AVG 9 Anti-Virus plus Firewall

ユーザーマニュアル

ドキュメント改訂　90.6　(14.9.2009)

目次

1. はじめに

このユーザーマニュアルは **AVG 9 Anti-Virus plus Firewall** の総合的なドキュメントです。

AVG 9 Anti-Virus plus Firewallのご購入ありがとうございました。

AVG 9 Anti-Virus plus Firewall 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。 **AVG 9 Anti-Virus plus Firewall** は、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、完全に再設計されました。

新しい**AVG 9 Anti-Virus plus Firewall** 製品は、よりアグレッシブで、より高速のスキャンを組み合わせた、効率的なインターフェースを提供します。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 Anti-Virus plus Firewall は以下のオペレーティングシステムに対応しています。

- 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、すべての版）
- Windows 7（x86 および x64、すべての版）

（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）

2.2. 最小ハードウェア要件

AVG 9 Anti-Virus plus Firewall の最低ハードウェア要件は以下の通りです。

- Intel Pentium CPU 1,2 GHz
- ハードディスク空き容量 250MB以上（インストールのため）
- 256MB RAM

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。これによって、最新バージョンをインストールすることが確実となりますAVG 9 Anti-Virus plus Firewall。

適切なインストールファイルの選択を支援する新しい AVG ダウンロードマネージャー ツールを試してみ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 ダウンロードマネージャー　適切な AVG 製品インストールファイルの選択を支援する簡単なツールです。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 ダウンロードマネージャー**　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 2000（SP4 + SRP ロールアップ）、Windows XP（SP2 以上）、Windows Vista（すべての版）のみです。*

AVG ダウンロードマネージャー　AVG ウェブサイト（http://www.avg.com/ ）からダウンロードできます。
AVG ダウンロードマネージャー　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 ダウンロードマネージャー　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

次のステップでは、アップデートを検索できるように **AVG ダウンロードマネージャー** はインターネット接続の確立を試みます。**AVG ダウンロードマネージャー** が接続性テストを完了するまでは、ダウンロードプロセス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 ダウンロードマネージャー 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 ダウンロードマネージャー** の次のステップに進みます。

4.4. ライセンス種別を選択

このステップでは、ダウンロードする製品のライセンス種別を選択するように要求されます。入力された説明によって、最も適した製品を選択することができます。

- ***完全版*** - つまり ***AVG Anti-Virus*** 、***AVG Anti-Virus plus Firewall*** 、または ***AVG Internet Security***

- ***試用版*** - 30 日間に限定して AVG 完全製品版の全機能を利用する機会を提供します
- ***無料版*** - 個人ユーザーに無料で保護を提供しますが、アプリケーション機能は制限されていますまた、無料版には有料製品版で利用できる機能の一部しか含まれません。

4.5. インストールするファイルをダウンロード

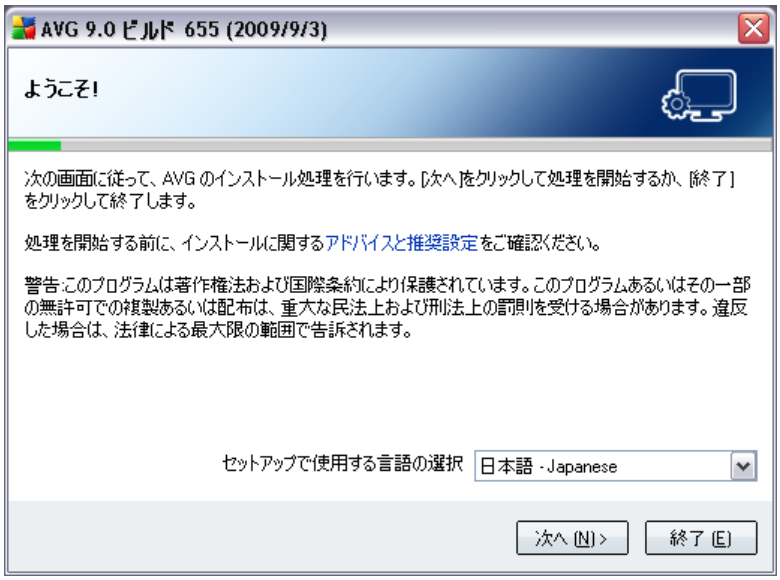
これで、**AVG ダウンロードマネージャー** でインストールパッケージダウンロードを開始し、インストールプロセスを起動するために必要なすべての情報を入力しました。次に、 AVG インストールプロセス に進んでください。

5. AVGインストールプロセス

コンピュータにをインストールするには、最新のインストールファイルを入手する必要があります。 **AVG 9 Anti-Virus plus Firewall** 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。ファイルはAVGのWebサイト（http://www.avg.com/ ）***)のダウンロード***セクションから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。

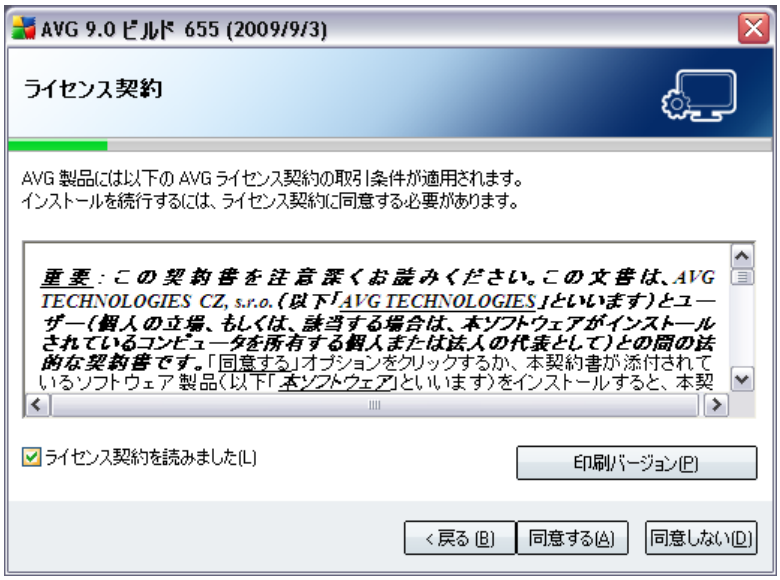
5.1. インストールの実行



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



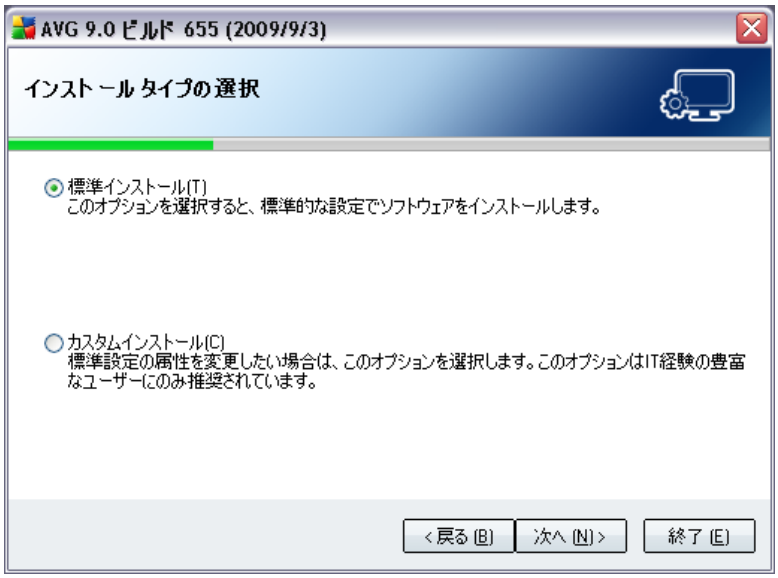
ライセンス契約 ダイアログは、AVGライセンス契約の全文を提供します。契約内容をよく読んで、[***ライセンス契約を読みました***] チェックボックスにチェックを付け、[***同意する***] ボタンをクリックして、契約を読んで理解して同意することを確認します。

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。例えば、特定のシステム要件を満たすため等。

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 Anti-Virus plus Firewall** の箱の 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 Anti-Virus plus Firewall** 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。

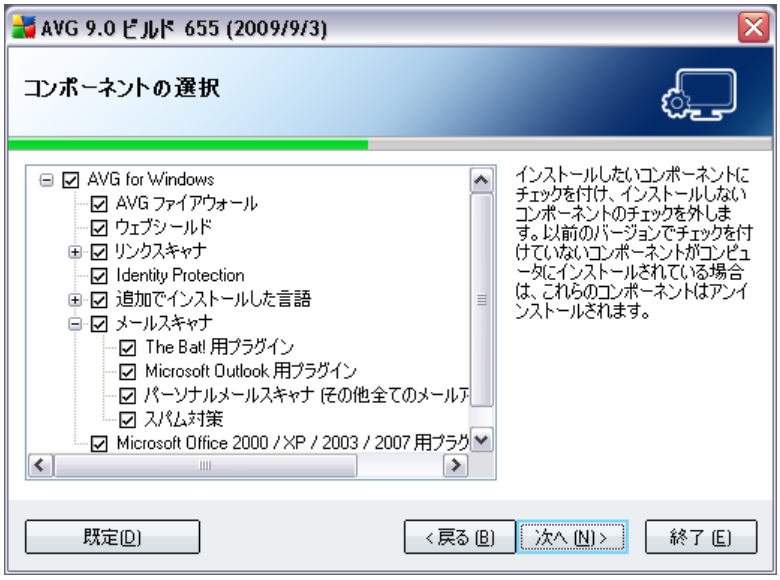
5.6. カスタムインストール - インストール先フォルダ

[***インストール先 フォルダ***] ダイアログでは、がインストールされる場所を指定します。 **AVG 9 Anti-Virus plus Firewall** 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。

この場所を変更したい場合は、 ***ブラウズ***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 ダイアログでは、インストール可能なすべてのコンポーネントが表示されます。 **AVG 9 Anti-Virus plus Firewall** 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/追加します。

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。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。

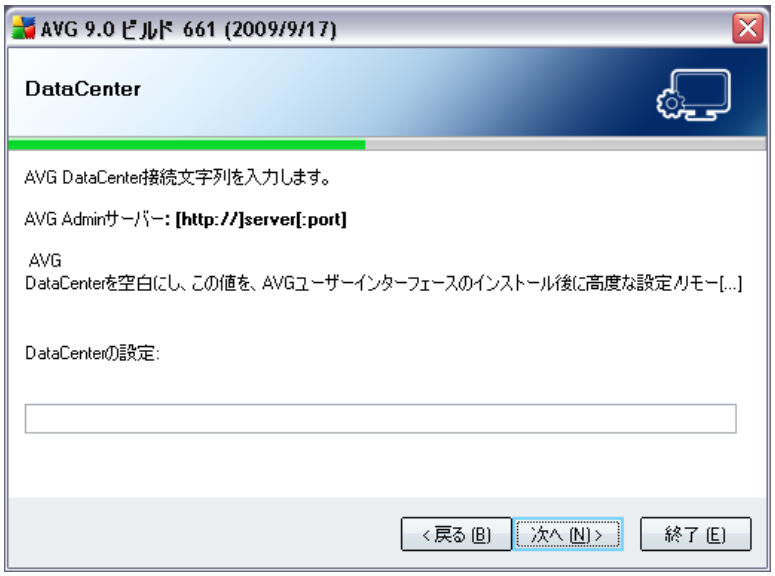
- ***リモート管理***

  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

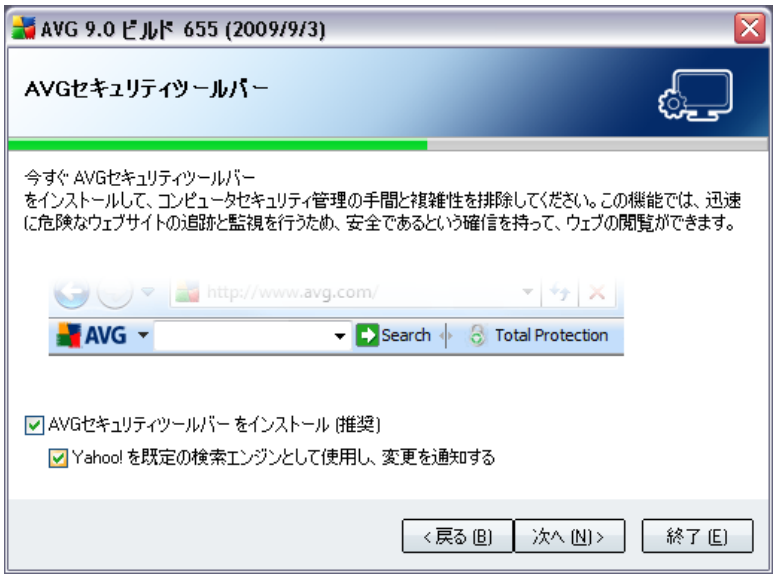
前の [***カスタムインストール - コンポーネント選択***] ダイアログで、[***遠隔管理***] アイテムのインストールを選択した場合、***AVG DataCenter*** パラメータを指定する必要があります。



[***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/遠隔管理***] 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。*

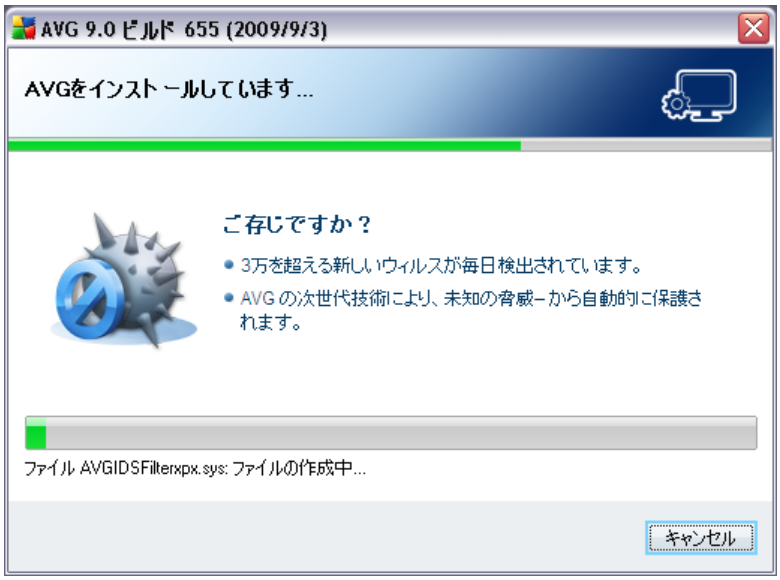
5.9. AVGセキュリティツールバー



[***AVG Security Toolbar***] ダイアログでは、***AVG Security Toolbar*** (*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。既定の設定を変更しない場合、このコンポーネントは自動的にインターネットブラウザにインストールされ、インターネット閲覧中の包括的なオンライン保護を提供します。

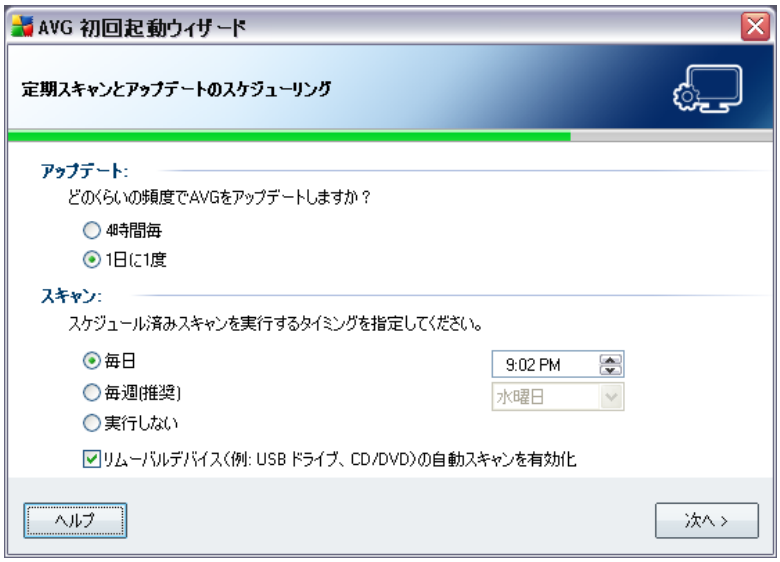
5.10. AVGのインストール

[***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。



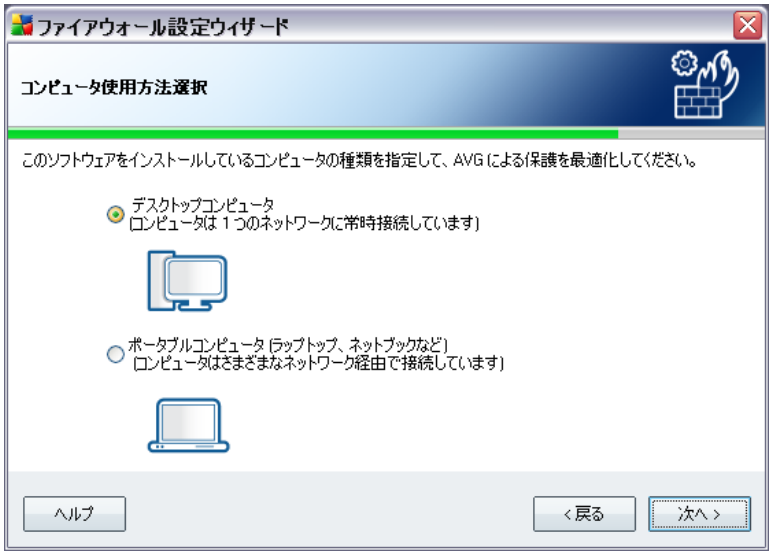
インストールプロセスの終了後、自動的に次のダイアログに進みます。

5.11. 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で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。

5.12. 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。

5.13. コンピュータネットワーク設計

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。

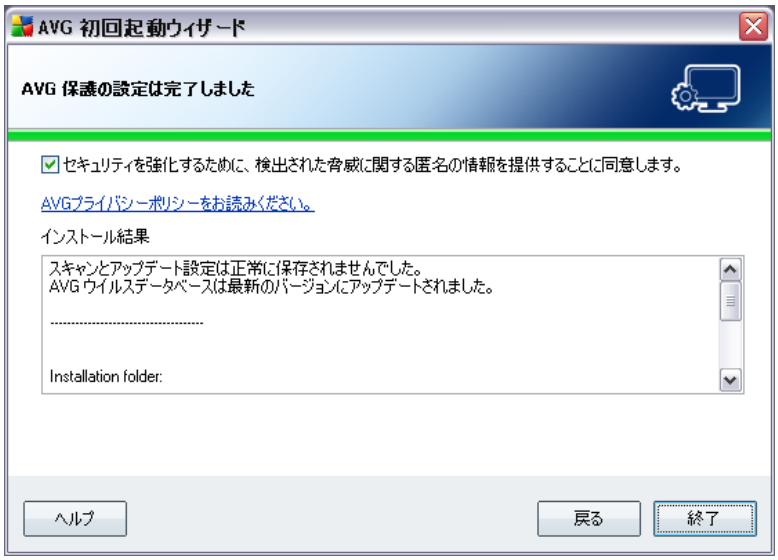
3 つの代替オプションから選択できます。

- ***直接インターネットに接続***
- ***小規模家庭用ネットワーク***
- ***ドメインにあるコンピュータ***

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。

5.14. AVG 保護設定は完了しています



AVG 9 Anti-Virus plus Firewall は設定されました。

このダイアログでは、AVG ウイ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. 製品登録

AVG 9 Anti-Virus plus Firewall 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 で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。

6.2. 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。***

6.3. 全コンピュータをスキャン

AVG 9 Anti-Virus plus Firewall 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。

6.4. Eicarテスト

AVG 9 Anti-Virus plus Firewall インストールが正常に行われたことを確認するために、EICARテストを実行することができます。

EICARテストは、ウイルス対策システムの機能を検査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、 ***Web シールド*** が警告とともにそれに反応します。この ***Web シールド*** 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。

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。

6.5. 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 Anti-Virus plus Firewall** 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。設定変更は、経験のあるユーザーが行うことを推奨します。

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 Anti-Virus plus Firewall　　メインウィンドウで開く

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 Anti-Virus plus Firewall** メインウィンドウの上部に配置されています。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 Anti-Virus plus Firewall** 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。
- ***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。
- ***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。
- ***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。
- ***Webシールド*** - ***Web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。
- ***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。***
- ***メールスキャン検出*** - ***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。
- ***Web シールド検出*** - Web 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。***
- ***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 Anti-Virus plus Firewall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 Anti-Virus plus Firewall**
- ***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 Anti-Virus plus Firewall** 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下さい。 AVG製品を登録した顧客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。
- ***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 Anti-Virus plus Firewall** の現在のセキュリティステータスに関する情報が表示されます。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。コンポーネント名は ***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。

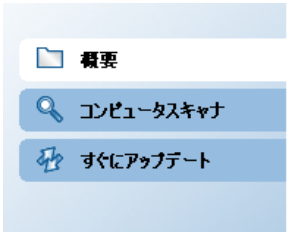

赤のアイコンはAVGが危険な状態にあることを示しています。1つあるいは複数のコンポーネントが適切に動作しておらず、AVGがコンピュータを保護できません。報告された問題を修復してください。エラーを自分で修復できない場合、 AVGテクニカルサポート チームにお問い合わせください。

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機能に直接アクセスすることができます。



- ***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（ *図 2を参照* ）。

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 Anti-Virus plus Firewall ***コンポーネント概要*** セクションには、以下のコンポーネントの情報が含まれます。

- ***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>>
- ***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>>
- ***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>>
- ***ライセンス*** は、AVGライセンス契約内容を表示します。 - 詳細>>
- ***Webシールド*** は、Web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 のグレイ色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、8.0.xxの形式で表示され、8.0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。

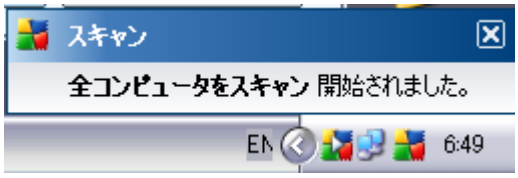
7.6. システムトレイアイコン

システムトレイアイコン （*Windowsタスクバー上*）は現在の **AVG 9 Anti-Virus plus Firewall** のステータスを示します。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（黄、黒、緑、赤）表示の場合 、***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。

エクスクラメーションマークのあるグレイのアイコンは、 問題（無効なコンポーネント、エラーステータス等）を意味します。). ***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 の活動およびプログラムの可能性のあるステータス変更（ *例：スケジュール済みのスキャンあるい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、コンポーネントステータス変化、エラーステータス発生等* ）も AVG システムトレイアイコンから開かれるポップアップウィンドウで通知します。



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、AVGインストール前にマルウェアに感染したり、**AVG 9 Anti-Virus plus Firewall** 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存在します。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. 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。*

8.3.1. 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。
- すべての定義済みプロファイルと設定の アーカイブを保持します。
- 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。

8.3.2. 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*** -予め設定され、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*** - 予め設定され、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***：

  - ***移動中のコンピュータ*** - 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することができます。このダイアログでは、使用したく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。

8.3.3. ファイアウォールインターフェース

ファイアウォール 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等）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* ***ファイル/ 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

8.4. 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。

8.4.1. 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。

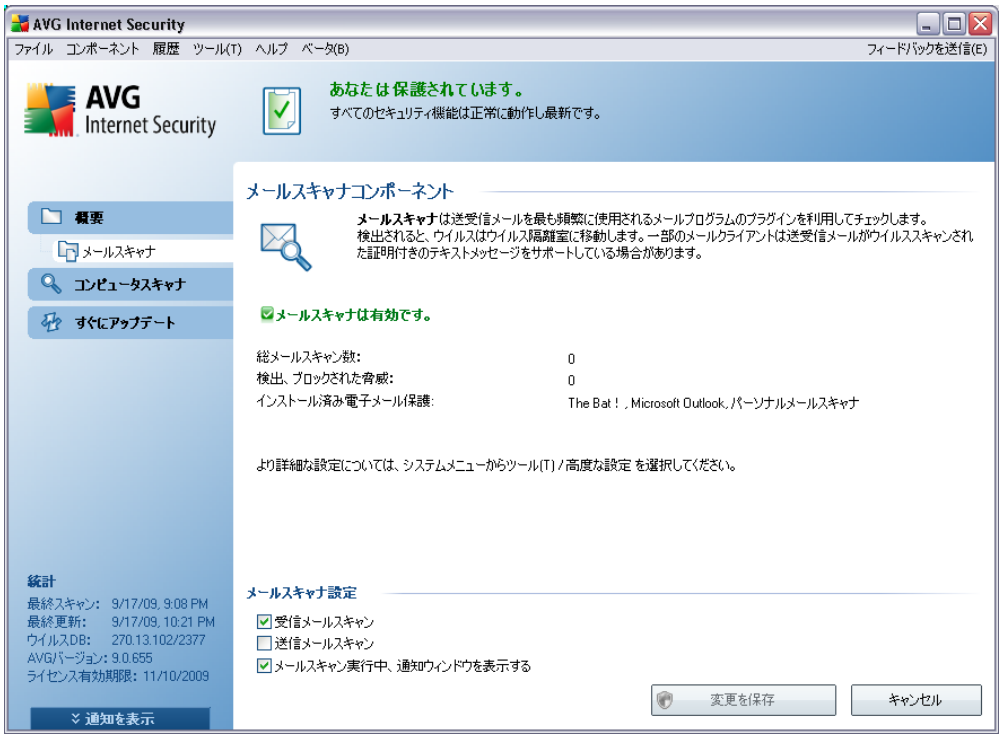
パーソナルメールスキャナ はメールクライアントとインター ネット上のメールサーバーのインターフェースとして動作します。

- ***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。*

8.4.2. 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。

- ***総メールスキャン数*** - ***メールスキャナ*** 起動後、スキャンされたメールの総数が表示されます。（ *必要に応じて、この値はリセットされます。例えば、統計目的 - 値のリセット* など）
- ***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）

- *メールがスキャン中は通知アイコンを表示* _ スキャン中に ***メールスキャナ*** コンポーネントが処理をしているタスク（サーバーへの接続、メッセージのダウンロード、メッセージスキャン等）に関する通知ダイアログを表示します（*サーバーに接続中*、*メッセージのダウンロード中*、*メッセージのスキャン中…* ）。このオプションは有効になっています。編集はできません。

メールスキャナ コンポーネントの高度な設定は、システムメニューの ***ファイル/ 高度な設定*** で変更できます。ただし、高度な設定は経験のあるユーザー向けの設定です。

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。*

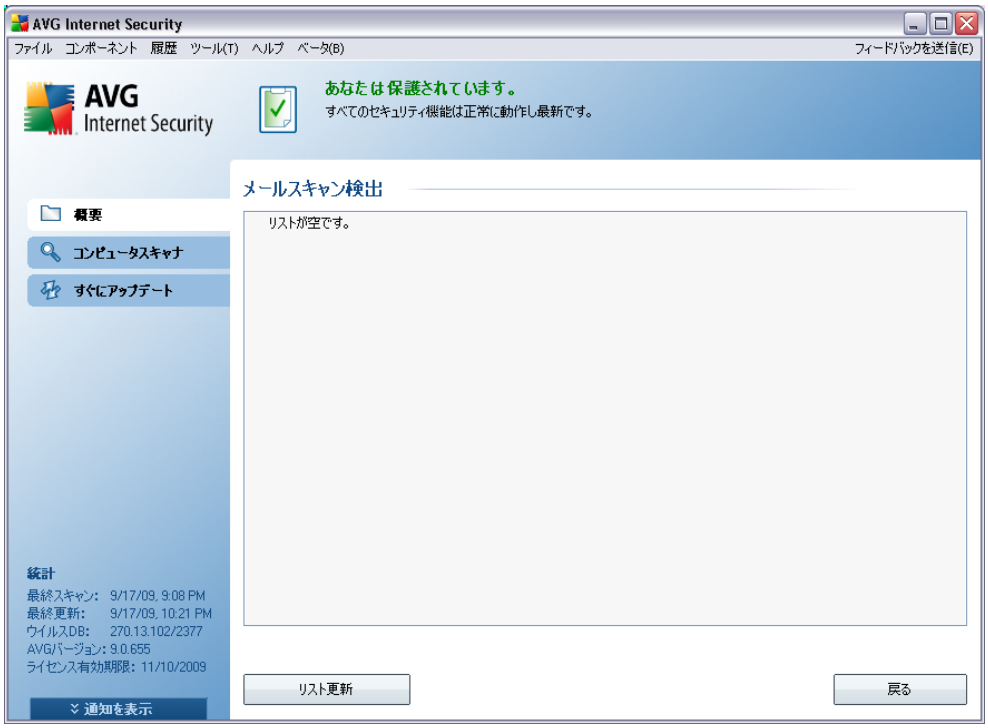
コントロールボタン

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

8.4.3. メールスキャナ検出



[***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/ メールスキャナ検出] からアクセスできます*）では、***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

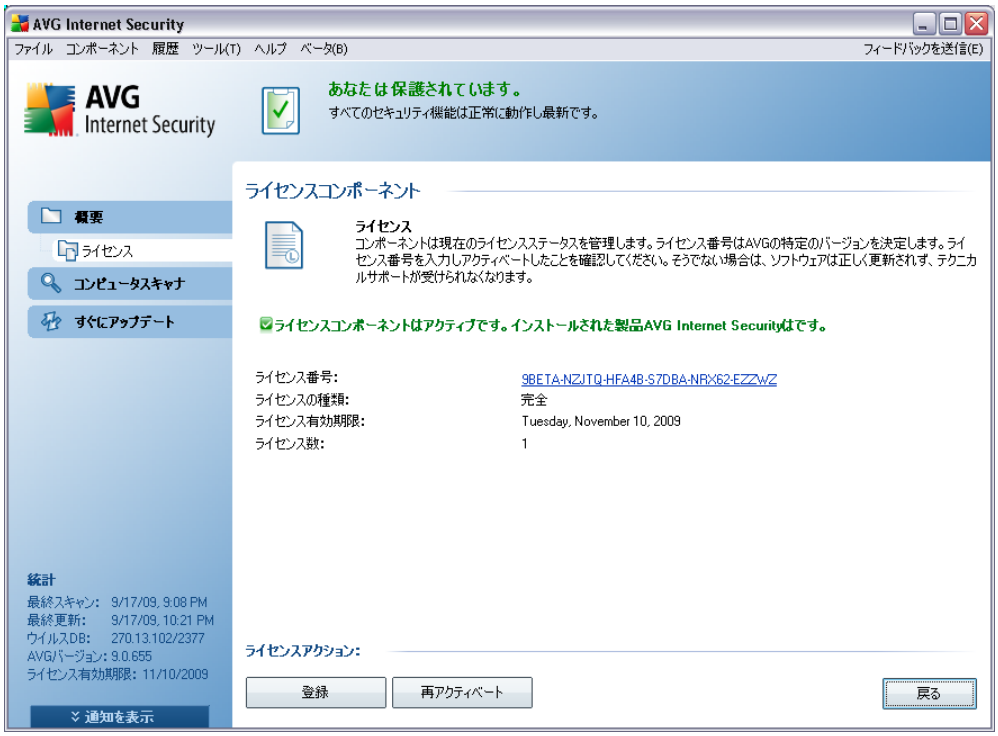
ダイアログの下部では、リストの下に上記でリストされた検出オブジェクトの総数に関する情報が表示されます。さらに、検出オブジェクトの完全なリストをファイルにエクスポート（ ***ファイルにエクスポート***）し、検出オブジェクトのすべてのエントリを削除（ ***リストを空にする***）ことができます。

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。

8.5. 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 Anti-Virus plus Firewall** 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 Anti-Virus plus Firewall**

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*** - ***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。

- ***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。

8.6. リンクスキャナ

8.6.1. リンクスキャナ原理

リ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!、MSN、Baidu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。*

8.6.2. 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。*）を提供します。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、MSNの検索検索エンジンによる検索結果を予めチェックし、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。

8.6.3. 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、MSN等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セキュリティツールバー*** 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Web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* ）。

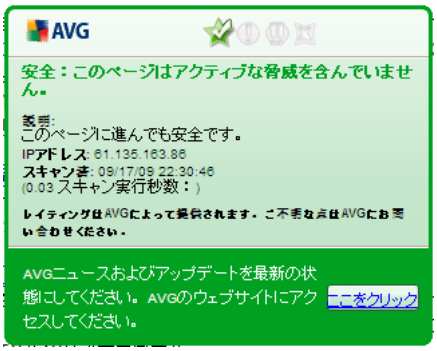
リンクされたページは脅威を含んでいませんが、疑わしいコンテンツを含みます（ *または目的が疑わしいため、電子ショッピングが推奨されない等* ）。

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。

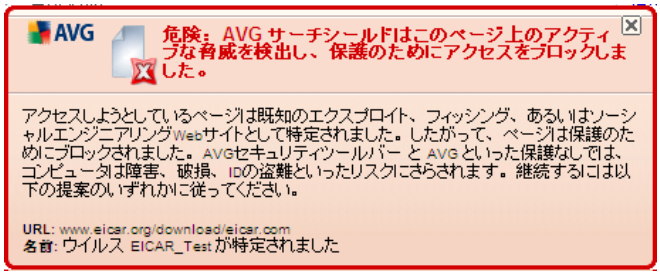
個々の評価アイコンは、問題のあるリンクに関する詳細を表示します。この情報には、存在する場合）脅威についての追加詳細、リンクのIPアドレス、スキャン実行日時が含まれています。



8.6.4. 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セキュリティツールバー*** 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セキュリティツールバー*** 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。

8.7. Web シールド

8.7.1. Web シールド原理

Web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。

Web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 Web 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。*

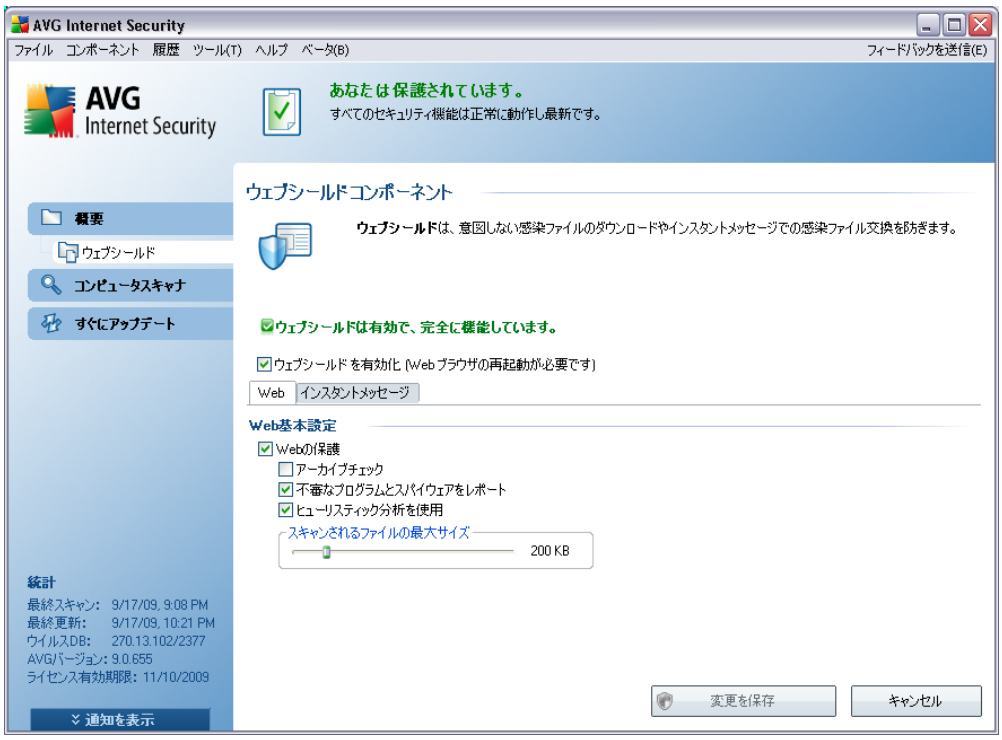
8.7.2. Web シールドインターフェース

Web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（*Webシールドは有効で完全に機能しています。等）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

Webシールド有効化 にチェックを付けると、***Web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、***Web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、***Web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。

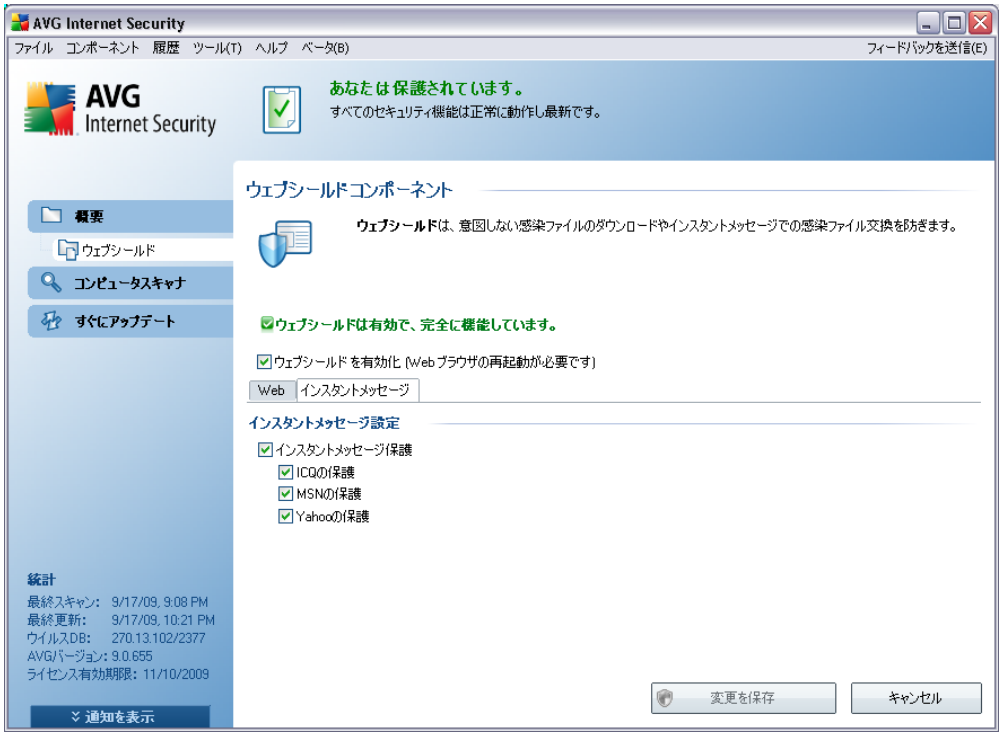


o ***Web保護*** - このオプションがチェックされている場合、***Webシールド*** はWWWページコンテンツをスキャンします。このオプションがオン（*デフォルト*）の場合、さらに以下の項目のオン/オフを変更することができます。

- ***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のレポート*** - WWWページに含まれる不審なプログラム（*スパイウェアやアドウェアとして動作する実行可能なプログラム*）とスパイウェアをスキャンします。
- ***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 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、 ***Webシールド*** でスキャンされるファイルの最大サイズを変更します。 ダウンロードファイルが指定値より大きく、Webシールドでスキャンされない場合でも、コンピュータは保護されます。この場合、 ***常駐シールド が感染 ファイルを検出します。***

- ***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 - 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 Anti-Virus plus Firewall** 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

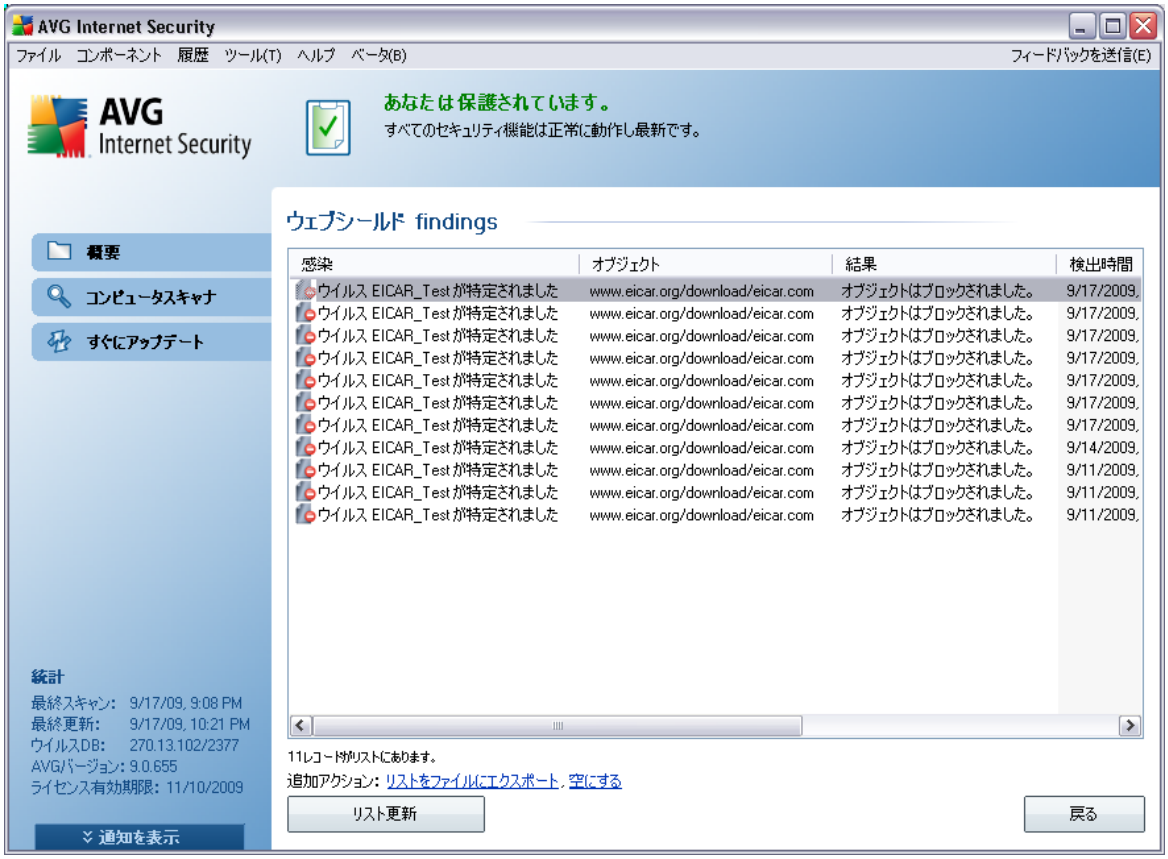
Webシールド インターフェースで利用できるコントロールボタンは以下の通りです。

- ***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

8.7.3. ウェブシールド検出

Web シールドは 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 ***Web 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/Web 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 ***Web 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。

8.8. 常駐シールド

8.8.1. 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。

8.8.2. 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、ブロックされた脅威*** - 検出された感染数（必要に応じて、この値はリセットされます。例えば、統計目的 - 値のリセットなど）

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。

o 自動（***すべての脅威を自動的に除去***）

o 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、***Cookieを自動的に除去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。

- ***例外管理*** - は***常駐シールドの例外ディレクトリ***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*** 口ンポーネント概要）に戻ります

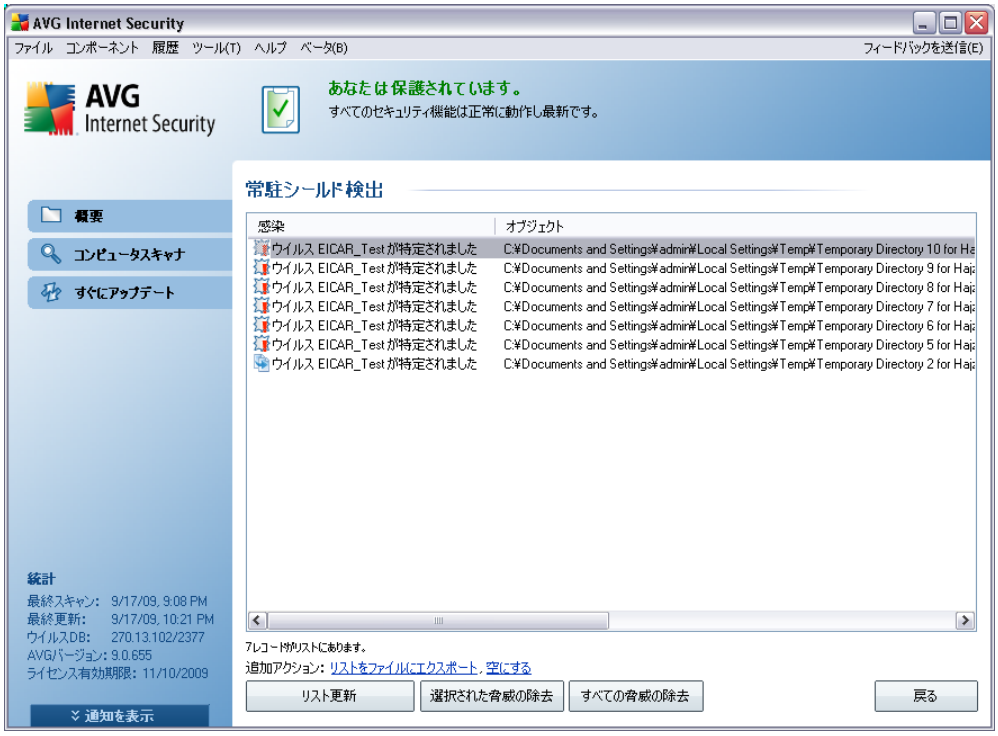
8.8.3. 常駐シールド検出

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。検出されたオブジェクトについては、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。

8.9. アップデートマネージャ

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。*

AVG Download Manager は、AVG ホーム製品のダウンロードの管理を容易にする簡単なツールです。選択内容に基づいて、ダウンロードマネージャーは特定の製品、ライセンス種別、言語に合わせて構成を行います。このユーティリティの最大の利点は、自分の条件に合わせて AVG 製品のダウンロードを管理できるということです。さらに、最新のインストールファイルが常にダウンロードされるため、AVG プログラムはインストール後に完全に更新されている状態となります。

AVG Download Manager

- 必ず最新のインストールファイルをダウンロードします。
- ダウンロードするファイルのサイズが縮小されます。
- 何からの理由によりダウンロードが失敗した場合はダウンロードの再開ができます。
- すべての AVG プログラム版の操作は、個人利用を目的としています。

注意：*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 2000 (SP4 + SRP ロールアップ)、Windows XP (SP2 以上)、Windows Vista (すべての版) のみです。*

8.9.1. アップデートマネージャ原理

AVG Download Manager は次のステップで動作します。

- まず、***AVG Download Manager*** アプリケーションをダウンロードする必要があります。起動したら、***AVG Download Manager*** が、インストールプロセスの言語を選択するよう要求します。
- 次に、***AVG Download Manager*** が、接続テストを実行するためにインターネット接続の確立

を試みます。接続テストに成功した場合は、インストールするAVG プログラムのバージョンを選択できます 完全製品版、試用版、無料版)。

- AVG プログラムバージョンを選択すると、インストールする製品を選択するように求められます。
- 最後に、すべての必要なインストールファイルがダウンロードされます。 ***AVG ダウンロードマネージャが終了して、AVG インストールが起動します 。***

8.9.2. 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。

- o ***定期的*** - 時間間隔を定義します。
- o ***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し、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。

8.10. 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*、*MSN*、*百度* ）の検索結果をチェックする新しいツールです。

AVG 9 Anti-Virus plus Firewall 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。

AVG セキュリティツールバー を使用して、***リンクスキャナ*** 機能を制御し、動作を調整し、新しいアップデートが利用できる場合には **AVG 9 Anti-Virus plus Firewall** をアップデートできます。

注意：*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。*

8.10.1. 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1.5以上）で動作するよう設計されています。

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 Security Toolbar 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。

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ロゴボタン*** - 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。
  - ***Launch AVG 9.0*** - AVG 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。
  - ***Update*** - ***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、***AVGテクニカルサポート*** に問い合わせたり、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。
- ***Yahoo! 検索ボックス*** - Yahoo!を使用して安全に Webを検索することができます。単語あるい

はフレーズを検索ボックスに入力し、 ***Search*** を押してください。現在表示されているページに関係なく、Yahoo!サーバーの検索が開始されます。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。***

- ***AVG Active Surf-Shield*** ボタン - このボタンのオン/ オフは、***AVGサーフシールド*** のステータスをコントロールします。
- ***AVG Search-Shield*** ボタン - このボタンのオン/ オフは、***AVGサーチシールド*** のステータスをコントロールします。
- ***AVG 情報ボタン*** - 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。

8.10.2. AVGセキュリティツールバーオプション

すべての ***AVG Security Toolbar*** パラメータ設定には、[***AVG Security Toolbar***] 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 3 つのセクションがあります。

- ***全般***

タブでは、[***AVG Security Toolbar***] パネル内の表示/非表示を切り替えるボタンを指定できます。

- ***AVG ニュースボタン*** - このオプションは [***AVG ニュース***] ボタンを表示します。[***AVG Security Toolbar***] パネルのボタンをクリックすると、最新の AVG 関連記者発表記事へのリンクがあるドロップダウンメニューを表示できます。

- ***AVG 情報ボタン*** - [***AVG 情報***] ボタンは、次のオプションを持つメニューを開きます。

  - *ツールバー情報* - コンポーネントに関する詳細情報を掲載した ***AVG Security Toolbar*** 製品ページを開きます。

  - *脅威について* - 現在の脅威、ウイルス除去の推奨、FAQ リストなどを掲載した AVG ウィルスラボのウェブページを開きます。

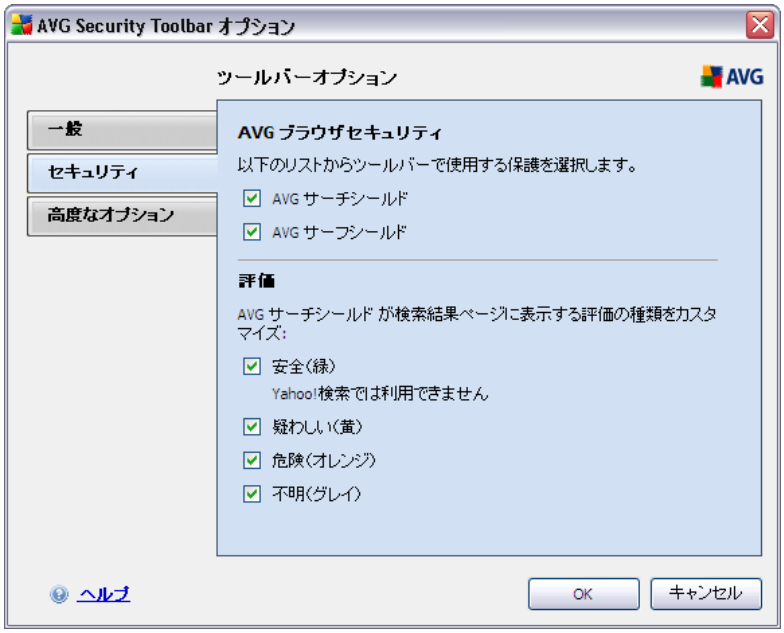
  - *AVG ニュース* - 最新の AVG 関連記者発表記事を掲載したウェブページを開きます。

  - *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。

- ***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。

- ***セキュリティ***



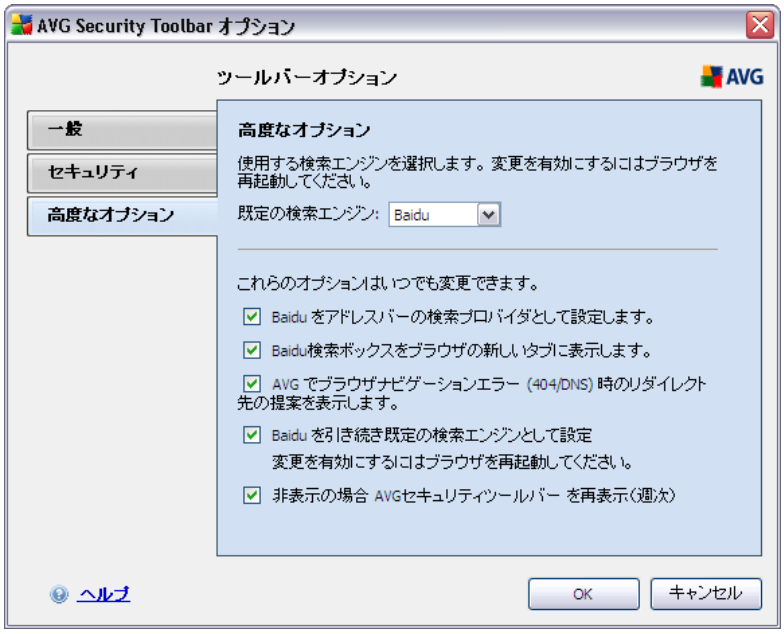
[***セキュリティ***] タブには、[***AVG ブラウザセキュリティ***] と [***評価***] という 2 つのセクションがあり、特定のチェックボックスをオンにして、使用する ***AVG Security Toolbar*** 機能を割り当てられます。

- ***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 Search-Shield*** または ***AVG Active Surf-Shield*** 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*** コンポーネントで、検索結果評価に使用するグラフィカルな記号を選択します。記号には次の種類があります。
  - 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。

- ***高度なオプション***



[***高度なオプション***] タブでは、さらに特定の ***AVG Security Toolbar*** 設定を有効化または無効化できます。

- ***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。

- ***Yahoo!検索ボックスをブラウザの新しいタブに表示*** - *既定ではオン*) このオプションをオンにしている場合、Yahoo!検索ボックスが新しく開かれた各インターネットブラウザのタブに表示されます。

- ***ブラウザナビゲーションエラー時にAVG で提案を行う(404/DNS)*** - *既定ではオン*) ウェブ上の検索でページが存在しない場合や、ページを表示できない場合 (*404 error*)、***AVG Security Toolbar*** は自動的に別のトピック関連のページの概要を表示します。

- ***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 Security Toolbar*** 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。

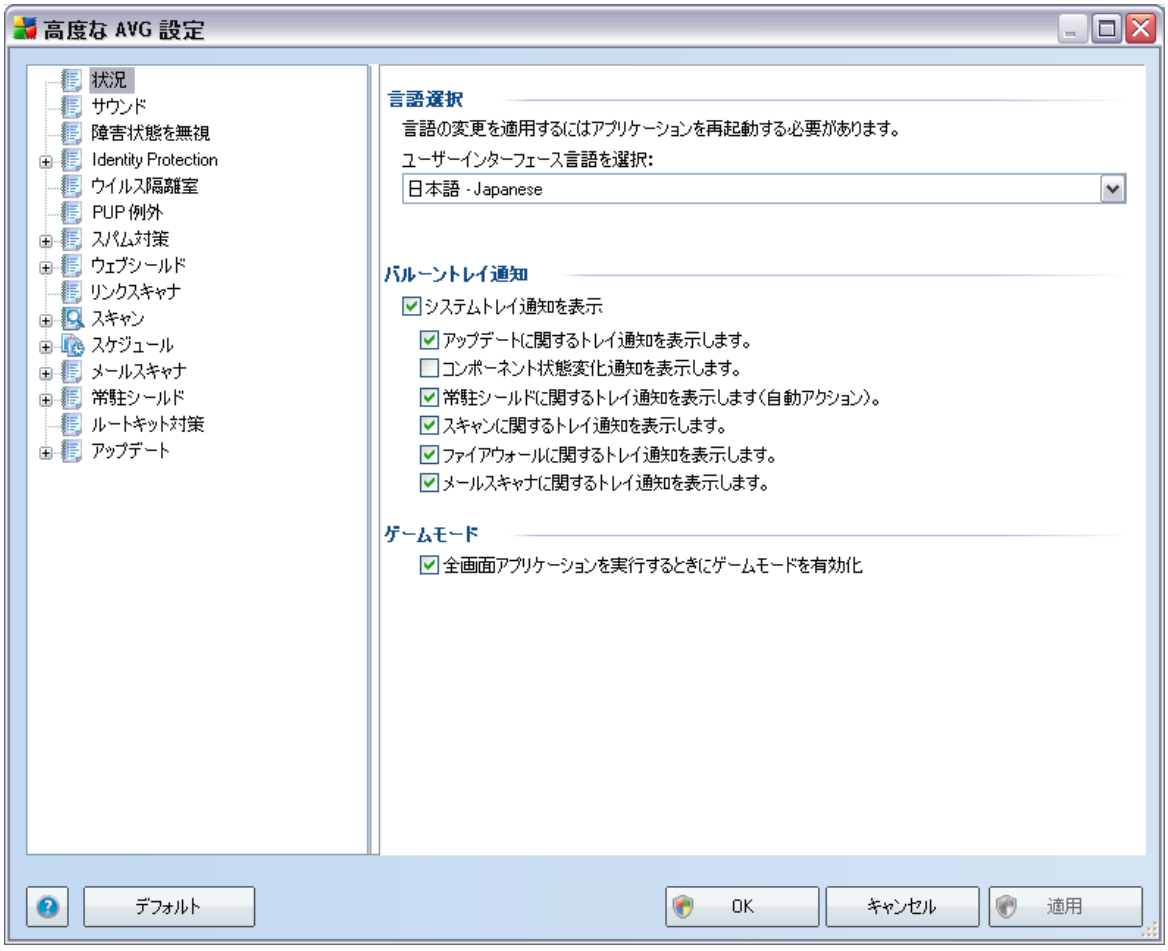
- ***非表示の場合は AVG Security Toolbar を再表示（毎週）*** - *既定ではオン*）このオプションは既定では有効です。 ***AVG Security Toolbar*** が偶然非表示になってしまった場合でも、1 週間以内に再度表示されます。

9. AVG 高度な設定

AVG 9 Anti-Virus plus Firewall の高度な設定ダイアログ ***は、高度なAVG設定*** という新しいウィンドウで表示されます。このウィンドウは2つのセクションにわかれています。左部はにツリー状のナビゲーションが表示されます。設定を変更したいコンポーネントを選択すると、ウィンドウ右側に設定項目が表示されます。

9.1. 表示

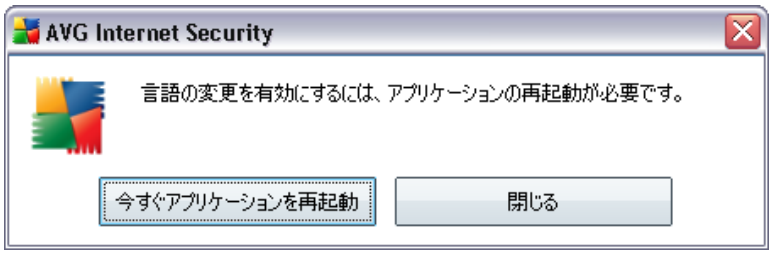
ナビゲーションツリーの最初の項目は、 ***表示*** であり、AVGユーザーインターフェース と、いくつかの動作の基本オプションを設定します。



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*に関するトレイ通知を表示** - ファイルの保存、コピー、オープンに関する情報が表示されるかどうかを決定します。

- ***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。

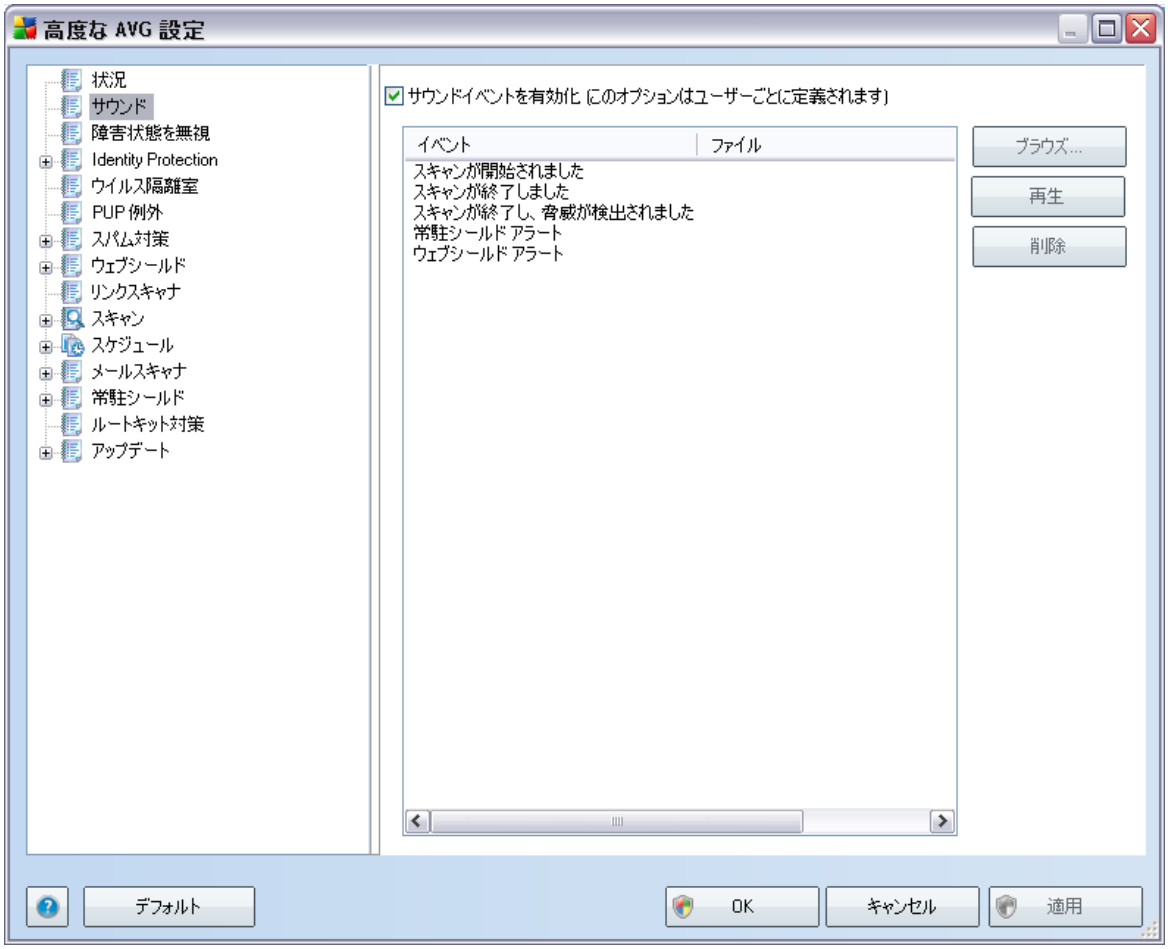
- ***メールスキャナに関するトレイ通知を表示*** - すべての送受信メールに関する情報が表示されるかどうかを決定します。

ゲームモード

この AVG の機能は、インターネット上での通信を必要とする全画面アプリケーション用に設計されています。AVG の確認ダイアログがアプリケーションに影響する（*最小化されたり、グラフィックが正しく表示されなかったりする*）場合があります。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*）。

9.2. サウンド

[***サウンド***] ダイアログでは、サウンド通知によって特定の AVG 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。

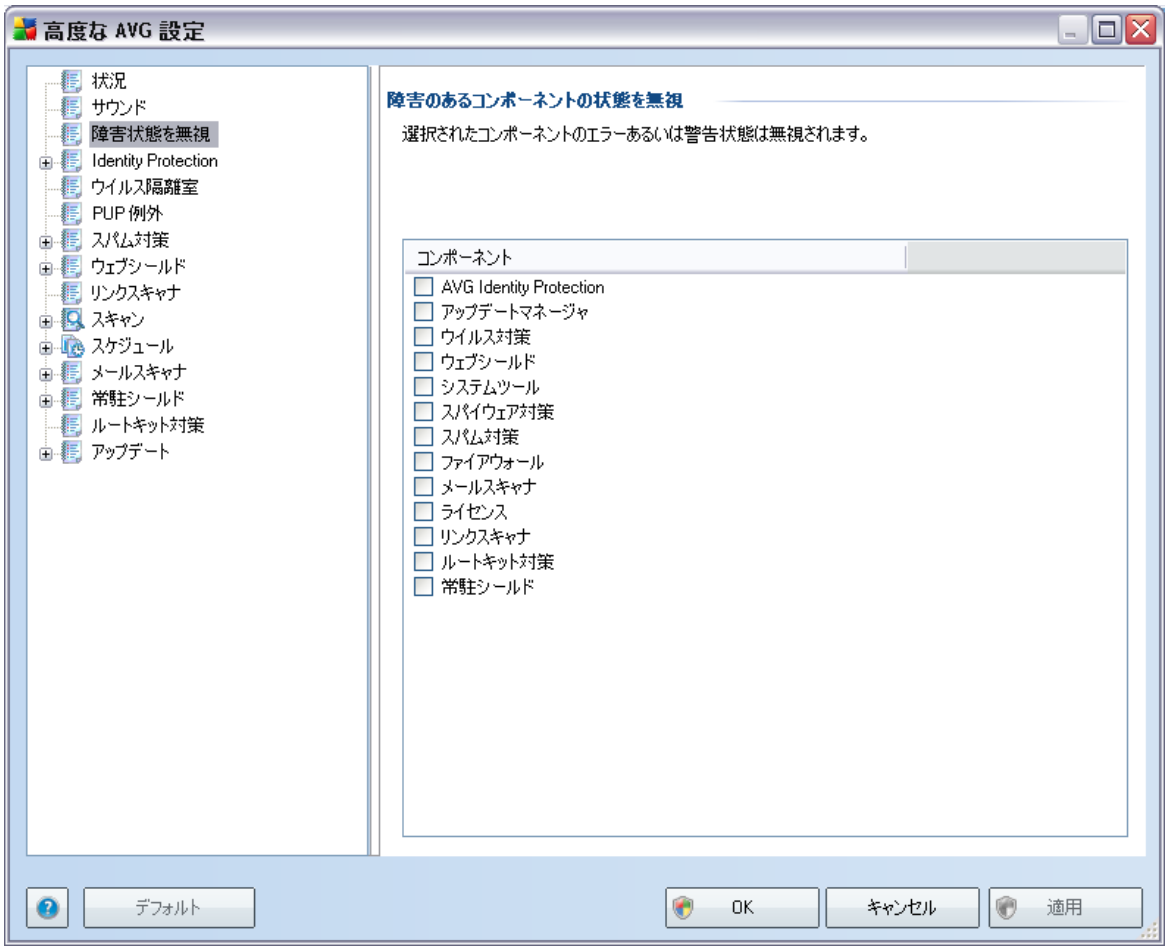


次に、リストから該当するイベントを選択し、このイベントに割り当てる適切なサウンドをディスクから参照 ([***参照***]) します。選択されたサウンドを聴くには、リストのイベントをハイライトし、[***再生***] ボタンをクリックします。[***削除***] ボタンをクリックすると、特定のイベントに割り当てられたサウンドを削除します。

注意 :**.wav サウンドのみがサポートされています。*

9.3. 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。



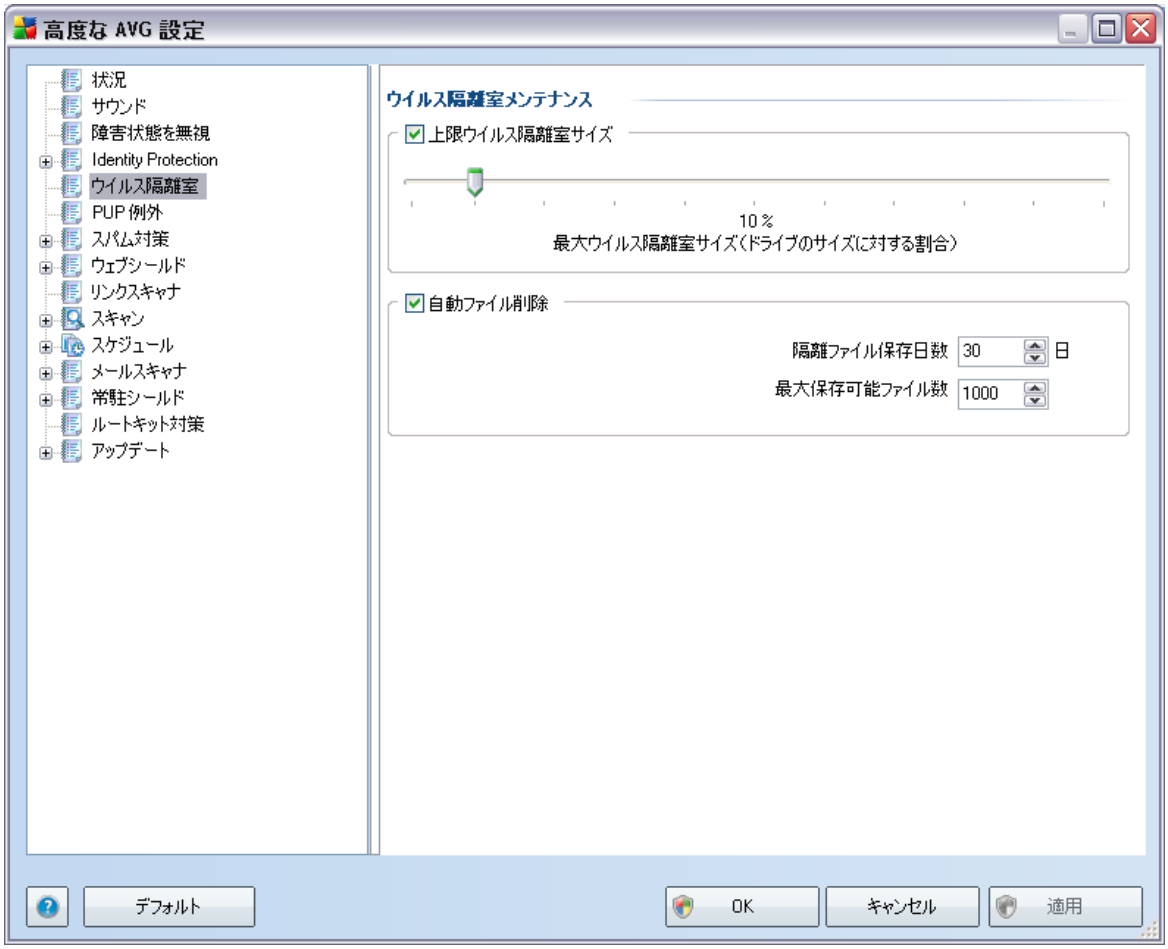
既定値では、リストのどのコンポーネントも選択されていません。つまり、すべてのコンポーネントがエラー状態となる場合は、すぐに以下の方法で通知されます。

- ***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。

9.4. ウイルス隔離室



ウイルス隔離室メンテナンス ダイアログでは、***ウイルス隔離室*** に格納されるオブジェクトに関するパラメータを設

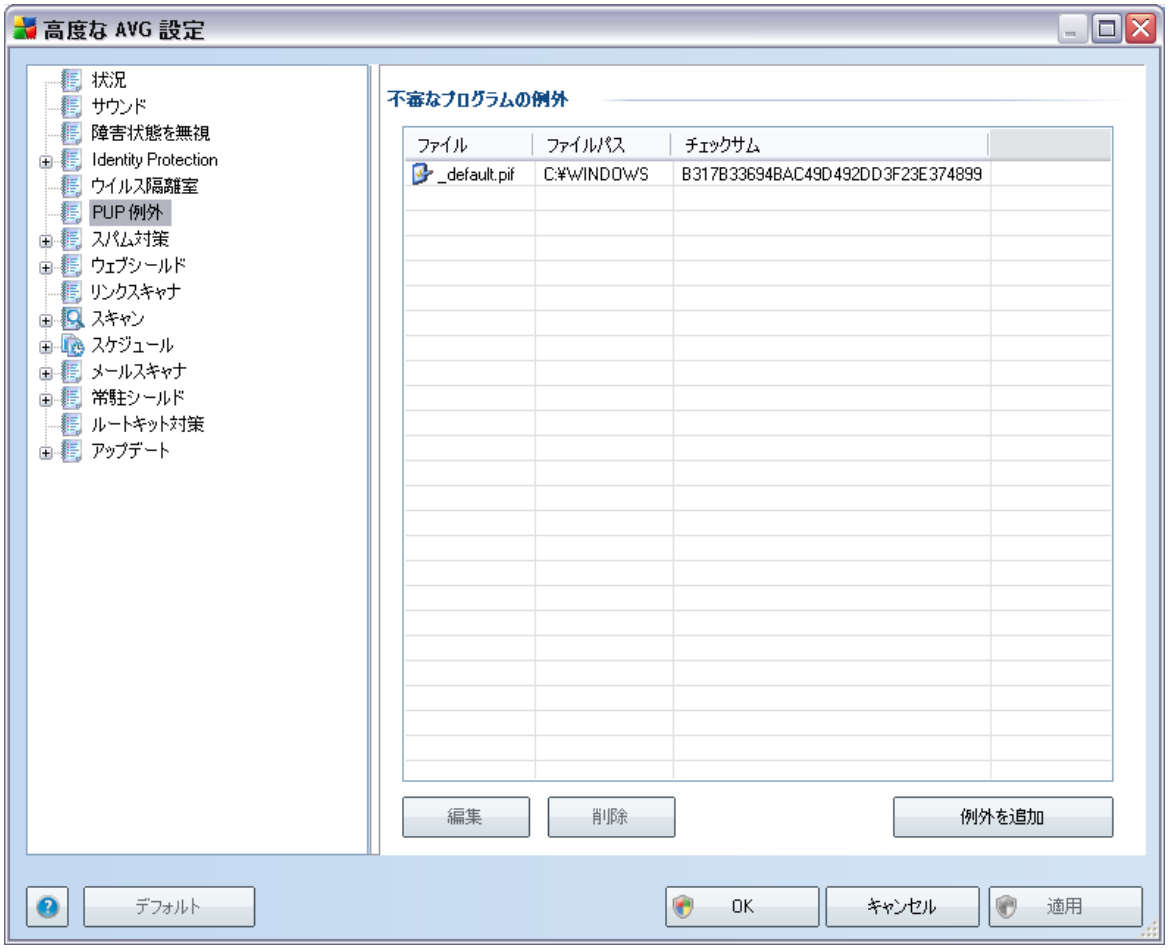
定します。

- ***ウイルス隔離のサイズを制限*** - スライダを使用して、***ウイルス隔離***の最大サイズを設定できます。サイズは、ローカルディスクのサイズに対する割合で指定されます。

- ***自動ファイル削除*** - このセクションでは、***ウイルス隔離室***にオブジェクトが格納される最大日数（***日数を経過したファイルの削除***）、と***ウイルス隔離室***に格納される最大ファイル数（***格納されるファイルの最大数***）を定義します。

9.5. PUP 例外

AVG 9 Anti-Virus plus Firewall 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。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。

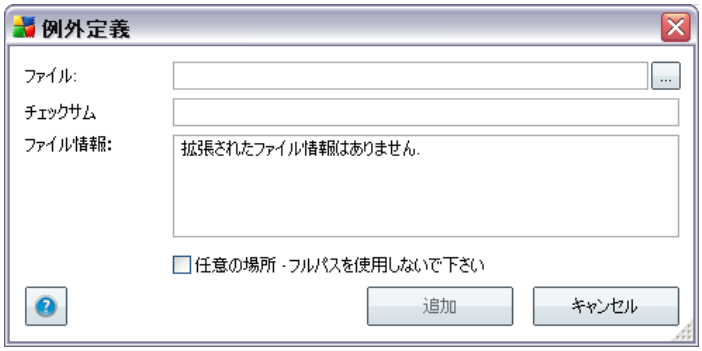


不審なプログラム例外 ダイアログでは、既に定義された 不審なプログラムの例外リストが表示されます。リストの編集、既存のアイテムの削除、新しい例外の追加ができます。次の情報は、各例外のリストにあります。

- ***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。

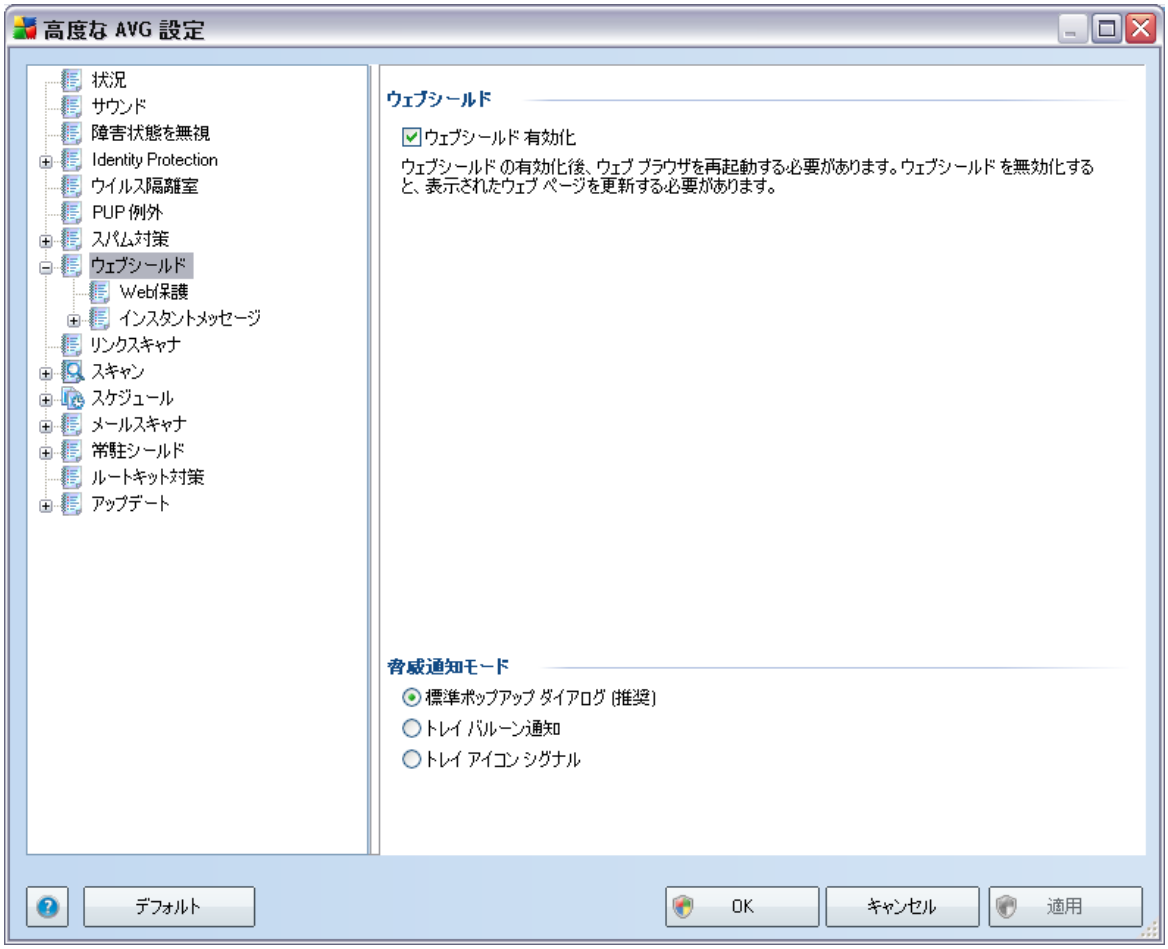
コントロールボタン

- ***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。

9.6. Web シールド



[***Web 保護***] ダイアログでは、[***Web シールドを有効化***] オプション（*既定では有効*）を使用して、***Web 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。

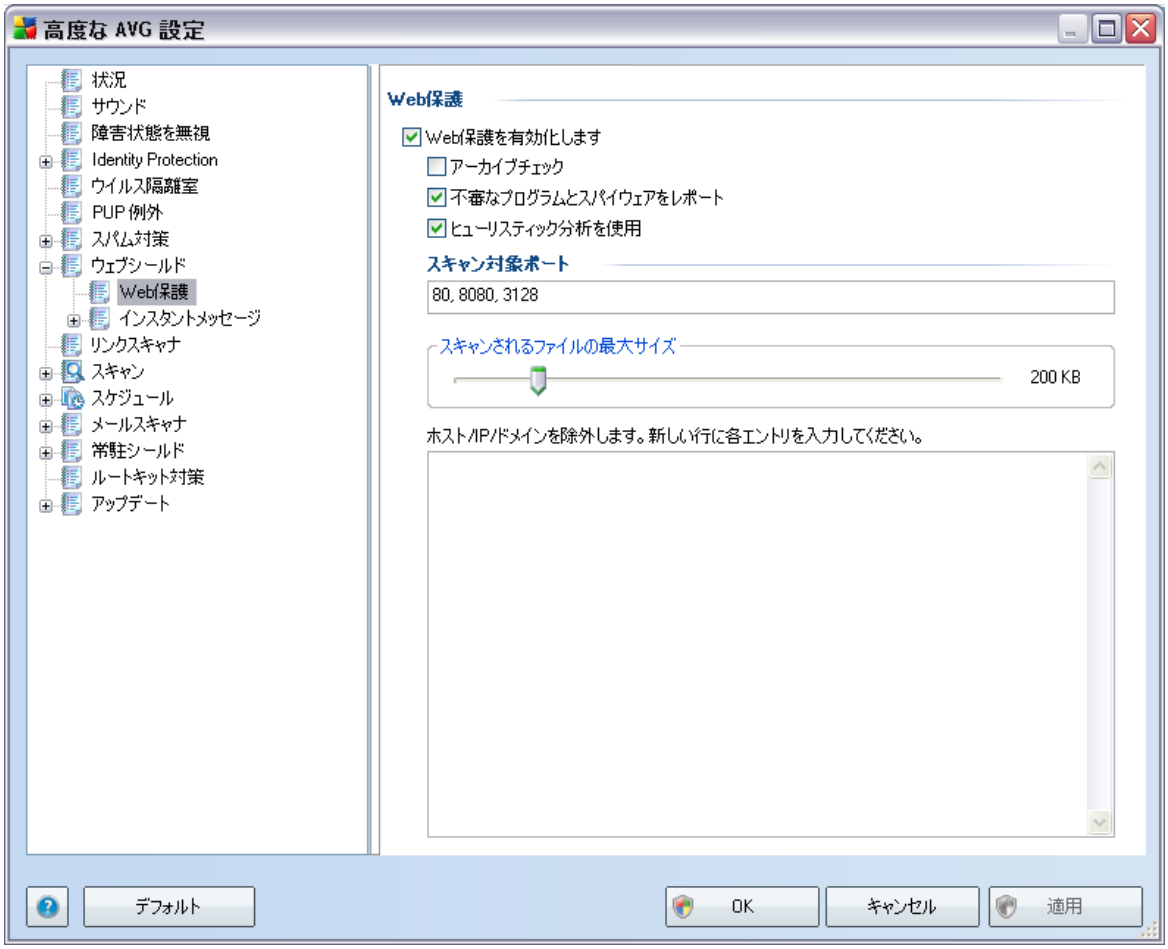
- ***Web保護***
- ***インスタントメッセージ***

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。

9.6.1. 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、 ***Web 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*** - WWW ページに含まれ、表示される不審なプロ

グラム（*スパイウェアやアドウェアとして動作する実行可能なプログラム*）とスパイウェア感染をスキャン

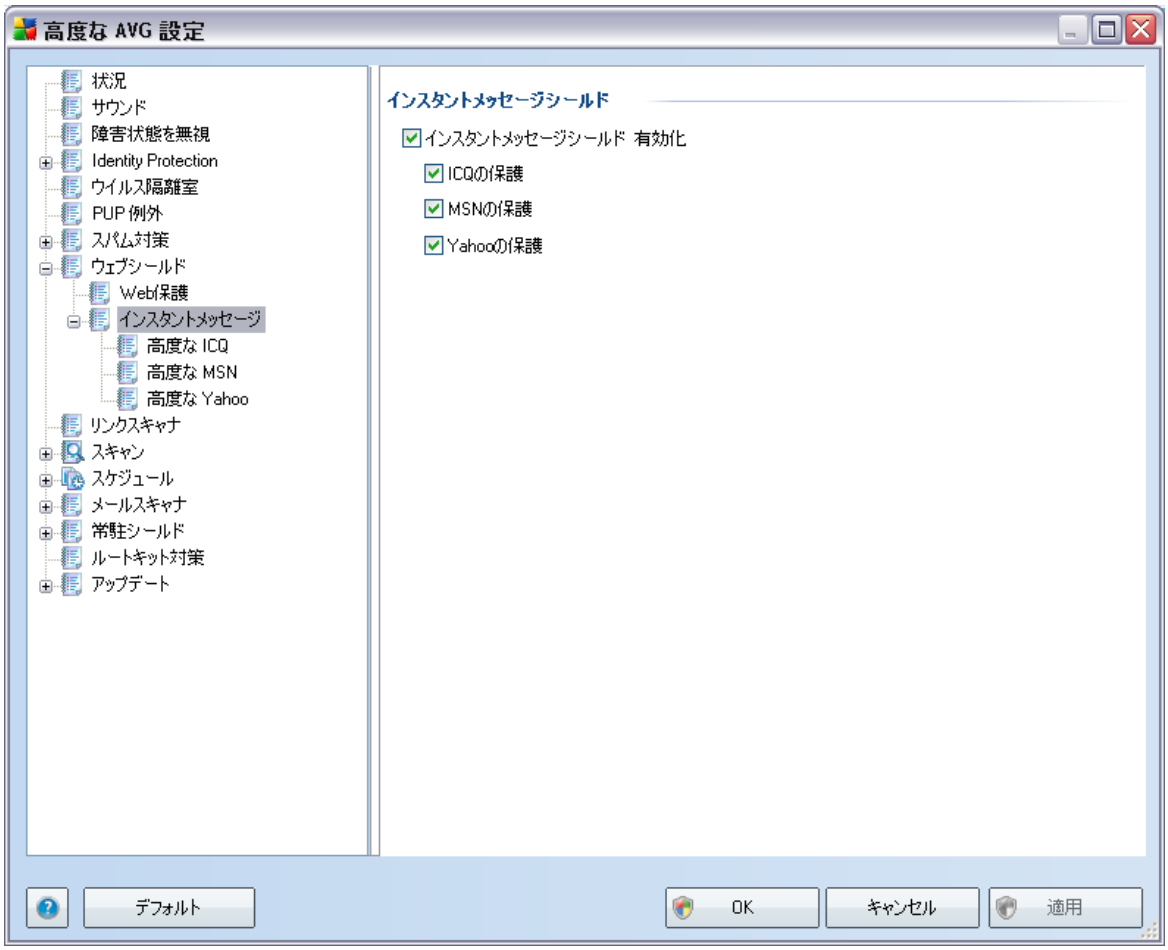
- ***ヒューリスティック分析の使用*** - ヒューリスティック分析（*仮想コンピュータ環境での スキャンオブジェクトの動的エミュレーション*）を使用して、表示されるページコンテンツをスキャンします。

- ***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、***Webシールド*** でスキャンされるファイルの最大サイズを変更します。ダウンロードファイルが指定値より大きく、Webシールドでスキャンされない場合でも、コンピュータは保護されます。この場合、***常駐シールド*** が感染ファイルを検出します。

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

9.6.2. インスタントメッセージ

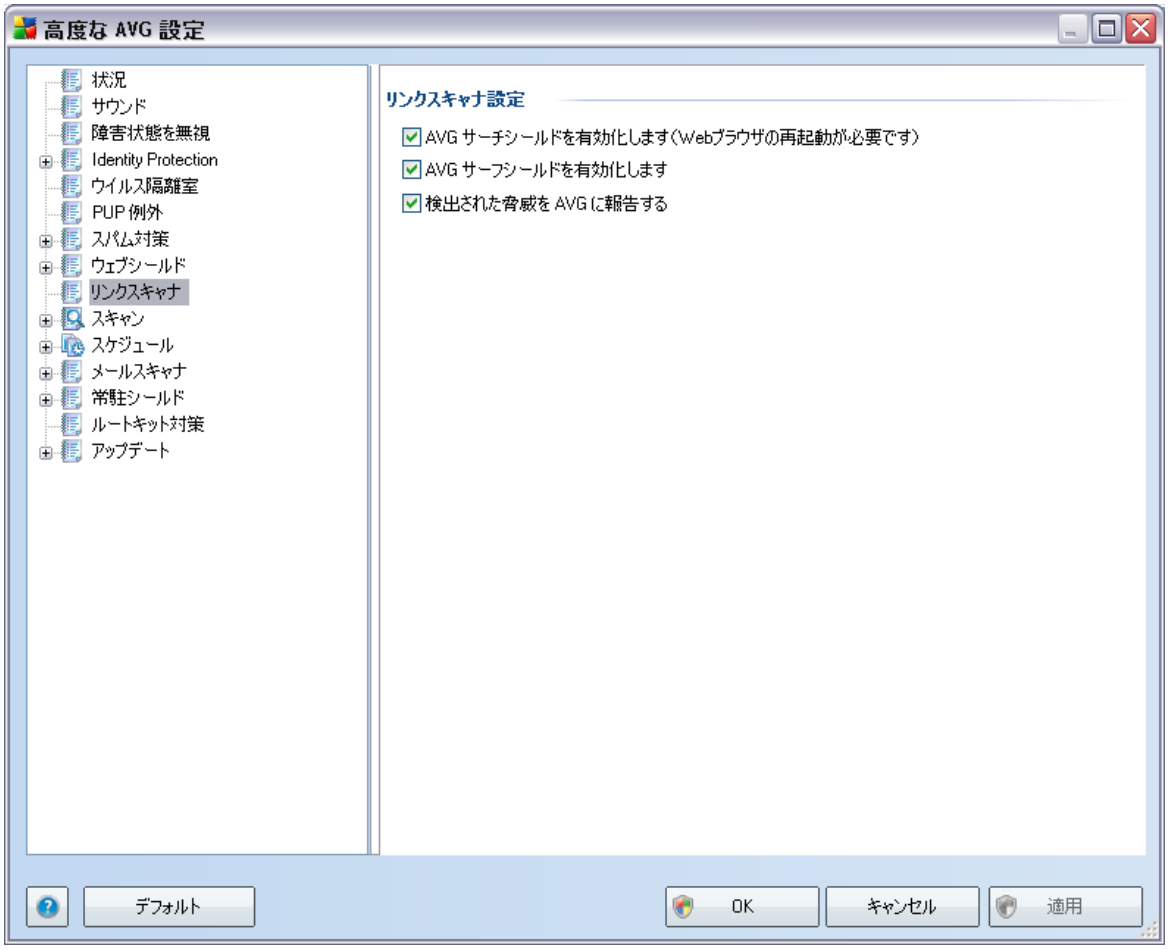


インスタントメッセージシールド ダイアログでは、***Webシールド*** コンポーネントのインスタントメッセージスキャンに関する設定を編集します。現在は次の 3 つのメッセージングプログラムがサポートされています。 ***ICQ***、***MSN***、***Yahoo*** - ***Webシールド*** がオンライン通信がウィルスフリーだということを確認するようにしたい場合は、この中から該当するアイテムをチェックします。

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。

9.7. 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、MSN、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。

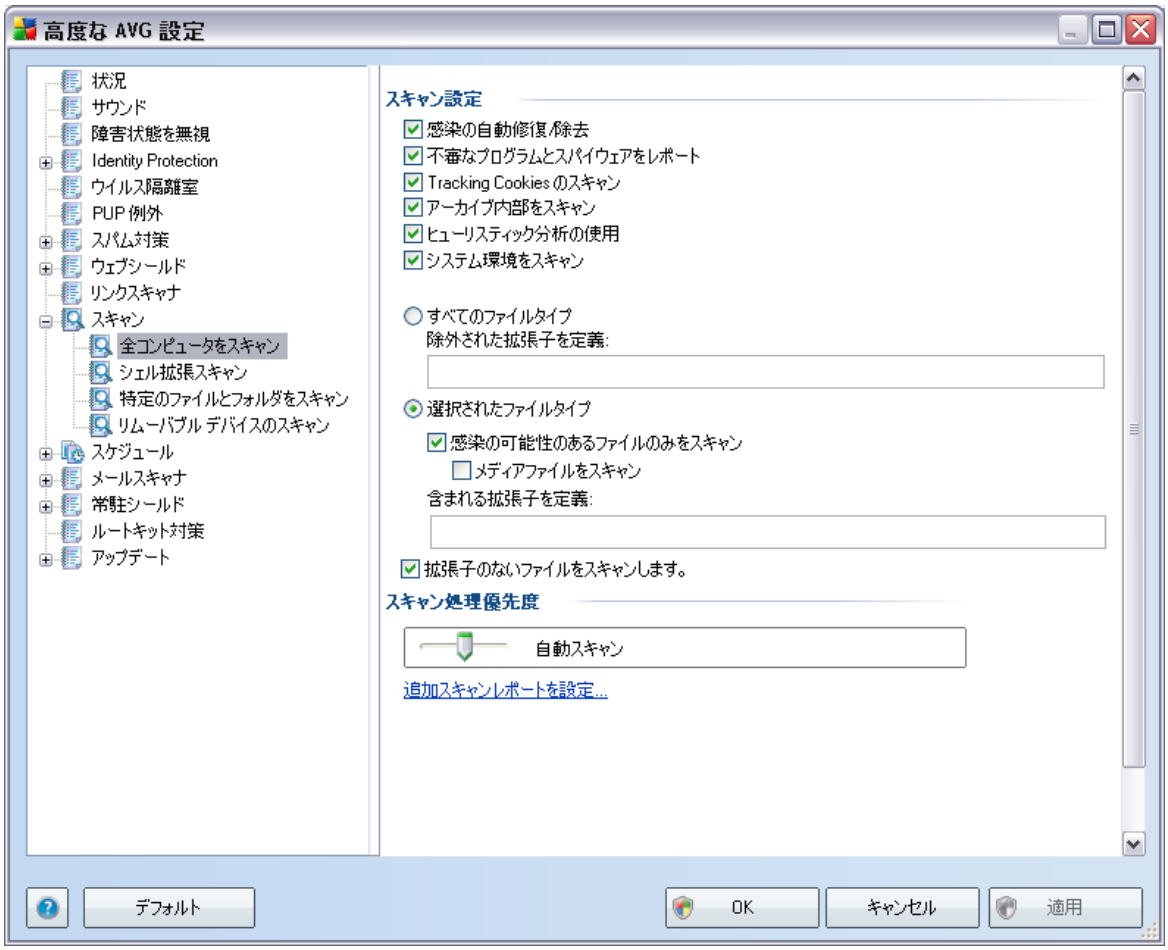
9.8. スキャン

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

9.8.1. 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脅威をレポート*** - (デフォルトではオン) このパラメータは、不審なプログラム (***スパイウェアやアドウェアとして実行される実行可能ファイル***) を検出できるようにします。これらはブロック、または除去されます。

- ***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を入力することで、スキャンからの除外を定義できます。あるいは、

- ***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、ウイ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。

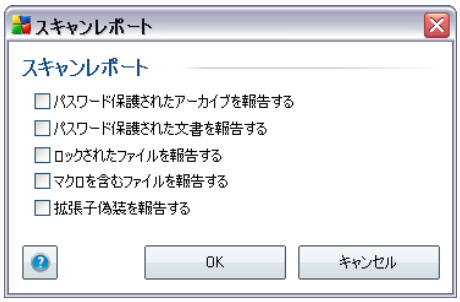
- オプションとして、***拡張子のないファイルをスキャン*** できます。このオプションは既定ではオンになっています。変更する理由がない場合は、この設定を保持することをお勧めします。拡張子のないファイルは不審なものであり、常にスキャンするべきです。

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。

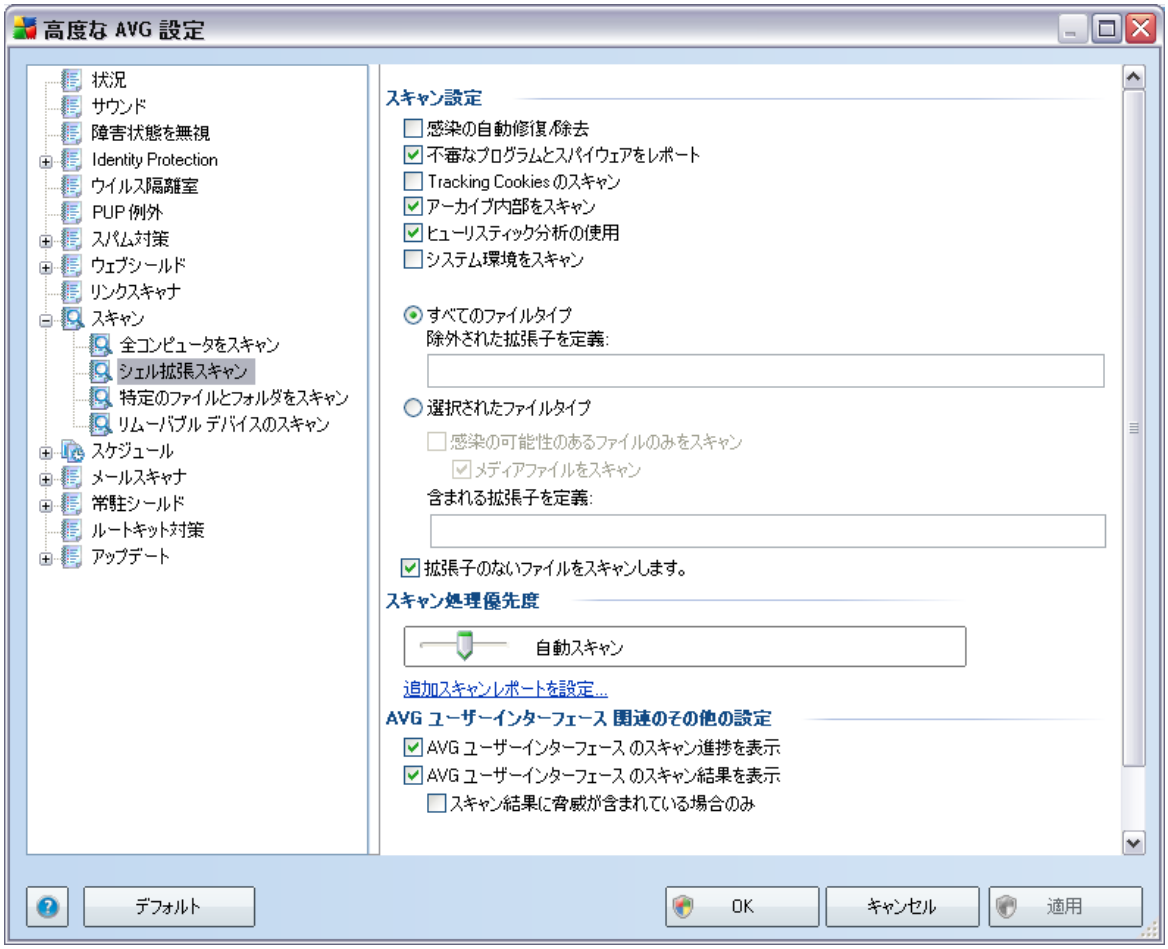
追加スキャンレポートを設定...

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。



9.8.2. 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*** 。

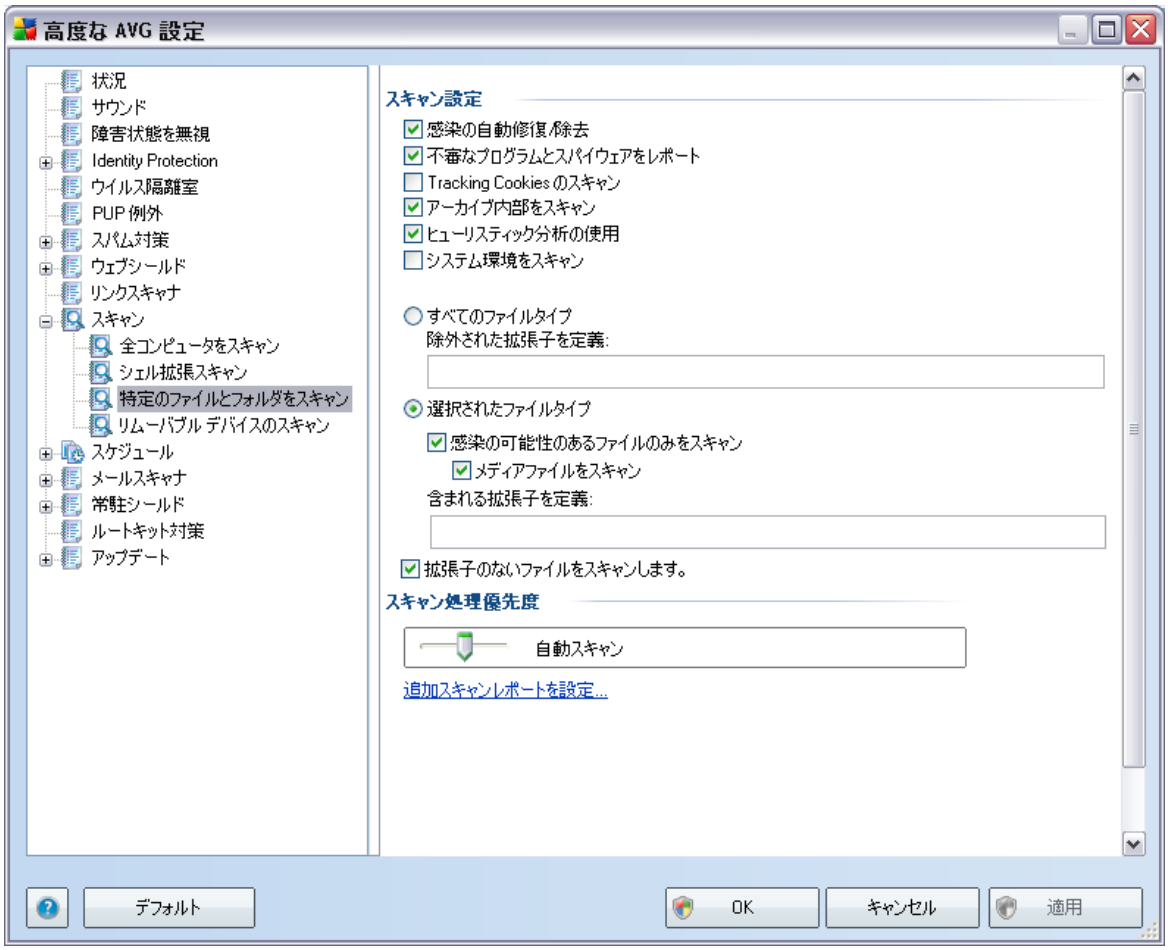


パラメータのリストは ***完全 コンピュータスキャン*** で利 用 できるものと同 一 です。ただし、デフォルト設 定 が異 なります。***完全 コンピュータスキャン*** では、ほとんどのパラメータは選 択 されていますが、 ***シェル拡 張 スキャン*** （ ***Windows Explorerのスキャン*** ）では、関 連 パラメータのみがオンとなっています。

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。*

9.8.3. 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。すべての設定オプションは同一です。ただし、デフォルト設定では、 ***完全スキャン*** の設定はより厳密なものとなっています。

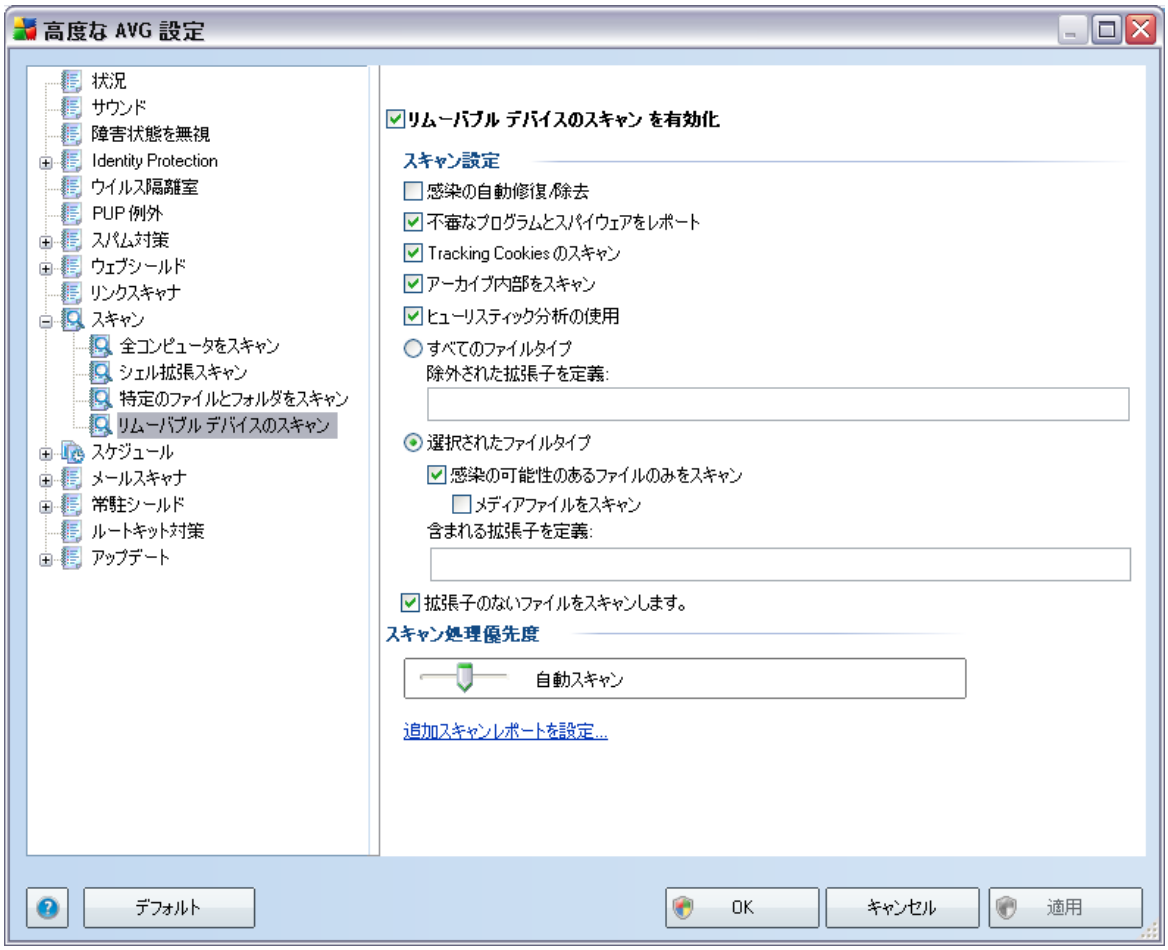


この設定ダイアログで設定されるすべてのパラメータは、 ***特定のファイルとフォルダをスキャン*** で選択されたスキャンエリアのみに適用されます。この設定ダイアログで、 ***ルートキットをスキャン*** オプションをチェックした場合、選択されたエリアに対してのみ、クイックルートキットスキャンが実行されます。

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。*

9.8.4. 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。*

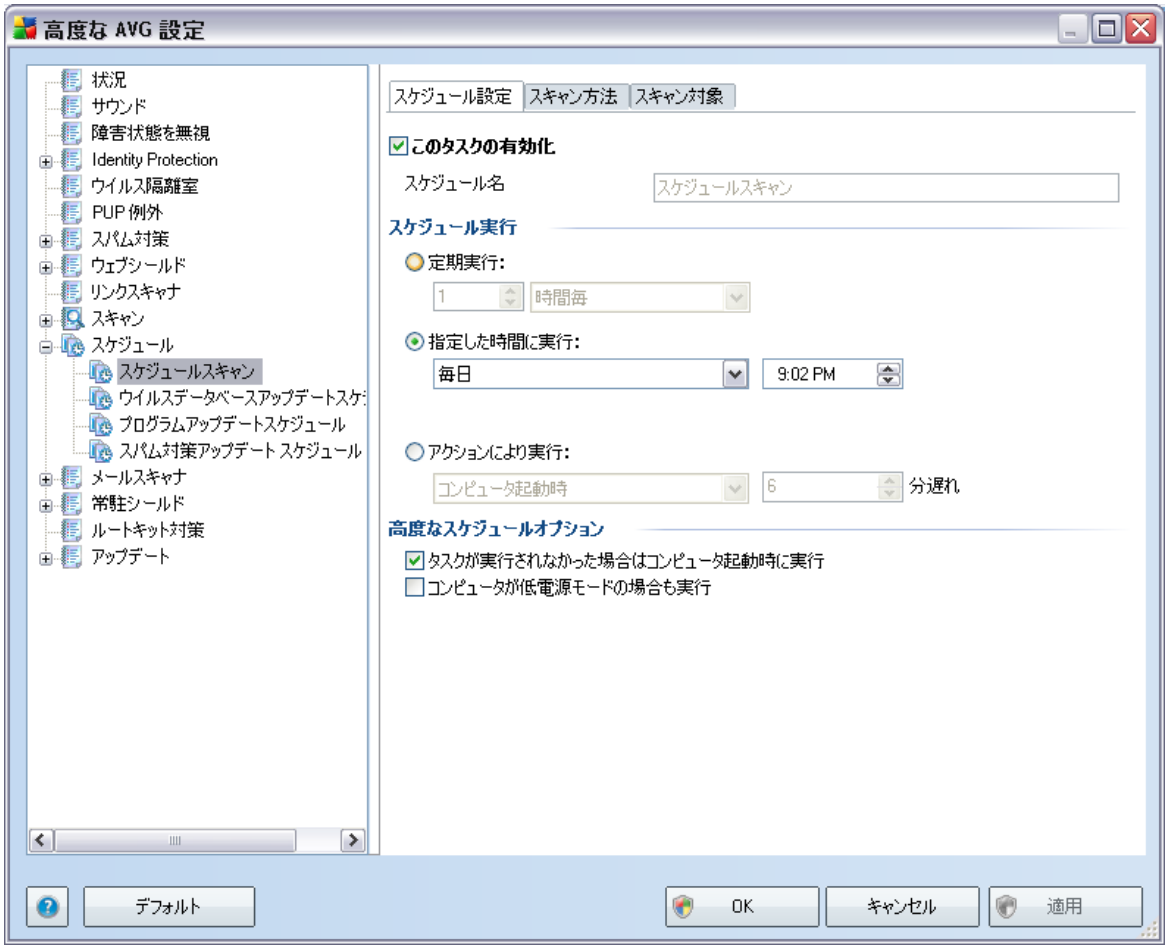
9.9. スケジュール

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

9.9.1. 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。新規に設定するスキャンスケジュールは* [*特定のファイルとフォルダをスキャン*](#) *と同様のも*

のとなります。

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

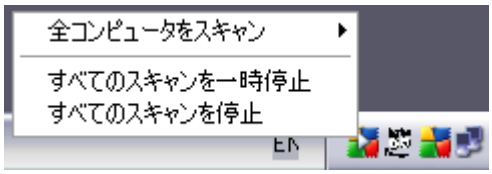
ここでは、新しくスケジュールされたスキャンを起動する時間間隔を指定できます。特定の期間が経過した後に繰り返しスキャンを起動（***定期実行...***）、正確な日時を定義（***特定の時間間隔で実行...***）または、スキャン起動のトリガとなるイベントを定義（***コンピュータ起動時のアクションベース***）することでタイミングを定義できます。

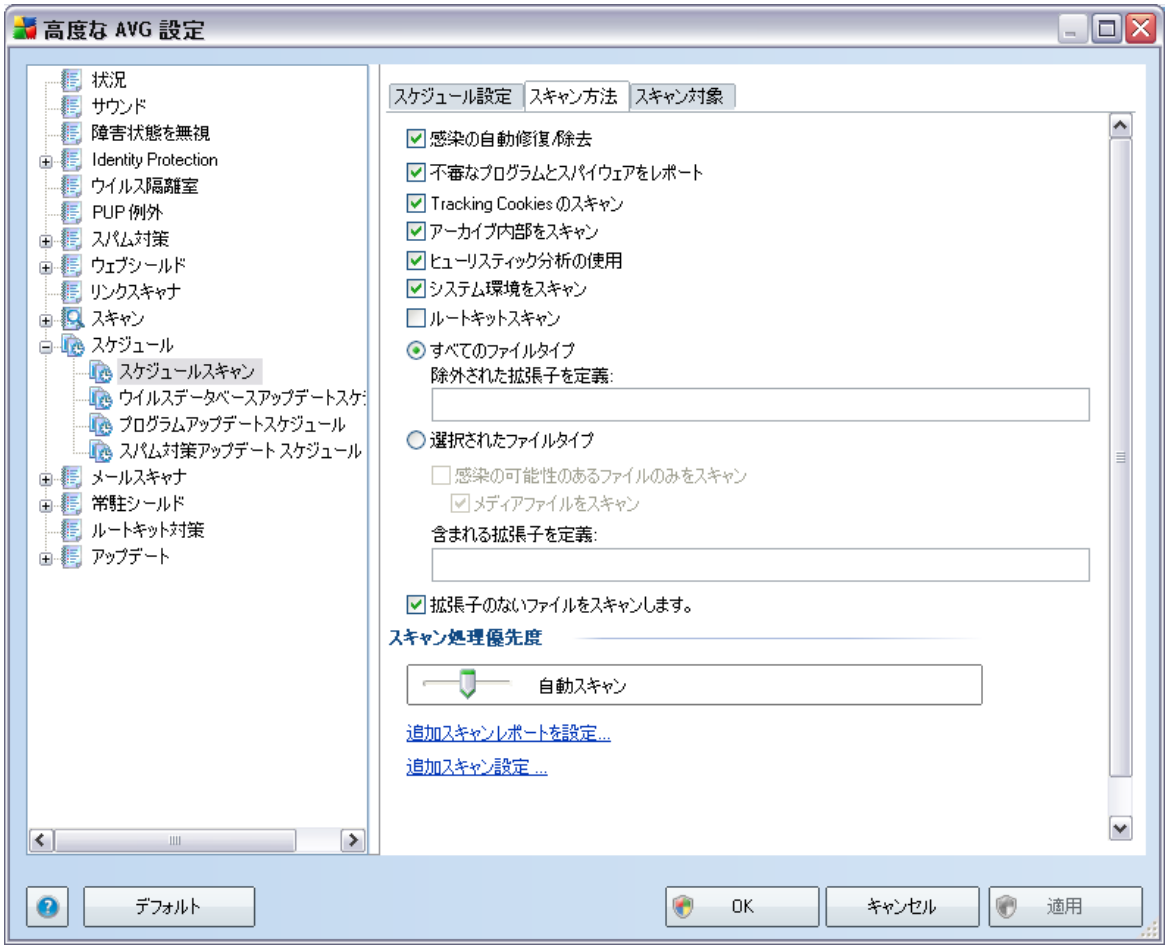
高度なスケジュールオプション

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脅威をレポート*** - *(既定ではオンになっています)* このパラメータは、ウィルス対策 機能を制御し、不審なプログラム *(スパイウェアやアドウェアとして実行される実行可能ファイル)* を検出できるようにします。これらはブロックまたは除去されます。

- ***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を入力することで、スキャンからの除外を定義できます。あるいは、

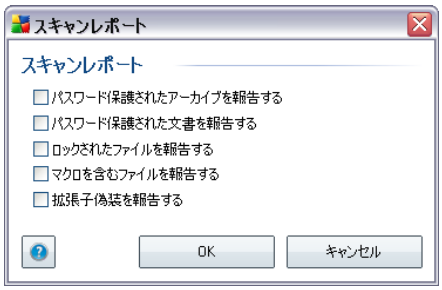
- ***選択されたファイルタイプ*** - 感染の可能性のあるファイルのみを指定できます *(一部のプレーンテキストファイルやその他の非実行可能ファイル など、感染の可能性がないファイルはスキャンされません)*。これには、メディアファイル *(ビデオ、オーディオファイル - これらのファイルは多くの場合、サイズが非常に大きく、ウィルスに感染している可能性が非常に低いため、このボックスのチェックを外している場合、スキャン時間がさらに短縮されます)* が含まれます。ここでも、必ずスキャンする必要があるファイルの拡張子を指定できます。

- 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。

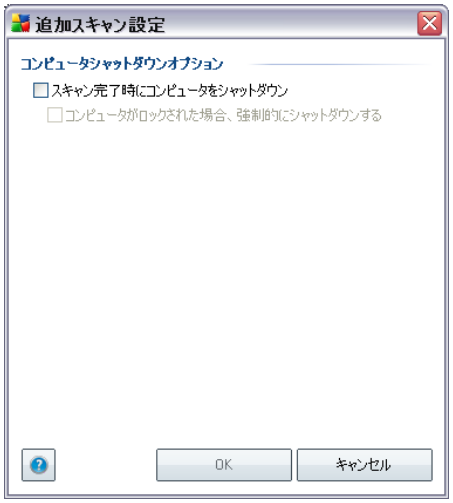
スキャン処理優先度

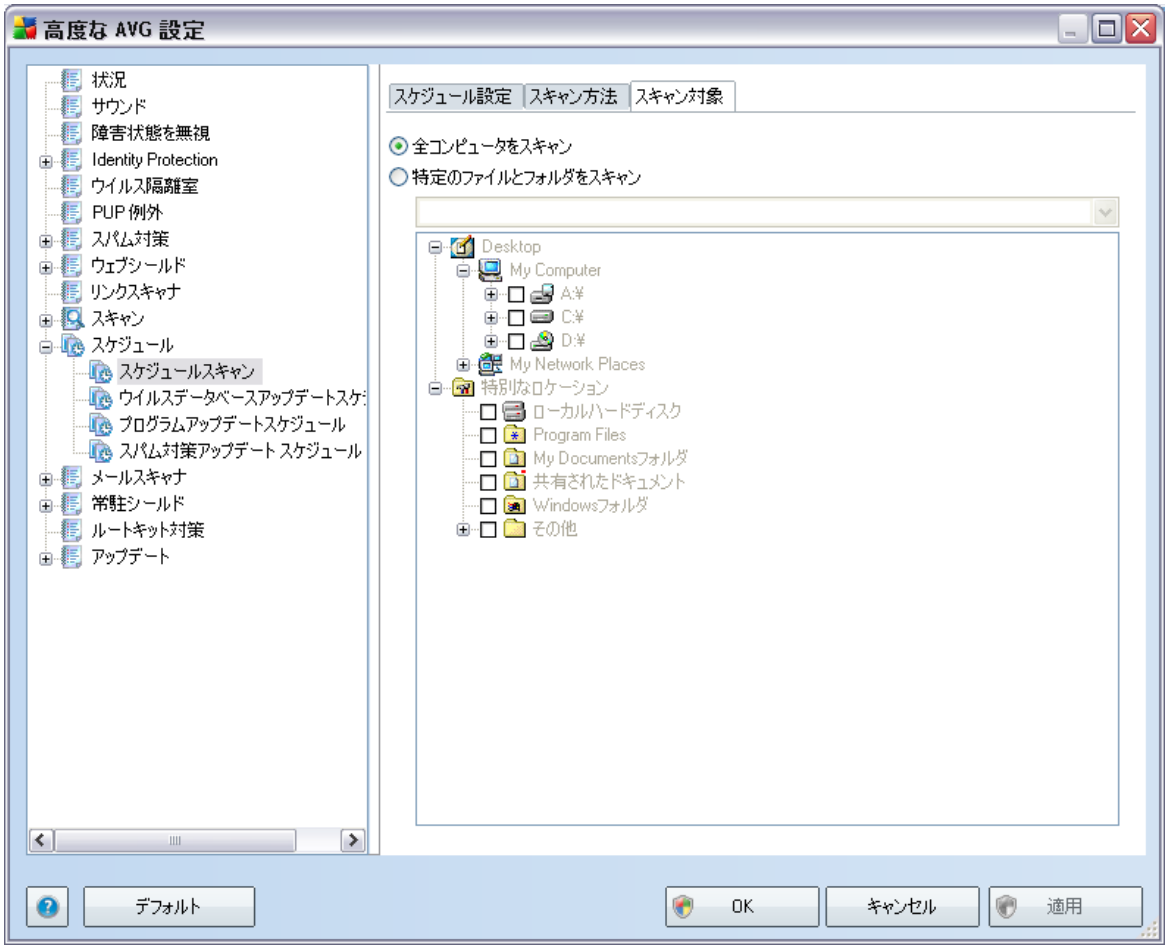
スキャン処理優先度 セクションでは、システムリソース使用度に応じて、希望するスキャン速度を指定することができます。デフォルトでは、このオプションの値は、自動的にリソースを使用する中レベルの値に設定されています。スキャンの速度を上げたい場合、スキャンにかかる時間を削減することができますが、スキャン実行中、システムリソース使用度は著しく上がり、PC上の他の作業の速度が低下します。(*このオプションは、コンピュータの電源がオンであり、コンピュータ上で作業をしているユーザーがいない場合等に適しています。*)一方、スキャンの時間を延長することで、システムリソース使用度を下げることができます。

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。



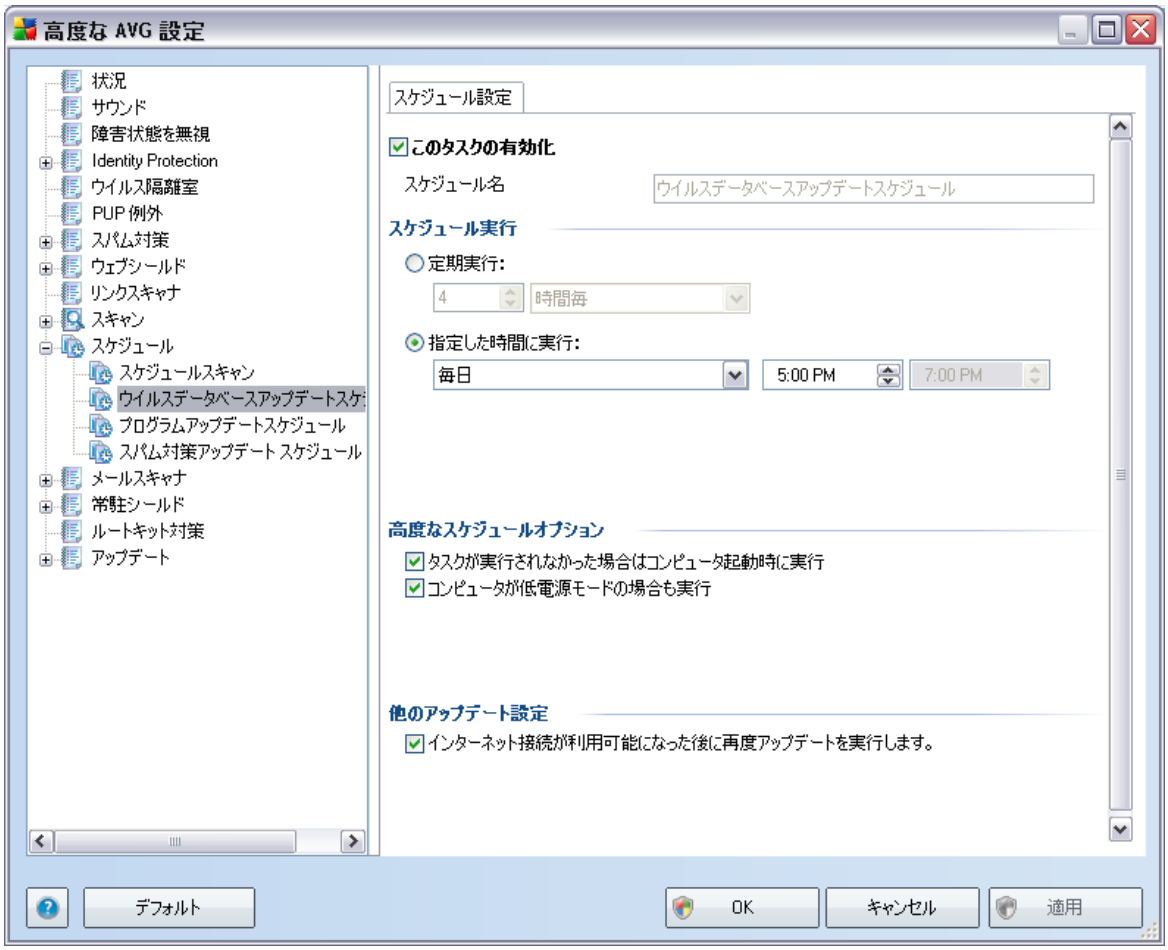
追加スキャン設定 ... をクリックすると、 ***コンピュータシャットダウンオプション*** ダイアログが表示されます。このダイアログでは、スキャンプロセス終了時に自動的にコンピュータをシャットダウンするかどうかを決定します。このオプション（***スキャン完了時にコンピュータをシャットダウン*** ）を選択すると、現在コンピュータがロックされている場合でもコンピュータをシャットダウンするためのオプション（ ***コンピュータがロックされた場合、強制的にシャットダウンする***）が有効化されます。





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。

9.9.2. 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。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 [*ウィルスデータベースアップデートスケジュール*] ***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。後からスケジュールを簡単に識別できるように、必ず簡潔で説明になっている適切な名前を付けるようにしてください。

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、***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

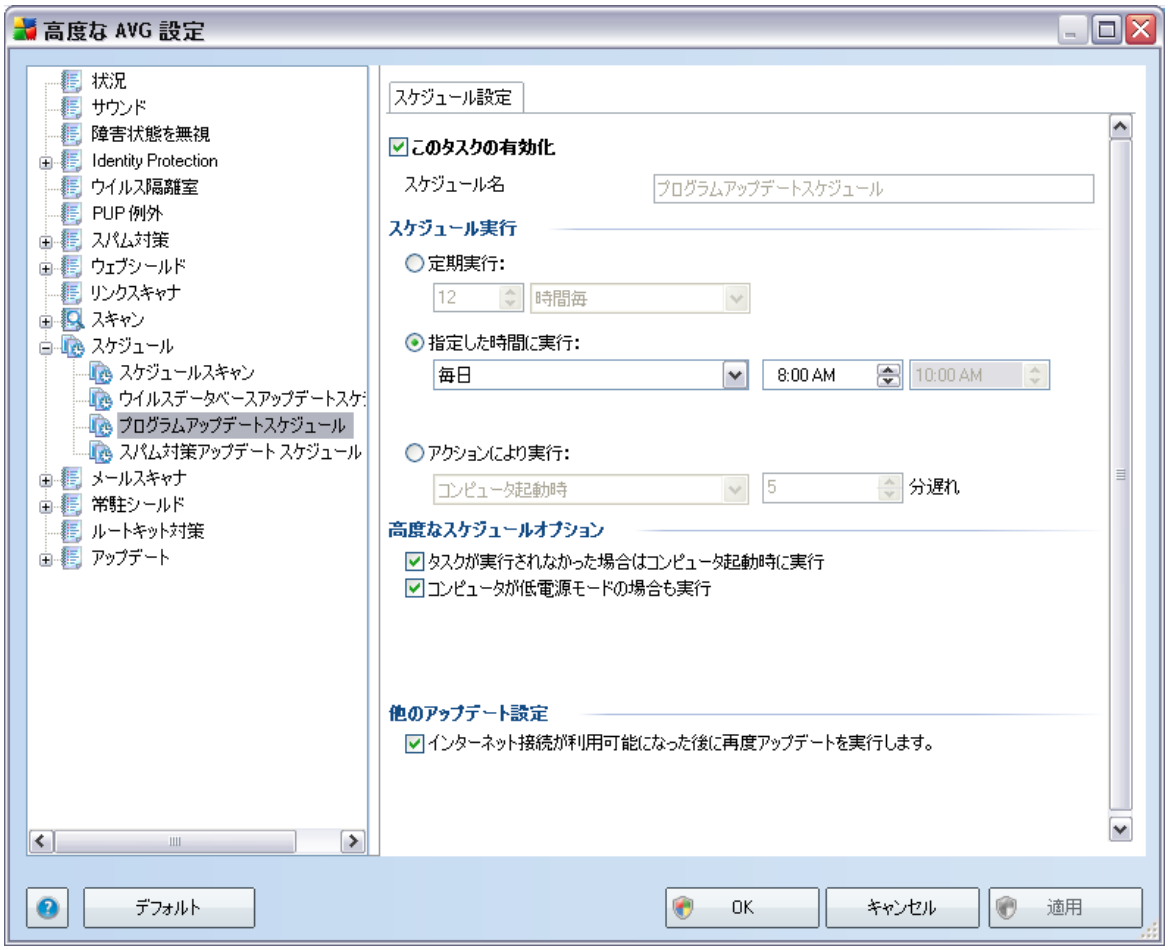
このセクションでは、コンピュータが低電源モードあるいは完全に電源オフになっている場合に、ウイルスデータベースアップデートが実行される条件を定義します。

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）。

9.9.3. プログラム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。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 [*プログラムアップデートスケジュール*] ***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。後からスケジュールを簡単に識別できるように、必ず簡潔で説明になっている適切な名前を付けるようにしてください。

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

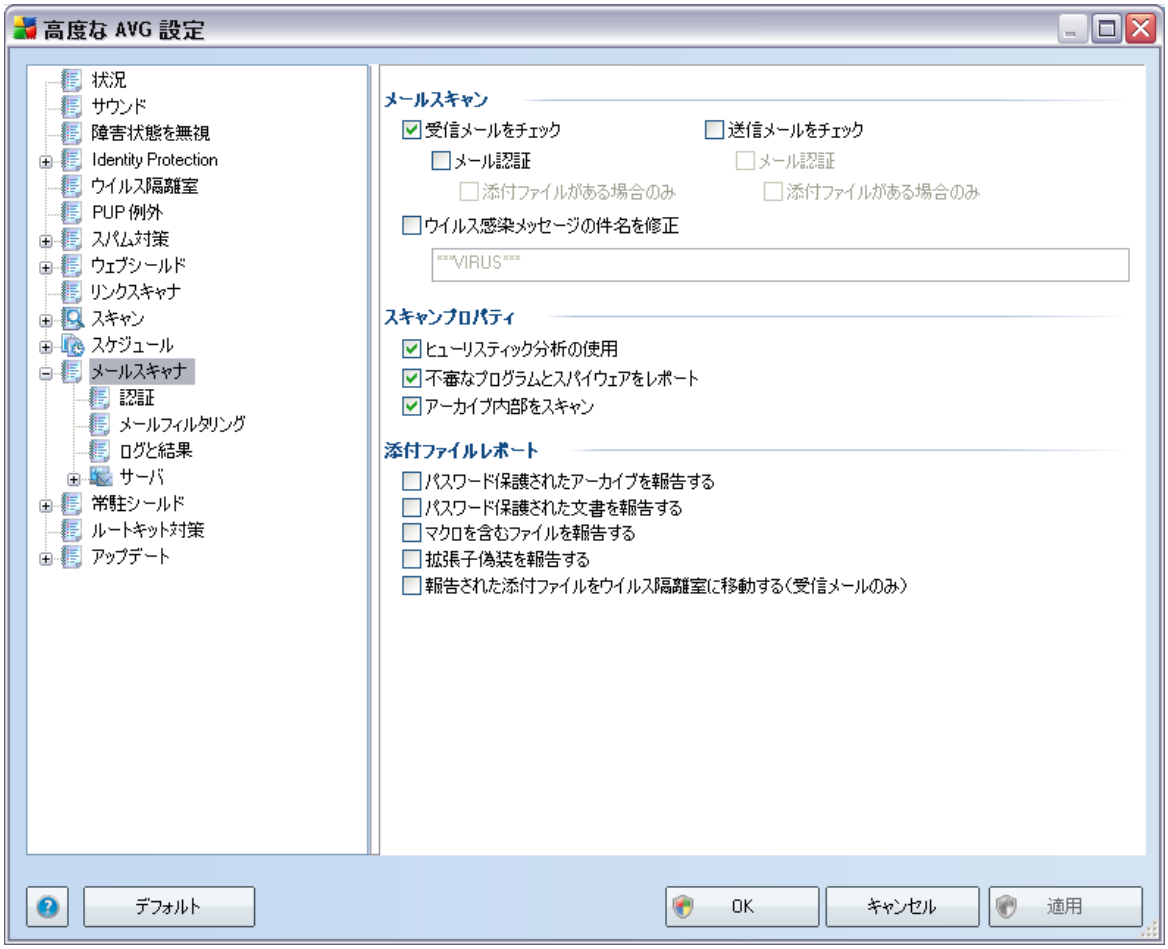
このセクションでは、コンピュータが低電源モードあるいは完全に電源オフになっている場合に、 プログラム アップデートが実行される条件を定義します。

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）。

9.10. メールスキャナ



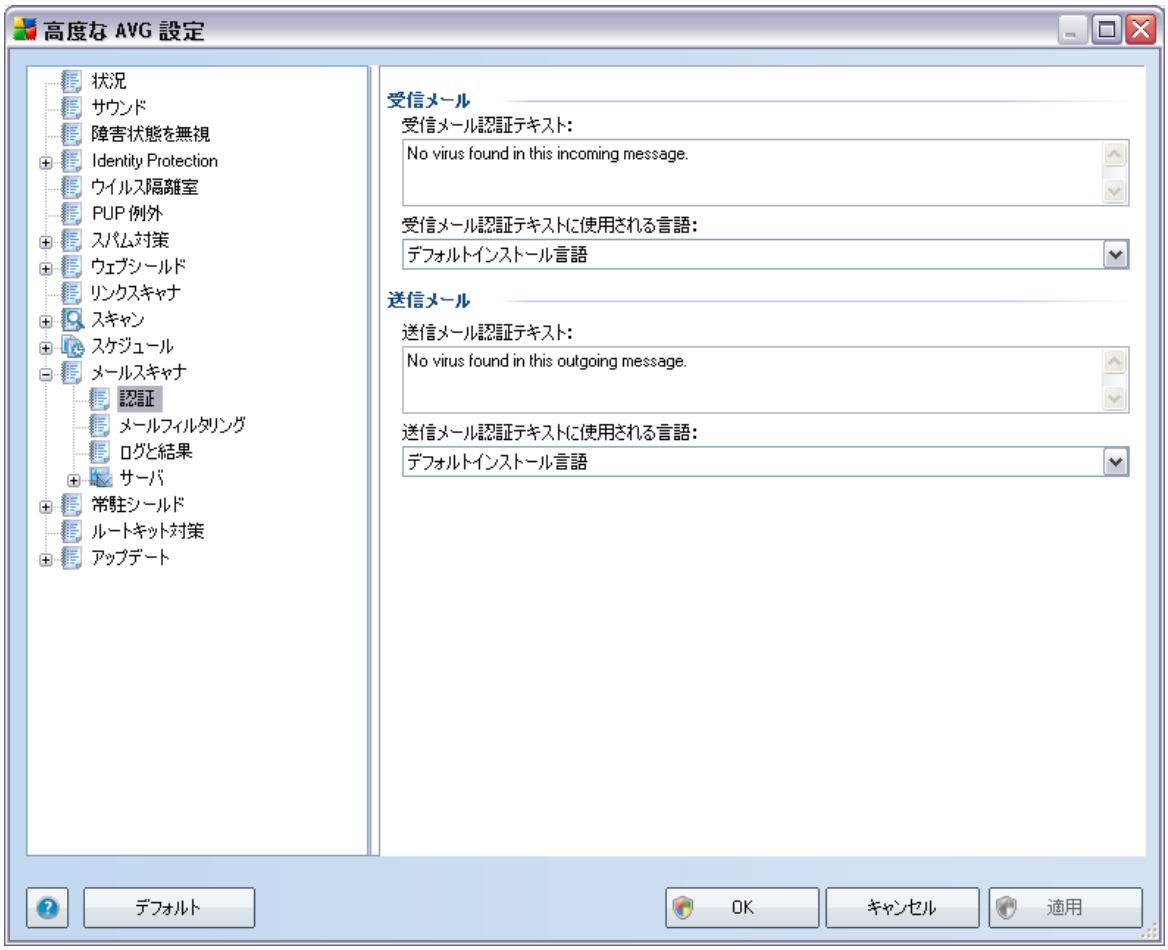
メールスキャナ ダイアログは3つのセクションに分けられます。

- ***メールスキャン*** - このセクションでは、送受信メールのスキャン、認証テキストの使用、添付ファイルのあるメールの認証テキスト使用を設定します（*メール認証はHTML/RTF形式でサポートされています。*）。また、潜在的なウイルスを含むメールを検出した場合、件名を修正するかどうかを選択します。***ウイルス感染メッセージの件名を修正*** チェックボックスにチェックを付けると、件名が指定したテキストに変更されます。（*デフォルト値は***VIRUS*** です。*）。

- ***スキャンプロパティ*** - ヒューリスティック分析 法をスキャン中に使用するかどうか（***ヒューリスティック分析を使用***）、不審なプログラム ***潜在的に望ましくないプログラムとスパイウェア脅威をレポート*** ）をスキャンするかどうか、アーカイブもスキャンされるかどうか（ ***アーカイブ内をスキャン***）を指定します。

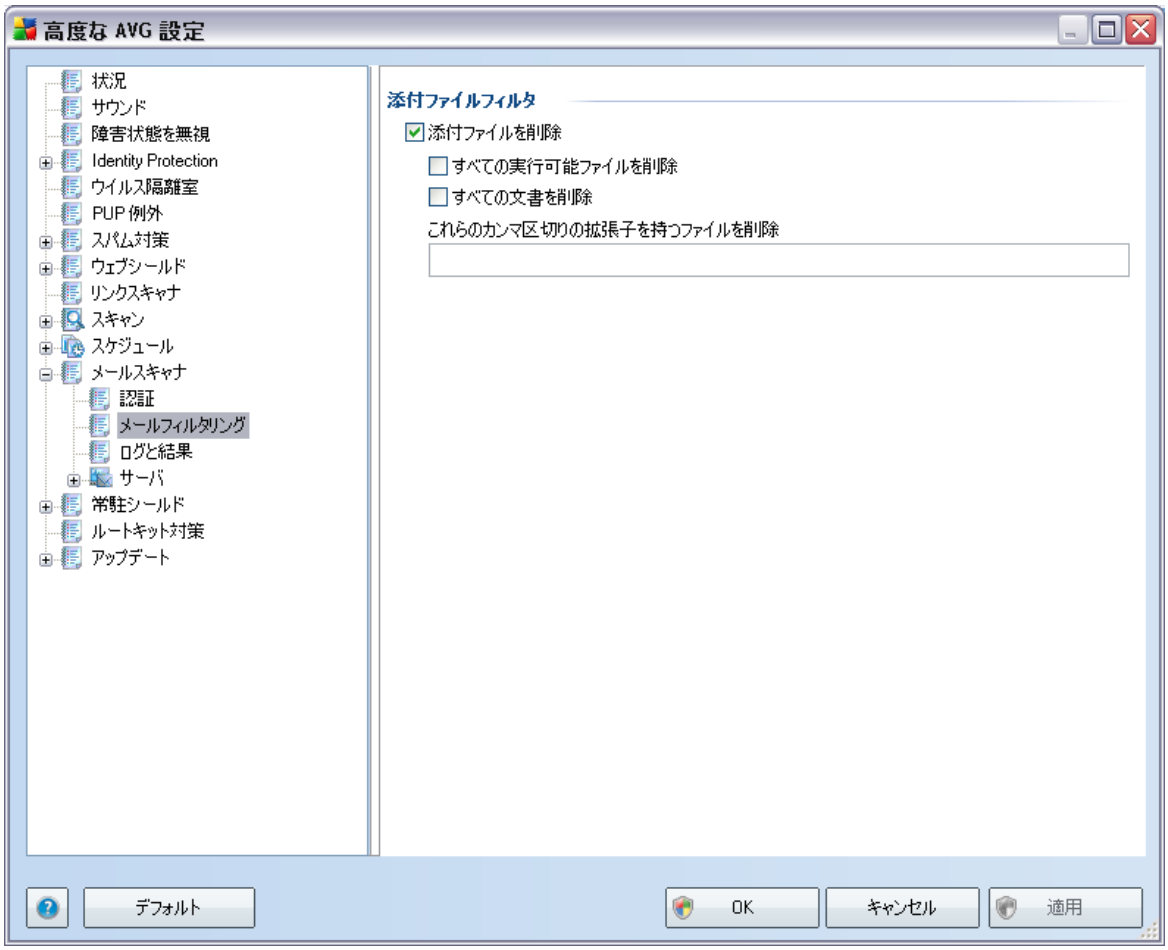
- ***メール添付ファイルレポート*** - 添付ファイルがパスワード保護されたアーカイブ、 パスワード保護されたドキュメント、マクロを含むファイル、拡張子偽装を含む場合、それらをレポートするかどうかを指定します。このようなメールがスキャン中に検出された場合、検出された感染オブジェクトを ***ウイルス隔離室***に移動するかどうかについても指定することができます。

9.10.1. 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***で個別に指定することができます。

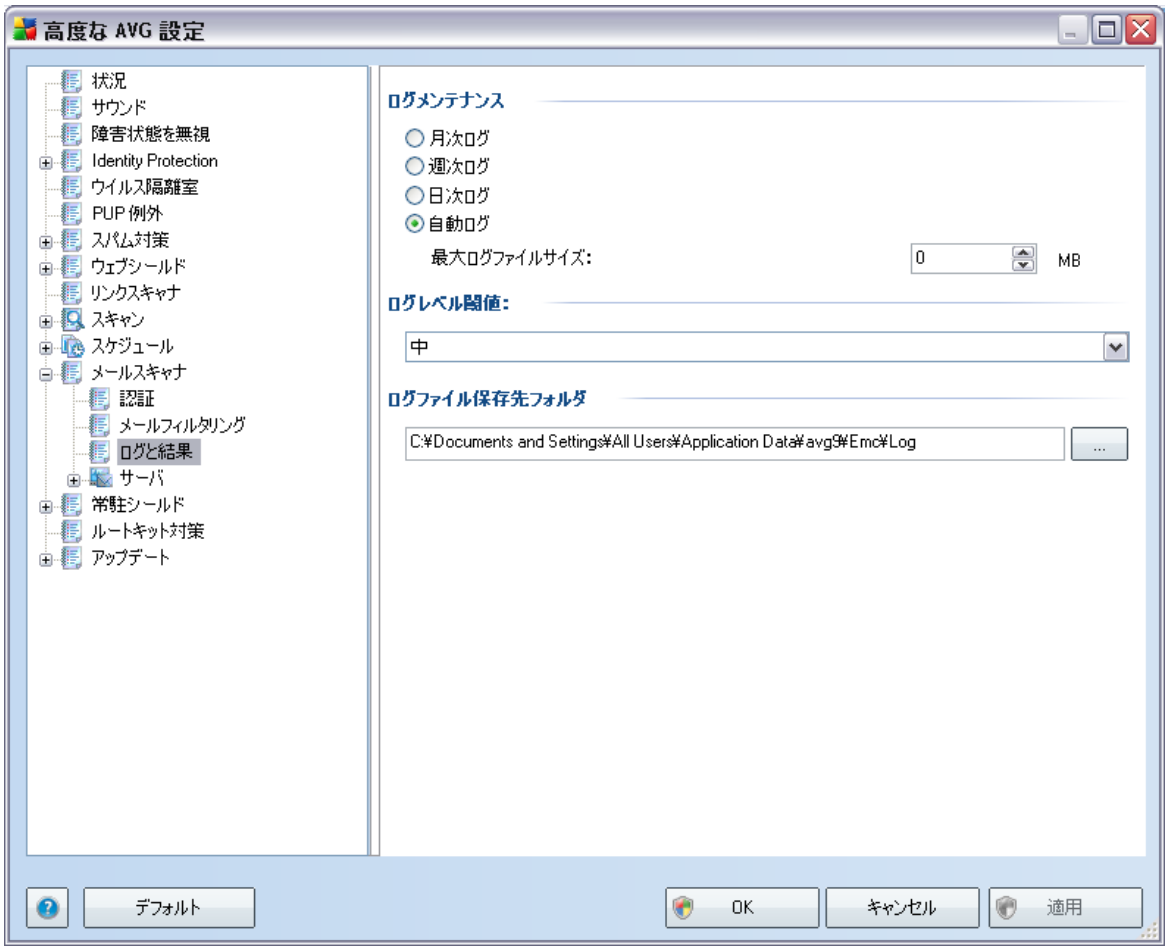
9.10.2. メールフィルタリング



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 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

9.10.3. ログと結果

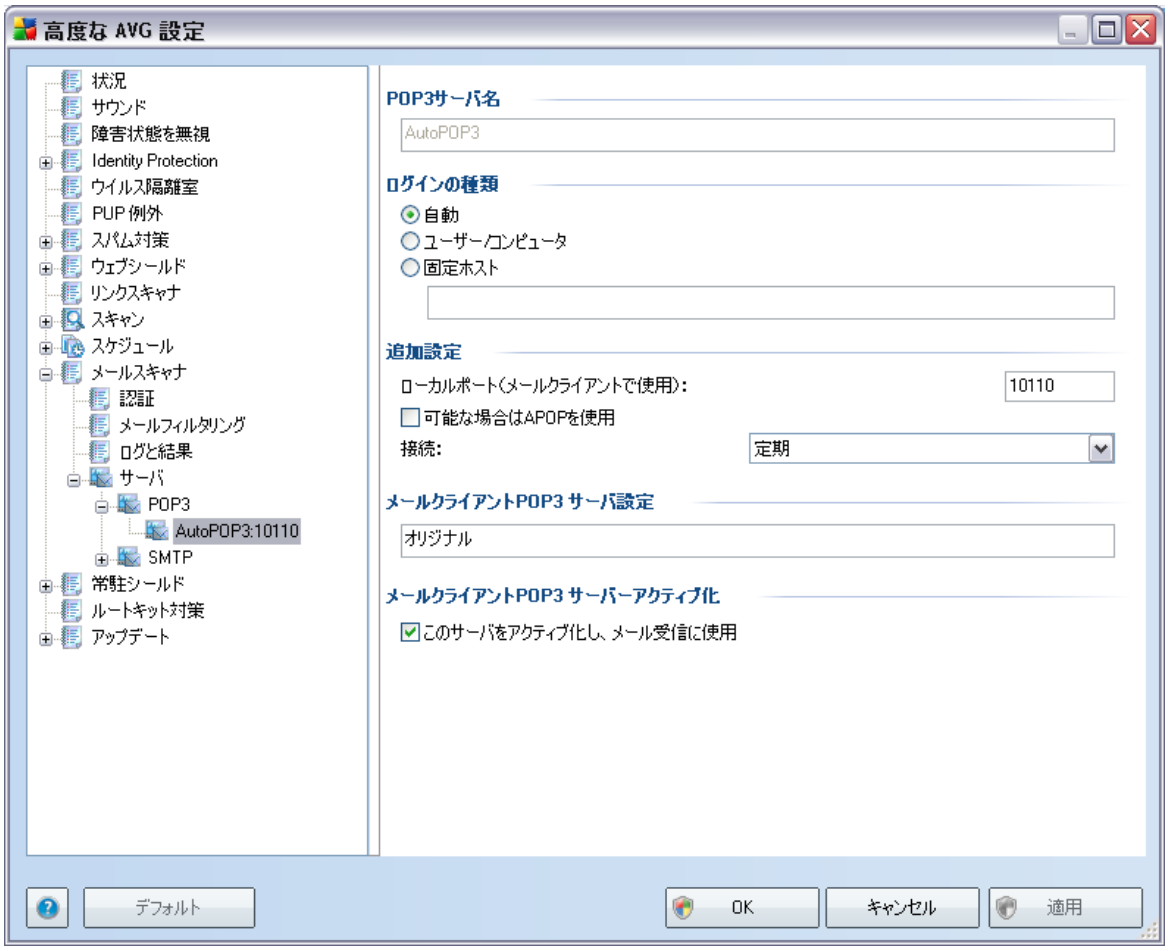


ログと結果 から開かれるダイアログでは、メールスキャナの結果のためのパラメータを指定できます。このダイアログは複数のセクションに分けられます。

- ***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。

9.10.4. 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。
  - o ***自動*** - メールクライアントの設定にしたがって、自動的ログインが実行されます。

- ***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。

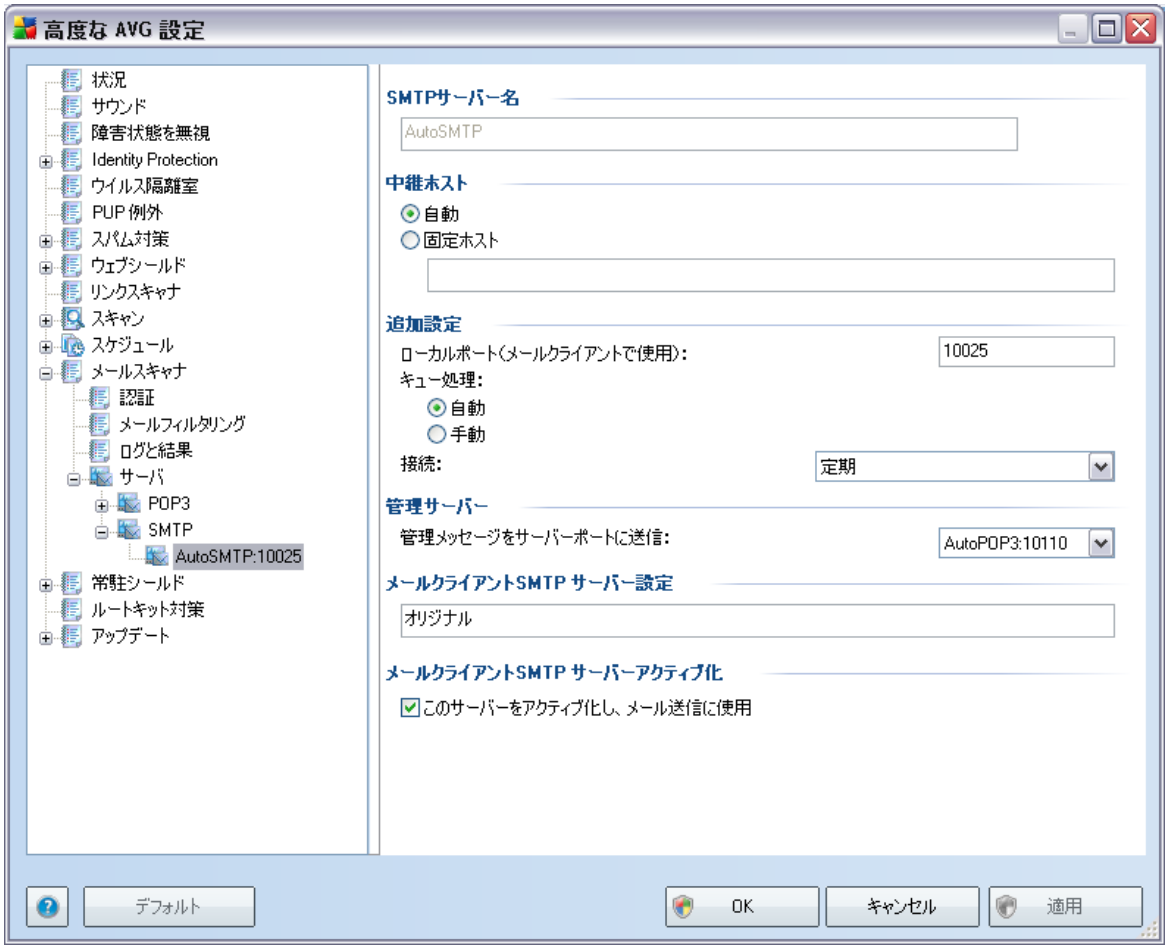
  - ***ローカルポート*** - メールアプリケーションからの通信用ポートを指定します。メールアプリケーション上で、このポートをPOP3通信のポートとして指定する必要があります。

  - ***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 POP3 サーバ設定*** - （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情報を表示します。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。

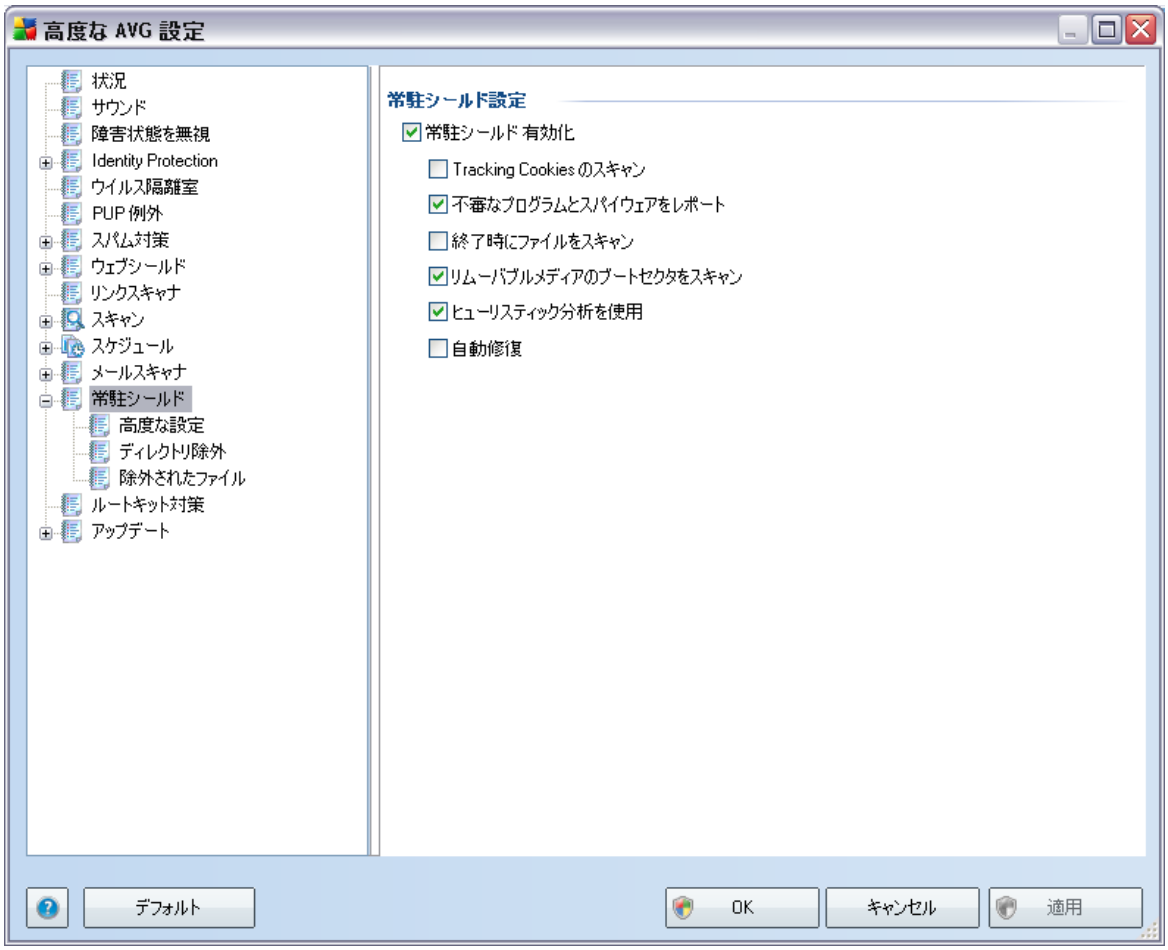
- ***SMTPサーバー名*** - サーバー名を入力するか、デフォルトのAutoSMTP名を。
- ***中継ホスト*** - 送信メールに使用されるメールサーバー決定方法を定義します。
  - o ***自動*** - メールクライアントの設定にしたがって、自動的ログインが実行されます。
  - o ***固定ホスト*** - プログラムは常にここで指定されたサーバーを使用します。メールサーバーのアドレスと名前を指定してください。IPアドレス（例えば、123.45.67.89）と同様に、ドメイン名（例えば、smtp.acme.com）を使用することもできます。メールサーバーが標準でないポ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。

9.11. 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 では、***常駐シールド有効化*** のチェックによって、***常駐シールド***保護の有効化、無効化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はオンです*）。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。

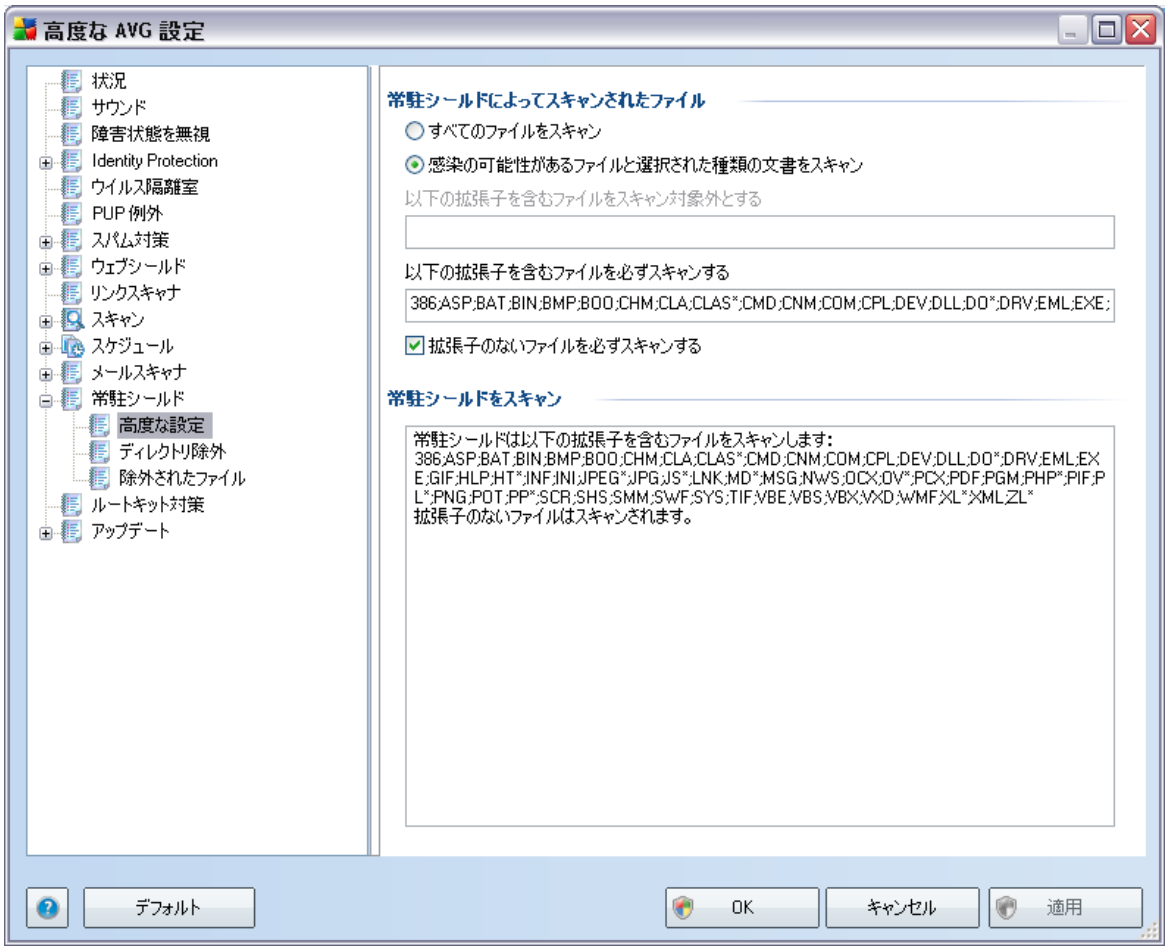
- ***Tracking Cookieをスキャン*** - このパラメータはcookieがスキャン中に検出されるかどうかを定義します。（*HTTP cookies は、認証、トラッキング、サイトのプリファレンスや電子ショッピングカードの内容等の特定のユーザー情報の保持に使用されます*）
- ***不審なプログラムとスパイウェア脅威をレポート*** - *デフォルトではオン*）不審なプログラム（*スパイウェ*

アやアドウェアのように動作する様々なタイプの実行可能アプリケーション）をスキャンします。

- ***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。

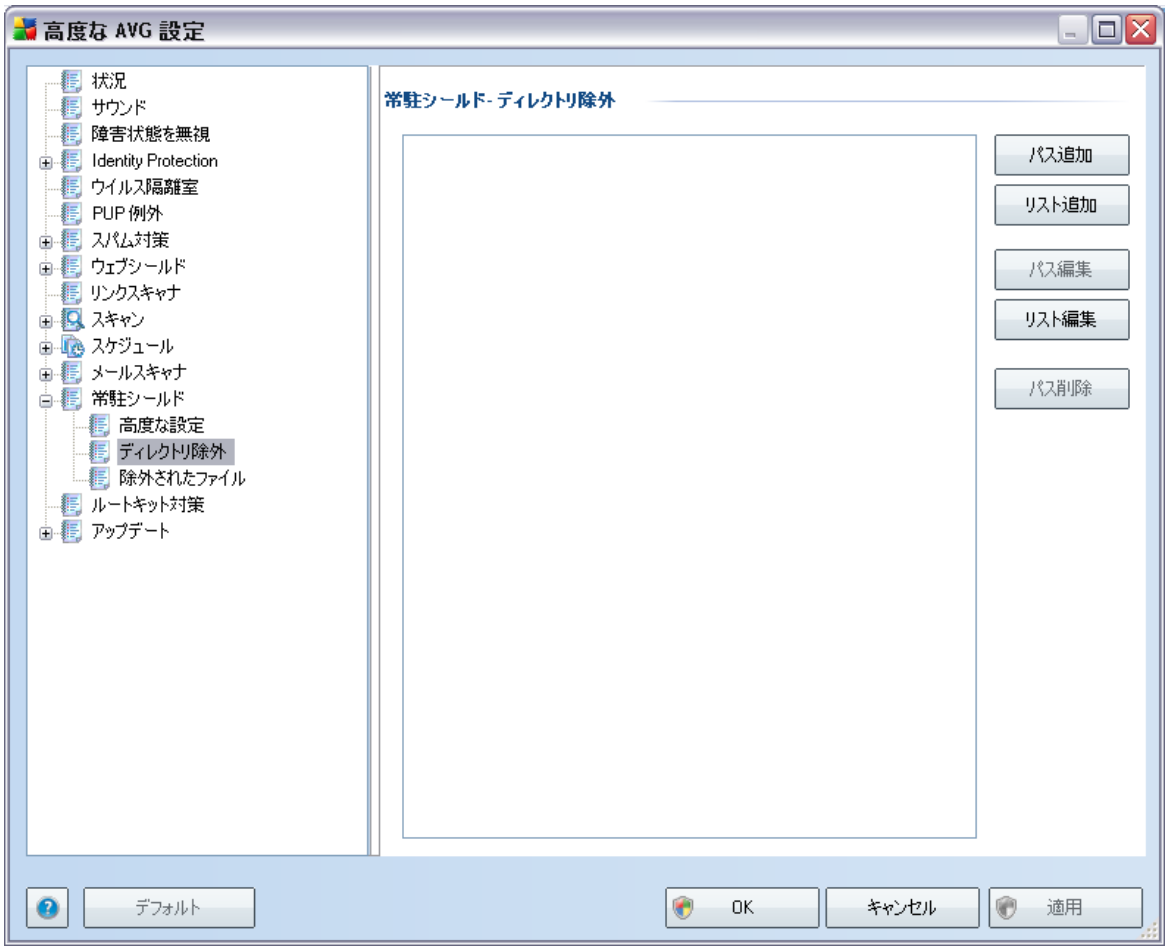
9.11.1. 高度な設定

常駐シールドスキャン対象ファイル 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。

9.11.2. 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。

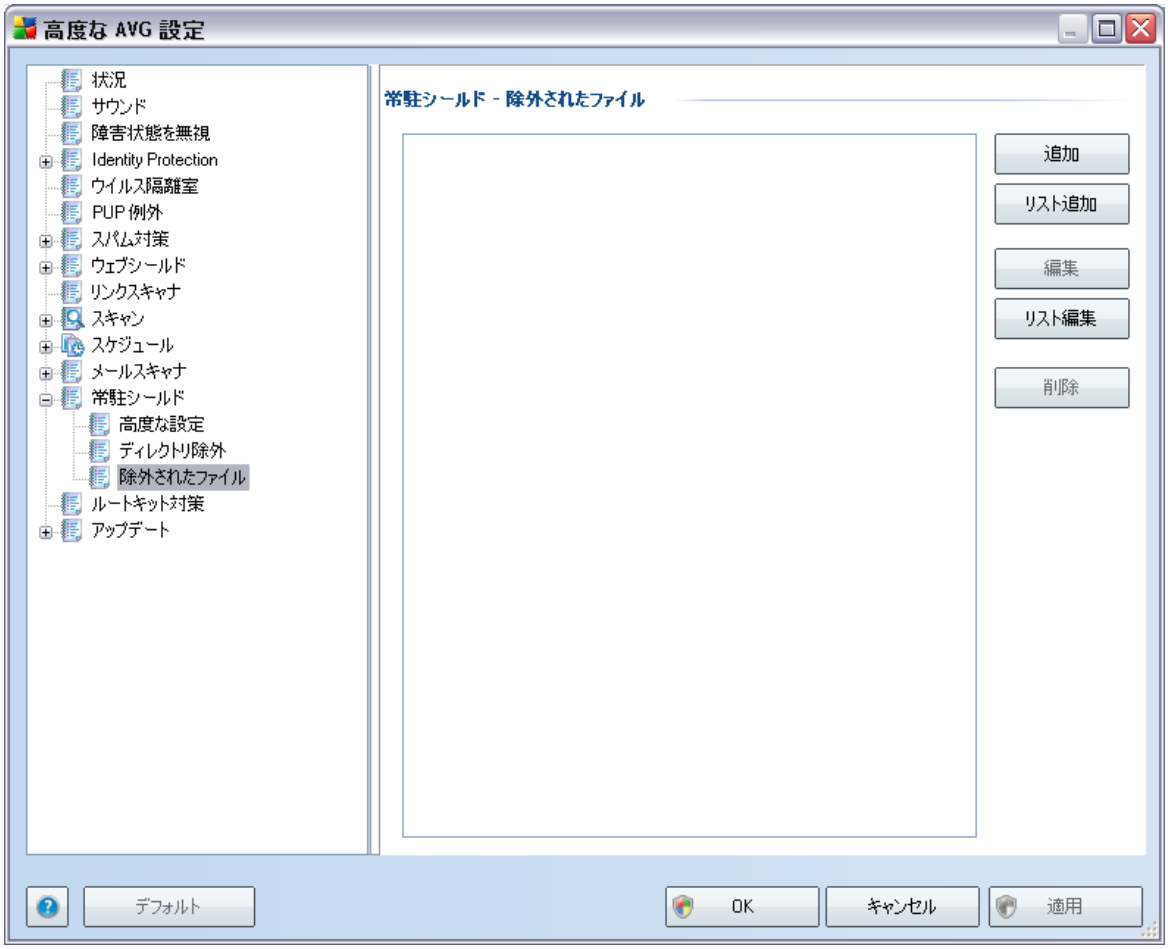
必要でない場合、ディレクトリを除外しないことを強く推奨します。

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

9.11.3. 除外されたファイル



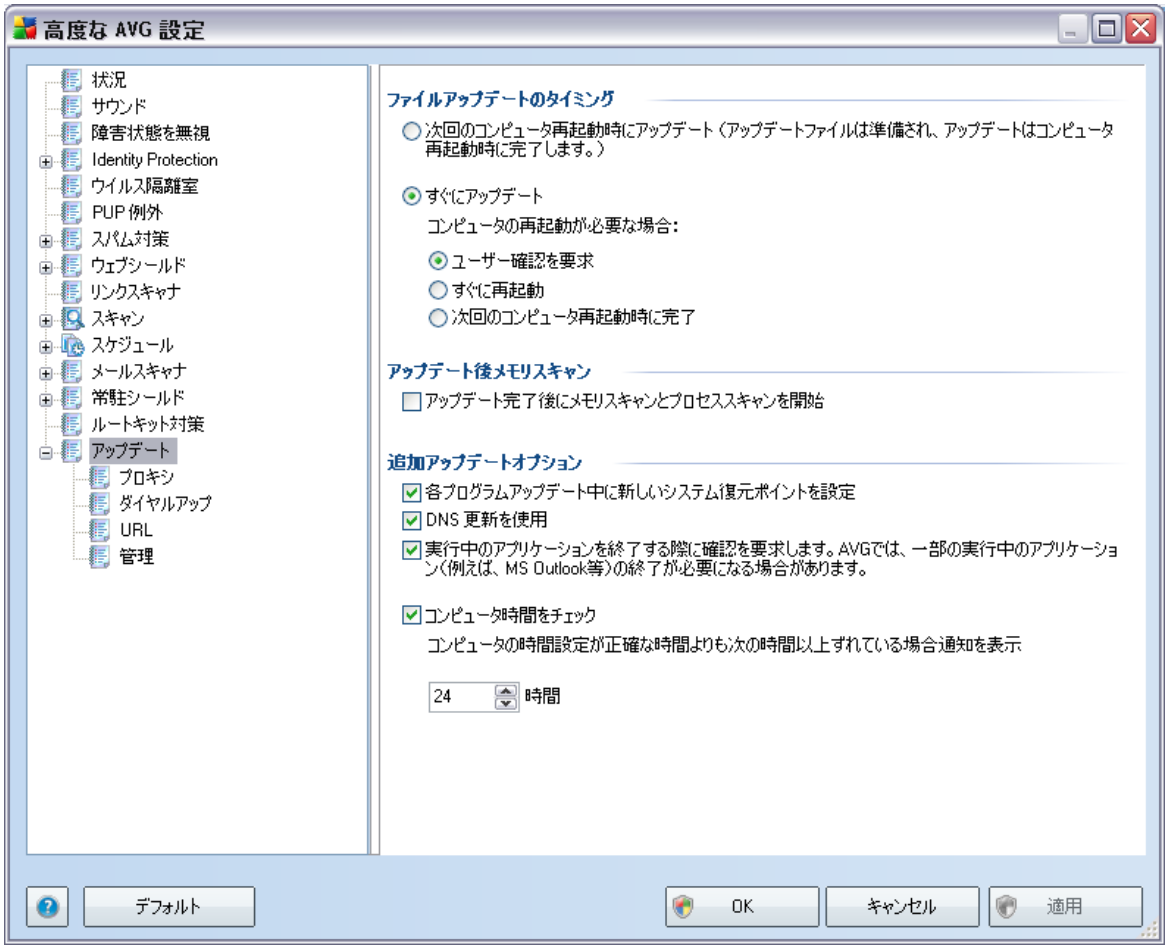
[***常駐シールド - 除外されたファイル***] ダイアログは、先に説明した ***常駐シールド - 除外されたディレクトリ*** と類似した方法で動作しますが、 ***常駐シールド*** スキャンから除外するフォルダではなく、特定のファイルを定義できます。

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。
- ***編集*** _ 選択フォルダへの特定のパスを編集できます
- ***リスト編集*** ?フォルダリストを編集します。
- ***削除*** ?選択したフォルダのパスを削除できます

9.12. 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。

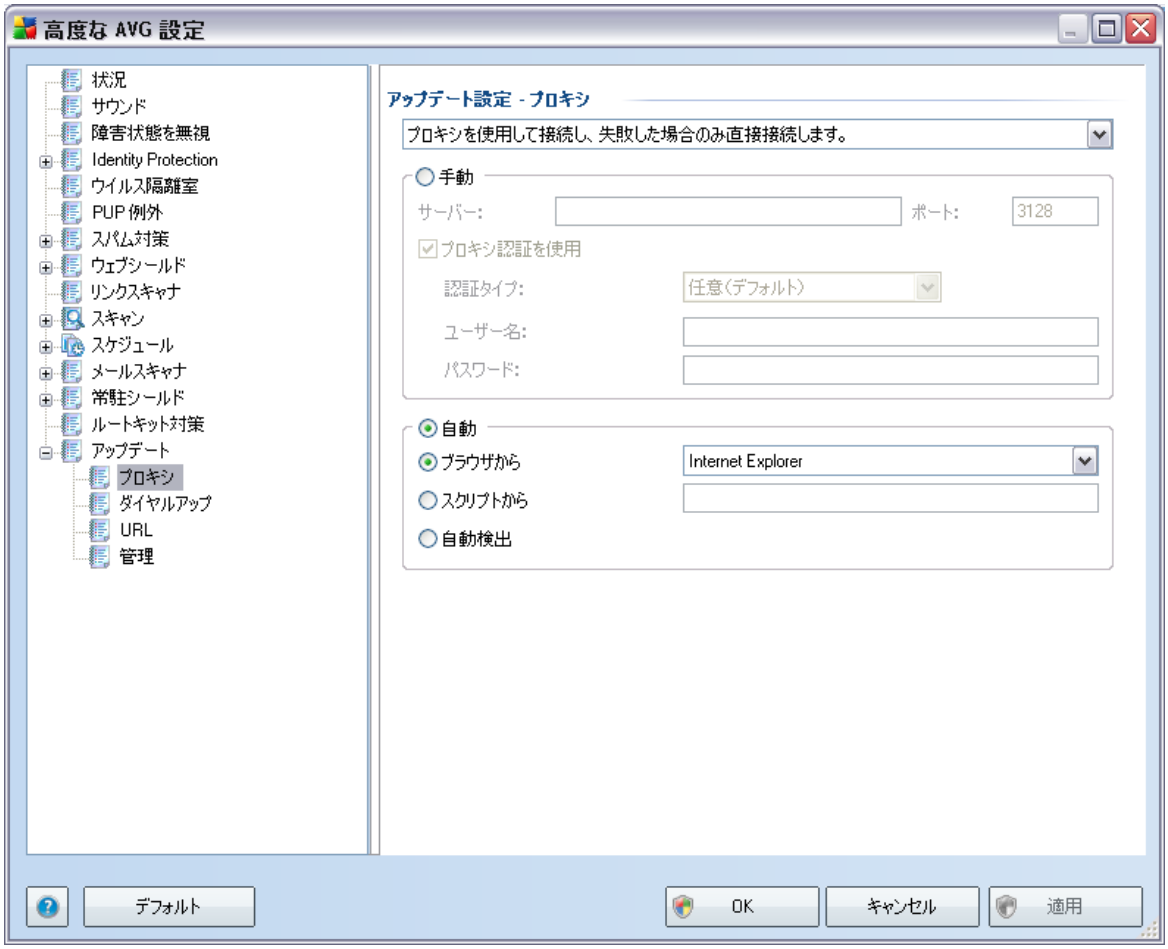
追加アップデートオプション

- ***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。

9.12.1. 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項目で、コンボボックスメニューから希望するものを選択してください。

- ***プロキシを使用***

- ***プロキシを使用しない***
- ***プロキシを使用して接続し、失敗した場合のみ直接接続する*** - デフォルト設定

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、変更で可能です?不明な場合は、ネットワーク管理者にお問い合わせ下さい）

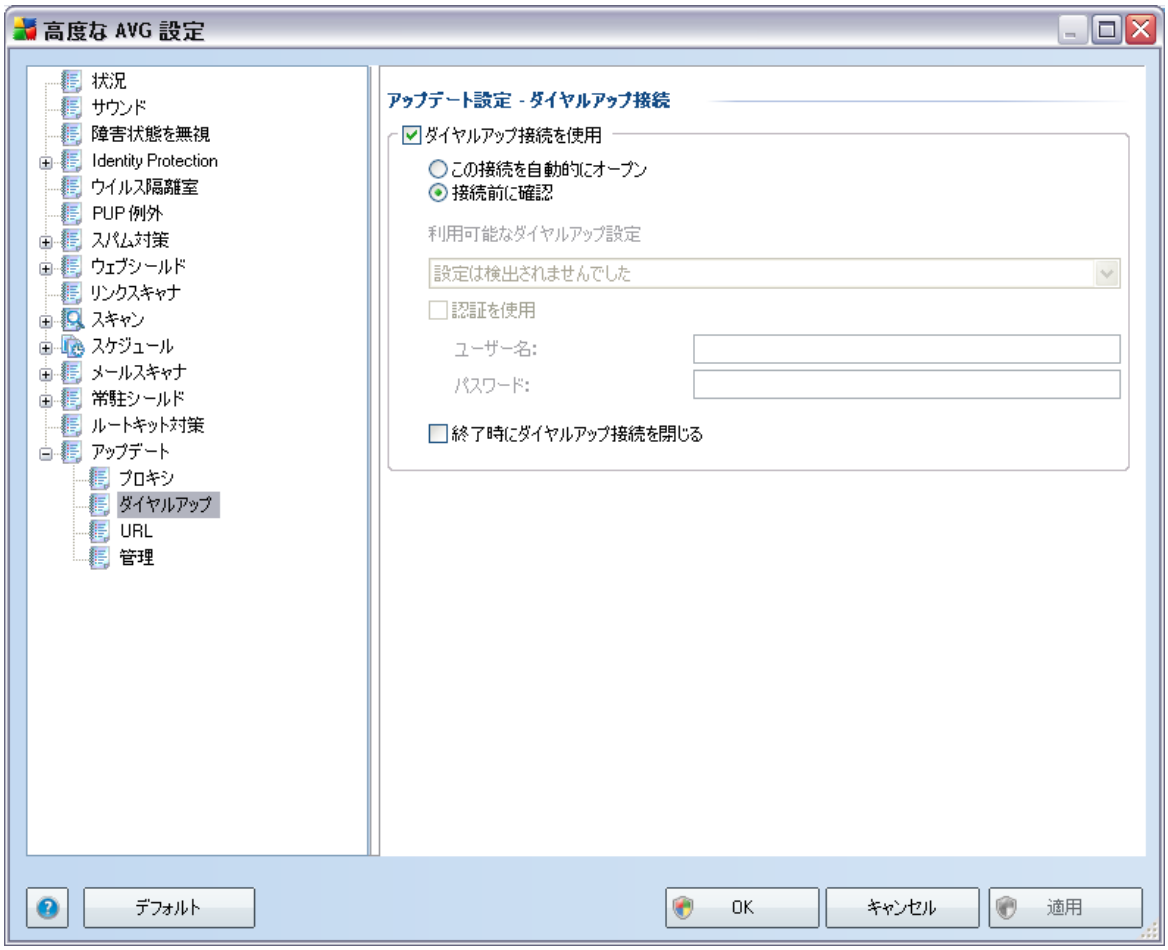
プロキシサーバーは、各ユーザーのルールを設定することもできます。プロキシサーバーがこのように設定されている場合、***プロキシ認証を使用***にチェックを付け、有効なユーザー名とパスワードを入力してください。

自動設定

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

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

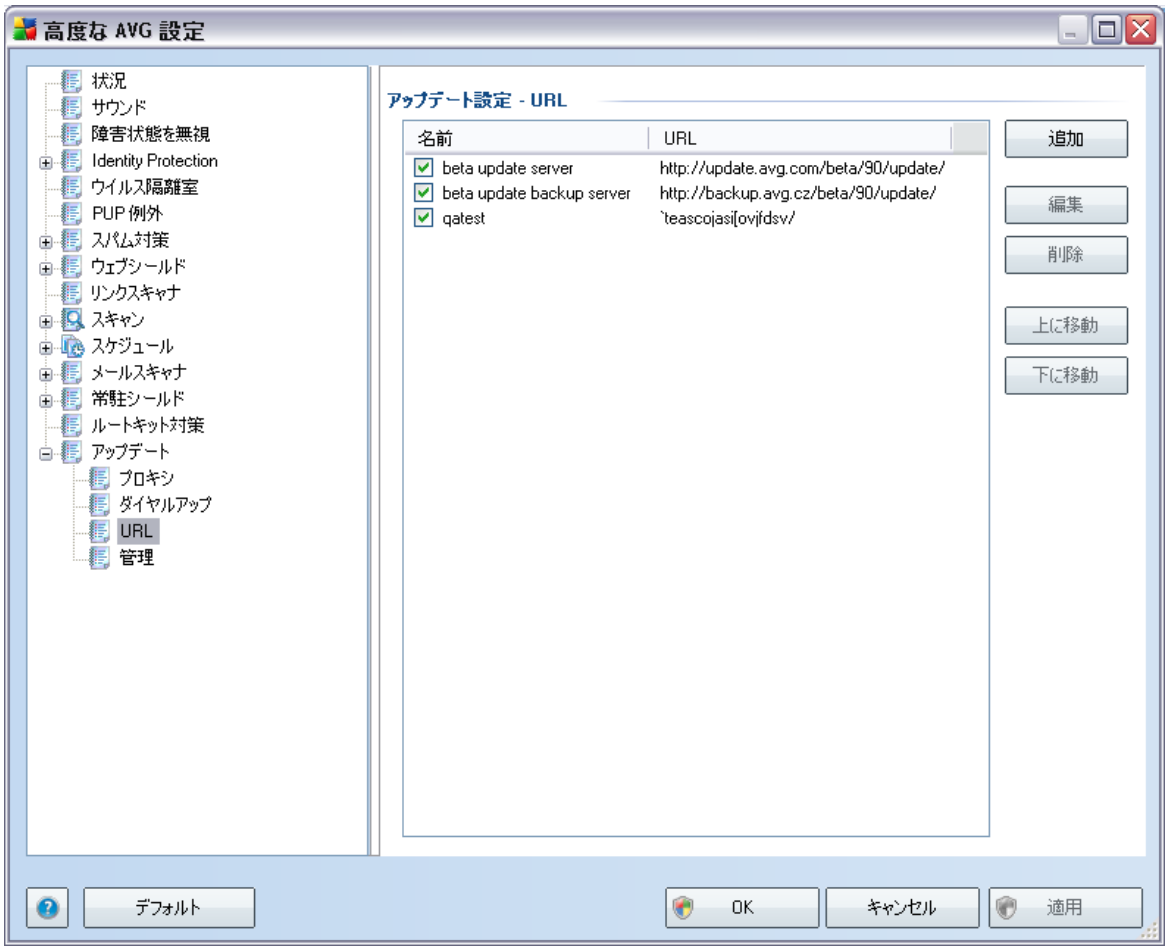
9.12.2. ダイヤルアップ



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（***この接続を自動的にオープン***）、または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、アップデート終了後に接続を切断するかどうかを選択します。（***終了時にダイヤルアップ接続を閉じる***）。

9.12.3. 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。

9.12.4. 管理

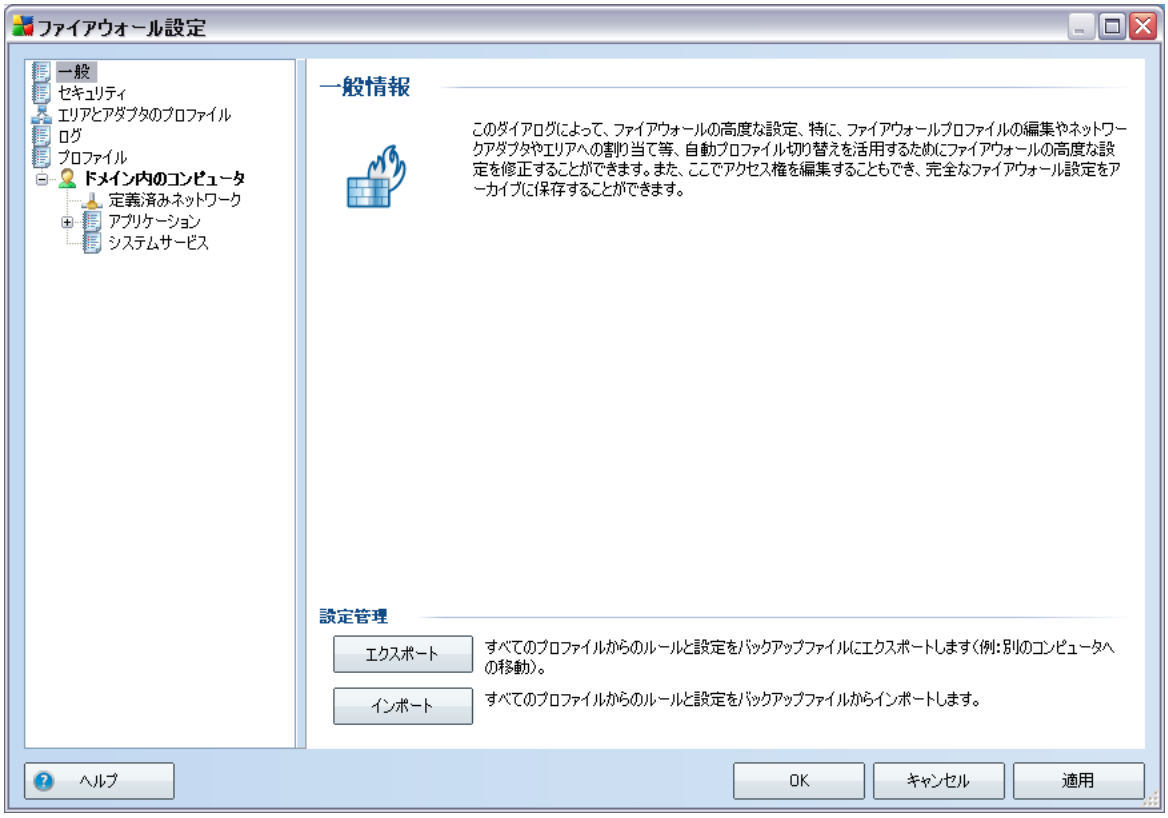
[***管理***] ダイアログには 2 つのオプションがあり、2 つのボタンを使用してアクセスできます。

- ***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. ファイアウォール設定

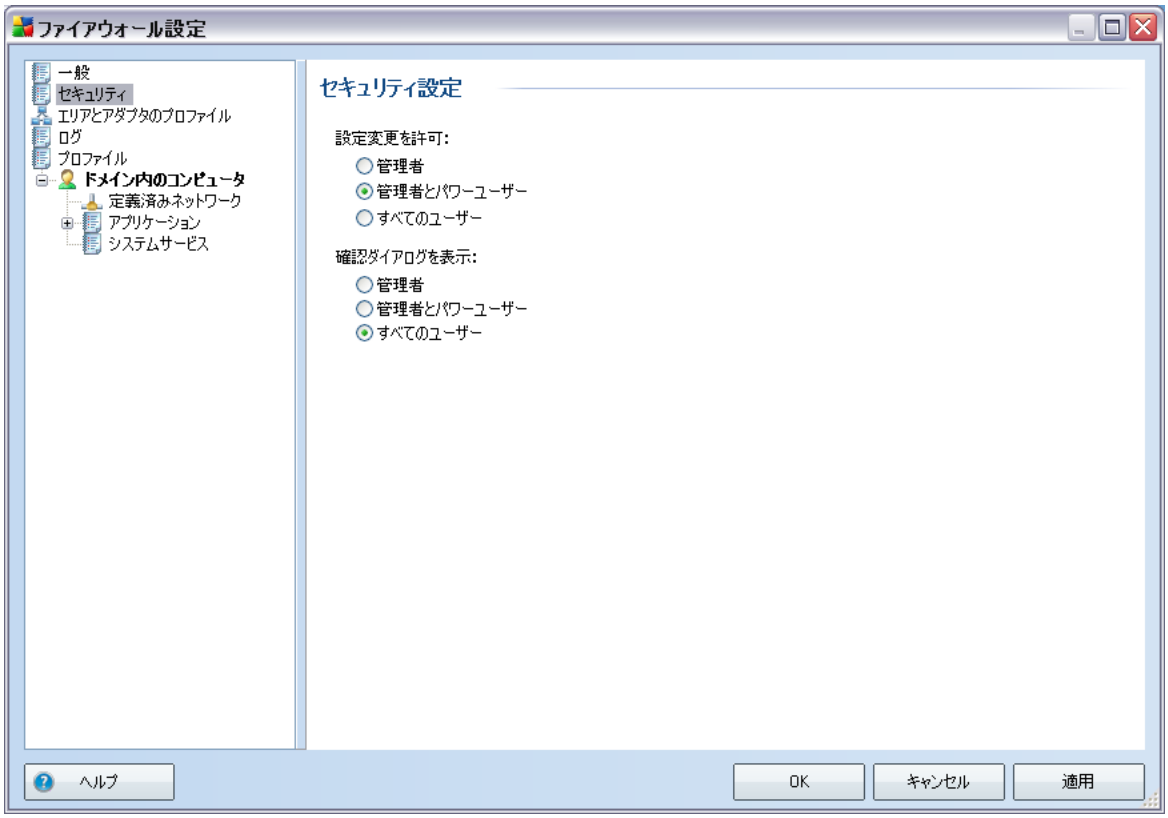
ファイアウォール 設定は新しいウィンドウで表示されます。ここでは、いくつかのダイアログで、コンポーネントの高度なパラメータを設定することができます。 ***ただし、高度な設定編集は専門家と経験のあるユーザーのみを対象としています。***

10.1. 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。

10.2. セキュリティ



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

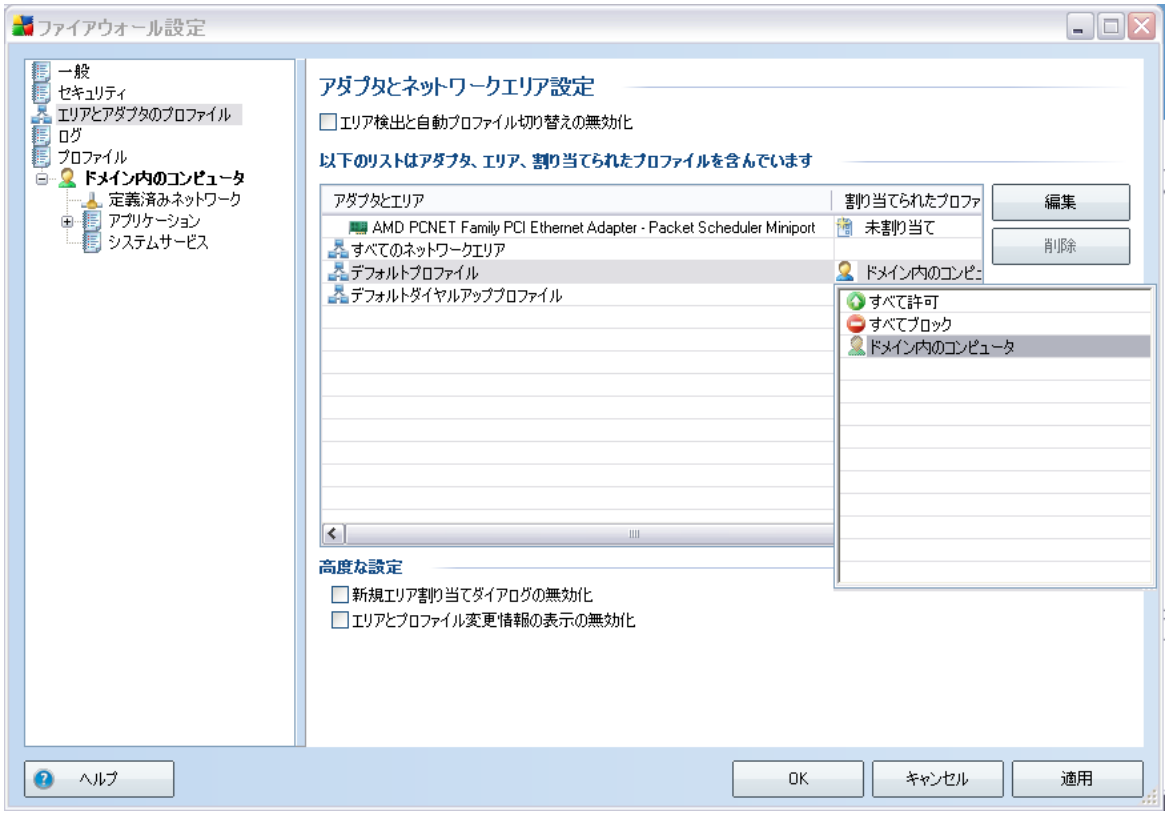
- 設定変更を許可 - ***ファイアウォール*** の設定変更を許可するユーザーを指定します。
- 確認ダイアログを表示 - 設定ダイアログ（*定義された* ***ファイアウォール*** *ルール*に含まれていない状況での決定ダイアログ）が表示されるユーザーを指定します。

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

- ***管理者*** _PCを完全にコントロールし、すべてのユーザーを定義されたグループに割り当てる権限を持っています。
- ***管理者とパワーユーザー*** ?管理者は任意のユーザーを指定されたグループ（ パワーユーザー）に割り当て、グループメンバーの権限を定義することができます。

o ***すべてのユーザー*** ?特定のグループに割り当てられていないその他のユーザー

10.3. エリアとアダプタのプロファイル



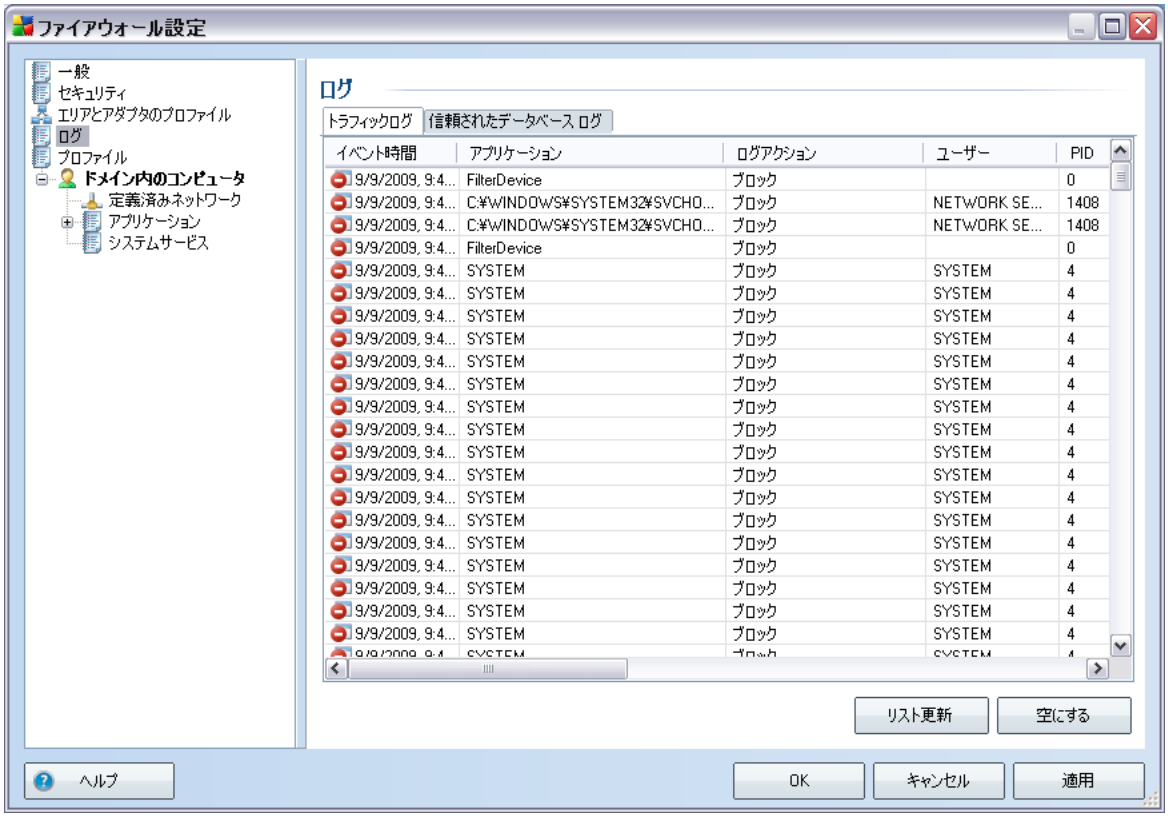
アダプタとネットワークエリア設定 ダイアログでは、定義済みプロファイルの特定のアダプタへの割り当てと、該当するネットワークの参照に関する設定を編集します。

- ***エリア検出と自動プロファイル切り替えの無効化*** - 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。.

10.4. 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

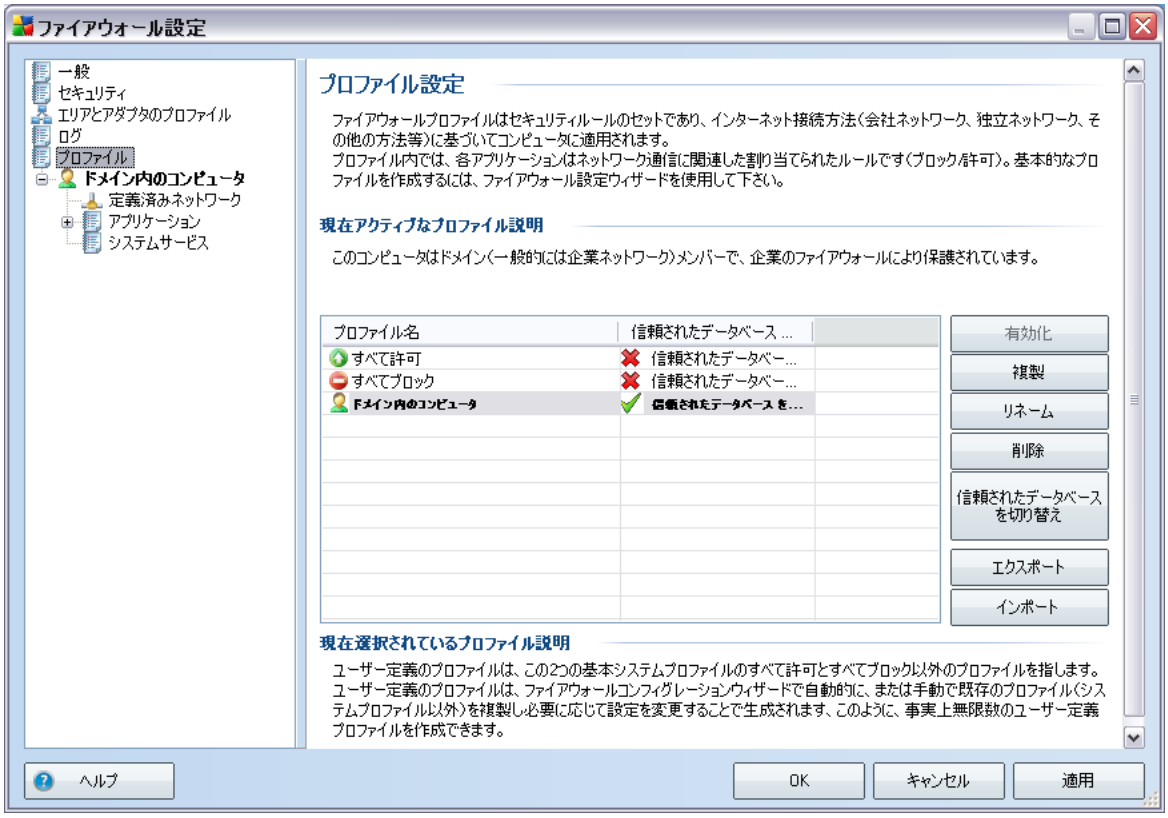
きる情報がない場合、アプリケーションのネットワークアクセスを許可するかどうかを確認するスタンドアロンダイアログが表示されます。

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。

10.5. 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*

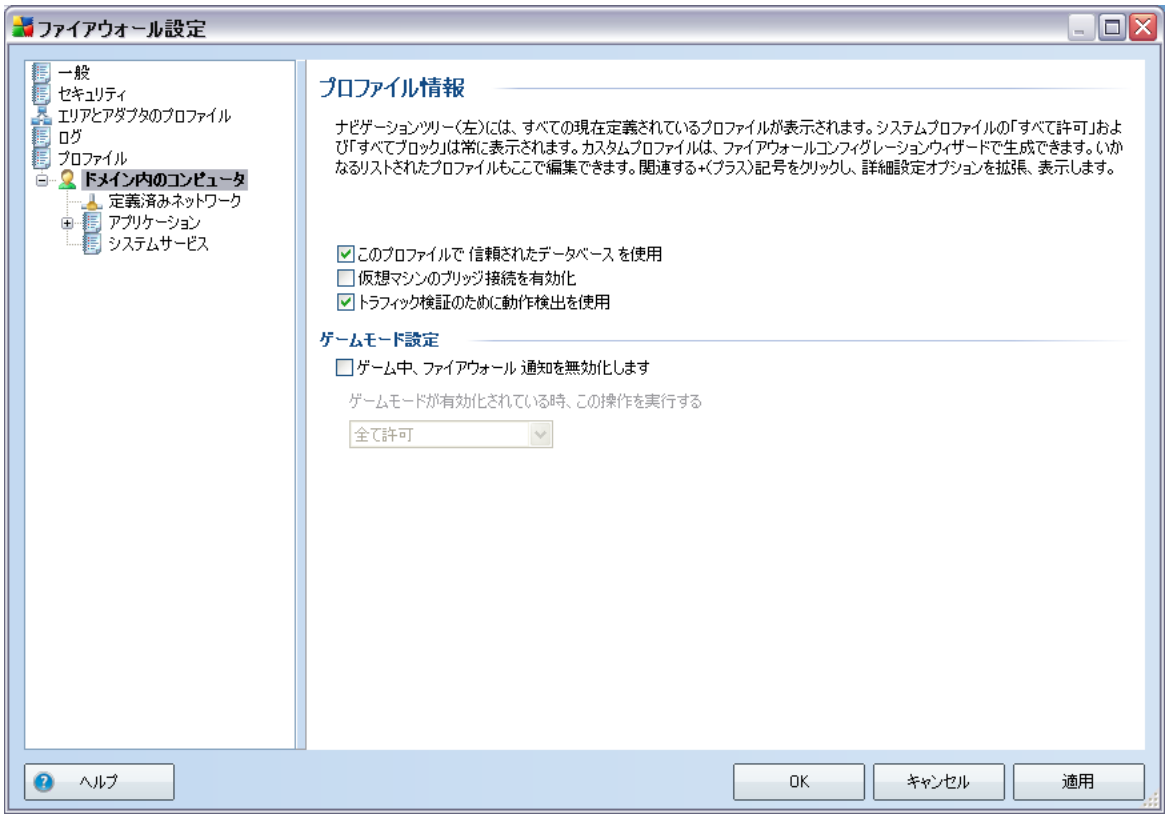
に関する情報を収集するデータベースです ）を使用するかどうかを決定できます。

- ***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。

10.5.1. 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。

- ***Pro tento profil použít Důvěryhodnou databázi*** - *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。

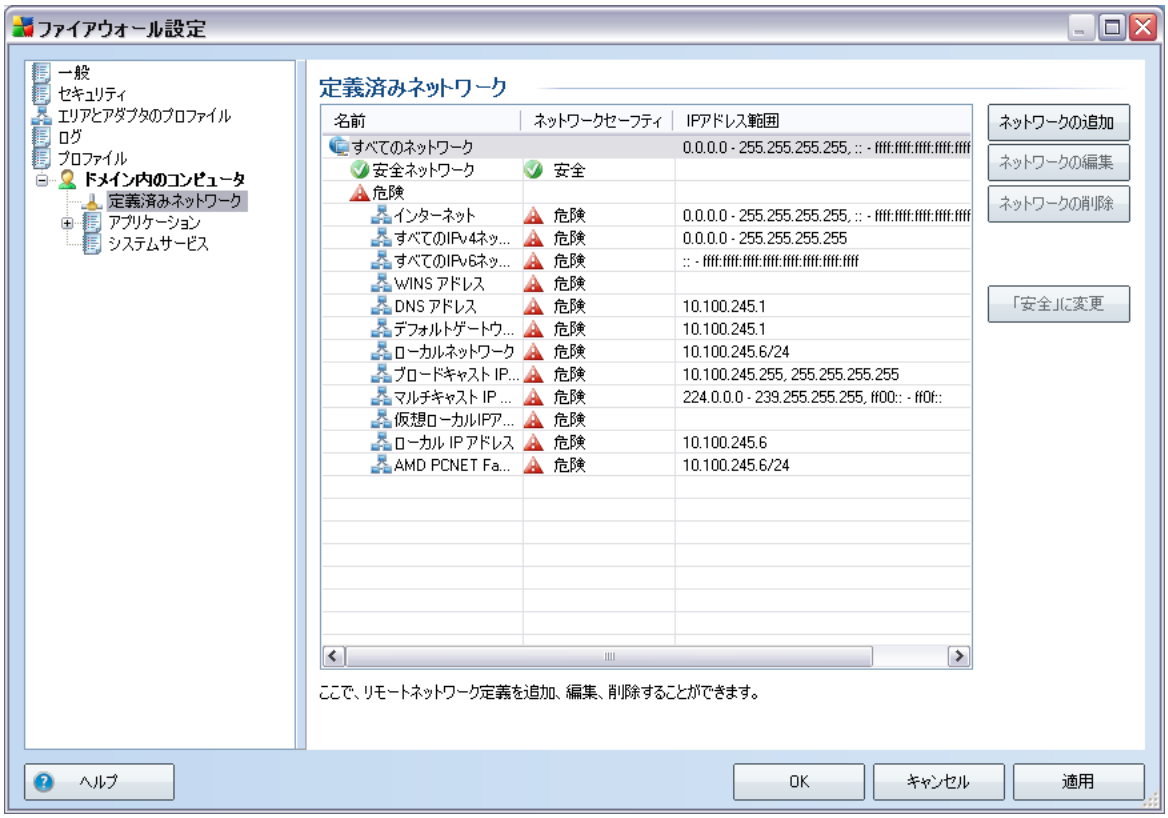
- ***トラフィック資格の動作検出を使用*** - (*既定ではオン*) このオプションをオンにすると、アプリケーションを評価するときに、***ファイアウォール*** を使用して、***LinkScanner*** 機能を使用します。***LinkScanner*** は、アプリケーションが不審な動作をしめしているか、あるいは信頼されオンライン通信を許可されているかどうかを判断できます。

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。

10.5.2. 定義済みネットワーク



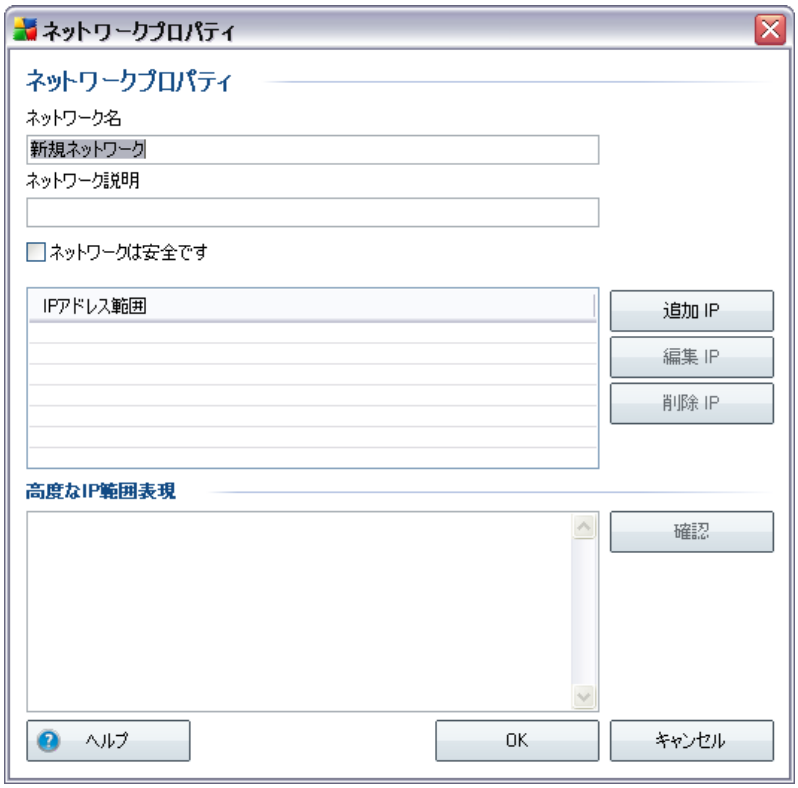
定義済みネットワークダイアログはコンピュータが接続するすべてのネットワークのリストを提供します。検出されたネットワークに関して、以下の情報が提供されます。

- ***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。



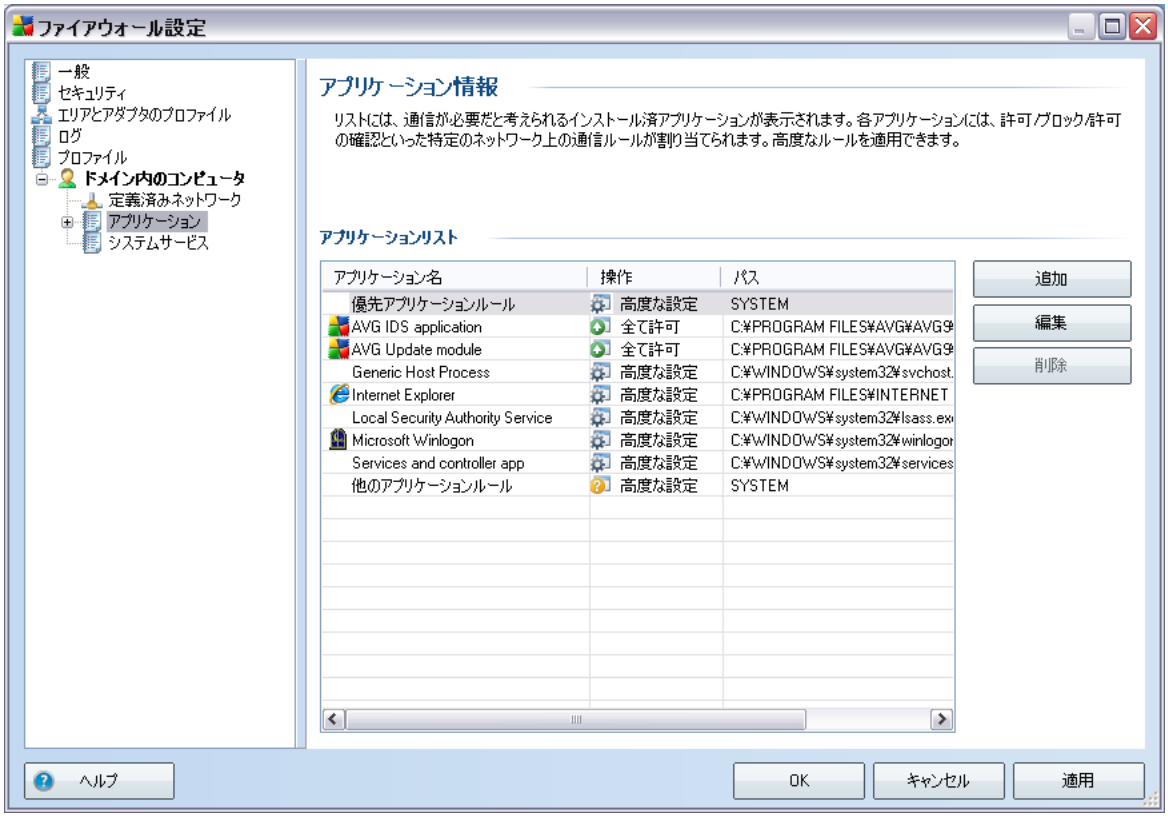
このダイアログでは、***ネットワーク名*** し、***ネットワーク説明*** を入力し、ネットワークが安全かどうかを指定することができます。新しいネットワークは ***IPの追加*** ボタン または***IPの編集*** / ***IPの削除*** ）で開かれるダイアログで定義されます。このダイアログでは、IPの範囲やマスクを指定することでネットワークを設定することができます。

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に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」に変更*** - 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考えられます。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、このボタンを使用して、「安全」に変更してください。

- ***ヘルプ*** - ヘルプファイルに関するダイアログを開きます。

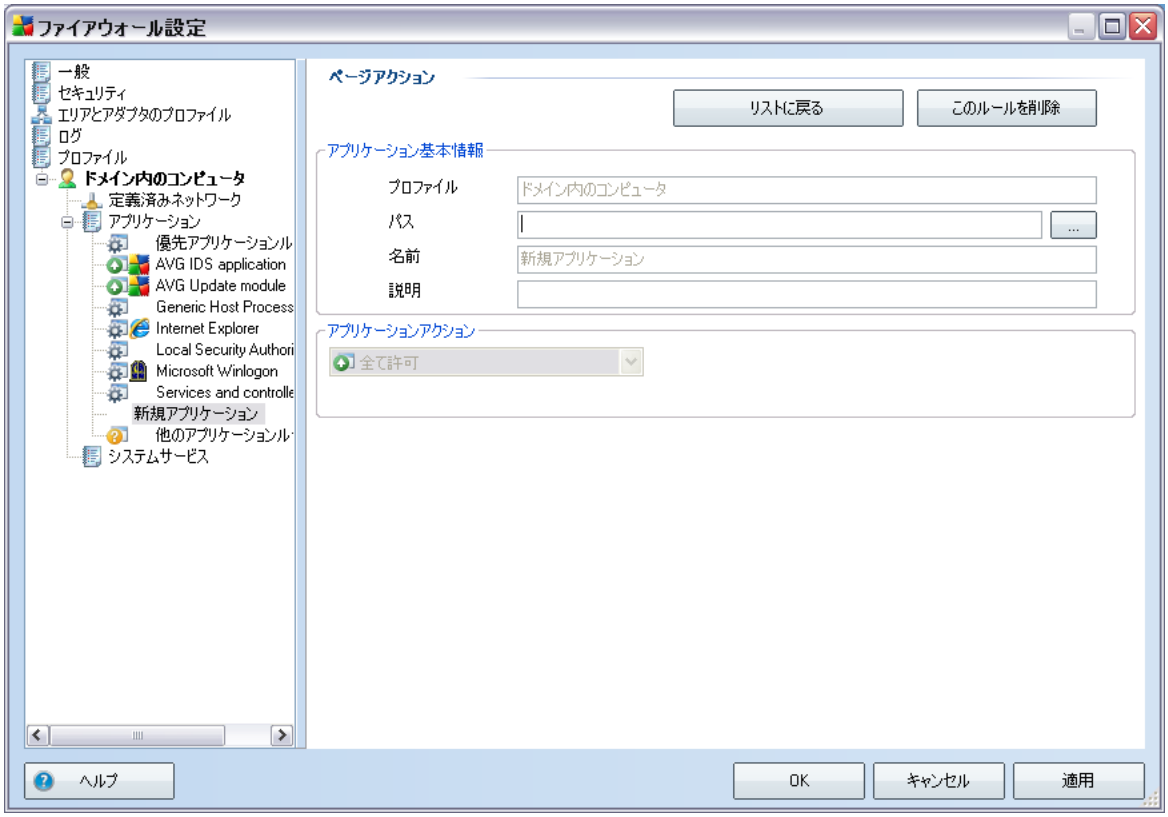
10.5.3. アプリケーション



[***アプリケーション情報***] ダイアログでは、ネットワーク上で通信するすべてのアプリケーションの概要が表示されます。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のルールセットを作成するためのイアログを開きます。
- ***編集*** - 既存のアプリケーションルールセットの編集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。

新しいアプリケーションルールセットを定義するダイアログを表示するには、 ***ファイアウォール設定*** の ***アプリケーションダイアログで*** 追加 ***ボタンを押します*** 。



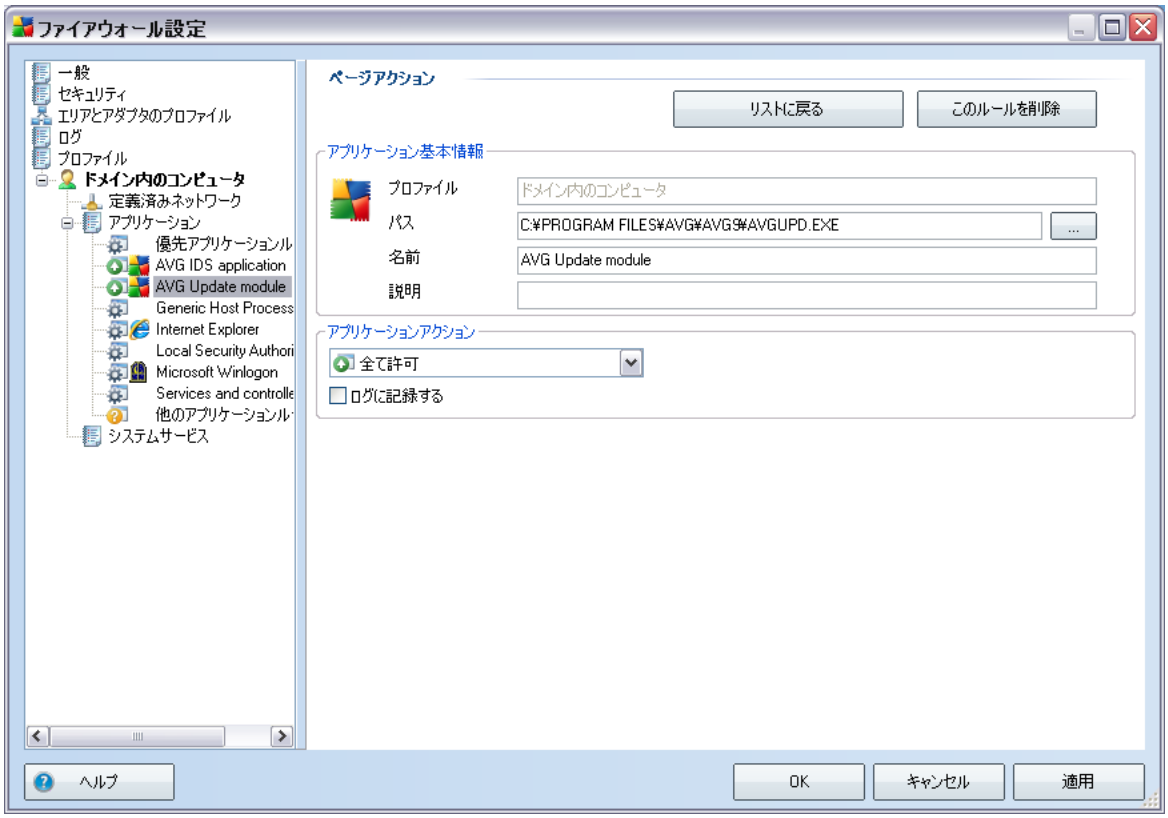
このダイアログでは以下を設定することができます。

- ***アプリケーション基本情報*** - アプリケーション名、簡潔な説明、ディスク上のパス
- ***アプリケーションアクション*** - ドロップダウンメニューから、アプリケーションの動作に適用されるルールを選択します。
  - ***高度な設定*** - このオプションを選択すると、このダイアログの下部で詳細にルールセットを編集することができます。 *このセクションの説明については、* ***アプリケーションを編集*** *の章を参照してください。*
  - ***全て許可*** - アプリケーションのすべての通信が許可されます。
  - ***許可*** - アプリケーションは、安全なネットワーク上での通信のみ許可されます。 *例えば、保*

護された会社のネットワークへの通信は許可されますが、インターネットへの通信はブロックされます。)。安全なネットワークについての概要と説明は、 ***ネットワーク***ダイアログを参照してください。

- ***確認*** - アプリケーションがネットワーク上で通信する場合、通信の許可、またはブロックを選択する画面が表示されます。
- ***ブロック*** - アプリケーションのすべての通信はブロックされます。

既存のアプリケーションルールセットを編集するダイアログを表示するには、 ***ファイアウォール設定*** の***アプリケーションダイアログで***編集 ***ボタンを押します。*** 。



このダイアログでは、すべてのアプリケーションパラメータを編集できます。

- ***アプリケーション基本情報*** - アプリケーション名、簡潔な説明、ディスク上のパス
- ***アプリケーションアクション*** - ドロップダウンメニューから、アプリケーションの動作に適用されるルールを

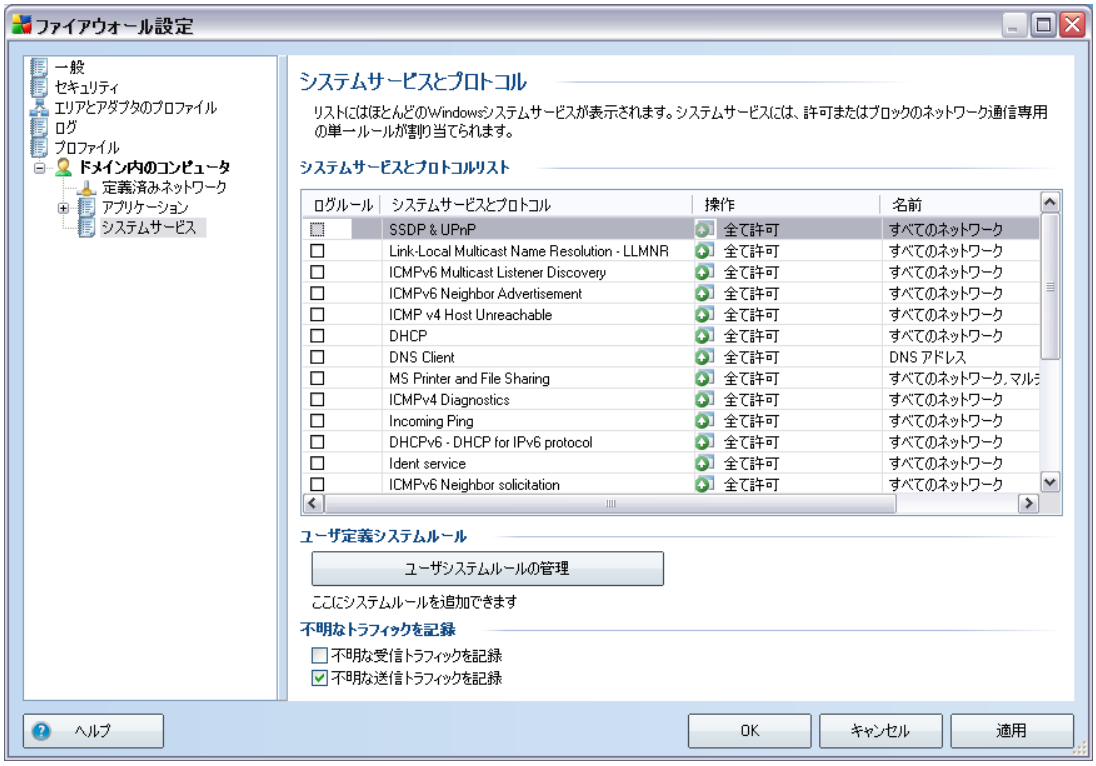
選択します。

- ***高度な設定*** **-** このオプションを選択すると、ダイアログ下部で詳細なルールセットを編集することができます。
- ***全て許可*** - アプリケーションのすべての通信が許可されます。
- ***許可*** - アプリケーションは、安全なネットワーク上での通信のみ許可されます。 *例えば、保護された会社のネットワークへの通信は許可されますが、インターネットへの通信はブロックされます。*)。安全なネットワークについての概要と説明は、 ***ネットワーク***ダイアログを参照してください。
- ***確認*** **-** アプリケーションがネットワーク上で通信する場合、通信の許可、またはブロックを選択する画面が表示されます。
- ***ブロック*** - アプリケーションのすべての通信はブロックされます。

- ***ログに記録する*** - このオプションにチェックを付けると、このルールが適用されているアプリケーションに関するすべての ***ファイアウォール*** アクションが記録されます。各ログエントリは ***ログ***ダイアログに表示されます。

10.5.4. 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 ダイアログは、ネットワーク上で通信するシステムサービスとプロトコルの概要を開きます。リストの下に、2つのオプションがあります。 すべての不明なトラフィックの ログを取る場合、チェックを付けます *(受信、送信)*。

コントロールボタン

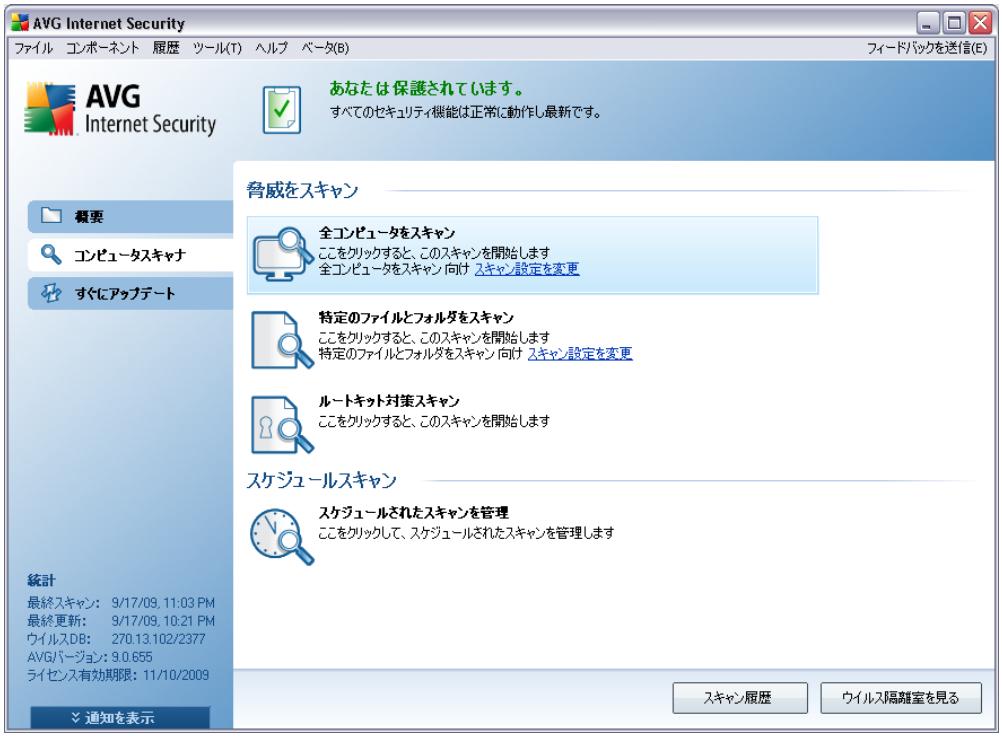
- ***追加/編集*** - 両方のボタンはシステムパラメータを編集するためのダイアログを開きます。[***追加***] ボタンは、空のダイアログを基本モード（ *高度な設定セクションはありません。このセクションはアプリケーションアクションの高度な設定を選択することで開かれます* ）で開きます。[***編集***] ボタンは、選択されたシステムサービスに関する既に入力済のデータを表示します。

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。

11. AVGスキャン

スキャンは **AVG 9 Anti-Virus plus Firewall** 重要な機能です。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。

11.1. スキャンインターフェース



AVG スキャンインターフェースには ***コンピュータスキャナ*** クイックリンクからアクセスすることができます。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***
- スキャンスケジュール セクション - ここでは必要に応じて、新しいスキャンを作成することができます。

コントロールボタン

スキャンインターフェースで利用できるコントロールボタンは以下の通りです。

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

11.2. 定義済みスキャン

AVG 9 Anti-Virus plus Firewall のメイン機能の1つはオンデマンドのスキャンです。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。

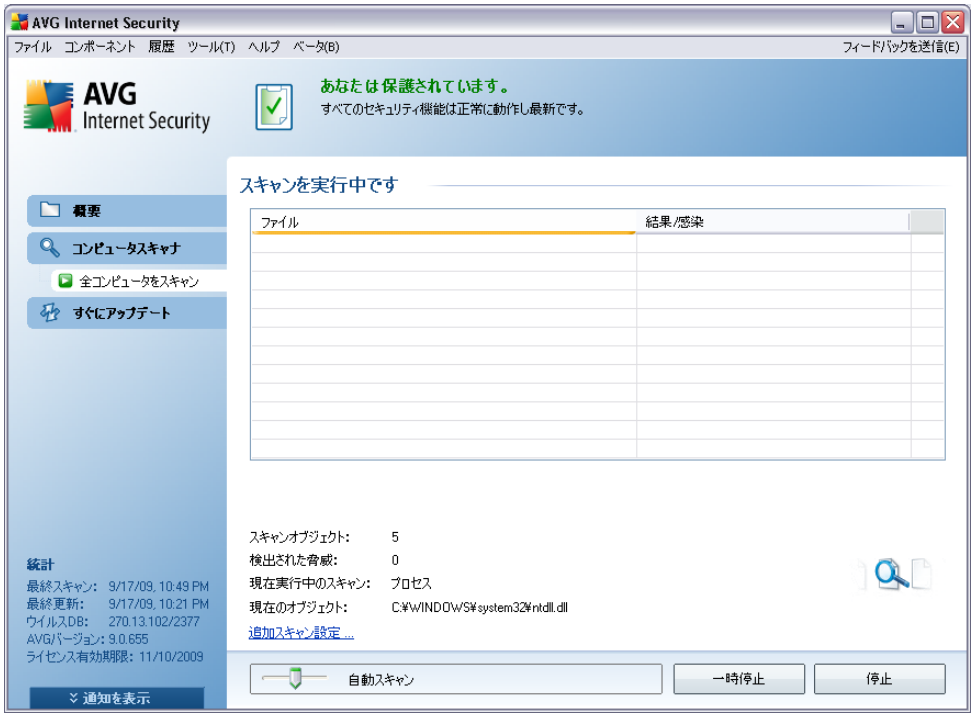
AVG 9 Anti-Virus plus Firewall では、2種類の定義済みスキャンが表示されます。

11.2.1. 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。。

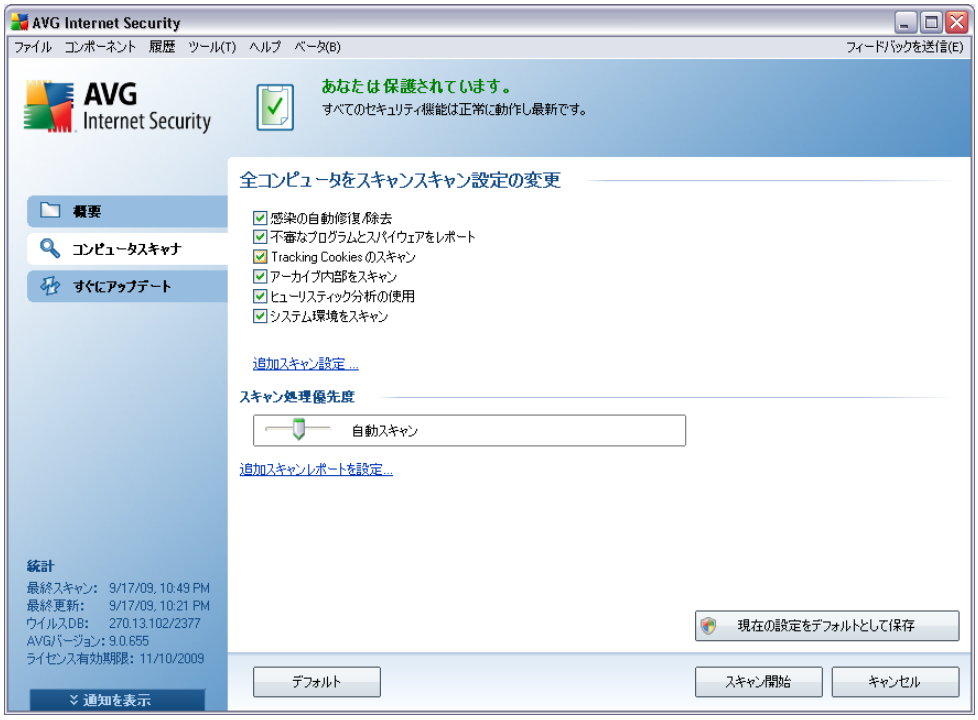
スキャン実行

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。



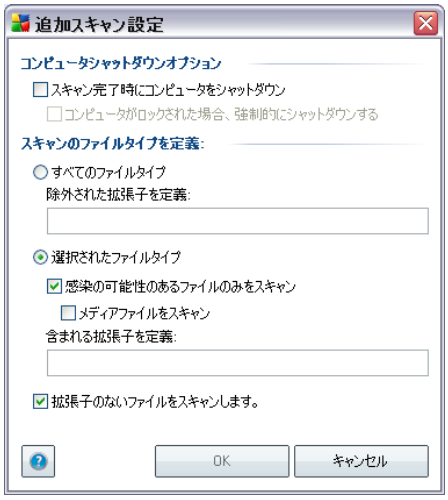
スキャン設定編集

完全コンピュータスキャンのデフォルト設定 ***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***）を選択すると、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するためのオプション（ ***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。

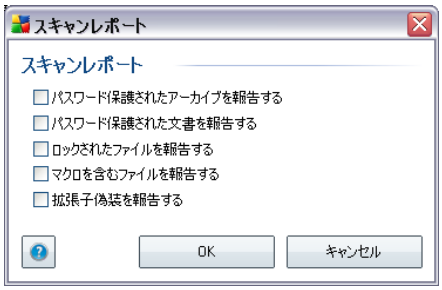
  - ***すべてのファイルタイプと*** スキャン対象ではないファイル拡張子をカンマで区切ったリストを入力することで、スキャンからの除外を定義できます。あるいは、

  - ***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、ウイ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、新規作成する場合の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。*

11.2.2. 特定のファイルとフォルダのスキャン

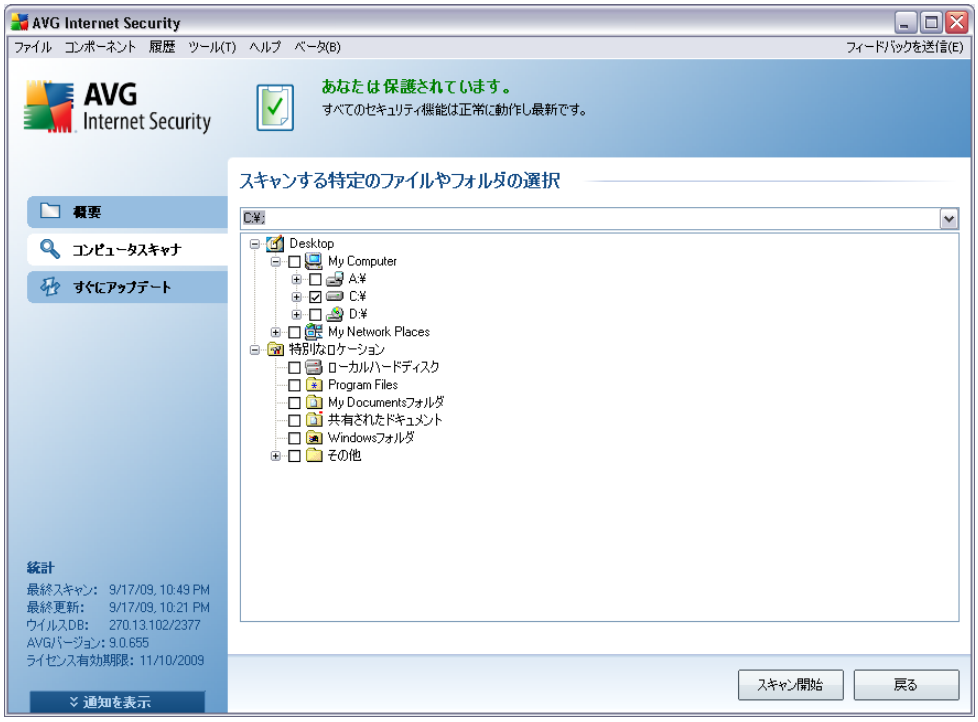
特定のファイルやフォルダをスキャン - 選択場所のみをスキャンします（*選択されたフォルダ、ハードディスク、フロッピーディスク、CD等*）. ウイルス検出、処置等のスキャン進捗 ***は、完全コンピュータスキャンと同じです。検出ウイルスは修復、またはウイルス隔離室に移動されます。*** 特定のファイルやフォルダをスキャンは、ユーザー独自のスキャン設定とスケジュールのために使用されます。

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。

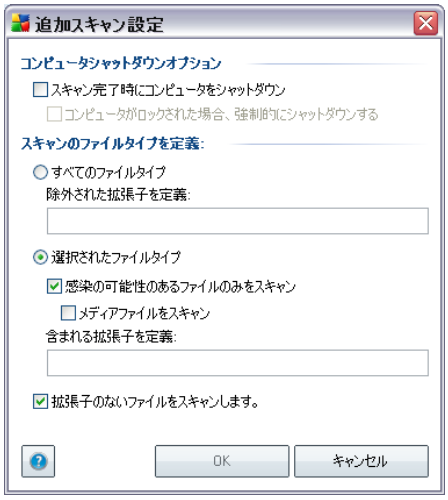
スキャンを実行するには、 ***スキャン開始*** ボタンを押します。スキャンプロセス自体は基本的に 完全コンピュータスキャンと同一です。



スキャン設定編集

特定のファイルとフォルダをスキャンのデフォルト設定 ***を編集することができます*** 。***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***）を選択すると、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するためのオプション（ ***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。

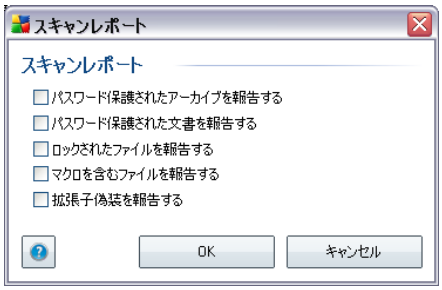
  - ***すべてのファイルタイプと*** スキャン対象ではないファイル拡張子をカンマで区切ったリストを入力することで、スキャンからの除外を定義できます。あるいは、

  - ***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、ウイ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。

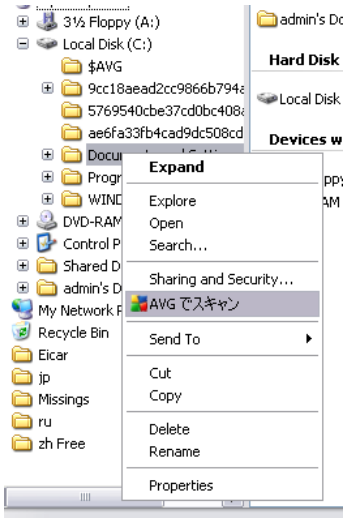
- ***追加スキャンレポートを設定*** - このリンクは、***スキャンレポート***ダイアログを開きます。このダイアログでは、レポートされる検出の種類を選択することができます。



警告：*これらのスキャン設定は、新規作成する場合の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)。*

11.3. シェル拡張スキャン

全コンピュータのスキャン、特定エリアのスキャンで実行されるスキャンのほかにも、 **AVG 9 Anti-Virus plus Firewall** は Windows Explorer 環境での特定オブジェクトを直接キャンすることができます。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。

11.4. コマンドラインスキャン

AVG 9 Anti-Virus plus Firewall には、コマンドラインからスキャンを実行する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、値はカンマ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、プロセスを停止することができます。

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ザー***ダイアログでは、便利なグラフィックインターフェースでは大部分のスキャンパラメータを指定できます。

このダイアログはWindowsセーフモードでのみ利用可能です。このダイアログの詳細説明については、ダイアログから直接開かれるヘルプファイルを参照してください。

11.4.1. CMDスキャンパラメータ

以下は、コマンドラインスキャンで利用可能なすべてのパラメータです。

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

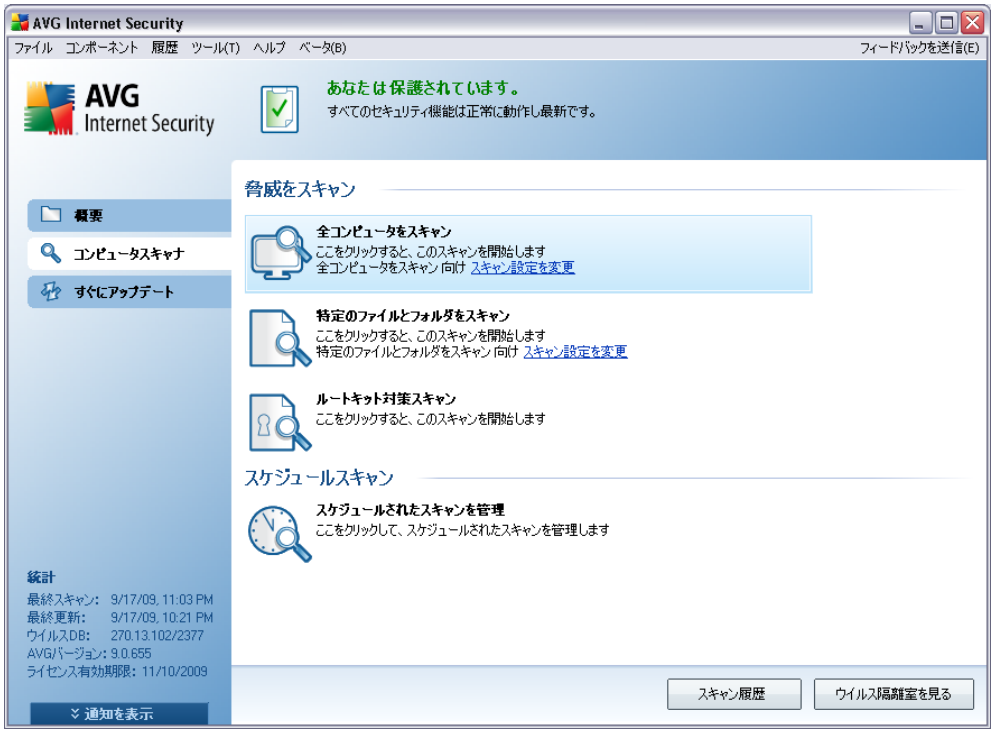
- ***/NOBREAK*** CTRL-BREAKで中断しない
- ***/BOOT*** MBR/BOOT チェックを有効化
- ***/PROC*** アクティブプロセスをスキャンする
- ***/PUP*** 「不審なプログラム」を報告する
- ***/REG*** レジストリをスキャンする
- ***/COO*** cookieをスキャンする
- ***/?*** このトピックに関するヘルプを表示
- ***/HELP*** このトピックに関するヘルプを表示
- ***/PRIORITY*** スキャン優先度を設定/Low, Auto, High/（高度な設定/スキャンを参照）
- ***/SHUTDOWN*** スキャン完了時にコンピュータをシャットダウン
- ***/FORCESHUTDOWN*** スキャン完了時にコンピュータを強制シャットダウン
- ***/ADS*** Alternate Data Streams をスキャン(NTFSのみ)

11.5. スキャンスケジュール

AVG 9 Anti-Virus plus Firewall 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。これによって、コンピュータが感染から保護されていることを保証でき、スキャンをいつ実行するかを考慮する必要はなくなります。

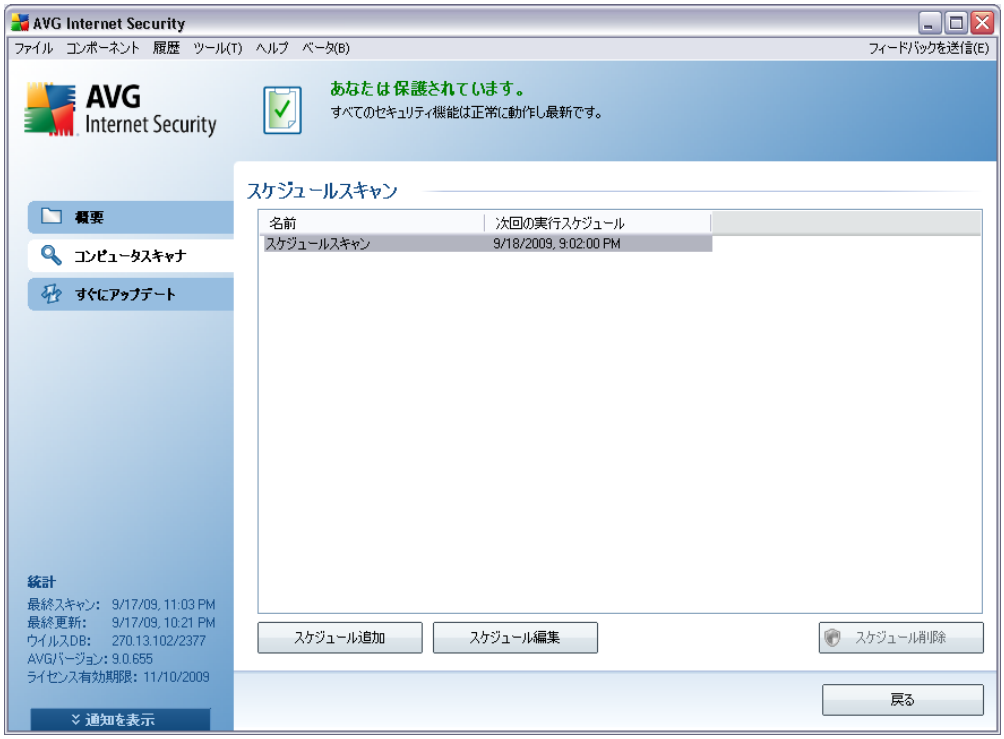
全コンピュータをスキャン を少なくとも週に1度定期的に実行して下さい。ただし、可能な場合は、コンピュータのスキャンを毎日行ってください。デフォルトのスキャンスケジュールはこのように設定されています。 コンピュータが常にオンとなっている場合、作業時間外にスキャンを実行するよう設定することができます 。コンピュータがオフになり、スケジュールが実行されなかった場合、スケジュールは コンピュータの起動時にスキャンを実行するように設定してください

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。

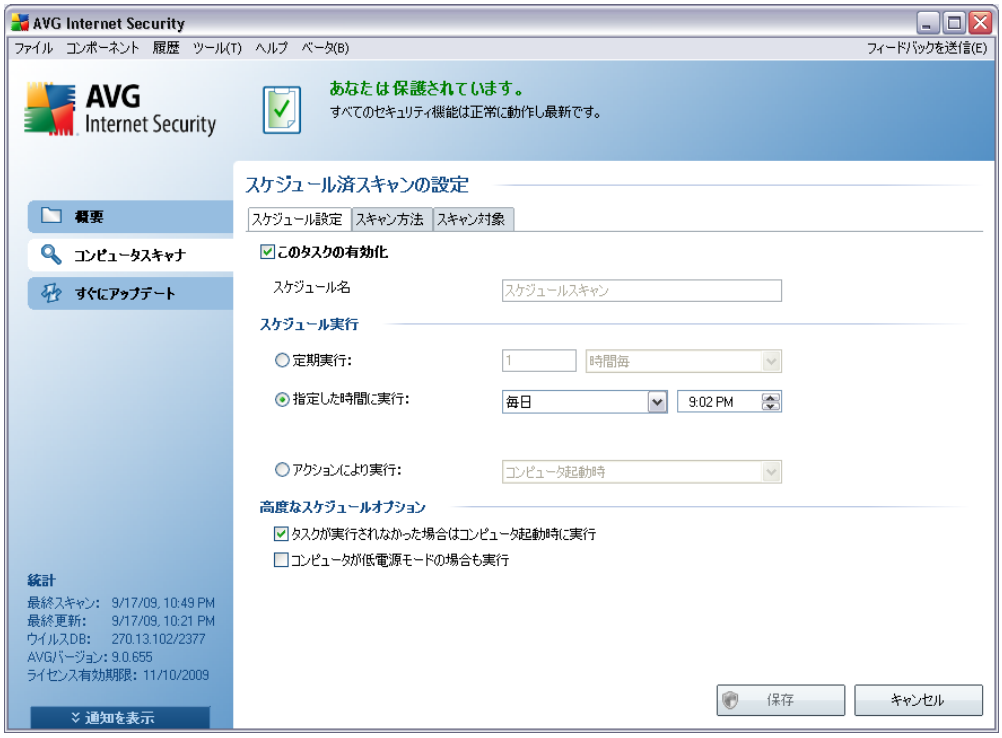


次のコントロールボタンを使用して、スキャンの編集および追加ができます。

- ***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

11.5.1. 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」という名前を付けるの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。新規に設定するスキャンスケジュールは* *特定のファイルとフォルダをスキャン* *と同様のものとなります。*

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。

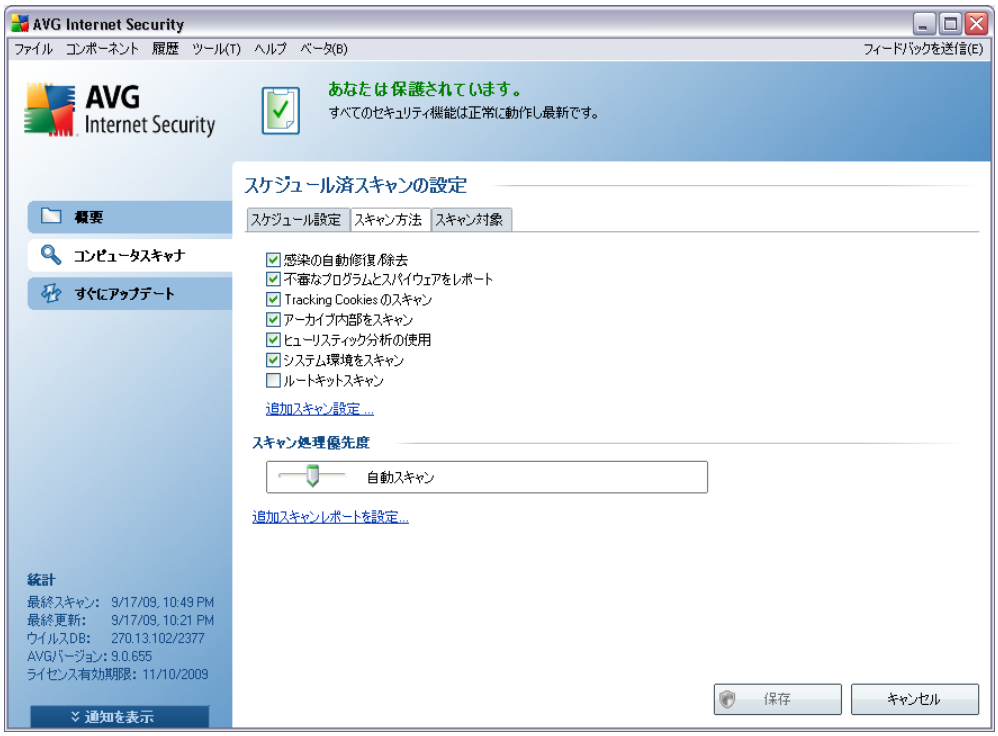
- ***スケジュール実行*** - スキャン起動時間を指定します。タイミングは、 ***定期実行***、***指定した時間に実行***、***アクションにより実行*** のいずれかによって定義することができます。
- ***高度なスケジュールオプション*** - このセクションでは、コンピュータが低電源モードあるいは完全に電源オフになっている場合に、スキャンが実行される条件を定義します。

スケジュール済の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。

11.5.2. スキャン方法



スキャン方法 タブには、任意でオン/オフ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。

- ***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脅威をレポート*** - *既定ではオンになっています*) このパラメータは、***ウィルス対策*** 機能を制御し、不審なプログラム (*スパイウェアやアドウェアとして実行される実行可能ファイル*) を検出できるようにします。これらはブロックまたは除去されます。

- ***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*)

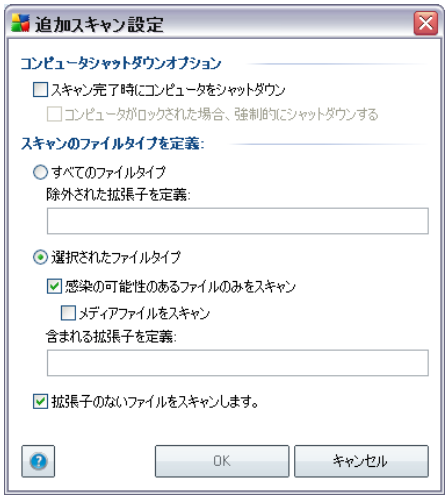
- ***アーカイブ内をスキャン*** - (*デフォルトではオン*) このパラメータは、ZIPやRAR等のアーカイブ形式で圧縮されている場合でも、すべてのファイルがスキャンによりチェックされるように定義します。

- ***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。

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。



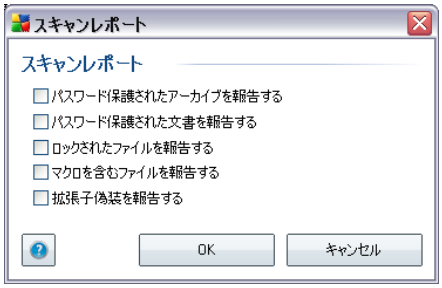
  - ***コンピュータのシャットダウンオプション*** - 実行中のスキャンプロセスが終了した時点で自動的にコンピュータをシャットダウンするかどうかを決定します。このオプション (***スキャン完了時にコン***

ピュータをシャットダウン）を選択すると、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するためのオプション（***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*** 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。あるいは、
  - ***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。



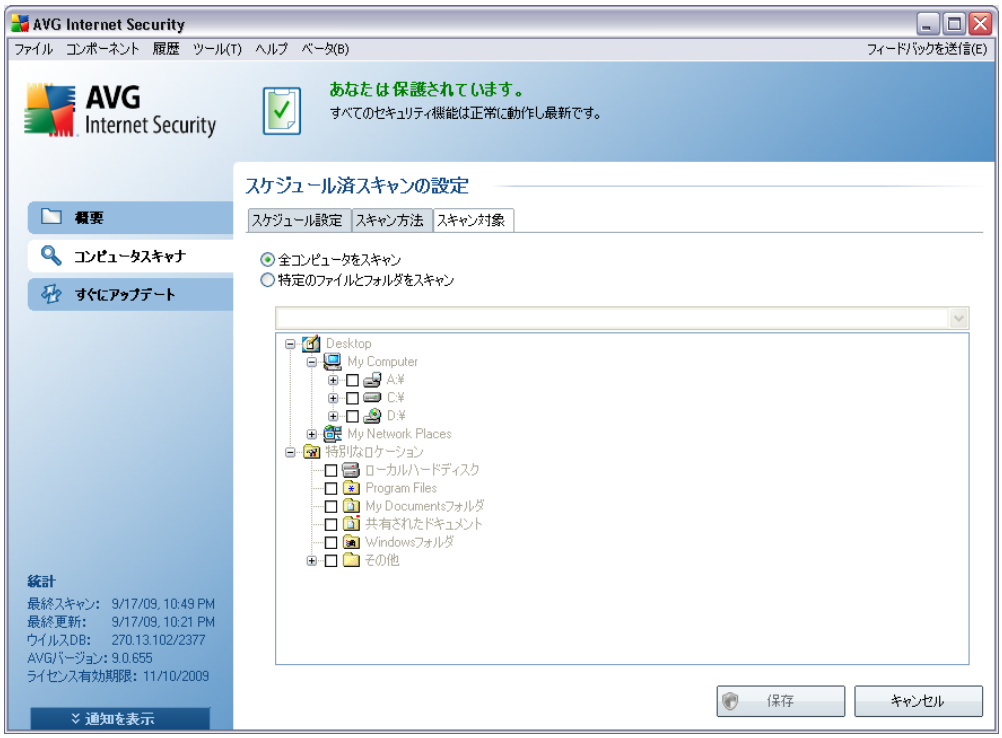
注意：*デフォルトでは、スキャンには最適なパフォーマンスで実行されるように設定されています。このスキャンの設定を変更する合理的な理由がない場合は、あらかじめ定義された設定を維持することを強く推奨します。設定変更は経験のあるユーザーが行ってください。これ以外のスキャンの設定オプションについては、* ***ファイル/高度な設定*** *システムメニューアイテム* ***からアクセスできる*** *高度な設定ダイアログを参照してください。*

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。

11.5.3. 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。

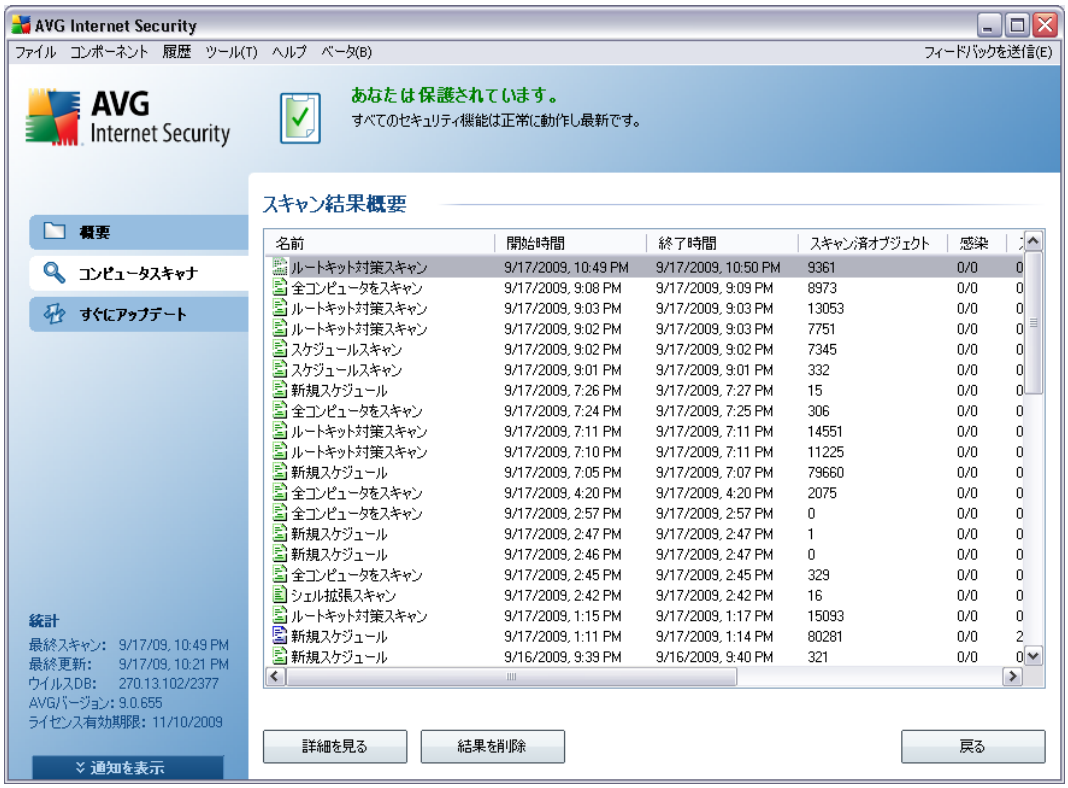
スケジュール済スキャンダイアログのコントロールボタン

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。

11.6. スキャン結果概要



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

- ***名前*** - 予め定義されたスキャンの名前 、または自分で作成したスキャンスケジュール 名です。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検出され、感染したオブジェクトが自動的に除去されたことを示します。

- 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
- ***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。

- ***詳細を見る*** - このボタンは、スキャンが選択された場合にのみ有効化されます。これを押すと、***スキャン結果*** ダイアログに切り替わり、選択されたスキャンの詳細データを見ることができます。
- ***結果を削除*** - このボタンはスキャンが選択された場合にのみ有効化されます。これを押すと、スキャン結果概要から選択されたアイテムが削除されます。
- ***戻る*** - AVGスキャンインターフェース のデフォルトダイアログに切り替わります。

11.7. スキャン結果詳細

スキャン結果概要 ダイアログで、特定のスキャンが選択された場合、 ***詳細を表示*** ボタンをクリックすると、 ***スキャン結果*** ダイアログが表示されます。このダイアログでは、選択されたスキャン結果に関する詳細なデータが表示されます。

このダイアログはさらにいくつかのタブに分けられます。

- ***結果概要*** - このタブは常に表示され、スキャン進捗を示す統計データが表示されます。
- ***感染*** - このタブは、スキャン実行中に ウイルス感染 が検出された場合にのみ表示されます。
- ***スパイウェア*** - このタブは、スキャン実行中に スパイウェア が検出された場合にのみ表示されます。
- ***警告*** - このタブは、スキャン実行中にスキャン不可能なオブジェク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。

11.7.1. 結果概要タブ

スキャン結果 タブには、以下の情報に関する詳細な統計が表示されます。

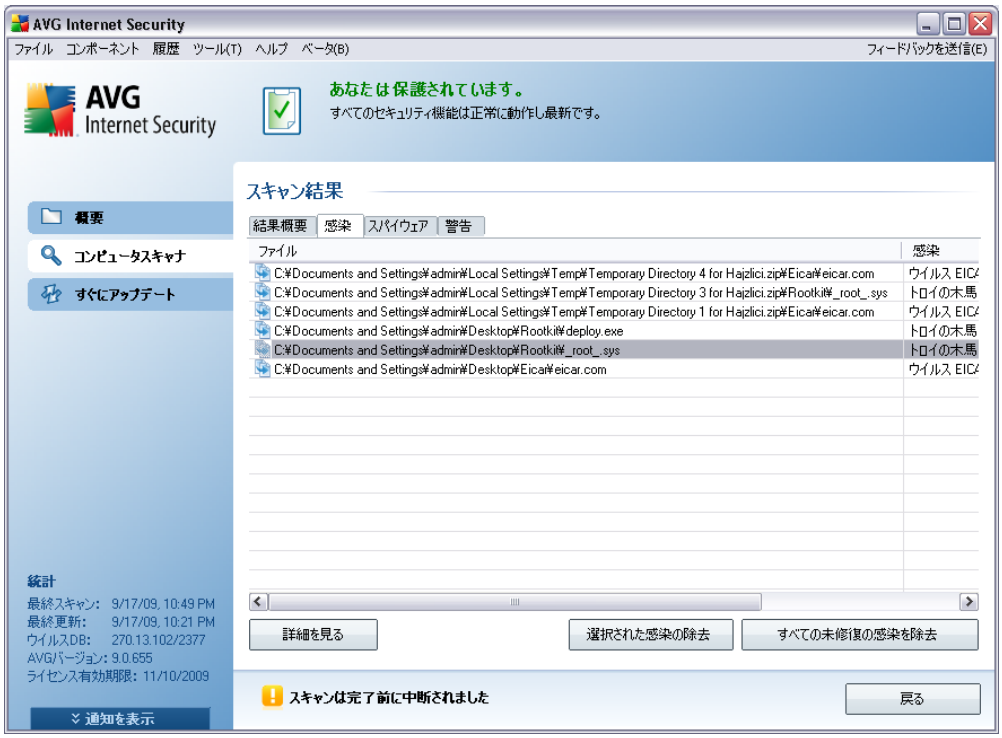
- 検出されたウイルス感染 / スパイウェア
- 除去されたウイルス感染 / スパイウェア
- 除去あまたは修復不可能なウイルス感染 / スパイウェア数

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。

11.7.2. 感染タブ



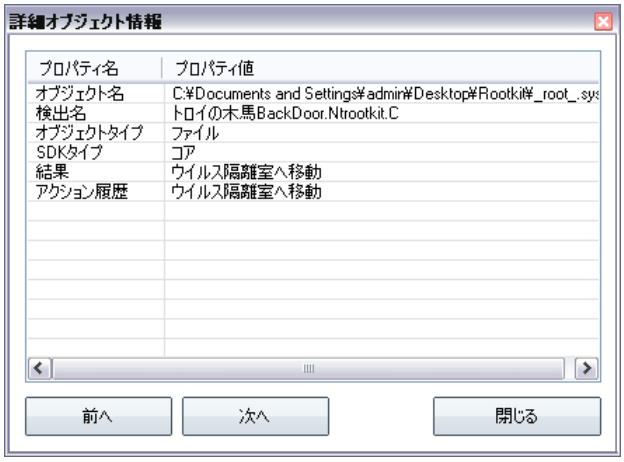
感染 タブは、スキャン中にウイルス感染が検出された場合、 ***スキャン結果*** ダイアログでのみ表示されます。このタブは3つのセクションに分かれ、以下の情報が表示されます。

- ***ファイル*** - 感染オブジェクトの元の場所へのフルパス
- ***感染*** - 検出されたウイルス名（*ウイルスの詳細は、オンラインの ウイルスエンサイクロペディア を参照してください*）
- ***結果*** - スキャン中に検出された感染オブジェクトの現在のステータス
    - ***感染*** - 感染オブジェクトが検出され、元の場所に存在します。（ *例えば、自動修復オプションを特定のスキャン設定でオフにしている場合* ）
    - ***修復*** - 感染オブジェクトは自動修復され、元の場所に存在しますす。
    - ***ウイルス隔離室に移動*** - 感染オブジェクトは ***ウイルス隔離室*** に移動されました。
    - ***削除*** - 感染オブジェクトは削除されました。
    - ***PUP例外を追加*** - 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。

11.7.3. スパイウェアタブ

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

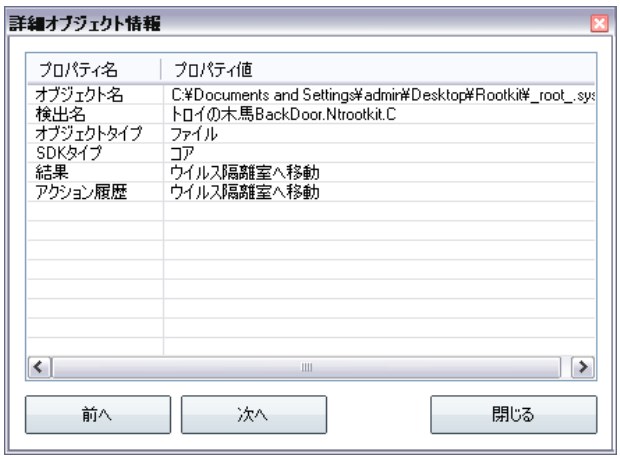
- ***ファイル*** - 感染オブジェクトの元の場所へのフルパス
- ***感染*** - 検出されたウイルス名（*ウイルスの詳細は、オンラインの* ***ウイルスエンサイクロペディア*** *を参照してください*）
- ***結果*** - スキャン中に検出された感染オブジェクトの現在のステータス
  - ***感染*** - 感染オブジェクトが検出され、元の場所に存在します。例えば、 自動修復オプションを特定のスキャン設定でオフにしている場合）
  - ***修復*** - 感染オブジェクトは自動修復され、元の場所に存在しますす。
  - ***ウイルス隔離室に移動*** - 感染オブジェクトは ***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*** - 感染オブジェクトは除去できません。完全に除去するには、コンピュータの再起動がひつようです

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。

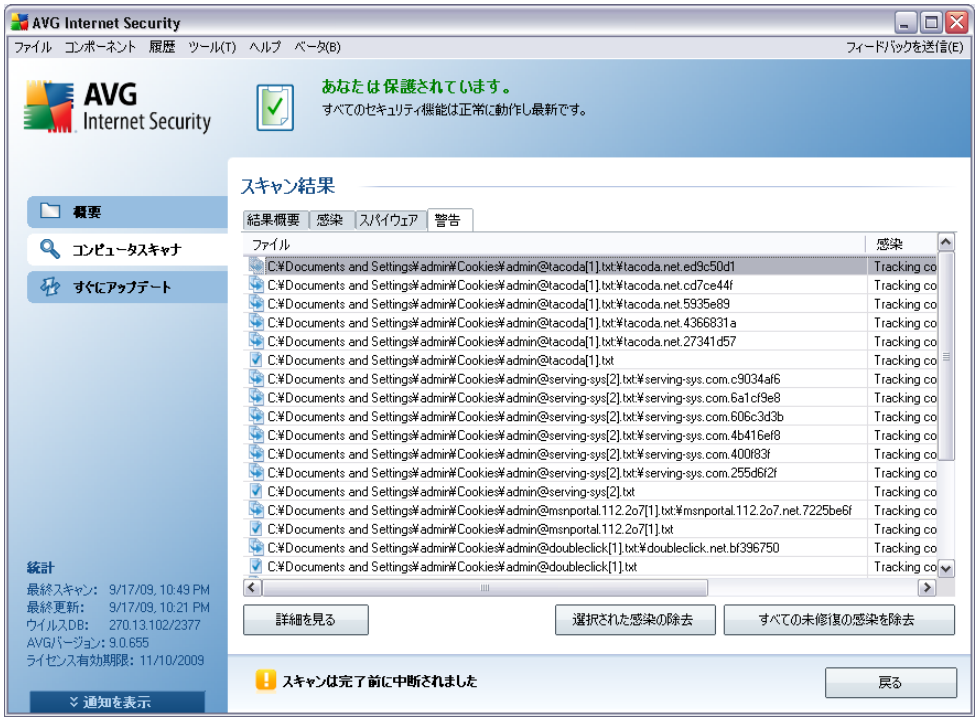
- ***選択された感染を除去*** - このボタンを使用して、選択された検出を ***ウイルス隔離室に移動します。***
- ***すべての未修復の感染を削除*** - このボタンはすべての修復不可能な検出や ***ウイルス隔離室に移***

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。

11.7.4. 警告タブ

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

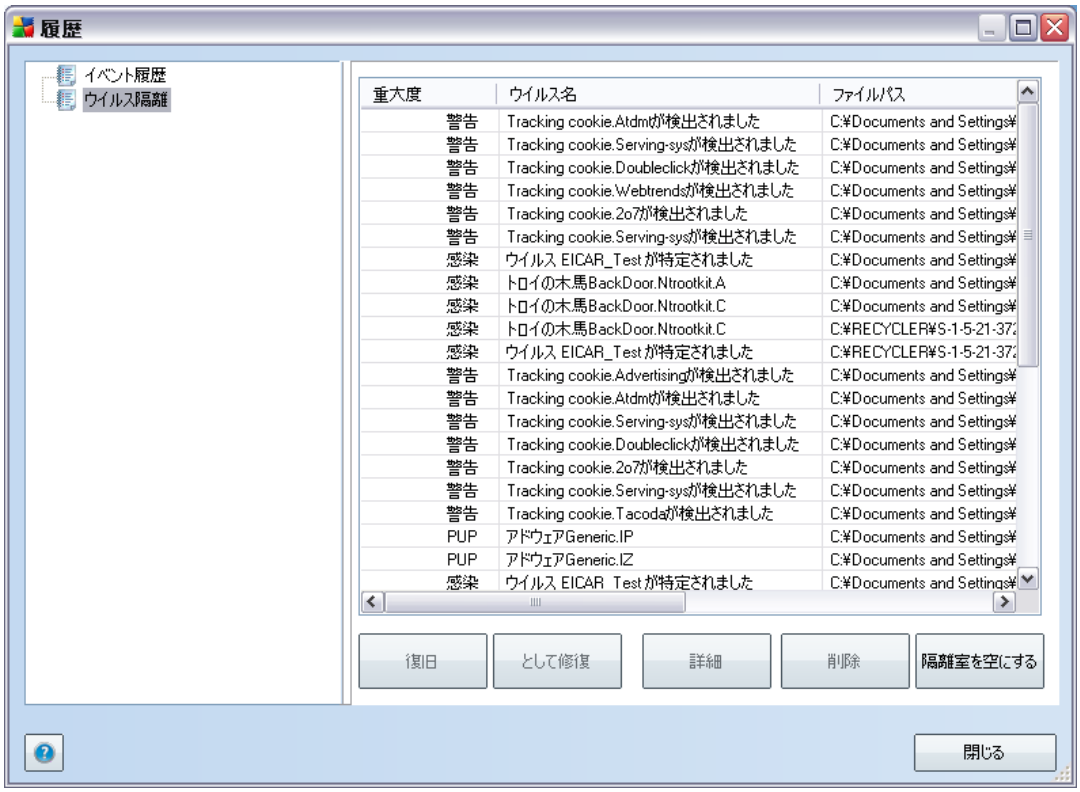
11.7.5. 情報タブ

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*）。

11.8. ウイルス隔離室



ウイルス隔離室 は、AVGスキャン中に検出された疑わしい、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 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。

- ***重要度*** - 好ましくない（■□□□）から非常に危険（■■■■）までの 4 段階方式で各検出の重要度をグラフィカルに示します。
- ***感染タイプ***- 感染レベルに基づいて、検出タイプを区別します（ *すべてのオブジェクトは感染、または感染の可能性があります。* ）。
- ***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。
- ***削除*** - 感染ファイルを ***ウイルス隔離室*** から完全に削除します。
- ***空にする*** - 全ての ***ウイルス隔離室*** 内のファイルを 削除します。

12. 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時間毎に確認すると、AVGウィルスベースがその日中最新の状態に保たれていることを保証します。

12.1. アップデートレベル

AVGでは2つのアップデートレベルを選択できます。

- ***定義アップデート***には信頼できるウィルス対策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ず、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、すぐに適用されるべきです。
- ***プログラムアップデート***には、様々なプログラム変更、修正、改良が含まれます。

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。

12.2. アップデートタイプ

2種類のアップデートを区別できます。

- ***オンデマンドアップデート*** は、必要に応じて実行可能な即時アップデートです。
- ***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。

12.3. アップデートプロセス

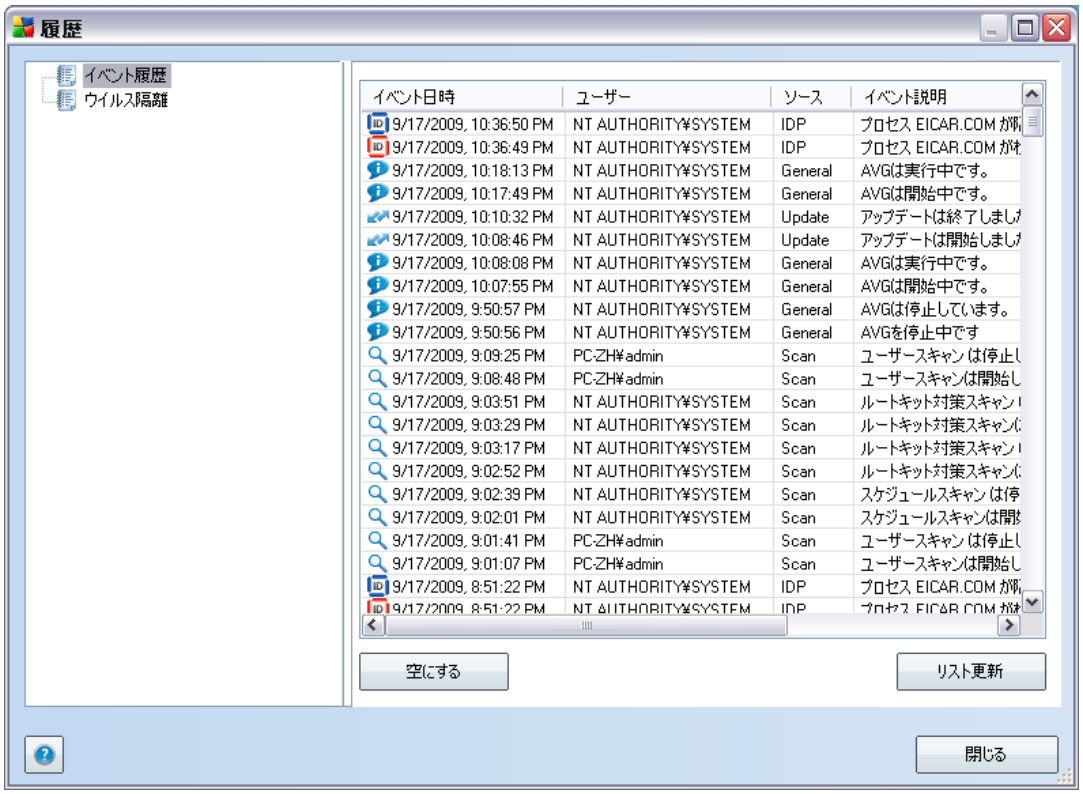
すぐにアップデート クイックリンクによって、アップデートプロセスすぐに実行することができます。このリンクは、AVGユーザーインターフェース ダイアログからいつでも使用可能です。ただし、 アップデートマネージャ コンポーネントのアップデートスケジュール編集で説明されているように、定期的にアップデートを実行することが強く推奨されます。

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***インターフェースが表示されます。ここでは、グラフィカルな表示や関連統計パラメータ（ *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}* ）とともに処理状況を確認することができます。

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。このオプションにはスタート/ すべてのプログラム/ アクセサリ/ システムツール/ システムの復元からアク*

セスできます。経験者ユーザーのみに推奨されます。

13. 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 Anti-Virus plus Firewall** 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

14. 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。

この方法でも解決しない場合は、メールでテクニカルサポート部門に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。