AVG Internet Security

ユーザーマニュアル

ドキュメント改訂 AVG.05
2016/06/16

目次

1. はじめに

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

AVG Internet Security 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組み込まれており、AVG が収集した脅威に関する最新の情報をコミュニティと共有して、最高レベルの保護を確実に提供します。 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 *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 は次のオペレーティング システムのワークステーションの保護を目的としています:

- Windows XP Home Edition SP3
- Windows XP Professional SP3
- Windows Vista (すべてのエディション)
- Windows 7 (すべてのエディション)
- Windows 8 (すべてのエディション)
- Windows 10 (すべてのエディション)

(および特定のオペレーティング システム用のより新しいサービス パック)

2.2. 最低・推奨ハードウェア要件

AVG Internet Securityの最低ハードウェア要件:

- 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 GB のディスク空き領域 *(インストールのため)*

AVG Internet Security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 GB のディスク空き領域 *(インストールのため)*

3. AVG インストール プロセス

コンピュータにAVG Internet Security をインストールする場合は、最新のインストール ファイルを取得する必要があります。最新バージョンの AVG Internet Security 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!

インストール プロセスは [*AVG Internet Security へようこそ*] ダイアログで始まります。

言語選択

このダイアログでは、インストール プロセスで使用する言語を選択できます。 [*言語*] オプションの横にあるコンボ 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 プロセスを続行できます。 また、アプリケーションも選択した言語でインストールされます。英語は常にデフォルトでインストールされるため、必要に応じて英語に切り替えることができます。

エンド ユーザー ライセンス契約およびプライバシー ポリシー

インストール プロセスを続行する前に、*エンド ユーザー ライセンス契約*と*プライバシー ポリシー*の文面を一読しておくことをお勧めします。 この 2 つの文書は、ダイアログの下部にあるアクティブ リンクを経

由して参照できます。 いずれかのハイパーリンクをクリックすると、新しいダイアログ/ブラウザ ウィンドウが開き、対応する文書が表示されます。 これらは法的拘束力を持つ文書であるため、注意深くお読みください。 [*続行*] ボタンをクリックすることにより、ユーザーは文書に同意したことになります。

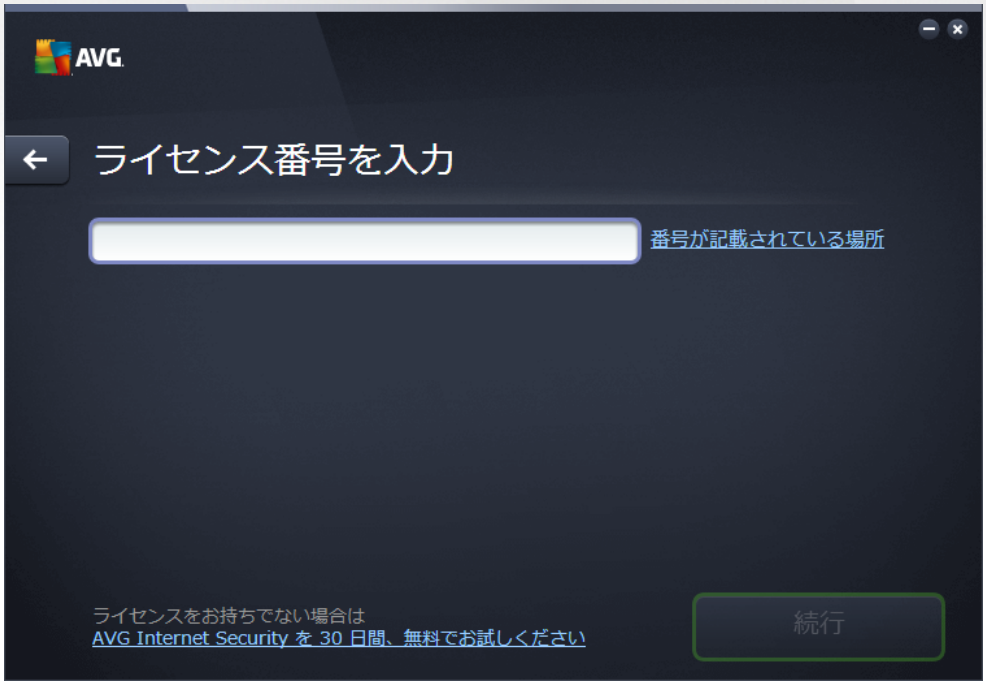
インストールの続行

インストールを続行するには、[*続行*] ボタンをクリックします。 表示されたダイアログでライセンス番号を入力した後、インストール プロセスが完全に自動モードで実行されます。 AVG Internet Security のインストールでは、プログラム ベンダーによってすべての設定があらかじめ指定されている標準オプションを使用することを、ほとんどのユーザーにお勧めします。 この設定は、最適なリソース消費で最大のセキュリティを実現します。 インストール後に、設定を変更する必要が生じた場合は アプリケーション内でいつでも直接変更できます。

また、[*カスタム インストール*] オプションも用意されています。このオプションはハイパーリンクの形式で、[*続行*] ボタンの下にあります。 カスタム インストールは、特定のシステム要件に適合させるなど、アプリケーションを標準以外の設定でインストールする合理的な理由がある上級ユーザーのみが行ってください。 このインストール方法を選択した場合は、ライセンス番号を入力した後で [*インストールのカスタマイズ*] ダイアログに移動し、設定を指定することができます。

3.2. ライセンス番号の入力

[*ライセンス番号を入力*] 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し *(またはコピーと貼り付けを使用して入力)* ライセンスを有効化するように指示されます。



ライセンス番号が記載されている場所

セールス番号は AVG Internet Security の箱の中にある 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 をオンラインで購入後に受信した確認メールに記載されています。 この番号を記載どお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 (*メールに記載されている*) 場合は、コピーと貼り付けを使用して入力することをお勧めします。

コピーと貼り付けの方法

*コピーと貼り付け*機能を使用して AVG Internet Security のライセンス番号をプログラムに入力すると、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でマウスの左ボタンをクリックし、ボタンを押したまま番号の末尾までドラッグします。 番号が強調表示されるはずです。
- *Ctrl* を押しながら *C* を押します。 これにより、番号がコピーされます。
- コピーした番号を貼り付ける位置 (*のテキスト フィールド*) にマウス ポインタを置いてクリックし、*ライセンス番号*ダイアログを入力します。
- *Ctrl* を押しながら *V* を押します。 これにより、選択した場所に番号が貼り付けられます。

インストールの続行

ダイアログの下部には [*今すぐインストール*] ボタンがあります。 ライセンス番号を入力するとボタンが有効になります。 有効化されたら、ボタンをクリックしてインストールを起動します。 有効なライセンス番号がない場合は、アプリケーションの*AVG AntiVirus Free Edition*をインストールすることもできます。 無料版は完全プロフェッショナル版で利用可能な機能をすべてサポートしていません。 このため、AVG ウェブサイト (http://www.avg.com/) にアクセスし、AVG 商品の購入とアップグレードについて情報詳細をご覧ください。

3.3. インストールのカスタマイズ

[*インストールのカスタマイズ*] 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。

どこにインストールしますか?

アプリケーションをインストールする場所を指定します。 テキスト フィールドのアドレスは、プログラム ファイル フォルダの中で推奨される場所を表します。 別の場所を指定する場合は、*場所を変更*リンクをクリックすると、新しいウィンドウが開いてディスクのツリー構造が表示されます。 希望する場所を選択し、確認します。

どのコンポーネントをインストールしますか?

このセクションには、インストール可能なすべての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します。 ただし、AVG Internet Security に含まれるコンポーネントのみを選択できます。 唯一の例外は*コンピュータ保護*コンポーネントで、これはインストールから除外できません。 このセクション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。

インストールの続行

インストールを続行するには、[*今すぐインストール*] ボタンをクリックします。 または、言語設定を変更または確認するには、このダイアログの上部にある矢印ボタン←を使って 1 つ前のダイアログに戻ります。

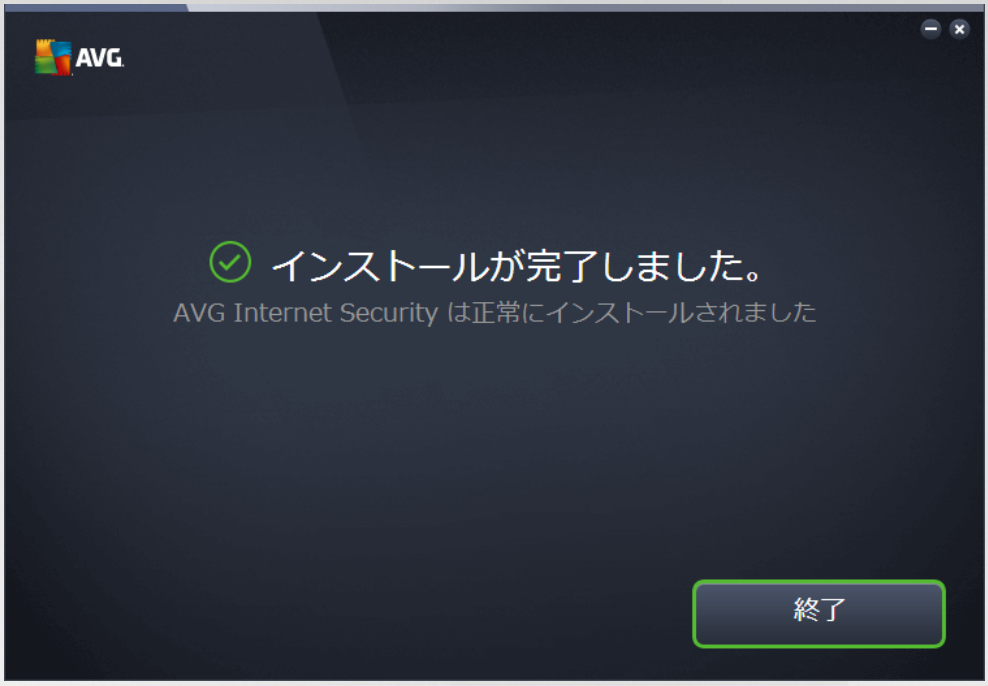
3.4. AVG のインストール

前のダイアログでインストールの起動を確認すると、インストールプロセスが自動モードで動作します。ユーザーの操作は必要としません。

インストールプロセスが完了すると、自動的に次のダイアログに移動します。

3.5. インストールが完了しました

[*インストールが完了しました*] ダイアログが表示され、AVG Internet Security のインストールと設定が完了したことを確認できます。



[*OK*] ボタンをクリックして、インストールを完了します。

4. インストール後

4.1. ウイルス データベースのアップデート

インストール時には *（必要に応じてコンピュータを再起動した後）*、AVG Internet Security はウイルスデータベースとすべてのコンポーネントを自動的に更新し、完全に動作する状態にします。この処理には数分かかる場合があります。 アップデート処理の実行中は、メイン ダイアログに表示される情報によって処理が通知されます。 アップデート処理が完了し、AVG Internet Security が完全に作動可能でユーザーを保護できる状態になるまで、しばらくお待ちください。

4.2. 製品の登録

AVG Internet Security 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 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。

4.3. 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 Internet Security システムトレイアイコンをダブルクリックする
- デスクトップにある AVG Protection アイコンをダブルクリックする
- メニューで *スタート/すべてのプログラム/AVG/AVG Protection の順に選択する*

4.4. コンピュータ全体のスキャン

AVG Internet Security 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。

4.5. Eicar 検査

AVG Internet Security インストールが正常に行われたことを確認するために、EICAR 検査を実行することができます。

EICAR 検査は、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 のウェブサイト 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 検

査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 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。

4.6. AVG の既定の設定

AVG Internet Security *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 が起動すると、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かれています:

- *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 *(その他の AVG、レポート、サポート、オプション)* で構成されています。 詳細 >>
- *セキュリティステータス情報*には、AVG Internet Security の現在のステータスの基本情報が表示されます。 詳細 >>
- *インストールされているコンポーネントの概要*は、メイン ウィンドウの中央セクションにある水平の一連の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、すで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 AVG Internet Security の追加アプリケーションの概要を示します。 詳細 >>
- *スキャン / 修復 / アップデートのクイック リンク*は、メイン ウィンドウにあるブロックの下部の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 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、モニターの右下端 *(システム トレイ上)* にあり、AVG Internet Security の現在の状態を示します。 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. その他の AVG

このリンクを 1 回クリックすると、インターネット セキュリティを最大限に高めるための AVG の保護に関するすべての情報が掲載されている AVG ウェブサイトに接続します。

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 つのタブで構成されている新しいダイアログが開き、AVG Internet Security に関連するすべての情報が表示されます。

- *ライセンスおよびサポート* - このタブには製品名、ライセンス番号、有効期限に関する情報が表示されます。 ダイアログの下部には利用可能なカスタマー サポートのすべての連絡先の概要も分かりやすく整理されて表示されます。 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 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* - 現在のライセンスの有効期限が切れる 1 か月以上前の適切な時期に、AVG Internet Security ライセンスの更新を行うことをお勧めします。 有効期限が近づくと通知が行われます。 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、ライセンスのステータス、有効期限、更新/アップグレードの割引に関する詳細な情報が表示されます。

- *製品* - このタブには、AV 製品情報、インストールされているコンポーネント、インストールされているメール保護などに関する AVG Internet Security の最も重要な技術データの概要が表示されます。

- *プログラム* - このタブには、主な商品のバージョン番号や、対応する全製品 *(Zen、PC TuneUp など)* のバージョン番号一覧など、インストールされているAVG Internet Securityに関する技術情報詳細が表示されます。 次に、このタブには、インストールされたコンポーネントの概要と、特定の

セキュリティ情報 *(ウイルスデータベースのバージョン番号、LinkScanner、およびスパム対策)* が表示されます。

- *ライセンス契約* - このタブでは、ユーザーと AVG Technologies との間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 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のスキャン...* - 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 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 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 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デフォルト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。
- *(再) 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 の試用版を使用している場合は、最後の 2 つの項目が [*今すぐ購入*] および [*アクティベート*] として表示され、完全バージョンの製品をすぐに購入できます。 セールス番号でインストールされている AVG Internet Security の場合、[*登録*] および [*アクティベート*] として表示されます。
- *今すぐ登録 / MyAccount* - 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 のメイン ウィンドウの上部にあります。 このセクションには、AVG Internet Security の現在のセキュリティステータスに関する情報が表示されます。 このセクションに表示されるアイコンの概要および意味は以下のとおりです:

 - 緑のアイコンは *AVG Internet Security 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正しく設定されておらず*、プロパティ/設定を確認する必要があるという警告です。 AVG Internet Security に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がオフにされている可能性があります。 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。 正しく設定されていないコンポーネントは、メイン ユーザーインターフェースでオレンジの細長い警告マーク付きで表示されます。

黄色のアイコンは、何らかの理由でコンポーネントのエラー状態を無視することにした場合も表示されます。 [*エラー状態を無視*] オプションは、高度な設定 / エラー状態を無視でアクセスできます。 ここでは、コンポーネントのエラー状態は認識しているが、何らかの理由により AVG Internet Security を現状のまま維持し、警告を表示しないオプションも選択できます。 特定の状況では、このオプションを使用する必要が生じることがありますが、[*エラー状態を無視*] オプションはできる限り早くオフにすることを強くお勧めします。

また、黄色のアイコンは AVG Internet Security でコンピュータの再起動が必要な場合にも表示されます（*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 が致命的な状態であることを示しています*! 1 つあるいは複数のコンポーネントが適切に動作していないため、AVG Internet Security 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、直ちに修復してください。 ユーザー自身ではエラーを修復できない場合は、AVG テクニカルサポートチームにご連絡ください。

AVG Internet Security のパフォーマンスが最適な状態に設定されていない場合は、[クリックして修復] という新しいボタン（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、プログラムの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 のパフォーマンスを最適な状態に設定し、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、レポートで問題が指摘された場合は直ちに解決することを強くお勧めします。 解決しなければ、お使いのコンピュータが危険にさらされます。

注意: AVG Internet Security ステータス情報は、システムトレイアイコンからも、いつでも取得可能です。

5.3. コンポーネント概要

*インストールされているコンポーネントの概要*は、メイン ウィンドウの中央セクションにある水平の一連の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薄い緑色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、機能が制限されているか、コンポーネントがエラー状態です。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。***

コンポーネント上にマウス カーソルを重ねると、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するものです。 また、コンポーネントの現在の状態を通知し、コンポーネントのどのサービスが正しく設定されていないかを示します。

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 の [*コンポーネントの概要*] セクションには、以下のコンポーネントに関する情報が含まれます:

- *コンピュータ* - このコンポーネントは 2 つのサービスが対象です: *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、不要な実行可能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*は、アプリケーション、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* - インターネットでの検索および閲覧中にウェブ ベースの攻撃からユーザーを保護します。 詳細 >>
- *Identify* - このコンポーネントは、インターネット上の新規または未知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* - 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チェックし、ウイルス、フィッシング攻撃や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

- *コンポーネントの概要で、任意のコンポーネントのアイコンにマウス カーソルを重ねると*、そのコンポーネントが強調表示されます。 同時に、そのコンポーネントの基本機能に関する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*] エリア *(コンポーネント セットの下にある一連の緑色のブロック)* には、すで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。 ブロックは条件に応じて表示され、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、携帯電話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操作で追跡する機能も提供します。
- *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。

マイ アプリ アプリケーションの詳細については、各ブロックをクリックしてください。 専用の AVG ウェブページに転送されます。このウェブページでは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 ユーザーインターフェースのボタン類の下の行にあります。これらのリンクをクリックすると、スキャンやアップデートなど最も重要で最も頻繁に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 つのセクションで構成されています。 *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が直ちに起動し、[レポート] ウィンドウが開いてスキャンの進行状況と結果を確認できます。 [*オプション*] ボタンをクリックすると、スキャン オプション全コンピュータをスキャン ダイアログが開き、スケジュールされたスキャンを管理し、全コンピュータをスキャン / 特定のファイルとフォルダをスキャン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)*

- *パフォーマンスを修復* - このボタンをクリックすると、*PC Analyzer* サービスに移動します。PC Analyzer 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ついて、詳細なシステム分析と修復を行うための高度なツールです。

- *すぐにアップデート* - このボタンをクリックすると、製品アップデートが直ちに開始されます。AVG システムトレイ アイコンのスライド ダイアログに、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 (モニター右下端の Windows タスクバー上) には、AVG Internet Security の現在のステータスが表示されます。 このアイコンは、AVG Internet Security のユーザーインターフェースが開いているか閉じているかにかかわらず、システム トレイに常に表示されます:

AVG システムトレイアイコンの表示

- 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 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ている場合も、アイコンはこの状態で表示されます。 *([コンポーネント状態を無視する] オプションを選択すると、ユーザーはコンポーネントのエラー状態は認識しているが、何らかの理由により現状のまま維持し、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。)*

- 感嘆符 (!) 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。 常に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、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。 どのコンポーネントがエラー状態になっているかについての詳細は、「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。

-  フルカラーで表示されているアイコンに矢印が付いている場合は、AVG Internet Security スキャンのいずれかが実行中であることを示します。

AVG システムトレイアイコンの情報

*AVG システムトレイアイコン*は、システムトレイアイコンから開くポップアップ ウィンドウを通じて、AVG Internet Security 内の現在のアクティビティ、およびプログラム内で発生する可能性のある状態の変化 (*スケジュールスキャンまたはアップデートの自動起動、ファイアウォール プロファイルの切替、コンポーネントの状態の変化、エラー状態の発生など*) に関しても通知を行います。

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 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、簡単なコンテキスト メニューが開いて以下のオプションが表示されます:

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

- *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 による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推奨されないことにご留意ください。 新しいソフトウェアまたはドライバをインストールする場合、インストールのプロセス中に望ましくない中断が発生しないよう、インストーラまたはソフトウェア 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ことがありますが、ほとんどの場合、インストール前に AVG Internet Security を無効にする必要はありません。 AVG Internet Security を一時的に無効にする必要がある場合は、作業が終わったら直ちに再び有効にしてください。 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すると、コンピュータが攻撃の危険にさらされます。

- *スキャン* - クリックすると、あらかじめ定義されたスキャン (*全コンピュータをスキャン*、*および特定のファイルとフォルダをスキャン*) のコンテキスト メニューが開き、目的のスキャンを選択すると、スキャンが直ちに実行されます。

- *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。

- *スキャンを実行しています...* - この項目は、現在コンピュータでスキャンが実行されている場合に限り表示されます。 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。 また、以下の操作も選択可能です: *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*または *すべてのスキャンの停止*。

- *パフォーマンスの修復* - クリックすると、PC Analyzer コンポーネントが起動します。

- *AVG MyAccount にログイン* - サブスクリプション製品の管理、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、個人情報の管理を実行できる MyAccount の

ホームページを開きます。

- *すぐにアップデート* - アップデートが直ちに開始されます。
- *ヘルプ* - スタート ページでヘルプ ファイルが開きます。

5.7. AVG アドバイス

*AVG アドバイス*は、コンピュータを危険にさらす可能性のある問題を検出し、その状況を解決するための対策を提案するために設計されました。 *AVG アドバイスは、システムトレイ上をスライドするポップアップとして表示されます。* このサービスでは、*よくある名前の付いた不明なネットワーク*である可能性があるものを検出します。 これは通常、一般に携帯型コンピュータでさまざまなネットワークに接続するユーザーのみに該当します: 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、まったく不明で安全ではない可能性があるネットワークに誤って接続してしまう恐れがあります。 *AVG アドバイス*は、既知の名前が実は新しいネットワークを示していることを警告することにより、この問題を防止できます。 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 アドバイス*の既知のネットワーク リストに保存できます。

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 アクセラレータ

AVG Accelerator 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。 ビデオ高速化処理の進行中は、システムトレイのポップアップ 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*コンポーネントは次の 2 つの主要なセキュリティ サービスを提供します: *ウイルス対策*および*データ セーフ*:

- *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 ディスクなど)* を保護するスキャン エンジンで構成され、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、駆除されるか、またはウイルス隔離室に隔離されます。 この処理はいわゆる常駐保護と呼ばれるもので、「バックグラウンドで」動作するため、通常ユーザーはこの処理に気が付きません。 ウイルス対策では、ヒューリスティック スキャンも使用され、一般的なウイルスの特性についてファイルがスキャンされます。 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 は、システム内で不要と考えられる実行可能アプリケーションや DLL ライブラリを分析し、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がないかシステム レジストリをスキャンするため、ユーザーは不要と考えられる項目を他の感染と同様に処理できます。

- *データ セーフ*ではセキュアな仮想隔離室を作成して貴重なデータや機密データを保管できます。データ セーフのコンテンツは暗号化され、ユーザーが設定した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。

ダイアログでの操作

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します。 切り替えた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、以下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 / 無効 - このボタンは外観が交通信号に似ていますが、機能的にも同様の役割を果たします。 有効 / 無効を切り替えるには、1 回クリックします。 緑色は*有効*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。 赤は、サービスが*無効*、すなわちアクティブではない状態を表します。 サービスを無効にする理由が特になければ、すべてのセキュリティ設定をデフォルトのままで維持することを強くお勧めします。 デフォルト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が保証されます。 何らかの理由でサービスを無効にすると、赤の*警告*サインとともに現在完全に保護されていないという情報が表示され、危険の可能性に関して直ちに警告されます。 *できるだけ早く、再びサービスを有効に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 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。このボタンを押すと、同じ名前の新しいダイアログが開き、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する必要があります。

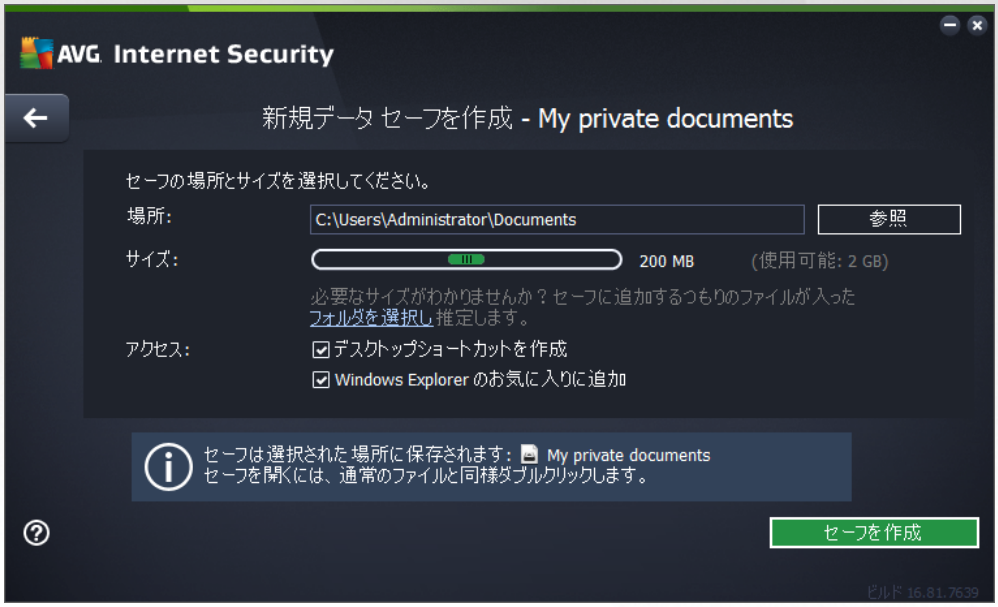
- *セーフの名前* - 新しいデータ セーフを作成するには、まず判別しやすいように適切な名前を選ぶ必要があります。 コンピュータを家族と一緒に使用している場合、セーフの内容を示すと共に自分の

名前も入ったセーフ名を付けるとよいでしょう。例えば、*父のメール*などです。

- *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、該当するテキスト フィールドに入力します。 右側の画像インジケータは、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)* か、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にすることをお勧めします。 パスワードの強度を高めるには、大文字、数字およびドット、ダッシュなどのその他の文字を含めます。パスワードが正しく入力されていることを確認するには、[*パスワードを表示する*] ボックスにチェックを入れます *(他の人が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備えて、思い出す助けとなるパスワードのヒントを作成しておく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により、ユーザーのファイルを保護する仕組みになっています。これには例外がないため、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 セーフが置かれる物理的な場所を示します。 ハードドライブの適切な場所を参照するか、あらかじめ定義された場所である [*ドキュメント*]フォルダに設定します。 一度データ セーフを作成すると、その場所は変更できないことにご留意ください。

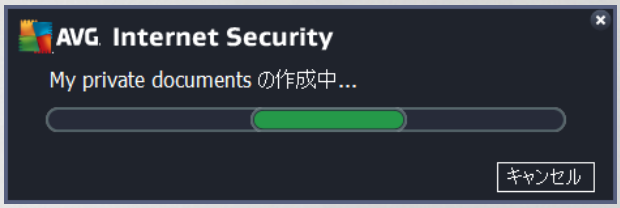
- *サイズ* - データ セーフのサイズをあらかじめ決定し、ディスク上の必要な領域を割り当てることができます。 その値は、小さすぎたり *(必要を満たさない)*、大きすぎたり *(必要以上にディスク領域を占める)* しないようにします。 データセーフに何を入れるかがすでに分かっている場合は、すべてのファイルを 1 つのフォルダに入れ、[*フォルダを選択する*] リンクを使用して、合計サイズを自動計算することができます。 ただし、必要に応じて、後でサイズ変更することも可能です。

- *アクセス* - このセクション内のチェックボックスを使用すると、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

設定が問題なく完了したら、[*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が通知されます。この時点でセーフは開いており、直ち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います:



新しいデータ セーフを使用するには、まず [*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 メニューで任意の文字を割り当てます (*現在空きのあるディスクのみが選択可能です*)。 一般的に、C *(通常は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)*、または D *(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。 新しいデータ 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、必要に応じてファイルを追加/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。*

ダイアログでの操作

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します。 切り替えた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、以下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 / 無効* - このボタンは外観が交通信号に似ていますが、機能的にも同様の役割を果たします。 有効 / 無効を切り替えるには、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。 赤は、サービスが *無効*、すなわちアクティブではない状態を表します。 サービスを無効にする理由が特になければ、すべてのセキュリティ設定をデフォルトのままで維持することを強くお勧めします。 デフォルト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が保証されます。 何らかの理由でサービスを無効にすると、赤の *警告* サインとともに現在完全に保護されていないという情報が表示され、危険の可能性に関して直ちに警告されます。 ***できるだけ早く、再びサービスを有効にするようにしてください。***

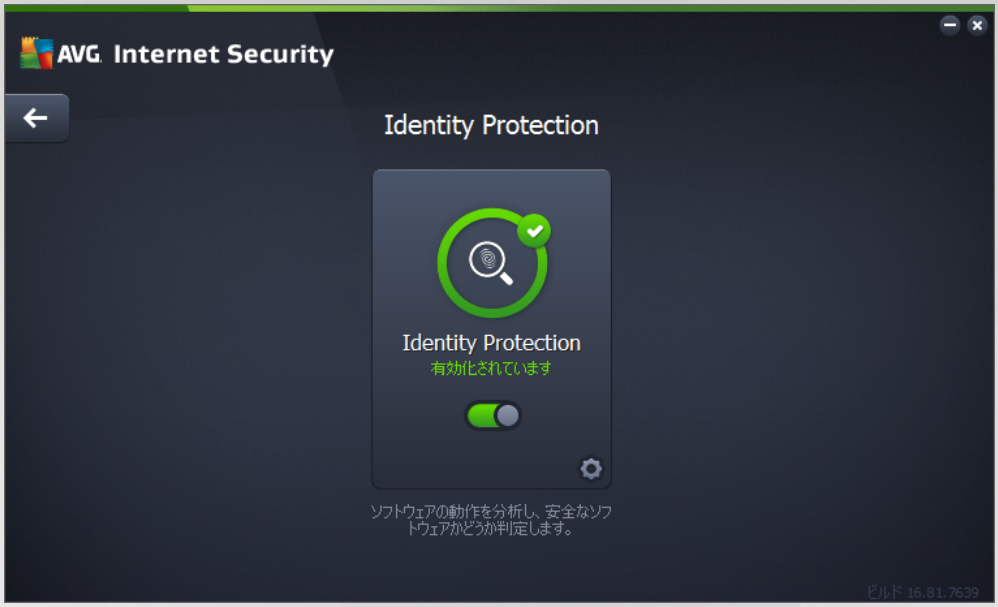
 *設定* - このボタンをクリックすると、高度な設定インターフェースに移動します。 各ダイアログが開き、リンクスキャナ サーフシールドまたはオンラインシールドなど、選択したサービスの設定ができます。 高度な設定インターフェースでは、AVG Internet Security 内の各セキュリティ サービスの設定をすべて編集できます。ただし、設定は上級ユーザーのみが行うことをお勧めします。

 *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未知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*) からユーザーを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、銀行口座情報、クレジットカード番号およびその他の貴重な個人のデジタル情報の窃盗を防止することを主な目的としています。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 は継続的に作動して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も含めて、お使いのコンピュータをリアルタイムで保護します。 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 はコードを削除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)* をすべて元に戻します。 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。 この技術は非常に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。常に保護が有効になっています。



ダイアログでの操作

ダイアログには、以下のコントロールが表示されます。

有効 / 無効 - このボタンは外観が交通信号に似ていますが、機能的にも同様の役割を果たします。 有効 / 無効を切り替えるには、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。 赤は、サービスが*無効*、すなわちアクティブではない状態を表します。 サービスを無効にする理由が特になければ、すべてのセキュリティ設定をデフォルトのままで維持することを強くお勧めします。 デフォルト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が保証されます。 何らかの理由でサービスを無効にすると、赤の*警告*サインとともに現在完全に保護されていないという情報が表示され、危険の可能性に関して直ちに警告されます。 *できるだけ早く、再びサービスを有効に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を行うことができます。 高度な設定インターフェースでは、AVG Internet Security 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 には Identity Alert サービスは含まれていません。 このタイプの保護を利用する場合は、[*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 エディションの場合も、Identity Alert サービスが利用できるのは次の地域のみとなります: 米国、英国、カナダ、アイルランド。

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 サービスを提供します: *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 1 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ますが *(めったにスパム対策技術を導入していないため)*、かなりのホームユーザーはこのようなメールを利用しています。 また、ホームユーザーは、不明なサイトをインターネットサーフィンしたり、個人情報 *(メール アドレスなど)* を含むオンラインフォームに情報を入力し、メールを介しての攻撃にさらされる機会を増やします。 会社は、通常会社のメールアカウントを使用し、スパム対策フィルタ等を導入してリスクを削減します。 メール保護コンポーネントは、すべての送受信されるメール 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しない)* 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。

ダイアログでの操作

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します。 切り替えた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、以下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 / 無効* - このボタンは外観が交通信号に似ていますが、機能的にも同様の役割を果たします。 有効 / 無効を切り替えるには、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。 赤は、サービスが *無効*、すなわちアクティブではない状態を表します。 サービスを無効にする理由が特になければ、すべてのセキュリティ設定をデフォルトのままで維持することを強くお勧めします。 デフォルト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が保証されます。 何らかの理由でサービスを無効にすると、赤の *警告*サインとともに現在完全に保護されていないという情報が表示され、危険の可能性に関して直ちに警告されます。 *できるだけ早く、再びサービスを有効に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 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 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にして、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 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推奨されます。

- *インタラクティブ* - 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くなり、外部からユーザーのコンピュータにアクセスすることもできません。 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 (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、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 ID 保護 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。

ダイアログでの操作

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横にある [*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、前の段落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、2 つのオプションを示すポップアップ メニューが開きます。

  - *高度な設定* - 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。 ただし、設定の変更はすべて上級ユーザーのみが行って下さい。

  - *ファイアウォール保護を削除する* - このオプションを選択すると、ファイアウォール コンポーネントをアンインストールします。これにより、セキュリティ保護が脆弱になります。 それでもファイアウォール コンポーネントを削除する場合は、決定を確認して、コンポーネントを完全にアンインストールします。

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。

6.6. PC Analyzer

PC Analyzer コンポーネントは、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。 このコンポーネントは、メイン ユーザーインターフェース ダイアログにある [*パフォーマンスを修復*] ボタン、またはシステムトレイの AVG アイコンのコンテキスト メニューにある、同じ名称のオプションを使用して開きます。 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、コンピュータの処理速度低下またはエラー メッセージの表示の原因となっている可能性のある Windows レジストリのエラー件数を示します。
- *不要なファイル*は、ディスク領域を占有しており、削除できる可能性が高いファイルの数を示します。 通常、これらのファイルはさまざまな種類の一時ファイルやごみ箱にあるファイルです。
- *断片化*では、長期間の使用によりほとんどのファイルが物理ディスクのいたるところに分散してしまったハードディスクの断片化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見つけます。

結果の概要には、検出されたシステム上の問題の件数が各検査カテゴリに従って分類されて表示されます。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中断されます。
- *今すぐ解決*（*分析が完了すると表示*）- 残念ながら、AVG Internet Security 内の PC Analyzer の機能は、お使いの PC の現在の状態分析に限定されています。 ただし、AVG では、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を提供しています。 ボタンをクリックすると、詳細な情報の専用ウェブサイトにリダイレクトされます。

7. AVG 高度な設定

AVG Internet Security の高度な設定ダイアログは [*高度な AVG 設定*] という名前の新しいダイアログで開きます。 このウィンドウは2つのセクションにわかれています。左部はにツリー状のナビゲーションが表示されます。設定を変更したいコンポーネント（*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。

7.1. 表示

ナビゲーション ツリーの最初の項目である [*表示*] とは、AVG Internet Security ユーザーインターフェースの一般設定のことで、アプリケーションの動作のいくつかの基本的なオプションを提供します。

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 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 (*デフォルトで自動的にインストール*) のみが表示されます。 AVG Internet Security の言語切り替えを完了させるには、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

- アプリケーションの言語を変更するには AVG Internet Security の再起動が必要であることを通知する、新しいダイアログがポップアップ表示されます

- [*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に同意すると、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 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。 デフォルトでは、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 コンポーネントのステータス変更などを通知します。 これらの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、この方法で通知を行わない場合、またはある通知 *(特定の AVG Internet Security コンポーネントに関するもの)* 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 (デフォルトではオン)* - デフォルト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オフになります。 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 (デフォルトではオン)* - AVG Internet Security 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。

  - *常駐シールド自動脅威削除の通知 (デフォルトではオン)* - ファイルの保存、コピー、および開く処理に関する情報を表示するか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のみ有効*)。

  - *スキャン 通知 (デフォルトではオン)* - 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 (デフォルトではオン)* - コンポーネントの有効化/無効化の警告、トラフィック ブロックの可能性など、ファイアウォールの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。 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 (デフォルトではオフ)* - 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、ファイルとプリンタの共有がどのように設定されるかを通知します。

    - *ブロックされたアプリケーション (デフォルトではオン)* - 不明または不審なアプリケー

ションがネットワークに接続しようとしている場合、ファイアウォールがその試みをブロックし、通知を表示します。 必ず通知が行われて便利なため、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 (デフォルトではオン)* - 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 (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、定期的な統計情報確認通知がシステムトレイに表示されます。
- *AVG アドバイスに関する通知 (デフォルトではオン)* - AVG アドバイス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 スキャンが開始されるときなどに表示*) 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または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 (*デフォルトの設定*)。

7.2. サウンド

*サウンド設定*ダイアログでは、サウンド通知によって特定の AVG Internet Security 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 (*このオプションはデフォルトでは有効*) 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。

7.3. 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 の保護機能をすべて一度にオフにできます。

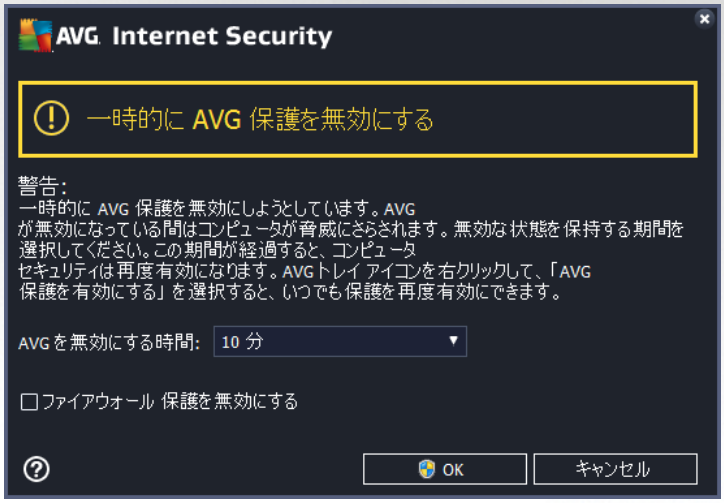
やむを得ない場合を除き、このオプションの使用は推奨されないことにご留意ください。

新しいソフトウェアまたはドライバをインストールする場合、インストールのプロセス中に望ましくない中断

が発生しないよう、インストーラまたはソフトウェア 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ことがありますが、ほとんどの場合、インストール前に AVG Internet Security 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 を一時的に無効にする必要がある場合は、作業が終わったら直ちに再び有効にしてください。 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。 新しく開く [*一時的に AVG 保護を無効にする*] ダイアログで、AVG Internet Security を無効にする時間を指定します。 デフォルトでは、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。より長い時間を設定することも可能ですが、やむを得ない場合を除き、このオプションはお勧めしません。 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。



7.4. コンピュータの保護

7.4.1. 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にする*] 項目 (*このオプションはデフォルトではオン*) のチェックを付けるか外して、常駐保護を完全に有効または無効にできます。 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* (*デフォルトではオン*) - 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 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。

- *不要と考え得るアプリケーションとスパイウェアの脅威を報告する* (*デフォルトではオン*): チェックを付けると、スキャンが有効になり、ウイルスに加えてスパイウェアもスキャンされます。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 リスクとなりますが、このプログラムの一部は意図的にインストールできます。 コンピュータのセキュリティが高まるため、この機能を有効にしておくことをお勧めします。

- *不要と考え得るアプリケーション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、製造元から直接入手したときには完全に問題がなく無害ですが、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のセキュリティをさらに高めるための追加的な手段ですが、合法的なプログラムもブロックする可能性があるため、デフォルトではオフになっています。

- *終了時にファイルをスキャン* (*デフォルトではオフ*) - 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) の起動および終了時に AVG による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* (*デフォルトではオン*) - 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 1 つです。

- *レジストリで参照するファイルをスキャン* (*デフォルトではオン*) - 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* (*デフォルトではオフ*) - 特定の状況 (*緊急事態*) では、このオプションにチェックを付けて、最も完全なアルゴリズムを有効にし、脅威の原因となる可能性のあるすべてのオブジェクトを徹底的にチェックすることができます。 ただし、この方法を実行すると多少時間がかかることにご留意ください。

- *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* (*デフォルトではオン*) - 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!、ICQ、Skype、MSN Messenger など*) 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にウイルスが含まれていないことを確認します。

注意: AVG 製品が Windows 10 にインストールされた場合は、リストの中に「より綿密なソフトウェア スキャンのために Windows Antimalware Scan Interface (AMSI) を有効にする」というもう 1 つの項目があります。この機能により、Windows と AVG が緊密に連携して悪意のあるコードを明らかにし、保護の信頼性を高めて誤検出の件数を減らすことが可能になるため、ウイルスからの保護が強化されます。

[*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、*特定の拡張子を指定して*スキャン対象のファイルを設定できます。

該当するチェック ボックスにチェックを付けて、*すべてのファイルをスキャン*するか、*感染の可能性があるファイルと選択された種類の文書をスキャン*するかを決定します。 スキャンを高速化すると同時に最高水準の保護を維持するには、デフォルトの設定を維持することをお勧めします。 こうすることにより、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、スキャンに含まれるファイルを指定する拡張子の編集可能なリストが表示されます。

[*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のファイルも常駐シールドによって確実にスキャンされます。 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お勧めします。

7.4.2. 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] に含まれるデフォルトの処理です。

*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できます。 これらの設定は上級ユーザー向けです。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。

7.4.3. 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 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安全で再スキャンの必要がないファイルと自動的にみなされるため、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*がオフに切り替わり、キャッシュ メモリが空になります。 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、すで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、デフォルトの設定を保持し、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。

7.5. 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。

7.5.1. メールスキャナ

[*メールスキャナ*] ダイアログは 3 つのセクションに分かれています。

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* (*デフォルトではオン*) - このボックスにチェックを付けると、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オプションがオンになります
- *送信メールをチェックする* (*デフォルトではオフ*) - このボックスにチェックを付けると、ユーザー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オプションがオンになります。
- *ウイルスに感染したメッセージの件名を修正する* (*デフォルトではオフ*) - スキャンしたメール メッセージが感染していることが検出された場合に警告を表示するには、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。 検出された各メール メッセージの [件名] フィールドにこのテキストが追加され、感染メッセージを簡単に識別して除外できます。 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* (*デフォルトではオン*) - チェックを付けると、メール メッセージをスキャンする際にヒューリスティック検出方式が使用されます。 このオプションをオンにすると、拡張子だけでなく実際の添付ファイルの内容も考慮して、メールの添付ファイルをフィルタリングできます。 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。

- *不要と考え得るアプリケーションとスパイウェアの脅威を報告する* (*デフォルトではオン*) - チェックを付けると、スキャンが有効になり、ウイルスに加えてスパイウェアもスキャンされます。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 リスクとなりますが、このプログラムの一部は意図的にインストールできます。 コンピュータのセキュリティが高まるため、この機能を有効にしておくことをお勧めします。

- *不要と考え得るアプリケーション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、製造元から直接入手したときには完全に問題がなく無害ですが、後から悪意のある目的で誤用されるおそれのあるプログラムです。 これは、コンピュータ セキュリティをさらに高めるための追加的な手段ですが、合法的なプログラムもブロックする可能性があるため、デフォルトではオフになっています。

- *アーカイブ内部をスキャン* (*デフォルトではオン*) - 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* (*デフォルトではオフ*) - 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*) が発生した場合には、このオプションにチェックを付けると、最も完全なスキャン アルゴリズムが有効になり、感染の可能性が低いコンピュータ領域もスキャンされます。これにより、問題がないことが確認できます。 ただし、この方法を実行すると多少時間がかかることにご留意ください。

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ないことにご注意ください。認証テキストのみがメール メッセージの最後に追加され、このようなレポートは [メール保護検出] ダイアログにリスト表示されます。

- *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*) はウイルスのスキャンができません。このボックスにチェックを付けると、アーカイブは潜在的に危険なものとして報告されます。

- *パスワード保護された文書を報告する* - パスワードで保護された文書はウイルスのスキャンができません。このボックスにチェックを付けると、これらの文書が潜在的に危険なものとして報告されます。

- *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手順です (*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るため、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が不審なファイルとして報告されます。

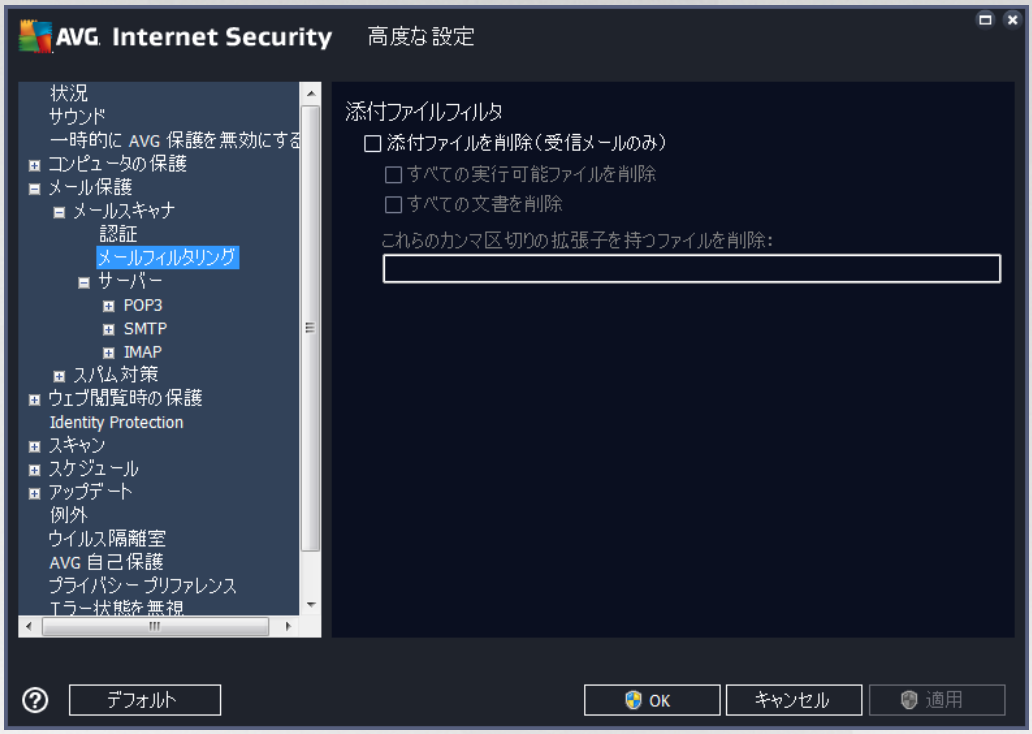
- *拡張子偽装を報告する* - 拡張子偽装を行うと、例えば、不審な実行可能ファイル「something.txt.exe」を無害なテキスト ファイル「something.txt」のように見せかけることができます。このボックスにチェックを付けると、このような拡張子が潜在的に危険なオブジェクトとして報告されます。

- *レポートされた添付ファイルをウイルス隔離室に移動* - メール メッセージのスキャンで検出された添付ファイルがパスワードで保護されたアーカイブ、パスワードで保護された文書、マクロを含むファイル、および/または拡張子偽装が行われたファイルの場合にメールで通知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に、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も指定できます。

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。

デフォルトでは、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、自動生成される認証テキスト (*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デフォルト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

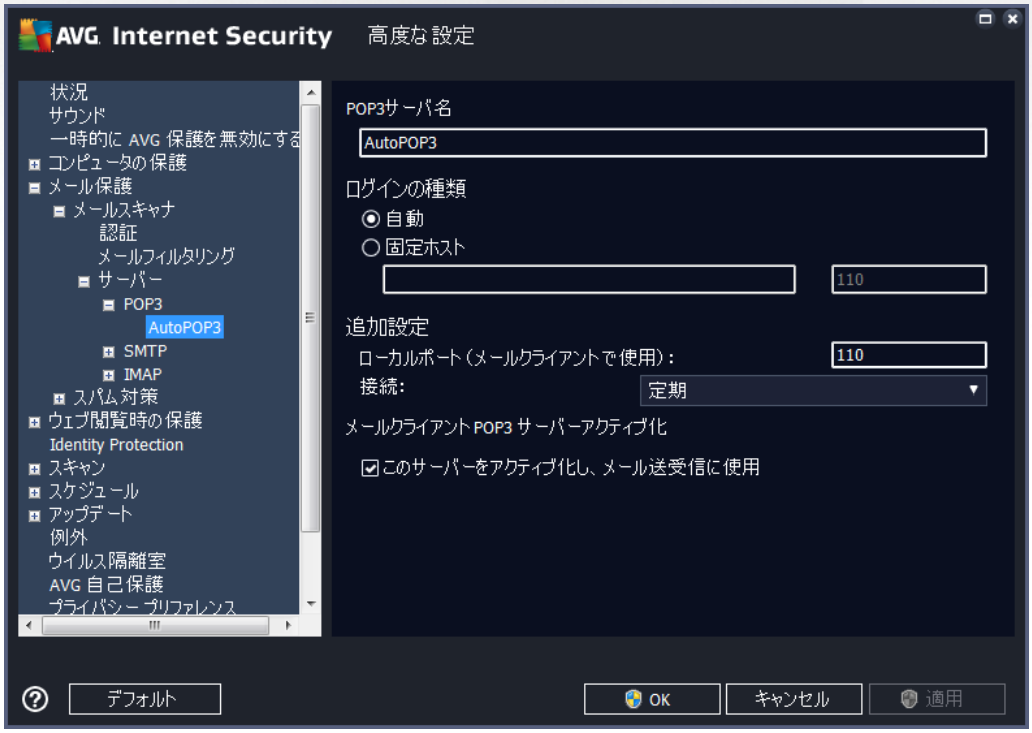
サーバー セクションでは、メールスキャナ サーバーのパラメータを編集することができます。

- 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

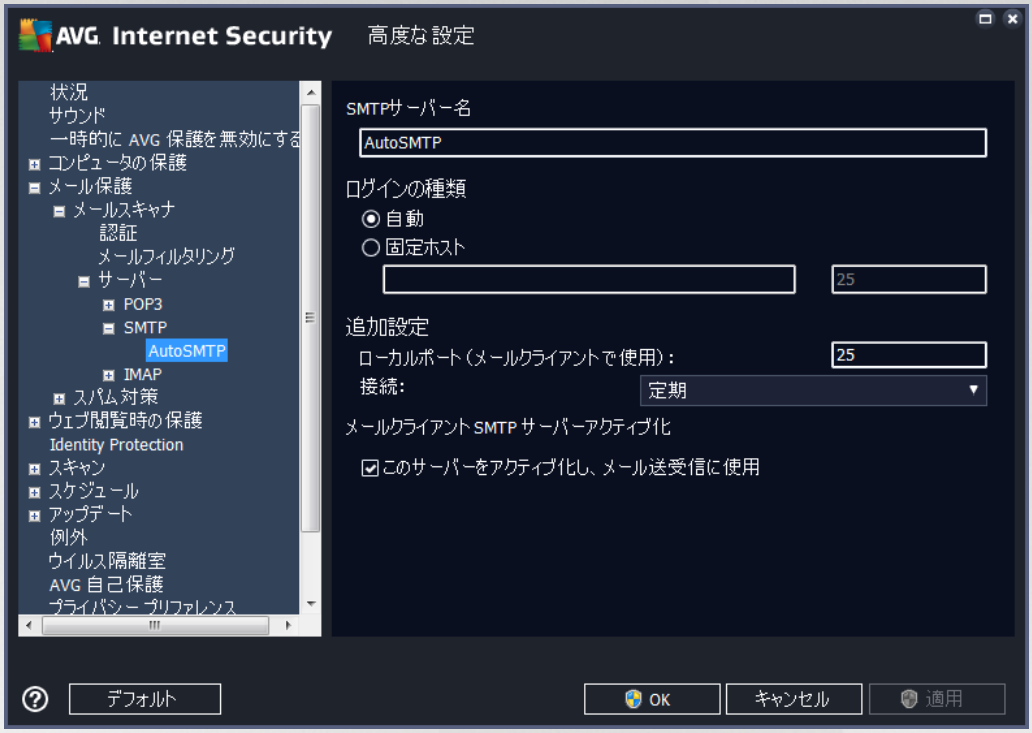
す。

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しく追加したサーバー名を指定できます (*POP3 サーバーを追加するには、左側のナビゲーション メニューの POP3 項目を右クリックします*)。
- *ログインの種類* - 受信メールに使用されるメールサーバー決定方法を定義します。
    - *自動* - ログインは、メール クライアント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または名前を指定してください。 ログイン名は変更されないままになります。 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 アプリケーションで、このポートを POP3 通信用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 デフォルト*) 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。

このダイアログでは、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* - メールクライアントの設定に応じて、 ログインが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または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。

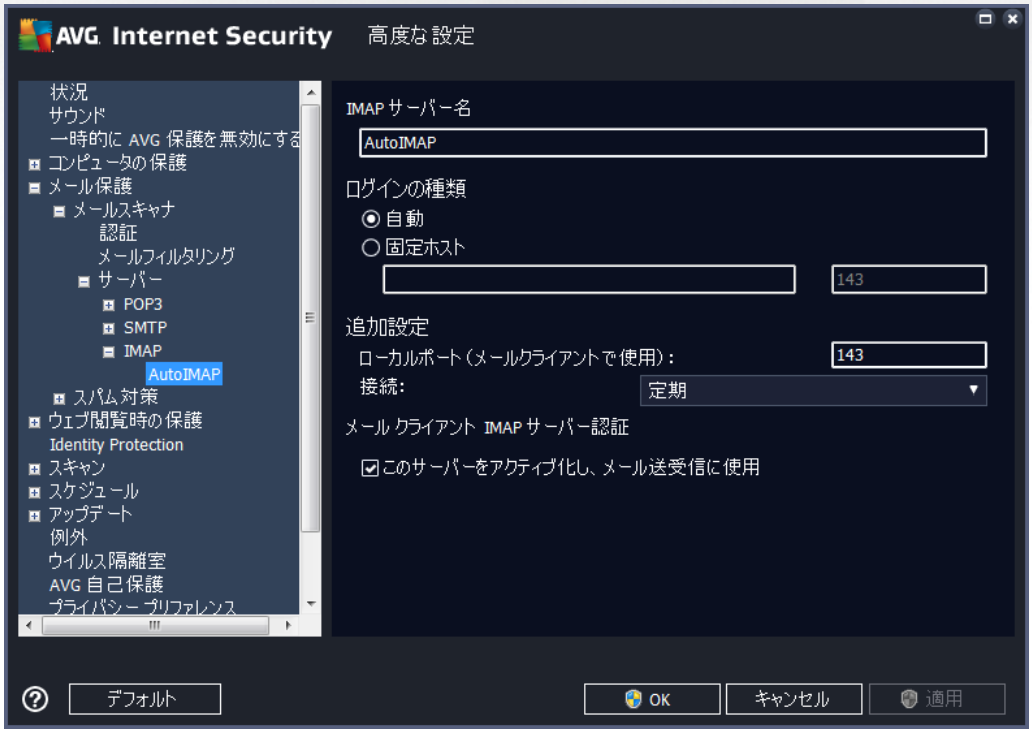
  - *ローカルポート* - メールアプリケーションからの通信用ポートを指定します。 このポートをメール アプリケーションの SMTP 通信ポートとして指定する必要があります。

  - *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 デフォルト*) 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* - このボックスを選択/クリアすると、指定した

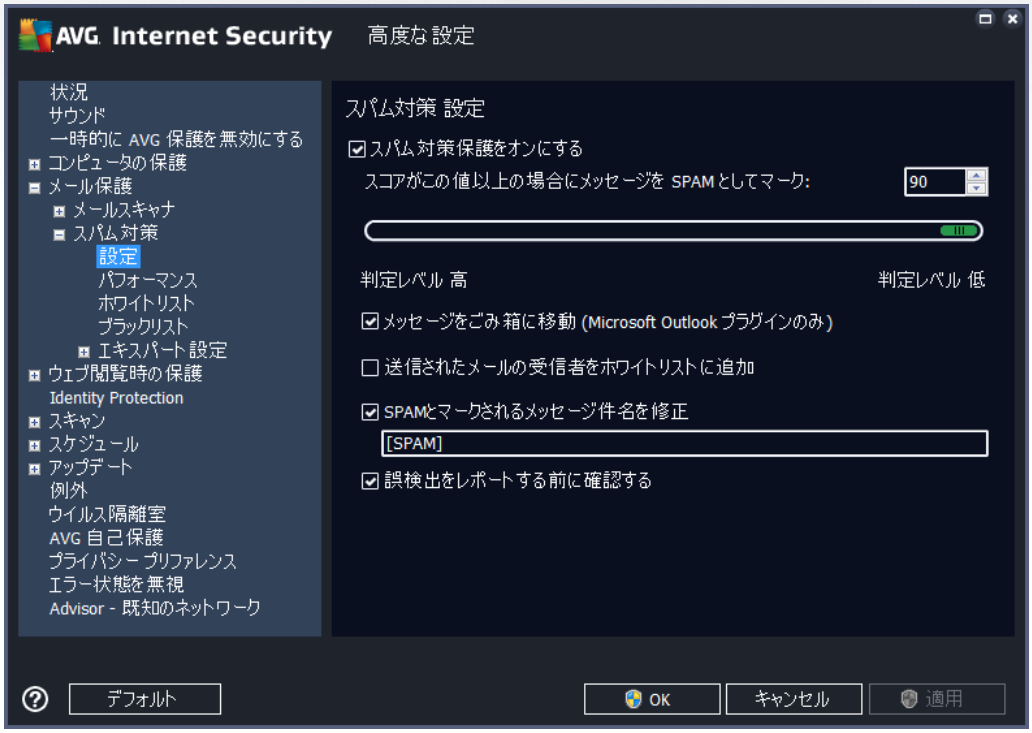
SMTP サーバーを有効/無効にします。

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しく追加したサーバー名を指定できます (*IMAP サーバーを追加するには、左側のナビゲーション メニューで右クリックします*)。
- *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* - メールクライアントの設定に応じて、 ログインが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または名前を指定してください。 名前については、ドメイン名 (*smtp.acme.com など*) および IP アドレス (*123.45.67.89 など*) を使用できます。 メール サーバーが標準以外のポートを使用する場合、このポートをコロンで区切り、サーバー名の後に指定できます (*smtp.acme.com:8200 など*)。 IMAP 通信の標準ポートは 143 です。
- *追加設定* - より詳細なパラメータを設定します。
    - *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デフォルト*) 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。

7.5.2. 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。 このオプションはデフォルト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 (*メッセージの内容と スパム メッセージとの類似性など*)。 値を入力するか、スライダーを左右に動かして、[*スコアがこの値を超える場合はメッセージをスパムとみなす*] 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去される可能性があります。
- *値 60 ~ 79* - かなり積極的な設定です。 スパムの可能性があるメールは除外されます。 正常なメッセージも除外される可能性があります。
- *値 50 ~ 59* - 非常に積極的な設定です。 正常なメールが本物のスパム メッセージと同様に除外される可能性が高くなります。 *この値は通常の使用には推奨されません。*

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

- *メッセージをゴミ箱に移動 (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ゴミ箱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確認します。
- *スパムとして判定されたメッセージの件名を修正* - スパムとして検出されたメッセージの件名にを特定の単語や文字を追加する場合は、このチェックボックスにチェックを付けます。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、プライバシー設定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する場合に選択します。

*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化*] はデフォルトでオンとなっています。 これにより、Mailshell サーバーとの通信によってスキャン 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*) のリストを編集できます。 すで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 項目 (*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、このボタンを押します。 すべてのレコードがプレーン テキスト ファイルに保存されます。
- *インポート* - メール アドレスやドメイン名のテキスト ファイルがすでにある場合は、このボタンを選択するだけで簡単にそのファイルをインポートできます。 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/ドメインからのメールは、すべてスパムとして認識されます。 すで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 項目 (*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、このボタンを押します。 すべてのレコードがプレーン テキスト ファイルに保存されます。
- *インポート* - メール アドレスやドメイン名のテキスト ファイルがすでにある場合は、このボタンを選択するだけで簡単にそのファイルをインポートできます。

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、マルチヒント、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

7.6. 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* - (*デフォルトではオン*) 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。

7.6.1. 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 (デフォルトではオン)* - *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、この後に表示される [ウェブ保護] というダイアログで設定します。

- *AVG Accelerator を有効にする (デフォルトではオン)* - 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 ビデオの再生をスムーズにして、ダウンロードを簡単にします。 ビデオ高速化処理の進行中は、システムトレイのポップアップ 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。

[*ウェブ保護*] ダイアログでは、ウェブサイトの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できます。 編集インターフェースでは、以下の基本的なオプションを設定できます:

- *アーカイブチェック* - (*デフォルトではオフ*): 表示される www ページに含まれるアーカイブのコンテンツをスキャンします。
- *不要と考え得るアプリケーションとスパイウェアの脅威を報告する* - (*デフォルトではオン*): チェックを付けると、ウイルスに加えてスパイウェアのスキャンも有効になります。 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 リスクとなりますが、このプログラムの一部は意図的にインストールできます。 コンピュータのセキュリティが高まるため、この機能を有効にしておくことをお勧めします。
- *不要と考え得るアプリケーションの拡張セットについて報告する* - (*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、製造元から直接入手したときには完全に問題がなく無害ですが、後から悪意のある目的で誤用されるおそれのあるプログラムです。 これは、コンピュータ セキュリティをさらに高めるための追加的な手段ですが、合法的なプログラムもブロックする可能性があるため、デフォルトではオフになっています。
- *ヒューリスティック分析を使用* - (*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 オブジェクトの命令の動的エミュレーション*) を使用して、表示されるページの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*): 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*) が発生した場合には、このオプションにチェックを付けると、最も完全なスキャン アルゴリズムが有効になり、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されます。これにより、問題がないことが確認できます。 ただし、この方法を実行すると多少時間がかかることにご留意ください。

- *暗号化 (TLS および SSL) ネットワーク トラフィックをスキャン* - (*デフォルトではオン*): このオプションにチェックを付けたままにすると、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 とその新バージョン、TLS) での接続も AVG によってスキャンされます。 これには HTTPS を使用するウェブサイト、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なため、この証明書の下に運営されるウェブ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をスキャンしないことにし、暗号化通信を比較的高速にすることができます。

- *ダウンロードされた実行可能ファイルを常駐シールドでスキャンする* - (*デフォルトではオン*): 実行可能ファイル *(一般に、拡張子が exe、bat、com のファイル)* をダウンロードした後でスキャンを行います。 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、悪意のあるコードがコンピュータに侵入するのを防ぎます。 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*により制限されます - このダイアログの次の項目を参照してください。 そのため、大きなファイルは部分ごとにスキャンされますが、ほとんどの実行可能ファイルもこれに該当します。 実行可能ファイルは、コンピュータでさまざまなタスクを実行できるため、100% 安全である必要があります。 これは、ダウンロード前に部分ごとのファイル スキャンを行い、ダウンロード完了直後にもスキャンを行うことで確実になります。 このオプションにチェックを付けておくことをお勧めします。 このオプションを無効にした場合も、AVG では潜在的に危険なコードを検出するため、心配は無用です。 ただし、通常の場合、実行可能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*スキャンされるファイルの最大部分サイズ*を定義できます - 含まれるファイルが表示されているページにある場合、それをコンピュータにダウンロードする前に、内容をスキャンすることも可能です。 ただし、大きいファイルのスキャンにはかなりの時間がかかり、ウェブページのダウンロード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*でスキャンするファイルの最大サイズを指定できます。 ダウンロードする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。ファイルが感染している場合、*常駐シールド*がそれを直ちに検出します。

7.7. 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 をアクティベート (デフォルトではオン) - 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。
- ***検出された脅威を自動的に隔離する*** - 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。 デフォルト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。
- ***既知の脅威を自動的に隔離する*** *(デフォルトではオン)* - マルウェアの可能性があるものとして検出された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。

7.8. 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。

7.8.1. 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* (*デフォルトではオン*) - スキャン中にウイルスが検出されると、修復可能な場合は自動的に修復されます。 感染したファイルを自動的に修復できない場合、感染したオブジェクトはウイルス隔離室に移されます。
- *不要と考え得るアプリケーションとスパイウェアの脅威を報告する* (*デフォルトではオン*): チェックを付けると、スキャンが有効になり、ウイルスに加えてスパイウェアもスキャンされます。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 リスクとなりますが、このプログラムの一部は意図的にインストールできます。 コンピュータのセキュリティが高まるため、この機能を有効にしておくことをお勧めします。

- *不要と考え得るアプリケーション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、製造元から直接入手したときには完全に問題がなく無害ですが、後から悪意のある目的で誤用されるおそれのあるプログラムです。 これは、コンピュータ セキュリティをさらに高めるための追加的な手段ですが、合法的なプログラムもブロックする可能性があるため、デフォルトではオフになっています。

- *Tracking Cookie 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、Cookie の検出が行われます (*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、維持に使用されます*)。

- *アーカイブ内部をスキャン* (*デフォルトではオフ*) - このパラメータを指定すると、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がスキャンされます。

- *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 オブジェクトの命令の動的エミュレーション*) は、スキャン中に使用されるウイルス検出方法の 1 つです。

- *システム環境をスキャン* (*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領域もチェックされます。

- *完全スキャンを有効にする* (*デフォルトではオフ*) - 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*) が発生した場合には、このオプションにチェックを付けると、最も完全なスキャン アルゴリズムが有効になり、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されます。これにより、問題がないことが確認できます。 ただし、この方法を実行すると多少時間がかかることにご留意ください。

- *ルートキットをスキャンする* (*デフォルトではオン*) - 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が PC にないかどうか調べます。 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わけではありません。 場合によっては、通常のアプリケーションの特定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ます。

スキャンするかどうかを判断する必要もあります

- *すべてのファイルタイプ* このオプションでは、スキャンが不要なファイルの拡張子をコンマで区切ったリスト (*保存後、コンマはセミコロンに変化*) を指定することにより、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低いため、このボックスのチェックを外すと、スキャン時間がさらに短縮されます*) 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を、拡張子を用いて指定できます。

- 任意で*拡張子のないファイルをスキャン*できます。このオプションはデフォルト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

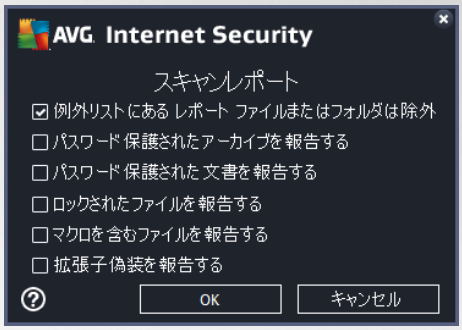
イルは不審であるため、常にスキャンすることをお勧めします。

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。 デフォルトでは、このオプションの値は、自動的にリソースを使用する*ユーザー依存*レベルに設定されています。 スキャンの処理速度を高めた場合、スキャンにかかる時間は短くなりますが、スキャン実行中に使用されるシステム リソースの量は大幅に増え、PC での他の作業の処理速度が低下します (*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 レポートを設定...*] リンクをクリックすると、「*スキャン レポート*」というダイアログウィンドウが開き、報告する検出項目を選択できます:



7.8.2. 特定のファイルとフォルダをスキャン

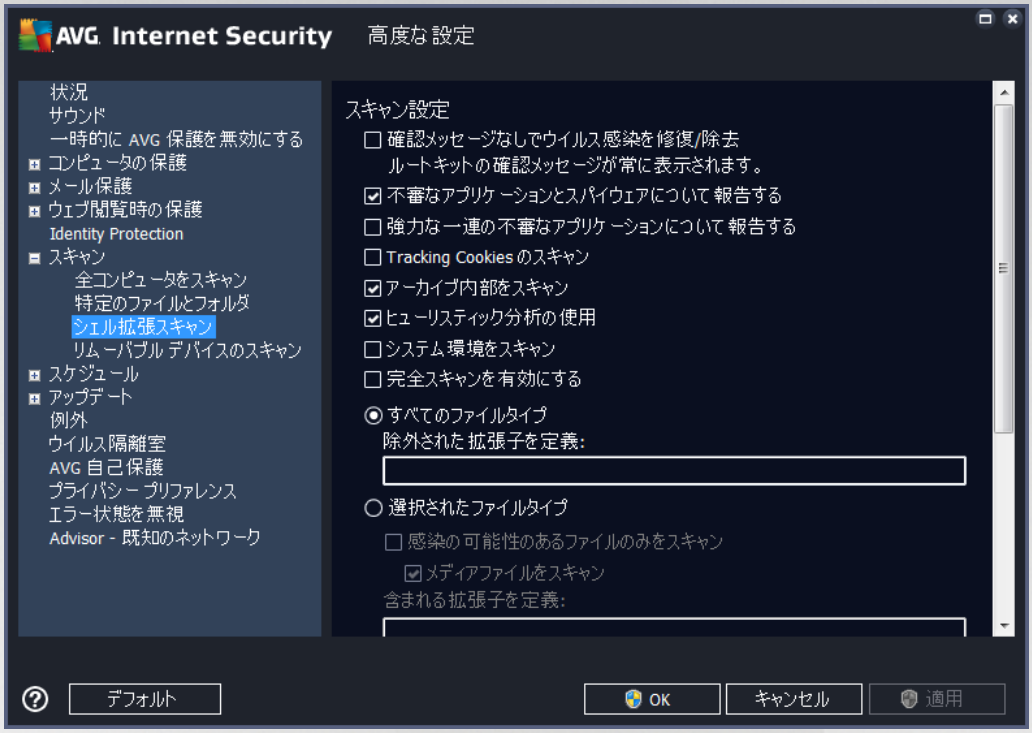
*特定のファイルとフォルダをスキャン*の編集インターフェースは、全コンピュータをスキャンの編集ダイアログとほぼ同じですが、全コンピュータのスキャンのデフォルト設定の方が厳密です:

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

注意: 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」の章を参照してください。

7.8.3. シェル拡張スキャン

前述した「全コンピュータをスキャン」の項目と同様に、「*シェル拡張スキャン*」というこの項目も、ソフトウェア ベンダーがあらかじめ定義したスキャンを編集するための複数のオプションを備えています。 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。



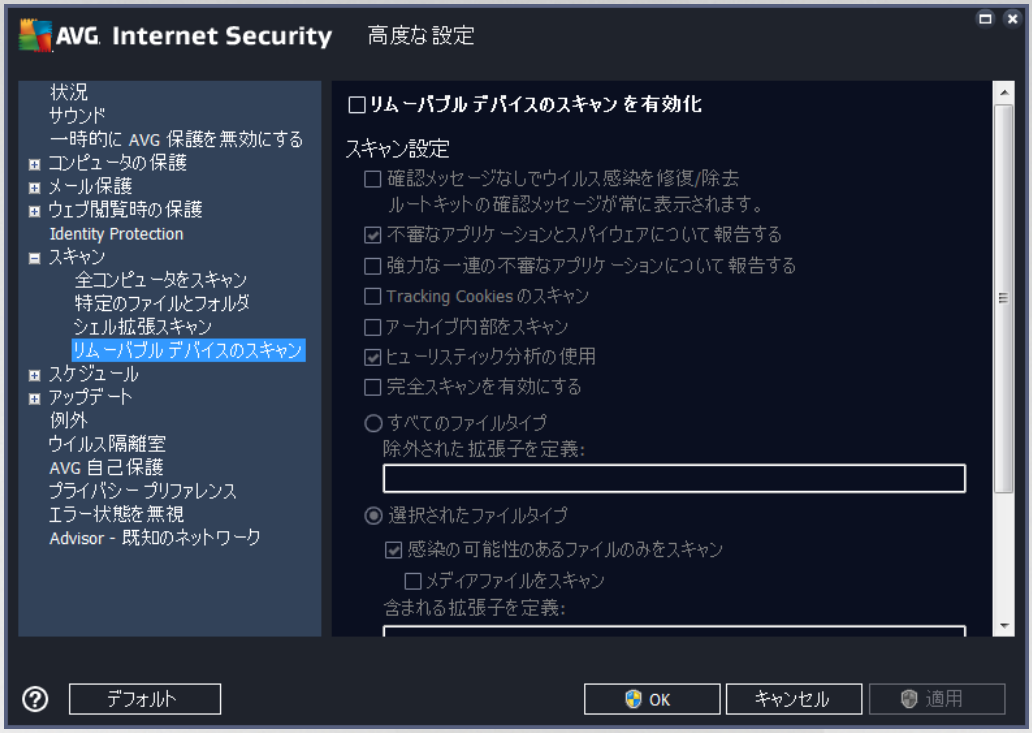
編集オプションは、全コンピュータをスキャンスキャンで利用可能なオプションとほぼ同じですが、デフォルト設定は異なります (*例えば、「全コンピュータをスキャン」の場合、デフォルトではアーカイブをチェックせずにシステム環境をスキャンしますが、「シェル拡張スキャン」では逆になります*)。

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」の章を参照してください。

[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「*スキャンの進度と結果の表示*」というセクションがあり、スキャンの進度と結果を表示するかどうか、および 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どうかを指定できます。 また、スキャンで感染が検出された場合のみスキャン結果を表示するように指定することもできます。

7.8.4. 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。 デフォルトでは、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」の章を参照してください。

7.9. 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

7.9.1. 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 (*すべてのデフォルト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、分かりやすく、適切な名前を使用して、後で他のスキャンと簡単に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、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、適切ではありません。 一方、分かりやすい適切な名前の例としては、「システム領域スキャン」などが挙げられます。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します。

スケジュール実行

ここでは、新しくスケジュールされたスキャンを起動する時間間隔を指定できます。 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。 デフォルトではほとんどのパラメータがオンになっており、その機能はスキャン実行中に適用されます。 *この設定を変更する合理的な理由がない場合は、あらかじめ定義された設定を維持することをお勧めします*:

- *確認メッセージなしでウイルス感染を修復/除去 (デフォルトではオン):* スキャン実行中にウイルスが検出され、修復可能な場合は自動的に修復できます。 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されます。

- *不要と考え得るアプリケーションとスパイウェアの脅威について報告する (デフォルトではオン):* チェックを付けると、スキャンが有効になり、ウイルスに加えてスパイウェアもスキャンされます。 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 リスクとなりますが、このプログラムの一部は意図的にインストールできます。 コンピュータのセキュリティが高まるため、この機能を有効にしておくことをお勧めします。

- *不要と考え得るアプリケーションの拡張セットについて報告する* (*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、製造元から直接入手したときには完全に問題がなく無害ですが、後から悪意のある目的で誤用されるおそれのあるプログラムです。 これは、コンピュータ セキュリティをさらに高めるための追加的な手段ですが、合法的なプログラムもブロックする可能性があるため、デフォルトではオフになっています。

- *Tracking Cookie 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、スキャンで Cookie の検出を行います (*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、維持に使用されます*)。

- *アーカイブ内部をスキャン (デフォルトではオフ)*: このパラメータを指定すると、ファイルが ZIP や RAR などのアーカイブ内に保存されている場合でも、スキャンではすべてのファイルがチェックされます。

- *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 オブジェクトの命令の動的エミュレーション*) は、スキャンの際に使用されるウイルス検出方法の 1 つです。

- *システム環境をスキャン (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領域もチェックされます。

- *完全スキャンを有効にする (デフォルトではオフ)*: 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*) が発生した場合には、このオプションにチェックを付けると、最も完全なスキャン アルゴリズムが有効になり、感染の可能性が低いコンピュータ領域もスキャンされます。これにより、問題がないことが確認できます。 ただし、この方法を実行すると多少時間がかかることにご留意ください。

- *ルートキットをスキャン (デフォルトではオン)*: ルートキット対策スキャンではルートキット、すなわち悪意のある活動をコンピュータ内で隠すことができるプログラムや技術がないかどうか、コンピュータを検索して確認します。 ルートキットが検出されても、必ずしもコンピュータが感染しているわけではありません。 場合によっては、通常のアプリケーションの特定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ます。

スキャンするかどうかを判断する必要もあります

- *すべてのファイルタイプ* このオプションでは、スキャンが不要なファイルの拡張子をコンマで区切ったリスト (*保存後、コンマはセミコロンに変化*) を指定することにより、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低いため、このボックスのチェックを外すと、スキャン時間がさらに短縮されます*) 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を、拡張子を用いて指定できます。

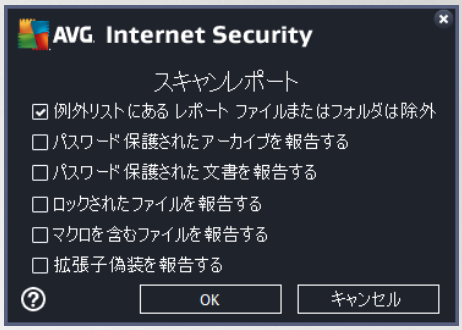
- 任意で*拡張子のないファイルをスキャン*できます。このオプションはデフォルトではオンになっています。変更する理由がない場合は、この設定を保持することをお勧めします。 拡張子のないファイルは不審であるため、常にスキャンすることをお勧めします。

スキャン速度を調整

このセクションでは、システム リソースの使用状況に応じて、希望するスキャン速度を指定することができます。 デフォルトでは、このオプションの値は自動的にリソースを使用する*ユーザー依存*レベルに設定されています。 スキャンの処理速度を高めた場合、スキャンにかかる時間は短くなりますが、スキャン実行中に使用されるシステム リソースの量は大幅に増え、PC での他の作業の処理速度が低下します (*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 レポートを設定...*] リンクをクリックすると、「*スキャン レポート*」というダイアログ ウィンドウが開き、報告する検出項目を選択できます:



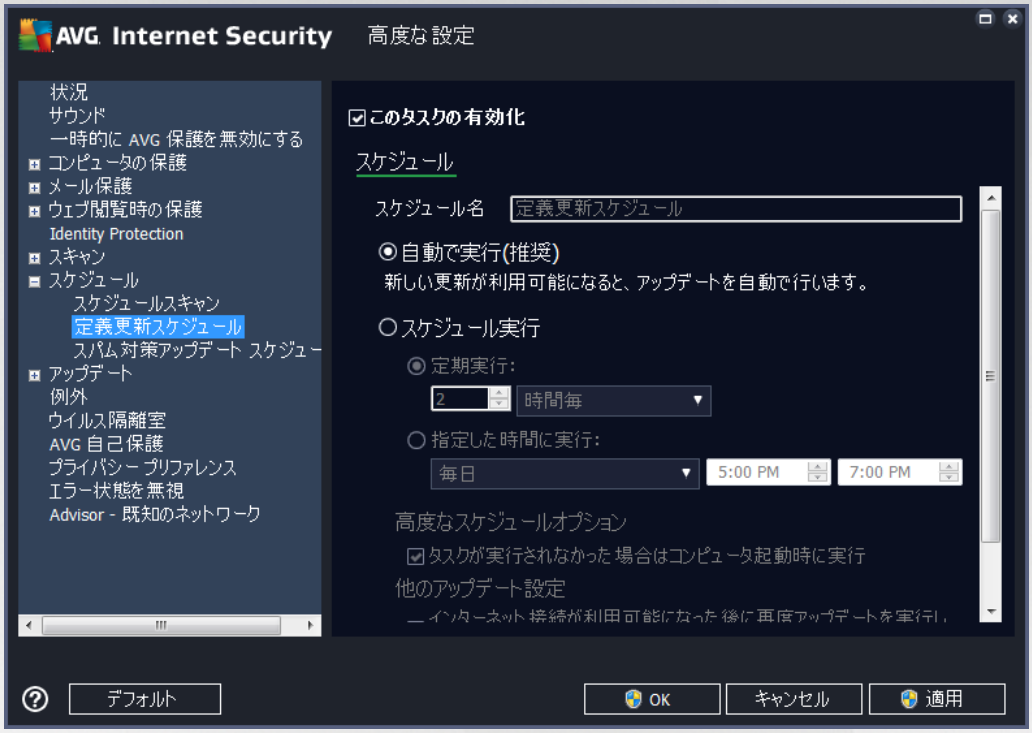
コンピュータ シャットダウン オプション

[*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をスキャン] 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スキャンを選択した場合、ダイアログ下部のツリービューで対象フォルダを指定することができます。

7.9.2. 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（*すべてのデフォルト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*）。

7.9.3. 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)。*

7.10. 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 (デフォルト)* - 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 (デフォルトではオン)* - 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 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。

7.10.1. 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。両方の可能性が同時に可能です。 次に、*アップデート設定 - プロキシ*ダイアログの最初のアイテムで、コンボボックス メニューから希望するものを選択する必要があります。

- *プロキシを使用しない* - 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。

7.10.2. 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を削除* - 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。*)

7.11. 例外

[*例外*] ダイアログでは、例外、すなわち AVG Internet Security によって無視される項目を定義できます。通常、AVG が同じプログラムやファイルを脅威として検出し続けたり、安全なウェブサイトを危険とみなしてブロックし続けたりする場合、例外を定義する必要があります。 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。

すでに例外が定義されている場合、ダイアログの表に例外の一覧が表示されます。 各項目の横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、その例外は有効です。選択解除されている場合、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、オブジェクトがアプリケーションまたはファイル、フォルダ、URL、証明書のうちどのタイプであるかを定義します。 次に、ディスクを参照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 の機能を選択できます *(常駐シールド、Identity Protection、スキャン)*。

- *編集* - このボタンは、すでに例外が定義されており、表に表示されている場合のみ有効です。 その場合、このボタンを使用して、選択した例外の編集ダイアログを開き、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取り消すことができます。 個別に削除することも、一覧で例外をまとめてハイライトし、定義した例外を一括して取り消すこともできます。 例外を取り消すと、該当するファイル、フォルダ、URL が再び AVG でスキャンされるようになります。 ファイルまたはフォルダ自体ではなく、例外のみが削除されることにご留意ください。

- *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。

7.12. 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。

7.13. AVG 自己保護

*AVG 自己保護*は、AVG Internet Security 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保護し、改ざんや無効化を防ぎます。 この種の保護を行う主な理由は、一部の巧妙な脅威がウイルス対策の解除を試みて、コンピュータに無制限に被害をもたらさないようにするためです。

この機能を有効にしておくことをお勧めします。

7.14. プライバシー設定

[*プライバシー設定*] 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 (デフォルトではオン)* - AVG Internet Security 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 (デフォルトではオン)* - 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 (デフォルトではオン)* - 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 (デフォルトではオン)* - 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。

7.15. 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。

デフォルト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四色で表示されますが、エラーが発生すると、黄色のエクスクラメーションマークのついたアイコンが表示されます。

- AVG メイン ウィンドウの [セキュリティステータス情報] セクション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。

7.16. 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ことを推奨します。 新しいネットワークへの接続が安全であるとユーザーが判断した場合は、このリストに保存することもできます *(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にスライド表示され、そこにリンクが表示されます。 詳細については、AVG Advisor に関する章を参照してください)*。 リストに保存すると、AVG Advisor はその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。 ユーザーが接続する各ネットワークは自動的に既知のネットワークとみなされ、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。削除すると、そのネットワークは、再び不明で危険である可能性があるとみなされます。

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。

8. 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

8.1. 一般

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、ソフトウェアの製造元はすべての AVG Internet Security 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。 設定変更は上級ユーザーが行うことをお勧めします。

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推奨されます。*

- *インタラクティブ* - 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、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 ID 保

護 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。

8.2. 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。 以下のアクションの種類が使用できます。

- - 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

すで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。 デフォルトトでは、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、あるいは通信を許可またはブロックするかをユーザーに尋ねます。 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、直ち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ます。このダイアログで [*追加*] をクリックし、アプリケーション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に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など、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通信を試みた場合に実行す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ユーザーが決定できます)*。 *これらの項目には一般のアプリケーションとは異なる設定オプションがあるため、上級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。

8.3. 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、すで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。

8.4. 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通信の試行 *(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 ファイルの変更が行われると、ファイアウォールは信頼できるアプリケーションのデータベースを参照して証明書を検証するという標準的な方法で、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だと考えられない場合、ファイアウォールは選択されているモードに基づいてアプリケーションにさらに対処します。
  - ファイアウォールが *自動モード* で動作している場合、アプリケーションはデフォルトにより許可されます。
  - 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処理する方法を決定するようユーザーに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手順は、[アプリケーション] ダイアログで各アプリケーションについて個別に定義できます。

8.5. 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、すで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。

8.6. 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。
    - すべてのネットワークの通信を許可
    - 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。

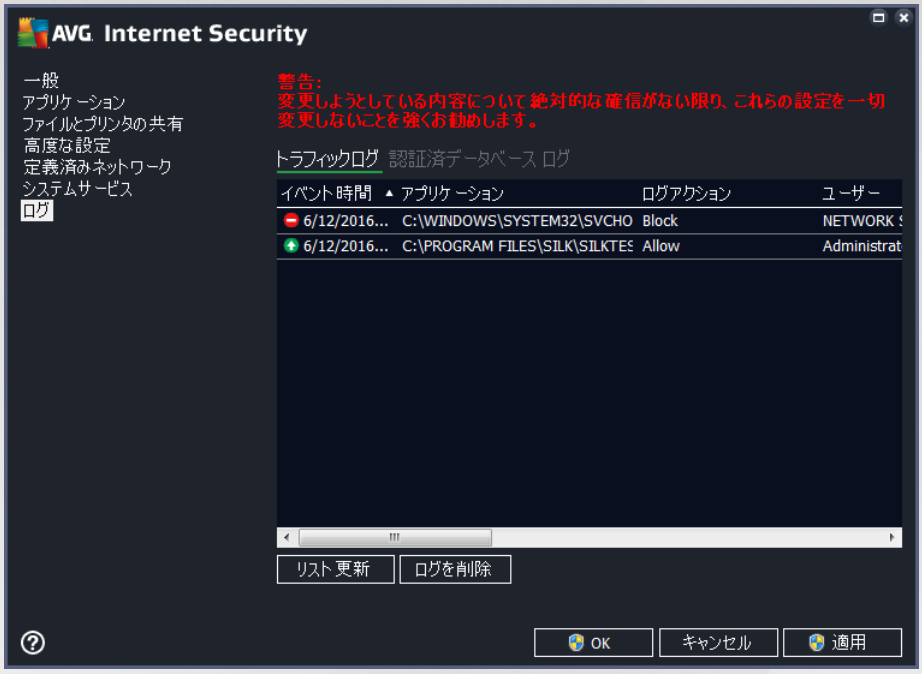
詳細ルール設定は高度な設定であり、主としてファイアウォール設定を完全に制御する必要のあるネットワーク管理者を対象としています。 通信プロトコル、ネットワーク ポート番号、IP アドレス定義などについての知識がない場合は、この設定を変更しないでください。 設定を変更する必要がある場合は、詳細について、各ダイアログ ヘルプ ファイルを参照してください。

8.7. ログ

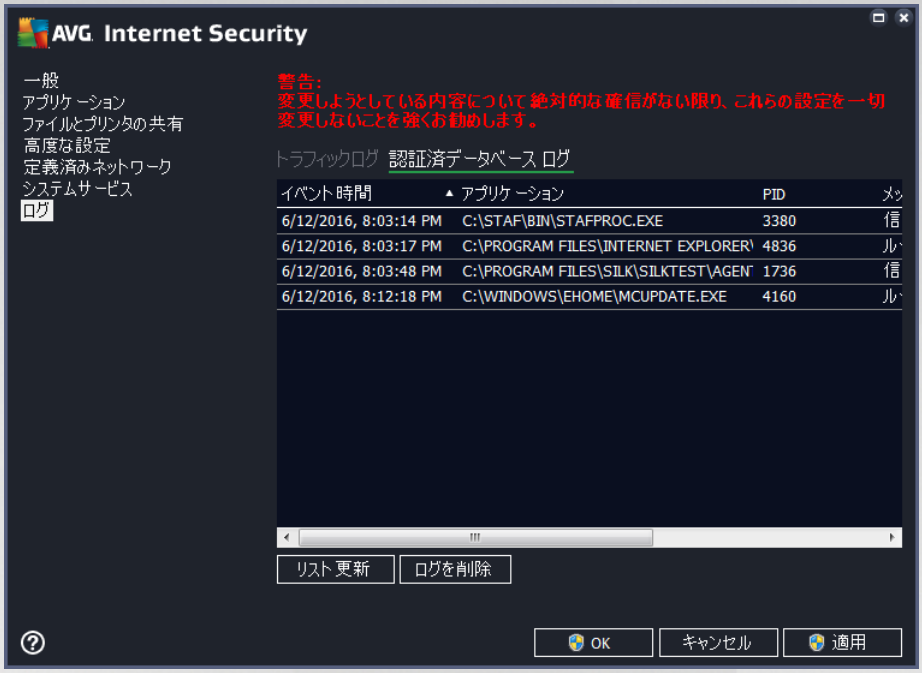
ログ ダイアログ内の編集は、すべて経験のあるユーザーのみを対象としています。

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。



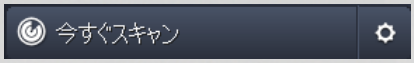
コントロール ボタン

- *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。

9. AVG スキャン

デフォルトでは、AVG Internet Security はスキャンを実行しません。初回のスキャン *(実行するよう指示されます)* の後、常に監視状態にある AVG Internet Security 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。 もちろん、一定の間隔で実行されるようにスキャンのスケジュールを設定し、または必要に応じて適宜スキャンを手動で起動することも可能です。

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直ちに起動し、[レポート] ウィンドウが自動的に開いて進行状況と結果を確認できます。

- *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、スケジュールされた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を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:

- *スケジュールされたスキャンを管理* - このオプションををクリックすると、すべてのスキャン スケジュールの概要が表示されたダイアログが新たに開きれます。 スキャンを個別に定義する前に、一覧に表示された、ソフトウエア 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オフになっています。 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 [*タスクを有効にする*] オプションを選択します。 スケジュール スキャンが有効化されると、[スキャン スケジュールを編集] ボタンを使って *設定を編集*することができます。 [*スキャン スケジュールを追加*] 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います。 [*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、コンピュータ全体のスキャンが直ちに開始されます *(コンピュータ全体の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」という章をそれぞれ参照してください)*。 [*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をスキャン / 設定* - このボタンも 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をスキャン*] 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が直ちに開始されます *(選択したファイルまたは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スキャン」という章をそれぞれ参照してください)*。 [*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をスキャン」の設定ダイアログに移動します。

- *コンピュータ内をルートキット スキャン / 設定* - *コンピュータ内をルートキット スキャン* というラベルの付いたボタンの左側の部分は、ルートキット対策スキャンが直ちに開始されます *(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 / コンピュータ内をルートキット スキャン」という章をそれぞれ参照してください)*。 [*設定*] セクションをクリックすると、ルートキット スキャンの設定ダイアログに移動します。

9.1. 定義済みスキャン

AVG Internet Securityのメイン機能の1つはオンデマンドのスキャンです。 オンデマンドのスキャンは、ウイルス感染の疑いがある場合、コンピュータの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 では、次の種類のソフトウェアベンダーによってあらかじめ定義されたスキャンが表示されます。

9.1.1. コンピュータ全体のスキャン

*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、感染や不要と考え得るアプリケーションがあるかどうか確認します。 このスキャンではコンピュータのすべてのハード ドライブがスキャンされ、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。 このタイプのスキャンについては、さらに特別な設定を行う必要はありません。スキャンは直ちに開始されます。 *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 - 設定*]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)。 デフォルトの設定を保持し、合理的な理由がある場合のみ変更することをお勧めします。

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 (デフォルトではオン)*: 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されます。

- *不要と考え得るアプリケーションとスパイウェアの脅威を報告する (デフォルトではオン)* チェックを付けると、ウイルスに加えてスパイウェアのスキャンも有効になります。 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 リスクとなりますが、このプログラムの一部は意図的にインストールできます。 コンピュータのセキュリティが高まるため、この機能を有効にしておくことをお勧めします。

- *不要と考え得るアプリケーション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、製造元から直接入手したときには完全に問題がなく無害ですが、後から悪意のある目的で誤用されるおそれのあるプログラムです。 これは、コンピュータ セキュリティをさらに高めるための追加的な手段ですが、合法的なプログラムもブロックする可能性があるため、デフォルトではオフになっています。

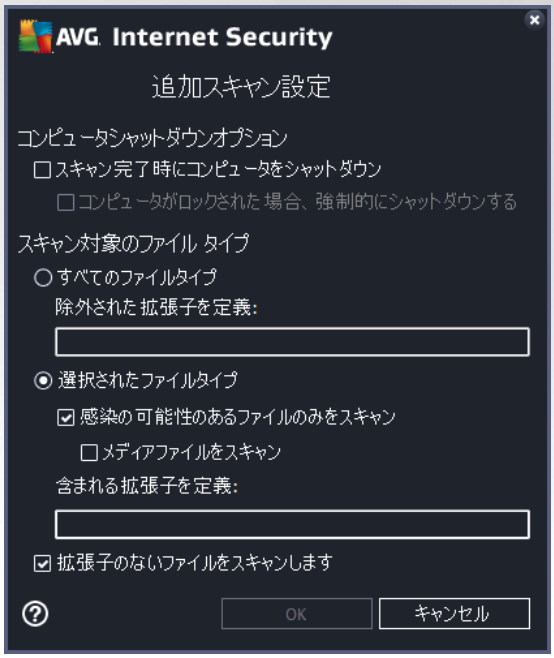
- *Tracking Cookie のスキャン (デフォルトではオフ)* - このパラメータは、Cookie を検出するか否かを指定します *(HTTP Cookie は、サイトのプリファレンスや電子ショッピング カートの内容など、ユーザーに関する特定の情報の認証、追跡、維持に使用されます)*。

- *アーカイブ内部をスキャン (デフォルトではオフ)* - このパラメータを指定すると、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がスキャンされます。

- *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 オブジェクトの命令の動的エミュレーション)*は、スキャン中に使用されるウイルス検出方法の 1 つです。

- *システム環境をスキャン (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領域もチェックされます。
- *完全スキャンを有効にする (デフォルトではオフ)* - 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)* が発生した場合には、このオプションにチェックを付けると、最も完全なスキャンアルゴリズムが有効になり、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されます。これにより、問題がないことが確認できます。 ただし、この方法を実行すると多少時間がかかることにご留意ください。
- *ルートキットのスキャン (デフォルトではオン)*: コンピュータ全体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を別に実行することもできます。
- *追加スキャン設定* - このリンクをクリックすると、新しい [追加スキャン設定] ダイアログが開き、以下のパラメータを指定できます:



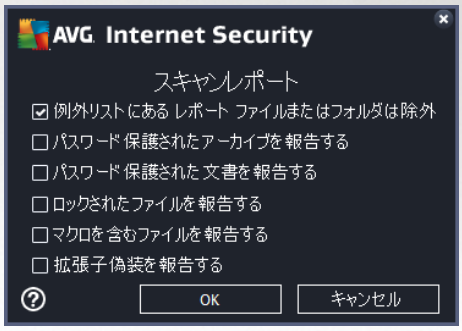
  - *コンピュータのシャットダウン オプション* - 実行中のスキャン プロセスが終了したら自動的にコンピュータをシャットダウンするかどうかを決定します。 このオプション (*スキャン完了時にコンピュータをシャットダウン*) を選択すると、現時点でコンピュータがロックされている場合でも、コンピュータをシャットダウンさせる新しいオプション (*コンピュータがロックされた場合、強制的にシャットダウンする*) が有効になります。
  - *スキャンのファイル タイプ* - 以下のスキャン設定も決定する必要があります:
    - *すべてのファイル タイプ* このオプションでは、スキャンが不要なファイルの拡張子をコンマで区切ったリストを指定することにより、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低いため、このボックスのチェックを外すと、スキャン時間がさらに短縮されます*) 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を、拡張子を用いて指定できます。

➢ 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。このオプションはデフォルト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* - スライダーを使用して、スキャン処理の優先度を変更できます。デフォルトでは、このオプションの値は自動的にリソースを使用する*ユーザー依存*レベルに設定されています。 あるいは、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したり (*コンピュータで作業を続ける必要があり、スキャンに時間がかかってもよい場合に便利です*)、システム リソース消費量の多い高速スキャン (*コンピュータが一時的に使用されていない場合などに便利です*) を実行したりできます。

- *追加スキャン レポートを設定* - このリンクをクリックすると、新しい [*スキャン レポート*] ダイアログが開き、報告するスキャン結果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」の章で説明されています。 全コンピュータをスキャンのデフォルト設定を変更することを決定した場合は、新しい設定をデフォルト設定として保存し、その後のすべてのコンピュータ全体のスキャンに使用できます。

9.1.2. 特定のファイルとフォルダをスキャン

特定のファイルとフォルダをスキャン - コンピュータの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、コンピュータ全体のスキャンを実行する場合と同じです。検出されたウイルスは修復されるか、ウイルス隔離室に移されます。 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をスキャン*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をスキャン] ボタンをクリックして直接起動できます。 [*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。 コンピュータのツリー構成内でスキャンするフォルダを選択します。 選択した各フォルダへ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、特定のフォルダを、すべてのサブフォルダを除外してスキャンするオプションもあります。 これを行うには、自動生成されたパスの前にマイナス記号「-」を入力します (*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*の設定は、[*特定のファイルとフォルダをスキャン - 設定*] ダイアログで編集できます *(このダイアログは [スキャン オプション] ダイアログにある特定のファイルとフォルダをスキャンするための設定リンクからアクセスできます)。 デフォルトの設定を保持し、合理的な理由がある場合のみ変更することをお勧めします。*

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。

- *確認メッセージなしでウイルス感染を修復/除去 (デフォルトではオン)*: スキャン実行中にウイルスが検出され、修復可能な場合は自動的に修復できます。 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されます。

- *不要と考え得るアプリケーションとスパイウェアの脅威について報告する (デフォルトではオン)*: チェックを付けると、スキャンが有効になり、ウイルスに加えてスパイウェアもスキャンされます。 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 リスクとなりますが、このプログラムの一部は意図的にインストールできます。 コンピュータのセキュリティが高まるため、この機能を有効にしておくことをお勧めします。

- *不要と考え得るアプリケーションの拡張セットについて報告する (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、製造元から直接入手したときには完全に問題がなく無害ですが、後から悪意のある目的で誤用されるおそれのあるプログラムです。 これは、コンピュータ セキュリティをさらに高めるための追加的な手段ですが、合法的なプログラムもブロックする可能性があるため、デフォルトではオフになっています。

- *Tracking Cookie のスキャン (デフォルトではオフ)*: 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)*。

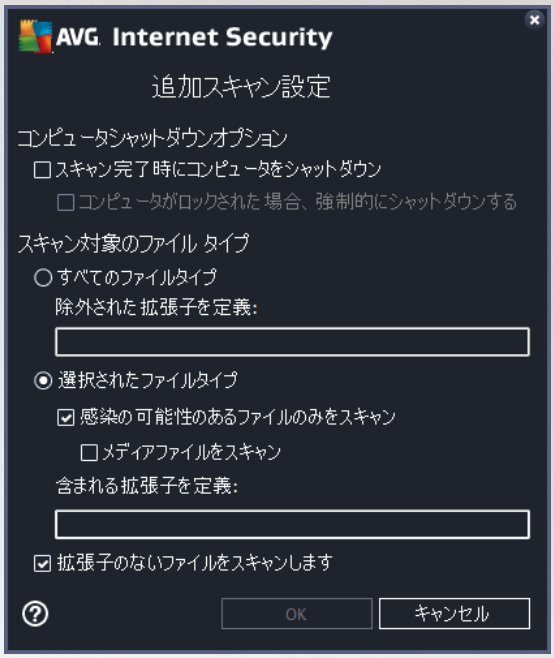
- *アーカイブ内部をスキャン (デフォルトではオン)*: このパラメータは、ZIP や RAR などのアーカイブ内に格納されているすべてのファイルをスキャンでチェックすることを指定します。

- *ヒューリスティック分析を使用 (デフォルトではオン)*: ヒューリスティック分析 *(仮想コンピュータ環境でのスキャン オブジェクトの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 (デフォルトではオフ)*: スキャンでは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 (デフォルトではオフ)*: 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)* が発生した場合には、このオプションにチェックを付けて、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することができます。これにより、問題がないことが確認できます。 ただし、この方法を実行すると多少時間がかかることにご留意ください。

- *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、以下のパラメータを指定できます:



  - *コンピュータのシャットダウン オプション* - 実行中のスキャン プロセスが終了したら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* - 以下のスキャン設定も決定する必要があります:

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

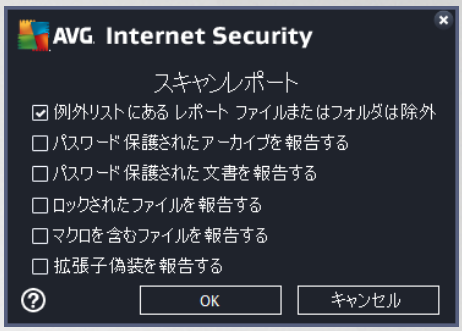
    - *選択されたファイルタイプ* - 感染の可能性のあるファイルのみをスキャンするよう指定できます (*一部のプレーン テキスト ファイルやその他の非実行可能ファイルなど、感染の可能性がないファイルはスキャンされません*)。これには、メディア ファイル (*ビデオ、オーディオ ファイル - 多くの場合、これらのファイルはサイズが非常に大きく、ウイルスに感染している可能性が低いため、このボックスのチェックを外すと、スキャン時間がさらに短縮されます*) が含まれます。 ここでも、必ずスキャンする必要があるファイルを、拡張子を用いて指定できます。

    - 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。このオプションはデ

フォルト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* - スライダーを使用して、スキャン処理の優先度を変更できます。 デフォルトでは、このオプションの値は自動的にリソースを使用する*ユーザー依存*レベルに設定されています。 あるいは、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したり (*コンピュータで作業を続ける必要があり、スキャンに時間がかかってもよい場合に便利です*)、システム リソース消費量の多い高速スキャン (*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 レポートを設定する* - 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、報告する検出結果の種類を選択できます:



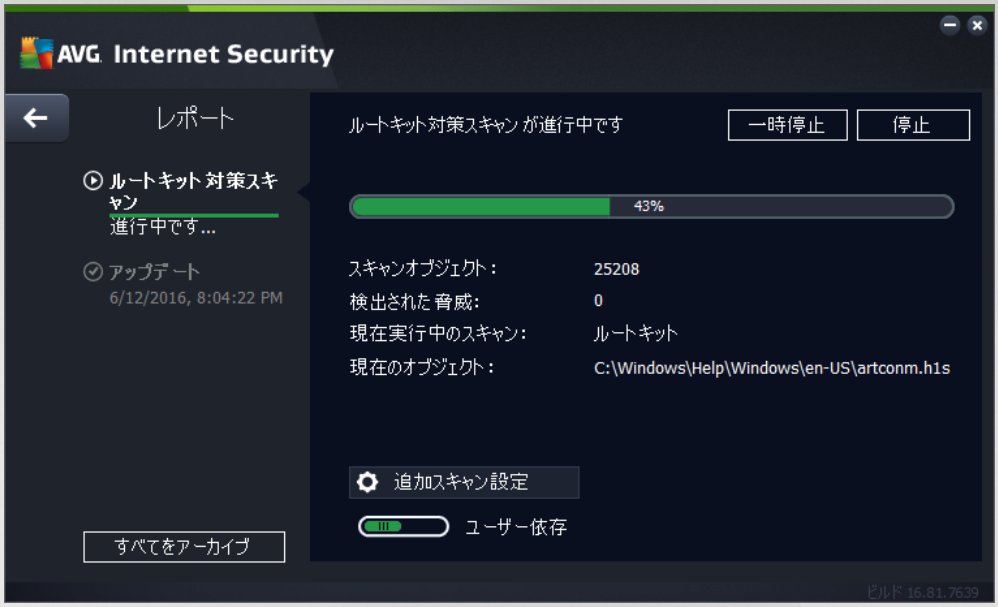
警告: これらのスキャン設定は、新規に定義するスキャンのパラメータと同一です。これは「AVG スキャン / スキャン スケジュール/ スキャン方法」の章で説明されています。 特定のファイルとフォルダをスキャンのデフォルトの設定を変更した場合は、新しい設定をデフォルトの設定として保存し、その後で実行する特定のファイルまたはフォルダのスキャンに使用することができます。 また、この設定はすべての新規スケジュールスキャンのテンプレートとして使用されます (すべてのカスタマイズ スキャンは、選択したファイルまたはフォルダのスキャンの現在の設定に基づいて実行されます)。

9.1.3. 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、*コンピュータ内の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)。* ***デフォルトの設定を保持し、合理的な理由がある場合のみ変更することをお勧めします。***

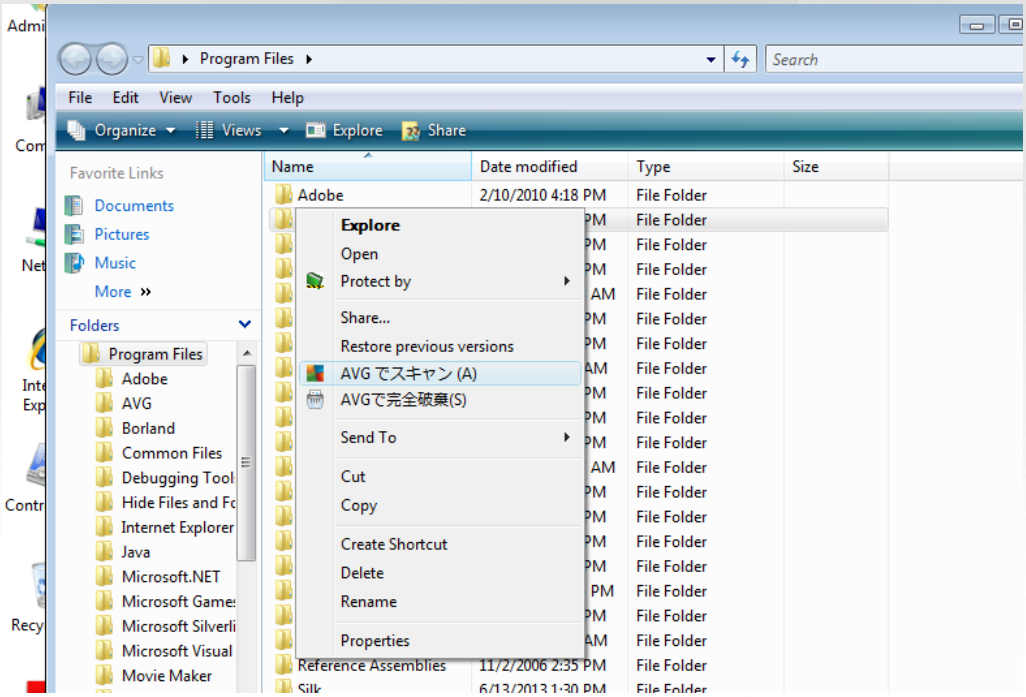
*アプリケーションスキャンと ドライバスキャン*では、ルートキット対策スキャンの対象を詳細に指定でき

ます。 これらの設定は上級ユーザー向けです。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

9.2. Windows エクスプローラのスキャン

AVG Internet Security 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

9.3. コマンド ライン スキャン

AVG Internet Securityには、コマンドラインからスキャンを実行するオプションがあります。 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

9.3.1. コマンドの構文

コマンドの構文は次のとおりです。

- *avgscanx /parameter* ... たとえば、コンピュータ全体のスキャンの場合 *avgscanx /comp*
- *avgscanx /parameter /parameter* .. 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:*

9.3.2. スキャン パラメータ

利用可能なパラメータの概要をすべて表示するには、パラメータ /? または /HELP を付加して該当するコマンドを入力します (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。

9.3.3. 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。

セーフ モードでは、コマンドラインからスキャンを実行します。 このダイアログでは、安定したグラフィック インターフェースでスキャン パラメータを指定できます。

まず、スキャン対象のコンピュータの領域を選択します。 定義済みの*全コンピュータをスキャン*、または*選択されたフォルダまたはファイルをスキャン*オプションを決定することができます。 3 つ目のオプションである *クイック スキャン*は、セーフモードで使用するための特定のスキャンを起動します。このスキャンは、起動に必要なコンピュータの重要部分をすべて検査します。

次のセクションのスキャン設定では、詳細なスキャン パラメータを指定できます。 デフォルトではすべてチェックされています。特別な理由がある場合に限り、パラメータのチェックを外してください。

- *「不要と考えられるアプリケーション」をスキャンする* - スパイウェアを (一般的なウイルスに加えて) スキャンします
- *Alternate Data Streams (NTFS のみ) をスキャン* - NTFS Alternate Data Streams のスキャンは Windows の機能であり、ハッカーによって、 データ、特に悪意のあるコードを隠したりするために悪用されます
- *ウイルス感染を自動的に修復 / 除去する* - 検出した感染にすべて対処し、自動的に修復またはコンピュータから除去します
- *アクティブなプロセスをスキャンする* - コンピュータ メモリにロードされているプロセスとアプリケーションをスキャンします
- *レジストリをスキャンする* - Windows レジストリをスキャンします
- *マスター ブート レコード チェックを有効にする* - パーティション テーブルとブート セクタを

スキャンします

最後に、ダイアログの下部でスキャン レポートのファイル名と種類を設定できます。

9.3.4. 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。

- /? このトピックに関するヘルプを表示
- /@ コマンド ファイル/ファイル名/
- /ADS Alternate Data Stream をスキャン *(NTFSのみ)*
- /ARC アーカイブをスキャン
- /ARCBOMBSW 再圧縮されたアーカイブ ファイルを報告
- /ARCBOMBSW アーカイブ ボムを報告する *(繰り返し圧縮されたアーカイブ)*
- /BOOT MBR/ブート チェックを有効にする
- /BOOTPATH QuickScan を起動
- /CLEAN 自動的にクリーンアップ
- /CLOUDCHECK 誤検出を確認
- /COMP 全コンピュータをスキャン
- /COO Cookie をスキャン
- /EXCLUDE スキャンからパスまたはファイルを除外
- /EXT 指定した拡張子のファイルをスキャン *(例： EXT=EXE,DLL)*
- /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する
- /HELP このトピックに関するヘルプを表示
- /HEUR ヒューリスティック分析を使用
- /HIDDEN 拡張子を偽装したファイルを報告する
- /IGNLOCKED ロックされたファイルを無視
- /INFECTABLEONLY 感染の可能性がある拡張子を持つファイルのみスキャンする
- /LOG スキャン結果ファイルを生成

- /MACROW　マクロを報告する
- /NOBREAK　CTRL-BREAK キーでの中断を許可しない
- /NOEXT　これらの拡張子をスキャンしない *(例: NOEXT=JPG)*
- /PRIORITY　*スキャン優先度* (低、自動、高) を設定する (「*高度な設定 / スキャン*」*を参照)*
- /PROC　アクティブなプロセスをスキャン
- /PUP　不要と考え得るアプリケーションを報告する
- /PUPEXT　不要と考え得るアプリケーションの拡張セットを報告する
- /PWDW　パスワード保護されたファイルを報告する
- /QT　クイック テスト
- /REG　レジストリをスキャン
- /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
- /REPORT　ファイルにレポート *(ファイル名)*
- /SCAN　特定のファイルまたはフォルダをスキャン *(SCAN=path;path) (例 : /SCAN=C:\;D:\)*
- /SHUTDOWN　スキャン完了時にコンピュータをシャットダウン
- /THOROUGHSCAN　完全スキャンを有効にする
- /TRASH　感染ファイルをウイルス隔離室に移動

9.4. スキャンスケジュール

AVG Internet Security 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。 全コンピュータをスキャンを週に 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、全コンピュータのスキャンを毎日行ってください。デフォルトのスキャンスケジュールはこのように設定されています。 コンピュータが常にオンとなっている場合、作業時間外にスキャンを実行するよう設定することができます。 コンピュータがオフにな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 [*スケジュールされたスキャン*

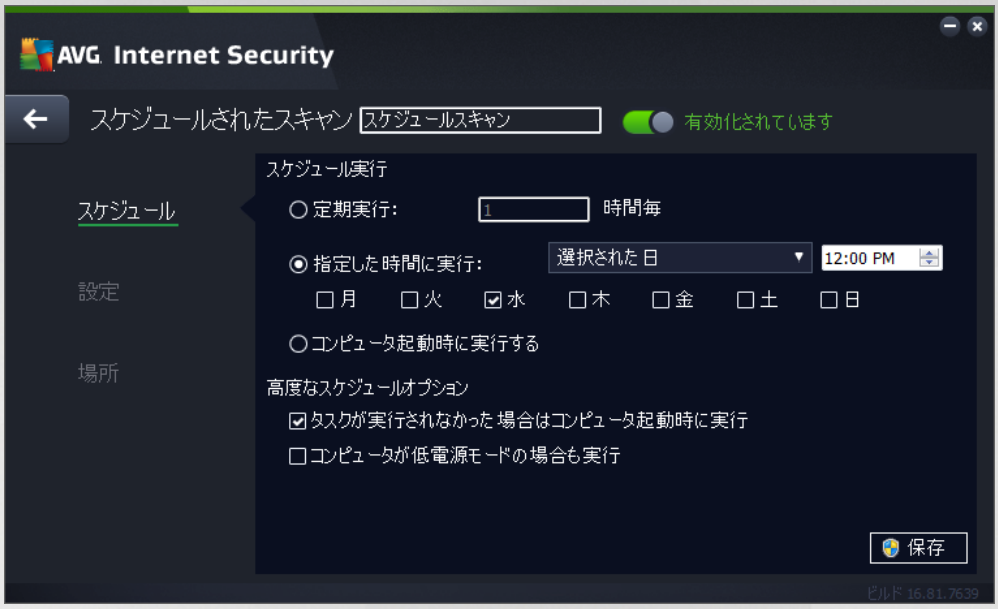
を管理] ボタンからアクセスできます。ここではスキャンのスケジュールを作成または編集できます。 新しい *スケジュールスキャン*ダイアログが開き、現在スケジュールされているすべてのスキャンの完全な概要が表示されます。

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。 *スケジュール追加*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「交通信号」ボタン  を [スケジュール スキャンを一時的に無効にする] に切り替えます。必要に応じて、もう一度このボタンをオンにします。

9.4.1. 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、分かりやすく、適切な名前を使用して、後で他のスキャンと簡単に区別できるようにしてください。 例えば、「新規スキャン」あるいは「マイスキャン」という名前は、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、適切ではありません。一方、分かりやすい適切な名前の例としては、「システム領域スキャン」などが挙げられます。

このダイアログでは、さらに以下のスキャンパラメータを定義します。

- *スケジュール実行* - ここでは、新しくスケジュールされたスキャンを起動する時間間隔を指定できます。 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。

ダイアログ内のコントロール

- *保存* - このタブまたはこのダイアログ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の概要に戻ります。 このため、すべてのタブで検査パラメータを設定する場合は、必要な項目をすべて指定した後でこのボタンを押して保存してください。

- ← - 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の概要に

戻ります。

9.4.2. 設定

ダイアログの上部にある [*設定*] タブには、現在設定を行っ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、分かりやすく、適切な名前を使用して、後で他のスキャンと簡単に区別できるようにしてください。 例えば、「新規スキャン」あるいは「マイ スキャン」という名前は、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、適切ではありません。 一方、分かりやすい適切な名前の例としては、「システム領域スキャン」などが挙げられます。

[*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。 ***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お勧めします***:

- *確認メッセージなしでウイルス感染を修復/除去 (デフォルトではオン):* スキャン実行中にウイルスが検出され、修復可能な場合は自動的に修復できます。 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されます。

- *不要と考え得るアプリケーションとスパイウェアの脅威について報告する (デフォルトではオン):* チェックを付けると、スキャンが有効になり、ウイルスに加えてスパイウェアもスキャンされます。 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 リスクとなりますが、このプログラムの一部は意図的にインストールできます。 コンピュータのセキュリティが高まるため、この機能を有効にしておくことをお勧めします。

- *不要と考え得るアプリケーションの拡張セットについて報告する* (*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、製造元から直接入手したときには完全に問題がなく無害ですが、後から悪意のある目的で誤用されるおそれのあるプログラムです。 これは、コンピュータ セキュリティをさらに高めるための追加的な手段ですが、合法的なプログラムもブロックする可能性があるため、デフォルトではオフになっています。

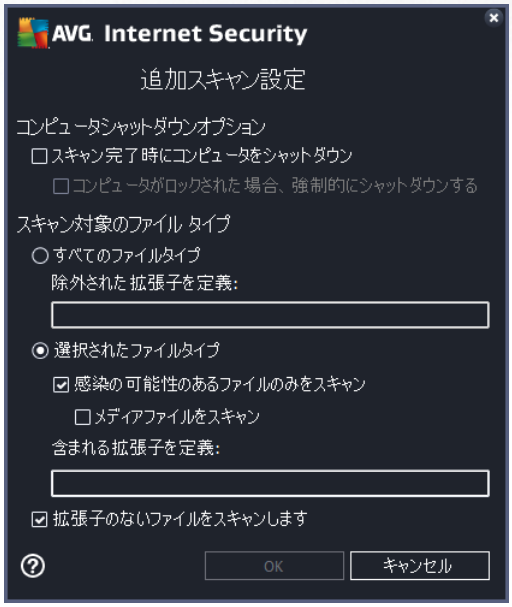
- *Tracking Cookie のスキャン* (*デフォルトではオフ*): このパラメータを指定すると、スキャンで Cookie の検出を行います (*HTTP Cookie は、サイトの設定や電子ショッピング カートの内容など*、

ユーザー固有の情報の認証、追跡、維持に使用されます)。

- *アーカイブ内部をスキャン* (*デフォルトではオフ*): このパラメータを指定すると、ファイルが ZIP や RAR などのアーカイブ内に保存されている場合でも、スキャンではすべてのファイルがチェックされます。
- *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 オブジェクトの命令の動的エミュレーション*) は、スキャンの際に使用されるウイルス検出方法の 1 つです。
- *システム環境をスキャン* (*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領域もチェックされます。
- *完全スキャンを有効にする* (*デフォルトではオフ*): 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*) が発生した場合には、このオプションにチェックを付けると、最も完全なスキャン アルゴリズムが有効になり、感染の可能性が低いコンピュータ領域もスキャンされます。これにより、問題がないことが確認できます。 ただし、この方法を実行すると多少時間がかかることにご留意ください。
- *ルートキットをスキャン (デフォルトではオン):* ルートキット対策スキャンではルートキット、すなわち悪意のある活動をコンピュータ内で隠すことができるプログラムや技術がないかどうか、コンピュータを検索して確認します。 ルートキットが検出されても、必ずしもコンピュータが感染しているわけではありません。 場合によっては、通常のアプリケーションの特定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 プロセスが終了したら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* - 以下のスキャン設定も決定する必要があります:

    - *すべてのファイル タイプ* このオプションでは、スキャンが不要なファイルの拡張子をコンマで区切ったリストを指定することにより、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低いため、このボックスのチェックを外すと、スキャン時間がさらに短縮されます*) 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を、拡張子を用いて指定できます。

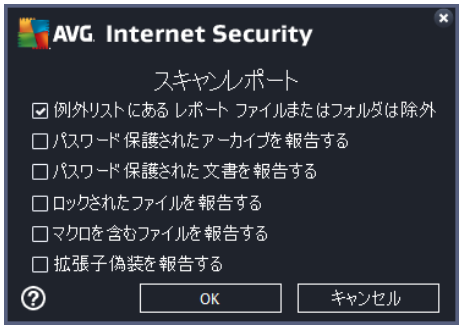
    - 任意で*拡張子のないファイルをスキャン*できます。このオプションはデフォルトではオンになっています。変更する理由がない場合は、この設定を保持することをお勧めします。 拡張子のないファイルは不審であるため、常にスキャンすることをお勧めします。

スキャン速度を調整

このセクションでは、システム リソースの使用状況に応じて、希望するスキャン速度を指定することができます。 デフォルトでは、このオプションの値は自動的にリソースを使用する*ユーザー依存*レベルに設定されています。 スキャンの処理速度を高めた場合、スキャンにかかる時間は短くなりますが、スキャン実行中に使用されるシステム リソースの量は大幅に増え、PC での他の作業の処理速度が低下します (*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 レポートを設定...*] リンクをクリックすると、「*スキャン レポート*」というダイアログ ウィンドウが開き、報告する検出項目を選択できます:



ダイアログ内のコントロール

- *保存* - このタブまたはこのダイアログ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の概要に戻ります。 このため、すべてのタブで検査パラメータを設定する場合は、必要な項目をすべて指定した後でこのボタンを押して保存してください。
- ← - 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の概要に戻ります。

9.4.3. 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をスキャン] 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 および Settings\Default User\My Documents\
    - *Windows Vista/7*: C:\Users\user\Documents\
- *共有ドキュメント*
    - *Win XP*: C:\Documents および 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 および Settings\User\Local\ (*Windows XP*) または C:\Users\user\AppData\Local\Temp\ (*Windows Vista/7*)
    - *一時インターネット ファイル* - C:\Documents および Settings\User\Local Settings\Temporary Internet Files\ (*Windows XP*) または C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (*Windows Vista/7*)

ダイアログ内のコントロール

- *保存* - このタブまたはこのダイアログ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の概要に戻ります。 このため、すべてのタブで検査パラメータを設定する場合は、必要な項目をすべて指定した後でこのボタンを押して保存してください。
- ← - 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の概要に戻ります。

9.5. 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。

ダイアログでの操作

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。

9.6. スキャン結果の詳細

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リダイレクトされます。 情報は 3 つのタブに分けられています:

- *概要* - このタブにはスキャンに関する基本情報が表示されます: スキャンが正常に完了したかどうか、脅威が見つかったかどうか、および脅威をどう処理したかです。
- *詳細* - このタブには、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が表示されます。概要をファイルに エクスポートすると、.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のみ表示され、その脅威に関する詳細情報が提示されます。

  低い危険性: 情報または警告で、実際の脅威ではありません。 通常はマクロを含む文書、パスワードで保護された文書またはアーカイブ、ロックされたファイルなどです。

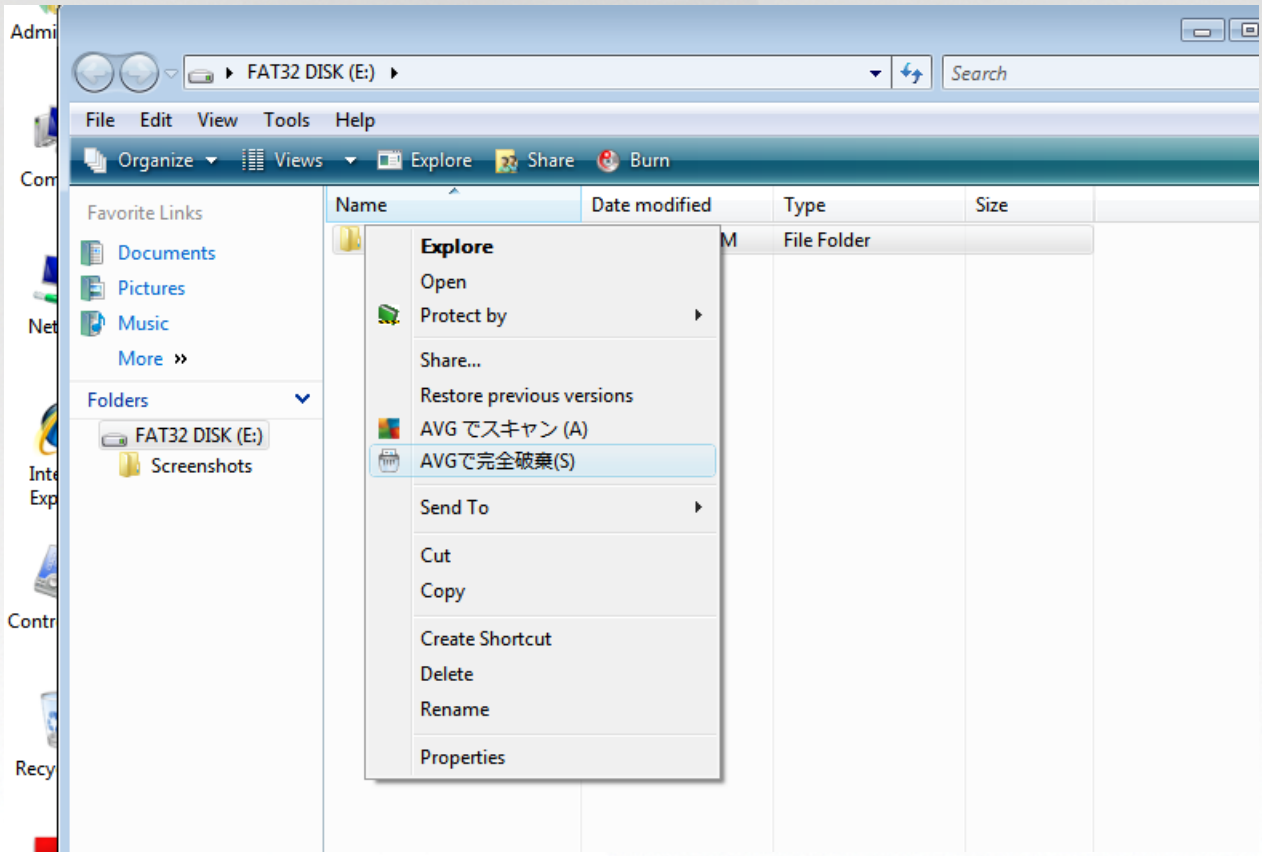
  中程度の危険性: 通常は不要と考えられるアプリケーション *（アドウェアなど）* またはトラッキング Cookie です

  高い危険性: ウイルス、トロイの木馬、セキュリティ上の弱点などの深刻な脅威です。ヒューリスティックの検出方法により検出されたオブジェクト、すなわちウイルス データベースにはまだ記録されていない脅威も含まれます。

10. 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、復元のための高度なソフトウェア 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シュレッダーにかけるには、ファイル マネージャ *(Windows Explorer、Total Commander など)* を右クリックし、コンテキスト メニューで [*AVG で永久にシュレッダーにかける*] を選択します。 ごみ箱にあるファイルもシュレッダーにかけることができます。 特定の場所にある特定のファイル *(CD ROMなど)* を確実にシュレッダーにかけることができない場合、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。



常にご留意ください: ファイルをシュレッダーにかけると、ファイルは永久に失われます。

11. 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 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 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)。

12. 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

12.1. 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 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数

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。

12.2. 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。 その他の選択肢が推奨として表示されます: ***今すぐユーザーを保護 (推奨) 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 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みなして検出し、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*] 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 シールドの検出結果リストを更新*
- *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
- *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。

12.3. Identity Protection の結果

*Identity Protection の結果*ダイアログには、AVG Internet Security メインウィンドウの上にある*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 の結果 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。

12.4. メール保護の結果

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

このダイアログには、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。

12.5. 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*のリストに口グ出力されます。 検出された脅威の概要には、AVG Internet Security 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。

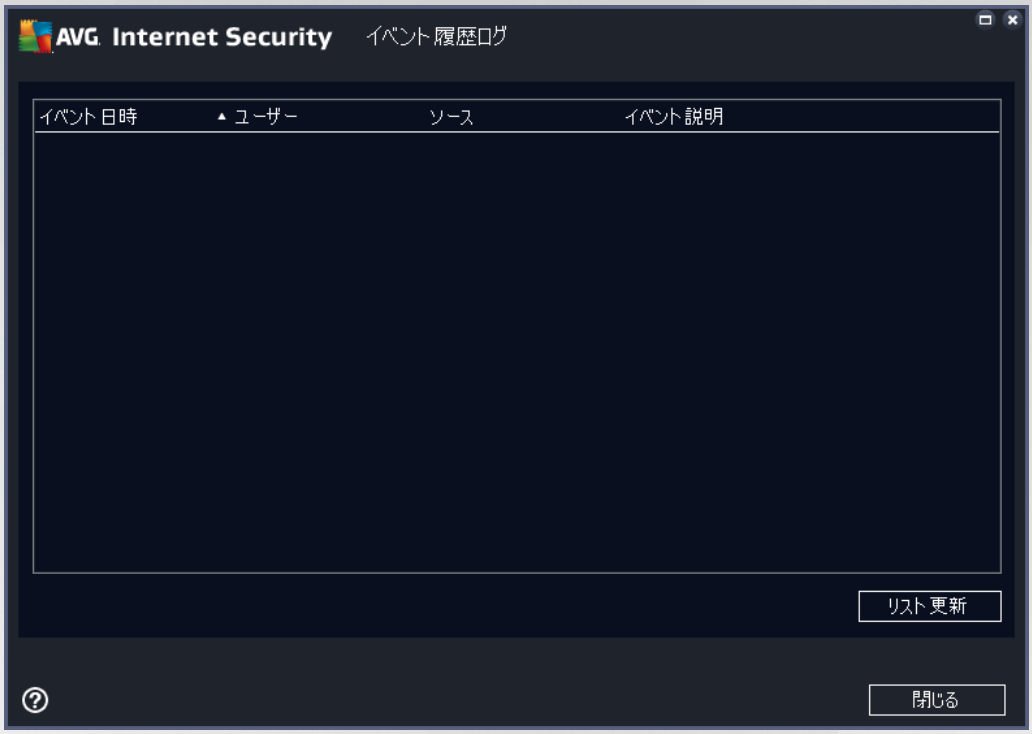
検出された各オブジェクトについて、以下の情報が提供されます。

- *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 シールドの検出結果リストを更新*
- *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。

12.6. イベント履歴



[*イベント履歴*] ダイアログには、AVG Internet Security 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動作中に発生した重要なイベントのサマリを見ることができます。 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

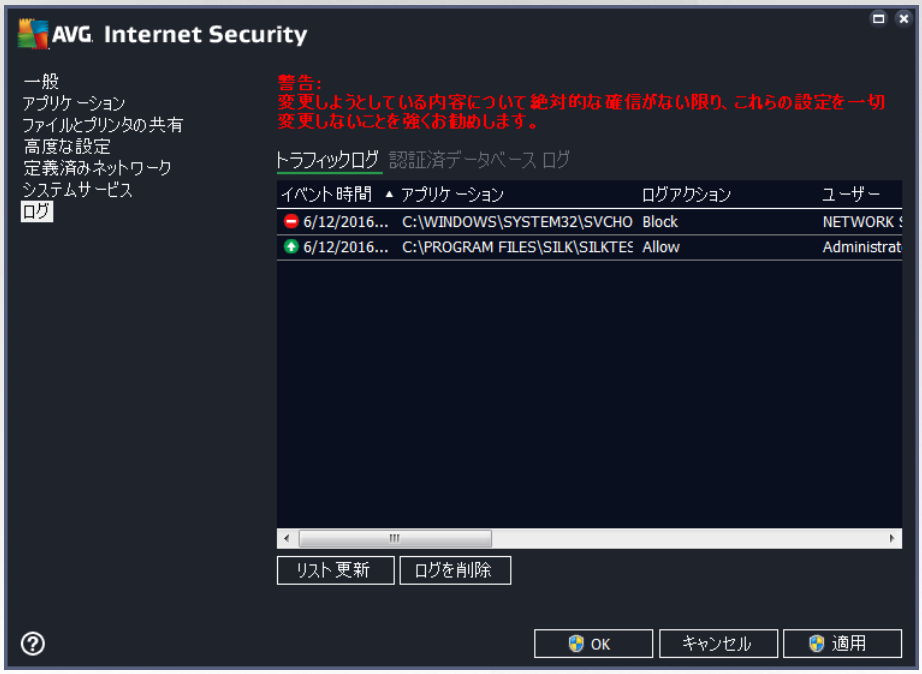
- *リスト更新* - このボタンをクリックすると、イベント リストのすべてのエントリが更新されます。
- *閉じる* - このボタンをクリックすると、 AVG Internet Security メイン ウィンドウに戻ります。

12.7. 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。

13. 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 システムの両方の新しい欠陥を常に探して、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 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デフォルト設定に従うことです。 AVG Internet Security 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。

お使いの 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、ウイルス定義の更新を毎日実行してください。 緊急度の低いプログラムのアップデートは週次で実行してもかまいません。

最高のセキュリティを実現するために、デフォルトでは、AVG Internet Security が 2 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 更新は定められた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 [すぐにアップデート] 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、AVG Internet Security はダウンロードを開始し、アップデート プロセスを開始します。 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行することを強くお勧めします。* 設定は [高度な設定/スケジュール] セクションで編集できます。具体的には次のダイアログが表示されます。

- 定義アップデート スケジュール
- スパム対策アップデート スケジュール

14. FAQ およびテクニカルサポート

AVG Internet Security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*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。