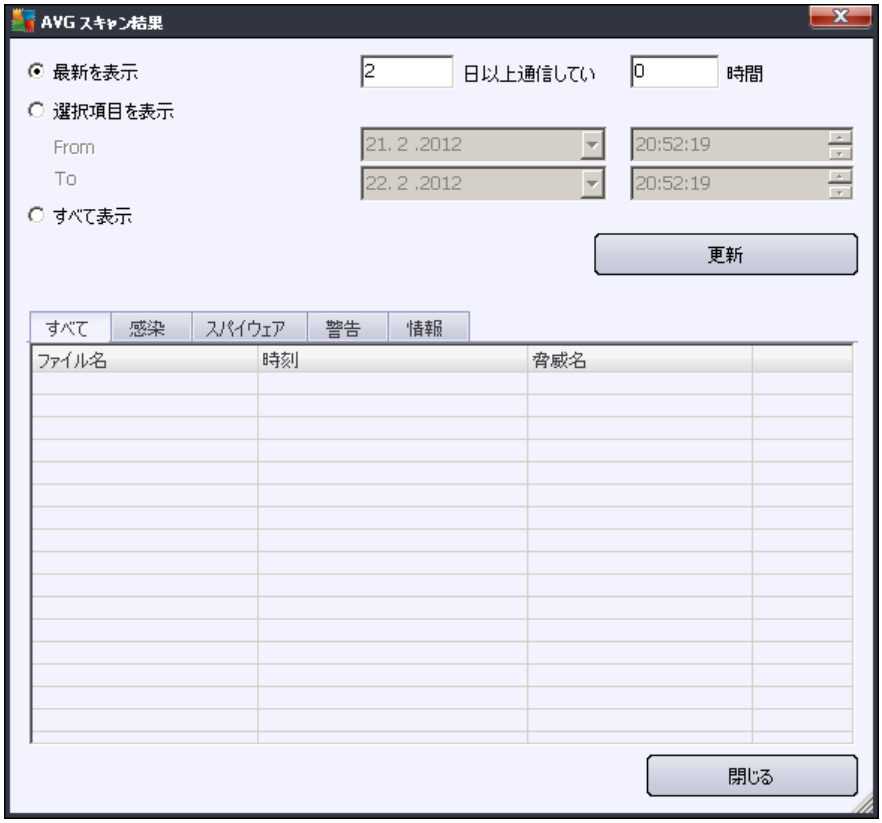
7.1. スパム対策インターフェース

[サーバーコンポーネント] セクション (左側のメニュー) に、スパム対策 ***サーバー***コンポーネントのダイアログが表示されます。ここには、サーバーコンポーネントの機能に関する概要情報、現在のステータスに関する情報 (*MS Exchange 向けスパム対策 サーバーコンポーネントはアクティブです*)、および一部の統計情報が表示されます。

利用可能なリンク:

- ***スキャン結果***

  スパム対策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。



ここでは、SPAM (望ましくないメッセージ) またはフィッシングの試み (個人情報データ、銀行詳細情報、ID などを盗む試み) のいずれかとして検出されたメッセージを確認できます。既定では、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。
- ***統計値のリセット*** - すべての統計値をゼロにリセットします。

ダイアログの [**スパム設定**] セクションには、[***スパム対策を有効にする***] チェックボックスのみがあります。チェックを外すと、スパム対策保護を無効にします (コンポーネント全体を無効にします)。このチェックボックスを使用するか、同様の [スパム対策設定] のチェックボックスを選択すると、スパム対策保護を再度有効にできます。

以下のような操作ボタンがあります。

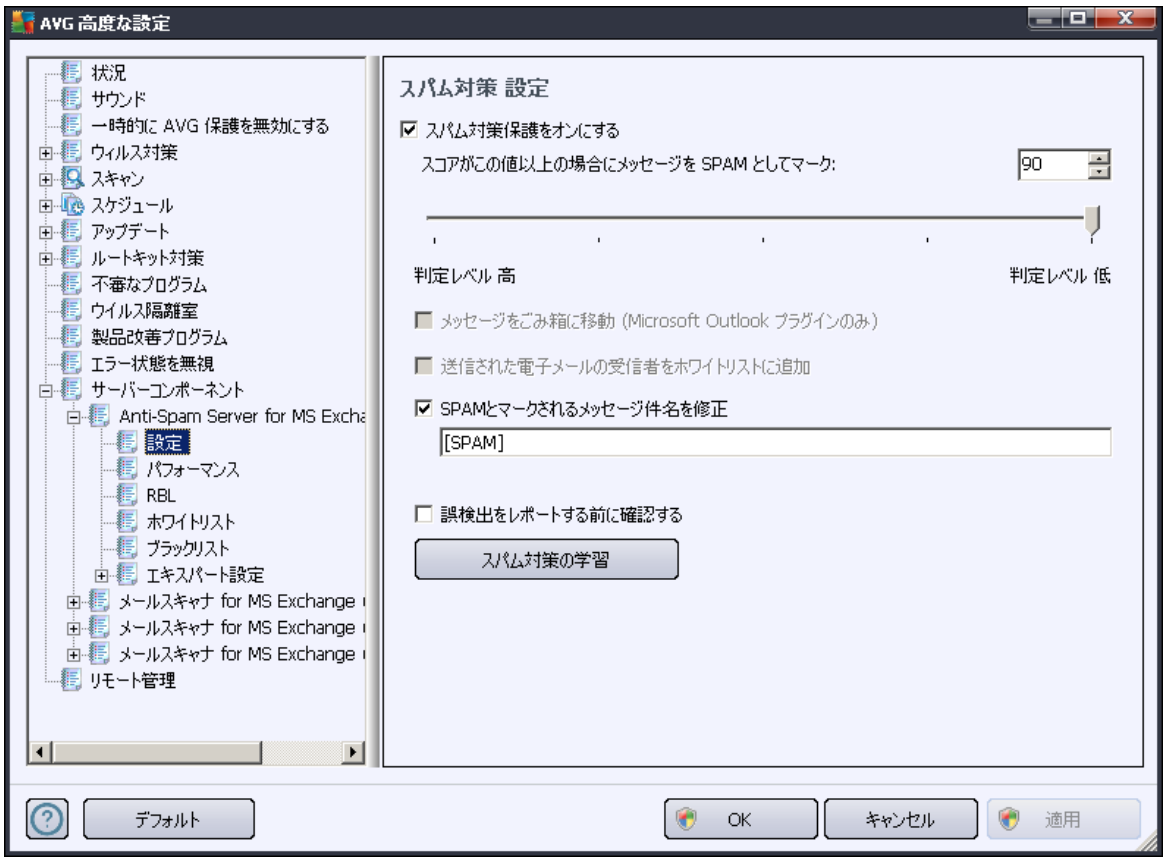
- ***設定*** – このボタンを使用すると、[スパム対策設定] を開きます。
- ***戻る*** – このボタンをクリックすると、サーバーコンポーネント概要

7.2. スパム対策の原理

スパムとは望まない電子メールのことです。一般的に、製品やサービスの広告メールが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占拠します。消費者が同意をした合法的な商業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、望ましくない電子メールを SPAM と特定します。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メッセージに対する最大限の保護を提供します。

7.3. スパム対策設定



[***スパム対策基本設定***] ダイアログの [***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ができます。[***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 メッセージは通常通りに配信されます (スパムとは見なされません)。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許可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 メッセージは除外されます。一部の正常な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。スパムの可能性があるメールは除外されます。正常なメッセージも除外される可能性があります。
- ***値 50 ～ 59*** - 非常に積極的な設定です。正常なメールが本物のスパム メッセージと同様に除外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。

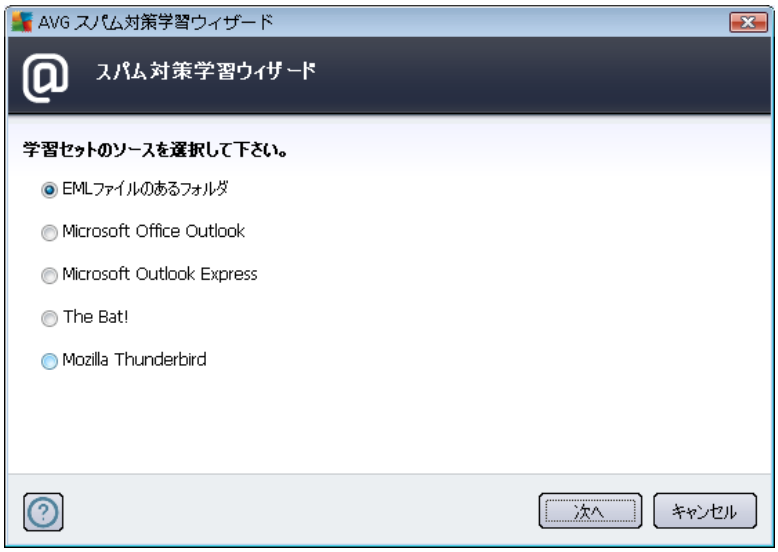
さらに、検出したスパム電子メール メッセージを処理する方法を定義できます。

- ***スパムとして判定されたメッセージの件名を修正する*** - スパムとして検出されたメッセージの件名にを特定の単語や文字を追加する場合は、このチェック ボックスを選択し、追加する任意のテキストをテキスト フィールドに入力します。
- ***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、AVG へ検出された脅威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 ボックスを選択すると、ダイアログ ボックスを表示し、メッセージがスパム メールであるかどうかを確認してから、検出されたスパムを AVG に送信できます。

[***スパム対策の学習***] ボタンをクリックすると、***スパム対策学習ウィザード***を開きます。詳細については、次の章を参照してください。

7.3.1. スパム対策学習ウィザード

スパム対策学習ウィザードの最初のダイアログでは、学習のためのメールソースを選択します。通常は、間違ってSPAMとしてマークされたメールや、認識されなかったスパムメッセージを使用します。



以下のオプションがあります。

- ***特定のメールクライアント*** - リストされたメールクライアントの1つ（*MS Outlook, Outlook Express, The Bat!, Mozilla Thunderbird*）を使用する場合、該当するオプションを選択します。
- ***EMLファイルのあるフォルダ*** - 他のメールプログラムを利用する場合、まずメッセージを特定のフォルダに保存（*eml*形式）、またはメールクライアントメッセージフォルダの場所を確認します。次に、***EMLファイルのあるフォルダ***を選択します。次のステップで希望するフォルダを指定します。

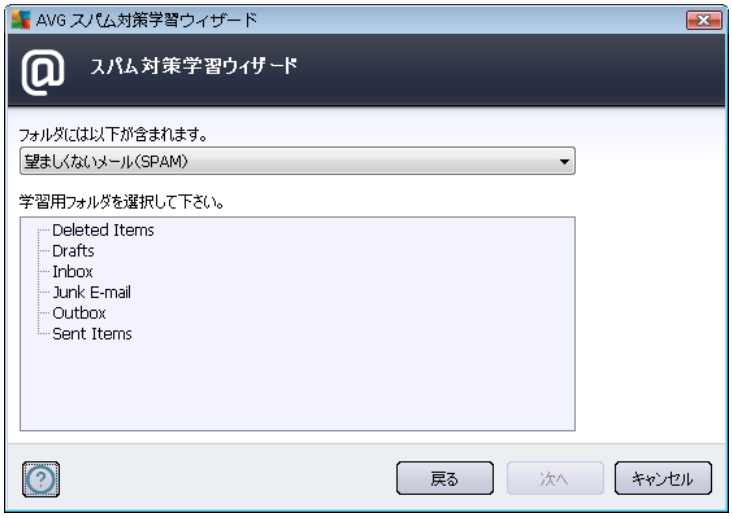
学習プロセスをより速く簡単にするために、学習に使用するフォルダーには学習用メッセージ（望ましいもの、望ましくないもの）のみを含むよう、予め整理しておくことをお勧めします。ただし、このウィザードでは、後のステップでメールをフィルタできるため、これは必ずしも必要ではありません。

適切なオプションを選択し、***次へ***をクリックしてウィザードを継続します。

7.3.2. メッセージのあるフォルダを選択

このステップで表示されるダイアログはこれまでの選択内容によって異なります。

EML ファイルのあるフォルダ



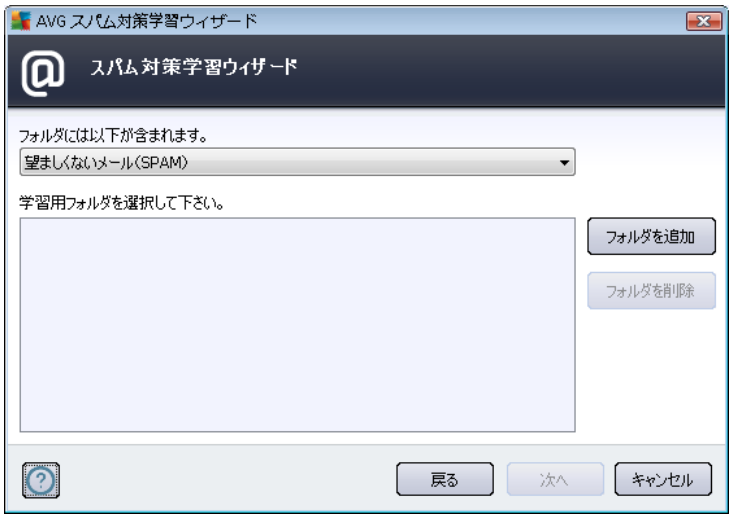
このダイアログでは学習に使用するメッセージ フォルダを選択します。[***フォルダの追加***] ボタンをクリックして、.eml ファイル (*保存された電子メール メッセージ*) のあるフォルダを参照します。選択したフォルダがダイアログに表示されます。

フォルダには次の内容が含まれます。 ドロップダウン メニューには 2 つのオプションが表示されます。ここでは選択したフォルダが望ましい (*HAM*) メールあるいは望ましくない (*SPAM*) メールのいずれを含むかを選択します。次のステップでメッセージをフィルタリングできます。フォルダには学習メールのみを含む必要はありません。また、[***フォルダの削除***] ボタンをクリックして、選択した望ましくないフォルダを一覧から削除できます。

完了したら、[***次へ***] をクリックして、[メッセージ フィルタリング オプション] に進みます。

特定の電子メール クライアント

オプションのいずれかを確認した場合、新しいダイアログが表示されます。

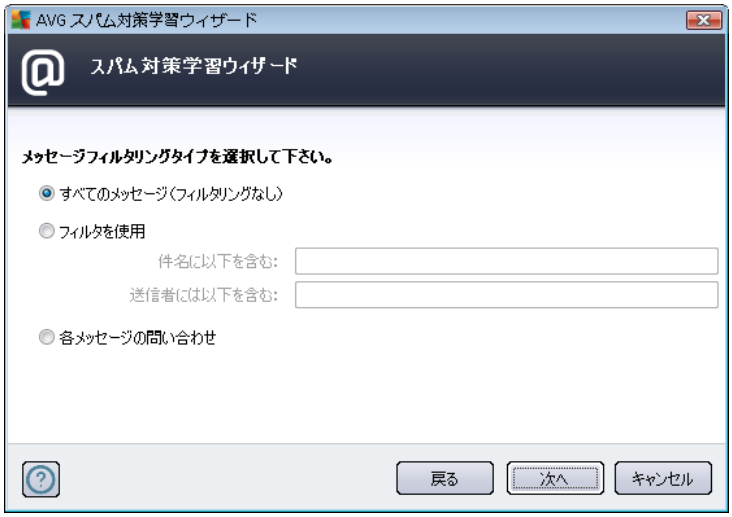


メモ: *Microsoft Office Outlook の場合、最初に Microsoft Office Outlook プロファイルを選択するように指示されます。*

フォルダには次の内容が含まれます。 ドロップダウン メニューには 2 つのオプションが表示されます。ここでは選択したフォルダが望ましい (*HAM*) メールあるいは望ましくない (*SPAM*) メールのいずれを含むかを選択します。次のステップでメッセージをフィルタリングできます。フォルダには学習メールのみを含む必要はありません。選択した電子メール クライアントのナビゲーション ツリーがダイアログのメイン セクションに表示されます。ツリー上で任意のフォルダを選択して強調表示させます。

完了したら、[***次へ***] をクリックして、[メッセージ フィルタリング オプション] に進みます。

7.3.3. メッセージ フィルタリング オプション

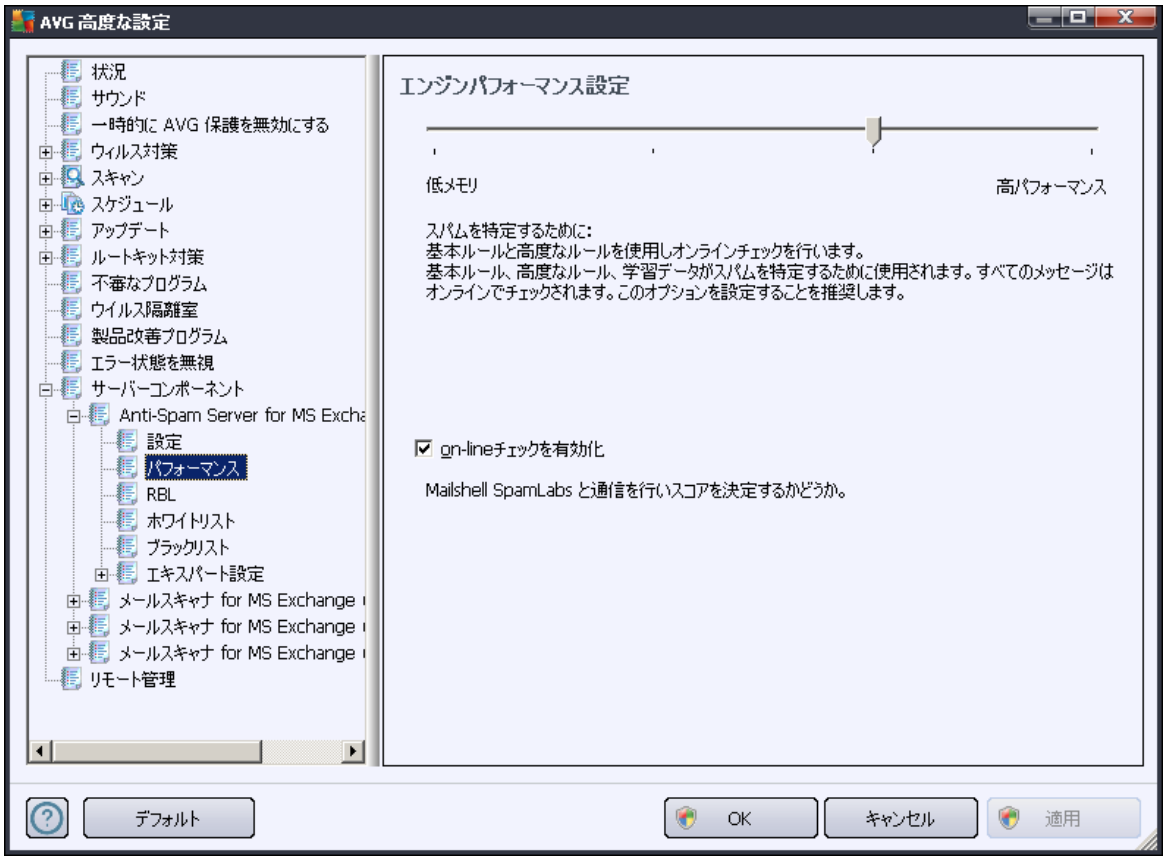


このダイアログでは、メールメッセージのフィルタリングを設定します。

- ***すべてのメッセージ (フィルタなし)*** - 選択したフォルダに学習で使用するメッセージしか含まれていないことが確実な場合は、[***すべてのメッセージ (フィルタなし)***] オプションを選択します。
- ***フィルタを使用*** - 高度なフィルタを使用する場合、[フィルタを使用] ***オプションを選択します。*** メールの件名、送信者欄で検索する場合、単語 (*名前*)、単語の一部、フレーズを入力します。入力した条件に正確に一致するメッセージすべてが学習に使用されます。プロンプトは表示されません。両方のテキスト フィールドに入力すると、2 つの条件のうちのいずれかにマッチするアドレスが使用されます。
- ***各メッセージを確認*** - フォルダに含まれるメッセージが不明で、すべてのメッセージについて確認 (*学習するかどうかを決定できるように*) する場合、[***各メッセージを確認***] オプションを選択します。

適切なオプションを選択し、[***次へ***] をクリックします。以後のダイアログは情報のみが表示され、ウィザードがメッセージを処理する準備ができていることを示します。学習を開始するには***次へ***ボタンを再度クリックします。学習は、選択された条件に応じて開始されます。

7.4. 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。

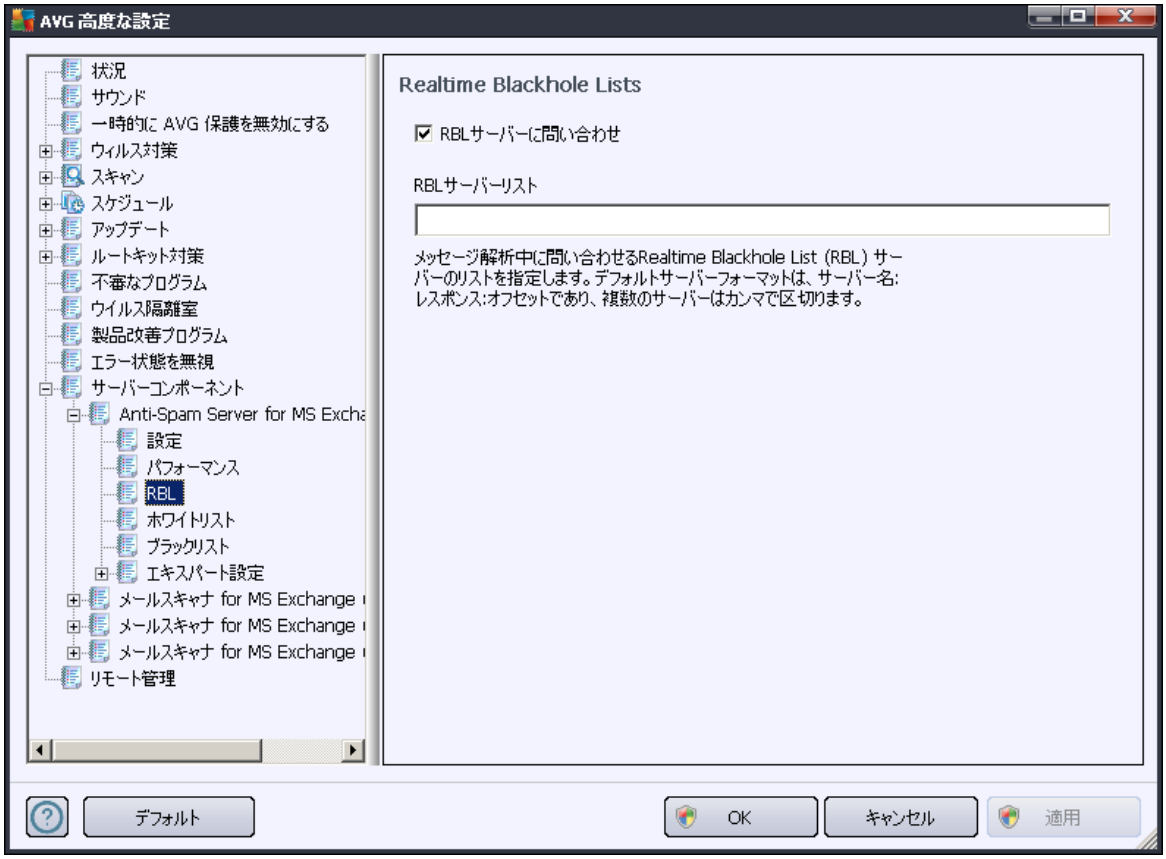
- ***低メモリ消費*** - スキャン処理でスパムを判定するときに、ルールは使用されません。学習データのみが判定に使用されます。コンピュータ ハードウェア性能が著しく低い場合などをのぞき、このモードは一般の利用には推奨されません。
- ***高パフォーマンス*** - このモードでは大量のメモリを消費します。スパム スキャン中には、ルールとスパム データベース キャッシュ、基本ルール、高度なルール、スパム送信者 IP アドレス、スパム送信者データベース機能が使用されます。

[***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。

7.5. RBL

[***RBL***] 項目をクリックすると、***リアルタイム ブラックホール リスト***と呼ばれる編集ダイアログが開きます。



このダイアログでは、[***RBL サーバーに問い合わせる***] 機能をオン/オフにすることができます。

RBL (*リアルタイム ブラックホール リスト*) サーバーは、既知のスパム送信者の拡張データベースを含む DNS サーバーです。この機能がオンの場合、すべてのメールが RBL サーバー データベースと照合され、このデータベース エントリと一致する場合には、スパムとして判定されます。

RBL サーバー データベースには最新スパム フィンガープリントが含まれ、最高レベルの最も正確なスパム検出を実現します。この機能は、特に通常のスパム対策エンジンでは検出されないような大量のスパムを受信するユーザーに適しています。

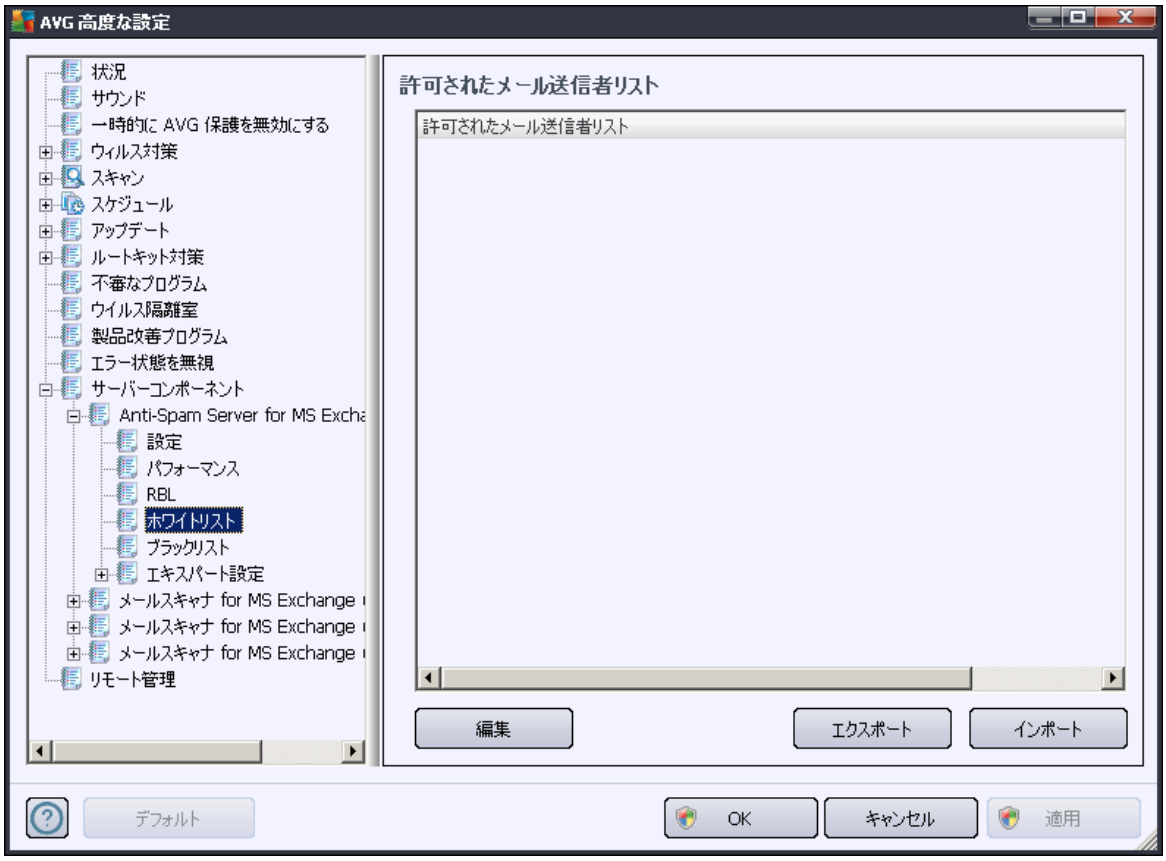
[***RBL サーバー リスト***] では、特定の RBL サーバーの場所を定義できます。既定では 2 つの RBL サーバー アドレスが指定されています。特にこの設定を変更する理由のない一般ユーザーの場合は、既定の設定を保持することをお勧めします。

***メモ**: この機能を有効にすると、各メッセージが RBL サーバー データベースと照合されるため、システム性能と設定によってはメール受信処理の速度が低下する場合があります。*

いかなる個人データもサーバーには送信されません。

7.6. 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。



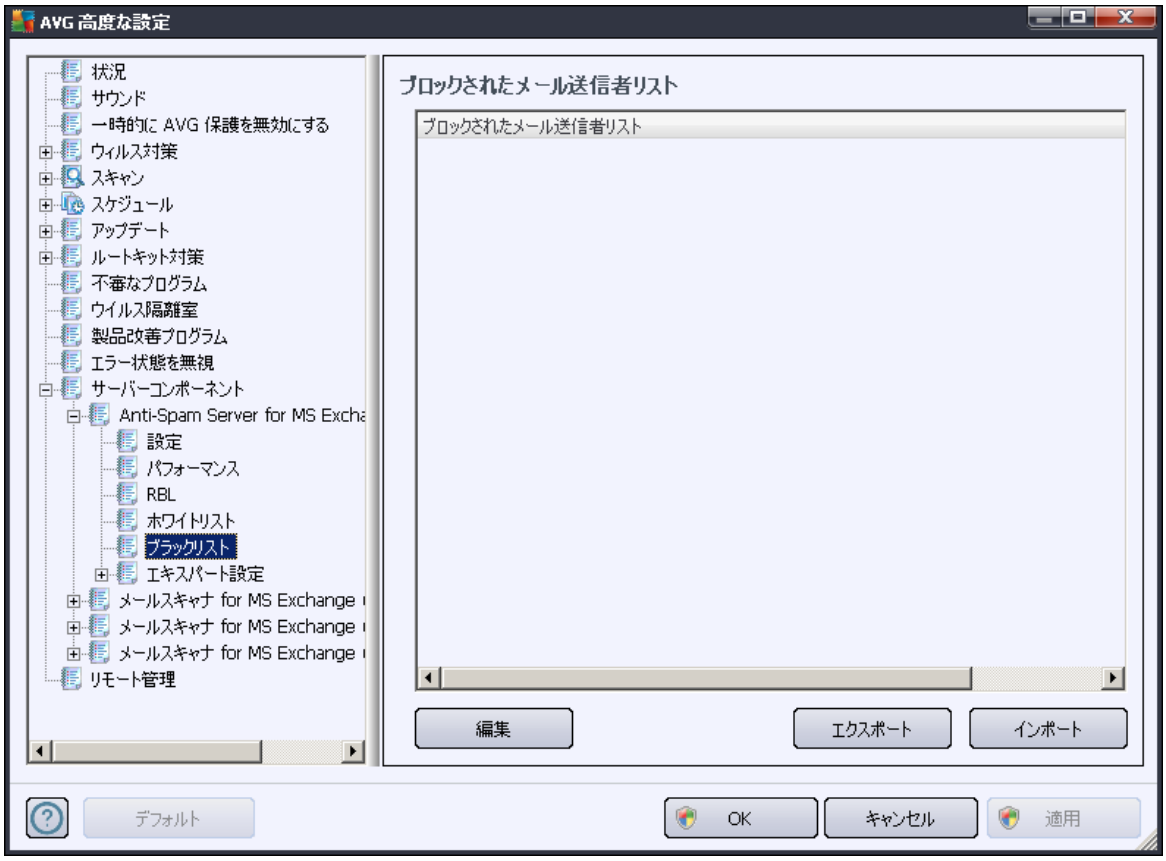
編集インターフェースでは、望ましくないメッセージ (スパム) を送信しない送信者のリストを編集できます。また、スパムメッセージが生成されないことがわかっているドメイン名 (*avg.com など*) のリストを編集できます。

既にスパム送信者やドメイン名のリストがある場合は、各メールアドレスを直接入力するか、一度にアドレスの全リスト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。

7.7. 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。リストにあるアドレスとドメインから送信されるメールはすべてスパムと見なされます。

既にスパム送信者やドメイン名のリストがある場合は、各メールアドレスを直接入力するか、一度にアドレスの全リスト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。

7.8. エキスパート設定

通常はデフォルト設定を保持し、合理的な理由がある場合にのみ設定を変更することを推奨します。この設定の変更は経験のあるユーザーのみが行ってください。

スパム対策の設定をエキスパートレベルで変更するやむを得ない事情がある場合は、直接ユーザーインターフェースの指示に従ってください。一般的には、各ダイアログでは 1 つの特定の機能の確認と編集ができます。その説明は常にダイアログに表示されます。

- ***キャッシュ*** - フィンガープリント、ドメインレピュテーション、LegitRepute
- ***トレーニング*** - 最大ワードエントリ、自動学習しきい値、重み
- ***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

8. AVG 設定マネージャ

AVG 設定マネージャは主に、AVG 設定をコピー、編集、配布ができる小規模ネットワークに適したツールです。設定をポータブル デバイス (USB フラッシュ ドライバなど) に保存して、選択したステーションに手動で適用できます。

ツールは AVG インストールに含まれており、Windows の [スタート] メニューから利用可能です。

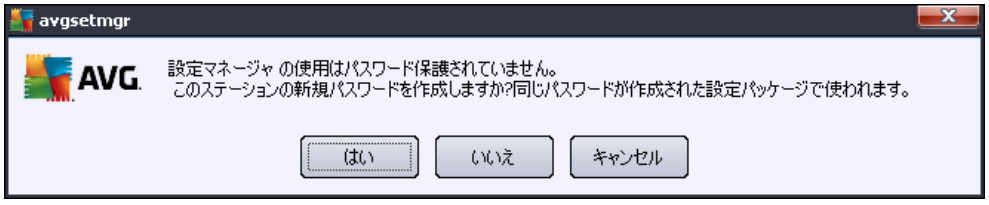
すべてのプログラム/AVG 2012/AVG 設定マネージャ

- **AVG 設定**
    - ***AVG 設定の編集*** - このリンクを使用すると、ローカル AVG の高度な設定ダイアログを開きます。ここで行われたすべての変更は、ローカル AVG インストールにも反映されます。
    - ***AVG 設定のロードと編集*** - 既に AVG 設定ファイル (.pck) がある場合は、このボタンを使用してファイルを開き、編集します。[***OK***] または [***適用***]ボタンをクリックして変更を確定すると、ファイルは新しい設定に置き換えられます。
- **AVG ファイアウォール設定**

    このセクションでは、ローカル AVG インストールのファイアウォール設定の変更や、既に準備されている AVG 設定ファイル (.pck) のファイアウォール設定の変更ができます。ただし、AVG Email Server Edition 2012 にファイアウォール コンポーネントが含まれない場合、リンクがグレイ表示されて機能しなくなります。
- **ロード オプション**
    - ***保存した設定を AVG にロード*** - このリンクを使用すると、AVG 設定ファイル (.pck) が開き、AVG のローカル インストールに適用されます。

- **保存オプション**

  - ***ローカル AVG 設定をファイルに保存*** - このリンクを使用すると、ローカル AVG インストールの AVG 設定ファイルを保存します。[許可されたアクション] にパスワードを設定しなかった場合は、次のダイアログが表示されることがあります。



  許可された項目へのアクセスにパスワードを設定する場合は、[***はい***] をクリックして必要な項目に情報を入力してから入力内容を確認します。パスワードの作成をスキップし、ローカル AVG 設定をファイルに保存する場合は [***いいえ***] をクリックします。

- **コピー オプション**

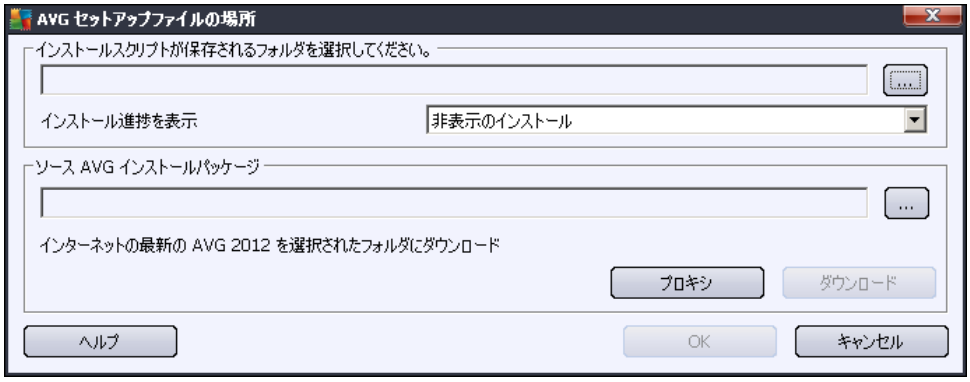
  - ***同じ設定をネットワーク全体に適用*** - このリンクをクリックすると、カスタム オプションでインストール パッケージを作成し、ローカル AVG のコピーを作成できます。クローンには、次の設定を除くほとんどの AVG 設定を含めることができます。

    ✓ *言語設定*

    ✓ *サウンド設定*

    ✓ *個人情報保護コンポーネントの許可されたリストと不審なプログラム例外*

  実行するには、まずインストール スクリプトを保存するフォルダを選択します。



  次に、ドロップダウン メニューから次のいずれかを選択します。

  ✓ *インストールを表示しない* - セットアップ処理中は情報が一切表示されません。

  ✓ *インストールの進行状況のみを表示する* - インストール中にユーザー操作は必要はありません。進行状況のみが表示されます。

✓ *インストール ウィザードを表示する*-インストール ステップが表示され、ユーザーはすべてのステップを手動で確定する必要があります。

[***ダウンロード***] ボタンをクリックして、最新の AVG インストール パッケージを AVG Web サイトから選択しフォルダに直接ダウンロードするか、AVG インストール パッケージを手動でフォルダに保存します。

プロキシ サーバーを設定してネットワーク接続する必要がある場合は、[***プロキシ***] ボタンをクリックしてプロキシ サーバーを定義できます。

[***OK***] ボタンをクリックすると、コピー処理が開始され、短時間で完了します。許可された項目 (前述の説明を参照) の設定パスワードを確認するダイアログが表示される場合があります。完了すると、***AvgSetup.bat*** が選択したフォルダに保存され、その他のファイルとともに利用可能になります。***AvgSet.bat*** ファイルを実行すると、前の手順で選択したパラメータに基づいて AVG がインストールされます。

9. 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。

