AVG Internet Security 2015

ユーザーマニュアル

ドキュメント改訂 2015.03 (10/24/2014)

目次

1. はじめに

このユーザー マニュアルは、**AVG Internet Security 2015** の包括的なユーザー マニュアルです。

AVG Internet Security 2015 は複数の保護機能を備え、あらゆるオンライン活動からユーザーを守ります。ユーザーは ID 窃盗、ウイルス、有害なサイトへのアクセスについて心配せずにすみます。AVG 保護クラウド技術とAVG コミュニティ保護ネットワークが導入されています。この機能では、AVG が最新の脅威情報を収集し、その情報をコミュニティで共有することで、最高レベルの保護を提供します。ユーザーは安全にオンライン ショッピングやバンキングを利用できます。リアルタイム保護により、ソーシャル ネットワークやインターネットでの閲覧・検索を安心して楽しむことができます。

その他の情報ソースを使用することも可能です。

- ***ヘルプ ファイル***: *トラブルシューティング セクションは、**AVG Internet Security 2015**に含まれるヘルプファイルで直接使用可能です（ヘルプ ファイルを開くには、アプリケーションのダイアログで F1 キーを押します）。*このセクションには、ユーザーが技術的な問題について専門家のヘルプを検索するときに最も多く発生している状況の一覧が表示されます。現在発生している問題に最も近い状況を選択してクリックすると、問題の解決策を示す詳細手順が表示されます。

- ***AVG ウェブサイトのサポート センター***: AVG ウェブサイト（http://www.avg.com/）で問題の解決策を検索することもできます。「***サポート***」セクションには、販売上の問題と技術的な問題の両方を取り扱うテーマ別のグループの概要、よくある質問の体系的なセクション、および利用可能なすべての連絡先が掲載されています。

- ***AVG ThreatLabs***: AVG 関連の専門ウェブサイト（http://www.avg.com/about-viruses）であり、ウイルス問題に特化し、オンラインの脅威についての概要を提供します。また、ウイルスやスパイウェアの駆除手順や脅威に対する保護方法の提案も確認できます。

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

2. AVG インストール要件

2.1. 対応オペレーティング システム

AVG Internet Security 2015 は、次のオペレーティング システムで稼動するワークステーションの保護を目的としています。

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista（x86 および x64、すべてのエディション）
- Windows 7（x86 および x64、すべてのエディション）
- Windows 8（x86 および x64、すべてのエディション）

（また、特定のオペレーティング システム用サービス パック）

注意: *Identity コンポーネントは Windows 2000 および XP x64 ではサポートされていません。これらのオペレーティング システムでは、AVG Internet Security 2015 のインストールはできますが、Identity protection コンポーネントのインストールはできません。*

2.2. 最低および推奨ハードウェア要件

AVG Internet Security 2015 の必須ハードウェア要件：

- Intel Pentium CPU 1.5 GHz 以上
- 512 MB (Windows XP) / 1024 MB (Windows Vista、Windows 7) の RAM メモリ
- 1.3 MB のハードディスク空き領域　*（インストール用）*

AVG Internet Security 2015 の推奨ハードウェア要件：

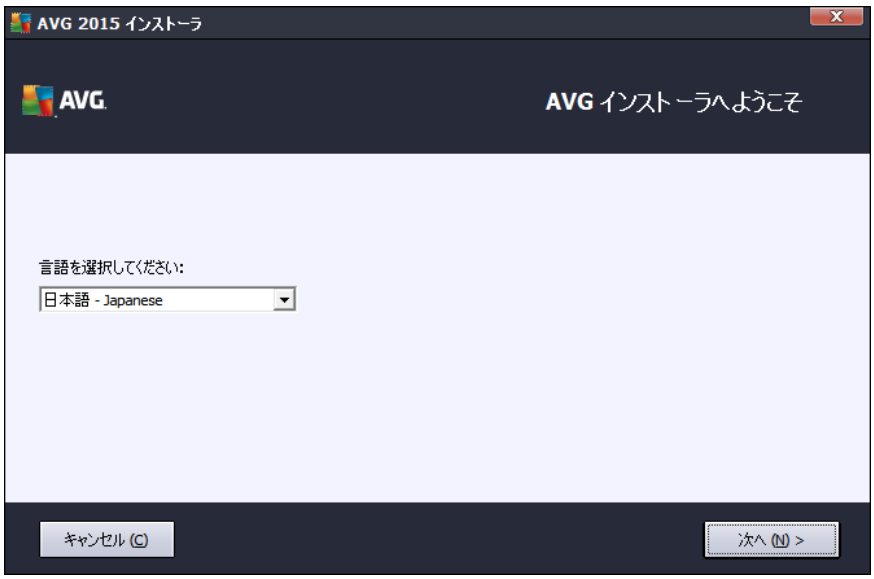
- Intel Pentium CPU 1.8 GHz 以上
- 512 MB (Windows XP) / 1024 MB (Windows Vista、Windows 7) の RAM メモリ
- 1.6 MB のハードディスク空き領域　*（インストール用）*

3. AVG インストール処理

コンピュータにAVG Internet Security 2015 をインストールする場合は、最新のインストール ファイルを取得する必要があります。最新バージョンの AVG Internet Security 2015 を確実にインストールするために、AVG Web サイト(http://www.avg.com/)からインストール ファイルをダウンロードすることをお勧めします。[***サポート***] セクションには、各 AVG 製品のインストール ファイルの体系的な概要が表示されます。インストールファイルをハードディスクにダウンロードして保存した後、インストール プロセスを実行できます。インストールは一連のシンプルでわかりやすいダイアログから構成されています。各ダイアログではインストール処理の各ステップの概要を説明しています。各ダイアログ ウィンドウの詳細については次のとおりです。

3.1. ようこそ :言語の選択

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

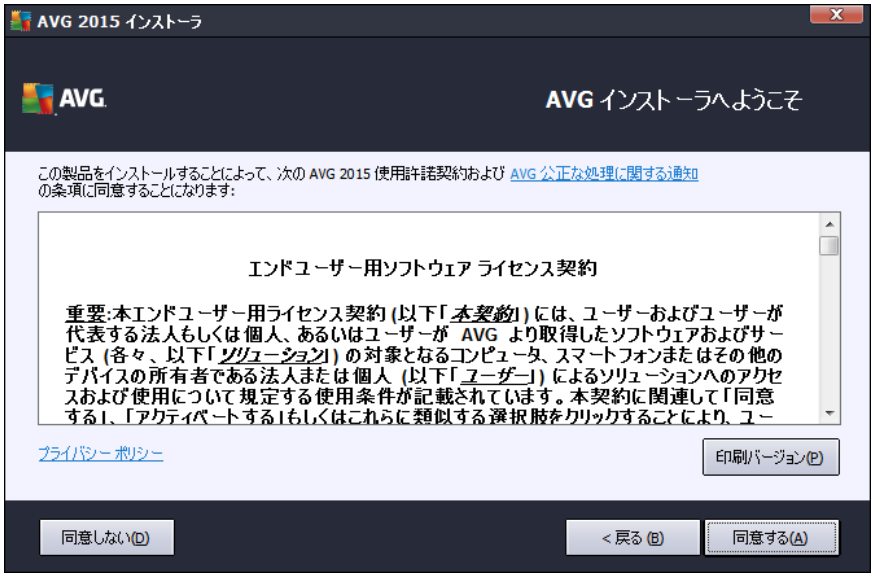


このダイアログでは、インストール処理で使用する言語を選択できます。コンボ ボックスをクリックすると、言語メニューがロールダウンします。任意の言語を選択すると、選択した言語でインストール処理が続行します。

注意 :この時点では、インストール処理の言語のみを選択しています。AVG Internet Security 2015 アプリケーションは選択した言語でインストールされます。英語は必ず自動的にインストールされます。ただし、その他の言語をインストールして、AVG Internet Security 2015 で使用することもできます。次の [カスタム オプション] 設定ダイアログの 1つでは、別の言語を選択できます。

3.2. ようこそ :ライセンス使用許諾契約

[***AVG インストーラへようこそ***] ダイアログでは、AVG ライセンス契約の全文が表示されます。



契約内容の全体をよくお読みください。全文をよく読み、内容を理解した上で、この使用許諾契約に同意する場合は、[***同意する***] ボタンをクリックします。使用許諾契約に同意しない場合は、[***同意しない***] ボタンをクリックします。インストール処理がただちに中断されます。

AVG 公正取扱通知およびプライバシー ポリシー

ライセンス契約の他に、このセットアップ ダイアログでは ***AVG 公正取引通知***および***ライセンス ポリシー***の詳細も確認できます。詳しい情報を見ることができるウェブサイトへのアクティブなハイパーリンクとして、ここで紹介された機能はダイアログ内に表示されます。各リンクをクリックすると、AVG Web サイト (http://www.avg.com/)に移動し、これらのデフォルトの全文を確認できます。

コントロール ボタン

最初のセットアップ ダイアログでは、以下のコントロール ボタンが利用できます。

- ***印刷バージョン*** - このボタンをクリックすると、AVG ライセンス契約の全文を、印刷に適した配置でウェブ上に表示します。
- ***拒否*** - クリックすると、ライセンス契約を拒否します。セットアップ処理はただちに終了します。**AVG Internet Security 2015** はインストールされません！
- ***戻る*** - クリックすると、1つ前のセットアップ ダイアログに戻ります。
- ***同意*** - クリックすると、ライセンス契約を読んで理解して同意したことを確認します。インストールは続行され、次のセットアップ ダイアログに進みます。

3.3. ライセンスをアクティベート

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

どこでライセンス番号を見つけることができますか

セールス番号は、**AVG Internet Security 2015** ボックスの CD パッケージに記載されています。ライセンス番号は **AVG Internet Security 2015** 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する必要があります。デジタル形式のライセンス番号が利用できる（*メールに記載*）場合は、コピーと貼り付けを使用して入力することを推奨します。

コピーと貼り付け機能を使用する方法

コピーと貼り付け機能を使用して **AVG Internet Security 2015** ライセンス番号をプログラムに入力することで、番号を確実に正しく入力できます。次の手順を実行してください。

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

コントロール ボタン

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

- ***キャンセル*** - クリックすると、ただちにセットアップ処理を中止します。**AVG Internet Security 2015** はインストールされません。
- ***戻る*** - クリックすると、1つ前のセットアップ ダイアログに戻ります。
- ***次へ*** - クリックすると、インストールを続行し、1つ次のステップに進みます。

3.4. インストール種別の選択

[***インストール種別の選択***] ダイアログでは、[***エクスプレス インストール***] と[***カスタム インストール***] の2つのインストール オプションから選択できます。

エクスプレス インストール

ほとんどのユーザーには、標準の***エクスプレス***インストールの選択を強くお勧めします。この方法では **AVG Internet Security 2015** は完全自動モードで、プログラム ベンダーがあらかじめ定義した設定でインストールされます。この設定は、最適なリソース消費で最大のセキュリティを実現します。将来的には、設定の変更の必要が生じた場合、常に **AVG Internet Security 2015** アプリケーションで直接変更できます。

[***次へ***] ボタンをクリックすると、次のインストール処理のダイアログに進みます。

カスタムインストール

カスタムインストールは、**AVG Internet Security 2015** を標準設定でインストールしない妥当な理由がある場合（特定のシステム要件への適合など）経験のあるユーザーのみが行ってください。この方法に決定した場合、ダイアログで ***インストール先 フォルダ***の新しい部分が有効に成ります。ここでは、**AVG Internet Security 2015** のインストール場所を指定します。既定では、ダイアログのテキスト フィー

ルドに記載されているように **AVG Internet Security 2015** は C:ドライブの Program Files フォルダにインストールされます。この場所を変更する場合は、[***参照***] ボタンを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。ソフトウェア ベンダーが事前設定したデフォルトのインストール先に戻すには、[***デフォルト***] ボタンをクリックします。

[***次へ***] ボタンをクリックして、[カスタム オプション] ダイアログに進みます。

コントロール ボタン

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

- ***キャンセル*** - クリックすると、ただちにセットアップ処理を中止します。**AVG Internet Security 2015** はインストールされません。
- ***戻る*** - クリックすると、1つ前のセットアップ ダイアログに戻ります。
- ***次へ*** - クリックすると、インストールを続行し、1つ次のステップに進みます。

3.5. カスタム オプション

カスタム オプション ダイアログではインストールの詳細なパラメータが設定できます。

[***コンポーネント選択***] セクションには、インストール可能なすべての **AVG Internet Security 2015** コンポーネントの概要が表示されます。デフォルト設定が適当でない場合、特定のコンポーネントを削除 / 追加することができます。***ただし、選択できるコンポーネントは購入した AVG 製品に含まれているコンポーネントのみです。*** [***コンポーネント選択***] リストの項目を強調表示すると、該当するコンポーネントの簡単な説明がこのセクションの右側に表示されます。各コンポーネントの機能に関する詳細については、このマニュアルの「コンポーネント概要」の章を参照してください。ソフトウェア ベンダーが事前設定した既定の設定に戻すには、[***既定***] ボタンをクリックします。

この手順では、製品のデフォルトの言語ではなく、別の言語を選択することもできます *(デフォルトでは、アプリケーションは設定に使用する言語としてユーザーが選択した言語、および英語でインストールされます)*

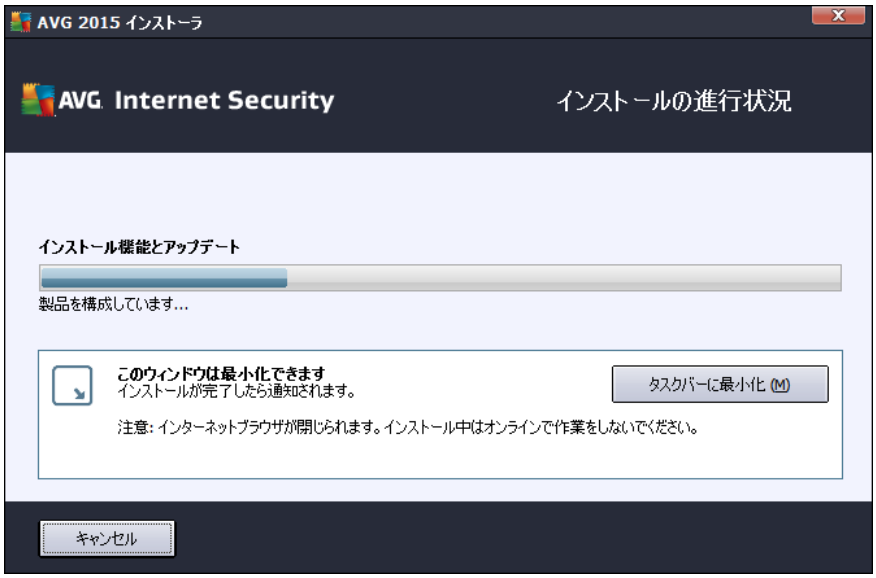
コントロール ボタン

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

- ***キャンセル*** - クリックすると、ただちにセットアップ処理を中止します。**AVG Internet Security 2015** はインストールされません。
- ***戻る*** - クリックすると、1つ前のセットアップ ダイアログに戻ります。
- ***次へ*** - クリックすると、インストールを続行し、1つ次のステップに進みます。

3.6. インストールの進行状況

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



インストール処理の終了後、次のダイアログに自動的に進みます。

コントロール ボタン

このダイアログにはコントロール ボタンが 2つあります。

- ***最小化*** - インストール処理には数分かかる場合があります。ボタンをクリックすると、ダイアログ ウィンドウを最小化してシステム バー上にアイコンとして表示できます。インストールが完了すると、ダイアログが再度表示されます。
- ***キャンセル*** - このボタンを使用するのは、現在のインストール処理を停止する場合のみです。キャンセルすると、**AVG Internet Security 2015** はインストールされません。

3.7. おめでとうございます。

おめでとうございます。 **AVG Internet Security 2015**が正 常 にインストールおよび設 定 されたことを確認 できます。

製 品 改 善 プログラムおよび プライバシー ポリシー

このダイアログでは、***製 品 改 善 プログラム*** (*詳細 については、AVG 高 度 な設 定 製 品 改 善 プログラム* の章 を参 照)に参 加 するかどうかを決 定 します。このプログラムでは、全 体 的 なインターネット セキュリティレベルを高 める目 的 で、検 出 された脅 威 に関 する匿 名 の情 報 を収 集 します。すべてのデータは AVG のプライバシー ポリシーに従 って機 密 として処 理 されます。***プライバシー ポリシー*** リンクをクリックすると、AVG Web サイト (http://www.avg.com/)に移 動 し、AVG のプライバシー ポリシー規 定 の全 文 を確認 できます。この内 容 に同 意 する場 合 は、オプションを選 択 してください *(既 定 ではこのオプションが選 択 されています)*。

[***終 了***] ボタンをクリックして、インストール処 理 を完 了 します。

4. インストール後

4.1. 製品登録

AVG Internet Security 2015 のインストールが終了したら、AVG Web サイト(*http://www.avg.com/*)でオンライン製品登録を行ってください。登録後、AVG ユーザー アカウント、AVG アップデート ニュースレター、その他登録ユーザーのみに提供されるサービスが利用できるようになります。最も簡単な登録方法は、**AVG Internet Security 2015** ユーザー インターフェースから直接行う方法です。上の行の [ナビゲーション /オプション /今すぐ登録] の項目を選択してください。AVG Web サイト(*http://www.avg.com/*) の [***登録***] ページに移動します。ページ上の指示にしたがってください。

4.2. ユーザー インターフェースへのアクセス

AVG メイン ダイアログには複数の方法でアクセスできます。

- AVG システム トレイ アイコン
- デスクトップの AVG アイコンをダブルクリックします。
- メニューから、***スタート /すべてのプログラム /AVG / AVG 2015***

4.3. 全コンピュータをスキャン

AVG Internet Security 2015 のインストール前にコンピュータがウイルスに感染していた可能性あります。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。最初のスキャンにはかなりの時間 *(1 時間程度)*を要することがありますが、コンピュータが脅威にさらされていないことを確認するため、スキャンの実行をお勧めします。 全 コンピュータをスキャンを実行する方法については、AVG スキャンの章を参照してください。

4.4. Eicar 検査

AVG Internet Security 2015 が正常にインストールされたことを確認するために、EICAR テストを実行できます。

EICAR テストは、ウイルス対策システムの動作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、**AVG Internet Security 2015** が警告とともにそれに反応します。この通知は、AVG が正常にコンピュータにインストールされていることを証明します。

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

4.5. AVG の既定の設定

AVG Internet Security 2015 *の既定の設定* ***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***) 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ソフトウェア ベンダーによって設定されています。***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 設定を変更する必要がある場合、AVG 高度な設定 *に移動します。メインメニューの [オプション 高度な設定*] 項目を選択し、新しく開いた AVG 高度な設定ダイアログで AVG 設定を変更します。

5. AVG ユーザー インターフェース

AVG Internet Security 2015 メイン ウィンドウが開きます。

メインウィンドウは複数のセクションに分けられます。

- ***上部の行 ナビゲーション***は、メイン ウィンドウの上部セクションに並んだ 4つのアクティブなリンクで構成されます *(AVG は気に入っていますか？、レポート、サポート、オプション)*。詳細 >>
- ***セキュリティステータス情報***には、現在の **AVG Internet Security 2015** のステータスの基本情報が表示されます。詳細 >>
- ***インストールされたコンポーネント概要*** は、メイン ウィンドウの中央セクションの中の水平の細長いブロックに表示されます。コンポーネントは、各コンポーネントのアイコンが付いたライトグリーンのブロックとして表示されます。また、コンポーネントのステータス情報も合わせて表示されます。詳細 >>
- ***マイ アプリケーション***は、メイン ウィンドウの中央下部の細長い部分に図で表示され、既にコンピュータにインストールされているか、インストールが推奨される追加の **AVG Internet Security 2015** アプリケーションの概要を示します。詳細 >>
- ***スキャン /アップデートのクイックリンク***はメイン ウィンドウ下部のブロック行に配置されています。これらのボタンを使うと、最も重要で頻繁に使用する AVG の機能にすぐにアクセスできます。詳細 >>

AVG Internet Security 2015のメインウィンドウの外側に、アプリケーションにアクセスするために使用するもう一つのコントロール エレメントがあります。

- ***システム トレイ アイコン***は、モニター右下端に位置し *(システム トレイ上)*、現在の **AVG Internet Security 2015** の状態を示します。詳細 >>

5.1. 上部の行ナビゲーション

上部の行ナビゲーションは、メイン ウィンドウの上部セクションに複数のアクティブなリンクが並んで構成されています。ナビゲーションには次のボタンが含まれます。

5.1.1. Facebook で AVG に参加

このリンクをクリックすると、インターネット セキュリティを最大限に高めるための最新の AVG 情報、ニュース、ヒント、秘訣などを共有する、AVG Facebook コミュニティに接続します。

5.1.2. レポート

新しい***レポート***ダイアログを開くと、以前に実行したスキャンとアップデート処理の関連レポートの概要がすべて表示されます。スキャンまたはアップデートが現在実行中の場合、メイン ユーザー インターフェースの上部ナビゲーションの中にある***レポート***の文字の隣に回転中の円の形が表示されます。この円をクリックすると、実行中の処理の進捗を示すダイアログに移動します。

5.1.3. サポート

4 つのタブ構成の新しいダイアログを開くと、**AVG Internet Security 2015** に関連するすべての情報が表示されます。

- ***ライセンスとサポート*** - このタブには製品名、ライセンス番号、有効期限が表示されます。ダイアログの下部にはご利用いただけるすべてのカスタマーサポートの連絡先の概要が順に明記されています。タブでは次のアクティブ リンクとボタンが使用できます。

  - *(再) アクティベート* - クリックすると新しい [***AVG アクティベート ソフトウェア***] ダイアログが開きます。該当するフィールドにライセンス番号を入力してセールス番号 *(AVG Internet Security 2015 のインストール中に使用した番号)* を置き換えるか、現在のライセンス番号を別の番号に変更します *(上位の AVG 製品にアップグレードする場合など)*。

  - *クリップボードにコピー* - このリンクを使ってライセンス番号をコピーし、必要な場所に貼り付けます。この方法でライセンス番号を正しく確実に入力できます。

  - *今すぐ更新* - 少なくとも、現在のライセンスが切れる 1ヶ月前の適切な時期に **AVG Internet Security 2015** ライセンス更新を購入することを推奨します。有効期限が近づくと通知されます。このリンクをクリックすると AVG ウェブサイト *(http://www.avg.com/)* に移動し、ライセンス状況、有効期限、更新 *アップグレード*の提供についての詳細な情報が表示されます。

- ***製品*** - このタブでは、製品情報、インストール済みコンポーネント、インストール済みのメール保護、システム情報など、**AVG Internet Security 2015** の最も重要な技術データの概要を提供します。

- ***プログラム*** - このタブでは、プログラム ファイルのバージョン情報、および製品に使用されているサードパーティ コード情報を参照できます。

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

5.1.4. オプション

AVG Internet Security 2015 のメンテナンスには、[***オプション***] 項目からアクセスできます。矢印をクリックすると、ロールダウン メニューが開きます。

- ***コンピュータ スキャン*** 全コンピュータをスキャンを実行します。
- ***選択されたフォルダをスキャン ...*** - AVG スキャン インターフェースに切り替わり、コンピュータのツリー構造からスキャンするファイルとフォルダを設定できます。
- ***ファイルスキャン ...*** - 特定のファイルを 1つ指定してオンデマンド テストを実行できます。このオプションをチェックすると、新しいウィンドウが開いてデスクトップのツリー構造が表示されます。対象のファイルを選択し、スキャンの実行を確認します。
- ***アップデート*** - **AVG Internet Security 2015** のアップデート処理を自動的に実行します。
- ***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。インターネットに接続できない場合（たとえば、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、コンピュータはあるネットワークに接続されているがインターネットへアクセスができない場合など）がその例です。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。
- ***ウイルス隔離室*** - AVG が検出したすべての感染ファイルを削除して保存する隔離スペース、「ウイルス隔離室」のインターフェースを開きます。隔離室内では、感染ファイルは隔離され、コンピュータの安全は保証されます。同時に感染ファイルは将来の修復に備えて保存されます。
- ***履歴*** - さらに詳細なサブメニュー オプションを提供します。
  - *スキャン結果* - スキャン結果の概要を表示するダイアログが開きます。
  - *常駐シールドの結果* - 常駐シールドによって検出された脅威の概要が表示されるダイアログを開きます。
  - *Identity Protection の結果* - Identity コンポーネントによって検出された脅威の概要が表示されるダイアログを開きます。
  - *メール保護の結果* - メール保護コンポーネントによって危険とみなされ、検出されたメールの添付ファイルの概要が表示されるダイアログを開きます。
  - *オンライン シールドの結果* - オンライン シールドによって検出された脅威の概要が表示されるダイアログを開きます。
  - *イベント履歴ログ* - すべてのログに記録された **AVG Internet Security 2015** アクションの概要を表示する履歴ログ インターフェースを開きます。
  - *ファイアウォール ログ* - すべてのファイアウォールの活動の詳細な概要を表示するダイアログが開きます。
- ***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 Internet Security 2015** の設定を編集できます。通常はソフトウェア ベンダーが定義している既定のアプリケーション設定の使用をお勧めします。

- ***ファイアウォール設定 ...*** - ファイアウォール コンポーネントの高度な設定のダイアログを開きます。
- ***ヘルプの内容*** - AVG ヘルプ ファイルを開きます。
- ***サポートを利用する*** - サポート ダイアログを開き、アクセス可能なすべての連絡先とサポート情報を表示します。
- ***AVG Web サイト*** - 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百科事典をAVG ウェブサイトから開きます (*http://www.avg.com/*)。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。
- ***アクティベート*** - インストールプロセス時に入力したライセンス番号を使ってアクティベート ダイアログを開きます。このダイアログではライセンス番号を変更してセールス番号 (*AVG をインストールしたときの番号*)を置き換えたり、古いライセンス番号 (*新しい AVG 製品にアップグレードした場合など*) を置き換えたりできます。**AVG Internet Security 2015** の試用版を使用している場合は、最後の 2つの項目が [***今すぐ購入***] および [***アクティベート***] として表示され、製品版をすぐに購入できます。セールス番号でインストールされている **AVG Internet Security 2015** の場合、[***登録***] および [***アクティベート***] として表示されます。
- ***今すぐ登録 /マイアカウント*** - AVG ウェブサイトの登録ページ (*http://www.avg.com/*) に接続します。登録データを入力してください。AVG 製品を登録したお客様のみが無料テクニカル サポートをご利用いただけます。
- ***AVG について*** - 新しいダイアログが開き、購入したライセンスに関するデータ、アクセス可能なサポート、製品およびプログラム情報、ライセンス契約書の全文が 4つのタブに表示されます。(*同じダイアログを、メイン ナビゲーションのサポートリンクを介して開くことができます。*)

5.2. セキュリティ ステータス情報

[***セキュリティステータス情報***] セクションは **AVG Internet Security 2015** 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 Internet Security 2015** の現在のセキュリティステータスに関する情報が常に表示されます。このセクションで表示されるアイコンの意味は以下の通りです。

- 緑のアイコンは ***AVG Internet Security 2015 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すべて適切に動作しています。

- 黄色のアイコンは、***1つ以上のコンポーネントが間違って設定され***、プロパティ設定を確認する必要があることを警告しています。**AVG Internet Security 2015** には致命的な問題はなく、おそらく何らかの理由で一部のコンポーネントをオフにしたものと思われます。保護は適用されています。ただし、問題のコンポーネントの設定に注意してください。誤って設定されたコンポーネントは、オレンジの細長いメイン ユーザー インターフェースに警告とともに表示されます。

何らかの理由でコンポーネントのエラー状態を無視することにした場合にも黄色のアイコンが表示されます。***エラー状態を無視*** オプションは、高度な設定 /エラー状態を無視 からアクセスできます。コンポーネントのエラー状態を認識しながらも、何らかの理由によって **AVG Internet Security 2015** のエラー状態を保持し、警告を表示したくない場合にこのオプションを選択します。特別な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、[***エラー状態を無視***]

オプションはすぐにオフにすることを強く推奨します。

また、**AVG Internet Security 2015** でコンピュータの再起動が必要な場合にも黄色のアイコンが表示されます ***再起動が必要です***)。この警告に注意して、PC を再起動してください。

 - オレンジのアイコンは ***AVG Internet Security 2015 が致命的な状態であることを示しています***。1つ以上のコンポーネントが適切に動作していないため、**AVG Internet Security 2015** はコンピュータを保護できません。報告された問題に注意し、ただちに修復してください。エラーを自分で修復できない場合、AVGテクニカルサポートチームにお問い合わせください。

AVG Internet Security 2015 が最適なパフォーマンスに設定されていない場合は、新しい [クリックして修復] ボタン 問題が複数のコンポーネントに関連している場合は [クリックしてすべてを修復] ボタン)がセキュリティステータス情報の横に表示されます。このボタンをクリックすると、プログラム チェックおよび設定の自動処理が実行されます。これは AVG Internet Security 2015 を最適なパフォーマンスに設定し、最高レベルのセキュリティを実現するための最も簡単な方法です。

セキュリティステータス情報 に注意し、問題がレポートされた場合にはすぐに解決するように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 Internet Security 2015 ステータス情報は、システム トレイ アイコンからも常時確認できます。*

5.3. コンポーネント概要

インストールされたコンポーネント概要 は、メイン ウィンドウの中央セクションの中の水平の細長いブロックに表示されます。コンポーネントは、各コンポーネントのアイコンが付いたライト グリーンのブロックとして表示されます。各ブロックには保護の現在の状態についての情報が表示されます。コンポーネントが正しく設定され、完全に機能している場合、情報は緑色の文字で表示されます。コンポーネントが停止した場合、機能は制限されるか、コンポーネントがエラーの状態です。オレンジ色のテキスト フィールドに警告の文字が表示され、ユーザーに通知されます。***各コンポーネントの設定に注意することを強く推奨します。***

コンポーネント上でマウスを動かすと、メイン ウィンドウの下部に簡単な説明が表示されます。その説明は、コンポーネントの機能について簡単に紹介しています。また、コンポーネントの現在の状態を通知し、正しく設定されていないコンポーネントのサービスを特定します。

インストールされているコンポーネントのリスト

AVG Internet Security 2015 の [***コンポーネント概要***] セクションには、次のコンポーネントの情報が示されます。

- ***コンピュータ*** - このコンポーネントは 2つのサービスに対応しています。***ウイルス対策シールド*** は、システム内のウイルス、スパイウェア、ワーム、トロイの木馬、望ましくない実行ファイルまたはライブラリを検出し、悪意のあるアドウェアからユーザーを保護します。また、***ルートキット対策*** スキャンは、アプリケーションやドライバ、ライブラリの内部に潜む危険なルートキットをスキャンします。詳細 >>
- ***ウェブ閲覧*** - インターネット検索や閲覧中に Web ベースの攻撃からユーザーを保護します。詳細 >>

- ***個人情報*** - コンポーネントが、インターネット上の新しいまたは不明の脅威からユーザーのデジタル資産を常に保護する***Identity Shield*** サービスを実行します。詳細 >>

- ***メール*** - は受信メールのメッセージにスパム メールがあるかどうかをチェックし、ウイルス、フィッシング攻撃、その他の脅威をブロックします。 詳細 >>

- ***ファイアウォール*** - 各ネットワークポートのすべての通信を制御し、悪意のある攻撃からユーザーを保護し、侵入の試みをすべてブロックします。詳細 >>

利用可能なアクション

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

- ***コンポーネントのアイコンを 1回 クリックすると***、コンポーネントの独自のインターフェースが開いて、コンポーネントの現在のステータスの情報が表示されます。また、コンポーネントの設定と統計データにアクセスできます。

5.4. マイ アプリケーション

[***マイ アプリケーション***] エリア *(コンポーネント セットの下にある緑色のブロックの線)では*、既にコンピュータにインストールされているか、インストールが推奨される追加の AVG アプリケーションの概要が表示されます。ブロックは条件付きで表示され、次のアプリケーションのいずれかを示す場合があります。

- ***モバイル保護***は、携帯端末をウイルスおよびマルウェアから保護するアプリケーションです。また、スマートフォンを紛失した際に遠隔で追跡する機能も提供します。

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

- ***Family Safety*** は不適切な Web サイト、メディア コンテンツ、オンライン検索からお子様を守り、オンライン活動に関するレポートを提供します。AVG Family Safety はキー入力技術を採用し、チャットルームやソーシャル ネットワーク サイトでのお子様の活動を監視します。オンラインで子供たちを被害に遭わせる既知の単語やフレーズ、言語を検出し、SMS またはメールで直ちに通知します。アプリケーションは、お子様一人ひとりを適切な水準で保護するよう設定でき、一意なログインで個別に監視します。

- ***PC Tuneup*** アプリケーションは、コンピュータの処理速度と全体的なパフォーマンスを改善する方法に関して、詳細なシステム分析と修正を行うための高度なツールです。

- ***AVG Toolbar*** はインターネット ブラウザから直接使用できます。インターネットの閲覧中に最大限のセキュリティを確保します。

マイ アプリケーション アプリケーションの詳細な情報については、各ブロックをクリックします。専用の AVG Web ページに転送されますので、そこでコンポーネントをすぐにダウンロードすることもできます。

5.5. スキャン / アップデートのクイック リンク

クイックリンクは**AVG Internet Security 2015** ユーザーインターフェイスのボタン下部に位置しています。これらのリンクをクリックすると、スキャンやアップデートなど最も重要で最も多く使用されるアプリケーション機能に素早くアクセスできます。クイック リンクはユーザー インターフェースのすべてのダイアログにあります。

- ***今すぐスキャン*** - このボタンは 2つのセクションに分かれて表示されます。***今すぐスキャン*** リンクをクリックすると、全コンピュータをスキャンをただちに起動し、自動的にレポート ウィンドウが開いて進行状況と結果を見ることができます。[***オプション***] ボタンをクリックすると、***スキャン オプション*** ダイアログが開きます。ダイアログでは、スケジュール スキャンの管理と、全コンピュータをスキャン / 特定のファイルとフォルダのパラメータを編集できます。*(詳細については、「AVG スキャン」の章を参照してください。)*

- ***今すぐアップデート*** - このボタンをクリックすると、ただちに製品アップデートを開始します。AVG システムトレイ アイコンのスライドダイアログ内に、アップデート結果についての情報が表示されます。*(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。)*

5.6. システム トレイ アイコン

AVG システム トレイ アイコン *(Windows タスクバー上、モニター右下端のシステムトレイ)* では、現在の **AVG Internet Security 2015** のステータスが表示されます。このアイコンは **AVG Internet Security 2015** のユーザーインターフェースが表示されているかどうかにかかわらず、システム トレイ上に常に表示されます。

AVG システム トレイ アイコン表示

- フルカラーでその他の要素がない場合、アイコンはすべての **AVG Internet Security 2015** コンポーネントがアクティブで完全に機能していることを示しています。ただし、コンポーネントのいずれかが完全に機能していない状態で、ユーザーがコンポーネント状態を無視することを選択した場合にも、同じ方法でアイコンが表示されます。*([コンポーネント状態を無視] オプションを確認すると、コンポーネントのエラー状態を認識しつつ、何らかの理由でその状態を保持し、エラー状態に関する警告を表示しないことを明示したことになります。)*

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

テータス情報」セクションを参照してください。

- フルカラーで表示されているシステム トレイ アイコンが点滅し、光が回転している場合があります。この状態は現在アップデート処理が実行されていることを示します。

- 表示されているフルカラー アイコンに矢印が付いている場合は、**AVG Internet Security 2015** スキャンが実行中であることを示しています。

AVG システム トレイ アイコン情報

さらに、***AVG システム トレイ アイコン***は現在の **AVG Internet Security 2015** 内の活動およびプログラムでのステータス変更の可能性 *(例：スケジュールスキャンあるいはアップデートの自動起動、ファイアウォールのプロファイル切り替え、コンポーネントのステータス変更、エラーステータスの発生など)* についてもシステム 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。

AVG システム トレイ アイコンから実行できるアクション

AVG システム トレイ アイコンは、**AVG Internet Security 2015** のユーザーインターフェースへのクイックリンクとして使用することもできます。アイコンをダブルクリックするだけです。アイコンを右クリックすると、次のオプションの簡単なコンテキスト メニューを開きます。

- ***AVG を開く*** - クリックすると、のユーザーインターフェース**AVG Internet Security 2015**が開きます。

- ***一時的に AVG 保護を無効にする*** - このオプションでは、**AVG Internet Security 2015** による保護機能すべてを一度にオフにすることができます。やむを得ない場合を除き、このオプションの使用はお勧めしません。インストール処理中に望ましくない中断が発生しないようにするために、インストーラやソフトウェア ウィザードで実行中のプログラムやアプリケーションを終了するように指示される場合があります。それでも通常は、新しいソフトウェアやドライバをインストールする前に **AVG Internet Security 2015** を無効にする必要はありません。**AVG Internet Security 2015** を一時的に無効にしなければならない場合は、必要な作業が終わったらすぐに再有効化する必要があります。ウィルス対策ソフトウェアが無効な状態でインターネットやネットワークに接続している場合は、コンピュータが攻撃の危険にさらされています。

- ***スキャン*** - クリックすると、定義されたスキャンのコンテキストメニュー (*全コンピュータをスキャン*、*特定のファイルとフォルダ*) が開きます。目的のスキャンを選択すると、すぐにスキャンが実行されます。

- ***ファイアウォール*** - クリックするとコンテキスト メニューが開き、すべての選択可能なファイアウォール モードにすばやくアクセスできます。概要から選択し、現在設定されているファイアウォール モードを変更することを確認するためにクリックします。

- ***実行中のスキャン ...*** - 現在コンピュータでスキャンが実行されている場合にのみこの項目が表示されます。この場合、スキャンの優先度の設定、実行中のスキャンの停止または一時停止を実行できます。さらに、*すべてのスキャンの優先度の設定*、*すべてのスキャンの一時停止*、*すべてのスキャンの停止* アクションも実行できます。

- ***Quick Tune*** を実行 - クリックすると、Quick Tune コンポーネントが起動します。

- ***AVG MyAccount にログイン*** - 登録製品の管理、追加の保護の購入、インストール ファイル

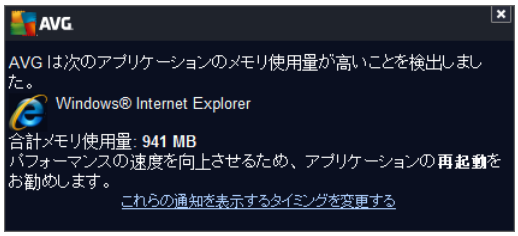
のダウンロード、過去の注文と請求書の確認、個人情報の管理ができるマイアカウント ホームページを開きます。

- ***今すぐアップデート*** - すぐにアップデートを起動します。
- ***ヘルプ*** - スタート ページがらヘルプ ファイルを開きます。

5.7. AVG Advisor

AVG Advisor は、コンピュータの速度を低下させたり、危険にさらすような問題を検出し、その状況を解決するためのアクションを提案するために設計されました。突然コンピュータの速度が落ちた場合 *(インターネットの閲覧や、全体的なパフォーマンスで)*、通常その原因が何なのか、またその後の問題の解決方法についてははっきりとはわかりません。そこで ***AVG Advisor*** が登場します。システムトレイに表示される通知により問題が何であるかを知らせ、その修復方法を提案します。***AVG Advisor*** は、潜在的な問題を発見するため、PC で実行中のすべての処理を監視し、問題の回避方法のヒントを提供するパフォーマンス機能です。

AVG Advisor は、ポップアップがシステム トレイ上をスライドする形で表示されます。



具体的には、***AVG Advisor*** は次のことを監視します。

- ***現在開いている Web ブラウザの状態***。Web ブラウザは、特に複数のタブやウィンドウを開いたままにしているとメモリに負担をかけ、コンピュータの速度が低下するなど、システムのリソースを過剰に消費する場合があります。そのような場合は、通常 Web ブラウザを再起動することが役立ちます。
- ***ピアツーピア接続の実行***。ファイルの共有で P2P プロトコルを使用した後、接続が時々アクティブなまま残り、相当量の帯域幅を消費することがあります。その結果、Web の閲覧スピードの低下を招く可能性があります。
- ***よくある名前の付いた不明なネットワーク***。これは通常、ポータブル コンピュータを使ってさまざまなネットワークに接続しているユーザにのみ該当します。新しい未知のネットワークが、よく知られていて頻繁に使われるネットワーク *(Home や MyWifi など)* と同じ名前である場合、混乱を来たし、誤ってまったく不明な危険の可能性があるネットワークに接続してしまう恐れがあります。***AVG Advisor*** は、既知の名前が実際に新しいネットワークを示していることを警告することで、この問題を防止します。もちろん、不明なネットワークが安全だと判断した場合は、以降に再度報告されることがないように、***AVG Advisor*** の既知のネットワーク リストに保存することができます。

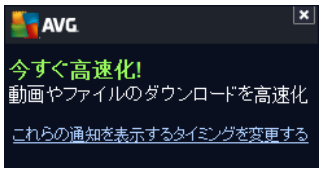
これらの各状況においては、***AVG Advisor*** は、発生の可能性がある問題を警告し、競合するプロセスやアプリケーションの名前とアイコンが表示されます。さらに、***AVG Advisor*** は発生の可能性がある問題を避けるために必要な手順を提案します。

サポートされているウェブ ブラウザ

この機能は次のウェブ ブラウザで動作します。Internet Explorer、Chrome、Firefox、Opera、Safari

5.8. AVG Accelerator

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



6. AVG コンポーネント

6.1. コンピュータの保護

コンピュータコンポーネントは、***ウイルス対策***と***データセーフ***の 2つの主なセキュリティサービスを提供します。

- ***ウイルス対策*** は、すべてのファイル、コンピュータのシステム領域、リムーバブル メディア *(フラッシュディスク等)*を保護するスキャン エンジンから構成され、既知のウイルスをスキャンします。検出されたウイルスは動作をブロックされ、駆除またはウイルス隔離室に隔離されます。常駐保護は「バックグラウンドで」動作するため、通常、ユーザーがこの処理を意識することはありません。ウイルス対策は、ヒューリスティック スキャンも使用します。ファイルは一般的なウイルスの特性についてスキャンされます。これは、新種のウイルスが既存の一般的なウイルス特性を含む場合、新種で未知のウイルスであってもウイルス対策で検出可能であることを意味します。**AVG Internet Security 2015** はまた、システム内の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。*(さまざまな種類のスパイウェア、アドウェアなど)* . さらに、ウイルス対策は疑わしいエントリ、インターネット一時ファイル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。

- ***データセーフ***により、安全な仮想隔離室を作成し、重要または機微なデータを保存することができます。データセーフのコンテンツは暗号化され、ユーザーが選んだパスワードで保護されるため、承認のない人はアクセスできません。

ダイアログ コントロール

ダイアログの 2つのセクションを切り替えるには、各サービス パネルの任意の場所をクリックするだけです。パネルは水色でハイライトされます。ダイアログの 2つのセクションには、次のコントロールが表示されます。それぞれの機能は、どちらのセキュリティサービス *(ウイルス対策またはデータセーフ)* に属していても同じです。

有効化　/無効化 - このボタンは交通信号に似ていますが、視覚的にも機能的にも同様の役割を果たします。有効化　/無効化を切り替えるには、1回クリックします。緑色は***有効化***を意味し、ウイルス対策セキュリティサービスはアクティブで完全に機能しています。赤色は、サービスが無効化された場合など、***無効化***された状態を表します。サービスを無効化する理由が特になければ、すべてのセキュリティ設定を既定のままで維持することを強くお勧めします。既定の設定ではアプリケーションの最適なパフォーマンスと最大限の安全性を保証します。何らかの理由によってサービスを無効にする場合、現在完全に保護されていないという情報と赤色の***警告***サインが表示され、ただちに危険の可能性に関して警告されます。***できるだけ早く、再度サービスを有効化するようにしてください。***

設定 - このボタンをクリックすると、高度な設定インターフェースに移動します。各ダイアログが開き、ウイルス対策など、選択したサービスの設定ができます。高度な設定インターフェースでは、**AVG Internet Security 2015** 内の各セキュリティサービスの設定をすべて編集できます。ただし、設定は上級者ユーザーのみが行うことをお勧めします。

矢印 - ダイアログ左上のセクションにある緑色の矢印を使用すると、メインユーザーインターフェースに戻り、コンポーネントの概要が表示されます。

データセーフの作成方法

コンピュータの保護ダイアログの***データセーフ***セクションに、***セーフを作成***ボタンがあります。ボタンを押して、同じ名前の新しいダイアログを開き、ここで作成するセーフのパラメータを設定できます。必要な情報をすべて入力し、アプリケーションの指示に従います。

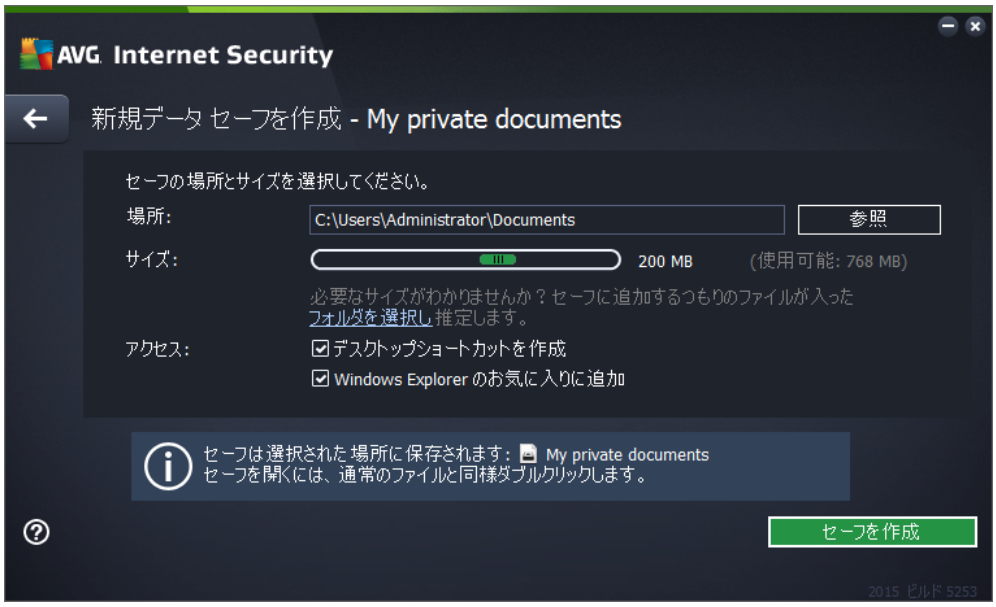
最初に、セーフの名前を指定し、強力なパスワードを設定します。

- ***セーフの名前*** - 新しいデータセーフを作成するには、まず、わかりやすいように適切な名前を選びます。家族とコンピュータを一緒に使用している場合、セーフのコンテンツに加えて、*父のメール*など名前も入れるとよいでしょう。
- ***パスワードの作成　/パスワードの再入力*** - データセーフに使用するパスワードを作成し、適

切なテキストフィールドに入力します。右側の画像インジケータがパスワードが弱い *(ソフトウェアツールによって比較的容易に解読される)* または強いかを示します。パスワードは少なくとも中程度の強度であることが推奨されます。大文字、数字、ドットやダッシュなどといったその他の文字を含めることでパスワードをより強く作ることができます。パスワードがきっちりと入力されていることを確認するには、***パスワードを表示***ボックスにチェックを入れます *(誰もあなたの画面を見ていないことを確認してください)*。

- ***パスワードのヒント*** - パスワードを忘れてしまった場合に思い出す助けとなるパスワードのヒントを作成しておかれることを強くお勧めします。データセーフは、パスワードがある場合のみアクセスを許可することでユーザーのファイルを保護しています。これには例外はなく、つまりパスワードを忘れてしまうとデータセーフにアクセスできなくなります。

テキストフィールドに必要なデータをすべて設定したら、***次へ***ボタンをクリックして次のステップに進みます。



このダイアログには次の設定オプションがあります。

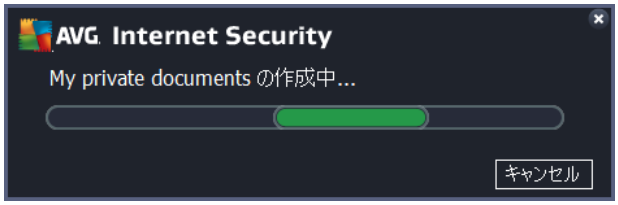
- ***ロケーション*** - は、データセーフが置かれている物理的な場所を示します。バードドライブの適切な場所を参照するか、予め定義された場所である*ドキュメントフォルダに保持します*。一度データセーフを作成すると、その場所を変更することができないことに、ご留意ください。

- ***サイズ*** - データセーフのサイズを予め決定し、ディスク上の必要な領域を割り当てることができます。その値は、小さすぎたり *(必要を満たさない)* 大きすぎたり *(必要以上にディスク領域を占める)* しないようにします。データセーフに何を入れるかがすでに分かっている場合、すべてのファイルを1つのフォルダに入れ、***フォルダを選択***リンクを使用して、合計サイズを自動計算することができます。必要に応じて、後でサイズ変更することも可能です。

- ***アクセス*** - このセクション内のチェックボックスにより、データセーフへの便利なショートカットを作成できます。

データセーフの使用方法

設定が納得いくものであれば、***セーフを作成***ボタンをクリックします。***データセーフが使用できます***という新しいダイアログが表示され、ファイルを保存するためのセーフが使用できることを知らせます。セーフが開いており、すぐにアクセスできます。次回以降セーフにアクセスする際は、設定したパスワードを使用してセーフのロック解除を行ってください。



新しいデータセーフを使用する場合は、***今すぐ開く***ボタンをクリックして、データセーフを開く必要があります。開くとすぐに、新しい仮想ディスクとしてデータセーフがコンピュータに表示されます。ドロップダウンメニューから任意の文字を割り当てます（*現在空きのあるディスクからしか選択できません*）。概して、C（*通常、ハードドライブに割り当て*）、A（*フロッピーディスクドライブ*）、（*DVD ドライブ*）の選択は許可されません。データセーフをロック解除する度に、後で使用可能なドライブを選択いただけます。

データセーフをロック解除する方法

次回データセーフにアクセスする際は、設定したパスワードを使用してセーフのロック解除を行ってください。

テキストフィールドに、ユーザーを認証するパスワードを入力して、***ロック解除***ボタンをクリックします。パスワードを思い出すための助けが必要な場合は、***ヒント***をクリックして、データセーフの作成時に設定したパスワードのヒントを表示します。新規データセーフは、データセーフの概要にロック解除の状態で表示され、ファイルを必要に応じて追加/削除できます。

6.2. ウェブ閲覧時の保護

ウェブ閲覧保護は 2つのサービスから構成されます。***リンクスキャナ サーフシールド***と***オンライン シールド***です。

- ***リンクスキャナ サーフシールド***は、日進月歩でますます増加するWeb上の脅威からユーザーを保護します。このような脅威は、政府機関のサイト、有名な大企業のサイト、中小企業のサイトなど、あらゆる種類のWebサイトに潜み、そのサイトに 24時間以上存在することはほとんどありません。リンクスキャナは表示しようとするすべてのWebページにある各リンクを

チェックし、リンク先の Web ページを解析することでユーザーを保護します。安全性の確認が必要である、ユーザーがリンクをクリックしようとしたタイミングでチェックが実行され、サイトの安全性が保証されます。***リンクスキャナ サーフシールドはサーバー プラットフォームの保護には対応していません。***

- ***オンライン シールド***は、リアルタイムの常駐保護の一種です。Web ブラウザに表示され、コンピュータにダウンロードされる前に、Web ページの内容とそのページに含まれる可能性のあるファイルをスキャンします。オンライン シールドは、アクセスしようとしているページが危険な javascript を含んでいる場合、ページの表示を防ぎます。また、ページに含まれるマルウェアも検出することができ、コンピュータにダウンロードされないようにします。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ることを覚えておくことが重要です。***オンライン シールドはサーバー プラット フォームには対応していません。***

ダイアログ コントロール

ダイアログの 2つのセクションを切り替えるには、各サービス パネルの任意の場所をクリックするだけです。パネルは水色でハイライトされます。ダイアログの 2つのセクションには、次のコントロールが表示されます。それぞれの機能は、どちらのセキュリティサービス *(リンクスキャナ サーフシールドまたはオンライン シールド)*に属していても同じです。

 ***有効化 /無効化*** - このボタンは交通信号に似ていますが、視覚的にも機能的にも同様の役割を果たします。有効化 /無効化を切り替えるには、1回クリックします。緑色は***有効化***を意味し、リンクスキャナ サーフシールドまたはオンライン シールド セキュリティサービスはアクティブで完全に機能しています。赤色は、サービスが無効化された場合など、***無効化***された状態を表します。サービスを無効化する理由が特になければ、すべてのセキュリティ設定を既定のままで維持することを強くお勧めします。既定の設定ではアプリケーションの最適なパフォーマンスと最大限の安全性を保証します。何らかの理由によってサービスを無効にする場合、現在完全に保護されていないという情報と赤色の***警告***サインが表示され、ただちに危険の可能性に関し

て警告されます。***できるだけ早く、再度サービスを有効化するようにしてください。***

設定 - このボタンをクリックすると、高度な設定インターフェースに移動します。各ダイアログが開き、リンクスキャナ サーフシールドまたはオンライン シールドなど、選択したサービスの設定ができます。高度な設定インターフェースでは、**AVG Internet Security 2015** 内の各セキュリティサービスの設定をすべて編集できます。ただし、設定は上級者ユーザーのみが行うことをお勧めします。

矢印 - ダイアログ左上のセクションにある緑色の矢印を使用すると、メイン ユーザーインターフェースに戻り、コンポーネントの概要が表示されます。

6.3. Identity Protection

Identity Protection コンポーネントは、インターネット上の新しい脅威または不明の脅威からユーザーのデジタル資産を常に保護する ***Identity Shield*** サービスを実行します。

- ***Identity Protection*** はあらゆる種類のマルウェア *(スパイウェア、ボット、ID 窃盗など)* から保護するマルウェア対策サービスです。行動分析技術を使用して、発生したばかりの新しいウイルスに対する保護を提供します。Identity Protection は ID 窃盗によるパスワード、銀行アカウント情報、クレジットカード番号、その他の貴重な個人デジタル情報の窃盗を防止することに特化しています。PC を狙うあらゆる種類の悪意のあるソフトウェア *(マルウェア)* を対象とします。PC または共有ネットワーク上で実行中のすべてのプログラムが正常に動作していることを確認します。Identity Protection は継続的に疑わしい動作を検出およびブロックし、あらゆる新しいマルウェアからコンピュータを保護します。Identity Protection は新しく未知の脅威に対するリアルタイムのコンピュータ保護を提供します。このコンポーネントはすべてのプロセス *(非表示のプロセスを含む)* と *286* 以上の異なる動作パターンを監視し、システム内で悪意のある活動が発生しているかどうかを判断できます。このため、ウイルス データベースにはまだ登録されていない脅威でも検出できます。不明なコードがコンピュータに侵入すると、悪意のある動作の監視と追跡が即時実行されます。ファイルが悪意のあるものだと判定された場合、Identity Protection はコードを除去してウイルス隔離室に移し、システムに対して実行された変更 *(コード挿入、レジストリ変更、ポート オープンなど)* すべてを元に戻します。保護を適用するためにスキャンを実行する必要はありません。この技術はきわめて積極的な保護であるため、アップデートはほとんど必要ありません。常に保護が適用されています。

ダイアログ コントロール

ダイアログ内で、次の制御を行うことができます：

有効化 /無効化 - このボタンは交通信号に似ていますが、視覚的にも機能的にも同様の役割を果たします。有効化 /無効化を切り替えるには、1回クリックします。緑色は***有効化***を意味し、Identity Protection セキュリティサービスはアクティブで完全に機能しています。赤色は、サービスが無効化された場合など、***無効化***された状態を表します。サービスを無効化する理由が特になければ、すべてのセキュリティ設定を既定のままで維持することを強くお勧めします。既定の設定ではアプリケーションの最適なパフォーマンスと最大限の安全性を保証します。何らかの理由によってサービスを無効にする場合、現在完全に保護されていないという情報と赤色の***警告***サインが表示され、ただちに危険の可能性に関して警告されます。***できるだけ早く、再度サービスを有効化するようにしてください。***

設定 - このボタンをクリックすると、高度な設定インターフェースに移動します。各ダイアログが開き、Identity Protection など、選択したサービスの設定ができます。高度な設定インターフェースでは、**AVG Internet Security 2015** 内の各セキュリティサービスの設定をすべて編集できます。ただし、設定は上級者ユーザーのみが行うことをお勧めします。

矢印 - ダイアログ左上のセクションにある緑色の矢印を使用すると、メイン ユーザーインターフェースに戻り、コンポーネントの概要が表示されます。

残念ながら**AVG Internet Security 2015** には Identity Alert サービスは含まれません。このタイプの保護を利用したい場合、[***アップグレードしてアクティベート***] ボタンをクリックすると専用ウェブページに移動し、Identity Alert ライセンスを購入することができます。

AVG Premium Security エディションであっても、Identity Alert サービスは特定の地域でしかご利用いただけません :米国、英国、カナダ、アイルランドのみ。

6.4. メール保護

メール保護 コンポーネントは、次の 2つのセキュリティサービスを対象とします :***メールスキャナ***および***スパム対策*** *(スパム対策サービスは Internet / Premium Security エディションのみで利用可能です)*:

- ***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。企業では、通常業務用のメールアカウントを使用し、スパム対策フィルタ等を導入してリスクを削減します。メール保護コンポーネントは、すべての送受信されるメール メッセージをスキャンします。メールでウイルスが検出されると、必ずウイルス隔離室にただちに移動されます。このコンポーネントでは特定の種類のメールの添付ファイルを除外できます。また、メールが感染していないことを示す認証テキストを送信メールに追加できます。***メール 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。***

- ***スパム対策***は、すべてのメール メッセージをチェックし、好ましくないメールをスパムとしてマークします *(スパムとは未承諾で送られてくるメールであり、たいていは膨大な数のメールアドレス宛に大量に一斉送信され、受信者のメールボックスをいっぱいにする製品やサービスの広告です。スパムは消費者が同意をした合法的な商業メールではありません)*。スパム対策は、特別なテキスト文字列を追加して、メール *(スパムとして特定されたメール)*の件名を修正できます。これで、メールクライアントでメールを簡単にフィルタリングできます。スパム対策コンポーネントは、複数の分析手法を使用して各メールを処理し、好ましくないメールに対する最大限の保護を提供します。スパム対策コンポーネントは、スパム保護のため、定期的に更新されるデータベースを使用します。また、RBLサーバー *(既知のスパム送信者」メールアドレスの公開データベース)*を使用したり、手動でメールアドレスをホワイトリスト *(スパムとしてマークされない)*およびブラックリスト *(常にスパムとしてマーク)*に追加できます。

ダイアログ コントロール

ダイアログの 2つのセクションを切り替えるには、各サービス パネルの任意の場所をクリックするだけです。パネルは水色でハイライトされます。ダイアログの 2つのセクションには、次のコントロールが表示されます。それぞれの機能は、どちらのセキュリティサービス *(メール スキャナまたはスパム対策)*に属していても同じです。

 ***有効化 /無効化*** - このボタンは交通信号に似ていますが、視覚的にも機能的にも同様の役割を果たします。有効化 /無効化を切り替えるには、1回クリックします。緑色は***有効化***を意味し、セキュリティサービスはアクティブで完全に機能しています。赤色は、サービスが無効化された場合など、***無効化***された状態を表します。サービスを無効化する理由が特になければ、すべてのセキュリティ設定を既定のままで維持することを強くお勧めします。既定の設定ではアプリケーションの最適なパフォーマンスと最大限の安全性を保証します。何らかの理由によってサービスを無効にする場合、現在完全に保護されていないという情報と赤色の***警告***サインが表示され、ただちに危険の可能性に関して警告されます。***できるだけ早く、再度サービスを有効化するようにしてください。***

 ***設定*** - このボタンをクリックすると、高度な設定インターフェースに移動します。各ダイアログが開き、メール スキャナまたはスパム対策など、選択したサービスの設定ができます。高度な設定インターフェースでは、**AVG Internet Security 2015** の各セキュリティサービスの設定をすべて編集できます。ただし、設定は上級ユーザーのみが行うことをお勧めします。

 ***矢印*** - ダイアログ左上のセクションにある緑色の矢印を使用すると、メイン ユーザーインターフェースに戻り、コンポーネントの概要が表示されます。

6.5. ファイアウォール

ファイアウォールは、トラフィックをブロック、または許可することで、2つ以上のネットワーク間のアクセスコントロール ポリシーを実行するためのシステムです。ファイアウォールには 1セットのルールが含まれます。このルールは*外部から（一般的にはインターネットから）*の攻撃から内部ネットワークを保護し、あらゆるネットワーク ポート上のすべての通信をコントロールします。定義されたルールにしたがって、通信が評価され、許可、または禁止されます。ファイアウォールが侵入の試みを認識すると、その試みを「ブロック」し、侵入者のコンピュータへのアクセスを許可しません。ファイアウォールを設定して、定義されたポート経由および定義されたソフトウェア アプリケーションに対する内部 外部通信 *（双方向、受信または送信）*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 Internet 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。これにより、個人を特定できる情報が許可なくコンピュータから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。

AVG Internet Security 2015 では、***ファイアウォール***がコンピュータのすべてのネットワーク ポート上のトラフィックを制御します。ファイアウォールは、定義されたルールに基づいて、*インターネットまたはローカル ネットワークに接続*しようとするコンピュータで実行中のアプリケーションまたはコンピュータに接続しようとする外部アプリケーションを評価します。これらのアプリケーションに関して、ファイアウォールはネットワーク ポートでの通信を許可あるいは禁止します。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。

AVG ファイアウォールはサーバー プラットフォームの保護には対応していません。

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。

注意：*AVG Internet Security 2015のインストール後、ファイアウォール コンポーネントがコンピュータの再起動を必要とすることがあります。その場合、コンポーネントのダイアログが表示され、再起動の必要性を知らせます。ダイアログ内に****今すぐ再起動****ボタンがあります。再起動が行われるまで、ファイアウォールのコンポーネントは完全にアクティベートされません。さらに、ダイアログ内の変更オプションはすべて無効になります。警告に注意し、お使いのPC をすぐに再起動させてください。*

使用できるファイアウォール　モード

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、ノートパソコンかによって、特定のセキュリティルールを定義することができます。各コンピュータ タイプによって異なるレベルの保護が必要になります。これらのレベルには該当するモードが適用されます。要するに、ファイアウォール モードとはファイアウォール コンポーネントの特別な設定です。ユーザーはこのような予め定義された数々の設定を利用することができます。

- ***自動*** - このモードでは、ファイアウォールはすべてのネットワーク トラフィックを自動的に処理します。どのような決定もユーザーが下すことはありません。ファイアウォールは、既知の各アプリケーションの接続を許可すると同時にアプリケーションのルールを作成して、今後アプリケーションが常に接続できるよう指定します。その他のアプリケーションについては、アプリケーションの動作によってファイアウォールが接続を許可するかブロックするかを決定します。ただし、そのような状況下ではルールは作成されません。またアプリケーションは接続を試みる時に再度チェックされます。自動モードは安定しているため、ほとんどのユーザーに対して推奨されます。

- ***対話*** - このモードはコンピュータとやりとりするすべてのネットワーク トラフィックを完全に制御する場合に便利です。ファイアウォールはトラフィックを監視し、データの通信や転送のそれぞれの試みをユーザーに通知します。ユーザーは自分が適切だと判断したとおりに、その試みを許可したりブロックしたりできます。上級ユーザーのみにお勧めします。

- ***インターネットへのアクセスをブロック*** - インターネット接続が完全にブロックされます。インターネットにまったくアクセスできなくなり、外部からあなたのコンピュータにアクセスできることはありま

せん。特別な場合や短期間の使用の場合に限ります。

- ***ファイアウォール保護を無効にする（推奨しません）*** - ファイアウォールを無効にして、コンピュータと通信するすべてのネットワークトラフィックを許可します。これによって、結果的にハッカーによる攻撃を受けやすくなります。このオプションは常によく考えた上で、慎重に設定してください。

特定の自動モードはファイアウォール内でも有効であることに注意してください。コンピュータまたはIdentity protection コンポーネントが無効になった場合、このモードは暗黙で有効化されます。そのため、コンピュータはさらに脆弱になります。そのような場合、ファイアウォールは既知の絶対に安全なアプリケーションのみを自動的に許可します。その他の場合はすべてユーザーが決定を行います。これは無効化された保護コンポーネントを補完するためであり、コンピュータを安全に保つための対策です。

ファイアウォールは決してオフにしないことを強くお勧めします。ただし、ファイアウォールコンポーネントを無効にする必要が生じ、どうしてもオフにしなければならない場合は、上記の利用可能なファイアウォールモードのリストから[ファイアウォール保護を無効にする]モードを選択できます。

ダイアログコントロール

ダイアログには、ファイアウォールコンポーネントの状態に関する基本情報の概要が表示されます。

- ***ファイアウォールモード*** - 現在選択されているファイアウォールモードの情報を表示します。現在のモードを別のモードに変更する場合は、表示されている情報の隣にある[***変更***]ボタンを使用すると、ファイアウォール設定インターフェースに切り替わります *(ファイアウォールプロファイルの使用上の説明と推奨については、前のパラグラフを参照してください)*。

- ***ファイルとプリンタの共有*** - では、ファイルとプリンタの共有が*(双方向で現在許可されているかどうかを通知します。ファイルとプリンタの共有とは、実際には Windows で「共有」としてマークしたファイルまたはフォルダ、共通のディスクユニット、プリンタ、スキャナ、および同様のあらゆるデバイスを共有するということです。このようなアイテムは、安全と考えられるネットワーク(家庭、職場、学校など)*内でのみ共有することが望ましいです。ただし、公開ネットワーク*(空港の Wi-Fi やインターネットカフェなど)*に接続している場合は、おそらく一切の共有を望まないでしょう。

- ***接続先*** - 現在接続しているネットワークの名前情報を表示します。Window XP の場合、ネットワーク名は、最初に接続した時に特定のネットワークに付けた名称に対応しています。Window Vista 以降の場合、ネットワーク名は、[ネットワークと共有センター]で自動的に付けられます。

- ***デフォルトにリセット*** - このボタンをクリックすると、現在のファイアウォール設定が上書きされ、自動検出を基にしたデフォルトの設定に戻ります。

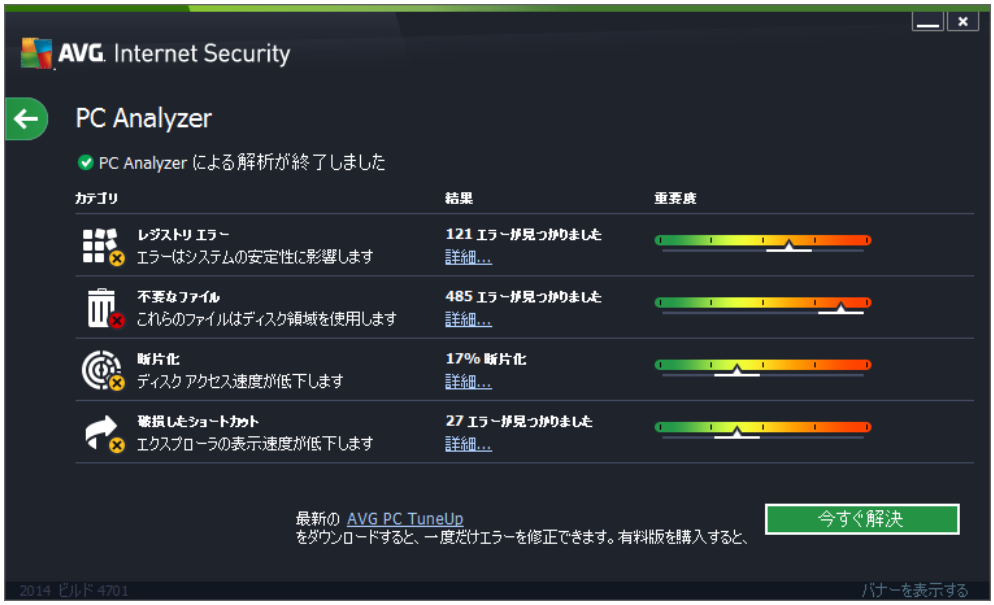
このダイアログには次のグラフィックコントロールがあります。

設定 - このボタンをクリックすると、ファイアウォール設定インターフェースに移動します。ここでは、すべてのファイアウォール設定を編集できます。設定の変更はすべて上級者ユーザーのみが行って下さい。

矢印 - ダイアログ左上のセクションにある緑色の矢印を使用すると、メインユーザーインターフェースに戻り、コンポーネントの概要が表示されます。

6.6. PC Analyzer

PC Analyzer コンポーネントは詳細なシステム分析と修正のための高度なツールです。このツールはコンピュータの速度と全体的なパフォーマンスを改善する方法を分析します。このコンポーネントは、システムトレイにある AVG アイコンのコンテキスト メニューに含まれている ***PC Analyzer を実行*** オプションを選択して開きます。すると、分析の進行状況と分析結果がグラフに直接表示されます。



このコンポーネントでは、レジストリエラー、不要なファイル、断片化および破損したショートカットが解析されます。

- ***レジストリエラー***は、コンピュータの速度低下やエラー メッセージの表示を引き起こす可能性のある Windows レジストリのエラー数を示します。
- ***不要なファイル***は、削除された可能性が高く、ディスク領域を占有しているファイルの数を示します。一般的には、各種一時ファイルやごみ箱のファイルが不要なファイルとして判断されます。
- ***断片化***では、長期間の使用により物理ディスクのいたるところに分散して断片化したハードディスクの割合を計算します。
- ***破損したショートカット***は、動作しないショートカットや存在しない場所へのショートカットなどの問題を示します。

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

コントロール ボタン

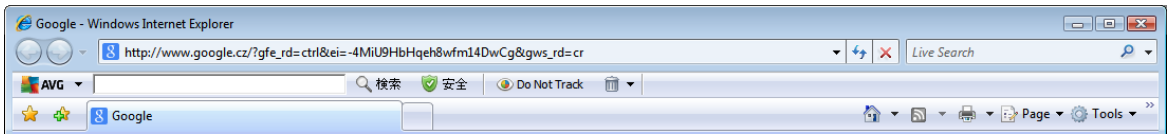
- ***分析を停止*** (*分析の実行中に表示*) - このボタンをクリックすると、コンピュータの分析が直ちに中断されます。
- ***今すぐ修正*** (*分析が完了すると表示*) - このボタンをクリックすると、検出されたエラーがすべて

修正されます。

- ***キャンセル*** - このボタンをクリックすると、分析の実行を停止するか、分析完了時にデフォルトのAVG メイン ダイアログ (*コンポーネント概要*) に戻ります。

7. AVG Security Toolbar

AVG Security Toolbarはリンクスキャナ サーフシールド サービスと密接に連携し、インターネット閲覧中に最大限のセキュリティで保護するツールです。**AVG Internet Security 2015** では ***AVG Security Toolbar***のインストールは任意です。インストール処理中にこのコンポーネントをインストールするかどうかを確認します。***AVG Security Toolbar***はインターネット ブラウザから直接利用できます。現在、Internet Explorer (*バージョン 6.0以上*) および Mozilla Firefox (*バージョン 3.0以上*) のインターネット ブラウザに対応しています。それ以外のインターネット ブラウザには対応していません *(例 :Avant ブラウザなど、別のインターネット ブラウザを使用している場合は、予期しない動作を起こす場合があります)*。



AVG Security Toolbarは次の項目から構成されています。

- ***AVG ロゴ***とドロップダウン メニュー：
  - ***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。
  - ***AVG 脅威 ラボ*** - 特定の***AVG 脅威 ラボ***のウェブサイト(*http://www.avgthreatlabs.com*)を開き、さまざまなウェブサイトのセキュリティ情報や現在の脅威のレベルをオンラインで探すことができます。
  - ***Toolbar ヘルプ*** - すべての ***AVG Security Toolbar***の機能に対応しているオンライン ヘルプを開きます。
  - ***製品 フィードバックの送信*** - Web ページのフォームが開き、***AVG Security Toolbar***についてのご意見を入力できます。
  - ***エンドユーザー ライセンス契約*** - お使いの**AVG Internet Security 2015**に関するライセンス契約の全文が見られるAVG ウェブサイトのページを開きます。
  - ***プライバシー ポリシー*** - AVG プライバシー ポリシーの全文が見られる AVG ウェブサイトのページを開きます。
  - ***AVG Security Toolbar のアンインストール*** - 各対応ウェブ ブラウザでの ***AVG Security Toolbar***のアンインストール方法について詳細に説明したウェブページを開きます。
  - ***AVG Security Toolbar について ...*** - 新しいウィンドウが開き、現在インストールされているバージョンの ***AVG Security Toolbar***に関する情報が表示されます。
- ***検索 フィールド*** - ***AVG Security Toolbar***を使用してインターネットを検索します。表示される検索結果は 100パーセント安全であるため、安全性と快適性が保証されます。検索フィールドにキーワードまたはフレーズを入力して、[***検索***] ボタンをクリックします *(または Enter キーを押します)*。
- ***サイト セーフティ*** - このボタンは、新しいダイアログを開いて、今開いているページの現在の脅威レベル *(安全です)* についての情報を提供します。この概要は展開可能であり、ブラウザ ウィンドウ内のページの右側に関するすべてのセキュリティ活動の全詳細が表示できます *(ウェ*

ブサイトの完全な報告)。

- ***Do Not Track*** - DNT サービスは、ユーザーのオンラインアクティビティに関するデータを収集するウェブサイトの識別に役立ち、許可またま禁止を選択できます。詳細 >>

- ***削除*** - 「ごみ箱」ボタンを押すと、閲覧、ダウンロード、オンライン フォームに関する情報を削除するか、あるいは検索履歴を一括ですべて削除するかを選択できるロールダウン メニューが表示されます。

- ***天気*** - このボタンをクリックすると、新しいダイアログが開き、選択した場所の現在の天気と 2 日間の天気予報が表示されます。この情報は 3~ 6時間ごとに定期的に更新されます。このダイアログでは、目的の場所を手動で変更したり、気温を摂氏で表示するか華氏で表示するかを選択したりできます。

- ***Facebook*** - このボタンをクリックすると、AVG Security Toolbarから直接 ***Facebook*** ソーシャル ネットワークに接続できます。

- 次のアプリケーションへのクイック アクセス ショートカット ボタン:***電卓***、***メモ帳***、***Windows Explorer***.

8. AVG Do Not Track

オンライン活動に関するデータを収集しているウェブサイトを識別できるように、***AVG Do Not Track*** アイコンを常に表示しておくことをお勧めします。***AVG Do Not Track*** は AVG Security Toolbar の一部であり、ユーザーのアクティビティに関するデータを収集するウェブサイトや広告主を表示し、許可または禁止を選択できます。

- ***AVG Do Not Track***は、各サービスのプライバシーポリシーについての詳細な情報に加え、可能な場合はサービスを拒否する直接リンクを表示します。
- さらに、***AVG Do Not Track*** では、追跡されたくないことを自動的にサイトに通知する W3C DNT プロトコル をサポートしています。この通知はデフォルトで有効化されていますが、いつでも変更ができます。
- ***AVG Do Not Track*** は、これらの契約条件の下で提供されます。
- ***AVG Do Not Track*** はデフォルトで有効化されていますが、いつでも簡単に無効にできます。手順については FAQ のAVG Do Not Track 機能を無効にするの記事を参照してください。
- ***AVG Do Not Track*** についての詳細は、弊社ウェブサイトを参照してください。

現在、***AVG Do Not Track*** 機能は Mozilla Firefox、Chrome、および Internet Explorer ブラウザでのみサポートされています。

8.1. AVG Do Not Track インターフェース

オンライン中、***AVG Do Not Track*** は、どんな種類のデータ収集活動でも発見次第すぐに警告します。このような場合 AVG Security Toolbarにある***AVG Do Not Track*** アイコンは見た目が変わります。

アイコンのそばに検出されたデータ収集サービスの数を示す小さな数字が表示されます：  アイコンをクリックすると次のダイアログが表示されます：

検出されたデータ収集サービスはすべて [***このページのトラッカー***] 概要に一覧表示されます。***AVG Do Not Track*** で識別されるデータ収集活動は 3種類あります。

- ***Web analytics*** *(デフォルトでは許可):*パフォーマンスと個々のウェブサイト機能の向上のために使用されるサービス。Google Analytics、Omniture、Yahoo Analytics などのサービスはこのカテゴリに入ります。ウェブサイトが目的通りに動作しない可能性があるため、Web analytics サービスをブロックしないことを推奨します。

- ***Ad Networks*** *(デフォルトでは一部をブロック):*ユーザーのオンライン活動について、直接的または間接的に複数のサイトでデータを収集または共有するサービスは、コンテンツベースの広告とは違った、個人向けに特化した広告を提供します。これはウェブサイトで有効な各アドネットワークのプライバシーポリシーに基づいて決定されます。一部のアドネットワークはデフォルトでブロックされます。

- ***Social Buttons*** *(デフォルトでは許可):*ソーシャル ネットワーク機能の向上のために設計された構成要素です。ソーシャル ボタンはソーシャル ネットワークから訪問中のサイトにわたって動作します。ログインしている間、オンライン活動についてのデータを収集することがあります。ソーシャル ボタンの例 :Facebook ソーシャル プラグイン、Twitter ボタン、Google +1など。

注意 :*ウェブサイトのバックグラウンドで実行されているサービスによっては、上述の 3つのセクションのうちの一部がAVG Do Not Track ダイアログに表示されない場合があります。*

ダイアログ コントロール

- ***追跡とは何ですか?*** - ダイアログの上部セクションにあるこのリンクをクリックすると、トラッキングの基本的な性質についての詳細な説明および特定のトラッキングの種類の説明が記載された専用ウェブページにリダイレクトされます。

- ***すべてをブロック*** - ダイアログの下部セクションにあるこのボタンをクリックすると、すべてのデータ収集活動を希望しないことになります。*(詳細は トラッキング プロセスの章を参照してください。*

- ***Do Not Track 設定*** - ダイアログの下部セクションにあるこのリンクをクリックすると、様々な ***AVG Do Not Track*** パラメータの個別の設定ができる専用ウェブページにリダイレクトされます *(詳細は 「AVG Do Not Track 設定」の章を参照)*

8.2. 追跡プロセスの情報

検出されたデータ収集サービスのリストは特定のサービスの名前のみを提供します。個々のサービスをブロックすべきか許可すべきかを熟知した上で決定するには、詳細を知る必要があるかもしれません。その場合は、個々のリストの上にマウスを移動します。情報のポップアップにサービスの詳細なデータが表示されます。サービスがお客様の個人データ、あるいはその他の有効なデータを収集しているかどうか、データがその他の第三者と共有されているかどうか、また収集されたデータが保管され、さらなる利用の可能性があるかどうかがわかります。

情報ポップアップの下部のセクションに、検出された個々のサービスのプライバシー ポリシーの専用ウェブサイトを表示する ***プライバシー ポリシー*** のリンクが表示されます。

8.3. 追跡プロセスのブロック

アドネットワーク /ソーシャル ボタン /ウェブ分析のすべてのリストに、どのサービスをブロックするかを制御するオプションが表示されます。次の 2つの方法でブロックを設定できます。

- ***すべてをブロック*** - ダイアログの下部セクションにあるこのボタンをクリックすると、すべてのデータ収集活動を希望しないことになります。*(ただし、この操作によって、サービスを実行している個々のウェブページが機能しなくなる場合がありますので留意してください。)*

-  - 検出されたサービスを一度に全部ブロックしたくない場合は、サービスを個別に許可するかブロックするかを指定できます。また、検出されたシステムの実行を部分的に許可することができます *(ウェブ分析など)*。これらのシステムではウェブサイトの最適化のために収集したデータを使用しますが、このような方法ですべてのユーザーに共通するインターネット環境の改善に役立てます。一方で、アドネットワークと分類されたすべてのプロセスのデータ収集アクティビティを同時にブロックすることができます。各サービスの隣にある  アイコンをクリックするだけで、データ収集をブロック*(処理名に取り消し線が入った状態で表示されます)*したり、データ収集を再度許可することができます。

8.4. AVG Do Not Track 設定

Do Not Track オプション ダイアログは次の構成オプションを提供します。

- ***Do Not Track は有効です*** - デフォルトでは、DNT サービスは有効化されています。*(スイッチON)*サービスを無効化するには、スイッチをOFFにします。

- ダイアログの中央セクションでは、アドネットワークに分類される既知のデータ収集サービスがリストされたボックスが表示されます。デフォルトでは、***Do Not Track*** は一部のアドネットワークを自動でブロックします。残りも同様にブロックするか、許可しておくかはユーザが決定します。そのような場合は、リストの下の [***すべてをブロック***] ボタンをクリックします。または[***デフォルト***] ボタンを使って変更されたすべての設定をキャンセルし、元の構成に戻ることができます。

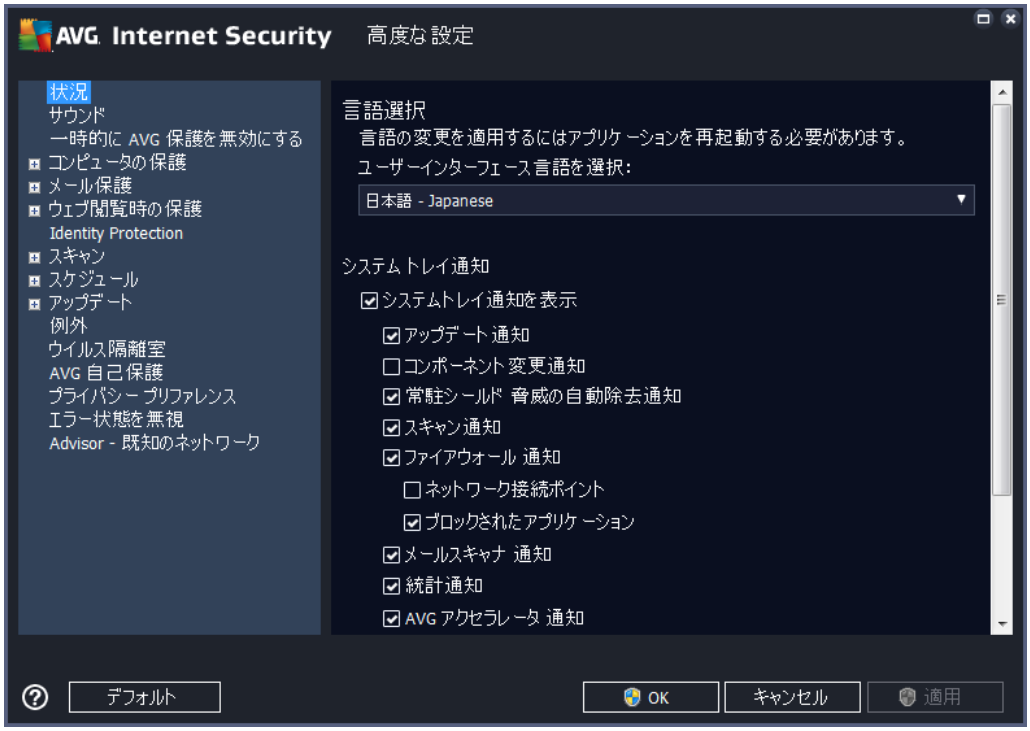
- ***Notify web sites ウェブサイトの通知 ...*** - このセクションでは ***トラックしたくないウェブサイトを通知*** オプション *をオン/オフに切り替えられます (デフォルトではオン)*。追跡されたくない検知データをプロバイダーに知らせるには ***Do Not Track*** の機能を選択します。

9. AVG 高度な設定

AVG Internet Security 2015 の高度な設定ダイアログは [***高度な AVG 設定***] という名前の新しいダイアログで開きます。このウィンドウは 2つのセクションにわかれています。左部はにツリー状のナビゲーションが表示されます。設定を変更したいコンポーネント (*または特定の部分*) を選択すると、ウィンドウ右側のセクションに編集ダイアログが表示されます。

9.1. 表示

ナビゲーション ツリーの最初の項目である [***状況***] は **AVG Internet Security 2015** ユーザーインターフェースの全般設定を参照し、アプリケーションの動作の基本オプションを示します。



言語選択

[***言語選択***] セクションでは、任意の言語をドロップダウン メニューから選択できます。選択した言語は、**AVG Internet Security 2015** ユーザーインターフェース全体で使用されます。ドロップダウン メニューには、インストール処理中に選択した言語と英語 (*既定で自動的にインストール*) のみが表示されます。**AVG Internet Security 2015** の言語切り替えが完了した場合は、アプリケーションを再起動する必要があります。次の手順を実行してください。

- ドロップダウン メニューで任意のアプリケーション言語を選択します。
- [***適用***] ボタン (ダイアログの右下端)をクリックして選択内容を確定します。
- [*OK*] ボタンをクリックして、確定します。
- 新しいダイアログがポップアップ表示され、アプリケーションの言語を変更するには **AVG Internet Security 2015**

- [***今すぐAVG を再起動***] ボタンをクリックしてプログラムの再起動を許可し、その後すぐに言語変更が有効になります。

システム トレイ通知

このセクションでは、**AVG Internet Security 2015** アプリケーションのステータスに関するシステム トレイ通知を非表示に設定できます。既定ではシステム通知の表示は有効です。この設定を保持することをお勧めします。システム通知は、スキャンまたはアップデート プロセスの実行や ,**AVG Internet Security 2015** コンポーネントのステータス変更などを通知します。このような通知には特に注意する必要があります。

ただし、何らかの理由で、このような方法で通知しない場合や、ある通知 *(特定の AVG Internet Security 2015 コンポーネントに関する)*のみを表示する場合は、次のオプションにより任意の内容を定義および指定できます。

- ***システム トレイ通知を表示する****(既定では有効)* 既定ではすべての通知が表示されます。この項目のチェックを外すとすべてのシステム通知表示は無効になります。オンにした場合は、表示する通知を選択できます。
    - ***アップデート通知*** *(既定では有効)* **AVG Internet Security 2015**アップデート処理の起動、進行、完了に関する情報を表示するかどうかを決定します。
    - ***コンポーネント変更の通知*** *(既定では無効)* コンポーネントの有効/無効、または潜在的な問題に関する情報を表示するかどうかを決定します。コンポーネントの不具合状態をレポートする際、このオプションは、すべての **AVG Internet Security 2015** コンポーネントの問題をレポートするシステム トレイ アイコンの便利な機能と同様の役割を果たします。
    - ***常駐シールド自動脅威削除の通知 (自動アクション)****(既定では有効)* ファイルの保存、コピー、開く処理に関する情報を表示するかどうかを決定します *(この設定は、常駐シールドの [自動修復] オプションが選択されている場合にのみ有効です)*。
    - ***スキャン通知*** *(既定では有効)* スケジュールされたスキャンの自動起動、進行、結果に関する情報を表示するかどうかを決定します。
    - ***ファイアウォール通知*** *(既定では有効)* コンポーネントの有効化/無効化の警告、トラフィック ブロックなど、ファイアウォール状態とプロセスに関する情報を表示するかどうかを決定します。たとえば、コンポーネントの有効化/非有効化警告、トラフィックのブロックなどが表示されます。この項目にはさらに 2つの選択オプションがあります *(各オプションの詳細については、このマニュアルの「ファイアウォール」の章を参照してください)*。
        - ***ネットワーク接続ポイント*** *(規定では無効)* ネットワークに接続している場合、はネットワークが既知であるかどうか、プリンタの共有がどのように設定されているかを通知します。

-***ブロックされたアプリケーション***(*規定では有効*) - 不明または不審なアプリケーションがネットワークへ接続しようとしている場合にはその試みをブロックし、通知を表示します。必ず通知されて便利なため、常にこの機能を有効にしておくことをお勧めします。

- ***メール スキャナ通知*** (*既定では有効*) - すべての送受信メールに関する情報を表示するかどうかを決定します。
- ***統計情報に関する通知*** (*既定では有効*) - このオプションにチェックを付けると、定期的な統計情報確認通知をシステム トレイに表示できます。
- ***AVG アクセラレータに関する通知***(*既定では有効*) - ***AVG アクセラレータ***動作に関する通知を表示するかどうかを決定します。***AVG アクセラレータ*** サービスはオンラインビデオの再生をスムーズにして、ダウンロードを簡単にします。
- ***ブート時間向上に関する通知*** (*規定では無効*) - お使いのコンピュータのブート時間の短縮について通知するかどうかを決定します。
- ***AVG Advisor に関する通知***(*既定では有効*) - AVG Advisor の活動に関する情報をシステム トレイ上のスライド パネルに表示するかどうかを決定します。

ゲーム モード

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

9.2. サウンド

サウンドダイアログでは、サウンド通知によって特定の **AVG Internet Security 2015** アクションの通知を行うかどうかを指定できます。

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

コントロール ボタン

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

9.3. 一時的に AVG 保護を無効にする

[***一時的に AVG 保護を無効にする***] ダイアログでは、**AVG Internet Security 2015** の保護機能をすべて一度にオフにできます。

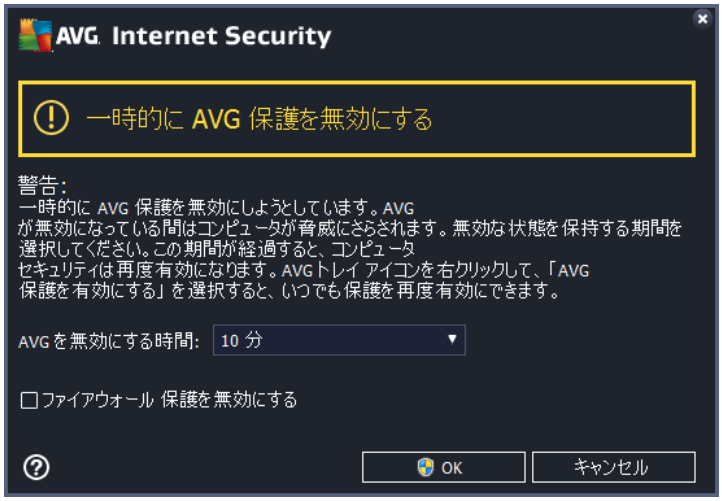
やむを得ない場合を除き、このオプションの使用はお勧めしません。

インストール処理中に望ましくない中断が発生しないようにするために、インストーラやソフトウェア ウィザードで実行中のプログラムやアプリケーションを終了するように指示される場合がありますが、それでも通常は新しいソフトウェアやドライバをインストールする前に、**AVG Internet Security 2015** を無効にする***必要はありません***。インストール中に問題が発生した場合は、常駐保護を無効にすることを試みてください。*(リンク先のダイアログで、最初に [**常駐シールドを有効化する**] 項目のチェックを外します)*。**AVG Internet Security 2015** を一時的に無効にしなければならない場合は、必要な作業が終わったらすぐに再度有効にする必要があります。ウイルス対策ソフトウェアが無効な状態でインターネットやネットワークに接続している場合は、コンピュータが攻撃の危険にさらされています。

AVG 保護を一時的に無効にする方法

[***一時的に AVG 保護を無効にする***] チェックボックスを選択し、[***適用***] ボタンをクリックして選択内容を確定します。新しく開いた ***一時的に AVG 保護を無効にする*** ダイアログで、**AVG Internet Security 2015** を無効にする時間を指定します。既定では、保護は 10分間無効になります。新しいソフトウェアのインストールなどの一般的なタスクを実行するには十分な時間です。もう少し時間を長くすることもできますが、このオプションはどうしても必要な場合を除き、推奨されません。その後、無効にされたコンポーネントはすべて自動的に再度有効になります。最長で、次のコンピュータの再起動まで AVG 保護を無効にできます。***一時的に AVG 保護を無効にする*** ダイアログには、***ファイアウォール*** コンポーネントをオフにする別のオプションがあります。これを行うには、[***ファイアウォール保護を無効に***

する] にチェックを付けます。



9.4. コンピュータの保護

9.4.1. ウイルス対策

ウイルス対策は、***常駐シールド***と連携し、あらゆる既知の種類のウイルスとスパイウェア、マルウェア一般 *(ダウンロードされた後まだ有効化されていないマルウェアなど、いわゆる休止状態の非アクティブなマルウェアを含む)*からコンピュータを継続的に保護します。

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

- ***脅威を駆除する前に確認する*** (*既定ではオン*) - チェックを付けると、常駐シールドによってアクションが自動的に実行されなくなり、代わりに検出された脅威について説明し、処理方法を決定するダイアログが表示されます。チェックを外したままにすると、**AVG Internet Security 2015** は自動的に感染を修復し、修復できない場合はオブジェクトをウイルス隔離室に移動します。

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

- ***不審なプログラムの拡張セットをレポート*** (*既定ではオフ*) - チェックを付けると、スパイウェアの拡張パッケージを検出します。スパイウェアとは、直接製造元から入手する場合には完全に問題がなく無害なプログラムですが、後から悪意のある目的で誤用されるおそれのあるプログラムです。これは、コンピュータセキュリティをさらに高めるための追加的な手段ですが、合法的なプログラムもブロックする可能性があるため、既定ではオフになっています。

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

- ***リムーバブルメディアの起動セクタをスキャンする*** (*既定ではオン*) - チェックを付けると、挿入された USB フラッシュディスク、外部ディスクドライブ、その他のリムーバブルメディアの起動セクタで脅威スキャンを実行します。

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

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

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

- ***インスタントメッセージと P2P ダウンロード保護を有効にする*** (*既定ではオン*) - この項目にチェックを付けると、インスタントメッセージの通信 (*AIM、Yahoo!、Windows Live Messenger、ICQ、Skype...*) と、ピアツーピアのネットワーク (*サーバーを介さずにクライアント間の直接の接続を許可する、潜在的に危険なネットワーク。通常は音楽ファイルの共有に使用*) 内でダウンロードされるデータを確認してウイルスを除去します

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

該当するチェックボックスを選択すると、***すべてのファイルをスキャン***するか、***感染可能なファイルと選択した種類のドキュメント***のみをスキャンするかどうかを決定します。スキャンを高速化しながら最高水準の保護を維持するために、既定の設定を維持することをお勧めします。既定の設定では、感染の可能性があるファイルのみがスキャンされます。ダイアログの各セクションには、スキャン対象の定義ファイルの拡張子リストが表示されます。このリストは編集可能です。

拡張子のないファイルを必ずスキャンする (*デフォルトではオン*) にチェックを付けると、拡張子がなく未知の形式でも常駐シールドによってスキャンされることが保証されます。拡張子のないファイルは疑わしいため、この機能をオンにしておくことを推奨します。

9.4.2. ルートキット対策

ルートキット対策設定 ダイアログでは、***ルートキット対策***サービスの設定とルートキット対策スキャンの特定のパラメータを編集できます。ルートキット対策スキャンは、全コンピュータをスキャンに含まれる既定の処理です。

アプリケーション スキャンと***ドライバ スキャン***では、ルートキット対策スキャンの対象を詳細に指定することができます。これらの設定は上級者ユーザー向けです。すべてのオプションをオンにしておくことをお勧めします。また、ルートキット スキャン モードを選択することもできます。

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

9.4.3. キャッシュサーバー

[***キャッシュ サーバー設定***] ダイアログは、すべての種類の **AVG Internet Security 2015** スキャンを高速化するためのキャッシュ サーバー プロセスを参照します。

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

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

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

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

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

9.5. メール スキャナ

このセクションでは、メール スキャナとスパム対策の詳細設定を編集できます。

9.5.1. メールスキャン

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 されるメールに関 する基 本 項 目 を設 定 できます。

- ***受 信 メールをチェックする*** (*既 定 ではオン*) - このボックスを選 択 */*クリアすることで、メール クライアントに配 信 されるすべてのメール メッセージをスキャンするかどうかを選 択 します。
- ***送 信 メールをチェックする*** (*既 定 ではオフ*) - このボックスを選 択 */*クリアすることで、自 分 のアカウントから送 信 されるすべてのメール メッセージをスキャンするかどうかを選 択 します。
- ***ウイルス感 染 したメッセージの件 名 を修 正 する*** (*既 定 ではオフ*) - スキャンによって感 染 メッセージとして検 出 されたメール メッセージに関 する警 告 を表 示 する場 合 は、この項 目 にチェックを付 け、テキスト フィールドに任 意 のテキストを入 力 します。このテキストがすべての感 染 メールの [件 名] フィールドに追 加 されるため、感 染 メッセージを簡 単 に識 別 し除 外 できます。 初 期 値 は ***VIRUS*** です。この値 を使 用 することをお勧 めします。

スキャン プロパティ

このセクションでは、メール メッセージのスキャン方 法 を指 定 できます。

- ***ヒューリスティック分 析 を使 用 する*** (*既 定 ではオン*) - チェックを付 けると、メール メッセージをスキャンするときにヒューリスティック検 出 方 式 使 用 します。 このオプションをオンにすると、拡 張 子 だけでなく実 際 の添 付 ファイルの内 容 を考 慮 して、メールの添 付 ファイルをフィルタできます。フィルタリングは [メール フィルタリング] ダイアログで設 定 できます。

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

- ***不審なプログラムの拡張セットを報告する*** (*既定ではオフ*) - チェックを付けると、スパイウェアの拡張パッケージを検出します。スパイウェアとは、直接製造元から入手する場合には完全に問題がなく無害なプログラムですが、後から悪意のある目的で誤用されるおそれのあるプログラムです。これは、コンピュータセキュリティをさらに高めるための追加的な手段ですが、合法的なプログラムもブロックする可能性があるため、既定ではオフになっています。

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

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

メール添付ファイルの報告

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

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

- ***パスワード保護された文書を報告する*** - パスワード保護された文書はウイルススキャンできません。ボックスにチェックを付けると、潜在的に危険なものとしてこれらの文書を報告します。

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

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

- ***レポートされたメール添付ファイルをウイルス隔離室に移動*** - メールスキャンで検出された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、拡張子偽装を含むファイルの場合、メールでレポートするかどうかを指定します。このようなメールがスキャン中に検出された場合、検出された感染オブジェクトをウイルス隔離室に移動するかどうかについても指定することができます。

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

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

注意 :*指定された言語で表示されるのは既定のテキストのみであり、カスタマイズされたテキストは自動的に翻訳されないことに注意してください。*

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。アクティブ化する場合は、感染あるいは潜在的に危険だと検出されたすべてのメールメッセージ添付ファイルは自動的に除去されます。削除する添付ファイルのタイプを定義したい場合、各オプションを選択します。

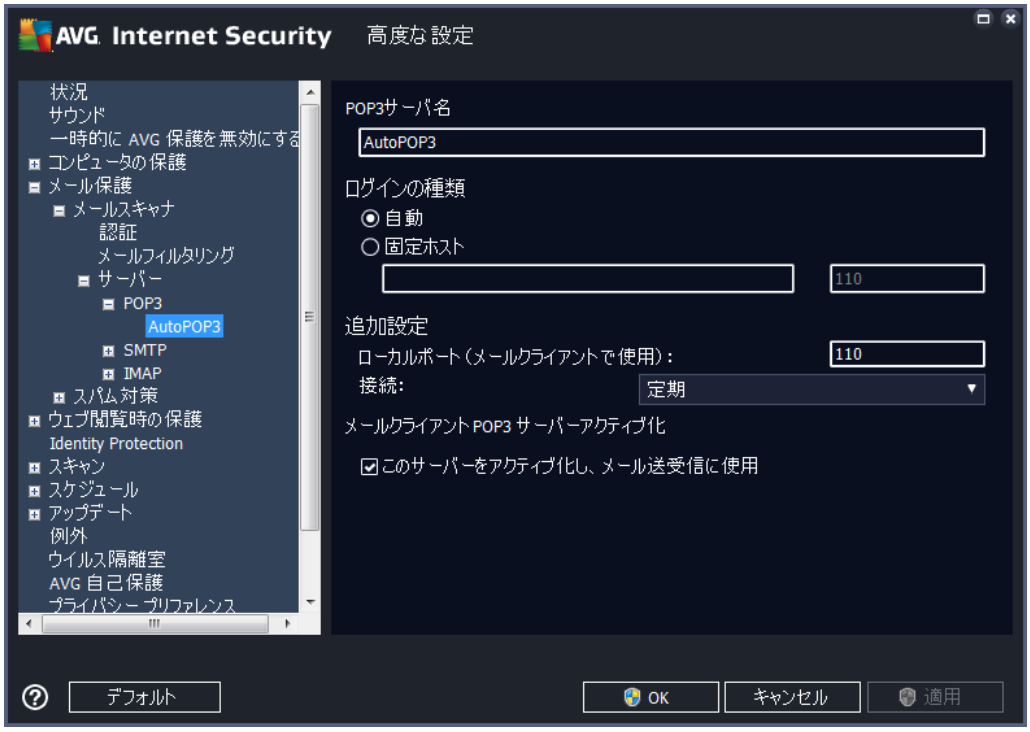
- ***すべての実行可能ファイルを削除*** - すべての *exe ファイルが削除されます。
- ***すべての文書を削除*** - すべての *doc、*docx、*xls、*xlsx ファイルが削除されます。
- ***これらのカンマ区切りの拡張子を含むファイルを除去*** - 定義された拡張子のすべてのファイルを削除します

サーバー セクションでは、メールスキャナ サーバーのパラメータを編集することができます。

- POP3 サーバー
- SMTPサーバー
- IMAP サーバー

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

受信メール用の POP3 プロトコルを使用してメール スキャナサーバーを設定できます。

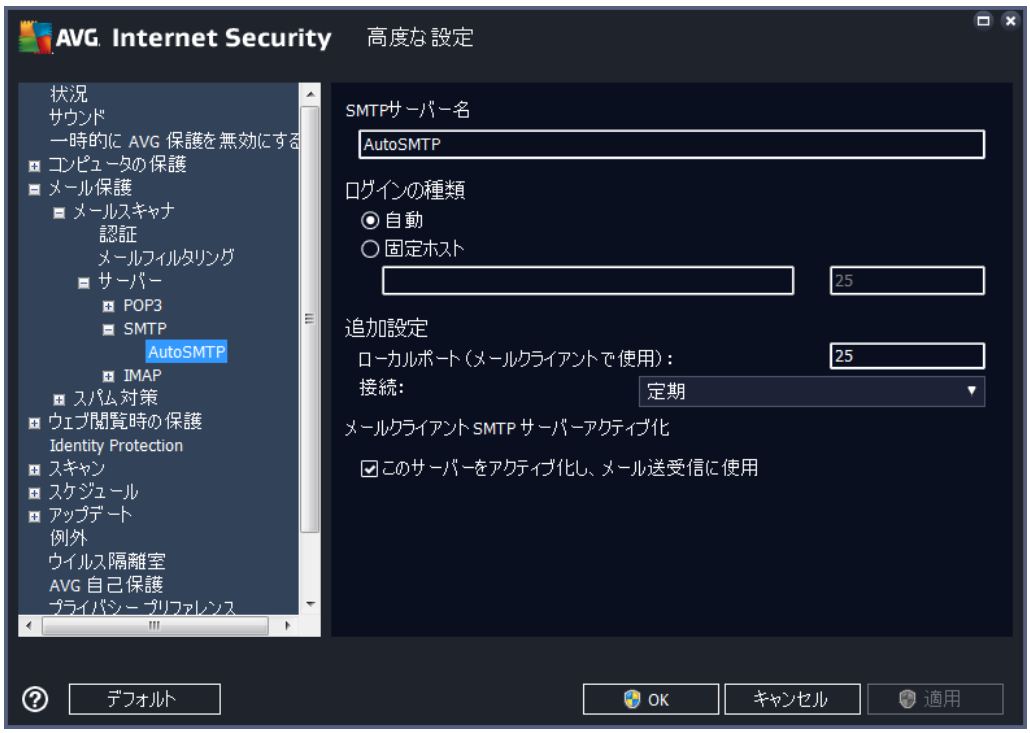


- ***POP3 サーバー名*** - このフィールドでは、新たに追加したサーバーの名前を指定できます（*POP3 サーバーを追加するには、左側のナビゲーション メニューの POP3 項目でマウスを右ク*

リックします）。

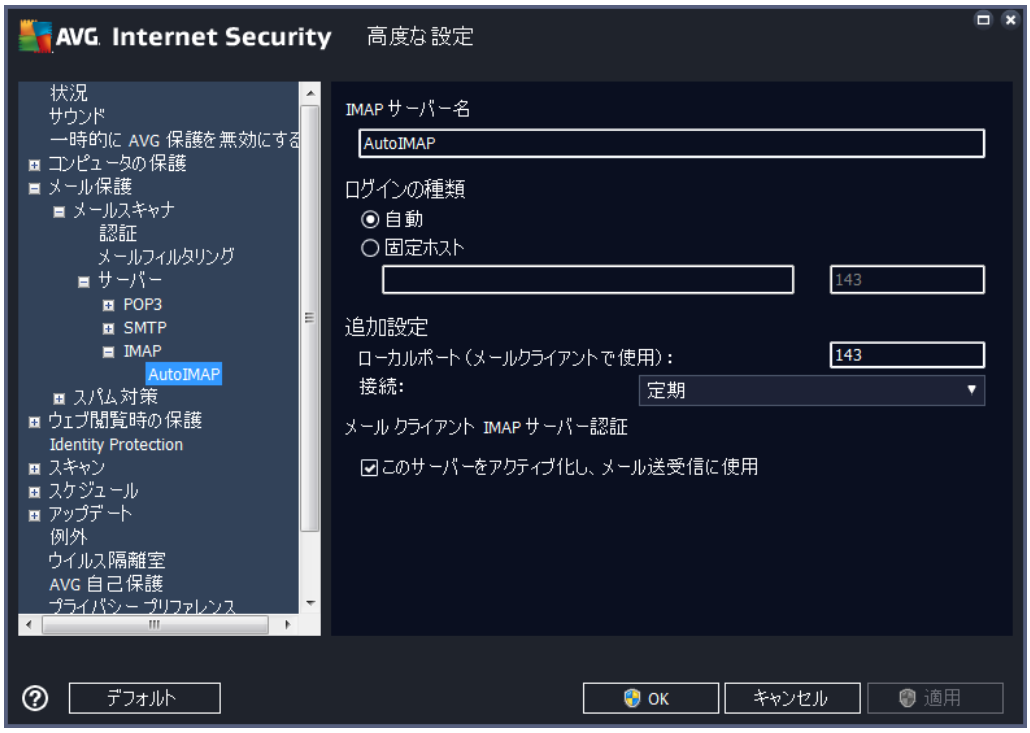
- ***ログインの種類*** - 受信メールに使用されるメールサーバーを決定する方法を定義します。
  - ***自動*** - メールクライアントの設定に従って、自動的にログインが行われます。
  - ***固定ホスト*** - プログラムは常にここで指定されたサーバーを使用します。メールサーバーのアドレスと名前を指定してください。ログイン名は変更されません。名前については、IP アドレス（*123.45.67.89* など）とドメイン名（*pop.acme.com* など）を使用できます。メールサーバーが標準以外のポートを使用する場合、このポートをコロンで区切り、サーバー名の後に指定できます（*pop.acme.com:8200*など）。POP3 通信の標準ポートは 110 です。
- ***追加設定*** - より詳細なパラメータを設定します。
  - ***ローカルポート*** - メールアプリケーションからの通信用ポートを指定します。メールアプリケーション上で、このポートをPOP3通信のポートとして指定する必要があります。
  - ***接続*** - *このドロップダウンメニューでは、使用する接続の種類*（通常 /SSL/SSL 既定）を指定できます。SSL 接続を選択した場合、送信データは第三者に追跡、監視されるリスクを負うことなく暗号化されます。この機能は送信先のメールサーバーが対応している場合にのみ使用可能です。
- ***メールクライアント POP3 サーバー有効化*** - このアイテムをチェック/チェック解除すると、指定された POP3 サーバーを有効化/無効化します。

送信メール用の SMTP プロトコルを使用して[メール スキャナ](#)サーバーを設定できます。



- ***SMTP サーバー名*** - このフィールドでは新しく追加したサーバー名を指定できます（*SMTP サーバーを追加するには、左側のナビゲーション メニューで SMTP 項目右クリックします*）。自動的に作成された「AutoSMTP」サーバーの場合は、このフィールドは無効になっています。
- ***ログイン タイプ*** - メール送信で使用するメール サーバーを決定する方法を定義します。
  - ***自動*** - ログインは、メール クライアントの設定に従って自動的に実行されます。
  - ***固定ホスト*** - プログラムは常にここで指定されたサーバーを使用します。メール サーバーのアドレスと名前を指定してください。名前については、ドメイン名（*smtp.acme.com* など）および IP アドレス（*123.45.67.89* など）を使用できます。メール サーバーが標準以外のポートを使用する場合、このポートをコロンで区切り、サーバー名の後に記述することができます（*たとえば、smtp.acme.com:8200*）。SMTP 通信の標準ポートは 25 です。
- ***追加設定*** - より詳細なパラメータを設定します。
  - ***ローカル ポート*** - メール アプリケーションからの通信用ポートを指定します。メール アプリケーション上で、このポートを SMTP 通信のポートとして指定する必要があります。
  - ***接続*** - このドロップダウン メニューでは、使用する接続の種類（*通常 / SSL/SSL 既定*）を指定できます。SSL 接続を選択した場合、送信データは第三者に追跡、監視されるリスクを負うことなく暗号化されます。この機能は送信先のメール サーバーがそれに対応している場合のみ使用可能です。
- ***メール クライアント SMTP サーバー有効化*** - このボックスのオン / オフを切り替えると、指定した SMTP サーバーの有効化と無効化を切り替えます。

このダイアログでは、送信メール用の IMAP プロトコルを使用して新しいメール スキャナサーバーを設定できます。

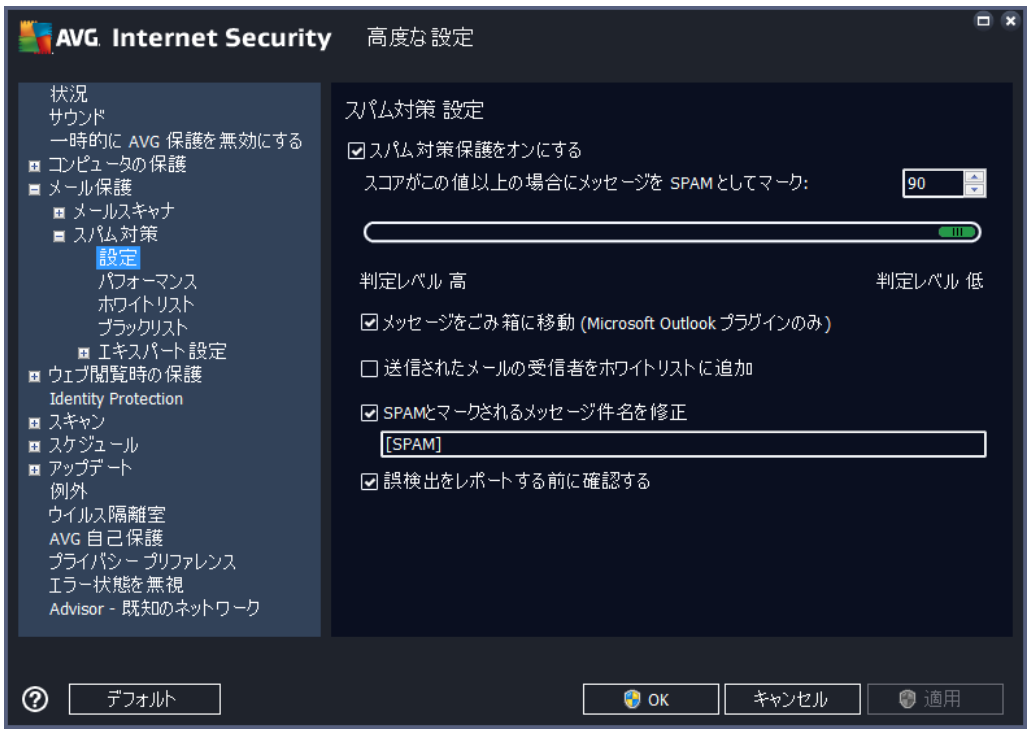


- ***IMAP サーバー名*** - このフィールドでは新たに追加したサーバーの名前を指定できます（*IMAP*

サーバーを追加するには、左側のナビゲーション メニューの IMAP の項目でマウスを右クリックします)。

- ***ログインの種類*** - メール送信で使用するメール サーバーを決定する方法を定義します。
  - ***自動*** - ログインは、メール クライアントの設定に従って自動的に実行されます。
  - ***固定ホスト*** - プログラムは常にここで指定されたサーバーを使用します。メール サーバーのアドレスと名前を指定してください。名前については、ドメイン名 (*mtp.acme.com* など)および IP アドレス (*123.45.67.89* など)を使用できます。メール サーバーが標準以外のポートを使用する場合、このポートをコロンで区切り、サーバー名の後に指定できます (*mtp.acme.com:8200* など)。IMAP 通信の標準ポートは 143です。
- ***追加設定*** - より詳細なパラメータを設定します。
  - ***ローカルポート*** - メールアプリケーションからの通信用ポートを指定します。IMAP 通信用ポートとして、このポートをメール アプリケーションで指定する必要があります。
  - ***接続*** - このドロップダウン メニューでは、使用する接続の種類 (*通常 /SSL/SSL 既定*)を指定できます。SSL 接続を選択した場合、送信データは暗号化され、データが第三者によって追跡あるいは監視されるリスクを回避できます。この機能は送信先のメール サーバーがそれに対応している場合のみ使用可能です。
- ***メール クライアント IMAP サーバーを有効にする*** - このボックスを選択/クリアすると、指定した IMAP サーバーを有効/無効にします。

9.5.2. スパム対策



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

次に、スコアの判定レベルを選択することができます。***スパム対策*** フィルタは、複数の動的スキャン技術に基づいて、各メッセージにスコアを割り当てます（*例えば、メッセージの内容がSPAMにどの程度類似しているか*等）。値を入力するか、スライダを左右に動かして、[***スコアがこの値を超える場合はメッセージをスパムと見なす***] 設定を調整できます。

値の範囲は 50～ 90に制限されています。以下はスコアの閾値の一般的な概要です。

- ***値 80～ 90*** - スパムの可能性が高いメールは除外されます。一部の正常なメッセージも誤って除外される可能性があります。
- ***値 60～ 79*** - かなり積極的な設定でスパムの可能性があるメールは除外されます。正常なメッセージも除外される可能性があります。
- ***値 50～ 59*** - 非常に積極的な設定です。スパムではないメールが、本物のスパムメールと同様に除去される可能性が高くなります。***通常、この値は推奨されません。***

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

- ***メッセージを迷惑メールフォルダに移動*** *(Microsoft Outlook プラグインのみ)* この項目をチェックすると、検出された各スパムメッセージが自動的に MS Outlook メールクライアントの特定の迷惑メールフォルダに移動するよう指定できます。現時点では、この機能はほかのメールクライアントではサポートされていません。
- ***送信メールの受信者をホワイトリストに追加*** - このチェックボックスにチェックを付けると、すべての送信メールの受信者が信頼でき、その受信者のメールアカウントから送信されるすべてのメールメッセージの配信を許可することを承認します。
- ***スパムとして判定されたメッセージの件名を修正*** - スパムとして検出されたメッセージの件名にを特定の単語や文字を追加したい場合、このチェックボックスにチェックを付けます。追加するテキストをテキストフィールドに入力します。
- ***誤検出をレポートする前に確認する*** - インストール処理中に、プライバシーのプリファレンスプロジェクトに参加することに参加した場合に指定できます。検出された脅威が AVG に報告されます。レポートは自動的に作成されます。ただしこのチェックボックスは、検出されたスパムを AVG に報告する前に、通知を表示してメッセージが本当にスパムメールであるかどうかを確認したい場合に選択します。

エンジン パフォーマンス設定ダイアログ（左側のナビゲーションの***パフォーマンス***を選択すると表示されます）では、***スパム対策***コンポーネントのパフォーマンスを設定します。

スライダを左右に動かして、***ローエンド デスクトップ/ハイエンド デスクトップ***の間で、スキャン パフォーマンス範囲のレベルを変更します。

- ***ローエンド デスクトップ***- スパムを判定するスキャン処理中に、ルールは使用されません。学習データのみが判定に使用されます。コンピュータ ハードウェア性能が著しく低い場合などをのぞき、このモードは一般の利用には推奨されません。
- ***ハイエンド デスクトップ***- このモードでは大量のメモリを消費します。スパムを判定するスキャンの処理中には、ルールとスパム データベース キャッシュ、基本ルールと高度なルール、スパム送信者 IP アドレス、スパム送信者データベースの機能が使用されます。

[***オンライン チェックを有効にする***] は既定でオンとなっています。これにより、Mailshell サーバーとの通信によってスキャン データが Mailshell データベースとオンラインで比較されるため、より正確なスパム検出が実行されます。

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

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

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

コントロール ボタン

次のコントロール ボタンを利用できます。

- ***編集*** - このボタンをクリックすると、ダイアログが開きます。このダイアログでは、手動でアドレスのリストを入力できます（*コピーとペースト*も使用できます）。1行に1アイテム（*送信者*、*ドメイン名*）を入力します。
- ***エクスポート*** - 何らかの目的でレコードをエクスポートする場合は、このボタンをクリックします。すべてのレコードがプレーン テキスト形式で保存されます。
- ***インポート*** - すでにメールアドレスやドメイン名のテキストファイルお持ちの場合、このボタンを選択することで単純にそのリストをインポートすることができます。ファイルの内容については、1行につき 1項目（*アドレス*、*ドメイン名*）のみを含める必要があります。

ブラックリストは、スパム送信者としてブロックするメール アドレスとドメイン名のリストを含むダイアログを開きます。

編集インターフェースでは、望ましくないメッセージ（スパム）を送信するであろう送信者のリストを編集します。また、スパムメッセージが送信される完全なドメイン名リスト（*spammingcompany.com* など）を編集できます。リスト中のアドレスとドメインからのメールは、すべてスパムとして判定されます。既にスパム送信者やドメイン名のリストがある場合は、各メールアドレスを直接入力するか、一度にアドレスの全リストをインポートすることでリストを入力できます。

コントロール ボタン

次のコントロール ボタンを利用できます。

- ***編集*** - このボタンをクリックすると、ダイアログが開きます。このダイアログでは、手動でアドレスのリストを入力できます（*コピーとペースト*も使用できます）。1行に1アイテム（*送信者*、*ドメイン名*）を入力します。
- ***エクスポート*** - 何らかの目的でレコードをエクスポートする場合は、このボタンをクリックします。すべてのレコードがプレーン テキスト形式で保存されます。
- ***インポート*** - すでにメールアドレスやドメイン名のテキストファイルお持ちの場合、このボタンを選択することで単純にそのリストをインポートすることができます。

エキスパート設定には、スパム対策機能の多数の設定オプションが含まれています。これらの設定は、詳細なスパム対策設定が必要とするネットワーク管理者のような、経験あるユーザー専用です。このため、個々のダイアログに関する詳細なヘルプは提供されていません。各オプションの簡単な説明については、ユーザー インターフェース上に直接表示されます。Spamcatcher (MailShell Inc.) の高度な設定に精通していない場合は、設定変更を行わないことを強くお勧めします。ファイルが不適切に変更された場合は、パフォーマンスの悪化やコンポーネント機能の不正動作につながるおそれがあります。

それでも高度なレベルでスパム対策の設定を変更する必要があると考えられる場合、ユーザー インターフェースで直接提供される指示に従ってください。一般には、各ダイアログで 1つの特定の機能を見ることができ、それを編集できます。その説明は常にダイアログに表示されます。ユーザーは、次のパラメータを編集することができます。

- ***フィルタリング*** - 言語リスト、国リスト、許可された IP、ブロックする IP、ブロックする国、ブロックする文字セット、スプーフィング送信者
- ***RBL*** - RBL サーバー、マルチヒット、しきい値、タイムアウト、最大 IP
- ***インターネット接続*** - タイムアウト、プロキシサーバー、プロキシ認証

9.6. ウェブ閲覧時の保護

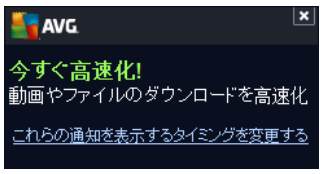
リンクスキャナ設定 ダイアログでは、次の機能のオン/オフを切り替えることができます。

- ***サーフシールドを有効化*** - (*既定ではオン*) エクスプロイト サイトにアクセスした時、サイトに対するアクティブな (*リアルタイムの*) 保護を有効化します。ユーザーが Web ブラウザ (*あるいは他のHTTP を使用するアプリケーション*) から Web ページにアクセスする際、既知の悪意のあるサイトへの接続と、エクスプロイト コンテンツがブロックされます。

9.6.1. オンライン シールド

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

- ***オンライン シールドを有効にする*** *(既定では有効)* ***オンライン シールド*** サービス全体を有効または無効にします。***オンライン シールド***の高度な設定については、次に表示される [Web 保護] ダイアログで設定します。
- ***AVG Accelerator を有効にする*** *(既定では有効)* AVG Accelerator サービスを有効または無効にします。AVG Accelerator はオンライン ビデオのサービスをスムーズにして、ダウンロードを簡単にします。ビデオ高速化処理を実行しているときには、システム トレイ ポップアップ ウィンドウに通知が表示されます。



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 (標準ポップアップ ダイアログ、トレイ バルーン通知、あるいはトレイ アイコン情報)を選択します。

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。

- ***アーカイブをチェックする*** - (*既定ではオフ*): WWW ページに含まれるアーカイブ コンテンツをスキャンします。
- ***不審なプログラムとスパイウェア脅威を報告する*** - (*デフォルトではオン*): チェックを付けると、ウイルスと同時にスパイウェアのスキャンもアクティベートします。スパイウェアは疑わしいマルウェアのカテゴリに含まれます。通常は、セキュリティリスクとなる場合でも、このようなプログラムを故意にインストールすることができます。コンピュータのセキュリティを高めるため、この機能を有効にしておくことをお勧めします。
- ***不審なプログラムの拡張セットをレポート*** - (*デフォルトではオフ*): チェックを付けると、スパイウェアの拡張パッケージを検出します。スパイウェアとは、直接製造元から入手する場合には、完全に問題がなく、無害なプログラムですが、後から悪意のある目的で誤用される可能性のあるプログラムです。これは、コンピュータセキュリティをさらに高めるための追加的な手段ですが、合法的なプログラムもブロックする可能性があるため、既定ではオフになっています。
- ***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*）を使用して、*表示されるページコンテンツをスキャンします*。
- ***完全スキャンを有効にする*** - (*デフォルトではオフ*): このオプションにチェックを付けると、特定の状況（*コンピュータが感染している疑いがある場合など*）が発生した場合に最も完全なスキャン アルゴリズムを有効にし、感染の可能性が非常に低いコンピュータ領域もスキャンします。これにより、問題がないことを確実にします。この方法を実行すると多少時間がかかります。

- ***暗号化 (TLS および SSL) ネットワークトラフィック*** - (*デフォルトではオン*) すべての暗号化されたネットワーク、すなわちセキュリティプロトコル (SSL とその新しいバージョンである TLS) のスキャンも AVG に許可するにはこのオプションにチェックを付けたままにします。これは HTTPS を使用する Web サイト、および TLS/SSL を使用するメールクライアント接続が該当します。保護されたトラフィックは復号、およびマルウェアのスキャンが行われ、ユーザーのコンピュータに安全に配信するために再度暗号化されます。このオプションでは、***拡張検証 (EV) 証明書付きサーバーからのトラフィックを含める***て、拡張検証証明書付きサーバーからの暗号化されたネットワーク通信もスキャンするかどうかを決定できます。*EV 証明書の発行には認証機関による詳細な検証が必要とされるため、この証明書の下に運営される Web サイトは信頼性が非常に高い (マルウェアを配布する可能性が低い) です。*この理由のため、EV 証明書付きサーバーからのトラフィックはスキャンしないことにすると、暗号化通信を比較的高速に実行できます。

- ***常駐シールドで、ダウンロードした実行ファイルをスキャン*** - (*デフォルトではオン*): 実行ファイル (*一般的な拡張子は exe、bat、com など*) をダウンロード後にスキャンします。常駐シールドは、ダウンロードを行う前にファイルをスキャンし、コンピュータに悪意のあるファイルが入り込まないようにします。しかし、このスキャンは***スキャン対象ファイルの最大部分サイズ***による制限があります -このダイアログの次の事項をご覧ください。そのため大きなファイルのスキャンは部分ごとに実施されますが、これがほとんどの実行ファイルにも当てはまります。実行ファイルは、コンピュータ内でさまざまなタスクを実施できるため、100% 安全でなければなりません。これは、ダウンロード前に部分的なファイルスキャンを行い、ダウンロード完了後にもスキャンを行うことで確実になります。このオプションをチェックされることを推奨します。このオプションを無効にしても、AVG が潜在的に危険なコードを検出するため安心はできます。通常の場合、実行ファイルをひとつの複合体として評価できないため、誤検出が発生する可能性があります。

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

9.7. Identity Protection

Identity Protection はマルウェア対策コンポーネントであり、あらゆる種類のマルウェア (*スパイウェア、ボット、ID 窃盗など*) に対する保護を提供します。行動分析技術を使用して、発生したばかりの新しいウイルスに対する保護を提供します (*コンポーネントの機能に関する詳細については、Identity Protection の章を参照してください*)。

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

Identity Protection を有効化 *(既定ではオン)* -チェックを外すと、Identity Protection コンポーネントがオフになります。***やむを得ない場合を除き、このオプションをオフにしないことを強くお勧めします。*** Identity Protection が有効化されている場合は、脅威が検出されたときの動作を指定できます。

- ***常にプロンプトを表示*** - 脅威が検出されたときに、隔離室に移動するか否か確認するプロンプトが表示され、実行するアプリケーションが削除されることがなくなります。
- ***自動的に検出された脅威を隔離*** - このチェックボックスをオンにすると、検出されたすべての潜在的な脅威は、即座にウイルス隔離室の安全な場所に移動されます。既定の設定を保持していると、脅威が検出されたときに、隔離室に移動するかを確認するプロンプトが表示され、実行するアプリケーションが削除されないようになります。
- ***自動的に既知の脅威を隔離*** *(既定ではオン)* -マルウェアの可能性があるものとして検出されたすべてのアプリケーションを自動的に即時にウイルス隔離室に移動する場合は、この項目をオンにしておきます。

9.8. スキャン

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

- 全コンピュータをスキャン - 事前に定義された標準のコンピュータ全体のスキャンです。
- 特定のファイルとフォルダ - 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。
- 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。
- 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です。

9.8.1. 全コンピュータをスキャン

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

スキャン設定

スキャン設定セクションでは、任意にオン/オフできるスキャンパラメータのリストを提供します。

- ***感染を修復/除去する際に確認メッセージを表示しない***(*既定ではオン*) - スキャン実行中にウイルスが特定された際、修復可能な場合は自動で修復されます。感染したファイルを自動的に修復できない場合、感染したオブジェクトはウイルス隔離室に移動されます。
- ***不審なプログラムとスパイウェア脅威をレポート***(*既定ではオン*) - チェックを付けると、スキャンを有効にし、ウイルスと同時にスパイウェアもスキャンします。スパイウェアは疑わしいマルウェアのカテゴリに含まれます。通常は、セキュリティリスクとなる場合でも、このようなプログラムを故意にインストールすることができます。コンピュータのセキュリティを高めるため、この機能を有効にしておくことをお勧めします。
- ***不審なプログラムの拡張セットを報告する***(*デフォルトではオフ*) - チェックを付けると、スパイウェアの拡張パッケージを検出します。スパイウェアとは、直接製造元から入手する場合には完全に問題がなく無害なプログラムですが、後から悪意のある目的で誤用されるおそれのあるプログラムです。これは、コンピュータセキュリティをさらに高めるための追加的な手段ですが、合法的なプログラムもブロックする可能性があるため、既定ではオフになっています。
- ***Tracking Cookie をスキャンする***(*デフォルトではオフ*) - このパラメータを定義することでCookieを検出します。(*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トの内容など、ユーザー固有の情報の認証、追跡、メンテナンスに使用されます*)。

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

- ***ヒューリスティック分析を使用*** (*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実行されるスキャン対象オブジェクト命令の動的エミュレーション*) は、スキャン実行中に採用されるウイルス検出方法の一つです。

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

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

- ***ルートキットをスキャンする*** (*既定ではオン*) - ルートキット対策スキャンでは、ルートキット、すなわちコンピュータ上でマルウェアの活動を隠すことができるプログラムや技術に該当するものが PC にあるかどうか調べます。ルートキットが検出されても、必ずしもコンピュータが感染しているというわけではありません。通常のアプリケーションの特有のドライバやセクションが誤ってルートキットとして検出される場合もあります。

スキャンするかどうかを判断することも必要です。

- ***すべてのファイルタイプ*** スキャンが不要なファイルの拡張子をカンマで区切って指定することにより (*保存後、カンマはセミコロンに変化*)、スキャンから除外するファイルを定義するオプションを備えています。

- ***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スキャンするよう指定できます (*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 - 多くの場合、これらのファイルは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は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、常に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。

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

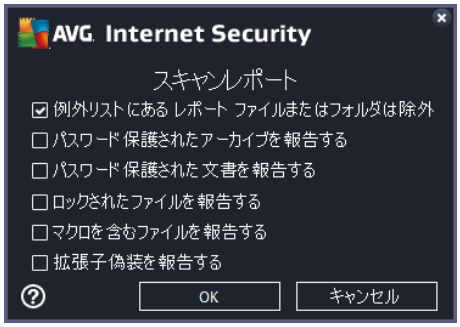
スキャン速度を調整

[***スキャン速度を調整***] セクションでは、システムリソース使用状況に応じて、任意のスキャン速度を指定できます。*既定ではこのオプションの値は、自動的にリソースを使用する*ユーザー依存レベルに設定されています。スキャン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量は著しく上がり、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量を下げることができます。

追加スキャンレポートを設定 ...

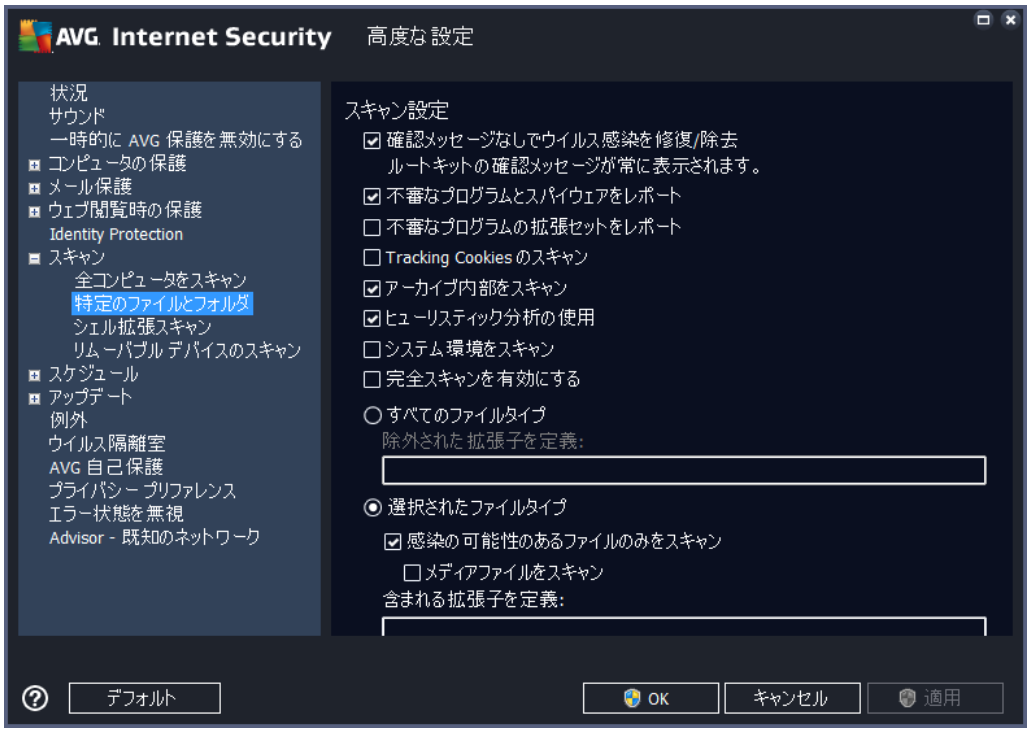
[***追加スキャンレポート...***] リンクをクリックすると、[***スキャンレポート***] ダイアログが開きます。このウィン

ドウでは報告する検出項目を定義します。



9.8.2. 特定のファイルとフォルダ

特定のファイルとフォルダの編集インターフェースは全コンピュータを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、デフォルト設定は全コンピュータをスキャンの場合にはより厳密なものとなっています。

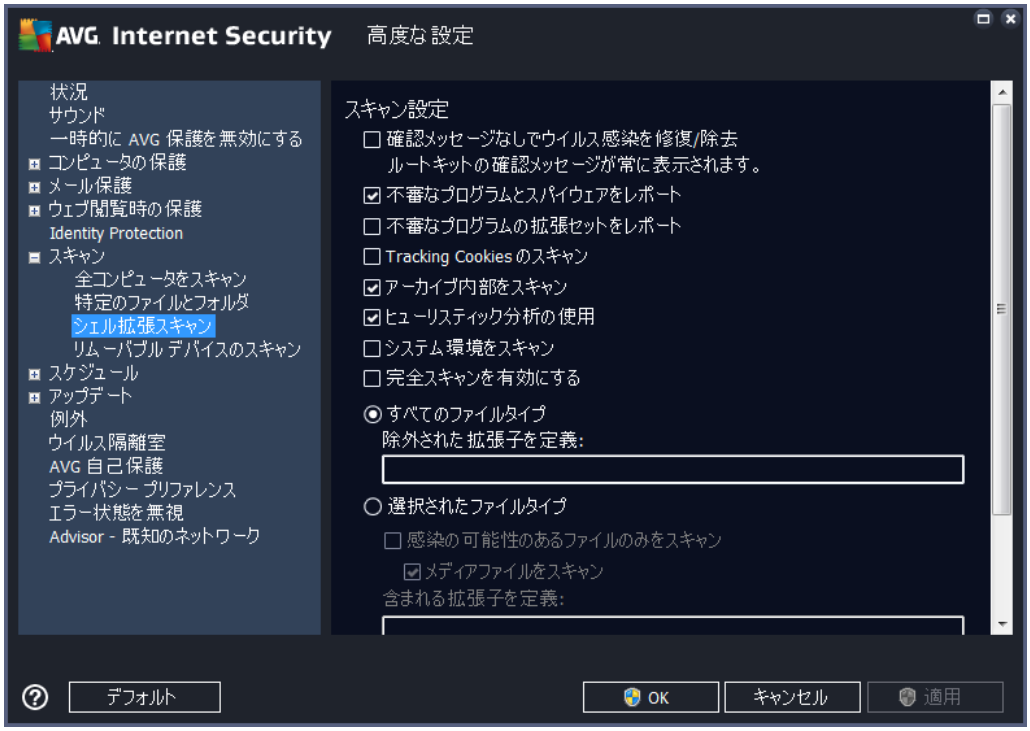


この設定ダイアログで設定されるすべてのパラメータは、特定のファイルとフォルダで選択されたスキャンエリアのみに適用されます。

注意:*特定のパラメータの説明については、AVG 高度な設定 /スキャン /全コンピュータをスキャンの章を参照して下さい。*

9.8.3. シェル拡張スキャン

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



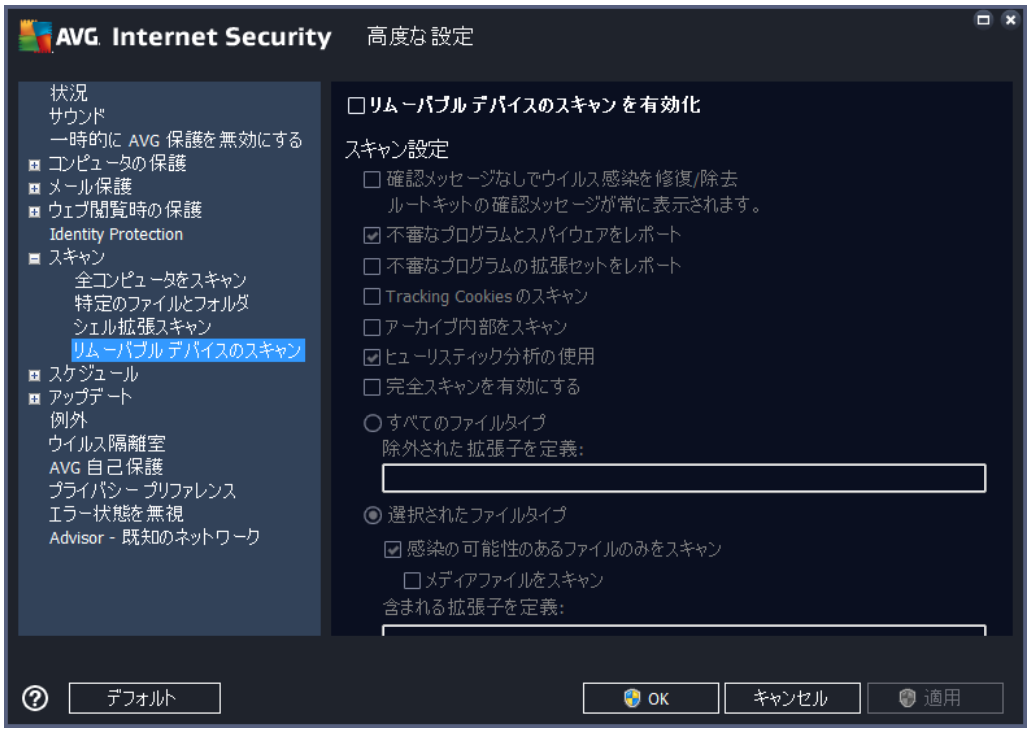
パラメータのリストは全 コンピュータをスキャンで利 用 できるものと同 一 です。ただし、既 定 の設 定 が異 なります *(たとえば、全 コンピュータをスキャンの場 合 、既 定 ではアーカイブをチェックせずにシステム環 境 をスキャンしますが、シェル拡 張 スキャンでは逆 になります)*。

注 意 :*特 定 のパラメータの説 明 については、AVG 高 度 な設 定 /スキャン /全 コンピュータをスキャンの章 を参 照 して下 さい。*

全 コンピュータをスキャン ダイアログと比 較 すると、***シェル拡 張 スキャン*** ダイアログには ***AVG ユーザー インターフェースのその他 の設 定*** セクションがあり、スキャンの進 行 状 況 を表 示 するかどうか、AVG ユーザー インターフェースからスキャン結 果 にアクセスできるようにするかを指 定 できます。また、スキャンで感 染 が検 出 された場 合 にのみスキャン結 果 を表 示 するように指 定 できます。

9.8.4. リムーバブル デバイスのスキャン

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



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

注意 :*特定のパラメータの説明については、AVG 高度な設定 /スキャン /全コンピュータをスキャンの章を参照して下さい。*

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。

- スケジュール スキャン
- 定義アップデート スケジュール
- プログラム アップデート スケジュール
- スパム対策アップデート スケジュール

9.9.1. スケジュール スキャン

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

次に、[***名前***] テキスト フィールド（*すべての既定のスケジュールでは無効化*）には、プログラム ベンダーによってこのスケジュールに割り当てられた名前を指定します。新しく追加されたスケジュール（*左側のナビゲーション ツリーにある [**スケジュール スキャン**] 項目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。一方で適切な名前の例としては、「システム エリア スキャン」などがあります。また、スキャンが全コンピュータをスキャンか、選択されたファイルと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必要もありません。ユーザー独自のスキャンは常に選択されたファイルとフォルダのスキャンの特定のバージョンになります。*

このダイアログでは、さらに以下のスキャン パラメータを定義できます。

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。タイミングは、一定の期間の後に繰り返されるスキャン開始を設定（***定期実行 ...***）または正確な日時を設定（***指定した時間に実行***）、あるいはスキャンの開始が関連付けられるイベントを設定（***コンピュータ起動時に実行***）する方法により定義できます。

高度なスケジュール オプション

- ***タスクが実行されなかった場合はコンピュータ起動時に実行*** ?指定した時間にタスクを実行するようスケジュールしていた場合、このオプションをチェックすると、スケジュールされた時間にコンピュータの電源がオフになっていた時でも必ず後でスキャンが実行されます。

- ***コンピュータが低電源モードの場合も実行*** ?スケジュールされた時刻にコンピュータがバッテリー電源で動作している場合も、タスクが実行されます。

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

- ***感染を修復/除去する際に確認メッセージを表示しない*** *(既定ではオン)*:スキャン実行中にウイルスが特定された際、修復可能な場合は自動で修復されます。感染したファイルを自動的に修復できない場合、感染したオブジェクトはウイルス隔離室に移動されます。

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

- ***不審なプログラムの拡張セットを報告する*** *(既定ではオフ)*: チェックを付けると、スパイウェアの拡張パッケージを検出します。スパイウェアとは、直接製造元から入手する場合には完全に問題がなく無害なプログラムですが、後から悪意のある目的で誤用されるおそれのあるプログラムです。これは、コンピュータ セキュリティをさらに高めるための追加的な手段ですが、合法的

なプログラムもブロックする可能性があるため、既定ではオフになっています。

- ***Tracking Cookies のスキャン*** (*デフォルトではオフ*): このパラメータを指定すると、スキャン実行中に Cookie を検出します (*HTTP cookie は、サイトの設定や電子ショッピングカートの内容など、ユーザー固有の情報の認証、追跡、メンテナンスに使用されます*)。

- ***アーカイブの内容をスキャンする*** (*既定ではオフ*): このパラメータを指定すると、ファイルが ZIP や RAR などのアーカイブで保存されている場合でも、すべてのファイルに対してスキャンチェックを実行します。

- ***ヒューリスティック分析を使用する*** (*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実行されるスキャン対象オブジェクト命令の動的エミュレーション*) は、スキャン実行中に採用されるウイルス検出方法の一つです。

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

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

- ***ルートキットのスキャン*** (*既定ではオン*):ルートキット対策スキャンは、コンピュータ上でマルウェアの活動を隠すことができるプログラムや技術など、可能なルートキットを検索します。ルートキットが検出されても、必ずしもコンピュータが感染しているというわけではありません。通常のアプリケーションの特有のドライバやセクションが誤ってルートキットとして検出される場合もあります。

スキャンするかどうかを判断することも必要です。

- ***すべてのファイルタイプ*** このオプションを使用すると、スキャンが不要なファイルの拡張子をカンマで区切ったリスト (*保存すると、カンマはセミコロンに変わります*) を指定することによってスキャンの例外を定義できます。

- ***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スキャンするよう指定できます (*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は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。

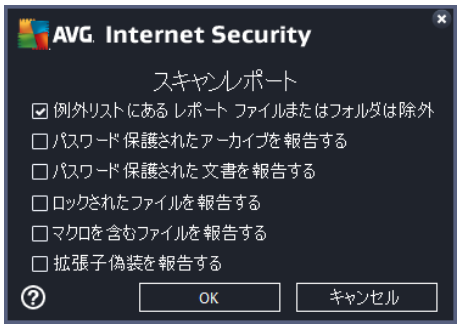
- 任意で***拡張子のないファイルをスキャン***できます。このオプションは既定ではオンになっています。変更する理由がない場合は、この設定を保持することをお勧めします。拡張子のないファイルは不審であるため、常にスキャンすることをお勧めします。

スキャン速度を調整

このセクションでは、さらに、システムリソース使用状況に応じて、希望するスキャン速度を指定することができます。既定ではこのオプションの値は、自動的にリソースを使用する*ユーザー依存*レベルに設定されています。スキャン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量は著しく上がり、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量を減らすことができます。

追加スキャンレポートを設定

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



コンピュータシャットダウンオプション

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

[***場所***] タブでは、[全コンピュータをスキャン] あるいは [特定のファイルとフォルダ] のどちらでスケジュール

するかを定義できます。特定のファイルとフォルダを選択した場合、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. 定義アップデート スケジュール

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

このダイアログ内では、定義アップデート スケジュールの一部の詳細パラメータを設定できます。[***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表示されます。

スケジュール実行

デフォルトでは、新しいウイルス検出のアップデートが使用可能になる度に、タスクが自動的に開始します。（***自動で実行***）。何か特別な理由がない限り、この設定を保持されることを推奨します。保持しない場合は、タスク開始を手動で設定でき、アップデート開始についての新しいスケジュール定義として、時間の間隔を指定できます。タイミングは、一定の期間の後に繰り返されるアップデートの開始を設定（***定期実行 ...***）、または正確な日時を設定（***指定した時間に実行***）する方法のいずれかにより定義できます。

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、定義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できます。スケジュールされた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

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

[***名前***] テキスト フィールド（*すべての既定のスケジュールで無効化*）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表示されます。

スケジュール実行

ここでは、新しくスケジュールされたプログラム アップデートを実行する時間を指定します。タイミングは、一定の期間の後に繰り返されるアップデート開始を設定（***定期実行***）または正確な日時を設定（***指定した時間に実行***）、あるいはアップデートの開始が関連付けられるイベントを設定（***コンピュータ起動時に実行***）する方法により定義できます。

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、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できます。スケジュール済みのアップデートが指定した時間に起動すると、AVG システム トレイ アイコン上に開くポップアップ ウィンドウによってこのことが通知されます（*高度な設定 表示ダイアログの既定の設定を保持している場合*）。

注意：*スケジュール済みのプログラム アップデートとスケジュール スキャンの時間が一致する場合は、アップデート プロセスが優先され、スキャンは中断されます。その場合はコリジョンについて通知されます。*

9.9.4. スパム対策アップデート スケジュール

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

このダイアログ内では、アップデート スケジュールの一部の詳細パラメータを設定できます。[***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を指定します。

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パム対策アップデート起動までの時間を指定します。タイミングは、一定の期間の後に繰り返されるスパム対策を設定（***定期実行***）または正確な日時を設定（***指定した時間に実行***）、あるいはアップデートの開始が関連付けられるイベントを設定（***コンピュータ起動時***

に実行）する方法により定義できます。

高度なスケジュール オプション

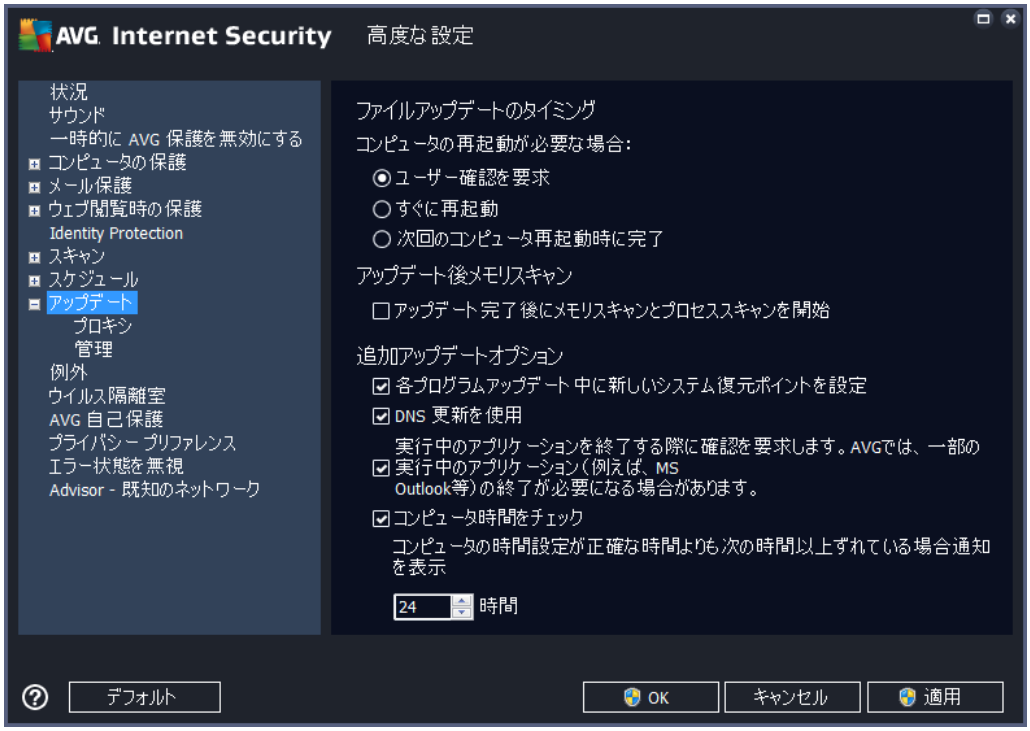
このセクションでは、コンピュータが低電力モードあるいは完全に電源オフになっている場合に、スパム対策アップデートが実行される条件を定義します。

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付けると、インターネット接続に障害が発生し、スパム対策アップデート処理が失敗した場合、インターネット接続が復旧した時点で必ず直ちにアップデートを再開できます。スケジュール済みのスキャンが指定した時間に起動すると、AVG システム トレイ アイコン上にポップアップ ウィンドウが開き、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. 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、アップデート処理によって PC の再起動が必要な場合に、3つのオプションから選択できます。次回の PC の再起動時にアップデートを完了するようにスケジュール設定するか、ただちに再起動できます。

- ***ユーザーの確認を要求***（*既定*）- アップデート処理完了に必要なPC再起動を確認する画面が表示されます。

- ***すぐに再起動*** - コンピュータはアップデート処理が完了した時点で、自動的に即時再起動されます。ユーザー確認は要求されません。

- ***次回のコンピュータの再起動時に完了*** - アップデート処理の完了は次回のコンピュータの再起動時まで延期されます。コンピュータが少なくとも1日に1回定期的に再起動することが確実である場合にのみ、このオプションが推奨されます。

アップデート後のメモリスキャン

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イルス定義が含まれている場合がありますが、即座にスキャン適用されます。

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時に新しいシステム復旧ポイントを作成*** - (*デフォルトではオン*) 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。アップデート処理が失敗し、オペレーティングシステムがクラッシュする場合には、必ずこのポイントから元の設定でOSを復旧できます。このオプションは、スタート/*プログラム*/*アクセサリ*/*システムツール*/システムの復元からアクセスできますが、上級ユーザーのみが変更を行うことをお勧めします。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する***(*既定ではオン*) - この項目にチェックを付けると、アップデートが実行された時点で、**AVG Internet Security 2015**がDNSサーバー上の最新のウイルスデータベースバージョンと最新のプログラムバージョンに関する情報を検索します。次に、最小限の必須のアップデートファイルのみがダウンロードされ、適用されます。この方法ではダウンロードされるデータ量が最低限に抑えられるため、アップデート処理が高速で実行されます。

- ***実行中のアプリケーションを終了する確認を要求***(*デフォルトではオン*) - をチェックすることで、アップデート処理の完了に必要な場合、現在実行中のアプリケーションが許可なく終了しないように確認できます。

- ***コンピュータ時間を確認***（*デフォルトではオン*） -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。

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

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

手動設定

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

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

プロキシ サーバーは、各ユーザーの独自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*** - 設定はデフォルトのインターネットブラウザから読み込まれます。
- ***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。

9.10.2. 管理

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

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

9.11. 例外

例外ダイアログでは、例外を定義できます。例外とは、**AVG Internet Security 2015** によって無視される項目です。通常、AVG が脅威としてプログラムやファイルを検出し続けたり、安全なウェブサイトを危険とみなしてブロックし続ける場合に例外の定義が必要になります。この例外リストにそのようなファイルやウェブサイトを追加すると、以降は AVG による報告やブロックがされなくなります。

問題になっているファイルやプログラム、ウェブサイトが本当に間違いなく安全かを常に確認してください。

既に例外が定義されている場合、ダイアログの表には例外の一覧が表示されます。各項目の隣にはチェックボックスがあります。チェックボックスが選択されている場合は、例外が有効です。選択解除されている場合は、例外は定義されていますが、現在使用されていません。列ヘッダーをクリックすると、該当する条件に基づいて許可されたアイテムを並べ替えることができます。

コントロール ボタン

- ***例外を追加*** - クリックすると新しいダイアログが開き、AVG のスキャンから除外する必要がある項目を指定できます。最初に、アプリケーションやファイル、フォルダ、URL、証明書などのオブジェクトのタイプを定義します。次に、ディスクを探して各オブジェクトのパスを指定するか、または URL を入力します。最後に、選択したオブジェクトを無視する AVG の機能を選択します（*常駐シールド*、*Identity Protection*、*スキャン*）。

- ***編集*** - このボタンは既に例外が定義されていて、表に表示されている場合にのみ有効です。また、このボタンを使うと選択した例外の編集ダイアログが開き、例外のパラメータを設定することができます。

- ***削除*** - このボタンを使うと以前に定義した例外をキャンセルできます。個別に削除することも、

一覧から例外をまとめてハイライトし、定義した例外を一括でキャンセルすることもできます。例外をキャンセルすると、個々のファイルやフォルダ、URL は再度 AVG でスキャンされます。ファイルやフォルダ自体ではなく、例外が削除された場合にのみスキャンされることに注意してください。

- ***すべて削除*** - このボタンは、リストにある定義済みの例外をすべて削除するために使用します。

9.12. 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管理に関するパラメータを定義できます。

- ***ウイルス隔離室のサイズを制限*** - スライダを使用して、ウイルス隔離室の最大サイズを設定できます。サイズは、ローカルディスクのサイズに対する割合で指定されます。
- ***自動ファイル検出*** - 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時間 (***..日以降経過したファイルを削除***) 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。

9.13. AVG 自己保護

AVG 自己保護 は、**AVG Internet Security 2015** がそれ自身のプロセス、ファイル、レジストリキーおよびドライバを改ざんされたり無効化されることから保護することができます。この種の保護をする主な理由としては、一部の巧妙な脅威がウイルス対策保護の解除を試みた後、コンピュータに無制限に被害をもたらすことが挙げられます。

この機能を有効にしておくことをお勧めします。

9.14. プライバシー設定

[***プライバシー プリファレンス***] ダイアログは、AVG 製品改善に参加し、全体的なインターネット セキュリティレベルの向上を支援するものです。お客様による報告は、世界中のすべての参加者から最新の脅威に関する情報を収集し、全ユーザーに対する保護を向上させるために役立てられます。報告は自動的に行われるため、お客様にご不便をおかけすることはありません。また、報告に個人情報は一切含まれません。検出した脅威の報告は任意ですが、このオプションを有効にしておくようにお願いしております。これにより、すべての AVG ユーザーの保護機能が強化されます。

ダイアログでは、次の設定オプションが使用できます。

- ***AVG 製品改善プログラムに参加して AVG による製品の改善に協力する*** *(既定ではオン)*: **AVG Internet Security 2015** のさらなる機能改善にご協力いただける場合は、チェックボックスをオンにしてください。これにより、検出された脅威はすべて AVG に報告されます。AVG では世界中の参加者全員からマルウェアに関する最新情報を収集することで、メンバー全員の保護レベルを向上させることができます。報告は自動的に行われるため、お客様にご不便をおかけすることはありません。また、報告に個人情報は一切含まれません。
  - ***誤検出されたメールに関するユーザー確認データの送信を許可する*** *(既定ではオン)*: スパム対策サービスの誤検出によってスパムとして認識されたメールメッセージ、あるいは検出されなかったスパムメッセージに関する情報を送信します。この種類の情報の送信時には、確認ダイアログが表示されます。
  - ***特定された脅威または不審な脅威に関する匿名データの送信を許可する*** *(既定ではオン)*: コンピュータで検出された不審あるいは明らかに危険なコードや動作パターン *(ウイルス、スパイウェア、アクセスしようとしている悪意のある Web ページ)* に関する情報を送信します。
  - ***製品の使用状況に関する匿名データの送信を許可する*** *(既定ではオン)*: 検出数、実行されたスキャン、成功/失敗した更新など、アプリケーションの使用状況に関する基本統計情報を送信します。
- ***クラウド検出検証を許可する*** *(デフォルトではオン)*: 検出された脅威が本当に感染しているのか、誤検出であるのかを確認します。
- ***AVG パーソナライズをオンにしてユーザーの AVG 使用体験をパーソナライズします*** *(デフォルトではオフ)* - この機能はお使いのPCにインストールされたプログラムやアプリケーションの動作を匿名で分析します。この分析に基づいて、AVG はユーザーのニーズに直接応えるサー

ビスを提供し、最大限の安全性を維持することができます。

9.15. エラー状態を無視

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

既定では一覧で選択されているコンポーネントはありません。つまり、すべてのコンポーネントは、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 4 色で表示されますが、エラーが発生すると、黄色のエクスクラメーション マークのついたアイコンが表示され、
- AVG メイン ウィンドウの [セキュリティ ステータス情報] セクションに既存の問題に関する説明が表示されます。

何らかの理由のため、ある状況で一時的にコンポーネントをオフにする必要があるかもしれません。***すべてのコンポーネントを永続的にオンにし続け、既定の設定を保持することが望ましいため、この操作は推奨されません。*** しかし、このような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、ユーザーが自分で慎重に設定を行い、潜在的なリスクを認識しているため、実際のエラーについては説明できません。同時に、グレイ色で表示されると、アイコンは表示される可能性のある他のエラーを実際に報告できません。

この場合、***エラー状態を無視*** ダイアログでエラー状態となる可能性のある *(あるいはオフになる)* コンポーネントを選択できますが、その状態は通知されません。[***OK***] ボタンをクリックして、すべての変更を確認します。

9.16. Advisor - 既知のネットワーク

AVG Advisor には、接続中のネットワークを監視する機能が含まれています。新しいネットワークが見つかった場合 *(すでにネットワーク名が使用済みの場合は混乱を招く可能性があります)* に通知して、ネットワークの安全性を確認するよう推奨します。新しいネットワークへの接続が安全であると判断した場合、安全なネットワークリストにも保存することができます。*(不明なネットワークが検出されると、AVG Advisor トレイ通知がシステム トレイからスライド表示され、そこにリンクが表示されます。詳細については AVG Advisor の章を参照してください)*。AVG Advisor はネットワークの一意的な属性 *(具体的には MAC アドレス)* を記憶し、次回は通知を表示しません。接続中の各ネットワークは自動的に既知のネットワークと認識され、リストに追加されます。[***削除***] ボタンを押すことで、各エントリを削除できます。個々のネットワークは、再度不明で危険の可能性があると見なされます。

このダイアログ ウィンドウでは、既知と考えられるネットワークを確認できます。

注意 :*AVG Advisor の既知のネットワーク機能は Windows XP 64 ビット版ではサポートされていません。*

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。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編集することができます。設定は基本モードまたはエキスパートモードで実行できます。設定ウィンドウを初めて開く場合は基本バージョンで表示され、次のパラメータを編集できます。

- 全般
- アプリケーション
- ファイルとプリンタの共有

ダイアログ下部には、[***エキスパートモード***] ボタンが表示されます。ボタンをクリックすると、非常に高度なファイアウォール設定の詳細項目がダイアログのナビゲーションに表示されます。

- 高度な設定
- 定義済みネットワーク
- システムサービス
- ログ

10.1. 全般

一般的な情報 ダイアログには、利用可能なすべてのファイアウォールモードの概要が表示されます。現在選択されているファイアウォールモードは、メニューから別のモードを選択するだけで変更できます。

ただし、製造元はすべての AVG Internet Security 2015 コンポーネントを最適なパフォーマンスを実現できるように設定しています。特に理由がない場合は、既定の設定を変更しないでください。設定変更は経験のあるユーザーのみが行うことを推奨します。

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、ノートパソコンかによって、特定のセキュリティルールを定義することができます。各コンピュータタイプによって異なるレベルの保護が必要になります。これらのレベルには該当するモードが適用されます。要するに、ファイアウォール モードとはファイアウォール コンポーネントの特別な設定です。ユーザーはこのような予め定義された数々の設定を利用することができます。

- ***自動*** - このモードでは、ファイアウォールはすべてのネットワーク トラフィックを自動的に処理します。どのような決定もユーザーが下すことはありません。ファイアウォールは、既知の各アプリケーションの接続を許可すると同時にアプリケーションのルールを作成して、今後アプリケーションが常に接続できるよう指定します。その他のアプリケーションについては、アプリケーションの動作によってファイアウォールが接続を許可するかブロックするかを決定します。ただし、そのような状況下ではルールは作成されません。またアプリケーションは接続を試みる時に再度チェックされます。***自動モードは安定しているため、ほとんどのユーザーに対して推奨されます。***

- ***対話*** - このモードはコンピュータとやりとりするすべてのネットワーク トラフィックを完全に制御する場合に便利です。ファイアウォールはトラフィックを監視し、データの通信や転送のそれぞれの試みをユーザーに通知します。ユーザーは自分が適切だと判断したとおりに、その試みを許可したりブロックしたりできます。上級ユーザーのみにお勧めします。

- ***インターネットへのアクセスをブロック*** - インターネット接続が完全にブロックされます。インターネットにアクセスできないため、外部からはコンピュータにアクセスできません。特別な場合や短期間の使用の場合に限ります。

- ***ファイアウォール保護を無効にする*** - ファイアウォールを無効にして、コンピュータとやりとりするすべてのネットワーク トラフィックを許可します。これによって、結果的にハッカーによる攻撃を受けやすくなります。このオプションは常によく考えた上で、慎重に設定してください。

特定の自動モードはファイアウォール内でも有効であることに注意してください。コンピュータまたは Identity protection コンポーネントが無効になった場合、このモードは暗黙で有効化されます。そのため、コンピュータはさらに脆弱になります。そのような場合、ファイアウォールは既知の絶対に安全なアプリケーションのみを自動的に許可します。その他の場合はすべてユーザーが決定を行います。これは無効

化された保護コンポーネントを補完するためであり、コンピュータを安全に保つための対策です。

10.2. アプリケーション

アプリケーションダイアログでは、過去にネットワーク上で通信を試みたすべてのアプリケーションのリストと、それらに割り当てられたアクションのアイコンが表示されます。

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

- - すべてのネットワークの通信を許可
- - 通信をブロック
- - 定義された高度な設定

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

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

アプリケーション以外にも、リストには2つの特別な項目が表示されます。***優先アプリケーションルール***(*リストの上部*)は、常に他の個々のアプリケーションルールよりも優先して適用されます。***他のアプリケーションルール***(*リストの下部*)は、不明で未定義のアプリケーションのように特定のアプリケーションルールが適用されない場合、「最終インスタンス」として使用されます。このよう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に実行されるアクションを選択します。ブロック(*通信は常にブロックされま*

*す」許可 (通信はすべてのネットワークで許可されます」確認 (通信を許可するかブロックするかを決定するため、確認が表示されます」**これらの項目には一般のアプリケーションとは異なった設定オプションがあり、上級者ユーザー向けの設定です。設定を修正しないことを強くお勧めします。***

コントロール ボタン

以下のコントロール ボタンを使用してリストを編集することができます。

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

10.3. ファイルとプリンタの共有

ファイルとプリンタの共有とは、実際には Windows で 共有」としてマークしたファイルまたはフォルダ、共通のディスク ユニット、プリンタ、スキャナ、および同様のあらゆるデバイスを共有するということです。このようなアイテムは、安全と考えられるネットワーク*(家庭、職場、学校など)*内でのみ共有することが望ましいです。ただし、公開ネットワーク*(空港の Wi-Fi やインターネット カフェなど)*に接続している場合は、おそらく一切の共有を望まないでしょう。AVG ファイアウォールは共有を簡単にブロックまたは許可できます。また、既にアクセスしたネットワークに対してその選択を保存することができます。

ファイルとプリンタの共有 ダイアログでは、ファイルとプリンタの共有の設定と、現在接続されているネットワークを編集できます。Window XP の場合、ネットワーク名は、最初に接続した時に特定のネットワークに付けた名称に対応しています。Window Vista 以降の場合、ネットワーク名は、[ネットワークと共有センター] で自動的に付けられます。

10.4. 高度な設定

高度な設定 ダイアログの編集は、経験のあるユーザーのみを対象としています。

高度な設定 ダイアログでは、次のファイアウォール パラメータの選択または選択解除ができます。

- ***ファイアウォールでサポートしている仮想マシンへのトラフィック、または仮想マシンからのトラフィックをすべて許可*** - VMWare などの仮想マシンでのネットワーク接続をサポートします。
- ***仮想プライベート ネットワーク (VPN) へのトラフィックをすべて許可*** - VPN 接続をサポートします *(リモート コンピュータへの接続に使用)*。
- ***不明な送受信トラフィックを記録*** - 不明なアプリケーションによる接続の試行 *(送受信)*をすべてファイアウォール ログに記録します。
- ***すべてのアプリケーションルールのルール検証を無効にする*** - 各アプリケーションルールが適用されるすべてのファイルをファイアウォールが継続的に監視します。バイナリファイルの変更があると、証明書を確認したり、信頼されたアプリケーションのデータベースを参照するといった標準的な方法で、ファイアウォールがアプリケーションの信頼性をもう一度確認しようとします。アプリケーションが安全であると確認できない場合、ファイアウォールは選択されたモードに基づいて、アプリケーションに対処します。
    - ファイアウォールが***自動モード***で動作している場合、デフォルトとしてアプリケーションは許可されます。
    - ファイアウォールが ***インタラクティブ モード***で動作している場合、アプリケーションはブロックされ、アプリケーションをどう処理するべきかユーザーに判断を求める質問ダイアログが表示されます。

特定のアプリケーションに対処する望ましい方法について、アプリケーション ダイアログ内で各アプ

リケーションに個別に定義できます。

10.5. 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内の編集は、経験のあるユーザー向けです。

定義済みネットワークダイアログはコンピュータが接続するすべてのネットワークのリストを提供します。このリストには検出されたすべてのネットワークに関する次の情報が表示されます。

- ***ネットワーク***- コンピュータが接続されているすべてのネットワーク名の一覧が表示されます。
- ***IP アドレス範囲*** - 各ネットワークは自動的に検出され、IP アドレス範囲の形式で指定されます。

コントロール ボタン

- ***ネットワークの追加*** - 新しいダイアログ ウィンドウを開きます。ここでは、***ネットワーク名***の入力や ***IP アドレス範囲***の指定など、新しく定義されたネットワークのパラメータを編集することができます。

- ***ネットワークの編集*** - ***ネットワークプロパティ***ダイアログ ウィンドウ (*上記を参照*) を開きます。ここでは、既に定義されたネットワークのパラメータを編集できます (*ダイアログは新しいネットワークの追加ダイアログと同一です。前のパラグラフを参照してください。*)。

- ***ネットワークの削除*** - ネットワークのリストから選択したネットワークへの参照を削除します。

10.6. システム サービス

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

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

- ***システム サービスとプロトコル*** - この列には、各システム サービス名が表示されます。

- ***アクション*** - この列には、割り当てられたアクションのアイコンが表示されます。
    - o すべてのネットワークの通信を許可
    - o 通信をブロック

リストのアイテム（割り当てられたアクションを含む）の設定を編集するには、アイテムを右クリックして、[***編集***] を選択します。***システム ルールの編集は上級者ユーザーによってのみ実施されることが望ましいですが、一般にはシステム ルールを編集しないことを強くお勧めします。***

ユーザ定義システムルール

独自のシステム サービス ルール（*次の図を参照*）を定義するために新しいダイアログを開くには、[***ユーザー システム ルールの管理***] ボタンをクリックします。システム サービスおよびプロトコルのリスト内に表示されているいずれかの項目について設定の編集を行う場合、同じダイアログが開きます。ダイアログ上部のセクションには、現在編集されたシステム ルールの詳細すべての概要が表示され、下部のセクションには選択した詳細が表示されます。ルール詳細では、各ボタンを使用して編集、追加、削除ができます。

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

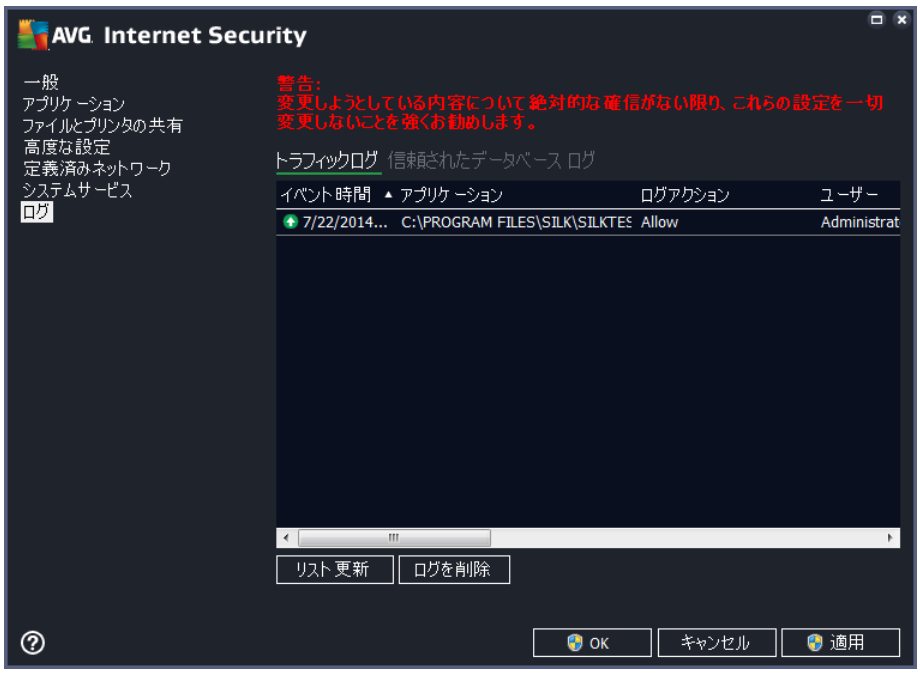
10.7. ログ

ログ ダイアログ内の編集は、すべて経験のあるユーザーのみを対象としています。

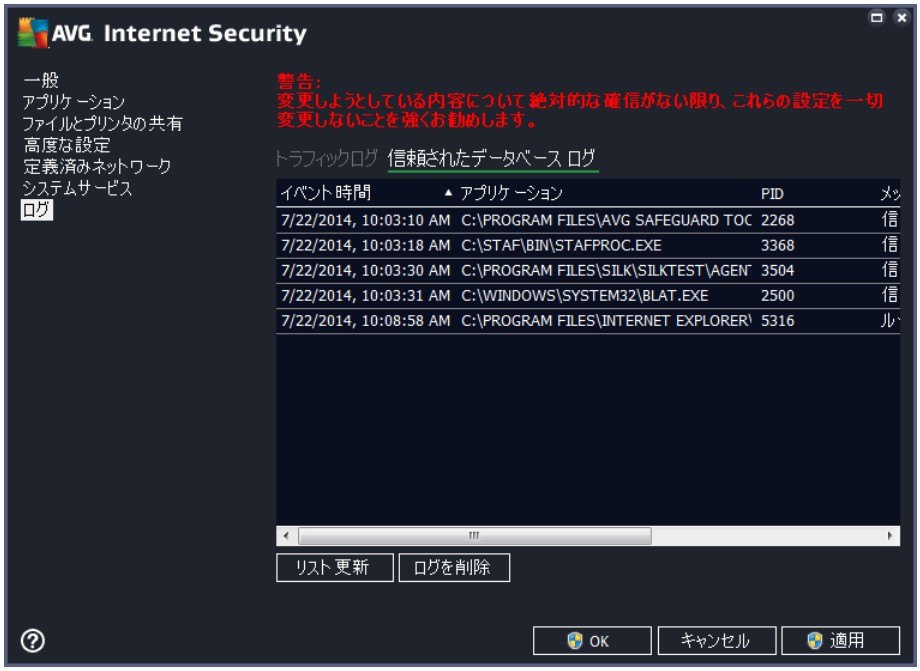
ログ ダイアログでは、すべてのログに記録されたファイアウォール アクションとイベントのリストを確認することができます。2つのタブには関連するパラメータの詳細な説明が付属しています。

- ***トラフィック ログ*** - このタブでは、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

に関する情報を表示します。各項目では、イベント時刻、アプリケーション名、各ログ アクション、ユーザー名、PID、トラフィック方向、プロトコル タイプ、リモートおよびローカル ポート番号、リモートおよびローカル IP アドレスの情報などを見ることができます。



- ***信頼されたデータベース ログ*** - *信頼されたデータベース*とは、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

- ***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。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。

- ***ログを削除*** - 表のすべてのエントリを削除します。

11. AVG スキャン

既定では、**AVG Internet Security 2015** はスキャンを実行しません。初回のスキャンの後 *(実行するよう指示されます)*、常に監視状態にある **AVG Internet Security 2015** の常駐コンポーネントによって完全に保護され、悪意のあるコードはコンピュータに侵入できないためです。当然、定期的にスキャンを実行するようにスケジュール設定したり、ニーズに合わせていつでもスキャンを手動で起動したりできます。

AVG スキャン インターフェースはメイン ユーザーインターフェースから2 つのセクションに分かれたボタンを使ってアクセスできます。 

- ***今すぐスキャン*** - ボタンをクリックすると、全コンピュータをスキャンをただちに起動し、自動的にレポート ウィンドウが開いて進行状況と結果を見ることができます。

- ***オプション*** - このボタン *(緑色の背景に水平の線が 3本表示されている)* を選択すると、[***スキャン オプション***] ダイアログが開き、スケジュール済みのスキャンを管理したり、全コンピュータをスキャン / 特定のファイルとフォルダのスキャンのパラメータを編集したりできます。

スキャン オプション ダイアログには、3つのメイン スキャン設定 セクションが表示 されます。

- ***スケジュール スキャンを管理*** - このオプションををクリックすると、新 しいダイアログが開き、すべてのスキャン スケジュールの概要 が表示 されます。スキャンを個別 に定義 する前 に、一覧 に表示 された、ソフトウェア ベンダーが事前 に定義 したスケジュール スキャンを参照 できます。スキャンはデフォルトでは無効 になっています。有効 にするには、スキャンを右 クリックしてコンテキスト メニューから [*タスクの有効化*] オプションを選択 します。スケジュールされたスキャンが有効化 されると、[*スケジュール編集*] ボタンを使 って設定 を編集 することができます。[*スケジュール追加*] ボタンをクリックすると、新 しい独自 のスキャン スケジュールを作成 することもできます。

- ***全 コンピュータをスキャン 設定*** - このボタンは 2つのセクションに分 かれて表示 されます。[*全 コンピュータをスキャン*] オプションをクリックすると、ただちにコンピュータ全 体 をスキャンを開始 します (*コンピュータ全 体 をスキャンの詳細 については、事前 に定義 されたスキャン /全 コンピュータをスキャンの各 章 を参照 してください*)。[*設定*] セクションをクリックすると、全 コンピュータをスキャンの設定 ダイアログに移動 します。

- ***特定 のファイルとフォルダ /設定*** - ボタンは 2つのセクションに分 かれています。[*特定 のファイルとフォルダ*] オプションをクリックすると、コンピュータの選択 した範囲 のスキャンをただちに開始 します (*選択 したファイルとフォルダのスキャンに関 する詳細 は、事前 に定義 されたスキャン /特定 のファイルとフォルダの各 章 を参照 してください*)。[*設定*] セクションをクリックすると、特定 のファイルとフォルダの設定 ダイアログに移動 します。

- ***コンピュータ内 のルートキット /設定 をスキャン*** - *ルートキットについてコンピュータをスキャンとラベルされたボタンの左 側 セクションですぐにルートキット対策 スキャンを開始 し、(ルートキットのスキャンに関 する詳細 は、あらかじめ定義 されたスキャン /コンピュータ内 のルートキットをスキャンの章 をご参照 ください*)。*設定* セクションがクリックされるとルートキットスキャンの設定 ダイアログに移動 します。

11.1. 定義済みスキャン

AVG Internet Security 2015 の主 要 な機能 の 1つは、オンデマンド スキャンです。オンデマンドのスキャンは、ウイルス感染 の疑 いがある場合 、コンピュータのさまざまな箇所 をいつでもスキャンできるように設計 されています。いずれにせよ、このような検査 を、たとえウイルスがコンピュータにないと思 われる場合 でも、定期的 に実行 することを強 く推奨 します。

AVG Internet Security 2015 には、ソフトウェア ベンダーがあらかじめ定義 した次 の種類 のスキャンがあります。

11.1.1. 全コンピュータをスキャン

全 コンピュータをスキャンは、コンピュータ全 体 をスキャンして、感染 と不審 なプログラムがあるかどうかを確認 します。 このスキャンはコンピュータのすべてのハード ドライブをスキャンし、ウイルス感染 を検出 して修復 するか、検出 した感染 をウイルス隔離室 に移動 します。コンピュータ全 体 のスキャンは、最低 でも週 に 1度 は実行 されるようスケジュールすることが推奨 されます。

スキャン実行

全 コンピュータをスキャンは、[今 すぐスキャン] ボタンをクリックして、***メイン ユーザーインターフェース***から直接 起動 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。スキャンはただちに開始 されます。***全 コンピュータをスキャンの進行 状況*** ダイアログ (*スクリーンショットを参照*) に

は、進行状況と結果が表示されます。必要に応じて、スキャンを一時的に中断 (***一時停止***)、またはキャンセル (***停止***) することができます。

スキャン設定編集

[***全コンピュータをスキャン -般定***]ダイアログで、***全コンピュータをスキャン***の設定を編集できます *(ダイアログには、[スキャン オプション] ダイアログ内の [全コンピュータをスキャン] の [設定] リンクを使ってアクセスできます)* ***。一般的には、既定の設定を保持し、合理的な理由がある場合にのみ変更することを推奨します。***

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。

- ***感染を修復/除去する際に確認メッセージを表示しない*** *(既定ではオン)* スキャン実行中にウイルスが特定された際、修復可能な場合は自動で修復されます。感染したファイルを自動的に修復できない場合、感染したオブジェクトはウイルス隔離室に移動されます。

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

- ***不審なプログラムの拡張セットを報告する*** *(既定ではオフ)* チェックを付けると、スパイウェアの拡張パッケージを検出します。スパイウェアとは、直接製造元から入手する場合には完全に問題がなく無害なプログラムですが、後から悪意のある目的で誤用されるおそれのあるプログラムです。これは、コンピュータセキュリティをさらに高めるための追加的な手段ですが、合法的なプログラムもブロックする可能性があるため、既定ではオフになっています。

- ***Tracking Cookie をスキャンする*** *(既定ではオフ)* - このパラメータは、cookie を検出するか否かを指定します *(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トの内容など、ユーザーに関する特定の情報の認証、追跡、維持に使用されます)*。

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

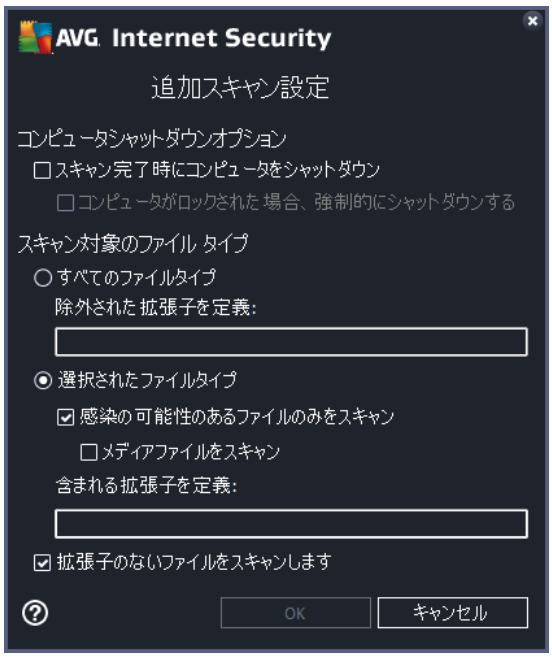
- ***ヒューリスティック分析を使用する*** *(既定ではオン)* ヒューリスティック分析 *(仮想コンピュータ環境で実行されるスキャン対象オブジェクト命令の動的エミュレーション)*は、スキャン実行中にウイルス検出に使用される方法の 1つです。

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

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

- ***ルートキットのスキャン*** *(デフォルトではオン)* 全コンピュータのスキャンにルートキット対策スキャンが含まれます。ルートキット対策スキャンは別に開始されます。

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

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

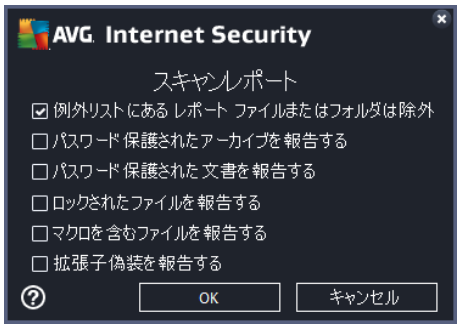
  - ***すべてのファイル タイプ*** - このオプションを使用すると、スキャンが不要なファイルの拡張子をカンマで区切ったリストを指定することによって、スキャンの例外を定義できます。

  - ***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スキャンするよう指定できます (*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 - 多くの場合、これらのファイルは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は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であるため、常にスキャンすることをお勧めします。

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

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



警告 :*これらのスキャン設定は、新規に定義するスキャンの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。****全コンピュータをスキャン****の既定の設定を変更する場合は、新しい設定を既定の設定として保存し、以降のすべての全コンピュータをスキャンに使用できます。*

11.1.2. 特定のファイルとフォルダをスキャン

特定ファイルとフォルダをスキャン - 選択した領域のみスキャンします *(選択したフォルダ、ハードディスク、フロッピーディスク、CD など)*。ウイルスが検出され、処置される場合のスキャンの進行状況は、全コンピュータのスキャンを実行している時と同じです。検出されたウイルスは修復されるか、ウイルス隔離室に移されます。特定のファイルとフォルダでは、ユーザー独自のスキャン設定とスケジュールを実行できます。

スキャン実行

特定のファイルとフォルダは、[スキャンオプション] ダイアログから[**特定のファイルとフォルダ**] ボタンをクリックすることで直接起動できます。[***スキャンする特定のファイルとフォルダを選択***] 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するフォルダを選択します。選択したフォルダへのそれぞれのパスが自動的に作成され、このダイアログの上部のテキストボックスに表示されます。また、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***] ボタンをクリックします。スキャン処理自体は基本的に全コンピュータをスキャンと同じです。

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設定を***特定のファイルとフォルダをスキャン -設定***ダイアログで調整できます　ダイアログは、*スキャン オプション*ダイアログ内の特定のファイルとフォルダをスキャンの設定リンクからアクセスできます*）* ***一般的には、デフォルト設定を保持し、合理的な理由がある場合にのみ変更することを推奨します。***

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。

- ***感染を修復/除去する際に確認メッセージを表示しない****(既定ではオン)*スキャン実行中にウイルスが特定された際、修復可能な場合は自動で修復されます。感染したファイルを自動的に修復できない場合、感染したオブジェクトはウイルス隔離室に移動されます。

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

- ***不審なプログラムの拡張セットを報告する*** *(既定ではオフ)*: チェックを付けると、スパイウェアの拡張パッケージを検出します。スパイウェアとは、直接製造元から入手する場合には完全に問題がなく無害なプログラムですが、後から悪意のある目的で誤用されるおそれのあるプログラムです。これは、コンピュータセキュリティをさらに高めるための追加的な手段ですが、合法的なプログラムもブロックする可能性があるため、既定ではオフになっています。

- ***Tracking Cookie をスキャンする*** *(既定ではオフ)*: このパラメータは、cookie を検出するか否かを指定します *(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トの内容など、ユーザーに関する特定の情報の認証、追跡、維持に使用されます)*。

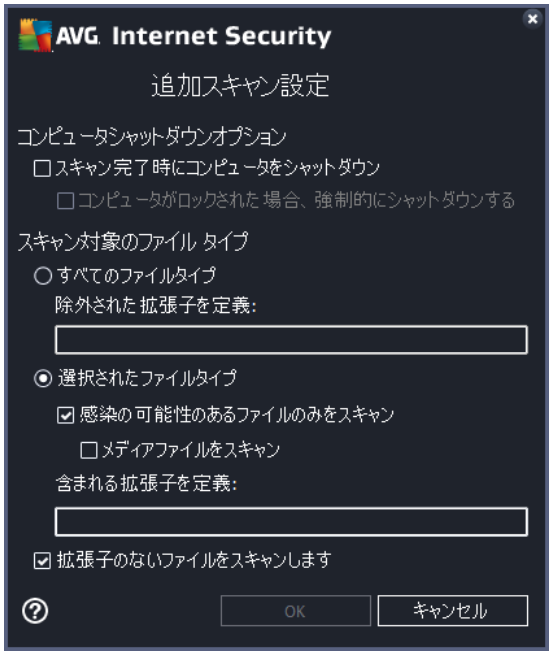
- ***アーカイブの内容をスキャン*** *(既定ではオン)*: ZIP や RAR などのアーカイブ内に格納されているすべてのファイルをスキャンします。

- ***ヒューリスティック分析を使用する*** *(既定ではオン)*: ヒューリスティック分析 *(仮想コンピュータ環境で実行されるスキャン対象オブジェクト命令の動的エミュレーション)* は、スキャン実行中に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する*** *(既定ではオフ)*: コンピュータのシステム領域もチェックされます。

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

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



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

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

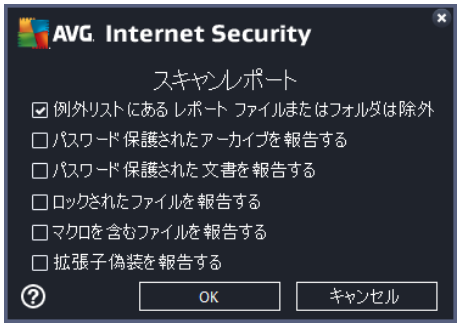
  - ***すべてのファイル タイプ*** このオプションを使用すると、スキャンが不要なファイルの拡張子をカンマで区切ったリストを指定することによって、スキャンの例外を定義できます。

  - ***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スキャンするよう指定できます (*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は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であるため、常にスキャンすることをお勧めします。

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

- ***追加スキャンレポートを設定*** - このリンクは、***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、新規に定義するスキャンの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。****特定のファイルとフォルダ****の既定の設定を変更する場合、新しい設定を既定の設定として保存し、すべての特定のファイルとフォルダに適用できます。また、この設定はすべての新規スキャン スケジュールのテンプレートとして使用できます (すべてのカスタマイズ スキャンは、選択したファイルやフォルダのスキャンの現在の設定に基づいて実行されます)。*

11.1.3. コンピュータ内をルートキットスキャン

コンピュータ内 のルートキット スキャンは、コンピュータ上 の悪 意 のあるソフトウェアの存 在 を隠 すプログラムや技 術 等 の危 険 なルートキットを検 出 し、効 果 的 に除 去 する特 別 なツールです。ルートキットは、システムの所 有 者 や正 式 な管 理 者 の許 可 なくコンピュータ システムの基 本 的 なコントロールを実 行 するように設 計 されたプログラムです。スキャンすることで、あらかじめ定 義 されたルールに基 づいて、ルートキットを検 出 できます。ルートキットが検 出 されても、必 ずしも感 染 しているというわけではありません。時 々 、ルートキットはドライバとして使 用 されたり、正 しいアプリケーションの一 部 の場 合 もあります。

スキャン実 行

コンピュータ内 のルートキットスキャンは、***コンピュータ内 をルートキットスキャン***ボタンをクリックすることで、スキャン オプションダイアログから直 接 開 始 できます。***ルートキット対 策 スキャンの進 行 中***の新 しいダイアログが開 き、開 始 したスキャンの進 行 状 況 が表 示 されます。

スキャン設 定 編 集

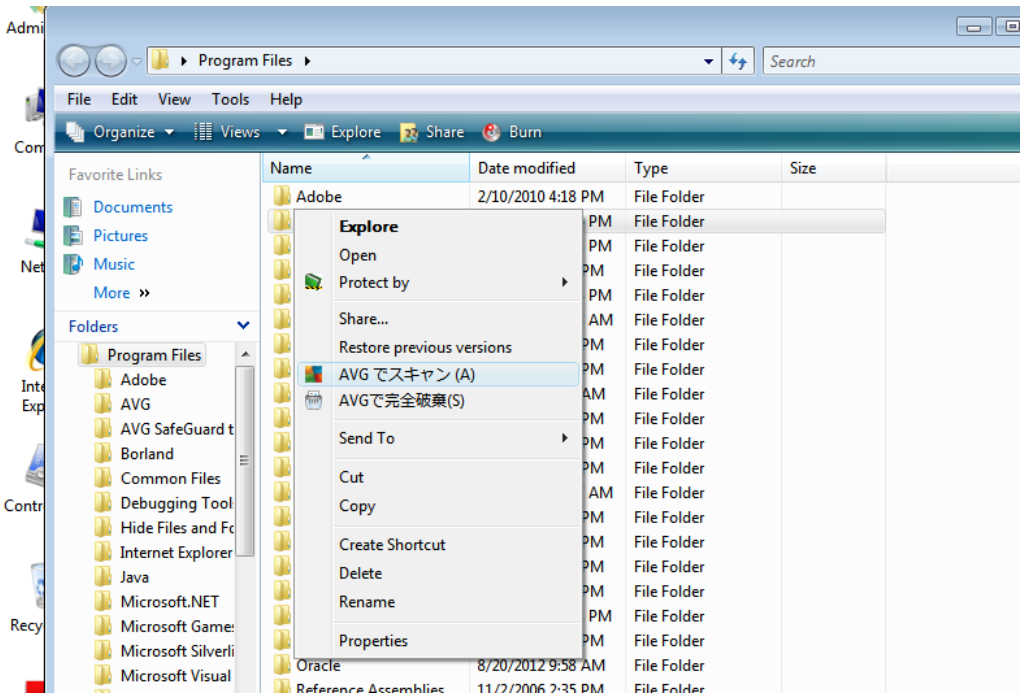
ルートキット対 策 の設 定ダイアログでルートキット対 策 スキャンの設 定 を編 集 できます(*ダイアログへは、スキャン オプションダイアログで、ルートキットスキャンのためにコンピュータをスキャンの設 定 リンクを使 ってアクセスできます*)。***一 般 的 には、既 定 の設 定 を保 持 し、合 理 的 な理 由 がある場 合 にのみ変 更 することを推 奨 します。***

アプリケーション スキャンと***ドライバ スキャン***では、ルートキット対策スキャンの対象を詳細に指定することができます。これらの設定は上級者ユーザー向けです。すべてのオプションをオンにしておくことをお勧めします。また、ルートキット スキャン モードを選択することもできます。

- ***クイック ルートキット スキャン*** - 実行中のすべてのプロセス、ロードされているすべてのドライバのほか、システム フォルダ (*通常は c:\Windows*) もスキャンします
- ***フル ルートキット スキャン*** - 実行中のすべてのプロセス、ロードされているすべてのドライバ、およびシステム フォルダ (*通常は c:\Windows*) に加えて、すべてのローカル ディスク (*フラッシュ ディスクは含むが、フロッピー ディスク/CD ドライブは含まない*) をスキャンします

11.2. シェル拡張スキャン

AVG Internet Security 2015 では、全コンピュータをスキャンあるいは特定領域のスキャンで実行されるあらかじめ定義されたスキャン以外にも、クイック スキャン オプションを使用して、Windows Explorer 環境で特定オブジェクトのスキャンを直接実行できます。内容が不明なファイルを開く場合、そのファイルのみをチェックできます。次の方法で実行します。



- Windows Explorer で、チェックするファイル *あるいはフォルダ*) を選択します。
- マウスをオブジェクトに移動して右クリックし、コンテキスト メニューを開きます。
- [***でスキャン***] オプションを選択して、ファイルを AVG でスキャンします**AVG Internet Security 2015**

11.3. コマンドライン スキャン

AVG Internet Security 2015 ではコマンド ラインからスキャンを実行するときにオプションを利用できます。このオプションはサーバー上のインスタンスに対して利用できます。あるいは、コンピュータのブート後に自動的に起動するバッチ スクリプトを作成するときに利用できます。コマンド ラインからスキャンを起動するときには、AVG のグラフィカル ユーザー インターフェースで提供されるほとんどのパラメータを使用できます。

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

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

コマンドの構文

コマンドの構文は次のとおりです。

- ***avgscanx /パラメータ***... たとえば、完全コンピュータ スキャンの場合 ***avgscanx /comp***
- ***avgscanx /パラメータ /パラメータ***.. 複数のパラメータを使用する場合、これらのパラメータをス

ペースとスラッシュで区切り、1行に並べる必要があります。

- パラメータが特定の値を必要とする場合（例：***/scan*** パラメータにはスキャンの対象として選択したコンピュータの場所の情報が必要であり、選択した場所への正確なパスを指定する必要があります）は、値をセミコロンで区切る必要があります。例：***avgscanx /scan=C:\;D:***

スキャン パラメータ

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

スキャンを実行するには、[***Enter***] を押します。スキャン中は、***Ctrl+C*** または ***Ctrl+Pause*** を押して、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する CMD スキャン

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

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

11.3.1. 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の一覧です。

- /SCAN　特定のファイルとフォルダ /SCAN=path;path *(例：/SCAN=C:\;D:\)*
- /COMP　全コンピュータをスキャン
- /HEUR　ヒューリスティック分析を使用
- /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 *(ファイル名 /)*
- /EXT　指定した拡張子のファイルをスキャン *(例：EXT=EXE,DLL/)*
- /NOEXT　これらの拡張子をスキャンしない *(例：NOEXT=JPG/)*
- /ARC　アーカイブをスキャン
- /CLEAN　自動的に駆除
- /TRASH　感染ファイルをウイルス隔離室
- /QT　クイック スキャン

- /LOG　スキャン結果ファイルを生成
- /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
- /ARCBOMBSW　アーカイブボムを報告する*(何度も圧縮されたアーカイブ)*
- /IGNLOCKED　ロックされたファイルを無視
- /REPORT　ファイルにレポート *(ファイル名)*
- /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 キーでの中断を許可しない
- /BOOT　MBR/ブートチェックを有効化
- /PROC　アクティブなプロセスをスキャン
- /PUP　不審なプログラムを報告する
- /PUPEXT　不審なプログラムの拡張設定を報告する
- /REG　レジストリをスキャン
- /COO　cookie をスキャン
- /?　このトピックに関するヘルプを表示
- /HELP　このトピックに関するヘルプを表示
- /PRIORITY　スキャン優先度 (低、自動、高)を設定 (*高度な設定 /スキャンを参照*)
- /SHUTDOWN　スキャン完了時にコンピュータをシャットダウン
- /FORCESHUTDOWN　スキャン完了時にコンピュータを強制シャットダウン
- /ADS　Alternate Data Stream をスキャン *(NTFS のみ)*
- /HIDDEN　拡張子を偽装したファイルを報告する
- /INFECTABLEONLY　感染の可能性がある拡張子を持つファイルのみをスキャン
- /THOROUGHSCAN　完全スキャンを有効にする
- /CLOUDCHECK　誤検出を確認
- /ARCBOMBSW　再圧縮されたアーカイブファイルを報告

11.4. スキャン スケジュール

AVG Internet Security 2015では、オンデマンドで *(コンピュータにウイルスが侵入した疑いがある場合など)*またはスケジュールに基づいてスキャンを実行できます。スケジュールに基づいてスキャンを実行することを強く推奨します。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。全コンピュータスキャンを週に 1度以上定期的に実行することをお勧めします。ただし、可能な場合は、コンピュータのスキャンを毎日実行してください。既定のスキャン スケジュールはこのように設定されています。コンピュータが常にオンとなっている場合、作業時間外にスキャンを実行するよう設定することができます。コンピュータがオフになっていたためスケジュールが実行されなかった場合に備えて、コンピュータの起動時にスキャンを実行するようにスケジュールを設定します。

スケジュール スキャンダイアログは、[スキャン オプション] ダイアログの[***スケジュール スキャンの管理***]ボタンからアクセスできます。ここではスキャンのスケジュールを作成または編集できます。新しい***スケジュール スキャン***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完全な概要が表示されます。

ダイアログ内でユーザー個別のスキャンを指定できます。***スキャン スケジュールを追加***ボタンを使用して、新しい独自のスキャン スケジュールを作成することができます。スケジュール スキャン *(または新しいスケジュール設定)* のパラメータは、3つのタブで編集できます。

- スケジュール
- 設定
- 場所

各タブで「信号」ボタンを切り替えるだけで必要に応じてスケジュールされたテストを一時的に有効化/無効化できます。

11.4.1. スケジュール

ダイアログの上部にある [***スケジュール***] タブには、現在定義されているスキャンのスケジュール名を指定できるテキストフィールドが表示されます。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。たとえば、「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示していないためです。一方で適切な名前の例としては、「システムエリアスキャン」などがあります。

このダイアログでは、さらに以下のスキャンパラメータを定義できます。

- ***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。タイミングは、一定の期間の後に繰り返されるスキャン開始を設定（*定期実行 ..*）または正確な日時を設定（*指定した時間に実行*）、あるいはスキャンの開始が関連付けられるイベントを設定（*コンピュータ起動時に実行*）する方法により定義できます。

- ***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できます。スケジュールスキャンが指定した時間に起動すると、AVG システムトレイアイコン上に開かれるポップアップウィンドウで通知されます。次に、スケジュールスキャンが実行中であることを通知する新しい AVG システムトレイアイコン (フルカラーで点滅表示)が表示されます。AVG アイコンを右クリックすると、コンテキストメニューが開き、実行中のスキャンを一時停止または停止することができます。また、現在実行中のスキャンの優先度も変更できます。

ダイアログ内の制御

- ***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、スケジュールスキャン概要に戻ります。したがって、すべてのタブで検査パラメータを設定したい場合は、すべての必要項目を指定した後で、このボタンを押し、保存して下さい。

- ← - ダイアログ左上のセクションにある緑色の矢印を使用すると、スケジュールスキャン概要に戻ります。

11.4.2. 設定

ダイアログの上部にある [***設定***] タブには、現在定義されているスキャンのスケジュール名を指定できるテキスト フィールドが表示されます。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。たとえば、「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示していないためです。一方で適切な名前の例としては、「システム エリア スキャン」などがあります。

[***設定***] タブには、任意でオン/オフ可能なスキャン パラメータのリストが表示されます。***この設定を変更する合理的な理由がない場合は、あらかじめ定義された設定を維持することを推奨します***。

- ***感染を修復/除去する際に確認メッセージを表示しない*** *(既定ではオン)*:スキャン実行中にウイルスが特定された際、修復可能な場合は自動で修復されます。感染したファイルを自動的に修復できない場合、感染したオブジェクトはウイルス隔離室に移動されます。
- ***不審なプログラムとスパイウェア脅威を報告する*** *(デフォルトではオン)*:チェックを付けると、スキャンを有効にし、ウイルスと同時にスパイウェアもスキャンします。スパイウェアは疑わしいマルウェアのカテゴリに含まれます。通常は、セキュリティ リスクとなる場合でも、このようなプログラムを故意にインストールすることができます。コンピュータのセキュリティを高めるため、この機能を有効にしておくことをお勧めします。
- ***不審なプログラムの拡張セットを報告する*** *(既定ではオフ)*: チェックを付けると、スパイウェアの拡張パッケージを検出します。スパイウェアとは、直接製造元から入手する場合には完全に問題がなく無害なプログラムですが、後から悪意のある目的で誤用されるおそれのあるプログラムです。これは、コンピュータ セキュリティをさらに高めるための追加的な手段ですが、合法的なプログラムもブロックする可能性があるため、既定ではオフになっています。
- ***Tracking Cookies のスキャン*** *(デフォルトではオフ)*: このパラメータを指定すると、スキャン実行中に Cookie を検出します *(HTTP cookie は、サイトの設定や電子ショッピング カートの内容など、ユーザー固有の情報の認証、追跡、メンテナンスに使用されます)*。
- ***アーカイブの内容をスキャンする*** *(既定ではオフ)*: このパラメータを指定すると、ファイルが ZIP や RAR などのアーカイブで保存されている場合でも、すべてのファイルに対してスキャン チェックを実行します。

- ***ヒューリスティック分析を使用する*** (*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実行されるスキャン対象オブジェクト命令の動的エミュレーション*) は、スキャン実行中に採用されるウイルス検出方法の一つです。

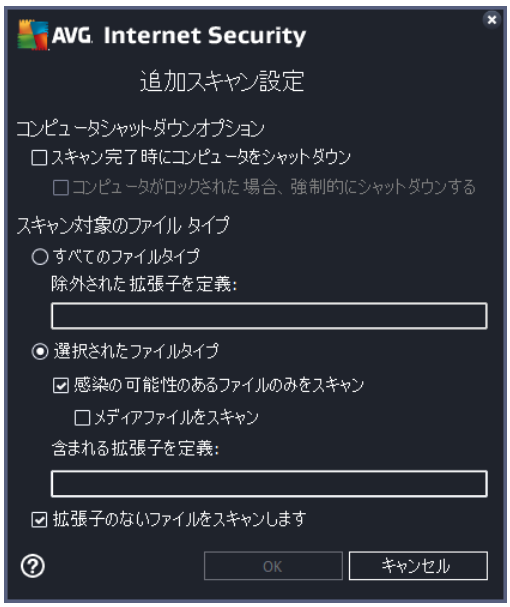
- ***システム環境をスキャンする*** (*既定ではオン*): コンピュータのシステム領域もチェックされます。

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

- ***ルートキットのスキャン*** (*既定ではオン*):ルートキット対策スキャンは、コンピュータ上でマルウェアの活動を隠すことができるプログラムや技術など、可能なルートキットを検索します。ルートキットが検出されても、必ずしもコンピュータが感染しているというわけではありません。通常のアプリケーションの特有のドライバやセクションが誤ってルートキットとして検出される場合もあります。

追加スキャン設定

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



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

- ***スキャンのファイルタイプ*** - 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*** このオプションを使用すると、スキャンが不要なファイルの拡張子をカンマで区切ったリストを指定することによって、スキャンの例外を定義できます。

- ***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スキャンするよう指定できます (*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 が含まれます(*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はスキャン時間がさらに短縮されます*)。ここでも、必ずスキャンする必要があるファイルの拡張子を指定できます。

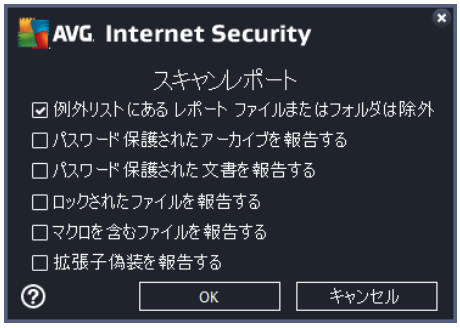
- 任意で***拡張子のないファイルをスキャン***できます。このオプションは既定ではオンになっています。変更する理由がない場合は、この設定を保持することをお勧めします。拡張子のないファイルは不審であるため、常にスキャンすることをお勧めします。

スキャン速度を調整

このセクションでは、さらに、システム リソース使用状況に応じて、希望するスキャン速度を指定することができます。既定ではこのオプションの値は、自動的にリソースを使用する*ユーザー依存*レベルに設定されています。スキャン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量は著しく上がり、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 リソース使用量を減らすことができます。

追加スキャン レポートを設定

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



ダイアログ内の制御

- ***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、スケジュール スキャン概要 に戻ります。したがって、すべてのタブで検査パラメータを設定したい場合は、すべての必要項目を指定した後で、このボタンを押し、保存して下さい。

- - ダイアログ左上のセクションにある緑色の矢印を使用すると、スケジュール スキャン概要に戻ります。

11.4.3. 場所

[***場所***] タブでは、[全コンピュータをスキャン] あるいは [特定のファイルとフォルダ] のどちらでスケジュールするかを定義できます。特定のファイルまとフォルダをスキャンを選択する場合は、このダイアログの下部に表示されるツリー構造がアクティブになり、スキャンするフォルダを選択できます (*スキャンするフォルダが見つかるまでプラス ノードをクリックして項目を展開します*)。各ボックスにチェックを付けると複数のフォルダを選択できます。選択されたフォルダは、ダイアログ上部のテキストフィールドに表示され、ドロップダウンメニューに選択されたスキャン履歴が保持されます。希望するフォルダへのフルパスを手動で入力することもできます (*複数のパスを入力する場合は、スペースを入れずセミコロンで区切る必要があります*)。

ツリー構造内には、[***特別な場所***] という部分もあります。各チェックボックスにマークを付けると、次のようにスキャンする場所の一覧が表示されます。

- ***ローカル ハード ドライブ*** - コンピュータのすべてのハードドライブ
- ***プログラム ファイル***
  - C:\Program Files\
  - *64 ビット バージョン* C:\Program Files (x86)
- ***マイ ドキュメント フォルダ***
  - *Win XP:* C:\Documents and Settings\Default User\My Documents\
  - *Windows Vista/7*: C:\Users\user\Documents\
- ***共有ドキュメント***
  - *Win XP*: C:\Documents and Settings\All Users\Documents\
  - *Windows Vista/7*: C:\Users\Public\Documents\

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

ダイアログ内 の制 御

- ***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、スケジュール スキャン概 要 に戻 ります。したがって、すべてのタブで検 査 パラメータを設 定 したい場 合 は、すべての必 要 項 目 を指 定 した後 で、このボタンを押 し、保 存 して下 さい。
- ← - ダイアログ左 上 のセクションにある緑 色 の矢 印 を使 用 すると、スケジュール スキャン概 要 に戻 ります。

11.5. スキャン結果

スキャン結 果 概 要 ダイアログには、過 去 に実 行 されたすべてのスキャンの結 果 が一 覧 で表 示 されます。この表 には、各 スキャン結 果 に関 する次 の情 報 が表 示 されます。

- ***アイコン*** - 最 初 の列 に、スキャンの状 況 を示 す情 報 アイコンが表 示 されます。
    - 感 染 は検 出 されませんでした、スキャンは完 了 しました

-  感染は検出されませんでした、スキャンは完了前に中断されました
-  感染は修復されました、スキャンは完了しました
-  感染が検出されましたが、修復されませんでした。スキャンは完了前に中断されました
-  感染が検出され、すべて修復または削除されました。スキャンは完了しました
-  感染が検出され、すべて修復または削除されました。スキャンは完了前に中断されました

- ***名前*** - この項目では個々のスキャン名を表示します。2つの事前に定義されたスキャンの 1つか、独自のスケジュール スキャンのいずれかです。
- ***開始時間*** - スキャンが起動された正確な日時を示します。
- ***終了時間*** - スキャンが終了、一時停止、中断した正確な日時を示します。
- ***検査されたオブジェクト*** - スキャンされたすべてのオブジェクトの合計数を示します。
- ***感染*** - 除去/検出された感染の合計数を示します。
- ***高/中/低*** - 次の 3項目では、重要度が高、中、低のそれぞれについて、検出された感染の数を示します。
- ***ルートキット*** - スキャン中に見つかったルートキットの合計数を示します。

ダイアログ コントロール

詳細を見る - ボタンをクリックすると、選択したスキャンに関する詳細情報 *(表の上にハイライトされています)* を参照できます。

結果を削除 - ボタンをクリックすると、一覧表から選択されたスキャン結果情報が削除されます。

 - ダイアログ左上のセクションにある緑色の矢印を使用すると、メイン ユーザーインターフェースのコンポーネント概要に戻ります。

11.6. スキャン結果詳細

選択したスキャン結果の詳細情報の概要を開くには、[***詳細を表示***] ボタンをクリックすると、[スキャン結果概要] ダイアログにアクセスできます。それぞれのスキャン結果の情報が詳細に記載された同じダイアログ インターフェースに移動します。これらの情報は 3つのタブに分けられます。

- ***概要*** - この概要では、スキャンが正常に完了したかどうかや脅威が見つかった場合に何が起こったかなど、スキャンに関する基本情報を提供します。
- ***詳細*** - このタブでは、検出された脅威の詳細など、スキャンに関するすべての情報を表示します。概要をファイルにエクスポートを使用すると、csv ファイルにスキャン結果を保存できます。

- ***検出*** - このタブはスキャン中に脅威が検出された場合にのみ表示され、その脅威に関する詳細情報を提供します。

  低い重要度: 情報または警告で、本物の脅威ではありません。通常はマクロを含むドキュメント、パスワードで保護されたドキュメントやアーカイブ、ロックされたファイルなど。

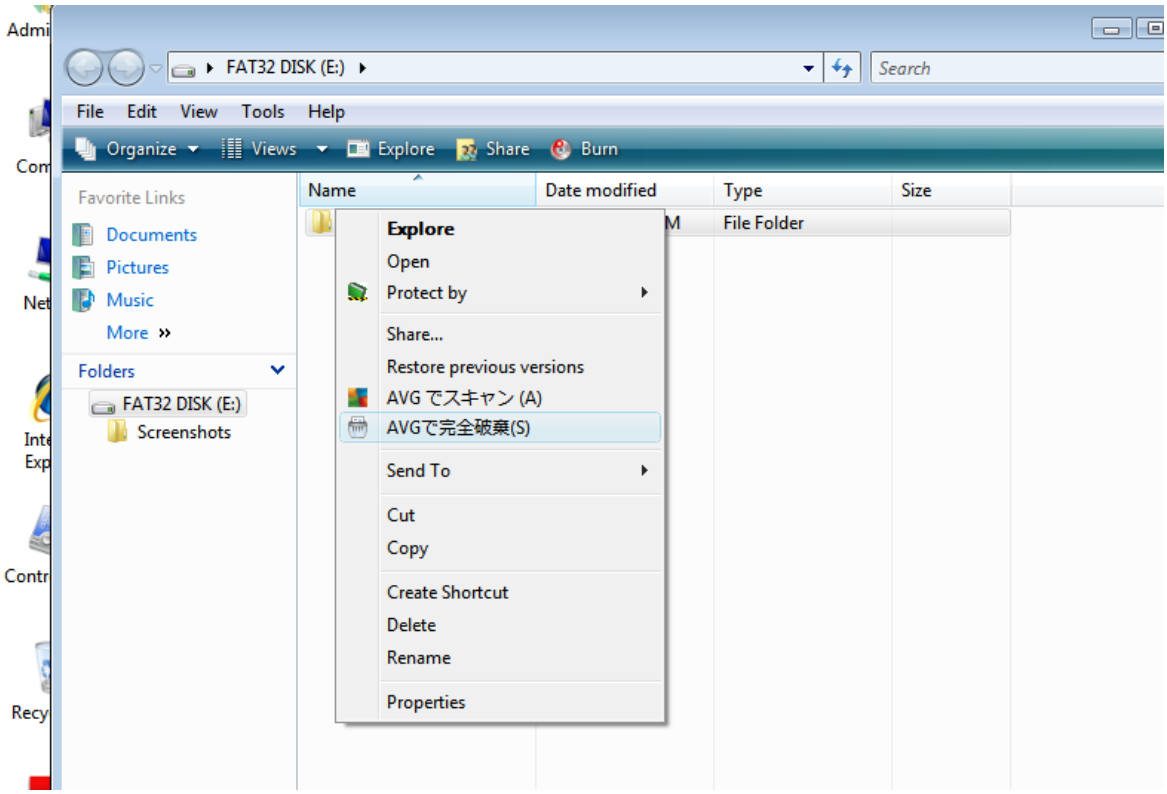
  中程度の重要度: 通常は PUP *(アドウェアなど、潜在的に望ましくないプログラム)または* tracking cookie。

  高い重要度: ウイルス、トロイの木馬、エクスプロイトなどの深刻な脅威。さらに、ヒューリスティックによる検出方法によって検出されたオブジェクト (つまり、ウイルス データベースにまだ記載されていない脅威)も挙げられます。

12. AVG File Shredder

AVG File Shredderは、完全に安全な方法でファイルを削除するように設計されており、復元のためのソフトウェアツールを使用してもまったく復元不可能です。

ファイルまたはフォルダを破棄するには、ファイルマネージャー(*Windows Explorer*、*Total Commander* など)を右クリックし、***AVGで永久に破棄***を選択します。ごみ箱にあるファイルも破棄することができます。特定の場所にある特定のファイル(*CD ROM*など)が確実に破棄できない場合、通知が表示されるか、またはコンテキストメニューのオプションが使用可能な状態になりません。



ご注意ください :破棄すると、ファイルは永久に消滅します。

13. ウイルス隔離室

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

ウイルス隔離室インターフェースが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の概要が表示されます。

- ***追加日*** - 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を表示します。
- ***脅威*** - Identity コンポーネントを **AVG Internet Security 2015** 内にインストールすることを決定した場合、検出された深刻度がこのセクションにグラフィック表示されます。深刻度は、問題なし *(緑色のドット 3個)* から、非常に危険 *(赤のドット 3個)* までです。また、感染の種類とその元の場所に関する情報も表示されます。[*詳細*] リンクをクリックすると、検出された脅威に関する詳細情報が掲載されているオンライン ウイルス百科事典のページに移動します。
- ***ソース*** - **AVG Internet Security 2015** のどのコンポーネントが各脅威を検出したかを示します。
- ***通知*** - 非常にまれな状況では、この欄に注意事項が表示され、検出された脅威のそれぞれについて、詳細なコメントが提供されます。

コントロール ボタン

ウイルス隔離室インターフェースでは次のコントロール ボタンが利用できます。

- ***復元*** - 感染ファイルをディスク上の元の場所に復元します。
- ***場所を指定して復元*** - 感染したファイルを選択したフォルダに移動します。
- ***分析に送信*** - このボタンは、上記の検出結果のリストでオブジェクトをハイライトした場合のみ選択可能になります。その場合、さらに詳細な分析を行うために、選択した検出ファイルをAVG ウイルス実験室に送信するオプションが利用できます。この機能は、主に誤検出、すなわち AVG により感染またはその疑いがあるものとして検出されたが、ユーザーは無害だと考えるファイルを送信する場合に役立つものであることにご留意ください。
- ***詳細*** - ***ウイルス隔離室***に隔離された特定の脅威に関する詳細情報については、リスト内の選択した項目をハイライトし、[***詳細***] ボタンをクリックすると、新しいダイアログが開いて検出された脅威の説明が表示されます。
- ***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。元に戻すことはできません。
- ***空にする*** - すべての***ウイルス隔離室***内のファイルを完全に削除します。***ウイルス隔離室***から削除するとファイルはディスクから削除されるため、元に戻すことはできません (*ごみ箱には移動されません*)。

14. 履歴

[***履歴***] セクションには、過去のすべてのイベント *(たとえばアップデート、スキャン、検出、その他)*に加え、これらのイベントに関するレポートが含まれます。このセクションは、メイン ユーザーインターフェースの [***オプション /履歴***] の項目からアクセスできます。さらに、すべてのイベントが記録された履歴は、次の部分に分けられます。

- スキャン結果
- 常駐シールドの結果
- メール保護の結果
- オンライン シールドの結果
- イベント履歴
- ファイアウォール ログ

14.1. スキャン結果

スキャン結果の概要 ダイアログには、**AVG Internet Security 2015** メイン ウィンドウの上の行にあるナビゲーションの [***オプション/ 履歴 /スキャン結果***] メニュー項目からアクセスできます。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
- ***高/中*** - これらの項目は、重要度が高と中のそれぞれについて、除去/検出された感染の合計数を示します
- ***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）
- ***ルートキット*** - 検出されたルートキット

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*** - クリックすると、[スキャン結果] ダイアログに切り替わり、選択したスキャンの詳細データを表示します。
- ***結果を削除*** - クリックすると、スキャン結果概要から選択したアイテムを削除します。
-  - AVG メイン ダイアログ *(コンポーネント概要)をデフォルトに戻すには、*このダイアログの左上端にある矢印を使います。

14.2. 常駐シールドの結果

常駐シールドサービスは***コンピュータ***のコンポーネントの一部であり、ファイルがコピーされたり、開かれたり、保存される時にそのファイルをスキャンします。ウイルスや何らかの種類の脅威が検出されると、以下のダイアログ経由で即時に警告が表示されます。

警告ダイアログでは、検出され感染と判断されたオブジェクトに関する情報 *(脅威)*、および認められた感染の事実的な説明 *(説明)* が表示されます。[*詳細*] リンクをクリックすると、検出された脅威が既知のものである場合、その詳細情報が記載されているオンライン ウイルス百科事典のページに移動します。ダイアログでは、検出された脅威の対処方法について、可能な解決策の概要を参照することもできます。その他の選択肢としては [***保護してください (推奨) が推奨として表示されます。可能な限り、常にこのオプションに設定しておくことをお勧めします。***

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

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

常駐シールド検出のすべてのリストが***常駐シールド検出*** ダイアログ内の概要に表示されます。このダイアログには、**AVG Internet Security 2015**メイン ウィンドウの上の行にあるナビゲーションの [***オプション / 履歴 /常駐シールド検出***] メニュー項目からアクセスできます。ダイアログには、常駐シールドが危険と見なして検出し、修復あるいはウイルス隔離室に移動し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。

- ***脅威の名前*** - 検出されたオブジェクトの説明 *(場合によっては名前)* およびその場所。[*詳細情報*] リンクをクリックすると、検出された脅威に関する詳細情報が掲載されているオンラインウイルス百科事典のページに移動します。
- ***状況*** - 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*** - 検出ができるように、潜在的に危険なオブジェクトを呼び出すために実行されたアクション

コントロール ボタン

- ***更新*** - ***オンライン シールド***
- ***エクスポート*** - 検出された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します。
- ***選択して削除*** - リスト内で選択した項目をハイライトした後にこのボタンをクリックすると、選択した項目が削除されます。
- ***すべての脅威を削除*** - このボタンをクリックすると、ダイアログのリストにあるすべての項目を削除します。
- ← - AVG メイン ダイアログ *(コンポーネント概要)をデフォルトに戻すには、*このダイアログの左上端にある矢印を使います。

14.3. Identity Protection の結果

Identity Protection の結果 ダイアログには、**AVG Internet Security 2015** メインウィンドウの上にあるナビゲーションの***オプション / 履歴 /Identity Protection の結果*** メニューからアクセスできます。

このダイアログには、Identity Protection コンポーネントによって検出された結果がすべて一覧で表示されます。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。

- ***脅威の名前*** - 検出されたオブジェクトの説明 *(場合によっては名前)* およびその場所。*[詳細]* リンクをクリックすると、検出された脅威に関する詳細情報が掲載されているオンライン ウイルス百科事典のページに移動します。
- ***状況*** - 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*** - 検出ができるように、潜在的に危険なオブジェクトを呼び出すために実行されたアクション

ダイアログの下部には、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 (***リストを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

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

- ***リストを更新*** - 検出された脅威のリストの更新
- - AVG メイン ダイアログ *(コンポーネント概要)をデフォルトに戻すには、このダイアログの左*

上端にある矢印を使います。

14.4. メール保護の結果

メール保護の検出ダイアログには、**AVG Internet Security 2015** メインウィンドウの上にあるナビゲーションの***オプション*/ 履歴 /メール保護の検出** メニューからアクセスできます。

このダイアログには、メールスキャナコンポーネントによって検出された結果がすべて一覧で表示されます。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。

- ***検出名*** - 検出されたオブジェクトの説明 *(場合によっては名前)* およびそのソース
- ***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
- ***プロセス*** - 検出ができるように、潜在的に危険なオブジェクトを呼び出すために実行されたアクション

ダイアログの下部には、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 (***リストを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
- - AVG メイン ダイアログ *(コンポーネント概要)をデフォルトに戻すには、このダイアログの左*

上端にある矢印を使います。

14.5. オンラインシールドの結果

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

警告ダイアログでは、検出され感染と判断されたオブジェクトに関する情報 *(脅威)*、および認められた感染の事実的な説明 *(オブジェクトの名前)* が表示されます。[*詳細*] リンクをクリックすると、オンラインウイルス百科事典に移動します。ここでは、既知のウイルスであれば、検出された感染の詳細な情報を調べることができます。ダイアログには次のコントロール エレメントがあります。

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

疑わしいウェブページは開かれません。また、脅威の検出は ***オンライン シールド検出結果*** のリストにログ出力されます。検出された脅威の概要には、**AVG Internet Security 2015**メイン ウィンドウの上部にある行ナビゲーションの [***オプション/履歴 /オンライン シールド検出結果***] メニュー項目からアクセスできます。

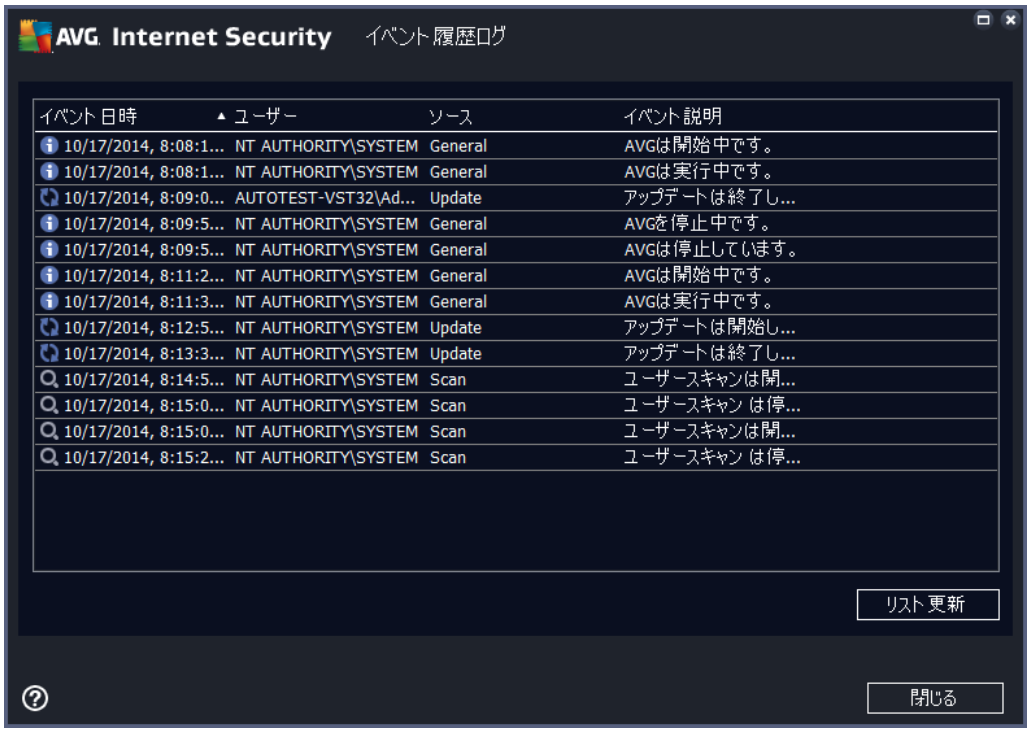
検出された各オブジェクトについて、以下の情報が提供されます。

- ***脅威の名前*** - 検出されたオブジェクトの説明 *(場合によっては名前)*、およびそのソース *(ウェブページ)*。[*詳細*] リンクをクリックすると、検出された脅威の詳細情報が記載されているオンライン ウイルス百科事典のページに移動します。
- ***状況*** - 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

コントロール ボタン

- ***更新*** - ***オンライン シールド***
- ***エクスポート*** - 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
- ← - AVG メイン ダイアログ *(コンポーネント概要)をデフォルトに戻すには、*このダイアログの左上端にある矢印を使います。

14.6. イベント履歴



イベント履歴ダイアログには、**AVG Internet Security 2015**メイン ウィンドウの上 のナビゲーションにある ***オプション/ 履歴 /イベント履歴***メニュー項目 からアクセスできます。 このダイアログでは、**AVG Internet Security 2015**動作中 に発生 した重要 なイベントの概要 を確認 できます。ダイアログでは次 のタイプのイベントの記録 が表示 されます。AVG アプリケーションのアップデートに関する情報 、スキャン の開始 、終了 、停止 に関する情報 *(自動的に実行されるテストを含む)*、ウイルス検出 *(常駐シールド または*スキャンによる)に関連するイベント情報 *(発生場所など)*、その他 の重要 なイベント。

イベントごとに次 の情報 が一覧表示 されます。

- ***イベント日時***はイベントが発生 した正確 な日付 と時刻 です。
- ***ユーザー***はイベント発生 時 にログインしていたユーザー名 を示 します。
- ***ソース***はイベントのトリガーとなったソース コンポーネントまたはその他 の AVG システムの一部 に関する情報 です。
- ***イベント説明***は実際 に発生 したイベント内容 の簡単 な概要 です。

コントロール ボタン

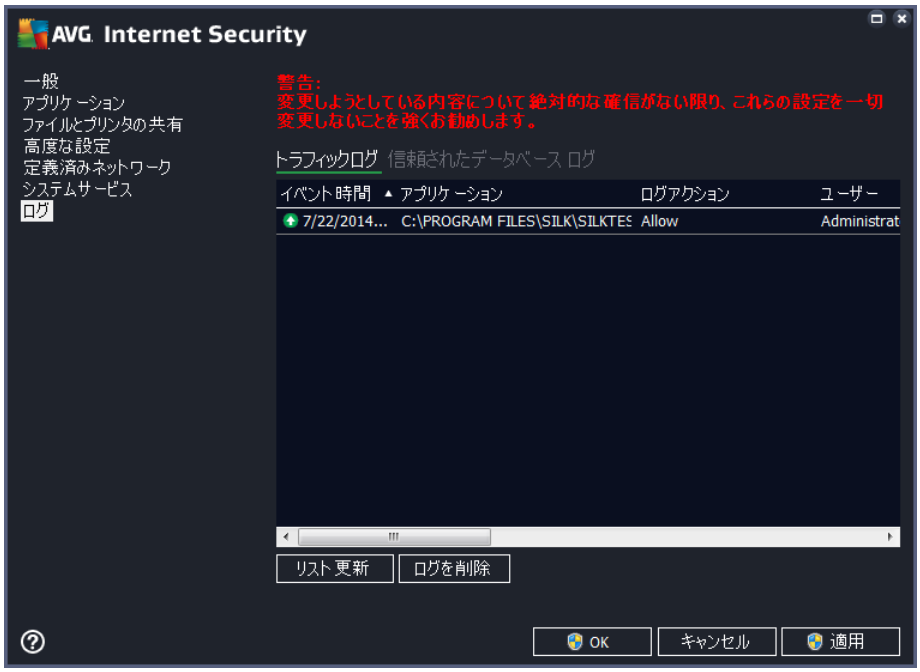
- ***リスト更新*** - このボタンをクリックすると、イベント リストのすべてのエントリが更新 されます。
- ***閉じる*** - このボタンをクリックすると、**AVG Internet Security 2015**メイン ウィンドウ

14.7. ファイアウォール ログ

このダイアログは高度な構成として用意されており、明確にその設定について知っている場合を除いて、いずれの設定も変更しないことを推奨します！

ログダイアログでは、すべてのログに記録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確認することができます。2つのタブには関連するパラメータの詳細な説明が付属しています。

- ***トラフィック ログ*** - このタブでは、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表示します。各項目では、イベント時刻、アプリケーション名、各ログ アクション、ユーザー名、PID、トラフィック方向、プロトコル タイプ、リモートおよびローカル ポート番号、リモートおよびローカル IP アドレスの情報などを見ることができます。



- ***信頼されたデータベース ログ*** - *信頼されたデータベース*とは、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

- ***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。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。

- ***ログを削除*** - 表のすべてのエントリを削除します。

15. AVG 更新

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

あらゆるコンピュータの脅威が新しく出現し、高速で拡大することを考えると、**AVG Internet Security 2015** を定期的にアップデートすることは絶対に不可欠です。最善の方法は、自動アップデートが設定されているプログラムの既定の設定に従うことです。**AVG Internet Security 2015** のウイルス データベースが最新でない場合、プログラムは最新の脅威を検出できません。

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

15.1. アップデートの実行

最高のセキュリティを実現するために、既定では、**AVG Internet Security 2015** が 4時間ごとに新しいウイルス データベースのアップデートを検索するようにスケジュール設定されています。AVG アップデートは固定のスケジュールではなく、新しい脅威の量と重要度に応じてリリースされるため、AVG ウイルス データベースが常に最新の状態であることを保証するためにはこのチェック機能が非常に重要です。

新しいアップデート ファイルをただちに確認する場合は、メイン ユーザー インターフェースの [今すぐアップデート] クイック リンクを使用します。このリンクはいつでもユーザーインターフェースダイアログから利用できます。アップデートを開始すると、AVGはまず利用可能な新しいアップデートファイルがあるかどうかを確認します。ある場合は、**AVG Internet Security 2015** はダウンロードを開始し、アップデート処理を実行します。AVG システムトレイ アイコンのスライドダイアログ内に、アップデート結果についての情報が表示されます。

アップデートの実行回数を減らす場合は、独自のアップデート実行パラメータを設定できます。しかし、***1日に少なくとも1回アップデートを実施されることが強く推奨されます。*** 設定は [高度な設定 /スケジュール] セクションで編集できます。具体的には次のダイアログが表示されます。

- 定義アップデート スケジュール
- プログラム アップデート スケジュール
- スパム対策 アップデート スケジュール

15.2. アップデート レベル

AVG Internet Security 2015 では 2つのアップデート レベルから選択できます。

- ***定義更新***には、信頼できるウイルス対策、スパム対策、およびマルウェア対策保護に必要な変更が含まれています。通常、コードの変更は含まれず、定義データベースのみをアップデートします。このアップデートは、提供され次第、すぐに適用する必要があります。
- ***プログラム アップデート***には、様々なプログラム変更、修正、改善が含まれます。

アップデートのスケジュールを作成するときには、両方のアップデート レベルのパラメータを定義できます。

- 定義 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

注意 :*プログラムのアップデートとスケジュールスキャンが同時になった場合、アップデート処理が優先度が高く、スキャンは中断されます。そのような場合、コリジョンについての通知が行われます。*

16. FAQ およびテクニカル サポート

AVG Internet Security 2015アプリケーションに関する販売や技術的な問題がある場合は、さまざまな方法でサポートを検索できます。次のオプションから選択してください。

- ***サポートを利用する***: AVG アプリケーションから AVG ウェブサイト (*http://www.avg.com/*)の専用カスタマーサポートページを表示できます。***ヘルプ /サポートを利用する*** メイン メニュー項目を選択すると、利用可能なサポート手段が掲載された AVG ウェブサイトに移動します。続行するには、Web ページの指示に従ってください。

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

- ***ヘルプ ファイルのトラブルシューティング***: 新しい ***トラブルシューティング*** セクションは、**AVG Internet Security 2015***に含まれるヘルプファイルで直接使用可能です (ヘルプ ファイルを開くには、アプリケーションのダイアログで F1 キーを押します)*。このセクションには、ユーザーが技術的な問題について専門家のヘルプを検索するときに最も多く発生している状況の一覧が表示されます。現在発生している問題に最も近い状況を選択してクリックすると、問題の解決策を示す詳細手順が表示されます。

- ***AVG ウェブサイトのサポート センター***: AVG ウェブサイト (*http://www.avg.com/*) で問題の解決策を検索することもできます。「***サポート***」セクションには、販売上の問題と技術的な問題の両方を取り扱うテーマ別のグループの概要、よくある質問の体系的なセクション、および利用可能なすべての連絡先が掲載されています。

- ***AVG ThreatLabs***: AVG 関連の専門ウェブサイト (*http://www.avg.com/about-viruses*) であり、ウイルス問題に特化し、オンラインの脅威についての概要を提供します。また、ウイルスやスパイウェアの駆除手順や脅威に対する保護方法の提案も確認できます。

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