# AVG Internet Security 2011

## ユーザーマニュアル

**ドキュメント改訂 2011.21 (16.5.2011)**

# 目次


**1. はじめに ..... 8**

**2. AVG インストール要件 ..... 9**

2.1 対応オペレーティング システム ..... 9
2.2 最低および推奨ハードウェア要件 ..... 9

**3. AVG インストール オプション ..... 10**

**4. AVG インストール処理 ..... 11**

4.1 ようこそ ..... 11
4.2 AVG ライセンスのアクティベート ..... 12
4.3 インストール種別の選択 ..... 13
4.4 カスタム オプション ..... 14
4.5 AVG セキュリティツールバー のインストール ..... 15
4.6 インストールの進行状況 ..... 16
4.7 インストールに成功しました ..... 16

**5. インストール後 ..... 18**

5.1 製品登録 ..... 18
5.2 ユーザー インターフェースへのアクセス ..... 18
5.3 完全コンピュータ スキャン ..... 18
5.4 Eicar 検査 ..... 18
5.5 AVG の既定の設定 ..... 19

**6. AVG ユーザー インターフェース ..... 20**

6.1 システム メニュー ..... 21
*6.1.1 ファイル ..... 21*
*6.1.2 コンポーネント ..... 21*
*6.1.3 履歴 ..... 21*
*6.1.4 ツール ..... 21*
*6.1.5 ヘルプ ..... 21*
6.2 セキュリティ ステータス情報 ..... 24
6.3 クイック リンク ..... 25
6.4 コンポーネント概要 ..... 25
6.5 統計 ..... 27
6.6 システム トレイ アイコン ..... 27
6.7 AVG ガジェット ..... 29

**7. AVG コンポーネント ..... 32**

7.1 ウィルス対策 ..... 32
*7.1.1 ウィルス対策の原理 ..... 32*
*7.1.2 ウイルス対策インターフェース ..... 32*
7.2 スパイウェア対策 ..... 33
*7.2.1 スパイウェア対策の原理 ..... 33*
*7.2.2 スパイウェア対策インターフェース ..... 33*
7.3 スパム対策 ..... 35
*7.3.1 スパム対策基本 ..... 35*
*7.3.2 スパム対策インターフェース ..... 35*
7.4 ファイアウォール ..... 37
*7.4.1 ファイアウォールの原理 ..... 37*
*7.4.2 ファイアウォール プロファイル ..... 37*
*7.4.3 ファイアウォール インターフェース ..... 37*
7.5 リンクスキャナ ..... 41
*7.5.1 リンクスキャナの原理 ..... 41*
*7.5.2 リンクスキャナ インターフェース ..... 41*
*7.5.3 サーチ シールド ..... 41*
*7.5.4 サーフ シールド ..... 41*
7.6 常駐シールド ..... 44
*7.6.1 常駐シールドの原理 ..... 44*
*7.6.2 常駐シールド インターフェース ..... 44*
*7.6.3 常駐シールド検出 ..... 44*
7.7 ファミリー セーフティ ..... 49
7.8 AVG LiveKive ..... 49
7.9 メール スキャナ ..... 49
*7.9.1 メール スキャナの原理 ..... 49*
*7.9.2 メール スキャナ インターフェース ..... 49*
*7.9.3 メール スキャナ検出 ..... 49*
7.10 アップデート マネージャ ..... 54
*7.10.1 アップデート マネージャの原理 ..... 54*
*7.10.2 アップデート マネージャ インターフェース ..... 54*
7.11 ライセンス ..... 56
7.12 遠隔管理 ..... 57
7.13 オンライン シールド ..... 58
*7.13.1 オンライン シールドの原理 ..... 58*
*7.13.2 オンライン シールド インターフェース ..... 58*

7.13.3 オンライン シールド検出 ..... 58
7.14 ルートキット対策 ..... 61
7.14.1 ルートキット対策の原理 ..... 61
7.14.2 ルートキット対策インターフェース ..... 61
7.15 システム ツール ..... 63
7.15.1 プロセス ..... 63
7.15.2 ネットワーク接続 ..... 63
7.15.3 自動起動 ..... 63
7.15.4 ブラウザ拡張 ..... 63
7.15.5 LSP ビューア ..... 63
7.16 PC Analyzer ..... 69
7.17 Identity Protection ..... 71
7.17.1 Identity Protection の原理 ..... 71
7.17.2 Identity Protection インターフェース ..... 71
7.18 セキュリティ ツールバー ..... 73

**8. AVG セキュリティ ツールバー ..... 75**

8.1 AVG セキュリティ ツールバー インターフェース ..... 75
8.1.1 AVG ロゴ ボタン ..... 75
8.1.2 AVG Secure Search (powered by Google) による検索ボックス ..... 75
8.1.3 ページ ステータス ..... 75
8.1.4 AVG ニュース ..... 75
8.1.5 ニュース ..... 75
8.1.6 履歴の削除 ..... 75
8.1.7 メール通知 ..... 75
8.1.8 天気予報情報 ..... 75
8.1.9 Facebook ..... 75
8.2 AVG セキュリティ ツールバー オプション ..... 82
8.2.1 タブ全般 ..... 82
8.2.2 タブの便利なボタン ..... 82
8.2.3 タブ セキュリティ ..... 82
8.2.4 タブの高度なオプション ..... 82

**9. AVG 高度な設定 ..... 87**

9.1 表示 ..... 87
9.2 サウンド ..... 89
9.3 エラー状態を無視 ..... 91
9.4 Identity Protection ..... 92
9.4.1 Identity Protection 設定 ..... 92

*9.4.2 許可リスト* ..... *92*
9.5 ウイルス隔離室 ..... 96
9.6 PUP 例外 ..... 96
9.7 スパム対策 ..... 98
*9.7.1 設定* ..... *98*
*9.7.2 パフォーマンス* ..... *98*
*9.7.3 RBL* ..... *98*
*9.7.4 ホワイトリスト* ..... *98*
*9.7.5 ブラックリスト* ..... *98*
*9.7.6 高度な設定* ..... *98*
9.8 オンライン シールド ..... 110
*9.8.1 Web 保護* ..... *110*
*9.8.2 インスタント メッセージ* ..... *110*
9.9 リンクスキャナ ..... 114
9.10 スキャン ..... 115
*9.10.1 完全コンピュータ スキャン* ..... *115*
*9.10.2 シェル拡張スキャン* ..... *115*
*9.10.3 特定のファイルやフォルダをスキャン* ..... *115*
*9.10.4 リムーバブル デバイスのスキャン* ..... *115*
9.11 スケジュール ..... 120
*9.11.1 スケジュール済スキャン* ..... *120*
*9.11.2 ウイルス データベース アップデート スケジュール* ..... *120*
*9.11.3 プログラム アップデート スケジュール* ..... *120*
*9.11.4 スパム対策アップデート スケジュール* ..... *120*
9.12 メール スキャナ ..... 132
*9.12.1 認証* ..... *132*
*9.12.2 メール フィルタリング* ..... *132*
*9.12.3 サーバー* ..... *132*
9.13 常駐シールド ..... 141
*9.13.1 高度な設定* ..... *141*
*9.13.2 除外された項目* ..... *141*
9.14 キャッシュ サーバー ..... 145
9.15 ルートキット対策 ..... 146
9.16 更新 ..... 147
*9.16.1 プロキシ* ..... *147*
*9.16.2 ダイヤルアップ* ..... *147*
*9.16.3 URL* ..... *147*
*9.16.4 管理* ..... *147*

9.17 一時的に AVG 保護を無効にする ..... 154
9.18 製品改善プログラム ..... 154

**10. ファイアウォール設定 ..... 157**

10.1 一般 ..... 157
10.2 セキュリティ ..... 159
10.3 エリアとアダプタのプロファイル ..... 160
10.4 IDS ..... 161
10.5 ログ ..... 163
10.6 プロファイル ..... 164

**11. AVG スキャン ..... 166**

11.1 スキャン インターフェース ..... 166
11.2 定義済みスキャン ..... 167
*11.2.1 完全コンピュータ スキャン ..... 167*
*11.2.2 特定のファイルとフォルダのスキャン ..... 167*
*11.2.3 ルートキット スキャン ..... 167*
11.3 シェル拡張スキャン ..... 177
11.4 コマンドライン スキャン ..... 178
*11.4.1 CMD スキャン パラメータ ..... 178*
11.5 スキャン スケジュール ..... 181
*11.5.1 スケジュール設定 ..... 181*
*11.5.2 スキャン方法 ..... 181*
*11.5.3 スキャン対象 ..... 181*
11.6 スキャン結果概要 ..... 190
11.7 スキャン結果詳細 ..... 191
*11.7.1 結果概要タブ ..... 191*
*11.7.2 感染タブ ..... 191*
*11.7.3 スパイウェア タブ ..... 191*
*11.7.4 警告タブ ..... 191*
*11.7.5 ルートキット タブ ..... 191*
*11.7.6 情報タブ ..... 191*
11.8 ウイルス隔離室 ..... 199

**12. AVG 更新 ..... 201**

12.1 更新レベル ..... 201
12.2 更新タイプ ..... 201
12.3 更新処理 ..... 201

13. イベント履歴 ..... 203

14. FAQ とテクニカル サポート ..... 205

# 1. はじめに

このユーザー マニュアルは、**AVG Internet Security 2011** の包括的なマニュアルです。

**AVG Internet Security 2011 をご購入いただき、どうもありがとうございます。**

**AVG Internet Security 2011**は、コンピュータの総合的なセキュリティを提供するように設計された、受賞経験のある AVG 製品の 1 つです。すべての AVG 製品と同様に、AVG の信頼性のあるセキュリティ機能をより分かりやすく、効率的な方法で提供するために、**AVG Internet Security 2011** は完全に再設計されました。新しい **AVG Internet Security 2011** 製品は、合理化されたインターフェースとより積極的で高速化されたスキャンを提供します。より多くのセキュリティ機能が自動化され便利になりました。新しい「インテリジェント」ユーザーオプションが搭載され、セキュリティ機能をカスタマイズしやすい製品となりました。妥協のないユーザビリティを提供します。

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

## すべての AVG 製品提供

- インターネット バンキング、インターネット ショッピング、閲覧、検索、チャット、電子メール、ファイルのダウンロード、ソーシャル ネットワークなど、あらゆるコンピュータの利用環境でユーザーを保護します。AVG はユーザーのニーズに最適な製品を提供しています。
- 世界中の 1 億 1,000 万人ものユーザーが AVG の保護を信頼しています。AVG のソリューションは世界中に広がる経験豊富な研究者のネットワークによって開発されています。また、導入も簡単です。
- 24 時間年中無休で専門技術者が AVG の保護を支えています。

# 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 2011** は、次のオペレーティング システムで稼動するワークステーションの保護を目的としています。

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

（また、特定のオペレーティングシステム用サービスパック）

***メモ:*** *個人情報保護コンポーネントは Windows XP x64 ではサポートされていません。これらのオペレーティング システムでは、AVG Internet Security 2011 のインストールはできますが、個人情報保護コンポーネントのインストールはできません。*

## 2.2. 最低および推奨ハードウェア要件

**AVG Internet Security 2011** の最低ハードウェア要件:

- Intel Pentium CPU 1,5 GHz
- 512 MB の RAM メモリ
- ハードディスク空き容量 750MB以上（インストールのため）

**AVG Internet Security 2011** の推奨ハードウェア要件:

- Intel Pentium CPU 1,8 GHz
- 512 MB の RAM メモリ
- ハードディスク空き容量 1400MB以上（インストールのため）

# 3. AVG インストール オプション

インストール CD にあるインストール ファイルを使用して AVG をインストールできます。あるいは、AVG Web サイト (http://www.avg.com/) から最新のインストール ファイルをダウンロードしてインストールできます。

**AVG のインストールを開始する前に、AVG の Web サイト (http://www.avg.com/) で最新のインストール ファイルを確認することを強くお勧めします。このような手順によって、確実に利用可能な最新バージョンの AVG Internet Security 2011 をインストールできます。**

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

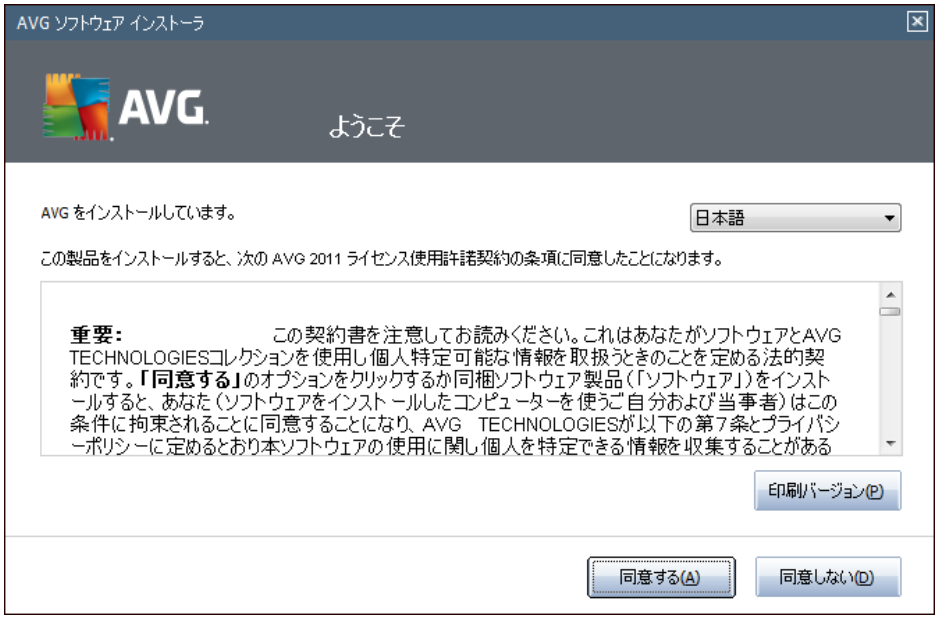
# 4. AVG インストール処理

コンピュータに **AVG Internet Security 2011** をインストールする場合は、最新のインストール ファイルを取得する必要があります。パッケージ版の CD にあるインストール ファイルも使用できますが、このファイルは古い可能性があります。したがって、最新のインストール ファイルをオンラインで入手することをお勧めします。AVG ウェブサイト (http://www.avg.com/) の ***サポート センター/ダウンロード*** セクションからファイルをダウンロードできます。

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

## 4.1. ようこそ

インストール処理で最初に開くウィンドウは [***ようこそ***] ダイアログです。このダイアログでは、インストール処理の言語と AVG ユーザー インターフェースの既定の言語を選択します。 ダイアログ ウィンドウの上部には、言語リスト ドロップダウン メニューが表示され、任意の言語を選択できます。



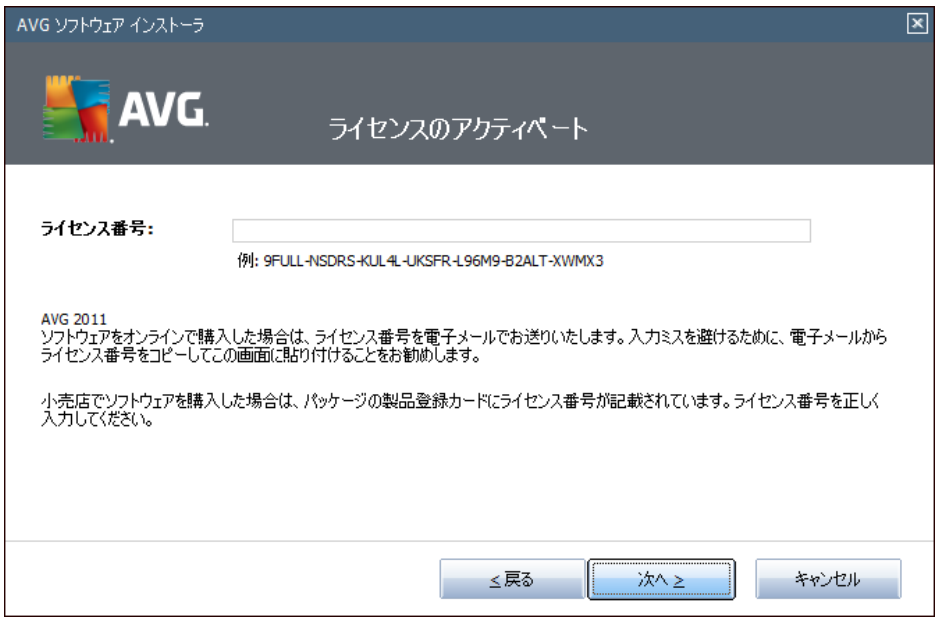

***注意**: ここで選択する言語はインストール処理で使用する言語です。ここで選択する言語は AVG ユーザー インターフェースの既定の言語としてインストールされます。また、英語も自動的にインストールされます。他の言語をインストールしてユーザー インターフェースで使用する場合は、[**カスタム オプション**] という名前のセットアップ ダイアログのいずれかで定義してください。*

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

## 4.2. AVG ライセンスのアクティベート

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

セールス番号は、**AVG Internet Security 2011** ボックスの CD パッケージに記載されています。ライセンス番号は**AVG Internet Security 2011**をオンラインで購入後に受信する確認メールに記載されています。この番号を記載通り正確に入力してください。デジタル形式のライセンス番号が利用できる（メールで）場合は、コピーとペーストを使用して、それを入力することを推奨します。




***次へ***ボタンをクリックし、インストールプロセスを継続します。

## 4.3. インストール種別の選択


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

通常ユーザーの場合は、標準の [***クイック インストール***] を選択し、プログラム ベンダーが事前定義した設定を使用して AVG を自動モードでインストールすることが強く推奨されます。この設定は、最適なリソース消費で最大のセキュリティを実現します。将来的に設定の変更の必要が生じた場合、常にAVGアプリケーションで直接変更することができます。[***クイック インストール***] オプションを選択した場合は、[**次へ**] ボタンをクリックして、次の [***AVG セキュリティ ツールバーのインストール***] ダイアログに進みます。

***カスタム インストール***は、AVG を標準設定でインストールしない合理的な理由がある場合、経験のあるユーザーのみが行ってください (特定のシステム要件への適合など)。このオプションを選択したら、[**次へ**] ボタンをクリックして、[***カスタム オプション***] に進みます。

ダイアログの右側のセクションには ***AVG ガジェット*** (*Windows Vista/Windows 7 で対応*) 関連のチェック ボックスが表示されます。このガジェットをインストールする場合は、該当するチェック ボックスを選択します。***AVG ガジェット***には Windows サイドバーからアクセスでき、スキャンや更新など **AVG Internet Security 2011** の最も重要な機能を簡単に実行できます。

## 4.4. カスタム オプション

[***カスタム オプション***] ダイアログでは 2 つのインストール パラメータを設定できます。


### インストール先フォルダ

ダイアログの [***インストール先フォルダ***] セクションでは、**AVG Internet Security 2011** のインストール場所を指定します。既定では AVGは C ドライブの program files フォルダにインストールされます。この場所を変更する場合は、[***参照***] ボタンをクリックしてドライブ構成を表示し、対象フォルダを選択します。

### コンポーネントの選択

[***コンポーネント選択***] セクションには、インストール可能なすべての **AVG Internet Security 2011** コンポーネントの概要が表示されます。既定の設定が適当でない場合は、特定のコンポーネントを追加または削除できます。

***ただし、選択できるコンポーネントは購入した AVG 製品に含まれるコンポーネントのみです。***

[***コンポーネント選択***] リストの項目を強調表示すると、該当するコンポーネントの簡単な説明がこのセクションの右側に表示されます。各コンポーネントの機能に関する詳細については、このマニュアルの「***コンポーネント概要***」の章を参照してください。ソフトウェア ベンダーが事前設定した既定の設定に戻すには、[***既定***] ボタンをクリックします。

[***次へ***] ボタンをクリックして続行します。

## 4.5. AVG セキュリティツールバー のインストール


[*AVG セキュリティツールバー のインストール*] ダイアログでは、***セキュリティツールバー*** 機能をインストールするかどうかを決定します。既定の設定を変更しない場合は、このコンポーネントはインターネット ブラウザに自動的にインストールされ (*現在サポートされているブラウザは Microsoft Internet Explorer v. 6.0 以上および Mozilla Firefox v. 3.0 以上*)、インターネット閲覧中の包括的オンライン保護を提供します。

また、既定の検索プロバイダとして *AVG Secure Search (powered by Google)* を選択するかどうかを決定できます。この場合は、該当するチェック ボックスを選択します。

## 4.6. インストールの進行状況

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


インストール処理の終了後、次のダイアログに進みます。

## 4.7. インストールに成功しました

[***インストールに成功しました***] ダイアログでは、**AVG Internet Security 2011** が正常にインストールおよび設定されたことを確認できます。

製品関連情報とニュースをすべて受信できるように、このダイアログで連絡先情報を入力してください。登録フォームでは次の項目を選択できます。

- ***はい。セキュリティ ニュースと AVG 2011 の特別提供に関するお知らせを電子メールで通知します*** - このチェック ボックスを選択すると、インターネット セキュリティ関連ニュース、AVG 製品の特別提供情報、製品改良、アップグレードなどに関する情報を受信します。

- ***AVG 2011 Web 安全および製品改善プログラムに参加します...*** - このチェック ボックスを選択すると、製品改善プログラム (*詳細については、「AVG 高度な設定/製品改善プログラム」の章を参照してください*) に参加することで、検出された脅威に関する匿名情報を提供し、インターネット セキュリティ レベル全体の向上に協力することに同意します。

インストール処理を完了するには、コンピュータの再起動が必要です。[***今すぐ再起動***] をクリックするか、[***後で再起動***] をクリックして再起動処理を延期します。

***メモ:*** *AVG ビジネス版ライセンスを使用し、遠隔管理コンポーネントのインストール (「カスタム オプション」を参照) を選択した場合は、次のインターフェースで [インストールに成功しました] ダイアログが表示されます。*

*AVG DataCenter パラメータを指定する必要があります。「サーバー:ポート」の形式で AVG DataCenter への接続文字列を入力してください。この時点でこの情報がない場合は、このフィールドを空白にしておくと、後から [**高度な設定/遠隔管理**] ダイアログで設定できます。AVG 遠隔管理の詳細については、『AVG Business Edition ユーザー マニュアル』 を参照してください。このマニュアルは AVG Web サイト (http://www.avg.com/) からダウンロードできます。*

# 5. インストール後

## 5.1. 製品登録

**AVG Internet Security 2011** インストールが終了したら、AVG Webサイト（http://www.avg.com/）、[***登録***] ページ*で製品のオンライン登録を行ってください（画面上の指示にしたがってください*）。登録後、AVGユーザーアカウント、AVGアップデートニュースレター、その他登録ユーザーのみに提供されるサービスが利用できるようになります。

## 5.2. ユーザー インターフェースへのアクセス

***AVGユーザー インターフェース***には複数の方法でアクセスできます。

- ***AVG システム トレイ アイコン***
- デスクトップの AVG アイコンをダブルクリックします。
- ***AVG ガジェット*** (*インストールされている場合。Windows Vista/ Windows 7 に対応*)
- メニューから ***[スタート/すべてのプログラム/AVG 2011/AVG ユーザー インターフェース] の順に選択します。***
- ***AVG Security Toolbar*** の [***AVG の起動***

## 5.3. 完全コンピュータ スキャン

**AVG Internet Security 2011**インストール前にウイルスが感染している可能性あります。このため、***全コンピュータをスキャン***を実行して、PCが感染していないことを確認してください。

***全コンピュータをスキャン***を実行する方法については、***AVGスキャン***の章を参照してください。

## 5.4. Eicar 検査

**AVG Internet Security 2011** が正常にインストールされたことを確認するために、EICARテストを実行できます。

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

***eicar.com***ファイルをダウンロードし、それをローカルディスクに保存します。検査

ファイルのダウンロードを確認後すぐに、***オンライン シールド***が警告とともにそれに反応します。この通知は、AVG が正常にコンピュータにインストールされていることを証明します。


http://www.eicar.com ウェブサイトから、圧縮された (*eicar_com.zip 形式*) EICAR ウィルスをダウンロードすることもできます。***オンライン シールド***によって、このファイルをダウンロードし、ローカル ディスクに保存できますが、解凍しようとすると***常駐シールド***がウィルスを検出します。**AVGがEICARテストファイルをウイルスとして特定できない場合、プログラム設定を再度確認する必要があります。**

## 5.5. AVG の既定の設定

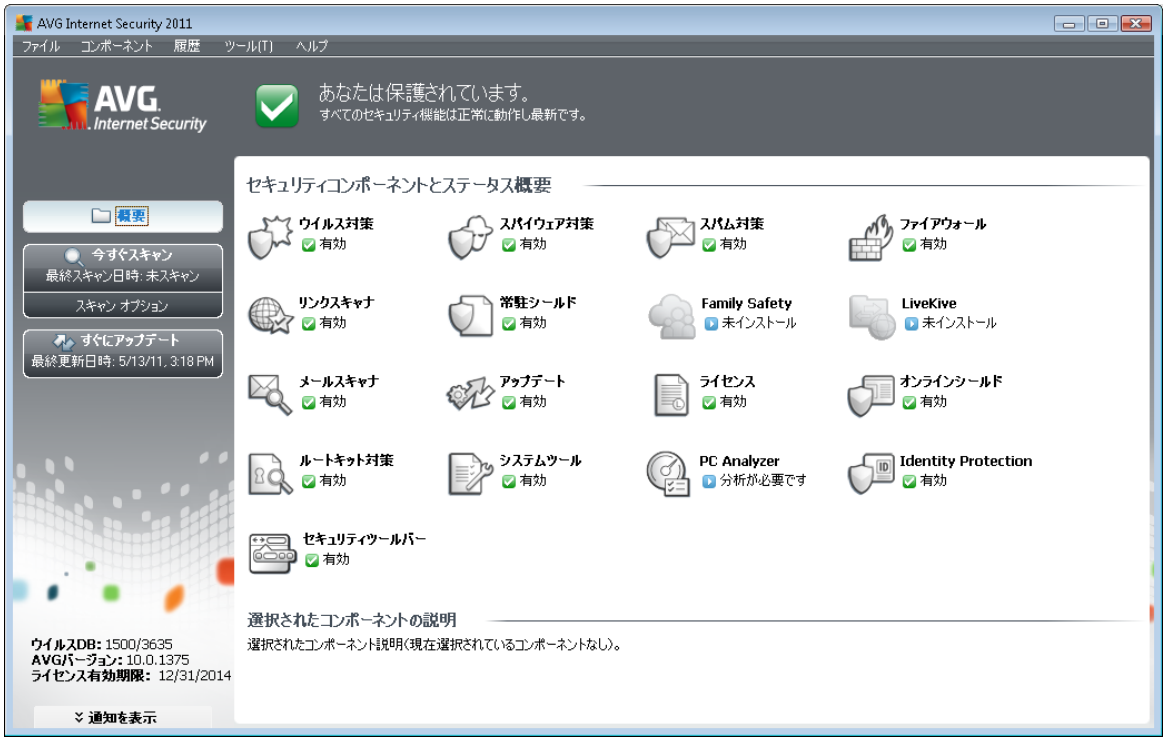
のデフォルト設定（*アプリケーションがインストール後に正しく動作するための初期設定*) **AVG Internet Security 2011** では、すべてのコンポーネントと機能が最適なパフォーマンスで動作するよう設定されています。

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

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

# 6. AVG ユーザー インターフェース

**AVG Internet Security 2011** はメイン ウィンドウで開きます。




メインウィンドウは複数のセクションに分けられます。

- ***システムメニュー***（*ウィンドウ上のシステムライン*）は標準ナビゲーションであり、すべてのAVGコンポーネント、サービス、機能にアクセスすることができます。 - 詳細 >>
- ***セキュリティステータス情報***（*ウィンドウ上部のセクション*）には、現在のAVGプログラムのステータスが表示されます。- 詳細 >>
- ***クイックリンク***（*ウィンドウの左のセクション*）では、最も重要で最も頻繁に使用されるAVGタスクにすぐにアクセスすることができます。 - 詳細 >>
- ***コンポーネント概要***（*ウィンドウ中央部*）は、インストールされたAVGコンポーネントの概要が表示されます。 - 詳細 >>
- ***統計***（*ウィンドウ左下部*）では、プログラムに関する統計データが表示されます。-詳細 >>
- ***システムトレイアイコン***（*モニター右下端のシステムトレイ*）では、現在のAVGステータスが表示されます。 -詳細 >>
- ***AVG ガジェット*** *(ウィンドウ サイドバー。Windows Vista/7 に対応)* を使用すると、AVG スキャンと更新 - 詳細 >>

## 6.1. システム メニュー

***システムメニュー***は、すべてのWindowsアプリケーションで使用される標準のナビゲーションです。**AVG Internet Security 2011** メイン ウィンドウの最上部に横方向に表示されます。システムメニューを使用して、AVGの各コンポーネント、機能、サービスにアクセスします。

システムメニューは5つの主要なセクションにわかれています。

### 6.1.1. ファイル

- ***終了*** - **AVG Internet Security 2011**のユーザーインターフェースを閉じます。ただし、AVGアプリケーションはバックグラウンドで実行され、コンピュータは保護されます。

### 6.1.2. コンポーネント

システム メニューの***コンポーネント***には、インストールされたすべての AVG コンポーネントへのリンクが表示されます。リンクをクリックすると、各コンポーネントの既定のダイアログ ページが表示されます。

- ***システム概要*** - インストールされたすべてのコンポーネントとそのステータスの概要を表示します。
- ***ウイルス対策***は、コンピュータに侵入しようとするウイルスからコンピュータを確実に保護します。- 詳細>>
- ***スパイウェア対策***は、スパイウェアとアドウェアからコンピュータを確実に保護します。 - 詳細 >>
- ***スパム対策***は、すべての受信メールをチェックし、望ましくないメールをSPAMとして判定します。 - 詳細>>
- ***ファイアウォールは、コンピュータがインターネット上やローカルネットワーク上の他のコンピュータとデータを交換する方法をコントロールします。*** - 詳細>>
- ***リンクスキャナ***は、インターネットブラウザに表示される検索結果をチェックします - 詳細>>
- ***メール スキャナ***は、すべての送受信メールのウイルス チェックを行います。 - 詳細>>
- ***ファミリー セーフティ***を使用すると、子供のオンライン活動を監視し、不適切な Web コンテンツから子供を保護できます。- 詳細 >>
- ***LiveKive*** はオンライン データを自動的にバックアップします。- 詳細 >>
- ***常駐シールド***はバックグラウンドで実行され、ファイルがコピーされたり、開かれたり、保存される際にそのファイルをスキャンします。 - 詳細>>

- ***更新マネージャ***はすべての AVG 更新を制御します。 - 詳細>>
- ***ライセンス***には、ライセンス番号、種類、有効期限が表示されます - 詳細 >>
- ***オンライン シールド***は、ウェブ ブラウザからダウンロードされるすべてのデータをスキャンします - 詳細>>
- ***ルートキット対策***はマルウェアを隠そうとするプログラムと技術を検出します。-詳細>>
- ***システム ツール***は、AVG 環境の詳細な概要とオペレーティング システム情報を提供します。 - 詳細 >>
- ***PC Analyzer***は、コンピュータ ステータスに関する情報を提供します。 - 詳細 >>
- ***個人情報保護*** - ID 窃盗による個人デジタル資産の盗難防止に特化したマルウェア対策コンポーネント - 詳細 >>
- ***セキュリティ ツールバー***をインストールすると、選択した AVG の機能をインターネットから直接利用できます。- 詳細 >>
- ***遠隔管理***は AVG Business Edition でのみ表示されます。インストール処理中にこのコンポーネントのインストールを指定した場合に限ります。

### 6.1.3. 履歴

- ***スキャン結果*** - AVGスキャンインターフェースの***スキャン結果概要***ダイアログを表示します。
- ***常駐シールド検出*** - 常駐シールド***によって検出された脅威の概要ダイアログを開きます。***
- ***メール スキャナ検出*** - ***メール スキャナ***コンポーネントによって検出されたメールの概要ダイアログを開きます。
- ***オンライン シールド検出*** - ***オンライン シールド***
- ***ウイルス隔離室*** - 隔離スペース（***ウイルス隔離室***）インターフェースを開きます。AVGは、検出、または何らかの理由で自動修復できなかったすべての感染をここに移動します。隔離室内では、感染ファイルは隔離され、コンピュータの安全は保証されます。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。
- ***イベント履歴ログ*** - すべてのログに記録された**AVG Internet Security 2011**アクションの概要履歴インターフェースを開きます。
- ***ファイアウォール*** - すべてのファイアウォールアクションに関する詳細概要が表示されている [***ログ***] タブのファイアウォール設定インターフェースを開きます。

### 6.1.4. ツール

- ***コンピュータ スキャン*** - AVG スキャン インターフェースに切り替わり、スキャンを実行します。
- ***特定フォルダのスキャン*** - AVG スキャン インターフェースに切り替わり、スキャンするファイルとフォルダを設定できます。
- ***ファイル スキャン*** - 特定のファイルを指定してスキャンを実行することができます。
- ***更新*** - **AVG Internet Security 2011**更新処理を自動的に実行します。
- ***ディレクトリからの更新*** - ローカル ディスクで指定したフォルダの更新ファイルを使用して更新処理を実行します。ただし、このオプションは緊急時にのみ推奨されます。たとえば、インターネットに接続できない場合 (*コンピュータが感染し、インターネットから切断されている状況など。コンピュータはネットワークに接続されているがインターネットアクセスがない場合など*) などです。フォルダの参照ウィンドウで、更新ファイルを保存したフォルダを選択し、更新処理を実行します。
- ***高度な設定*** - [***AVG 高度な設定***] ダイアログが開きます。ここでは**AVG Internet Security 2011**各項目の設定を編集できます。通常はソフトウェア ベンダーが定義している既定のアプリケーション設定の使用をお勧めします。
- ***ファイアウォール設定*** - ***ファイアウォール*** コンポーネントの高度な設定ダイアログを開きます。

### 6.1.5. ヘルプ

- ***目次*** - AVG ヘルプ ファイルが開きます。
- ***オンライン ヘルプ*** - AVG Free Web サイトのカスタマー サポート センター ページが開きます (http://www.avg.com/)。
- ***AVG Web*** - AVG Web サイト (http://www.avg.com/) が開きます。
- ***ウイルスと脅威について*** - オンラインの***ウイルスエンサイクロペディア***を開きます。ここでは、特定されたウイルスに関する詳細情報を検索することができます。
- ***再アクティベート*** - ***インストール処理***の [***AVG のパーソナライズ***] ダイアログで入力したデータが [AVG のアクティベート] ダイアログに表示されます。このダイアログではライセンス番号を入力してセールス番号（*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。
- ***今すぐ登録*** - AVG Web サイト（http://www.avg.com/）の登録ページに接続します。登録データを入力してください。AVG 製品を登録したお客様のみが無料テクニカル サポートを利用できます。

***メモ**: AVG Internet Security 2011 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。セールス番号を使用して AVG Internet Security 2011 をインストールした場合は、各項目が [**登録**] および [**アクティベート**] として表示されます。 詳細については、このマニュアルの「ライセンス」セクションを参照してください。*

- ***AVG について** - **情報**ダイアログを開きます。このダイアログでは、プログラム名、プログラムとウイルス データベース バージョン、システム情報、ライセンス契約、**AVG Technologies CZ**の問い合わせ先情報を確認できます。

## 6.2. セキュリティ ステータス情報

***セキュリティステータス情報***セクションはAVGメインウィンドウの上部にあります。このセクションでは、**AVG Internet Security 2011**の現在のセキュリティステータスに関する情報が常に表示されます。このセクションで表示されるアイコンの意味は以下の通りです。

 - 緑のアイコンは AVG が完全に機能していることを示します。コンピュータは完全に保護され、最新のインストール済みのコンポーネントが適切に動作しています。

 - オレンジのアイコンは、1 つ以上のコンポーネントが不正に設定され、プロパティ/設定に注意する必要があることを警告しています。AVGには致命的な問題はなく、おそらく何らかの理由で一部のコンポーネントをオフにしたものと思われます。コンピュータはAVGによって保護されています。ただし、問題のコンポーネントの設定に注意してください。その名前は***セキュリティステータス情報***セクションに表示されます。

このアイコンは、何らかの理由で、コンポーネントのエラー状態を無視することにした場合にも表示されます（*[コンポーネント状態を無視]オプションはAVGメインウィンドウのコンポーネント概要にある該当するコンポーネントアイコンを右クリックすると開くコンテキストメニューで利用できます*）。特定の場合にこのオプションを使用する必要があるかもしれませんが、[***コンポーネント状態を無視***]オプションはすぐにオフにすることを強く推奨します。

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

**AVG が最適なパフォーマンスに設定されていない場合は、新しい [修正] 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 [すべてを修正] ボタン) がセキュリティ ステータス情報の横に表示されます。このボタンをクリックすると、プログラム チェックおよび設定の自動処理が実行されます。これは最適なパフォーマンスに AVG を設定し、最高レベルのセキュリティを実現するための最も簡単**

**な方法です。**

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

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

## 6.3. クイック リンク

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


- ***概要*** - このリンクをクリックすると、すべてのインストール済みコンポーネントの概要を表示する既定のインターフェースへ切り替わります。「***コンポーネント概要***」の章を参照してください。 >>
- ***今すぐスキャン*** - 既定ではこのボタンをクリックすると、前回実行したスキャンの情報 (*スキャン タイプ*、*前回実行日*) が表示されます。[***今すぐスキャン***] コマンドを実行して同じスキャンを再度実行するか、[***スキャン オプション***] リンクをクリックして、AVG スキャン インターフェースを表示できます。AVG スキャン インターフェースでは、スキャンの実行、スキャンのスケジュール作成、パラメータの編集ができます。「***AVG スキャン***」の章を参照してください。>>
- ***今すぐ更新*** - このリンクをクリックすると、前回の更新処理実行日が表示されます。このボタンをクリックすると、更新インターフェースが開き、AVG 更新処理がただちに実行されます「***AVG 更新***」の章を参照してください。>>

これらのリンクはユーザー インターフェースで使用できます。一度、クイック リンクを使用して特定のプロセスを実行すると、GUI は新しいダイアログに切り替わりますが、クイック リンクはまだ利用できます。さらに、実行中のプロセスはよりグラフィカルに表示されます。

## 6.4. コンポーネント概要

[***コンポーネント概要***] セクションはAVG ユーザー インターフェースの中央部にあります。このセクションは 2 つに分かれます。

- パネル上にインストール済みコンポーネントの概要がアイコン表示されるとと

もに、各コンポーネントの有効/無効状態が表示されます。

- 選択したコンポーネントの説明

**AVG Internet Security 2011** の [***コンポーネント概要***] セクションには、次のコンポーネントの情報が示されます。

- ***ウイルス対策***はコンピュータに侵入しようとするウイルスからコンピュータを確実に保護します。- 詳細>>
- ***スパイウェア対策***は、スパイウェアとアドウェアからコンピュータを確実に保護します。 - 詳細 >>
- ***スパム対策***は、すべての受信メールをチェックし、望ましくないメールをSPAMとして判定します。 - 詳細>>
- ***ファイアウォールは、コンピュータがインターネット上やローカルネットワーク上の他のコンピュータとデータを交換する方法をコントロールします。*** - 詳細>>
- ***リンクスキャナ***は、インターネットブラウザに表示される検索結果をチェックします - 詳細>>
- ***メール スキャナ***は、すべての送受信メールのウイルス チェックを行います。 - 詳細>>
- ***常駐シールド***はバックグラウンドで実行され、ファイルがコピーされたり、開かれたり、保存される際にそのファイルをスキャンします。 - 詳細>>
- ***ファミリー セーフティ***を使用すると、子供のオンライン活動を監視し、不適切な Web コンテンツから子供を保護できます。- 詳細 >>
- ***LiveKive*** はオンライン データを自動的にバックアップします。- 詳細 >>
- ***更新マネージャ***はすべての AVG 更新を制御します。 - 詳細>>
- ***ライセンス***には、ライセンス番号、種類、有効期限が表示されます - 詳細 >>
- ***オンライン シールド***は、ウェブ ブラウザからダウンロードされるすべてのデータをスキャンします - 詳細>>
- ***ルートキット対策***はマルウェアを隠そうとするプログラムと技術を検出します。-詳細>>
- ***システム ツール***は、AVG 環境の詳細な概要とオペレーティング システム情報を提供します。 - 詳細 >>
- ***PC アナライザ*** は、コンピュータ ステータスに関する情報を提供します。 - 詳細 >>
- ***個人情報保護*** - ID 窃盗による個人デジタル資産の盗難防止に特化したマルウェ

ア対策コンポーネント - 詳細 >>

- ***セキュリティ ツールバー***をインストールすると、選択した AVG の機能をインターネットから直接利用できます。- 詳細 >>
- ***遠隔管理***は AVG Business Edition でのみ表示されます。インストール処理中にこのコンポーネントのインストールを指定した場合に限ります。

任意のコンポーネント アイコンをクリックすると、コンポーネント概要のコンポーネントが強調表示されます。同時に、コンポーネントの基本機能説明がユーザー インターフェースの下部に表示されます。アイコンをダブルクリックすると、コンポーネントのインターフェースが開き、基本統計情報データの一覧が表示されます。

コンポーネントのアイコンを右クリックし、コンテキスト メニューを展開します。コンポーネントのグラフィック インターフェースを開き、***コンポーネント状態を無視***することもできます。特別な理由がある場合にこのオプションを選択すると、コンポーネントのエラー状態を認識しながらも、システム トレイ アイコンによる警告を表示せずに AVG のエラー状態を保持できます。

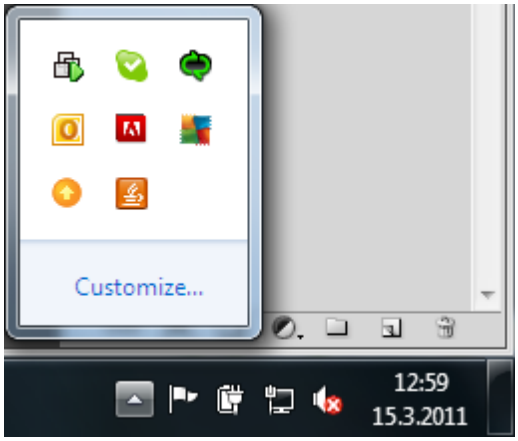
## 6.5. 統計

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

- ***ウイルスDB*** - 現在インストール済みのウイルスデータベースのバージョンを表示します。
- ***AVG バージョン*** - インストール済みの AVG のバージョンを表示します (*番号は、10.0.xxx の形式で表示されます。10.0 は製品ライン バージョンであり、xxx はビルド番号を表します*)。
- ***ライセンス有効期限*** - AVGライセンスの有効期限を表示します。

## 6.6. システム トレイ アイコン

***システム トレイ アイコン*** (*Windows タスクバー上*) は、**AVG Internet Security 2011** の現在の状態を示します。このアイコンは、AVG のメイン ウィンドウが表示されているかどうかにかかわらず、システム トレイ上に常に表示されます。




全色の場合、***システム トレイ アイコン***はすべての AVG コンポーネントが有効であり、完全に機能していることを意味します。また、AVG システムトレイアイコンは、AVG がエラー状態にある場合にも全色で表示されますが、ユーザーはこの状況を完全に認識しており、慎重に***コンポーネント状態を無視***することを決定しています。アイコンとエクスクラメーション マークは、問題を示します (*非アクティブなコンポーネント、エラー状態など*)。***システムトレイアイコン***をダブルクリックして、メインウィンドウを開き、コンポーネントを編集します。

さらに、システム トレイ アイコンは、現在の AVG 活動とプログラム内で起こりうるステータス変更を通知します (*スケジュールされたスキャンまたはアップデートの自動起動、ファイアウォールプロファイル切り替え、コンポーネントのステータス変更、エラー ステータスの発生など*)。これは、AVG システム トレイ アイコンから開くポップアップ ウィンドウに表示されます。


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

- ***AVGユーザーインターフェースを開く*** - クリックするとAVGユーザーインターフェースが表示されます。
- ***スキャン*** - クリックすると、
- ***ファイアウォール*** - クリックすると、ファイアウォール設定オプションのコンテキスト メニューが開き、ファイアウォール ステータス (*ファイアウォール有効/ファイアウォール無効/緊急モード*)、ゲーム モード切替、ファイアウォール プロファイル
- ***PC Analyzer***を実行 - クリックすると、PC Analyzer コンポーネントが起動します。

- ***実行中のスキャン*** - 現在コンピュータでスキャンが実行されている場合にのみこの項目が表示されます。この場合、スキャンの優先度の設定、実行中のスキャンの停止または一時停止を実行できます。さらに、*すべてのスキャンの優先度の設定*、*すべてのスキャンの一時停止*、*すべてのスキャンの停止*アクションも実行できます。
- ***今すぐアップデート*** - すぐにアップデートを起動します。
- ***ヘルプ*** - スタート ページにヘルプ ファイルが開きます。

## 6.7. AVG ガジェット

***AVG ガジェット***は Windows デスクトップ (*Windows サイドバー*) に表示されます。このアプリケーションは Windows Vista と Windows 7 オペレーティング システムにのみ対応しています。***AVG ガジェット***を使用すると、スキャンや更新など最も重要な **AVG Internet Security 2011** 機能に簡単にアクセスできます。


***AVG ガジェット***には次のクイック アクセス オプションがあります。

- ***今すぐスキャン*** - [***今すぐスキャン***] リンクをクリックすると、***完全コンピュータ スキャン***を直接開始できます。ガジェットで表示されるユーザー インターフェースでスキャン処理の進行状況を確認できます。簡単な統計情報概要が表示され、スキャンされたオブジェクト、検出された脅威、修復された脅威の数に関する情報が示されます。スキャン中はいつでも、スキャン処理を一時停止または停止できます。スキャン結果に関する詳細データについては、標準の [***スキャン結果概要***] ダイアログを確認してください。このダイアログは [***詳細を表示***] オプションのガジェットから直接開くことができます (各スキャン結果は***サイドバー ガジェット スキャン***の下に一覧表示されます)。


- ***今すぐ更新*** - [***今すぐ更新***] リンクをクリックすると、ガジェットから直接 AVG 更新を実行できます。


- ***Twitter リンク*** - 新しい ***AVG ガジェット*** インターフェースが開き、Twitter に投稿される最新の AVG フィードの概要が表示されます。[***すべての AVG Twitter フィードを表示する***] リンクをクリックすると、インターネット ブラウザで新しいウィンドウが開き、Twitter Web サイトの AVG 関連ニュース ページに直接リダイレクトされます。


- ***Facebook リンク*** - インターネット ブラウザで Facebook Web サイトが開き、***AVG コミュニティ*** ページが表示されます。

- ***LinkedIn*** - このオプションはネットワーク インストールでのみ利用できます

(*AVG Business Edition ライセンスを使用して AVG をインストールした場合*)。LinkedIn ソーシャル ネットワークの ***AVG SMB Community*** でインターネット ブラウザが開きます。

- ***PC Analyzer***  - ***PC Analyzer***コンポーネントのユーザー インターフェースが開きます。
- ***検索ボックス*** - キーワードを入力すると、検索結果が既定の Web ブラウザで新しく開くウィンドウにただちに表示されます。

# 7. AVG コンポーネント

## 7.1. ウィルス対策

### 7.1.1. ウィルス対策の原理

ウイルス対策ソフトウェアのスキャン エンジンはすべてのファイルとファイル操作 (ファイルを開く/閉じるなど) をスキャンし、既知のウィルスの存在をチェックします。検出されたすべてのウイルスの動作はブロックされ、ウィルス自体は除去または隔離されます。大部分のウイルス対策ソフトウェアではヒューリスティック スキャンも使用されています。これにより、ファイルは一般的なウイルスの特性 (ウイルス シグネチャ) に基づいてスキャンされます。このため、新種のウィルスに既存のウィルスの一般的な特性が含まれる場合は、新種の未知のウィルスでもウィルス対策スキャナによって検出できます。

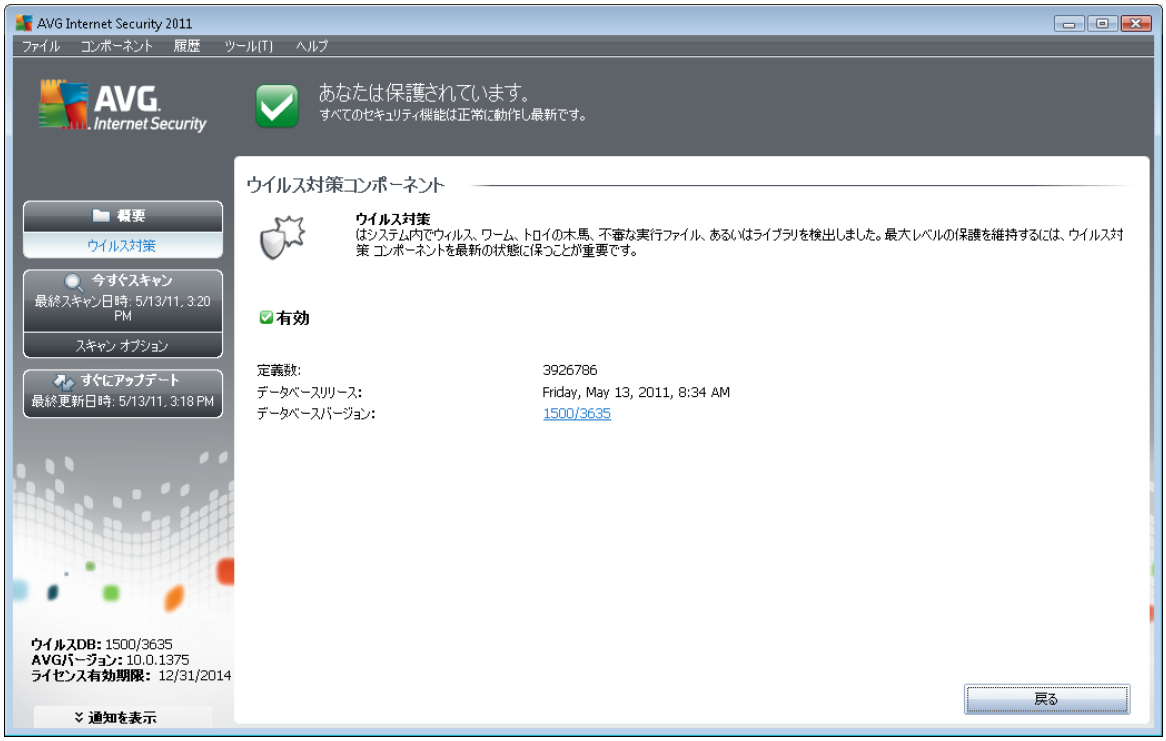
***ウイルス対策保護の重要な機能は、コンピュータ上での既知のウイルスの実行が防止されるという点です。***

1 つの技術だけではウイルスの検出や特定ができない場合、***ウイルス対策***は複数の技術を統合して、コンピュータがウイルスから保護されていることを保証します。

- スキャン - ウィルス特性文字列の検索
- ヒューリスティック分析 - 仮想コンピュータ環境におけるスキャン オブジェクト命令の動的エミューレーション
- 一般検出 - ウイルス/ウイルスグループの命令特性の検出

また、AVG はシステム内の不審な実行可能アプリケーションや DLL ライブラリの分析や検出もできます。このような脅威は不審なプログラムと呼ばれます (各種スパイウェア、アドウェアなど)。さらに、AVG はシステムレジストリをスキャンして、不審なエントリ、インターネット一時ファイル、tracking cookies の存在をチェックするため、あらゆる潜在的に有害なアイテムを他の感染と同様に処理できます。

### 7.1.2. ウイルス対策インターフェース




***ウイルス対策***コンポーネントのインターフェースには、コンポーネントの機能に関する基本情報、コンポーネントの現在のステータスに関する情報 (*ウイルス対策コンポーネントはアクティブです*)、な***ウイルス対策***統計情報の概要が表示されます。

- ***ウイルス定義数*** - ウイルス データベースの最新バージョンで定義されているウイルス数を示す番号が表示されます。
- ***データベース リリース*** - ウィルス データベースが最後に更新された日時を指定します。
- ***データベース バージョン*** - 現在インストールされているウィルス データベースのバージョン番号が表示されます。この番号はウィルス ベースが更新されるたびに増加します。

このコンポーネントのインターフェースで利用できる操作ボタンは 1 つです (***戻る***)。このボタンをクリックすると、既定の AVG ユーザー インターフェース (*コンポーネント概要*) に戻ります。

## 7.2. スパイウェア対策

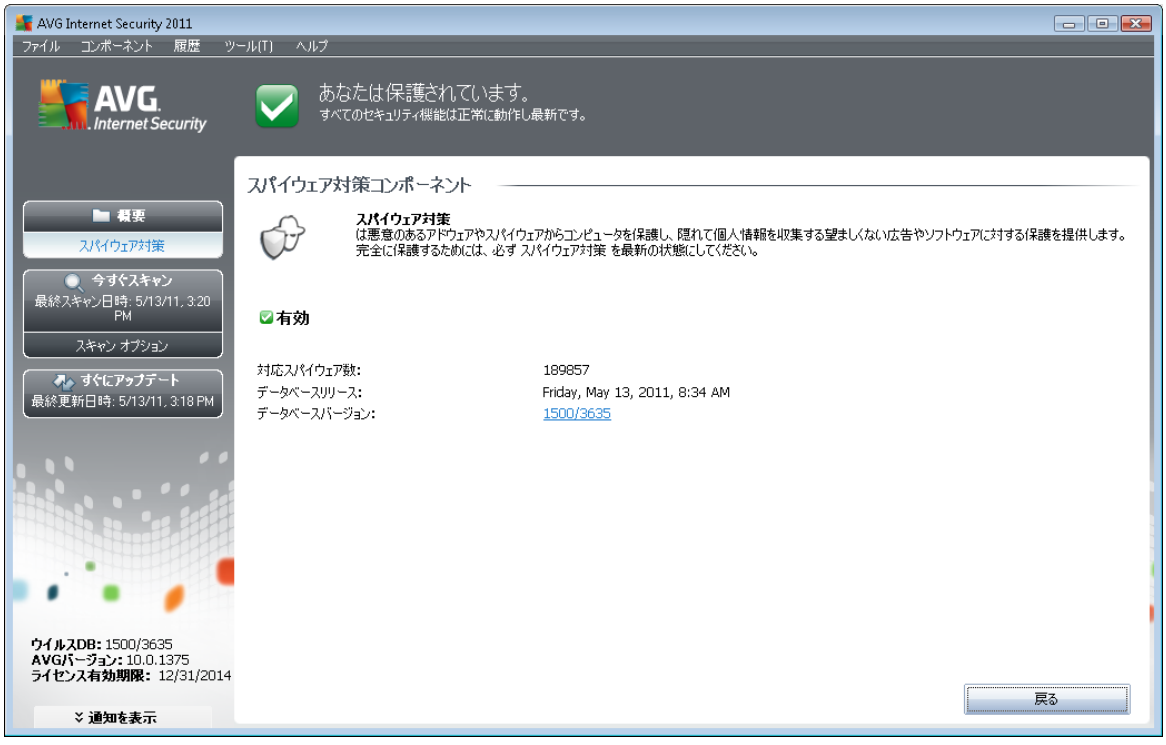
### 7.2.1. スパイウェア対策の原理

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

現在、最も一般的な感染原因は潜在的に危険な内容を含む Web サイトです。電子メールなどによる感染、ワームやウィルスによる感染なども広がりつつあります。最も効果的な保護方法は、常にバックグラウンド スキャナをオンにして、***スパイウェア対策***を使用することです。このコンポーネントは常駐シールドのように機能し、アプリケーションの実行時にバックグラウンドでスキャンします。

また、AVG のインストール前にマルウェアがコンピュータに侵入した場合や、最新のデータベースおよびプログラム更新を使用して **AVG Internet Security 2011** を最新の状態に維持していない場合も潜在的なリスクとして考えられます。このため、AVG のスキャン機能を使用してマルウェアやスパイウェアを検出できます。また、休止状態でアクティブではないマルウェアも検出されます。したがって、ダウンロードされた後アクティブ化されていないマルウェアも検出されます。

### 7.2.2. スパイウェア対策インターフェース




***スパイウェア対策***コンポーネントのインターフェースには、コンポーネントの機能に関する概要情報、コンポーネントの現在のステータスに関する情報、***スパム対策***統計情報が表示されます。

- ***スパイウェア定義数***- 最新のスパイウェア データベース バージョンで定義されたスパイウェア サンプル数が表示されます。

- ***データベース リリース*** - スパイウェア データベースが最後に更新された日時を指定します。
- ***データベース バージョン*** - 最新のスパイウェア データベース バージョン番号が表示されます。この番号はウィルス ベースが更新されるたびに増加します。

このコンポーネントのインターフェースで利用できる操作ボタンは 1 つです (***戻る***)。このボタンをクリックすると、既定の AVG ユーザー インターフェース (*コンポーネント概要*) に戻ります。

## 7.3. スパム対策

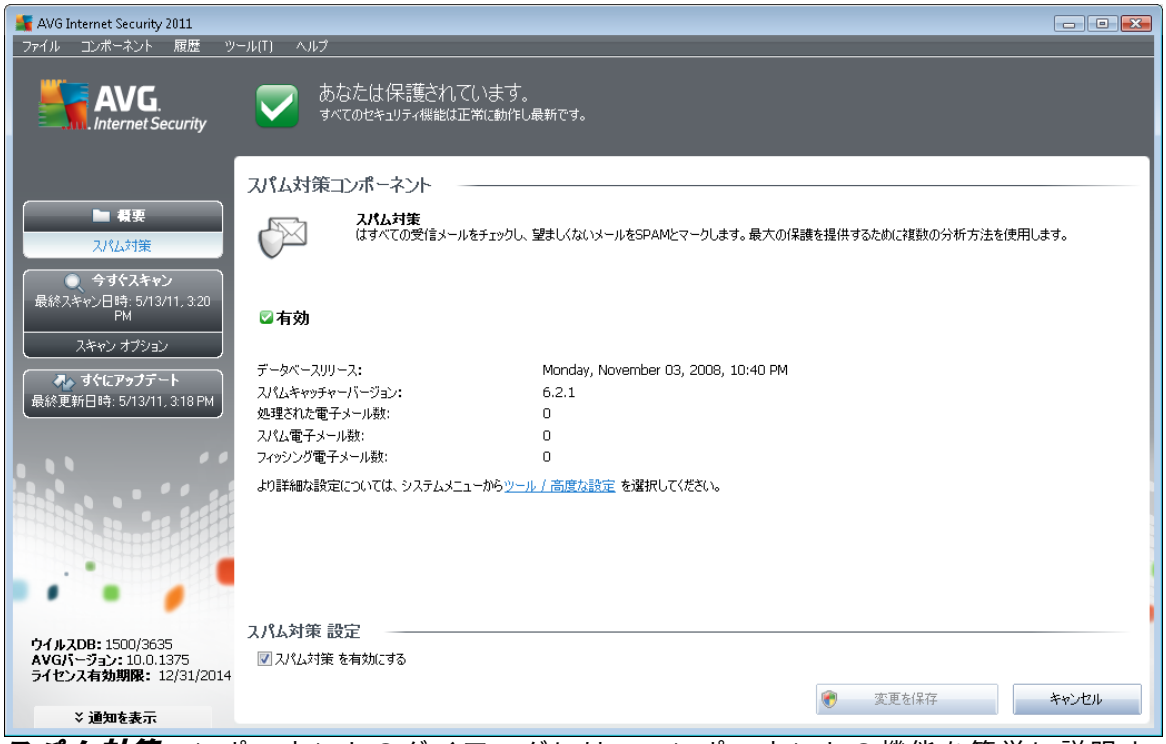
スパムとは、望まないメールであり、たいていは大量のメールアドレスに一度に送信され、受信者のメールボックスをいっぱいにする、製品やサービスの広告です。消費者が同意をした合法的な商業メールはスパムではありません。スパムは単に迷惑なだけではなく、しばしば詐欺、ウイルス、不快な内容を含んでいます。

### 7.3.1. スパム対策基本

***AVG Anti-Spam*** は、すべての受信メールをチェックし、望ましくないメールをSPAM とマークします。***AVG Anti-Spam*** は、特別なテキスト文字列を追加して、メールの件名（*スパムとして特定されたメール*）を修正できます。これで、メールクライアントでメールを簡単にフィルタリングできます。

***AVG Anti-Spam コンポーネントは、複数の分析手法を使用して各メールを処理し、最大限の保護を提供します。*** ***AVG Anti-Spam*** コンポーネントは、スパム保護のため、定期的にアップデートされるデータベースを使用します。また、RBL サーバー（*「既知のスパム送信者」メールアドレスの公開データベース*）を使用したり、手動でメールアドレスをホワイトリスト（*スパムとしてマークされない*）およびブラックリスト（*常にスパムとしてマーク*）に追加できます。

### 7.3.2. スパム対策インターフェース




***スパム対策***コンポーネントのダイアログには、コンポーネントの機能を簡単に説明するテキスト、現在のステータスに関する情報、次の統計情報が表示されます。

- ***データベース リリース***- スパム データベースが更新および発行された日時を指定します。
- ***Spamcatcher バージョン***- 最新のスパム対策エンジンのバージョンを表示します。
- ***処理された電子メール数*** - 前回のスパム対策 エンジンの起動以降にスキャンされた電子メール メッセージ数を指定します。
- ***スパム メール数*** - すべてのスキャンされた電子メールのうち、スパムとして判定されたメッセージ数を指定します。
- ***フィッシング メール数*** - すべてのスキャンされた電子メールのうち、フィッシングの試みとして割り当てられたメッセージ数を指定します。

[***スパム対策***] ダイアログには、[***ツール/高度な設定***] リンクも表示されます。このリンクをクリックすると、すべての **AVG Internet Security 2011** コンポーネントの高度な設定環境にリダイレクトされます。

***メモ:*** *すべての AVG コンポーネントはあらかじめ設定され、最適なパフォーマンスが保証されています。特に理由がない場合は、AVG の設定を変更しないでください。上級者ユーザーのみが設定変更を行うことをお進めします。*

このコンポーネントのインターフェースで利用できる操作ボタンは 1 つです (***戻る***)。このボタンをクリックすると、既定の AVG ユーザー インターフェース (*コンポーネント概要*) に戻ります。

## 7.4. ファイアウォール

ファイアウォールは、トラフィックをブロック、または許可することで、2つ以上のネットワーク間のアクセスコントロールポリシーを実行するためのシステムです。ファイアウォールにはルールセットを持っており、このルールは外部（一般的にはインターネットから）からの攻撃から内部ネットワークを保護し、あらゆるネットワークポート上のすべての通信をコントロールします。定義されたルールにしたがって、通信が評価され、許可、または禁止されます。ファイアウォールが侵入を検出すると、その通信を「ブロック」し、侵入者のコンピュータへのアクセスを許可しません。

ファイアウォールを設定して、定義されたポート経由および定義されたソフトウェアアプリケーションに対する内部/外部通信（双方向、受信、送信）を許可または禁止します。例えば、ファイアウォールを設定して、Microsoft Explorer を使用したウェブデータの送受信のみを許可することができます。その他のブラウザによるウェブデータの送信の試みはブロックされます。

ファイアウォールは、個人を特定できる情報が、コンピュータから許可なく送信されないように保護します。コンピュータが、インターネット上やローカルネットワーク上の他のコンピュータとデータを交換する方法をコントロールします。また、組織内では、ファイアウォールは、ネットワーク上の他のコンピュータからの内部ユーザーによる攻撃から、コンピュータを保護します。

***推奨：****一般には、個々のコンピュータで複数のファイアウォールを使用することは推奨されていません。コンピュータのセキュリティは複数のファイアウォールをインストールしても向上しません。;これらの2つのアプリケーションで競合が発生する可能性が高いです。したがって、コンピュータではファイアウォールを1つだけ使用し、他のすべてのファイアウォールを無効化して、起こりうる競合とそれに関する問題のリスクを排除することを推奨します。*

### 7.4.1. ファイアウォールの原理

AVGでは、***ファイアウォール***コンポーネントは、コンピュータのすべてのネットワークポート上のトラフィックをコントロールします。***ファイアウォール***は、定義されたルールに基づいて、コンピュータで実行中のアプリケーション、またはコンピュータに接続しようとする外部アプリケーションを評価します。これらのアプリケーションに関して、***ファイアウォール***はネットワークポートでの通信を許可、または禁止します。デフォルトでは、アプリケーションが不明な場合（定義された***ファイアウォール***ルールがない場合等）、***ファイアウォール***はその通信を許可するかブロックするかを確認します。

***注意：****AVG ファイアウォールはサーバープラットフォームには対応していません。*

**AVG ファイアウォールの機能：**

- 既知のアプリケーションの通信を自動的に許可、またはブロックするかどうかを確認します。

- 必要に応じて、予め定義されたルールを持つプロファイルを使用します。
- 様々なネットワークに接続したり、様々なネットワークアダプタを使用する際のプロファイルを自動的に切り替えます。

### 7.4.2. ファイアウォール プロファイル

***ファイアウォール***では、コンピュータがドメイン内にあるか、スタンドアロンか、ノートブックであるかに基づいて、特定のセキュリティルールを定義することができます。これらのオプションは、異なったレベルの保護を必要とし、レベルは該当するプロファイルによってカバーされています。***ファイアウォール***プロファイルは、予め定義された***ファイアウォール***コンポーネント設定です。

**利用可能なプロファイル**

- ***すべて許可 - あらかじめ設定され、常に存在するファイアウォール***システム プロファイルです。このプロファイルが有効化されると、すべてのネットワーク通信が許可されます。***ファイアウォール***保護がオフになった状態に近くなり、安全ポリシー ルールが適用されません *(すべてのアプリケーションは許可されますが、パケットは引き続きチェックされます。すべてのフィルターを完全に無効化するには、ファイアウォールを無効化する必要があります)*。システムプロファイルは複製、削除することができません。また設定を変更することもできません。
- ***すべてブロック - あらかじめ設定され、常に存在するファイアウォール***システム プロファイルです。このプロファイルが有効化されると、すべてのネットワーク通信はブロックされ、コンピュータは外部ネットワークからアクセスできなくなり、外部への通信もできなくなります。システムプロファイルは複製、削除することができません。また設定を変更することもできません。
- ***カスタムプロファイル***:
  - ***インターネットに直接接続*** - インターネットに直接接続する一般的なデスクトップ型家庭用コンピュータや安全な企業ネットワーク外のインターネットに接続するノート PC に適しています。家庭から接続している場合や、一元制御がない小規模企業ネットワークにいる場合に、このオプションを選択します。また、旅行中や、さまざまな不明で潜在的に危険な場所からノート PC で接続する場合にもこのオプションを選択します（*インターネットカフェ、ホテルの部屋など*). これらのコンピュータは追加の保護がなく、それゆえ最大限の保護を必要としていると想定されるため、より制限されたルールが作成されます。
  - ***ドメイン内のコンピュータ*** – 学校や会社のネットワーク等のローカルネットワーク内のコンピュータに適しています。ネットワークはいくつかの追加的な方法によって保護されていることが想定されるため、セキュリティレベルはスタンドアロンコンピュータよりも低い可能性があります。
  - ***ご家庭、または小規模オフィスのネットワーク*** – 家庭や小規模ビジネスのコンピュータに適しています。一般的には数台のコンピュータのみ

が接続されており、一元管理者はいません。

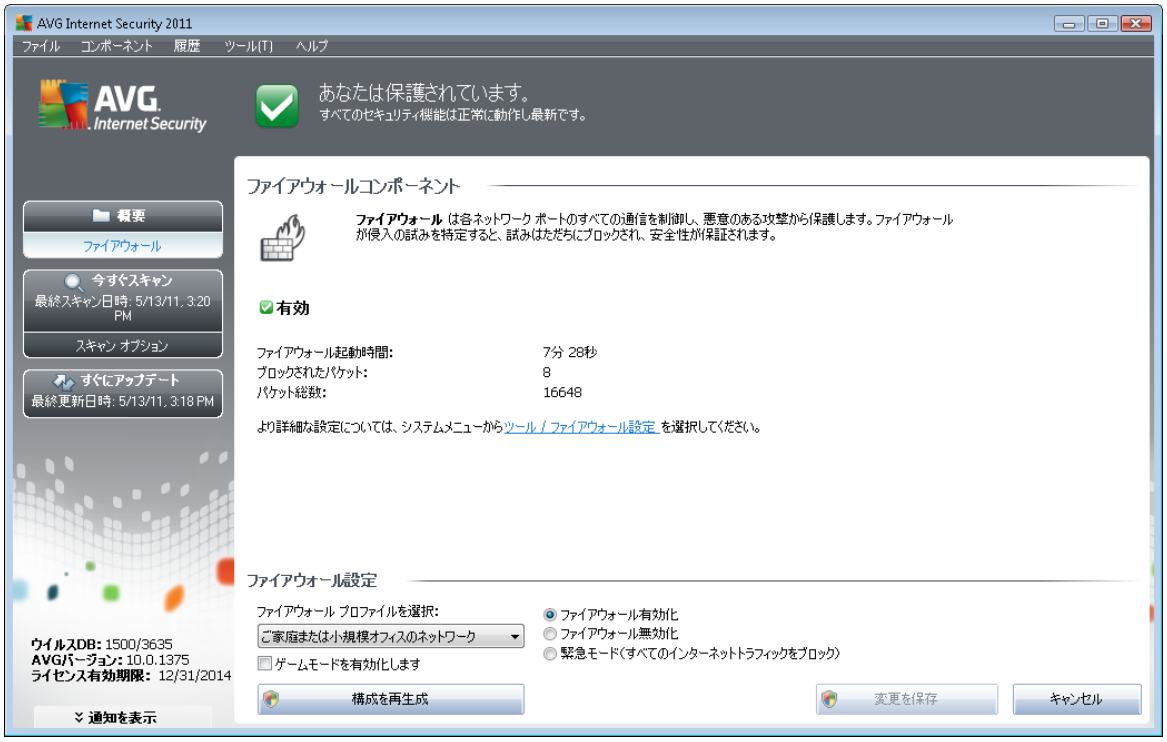
### プロファイル切り替え

プロファイル切り替え機能によって、あるネットワークアダプタを使用している時、またはある種類のネットワークに接続する時、***ファイアウォール***は自動的に定義済みプロファイルを切り替えることができます。ネットワークエリアにプロファイルが割り当てられていない場合、そのエリアへの次回の接続時に、***ファイアウォール***はプロファイルの割り当てを確認するダイアログを表示します。

すべてのローカル ネットワーク インターフェースにプロファイルを割り当てるか、または***エリアとアダプタ プロファイル***ダイアログで詳細設定を指定できます。このダイアログでは、使用しない機能を無効化することもできます（*すべての接続で、デフォルト プロファイルが使用されます*）。

通常、ノートブックを持ち、様々な種類の接続を行うユーザーにとってこの機能は役に立ちます。デスクトップコンピュータを持っている場合で、1種類の接続しか使用していない（*例えば、インターネットへのケーブル接続*）場合、プロファイル切り替えを行う必要はありません。

## 7.4.3. ファイアウォール インターフェース




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

- ファイアウォール起動時間 - ファイアウォールが最後に起動されてからの経過

時間

- ***ブロックされたパケット*** - ブロックされたパケット数
- ***パケット総数*** - ファイアウォール実行中にチェックされたすべてのパケット数

## ファイアウォール設定

- ***ファイアウォールプロファイルを選択*** - ロールダウンメニューから定義されたプロファイルを 1 つ選択します -*すべてを許可*、*すべてをブロック*の ***2 つのプロファイルは常に選択項目として表示されます***。他のプロファイルは [***ファイアウォール設定***] の [***プロファイル***] ダイアログで手動で追加されたものです。

- ***ゲーム モードを有効にする*** - このオプションにチェックを付けると、全画面アプリケーション (*ゲーム*、*プレゼンテーション*、*動画など*) を実行するときに、***ファイアウォール*** によって不明なアプリケーションの通信を許可するかブロックするかどうかを確認するダイアログが表示されません。不明なアプリケーションがネットワーク上で通信を試みる場合、***ファイアウォール***は現在のプロファイルの設定に応じて、自動的にその試みを許可あるいはブロックします。***メモ:*** ゲーム モードが有効になっている場合は、アプリケーションが終了するまで、すべてのスケジュール タスク (スキャン、更新) が延期されます。

- ***ファイアウォール ステータス*** :

  - ***ファイアウォールを有効にする*** - 選択した***ファイアウォール***プロファイルで定義されたルールセットに基づいて、アプリケーションの通信を許可します。

  - ***ファイアウォールを無効にする*** - このオプションは***ファイアウォール***を完全にオフに切り替えます。すべてのネットワークトラフィックは許可され、チェックされません。

  - ***緊急モード (すべてのインターネット トラフィックをブロック)*** - このオプションを選択すると、各ネットワーク ポートでのすべてのトラフィックをブロックします。***ファイアウォール***は実行中ですが、すべてのネットワークトラフィックは停止します。

***メモ:*** *すべての AVG コンポーネントはあらかじめ設定され、最適なパフォーマンスが保証されています。特に理由がない場合は、AVG の設定を変更しないでください。設定変更は、経験のあるユーザーが行うことを推奨します。AVG の設定を変更する必要がある場合、システム メニュー アイテムの****ツール/ファイアウォール設定****を選択し、****AVG ファイアウォール設定****ダイアログで設定を編集します。*

## コントロールボタン

- ***設定の再作成*** - このボタンをクリックすると、現在の***ファイアウォール***設定を上書きし、既定の自動検出設定に戻します。

- ***変更を保存*** - このボタンを押すと、ダイアログで行われた変更を保存、適用します。
- ***キャンセル*** - このボタンを押すと、デフォルトの***AVGユーザーインターフェース***（*コンポーネント概要*）に戻ります

## 7.5. リンクスキャナ

### 7.5.1. リンクスキャナの原理

***リンクスキャナ***は、ますます増加する一時的にしか存在しない 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。

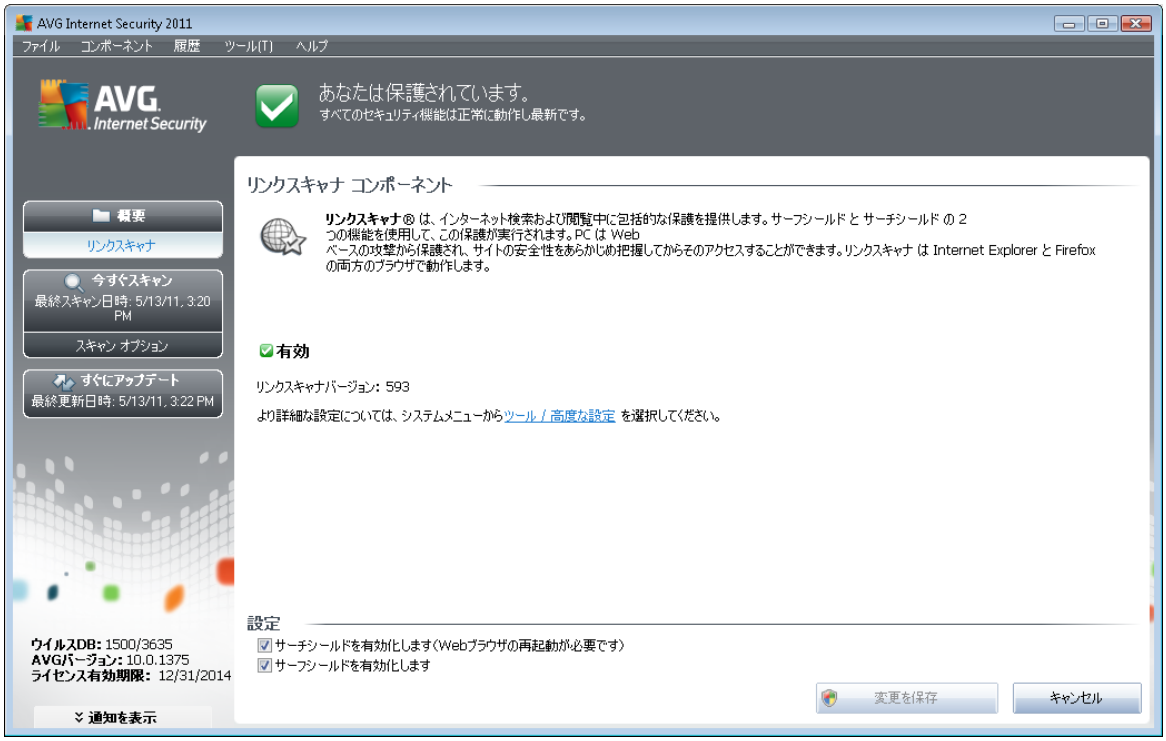
***リンクスキャナ***技術は、***サーチシールド***と***AVG アクティブ サーフ シールド***の 2 つの機能から構成されています。

- ***サーチ シールド***には、危険性が確認されている Web サイト (*URL アドレス*) のリストが含まれています。Google、Yahoo! JP、Yahoo!、WebHledani、Yandex、Baidu、Bing、AOL、AltaVista、EarthLink、Ask、Seznam、eBay、Twitter、Digg、SlashDot で検索を実行すると、このリストに従ってすべての検索結果がチェックされ、判定アイコンが表示されます (*Yahoo! の検索結果の場合、「エクスプロイトに感染した Web サイト」 判定アイコンのみが表示されます*)。
- ***サーフ シールド***は Web サイト アドレスに関係なく、アクセスしようとしている Web サイトのコンテンツをスキャンします。***サーチ シールド***で検出されない Web サイト (*新しい悪意のある Web サイトが作成された、以前に安全であった Web サイトに今はマルウェアが含まれているなど*) にアクセスを試みると、***サーフ シールド***によってブロックされます。

***メモ:*** *リンクスキャナはサーバー プラットフォームに対応していません。*

### 7.5.2. リンクスキャナ インターフェース

***リンクスキャナ***コンポーネント インターフェースには、コンポーネント機能の概要説明と現在のステータスに関する情報が表示されますさらに、最新の***リンクスキャナ*** データベース バージョン番号 (*リンクスキャナ バージョン*) に関する情報を表示できます。




## リンクスキャナ設定

ダイアログの下部の一部のオプションは編集できます。

- ***サーチ シールド***を有効にする - (*既定ではオン*): Google、Yahoo! JP、WebHledani、Yandex、Baidu、Bing、AOL、AltaVista、EarthLink、Ask、Seznam、eBay、Twitter、Digg、SlashDot を使用して実行した検索結果に対して評価通知アイコンが表示されます。検索エンジンで返されたサイトの内容が事前にチェックされます。

- ***サーフ シールド***を有効にする - (*既定ではオン*): ユーザーがサイトにアクセスしようとするときに、積極的に*リアルタイム*でエクスプロイト サイトを検出し、保護を実施します。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。

### 7.5.3. サーチ シールド

***サーチシールド***をオンにしてインターネットを検索すると、最も一般的な検索エンジン (*Google*、*Yahoo! JP*、*WebHledani*、*Yandex*、*Baidu*、*Bing*、*AOL*、*AltaVista*、*EarthLink*、*Ask*、*Seznam*、*eBay*、*Twitter*、*Digg*、*SlashDot*) の検索結果すべてが評価され、危険なリンクか疑わしいリンクかどうかが判定されます。これらのリンクをチェックし、悪意のあるリンクとして判定されると、***AVG リンク スキャナ***は、危険、または疑わしいリンクをクリックする前に警告を表示します。したがて、安全なウェブサイトにのみアクセスすることが保証されます。

検索結果ページのリンクが評価されている間、リンクの隣にリンク検証が実行中であることを示すアイコンが表示されます。判定が終了すると、各情報アイコンが表示されます。

リンクされたページは安全です (*このアイコンは安全な Yahoo! JP 検索結果*については表示されません)。

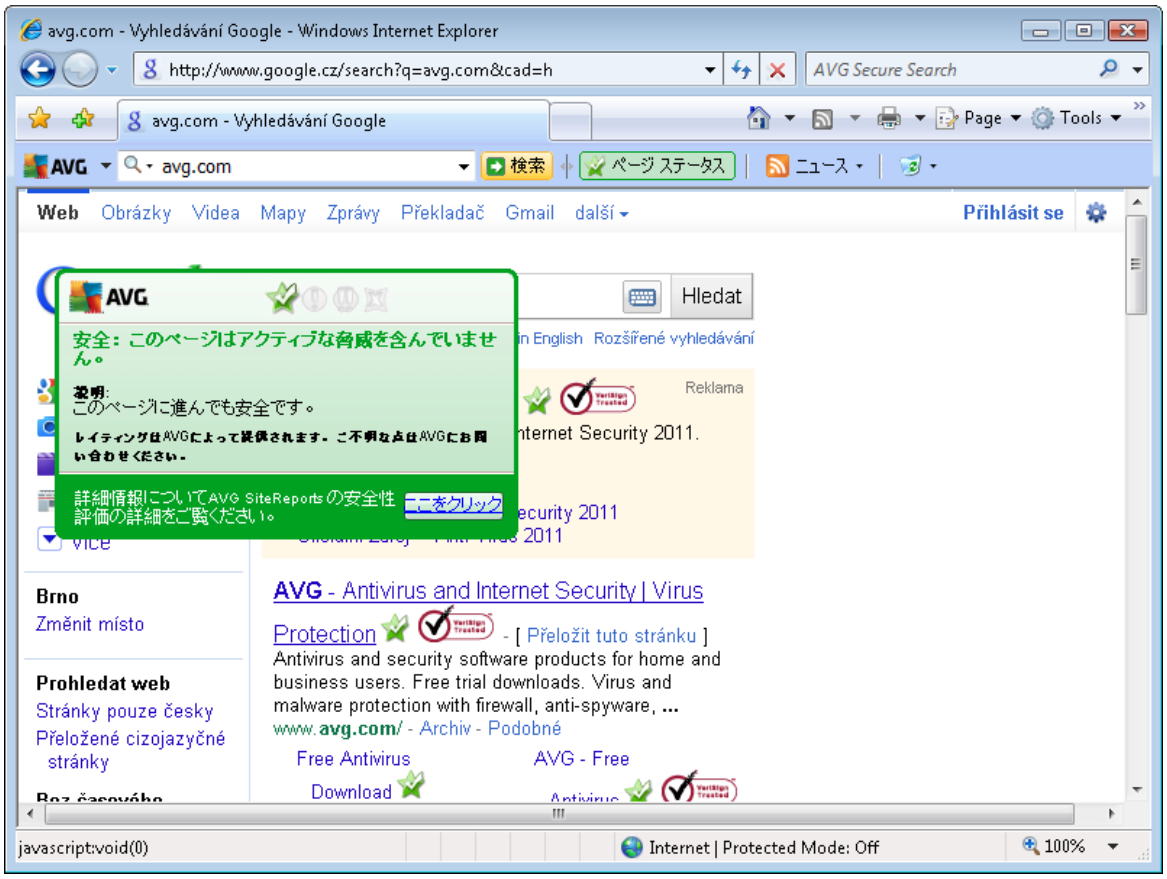
リンクされたページは脅威を含んでいませんが、疑わしいコンテンツを含みます（*または目的が疑わしいため、電子ショッピングが推奨されないなど*）。).

リンクされたページはそれ自体安全ですが、明らかに危険なページへのリンクを含んでいます。あるいは、現段階では脅威ではないものの、疑わしいコードを含んでいます。

リンクされたページはアクティブな脅威を含んでいます。安全のために、このページへのアクセスは禁止されています。

リンクされたページは、アクセスできないかスキャンできませんでした。

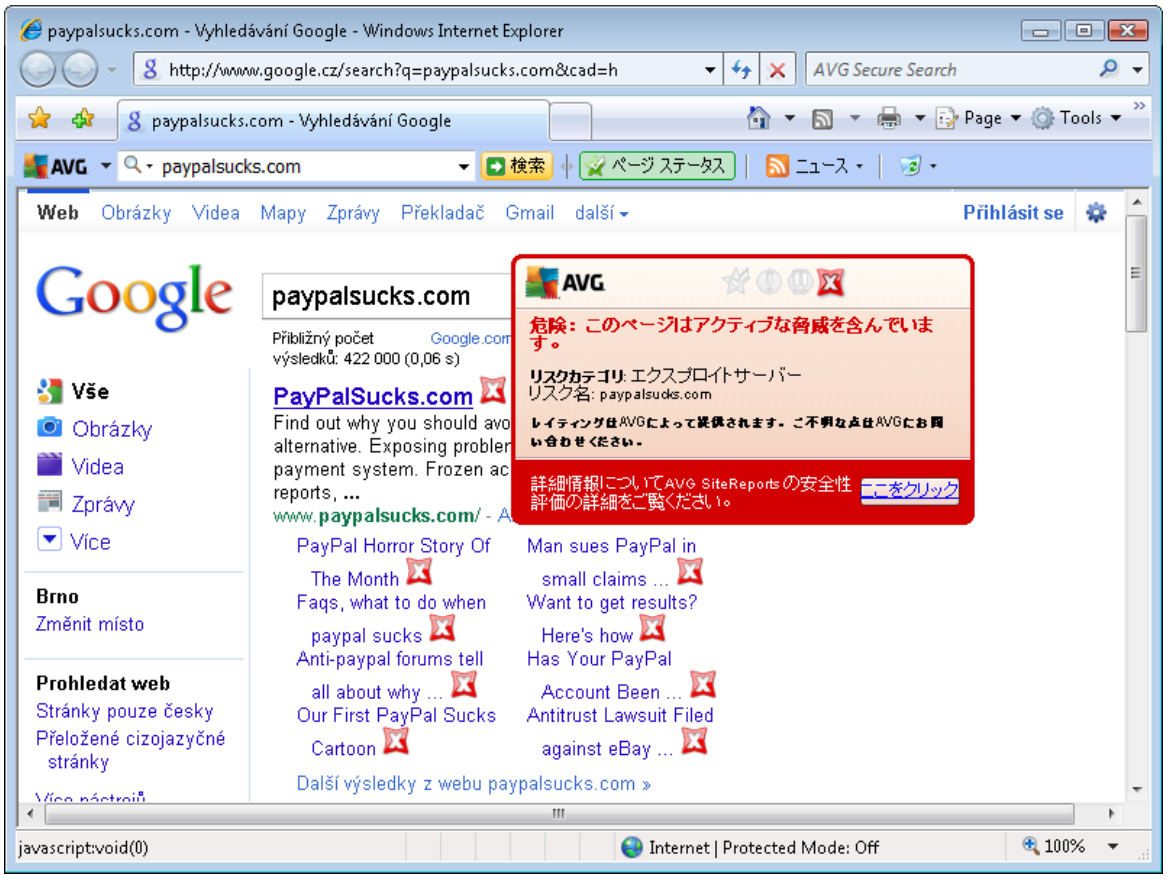
個々の評価アイコンは、問題のあるリンクに関する詳細を表示します。脅威の詳細情報 (*提供されている場合*) が含まれます。



### 7.5.4. サーフ シールド

この強力な保護は開こうとするWebページの悪意のある内容をブロックし、コンピュータへのダウンロードを防止します。この機能が有効化されていると、危険なサイトへのリンクをクリックしたり、URLを入力したりすると、自動的にWebページを開かないようにブロックし、不注意な感染から保護します。エクスプロイト Web ページは、単にサイトにアクセスするだけでコンピュータが感染する可能性があります。エクスプロイトや他の深刻な脅威を含む Web ページにアクセスする際、***AVG リンクスキャナ***は、これらのページを表示させません。

悪意のあるWebサイトに遭遇した場合、***AVG リンクスキャナ***は以下のような画面で警告を表示します。




***このようなウェブサイトへのアクセスは非常に危険であり、お勧めしません。***

## 7.6. 常駐シールド

### 7.6.1. 常駐シールドの原理

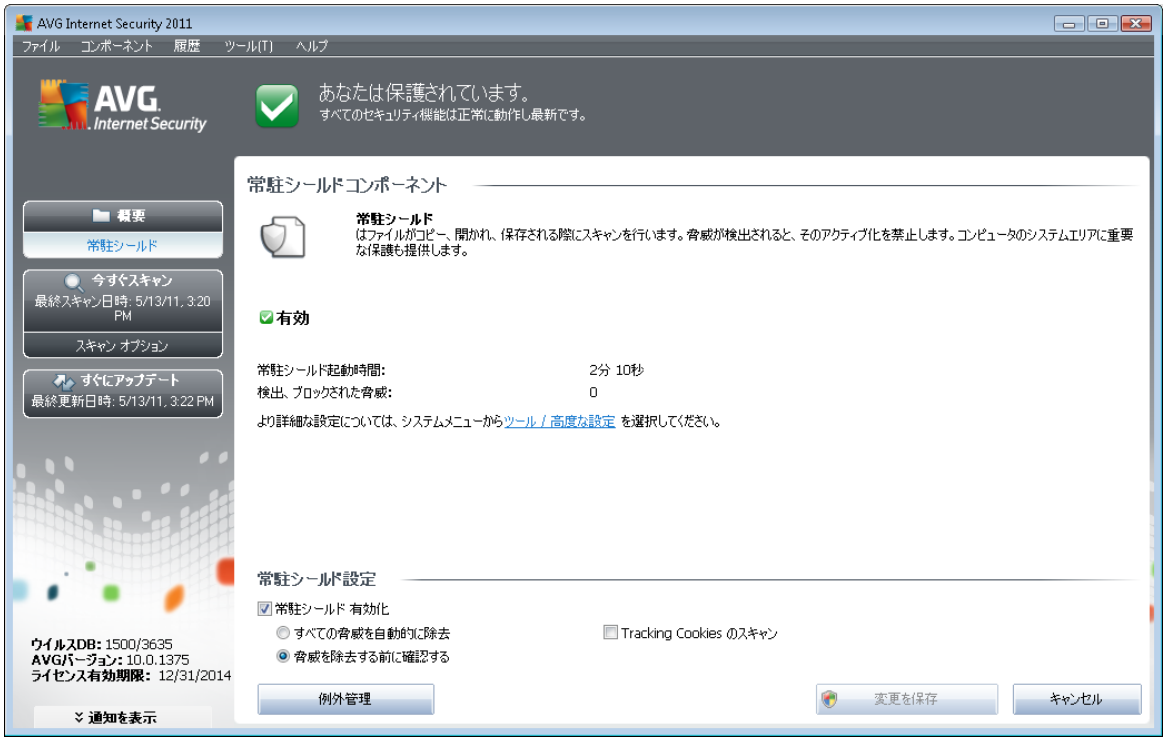
***常駐シールド***コンポーネントはコンピュータに継続した保護を提供します。開く、保存、コピー処理対象となるすべてのファイルをスキャンすることで、コンピュータのシステム領域を保護します。***常駐シールド***がアクセスされるファイルにウイルスを検出する場合、現在実行されている操作を停止し、ウイルスが活性化しないようにします。通常、「バックグラウンド」で実行されるため、このプロセスに気づくことはありません。脅威が検出された場合のみ通知されます。同時に、常駐シールドは脅威のアクティブ化をブロックし、それを除去します。***常駐シールド***は、システムの起動中にコンピュータメモリにロードされます。

常駐シールドでできること：

- 脅威のスキャン
- リムーバル メディアのスキャン (フラッシュ ディスクなど)
- 特定の拡張子を持つファイルや拡張子のないファイルのスキャン
- スキャン例外の設定 – スキャンされない特定のファイルやフォルダ

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

### 7.6.2. 常駐シールド インターフェース




***常駐シールド***機能の概要とコンポーネント ステータス情報だけではなく、***常駐シールド*** インターフェースには統計情報データも表示されます。

- ***常駐シールド実行時間*** - コンポーネントが起動している時間
- ***検出およびブロックされた脅威*** - 検出後に実行や開く操作がブロックされた感染の数 (*統計目的など必要に応じてこの値をリセットできます - 値のリセット*)。

## 常駐シールド設定

ダイアログの下部には [***常駐シールド設定***] セクションがあります。ここではコンポーネントの機能の基本設定 (*他のコンポーネントと同様にシステム メニューのファイル/高度な設定*で詳細設定が可能です) を編集できます。

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

o 自動 (***すべての脅威を自動的に除去***)

o あるいはユーザー許可の後のみ (***脅威を削除する前に確認する***)

この選択はセキュリティ レベルに影響しません。

いずれの場合も、***Tracking Cookie*** をスキャンするかどうかを選択できます。必要に応じてこのオプションをオンにして、セキュリティ レベルを最大限に変更できます。既定ではオフになっています。（*cookie とはサーバーから Web ブラウザに送信され、そのサーバーにアクセスするたびにブラウザによって変更されずに返信されるテキストのことです。HTTP cookie は認証トラッキング、サイトの好み、電子ショッピング カートの内容といったユーザーに関する特定の情報を保持するために使用されます*）。

***メモ:*** *すべての AVG コンポーネントは最適なパフォーマンスを実現できるようにあらかじめ設定されています。特に理由がない場合は AVG の設定を変更しないでください。設定変更は上級者ユーザーが行うことをお勧めします。AVG の設定を変更する必要がある場合は、システム メニュー項目の [****ツール/高度な設定****] を選択し、[AVG 高度な設定ダイアログで設定を編集します。*

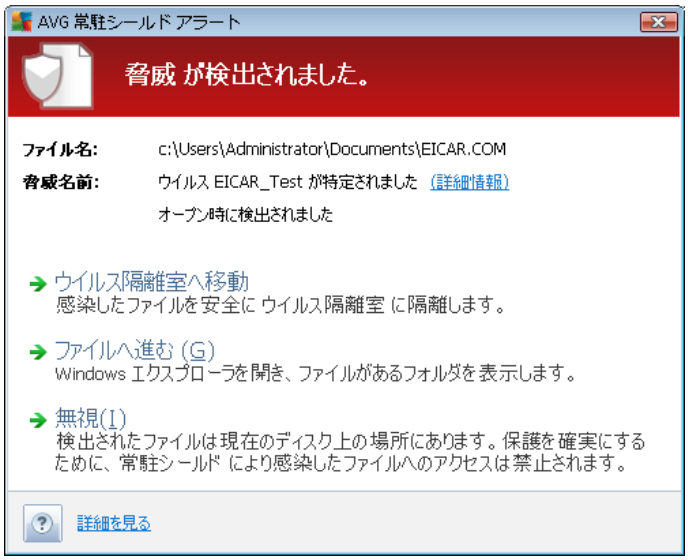
## コントロール ボタン

***常駐シールド*** インターフェースで利用できるコントロール ボタンは次のとおりです。

- ***例外の管理*** - [***常駐シールド - 例外ディレクトリ***] ダイアログが開きます。このダイアログでは、***常駐シールド*** スキャンから除外するフォルダとファイルを定義します。
- ***変更の保存*** - このボタンをクリックすると、ダイアログで行われた変更を保存して適用します。
- ***キャンセル*** - このボタンをクリックすると、既定の ***AVG ユーザー インターフェース*** (*コンポーネント概要*) に戻ります。

### 7.6.3. 常駐シールド検出

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




警告ダイアログでは、検出され感染と判定されたファイルに関するデータ (*ファイル名*)、認識された感染名 (*脅威名*)、既知の脅威の場合に検出された脅威に関する詳細情報を確認できる (*詳細情報*) ***ウィルス エンサイクロペディア*** へのリンクが表示されます。

さらに、この時点で実行するアクションを選択する必要があります。次の選択肢があります。

***特定の条件 (感染したファイルの種類やファイルの場所) によっては、利用できないオプションがあります。***

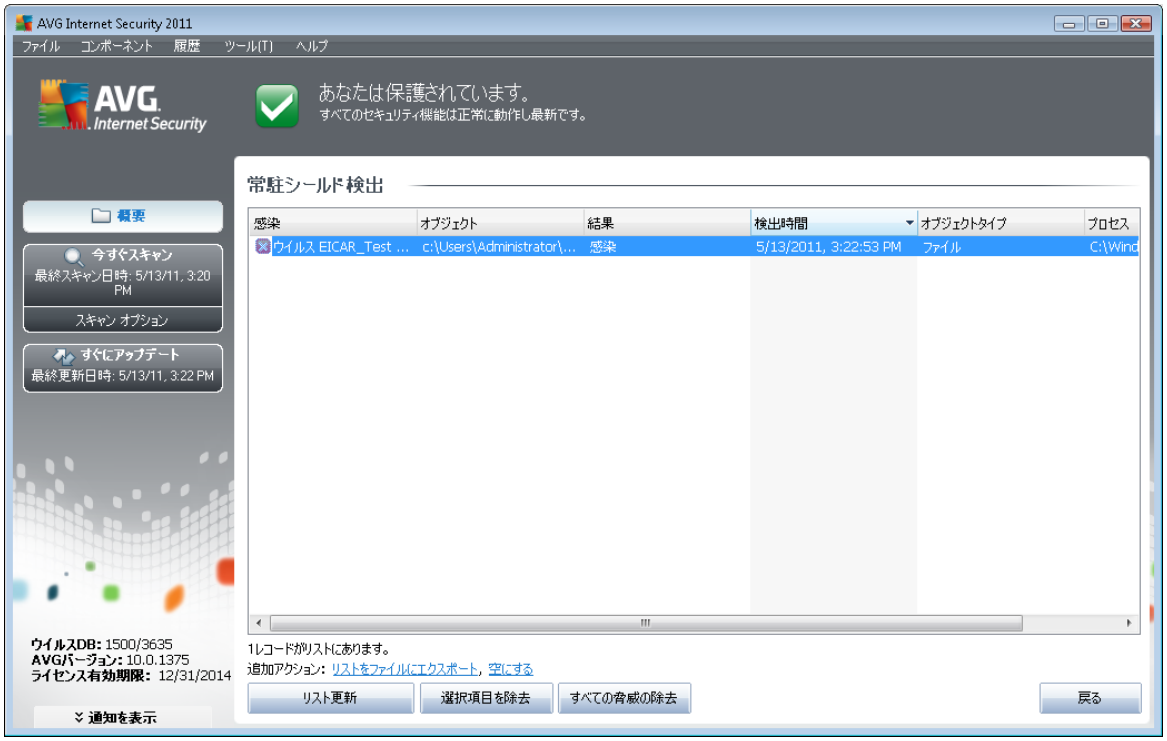
- ***パワーユーザーとして脅威を除去*** – 一般ユーザーとして脅威を除去する権限がない場合はボックスにチェックをします。パワーユーザーにはより強いアクセス権限があります。脅威がシステムフォルダにある場合等、このチェックボックスを使用して除去する場合があります。
- ***修復*** - 検出された感染が修復可能な場合にのみこのボタンが表示されます。これで感染がファイルから削除され、ファイルが元の状態に復元されます。ファイル自体がウィルスでアル場合は、この機能を使用してウィルスを削除 (***ウィルス隔離室に移動***) します。
- ***ウイルス隔離室に移動*** - ウイルスは AVG ***ウイルス隔離室に移動します。***
- ***ファイルに移動*** - このオプションは不審なオブジェクトの正確な場所に移動します（*新しい Windows Explorer ウィンドウを開きます*）
- ***無視*** - しかるべき理由がない場合は、このオプションを使用しないでくださ

い。

***メモ:*** *検出されたオブジェクトのサイズがウィルス隔離室の空き領域上限サイズ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ィ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、ウィルス隔離室のサイズを変更することができます。ウィ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。ウィルス隔離室のサイズを増やすには、[AVG 高度な設定] の [ウィルス隔離室サイズの上限] オプションを使用して [ウィルス隔離室] 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、ポップアップ 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***によって検出されたすべての脅威の概要は、システム メニュー オプションの [***履歴/常駐シールド検出***] の [***常駐シールド検出***] ダイアログに表示されます。




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

- ***感染*** - 検出されたオブジェクトの説明（可能な場合は名前も）
- ***オブジェクト*** - オブジェクトの場所
- ***結果*** - 検出されたオブジェクトで実行されたアクション

- ***検出時刻*** - オブジェクトが検出された日時
- ***オブジェクトタイプ*** - 検出されたオブジェクトの種類
- ***プロセス*** - 呼び出すために実行されたアクション

ダイアログの下部では、リストの下に上記でリストされた検出オブジェクトの総数に関する情報が表示されます。さらに、検出オブジェクトの完全なリストをファイルにエクスポート（***ファイルにエクスポート***）し、検出オブジェクトのすべてのエントリを削除（***リストを空にする***）することができます。[***リストを更新***] ボタンは***常駐シールド***の検出結果リストを更新します。[***戻る***] ボタンをクリックすると、既定の ***AVG ユーザー インターフェース*** （*コンポーネント概要*）に戻ります。

## 7.7. ファミリー セーフティ

***AVG Family Safety*** は不適切な Web サイト、メディア コンテンツ、オンライン検索から子供を守り、オンライン活動に関するレポートを提供します。子供に合わせて適切な保護レベルを設定し、一意のログイン ID で個別に監視します。

このコンポーネントは ***AVG Family Safety*** 製品がコンピュータにインストールされている場合にのみ有効です。***AVG Family Safety*** 製品がインストールされていない場合は、**AVG Internet Security 2011** ユーザー インターフェースのアイコンをクリックすると、製品の Web サイトに移動します。ここで詳細情報を確認できます。

## 7.8. AVG LiveKive

***AVG LiveKive*** は自動的にすべてのファイル、写真、音楽を安全な場所にバックアップします。家族や友人と共有したり、iPhone や Android デバイスなどのあらゆる Web 対応デバイスからアクセスしたりできます。

このコンポーネントは ***AVG LiveKive*** 製品がコンピュータにインストールされている場合にのみ有効です。***AVG LiveKive*** 製品がインストールされていない場合は、**AVG Internet Security 2011** ユーザー インターフェースのアイコンをクリックすると、製品の Web サイトに移動します。ここで詳細情報を確認できます。

## 7.9. メール スキャナ

最も一般的なウイルスとトロイの木馬の感染源の一つはメールです。フィッシング、スパムはメールをさらに大きなリスクソースとします。無料メールアカウントは、さらにこのような悪意のあるメールを受信する可能性が高くなり（*これらはめったにスパム対策技術を導入していないため*）、かなりのホームユーザーはこのようなメールを利用しています。また、ホームユーザーは、不明なサイトをインターネットサーフィンしたり、個人情報（*メールアドレスなど*）を含むオンラインフォームに情報を入力し、メールを介しての攻撃にさらされる機会を増やします。会社は、通常会社のメールアカウントを使用し、スパム対策フィルタ等を導入してリスクを削減します。

### 7.9.1. メール スキャナの原理

***パーソナル電子メール スキャナ*** コンポーネントは、送受信メールを自動的にスキャンします。このコンポーネントは独自の AVG プラグインがない電子メール クライアントで使用できます (*Microsoft Outlook や The Bat など特定のプラグインを提供することで、AVG がサポートしている電子メール クライアントで電子メール メッセージをスキャンする場合にも使用できます*)。このコンポーネントは、主に Outlook Express、Mozilla、Incredimail などの電子メール アプリケーションで使用することを想定しています。

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

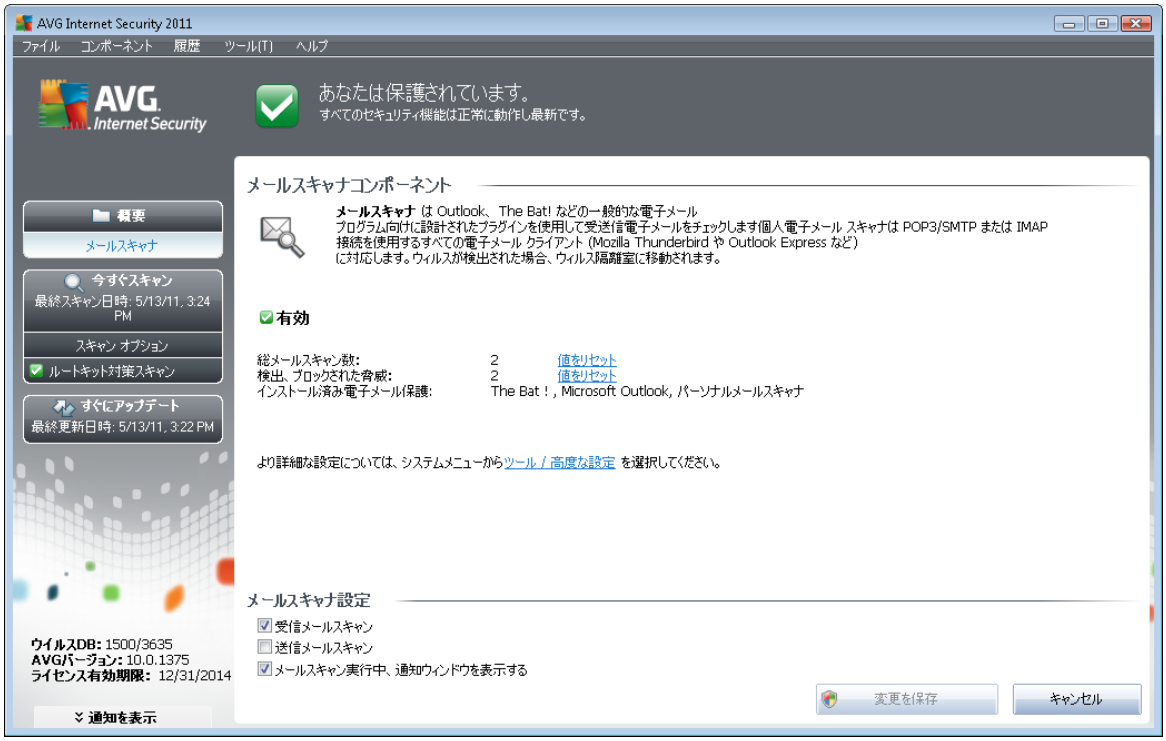
***パーソナルメールスキャナ***はメールクライアントとインター―ネット上のメールサーバーのインターフェースとして動作します。

- ***受信メール：***サーバーからメッセージを受信している間、***メールスキャナ***コンポーネントはウイルススキャンを行い、感染した添付ファイルを削除し、証明書を追加します。検出されたウイルスは、即時に***ウイルス隔離室***に隔離されます。次にメッセージはメールクライアントに渡されます。

- ***送信メール：***メールクライアントからメールスキャナにメッセージが送信されます。メッセージと添付ファイルはウイルススキャンされ、その後にメッセージが SMTP サーバーに送信されます（*送信メールのスキャンは既定では無効で、手動で設定できます*）。

***注意：****AVG メールスキャナはサーバープラットフォームには対応していません。*

### 7.9.2. メール スキャナ インターフェース




電子メール スキャナ コンポーネントのダイアログには、コンポーネントの機能を簡単に説明するテキスト、現在のステータスに関する情報、次の統計情報が表示されます。

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

#### メール スキャナ設定

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

- ***受信メッセージのスキャン*** - アイテムをチェックすると、すべてのアカウントに送信されたメールがウイルススキャンされるように指定できます。既定では、このアイテムはオンです。この設定を変更しないことをお勧めします。
- ***送信メールスキャン*** - このアイテムにチェックを付けると、アカウントから

の送信されるすべてのメールのウイルススキャンが実行されるようになります（既定ではこのアイテムはオフになっています

- ***電子メールのスキャン中に通知アイコンを表示する*** - この項目にチェックを付けると、電子***メール スキャナ***コンポーネントで電子メールをスキャンしているときに、システム トレイの AVG アイコン上の通知ダイアログに通知メッセージが表示されます。既定では、このアイテムはオンです。この設定を変更しないことをお勧めします。

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

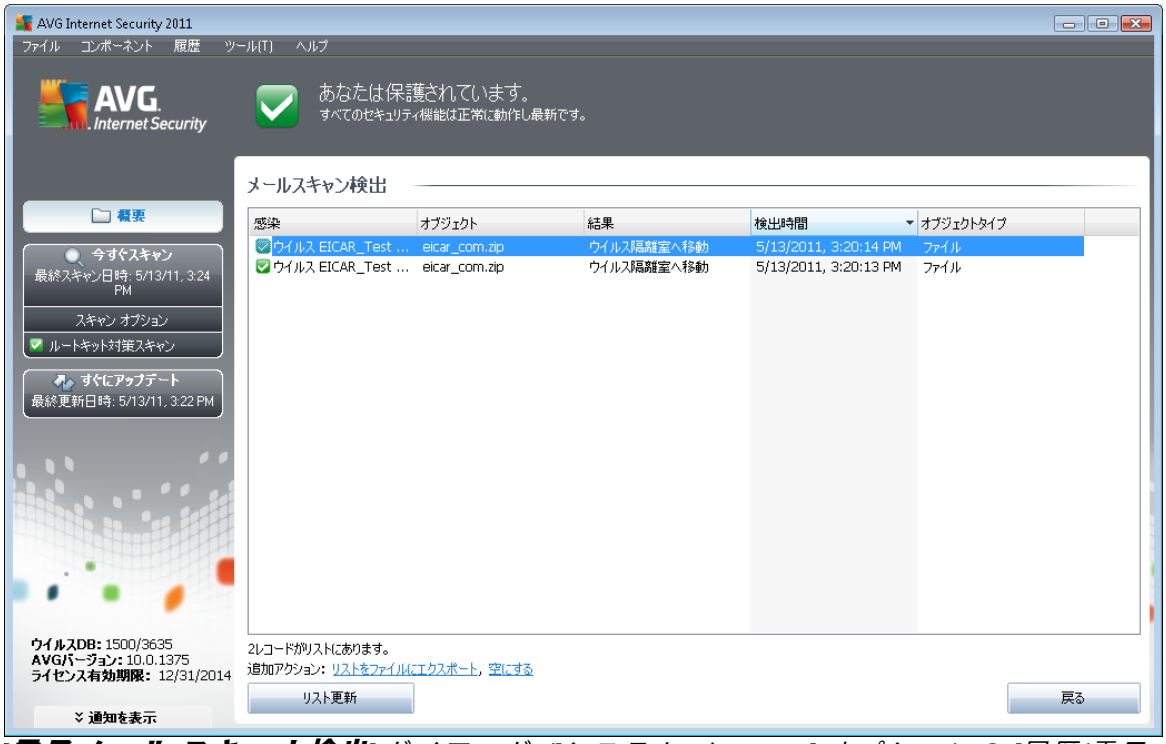
***注意：****すべてのAVGコンポーネントは、最適なパフォーマンスを提供するようにあらかじめ設定されています。特に理由がない場合は AVG の設定を変更しないでください。設定変更は上級者ユーザーが行うことをお勧めします。AVG の設定を変更する必要がある場合は、システム メニュー項目の [****ツール/高度な設定****] を選択し、[AVG 高度な設定ダイアログで設定を編集します。*

## コントロールボタン

***メールスキャナ***インターフェースで利用できるコントロールボタンは以下の通りです。

- ***変更の保存*** - このボタンをクリックすると、ダイアログで行われた変更を保存して適用します。
- ***キャンセル*** - このボタンをクリックすると、既定の ***AVG ユーザー インターフェース*** (*コンポーネント概要*) に戻ります。

### 7.9.3. メール スキャナ検出




[***電子メール スキャナ検出***] ダイアログ (*[システム メニュー] オプションの [履歴/電子メール スキャナ検出] からアクセスできます*) では、***電子メール スキャナ*** コンポーネントによって検出されたすべての結果リストが表示されます。検出された各オブジェクトについて、以下の情報が提供されます。

- ***感染*** - 検出されたオブジェクトの説明（可能な場合は名前も）
- ***オブジェクト*** - オブジェクトの場所
- ***結果*** - 検出されたオブジェクトで実行されたアクション
- ***検出時刻*** - 不審なオブジェクトが検出された日時
- ***オブジェクトタイプ*** - 検出されたオブジェクトの種類

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

#### コントロールボタン

***メールスキャナ検出***インターフェースで利用できるコントロールボタンは以下の通りです。

- ***リストを更新*** - 検出された脅威のリストの更新
- ***戻る*** - 最初に表示していたダイアログに戻ります。

## 7.10. アップデート マネージャ

### 7.10.1. アップデート マネージャの原理

更新が定期的に実行されていない場合、セキュリティ ソフトウェアは脅威からの保護を保証できません。ウイルス作成者はソフトウェアとオペレーティング システムの両方の欠陥を常に探して、それを利用しようとしています。新しいウイルス、新しいマルウェア、新しいハッキング攻撃は日々出現しています。このため、ソフトウェア ベンダーは更新とセキュリティ 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。

***AVG を定期的に更新することは非常に重要です。***

***更新マネージャ***を使用することで定期的な更新を管理できます。このコンポーネントでは、インターネットまたはローカル ネットワークからの更新ファイルの自動ダウンロードをスケジュールできます。可能な限り、ウイルス定義更新を毎日実行してください。緊急度の低いプログラム更新は週次で実行してもかまいません。

***メモ:*** *更新の種類とレベルの詳細については、「AVG 更新」の章を参照してください。*

### 7.10.2. アップデート マネージャ インターフェース

***アップデート マネージャ*** のインターフェースにはコンポーネントの機能、現在のステータスに関する情報、関連統計情報データが表示されます。

- ***前回の更新*** - 前回のデータベース更新日時を指定します。
- ***ウィルス データベース バージョン*** - 現在インストールされているウィルス データベースのバージョン番号が表示されます。この番号はウィルス ベースが更新されるたびに増加します。
- ***次回のスケジュール更新*** - 次回のデータベース更新日時を指定します。

## アップデート マネージャ設定

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

さらに、アップデートが起動するタイミングを指定することができます。

- o ***定期的***- 時間間隔を定義します。
- o ***指定した間隔*** - 更新を実行する正確な日時を定義します。

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

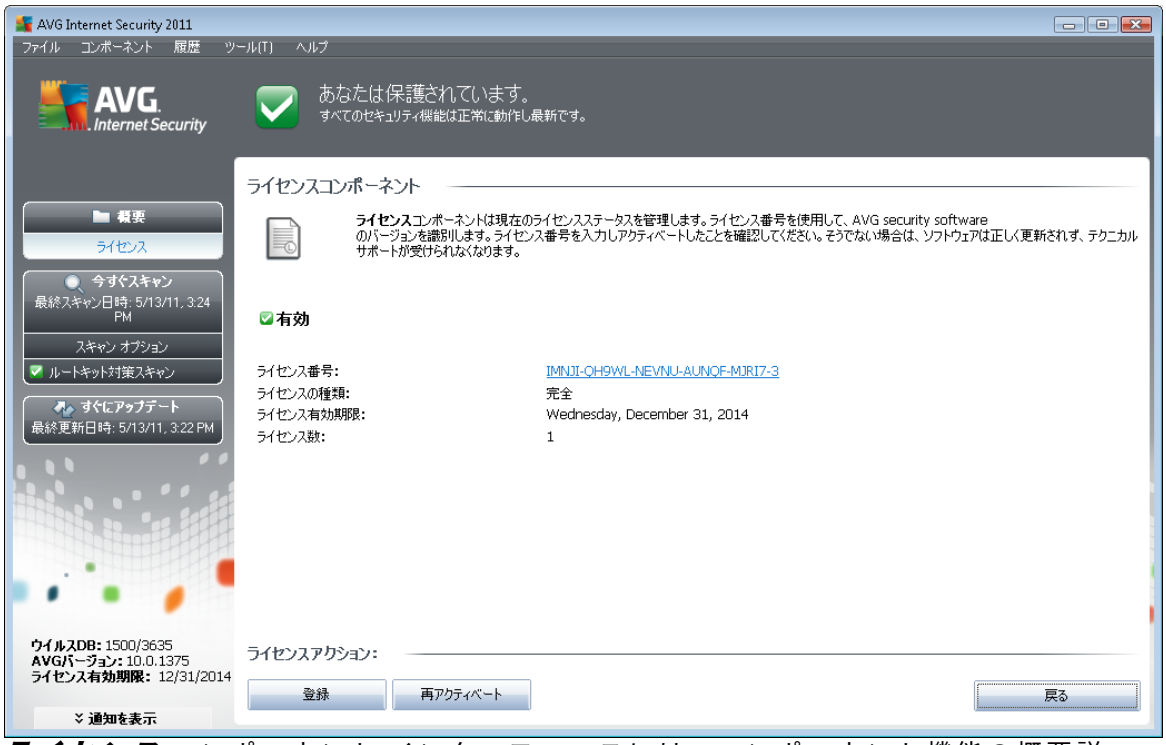
***注意：****すべてのAVGコンポーネントは、最適なパフォーマンスを提供するようにあらかじめ設定されています。特に理由がない場合は AVG の設定を変更しないでください。設定変更は上級者ユーザーが行うことをお勧めします。AVG の設定を変更する必要がある場合は、システム メニュー項目の [**ツール/高度な設定**] を選択し、[AVG 高度な設定ダイアログで設定を編集します。*

## コントロールボタン

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

- ***すぐにアップデート***- オンデマンドで即時アップデートを実行します。
- ***変更の保存*** - このボタンをクリックすると、ダイアログで行われた変更を保存して適用します。
- ***キャンセル*** - このボタンをクリックすると、既定の ***AVG ユーザー インターフェース*** (*コンポーネント概要*) に戻ります。

## 7.11. ライセンス




***ライセンス*** コンポーネント インターフェースには、コンポーネント機能の概要説明、現在のステータスに関する情報、および次の情報が表示されます。

- ***ライセンス番号*** - ライセンス番号の一部が表示されます (*セキュリティ上の理由から、最後の 4 文字は表示されません*)。ライセンス番号は正確に表示されているとおりに入力する必要があります。このため、ライセンス番号を誤って入力しないように、「コピーと貼り付け」を必ず使用することを強くお勧めします。
- ***ライセンス タイプ*** - インストールされている製品のタイプを指定します。
- ***ライセンス有効期限*** - この日付はライセンスの有効期間です。この日付を過ぎても**AVG Internet Security 2011**の使用を継続する場合は、ライセンスを更新する必要があります。ライセンスの更新は AVG Web サイトからオンラインで行うことができます。
- ***ワークステーション数***- **AVG Internet Security 2011**をインストールできるワークステーションの数です。

### コントロール ボタン

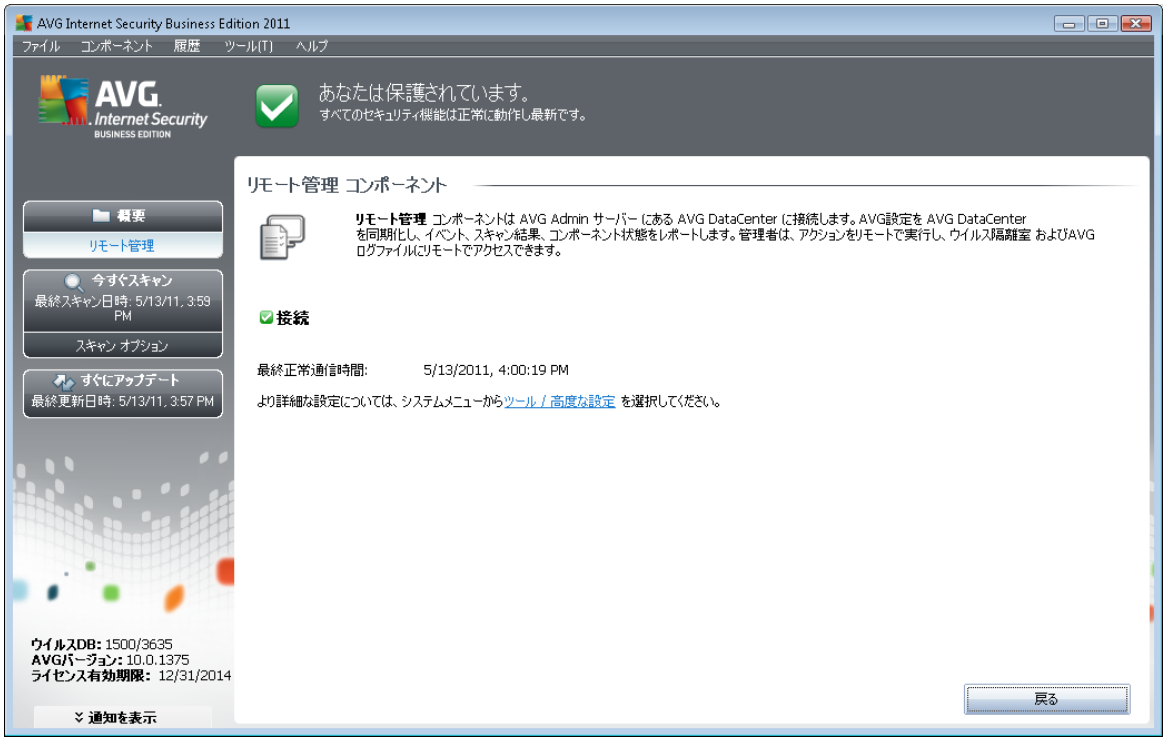
- ***登録*** - AVG Web サイト（http://www.avg.com/）の登録ページに接続します。登録データを入力してください。AVG 製品を登録したお客様のみが無料テクニカル サポートを利用できます。

- ***再アクティベート*** - インストール処理の [***AVG のパーソナライズ***] ダイアログで入力したデータが [***AVG のアクティベート***] ダイアログに表示されます。このダイアログではライセンス番号を入力してセールス番号（*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。

***メモ***: **AVG Internet Security 2011** *の試用版を使用している場合は、このボタンが [****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。セールス番号を使用して* **AVG Internet Security 2011** *をインストールした場合は、各ボタンが [****登録****] および [****アクティベート****] として表示されます。*

- ***戻る*** - このボタンをクリックすると、既定の ***AVG ユーザー インターフェース*** (*コンポーネント概要*) に戻ります。

## 7.12. 遠隔管理




***遠隔管理***コンポーネントは、製品の Business Edition (「***ライセンス***」コンポーネントを参照) をインストールした場合にのみ、 **AVG Internet Security 2011** のユーザー インターフェースに表示されます。[***遠隔管理***] ダイアログでは、コンポーネントがアクティブであるかどうか、サーバーに接続しているかどうかに関する情報が表示されます。. ***遠隔管理***コンポーネントは [***高度な設定/遠隔管理***] で設定できます。

コンポーネントのオプションと AVG Remote Administration システムの機能については、このトピック専用の特定のマニュアルを参照してください。このマニュアルは AVG Web サイト (www.avg.com) の ***サポート センター/ ダウンロード / マニュアル*** セクションからダウンロードできます。

### コントロール ボタン

- ***戻る*** - このボタンをクリックすると、既定の AVG ユーザー インターフェース ( *コンポーネント概要*) に戻ります。

## 7.13. オンライン シールド

### 7.13.1. オンライン シールドの原理

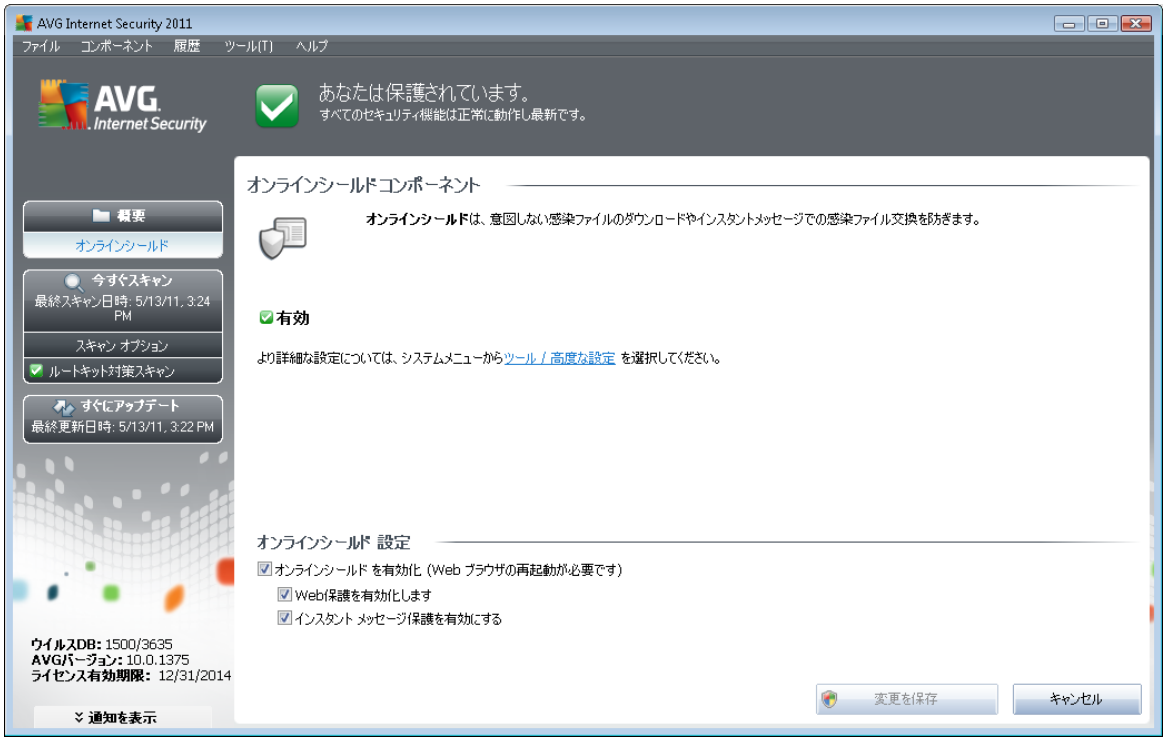
***オンライン シールド***は、*リアルタイムの常駐保護の一種です。Web ブラウザに表示され、コンピュータにダウンロードされる前に、Web ページの内容とそのページに含まれる可能性のあるファイルをスキャンします。*

***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。

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

### 7.13.2. オンライン シールド インターフェース

***オンライン シールド***コンポーネントのインターフェースには、保護の説明が表示されます。さらに、コンポーネントの現在の状態に関する情報も表示されます。ダイアログの下部には、このコンポーネント機能の基本編集オプションが表示されます。




## オンライン シールド設定

***オンライン シールド 有効化***にチェックを付けると、***オンライン シールド***のオン/オフを切り替えることができます。このオプションはデフォルトでチェックされており、***オンライン シールド***コンポーネントは有効です。この設定を変更する理由がない場合、コンポーネントを有効のままにすることを推奨します。***オンライン シールド***が実行中の場合、この項目にチェックを付けると、さらに別の 2 つの設定オプションが有効になります。

- ***Web 保護を有効にする*** - - このオプションにチェックを付けると、***オンライン シールド***は Web サイト コンテンツのスキャンを実行します。
- ***インスタント メッセージ保護を有効にする*** - この項目にチェックを付けると、***オンライン シールド***でインスタント メッセージ通信 (*ICQ*、*MSN* メッセンジャー、 ...) がウィルスに感染していないことを確認します。

***メモ:*** *すべての AVG コンポーネントは最適なパフォーマンスを実現できるようにあらかじめ設定されています。特に理由がない場合は AVG の設定を変更しないでください。設定変更は上級者ユーザーが行うことをお勧めします。AVG の設定を変更する必要がある場合は、システム メニュー項目の [**ツール/高度な設定**] を選択し、[AVG 高度な設定ダイアログで設定を編集します。*

## コントロールボタン

***オンライン シールド***インターフェースで利用できるコントロールボタンは以下の通

りです。

- ***変更を保存*** - このボタンを押すと、ダイアログで行われた変更を保存、適用します。
- ***戻る*** - このボタンをクリックすると、既定の ***AVG ユーザー インターフェース*** (*コンポーネント概要*) に戻ります

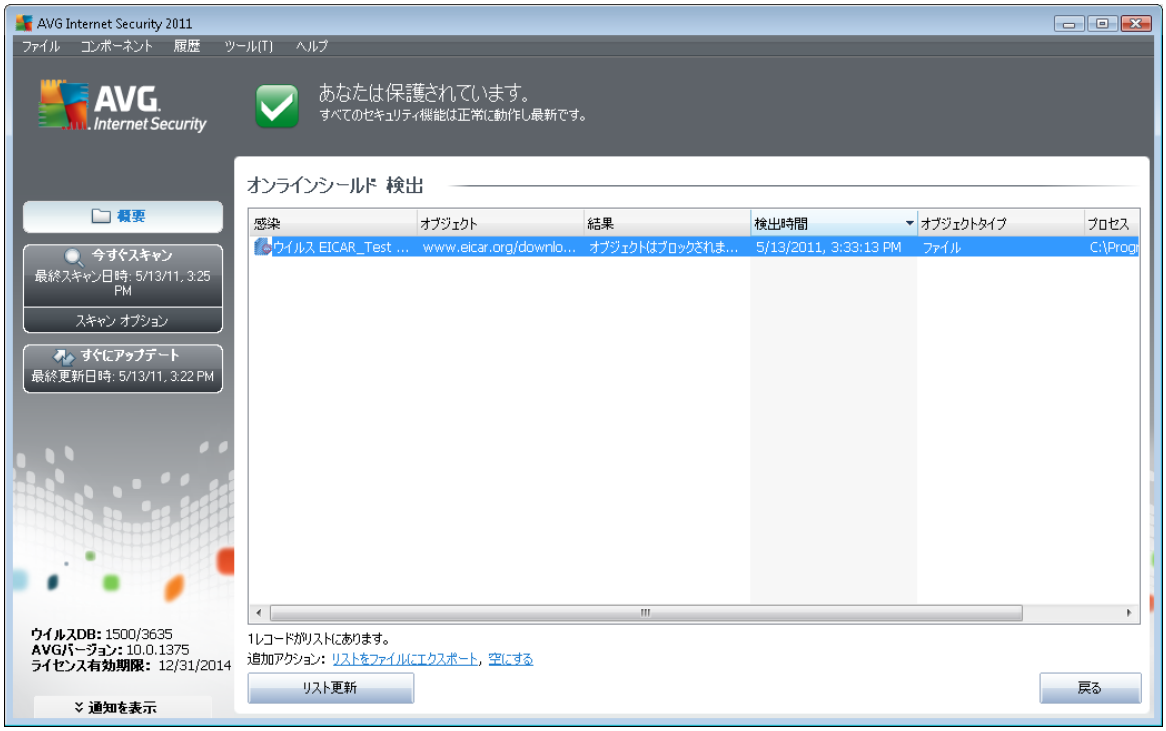
### 7.13.3. オンライン シールド検出

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


警告ダイアログでは、検出され感染と判定されたファイルに関するデータ (*ファイル名*)、認識された感染名 (*脅威名*)、*既知の脅威の場合*に検出された脅威に関する詳細情報を確認できる***ウィルス エンサイクロペディア***へのリンクが表示されます。ダイアログには次のボタンがあります。

- ***詳細を表示*** - [***詳細を表示***] ボタンをクリックすると、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、脅威検出は ***オンライン シールド検出結果***のリストにログ出力されます。この検出された脅威の概要は、システムメニューの [***履歴/オンライン シールド検出結果***] からアクセス可能です。




検出された各オブジェクトについて、以下の情報が提供されます。

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

ダイアログの下部では、リストの下に上記でリストされた検出オブジェクトの総数に関する情報が表示されます。さらに、検出オブジェクトの完全なリストをファイルにエクスポート（***ファイルにエクスポート***）し、検出オブジェクトのすべてのエントリを削除（***リストを空にする***）ことができます。[***リストを更新***] ボタンは***オンラインシールド***の検出結果リストを更新します。[***戻る***] ボタンをクリックすると、既定の ***AVG ユーザー インターフェース***（*コンポーネント概要*）に戻ります。

## 7.14. ルートキット対策

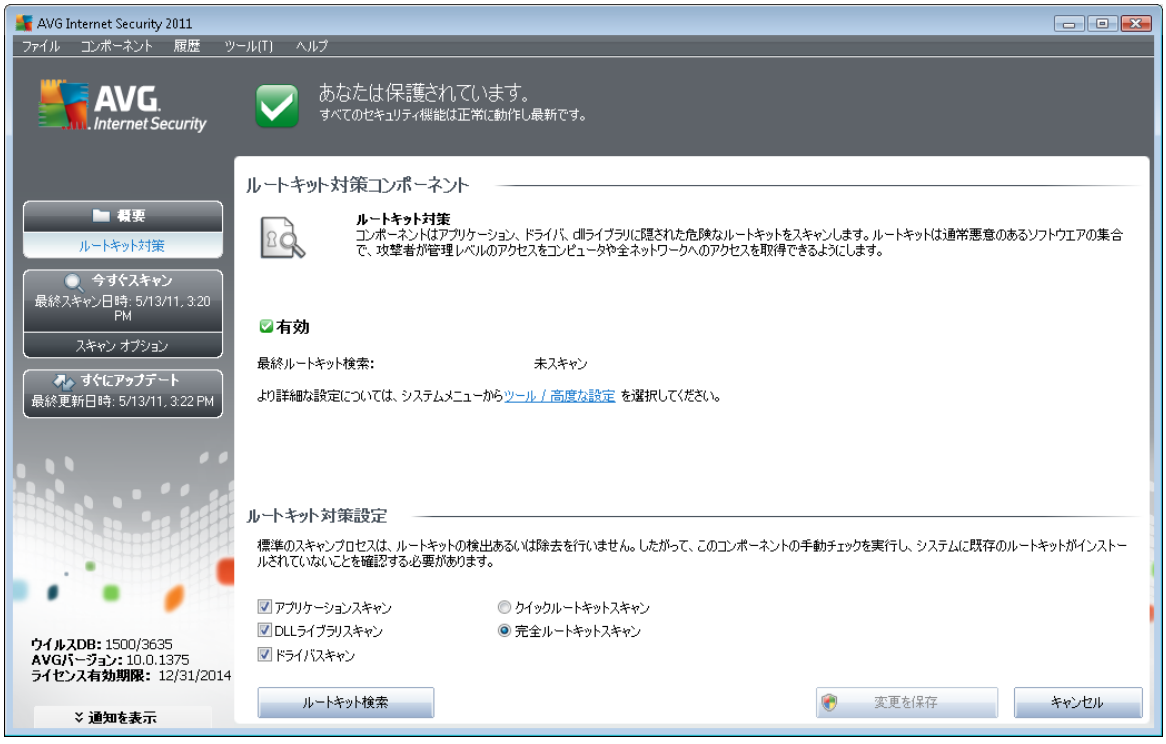
ルートキットは、システムの所有者や正式な管理者の許可なく、コンピュータ システムの基本機能を制御するように設計されたプログラムです。ルートキットはハードウェア上で実行されているオペレーティング システムを乗っ取ることを目的としているため、ハードウェアへのアクセスが必要になることはほとんどありません。一般的

には、ルートキットは標準のオペレーティング システムのセキュリティ メカニズムを破壊したり回避したりすることによって、システム上でその存在を隠しながら動作します。一般的に、ルートキットはトロイの木馬の一種でもあり、システムで実行しても安全であるかのように見せかけてユーザーを騙し、信じこませます。このような技術によって、プログラム監視の対象にならないように実行中のプロセスが隠されたり、オペレーティング システムからファイルやシステム データが隠されることもあります。

### 7.14.1. ルートキット対策の原理

***AVG Anti-Rootkit*** は、コンピュータ上の悪意のあるソフトウェアの存在を隠すプログラムや技術等の危険なルートキットを検出し、効果的に除去する特別なツールです。***AVG Anti-Rootkit*** は、あらかじめ定義されたルールセットに基づいて、ルートキットを検出できます。すべてのルートキットが検出されます（*感染したものだけではありません*）。***AVG Anti-Rootkit*** がルートキットを検出しても、必ずしもルートキットが感染しているというわけではありません。時々、ルートキットはドライバとして使用されたり、正しいアプリケーションの一部であったりします。

### 7.14.2. ルートキット対策インターフェース




***ルートキット*** ユーザー インターフェースには、コンポーネントの機能概要に関する説明が表示され、コンポーネントの現在の状態が通知されます。また、前回の***ルートキット対策***検査の実行日時 (***前回のルートキット検索***) 情報が表示されます。[***ルートキット対策***] ダイアログには、[***ツール/高度な設定***] リンクも表示されます。リンクをクリックすると、***ルートキット対策***コンポーネントの高度な設定環境にリダイレクトされます。

***メモ:*** *すべての AVG コンポーネントはあらかじめ設定され、最適なパフォーマンスが*

*保証されています。特に理由がない場合は、AVG の設定を変更しないでください。上級者ユーザーのみが設定変更を行うことをお進めします。*

### ルートキット対策設定

ダイアログの下部の [***ルートキット対策設定***] セクションでは、基本的なルートキット スキャン機能を設定できます。まず、該当するチェック ボックスにチェックを付け、スキャン対象オブジェクトを指定します。

- ***アプリケーション スキャン***
- ***DLL ライブラリ スキャン***
- ***ドライバ スキャン***

さらに、ルートキット スキャン モードを選択できます。

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

### コントロール ボタン

- ***ルートキット スキャン*** - ***完全コンピュータ スキャン***にはルートキット スキャンは含まれていません。***ルートキット対策*** インターフェースでこのボタンを使用することで、ルートキットスキャンを直接実行できます。
- ***変更を保存*** - このボタンをクリックすると、このインターフェースで実行されたすべての変更を保存し、既定の ***AVG ユーザー インターフェース*** *(コンポーネント概要) に戻ります。*
- ***キャンセル*** - このボタンをクリックすると、実行した変更を保存せずに ***AVG ユーザー インターフェース*** *(コンポーネント概要) に戻ります。*

## 7.15. システム ツール

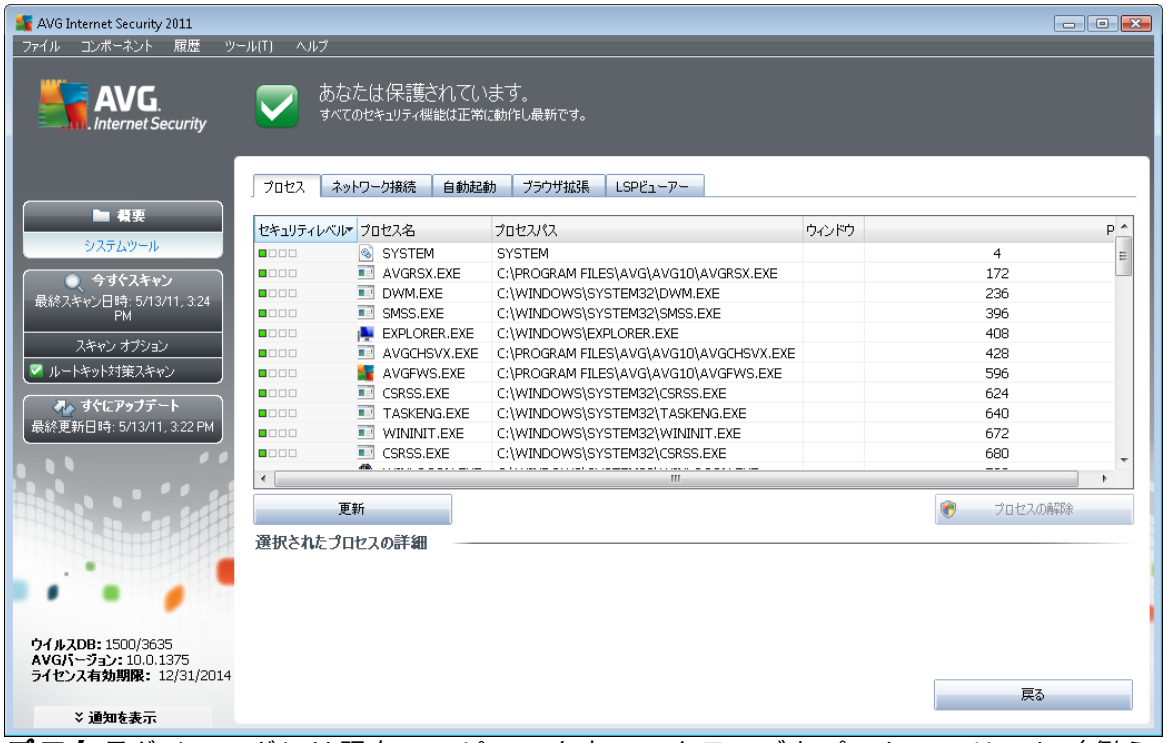
***システム ツール***とは、**AVG Internet Security 2011** 環境とオペレーティング システムの詳細サマリーを提供するツールのことです。コンポーネントには以下の概要が表示されます。

- プロセス - プロセスのリスト (*コンピュータ上で現在アクティブな実行中のアプリケーション*)。
- ネットワーク接続 - 現在アクティブな接続のリスト

- 自動起動 - Windows システム起動中に実行されるすべてのアプリケーションのリスト
- ブラウザ拡張 - プラグインのリスト (*インターネット ブラウザにインストールされているアプリケーション*)。
- LSP ビューア - レイヤード サービス プロバイダのリスト (*LSP*)

***これらの情報を編集することもできますが、特に経験のあるユーザー向けとして推奨されています。***

### 7.15.1. プロセス




***プロセス***ダイアログには現在コンピュータ上でアクティブなプロセスのリスト（*例えば、実行中のアプリケーション*）が表示されます。リストは複数のカラムに分けられます。

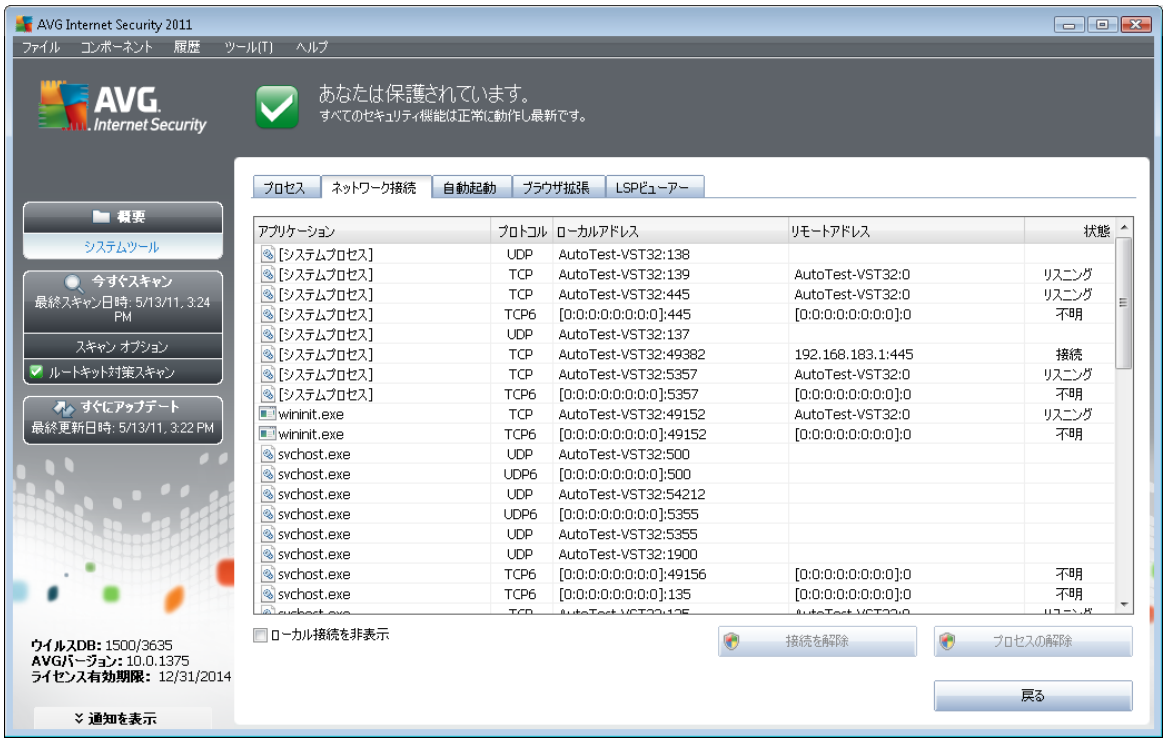
- ***重要度レベル*** - 重要度の低いもの（■□□□）から重大なもの（■■■■）までの 4 段階方式で各プロセスの重要度をグラフィカルに示します。
- ***プロセス名*** - 実行中のプロセス名
- ***プロセス パス*** - 実行中のプロセスへの物理パス
- ***ウィンドウ*** - アプリケーションウィンドウ名（存在する場合のみ）
- ***PID*** - 一意のWindows内部プロセス識別番号

### コントロールボタン

***システムツール***インターフェースで利用できるコントロールボタンは以下の通りです。

- ***更新*** - 現在のステータスに応じてプロセスのリストを更新します
- ***プロセスの終了*** - 1つ以上のアプリケーションを選択し、このボタンをクリックするとそのアプリケーションを終了できます。***本当に脅威であることが確実である場合以外は、プロセス、または接続を解除しないことを強く推奨します。***
- ***戻る*** - 既定の AVG ユーザー インターフェース (*コンポーネント概要*) に戻ります。

## 7.15.2. ネットワーク接続




***ネットワーク接続***ダイアログには、現在アクティブな接続のリストが表示されます。リストは以下のカラムに分けられます。

- ***アプリケーション*** - 接続に関するアプリケーション名 (*情報がない Windows 2000 を除く*)
- ***プロトコル*** - 接続に使用されるプロトコルタイプ
  - o TCP - インターネット上の情報を送信するインターネットプロトコル

（IP）と合わせて使用されるプロトコル

o UDP - TCPプロトコルの代替

- ***ローカルアドレス*** - ローカルコンピュータで使用されるIPアドレスとポート番号
- ***リモートアドレス*** - 接続されるリモートコンピュータのIPアドレスとポート番号可能な場合、リモートコンピュータのホスト名も表示されます。
- ***状態*** - 現在の状態（*接続、サーバーシャットダウン、リッスン、アクティブ終了、受動終了、アクティブ終了*）を表示します。

外部接続のみをリスト表示する場合、リストの下のダイアログの下部セクションの [***ローカル接続を非表示***] チェックボックスをオンにします。

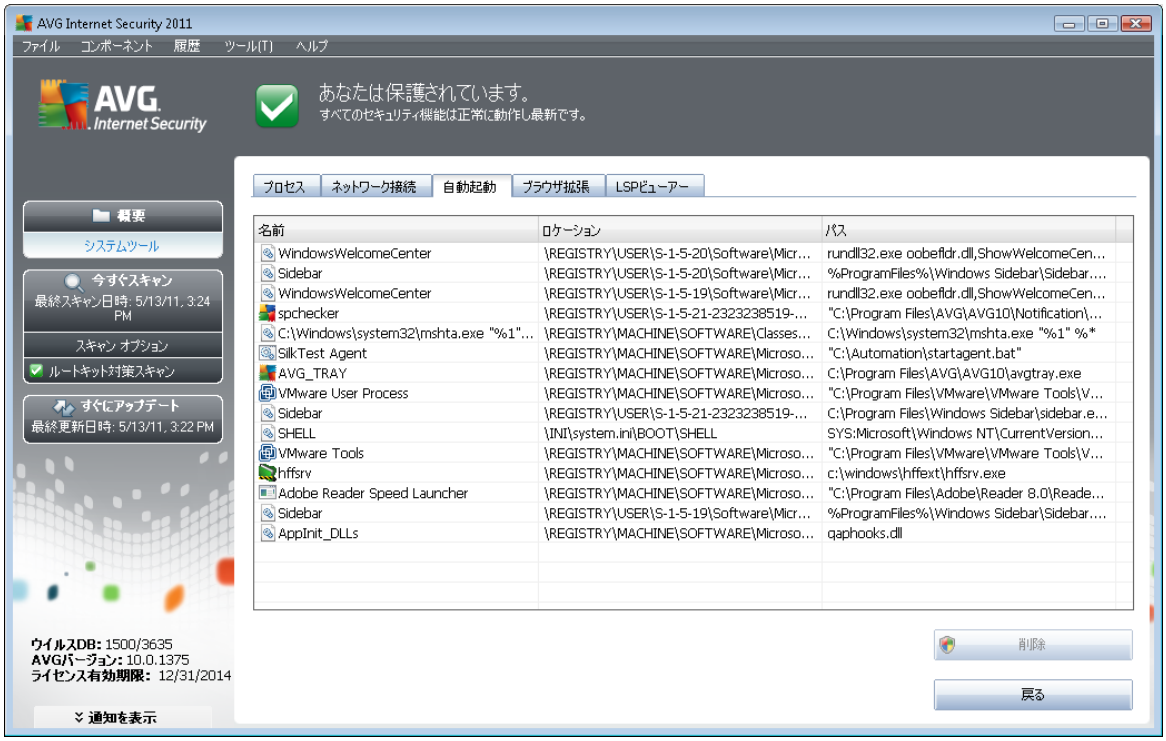
## コントロールボタン

以下のコントロールボタンが利用可能です。

- ***接続を解除*** - リストで選択された1つ以上の接続を終了します。
- ***プロセスを終了*** - リストで選択された接続に関する 1 つ以上のアプリケーションを終了します。
- ***戻る*** - 既定の ***AVG ユーザーインターフェース***（コンポーネント概要）に切り替わります。

***現在接続状態にあるアプリケーションのみを解除できる場合があります。警告：本当に脅威であることが確実である場合以外は、接続を解除しないことを強く推奨します。***

### 7.15.3. 自動起動

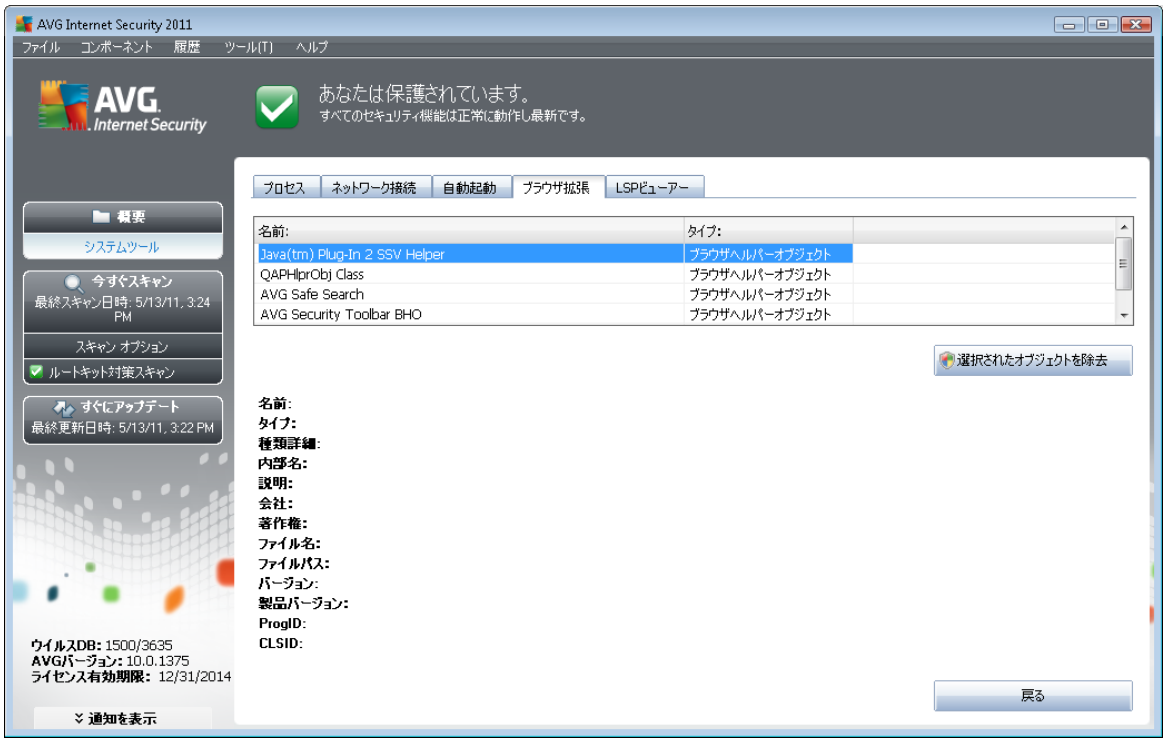



***自動起動***ダイアログには、Windowsシステム起動中に実行されるすべてのアプリケーションリストが表示されます。一部のマルウェアは、頻繁にレジストリエントリを追加します。

1つ以上のエントリを選択し、***除去***ボタンを押すと、それを削除できます。[***戻る***] ボタンをクリックすると、既定の AVG ユーザー インターフェース（*コンポーネント概要*）に戻ります。

***脅威であることが確実である場合以外は、リストからアプリケーションを削除しないことを強く推奨します。***

### 7.15.4. ブラウザ拡張



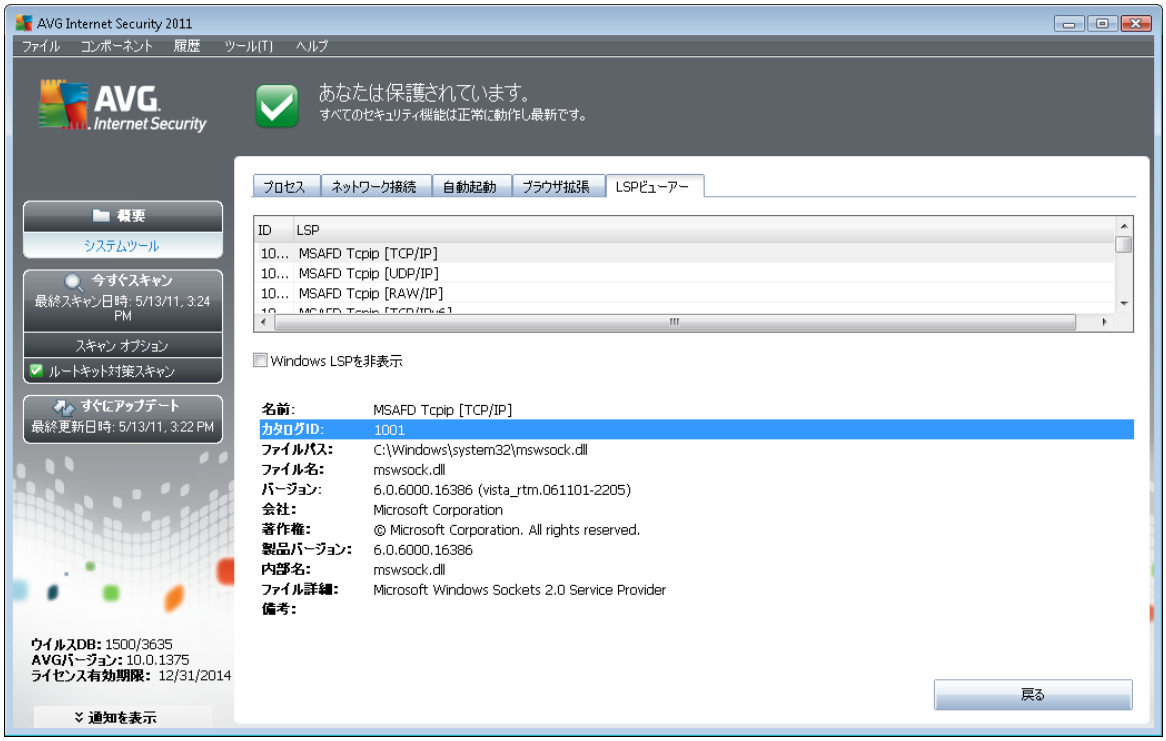

[***ブラウザ拡張***] ダイアログにはインターネット ブラウザにインストールされているプラグインのリスト（アプリケーションな）が含まれます。このリストには、潜在的なマルウェアプログラムだけでなく、通常のアプリケーションプラグインが含まれる場合があります。リストのオブジェクトをクリックすると、ダイアログの下部セクションに表示される選択したプラグインに関する詳細を取得します。

#### コントロールボタン

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

- ***選択したオブジェクトの削除*** - 現在リストで強調表示されているプラグインを削除します。***脅威であることが確実である場合以外は、リストからプラグインを削除しないことを強く推奨します。***
- ***戻る*** - 既定の ***AVG ユーザーインターフェース***（コンポーネント概要）に戻ります。

### 7.15.5. LSP ビューア




***LSP ビューアー*** ダイアログでは、レイヤードサービスプロバイダ（LSP）のリストが表示されます。

***レイヤードサービスプロバイダ***（LSP）は、Windowsオペレーティングシステムのネットワークサービスにリンクしたシステムドライバです。これは、データの修正を含め、コンピュータに入出力されるすべてのデータにアクセスします。一部のLSPでは、Windowsによりコンピュータがインターネットを含めた他のコンピュータに接続できるように許可する必要があります。ただし、あるマルウェアは、それ自体をLSPとしてインストールし、コンピュータが送信するすべてのデータにアクセスする可能性があります。したがって、このレビューはすべてのLSPの脅威をチェックする上で役に立つかもしれません。

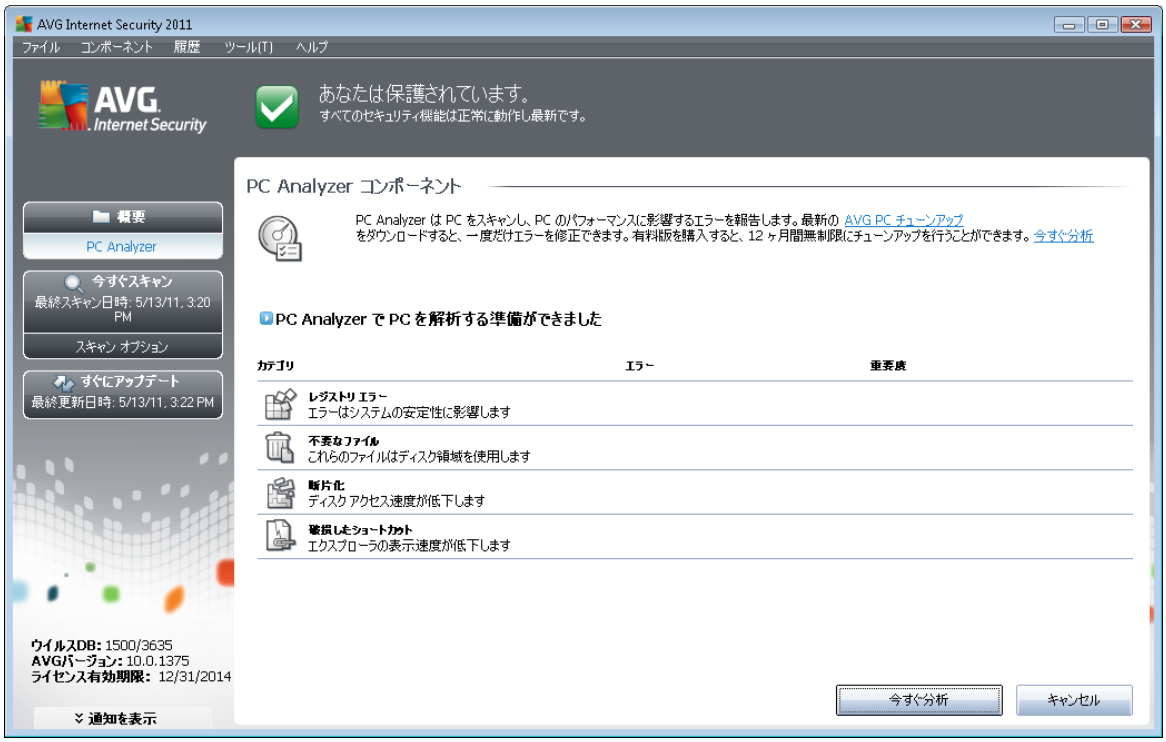
また、ある状況下では、壊れたLSP（*例えば、ファイルは除去されたがレジストリエントリが残っている場合等*）を修復できることもあります。修復可能なLSPが検出された場合にのみ、問題解決のためのボタンが表示されます。

リストにWindows LSP を含める場合は、***Windows LSP を非表示***チェックボックスのチェックを外します。[***戻る***] ボタンをクリックすると、既定の ***AVG ユーザー インターフェース***（*コンポーネント概要*）に戻ります。

## 7.16. PC Analyzer

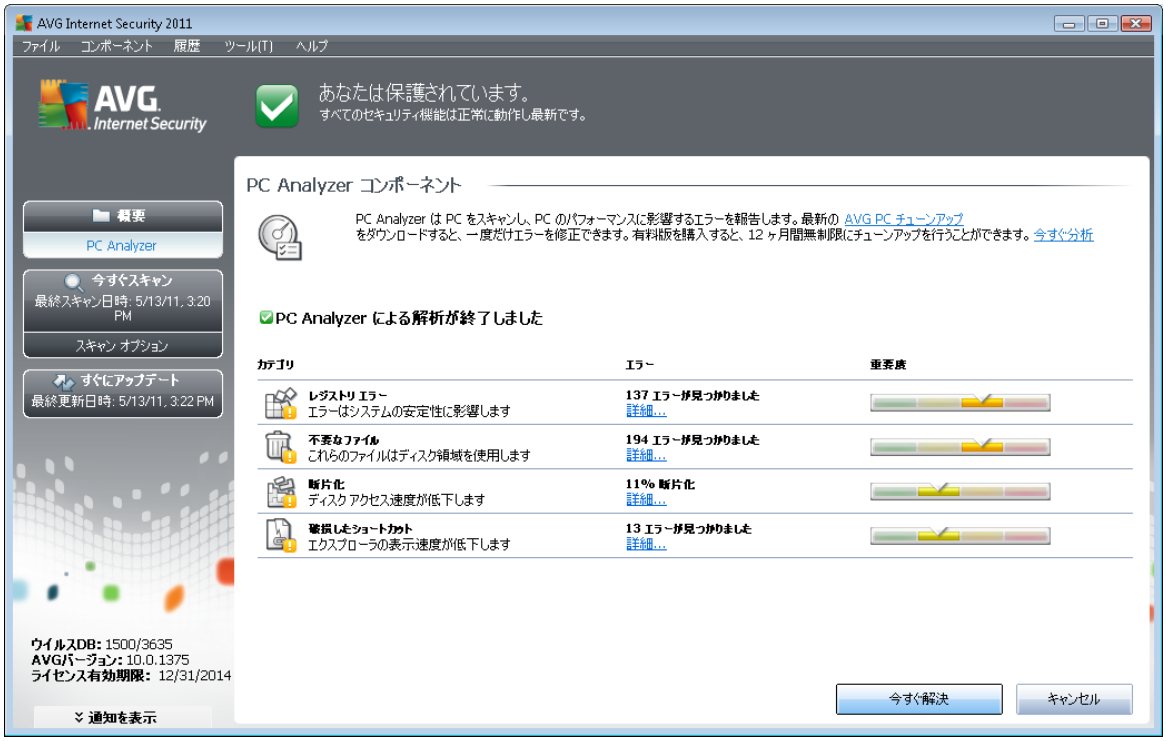
***PC Analyzer*** コンポーネントではコンピュータをスキャンし、システムの問題があるかどうかを確認します。コンピュータ全体のパフォーマンスを集約したわかりやすい概要が表示されます。コンポーネントのユーザー インターフェースには、レジストリ エ

ラー、不要なファイル、断片化、破損したショートカットの各カテゴリを示す 4 つの線で区別されたグラフが表示されます。




- ***レジストリ エラー***は、Windows レジストリの数を示します。レジストリの問題を解決するには高度な知識が必要であるため、レジストリ修正を自分で行わないことをお勧めします。
- ***不要なファイル***は、不要な可能性が高いファイルの数を示します。一般的には、各種一時ファイルやごみ箱のファイルが不要なファイルとして判断されます。
- ***断片化***では、長期間の使用により物理ディスクのいたるところに分散して断片化したハードディスクの割合を計算します。デフラグ ツールを使用してこの問題を解決できます。
- ***破損したショートカット***は、動作しないショートカットや存在しない場所へのショートカットなどの問題を示します。

システムの分析を開始するには、[***今すぐ分析***] ボタンをクリックします。次に、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。




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

## コントロール ボタン

- ***今すぐ分析*** (*分析前に表示*) - このボタンをクリックすると、コンピュータの分析をただちに実行します。
- ***今すぐ修正*** (*分析完了時に表示*) - このボタンをクリックすると、AVG Web サイト (http://www.avg.com/) の ***PC Analyzer*** コンポーネントに関する最新詳細情報を提供するページが開きます。
- ***キャンセル*** - このボタンをクリックすると、分析の実行を停止するか、分析完了時に既定の AVG ユーザー インターフェース (*コンポーネント概要*) に戻ります。

## 7.17. Identity Protection

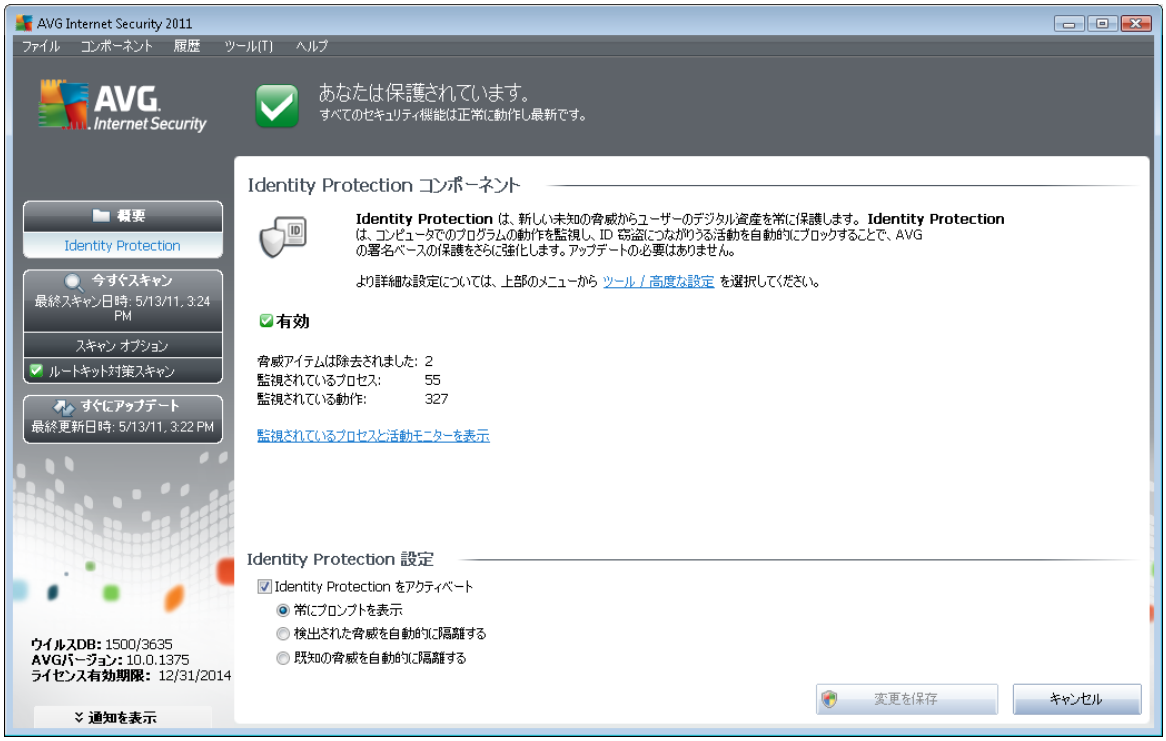
***AVG Identity Protection*** は ID 窃盗によるパスワード、銀行アカウント情報、クレジットカード番号、その他の貴重な個人デジタル情報の窃盗を防止することに特化したマルウェア対策製品です。PC を狙うあらゆる種類の悪意のあるソフトウェア（*マルウェア*）を対象とします。PC 上のすべてのプログラムが正常に動作していることを確認します。***AVG Identity Protection*** は継続的に疑わしい動作を検出およびブロックし、あらゆる新しいマルウェアからコンピュータを保護します。

### 7.17.1. Identity Protection の原理

***AVG Identity Protection*** はマルウェア対策コンポーネントであり、*スパイウェア、ボット、ID 窃盗*などのあらゆる種類のマルウェアに対する保護を提供します。行動分析技術を使用して、発生したばかりの新しいウイルスに対する保護を提供します。マルウェアはますます高度化し、離れた場所にいる ID 窃盗攻撃者が PC で開くことができる通常のプログラムの形で侵入してくるため、***AVG Identity Protection*** はこのような実行ベースのマルウェアに対する保護を提供します。これは、署名機能とスキャンを使用して、ファイルベースの既知のウィルスに対する保護を提供する ***AVG Anti-Virus*** の補完的な保護です。

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

### 7.17.2. Identity Protection インターフェース




***Identity Protection***コンポーネント インターフェースには、コンポーネントの基本機能、ステータス、統計情報データの概要が表示されます。

- ***除去されたマルウェアアイテム*** - マルウェアとして検出され除去されたアプリケーションの数を表示します
- ***監視されているプロセス*** - Identity Protection によって監視されている現在実行中のアプリケーションの数
- ***監視されている動作*** - 監視されているアプリケーションで実行中の特定のアクションの数

下には [***監視プロセスと活動モニターを表示する***] リンクがあり、***システム ツール*** コンポーネントのユーザー インターフェースに移動します。このインターフェースでは、すべての監視プロセスの詳細概要が表示されます。

### Identity Protection 設定

ダイアログの下部には、[***Identity Protection 設定***] セクションが表示されます。ここではコンポーネント機能の基本的な機能を編集できます。

- ***Identity Protectionを有効化*** - (*既定ではオン*): チェックを付けると、Identity Protection コンポーネントがアクティブになり、詳細編集オプションが開きます。

場合によっては、***Identity Protection***が問題のないファイルを、不審なファイルまたは危険なファイルとして報告する場合があります。***Identity Protection***は脅威の動作に基づいて脅威を検出します。通常は、プログラムがキーの押下を監視しようとしている場合、他のプログラムをインストールしようとしている場合、コンピュータに新しいドライバがインストールされる場合に検出します。したがって、不審な活動が検出された場合に、***Identity Protection***コンポーネントの動作を指定する次のオプションのいずれかを選択してください。

  - ***常にプロンプトを表示*** - アプリケーションがマルウェアとして検出された場合、アプリケーションをブロックするかどうかを確認するプロンプトが表示されます (*このオプションはデフォルトではオンになっています。特に理由がない限り、変更しないことをお勧めします*)。
  - ***自動的に検出された脅威を隔離*** - マルウェアとして検出されたすべてのアプリケーションは自動的にブロックされます
  - ***自動的に既知の脅威を隔離*** - 絶対的に確実にマルウェアとして検出されたアプリケーションのみをブロックします。

### コントロールボタン

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

- ***変更の保存*** - このボタンをクリックすると、ダイアログで行われた変更を保存して適用します。
- ***キャンセル*** - このボタンをクリックすると、既定の ***AVG ユーザー インターフェース*** (*コンポーネント概要*) に戻ります。

## 7.18. セキュリティ ツールバー

***セキュリティ ツールバー***は、Web 閲覧時に AVG 保護とさまざまな機能とツールを簡単に強化できるオプションの Web ブラウザ ツールバーです。現在、***セキュリティ ツールバー***は Internet Explorer (*6.0 以上*) および Mozilla Firefox (*3.0 以上*) Web ブラウザでサ

ポートされています。


ブラウザの***セキュリティ ツールバー***から***セキュリティ ツールバー*** コンポーネントのすべての設定に直接アクセスできます。

# 8. AVG セキュリティ ツールバー

***AVG セキュリティ ツールバー***は ***リンクスキャナ*** コンポーネントと連動して機能する新しいツールです。***AVG セキュリティ ツールバー***を使用して、***リンクスキャナ***の機能を制御し、動作を調整できます。

**AVG Internet Security 2011** のインストール中にツールバーのインストールを選択した場合は、ツールバーが Web ブラウザ (*Internet Explorer 6.0 以上および Mozilla Firefox 3.0 以上*) に自動的に追加されます。現時点では他のインターネット ブラウザには対応していません。

***メモ:*** *別のインターネットブラウザ (Avant ブラウザなど) を使用している場合は、予期しない動作を起こす場合があります。*

## 8.1. AVG セキュリティ ツールバー インターフェース

***AVG セキュリティ ツールバー***は、***MS Internet Explorer*** (*バージョン 6.0 以上*) および ***Mozilla Firefox*** (*バージョン 3.0 以上*) で動作するよう設計されています。***AVG セキュリティ ツールバー*** *のインストールを選択 (AVG インストール処理中にこのコンポーネントをインストールするかどうかを決定する必要があります*) した場合、このコンポーネントが Web ブラウザのアドレス バーの下に表示されます。


***AVG セキュリティツールバー***は以下のように構成されています。

### 8.1.1. AVG ロゴ ボタン

このボタンを使用して、一般的なツールバー項目にアクセスできます。ロゴ ボタンをクリックすると、AVG の Web サイト () が表示されます。AVG アイコンの横のポインタをクリックすると、次の情報が表示されます。

- ***ツールバー情報*** - ツールバーの保護に関する詳細情報を提供する ***AVG セキュリティ ツールバー ホームページへのリンクです。***
- ***AVG の起動*** - **AVG Internet Security 2011*****ユーザー インターフェース***
- ***AVG 情報*** - コンテキスト メニューが開き、リンクをクリックすると、**AVG Internet Security 2011**に関する重要なセキュリティ情報が表示されます。
  - *脅威について* - AVG Web サイトが開き、上位の脅威に関する最も重要なデータ、推奨されるウィルス削除方法、AVG 更新情報、ウィルス データベースへのアクセス、その他の関連情報について説明するページが表示されます。
  - *AVG ニュース* - 最新の AVG 関連記者発表記事を掲載したウェブページを開きます。

- *現在の脅威レベル* - Web 上の現在の脅威レベルをグラフィカルに表示したウイルス ラボの Web ページを開きます。

- *AVG 脅威研究所* - AVG サイト レポート Web サイトが開きます。このサイトで脅威名を入力すると、特定の脅威を検索し、各脅威の詳細情報を確認できます。

- ***オプション*** - 設定ダイアログが開き、***AVG セキュリティ ツールバー***の設定をニーズに合わせて調整できます。「***AVG セキュリティ ツールバー オプション***

- ***履歴の削除*** - ***AVG セキュリティツールバー*** の履歴の完全削除、検索履歴の削除、ブラウザ履歴の削除、ダウンロード履歴の削除、Cookies の削除処理を実行できます。

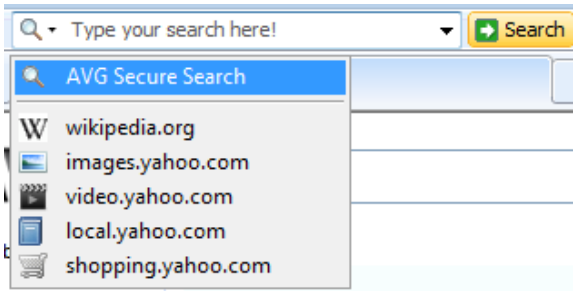
- ***更新*** - ***AVG セキュリティ ツールバーの新しい更新をチェックします。***

- ***ヘルプ*** - ヘルプ ファイルの確認、AVG テクニカル サポートへの問い合わせ、製品関連フィードバックの送信、最新バージョンのツールバーの詳細の確認ができます。

### 8.1.2. AVG Secure Search (powered by Google) による検索ボックス

***AVG Secure Search (powered by Google)*** ボックスを使用すると、AVG Secure Search (powered by Google) を使用して容易かつ安全な方法で Web を検索できます。検索ボックスに単語またはフレーズを入力して、[***検索***] ボタンをクリックするか、[***Enter***] キーを押すと、現在表示されているページに関係なく、AVG Secure Search (powered by Google) サーバー上で直接検索が開始されます。検索ボックスには検索履歴のリストも表示されます。検索ボックスで行われた検索は***サーチ シールド***保護で分析されます。

あるいは、検索フィールドでウィキペディアやその他の特定の検索サービスに切り替えることもできます。写真を参照してください。




### 8.1.3. ページ ステータス

このボタンをツールバーから直接クリックすると、***サーフ シールド*** コンポーネントの条件に基づいて、現在表示されている Web ページの評価が表示されます。

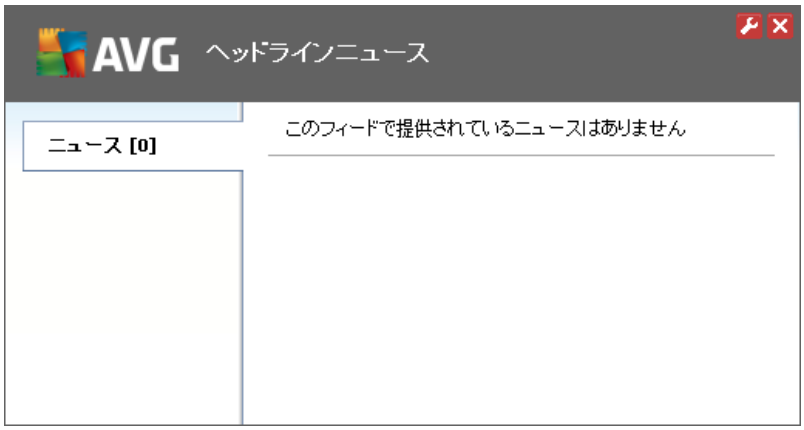
- - リンクされたページは安全です。

- - ページには不審な部分があります。
- - ページには明らかに危険なページへのリンクが含まれます。
- - リンクされたページにはアクティブな脅威が含まれています。安全のために、このページへのアクセスは禁止されています。
- リンクされたページは、アクセスできないかスキャンできませんでした。

ボタンをクリックすると、情報パネルと、特定のウェブページに関する詳細データが表示されます。

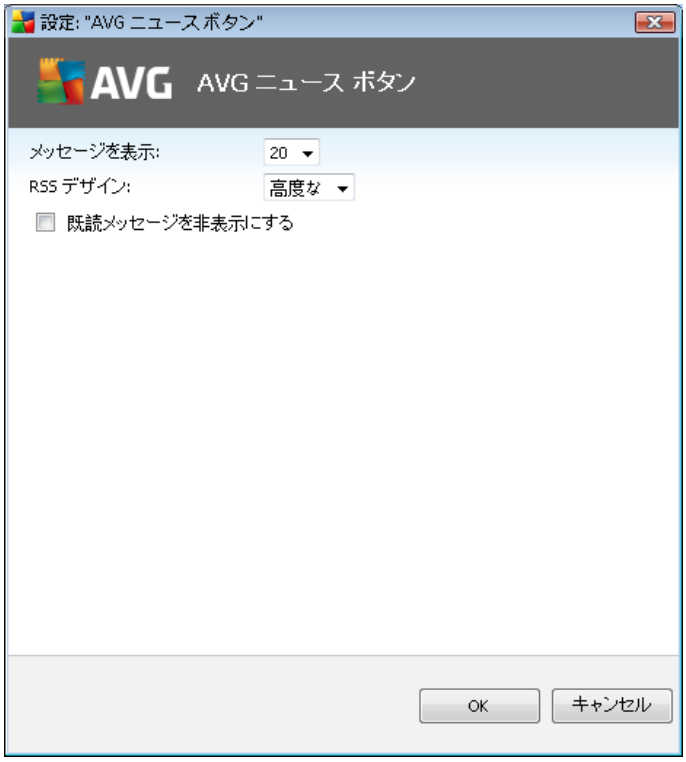
### 8.1.4. AVG ニュース

***AVG セキュリティツールバー*** でこのボタンを直接使用すると、最新の AVG 関連***ヘッドライン ニュース***の概要、一般メディア ニュース、企業プレス リリース ニュースが開きます。




右下端には 2 つの赤色のコントロール ボタンがあります。

- - このボタンを使用すると、編集ダイアログが開き、***AVG セキュリティツールバー*** に表示される [***AVG ニュース***] ボタンのパラメータを指定できます。

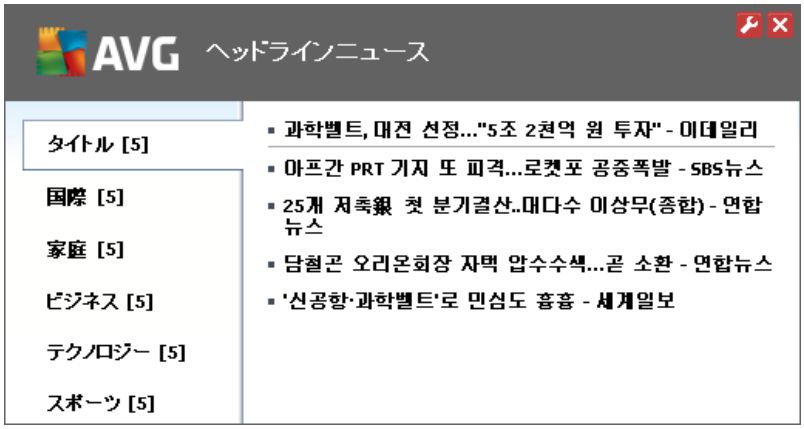



- ***メッセージを表示する*** - 同時に表示するメッセージ数を変更します。
- ***RSS デザイン*** - ニュース概要の現在の表示の高度/基本モードを切り替えます (*既定では高度モードが選択されています。上記の写真を参照*)。
- ***既読のメッセージを非表示にする*** - この項目を選択すると、既読メッセージは表示されません。新しいメッセージのみが表示されます。

- - このボタンをクリックすると、現在開いているニュース概要が閉じます。

### 8.1.5. ニュース

同様に、***AVG セキュリティ ツールバー***内から直接このボタンをクリックすると、選択したメディアが提供する最新ニュースの概要が複数のセクションに分かれて表示されます。




右下端には 2 つの赤色のコントロール ボタンがあります。

- - このボタンを使用すると編集ダイアログが開き、***AVG セキュリティ ツールバー***に表示される [***ニュース***] ボタンのパラメータを指定できます。


o ***ボタン名*** - ***AVG セキュリティ ツールバー***

o ***ニュース エディション*** - リストから国を選択すると、選択した地域のニュースが表示されます。
o ***メッセージを表示する*** - 同時に表示するメッセージ数を指定します。
o ***RSS デザイン*** - 基本/高度オプションを切り替え、ニュース概要のデザインを選択します (***既定では高度なデザインが設定されています。上記の写真を参照***)。
o ***既読のメッセージを非表示にする*** - この項目にチェックを付けると、既読のメッセージはニュース概要に表示されず、新しいニュースのみが表示されます。
o ***ボタン表示*** - このフィールドでは ***AVG セキュリティ ツールバー*** ニュース概要に表示するニュースの種類を割り当てることができます。

- このボタンをクリックすると、現在開いているニュース概要が閉じます。

### 8.1.6. 履歴の削除

このボタンを使用すると、[***AVG ロゴ -> 履歴を削除***] オプションと同じようにブラウザの履歴を削除できます。

### 8.1.7. メール通知

[***メール通知***] ボタンをクリックすると、新着の電子メール メッセージを ***AVG セキュリティ ツールバー*** インターフェースで直接通知するオプションを有効にできます。ボタンをクリックすると、次の編集ダイアログが開き、電子メール アカウントと電子メール表示ルールに関するパラメータを定義できます。ダイアログに表示される指示に従ってください。


- ***アカウント タイプ*** - 電子メール アカウントが使用するプロトコル タイプを指定します。*Gmail*、*POP3* のいずれかを選択するか、[*その他*] 項目のドロップダウン メニューからサーバー名を選択できます (*現時点では、Yahoo! JP メールまたは Hotmail アカウントを使用している場合にこのオプションを使用できます*)。アカウントで使用している電子メール サーバーの種類がわからない場合は、電子メール プロバイダまたはインターネット サービス プロバイダに確認してください。

- ***ログイン*** - 下のセクションには有効な *電子メール アドレス*と該当する *パスワードを*入力します。[*自動ログイン*] オプションを選択しておくと、データを何

度も入力せずにすみます。

- ***テスト アカウント*** - このボタンを使用して、入力した詳細情報をテストします。
- ***設定のリセット*** - 入力した電子メール アドレス詳細情報をただちに削除します。
- ***次の時間ごとに新規メールを確認する*** - 新しい電子メール メッセージを確認する時間間隔 (*5 ～ 120 分*) を定義し、新しいメッセージの到着を通知するかどうかを指定します。
- ***新しい電子メール アラートを許可する*** - チェックを外すと、新しい電子メール メッセージの到着を示すビジュアル通知を無効にします。
    - ***新しい電子メールが到着したときにサウンドを鳴らす*** - チェックを外すと、新しい電子メール メッセージの到着を示すサウンド通知を無効にします。
    - ***5 秒後に通知ウィンドウを閉じる*** - チェックを付けると、新しい電子メール メッセージの到着の 5 秒後にビジュアル通知ウィンドウを自動的に閉じます。

### 8.1.8. 天気予報情報

[***天気***] ボタンを使用すると、選択した地域の現在の気温 (*3 ～ 6 時間ごとに更新*) を ***AVG セキュリティ ツールバー*** インターフェースから直接表示できます。このボタンをクリックすると、新しい情報パネルが開き、天気予報詳細概要が表示されます。


次の編集オプションがあります。

- ***地域を変更*** - [***地域を変更***] テキストをクリックすると、新しい [***地域の検索***] ダイアログが表示されます。テキスト フィールドに任意の地域名を入力し、[

***検索***] ボタンをクリックして確定します。次に、同じ名前のすべての地域のリストから目的の地域を選択します。最後に、再度情報パネルが開き、選択した地域の天気予報が表示されます。

- ***華氏/摂氏変換*** - 情報パネルの右上端では華氏と摂氏を選択できます。選択した地域に応じて、気温情報が選択した華氏または摂氏で表示されます。
- ***詳細天気予報*** - 詳細な天気予報を表示する場合は、[***詳細天気予報***] リンクをクリックして、専門天気 Web サイトにアクセスできます。

### 8.1.9. Facebook

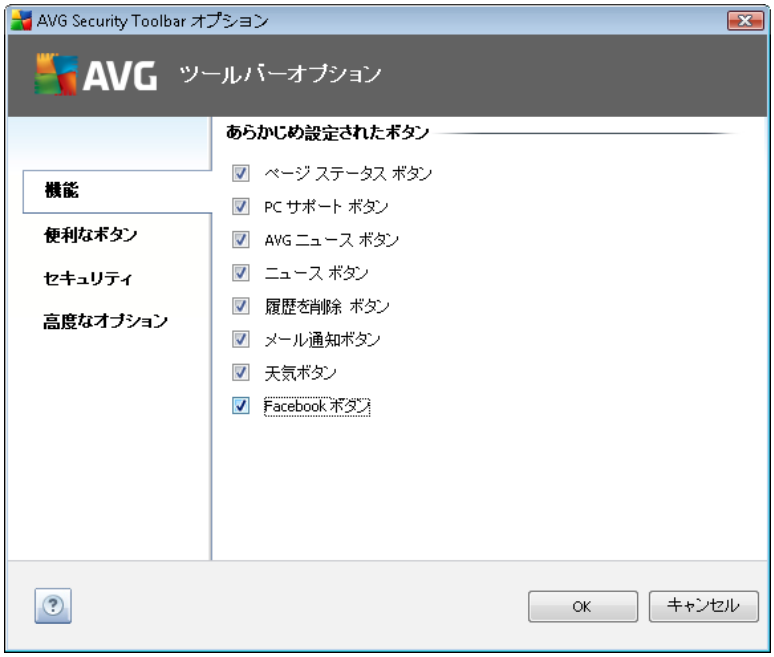
[***Facebook*** ] ボタンをクリックすると、***AVG セキュリティ ツールバー***から Facebook ソーシャル ネットワークに直接接続できます。ボタンをクリックすると、ログイン案内画面が表示されます。再度クリックすると、[***Facebook Login***] ダイアログが表示されます。認証資格情報データを入力し、[***Connect***] ボタンをクリックします。Facebook アカウントを持っていない場合は、[***Sign up for Facebook***] リンクからアカウントを直接作成できます。

Facebook での登録処理が完了した時点で、***AVG ソーシャル ネットワーク拡張***アプリケーションを許可するように指示されます。ツールバーの Facebook 接続を使用する場合には、このアプリケーション機能が必要です。したがって、この機能を許可し使用可能にすることをお勧めします。その後で、Facebook 接続が有効になり、***AVG セキュリティ ツールバー***の [***Facebook***] ボタンを使用して、標準の Facebook メニュー オプションにアクセスできます。

## 8.2. AVG セキュリティ ツールバー オプション

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

### 8.2.1. タブ全般




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

- ***ページ ステータス ボタン*** - このボタンを使用すると、現在開いているページのセキュリティ ステータスに関する情報を***AVG セキュリティ ツールバー***
- ***AVG ニュース ボタン*** - このボタンを使用すると、最新の AVG 関連記者発表記事を掲載したウェブページを開きます。
- ***ニュース ボタン*** - このボタンを使用すると、毎日のニュース記事から最新のニュースの構造化された概要を表示します。
- ***履歴の削除ボタン*** - このボタンを使用すると、完全な履歴の削除または検索履歴の削除、ブラウザ履歴の削除、あるいは Cookies の削除を AVG セキュリティ ツールバーから直接実行できます。
- ***電子メール通知ボタン*** - このボタンを使用すると、新しく到着した電子メール メッセージを ***AVG セキュリティ ツールバー*** インターフェースに表示できます。
- ***天気ボタン*** - このボタンを使用すると、選択した地域のリアルタイムの天気情報を表示できます。
- ***Facebook ボタン*** - このボタンを使用すると、Facebook ソーシャル ネットワークに直接接続できます。

### 8.2.2. タブの便利なボタン


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

### 8.2.3. タブ セキュリティ


[***セキュリティ***] タブには、[***AVG ブラウザセキュリティ***] と [***評価***] という 2 つのセク

ションがあり、特定のチェックボックスをオンにして、使用する ***AVG Security Toolbar*** 機能を割り当てられます。

- ***ブラウザ セキュリティ*** - この項目にチェックを付けると、***AVG サーチ シールド***または***サーフ シールド*** サービスの有効化/無効化を切り替えられます。
- ***評価*** - 使用する ***Search-Shield***
  - ページは安全です
  - ページには不審な部分があります
  - ページには明らかに危険なページへのリンクが含まれます
  - ページにはアクティブな脅威が含まれます
  - リンクされたページはアクセスできないかスキャンできませんでした

各オプションをオンにして、この特定の脅威レベルに対する通知方法を確認します。ただし、アクティブかつ危険な脅威を含むページに割り当てられる赤いマークをオフにすることはできません。***ここでも、変更する理由がない限り、プログラムベンダーが設定した既定の設定を保持することをお勧めします。***

### 8.2.4. タブの高度なオプション


[***高度なオプション***] タブでは、まず既定で使用する検索エンジンを選択します。*AVG Secure Search (powered by Google)*、*Baidu*、*WebHledani*、*Yandex*、*Yahoo!JP* から選択できま

す。既定の検索エンジンを変更した場合は、変更を有効にするために、インターネット ブラウザを再起動してください。

さらに、特定の***AVG セキュリティ ツールバー***設定 *(リストの説明文は既定の AVG Secure Search (powered by Google) 設定を指す) のオン/オフを切り替えることができます*。

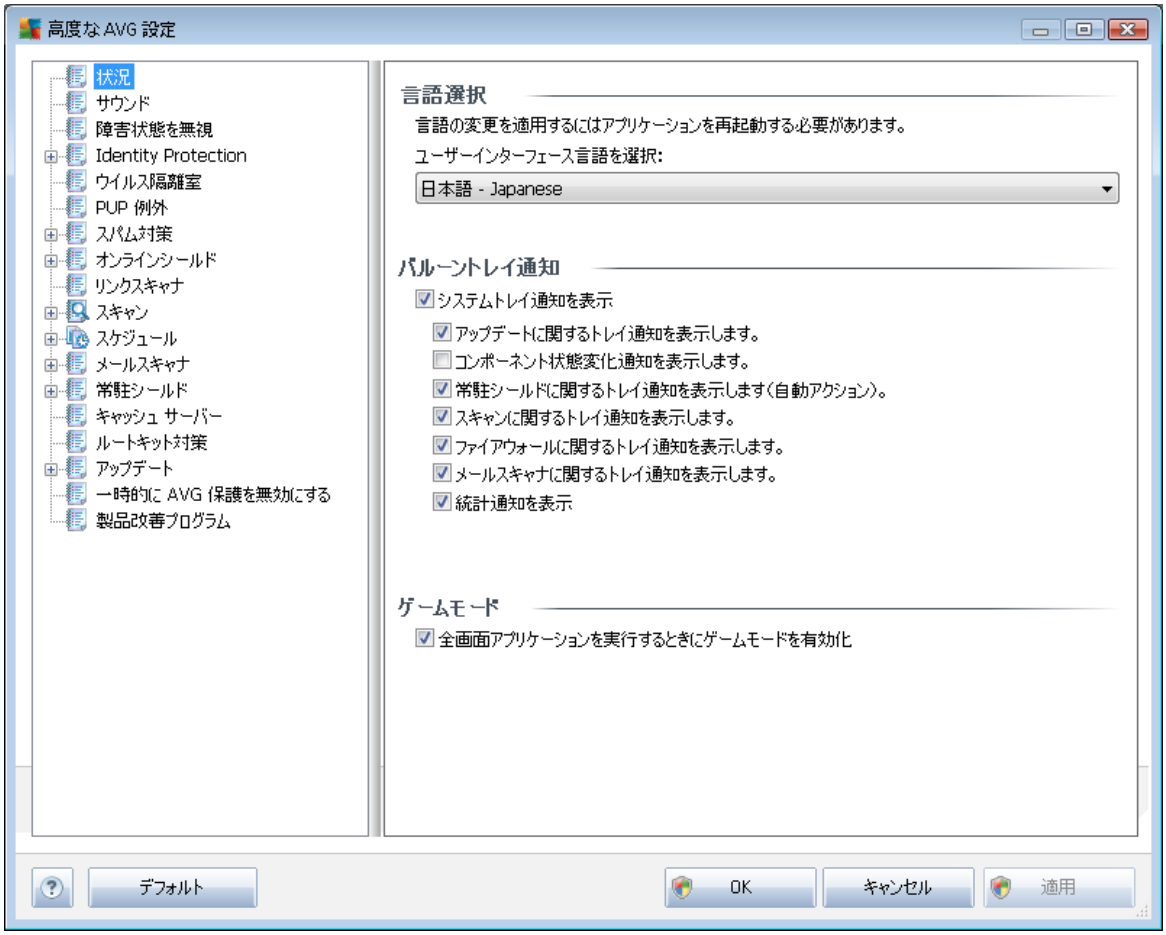
- ***アドレス バーの検索プロバイダとしてAVG Secure Search (powered by Google)を設定して保持する*** - このオプションにチェックを付けると、検索キーワードを直接インターネット ブラウザのアドレス バーに入力できます。Google サービスを使用して、自動的に関連する Web サイトを検索します。
- ***AVG でブラウザ ナビゲーション エラー (404/DNS) に関する提案を表示する*** - Web を検索しているときに存在しないページがあった場合や、表示できないページ (404 エラー) があった場合、自動的に代わりのトピック関連のページの概要から選択できるページにリダイレクトします。
- ***AVG Secure Search (powered by Google)を既定の検索プロバイダとして設定して保持する*** - Google は ***AVG セキュリティ ツールバー***の既定の Web 検索エンジンです。このオプションを有効にすると、Google が Web ブラウザの既定の検索エンジンになります。

# 9. AVG 高度な設定

**AVG Internet Security 2011** の高度な設定ダイアログは [***高度な AVG 設定***] という名前の新しいダイアログで開きます。 このウィンドウは2つのセクションにわかれています。左部はにツリー状のナビゲーションが表示されます。設定を変更したいコンポーネントを選択すると、ウィンドウ右側に設定項目が表示されます。

## 9.1. 表示

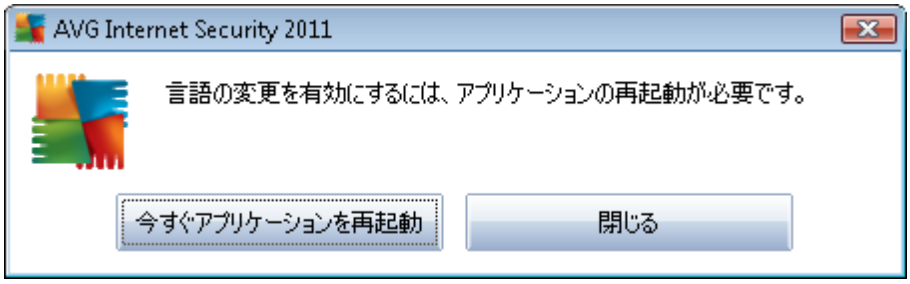
ナビゲーション ツリーの最初の項目の [***表示***] では、AVG ユーザー インターフェースとアプリケーション動作の基本オプションの一部を設定します。




### 言語選択

[***言語選択***] セクションでは、ドロップダウン メニューから任意の言語を選択します。この言語はすべてのAVG ユーザー インターフェースで使用されます。ドロップダウン メニューには、インストール処理中に選択した言語 (「カスタム オプション」の章を参照) と英語 (*既定でインストール*)のみが表示されます。ただし、アプリケーションを他の言語に切り替える際には、次の方法でユーザー インターフェースを再起動する必要があります。

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




## バルーン トレイ通知

このセクションでは、アプリケーション ステータスに関するシステム トレイ バルーン通知の表示を制御できます。既定ではバルーン通知が表示されます。この設定を保持することをお勧めします。通常、バルーン通知は AVG コンポーネントのステータス変更を通知します。この通知には気を付ける必要があります。

ただし、何らかの理由で、この通知を非表示にする場合や特定の AVG コンポーネントの通知のみを表示する場合は、次のオプションを使用して設定を定義できます。

- ***システム トレイ通知を表示する*** - 既定ではこの項目は*オン*であり、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バルーン通知表示がオフになります。オンにした場合は、表示する通知を選択できます。
  - ***更新***に関するトレイ通知を表示する - AVG 更新処理の起動、進行、完了に関する情報を表示するかどうかを決定します。
  - ***コンポーネントの状態変更に関するトレイ通知を表示する*** - コンポーネントの有効/無効状態または問題が発生している可能性に関する情報を表示するかどうかを決定します。コンポーネントでエラー状態が発生している場合には、このオプションはシステム トレイ アイコン (色変更) が特定の AVG コンポーネントで発生している問題を報告するときと同じ方法でエラーを報告します。
  - ***常駐シールド関連のトレイ通知を表示する (自動アクション)*** - ファイルの保存、コピー、開く処理に関する情報を表示するかどうかを決定します (*この設定は、常駐シールドの [自動修復] オプションがオンになっている場合にのみ有効です*)。
  - ***スキャン***に関するトレイ通知を表示する - スケジュール 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*に関するトレイ通知を表示** - ファイアウォール状態とプロセスに関する情報を表示するかどうかを決定します。例えば、コンポーネントの有効化/非有効化、警告、トラフィックのブロック等が表示されます。

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

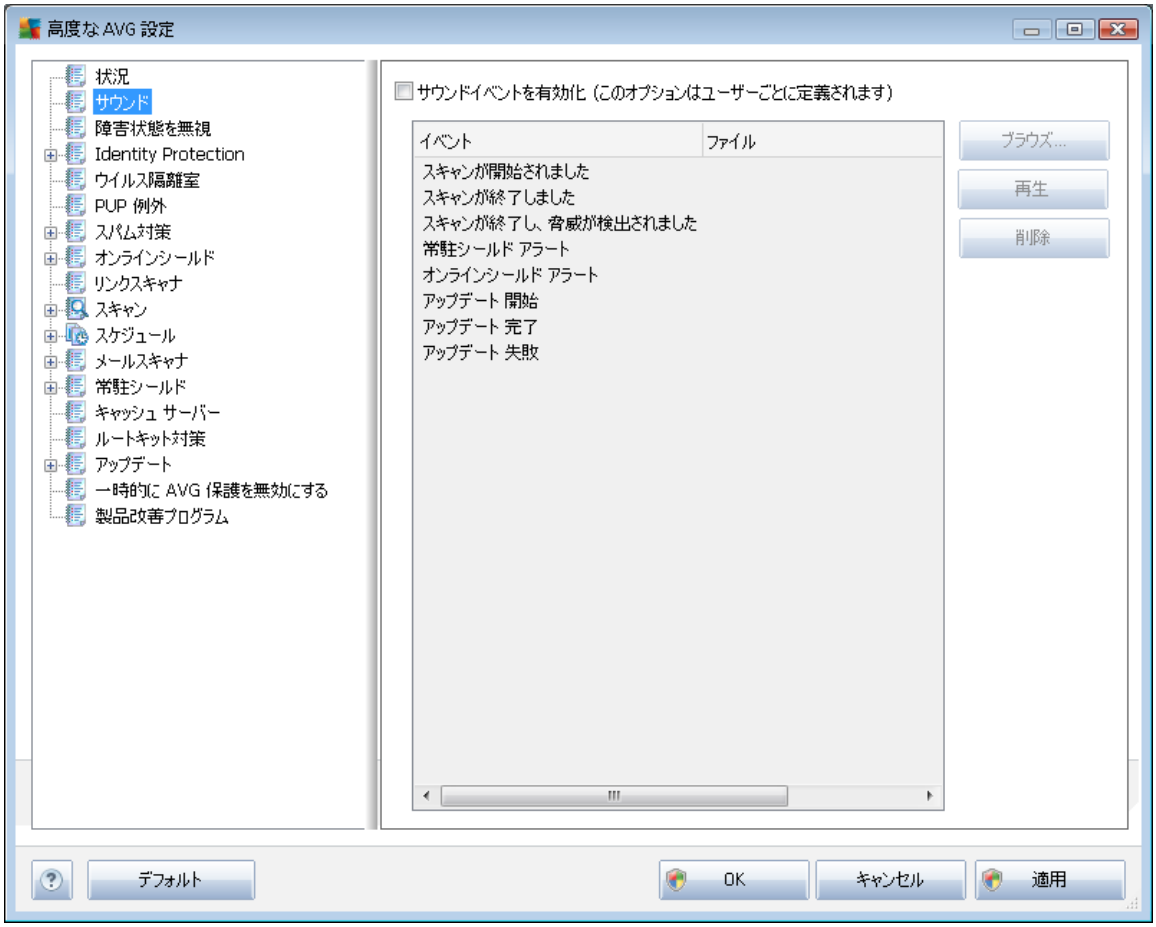
- ***統計情報通知を表示する*** - このオプションにチェックを付けると、定期的な統計情報確認通知をシステム トレイに表示できます。

### ゲーム モード

この AVG 機能は、AVG 情報バルーン (*スケジュール スキャンが開始するときなどに表示*) によって妨害される可能性がある全画面アプリケーション用に設計されています (*情報バルーンはアプリケーションの最小化やグラフィックの破損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ばときにゲームモードを有効にする***] オプションのチェックボックスを付けた状態にしておきます（*既定の設定*）。

## 9.2. サウンド

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

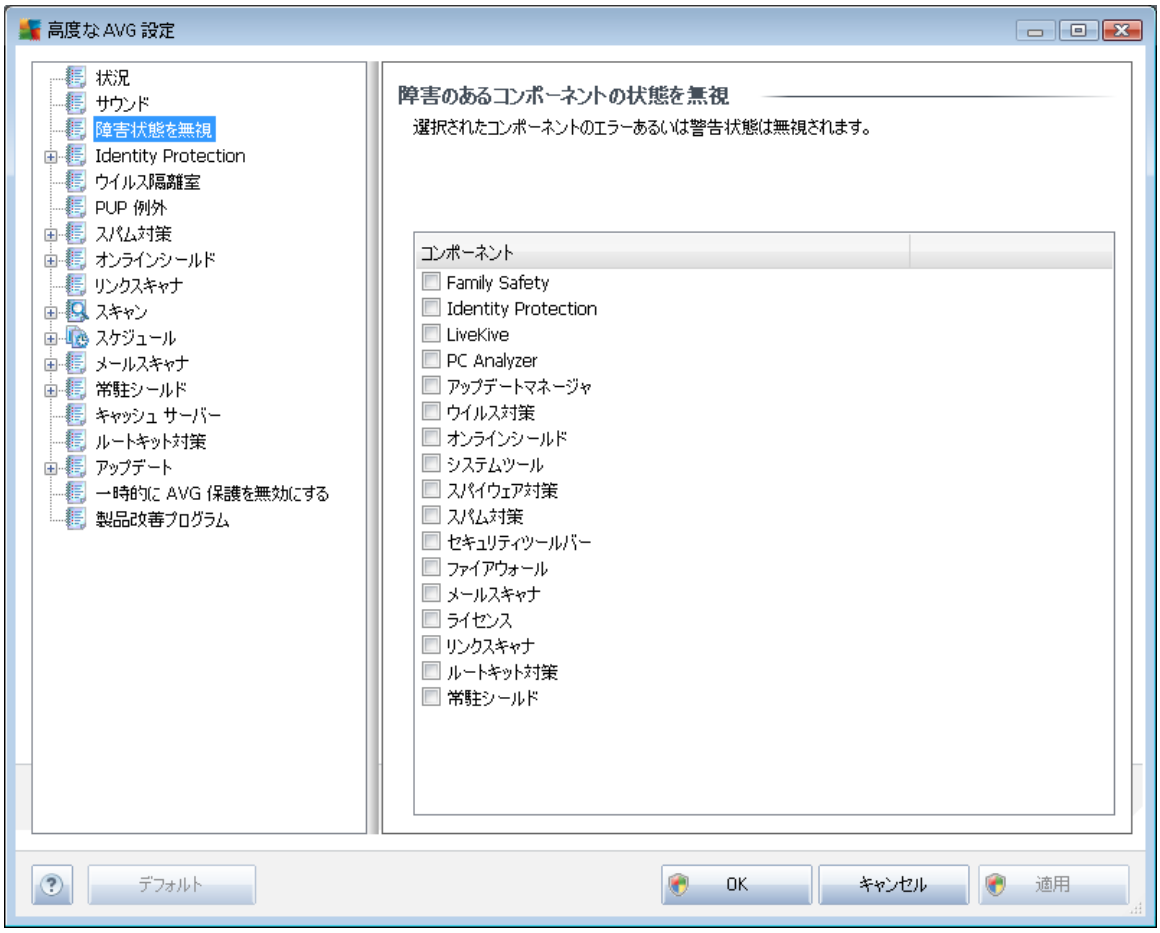



次に、リストから該当するイベントを選択し、このイベントに割り当てる適切なサウンドをディスクから参照（[***参照***]）します。選択されたサウンドを聴くには、リストのイベントをハイライトし、[***再生***] ボタンをクリックします。[***削除***] ボタンをクリックすると、特定のイベントに割り当てられたサウンドを削除します。

***注意：****.wav サウンドのみがサポートされています。*

## 9.3. エラー状態を無視

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




既定では一覧で選択されているコンポーネントはありません。つまり、コンポーネントがエラーになると、すぐに次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、
- 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。

何らかの理由で一時的にコンポーネントをオフにする必要がある場合が考えられます (*これは推奨されません。すべてのコンポーネントを永久的にオンにし続け、既定の設定を保持する必要があります。ただし、コンポーネントをオフにしなければならない状況が発生する可能性はあります*)。この場合、システム トレイ アイコンがコンポーネントのエラー状態を自動的に報告します。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

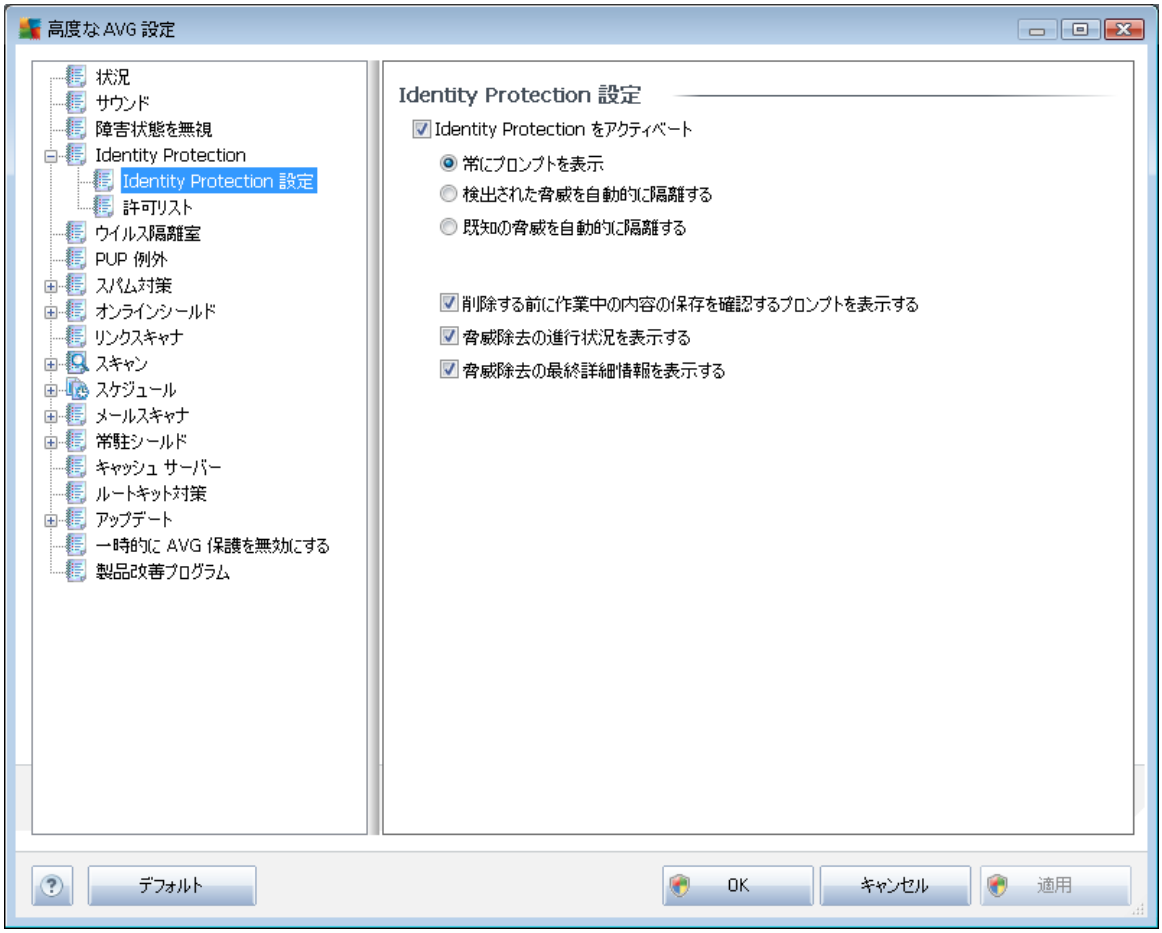
明できません。同時に、グレイ色で表示されると、アイコンは表示される可能性のある他のエラーを実際に報告できません。

この場合、上記のダイアログでエラー状態となる可能性のある（*あるいはオフになる*）コンポーネントを選択できますが、その状態は通知されません。特定のコンポーネントについては、***コンポーネント状態を無視***と同じオプションが AVG メイン ウィンドウのコンポーネント概要から直接利用できます。

## 9.4. Identity Protection

### 9.4.1. Identity Protection 設定

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




***Identity Protection を有効化*** (*既定ではオン*) - チェックを外すと、***Identity Protection***コンポーネントをオフにします。

***必要でない場合は、これを行わないことを強く推奨します。***

*Identity Protection*が有効化されている時は、脅威が検出された時の動作を指定できます。

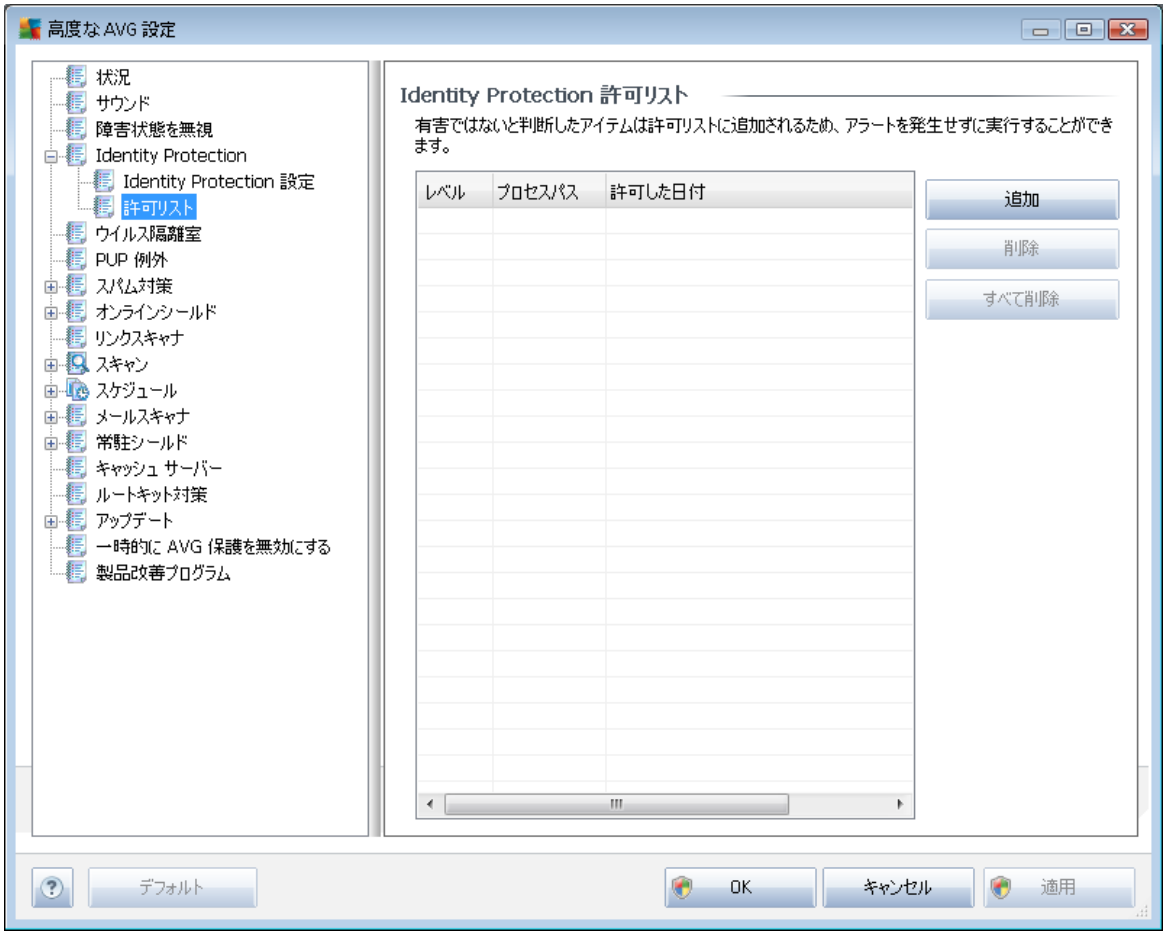
- ***常にプロンプトを表示*** *(デフォルトではオン)* - 脅威が検出されたときに、隔離室に移動するかを確認するプロンプトが表示され、実行するアプリケーションが削除されないようになります。
- ***自動的に検出された脅威を隔離*** - (デフォルトではオフ) このチェックボックスをオンにすると、すべての検出された潜在的な脅威は即時 ***AVG ウイルス隔離室***の安全な場所に移動されます。既定の設定を保持していると、脅威が検出されたときに、隔離室に移動するかを確認するプロンプトが表示され、実行するアプリケーションが削除されないようになります。
- ***自動的に既知の脅威を隔離*** - マルウェアの可能性があるものとして検出された全てのアプリケーションを自動的に即時に ***AVG ウィルス隔離室***に移動する場合は、この項目にマークを付けておきます。

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

- ***除去前に作業内容の保存を確認するプロンプトを表示*** - *(デフォルトではオン)* - マルウェアの可能性があるものとして検出されたアプリケーションを隔離に移動する前に警告メッセージを表示する場合は、この項目をオンにしておきます。そのアプリケーションでのみ作業している場合は、プロジェクトが失われる可能性があるため、最初に保存しておく必要があります。デフォルトでは、この項目はオンであり、この設定を保持することをお勧めします。
- ***マルウェア除去の進捗を表示*** - *(デフォルトではオン)* - この項目をオンにすると、潜在的なマルウェアが検出された時点で、新しいダイアログが開き、マルウェアの隔離除去の進捗が表示されます。
- ***最終マルウェア除去の詳細情報を表示*** - *(デフォルトではオン)* - このアイテムをオンにすると、***ID 保護***は、隔離に移動された各オブジェクトに関する詳細 *(重要度レベル、場所など) を表示します*.

### 9.4.2. 許可リスト

[***Identity Protection 設定***] ダイアログで、[***検出された脅威を自動的に隔離する***] 項目のチェックを外すと、潜在的な危険性のあるマルウェアが検出されるたびに、削除確認ダイアログが表示されます。*動作に応じて検出された*不審なアプリケーションを安全なアプリケーションとして指定し、コンピュータ上で保持することを確認すると、そのアプリケーションはいわゆる ***Identity Protection 許可リスト***に追加され、今後は潜在的に危険なアプリケーションとして報告されなくなります。



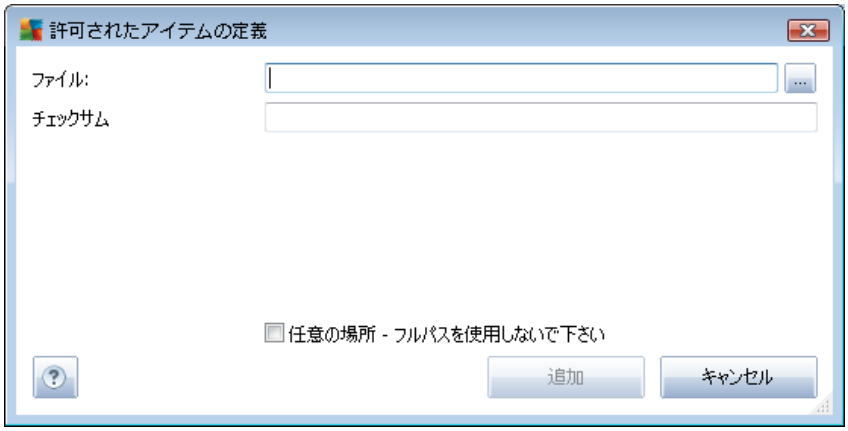

***Identity Protection 許可リスト***は、各アプリケーションに関する次の情報を提供します。

- ***レベル*** - 重要度の低いもの (■□□□) から重大なもの (■■■■) までの 4 段階方式で各プロセスの重要度をグラフィカルに示します。
- ***プロセス パス*** - アプリケーションの (*プロセス*) 実行ファイルの場所へのパス
- ***許可された日付*** - 手動でアプリケーションを安全なアプリケーションとして指定した日

## コントロール ボタン

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

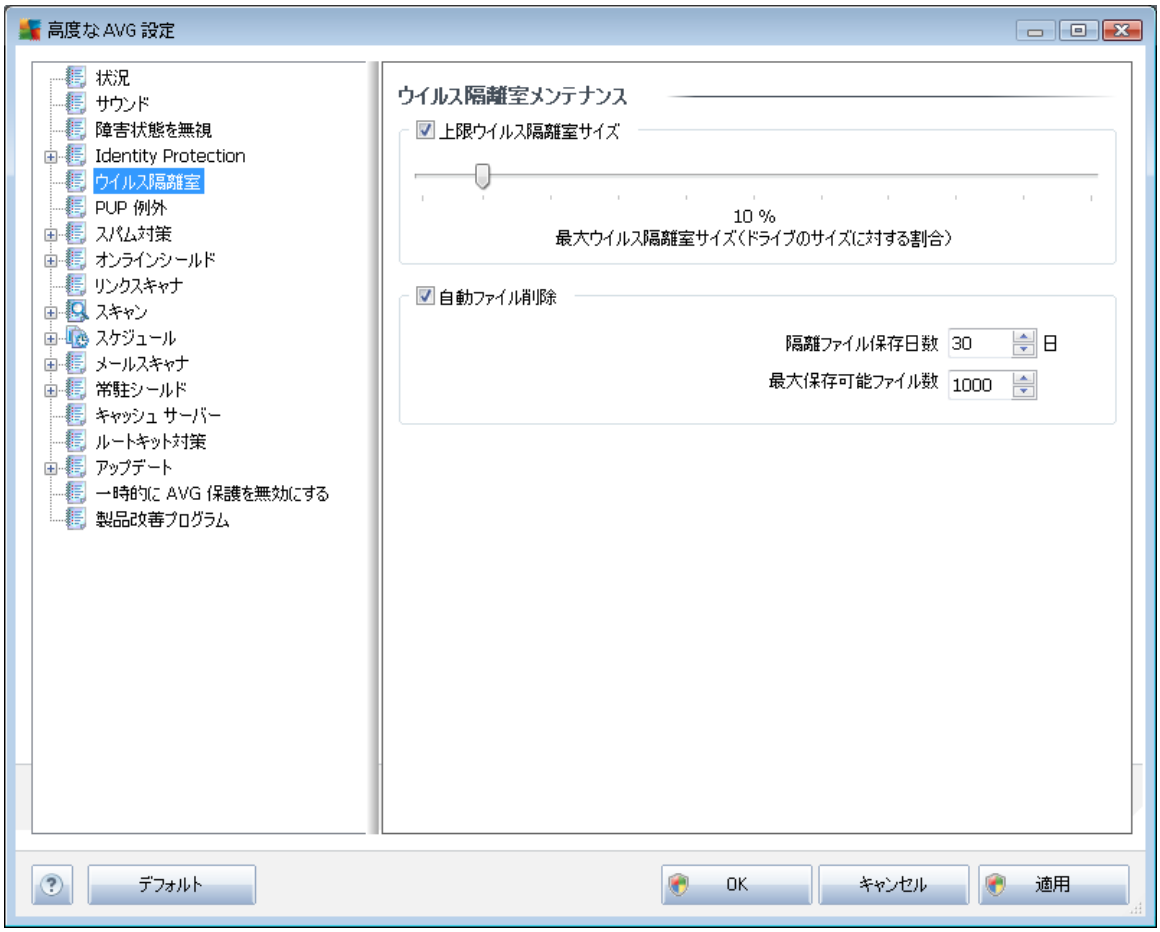
- ***追加*** - このボタンをクリックすると、許可リストに新しいアプリケーションを追加します。次のポップアップ ダイアログが表示されます。




- ***ファイル*** - 例外として指定するファイル (*アプリケーション*) への完全パスを入力します。
- ***チェックサム*** - 選択されたファイルの一意の「シグネチャ」を表示します。このチェックサムは自動的に生成された文字列です。AVG はこの文字列を使用して、選択されたファイルとその他のファイルを区別します。チェックサムはファイルが正常に追加された後で生成および表示されます。
- ***任意の場所 - 完全パスを使用しない*** - 特定の場所のみに関連する例外としてこのファイルを定義する場合は、このチェックボックスのチェックを外します。

- ***削除*** - このボタンをクリックすると、選択したアプリケーションをリストから削除します。
- ***すべて削除*** - このボタンをクリックすると、リストに表示されているすべてのアプリケーションを削除します。

## 9.5. ウイルス隔離室



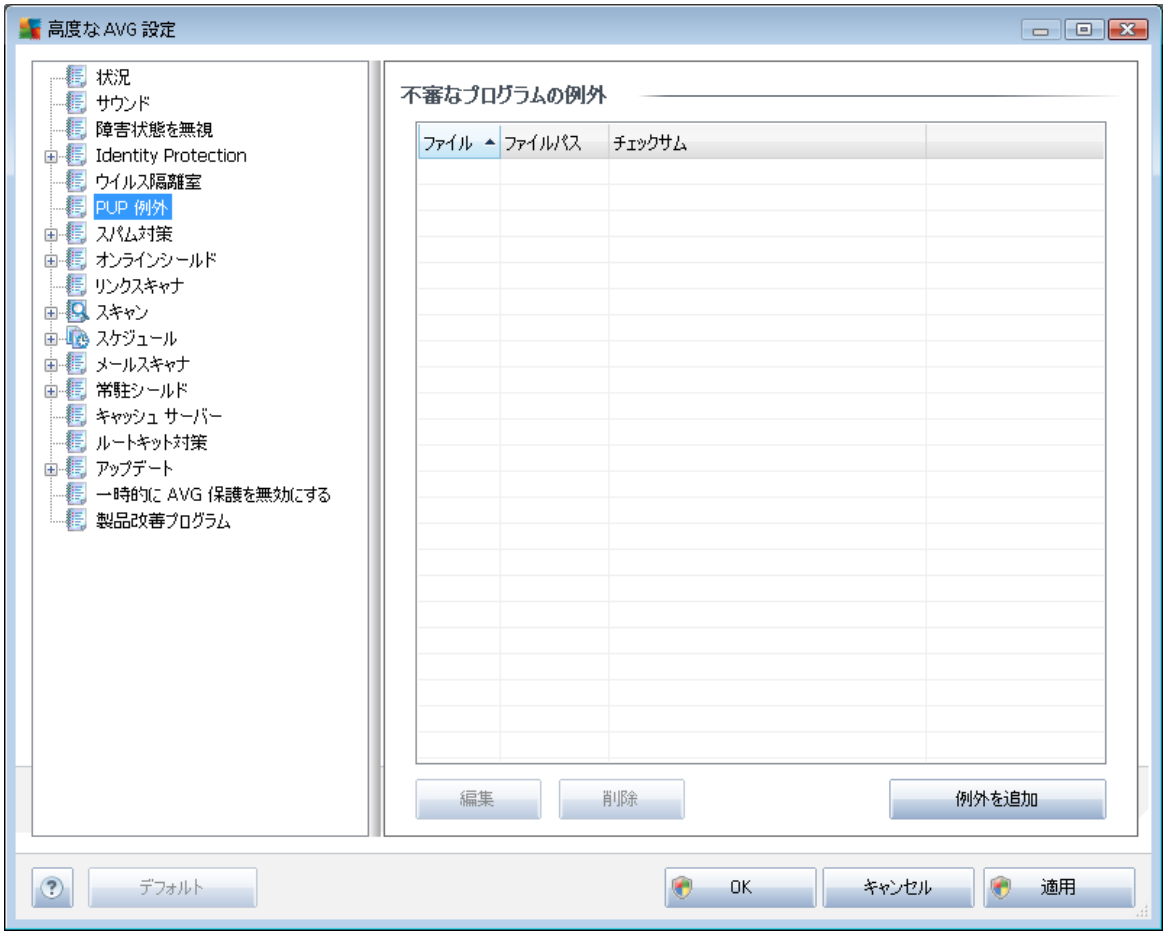

***ウィルス隔離メンテナンス***ダイアログでは、***ウィルス隔離***に格納されるオブジェクト管理に関するパラメータを定義できます。

- ***ウイルス隔離室のサイズを制限***- スライダを使用して、***ウイルス隔離室***の最大サイズを設定できます。サイズは、ローカルディスクのサイズに対する割合で指定されます。
- ***自動ファイル削除***- このセクションでは、***ウイルス隔離室***にオブジェクトが格納される最大日数（***日数を経過したファイルの削除***）、と***ウイルス隔離室***に格納される最大ファイル数（***格納されるファイルの最大数***）を定義します。

## 9.6. PUP 例外

**AVG Internet Security 2011** はシステム内に存在する不審な実行可能アプリケーションや DLL ライブラリの分析と検出ができます。ユーザーが望ましくないプログラムをコンピュータに残しておきたい場合もあります (*故意にインストールされたプログラム*)。一部のプログラム (特に無料のプログラム) にはアドウェアが含まれています。このようなアドウェアは AVG によって***不審な***

***プログラム***として検出され、報告される場合があります。このようなプログラムをコンピュータに残す場合は、不審なプログラムの例外として定義できます。




[***不審なプログラム例外***] ダイアログでは、既に定義された不審なプログラムの例外リストが表示されます。リストの編集、既存の項目の削除、新しい例外の追加ができます。各例外リストには次の情報が表示されます。

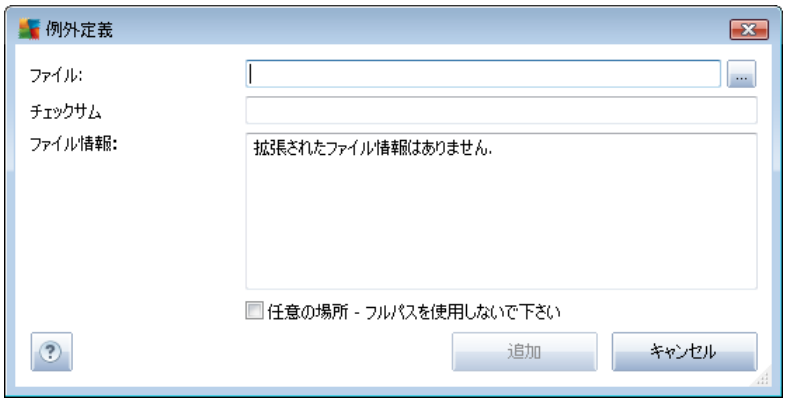
- ***ファイル*** - 各アプリケーション名。
- ***ファイル パス*** - アプリケーションの場所。
- ***チェックサム*** - 選択したファイルの一意の「シグネチャ」を表示します。このチェックサムは自動的に生成された文字列です。AVG はこの文字列を使用して、選択したファイルとその他のファイルを区別します。チェックサムはファイルが正常に追加された後で生成および表示されます。

## コントロール ボタン

- ***編集*** - 既に定義された例外の編集ダイアログ (*新しい例外定義ダイアログと同*

じです。次を参照) を開きます。ここで例外パラメータを変更します。

- ***削除*** - 選択した項目を例外リストから削除します。
- ***例外の追加***- 編集ダイアログが開きます。ここでは作成する例外のパラメータを定義します。




o ***ファイル*** - 例外として指定するファイルへの完全パスを入力します。

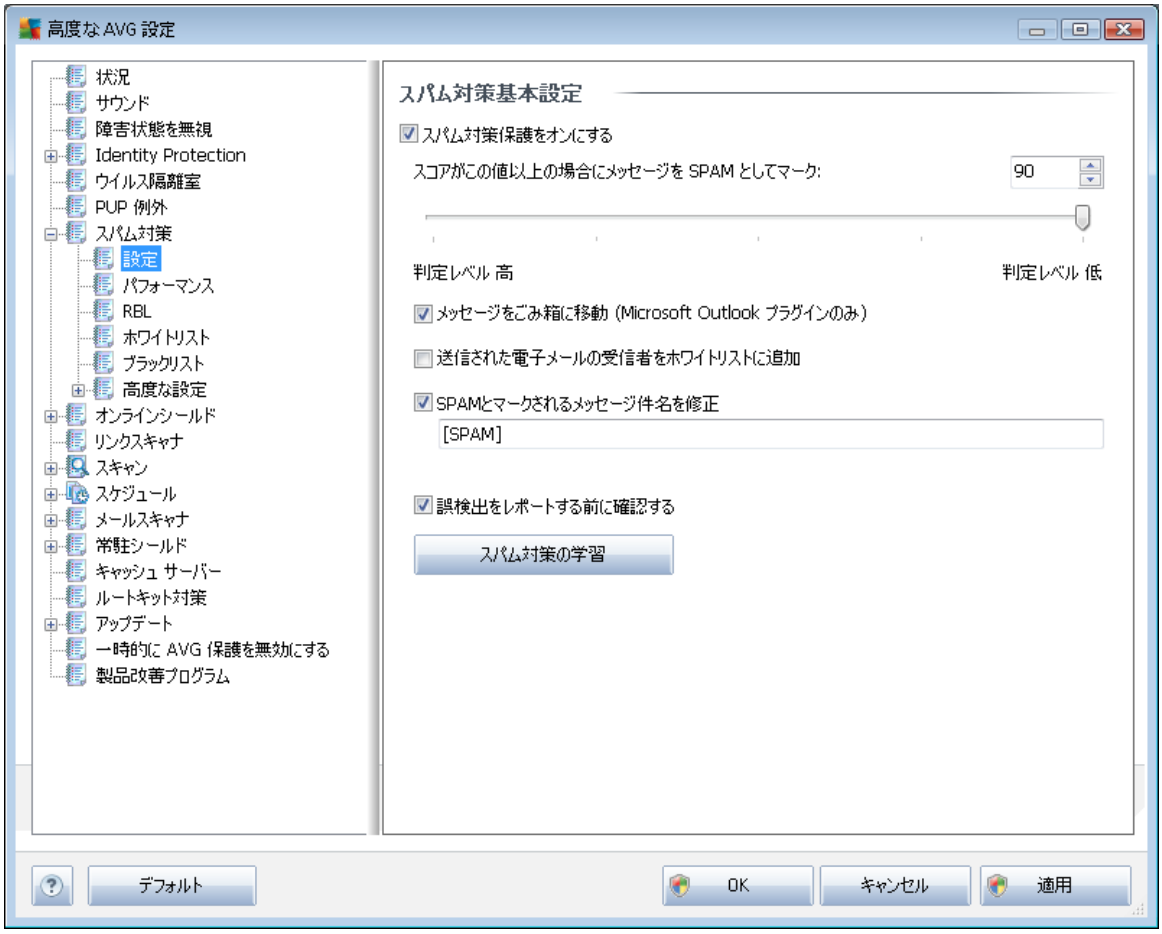
o ***チェックサム*** - 選択したファイルの一意の「シグネチャ」を表示します。このチェックサムは自動的に生成された文字列です。AVG はこの文字列を使用して、選択したファイルとその他のファイルを区別します。チェックサムはファイルが正常に追加された後で生成および表示されます。

o ***ファイル情報*** - ファイルに関する追加情報 (*ライセンス/バージョンなど*)。

o ***任意の場所 - 完全パスを使用しない*** - 特定の場所のみに関連する例外としてこのファイルを定義する場合は、このチェックボックスのチェックを外します。このチェック ボックスを選択すると、ファイルの保存場所に関係なく、指定したファイルが例外として定義されます (*ただし、特定のファイルへの完全パスを入力する必要があります。これにより、システムに同じ名前のファイルが 2 つ存在している場合にファイルが一意の例として使用されます*)。

## 9.7. スパム対策

### 9.7.1. 設定




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

次に、スコアの判定レベルを選択することができます。***スパム対策***フィルタは、複数の動的スキャン技術に基づいて、各メッセージにスコアを割り当てます（*例えば、メッセージの内容がSPAMにどの程度類似しているか等*）。値を入力するかスライダを左右に動かす（*値の範囲は 50 ～ 90*）ことによって、[***スコアがこの値を超える場合スパムとしてメッセージを判定する***] 設定を調整できます。

一般的には、閾値を50から90の間、不明な場合は、90に設定することを推奨します。以下はスコアの閾値の一般的な概要です。

- ***値 80 ～ 90*** - スパムの可能性が高いメールは除外されます。一部の正常なメッセージも誤って除外される可能性があります。
- ***値 60 ～ 79*** - かなり積極的な設定です。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。通常、この値は推奨されません。

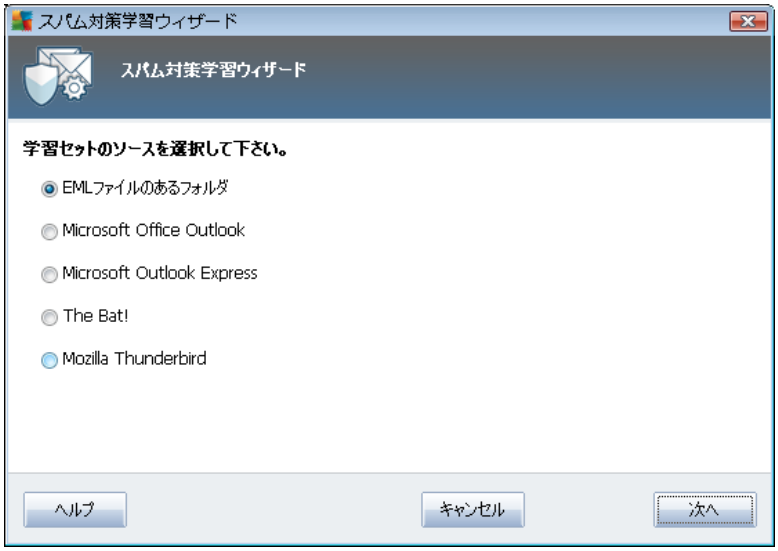
***スパム対策基本設定***ダイアログでは、さらに検出されたスパムメールメッセージが処理される方法を定義することができます。

- ***メッセージをスパムフォルダに移動*** - この項目をチェックすると、検出されたスパムメッセージは、自動的にメールクライアントの迷惑メールフォルダに移動されます。
- ***送信メールの受信者を*****ホワイトリスト**に追加 - このチェックボックスにチェックを付けると、すべての送信メールの受信者が信頼でき、その受信者のメールアカウントから送信されるすべてのメールメッセージの配信を許可することを確認します。
- ***スパムとして判定されたメッセージの件名を修正*** - スパムとして検出されたメッセージの件名にを特定の単語や文字を追加したい場合、このチェックボックスにチェックを付けます。追加するテキストをテキストフィールドに入力します。
- ***誤検出を報告する前に確認する*** - インストール処理中に***製品改善プログラム***に参加することに同意した場合、検出された脅威が AVG に報告されます。報告は自動的に実行されます。ただし、このチェック ボックスを選択すると、ダイアログ ボックスを表示し、メッセージがスパム メールであるかどうかを確認してから、検出されたスパムを AVG に送信することができます。

## コントロールボタン

[***スパム対策の学習***] ボタンは、***次の章***で詳しく説明されているスパム対策学習ウィザードを実行します。

***スパム対策学習ウィザード***の最初のダイアログでは、学習のためのメールソースを選択します。通常は、間違ってSPAMとしてマークされたメールや、認識されなかったスパムメッセージを使用します。




以下のオプションがあります。

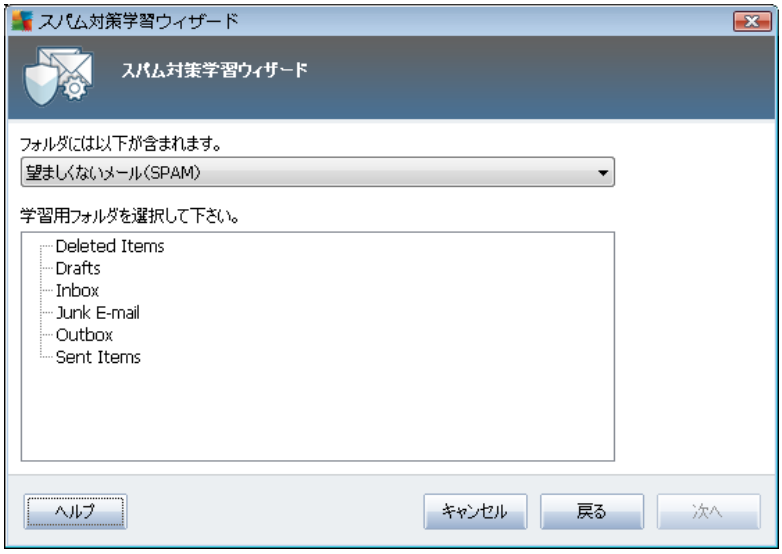
- ***特定のメールクライアント*** - リストされたメールクライアントの 1 つ (*MS Outlook*、*Outlook Express*、*The Bat!*) を使用する場合、該当するオプションを選択します。
- ***EML ファイルのあるフォルダ*** - 他のメールプログラムを利用する場合、まずメッセージを特定のフォルダに保存（*.eml*形式）、またはメールクライアントメッセージフォルダの場所を確認します。次に、***EML ファイルのあるフォルダ***を選択します。次のステップで希望するフォルダを指定します。

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

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

このステップで表示されるダイアログはこれまでの選択内容によって異なります。

## EML ファイルのあるフォルダ



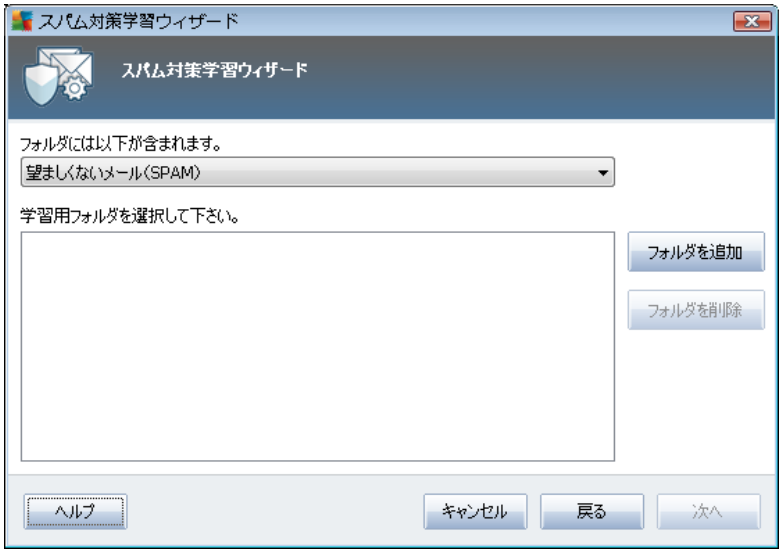

このダイアログでは学習に使用するメッセージ フォルダを選択します。[***フォルダの追加***] ボタンをクリックして、.eml ファイル (*保存された電子メール メッセージ*) のあるフォルダを参照します。選択したフォルダがダイアログに表示されます。

***フォルダには次の内容が含まれます。*** ドロップダウン メニューには 2 つのオプションが表示されます。ここでは選択したフォルダが望ましい (*HAM*) メールあるいは望ましくない (*SPAM*) メールのいずれを含むかを選択します。次のステップでメッセージをフィルタリングできます。フォルダには学習メールのみを含む必要はありません。また、[***フォルダの削除***] ボタンをクリックして、選択した望ましくないフォルダを一覧から削除できます。

完了したら、[**次へ**] をクリックして、[***メッセージ フィルタリング オプション***] に進みます。

## 特定の電子メール クライアント

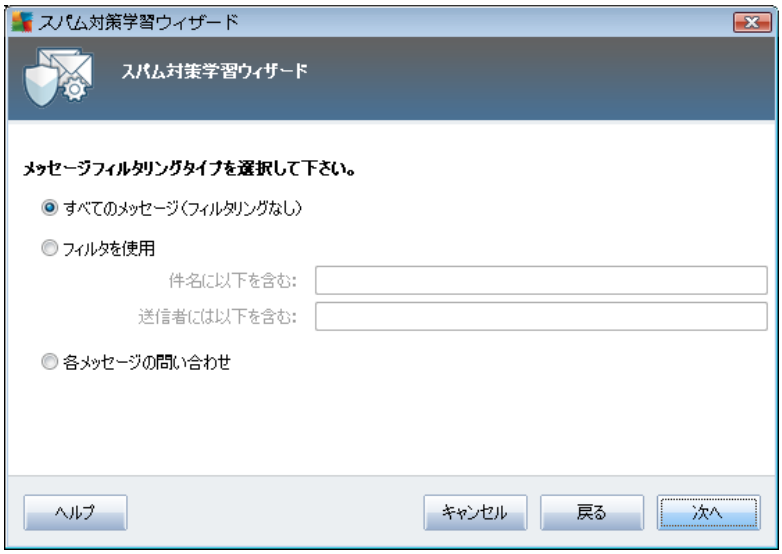
オプションのいずれかを確認した場合、新しいダイアログが表示されます。




***メモ:** Microsoft Office Outlook の場合、最初に Microsoft Office Outlook プロファイルを選択するように指示されます。*

***フォルダには次の内容が含まれます。*** ドロップダウン メニューには 2 つのオプションが表示されます。ここでは選択したフォルダが望ましい (*HAM*) メールあるいは望ましくない (*SPAM*) メールのいずれを含むかを選択します。次のステップでメッセージをフィルタリングできます。フォルダには学習メールのみを含む必要はありません。選択した電子メール クライアントのナビゲーション ツリーがダイアログのメイン セクションに表示されます。ツリー上で任意のフォルダを選択して強調表示させます。

完了したら、[**次へ**] をクリックして、[***メッセージ フィルタリング オプション***] に進みます。




このダイアログでは、メールメッセージのフィルタリングを設定します。

選択されたフォルダが学習に使用したいメッセージのみを含むことが確実な場合は、***すべてのメッセージ（フィルタなし）***オプションを選択します。

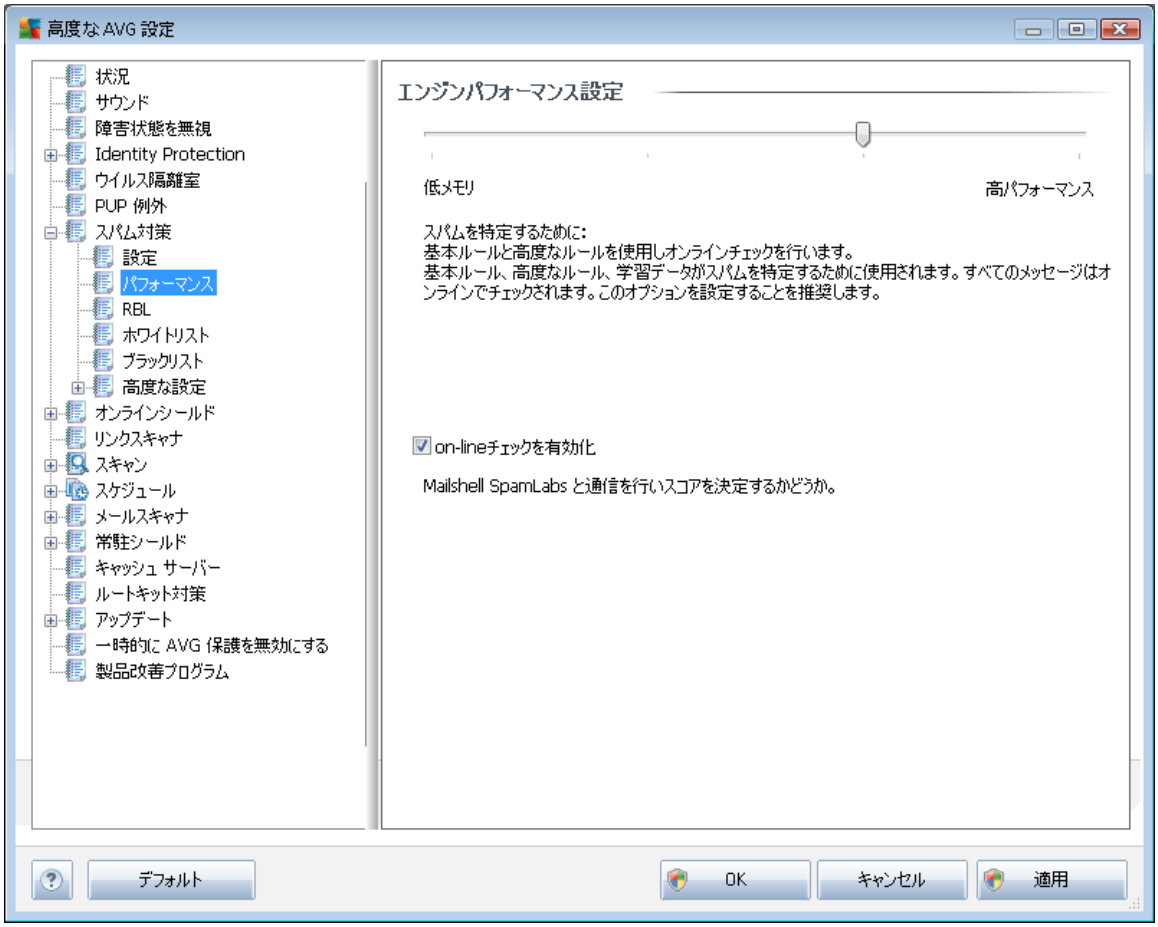
フォルダに含まれるすべてのメッセージについて確認（学習するかどうかを決定できるように）する場合、***各メッセージを確認***オプションを選択します。

高度なフィルタを使用する場合、***フィルタを使用***オプションを選択します。メールの件名、送信者欄で検索する場合、単語（*名前*）、単語の一部、フレーズを入力します。正確に条件にマッチするメッセージ全てが学習に使用されます。

***注意！****両方のテキストフィールドに入力すると、2つの条件のうちのいずれかにマッチするアドレスが使用されます。*

適切なオプションを選択し、[**次へ**] をクリックします。以後のダイアログは情報のみが表示され、ウィザードがメッセージを処理する準備ができていることを示します。学習を開始するには**次へ**ボタンを再度クリックします。学習は、選択された条件に応じて開始されます。

### 9.7.2. パフォーマンス




[***エンジン パフォーマンス設定***] ダイアログ (*左側のナビゲーションの [**パフォーマンス**] からリンク*) 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できます。

スライダを左右に動かして、***低メモリ消費***モードと***高パフォーマンス*** モードの間でスキャン パフォーマン レベルを変更します。

- ***低メモリ消費*** - スキャン処理でスパムを判定するときに、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。

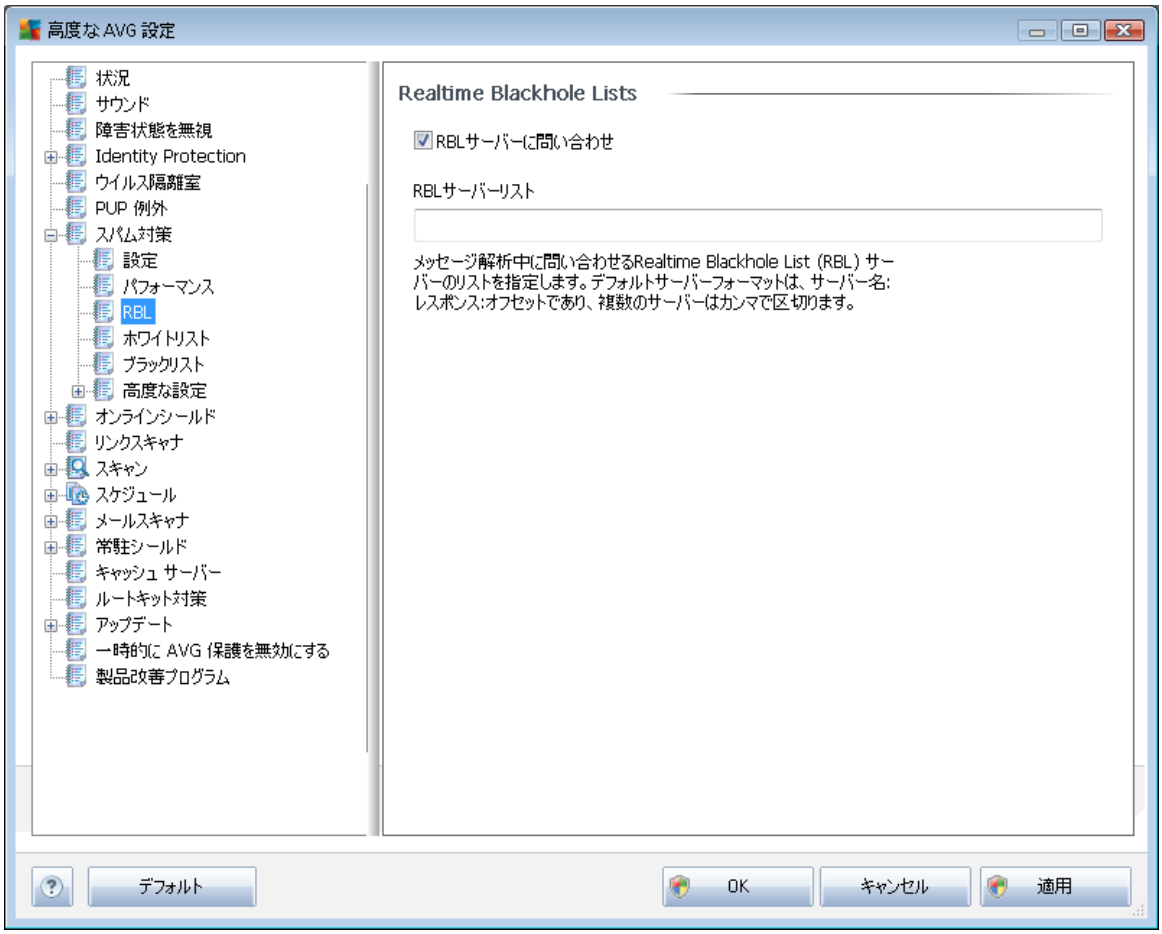
- ***高パフォーマンス*** - このモードでは大量のメモリを消費します。スパム スキャン中には、ルールとスパム データベース キャッシュ、基本ルール、高度なルール、スパム送信者 IP アドレス、スパム送信者データベース機能が使用されます。

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

***通常、やむを得ない理由がある場合を除き、既定の設定を保持することをお勧めします。この設定の変更は上級者ユーザーのみが行ってください。***

### 9.7.3. RBL

[***RBL***] 項目をクリックすると、***リアルタイム ブラックホール リスト***と呼ばれる編集ダイアログが開きます。




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

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

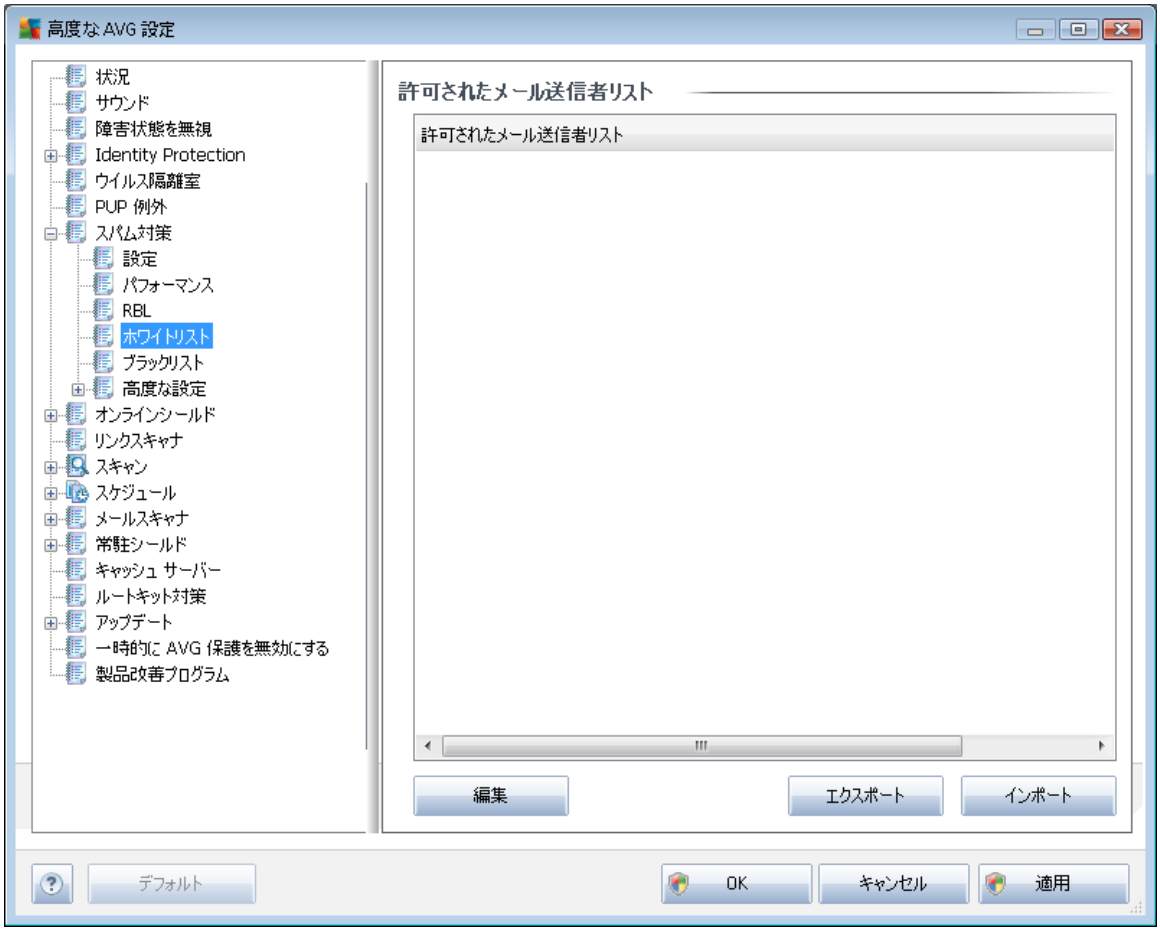
***RBLサーバーリスト***では、特定のRBLサーバーの場所を定義できます。

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

***いかなる個人データもサーバーには送信されません。***

### 9.7.4. ホワイトリスト

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




編集インターフェースでは、望ましくないメッセージ（スパム）が送信されないことが確実である送信者のリストを編集できます。また、スパムメッセージが生成されないことがわかっているドメイン名（*avg.com*等）のリストを編集します。

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

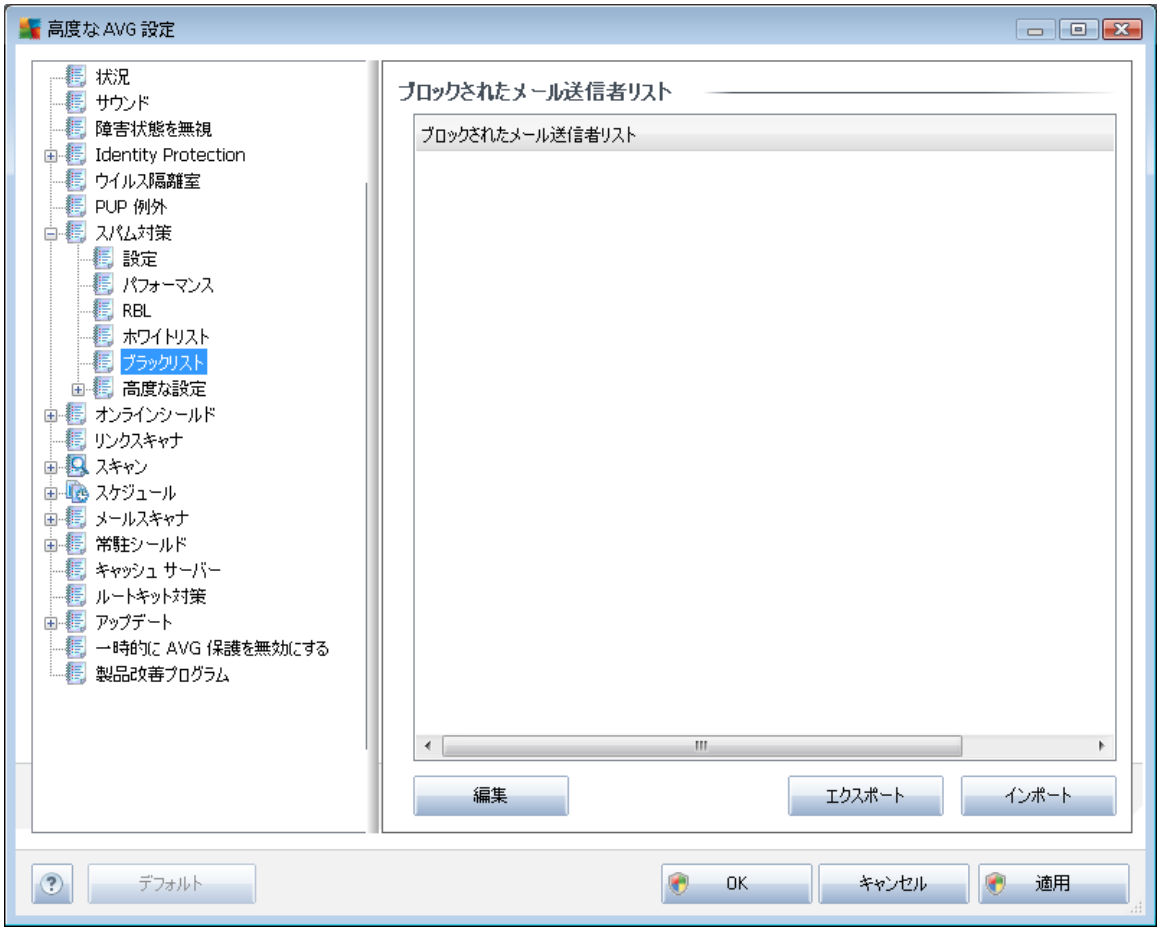
- ***編集*** - このボタンをクリックすると、ダイアログが開きます。このダイアログでは、手動でアドレスのリストを入力できます（*コピーとペースト*も使用できます）。1行に1アイテム（*送信者*、*ドメイン名*）を入力します。
- ***エクスポート*** - 何らかの目的でレコードをエクスポートする場合は、このボタ

ンをクリックします。すべてのレコードがプレーン テキスト形式で保存されます。

- ***インポート***- すでにメールアドレスやドメイン名のテキストファイルお持ちの場合、このボタンを選択することで単純にそのリストをインポートすることができます。ファイルの内容については、1 行につき 1 項目 (*アドレス*、*ドメイン名*) のみを含める必要があります。

### 9.7.5. ブラックリスト

[***ブラックリスト***] 項目は、常に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グローバル リストが表示されるダイアログを開きます。




編集インターフェースでは、望ましくないメッセージ （スパム） を送信するであろう送信者のリストを編集します。また、スパムメッセージが送信される完全なドメイン名リスト （*spammingcompany.com* など） を編集できます。リスト中のアドレスとドメインからのメールは、すべてスパムとして判定されます。

既にスパム送信者やドメイン名のリストがある場合は、各メールアドレスを直接入力するか、一度にアドレスの全リストをインポートすることでリストを入力できます。次のコントロールボタンが提供されています。

- ***編集*** - このボタンをクリックすると、ダイアログが開きます。このダイアログでは、手動でアドレスのリストを入力できます（*コピーとペースト*も使用できます）。1行に1アイテム（*送信者*、*ドメイン名*）を入力します。

- ***エクスポート*** - 何らかの目的でレコードをエクスポートする場合は、このボタンをクリックします。すべてのレコードがプレーン テキスト形式で保存されます。

- ***インポート*** - すでにメールアドレスやドメイン名のテキストファイルお持ちの場合、このボタンを選択することで単純にそのリストをインポートすることができます。

### 9.7.6. 高度な設定

***高度な設定の部分には、スパム対策コンポーネントに関するさまざまな設定オプションが表示されます。これらの設定は、電子メール サーバーの保護を最適化する目的で詳細なスパム対策保護設定を行う必要があるネットワーク管理者などの上級ユーザー向けです。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.) の高度な設定について十分に理解していない場合は、設定変更を行わないことを強くお勧めします。不適切にファイルが変更された場合は、パフォーマンスの悪化やコンポーネント機能の不正動作につながる可能性があります。***

非常に高度なレベルで***スパム対策***設定を変更する必要がある場合は、ユーザー インターフェースに直接表示される指示に従ってください。一般的には、各ダイアログでは 1 つの特定の機能の確認と編集ができます。その説明は常にダイアログに表示されます。

- ***キャッシュ*** - フィンガープリント、ドメイン レピュテーション、LegitRepute

- ***トレーニング*** - 最大ワード エントリ、自動学習しきい値、重み

- ***フィルタリング*** - 言語リスト、国リスト、許可された IP、ブロックする IP、ブロックする国、ブロックする文字セット、スプーフィング送信者

- ***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

## 9.8. オンライン シールド

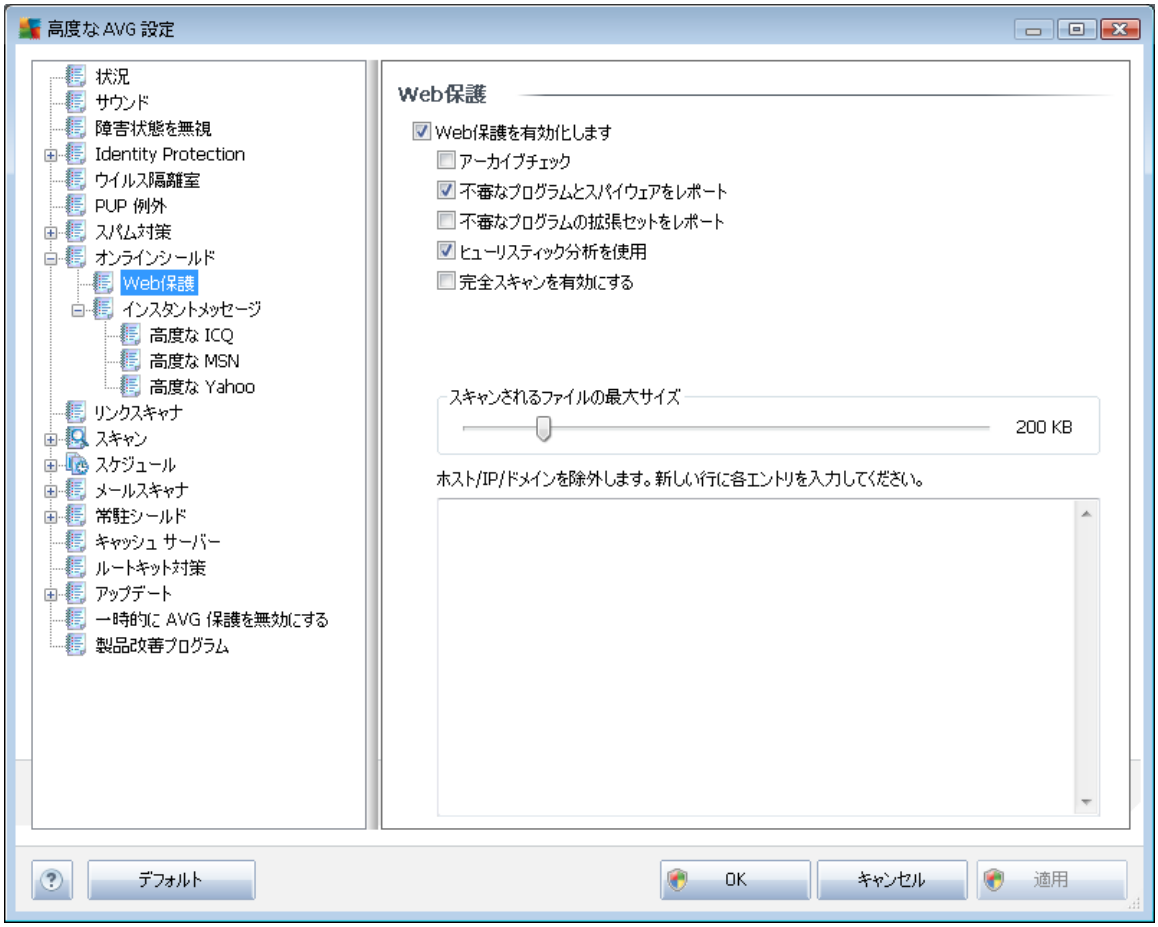

[***オンライン シールド***] ダイアログでは、[***オンライン シールドを有効にする***] オプション (***既定では有効***) を使用して、*オンライン シールド* コンポーネントを有効化/無効化できます。このコンポーネントのさらに高度な設定については、ツリーナビゲーションのリストの後に続くダイアログにしたがってください。

- ***Web保護***
- ***インスタントメッセージ***

### 脅威通知モード

ダイアログの下部では、検出された起こりうる脅威に関する情報を通知する方法を選択します：標準ポップアップダイアログ経由、トレイバルーン通知経由、あるいはトレイアイコン情報経由。

### 9.8.1. Web 保護




***Web保護***ダイアログでは、Webコンテンツのスキャンに関するコンポーネント設定を編集することができます。編集インターフェースでは、以下の基本オプションを設定します。

- ***Web の保護を有効化*** - このオプションがチェックされている場合、***オンライン シールド***は WWW ページのスキャンを実行します。このオプションがオン（デフォルト）の場合、さらに以下の項目のオン/オフを変更することができます。
    - ***アーカイブをチェックする*** - (*既定ではオフ*): WWW ページに含まれるアーカイブ コンテンツをスキャンします。
    - ***不審なプログラムとスパイウェアをレポート*** - (*デフォルトではオン*): チェックを付けると、***スパイウェア対策エンジンを有効化し、ウイルスと同時にスパイウェアもスキャンします。***スパイウェアは疑わしいマルウェアのカテゴリに含まれます。通常は、セキュリティ リスクとなる場合でも、このようなプログラムを故意にインストールすることができます。コンピュータのセキュリティを高めるため、この機能を有効にしておくことをお勧めします。

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

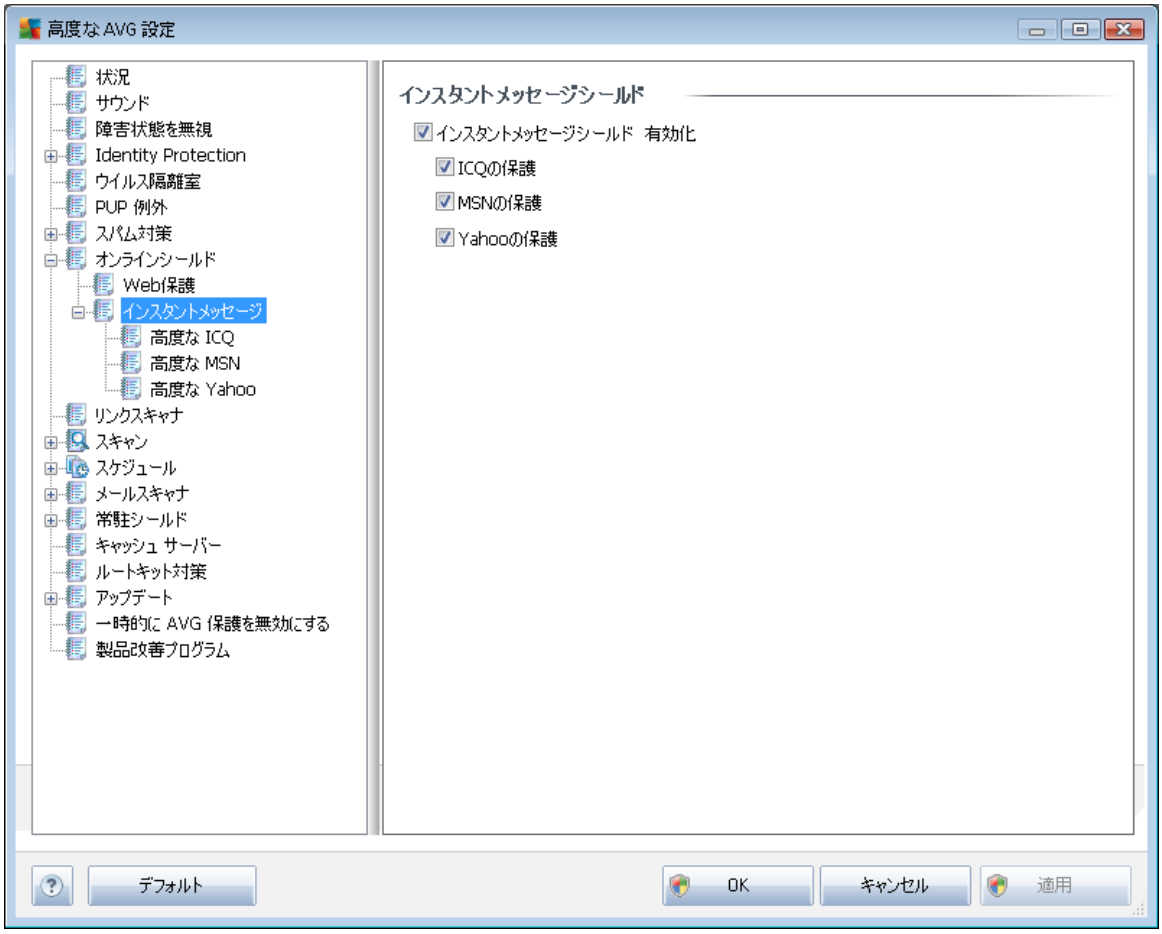
- ***ヒューリスティック分析を使用する*** - (*既定ではオン*): ヒューリスティック分析 (仮想コンピュータ環境での*スキャン オブジェクトの動的エミュレーション*) を使用して、表示されるページ コンテンツをスキャンします。

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

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

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

### 9.8.2. インスタント メッセージ

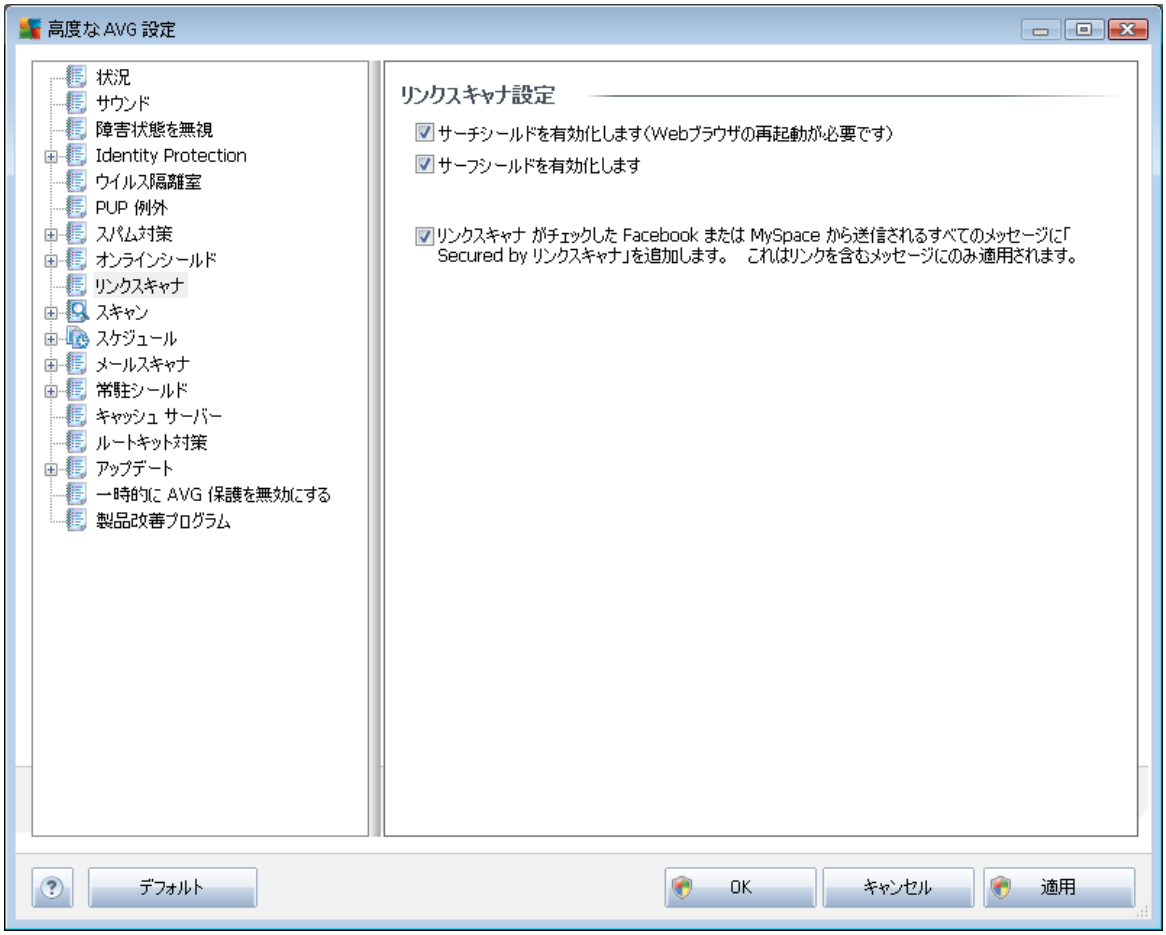



[***インスタント メッセージ シールド***] ダイアログでは、***オンライン シールド***コンポーネントのインスタント メッセージ スキャンに関する設定を編集します。現在は次の3つのメッセージング プログラムがサポートされています。***ICQ***、***MSN***、***Yahoo*** - ***オンライン シールド***がオンライン通信がウィルス フリーだということを確認するようにしたい場合は、この中から該当するアイテムをチェックします。

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

## 9.9. リンクスキャナ

[*リンク スキャナ設定*] ダイアログでは、*リンク スキャナ* 基本機能のオフ/オンを切り替えることができます。




- サーチ シールドを有効にする - (既定ではオン): Google、Yahoo! JP、WebHledani、Yandex、Baidu、Bing、AOL、AltaVista、EarthLink、Ask、Seznam、eBay、Twitter、Digg、SlashDot を使用して実行した検索結果に対して評価通知アイコンが表示されます。検索エンジンで返されたサイトの内容が事前にチェックされます。

- サーフ シールドを有効にする - (既定ではオン): ユーザーがサイトにアクセスしようとするときに、積極的にリアルタイムでエクスプロイト サイトを検出し、保護を実施します。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。

- ***「Secured by LinkScanner」を追加する...*** - この項目にチェックを付けると、Facebook および MySpace ソーシャル ネットワークから送信されるメッセージにアクティブなハイパーリンクが含まれる場合に、*リンクスキャナ* チェックに関する認証通知をすべてのメッセージに追加します。

## 9.10. 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。

- ***完全コンピュータ スキャン*** - 標準の事前定義された完全コンピュータ スキャンです。
- ***シェル拡張スキャン***- Windows Explorer 環境から直接選択されたオブジェクトのスキャンです。
- ***特定ファイルまたはフォルダのスキャン*** 予め定義されたコンピュータの特定エリアのスキャンです。
- ***リムーバブルデバイスのスキャン*** - コンピュータに接続した特定のリムーバブルデバイスのスキャン

### 9.10.1. 完全コンピュータ スキャン

[***完全コンピュータ スキャン***] オプションでは、ソフトウェア ベンダーがあらかじめ定義したスキャン パラメータの***完全コンピュータ スキャン***を編集できます。

## スキャン設定

[***スキャン設定***] セクションに表示されているスキャン パラメータを任意でオン/オフにできます。

- ***自動的に感染を修復/除去する*** (*既定ではオン*) - スキャン実行中にウイルスが特定され、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***ウィルス隔離室***に移動されます。

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

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

- ***Tracking Cookie をスキャンする*** (*既定ではオフ*) - スパイウェア対策コンポーネントのこのパラメータを定義すると、Cookie を検出します (HTTP cookie は、サイトの設定や電子ショッピング カートの内容など、ユーザー固有の情報の認証、追跡、メンテナンスに使用されます)。

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

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

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

さらに、スキャンするかどうかを決定する必要があります。

- ***すべてのファイル タイプとスキャン対象ではないファイル拡張子をカン***

***マで区切ったリスト*** *(保存すると、カンマはセミコロンに変わります)* を入力することで、スキャンからの除外を定義できます。

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

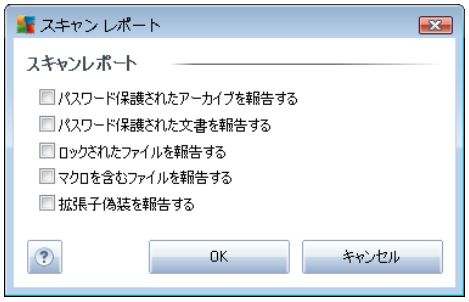
- 任意で***拡張子のないファイルをスキャン***できます。このオプションは既定ではオンになっています。変更する理由がない場合は、この設定を保持することをお勧めします。拡張子のないファイルは不審であるため、常にスキャンすることをお勧めします。

### スキャン速度を調整

[***スキャン速度を調整***] セクションでは、システム リソース使用度に応じて、任意のスキャン速度を指定できます。*既定ではこのオプションの値は、自動的にリソースを使用する*ユーザー依存レベルに設定されています。スキャンを高速化すると、スキャン時間を短縮できますが、スキャン実行中にシステム リソース消費量が著しく上がり、PC で実行されている他の作業の速度が低下します *(このオプションは、コンピュータの電源がオンであり、コンピュータ上で作業をしているユーザーがいない場合などに適しています)*。一方、スキャンの時間を延長することで、システム リソース消費量を下げることができます。

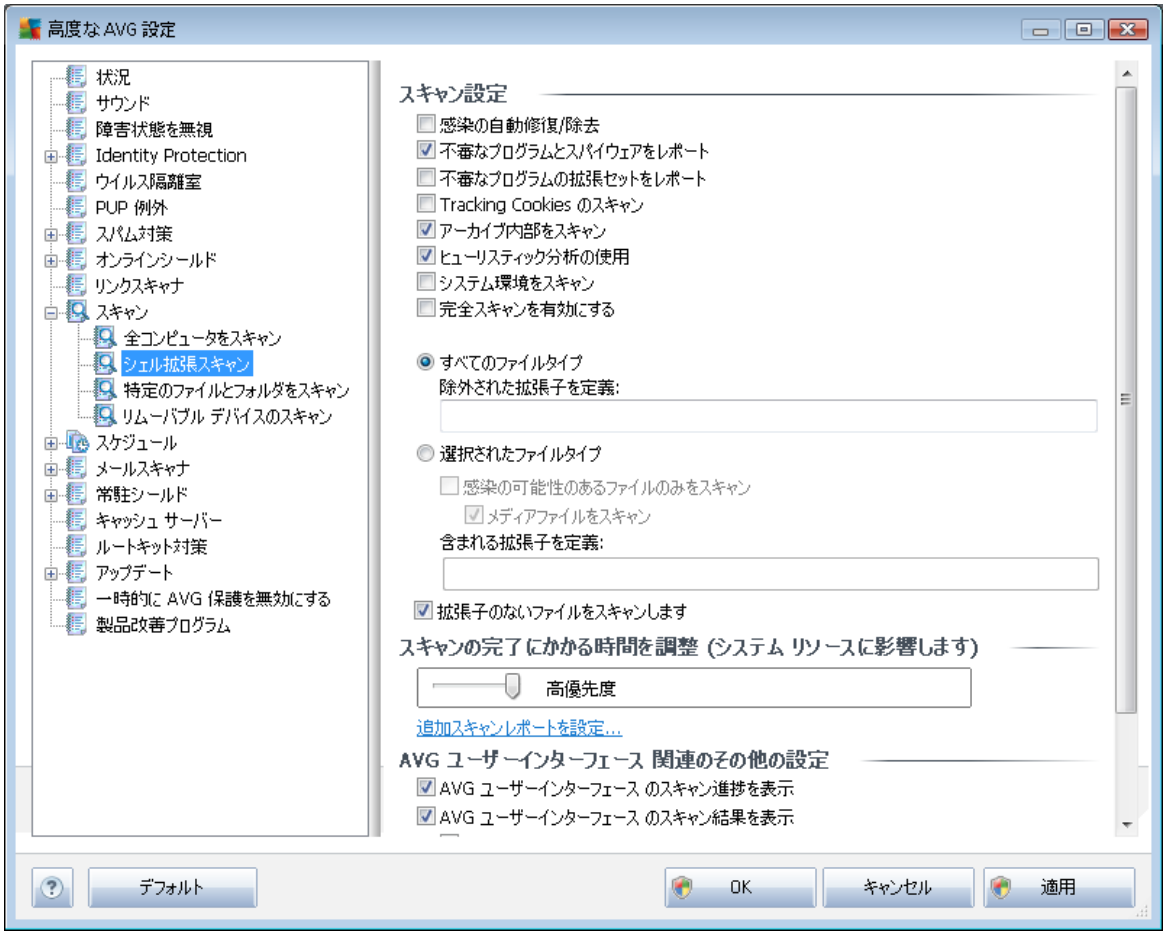
### 追加スキャン レポートを設定...

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




## 9.10.2. シェル拡張スキャン

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




パラメータのリストは***完全コンピュータスキャン***で利用できるものと同一です。ただし、既定の設定が異なります (*たとえば、完全コンピュータ スキャンの場合、既定ではアーカイブをチェックせずにシステム環境をチェックしますが、シェル拡張スキャンでは逆になります*)。

***メモ**: 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 / 完全コンピュータ スキャン**」の章を参照してください。*

[***完全コンピュータ スキャン***]ダイアログと比較すると、[***シェル拡張スキャン***] ダイアログには [***AVG ユーザー インターフェースのその他の設定***] というセクションがあり、スキャンの進行状況を表示するかどうか、AVG ユーザー インターフェースからスキャン結果にアクセスできるようにするかを指定できます。また、スキャンで感染が検出された場合にのみスキャン結果を表示するように定義できます。

### 9.10.3. 特定のファイルやフォルダをスキャン

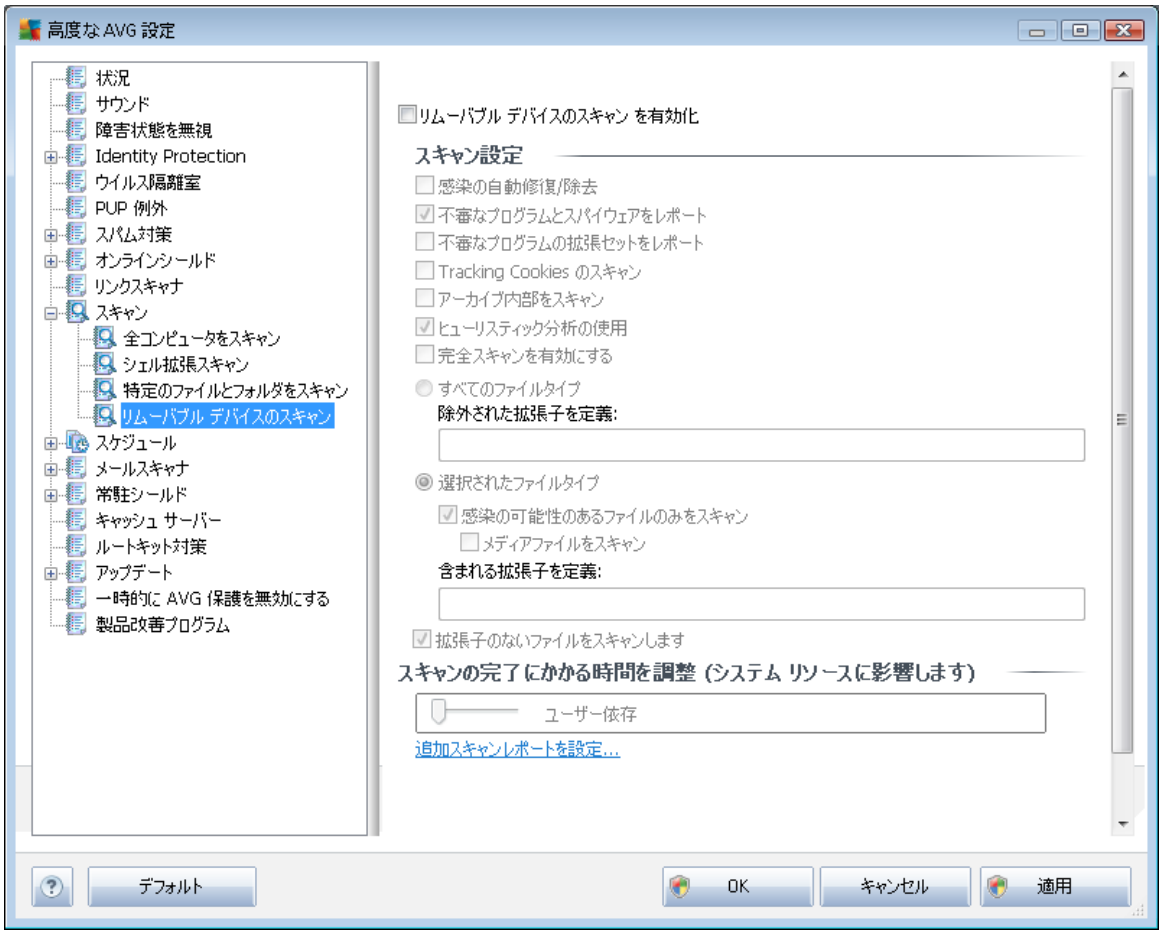
***特定のファイルまたはフォルダをスキャン***の編集インターフェースは***完全コンピュータ スキャン***編集ダイアログと同一です。すべてのコンフィグレーションオプションは同一です。ただし、デフォルト設定は***完全コンピュータスキャン***の場合にはより厳密なものとなっています。


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

***メモ:*** *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 / 完全コンピュータ スキャン**」の章を参照してください。*

### 9.10.4. リムーバブル デバイスのスキャン

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




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

***メモ:*** *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 / 完全コンピュータ スキャン**」の章を参照してください。*

## 9.11. スケジュール

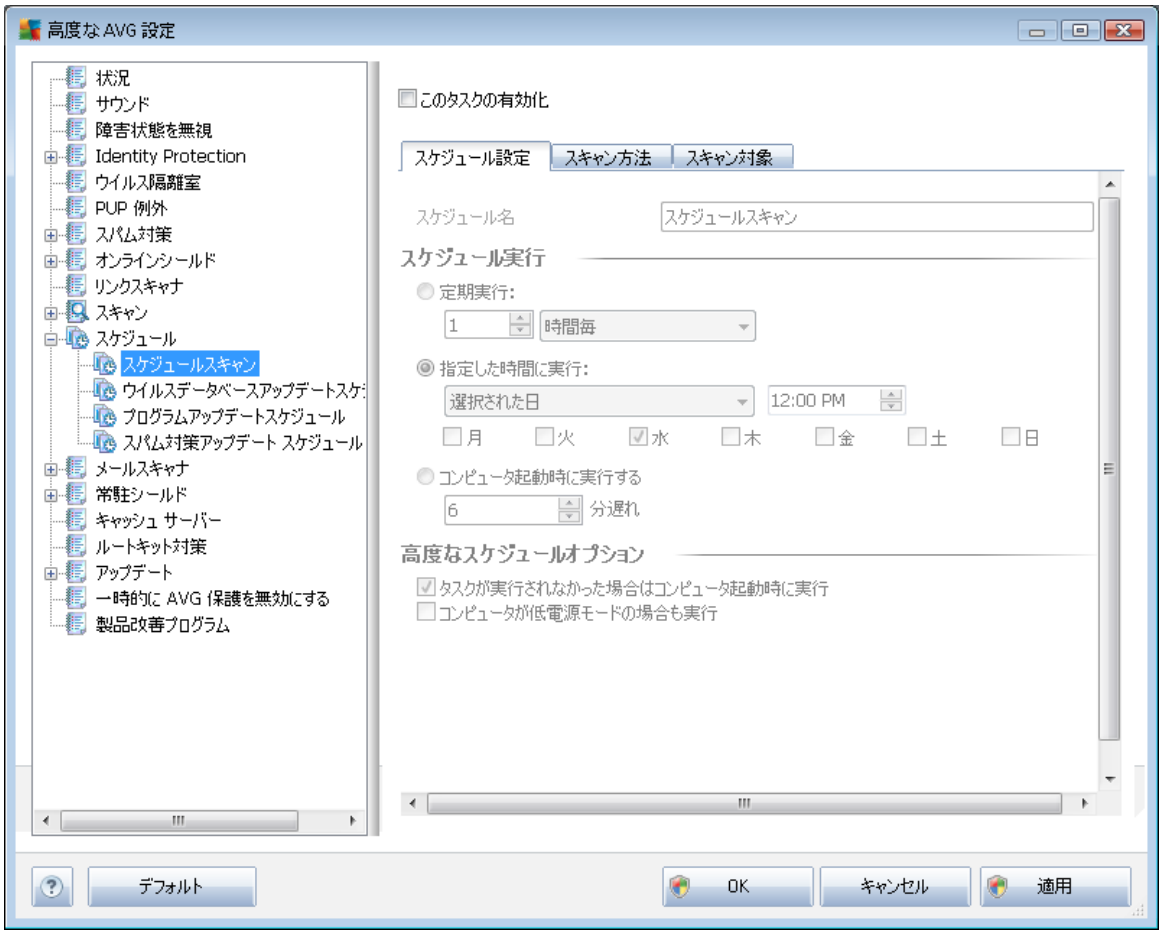
***スケジュール***セクションでは、デフォルト設定を編集することができます。

- スケジュールスキャン

- ウイルスデータベースアップデートスケジュール
- プログラムアップデートスケジュール
- スパム対策アップデートスケジュール

### 9.11.1. スケジュール済スキャン

スケジュールされたスキャン（*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、スケジュールされたスキャンを一時的に有効化/無効化できます。




次に、[***名前***] テキストフィールド（*すべての既定のスケジュールでは無効化*）には、プログラムベンダーによってこのスケジュールに割り当てられた名前があります。新しく追加されたスケジュール（ナビゲーションツリーの [*スキャンのスケジュール*] ***アイテムを右クリックして新しいスケジュールを追加できます***）の場合、*独自の名前を指定できます。その場合は、テキストフィールドが開き、編集できるようになります。*スキャンには、必ず簡潔で、説明的で、適切な名前を使用して、後に他のスキャンと区別できるようにしてください。

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

このダイアログでは、さらに以下のスキャンパラメータを定義します。

## スケジュール実行

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

## 高度なスケジュールオプション

このセクションでは、コンピュータが低電源モードあるいは完全に電源オフになっている場合に、スキャンが実行される条件を定義します。

スケジュール済みのスキャンが指定した時間に起動すると、AVGシステムトレイアイコン上に開かれるポップアップウィンドウで通知されます。


次に、スケジュール 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 (*全色で点滅表示*) 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、実行中のスキャンの一時停止または停止を行えます。また、現在実行中のスキャンの優先度も変更できます。


[***スキャン方法***] タブには、任意でオン/オフを切り替えられるスキャン パラメータの一覧が表示されます。既定ではほとんどのパラメータがオンになっており、その機能はスキャン実行中に適用されます。やむを得ない理由がない場合は、あらかじめ定義された設定を保持することをお勧めします。

- ***自動的に感染を修復/除去する*** *(既定ではオン)*: スキャン実行中にウイルスが特定され、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***ウィルス隔離室***に移動されます。

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

- ***不審なプログラムの拡張セットを報告する*** *(既定ではオフ)*: チェックを付けると、スパイウェアの拡張パッケージを検出します。スパイウェアとは、直接製造元から入手する場合にはまったく問題がなく、無害なプログラムですが、後から悪意のある目的で誤用されるおそれのあるプログラムです。これは、コ

ンピュータ セキュリティをさらに高めるための追加的な手段ですが、合法的なプログラムもブロックする可能性があるため、デフォルトではオフになっています。

- ***Tracking Cookie をスキャンする*** (*既定ではオフ*): ***スパイウェア対策コンポーネントのこのパラメータを定義すると、スキャン実行中に Cookie を検出します (HTTP cookie は、サイトの設定や電子ショッピング カートの内容など、ユーザー固有の情報の認証、追跡、メンテナンスに使用されます***)。
- ***アーカイブの内容をスキャンする*** (*既定ではオフ*): このパラメータを定義すると、ファイルが ZIP や RAR などのアーカイブで保存されている場合でも、すべてのファイルに対してスキャン チェックを実行します。
- ***ヒューリスティック分析を使用する*** (*既定ではオン*): ヒューリスティック分析 (*仮想コンピュータ環境で実行されるスキャン対象オブジェクト命令の動的エミュレーション*) は、スキャン実行中に採用されるウイルス検出方法の 1 つです。
- ***システム環境をスキャンする*** (*既定ではオン*): コンピュータのシステム領域もチェックされます。
- ***完全スキャンを有効にする*** (*既定ではオフ*) - このオプションをチェックすると、特定の状況 (*コンピュータが感染している疑いがある場合など*) が発生した場合に最も完全なスキャン アルゴリズムを有効にし、感染の可能性が非常に低いコンピュータ領域もスキャンします。これにより、問題がないことを確実に確認します。この方法を実行すると多少時間がかかります。
- ***ルートキットをスキャンする*** (*既定ではオフ*): この項目にチェックを付けると、完全コンピュータ スキャン中にルートキットをスキャンします。また、ルートキット スキャンは***ルートキット対策***コンポーネントでも独自に実行できます。

さらに、スキャンするかどうかを決定する必要があります。

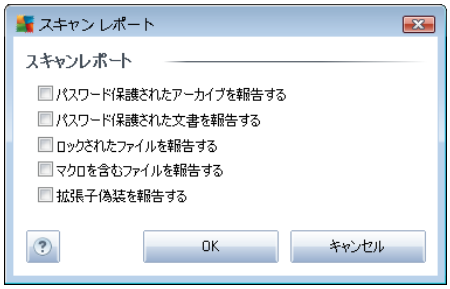
- ***すべてのファイル タイプとスキャン対象ではないファイル拡張子をカンマで区切ったリスト*** (*保存すると、カンマはセミコロンに変わります*) を入力することで、スキャンからの除外を定義できます。
- ***選択したファイル タイプ*** - 感染の可能性のあるファイルのみを指定できます (*一部のプレーン テキスト ファイルやその他の非実行可能ファイル*など感染の可能性がないファイルはスキャンされません)。これには、メディア ファイル (*ビデオ、オーディオ ファイル*) が含まれます。 多くの場合、このようなファイルはサイズが非常に大きく、ウィルスに感染している可能性が非常に低いため、このボックスのチェックを外すと、スキャン時間がさらに短縮されますここでも、必ずスキャンするファイルの拡張子を指定できます。
- 任意で***拡張子のないファイルをスキャン***できます。このオプションは既定ではオンになっています。変更する理由がない場合は、この設定を保持することをお勧めします。拡張子のないファイルは不審であるため、常にスキャンすることをお勧めします。

## スキャン速度を調整

[***スキャン速度を調整***] セクションでは、システム リソース使用度に応じて、任意のスキャン速度を指定できます。*既定ではこのオプションの値は、自動的にリソースを使用する*ユーザー依存レベルに設定されています。スキャンを高速化すると、スキャン時間を短縮できますが、スキャン実行中にシステム リソース消費量が著しく上がり、PC で実行されている他の作業の速度が低下します (*このオプションは、コンピュータの電源がオンであり、コンピュータ上で作業をしているユーザーがいない場合などに適しています*)。一方、スキャンの時間を延長することで、システム リソース消費量を下げることができます。

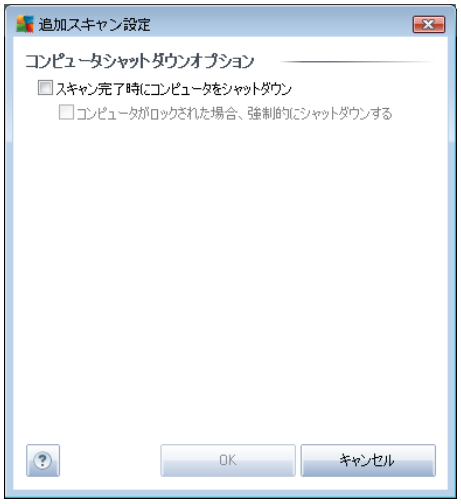
## 追加スキャン レポートを設定

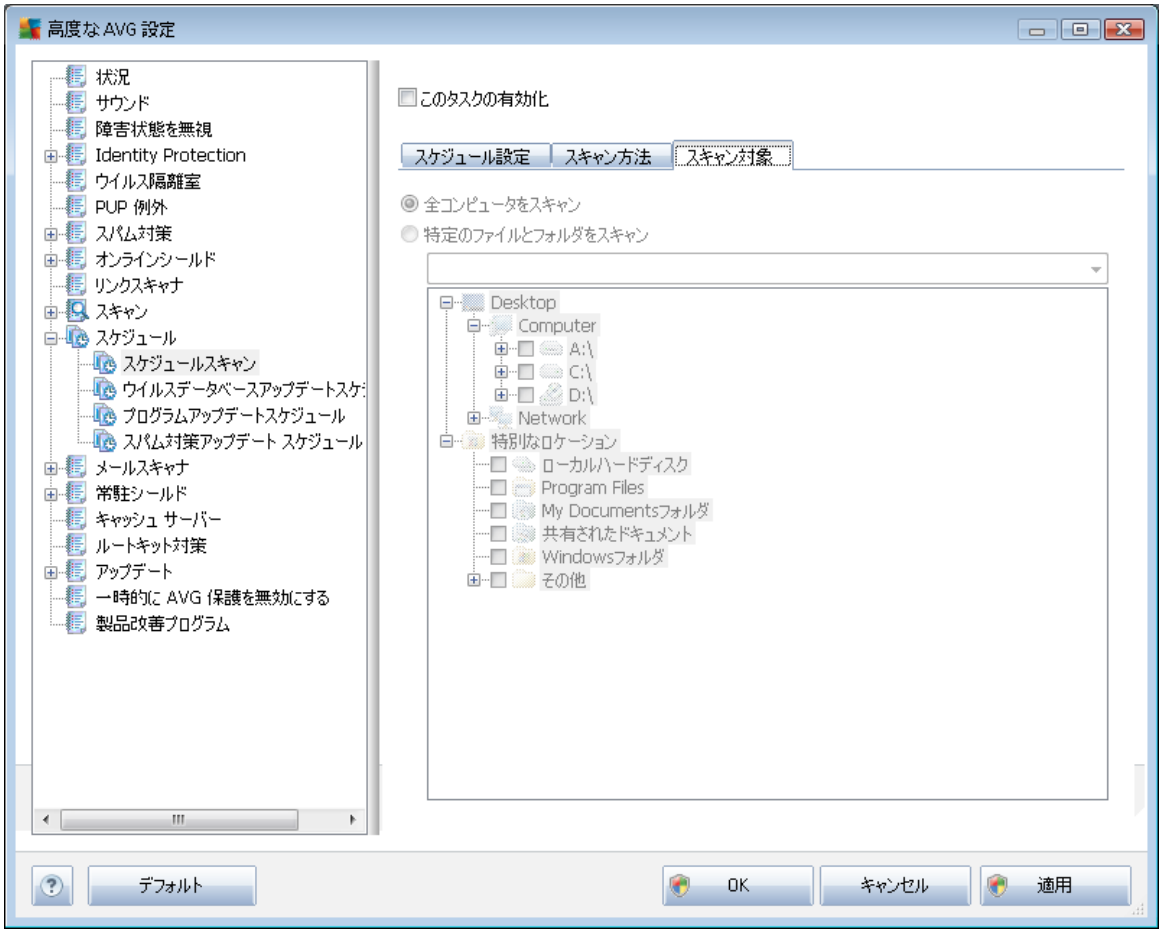
[***追加スキャン レポート...***] リンクをクリックすると、[***スキャン レポート***] ダイアログが開きます。このウィンドウでは報告する検出項目を定義します。




## 追加スキャン設定

[***追加スキャン設定...***] をクリックすると、新しい***コンピュータ シャットダウン オプション*** ダイアログが表示されます。このダイアログではスキャン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。



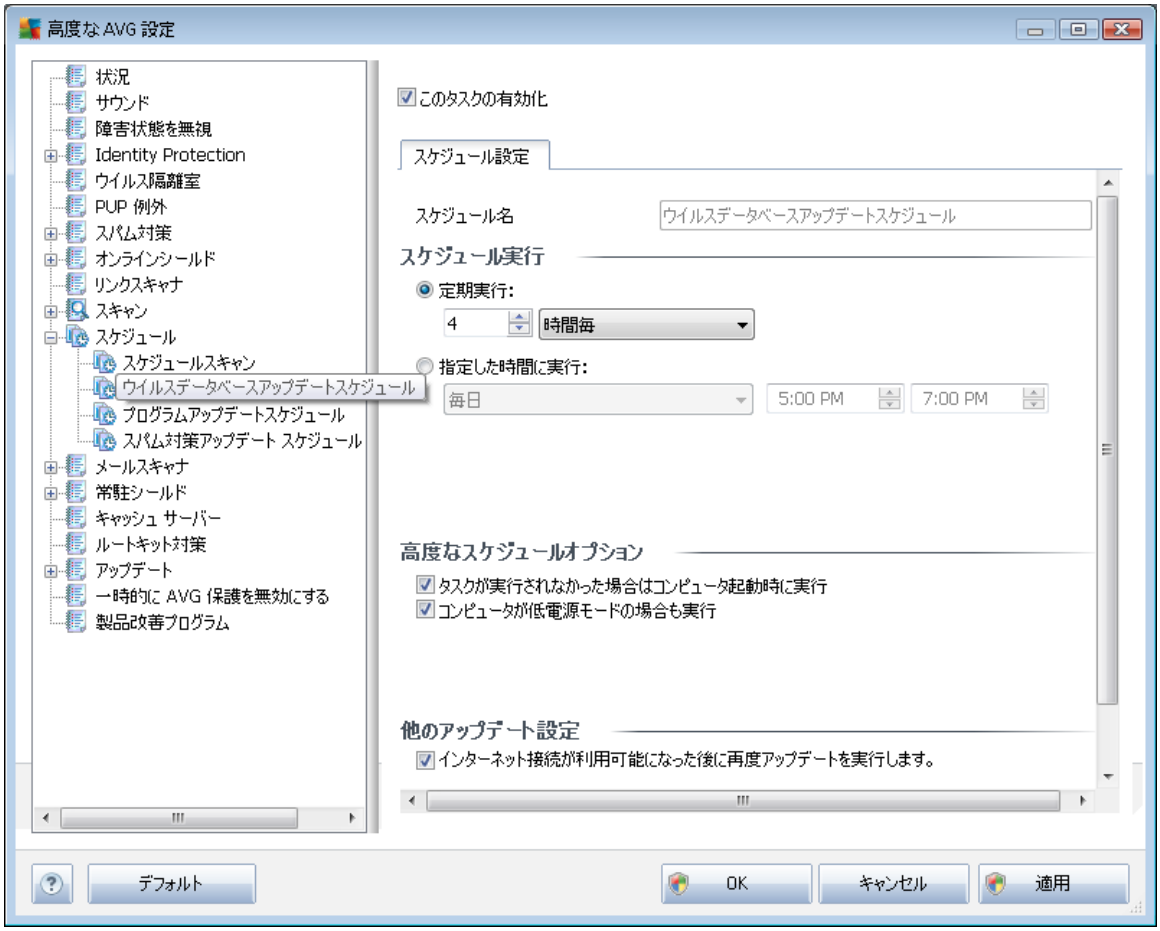




[***スキャン対象***] タブでは、全コンピュータをスキャン、あるいは特定のファイルやフォルダをスキャンのいずれかを選択します。特定のファイルやフォルダスキャン を選択した場合、ダイアログ下部のツリービューで対象フォルダを指定することができ

ます。

### 9.11.2. ウイルス データベース 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ウィルス データベース更新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。




基本的なウイルス データベース更新スケジュールは***更新マネージャ***コンポーネントに含まれます。このダイアログでは、一部の詳細なウイルスデータベースアップデートスケジュールのパラメータを設定します。[***名前***] テキストフィールド（*すべての既定のスケジュールでは無効化*）には、プログラムベンダーによってこのスケジュールに割り当てられた名前があります。

#### スケジュール実行

このセクションでは、新しくスケジュールされたウィルスデータベースを起動する時間間隔を指定します。タイミングは、特定の期間の後に繰り返し起動するアップデート (***...ごとに実行***) または正確な日時 (***特定の時刻に実行...***) を指定することで、定義できます。

### 高度なスケジュールオプション

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

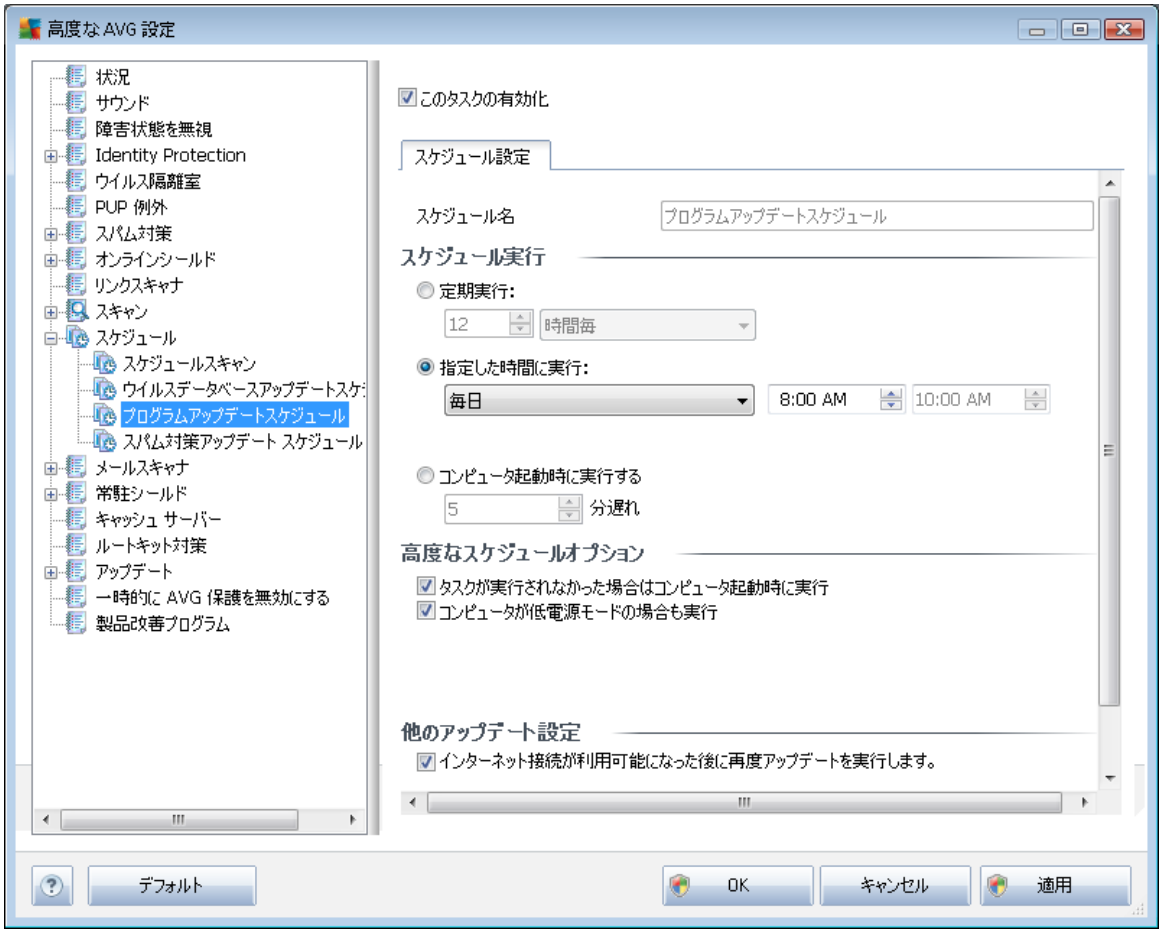
### 他のアップデート設定

最後に、[***インターネット接続が利用できるようになった時点ですぐにアップデートを再実行する***] オプションにチェックをすると、インターネット接続に障害が発生し、アップデート処理が失敗した場合、インターネット接続が復旧した時点で必ずすぐにアップデートを再開するようにできます。

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

## 9.11.3. プログラム アップデート スケジュール

***やむを得ない理由がある場合***、[***このタスクを有効にする***] 項目のチェックを外してスケジュールされたプログラム更新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。




[***名前***] テキスト フィールド（*すべての既定のスケジュールでは無効化*）には、プログラム ベンダーによってこのスケジュールに割り当てられた名前があります。

## スケジュール実行

ここでは、プログラムアップデート実行時間を指定します。タイミングは、***定期実行***、***指定した時間に実行***、***アクションにより実行***のいずれかによって定義することができます。

## 高度なスケジュールオプション

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

## 他のアップデート設定

[***インターネット接続が利用できるようになった時点ですぐにアップデートを再実***

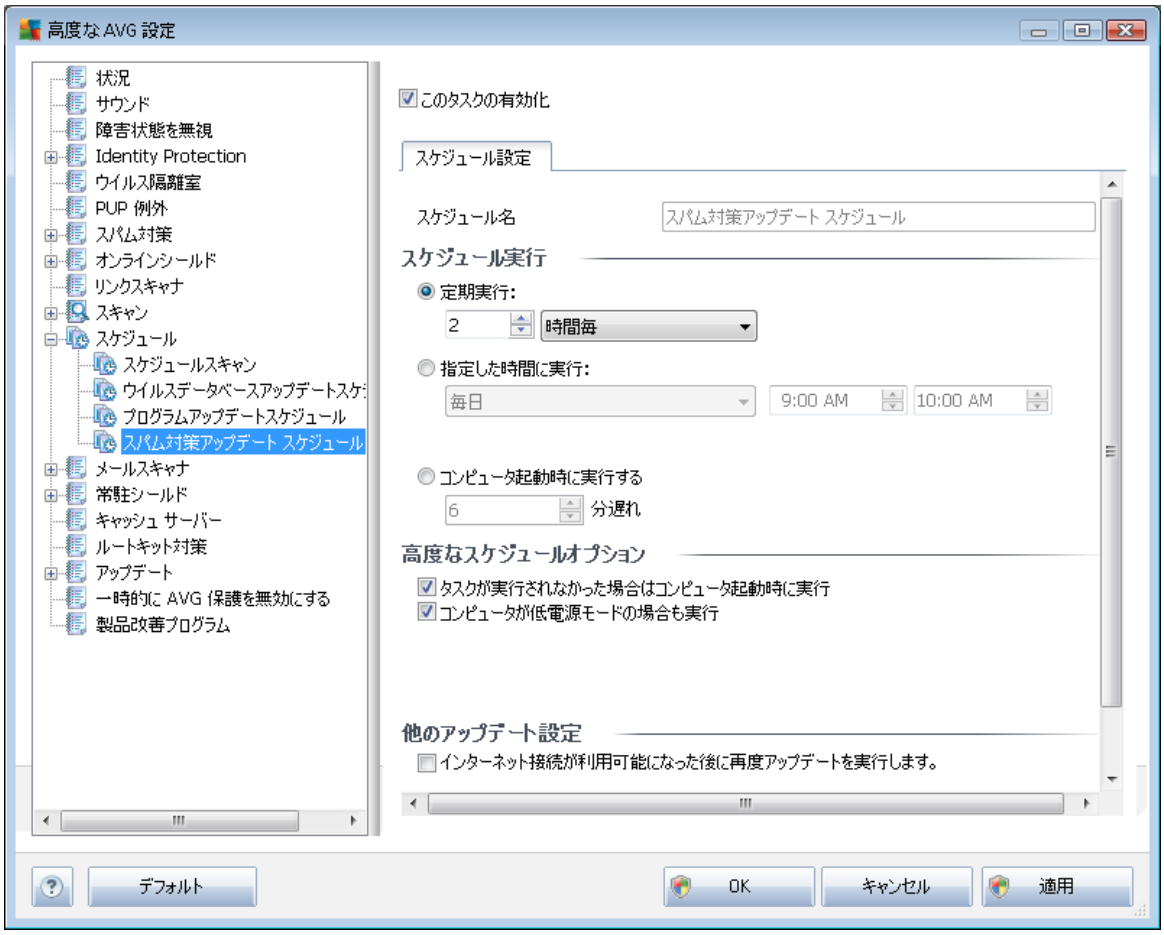
***行する***] オプションにチェックをすると、インターネット接続に障害が発生し、アップデート処理が失敗した場合、インターネット接続が復旧した時点で必ずすぐにアップデートを再開するようにできます。

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

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

### 9.11.4. スパム対策アップデート スケジュール

***やむを得ない理由がある場合***、[***このタスクを有効にする***] 項目のチェックを外してスケジュールされた***スパム対策***更新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。




基本***スパム対策***更新スケジュールは***更新マネージャ***コンポーネントに含まれます。このダイアログでは、一部の詳細なアップデートスケジュールのパラメータを設定します。[***名前***] テキストフィールド（*すべての既定のスケジュールでは無効化*）には、プログラムベンダーによってこのスケジュールに割り当てられた名前があります。

## スケジュール実行

ここでは、新しくスケジュールされた***スパム対策***アップデート起動までの時間を指定します。タイミングは、ある期間の後に（***...ごとに実行***）の繰り返される***スパム対策***更新起動を定義することによって、あるいは正確な日時（***特定の時間...に実行***）を定義することによって、あるいは、アップデート起動が関連付けられるイベント（***コンピュータ起動に基づくアクション***）を定義することによっても可能です。

## 高度なスケジュールオプション

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

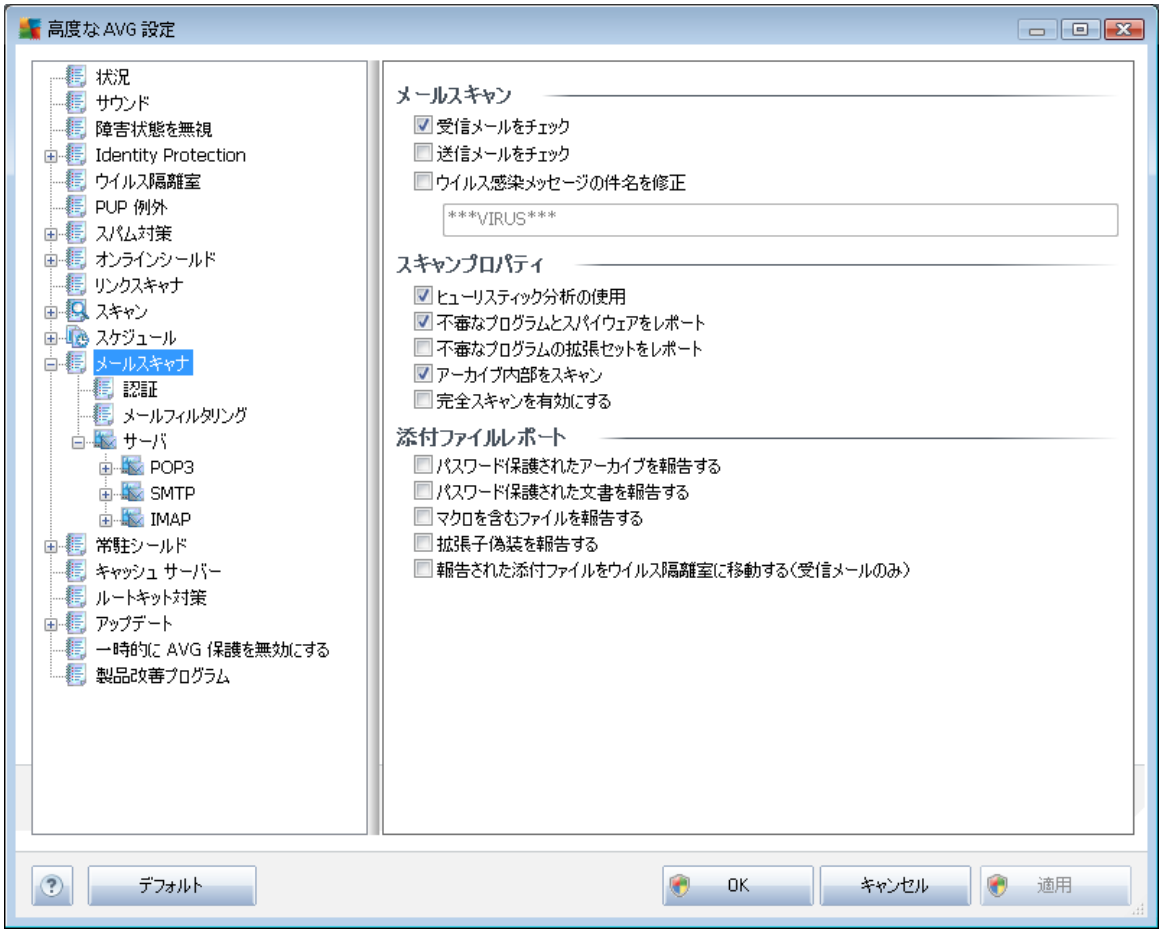
## 他のアップデート設定

[***インターネット接続が利用できるようになった時点ですぐにアップデートを再実行する***] オプションにチェックをすると、インターネット接続に障害が発生し、***スパム対策***アップデート処理が失敗した場合、インターネット接続が復旧した時点で必ずすぐにアップデートを再開するようにできます。

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

## 9.12. メール スキャナ

***メールスキャナ***ダイアログは3つのセクションに分けられます。




### メール スキャン

このセクションでは、送受信メールに関する基本項目を設定できます。

- ***受信電子メールをチェックする*** (*既定ではオン*) - このボックスを選択/クリアすることで、電子メール クライアントに配信されるすべての電子メール メッセージをスキャンするかどうかを選択します。
- ***送信電子メールをチェックする*** (*既定ではオフ*) - このボックスを選択/クリアすることで、自分のアカウントから送信されるすべての電子メール メッセージをスキャンするかどうかを選択します。
- ***ウィルス感染したメッセージの件名を修正する*** (*既定ではオフ*) - スキャンによって感染メッセージとして検出された電子メール メッセージに関する警告を表示する場合は、この項目にチェックを付け、テキスト フィールドに任意のテキストを入力します。このテキストがすべての感染電子メールの [件名] フィールドに追加されるため、感染メッセージを簡単に識別し除外できます。初期値

は***VIRUS*** です。この値の使用をお勧めします。

## スキャン プロパティ

このセクションでは、電子メール メッセージのスキャン方法を指定できます。

- ***ヒューリスティック分析を使用する*** (*既定ではオン*) - チェックを付けると、電子メール メッセージをスキャンするときにヒューリスティックス検出方式使用します。このオプションをオンにすると、拡張子だけでなく実際の添付ファイルの内容も考慮して、電子メールのメール添付ファイルをフィルタできます。フィルタリングは [***メール フィルタリング***] ダイアログで設定できます。

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

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

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

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

## 添付ファイル レポート

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

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

- ***パスワードによって保護された文書を報告する*** – パスワードによって保護

された文書のウイルス スキャンはできません。ボックスにチェックを付けると、潜在的に危険なオブジェクトとしてこのようなドキュメントを報告します。

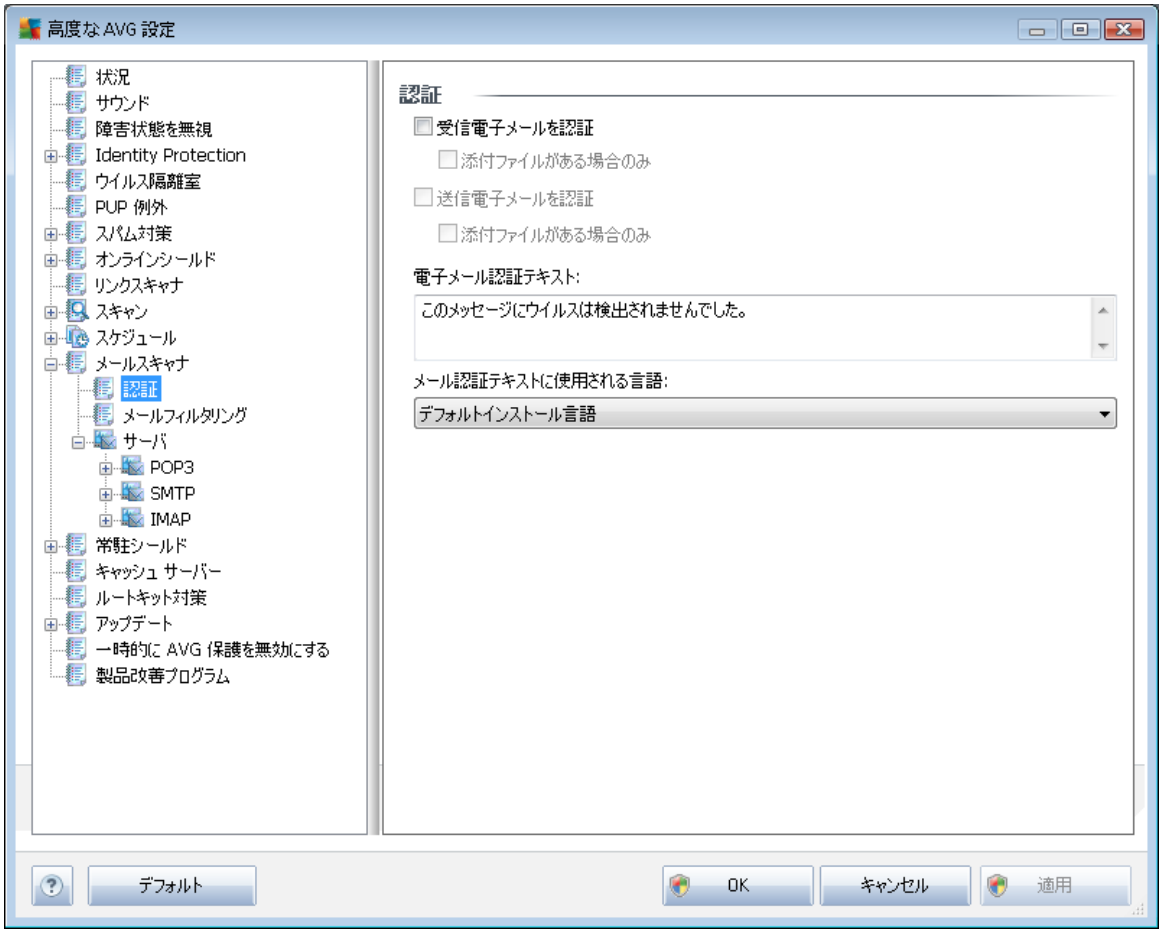
- ***マクロを含むファイルを報告する*** – マクロはあるタスクを簡単に実行するためのあらかじめ定義された一連の命令です (*MS Wordのマクロが広く知られています*)。マクロには潜在的に危険な命令が含まれる可能性があります。ボックスにチェックを付けると、マクロを含むファイルを不審なファイルとして報告します。

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

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

### 9.12.1. 認証

[***認証***] ダイアログでは、送受信メールの認証用テキストと言語を指定できます。




認証テキストには、ユーザー定義部分とシステム部分の 2 つの部分があります。次の例では、最初の行がユーザー定義テキストで、残りの部分は自動的に作成されています。

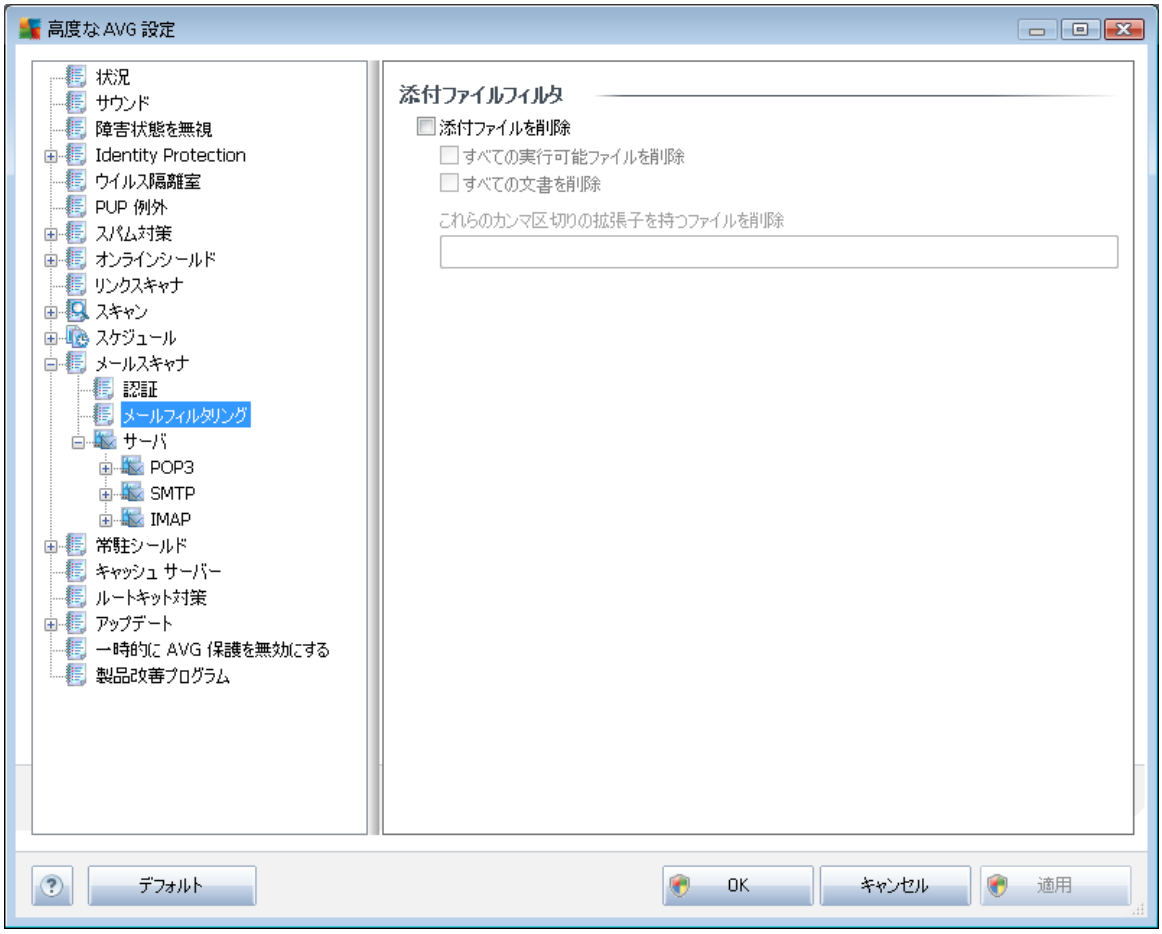
*No virus found in this message.*

*Checked by AVG.*

*Version: x.y.zz / Virus Database: xx.y.z - Release Date: 12/9/2010*

送受信電子メール メッセージに認証を適用する場合は、このダイアログで認証テキストのユーザー定義部分のテキスト (***電子メール認証テキスト***) を正確に指定し、認証テキストのうちシステムで自動生成するテキストの言語 (***電子メール認証テキストの言語***) を選択できます。

### 9.12.2. メール フィルタリング

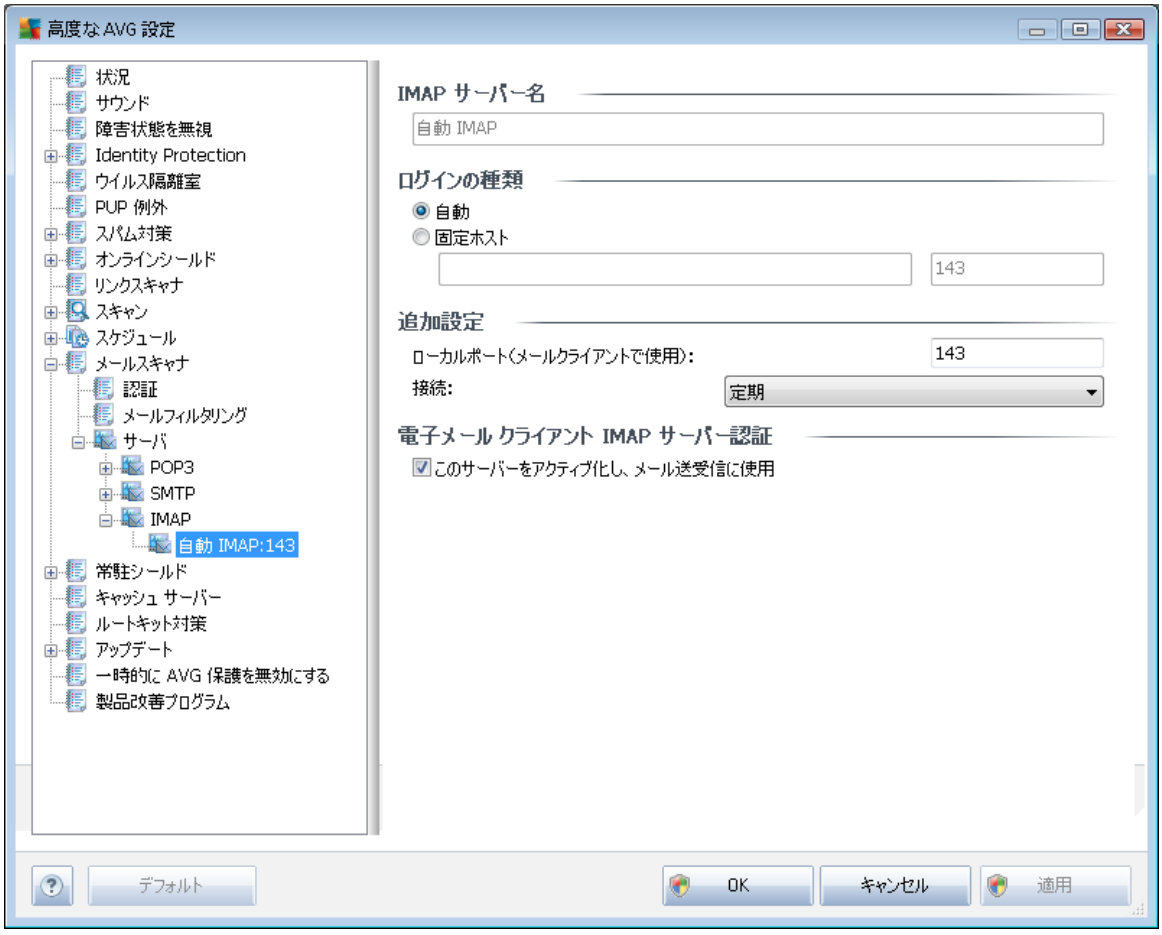



***添付ファイルフィルタ***ダイアログでは、メール添付ファイルのスキャンパラメータを設定できます。デフォルトでは、***添付ファイルを削除***オプションはオフとなっています。有効化した場合、感染、または潜在的に危険だと検出されたすべての添付ファイルは自動的に削除されます。削除する添付ファイルのタイプを定義したい場合、各オプションを選択します。

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

### 9.12.3. サーバー

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

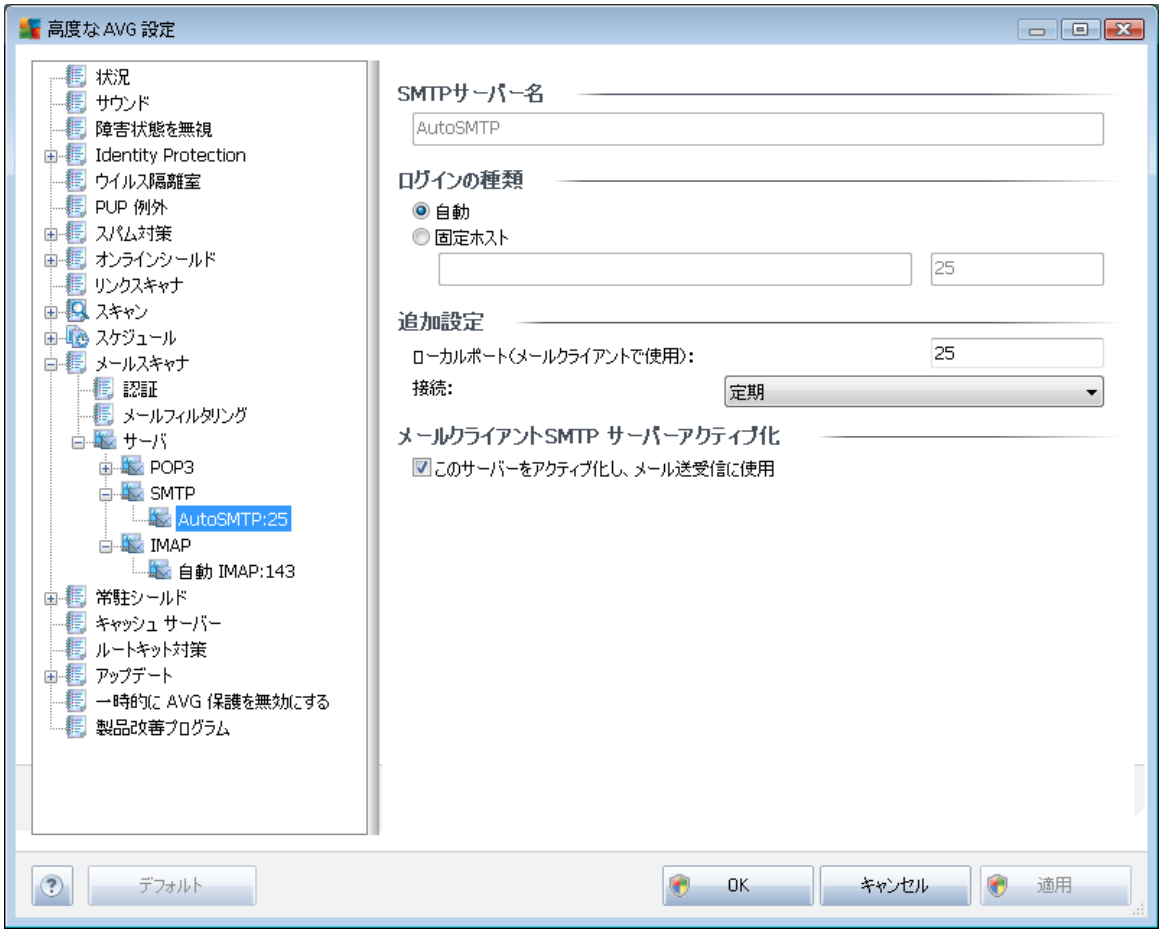



[*サーバー/POP3*] をクリックすると、このダイアログが開きます。受信メール用の POP3 プロトコルを使用して、新規の ***メール スキャナ*** サーバーを設定できます。

- ***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*)。自動的に作成された「AutoPOP3」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***- 受信メールに使用されるメールサーバー決定方法を定義します。
  - ***自動*** - メールクライアントの設定にしたがって、自動的ログインが実行されます。
  - ***固定ホスト*** - プログラムは常にここで指定されたサーバーを使用します。メール サーバーのアドレスと名前を指定してください。ログイン名は変更されません。名前については、IP アドレス (*123.45.67.89 など*) とドメイン名 (*pop.acme.com など*) を使用できます。メール サーバーが標準以外のポートを使用する場合、このポートをコロンで区切り、サーバー名の後に指定できます (*smtp.acme.com:8200 など*)。POP3 通信の標準ポート

は 110 です。

- ***追加設定*** - より詳細なパラメータを設定します。
  - ***ローカルポート*** - メールアプリケーションからの通信用ポートを指定します。メールアプリケーション上で、このポートをPOP3通信のポートとして指定する必要があります。
  - ***接続*** - *このドロップダウン メニューでは、使用する接続の種類* (通常/SSL/SSL 既定) を指定できます。SSL 接続を選択した場合、送信データは第三者に追跡、監視されるリスクを負うことなく暗号化されます。この機能は送信先のメール サーバーが対応している場合にのみ使用可能です。
- ***メールクライアント POP3 サーバー有効化*** - このアイテムをチェック/チェック解除すると、指定された POP3 サーバーを有効化/無効化します。




***[サーバー/SMTP] をクリックすると、このダイアログが開きます。送信メール用の SMTP プロトコルを使用して、新規の***メール スキャナ ***[サーバーを設定できます。](#)***

- ***SMTP サーバー名*** - このフィールドでは新しく追加したサーバー名を指定できます (*SMTP サーバーを追加するには、左側のナビゲーション メニューで SMTP 項目右クリックします*)。自動的に作成された「AutoSMTP」サーバーの場合は、このフィールドは無効になっています。

- ***ログイン タイプ*** - メール送信で使用するメール サーバーを決定する方法を定義します。

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

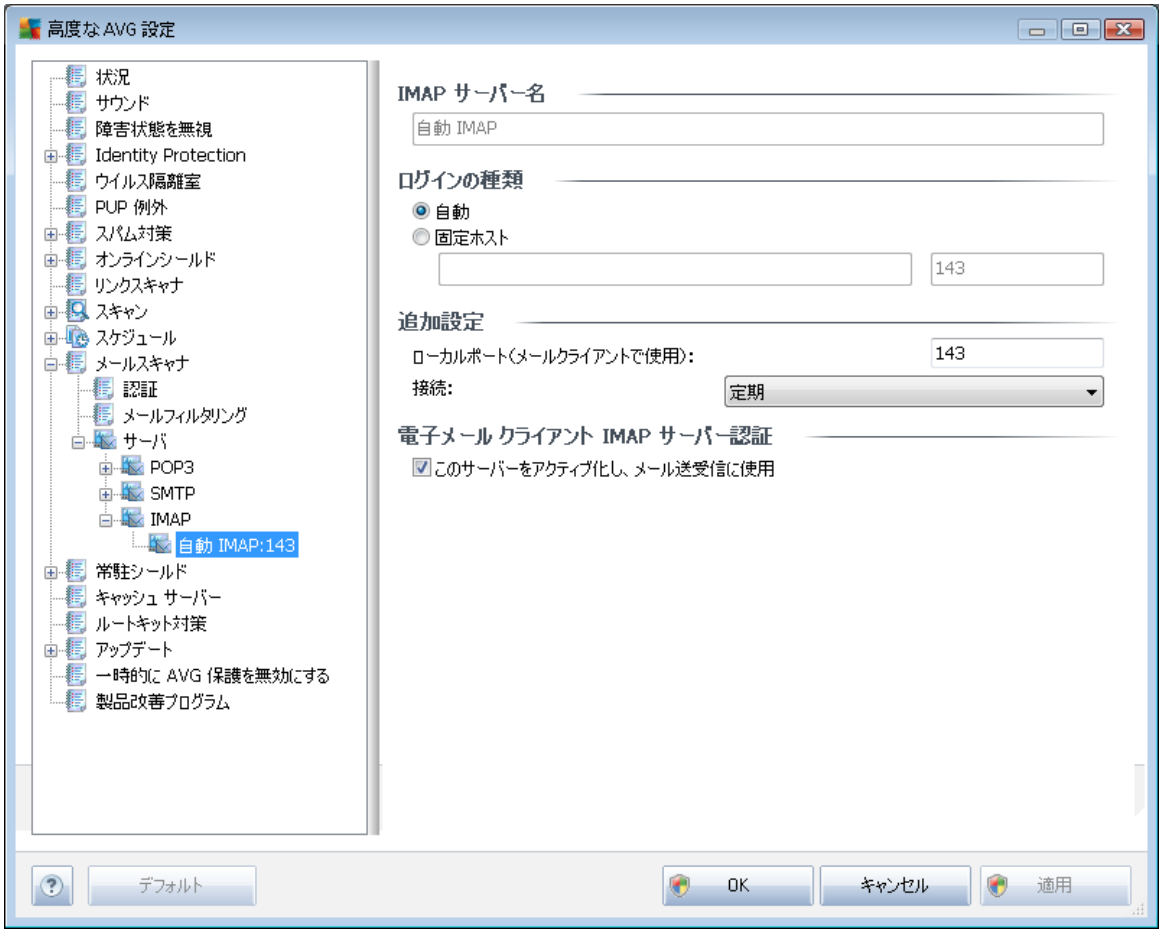
    - ***固定ホスト*** - プログラムは常にここで指定されたサーバーを使用します。メール サーバーのアドレスと名前を指定してください。名前については、ドメイン名 (*smtp.acme.com* など) および IP アドレス (*123.45.67.89* など) を使用できます。メール サーバーが標準以外のポートを使用する場合、このポートをコロンで区切り、サーバー名の後に記述することができます（*たとえば、smtp.acme.com:8200*）。SMTP 通信の標準ポートは 25 です。

- ***追加設定*** - より詳細なパラメータを設定します。

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

    - ***接続*** - このドロップダウン メニューでは、使用する接続の種類 (*通常/SSL/SSL 既定*) を指定できます。SSL接続を選択した場合、送信データは第三者に追跡、監視されるリスクを負うことなく暗号化されます。この機能は送信先のメール サーバーがそれに対応している場合のみ使用可能です。

- ***電子メール クライアント SMTP サーバー有効化*** - このボックスのオン/オフを切り替えると、指定した SMTP サーバーの有効化と無効化を切り替えます。



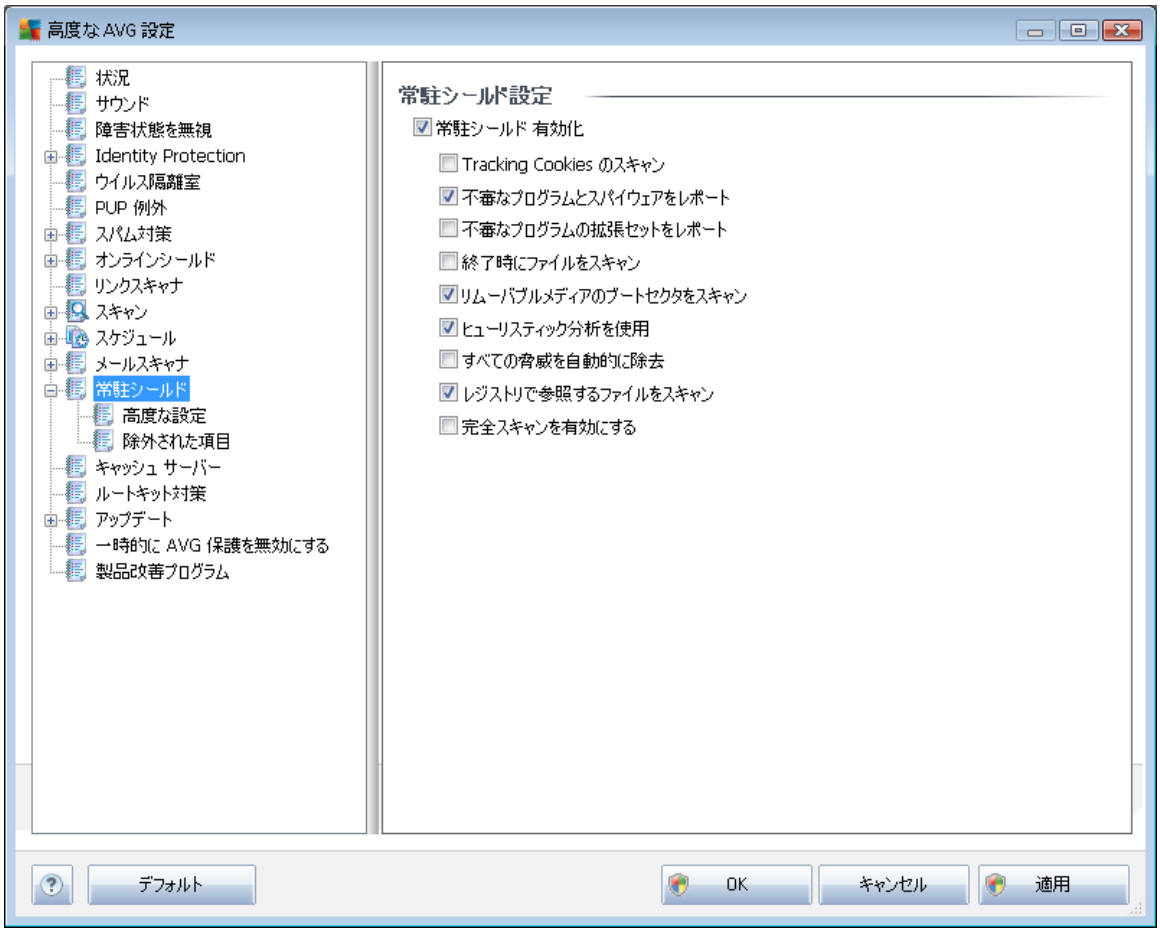

[***サーバー/IMAP***] をクリックすると、このダイアログが開きます。送信メール用の IMAP プロトコルを使用して、新規の ***メール スキャナ*** サーバーを設定できます。

- ***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*)。自動的に作成された「AutoIMAP」サーバーの場合は、このフィールドは無効になっています。
- ***ログイン タイプ*** - メール送信で使用するメール サーバーを決定する方法を定義します。
  - ***自動*** - メールクライアントの設定にしたがって、自動的ログインが実行されます。
  - ***固定ホスト*** - プログラムは常にここで指定されたサーバーを使用します。メール サーバーのアドレスと名前を指定してください。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 既定*) を指定できます。SSL接続を選択した場合、送信データは第三者に追跡、監視されるリスクを負うことなく暗号化されます。この機能は送信先のメール サーバーがそれに対応している場合のみ使用可能です。
- ***電子メール クライアント IMAP サーバーを有効にする*** - このボックスを選択/クリアすると、指定した IMAP サーバーを有効/無効にします。

## 9.13. 常駐シールド

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




[***常駐シールド設定***] ダイアログでは、[***常駐シールドを有効化***] 項目 (***このオプションは既定ではオンです***) をオン/オフにして、*常駐シールド*保護を完全に有効化または

無効化できます。また、どの***常駐シールド***機能を有効化するかを選択します。

- ***Tracking Cookie をスキャンする*** (*既定ではオフ*) - このパラメータを指定すると、スキャン中に Cookies が検出されます。（*HTTP cookies は、認証、トラッキング、サイトのプリファレンスや電子ショッピングカードの内容等の特定のユーザー情報の保持に使用されます*

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

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

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

- ***リムーバブル メディアのブート セクターをスキャンする*** - (*既定ではオン*)

- ***ヒューリスティック分析を使用する*** - (*既定ではオン*) ヒューリスティック分析 (*仮想コンピュータ環境でのスキャン オブジェクトの動的エミュレーション*) を使用して検出します。

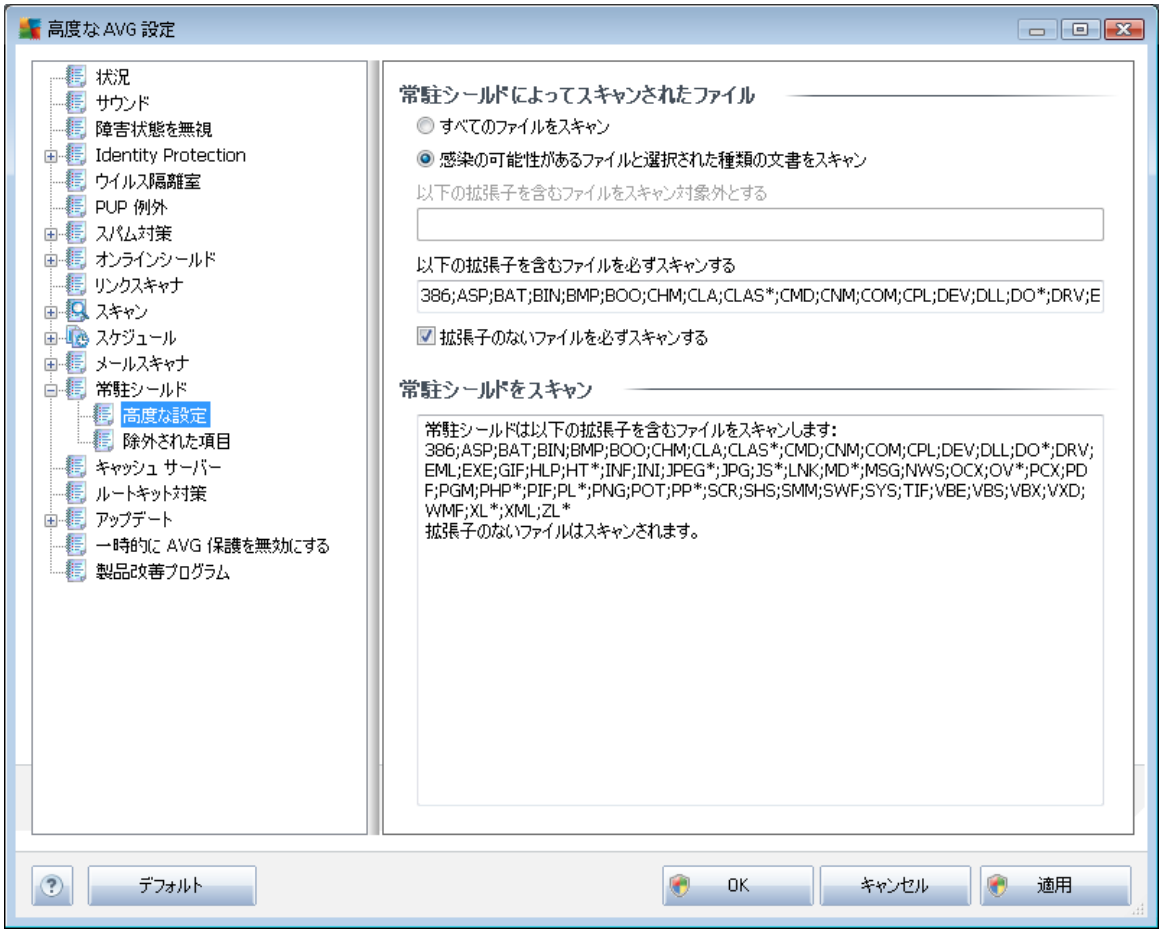
- ***すべての脅威を自動的に駆除する*** (*既定ではオフ*) - 修復が可能な場合は、検出されたファイルはすべて自動的に修復されます。修復できない感染はすべて駆除されます。

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

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

### 9.13.1. 高度な設定

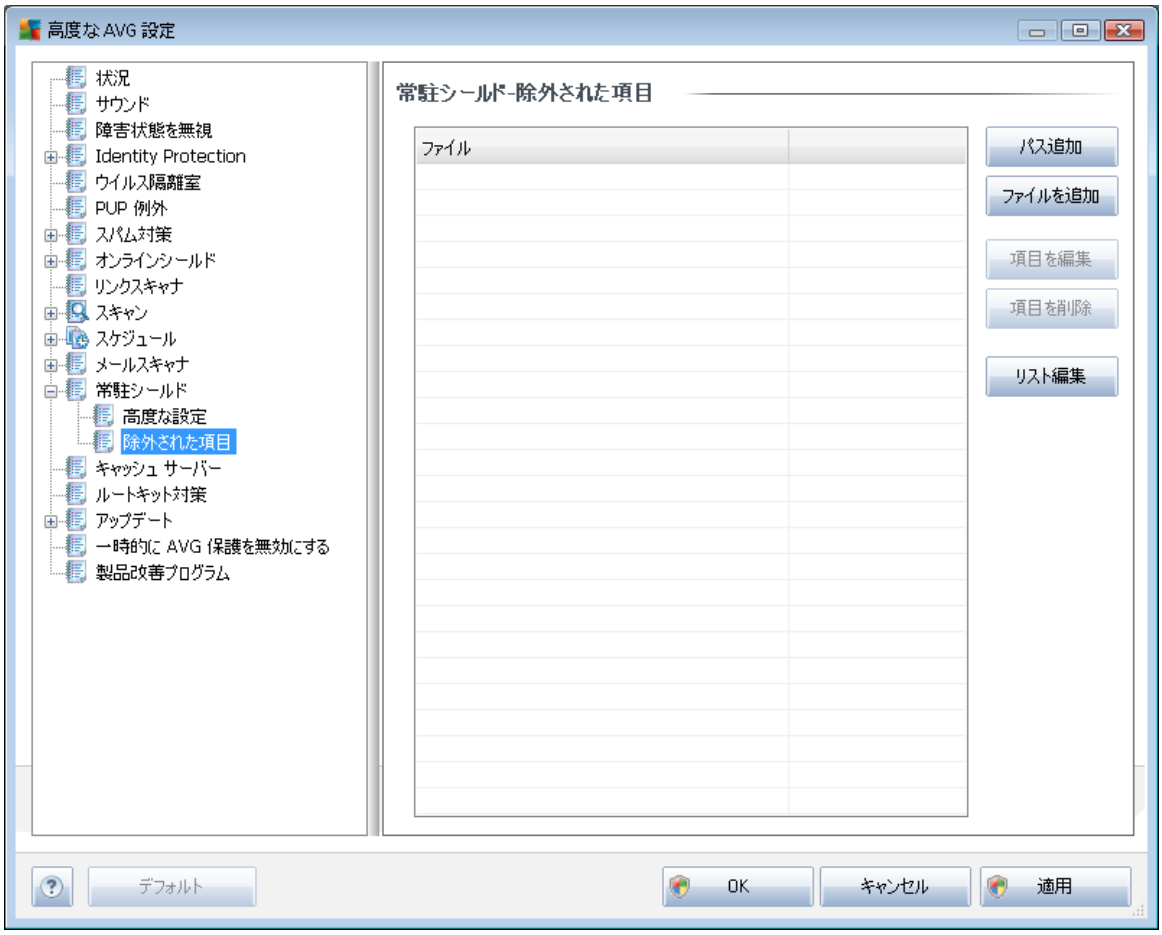
[***常駐シールドによってスキャンされたファイル***] ダイアログでは、スキャン対象のファイルを*特定の拡張子を指定して*設定できます。




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

下の [***常駐シールドがスキャンするアイテム***] セクションには現在の設定がまとめて表示されます。

### 9.13.2. 除外された項目




[***常駐シールド - 例外項目***] ダイアログでは、***常駐シールド***スキャンから除外されるフォルダを定義できます。

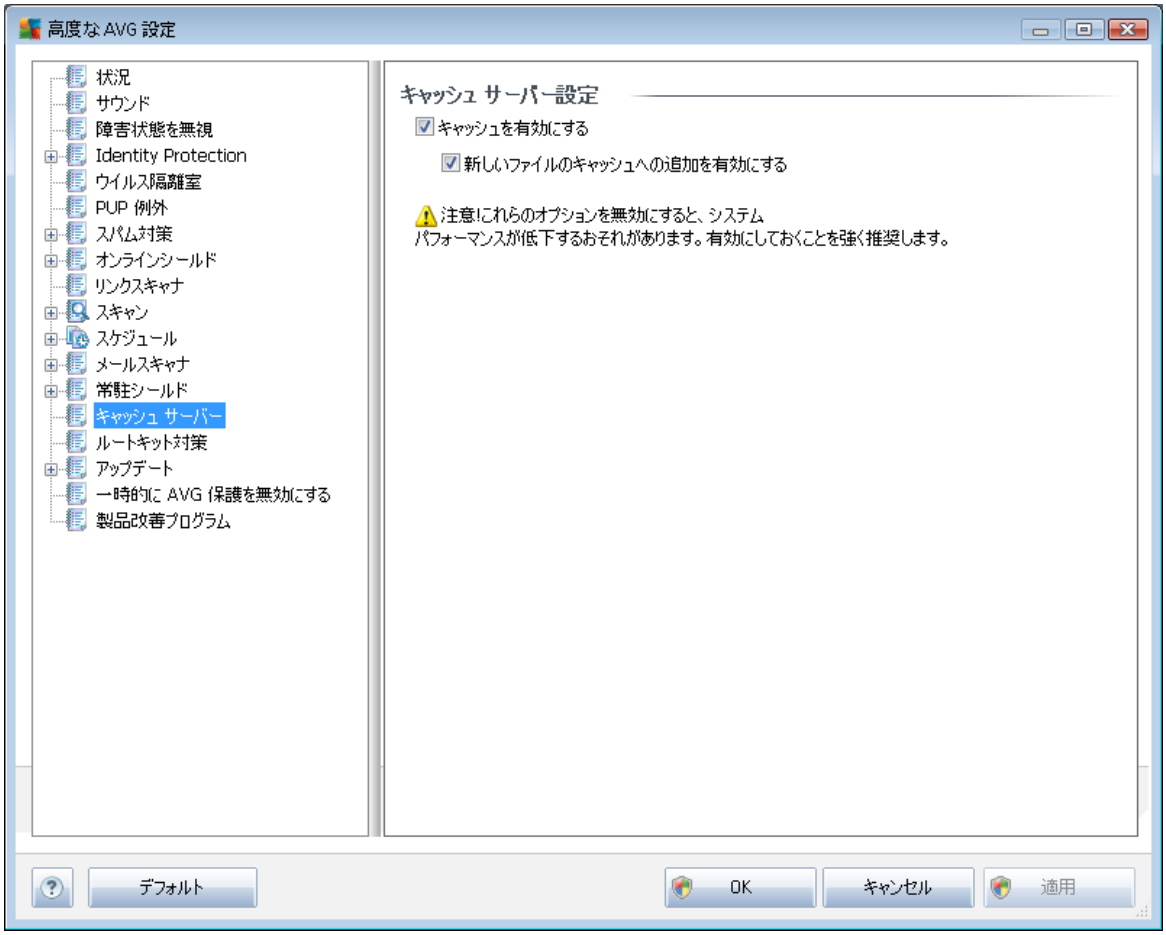
***必要な場合を除き、すべての項目を含めることを強くお勧めします。***

ダイアログには次のコントロール ボタンがあります。

- ***パスの追加*** – ローカル ディスクのナビゲーション ツリーからディレクトリを 1 つずつ選択してスキャン対象から除外するディレクトリを指定します。
- ***ファイルの追加*** –ローカル ディスク ナビゲーション ツリーからファイルを 1 つずつ選択してスキャン対象から除外するファイルを指定します。
- ***項目の編集*** –選択したファイルまたはフォルダへの特定のパスを編集できます。
- ***項目の削除***–選択した項目へのパスをリストから削除できます

## 9.14. キャッシュ サーバー

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



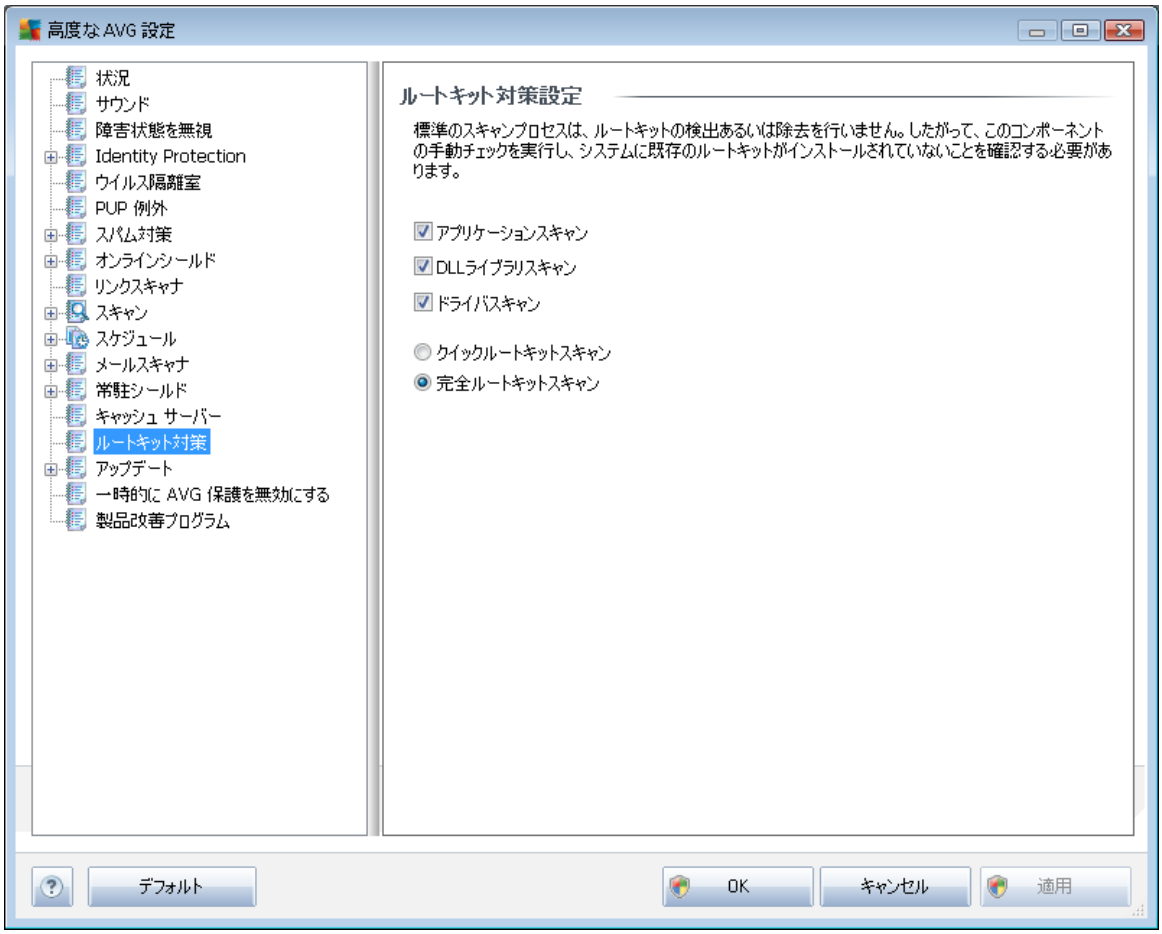

設定ダイアログには 2 つのオプションがあります。

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

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

## 9.15. ルートキット対策

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




このダイアログ内で提供されている***ルートキット***コンポーネントのすべての機能に対する編集は、***ルートキット対策コンポーネントのインターフェース***から直接行うこともできます。

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

- ***アプリケーション スキャン***
- ***DLL ライブラリ スキャン***
- ***ドライバ スキャン***

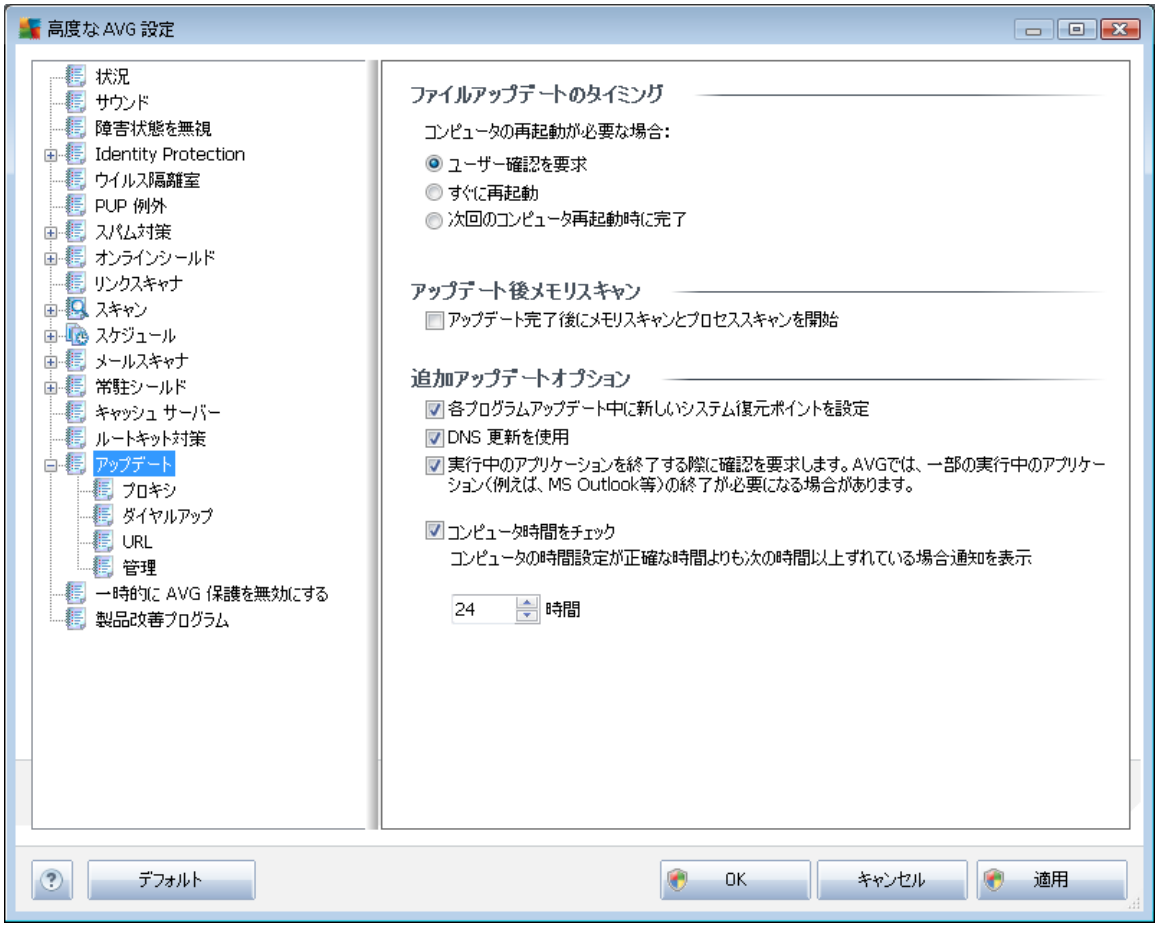
さらに、ルートキット スキャン モードを選択できます。

- ***クイック ルートキット スキャン*** - すべての実行中のプロセス、ロードされた

ドライバ、およびシステム フォルダ (*通常は、c:\Windows*) をスキャンします。

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

## 9.16. 更新




***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、更新処理によって 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 の再起動時に更新を完了するようにスケジュール設定するか、ただちに再起動できます。

- ***ユーザーの確認を要求***（*既定*）- 更新処理

- ***すぐに再起動*** - コンピュータはアップデートプロセスが完了した時点で、自動的に即時再起動されます。

- ***次回のコンピュータの再起動時に完了*** - 更新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。

## アップデート後メモリスキャン

このチェックボックスをオンにすると、各アップデートが正常に完了した後に、新しいメモリスキャンを起動するように定義します。ダウンロードした最新のアップデートには新しいウィルス定義が含まれている場合がありますが、即時スキャンに適用されます。

## 追加アップデートオプション

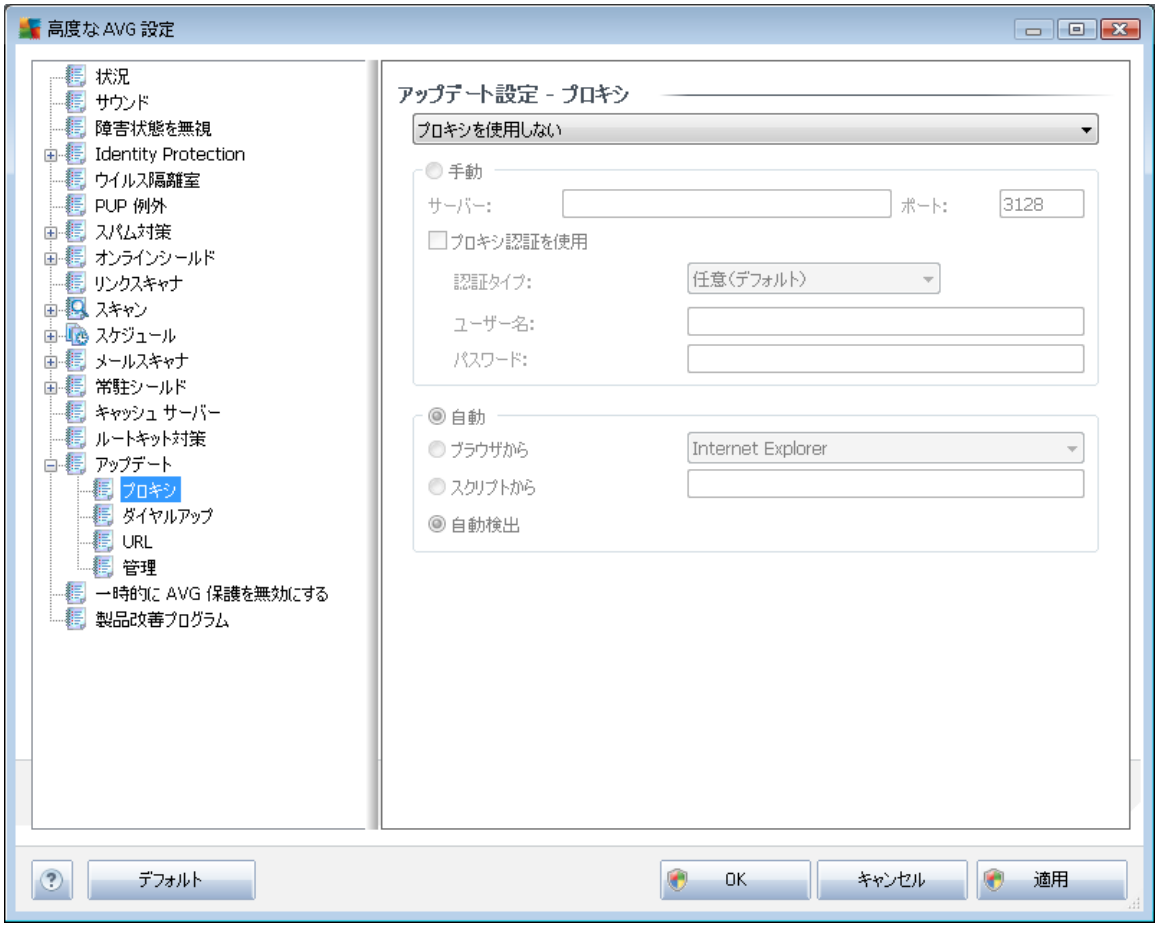
- ***各プログラム更新中に新しいシステム復旧ポイントを作成する*** - 各 AVG プログラム更新の起動前に、システム復旧ポイントが作成されます。アップデートプロセスが失敗し、オペレーティングシステムがクラッシュする場合には、必ずこのポイントから元のコンフィグレーションでOSを復旧できます。このオプションは、スタート/プログラム/アクセサリ/システムツール/システムの復元からアクセスできますが、上級ユーザーのみが変更を行うようにすることをお勧めします。この機能を使用する場合は、このチェックボックスにチェックを付けておきます。

- ***DNS 更新を使用する*** (*既定ではオン*) - この項目にチェックを付けると、更新が実行された時点で、**AVG Internet Security 2011** が DNS サーバー上の最新のウィルス 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、最小限の必須の更新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、更新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、アップデートプロセスの完了に必要な場合、現在実行中のアプリケーションが許可なく終了しないように確認できます。

  - ***コンピュータ時間を確認*** - このオプションにチェックを付けると、コンピュータ時間と正確な時間との差が指定された時間よりも大きい場合に通知を表示するよう宣言します。

### 9.16.1. プロキシ




プロキシサーバーとは、より安全なインターネット接続を保証するスタンドアロンサーバー、またはPC上のサービスです。特定のネットワークルールによって、インターネットに直接またはプロキシサーバーを介して接続できます。次に、***アップデート設定- プロキシ***ダイアログの最初のアイテムで、コンボボックスメニューから希望するものを選択する必要があります。

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

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

**手動設定**

手動設定（***手動****オプションをチェックすると、該当する入力欄が有効化されます*）を

選択する場合、以下の項目を指定してください。

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

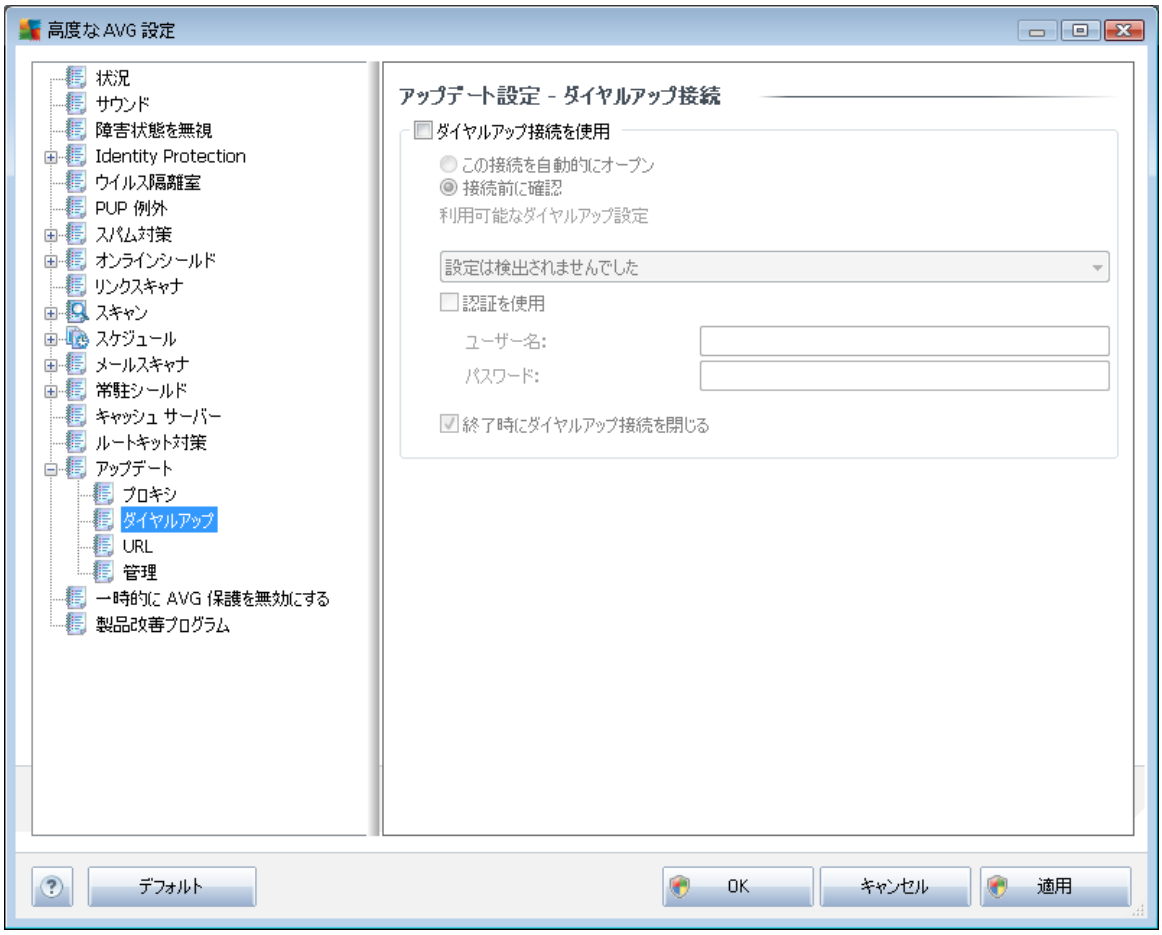
プロキシサーバーは、各ユーザーのルールを設定することもできます。プロキシサーバーがこのように設定されている場合、***プロキシ認証を使用***にチェックを付け、有効なユーザー名とパスワードを入力してください。

## 自動設定

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

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

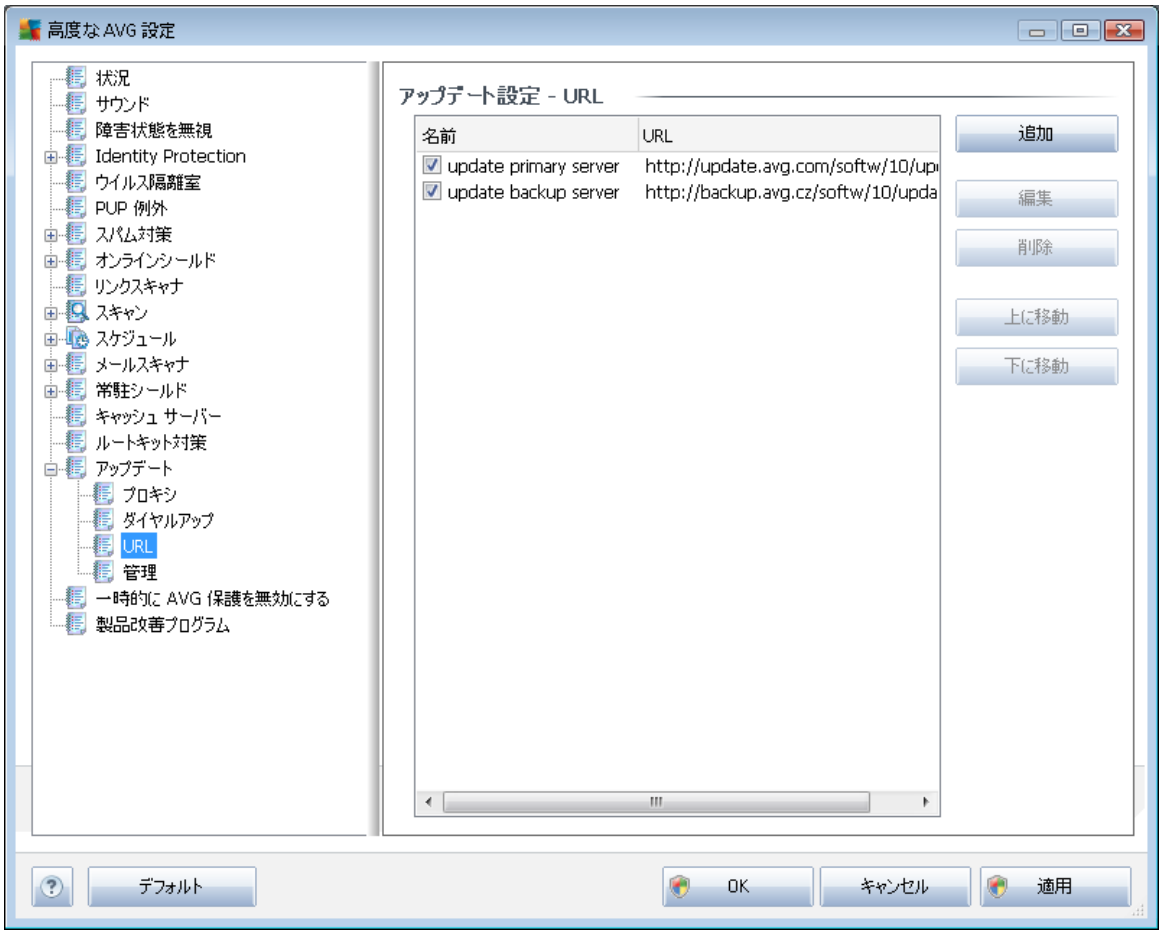
### 9.16.2. ダイヤルアップ




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

インターネットに自動接続（***自動的にこの接続をオープン***）するか、毎回手動で接続を確認（***接続前に確認***）するかを指定します。自動接続については、さらに接続がアップデート終了後に切断されるかどうかを選択します（***終了後ダイヤルアップ接続を閉じる***）。

### 9.16.3. URL

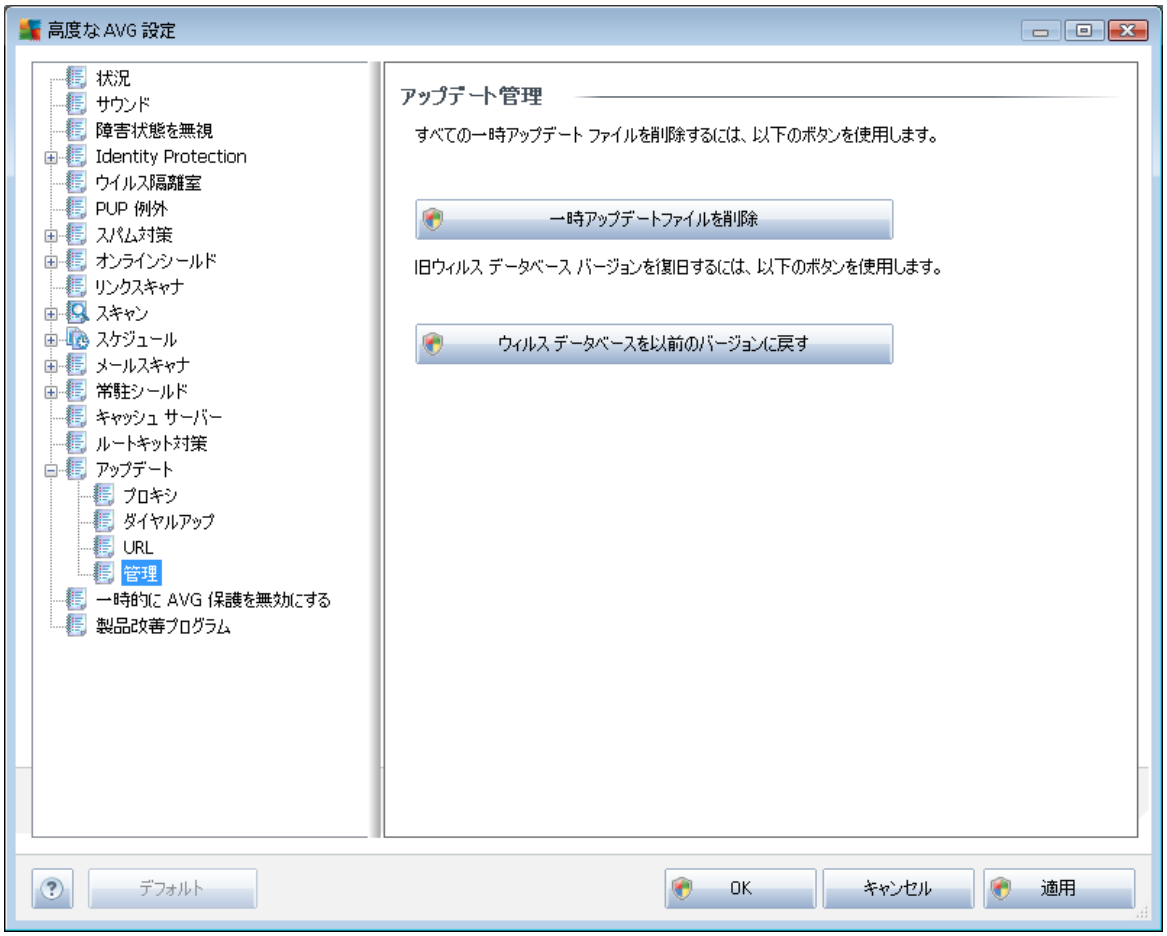



***URL***ダイアログでは、アップデートファイルがダウンロードされるインターネットアドレスのリストが表示されます。このリストは、以下のコントロールボタンを使用して修正します。

- ***追加***–ダイアログを開き、新しいURLを指定してリストに追加します
- ***編集***–ダイアログを開き、選択されたURLパラメータを編集します。
- ***削除***–選択されたURLをリストから削除します。
- ***上に移動***–選択されたURLを1つ上の場所に移動します。
- ***下に移動***– 選択されたURLを1つ下の場所に移動します。

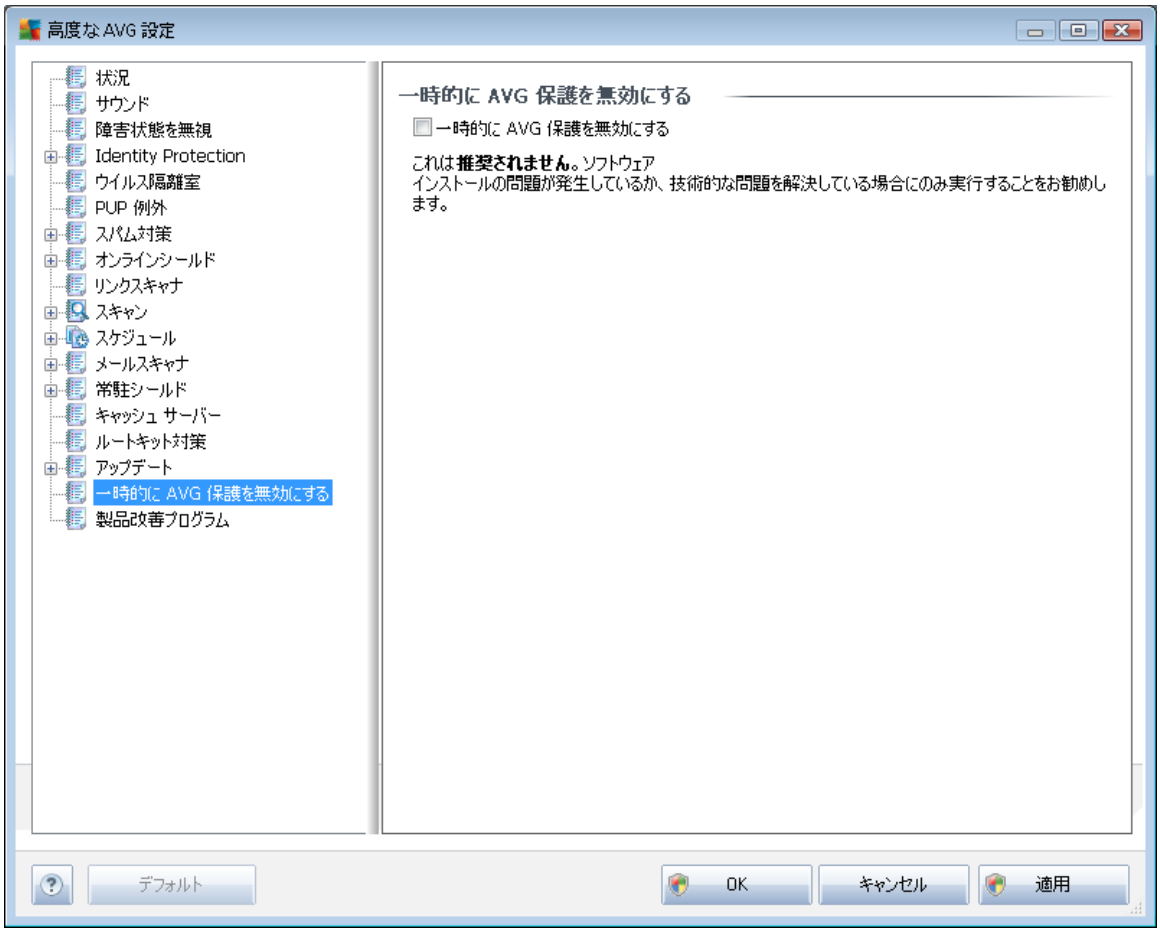
### 9.16.4. 管理

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




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

## 9.17. 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 2011** の保護機能すべてを一度にオフにすることができます。

***やむを得ない場合を除き、このオプションの使用はお勧めしません。***

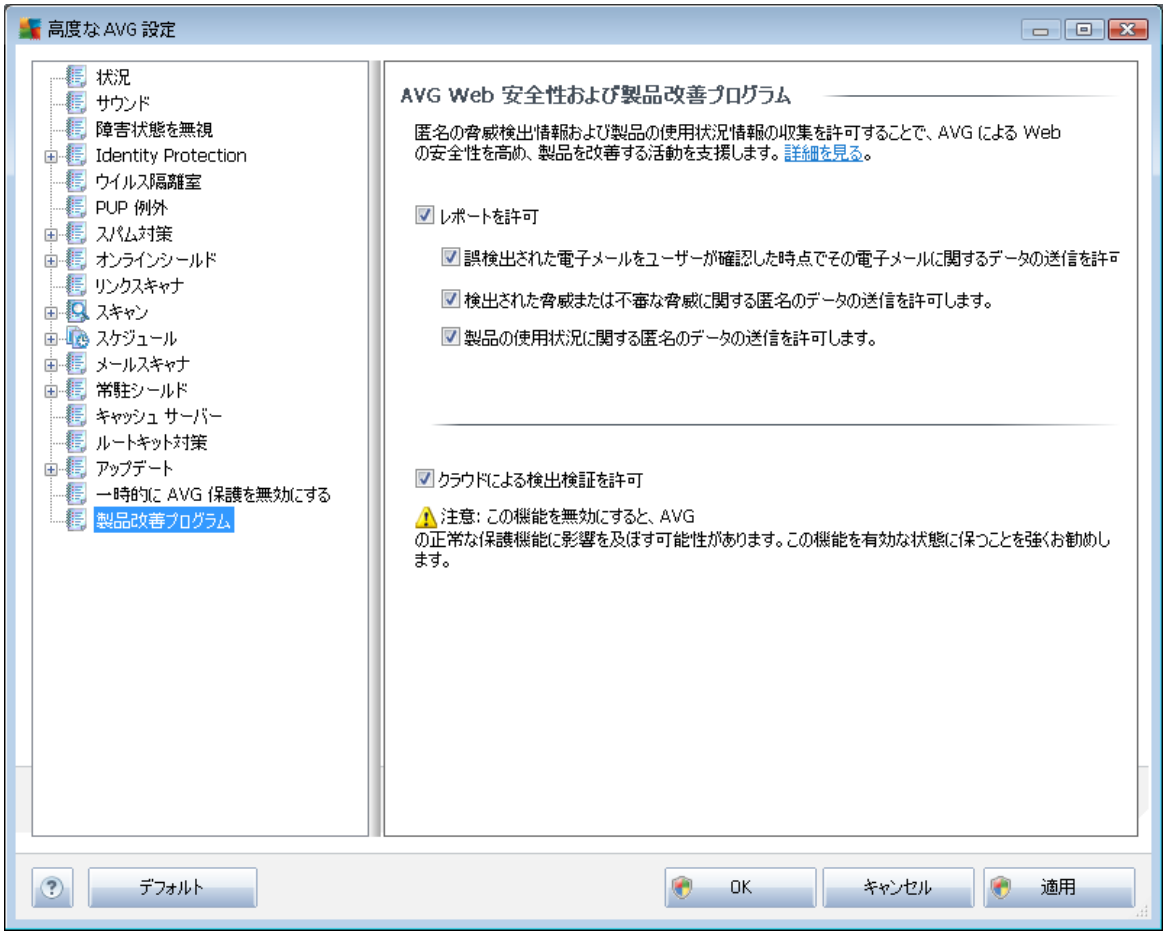
インストール処理中に望ましくない中断が発生しないようにするために、インストーラやソフトウェア ウィザードで実行中のプログラムやアプリケーションを終了するように指示される場合がありますが、それでも通常は新しいソフトウェアやドライバをインストールする前に、AVG を無効にする***必要はありません***。インストール中に問題が発生した場合は、まず***常駐シールド*** コンポーネントを無効にしてください。一時的に AVG を無効にする必要がある場合は、できる限り速やかに再有効化することをお勧めします。ウィルス対策ソフトウェアが無効な状態でインターネットやネットワークに接続している場合は、コンピュータが攻撃の危険にさらされています。

## 9.18. 製品改善プログラム

[***AVG Web 安全性および製品改善プログラム***] ダイアログでは、AVG 製品改善プログラムへの参加で実現できる全体的なインターネット セキュリティ レベルの向上について案内されます。[***報告を許可する***] オプションにチェックを付けると、検出した脅威

を AVG に報告します。 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、保護を向上させます。

***報告は自動的に実行され、面倒な手間はありません。また、個人情報は一切含まれません。*** 検出された脅威の報告は任意ですが、お客様にはこの機能をオンにしていただくようにお願いしております。これはお客様を含むすべての AVG ユーザーの保護を向上させる上で役立ちます。




今日においては、単なるウイルスだけではなく、さまざまな脅威が存在します。悪意のあるコードと危険な Web サイトの作成者は非常に革新的であり、新しい種類の脅威が常に出現しています。そしてその多くはインターネット上に存在しているのです。一般的な脅威:

- ***ウイルスとは、それ自体をコピーし、拡大させる悪意のあるコードで、多くの場合、被害が出るまで気が付きません。*** 一部のウイルスは深刻な脅威であり、独自の方法で、ファイルを削除したり意図的に変更したりします。ウイルスには、音楽を演奏するなど、一見無害のように見えるものもあります。ただし、すべてのウイルスは基本的に増殖する能力を持つため危険です。1 つのウイルスでさえコンピュータメモリ全体をすぐに制御し、障害を引き起こします。

- ***ワーム***はウイルスの下位カテゴリに含まれています。通常のウイルスと異なり、ワームは感染する「キャリア」を必要としません。通常、ワームが含まれたメールが他のコンピュータに送信されます。その結果、メール サーバーとネットワーク システムの過負荷状態などを引き起こします。

- ***スパイウェア***は、通常マルウェアのカテゴリとして定義されます (*マルウェアとはウイルスを含む悪意のあるソフトウェアのことです)。このマルウェアには、コンピュータの所有者が知らない間に同意なく個人情報、パスワード、クレジット カード番号を盗んだり、コンピュータに侵入し、攻撃者にリモートでコンピュータをコントロールさせたりすることを目的とするプログラム (通常はトロイの木馬) が含まれます。*

- ***不審なプログラム***はスパイウェアの一種ですが、必ずしもコンピュータに被害を及ぼすとは限りません。PUP の具体的な例としては、ポップアップ広告を表示させ、広告を配信することを目的としたソフトウェアであるアドウェアがあります。これらは迷惑ではあるものの実際には無害です。

- □□□***Tracking cookie*** もスパイウェアの一種と見なされます。この小さなファイルは Web ブラウザに保存され、再度アクセスした際、自動的に「親」Web サイトに送信されます。Tracking cookie には閲覧履歴などのデータが含まれています。

- ***エクスプロイト***はオペレーティング システム、インターネット ブラウザ、あるいは重要なプログラムの欠陥や脆弱性を利用する悪意のあるコードです。

- ***フィッシング***は信頼できる有名な組織を装って重要な個人情報データを取得しようとする試みです。たとえば、被害者宛てに銀行口座の詳細情報を更新するように求める大量のメールが送信されます。ユーザーはリンクに従い、偽の銀行の Web サイトに誘導されます。

- ***Hoax は危険な情報、何かを警告する情報、あるいはただ単に迷惑で無用な情報を含む大量のメールです。*** 上記の脅威の多くは Hoax メール メッセージを使用して広がります。

- 悪意のある Web サイトとは、故意に悪意のあるソフトウェアをコンピュータにインストールするものです。ハッカーに攻撃されたサイトにも同様にアクセスしたユーザーを感染させる危険が潜んでいますが、このようなサイトは本来は合法的な Web サイトです。

***このようなさまざまな脅威からコンピュータを保護するために、AVG には次の特別なコンポーネントが含まれています。***

- ***コンピュータをウイルスから保護するウイルス対策***

- ***コンピュータをスパイウェアから保護するスパイウェア対策***

- ***インターネット閲覧中のユーザーをウイルスとスパイウェアから保護するオンライン シールド***

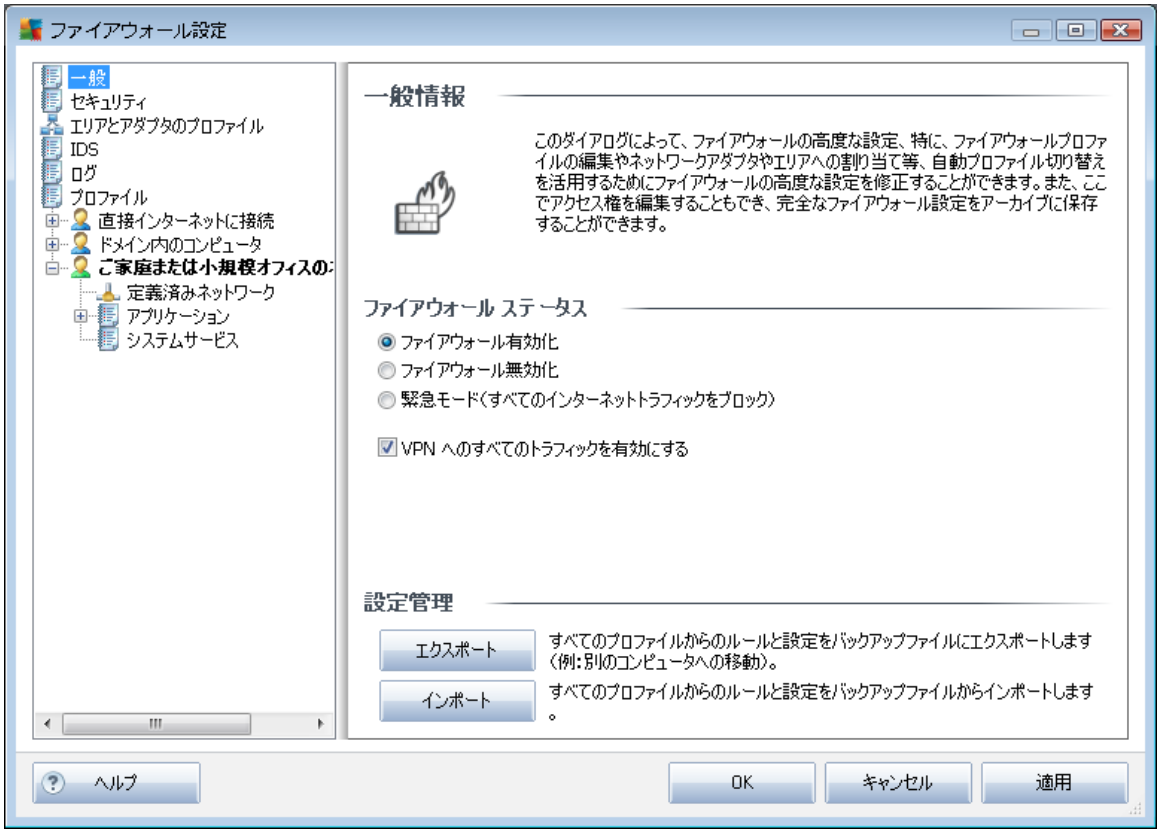
- ***本章で述べられたその他のオンライン脅威から保護するリンクスキャナ***

# 10. ファイアウォール設定

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

## 10.1. 一般

[***全般情報***] ダイアログには 2 つのセクションがあります。




### ファイアウォール ステータス

[***ファイアウォール ステータス***] セクションでは、必要に応じて、***ファイアウォール***ステータスを切り替えることができます。

- ***ファイアウォール有効化*** - 選択された***ファイアウォールプロファイル***で定義されたルールセットに基づいて、アプリケーションの通信を許可します。
- ***ファイアウォール無効化*** - このオプションは***ファイアウォール***を完全にオフに切り替えます。すべてのネットワークトラフィックは許可され、チェックされません。
- ***緊急モード*** *(すべてのインターネット トラフィックをブロック)* - このオプショ

ンを選択すると、各ネットワーク ポートでのすべてのトラフィックをブロックします。***ファイアウォール***は実行中ですが、すべてのネットワーク トラフィックは停止されます。

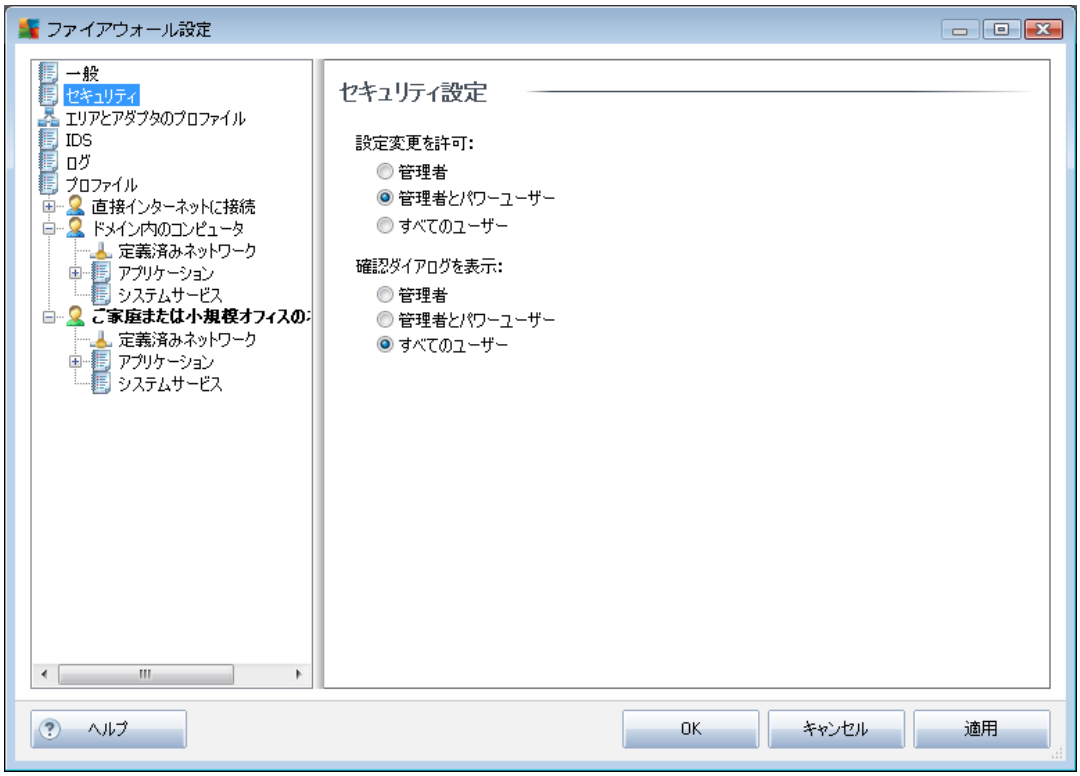
- ***VPN へのすべてのトラフィックを有効にする*** - 自宅からオフィスに接続している場合など、VPN (*仮想プライベート ネットワーク*) 接続を使用する場合、ボックスを選択することをお勧めします。***AVG ファイアウォール***はネットワーク アダプタを自動的に検索し、VPN 接続で使用されているものを検出し、すべてのアプリケーションによるターゲット ネットワークへの接続を許可します (*特定のファイアウォールはネットワーク ルールが割り当てられていないアプリケーションにのみ適用されます*)。一般的なネットワーク アダプタを使用する標準的なシステムでは、このシンプルなステップにより、VPN で使用する各アプリケーションについて詳細なルールを設定する必要がありません。

***メモ:*** *VPN 接続を有効にするには、GRE、ESP、L2TP、PPTP システム プロトコルとの通信を許可する必要があります。これは [システム サービス] ダイアログで設定できます。*

## 設定管理

[***設定管理***] セクションでは、***ファイアウォール***設定の***エクスポート***と***インポート***ができます。たとえば、定義済みの***ファイアウォール*** ルールと設定をバックアップ ファイルにエクスポートしたり、バックアップ ファイル全体をインポートしたりできます。

## 10.2. セキュリティ




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

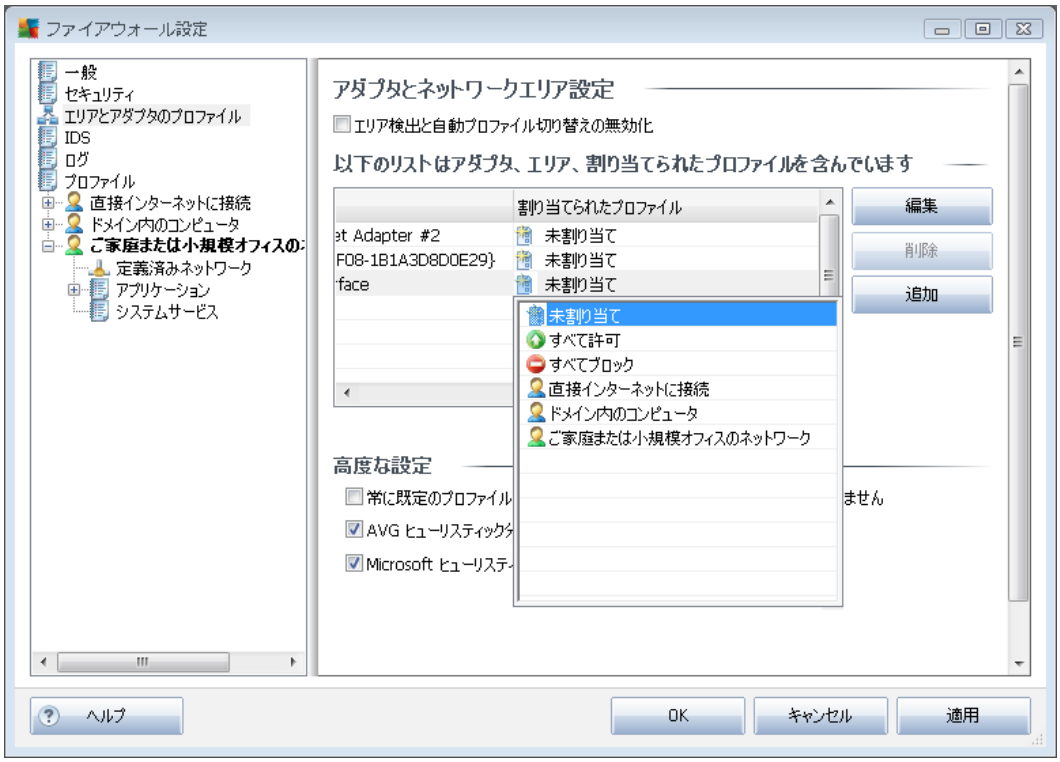
- 設定変更を許可 - ***ファイアウォール***の設定変更を許可するユーザーを指定します。
- 確認ダイアログを表示 - 設定ダイアログ（*定義された****ファイアウォール****ルールに含まれていない状況での決定ダイアログ*）が表示されるユーザーを指定します。

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

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

## 10.3. エリアとアダプタのプロファイル

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




- ***エリア検出と自動プロファイル切り替えの無効化***- 定義されたプロファイルの 1 つは、各ネットワークのインターフェース タイプ、各エリアにそれぞれ割り当てられます。特定のプロファイルを定義しない場合は、1 つの共通プロファイルを使用します。ただし、プロファイルを区別し特定のアダプタとエリアに割り当てた後でこの設定を一時的に切り替える場合は、[***エリア検出と自動プロファイル切り替えを無効にする***] にチェックを付けます。

- ***アダプタとエリア、割り当てられたプロファイルのリスト*** - このリストでは検出されたアダプタとエリアの概要が表示されます。定義されたプロファイルのメニューの特定のプロファイルを各アダプタに割り当てることができます。このメニューを開くには、アダプタリストで該当するアイテムをクリックし、プロファイルを選択します。

### 高度な設定

  - ***常に既定のプロファイルを使用し、新しいネットワーク検出ダイアログを表示しない*** - コンピュータが新しいネットワークに接続するたびに、***ファイアウォール***によってアラート通知が行われ、***ファイアウォール プロファイル***に割り当てるネットワーク接続の種類を選択するた

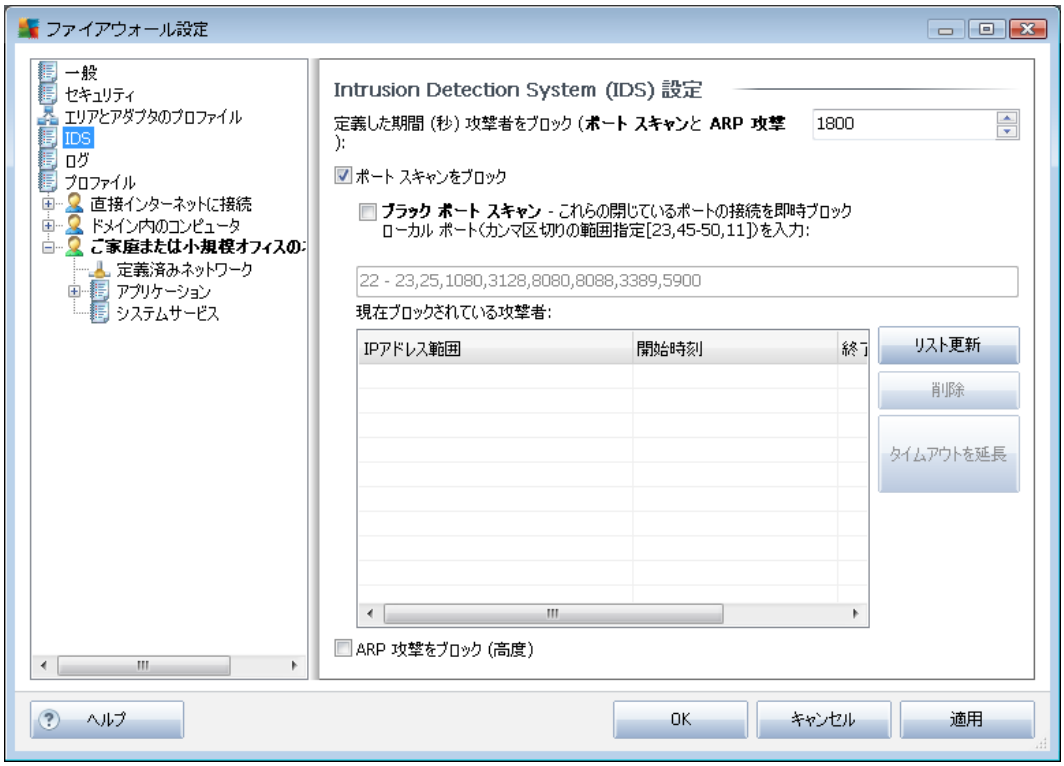
めのダイアログが表示されます。このダイアログを表示しない場合は、このボックスを選択します。

- ***新しいネットワークを検出するときに AVG ヒューリスティックを使用する*** - AVG 独自のメカニズムを使用して、新しく検出されたネットワークに関する情報を収集できます (*ただし、このオプションは Vista OS 以降でのみ利用できます*)。

- ***Microsoft のヒューリスティックを使用して新しいネットワークを検出する*** - 新しく検出されたネットワークに関する情報を Windows サービス (*このオプションは Windows Vista 以降のバージョンでのみ利用できます*) から取得します。

## 10.4. IDS

***侵入検出システム***は、コンピュータの特定のポートで実行される不審な通信の試みを特定してブロックするための特殊な動作分析機能です。次のインターフェースで IDS パラメータを設定できます。




[***侵入検出システム (IDS) 設定***] ダイアログには次の設定オプションがあります。

- ***指定した期間攻撃者をブロックする*** - ポート上で不審な通信の試みが検出されたときに、ポートをブロックする秒数を設定できます。既定では 1800 秒 (*30 分*) に時間設定されています。

- ***ポート ブロック スキャン*** - ボックスにチェックを付けると、外部からコン

ピュータに入るすべての TCP ポートおよび UDP ポート上での通信の試みをブロックします。このような接続では、5 つの試みが許可され、6 番目の試みがブロックされます。

- ***ポート ブロック スキャン*** - ボックスにチェックを付けると、次のテキスト フィールドに指定したポート上でのすべての通信を即時にブロックします。各ポートまたはポート範囲を指定する場合は各ポートをカンマで区切る必要があります。この機能を利用する場合には、事前定義された推奨ポートの一覧があります。

- ***現在ブロックされている攻撃者*** - このセクションには、現在***ファイアウォール***によってブロックされている通信の試みがすべて一覧表示されます。ブロックされた試みの全履歴は [***ログ***] ダイアログの [*ポート スキャン ログ*] *タブに表示されます。*

- [***ARP 攻撃をブロックする***] では、潜在的に危険であると ***IDS*** が判断したローカル ネットワーク内 (ルーターの後) の特定の種類の通信の試みをブロックします。[***指定した期間攻撃者をブロックする] で設定した時間が適用されます。*** ローカル ネットワークの種類とリスク レベルを十分に把握している上級者ユーザーのみがこの機能を使用することをお勧めします。

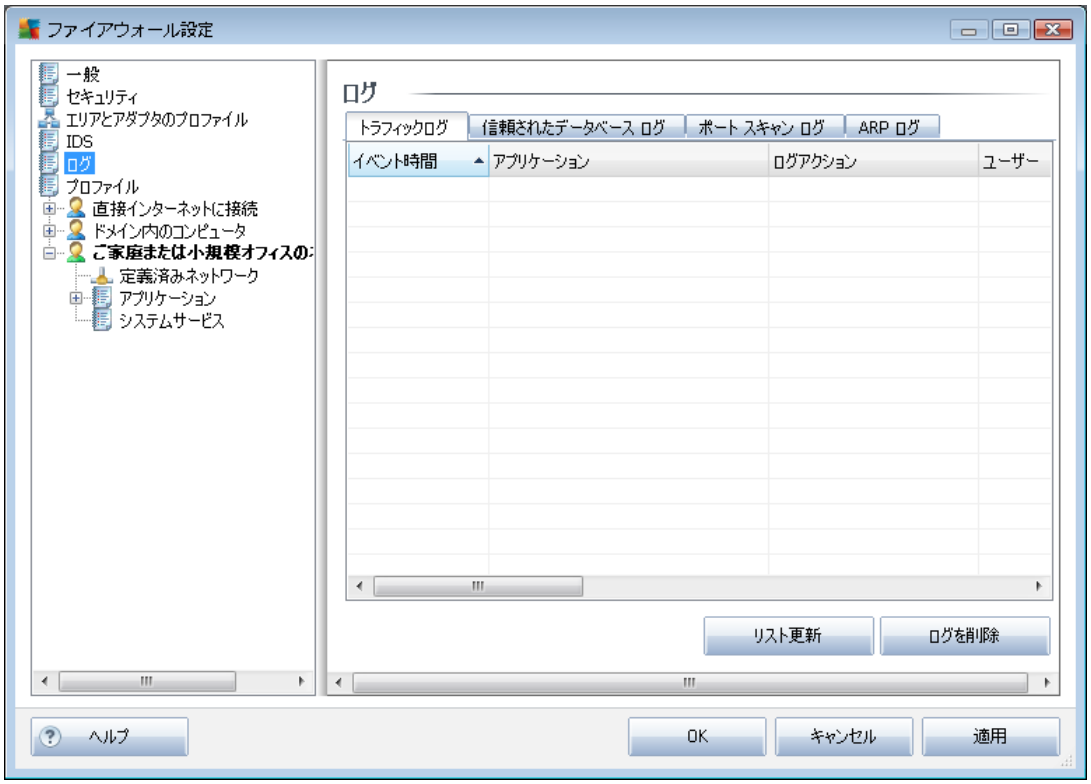
## コントロール ボタン

- ***リストの更新*** - このボタンをクリックすると、リストを更新し、*最新のブロックされた試みを反映します。*

- ***削除*** - このボタンをクリックすると、選択したブロックをキャンセルします。

- ***タイムアウト期間の延長*** - このボタンをクリックすると、選択した試みがブロックされる期間を延長します。新しいダイアログが開き、拡張オプションが表示されます。このダイアログで日時を設定するか、期間を無制限に設定できます。

## 10.5. ログ




[***ログ***] ダイアログでは、すべてのログ出力された***ファイアウォール***アクション、イベントのリスト、関連するパラメータの詳細説明 (*イベント時刻*、*アプリケーション名*、*各ログ アクション*、*ユーザー名*、*PID*、*トラフィック方向*、*プロトコル タイプ*、*リモートおよびローカルポート番号など*) が 4 つのタブに表示されます。

- ***トラフィックログ*** - ネットワークに接続しようとしたすべてのアプリケーションの活動に関する情報を提供します。
- ***信頼されたデータベースログ*** - *信頼されたデータベース*は、常にオンライン通信を許可できる認証され信頼されたアプリケーションに関する情報を収集する AVG 内部データベースです。新しいアプリケーションが初めてネットワークに接続しようとするとき（*つまり、まだこのアプリケーションに指定されたファイアウォールルールがない場合*）、そのアプリケーションに対してネットワーク通信を許可するかどうかを決定する必要があります。まず、AVG は*信頼されたデータベース*を検索し、アプリケーションがリストにある場合は、自動的にネットワークアクセスを付与します。その後に初めて、データベースに利用できる情報がない場合、アプリケーションのネットワークアクセスを許可するかどうかを確認するスタンドアロンダイアログが表示されます。
- ***ポート スキャン ログ*** - すべての***侵入検出システム***活動のログを出力します。
- ***ARP ログ*** - ***侵入検出システム***で危険な可能性がある試みとして検出されたローカル ネットワーク内での特定の種類の通信の試みのブロックに関するログ情

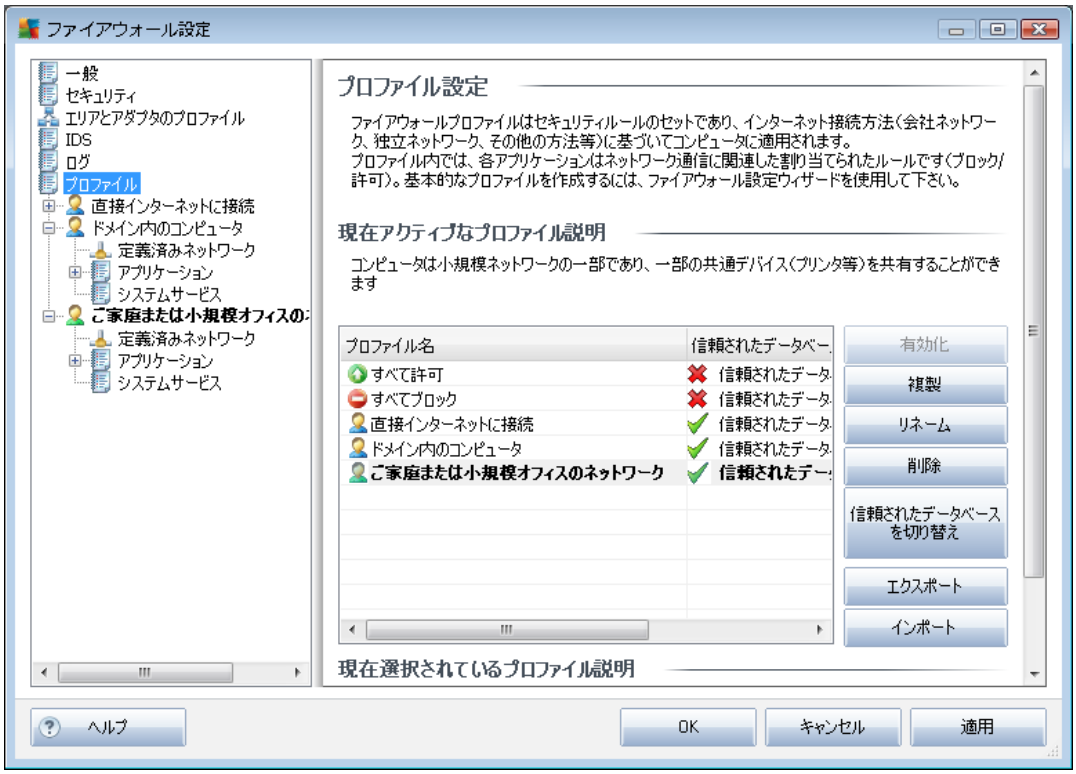
報 ([*ARP 攻撃をブロックする*] オプション)。

### 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。です。各カラムヘッダーをクリックするだけです。***リスト更新***ボタンを使用して、現在表示されている情報を更新します。
- ***リストを空にする***-表のすべてのエントリを削除します。

## 10.6. プロファイル

***プロファイル設定***ダイアログでは、すべての利用可能なプロファイルが表示されます。




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

- ***有効化*** - このボタンは選択されたプロファイルを有効化します。これによって、***ファイアウォール***でネットワークトラフィックをコントロールするために、選択されたプロファイルが使用されます。
- ***複製*** - 選択されたプロファイルのコピーを作成します。コピーを編集し、複製されたプロファイルをベースに新しいプロファイルを作成することができま

す。

- ***プロファイルの名前変更*** - 選択したプロファイルの新しい名前を定義できます。
- ***削除***–選択されたプロファイルをリストから削除します。
- ***信頼されたデータベースを切り替え*** - 選択されたプロファイルに対して、*信頼されたデータベース*情報（*信頼されたデータベースは、常にオンライン通信を許可された信頼され認証されたアプリケーションに関する情報を収集するデータベースです*）を使用するかどうかを決定できます。
- ***エクスポート*** - 選択されたプロファイル設定をファイルに保存します。
- ***インポート*** - 選択されたプロファイル設定をバックアップした設定ファイルからインポートします。

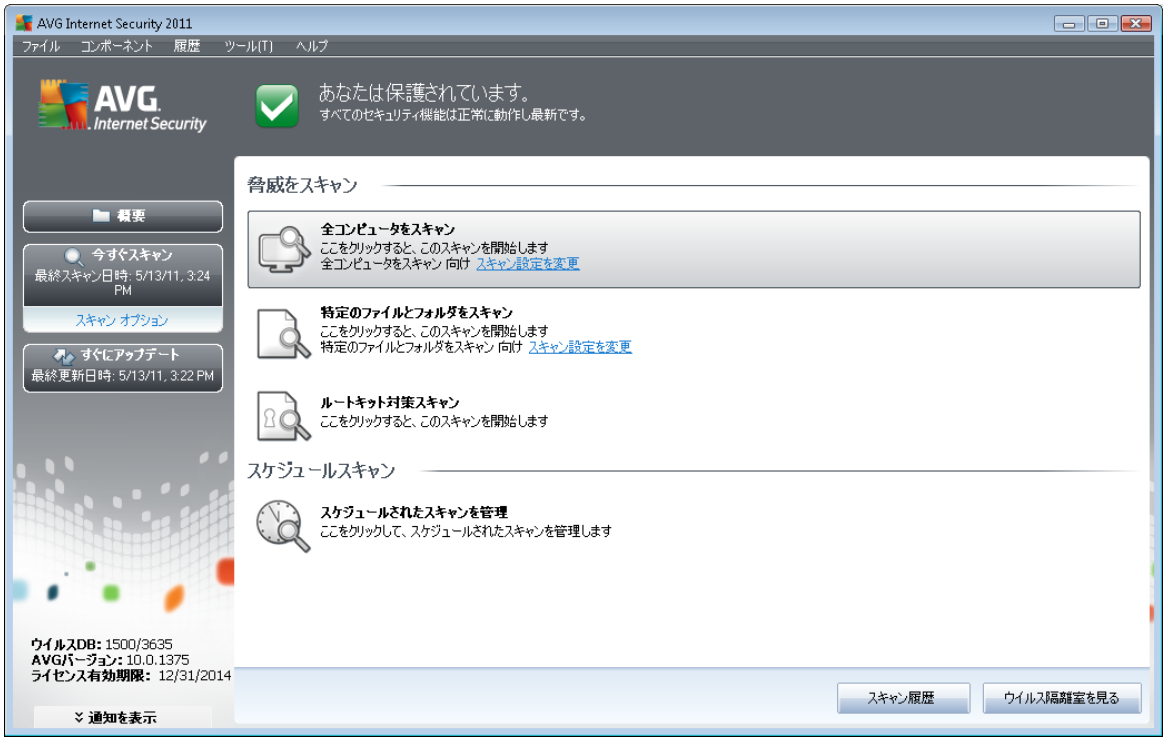
ダイアログ下部のセクションには、現在上記リストで選択されているプロファイルの説明が表示されます。

***プロファイル***ダイアログ内のリストで定義されているプロファイル数に基づいて、左のナビゲーションメニューの構造が変化します。***プロファイル***以下に、各定義済みプロファイルが作成されます。各プロファイルは、以下のダイアログ（*すべてのプロファイルで同一*）で編集可能です。

# 11. AVG スキャン

スキャンは **AVG Internet Security 2011** 機能の最重要な要素です。オンデマンドでスキャンを実行したり、時間を指定して定期的に実行されるようにスケジュールすることもできます。

## 11.1. スキャン インターフェース




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

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

**コントロールボタン**

スキャンインターフェースで利用できるコントロールボタンは以下の通りです。

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

## 11.2. 定義済みスキャン

**AVG Internet Security 2011** の主要な機能の 1 つは、オンデマンド スキャンです。オンデマンド スキャンは、ウイルス感染の疑いがある場合、コンピュータの各領域をいつでもスキャンできるように設計されています。たとえウイルスがコンピュータに存在しないと思われる場合でも、このスキャンを定期的に実行することを強くお勧めします。

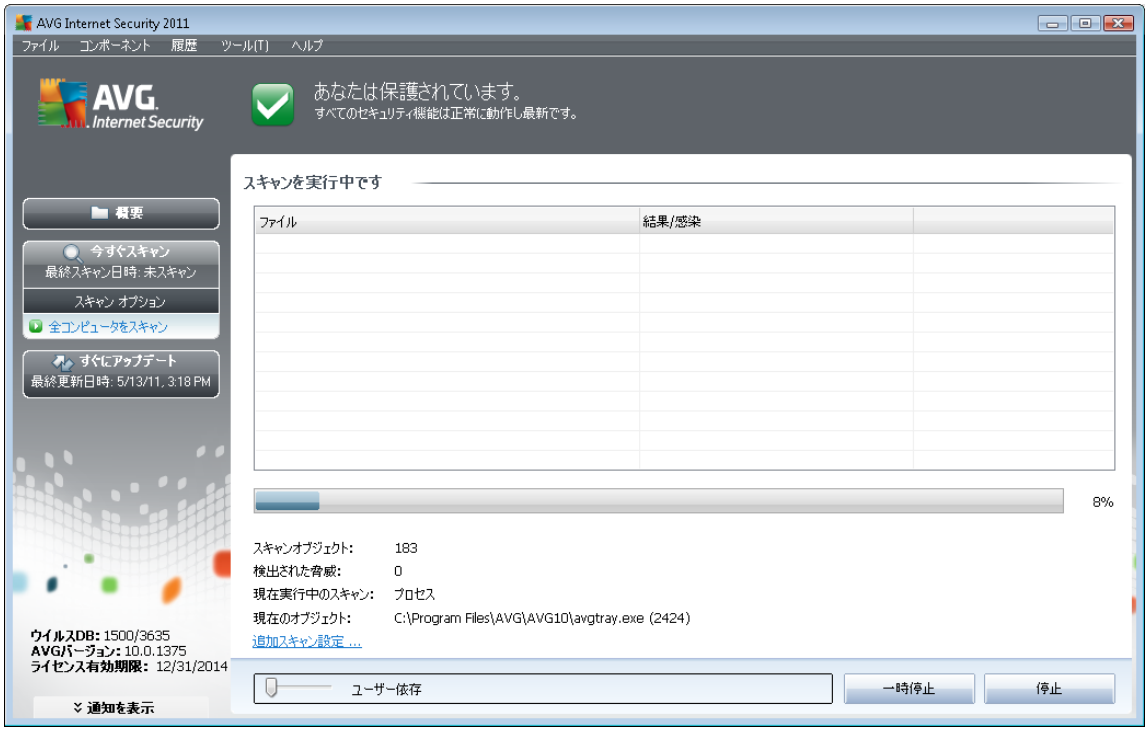
**AVG Internet Security 2011** には、ソフトウェア ベンダがあらかじめ定義した次のスキャンがあります。

### 11.2.1. 完全コンピュータ スキャン

***完全コンピュータ スキャン*** - コンピュータを完全にスキャンして、感染と不審なプログラムがあるかどうかを確認します。このスキャンはコンピュータのハード ドライブ全体をスキャンし、ウイルス感染の検出、修復、検出した感染の***ウイルス隔離室***への移動を実行します。週に 1 度以上は完全コンピュータ スキャンを実行するようにスケジュールを設定してください。。

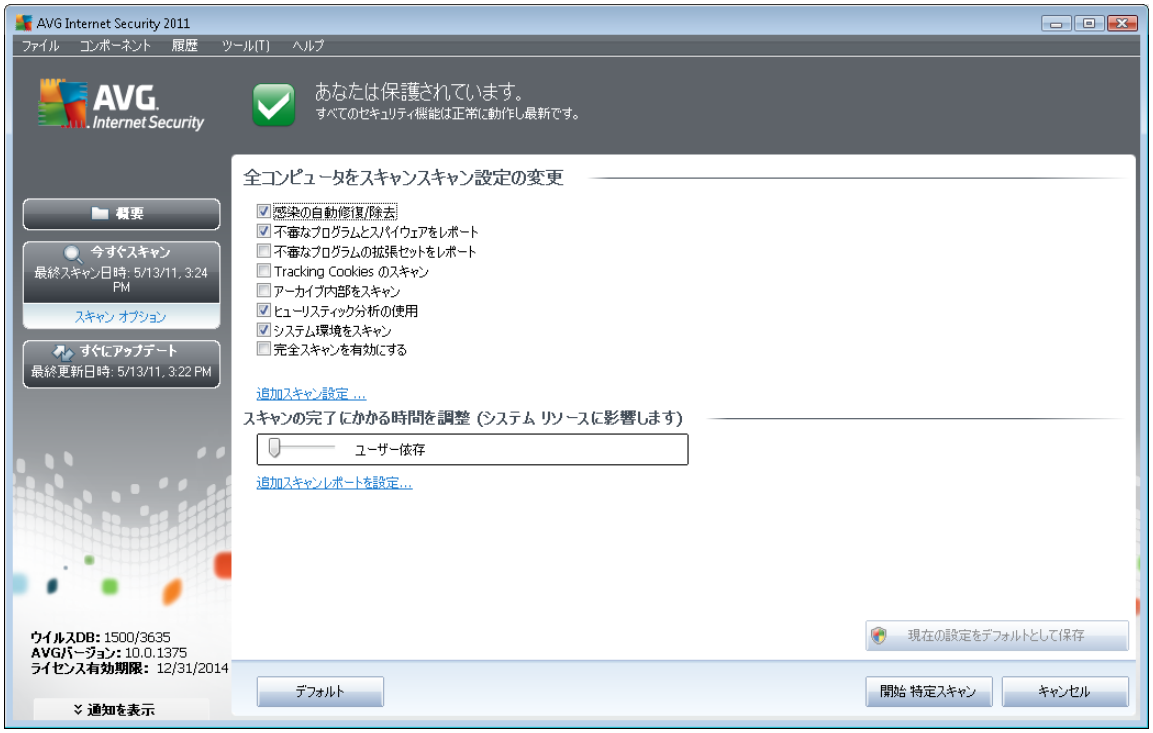
#### スキャン実行

スキャン アイコンをクリックすると、***完全コンピュータ スキャン***をスキャン インターフェースから直接実行できます。このスキャンに対して、さらに特別な設定は必要ありません。スキャンは [***スキャン実行中***] ダイアログ内で即時開始されます (*スクリーンショット*を参照)。必要に応じて、スキャンを一時的に中断 (***一時停止***) またはキャンセル (***停止***) できます。




## スキャン設定編集

***完全コンピュータ スキャン***の既定の設定を編集することもできます。[***スキャン設定を変更***] リンクをクリックすると、[***完全コンピュータ スキャンのスキャン設定の変更***] ダイアログ (*完全コンピュータ スキャンの [スキャン設定を変更] リンク経由でスキャン インターフェースからアクセス可能*) が表示されます。***特に理由がない場合は、この既定の設定を保持することをお勧めします。***




- ***スキャン パラメータ*** - スキャン パラメータの一覧では、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。

  - ***自動的に感染を修復/除去する*** (*既定ではオン*): スキャン実行中にウイルスが特定され、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***ウィルス隔離室***に移動されます。

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

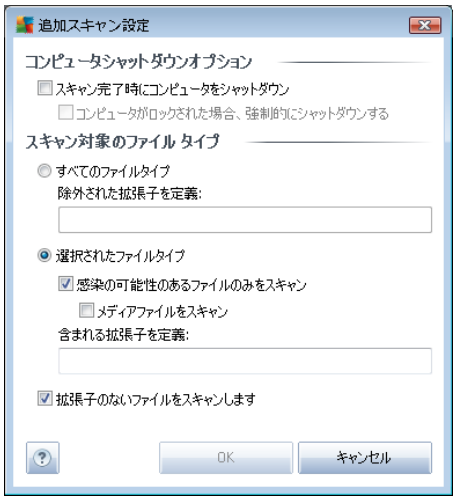
  - ***不審なプログラムの拡張セットを報告する*** (*既定ではオフ*): チェックを付けると、スパイウェアの拡張パッケージを検出します。スパイウェアとは、直接製造元から入手する場合にはまったく問題がなく、無害なプログラムですが、後から悪意のある目的で誤用されるおそれのあるプログラムです。これは、コンピュータ セキュリティをさらに高めるための追加的な手段ですが、合法的なプログラムもブロックする可能性があるため、デフォルトではオフになっています。

  - ***Tracking Cookie をスキャンする*** (*既定ではオフ*) - ***スパイウェア対策コンポーネントのこのパラメータを定義すると、Cookie を検出します (***HTTP cookie は、サイトの設定や電子ショッピング カートの内容など、ユ

ーザー固有の情報の認証、追跡、メンテナンスに使用されます)。

- ***アーカイブの内容をスキャンする*** (*既定ではオフ*) - ZIP や RAR などのアーカイブ内に格納されているすべてのファイルをスキャンします。
- ***ヒューリスティック分析を使用する*** (*既定ではオン*) - ヒューリスティック分析 (*仮想コンピュータ環境で実行されるスキャン対象オブジェクト命令の動的エミュレーション*) は、スキャン実行中に採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する*** (*既定ではオン*) - コンピュータのシステム領域もチェックされます。
- ***完全スキャンを有効にする*** (*既定ではオフ*) - このオプションをチェックすると、特定の状況 (*コンピュータが感染している疑いがある場合など*) が発生した場合に最も完全なスキャン アルゴリズムを有効にし、感染の可能性が非常に低いコンピュータ領域もスキャンします。これにより、問題がないことを確実に確認します。この方法を実行すると多少時間がかかります。

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




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

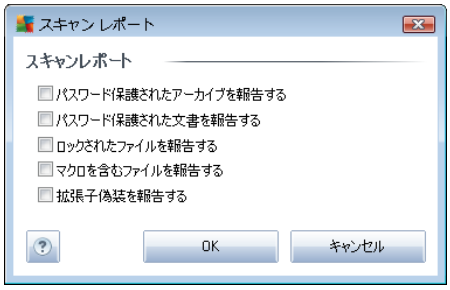
- ***すべてのファイル タイプと***スキャン対象ではないファイル拡張子をカンマで区切ったリストを入力することで、スキャンからの除外を定義できます。

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

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

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

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




***警告:*** *これらのスキャン設定は新規に定義されたスキャン パラメータと同じです。「****AVG スキャン/スキャン スケジュール/スキャン方法****」の章を参照してください。****完全コンピュータ スキャン****の既定の設定を変更する場合、新しい設定を既定の設定として保存し、すべての完全コンピュータ スキャンに適用できます。*

### 11.2.2. 特定のファイルとフォルダのスキャン

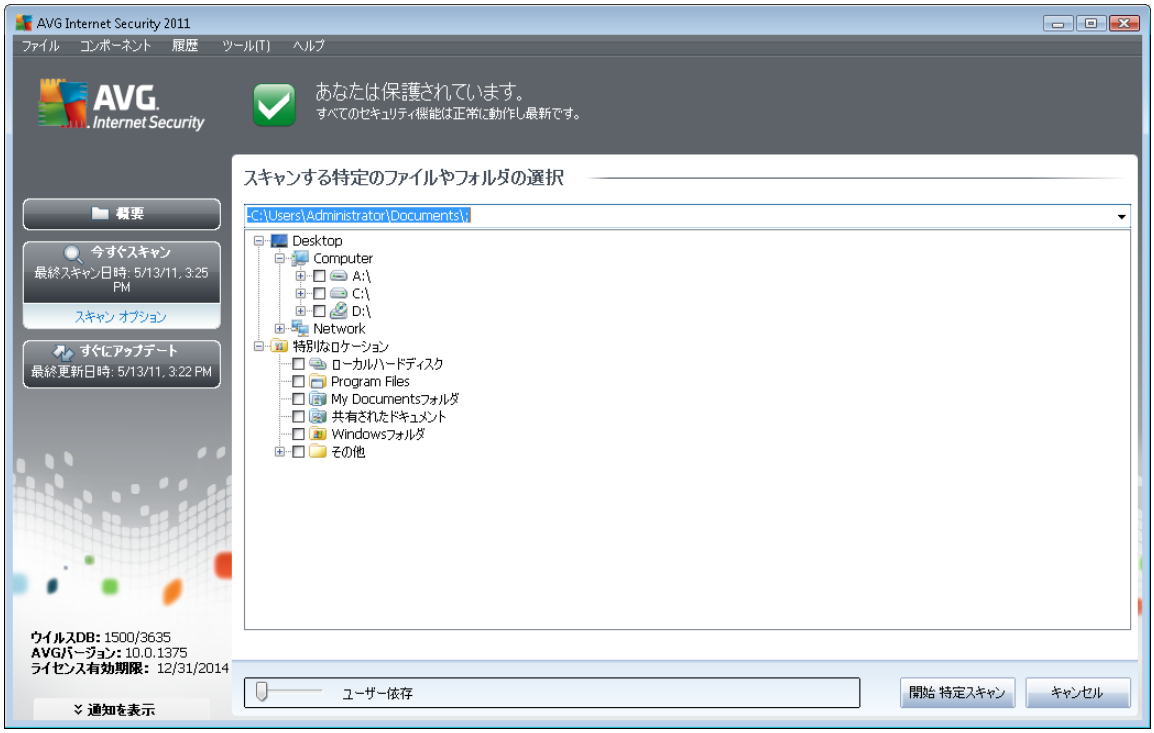
***特定のファイルやフォルダをスキャン*** - 選択した領域のみスキャンします (*選択したフォルダ、ハード ディスク、フロッピー ディスク、CD など*)。ウイルス検出や処理のスキャン進捗は完全コンピュータ スキャンの場合と同じです。検出されたウイルスは修復されるか***ウイルス隔離室***に移動されます。特定のファイルやフォルダのスキャンでは、ユーザー独自のスキャン設定とスケジュールを実行できます。

## スキャン実行

をスキャン インターフェースから直接起動できます。[***スキャンする特定のファイルまたはフォルダの選択***] 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造でスキャンするフォルダを選択します。選択したフォルダへのパスは自動的に作成され、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。

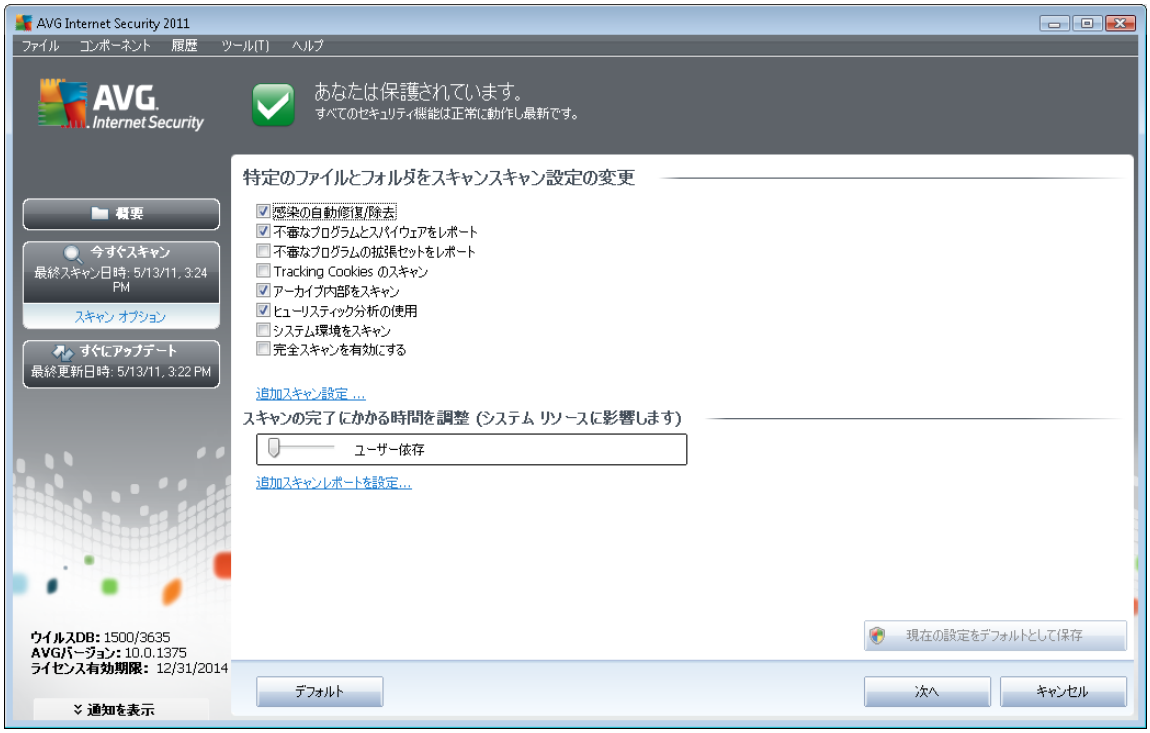
また、すべてのサブフォルダをスキャンしない場合、自動作成されたパスの前にマイナス記号「-」を記述します (*スクリーンショットを参照*)。スキャンからフォルダ全体を除外するには「!」パラメータを使用します。

スキャンを実行するには、[***スキャン開始***] ボタンをクリックします。スキャン処理自体は基本的に完全コンピュータ スキャンと同じです。




## スキャン設定編集

特定のファイルやフォルダスキャンのあらかじめ定義された既定の設定***を編集できます***。[***スキャン設定の変更***] リンクをクリックすると、[***特定のファイルとフォルダのスキャン設定の変更***] ダイアログが表示されます。***特に理由がない場合は、この既定の設定を保持することをお勧めします。***




- ***スキャン パラメータ*** - スキャン パラメータの一覧では、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。

  - ***自動的に感染を修復/除去する*** (*既定ではオン*): スキャン実行中にウイルスが特定され、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***ウィルス隔離室***に移動されます。

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

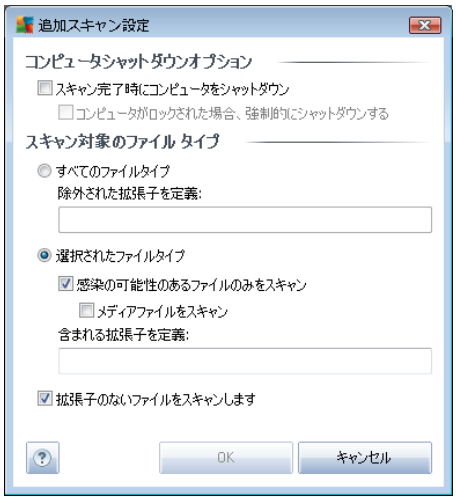
  - ***不審なプログラムの拡張セットを報告する*** (*既定ではオフ*): チェックを付けると、スパイウェアの拡張パッケージを検出します。スパイウェアとは、直接製造元から入手する場合にはまったく問題がなく、無害なプログラムですが、後から悪意のある目的で誤用されるおそれのあるプログラムです。これは、コンピュータ セキュリティをさらに高めるための追加的な手段ですが、合法的なプログラムもブロックする可能性があるため、デフォルトではオフになっています。

  - ***Tracking Cookie をスキャンする*** (*既定ではオフ*) - ***スパイウェア対策コンポーネント***のこのパラメータを定義すると、Cookie を検出します ( *HTTP cookie は、サイトの設定や電子ショッピング カートの内容など、ユ*

*ーザー固有の情報の認証、追跡、メンテナンスに使用されます*)。

- ***アーカイブの内容をスキャン*** (*既定ではオン*) - ZIP や RAR などのアーカイブ内に格納されているすべてのファイルをスキャンします。
- ***ヒューリスティック分析を使用する*** (*既定ではオフ*) - 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。
- ***システム環境をスキャンする*** (*既定ではオフ*) - コンピュータのシステム領域もチェックされます。
- ***完全スキャンを有効にする*** (*既定ではオフ*) - このオプションをチェックすると、特定の状況 (*コンピュータが感染している疑いがある場合など*) が発生した場合に最も完全なスキャン アルゴリズムを有効にし、感染の可能性が非常に低いコンピュータ領域もスキャンします。これにより、問題がないことを確実に確認します。この方法を実行すると多少時間がかかります。

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




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

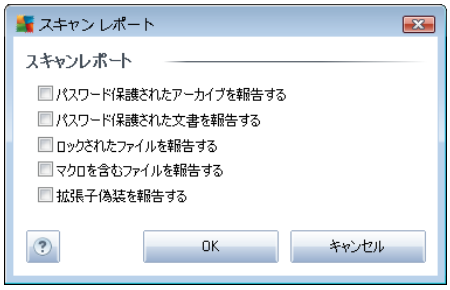
- ***すべてのファイル タイプと***スキャン対象ではないファイル拡張子をカンマで区切ったリストを入力することで、スキャンからの除外を定義できます。

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

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

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

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



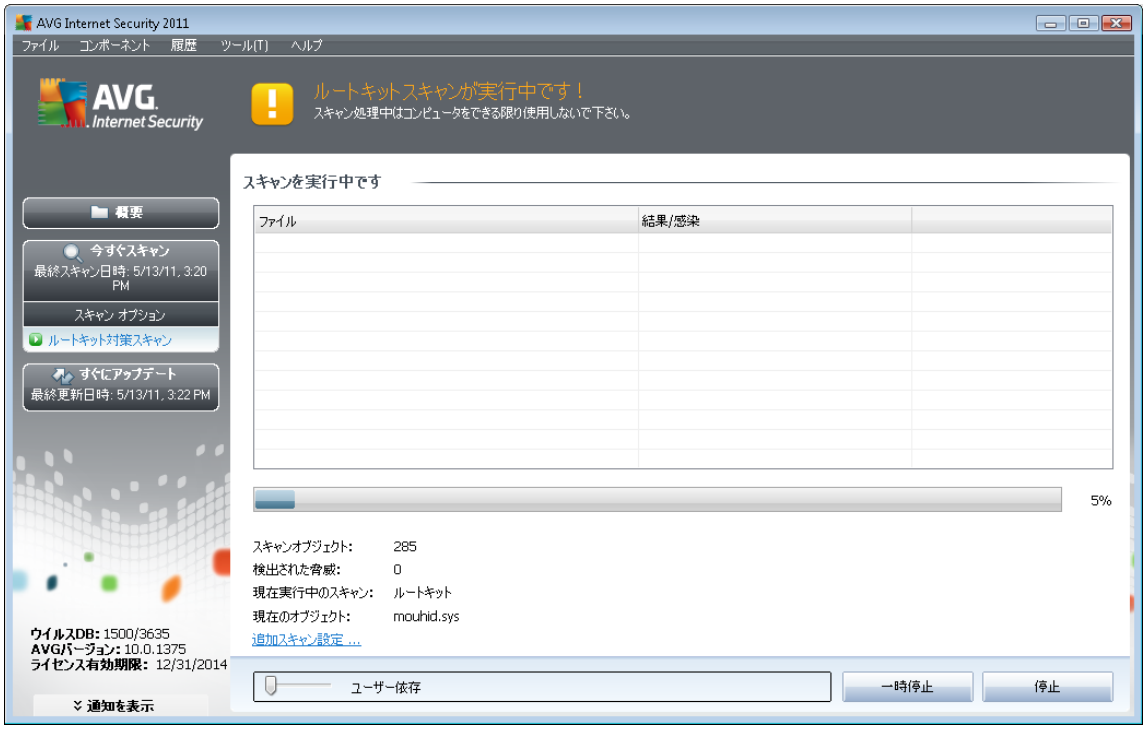

***警告:*** *これらのスキャン設定は新規に定義されたスキャン パラメータと同じです。「**AVG スキャン/スキャン スケジュール/スキャン方法**」の章を参照してください。**特定のファイルやフォルダのスキャン**の既定の設定を変更する場合、新しい設定を既定の設定として保存し、すべての特定のファイルやフォルダのスキャンに適用できます。また、この設定はすべての新規スケジュールのテンプレートとして使用できます (すべてのカスタマイズ スキャンは、選択したファイルやフォルダのスキャンの現在の設定に基づいて実行されます)。*

### 11.2.3. ルートキット スキャン

***ルートキット対策スキャンはコンピュータを検索し、***ルートキット (*悪意のある活動をコンピュータで隠すことができるプログラムや技術*) が存在している可能性があるかどうかを確認します。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というわけではありません。通常のアプリケーションの特有のドライバやセクションが誤ってルートキットとして検出される場合もあります。

#### スキャン実行

スキャンのアイコンをクリックすると、***ルートキット対策スキャン***をスキャン インターフェースから直接実行できます。このスキャンに対して、さらに特別な設定は必要ありません。スキャンは [***スキャン実行中***] ダイアログ内で即時開始されます (*スクリーンショットを参照*)。必要に応じて、スキャンを一時的に中断 (***一時停止***) またはキャンセル (***停止***) できます。



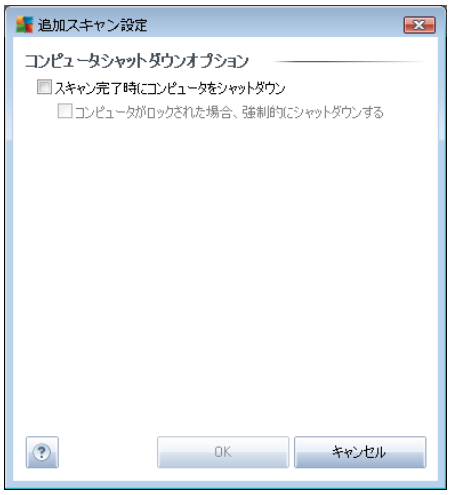

#### スキャン設定編集

***ルートキット対策スキャン***は常に既定の設定で起動し、スキャン パラメータは [***AVG 高度な設定/ルートキット対策***] ダイアログからのみ編集できます。スキャンの実行中に限り、次のスキャン インターフェース設定を利用できます。

- ***自動スキャン*** - スライダを使用して、スキャン処理の優先度を変更します。既定ではこのオプションの値は、自動的にリソースを使用する*ユーザー依存レベルに設定されています*。低速でスキャン処理を実行してシステム リソース負荷

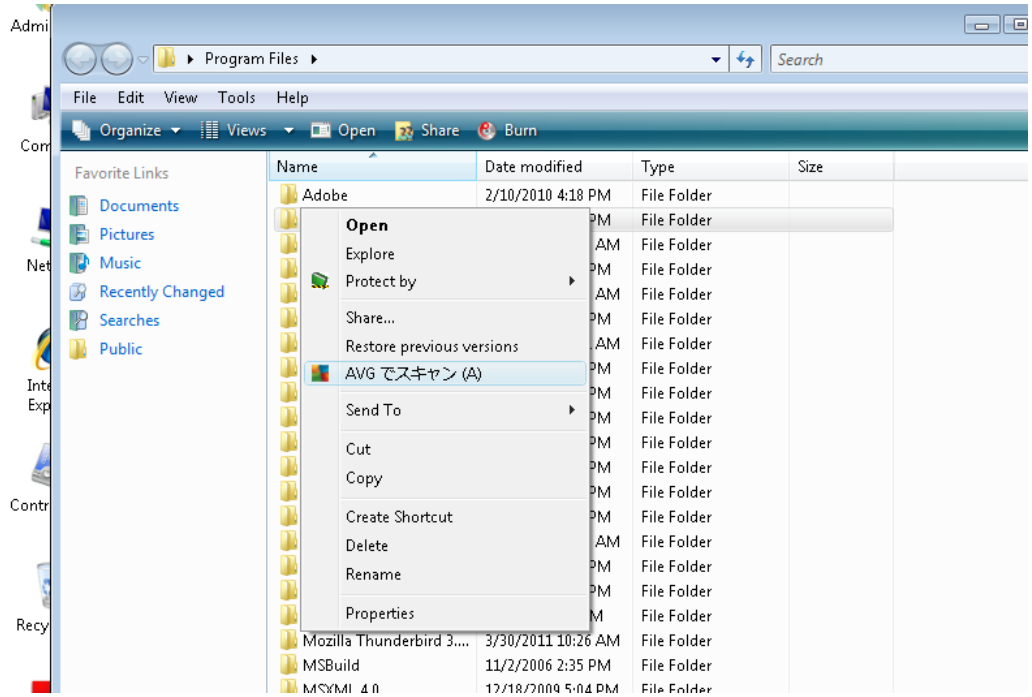
を最小化 (*コンピュータで同時に作業をする必要があり、スキャンに時間がかかってもよい場合に便利です*) したり、システム リソース消費量の高い高速スキャン（*コンピュータが一時的に使用されていない場合などに便利です*）を実行したりできます。

- ***追加のスキャン設定*** - このリンクをクリックすると、新しい [***追加のスキャン設定***] ダイアログが開きます。このダイアログでは、***ルートキット対策スキャン処理に伴うコンピュータ シャットダウンのタイミング*** (***スキャン完了時にコンピュータをシャットダウン****あるいは****コンピュータがロックされた場合は強制シャットダウン***) を定義できます。




## 11.3. シェル拡張スキャン

**AVG Internet Security 2011**では、完全コンピュータ　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。
- [***AVG 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。

## 11.4. コマンドライン スキャン

**AVG Internet Security 2011** ではコマンド ラインからスキャンを実行するときにオプションを利用できます。このオプションはサーバー上のインスタンスに対して利用できます。あるいは、コンピュータのブート後に自動的に起動するバッチ スクリプトを作成するときに利用できます。コマンド ラインからスキャンを起動するときには、AVG のグラフィカル ユーザー インターフェースで提供されるほとんどのパラメータを使用できます。

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

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

### コマンドの構文

コマンドの構文は次のとおりです。

- ***avgscanx /パラメータ*** ... たとえば、完全コンピュータ スキャンの場合 ***avgscanx /comp***

- ***avgscanx /パラメータ /パラメータ*** .. 複数のパラメータを使用する場合、パラメータを 1 行に並べ、スペースとスラッシュで区切る必要があります。

- パラメータが特定の値を必要とする場合 (例: ***/scan*** パラメータには選択した場所への正確なパスを指定する必要があります) は、値をセミコロンで区切る必要があります。例: ***avgscanx /scan=C:\,D:***

## スキャン パラメータ

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

スキャンを実行するには、[***Enter***] を押します。スキャン中は ***Ctrl+C*** または ***Ctrl+Pause*** を押して処理を停止できます。

## グラフィック インターフェースから起動する 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 スキャンを実行することもできます。スキャン自体はコマンド ラインから実行されます。[***コマンド ライン コンポーサー***] ダイアログでは、便利なグラフィック インターフェースでは大部分のスキャン パラメータを指定できます。

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

### 11.4.1. CMD スキャン パラメータ

以下は、コマンドラインスキャンで利用可能なすべてのパラメータです。

- ***/SCAN*** 特定のファイルまたはフォルダのスキャン /SCAN=パス;パス（例：/SCAN=C:\;D:\）
- ***/COMP*** 完全コンピュータ スキャン
- ***/HEUR*** ヒューリスティック分析の使用
- ***/EXCLUDE*** スキャンからパス、またはファイルを除外
- ***/@*** コマンドファイル /file name/
- ***/EXT*** これらの拡張子をスキャンする /例えば、 EXT=EXE,DLL/

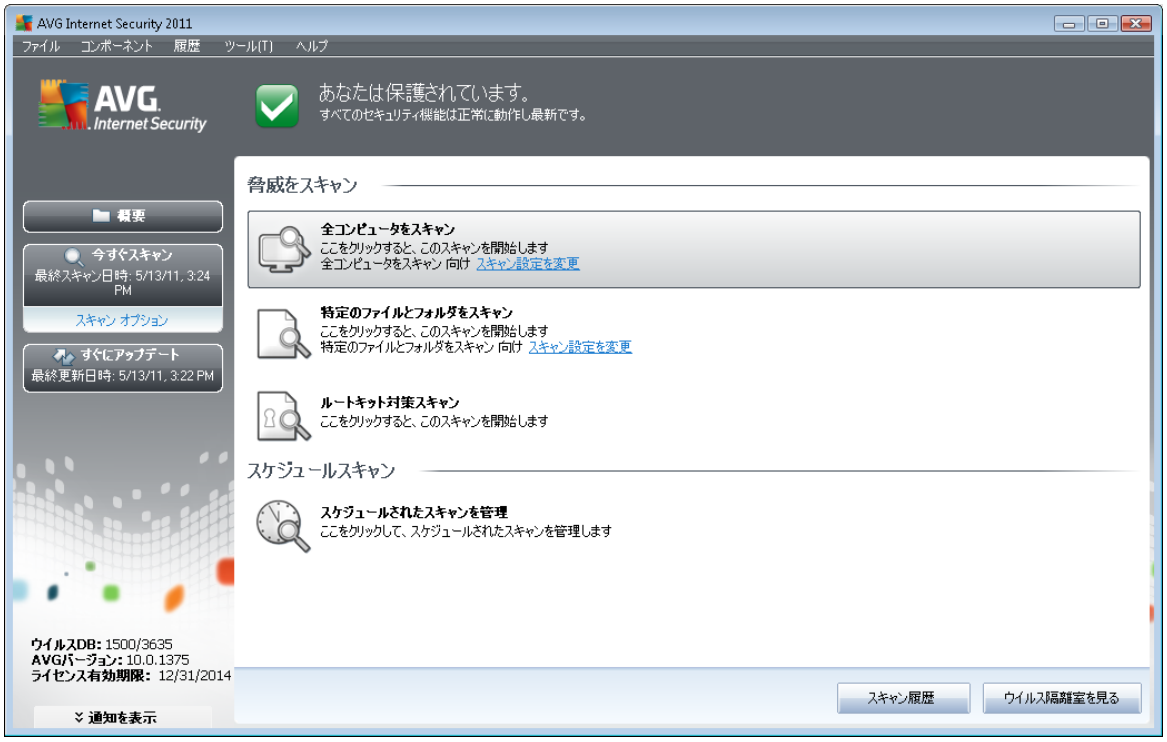
- ***/NOEXT*** これらの拡張子をスキャンしない /例えば、 NOEXT=JPG/
- ***/ARC*** アーカイブをスキャン
- ***/CLEAN*** 自動的駆除
- ***/TRASH*** 感染ファイルをウイルス隔離室に移動
- ***/QT*** クイックスキャン
- ***/MACROW*** マクロを報告する
- ***/PWDW*** パスワード保護されたファイルを報告する
- ***/IGNLOCKED*** ロックされたファイルを無視
- ***/REPORT*** ファイルにレポート/file name/
- ***/REPAPPEND*** レポートファイルに追加
- ***/REPOK*** 未感染ファイルを「OK」として報告する
- ***/NOBREAK*** CTRL-BREAKで中断しない
- ***/BOOT*** MBR/BOOT チェックを有効化
- ***/PROC*** アクティブプロセスをスキャンする
- ***/PUP*** 「不審なプログラム」を報告する
- ***/REG*** レジストリをスキャンする
- ***/COO*** cookieをスキャンする
- ***/?*** このトピックに関するヘルプを表示
- ***/HELP*** このトピックに関するヘルプを表示
- ***/PRIORITY*** スキャン優先度 (低、自動、高) を設定 (高度な設定 / Scans を参照)
- ***/SHUTDOWN*** スキャン完了時にコンピュータをシャットダウン
- ***/FORCESHUTDOWN*** スキャン完了時にコンピュータを強制シャットダウン
- ***/ADS*** Alternate Data Streams をスキャン(NTFSのみ)
- ***/ARCBOMBSW*** 再圧縮されたアーカイブ ファイルを報告

## 11.5. スキャン スケジュール

**AVG Internet Security 2011** では、オンデマンドで (ウイルスに感染した場合など) 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お勧めします。この方法を採用すること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。

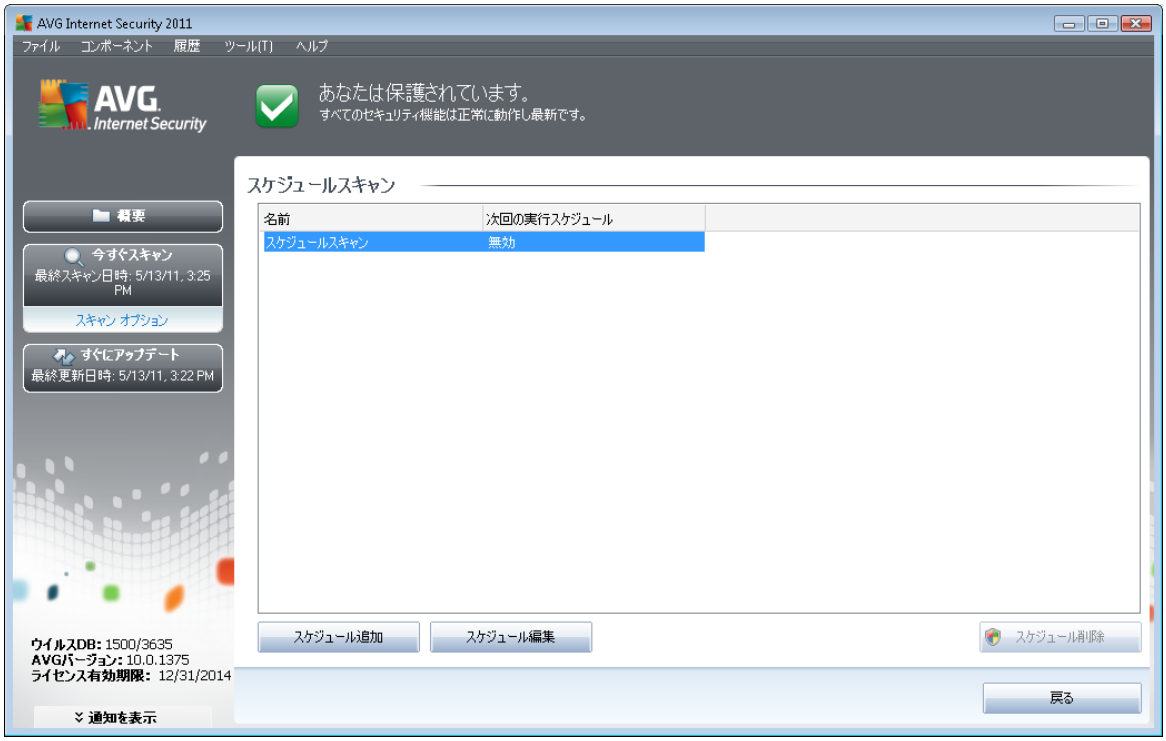
***完全コンピュータ スキャン***を週に 1 度以上定期的に実行することをお勧めします。ただし、可能な場合は、コンピュータのスキャンを毎日実行してください。既定のスキャン スケジュールはこのように設定されています。コンピュータが常にオンとなっている場合、作業時間外にスキャンを実行するよう設定することができます。コンピュータがオフになっていたためスケジュールが実行されなかった場合に備えて、コンピュータの起動時にスキャンを実行するようにスケジュールを設定します。

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




### スケジュール スキャン

[***スキャンのスケジュール***] セクションのグラフィカルなアイコンをクリックすると、新しい [***スキャンのスケジュール***] ダイアログが開き、現在スケジュールされているすべてのスキャンの一覧が表示されます。

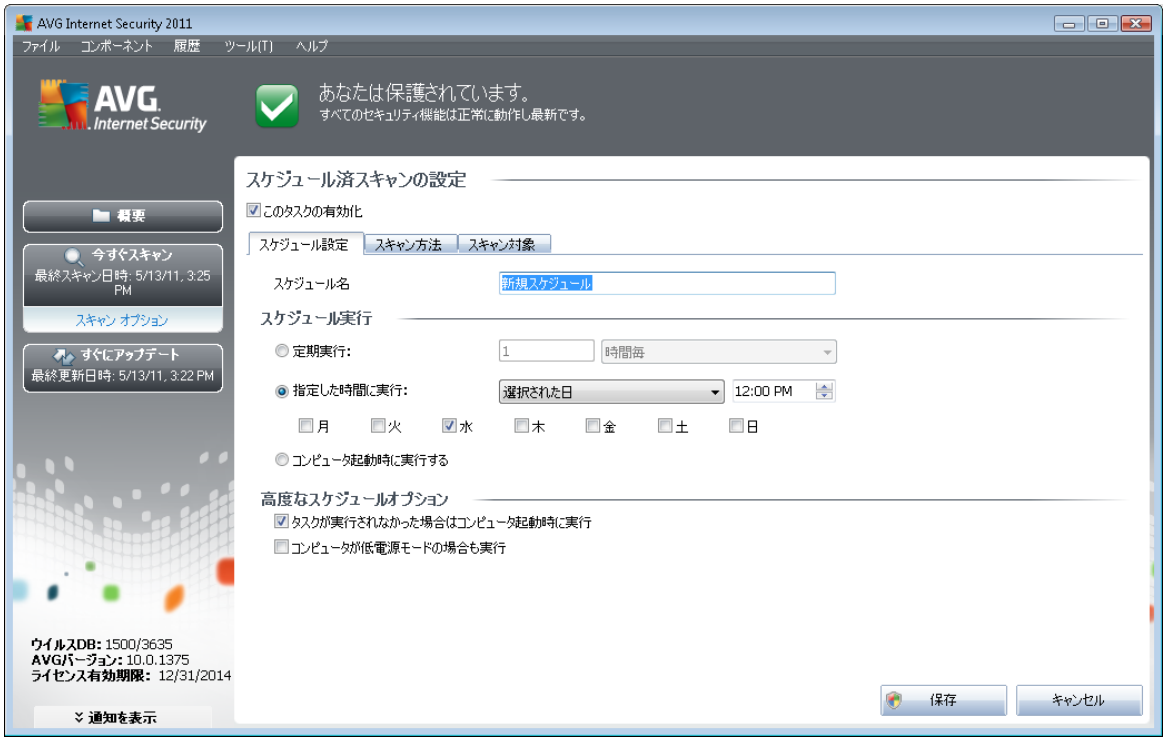



次のコントロール ボタンを使用して、スキャンの編集および追加ができます。

- ***スキャン スケジュールの追加*** - [***スケジュール スキャン設定***] ダイアログの [***スケジュール設定***] タブを開きます。このダイアログでは、スキャン パラメータを指定できます。
- ***スキャン スケジュールの編集*** - スケジュール スキャンの一覧から既存のスキャン スケジュールを選択した場合にのみこのボタンを使用できます。このボタンをクリックすると、[***スケジュール スキャン設定***] ダイアログの [***スケジュール設定***] タブが表示されます。選択したスキャンのパラメータがこのタブで指定され、編集できます。
- ***スキャン スケジュールの編集*** - スケジュール スキャンの一覧から既存のスキャン スケジュールを選択した場合にのみこのボタンを使用できます。コントロール ボタンをクリックすると、選択したスキャンを一覧から削除できます。ただし、自分で作成したスケジュールのみを削除できます。既定で定義されている***完全コンピュータ スキャン スケジュール***は削除できません。
- ***戻る*** - AVG スキャン インターフェースに戻ります

### 11.5.1. スケジュール設定

新しい検査と定期実行をスケジュールする場合、[***スケジュール済みの検査の設定***] ダイアログ *([スキャンのスケジュール]* ***ダイアログで*** *[****スキャン スケジュールの追加****]* *ボタンをクリック)* を入力します。このダイアログは 3 つのタブに分けられます。***スケジュール設定****- 以下の図を参照（自動的にリダイレクトされるデフォルトタブ）、****スキャン方法****、****スキャン対象***




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

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

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

このダイアログでは、さらに以下のスキャンパラメータを定義します。

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

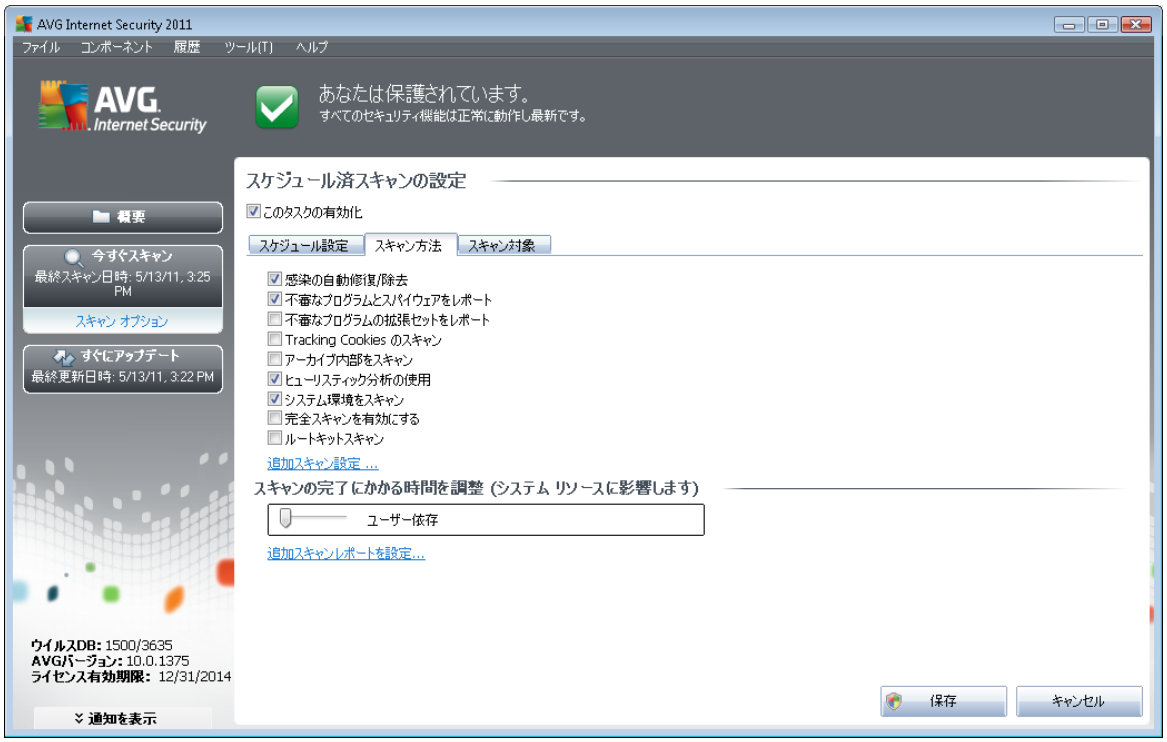
## スケジュール済スキャンダイアログのコントロールボタン

スケジュール済のスキャンの設定***ダイアログのすべてのタブ（***スケジュール設定、スキャン方法、スキャン対象***）には2つのコントロールボタンがあり、***これらは同一の機能を持っています。

- ***保存*** - このタブまたはこのダイアログのその他のタブで行ったすべての変更を保存し、AVG スキャン インターフェースの既定のダイアログに戻ります。したがって、すべてのタブでスキャン パラメータを設定する場合、すべての必要項目を指定した後でこのボタンをクリックしてください。

- ***キャンセル*** - このタブまたはこのダイアログのその他のタブで行ったすべての変更をキャンセルし、AVG スキャン インターフェースの既定のダイアログに戻ります。

## 11.5.2. スキャン方法




[***スキャン方法***] タブには、任意でオン/オフを切り替えられるスキャン パラメータの一覧が表示されます。既定ではほとんどのパラメータがオンになっており、その機能はスキャン実行中に適用されます。やむを得ない理由がない場合は、あらかじめ定義された設定を保持することを推奨します。

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

- ***不審なプログラムとスパイウェア脅威を報告する***(*既定ではオン*): チェック

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

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

- ***Tracking Cookie をスキャンする*** (*既定ではオフ*): ***スパイウェア対策コンポーネント***のこのパラメータを定義すると、スキャン実行中に Cookie を検出します *'HTTP cookie は、サイトの設定や電子ショッピング カートの内容など、ユーザー固有の情報の認証、追跡、メンテナンスに使用されます*)。

- ***アーカイブの内容をスキャンする*** (*既定ではオン*): このパラメータを定義すると、ファイルが ZIP や RAR などのアーカイブ形式で圧縮されている場合でも、すべてのファイルに対してスキャン チェックを実行します。

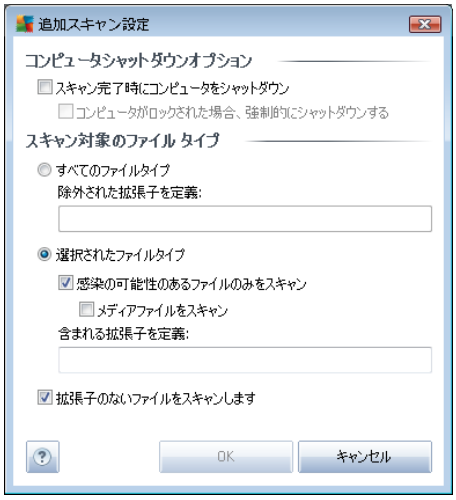
- ***ヒューリスティック分析を使用する*** (*既定ではオン*): ヒューリスティック分析 (*仮想コンピュータ環境で実行されるスキャン対象オブジェクト命令の動的エミュレーション*) は、スキャン実行中に採用されるウイルス検出方法の 1 つです。

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

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

次の方法でスキャン設定を変更できます。

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




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

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

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

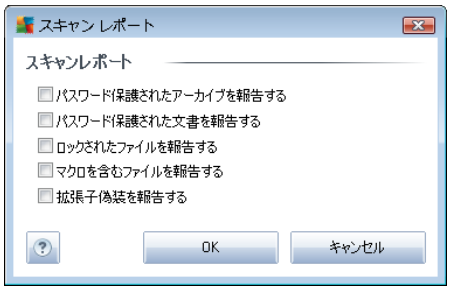
  - ***選択したファイル タイプ*** - 感染の可能性のあるファイルのみを指定できます (*一部のプレーン テキスト ファイルやその他の非実行可能ファイル*など感染の可能性がないファイルはスキャンされません)。これには、メディア ファイル (*ビデオ、オーディオ ファイル*) が含まれます。 多くの場合、このようなファイルはサイズが非常に大きく、ウィルスに感染している可能性が非常に低いため、このボックスのチェックを外すと、スキャン時間がさらに短縮されますここでも、必ずスキャンするファイルの拡張子を指定できます。

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

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

*場合などに便利です*）を実行したりできます。

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




***メモ:*** *既定ではスキャンは最適なパフォーマンスで実行されるように設定されています。やむを得ない理由がない場合は、あらかじめ定義された設定を保持することを強くお勧めします。設定変更は上級者ユーザーが行ってください。その他のスキャンの設定オプションについては、[****ファイル/高度な設定****] システム メニュー項目からアクセスできる[****高度な設定****] ダイアログを参照してください。*

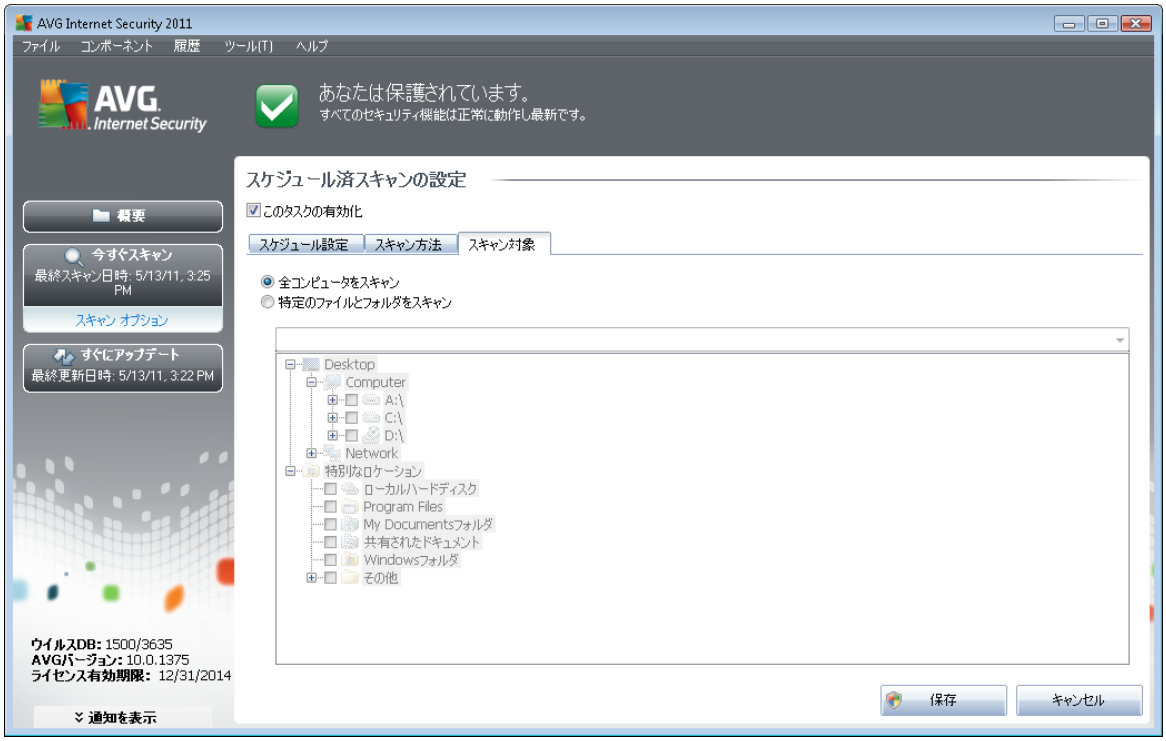
## コントロール ボタン

[***スケジュール スキャンの設定***] ダイアログのすべてのタブ (***スケジュール設定***、***スキャン方法***、***スキャン対象***) には 2 つのコントロール ボタンがあり、これらは同一の機能を持っています。

- ***保存*** - このタブまたはこのダイアログのその他のタブで行ったすべての変更を保存し、AVG スキャン インターフェースの既定のダイアログに戻ります。したがって、すべてのタブでスキャン パラメータを設定する場合、すべての必要項目を指定した後でこのボタンをクリックしてください。

- ***キャンセル*** - このタブまたはこのダイアログのその他のタブで行ったすべての変更をキャンセルし、AVG スキャン インターフェースの既定のダイアログに戻ります。

### 11.5.3. スキャン対象




[***スキャン対象***] タブでは、[完全コンピュータ スキャン] あるいは [特定のファイルやフォルダのスキャン] のいずれかを定義できます。

特定のファイルまたはフォルダのスキャンを選択する場合は、このダイアログの下部に表示されるツリー構造がアクティブになり、スキャンするフォルダを選択できます (*スキャンするフォルダが見つかるまでプラス ノードをクリックして項目を展開します*)。各ボックスにチェックを付けることで複数のフォルダを選択できます。選択し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ます。選択したスキャン履歴はドロップダウン メニューに保持されるため、後から使用できます。任意のフォルダへの完全パスを手入力することもできます (*複数パスを入力する場合は、スペースを入れずセミコロンで区切る必要があります*)。

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

- ***ローカル ハード ドライブ*** - コンピュータのすべてのハード ドライブ
- ***プログラム ファイル***
    - C:\Program Files\
    - *64 ビット バージョン* C:\Program Files (x86)
- ***マイ ドキュメント フォルダ***

- *Win XP:* C:\Documents and Settings\Default User\My Documents\
- *Windows Vista/7*: C:\Users\user\Documents\

- ***共有ドキュメント***
  - *Win XP*: C:\Documents and Settings\All Users\Documents\
  - *Windows Vista/7*: C:\Users\Public\Documents\

- ***Windows フォルダ*** - C:\Windows\

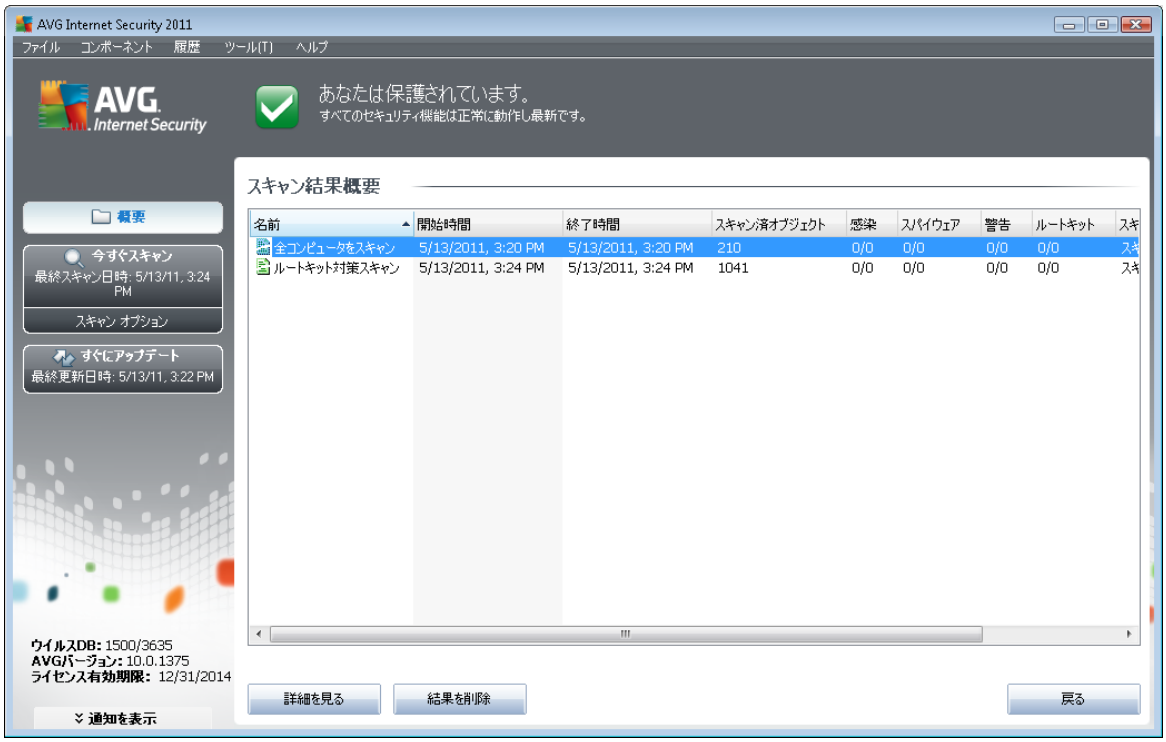
- ***その他***
  - *システム ドライブ* - オペレーティング システムがインストールされているハードドライブ (通常は C:)
  - *システム フォルダ* - C:\Windows\System32\
  - *一時ファイル フォルダ* - C:\Documents and Settings\User\Local\ (*Windows XP*); or C:\Users\user\AppData\Local\Temp\ (*Windows Vista/7*)
  - *一時インターネット ファイル* - C:\Documents and Settings\User\Local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

## スケジュール スキャン ダイアログのコントロール ボタン

[***スケジュール スキャンの設定***] ダイアログのすべてのタブ (***スケジュール設定***、***スキャン方法***、***スキャン対象***) には 2 つのコントロール ボタンがあり、これらは同一の機能を持っています。

- ***保存*** - このタブまたはこのダイアログのその他のタブで行ったすべての変更を保存し、AVG スキャン インターフェースの既定のダイアログに戻ります。したがって、すべてのタブでスキャン パラメータを設定する場合、すべての必要項目を指定した後でこのボタンをクリックしてください。
- ***キャンセル*** - このタブまたはこのダイアログのその他のタブで行ったすべての変更をキャンセルし、AVG スキャン インターフェースの既定のダイアログに戻ります。

## 11.6. スキャン結果概要




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

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

  緑のアイコンはスキャン中に感染が検出されなかったことを示します。

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

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

  各アイコンは完全な形、または半分のアイコンで表示されます。完全な形のアイコンは正常終了したスキャンを示しています。半分になったアイコンはスキャンがキャンセルされたか中断されたことを示しています。

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

- ***開始時間***- スキャンが実行された日時
- ***終了時間***- スキャンが終了した日時
- ***スキャン済オブジェクト***- スキャンでチェックされたオブジェクトの数
- ***感染***- 検出/除去されたウイルス感染の数
- ***スパイウェア***- 検出/除去されたスパイウェアの数
- ***警告*** - 検出された不審なオブジェクト
- ***ルートキット*** - 検出されたルートキット
- ***スキャンログ情報***- スキャン過程と結果に関する情報（一般的には完了か中断かの情報）

**コントロールボタン**

***スキャン結果概要***ダイアログには、以下のコントロールボタンがあります。

- □□□□□ - クリックすると、[***スキャン結果***] ダイアログに切り替わり、選択したスキャンの詳細データを表示します。
- ***結果を削除*** - クリックすると、スキャン結果概要から選択したアイテムを削除します。
- ***戻る***- AVGスキャンインターフェースのデフォルトダイアログに切り替わります。

## 11.7. スキャン結果詳細

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

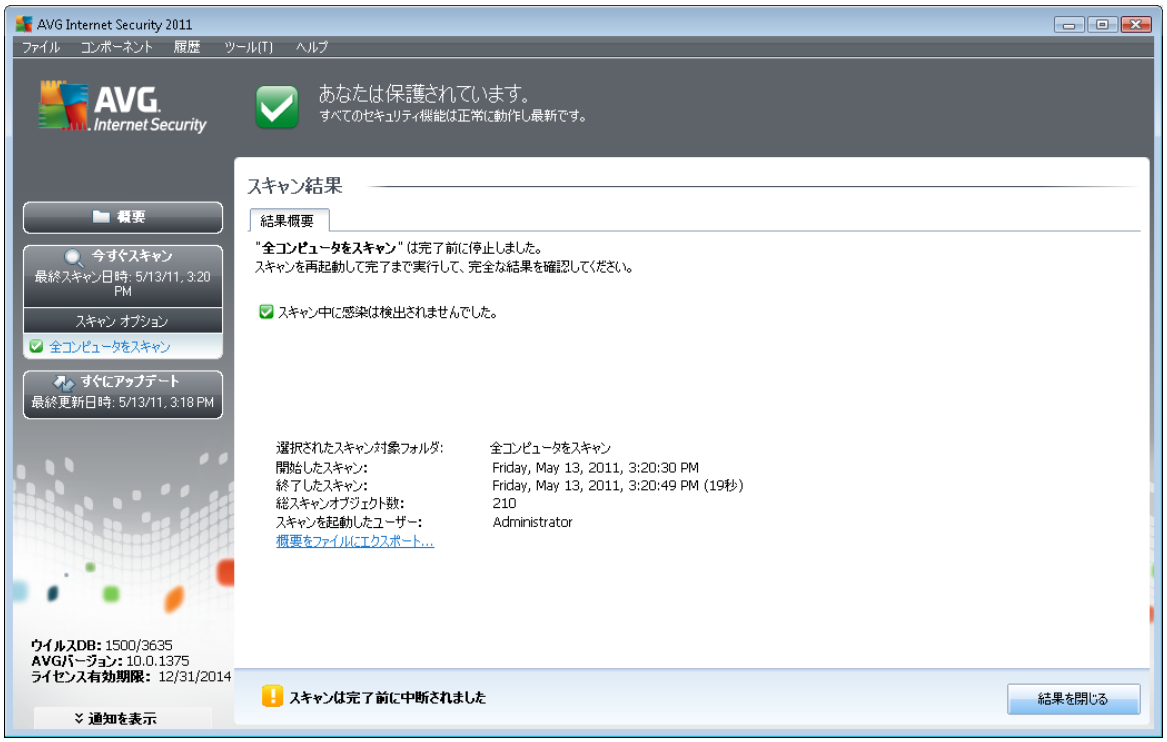
このダイアログはさらにいくつかのタブに分けられます。

- ***結果概要*** - このタブは常に表示され、スキャン進捗を示す統計データが表示されます。
- ***感染*** - このタブは、スキャン実行中にウイルス感染が検出された場合にのみ表示されます。
- ***スパイウェア*** - このタブは、スキャン実行中にスパイウェアが検出された場合にのみ表示されます。
- ***警告*** - Cookie がスキャン中に検出されると、このタブがインスタンスごとに表示されます。

- ***ルートキット*** - このタブは、スキャン実行中にルートキットが検出された場合にのみ表示されます。

- ***情報*** - このタブは潜在的な脅威が検出され、これらが上記のいずれのカテゴリにも分類できない場合にのみ表示されます。このタブでは警告メッセージが表示されます。また、スキャンできなかったオブジェクトに関する情報も表示されます (パスワード保護されたアーカイブなど)。

### 11.7.1. 結果概要タブ




***スキャン結果***タブには、以下の情報に関する詳細な統計が表示されます。

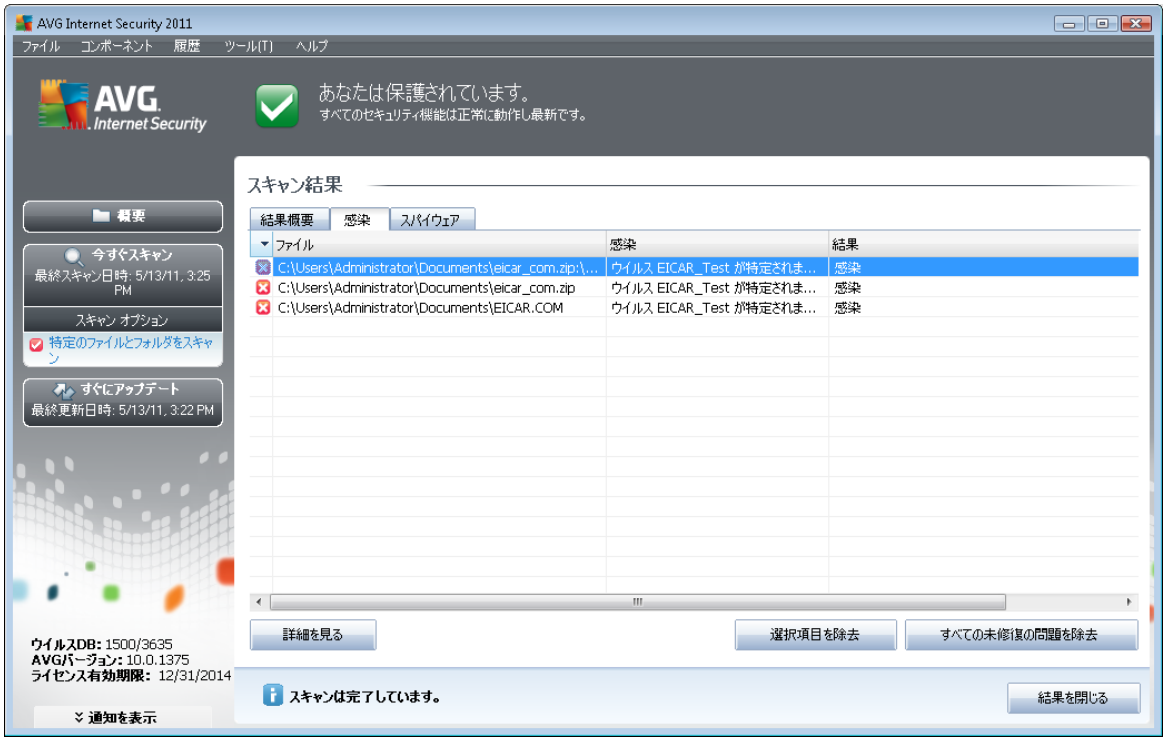
- 検出されたウイルス感染/スパイウェア
- 除去されたウイルス感染/スパイウェア
- 除去あまたは修復不可能なウイルス感染/スパイウェア数

また、スキャン開始の正確な日時、スキャンされたオブジェクトの合計数、スキャン期間、スキャン実行中に発生したエラー数に関する情報も表示されます。

#### コントロールボタン

このダイアログで利用できるコントールボタンは1つです。***結果を閉じる***ボタンを押すと、***スキャン結果概要***ダイアログに戻ります。

### 11.7.2. 感染タブ




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

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

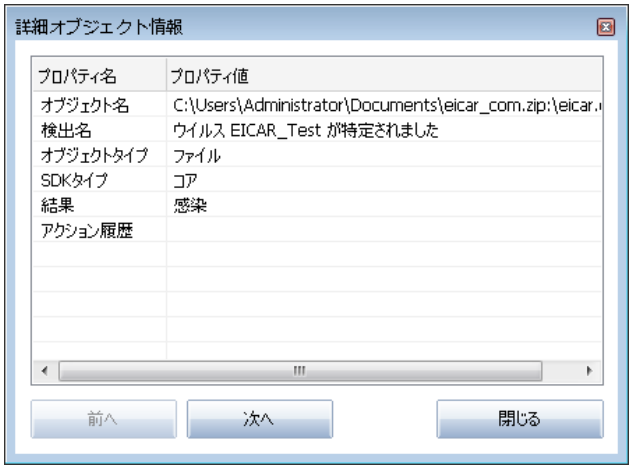
いるため、AVGはスキャンできません。

- o ***潜在的に危険なオブジェクト*** - オブジェクトは潜在的に危険なものとして検出されましたが、感染していません（*例えば、マクロを含む等*）。
- o ***アクションを終了するために再起動を要求*** - 感染オブジェクトを除去できません。完全に除去するには、コンピュータの再起動が必要です。

## コントロールボタン

このダイアログには3つのコントロールボタンがあります。

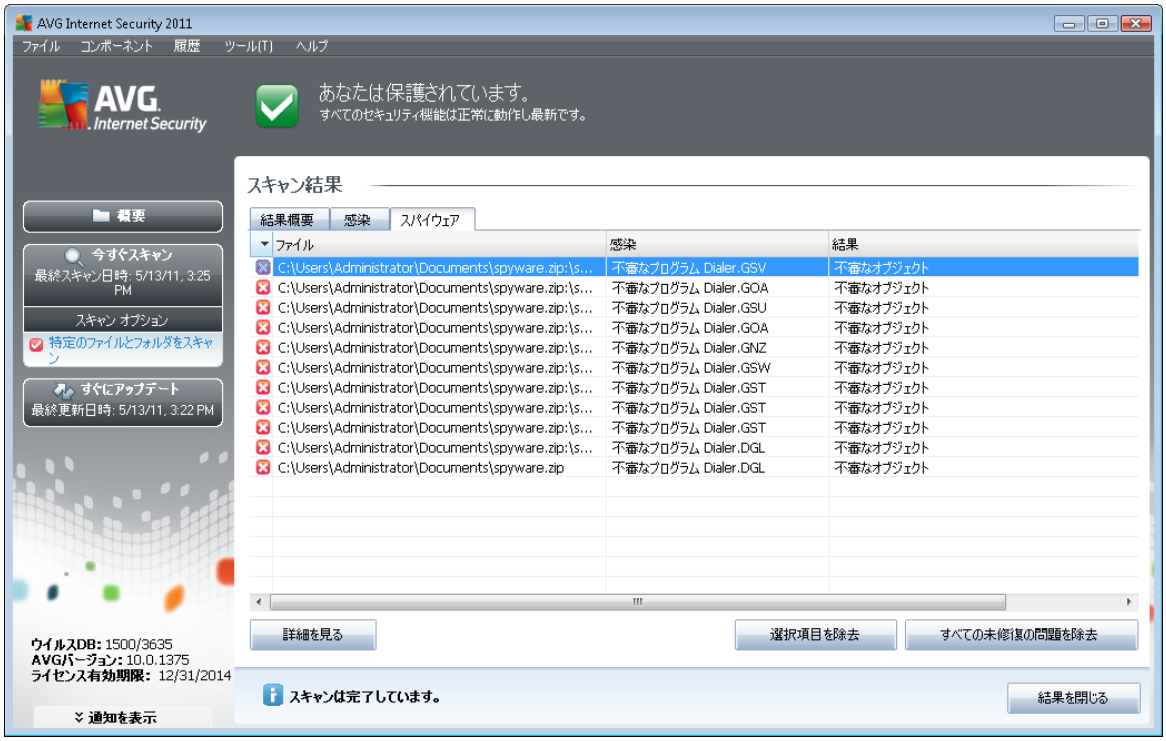
- ***詳細を見る*** - このボタンは [***詳細オブジェクト情報***] という新しいダイアログを開きます。




このダイアログには、検出された感染オブジェクトに関する詳細情報 (*感染したオブジェクト名と場所、オブジェクトの種類、SDK の種類、検出結果、検出されたオブジェクトに関するアクションの履歴など*) が表示されます。***前へ***/***次へ***ボタンを使用して、特定の検出情報を見ることができます。***閉じる***ボタンを使用して、このダイアログを閉じることができます。

- ***選択した感染を除去*** - このボタンをクリックすると、選択した検出を***ウイルス隔離室に移動します***
- ***すべての未修復の感染を削除*** - このボタンはすべての修復不可能な検出や***ウイルス隔離室***
- ***結果を閉じる*** - 詳細情報概要を終了し、***スキャン結果概要***ダイアログに戻ります。

### 11.7.3. スパイウェア タブ




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

- ***ファイル*** - 感染オブジェクトの元の場所へのフルパス
- ***感染*** - 検出されたスパイウェア名 (*特定のウィルスの詳細については、オンラインの****ウィルス エンサイクロペディア***を参照してください)。
- ***結果*** - スキャン中に検出された感染オブジェクトの現在のステータス
  - ***感染*** - 感染オブジェクトが検出され、元の場所に存在します。（例えば、自動修復オプションを特定のスキャン設定でオフにしている場合）
  - ***修復*** - 感染オブジェクトは自動修復され、元の場所に存在しますす。
  - ***ウイルス隔離室に移動*** - 感染オブジェクトは***ウイルス隔離室に移動されました。***
  - ***削除*** - 感染オブジェクトは削除されました。
  - ***PUP例外に追加*** - 検出は例外として評価され、PUP例外リスト（*高度な設定の****PUP例外****ダイアログで設定）に追加されました。*
  - ***ロックされたファイル - 未スキャン*** - 対象オブジェクトはロックされて

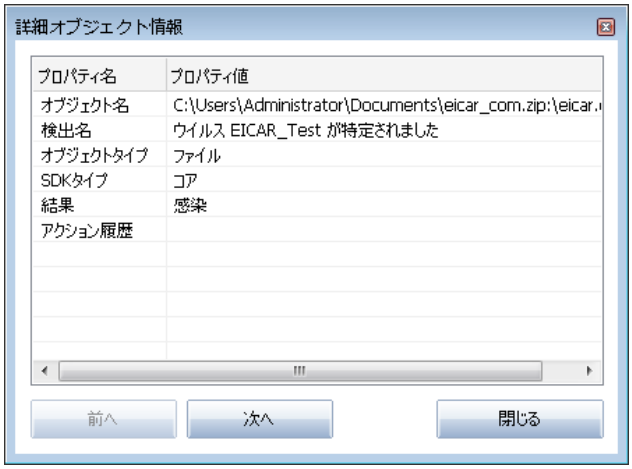
いるため、AVGはスキャンできません。

- ***潜在的に危険なオブジェクト*** - オブジェクトは潜在的に危険なものとして検出されましたが、感染していません（例えば、マクロを含む等）。
- ***アクションを終了するために再起動を要求*** - 感染オブジェクトを除去できません。完全に除去するには、コンピュータの再起動が必要です。

## コントロールボタン

このダイアログには3つのコントロールボタンがあります。

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




このダイアログには、検出された感染オブジェクトに関する詳細情報 (*感染したオブジェクト名と場所、オブジェクトの種類、SDK の種類、検出結果、検出されたオブジェクトに関するアクションの履歴など*) が表示されます。***前へ***/***次へ***ボタンを使用して、特定の検出情報を見ることができます。***閉じる***ボタンを使用して、このダイアログを閉じることができます。

- ***選択した感染を除去*** - このボタンをクリックすると、選択した検出を***ウイルス隔離室に移動します***
- ***すべての未修復の感染を削除*** - このボタンはすべての修復不可能な検出や***ウイルス隔離室***
- ***結果を閉じる*** - 詳細情報概要を終了し、***スキャン結果概要***ダイアログに戻ります。

### 11.7.4. 警告タブ

***警告***タブには、スキャンで検出された「疑わしい」オブジェクトに関する情報（*一般的にはファイル*）が表示されます。***常駐シールド***によって検出された場合は、これらのファイルへのアクセスはブロックされます。この種の検出の一般的な例は、隠され

たファイル、cookie、疑わしいレジストリキー、パスワードで保護されたドキュメント、アーカイブ等です。このようなファイルはコンピュータやセキュリティにとって、何ら直接的な脅威を与えるものではありません。これらのファイルに関する情報は一般的に、コンピュータでアドウェアやスパイウェアが検出される場合に有用です。AVG検査によって警告のみが検出される場合は、何も対応する必要はありません。

このようなオブジェクトに関する最も一般的な例を以下に簡潔に説明しました。

- ***非表示のファイル*** - 非表示のファイルはデフォルトでは、Windows上では見ることができません。あるファイルやその他の脅威はこの属性を持ってファイルを格納することによって検出されることを避けようとする場合があります。AVG で悪意のあるファイルの疑いがある非表示のファイルが報告される場合、***AVG ウイルス隔離室***に移動できます。

- ***Cookies*** - Cookies はウェブサイトによって使用されるプレーンテキストファイルです。これは、後にカスタムウェブサイトレイアウトや予め入力されたユーザー名等をロードするために使用されるユーザー特有の情報を格納するために使用されます。

- ***不審なレジストリキー*** - 一部のマルウェアはその情報を Windows レジストリに格納し、起動時にそれがロードされるようにしたり、それがオペレーティングシステムにまで影響するようにします。

### 11.7.5. ルートキット タブ

***ルートキット対策スキャン***を実行した場合、[***ルートキット***] タブには、スキャン中に検出されたルートキットに関する情報が表示されます。

***ルートキット***は、システムの所有者や正式な管理者の許可なくコンピュータ 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。ルートキットはハードウェア上で実行されているオペレーティング システムを乗っ取ることを目的としているため、ハードウェアへのアクセスが必要になることはほとんどありません。一般的には、ルートキットは標準のオペレーティング システムのセキュリティ メカニズムを破壊したり回避したりすることによって、システム上でその存在を隠しながら動作します。一般的に、ルートキットはトロイの木馬の一種でもあり、システムで実行しても安全であるかのように見せかけてユーザーを騙し、信じこませます。このような技術によって、プログラム監視の対象にならないように実行中のプロセスが隠されたり、オペレーティング システムからファイルやシステム データが隠されることもあります。

このタブの基本構成は [***感染***] タブや [***スパイウェア***] タブと同じです。

### 11.7.6. 情報タブ

***情報***タブには、感染、スパイウェア等と分類できない「検出」に関するデータが表示されます。それらは危険なものと断定はされませんが、注意する価値はあります。AVG スキャンは、感染していない可能性があるが、疑わしいファイルを検出することができます。このようなファイルは***警告***か***情報***として報告されます。

重大度***情報***は次の理由のいずれかで報告されます。

- ***ランタイムパック*** - このファイルは、少ない共通ランタイムパッカーのいずれ

かで圧縮されており、このようなファイルのスキャンを防ぐ試みを示している可能性があります。ただし、このようなファイルの報告のすべてがウイルスを示唆しているわけではありません。

- ***ランタイムパック再帰*** - 上記と同様ですが、共通ソフトウェア間の頻度は低くなります。このようなファイルは疑わしく、分析のためファイルの除去または提出を考える必要があります。

- ***パスワード保護されたアーカイブまたは文書*** - パスワード保護されたファイルは AVG（*あるいは一般的にはその他のウイルスソフトウェア*）でスキャンできません。

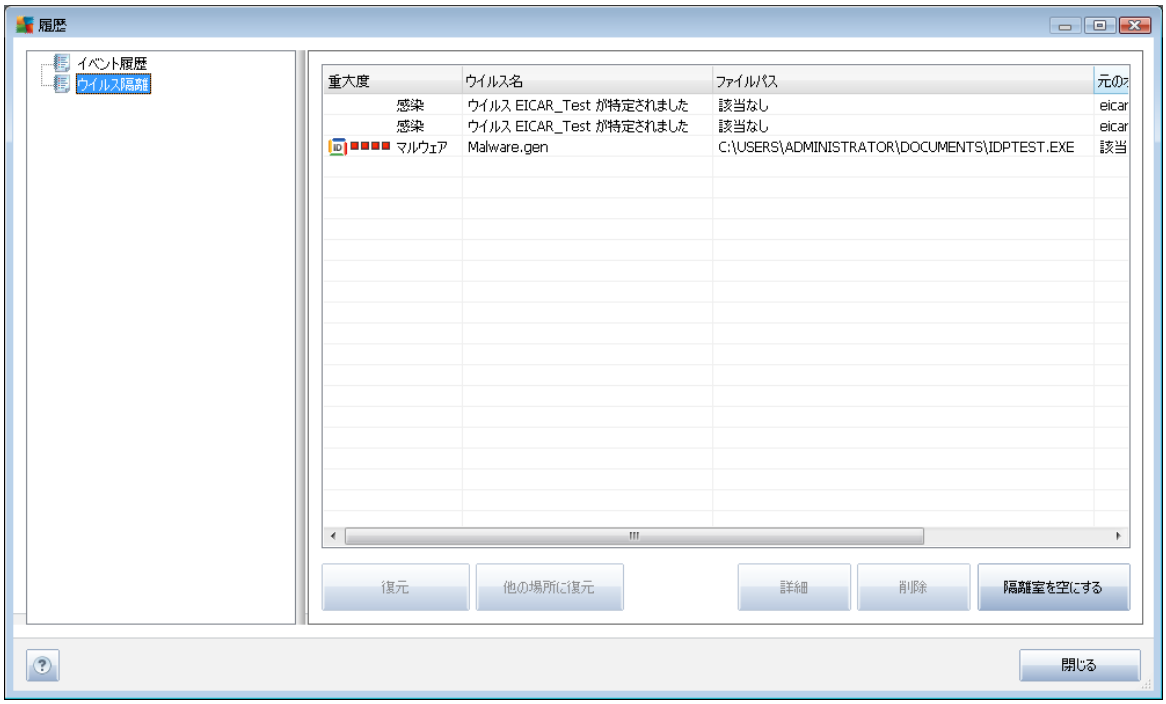
- ***マクロを含んだ文書*** - 報告された文書には、悪意のあるプログラムである可能性があるマクロが含まれます。

- ***拡張子偽装*** - 拡張子偽装のファイルは、画像などのように見える場合がありますが、実際には実行可能形式ファイル（*例：picture.jpg.exe*）です。Windows の既定の設定では、2 番目の拡張子は表示されませんが、AVG はこのようなファイルをレポートし、間違って開いてしまうことを防止します。

- ***不適切なファイルパス*** - 一部の重要なシステムファイルが既定以外のパスで実行中の場合（*例：Windows フォルダ以外で実行中の winlogon.exe*）、AVG はこの不一致を報告します。一部の場合、ウイルスは標準システムプロセス名を使用し、システム内でその存在を目立たなくします。

- ***ロックしたファイル*** - 報告されたファイルはロックされるため、AVG がスキャンできません。これは通常一部のファイルが常にシステムによって使用されていることを意味しています（*例：スワップファイル*）。

## 11.8. ウイルス隔離室




***ウイルス隔離室***は、AVGスキャン中に検出された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***インターフェースは別ウィンドウで開き、隔離された感染オブジェクトに関する情報概要が表示されます。

- ***重大度*** - ***ID 保護*** コンポーネントを**AVG Internet Security 2011**にインストールする場合、問題なし (■□□□) から非常に危険 (■■■■) までの 4 レベルの検出重大度がグラフィカルにこのセクションに表示されます。感染タイプ情報 (*感染レベルに基づいて、リストに表示されているすべてのオブジェクトは実際に感染しているか感染の可能性があります*) も表示されます。

- ***ウィルス名*** - ***ウィルス エンサイクロペディア***（オンライン）に従って、検出された感染名を指定します。

- ***ファイル パス*** - 検出された感染ファイルへの完全パス

- ***元のオブジェクト名*** - 一覧表示されているすべての検出されたオブジェクトは、スキャン処理中に AVG によって指定される標準名で表示されます。オブジェクトに既知の特定の元の名前があった場合 (*例: 添付ファイルの実際の内容*

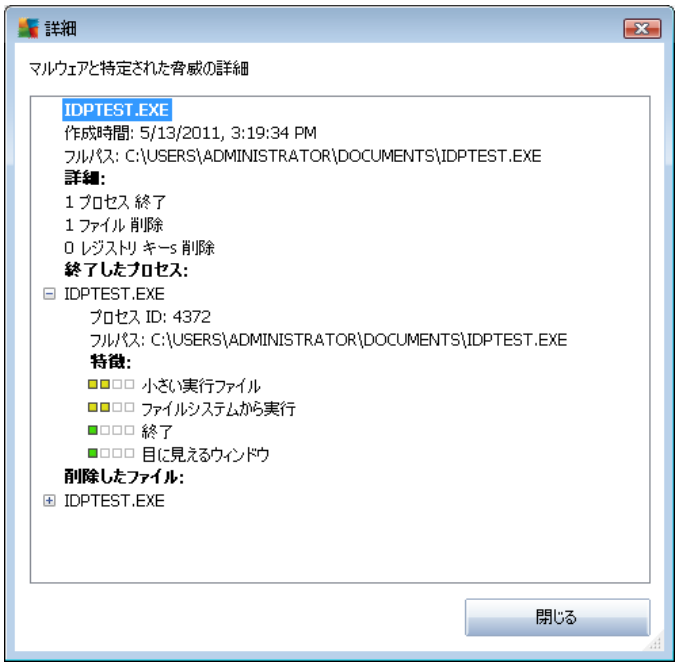
*に対応しないメール添付ファイル名*)、この名前がこの列に表示されます。

- ***保存日*** - 不審なファイルが検出され、***ウイルス隔離室***

## 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。
- ***詳細*** - このボタンは、***ID 保護***で検出された脅威にのみ適用されます。クリックすると、*脅威の詳細の概要 (影響するファイルやプロセス、プロセスの特性など) が表示されます。*). IDP で検出されるその他のすべての項目では、このボタンはグレイ表示になり無効です。




- ***削除*** - 感染ファイルを***ウイルス隔離室***から完全に削除し、元に戻すことはできません。
- ***空にする*** - すべての***ウイルス隔離室***内のファイルを 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. AVG 更新

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

AVG 更新は定期的なスケジュールではリリースされませんが、新しい脅威の数と重要度を考えると、最低でも毎日新しいアップデートを確認することをお勧めします。この方法でのみ **AVG Internet Security 2011** が一日中最新の状態であることを保証できます。

## 12.1. 更新レベル

AVG は、2 つの選択可能なアップデートレベルを提供します。

- ***定義アップデート***には信頼できるウィルス対策保護に必要な変更が含まれます。通常、コードの変更は含まれず、定義データベースのみを更新します。この更新が提供され次第、すぐに適用する必要があります。
- ***プログラム更新***には、各種プログラム変更、修正、改良点が含まれています。

更新をスケジュールするときには、ダウンロードと適用の優先レベルを選択できます。

***メモ:*** *スケジュール プログラム更新の時間がスケジュール スキャンの時間と同じになった場合は、更新処理が最優先され、スキャンは中断されます。*

## 12.2. 更新タイプ

2 種類の更新があります。

- ***オンデマンド更新***は、必要に応じていつでも実行できる即時 AVG 更新です。
- ***スケジュール更新*** - AVG では更新計画を事前に設定することも可能です。スケジュール更新は設定に従って定期的に実行されます。新しい更新ファイルが特定の場所にある場合、インターネットから直接ダウンロードされます。あるいは、ネットワーク ディレクトリを介してダウンロードされます。新しい更新がない場合は何も実行されません。

## 12.3. 更新処理

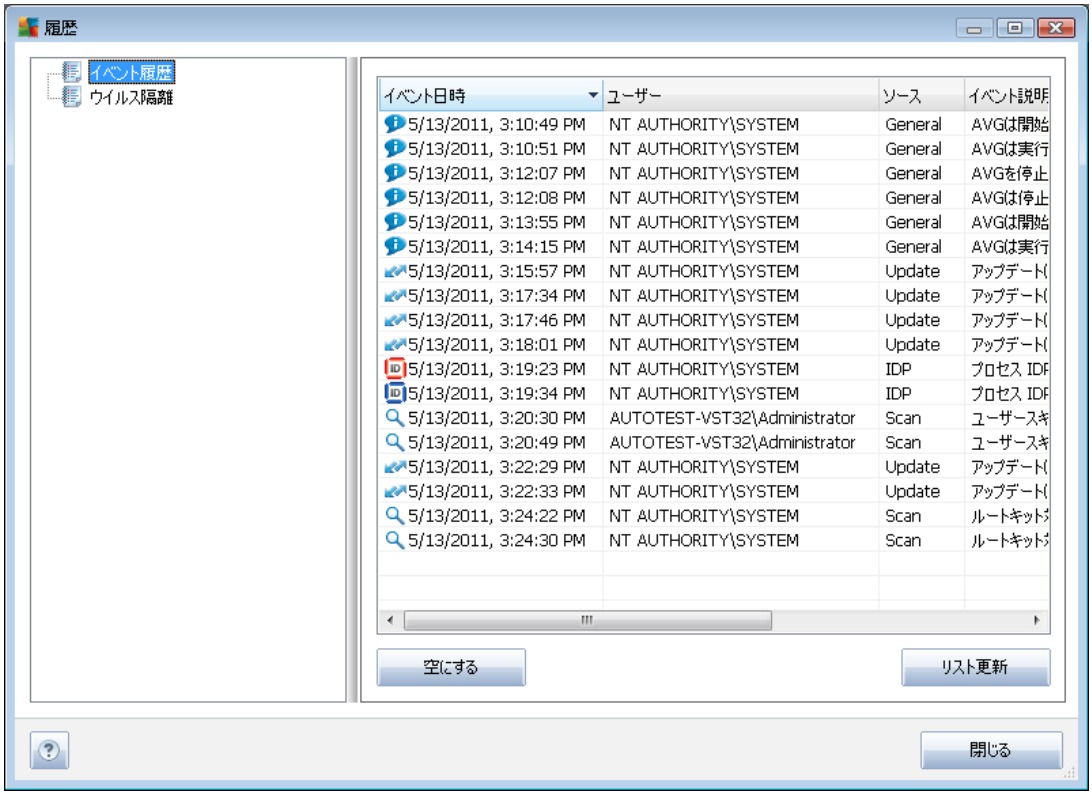
***すぐにアップデート***クイックリンクによって、アップデートプロセスをすぐに実行できます。このリンクは、AVGユーザーインターフェースダイアログからいつでも使用可能です。ただし、アップデートマネージャコンポーネントのアップデートスケジュール編集で説明されているように、定期的にアップデートを実行することが強く推奨されます。

アップデートを開始すると、AVGはまず利用可能な新しいアップデートファイルがあるかどうかを確認します。この場合、AVGはダウンロードを開始し、アップデートプロセスが実行されます。アップデートプロセス中は、***アップデート***インターフェースにリダイレクトされます。ここでは、グラフィカルな表示や関連統計パラメータの概要で処理の状況を見ることができます（*アップデートファイルサイズ、受信データ、ダ*

*ウンロード速度、経過時間等*）。

***注意***：*AVGプログラムアップデートの前に、システム復旧ポイントが作成されます。アップデートプロセスが失敗し、オペレーティングシステムがクラッシュする場合には、必ずこのポイントから元のコンフィグレーションでOSを復旧できます。このオプションは、スタート/プログラム/アクセサリ/システムツール/システムの復元からアクセスできますが、上級ユーザーのみが変更を行うことをお勧めします。*

# 13. イベント履歴




[***イベント履歴***] ダイアログには、システム メニューの [履歴/イベント履歴ログ] 項目からアクセスできます。このダイアログでは、**AVG Internet Security 2011** 動作中に発生した重要なイベントの概要を確認できます。***履歴***には次の種類のイベントが記録されます。

- AVG アプリケーションの更新情報
- スキャンの開始、終了、停止 (*自動実行スキャンを含む*)
- 発生場所などウィルス検出に関連するイベント (*常駐シールド*または*スキャン*)
- 他の重要イベント

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***は正確なイベント発生日時です。
- ***ユーザー***はイベントを開始したユーザーです。
- ***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 AVG システムの一部です。

- ***イベント説明***は実際の動作の簡単な概要です。

**コントロールボタン**

- ***空にする***- すべてのイベントリストエントリを削除します
- ***リスト更新*** - イベントリストエントリをすべて更新します

# 14. FAQ とテクニカル サポート

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

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