AVG Anti- Virus 2012

User Manual

Document revision 2012.01 (27.7.2011)

Contents

1. はじめに

このユーザー マニュアルは、**AVG Anti-Virus 2012** の包括的なマニュアルです。

AVG Anti-Virus 2012 は複数の保護機能を備え、あらゆるオンライン活動からユーザーを守ります。ユーザーは ID 窃盗、ウイルス、有害なサイトへのアクセスについて心配せずにすみます。AVG 保護クラウド技術とAVG コミュニティ保護ネットワークが導入されています。この機能では、AVG が最新の脅威情報を収集し、その情報をコミュニティで共有することで、最高レベルの保護を提供します。

- AVG ファイアウォール、スパム対策、Identity Protection による安全なオンライン ショッピングとバンキング
- AVG ソーシャル ネットワーク保護によるソーシャル ネットワーク サイトでの継続的な保護
- リンクスキャナのリアルタイム保護による安心できる Web 閲覧と検索

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 Anti-Virus 2012 は、次のオペレーティング システムで稼動するワークステーションの保護を目的としています。

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 および x64、すべてのエディション)
- Windows 7 (x86 および x64、すべてのエディション)

(また、特定のオペレーティングシステム用サービスパック)

メモ: *個人情報保護コンポーネントは Windows XP x64 ではサポートされていません。これらのオペレーティング システムでは、AVG Anti-Virus 2012 のインストールはできますが、個人情報保護コンポーネントのインストールはできません。*

2.2. 最低および推奨ハードウェア要件

AVG Anti-Virus 2012 の最低ハードウェア要件:

- Intel Pentium CPU 1,5 GHz
- 512 MB の RAM メモリ
- 1000 MB のディスク空き領域 (インストールのため)

AVG Anti-Virus 2012 の推奨ハードウェア要件:

- Intel Pentium CPU 1,8 GHz
- 512 MB の RAM メモリ
- 1550 MB のディスク空き領域 (インストールのため)

3. AVG インストール処理

インストール ファイルが保存されている場所

コンピュータにAVG Anti-Virus 2012 をインストールする場合は、最新のインストール ファイルを取得する必要があります。最新バージョンの AVG Anti-Virus 2012 を確実にインストールするために、AVG Web サイト (http://www.avg.com/) からインストール ファイルをダウンロードすることをお勧めします。[***サポート センター/ダウンロード***] セクションには、各 AVG 製品のインストール ファイルの概要が構造化された形式で表示されます。

ダウンロードしてインストールするファイルがわからない場合は、Web ページ下部の [***製品の選択***] サービスを使用できます。3 つの簡単な質問に回答すると、必要なファイルが正確に定義されます。[***続行***] ボタンをクリックすると、ユーザーのニーズに合わせてカスタマイズされたダウンロード ファイル一覧に移動します。

インストール処理の概要

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、インストール処理を実行することができます。インストールは一連のシンプルでわかりやすいダイアログから構成されています。各ダイアログではインストール処理の各ステップの概要を説明しています。各ダイアログ ウィンドウの詳細については次のとおりです。

3.1. ようこそ

インストール処理の最初のウィンドウは、[***AVG インストーラへようこそ***] ダイアログです。

インストール言語を選択

このダイアログではインストール処理で使用する言語を選択できます。ダイアログの右端のコンボボックスをクリックすると、言語メニューがロールダウンします。任意の言語を選択すると、選択した言語でインストール処理が続行します。

注意: この時点では、インストール処理の言語のみを選択しています。AVG Anti-Virus 2012 アプリケーションは選択した言語でインストールされます。英語は必ず自動的にインストールされます。ただし、その他の言語をインストールして、AVG Anti-Virus 2012 で使用することもできます。次の [カスタム オプション] 設定ダイアログの 1 つでは、別の言語を選択できます。

ライセンス契約

さらに、[***AVG インストーラへようこそ***] ダイアログでは、AVG ライセンス契約の全文が表示されます。よくお読みください。全文をよく読み、内容を理解した上で、この使用許諾契約に同意する場合は、[***同意する***] ボタンをクリックします。使用許諾契約に同意しない場合は、[***同意しない***] ボタンをクリックします。インストール処理がただちに中断されます。

AVG プライバシー ポリシー

ライセンス契約の他に、このセットアップ ダイアログでは AVG プライバシー ポリシーの詳細も確認できます。ダイアログの左下端には [***AVG プライバシー ポリシー***] リンクが表示されます。このリンクをクリックすると、AVG Web サイト (http://www.avg.com/) に移動し、AVG Technologies のプライバシー ポリシー規定の全文を確認できます。

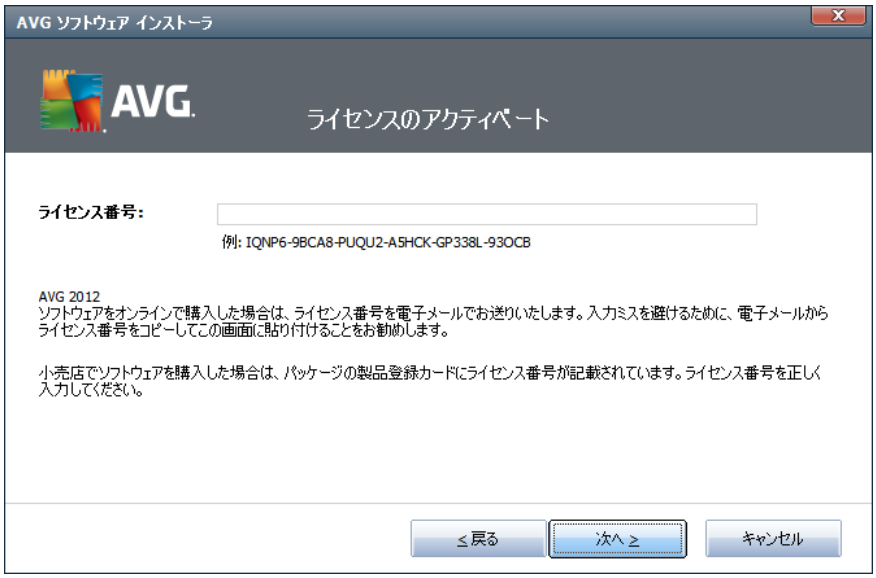
コントロール ボタン

最初のセットアップ ダイアログでは 2 つのコントロール ボタンのみが利用できます。

- ***同意*** - クリックすると、ライセンス契約を読んで理解して同意したことを確認します。インストールは続行され、次のセットアップ ダイアログに進みます。
- ***拒否*** - クリックすると、ライセンス契約を拒否します。セットアップ処理はただちに終了します。**AVG Anti-Virus 2012** はインストールされません!

3.2. ライセンスをアクティベート

[***ライセンスのアクティベート***] ダイアログでは、指定されたテキスト フィールドにライセンス番号を入力するように指示されます。



どこでライセンス番号を見つけることができますか

セールス番号は、**AVG Anti-Virus 2012** ボックスの CD パッケージに記載されています。ライセンス番号は**AVG Anti-Virus 2012**をオンラインで購入後に受信す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してください。デジタル形式のライセンス番号が利用できる (*メールで*) 場合は、コピーとペーストを使用して、それを入力することを推奨します。

コピーと貼り付け機能を使用する方法

コピーと貼り付け機能を使用して **AVG Anti-Virus 2012** ライセンス番号をプログラムに入力することで、番号を確実に正しく入力できます。次の手順を実行してください。

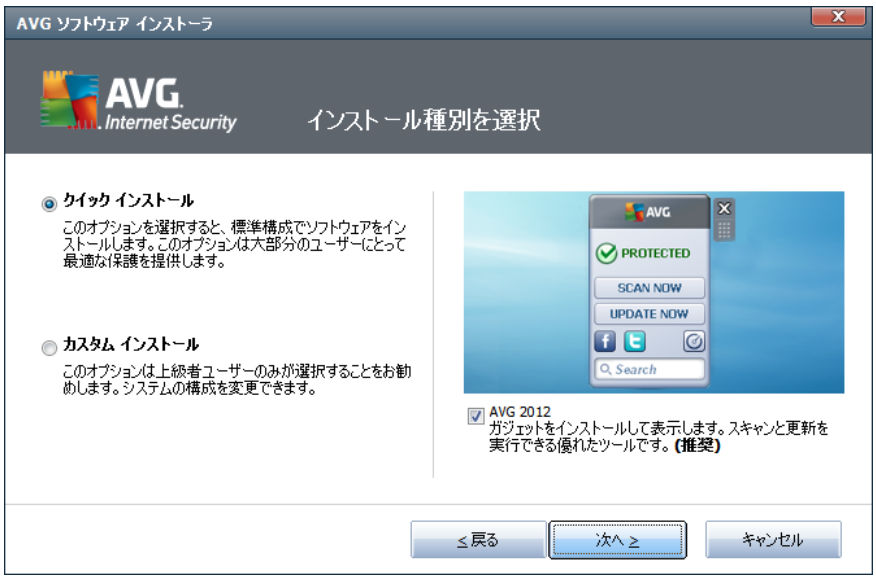
- ライセンス番号が記載されているメールを開きます。
- ライセンス番号の先頭をクリックして番号の末尾までドラッグしたところでボタンを放します。番号が強調表示されるはずです。
- ***Ctrl*** キーを押しながら***C*** キーを押します。番号がコピーされます。
- コピーした番号を貼り付ける場所をポイント・アンド・クリックします。
- ***Ctrl*** キーを押しながら***V*** キーを押します。選択した場所に番号が貼り付けられます。

コントロール ボタン

通常のセットアップ ダイアログと同様に、3 つのコントロール ボタンがあります。

- ***戻る*** - クリックすると、1 つ前のセットアップ ダイアログに戻ります。
- ***次へ*** - クリックすると、インストールを続行し、1 つ次のステップに進みます。
- ***キャンセル*** - クリックすると、ただちにセットアップ処理を中止します。**AVG Anti-Virus 2012**はインストールされません。

3.3. インストール種別の選択



インストール種別

[***インストール種別の選択***] 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、標準の [クイック インストール] オプションを保持し、プログラム ベンダーが事前定義した設定を使用して**AVG Anti-Virus 2012** を完全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。将来的には、設定の変更の必要が生じた場合、常に **AVG Anti-Virus 2012** アプリケーションで直接変更できます。[***クイック インストール***] オプションを選択した場合は、[***次へ***] ボタンをクリックして、次の [AVG セキュリティツールバーのインストール] ダイアログに進みます。

カスタム インストールは、**AVG Anti-Virus 2012** 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)。このオプションを選択したら、[***次へ***] ボタンをクリックして、[カスタム オプション] に進みます。

AVG ガジェットのインストール

ダイアログの右側のセクションには AVG ガジェット (*Windows Vista/Windows 7 で対応*) 関連のチェックボックスが表示されます。このガジェットをインストールする場合は、該当するチェックボックスを選択します。AVG ガジェットには Windows サイドバーからアクセスでき、スキャンや更新など **AVG Anti-Virus 2012** の最も重要な機能を簡単に実行できます。

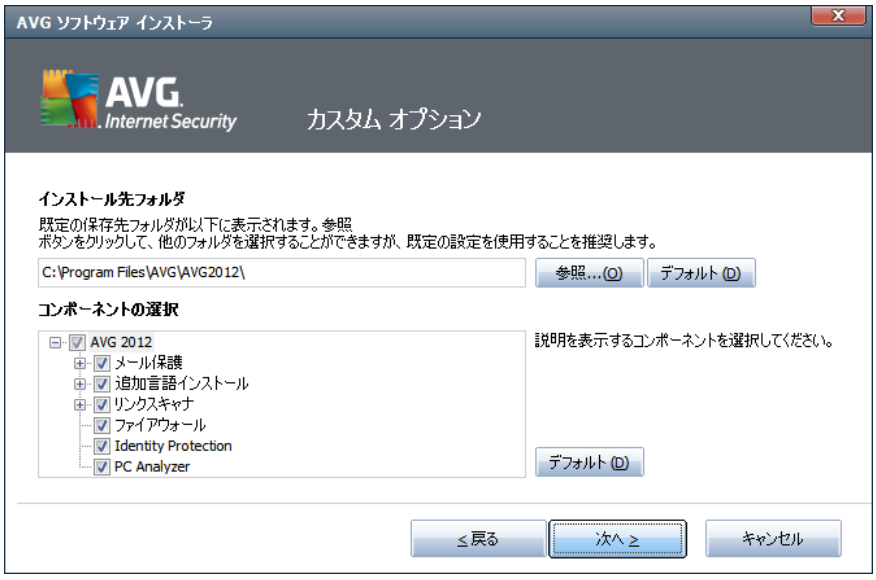
コントロール ボタン

通常のセットアップ ダイアログと同様に、3 つのコントロール ボタンがあります。

- ***戻る*** - クリックすると、1 つ前のセットアップ ダイアログに戻ります。
- ***次へ*** - クリックすると、インストールを続行し、1 つ次のステップに進みます。
- ***キャンセル*** - クリックすると、ただちにセットアップ処理を中止します。**AVG Anti-Virus 2012**はインストールされません。

3.4. カスタム オプション

[***カスタム オプション***] ダイアログでは 2 つのインストール パラメータを設定できます。



インストール先 フォルダ

ダイアログの [***インストール先 フォルダ***] セクションでは、**AVG Anti-Virus 2012** のインストール場所を指定します。既定では、**AVG Anti-Virus 2012** 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。

コンポーネントの選択

[***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 Anti-Virus 2012** 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 製品に含まれるコンポーネントのみです。

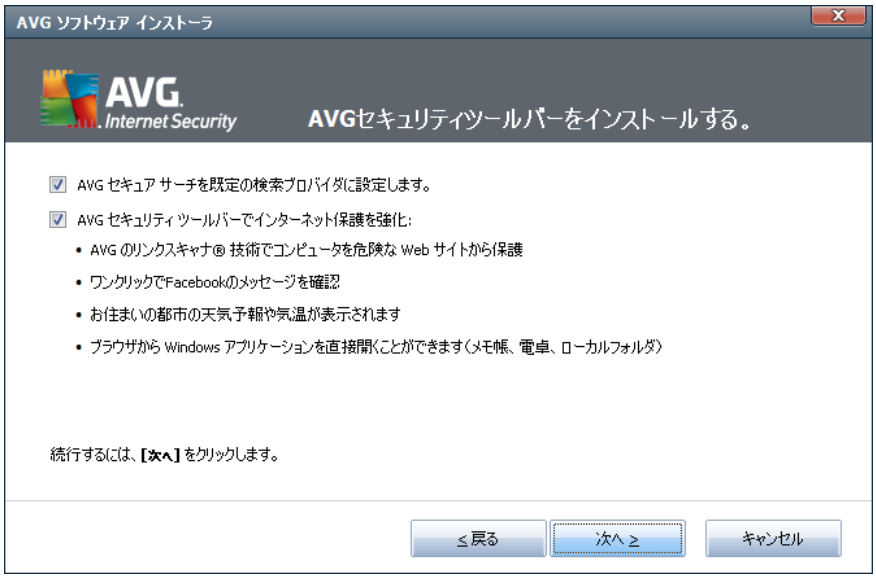
[***コンポーネント選択***] リストの項目を強調表示すると、該当するコンポーネントの簡単な説明がこのセクションの右側に表示されます。各コンポーネントの機能に関する詳細については、このマニュアルの「コンポーネント概要」の章を参照してください。ソフトウェアベンダーが事前設定した既定の設定に戻すには、[***既定***] ボタンをクリックします。

コントロール ボタン

通常のセットアップダイアログと同様に、3 つのコントロール ボタンがあります。

- ***戻る*** - クリックすると、1 つ前のセットアップ ダイアログに戻ります。
- ***次へ*** - クリックすると、インストールを続行し、1 つ次のステップに進みます。
- ***キャンセル*** - クリックすると、ただちにセットアップ処理を中止します。**AVG Anti-Virus 2012**はインストールされません。

3.5. AVG セキュリティツールバー のインストール



[***AVG セキュリティツールバー のインストール***] ダイアログでは、セキュリティツールバー機能をインストールするかどうかを決定します。既定の設定を変更しない場合は、このコンポーネントはインターネットブラウザに自動的にインストールされ (*現在サポートされているブラウザは Microsoft Internet Explorer v.*

6.0 以上 および Mozilla Firefox v. 3.0 以上)、インターネット閲覧中の包括的オンライン保護を提供します。

また、既定の検索プロバイダとして *AVG Secure Search (powered by Google)* を選択するかどうかを決定できます。この場合は、該当するチェックボックスを選択します。

3.6. インストールの進行状況

[***インストールの進行状況***] ダイアログにはインストール処理の進行状況が表示されます。ユーザー操作は必要ありません。

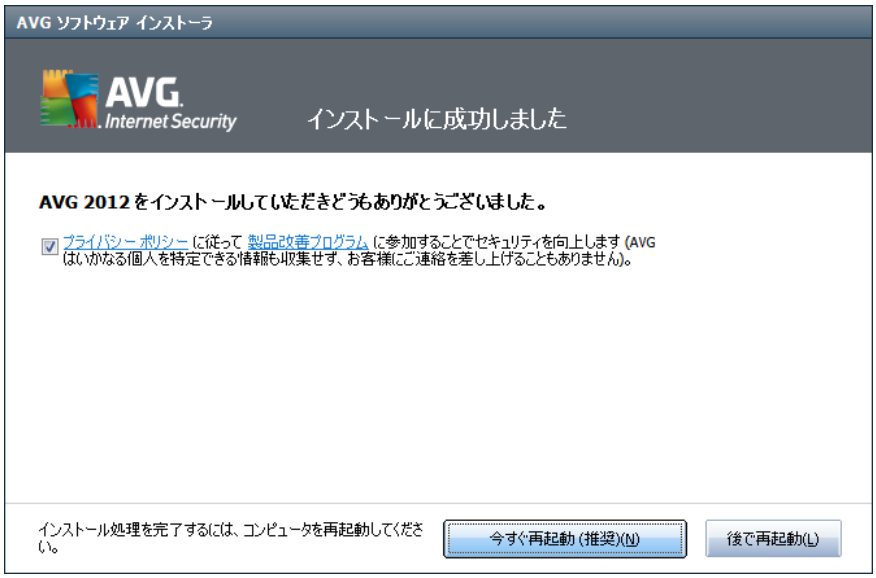
インストール処理の終了後、次のダイアログに自動的に進みます。

コントロール ボタン

このダイアログには [***キャンセル***] ボタンしかありません。このボタンを使用するのは、実行中のインストール処理を停止する場合のみです。キャンセルすると、**AVG Anti-Virus 2012** はインストールされません。

3.7. インストールに成功しました

[***インストールに成功しました***] ダイアログでは、**AVG Anti-Virus 2012** が正常にインストールおよび設定されたことを確認できます。



製品改善プログラム

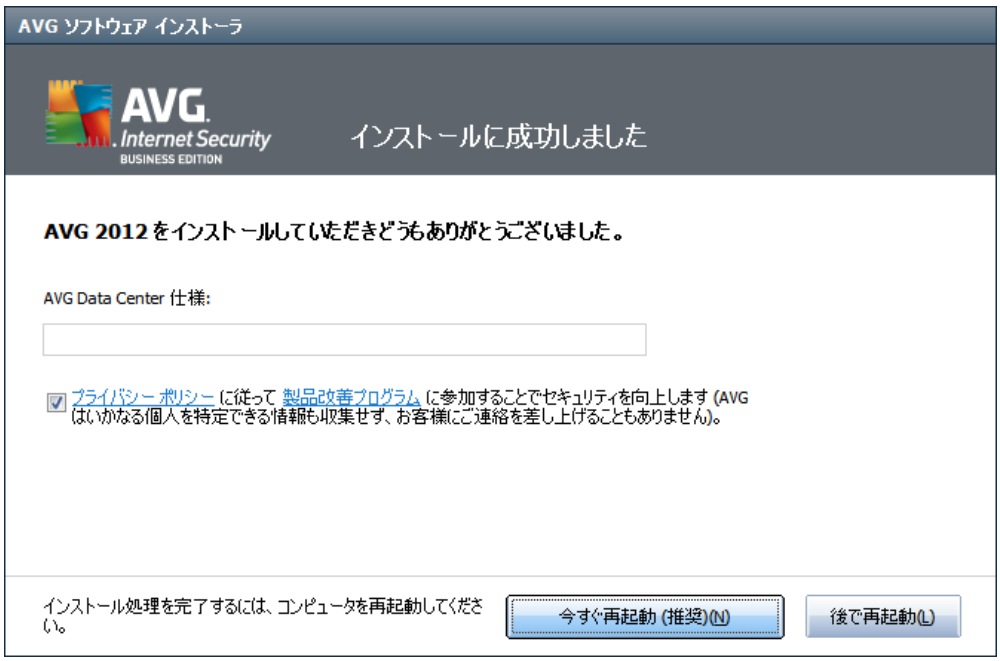
このダイアログでは、製品改善プログラム (*詳細については、AVG 高度な設定/製品改善プログラム*を参照) に参加するかどうかを決定します。このプログラムでは、全体的なインターネット セキュリティレベルを高める目的で、検出された脅威に関する匿名の情報を収集します。この内容に同意する場合は、[***AVG 2012 Web 安全および製品改善プログラムに同意して参加する...***] オプションを選択してください *(既定ではこのオプションが選択されています)*。

コンピュータの再起動

インストール処理を完了するには、コンピュータの再起動が必要です。[***今すぐ再起動***] をクリックするか、[***後で再起動***] をクリックして再起動処理を延期します。

ビジネス ライセンスのインストール

AVG ビジネス版 ライセンスを使用し、リモート管理 コンポーネントのインストール *(カスタム オプション) を参照)* を選択した場合は、次のインターフェースで [インストールに成功しました] ダイアログが表示されます。



AVG DataCenter パラメータを指定する必要があります。 「サーバー:ポート」の形式で AVG DataCenter への接続文字列を入力してください。この時点でこの情報がない場合は、このフィールドを空白にしておくと、後から [高度な設定/リモート管理] ダイアログで設定できます。AVG リモート管理の詳細については、AVG Business Edition ユーザー マニュアルを参照してください。このマニュアルは、AVG Web サイト (http://www.avg.com/) からダウンロードできます。

このマニュアルの「コンポーネント概要」の章を参照してください。ソフトウェア ベンダーが事前設定した既定の設定に戻すには、[***既定***] ボタンをクリックします。

コントロール ボタン

このダイアログでは、次のコントロール ボタンを利用できます。

- ***今すぐ再起動 (推奨)*** - **AVG Anti-Virus 2012**のインストール処理を完了するには再起動が必要です。コンピュータをただちに再起動することをお勧めします。再起動後にのみ**AVG Anti-Virus 2012**が完全にインストールされ、ユーザーが保護された安全な状態になります。
- ***後で再起動*** - 何らかの理由によりコンピュータをすぐに再起動できない場合は、処理を延期できます。ただし、ただちに再起動することをお勧めします。再起動後にのみ、コンピュータは**AVG Anti-Virus 2012**によって完全に保護されます。

4. インストール後

4.1. 製品登録

AVG Anti-Virus 2012 のインストールが完了したら、AVG Web サイト (http://www.avg.com/) でオンライン製品登録を行ってください。登録後、AVG ユーザー アカウント、AVG アップデート ニュースレター、その他登録ユーザーのみに提供されるサービスが利用できるようになります。

最も簡単な登録方法は、AVG Anti-Virus 2012 **ユーザー インターフェース**から直接行う方法です。メイン メニューで [ヘルプ/今すぐ登録] 項目を選択してください。AVG Web サイト (http://www.avg.com/) の [***登録***] ページに移動します。ページの指示に従ってください。

4.2. ユーザー インターフェースへのアクセス

AVG メイン ダイアログには複数の方法でアクセスできます。

- AVG システム トレイ アイコン
- デスクトップの AVG アイコンをダブルクリックします。
- AVG ガジェット (*インストールされている場合。Windows Vista/ Windows 7 に対応*)
- メニューから ***[スタート/すべてのプログラム/AVG 2012/AVG ユーザー インターフェース] の順に選択します。***

4.3. 完全コンピュータ スキャン

AVG Anti-Virus 2012インストール前にウイルスが感染している可能性あります。このため、全コンピュータをスキャンを実行して、PCが感染していないことを確認してください。

全コンピュータをスキャンを実行する方法については、AVGスキャンの章を参照してください。

4.4. Eicar 検査

AVG Anti-Virus 2012 が正常にインストールされたことを確認するために、EICAR テストを実行できます。

EICARテストは、ウイルス対策システムの機能をテストするために使用される、標準的で完全に安全な方法です。これは実際のウイルスではなく、危険なコードを一切含まないため、万一検出されなくてもコンピュータが危険にさらされることはありません。ほとんどの製品は、これがあたかもウイルスであるかのように反応します（*「EICAR-AV-Test」のような明確な名称で報告されます。*）。EICARのWebサイトwww.eicar.comでEICARウイルスをダウンロードすることができ、また、そこですべての必要なEICARテスト情報も入手できます。

eicar.comファイルをダウンロードし、それをローカルディスクに保存します。検査ファイルのダウンロードを確認するとただちに、オンライン シールド (*リンクスキャナ コンポーネントの一部*) によって警告が表示されます。この通知は、AVG が正常にコンピュータにインストールされていることを証明します。

http://www.eicar.com ウェブサイトから、圧縮された (*eicar_com.zip 形式*) EICAR ウィルスをダウンロードすることもできます。オンライン シールドでこのファイルのダウンロードを許可し、ローカル ディスクに保存できますが、解凍しようとすると常駐シールド (*ウイルス対策 コンポーネント*) がウィルスを検出します。

AVGがEICARテストファイルをウイルスとして特定できない場合、プログラム設定を再度確認する必要があります。

4.5. AVG の既定の設定

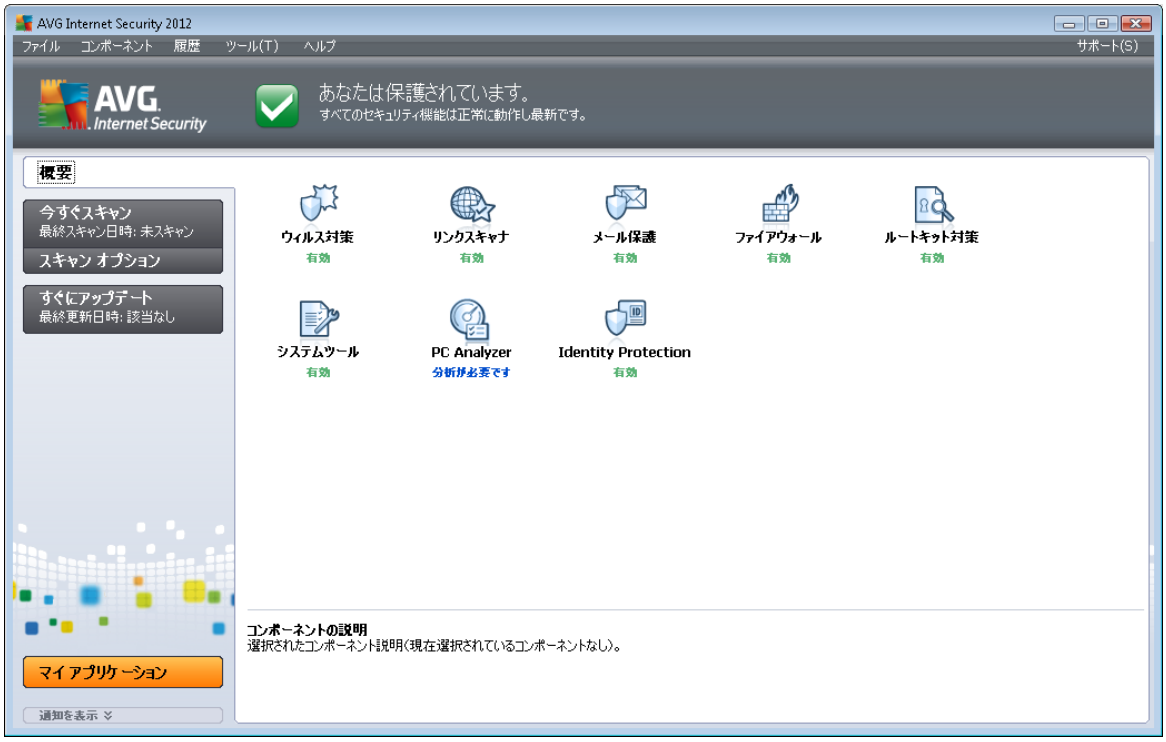
のデフォルト設定 (*アプリケーションがインストール後に正しく動作するための初期設定*) **AVG Anti-Virus 2012** では、すべてのコンポーネントと機能が最適なパフォーマンスで動作するよう設定されています。

特に理由がない場合、AVGの設定を変更しないでください。設定に対するいかなる変更も、経験者ユーザーのみが行うようにして下さい。

AVGコンポーネントの基本的な設定は、各コンポーネントのユーザーインターフェースから直接変更することができます。AVG設定を変更する必要がある場合、AVG高度な設定を使用します。システムメニューアイテム***ツール/高度な設定***を選択し、AVG高度な設定ダイアログでAVG設定を変更します。

5. AVG ユーザー インターフェース

AVG Anti-Virus 2012 メイン ウィンドウが開 きます。



メインウィンドウは複数のセクションに分けられます。

- ***システム メニュー*** *(ウィンドウ上のシステム ライン)* は標準ナビゲーションであり、**AVG Anti-Virus 2012** のすべてのコンポーネント、サービス、機能にアクセスできます - 詳細 >>
- ***セキュリティステータス情報*** *(ウィンドウ上部のセクション)* には、**AVG Anti-Virus 2012** の最新ステータスが表示されます - 詳細 >>
- ***クイック リンク*** *(ウィンドウの左のセクション)* では、最も重要で最も頻繁に使用される**AVG Anti-Virus 2012**のタスクに簡単にアクセスできます - 詳細 >>
- ***マイ アプリケーション*** *(ウィンドウの左下のセクション)* には **AVG Anti-Virus 2012** で利用できる LiveKive、Family Safety、PC チューンアップ
- ***コンポーネント概要*** *(ウィンドウ中央部)* は、インストールされた**AVG Anti-Virus 2012**コンポーネントの概要が表示されます - 詳細 >>
- ***システム トレイ アイコン*** *(モニター右下端のシステム トレイ)* には**AVG Anti-Virus 2012**の最新ステータスが表示されます - 詳細 >>
- ***AVG ガジェット*** *(ウィンドウ サイドバー。Windows Vista/7 で対応)* を使用すると、**AVG Anti-Virus 2012**のスキャンと更新に簡単にアクセスできます - 詳細 >>

5.1. システム メニュー

システムメニューは、すべてのWindowsアプリケーションで使用される標準のナビゲーションです。**AVG Anti-Virus 2012** メイン ウィンドウの最上部に横方向に表示されます。システムメニューを使用して、AVGの各コンポーネント、機能、サービスにアクセスします。

システムメニューは5つの主要なセクションにわかれています。

5.1.1. ファイル

- ***終了*** - **AVG Anti-Virus 2012**のユーザーインターフェースを閉じます。ただし、AVGアプリケーションはバックグラウンドで実行され、コンピュータは保護されます。

5.1.2. コンポーネント

システム メニューのコンポーネントには、インストールされたすべての AVG コンポーネントへのリンクが表示されます。リンクをクリックすると、各コンポーネントの既定のダイアログ ページが表示されます。

- ***システム概要*** - インストールされたすべてのコンポーネントとそのステータスの概要を表示します。
- ***ウイルス対策***はシステム内のウイルス、スパイウェア、ワーム、トロイの木馬、望ましくない実行ファイルまたはライブラリを検出し、悪意のあるアドウェアからユーザーを保護します - 詳細 >>
- ***リンクスキャナ***はインターネット検索や閲覧中に Web ベースの攻撃からユーザーを保護します - 詳細 >>
- ***メール保護***は受信 電子メール メッセージにスパム メールがあるかどうかをチェックし、ウイルス、フィッシング攻撃、その他の脅威をブロックします - 詳細 >>
- ***ファイアウォール***は各ネットワーク ポートのすべての通信を制御し、悪意のある攻撃からユーザーを保護し、侵入の試みをすべてブロックします - 詳細 >>
- ***ルートキット対策***はアプリケーション、ドライバ、ライブラリに隠れている危険なルートキットをスキャンします - 詳細 >>
- ***システム ツール***は、AVG 環境の詳細な概要とオペレーティング システム情報を提供します。 - 詳細 >>
- ***PC Analyzer***は、コンピュータ ステータスに関する情報を提供します。 - 詳細 >>
- ***Identity Protection*** はデジタル資産を新しい未知の脅威から継続的に保護します - 詳細 >>
- ***セキュリティ ツールバー***をインストールすると、選択した AVG の機能をインターネットから直接利用できます。 - 詳細 >>
- ***リモート管理***は AVG Business Edition でのみ表示されます。インストール処理中にこのコンポーネントのインストールを指定した場合に限ります。

5.1.3. 履歴

- スキャン結果 - AVGスキャンインターフェースのスキャン結果概要ダイアログを表示します。
- 常駐シールド検出 - 常駐シールドによって検出された脅威の概要ダイアログを開きます。
- メール スキャナ検出 - メール保護コンポーネントによって検出されたメールの概要ダイアログを開きます。
- オンライン シールド検出 - リンクスキャナ コンポーネントのオンライン シールド サービスによって検出された脅威の概要ダイアログを開きます。
- ウイルス隔離室 - 隔離スペース (ウイルス隔離室) インターフェースを開きます。AVGは、検出、または何らかの理由で自動修復できなかったすべての感染をここに移動します。隔離室内では、感染ファイルは隔離され、コンピュータの安全は保証されます。同時に感染ファイルは将来の修復に備えて保存されます。
- イベント履歴ログ - すべてのログに記録された**AVG Anti-Virus 2012**アクションの概要履歴インターフェースを開きます。
- ファイアウォール - すべてのファイアウォールアクションに関する詳細概要が表示されている [ログ] タブのファイアウォール設定インターフェースを開きます。

5.1.4. ツール

- コンピュータ スキャン - AVG スキャン インターフェースに切り替わり、スキャンを実行します。
- 特定フォルダのスキャン - AVG スキャン インターフェースに切り替わり、スキャンするファイルとフォルダを設定できます。
- ファイル スキャン - 特定のファイルを指定してスキャンを実行することができます。
- アップデート - 自動的に**AVG Anti-Virus 2012**の更新処理を実行します。
- ***ディレクトリからの更新*** - ローカル ディスクで指定したフォルダの更新ファイルを使用して更新処理を実行します。ただし、このオプションは緊急時にのみ推奨されます。たとえば、インターネットに接続できない場合 (*コンピュータが感染し、インターネットから切断されている状況など。コンピュータはネットワークに接続されているがインターネットアクセスがない場合など*) などです。フォルダの参照ウィンドウで、更新ファイルを保存したフォルダを選択し、更新処理を実行します。
- 高度な設定... - [AVG 高度な設定] ダイアログを開きます。ここではAVG Anti-Virus 2012各項目の設定を編集できます。通常はソフトウェア ベンダーが定義している既定のアプリケーション設定の使用をお勧めします。
- ファイアウォール設定 - ファイアウォールコンポーネントの高度な設定ダイアログを開きます。

5.1.5. ヘルプ

- ***目次*** - AVG ヘルプ ファイルが開きます。
- ***オンラインヘルプ*** - AVG Webサイト (http://www.avg.com/) のカスタマー サポート センター ペー

ジを開きます。

- ***AVG Web*** - AVG Web サイト（http://www.avg.com/）を開きます。
- ***ウイルスと脅威について*** - オンラインのウイルス エンサイクロペディアが開きます。ここでは、検出されたウイルスに関する詳細情報を検索できます。
- ***再アクティベート*** - ***インストール処理*** の [AVG のパーソナライズ] ダイアログで入力したデータが [AVG のアクティベート] ダイアログに表示されます。このダイアログではライセンス番号を入力してセールス番号（*AVG をインストールしたときの番号*）を置き換えたり、古いライセンス番号（*新しい AVG 製品にアップグレードした場合など*）を置き換えたりできます。
- ***今すぐ登録*** - AVG Web サイト（http://www.avg.com/）の登録ページに接続します。登録データを入力してください。AVG 製品を登録したお客様のみが無料テクニカル サポートをご利用いただけます。

メモ **AVG Anti-Virus 2012** *の試用版を使用している場合は、最後の 2 つの項目が [****今すぐ購入****] および [****アクティベート****] として表示され、完全バージョンの製品をすぐに購入できます。セールス番号でインストールされている* **AVG Anti-Virus 2012** *の場合、[****登録****] および [****アクティベート****] として表示されます。*

- ***AVG について*** - ***情報*** ダイアログを開きます。このダイアログでは、プログラム名、プログラムとウイルス データベース バージョン、システム情報、ライセンス契約、***AVG Technologies CZ*** の問い合わせ先情報を確認できます。

5.1.6. サポート

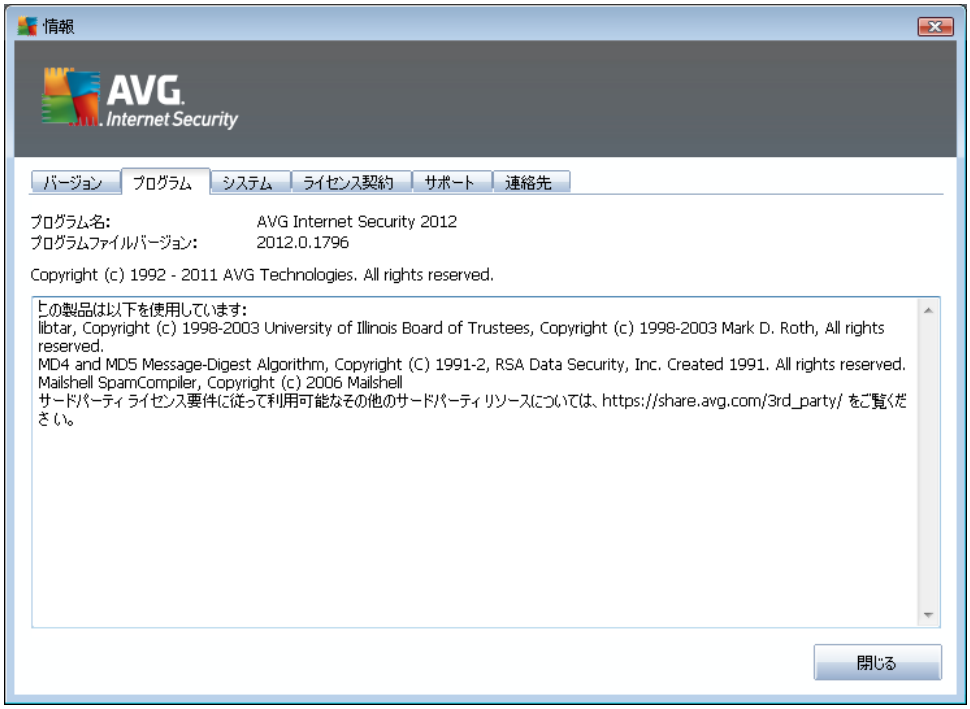
[***サポート***] リンクをクリックすると、新しい [***情報***] ダイアログが開き、ヘルプの検索時に必要になると思われるあらゆる種類の情報が表示されます。このダイアログにはインストールされている AVG プログラムに関する基本データ（*プログラム/データベース バージョン*）、ライセンス詳細情報、クイック サポート リンクの一覧が表示されます。

[***情報***] ダイアログには 6 つのタブがあります。

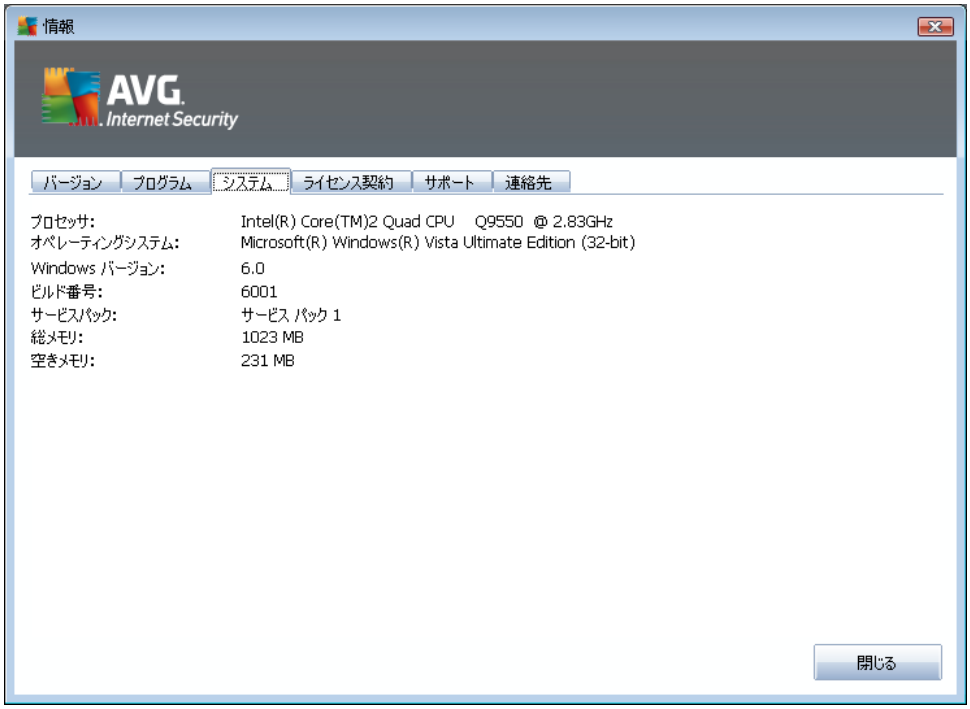
[***バージョン***] タブには次の 3 つのセクションがあります。

- ***サポート情報*** - **AVG Anti-Virus 2012**バージョン、ウイルス データベース バージョン、スパム対策 データベース バージョン、リンクスキャナ バージョンに関する情報が表示されます。
- ***ユーザー情報*** - ライセンス供与されたユーザーおよび企業に関する情報が表示されます。
- ***ライセンス詳細*** - ライセンスに関する情報 (*製品名*、*ライセンスの種類*、*ライセンス番号*、*有効期限*、*接続クライアント数*) が表示されます。このセクションでは、[***登録***] リンクを使用して **AVG Anti-Virus 2012**をオンラインで登録することもできます。登録することで、AVG テクニカル サポートのサービスを利用できます。また、[***再アクティベート***] リンクをクリックすると、[***AVG のアクティベート***] ダイアログが表示されます。該当するフィールドにライセンス番号を入力してセールス番号 *(AVG Anti-Virus 2012 インストール中に使用した番号)* を置き換えるか、現在のライセンス番号を別の番号に置き換えます (*上位の AVG 製品にアップグレードする場合など*)。

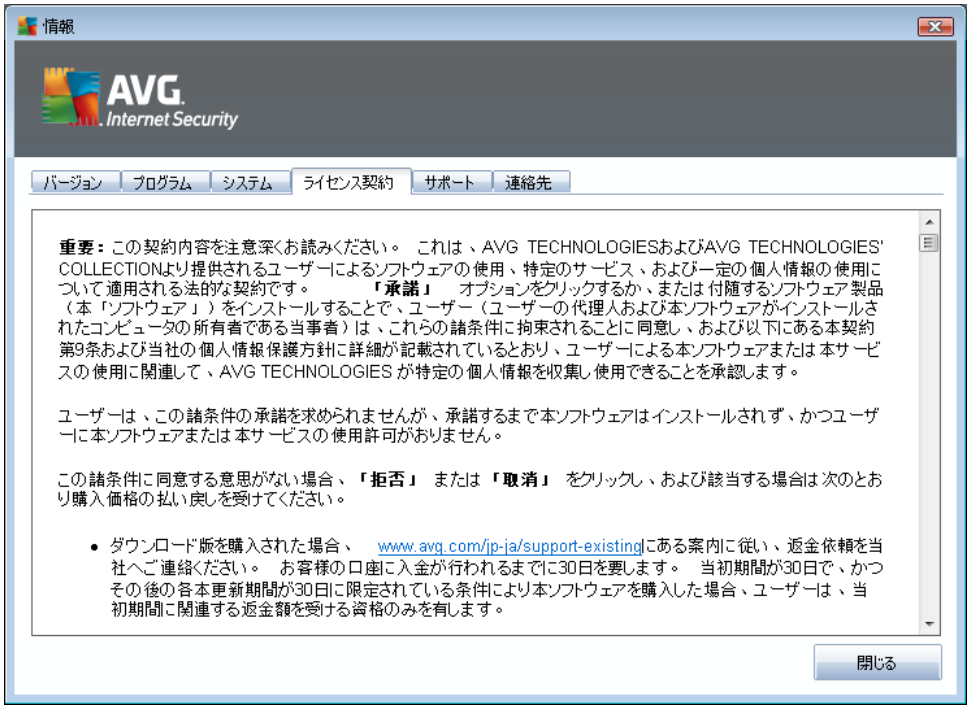
[***プログラム***] タブには、**AVG Anti-Virus 2012** のプログラム ファイル バージョンと製品で使用されているサード パーティ コード情報が表示されます。



[***システム***] タブにはオペレーティング システムのパラメータの一覧 (*プロセッサ タイプ、オペレーティング システムとバージョン、ビルド番号、使用しているサービス パック、合計メモリ サイズ、空きメモリ サイズ*) が表示されます。



[***ライセンス契約***] タブでは、AVG Technologies のライセンス契約の全文を読むことができます。



[***サポート***] タブにはカスタマー サポートに問い合わせるあらゆる可能性の一覧が表示されます。また、AVG Web サイト (http://www.avg.com/)、AVG フォーラム、FAQ などへのリンクも表示されます。さらに、カスタマー サポート チームに問い合わせる際に必要になる可能性のある情報も表示されます。

[***連絡先***] タブには AVG Technologies、各国 AVG の事業所、リセラーの問い合わせ先一覧が表示されます。

5.2. セキュリティ ステータス情報

[***セキュリティステータス情報***] セクションは **AVG Anti-Virus 2012** メイン ウィンドウの上部にあります。このセクションでは、**AVG Anti-Virus 2012**の現在のセキュリティステータスに関する情報が常に表示されます。このセクションで表示されるアイコンの意味は以下の通りです。

 - 緑のアイコンは ***AVG Anti-Virus 2012 が完全に機能していることを示します。*** コンピュータは完全に保護され、最新のインストール済みのコンポーネントが適切に動作しています。

 - オレンジのアイコンは、1 つ以上のコンポーネントが不正に設定され、プロパティ設定に注意する必要があることを警告しています。**AVG Anti-Virus 2012** には致命的な問題はなく、おそらく何らかの理由で一部のコンポーネントをオフにしたものと思われます。保護は適用されています。ただし、問題のコンポーネントの設定に注意してください。その名前は ***セキュリティステータス情報*** セクションに表示されます。

何らかの理由でコンポーネントのエラー状態を無視することを決定した場合にもオレンジのアイコンが表示されます。[***コンポーネント状態を無視***] オプションは、**AVG Anti-Virus 2012** メイン ウィンドウのコンポーネント概要の各コンポーネントのアイコンから開くコンテキスト メニュー (*右クリック*) で選択できます。何らかの理由がある場合にこのオプションを選択すると、コンポーネントの

エラー状態を認識しながらも、のエラー状態を保持できます。特定の場合にこのオプションを使用する必要があることが考えられますが、[***コンポーネント状態を無視***] オプションはすぐにオフにすることを強く推奨します。

 - 赤いアイコンは ***AVG Anti-Virus 2012 が致命的な状態であることを示しています。*** 1つ以上のコンポーネントが適切に動作していないため、**AVG Anti-Virus 2012** はコンピュータを保護できません。報告された問題を修復してください。エラーを自分で修復できない場合、AVGテクニカルサポートチームにお問い合わせください。

AVG Anti-Virus 2012 が最適なパフォーマンスに設定されていない場合は、新しい [修正] ボタン (問題が複数のコンポーネントに関連している場合は [すべてを修正] ボタン) がセキュリティステータス情報の横に表示されます。このボタンをクリックすると、プログラム チェックおよび設定の自動処理が実行されます。これは AVG Anti-Virus 2012 を最適なパフォーマンスに設定し、最高レベルのセキュリティを実現するための最も簡単な方法です。

セキュリティステータス情報に注意し、問題がレポートされた場合にはすぐに解決することを強く推奨します。そうでない場合、コンピュータが危険にさらされます。

メモ: *AVG Anti-Virus 2012 ステータス情報は、システム トレイ アイコンからも取得可能です。*

5.3. クイック リンク

クイック リンクは **AVG Anti-Virus 2012** ユーザー インターフェースの左側にあります。これらのリンクをクリックすると、スキャンや更新など最も重要で最も多く使用されるアプリケーション機能に素早くアクセスできます。クイック リンクはユーザー インターフェースのすべてのダイアログにあります。

クイック リンクはグラフィカルな方法で 3 つのセクションに分割されています。

- ***概要*** - このリンクを使用して、現在開いている AVG ダイアログから、すべてのインストールされたコンポーネントの概要を含む既定のインターフェースへ切り替わります。*(詳細については、「コンポーネント概要」を参照してください。)*
- ***今すぐスキャン*** - 既定では前回実行されたスキャンに関する情報 (スキャン タイプ、前回実行日) などを表示します。[***今すぐスキャン***] コマンドをクリックすると、同じスキャンをもう一度実行します。別のスキャンを実行する場合は、[***スキャン オプション***] リンクをクリックします。この方法で AVG スキャン インターフェースを開き、スキャンの実行、スキャン スケジュールの作成、パラメータの編集ができます。*(詳細については、「AVG スキャン」の章を参照してください。)*
- ***今すぐ更新*** - このリンクをクリックすると、前回実行した更新の日時が表示されます。このボタ

ンをクリックすると、更新処理がただちに実行され、進行状況が表示されます。*(詳細については、「AVG 更新」の章を参照してください。)*

クイック リンクには AVG ユーザー インターフェースからいつでもアクセスできます。一度、クイック リンクを使用して、スキャンや更新の特定のプロセスを実行すると、アプリケーションは新しいダイアログに切り替わりますが、クイック リンクはまだ利用できます。さらに、実行中のプロセスはグラフィカルな方法でナビゲーションに表示されるため、現時点で **AVG Anti-Virus 2012** で実行中のすべてのプロセスを完全に管理できます。

5.4. コンポーネント概要

コンポーネント概要セクション

[***コンポーネント概要***] セクションは**AVG Anti-Virus 2012** ユーザー インターフェースの中央部にあります。このセクションは 2 つに分かれます。

- □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ □□□□□□□□□□***インストールされているすべてのコンポーネントの概要***各パネルにはコンポーネントのアイコンが表示され、各コンポーネントがその時点で有効かどうかを示します。
- □□□□□□□□□□□□□***コンポーネントの説明***が表示されます。この部分にはコンポーネントの基本機能に関する概要説明が表示されます。また、選択したコンポーネントの最新ステータス情報も表示されます。

インストールされているコンポーネントのリスト

AVG Anti-Virus 2012 の [***コンポーネント概要***] セクションには、次のコンポーネントの情報が示されます。

- ***ウイルス対策***はシステム内のウイルス、スパイウェア、ワーム、トロイの木馬、望ましくない実行ファイルまたはライブラリを検出し、悪意のあるアドウェアからユーザーを保護します - 詳細 >>
- ***リンクスキャナ***はインターネット検索や閲覧中に Web ベースの攻撃からユーザーを保護します - 詳細 >>
- ***メール保護***は受信 電子メール メッセージにスパム メールがあるかどうかをチェックし、ウイルス、フィッシング攻撃、その他の脅威をブロックします - 詳細 >>
- ***ファイアウォール***は各ネットワーク ポートのすべての通信を制御し、悪意のある攻撃からユーザーを保護し、侵入の試みをすべてブロックします - 詳細 >>
- ***ルートキット対策***はアプリケーション、ドライバ、ライブラリに隠れている危険なルートキットをスキャンします - 詳細 >>
- ***システム ツール***は、AVG 環境の詳細な概要とオペレーティング システム情報を提供します。 - 詳細 >>
- ***PC Analyzer***は、コンピュータ ステータスに関する情報を提供します。 - 詳細 >>

- ***Identity Protection*** はデジタル資産を新しい未知の脅威から継続的に保護します - 詳細 >>

- ***セキュリティツールバー***をインストールすると、選択した AVG の機能をインターネットから直接利用できます。- 詳細 >>

- ***リモート管理***は AVG Business Edition でのみ表示されます。インストール処理中にこのコンポーネントのインストールを指定した場合に限ります。

利用可能なアクション

- ***コンポーネント概要で、任意のコンポーネントのアイコン***の上にマウスを移動すると、コンポーネントが強調表示されます。同時に、コンポーネントの基本機能説明がユーザー インターフェースの下部に表示されます。

- ***任意のコンポーネントのアイコン***をクリックすると、コンポーネントのインターフェースが開き、基本統計情報リストが表示されます。

- ***コンポーネントのアイコン***を右クリックすると、コンテキスト メニューが開き、次のオプションが表示されます。

  - ***開く***- このオプションをクリックすると、コンポーネントのダイアログが開きます (コンポーネントのアイコンをクリックした場合と同じ)。

  - ***コンポーネントの状態を無視*** - このオプションを選択すると、コンポーネントのエラー状態を認識していても、何らかの理由でこの状態を保持し、システム トレイ アイコンによる警告を表示しません。

  - ***高度な設定で開く..*** - このオプションは高度な設定が可能である一部のコンポーネントでのみ表示されます。

5.5. システム トレイ アイコン

AVG システム トレイ アイコン *(モニタの右下端の Windows タスクバーの上)* は、**AVG Anti-Virus 2012** の最新ステータスを示します。このアイコンは **AVG Anti-Virus 2012** のユーザー インターフェースが表示されているかどうかにかかわらず、システム トレイ上に常に表示されます。

AVG システム トレイ アイコン表示

- 全色でその他の要素がない場合、アイコンはすべての**AVG Anti-Virus 2012**コンポーネントがアクティブで完全に機能していることを示しています。ただし、コンポーネントのいずれかが完全に機能していない状態で、ユーザーがコンポーネント状態を無視することを選択した場合にも、同じ方法でアイコンが表示されます。*([コンポーネント状態を無視] オプションを確認すると、コンポーネントのエラー状態を認識しつつ、何らかの理由でその状態を保持し、エラー状態に関する警告を表示しないことを明示的に示したことになります。)*

- エクスクラメーション マークの付いたアイコンは、1 つ以上のコンポーネントがエラー状態になっていることを示します。必ずこのような警告に注意し、適切に設定されていないコンポーネントの設定の問題を解決するようにしてください。コンポーネントの設定を変更するには、システム トレイ アイコンをダブルクリックして、アプリケーションのユーザー インターフェースを開きます。エラー状態になっているコンポーネントの詳細については、「セキュリティ ステータス情報」セクションを参照してください。

- 全色で表示されているシステム トレイ アイコンが点滅し、光が回転している場合があります。この状態は現在更新処理が実行されていることを示します。

- 全色で表示されているシステム トレイ アイコンに矢印が付いている場合は、**AVG Anti-Virus 2012**スキャンが実行中であることを示しています。

AVG システム トレイ アイコン情報

AVG システム トレイ アイコンは **AVG Anti-Virus 2012** で現在実行されている処理やプログラムのステータス変更の可能性 (*スケジュールされたスキャンまたは更新の自動起動、ファイアウォール プロファイル切り替え、コンポーネントのステータス変更、エラー ステータスの発生など*) を通知しています。これは、システム トレイ アイコンから開くポップアップ ウィンドウに表示されます。

AVG システム トレイ アイコンから実行できるアクション

AVG Anti-Virus 2012 のユーザー インターフェースへのクイック リンクとして ***AVG システム トレイ アイコン***を使用することもできます。アイコンをダブルクリックするだけです。アイコンを右クリックすると、次のオプションの簡単なコンテキスト メニューを開きます。

- ***AVG ユーザー インターフェースを開く*** - クリックすると、**AVG Anti-Virus 2012**のユーザー インターフェースが開きます。

- ***スキャン*** - クリックすると、定義されたスキャンのコンテキスト メニュー (*完全コンピュータ スキャン*、*特定のファイルまたはフォルダをスキャン*、*ルートキット対策スキャン*) が開きます。目的のスキャンを選択すると、すぐにスキャンが実行されます。

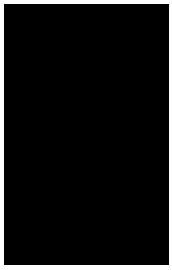
- ***ファイアウォール*** - クリックすると、ファイアウォール設定オプションのコンテキスト メニューが開き、

ファイアウォール ステータス (*ファイアウォール有効/ファイアウォール無効/緊急モード*)、ゲーム モード切替、ファイアウォール プロファイルなどの主要パラメータを編集できます。

- ***PC Analyzer***を実行 - クリックすると、PC Analyzer コンポーネントが起動します。
- ***実行中のスキャン*** - 現在コンピュータでスキャンが実行されている場合にのみこの項目が表示されます。この場合、スキャンの優先度の設定、実行中のスキャンの停止または一時停止を実行できます。さらに、*すべてのスキャンの優先度の設定*、*すべてのスキャンの一時停止*、*すべてのスキャンの停止*アクションも実行できます。
- ***今すぐアップデート*** - すぐにアップデートを起動します。
- ***ヘルプ*** - スタート ページにヘルプ ファイルが開きます。

5.6. AVG ガジェット

AVG ガジェットは Windows デスクトップ (*Windows サイドバー*) *に表示されます。*このアプリケーションは Windows Vista とWindows 7 オペレーティング システムにのみ対応しています。***AVG ガジェット***を使用すると、スキャンや更新など最も重要な **AVG Anti-Virus 2012** 機能に簡単にアクセスできます。



スキャンと更新へのクイック アクセス

必要に応じて、***AVG ガジェット***を使用して、スキャンや更新をただちに起動できます。

- ***今すぐスキャン*** - [***今すぐスキャン***] リンクをクリックすると、完全コンピュータ スキャンを直接開始できます。ガジェットで表示されるユーザー インターフェースでスキャン処理の進行状況を確認できます。簡単な統計情報概要が表示され、スキャンされたオブジェクト、検出された脅威、修復された脅威の数に関する情報が示されます。スキャン中はいつでも、スキャン処理を一時停止  または停止できます。  スキャン結果に関する詳細データについては、標準の [スキャン結果概要] ダイアログを確認してください。このダイアログは [***詳細を表示***] *オプションのガジェットから直接開くことができます (各スキャン結果はサイドバー ガジェット スキャン*の下に一覧表示されます)。

- ***今すぐ更新*** - [***今すぐ更新*** **AVG Anti-Virus 2012**] リンクをクリックすると、ガジェットから直接更新を実行できます。

ソーシャル ネットワークへのアクセス

AVG ガジェットには主なソーシャル ネットワーク サービスに接続するクイック リンクがあります。各ボタンを使用すると、Twitter、Facebook、LinkedIn の AVG コミュニティに接続します。

- ***Twitter リンク*** - 新しい ***AVG ガジェット*** インターフェースが開き、Twitter に投稿される最新の AVG フィードの概要が表示されます。[***すべての AVG Twitter フィードを表示する***] リンクをクリックすると、インターネット ブラウザで新しいウィンドウが開き、Twitter Web サイトの AVG 関連ニュース ページに直接リダイレクトされます。

- ***Facebook リンク*** - インターネット ブラウザで Facebook Web サイトが開き、***AVG コミュニティ***ページが表示されます。

- ***LinkedIn*** - このオプションはネットワーク インストールでのみ利用できます (*AVG Business Edition ライセンスを使用して AVG をインストールした場合*)。LinkedIn ソーシャル ネットワークの ***AVG SMB Community*** でインターネット ブラウザが開きます。

ガジェットで利用できるその他の機能

- ***PC Analyzer***  - PC Analyzerコンポーネントのユーザー インターフェースが開きます。
- ***検索ボックス*** - キーワードを入力すると、検索結果が既定の Web ブラウザで新しく開くウィンドウにただちに表示されます。

6. AVG コンポーネント

6.1. ウィルス対策

ウイルス対策コンポーネントは **AVG Anti-Virus 2012** の基本であり、さまざまな基本セキュリティプログラム機能をが統合されています。

- スキャン エンジン
- 常駐保護
- スパイウェア対策保護

6.1.1. スキャン エンジン

ウイルス対策コンポーネントの基本であるスキャン エンジンはすべてのファイルとフォルダの動作 *(ファイルを開く、閉じるなど) をスキャンします。*既知のウィルスの存在をチェックします。検出されたウィルスはブロックされ動作しなくなり、駆除またはウイルス隔離室に隔離されます。

AVG Anti-Virus 2012 保護の重要な機能は、既知のウイルスがコンピュータで実行されないようにすることです。

検出方法

大部分のウイルス対策ソフトウェアではヒューリスティック スキャンも使用されています。これにより、ファイルは一般的なウイルスの特性 (ウイルス シグネチャ) に基づいてスキャンされます。このため、新種のウィルスに既存のウィルスの一般的な特性が含まれる場合は、新種の未知のウィルスでもウィルス対策スキャナによって検出できます。***ウイルス対策***は次の検出方式を使用します。

- スキャン - ウィルス特性文字列の検索
- ヒューリスティック分析 - 仮想コンピュータ環境におけるスキャン オブジェクト命令の動的エミュレーション
- 一般検出 - ウイルス/ウイルスグループの命令特性の検出

1つの技術だけではウイルスを検出、特定できない場合、***ウイルス対策***は、複数の技術を結合し、コンピュータがウイルスから保護されていることを保証します。**AVG Anti-Virus 2012** はシステム内に存在する不審な実行可能アプリケーションや DLL ライブラリの分析と検出もできます。このような脅威を不審なプログラム*と呼んでいます (各種スパイウェア、アドウェアなど)*。さらに、**AVG Anti-Virus 2012** はシステム レジストリをスキャンし、疑わしいエントリ、インターネット一時ファイル、トラッキング cookie を検出することで、潜在的に有害なアイテムを他の感染と同様に処理できます。

AVG Anti-Virus 2012 はコンピュータを継続的に保護します。

6.1.2. 常駐保護

AVG Anti-Virus 2012 は常駐保護の形式で継続的な保護を行います。***ウイルス対策*** コンポーネントはファイル *(特定の拡張子のファイルまたは拡張子のないファイル)* が開く、保存、コピーされるときに必ずスキャンを実行します。コンピュータのシステム領域とリムーバブル メディア (*フラッシュ ディスクなど*) を保護します。アクセスされるファイルにウイルスが検出された場合、現在実行されている操作を停止し、ウイルスが活性化しないようにします。常駐保護は「バックグラウンド」で動作するため、通常、ユーザーがこの処理を意識することはありません。脅威の検出時にのみユーザー通知が表示されます。同時に、***ウイルス対策*** は脅威の有効化を阻止し、脅威を駆除します。

常駐保護は起動時にコンピュータのメモリ内にロードされるため、常にこのコンポーネントを有効にしておくことが非常に重要です。

6.1.3. スパイウェア対策保護

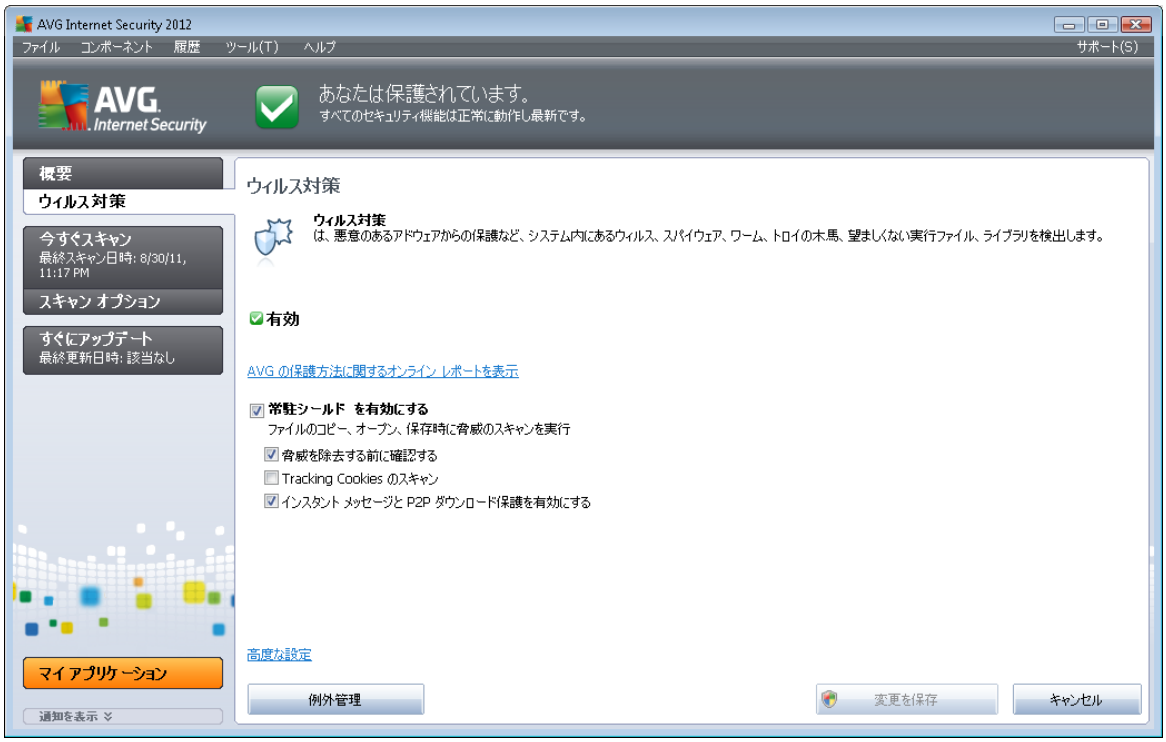
スパイウェア対策 は、既知の種類のスパイウェア定義を特定するために使用されるスパイウェア データベースから構成されています。最新のスパイウェア パターンが出現するとすぐに、AVG のスパイウェアの専門技術者が総力をあげて新しいスパイウェアの特定と解明に努め、AVG スパイウェア データベースに定義を追加しています。これらの新しい定義は更新プロセスを介してコンピュータにダウンロードされ、最新種のスパイウェアからも保護されます。***スパイウェア対策*** では、コンピュータのマルウェアやスパイウェアを完全にスキャンできます。また、休止状態でアクティブではないマルウェアも検出されます。したがって、ダウンロードされた後アクティブ化されていないマルウェアも検出されます。

スパイウェアの概要

通常、スパイウェアはマルウェアの一種として定義され、ユーザーが知らない間に許可なくコンピュータから情報を収集します。一部のスパイウェア アプリケーションは、故意にインストールされることもあり、広告やウィンドウ ポップアップ、その他の不快なソフトウェアを含む場合があります。現在、大部分の感染原因は、潜在的に危険な内容を含むWebサイトです。電子メールなどによる感染、ワームやウィルスによる感染なども広がりつつあります。最も効果的な保護方法は、常にバックグラウンド スキャナをオンにして、***スパイウェア対策*** を使用することです。このコンポーネントは常駐シールドのように機能し、アプリケーションの実行時にバックグラウンドでスキャンします。

6.1.4. ウイルス対策インターフェース

ウイルス対策 コンポーネントのインターフェースには、コンポーネントの機能に関する概要、コンポーネントの現在のスタータス *(アクティブ)* に関する情報、コンポーネントの基本設定オプションが表示されます。



設定オプション

ダイアログには ***ウイルス対策*** コンポーネントで利用可能な機能の基本的な設定オプションが表示されます。オプションの概要は次のとおりです。

- ***AVG の保護方法に関するオンライン レポートを表示する*** - このリンクをクリックすると、AVG Web サイトの特定のページに移動します。http://www.avg.com/ このページには、特定の期間にコンピュータで実行されたすべての**AVG Anti-Virus 2012**活動全体の活動に関する詳細統計情報が表示されます。

- ***常駐シールドを有効にする*** - このオプションでは、常駐保護を簡単に有効/無効にできます。常駐シールドは、ファイルがコピー、オープン、保存される時にファイルをスキャンします。ウイルスや何らかの種類の脅威が検出されると、ただちに警告が表示されます。既定ではこの機能は有効です。この設定を保持することをお勧めします。常駐シールドをオンにすると、さらに検出された感染の処理方法を決定できます。

  - ***すべての脅威を自動的に駆除する/脅威を駆除する前に確認する*** - いずれかのオプションを選択します。この選択はセキュリティレベルに影響しません。

  - ***Tracking Cookie をスキャンする*** - 前のオプションとは別に、Tracking Cookie をスキャンするかどうかを決定できます。 *Cookie とはサーバーからWeb ブラウザに送信され、そ*

*のサーバーにアクセスするたびにブラウザによって変更されずに返信されるテキストのことです。HTTP cookie は認証トラッキングやサイトの好み、あるいは電子ショッピングカートの内容といったユーザーに関する特定情報の保持のために使用されます)。*特定の場合、このオプションをオンにし、最大限のセキュリティレベルに変更することができます。デフォルトではオフになっています。

- ***インスタント メッセージ保護を有効にする*** - インスタント メッセージ通信 (*ICQ、MSN Messenger など*) にウイルスが含まれていないことを確認する場合は、この項目を選択します。

- ***高度な設定*** - このリンクをクリックすると、**AVG Anti-Virus 2012**の高度な設定の該当するダイアログに移動します。このダイアログではコンポーネントの設定を詳細に編集できます。ただし、すべての既定の設定は**AVG Anti-Virus 2012**で最適なパフォーマンスと最大のセキュリティが実現されるように設定されています。絶対に必要な場合以外は、既定の設定を保持することをお勧めします。

コントロール ボタン

ダイアログでは次のコントロール ボタンを使用できます。

- ***例外の管理*** - 新しい [常駐シールド - 例外] ダイアログを開きます。このダイアログにはメインメニューからもアクセスできます。*[高度な設定/ウイルス対策/常駐シールド/例外] の順にクリックします (詳細については、各章を参照してください)。*このダイアログでは、常駐シールド スキャンから除外するファイルとフォルダを指定できます。必要な場合を除き、すべての項目を含めることを強くお勧めします。ダイアログには次のコントロール ボタンがあります。

  - *パスの追加* – ローカル ディスクのナビゲーション ツリーからディレクトリを 1 つずつ選択してスキャン対象から除外するディレクトリを指定します。

  - *ファイルの追加* –ローカル ディスク ナビゲーション ツリーからファイルを 1 つずつ選択してスキャン対象から除外するファイルを指定します。

  - *項目の編集* –選択したファイルまたはフォルダへの特定のパスを編集できます。

  - *項目の削除*–選択した項目へのパスをリストから削除できます.

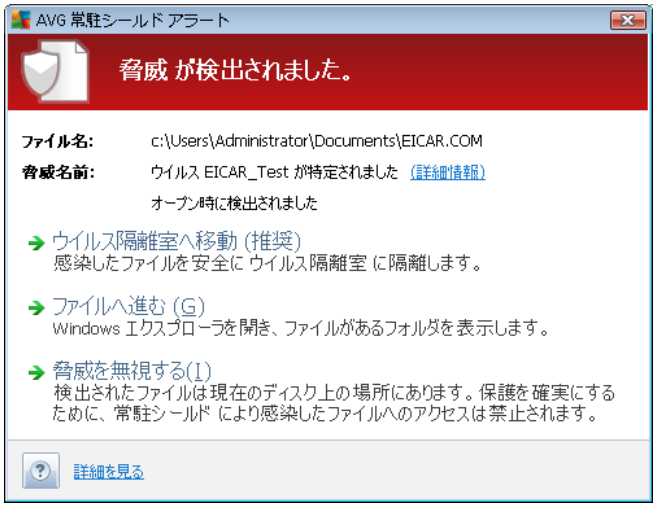
- ***変更の保存*** - このダイアログで実行したコンポーネントの設定変更をすべて保存して、**AVG Anti-Virus 2012**のユーザー インターフェース (*コンポーネント概要*) に戻ります。

- ***キャンセル*** - このダイアログで実行したコンポーネントの設定変更をすべて取り消します。変更は保存されません。**AVG Anti-Virus 2012**のメインのユーザー インターフェース (*コンポーネント概要*) に戻ります。

6.1.5. 常駐シールド検出

検出された脅威!

常駐シールドは、ファイルがコピー、オープン、保存される時にファイルをスキャンします。ウイルスや何らかの種類の脅威が検出されると、以下のダイアログ経由で即時に警告が表示されます。



警告ダイアログでは、検出され感染と判定されたファイルに関するデータ(*ファイル名*)、認識された感染名 (*脅威名*)、既知の脅威の場合に検出された脅威に関する詳細情報を確認できる (詳細情報) *ウィルス エンサイクロペディア*へのリンクが表示されます。

さらに、今すぐ実行する処理を決定する必要があります。複数のオプションから選択できます。***特定の条件 (感染したファイルの種類やファイルの場所) によっては、利用できないオプションがあります。***

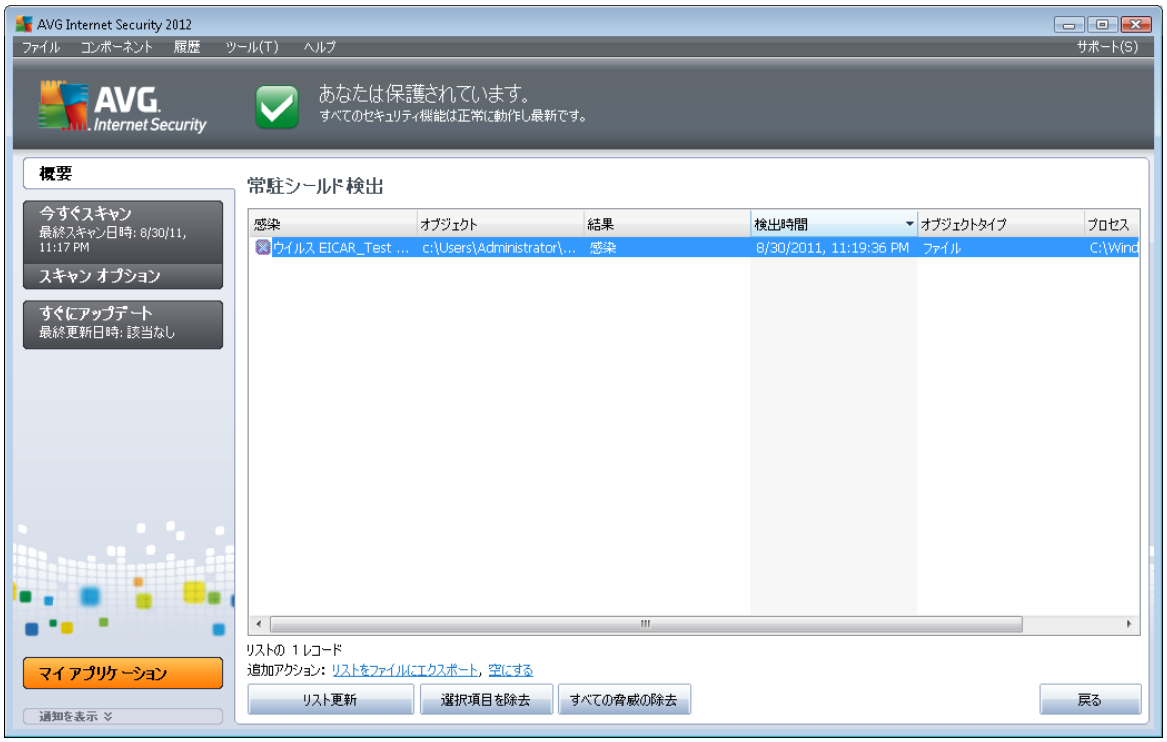
- ***パワーユーザーとして脅威を除去*** – 一般ユーザーとして脅威を除去する権限がない場合はボックスにチェックをします。パワーユーザーにはより強いアクセス権限があります。脅威がシステムフォルダにある場合等、このチェックボックスを使用して除去する場合があります。
- ***修復*** - 検出された感染が修復可能な場合にのみこのボタンが表示されます。これで感染がファイルから削除され、ファイルが元の状態に復元されます。ファイル自体がウィルスでアル場合は、この機能を使用してウィルスを削除 (*ウィルス隔離室に移動*) します。
- ***ウイルス隔離室に移動*** - ウイルスは ウイルス隔離室に移動します。
- ***ファイルに移動*** - このオプションは不審なオブジェクトの正確な場所に移動します (*新しい Windows Explorer ウィンドウを開きます*)
- ***無視*** - しかるべき理由がない場合は、このオプションを使用しないでください。

メモ: *検出されたオブジェクトのサイズがウィルス隔離室の空き領域上限サイズを超えている場合があります。この場合、感染したオブジェクトをウィルス隔離室に移動しようとすると、この問題を通知する警告メッセージがポップアップ表示されます。ただし、ウィルス隔離室のサイズを変更することができます。ウィルス隔離室のサイズは、ハードディスクの実際のサイズに対する調整可能な割合として定義されます。ウィルス隔離室のサイズを増やすには、[AVG 高度な設定] の [ウィルス隔離室サイズの上限] オプションを使用して [ウィルス隔離室] ダイアログに移動します。*

ダイアログの下部には [***詳細を表示する***] リンクがあります。このリンクをクリックすると、ポップアップ ウィンドウが開き、感染の検出時に実行していたプロセスに関する詳細情報およびプロセス ID が表示されます。

常駐シールドの検出機能の概要

常駐シールドによって検出されたすべての脅威の概要は、システム メニュー オプションの [***履歴/常駐シールド検出***] の [常駐シールド検出] ダイアログに表示されます。



常駐シールド検出 では、常駐シールドによって検出され、修復あるいはウイルス隔離室に移動されたオブジェクトの概要が表示されます。検出された各オブジェクトについて、以下の情報が提供されます。

- ***感染*** - 検出されたオブジェクトの説明（可能な場合は名前も）
- ***オブジェクト*** - オブジェクトの場所
- ***結果*** - 検出されたオブジェクトで実行されたアクション
- ***検出時刻*** - オブジェクトが検出された日時
- ***オブジェクトタイプ*** - 検出されたオブジェクトの種類
- ***プロセス*** - 呼び出すために実行されたアクション

ダイアログの下部では、リストの下に上記でリストされた検出オブジェクトの総数に関する情報が表示されます。さらに、検出オブジェクトの完全なリストをファイルにエクスポート（***ファイルにエクスポート***）し、検出オブジェクトのすべてのエントリを削除（***リストを空にする***）ことができます。[***リストを更新***] ボタンは ***常駐シールド*** の検出結果リストを更新します。[***戻る***] ボタンをクリックすると、既定の ***AVG メイン ダイアログ（コンポーネント概要）に戻ります。

6.2. リンクスキャナ

リンクスキャナは、ますます増加する一時的にしか存在しない Web 上の脅威からユーザーを保護します。このような脅威は、政府機関のサイト、有名な大企業のサイト、中小企業のサイトなど、あらゆる種類の Web サイトに潜み、そのサイトに 24 時間以上存在することはほとんどありません。***リンクスキャナ***は表示しようとするすべての Web ページにある各リンクをチェックし、リンク先の Web ページを解析することでユーザーを保護します。安全性の確認が必要である、ユーザーがリンクをクリックしようとしたタイミングでチェックが実行され、サイトの安全性が保証されます。

リンクスキャナはサーバー プラットフォームに対応していません。

リンクスキャナ技術は次の主要な機能から構成されています。

- サーチ シールドには、危険性が確認されている Web サイト (URL アドレス) のリストが含まれています。Google、Yahoo!、WebHledani、Yandex、Baidu、Bing、AOL、AltaVista、EarthLink、Ask、Seznam で検索を実行すると、このリストに従ってすべての検索結果がチェックされ、判定アイコンが表示されます (*Yahoo! での検索結果の場合、「エクスプロイト Web サイト」という判定アイコンのみ表示されます*)。

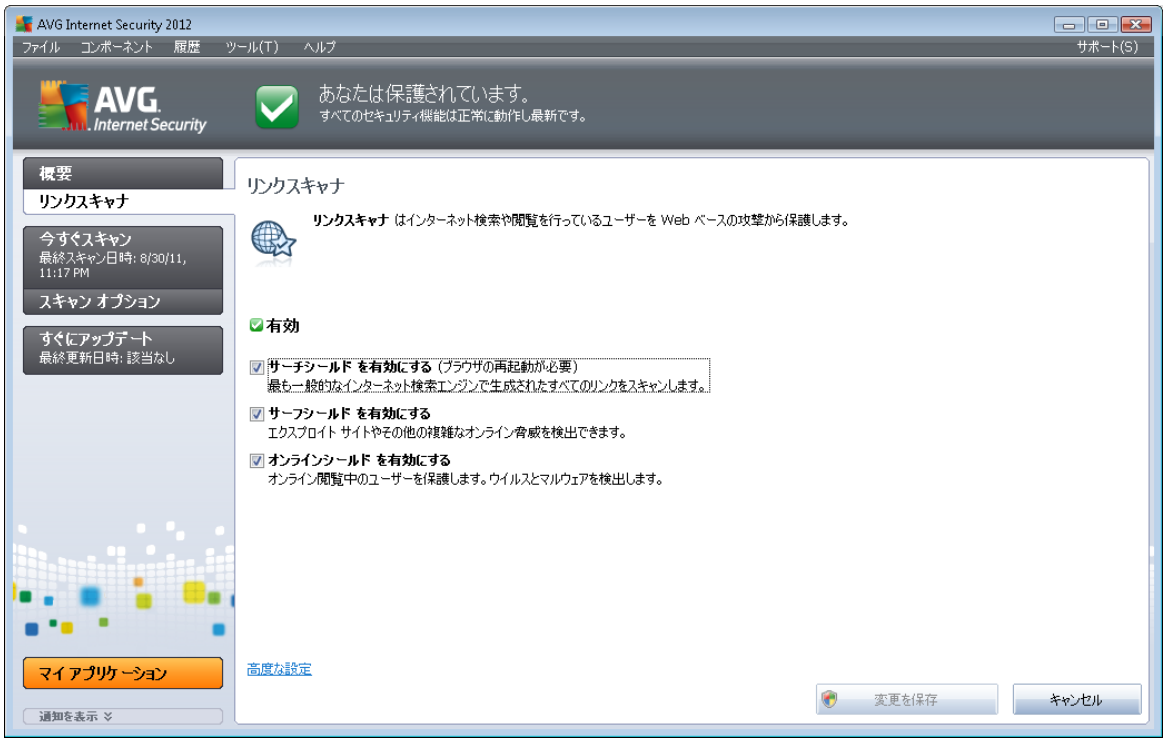
- サーフ シールドは Web サイト アドレスに関係なく、アクセスしようとしている Web サイトのコンテンツをスキャンします。サーチ シールド*で検出されない Web サイト (新しい悪意のある Web サイトが作成された、以前に安全であった Web サイトに今はマルウェアが含まれているなど)* にアクセスを試みると、サーフ シールドによってブロックされます。

- オンライン シールド□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ アクセスした Web ページのコンテンツとページに含まれるファイルをスキャンします。Web ブラウザに表示されたりコンピュータにダウンロードされたりする前にスキャンを実行します。オンライン シールドはアクセスしようとしているページに含まれるウイルスとスパイウェアを検出し、ダウンロードをただちにブロックするため、脅威がコンピュータに侵入することはありません。

- ***AVG Accelerator*** はオンライン ビデオのサービスをスムーズにして、ダウンロードを簡単にします。ビデオ高速化処理を実行しているときには、システム トレイ ポップアップ ウィンドウに通知が表示されます。

6.2.1. リンクスキャナ インターフェース

リンクスキャナ コンポーネントのメイン ダイアログには、コンポーネント機能の概要説明と最新ステータス *(アクティブ)* に関する情報が表示されます



ダイアログの下部にはコンポーネントの基本設定が表示されます。

- ***サーチ シールド***を有効にする - (*既定では有効*): サーチ シールドの機能を無効にする合理的な理由がある場合にのみボックスをクリアします。
- ***サーフシールド***を有効にする - (*既定ではオン*): ユーザーがサイトにアクセスしようとするときに、積極的に*リアルタイム*でエクスプロイト サイトを検出し、保護を実施します。ユーザーがWebブラウザ *(あるいは他のHTTPを使用するアプリケーション)* からWebページにアクセスする際、既知の悪意のあるサイトへの接続と、エクスプロイトコンテンツがブロックされます。
- ***オンライン シールド***を有効にする - (*既定ではオン*): アクセスしようとしているWebページをリアルタイムでスキャンしてウイルスやスパイウェアの可能性を検出します。脅威が検出された場合は、ダウンロードがただちにブロックされるため、脅威がコンピュータに侵入することはありません。

6.2.2. サーチ シールドの検出機能

サーチシールドをオンにしてインターネットを検索すると、最も一般的な検索エンジン (*Google*、*Yahoo! JP*、*WebHledani*、*Yandex*、*Baidu*、*Bing*、*AOL*、*AltaVista*、*EarthLink*、*Ask*、*Seznam*、*eBay*、*Twitter*、*Digg*、*SlashDot*) の検索結果すべてが評価され、危険なリンクか疑わしいリンクかどうかが判定されます。これらのリンクをチェックし、悪意のあるリンクとして判定されると、リンクスキャナは、危険、または疑わしいリンクをクリックする前に警告を表示します。したがって、安全なウェブサイトにのみアクセスすることが保証されます。

検索結果ページのリンクが評価されている間、リンクの隣にリンク検証が実行中であることを示すアイコンが表示されます。判定が終了すると、各情報アイコンが表示されます。

リンクされたページは安全です (*このアイコンは安全な Yahoo! JP 検索結果*については表示されません)。

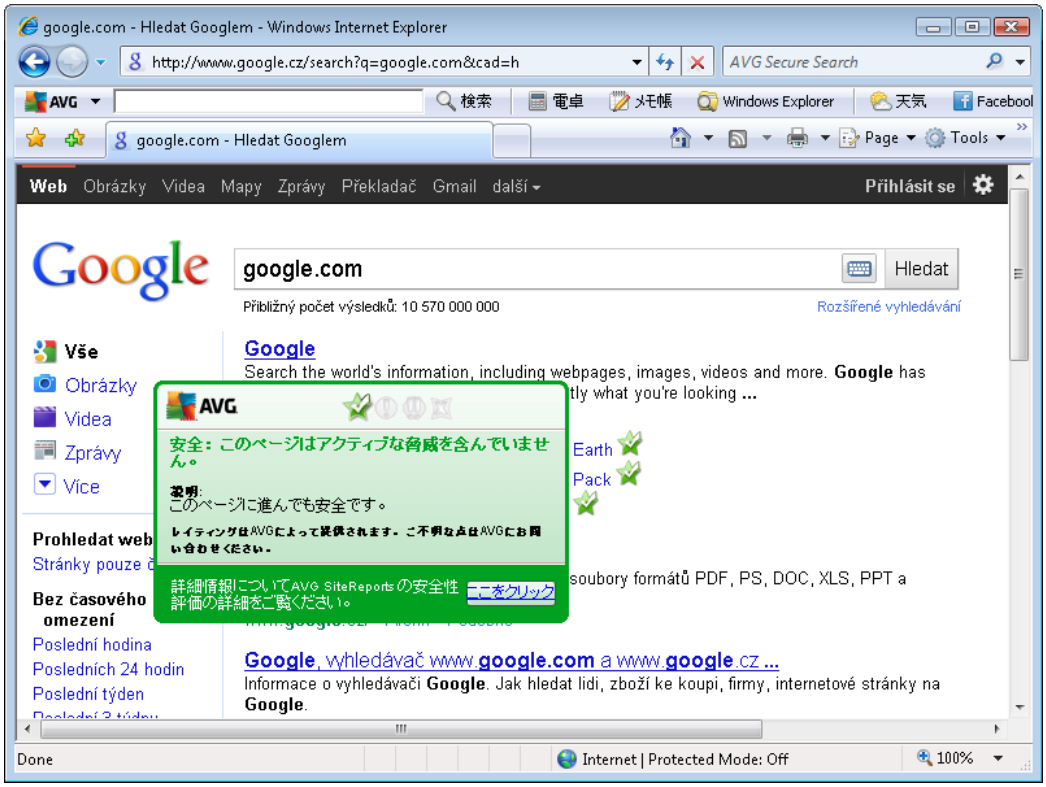
リンクされたページは脅威を含んでいませんが、疑わしいコンテンツを含みます (*または目的が疑わしいため、電子ショッピングが推奨されないなど*)。).

リンクされたページはそれ自体安全ですが、明らかに危険なページへのリンクを含んでいます。あるいは、現段階では脅威ではないものの、疑わしいコードを含んでいます。

リンクされたページはアクティブな脅威を含んでいます。安全のために、このページへのアクセスは禁止されています。

リンクされたページは、アクセスできないかスキャンできませんでした。

個々の評価アイコンは、問題のあるリンクに関する詳細を表示します。脅威の詳細情報 (*提供されている場合*) が含まれます。



6.2.3. サーフ シールドの検出機能

この強力な保護は開こうとするWebページの悪意のある内容をブロックし、コンピュータへのダウンロードを防止します。この機能が有効化されていると、危険なサイトへのリンクをクリックしたり、URLを入力したりすると、自動的にWebページを開かないようにブロックし、不注意な感染から保護します。エクスプロイト Web ページは、単にサイトにアクセスするだけでコンピュータが感染する可能性があります。エクスプロイトや他の深刻な脅威を含む Web ページにアクセスする際、リンクスキャナは、これらのページを表示させません。

悪意のあるWebサイトに遭遇した場合、リンクスキャナは以下のような画面で警告を表示します。

このようなウェブサイトへのアクセスは非常に危険であり、お勧めしません。

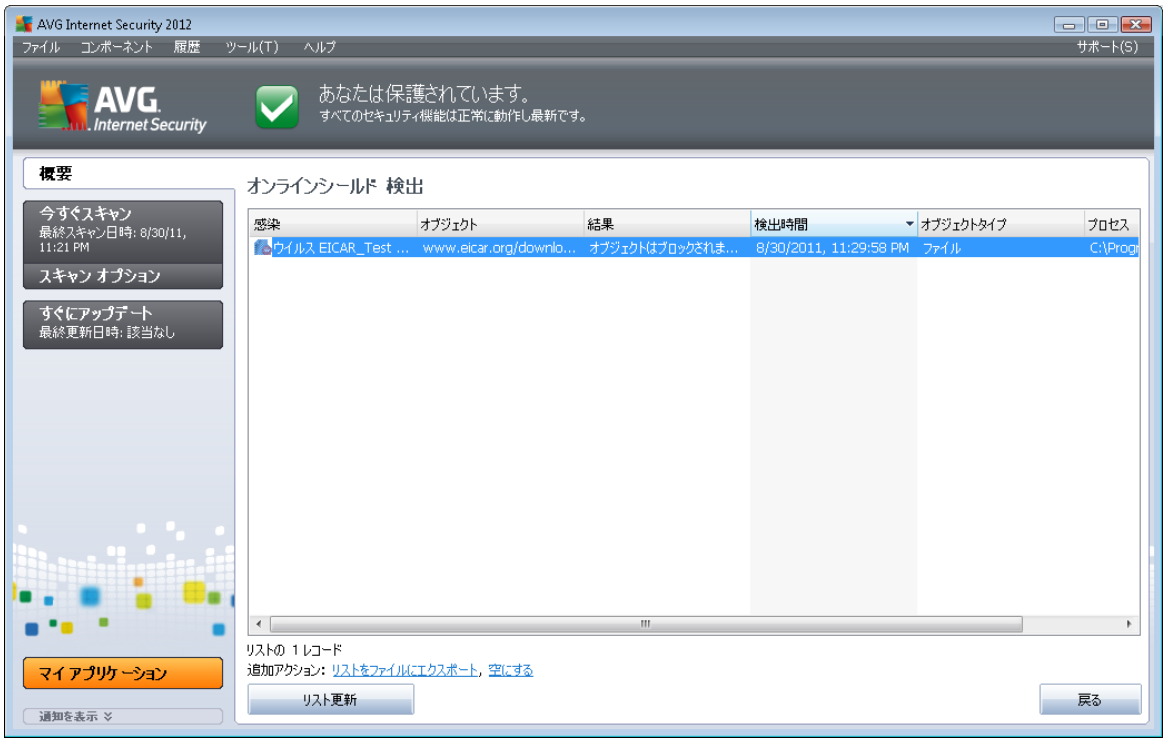
6.2.4. オンライン シールドの検出機能

オンライン シールドは ウェブブラウザに表示され、コンピュータにダウンロードされる前に、ウェブページの内容およびそこに含まれる可能性のあるファイルをスキャンします。脅威が検出されると、次のダイアログで即時に警告が表示されます。

警告ダイアログでは、検出され感染と判定されたファイルに関するデータ(*ファイル名*)、認識された感染名 (*脅威名*)、既知の脅威の場合に検出された脅威に関する詳細情報を確認できる*ウィルス エンサイクロペディア*へのリンクが表示されます。ダイアログには次のボタンがあります。

- ***詳細を表示*** - [***詳細を表示***] ボタンをクリックすると、新しいポップアップ ウィンドウが開き、感染が検出されたときに実行中であったプロセスの情報とプロセス ID が表示されます。
- ***閉じる*** - ボタンをクリックすると、警告ダイアログを閉じます。

疑わしいウェブページは開かれません。また、脅威検出は ***オンライン シールド検出結果*** のリストにログ出力されます。この検出された脅威の概要は、システムメニューの [履歴/オンライン シールド検出結果] からアクセス可能です。



検出された各オブジェクトについて、以下の情報が提供されます。

- ***感染*** - 検出されたオブジェクトの説明 (*可能な場合は名前も*)
- ***オブジェクト*** - オブジェクトソース (*ウェブページ*)

- ***結果*** - 検出されたオブジェクトで実行されたアクション
- ***検出時刻*** - 脅威が検出された日時
- ***オブジェクトタイプ*** - 検出されたオブジェクトの種類
- ***プロセス*** - 呼び出すために実行されたアクション

ダイアログの下部では、リストの下に上記でリストされた検出オブジェクトの総数に関する情報が表示されます。さらに、検出オブジェクトの完全なリストをファイルにエクスポート (***ファイルにエクスポート***) し、検出オブジェクトのすべてのエントリを削除 (***リストを空にする***) ことができます。》

コントロール ボタン

- ***リストを更新***] - ***オンライン シールド***
- ***戻る*** - 既定の AVG メイン ダイアログ (*コンポーネント概要*)

6.3. メール保護

最も一般的なウイルスとトロイの木馬の感染源の一つはメールです。フィッシング、スパムはメールをさらに大きなリスクソースとします。無料メールアカウントは、さらにこのような悪意のあるメールを受信する可能性が高くなり (*これらはめったにスパム対策技術を導入していないため*)、かなりのホームユーザーはこのようなメールを利用しています。また、ホームユーザーは、不明なサイトをインターネットサーフィンしたり、個人情報 (*メールアドレスなど*) を含むオンラインフォームに情報を入力し、メールを介しての攻撃にさらされる機会を増やします。会社は、通常会社のメールアカウントを使用し、スパム対策フィルタ等を導入してリスクを削減します。

メール保護 コンポーネントは、すべての送受信される電子メール メッセージをスキャンします。電子メールでウィルスが検出されると、必ずウィルス隔離室にただちに移動されます。このコンポーネントでは特定の種類の電子メールの添付ファイルを除外できます。また、電子メールが感染していないことを示す認証テキストを送信メールに追加できます。***メール保護*** には 2 つの主要な機能があります。

- メールスキャナ
- スパム対策

6.3.1. メール スキャナ

パーソナル電子メール スキャナ コンポーネントは、送受信メールを自動的にスキャンします。このコンポーネントは独自の AVG プラグインがない電子メール クライアントで使用できます (*Microsoft Outlook や The Bat など特定のプラグインを提供することで、AVG がサポートしている電子メール クライアントで電子メール メッセージをスキャンする場合にも使用できます*)。このコンポーネントは、主に Outlook Express、Mozilla、Incredimail などの電子メール アプリケーションで使用することを想定しています。

インストール中に AVG ではメール制御用の自動サーバーが作成されます。1 つは受信メール チェック用で、もう1 つは送信電子メール チェック用です。この 2 つのサーバーを使用して、メールは自動的にポート 110 と25 (*送受信メールの標準ポート*) でチェックされます。

パーソナルメールスキャナはメールクライアントとインターネット上のメールサーバーのインターフェースとし

て動作します。

- ***受信メール:***サーバーからメッセージを受信している間、***メールスキャナ***コンポーネントはウイルススキャンを行い、感染した添付ファイルを削除し、証明書を追加します。検出されたウィルスは、即時にウィルス隔離に隔離されます。次にメッセージはメールクライアントに渡されます。

- ***送信メール:***メールクライアントからメールスキャナにメッセージが送信されます。メッセージと添付ファイルはウイルススキャンされ、その後にメッセージがSMTPサーバーに送信されます(*送信メールのスキャンは既定では無効で、手動で設定できます*)。

メールスキャナはサーバープラットフォームには対応していません。

6.3.2. スパム対策

スパム対策の仕組み

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SPAMに設定します。***スパム対策***は、特別なテキスト文字列を追加して、メールの件名(*スパムとして特定されたメール*)を修正できます。これで、メールクライアントでメールを簡単にフィルタリングできます。***スパム対策コンポーネントは、複数の分析手法を使用して各メールを処理し、最大限の保護を提供します。スパム対策***コンポーネントは、スパム保護のため、定期的に更新されるデータベースを使用します。また、RBLサーバー(*既知のスパム送信者」メールアドレスの公開データベース*)を使用したり、手動でメールアドレスをホワイトリスト(*スパムとしてマークされない*)およびブラックリスト(*常にスパムとしてマーク*)に追加できます。

スパムの概要

スパムとは、望まないメールであり、たいていは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いっぱいにする、製品やサービスの広告です。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。

6.3.3. メール保護インターフェース

[***メール保護***] ダイアログでは、コンポーネントの機能を説明する簡潔なテキスト、最新のステータスに関する情報 (*アクティブ*) などが表示されます。[***AVG の保護方法に関するオンライン レポートを表示***] リンクをクリックすると、AVG Web サイト (http://www.avg.com/) の専用ページに **AVG Anti-Virus 2012** 処理の統計詳細情報が表示されます。

基本メール保護設定

[***メール保護***] ダイアログでは、コンポーネントの基本機能を編集できます。

- ***受信メッセージのスキャン*** (*既定では有効*) - この項目を選択すると、すべてのアカウントに送信されたメールがウイルス スキャンされるように指定できます。
- ***送信メッセージのスキャン*** (*既定では無効*) - この項目を選択すると、自分のアカウントから送信されるすべての電子メールがウイルス スキャンされるように指定できます。
- ***電子メールのスキャン中に通知アイコンを表示する*** - この項目を選択すると、メールのスキャン中に、システム トレイの スパム対策 を有効にする (既定では有効) - この項目を選択すると、未承認広告メールを受信メールから除外するかどうかを指定します。

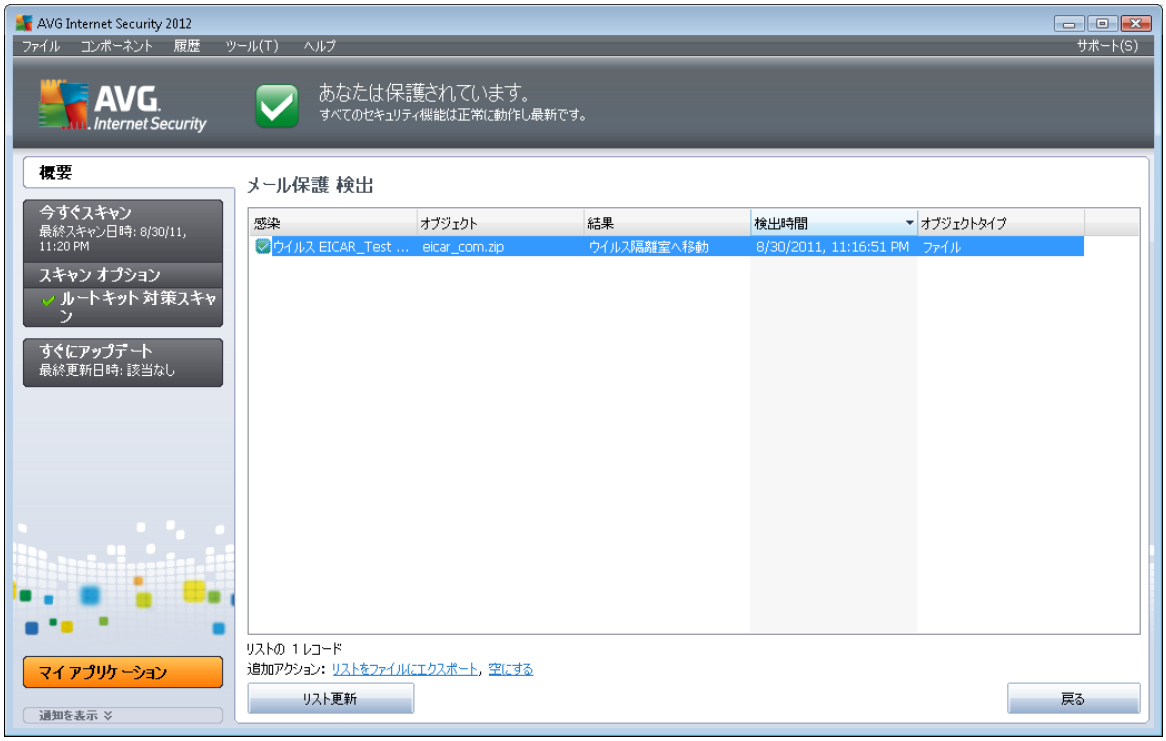
すべての AVG コンポーネントは最適なパフォーマンスを実現できるようにあらかじめ設定されています。特に理由がない場合は AVG の設定を変更しないでください。設定変更は上級者ユーザーが行うことをお勧めします。AVG の設定を変更する必要がある場合は、システム メニュー項目の [ツール/高度な設定] を選択し、[AVG 高度な設定] ダイアログで設定を編集します。

コントロール ボタン

[***メール保護***] ダイアログで利用できるコントロール ボタンは次のとおりです。

- ***変更の保存*** - このボタンをクリックすると、ダイアログで行われた変更を保存して適用します。
- ***戻る*** - このボタンをクリックすると、既定の AVG メイン ダイアログ (*コンポーネント概要*) に戻ります。

6.3.4. メール保護の検出機能



[***メール スキャナ検出***] ダイアログ (*[システム メニュー] オプションの [履歴/電子メール スキャナ検出] からアクセスできます*) では、メール保護 コンポーネントによって検出されたすべての結果リストが表示されます。検出された各オブジェクトについて、以下の情報が提供されます。

- ***感染*** - 検出されたオブジェクトの説明 (可能な場合は名前も)
- ***オブジェクト*** - オブジェクトの場所
- ***結果*** - 検出されたオブジェクトで実行されたアクション
- ***検出時刻*** - 不審なオブジェクトが検出された日時
- ***オブジェクトタイプ*** - 検出されたオブジェクトの種類

ダイアログの下部では、リストの下に上記でリストされた検出オブジェクトの総数に関する情報が表示さ

れます。さらに、検出オブジェクトの完全なリストをファイルにエクスポート（***ファイルにエクスポート***）し、検出オブジェクトのすべてのエントリを削除（***リストを空にする***）ことができます。

コントロールボタン

メールスキャナ検出インターフェースで利用できるコントロールボタンは以下の通りです。

- ***リストを更新*** - 検出された脅威のリストの更新.
- ***戻る*** - 最初に表示していたダイアログに戻ります。

6.4. ファイアウォール

ファイアウォールは、トラフィックをブロック、または許可することで、2つ以上のネットワーク間のアクセスコントロールポリシーを実行するためのシステムです。ファイアウォールには1セットのルールが含まれます。このルールは外部から*（一般的にはインターネットから）*の攻撃から内部ネットワークを保護し、あらゆるネットワークポート上のすべての通信をコントロールします。定義されたルールにしたがって、通信が評価され、許可、または禁止されます。***ファイアウォール***が侵入の試みを認識すると、その試みを「ブロック」し、侵入者のコンピュータへのアクセスを許可しません。

ファイアウォールを設定して、定義されたポート経由および定義されたソフトウェアアプリケーションに対する内部/外部通信（双方向、受信、送信）を許可または禁止します。例えば、ファイアウォールを設定して、Microsoft Explorer を使用したウェブデータの送受信のみを許可することができます。その他のブラウザによるウェブデータの送信の試みはブロックされます。

ファイアウォールは、個人を特定できる情報が、コンピュータから許可なく送信されないように保護します。コンピュータが、インターネット上やローカルネットワーク上の他のコンピュータとデータを交換する方法をコントロールします。また、組織内では、***ファイアウォール***はネットワーク上の他のコンピュータからの内部ユーザーによる攻撃から、コンピュータを保護します。

ファイアウォールによって保護されていないコンピュータは、容易にコンピュータハッカーやデータ窃盗犯罪者のターゲットとなります。

推奨：*一般には、個々のコンピュータで複数のファイアウォールを使用することは推奨されていません。コンピュータのセキュリティは複数のファイアウォールをインストールしても向上しません。; これらの2つのアプリケーションで競合が発生する可能性が高いです。したがって、コンピュータではファイアウォールを1つだけ使用し、他のすべてのファイアウォールを無効化して、起こりうる競合とそれに関する問題のリスクを排除することを推奨します。*

6.4.1. ファイアウォールの原理

AVG Anti-Virus 2012 では、***ファイアウォール***がコンピュータのすべてのネットワークポート上のトラフィックを制御します。***ファイアウォール***は、定義されたルールに基づいて、*インターネットまたはローカルネットワークに接続*しようとするコンピュータで実行中のアプリケーションまたはコンピュータに接続しようとする外部アプリケーションを評価します。これらのアプリケーションに関して、***ファイアウォール***はネットワークポートでの通信を許可、または禁止します。*既定では、アプリケーションが不明な場合（定義されたファイアウォールルールがない場合など）*、***ファイアウォール***はその通信の試みを許可するかブロックするかを確認します。

AVG ファイアウォールはサーバープラットフォームには対応していません。

AVG ファイアウォールの機能：

- 既知のアプリケーションの通信を自動的に許可、またはブロックするかどうかを確認します。
- 必要に応じて、予め定義されたルールを持つプロファイルを使用します。
- 様々なネットワークに接続したり、様々なネットワークアダプタを使用する際のプロファイルを自動的に切り替えます。

6.4.2. ファイアウォール プロファイル

ファイアウォールでは、コンピュータがドメイン内にあるか、スタンドアロンか、ノートブックであるかに基づいて、特定のセキュリティルールを定義することができます。これらのオプションは、異なったレベルの保護を必要とし、レベルは該当するプロファイルによってカバーされています。ファイアウォールプロファイルは、予め定義されたファイアウォールコンポーネント設定です。

利用可能なプロファイル

- ***すべて許可 - あらかじめ設定され、常に存在する***ファイアウォールシステム プロファイルです。このプロファイルが有効化されると、すべてのネットワーク通信が許可されます。ファイアウォール保護がオフになった状態に近くなり、安全ポリシー ルールが適用されません (すべてのアプリケーションは許可されますが、パケットは引き続きチェックされます。すべてのフィルターを完全に無効化するには、ファイアウォールを無効化する必要があります)。システム プロファイルは複製、削除できません。設定の変更もできません。
- ***すべてブロック - あらかじめ設定され、常に存在する***ファイアウォールシステム プロファイルです。このプロファイルが有効になると、すべてのネットワーク通信はブロックされ、コンピュータは外部ネットワークからアクセスできなくなり、外部への通信もできなくなります。システムプロファイルは複製、削除することができません。また設定を変更することもできません。
- ***カスタム プロファイル*** - カスタム プロファイルを使用すると、*ノートブックPC などでさまざまなネットワークに頻繁に接続する場合に特に便利な自動プロファイル切り替えを利用できます。*カスタム プロファイルが**AVG Anti-Virus 2012** インストール後に自動的に生成され、ファイアウォール ポリシー ルールに関する独自のニーズに対応します。次のカスタム プロファイルを利用できます。
  - ***直接インターネットに接続*** - 追加の保護を適用せずにインターネットに直接接続している一般的な家庭用デスクトップ コンピュータやノートブック コンピュータ向けです。ノート PC をさまざまな不明で保護されていない可能性のあるネットワーク (*インターネット カフェ、ホテルの客室など*) に接続するときにもこのオプションが推奨されます。このプロファイルで最も厳しいファイアウォール ポリシー ルールを適用することで、このようなコンピュータが適切に保護されます。
  - ***ドメイン内のコンピュータ***- 学校や企業などローカル ネットワークのコンピュータに最適です。ネットワークには専門知識を持つ管理者が存在し、ネットワークがさまざまな方法で保護されていることが前提となっています。したがって、上記の他の場合よりもセキュリティレベルが低く設定され、共有フォルダやディスク装置などへのアクセスが許可されています。

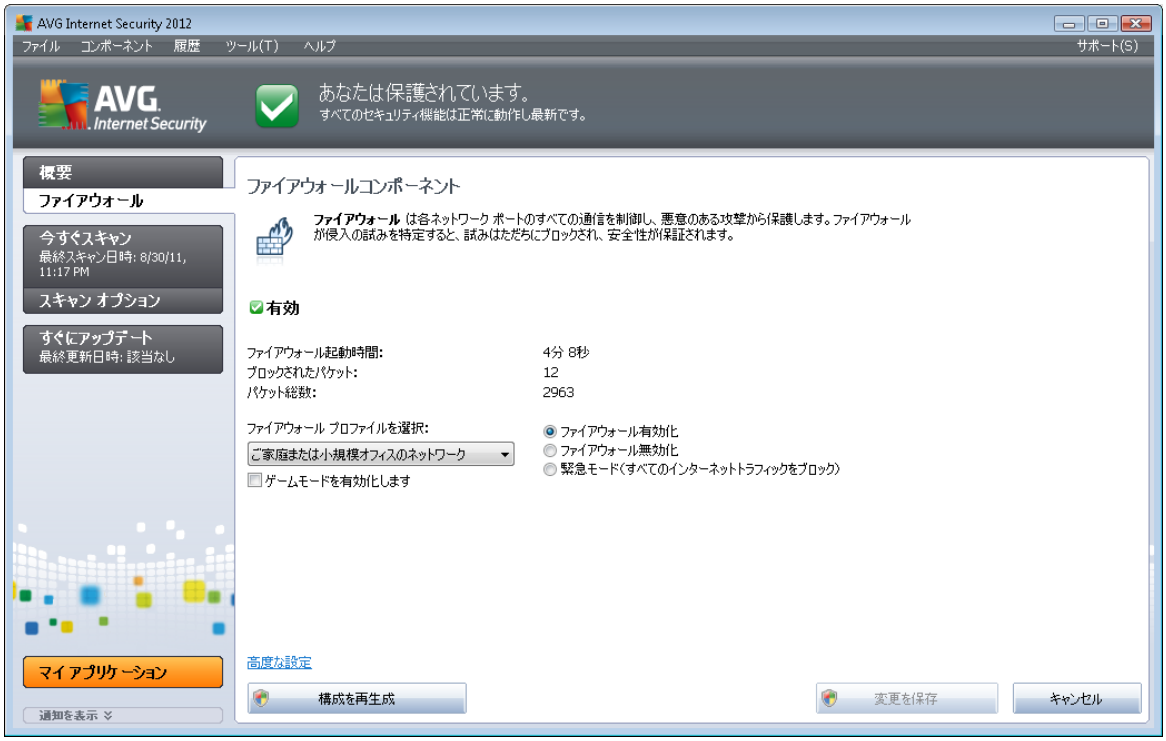
- ***ご家庭または小規模オフィスのネットワーク***- 家庭や小規模オフィスなどの小規模ネットワークのコンピュータに最適です。一般的に、この種類のネットワークには中央管理者がいません。また、ネットワークには複数のコンピュータが接続され、多くの場合はプリンタやスキャナなどのデバイスを共有しています。ファイアウォールにはこのような状況を反映しなければなりません。

プロファイル切り替え

プロファイル切り替え機能によって、あるネットワークアダプタを使用している時、またはある種類のネットワークに接続する時、ファイアウォールは自動的に定義済みプロファイルを切り替えることができます。ネットワークエリアにプロファイルが割り当てられていない場合、そのエリアへの次回の接続時に、ファイアウォールはプロファイルの割り当てを確認するダイアログを表示します。すべてのローカルネットワークインターフェースにプロファイルを割り当てるか、またはエリアとアダプタプロファイルダイアログで詳細設定を指定できます。このダイアログでは、使用しない機能を無効化することもできます（*すべての接続*で、*デフォルトプロファイルが使用されます*）。

通常、ノートブックを持ち、様々な種類の接続を行うユーザーにとってこの機能は役に立ちます。デスクトップコンピュータを持っている場合で、1種類の接続しか使用していない（*例えば、インターネットへのケーブル接続*）場合、プロファイル切り替えを行う必要はありません。

6.4.3. ファイアウォール インターフェース



[***ファイアウォール コンポーネント***] メインダイアログには、コンポーネントの機能、ステータス（*アクティブ*）、コンポーネント統計情報の概要に関する基本情報が表示されます。

- ***ファイアウォール起動時間 - ファイアウォールが最後に起動されてからの経過時間

- ***ブロックされたパケット*** - ブロックされたパケット数
- ***パケット総数*** - ファイアウォール実行中にチェックされたすべてのパケット数

基本ファイアウォール設定

- ***ファイアウォール プロファイルを選択*** - ロールダウン メニューから定義されたプロファイルのいずれか (*各プロファイルの詳細と推奨される使用方法については、「ファイアウォール プロファイル」の章を参照*) を選択します。
- ***ゲーム モードを有効にする*** - このオプションにチェックを付けると、全画面アプリケーション (*ゲーム、プレゼンテーション、動画など*) を実行するときに、ファイアウォールによって不明なアプリケーションの通信を許可するかブロックするかどうかを確認するダイアログが表示されません。不明なアプリケーションがネットワーク上で通信を試みる場合、ファイアウォールは現在のプロファイルの設定に応じて、自動的にその試みを許可あるいはブロックします。***メモ:*** ゲーム モードが有効になっている場合は、アプリケーションが終了するまで、すべてのスケジュール タスク (スキャン、更新) が延期されます。
- さらに、この基本設定セクションでは、ファイアウォール コンポーネントの最新ステータスを定義する 3 つのオプションから選択できます。
  - ***ファイアウォールを有効にする*** (*既定*) - 選択したファイアウォールプロファイルで定義されたルールセットに基づいて、アプリケーションの通信を許可します。
  - ***ファイアウォールを無効にする*** - このオプションはファイアウォールを完全にオフに切り替えます。すべてのネットワークトラフィックは許可され、チェックされません。
  - ***緊急モード (すべてのインターネット トラフィックをブロック)*** - このオプションを選択すると、各ネットワーク ポートでのすべてのトラフィックをブロックします。ファイアウォールは実行中ですが、すべてのネットワーク トラフィックは停止します。

メモ: *ソフトウェア ベンダーはすべての AVG Anti-Virus 2012 コンポーネントが最適なパフォーマンスを発揮するように設定しています。特に理由がない場合は、AVGの設定を変更しないでください。設定変更は、経験のあるユーザーが行うことを推奨します。AVG の設定を変更する必要がある場合、システム メニュー アイテムの****ツール/ファイアウォール設定*** *を選択し、AVG ファイアウォール設定ダイアログで設定を編集します。*

コントロールボタン

- ***設定の再作成*** - このボタンをクリックすると、現在のファイアウォール設定を上書きし、既定の自動検出設定に戻します。
- ***変更を保存*** - このボタンをクリックすると、ダイアログで行われた変更を保存し、適用します。
- ***戻る*** - このボタンをクリックすると、既定の AVG メイン ダイアログ (*コンポーネント概要*) に戻ります。

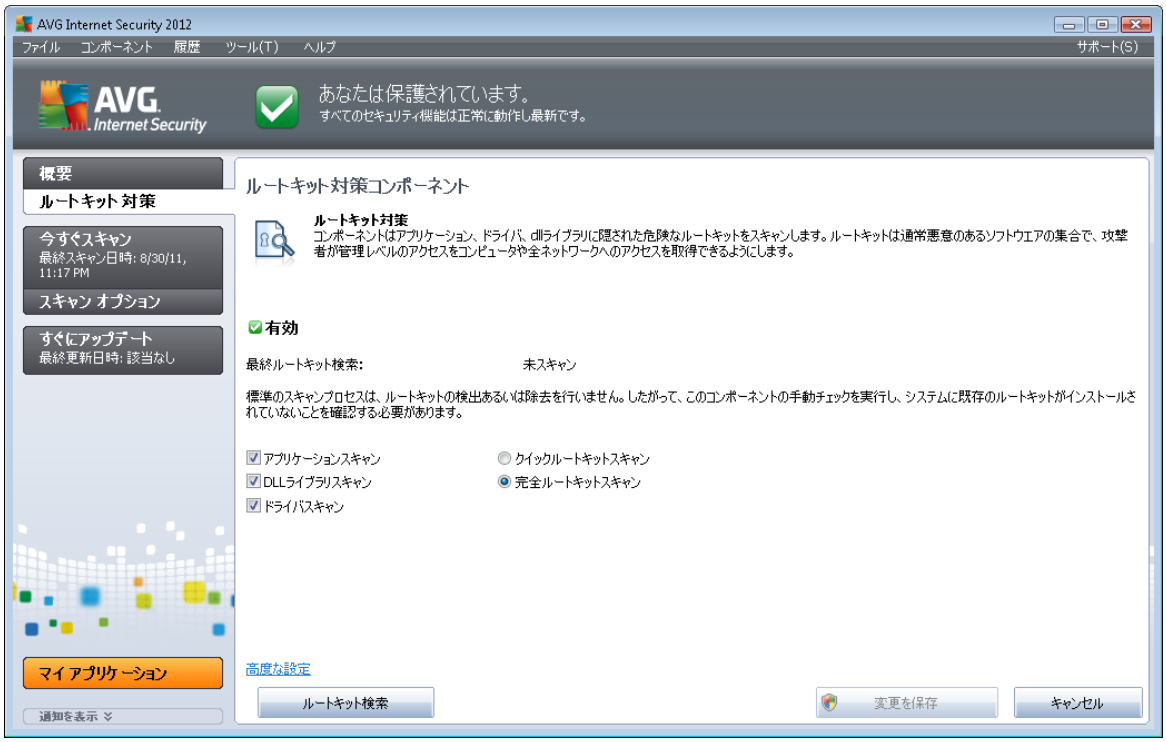
6.5. ルートキット対策

ルートキット対策は、コンピュータ上の悪意のあるソフトウェアの存在を隠すプログラムや技術等、危険なルートキットを検出し、効果的に除去するための特別なツールです。***ルートキット対策***は、あらかじめ定義されたルールセットに基づいて、ルートキットを検出できます。すべてのルートキットが検出されます *(感染したものだけではありません)*。***ルートキット対策***がルートキットを検出しても、必ずしもルートキットが感染しているというわけではありません。時々、ルートキットはドライバとして使用されたり、正しいアプリケーションの一部であったりします。

ルートキットとは何ですか?

ルートキットは、システムの所有者や正式な管理者の許可なく、コンピュータシステムの基本機能を制御するように設計されたプログラムです。ルートキットはハードウェア上で実行されているオペレーティングシステムを乗っ取ることを目的としているため、ハードウェアへのアクセスが必要になることはほとんどありません。一般的には、ルートキットは標準のオペレーティング システムのセキュリティメカニズムを破壊したり回避したりすることによって、システム上でその存在を隠しながら動作します。一般的に、ルートキットはトロイの木馬の一種でもあり、システムで実行しても安全であるかのように見せかけてユーザーを騙し、信じこませます。このような技術によって、プログラム監視の対象にならないように実行中のプロセスが隠されたり、オペレーティング システムからファイルやシステム データが隠されることもあります。

6.5.1. ルートキット対策インターフェース



[***ルートキット対策***] ダイアログには、コンポーネントの機能概要に関する説明が表示され、コンポーネントの現在の状態が通知されます。また、前回の***ルートキット対策***検査の実行日時 (***前回のルートキット検索***) 情報が表示されます。[***ルートキット対策***] ダイアログには、[ツール/高度な設定] リンクも表示されます。リンクをクリックすると、***ルートキット対策***コンポーネントの高度な設定環境にリダイレク

トされます。

すべての AVG コンポーネントは最適なパフォーマンスを実現できるようにあらかじめ設定されています。特に理由がない場合は、AVG の設定を変更しないでください。上級者ユーザーのみが設定変更を行うことをお進めします。

基本ルートキット対策設定

ダイアログの下部では、ルートキット スキャンの基本機能を設定できます。まず、該当するチェックボックスにチェックを付け、スキャン対象オブジェクトを指定します。

- ***アプリケーション スキャン***
- ***DLL ライブラリ スキャン***
- ***ドライバ スキャン***

さらに、ルートキット スキャン モードを選択できます。

- ***クイック ルートキット スキャン*** - すべての実行中のプロセス、ロードされたドライバ、およびシステム フォルダ (*通常は、c:\Windows*) をスキャンします。
- ***完全 ルートキット スキャン*** - すべての実行中のプロセス、ロードされたドライバ、システム フォルダ (*通常は、c:\Windows*)、およびすべてのローカル ディスク (*フラッシュ ディスクは含まれますが、フロッピー ディスクおよび CD ドライブは含まれません*) をスキャンします。

コントロール ボタン

- ***ルートキットの検索*** - ルートキットスキャンは完全コンピュータスキャンに暗黙的に含まれていないため、***ルートキット対策*** インターフェースからこのボタンを使用して直接ルートキットスキャンを実行できます。
- ***変更を保存*** - このボタンをクリックすると、このインターフェースで実行されたすべての変更を保存し、既定の AVG ユーザー インターフェース (*コンポーネント概要*) に戻ります。
- ***キャンセル*** - このボタンをクリックすると、実行した変更を保存せずに AVG メイン ダイアログ (*コンポーネント概要*) に戻ります。

6.6. システム ツール

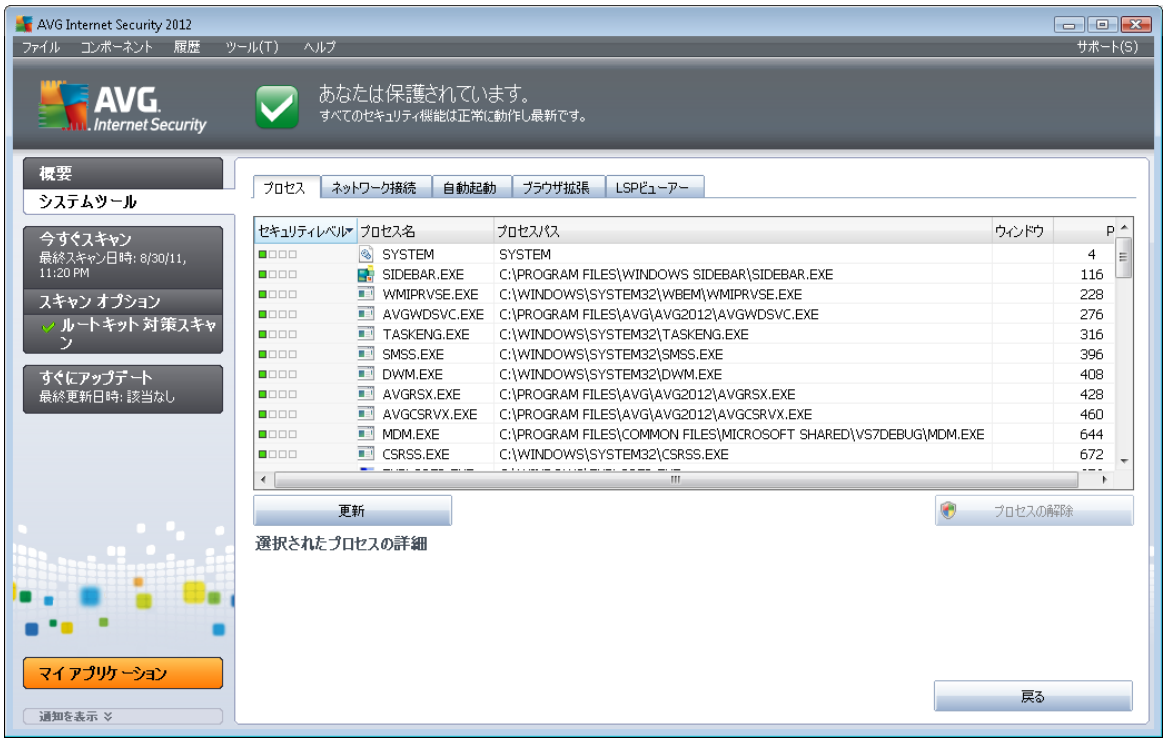
システム ツールとは、**AVG Anti-Virus 2012** 環境とオペレーティング システムの詳細サマリーを提供するツールのことです。コンポーネントには以下の概要が表示されます。

- プロセス - プロセスのリスト (*コンピュータ上で現在アクティブな実行中のアプリケーション*)。
- ネットワーク接続 - 現在アクティブな接続のリスト
- 自動起動 - Windows システム起動中に実行されるすべてのアプリケーションのリスト

- ブラウザ拡張 - プラグインのリスト (*インターネット ブラウザにインストールされているアプリケーション*)。
- LSP ビューア - レイヤード サービス プロバイダのリスト (*LSP*)

これらの情報を編集することもできますが、特に経験のあるユーザー向けとして推奨されています。

6.6.1. プロセス



プロセスダイアログには現在コンピュータ上でアクティブなプロセスのリスト *例えば、実行中のアプリケーション*) が表示されます。リストは複数のカラムに分けられます。

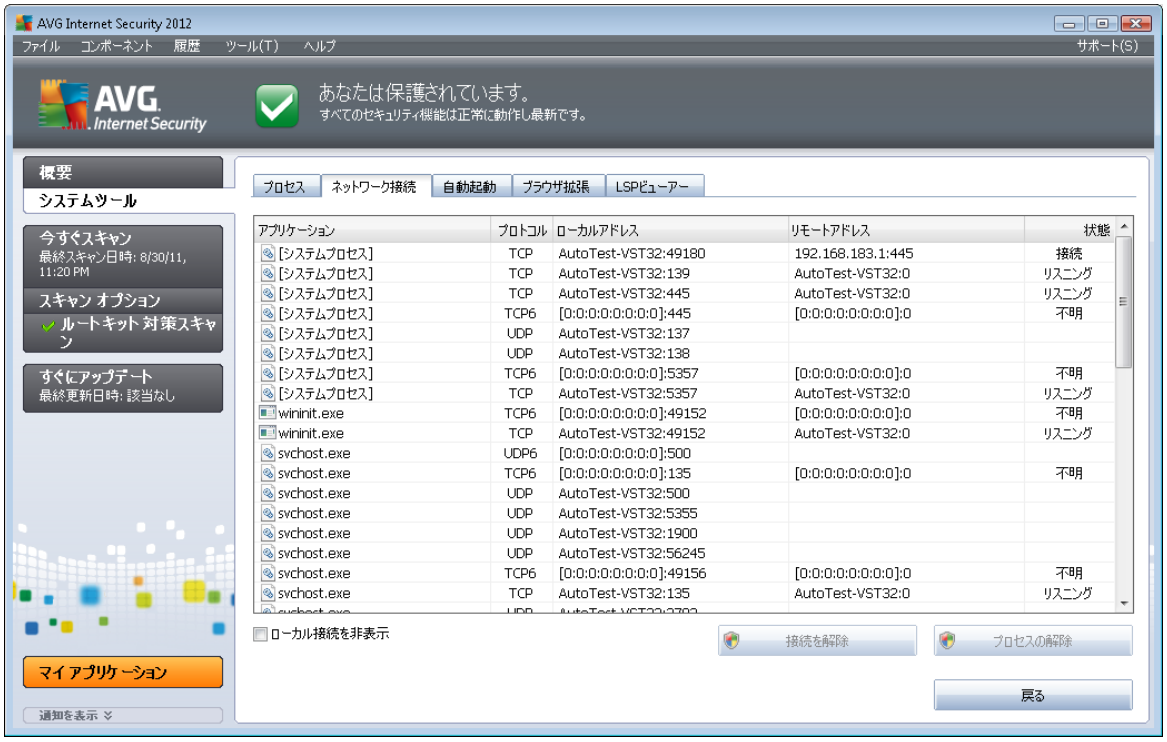
- ***重要度レベル*** - 重要度の低いもの (□□□□) から重大なもの (■■■■) までの 4 段階方式で各プロセスの重要度をグラフィカルに示します。
- ***プロセス名*** - 実行中のプロセス名
- ***プロセス パス*** - 実行中のプロセスへの物理パス
- ***ウィンドウ*** - アプリケーションウィンドウ名 (存在する場合のみ)
- ***PID*** - 一意のWindows内部プロセス識別番号

コントロールボタン

[***プロセス***] タブで利用できるコントロール ボタンは次のとおりです。

- ***更新*** - 現在のステータスに応じてプロセスのリストを更新します
- ***プロセスの終了*** - 1 つ以上のアプリケーションを選択し、このボタンをクリックするとそのアプリケーションを終了できます。***本当に脅威であることが確実である場合以外は、プロセス、または接続を解除しないことを強く推奨します。***
- ***戻る*** - 既定の AVG メイン ダイアログ(*コンポーネント概要*)に戻ります。

6.6.2. ネットワーク接続



ネットワーク接続ダイアログには、現在アクティブな接続のリストが表示されます。リストは以下のカラムに分けられます。

- ***アプリケーション*** - 接続に関するアプリケーション名 (*情報がない Windows 2000 を除く*)
- ***プロトコル*** - 接続に使用されるプロトコルタイプ
  - o TCP - インターネット上の情報を送信するインターネットプロトコル (IP) と合わせて使用されるプロトコル
  - o UDP - TCP プロトコルの代替
- ***ローカルアドレス*** - ローカルコンピュータで使用されるIPアドレスとポート番号
- ***リモートアドレス*** - 接続されるリモートコンピュータのIPアドレスとポート番号可能な場合、リモ

ートコンピュータのホスト名も表示されます。

- ***状態*** - 現在の状態 *(接続、サーバーシャットダウン、リッスン、アクティブ終了、受動終了、アクティブ終了)* を表示します。

外部接続のみをリスト表示する場合、リストの下のダイアログの下部セクションの [***ローカル接続を非表示***] チェックボックスをオンにします。

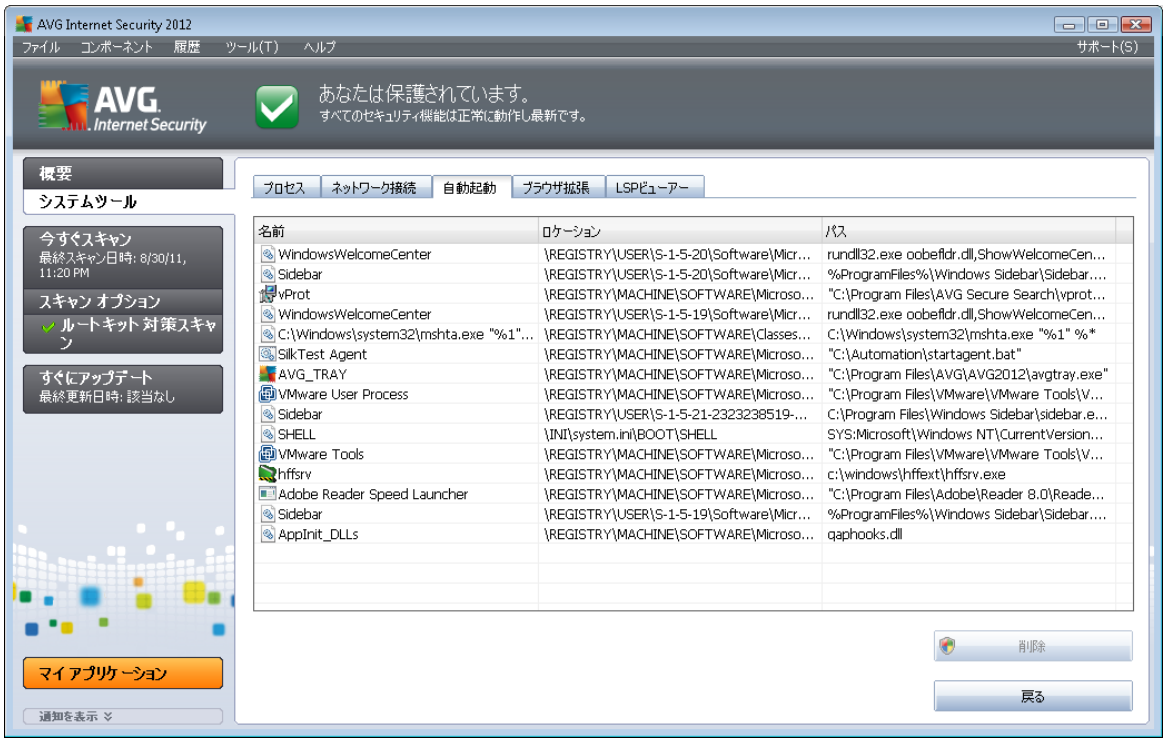
コントロールボタン

[***ネットワーク接続***] タブで利用できるコントロールボタンは次のとおりです。

- ***接続を解除*** - リストで選択された1つ以上の接続を終了します。
- ***プロセスを終了*** - リストで選択された接続に関する1つ以上のアプリケーションを終了します。
- ***戻る*** - 既定の AVG メイン ダイアログ (コンポーネント概要) に切り替わります。

現在接続状態にあるアプリケーションのみを解除できる場合があります。警告:本当に脅威であることが確実である場合以外は、接続を解除しないことを強く推奨します。

6.6.3. 自動起動



自動起動ダイアログには、Windowsシステム起動中に実行されるすべてのアプリケーションリストが表示されます。一部のマルウェアは、頻繁にレジストリエントリを追加します。

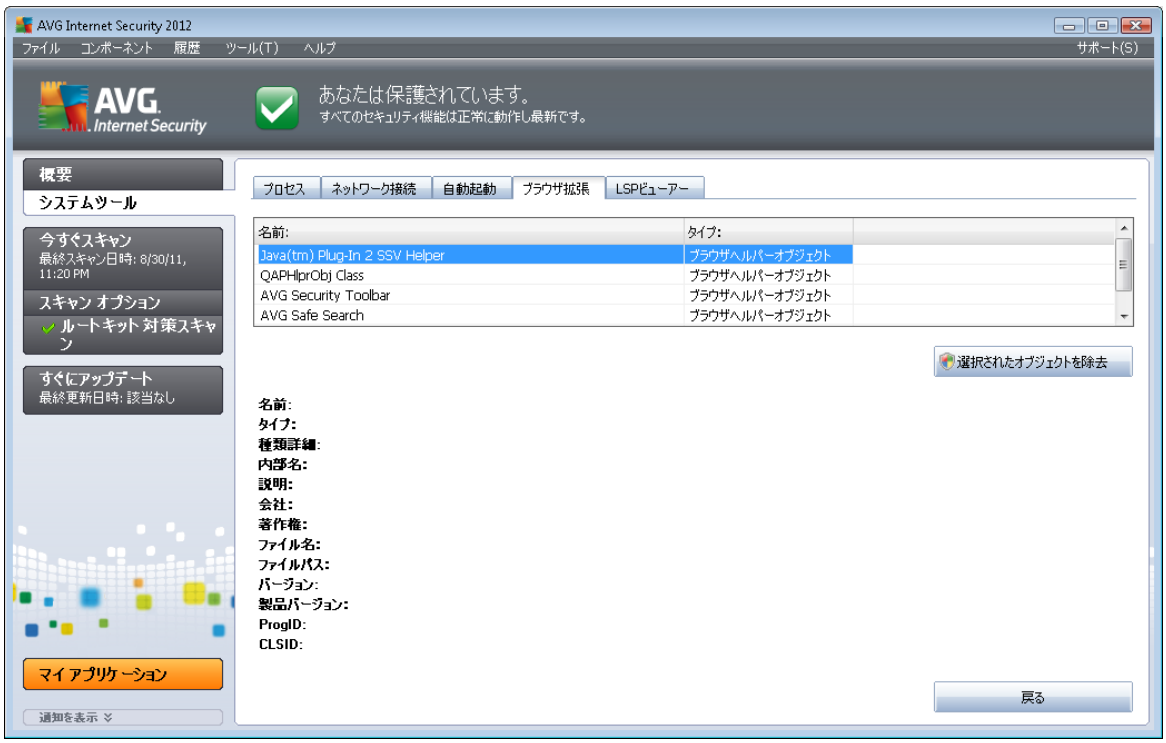
コントロール ボタン

[***自動起動***] タブで利用できるコントロール ボタンは次のとおりです。

- ***選択した項目を削除*** - ボタンをクリックすると、1 つ以上の選択した項目を削除します。
- ***戻る*** - 既定の ***AVG メイン ダイアログ *(コンポーネント概要)* に戻ります。

脅威であることが確実である場合以外は、リストからアプリケーションを削除しないことを強く推奨します。

6.6.4. ブラウザ拡張



[***ブラウザ拡張***] ダイアログにはインターネット ブラウザにインストールされているプラグインのリスト (*アプリケーション*な) が含まれます。このリストには、潜在的なマルウェアプログラムだけでなく、通常のアプリケーションプラグインが含まれる場合があります。リストのオブジェクトをクリックすると、ダイアログの下部セクションに表示される選択したプラグインに関する詳細を取得します。

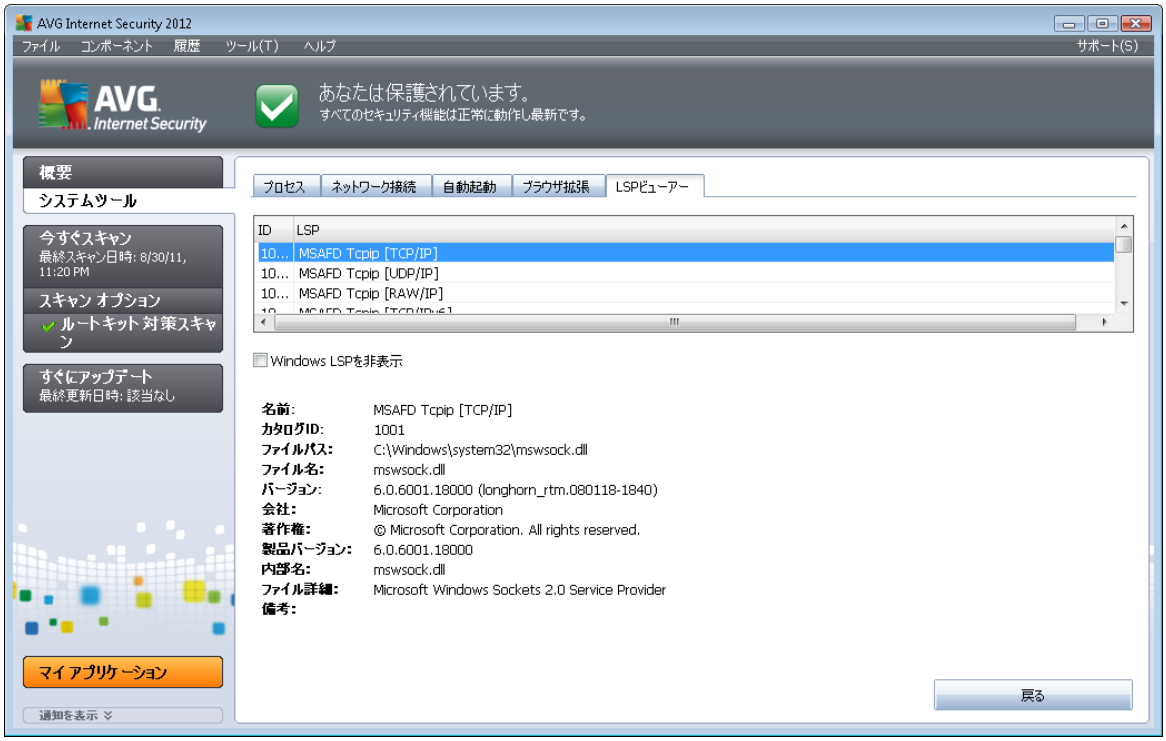
コントロールボタン

[***ブラウザ拡張***] タブで利用できるコントロール ボタンは次のとおりです。

- ***選択したオブジェクトの削除*** - 現在リストで強調表示されているプラグインを削除します。
  脅威であることが確実である場合以外は、リストからプラグインを削除しないことを強く推奨します。

- ***戻る*** - 既定の AVG メイン ダイアログ *(コンポーネント概要)に戻ります。*

6.6.5. LSP ビューア



LSP ビューアー ダイアログでは、レイヤードサービスプロバイダ(LSP)のリストが表示されます。

レイヤードサービスプロバイダ (LSP)は、Windowsオペレーティングシステムのネットワークサービスにリンクしたシステムドライバです。これは、データの修正を含め、コンピュータに入出力されるすべてのデータにアクセスします。一部のLSPでは、Windowsによりコンピュータがインターネットを含めた他のコンピュータに接続できるように許可する必要があります。ただし、あるマルウェアは、それ自体をLSPとしてインストールし、コンピュータが送信するすべてのデータにアクセスする可能性があります。したがって、このレビューはすべてのLSPの脅威をチェックする上で役に立つかもしれません。

また、ある状況下では、壊れたLSP *(例えば、ファイルは除去されたがレジストリエントリが残っている場合等)*を修復できることもあります。修復可能なLSPが検出された場合にのみ、問題解決のためのボタンが表示されます。

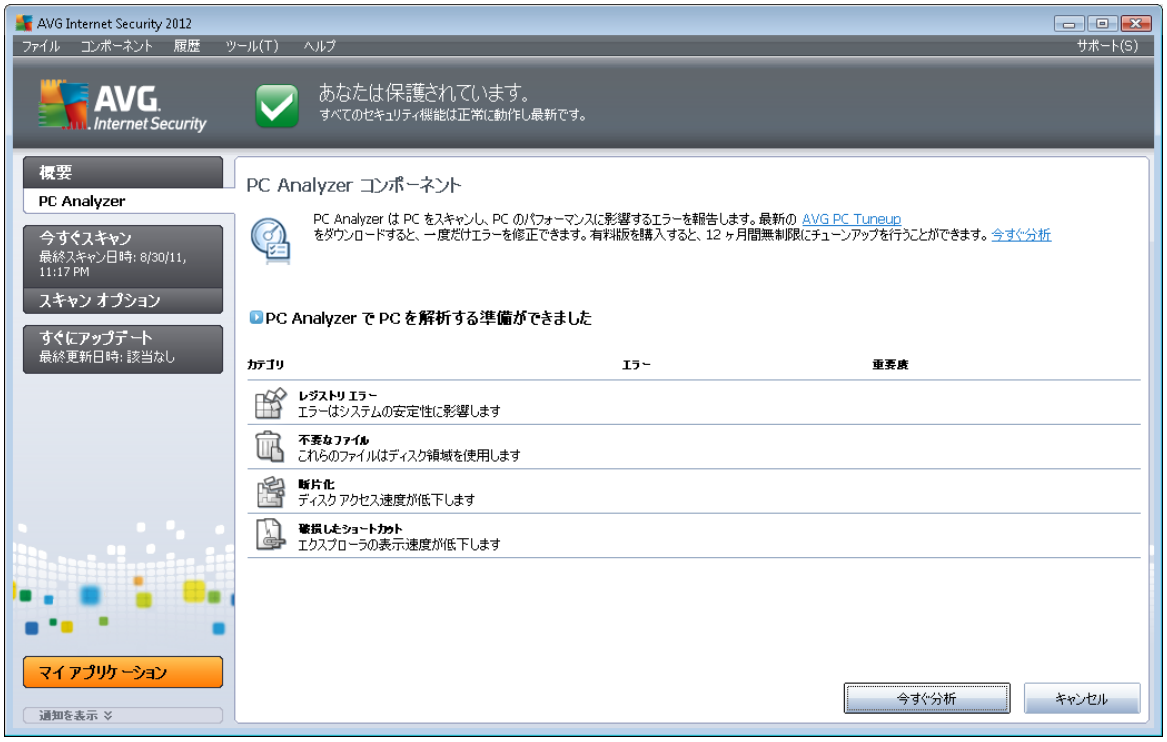
コントロール ボタン

[***LSP ビューア***] タブで利用できるコントロール ボタンは次のとおりです。

- ***Windows LSP を表示しない*** - Windows LSP をリストに表示するにはこの項目をクリアします。
- ***戻る*** - 既定の AVG メイン ダイアログ(*コンポーネント概要*)に戻ります。

6.7. PC Analyzer

PC Analyzer コンポーネントではコンピュータをスキャンし、システムの問題があるかどうかを確認します。コンピュータ全体のパフォーマンスを集約したわかりやすい概要が表示されます。コンポーネントのユーザー インターフェースには、レジストリエラー、不要なファイル、断片化、破損したショートカットの各カテゴリを示す 4 つの線で区別されたグラフが表示されます。



- ***レジストリエラー***は、Windows レジストリの数を示します。レジストリの問題を解決するには高度な知識が必要であるため、レジストリ修正を自分で行わないことをお勧めします。
- ***不要なファイル***は、不要な可能性が高いファイルの数を示します。一般的には、各種一時ファイルやごみ箱のファイルが不要なファイルとして判断されます。
- ***断片化***では、長期間の使用により物理ディスクのいたるところに分散して断片化したハードディスクの割合を計算します。デフラグ ツールを使用してこの問題を解決できます。
- ***破損したショートカット***は、動作しないショートカットや存在しない場所へのショートカットなどの問題を示します。

システムの分析を開始するには、[***今すぐ分析***] ボタンをクリックします。次に、分析の進行状況と分析結果がグラフに直接表示されます。

結果概要には、検出されたシステム上の問題 (***エラー***) の数が各検査済みカテゴリに従って分類された形で表示されます。分析結果は [***重要度***] 列の軸上にグラフィカルに表示されます。

コントロール ボタン

- ***今すぐ分析*** (*分析前に表示*) - このボタンをクリックすると、コンピュータの分析をただちに実行します。
- ***今すぐ修正*** (*分析完了時に表示*) - このボタンをクリックすると、AVG Web サイト (http://www.avg.com/) の ***PC Analyzer*** コンポーネントに関する最新詳細情報を提供するページが開きます。
- ***キャンセル*** - このボタンをクリックすると、分析の実行を停止するか、分析完了時に既定の AVG メイン ダイアログ (*コンポーネント概要*) に戻ります。

6.8. Identity Protection

Identity Protection はマルウェア対策コンポーネントであり、*スパイウェア、ボット、ID 窃盗*などのあらゆる種類のマルウェアに対する保護を提供します。行動分析技術を使用して、発生したばかりの新しいウイルスに対する保護を提供します。***Identity Protection*** は ID 窃盗によるパスワード、銀行アカウント情報、クレジットカード番号、その他の貴重な個人デジタル情報の窃盗を防止することに特化しています。PC を狙うあらゆる種類の悪意のあるソフトウェア (*マルウェア*) を対象とします。PC 上のすべてのプログラムが正常に動作していることを確認します。***Identity Protection*** は継続的に疑わしい動作を検出およびブロックし、あらゆる新しいマルウェアからコンピュータを保護します。

Identity Protection は新しく未知の脅威に対するリアルタイムのコンピュータ保護を提供します。このコ

ンポーネントはすべてのプロセス *(非表示のプロセスを含む)* と286 以上の異なる動作パターンを監視し、システム内で悪意のある活動が発生しているかどうかを判断できます。このため、ウィルス データベースにはまだ登録されていない脅威でも検出できます。不明なコードがコンピュータに侵入すると、悪意のある動作の監視と追跡が即時実行されます。ファイルが悪意のあるものだと判定された場合、***Identity Protection*** はコードをウイルス隔離室に除去し、システムで実行された変更 *(コード挿入、レジストリ変更、ポート オープンなど)* すべてを元に戻します。保護を適用するためにスキャンを実行する必要はありません。この技術はきわめて積極的な保護であるため、アップデートはほとんど必要ありません。常に保護が適用されています。

Identity Protection はウイルス対策を補完する保護機能です。両方のコンポーネントをインストールして、PC の保護を完全にすることを強くお勧めします。

6.8.1. Identity Protection インターフェース

[***Identity Protection***] ダイアログには、コンポーネントの基本機能、ステータス *(アクティブ)*、統計情報データの概要が表示されます。

- ***除去された脅威アイテム*** - マルウェアとして検出され除去されたアプリケーションの数を表示します
- ***監視されているプロセス*** - Identity Protection によって監視されている現在実行中のアプリケーションの数
- ***監視されている動作*** - 監視されているアプリケーションで実行中の特定のアクションの数

下には [監視プロセスと活動モニターを表示する] リンクがあり、システム ツール コンポーネントのユーザーインターフェースに移動します。このインターフェースでは、すべての監視プロセスの詳細概要が表示されます。

基本 Identity Protection 設定

ダイアログの下部では、コンポーネントの基本機能の一部を編集できます。

- ***Identity Protection*を有効化** - (*既定ではオン*): チェックを付けると、Identity Protection コンポーネントがアクティブになり、詳細編集オプションが開きます。

場合によっては、***Identity Protection***が問題のないファイルを、不審なファイルまたは危険なファイルとして報告する場合があります。***Identity Protection***は脅威の動作に基づいて脅威を検出します。通常は、プログラムがキーの押下を監視しようとしている場合、他のプログラムをインストールしようとしている場合、コンピュータに新しいドライバがインストールされる場合に検出します。したがって、不審な活動が検出された場合に、***Identity Protection***コンポーネントの動作を指定する次のオプションのいずれかを選択してください。

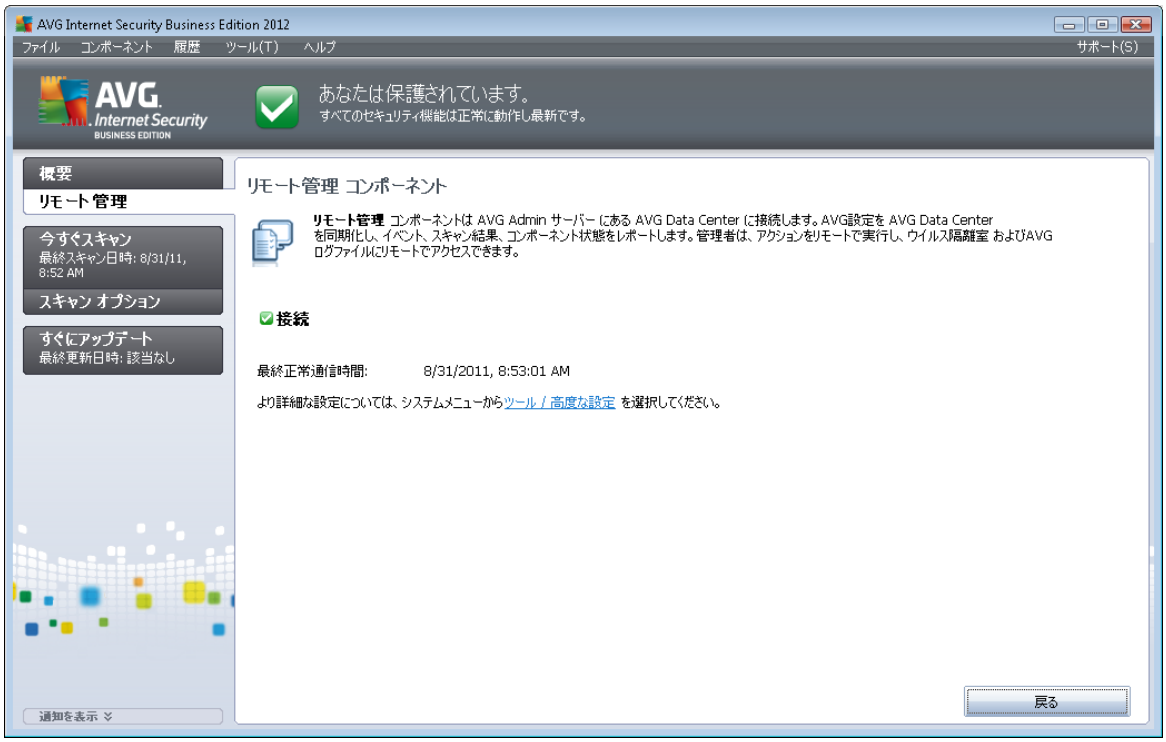
  - ***常にプロンプトを表示*** - アプリケーションがマルウェアとして検出された場合、アプリケーションをブロックするかどうかを確認するプロンプトが表示されます (*このオプションはデフォルトではオンになっています。特に理由がない限り、変更しないことをお勧めします*)。
  - ***自動的に検出された脅威を隔離*** - マルウェアとして検出されたすべてのアプリケーションは自動的にブロックされます
  - ***自動的に既知の脅威を隔離*** - 絶対的に確実にマルウェアとして検出されたアプリケーションのみをブロックします。

コントロールボタン

Identity Protectionインターフェースで利用できるコントロールボタンは以下の通りです。

- ***変更の保存*** - このボタンをクリックすると、ダイアログで行われた変更を保存して適用します。
- ***戻る*** - このボタンをクリックすると、既定の AVG メイン ダイアログ (*コンポーネント概要*) に戻ります

6.9. リモート管理



リモート管理 コンポーネントは、製品の Business Edition をインストールした場合にのみ、**AVG Anti-Virus 2012** のユーザー インターフェースに表示されます。*インストールで使用されたライセンス情報については、[サポート] システム メニュー項目から開く[情報] ダイアログの [バージョン] タブを参照してください。*[***リモート管理***] コンポーネント ダイアログでは、コンポーネントがアクティブであるかどうか、サーバーに接続しているかどうかに関する情報が表示されます。. ***遠隔管理*** コンポーネントは [***高度な設定/遠隔管理***] で設定できます。

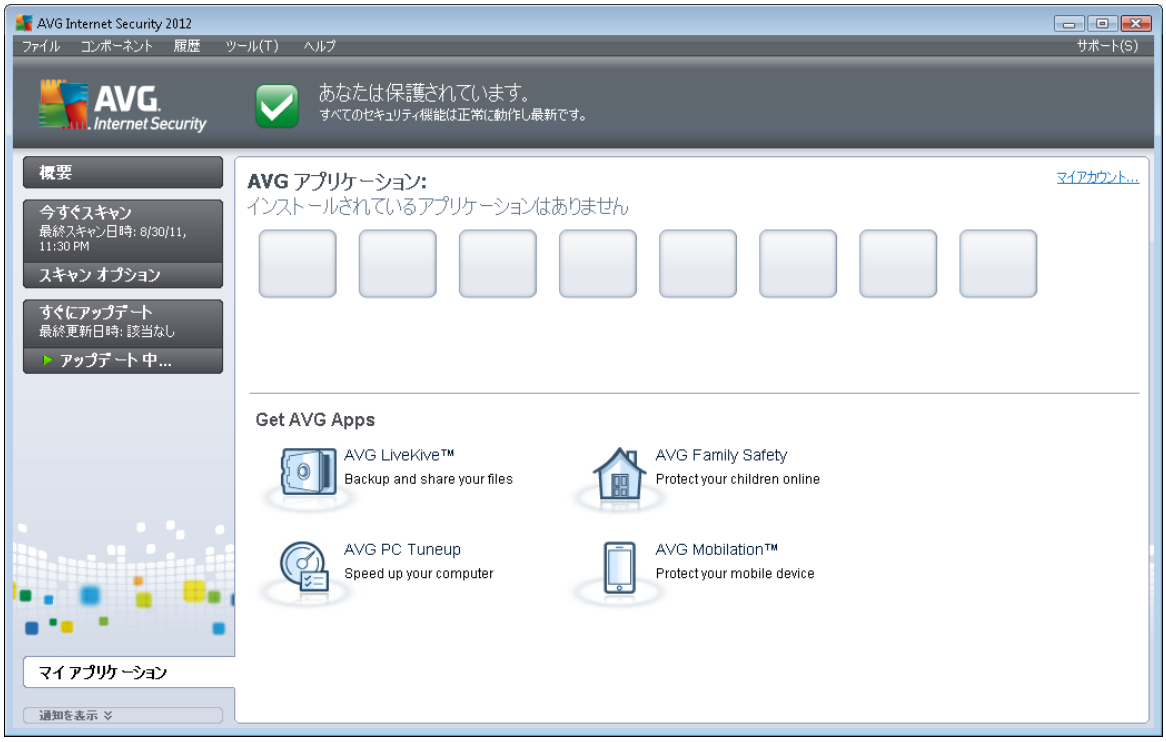
コンポーネントのオプションとAVG Remote Administration システムの機能については、このトピック専用の特定のマニュアルを参照してください。このマニュアルは AVG Web サイト (http://www.avg.com/) の***サポート センター/ ダウンロード/ マニュアル*** セクションからダウンロードできます。

コントロール ボタン

- ***戻る*** - このボタンをクリックすると、既定の AVG メイン ダイアログ (コンポーネント概要

7. マイ アプリケーション

LiveKive、Family Safety、PC Tuneup アプリケーションはそれぞれ単体の AVG 製品として提供されていますが、**AVG Anti-Virus 2012** インストールにも含まれています。[***AVG アプリケーション***] ダイアログ *(AVG メイン ダイアログの [マイ アプリケーション] ボタンをクリックすると直接開きます)* には、すでにインストールされたアプリケーションの概要が表示されます。また、任意で次のアプリケーションをインストールできます。



7.1. LiveKive

LiveKive は安全なサーバーでのオンライン データ バックアップ専用です。***LiveKive*** は自動的にすべてのファイル、写真、音楽を安全な場所にバックアップします。家族や友人と共有したり、iPhone や Android デバイスなどのあらゆる Web 対応デバイスからアクセスしたりできます。***LiveKive*** 機能は次のとおりです。

- コンピュータやハードディスクが破損した場合の安全対策
- インターネットに接続するすべてのデバイスからアクセス可能
- 簡単な整理
- 許可したユーザーと共有

詳細については、専用の AVG Web ページをご覧ください。コンポーネントをすぐにダウンロードすることもできます。[マイ アプリケーション] ダイアログの LiveKive リンクをクリックすると、専用ページに移動します。

7.2. ファミリー セーフティ

Family Safety は不適切な Web サイト、メディア コンテンツ、オンライン検索から子供を守り、オンライン活動に関するレポートを提供します。子供に合わせて適切な保護レベルを設定し、一意のログイン ID で個別に監視します。

詳細については、専用の AVG Web ページをご覧ください。コンポーネントをすぐにダウンロードすることもできます。[マイ アプリケーション] ダイアログのファミリー セーフティ リンクをクリックすると、専用ページに移動します。

7.3. PC チューンアップ

PC チューンアップ アプリケーションは詳細システム分析と訂正用の高度なツールです。このツールはコンピュータの速度とパフォーマンスを改善する方法を分析します。***PC チューンアップ*** の機能は次のとおりです。

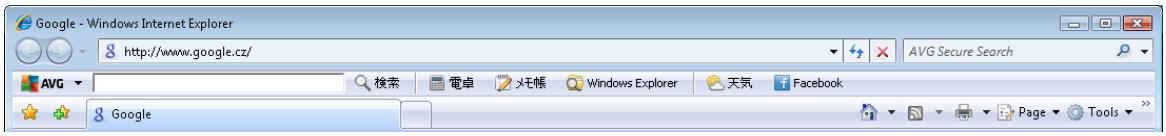
- ディスク クリーナー - コンピュータの速度を低下させる不要なファイルを削除します。
- ディスク デフラグ - ディスク ドライブをデフラグ処理し、システム ファイルの配置を最適化します。
- レジストリ クリーナー - レジストリエラーを修復して PC の安定性を高めます。
- レジストリ デフラグ - レジストリを圧縮しメモリを消費するギャップを解消します。
- ディスク ドクター - 不良セクター、失われたクラスタ、ディレクトリエラーを検出して修正します。
- インターネット オプティマイザ - 特定のインターネット接続に対するオールインワンの設定をカスタマイズします。
- トラック イレイザー - コンピュータとインターネット使用状況に関する履歴を削除します。
- ディスク ワイパー - ディスクの空き領域をワイプし、重要データの回復を防止します。
- ファイル シュレッダー - ディスクまたは USB スティックのデータを回復できないように選択したファイルを消去します。
- ファイル リカバリ - 誤ってディスク、USB スティック、カメラから削除したファイルを回復します。
- 重複ファイル ファインダー - ディスク領域の無駄となる重複したファイルを検索して削除します。
- サービス マネージャ - コンピュータの速度を低下させる不要なサービスを無効にします。
- スタートアップ マネージャ - ユーザーによる Windows 起動時に自動起動するプログラムの管理を可能にします。
- アンインストール マネージャ - 不要なソフトウェア プログラムを完全にアンインストールします。
- 調整マネージャ - ユーザーによる多数の非表示の Windows 設定の調整を可能にします。

- タスク マネージャ - すべての実 行 中 のプロセス、サービス、ロックされたファイルの一 覧 を表 示 します。
- ディスク エクスプローラ - コンピュータの領 域 を最 も占 有 しているファイルを表 示 します。
- システム情 報 - インストールされているハードウェアとソフトウェアに関 する詳 細 情 報 を表 示 します。

詳 細 については、専 用 の AVG Web ページをご覧 ください。コンポーネントをすぐにダウンロードすることもできます。[マイ アプリケーション] ダイアログの PC チューンアップ リンクをクリックすると、専 用 ページに移 動 します。

8. AVGセキュリティツールバー

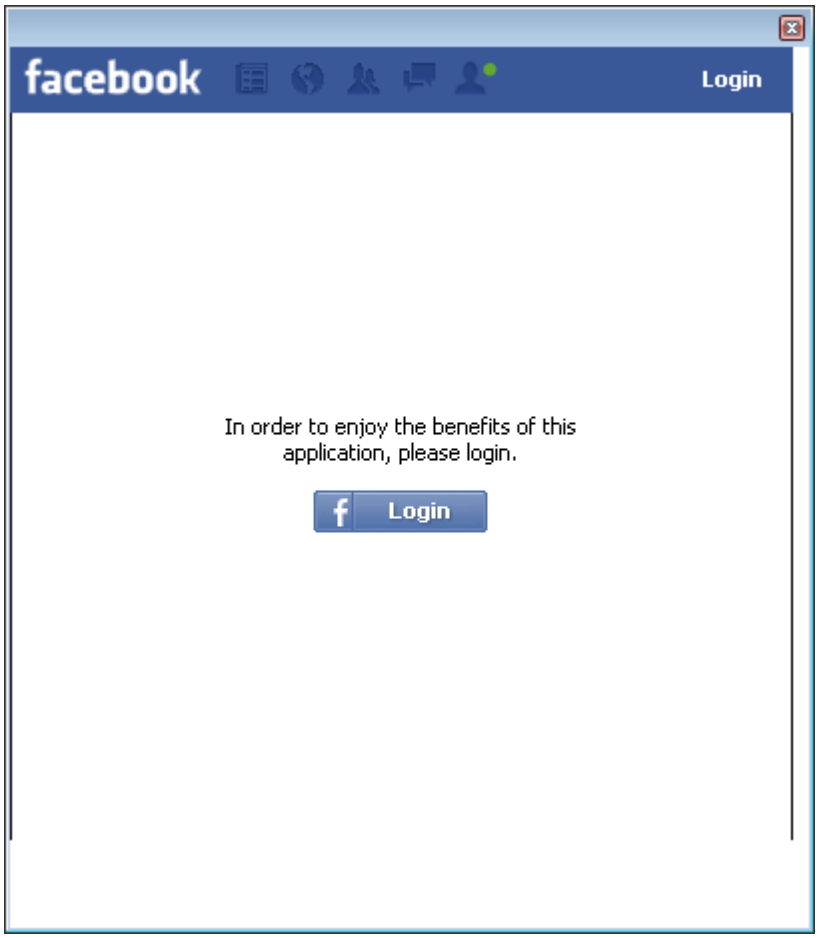
AVG セキュリティツールバーはリンクスキャナ コンポーネントと強力に連携し、インターネット閲覧中の最大限のセキュリティを保証するツールです。**AVG Anti-Virus 2012** では ***AVG セキュリティツールバー***のインストールは任意です。インストール処理中にこのコンポーネントをインストールするかどうかを確認します。***AVG セキュリティツールバー***はインターネット ブラウザから直接利用できます。現在、Internet Explorer (*バージョン6.0 以上*) および Mozilla Firefox (*バージョン3.0 以上*) のインターネット ブラウザに対応しています。*別のインターネットブラウザ (例: Avant ブラウザ) を使用している場合は、予期しない動作を起こす場合があります。*



AVG セキュリティツールバーは次の項目から構成されています。

- ***AVG ロゴ***とドロップダウン メニュー:
  - ***AVG セキュア サーチを使用する*** - ***AVG セキュア サーチ***エンジンを使用した ***AVG セキュリティツールバー***による直接検索を許可します。すべての検索結果はサーチ シールド サービスによって継続的に確認され、オンラインの安全性が確実に保証されます。
  - ***現在の脅威 レベル*** - Web 上の現在の脅威レベルをグラフィカルに表示したウイルス ラボの Web ページを開きます。
  - ***AVG 脅威 ラボ*** - AVG Web サイト (http://www.avg.com/) の [***サイト レポート***] ページ Web サイトが開きます。このサイトで脅威名を入力すると、特定の脅威を検索し、各脅威の詳細情報を確認できます。
  - ***ツールバー ヘルプ*** - すべての ***AVG セキュリティツールバー***の機能に対応しているオンライン ヘルプを開きます。
  - ***製品 フィードバックの送信*** - Web ページのフォームが開き、***AVG セキュリティツールバー***についてのご意見を入力できます。
  - ***AVG セキュリティツールバーについて...*** - 新しいウィンドウが開き、現在インストールされたいるバージョンの ***AVG セキュリティツールバー***に関する情報が表示されます。
- ***検索 フィールド*** - ***AVG セキュリティツールバー***を使用してインターネットを検索します。表示される検索結果は絶対に安全であるため、安全性と快適性が保証されます。検索フィールドにキーワードまたはフレーズを入力して、[***検索***] ボタンをクリックするか *Enter* キーを押します。すべての検索結果がサーチ シールド サービス (*リンクスキャナ コンポーネント*) によって継続的にチェックされます。
- 次のアプリケーションへのクイック アクセス ショートカット ボタン: ***電卓***、***メモ帳***、***Windows エクスプローラ***
- ***天気*** - このボタンをクリックすると、新しいダイアログが開き、選択したロケーションの現在の天気と2日間の天気予報が表示されます。この情報は 3 ～ 6 時間ごとに定期的に更新され

ます。このダイアログでは、目的のロケーションを手動で変更したり、気温を摂氏で表示するか華氏で表示するかを選択したりできます。



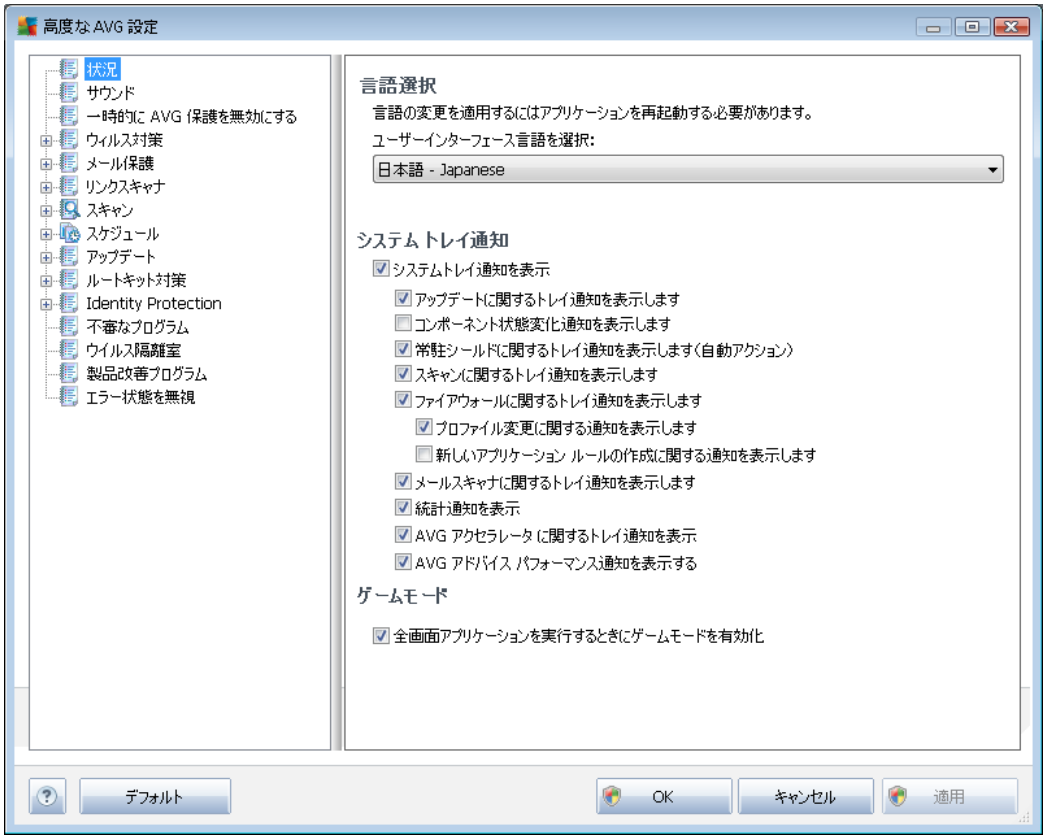
- ***Facebook*** - このボタンをクリックすると、***AVG セキュリティツールバー***から直接 Facebook ソーシャル ネットワークに接続できます。*動作*

9. AVG 高度な設定

AVG Anti-Virus 2012 の高度な設定ダイアログは [***高度な AVG 設定***] という名前の新しいダイアログで開きます。 このウィンドウは2つのセクションにわかれています。左部はにツリー状のナビゲーションが表示されます。設定を変更したいコンポーネントを選択すると、ウィンドウ右側に設定項目が表示されます。

9.1. 表示

ナビゲーション ツリーの最初の項目である [***表示***] は**AVG Anti-Virus 2012** ユーザー インターフェースの全般設定を参照し、アプリケーションの動作の基本オプションを示します。

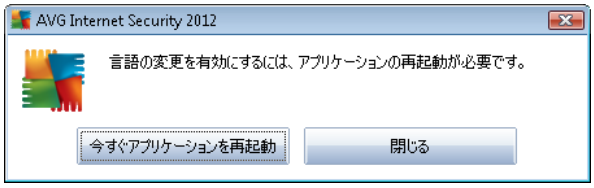


言語選択

[***言語選択***] セクションでは、任意の言語をドロップダウン メニューから選択できます。選択した言語は、**AVG Anti-Virus 2012** ユーザー インターフェース全体で使用されます。ドロップダウン メニューには、インストール処理中に選択した言語 (**** カスタム オプション* の章を参照) と英語 (*既定で自動的にインストール*) のみが表示されます。**AVG Anti-Virus 2012** の言語切り替えが完了した場合は、アプリケーションを再起動する必要があります。次の手順を実行してください。

- ドロップダウン メニューで任意のアプリケーション言語を選択します。
- [***適用***] ボタン (ダイアログの右下端) をクリックして選択内容を確定します。

- [***OK***] ボタンをクリックして、確定します。
- 新しいダイアログがポップアップ表示され、アプリケーションの言語を変更するには**AVG Anti-Virus 2012**
- [***今すぐアプリケーションを再起動***] ボタンをクリックしてプログラムの再起動を許可し、その後すぐに言語変更が有効になります。



システム トレイ通知

このセクションでは、**AVG Anti-Virus 2012** アプリケーションのステータスに関するシステム トレイ通知を非表示に設定できます。既定ではシステム通知の表示は有効です。この設定を保持することを強くお勧めします。システム通知は、スキャンまたは更新プロセスの実行や **AVG Anti-Virus 2012** コンポーネントのステータス変更などを通知します。このような通知には特に注意をする必要があります。

ただし、なんからの理由で、このような方法で通知しない場合や、ある通知 (特定の AVG Anti-Virus 2012 コンポーネントに関する) のみを表示する場合は、次のオプションのにより任意の内容を定義および指定できます。

- ***システム トレイ通知を表示する****(既定では有効)* - 既定ではすべての通知が表示されます。この項目のチェックを外すとすべてのシステム通知表示は無効になります。オンにした場合は、表示する通知を選択できます。
  - ***アップデート****に関するトレイ通知を表示する(既定では有効)* - 更新処理の起動、進行、完了に関する情報を表示するかどうかを決定します。**AVG Anti-Virus 2012**
  - ***コンポーネントの状態変化に関するトレイ通知を表示する****(既定では無効)* - コンポーネントの有効/無効または問題の可能性に関する情報を表示するかどうかを決定します。コンポーネントの不具合状態をレポートする際、このオプションは、システム トレイ アイコンと同等のものとなります。**AVG Anti-Virus 2012**
  - ***常駐シールド関連のトレイ通知を表示する(自動アクション)****(既定では有効)* - ファイルの保存、コピー、開く処理に関する情報を表示するかどうかを決定します (*この設定は、常駐シールドの [自動修復] オプションが選択されている場合にのみ有効です*)。
  - ***スキャン****に関するトレイ通知を表示する(既定では有効)* - *スケジュールされたスキャンの自動起動、進行、結果に関する情報を表示するかどうかを決定します。*
  - ***ファイアウォール****に関するトレイ通知を表示する(既定では有効)* - ファイアウォール状態とプロセスに関する情報を表示するかどうかを決定します。たとえば、コンポーネントの有効化/非有効化警告、トラフィックのブロックなどが表示されます。この項目にはさらに 2 つの選択オプションがあります *(各オプションの詳細については、このマニュアルの「*

ファイアウォール」の章を参照してください)。

- ***プロファイル変更に関する通知を表示する****(既定では有効)* - ファイアウォール プロファイルの自動変更を通知します。

- ***新しく作成されたアプリケーション ルールに関する通知を表示する****(既定では無効)* - 安全なリストに基づく新しいアプリケーション ファイアウォール ルールの自動作成を通知します。

o ***メール スキャナ*****に関するトレイ通知を表示する***(既定では有効)* - すべての送受信メールに関する情報を表示するかどうかを決定します。

o ***統計情報通知を表示する****(既定では有効)* - このオプションにチェックを付けると、定期的な統計情報確認通知をシステム トレイに表示できます。

o ***AVG Accelerator に関するトレイ通知を表示する****(既定では有効)* - ***AVG Accelerator*** 動作に関する通知を表示するかどうかを決定します。***AVG Accelerator*** はオンライン ビデオのサービスをスムーズにして、ダウンロードを簡単にするサービスです。

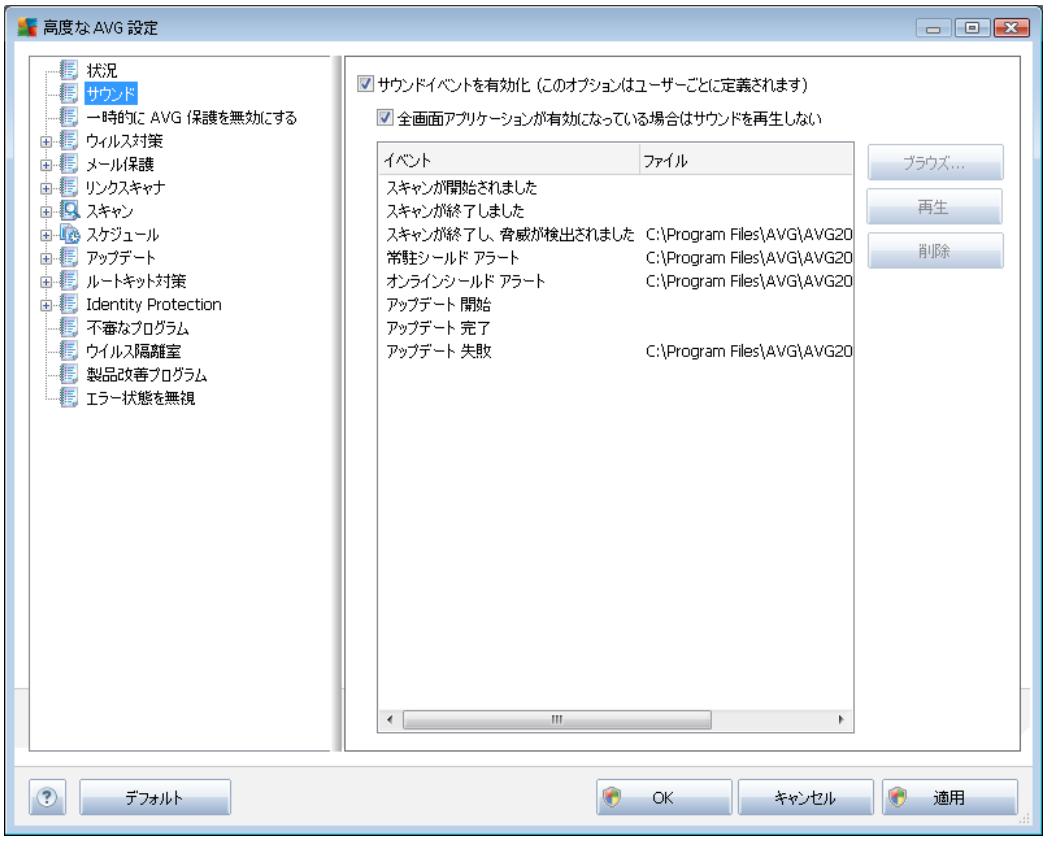
o ***AVG Advice のパフォーマンス通知を表示する****(既定では有効)* - ***AVG Advice*** はサポートされているインターネット ブラウザ *(Internet Explorer、Chrome、Firefox、Opera、Safari)* のパフォーマンスを監視し、ブラウザのメモリ消費量が推奨量を超えた場合に通知します。このような状況ではコンピュータのパフォーマンスが大幅に低下するおそれがあるため、インターネット ブラウザを再起動してプロセスを高速化することが推奨されます。通知を表示する場合は、***AVG Advice のパフォーマンス通知*** 項目を選択した状態にします。

ゲーム モード

この AVG 機能は、AVG 情報バルーン *(スケジュール スキャンが開始するときなどに表示)* によって妨害される可能性がある全画面アプリケーション用に設計されています *(情報バルーンはアプリケーションの最小化やグラフィックの破損を引き起こす可能性があります)*。このような問題を回避するには、 [***全画面アプリケーションが実行されているときにゲームモードを有効にする***] オプションのチェックボックスを付けた状態にしておきます *(既定の設定)*。

9.2. サウンド

[***サウンド***] ダイアログでは、サウンド通知によって特定の **AVG Anti-Virus 2012** アクションの通知を行うかどうかを指定できます。



この設定は現在のユーザー アカウントでのみ有効です。つまり、各コンピュータ ユーザーに固有のサウンド設定が行われます。サウンド通知を有効にする場合は、[***サウンド イベントを有効にする***] オプションを選択 (*このオプションは既定では有効*) し、関連するすべてのアクションのリストを有効にします。さらに、[***全画面アプリケーションがアクティブのときにはサウンドを再生しない***] オプションを選択すると、サウンド通知が邪魔になるような状況でサウンド通知を非表示にすることができます *(このマニュアルの「高度な設定/表示」の章の「ゲーム モード」セクションを参照)*。

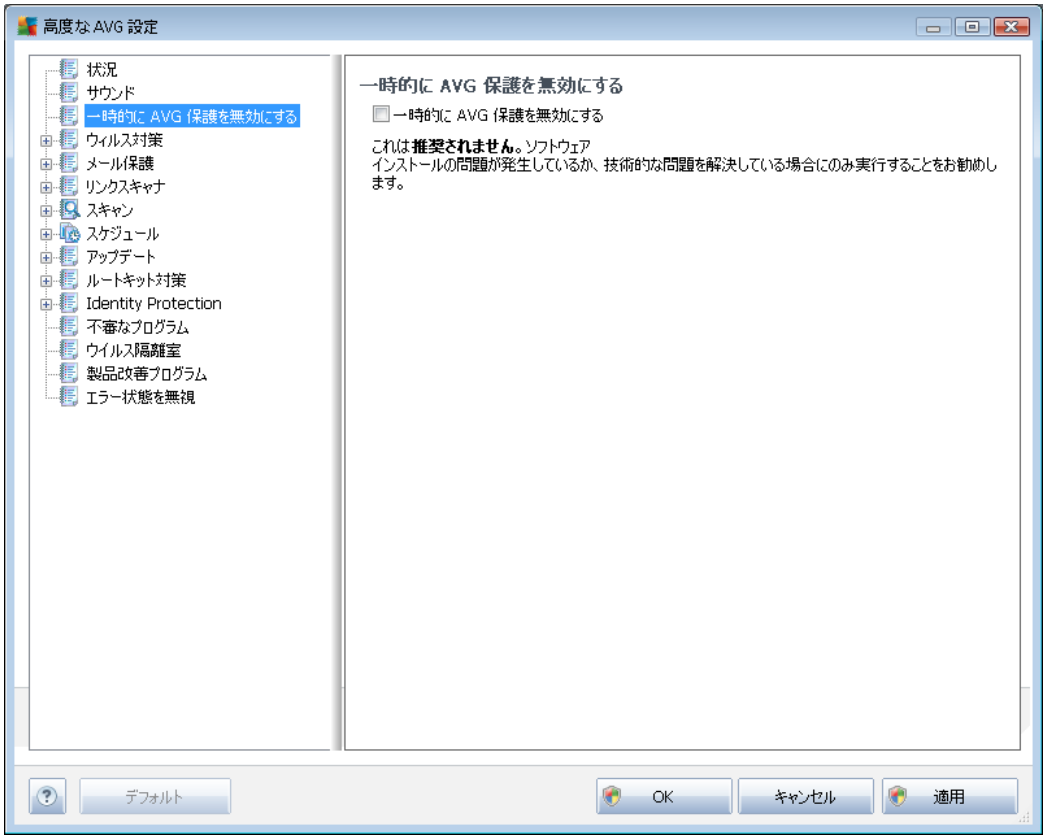
コントロール ボタン

- ***参照*** - リストから各イベントを選択し、[***参照***] ボタンをクリックすると、ディスクを参照してイベントに割り当てるサウンド ファイルを検索できます。*(現時点では、*.wav サウンドのみがサポートされています。)*
- 選択したサウンドを再生するには、リストのイベントを強調表示し、***[再生] ボタンをクリックします。***
- ***削除*** - [***削除***] ボタンをクリックすると、特定のイベントに割り当てられたサウンドを削除します。

9.3. 一時的に AVG 保護を無効にする

[***一時的に AVG 保護を無効にする***] ダイアログでは、**AVG Anti-Virus 2012** の保護機能すべてを一度にオフにすることができます。

やむを得ない場合を除き、このオプションの使用はお勧めしません。

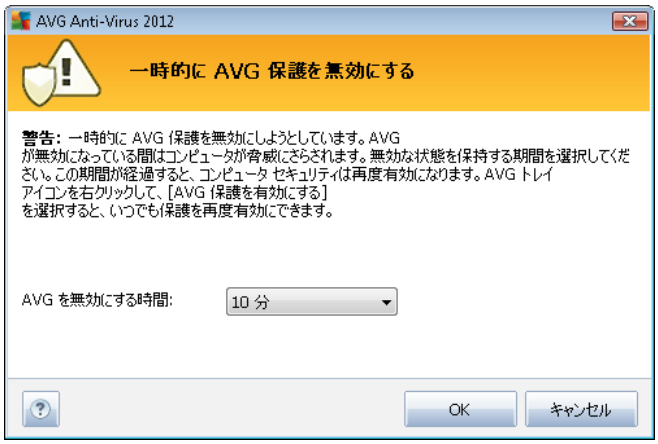


インストール処理中に望ましくない中断が発生しないようにするために、インストーラやソフトウェア ウィザードで実行中のプログラムやアプリケーションを終了するように指示される場合がありますが、それでも通常は新しいソフトウェアやドライバをインストールする前に、**AVG Anti-Virus 2012**を無効にする***必要はありません***。インストール中に問題が発生した場合は、まず常駐保護を無効にしてください (*常駐シールド*を有効にする)。**AVG Anti-Virus 2012** を一時的に無効にしなければならない場合は、必要な作業が終わったらすぐに再度有効にする必要があります。ウィルス対策ソフトウェアが無効な状態でインターネットやネットワークに接続している場合は、コンピュータが攻撃の危険にさらされています。

AVG 保護を一時的に無効にする方法

- [***一時的に AVG 保護を無効にする***] チェックボックスを選択して、[***適用***] ボタンをクリックして選択内容を確定します。
- 新しく開く[***一時的に AVG 保護を無効にする***] ダイアログで、**AVG Anti-Virus 2012**を無効にする時間を指定します。既定では、保護は 10 分間無効になります。新しいソフトウェアのインストールなどの一般的なタスクを実行するには十分な時間です。設定可能な初期上限

値は 15 分です。セキュリティ上の理由からこの値の上書きはできません。指定した時間が経過すると、無効にされたコンポーネントはすべて自動的に再度有効になります。

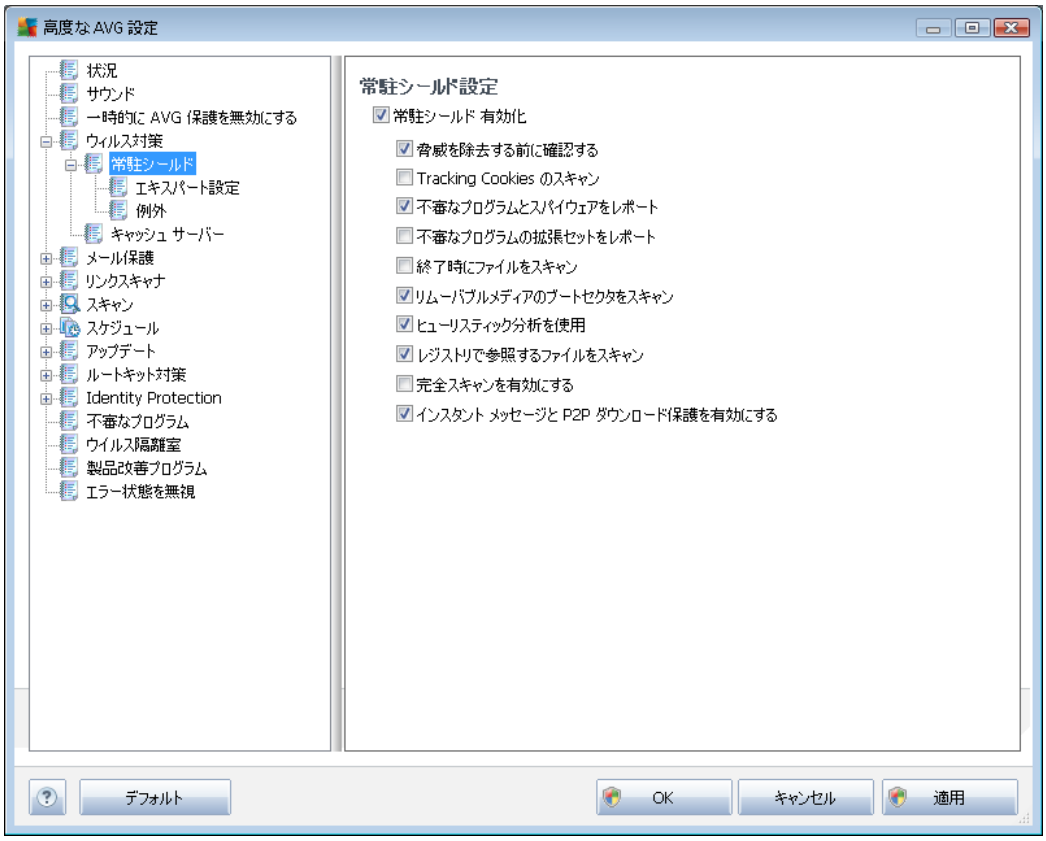


9.4. ウイルス対策

ここにトピックの文字を入力してください。

9.4.1. 常駐シールド

常駐シールドは、ウイルス、スパイウェア、他のマルウェアに対してファイルとフォルダをリアルタイムで保護します。



[***常駐シールド設定***] ダイアログでは、[***常駐シールドを有効化***] 項目 (*このオプションは既定では有効*) を有効/無効にして、常駐保護を完全に有効化または無効化できます。また、有効にする常駐保護機能を選択できます。

- ***Tracking Cookie をスキャンする*** (*既定ではオフ*) - このパラメータを指定すると、スキャン中に Cookies が検出されます。 (*HTTP cookies は、認証、トラッキング、サイトのプリファレンスや電子ショッピングカードの内容等の特定のユーザー情報の保持に使用されます*)

- ***不審なプログラムとスパイウェア脅威を報告する*** (*既定では有効*): チェックを付けると、スパイウェア対策エンジンを有効にし、ウイルスと同時にスパイウェアもスキャンします。スパイウェアは疑わしいマルウェアのカテゴリに含まれます。通常は、セキュリティリスクとなる場合でも、このようなプログラムを故意にインストールすることができます。コンピュータのセキュリティを高めるため、この機能を有効にしておくことをお勧めします。

- ***不審なプログラムの拡張セットを報告する*** (*既定ではオフ*) - 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。スパイウェアとは、直接製造元から入手する場合には、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誤用されるおそれのあるプログラムです。これは、コンピュータセキュリティ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。

- ***ファイルを閉じるときにスキャン***(*既定では無効*) - 終了時のスキャンを有効にすると、アクティブなオブジェクト (アプリケーションやドキュメントなど) の実行または終了時に AVG スキャンが実行されます。この機能はコンピュータを一部の高度なウイルスから保護する上で役立ちます。

- ***リムーバブル メディアのブート セクターをスキャンする*** - (*既定では有効*)

- ***ヒューリスティック分析を使用する*** - (*既定では有効*) ヒューリスティック分析 (*仮想コンピュータ環境でのスキャンオブジェクトの動的エミュレーション*) を使用して検出します。

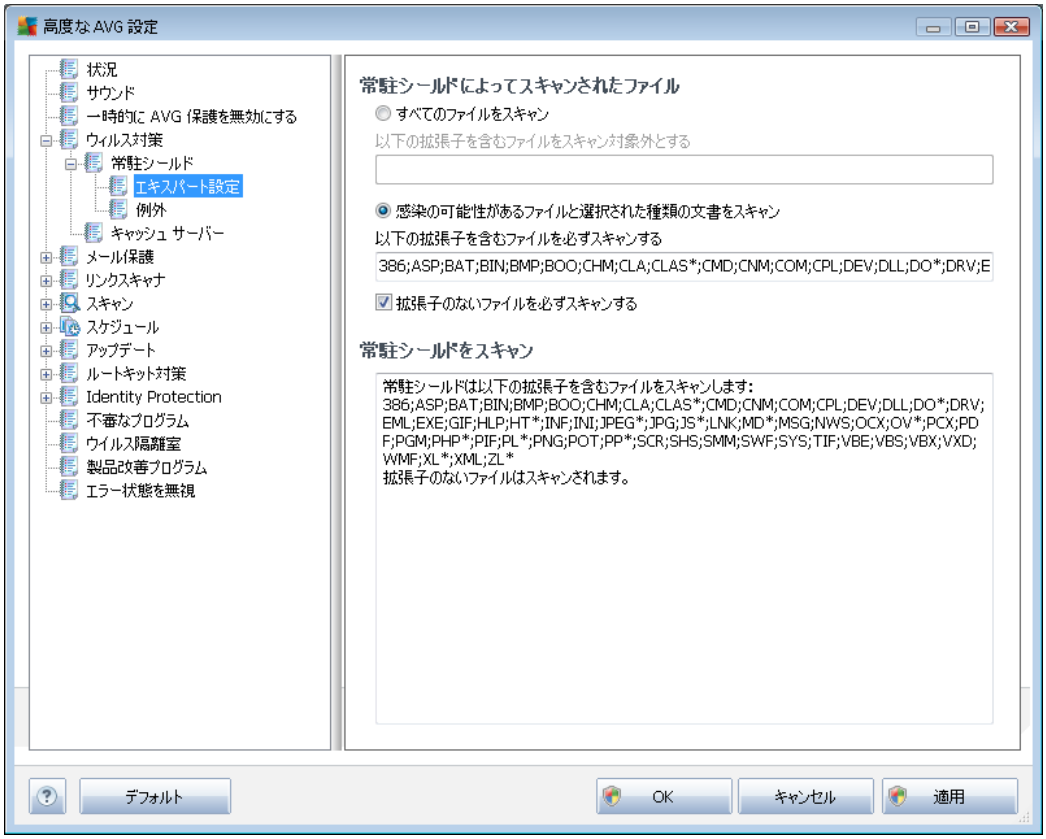
- ***すべての脅威を自動的に駆除する***(*既定では無効*) - 修復が可能な場合は、検出されたファイルはすべて自動的に修復されます。修復できない感染はすべて駆除されます。

- ***レジストリで参照されるファイルをスキャンする***(*既定では有効*) - このパラメータを定義すると、スタートアップ レジストリに追加されたすべての実行ファイルが AVG によってスキャンされるため、次回のコンピュータ再起動時に既知の感染が実行されることはありません。

- ***完全スキャンを有効にする***(*既定では無効*) - このオプションにチェックを付けると、特定の状況 (*緊急事態*) において最も完全なアルゴリズムを有効にして、脅威の原因となる可能性のあるすべてオブジェクトを徹底的にチェックします。この方法を実行すると多少時間がかかります。

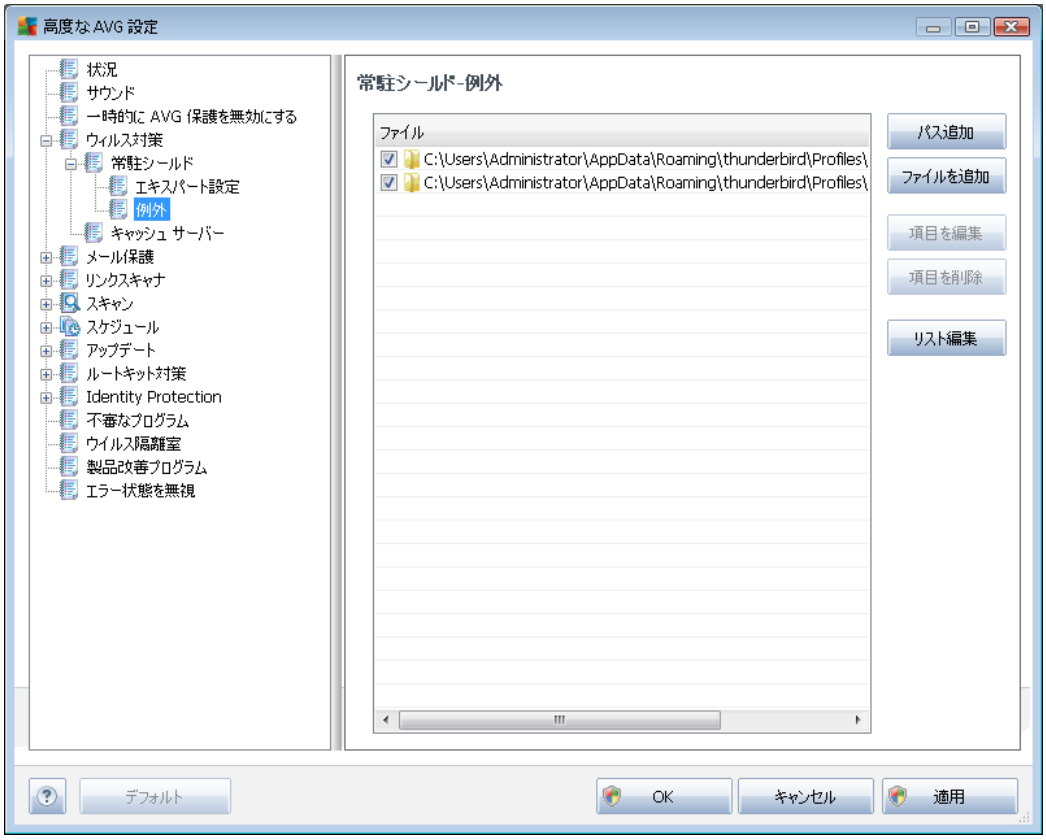
- ***インスタント メッセージ保護とP2P ダウンロード保護を有効にする***(*既定では有効*) - インスタント メッセージ通信 (*ICQ、MSN Messenger など...*) とP2P ダウンロードにウイルスが含まれない

[***常駐シールドによってスキャンされたファイル***] ダイアログでは、スキャン対象のファイルを*特定の拡張子を指定*して設定できます。



該当するチェックボックスを選択すると、***すべてのファイルをスキャン***するか、***感染可能なファイルと選択した種類のドキュメントのみをスキャン***するかどうかを決定します。後者のオプションを選択した場合は、スキャンから除外するファイルを定義する拡張子のリストと、あらゆる状況においてスキャンが必要なファイルを定義するファイル拡張子のリストを指定できます。

下の [***常駐シールドがスキャンするアイテム***] セクションには現在の設定がまとめて表示されます。***常駐シールド***が実際にスキャンするアイテムの詳細な概要が表示されます。



[***常駐シールド- 例外***] ダイアログでは、***常駐シールド***スキャンから除外されるフォルダを定義できます。

必要な場合を除き、すべての項目を含めることを強くお勧めします。

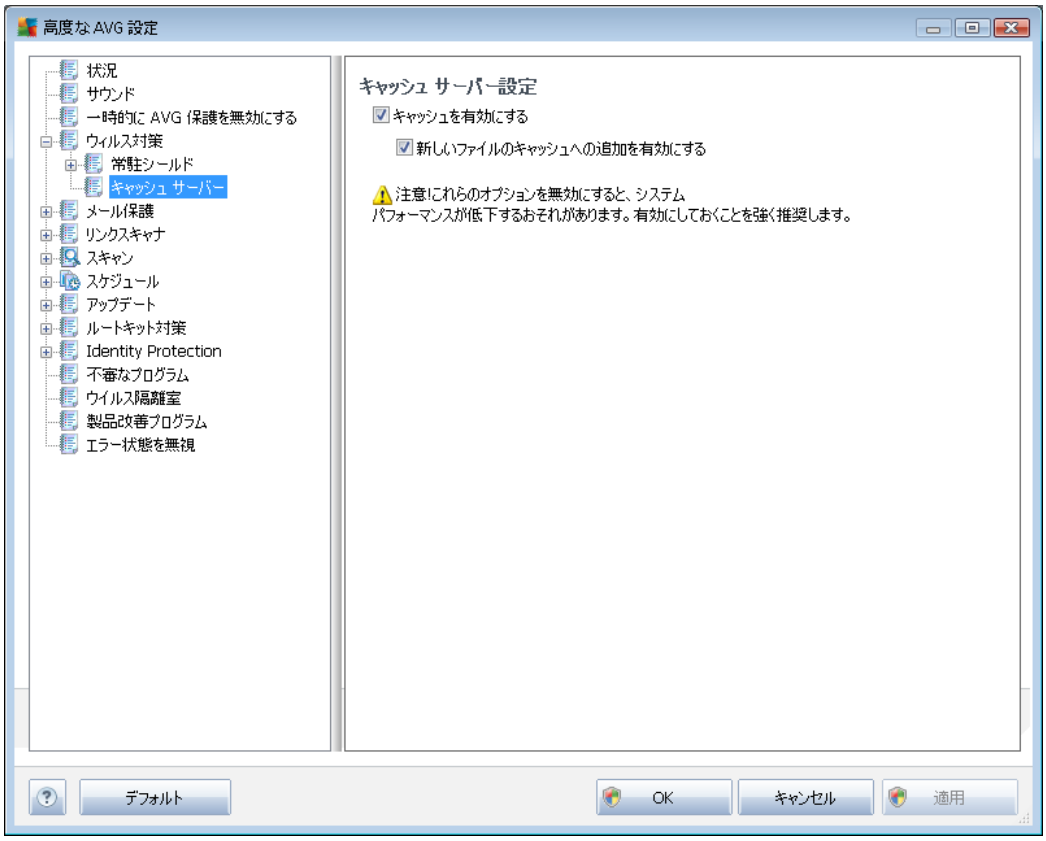
コントロール ボタン

ダイアログには次のコントロール ボタンがあります。

- ***パスの追加*** – ローカル ディスクのナビゲーション ツリーからディレクトリを 1 つずつ選択してスキャン対象から除外するディレクトリを指定します。
- ***ファイルの追加*** –ローカル ディスク ナビゲーション ツリーからファイルを 1 つずつ選択してスキャン対象から除外するファイルを指定します。
- ***項目の編集*** –選択したファイルまたはフォルダへの特定のパスを編集できます。
- ***項目の削除***–選択した項目へのパスをリストから削除できます
- ***リストの編集*** - 標準のテキスト エディタに近い新しいダイアログを使用して、定義された例外のすべてのリストを編集できます。

9.4.2. キャッシュ サーバー

[***キャッシュ サーバー設定***] ダイアログは、すべての種類の **AVG Anti-Virus 2012** スキャンを高速化するためのキャッシュ サーバー プロセスを参照します。



キャッシュ サーバーは信頼できるファイル (*信頼できるソースのデジタル署名があるファイルは信頼できるファイルと見なされます*) の情報を収集して保持します。これらのファイルは自動的に安全で再スキャンの必要がないファイルと見なされるため、スキャン中にスキップされます。

[***キャッシュ サーバー設定***] ダイアログには次の設定オプションがあります。

- ***キャッシュを有効にする*** (*デフォルトではオン*) - チェックを外すと、***キャッシュ サーバー***をオフに切り替え、キャッシュ メモリを空にします。最初に使用中のすべてのファイルが 1 つずつウィルスおよびスパイウェア スキャンされるため、スキャンの速度が低下し、コンピュータの全体的なパフォーマンスが低下する可能性があります。

- ***新しいファイルのキャッシュへの追加を有効にする*** (*デフォルトではオン*) - チェックを外すと、キャッシュ メモリへのファイルの追加を停止します。キャッシュを完全にオフにするか、次回のウィルス データベース アップデートまで、既にキャッシュに保存されたファイルのすべてが保持され使用されます。

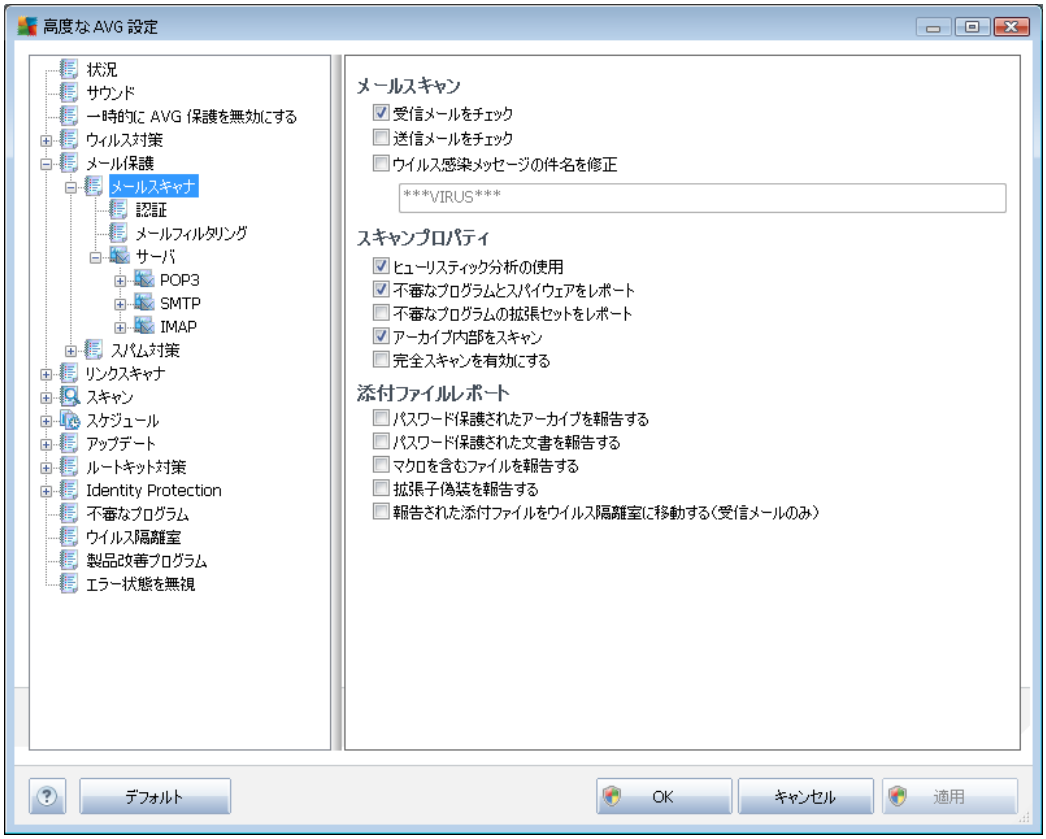
キャッシュ サーバーを無効にする理由がない場合は、既定の設定を保持し、両方のオプションを有効にすることを強くお勧めします。そうでない場合は、システムの速度とパフォーマンスが大幅に低下するおそれがあります。

9.5. メール保護

[***メール保護***] セクションでは、メール スキャナとスパム対策の詳細設定を編集できます。

9.5.1. メール スキャナ

メールスキャナダイアログは3つのセクションに分けられます。



メール スキャン

このセクションでは、送受信メールに関する基本項目を設定できます。

- ***受信電子メールをチェックする*** (*既定ではオン*) - このボックスを選択/クリアすることで、電子メール クライアントに配信されるすべての電子メール メッセージをスキャンするかどうかを選択します。
- ***送信電子メールをチェックする*** (*既定ではオフ*) - このボックスを選択/クリアすることで、自分のアカウントから送信されるすべての電子メール メッセージをスキャンするかどうかを選択します。
- ***ウィルス感染したメッセージの件名を修正する*** (*既定ではオフ*) - スキャンによって感染メッセージとして検出された電子メール メッセージに関する警告を表示する場合は、この項目にチェックを付け、テキスト フィールドに任意のテキストを入力します。このテキストがすべての感染電子メールの [件名] フィールドに追加されるため、感染メッセージを簡単に識別し除外できます。初期値は***VIRUS*** です。この値の使用をお勧めします。

スキャン プロパティ

このセクションでは、電子メール メッセージのスキャン方法を指定できます。

- ***ヒューリスティック分析を使用する*** (*既定ではオン*) - チェックを付けると、電子メール メッセージをスキャンするときにヒューリスティック検出方式使用します。このオプションをオンにすると、拡張子だけでなく実際の添付ファイルの内容も考慮して、電子メールのメール添付ファイルをフィルタできます。フィルタリングは [メール フィルタリング] ダイアログで設定できます。

- ***不審なプログラムとスパイウェア脅威を報告する*** (*既定ではオン*) - チェックを付けると、スパイウェア対策エンジンを有効化し、ウイルスと同時にスパイウェアもスキャンします。スパイウェアは疑わしいマルウェアのカテゴリに含まれます。通常は、セキュリティリスクとなる場合でも、このようなプログラムを故意にインストールすることができます。コンピュータのセキュリティを高めるため、この機能を有効にしておくことをお勧めします。

- ***不審なプログラムの拡張セットを報告する*** (*既定ではオフ*) - 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。スパイウェアとは、直接製造元から入手する場合には、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誤用されるおそれのあるプログラムです。これは、コンピュータセキュリティ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。

- ***アーカイブ ファイルの内容をスキャンする*** (*既定ではオン*) – チェックを付けると、電子メール メッセージに添付されたアーカイブ ファイルの内容をスキャンします。

- ***完全スキャンを有効にする*** (*既定ではオフ*) - このオプションをチェックすると、特定の状況 (*コンピュータがウィルスやエクスプロイトに感染している疑いがある場合など*) が発生した場合に最も完全なスキャン アルゴリズムを有効にし、感染の可能性が非常に低いコンピュータ領域もスキャンします。これにより、問題がないことを確実に確認します。この方法を実行すると多少時間がかかります。

添付ファイル レポート

このセクションでは、潜在的に危険なファイルまたは不審なファイルに関する追加レポートを設定できます。警告ダイアログは表示されませんのでご注意ください。認証テキストのみがメールの最後に追加されます。このようなレポートはメール スキャナ検出ダイアログにリストされます。

- ***パスワード保護されたアーカイブを報告する*** - パスワードで保護されたアーカイブ (ZIP、RAR など)のウイルス スキャンはできません。ボックスにチェックを付けると、潜在的に危険なオブジェクトとしてこのようなアーカイブを報告します。

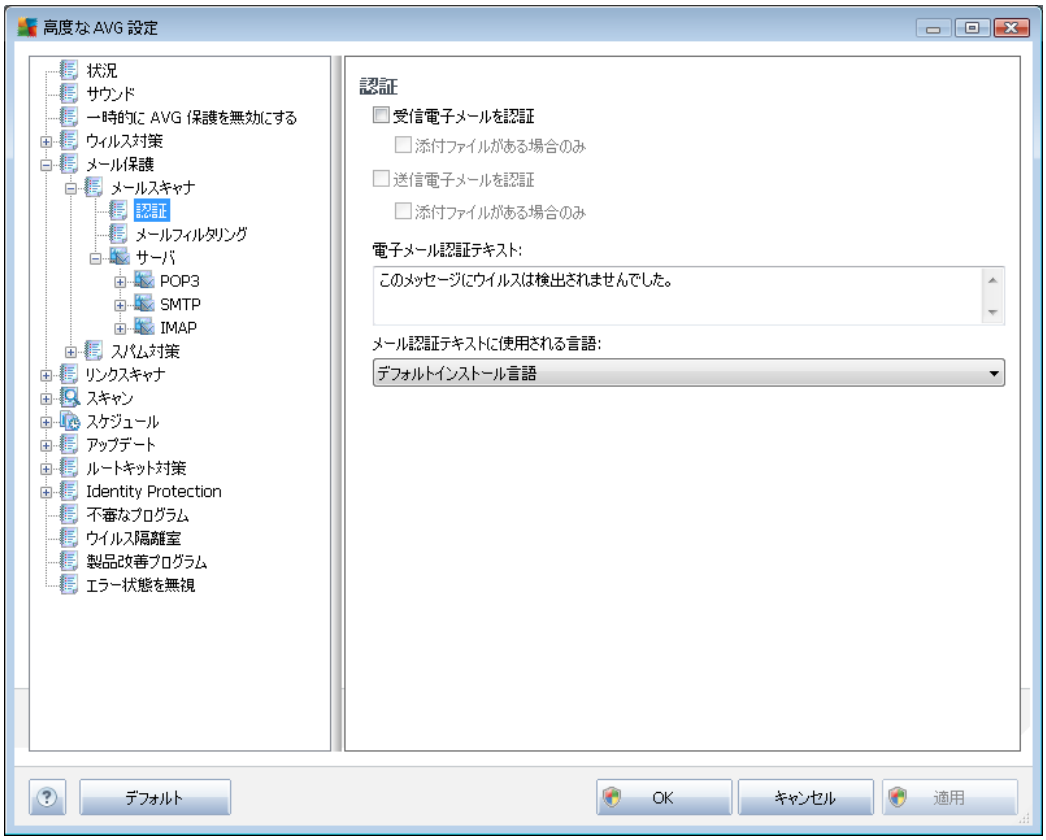
- ***パスワードによって保護された文書を報告する*** – パスワードによって保護された文書のウイルス スキャンはできません。ボックスにチェックを付けると、潜在的に危険なオブジェクトとしてこのようなドキュメントを報告します。

- ***マクロを含むファイルを報告する*** – マクロはあるタスクを簡単に実行するためのあらかじめ定義された一連の命令です (*MS Wordのマクロが広く知られています*)。マクロには潜在的に危険な命令が含まれる可能性があります。ボックスにチェックを付けると、マクロを含むファイルを不審なファイルとして報告します。

- ***拡張子偽装を報告する*** – たとえば、不審な実行可能ファイル「something.txt.exe」が、無害なテキストファイル「something.txt」として偽装されている場合があります。ボックスにチェックを付けると、このような拡張子を潜在的に危険なオブジェクトとして報告します。

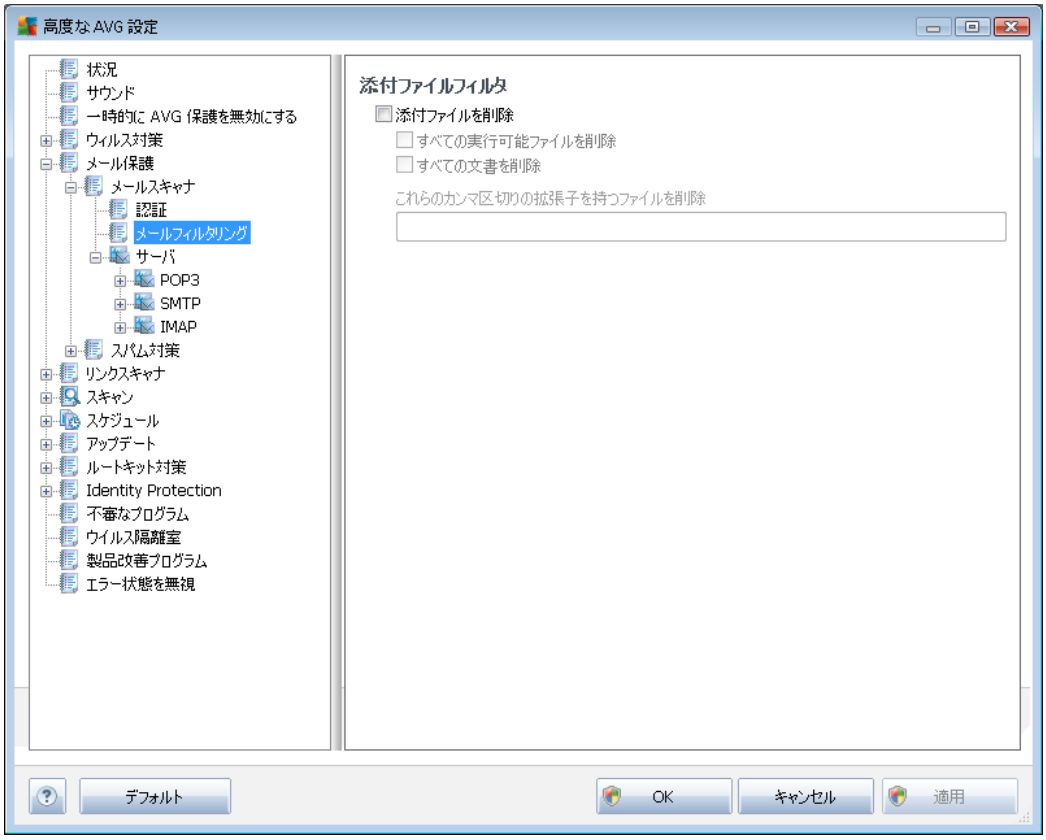
- ***レポートされたメール添付ファイルをウィルス隔離室に移動*** - 添付ファイルがパスワード保護されたアーカイブ、パスワード保護されたドキュメント、マクロを含むファイル、拡張子偽装を含む場合、それらをレポートするかどうかを指定します。このようなメールがスキャン中に検出された場合、検出された感染オブジェクトをウイルス隔離室に移動するかどうかについても指定することができます。

[***認証***] ダイアログの特定のチェックボックスを選択すると、受信メール (***受信電子メールを認証***) と送信メール (***送信電子メールを認証***) を認証するかどうかを決定できます。各オプションについては、さらに [***添付ファイルがある場合のみ***] パラメータを指定することで、添付ファイル付きの電子メールメッセージにのみ認証を追加することができます。



既定では、認証テキストには *このメッセージでウイルスが検出されなかったことを示す基本情報のみが含まれます。ただし、ニーズに合わせてこの情報を拡張したり変更したりできます。その場合は、任意の認証テキストを [電子メール認証テキスト]* ***フィールドに入力します。*** [***メール認証テキストに使用される言語***] セクションでは、自動生成された認証テキスト (*このメッセージにウイルスは検出されませんでした*) を表示する言語を定義できます。

メモ: *既定のテキストは指定された言語でのみ表示され、カスタマイズされたテキストは自動的に翻訳されません。*



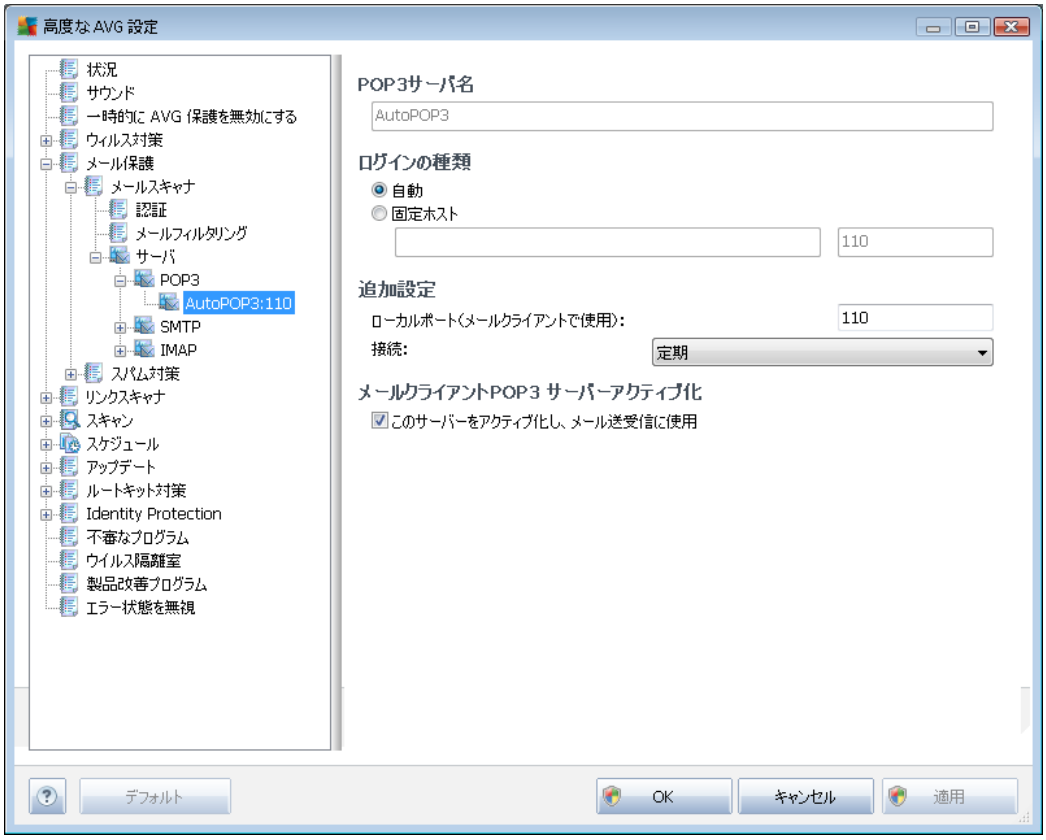
添付ファイルフィルタダイアログでは、メール添付ファイルのスキャンパラメータを設定できます。デフォルトでは、***添付ファイルを削除***オプションはオフとなっています。有効化した場合、感染、または潜在的に危険だと検出されたすべての添付ファイルは自動的に削除されます。削除する添付ファイルのタイプを定義したい場合、各オプションを選択します。

- ***すべての実行可能ファイルを削除*** -すべての*.exe ファイルが削除されます。
- ***すべての文書を削除***-すべての *.doc、*.docx、*.xls、*.xlsx ファイルが削除されます。
- ***これらのカンマ区切りの拡張子を含むファイルを除去*** - 定義された拡張子のすべてのファイルを削除します

[***サーバー***] セクションでは、メール スキャナ サーバーのパラメータを編集できます。

- POP3 サーバー
- SMTPサーバー
- IMAP サーバー

また、[***新しいサーバーの追加***] ボタンを使用して、新しい送受信メール サーバーを定義できます。

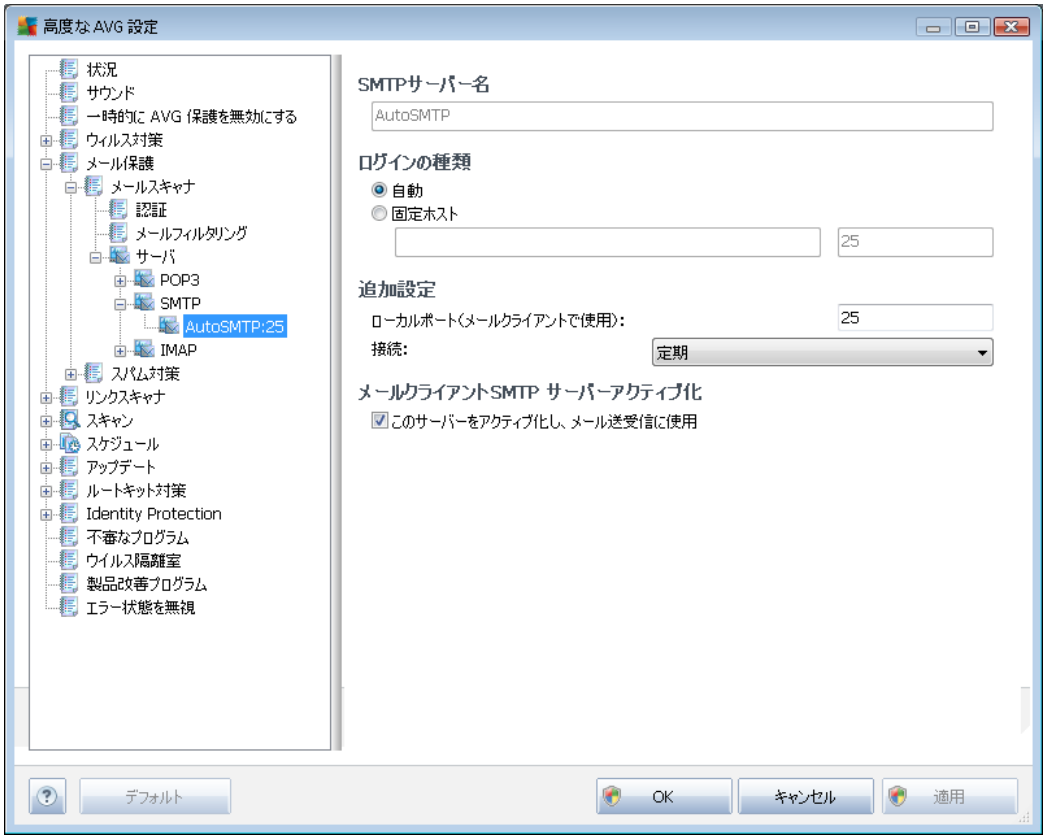


[*サーバー/POP3*] をクリックすると、このダイアログが開きます。受信メール用の POP3 プロトコルを使用して、新規のメール スキャナ サーバーを設定できます。

- ***POP3 サーバー名*** - このフィールドでは新しく追加したサーバー名を指定できます (*POP3 サーバーを追加するには、左側のナビゲーション メニューの POP3 項目を右クリックします*)。自動的に作成された「AutoPOP3」サーバーの場合は、このフィールドは無効になっています。
- ***ログインの種類*** - 受信メールに使用されるメールサーバー決定方法を定義します。
  - ***自動*** - メールクライアントの設定にしたがって、自動的ログインが実行されます。
  - ***固定ホスト*** - プログラムは常にここで指定されたサーバーを使用します。メール サーバーのアドレスと名前を指定してください。ログイン名は変更されません。名前については、IP アドレス (*123.45.67.89 など*) とドメイン名 (*pop.acme.com など*) を使用できます。メール サーバーが標準以外のポートを使用する場合、このポートをコロンで区切り、サーバー名の後に指定できます (*smtp.acme.com:8200 など*)。POP3 通信の標準ポートは 110 です。
- ***追加設定*** - より詳細なパラメータを設定します。
  - ***ローカルポート*** - メールアプリケーションからの通信用ポートを指定します。メールアプリケーション上で、このポートをPOP3通信のポートとして指定する必要があります。

- o ***接続*** - *このドロップダウン メニューでは、使用する接続の種類 (*通常/SSL/SSL 既定) を指定できます。SSL 接続を選択した場合、送信データは第三者に追跡、監視されるリスクを負うことなく暗号化されます。この機能は送信先のメール サーバーが対応している場合にのみ使用可能です。

- ***メールクライアント POP3 サーバー有効化*** - このアイテムをチェック/チェック解除すると、指定された POP3 サーバーを有効化/無効化します。



[*サーバー/SMTP*] ***をクリックすると、このダイアログが開きます。送信メール用の SMTP プロトコルを使用して、新規の***メール スキャナ サーバーを設定できます。

- ***SMTP サーバー名*** - このフィールドでは新しく追加したサーバー名を指定できます (*SMTP サーバーを追加するには、左側のナビゲーション メニューで SMTP 項目右クリックします*)。自動的に作成された「AutoSMTP」サーバーの場合は、このフィールドは無効になっています。

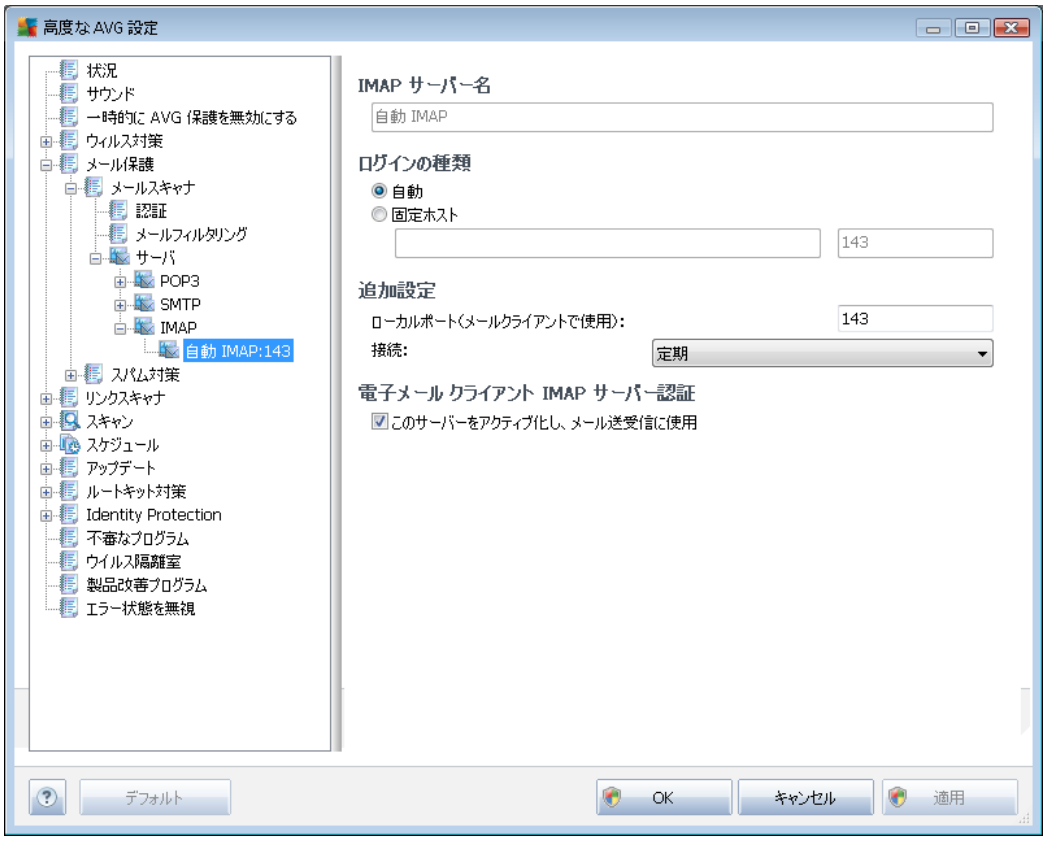
- ***ログイン タイプ***- メール送信で使用するメール サーバーを決定する方法を定義します。

  - o ***自動*** - メールクライアントの設定にしたがって、自動的ログインが実行されます。

  - o ***固定ホスト***- プログラムは常にここで指定されたサーバーを使用します。メール サーバーのアドレスと名前を指定してください。名前については、ドメイン名 (*smtp.acme.com* など) および IP アドレス (*123.45.67.89* など) を使用できます。メール サーバーが標準以外のポートを使用する場合、このポートをコロンで区切り、サーバー名の後に記述す

ることができます（*たとえば、smtp.acme.com:8200*）。SMTP 通信の標準ポートは 25 です。

- ***追加設定*** - より詳細なパラメータを設定します。
  - ***ローカルポート*** - メールアプリケーションからの通信用ポートを指定します。メールアプリケーション上で、このポートをSMTP通信のポートとして指定する必要があります。
  - ***接続*** - このドロップダウンメニューでは、使用する接続の種類（*通常/SSL/SSL 既定*）を指定できます。SSL接続を選択した場合、送信データは第三者に追跡、監視されるリスクを負うことなく暗号化されます。この機能は送信先のメールサーバーがそれに対応している場合のみ使用可能です。
- ***電子メールクライアント SMTP サーバー有効化*** - このボックスのオン/オフを切り替えると、指定した SMTP サーバーの有効化と無効化を切り替えます。



[***サーバー/IMAP***] をクリックすると、このダイアログが開きます。送信メール用の IMAP プロトコルを使用して、新規のメール スキャナ サーバーを設定できます。

- ***IMAP サーバー名*** - このフィールドでは新しく追加したサーバー名を指定できます（*IMAP サーバーを追加するには、左側のナビゲーション メニューで右クリックします*）。自動的に作成された「AutoIMAP」サーバーの場合は、このフィールドは無効になっています。
- ***ログイン タイプ*** - メール送信で使用するメール サーバーを決定する方法を定義します。

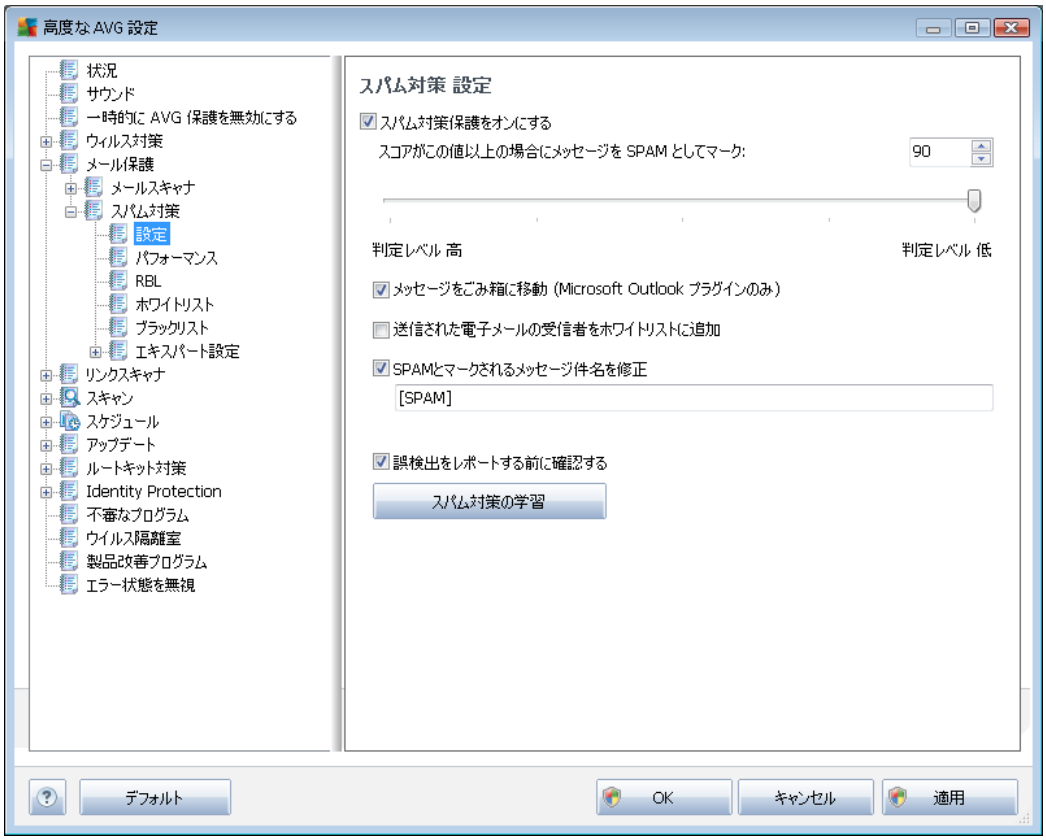
- o ***自動*** - メールクライアントの設定にしたがって、自動的ログインが実行されます。
- o ***固定ホスト*** - プログラムは常にここで指定されたサーバーを使用します。メール サーバーのアドレスと名前を指定してください。名前については、ドメイン名 (*smtp.acme.com* など) および IP アドレス (*123.45.67.89* など) を使用できます。メール サーバーが標準以外のポートを使用する場合、このポートをコロンで区切り、サーバー名の後に指定できます (*smtp.acme.com:8200* など)。IMAP 通信の標準ポートは 143 です。

- ***追加設定*** - より詳細なパラメータを設定します。
  - o ***ローカルポート*** - メールアプリケーションからの通信用ポートを指定します。IMAP 通信用ポートとして、このポートをメール アプリケーションで指定する必要があります。
  - o ***接続*** - このドロップダウン メニューでは、使用する接続の種類 (*通常/SSL/SSL 既定*) を指定できます。SSL接続を選択した場合、送信データは第三者に追跡、監視されるリスクを負うことなく暗号化されます。この機能は送信先のメール サーバーがそれに対応している場合のみ使用可能です。

- ***電子メール クライアント IMAP サーバーを有効にする*** - このボックスを選択/クリアすると、指定した IMAP サーバーを有効/無効にします。

9.5.2. スパム対策

ここにトピックの文字を入力してください。



[***スパム対策設定***] ダイアログでは、[***スパム対策保護をオン***] チェックボックスによって、スパム対策スキャンのオン/オフを切り替えることができます。このオプションは既定ではオンになっています。また、変更する理由がない場合は、この設定を保持することをお勧めします。

次に、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 *(例えば、メッセージの内容がSPAMにどの程度類似しているか等)*。値を入力するかスライダを左右に動かす *(値の範囲は 50 ～ 90)* ことによって、[***スコアがこの値を超える場合スパムとしてメッセージを判定する***] 設定を調整できます。

一般的には、閾値を50から90の間、不明な場合は、90に設定することを推奨します。以下はスコアの閾値の一般的な概要です。

- ***値 80 ～ 90*** - 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。

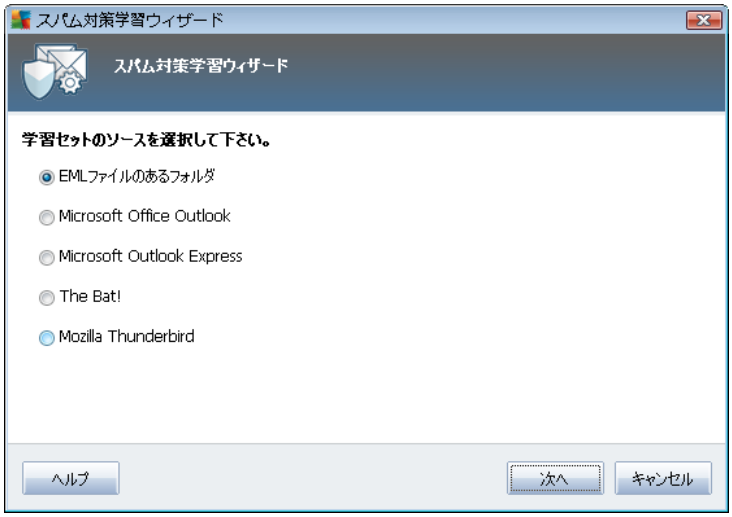
スパム対策設定ダイアログでは、さらに検出されたスパムメールメッセージが処理される方法を定義することができます。

- ***メッセージをスパムフォルダに移動*** - この項目をチェックすると、検出されたスパムメッセージは、自動的にメールクライアントの迷惑メールフォルダに移動されます。
- ***送信メールの受信者をホワイトリスト***に追加 - このチェックボックスにチェックを付けると、すべての送信メールの受信者が信頼でき、その受信者のメールアカウントから送信されるすべてのメールメッセージの配信を許可することを確認します。
- ***スパムとして判定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メッセージの件名にを特定の単語や文字を追加したい場合、このチェックボックスにチェックを付けます。追加する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に参加することに同意した場合、検出された脅威がAVGに報告されます。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に送信することができます。

コントロールボタン

[***スパム対策の学習***] ボタンは、次の章で詳しく説明されているスパム対策学習ウィザードを実行します。

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。

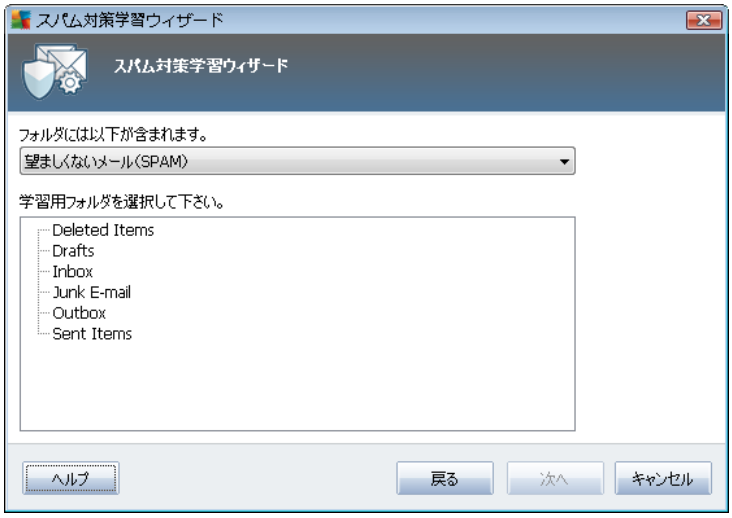
- ***特定のメールクライアント*** - リストされたメールクライアントの1つ(*MS Outlook*、*Outlook Express*、*The Bat!*)を使用する場合、該当するオプションを選択します。
- ***EML ファイルのあるフォルダ*** - 他のメールプログラムを利用する場合、まずメッセージを特定のフォルダに保存(*eml*形式)、またはメールクライアントメッセージフォルダの場所を確認します。次に、***EML ファイルのあるフォルダ***を選択します。次のステップで希望するフォルダを指定します。

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。

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



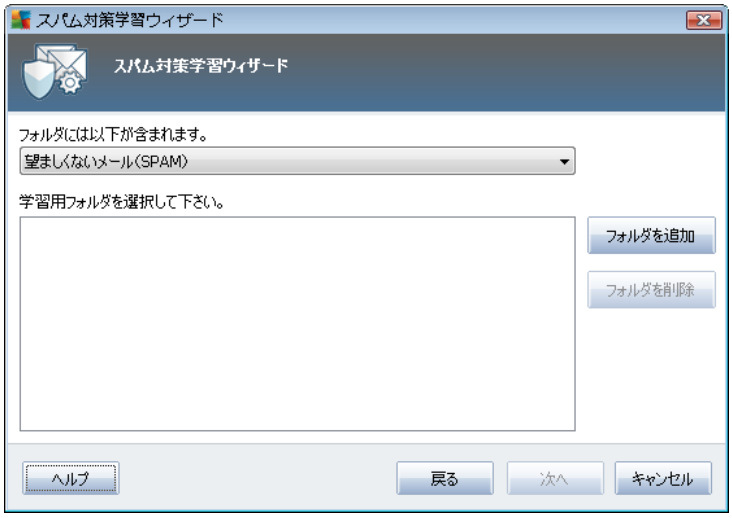
このダイアログでは学習に使用するメッセージ フォルダを選択します。[***フォルダの追加***] ボタンをクリックして、.eml ファイル (*保存された電子メール メッセージ*) のあるフォルダを参照します。選択したフォルダがダイアログに表示されます。

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

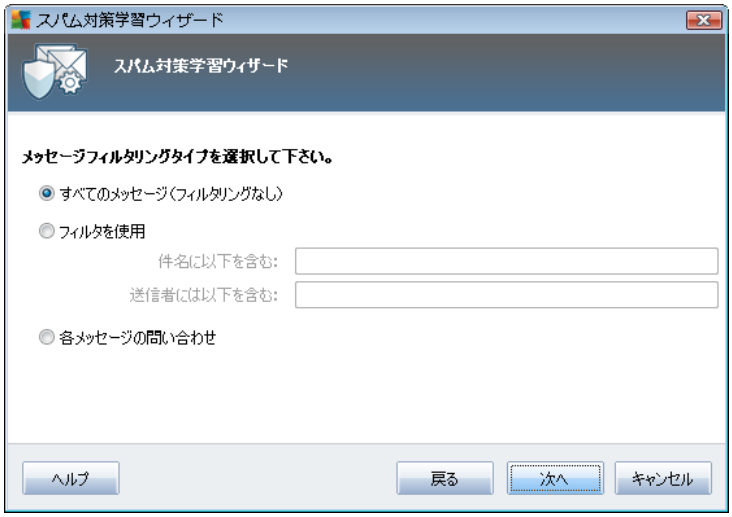
オプションのいずれかを確認した場合、新しいダイアログが表示されます。



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。

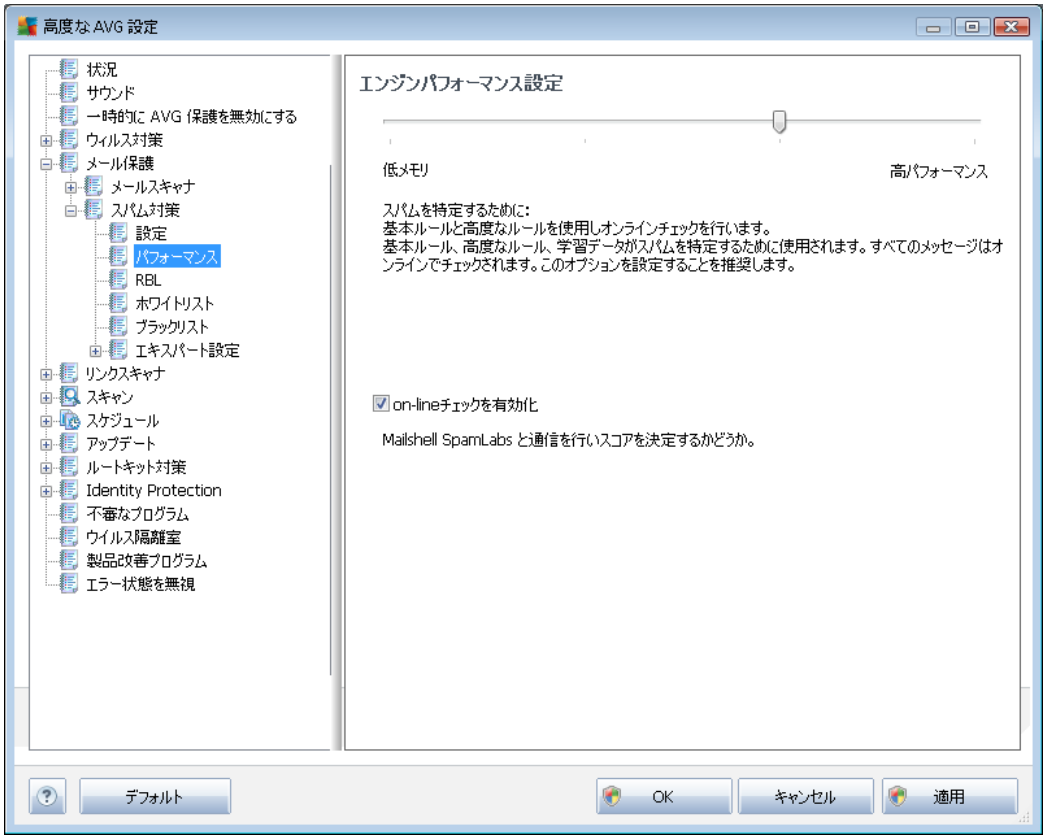


このダイアログでは、メールメッセージのフィルタリングを設定します。

- ***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。

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***を選択すると表示されます）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します。



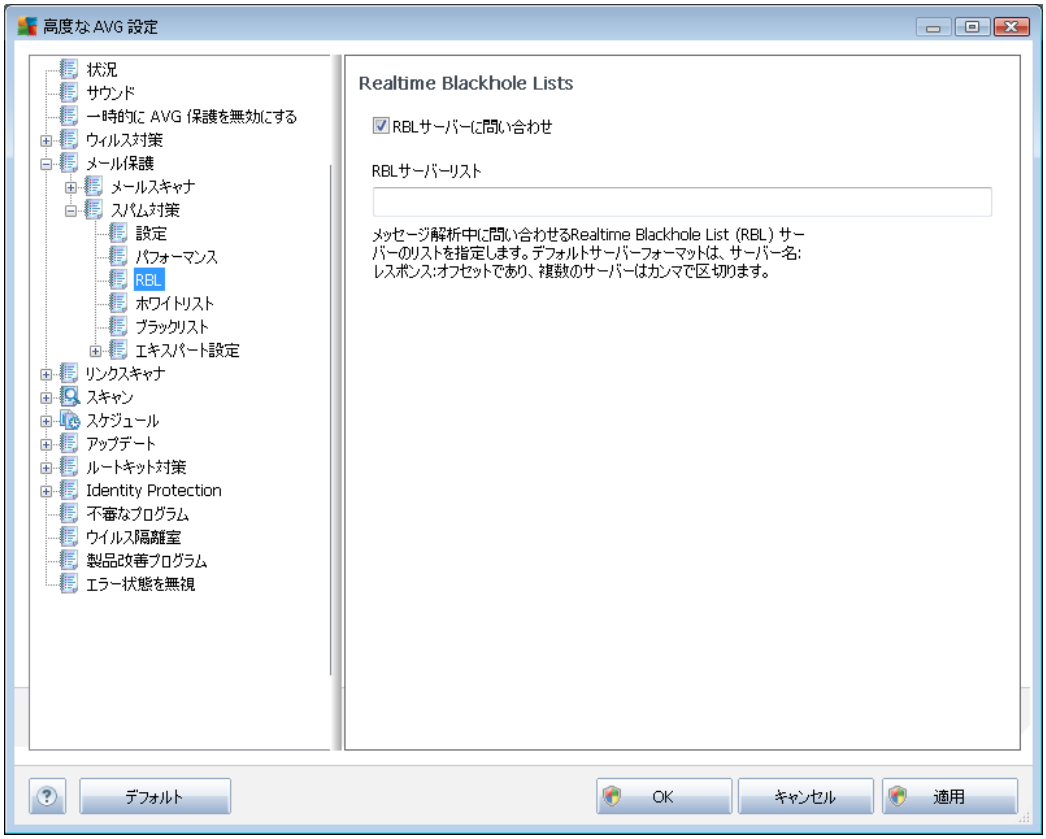
スライダを左右に動かして、***低メモリ消費***モードと***高パフォーマンス***モードの間でスキャンパフォーマンスレベルを変更します。

- ***低メモリ***- スパムを判定するスキャン処理中に、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。

[***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***] 編集ダイアログが開き、***RBL サーバーへの問い合わせ***機能を有効/無効にできます。

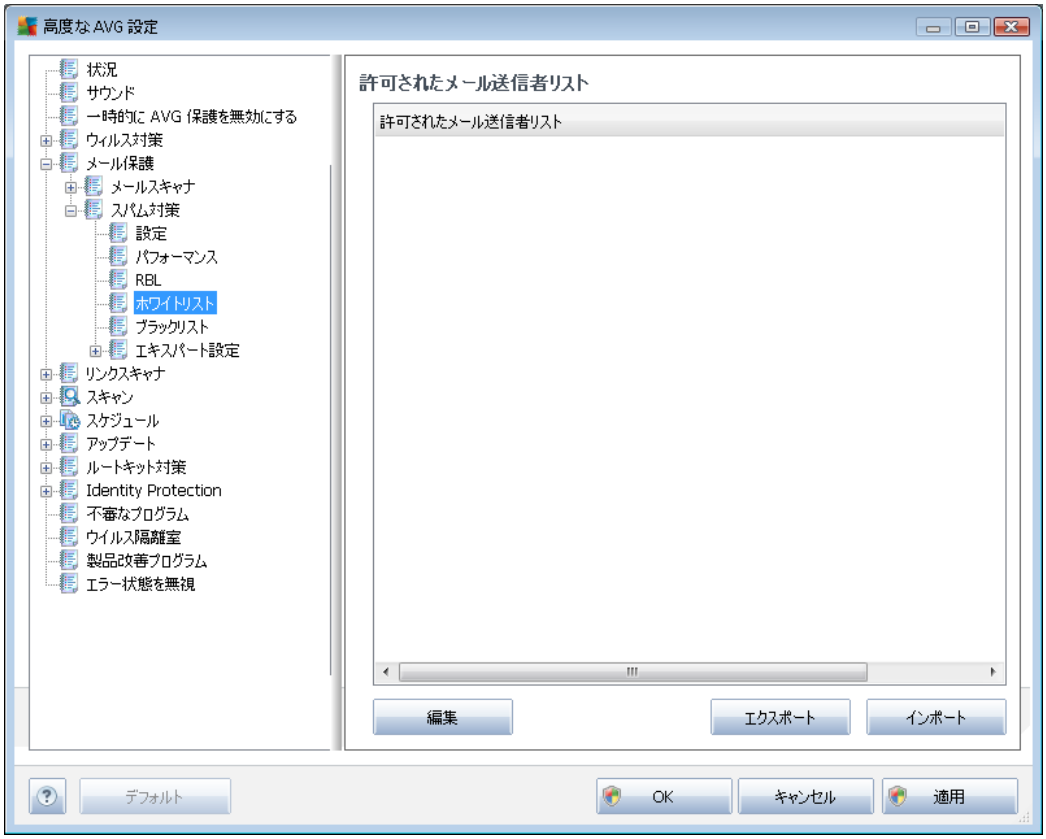


RBL (*リアルタイム ブラックホール リスト*) サーバーは、既知のスパム送信者の拡張データベースを含む DNS サーバーです。この機能がオンの場合、すべてのメールが RBL サーバー データベースと照合され、このデータベース エントリと一致する場合には、スパムとして判定されます。RBL サーバー データベースには最新スパム フィンガープリントが含まれ、最高レベルの最も正確なスパム検出を実現します。この機能は、特に通常のスパム対策エンジンでは検出されないような大量のスパムを受信するユーザーに適しています。

[***RBL サーバー リスト***] では、特定の RBL サーバー ロケーションを定義できます (*この機能を有効にすると、すべての電子メール メッセージが RBL サーバー データベースに照合されるため、システムや設定によっては、電子メール受信処理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。

ホワイトリストアイテムは、[***承認されたメール送信者リスト***] ダイアログを開きます。このダイアログには、許可され、メッセージが決してスパムとしてマークされない送信者メール アドレスとドメイン名のグローバル リストを含むリストが表示されます。



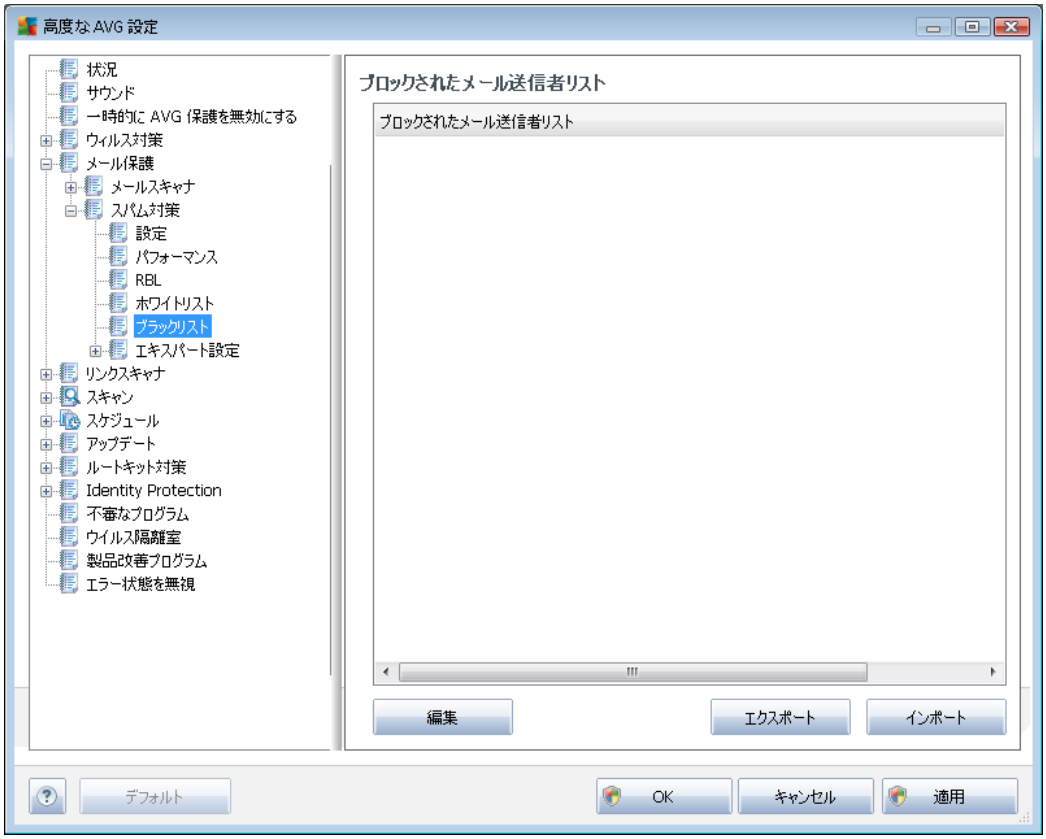
編集インターフェースでは、望ましくないメッセージ (スパム) を送信しない送信者のリストを編集できます。また、スパムメッセージが生成されないことがわかっているドメイン名（*avg.com*等）のリストを編集します。既にスパム送信者やドメイン名のリストがある場合は、各メールアドレスを直接入力するか、一度にアドレスの全リストをインポートすることでリストを入力できます。

コントロール ボタン

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（*コピーとペースト*も使用できます）。1行に1アイテム（*送信者*、*ドメイン名*）を入力します。
- ***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。
- ***インポート*** - すでにメールアドレスやドメイン名のテキストファイルお持ちの場合、このボタンを選択することで単純にそのリストをインポートすることができます。ファイルの内容については、1 行につき 1 項目 (*アドレス*、*ドメイン名*) のみを含める必要があります。

ブラックリストは、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リストを含む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）を送信するであろう送信者のリストを編集します。また、スパムメッセージが送信される完全なドメイン名リスト（*spammingcompany.com* など）を編集できます。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。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。

コントロール ボタン

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（*コピーとペースト*も使用できます）。1行に1アイテム（*送信者*、*ドメイン名*）を入力します。
- ***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。
- ***インポート*** - すでにメールアドレスやドメイン名のテキストファイルお持ちの場合、このボタンを選択することで単純にそのリストをインポートすることができます。

高度な設定の部分には、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、詳細なスパム対策設定が必要とするネットワーク管理者のような、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.) の高度な設定について十分に理解していない場合は、設定変更を行わないことを強くお勧めします。不適切にファイルが変更された場合は、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可能性があります。

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。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

9.6. リンクスキャナ

9.6.1. リンクスキャナ設定

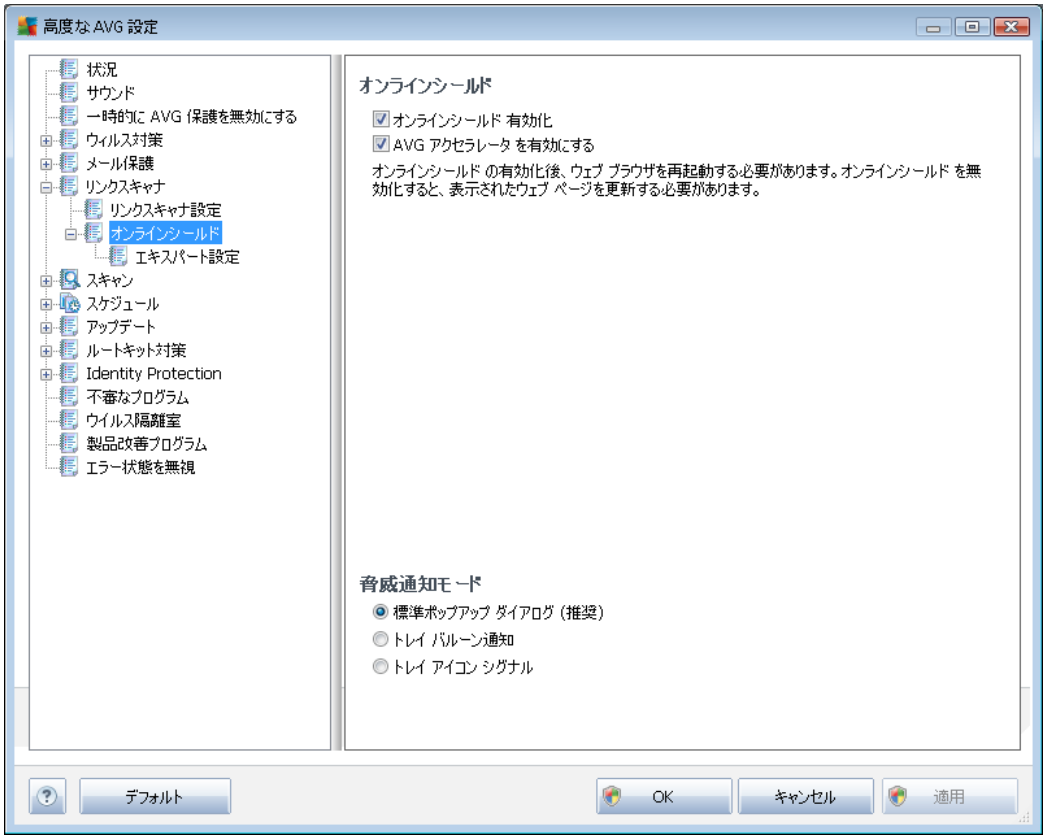
[***リンクスキャナ設定***] ダイアログでは、リンクスキャナ基本機能のオフ/オンを切り替えることができます。

- サーチシールド*を有効にする* - *(*既定ではオン*)*: Google、Yahoo! JP、WebHledani、Yandex、Baidu、Bing、AOL、AltaVista、EarthLink、Ask、Seznam、eBay、Twitter、Digg、SlashDot を使用して実行した検索結果に対して評価通知アイコンが表示されます。検索エンジンで返されたサイトの内容が事前にチェックされます。

- サーフシールド*を有効にする* - *(*既定ではオン*): ユーザーがサイトにアクセスしようとするときに、積極的に*リアルタイムでエクスプロイトサイトを検出し、保護を実施します。ユーザーがWebブラウザ*(あるいは他のHTTPを使用するアプリケーション)*からWebページにアクセスする際、既知の悪意のあるサイトへの接続と、エクスプロイトコンテンツがブロックされます。

- ***「Secured by LinkScanner」を追加する...*** - *(既定では有効)*: この項目を選択すると、Facebook および MySpace ソーシャルネットワークから送信されるメッセージにアクティブなハイパーリンクが含まれる場合に、リンクスキャナチェックに関する認証通知をすべてのメッセージに追加します。

9.6.2. オンライン シールド

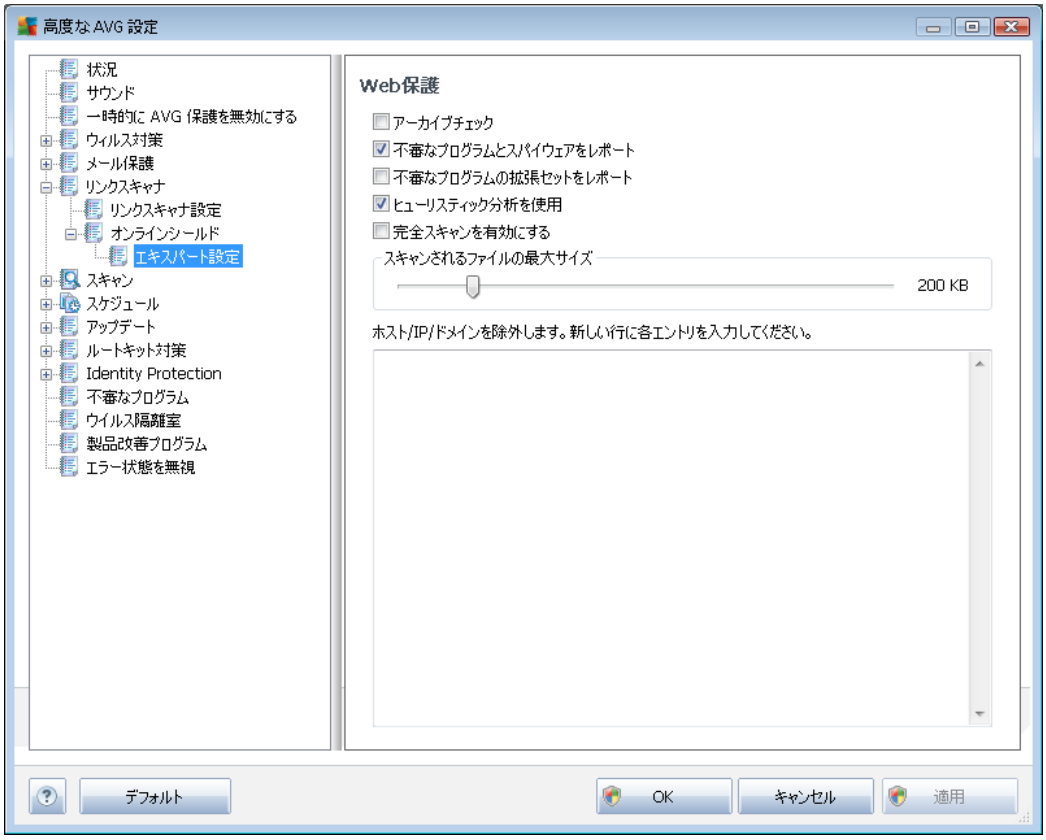


[***オンライン シールド***] ダイアログには次のオプションがあります。

- ***オンライン シールドを有効にする*** *(既定では有効)* - ***オンライン シールド*** サービス全体を有効/無効にします。***オンライン シールド***の高度な設定については、次に表示される [Web 保護] ダイアログで設定します。
- ***AVG Accelerator を有効にする*** *(既定では有効)* - オンライン ビデオのサービスをスムーズにして、ダウンロードを簡単にするサービスである AVG Acceleratorを有効/無効にします。

脅威通知モード

ダイアログの下部では、検出された起こりうる脅威に関する情報を通知する方法を選択します :標準ポップアップダイアログ経由、トレイバルーン通知経由、あるいはトレイアイコン情報経由。



Web保護ダイアログでは、Webコンテンツのスキャンに関するコンポーネント設定を編集することができます。編集インターフェースでは、以下の基本オプションを設定します。

- ***Web の保護を有効化*** - このオプションがチェックされている場合、***オンライン シールド***は WWW ページのスキャンを実行します。このオプションがオン (*デフォルト*) の場合、さらに以下の項目のオン/オフを変更することができます。

  - ***アーカイブをチェックする*** - (*既定ではオフ*): WWW ページに含まれるアーカイブ コンテンツをスキャンします。

  - ***不審なプログラムとスパイウェア脅威を報告する*** - (*既定では有効*)チェックを付けると、スパイウェア対策エンジンを有効にし、ウイルスと同時にスパイウェアもスキャンします。スパイウェアは疑わしいマルウェアのカテゴリに含まれます。通常は、セキュリティリスクとなる場合でも、このようなプログラムを故意にインストールすることができます。コンピュータのセキュリティを高めるため、この機能を有効にしておくことをお勧めします。

  - ***不審なプログラムの拡張セットを報告する*** - (*既定ではオフ*): 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。スパイウェアとは、直接製造元から入手する場合には、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誤用されるおそれのあるプログラムです。これは、コンピュータセキュリティ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。

- ***ヒューリスティック分析を使用する*** - (*既定ではオン*): ヒューリスティック分析 (仮想コンピュータ環境での*スキャンオブジェクトの動的エミュレーション*) を使用して、表示されるページコンテンツをスキャンします。

- ***完全スキャンを有効にする*** (*既定ではオフ*) - このオプションをチェックすると、特定の状況 (*コンピュータが感染している疑いがある場合など*) が発生した場合に最も完全なスキャンアルゴリズムを有効にし、感染の可能性が非常に低いコンピュータ領域もスキャンします。これにより、問題がないことを確実に確認します。この方法を実行すると多少時間がかかります。

- ***スキャンされる最大ファイルサイズ*** - 含まれるファイルが表示されるページにある場合、これがコンピュータにダウンロードされる前にスキャンできます。ただし、大きいファイルのスキャンは時間がかかり、Webページのダウンロードの速度が著しく遅くなる場合があります。スライドバーを使用して、***オンラインシールド***でスキャンされるファイルの最大サイズを指定できます。ダウンロードファイルが指定値より大きく、オンラインシールドでスキャンされない場合でも、保護は続きます。この場合、ファイルは感染し、***常駐シールド***がそれをすぐに検出します。

- ***ホスト/IP/ドメインを除外*** - テキストフィールド内にオンラインシールドの*スキャンの対象外となるべきサーバー* (ホスト、IPアドレス、マスク付きIPアドレス、あるいはURL) *あるいはドメインの正確な名称を入力します*。このため、絶対に危険なウェブサイトコンテンツを送信しないことが確実であるホストのみを除外してください。

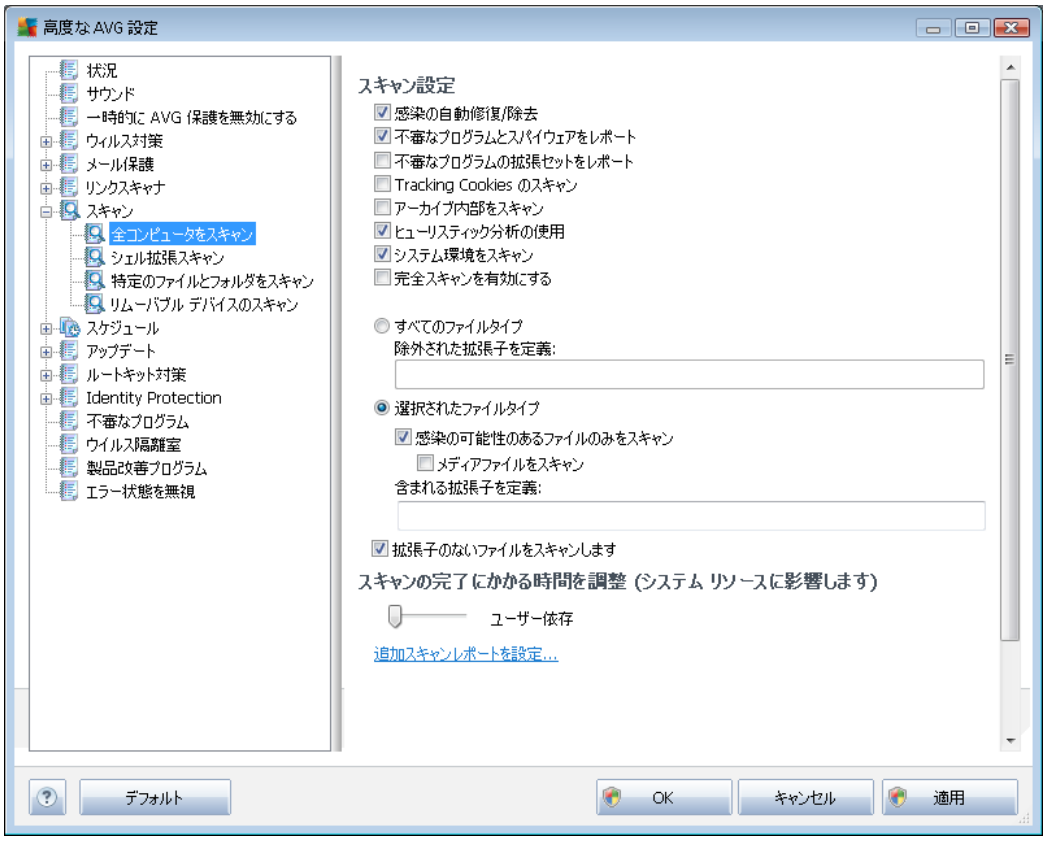
9.7. スキャン

高度なスキャン設定は 4 つのカテゴリに分けられ、このカテゴリは AVG が定義した特定のスキャンタイプを示します。

- ***完全コンピュータスキャン*** - 標準の事前定義された完全コンピュータスキャンです。
- ***シェル拡張スキャン*** - Windows Explorer 環境から直接選択されたオブジェクトのスキャンです。
- ***特定のファイルまたはフォルダのスキャン*** - あらかじめ定義された標準スキャンで、コンピュータの特定の領域をスキャンします。
- ***リムーバブルデバイスのスキャン*** - コンピュータに接続した特定のリムーバブルデバイスのスキャン

9.7.1. 完全コンピュータ スキャン

[***完全コンピュータ スキャン***] オプションでは、ソフトウェア ベンダーがあらかじめ定義したスキャンの 1 つである完全コンピュータ スキャンのパラメータを編集できます。



スキャン設定

[***スキャン設定***] セクションに表示されているスキャン パラメータを任意でオン/オフにできます。

- ***自動的に感染を修復/除去する*** (*既定ではオン*): スキャン実行中にウイルスが特定され、修復可能な場合は、自動的に修復されます。感染したファイルを自動的に修復できない場合、感染したオブジェクトはウィルス隔離室に移動されます。

- ***不審なプログラムとスパイウェア脅威を報告する*** (*既定ではオン*) - チェックを付けると、スパイウェア対策エンジンを有効化し、ウイルスと同時にスパイウェアもスキャンします。スパイウェアは疑わしいマルウェアのカテゴリに含まれます。通常は、セキュリティリスクとなる場合でも、このようなプログラムを故意にインストールすることができます。コンピュータのセキュリティを高めるため、この機能を有効にしておくことをお勧めします。

- ***不審なプログラムの拡張セットを報告する*** (*既定ではオフ*) - 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。スパイウェアとは、直接製造元から入手する場合にはまったく問題がなく、無害なプログラムですが、後から悪意のある目的で誤用されるおそれのあるプログラムです。これは、コンピュータ セキュリティ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。

- ***Tracking Cookie をスキャンする*** (*既定ではオフ*) - スパイウェア対策コンポーネントのこのパラメータを定義すると、Cookie を検出します (HTTP cookie は、サイトの設定や電子ショッピングカートの内容など、ユーザー固有の情報の認証、追跡、メンテナンスに使用されます)。
- ***アーカイブの内容をスキャンする*** (*既定ではオフ*) - ZIP や RAR などのアーカイブ内に格納されているすべてのファイルをスキャンします。
- ***ヒューリスティック分析を使用する*** (*既定ではオン*) - ヒューリスティック分析 (*仮想コンピュータ環境で実行されるスキャン対象オブジェクト命令の動的エミュレーション*) は、スキャン実行中に採用されるウイルス検出方法の 1 つです。
- ***システム環境をスキャンする*** (*既定ではオン*) - コンピュータのシステム領域もチェックされます。
- ***完全スキャンを有効にする*** (*既定ではオフ*) - このオプションをチェックすると、特定の状況 (*コンピュータが感染している疑いがある場合など*) が発生した場合に最も完全なスキャン アルゴリズムを有効にし、感染の可能性が非常に低いコンピュータ領域もスキャンします。これにより、問題がないことを確実に確認します。この方法を実行すると多少時間がかかります。

さらに、スキャンするかどうかを決定する必要があります。

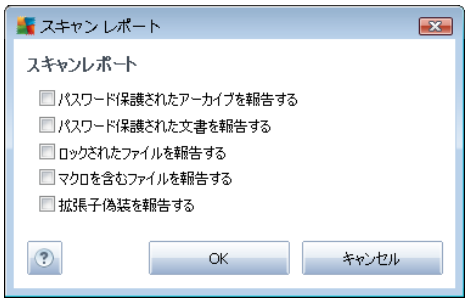
- ***すべてのファイル タイプとスキャン対象ではないファイル拡張子をカンマで区切ったリスト*** (*保存すると、カンマはセミコロンに変わります*) を入力することで、スキャンからの除外を定義できます。
- ***選択したファイル タイプ*** - 感染の可能性のあるファイルのみを指定できます (*一部のプレーンテキスト ファイルやその他の非実行可能ファイルなど*感染の可能性がないファイルはスキャンされません)。これには、メディア ファイル (*ビデオ、オーディオ ファイル*) が含まれます。多くの場合、このようなファイルはサイズが非常に大きく、ウィルスに感染している可能性が非常に低いため、このボックスのチェックを外すと、スキャン時間がさらに短縮されますここでも、必ずスキャンするファイルの拡張子を指定できます。
- 任意で***拡張子のないファイルをスキャン***できます。このオプションは既定ではオンになっています。変更する理由がない場合は、この設定を保持することをお勧めします。拡張子のないファイルは不審であるため、常にスキャンすることをお勧めします。

スキャン速度を調整

[***スキャン速度を調整***] セクションでは、システム リソース使用度に応じて、任意のスキャン速度を指定できます。*既定ではこのオプションの値は、自動的にリソースを使用する*ユーザー依存レベルに設定されています。スキャンを高速化すると、スキャン時間を短縮できますが、スキャン実行中にシステム リソース消費量が著しく上がり、PC で実行されている他の作業の速度が低下します (*このオプションは、コンピュータの電源がオンであり、コンピュータ上で作業をしているユーザーがいない場合などに適しています*)。一方、スキャンの時間を延長することで、システム リソース消費量を下げることができます。

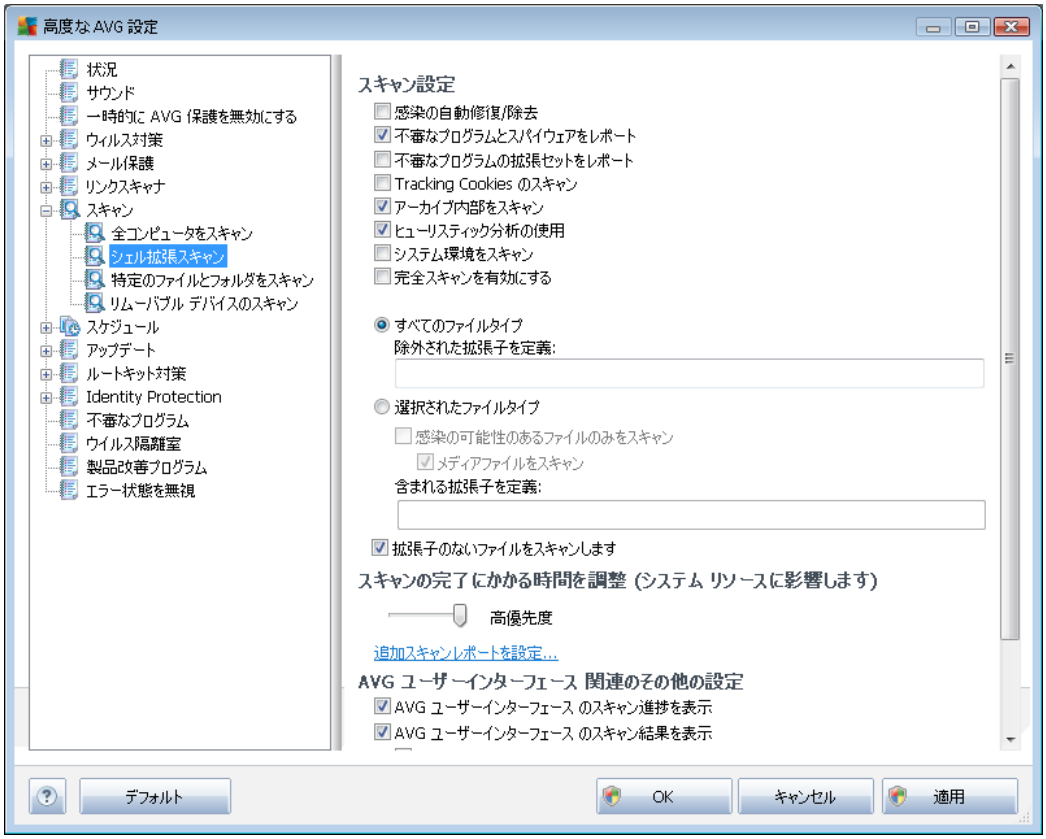
追加スキャン レポートを設定...

[***追加スキャンレポート...***] リンクをクリックすると、[***スキャンレポート***] ダイアログが開きます。このウィンドウでは報告する検出項目を定義します。



9.7.2. シェル拡張スキャン

この項目はシェル拡張スキャンと呼ばれ、以前の完全コンピュータスキャン同様、ソフトウェアベンダーが事前定義したスキャンを編集できます。設定が Windows Explorer環境から直接起動される特定オブジェクトスキャンに関連している (*シェル拡張*) 場合、Windows Explorerのスキャンの章を参照してください。



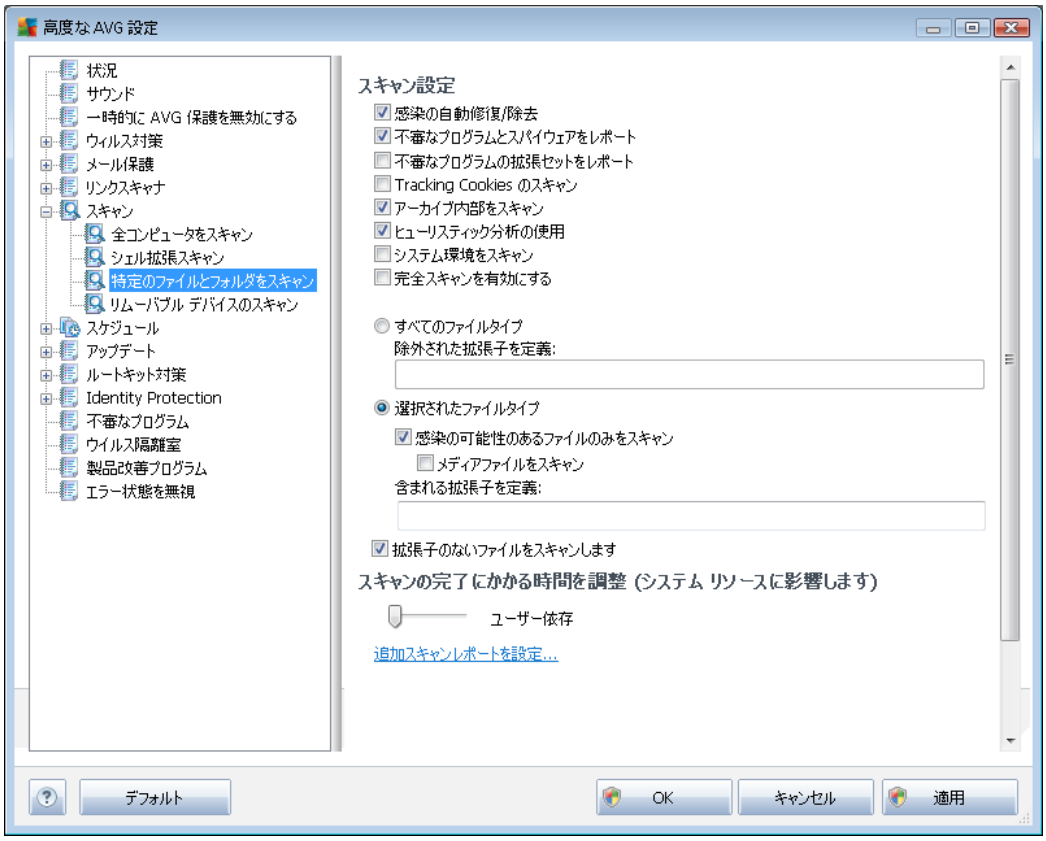
パラメータのリストは完全コンピュータスキャンで利用できるものと同一です。ただし、既定の設定が異なります (*たとえば、完全コンピュータスキャンの場合、既定ではアーカイブをチェックせずにシステム環境をチェックしますが、シェル拡張スキャンでは逆になります*)。

***メモ**: 特定のパラメータの説明については、 AVG 高度な設定 / スキャン/ 完全コンピュータスキャン の章を参照してください。*

[完全コンピュータスキャン] ダイアログと比較すると、[***シェル拡張スキャン***] ダイアログには [***AVG ユーザーインターフェースのその他の設定***] というセクションがあり、スキャンの進行状況を表示するかどうか、AVG ユーザーインターフェースからスキャン結果にアクセスできるようにするかを指定できます。また、スキャンで感染が検出された場合にのみスキャン結果を表示するように定義できます。

9.7.3. 特定のファイルとフォルダをスキャン

特定のファイルまたはフォルダをスキャンの編集インターフェースは完全コンピュータスキャン編集ダイアログと同一です。すべてのコンフィグレーションオプションは同一です。ただし、デフォルト設定は完全コンピュータスキャンの場合にはより厳密なものとなっています。

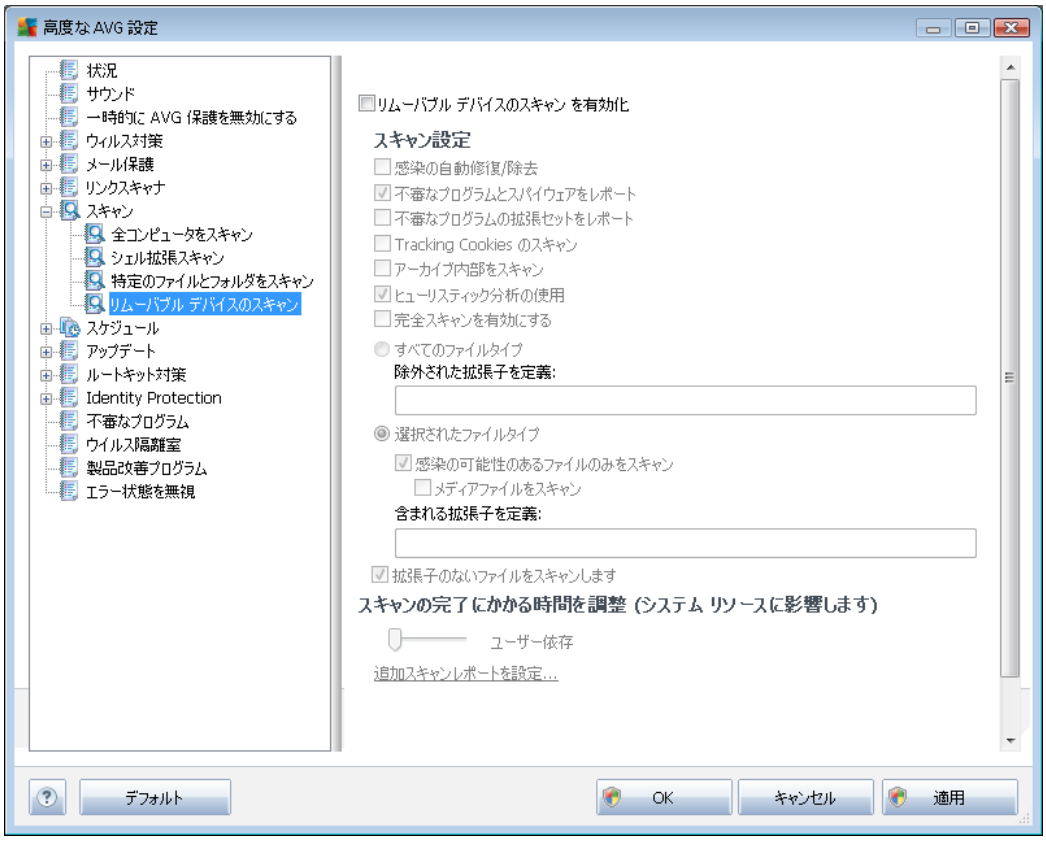


この設定ダイアログで設定されるすべてのパラメータは、特定のファイルとフォルダをスキャンで選択されたスキャンエリアのみに適用されます。

***メモ**: 特定のパラメータの説明については、 AVG 高度な設定 / スキャン/ 完全コンピュータスキャン の章を参照してください。*

9.7.4. リムーバブル デバイスのスキャン

[***リムーバブル デバイスのスキャン***] の編集インターフェースは [完全コンピュータスキャン] 編集ダイアログに非常に似ています。



リムーバブルデバイスのスキャンは、コンピュータにリムーバブルデバイスを接続したときに、自動的に起動します。既定では、このスキャンはオフになっています。ただし、リムーバブルデバイスは大きな脅威源なので、潜在的な脅威をスキャンすることが非常に重要です。このスキャンを準備し、必要なときに自動的に起動するようにするには、[***リムーバブルデバイスのスキャンを有効化***] オプションにチェックを付けます。

***メモ**: 特定のパラメータの説明については、 AVG 高度な設定 / スキャン/ 完全コンピュータスキャンの章を参照してください。*

9.8. スケジュール

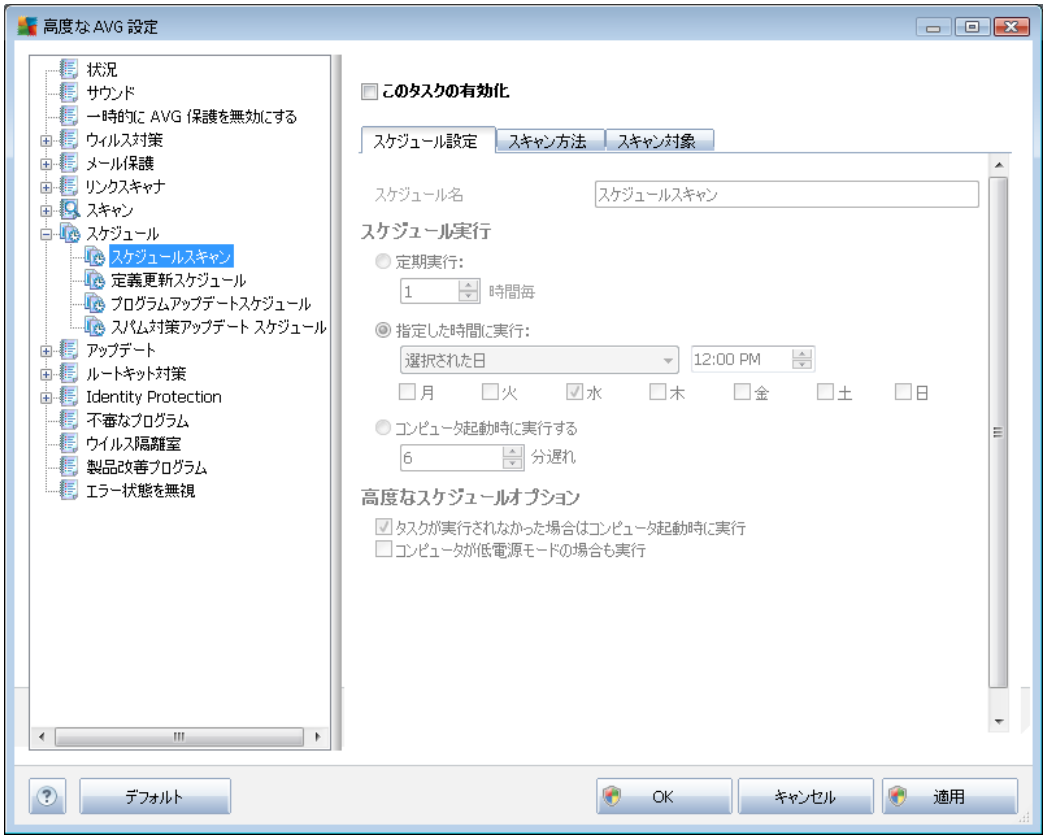
スケジュールセクションでは、デフォルト設定を編集することができます。

- スケジュール スキャン
- 定義更新スケジュール
- プログラムアップデートスケジュール

- スパム対策 アップデートスケジュール

9.8.1. スケジュール済スキャン

スケジュールされたスキャン（*または新しいスケジュール設定*）のパラメータは、3つのタブで編集できます。必要に応じて、各タブで [***このタスクを有効にする***] 項目のチェックをオン/オフにすると、スケジュールされたスキャンを一時的に有効化/無効化できます。



次に、[***名前***] テキストフィールド（*すべての既定のスケジュールでは無効化*）には、プログラムベンダーによってこのスケジュールに割り当てられた名前があります。新しく追加されたスケジュール（ナビゲーションツリーの [*スキャンのスケジュール*] ***アイテムを右クリックして新しいスケジュールを追加できます***）の場合、独自の名前を指定できます。その場合は、テキストフィールドが開き、編集できるようになります。スキャンには、必ず簡潔で、説明的で、適切な名前を使用して、後に他のスキャンと区別できるようにしてください。

例： *新規スキャン」あるいは「マイスキャン」という名前は適切ではありません。これらの名前は、実際にスキャンがチェックする対象を指さないからです。「システムエリアスキャン」というような名前が推奨されます。また、スキャンが完全コンピュータスキャンか単に選択されたファイルやフォルダのスキャンであるかを区別する名前を指定することも重要です - 自分のスキャンは常に[選択されたファイルやフォルダのスキャン](#)の特定バージョンにあります。*

このダイアログでは、さらに以下のスキャンパラメータを定義します。

スケジュール実行

ここでは、新しくスケジュールされたスキャンを起動する時間間隔を指定できます。特定の期間が経過した後に繰り返しスキャンを起動(***定期実行...***)、正確な日時を定義(***特定の時間間隔で実行...***)または、スキャン起動のトリガとなるイベントを定義(***コンピュータの起動時に実行***)することでタイミングを定義できます。

高度なスケジュール オプション

このセクションでは、コンピュータが低電源モードあるいは完全に電源オフになっている場合に、スキャンが実行される条件を定義します。スケジュール済みのスキャンが指定した時間に起動すると、AVGシステムトレイアイコン上に開かれるポップアップウィンドウで通知されます。

次に、スケジュール スキャンが実行中であることを通知する新しいAVG システム トレイ アイコン(*全色で点滅表示*)が表示されます。AVG アイコンを右クリックすると、コンテキスト メニューが開き、実行中のスキャンの一時停止または停止を行えます。また、現在実行中のスキャンの優先度も変更できます。

[***スキャン方法***] タブには、任意でオン/オフを切り替えられるスキャンパラメータの一覧が表示されます。既定ではほとんどのパラメータがオンになっており、その機能はスキャン実行中に適用されます。***この設定を変更する合理的な理由がない場合は、あらかじめ定義された設定を維持することを推奨します。***

- ***自動的に感染を修復/除去する*** *(既定ではオン)*: スキャン実行中にウイルスが特定され、修復可能な場合は、自動的に修復されます。感染したファイルを自動的に修復できない場合、感染したオブジェクトはウィルス隔離室に移動されます。
- ***不審なプログラムとスパイウェア脅威を報告する*** *(既定ではオン)*: チェックを付けると、スパイウェア対策エンジンを有効にし、ウイルスと同時にスパイウェアもスキャンします。スパイウェアは疑わしいマルウェアのカテゴリに含まれます。通常は、セキュリティリスクとなる場合でも、このようなプログラムを故意にインストールすることができます。コンピュータのセキュリティを高めるため、この機能を有効にしておくことをお勧めします。
- ***不審なプログラムの拡張セットを報告する*** *(既定ではオフ)*: 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。スパイウェアとは、直接製造元から入手する場合にはまったく問題がなく、無害なプログラムですが、後から悪意のある目的で誤用されるおそれのあるプログラムです。これは、コンピュータセキュリティ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。
- ***Tracking Cookie をスキャンする*** *(既定ではオフ)*: スパイウェア対策コンポーネントのこのパラメータを定義すると、スキャン実行中に Cookie を検出します (***HTTP cookie は、サイトの設定***

や電子ショッピング カートの内容など、ユーザー固有の情報の認証、追跡、メンテナンスに使用されます)。

- ***アーカイブの内容をスキャンする*** (*既定ではオフ*): このパラメータを定義すると、ファイルが ZIP や RAR などのアーカイブで保存されている場合でも、すべてのファイルに対してスキャン チェックを実行します。
- ***ヒューリスティック分析を使用する*** (*既定ではオン*): ヒューリスティック分析 (*仮想コンピュータ環境で実行されるスキャン対象オブジェクト命令の動的エミュレーション*) は、スキャン実行中に採用されるウイルス検出方法の 1 つです。
- ***システム環境をスキャンする*** (*既定ではオン*): コンピュータのシステム領域もチェックされます。
- ***完全スキャンを有効にする*** (*既定ではオフ*) - このオプションをチェックすると、特定の状況 (*コンピュータが感染している疑いがある場合など*) が発生した場合に最も完全なスキャン アルゴリズムを有効にし、感染の可能性が非常に低いコンピュータ領域もスキャンします。これにより、問題がないことを確実に確認します。この方法を実行すると多少時間がかかります。
- ***ルートキットをスキャンする*** (*既定ではオフ*): この項目にチェックを付けると、完全コンピュータ スキャン中にルートキットをスキャンします。また、ルートキット スキャンはルートキット対策 コンポーネントでも独自に実行できます。

さらに、スキャンするかどうかを決定する必要があります。

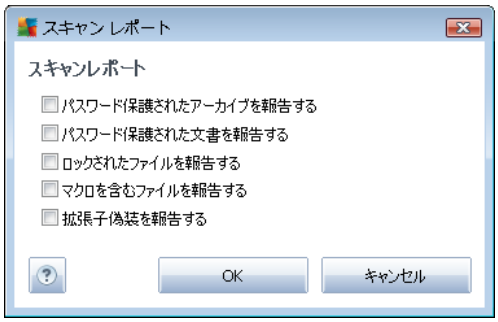
- ***すべてのファイル タイプとスキャン対象ではないファイル拡張子をカンマで区切ったリスト*** (*保存すると、カンマはセミコロンに変わります*) を入力することで、スキャンからの除外を定義できます。
- ***選択したファイル タイプ*** - 感染の可能性のあるファイルのみを指定できます (*一部のプレーン テキスト ファイルやその他の非実行可能ファイルなど*感染の可能性がないファイルはスキャンされません)。これには、メディア ファイル (*ビデオ、オーディオ ファイル*) が含まれます。多くの場合、このようなファイルはサイズが非常に大きく、ウィルスに感染している可能性が非常に低いため、このボックスのチェックを外すと、スキャン時間がさらに短縮されますここでも、必ずスキャンするファイルの拡張子を指定できます。
- 任意で***拡張子のないファイルをスキャン***できます。このオプションは既定ではオンになっています。変更する理由がない場合は、この設定を保持することをお勧めします。拡張子のないファイルは不審であるため、常にスキャンすることをお勧めします。

スキャン速度を調整

[***スキャン速度を調整***] セクションでは、システム リソース使用度に応じて、任意のスキャン速度を指定できます。*既定ではこのオプションの値は、自動的にリソースを使用するユーザー依存*レベルに設定されています。スキャンを高速化すると、スキャン時間を短縮できますが、スキャン実行中にシステム リソース消費量が著しく上がり、PC で実行されている他の作業の速度が低下します (*このオプションは、コンピュータの電源がオンであり、コンピュータ上で作業をしているユーザーがいない場合などに適しています*)。一方、スキャンの時間を延長することで、システム リソース消費量を下げることができます。

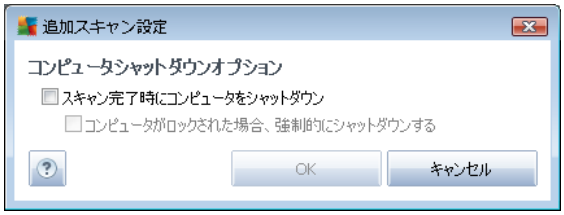
追加スキャン レポートを設定

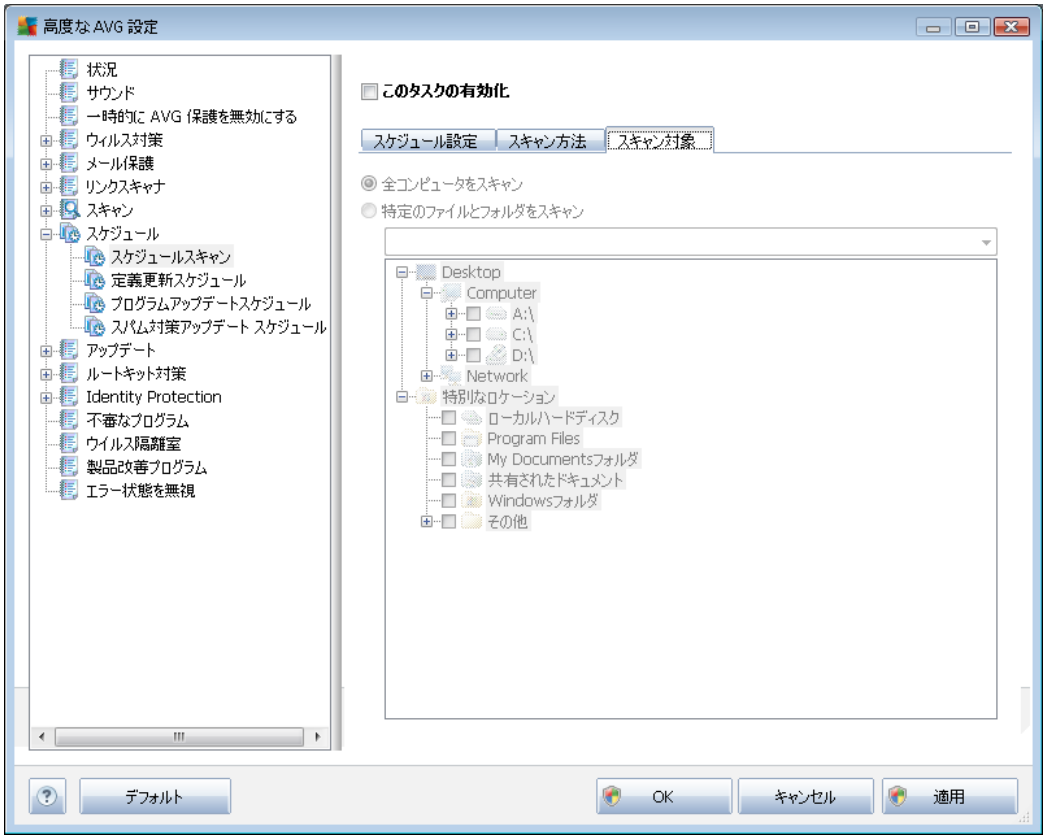
[***追加スキャン レポート...***] リンクをクリックすると、[***スキャン レポート***] ダイアログが開きます。このウィンドウでは報告する検出項目を定義します。



追加スキャン設定

[***追加スキャン設定...***] をクリックすると、新しい***コンピュータ シャットダウン オプション*** ダイアログが表示されます。このダイアログではスキャン処理の終了時に自動的にコンピュータをシャットダウンするかどうかを決定できます。このオプション (***スキャン完了時にコンピュータをシャットダウン***) を選択すると、現時点でコンピュータがロックされている場合でも、コンピュータをシャットダウンさせる新しいオプション (***コンピュータがロックされた場合強制的にシャットダウンする***) が有効になります。





[***スキャン対象***] タブでは、全 コンピュータをスキャン、あるいは特 定 のファイルやフォルダをスキャンのいずれかを選 択 します。特 定 のファイルやフォルダスキャン を選 択 した場 合 、ダイアログ下 部 のツリービューで対 象 フォルダを指 定 することができます。

9.8.2. 定義更新スケジュール

やむを得ない理由がある場合、[***このタスクを有効にする***] 項目のチェックを外してスケジュールされた定義更新を一時的に無効にして、後から再度有効にすることができます。

このダイアログでは、一部の詳細な定義更新スケジュールのパラメータを設定します。[***名前***] テキストフィールド（*すべての既定のスケジュールでは無効化*）には、プログラムベンダーによってこのスケジュールに割り当てられた名前があります。

スケジュール実行

このセクションでは、新しくスケジュールされた定義更新を実行する時間間隔を指定します。タイミングは、特定の期間の後に繰り返し起動するアップデート (***...ごとに実行***) または正確な日時 (***特定の時刻に実行...***) を指定することで、定義できます。

高度なスケジュールオプション

このセクションでは、コンピュータが低電力モードあるいは完全に電源オフになっている場合に、定義更新が実行される条件を定義します。

他のアップデート設定

最後に、[***インターネット接続が利用できるようになった時点ですぐにアップデートを再実行する***] オプションにチェックをすると、インターネット接続に障害が発生し、アップデート処理が失敗した場合、インターネット接続が復旧した時点で必ずすぐにアップデートを再開するようにできます。スケジュール済みのアップデートが指定した時間に起動すると、AVGシステムトレイアイコン上に開くポップアップウィンドウによってこのことが通知されます（*高度な設定/表示ダイアログ*の既定の設定を保持している場合）。

9.8.3. プログラム アップデート スケジュール

やむを得ない理由がある場合、[***このタスクを有効にする***] 項目のチェックを外してスケジュールされたプログラム更新を一時的に無効にして、後から再度有効にすることができます。

[***名前***] テキスト フィールド（*すべての既定のスケジュールでは無効化*）には、プログラム ベンダーによってこのスケジュールに割り当てられた名前があります。

スケジュール実行

ここでは、プログラムアップデート実行時間を指定します。タイミングは、***定期実行***、***指定した時間に実行***、***アクションにより実行***のいずれかによって定義することができます。

高度なスケジュールオプション

このセクションでは、コンピュータが低電源モードあるいは完全に電源オフになっている場合に、プログラムアップデートが実行される条件を定義します。

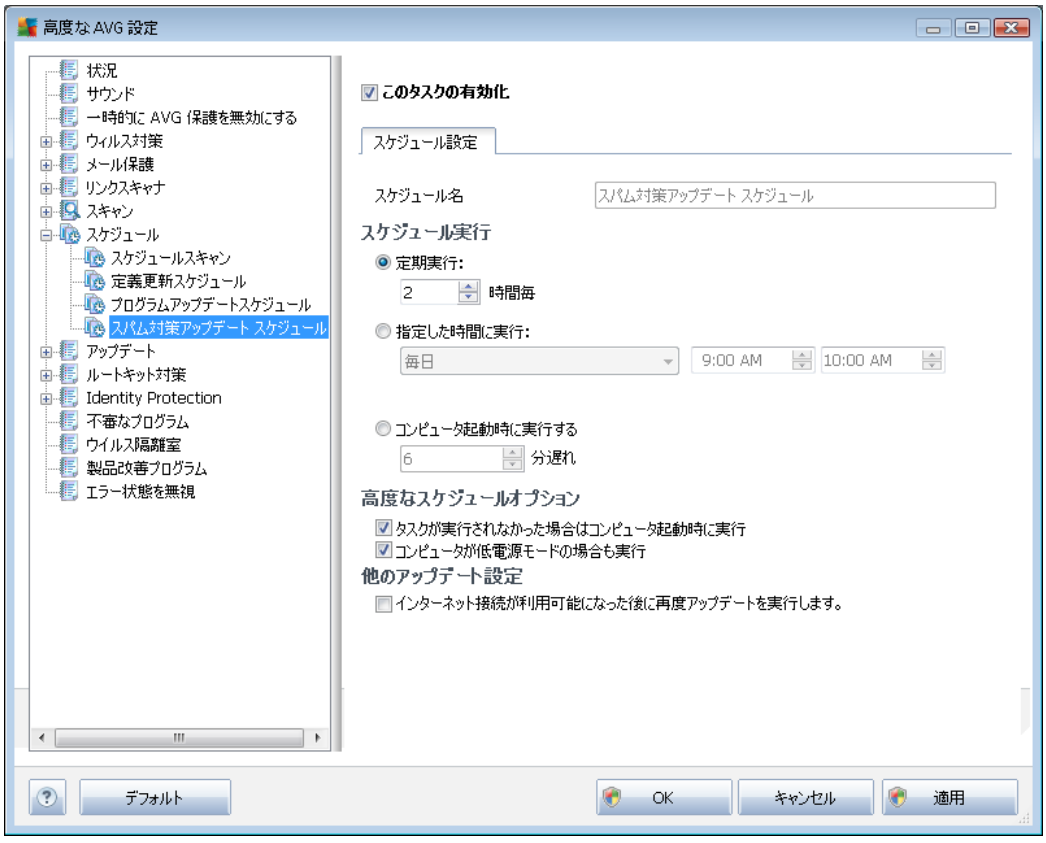
他のアップデート設定

[***インターネット接続が利用できるようになった時点ですぐにアップデートを再実行する***] オプションにチェックをすると、インターネット接続に障害が発生し、アップデート処理が失敗した場合、インターネット接続が復旧した時点で必ずすぐにアップデートを再開するようにできます。スケジュールされた更新が指定した時間に起動すると、AVG システム トレイ アイコン上に開くポップアップウィンドウによって通知されます（*高度な設定/表示ダイアログ*の既定の設定を保持している場合）。

***メモ**: スケジュール プログラム更新の時間がスケジュール スキャンの時間と同じになった場合は、更新処理が最優先され、スキャンは中断されます。*

9.8.4. スパム対策アップデート スケジュール

やむを得ない理由がある場合、[***このタスクを有効にする***] 項目のチェックを外してスケジュールされたスパム対策更新を一時的に無効にして、後から再度有効にすることができます。



このダイアログでは、一部の詳細なアップデートスケジュールのパラメータを設定します。[***名前***] テキスト

フィールド（*すべての既定のスケジュールでは無効化*）には、プログラムベンダーによってこのスケジュールに割り当てられた名前があります。

スケジュール実行

ここでは、新しくスケジュールされたスパム対策アップデート起動までの時間を指定します。ある期間の後に（..ごとに実行）繰り返される***スパム対策***更新起動を定義、正確な日時（***特定の間隔で実行***）を定義、あるいは更新起動が関連付けられるイベント（***コンピュータ起動に基づくアクション***）を定義する方法のいずれかでタイミングを定義できます。

高度なスケジュール オプション

このセクションでは、コンピュータが低電力モードあるいは完全に電源オフになっている場合に、スパム対策更新が実行される条件を定義します。

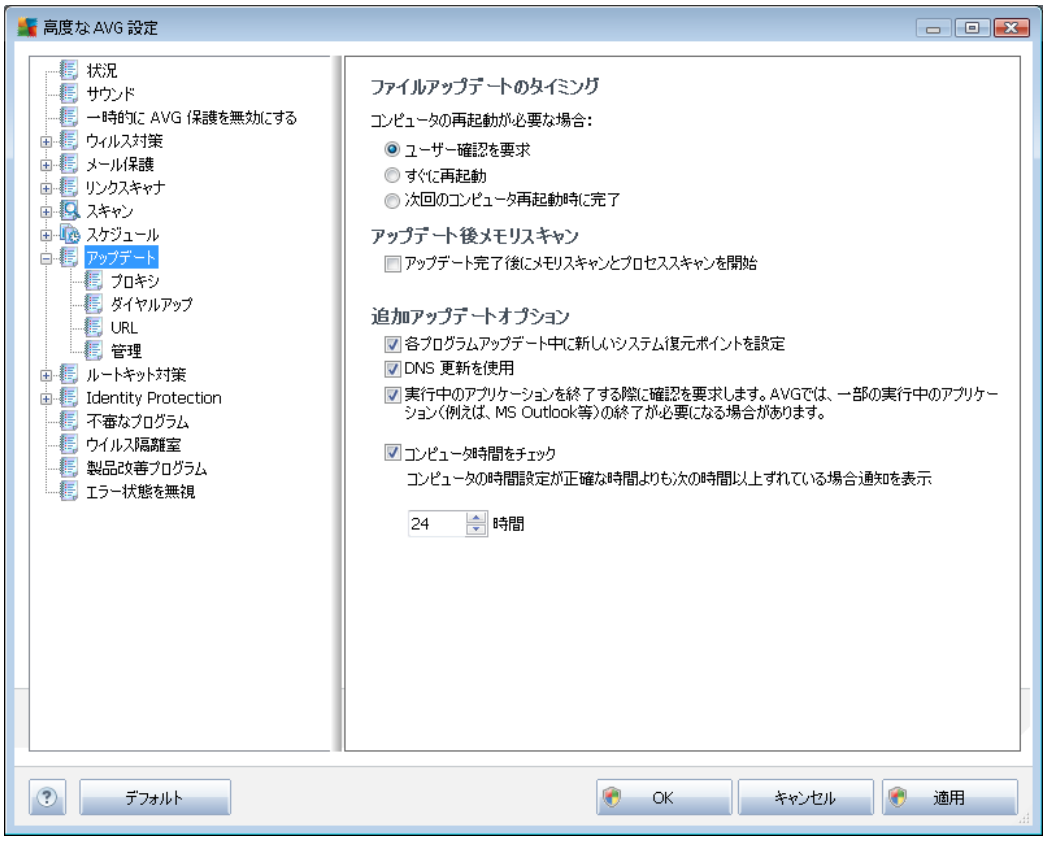
他のアップデート設定

[***インターネット接続が利用できるようになった時点ですぐにアップデートを再実行する***] オプションにチェックをすると、インターネット接続に障害が発生し、スパム対策更新処理が失敗した場合、インターネット接続が復旧した時点で必ずすぐに更新を再開するようにできます。

スケジュールされたスキャンが指定した時間に起動すると、AVG システム トレイ アイコン上に表示されるポップアップ ウィンドウによってこのことが通知されます（*高度な設定/表示ダイアログの既定の設定を保持している場合*）。

9.9. 更新

アップデートナビゲーションは、新しいダイアログを開きます。このダイアログでは、AVGアップデートに関する一般的なパラメータを指定します。



ファイルアップデートのタイミング

このセクションでは、更新処理によってPCの再起動が必要な場合に、3つのオプションから選択できます。次回のPCの再起動時に更新を完了するようにスケジュール設定するか、ただちに再起動できます。

- ***ユーザーの確認を要求***（既定）- 更新処理完了に必要なPC再起動を確認する画面が表示されます。
- ***すぐに再起動*** - コンピュータは更新処理が完了した時点で、自動的に即時再起動されます。ユーザー確認は要求されません。
- ***次回のコンピュータの再起動時に完了*** - 更新処理の完了は次回のコンピュータの再起動時まで延期されます。コンピュータが少なくとも1日に1回定期的に再起動することが確実である場合にのみ、このオプションが推奨されます。

アップデート後 メモリスキャン

このチェックボックスをオンにすると、各 アップデートが正 常 に完 了 した後 に、新 しいメモリスキャンを起 動 するように定 義 します。ダウンロードした最 新 のアップデートには新 しいウィルス定 義 が含 まれている場 合 がありますが、即 時 スキャンに適 用 されます。

追 加 アップデートオプション

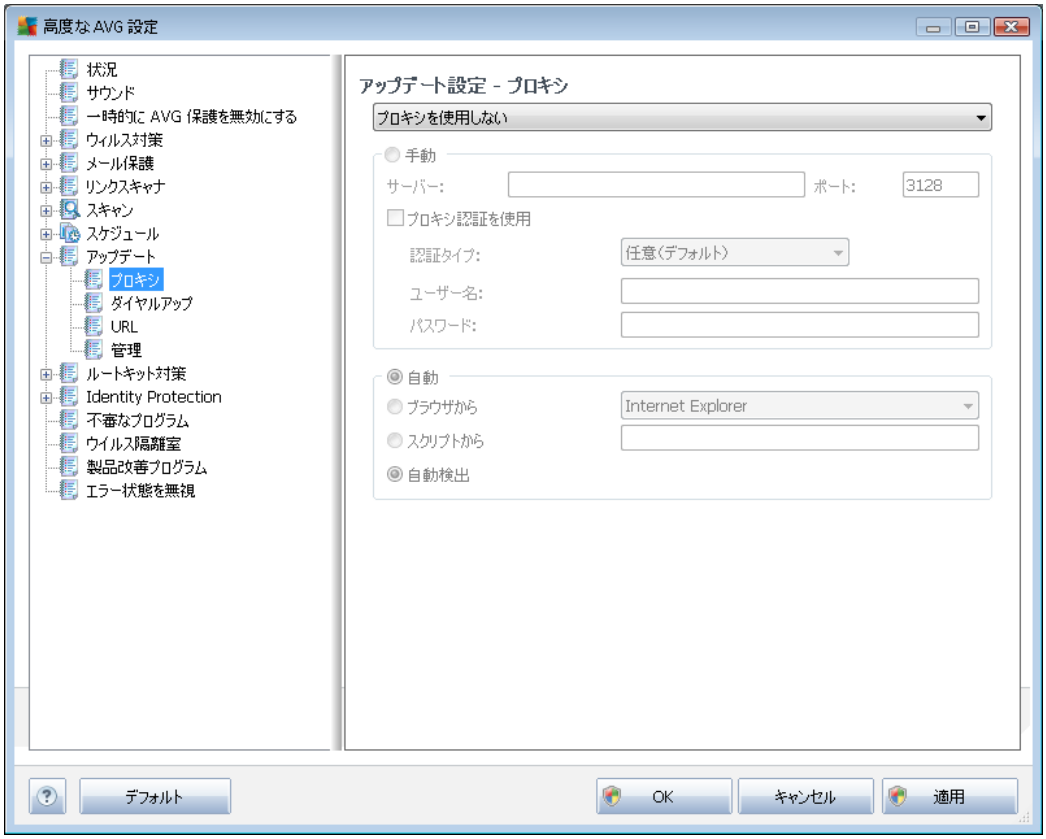
- ***各 プログラム更 新 中 に新 しいシステム復 旧 ポイントを作 成 する*** - 各 AVG プログラム更 新 の起 動 前 に、システム復 旧 ポイントが作 成 されます。アップデートプロセスが失 敗 し、オペレーティングシステムがクラッシュする場 合 には、必 ずこのポイントから元 のコンフィグレーションでOS を復 旧 できます。このオプションは、スタート/プログラム/アクセサリ/システムツール/システムの復 元 からアクセスできますが、上 級 ユーザーのみが変 更 を行 うようにすることをお勧 めします。この機 能 を使 用 する場 合 は、このチェックボックスにチェックを付 けておきます。

- ***DNS 更 新 を使 用 する*** (*既 定 ではオン*) - この項 目 にチェックを付 けると、更 新 が実 行 された時 点 で、**AVG Anti-Virus 2012** が DNS サーバー上 の最 新 のウィルス データベース バージョンと最 新 のプログラム バージョンに関 する情 報 を検 索 します。次 に、最 小 限 の必 須 の更 新 ファイルのみがダウンロードされ、適 用 されます。この方 法 ではダウンロードされるデータ量 が最 低 限 に抑 えられるため、更 新 処 理 が高 速 で実 行 されます。

- ***実 行 中 のアプリケーションを終 了 する確 認 を要 求*** (*既 定 では有 効*) をチェックすることで、更 新 処 理 の完 了 に必 要 な場 合 、現 在 実 行 中 のアプリケーションが許 可 なく終 了 しないように確 認 できます。

- ***コンピュータ時 間 を確 認*** - このオプションにチェックを付 けると、コンピュータ時 間 と正 確 な時 間 との差 が指 定 された時 間 よりも大 きい場 合 に通 知 を表 示 するよう宣 言 します。

9.9.1. プロキシ



プロキシサーバーとは、より安全なインターネット接続を保証するスタンドアロンサーバー、またはPC上のサービスです。特定のネットワークルールによって、インターネットに直接またはプロキシサーバーを介して接続できます。次に、***アップデート設定 - プロキシ***ダイアログの最初のアイテムで、コンボボックスメニューから希望するものを選択する必要があります。

- ***プロキシを使用***
- ***プロキシを使用しない*** - 既定の設定
- ***プロキシを使用して接続し、失敗した場合のみ直接接続します。***

プロキシを使用するオプションを選択した場合、さらにいくつかのデータを指定する必要があります。サーバー設定は手動あるいは自動で行われます。

手動設定

手動設定（***手動***オプションをチェックすると、該当する入力欄が有効化されます）を選択する場合、以下の項目を指定してください。

- ***サーバー***—サーバーのIPアドレスまたはサーバー名を指定します。

- ***ポート***–インターネットアクセスを許可するポート番号を指定します（*デフォルトでは、この番号は3128に設定されていますが、変更可能です–不明な場合は、ネットワーク管理者にお問い合わせください*）

プロキシサーバーは、各ユーザーのルールを設定することもできます。プロキシサーバーがこのように設定されている場合、***プロキシ認証を使用***にチェックを付け、有効なユーザー名とパスワードを入力してください。

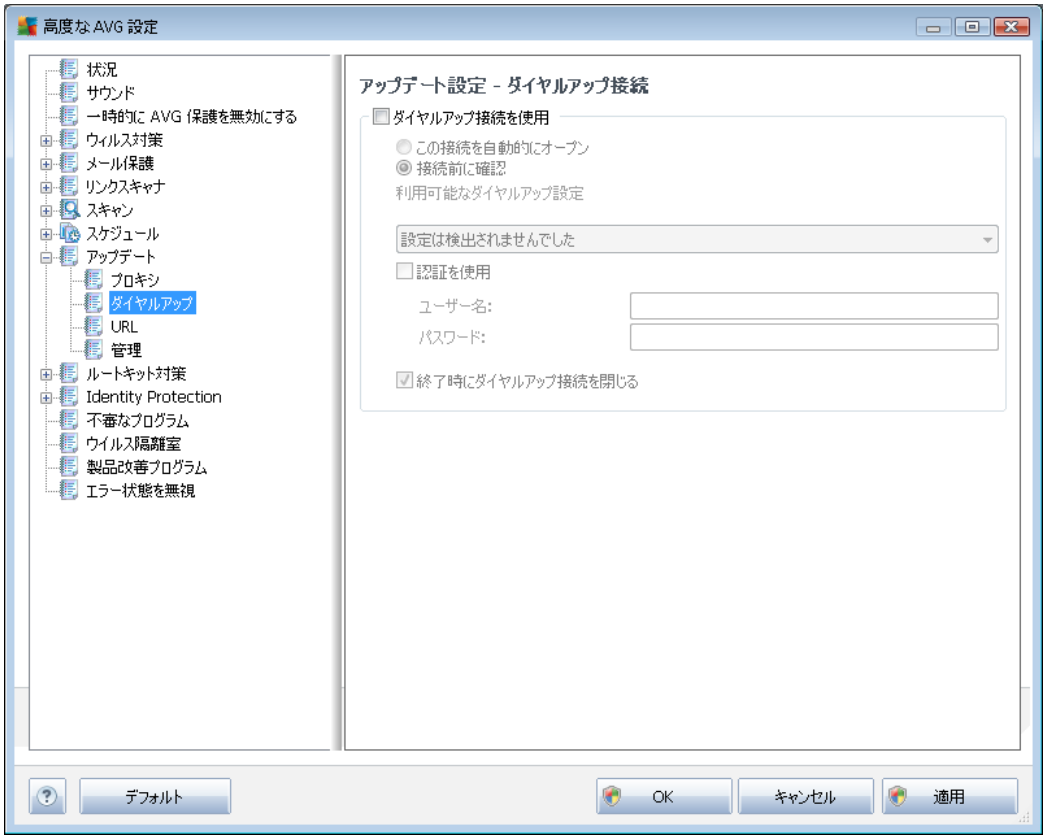
自動設定

自動設定を選択する場合（***自動***を*選択すると、該当する入力欄が有効化されます。*）、プロキシ設定をどこから取得するかを選択します。

- ***ブラウザから*** - 既定のインターネットブラウザから設定を読み取ります。
- ***スクリプトから*** - 設定は、プロキシアドレスを返す機能とともに、ダウンロードされたスクリプトから読み込まれます。
- ***自動検出*** - 設定は、プロキシサーバーから直接検出されます。

9.9.2. ダイヤルアップ

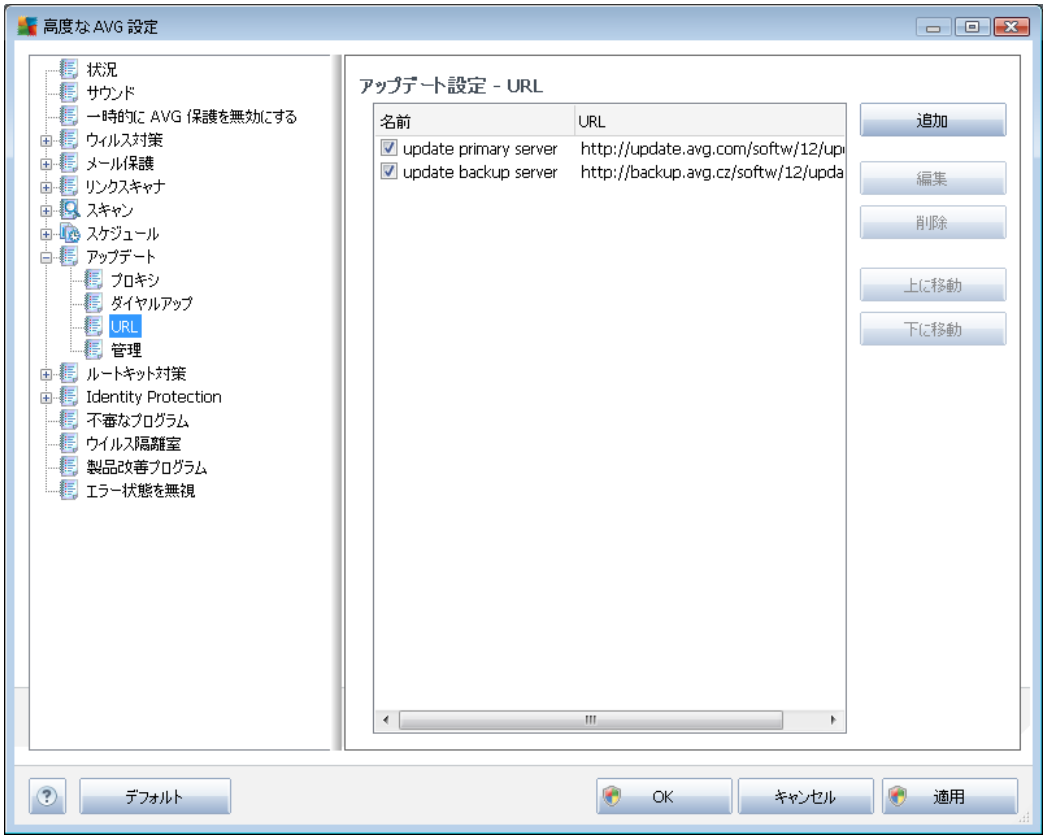
アップデート設定 - ダイヤルアップ接続ダイアログでは、インターネットへのダイヤルアップ接続のためのパラメータを設定します。各欄は[***ダイヤルアップ接続を使用***]オプションをチェックすると、変更可能となります。



インターネットに自動接続（***自動的にこの接続をオープン***）するか、毎回手動で接続を確認（***接続前に確認***）するかを指定します。自動接続については、さらに接続がアップデート終了後に切断されるかどうかを選択します（***終了後ダイヤルアップ接続を閉じる***）。

9.9.3. URL

[***URL***] ダイアログは更新ファイルがダウンロードされるインターネット アドレスのリストを提供します。



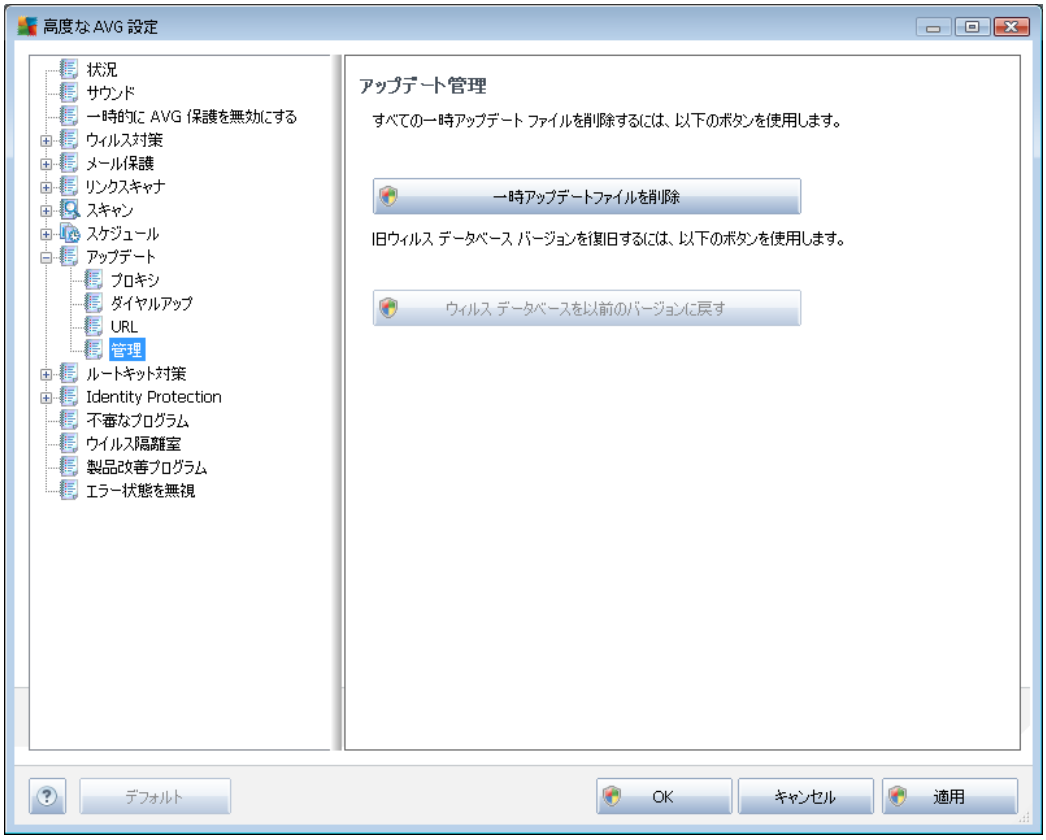
コントロール ボタン

このリストは、以下のコントロールボタンを使用して修正します。

- ***追加***–ダイアログを開き、新しいURLを指定してリストに追加します
- ***編集***–ダイアログを開き、選択されたURLパラメータを編集します。
- ***削除***–選択されたURLをリストから削除します。
- ***上に移動***–選択されたURLを1つ上の場所に移動します。
- ***下に移動***– 選択されたURLを1つ下の場所に移動します。

9.9.4. 管理

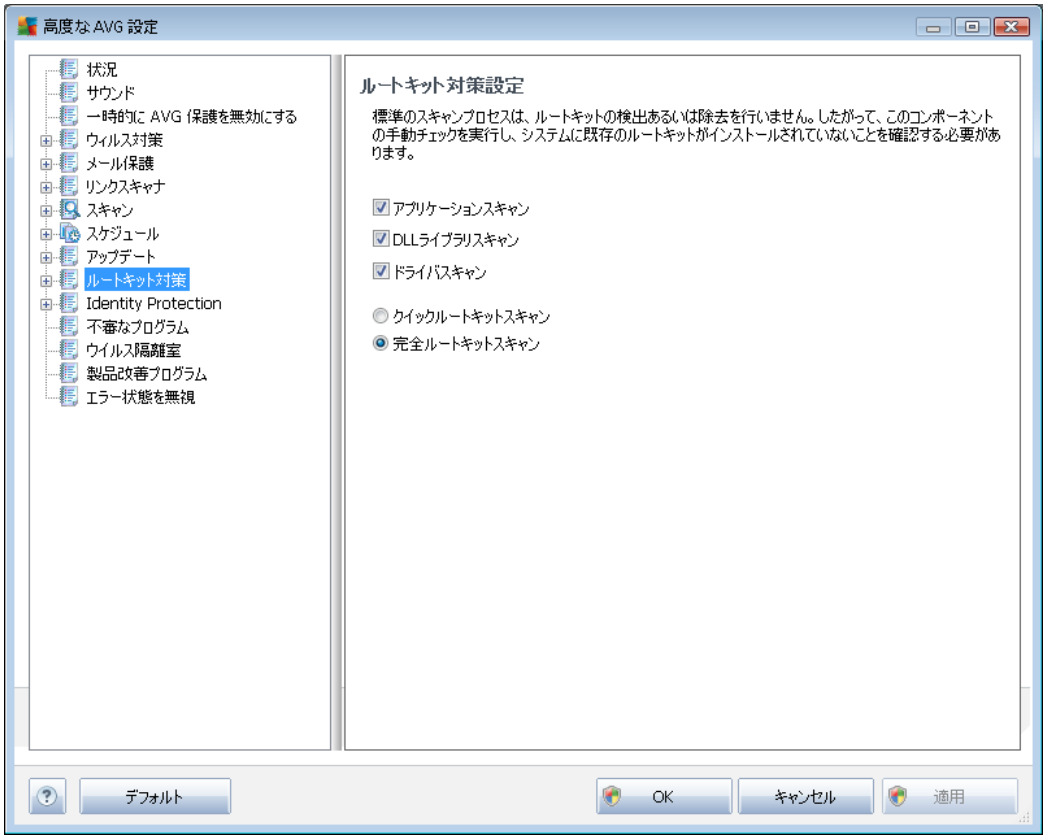
[***アップデート管理***] ダイアログには 2 つのオプションがあり、2 つのボタンを使用してアクセスできます。



- ***一時アップデートファイルの削除*** - このボタンをクリックすると、すべての重複するアップデートファイルをハードディスクから削除します（*デフォルトでは、これらのファイルは 30 日間保存されます*）
- ***ウイルスデータベースを以前のバージョンに戻す*** - このボタンをクリックすると、最新のウイルスベースのバージョンをハードディスクから削除し、以前に保存されたバージョンに戻します（*新しいウイルスベースのバージョンは次回のアップデートに含まれます*）

9.10. ルートキット対策

[***ルートキット対策設定***] ダイアログでは、ルートキット対策 コンポーネントの設定を編集できます。



このダイアログ内で提供されているルートキット対策***コンポーネントのすべての機能に対する編集は、ルートキット対策 コンポーネントのインターフェースから直接行うこともできます。

該当するチェックボックスにチェックを付け、スキャン対象オブジェクトを指定します。

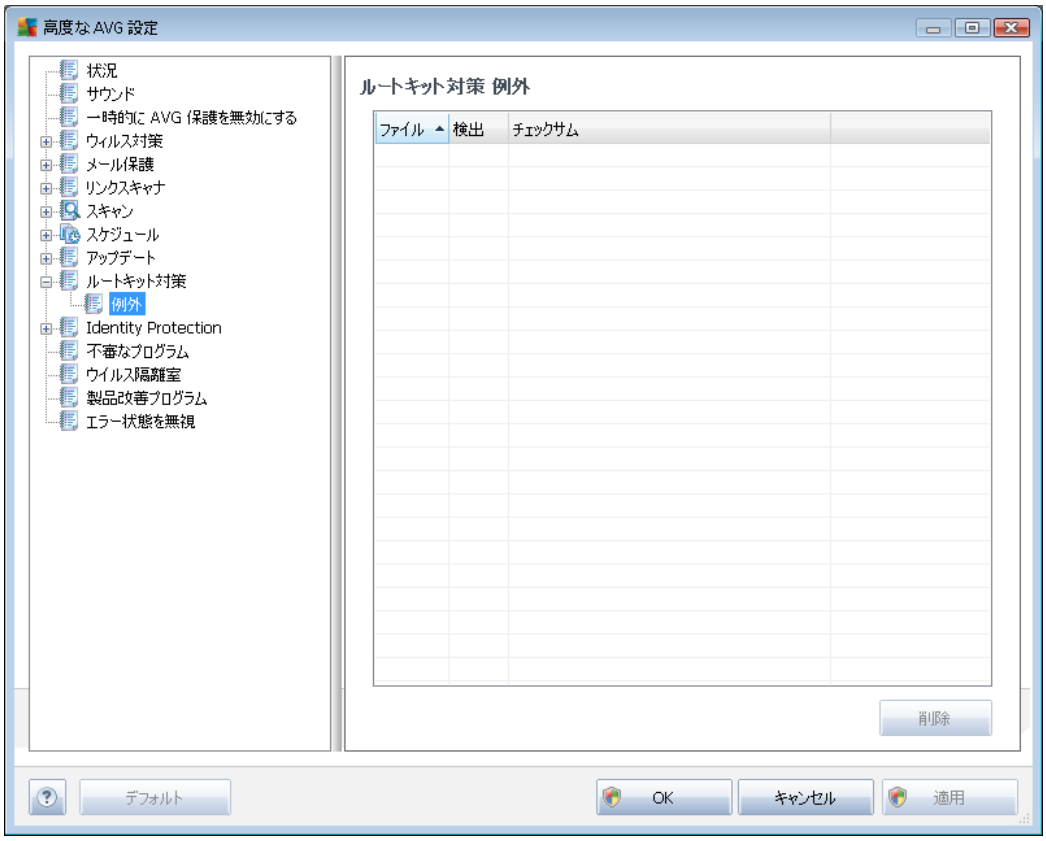
- ***アプリケーション スキャン***
- ***DLL ライブラリ スキャン***
- ***ドライバ スキャン***

さらに、ルートキット スキャン モードを選択できます。

- ***クイック ルートキット スキャン*** - すべての実行中のプロセス、ロードされたドライバ、およびシステム フォルダ (*通常は、c:\Windows*) をスキャンします。
- ***完全 ルートキット スキャン*** - すべての実行中のプロセス、ロードされたドライバ、システム フォルダ (*通常は、c:\Windows*)、およびすべてのローカル ディスク (*フラッシュ ディスクは含まれますが、フロッピー ディスクおよび CD ドライブは含まれません*) をスキャンします。

9.10.1. 例外

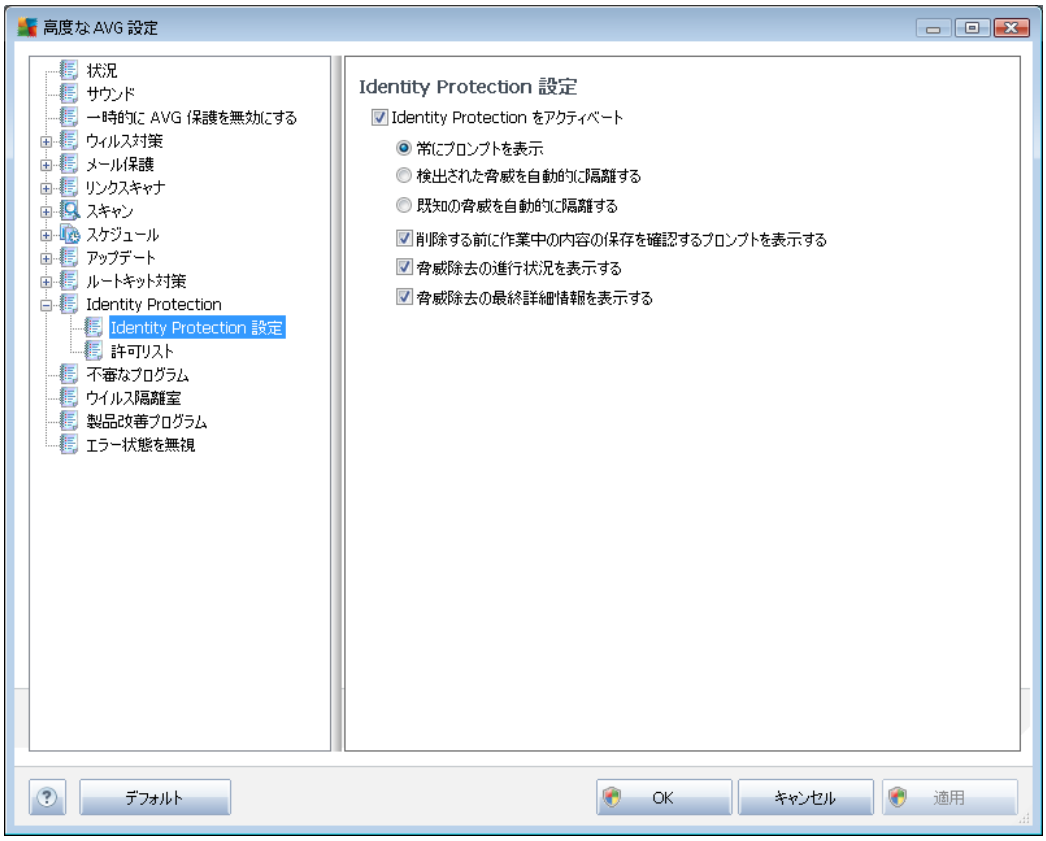
[***ルートキット対策 例外***] ダイアログでは、このスキャンから除外する特定のファイルを指定できます (*ルートキットとして誤検出される可能性のあるドライバなど*)。



9.11. Identity Protection

9.11.1. Identity Protection 設定

[***Identity Protection 設定***] ダイアログでは、Identity Protectionコンポーネントの基本機能のオン/オフを切り替えられます。



Identity Protection を有効化 (*既定ではオン*) - チェックを外すと、Identity Protectionコンポーネントをオフにします。

必要でない場合は、これを行わないことを強く推奨します。

Identity Protectionが有効化されている時は、脅威が検出された時の動作を指定できます。

- ***常にプロンプトを表示*** (*デフォルトではオン*) - 脅威が検出されたときに、隔離室に移動するかを確認するプロンプトが表示され、実行するアプリケーションが削除されないようになります。
- ***自動的に検出された脅威を隔離*** - (デフォルトではオフ) このチェックボックスをオンにすると、すべての検出された潜在的な脅威は即時 ウイルス隔離室 の安全な場所に移動されます。既定の設定を保持していると、脅威が検出されたときに、隔離室に移動するかを確認するプロンプトが表示され、実行するアプリケーションが削除されないようになります。
- ***自動的に既知の脅威を隔離*** - マルウェアの可能性があるものとして検出された全てのアプリケーションを自動的に即時に ウィルス隔離室 に移動する場合は、この項目にマークを付けておきます。

さらに、特定の項目を割り当てて、任意で他の ID 保護 の機能をアクティブ化できます。

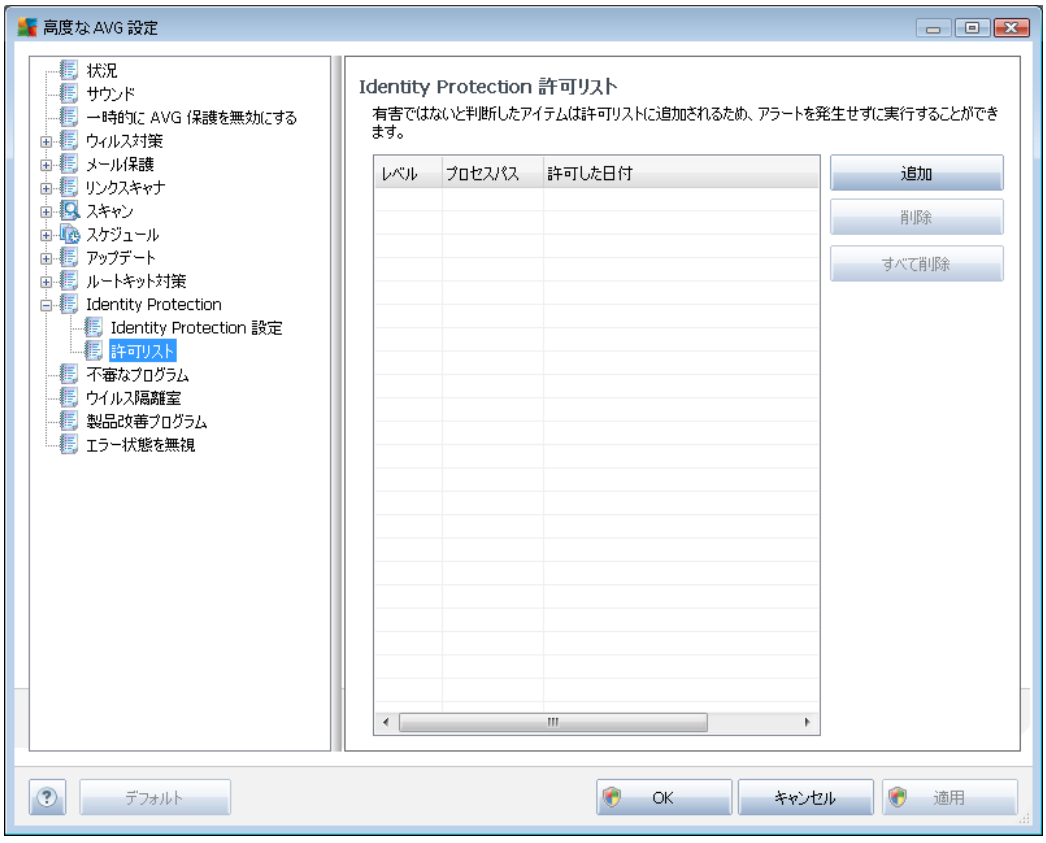
- ***除去前に作業内容の保存を確認するプロンプトを表示*** - (*デフォルトではオン*) - マルウェアの可能性があるものとして検出されたアプリケーションを隔離に移動する前に警告メッセージを表示する場合は、この項目をオンにしておきます。そのアプリケーションでのみ作業している場合は、プロジェクトが失われる可能性があるため、最初に保存しておく必要があります。デフォルトでは、この項目はオンであり、この設定を保持することをお勧めします。

- ***マルウェア除去の進捗を表示*** - (*デフォルトではオン*) - この項目をオンにすると、潜在的なマルウェアが検出された時点で、新しいダイアログが開き、マルウェアの隔離除去の進捗が表示されます。

- ***最終マルウェア除去の詳細情報を表示*** - (*デフォルトではオン*) - このアイテムをオンにすると、***ID 保護***は、隔離に移動された各オブジェクトに関する詳細 (*重要度レベル、場所など*) を*表示します*).

9.11.2. 許可リスト

[***Identity Protection 設定***] ダイアログで、[***検出された脅威を自動的に隔離する***] 項目のチェックを外すと、潜在的な危険性のあるマルウェアが検出されるたびに、削除確認ダイアログが表示されます。*動作に応じて検出された*不審なアプリケーションを安全なアプリケーションとして指定し、コンピュータ上で保持することを確認すると、そのアプリケーションはいわゆる***Identity Protection 許可リスト***に追加され、今後は潜在的に危険なアプリケーションとして報告されなくなります。



Identity Protection 許可リストは、各アプリケーションに関する次の情報を提供します。

- ***レベル*** - 重要度の低いもの (■□□□) から重大なもの (■■■■) までの 4 段階方式で各プロセス

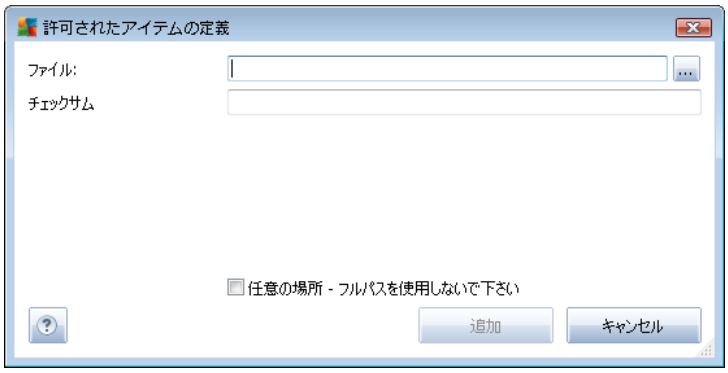
の重要度をグラフィカルに示します。

- ***プロセス パス*** - アプリケーションの (*プロセス*) 実行ファイルの場所へのパス
- ***許可された日付*** - 手動でアプリケーションを安全なアプリケーションとして指定した日

コントロール ボタン

[***個人情報保護許可リスト***] ダイアログでは次のコントロールボタンが利用できます。

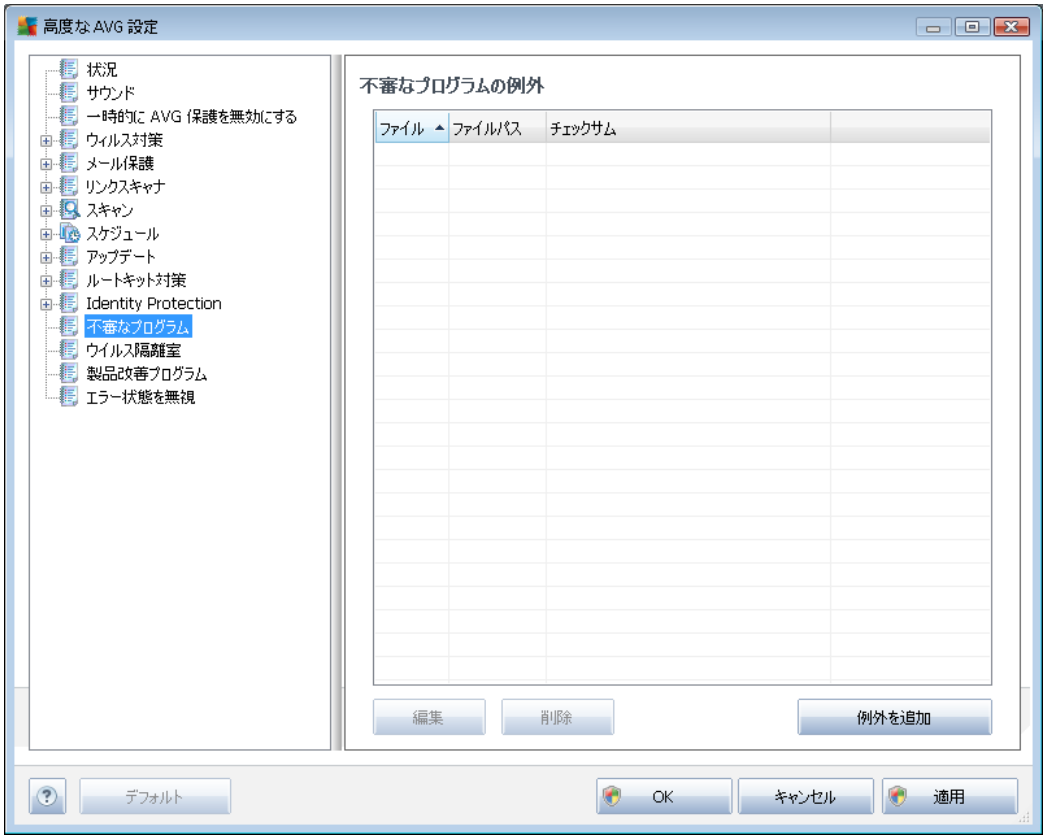
- ***追加*** - このボタンをクリックすると、許可リストに新しいアプリケーションを追加します。次のポップアップ ダイアログが表示されます。



  - ***ファイル*** - 例外として指定するファイル (*アプリケーション*) への完全パスを入力します。
  - ***チェックサム*** - 選択されたファイルの一意の「シグネチャ」を表示します。このチェックサムは自動的に生成された文字列です。AVG はこの文字列を使用して、選択されたファイルとその他のファイルを区別します。チェックサムはファイルが正常に追加された後で生成および表示されます。
  - ***任意の場所 - 完全パスを使用しない*** - 特定の場所のみに関連する例外としてこのファイルを定義する場合は、このチェックボックスのチェックを外します。
- ***削除*** - このボタンをクリックすると、選択したアプリケーションをリストから削除します。
- ***すべて削除*** - このボタンをクリックすると、リストに表示されているすべてのアプリケーションを削除します。

9.12. 不審なプログラム

AVG Anti-Virus 2012 はシステム内に存在する不審な実行可能アプリケーションや DLL ライブラリの分析と検出ができます。ユーザーが望ましくないプログラムをコンピュータに残しておきたい場合もあります (故意にインストールされたプログラム)。一部のプログラム (特に無料のプログラム) にはアドウェアが含まれています。このようなアドウェアは*不審なプログラム*として **AVG Anti-Virus 2012** によって検出および報告される場合があります。このようなプログラムをコンピュータに残す場合は、不審なプログラムの例外として定義できます。

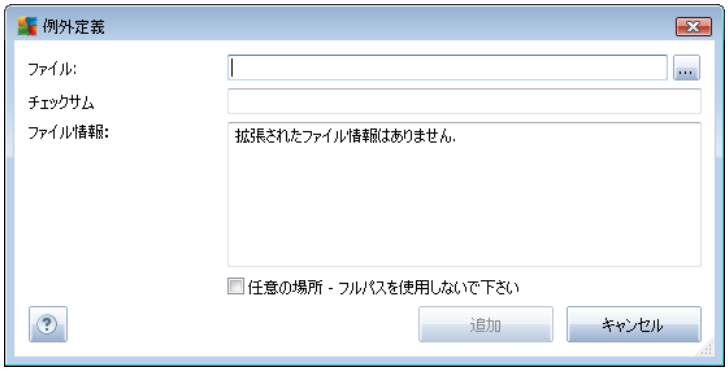


[***不審なプログラム例外***] ダイアログでは、既に定義された不審なプログラムの例外リストが表示されます。リストの編集、既存の項目の削除、新しい例外の追加ができます。各例外リストには次の情報が表示されます。

- ***ファイル*** - 各アプリケーションの正式名。
- ***ファイル パス*** - アプリケーションの場所。
- ***チェックサム***- 選択したファイルの一意の「シグネチャ」を表示します。このチェックサムは自動的に生成された文字列です。AVG はこの文字列を使用して、選択したファイルとその他のファイルを区別します。チェックサムはファイルが正常に追加された後で生成および表示されます。

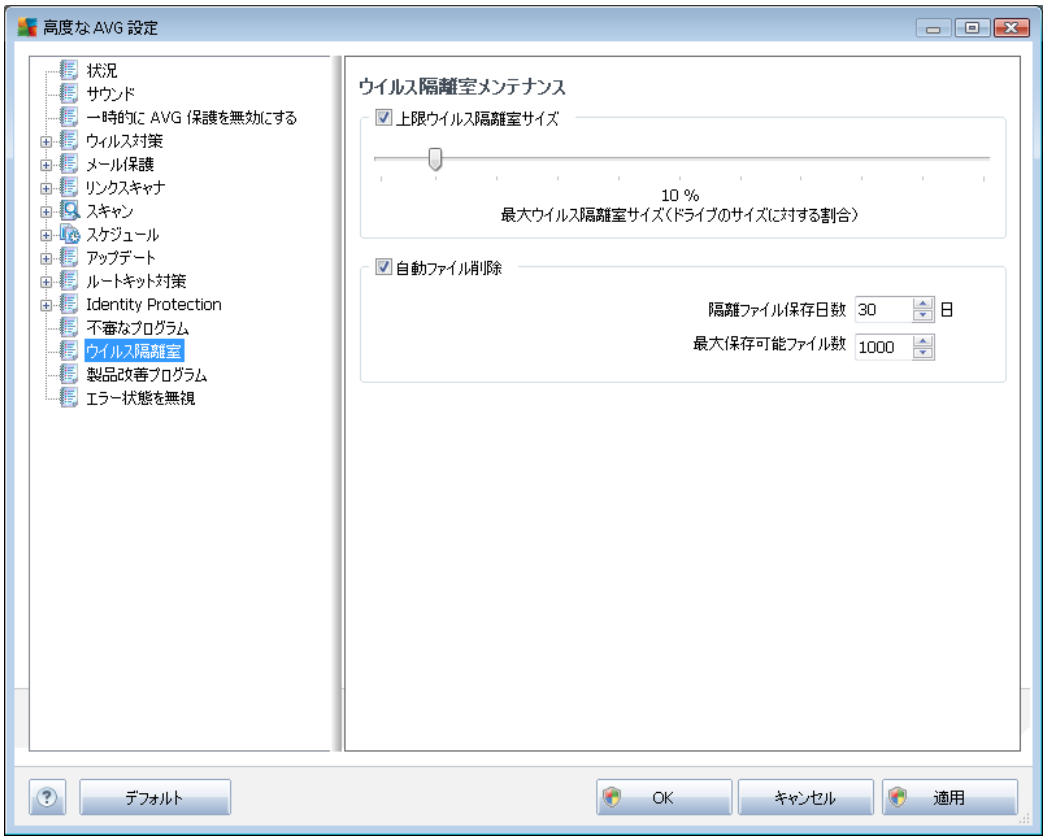
コントロール ボタン

- ***編集*** - 既に定義された例外の編集ダイアログ (*新しい例外定義ダイアログと同じです。次を参照*) を開きます。ここで例外パラメータを変更します。
- ***削除*** - 選択した項目を例外リストから削除します。
- ***例外の追加***- 編集ダイアログが開きます。ここでは作成する例外のパラメータを定義します。



- ***ファイル*** - 例外として指定するファイルへの完全パスを入力します。
- ***チェックサム*** - 選択したファイルの一意の「シグネチャ」を表示します。このチェックサムは自動的に生成された文字列です。AVG はこの文字列を使用して、選択したファイルとその他のファイルを区別します。チェックサムはファイルが正常に追加された後で生成および表示されます。
- ***ファイル情報*** - ファイルに関する追加情報 *(ライセンス/バージョンなど)*
- ***任意の場所 - 完全パスを使用しない*** - 特定の場所のみに関連する例外としてこのファイルを定義する場合は、このチェックボックスのチェックを外します。*このチェックボックスを選択すると、ファイルの保存場所に関係なく、指定したファイルが例外として定義されます (ただし、特定のファイルへの完全パスを入力する必要があります。これにより、システムに同じ名前のファイルが 2 つ存在している場合にファイルが一意の例として使用されます)*。

9.13. ウイルス隔離室



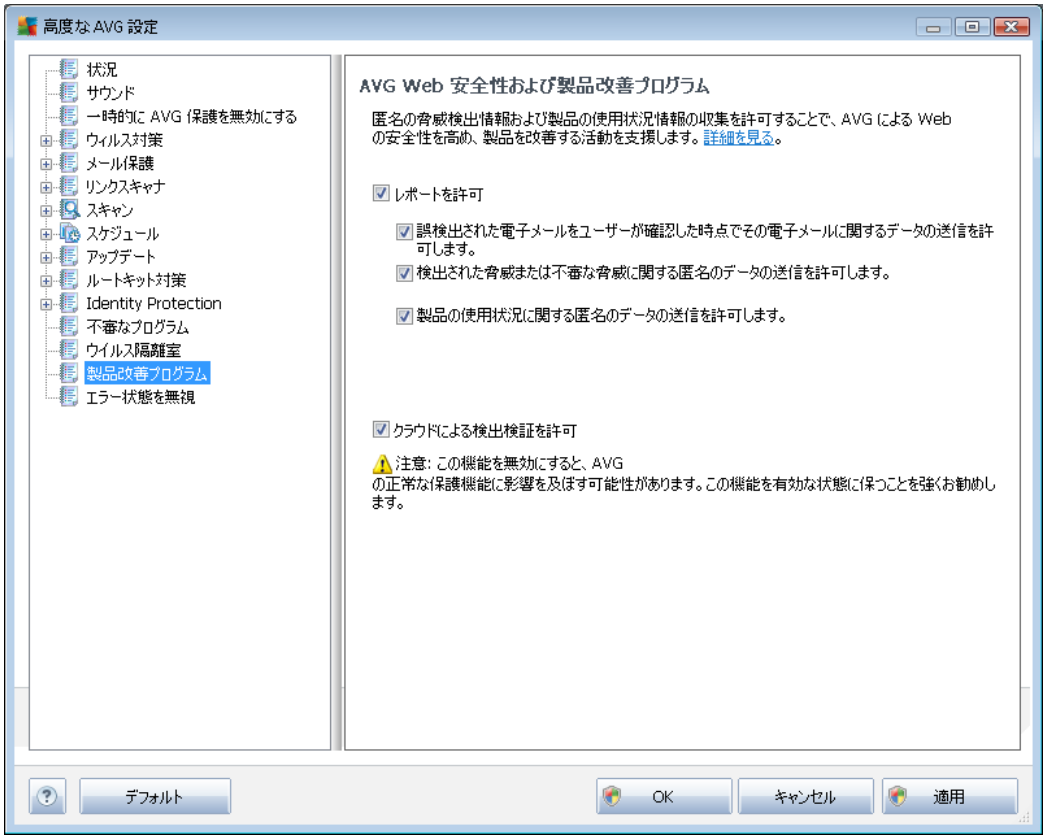
ウィルス隔離室メンテナンスダイアログでは、ウィルス隔離室に格納されるオブジェクト管理に関するパラメータを定義できます。

- ***ウイルス隔離室のサイズを制限*** - スライダを使用して、ウイルス隔離室の最大サイズを設定できます。サイズは、ローカルディスクのサイズに対する割合で指定されます。
- ***自動ファイル削除*** - このセクションでは、ウイルス隔離室にオブジェクトが格納される最大日数（***日数を経過したファイルの削除***）、とウイルス隔離室に格納される最大ファイル数（***格納されるファイルの最大数***）を定義します。

9.14. 製品改善プログラム

[***AVG Web 安全性および製品改善プログラム***] ダイアログでは、AVG 製品改善プログラムへの参加で実現できる全体的なインターネットセキュリティレベルの向上について案内されます。[***報告を許可する***] オプションにチェックを付けると、検出した脅威を AVG ラボに報告します。世界中のすべての参加者から最新の脅威に関する情報を収集し、保護を向上させます。

報告は自動的に実行され、面倒な手間はありません。また、個人情報は一切含まれません。検出した脅威の報告は任意ですが、このオプションを有効にしておくようにお願いしております。これにより、すべての AVG ユーザーの保護機能が強化されます。



今日においては、単なるウイルスだけではなく、さまざまな脅威が存在します。悪意のあるコードと危険な Web サイトの作成者は非常に革新的であり、新しい種類の脅威が常に出現しています。そしてその多くはインターネット上に存在しているのです。一般的な脅威:

- ***ウイルス***とは、それ自体をコピーし、拡大させる悪意のあるコードで、多くの場合、被害が出るまで気が付きません。一部のウイルスは深刻な脅威であり、独自の方法で、ファイルを削除したり意図的に変更したりします。ウイルスには、音楽を演奏するなど、一見無害のように見えるものもあります。ただし、すべてのウイルスは基本的に増殖する能力を持つため危険です。1 つのウイルスでさえコンピュータメモリ全体をすぐに制御し、障害を引き起こします。

- □□□□□□□□□□□□***ワーム***があります。通常のウイルスと異なり、ワームは感染する「キャリア」を必要としません。ワームは、通常それ自体を含んだメールで他のコンピュータに送信されます。結果、メールサーバーとネットワークシステムのオーバーロードなどを引き起こします。

- ***スパイウェア***は、通常マルウェアのカテゴリとして定義されます (*マルウェアとはウイルスを含む悪意のあるソフトウェアのことです*)。*このマルウェアには、コンピュータの所有者が知らない間に同意なく個人情報、パスワード、クレジットカード番号を盗んだり、コンピュータに侵入し、攻撃者にリモートでコンピュータをコントロールさせたりすることを目的とするプログラム (通常はトロイの木馬) が含まれます。*

- ***不審なプログラム***はスパイウェアの一種ですが、必ずしもコンピュータに被害を及ぼすとは限りません。PUP の具体的な例としては、ポップアップ広告を表示させ、広告を配信することを目的としたソフトウェアであるアドウェアがあります。これらは迷惑ではあるものの実際には無害です。

- □□□***Tracking cookie*** もスパイウェアの一種と見なされます。この小さなファイルは Web ブラウザに保存され、再度アクセスした際、自動的に「親」Web サイトに送信されます。Tracking cookie には閲覧履歴などのデータが含まれています。

- ***エクスプロイト***はオペレーティング システム、インターネット ブラウザ、あるいは重要なプログラムの欠陥や脆弱性を利用する悪意のあるコードです。

- ***フィッシング***は信頼できる有名な組織を装って重要な個人情報データを取得しようとする試みです。たとえば、被害者宛てに銀行口座の詳細情報を更新するように求める大量のメールが送信されます。ユーザーはリンクに従い、偽の銀行の Web サイトに誘導されます。

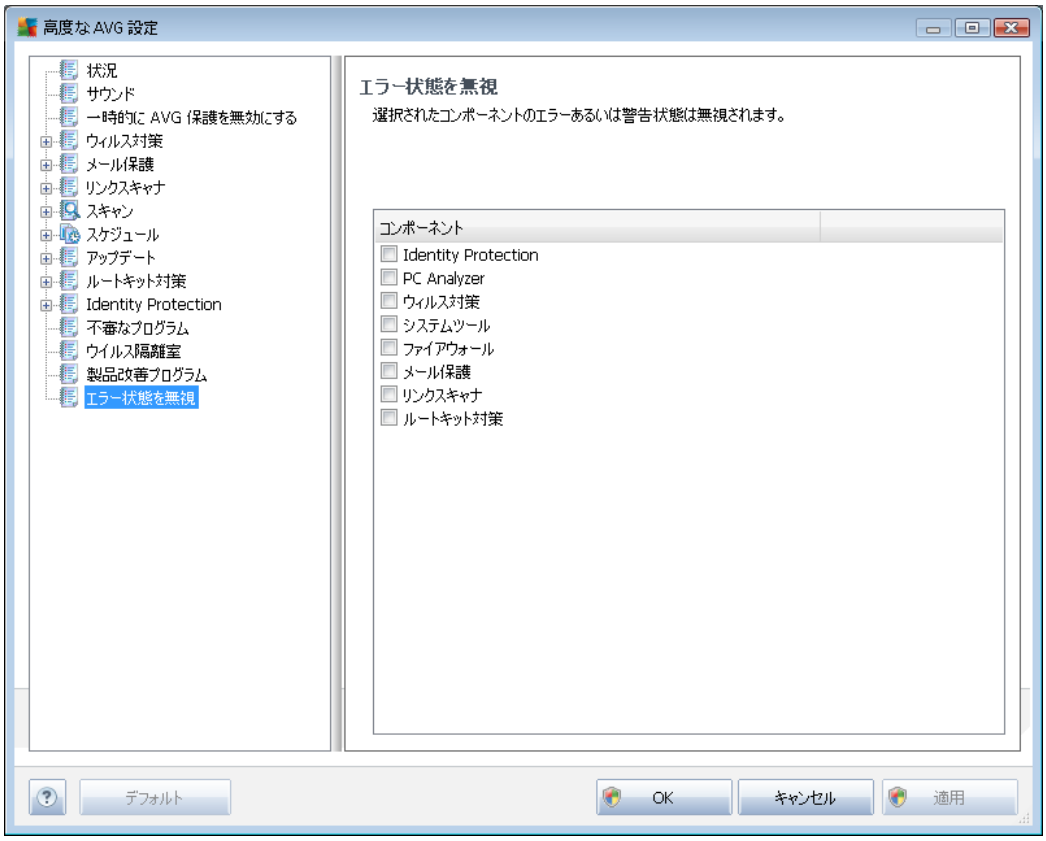
- ***Hoax は危険な情報、何かを警告する情報、あるいはただ単に迷惑で無用な情報を含む大量のメールです。***上記の脅威の多くは Hoax メール メッセージを使用して広がります。

- 悪意のある Web サイトとは、故意に悪意のあるソフトウェアをコンピュータにインストールするものです。ハッカーに攻撃されたサイトにも同様にアクセスしたユーザーを感染させる危険が潜んでいますが、このようなサイトは本来は合法的な Web サイトです。

このようなすべての種類の脅威からユーザーを保護するために、AVG Anti-Virus 2012 には特別なコンポーネントが含まれています。コンポーネントの概要については、「コンポーネント概要」の章を参照してください。

9.15. エラー状態を無視

[*エラー状態を無視*] ダイアログでは、情報の通知を表示しないコンポーネントにチェックを付けることができます。



既定では一覧で選択されているコンポーネントはありません。つまり、コンポーネントがエラーになると、すぐに次の方法で通知されます。

- システム トレイ アイコン - すべての AVG コンポーネントが正常に動作している間はアイコンは四色で表示されますが、エラーが発生すると、黄色のエクスクラメーション マークのついたアイコンが表示され、
- AVG メイン ウィンドウの [セキュリティステータス情報] セクションに既存の問題に関する説明が表示されます。

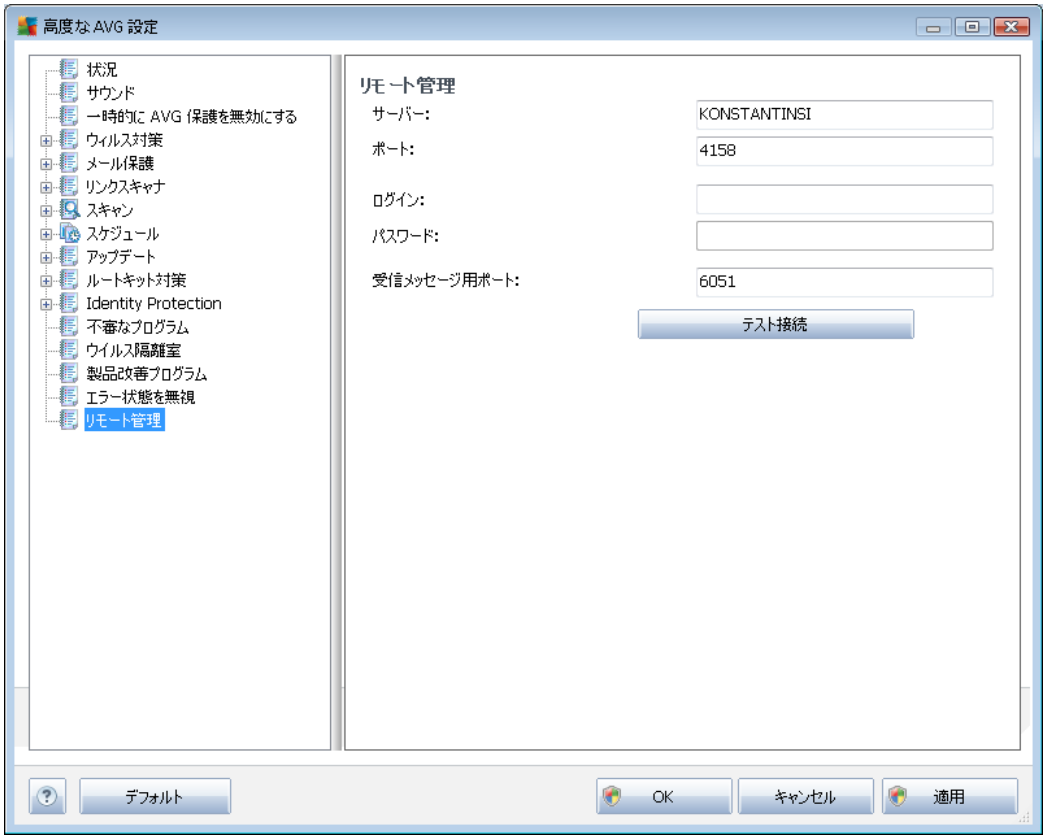
何らかの理由で一時的にコンポーネントをオフにする必要がある場合が考えられます (*これは推奨されません。すべてのコンポーネントを永久的にオンにし続け、既定の設定を保持する必要があります。ただし、コンポーネントをオフにしなければならない状況が発生する可能性はあります*)。この場合、システム トレイ アイコンがコンポーネントのエラー状態を自動的に報告します。ただし、この場合には、ユーザーが自分で慎重に設定を行い、潜在的なリスクを認識しているため、実際のエラーについては説明できません。同時に、グレイ色で表示されると、アイコンは表示される可能性のある他のエラーを実際に報告できません。

この場合、上記のダイアログでエラー状態となる可能性のある (*あるいはオフになる*) コンポーネントを選

択できますが、その状態は通知されません。同じオプション *(コンポーネント状態を無視)* はAVG メインウィンドウのコンポーネント概要からも直接特定のコンポーネントに対して提供されています。

9.16. リモート管理

リモート管理 と各ダイアログは、AVG Business Edition ライセンスを使用して **AVG Anti-Virus 2012** をインストールし、インストール処理中に ***リモート管理*** コンポーネントを選択した場合にのみ、ナビゲーションツリーに表示されます。リモート管理のインストールと設定の詳細については、AVG Web (http://www.avg.com/) サイトの [サポート センター/ダウンロード] セクションからダウンロードできる各 AVG Network Edition のマニュアルを参照してください。



遠隔管理 設定は、AVG クライアントを遠隔管理システムに接続させるための設定です。各ステーションを遠隔管理に接続する場合は、次のパラメータを指定してください。

- ***サーバー*** - AVG 管理サーバーがインストールされているサーバー名 (あるいはサーバー IP アドレス)
- ***ポート*** - AVG クライアントが AVG 管理サーバーと通信するポート番号を指定します (*既定のポート番号は 4158 です。このポート番号を使用しない場合は、ポート番号を明示的に指定する必要があります*)
- ***ログイン*** - AVG クライアントとAVG 管理サーバー間の通信が安全な通信として定義されている場合は、ユーザー名を指定します ...

- ***パスワード*** - パスワードも指定します。
- ***受信メッセージポート*** - AVG クライアントが受信メッセージを AVG 管理サーバーから受信するポート番号

コントロール ボタン

[***テスト接続***] ボタンをクリックすると、上記のすべてのデータが有効で DataCenter に正常に接続できていることを検証できます。

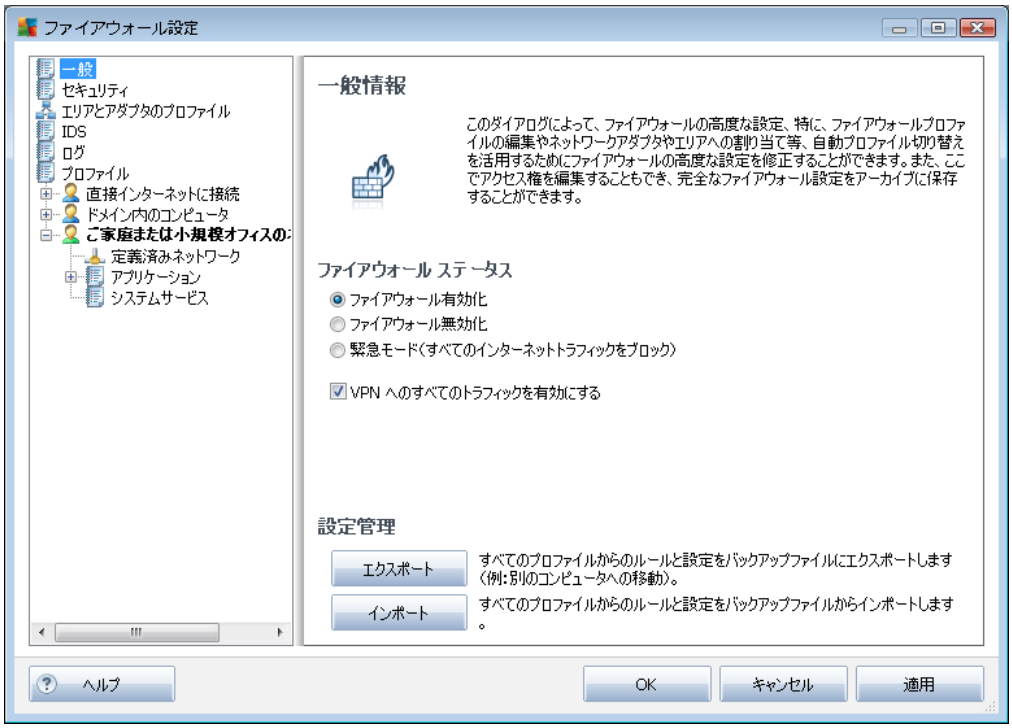
10. ファイアウォール設定

ファイアウォール設定は新しいウィンドウで表示されます。ここでは、いくつかのダイアログで、コンポーネントの高度なパラメータを設定することができます。

ただし、製造元はすべての AVG Anti-Virus 2012 コンポーネントを最適なパフォーマンスを実現できるように設定しています。特に理由がない場合は、既定の設定を変更しないでください。設定変更は経験のあるユーザーのみが行うことを推奨します。

10.1. 一般

[***全般情報***] ダイアログには 2 つのセクションがあります。



ファイアウォール ステータス

[***ファイアウォール ステータス***] セクションでは、必要に応じて、ファイアウォール ステータスを切り替えることができます。

- ***ファイアウォール有効化*** - 選択されたファイアウォールプロファイルで定義されたルールセットに基づいて、アプリケーションの通信を許可します。.
- ***ファイアウォール無効化*** - このオプションはファイアウォールを完全にオフに切り替えます。すべてのネットワークトラフィックは許可され、チェックされません。
- ***緊急モード(すべてのインターネット トラフィックをブロック)*** - このオプションを選択すると、各ネットワーク ポートでのすべてのトラフィックをブロックします。ファイアウォールは実行中ですが、

すべてのネットワーク トラフィックは停止します。

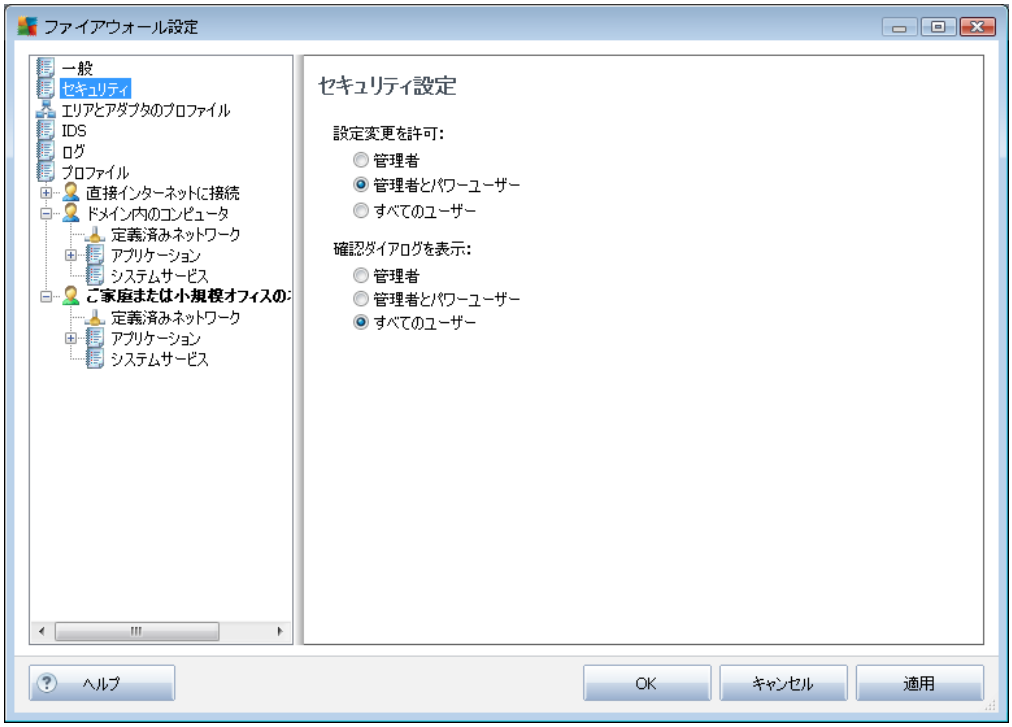
- ***VPN へのすべてのトラフィックを有効にする*** - 自宅からオフィスに接続している場合など、VPN *(仮想プライベート ネット)* 接続を使用する場合、ボックスを選択することをお勧めします。***AVG ファイアウォール***はネットワーク アダプタを自動的に検索し、VPN 接続で使用されているものを検出し、すべてのアプリケーションによるターゲット ネットワークへの接続を許可します *(特定のファイアウォールはネットワークルールが割り当てられていないアプリケーションにのみ適用されます)*。一般的なネットワーク アダプタを使用する標準的なシステムでは、このシンプルなステップにより、VPN で使用する各アプリケーションについて詳細なルールを設定する必要がありません。

メモ: *VPN 接続を有効にするには、GRE、ESP、L2TP、PPTP システム プロトコルとの通信を許可する必要があります。これは [システム サービス] ダイアログで設定できます。*

設定管理

[***設定管理***] セクションでは、***ファイアウォール***設定の***エクスポート***とインポートができます。たとえば、定義済みのファイアウォール ルールと設定をバックアップ ファイルにエクスポートしたり、バックアップ ファイル全体をインポートしたりできます。

10.2. セキュリティ



セキュリティ設定ダイアログでは、選択されたプロファイルに関係なく、ファイアウォールの動作の一般的なルールを定義します。

- 設定変更を許可 - ファイアウォールの設定変更を許可するユーザーを指定します。

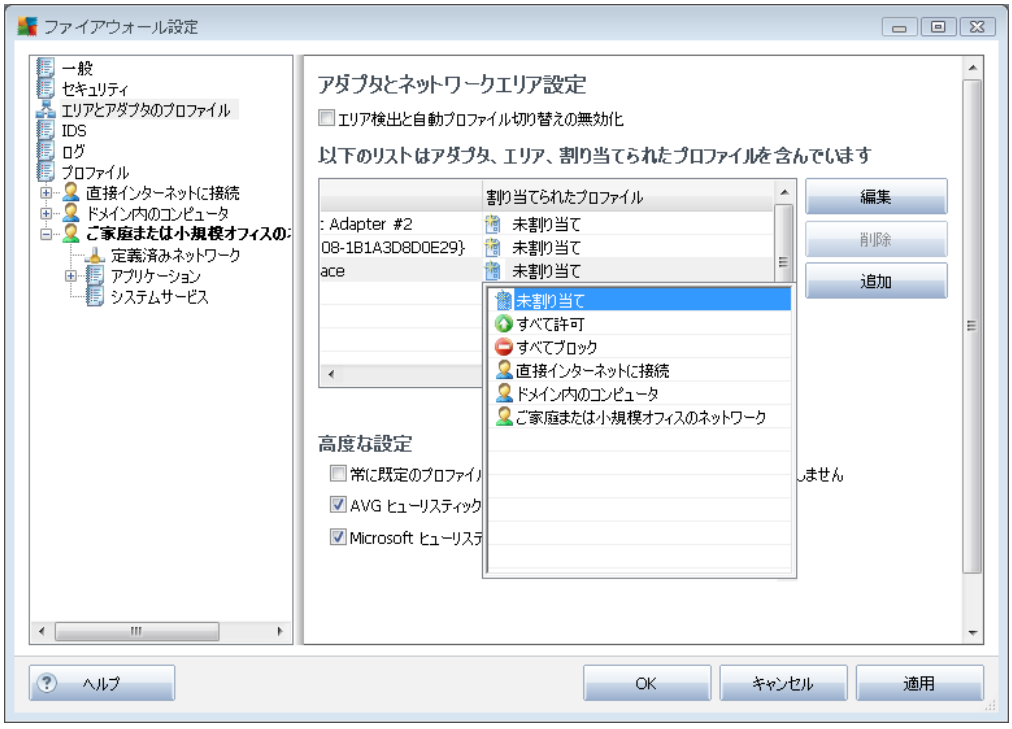
- 確認ダイアログを表示 - 設定ダイアログ (*定義されたファイアウォールルールに含まれていない状況での決定ダイアログ*) が表示されるユーザーを指定します。

いずれの場合でも、以下のユーザーグループに特定の権限を割り当てることができます。

- ***管理者*** –PC を完全にコントロールし、すべてのユーザーを定義されたグループに割り当てる権限を持っています。
- ***管理者とパワーユーザー*** –管理者は任意のユーザーを指定されたグループ (*パワーユーザー*) に割り当て、グループメンバーの権限を定義できます。
- ***すべてのユーザー***–特定のグループに割り当てられていないその他のユーザー.

10.3. エリアとアダプタのプロファイル

アダプタとネットワークエリア設定ダイアログでは、定義済みプロファイルの特定のアダプタへの割り当てと、該当するネットワークの参照に関する設定を編集します。



- ***エリア検出と自動プロファイル切り替えを無効にする*** (*既定では無効*) - 定義されたプロファイルのいずれかが、各ネットワークのインターフェースタイプ、各エリアにそれぞれ割り当てられます。特定のプロファイルを定義しない場合は、1 つの共通プロファイルを使用します。ただし、プロファイルを区別し特定のアダプタとエリアに割り当てた後でこの設定を一時的に切り替える場合は、[***エリア検出と自動プロファイル切り替えを無効にする***] にチェックを付けます。
- ***アダプタとエリア、割り当てられたプロファイルのリスト*** - このリストには検出されたアダプタと

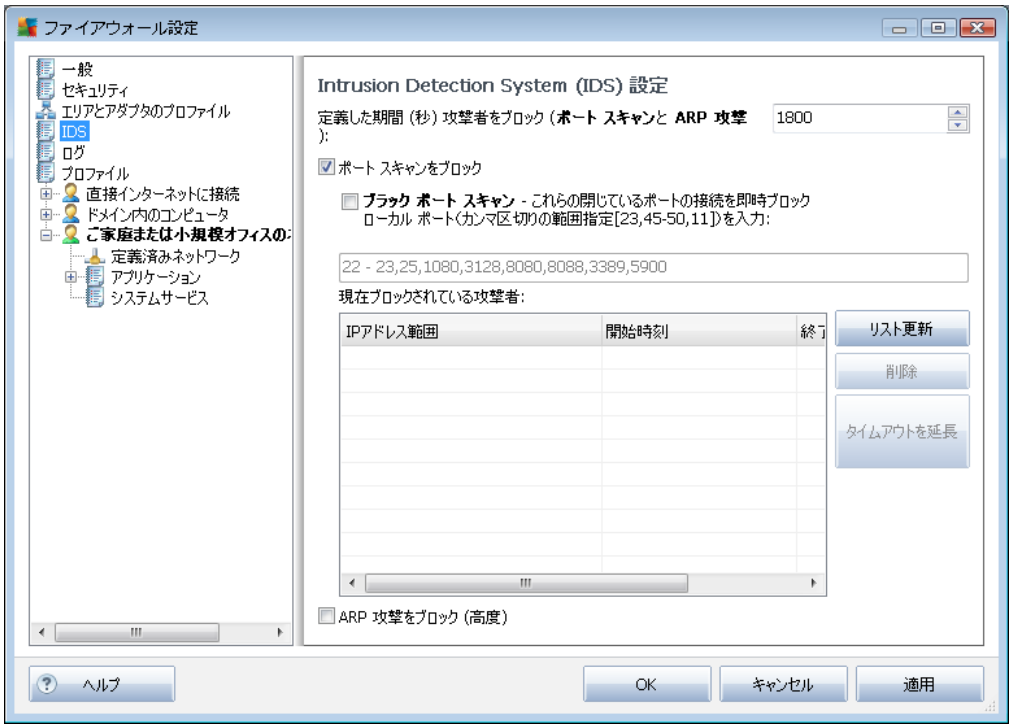
エリアの概要が表示されます。定義されたプロファイルのメニューの特定のプロファイルを各アダプタに割り当てることができます。このメニューを開くには、アダプタのリストの各項目 (*[割り当てられたプロファイル] 列*) を左クリックして、コンテキスト メニューからプロファイルを選択します。

高度な設定

- ***常に既定のプロファイルを使用し、新しいネットワーク検出ダイアログを表示しない*** - コンピュータが新しいネットワークに接続するたびに、ファイアウォールによってアラート通知が行われ、ファイアウォール プロファイルに割り当てるネットワーク接続の種類を選択するためのダイアログが表示されます。このダイアログを表示しない場合は、このボックスを選択します。
- ***新しいネットワークを検出するときに AVG ヒューリスティックを使用する*** - AVG 独自のメカニズムを使用して、新しく検出されたネットワークに関する情報を収集できます (*ただし、このオプションは Vista OS 以降でのみ利用できます*)。
- ***Microsoft のヒューリスティックを使用して新しいネットワークを検出する*** - 新しく検出されたネットワークに関する情報を Windows サービス (*このオプションは Windows Vista 以降のバージョンでのみ利用できます*) から取得します。

10.4. IDS

侵入検出システムは、コンピュータの特定のポートで実行される不審な通信の試みを特定してブロックするための特殊な動作分析機能です。[***侵入検出システム (IDS) 設定***] ダイアログでは IDS パラメータを設定できます。



[***侵入検出システム (IDS) 設定***] ダイアログには次の設定オプションがあります。

- ***指定した期間攻撃者をブロックする (ポートスキャンとARP攻撃)*** - ポート上で不審な通信の試みが検出されたときに、ポートをブロックする秒数を設定できます。既定では 1800 秒 (*30 分*) に時間設定されています。

- ***ポートスキャンをブロックする*** *(既定では有効) - ボックスにチェックを付けると、外部からコンピュータに入るすべての TCP ポートおよび UDP ポート上での通信の試みをブロックします。*このような接続では、5 つの試みが許可され、6 番目の試みがブロックされます。この項目は既定では有効です。この設定を保持することをお勧めします。[***ポートスキャンをブロックする***] オプションを有効にすると、詳細設定も可能です *(そうでない場合は次の項目が無効になります)*。

  - ***ブラックポートスキャン*** - ボックスにチェックを付けると、次のテキストフィールドに指定したポート上でのすべての通信を即時にブロックします。各ポートまたはポート範囲を指定する場合は各ポートをカンマで区切る必要があります。この機能を利用する場合には、事前定義された推奨ポートの一覧があります。

  - 現在ブロックされている攻撃者 - このセクションには、現在ファイアウォールによってブロックされている通信の試みがすべて一覧表示されます。ブロックされた試みの全履歴は [ログ] ダイアログの [*ポートスキャンログ*] タブに表示されます。

- ***ARP攻撃をブロックする (高度)*** *(既定では無効)* - このオプションを選択すると、***IDS*** によって危険な可能性があると判断されたローカルネットワーク内の特別な種類の通信の試みをブロックします。[***指定した期間攻撃者をブロックする] で設定した時間が適用されます。***ローカルネットワークの種類とリスクレベルを十分に把握している上級者ユーザーのみがこの機能を使用することをお勧めします。

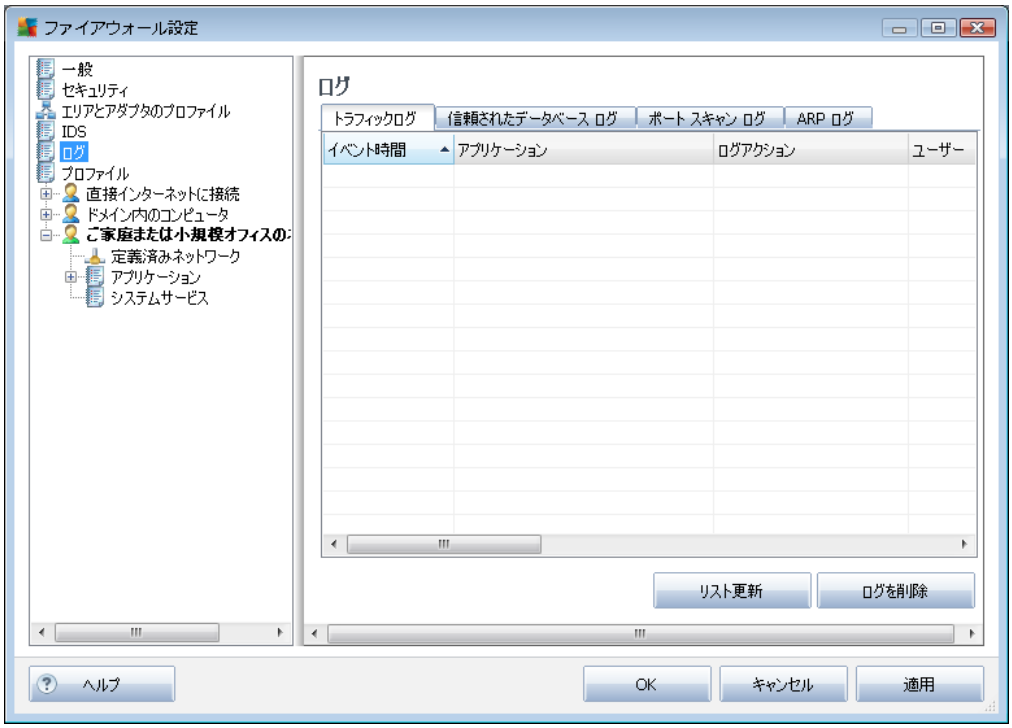
コントロール ボタン

- ***リストの更新*** - このボタンをクリックすると、リストを更新し、*最新のブロックされた試みを反映します。*

- ***削除*** - このボタンをクリックすると、選択したブロックをキャンセルします。

- ***タイムアウト期間の延長*** - このボタンをクリックすると、選択した試みがブロックされる期間を延長します。新しいダイアログが開き、拡張オプションが表示されます。このダイアログで日時を設定するか、期間を無制限に設定できます。

10.5. ログ



[***ログ***] ダイアログでは、すべてのログ出力されたファイアウォール アクション、イベントのリスト、関連するパラメータの詳細説明 (*イベント時刻*、*アプリケーション名*、*各ログ アクション*、*ユーザー名*、*PID*、*トラフィック方向*、*プロトコル タイプ*、*リモートおよびローカルポート番号など*) が 4 つのタブに表示されます。

- ***トラフィックログ*** - ネットワークに接続しようとしたすべてのアプリケーションの活動に関する情報を提供します。
- ***信頼されたデータベースログ*** - *信頼されたデータベース*は、常にオンライン通信を許可できる認証され信頼されたアプリケーションに関する情報を収集する AVG 内部データベースです。新しいアプリケーションが初めてネットワークに接続しようとするとき(*つまり、まだこのアプリケーションに指定されたファイアウォールルールがない場合*) 、そのアプリケーションに対してネットワーク通信を許可するかどうかを決定する必要があります。まず、AVG は*信頼されたデータベース*を検索し、アプリケーションがリストにある場合は、自動的にネットワークアクセスを付与します。その後に初めて、データベースに利用できる情報がない場合、アプリケーションのネットワークアクセスを許可するかどうかを確認するスタンドアロンダイアログが表示されます。
- ***ポート スキャン ログ*** - すべての侵入検出システム活動のログを出力します。
- ***ARP ログ*** - 侵入検出システムで危険な可能性がある試みとして検出されたローカル ネットワーク内での特定の種類の通信の試みのブロックに関するログ情報 ([*ARP 攻撃をブロックする*] *オプション*)。

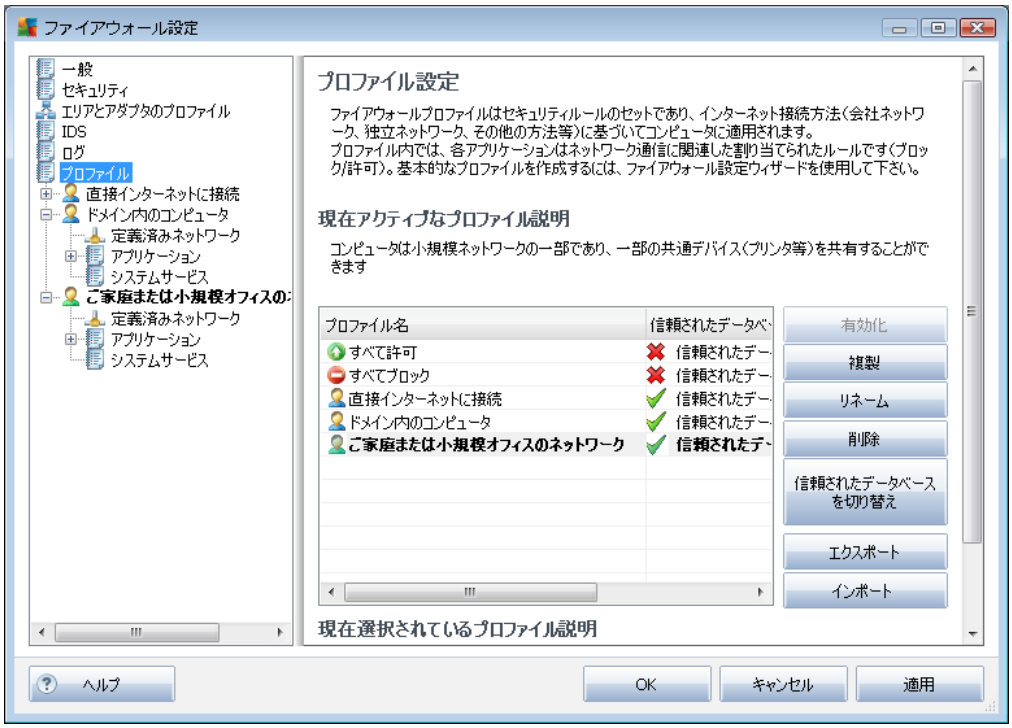
コントロール ボタン

- ***リストを更新***-すべてのログに記録されたパラメータは、各属性によって時系列 *(日付)* あるいはアルファベット順 *(他のカラム)* などでソート可能です。です。各列ヘッダーをクリックするだけです。***リストを更新***ボタンを使用して、現在表示されている情報を更新します。

- ***ログを削除*** - 表のすべてのエントリを削除します。

10.6. プロファイル

プロファイル設定ダイアログでは、すべての利用可能なプロファイルが表示されます。



システム プロファイル *(すべて許可、すべてブロック)* は編集できません。ただし、カスタム プロファイル *(直接インターネットに接続、ドメイン内のコンピュータ、ご家庭または小規模オフィスのネットワーク)* については、このダイアログの次のコントロール ボタンを使用して編集できます。

- ***有効化*** - このボタンは選択されたプロファイルを有効化します。これによって、ファイアウォールでネットワークトラフィックをコントロールするために、選択されたプロファイルが使用されます。

- ***複製*** - 選択されたプロファイルのコピーを作成します。コピーを編集し、複製されたプロファイルをベースに新しいプロファイルを作成することができます。

- ***プロファイルの名前変更*** - 選択したプロファイルの新しい名前を定義できます。

- ***削除***–選択されたプロファイルをリストから削除します。

- ***信頼されたデータベースを切り替え***- 選択されたプロファイルに対して、*信頼されたデータベース*情報 *(信頼されたデータベースは、常にオンライン通信を許可された信頼され認証されたアプリケーションに関する情報を収集するAVG の内部データベースです)* を使用するかどうか

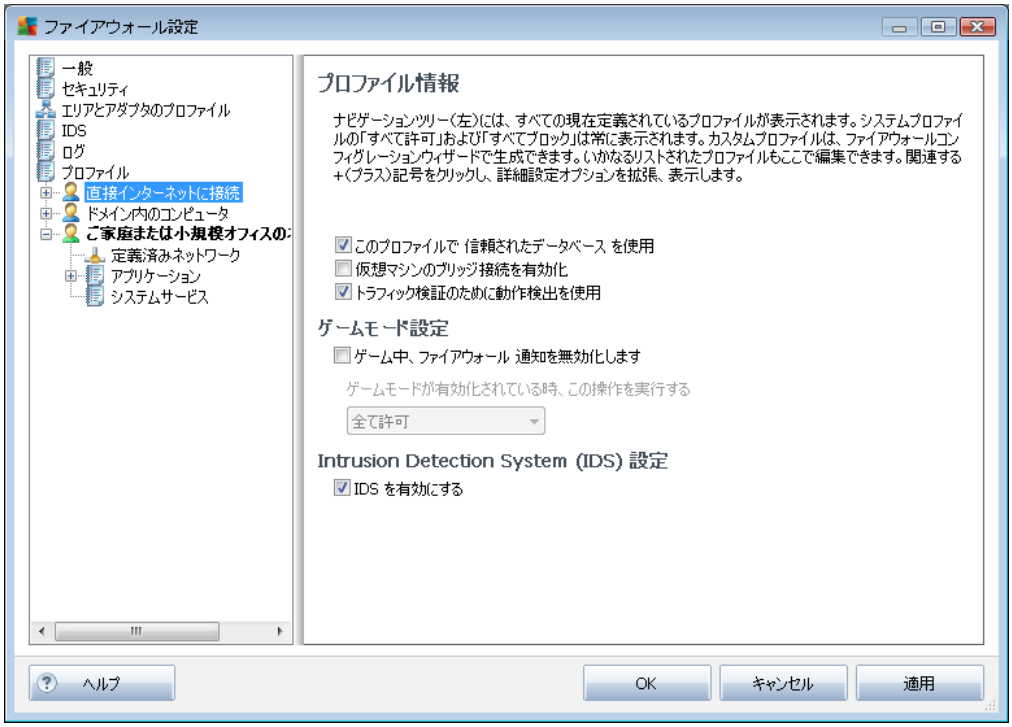
を決定できます。).

- ***エクスポート*** - 選択されたプロファイル設定をファイルに保存します。
- ***インポート*** - 選択されたプロファイル設定をバックアップした設定ファイルからインポートします。

ダイアログ下部のセクションには、現在上記リストで選択されているプロファイルの説明が表示されます。

プロファイルダイアログ内のリストで定義されているプロファイル数に基づいて、左のナビゲーションメニューの構造が変化します。***プロファイル***以下に、各定義済みプロファイルが作成されます。各プロファイルは、以下のダイアログ（*すべてのプロファイルで同一*）で編集可能です。

10.6.1. プロファイル情報



プロファイル情報ダイアログは、このセクションの最初のダイアログです。ここでは、各プロファイルの設定を個別のダイアログで編集することができます。

- ***このプロファイルで信頼データベースを使用する*** - (*既定では有効*) このオプションをオンにすると、*信頼データベース(オンラインで通信する信頼され認証されたアプリケーションに関する情報を収集するAVG内部データベース)*を有効にします。*まだこのアプリケーションに指定されたルールがない場合、ネットワークアクセスをこのアプリケーションに付与するかどうかを決定する必要があります。AVGはまず信頼されたデータベースを検索し、アプリケーションがリストにある場合は、安全だと見なしネットワーク上の通信を許可します。そうでない場合は、アプリケーションによるネットワーク通信を許可するかどうかを決定するように促されます*)。
- ***仮想コンピュータブリジットネットワークを有効にする*** - (*既定では無効*) この項目にチェックを付けると、WMwareの仮想コンピュータによるネットワークへの直接接続を許可します。

- ***トラフィック資格の動作検出を使用*** - (*既定では有効*) このオプションをオンにすると、アプリケーションを評価するときに、ファイアウォールを使用して、Identity Protection機能を使用します。LinkScanner***は、アプリケーションが不審な動作をしめしているか、あるいは信頼されオンライン通信を許可されているかどうかを判断できます。

ゲーム モード設定

ゲームモード設定セクションでは、該当するアイテムにチェックを付けることで、全画面アプリケーションが実行中の場合、画面操作を妨害するファイアウォール情報メッセージを表示するかどうかを決定、確認することができます。 (*一般的に、これらのアプリケーションはゲームですが、PPT プレゼンテーションなどのすべての全画面アプリケーションにも該当します。*)

ゲーム中にファイアウォール通知を無効化にチェックを付けると、ロールダウンメニューで、まだルールが指定されていないアプリケーション (*通常は確認ダイアログとなるアプリケーション*) が通信する際のアクションを選択することができます。これらのすべてのアプリケーションは許可、またはブロックされます。

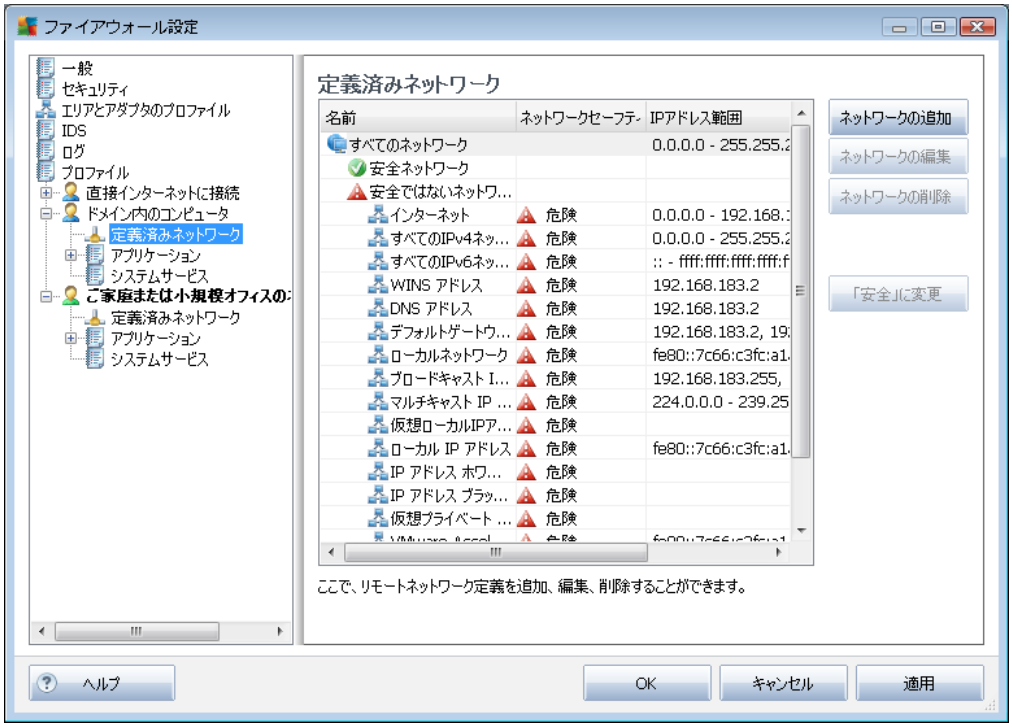
ゲーム モードが有効になっている場合は、アプリケーションが終了するまで、すべてのスケジュール タスク (*スキャン、更新*) が延期されます。

Intrusion Detection System (IDS) 設定

[***IDS を有効にする***] チェック ボックスを選択すると、コンピュータの特定のポートで実行される不審な通信の試みを特定してブロックするための特別な動作分析機能 *を有効にします (この機能設定の詳細については、このマニュアルの「IDS」の章を参照してください)*。

10.6.2. 定義済みネットワーク

定義済みネットワークダイアログはコンピュータが接続するすべてのネットワークのリストを提供します。

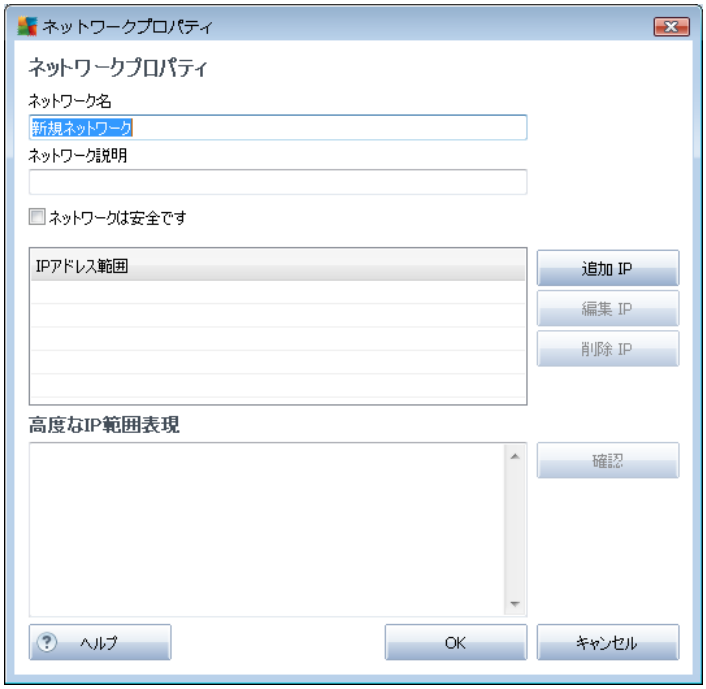


このリストには検出されたすべてのネットワークに関する次の情報が表示されます。

- ***ネットワーク*** - コンピュータが接続されているすべてのネットワーク名の一覧が表示されます。
- ***ネットワークの安全性*** - 既定では、すべてのネットワークは安全でないと考えられ、該当するネットワークが安全だということが確実な場合のみ、「安全」と表示されます。*該当するネットワークをクリックし、コンテキストメニューから「安全」を選択、または「安全」に変更ボタンを使用して、「安全」を割り当てることができます*) - すべての安全なネットワークは許可ルール上で通信可能なグループに含まれ、アプリケーションルールは安全を許可に設定されます。
- ***IPアドレス範囲*** - 各ネットワークは自動的に検出され、IPアドレス範囲で特定されます。

コントロール ボタン

- ***追加***}- ***ネットワークプロパティ***ダイアログウィンドウを開きます。ここでは、新しく定義されたネットワークのパラメータを編集できます。



このダイアログでは、***ネットワーク名*** し、***ネットワーク説 明***を入 力 し、ネットワークが安 全かどうかを指 定 することができます。新 しいネットワークは [***IPの追 加***] ボタン または***IPの編集***/***IPの削 除***) で開 かれるダイアログで定 義 されます。このダイアログでは、IPの範 囲 やマスクを指 定 することでネットワークを設 定 することができます。指 定 するネットワークの数 が多い場 合 、***IPアドレス入 力***欄 を使 用 できます。該 当 するにゅうりょくすべてのネットワークのリストを入 力 (*すべての標 準 フォーマット対 応*) し、***適 用***ボタンを押 してください。次 に***OK***を押 し、データを確 認 、保 存 します。

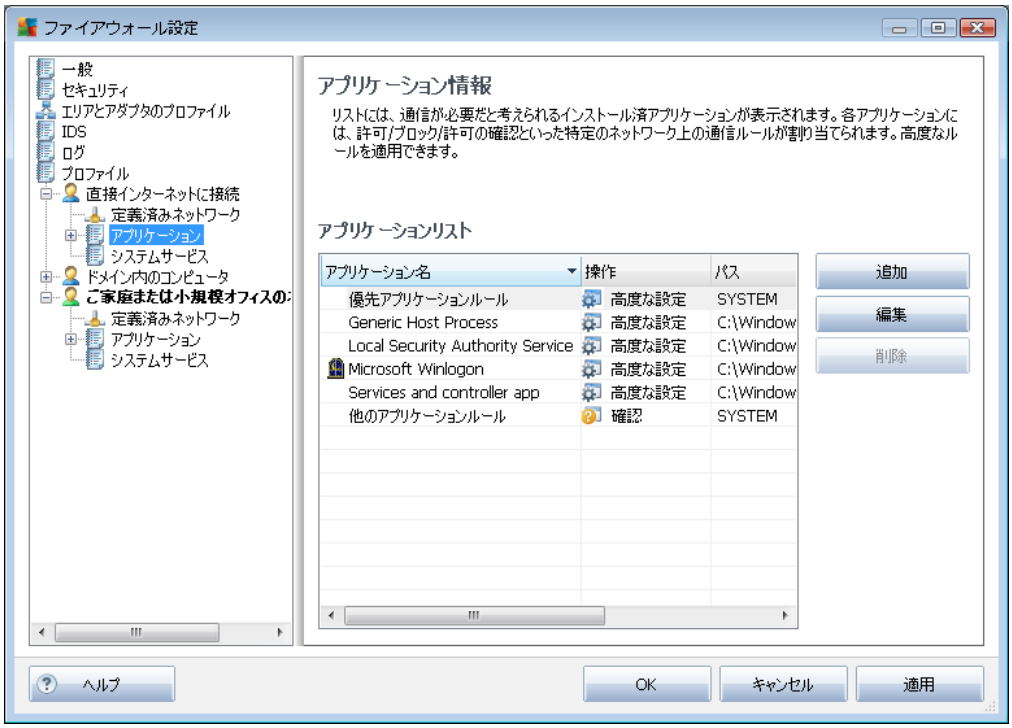
- ***編 集*** - ***ネットワークプロパティ***ダイアログ (*上 記 を参 照*) を開 きます。ここでは、既 に定 義 されたサービスのパラメータを編 集 できます。 (*ダイアログは新 規 ネットワーク追 加 ダイアログと同 一です。*)

- ***削 除***は、ネットワークのリストから選 択 されたネットワークを削 除 します。

- ***安 全 なネットワークとしてマーク***- 既 定 では、すべてのネットワークは安 全 ではないと見 なされます。該 当 するネットワークが安 全 であることが確 実 な場 合 のみ、このボタンを使 用 して、安全 なものとして割 り当 てることができます (*逆 に、ネットワークが安 全 なものとして割 り当 てられると、ボタンは [安 全 ではないネットワークとしてマーク] に変 わります*)。

10.6.3. アプリケーション

[***アプリケーション情報***] ダイアログでは、すべてのネットワーク上で通信するアプリケーションと、それらに割り当てられたアクションのアイコンが表示されます。



アプリケーションのリストには、コンピュータ上で検出されたアプリケーションと*各アプリケーションに割り当てられたアクションが表示されます。*次の種類のアクションを使用できます。

- - すべてのネットワークの通信を許可
- - 安全と定義されたネットワークの通信のみ許可
- - 通信をブロック
- - 確認ダイアログを表示 (*アプリケーションがネットワーク上での通信を試みるときに、通信を許可するかブロックするかどうかをユーザーが決定できます*)
- - 定義された高度な設定

既にインストールされたアプリケーションのみが検出されます。したがって、新しいアプリケーションを後からインストールした場合は、ファイアウォールルールを定義する必要があります。既定では、新しいアプリケーションが初めてネットワーク上での接続を試みるときに、ファイアウォールは信頼されたデータベースに基づいて自動的にアプリケーションのルールを作成するか、通信を許可またはブロックするかどうかを確認します。後者の場合、選択内容を永久ルールとして保存できます。永久ルールはこの後ダイアログにリスト表示されます。

もちろん、新しいアプリケーションルールを即時定義することもできます。このダイアログで、[***追加***] をクリックし、アプリケーション詳細を入力します。

アプリケーション以外にも、リストには2つの特別な項目が表示されます。

- ***優先アプリケーションルール***(*リストの上部*) は、常に他の個々のアプリケーションルールよりも優先して適用されます。
- ***他のアプリケーションルール***(*リストの下部*) は、不明で未定義のアプリケーションのように特定のアプリケーションルールが適用されない場合、 最終インスタンス」として使用されます。

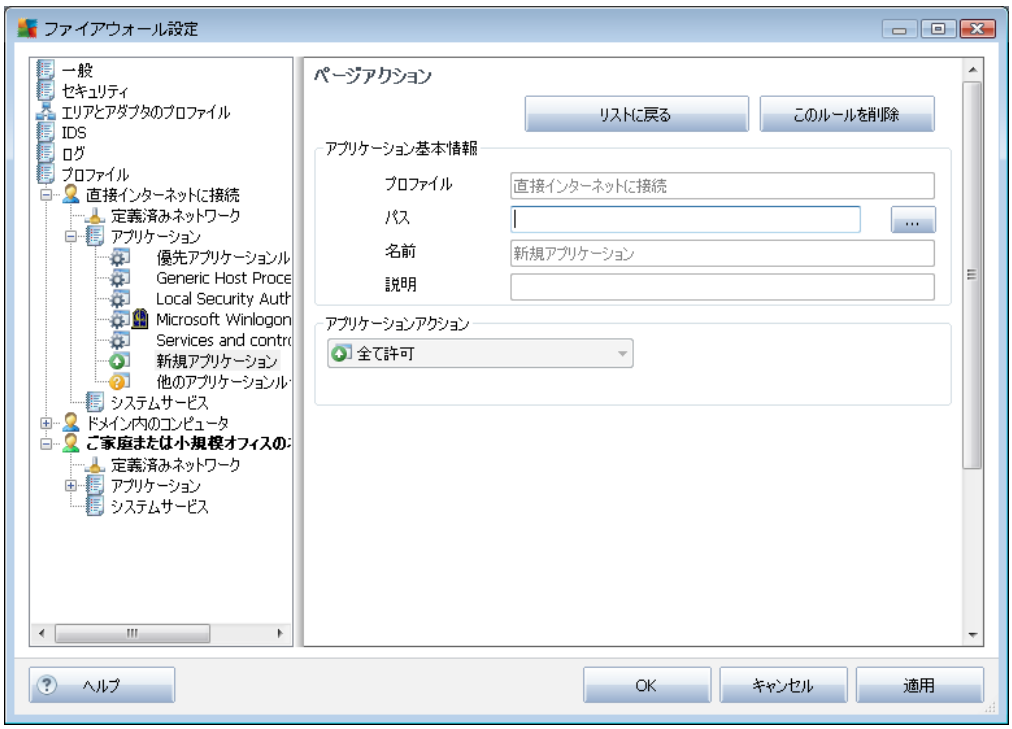
これらのアイテムは一般アプリケーションとは異なった設定オプションを持っており、経験のあるユーザーのみの使用を想定しています。設定を修正しないことを強くお勧めします。

コントロールボタン

以下のコントロールボタンを使用してリストを編集することができます。

- ***追加*** - 新しいアプリケーション ルールを定義するための空の [ページ アクション] ダイアログを開きます。
- ***編集*** - 既存のアプリケーションのルール セットを編集するための [ページ アクション] ダイアログを開きます。同じダイアログですが、データがすでに入力されています。
- ***削除*** - 選択されたアプリケーションをリストから削除します。

ページ アクション ダイアログでは、該当するアプリケーションの設定を詳細に定義できます。



コントロール ボタン

ダイアログの上部には 2 つのコントロール ボタンがあります。

- ***リストに戻る*** - クリックすると、すべての定義済みのアプリケーション ルールの概要を表示します。
- ***このルールを削除*** - クリックすると、現在表示されているアプリケーション ルールを削除します。***この操作は元に戻すことができないため注意してください。***

アプリケーション基本情報

このセクションには、アプリケーションの***名前***と任意で***説明*** (*簡単な情報用のコメント*) を入力します。[***パス***] フィールドには、ディスク上のアプリケーション (*実行ファイル*) への完全パスを入力します。[...] ボタンをクリックすると、ツリー構造でアプリケーションを簡単に参照できます。

アプリケーション アクション

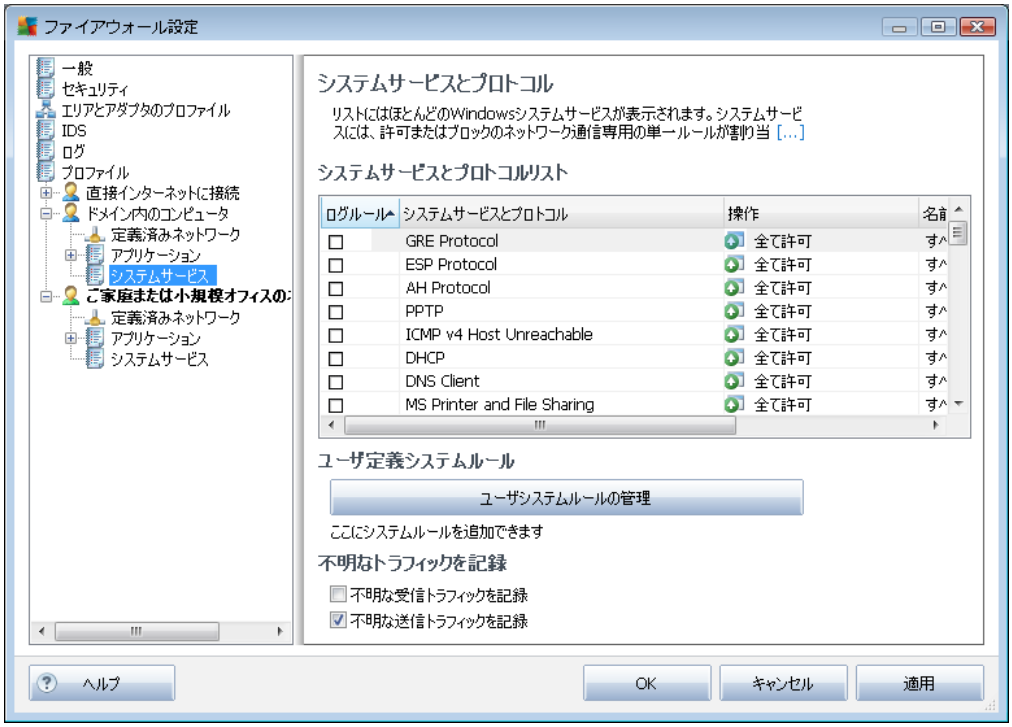
ドロップダウン メニューでは、アプリケーションに関するファイアウォール ルールを選択できます。たとえば、アプリケーションがネットワーク上で通信を試みたときのファイアウォールの動作などを指定できます。

- ***すべてを許可*** - すべての定義されたネットワークとアダプタ上で制限なく、アプリケーションの通信を許可します。
- ***安全を許可*** - 安全な *信頼できる* ネットワークとして定義されたネットワーク上でのアプリケーション通信のみを許可します。
- ***ブロック*** - 自動的に通信を禁止します。アプリケーションはいかなるネットワークに対しても接続できません。
- ***確認する*** - 通信を許可するかブロックするかを決定するダイアログを毎回表示します。
- ***高度な設定*** - [アプリケーション詳細ルール] ***セクションの***ダイアログの下部により広範囲で詳細な設定オプションが表示されます。詳細はリスト順に適用されます。設定を変更する場合は、リスト内でルールを***上に移動***、または***下に移動***できます。リスト内の特定のルールをクリックすると、ルール詳細の概要がダイアログの下部に表示されます。各設定ダイアログで青色の下線が付いている値をクリックすると、値を変更できます。強調表示されたルールを削除する場合は、[***削除***] をクリックします。新しいルールを定義する場合は、[***追加***] ボタンを使用して、[***ルール詳細の変更***] ダイアログを開きます。ここで、必要な詳細情報すべてを指定できます。

10.6.4. システム サービス

システム サービスとプロトコル ダイアログ内の編集は、経験のあるユーザー向けです。

[***システム サービスとプロトコル***] ダイアログには、ネットワーク通信が必要な可能性がある Windows 標準システムサービスおよびプロトコルがリスト表示されます。



システムサービスとプロトコルリスト

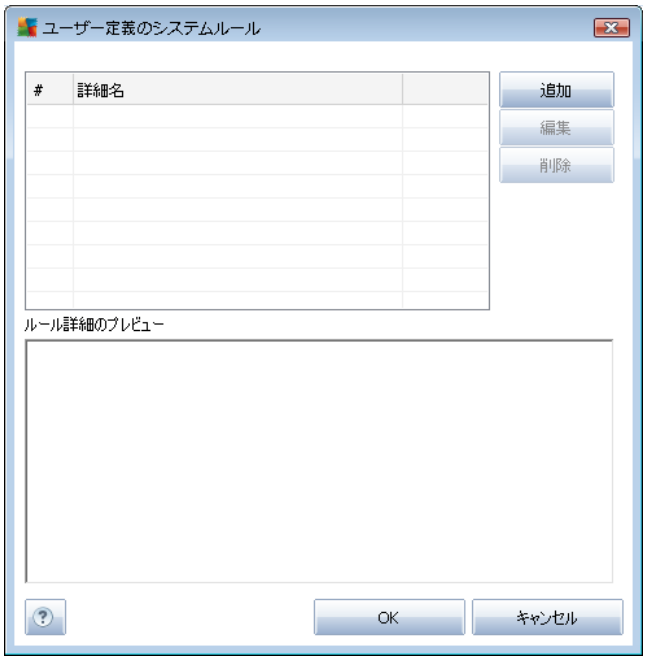
表には、次の列があります。

- ***ログ ルール アクション*** - このボックスでは、ログの各ルール適用の記録をオンにできます。
- ***システム サービスとプロトコル*** - この列には、各システム サービス名が表示されます。
- ***アクション*** - この列には、割り当てられたアクションのアイコンが表示されます。
  - o すべてのネットワークの通信を許可
  - o 安全と定義されたネットワークの通信のみ許可
  - o 通信をブロック
- ***ネットワーク*** - この列には、システム ルールが適用されている特定のネットワークが表示されます。

リストのアイテム（割り当てられたアクションを含む）の設定を編集するには、アイテムを右クリックして、[***編集***] を選択します。***システム ルールの変更は上級者ユーザーのみが実行してください。システム ルールの変更をしないことを強くお勧めします。***

ユーザ定義システムルール

独自のシステム サービス ルール (*次の図を参照*) を定義するために新しいダイアログを開くには、[***ユーザー システム ルールの管理***] ボタンをクリックします。[***ユーザー定義システム ルール***] ダイアログの上部のセクションには、現在編集されたシステムルールの詳細すべての概要が表示され、下部のセクションには選択した詳細が表示されます。ユーザー定義の詳細は、各ボタンを使用して、編集、追加、あるいは削除できます。製造元が定義したルール詳細は編集のみが可能です。



詳細ルール設定は高度な設定であり、ファイアウォール設定を完全に制御する必要のあるネットワーク管理者向けです。通信プロトコル、ネットワークポート番号、IP アドレス定義などについての知識がない場合は、この設定を変更しないでください。設定を変更する必要がある場合は、詳細について、各ダイアログ ヘルプ ファイルを参照してください。

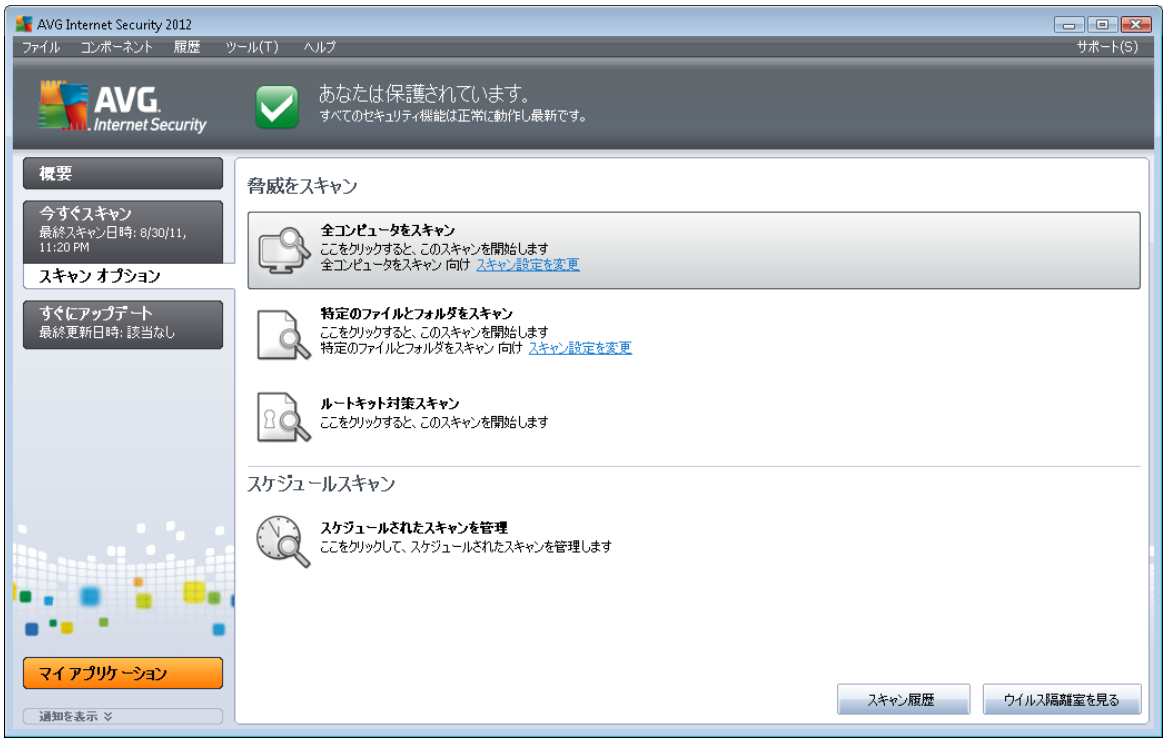
不明なトラフィックを記録

- ***不明な受信トラフィックを記録*** *(既定ではオフ)**** – このボックスにチェックを付けると、外部からのコンピュータへの不明な接続の試みをすべてログに記録します。
- ***不明な送信トラフィックを記録*** *(既定ではオン)**** – このボックスにチェックを付けると、コンピュータから外部への不明な接続をすべてログに記録します。

11. AVG スキャン

既定では、**AVG Anti-Virus 2012** はスキャンを実行しません。初回のスキャンの後、常に監視状態にある **AVG Anti-Virus 2012** の常駐コンポーネントによって完全に保護され、悪意のあるコードはコンピュータに侵入できないためです。当然、定期的にスキャンを実行するようにスケジュール設定したり、ニーズに合わせていつでもスキャンを手動で起動したりできます。

11.1. スキャン インターフェース



AVG スキャンインターフェースには [***スキャン オプション***] クイックリンクからアクセスできます。このリンクをクリックすると、***脅威のスキャン***ダイアログに切り替わります。このダイアログには、以下の情報が表示されます。

- あらかじめ定義されたスキャンの概要 - 3 種類のスキャン（ソフトウェアベンダにより定義）がオンデマンドでの即時使用またはスケジュールでの使用に準備されています。
    - 完全コンピュータ スキャン
    - 特定のファイルとフォルダをスキャン
    - ルートキット対策 スキャン
- スキャンスケジュールセクション - ここでは必要に応じて、新しいスキャンを作成することができます。

コントロールボタン

スキャンインターフェースで利用できるコントロールボタンは以下の通りです。

- ***スキャン履歴*** - スキャンの履歴全体を含むスキャン結果概要ダイアログを表示します。
- ***ウイルス隔離室を見る*** - ウイルス隔離室を表示します。

11.2. 定義済みスキャン

AVG Anti-Virus 2012 の主要な機能の 1 つは、オンデマンド スキャンです。オンデマンド スキャンは、ウイルス感染の疑いがある場合、コンピュータの各領域をいつでもスキャンできるように設計されています。たとえウイルスがコンピュータに存在しないと思われる場合でも、このスキャンを定期的に実行することを強くお勧めします。

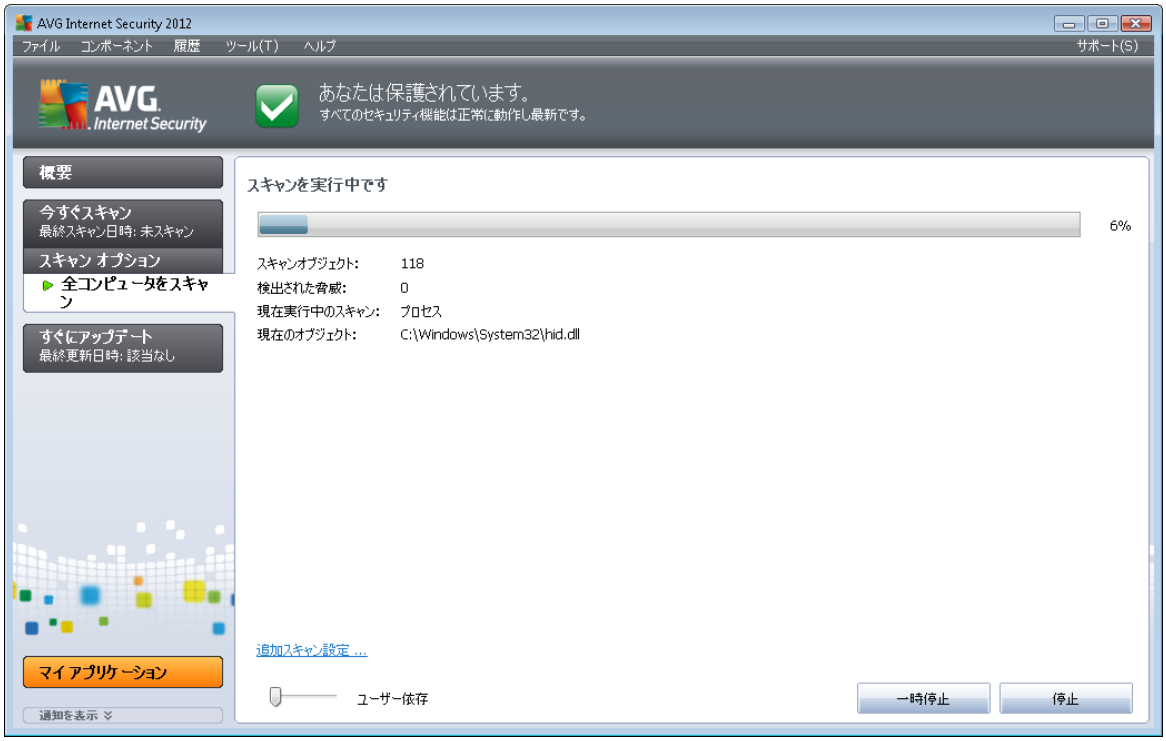
AVG Anti-Virus 2012 には、ソフトウェア ベンダがあらかじめ定義した次のスキャンがあります。

11.2.1. 完全コンピュータ スキャン

完全コンピュータスキャン - コンピュータを完全にスキャンして、感染と不審なプログラムがあるかどうかを確認します。このスキャンはコンピュータのハード ドライブ全体をスキャンし、ウイルス感染の検出、修復、検出した感染のウイルス隔離室への移動を実行します。週に 1 度以上は完全コンピュータ スキャンを実行するようにスケジュールを設定してください。。

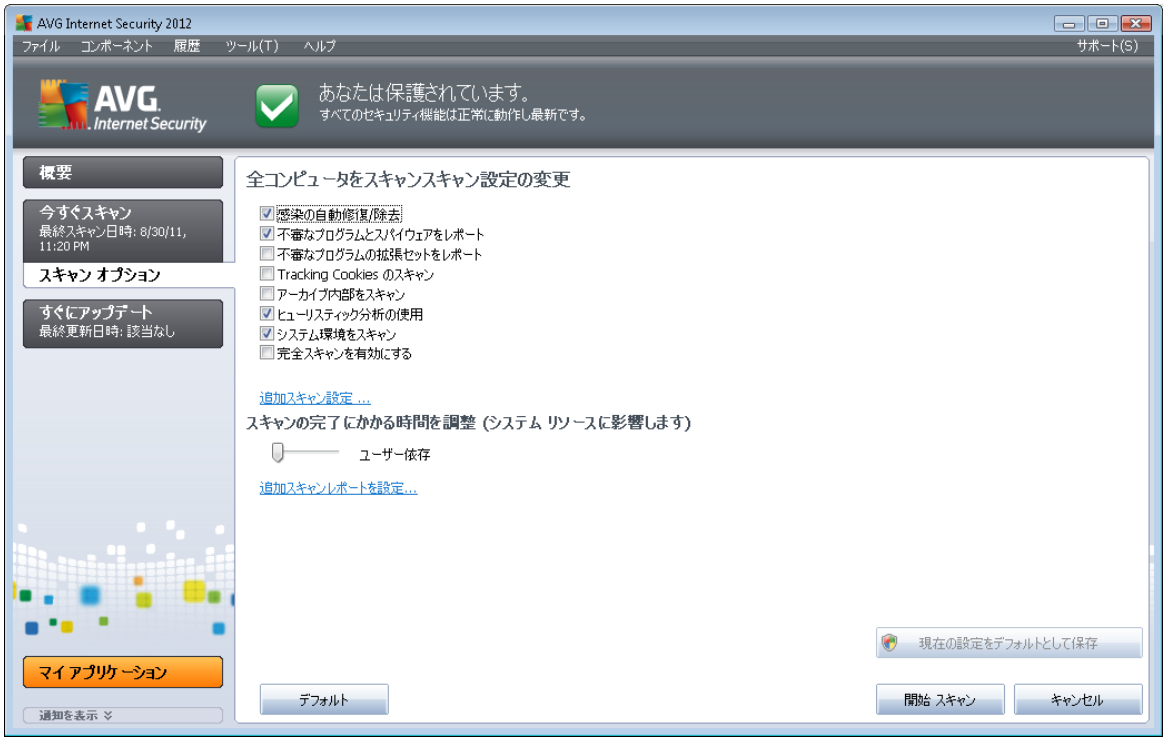
スキャン実行

スキャン アイコンをクリックすると、***完全コンピュータスキャン***をスキャン インターフェースから直接実行できます。このスキャンに対して、さらに特別な設定は必要ありません。スキャンは [***スキャン実行中***] ダイアログ内で即時開始されます (*スクリーンショット*を参照)。必要に応じて、スキャンを一時的に中断 (***一時停止***) またはキャンセル (***停止***) できます。



スキャン設定編集

完全コンピュータスキャンの既定の設定を編集することもできます。[***スキャン設定を変更***] リンクをクリックすると、[***完全コンピュータスキャンのスキャン設定の変更***] ダイアログ (*完全コンピュータスキャンの [スキャン設定を変更] リンク経由でスキャンインターフェースからアクセス可能*) が表示されます。***特に理由がない場合は、この既定の設定を保持することをお勧めします。***



- ***スキャン パラメータ***- スキャン パラメータの一覧では、必要に応じて特定のパラメータのオン/オフを切り替えることができます。

  - ***自動的に感染を修復/除去する*** (*既定ではオン*): スキャン実行中にウイルスが特定され、修復可能な場合は、自動的に修復されます。感染したファイルを自動的に修復できない場合、感染したオブジェクトはウィルス隔離室に移動されます。

  - ***不審なプログラムとスパイウェア脅威を報告する***(*既定ではオン*): チェックを付けると、スパイウェア対策エンジンを有効にし、ウイルスと同時にスパイウェアもスキャンします。スパイウェアは疑わしいマルウェアのカテゴリに含まれます。通常は、セキュリティリスクとなる場合でも、このようなプログラムを故意にインストールすることができます。コンピュータのセキュリティを高めるため、この機能を有効にしておくことをお勧めします。

  - ***不審なプログラムの拡張セットを報告する*** (*既定ではオフ*): 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。スパイウェアとは、直接製造元から入手する場合にはまったく問題がなく、無害なプログラムですが、後から悪意のある目的で誤用されるおそれのあるプログラムです。これは、コンピュータセキュリティ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。

  - ***Tracking Cookie をスキャンする*** (*既定ではオフ*) - スパイウェア対策 コンポーネントのこのパラメータを定義すると、Cookie を検出します (*HTTP cookie は、サイトの設定や電子ショッピング カートの内容など、ユーザー固有の情報の認証、追跡、メンテナンスに使用されます*)。

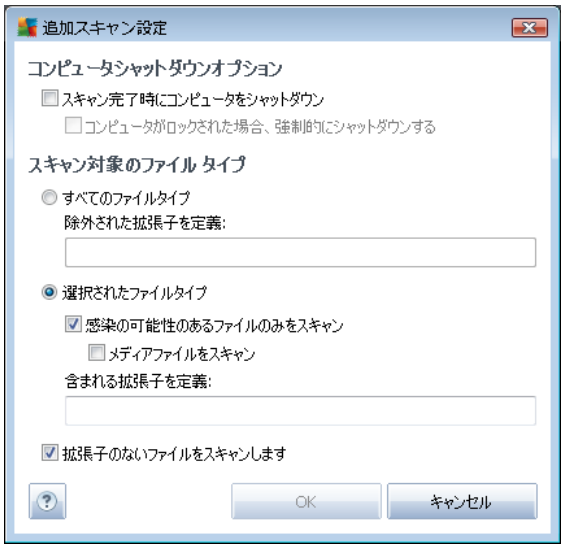
  - ***アーカイブの内容をスキャンする*** (*既定ではオフ*) - ZIP や RAR などのアーカイブ内に格納されているすべてのファイルをスキャンします。

- ***ヒューリスティック分析を使用する*** (*既定ではオン*) - ヒューリスティック分析 (*仮想コンピュータ環境で実行されるスキャン対象オブジェクト命令の動的エミュレーション*) は、スキャン実行中に採用されるウイルス検出方法の 1 つです。

- ***システム環境をスキャンする*** (*既定ではオン*) - コンピュータのシステム領域もチェックされます。

- ***完全スキャンを有効にする*** (*既定ではオフ*) - このオプションをチェックすると、特定の状況 (*コンピュータが感染している疑いがある場合など*) が発生した場合に最も完全なスキャンアルゴリズムを有効にし、感染の可能性が非常に低いコンピュータ領域もスキャンします。これにより、問題がないことを確実に確認します。この方法を実行すると多少時間がかかります。

- ***追加スキャン設定*** - このリンクをクリックすると、新しい [追加スキャン設定] ダイアログが開きます。このダイアログでは、次のパラメータを指定できます。



  - ***コンピュータのシャットダウンオプション*** - 実行中のスキャン処理が終了した時点で自動的にコンピュータをシャットダウンするかどうかを決定します。このオプション (***スキャン完了時にコンピュータをシャットダウン***) を選択すると、現時点でコンピュータがロックされている場合でも、コンピュータをシャットダウンさせる新しいオプション (***コンピュータがロックされた場合強制的にシャットダウンする***) が有効になります。

  - ***スキャンのファイルタイプ*** - さらに、スキャンするかどうかを決定する必要があります。

    - ***すべてのファイルタイプと***スキャン対象ではないファイル拡張子をカンマで区切ったリストを入力することで、スキャンからの除外を定義できます。

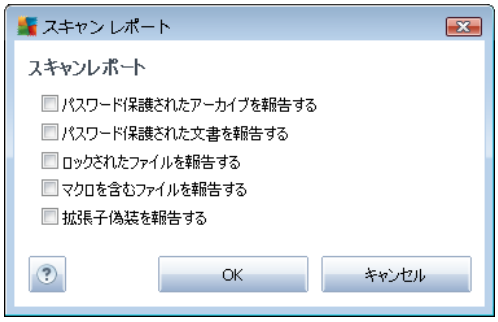
    - ***選択したファイルタイプ*** - 感染の可能性のあるファイルのみを指定できます (*一部のプレーンテキストファイルやその他の非実行可能ファイルなど*感染の可能性がないファイルはスキャンされません)。これには、メディアファイル (*ビデオ、オーディオファイル*) が含まれます。多くの場合、このようなファイルはサイズが非常に大きく、ウィルスに感染している可能性が非常に低いため、このボックスのチェックを外すと、スキャン時間がさらに短縮されますここでも、必ずスキャンするファイルの拡張子を

指定できます。

- 任意で***拡張子のないファイルをスキャン***できます。このオプションは既定ではオンになっています。変更する理由がない場合は、この設定を保持することをお勧めします。拡張子のないファイルは不審であるため、常にスキャンすることをお勧めします。

- ***スキャンの実行速度を調整*** - スライダを使用して、スキャン処理の優先度を変更できます。既定ではこのオプションの値は、自動的にリソースを使用するユーザー依存レベルに設定されています。低速でスキャン処理を実行してシステムリソース負荷を最小化 (*コンピュータで同時に作業をする必要があり、スキャンに時間がかかってもよい場合に便利です*) したり、システムリソース消費量の高い高速スキャン (*コンピュータが一時的に使用されていない場合などに便利です*) を実行したりできます。

- ***追加スキャンレポートを設定*** - このリンクをクリックすると [***スキャンレポート***] ダイアログが開きます。このダイアログでは、レポート対象の検出の種類を選択できます。



***警告**: これらのスキャン設定は新規に定義されたスキャンパラメータと同じです。「AVG スキャン/スキャンスケジュール/スキャン方法」の章を参照してください。**完全コンピュータスキャン**の既定の設定を変更する場合、新しい設定を既定の設定として保存し、すべての完全コンピュータスキャンに適用できます。*

11.2.2. 特定のファイルとフォルダのスキャン

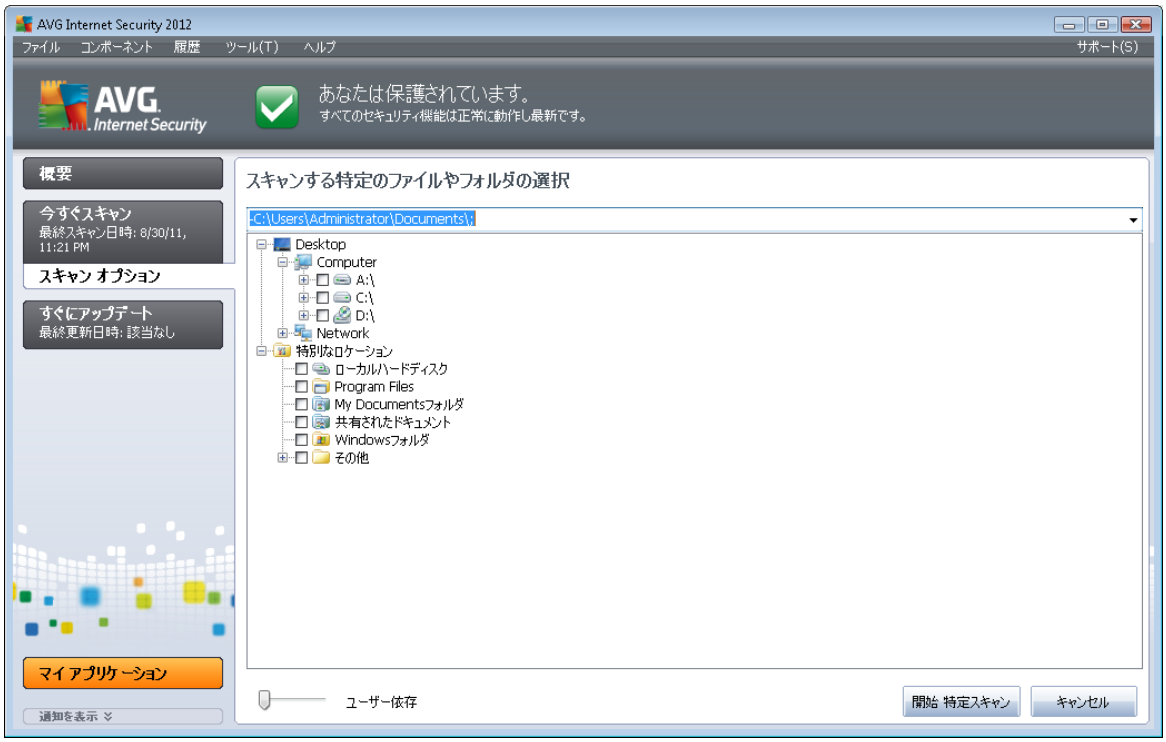
特定のファイルやフォルダをスキャン - 選択した領域のみスキャンします (*選択したフォルダ、ハードディスク、フロッピーディスク、CD など*)。ウイルス検出や処理のスキャン進捗は完全コンピュータスキャンの場合と同じです。検出されたウイルスは修復されるかウイルス隔離室に移動されます。特定のファイルやフォルダのスキャンでは、ユーザー独自のスキャン設定とスケジュールを実行できます。

スキャン実行

をスキャンインターフェースから直接起動できます。[***スキャンする特定のファイルまたはフォルダの選択***] という新しいダイアログが開きます。コンピュータのツリー構造でスキャンするフォルダを選択します。選択したフォルダへのパスは自動的に作成され、このダイアログの上部のテキストボックスに表示されます。

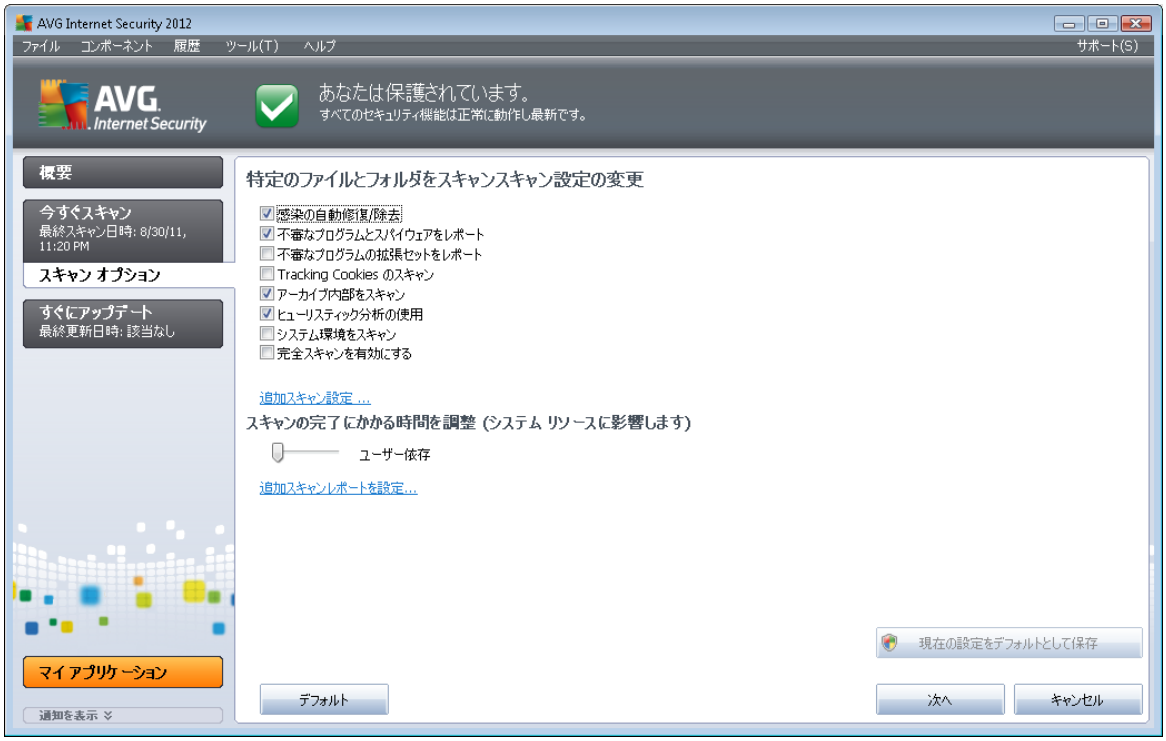
また、すべてのサブフォルダをスキャンしない場合、自動作成されたパスの前にマイナス記号 「-」を記述します (*スクリーンショットを参照*)。スキャンからフォルダ全体を除外するには 「!」 パラメータを使用します。

スキャンを実行するには、[***スキャン開始***] ボタンをクリックします。スキャン処理自体は基本的に完全コンピュータスキャンと同じです。



スキャン設定編集

特定のファイルやフォルダスキャンのあらかじめ定義された既定の設定***を編集できます***。[***スキャン設定の変更***] リンクをクリックすると、[***特定のファイルとフォルダのスキャン設定の変更***] ダイアログが表示されます。***特に理由がない場合は、この既定の設定を保持することをお勧めします。***



- ***スキャン パラメータ***- スキャン パラメータの一覧では、必要に応じて特定のパラメータのオン/オフを切り替えることができます。

    - ***自動的に感染を修復/除去する*** (*既定ではオン*): スキャン実行中にウイルスが特定され、修復可能な場合は、自動的に修復されます。感染したファイルを自動的に修復できない場合、感染したオブジェクトはウィルス隔離室に移動されます。

    - ***不審なプログラムとスパイウェア脅威を報告する***(*既定ではオン*): チェックを付けると、スパイウェア対策エンジンを有効にし、ウイルスと同時にスパイウェアもスキャンします。スパイウェアは疑わしいマルウェアのカテゴリに含まれます。通常は、セキュリティリスクとなる場合でも、このようなプログラムを故意にインストールすることができます。コンピュータのセキュリティを高めるため、この機能を有効にしておくことをお勧めします。

    - ***不審なプログラムの拡張セットを報告する*** (*既定ではオフ*): 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。スパイウェアとは、直接製造元から入手する場合にはまったく問題がなく、無害なプログラムですが、後から悪意のある目的で誤用されるおそれのあるプログラムです。これは、コンピュータセキュリティ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。

    - ***Tracking Cookie をスキャンする*** (*既定ではオフ*) - スパイウェア対策コンポーネントのこのパラメータを定義すると、Cookie を検出します (*HTTP cookie は、サイトの設定や電子ショッピングカートの内容など、ユーザー固有の情報の認証、追跡、メンテナンスに使用されます*)。

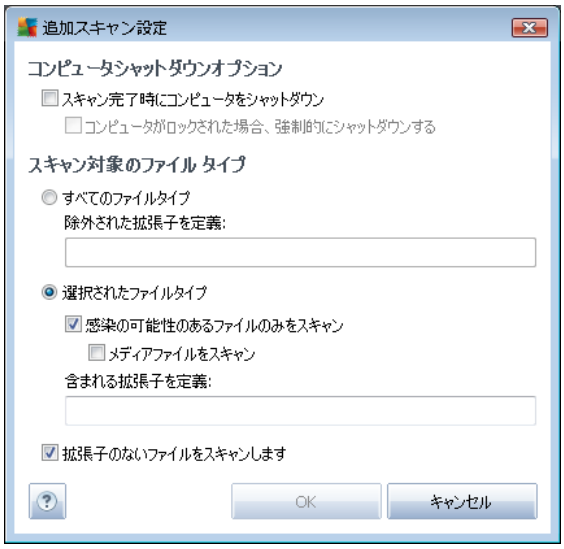
    - ***アーカイブの内容をスキャン*** (*既定ではオン*) - ZIP や RAR などのアーカイブ内に格納されているすべてのファイルをスキャンします。

- ***ヒューリスティック分析を使用する*** (*既定ではオフ*) - ヒューリスティック分析 (*仮想コンピュータ環境で実行されるスキャン対象オブジェクト命令の動的エミュレーション*) は、スキャン実行中に採用されるウイルス検出方法の 1 つです。

- ***システム環境をスキャンする*** (*既定ではオフ*) - コンピュータのシステム領域もチェックされます。

- ***完全スキャンを有効にする*** (*既定ではオフ*) - このオプションをチェックすると、特定の状況 (*コンピュータが感染している疑いがある場合など*) が発生した場合に最も完全なスキャンアルゴリズムを有効にし、感染の可能性が非常に低いコンピュータ領域もスキャンします。これにより、問題がないことを確実に確認します。この方法を実行すると多少時間がかかります。

- ***追加スキャン設定*** - このリンクをクリックすると、新しい [追加スキャン設定] ダイアログが開きます。このダイアログでは、次のパラメータを指定できます。



  - ***コンピュータのシャットダウンオプション*** - 実行中のスキャン処理が終了した時点で自動的にコンピュータをシャットダウンするかどうかを決定します。このオプション (***スキャン完了時にコンピュータをシャットダウン***) を選択すると、現時点でコンピュータがロックされている場合でも、コンピュータをシャットダウンさせる新しいオプション (***コンピュータがロックされた場合強制的にシャットダウンする***) が有効になります。

  - ***スキャンのファイル タイプ*** - さらに、スキャンするかどうかを決定する必要があります。

    - ***すべてのファイル タイプと***スキャン対象ではないファイル拡張子をカンマで区切ったリストを入力することで、スキャンからの除外を定義できます。

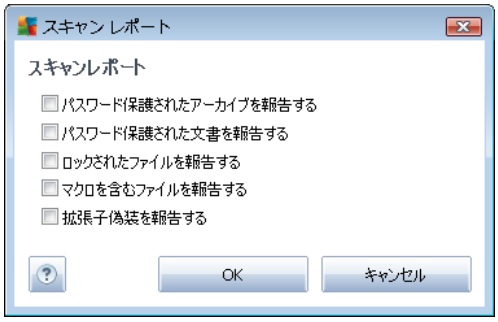
    - ***選択したファイル タイプ*** - 感染の可能性のあるファイルのみを指定できます (*一部のプレーンテキストファイルやその他の非実行可能ファイルなど*感染の可能性がないファイルはスキャンされません)。これには、メディアファイル (*ビデオ、オーディオファイル*) が含まれます。多くの場合、このようなファイルはサイズが非常に大きく、ウィルスに感染している可能性が非常に低いため、このボックスのチェックを外すとスキャン時間がさらに短縮されますここでも、必ずスキャンするファイルの拡張子を

指定できます。

- 任意で***拡張子のないファイルをスキャン***できます。このオプションは既定ではオンになっています。変更する理由がない場合は、この設定を保持することをお勧めします。拡張子のないファイルは不審であるため、常にスキャンすることをお勧めします。

- ***スキャン処理の優先度*** - スライダを使用して、スキャン処理の優先度を変更できます。既定ではこのオプションの値は、自動的にリソースを使用するユーザー依存レベルに設定されています。低速でスキャン処理を実行してシステムリソース負荷を最小化 (*コンピュータで同時に作業をする必要があり、スキャンに時間がかかってもよい場合に便利です*) したり、システムリソース消費量の高い高速スキャン (*コンピュータが一時的に使用されていない場合などに便利です*) を実行したりできます。

- ***追加スキャンレポートを設定*** - このリンクをクリックすると [***スキャンレポート***] ダイアログが開きます。このダイアログでは、レポート対象の検出の種類を選択できます。



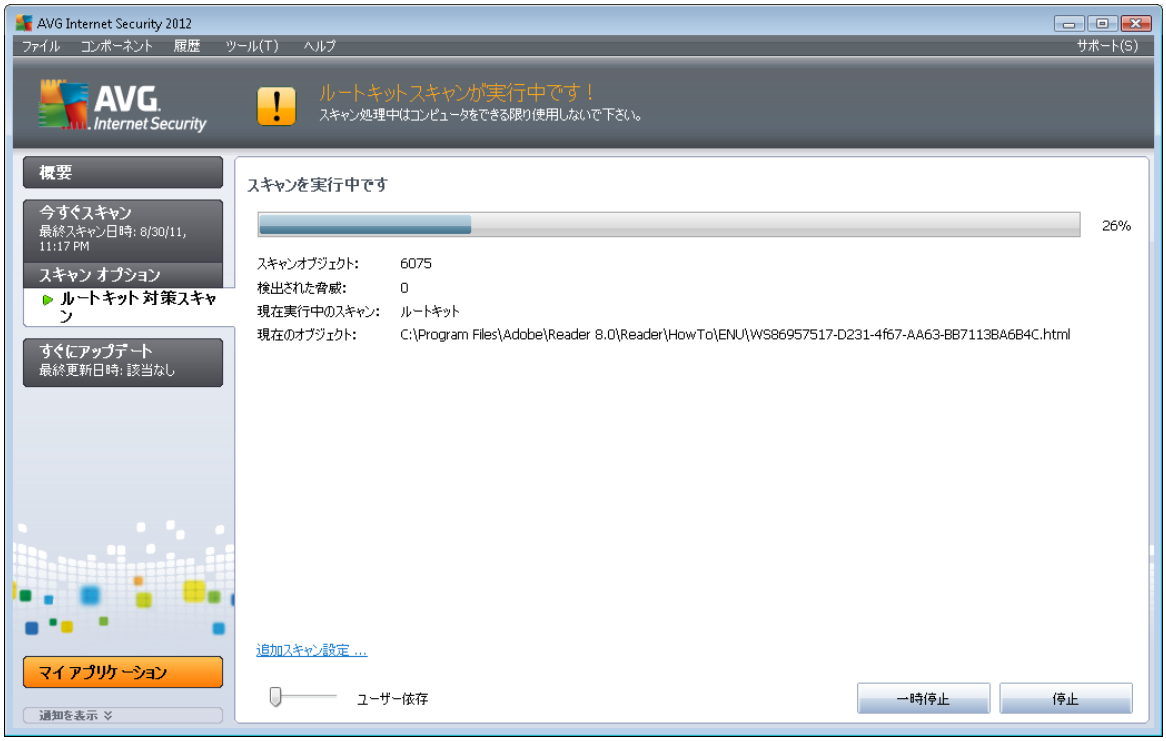
***警告**: これらのスキャン設定は新規に定義されたスキャンパラメータと同じです。「AVG スキャン/スキャンスケジュール/スキャン方法」の章を参照してください。**特定のファイルやフォルダのスキャン**の既定の設定を変更する場合、新しい設定を既定の設定として保存し、すべての特定のファイルやフォルダのスキャンに適用できます。また、この設定はすべての新規スケジュールのテンプレートとして使用できます (すべてのカスタマイズスキャンは、選択したファイルやフォルダのスキャンの現在の設定に基づいて実行されます)。*

11.2.3. ルートキットスキャン

ルートキット対策スキャンはコンピュータを検索し、ルートキット (*悪意のある活動をコンピュータで隠すことができるプログラムや技術*) が存在している可能性があるかどうかを確認します。ルートキットが検出されても、必ずしもコンピュータが感染しているというわけではありません。通常のアプリケーションの特有のドライバやセクションが誤ってルートキットとして検出される場合もあります。

スキャン実行

スキャンのアイコンをクリックすると、***ルートキット対策スキャン***をスキャンインターフェースから直接実行できます。このスキャンに対して、さらに特別な設定は必要ありません。スキャンは [***スキャン実行中***] ダイアログ内で即時開始されます (*スクリーンショットを参照*)。必要に応じて、スキャンを一時的に中断 (***一時停止***) またはキャンセル (***停止***) できます。

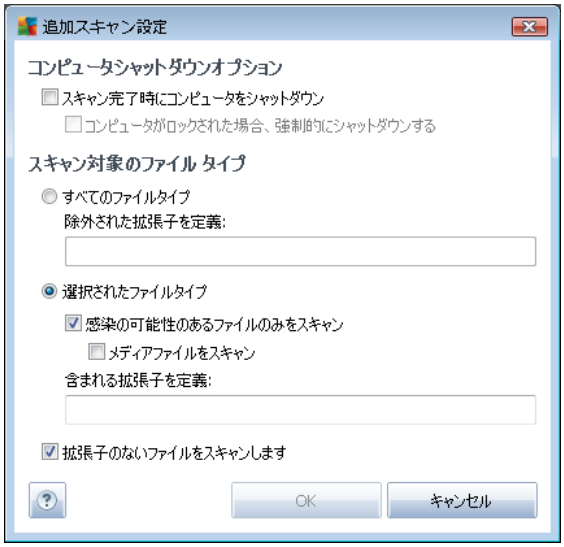


スキャン設定編集

ルートキット対策スキャンは常に既定の設定で起動し、スキャンパラメータは [AVG 高度な設定/ルートキット対策] ダイアログからのみ編集できます。スキャンの実行中に限り、次のスキャンインターフェース設定を利用できます。

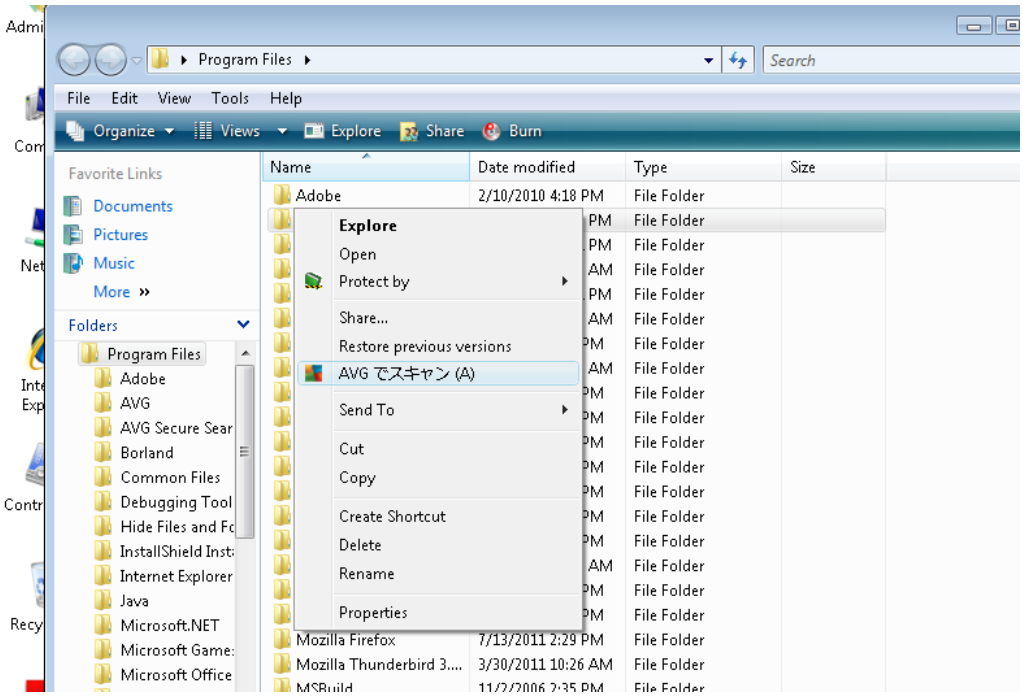
- ***自動スキャン*** - スライダを使用して、スキャン処理の優先度を変更します。既定ではこのオプションの値は、自動的にリソースを使用する*ユーザー依存レベルに設定されています。*低速でスキャン処理を実行してシステムリソース負荷を最小化 (*コンピュータで同時に作業をする必要があり、スキャンに時間がかかってもよい場合に便利です*) したり、システムリソース消費量の高い高速スキャン (*コンピュータが一時的に使用されていない場合などに便利です*) を実行したりできます。

- ***追加のスキャン設定*** - このリンクをクリックすると、新しい [***追加のスキャン設定***] ダイアログが開きます。このダイアログでは、***ルートキット対策スキャン処理に伴うコンピュータシャットダウンのタイミング*** (***スキャン完了時にコンピュータをシャットダウン***あるいは***コンピュータがロックされた場合は強制シャットダウン***) を定義できます。



11.3. シェル拡張スキャン

AVG Anti-Virus 2012では、完全コンピュータ スキャンあるいは特定領域のスキャンで実行されるあらかじめ定義されたスキャン以外にも、クイック スキャン オプションを使用して、Windows Explorer 環境で特定オブジェクトのスキャンを直接実行できます。内容が不明なファイルを開く場合、そのファイルのみをチェックできます。次の方法で実行します。



- Windows Explorerで、チェックするファイル *あるいはフォルダ*) を選択します。
- マウスをオブジェクトに移動して右クリックし、コンテキスト メニューを開きます。

- [***でスキャン***] オプションを選択して、ファイルを AVG でスキャンします。**AVG Anti-Virus 2012**

11.4. コマンドライン スキャン

AVG Anti-Virus 2012 ではコマンド ラインからスキャンを実行するときにオプションを利用できます。このオプションはサーバー上のインスタンスに対して利用できます。あるいは、コンピュータのブート後に自動的に起動するバッチ スクリプトを作成するときに利用できます。コマンド ラインからスキャンを起動するときには、AVG のグラフィカル ユーザー インターフェースで提供されるほとんどのパラメータを使用できます。

コマンド ラインから AVG スキャンを起動するには、AVG がインストールされているフォルダで次のコマンド ラインを実行します。

- ***32 ビット OS の場合*** avgscanx
- ***64 ビット OS の場合*** avgscana

コマンドの構文

コマンドの構文は次のとおりです。

- ***avgscanx /パラメータ***... たとえば、完全コンピュータ スキャンの場合 ***avgscanx /comp***
- ***avgscanx /パラメータ/パラメータ***.. 複数のパラメータを使用する場合、パラメータを 1 行に並べ、スペースとスラッシュで区切る必要があります。
- パラメータが特定の値を必要とする場合 (例: ***/scan*** パラメータには選択した場所への正確なパスを指定する必要があります) は、値をセミコロンで区切る必要があります。例: ***avgscanx /scan=C:\;D:***

スキャン パラメータ

利用可能なパラメータの完全な概要を表示するには、パラメータの /? を付加して該当するコマンドを入力します。あるいは、/HELP と入力します (例: ***avgscanx /?***)。唯一の必須のパラメータは、スキャン対象のコンピュータ領域を指定する /SCAN です。オプションの詳細については、「コマンド ライン パラメータ概要」を参照してください。

スキャンを実行するには、[***Enter***] を押します。スキャン中は ***Ctrl+C*** または***Ctrl+Pause*** を押して処理を停止できます。

グラフィック インターフェースから起動する CMD スキャン

Windows セーフ モードでコンピュータを実行している場合、グラフィック ユーザー インターフェースからコマンド ライン スキャンを実行することもできます。スキャン自体はコマンド ラインから実行されます。[***コマンド ライン コンポーザー***] ダイアログでは、便利なグラフィック インターフェースでは大部分のスキャン パラメータを指定できます。

このダイアログは Windows セーフ モードでのみ利用可能です。このダイアログの詳細説明については、

ダイアログから直接開くことができるヘルプファイルを参照してください。

11.4.1. CMD スキャン パラメータ

以下は、コマンドラインスキャンで利用可能なすべてのパラメータです。

- ***/SCAN*** 特定のファイルまたはフォルダのスキャン */SCAN=パス;パス 例：/SCAN=C:\;D:*）
- ***/COMP*** 完全コンピュータスキャン
- ***/HEUR*** ヒューリスティック分析の使用
- ***/EXCLUDE*** スキャンからパス、またはファイルを除外
- ***/@*** コマンドファイル /file name/
- ***/EXT*** これらの拡張子をスキャンする /例えば、EXT=EXE,DLL/
- ***/NOEXT*** これらの拡張子をスキャンしない /例えば、NOEXT=JPG/
- ***/ARC*** アーカイブをスキャン
- ***/CLEAN*** 自動的駆除
- ***/TRASH*** 感染ファイルをウイルス隔離室に移動
- ***/QT*** クイックスキャン
- ***/MACROW*** マクロを報告する
- ***/PWDW*** パスワード保護されたファイルを報告する
- ***/IGNLOCKED*** ロックされたファイルを無視
- ***/REPORT*** ファイルにレポート/file name/
- ***/REPAPPEND*** レポートファイルに追加
- ***/REPOK*** 未感染ファイルを「OK」として報告する
- ***/NOBREAK*** CTRL-BREAKで中断しない
- ***/BOOT*** MBR/BOOT チェックを有効化
- ***/PROC*** アクティブプロセスをスキャンする
- ***/PUP*** 「不審なプログラム」を報告する
- ***/REG*** レジストリをスキャンする

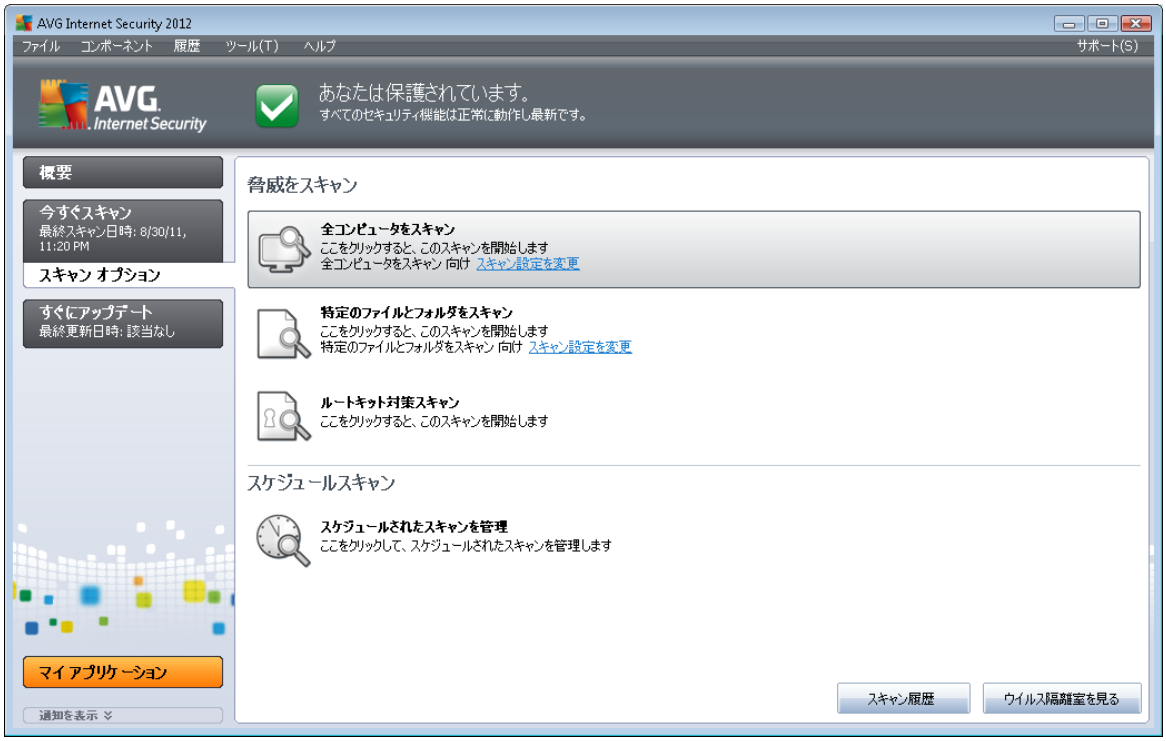
- ***/COO*** cookieをスキャンする
- ***/?*** このトピックに関するヘルプを表示
- ***/HELP*** このトピックに関するヘルプを表示
- ***/PRIORITY*** *スキャン優先度 (低、自動、高) を設定 (高度な設定/スキャン を参照)*
- ***/SHUTDOWN*** スキャン完了時にコンピュータをシャットダウン
- ***/FORCESHUTDOWN*** スキャン完了時にコンピュータを強制シャットダウン
- ***/ADS*** *Alternate Data Streams をスキャン(NTFSのみ)*
- ***/ARCBOMBSW*** 再圧縮されたアーカイブファイルを報告

11.5. スキャン スケジュール

AVG Anti-Virus 2012 では、オンデマンドで (ウイルスに感染した場合など) またはスケジュールに基づいてスキャンを実行できます。スケジュールに基づいてスキャンを実行することを強くお勧めします。この方法を採用することでコンピュータが感染の可能性から保護されていることを保証でき、スキャンがいつ起動しているかを考える必要がありません。

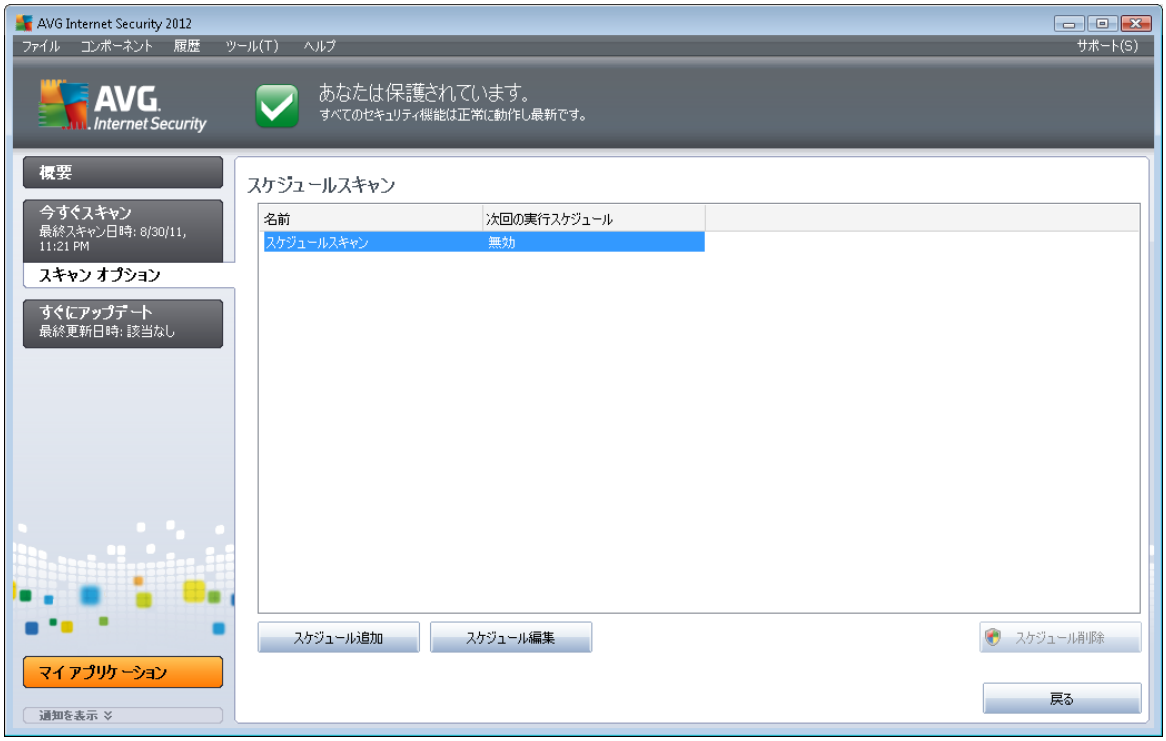
完全コンピュータスキャンを週に1度以上定期的に実行することをお勧めします。ただし、可能な場合は、コンピュータのスキャンを毎日実行してください。既定のスキャン スケジュールはこのように設定されています。コンピュータが常にオンとなっている場合、作業時間外にスキャンを実行するよう設定することができます。コンピュータがオフになっていたためスケジュールが実行されなかった場合に備えて、コンピュータの起動時にスキャンを実行するようにスケジュールを設定します。

新しいスキャン スケジュールを作成するには、AVG スキャン インターフェースを参照し、下部の***スケジュール スキャン***セクションを確認してください。



スケジュール スキャン

[***スキャンのスケジュール***] セクションのグラフィカルなアイコンをクリックすると、新しい [***スキャンのスケジュール***] ダイアログが開き、現在スケジュールされているすべてのスキャンのリストが表示されます。

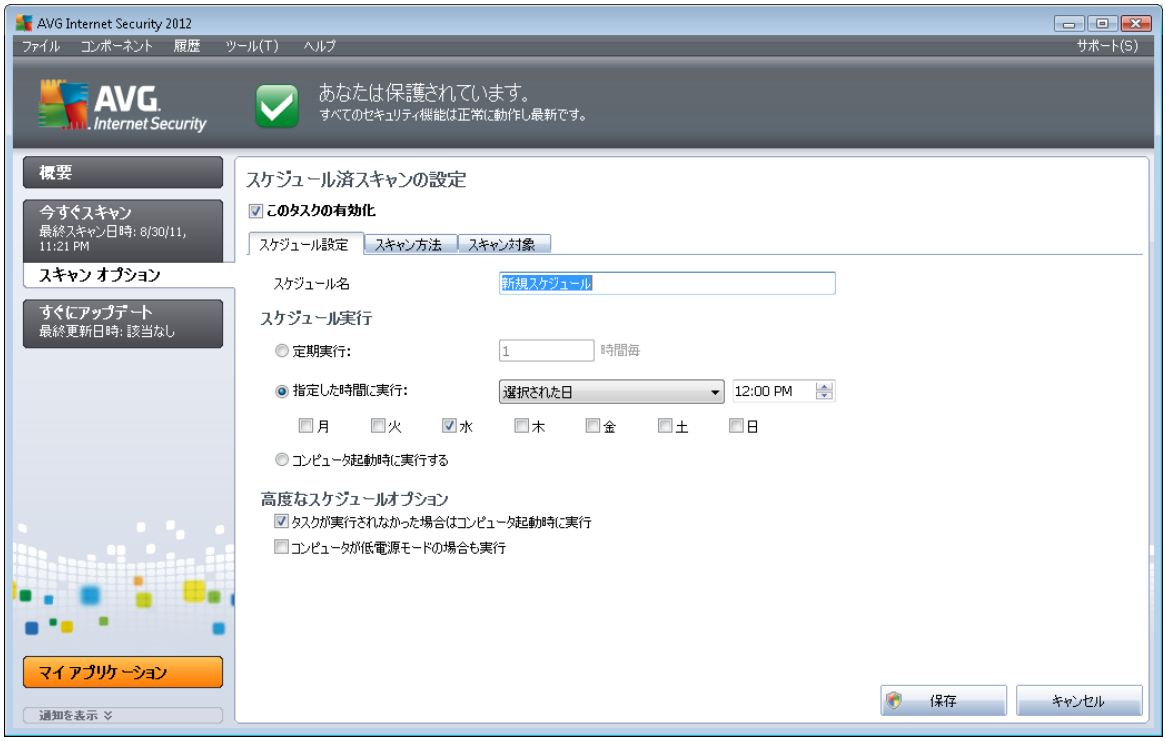


次のコントロール ボタンを使用して、スキャンの編集および追加ができます。

- ***スキャン スケジュールの追加*** - [***スケジュール スキャン設定***] ダイアログの [スケジュール設定] タブを開きます。このダイアログでは、スキャン パラメータを指定できます。
- ***スキャン スケジュールの編集*** - スケジュール スキャンの一覧から既存のスキャン スケジュールを選択した場合にのみこのボタンを使用できます。このボタンをクリックすると、[***スケジュール スキャン設定***] ダイアログの [スケジュール設定] タブが表示されます。選択したスキャンのパラメータがこのタブで指定され、編集できます。
- ***スキャン スケジュールの編集*** - スケジュール スキャンの一覧から既存のスキャン スケジュールを選択した場合にのみこのボタンを使用できます。コントロール ボタンをクリックすると、選択したスキャンを一覧から削除できます。ただし、自分で作成したスケジュールのみを削除できます。既定で定義されている***完全コンピュータ スキャン スケジュール***は削除できません。
- ***戻る*** - AVG スキャン インターフェースに戻ります

11.5.1. スケジュール設定

新しい検査と定期実行をスケジュールする場合、[***スケジュール済みの検査の設定***] ダイアログ (*[スキャンのスケジュール]* ***ダイアログで*** *[****スキャン スケジュールの追加****] ボタンをクリック*) を入力します。このダイアログは 3 つのタブに分けられます。***スケジュール設定*** *- 以下の図を参照 自動的にリダイレクトされる既定のタブ*)、スキャン方法、スキャン対象



[***スケジュール設定***] タブでは、[***このタスクの有効化***] アイテムのチェックをON/OFFすることによって、必要に応じて、スケジュール済みスキャンを一時的に有効化/無効化することができます。

次に、作成してスケジュールするスキャンの名前を付けます。***名前***アイテムの近くのテキストフィールドに名前を入力します。スキャンには、簡潔で、説明的で、適切な名前を使用して、のちに他のスキャンと区別できるようにしてください。

例： *新規スキャン」あるいは「マイスキャン」という名前は適切ではありません。これらの名前は、実際にスキャンがチェックする対象を指さないからです。「システムエリアスキャン」というような名前が推奨されます。また、スキャンが完全コンピュータスキャンか単に選択されたファイルやフォルダのスキャンであるかを区別する名前を指定することも重要です - 自分のスキャンは常に選択されたファイルやフォルダのスキャンの特定バージョンにあります。*

このダイアログでは、さらに以下のスキャンパラメータを定義します。

- ***スケジュール実行*** - スキャン起動時間を指定します。タイミングは、***定期実行***、***指定した時間に実行***、***アクションにより実行***のいずれかによって定義することができます。
- ***高度なスケジュールオプション*** - このセクションでは、コンピュータが低電源モードあるいは完全に電源オフになっている場合に、スキャンが実行される条件を定義します。

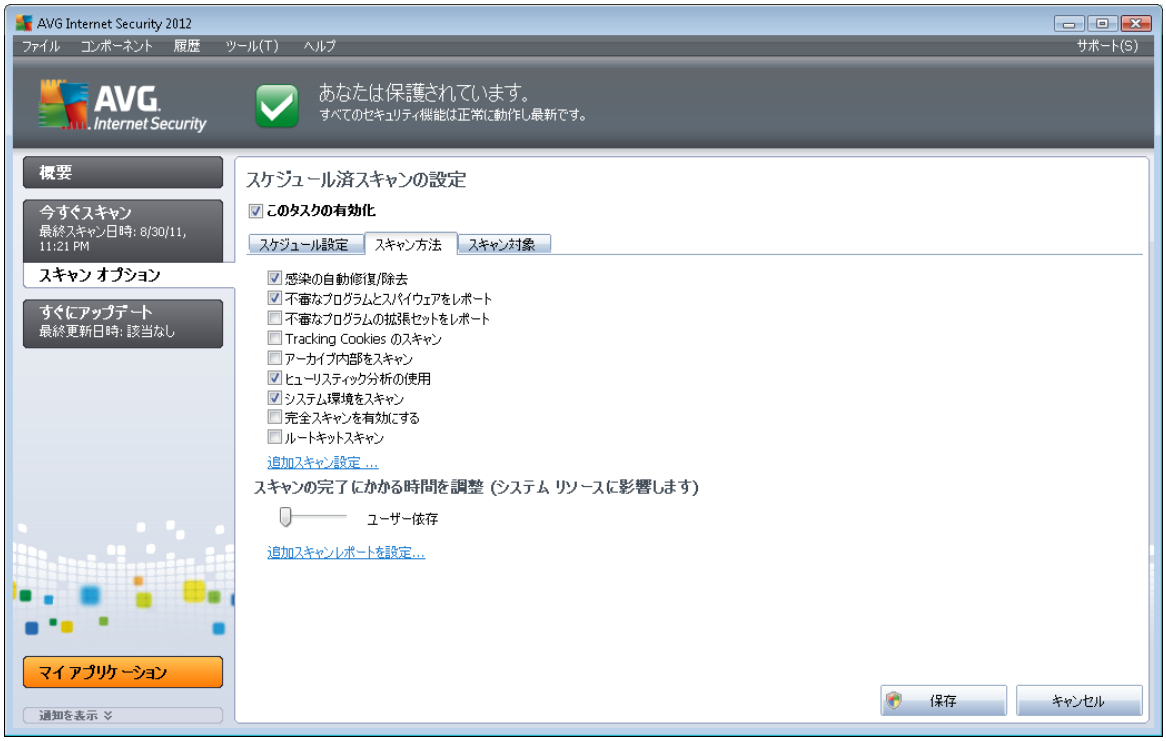
スケジュール済スキャンダイアログのコントロールボタン

スケジュールされたスキャンの設定***ダイアログのすべてのタブ***（スケジュール設定、スキャン方法、スキャン対象）には2つのコントロールボタンがあり、これらは同一の機能を持っています。

- ***保存*** - このタブまたはこのダイアログのその他のタブで行ったすべての変更を保存し、AVG スキャン インターフェースの既定のダイアログに戻ります。したがって、すべてのタブでスキャン パラメータを設定する場合、すべての必要項目を指定した後でこのボタンをクリックしてください。

- ***キャンセル*** - このタブまたはこのダイアログのその他のタブで行ったすべての変更をキャンセルし、AVG スキャン インターフェースの既定のダイアログに戻ります。

11.5.2. スキャン方法



[***スキャン方法***] タブには、任意でオン/オフを切り替えられるスキャン パラメータの一覧が表示されます。既定ではほとんどのパラメータがオンになっており、その機能はスキャン実行中に適用されます。やむを得ない理由がない場合は、あらかじめ定義された設定を保持することを推奨します。

- ***自動的に感染を修復/除去する*** (*既定ではオン*): スキャン実行中にウイルスが特定され、修復可能な場合は、自動的に修復されます。感染ファイルを自動的に修復できない場合やこのオプションをオフにした場合は、ウイルス検出が通知されるので、検出された感染の処理方法を決定する必要があります。推奨アクションは、感染ファイルのウイルス隔離室への移動です。

- ***不審なプログラムとスパイウェア脅威を報告する*** (*既定ではオン*): チェックを付けると、スパイウェア対策エンジンを有効にし、ウイルスと同時にスパイウェアもスキャンします。スパイウェアは疑わしいマルウェアのカテゴリに含まれます。通常は、セキュリティリスクとなる場合でも、このようなプログラムを故意にインストールすることができます。コンピュータのセキュリティを高めるため、この機能を有効にしておくことをお勧めします。

- ***不審なプログラムの拡張セットを報告する*** (*既定ではオフ*): 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。スパイウェアとは、直接製造元から入手する場合にはまったく問題がなく、無害なプログラムですが、後から悪意のある目的で誤用されるおそれのあるプロ

グラムです。これは、コンピュータセキュリティ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。

- ***Tracking Cookie をスキャンする*** (*既定ではオフ*): スパイウェア対策 コンポーネントのこのパラメータを定義すると、スキャン実行中に Cookie を検出します *'HTTP cookie は、サイトの設定や電子ショッピング カートの内容など、ユーザー固有の情報の認証、追跡、メンテナンスに使用されます*)。

- ***アーカイブの内容をスキャンする*** (*既定ではオン*): このパラメータを定義すると、ファイルが ZIP や RAR などのアーカイブ形式で圧縮されている場合でも、すべてのファイルに対してスキャンチェックを実行します。

- ***ヒューリスティック分析を使用する*** (*既定ではオン*): ヒューリスティック分析 (*仮想コンピュータ環境で実行されるスキャン対象オブジェクト命令の動的エミュレーション*) は、スキャン実行中に採用されるウイルス検出方法の 1 つです。

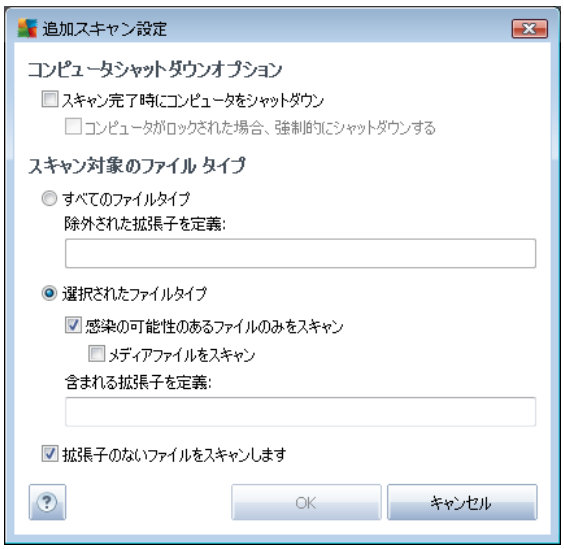
- ***システム環境をスキャンする*** (*既定ではオン*): コンピュータのシステム領域もチェックされます。

- ***完全スキャンを有効にする*** (*既定ではオフ*) - このオプションをチェックすると、特定の状況 (*コンピュータが感染している疑いがある場合など*) が発生した場合に最も完全なスキャン アルゴリズムを有効にし、感染の可能性が非常に低いコンピュータ領域もスキャンします。これにより、問題がないことを確実に確認します。この方法を実行すると多少時間がかかります。

- ***ルートキットをスキャンする*** (*既定ではオフ*): この項目にチェックを付けると、完全コンピュータスキャン中にルートキットをスキャンします。また、ルートキット スキャンはルートキット対策 コンポーネントでも独自に実行できます。

次の方法でスキャン設定を変更できます。

- ***追加スキャン設定*** - このリンクをクリックすると、新しい [追加スキャン設定] ダイアログが開きます。このダイアログでは、次のパラメータを指定できます。



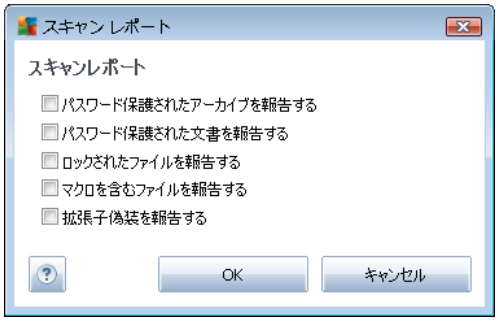
  - ***コンピュータのシャットダウン オプション*** - 実行中のスキャン処理が終了した時点で

自動的にコンピュータをシャットダウンするかどうかを決定します。このオプション (***スキャン完了時にコンピュータをシャットダウン***) を選択すると、現時点でコンピュータがロックされている場合でも、コンピュータをシャットダウンさせる新しいオプション (***コンピュータがロックされた場合強制的にシャットダウンする***) が有効になります。

- ***スキャンのファイル タイプ*** - さらに、スキャンするかどうかを決定する必要があります。
  - ***すべてのファイル タイプと***スキャン対象ではないファイル拡張子をカンマで区切ったリストを入力することで、スキャンからの除外を定義できます。
  - ***選択したファイル タイプ*** - 感染の可能性のあるファイルのみを指定できます (一部のプレーンテキストファイルやその他の非実行可能ファイルなど感染の可能性がないファイルはスキャンされません)。これには、メディアファイル (ビデオ、オーディオファイル) が含まれます。多くの場合、このようなファイルはサイズが非常に大きく、ウィルスに感染している可能性が非常に低いため、このボックスのチェックを外すと、スキャン時間がさらに短縮されますここでも、必ずスキャンするファイルの拡張子を指定できます。
  - 任意で***拡張子のないファイルをスキャン***できます。このオプションは既定ではオンになっています。変更する理由がない場合は、この設定を保持することをお勧めします。拡張子のないファイルは不審であるため、常にスキャンすることをお勧めします。

- ***スキャン実行速度を調整する*** - スライダを使用して、スキャン処理の優先度を変更できます。既定ではこのオプションの値は、自動的にリソースを使用するユーザー依存レベルに設定されています。低速でスキャン処理を実行してシステムリソース負荷を最小化 (コンピュータで同時に作業をする必要があり、スキャンに時間がかかってもよい場合に便利です) したり、システムリソース消費量の高い高速スキャン (コンピュータが一時的に使用されていない場合などに便利です) を実行したりできます。

- ***追加スキャンレポートを設定*** - このリンクをクリックすると、[***スキャンレポート***] ダイアログが開きます。このダイアログでは、レポート対象の検出の種類を選択できます。



コントロール ボタン

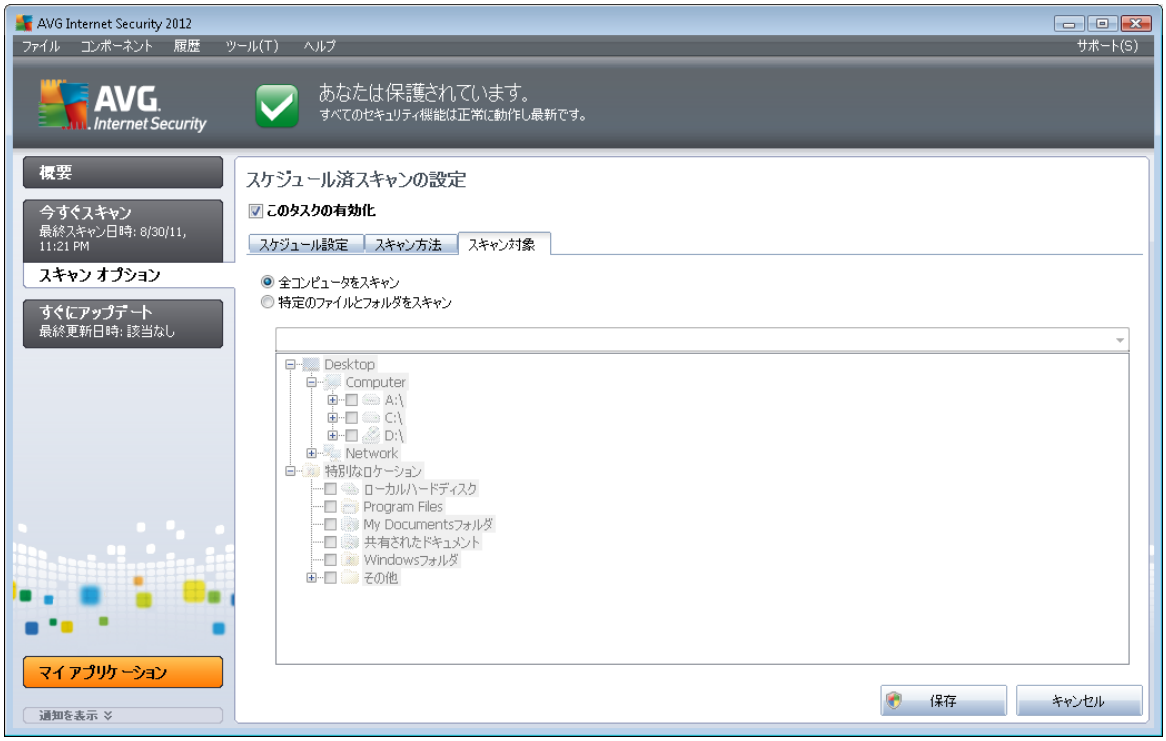
スケジュール済スキャンの設定***ダイアログのすべてのタブ*** (スケジュール設定、スキャン方法、スキャン対象) には 2 つのコントロールボタンがあり、これらは同一の機能を持っています。

- ***保存*** - このタブまたはこのダイアログのその他のタブで行ったすべての変更を保存し、AVG ス

キャン インターフェースの既 定 のダイアログに戻 ります。したがって、すべてのタブでスキャン パラメータを設 定 する場 合 、すべての必 要 項 目 を指 定 した後 でこのボタンをクリックしてください。

- ***キャンセル*** - このタブまたはこのダイアログのその他 のタブで行 ったすべての変 更 をキャンセルし、AVG スキャン インターフェースの既 定 のダイアログに戻 ります。

11.5.3. スキャン対象



[***スキャン対 象***] タブでは、[完 全 コンピュータ スキャン] あるいは [特 定 のファイルやフォルダのスキャン] のいずれかを定 義 できます。

特 定 のファイルまたはフォルダのスキャンを選 択 する場 合 は、このダイアログの下 部 に表 示 されるツリー構 造 がアクティブになり、スキャンするフォルダを選 択 できます (*スキャンするフォルダが見 つかるまでプラス ノードをクリックして項 目 を展 開 します*)。各 ボックスにチェックを付 けることで複 数 のフォルダを選 択 できます。選 択 したフォルダはダイアログ上 部 のテキスト フィールドに表 示 されます。選 択 したスキャン履 歴 はドロップダウン メニューに保 持 されるため、後 から使 用 できます。任 意 のフォルダへの完 全 パスを手 入 力することもできます (*複 数 パスを入 力 する場 合 は、スペースを入 れずセミコロンで区 切 る必 要 があります*)。

ツリー構 造 内 には、[***特 別 な場 所***] という部 分 もあります。各 チェック ボックスにマークを付 けると、次 のようにスキャンする場 所 の一 覧 が表 示 されます。

- ***ローカル ハード ドライブ*** - コンピュータのすべてのハード ドライブ
- ***プログラム ファイル***

- C:\Program Files\
- *64 ビット バージョン* C:\Program Files (x86)

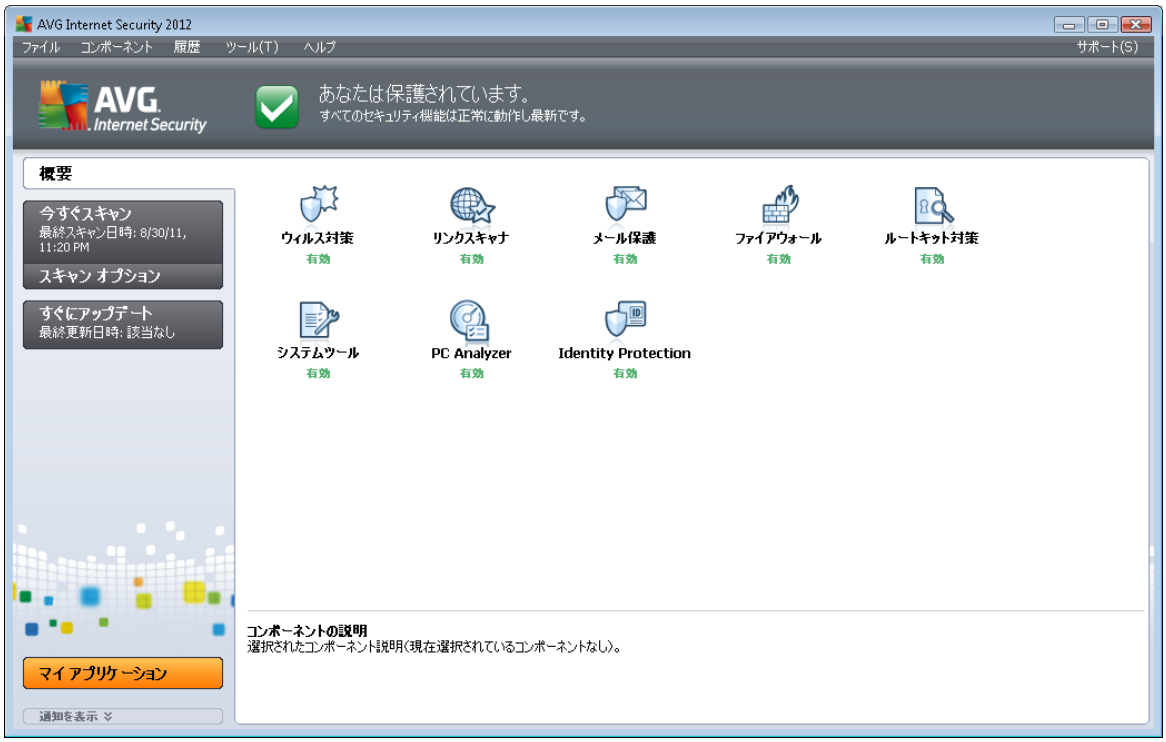
- ***マイ ドキュメント フォルダ***
  - *Win XP:* C:\Documents and Settings\Default User\My Documents\
  - *Windows Vista/7*: C:\Users\user\Documents\
- ***共有 ドキュメント***
  - *Win XP*: C:\Documents and Settings\All Users\Documents\
  - *Windows Vista/7*: C:\Users\Public\Documents\
- ***Windows フォルダ*** - C:\Windows\
- ***その他***
  - *システム ドライブ* - オペレーティング システムがインストールされているハードドライブ (通常は C:)
  - *システム フォルダ* - C:\Windows\System32\
  - *一時 ファイル フォルダ* - C:\Documents and Settings\User\Local\ (*Windows XP*); or C:\Users\user\AppData\Local\Temp\ (*Windows Vista/7*)
  - *一時 インターネット ファイル* - C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (*Windows XP*); or C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (*Windows Vista/7*)

コントロール ボタン

[***スケジュール済 スキャンの設定***] ダイアログの 3 つのタブのすべてで、次の同じ 2 つのコントロール ボタンが表示されます (*スケジュール設定*、*スキャン方法*、*スキャン対象*)。

- ***保存*** - このタブまたはこのダイアログのその他のタブで行ったすべての変更を保存し、AVG スキャン インターフェースの既定のダイアログに戻ります。したがって、すべてのタブでスキャン パラメータを設定する場合、すべての必要項目を指定した後でこのボタンをクリックしてください。
- ***キャンセル*** - このタブまたはこのダイアログのその他のタブで行ったすべての変更をキャンセルし、AVG スキャン インターフェースの既定のダイアログに戻ります。

11.6. スキャン結果概要



スキャン結果概要ダイアログは、AVGスキャンインターフェースから***スキャン履歴***ボタンを押すとアクセスすることができます。ダイアログには、以前実行されたすべてのスキャンと結果情報のリストが表示されます。

- ***名前*** - スキャン指定。予め定義されたスキャンの名前あるいは、自分のスケジュール済のスキャンに付けられた名前です。各名前には、スキャン結果を示すアイコンが表示されます。

  - 緑のアイコンはスキャン中に感染が検出されなかったことを示します。

  - 青のアイコンは、スキャン中に感染があり、感染したオブジェクトは自動的に除去されたことを知らせています。

  - 赤のアイコンは、スキャン中に感染が検出され、それを除去できなかったことを警告しています。

  各アイコンは完全な形、または半分のアイコンで表示されます。完全な形のアイコンは正常終了したスキャンを示しています。半分になったアイコンはスキャンがキャンセルされたか中断されたことを示しています。

  注意:*各スキャンの詳細情報については、詳細を見るボタン(ダイアログ下部)からアクセス可能なスキャン結果ダイアログを参照してください。*

- ***開始時間*** - スキャンが実行された日時
- ***終了時間*** - スキャンが終了した日時

- ***スキャン済オブジェクト***- スキャンでチェックされたオブジェクトの数
- ***感染***- 検出/除去されたウイルス感染の数
- ***スパイウェア***- 検出/除去されたスパイウェアの数
- ***警告*** - 検出された不審なオブジェクト
- ***ルートキット*** - 検出されたルートキット
- ***スキャンログ情報***- スキャン過程と結果に関する情報（一般的には完了か中断かの情報）

コントロールボタン

スキャン結果概要ダイアログには、以下のコントロールボタンがあります。

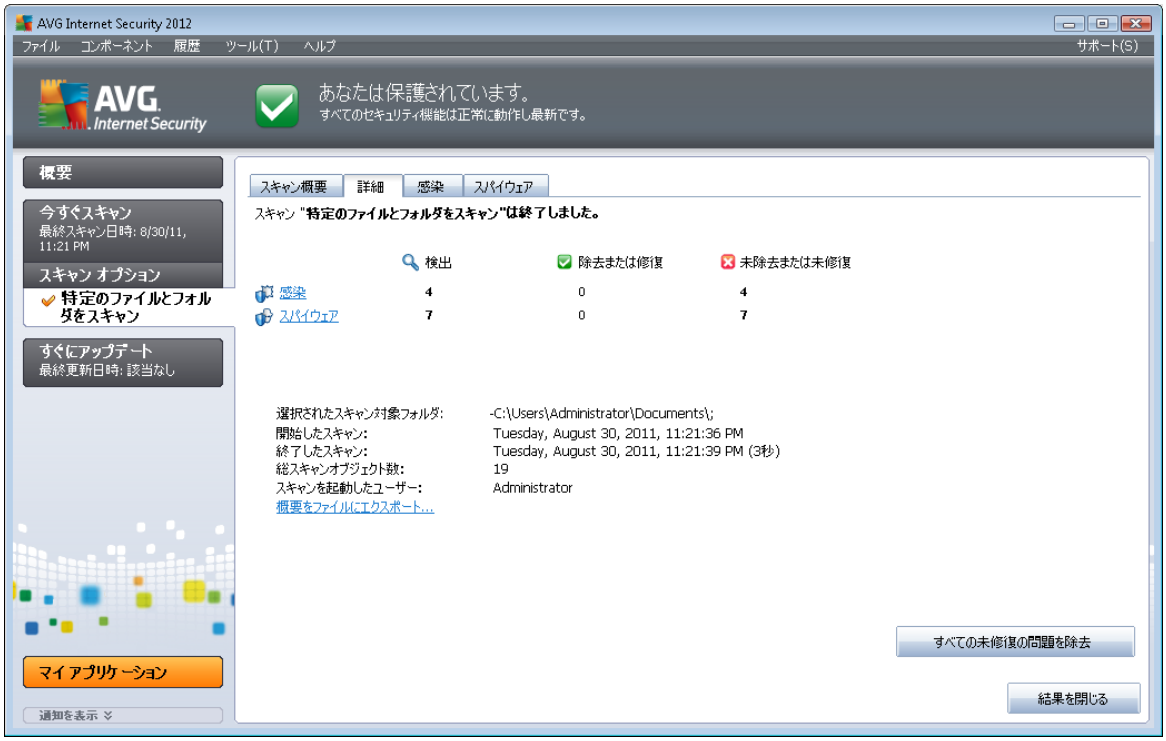
- □□□□□ - クリックすると、[スキャン結果] ダイアログに切り替わり、選択したスキャンの詳細データを表示します。
- ***結果を削除*** - クリックすると、スキャン結果概要から選択したアイテムを削除します。
- ***戻る***- AVGスキャンインターフェースのデフォルトダイアログに切り替わります。

11.7. スキャン結果詳細

スキャン結果概要ダイアログで、特定のスキャンが選択された場合、***詳細を表示***ボタンをクリックすると、***スキャン結果***ダイアログが表示されます。このダイアログでは、選択されたスキャン結果に関する詳細なデータが表示されます。このダイアログはさらにいくつかのタブに分けられます。

- 結果概要 - このタブは常に表示され、スキャン進捗を示す統計データが表示されます。
- 感染 - このタブは、スキャン実行中にウイルス感染が検出された場合にのみ表示されます。
- スパイウェア - このタブは、スキャン実行中にスパイウェアが検出された場合にのみ表示されます。
- 警告 - Cookieがスキャン中に検出されると、このタブがインスタンスごとに表示されます。
- ルートキット - このタブは、スキャン実行中にルートキットが検出された場合にのみ表示されます。
- 情報 - このタブは潜在的な脅威が検出され、これらが上記のいずれのカテゴリにも分類できない場合にのみ表示されます。このタブでは警告メッセージが表示されます。また、スキャンできなかったオブジェクトに関する情報も表示されます *(パスワード保護されたアーカイブなど)*。

11.7.1. 結果概要タブ



スキャン結果タブには、以下の情報に関する詳細な統計が表示されます。

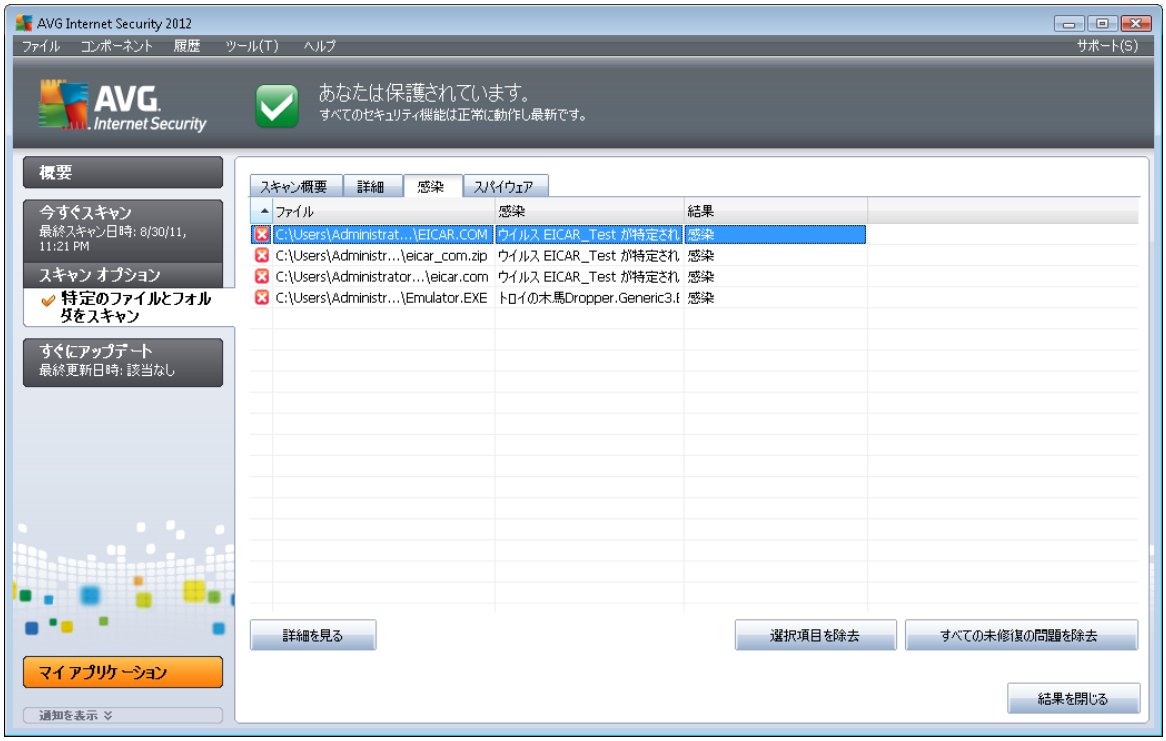
- 検出されたウィルス感染/スパイウェア
- 除去されたウイルス感染/スパイウェア
- 除去または修復不可能なウイルス感染/スパイウェア数

また、スキャン開始の正確な日時、スキャンされたオブジェクトの合計数、スキャン期間、スキャン実行中に発生したエラー数に関する情報も表示されます。

コントロールボタン

このダイアログで利用できるコントールボタンは1つです。***結果を閉じる***ボタンを押すと、スキャン結果概要ダイアログに戻ります。

11.7.2. 感染タブ



感染タブは、スキャン中にウイルス感染***が検出された場合、スキャン結果***ダイアログでのみ表示されます。このタブは3つのセクションに分かれ、以下の情報が表示されます。

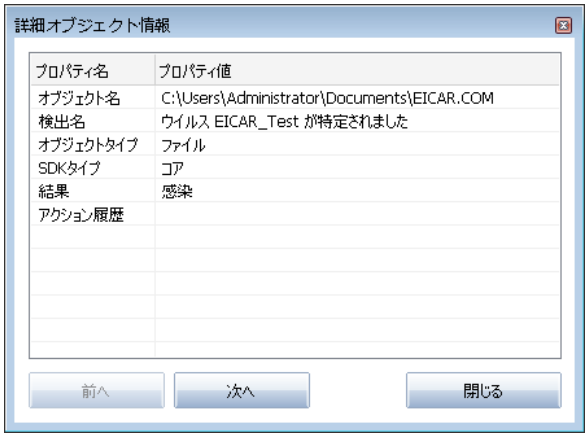
- ***ファイル*** - 感染オブジェクトの元の場所へのフルパス
- ***感染*** - 検出されたウイルス名（*ウイルスの詳細は、オンラインの[ウイルスエンサイクロペディア](#)を参照してください*）
- ***結果*** - スキャン中に検出された感染オブジェクトの現在のステータス
    - ***感染*** - 感染オブジェクトが検出され、元の場所に存在します。 *例えば、[自動修復オプション](#)を特定のスキャン設定でオフにしている場合*）
    - ***修復*** - 感染オブジェクトは自動修復され、元の場所に存在しますす。
    - ***ウイルス隔離室に移動*** - 感染オブジェクトは[ウイルス隔離室](#)に移動されました。
    - ***削除*** - 感染オブジェクトは削除されました。
    - ***PUP例外に追加*** - *検出は例外として評価され、PUP例外リスト（高度な設定の[PUP例外](#)ダイアログで設定）に追加されました。*
    - ***ロックされたファイル - 未スキャン*** - 対象オブジェクトはロックされているため、AVGはスキャンできません。

- ***潜在的に危険なオブジェクト*** - オブジェクトは潜在的に危険なものとして検出されましたが、感染していません(*例えば、マクロを含む等*)。
- ***アクションを終了するために再起動を要求*** - 感染オブジェクトを除去できません。完全に除去するには、コンピュータの再起動が必要です。

コントロールボタン

このダイアログには3つのコントロールボタンがあります。

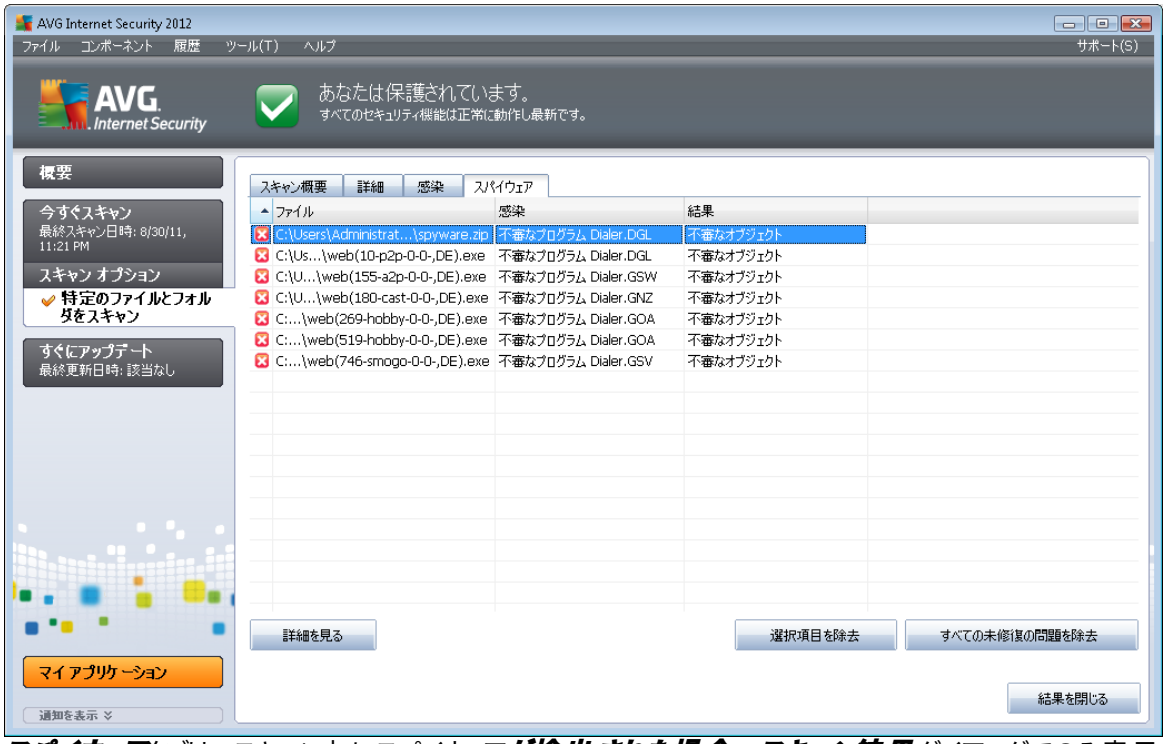
- ***詳細を見る*** - このボタンは [***詳細オブジェクト情報***] という新しいダイアログを開きます。



このダイアログには、検出された感染オブジェクトに関する詳細情報 (*感染したオブジェクト名と場所、オブジェクトの種類、SDK の種類、検出結果、検出されたオブジェクトに関するアクションの履歴など*) が表示されます。***前へ/次へ***ボタンを使用して、特定の検出情報を見ることができます。***閉じる***ボタンを使用して、このダイアログを閉じることができます。

- ***選択した感染を除去*** - このボタンをクリックすると、選択した検出をウイルス隔離室に移動します
- ***すべての未修復の感染を削除*** - このボタンはすべての修復不可能な検出やウイルス隔離室
- ***結果を閉じる*** - 詳細情報概要を終了し、スキャン結果概要ダイアログに戻ります。

11.7.3. スパイウェア タブ



スパイウェアタブは、スキャン中にスパイウェア***が検出された場合、スキャン結果***ダイアログでのみ表示されます。このタブは3つのセクションに分かれ、以下の情報が表示されます。

- ***ファイル*** - 感染オブジェクトの元の場所へのフルパス
- ***感染*** - 検出されたスパイウェア名 (*特定のウィルスの詳細については、オンラインの[ウィルス エンサイクロペディア](#)を参照してください*)。
- ***結果*** - スキャン中に検出された感染オブジェクトの現在のステータス
    - ***感染*** - *感染オブジェクトが検出され、元の場所に存在します。 例えば、[自動修復オプション](#)を特定のスキャン設定でオフにしている場合）*
    - ***修復*** - 感染オブジェクトは自動修復され、元の場所に存在しますす。
    - ***ウイルス隔離室に移動*** - 感染オブジェクトは[ウイルス隔離室](#)に移動されました。
    - ***削除*** - 感染オブジェクトは削除されました。
    - ***PUP 例外に追加*** - *検出項目は例外として評価され、PUP 例外リスト 高度な設定の[PUP 例外](#)ダイアログで設定）に追加されました。*
    - ***ロックされたファイル - 未スキャン*** - 対象オブジェクトはロックされているため、AVGはスキャンできません。
    - ***潜在的に危険なオブジェクト*** - オブジェクトは潜在的に危険なものとして検出されま

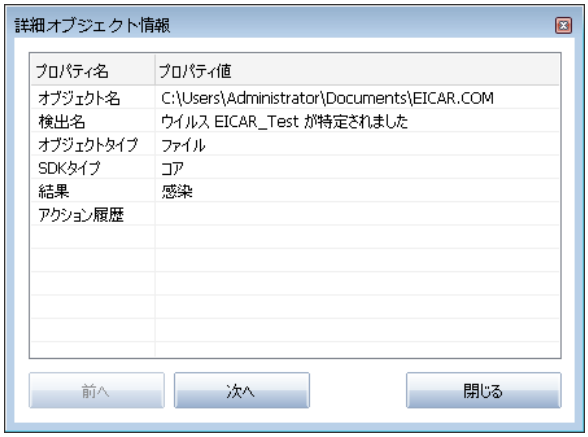
したが、感染していません 例えば、マクロを含む等)。

- ***アクションを終了するために再起動を要求*** - 感染オブジェクトを除去できません。完全に除去するには、コンピュータの再起動が必要です。

コントロールボタン

このダイアログには3つのコントロールボタンがあります。

- ***詳細を見る*** - このボタンは [***詳細オブジェクト情報***] という新しいダイアログを開きます。



このダイアログには、検出された感染オブジェクトに関する詳細情報 (*感染したオブジェクト名と場所、オブジェクトの種類、SDK の種類、検出結果、検出されたオブジェクトに関するアクションの履歴など*) が表示されます。***前へ/次へ***ボタンを使用して、特定の検出情報を見ることができます。***閉じる***ボタンを使用して、このダイアログを閉じることができます。

- ***選択した感染を除去*** - このボタンをクリックすると、選択した検出をウイルス隔離室に移動します
- ***すべての未修復の感染を削除*** - このボタンはすべての修復不可能な検出やウイルス隔離室
- ***結果を閉じる*** - 詳細情報概要を終了し、スキャン結果概要ダイアログに戻ります。

11.7.4. 警告タブ

警告タブには、スキャンで検出された「疑わしい」オブジェクトに関する情報 (*一般的にはファイル*) が表示されます。常駐シールドによって検出された場合は、これらのファイルへのアクセスはブロックされます。この種の検出の一般的な例は、隠されたファイル、cookie、疑わしいレジストリキー、パスワードで保護されたドキュメント、アーカイブ等です。このようなファイルはコンピュータやセキュリティにとって、何ら直接的な脅威を与えるものではありません。これらのファイルに関する情報は一般的に、コンピュータでアドウェアやスパイウェアが検出される場合に有用です。**AVG Anti-Virus 2012** の検査で警告のみが検出された場合は、対応は必要ありません。

このようなオブジェクトに関する最も一般的な例を以下に簡潔に説明しました。

- ***非表示のファイル*** - 既定では、非表示のファイルは Windows には表示されません。あるファイルやその他の脅威はこの属性を持ってファイルを格納することによって検出を避けようとする場合があります。**AVG Anti-Virus 2012** で悪意のあるファイルの疑いがある非表示のファイルが報告される場合、ウイルス隔離室に移動できます。

- ***Cookies*** - Cookies はウェブサイトによって使用されるプレーンテキストファイルです。これは、後にカスタムウェブサイトレイアウトや予め入力されたユーザー名等をロードするために使用されるユーザー特有の情報を格納するために使用されます。

- ***不審なレジストリキー*** - 一部のマルウェアはその情報を Windows レジストリに格納し、起動時にそれがロードされるようにしたり、それがオペレーティングシステムにまで影響するようにします。

11.7.5. ルートキットタブ

ルートキット対策スキャンを実行した場合、[***ルートキット***] タブには、スキャン中に検出されたルートキットに関する情報が表示されます。

ルートキットは、システムの所有者や正式な管理者の許可なくコンピュータシステムの基本的なコントロールを実行するように設計されたプログラムです。ルートキットはハードウェア上で実行されているオペレーティング システムを乗っ取ることを目的としているため、ハードウェアへのアクセスが必要になることはほとんどありません。一般的には、ルートキットは標準のオペレーティング システムのセキュリティメカニズムを破壊したり回避したりすることによって、システム上でその存在を隠しながら動作します。一般的に、ルートキットはトロイの木馬の一種でもあり、システムで実行しても安全であるかのように見せかけてユーザーを騙し、信じこませます。このような技術によって、プログラム監視の対象にならないように実行中のプロセスが隠されたり、オペレーティング システムからファイルやシステム データが隠されることもあります。

このタブの基本構成は [感染] タブや [スパイウェア] タブと同じです。

11.7.6. 情報タブ

情報 タブには、感染、スパイウェア等と分類できない「検出」に関するデータが表示されます。それらは危険なものと断定はされませんが、注意する価値はあります。**AVG Anti-Virus 2012** スキャンでは、感染している可能性がなくても不審なファイルを検出できます。このようなファイルは警告あるいは情報として報告されます。

重大度 ***情報*** は次の理由のいずれかで報告されます。

- ***ランタイムパック*** - このファイルは、少ない共通ランタイムパッカーのいずれかで圧縮されており、このようなファイルのスキャンを防ぐ試みを示している可能性があります。ただし、このようなファイルの報告のすべてがウイルスを示唆しているわけではありません。

- ***ランタイムパック再帰*** - 上記と同様ですが、共通ソフトウェア間の頻度は低くなります。このようなファイルは疑わしく、分析のためファイルの除去または提出を考える必要があります。

- ***パスワード保護されたアーカイブまたは文書*** - パスワード保護されたファイルは (**AVG Anti-Virus 2012***あるいは一般的にはその他のウイルスソフトウェア*) でスキャンできません。

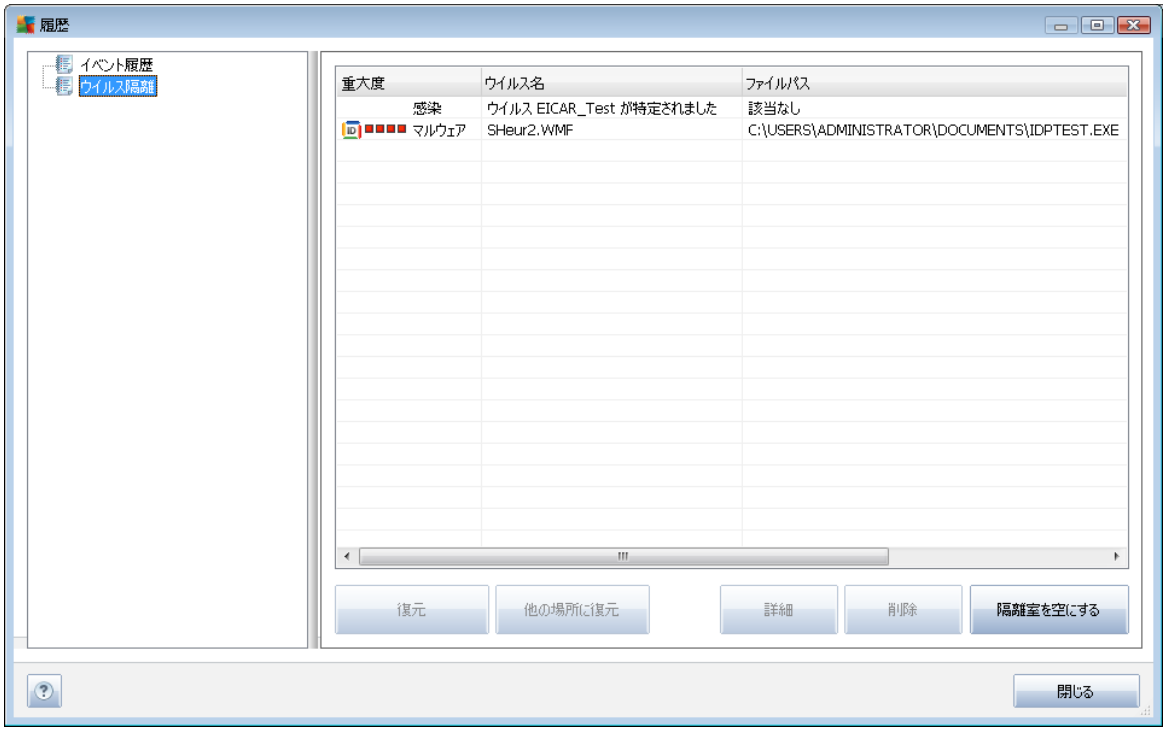
- ***マクロを含んだ文書*** - 報告された文書には、悪意のあるプログラムである可能性があるマクロが含まれます。

- ***拡張子偽装*** - 拡張子偽装のファイルは、画像などのように見える場合がありますが、実際には実行可能形式ファイル *例 :picture.jpg.exe*) です。Windows の既定の設定では、2 番目の拡張子は表示されませんが、**AVG Anti-Virus 2012** はこのようなファイルをレポートし、間違って開いてしまうことを防止します。

- ***不適切なファイルパス*** - 一部の重要なシステムファイルが既定以外のパスで実行中の場合 (*例 :Windows フォルダ以外で実行中の winlogon.exe*)、はこの不一致を報告します。**AVG Anti-Virus 2012**一部の場合、ウイルスは標準システムプロセス名を使用し、システム内でその存在を目立たなくします。

- ***ロックしたファイル*** - 報告されたファイルはロックされているため、**AVG Anti-Virus 2012** によってスキャンできません。これは通常一部のファイルが常にシステムによって使用されていることを意味しています *例 :スワップファイル*)。

11.8. ウイルス隔離室



ウイルス隔離室は、AVGスキャン中に検出された不審なオブジェクトまたは感染したオブジェクトを管理する安全な環境です。スキャン中に感染したオブジェクトが検出され、AVG で自動的に修復できない場合、この不審なオブジェクトの処理方法を決定するための画面が表示されます。推奨される解決方法は、このオブジェクトを***ウイルス隔離室***に移動することです。***ウイルス隔離室***の主な目的は、削除されたファイルを一定期間保存しておき、そのファイルが元の場所で必要がないものであることを確認できるようにすることです。ファイルが存在しないことによって問題が発生する場合は、問題のファイルを分析に送信したり、元の場所に復元したりできます。

ウイルス隔離室インターフェースは別ウィンドウで開き、隔離された感染オブジェクトに関する情報概要が表示されます。

- ***重大度*** - ID 保護 コンポーネントを**AVG Anti-Virus 2012**にインストールする場合、問題なし (■□□□) から非常に危険 (■■■■) までの 4 レベルの検出重大度がグラフィカルにこのセクションに表示されます。感染タイプ情報 (*感染レベルに基づいて、リストに表示されているすべてのオブジェクトは実際に感染しているか感染の可能性があります*) も表示されます。

- ***ウィルス名*** - ウィルス エンサイクロペディア (オンライン) に従って、検出された感染名を指定します。

- ***ファイル パス***- 検出された感染ファイルへの完全パス

- ***元のオブジェクト名*** - 一覧表示されているすべての検出されたオブジェクトは、スキャン処理中に AVG によって指定される標準名で表示されます。オブジェクトに既知の特定の元の名前があった場合 (*例: 添付ファイルの実際の内容に対応しないメール添付ファイル名*)、この名前がこの列に表示されます。

- ***保存日***- 不審なファイルが検出され、ウイルス隔離室

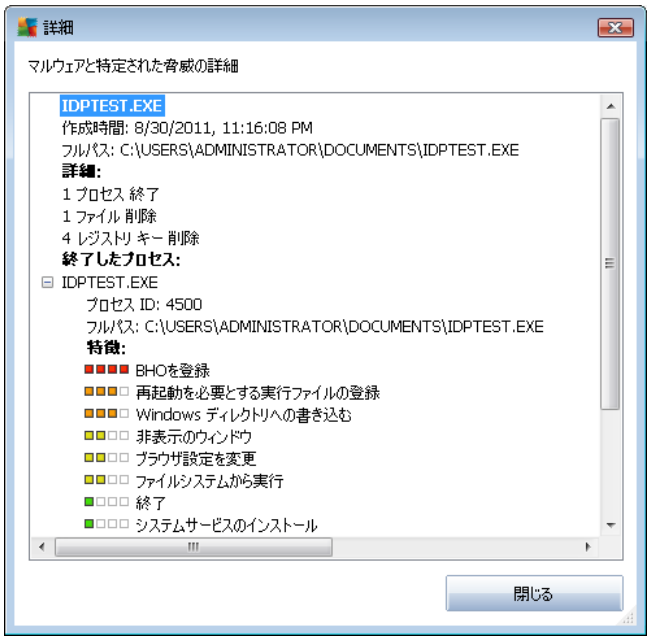
コントロール ボタン

ウイルス隔離室インターフェースでは次のコントロール ボタンが利用できます。

- ***復元***- 感染ファイルをディスク上の元の場所に復元します。

- ***場所を指定して復元*** - 感染したファイルを選択したフォルダに移動します。

- ***詳細*** - このボタンは、ID 保護で検出された脅威にのみ適用されます。クリックすると、脅威の詳細の概要 (*影響するファイルやプロセス、プロセスの特性など*) が表示されます。). IDP で検出されるその他のすべての項目では、このボタンはグレイ表示になり無効です。



- ***削除*** - 感染ファイルを***ウイルス隔離室***から完全に削除し、元に戻すことはできません。
- ***空にする*** - すべての***ウイルス隔離室***内のファイルを完全に削除します。***ウイルス隔離室***から削除するとファイルはディスクから削除されるため、元に戻すことはできません (*ごみ箱には移動されません*)。

12. AVG 更新

更新が定期的に実行されていない場合、セキュリティソフトウェアは脅威からの保護を保証できません。ウイルス作成者はソフトウェアとオペレーティング システムの両方の欠陥を常に探して、それを利用しようとしています。新しいウイルス、新しいマルウェア、新しいハッキング攻撃は日々出現しています。このため、ソフトウェア ベンダーは更新とセキュリティパッチを継続的に発行し、発見されたセキュリティホールを修正しています。

あらゆるコンピュータの脅威が新しく出現し、高速で拡大することを考えると、**AVG Anti-Virus 2012** を定期的に更新することは絶対に不可欠です。最善の方法は、自動更新が設定されているプログラムの既定の設定に従うことです。**AVG Anti-Virus 2012** のウイルス データベースが最新でない場合、プログラムは最新の脅威を検出できません。

AVG を定期的に更新することは非常に重要です。可能な限り、ウイルス定義更新を毎日実行してください。緊急度の低いプログラム更新は週次で実行してもかまいません。

12.1. 更新の実行

最高のセキュリティを実現するために、既定では、**AVG Anti-Virus 2012** が 4 時間ごとに新しい更新を検索するようにスケジュール設定されています。AVG 更新は固定のスケジュールではなく、新しい脅威の量と重要度に応じてリリースされるため、AVG ウイルス データベースが常に最新の状態であることを保証するためにはこのチェック機能が非常に重要です。

更新の実行回数を減らす場合は、独自の更新実行パラメータを設定できます。ただし、少なくとも 1 日に 1 回は更新を実行することを強くお勧めします。設定は [高度な設定/スケジュール] セクションで編集できます。具体的には次のダイアログが表示されます。

- 定義更新スケジュール
- プログラムアップデートスケジュール
- スパム対策 アップデートスケジュール

新しい更新ファイルをただちに確認する場合は、メイン ユーザー インターフェースの [今すぐアップデート] クイック リンクを使用します。このリンクはいつでもユーザーインターフェースダイアログから利用できます。

12.2. アップデート進捗

アップデートを開始すると、AVGはまず利用可能な新しいアップデートファイルがあるかどうかを確認します。ある場合は、**AVG Anti-Virus 2012** はダウンロードを開始し、更新処理を実行します。更新処理中は、***アップデート***インターフェースに移動します。ここでは、グラフィカルな表示や関連統計パラメータの概要で処理の状況を見ることができます (*更新ファイル サイズ、受信データ、ダウンロード速度、経過時間など*)。

***メモ**: AVG プログラム更新の前に、システム復元ポイントが作成されます。更新処理が失敗し、オペレーティング システムがクラッシュする場合には、必ずこのポイントから元の設定でオペレーティング システムを復元できます。このオプションには Windows メニューのスタート/すべてのプログラム/アクセサリ/システム ツール/システムの復元からアクセスできます。経験者ユーザーのみに推奨されます。*

12.3. 更新レベル

AVG Anti-Virus 2012 では 2 つの更新レベルから選択できます。

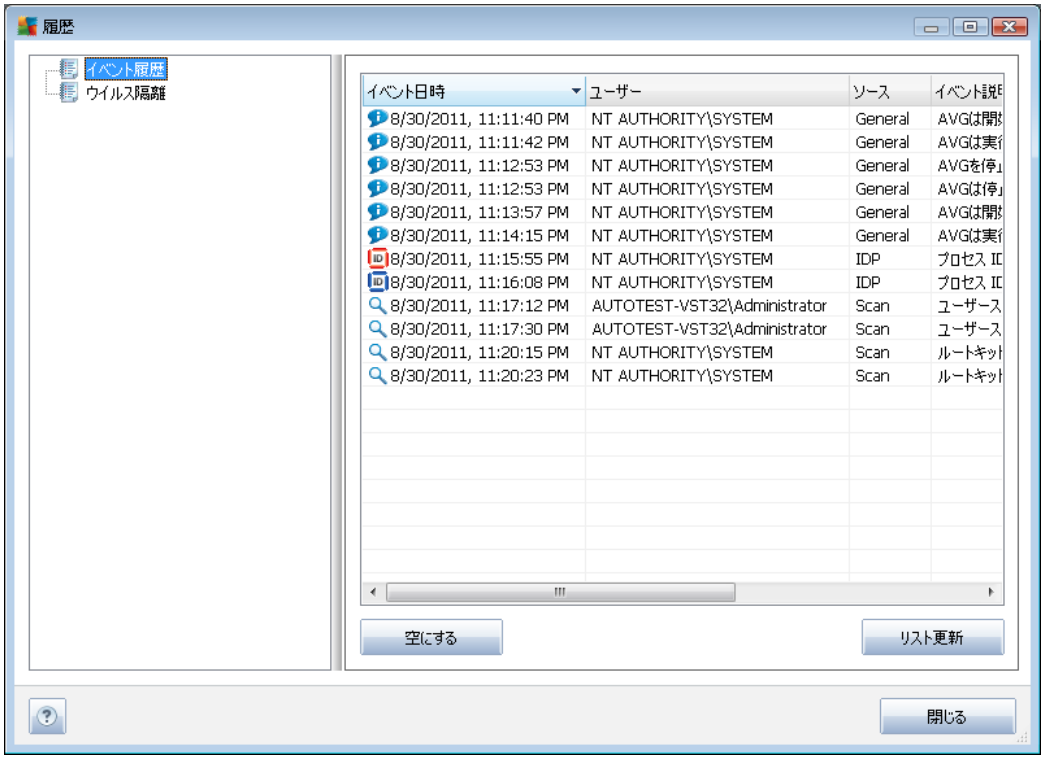
- ***定義アップデート***には信頼できるウィルス対策、スパム対策、マルウェア保護に必要な変更が含まれます。通常、コードの変更は含まれず、定義データベースのみを更新します。この更新が提供され次第、すぐに適用する必要があります。
- ***プログラム更新***には、各種プログラム変更、修正、改良点が含まれています。

更新のスケジュールを作成するときには、両方の更新レベルのパラメータを定義できます。

- 定義更新スケジュール
- プログラムアップデートスケジュール

***メモ**: スケジュール プログラム更新の時間がスケジュール スキャンの時間と同じになった場合は、更新処理が最優先され、スキャンは中断されます。*

13. イベント履歴



[***イベント履歴***] ダイアログには、システム メニューの [履歴/イベント履歴ログ] 項目からアクセスできます。このダイアログでは、**AVG Anti-Virus 2012** 動作中に発生した重要なイベントの概要を確認できます。***履歴***には次の種類のイベントが記録されます。

- AVG アプリケーションの更新情報
- スキャンの開始、終了、停止に関する情報 (*自動実行スキャンを含む*)
- 発生場所などウィルス検出に関連するイベントに関する情報 (*常駐シールド*または*スキャン*)
- 他の重要イベント

イベントごとに次の情報が一覧表示されます。

- ***イベント日時***は正確なイベント発生日時です。
- ***ユーザー***はイベント発生時にログインしていたユーザー名を示します。
- ***ソース***はイベントのトリガーとなったソース コンポーネントまたは AVG システムの一部に関する情報です。
- ***イベント説明***は実際の動作の簡単な概要です。

コントロール ボタン

- ***リストを空にする*** - このボタンをクリックすると、イベント リストのすべてのエントリが削除されます。
- ***リストを更新する*** - このボタンをクリックすると、イベント リストのすべてのエントリが更新されます。

14. FAQ とテクニカル サポート

AVG Anti-Virus 2012 アプリケーションに関する販売や技術的な問題がある場合は、さまざまな方法でサポートを検索できます。次のオプションから選択してください。

- ***カスタマー サポートに問い合わせる***: AVG アプリケーションから専門のカスタマー サポートに問い合わせることができます。[***ヘルプ/オンライン ヘルプ***] メイン メニュー項目を選択すると、オンラインのお問い合わせフォームに移動します。ここで 24 時間年中無休の AVG カスタマー サポートに連絡できます。ライセンス番号は自動入力されます。続行するには、Web ページの指示に従ってください。

- ***サポート (メイン メニューのリンク)***: AVG アプリケーション メニュー (*メイン ユーザー インターフェースの上*) の [***サポート***] リンクをクリックすると、新しいダイアログが開き、ヘルプの依頼に必要になる可能性のあるあらゆる種類の情報が表示されます。このダイアログにはインストールされている AVG プログラムに関する基本データ (プログラム/データベース バージョン)、*ライセンス詳細情報*、クイック サポート リンクの一覧が表示されます。

- ***ヘルプ ファイルのトラブルシューティング***: **AVG Anti-Virus 2012**のヘルプ ファイルからは、新しい [***トラブルシューティング***] セクションを直接表示できます。このセクションには、ユーザーが技術的な問題について専門のヘルプを検索するときに最も多く発生している状況の一覧が表示されます。現在発生している問題に最も近い状況を選択してクリックすると、問題の解決策を示す詳細手順が表示されます。

- ***AVG Web サイトの センター***: AVG Web サイト (http://www.avg.com/) で問題の解決策を検索することもできます。[***サポート センター***] セクションには、販売と技術的な問題の両方に対応するトピック グループの概要が構造化された方法で表示されます。

- ***よくある質問***: AVG Web サイト (http://www.avg.com/) では、よくある質問という個別の構造化されたセクションを検索することもできます。このセクションには、[***サポート センター/FAQ***] メ

ニュー オプションからアクセスできます。また、すべての質問は販売、技術、ウイルスというカテゴリに分割され整理されています。

- ***ウイルスと脅威について***: AVG Web サイト (http://www.avg.com/) の特定の章はウィルスに関する専用ページです。このメニューでは、[***サポート センター/ウイルスと脅威について***] を選択すると、オンラインの脅威の概要を構造化された方法で表示するページが開きます。また、ウイルスやスパイウェアの駆除手順や脅威に対する保護方法の提案も確認できます。

- ***ディスカッション フォーラム***: AVG ユーザーのディスカッション フォーラム (http://forums.avg.com) も利用できます。

