AVG 9.0 File Server

ユーザーマニュアル

ドキュメント改訂 90.3 (30.11.2009)

コンテンツ

1. はじめに

このユーザーマニュアルでは、**AVG 9.0 File Server**に関する包括的なドキュメントを提供します。

AVG 9.0 File Serverのご購入ありがとうございました。

AVG 9.0 File Server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 9.0 File Server**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 9.0 File Server**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. インストール要件

2.1. 対応オペレーションシステム

AVG 9.0 File Serverは次のオペレーティングシステムのワークステーションを保護を目的としています。

- Windows 2000 Server
- Windows 2003 Server および Windows 2003 Server x64 Edition
- Windows 2008 Server および Windows 2008 Server x64 Edition

（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. ハードウェア要件

AVG 9.0 File Serverの最低ハードウェア要件:

- Intel Pentium CPU 1,5 GHz
- ハードディスク空き容量 470MB以上（インストールのため）
- 512 MB の RAM メモリ

AVG 9.0 File Serverの推奨ハードウェア要件:

- Intel Pentium CPU 1,8 GHz
- ハードディスク空き容量 600MB以上（インストールのため）
- 512 MB の RAM メモリ

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 9.0 File Server。

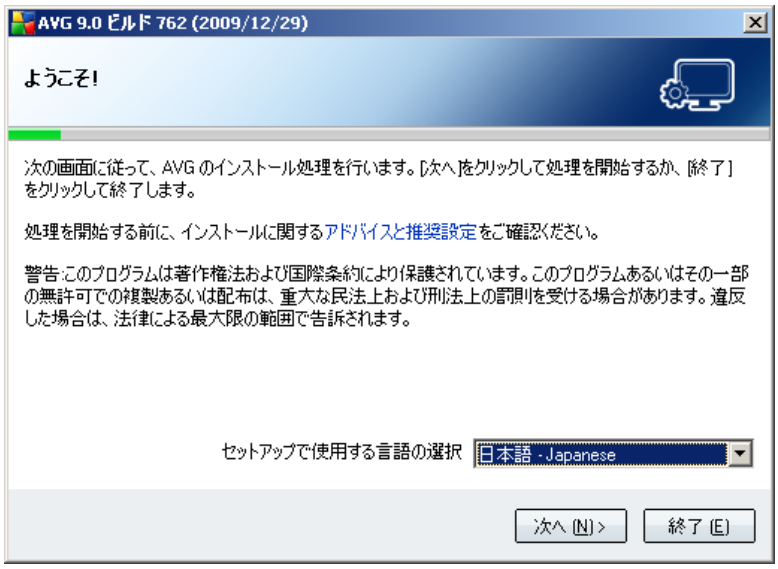
インストールプロセス中に、ライセンス番号/セールス番号が必要となります。インストールを開始する前にライセンス番号/セールス番号を準備してください。セールス番号はCDのパッケージ、購入時のメール中等に記載されています。AVGをオンラインで購入した場合、ライセンス番号/セールス番号はメールで送信されます。

4. AVGインストールプロセス

AVG 9.0 File Server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。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。

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。

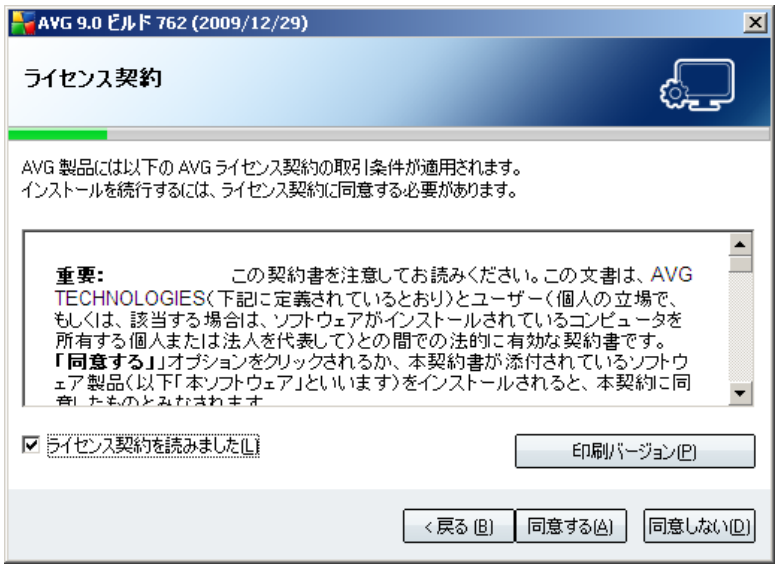
4.1. インストールの実行



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。

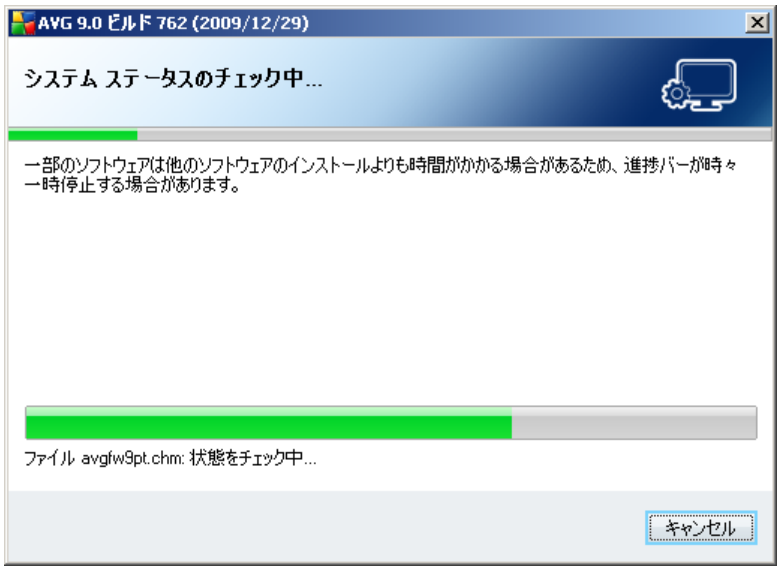
4.2. ライセンス契約



*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。

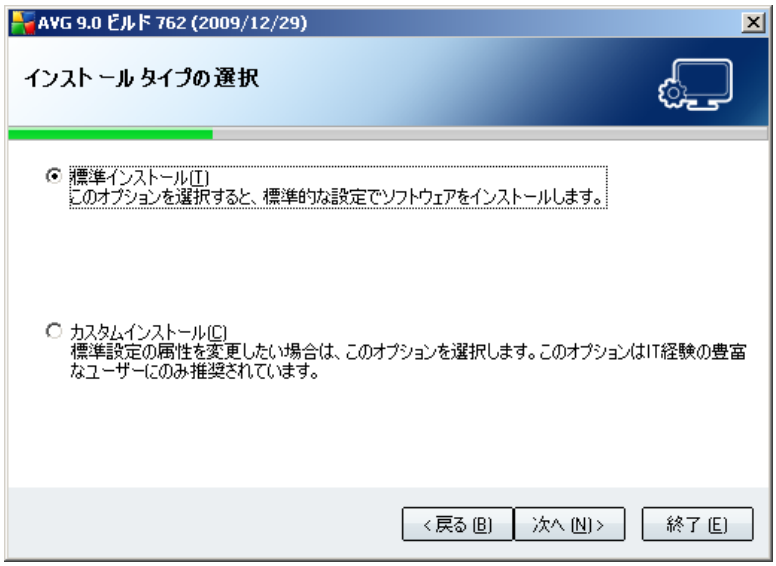
ライセンス契約に同意しない場合、*同意しない*ボタンを押してください。インストールプロセスがすぐに中断されます。

4.3. 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。

4.4. インストールタイプの選択



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

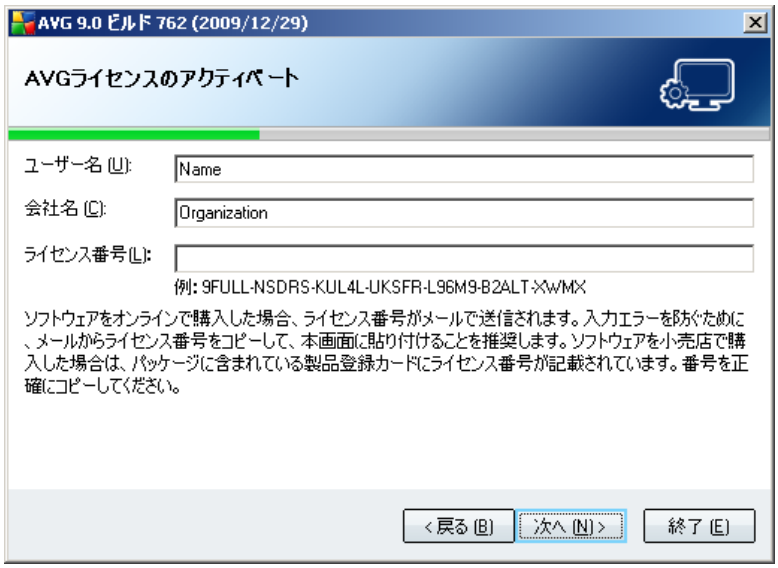
ほとんどのユーザーには、*標準インストール*を選択し、AVGを自動モードでインストールすることが強く推奨されます。この設定は、最適なリソース消費と最大のセキュリティを提供します。将来的に設定の変更の必要が生じた場合、常にAVGアプリケーションで直接変更することができます。

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

4.5. 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。

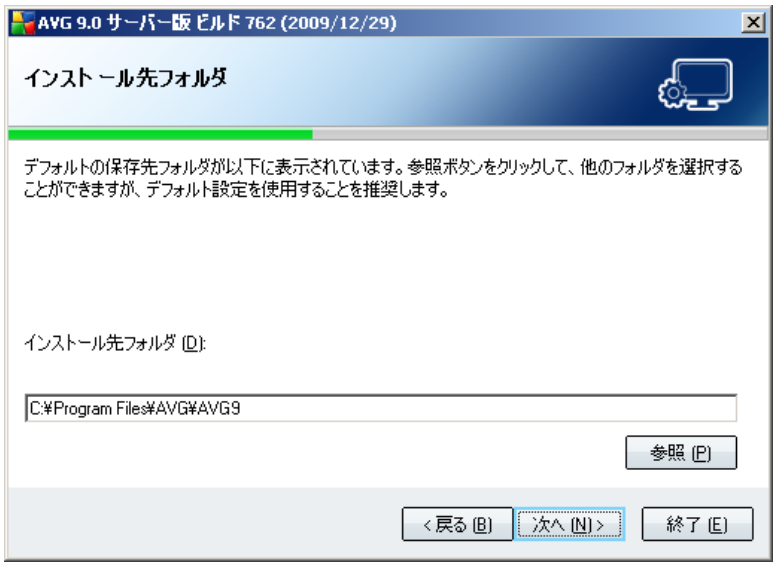
次に、ライセンス番号/セールス番号を*ライセンス番号*テキストフィールドに入力します。セールス番号は**AVG 9.0 File Server**の箱の CD パッケージに記載されています。ライセンス番号は**AVG 9.0 File Server**をオンラインで購入後に受信する確認メールに記載されています。この番号を記載通り正確に入力してください。デジタル形式のライセンス番号が利用できる（*メールで*）場合は、コピーとペーストを使用して、それを入力することを推奨します。



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 のインストール*] 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。

4.6. カスタムインストール - インストール先フォルダ

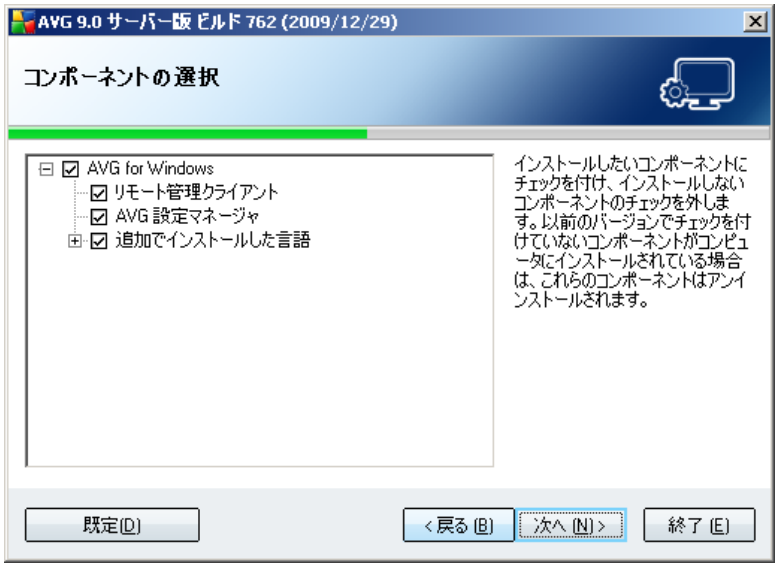


[*インストール先フォルダ*] ダイアログでは、がインストールされる場所を指定します。**AVG 9.0 File Server**デフォルトでは、AVGは、Cドライブのprogram filesフォルダにインストールされます。フォルダがまだ存在しない場合、新しいダイアログが開き、今すぐ AVG によってこのフォルダを作成してもよいかどうかを確認します。

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

*次へ*ボタンを押して確認します。

4.7. 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 9.0 File Server**デフォルト設定が適当でない場合、特定のコンポーネントを削除/追加することができます。

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

- *言語選択*

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

- *メールスキャナプラグイン*

  [*メールスキャナ*] アイテムをクリックして開き、メールのセキュリティを保証するためにインストールするプラグインを決定します。既定では、***Plugin for Microsoft Outlook*** がインストールされます。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

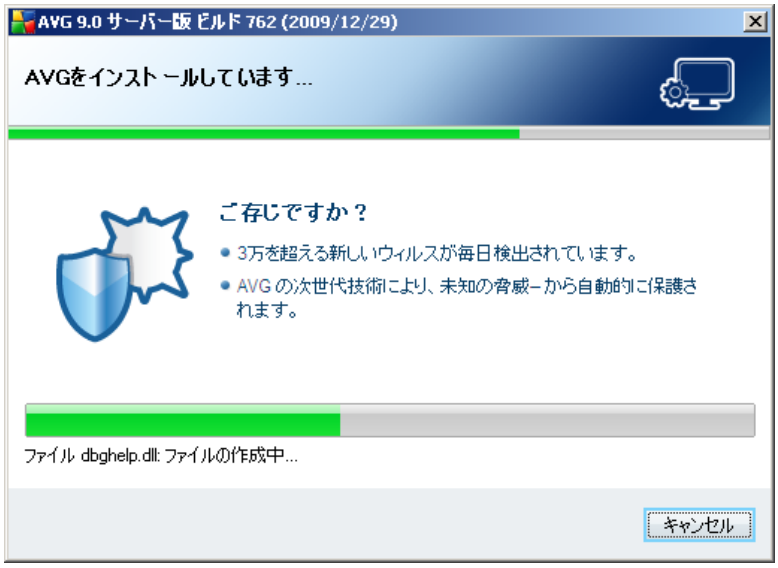
- *リモート管理*

  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。

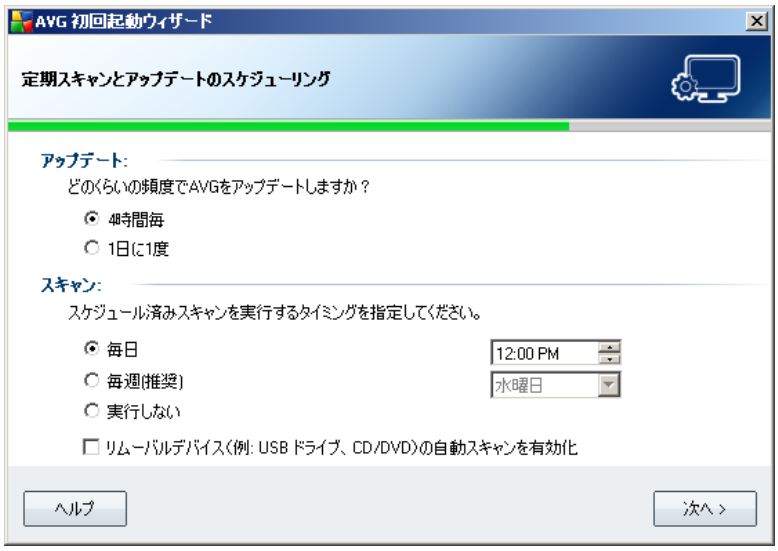
4.8. AVGのインストール

[*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。

4.9. 定期スキャンとアップデートのスケジューリング



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

4.10. AVG 保護設定は完了しています

AVG 9.0 File Serverは設定されました。

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

最後に、[*完了*] ボタンをクリックします。

5. インストール後

5.1. 製品登録

AVG 9.0 File Server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（*画面上の指示に従ってください*）。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。

5.2. 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。*

5.3. 全コンピュータをスキャン

AVG 9.0 File Server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。

5.4. Eicarテスト

AVG 9.0 File Server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 テストを実行できます。

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

eicar.comファイルをダウンロードし、それをローカルディスクに保存します。テストファイルのダウンロードを確認後すぐに、*常駐シールド*が警告とともにそれに反応します。この*常駐シールド*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。

5.5. 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 9.0 File Server**では、すべてのコンポーネントと機能が最適なパフォーマンスで動作するよう設定されています。

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

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

6. AVG ユーザーインターフェース

AVG 9.0 File Serverはメインウィンドウで開きます。

メインウィンドウは複数のセクションに分けられます。

- *システムメニュー（ウィンドウ上のシステムライン）*は標準ナビゲーションであり、すべてのAVGコンポーネント、サービス、機能にアクセスすることができます。 - 詳細 >>
- *セキュリティステータス情報（ウィンドウ上部のセクション）*には、現在のAVGプログラムのステータスが表示されます。- 詳細 >>
- *クイックリンク（ウィンドウの左のセクション）*では、最も重要で最も頻繁に使用されるAVGタスクにすぐにアクセスすることができます。 - 詳細 >>
- *コンポーネント概要（ウィンドウ中央部）*は、インストールされたAVGコン

ポーネントの概要が表示されます。 - 詳細 >>

- *統計（ウィンドウ左下部）*では、プログラムに関する統計データが表示されます。-詳細 >>
- *システムトレイアイコン（モニター右下端のシステムトレイ）*では、現在のAVGステータスが表示されます。 -詳細 >>

6.1. 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 9.0 File Server**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。

6.1.1. ファイル

- *終了* - **AVG 9.0 File Server**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。

6.1.2. コンポーネント

システムメニューの*コンポーネント*には、インストールされたすべてのAVGコンポーネントへのリンクが含まれ、選択すると各デフォルトページが表示されます。

- *システム概要* - インストールされたすべてのコンポーネントとそのステータスの概要を表示します。
- *ウイルス対策*- *ウイルス対策*コンポーネントのデフォルトページを表示します。
- *ルートキット対策*- *ルートキット対策*コンポーネントのデフォルトページを表示します。
- *スパイウェア対策*- *スパイウェア対策*コンポーネントのデフォルトページを表示します。
- *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。
- *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。

6.1.3. 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。*
- *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 9.0 File Server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。

6.1.4. 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 9.0 File Server**
- *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 9.0 File Server**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。

6.1.5. ヘルプ

- *目次* - AVGヘルプファイルを開きます。
- *オンラインヘルプ* - AVG Free Webサイトのカスタマーサポートセンターページを開きます（http://www.avg.com）。
- ***AVG Web*** - AVG ウェブサイト（http://www.avg.com）を開きます。
- *ウイルスと脅威について* - オンラインの*ウイルスエンサイクロペディア*を開きます。ここでは、特定されたウイルスに関する詳細情報を検索することができます。
- *再アクティベート* - *インストールプロセス*の [*AVG のパーソナライズ*] ダイアログで入力したデータとともに、[AVG のアクティベート] ダイアログが表示されます。このダイアログ内では、ライセンス番号を入力し、セールス番号（*AVGをインストールした際の番号*）を置き換えるか、古いライセンス番号（*例えば、新しいAVG製品にアップグレードした場合*）を置き換えることができます。
- *今すぐ登録* - AVG ウェブサイト（http://www.avg.com）の登録ページに接続します。登録データを入力してください。AVG製品を登録したお客様のみが無料テクニカルサポートを受けることができます。
- *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。

6.2. 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 9.0 File Server**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。

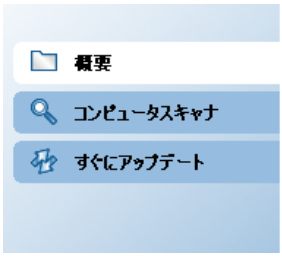
 赤のアイコンは AVG が重大な状況にあることを示しています。1つあるいは複数のコンポーネントが適切に動作しておらず、AVGがコンピュータを保護できません。報告された問題を修復してください。エラーを自分で修復できない場合、AVGテクニカルサポートチームにお問い合わせください。

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

注意：AVGステータス情報は、システムトレイアイコンからも取得可能です。

6.3. 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*）。

6.4. 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 9.0 File Server*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>>
- *ルートキット対策*はマルウェアを隠そうとするプログラムと技術を検出します。-詳細>>
- *ライセンス*は、AVGライセンス契約内容を表示します。 - 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。

6.5. 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。

6.6. 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 9.0 File Server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、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。

7. AVGコンポーネント

7.1. ウイルス対策

7.1.1. 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。

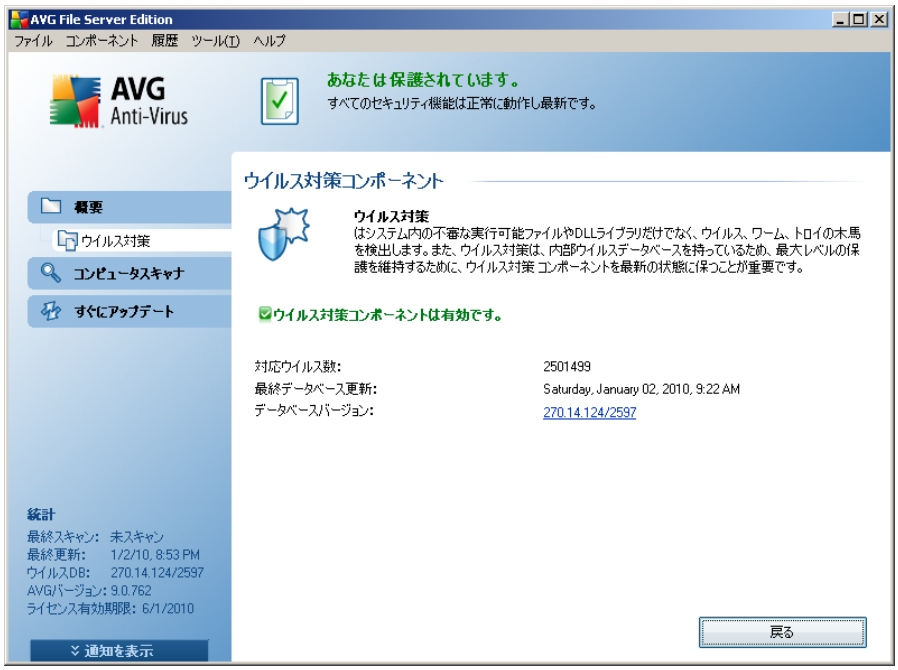
ウイルス対策の重要な機能は、既知のウイルスはコンピュータで実行されないということです。

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。

7.1.2. 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。

7.2. スパイウェア対策

7.2.1. スパイウェア対策 原理

スパイウェアは、通常、ユーザーが知らない間に許可なくコンピュータから情報を収集するようなマルウェアの一種として定義されます。一部のスパイウェアアプリケーションは、故意にインストールされることもあり、広告やウィンドウポップアップ、その他の不快なソフトウェアを含む場合があります。

現在、大部分の感染原因は、潜在的に危険な内容を含むWebサイトです。メールを介してのワーム、ウイルスの送信といったその他の感染方法も広まっています。常にバックグラウンドスキャンをオンにして、*スパイウェア対策*を使用することが重要です。これは常駐シールドのように機能し、アプリケーションを実行する際にそれをバックグラウンドでスキャンします。

また、マルウェアがAVGをインストールする前にコンピュータに送信されたり、あるいは、**AVG 9.0 File Server**最新のデータベースを維持し、プログラムのアップデートを行わなかったという潜在的なリスクもありますこのため、AVGでは、スキャン機能を使用して、マルウェアやスパイウェアを検出することができるようになっています。また、休止中で、アクティブではないマルウェアも検出します。例えば、ダウンロードされ、またアクティブ化されていないマルウェアも検出されます。

7.2.2. 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。

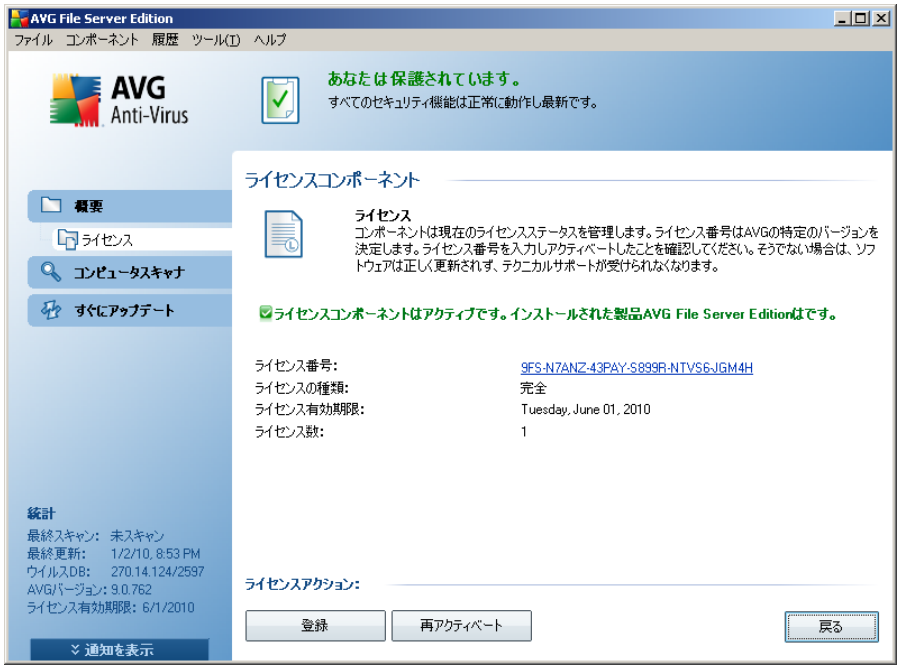
- *スパイウェア定義数*- 最新のスパイウェアデータベースバージョンで定義されたスパイウェアサンプルの数が表示されます。
- *最終データベース更新*- スパイウェアデータベースが最後にアップデートされた日時が表示されます。
- *データベースバージョン*- 最新のスパイウェアデータベースバージョン番号が表示されます。この番号はアップデートごとに増加します。

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。

7.3. 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 9.0 File Server**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 9.0 File Server**

コントロールボタン

- *今すぐ登録* - AVG ウェブサイト（http://www.avg.com）の登録ページに接続します。登録データを入力してください。AVG製品を登録したお客様のみが無料テクニカルサポートを受けることができます。

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

- *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。

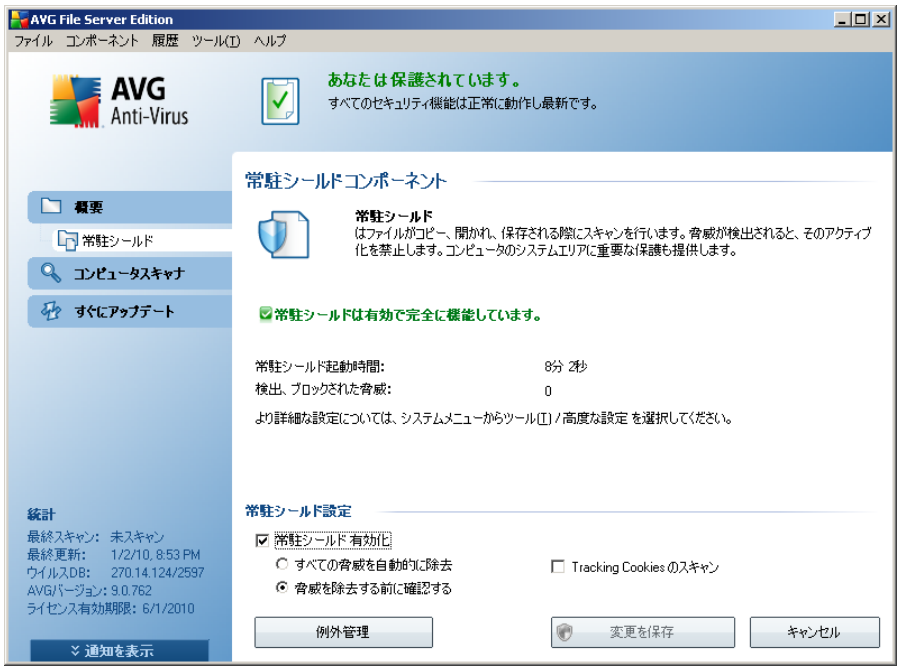
7.4. 常駐シールド

7.4.1. 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。

7.4.2. 常駐シールドインターフェース



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

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

基本コンポーネント設定

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

*常駐シールド有効化*オプションでは、常駐保護のオン/オフを簡単に切り替えることができます。デフォルトではこの機能はオンとなっています。常駐シールドをオンにすると、さらに検出された感染の処理（除去）方法を決定できます。

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

この選択はセキュリティレベルに影響はありません。

いずれの場合も、*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。

- *例外の管理* - [*常駐シールド - 例外ディレクトリ*] ダイアログを開きます。このダイアログでは、*常駐シールド*スキャンから除外されるフォルダを定義します。
- *変更を保存* - このボタンを押すと、ダイアログで行われた変更を保存、適用します。
- *戻る* - このボタンを押すと、デフォルトの*AVGユーザーインターフェース*（コンポーネント概要）に戻ります

7.4.3. 常駐シールド検出

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

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

- *修復* - 修復方法がある場合、AVG によって感染ファイルは自動的に修復されます。このオプションのアクションを取ることをお勧めします。
- *ウイルス隔離室に移動* - ウイルスは AVG *ウイルス隔離室に移動します。*
- *ファイルに移動* - このオプションは不審なオブジェクトの正確な場所に移動します（*新しい Windows Explorer ウィンドウを開きます*）
- *無視* - しかるべき理由がない場合は、このオプションを使用しないでください。

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

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

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

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

7.5. アップデートマネージャ

7.5.1. アップデートマネージャ 原理

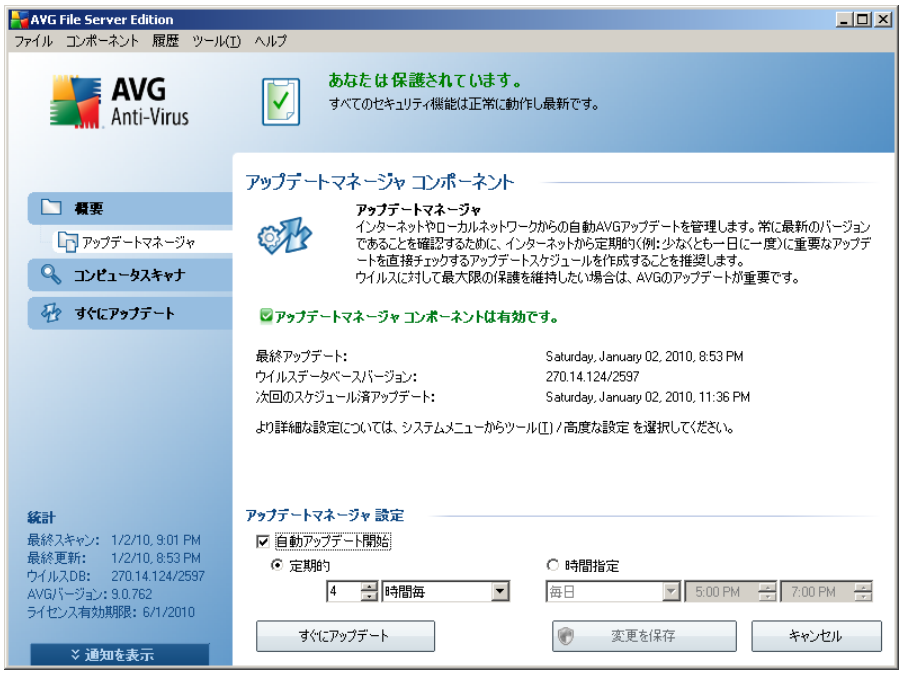
定期的にアップデートが実行されていない場合、どのようなセキュリティソフトウェアも様々な脅威からの保護を保証することはできません。ウイルス作成者は、常にソフトウェアとオペレーティングシステムの両方の欠陥を探しています。新しいウイルス、新しいマルウェア、新しいハッキング攻撃は日々出現しています。このため、ソフトウェアベンダーは継続的にアップデートとセキュリティパッチを発行し、発見されたセキュリティホールを修復しています。

AVGを定期的にアップデートすることは非常に重要です。

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

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

7.5.2. アップデートマネージャ インターフェース



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

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

基本コンポーネント設定

ダイアログの下部では、*アップデートマネージャ設定*セクションが表示され、ここでは、アップデートプロセスの実行ルールの一部を変更することができます。アップデートファイルのダウンロードを自動的に実行するか(*自動アップデート開始*)、またはオンデマンドで実行するかを指定します。デフォルトでは、*自動アップデート開始*オプションはオンであり、この設定を保持することを推奨します。最新アップデー

トファイルの定期的なダウンロードは、セキュリティソフトウェアが正しく機能するために、非常に重要です。

さらに、アップデートが起動するタイミングを指定することができます。

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

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

注意：すべてのAVGコンポーネントは、最適なパフォーマンスを提供するようにあらかじめ設定されています。特に理由がない場合は、AVGの設定を変更しないでください。設定変更は、経験のあるユーザーが行うことを推奨します。AVGの設定を変更する必要がある場合は、システムメニューアイテムツール/高度な設定を選択し、AVG高度な設定ダイアログで設定を編集します。

コントロールボタン

*アップデートマネージャ*インターフェースで利用できるコントロールボタンは以下の通りです。

- *すぐにアップデート*- オンデマンドで即時アップデートを実行します。
- *変更を保存* - このボタンを押すと、ダイアログで行われた変更を保存、適用します。
- *戻る* - このボタンを押すと、デフォルトの*AVGユーザーインターフェース*（コンポーネント概要）に戻ります

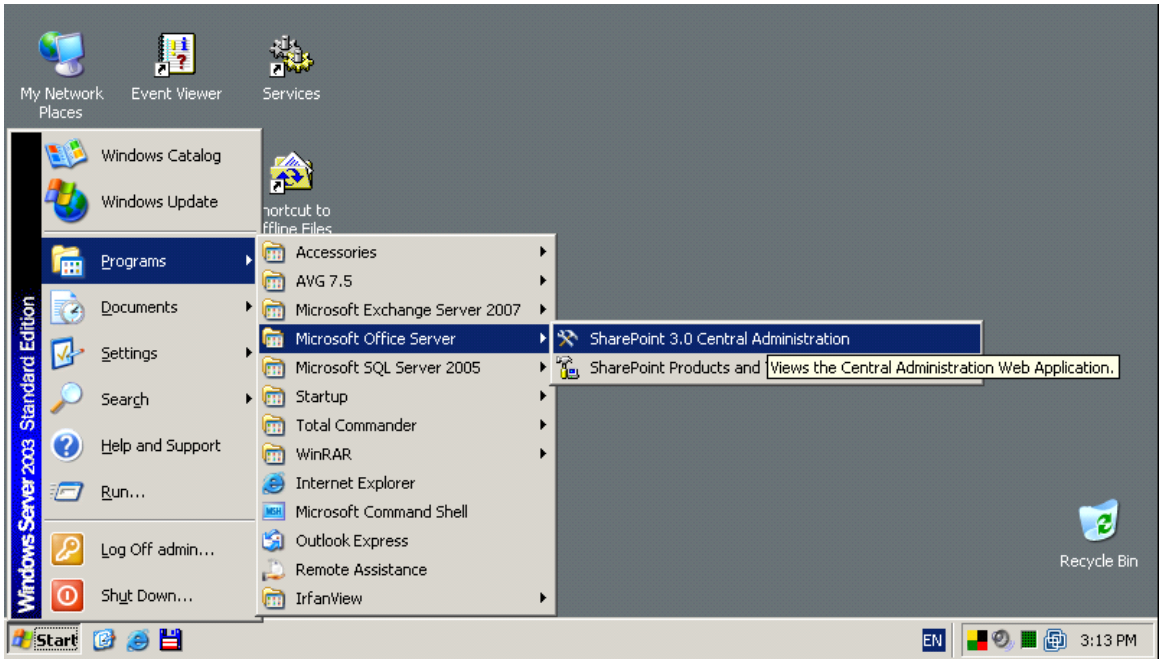
8. AVG for SharePoint Portal Server

この章では、特別な種類のファイルサーバーと考えられる ***MS SharePoint Portal Server***

8.1. プログラムメンテナンス

AVG for SharePoint Portal Serverは、ウィルス感染の可能性からサーバーを保護するために、Microsoft SP VSAPI 1.4 ウィルススキャンインターフェースを使用します。ユーザーがサーバー上でオブジェクトをダウンロードまたはアップロードするときに、サーバー上のオブジェクトにマルウェアが存在するかどうかが検査されます。ウィルス対策保護のコンフィグレーションは、SharePoint Portal Server の [*サーバーの全体管理*] インターフェースを使用して設定できます。[*サーバーの全体管理*] では、**AVG for SharePoint Portal Server**ログファイルの表示と管理もできます。

サーバーが稼動しているコンピュータにログインするときに、***SharePoint Portal Server サーバーの全体管理***を起動できます。管理インターフェースはウェブベース（と *SharePoint Portal Server* のインターフェース）であり、Windows の [*スタート*] メニューの [*プログラム / Microsoft Office Server*] フォルダ（*または SharePoint* ***Portal Server***）の [*SharePoint (3.0) サーバーの全体管理*] オプションを使用して開くことができます。

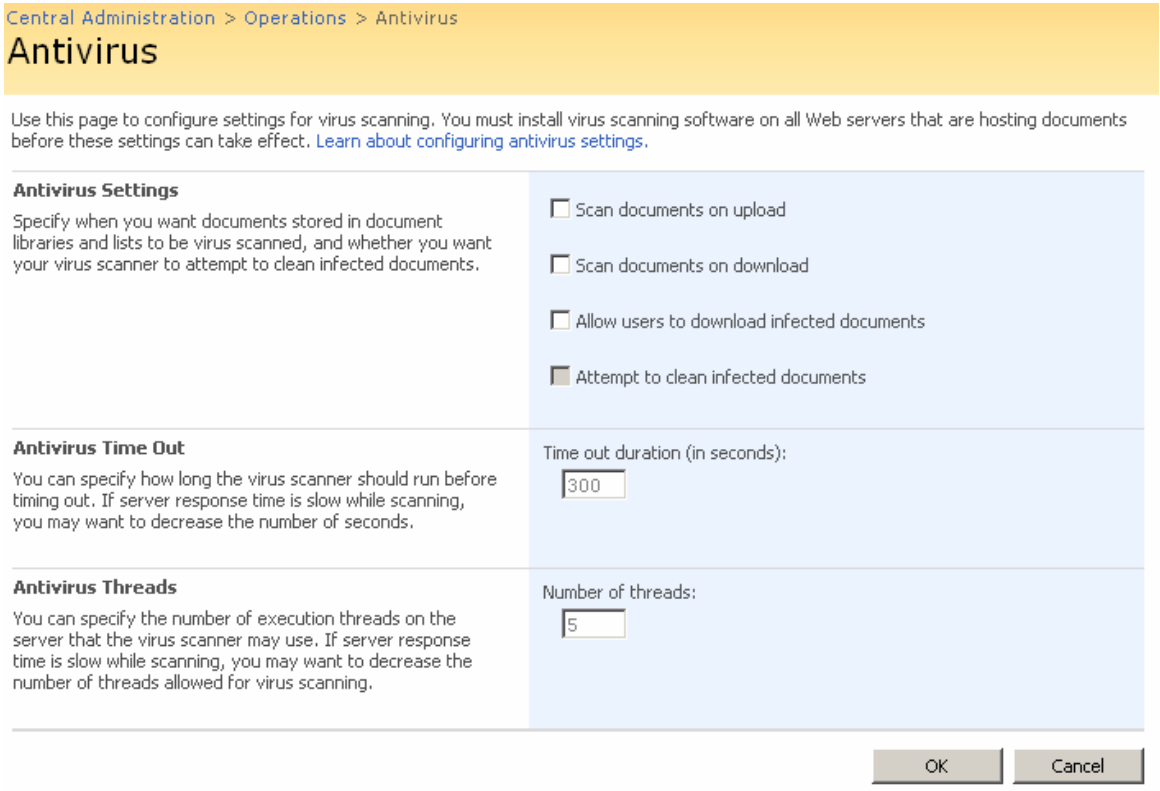


また、正しいアクセス権と URL を使用して、リモートで [***SharePoint Portal Server サーバーの全体管理***] ウェブページに入力できます。

8.2. AVG for SPPS Configuration - SharePoint 2007

[*SharePoint 3.0 ポータル サーバーの全体管理*] インターフェースでは、**AVG for SharePoint Portal Server**スキャナのパフォーマンスパラメータとアクションを簡単に設定できます。[*サーバーの全体管理*] セクションの [*動作*] オプションを選択します。新しいダイアログが表示されます。[*セキュリティコンフィグレーション*] 部の [*ウィルス対策*] 項目を選択します。

次のウィンドウが表示されます。



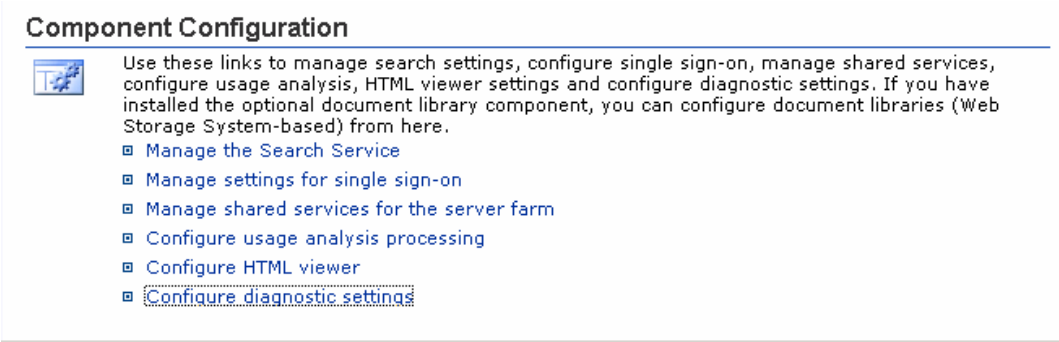
ここでは、さまざまな**AVG for SharePoint Portal Server**ウィルス対策スキャンアクションとパフォーマンス機能を設定できます。

- *アップロード中のドキュメントをスキャン* - アップロードされているドキュメントのスキャンを有効化/無効化します。
- *ダウンロード中のドキュメントをスキャン* - ダウンロードされているドキュメントのスキャンを有効化/無効化します。
- *ユーザーによる感染ドキュメントのダウンロードを許可* - ユーザーによる感染ドキュメントのダウンロードを許可/禁止します。
- *感染ドキュメントの除去を試みる* - 感染ドキュメントの自動消去を有効化/無効化します。
- *タイムアウト期間 (秒)* - 起動後にウィルススキャン処理が実行される最大時間 (秒)。ドキュメントスキャン中のサーバー の応答が遅いように思われる場合は値を下げます。

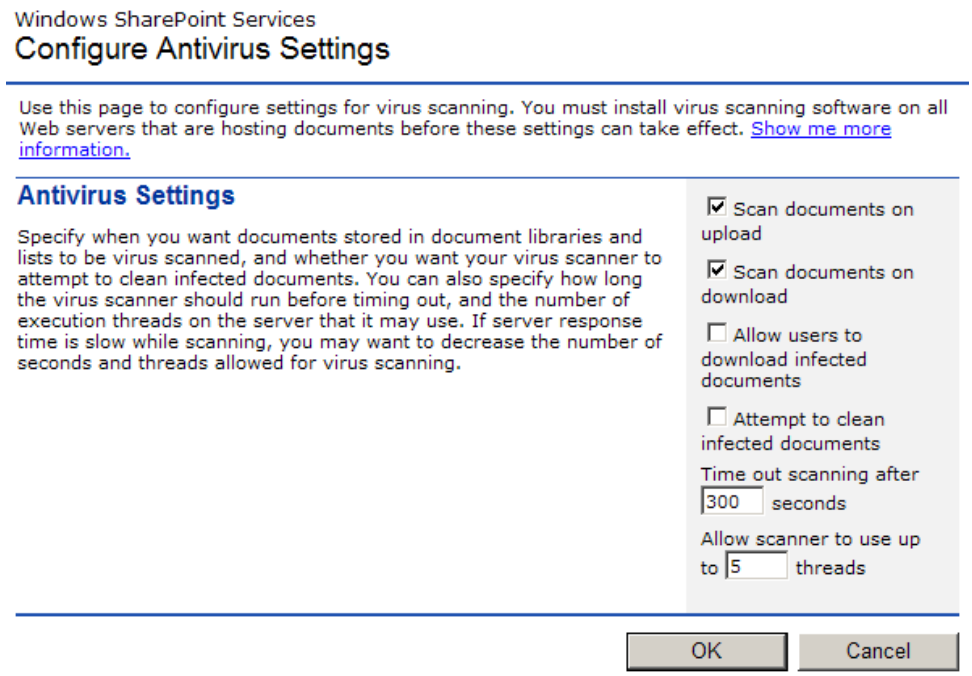
- *スレッド数* - 同時実行可能なウィルススキャンスレッド数を指定できます。値を大きくすると、並列化レベルが上がるためスキャン速度が上がる場合がありますが、一方でサーバーの応答時間が長くなる可能性があります。

8.3. AVG for SPPS Configuration - SharePoint 2003

[*SharePoint ポータル サーバーの全体管理*] インターフェースでは、**AVG for SharePoint Portal Server**スキャナのパフォーマンスパラメータとアクションを簡単に設定できます。[*セキュリティコンフィグレーション*] の [*ウィルス対策アクションコンフィグレーション*] オプションを選択します。



次のウィンドウが表示されます。



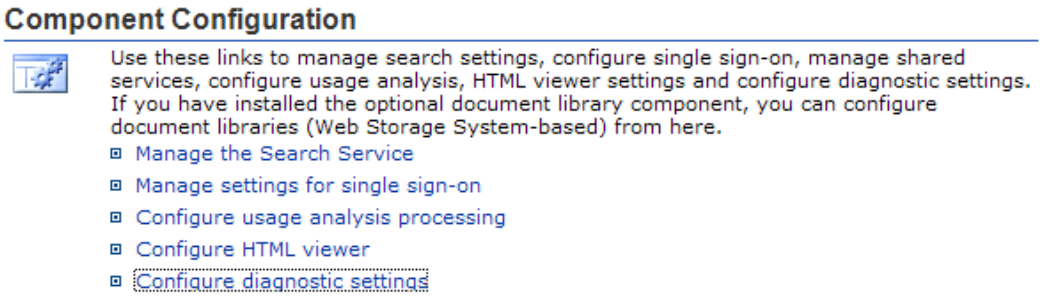
ここでは、さまざまな**AVG for SharePoint Portal Server**ウィルス対策スキャンアクションとパフォーマンス機能を設定できます。

- *アップロード中のドキュメントをスキャン* - アップロードされているドキュメントのスキャンを有効化/無効化します。
- *ダウンロード中のドキュメントをスキャン* - ダウンロードされているドキュメントのスキャンを有効化/無効化します。
- *ユーザーによる感染ドキュメントのダウンロードを許可* - ユーザーによる感染ドキュメントのダウンロードを許可/禁止します。
- *感染ドキュメントの除去を試みる* - 感染ドキュメントの自動消去を有効化/無効化します。
- *スキャンの時間制限* - 起動後にウィルススキャン処理が実行される最大時間(秒)。*ドキュメントスキャン中のサーバーの応答が遅いように思われる場合は値を下げます。*
- *最大値を使用します。ドキュメントスキャン中のXサブプロセス* - Xには同時に実行可能なウィルススキャンスレッド数を指定します。値を大きくすると、並列化レベルが上がるためスキャン速度が上がる場合がありますが、一方

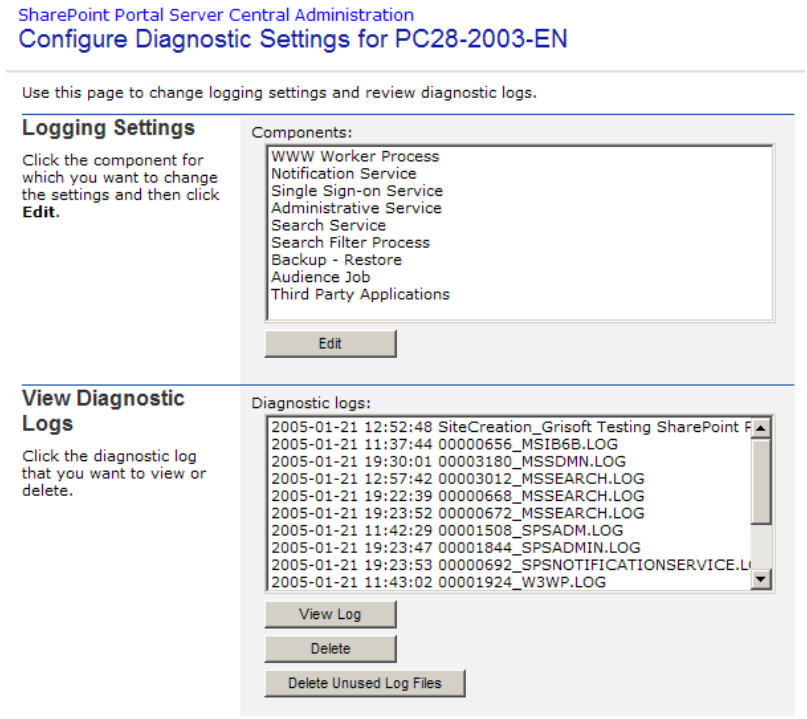
でサーバーの応答時間が長くなる可能性があります。

8.4. AVG for SPPS Edition Diagnostics

AVG for SharePoint Portal Serverの診断メッセージは、[*SharePoint サーバーの全体管理*] の [*コンポーネントコンフィグレーション*] セクションの [*診断設定コンフィグレーション*] を選択すると表示できます。



AVG for SharePoint Portal Serverパフォーマンスに関するすべての診断情報は、*_AVG4SPS.LOG ファイルに格納されています。このファイルの内容は、[*診断設定コンフィグレーション*] ウィンドウの [*診断プロトコルの表示*] セクションで選択すると表示できます。



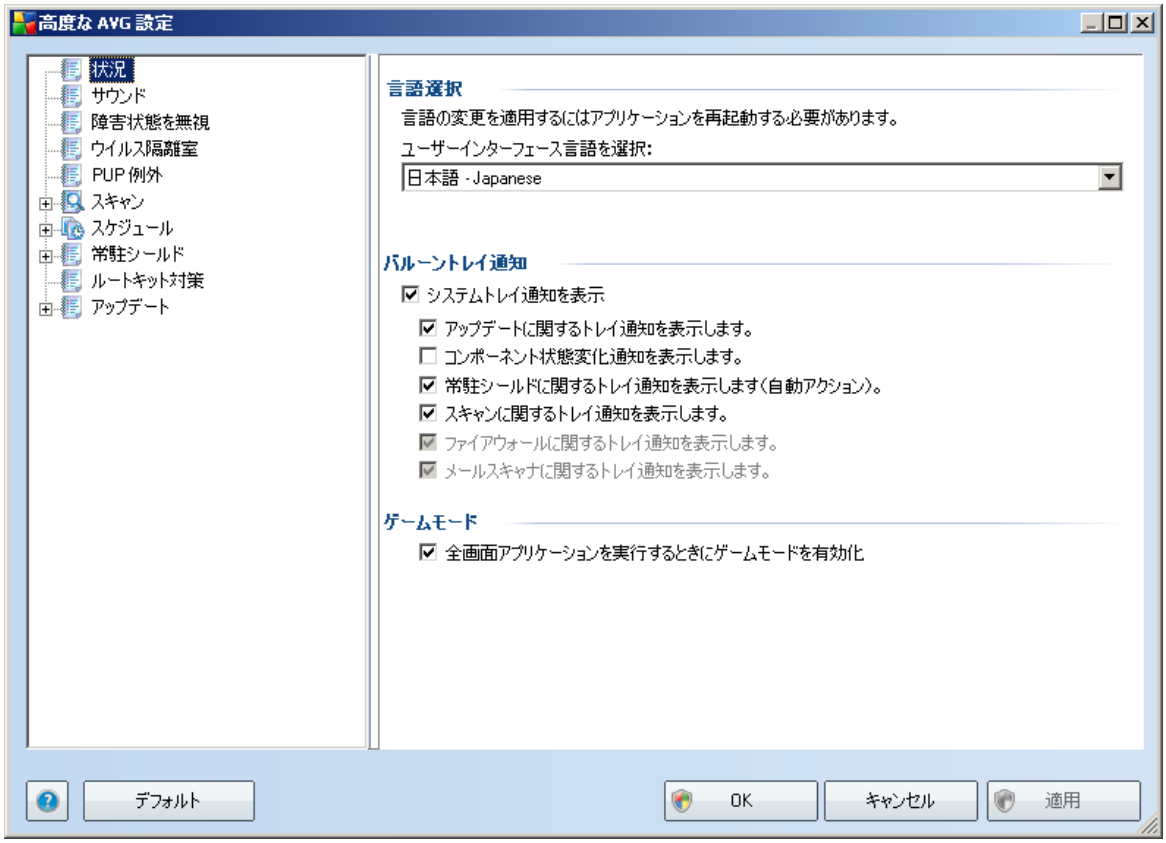
[*ログを表示*] ボタンをクリックすると、**AVG for SharePoint Portal Server**のログファイルを表示します。

9. AVG 高度な設定

AVG 9.0 File Server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。

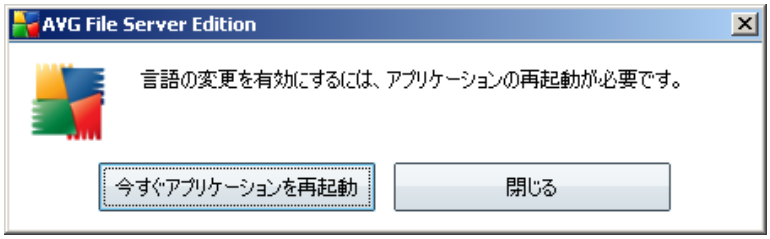


言語選択

*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ており、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。

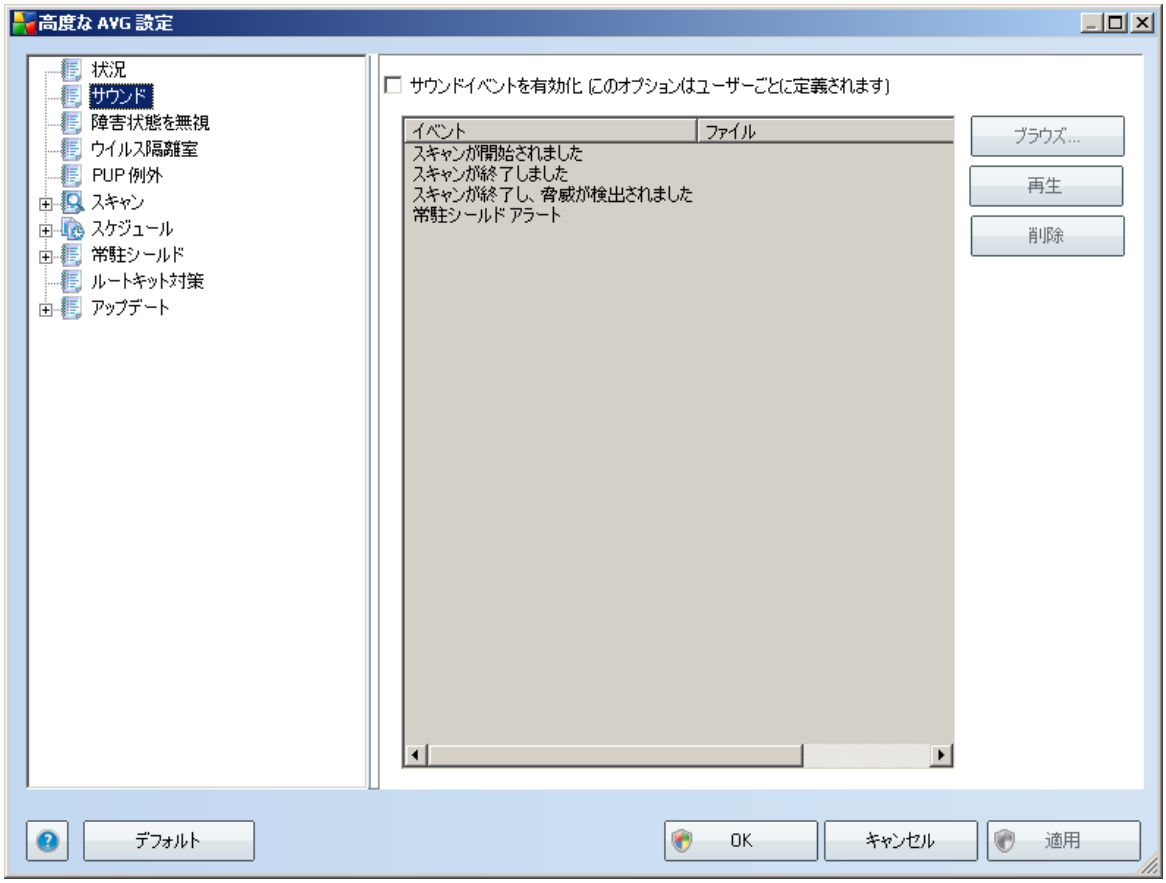
- *常駐シールドに関するトレイ通知を表示* - ファイルの保存、コピー、オープンに関する情報が表示されるかどうかを決定します。
- *スキャン*に関するトレイ通知を表示 - スケジュール済スキャンの自動起動、進行、結果に関する情報が表示されるかどうかを決定します。

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。

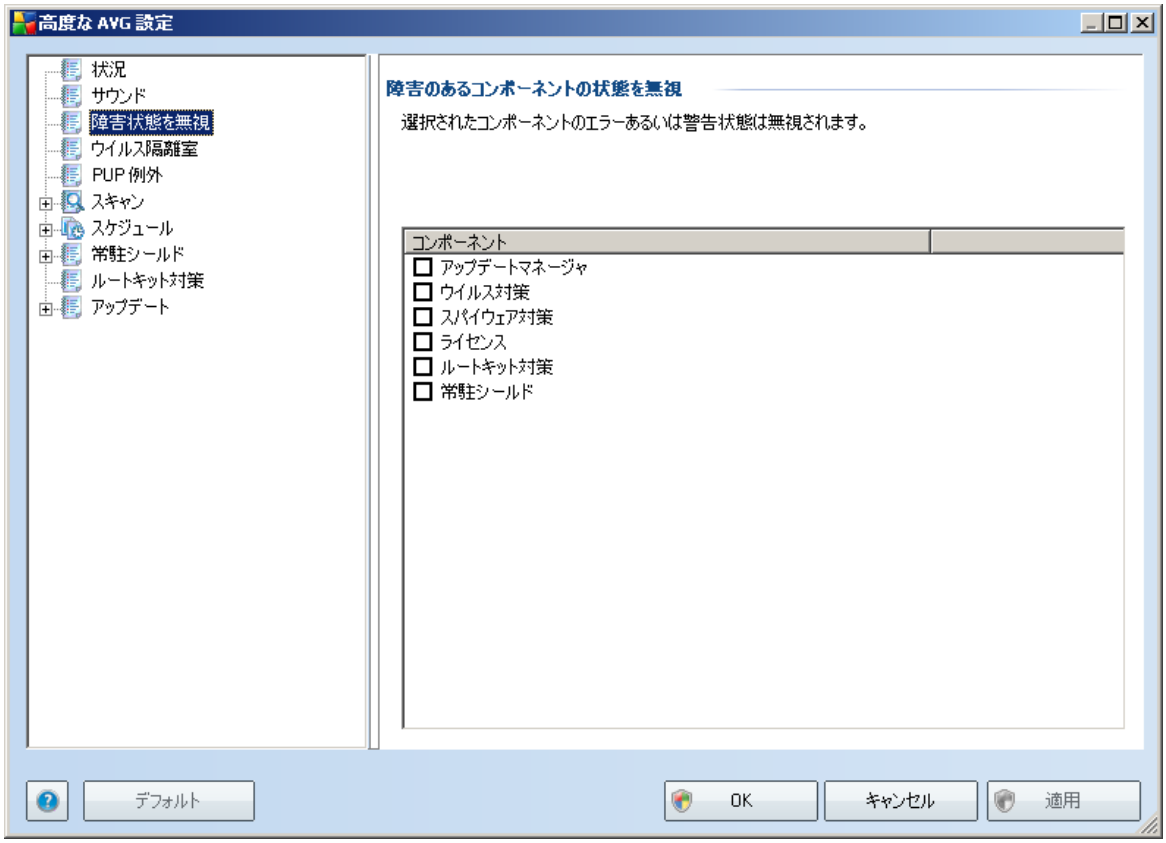


次に、リストから該当するイベントを選択し、このイベントに割り当てる適切なサウンドをディスクから参照 ([*参照*]) します。選択されたサウンドを聴くには、リストのイベントをハイライトし、[*再生*] ボタンをクリックします。[*削除*] ボタンをクリックすると、特定のイベントに割り当てられたサウンドを削除します。

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。

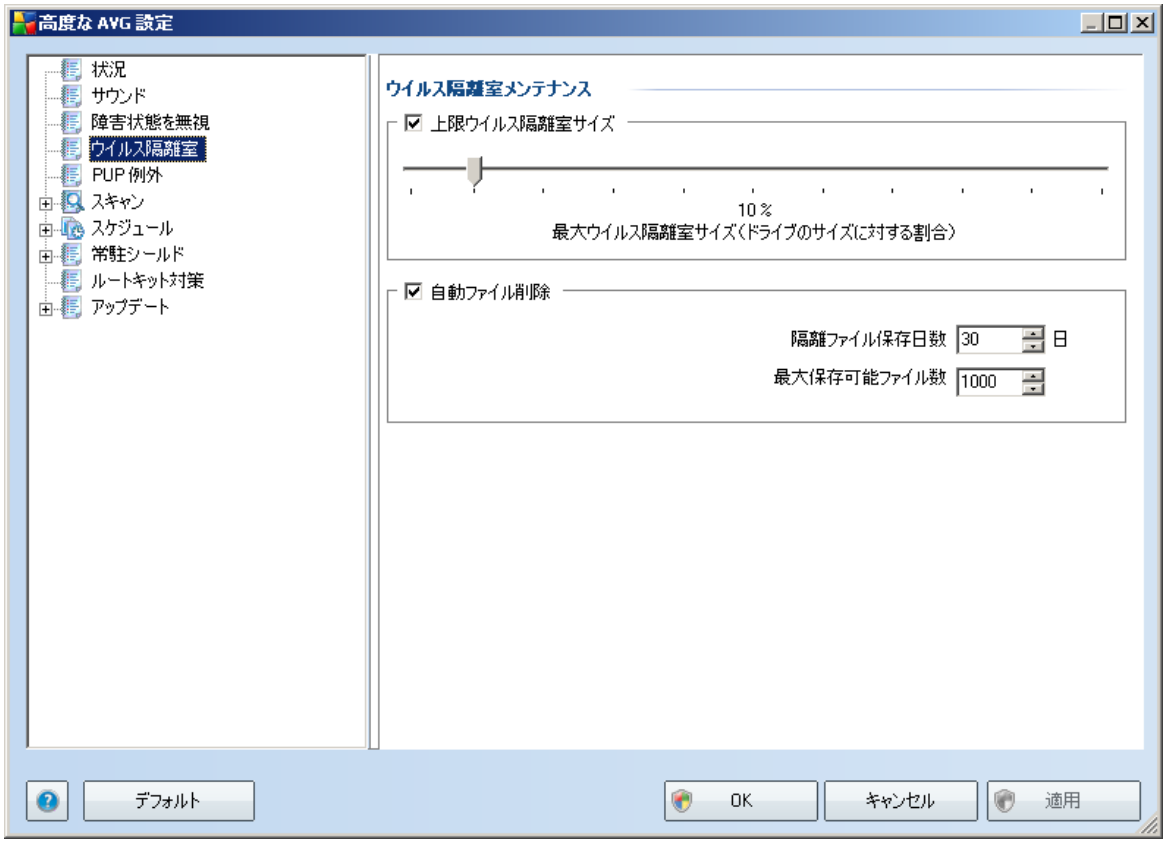
- *システムトレイアイコン*-すべてのAVGコンポーネントが正常に動作している間はアイコンは四色で表示されますが、エラーが発生すると、黄色のエクスクラメーションマークのついたアイコンが表示されます。
- AVGメインウィンドウの*セキュリティステータス情報*セクション既存の問題に関するテキスト説明

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



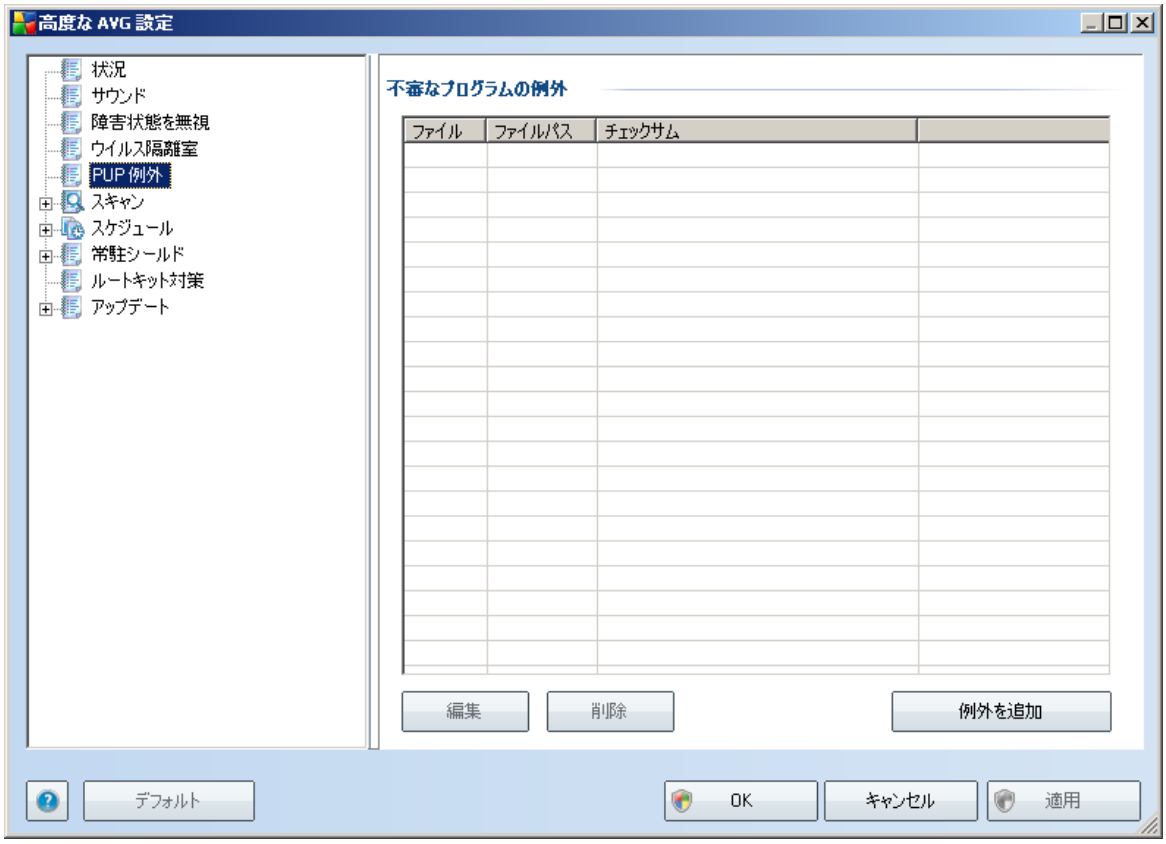
*ウイルス隔離室メンテナンス*ダイアログでは、*ウイルス隔離室*に格納されるオブジェクトに関するパラメータを設定します。

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

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

9.5. PUP 例外

AVG 9.0 File Server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。

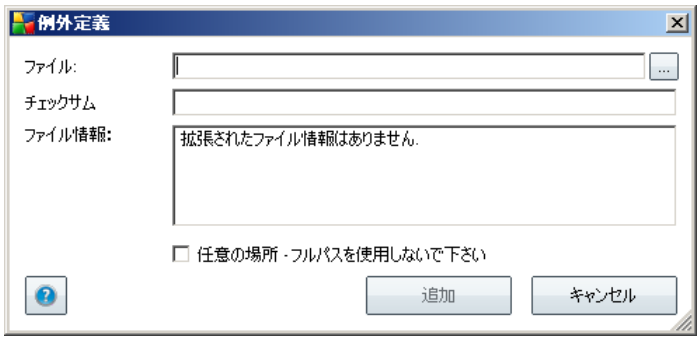
- *ファイル* - 各アプリケーション名を提供します。
- *ファイルパス* - アプリケーションの場所を示します。
- *チェックサム*- 選択されたファイルの一意の「シグネチャ」を表示します。このチェックサムは自動的に生成された文字列で、これによって、AVGは選択されたファイルとその他のファイルを区別します。チェックサムは、ファイルが正常に追加された後で生成、表示されます。

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*

ーです。*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. スキャン

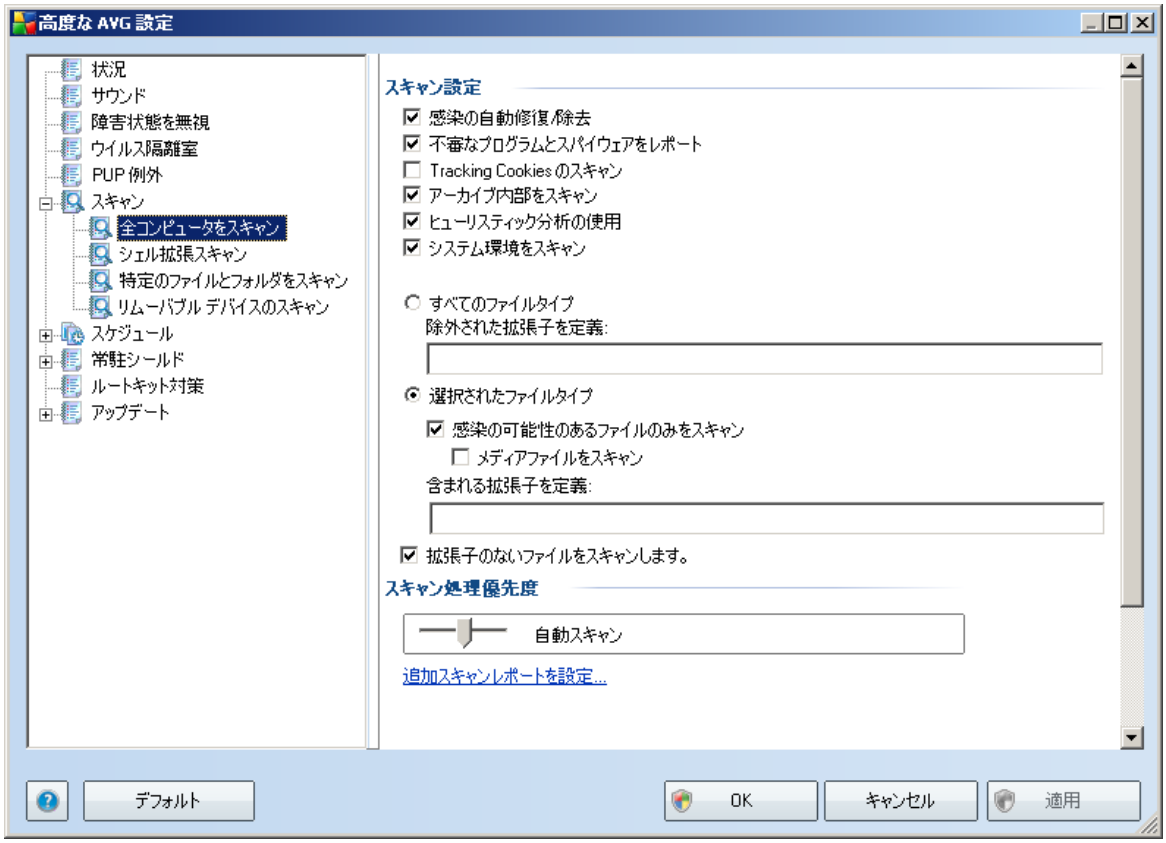
高度なスキャン設定は3つのカテゴリに分けられ、このカテゴリはソフトウェアベンダーによって定義された特定のスキャンタイプを示します。

- *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

9.6.1. 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。

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

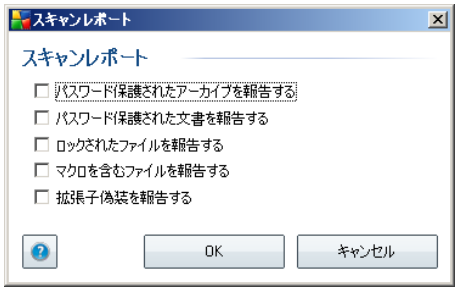
- オプションとして、*拡張子のないファイルをスキャン*できます。このオプションは既定ではオンになっています。変更する理由がない場合は、この設定を保持することをお勧めします。拡張子のないファイルは不審なものであり、常にスキャンするべきです。

スキャン処理優先度

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

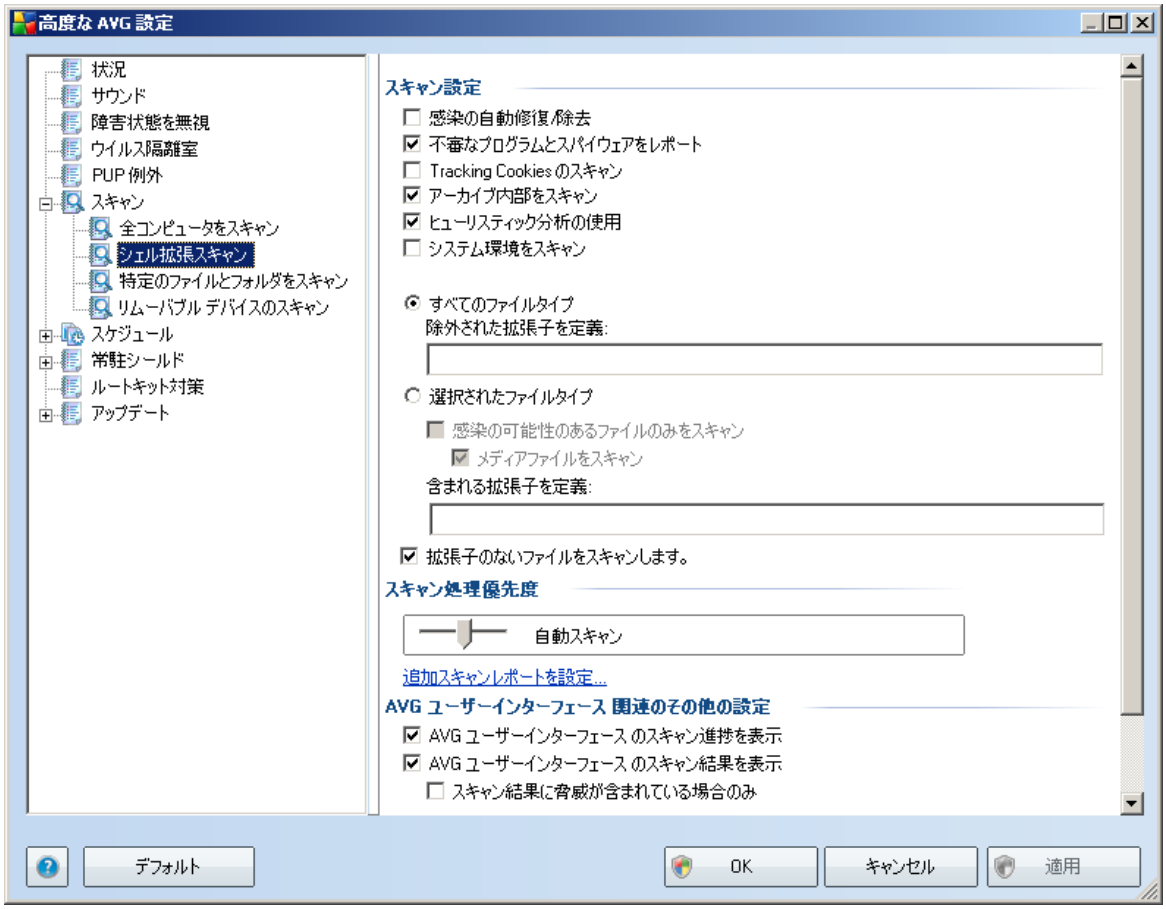
追加スキャンレポートを設定 ...

*追加スキャンレポート...*リンクをクリックすると、*スキャンレポート*ダイアログが開きます。このウィンドウでは、レポートされる検出項目を設定します。



9.6.2. 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。

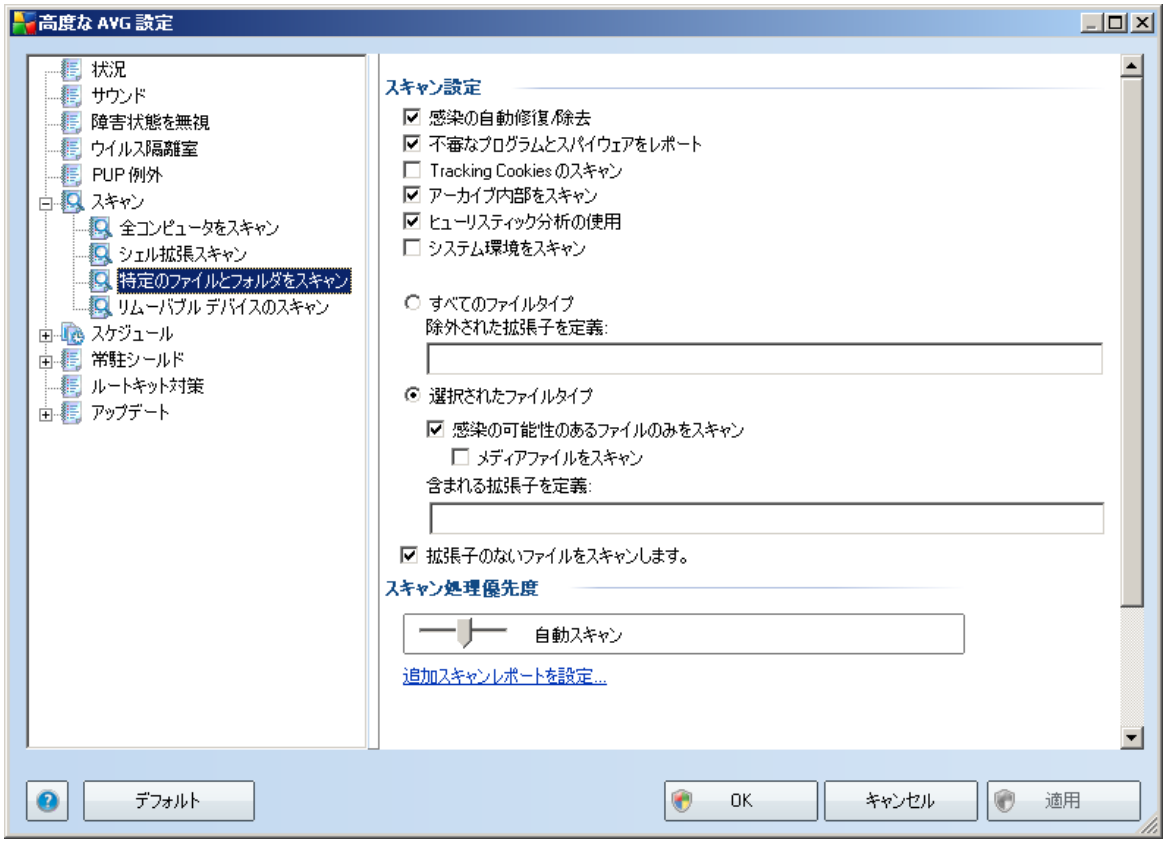


パラメータのリストは*完全コンピュータスキャン*で利用できるものと同一です。ただし、デフォルト設定が異なります。*完全コンピュータスキャン*では、ほとんどのパラメータは選択されていますが、*シェル拡張スキャン*（*Windows Explorerのスキャン*）では、関連パラメータのみがオンとなっています。

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。

9.6.3. 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。

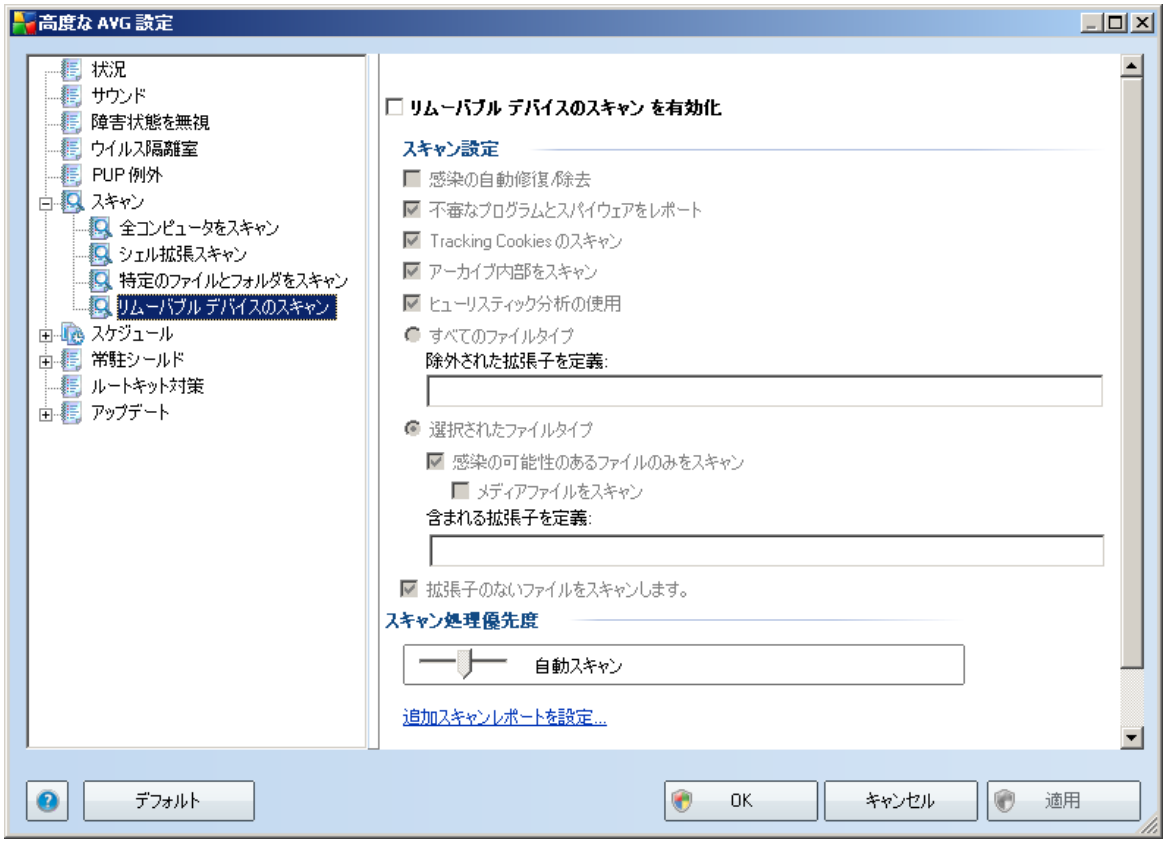


この設定ダイアログで設定されるすべてのパラメータは、*特定のファイルとフォルダをスキャン*で選択されたスキャンエリアのみに適用されます。この設定ダイアログで、*ルートキットをスキャン*オプションをチェックした場合、選択されたエリアに対してのみ、クイックルートキットスキャンが実行されます。

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。

9.6.4. 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。

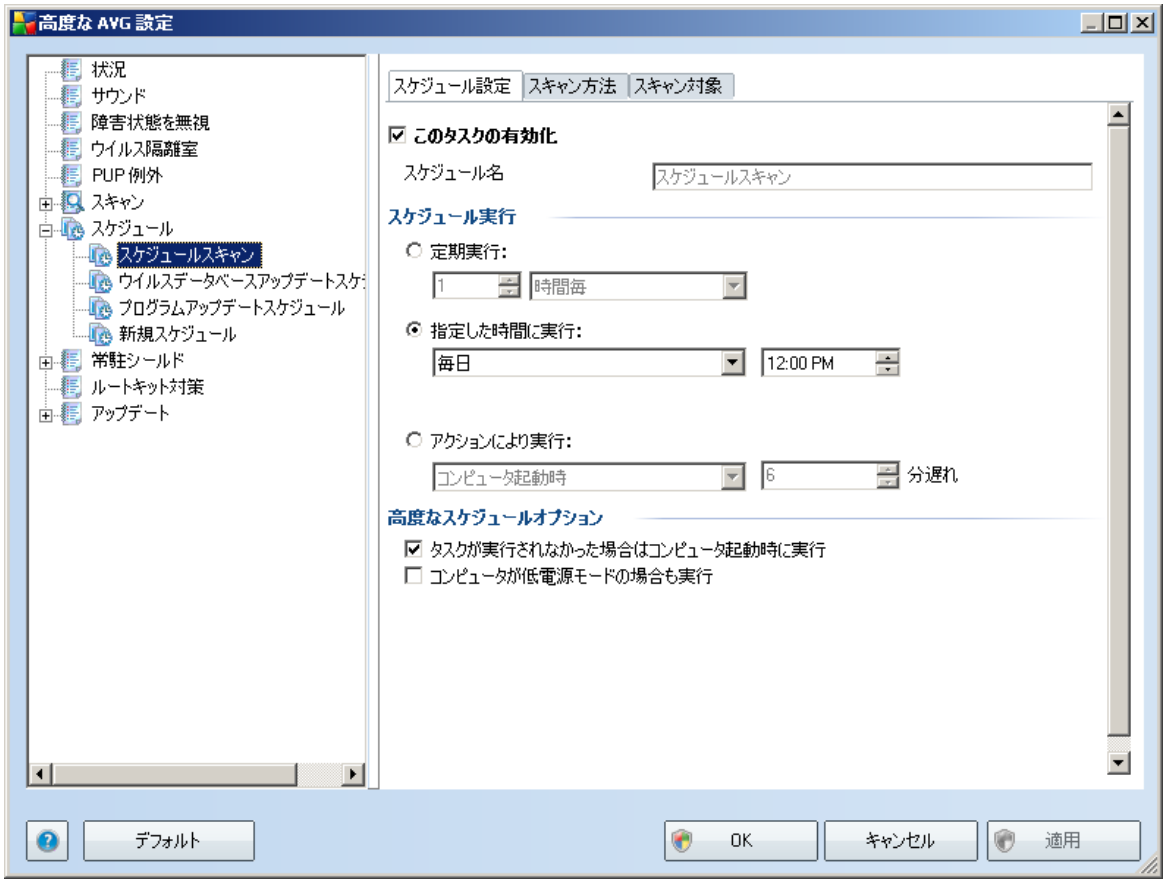
9.7. スケジュール

*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

9.7.1. 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。

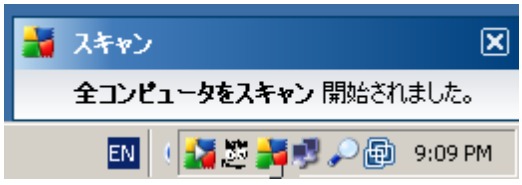
スケジュール実行

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。

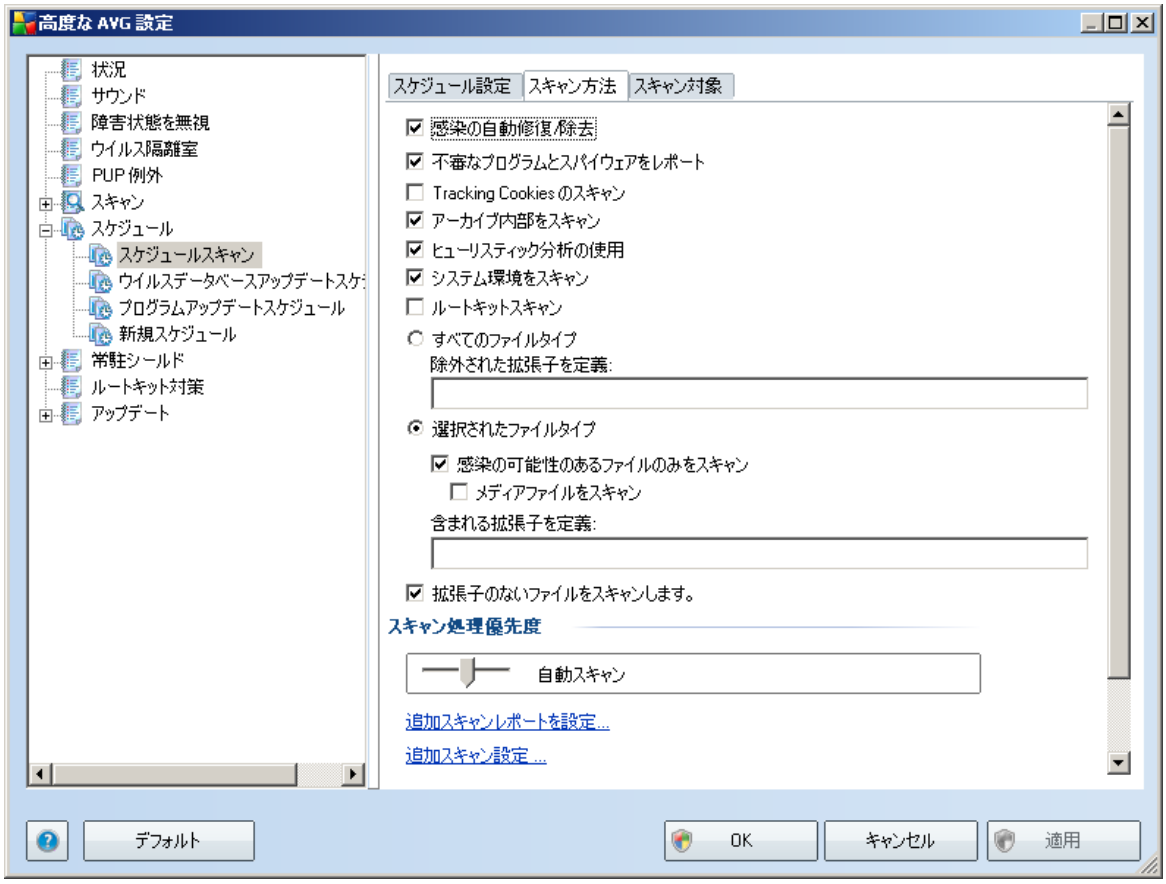
高度なスケジュールオプション

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。



*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。

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

- *不審なプログラムとスパイウェア脅威をレポート*- （*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。

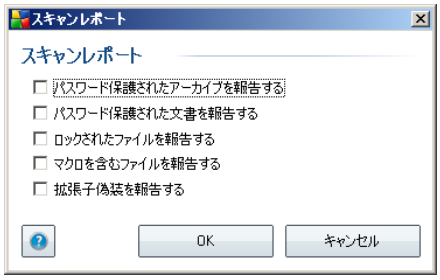
- *選択されたファイルタイプ* - 感染の可能性のあるファイルのみを指定できます（*一部のプレーンテキストファイルやその他の非実行可能ファイル*など、感染の可能性がないファイルはスキャンされません）。これには、メディアファイル（*ビデオ、オーディオファイル - これらのファイルは多くの場合、サイズが非常に大きく、ウィルスに感染している可能性が非常に低いため、このボックスのチェックを外している場合、スキャン時間がさらに短縮されます*）が含まれます。ここでも、必ずスキャンする必要があるファイルの拡張子を指定できます。

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

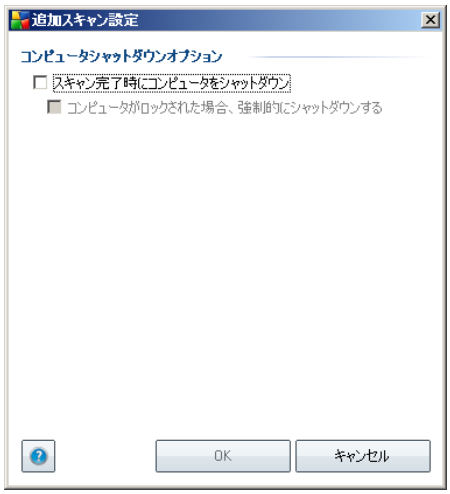
スキャン処理優先度

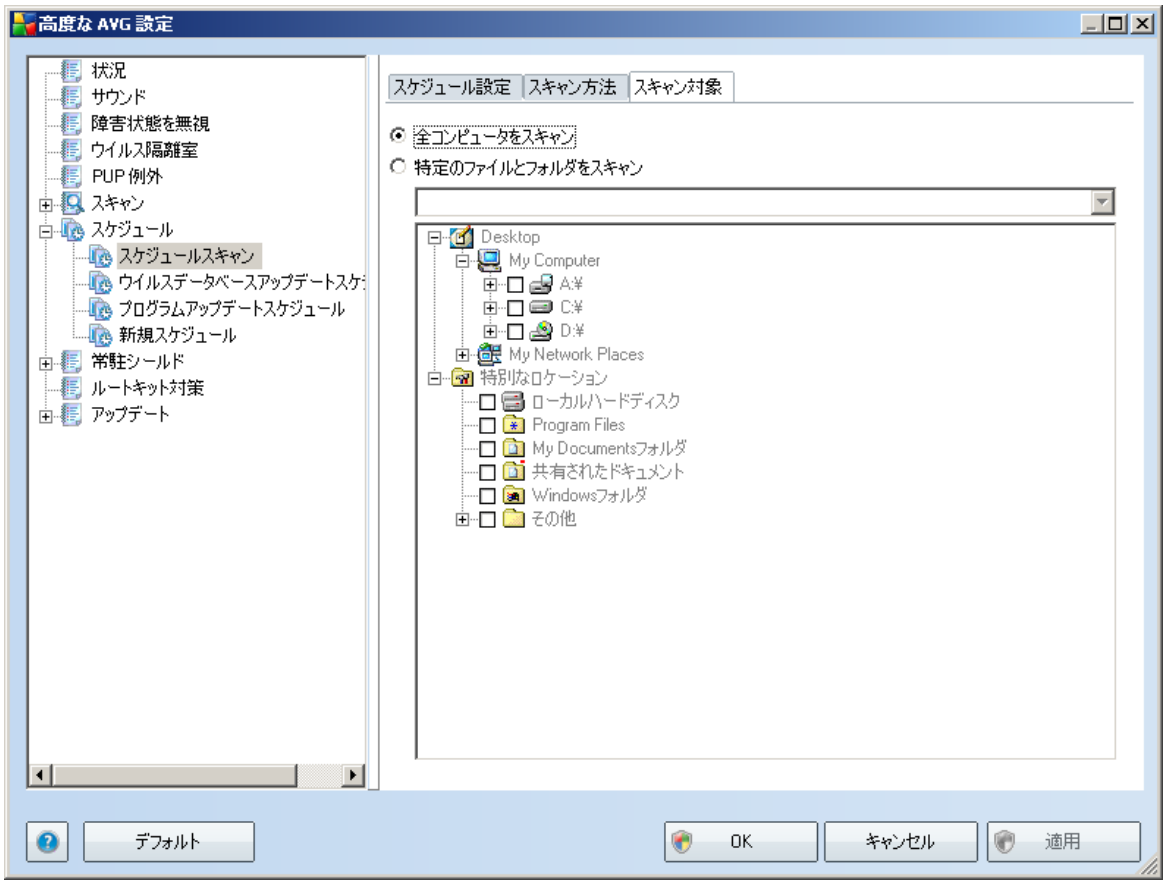
*スキャン処理優先度*セクションでは、システムリソース使用度に応じて、希望するスキャン速度を指定することができます。デフォルトでは、このオプションの値は、自動的にリソースを使用する中レベルの値に設定されています。スキャンの速度を上げたい場合、スキャンにかかる時間を削減することができますが、スキャン実行中、システムリソース使用度は著しく上がり、PC上の他の作業の速度が低下します。(*このオプションは、コンピュータの電源がオンであり、コンピュータ上で作業をしているユーザーがいない場合等に適しています。*)一方、スキャンの時間を延長することで、システムリソース使用度を下げることができます。

*追加スキャンレポート...*リンクをクリックすると、*スキャンレポート*ダイアログが開きます。このウィンドウでは、レポートされる検出項目を設定します。



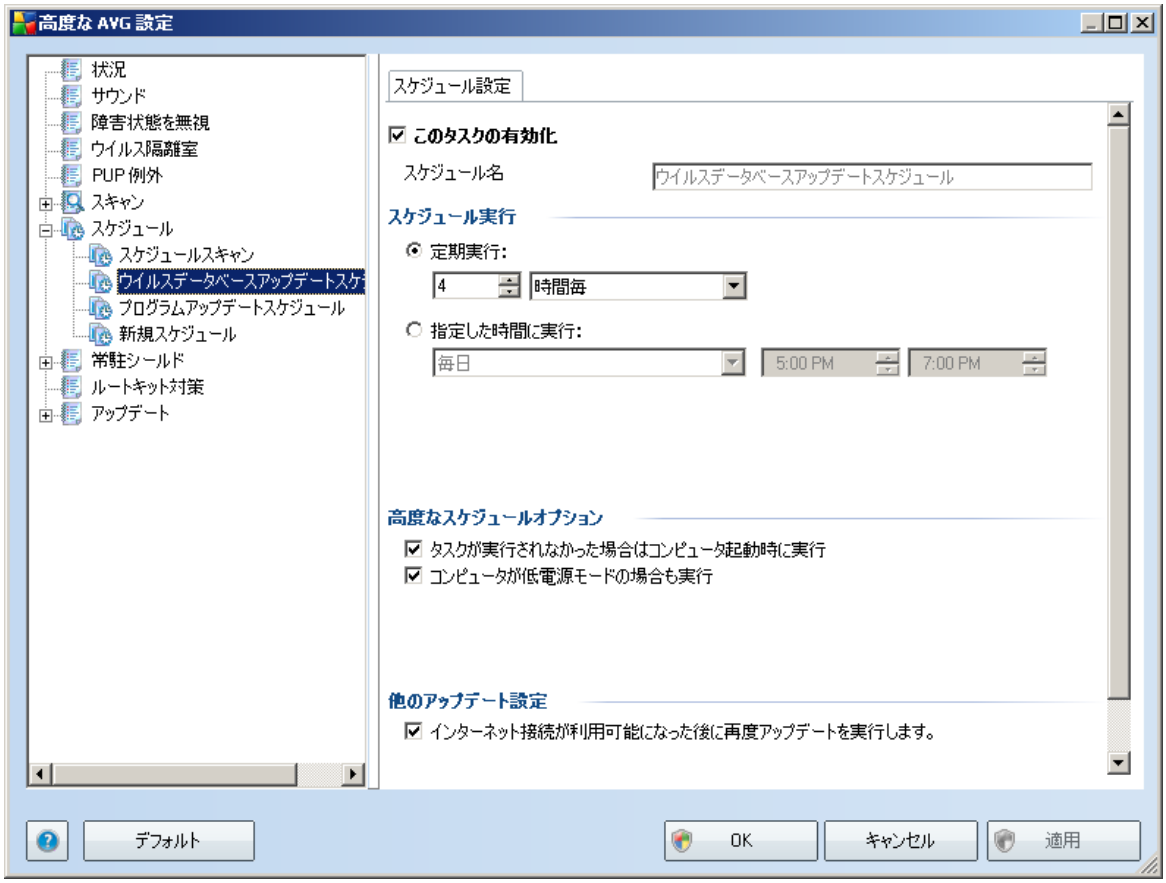
*追加スキャン設定 ...*をクリックすると、*コンピュータシャットダウンオプション*ダイアログが表示されます。このダイアログでは、スキャンプロセス終了時に自動的にコンピュータをシャットダウンするかどうかを決定します。このオプション(*スキャン完了時にコンピュータをシャットダウン*)確定すると、現在コンピュータがロックされている場合でも、コンピュータをシャットダウンさせる新しいオプション(*コンピュータがロックされた場合、強制的にシャットダウンする*)が有効化されます。





[*スキャン対象*] タブでは、全コンピュータをスキャン、あるいは特定のファイルやフォルダをスキャンのいずれかを選択します。特定のファイルやフォルダスキャン を選択した場合、ダイアログ下部のツリービューで対象フォルダを指定することができます。

9.7.2. 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

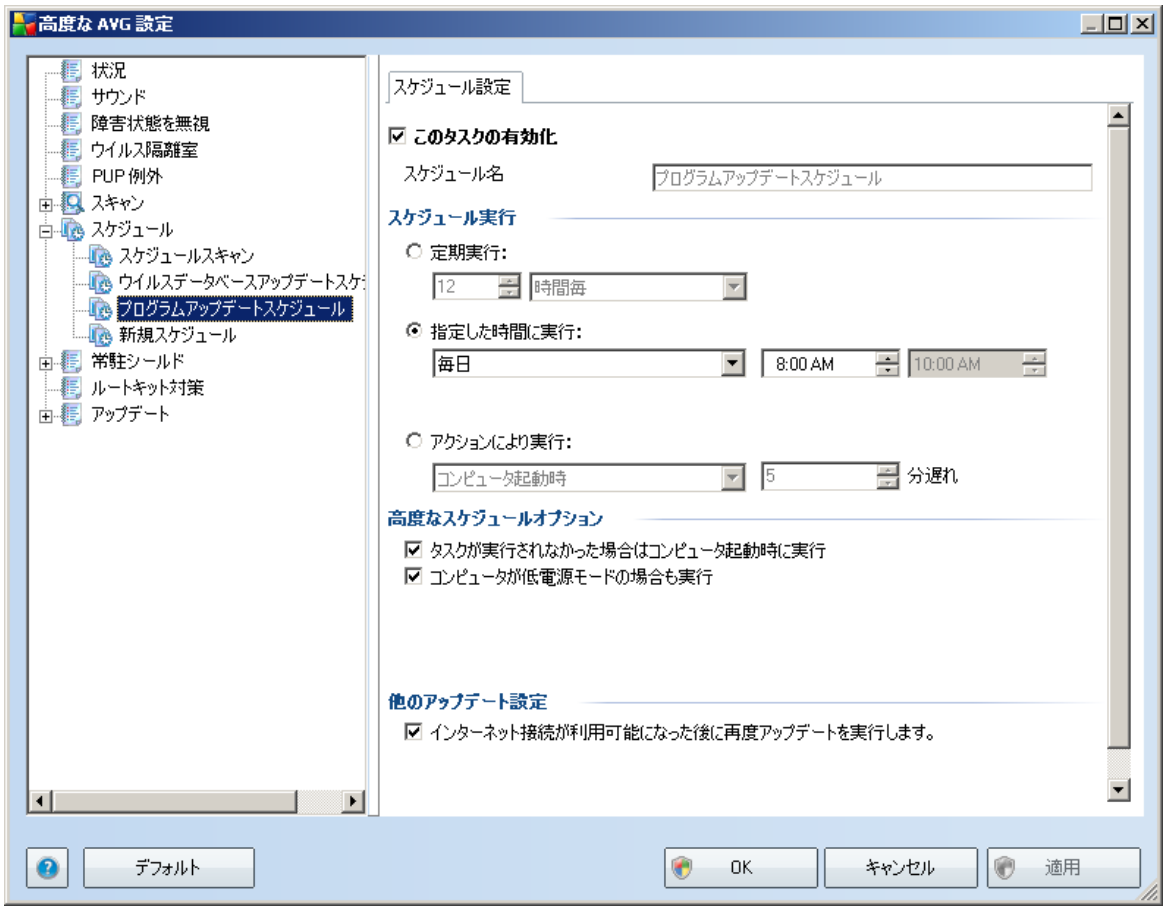
このセクションでは、コンピュータが低電源モードあるいは完全に電源オフになっている場合に、ウイルスデータベースアップデートが実行される条件を定義します。

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）。

9.7.3. 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。

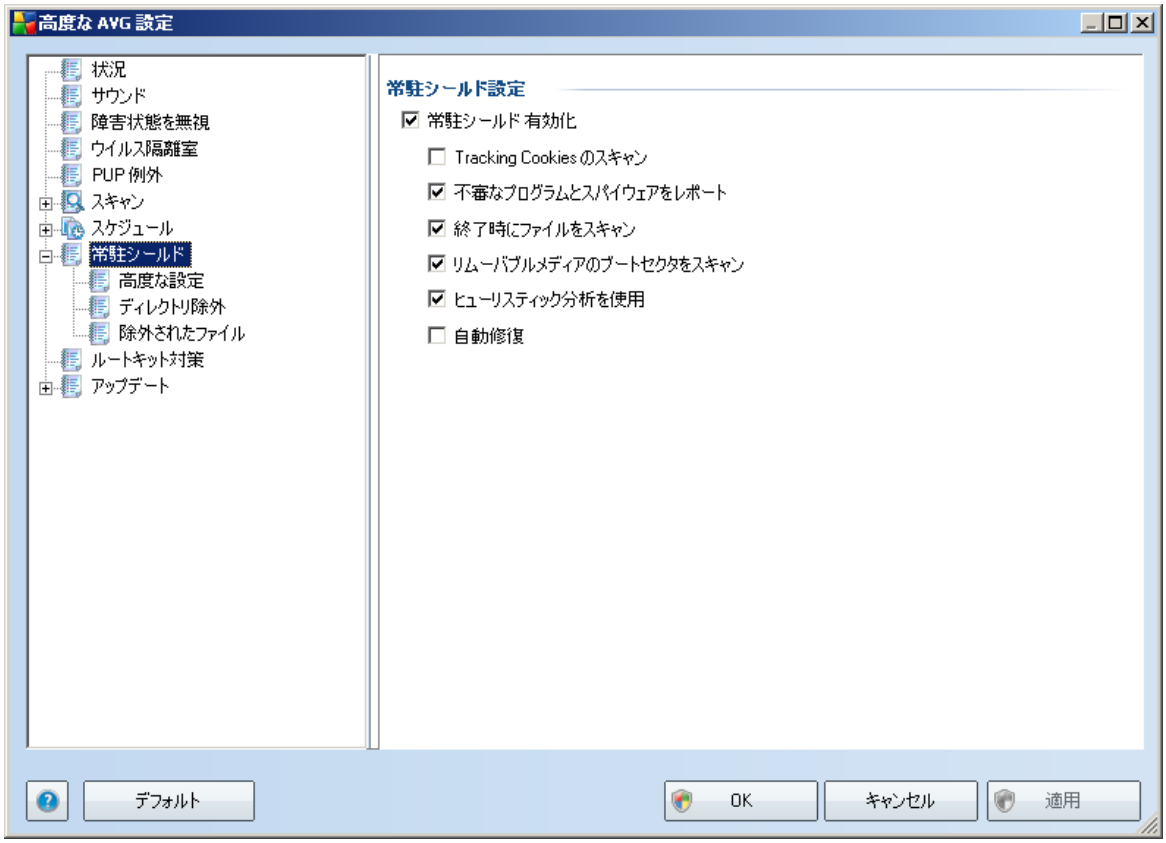
他のアップデート設定

[*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）。

9.8. 常駐シールド

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



[*常駐シールド設定*] ダイアログでは、[*常駐シールドを有効化*] 項目 (*このオプションは既定ではオンです*) をオン/オフにして、*常駐シールド*保護を完全に有効化または無効化できます。また、どの*常駐シールド*機能を有効化するかを選択します。

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

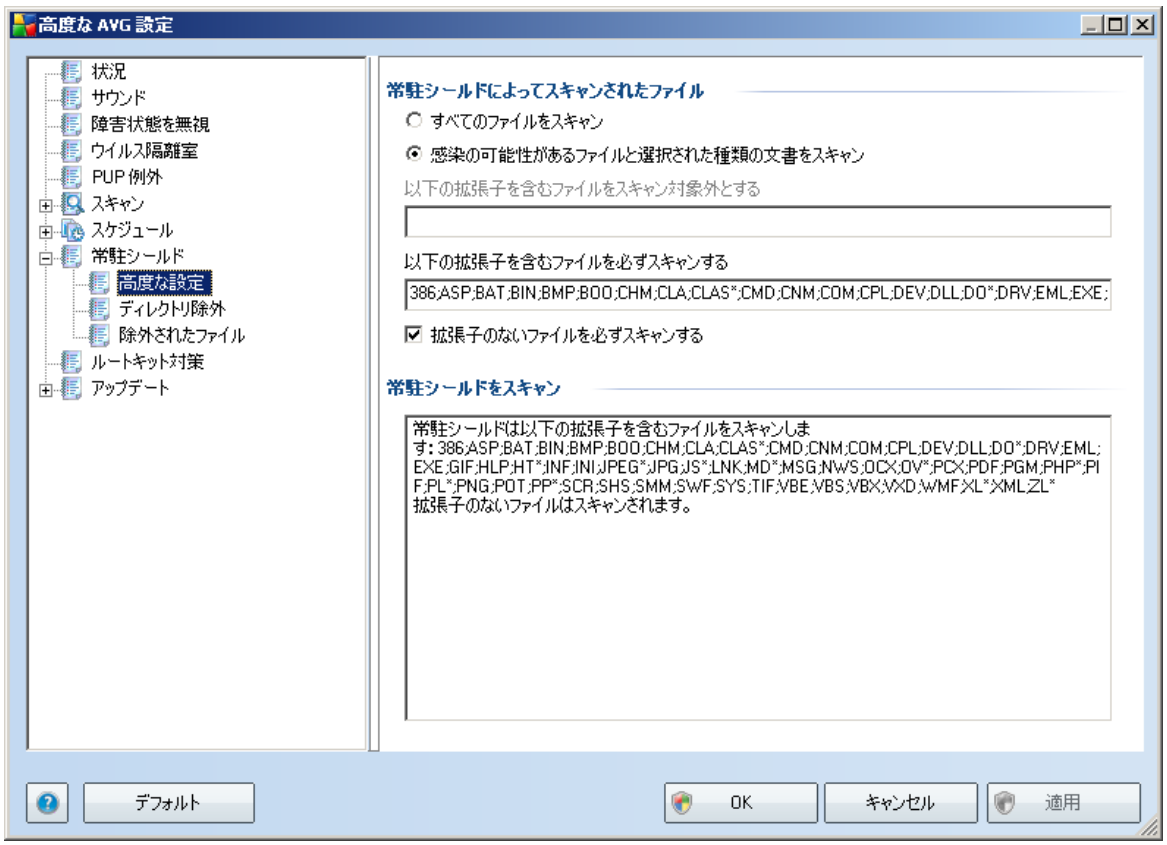
- *リムーバブルメディアのブートセクタをスキャン*-（*デフォルトではオン*）

- *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。

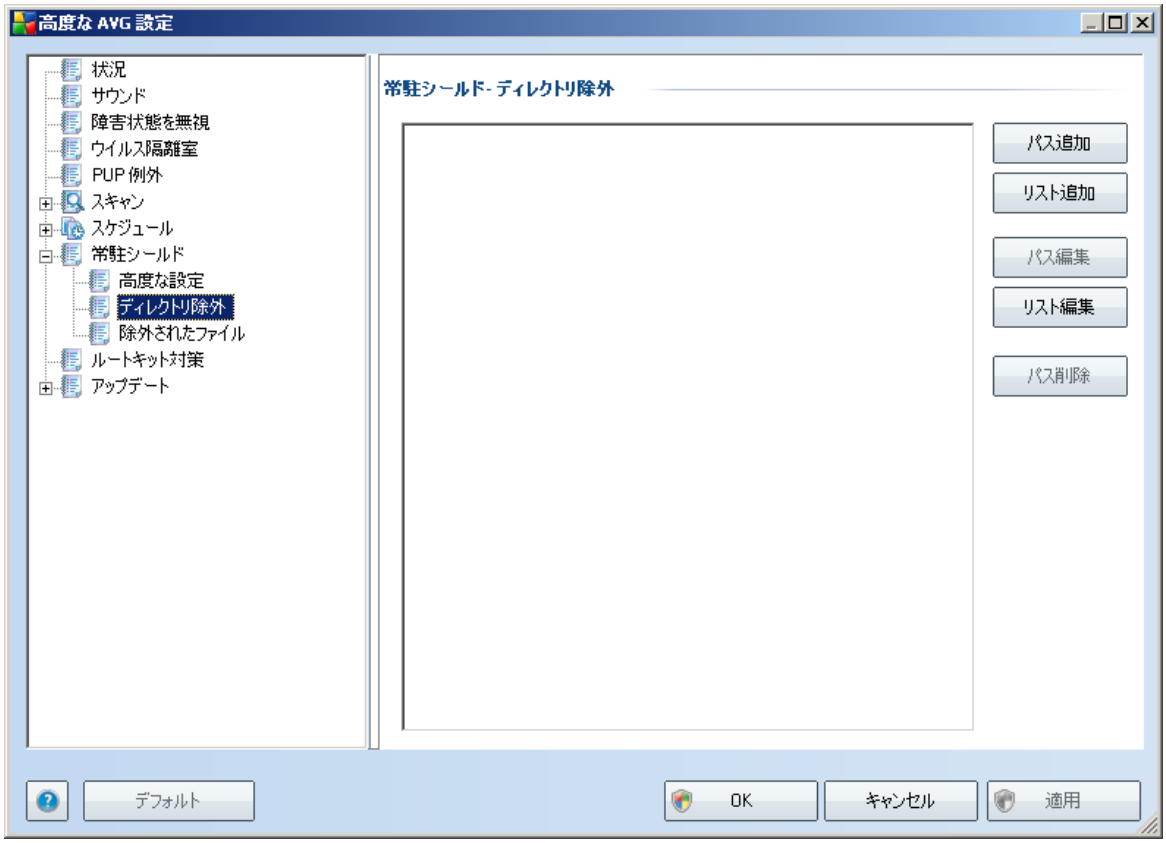
9.8.1. 高度な設定

*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。

9.8.2. 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。

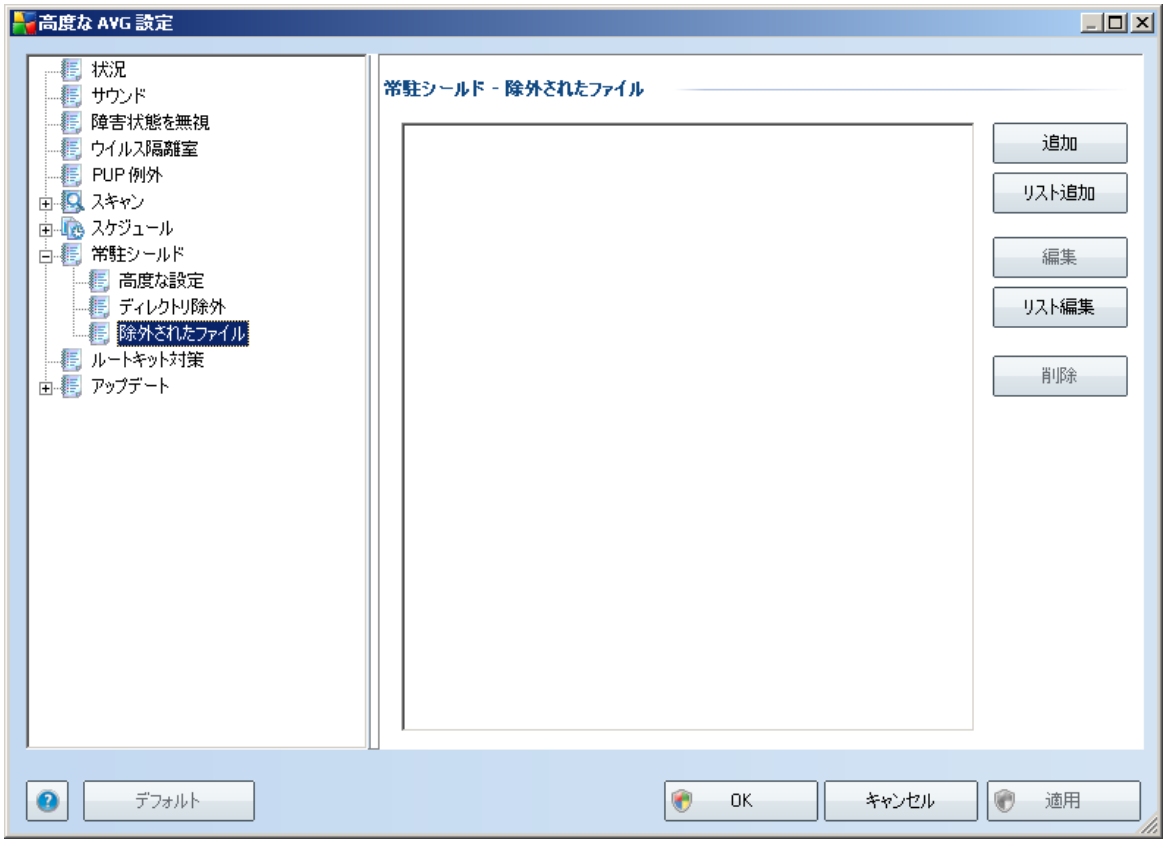
ダイアログは、以下のコントロールボタンを提供します。

- *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

9.8.3. 除外されたファイル



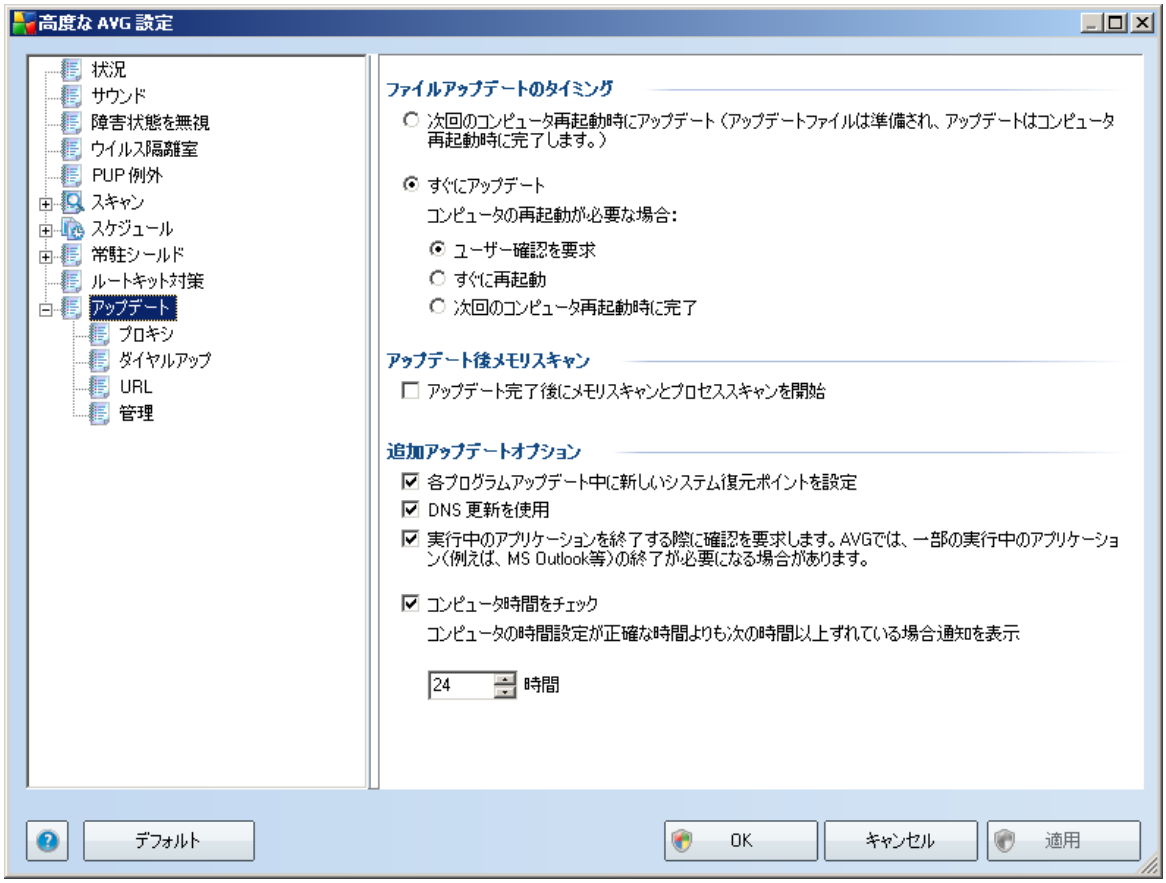
[*常駐シールド - 除外されたファイル*] ダイアログは、先に説明した*常駐シールド - 除外されたディレクトリ*と類似した方法で動作しますが、*常駐シールド*スキャンから除外するフォルダではなく、特定のファイルを定義できます。

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

9.9. 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。

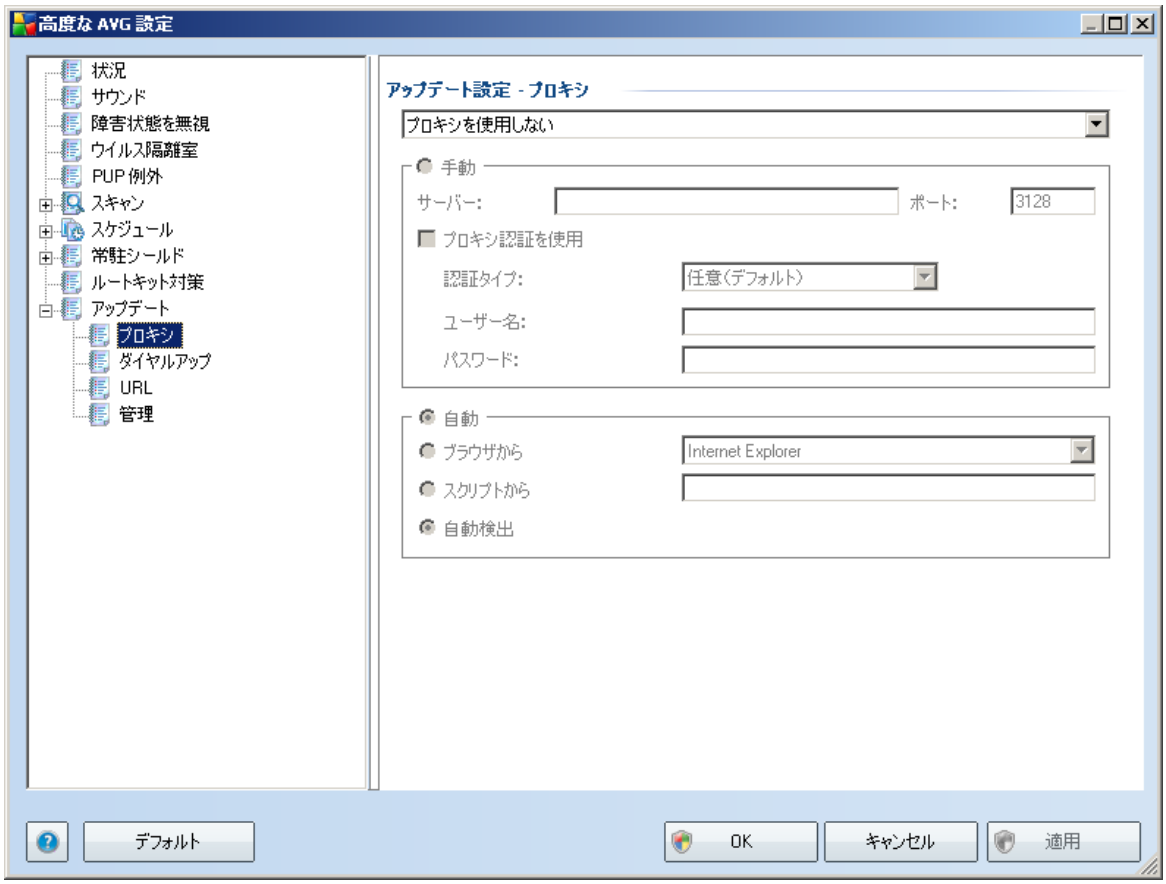
追加アップデートオプション

- *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。

9.9.1. プロキシ



プロキシサーバーとは、より安全なインターネット接続を保証するスタンドアロンサーバー、またはPC上のサービスです。特定のネットワークルールによって、インターネットに直接またはプロキシサーバーを介して接続できます。次に、*アップデート設*

*定 - プロキシ*ダイアログの最初のアイテムで、コンボボックスメニューから希望するものを選択する必要があります。

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

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

手動設定

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

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

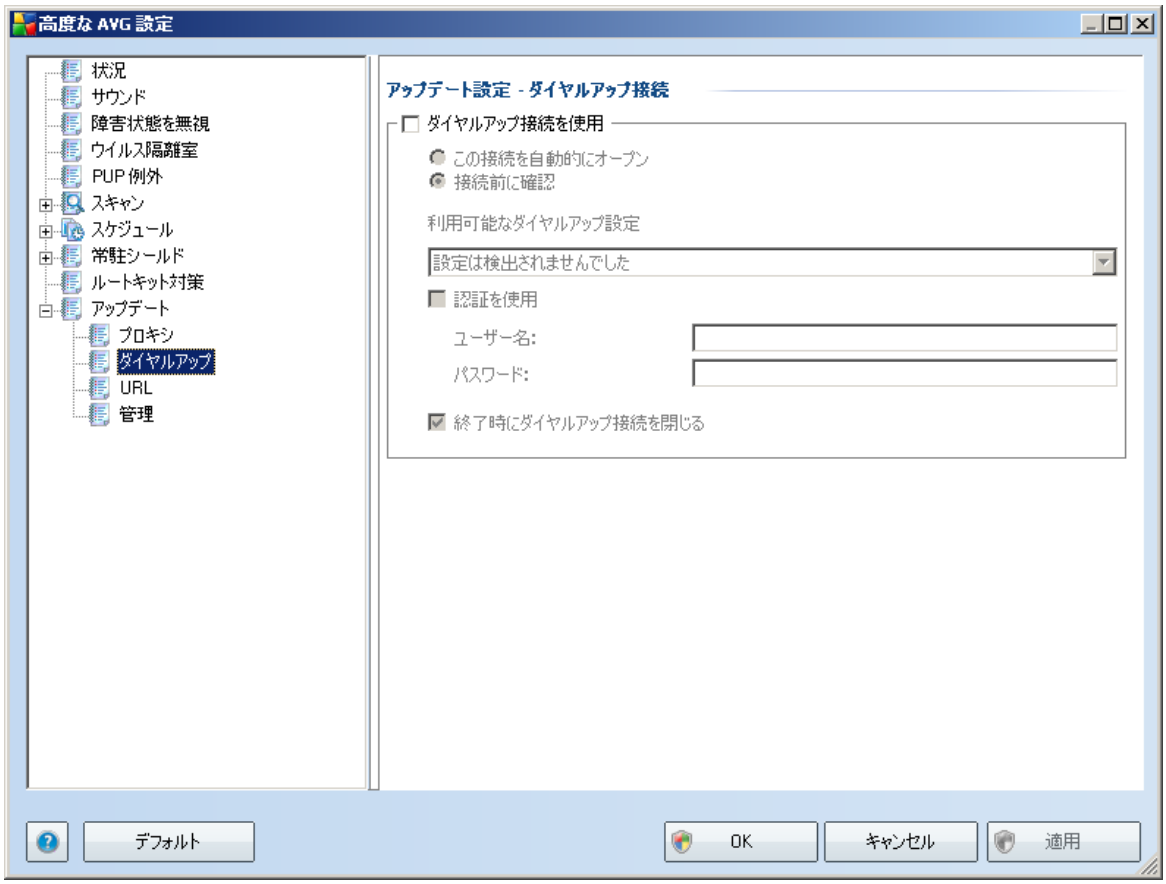
プロキシサーバーは、各ユーザーのルールを設定することもできます。プロキシサーバーがこのように設定されている場合、*プロキシ認証を使用*にチェックを付け、有効なユーザー名とパスワードを入力してください。

自動設定

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

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

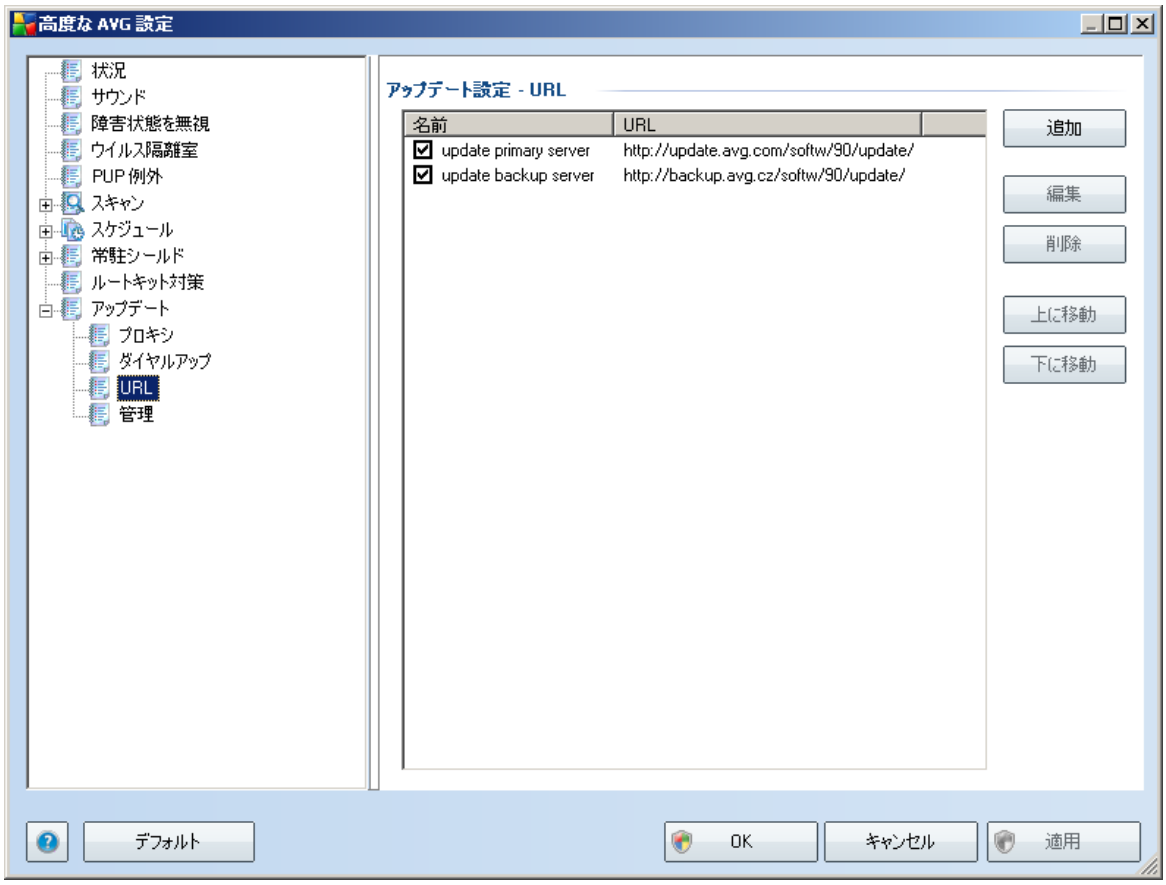
9.9.2. ダイヤルアップ



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

インターネットに自動接続（*自動的にこの接続をオープン*）するか、毎回手動で接続を確認（*接続前に確認*）するかを指定します。自動接続については、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*）。

9.9.3. URL

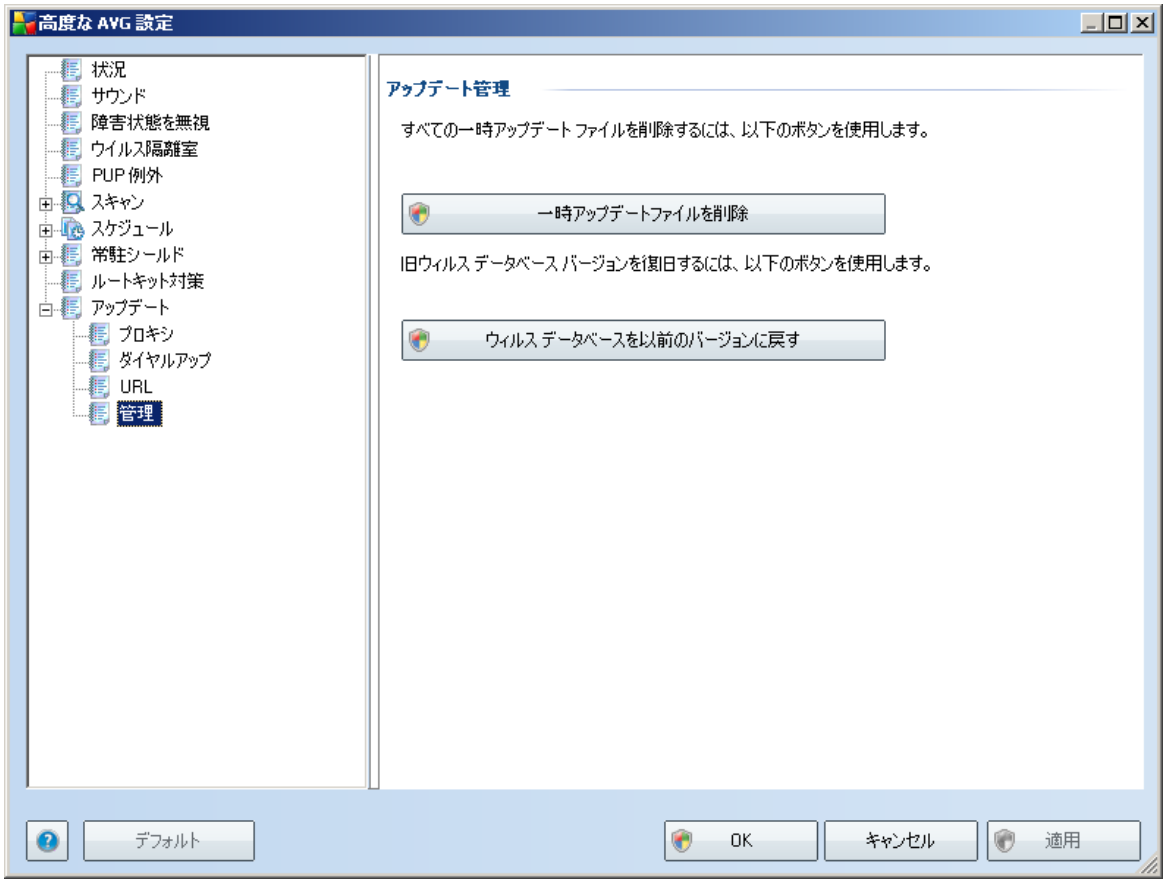


URLダイアログでは、アップデートファイルがダウンロードされるインターネットアドレスのリストが表示されます。このリストは、以下のコントロールボタンを使用して修正します。

- *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。

9.9.4. 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. AVGスキャン

スキャンは**AVG 9.0 File Server**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。

10.1. スキャンインターフェース

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

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

コントロールボタン

スキャンインターフェースで利用できるコントロールボタンは以下の通りです。

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

10.2. 定義済みスキャン

AVG 9.0 File Server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。

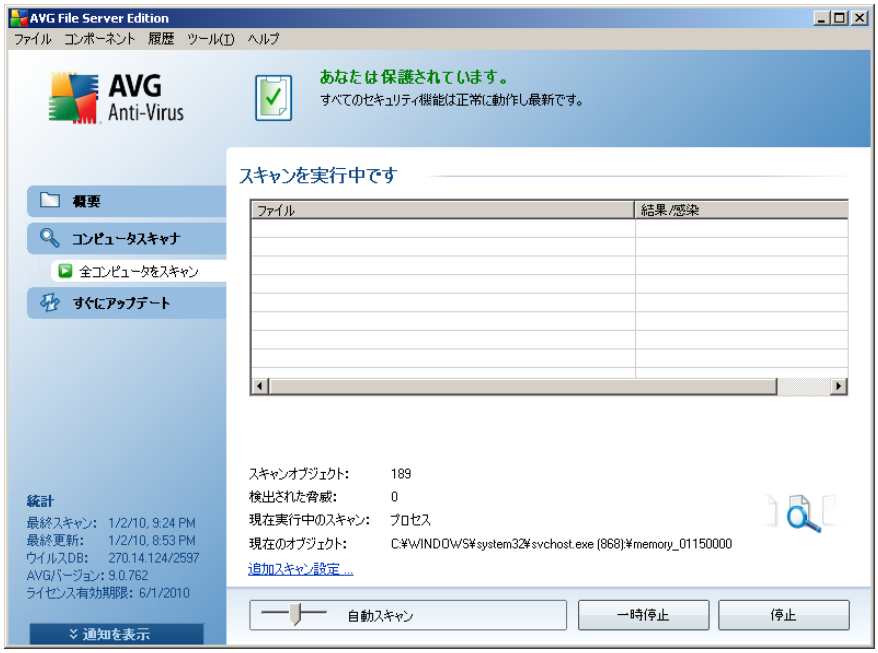
AVG 9.0 File Serverでは、次の種類のソフトウェアベンダによってあらかじめ定義されたスキャンが表示されます。

10.2.1. 全コンピュータをスキャン

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

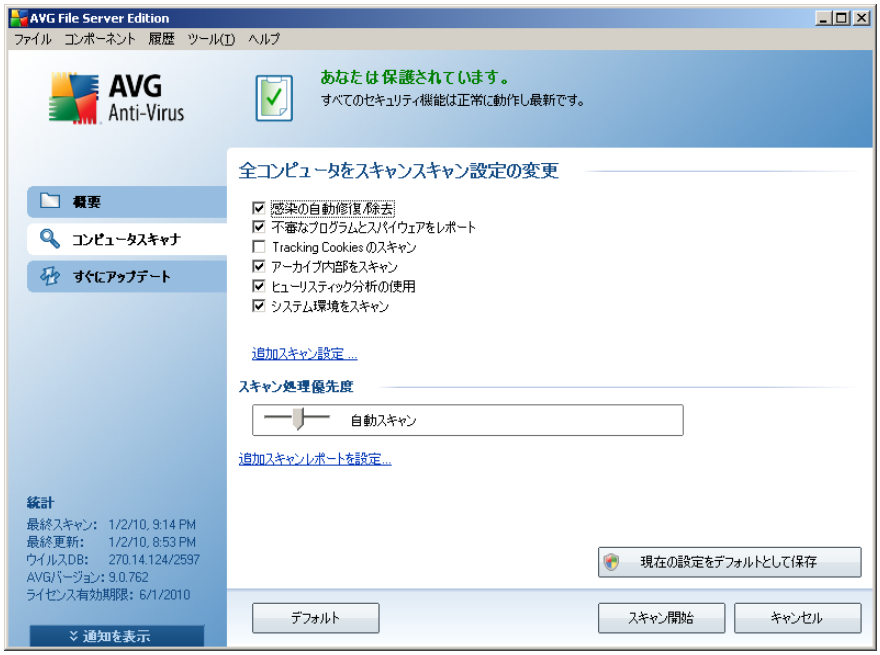
スキャン実行

*完全コンピュータスキャン*は、スキャンのアイコンをクリックして、スキャンインターフェースから直接実行することができます。このスキャンに対して、さらに特別な設定をする必要はありません。スキャンは*スキャン実行中*ダイアログ内で即時開始されます（*スクリーンショット*を参照）。必要に応じて、スキャンを一時的に中断（*一時中止*）、またはキャンセル（*停止*）することができます。



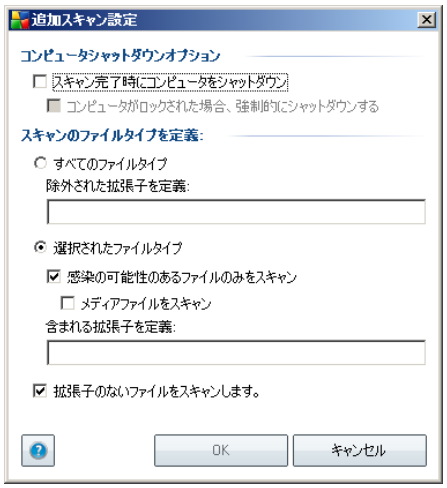
スキャン設定編集

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



- *スキャンパラメータ* - スキャンパラメータのリストでは、必要に応じて、特定のパラメータのオン/オフを切り替えることができます。デフォルトでは、ほとんどのパラメータがオンとなっており、スキャン中、自動的に使用されます。

- *追加スキャン設定* - このリンクからは、新しい [追加スキャン設定] ダイアログを開きます。このダイアログでは、次のパラメータを指定できます。



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

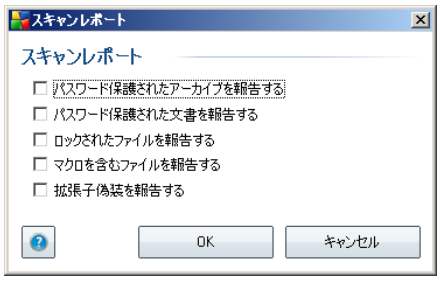
  - *すべてのファイルタイプと*スキャン対象ではないファイル拡張子をカンマで区切ったリストを入力することで、スキャンからの除外を定義できます。

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

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

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

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



警告：これらのスキャン設定は新規に定義されたスキャンパラメータと同一です- これは AVG スキャン / スキャンスケジュール / スキャン方法の章に記載されています。完全コンピュータスキャンのデフォルト設定を変更する場合、新しい設定をデフォルト設定として保存し、すべての完全コンピュータスキャンに使用することができます。

10.2.2. 特定のファイルとフォルダのスキャン

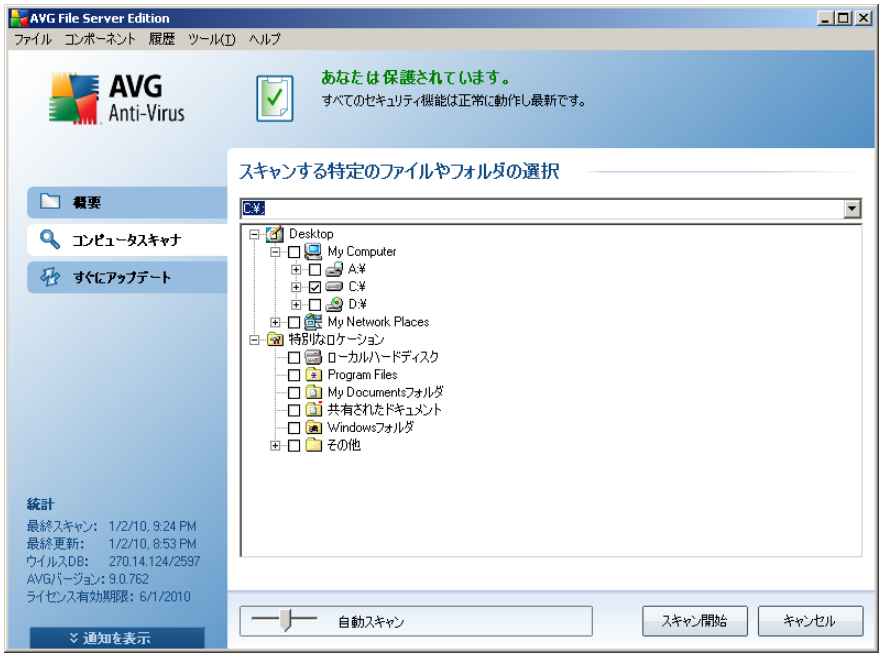
特定のファイルやフォルダをスキャン- 選択場所のみをスキャンします（*選択されたフォルダ、ハードディスク、フロッピーディスク、CD等*）. ウイルス検出、処置等のスキャン進捗*は、完全コンピュータスキャンと同じです。検出ウイルスは修復、またはウイルス隔離室に移動されます。* 特定のファイルやフォルダをスキャンは、ユーザー独自のスキャン設定とスケジュールのために使用されます。

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。

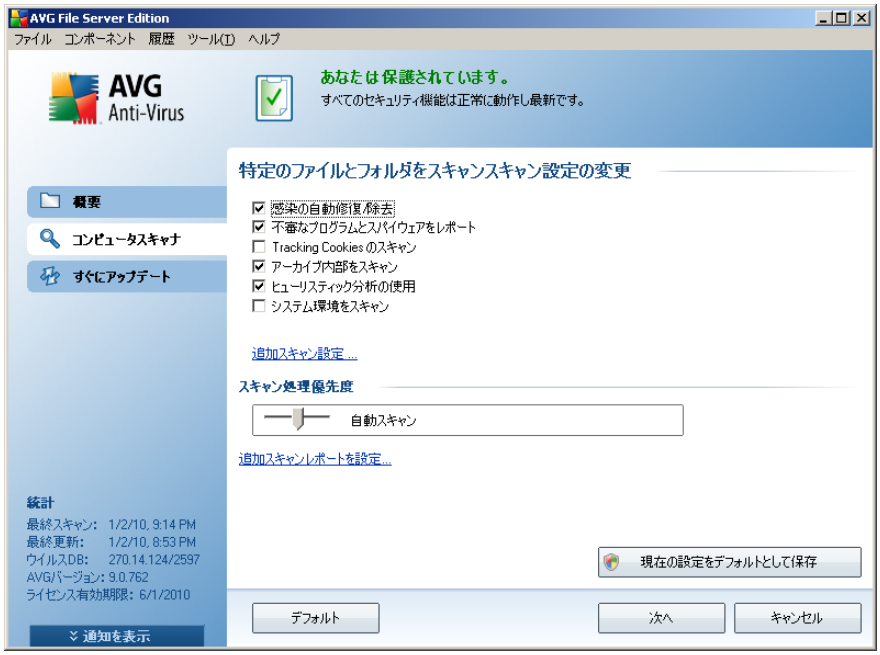
また、このスキャンからすべてのサブフォルダを除外する場合、自動生成されたパスの前にマイナス記号「-」を記述します（*スクリーションショットを参照*）。スキャンからフォルダ全体を除外するには「!」パラメータを使用します。

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



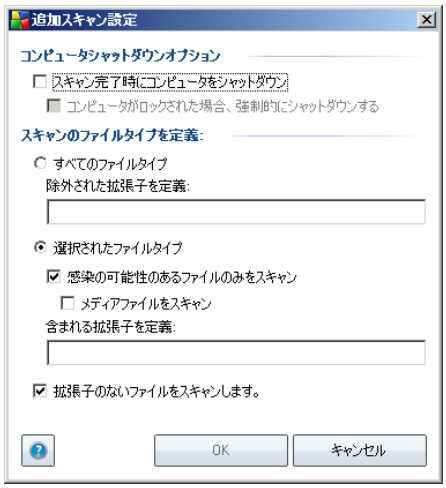
スキャン設定編集

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



- *スキャンパラメータ* - スキャンパラメータのリストでは、必要に応じて、特定のパラメータのオン/オフを切り替えることができます（*この設定の詳細説明については、AVG高度な設定/スキャン/特定のファイルとフォルダをスキャン*の章を参照してください）。

- *追加スキャン設定* - このリンクからは、新しい [追加スキャン設定] ダイアログを開きます。このダイアログでは、次のパラメータを指定できます。



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

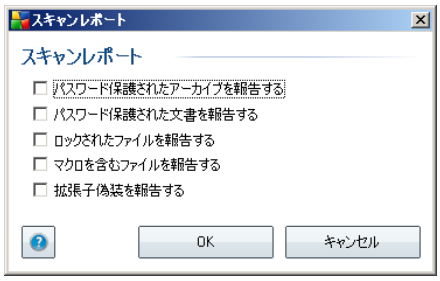
  - *すべてのファイルタイプと*スキャン対象ではないファイル拡張子をカンマで区切ったリストを入力することで、スキャンからの除外を定義できます。

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

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

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

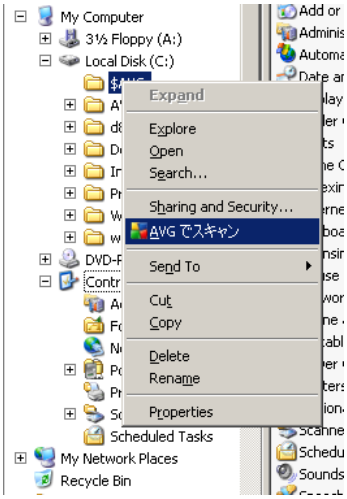
- *追加スキャンレポートを設定* - このリンクは、*スキャンレポート*ダイアログを開きます。このダイアログでは、レポートされる検出の種類を選択することができます。



警告：これらのスキャン設定は新規に定義されたスキャンパラメータと同一です- これは[AVG スキャン/スキャンスケジュール/スキャン方法](#)の章に記載されています。特定のファイルやフォルダスキャンのデフォルト設定を変更する場合、新しい設定をデフォルト設定として保存し、すべての特定のファイルやフォルダをスキャンに使用することができます。また、この設定はすべての新規スケジュールのテンプレートとして使用することができます（[すべてのカスタマイズされたスキャンは、現在のファイルやフォルダのスキャン設定に基づいています](#)）。

10.3. 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 9.0 File Server**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。

10.4. コマンドラインスキャン

AVG 9.0 File Server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。

10.4.1. CMDスキャンパラメータ

以下は、コマンドラインスキャンで利用可能なすべてのパラメータです。

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

- ***/IGNLOCKED*** ロックされたファイルを無視
- ***/REPORT*** ファイルにレポート/file name/
- ***/REPAPPEND*** レポートファイルに追加
- ***/REPOK*** 未感染ファイルを「OK」として報告する
- ***/NOBREAK*** CTRL-BREAKで中断しない
- ***/BOOT*** MBR/BOOT チェックを有効化
- ***/PROC*** アクティブプロセスをスキャンする
- ***/PUP*** 「不審なプログラム」を報告する
- ***/REG*** レジストリをスキャンする
- ***/COO*** cookieをスキャンする
- ***/?*** このトピックに関するヘルプを表示
- ***/HELP*** このトピックに関するヘルプを表示
- ***/PRIORITY*** スキャン優先度 (低、自動、高) を設定 (高度な設定 / Scans を参照)
- ***/SHUTDOWN*** スキャン完了時にコンピュータをシャットダウン
- ***/FORCESHUTDOWN*** スキャン完了時にコンピュータを強制シャットダウン
- ***/ADS*** Alternate Data Streams をスキャン(NTFSのみ)

10.5. スキャンスケジュール

AVG 9.0 File Serverでは、オンデマンドで(例えば、ウイルスに感染した場合)、あるいはスケジュールに基づいてスキャンを実行できます。スケジュールに基づいてスキャンを実行することを強く推奨します。この方法で、コンピュータが感染の可能性から保護されていることを保証でき、スキャンがいつ起動しているかを考える必要がありません。

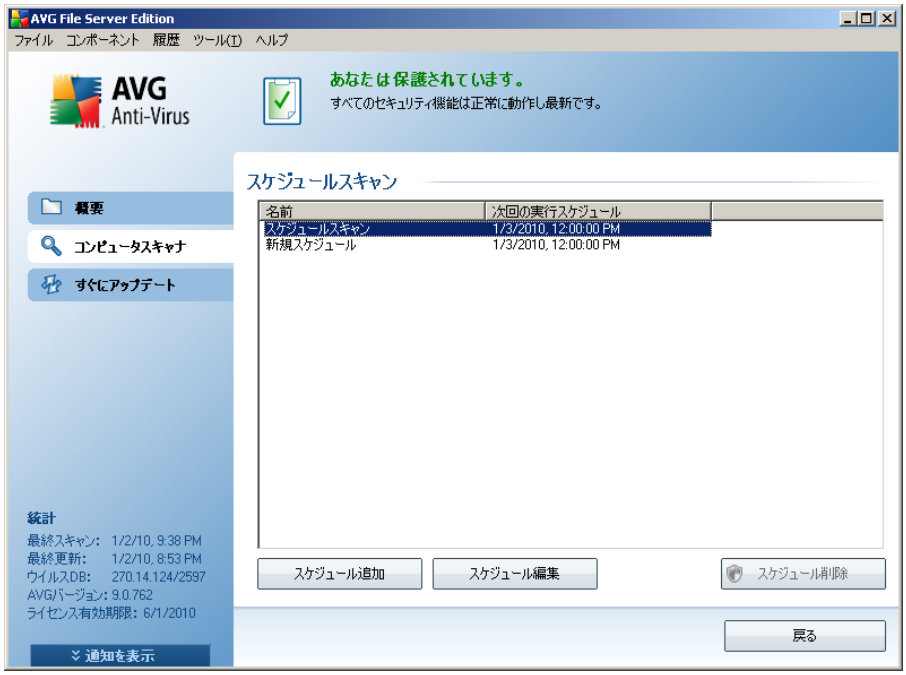
*全コンピュータをスキャン*を少なくとも週に1度定期的に実行して下さい。ただし、可能な場合は、コンピュータのスキャンを毎日行ってください。デフォルトのスキャンスケジュールはこのように設定されています。コンピュータが常にオンとなっている場

合、作業時間外にスキャンを実行するよう設定することができます。コンピュータがオフになり、スケジュールが実行されなかった場合、スケジュールは[コンピュータの起動時にスキャンを実行するように設定してください]

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

スケジュールスキャン

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



次のコントロールボタンを使用して、スキャンの編集および追加ができます。

- *スケジュール追加*- ボタンは*スケジュール済スキャン設定*ダイアログ、*スケジュール設定*タブを開きます。このダイアログでは、スキャンパラメータを指定することができます。
- *スケジュール編集*- このボタンは既存スケジュールを選択した場合にのみ使用されます。このボタンをクリックすると*スケジュール済スキャン設定*ダイアログ、*スケジュール設定*タブが表示されます。選択されたスキャンのパラメータを編集することができます。
- *スケジュール削除*- このボタンも既存スケジュールを選択した場合にのみ有効となります。選択したスキャンがリストから削除されます。ただし、自分で作成したスケジュールのみを削除できます。デフォルトで定義されている*スキャンスケジュール*は削除できません。
- *戻る* - AVG スキャンインターフェースに戻ります

10.5.1. スケジュール設定

新しいスキャンと通常の起動をスケジュールする場合、[*スケジュール済みの検査の設定*] ダイアログ ([*スキャンのスケジュール*] *ダイアログで* [*スキャンスケジュールの追加*] *ボタンをクリック*) を入力します。このダイアログは 3 つのタブに分けられ

ます。*スケジュール設定* - 以下の図を参照（自動的にリダイレクトされるデフォルトタブ）、*スキャン方法*、スキャン対象*****

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

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

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

10.5.2. スキャン方法

*スキャン方法*タブには、任意でオン/オフできるスキャンパラメータのリストが表示

されます。デフォルトでは、ほとんどのパラメータがオンになっており、その機能はスキャン実行中に適用されます。この設定を変更する合理的な理由がない場合は、予め定義された設定を維持することを推奨します。

- *自動感染修復/除去*- （*デフォルトではオン*）ウィルスがスキャン実行中に特定され、修復可能な場合は、自動で修復されます。感染ファイルを自動的に修復できない場合やこのオプションをオフにする場合、ウイルス検出が通知されるので、検出された感染の処理方法を決定する必要があります。推奨アクションは、感染ファイルの*ウイルス隔離室*への移動です。

- *不審なプログラムとスパイウェア脅威をレポート*- （*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。

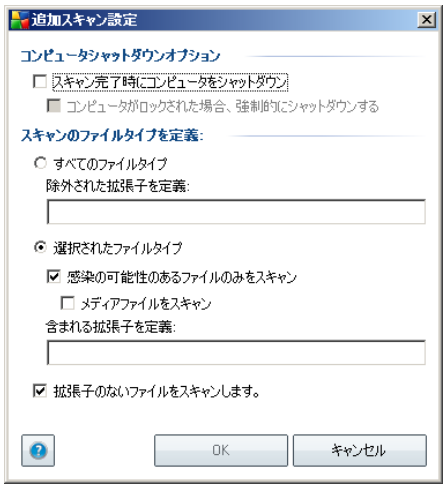
- *ヒューリスティック分析を使用*- （デフォルトではオン）ヒューリスティック分析（*仮想コンピュータ環境でのスキャンオブジェクトの動的エミュレーション*）は、スキャン実行中にウイルス検出に使用される方法の1つです。

- *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。

- *ルートキットをスキャン*- 完全コンピュータスキャン中にルートキットをスキャンする場合、この項目にチェックを付けます。また、ルートキットスキャンは*ルートキット対策*コンポーネントでも独自に行うことができます。

次の方法でスキャン設定を変更できます。

- *追加スキャン設定* - このリンクからは、新しい [追加スキャン設定] ダイアログを開きます。このダイアログでは、次のパラメータを指定できます。



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

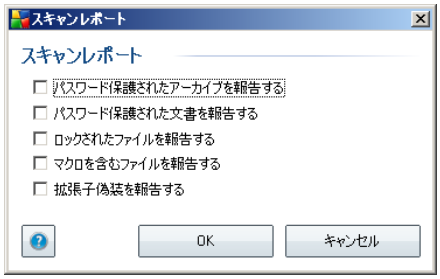
  - *すべてのファイルタイプ*とスキャン対象ではないファイル拡張子をカンマで区切ったリストを入力することで、スキャンからの除外を定義できます。

  - *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。

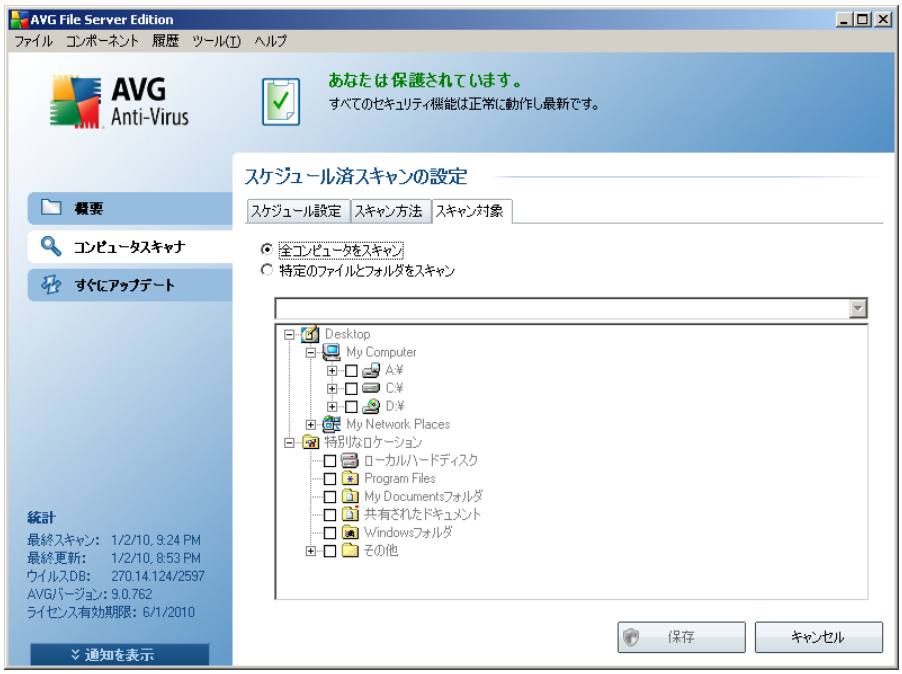
コントロールボタン

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。

10.5.3. 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。

10.6. スキャン結果概要

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

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

  緑のアイコンはスキャン中に感染が検出されなかったことを示します。

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

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

  各アイコンは完全な形、または半分のアイコンで表示されます。完全な形のアイコンは正常終了したスキャンを示しています。半分になったア

イコンはスキャンがキャンセルされたか中断されたことを示しています。

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

- *開始時間*- スキャンが実行された日時
- *終了時間*- スキャンが終了した日時
- *スキャン済オブジェクト*- スキャンでチェックされたオブジェクトの数
- *感染*- 検出/除去されたウイルス感染の数
- *スパイウェア*- 検出/除去されたスパイウェアの数
- *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。

10.7. 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。
- *ルートキット* - このタブは、スキャン実行中にルートキットが検出された場合にのみ表示されます。
- *情報* - このタブは潜在的な脅威が検出され、これらが上記のいずれのカテゴリにも分類できない場合にのみ表示されます。このタブでは警告メッセージが表示されます。

10.7.1. 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。

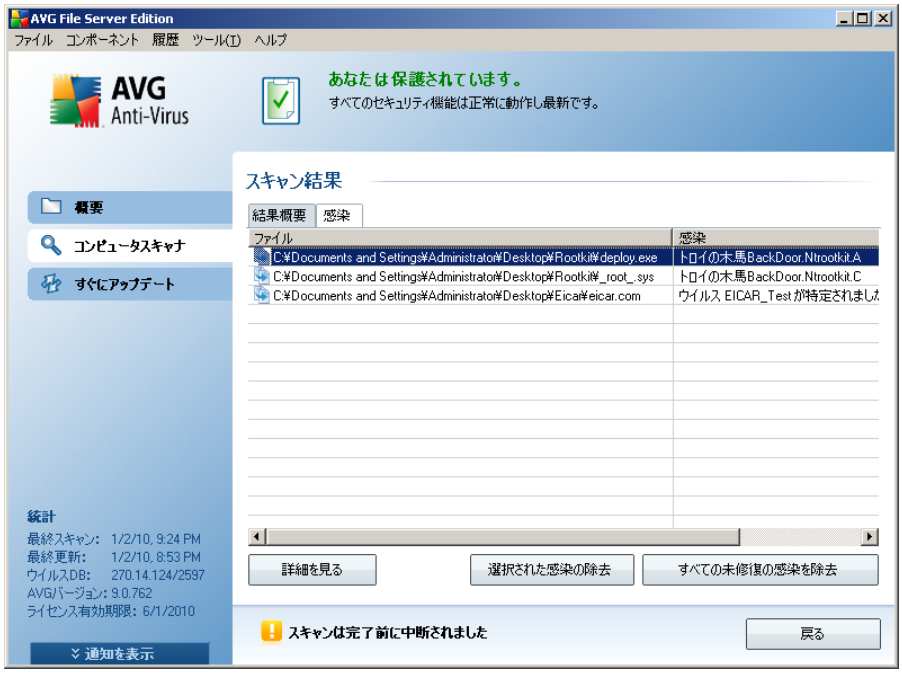
- 検出されたウイルス感染/スパイウェア
- 除去されたウイルス感染/スパイウェア
- 除去あまたは修復不可能なウイルス感染/スパイウェア数

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。

10.7.2. 感染タブ



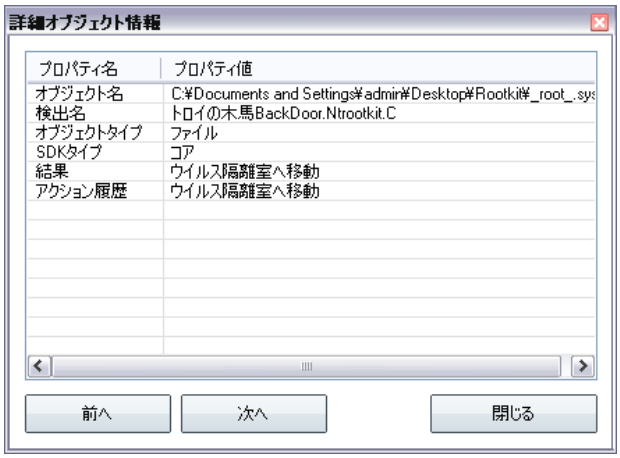
*感染*タブは、スキャン中にウイルス感染が検出された場合、*スキャン結果*ダイアログでのみ表示されます。***このタブは3つのセクションに分かれ、以下の情報が表示されます。

- *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。

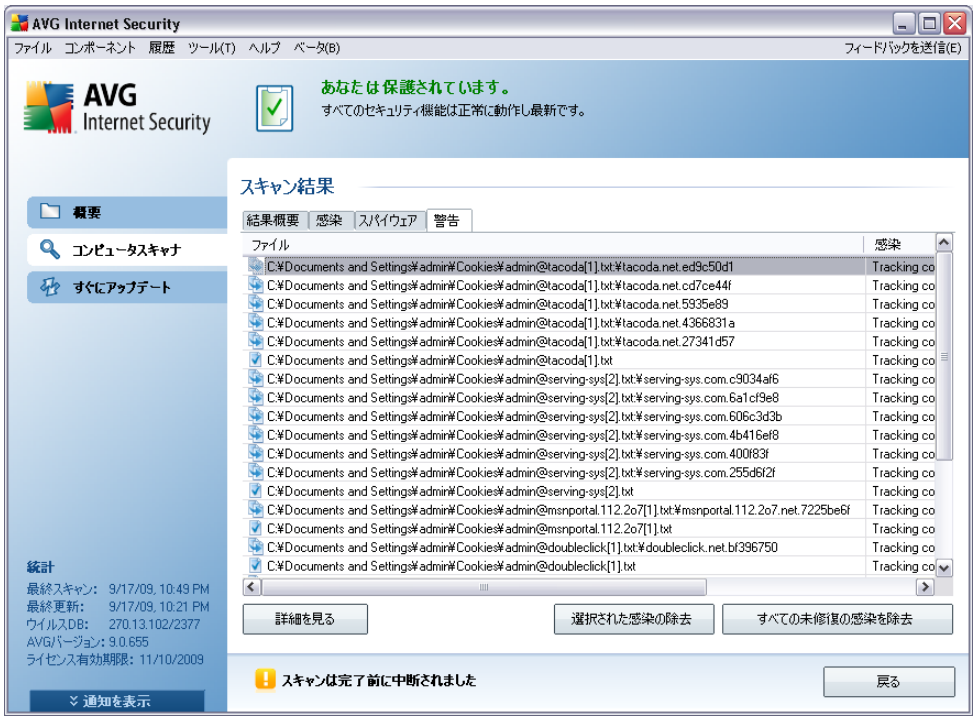
- *詳細を見る* - このボタンは [*詳細オブジェクト情報*] という新しいダイアログを開きます。



このダイアログでは、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。

10.7.3. スパイウェアタブ



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

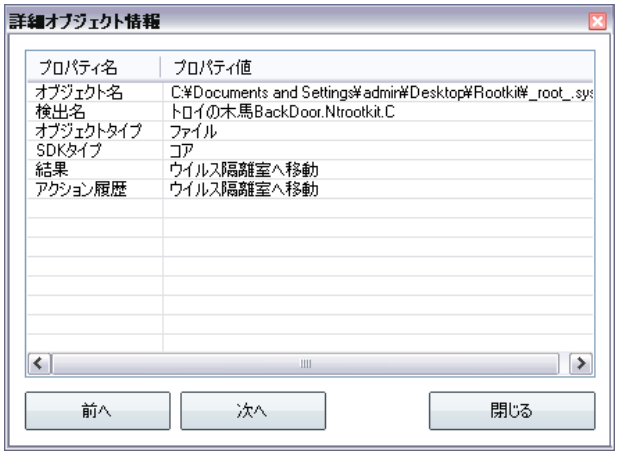
- *ファイル* - 感染オブジェクトの元の場所へのフルパス
- *感染* - 検出されたウイルス名（*ウイルスの詳細は、オンラインのウイルスエンサイクロペディアを参照してください*）
- *結果* - スキャン中に検出された感染オブジェクトの現在のステータス
    - *感染* - 感染オブジェクトが検出され、元の場所に存在します。（例えば、自動修復オプションを特定のスキャン設定でオフにしている場合）
    - *修復* - 感染オブジェクトは自動修復され、元の場所に存在しますす。
    - *ウイルス隔離室に移動* - 感染オブジェクトは*ウイルス隔離室に移動されました。*
    -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

- *PUP例外に追加* - 検出は例外として評価され、PUP例外リスト（*高度な設定のPUP例外ダイアログで設定*）に追加されました。
- *ロックされたファイル - 未スキャン* - 対象オブジェクトはロックされているため、AVGはスキャンできません。
- *潜在的に危険なオブジェクト* - オブジェクトは潜在的に危険なものとして検出されましたが、感染していません（例えば、マクロを含む等）。
- *アクションを終了するために再起動を要求* - 感染オブジェクトを除去できません。完全に除去するには、コンピュータの再起動が必要です。

コントロールボタン

このダイアログには3つのコントロールボタンがあります。

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



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

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

イルス隔離室に移動された検出を削除します。

- *結果を閉じる* - 詳細情報概要を終了し、*スキャン結果概要*ダイアログに戻ります。

10.7.4. 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スキャン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。

10.7.5. 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。

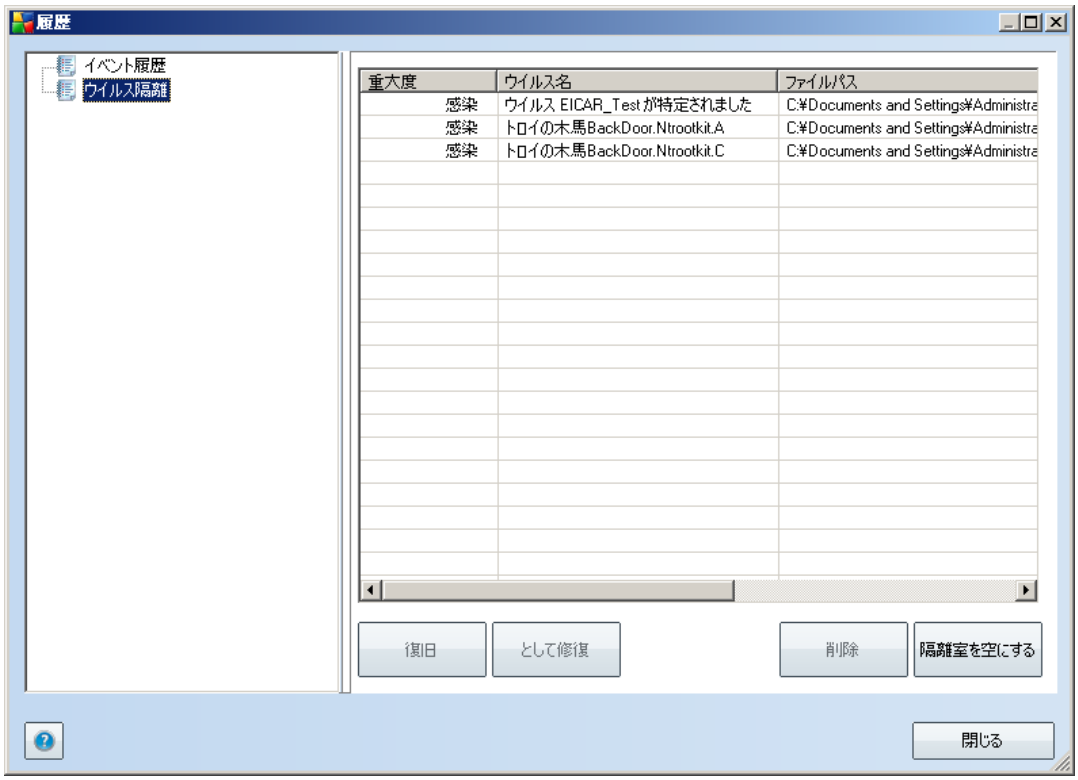
- *マクロを含んだ文書* - 報告された文書には、悪意のあるプログラムである可能性があるマクロが含まれます。

- *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*)。

10.8. 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。

11. 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。

11.1. アップデートレベル

AVG は、2 つの選択可能なアップデートレベルを提供します。

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

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

11.2. アップデートタイプ

2 つのタイプのアップデートを区別することができます。

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

11.3. アップデートプロセス

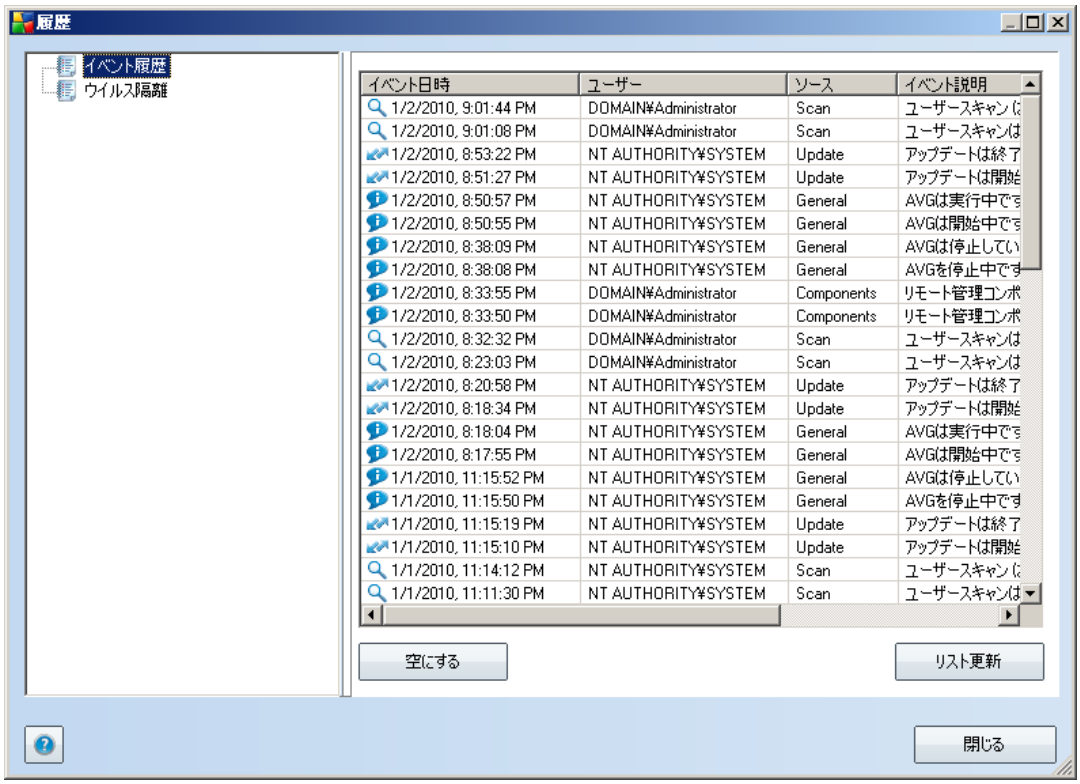
*すぐにアップデート*クイックリンクによって、アップデートプロセスをすぐに実行できます。このリンクは、AVGユーザーインターフェースダイアログからいつでも使用可能です。ただし、アップデートマネージャコンポーネントのアップデートスケジュール編集で説明されているように、定期的にアップデートを実行することが強く推奨されます。

アップデートを開始すると、AVGはまず利用可能な新しいアップデートファイルがあ

るかどうかを確認します。この場合、AVGはダウンロードを開始し、アップデートプロセスが実行されます。アップデートプロセス中は、*アップデート*インターフェースが表示されます。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。

12. 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 9.0 File Server**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

13. FAQとテクニカルサポート

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

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