AVG 9 Internet Security

ユーザーマニュアル

ドキュメント改訂 90.21 (3.2.2010)

目次

1. はじめに

このユーザー マニュアルは、**AVG 9 Internet Security** の包括的なマニュアルです。

AVG 9 Internet Security をご購入いただき、どうもありがとうございます。

AVG 9 Internet Securityは、コンピュータの総合的なセキュリティを提供するように設計された、受賞経験のある AVG 製品の 1 つです。すべての AVG 製品と同様に、AVG の信頼性のあるセキュリティ機能をより分かりやすく、効率的な方法で提供するために、**AVG 9 Internet Security** は完全に再設計されました。

新しい **AVG 9 Internet Security** 製品は、合理化されたインターフェースとより積極的で高速化されたスキャンを提供します。より多くのセキュリティ機能が自動化され便利になりました。新しい「インテリジェント」ユーザーオプションが搭載され、セキュリティ機能をカスタマイズしやすい製品となりました。妥協のないユーザビリティを提供します。

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

2. AVGインストール要件

2.1. 対応オペレーションシステム

AVG 9 Internet Security 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 2000 Professional SP4 + Update Rollup 1
- 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)

注意：*ID 保護コンポーネントは Windows 2000 および 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 システムには、AVG 9 Internet Security をインストールできますが、IDP 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 9 Internet Security の最低ハードウェア要件:

- Intel Pentium CPU 1,5 GHz
- 512 MB の RAM メモリ
- ハードディスク空き容量 390MB以上 (インストールのため)

AVG 9 Internet Security の推奨ハードウェア要件:

- Intel Pentium CPU 1,8 GHz
- 512 MB の RAM メモリ

- ハードディスク空き容量 510MB以上（インストールのため）

3. AVGインストールオプション

AVG はインストール CD にあるインストールファイルからあるいは AVG ウェブサイト (http://www.avg.com/) から最新のインストール ファイルをダウンロードしてインストールできます。

AVGのインストールを開始する前に、AVGのウェブサイト (http://www.avg.com/) で最新のインストールファイルを確認することを強く推奨します。このような手順によって、確実に利用可能な最新バージョンの AVG 9 Internet Security をインストールできます。

目的の言語でインストール ファイルをセットアップできるように、最新の AVG ダウンロード マネージャ ツールを使用することをお勧めします。

インストールプロセス中に、ライセンス番号/セールス番号が必要となります。インストールを開始する前にライセンス番号/セールス番号を準備してください。セールス番号はCDのパッケージ、購入時のメール中等に記載されています。AVGをオンラインで購入した場合、ライセンス番号/セールス番号はメールで送信されます。

4. AVG ダウンロードマネージャー

AVG Download Manager はシンプルなツールで、AVG 製品の試用版用の正しいインストールファイルを簡単に選択できます。入力されたデータに基づいて、マネージャーは特定の製品、ライセンス種別、必要なコンポーネント、言語を選択します。最後に、**AVG Download Manager** はダウンロードに進み、適切なインストール プロセスを起動します。

警告: *AVG Download Manager は、ネットワーク版および SBS 版のダウンロードには適していません。サポートされているオペレーティングシステムは、Windows 4 (f + SRP ロールアップ)、Windows XP、Windows Vista、Windows 7 のみです。*

AVG Download Manager は AVG のウェブサイト (http://www.avg.com/) でダウンロードできます。**AVG Download Manager で必要な各ステップを簡単な説明は以下を参照してください。**

4.1. 言語選択

AVG Download Manager のこの最初のステップでは、ロールダウンメニューからインストール言語を選択します。注意 :言語選択はインストールプロセスにのみ適用されます。インストール後は、プログラム設定から直接言語を変更できます。[**次へ**] ボタンを押して継続します。

4.2. 接続性チェック

このステップで、**AVG Download Manager は、アップデートを検索できるようにインターネット接続の確立を試みます。AVG Download Manager** が接続性テストを完了するまでは、ダウンロード処理を進めることはできません。

- テストで接続がないことが示された場合、本当にインターネットに接続していることを確認してください。次に、[***再試行***] ボタンをクリックします。

- プロキシ接続でインターネットに接続している場合、[***プロキシ設定***] ボタンをクリックして、プロキシ情報を指定します。

- 確認できたら、[***次へ***] ボタンをクリックして続行します。

4.3. プロキシ設定

AVG Download Manager がプロキシ設定を特定できなかった場合は、手動で指定する必要があります。以下のデータを入力してください。

- ***サーバー*** - 有効なプロキシサーバー名または IP アドレスを入力します
- ***ポート*** - 各ポート番号を入力します。
- ***プロキシ認証を使用*** - プロキシサーバーが認証を必要とする場合はこのチェックボックスにチェックを付けます。
- ***認証を選択*** - ドロップダウンメニューから認証タイプを選択します。既定値を保持することを強くお勧めします（*こうするとプロキシサーバーは自動的に要件を通知します*）。ただし、上級者ユーザーの場合、[基本]（*一部のサーバーで必要*）または [NTLM]（*すべての ISA サーバーで必要*）オプションを選択することもできます。次に、有効な***ユーザー名***と***パスワード***（任意）を入力します。

[***適用***] ボタンをクリックして設定を確定し、**AVG Download Manager** の次のステップに進みます。

4.4. インストールするファイルをダウンロード

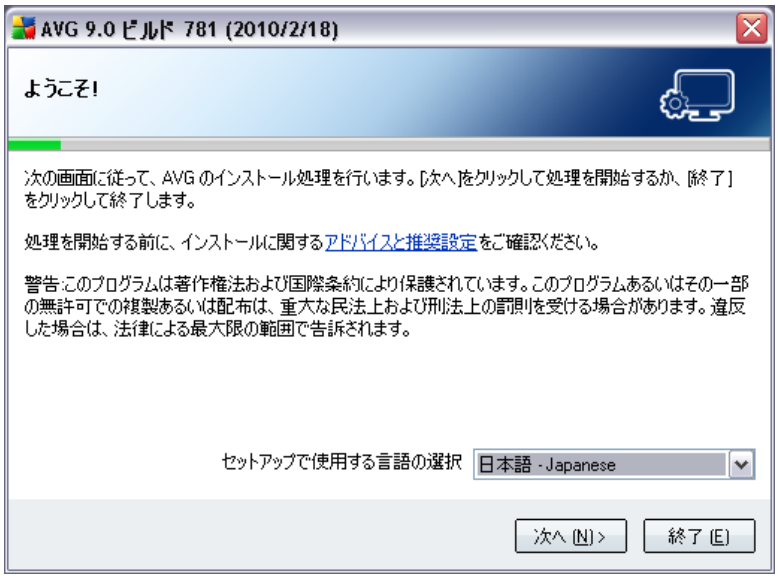
これで、**AVG Download Manager** でインストール パッケージのダウンロードを開始し、インストール処理を起動するために必要なすべての情報を入力しました。次に、AVG インストール処理に進んでください。

5. AVGインストールプロセス

コンピュータに**AVG 9 Internet Security** 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。パッケージ版内のCDからインストールファイルを使用できますが、このファイルは古い場合があります。したがって、最新のインストールファイルをオンラインで入手することを推奨します。AVG ウェブサイト (http://www.avg.com/) の***サポート センター/ ダウンロード*** セクションからファイルをダウンロードできます。あるいは、必要なインストールパッケージの作成およびダウンロードとインストールプロセスの起動を支援する新しい ***AVG Download Manager*** ツールを利用できます。

インストールは、各ステップの簡潔な操作を記載した一連のダイアログで構成されます。以下は、各ダイアログの説明です。

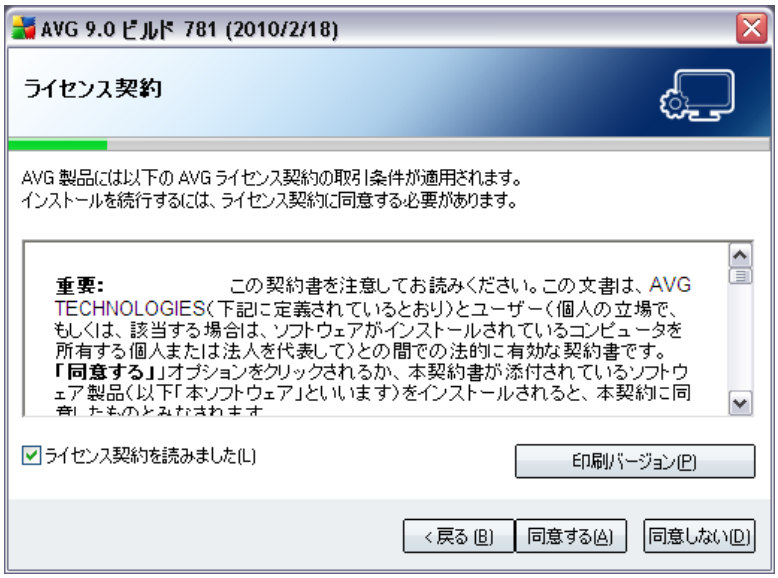
5.1. インストールの実行



インストールプロセスは、***AVG セットアッププログラムへようこそ***ウィンドウから開始します。ここで、インストールに使用される言語を選択します。ダイアログの下部に、***セットアップ言語の選択*** メニューが表示されます。ドロップダウンメニューから希望する言語を選択します。***次へ***ボタンを押し、次のダイアログへ進みます。

注意：*ここで選択する言語はインストールプロセスでのみ使用されます。AVGアプリケーションの言語を選択しているわけではありません。 - AVGアプリケーションの言語は、以後のインストールプロセス中で指定することができます。*

5.2. ライセンス契約



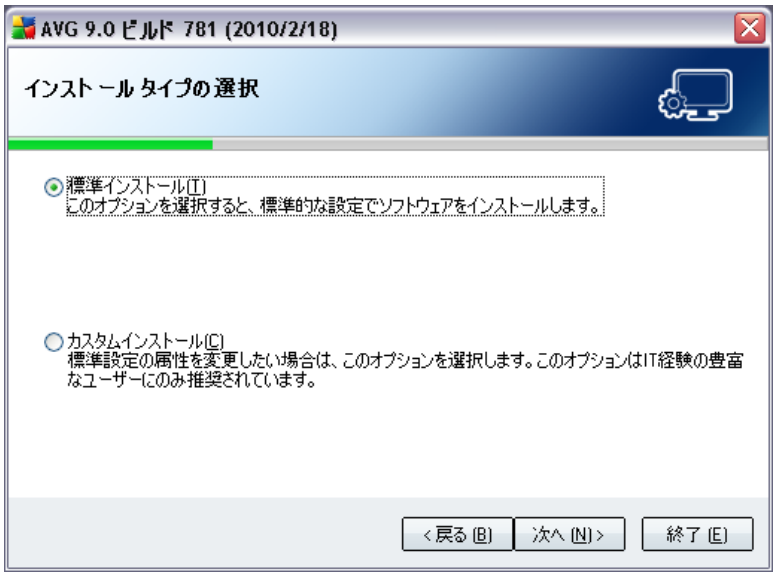
ライセンス契約ダイアログは、AVGライセンス契約の全文を提供します。契約内容をよく読んで、[***ライセンス契約を読みました***] チェックボックスにチェックを付け、[***同意する***] ボタンをクリックして、契約を読んで理解して同意することを確認します。

ライセンス契約に同意しない場合、***同意しない***ボタンを押してください。インストールプロセスがすぐに中断されます。

5.3. システムステータスのチェック

ライセンス使用許諾を確認したため、[***システムステータスの確認***] ダイアログにリダイレクトします。このダイアログでは一切の作業は必要ありません。AVGのインストール前にシステムがチェックされます。プロセスが終了するまでお待ちください。その後、自動的に次のダイアログが表示されます。

5.4. インストールタイプの選択



インストールタイプの選択ダイアログでは、2つのインストールオプションが提供されます。***標準***と***カスタム***インストールです。

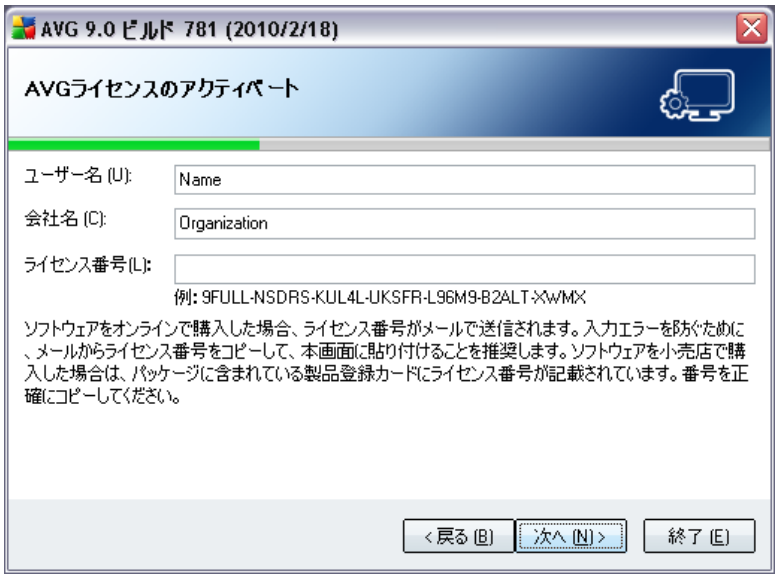
ほとんどのユーザーには、***標準インストール***を選択し、AVGを自動モードでインストールすることが強く推奨されます。この設定は、最適なリソース消費と最大のセキュリティを提供します。将来的に設定の変更の必要が生じた場合、常にAVGアプリケーションで直接変更することができます。

カスタムインストールは、AVGを標準設定でインストールしない正当な理由のある場合、経験のあるユーザーのみが行ってください（例：特定のシステムへの適合）。

5.5. AVG ライセンスをアクティベート

AVG ライセンスのアクティベートダイアログでは、登録データを入力する必要があります。名前（***ユーザー名***フィールド）と組織名（***会社名***フィールド）を入力します。

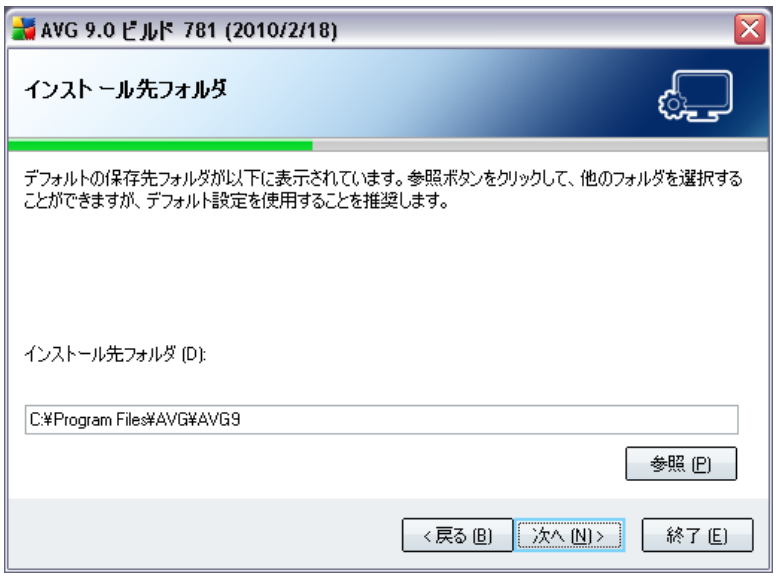
次に、ライセンス番号/セールス番号を***ライセンス番号***テキストフィールドに入力します。セールス番号は、**AVG 9 Internet Security** ボックスの CD パッケージに記載されています。ライセンス番号は**AVG 9 Internet Security**をオンラインで購入後に受信する確認メールに記載されています。この番号を記載通り正確に入力してください。デジタル形式のライセンス番号が利用できる（*メールで*）場合は、コピーとペーストを使用して、それを入力することを推奨します。



次へボタンをクリックし、インストールプロセスを継続します。

以前のステップで、標準インストールを選択した場合は、直接 [*AVG セキュリティツールバー*] ***ダイアログにリダイレクトされます。*** カスタムインストールが選択された場合は、***対象フォルダ***ダイアログに進みます。

5.6. カスタムインストール - インストール先フォルダ

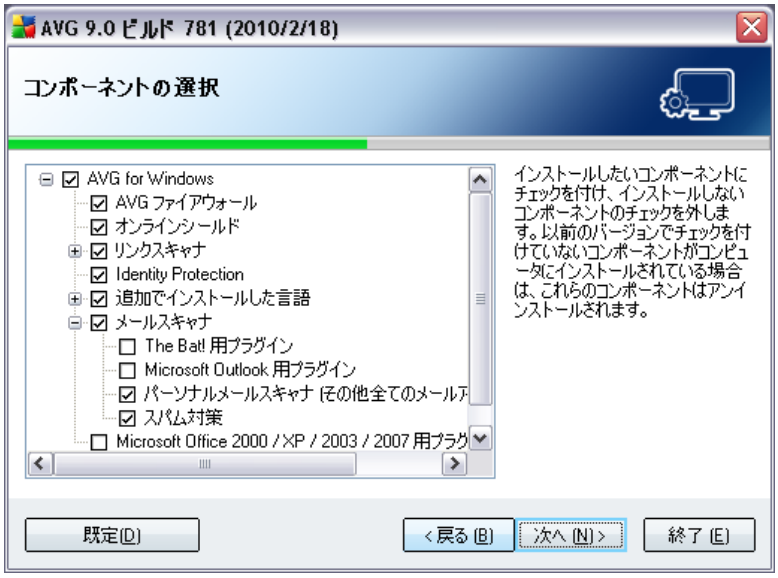


[***インストール先 フォルダ***] ダイアログでは、**AVG 9 Internet Security** をインストールする場所を指定できます。デフォルトでは、AVGは、Cドライブのprogram filesフォルダにインストールされます。フォルダがまだ存在しない場合、新しいダイアログが開き、今すぐAVGによってこのフォルダを作成してもよいかどうかを確認します。

この場所を変更する場合は、[***参照***] ボタンを使用してドライブ構成を表示し、対象フォルダを選択します。

次へボタンを押して確認します。

5.7. カスタムインストール - コンポーネントの選択



[***コンポーネント選択***] ダイアログには、インストール可能なすべての **AVG 9 Internet Security** コンポーネントの概要が表示されます。デフォルト設定が適当でない場合、特定のコンポーネントを削除/追加することができます。

ただし、購入したAVGに含まれるコンポーネントのみを選択することができます。コンポーネント選択ダイアログでは、これらのコンポーネントのみをインストール可能です。

- ***言語選択***

  インストールするコンポーネント内で、AVG のインストールで使用する言語を定義することができます。***追加でインストールする言語***をチェックし、希望の言語を選択します。

- ***メールスキャナプラグイン***

[***メールスキャナ***] アイテムをクリックして開き、メールのセキュリティを保証するためにインストールするプラグインを決定します。既定では、***Plugin for Microsoft Outlook*** がインストールされます。購入したライセンスに***スパム対策***が含まれる場合、スパム対策もインストールされます。その他の特定のオプションとしては、***Plugin for The Bat! があります。***その他のメールクライアント（*MS Exchange*、*Qualcomm Eudora*、...）を使用している場合は、[***パーソナルメールスキャナ***] オプションに進み、実行されるメールプログラムに関係なく自動的にメール通信の安全を保証してください。

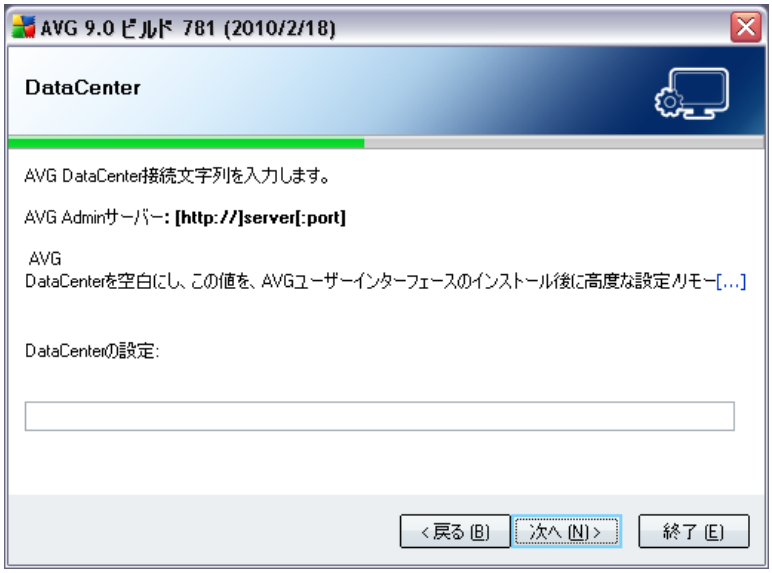
- ***リモート管理***

  後から AVG Remote Administration にコンピュータを接続する場合、各インストール対象アイテムにもマークを付けてください。

次へボタンを押して継続します。

5.8. AVG DataCenter

AVG ネットワークライセンスを使用し、前の [***カスタム インストール - コンポーネント選択***] ダイアログで、[***遠隔管理***] アイテムのインストールを選択した場合、***AVG DataCenter*** パラメータを指定する必要があります。



[***AVG DataCenter 指定***] テキストフィールドに、***AVG DataCenter*** への接続文字列を *サーバー:ポート* の形式で入力してください。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。

注意：*AVG Remote administration の詳細については、AVG Network Edition ユーザーマニュア*

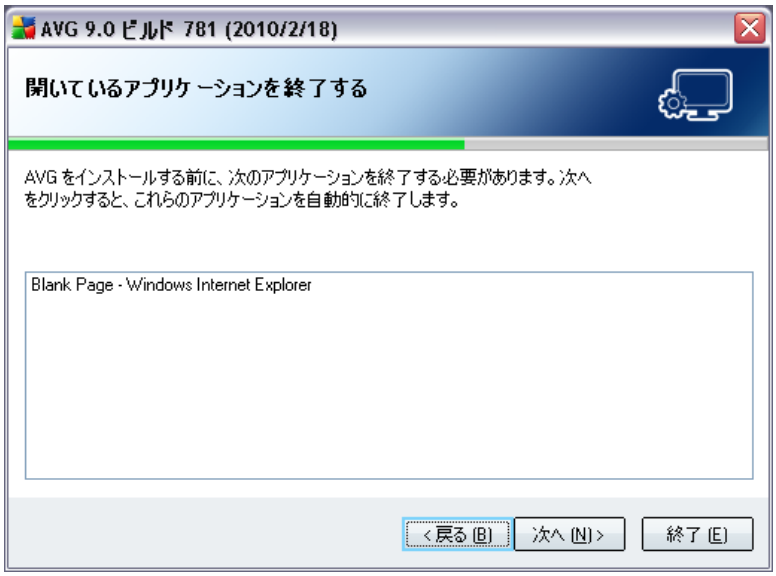
ルを参照してください。このマニュアルは、AVG ウェブサイト (http://www.avg.com/) からダウンロードできます。

5.9. AVGセキュリティツールバー

[***AVG セキュリティツールバー***] ダイアログでは、***AVG セキュリティツールバー***(*サポートされているインターネット検索エンジンによる検索結果の検証*) をインストールするかどうかを決定します。デフォルト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. 2.0 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、デフォルト検索プロバイダとしてYahoo! を選択するかどうかを決定するオプションがあります。この場合は、該当するチェックボックスにマークを付けてください。

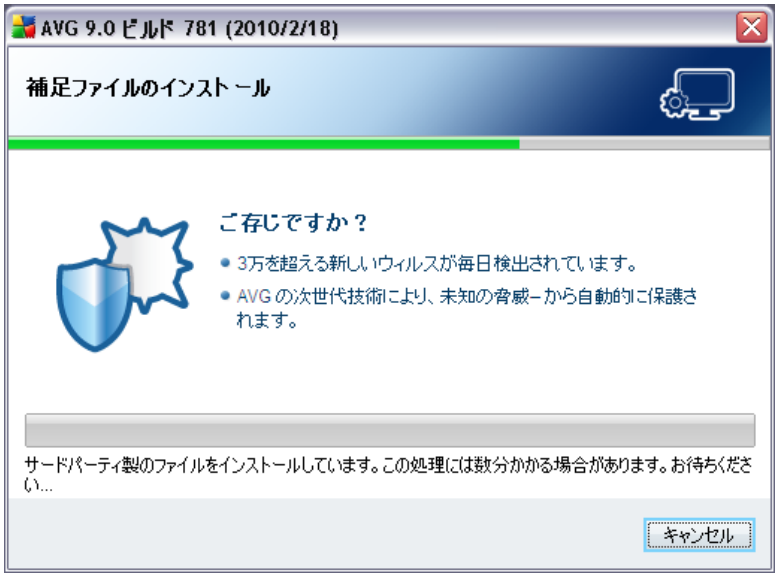
5.10. 開いているアプリケーションを終了する



インストール時点でコンピュータで実行中の他のプログラムが競合する場合にのみ、[***開いているアプリケーションを閉じる***] ダイアログがインストール処理中に表示されます。次に、インストール処理を正常終了させるために終了する必要のあるプログラムのリストが表示されます。[***次へ***] ボタンをクリックして、各アプリケーションを終了することに同意し、次のステップに進みます。

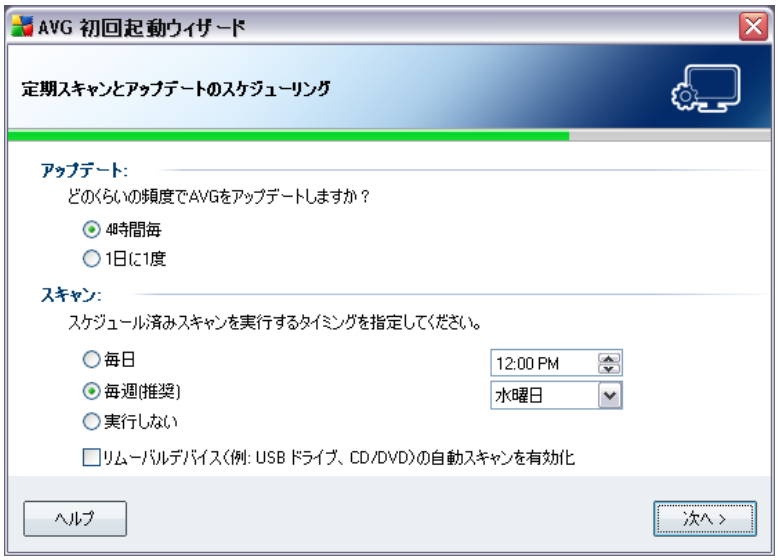
5.11. AVGのインストール

[***AVG のインストール***] ダイアログは、インストールプロセスの進捗を表示し、ユーザーの操作は必要としません。



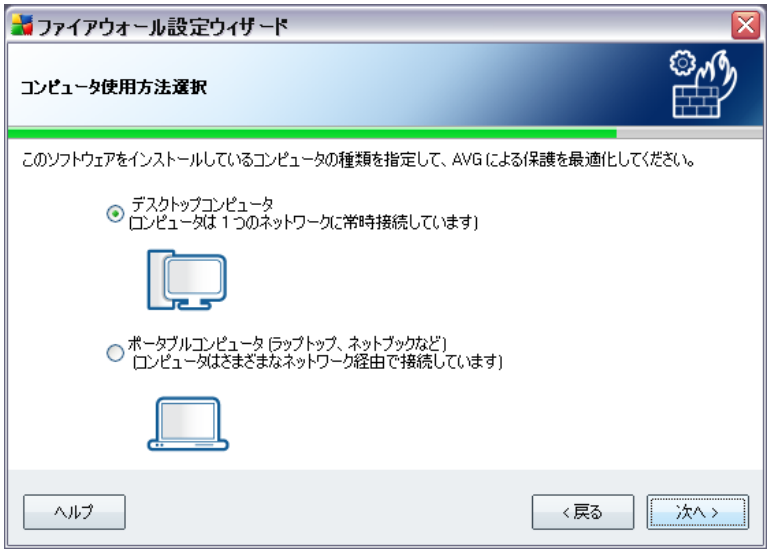
インストールプロセスの終了後、自動的に次のダイアログに進みます。

5.12. 定期スキャンとアップデートのスケジューリング



定期スキャンとアップデートのスケジューリングダイアログでは、アップデートファイルのアクセシビリティチェックの間隔と、スケジュール済スキャンの実行時間を設定します。デフォルト値を保持することを推奨します。***次へ***ボタンを押して継続します。

5.13. コンピュータ使用方法選択



このダイアログでは、***ファイアウォール設定ウィザード***が使用しているコンピュータの種類を確認します。例えば、多くの異なる場所（*空港、ホテルの部屋等*）からインターネットに接続するノートブックコンピュータはドメイン（*会社のネットワーク等*）内のコンピュータよりも*厳密なセキュリティルールを必要とします。*). ***ファイアウォール***のデフォルトルールは、選択されたコンピュータの使用タイプに基づいて異なったセキュリティレベルで定義されます。

2 つの代替オプションから選択できます。

- ***デスクトップコンピュータ***
- ***ポータブルコンピュータ***

次へボタンを押して、次のダイアログへ進みます。

5.14. コンピュータインターネット接続

このダイアログでは、インターネットに接続する方法を指定します。***ファイアウォール***のデフォルトルールは、選択された接続タイプに基づいて異なったセキュリティレベルで定義されます。

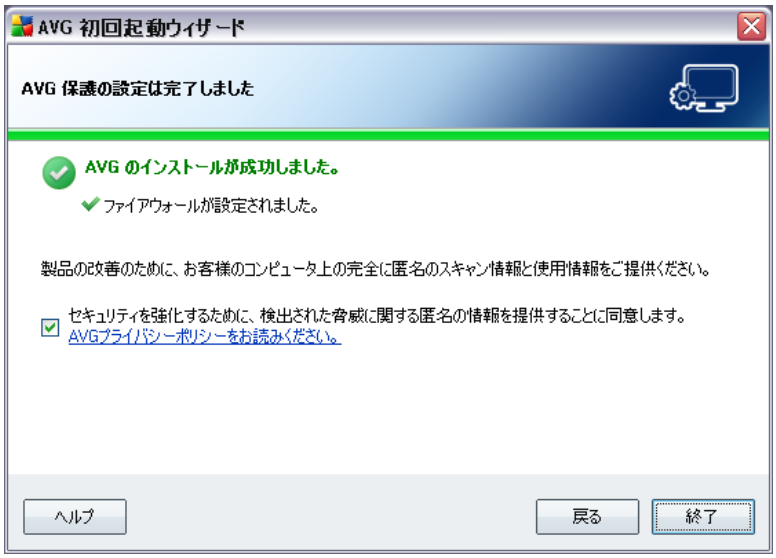
3 つの代替オプションから選択できます。

- ***モデム経由で直接***
- ***有線または無線ルーター直接***
- ***ドメインの一部***

コンピュータのインターネット接続方法に最も近い接続タイプを選択します。

次へボタンを押して、次のダイアログへ進みます。

5.15. AVG 保護設定は完了しています



AVG 9 Internet Security が構成されました。

このダイアログでは、AVG ウィルスラボへのエクスプロイトと悪意のあるサイトの匿名レポートのオプションを有効にするかどうかを決定します。有効にする場合、[***セキュリティ向上のために検出した脅威の情報を匿名で提供します***] オプションにチェックする。

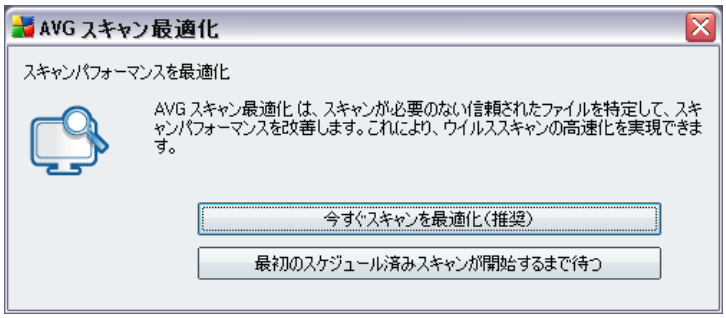
最後に、[***完了***] ボタンをクリックします。AVG を起動するには、コンピュータの再起動が必要な場合があります。

6. インストール後

6.1. スキャン最適化

スキャン最適化機能は、該当するファイルを検出する *Windows* と *Program files* フォルダを検索し(*現時点では、*.exe、*.dll、*.sys ファイル*)、これらのファイルの情報を保存します。次回のアクセス時には、これらのファイルは再度スキャンされず、これによって、スキャン時間が大幅に短縮されます。

インストール処理が完了すると、スキャンを最適化するための新しいダイアログ ウィンドウが表示されます。



[***今すぐスキャンを最適化k***] ボタンをクリックして、このオプションを使用し、スキャン最適化処理を実行することをお勧めします。

6.2. 製品登録

AVG 9 Internet Security インストールが終了したら、AVG Webサイト (http://www.avg.com/)、[***登録***] ページ(*製品のオンライン登録を行ってください 画面上の指示にしたがってください*)。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。

6.3. ユーザーインターフェースへのアクセス

AVGユーザーインターフェースには複数の方法でアクセスできます。

- システムトレイのAVGアイコンをダブルクリックします。
- デスクトップのAVGアイコンをダブルクリックします。
- メニューから***スタート/ すべてのプログラム/ AVG 9.0/ AVGユーザーインターフェース を選択します。***

6.4. 全コンピュータをスキャン

AVG 9 Internet Security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。

6.5. Eicarテスト

AVG 9 Internet Security 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後すぐに、***オンライン シールド***が警告とともにそれに反応します。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***によって、このファイルをダウンロードし、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***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。**

6.6. AVGデフォルト設定

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 9 Internet Security** 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。

7. AVG ユーザーインターフェース

AVG 9 Internet Security はメイン ウィンドウで開 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、すべてのAVGコンポーネント、サービス、機能にアクセスすることができます。 - 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、現在のAVGプログラムの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タスクにすぐにアクセスすることができます。 - 詳細 >>

- ***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コンポーネントの概要が表示されます。 - 詳細 >>
- ***統計*** *(ウィンドウ左下部)* では、プログラムに関する統計データが表示されます。- 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)* では、現在のAVGステータスが表示されます。 - 詳細 >>

7.1. 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 9 Internet Security** 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。

7.1.1. ファイル

- ***終了*** - **AVG 9 Internet Security**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。

7.1.2. 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含まれ、選択すると各デフォルト 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*** - ***ウイルス対策*** コンポーネントのデフォルトページを表示します。
- ***ルートキット対策*** - ***ルートキット対策*** コンポーネントのデフォルトページを表示します。
- ***スパイウェア対策*** - ***スパイウェア対策*** コンポーネントのデフォルトページを表示します。
- ***ファイアウォール*** - ***ファイアウォール*** コンポーネントのデフォルト ページを表示します。
- ***リンク スキャナ*** - ***リンク スキャナ*** コンポーネントのデフォルト ページを表示します。
- ***システム ツール*** - ***システム ツールのデフォルト ページを表示します。***
- ***スパム対策*** - ***スパム対策*** コンポーネントのデフォルト ページを表示します。
- ***メールスキャナ*** - ***メールスキャナ*** コンポーネントのデフォルト ページを表示します。

- ***ID 保護*** - ***ID 保護***コンポーネントのデフォルト ページを開 きます。
- ***ライセンス***- ***ライセンス***コンポーネントのデフォルト ページを表 示 します。
- ***オンライン シールド*** - ***オンライン シールド***コンポーネントのデフォルト ページを開 きます。
- ***常駐 シールド*** - ***常駐 シールド***コンポーネントのデフォルトページを表 示 します。
- ***アップデート*** - ***アップデートマネージャ***コンポーネントのデフォルトページを表 示 します。

7.1.3. 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 スキャナ***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*** - ***オンライン シールド***
- ***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 障 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*** - **AVG 9 Internet Security すべてのログに記 録 された**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。

7.1.4. 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 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 にアップデートプロセスを実 行 します。**AVG 9 Internet Security**
- ***ディレクトリからのアップデート*** - ローカルディスクの指 定 フォルダ内 のアップデートファイルから

アップデートプロセスを実行します。ただし、このオプションは緊急時にのみ推奨されます。例えば、インターネット接続がない場合（*例えば、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。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等*）．フォルダの参照ウィンドウで、アップデートファイルを保存したフォルダを選択し、アップデートプロセスを実行します。

- ***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 9 Internet Security**各項目の設定を編集できます。通常、定義済みのデフォルト設定を使用してください。
- ***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。

7.1.5. ヘルプ

- ***目次*** - AVGヘルプファイルを開きます。
- ***オンラインヘルプ*** - AVG Free Webサイトのカスタマーサポートセンターページを開きます（http://www.avg.com/）。
- ***AVG Web*** - AVG ウェブサイト（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***を開きます。ここでは、特定されたウイルスに関する詳細情報を検索することができます。
- ***再アクティベート*** - ***インストールプロセス***の［***AVG のパーソナライズ***］ダイアログで入力したデータとともに、［AVG のアクティベート］ダイアログが表示されます。このダイアログ内では、ライセンス番号を入力し、セールス番号（*AVGをインストールした際の番号*）を置き換えるか、古いライセンス番号（*例えば、新しいAVG製品にアップグレードした場合*）を置き換えることができます。
- ***今すぐ登録*** - AVG ウェブサイト（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受けることができます。

注意： ***AVG 9 Internet Security*** *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 9 Internet Security** *の場合、［****登録****］および［****アクティベート****］として表示されます。詳細については、このマニュアルの「ライセンス」を参照してください。*

- ***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***の連絡先情報を確認することができます。

7.2. 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 9 Internet Security**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つあるいは複数のコンポーネントが間違って設定され、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。コンピュータはAVGによって保護されています。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。

このアイコンは、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にした場合にも表示されます（*コンポーネント状態を無視]オプションはAVGメインウィンドウのコンポーネント概要にある該当するコンポーネントアイコンを右クリックすると開くコンテキストメニューで利用できます*）。特定の場合にこのオプションを使用する必要があるかもしれませんが、[***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。

 赤のアイコンは AVG が重大な状況にあることを示しています。1つあるいは複数のコンポーネントが適切に動作しておらず、AVGが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。

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。

注意：*AVG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。*

7.3. クイックリンク

クイックリンク(*AVGユーザーインターフェースの左側のセクション*)では、最も重要で、最も頻繁に使用されるAVG機能に直接アクセスできます。

- ***概要***- このリンクをクリックすると、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デフォルトインターフェースへ切り替わります- ***コンポーネント概要の章を参照 >>***
- ***コンピュータスキャナ***- このリンクをクリックすると、AVG スキャンインターフェースが表示されます。ここでは、直接スキャンを実行したり、スキャンをスケジュールしたり、パラメータを編集することができます - ***AVG スキャンの章を参照 >>***
- ***すぐにアップデート*** - このリンクはアップデートインターフェースを開き、AVGアップデートプロセスを実行します。- ***AVG アップデートの章を参照 >>***

これらのリンクは、ユーザーインターフェースから使用することができます。一度、クイックリンクを使用して特定のプロセスを実行すると、GUI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、よりグラフィカルに表示されます。

7.4. コンポーネント概要

[***コンポーネント概要***] セクションはAVG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つの箇所にわかれています。

- コンポーネントアイコン表示によるインストール済みコンポーネントの概要と、各コンポーネントの有効/無効を示す情報
- 選択されたコンポーネントの説明

AVG 9 Internet Security 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、コンピュータに侵入しようとするウイルスからコンピュータを確実に保護します。- 詳細>>
- ***スパイウェア対策***は、アプリケーションが実行されるときに、バックグラウンドでアプリケーションを

スキャンします。- 詳細>>

- ***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として判定します。 - 詳細>>
- ***ファイアウォールは、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。*** - 詳細>>
- ***リンクスキャナ***は、インターネットブラウザに表示される検索結果をチェックします - 詳細>>
- ***ルートキット対策***はマルウェアを隠そうとするプログラムと技術を検出します。- 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 >>
- ***メールスキャナ***は、すべての送受信メールのウイルスチェックを行います。 - 詳細>>
- ***ID 保護*** - ID 窃盗による個人デジタル資産の盗難防止に特化したマルウェア対策コンポーネント - 詳細 >>
- ***ライセンス***には、ライセンス番号、種類、有効期限が表示されます - 詳細 >>
- ***オンライン シールド***は、ウェブ ブラウザからダウンロードされるすべてのデータをスキャンします - 詳細>>
- ***常駐シールド***は、バックグラウンドで実行され、ファイルがコピーされたり、開かれたり、保存される際にそのファイルをスキャンします。 - 詳細>>
- ***アップデートマネージャ***は、すべてのAVGアップデートをコントロールします。 - 詳細>>

いずれかのコンポーネントアイコンをシングルクリックすると、コンポーネントが選択されます。同時に、ユーザーインターフェースの下部にコンポーネントの基本機能説明が表示されます。アイコンをダブルクリックすると、コンポーネントのインターフェースが表示されます。

コンポーネントのアイコン上でマウスを右クリックし、コンテキストメニューを展開します。コンポーネントのグラフィックインターフェースを開く以外にも、***コンポーネント状態を無視***することを選択できます。このオプションを選択して、コンポーネントのエラー状態を認識していると示しますが、何らかの理由で、システム トレイ アイコンによる警告を表示したくない場合は、AVG をそのままに保つことができます。

7.5. 統計

AVGユーザーインターフェースの左下部には[統計] セクションがあります。これはプログラム操作に関する情報のリストを提供します。

- ***最終スキャン*** - 最後にスキャンが実行された日付を表示します
- ***最終更新*** - 最後の更新が起動した日付を表示します。
- ***ウイルスDB*** - 現在インストール済みのウイルスデータベースのバージョンを表示します。
- ***AVGバージョン*** - インストール済みのAVGのバージョンを表示します *(番号は、9.0.xxの形式で表示され、9.0は製品ラインバージョンであり、xxはビルド番号を表します)*
- ***ライセンス有効期限*** - AVGライセンスの有効期限を表示します。

7.6. システムトレイアイコン

システム トレイ アイコン *(Windows タスクバー上)* は、**AVG 9 Internet Security** の現在の状態を示します。このアイコンは、AVG のメインウィンドウ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。

全色の場合 、***システム トレイ アイコン***はすべての AVG コンポーネントが有効であり、完全に機能していることを意味します。また、AVG システムトレイアイコンは、AVG がエラー状態にある場合にも全色で表示されますが、ユーザーはこの状況を完全に認識しており、慎重に***コンポーネント状態を無視***することを決定しています。

アイコンとエクスクラメーション マーク は、問題を示します (*非アクティブなコンポーネント、エラー状態など*)。 ***システムトレイアイコン***をダブルクリックして、メインウィンドウを開き、コンポーネントを編集します。

さらに、システム トレイ アイコンは、現在の AVG 活動とプログラム内で起こりうるステータス変更を通知します (*スケジュールされたスキャンまたはアップデートの自動起動、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*)。これは、AVG 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。

システムトレイアイコンはまた、クイックリンクとしても使用され、アイコンをダブルクリックすることでAVGメインウィンドウにいつでもアクセスできます。***システムトレイアイコン***を右クリックすると、以下のオプション

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ユーザーインターフェースが表示されます。
- ***アップデート*** - すぐにアップデートを起動します。

8. AVGコンポーネント

8.1. ウイルス対策

8.1.1. ウイルス対策 原理

ウイルス対策ソフトウェアのスキャンエンジンは、既知のウイルスに対して、すべてのファイルとその活動（ファイルオープン/クローズ等）をスキャンします検出されたウイルスは動作をブロックされ、除去、または隔離されます。大部分のウイルス対策ソフトウェアは、ヒューリスティックスキャンも使用します。これによりファイルは一般的なウイルスの特性、つまりウイルスシグネチャ、に基づいてスキャンされます。これは、新種のウイルスが既存のウイルス特性を含む場合、未知のウイルスであっても検出可能であることを意味します。

ウイルス対策の重要な機能は、既知のウイルスはコンピュータで実行されないということです。

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。

- スキャン- ウイルス特性文字列のスキャン
- 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ーレーション
- 一般検出 - ウイルス/ウイルスグループの命令特性の検出

AVGはまた、不審な実行可能アプリケーションやDLLライブラリを分析、検出することができます。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、アドウェア等）。さらに、AVGは疑わしいエントリ、インターネット一時ファイル、tracking cookiesに対しシステムレジストリをスキャンし、潜在的に有害なアイテムを他の感染と同様に処理することができます。

8.1.2. 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は、一部の基本的なコンポーネントの機能に関する情報、コンポーネントの現在のステータスに関する情報 (*ウイルス対策 コンポーネントがアクティブです等*)、簡単な ***ウイルス対策*** 統計の概要が表示されます。

- ***ウイルス定義数*** - 番号はウイルスデータベースの最新バージョンで定義されているウイルス数です。
- ***最新データベース更新*** - ウイルスデータベースが最後にアップデートされた日時を指定します。
- ***データベースバージョン*** - 最新のウイルスデータベースバージョン番号が表示されます。この番号はウイルスアップデートごとに変更されます。

コンポーネントのインターフェースで利用できる操作ボタンは1つです (***戻る***)。- このボタンを押すと、デフォルトの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。

注意：*すべてのAVGコンポーネントは、最適なパフォーマンスを提供す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、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は、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設定を編集します。*

8.2. スパイウェア対策

8.2.1. スパイウェア対策 原理

スパイウェアは、通常、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するようなマルウェアの一種として定義されます。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。メールを介してのワーム、ウイルスの送信といったその他の感染方法も広まっています。常にバックグラウンドスキャンをオンにして、***スパイウェア対策***を使用することが重要です。これは常駐シールドのように機能し、アプリケーションを実行する際にそれをバックグラウンドでスキャンします。

また、マルウェアがAVGをインストールする前にコンピュータに送信されたり、あるいは、最新の**AVG 9 Internet Security**データベースを維持し、プログラムのアップデートを行わなかったという潜在的なリスクもありますこのため、AVGでは、スキャン機能を使用して、マルウェアやスパイウェアを検出することができるようになっています。また、休止中で、アクティブではないマルウェアも検出します。例えば、ダウンロードされ、またアクティブ化されていないマルウェアも検出されます。

8.2.2. スパイウェア対策インターフェース

スパイウェア対策コンポーネントのインターフェースは、基本的なコンポーネントの機能、コンポーネントの現在のステータス(*スパイウェア対策コンポーネントがアクティブです。等*)、***スパイウェア対策***統計に関する情報が表示されます。

- ***スパイウェア定義数*** - 最新のスパイウェアデータベースバージョンで定義されたスパイウェアサンプルの数が表示されます。
- ***最終データベース更新*** - スパイウェアデータベースが最後にアップデートされた日時が表示されます。
- ***データベースバージョン*** - 最新のスパイウェアデータベースバージョン番号が表示されます。この番号はアップデートごとに増加します。

コンポーネントのインターフェースで利用できる操作ボタンは1つです(***戻る***)。- このボタンを押すと、デフォルトの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。

注意:*すべてのAVGコンポーネントは、最適なパフォーマンスを提供す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、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は、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設定を編集します。*

8.3. スパム対策

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。スパムは迷惑なだけでなく、しばしば詐欺、ウイルス、不快な内容を含んでいます。

8.3.1. スパム対策基本

AVG Anti-Spam 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 とマークします。***AVG Anti-Spam*** 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。

AVG Anti-Spam 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。AVG Anti-Spam コンポーネントは、スパム保護のため、定期的にアップデート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。

8.3.2. スパム対策インターフェース

スパム対策 コンポーネントダイアログでは、コンポーネントの機能を説明する簡潔なテキスト、現在のステータスに関する情報（*スパム対策 コンポーネントはアクティブです。*）、または以下の統計が表示されます。

- ***データベースリリース*** - スパムデータベースが更新、発行された日時を指定します。
- ***スパムキャッチャーバージョン*** - 最新のスパム対策エンジンのバージョンを表示します。

コンポーネントのインターフェースで利用できる操作ボタンは1つです（***戻る***）- このボタンをクリックすると、デフォルトの 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。

注意：*すべてのAVGコンポーネントは、最適なパフォーマンスを提供す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、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は、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設定を編集します。*

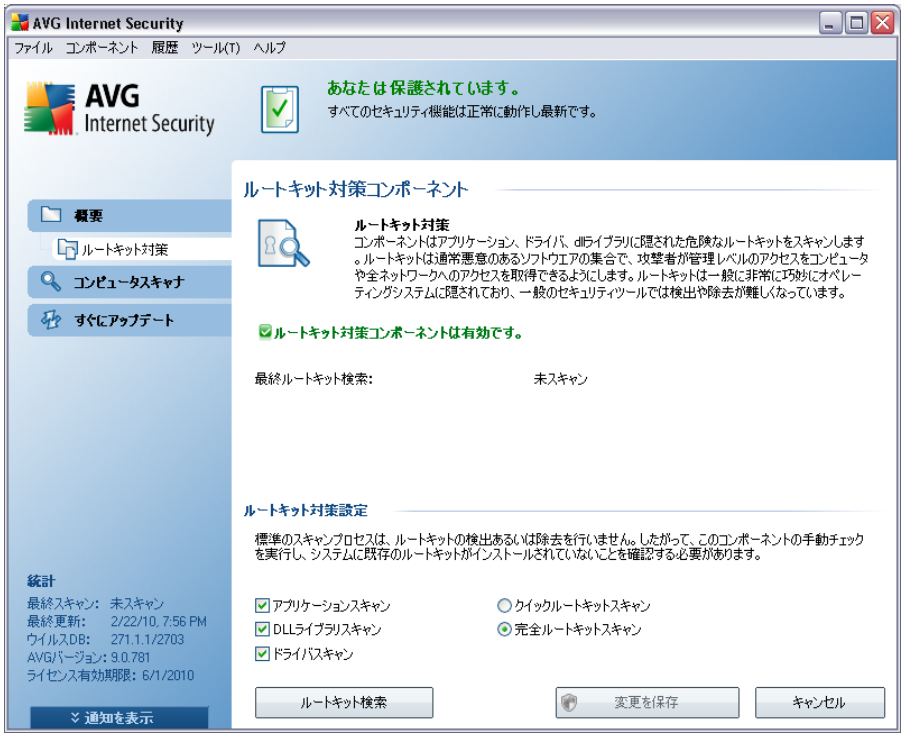
8.4. ルートキット対策

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しで、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のコントロールを掌握するよう意図されているため、ハードウェアへのアクセスはほとんど必要とされません。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で、システム上でその存在を隠すように動作します。一般的に、それは同時にトロイの木馬でもあり、システムで実行しても安全であるかのようにユーザーを騙し、信じこませます。これを実現させる技術によって、実行中のプロセスをプログラム監視から隠したり、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。

8.4.1. ルートキット対策 原理

AVG Anti-Rootkit 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の危険なルートキットを検出し、効果的に除去する特別なツールです。***AVG Anti-Rootkit*** 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*）。***AVG Anti-Rootkit*** 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。

8.4.2. ルートキット対策インターフェース



ルートキット対策ユーザーインターフェースは、コンポーネント機能の簡単な説明、コンポーネントの現在のステータス (*ルートキット対策 コンポーネントは有効です。等*)、***ルートキット対策***が実行された時間を表示します。

ダイアログの下部では、***ルートキット対策設定***セクションがあり、ここで基本的なルートキットスキャン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。

利用可能なコントロールボタン:

- ***ルートキットスキャン*** - ルートキットスキャンは***全 コンピュータをスキャン***に含まれていません。***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てして、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 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。

8.5. システムツール

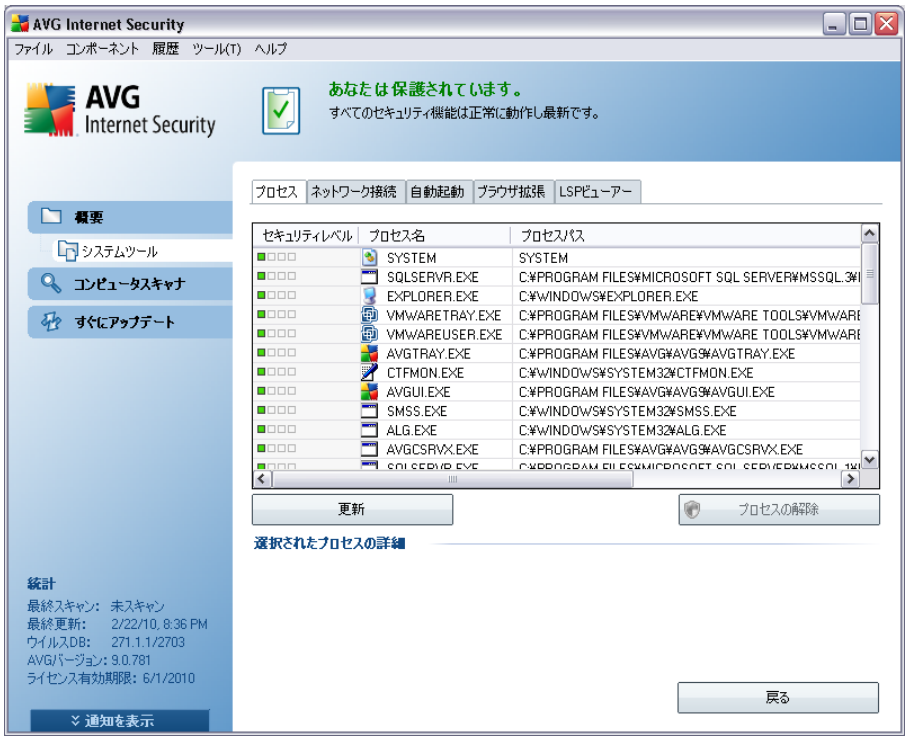
システム ツールとは、**AVG 9 Internet Security** 環境とオペレーティング システムの詳細サマリーを提供するツールのことです。コンポーネントには以下の概要が表示されます。

- プロセス - コンピュータ上で現在アクティブなプロセス (実行中のアプリケーション) のリスト
- 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 - インターネットブラウザにインストールするプラグイン（アプリケーション）のリスト
- LSP ビューア - レイヤードサービスプロバイダ（LSP）のリスト

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。

8.5.1. 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

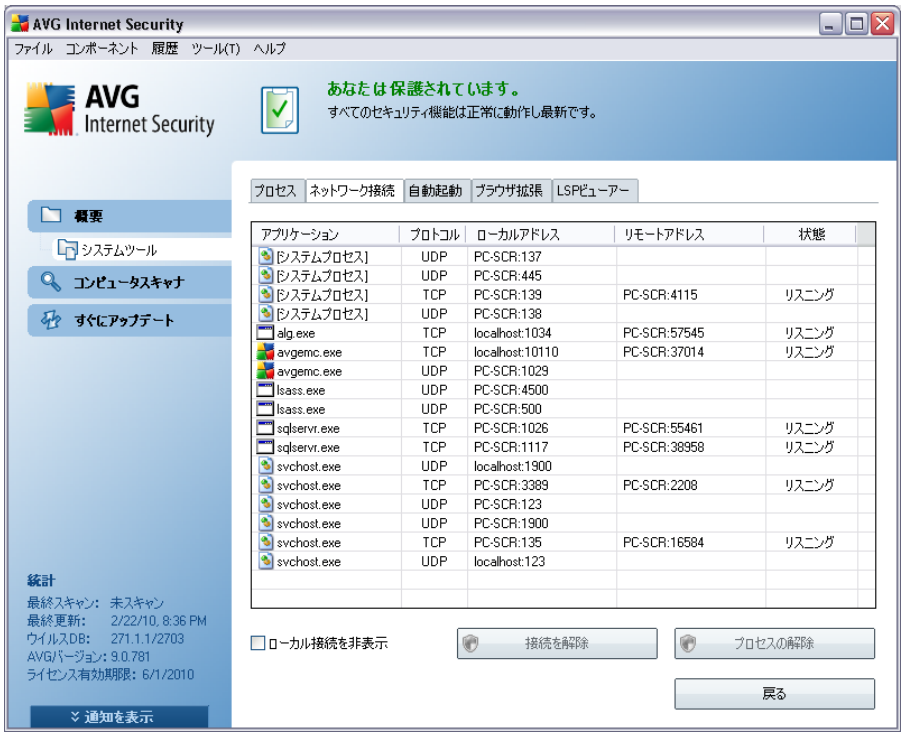
- ***ウィンドウ*** - アプリケーションウィンドウ名（存在する場合のみ）
- ***インターネット*** - 実行中のプロセスがインターネットにも接続しているかどうかを表示します（*はい*/*いいえ*）
- ***サービス*** - 実行中のプロセスがサービスであるかどうかを表示します（*はい*/*いいえ*）
- ***PID*** - 一意のWindows内部プロセス識別番号

コントロールボタン

システムツール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。

- ***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 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。

8.5.2. 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
  - 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
  - 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。

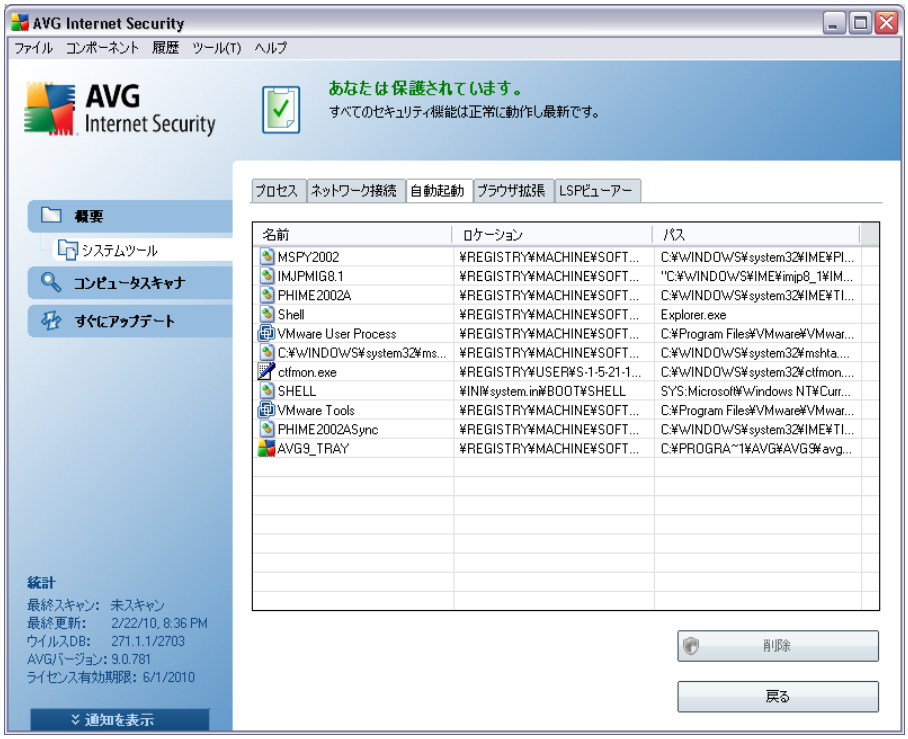
コントロールボタン

以下のコントロールボタンが利用可能です。

- ***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 ユーザーインターフェース*** (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。

8.5.3. 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。

1つ以上のエントリを選択し、***除去***ボタンを押すと、それを削除できます。*[*戻る] ボタンをクリックすると、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。

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。

8.5.4. 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 (*アプリケーション等*) 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

次のコントロールボタンを [***ブラウザ拡張***] タブで利用できます。

- ***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 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。

8.5.5. LSPビューアー

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。

リストにWindows LSPを含める場合は、***Windows LSPを非表示***チェックボックスのチェックを外します。[***戻る***] ボタンをクリックすると、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。

8.6. 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ルールセットを持っており、このルールは外部（一般的にはインターネットから）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を検出すると、その通信を「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。

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。*

8.6.1. ファイアウォール 原理

AVGでは、***ファイアウォール***コンポーネントは、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コントロールします。***ファイアウォール***は、定義されたルールに基づいて、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。デフォルトでは、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***ルールがない場合等）、***ファイアウォール***はその通信を許可するかブロックするかを確認します。

注意：*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。

8.6.2. 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、***ファイアウォール***保護がオフになった状態に近くなり、安全ポリシーとルールが適用されません *(つまり、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。

- ***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化されると、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***:

  - ***インターネットに直接接続*** - インターネットに直接接続する一般的なデスクトップ型家庭用コンピュータや安全な企業ネットワーク外のインターネットに接続するノート PC に適しています。家庭から接続している場合や、一元制御がない小規模企業ネットワークにいる場合に、このオプションを選択します。また、旅行中や、さまざまな不明で潜在的に危険な場所からノート PC で接続する場合にもこのオプションを選択します（*インターネットカフェ、ホテルの部屋など*）. これらのコンピュータは追加の保護がなく、それゆえ最大限の保護を必要としていると想定されるため、より制限されたルールが作成されます。

  - ***ドメイン内のコンピュータ***– 学校や会社のネットワーク等のローカルネットワーク内のコンピュータに適しています。ネットワークはいくつかの追加的な方法によって保護されていることが想定されるため、セキュリティレベルはスタンドアロンコンピュータよりも低い可能性があります。

  - ***ご家庭、または小規模オフィスのネットワーク***– 家庭や小規模ビジネスのコンピュータに適しています。一般的には数台のコンピュータのみが接続されており、一元管理者はいません。

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。

8.6.3. ファイアウォールインターフェース

ファイアウォールこのインターフェースでは、コンポーネントの機能に関する基本情報と***ファイアウォール***統計の基本概要が表示されます。

- 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

基本コンポーネント設定

- ***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を 1 つ選択します - *すべてを許可*、*すべてをブロック*の ***2 つのプロファイルは常に選択項目として表示されます***。他のプロファイルは [***ファイアウォール設定***] の [***プロファイル***] ダイアログで手動で追加されたものです。
- ***ゲームモードを有効化*** - このオプションにチェックを付けると、フル画面アプリケーション（ゲーム、PowerPoint プレゼンテーションなど）を実行する時に、***ファイアウォール***は不明なアプリケーションの通信を許可あるいはブロックするかどうかの確認ダイアログを表示しません。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は、***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。
- ***ファイアウォールステータス***:
  - ***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、すべての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されます。

注意：*すべてのAVGコンポーネントは、最適なパフォーマンスを提供す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、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

- ***設定ウィザード*** - このボタンをクリックすると、***コンピュータ使用状況選択***という各ダイアログ（*インストールプロセスで使用*）に切り替わります。ここでは、***ファイアウォール***コンポーネント設定を指定できます。

- ***変更を保存*** - このボタンを押すと、ダイアログで行われた変更を保存、適用します。
- ***キャンセル*** - このボタンを押すと、デフォルトの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

8.7. メールスキャナ

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。

8.7.1. メールスキャナ 原理

メールスキャナコンポーネントは、自動的に送受信メールをスキャンします。AVG にプラグインのないメールクライアント（*Outlook Express、Mozilla、Incredimail など*）で使用できます。).

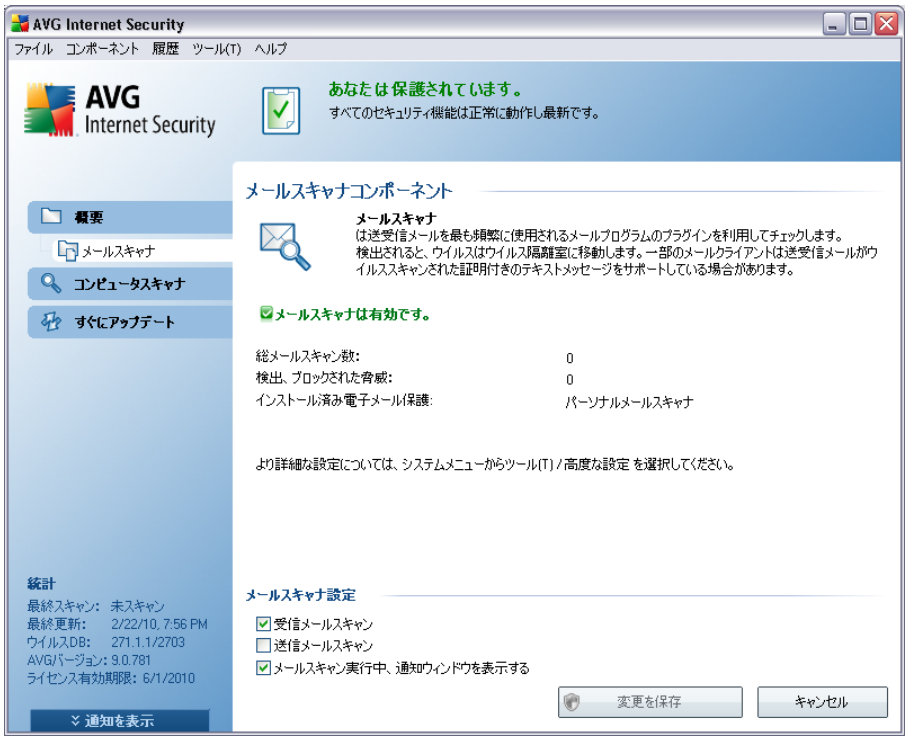
AVG インストール中に AVG ではメール制御用の自動サーバーが作成されます。1 つは受信メールチェック用で、もう1 つは送信電子メールチェック用です。この 2 つのサーバーを使用して、メールは自動的にポート 110 と25（*送受信メールの標準ポート*）でチェックされます。

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。検出されたウイルスは、即時に***ウイルス隔離室***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*）。

注意：*AVG 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。*

8.7.2. メールスキャナインターフェース



メールスキャナコンポーネントダイアログでは、コンポーネントの機能を説明する簡潔なテキスト、現在のステータスに関する情報（*メールスキャナはアクティブです。*等）、また以下の統計が表示されます。

- ***合計スキャン済み電子メール数*** - 前回***電子メール スキャナ***が起動してからスキャンされた電子メール メッセージ数（*必要に応じて、統計目的などで値のリセットを使用して、この値をリセットできます*）。
- ***検出、ロックされた脅威*** - ***メールスキャナ***起動後、検出された感染数が表示されます。
- ***インストール済みのメール保護*** - 既定のインストール済みメールクライアントに対応する特定の電子メール保護プラグインに関する情報

基本コンポーネント設定

ダイアログの下部には、***メールスキャナ設定***というセクションが表示されます。ここではコンポーネント機能の基本的な機能を編集することができます。

- ***受信メッセージのスキャン*** - アイテムをチェックすると、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。既定では、このアイテムはオンです。この設定を変更しないことをお勧めします。

- ***送信メールスキャン*** - このアイテムにチェックを付けると、アカウントからの送信されるすべてのメールのウイルススキャンが実行されるようになります（既定ではこのアイテムはオフになっています）

- ***電子メールのスキャン中に通知アイコンを表示*** - このアイテムにチェックを付けると、***電子メールスキャナ***コンポーネントで電子メールをスキャンしているときに、システムトレイのAVGアイコン上に表示される通知ダイアログで通知することを確認します。既定では、このアイテムはオンです。この設定を変更しないことをお勧めします。

メールスキャンコンポーネントの高度な設定はシステムメニューの***ツール/高度な設定***アイテムで利用できます。ただし、高度な設定は経験者ユーザー向けとして推奨されています！

注意：*すべてのAVGコンポーネントは、最適なパフォーマンスを提供す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、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は、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設定を編集します。*

コントロールボタン

メールスキャナ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。

- ***変更を保存*** - このボタンを押すと、ダイアログで行われた変更を保存、適用します。

- ***戻る*** - このボタンを押すと、デフォルトの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

8.7.3. メールスキャナ検出

[***電子メール 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、***電子メールスキャナ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*** - 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。

8.8. ID 保護

AVG 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たマルウェア対策製品です。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。***AVG 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。

8.8.1. IP 保護 原理

AVG 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。マルウェアはますます高度化し、離れた場所にいる ID 窃盗攻撃者が PC で開くことができる通常のプログラムの形で侵入してくるため、***AVG Identity Protection*** はこのような実行ベースのマルウェアに対する保護を提供します。これは、署名機能とスキャンを使用して、ファイルベースの既知のウィルスに対する保護を提供する ***AVG Anti-Virus*** の補完的な保護です。

AVG Anti-Virus と*AVG Identity Protection* ***の両方のコンポーネントをインストールし、PC の保護を完全にすることを強くお勧めします。***

8.8.2. ID 保護インターフェース

ID 保護 コンポーネントインターフェースは、コンポーネントの基本機能とステータス (*AVG Identity Protection はアクティブで完全に機能しています。*) および一部の統計データに関する概要説明を提供します。

- ***除去されたマルウェアアイテム*** - 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*** - IDP 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

基本コンポーネント設定

ダイアログの下部には、***ID 保護設定***セクションが表示されます。ここではコンポーネント機能の基本的な機能を編集することができます。

- ***ID 保護はアクティブです*** -（*既定ではオン*）：チェックを付けると、IDP 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。

一部の場合、***ID 保護***が問題のないファイルを、疑わしいまたは危険なファイルとしてレポートする場合があります。***ID 保護***は脅威の動作に基づいて脅威を検出するため、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発生します。

したがって、不審な活動が検出された場合に、***ID 保護***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*）。

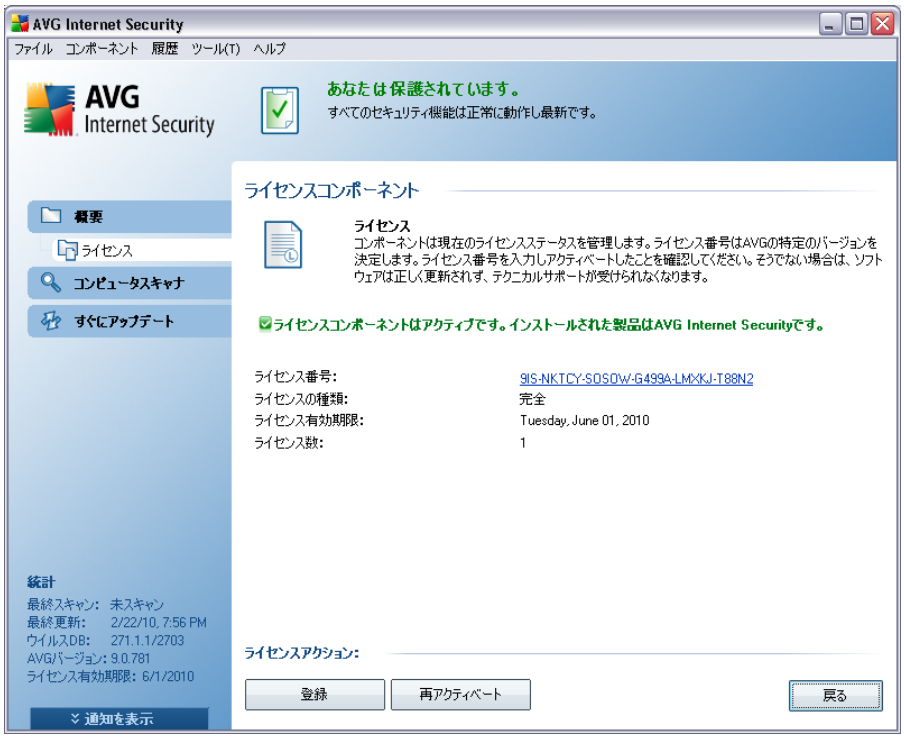
- ***自動的に検出された脅威を隔離*** - マルウェアとして検出されたすべてのアプリケーションは自動的にブロックされます
- ***自動的に既知の脅威を隔離*** - 絶対的に確実にマルウェアとして検出されたアプリケーションのみをブロックします。

コントロールボタン

ID 保護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。

- ***変更を保存*** - このボタンを押すと、ダイアログで行われた変更を保存、適用します。
- ***戻る*** - このボタンを押すと、デフォルトの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

8.9. ライセンス



ライセンスコンポーネントインターフェースでは、コンポーネントの機能を説明する簡潔なテキスト、現在のステータスに関する情報（*ライセンスコンポーネントは有効です。*等）、以下の情報が表示されます。

- ***ライセンス番号***- 正式なライセンス番号が表示されます。ライセンス番号を入力する際に、完全に正確に表示されているとおりにタイプする必要があります。したがって、ライセンス番号を誤って入力しないように、「コピーと貼り付け」を必ず使用することを強くお勧めします。

- ***ライセンスタイプ***- インストールされている製品のタイプを指定します。

- ***ライセンス有効期限***- この日付はライセンスの有効期間です。**AVG 9 Internet Security**この日付の後もを使用し続けたい場合は、ライセンスを更新する必要があります。ライセンスの更新はAVGのウェブサイト（http://www.avg.com/）でオンラインで行うことができます。

- ***ワークステーション数***- をインストールできるワークステーションの数です。**AVG 9 Internet Security**

コントロールボタン

- ***今すぐ登録*** - AVG ウェブサイト（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受けることができます。

- ***再アクティベート***- では、AVG のパーソナライズ] ダイアログで入力したデータとともに、[***AVG のアクティベート***] ダイアログが表示されます。このダイアログ内では、ライセンス番号を入力し、セールス番号（*AVGをインストールした際の番号*）を置き換えるか、古いライセンス番号（*例えば、新しいAVG製品にアップグレードした場合*）を置き換えることができます。

注意: *AVG 9 Internet Security* **の試用版を使用している場合は、[***今すぐ購入***] ボタンおよび** *[アクティベート] ボタンが表示され、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 9 Internet Security** *の場合、[****登録****] ボタンおよび [****アクティベート****] ボタンが表示されます。*

- ***戻る*** - このボタンを押すと、デフォルトの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。

8.10. リンクスキャナ

8.10.1. リンクスキャナ原理

LinkScanner は、ウェブブラウザやプラグイン経由でマルウェアをコンピュータにインストールするように設計されているウェブサイトに対する保護を提供します。***LinkScanner*** 技術は、***AVG サーチシールド*** と ***AVG アクティブサーフシールド*** の 2 つの機能から構成されています。

- ***AVG サーチシールド***には、危険であることが確認されているウェブサイト（*URL アドレス*）のリストが含まれています。Google、Yahoo!、Bing、百度、Altavista、Yandex での検索時、検索結果はすべてこのリストに従いチェックされ、決定アイコンが表示されます（*Yahoo! での検索結果の場合、「悪用されているウェブサイト」という決定アイコンのみ表示されます*）。また、ブラウザに直接アドレスを入力する場合や、メールにあるリンクなど任意のウェブサイトのリンクをクリックする場合には、自動的にリンクがチェックされ、必要に応じてブロックされます。

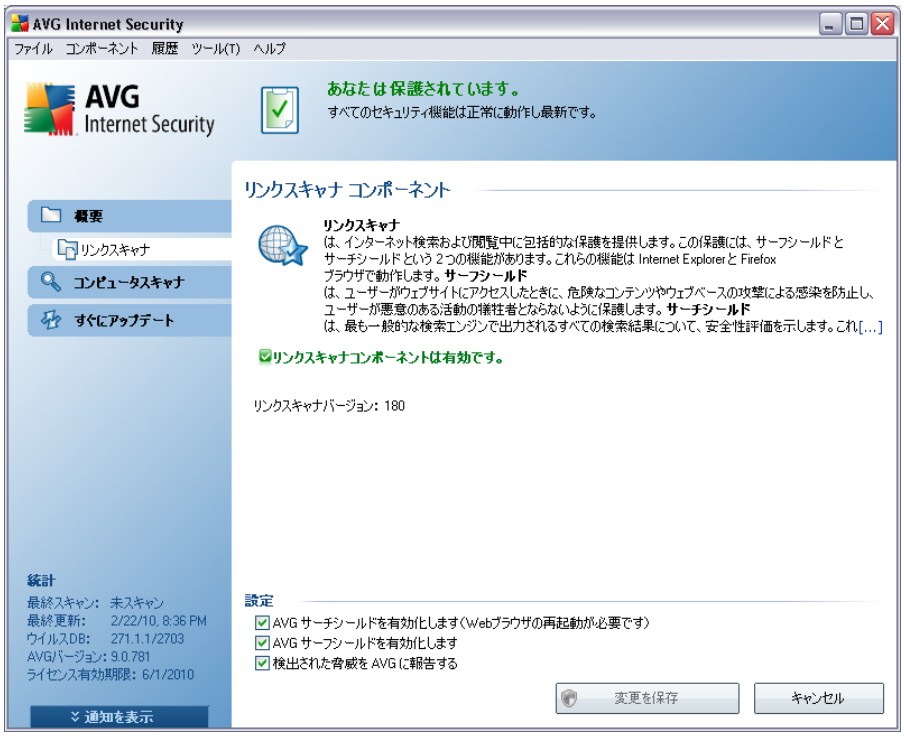
- ***AVG サーフシールド***はウェブサイトアドレスに関係なく、アクセスしようとしているウェブサイトのコンテンツをスキャンします。一部のウェブサイトが ***AVG サーチシールド***で検出されない場合（*例：新しい悪意のあるウェブサイトが作成された、以前に安全であったウェブサイトに今はマルウェアが含まれているなど*）には、そのサイトにアクセスしようとすると、***AVG サーフシールド***によってブロックされます。

注意：*AVG LinkScanner はサーバープラットフォームには対応していません。*

8.10.2. 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は、***リンクスキャナコンポーネント***インターフェースでオン/オフ可能な2つの機能から構成されています。

LinkScannerコンポーネントインターフェースは、コンポーネントの機能の概要と現在のステータスに関する情報（*LinkScanner コンポーネントはアクティブです。*）、さらに、最新の ***LinkScanner*** データベースバージョン番号（*LinkScanner バージョン*）に関する情報を表示できます。



ダイアログの下部の一部のオプションは編集できます。

- ***サーチシールドを有効化*** - (*デフォルトではオン*) Google、Yahoo、Bing、百度、Yandex、Altavistaの検索検索エンジンによる検索結果をあらかじめチェックし、その内容をアイコンで通知します。
- ***サーフシールドを有効化*** - (*デフォルトではオン*) アクセス時のアクティブな (*リアルタイムの*) エクスプロイトサイトに対する保護。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。
- ***検出された脅威のAVGへの報告を有効化*** - この項目にチェックを付けると、***サーフシールド***、または***サーチシールド***によって検出されたエクスプロイトと悪意のあるサイトが報告され、Web上の悪意のある活動に関する情報を収集するためのデータベースに送信されます。

8.10.3. AVGサーチシールド

AVG 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場合、Yahoo!、Google、Bing、Altavista、Yandex などの最も有名な検索エンジンの検索結果は、危険、または疑わしいリンクであるかどうかが評価されています。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、***AVG 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（*Yahoo!検索エンジンを AVG セキュリティツールバーとともに使用すると、このアイコンは表示されません。*）.

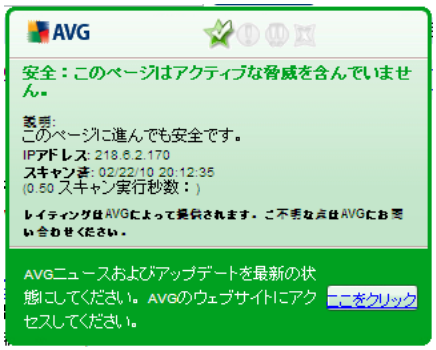
リンクされたページは脅威を含んでいませんが、疑わしいコンテンツを含みます（*または目的が疑わしいため、電子ショッピングが推奨されないなど*）。）.

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。

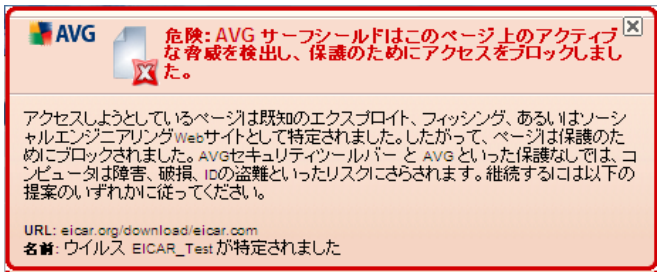
個々の評価アイコンは、問題のあるリンクに関する詳細を表示します。この情報には、（存在する場合）脅威についての追加詳細、リンクのIPアドレス、スキャン実行日時が含まれています。



8.10.4. AVGサーフシールド

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、***AVG 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、***AVG 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。

8.11. オンライン シールド

8.11.1. オンライン シールドの原理

オンライン シールドは、リアルタイムの常駐保護の一種です。Web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、Webページの内容（およびそこに含まれる可能なファイル）をスキャンします。

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が危険なjavascriptを含んでいる場合、ページの表示を防ぎます。また、ページに含まれるマルウェアも検出することができ、コンピュータにダウンロードされないようにします。

注意：*AVG オンライン シールドはサーバー プラット フォームには対応していません。*

8.11.2. オンライン シールド インターフェース

オンライン シールドコンポーネントのインターフェースには、保護の説明が表示されます。さらに、コンポーネントの現在のステータスに関する情報（*オンライン シールドは有効で完全に機能していますなど*）を*見ることができます。*）. ダイアログの下部には、このコンポーネント機能の基本編集オプションが表示されます。

基本コンポーネント設定

オンライン シールド有効化にチェックを付けると、***オンライン シールド***のオン/オフを切り替えることができます。このオプションはデフォルトでチェックされており、***オンライン シールド***コンポーネントは有効です。この設定を変更する理由がない場合、コンポーネントを有効のままにすることを推奨します。有効化にチェックがつけられており、***オンライン シールド***が実行中の場合、さらに設定を編集することができます。

- ***Web***- 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します。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。

o ***Web 保護*** - 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ページコンテンツをスキャンします。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。

- ***アーカイブチェック*** - WWWページに含ま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をレポート*** - (*デフォルトではオン*): 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レポート*** - 前のオプションが有効になっている場合、このボックスにチェックを付けると、スパイウェアの拡張パッケージも検出できます。拡張パッケージとは、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の使用*** - 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。したがって、ウイルスデータベースにまだ登録されていない悪意のあるコードを検出することも可能です（*ウィルス対策の原理*を参照）。

- ***スキャン対象ファイルの最大サイズ*** - このファイルサイズ以下のファイルがページに含まれる場合、コンピュータにダウンロードされる前にスキャンを実行します。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。***

- ***インスタントメッセージ*** - インスタントメッセージ（*例えば、ICQ、MSNメッセンジャー、Yahoo ...*）スキャンに関するコンポーネント設定を編集できます。

o インスタントメッセージ保護 - オンライン シールドでインスタントメッセージによるウイルス感染をチェックする場合、この項目をチェックします。このオプションがオンの場合、さらに制御するインスタントメッセージアプリケーションを指定します - **AVG 9 Internet**

Security現在サポートされているものはICQ、MSN、Yahoo です。

注意：*すべてのAVGコンポーネントは、最適なパフォーマンスを提供す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、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は、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設定を編集します。*

コントロールボタン

オンライン シールド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。

- ***変更を保存*** - このボタンを押すと、ダイアログで行われた変更を保存、適用します。
- ***キャンセル*** - このボタンを押すと、デフォルトの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

8.11.3. オンライン シールド検出

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。

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。[***リストを更新***] ボタンは***オンライン 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 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。

8.12. 常駐シールド

8.12.1. 常駐シールド 原理

常駐シールドコンポーネントはコンピュータに継続した保護を提供します。これは、オープン、保存、コピーされるあらゆるファイルをスキャンし、コンピュータのシステムエリアを保護します。***常駐シールド***がアクセスされるファイルにウイルスを検出する場合、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。通常、「バックグラウンド」で実行されるため、このプロセスに気づくことはありません。脅威が検出された場合のみ通知されます。同時に、常駐シールドは脅威のアクティブ化をブロックし、それを除去します。***常駐シールド***は、システムの起動中にコンピュータメモリにロードされます。

警告 :常駐シールドはシステム起動時にコンピュータのメモリ内にロードされます。したがって、常にそのスイッチを入れておくことが極めて重要です。

8.12.2. 常駐シールドインターフェース

最も重要な統計データとコンポーネントの現在のステータスに関する情報の概要 *(常駐シールドは有効で完全に機能しています。等)* に加えて、***常駐シールド***インターフェースには、いつくかの基本コンポーネント設定オプションも表示されます。統計は以下の通りです。

- 常駐シールド起動時間 - コンポーネントが起動されている時間
- ***検出およびブロックされた脅威*** - 実行したり開いたりできないようにされた検出された感染数 *(統計目的などで、必要に応じて、この値はリセットできます - 値のリセット)*。

基本コンポーネント設定

ダイアログの下部には、***常駐シールド設定***というセクションがあります。ここでは、コンポーネントの機能の基本設定 *(他のコンポーネントと同様に、詳細設定はシステムメニューのファイル/高度な設定で使用可能です)* を編集することができます。

常駐シールド有効化オプションでは、常駐保護のオン/オフを簡単に切り替えることができます。デフォルトではこの機能はオンとなっています。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 (除去) 方法を決定できます。

- 自動（***すべての脅威を自動的に除去***）
- あるいはユーザー許可の後のみ（***脅威を削除する前に確認する***）

この選択はセキュリティレベルに影響はありません。

いずれの場合も、***Tracking Cookie*** をスキャンするかどうかを選択することができます。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。（*cookie とはサーバーによって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*）。

注意：*すべてのAVGコンポーネントは、最適なパフォーマンスを提供す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、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は、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設定を編集します。*

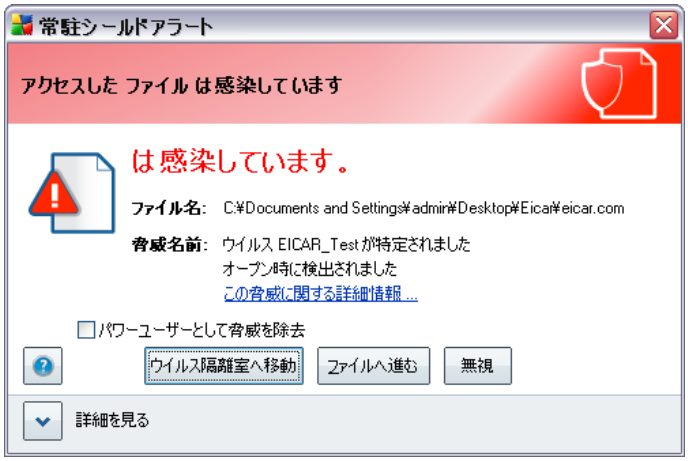
コントロールボタン

常駐シールド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。

- ***例外の管理*** - [***常駐シールド- 例外ディレクトリ***] ダイアログを開きます。このダイアログでは、***常駐シールド***スキャンから除外されるフォルダを定義します。
- ***変更を保存*** - このボタンを押すと、ダイアログで行われた変更を保存、適用します。
- ***戻る*** - このボタンを押すと、デフォルトの***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

8.12.3. 常駐シールド検出

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。



ダイアログには検出された脅威に関する情報が表示され、この時点で取るべきアクションを決定するように要求されます。

- ***修復*** - 修復方法がある場合、AVG によって感染ファイルは自動的に修復されます。このオプションのアクションを取ることをお勧めします。
- ***ウイルス隔離室に移動*** - ウイルスは AVG ***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。

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 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。

8.13. アップデートマネージャ

8.13.1. アップデートマネージャ 原理

定期的にアップデートが実行されていない場合、どのようなセキュリティソフトウェアも様々な脅威からの保護を保証することはできません。ウイルス作成者は、常に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探しています。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継続的にアップデートとセキュリティパッチを発行し、発見されたセキュリティホールを修復しています。

AVG を定期的にアップデートすることは非常に重要です。

アップデートマネージャによって、定期的なアップデートを管理することができます。このコンポーネントでは、インターネット、またはローカルネットワークからのアップデートファイル自動ダウンロードをスケジュールすることができます。可能であれば、ウイルス定義アップデートを毎日実行してください。より緊急度の低いプログラム更新は、週次で行うことを推奨します。

注意：*アップデートの種類とレベルの詳細については、AVGアップデートの章を参照してください。*

8.13.2. アップデートマネージャ インターフェース

アップデートマネージャのインターフェースには、コンポーネントの機能、現在のステータスに関する情報(*アップデートマネージャは有効です。*等)、関連する統計データが表示されます。

- ***最終アップデート*** - データベースが最後にアップデートされた日時が表示されます。
- ***ウイルスデータベースバージョン*** - 最新のウイルスデータベースバージョンが表示されます。この番号はウイルスアップデートごとに増加します。
- ***次回のスケジュール済みアップデート*** - データベースが再度アップデートされるようにスケジュールされている日時

基本コンポーネント設定

ダイアログの下部では、***アップデートマネージャ設定***セクションが表示され、ここでは、アップデートプロセスの実行ルールの一部を変更することができます。アップデートファイルのダウンロードを自動的に実行するか(***自動アップデート開始***)、またはオンデマンドで実行するかを指定します。デフォルトでは、***自動アップデート開始***オプションはオンであり、この設定を保持することを推奨します。最新アップデートファイルの定期的なダウンロードは、セキュリティソフトウェアが正しく機能するために、非常に重要で

す。

さらに、アップデートが起動するタイミングを指定することができます。

- ***定期的***- 時間間隔を定義します。
- ***時間指定***- 正確な日時を指定します。

デフォルトでは、アップデートは4時間おきに設定されています。特に変更する理由がない場合、この設定を保持することを強く推奨します。

注意：*すべてのAVGコンポーネントは、最適なパフォーマンスを提供す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、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は、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設定を編集します。*

コントロールボタン

アップデートマネージャ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。

- ***すぐにアップデート***- オンデマンドで即時アップデートを実行します。
- ***変更を保存*** - このボタンを押すと、ダイアログで行われた変更を保存、適用します。
- ***戻る*** - このボタンを押すと、デフォルトの***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

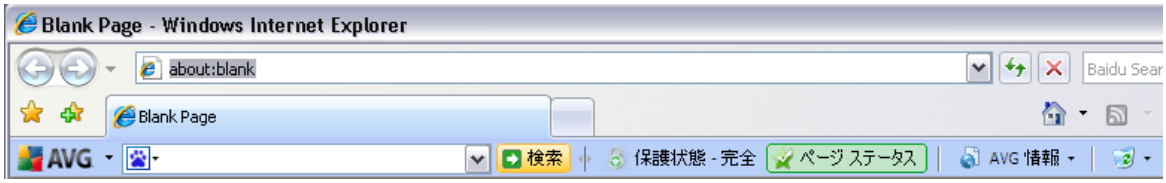
9. AVGセキュリティツールバー

AVG セキュリティツールバー は、***リンクスキャナ***コンポーネントと連携して動作し、サポートされたインターネット検索エンジン（*Yahoo!*、*Google*、*Bing*、*Altavista*、*百度*）の検索結果をチェックする新しいツールです。***AVG セキュリティツールバー***は ***AVG リンクスキャナ***機能を制御して、動作を調整するために使用できます。

AVG 9 Internet Security のインストール中にツールバーのインストールを選択した場合は、自動的にウェブブラウザに追加されます。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。

9.1. AVGセキュリティツールバー インターフェース

AVG セキュリティツールバーは、***MS Internet Explorer***（*バージョン 6.0 以上*）および***Mozilla Firefox***（*バージョン 2.0 以上*で動作するよう設計されています。***AVG セキュリティツールバー*** *のインストールを選択（AVG インストールプロセス中に、コンポーネントをインストールするかどうかを決定するように要求されます*）した場合、このコンポーネントがウェブブラウザのアドレスバーの下に表示されます。



注意：*AVG セキュリティツールバーはサーバープラットフォームには対応していません。*

AVG セキュリティツールバーは以下のように構成されています。

- ***AVG ロゴ*** - 一般ツールバー アイテムへのアクセスを提供します。ロゴボタンをクリックすると、AVG の Web サイト（http://www.avg.com/）が表示されます。AVGアイコンの隣のポインタをクリックすると、以下が表示されます。
    - ***Toolbar Info*** - ツールバーの保護に関する詳細情報を提供する***AVG セキュリティツールバーホームページへのリンクです。***
    - ***AVG 9 Internet Security*** を起動 - **AVG 9 Internet Security ユーザー インターフェースを開きます**
    - ***オプション*** - 設定ダイアログが開き、***AVG Security Toolbar*** の設定をニーズに合わせて調整できます。***AVG Security Toolbar オプションの章を参照してください。***
    - ***履歴の削除*** - AVGセキュリティツールバーの*完全な履歴の削除*または、*検索履歴の削除*、*ブラウザ履歴の削除*、*ダウンロード履歴の削除*および*Cookies の削除*ができます。

- ***アップデート*** - *AVG セキュリティツールバーの新しいアップデートをチェックします。*
- ***Help*** - ヘルプファイルを開いたり、製品フィードバックを送信したり、ツールバーの現行バージョンの詳細を見るオプションを提供します。

- ***検索ボックス*** - 単語またはフレーズを検索ボックスに入力します。[***検索***] をクリックすると、現在表示されているページに関係なく、指定した検索エンジンを使用して検索を開始します (*AVG セキュリティツールバー高度なオプションで使用する検索エンジンを指定できます。また、Yahoo!、Wikipedia、百度、WebHledani、Yandex* のいずれかを選択できます)。検索ボックスには検索履歴のリストも表示されます。検索ボックスで行われた検索はAVGサーチシールド***で分析されます。***
- ***総合的な保護*** - このボタンは、***総合的な保護/限定的な保護/保護なし***として、**AVG 9 Internet Security**設定
- ***ページステータス*** - このボタンは、ツールバーに直接、***AVG サーチシールド*** コンポーネントの条件に基づいて現在アップロードされているウェブページの評価を示します (*ページは安全です/不審/明らかに危険/脅威を含む/スキャンできませんでした*)。ボタンをクリックすると、情報パネルと、特定のウェブページに関する詳細データが表示されます。
- ***AVG 情報*** - AVG Webサイト (http://www.avg.com/) の重要なセキュリティ情報へのリンクを提供します。
  - ***Toolbar Info*** - ツールバーの保護に関する詳細情報を提供する***AVG セキュリティツールバーホームページへのリンクです。***
  - ***脅威について*** - 現在のインターネットウィルスと脅威に関する情報を示すAVGウェブページを開きます。
  - ***AVG ニュース*** - 最新のAVG関連記者発表記事を掲載したウェブページを開きます。
  - ***現在の脅威レベル*** - ウェブ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ウェブページを開きます。
  - ***ウイルスエンサイクロペディア*** - 名前ごとに特定のウイルスを検索し、ウイルスの詳細情報を確認できるウィルスエンサイクロペディアページを開きます。

9.2. AVGセキュリティツールバーオプション

すべての ***AVG セキュリティツールバー*** パラメータ設定には、[***AVG セキュリティツールバー***] パネル内から直接アクセスできます。インターフェースの編集は、新しい [*ツールバーオプション*] ダイアログの [***AVG/ オプション***] ツールバー メニュー アイテムで開きます。このダイアログには 4 つのセクションがあります。

9.2.1. タブ全般

このタブでは、[***AVG セキュリティツールバー***] パネル内の表示/非表示を切り替えるツールバー コントロール ボタンを指定できます。該当するボタンを表示する場合には、任意のオプションをマークします。各ツールバー ボタンの機能の詳細な説明は次のとおりです。

- ***AVG ニュース ボタン*** - このボタンを使用すると、最新の AVG 関連記者発表記事を掲載したウェブページを開きます。
- ***ニュース ボタン*** - このボタンを使用すると、毎日のニュース記事から最新のニュースの構造化された概要を表示します。
- ***AVG 情報 ボタン*** - このボタンを使用すると、AVG ツールバー、現在の脅威とインターネット脅威レベルに関する情報を表示し、ウィルス エンサイクロペディアを開き、詳細な AVG 製品関連ニュースを表示します。
- ***履歴の削除 ボタン*** - このボタンを使用すると、完全な履歴の削除または検索履歴の削除、ブラウザ履歴の削除、あるいは Cookies の削除を AVG Security Toolbar から直接実行できます。

9.2.2. タブの便利なボタン

[***便利なボタン***] タブでは、リストからアプリケーションを選択し、ツールバー インターフェースにアイコンを表示できます。アイコンは、各アプリケーションを即時起動できるクイック リンクとなります。

9.2.3. タブ セキュリティ

[***セキュリティ***] タブには、[***AVG ブラウザセキュリティ***] と [***評価***] という2 つのセクションがあり、特定のチェックボックスをオンにして、使用する ***AVG Security Toolbar*** 機能を割り当てられます。

- ***AVG ブラウザセキュリティ***- このアイテムにチェックすると、***AVG サーチシールド*** または ***AVG サーフシールド*** サービスの有効化/無効化を切り替えられます。
- ***評価*** - 使用する ***AVG Search-Shield***
  -  ページは安全です
  -  ページには不審な部分があります
  -  ページには明らかに危険なページへのリンクが含まれます
  -  ページにはアクティブな脅威が含まれます
  -  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

各オプションをオンにして、この特定の脅威レベルに対する通知方法を確認します。ただし、アクティブかつ危険な脅威を含むページに割り当てられる赤いマークをオフにすることはできません。***こ***

こでも、変更する理由がない限り、プログラムベンダーが設定した既定の設定を保持することをお勧めします。

9.2.4. タブの高度なオプション

[***高度なオプション***] タブでは、まず既定で使用する検索エンジンを選択します。*Yahoo!*、*百度*、*WebHledani*、および *Yandex* から選択できます。既定の検索エンジンを変更した場合は、変更を有効にするために、インターネット ブラウザを再起動してください。

特定の ***AVG セキュリティツールバー***設定のオン/オフを切り替えることができます。

- ***Yahoo! をアドレスバーの検索プロバイダとして設定*** - (*既定ではオン*) このオプションをオンにしている場合、インターネットブラウザのアドレスバーに直接検索キーワードを入力し、Yahoo!サービスを自動的に使用して関連するウェブサイトを検索できます。

- ***AVG でブラウザ ナビゲーション エラー (404/ DNS) に関する提案を表示*** - (*デフォルトではオン*) ウェブを検索しているときに存在しないページがあった場合や、表示できないページ (404 エラー) があった場合、自動的に代わりのトピック関連のページの概要から選択できるページにリダイレクトします。

- ***Yahoo! をブラウザの検索プロバイダとして設定*** - (*既定ではオフ*) Yahoo!は AVG セキュリティツールバー のウェブ検索時の既定の検索エンジンですが、このオプションを有効にすると、Yahoo! がウェブブラウザでも既定の検索エンジンとなります。

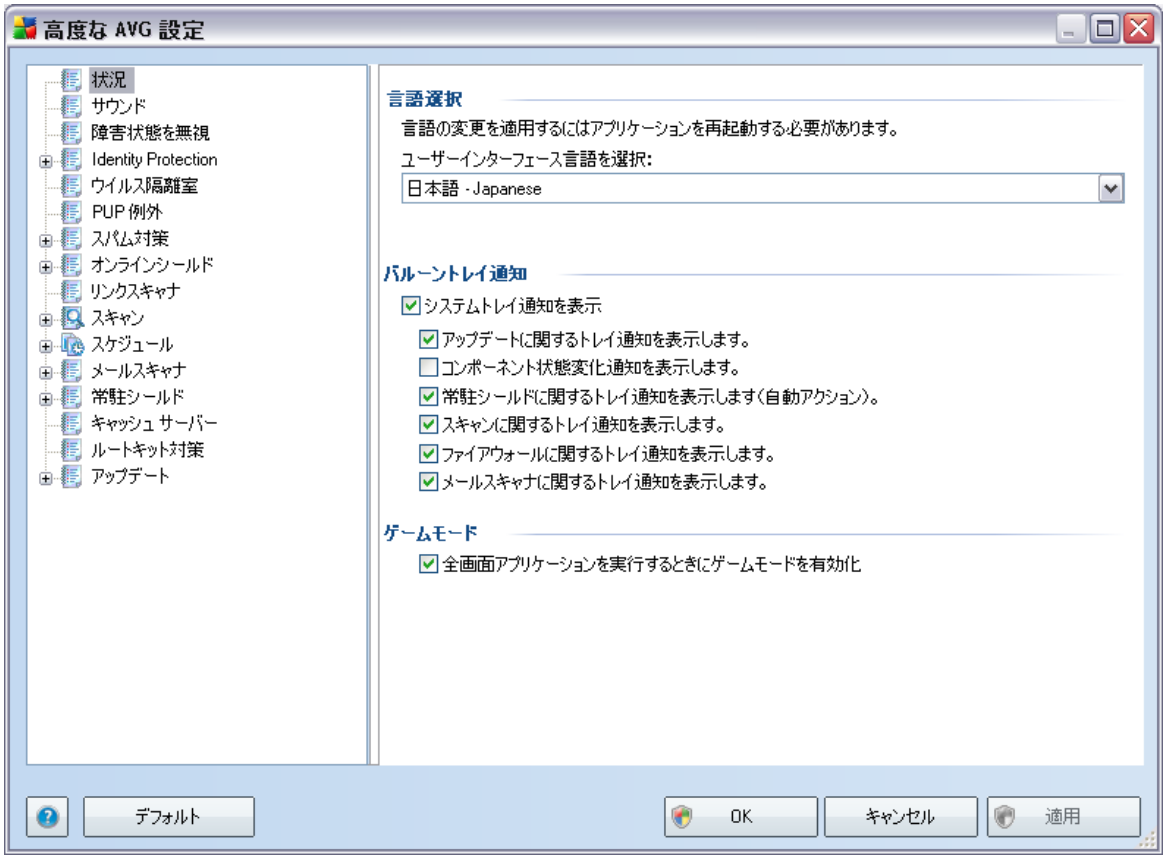
- ***非表示の場合は AVG Security Toolbar を再表示（毎週）*** - *（既定ではオン）* このオプションは既定では有効です。***AVG Security Toolbar*** が偶然非表示になってしまった場合でも、1 週間以内に再度表示されます。

10. AVG 高度な設定

AVG 9 Internet Security 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。

10.1. 表示

ナビゲーションツリーの最初の項目は、***表示***であり、AVGユーザーインターフェースと、いくつかの動作の基本オプションを設定します。

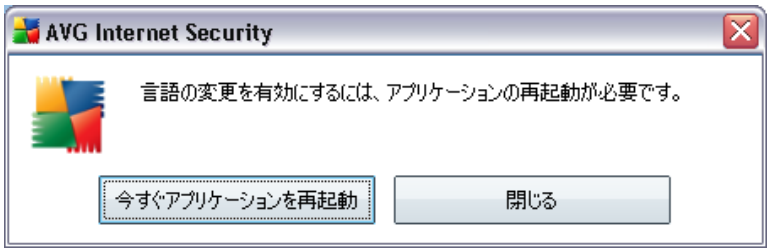


言語選択

言語選択セクションでは、ドロップダウンメニューから希望する言語を選択します。この言語は、すべてのAVGユーザーインターフェースで使用されます。ドロップダウンメニューには、インストールプロセス中にイ

ンストールされた言語のみが表示されます（カスタムインストール - コンポーネント選択の章を参照して下さい）。ただし、アプリケーションを他の言語に切り替える際には、以下の方法でユーザーインターフェースを再起動する必要があります。

- アプリケーションの希望する言語を選択し、***適用***ボタン（右側下端）を押します。
- [***OK***] ボタンをクリックして、確定します。
- AVG ユーザーインターフェースの言語を変更する場合は、アプリケーションの再起動が必要であることを通知する新しいポップアップダイアログウィンドウが表示されます。



バルーントレイ通知

このセクションでは、アプリケーションステータスに関するシステムトレイバルーン通知の表示を制御できます。デフォルトではバルーン通知は表示されるようになっており、この設定を保持することが推奨されます。バルーン通知は一般にAVGコンポーネントのステータス変更を通知します。

ただし、なんからの理由で、これらの通知を非表示にしたい場合や、ある通知のみを表示したい場合は、以下のオプションのチェックの付け外しにより、希望の内容を指定することができます。

- ***システムトレイ通知を表示*** - デフォルトでは、このアイテムはチェックされおり、通知が表示されます。このアイテムのチェックを外すとすべてのバルーン通知表示はオフになります。オンの場合、どの通知が表示されるかを選択することができます。
  - ***アップデート***に関するトレイ通知を表示 - AVGアップデートプロセスの起動、進行、完了に関する情報が表示されるかどうかを決定します。
  - ***コンポーネントの状態変化に関するトレイ通知を表示*** - コンポーネントの有効/無効、または問題に関する情報が表示され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（色変更）と同等のものとなります。
  - ***常駐シールド関連のトレイ通知を表示*** - ファイルの保存、コピー、および開く処理に関する情報を表示するかしないかを決定します（*この設定は、常駐シールドの［自動修復］オプションがオンになっ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 - スケジュール済スキャンの自動起動、進行、結果に関する情報が表示され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** - 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。例えば、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等が表示されます。

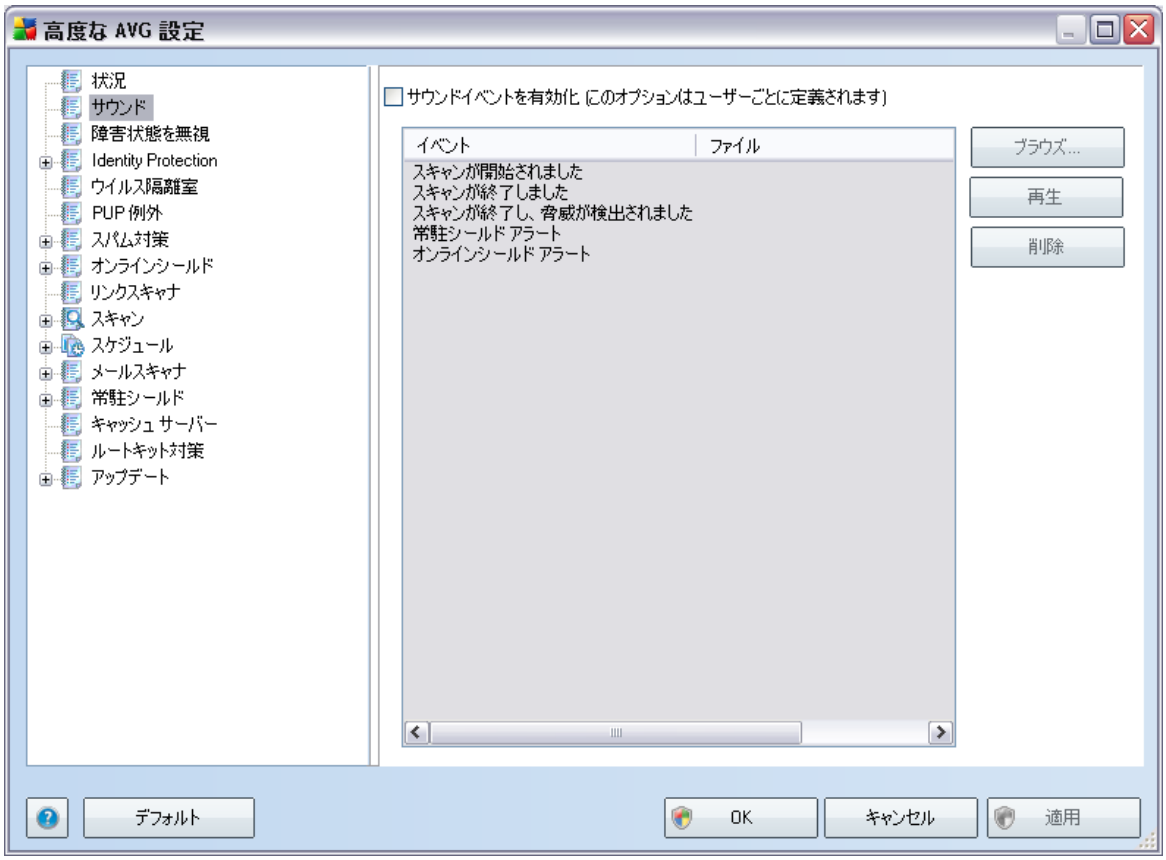
- ***メールスキャナ*に関するトレイ通知を表示** - すべての送受信メールに関する情報が表示されるかどうかを決定します。

ゲームモード

この AVG 機能は、AVG 情報バルーン(*スケジュールされているスキャンが開始するときなどに表示*)がアプリケーションを妨害する可能性の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を最小化したりグラフィックを壊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ば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*)。

10.2. 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 アクションの通知を行うかどうかを指定できます。このようにする場合は、[***サウンドイベントを有効化***]オプション(*既定ではオフ*)にチェックを付け、AVG アクションのリストを有効化します。

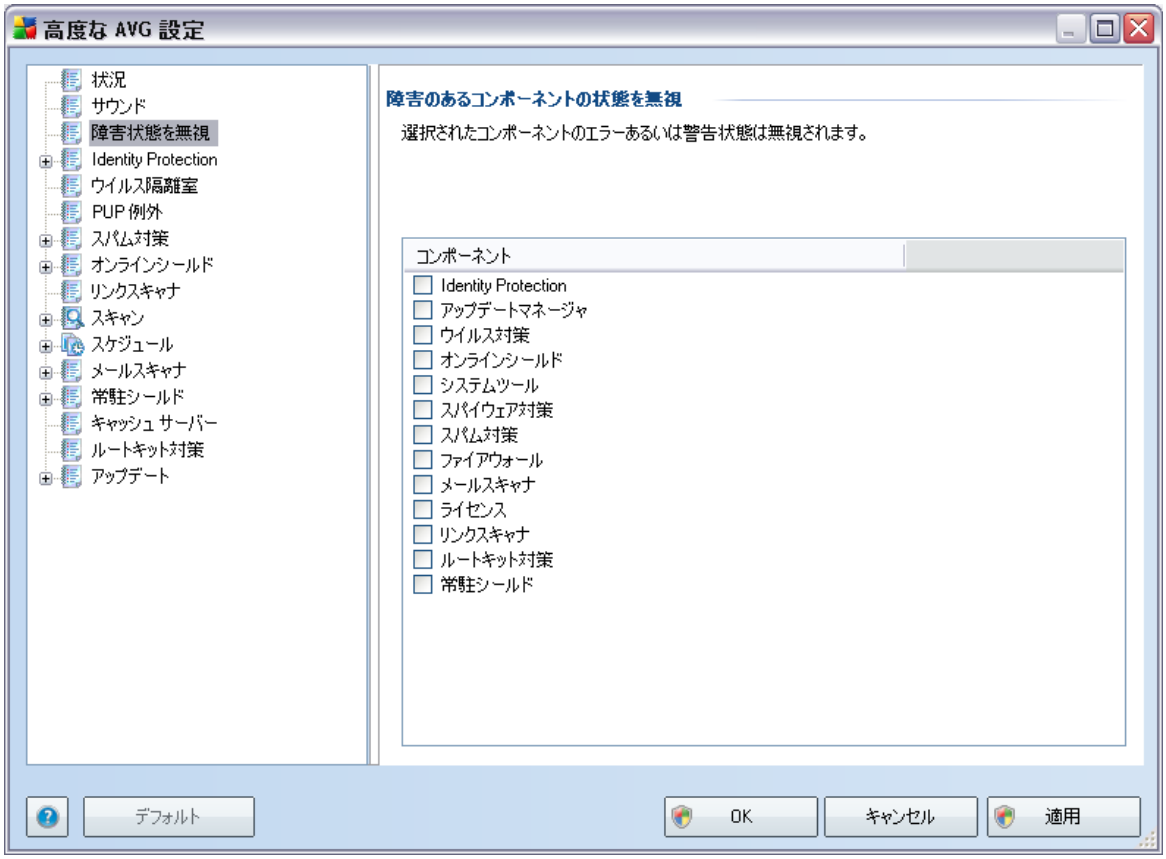


次に、リストから該当するイベントを選択し、このイベントに割り当てる適切なサウンドをディスクから参照（[***参照***]）します。選択されたサウンドを聴くには、リストのイベントをハイライトし、[***再生***] ボタンをクリックします。[***削除***] ボタンをクリックすると、特定のイベントに割り当てられたサウンドを削除します。

注意：*.wav サウンドのみがサポートされています。*

10.3. 障害状態を無視

コンポーネントの障害状態を無視ダイアログでは、情報の通知を受けたく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。



既定値では、リストのどのコンポーネントも選択されていません。つまり、すべてのコンポーネントがエラー状態となる場合は、すぐに以下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ます。
- AVGメインウィンドウの***セキュリティステータス情報***セクション既存の問題に関するテキスト説明

何らかの理由のため、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、既定のコンフィグレーションを保持する*

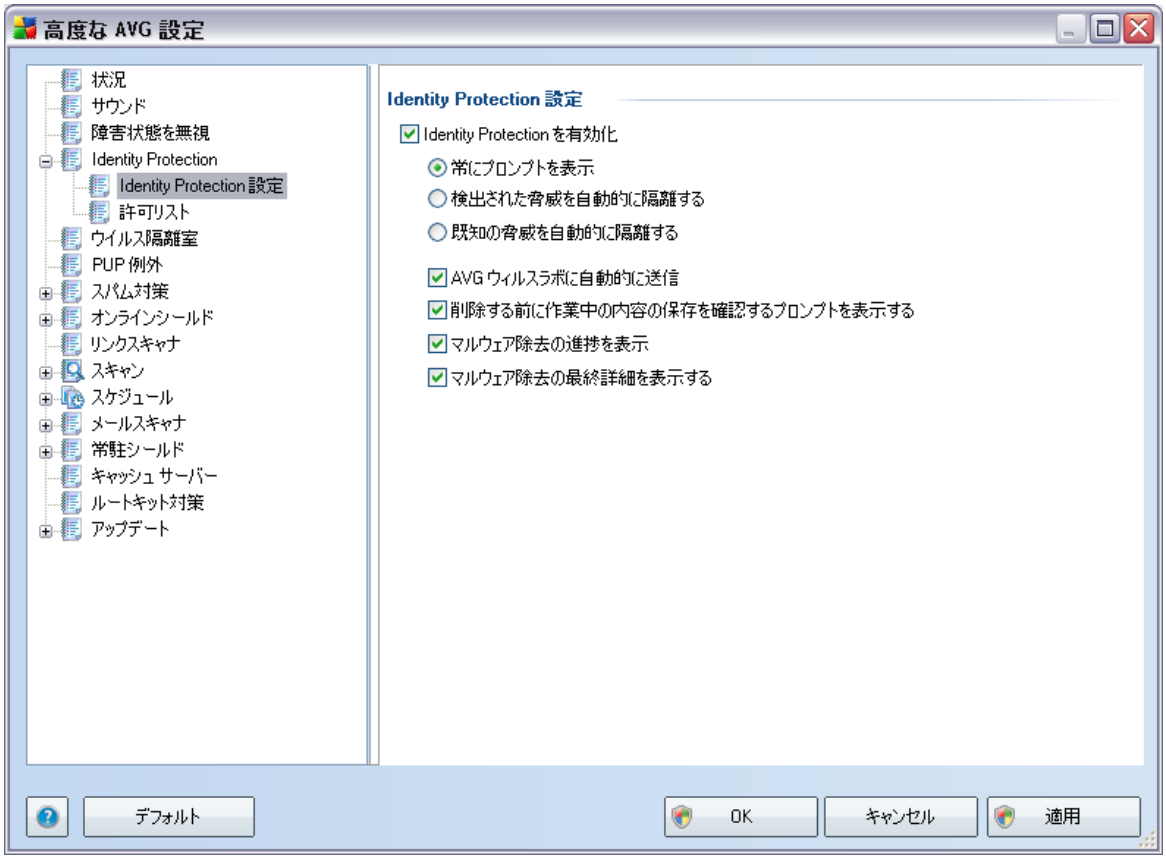
必要がありますが、この状況は起こりえます）。この場合、システムトレイアイコンが自動的にコンポーネントのエラーステータスをレポートします。ただし、この場合には、自分で慎重に行い、潜在的なリスクを認識しているため、実際のエラーについては説明できません。同時に、グレイ色で表示されると、アイコンは実際には表示される可能性のある他のエラーをレポートできません。

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、その状態は通知されません。***コンポーネント状態を無視***の同様のオプションは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。

10.4. 個人情報保護

10.4.1. ID 保護設定

[***ID 保護設定***] ダイアログでは、***ID 保護***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。



ID 保護はアクティブです *（デフォルトではオン）* - チェックを外すと、***ID 保護***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。

ID 保護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 ***AVG 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 ***AVG 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。

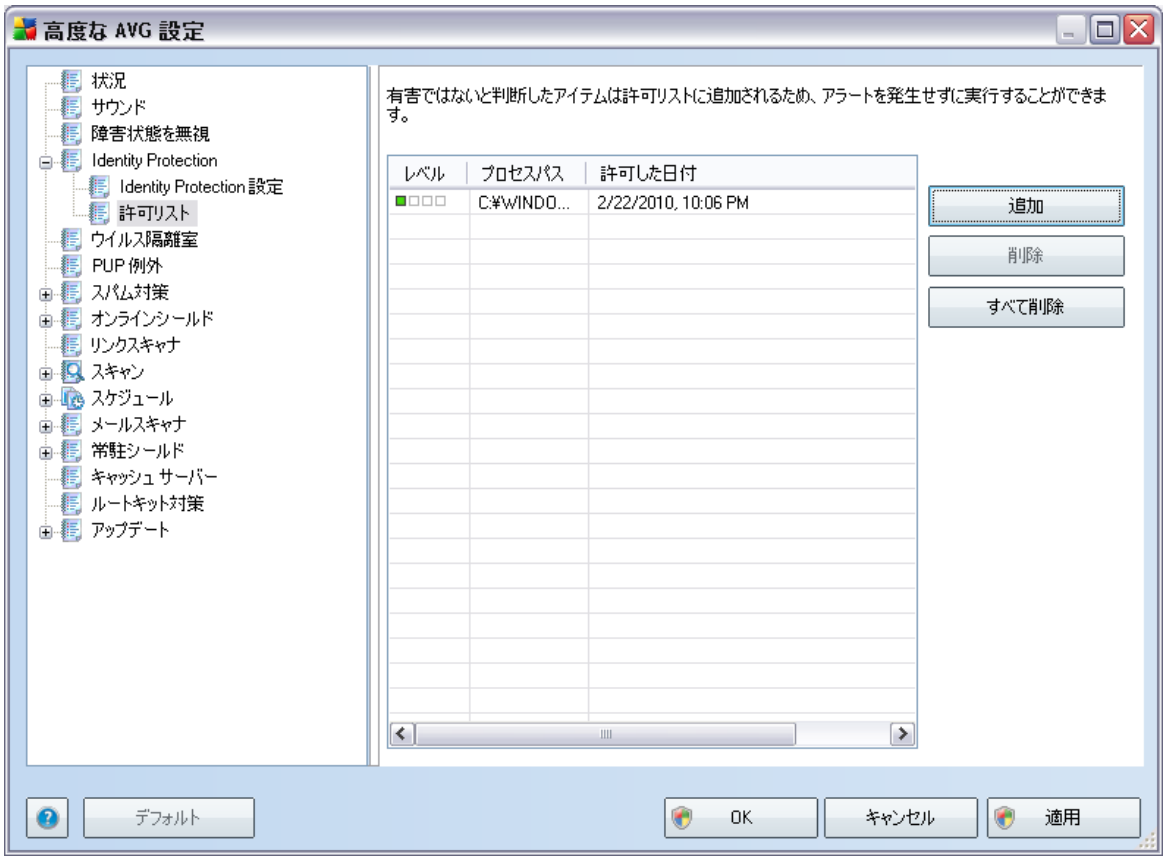
さらに、特定の項目を割り当てて、任意で他の***ID 保護***の機能をアクティブ化できます。

- ***自動的にAVG ウイルスラボに送信*** -(*既定ではオン*):このチェックボックスをオンにし、ウェブ上の悪意のある活動に関する情報を収集するデータベースに情報を提供し、新しい脅威の特定をサポートしてください。
- ***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*).

10.4.2. 許可リスト

[***ID 保護設定***] ダイアログで、[***検出された脅威を自動的に隔離する***] アイテムのチェックを外すと、危険な可能性のあるマルウェアが検出されるたびに、削除するかどうかを確認します。疑わしいアプリケーション *動作に応じて検出された*) を安全なアプリケーションとして割り当て、コンピュータ上で保持

するようにすると、そのアプリケーションは、いわゆる***許可リスト***に追加され、今後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。



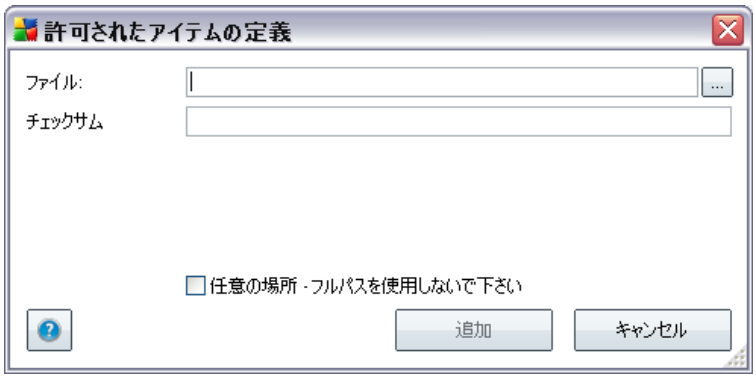
許可リストは、各アプリケーションに関する次の情報を提供します。

- ***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*）実行可能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割り当てた日

コントロールボタン

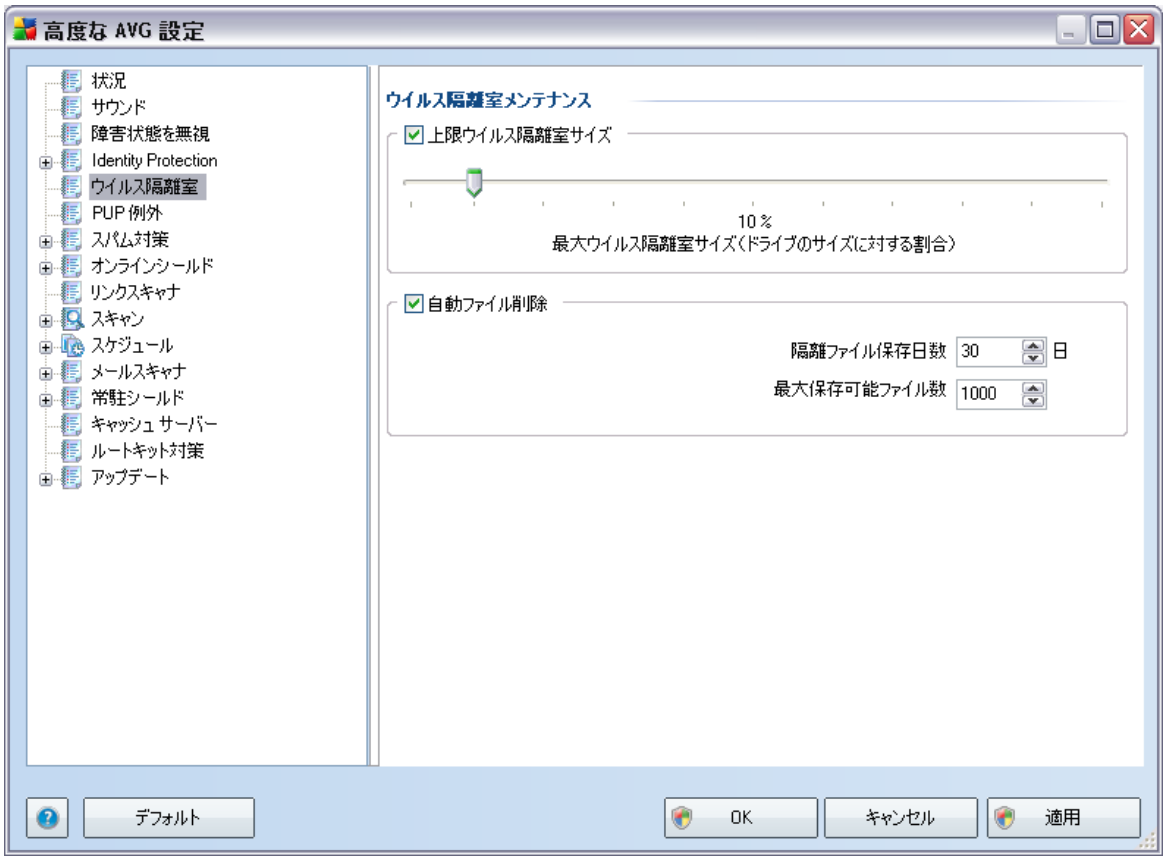
[***許可リスト***] ダイアログでは次のコントロールボタンが利用できます。

- ***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*** - 例外としてマークするファイル(*アプリケーション*)へのフルパスを入力します。
  - ***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、これによって、AVGは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、表示されます。
  - 任意の場所 - フルパスを使用しない - 特定の場所のみの例外としてこのファイルを定義する場合、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。

10.5. ウイルス隔離室



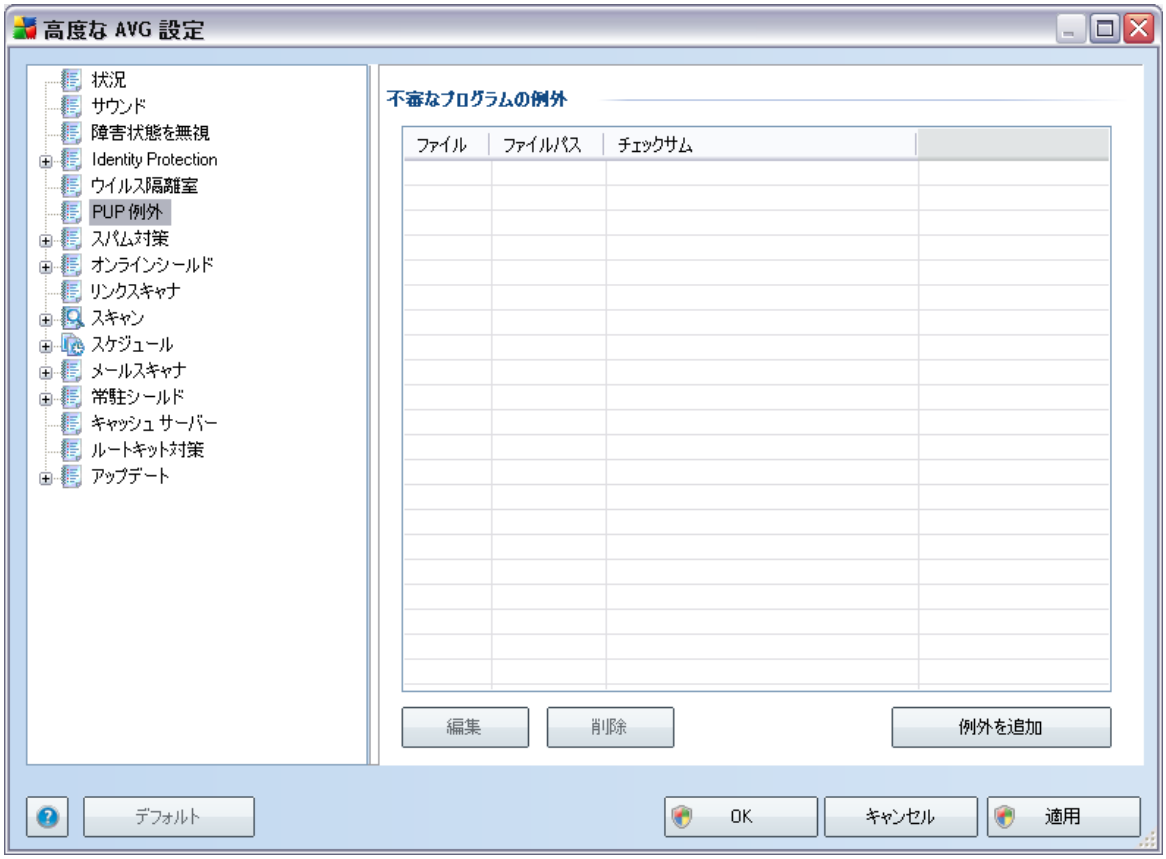
ウィルス隔離メンテナンスダイアログでは、***ウィルス隔離***に格納されるオブジェクト管理に関するパラメータを定義できます。

- ***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。

10.6. PUP 例外

AVG 9 Internet Securityはまた、潜在的にシステムに望ましくない実行可能アプリケーションやDLLライブラリを分析、検出することができます。一部の場合では、ユーザーは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があります（*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

料のものはアドウェアを含んでいます。このようなアドウェアはAVGによって***不審なプログラム***として検出され、レポート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したい場合、それを不審なプログラムの例外として定義することができます。

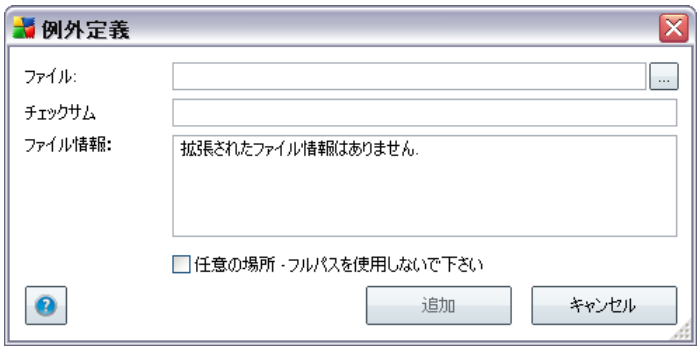


不審なプログラム例外ダイアログでは、既に定義された不審なプログラムの例外リストが表示されます。リストの編集、既存のアイテムの削除、新しい例外の追加ができます。次の情報は、各例外のリストにあります。

- ***ファイル*** - 各アプリケーション名を提供します。
- ***ファイルパス*** - アプリケーションの場所を示します。
- ***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、これによって、AVGは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、表示されます。

コントロールボタン

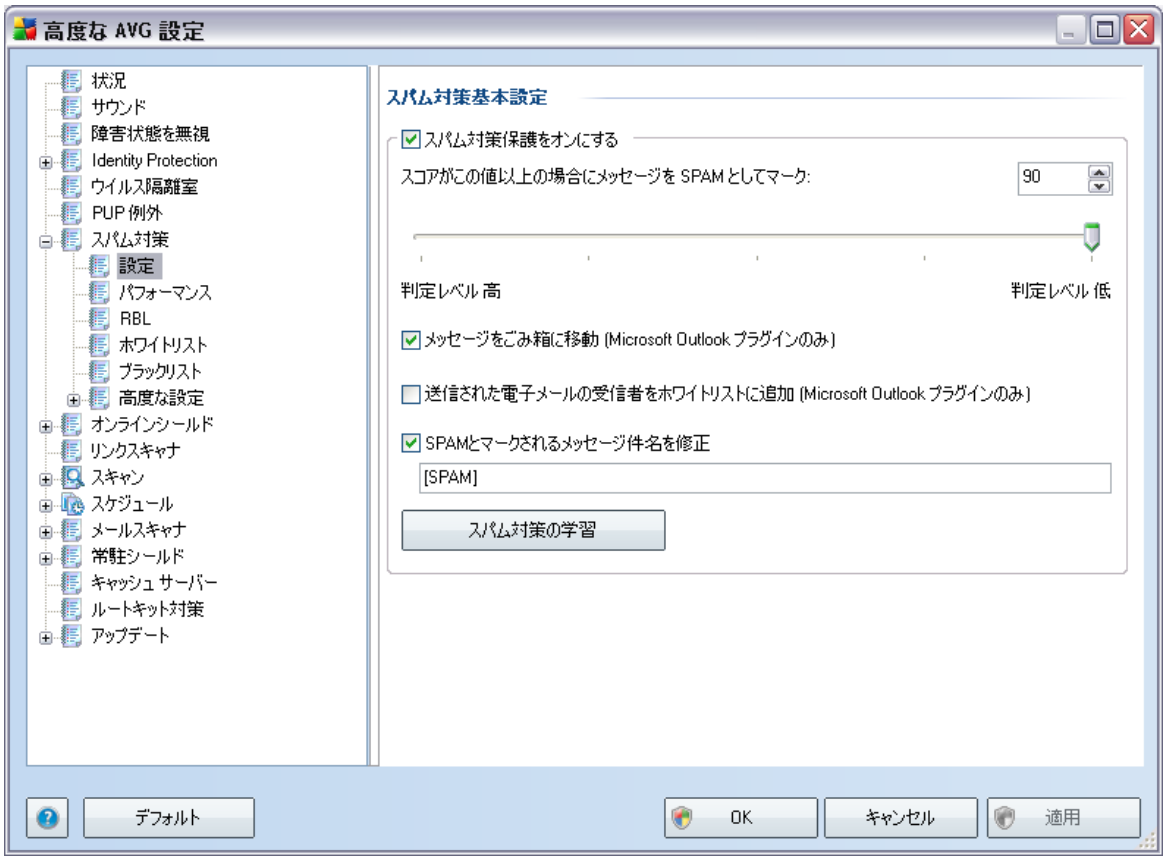
- ***編集*** - 既に定義された例外の編集ダイアログ（*新しい例外定義ダイアログと同一です。以下を参照*）を開きます。ここで例外パラメータを変更します。
- ***削除*** - 例外リストから選択された項目を削除します。
- ***例外を追加*** - 編集ダイアログを開きます。ここでは作成する例外のパラメータを定義します。



  - ***ファイル*** - 例外としてマークするファイルへのフルパスを入力します。
  - ***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、これによって、AVGは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、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/バージョン等*）
  - ***任意の場所 - フルパスを使用しない*** - 特定の場所のみの例外としてこのファイルを定義する場合、このチェックボックスのチェックを外します。

10.7. スパム対策

10.7.1. 設定



[***スパム対策基本設定***] 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 *(0 ～ 100)* を入力するか、スライダを左右に動すことによって *(スライダを使用すると値の範囲は 50 ～ 90に制限されます)*、スコアがこの値以上の場合、***スパムとして判定されるよう***設定を調整することができます。

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 90 ～ 99*** - 大部分の受信電子メール メッセージは通常通りに (スパムとしてマークされずに) 配信されます。簡単に特定されるスパムはフィルタリングされますが、かなりの数のスパム

が許可される可能性があります。

- ***値80-89*** - スパムの可能性が高いメールはフィルタリングされます。一部の正常なメッセージも誤って除去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去されます。一部の正常なメッセージも除去される可能性があります。
- ***値1-59***- 非常に積極的な設定です。正常なメールが、本物のスパムメールと同様に除去される可能性が高くなります。この値は通常の使用には推奨されません。
- ***値 0*** - このモードでは、***ホワイトリスト***にある送信者からのメールのみが受信されます。その他のいかなるメールもスパムとみなされます。***この値は通常の使用には推奨されません。***

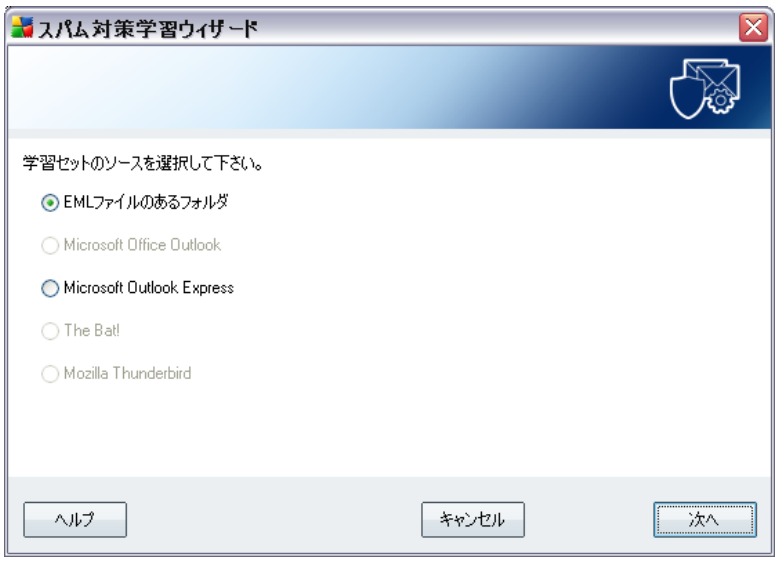
スパム対策基本設定ダイアログでは、さらに検出されたスパムメールメッセージが処理される方法を定義することができます。

- ***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。

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。

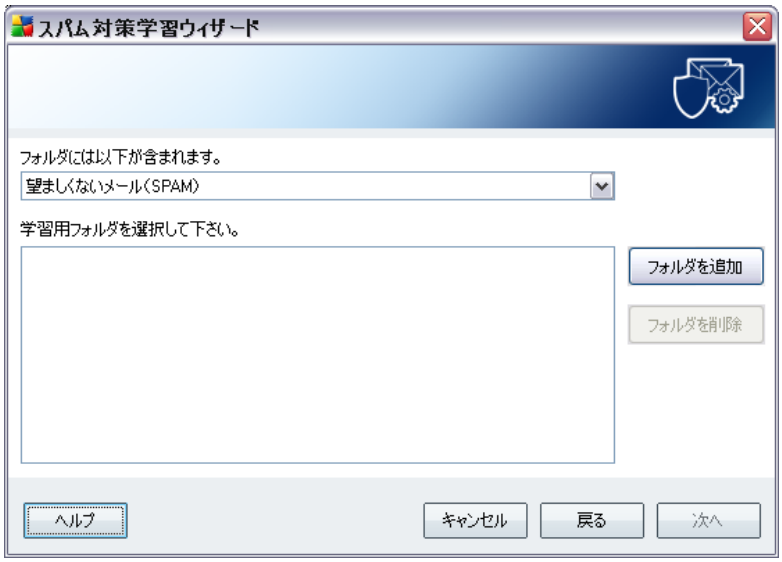
- ***特定のメールクライアント*** - リストされたメールクライアントの1つ (*MS Outlook, Outlook Express, The Bat!, Mozilla Thunderbird*) を使用する場合、該当するオプションを選択します。
- ***EML ファイルのあるフォルダ*** - 他のメールプログラムを利用する場合、まずメッセージを特定のフォルダに保存 (*eml*形式)、またはメールクライアントメッセージフォルダの場所を確認します。次に、***EML ファイルのあるフォルダ***を選択します。次のステップで希望するフォルダを指定します。

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

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

このステップで表示されるダイアログは、以前の設定により異なります。

EMLファイルのあるフォルダ



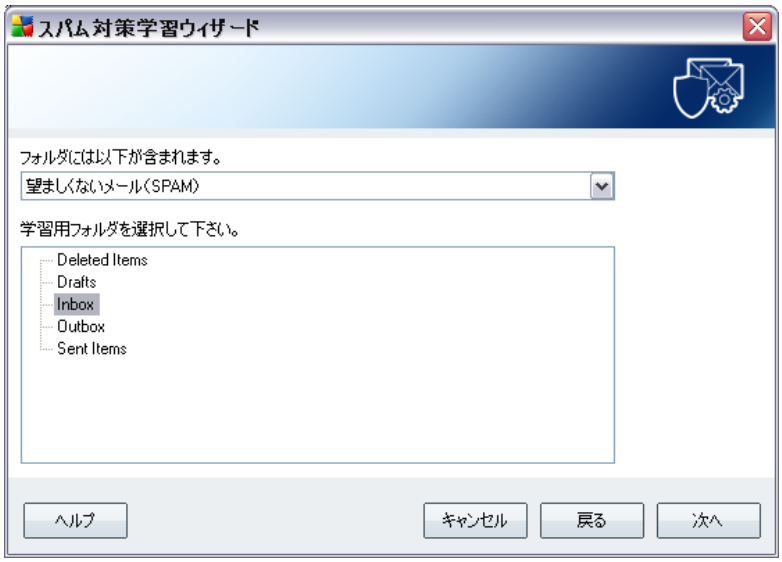
このダイアログでは学習に使用するメッセージフォルダを選択します。***フォルダを追加***ボタンを押し、.emlファイル（*保存されたメッセージ*）のあるフォルダを選択します。選択されたフォルダがダイアログに表示されます。

フォルダに以下が含まれます。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。ここでは選択されたフォルダが望ましい（*HAM*）メール、望ましくない（*SPAM*）メールのどちら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することができます。フォルダは学習メールのみを含む必要はありません。また、***フォルダを削除***ボタンをクリックして、リストから選択されたフォルダを削除することができます。

次へをクリックし、***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

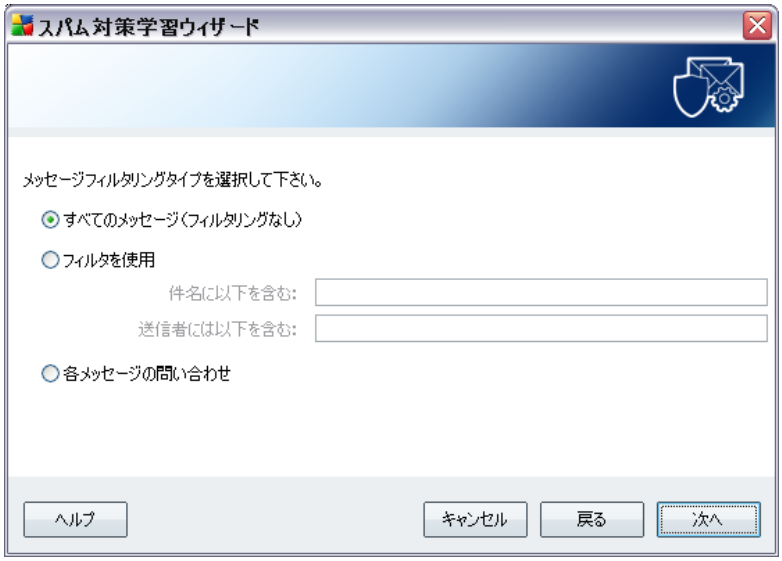
オプションのいずれかを確認した場合、新しいダイアログが表示されます。



注意：*Microsoft Office Outlookの場合、最初にMicrosoft Office Outlookプロファイルを選択します。*

フォルダに以下が含まれます。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。ここでは選択されたフォルダが望ましい（*HAM*）メール、望ましくない（*SPAM*）メールのどちら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することができます。フォルダは学習メールのみを含む必要はありません。選択されたメールクライアントナビゲーションツリーが表示されます。ツリー上で、希望のフォルダ選択します。

次へをクリックし、***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。

選択されたフォルダが学習に使用したいメッセージのみを含む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。

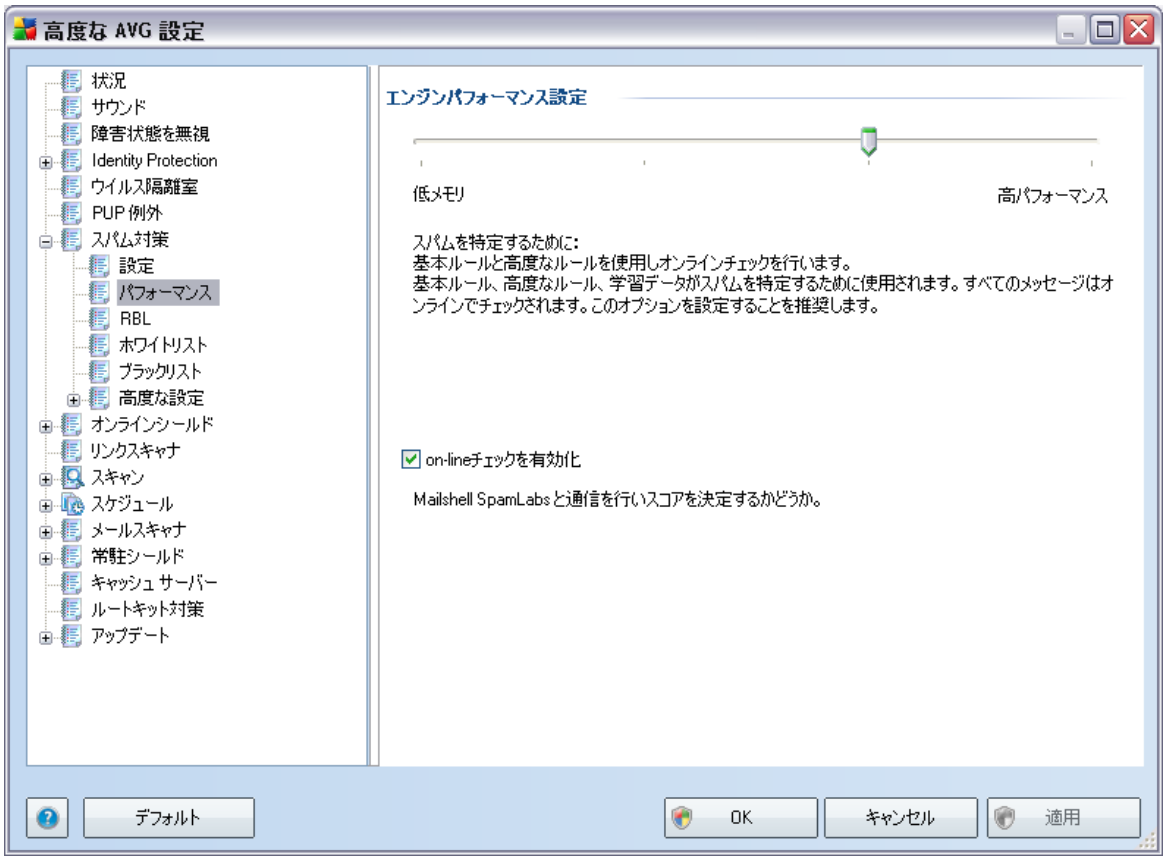
フォルダに含まれるすべてのメッセージについて確認 (学習するかどうかを決定できるように) する場合、***各メッセージを確認*** オプションを選択します。

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。正確に条件にマッチするメッセージ全てが学習に使用されます。

注意！ *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。*

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。

10.7.2. パフォーマンス



エンジンパフォーマンス設定ダイアログ（左側のナビゲーションの***パフォーマンス***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***/***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範囲のレベルを変更します。

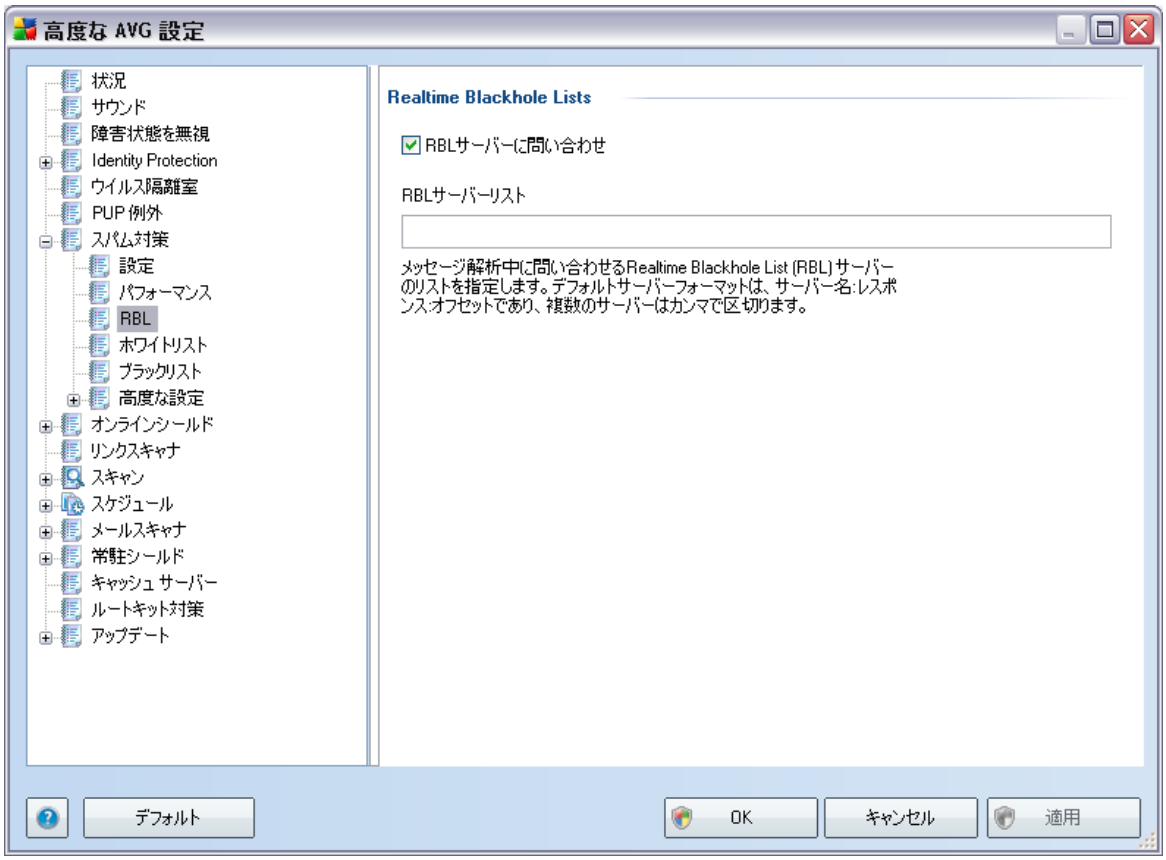
- ***低メモリ*** - スパムを判定するスキャンプロセス中に、ルールは使用されません。トレーニングデータのみが判定に使用されます。このモードは、コンピュータハードウェアが非常に劣っている場合等を除いて、一般の利用には推奨されません。
- ***高パフォーマンス*** - このモードでは大量のメモリを消費します。スパムスキャン中は、以下の機能が使用されます。ルールとスパムデータベースキャッシュ、基本ルール、高度なルール、スパム送信者IPアドレス、スパム送信者データベース。

on-line チェックを有効化はデフォルトでオンとなっています。これにより、Mailshellサーバーとの通信を介して、より正確なスパム***検出が実行されます。例えば、スキャンされたデータは、Mailshellデータベースとオンラインで比較されます。

一般的には、デフォルト設定を保持し、合理的な理由がある場合にのみ変更することを推奨します。この設定の変更は経験のあるユーザーのみが行ってください。

10.7.3. RBL

RBLアイテムは***リアルタイムブラックホールリスト***と呼ばれる編集ダイアログを開きます。



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

RBL(*リアルタイムブラックホールリスト*)サーバーは、既知のスパム送信者の拡張データベースを含むDNSサーバーです。この機能がオンの場合、すべてのメールはRBLサーバーデータベースに対して検証され、このデータベースエントリと一致する場合に、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のフィンガープリントが含まれ、最高で最も正確なスパム検出を提供します。この機能は、特に通常のスパム対策エンジンでは検出されないような大量のスパムを受信するユーザーに適しています。

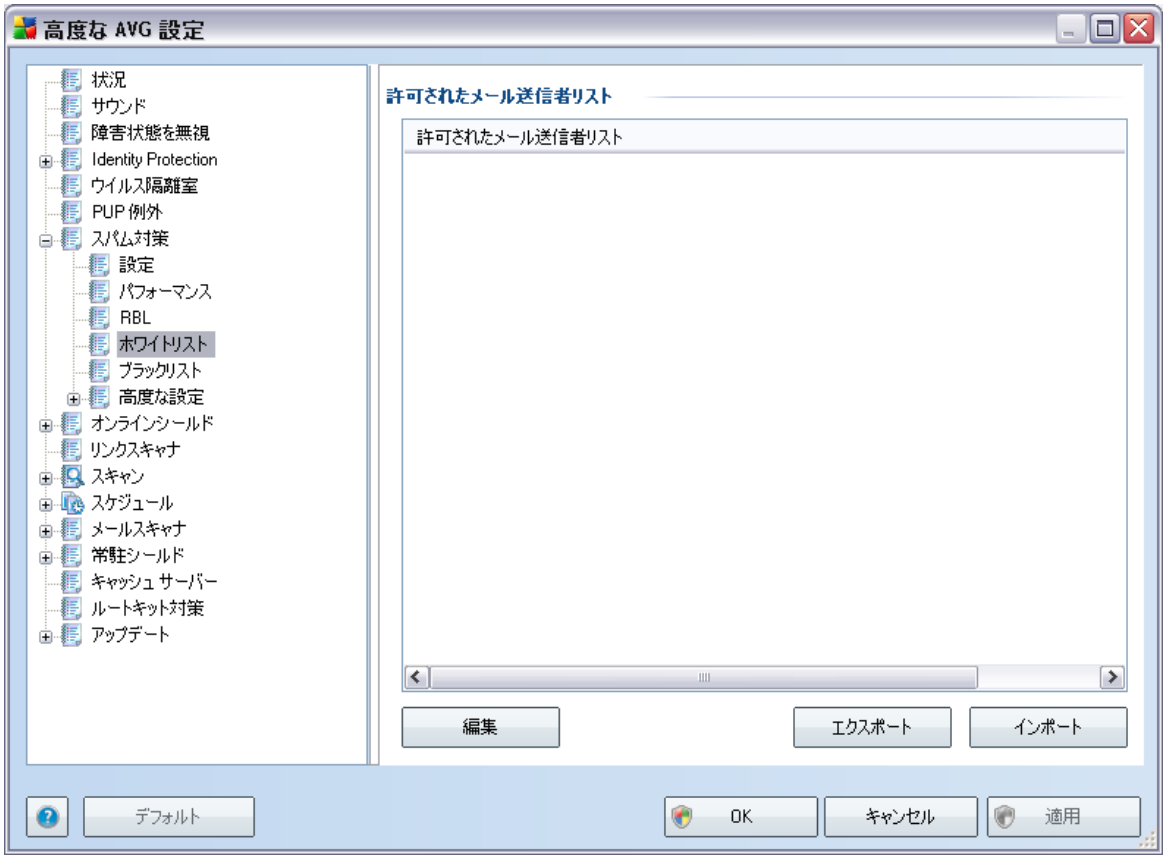
RBLサーバーリストでは、特定のRBLサーバーの場所を定義できます。

注意：*この機能を有効化すると、すべての個々のメッセージがRBLサーバーデータベースに対して検証されるため、一部のシステムと設定では、メール受信プロセスの速度が低下する場合があります。*

いかなる個人データもサーバーには送信されません。

10.7.4. ホワイトリスト

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）が送信されないことが確実である送信者のリストを編集できます。また、スパムメッセージ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。

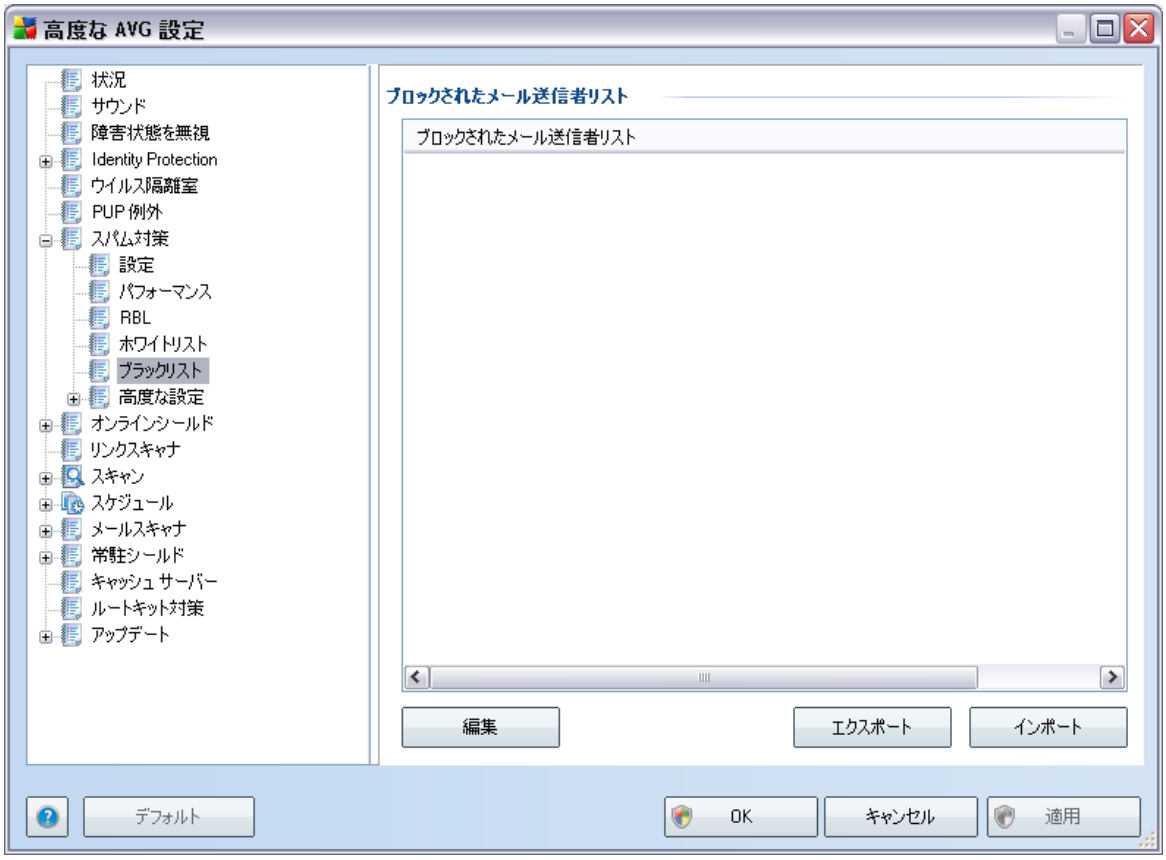
スパム送信者やドメイン名のリストをお持ちの場合、以下の方法でそのリストを入力することができます。各メールアドレスを直接入力、または一度にアドレスの全リストをインポートします。次のコントロー

ルボタンが提供されています。

- ***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*** - なんらかの目的で、レコードをエクスポートする場合は、このボタンを押してください。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。入力ファイルはプレーンテキスト形式であり、1行に1アイテム（*送信者*、*ドメイン名*）が記載されている要があります。

10.7.5. ブラックリスト

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。

スパム送信者やドメイン名のリストをお持ちの場合、以下の方法でそのリストを入力することができます。各メールアドレスを直接入力、または一度にアドレスの全リストをインポートします。次のコントロールボタンが提供されています。

- ***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*** - なんらかの目的で、レコードをエクスポートする場合は、このボタンを押してください。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。入力ファイルはプレーンテキスト形式であり、1行に1アイテム（*送信者*、*ドメイン名*）が記載されている要があります。

10.7.6. 高度な設定

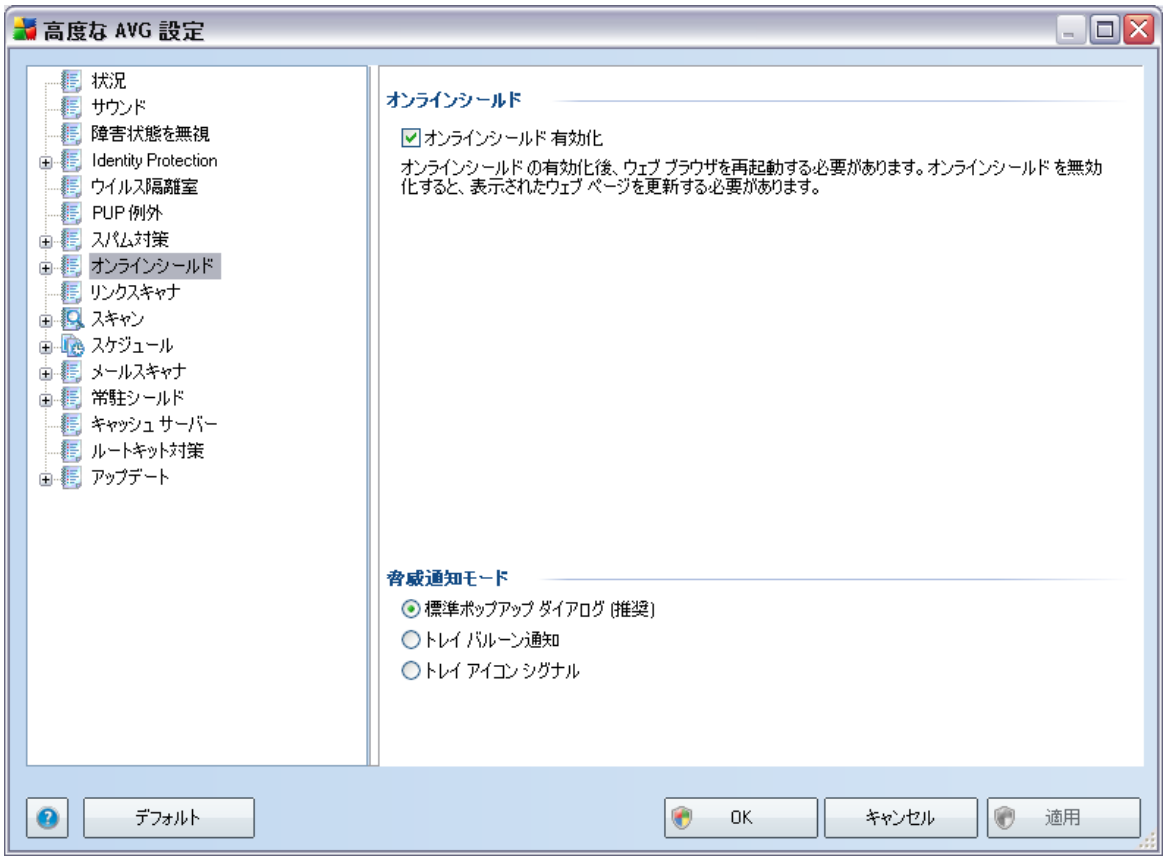
高度な設定の部分には、多数のスパム対策コンポーネントの設定オプションが含まれています。これらの設定は、詳細なスパム対策設定が必要とするネットワーク管理者のような、経験あるユーザー向けです。このため、個々のダイアログに関するこれ以上のヘルプは提供されていません。画面上に各オプションの簡単な説明があります。

Spamcatcher（MailShell Inc.）の高度な設定に精通していない場合は、設定変更を行わないことを推奨します。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。

高度なレベルで***スパム対策***設定を変更する必要があると思う場合、ユーザーインターフェースで直接提供される指示に従ってください。各ダイアログでは、1つの特定機能を確認することができ、それを編集することができます。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、Legit Reputе
- ***トレーニング*** - 最大ワードエントリ、自動トレーニングしきい値、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
- ***RBL*** - RBLサーバー、マルチヒント、閾値、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

10.8. オンライン シールド



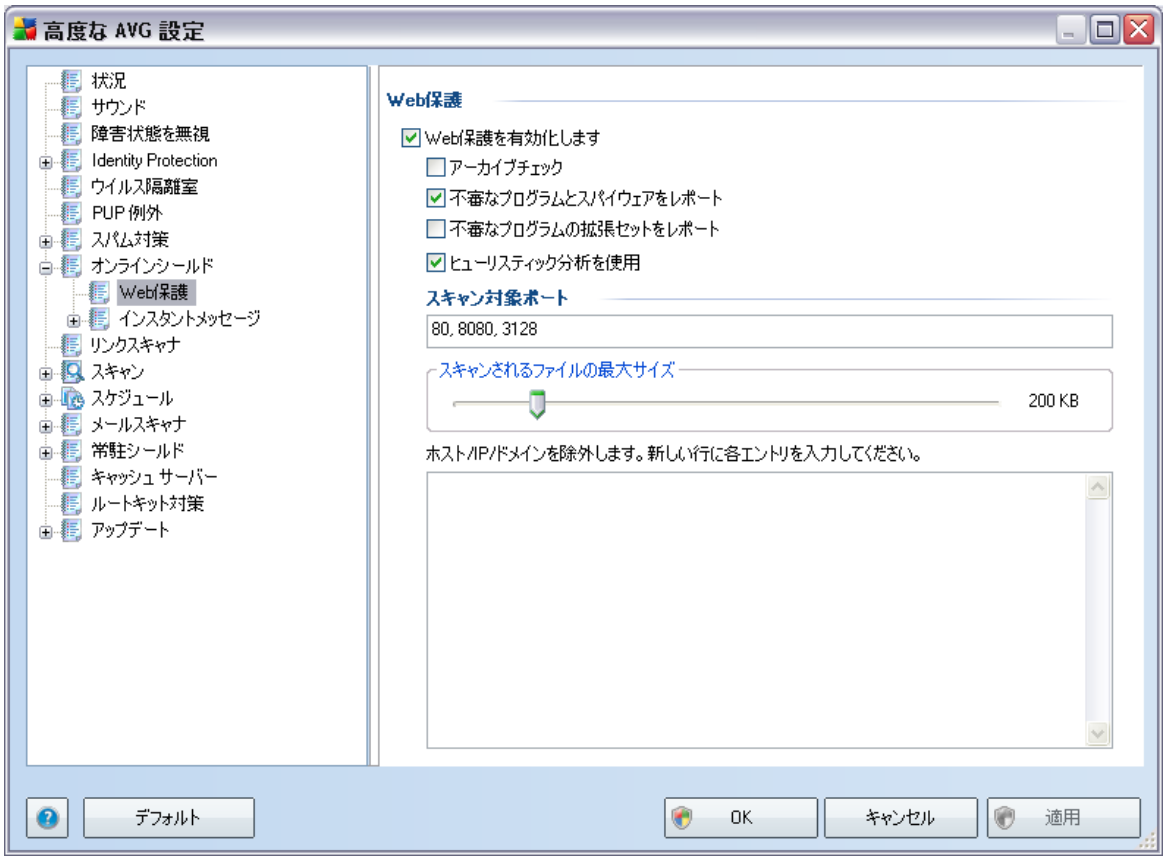
[***Web 保護***] ダイアログでは、[***オンライン シールドを有効化***] オプション (***既定では有効***) を使用して、*オンライン シールド*コンポーネントを有効化/無効化できます。このコンポーネントのさらに高度な設定については、ツリーナビゲーションのリストの後に続くダイアログにしたがってください。

- ***Web保護***
- ***インスタントメッセージ***

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。

10.8.1. Web保護



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。
    - ***アーカイブチェック*** - WWWページに含ま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をレポート*** - (*デフォルトではオン*): 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レポート*** - 前のオプションが有効になっている場合、このボックスにチェックを付けると、スパイウェアの拡張パッケージも検出できます。拡張パッケージとは、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。

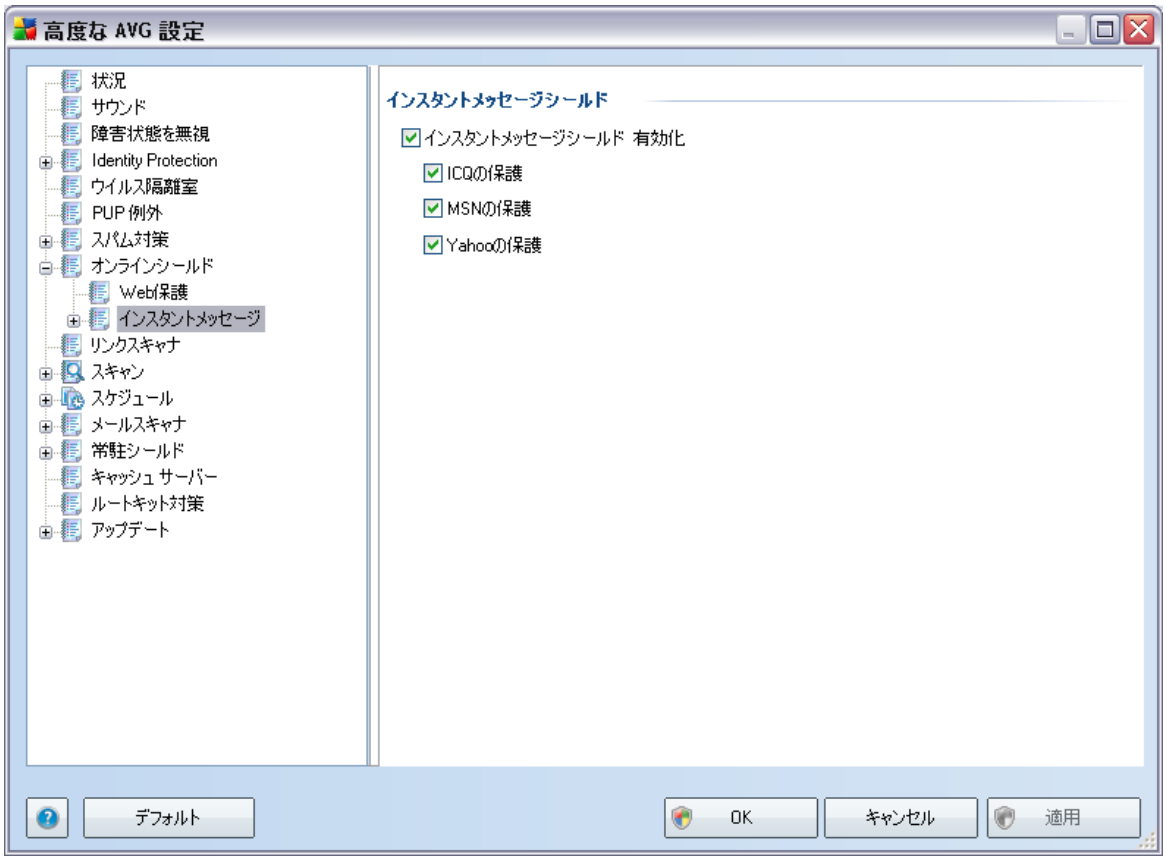
- ***ヒューリスティック分析の使用*** - ヒューリスティック分析（仮想コンピュータ環境でのスキャンオブジェクトの動的エミュレーション）を使用して、表示されるページコンテンツをスキャンします。

- ***スキャン対象ポート*** - この欄には標準http通信ポート番号が表示されます。コンピュータの設定が異なる場合は、必要に応じてポート番号を変更することができます。

- ***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。

10.8.2. インスタントメッセージ

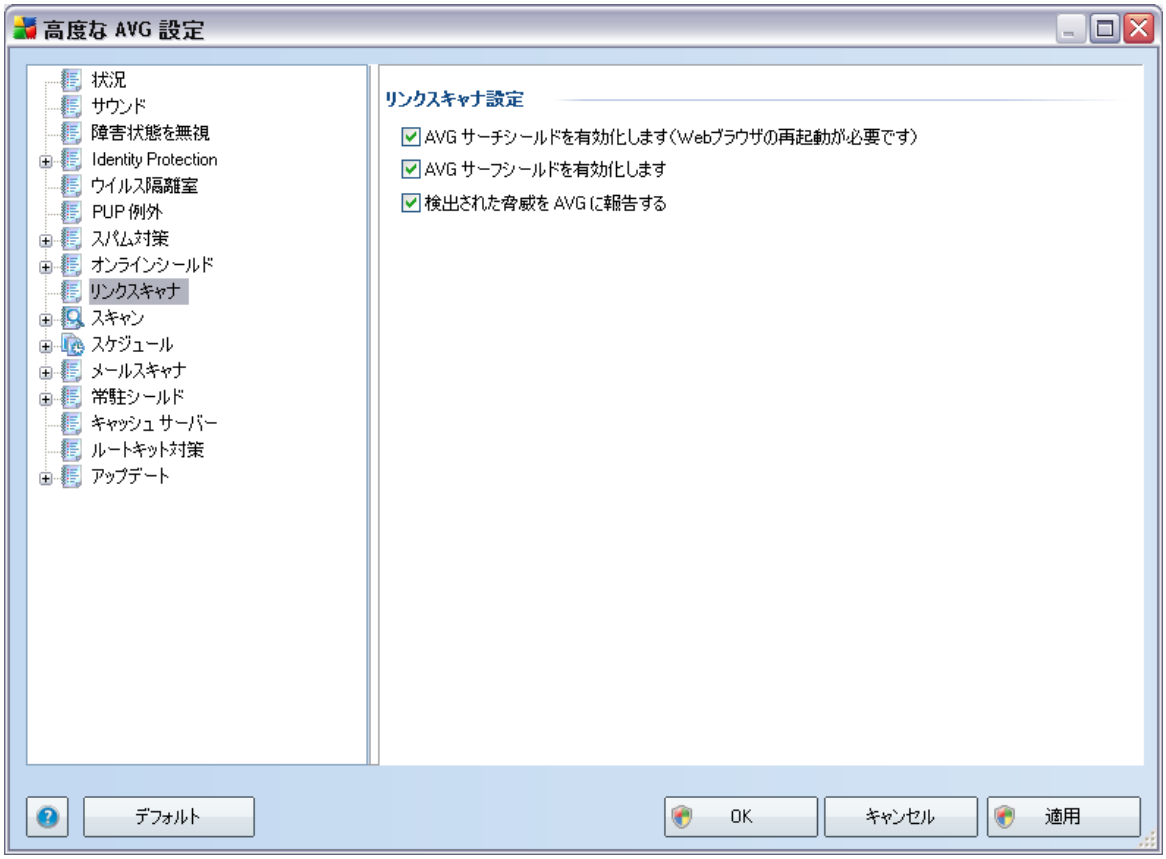


[***インスタント メッセージ シールド***] ダイアログでは、***オンライン シールド***コンポーネントのインスタントメッセージ スキャンに関する設定を編集します。現在は次の 3 つのメッセージング プログラムがサポートされています。***ICQ***、***MSN***、***Yahoo*** - ***オンライン シールド***がオンライン通信がウィルス フリーだということを確認するようにしたい場合は、この中から該当するアイテムをチェックします。

さらに、ユーザーを許可/ブロックする場合、各ダイアログで設定を参照、編集可能です。 ***高度な ICQ***、***高度な MSN***、***高度な Yahoo***)。また、***ホワイトリスト*** *通信を許可されるユーザーのリスト*) と ***ブラックリスト***(*ブロックされるユーザーのリスト*) を指定することができます。

10.9. リンクスキャナ

[***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 シールドを有効化*** - (*デフォルトではオン*) Google、Yahoo、Bing、Yandex、Altavista、百度の検索検索エンジンによる検索結果をあらかじめチェックし、その内容をアイコンで通知します。
- ***サーフシールドを有効化*** - (*デフォルトではオン*) アクセス時のアクティブな (*リアルタイムの*) エクスプロイトサイトに対する保護。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。
- ***検出された脅威の AVG への報告を有効化*** - (*デフォルトではオン*) : この項目をチェックすると、***AVG セーフサーフ***あるいは***AVG セーフサーチ***によって検出されたエクスプロイトと悪意のあるサイトのレポートを許可し、悪意のある活動に関する情報を収集しているデータベー

スに送信されます。

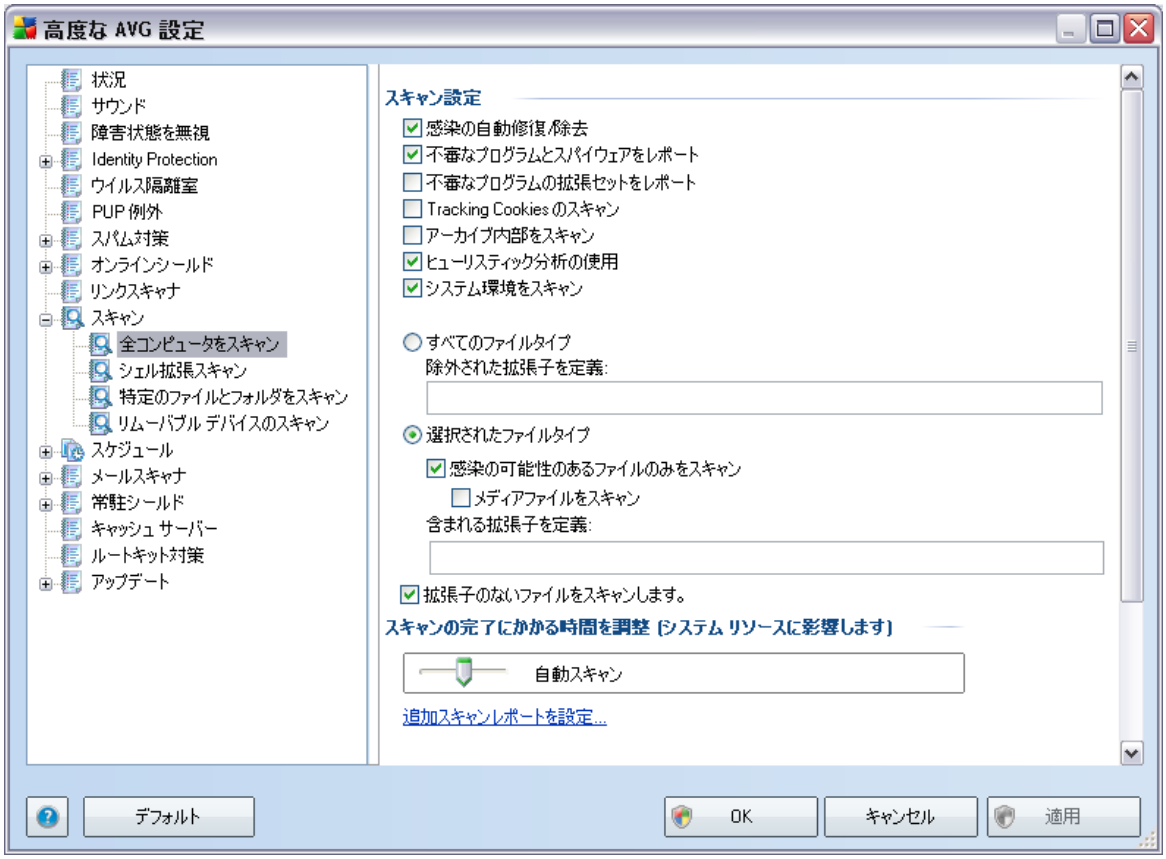
10.10. スキャン

高度なスキャン設定は3つのカテゴリに分けられ、このカテゴリはソフトウェアベンダーによって定義され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*** - 予め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。
- ***特定ファイルまたはフォルダのスキャン*** 予め定義されたコンピュータの特定エリアのスキャンです。
- ***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

10.10.1. 全コンピュータをスキャン

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によってあらかじめ定義されたスキャンパラメータ、***完全コンピュータスキャン***を編集することができます。



スキャン設定

スキャン設定セクションでは、オン/オフ可能なスキャンパラメータが表示されます。

- ***感染の自動修復/除去*** - デフォルトではオン) ウイルスがスキャン実行中に検出され、修復可能な場合、自動で修復されます。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をレポート*** - (*デフォルトではオン*): 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レポート*** - 前のオプションが有効になっている場合、このボックスにチェックを付けると、スパイウェアの拡張パッケージも検出できます。拡張パッケージとは、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。

- ***Tracking Cookie をスキャン*** - スパイウェア対策コンポーネントのこのパラメータは、スキャン実行中に Cookie が検出されるように定義します。(*HTTP cookie は、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ユーザーの特定の情報の認証、トラッキング、メンテナンスに使用されます*)

- ***アーカイブ内部をスキャン*** - ZIPやRAR等のアーカイブ内に格納されている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*** - (デフォルトではオン) 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*) は、スキャン実行中にウイルス検出に使用される方法の1つです。

- ***システム環境をスキャン*** - コンピュータのシステムエリアの部分もスキャンチェックします。

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。

- ***選択されたファイルタイプ*** - 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 - これらのファイルは多くの場合、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している場合、スキャン時間がさらに短縮されます*) が含まれます。ここでも、必ずスキャンする必要があるファイルの拡張子を指定できます。

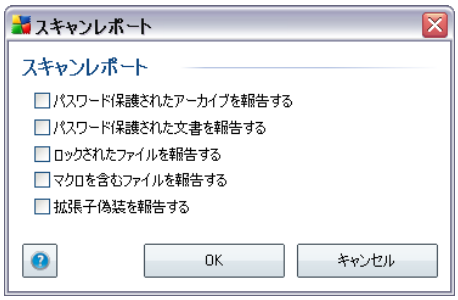
- オプションとして、***拡張子のないファイルをスキャン***できます。このオプションは既定ではオンになっています。変更する理由がない場合は、この設定を保持することをお勧めします。拡張子のないファイルは不審なものであり、常にスキャンするべきです。

スキャン処理優先度

スキャン処理優先度セクションでは、システムリソース使用度に応じて、希望するスキャン速度を指定することができます。デフォルトでは、このオプションの値は、自動的にリソースを使用する中レベルの値に設定されています。スキャンの速度を上げたい場合、スキャンにかかる時間を削減することができますが、スキャン実行中、システムリソース使用度は著しく上がり、PC上の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等に適しています。*)一方、スキャンの時間を延長することで、システムリソース使用度を下げることができます。

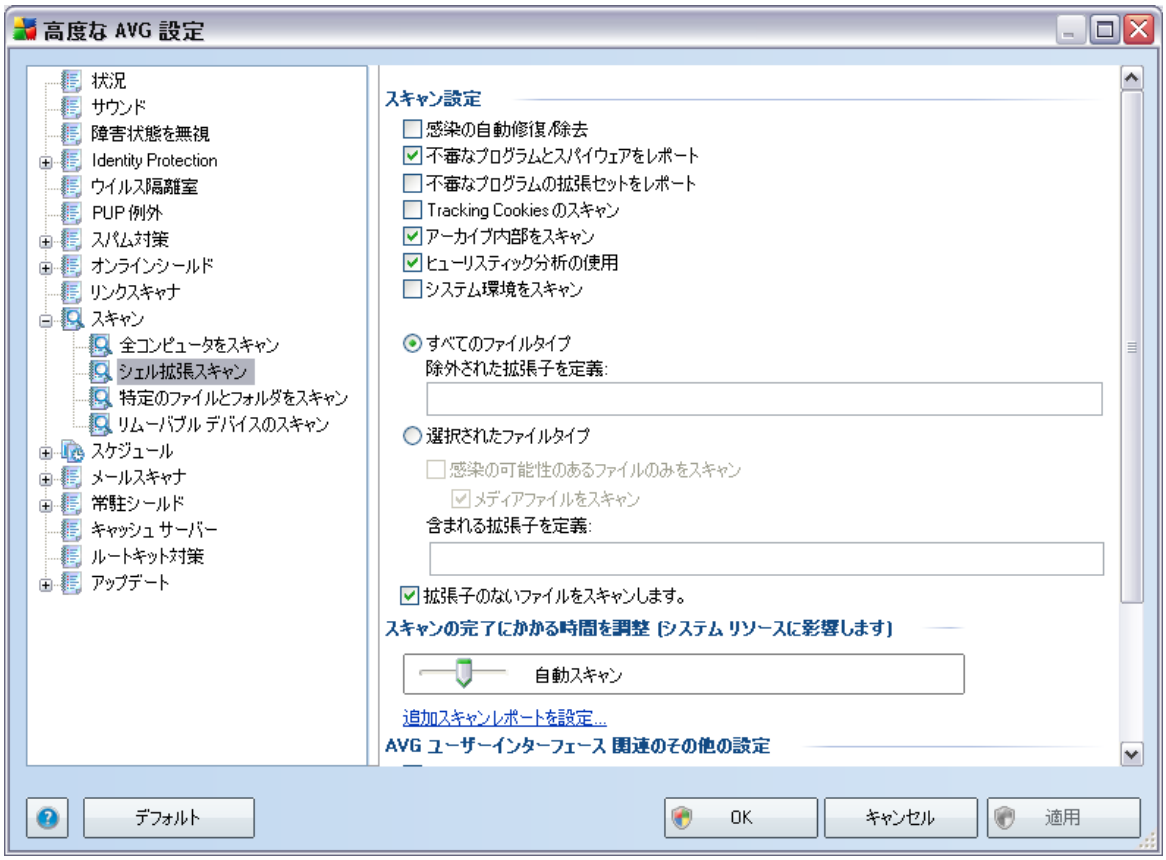
追加スキャンレポートを設定...

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、レポートされる検出項目を設定します。



10.10.2. シェル拡張スキャン

このアイテムは***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、あらかじめ定義されたスキャンを編集することができます。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。

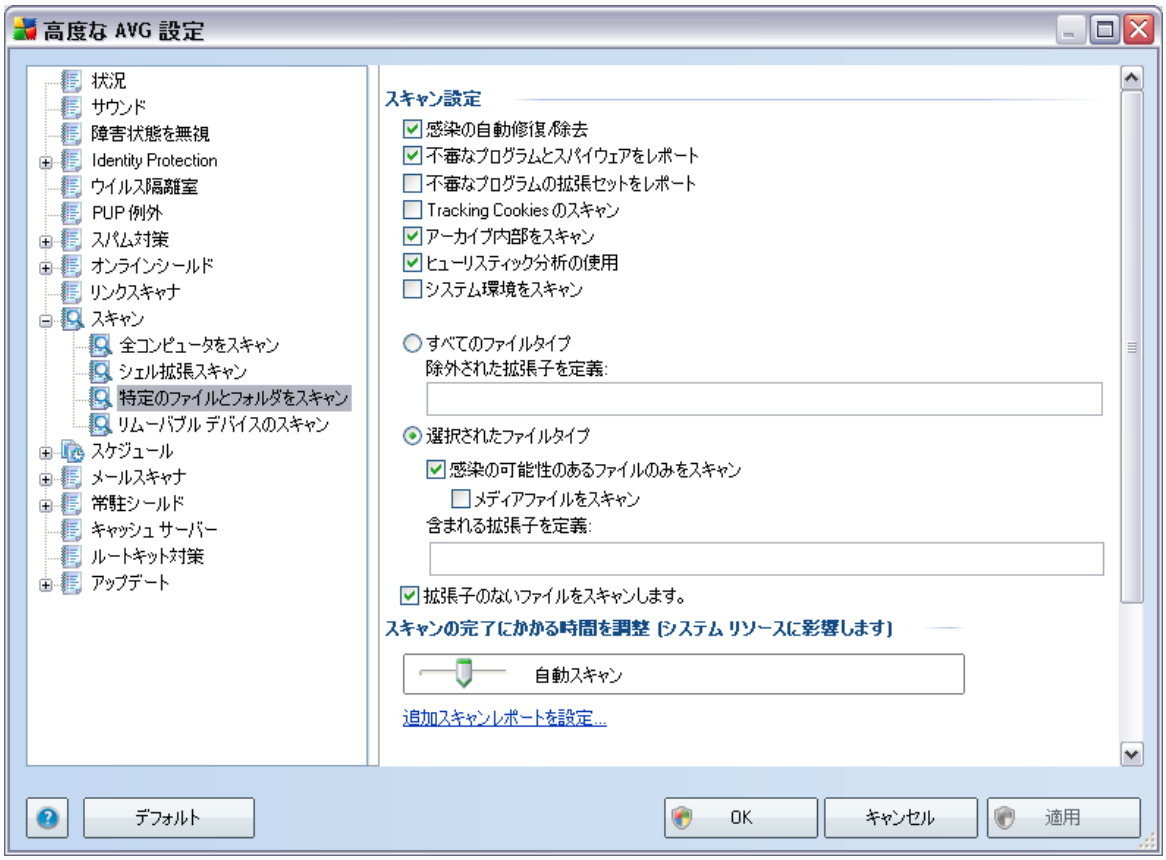


パラメータのリストは***完全 コンピュータスキャン***で利用できるものと同一です。ただし、デフォルト設定が異なります。***完全 コンピュータスキャン***では、ほとんどのパラメータは選択されていますが、***シェル拡張スキャン***(*Windows Explorerのスキャン*) では、関連パラメータのみがオンとなっています。

注意 :*各パラメータの説明については、**AVG高度な設定 / スキャン/ 完全スキャン**の章を参照してください。*

10.10.3. 特定のファイルやフォルダをスキャン

選択領域スキャンの編集インターフェースは***完全スキャン***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。

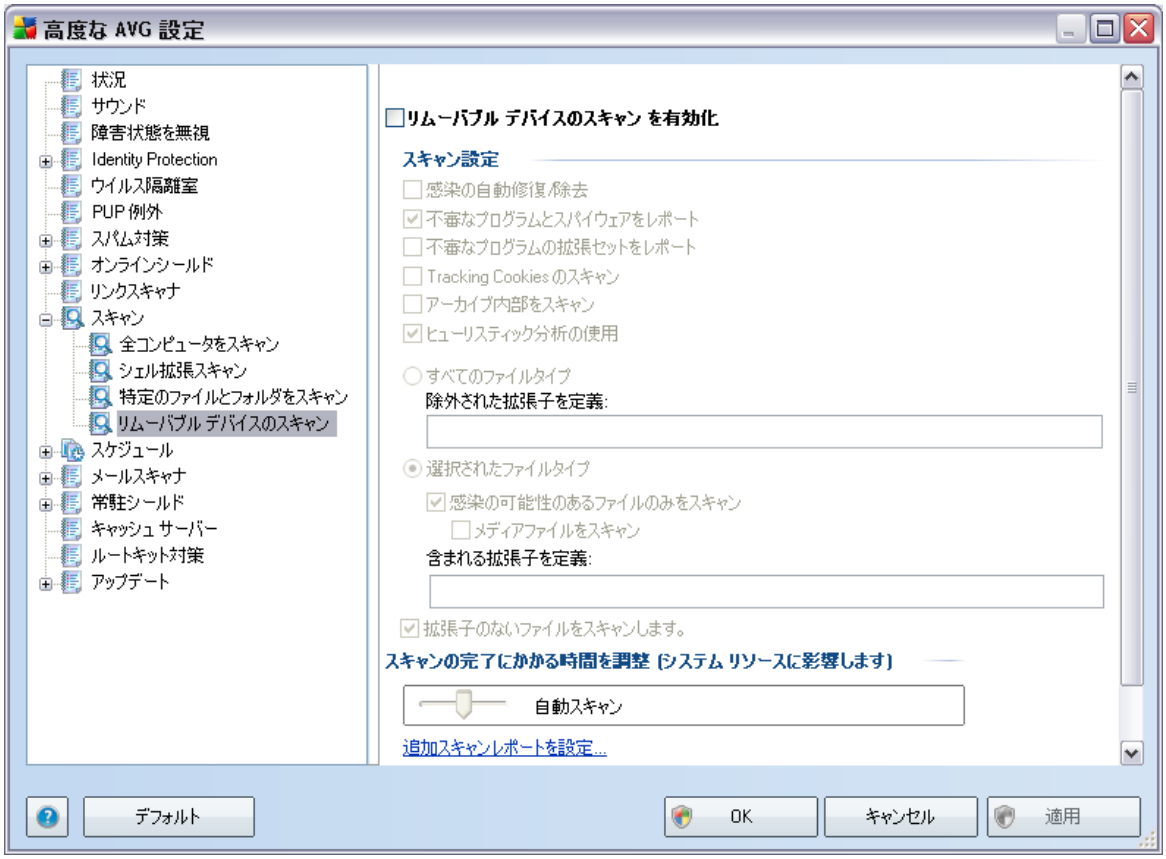


この設定ダイアログで設定されるすべてのパラメータは、***特定のファイルとフォルダをスキャン***で選択されたスキャンエリアのみに適用されます。

注意：*各パラメータの説明については、**AVG 高度な設定 / スキャン/ 完全スキャン**の章を参照してください。*

10.10.4. リムーバブルデバイスのスキャン

また、[***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。

注意 :*各パラメータの説明については、****AVG 高度な設定 / スキャン/ 完全スキャン****の章を参照してください。*

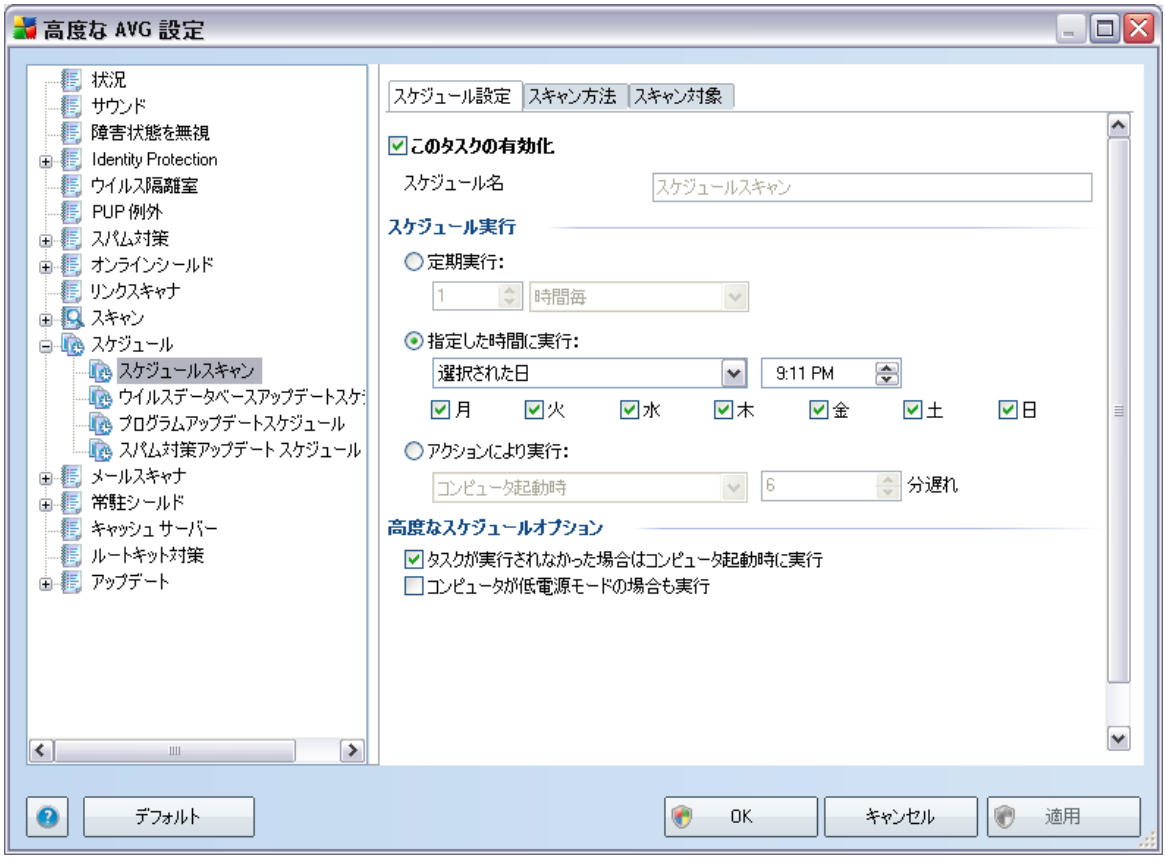
10.11. スケジュール

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。

- 完全スキャンスケジュール
- ウイルスデータベースアップデートスケジュール
- 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

10.11.1. スケジュール済スキャン

*スケジュール済スキャン（または新しいスケジュール設定）*のパラメータは、3つのタブで編集することができます。



[***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、[***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

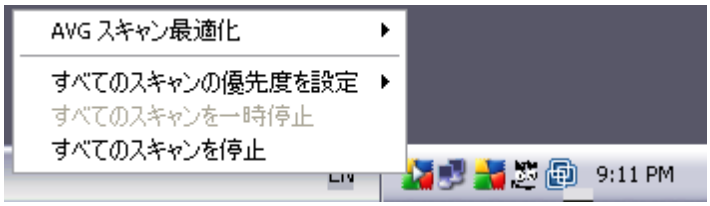
ここでは、新しくスケジュールされたスキャンを起動する時間間隔を指定できます。特定の期間が経過した後に繰り返しスキャンを起動（***定期実行...***）、正確な日時を定義（***特定の時間間隔で実行...***）または、スキャン起動のトリガとなるイベントを定義（***コンピュータ起動時のアクションベース***）することでタイミングを定義できます。

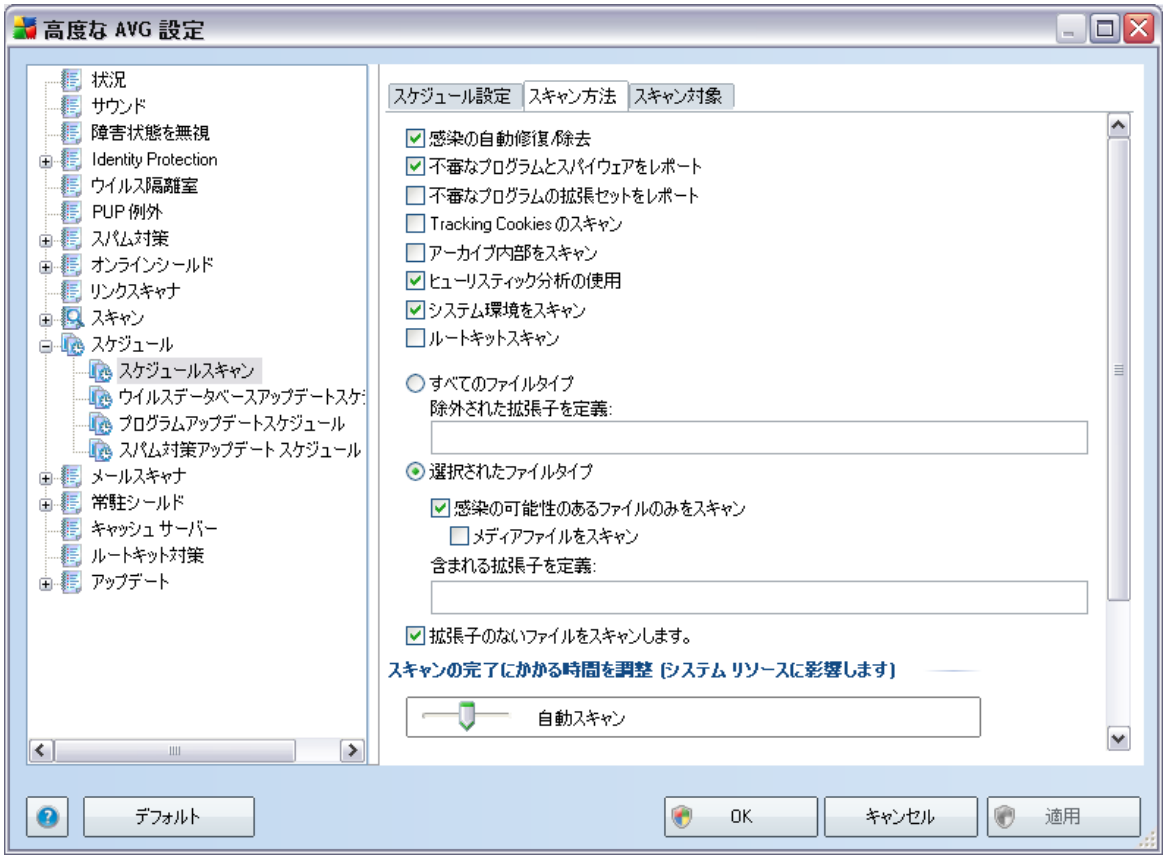
高度なスケジュールオプション

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、スケジュール済み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（*白の矢印の付いた全色で表示されます。上の画像を参照*）が表示されます。実行中のスキャン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、実行中のスキャンを一時停止あるいは停止することができます。





スキャン方法タブには、任意でオン/オフできるスキャンパラメータのリストが表示されます。デフォルトでは、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、予め定義された設定を維持することを推奨します。

- ***感染の自動修復/除去*** - (デフォルトではオン) ウイルスがスキャン実行中に検出され、修復可能な場合、自動で修復されます。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をレポート*** - (*デフォルトではオン*): 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レポート*** - 前のオプションが有効になっている場合、このボックスにチェックを付けると、スパイウェアの拡張パッケージも検出できます。拡張パッケージと

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。

- ***Tracking Cookie をスキャン*** - (*デフォルトではオン*) スパイウェア対策 ***コンポーネントのこのパラメータは、スキャン実行中に Cookie が検出されるように定義します。*** (*HTTP cookie は、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ユーザーの特定の情報の認証、トラッキング、メンテナンスに使用されます*)

- ***アーカイブ内部をスキャン*** - (*デフォルトではオン*) このパラメータは、ZIPやRAR等のアーカイブ形式で格納されている場合でも、すべてのファイルがスキャンされるように設定します。

- ***ヒューリスティック分析を使用*** - (*デフォルトではオン*) 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*) は、スキャン実行中にウイルス検出に使用される方法の1つです。

- ***システム環境をスキャン*** - (*デフォルトではオン*) コンピュータのシステムエリアもチェックされます。

- ***ルートキットをスキャン*** - 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する場合、この項目にチェックを付けます。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行うことができます。

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。

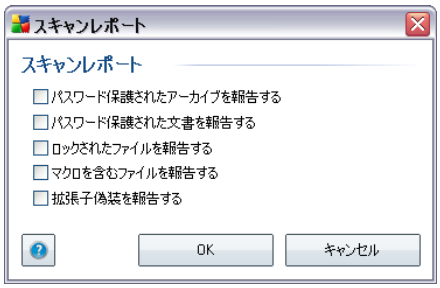
- ***選択されたファイルタイプ*** - 感染の可能性のあるファイルのみを指定できます (*一部のプレーンテキストファイルやその他の非実行可能ファイルなど、感染の可能性がないファイルはスキャンされません*)。これには、メディアファイル (*ビデオ、オーディオファイル - これらのファイルは多くの場合、サイズが非常に大きく、ウィルスに感染している可能性が非常に低いため、このボックスのチェックを外している場合、スキャン時間がさらに短縮されます*) が含まれます。ここでも、必ずスキャンする必要があるファイルの拡張子を指定できます。

- オプションとして、***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なものであり、常にスキャンするべきです。

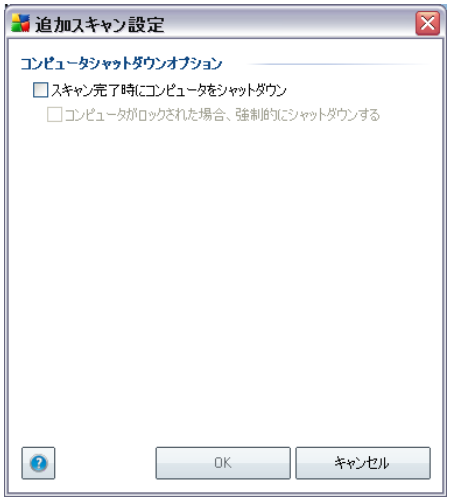
スキャン処理優先度

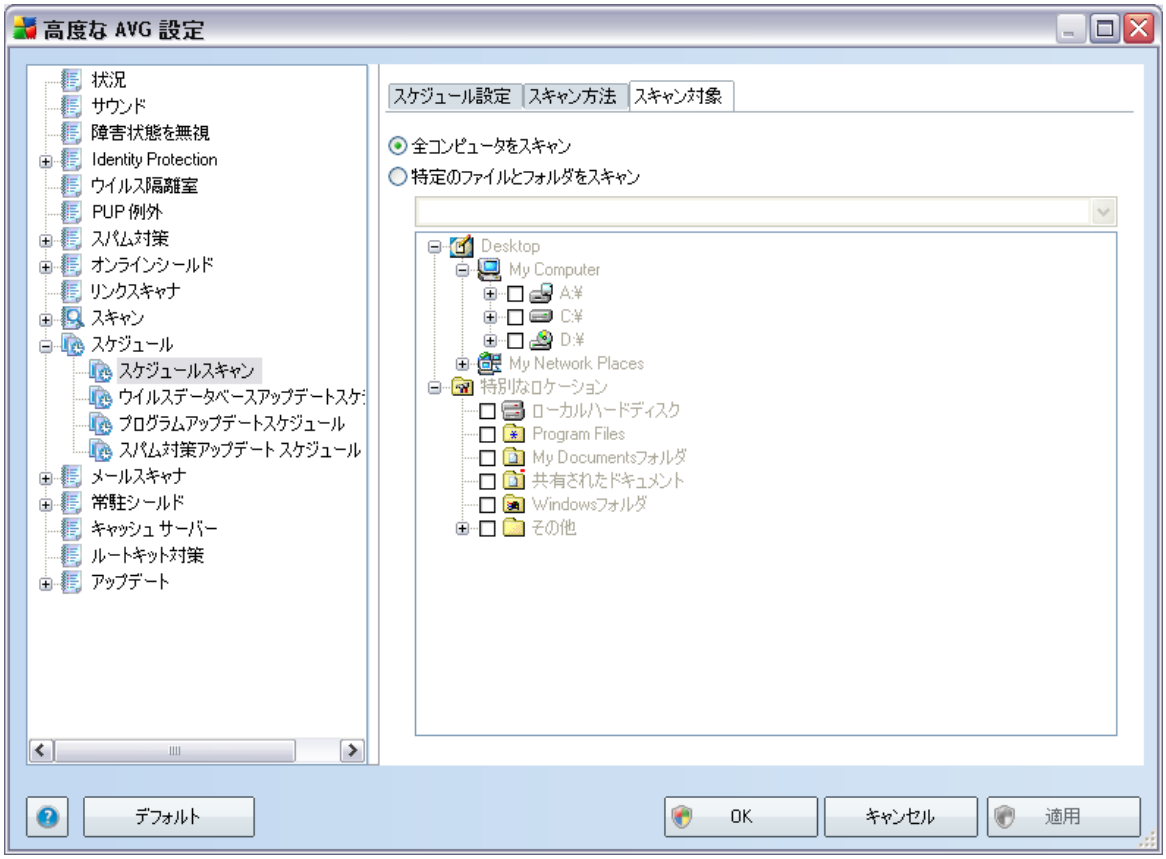
スキャン処理優先度セクションでは、システムリソース使用度に応じて、希望するスキャン速度を指定することができます。デフォルトでは、このオプションの値は、自動的にリソースを使用する中レベルの値に設定されています。スキャンの速度を上げたい場合、スキャンにかかる時間を削減することができますが、スキャン実行中、システムリソース使用度は著しく上がり、PC上の他の作業の速度が低下します。(*このオプションは、コンピュータの電源がオンであり、コンピュータ上で作業をしているユーザーがいない場合等に適しています。*)一方、スキャンの時間を延長することで、システムリソース使用度を下げることができます。

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、レポートされる検出項目を設定します。



追加スキャン設定 ... をクリックすると、***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、スキャンプロセス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***)確定すると、現在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***)が有効化されます。





[***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。

10.11.2. ウイルスデータベースアップデートスケジュール

[***スケジュール設定***] タブでは、[***このタスクの有効化***] アイテムにチェックを付けたり外したりすることによって、必要に応じて、簡単にスケジュール済みのウイルスデータベースアップデートを一時的に非アクティブにしたり、再度オンに切り替えたりすることができます。基本的なウイルスデータベースアップデートスケジュールは***アップデートマネージャ***コンポーネントに含まれます。このダイアログでは、一部の詳細なウイルスデータベース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

このセクションでは、新しくスケジュールされたウィルスデータベースを起動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。

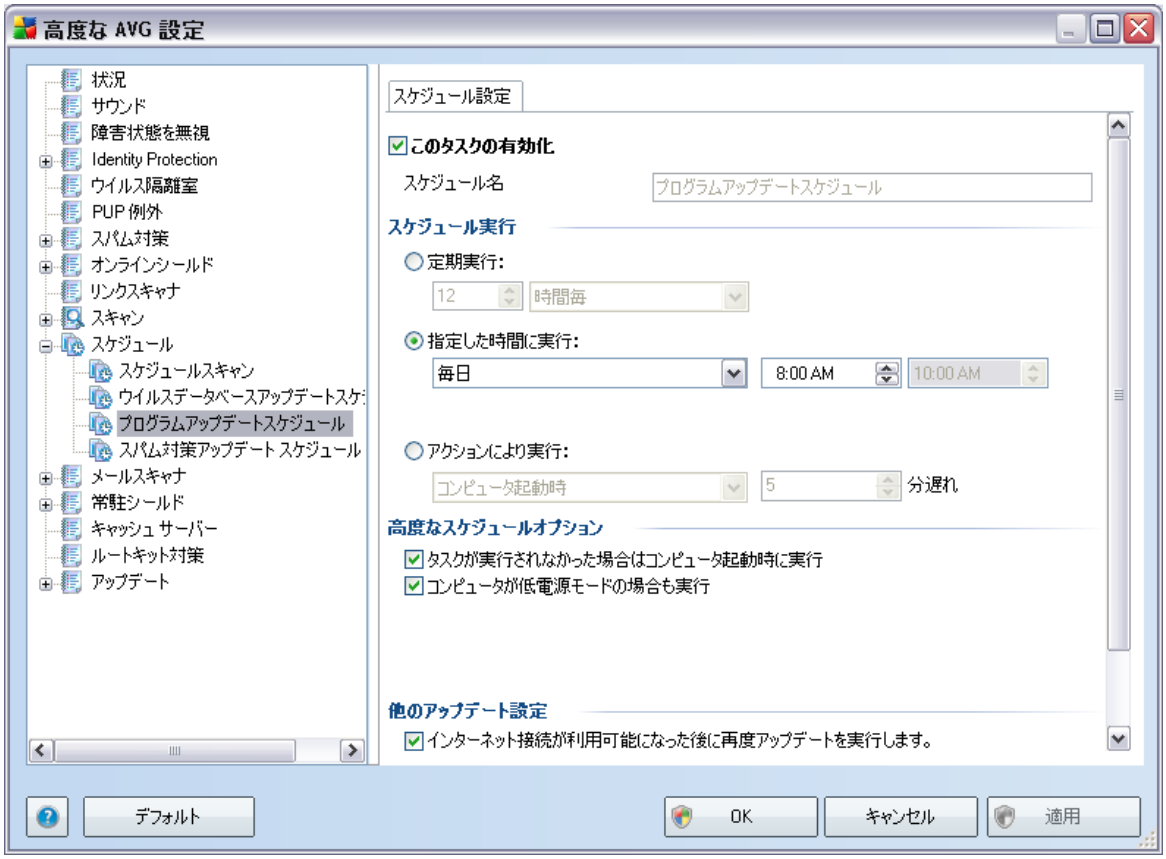
高度なスケジュールオプション

このセクションでは、コンピュータが低電源モードあるいは完全に電源オフになっている場合に、ウイルスデータベース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

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）。



[***スケジュール設定***] タブでは、[***このタスクの有効化***] アイテムにチェックを付けたり外したりすることによって、必要に応じて、簡単にスケジュール済みのプログラムアップデートを一時的に無効にしたり、再度有効に切り替えたり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。

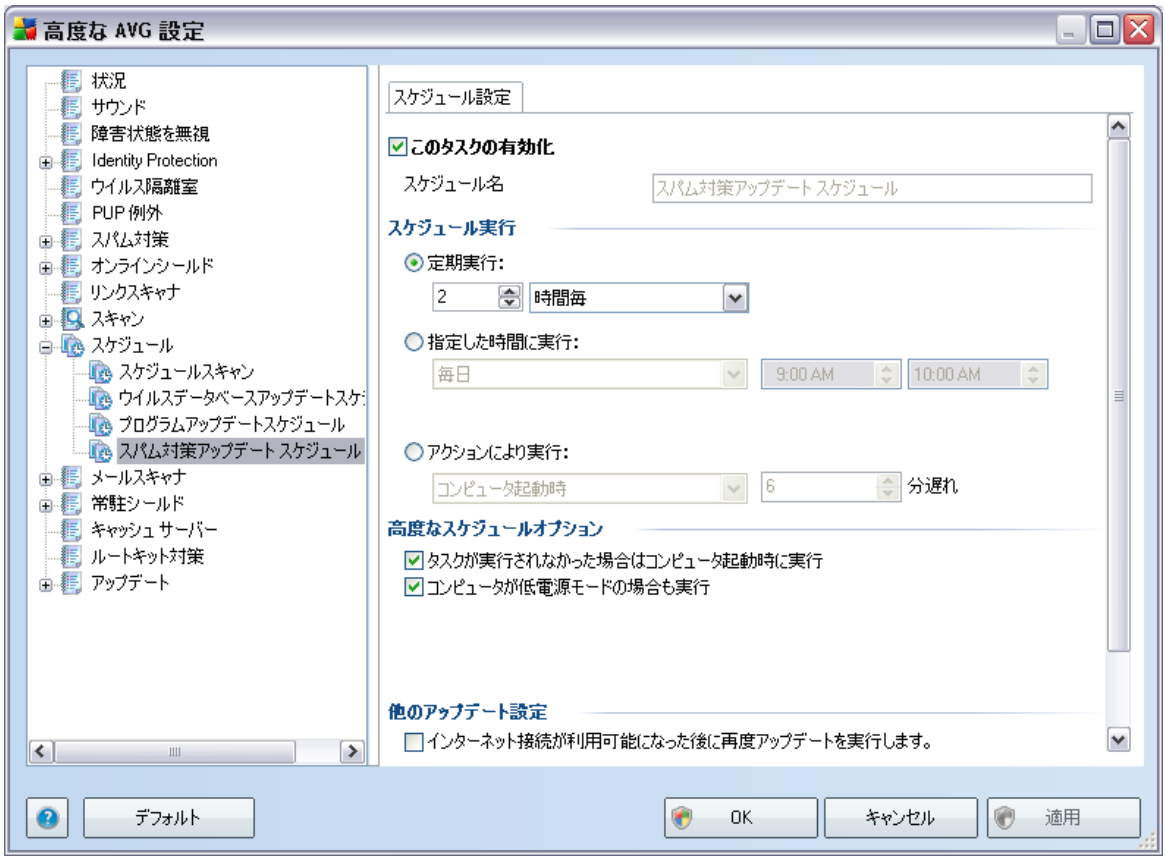
他のアップデート設定

[***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）。

注意: *スケジュール済みプログラムアップデートおよびスケジュール済みスキャンの時間と一致する場合は、アップデートプロセスが最優先され、スキャンは中断されます。*

10.11.3. スパム対策アップデートスケジュール



[***スケジュール設定***] タブでは、[***このタスクの有効化***] アイテムにチェックを付けたり外したりすることによって、必要に応じて、簡単にスケジュール済みの***スパム対策***アップデートを一時的に非アクティブにしたり、再度オンに切り替えたりすることができます。基本***スパム対策***アップデートスケジュールは***アップデートマネージャ***コンポーネントに含まれます。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。タイミングは、ある期間の後に (***...ごとに実行***) の繰り返される***スパム対策***更新起動を定義することによって、あるいは正確な日時 (***特定の時間...に実行***) を定義することによって、あるいは、アップデート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***) を定義することによっても可能です。

高度なスケジュールオプション

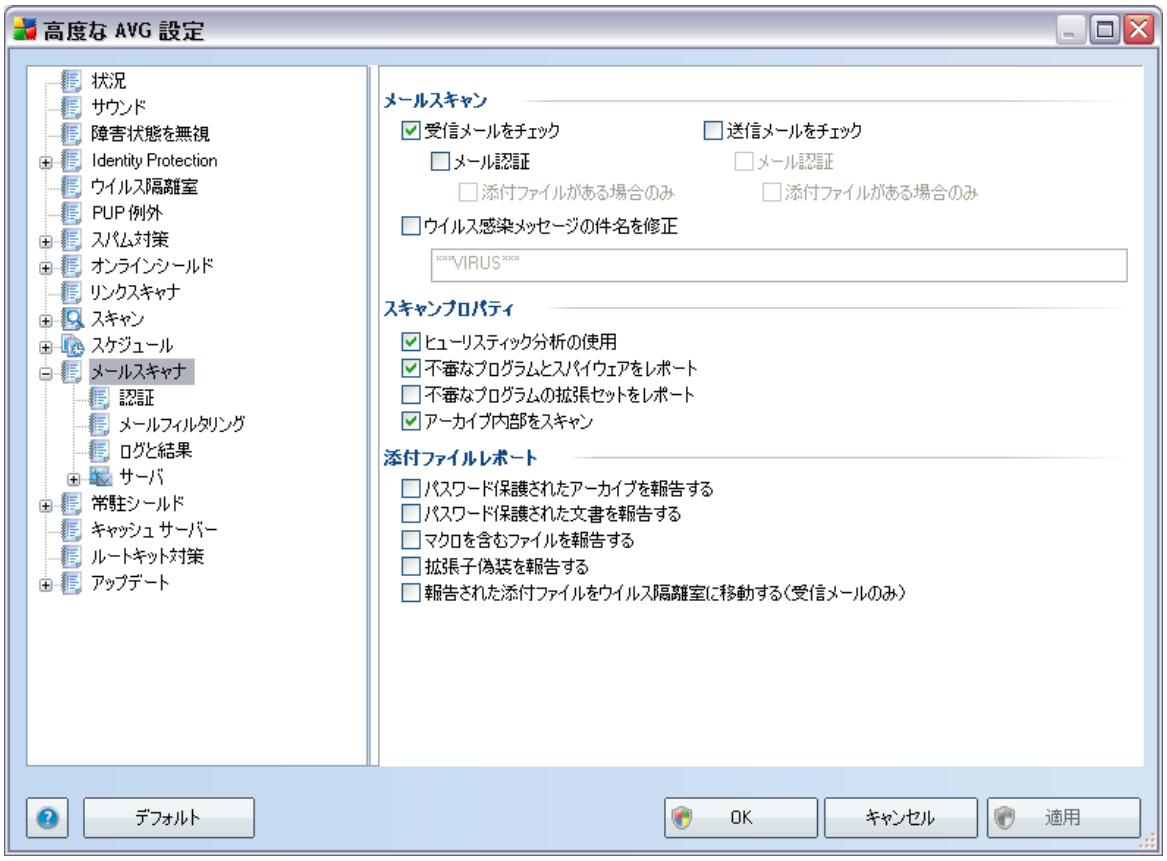
このセクションでは、コンピュータが低電源モードあるいは完全に電源オフになっている場合に、***スパム対策***アップデートが実行される条件を定義します。

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、***スパム対策***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)。

10.12. 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 スキャナ*** - このセクションでは、これらの送受信メールの基本項目を設定することができます。
    - o メールのウイルススキャンを実行する場合、
    - o 各メッセージの最後にウイルスが含まれていないことを示す認証テキストを追加する場合、テキストは、[認証] ダイアログで調整できます。
    - o 添付ファイルを含むメッセージにのみ認証テキストを追加する場合、

ウイルス感染メッセージの件名を修正、このチェックボックスにチェックを付け、テキストフィールドに希望する値を入力してください。その値は、より簡単に感染を特定し、フィルタリングするために、感染したメールの件名フィールドに追加されます。初期値は*** VIRUS*** であり、この値

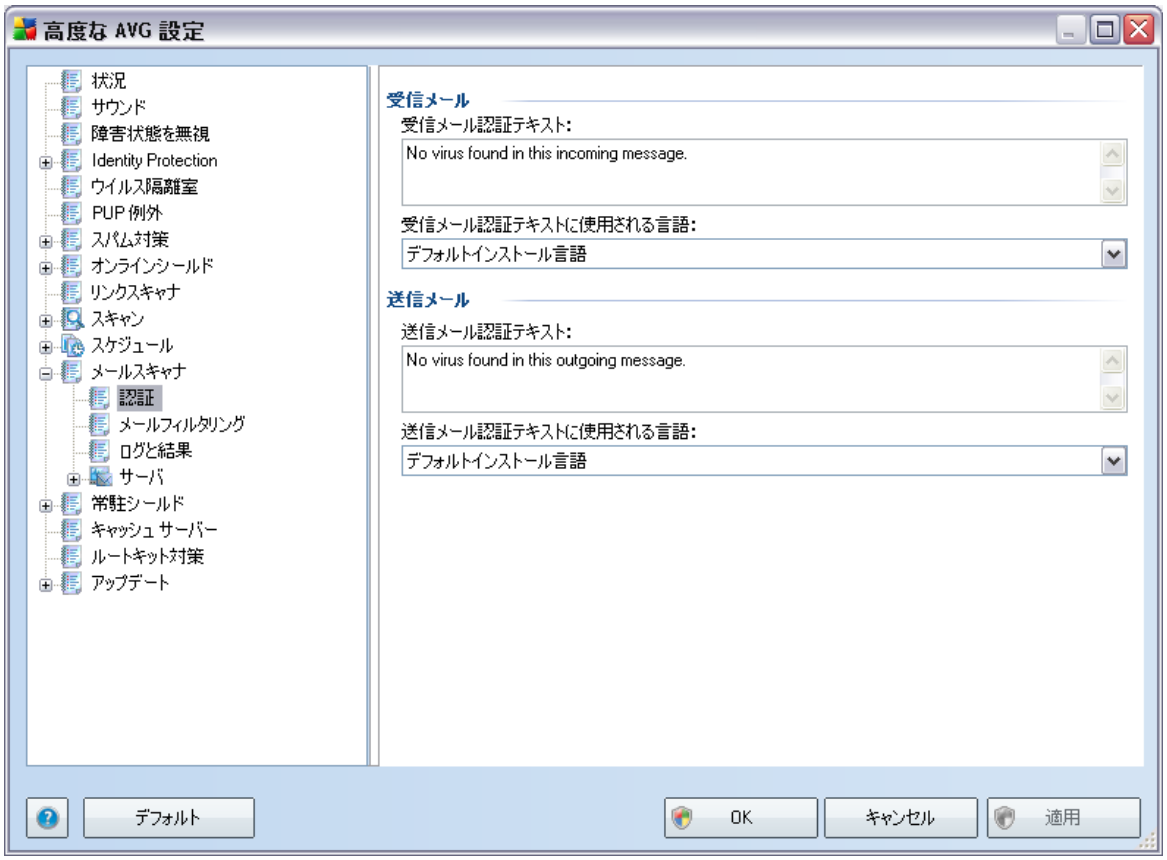
を使用することを推奨します。

- ***スキャン プロパティ*** - このセクションでは、メールがスキャンされる方法を指定することができます。
    - ***ヒューリスティック分析を使用*** - 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を使用する場合はチェックしてください。このオプションがオンの場合、メール添付ファイルを拡張子だけでなく、実際の添付ファイルの内容を考慮してフィルタできます。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をレポート*** - (*デフォルトではオン*): 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レポート*** - 前のオプションが有効になっている場合、このボックスにチェックを付けると、スパイウェアの拡張パッケージも検出できます。拡張パッケージとは、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。
    - ***アーカイブ内部をスキャン*** - メールメッセージに添付されたアーカイブの内容をスキャンする場合にチェックします。
- ***添付ファイル レポート*** - このセクションでは、潜在的に危険あるいは疑わしい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等) は、ウイルススキャンできません。潜在的に危険なものとして報告する場合はボックスをチェックします。
    - ***パスワード保護された文書を報告する*** - パスワード保護された文書はウイルススキャンできません。潜在的に危険なものとして報告する場合はボックスをチェックします。
    - ***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に予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。) マクロは潜在的に危険な命令を含むことがあります。ボックスにチェックを付けると、マクロを含むファイルが疑わしいものとして報告されます。

- ***拡張子偽装を報告する*** – 例えば、疑わしい実行可能ファイル「something.txt.exe」が、無害なテキストファイル「something.txt」と偽装されている場合があります。潜在的に危険なものとしてレポートする場合はボックスをチェックします。

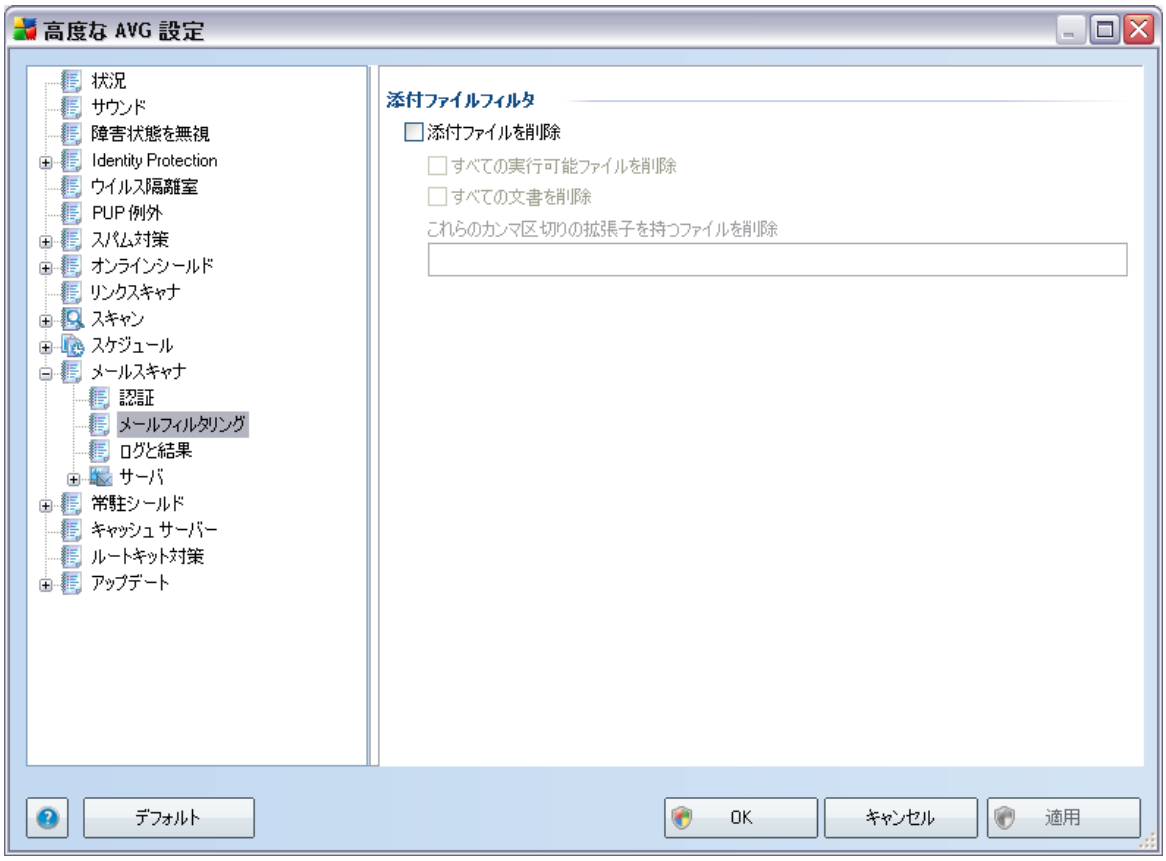
- ***レポートされたメール添付ファイルをウィルス隔離室に移動*** - 添付ファイルがパスワード保護されたアーカイブ、パスワード保護されたドキュメント、マクロを含むファイル、拡張子偽装を含む場合、それらをレポートするかどうかを指定します。このようなメールがスキャン中に検出された場合、検出された感染オブジェクトを***ウイルス隔離室***に移動するかどうかについても指定することができます。

10.12.1. 認証



認証ダイアログでは、認証テキストの内容と言語を指定します。これは***受信メール***と***送信メール***で個別に指定できます。

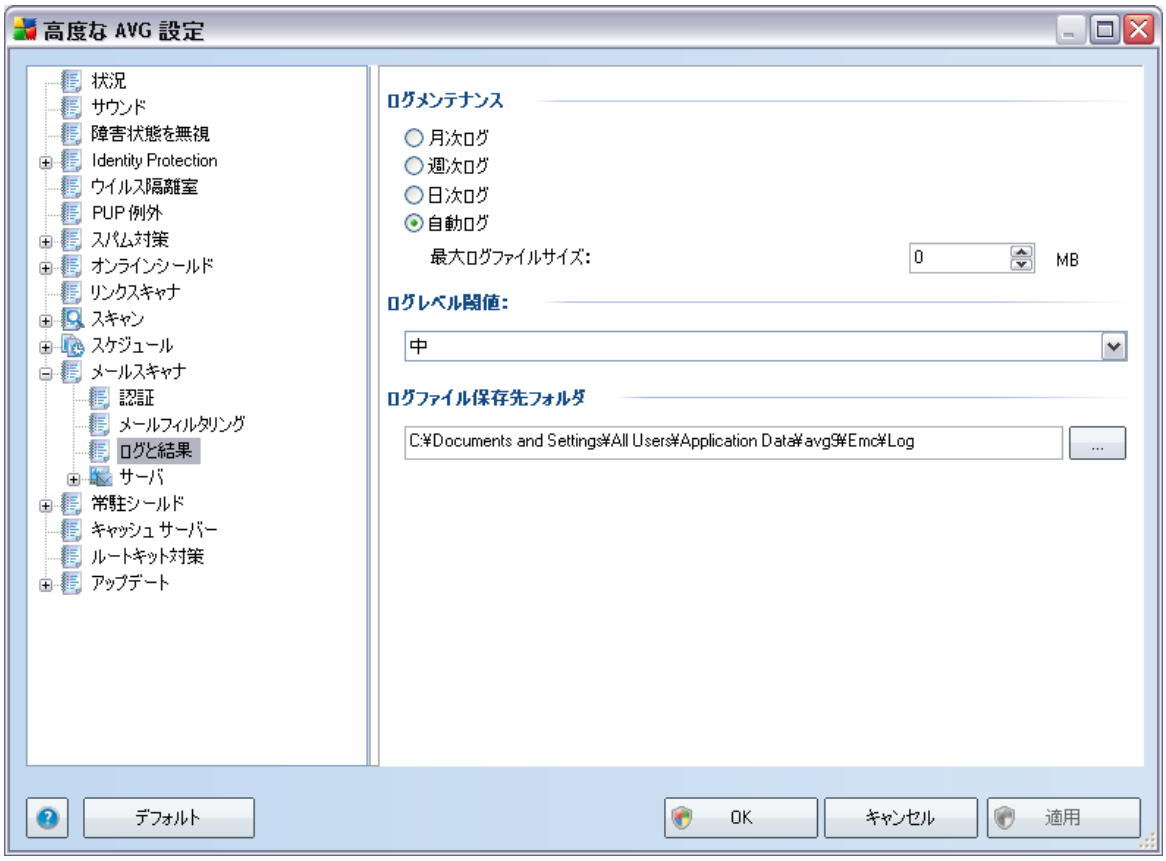
10.12.2. メールフィルタリング



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

10.12.3. ログと結果

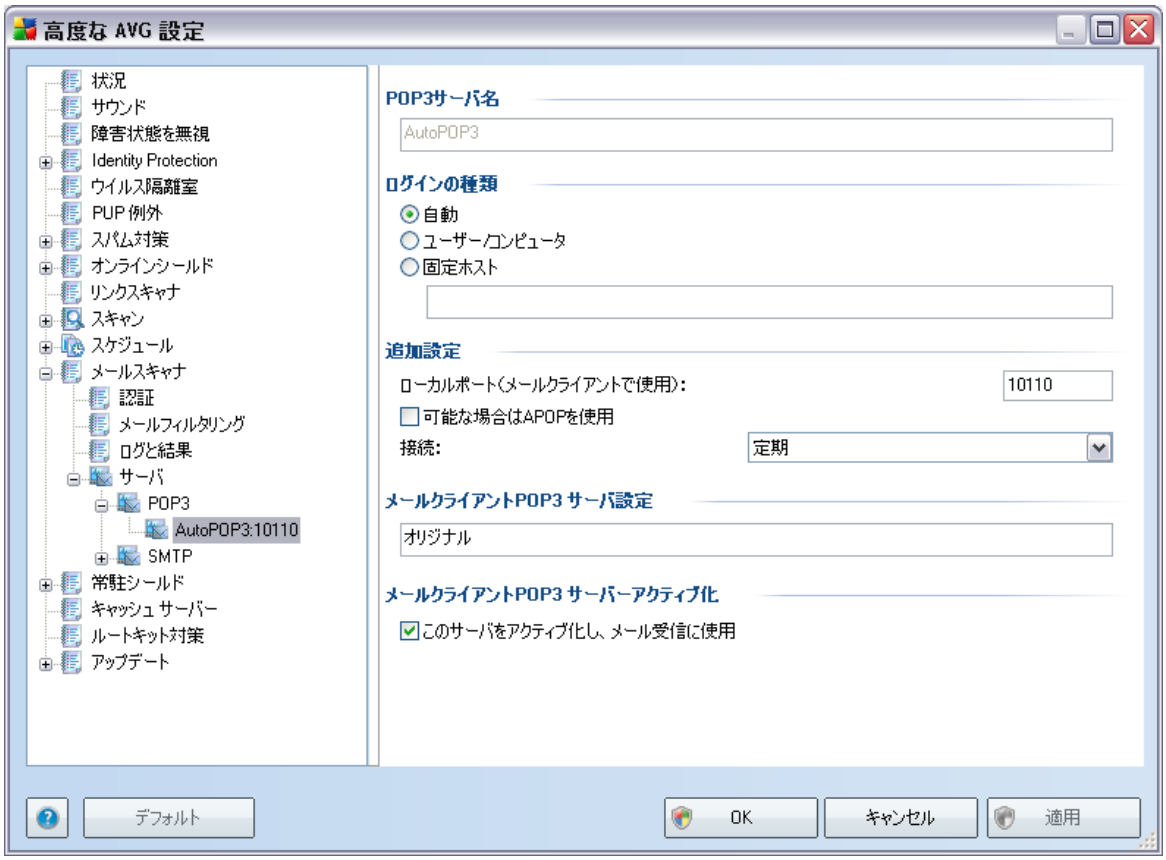


ログと結果から開かれるダイアログでは、メールスキャナの結果のためのパラメータを指定できます。このダイアログは複数のセクションに分けられます。

- ***ログメンテナンス*** - メールスキャナのログ出力間隔を日次、、週次、月次から選択します。また、最大ログファイルサイズ（*MB*）を指定することもできます。
- ***ログレベル閾値*** - デフォルトでは中レベルに設定されています - これより低いレベル（*基本接続情報のロギング*）、または高いレベル（*すべてのトラフィックのロギング*）を選択することもできます。
- ***ログファイル保存先フォルダ*** - ログファイルを保存する場所を定義します。

10.12.4. サーバー

[***サーバー***] セクションでは、***メールスキャナ***コンポーネントサーバーのパラメータを編集したり、[***新しいサーバーを追加***] ボタンを使用して新しいサーバーを設定できます。



このダイアログでは（***サーバー / POP3 で表示されます。***）、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***サーバーを設定することができます。

- ***POP3 サーバー名*** - サーバー名を入力するかAutoPOP3のデフォルト名のままにします。
- ***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。
  - ***USER/COMPUTER*** - メールサーバーを決定する最も簡単で多く使用される方法はプロキシ方法です。この方法を使用するためには、それぞれのメールサーバーのログイン

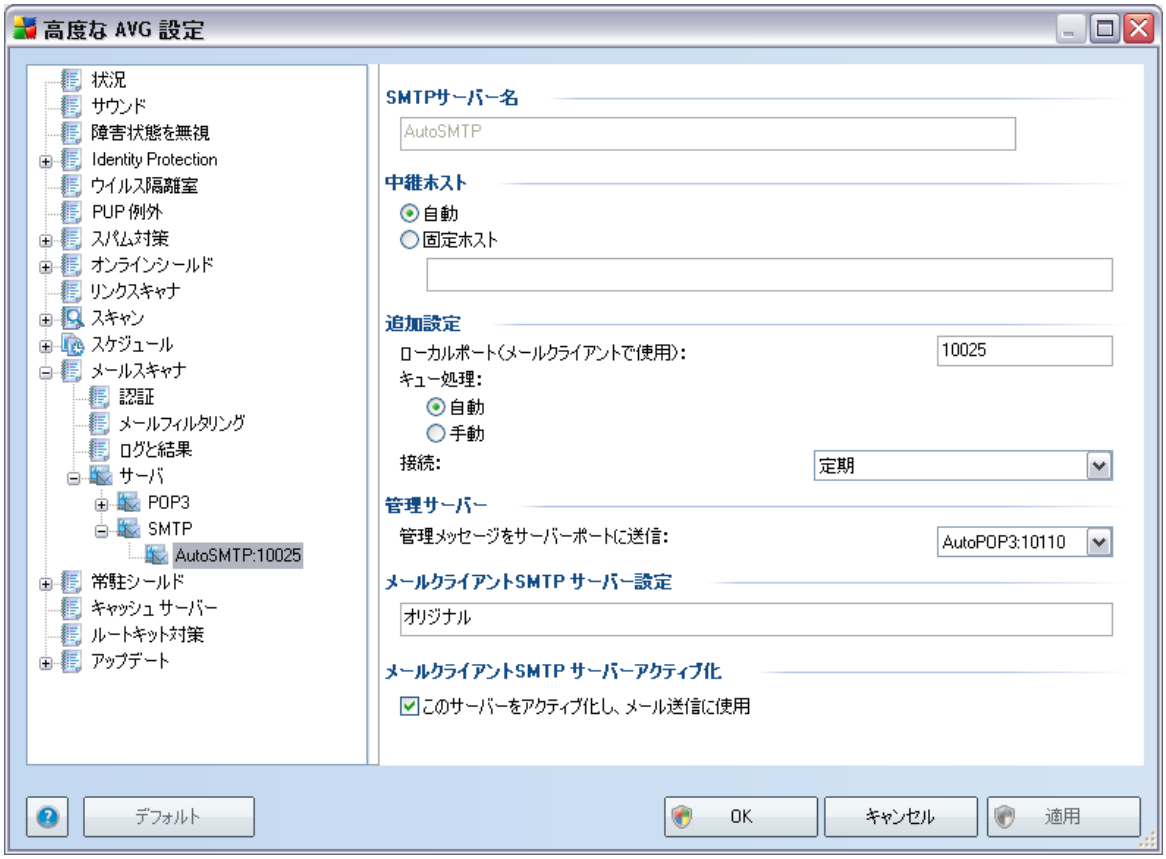
ユーザー名として、名前またはアドレス（ポート）を指定し、それらを / で区切ってください。例えば、サーバー pop.acme.com のアカウントをuser1、ポート番号を8200とすると、user1/pop.acme.com:8200 をログイン名として使用することになります。

- ***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。IPアドレス（例えば、123.45.67.89）と同様にドメイン名（例えば、pop.acme.com）を使用することができます。メールサーバーが標準でない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（例えば、smtp.acme.com:8200）。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。
  - ***可能であれば APOP を使用*** - このオプションはより安全なメールサーバーオプションを提供します。これにより、メールスキャナが、ユーザーアカウントパスワードを転送する他の方法を使用することができます。様々なチェーンを使用した暗号化フォーマットでサーバーにパスワードを送信します。***この機能は、対象メールサーバーがその機能をサポートしている場合にのみ使用可能です。
  - ***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デフォルト）を指定します。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、対象メールサーバーがその機能をサポートしている場合にのみ使用可能です。

- ***メールクライアントの POP3 サーバー設定*** - （AVG パーソナルメールスキャナがすべての受信メールをスキャンできるように）正しくメールクライアントを設定するために必要なコンフィグレーション設定についての簡単な情報を提供しています ***。これは、このダイアログと他の関連ダイアログで指定されたパラメータに基づくサマリです。

- ***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。



このダイアログでは（***サーバー / SMTP***で開かれます）、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***サーバーを設定することができます。

- ***SMTPサーバー名*** - サーバー名を入力するかAutoSMTPのデフォルト名のままにします。
- ***リレーホスト*** - 送信メールに使用されるメールサーバーを決定する方法を定義します。
  - ***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。IPアドレス（例えば、123.45.67.89）と同様に、ドメイン名（例えば、smtp.acme.com）を使用することもできます。メールサーバーが標準でない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（例えば、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。

  - ***キュー処理*** - 送信メールメッセージの要求を処理する際の***メールスキャン***の動作を決定します。

    - 自動 - 送信メールは即時に送信先メールサーバーに配信（送信）されます。

    - 手動 - メッセージは送信メッセージキューに追加され、後で送信されます

  - ***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デフォルト）を指定できます。SSL接続を選択した場合は、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。この機能は送信先メールサーバーの機能としてサポートされている場合のみ利用できます。

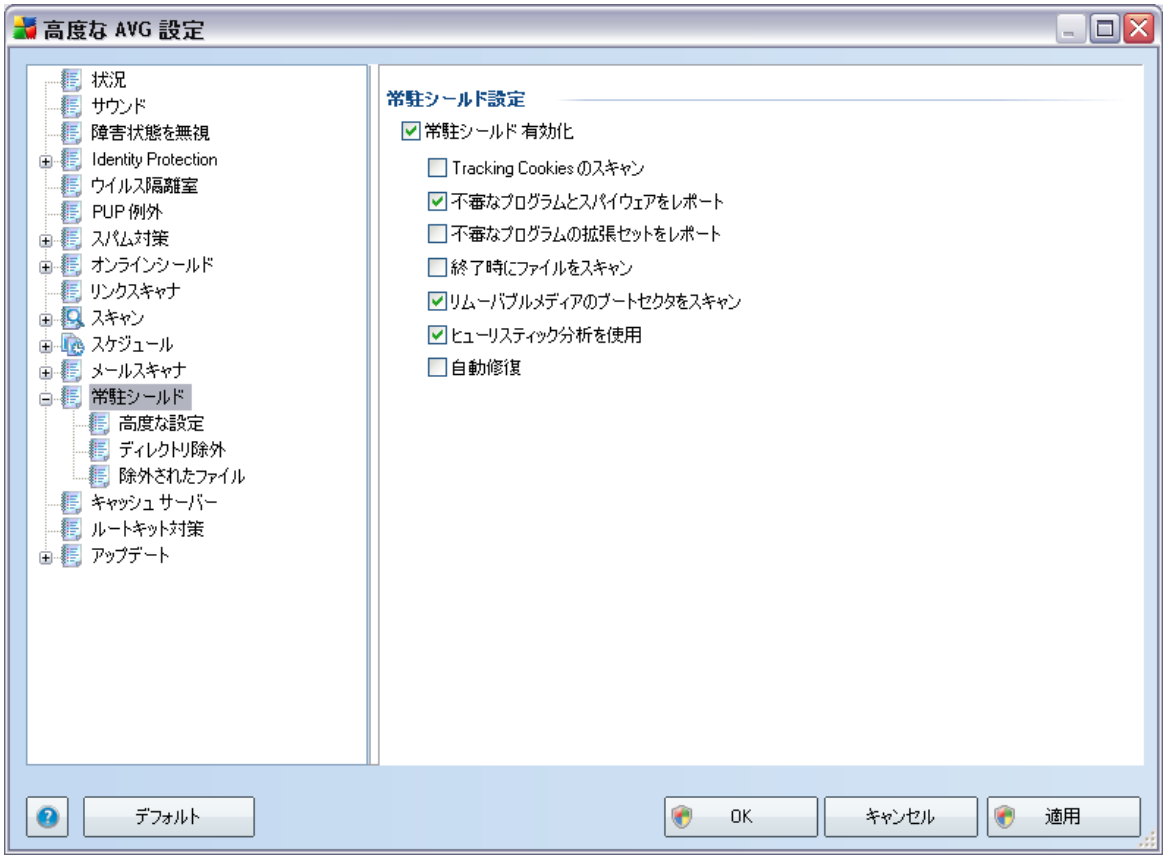
- ***管理サーバー*** - 管理レポートの逆配信に使用されるサーバーのポート番号を示しています。これらのメッセージは、対象メールサーバーが送信メッセージを拒否する場合やこのメールサーバーが利用不可能である場合に生成されます。

- ***メールクライアントSMTPサーバー設定*** - クライアントメールアプリケーションの設定方法についての簡潔な情報が表示されます。これを適用することにより、送信メールは、現在修正中の送信メールチェックサーバーを使用してチェックされます。これは、このダイアログと他の関連ダイアログで指定されたパラメータに基づくサマリです。

- ***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。

10.13. 常駐シールド

常駐シールドコンポーネントは、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オンです***) をオン/オフにして、*常駐シールド*保護を完全に有効化または無効化できます。また、どの***常駐シールド***機能を有効化するかを選択します。

- ***Tracking Cookie をスキャン*** - このパラメータはcookieがスキャン中に検出されるかどうかを定義します。 (*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をレポート*** - (*デフォルトではオン*): 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レポート*** - 前のオプションが有効になっている場合、このボックスにチェックを付けると、スパイウェアの拡張パッケージも検出できます。拡張パッケージとは、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*** - 終了時のスキャンを有効にすると、AVGが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等）が開かれるときや終了される時に確実にスキャンを実行します。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ために役立ちます。

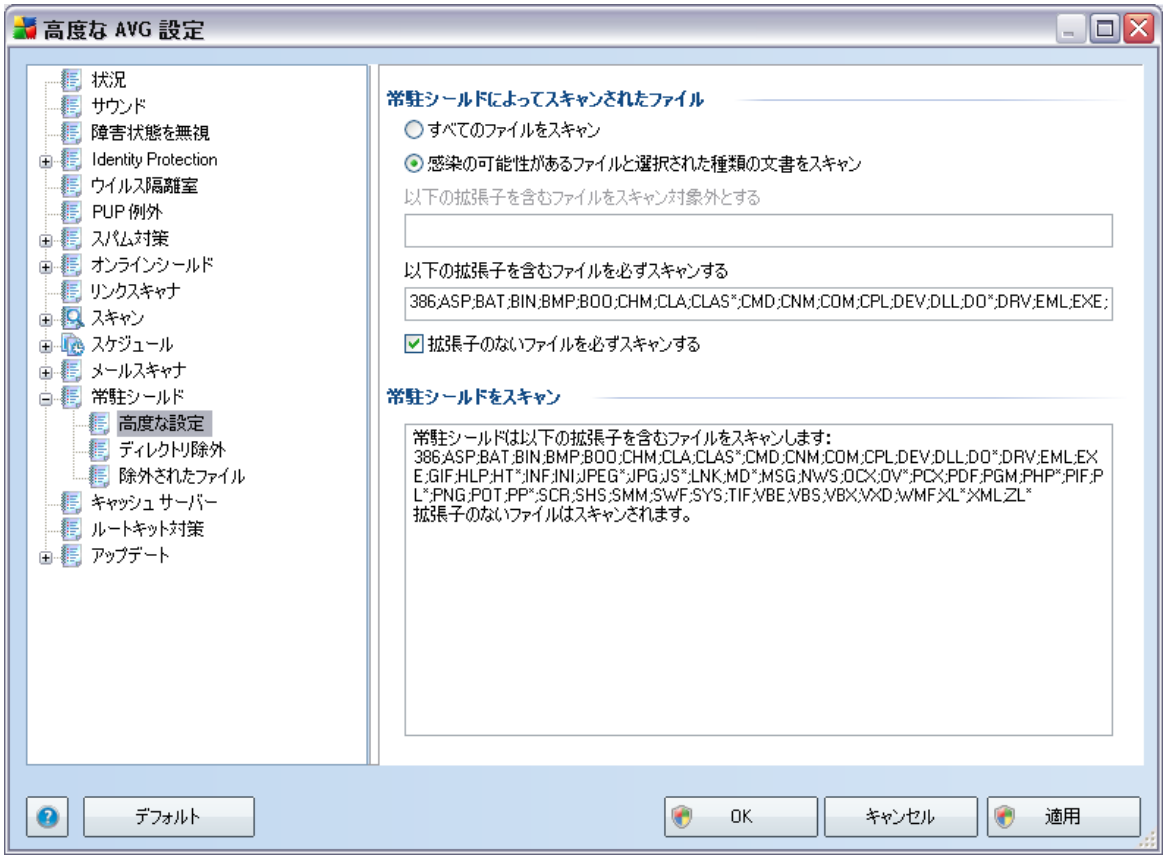
- ***リムーバブルメディアのブートセクタをスキャン*** - (*デフォルトではオン*)

- ***ヒューリスティック分析を使用*** - (*デフォルトではオン*) 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*) が検出に使用されます。

- ***自動修復*** - 修復方法がある場合、検出された感染は自動的に修復されます。

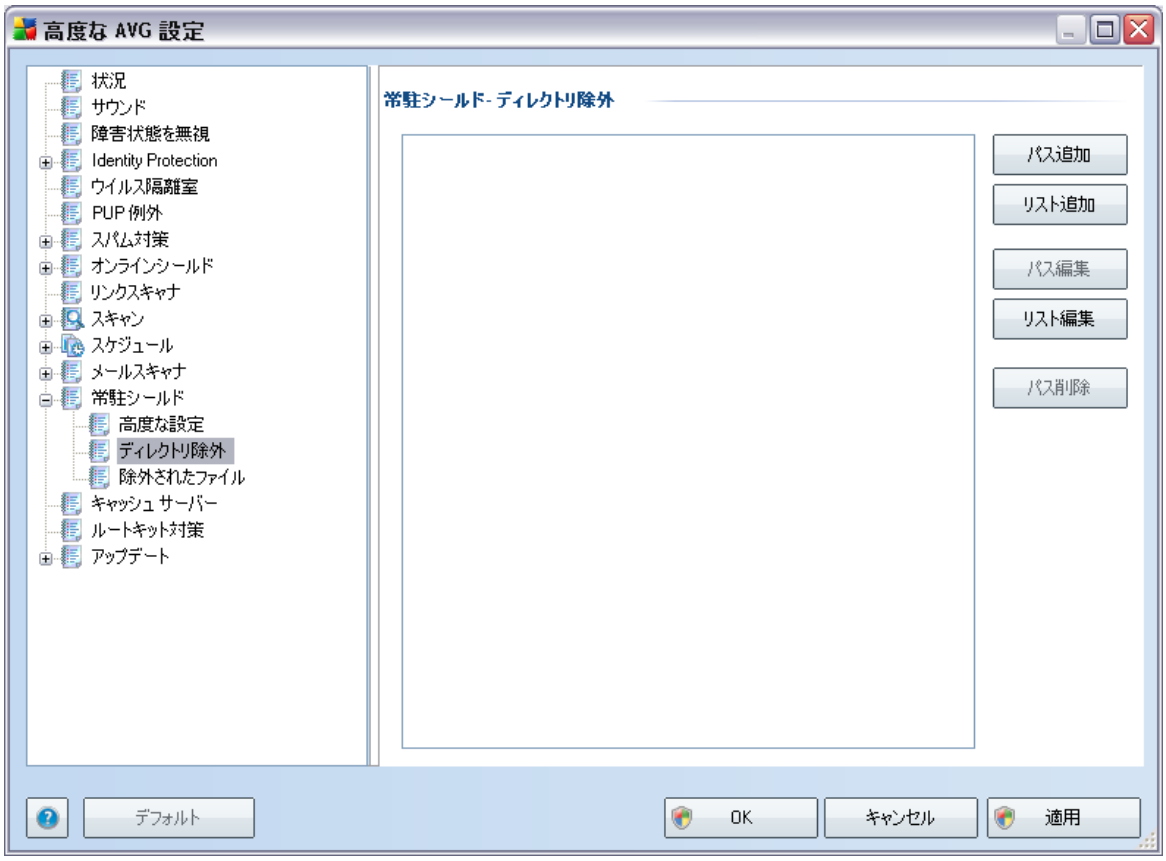
10.13.1. 高度な設定

[***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、スキャンされるファイルを *特定の拡張子によって* 設定することができます。



すべてのファイルをスキャンするか、感染の可能性のあるファイルのみをスキャンするかを指定します。後者の場合、さらに、スキャンから除外されるファイル拡張子を指定することができます。また、必ずスキャンされるファイル拡張子を指定することもできます。

10.13.2. 除外ディレクトリ



常駐シールド- ディレクトリ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します。

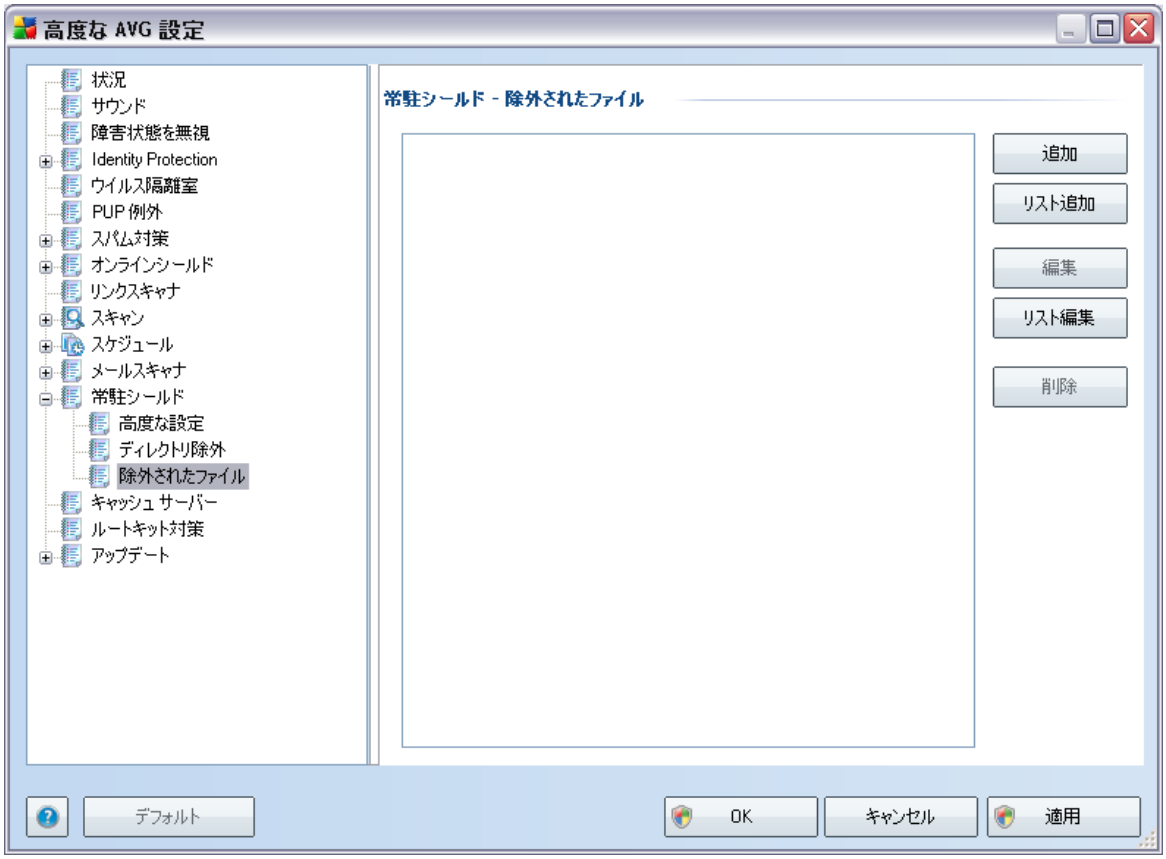
必要でない場合、ディレクトリを除外しないことを強く推奨します。

ダイアログは、以下のコントロールボタンを提供します。

- ***パス追加*** - フォルダの参照画面で、スキャンから除外されるディレクトリを指定します。
- ***リスト追加*** - ***常駐シールド***スキャンから除外されるディレクトリのリストを入力することができます。
- ***パス編集*** - 選択したフォルダのパスを編集します。
- ***リスト編集*** - フォルダリストを編集します。

- ***パス削除***–選択したフォルダのパスを削除できます

10.13.3. 除外されたファイル



[***常駐シールド - 除外されたファイル***] ダイアログは、先に説明した***常駐シールド - 除外されたディレクトリ***と類似した方法で動作しますが、***常駐シールド***スキャンから除外するフォルダではなく、特定のファイルを定義できます。

これは必要でない場合は、フォルダを除外しないことを強く推奨します。

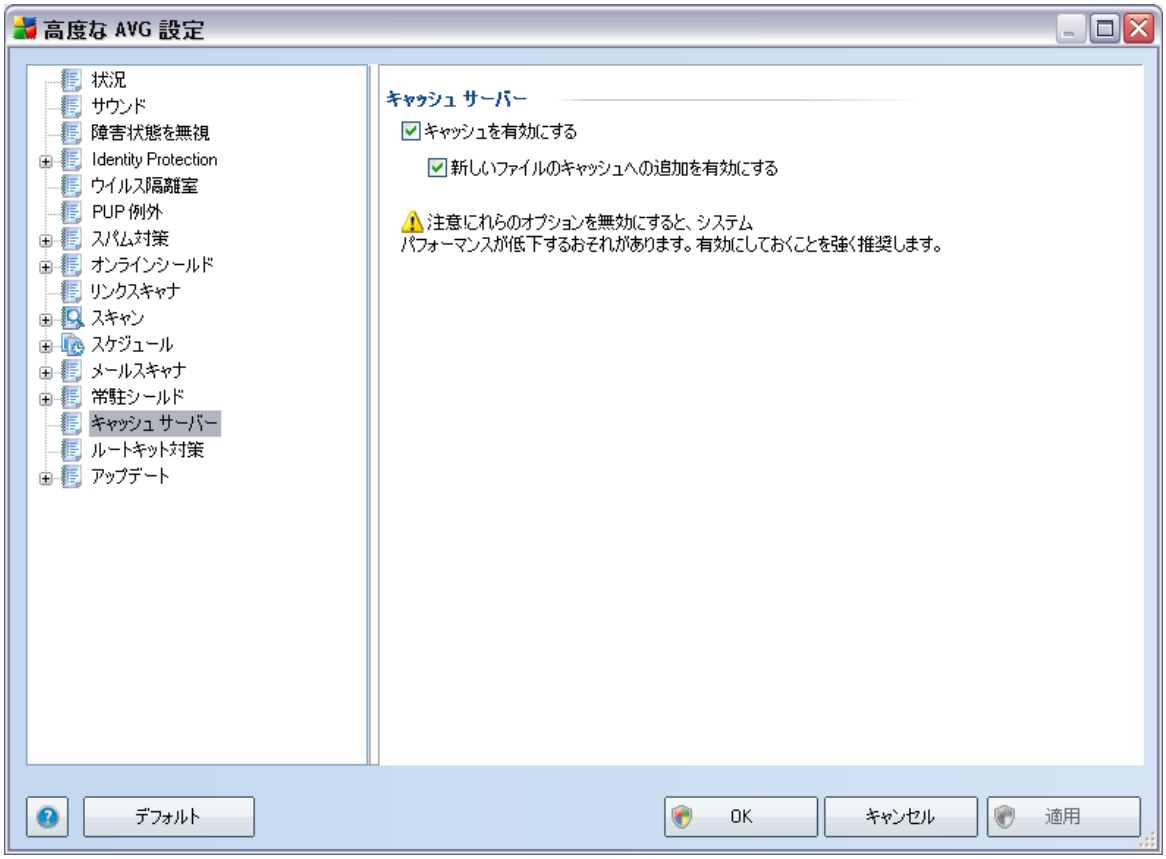
ダイアログは、以下のコントロールボタンを提供します。

- ***追加***–ローカル ディスク ナビゲーション ツリーから 1 つずつ選択することで、スキャンから除外されるファイルを指定します。
- ***リストを追加***–***常駐シールド***スキャンから除外されるファイルの完全リストを入力できます。

- ***編集***–選択ファイルへの特定のパスを編集できます
- ***リストを編集***–ファイル リストを編集できます
- ***削除***–選択したファイルのパスを削除できます

10.14. キャッシュ サーバー

キャッシュ サーバーは、すべてのスキャン (*オンデマンド スキャン、スケジュールされた完全コンピュータ スキャン、常駐シールド スキャン*) の速度を向上するために設計されている処理です。信頼できるファイル (*デジタル署名のあるシステム ファイルなど*) の情報を収集して保持します。このようなファイルは安全であると見なされ、スキャン処理中はスキップされます。



設定ダイアログには 2 つのオプションがあります。

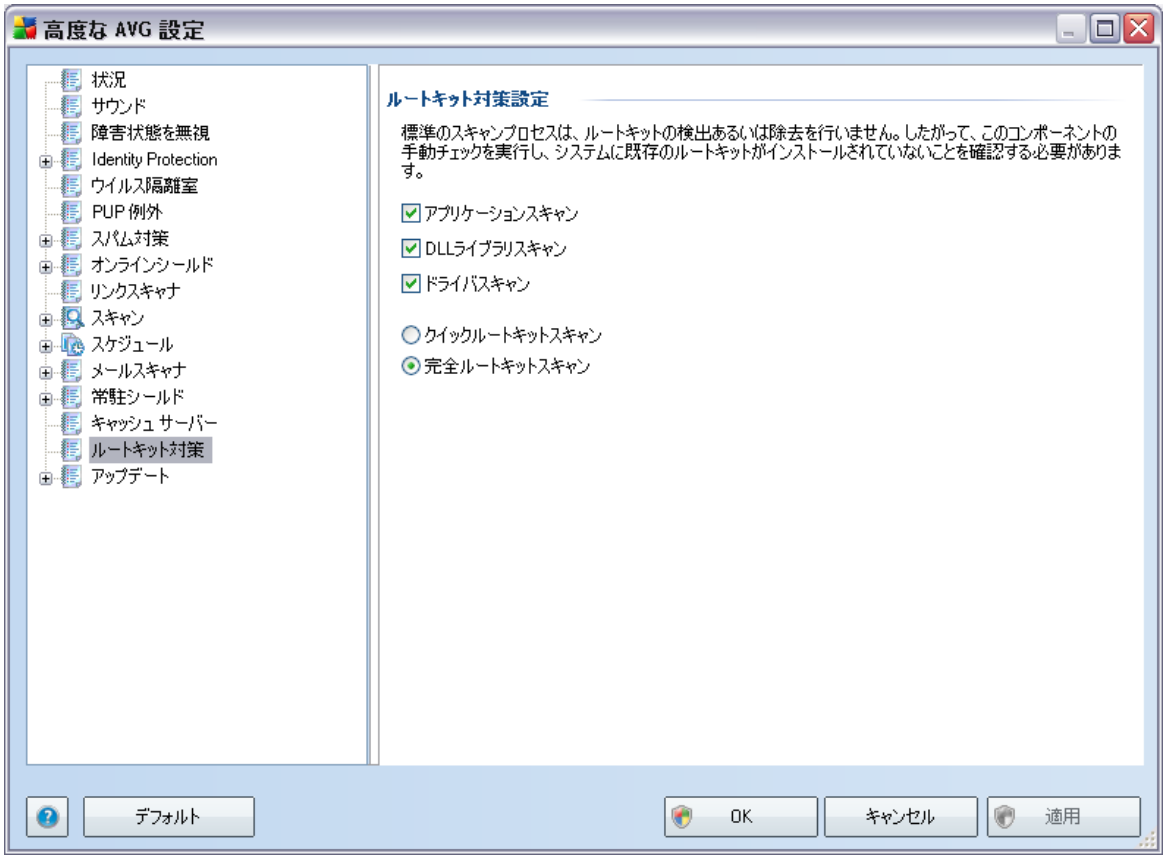
- ***キャッシュを有効にする*** (*デフォルトではオン*) - チェックを外すと、***キャッシュ サーバー***をオフに切り替え、キャッシュ メモリを空にします。最初に使用中のすべてのファイルが 1 つずつウィ

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。

10.15. ルートキット対策

このダイアログでは、***ルートキット対策***コンポーネントのコンフィグレーションを編集できます。



このダイアログ内で提供されている***ルートキット***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。

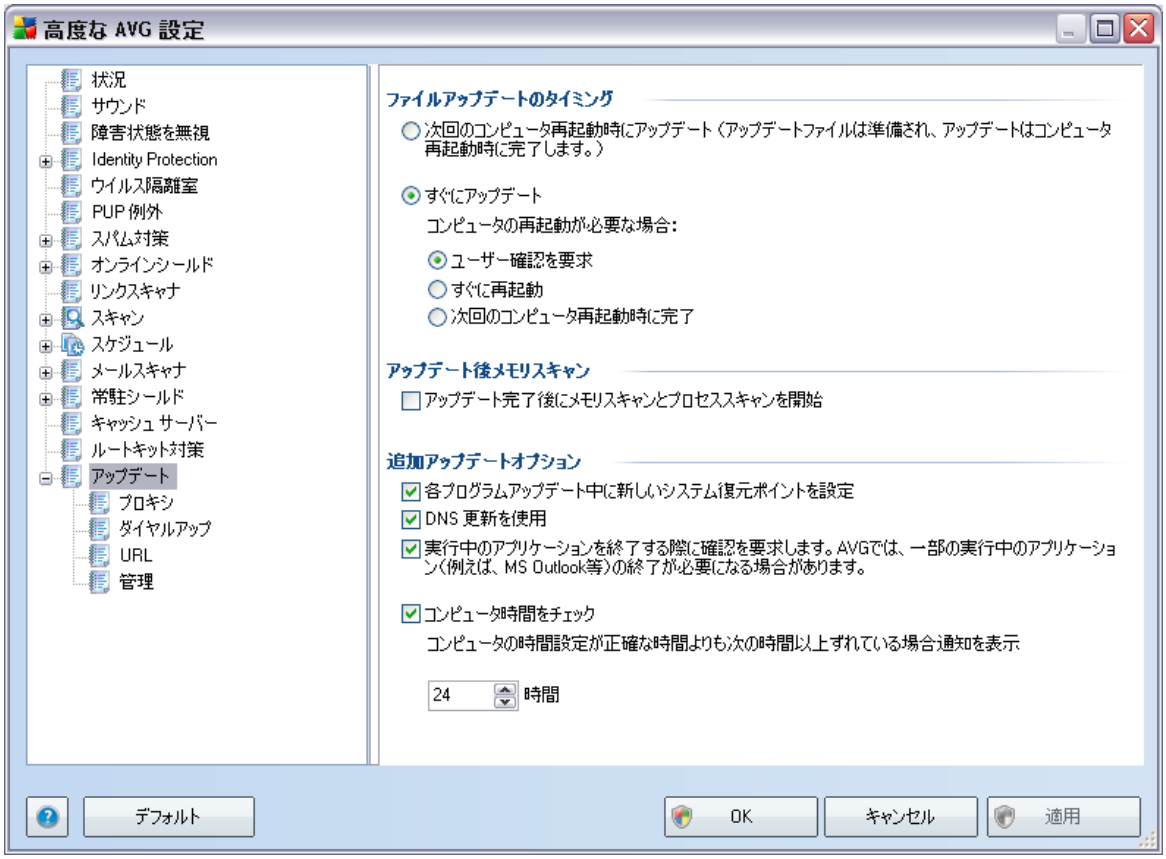
該当するチェックボックスにチェックを付け、スキャン対象オブジェクトを指定します。

- ***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。

10.16. アップデート



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、2つのオプションのうち1つを選択できます。アップデートは、次回のPCの再起動時、またはすぐにアップデートされます。デフォルトでは、すぐにアップデート が選択されています。この設定で、AVGは最大限の安全を保証します。次回のコンピュータ再起動時にアップデート オプションは、コンピュータが定期的に、少なくとも毎日再起動されるということが確実な場合にのみ推奨されます。

デフォルトの設定を保持し、アップデートプロセスをすぐに実行する場合、コンピュータを再起動する条件を指定します。

- ***ユーザーの確認を要求*** - アップデートプロセス完了に必要なPC再起動を確認する画面が表示されます。
- ***すぐに再起動*** - コンピュータはアップデートプロセスが完了した時点で、自動的に即時再起動されます。
- ***次回のコンピュータ再起動時に完了*** アップデートプロセスの完了は次回のコンピュータ再起動時まで延期されます。- また、このオプションは、コンピュータが定期的に、少なくとも毎日再起動されるということが確実な場合にのみ推奨されます。

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。

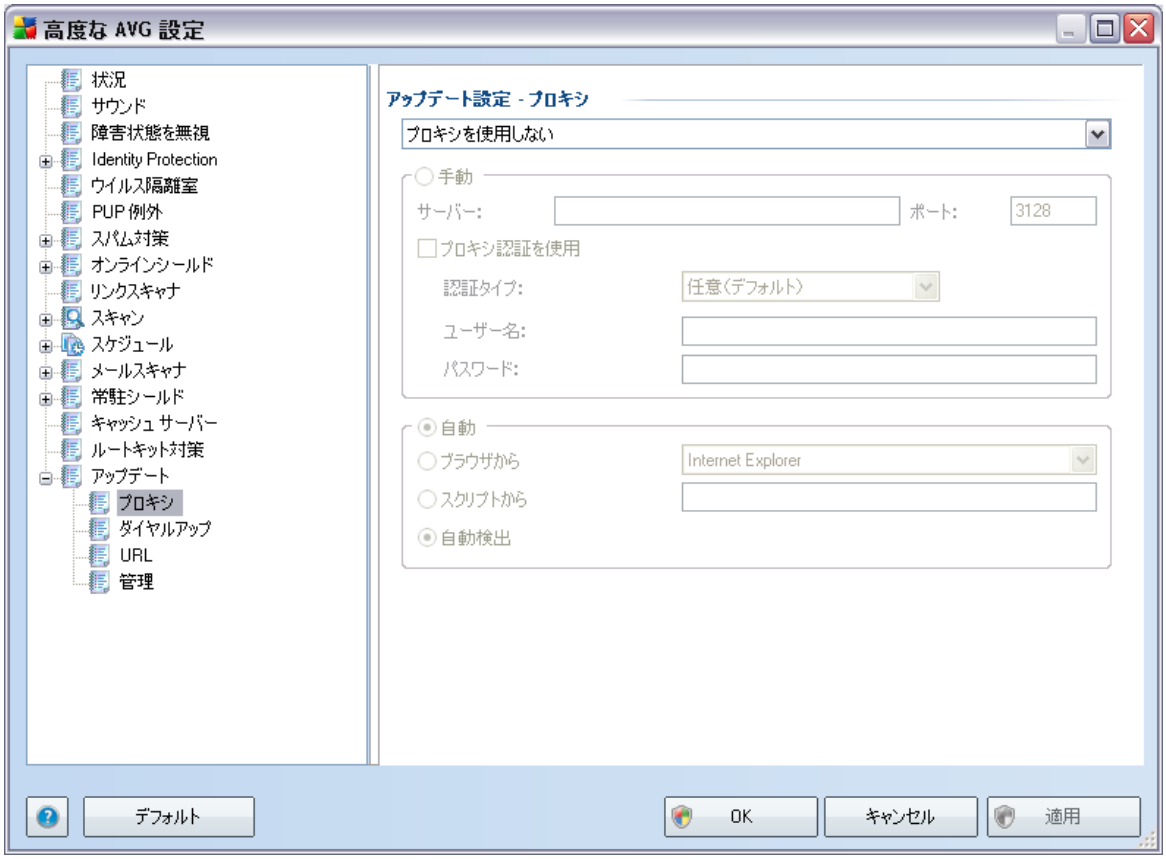
追加アップデートオプション

- ***各プログラムアップデート後に新しいシステム復旧ポイントを作成*** - 各 AVG プログラムアップデートの起動前に、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 アップデートを使用*** - このチェックボックスにチェックを付けると、アップデートサーバーとAVG クライアント間で転送されるデータ量を削減するアップデートファイル検出方法を使用します。

- ***実行中のアプリケーションを終了する確認を要求*** (*デフォルトではオン*) をチェックすることで、アップデートプロセス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。

10.16.1. 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 サーバーを使用しない*** - デフォルト設定

- ***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）

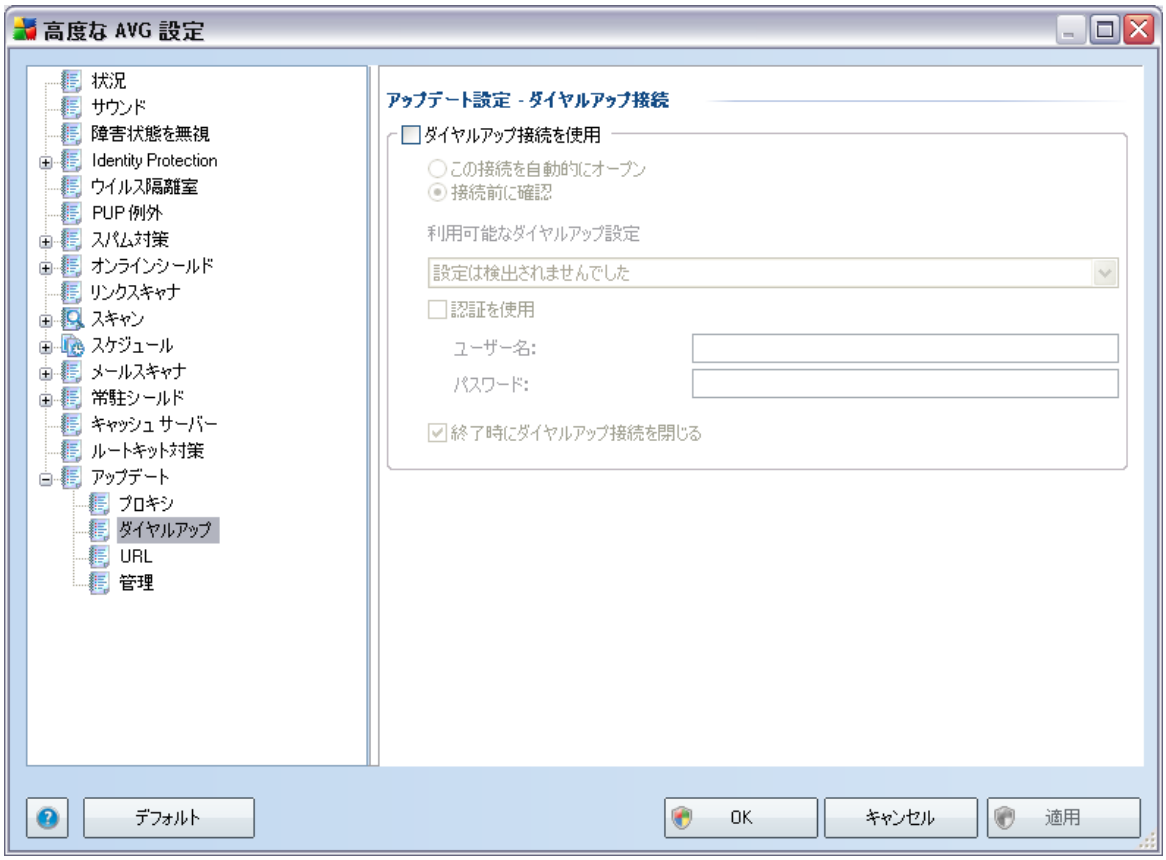
プロキシサーバーは、各ユーザーのルールを設定することもできます。プロキシサーバーがこのように設定されている場合、***プロキシ認証を使用***にチェックを付け、有効なユーザー名とパスワードを入力してください。

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。

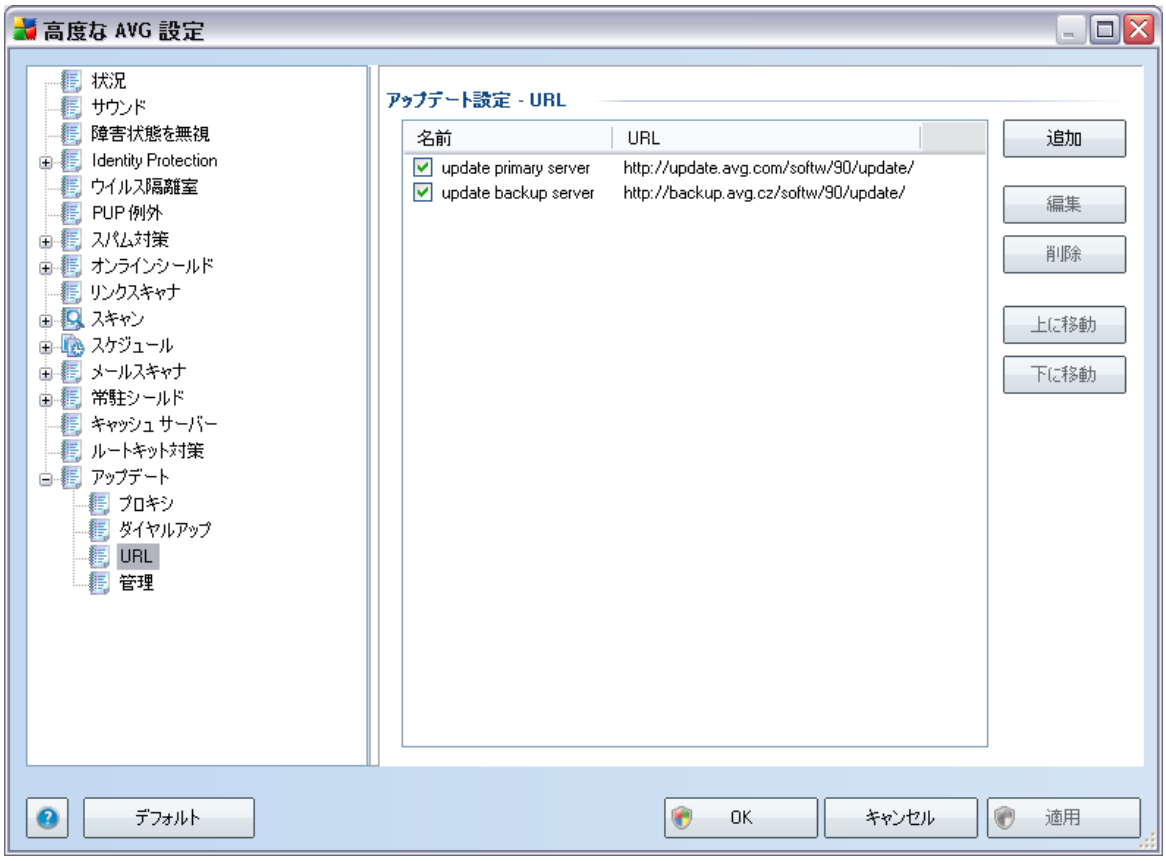
10.16.2. ダイヤルアップ



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***）。

10.16.3. URL

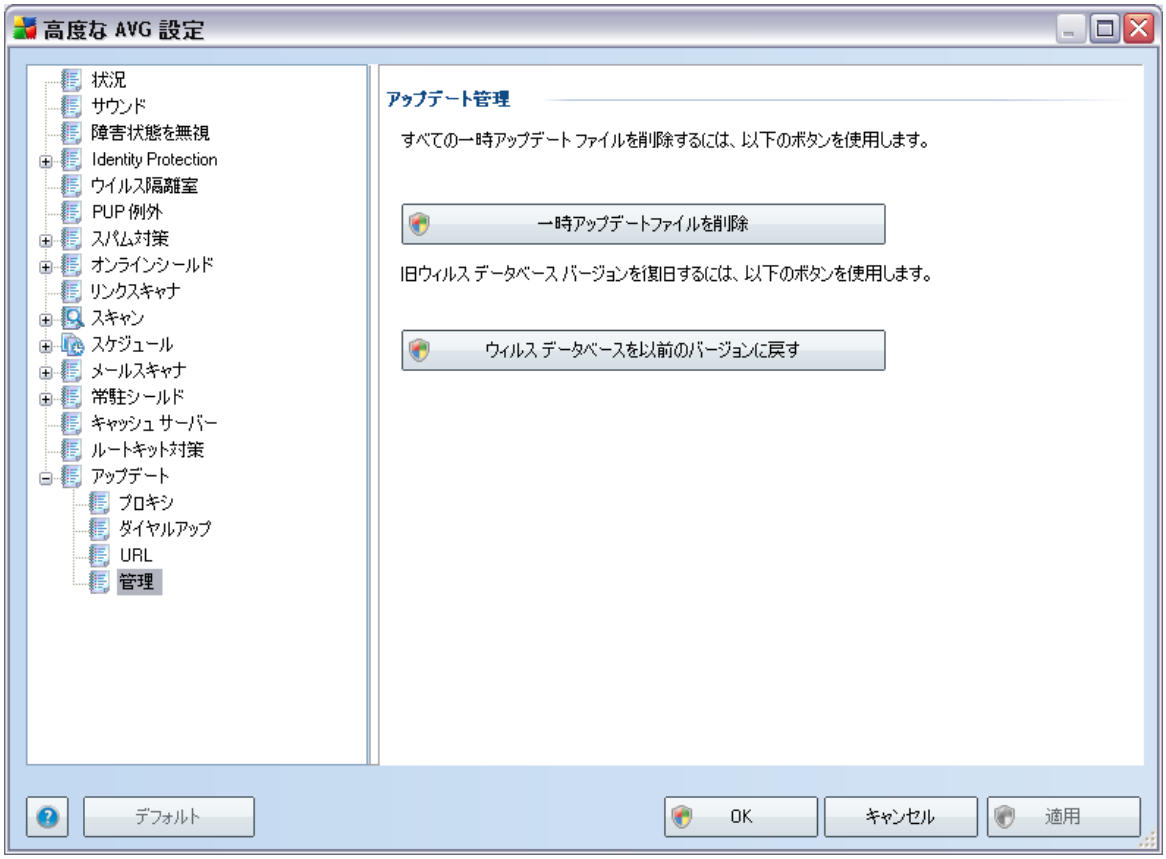


URLダイアログでは、アップデートファイルがダウンロードされるインターネットアドレスのリストが表示されます。このリストは、以下のコントロールボタンを使用して修正します。

- ***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。

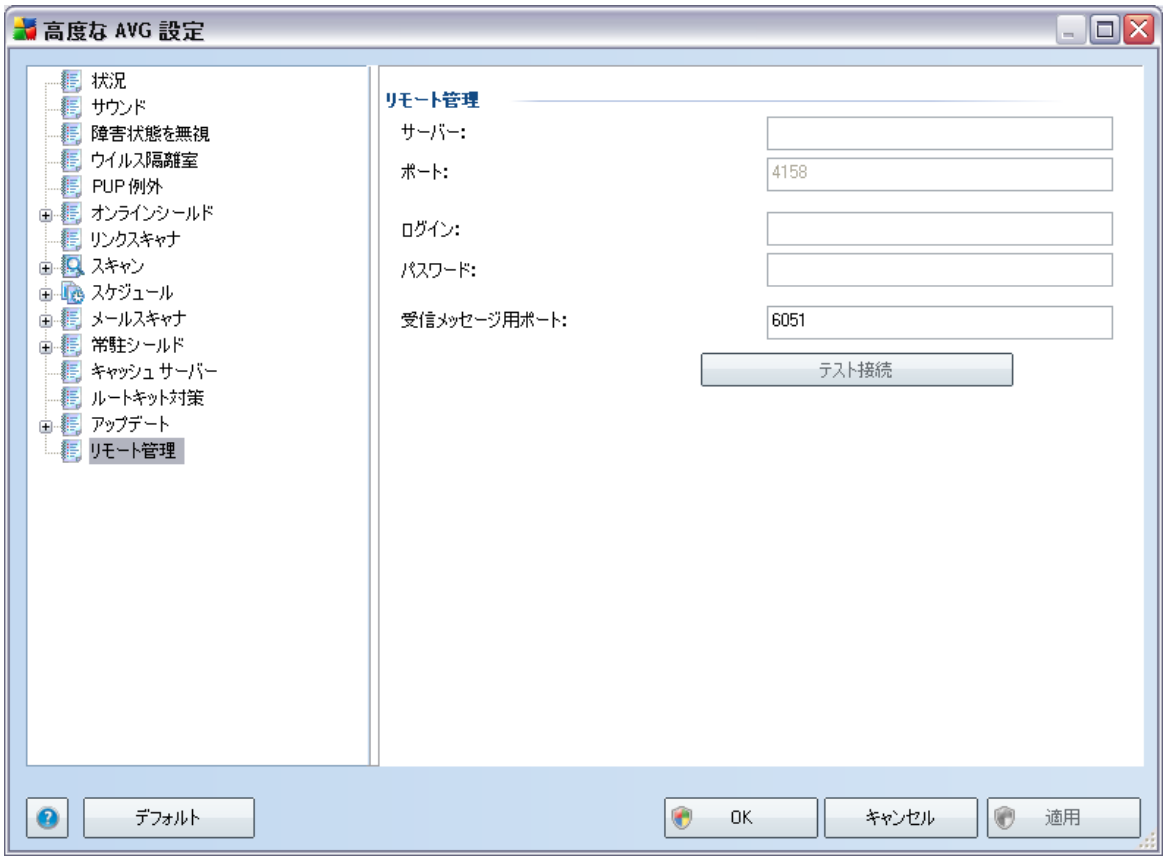
10.16.4. 管理

[***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*）

10.17. リモート管理



リモート管理設定は、AVGクライアントをリモート管理システムに接続させるたものものです。各ステーションをリモート管理に接続させる場合、以下のパラメータを指定してください。

- ***サーバー***- AVG Admin Server 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 Admin Server と通信するポート番号を提供します（*ポート番号4158はデフォルトとされています- 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 Admin Server 間の通信が安全だと定義される場合は、ユーザー名を提示します ...
- ***パスワード*** - パスワードも同様です。

- ***受信メッセージ用ポート*** - AVGクライアントが受信メッセージをAVG Admin Server から受け入れるポート番号

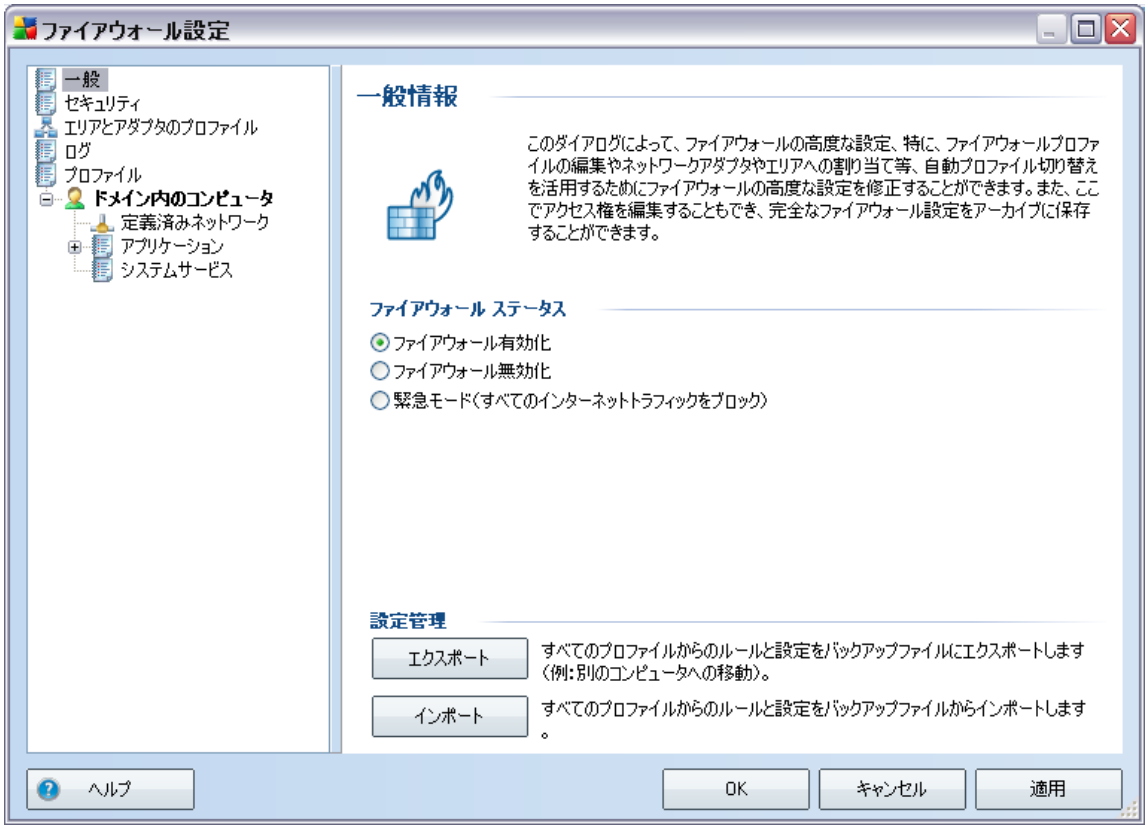
テスト接続ボタンによって、上記のすべてのデータが有効で、DataCenterに正常に接続するために使用されていることを検証できます。

注意：*リモート管理の詳細な説明については、AVG Network Edition のドキュメントを参照してください。*

11. ファイアウォール設定

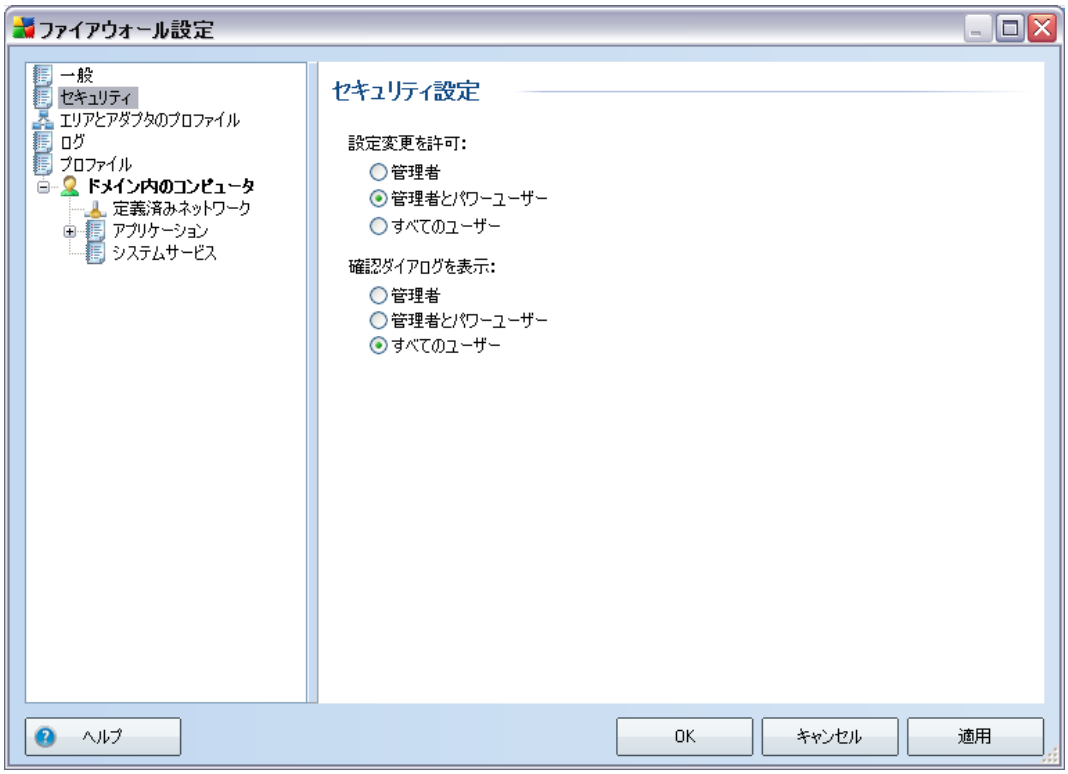
ファイアウォール設定は新しいウィンドウで表示されます。ここでは、いくつかのダイアログで、コンポーネントの高度なパラメータを設定することができます。***ただし、高度な設定編集は専門家と経験のあるユーザーのみを対象としています。***

11.1. 一般



[***一般情報***] では、ファイアウォール***設定の***エクスポート/インポート***ができます。つまり、定義された***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、逆に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。

11.2. セキュリティ



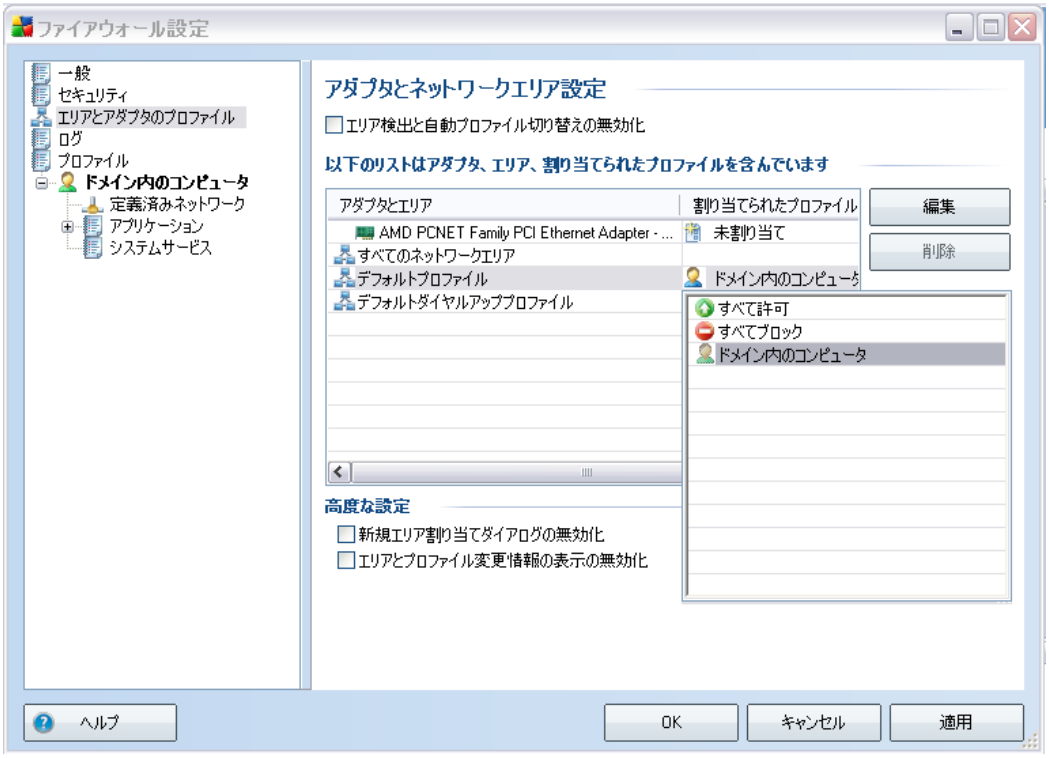
セキュリティ設定ダイアログでは、選択されたプロファイルに関係なく、***ファイアウォール***の動作の一般的なルールを定義します。

- 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することができます。
- ***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

11.3. エリアとアダプタのプロファイル



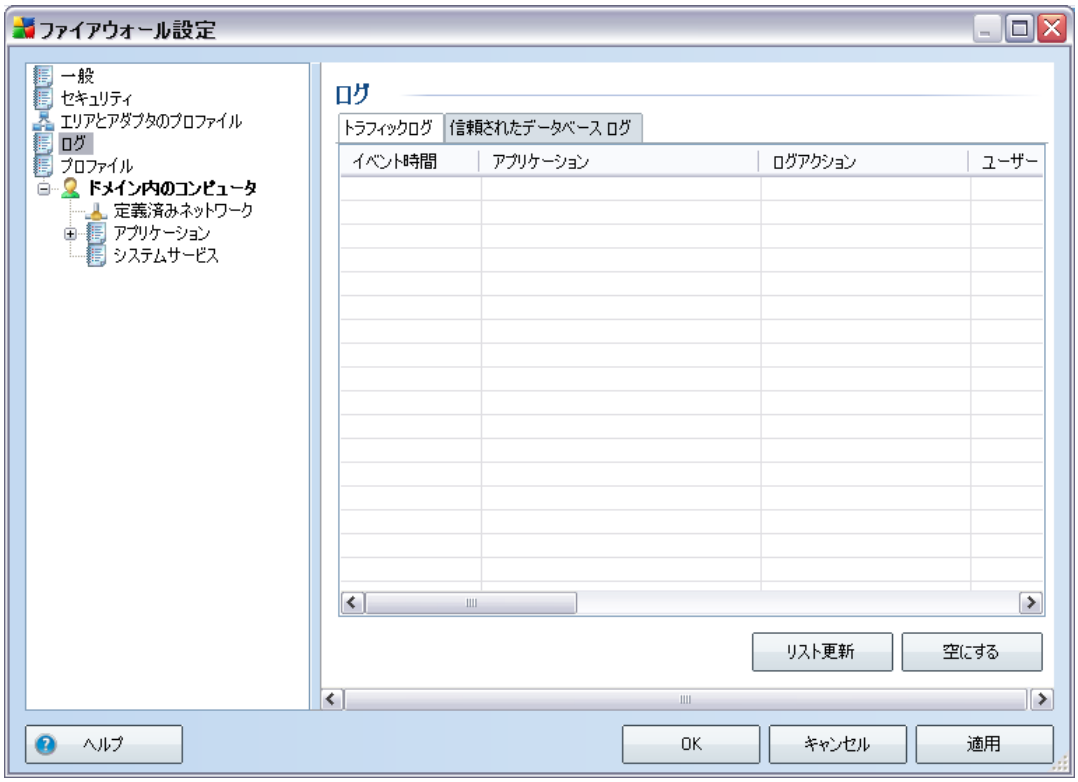
アダプタとネットワークエリア設定ダイアログでは、定義済みプロファイルの特定のアダプタへの割り当てと、該当するネットワークの参照に関する設定を編集します。

- ***エリア検出と自動プロファイル切り替えの無効化*** - 定義されたプロファイルの 1 つは、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、***インストールプロセス***中のコンピュータ使用状況およびコンピュータネットワーク設計の選択内容に基づいて定義された一般的なプロファイルが使用されます。ただし、プロファイルを区別し、それらを特定のアダプタとエリアに割り当て、後でこの設定を一時的に切り替えたい場合、***エリア検出と自動プロファイル切り替えを無効化***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*** - このリストでは、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から、各アダプタに特定のプロファイルを割り当てられます。このメニューを開くには、アダプタリストで該当するアイテムをクリックし、プロファイルを選択します。

- ***高度な設定*** - 該当するオプションをクリックすると、情報メッセージを表示する機能を無効化します。

11.4. 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***アクションとイベントのリストを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*、*各ダイアログアクション*、*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*）とともに 2 つのタブ上で確認できます。

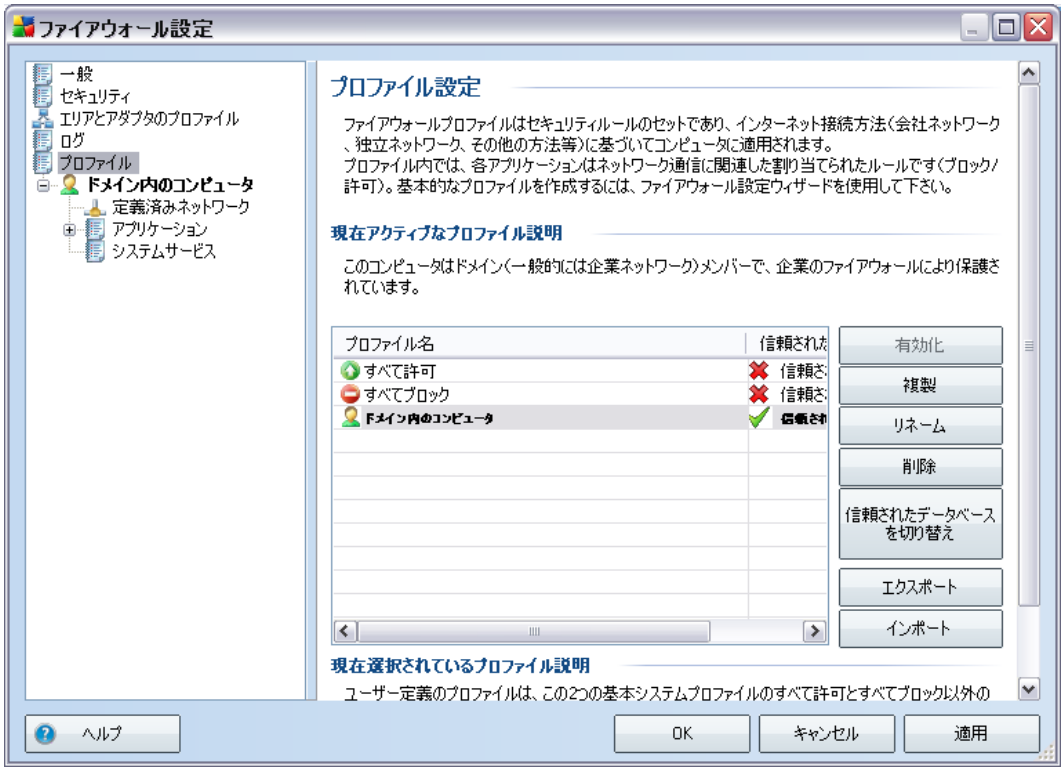
- ***トラフィックログ*** - ネットワークに接続しようとしたすべてのアプリケーションの活動に関する情報を提供します。
- ***信頼されたデータベースログ*** - *信頼されたデータベース*は、常にオンライン通信を許可できる認証され信頼されたアプリケーションに関する情報を収集する AVG 内部データベースです。新しいアプリケーションが初めてネットワークに接続しようとするとき（*つまり、まだこのアプリケーションに指定されたファイアウォールルールがない場合*）、そのアプリケーションに対してネットワーク通信を許可するかどうかを決定する必要があります。まず、AVG は*信頼されたデータベース*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。

コントロールボタン

- ***ヘルプ*** - ヘルプファイルに関するダイアログを開きます。
- ***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)* 等でソート可能です。です。各カラムヘッダーをクリックするだけです。***リスト更新***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。
- ***リストを空にする*** - 表のすべてのエントリを削除します。

11.5. 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。



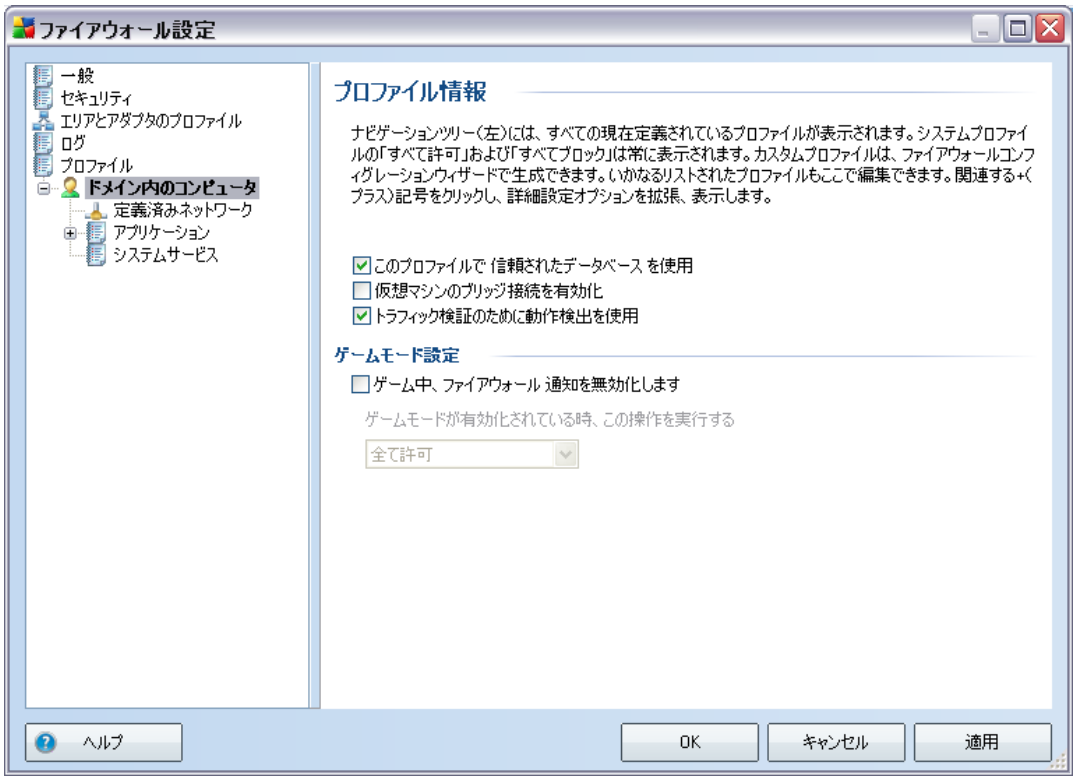
これらのシステムプロファイルは以下のコントロールボタンを使用して編集することができます。

- ***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*** - 選択されたプロファイルを新しく定義できます。
- ***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。
- ***ヘルプ*** - ヘルプファイルに関するダイアログを開きます。

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。

11.5.1. 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*** - (*既定ではオン*) このオプションをオンにすると、*信頼されたデータベース*を有効にします (*つまり、各プロファイルに対して、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 内部データベースです。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化*** - (*既定ではオフ*) このアイテムをチェックすると、WMware の仮想コンピュータの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*** - (*既定ではオン*) 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、***ID 保護***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

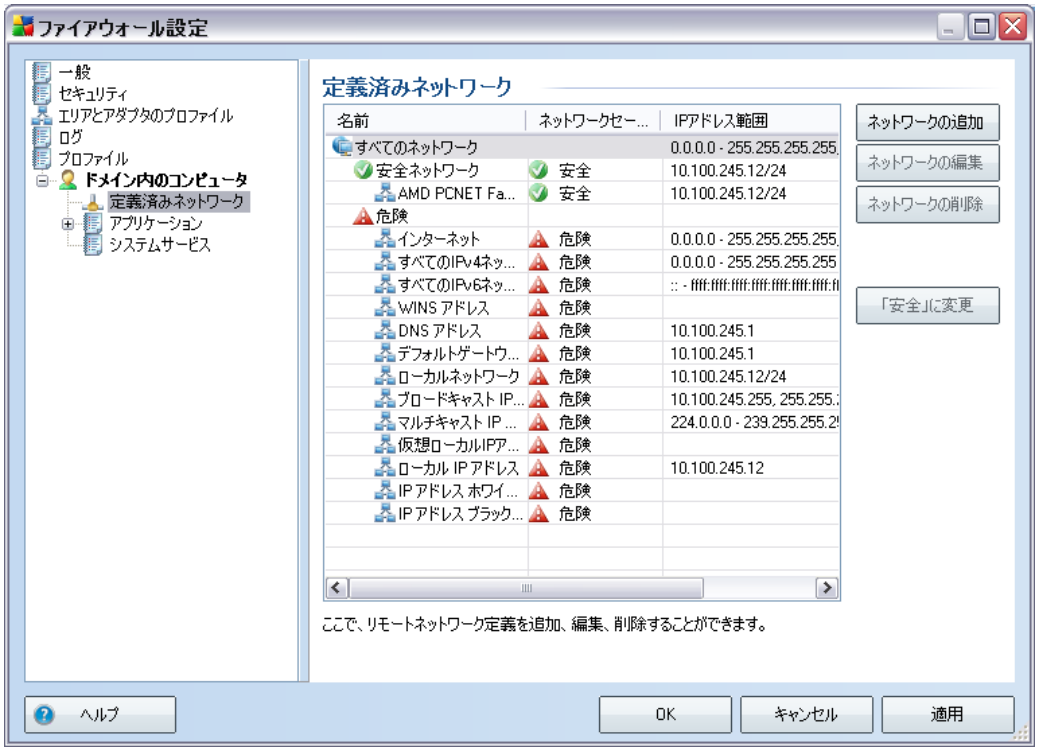
ライン通信を許可されているかどうかを判断できます。

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、フル画面アプリケーションが実行中の場合、***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等のすべてのフル画面アプリケーションにも該当します。*) 情報メッセージは邪魔になる場合があります。

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。

11.5.2. 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。検出されたネットワークに関して、以下の情報が提供されます。

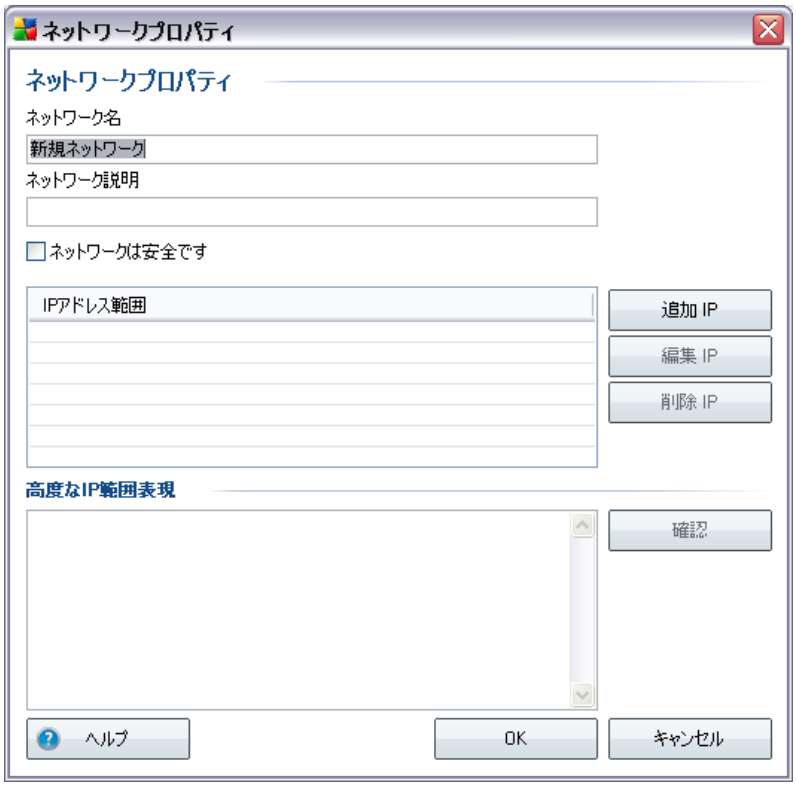
- ***名前*** - コンピュータが接続されているすべてのネットワークの名前

- ***安全性*** - デフォルトでは、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。

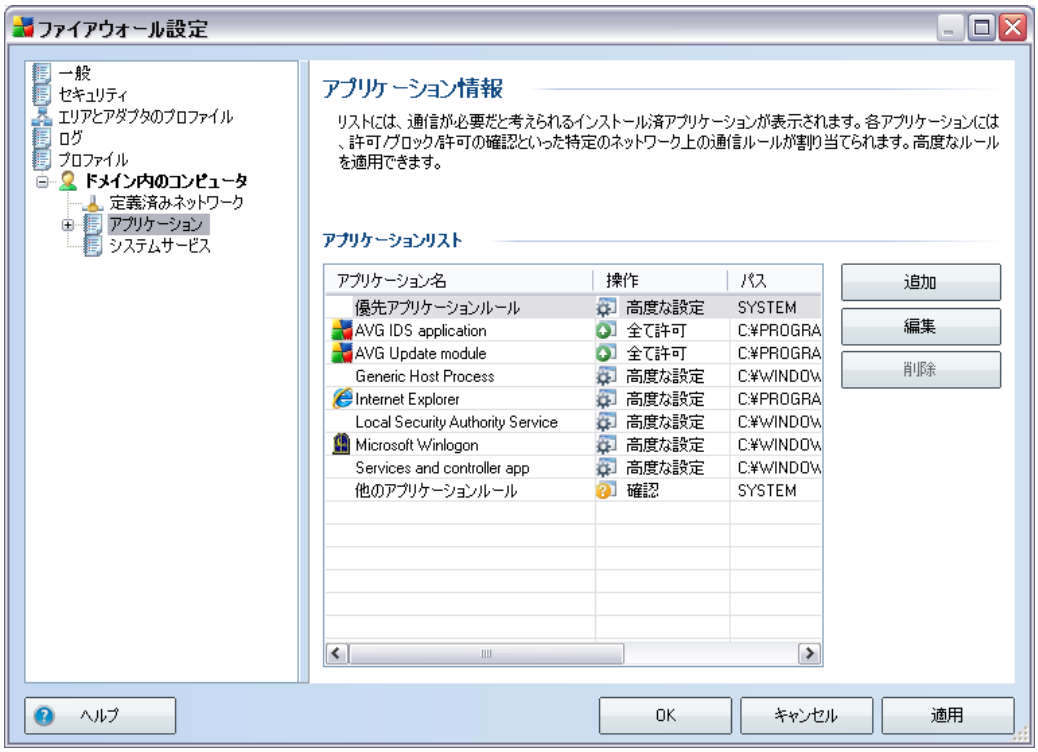


このダイアログでは、***ネットワーク名***し、***ネットワーク説明***を入力し、ネットワークが安全かどうかを指定することができます。新しいネットワークは [***IPの追加***] ボタン（または***IPの編集***/***IPの削除***）で開かれるダイアログで定義されます。このダイアログでは、IPの範囲やマスクを指定することでネットワークを設定することができます。

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*** - 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*** - デフォルトでは、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*）。
- ***ヘルプ*** - ヘルプファイルに関するダイアログを開きます。

11.5.3. 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。

- 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 (この時点でユーザーは通信を許可するか、ブロックするかを決定できます)*
- 高度な設定

リストのアプリケーションは、***ファイアウォール設定ウィザード***の検索中、あるいは不明な、または新規アプリケーションがインストールされた場合に検出されたものです。

注意: 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。

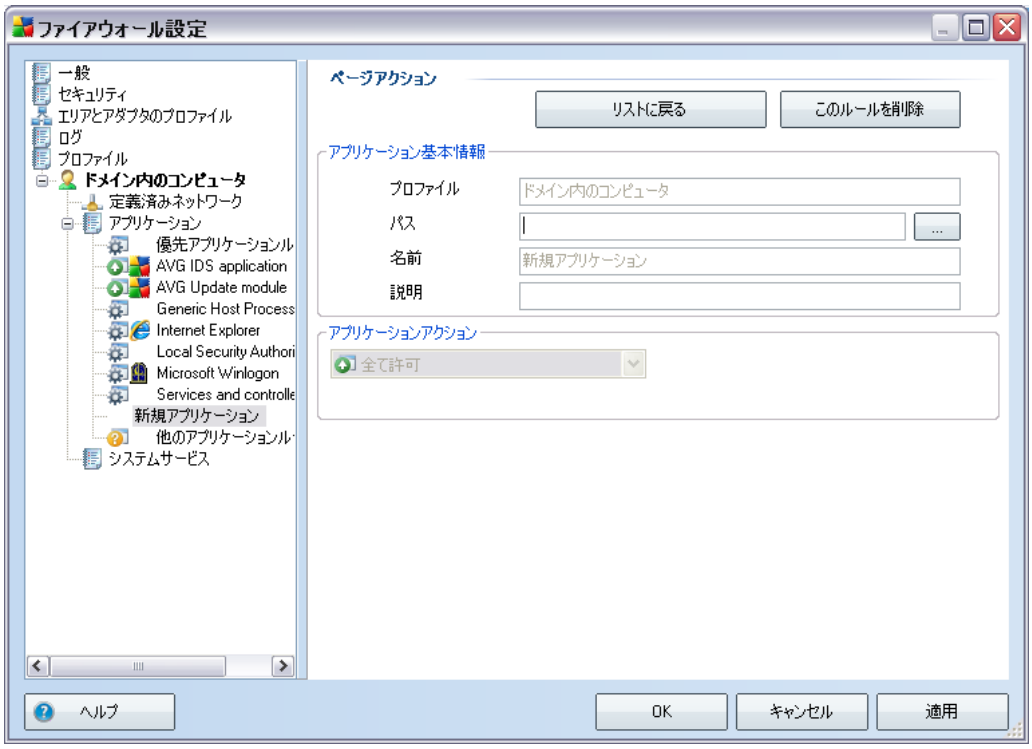
コントロールボタン

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データが表示された同じ [***ペ***

ージ アクション] ダイアログを開 きます。

- ***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。
- ***ヘルプ***- ヘルプファイルに関 するダイアログを開 きます。



このダイアログでは、該 当 するアプリケーションの設 定 を詳 細 に定 義 することができます。

ページアクション

- [***リストに戻 る***] ボタンは、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***] ボタンは、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

このセクションでは、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（*実行可能ファイル*）へのフルパスを入力します。「**...**」ボタンをクリックすると、ツリー構造で簡単にアプリケーションを指定することができます。

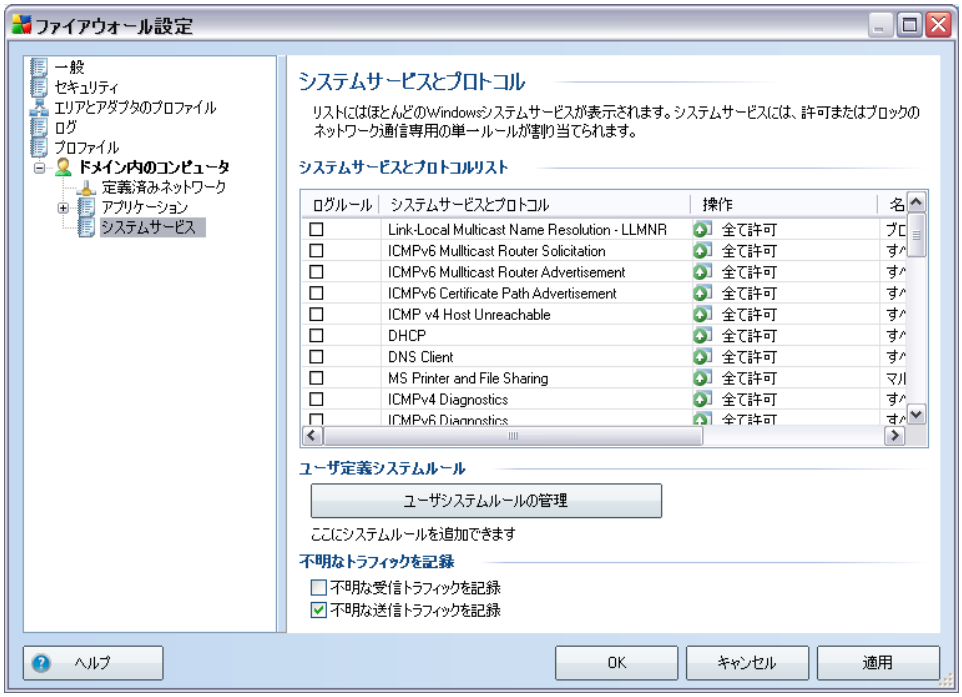
アプリケーションアクション

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します。

- ***全て許可***は、アプリケーションが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通信できるようにします。
- ***許可***は、安全な（信頼できる）もの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の通信のみを許可します。
- ***ブロック***は、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する接続も許可しません。
- ***確認***はその時の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表示します。
- ***高度な設定***には、[***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。設定を変更する必要がある場合、リスト内でルールを***上に移動***、または***下に移動***することができます。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。青色のリンクが付いている値は、各設定ダイアログでクリックすると変更できます。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。

11.5.4. 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。

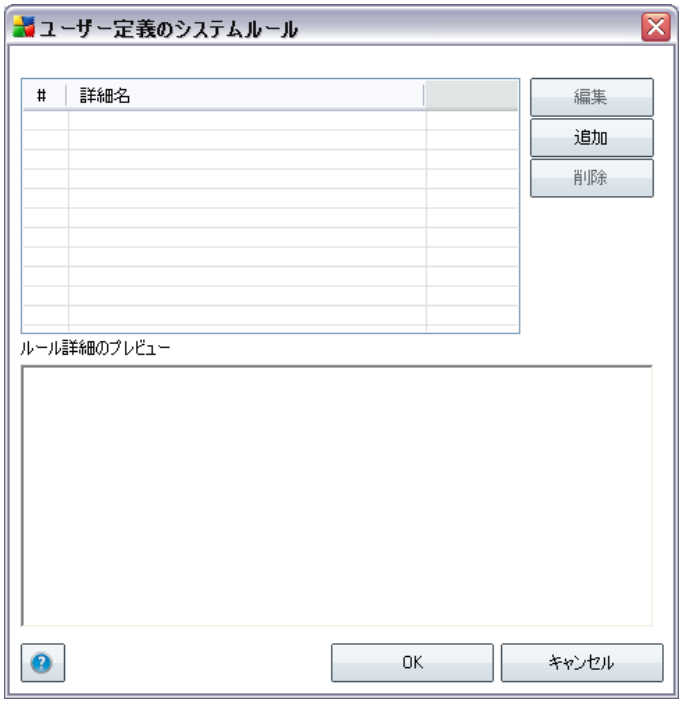


[***システム サービスとプロトコル***] ダイアログには、ネットワーク通信が必要な可能性がある Windows 標準システムサービスおよびプロトコルがリスト表示されます。表には、次の列があります。

- ***ログ ルール アクション*** - このボックスでは、ログ
- ***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。
  - 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
- ***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 (*割り当てられたアクションを含む*) は、次のボタンを使用して編集できます。

- 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。
- 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



警告: *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*** – このボックスにチェックを付けると、ログにすべての外部からのコンピュータへの不明な接続
- ***不明な送信トラフィックを記録*** – このボックスにチェックを付けると、ログにすべてのコンピュータから外部への不明な接続

12. AVGスキャン

スキャンは **AVG 9 Internet Security** 機能の最重要な要素です。オンデマンドでスキャンを実行したり、時間を指定して定期的に実行されるようにスケジュールすることもできます。

12.1. 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 ***コンピュータスキャン*** 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。
    - ***全コンピュータをスキャン***
    - ***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。

12.2. 定義済みスキャン

AVG 9 Internet Security の主要な機能の 1 つは、オンデマンド スキャンです。オンデマンドのスキャンは、ウイルス感染の疑いがある場合、コンピュータの様々な箇所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、このようなスキャンを定期的に実行することを強く推奨します。

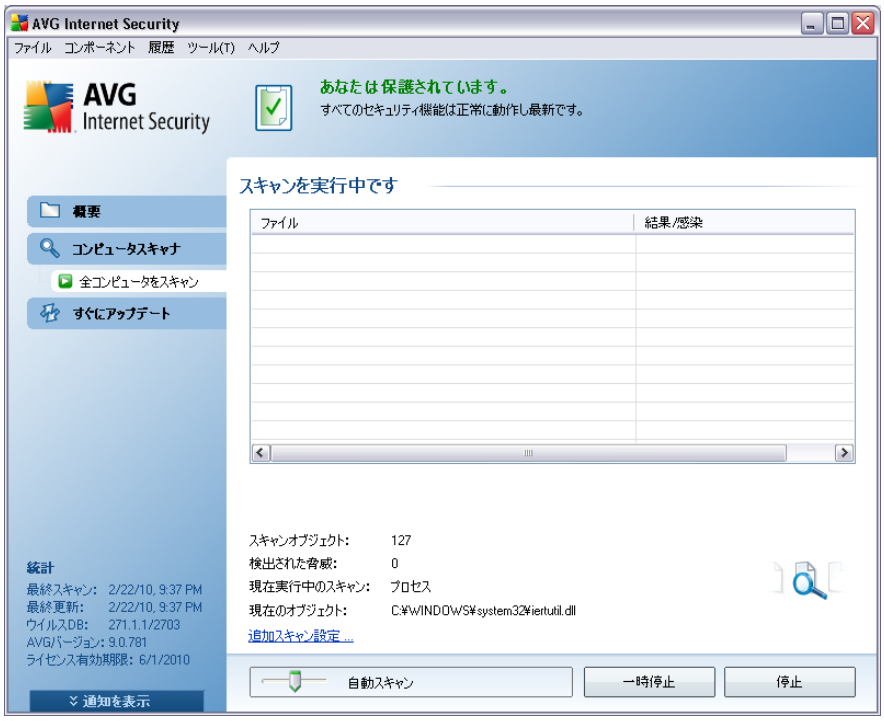
AVG 9 Internet Security には、ソフトウェア ベンダがあらかじめ定義した 2 種類のスキャンがあります。

12.2.1. 全コンピュータをスキャン

完全コンピュータスキャン - 感染と不審なプログラムに対してコンピュータを完全にスキャンします。このスキャンはすべてのコンピュータのハードドライブをスキャンし、ウイルス感染を検出、修復の実行、または検出した感染を***ウイルス隔離室***に移動します。完全コンピュータスキャンは、最低でも週に1度は実行され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

完全コンピュータスキャンは、スキャンのアイコンをクリックして、スキャンインターフェースから直接実行することができます。このスキャンに対して、さらに特別な設定をする必要はありません。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（***一時中止***）、またはキャンセル（***停止***）することができます。

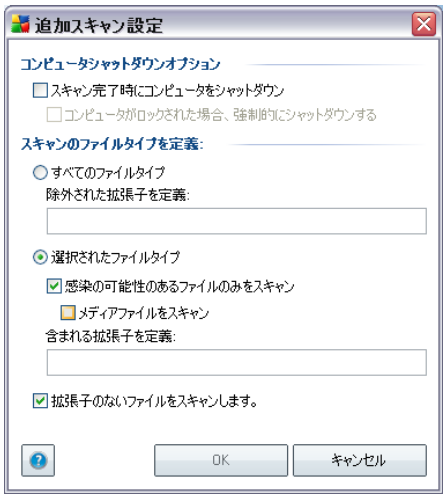


スキャン設定編集

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***リンクを押して、***完全コンピュータスキャンのスキャン設定を変更***ダイアログに進みます。***特に理由がない場合は、このデフォルト設定を保持することを推奨します。***

- ***スキャンパラメータ*** - スキャンパラメータのリストでは、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。デフォルトでは、ほとんどのパラメータがオンとなっており、スキャン中、自動的に使用されます。

- ***追加スキャン設定*** - このリンクからは、新しい [追加スキャン設定] ダイアログを開きます。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*** - 実行中のスキャンプロセス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***) 確定すると、現在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***) が有効化されます。

- ***スキャンのファイルタイプを定義*** - 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。

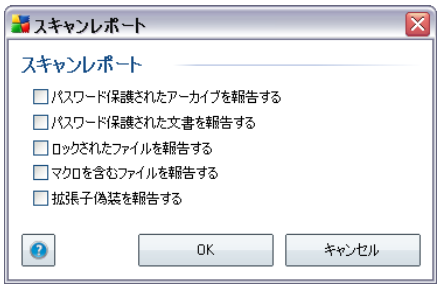
  - ***選択されたファイルタイプ*** - 感染の可能性のあるファイルのみを指定できます (*一部のプレーンテキストファイルやその他の非実行可能ファイルなど、感染の可能性がないファイルはスキャンされません*)。これには、メディアファイル (*ビデオ、オーディオファイル - これらのファイルは多くの場合、サイズが非常に大きく、ウィルスに感染している可能性が非常に低いため、このボックスのチェックを外している場合、スキャン時間がさらに短縮されます*) が含まれます。ここでも、必ずスキャンする必要があるファイルの拡張子を指定できます。

  - オプションとして、***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なものであり、常にスキャンするべきです。

- ***スキャンプロセス優先度*** - スライダを使用して、スキャンプロセス優先度を変更します。デフォルトでは、優先度は、スキャンプロセスの速度とシステムリソース消費を最適化する中レベル (*自動スキャン*) に設定されています。システムリソース負荷を最小限化するようにスキャンプ

ロセスの速度を遅くして実行（*コンピュータで作業をする必要があり、スキャンにかかる時間を問わない場合に有効*）したり、システムリソース消費量の高い高速スキャン（*例えば、コンピュータが一時的に使用されていない場合等に有効*）を実行できます。

- ***追加スキャンレポートを設定*** - このリンクは、***スキャンレポート***ダイアログを開きます。このダイアログでは、レポートされる検出の種類を選択することができます。



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一です- これは**AVG スキャン/スキャンスケジュール/ スキャン方法**の章に記載されています。**完全コンピュータスキャン**のデフォルト設定を変更する場合、新しい設定をデフォルト設定として保存し、すべての完全コンピュータスキャンに使用することができます。*

12.2.2. 特定のファイルとフォルダのスキャン

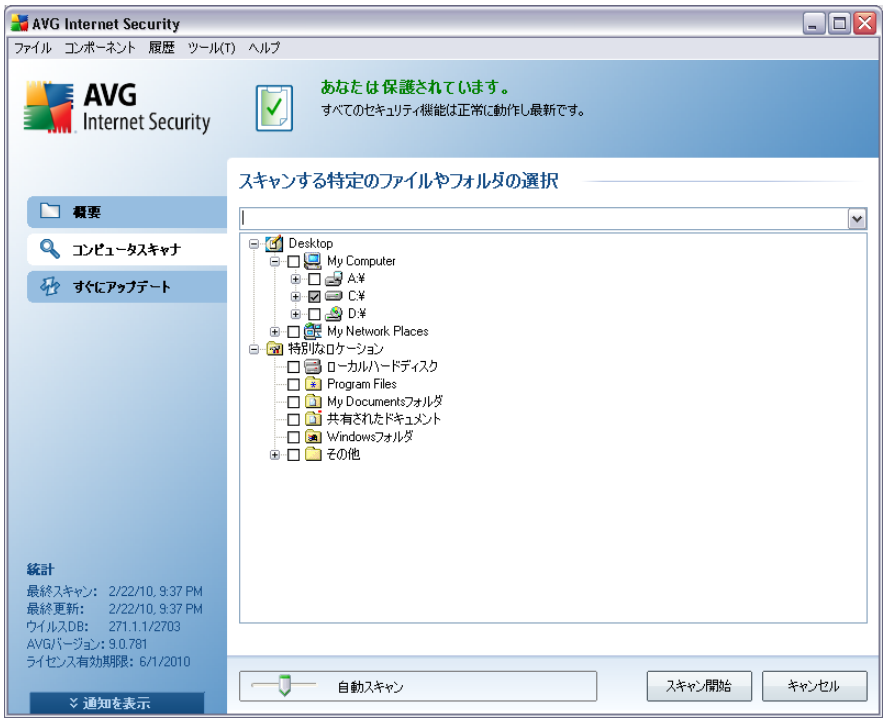
特定のファイルやフォルダをスキャン - 選択場所のみをスキャンします（*選択されたフォルダ、ハードディスク、フロッピーディスク、CD等*）. ウイルス検出、処置等のスキャン進捗***は、完全コンピュータスキャンと同じです。検出ウイルスは修復、またはウイルス隔離室に移動されます。***特定のファイルやフォルダをスキャンは、ユーザー独自のスキャン設定とスケジュールのために使用されます。

スキャン実行

特定ファイルあるいはフォルダのスキャンは、スキャンのアイコンをクリックして、スキャンインターフェースから直接起動することができます。***スキャンする特定のファイル、またはフォルダを選択***という新しいダイアログが開きます。ツリー上でスキャンしたいフォルダを選択します。選択されたフォルダへのパスは自動的に生成され、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、このスキャンからすべてのサブフォルダを除外する場合、自動生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***ボタンを押します。スキャンプロセス自体は基本的に完全コンピュータスキャンと同一です。

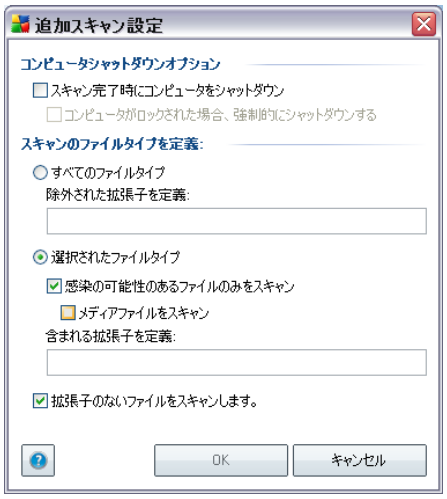


スキャン設定編集

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***を編集するオプションがあります***。***スキャン設定を変更***リンクを押して、***特定のファイルとフォルダをスキャンのスキャン設定を変更***ダイアログに進みます。***特に理由がない場合は、このデフォルト設定を保持することを推奨します。***

- ***スキャンパラメータ*** - スキャンパラメータのリストでは、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 (*この設定の詳細説明については、AVG高度な設定/スキャン/特定のファイルとフォルダをスキャン*の章を参照してください)。

- ***追加スキャン設定*** - このリンクからは、新しい [追加スキャン設定] ダイアログを開きます。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*** - 実行中のスキャンプロセス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***) 確定すると、現在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***) が有効化されます。

- ***スキャンのファイルタイプを定義*** - 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。

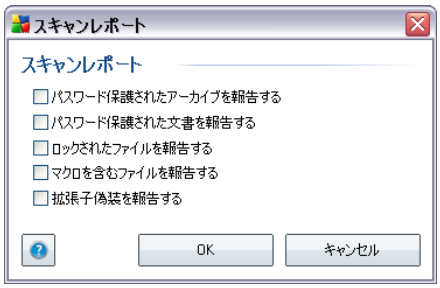
  - ***選択されたファイルタイプ*** - 感染の可能性のあるファイルのみを指定できます (*一部のプレーンテキストファイルやその他の非実行可能ファイルなど、感染の可能性がないファイルはスキャンされません*)。これには、メディアファイル (*ビデオ、オーディオファイル - これらのファイルは多くの場合、サイズが非常に大きく、ウィルスに感染している可能性が非常に低いため、このボックスのチェックを外している場合、スキャン時間がさらに短縮されます*) が含まれます。ここでも、必ずスキャンする必要があるファイルの拡張子を指定できます。

  - オプションとして、***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なものであり、常にスキャンするべきです。

- ***スキャンプロセス優先度*** - スライダを使用して、スキャンプロセス優先度を変更します。デフォルトでは、優先度は、スキャンプロセスの速度とシステムリソース消費を最適化する中レベル (*自動スキャン*) に設定されています。システムリソース負荷を最小限化するようにスキャンプ

ロセスの速度を遅くして実行（*コンピュータで作業をする必要があり、スキャンにかかる時間を問わない場合に有効*）したり、システムリソース消費量の高い高速スキャン（*例えば、コンピュータが一時的に使用されていない場合等に有効*）を実行できます。

- ***追加スキャンレポートを設定*** - このリンクは、***スキャンレポート***ダイアログを開きます。このダイアログでは、レポートされる検出の種類を選択することができます。



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一です- これは**AVG スキャン/スキャンスケジュール/ スキャン方法**の章に記載されています。**特定のファイルやフォルダスキャン**のデフォルト設定を変更する場合、新しい設定をデフォルト設定として保存し、すべての特定のファイルやフォルダをスキャンに使用することができます。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することができます（すべてのカスタマイズされたスキャンは、現在のファイルやフォルダのスキャン設定に基づいています）。*

12.2.3. ルートキットスキャン

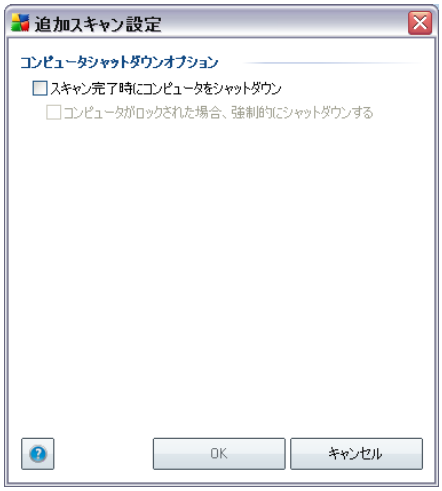
ルートキットスキャンは、ルートキット（*コンピュータの悪意のある活動を隠すことができるプログラムや技術*）の存在の可能性があるかどうかコンピュータを検索します。ルートキットが検出されても、必ずしもコンピュータが感染しているというわけではありません。通常のアプリケーションの特有のドライバやセクションが誤ってルートキットとして検出される場合があります。

スキャン実行

ルートキット対策スキャンは、スキャンのアイコンをクリックして、スキャンインターフェース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。スキャンインターフェースでは、次の設定のみが可能です。

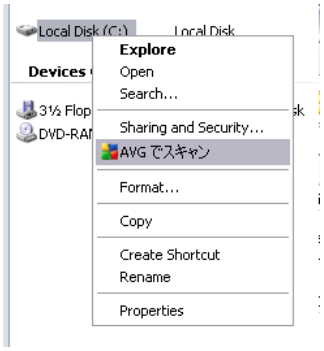
- ***自動スキャン*** - スライダを使用して、スキャンプロセス優先度を変更します。デフォルトでは、優先度は、スキャンプロセスの速度とシステムリソース消費を最適化する中レベル（*自動スキャン*）に設定されています。システムリソース負荷を最小限化するようにスキャンプロセスの速度を遅くして実行（*コンピュータで作業をする必要があり、スキャンにかかる時間を問わない場合に有効*）したり、システムリソース消費量の高い高速スキャン（*例えば、コンピュータが一時的に使用されていない場合等に有効*）を実行できます。

- ***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***(***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***) に関するコンピュータのシャットダウンのタイミングを定義できます。



12.3. シェル拡張スキャン

完全コンピュータスキャンあるいは特定エリアのスキャンで起動される予め定義されたスキャンのほかにも、**AVG 9 Internet Security**は Windows Explorer 環境での特定オブジェクトの直接クイックスキャンオプションを提供しています。不明なファイルを開きたい場合、そのファイルのみをチェックすることができます。以下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、右クリックして、コンテントメニューを開きます。
- ***AVG でスキャン***を選択します。

12.4. コマンドラインスキャン

AVG 9 Internet Security には、コマンド ラインからスキャンを実行時のオプションがあります。サーバー上のインスタンスに対して、またはコンピュータのブート後に自動的に起動されるバッチスクリプトを作成する際に、このオプションを使用することができます。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して、コマンドラインからスキャンを起動することができます。

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以下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

コマンドのシンタックス

コマンドの構文は以下の通りです。

- ***avgscanx / パラメータ*** ... 例えば、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、これらのパラメータを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、選択された場所の正確なパスを指定する必要があります）は、値は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、該当するコマンドをパラメータ/?を付加して入力します。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、スキャンされるコンピュータのエリアを指定する/SCANです。オプションのより詳細は説明については、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、プロセスを停止できます。

グラフィックインターフェースから起動される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起動する可能性もあります。スキャン自体はコマンドラインから起動され、***コマンドラインコンポーサー***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かれるヘルプファイルを参照してください。

12.4.1. 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 / Scans 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)

12.5. スキャンスケジュール

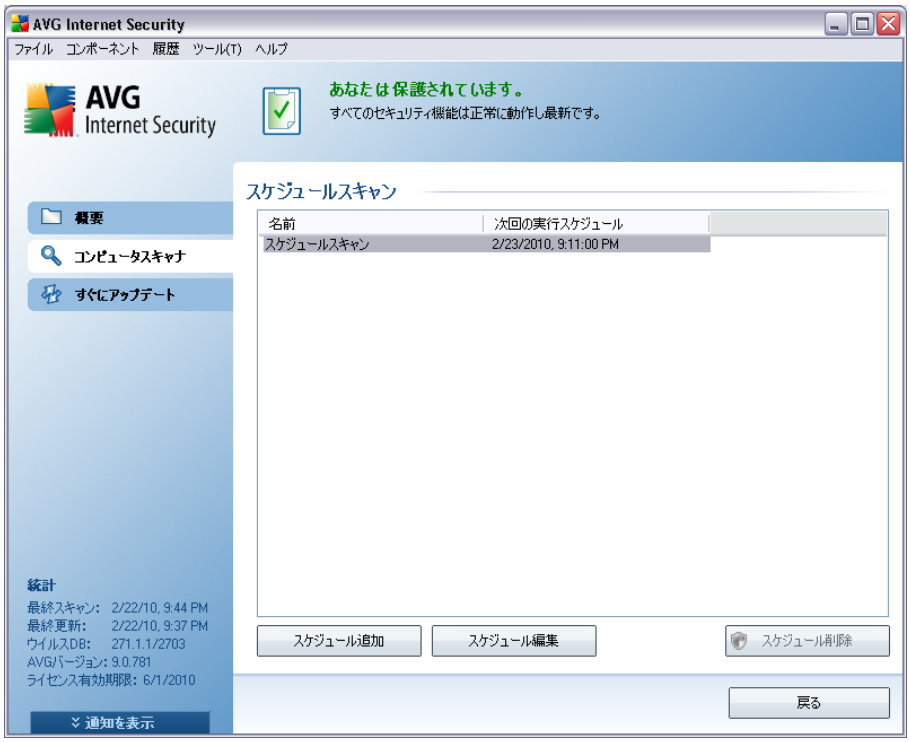
AVG 9 Internet Security では、オンデマンドで（例えば、ウイルスに感染した場合）、あるいはスケジュールに基づいてスキャンを実行できます。スケジュールに基づいてスキャンを実行することを強く推奨します。この方法で、コンピュータが感染の可能性から保護されていることを保証でき、スキャンがいつ起動しているかを考える必要がありません。

全コンピュータをスキャンを少なくとも週に1度定期的に実行して下さい。ただし、可能な場合は、コンピュータのスキャンを毎日行ってください。デフォルト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り、スケジュールが実行されなかった場合、スケジュールはコンピュータの起動時にスキャンを実行するように設定してください

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。

- ***スケジュール追加*** - ボタンは***スケジュール済スキャン設定***ダイアログ、***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することができます。
- ***スケジュール編集*** - このボタンは既存スケジュールを選択した場合にのみ使用されます。このボタンをクリックすると***スケジュール済スキャン設定***ダイアログ、***スケジュール設定***タブが表示されます。選択されたスキャンのパラメータを編集することができます。
- ***スケジュール削除*** - このボタンも既存スケジュールを選択した場合にのみ有効となります。選択したスキャンがリストから削除されます。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。デフォルトで定義されている***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

12.5.1. スケジュール設定

新しいスキャンと通常の起動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デフォルトタブ*)、***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

スケジュール済のスキャンの設定 ***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デフォルト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押してください。
- ***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デフォルトダイアログに戻ります。

12.5.2. スキャン方法

スキャン方法 タブには、任意でオン/オフできるスキャンパラメータのリストが表示されます。デフォルトでは、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、予め定義された設定を維持することを推奨します。

- ***自動感染修復/除去*** - (*デフォルトではオン*) ウィルスがスキャン実行中に特定され、修復可能な場合は、自動で修復されます。感染ファイルを自動的に修復できない場合やこのオプ

ションをオフにする場合、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をレポート*** - (*デフォルトではオン*): 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レポート*** - 前のオプションが有効になっている場合、このボックスにチェックを付けると、スパイウェアの拡張パッケージも検出できます。拡張パッケージとは、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。

- ***Tracking Cookieをスキャン*** - (*デフォルトではオン*) スパイウェア対策***コンポーネントのこのパラメータは、スキャン実行中にCookieが検出されるように定義します。***(*HTTP cookieは、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ユーザーの特定の情報の認証、トラッキング、メンテナンスに使用されます*)

- ***アーカイブ内をスキャン*** - (*デフォルトではオン*) このパラメータは、ZIPやRAR等のアーカイブ形式で圧縮されている場合でも、すべてのファイルがスキャンによりチェックされるように定義します。

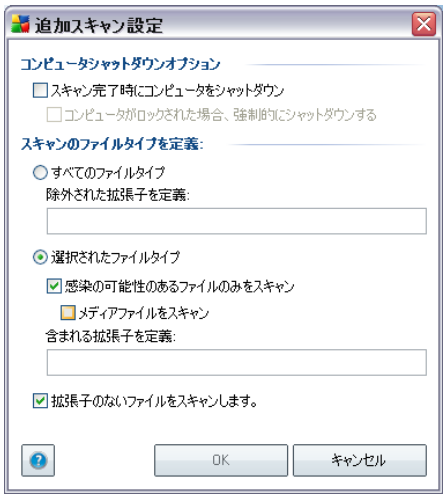
- ***ヒューリスティック分析を使用*** - (*デフォルトではオン*) ヒューリスティック分析 (*仮想コンピュータ環境でのスキャンオブジェクトの動的エミュレーション*) は、スキャン実行中にウイルス検出に使用される方法の1つです。

- ***システム環境をスキャン*** - (*デフォルトではオン*) コンピュータのシステムエリアもチェックされます。

- ***ルートキットをスキャン*** - 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する場合、この項目にチェックを付けます。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行うことができます。

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*** - このリンクからは、新しい [追加スキャン設定] ダイアログを開きます。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*** - 実行中のスキャンプロセス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***) 確定すると、現在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***) が有効化されます。

- ***スキャンのファイルタイプを定義*** - 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。

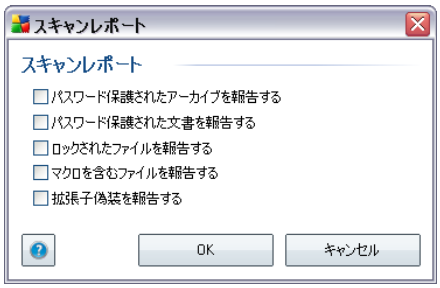
  - ***選択されたファイルタイプ*** - 感染の可能性のあるファイルのみを指定できます (*一部のプレーンテキストファイルやその他の非実行可能ファイルなど、感染の可能性がないファイルはスキャンされません*)。これには、メディアファイル (*ビデオ、オーディオファイル - これらのファイルは多くの場合、サイズが非常に大きく、ウィルスに感染している可能性が非常に低いため、このボックスのチェックを外している場合、スキャン時間がさらに短縮されます*) が含まれます。ここでも、必ずスキャンする必要があるファイルの拡張子を指定できます。

  - オプションとして、***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なものであり、常にスキャンするべきです。

- ***スキャンプロセス優先度*** - スライダを使用して、スキャンプロセス優先度を変更します。デフォルトでは、優先度は、スキャンプロセスの速度とシステムリソース消費を最適化する中レベル (*自動スキャン*) に設定されています。システムリソース負荷を最小限化するようにスキャンプ

ロセスの速度を遅くして実行（*コンピュータで作業をする必要があり、スキャンにかかる時間を問わない場合に有効*）したり、システムリソース消費量の高い高速スキャン（*例えば、コンピュータが一時的に使用されていない場合等に有効*）を実行できます。

- ***追加スキャンレポートを設定*** - このリンクは、***スキャンレポート***ダイアログを開きます。このダイアログでは、レポートされる検出の種類を選択することができます。



注意：*デフォルトでは、スキャンには最適なパフォーマンスで実行されるように設定されています。このスキャン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強く推奨します。設定変更は経験のあるユーザーが行ってください。これ以外のスキャンの設定オプションについては、****ファイル/ 高度な設定*** *システムメニューアイテム****からアクセスできる****高度な設定ダイアログを参照してください。*

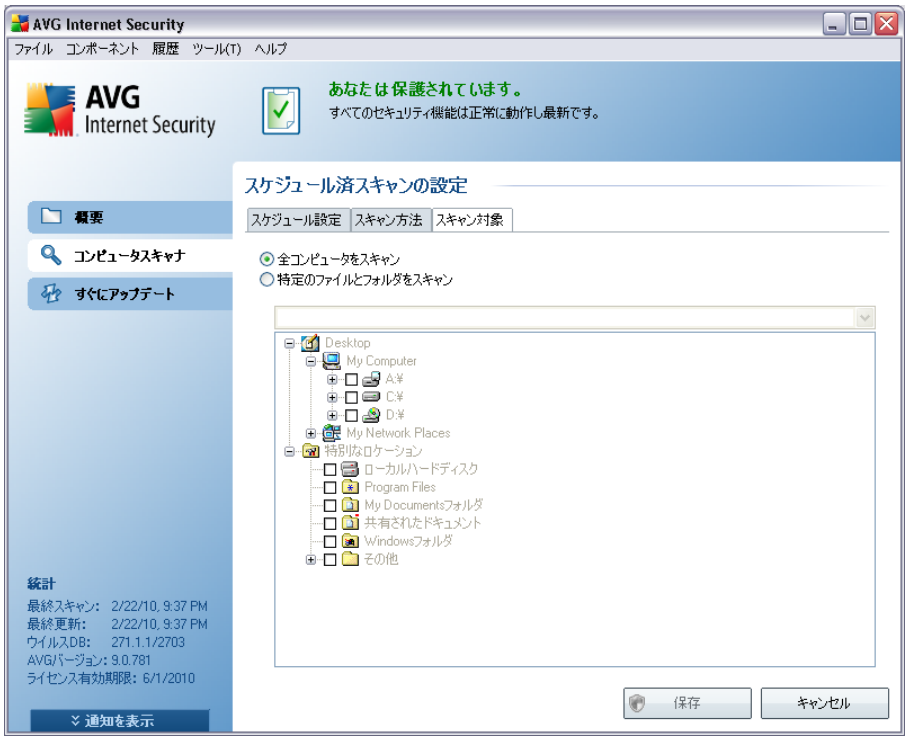
コントロールボタン

スケジュール済のスキャンの設定***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デフォルト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押してください。

- ***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デフォルトダイアログに戻ります。

12.5.3. スキャン対象



[***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。選択されたフォルダは、ダイアログ上部のテキストフィールドに表示され、ドロップダウンメニューに選択されたスキャン履歴が保持されます。希望するフォルダへのフルパスを手動で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リストが表示されます。

- ***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\
- ***マイ ドキュメント フォルダ*** - C:\Documents and Settings\User\My Documents\

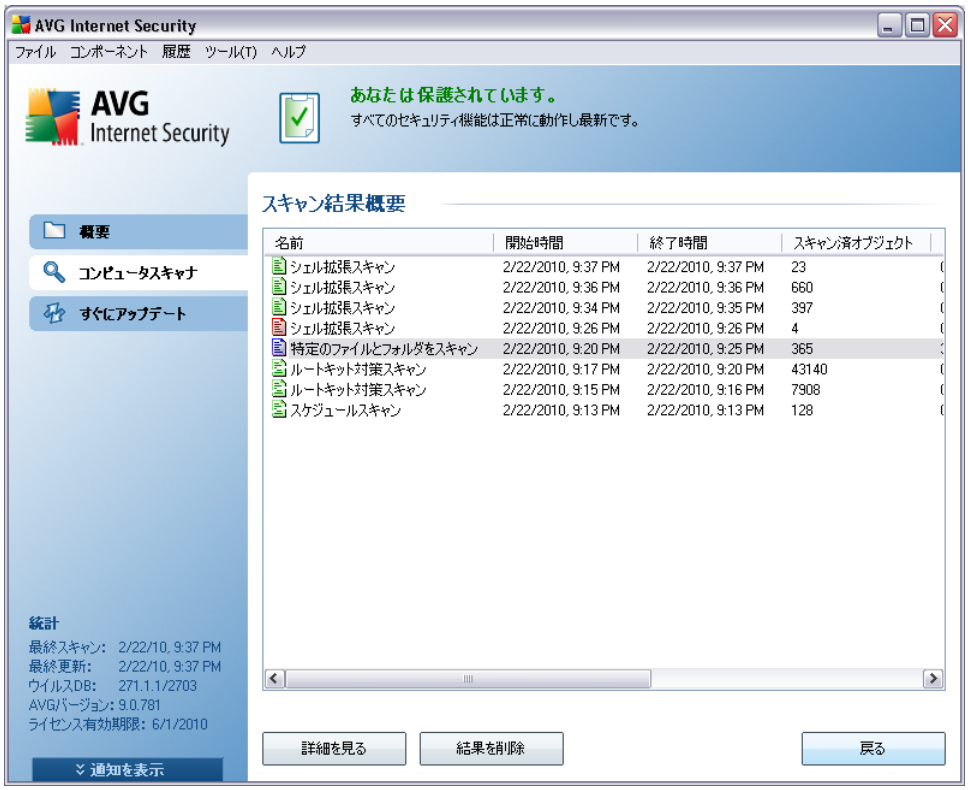
- ***共有ドキュメント*** - C:\Documents and Settings\All Users\Documents\
- ***Windows フォルダ*** - C:\Windows\
- ***その他***
    - *システム ドライブ* - オペレーティング システムがインストールされているハードドライブ (通常は C:)
    - *システム フォルダ* - Windows/System32
    - *一時 ファイル フォルダ* - Documents and Settings/User/Local Settings/Temp
    - *一時 インターネット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

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

スケジュール済のスキャンの設定 ***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デフォルト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押してください。
- ***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デフォルトダイアログに戻ります。

12.6. 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。

12.7. 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)。

12.7.1. 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。

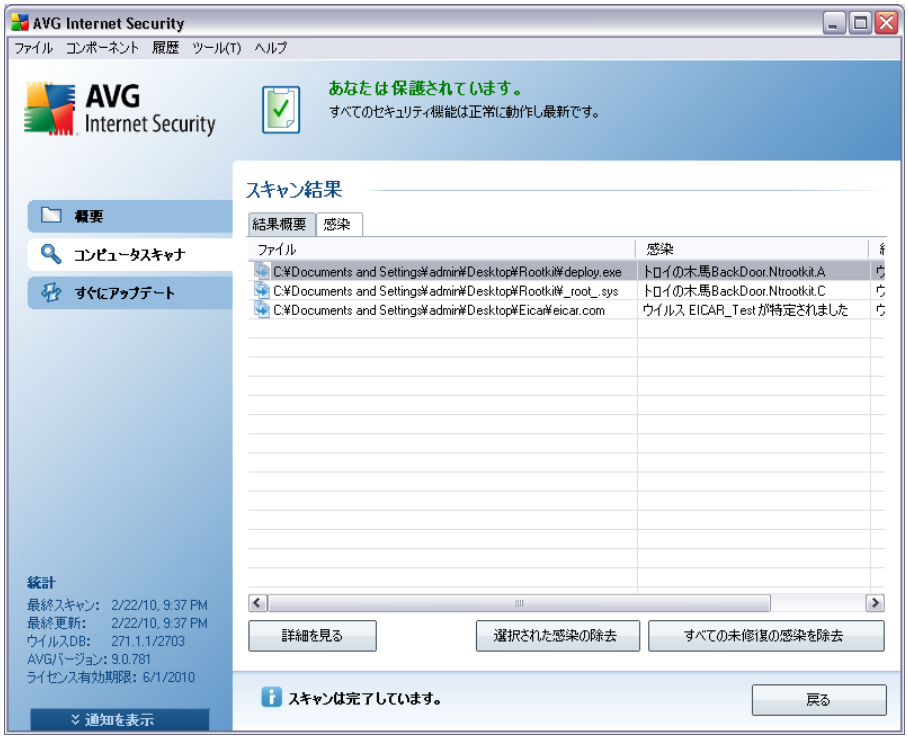
- 検出されたウイルス感染/スパイウェア
- 除去されたウイルス感染/スパイウェア
- 除去あまたは修復不可能なウイルス感染/スパイウェア数

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。

12.7.2. 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。

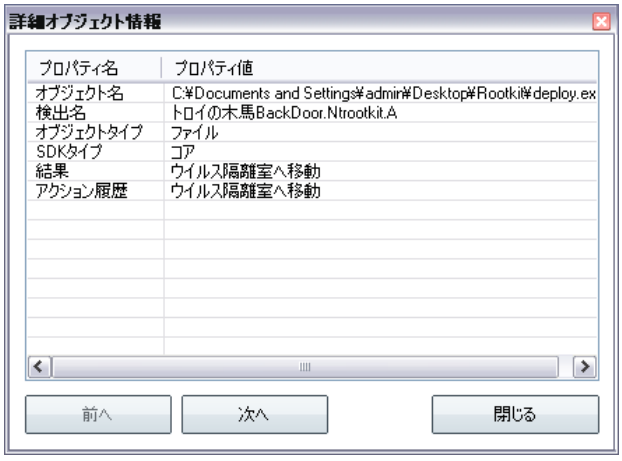
- ***ファイル*** - 感染オブジェクトの元の場所へのフルパス
- ***感染*** - 検出されたウイルス名 (*ウイルスの詳細は、オンラインのウイルスエンサイクロペディアを参照してください*)
- ***結果*** - スキャン中に検出された感染オブジェクトの現在のステータス

- ***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例外を追加*** - 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***詳細スキャン結果情報***という新しいダイアログを開きます。



このダイアログでは、感染オブジェクトの場所に関する情報が表示されます ***プロパティ名***

)。***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。

- ***選択された感染を除去*** - このボタンを使用して、選択された検出を***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***ウイルス隔離室に移動された検出を削除します。***
- ***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。

12.7.3. スパイウェアタブ

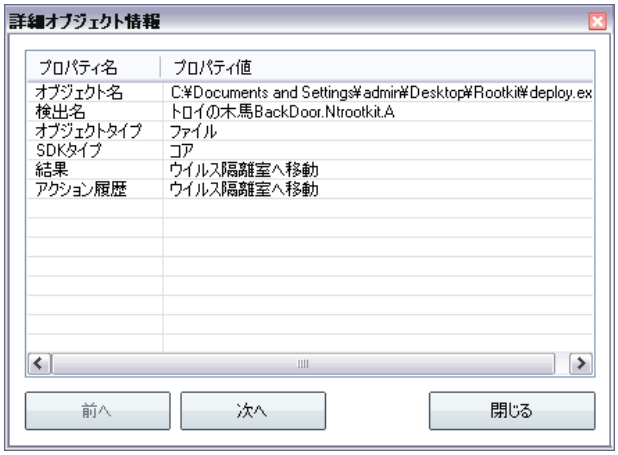
スパイウェアタブは、スキャン中にスパイウェアが検出された場合、***スキャン結果***ダイアログでのみ表示されます。***このタブは3つのセクションに分かれ、以下の情報が表示されます。

- ***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***詳細スキャン結果情報***という新しいダイアログウィンドウを開きます。

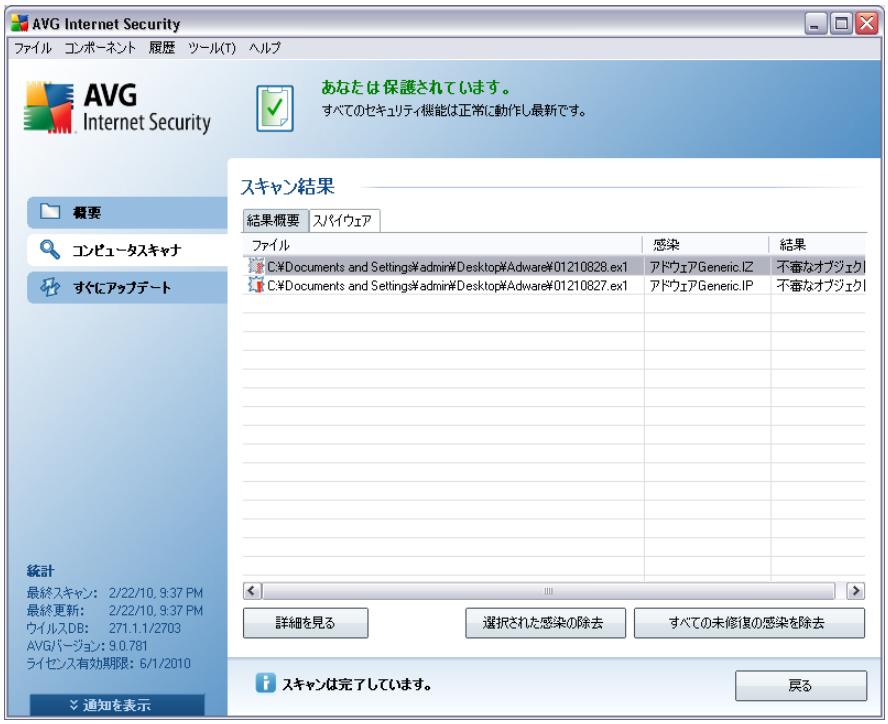


このダイアログでは、感染オブジェクトの場所に関する情報が表示されます(***プロパティ名***)。***前へ***/***次へ***ボタンを使用して、特定の検出情報を見ることができます。***閉じる***ボタンを使用して、このダイアログを閉じることができます。

- ***選択された感染を除去*** - このボタンを使用して、選択された検出を***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***ウイルス隔離室に移動された検出を削除します。***
- ***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。

12.7.4. 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検査によって警告のみが検出される場合は、何も対応する必要はありません。



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*** - 非表示のファイルはデフォルトでは、Windows上では見ることができません。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されることを避けようとする場合があります。AVG 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、***AVG 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。

12.7.5. ルートキットタブ

ルートキットスキャンを起動した場合や、手動でルートキット対策スキャンオプションを***完全コンピュータスキャン***(***このオプションは既定でオフになっています***)に追加した場合、[*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しで、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のコントロールを掌握するよう意図されているため、ハードウェアへのアクセスはほとんど必要とされません。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で、システム上でその存在を隠すように動作します。一般的に、それは同時にトロイの木馬でもあり、システムで実行しても安全であるかのようにユーザーを騙し、信じこませます。これを実現させる技術によって、実行中のプロセスをプログラム監視から隠したり、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。

このタブの構成は基本的に、***感染タブ***や***スパイウェアタブ***と同じです。

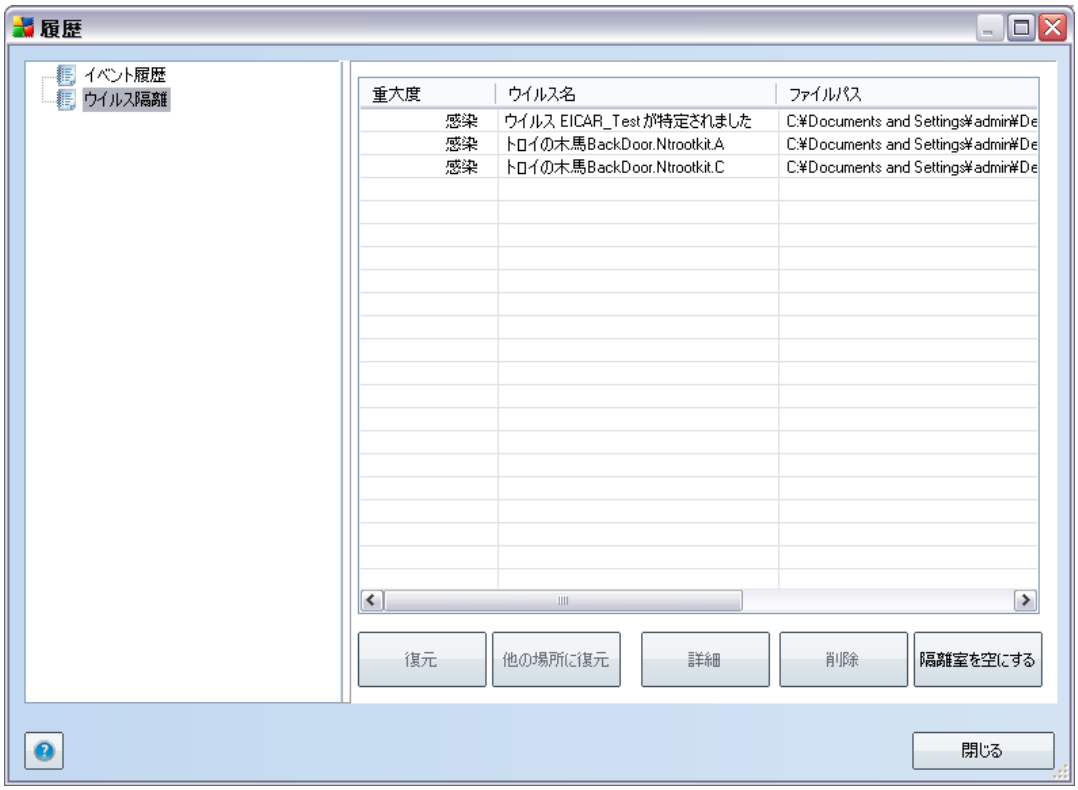
12.7.6. 情報タブ

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 スキャンは、感染していない可能性があるが、疑わしいファイルを検出することができます。このようなファイルは***警告***か***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 *(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 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)*、AVG はこの不一致を報告します。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るため、AVG が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)*。

12.8. 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疑わしい、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がそれを自動的に修復できない場合、この疑わしい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 9 Internet Security**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。

- ***ウイルス名*** - ウイルスエンサイクロペディア (オンライン) にしたがって、検出された感染名を表示します。
- ***ファイルパス*** - 検出された感染ファイルのフルパス
- ***元のオブジェクト名*** - 表にリストされるすべての検出されたオブジェクトは、スキャンプロセス中にAVGによって与えられる標準名で表示されます。オブジェクトの元の名前が既知の特定の名前であった場合 (*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*)、このカラムにこの名前が表示されます。
- ***保存日*** - 疑わしいファイルが検出され、***ウイルス隔離室に移動された日時***

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、以下のコントロールボタンが使用可能です。

- ***復旧*** - 感染ファイルをディスク上の元の場所に復元します。
- ***元の名前で復旧*** - 検出された感染オブジェクトを***ウイルス隔離室***から選択されたフォルダに移動する場合は、このボタンを使用します。疑わしい検出されたオブジェクトは元の名前で保存されます。元の名前がわからない場合は、標準名が使用されます。
- ***詳細*** - このボタンは、***IDP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***内のファイルを削除します。ウイルス隔離室から削除することで、これらのファイルは、ディスクから削除され、元に戻すことはできません (ごみ箱には移動されません)。

13. AVGアップデート

AVGを最新の状態に保つことはすべての新しいウイルスがすぐに検出されることを保証するうえで非常に重要です。

AVG のインストール処理中には、AVG を更新する頻度を指定するよう求められます。利用可能なオプションは、*4 時間ごと*または*毎日*（*定期スキャンと更新のスケジュール* ダイアログを参照）です。AVG アップデートは定期的なスケジュールでリリースされませんが、新しい脅威の量と重要度に対応するには、すくなくとも毎日新しいアップデートを確認することが推奨されます。4 時間ごとにチェックすることで、毎日 **AVG 9 Internet Security** が最新の状態に保たれる事が保証されます。

13.1. アップデートレベル

AVG は、2 つの選択可能なアップデートレベルを提供します。

- ***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。一般的には、コードの変更は含まれす、定義データベースのみをアップデートします。このアップデートは、利用可能な場合、すぐに適用する必要があります。
- ***プログラムアップデート***には、さまざまなプログラムの変更、修正、および改善が含まれています。

アップデートをスケジュールする際に、ダウンロードの優先レベルを選択できます。

***注意**: スケジュール済みプログラムアップデートおよびスケジュール済みスキャンの時間と一致する場合は、アップデートプロセスが最優先され、スキャンは中断されます。*

13.2. アップデートタイプ

2 つのタイプのアップデートを区別することができます。

- ***オンデマンドアップデート***は、必要に応じていつでも実行できる即時 AVG アップデートです。
- ***スケジュール済のアップデート*** - AVG ではアップデートスケジュールをあらかじめ設定することもできます。スケジュールされたアップデートは、設定にしたがって定期的に実行されます。新しいアップデートファイルが特定の場所にある場合、それらはインターネットから直接、またはネットワークディレクトリを介してダウンロードされます。入手可能な新しいアップデートがない場合は何も実行されません。

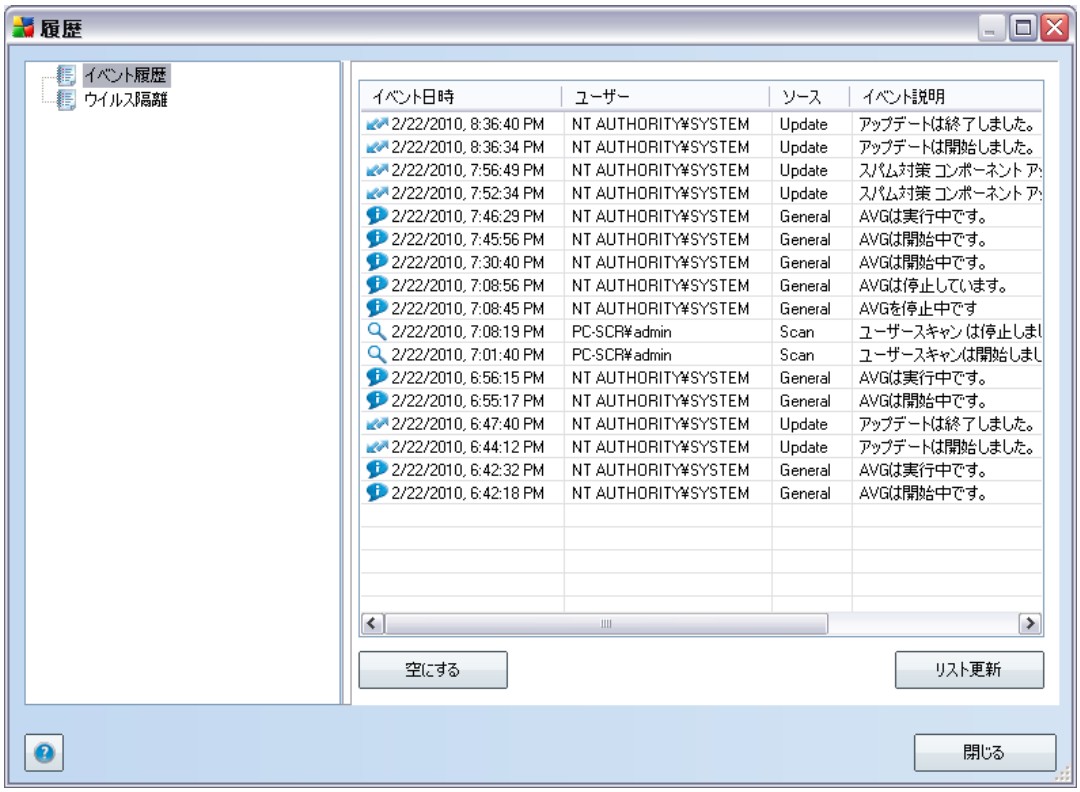
13.3. アップデートプロセス

すぐにアップデートクイックリンクによって、アップデートプロセスをすぐに実行できます。このリンクは、AVG ユーザーインターフェースダイアログからいつでも使用可能です。ただし、アップデートマネージャコンポーネントのアップデートスケジュール編集で説明されているように、定期的にアップデートを実行することが強く推奨されます。

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。この場合、AVGはダウンロードを開始し、アップデートプロセスが実行されます。アップデートプロセス中は、***アップデート***インターフェースにリダイレクトされます。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（*アップデートファイルサイズ、受信データ、ダウンロード速度、経過時間等*）。

注意：*AVGプログラムアップデートの前に、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ことをお勧めします。*

14. イベント履歴



イベント履歴ダイアログはシステムメニューの履歴/イベント履歴ログからアクセスできます。このダイアログでは、**AVG 9 Internet Security**動作中に発生した重要なイベントのサマリを見ることができます。***イベント履歴***は以下のイベントを記録します。

- AVGアプリケーションの更新情報
- スキャン開始、終了、定義（自動実行スキャンを含む）
- 発生場所を含む、常駐シールド、スキャンによるウイルス検出関連イベント
- 他の重要イベント

コントロールボタン

- ***空にする*** - すべてのイベントリストエントリを削除します

- ***リスト更新*** - イベントリストエントリをすべて更新します

15. FAQとテクニカルサポート

AVG に関する問題がある場合は、ビジネスの場合でも技術的な場合でも、AVG ウェブサイトの ***FAQ*** セクション (http://www.avg.com/) を参照してください。

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