Defend what you create

管理者ガイド

Dr.Web Anti-virus for Windows servers
バージョン7.0
管理者ガイド
17.09.2012

ロシア本社
2-12A, 3rd str. Yamskogo polya
Moscow, Russia
125124

ウェブサイト www.drweb.com
電話 +7 (495) 789-45-87

リージョナルオフィスに関しては、弊社オフィシャルサイトをご覧ください

Doctor Web, Ltd.

弊社はマルウェアおよび迷惑メールに対する効率的な保護を提供するDr.Web®情報セキュリティソリューションの開発および販売を行っています。

個人ユーザから政府機関、また中小企業から国際的な企業まで、世界中のあらゆる地域に弊社のお客様は広がっています。

Dr.Webアンチウイルスソリューションは1992年以来、卓越したマルウェアの検出能力と国際的な情報セキュリティ基準への適合で良く知られています。

Dr.Webソリューションには政府による認証や表彰が何度も与えられていること、また弊社製品のユーザが世界中に広がっていることは、弊社製品に対する皆さまからの絶大な信頼の証しだと自負しています。

お客様の多大なるご支援とご貢献に
心より感謝いたします。

目次

チャプター1 はじめに

Dr.Web Anti-virus for Windows servers はウイルス、ルートキット、トロイの木馬、スパイウェア、アドウェア、ハッカーユーティリティー、およびその他悪意のあるプログラムからRAM、ハードディスク、リムーバブルメディアを多角的に保護します。最大の 特徴 は **Dr.Web Anti-virus for servers** のモジュールの構造です。全てのコンポーネントとOSにおいて共通のアンチウイルスエンジンおよびアンチウイルスデータベースを使用します。現在では、Windows向け**Dr.Web 製品** に加えてIBM® OS/2®、Novell® NetWare®、Macintosh®、Microsoft Windows Mobile®、 Andorid®、 Symbian®、またいくつかのUnix®系のシステム（Linux®、FreeBSD®など）向けアンチウイルスがあります。

Dr.Web Anti-virus for servers はインターネット経由で簡単かつ効率的にデータベース・ソフトウェアコンポーネントの更新を行います。

Dr.Web Anti-virus for servers は、様々な望ましくないプログラム（アドウェア、ダイヤラープログラム、ジョークプログラム、リスクウェア、クラッキングツール）を検出し、それに対しアンチウイルスコンポーネントによるアクションを実行します。

Dr.Web Anti-virus for servers に含まれるコンポーネントは以下のとおりです。

- **Dr.Web Scanner for Windows** (**Scanner**) – グラフィックインターフェースを持つアンチウイルススキャナです。このプログラムはユーザーのリクエストまたはスケジュールによって動作し、コンピューターのウイルス検査を行います。コマンドラインでの実行も可能です（**Dr.Webコンソールスキャナfor Windows**）。
- **SpIDer Guard® for Windows** （または **Monitor**、 **Guard**）– メインメモリ内に常駐し、ファイルとメモリの「オンアクセス」検査を行うリアルタイムモニタ機能です。ウイルスと思われる活動を検出します。
- **Dr.Web Updater** – 登録済みユーザーのアンチウイルスデータベースとその他のコンポーネントのファイルを更新・自動インストトールします。
- **SpIDer Agent** – **Dr.Web Anti-virus for servers** のコンポーネントの起動と設定を行うモジュールです。

1.1. このマニュアルについて

この管理者 マニュアルには、**Dr.Web Anti-virus for servers** アンチウイルスプログラムのインストールと効果的な利用方法に関する必要な情報が記載されています。

グラフィックインターフェイス(GUI)に関する詳細な説明は、コンポーネントから起動できる **Dr.Web Anti-virus for servers** のヘルプ内にあります。

この管理者マニュアルには、**Dr.Web Anti-virus for servers** のインストールの詳細説明、プログラムの使用方法、ウイルス脅威による典型的な問題を解決するための方法が記載されています。主に、製品のコンポーネント動作の標準モード(デフォルト設定)について説明されています。

付録 には、上級者ユーザーの為の **Dr.Web Anti-virus for servers** の設定に関する詳細な情報が記載されています。

製品は常に進化しています。プログラムのインターフェースは、このドキュメントの図とは異なる場合があります。現状を反映したマニュアルは http://www.drweb.co.jp/ で常時ご覧いただけます。

1.2. 表記規則

本書では、以下の文字・記号を使用しています。

文字・記号	意味
太字	グラフィカルインターフェース（GUI）の要素の名称や本書のとおり正確に入力する必要のある入力例
緑色の太字	**Doctor Web** 製品またはコンポーネントの名称
緑色で下線付きの文字	本書の他のページや他のWebページへのリンク
固定幅フォント	コマンドラインの入力例、出力例
イタリック体	ユーザーが提供しなければならない情報を表すプレースホルダ。 コマンドラインの入力例がイタリック体の場合は、パラメータ値を示します。
大太字	キーボードのキー名称
プラス記号 ('+')	キーの同時押し（例： ALT+F1 は、ALTキーとF1キーを同時に押すことを意味します。）
感嘆符	重要な注釈、またはエラーなどを引き起こす可能性のある状況に関する警告

本管理者マニュアルでは以下の略語を使用します。

- GUI – Graphical User Interface（グラフィカルユーザーインターフェース、プログラムのGUIバージョン —GUIを使用したバージョン）
- OS – operating system（オペレーティングシステム）
- PC – personal computer（パーソナルコンピューター）
- RAM – Random Access Memory（ランダムアクセスメモリ）

1.3. システム要件

Dr.Web Anti-virus for servers のインストール前には次のことを行って下さい。

- オペレーティングシステムのメーカーが推奨している重要な更新を全てインストールして下さい。
- 他のアンチウイルスの常駐コンポーネントとの非互換性の問題を避けるために、コンピューターから他のアンチウイルスパッケージを削除して下さい。

コンポーネント	要件
OS	次のうちひとつ • Microsoft® Windows® 2000 Server SP4 with Update Rollup 1 • Microsoft® Windows Server® 2003 SP1 • Microsoft® Windows Server® 2008 32ビット、または64ビットのバージョンのオペレーティングシステムがサポートされています。 Microsoftのサイトからいつくかのシステムコンポーネントをダウンロードし、インストールすることが要求される可能性があります。必要に応じてプログラムがその名称とURLを通知します。
ハードディスクの空き領域	**Dr.Web Anti-virus for servers**コンポーネントに200 MB必要です。 インストールの際に作成されるファイルには上記と別に容量が必要になります。
CPU	i686互換
RAM	512MB以上
その他	ウイルスデータベースと**Dr.Web Anti-virus for servers**コンポーネントの更新のためのインターネットへの接続

1.4. ライセンス交付

Dr.Web Anti-virus for servers の使用権限はキーファイルで指定されています。

Dr.Web Anti-virus for servers を使用するにはキーファイルの 取得 および インストール が必要です。

ライセンスおよびキーファイルの種類についての情報は Doctor Web 公式サイト をご覧ください。

1.4.1. キーファイル

キーファイルには以下の情報が含まれています。

- 利用を許可されたコンポーネントの一覧
- アンチウイルスの利用可能期間
- その他の制限（アンチウイルスの利用が許可されたコンピューターの台数など）

キーファイルは .key 拡張子を持ち、デフォルトではプログラムのインストールフォルダにあります。

キーファイルは書込み保護されています。編集されるとキーは無効となりますので編集しないようにしてください。キーファイルを破損する恐れのあるテキストエディタで開くことは推奨できません。

Dr.Web Anti-virus for servers では、ライセンスキーファイルを使用します。このファイルはテクニカルサポートを利用する際にも必要となります。ライセンスキーファイルのパラメータは、ソフトウェア使用許諾契約に従って設定されます。ユーザーと販売会社の情報も含まれています。

キーファイルは、次の条件が同時に満たされている場合に*有効*です。

- ライセンスの有効期限内であること
- **Dr.Web Anti-virus for servers** に必要な全てのアンチウイルスポンポーネントがライセンスされていること

- キーの正常性が損なわれていないこと

上記いずれかの条件が満たされていない場合、キーファイルは*無効*となり、**Dr. Web Anti-virus for servers** はマルウェアの検出と駆除を停止します。

1.4.2. キーファイルの取得

キーファイルは.keyの拡張子が付いたファイル、それらのファイルを含んだZIPアーカイブの形で送付されます。

サイトでの登録プロセスでのキーファイルの取得

サイトでの登録とキーファイルのダウンロードはインターネット経由で行われます。インストール前にコンピューターがインターネットに接続されていることを確認して下さい。

ライセンスキーファイルを取得するには、製品のシリアルナンバーが必要です。

1. 製品付属の登録カードに記載しているアドレスのサイトにアクセスしてください。
2. お客様情報をフォームに入力して下さい。
3. シリアル番号（登録カードにあります）を入力して下さい。
4. 生成されたキーファイルは、登録フォームで指定した電子メールに、ZIPアーカイブの形で送信されます。登録後、登録ページからキーファイルをダウンロードすることもできます。WindowsOSではZIPフィアルが自動的に解凍されることがあります。追加ソフトウェアをインストールする必要はありません。
5. キーファイルを インストール して下さい。

再登録

キーファイルを紛失した場合に、再登録が必要な場合があります。再登録の際には、最初の登録で入力したものと同じ個人情報を入力する必要があります。他のメールアドレスを使用することはできますが、その場合、キーファイルは新しいアドレスに送信されます。

キーファイル取得の回数には上限があります。同じシリアルナンバーでの登録は25回までです。この回数を超えるとキーファイルは送信されません。その場合には、詳しい状況と、登録の際に入力した個人情報とシリアルナンバーを添えてテクニカルサポートセンター にご連絡ください。

有効なキーファイルが見つからない場合、プログラムの機能は動作しません。

1.4.3. ライセンスの延長

ライセンス有効期限の終了、またはシステム保護の強化などの理由によりライセンスを更新することができます。この場合、既存のシステムに登録されたライセンスキーファイルを交換する必要があります。アンチウイルスの動作を停止したり再インストールする必要がないよう、**Dr.Web Anti-virus for servers** はライセンスの「オンアクセス」更新をサポートしています。

キーファイルの更新

1. ライセンスマネージャー を開きます。新しいライセンスを取得する、またはお手持ちのライセンスを延長するために **Doctor Web** オフィシャルサイト上のお客様個人ページを使用することができます。ライセンスマネージャー または SpIDer Agent メニュー内で **マイDr.Web** の項目を選択してください。
2. 現在のキーファイルが無効の場合、 **Dr.Web Anti-virus for servers**は自動的に新しいキーファイルの使用に切り替わります。

1.5. アンチウイルスの動作検査

EICAR(European Institute for Computer Anti-Virus Research)テストファイルを使用して、ウイルスをシグネチャで検出するアンチウイルスプログラムの動作をチェックすることができます。

アンチウイルスの多くの開発者は、動作確認の為にtest.comというプログラムを使用しています。このプログラムは、自分のコンピューターを危険にさらすことなく、インストールされたアンチウイルスがウイルスの検出に関してどのように警告するかを見るために特別に開発されたものです。test.comプログラム自体は有害ではなく、多くのアンチウイルスプログラムによってウイルスと処理されるようにできています。**Dr. Web Anti-virus for servers**は、この「ウイルス」を検出すると `EICAR Test File (Not a Virus!)` と表示します。他のアンチウイルスプログラムも同様です。

test.comプログラムは、68バイトのCOMファイルです。実行するとコンソールにEICAR-STANDARD-ANTIVIRUS-TEST-FILE!というメッセージが表示されます。

test.comのファイルは、次の文字列のみで形成されています。

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

上記文字列でファイルを作成し、test.comのファイル名で保存すると、前述のような無害な「ウイルス」と認識されるプログラムができあがります。

EICARファイルの実行は、コンピュータのセキュリティを脅かさないため、**SpIDer Guard** の 最適化モード ではEICARファイルを悪意のあるソフトウェアとして検出しません。しかしながらデフォルトではファイルのコピーや作成は **SpIDer Guard** で検知され、隔離 フォルダに移動されます。

1.6. ウイルスの検出手法

Dr.Web アンチウイルスソリューション は、悪意のあるソフトウェア検出に複数の手法を同時に使用します。それにより、感染が疑われるファイルに対する徹底的な検査を実行し、ソフトウェアの動作をコントロールすることが出来ます。

1. 検査はまず、ファイルコードセグメントを既知のウイルス署名と比較する*シグネチャ解析*で始まります。*シグネチャ*はウイルスを特定する為に必要かつ十分な、連続するバイトの有限なシーケンスです。シグネチャ辞書のサイズを抑える為、**Dr.Web アンチウイルスソリューション** はシグネチャのシーケンス全体ではなくチェックサムを使用します。チェックサムは独特な方法でシグネチャを特定し、ウイルス検出および駆除の正確さを維持します。**Dr.Web ウイルスデータベース** は、1つのエントリによって特定のウイルスのみでなく脅威のクラスに属する全てのウイルスを検出できるように設計されています。
2. シグネチャ解析の完了後、**Dr.Web アンチウイルスソリューション** 既知の感染メカニズムを用いた新種・亜種ウイルスを検出するユニークなテクノロジー **Origins Tracing™** を使用します。それにより **Dr.Web** ユーザは Trojan.Encoder.18（別名 gpcode）のような悪質なウイルスから保護されます。**Origins Tracing** は、新種・亜種ウイルスの検出に加え、**Dr.Web** ヒューリスティック解析による誤検出を劇的に減らします。
3. *ヒューリスティックアナライザー*が使用する検出手法は、悪意のあるコードを特徴づける属性に関する情報に基づいています。各属性または特徴は、その重要度および信頼度を定義する重み係数を持っています。ヒューリスティックアナライザーはファイルの重み付け合計値に応じて、未知のウイルスに感染している可能性を計算します。不確実な状況で仮説を扱うあらゆるシステム同様、ヒューリスティックアナライザーもまたタイプ I またはタイプ II のエラーを侵す可能性があります（ウイルスを見逃す、または誤検知）。

上記の検出手法に加え、**Dr.Web アンチウイルスソリューション** は既知の悪意のあるソフトウェアに関する最も新しい情報も使用します。**Doctor Web ウイルスラボ** のエキスパートが新しい脅威を発見するとすぐに、ウイルスシグネチャおよびその振る舞い特性を記録したアップデートが配信されます。アップデートは1時間に数回行われる場合もあり、たとえ新種のウイルスが **Dr.Web 常駐保護** を通過してシステムに侵入した場合でも、アップデート後に検出され駆除されます。

チャプター2　プログラムのインストール

インストールの前に以下のことに注意してください。

- オペレーティングシステムに対するMicrosoft社からの全ての重要な更新をインストールして下さい（同社のサイトからダウンロードし、インストールすることができます。アドレス http://windowsupdate.microsoft.com）
- システムユーティリティーでファイルシステムを検査し、欠陥が発見された場合にはそれを取り除いて下さい。
- アクティブなアプリケーションを閉じて下さい。

Dr.Web Anti-virus for servers は他のアンチウイルスソフトウェアとの間に互換性を持ちません。同一コンピューター上に2つのアンチウイルスプログラムをインストールするとシステムのクラッシュおよび重要なデータの損失を招く恐れがあります。

インストールウィザードの指示に従って操作します。ファイルがコンピュータにコピーされるまでは、**戻る**　をクリックすることで前の手順に戻ることができます。インストールを続行するには **次へ** を、中断するには **キャンセル** をクリックします。

2.1. Dr.Web Anti-virus for serversのインストール

Dr.Web Anti-virus for serversをインストールするには、管理者権限が必要です。

アンチウイルスソフトウェアのインストールには次の2つのモードがあります。

1. バックグラウンドモード
2. ユーザーモード

バックグラウンドモードでのインストール

バックグラウンドモードで **Dr.Web Anti-virus for servers** をインストールするには、コマンドラインに実行ファイルの名前と必要なパラメータを入力します（このパラメータはロギングに影響を与えるため、インストール後には再起動を行ってください）。

インストール	パラメータ
再起動しません ロギングしません	`/S /V/qn`

再起動します
ロギングしません
	`/S /V"/qn REBOOT=Force"`
	or
	`/S /V"/qn REBOOT=F"`

再起動しません ロギングします	`/S /V"/qn /lv* \" <path>\drweb-setup.log\""`

再起動します
ロギングします
	`/S /V"/qn /lv* \" <path>\drweb-setup.log\" REBOOT=F"`
	or
	`/S /V"/qn /lv* \" <path>\drweb-setup.log\" REBOOT=Force"`

例:

Dr.Web Anti-virus for serversをインストールし、インストール後にロギングと再起動を行う場合は、次のコマンドを実行します。

```
C:\Documents and Settings\drweb-700-winsrv-x86.exe /S /V"/qn /lv* \"%temp%\drweb-setup.log\"REBOOT=F"
```

インストール時に言語を指定する場合は、次のパラメータを使用します。

/L<*言語_コード*>

例:

```
/L1049 /S /V"/qn REBOOT=Force"
```

言語一覧:

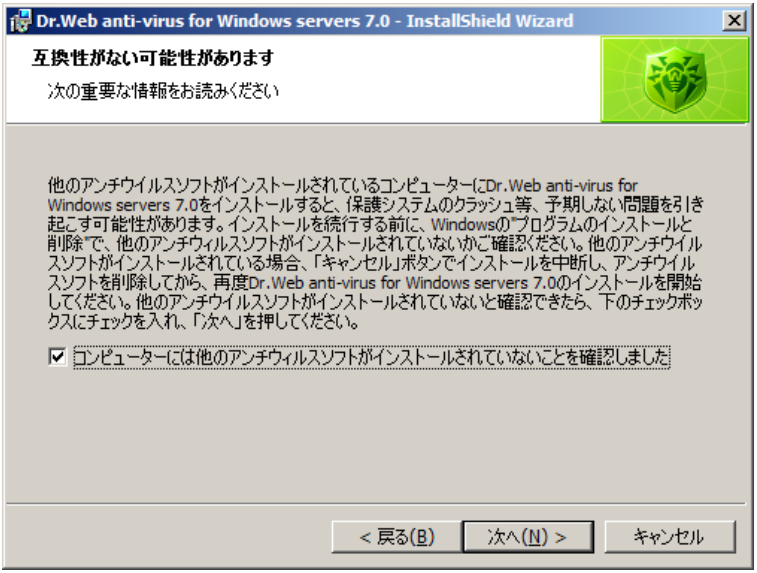
コード	言語
1026	ブルガリア語
2052	中国語(簡体字)
1028	中国語(繁体字)
1033	英語
1061	エストニア語
1036	フランス語(フランス)
1031	ドイツ語
1032	ギリシャ語
1038	ハンガリー語
1040	イタリア語
1041	日本語
1062	ラトビア語
1063	リトアニア語
1045	ポーランド語
2070	ポルトガル語

コード	言語
1049	ロシア語
1051	スロバキア語
1034	スペイン語（トラディショナルソート）
1055	トルコ語
1058	ウクライナ語

選択にかかわらず、英語はインストールされます。

通常モードでのインストール

1. 使用許諾契約書をお読みください。インストールを続けるには、契約に同意してください。
2. インストールウィザードは、 **Dr.Web** とコンピューターにインストールされている他のアンチウイルス間で起こり得る非互換性について警告し、それらを削除または無効にすることを提案します。他のアンチウイルスがインストールされている場合、**キャンセル**をクリックしてインストールを中断し、それらを削除または無効化した後に再度インストールを開始することを推奨します。インストールを続けるには **コンピューターには他のアンチウイルスソフトがインストールされていないことを確認しました** のチェックボックスにチェックを入れ **次へ**をクリックして下さい。



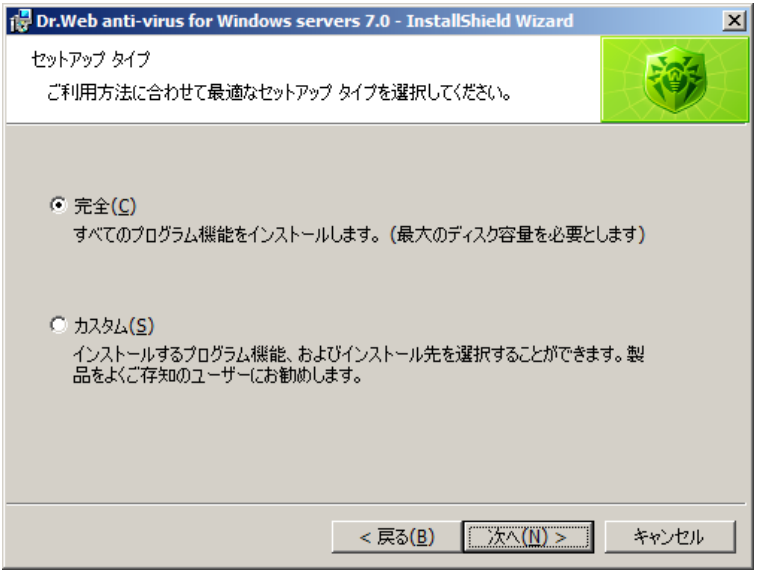
3. プログラムの操作に必要な キーファイル を要求するウィンドウが表示されます。キーファイルがハードドライブまたはリムーバブルメディア上にある場合、**参照**をクリックし、キーファイルを選択して**次へ**をクリックしてください。

キーファイルをお持ちでない場合、**キーファイルは後から取得します** を選択してください。有効なキーファイルを取得するまでプログラムコンポーネントは使用出来ません。

次へ をクリックしてください。

Dr.Web Anti-virus for servers キーファイルのみを使用してください。キーファイルは **.key**拡張子を持っています。

4. インストールウィザードでインストールのタイプを選択します。**完全インストール**は全てのコンポーネントおよび全ての補助的プログラムをステップ8まで自動的にインストールします。**カスタムインストール** は上級ユーザー向けです。カスタムインストールのプロセスで、インストールするコンポーネントの選択とプロキシサーバーの設定およびインストールの追加設定を求められます。

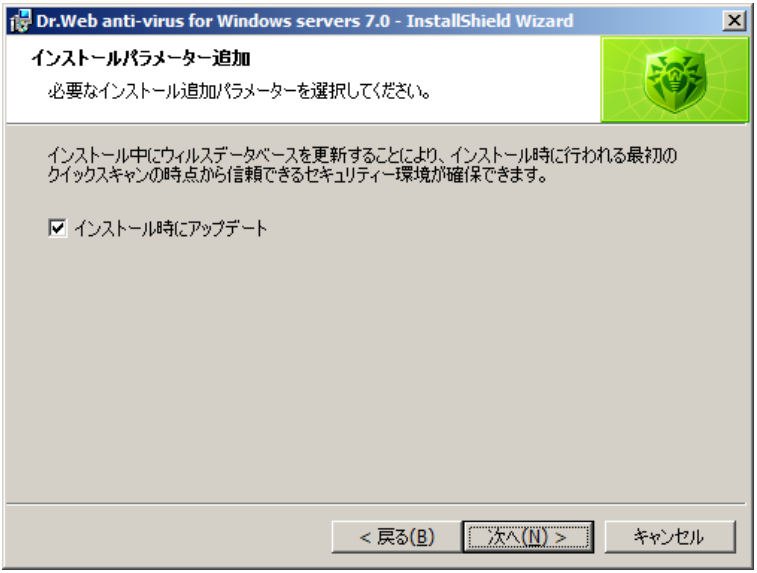


インストールのタイプを選択したら、**次へ** をクリックします。

5. デフォルトインストールを選択した場合、ステップ8の説明に進んで下さい。カスタムインストールを選択した場合、開いたウインドウでインストールするコンポーネントを選択して下さい。必要に応じてインストールフォルダを変更することが出来ます。

必要なコンポーネントの選択が完了したら **次へ** をクリックします。

6. **Dr.Web Anti-virus for servers** へのショートカットの作成を設定するウィンドウが開きます。必要なオプションを選択し **次へ**をクリックしてください。
7. ステップ3でライセンスキーファイルを指定した場合、次のウィンドウで **インストール時にアップデート** を選択し、インストール中に最新のウイルスデータベースをダウンロードすることができます。



次へ をクリックします。

8. プロキシサーバーの設定ウィンドウが開きます。

   プロキシサーバーを使用していない場合、**プロキシサーバーを使用しません** を選択してください。

   プロキシサーバーの設定を指定したい場合、**プロキシサーバーのIPアドレスとポートを手動で指定**を選択してください。

9. インストールの準備が完了したというメッセージが表示されたウィンドウが開きます。インストールを開始するには **インストール** を、インストールパラメータを変更する場合は **戻る**をクリックします。
10. ライセンスキーファイルを指定した場合、またはステップ7で **インストール時にアップデート**を選択した場合は、ウイルスデータベースおよび **Dr.Web Anti-virus for servers** のコンポーネントが自動でアップデートされます。
11. インストール完了後、スキャナ が クイックスキャン を実行します。検出された脅威に対するアクションを適用し、検査完了後に スキャナ を閉じてください。
12. インストールを完了するためにコンピューターを再起動して下さい。

2.2. Dr.Web Anti-virus for serversの再インストールと削除

インストールされた **Dr.Web Anti-virus for servers** を変更・修復・削除するには インストールウィザード を実行してください。

開いたウィンドウで以下の手順を実行してください。

1. インストールされたコンポーネントの設定を変更するには**変更**を選択し、**次へ**をクリックします。カスタムインストール ウィンドウが開きます。全てのコンポーネントを削除するには **削除**を選択してください。
2. **Dr.Web Anti-virus for servers** を削除する、またはインストールするコンポーネントのセットを変更するには、パスワードを入力して **セルフプロテクション**を無効にする必要があります（SpIDer Agent 設定 の **アドバンス** タブで **Dr.Webの設定をパスワードで保護する**フラグを設定している場合）。
3. インストールを完了するために、指示に従ってコンピューターを再起動してください。

変更・修復・削除は、Windows標準ユーティリティの **プログラムの追加と削除** でも行うことができます。

変更・修復・削除は、Windows標準ユーティリティの **プログラムの追加と削除** でも行うことができます。

チャプター3　作業の開始

インストールプログラムによって以下の **Dr.Web Anti-virus for servers** をインストールすることができます。

- スキャナ（GUIバージョンとコンソールバージョン）
- **SpIDer Guard**
- 自動更新ユーティリティ
- **SpIDer Agent**

Dr.Web Anti-virus for serversのコンポーネントは、共通のウイルスデータベースとアンチウイルスエンジンを使用しています。また、統一された検出・駆除アルゴリズムを採用しています。しかしながら検査対象の選択方法が大きく異なるため、コンピュータの保護にこれら複数のコンポーネントを相互補完的に使用することが可能です。

Dr.Webスキャナは、特定のファイル（全てのファイル、選択された論理ディスク、フォルダなど）をユーザー指定、またはスケジュールによって検査します。デフォルトではメインメモリおよびスタートアップファイルも検査されます。タスクの実行時をユーザーが選択するため、他の重要プロセスのリソースが足りなくなることを心配する必要はありません。

SpIDer Guard は、コンピューターのメモリー上に常駐し、ファイルシステムのオブジェクトへのアクセスを監視します。プログラムはハードドライブ上で実行・作成・変更されたファイル、またはリムーバブルメディアおよびネットワークディスク上で開かれたそのようなファイルのウイルス検査を実行します。バランスのとれたファイルシステムの検査レベルにより、プログラムはコンピュータの他のプロセスの動作に影響することはほとんどありません。ただし、検査レベルを下げるとウイルス検出の信頼性は若干低くなります。

このプログラムの利点は、コンピューターの作業を中断することなくウイルスを監視し続けることができるという点にあります。また **SpIDer Guard** のみが、その特殊な活動を基に検出することが可能なウイルスもあります。

ウイルス脅威からの保護を確実なものにする

包括的なアンチウイルス保護を確実なものにするために、以下のような **Dr.Web Anti-virus for servers** コンポーネントの使用を推奨します。

- コンピューターのファイルシステムをデフォルトの検査レベル（最大）で検査する
- **SpIDer Guard** をデフォルト設定で使用する
- ウイルスデータベースのアップデートと同時に、定期的にコンピューターのフルスキャンを行う（1週間に1回以上）
- **SpIDer Guard** が一時的に停止している時にコンピューターがインターネットに接続した、またはリムーバブルメディアからファイルをダウンロードした場合には直ちにフルスキャンを実行する

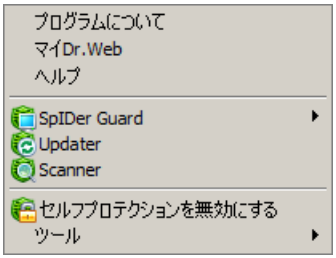
アンチウイルス保護は、ウイルスデータベースとその他コンポーネントファイルのアップデートが定期的に（毎時が望ましい）行われている状態で効果的なものとなります（詳細については 自動更新 をご覧ください）。

3.1. SpIDer Agent管理モジュール

Dr.Web Anti-virus for servers がインストールされると、Windowsの通知領域に**SpIDer Agent** のアイコン が追加されます。

マウスのカーソルをアイコンに合わせると、動作中のコンポーネント、アンチウイルスの最終更新日、ウイルスデータベース内の記録数についてのポップアップメッセージが表示されます。また設定によって、**SpIDer Agent** のアイコン 上に通知メッセージが表示されることがあります。

管理モジュールのアイコンのコンテキストメニューで、**Dr.Web Anti-virus for servers** コンポーネントの主な管理と設定を行うことができます。



プログラムについて の項目は、**Dr.Web Anti-virus for servers** のバージョンに関するウインドウを開きます。

マイDr.Web の項目は、**Doctor Web 公式サイト**上のあなたのパーソナルページを開きます。このページでライセンスに関する情報（有効期限、シリアル番号）の確認、ライセンスの期間の延長、サポートセンターへの問い合わせなどを行うことができます。

ヘルプの項目は、**Dr.Web Anti-virus for servers** のヘルプを開きます。

SpIDer Guard、更新 の項目は、該当するコンポーネントの管理および設定ウィンドウを開きます。

スキャナ の項目は **Dr.Webスキャナ** を起動させます。

セルフプロテクションを無効にする の項目は、**Dr.Web Anti-virus for servers** ファイル・レジストリキー・プロセスを破損および削除から保護する設定を無効／有効にすることができます。

ユーザーモード ではセルフプロテクションを無効にすることは出来ません。また、セルフプロテクションを無効にすることは推奨できません。

デフラグツールの動作中に何らかの問題が発生した場合には、一時的にセルフプロテクションを無効にしてください。

セルフプロテクションを無効にするには

- SpIDer Agent メニューで **セルフプロテクションを無効にする** の項目を選択します。
- パスワードを入力してください。
- **SpIDer Agent** メニューでセルフプロテクションを無効にすると、**セルフプロテクションを有効にする** 項目が表示されるようになります。

システムの復元ポイントにロールバックするには、セルフプロテクションを無効にしてください。

[ツール] ではサブメニューが表示され、以下の項目にアクセスできるようになります。

- ライセンスマネージャー
- **Dr.Web Anti-virus for servers** の 設定
- 隔離マネージャー
- アンチウイルスネットワーク
- レポートウィザード

Doctor Webテクニカルサポート にお問い合わせの際には、**Dr.Web**のレポートを作成してください。パラメータを調整するには、表示されているウィンドウで**[ログのパラメータ]**をクリックしてください。このレポートは、%USERPROFILE%フォルダ内のDoctorWebサブフォルダにアーカイブとして保存されます。

管理者モード/ユーザーモードの項目で、全ての機能を使用出来る **管理者モード** と制限のある **ユーザーモード** の切り換えが可能です。**ユーザーモード** では

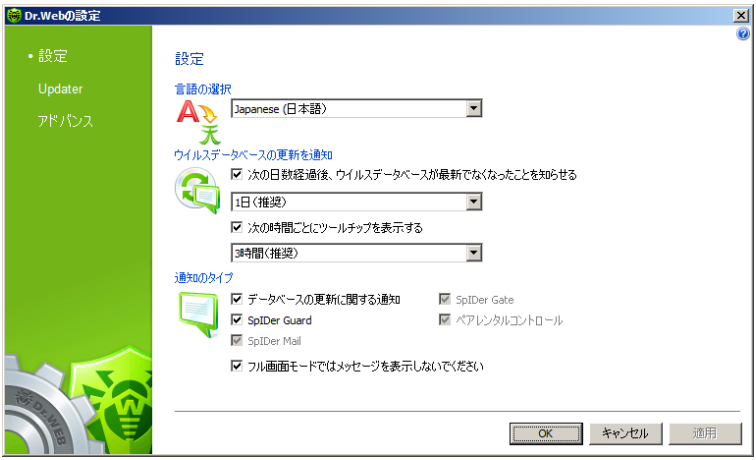
コンポーネント設定へのアクセス、また全てのコンポーネントとセルフプロテクションを無効にすることができません。**ライセンスマネージャー**および **アンチウイルスネットワーク** の項目も利用できません。**管理者モード** に切り換えるには管理者権限が必要です。

この項目は、管理者権限がない場合にのみ表示されます。例えば、Microsoft Windows Server 2008 のOSのユーザーアカウント制御（UAC）が有効になっている場合などです。そうでない場合、この項目は表示されず、**Dr.Web Anti-virus for servers** は常に完全な機能を持つモードで稼動します。

3.2. 全般設定

Dr.Webの設定 ウインドウで、**Dr.Web Anti-virus for servers** の全般設定を行うことができます。このウィンドウを開くには通知領域で**SpIDer Agent** アイコンをクリックし、**ツール** を選択して **設定** を選んでください。

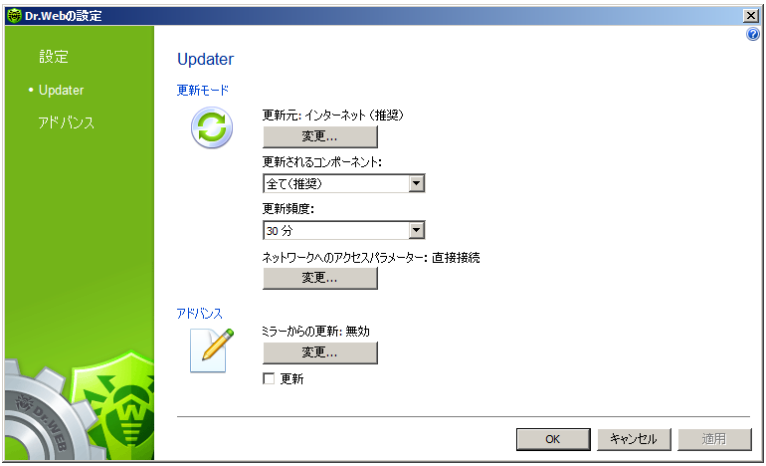
設定



このページで、 **言語の選択** リスト内から必要な言語を選択して **Dr.Web Anti-virus for servers** GUIの言語を設定することができます。インストールされていない言語が選択された場合、その言語をインストールするよう **Dr.Web Anti-virus for servers** が提案します。

またこのウインドウで、タスクバー通知領域の**SpIDer Agent**のアイコン上にポップアップメッセージの形で表示される通知メッセージのタイプの設定を行います。コンポーネントは、該当するイベント（脅威が検出されたまたはアップデートが実行されたなど）が発生した際に通知を行います。**更新**

このページで **Dr.Web Anti-virus for servers** のアップデートするコンポーネントや更新元、更新頻度、ミラーサイトなどを設定することができます。



更新元

更新元を変更するには、**変更** をクリックしてください。ウインドウ内の下記の更新元を選択します。

- **インターネット (推奨)** – 更新は **Doctor Web** のサーバからダウンロードされます。この更新元はデフォルト設定です。
- **ローカル、またはネットワークフォルダー** – 更新は更新分がコピーされたローカルフォルダ、もしくはネットワークフォルダからダウンロードされます。フォルダのパスを指定するには、**参照** ボタンをクリックしてフォルダを指定するか、手動でアドレスを入力してください。必要に応じてユーザー名とパスワードを入力します。
- **アンチウイルスネットワーク** – 更新は **Dr.Web** 製品がインストールされたほかのコンピュータでミラーが作成されていた場合にローカルネットワークのコンピュータからダウンロードされます。

ミラーからの更新

Dr.Web 製品がインストールされたコンピュータを更新元にして、他のローカルネットワークコンピュータからのアクセスを許可するには、**ミラーからの更新** の **変更** を

クリックし、ウインドウ内の **更新ミラーサイトを作成** を選択し、更新をコピーするフォルダのパスを指定します。コンピュータが複数のネットワークに接続している場合、1つのネットワークの特定のIPアドレスを許可するように指定できます。また、HTTP接続のポートの指定も可能です。

ネットワークアクセスモード

ネットワークアクセス(プロキシ)を設定することも可能です。**ネットワークへのアクセスパラメーター** で **変更** をクリックし、以下のモードのいずれかを選択してください。

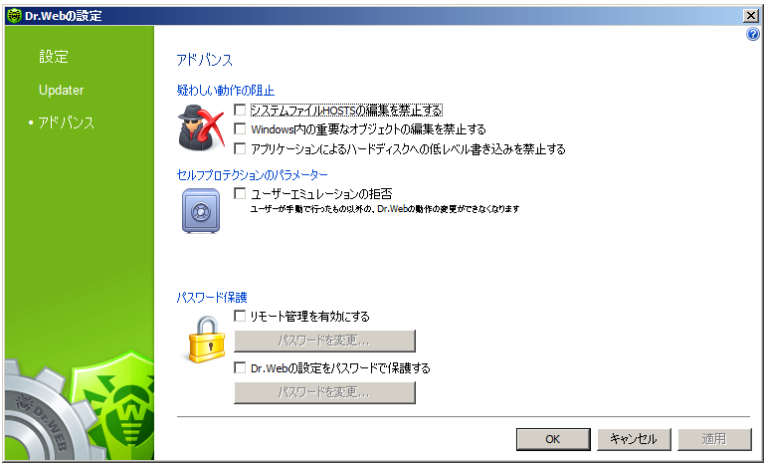
- インターネット接続にプロキシサーバーを使用していない場合、**直接接続** を選択します。
- プロキシサーバー設定を手動で行いたい場合、**ユーザー設定** を選択して接続パラメータを入力してください。

ログの詳細レベルを上げるには **詳細なログ** にフラグをセットしてください。行われた全ての変更が %allusersprofile%\Application Data\Doctor Web\Logs\(Windows Server 2008 の場合は %allusersprofile%\Doctor Web\Logs\ ) フォルダ内にある dwupdater.log に記録されます。

アドバンス

このページで、セルフプロテクションのパラメータを指定し、コンピューターのセキュリティを脅かす可能性のある操作を無効にすることができます。

重要なMicrosoft Updateのインストールや、プログラム(デフラグツールなど)のインストールまたは操作中に問題が発生した場合は、このグループの該当するオプションを無効にしてください。



パスワード保護

以下のオプションを設定することができます。

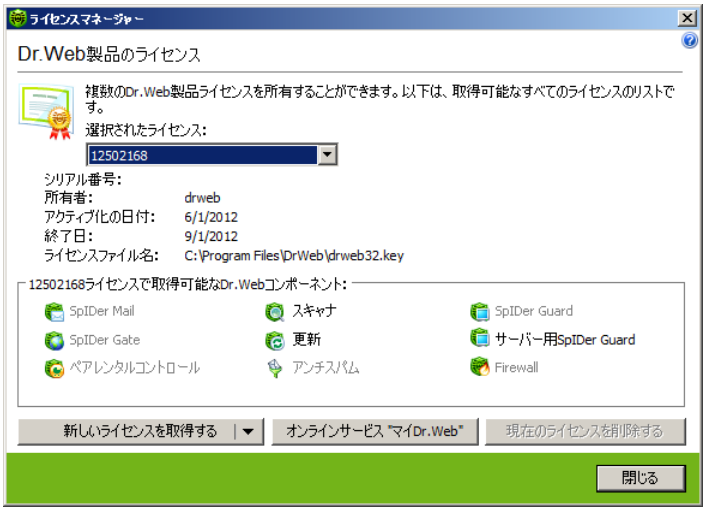
- コンピューター上の **Dr.Web Anti-virus for servers** へのリモートアクセスを許可し、他のコンピューターからアンチウイルスに接続する際に必要なパスワードを設定します。
- コンピューター上の **Dr.Web Anti-virus for servers** の設定をパスワードで保護します。**Dr.Web Anti-virus for servers** の設定にアクセスするためのパスワードを設定してください。

3.3. ライセンスマネージャー

ライセンスマネージャー は、**Dr.Web Anti-virus for servers** キーファイルにある情報を分かりやすく表示します。

ライセンスマネージャ の項目は 管理者モード で動作している場合のみメニュー上で使用可能になります。

ライセンスマネージャー を開くには通知領域の**SpIDer Agent** アイコンをクリックし、**ツール** を選択して **ライセンスマネージャー** を選びます。



お持ちのライセンスで使用可能な **Dr.Web Anti-virus for servers** コンポーネントが **Dr. Webコンポーネント** グループボックス内に表示されます。

オンラインサービス マイDr.Web は **Dr.Web Anti-virus for servers 公式サイト** のパーソナルページを開きます。このページでライセンスに関する情報（有効期限、シリアル番号）の確認、ライセンスの期間の延長、サポートセンターへの問い合わせなどを行うことができます。

取得したキーファイルのインストール

1. **新しいライセンスを取得する** をクリックします。ドロップダウンリストで **ディスク上のファイルから** を選択して下さい。
2. ファイルを選択します。
3. **Dr.Web Anti-virus for servers** は自動的にキーファイルの使用を開始します。

キーファイルをリストから削除するには、**現在のライセンスを削除する** をクリックしてください。最後に使用されているキーは削除されません。

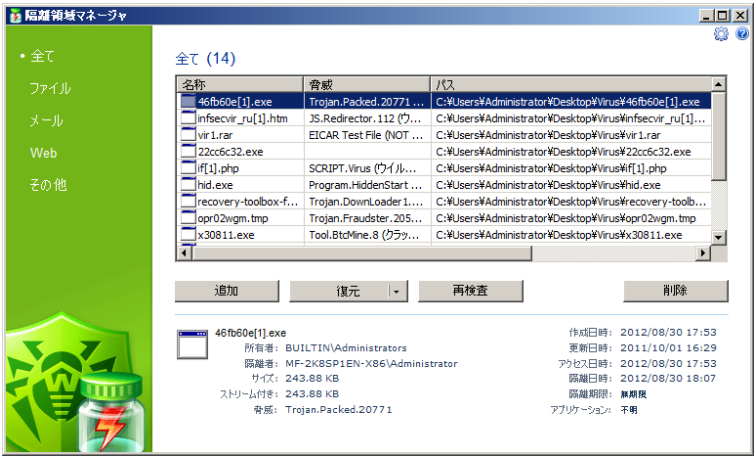
デフォルトでは、キーファイルは **Dr.Web Anti-virus for servers** のインストールフォルダに保存する必要があります。**Dr.Web Anti-virus for servers** は定期的にキーファイルを検証します。キーファイルの妥当性を維持する為に、キーファイルを編集しないでください。

有効なライセンス キーファイルが見つからなかった場合、**Dr.Web Anti-virus for servers** コンポーネントの動作はブロックされます。

3.4. 隔離

Dr.Web Anti-virus for servers の **隔離** セクションはマルウェアの疑いがあるファイルを隔離するためのものです。**隔離** フォルダは疑わしいファイルが検出されたそれぞれの論理ディスク上に個別に作成されます。書き込み可能なリムーバブルメディア上で感染したオブジェクトが検出された場合はメディア上に隔離フォルダが作成され、感染したオブジェクトがそのフォルダへ移されます。

隔離マネージャー を開くには、通知領域内の **SpIDer Agent** アイコンをクリックして **ツール** を選択し、**隔離マネージャー** を選びます。



ウインドウの中央に、隔離の状況に関する以下のフィールドを含んだ表が表示されます。

- **名称** – 隔離内にあるオブジェクトの名称
- **脅威** – オブジェクトが隔離へ自動移動された際の **Dr.Web Anti-virus for servers** によるマルウェアの分類
- **パス** – 隔離に移される前にオブジェクトがあった場所へのフルパス

ウィンドウ下部には選択されたオブジェクトに関する詳細が表示されます。情報は表に表示させることもできます。

表の表示設定

1. 表のヘッダを右クリックし、**カラムのカスタマイズ** を選択します。
2. 開いたウインドウで表に加えたい項目のチェックボックスにチェックを入れ、表から外したい項目のチェックを外して下さい。また以下のいずれかを実行することも可能です。
   - 全てのアイテムにチェックを入れるには、**全て選択** をクリックします。
   - 全てのチェックボックスをクリアするには、**全ての選択を外す** をクリックします。
3. 表内でのカラムの位置を変更するには **上へ移動** または **下へ移動** を使用します。
4. 編集後、変更を保存するには **OK** を、キャンセルするには **キャンセル** をクリックしてください。

左のサイドパネルで、表示される隔離オブジェクトのフィルタリングを行います。該当する項目をクリックすると、中央に全ての隔離オブジェクト、または指定されたグループのオブジェクト（ファイル、メールオブジェクト、webページ、またはこのカテゴリーに含まれない他の全てのオブジェクト）が表示されます。

隔離ウインドウでファイルを見ることができるのは、それらのファイルへのアクセス権を持つユーザーのみです。

次のボタンを使用して隔離を管理します。

- **追加** – ファイルを隔離に追加します。表示されたファイルシステムブラウザで必要なファイルを選択して下さい。
- **復元** – ファイルを隔離から移動し、元の場所に戻します（隔離される前にあったフォルダに戻します）。

この機能は、オブジェクトが無害であると分かっている場合のみ使用してください。

ドロップダウンリストで **指定場所に復元** を選択し、指定したフォルダにファイルを復元することができます。

- **再検査** – ファイルを再度検査します。再検査でクリーンと判定された場合、隔離マネージャー はファイルを復元するよう促します。
- **削除** – ファイルを隔離およびシステムから削除します。

表内のどこかで右クリックすると、以下のオプションが表示されます。

- **Doctor Webウイルスラボにファイルを送信** – ファイルを解析のため Doctor Web ウイルスラボ に送信します。
- **ハッシュ値をクリップボードにコピー** – MD5、SHA256で出力されたハッシュ値をクリップボードにコピーします。

複数のオブジェクトを同時に扱うにはSHIFTまたはCTRLを押しながら必要なファイルを選択し、右クリックしてドロップダウンリストから必要なアクションを選択して下さい。

選択されたアイテムに関する詳細が隔離ウィンドウ下部に表示されます。

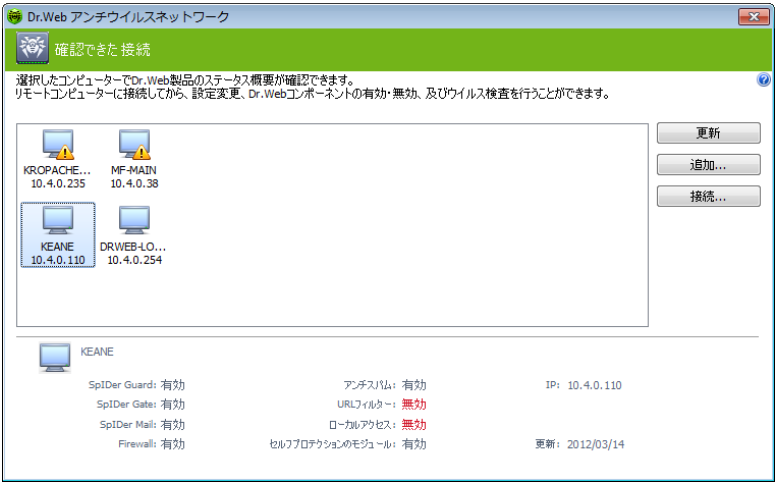
隔離 パラメータを設定するには、隔離 ウィンドウの 設定  ボタンをクリックします。開いた 隔離領域のプロパティウィンドウで以下のパラメータを変更することができます。

- **隔離領域サイズの設定** セクションで 隔離 フォルダが占めるディスク領域のサイズを管理できます。
- **ビュー** セクションでは **バックアップファイルの表示** チェックボックスにチェックを入れることで 隔離 ファイルのバックアップコピーを表に加えることができます。

バックアップコピーはファイルを 隔離 に移動する際、自動的に作成されます。隔離 ファイルが無期限で保存される場合でも、そのバックアップコピーの保存は一時的なものになります。

3.5. アンチウイルスネットワーク

このセクションでは、ネットワーク内にある他のコンピューター上への **Dr.Web Anti-virus for servers** のインストールを管理することができます。セクションを開くには **SpIDer Agent** アイコン のコンテキストメニュー内で **ツール** を選択し **アンチウイルスネットワーク** を選んでください。



リモートアンチウイルスにアクセスするにはリスト内でコンピューターを選択し、**接続** をクリックします。リモートアンチウイルスの設定内で指定したパスワードを入力してください。リモート **SpIDer Agent** のアイコン が通知領域に表示されます。リモートアンチウイルスのユーザーはリモート接続について通知されます。以下の項目を使用することができます（インストールされる **Dr.Web 製品** によってコンポーネントの組み合わせは変わります）。

- プログラムについて
- ライセンス登録
- マイ**Dr.Web**
- ヘルプ
- **SpIDer Guard**

- **SpIDer Mail**
- **SpIDer Gate**
- ペアレンタルコントロール
- **Dr.Web Firewall**
- ツール
- アップデーター
- セルフプロテクションを有効／無効にする

ツール には以下のサブメニューがあります。

- ライセンスマネージャー
- **Dr.Web** の動作に関する 一般設定
- レポートウィザード

設定の管理、コンポーネントの有効／無効化、統計の閲覧が可能です。

アンチウイルスネットワーク、隔離マネージャー、スキャナ は使用できません。ファイアーウォール 設定および統計も使用不可となっていますが、ファイアーウォール を有効／無効にすることはできます。**接続を切る** を選択してリモート接続を切ることもできます。

目的のコンピューターがリスト上に無い場合、手動で追加することが可能です。**追加** ボタンをクリックしIPアドレスを入力してください。

確立できる**Dr.Web 製品**へリモート接続は1つのみです。既に接続が1つ確立されている場合、**接続** ボタンが無効になります。

リモート接続が可能である**Dr.Web** 製品がコンピューター上にインストールされている場合、それらのコンピューターは アンチウイルスネットワーク のリスト内に表示されます。お使いの **Dr.Web Anti-virus for servers** への接続は 設定 の **アドバンス** タブ内で許可することができます。

アンチウイルスネットワーク の項目は 管理者モード で動作している場合のみメニュー上で使用可能になります。

チャプター4. Dr.Web スキャナ

デフォルトでは、プログラムはウイルスデータベースおよびヒューリスティックアナライザー（ウイルス開発の一般的なアルゴリズムに基づき、プログラムにとって未知なウイルスを高確率で検出する手法）を使用して全てのファイルを検査します。特別なパッカーによってパックされた実行ファイルは、検査時に解凍されます。一般的に使用されているタイプのアーカイブ（ACE、ALZIP、AR、ARJ、BGA、7-ZIP、BZIP2、CAB、GZIP、DZ、HA、HKI、LHA、RAR、TAR、ZIPなど）内、コンテナ（1C、CHM、MSI、RTF、ISO、CPIO、DEBなど）内、メールプログラムのメールボックス内（メールのフォーマットは、RFC822に従っていなければなりません）のファイルも検査されます。

デフォルトで **Dr.Web スキャナ** は全ての 検出手法 を使用してウイルスやその他の悪意あるソフトウェアを検知します。全ての感染オブジェクトや疑わしいオブジェクトの情報はアクションを手動で選択する表に表示されます。

デフォルトで、多くの場合に最適な設定がなされています。必要に応じて **Dr.Web Scanner** の スキャナの設定 で脅威を検出した時の動作を変更することができます。スキャンが完了した後に、検出された各脅威に対する処理を設定することができますが、特定の脅威の種類に応じた共通の処理を設定する必要があります。


Dr.Web Scanner
スキャンモードの選択
クイックスキャン
重要なシステムオブジェクトをスキャンします。週に1度、クイックスキャンを実行することを推奨します。
フルスキャン
論理ドライブ、リムーバブルメディア上の全ファイルをスキャンします。
カスタムスキャン
ここにファイルをドラッグ＆ドロップするか、クリックして選択してください。

4.1. スキャナの動作

Dr.Webスキャナ は通常のWindowsアプリケーションとしてインストールされ、自動的に、もしくはユーザによって起動されます (スキャナの自動起動 参照)。

管理者権限を持たないユーザーがアクセスできないファイルとフォルダ(システムフォルダを含む)は検査されません。スキャナの動作は管理者権限を持つユーザーが行うことを推奨します。

スキャナの起動

以下のいずれかを実行してください。

- デスクトップ上の **Dr. Webスキャナ** アイコンをクリックする。
- タスクバーの通知領域内にある **SpIDer Agent** アイコンのコンテキストメニューで **スキャナ** をクリックする(SpIDer Agent のチャプター参照)。
- Windows **スタート** メニューの全てのプログラム -> Dr.Webフォルダ内で **Dr. Webスキャナ** をクリックする。
- Windowsのコマンドライン内で該当するコマンドを実行する(コマンドラインモードでの検査 参照)。

スキャナ を起動するとメインウィンドウが開きます。

検査には**クイックスキャン**、**フルスキャン**、**カスタムスキャン**の3つのモードがあります。選択されたモードに応じて、検査されるオブジェクトのリストまたはファイルシステムツリーがウィンドウ中央に表示されます。

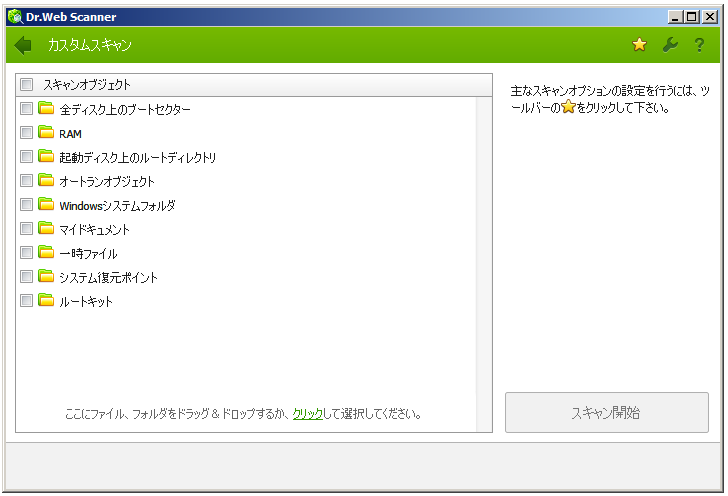
クイックスキャンモードでは次のオブジェクトを検査します。

- RAM
- 全てのディスクのブートセクター
- 自動起動オブジェクト
- ブートディスクのルートフォルダ
- Windowsインストールディスクのルートフォルダ
- Windowsのシステムフォルダ
- マイドキュメントフォルダ
- システムの一時フォルダ
- ユーザーの一時フォルダ

検査が管理者権限で実行された場合、このモードではシステム内にルートキットが存在するかどうかも検査されます。

フルスキャンモードでは、RAMおよび全てのハードドライブ（全てのディスクのブートセクターを含む）を検査します。またルートキットの検査も実行します。

カスタムスキャンモードでは、検査するオブジェクト（フォルダおよびファイル、RAM・自動起動オブジェクト・ブートセクターなどのオブジェクト）を選択することができます。選択したオブジェクトの検査を開始するには **スキャン開始** をクリックします。



検査が開始すると、**停止** と **中止** ボタンが有効になります。それぞれ、以下の事を行うことができます。

- 検査を一時停止したいときは、**停止** ボタンを押して下さい。中断された検査を再開したい場合は、**再開** ボタンを押して下さい。
- 検査を中止したい場合は、**中止** ボタンを押してください。

停止 ボタンは、検査の処理中とRAMの検査中は無効です。

4.2. ウイルス検出時のアクション

デフォルトでは、 **Dr.Web Scanner** は既知のウイルスまたは疑わしいオブジェクトが検出された際に通知を行います。**無効化** をクリックすると、検出された複数の脅威を同時に駆除することができます。**Dr.Web Scanner** は推奨されるデフォルトのアクションを検出された全ての脅威に対して適用します。必要に応じて、それぞれの脅威に対して個別の手順を実行することも可能です。

感染したオブジェクトの復元(修復)を試み、修復が不可能の場合は、オペレーティングシステムから感染したオブジェクトを削除します(削除)。

アクションの選択

1. 必要な場合、**アクション** フィールド内のドロップダウンリストからアクションを選択してください。デフォルトでは、検出された脅威の種類ごとに推奨されるアクションが選択されます。
2. **駆除** をクリックします。検出された脅威に対して、選択された全てのアクションが適用されます。

疑わしいオブジェクトは 隔離 に移されます。そのようなオブジェクトは解析の為 Doctor Webのウイルスラボに送信してください。ファイルを送信するには、隔離 ウィンドウ内で右クリックし Doctor Webウイルスラボに疑わしいファイルを送信 を選択します。

以下の制限があります。

- 疑わしいオブジェクトの修復はできません。
- ファイル以外のオブジェクト（ブートセクターなど）の隔離、名前の変更、または削除はできません。
- アーカイブ内、コンテナ内、メール添付内のファイルに対してはいかなるアクションも行うことができません。この場合、アクションはオブジェクト全体に対して行われます。

プログラムの動作に関する詳細なログが %allusersprofile%\Application Data\Doctor Web\Logs\ フォルダ（Windows 7では %allusersprofile%\Doctor Web\Logs\ ）内にある dwscanner.log ファイルに保存されます。

4.3. スキャナの設定

管理者権限を持たないユーザーがアクセスできないファイルとフォルダ（システムフォルダを含む）は検査されません。スキャナ の動作は管理者権限を持つユーザーが行うことを推奨します。

プログラムのデフォルト設定はほとんどの場合に最適な設定となっています。必要がなければ変更しないようにして下さい。

スキャナの設定

1. スキャナ 設定を開くには、ツールバーの **設定** アイコンをクリックします。**Dr.Webスキャナの設定** ウィンドウが開きます。
2. 必要な変更を行います。
3. それぞれのタブで行われる設定に関するより詳細な情報を得るには、**ヘルプ** ボタンを使用してください。
4. 編集終了後、変更を保存するには **OK** ボタンを、変更をキャンセルするには **キャンセル** ボタンをクリックしてください。

メインページ

このタブでは スキャナ 動作の全般的な設定を行うことができます。

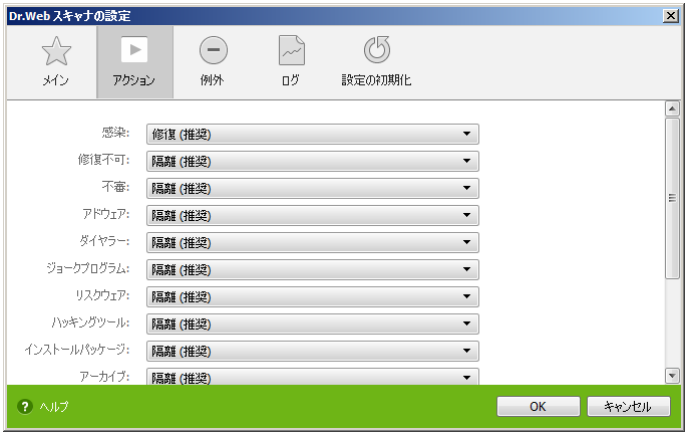
特定のイベントに対する警告音による通知を有効にする、検出された脅威に対して推奨されるアクションを自動的に適用するように設定する、OSと スキャナ 間のインタラクションを設定することが可能です。

スキャナ は管理者権限を持つアカウントで実行することを推奨します。そうでない場合、ユーザーがアクセス権限を持たないフォルダおよびファイル（システムフォルダを含む）は検査されません。スキャナ を管理者アカウントで実行するには **管理者権限でスキャンを開始** チェックボックスにチェックを入れてください。

アクションページ

検出された脅威に対するアクションを設定

1. **Dr.Webスキャナの設定** ウィンドウ内で **アクション** タブを選択します。



2. ドロップダウンリストで、感染したオブジェクト検出時にプログラムが実行するアクションを選択してください。
3. 修復不可能なオブジェクトに対するアクションは **修復不可** ドロップダウンリスト内から選択してください。**修復** アクションはありません。

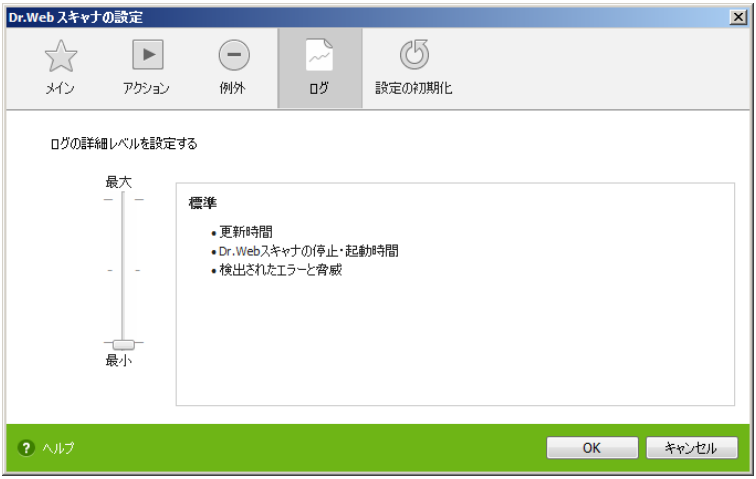
ほとんどの場合 **隔離** アクションが推奨となっています。

4. **疑わしい** オブジェクトのドロップダウンリストで疑わしいオブジェクト検出時のアクションを選択して下さい（前項と同様です）。
5. アドウェア、ダイヤラープログラム、ジョークプログラム、リスクウェア、クラッキングツールを含むオブジェクト検出時のアクションには同じものを指定してください。
6. ファイルアーカイブ、インストールパッケージ、メールボックス内でウイルスまたは疑わしいコードが検出された場合にそれらのオブジェクト全体に対して適用されるプログラムの自動アクションも、同様に設定します。
7. 感染したファイルの修復を完了する為にシステムの再起動が必要な場合があります。以下のいずれかを選択してください。

- **コンピューターを自動的に再起動する** ー 保存されていないデータは失われます。
- **再起動を提案する**

ログページ

ログ ページでログファイルに関する設定を行うことができます。



デフォルトで設定されているパラメータはそのまま使用してください。ログの詳細レベル（デフォルトでは、感染した、または疑わしいオブジェクトに関する情報は常に出力されます。また、パックされたファイルおよびアーカイブの検査に関する情報、検査が正常に完了したその他のファイルに関する情報は記録されません）は変更することができます。

4.4. コマンドラインモードでの検査

コマンドラインモードで スキャナ を実行することができます。このモードでは追加のパラメータとして、現在のスキャンセッションの設定を行い、検査の対象となるオブジェクトのリストを作成することができます。このモードではスケジュールによる スキャナ の自動起動が可能です。

コマンドラインから検査を実行する

次のようにコマンドを入力してください。

[*<プログラムへのパス>*]drweb32w [*<オブジェクト>*] [*<パラメータ>*]

検査するオブジェクトは空のまま、または空白で区切って複数指定することができます。

以下は、検査の対象となるオブジェクト指定の最も一般的な例です。

- **/FAST** システムのクイックスキャンを実行します（クイックスキャンモードに関する詳細は 検査モード を参照してください）。
- **/FULL** 全てのハードドライブおよびリムーバブルデータキャリア（ブートセクターを含む）のフルスキャンを実行します。
- **/LITE** RAM、全てのディスクのブートセクター、スタートアップオブジェクトの基本的な検査を実行します。

コマンドラインパラメータでプログラムの設定を指定します。パラメータが指定されていない場合、前回保存された設定で検査が実行されます（デフォルト設定を変更していない場合はデフォルト設定）。

各パラメータはスラッシュ (**/**) 記号で始まり、空白で区切られます。

4.5. コンソールスキャナ

Dr.Web Anti-virus for servers には、高度な設定が可能な コンソールスキャナ も含まれています。

コンソールスキャナ は疑わしいファイルを 隔離 には移しません。

コンソールスキャナの起動

次のコマンドを入力してください。

[*<プログラムへのパス>*]dwscancl [*<パラメータ>*] [*<オブジェクト>*]

検査するオブジェクトは空のまま、または空白で区切って複数指定することができます。

コマンドラインパラメータでプログラムの設定を指定します。空白で区切って複数のパラメータを指定することができます。使用可能なパラメータの一覧は 付録 A を参照してください。

リターンコード

- 0 – 検査は正常に終了しました。感染したオブジェクトは見つかりませんでした。
- 1 – 検査は正常に終了しました。感染したオブジェクトが検出されました。
- 10 – 無効なキーが指定されました。
- 11 – キーファイルが見つからないか、コンソールスキャナ に対するライセンスがあらりません。
- 12 – スキャニングエンジン が起動しませんでした。
- 255 – ユーザーによって検査が中断されました。

4.6 スキャナの自動起動

Dr.Web Anti-virus for servers のインストールプロセスの中で、自動的にアンチウイルス検査タスクを **タスクスケジューラ** に作成します(デフォルトではタスクは無効となっています)。

作成されたタスクのパラメータは、**コントロールパネル** → **管理ツール** → **タスクスケジューラ** を開いて、確認することができます。

作成されたタスクは、**Dr.Web Daily scan** というタスク名です。必要なパラメータと開始時間を設定して、このタスクを有効にすることができます。

On the **全般** タブで、表示したタスクの一般情報とセキュリティオプションを確認することができます。**トリガー** と **条件** タブで、タスクを起動するための様々な条件を設定することができます。**履歴** タブではイベントログが参照できます。

また、個別に検査タスクを作成することができます。システムスケジューラの操作の詳細については、ヘルプシステムやWindwosのドキュメントを参照してください。

Dr.Web Firewall がインストールコンポーネントに含まれていた場合、**Dr.Web Anti-virus for servers** のインストール終了後の一度目の再起動後、**Firewall** は **タスクスケジューラ** をブロックします。スケジュールされたタスクは、新しいルールが作成された二度目の再起動の後に動作します。

チャプター5. SpIDer Guard

デフォルトでは、**SpIDer Guard** はWindows起動時に自動的に起動し、そのセッションの間はアンロードすることはできません。必要な場合（プロセッサリソースを多く消費するタスクがリアルタイムモードで実行されている場合など）は **SpIDer Guard** を 一時的に無効にする ことが可能です。

SpIDer Guard を一時的に無効にできるのは管理者権限を持つユーザーのみです。

デフォルト設定では、**SpIDer Guard** はハードディスク上で作成中または変更中のファイル、およびリムーバブルメディア上で開かれた全てのファイルに対してオンアクセス検査を実行します。検査方法は **Scanner** と同様ですが、より柔軟な設定が可能です。また **SpIDer Guard** は、実行中のプロセス内にウイルスと思われる活動が無いか常にモニターし、検出した場合は悪意のあるプロセスをブロックしてユーザーに報告します。

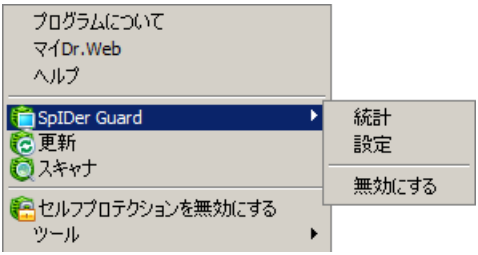
また **Dr.Web Anti-virus for servers** に含まれている **SpIDer Guard** は感染したオブジェクトを検出すると、デフォルト設定では アクションタブ で指定されたアクションを実行します。

該当する設定の変更を行うことでウイルスイベントに対するプログラムのアクションを指定することが可能です。**統計**ウインドウとログファイルによってそれらを管理することができます。

Dr.Web Anti-virus for servers と **MS Exchange Server** の間に互換性がない可能性があります。問題が発生した場合は、**SpIDer Guard** の例外リストにMS Exchange Serverデータベースとトランザクションログを追加します。

5.1. SpIDer Guard の管理

SpIDer Guard のメニューにはその設定および管理のためのメインツールが含まれています。



統計 は、セッション中の **SpIDer Guard** の動作に関する情報（検査されたオブジェクト数、感染した、または疑わしいオブジェクト数、実行されたアクションなど）を含むウインドウを開きます。

設定 は、プログラムの設定可能なパラメータが表示されます（詳細は SpIDer Guard の設定 をご覧ください）。

無効にする ではプログラムを一時的に無効にすることができます（管理者権限を持つユーザーのみ）。

5.2. SpIDer Guard の設定

SpIDer Guard の調整可能な主なパラメータはウィンドウ左側にある **設定** パネル上に表示されています。ページ内で指定するパラメータに関するヘルプを見るには、そのページへ移り **ヘルプ**  をクリックします。

設定終了後、変更を保存するには **OK** ボタンを、変更をキャンセルするには **キャンセル** ボタンをクリックしてください。

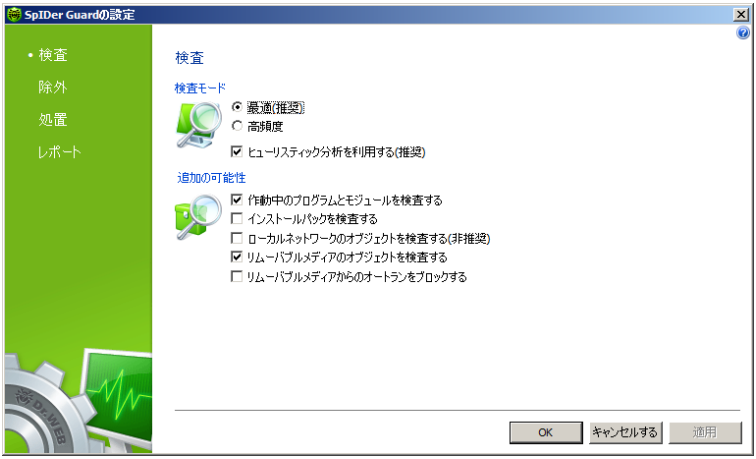
よく変更される設定は以下のとおりです。

検査

デフォルトでは **SpIDer Guard** の検査モードは **最適** に設定されています。ハードドライブ上で実行・作成・変更中のファイル、およびリムーバブルメディア上で開かれた全てのファイルが検査されます。

高頻度 モードでは、 **SpIDer Guard** はハードドライブ・リムーバブルメディア・ネットワークドライブ上で作成中・変更中・開かれているファイルをスキャンします。

ヒューリスティック分析を使用する のチェックボックスは、ヒューリスティックアナライザーモード（ウイルスに特有な動作の分析に基づいたウイルス検出モード）を有効にします。



いくつかの外付け記憶装置（USBポータブルハードディスクドライブ）はシステムによってハードドライブとして認識される可能性があります。そのため、このようなデバイスは特に慎重に使用する必要があり、接続時には スキャナ による検査を実行するようにしてください。

アーカイブの検査を無効にすると、例え **SpIDer Guard** が常時アクティブな状態であってもウイルスはコンピューターに侵入することが可能になりますがその検出は遅れます。感染したアーカイブの解凍時（または感染した画像を開く時）には感染したオブジェクトのハードドライブへの書き込みが行われますが、**SpIDer Guard** によって確実に検出されます。

追加の設定 では、以下のオブジェクトを検査するよう **SpIDer Guard** を設定することができます。

- 実行中のプロセスの実行ファイル（ロケーションに関係なく）
- インストールファイル
- ネットワークドライブ上のファイル
- リムーバブルデバイス上のファイルおよびブートセクター

これらのパラメータはいずれの検査モードでも適用されます。

また、**リムーバブルメディアからのオートランをブロックする** チェックボックスを選択すると、CD/DVDやフラッシュメモリーなどのポータブルデータストレージの自動再生

オプションを無効にすることができます。これにより、リムーバブルメディアを介して感染する恐れのあるウイルスからコンピュータを保護します。

自動起動オプションを設定したインストール中に問題が発生した場合は、**リムーバブルメディアからのオートランをブロックする**フラグのチェックを外すことを推奨しています。

除外

検査の対象から除外するフォルダとファイルを指定します。

除外されるフォルダとファイルのリスト フィールドで、検査の対象から除外するフォルダおよびファイルのリストを作成することができます。アンチウイルスの隔離フォルダ、いくつかのプログラムフォルダ、一時ファイル（スワップファイル）などを選択することが可能です。

ファイル、フォルダ、またはマスクをリストに追加するには、入力フィールドに名前を入力して **追加** をクリックしてください。既存のファイルやフォルダを加えるには **参照** をクリックし、オブジェクトを選択します。

リストから削除するには該当するファイルまたはフォルダを選択し **削除** をクリックします。

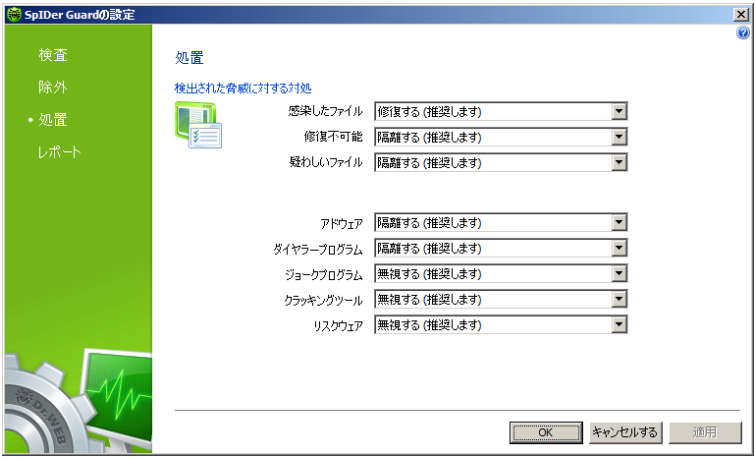
アクション

ここでは、感染したオブジェクトに対する **SpIDer Guard** のアクションを設定することができます。

修復、**無視**、**削除**、**隔離**アクションは スキャナ と同様です。ファイルに対する全てのアクションは 付録 B. コンピューター脅威と駆除手法 に記載されています。

SpIDer Guard のデフォルトアクションを変更する

1. **SpIDer Guard の設定** ウィンドウ内で **アクション** を選択します。



2. **感染したファイル** のドロップダウンリストで、感染したオブジェクトを検出した際のアクションを選択します。**修復** を推奨します。
3. **修復不可能** のドロップダウンリストで、修復できないオブジェクトを検出した際のアクションを選択します。**隔離** を推奨します。
4. **疑わしいファイル** のドロップダウンリストで、疑わしいオブジェクトを検出した際のアクションを選択します。**隔離** を推奨します。
5. **アドウェア** と **ダイヤラープログラム** のドロップダウンリストで、潜在的に危険なオブジェクトを検出した際のアクションを選択します。**隔離** を推奨します。
6. ジョークプログラム、リスクウェア、クラッキングツールを含むオブジェクトを検出した際のアクションも同様に設定できます。**無視** を推奨します。
7. 変更を適用し **SpIDer Guard の設定** ウィンドウを閉じるには **OK** をクリックしてください。

ログ

ここでは、ログの詳細レベルを設定することができます。

- **標準** – このモードでは、**SpIDer Guard** の最も重要な次のイベントのみを記録します。
  - 更新時刻
  - **SpIDer Guard** の起動および停止時刻
  - 検出された脅威およびエラー
- **アドバンス** – このモードでは、**SpIDer Guard** の最も重要なイベントおよび次の追加情報を記録します。
  - 検査されたオブジェクト
  - パッカー名
  - 検査された複合オブジェクト(アーカイブ、メールボックス、ファイルコンテナ)のコンテンツ

  SpIDer Guard によって最も頻繁に検査されているオブジェクトを確認したい場合にこのモードの使用を推奨します。
- **デバッグ** – このモードでは、**SpIDer Guard** の動作に関する全ての詳細な情報を記録します。ログファイルのサイズは大幅に増加します。

SpIDer Guard ログは %allusersprofile%\Application Data\Doctor Web\Logs\(Windows 7では %allusersprofile%\Doctor Web\Logs)フォルダ内にある spiderg3.log ファイルに保存されます。ログファイルは定期的に分析することを推奨します。

チャプター6 自動更新

Doctor Web のアンチウイルスソリューションは **Dr.Webウイルスデータベース** を使用してコンピューター脅威を検出します。データベースには、製品が発売された時点で既知である全てのウイルス脅威に関する詳細およびそのシグネチャが含まれています。しかし現代のコンピューター脅威はその進化と亜種作成の速さが特徴であり、数日、また時には数時間の間に新しいウイルスや悪意のあるプログラムが出現しています。感染の危険性を減らすため、**Doctor Web** はライセンスを所有するユーザーに対してウイルスデータベースおよび製品コンポーネントの定期的な更新をインターネット経由で配信しています。更新によって **Dr.Web Anti-virus for servers** は新しいウイルスを検出する為に必要な情報を受け取り、その拡散を防ぎます。また、更新前には修復不可能であった感染したファイルが修復されることもあり、更新によってアンチウイルスアルゴリズムが強化され、ソフトウェアやドキュメント内のバグが修正される場合もあります。

ライセンス有効期間中は、**Dr.Web Updater** を使用して更新をダウンロード・インストールすることができます。

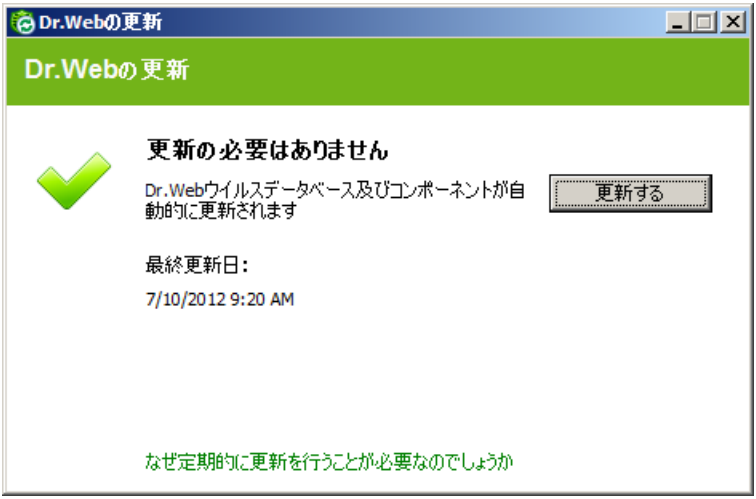
6.1. アップデーターの起動

アップデーター は次のいずれかの方法で起動することができます。

- **Dr.Web Anti-virus for servers** インストールフォルダ内にある drwupsrv.exe ファイルを実行することによってコマンドラインから
- **SpIDer Agent** メニューで **更新** を選択する

アップデーター が起動されると、**Dr.Webウイルスデータベース** および **Dr.Web Anti-virus for servers** コンポーネントに関する情報を表示するウィンドウが開きます。更新の設定は **Dr.Web Anti-virus for servers** 設定の **更新** ページで行います。

Dr.Web アップデーター を自動的に起動した場合、変更に関するログは %allusersprofile%\Application Data\Doctor Web\Logs\ フォルダ（Windows 7の場合 %allusersprofile%\Doctor Web\Logs\ ）内にある dwupdater.log ファイルに記録されます。



更新手順

更新を開始する前に アップデーター は、 キーファイル （ライセンスまたはデモ）の有無を確認し、キーファイルが見つからなかっ場合、ユーザー登録手続きの際にインターネット経由でキーを取得するよう提案します。

キーファイルが見つかった場合、アップデーター は **Doctor Web** サーバー上でのその有効性を確認します（ファイルが不法に配信されたものであると発覚した場合など、信用性に問題があった場合そのファイルはブロックされることがあります）。キーファイルがブロックされた場合、アップデーター は警告を表示し、更新を中断してDr.Webコンポーネントをブロックします。

キーがブロックされた場合は **Dr.Web Anti-virus for servers** を購入したディーラーに連絡してください。

キーファイルが正常に確認された後 アップデーター は、お使いの **Dr.Web Anti-virus for servers** のバージョンに応じた全ての更新ファイルを自動的にダウンロード・インストールします。新しいソフトウェアバージョンへのアップグレードが規約で許可されている場合、**Dr.Web Anti-virus for servers** の新しいバージョンがリリースされた際に アップデーター はそれもダウンロード・インストールします。

Dr.Web Anti-virus for servers の実行ファイルまたはライブラリの更新後、プログラムの再起動を要求されることがあります。その場合、アップデーターによって警告が表示されます。

スキャナ、**SpIDer Guard** は自動的に、更新されたデータベースを使用するようになっています。

アップデーター がコマンドラインモードで実行される場合はコマンドラインパラメーターを使用することができます（ 付録 A 参照）。

付録

付録 A. コマンドラインパラメーター

コマンドラインの追加パラメーター（キー）は、実行ファイルを開くことによって起動できるプログラムのパラメーターを設定するために使用されます。これらはスキャナ、コンソールスキャナ、 アップデーター に関連します。設定ファイルでは使用できないパラメーターを設定することができ、また設定ファイルで指定されたパラメーターよりも高いプライオリティを持ちます。

スイッチは、/ 記号で始まり、その他のコマンドラインパラメーター同様スペースで分けられます。

スキャナとコンソールスキャナパラメータ

/AA – 検出された脅威に対して自動的にアクションを適用します（スキャナ のみ）

/AR – アーカイブファイルを検査します。デフォルトで有効になっています。

/AC – インストールパッケージを検査します。デフォルトで有効になっています。

/AFS – アーカイブ内でパスを区切る際にスラッシュ(/)を使用します。デフォルトで無効になっています。

/ARC:*<圧縮率>* – オブジェクトの最大圧縮率。アーカイブの圧縮率が上限を超えた場合、コンソールスキャナ はアーカイブの解凍も検査も行いません（*無制限*）。

/ARL:*<レベル>* – 最大アーカイブレベル（*無制限*）

/ARS:*<サイズ>* – 最大アーカイブサイズ。アーカイブのサイズが上限を超えた場合、スキャナ はアーカイブの解凍も検査も行いません（*無制限*、KB）。

/ART:*<サイズ>* – **/ARC**に一致した最小アーカイブオブジェクト。圧縮率チェックが行なわれるアーカイブ内のファイルの最小サイズ（*無制限*、KB）。

/ARX:〈*サイズ*〉 – アーカイブオブジェクトの最大サイズ(*無制限*、KB)

/BI – ウイルスデータベースの情報を表示します。デフォルトで有効になっています。

/DR – ディレクトリを繰り返し検査します。デフォルトで有効になっています。

/E:〈*エンジン*〉 – **Dr.Web**エンジンの最大使用数

/FAST – システムのクイックスキャンを実行します(クイックスキャンについての詳細は 検査モード を参照してください)。(スキャナ のみ)

/FL:〈*パス*〉 – 指定したファイルに一覧表示されているファイルを検査します。

/FM:〈*マスク*〉 – 「マスク」に一致するファイルを検査します。デフォルトでは全てのファイルが検査されます。

/FR:〈*正規表現*〉 – 表現が一致するファイルを検査します。デフォルトでは全てのファイルが検査されます。

/FULL – 全てのハードドライブおよびリムーバブルメディア(ブートセクタを含む)のフルスキャンを実行します。(スキャナ のみ)

/H または **/?** – 該当するメッセージを表示します。(コンソールスキャナ のみ)

/HA – ヒューリスティック解析を使用します。デフォルトで有効になっています。

/KEY:〈*キーファイル*〉 – アクティベーションキーとして「キーファイル」を使用します(デフォルトでは C:\Program Files\DrWeb\ の drweb32.key またはその他適切なもの)。

/LITE – RAM、全てのディスクのブートセクタおよびスタートアップオブジェクトの基本的な検査を実行します。スキャナ はルートキットの検査も行います。(スキャナ のみ)

/LN – シェルリンクを解決します。デフォルトで無効になっています。

/LS – LocalSystemアカウントの権限を使用します。デフォルトで無効になっています。

/MA – メールに似たファイルを検査します。デフォルトで有効になっています。

/MC:〈*上限*〉 – 「上限」に指定した値を修復の最大試行回数として設定します（*デフォルトで無制限*）。

/NB – ファイルの修復、または削除のバックアップを行いません。デフォルトで無効になっています。

/NI[:X] – niceモード（0-100）、低リソース使用率（*無制限*、%）。

/NOREBOOT – 検査終了後に再起動またはシャットダウンを行いません。（スキャナ のみ）

/NT – NTFSストリームを検査します。デフォルトで有効になっています。

/OK – 感染していないファイルにOKを表示します。デフォルトで無効になっています。

/P:〈*優先度*〉 – 検査の優先度

0 – 最低
L – 低い
N – 通常、デフォルト設定
H – 高い
M – 最高

/PAL:〈*レベル*〉 – 最大圧縮レベル。デフォルト値は1000です。

/RA:<*file.log*> – file.logにログを追加します。デフォルトではログはありません

/RP:<*file.log*> – file.logにログを書き込みます。デフォルトではログはありません

/RPC:〈*秒*〉 – **Dr.Web Scanning Engine** の接続タイムアウト。デフォルトでは30秒です。（コンソールスキャナ のみ）

/RPCD – 動的RPC IDを使用します。（コンソールスキャナ のみ）

/RPCE – 動的RPCエンドポイントを使用します。（コンソールスキャナ のみ）

/RPCE:〈*名前*〉 – 指定したRPCエンドポイントを使用します。（コンソールスキャナ のみ）

/RPCH:〈*名前*〉 – リモートコールに指定したホスト名を使用します。（コンソール

スキャナ のみ）

/RPCP:*〈名前〉* – 指定したRPCプロトコルを使用します。使用可能なプロトコルは lpc、np、またはtcpです。（コンソールスキャナ のみ）

/QL – 全てのディスク上の隔離ファイルを一覧表示します。（コンソールスキャナ のみ）

/QL:*〈ドライブ〉* – 「ドライブ」（*文字*）ドライブ上の隔離されたファイルを一覧表示します。（コンソールスキャナ のみ）

/QR[:[d][:p]] – 「**p**」日（*数字*）以上経過した「**d**」（*文字*）ドライブ上の隔離ファイルを削除します。指定しなかった場合 「**p**」は0日、「**d**」は全てのドライブになります。（コンソールスキャナ のみ）

/QNA – ファイル名を常に二重引用符で囲みます。

/QUIT – スキャナ はコマンドラインで指定されたオブジェクト（ファイル、ディスク、フォルダ）の検査を実行し、自動的に終了します。（スキャナ のみ）

/REP – リパースポイントを使用します。デフォルトで無効になっています。

/SCC – 複合オブジェクトの内容を表示します。デフォルトで無効になっています。

/SCN – インストールパッケージ名を表示します。デフォルトで無効になっています。

/SPN – パッカー名を表示します。デフォルトで無効になっています。

/SLS – ログを画面を表示します。デフォルトで有効になっています。（コンソールスキャナ のみ）

/SPS – 画面に進捗を表示します。デフォルトで有効になっています。（コンソールスキャナ のみ）

/SST – ファイルの検査時間を表示します。デフォルトで無効になっています。

/TB – ブートセクタを検査します。デフォルトで無効になっています。

/TM – メモリー内のプロセスを検査します。デフォルトで無効になっています。

/TS – システム起動プロセスを検査します。デフォルトで無効になっています。

/TR – システム復元ポイントのディレクトリを検査します。デフォルトで無効になっています。

/W:*〈秒〉* – 最大検査時間（*無制限*、秒）。

/WCL – drwebwcl互換出力（コンソールスキャナ のみ）

/X:S[:R] – 電力の状態（シャットダウン、再起動、一時停止、休止状態など）を理由「**R**」（シャットダウンおよび再起動の場合）とともに設定します。

異なるオブジェクトに対するアクション（**C** - 修復、**Q** - 隔離、**D** - 削除、**I** - 無視、**R** - 通知。**R** は コンソールスキャナ のみで、デフォルトでは全てのオブジェクトに対して設定されています）:

/AAD:X – アドウェアに対するアクション（**R**、DQIR可）

/AAR:X – 感染したアーカイブファイルに対するアクション（**R**、DQIR可）

/ACN:X – 感染したインストールパッケージに対するアクション（**R**、DQIR可）

/ADL:X – ダイアラーに対するアクション（**R**、DQIR可）

/AHT:X – 侵入用ツールに対するアクション（**R**、DQIR可）

/AIC:X – 修復不可能ファイルに対するアクション（**R**、DQR可）

/AIN:X – 感染ファイルに対するアクション（**R**、CDQR可）

/AJK:X – ジョークプログラムに対するアクション（**R**、DQIR可）

/AML:X – 感染したメールファイルに対するアクション（**R**、QIR可）

/ARW:X – リスクウェアに対するアクション（**R**、DQIR可）

/ASU:X – 不審なファイルに対するアクション（**R**、DQIR可）

指定されたモードを無効／有効にする修飾子を持つことのできるパラメーターもあ

ります。

例:

/AC-　モードは無効になります。
/AC, **/AC+**　モードは有効です。

これらの修飾子は、あるモードがデフォルトで有効／無効になっている、または以前に設定ファイルで設定されている場合に便利です。修飾子を使用することができるパラメーターは次のとおりです。

/AR、**/AC**、**/AFS**、**/BI**、**/DR**、**/HA**、**/LN**、**/LS**、**/MA**、**/NB**、**/NT**、**/OK**、**/QNA**、**/REP**、**/SCC**、**/SCN**、**/SPN**、**/SLS**、**/SPS**、**/SST**、**/TB**、**/TM**、**/TS**、**/TR**、**/WCL**

/FL　パラメーターに"**-**"修飾子を使用すると、指定したファイルに一覧表示されているパスを検査した後そのファイルを削除します。

/ARC、**/ARL**、**/ARS**、**/ART**、**/ARX**、**/NI[:X]**、**/PAL**、**/RPC**、**/W**　パラメーター値に「0」を指定すると、無制限であることを意味します。

コンソールスキャナ でのコマンドラインパラメーター使用例です。

[*<ファイルへのパス>*]dwscancl /AR- /AIN:C /AIC:Q C:¥

C:ディスク上にある、アーカイブ内のものを除く全てのファイルを検査し、感染したファイルを修復し、修復不可能なものを隔離へ移動します。同様の動作を スキャナ に設定するには dwscancl の代わりに `dwscanner` を入力してください。

Dr.Web アップデーターコマンドパラメータ

一般オプション:

パラメータ	説明
-h [--help]	このメッセージの表示
-v [--verbosity] arg	ログレベル 設定可能な値: error, info, debug
-d [--data-dir] arg	レポジトリと設定があるフォルダ
--log-dir arg	ログファイル保存フォルダ
--log-file arg (=dwupdater.log)	ログファイル名
-r [--repo-dir] arg	レポジトリフォルダ (デフォルト <data_dir>/repo)
-t [--trace]	バックトレース有効
-c [--command] arg (=update)	実行コマンド: getversions, getcomponents, getrevisions, init, update, uninstall, exec, keyupdate
-z [--zone] arg	設定ファイルで指定したものの代わりに使用するゾーンのリスト

init コマンドパラメータ:

パラメータ	説明
-s [--version] arg	バージョン
-p [--product] arg	製品名
-a [--path] arg	製品フォルダへのパス デフォルトでは製品のコンポーネントが設置されます。また、Dr.Web アップデーターがキーファイルを検索するフォルダです。

パラメータ	説明
-n [--component] arg	コンポーネント名とインストールフォルダ *<名前>*, *<インストール パス>*
-u [--user] arg	プロキシサーバのユーザー名
-k [--password] arg	プロキシサーバのパスワード
-g [--proxy] arg	アップデートで使用するプロキシサーバ *<アドレス>*:*<ポート>*
-e [--exclude] arg	インストール時に除外するコンポーネント名

アップデートコマンドパラメータ:

パラメータ	説明
-p [--product] arg	製品名 指定した場合、指定製品のみアップデートします。 指定しなかった場合、全ての製品をアップデートします。 コンポーネントが指定された場合、指定コンポーネントのみアップデートします。
-n [--component] arg	指定バージョンにアップデートするコンポーネント *<名前>* , *<ターゲット バージョン>*
-x [--selfrestart] arg (=yes)	**Dr.Web アップデータ**でのアップデート後に再起動 デフォルトは`yes` `no` に設定された場合は再起動を促す通知を表示します。
--geo-update	アップデートの前にupdate.drweb.comからIPアドレスのリスト取得
--type arg (=normal)	以下のうちの1つを実行: • reset-all – 全てのコンポーネントのリビジョンを0にリセット • reset-failed – 失敗したコンポーネントのリビジョンを0にリセット

パラメータ	説明
	• normal-failed – 失敗したコンポーネントを含む全てのコンポーネントを、現在のリビジョンから最新か指定したリビジョンにアップデート • update-revision – 全てのコンポーネントを現在のリビジョンから最新にアップデート • normal – 全てのコンポーネントをアップデート
-g [--proxy] arg	アップデートで使用するプロキシサーバ *<アドレス>*:*<ポート>*
-u [--user] arg	プロキシサーバのユーザー名
-k [--password] arg	プロキシサーバのパスワード
--param arg	スクリプトに追加パラメータを渡す *<名前>*: *<値>*
-l [--progress-to-console]	コンソールにダウンロードとスクリプト実行の情報を表示

exec コマンドパラメータ:

パラメータ	説明
-s [--script] arg	このスクリプトを実行
-f [--func] arg	指定した場合は、スクリプトでこのファンクションを実行
-p [--param] arg	スクリプトに追加パラメータを渡す *<名前>*: *<値>*
-l [--progress-to-console]	コンソールにスクリプト実行の情報を表示

getcomponents コマンドパラメータ:

パラメータ	説明
-s [--version] arg	バージョン

パラメータ	説明
-p [--product] arg	製品を指定して、この製品に付属するコンポーネントのリストを取得 製品が指定されなかった場合は、そのバージョンの全てのコンポーネントをリストアップします。

getrevisions コマンドパラメータ:

パラメータ	説明
-s [--version] arg	バージョン
-n [--component] arg	コンポーネント名

uninstall コマンドパラメータ:

パラメータ	説明
-n [--component] arg	アンインストールするコンポーネント名
-l [--progress-to-console]	コンソールにコマンド実行の情報を表示
--param arg	スクリプトに追加パラメータを渡す *<名前>*: *<値>*
-e [--add-to-exclude]	削除されるコンポーネント 指定されたコンポーネントはアップデート実行されません。

keyupdate コマンドパラメータ:

パラメータ	説明
-m [--md5] arg	前のキーファイルのMD5ハッシュ値
-o [--output] arg	新しいキーファイル名
-b [--backup]	存在する場合は古いキーをバックアップ
-g [--proxy] arg	アップデートで使用するプロキシサーバ *<アドレス>:<ポート>*
-u [--user] arg	プロキシサーバのユーザー名
-k [--password] arg	プロキシサーバのパスワード
-l [--progress-to-console]	コンソールにダウンロード情報を表示

download コマンドパラメータ:

パラメータ	説明
--zones arg	ゾーンファイル
--key-dir arg	キーファイル保存フォルダ
-l [--progress-to-console]	コンソールにコマンド実行情報を表示
-g [--proxy] arg	アップデートで使用するプロキシサーバ *<アドレス>:<ポート>*
-u [--user] arg	プロキシサーバのユーザー名
-k [--password] arg	プロキシサーバのパスワード
-s [--version] arg	バージョン

パラメータ	説明
-p [--product] arg	製品名

リターンコード

リターンコードと対応するイベントは以下の通りです。

リターンコード	イベント
0	ウイルスは検知されませんでした
1	既知のウイルスが検知されました
2	ウイルスの亜種が検知されました
4	疑わしいオブジェクトが検知されました
8	アーカイブ、メールアーカイブ、コンテナ内に既知のウイルスが検知されました
16	アーカイブ、メールアーカイブ、コンテナ内にウイルスの亜種が検知されました
32	アーカイブ、メールアーカイブ、コンテナ内に疑わしいファイルが検知されました
64	少なくとも1つの感染オブジェクトの修復に成功しました
128	少なくとも1つの感染オブジェクト、もしくは疑わしいファイルを削除/名前変更/隔離しました

プログラムから返る実際の値は、スキャン中に発生したイベントのコードの合計値と同じです。合計値はそれぞれのイベントコードに分解して考えることができます。

例えば、リターンコード9の場合、9 = 1 + 8 と考えられます。これは、既知のウイルスが検知され、アーカイブ、メールアーカイブ、コンテナの何れかに含まれており、修復や他のアクションは実行されず、スキャン中にこれ以外のウイルスに関するイベントは発生しなかったことを意味しています。

付録 B. コンピューター脅威と駆除手法

コンピューター技術およびネットワークソリューションの発達に伴い、ユーザーに害をもたらす様々な悪意のあるプログラム（マルウェア）が益々広く拡散されるようになりました。その発達はコンピューターサイエンスと同時に始まり、そしてそれらに対抗するための保護技術もまた並行して進化してきました。しかしながら、そのようなプログラムの成長が予測できない性質のものであること、また適応される技術が常に改良されていることから、起こりうる全ての脅威に対する統一された分類は未だ存在しません。

マルウェアはインターネット、ローカルネットワーク、電子メール、リムーバブル情報メディアを経由して拡散されます。それらの中にはユーザーの不注意や経験のなさを悪用するものもあり、完全に自動モードで動作することができます。その他のものはハッカーによって操作されるツールであり、セキュリティの高いシステムにさえ危害を与えることができます。

このチャプターでは、最も一般的かつ広く拡散しているタイプのマルウェアについて説明します。**Doctor Web** 製品はそれらのマルウェアに対抗するためのものです。

コンピューター脅威の分類

コンピューターウイルス

この種類のコンピューター脅威は、他のオブジェクト内にそのコードを挿入する（これを感染と呼びます）ことが出来るという特徴を持っています。多くの場合、感染したファイルはそれ自体がウイルスのキャリアとなり、また挿入されたコードは必ずしもオリジナルのものと一致するとは限りません。ほとんどのウイルスは、システム内のデータを破損させる、または破壊する目的を持っています。オペレーションシステムのファイル（通常、実行ファイルとダイナミックライブラリー）を感染させ、ファイルが起動されると同時にアクティブになるウイルスはファイルウイルスと呼ばれています。

ディスクのブートレコード、ハードディスクドライブのパーティションまたはマスターブートレコードを感染させるウイルスはブートウイルスと呼ばれます。メモリをほとんど消費せず、システムがロールアウト、再起動、またはシャットダウンするまで、そのタスクを続行出来る状態を保ちます。

マクロウイルスはMicrosoft Office、およびマクロコマンド（通常、Visual Basicで記述されている）に対応しているその他のアプリケーションで使用されるドキュメントを

感染させるウイルスです。マクロコマンドは、完全なプログラミング言語で書かれた埋め込み型のプログラムで、例えばMicrosoft Wordでは、ドキュメントを開く（または閉じる、保存するなど）と自動的にマクロが開始されます。

コンピューターが特定の状態（例えばある特定の日時など）に達するとアクティブ化し、ウイルス作成者によって指定された活動を実行することができるウイルスをメモリ常駐型ウイルスと呼びます。

多くのウイルスは検出に対抗する何らかの手段を持ち、その手法は常時改良され続けています。しかしそれと同時に、それらに対抗するための技術も開発されています。

例えば暗号化ウイルスは、ファイル、ブートセクター、メモリ内で検出されるのを防ぐため、感染の度に自身のコードを暗号化します。このウイルスのコピーは全て、ウイルス署名として使用可能な共通のコードフラグメント（復号化プロシージャ）のみを含んでいます。

ポリモーフィック型ウイルスも同様に自身のコードを暗号化しますが、各コピーごとに異なる特別な復号化プロシージャの生成も行います。つまり、この種類のウイルスはシグネチャバイトを持ちません。

ステルスウイルスはその活動を偽り、感染したオブジェクト内に潜むための動作を実行します。この種類のウイルスは、感染させる前のオブジェクトの情報を「ダミー」として表示させ、改変したファイルが検出されないようにします。

また、ウイルスは記述された言語（ほとんどの場合アセンブラ、高級プログラミング言語、スクリプト言語など）、または感染させるOSに応じて分類することも出来ます。

コンピューターワーム

ワームは、ウイルスやその他のコンピューター脅威よりも多く見られるようになってきています。ウイルス同様、自身を複製し拡散することが出来ますが、他のプログラムを感染させることはできません。ワームは、インターネットまたはローカルネットワークからコンピューターに侵入し（通常、電子メールの添付経由で）、ネットワーク内にある他のコンピューターに自身の機能のコピーを配信します。ユーザのアクションに応じて、または攻撃するコンピューターを自身で選択し自動モードで拡散を開始します。

ワームは1つのファイル（ワームのボディ）から成っているとは限りません。多くのワームが、メインメモリ（RAM）内にロードした後にワームのボディを実行ファイルとしてネットワーク経由でダウンロードする感染部分（シェルコード）を持っています。シェルコード

がシステム内に存在するだけであれば、システムを再起動することで（RAMが削除されリセットされます）ワームを削除することが出来ますが、ワームのボディがコンピューターに侵入してしまった場合はアンチウイルスプログラムのみが対処可能です。

ワームはその集中的な拡散によって、例えペイロードを持っていない（直接的な被害を与えない）場合でも、ネットワーク全体の機能を破壊する能力を持っています。

トロイの木馬

このタイプの悪意のあるプログラムは自身を複製せず、他のプログラムを感染させません。トロイの木馬は頻繁に使用されるプログラムに成り代わり、その機能を実行します（または動作を模倣します）。同時に、システム内で悪意のある動作（データを破損または破壊、機密情報を送信など）を実行したり、ハッカーが許可無しにコンピューターにアクセス（例えば第三者のコンピューターに損害を与えるために）することを可能にします。

トロイの木馬の悪意のある特徴はウイルスのものと類似しており、また、それ自体がウイルスの構成要素にもなりえます。しかしほとんどのトロイの木馬は、ユーザまたはシステムタスクによって起動される別の実行ファイルとして配布されます（ファイル交換サーバ、リムーバブルストレージ、メール添付ファイルなどを介して）。

ルートキット

その存在を隠す目的で、OSのシステム機能を妨害するように設計された悪意のあるプログラムです。さらに、他のプログラムのタスク、異なるレジストリキー、フォルダ、ファイルを隠ぺいすることもできます。ルートキットは独立したプログラムとして、または他の悪意のあるプログラムに含まれるコンポーネントとして拡散します。基本的に、クラッカーがアクセス可能になったシステム上にインストールされるユーティリティのセットです。

ルートキットはその動作モードによって2つのグループに分けられます。ユーザモードで動作するユーザモードルートキット（UMR）と、カーネルモードで動作するカーネルモードルートッキット（KMR）です。UMRはユーザモードライブラリ機能を妨害し、一方、KMRはシステムのカーネルレベルで機能を妨害し、自身の検出を困難にします。

侵入用ツール

侵入用ツールは、侵入者によるハッキングを可能にするプログラムです。最も一般的なものは、ファイアーウォールまたはその他のコンピューター保護システムコンポーネントの脆弱性を検出するポートスキャナです。それらのツールはハッカーだけでは

なく、管理者がネットワークのセキュリティを検査するためにも用いられます。ハッキングに使用することの出来る一般的なソフトウェアや、ソーシャルエンジニアリングテクニックを使用する様々なプログラムも侵入用ツールに含まれることがあります。

スパイウェア

このタイプの悪意のあるプログラムはシステムの監視を行い、収集した情報を第三者（プログラムの作成者またはその関係者）に送信します。そのような第三者と成り得るのはスパムや広告の配信者、詐欺者、マーケティングエージェント、スパムエージェント、犯罪グループ、産業スパイなどです。

スパイウェアは他のソフトウェアと一緒に、または特定のHTMLページやポップアップ広告のウインドウを閲覧した際に密かにシステムロードされ、ユーザーの許可なしに自身をインストールします。このプログラムによる副次的な症状はブラウザ操作が不安定になり、システムパフォーマンスが低下することです。

アドウェア

通常、ユーザの画面に強制的に広告を表示させるフリーウェアプログラム内に組み込まれたプログラムコードを指します。ただしそのようなコードは、他の悪意のあるプログラム経由で配布されてWebブラウザ上に広告を表示させる場合もあります。アドウェアプログラムの多くは、スパイウェアによって収集されたデータを用いています。

ジョークプログラム

アドウェア同様、このタイプの悪意のあるプログラはシステムに対して直接的な被害を与えることはありません。ジョークプログラムは通常、実際には起こっていないエラーに関するメッセージを表示させ、データの損失につながるアクションの実行を要求します。その目的はユーザを驚かせ不快感を与えることにあります。

ダイアラー

広範囲に渡る電話番号をスキャンし、モデムとして応答するものを見つける為の特別なコンピュータープログラムです。その後、攻撃者がその番号を使用することによって被害者に通話料の請求書が送られます。または被害者が気づかぬうちに、モデム経由で高額な電話サービスに接続されます。

上記全てのタイプのプログラムは、ユーザのデータまたは機密情報を危険にさらすため悪意があるものとみなされます。姿を隠さないプログラム（スパム配信ソフトウェアや様々なトラフィックアナライザなど）は、状況によっては脅威と化す可能性はありますが、通常はコンピューター脅威とみなされません。

その他のプログラムの中にリスクウェアに分類されるものがあります。これらは害をもたらすために作成されたわけではないものの、その機能によってシステムセキュリティに対する脅威となる可能性を持っています。リスクウェアプログラムはデータを破損または削除してしまう可能性があるのみならず、クラッカーや悪意のあるプログラムによってシステムに被害を与える為に使用されることがあります。そのようなプログラムの中には、様々なリモートチャットおよび管理ツール、FTPサーバなどがあります。

以下は、ハッカーによる攻撃またはインターネット詐欺の一覧です。

- **ブルートフォースアタック** – 特別なトロイの木馬によって実行されます。内蔵されたパスワード辞書を利用して、またはランダムな文字列を作成することで、ネットワークにアクセスするためのパスワードを順番に試す攻撃方法です。
- **DoS攻撃**（サービス拒否）または **DDoS攻撃**（分散サービス拒否）– テロに近いネットワーク攻撃で、攻撃されるサーバーに対して膨大な数のサービスリクエストを送信します。受信するリクエストが一定の量（サーバーハードウェアの能力による）に達するとサーバーはそれらを処理できなくなりサービスを拒否するようになります。DDoS攻撃は、1つのIPアドレスからリクエストを送信するDoS攻撃とは異なり同時に大量のIPアドレスから攻撃を行います。
- **メールボム** – 単純なネットワーク攻撃で、コンピューターまたは企業のメールサーバーに大容量のメールを1通（または小容量のメールを数千通）送信し、システム障害を引き起こします。Dr.Webのメールサーバー向けアンチウイルス製品はそのような攻撃に対抗するための特別な保護メカニズムを持っています。
- **スニッフィング** – 「ネットワークの受動的な盗聴」とも呼ばれるネットワーク攻撃の一種です。パケットスニッファと呼ばれる悪意の無い特別なプログラムによって実行される、データおよびトラフィックフローの許可されていないモニタリングです。パケットスニッファは監視しているドメインのネットワークパケットを全て捉えます。
- **スプーフィング** – 接続を偽装することにより、ネットワークへのアクセスを取得するネットワーク攻撃の一種です。
- **フィッシング** – アクセスパスワード、銀行やIDカードの情報といった個人データや機密データを盗むためのインターネット詐欺手法です。犯罪者はスパムメールやメールワームを使って、正規の組織からと思われる偽のメッセージを被害者に送信します。このメッセージで被害者は、犯罪者によって予め作られた組織の偽のサイトを訪れ、パスワードやPIN番号、その他の個人情報を確認するよう促されます。これらのデータは犯罪者が被害者のアカウントからお金を盗むために、またはその他の犯罪に利用されます。
- **ヴィッシング** – フィッシングの一種ですが、電子メールの代わりにウォーダイアラーやVoIPが使用されます。

脅威に対するアクション

コンピューター脅威を駆除する方法には様々なものがあります。**Doctor Web** はコンピューターとネットワークに対する最も信頼できる保護を実現するためにそれらの手法を組み合わせ、柔軟でユーザフレンドリーな設定および確かなセキュリティのための総括的なアプローチを使用しています。悪意のあるプログラムを駆除するための主なアクションは以下のとおりです。

修復 – ウイルス、ワーム、トロイの木馬に対して適用されるアクションです。感染したオブジェクトから悪意のあるコードを削除、悪意のあるプログラムのコピーを削除、そして可能であればオブジェクトを復元（オブジェクトを感染前の構造および動作に戻す、など）します。　悪意のあるプログラムが全て修復可能なわけではありませんが、**Doctor Web** は他のアンチウイルスソフトに比べより効果的な修復およびファイル復元のアルゴリズムを使用しています。

隔離 – 悪意のあるオブジェクトを特別なフォルダに移し、残りのシステムから隔離します。このアクションは修復が不可能な場合、また全ての疑わしいオブジェクトに適しています。そのようなファイルのコピーは解析の為 **Dr.Web ウイルスラボ** に送信することを推奨します。

削除 – コンピューター脅威を駆除する最も効果的なアクションで、あらゆる種類の悪意のあるオブジェクトに対して適用可能です。このアクションは、修復アクションが選択されているオブジェクトに対して適用されることがあり、これはオブジェクトが悪意のあるコードのみで構成され有益な情報を持っていない場合（例えばコンピューターワームの修復は、そのコピーを全て削除することを意味します）に起こります。

ブロック、名前の変更 – これらのアクションも悪意のあるプログラムを駆除するために使用されます。ただし、そのようなプログラムの動作可能なコピーはファイルシステム内に残ることになります。ブロックアクションでは、それらのファイルからのまたはファイルへのアクセスを全てブロックします。名前の変更アクションでは、ファイルが操作されないようその拡張子を変更します。

付録 C. ウイルスの名称

Dr.Webウイルスラボ のスペシャリストによって、集められたコンピューター脅威のサンプル全てに名前が付けられます。これらの名称はある特定の原則に基づき、また脅威の構造・脆弱性のあるオブジェクトの分類・拡散環境（OS、アプリケーション）およびその他の特徴を反映しています。そのような原則を知ることは、保護するシステム上のソフトウェアや脆弱性を理解する上で有益となるでしょう。この分類方法は、同時に複数の特徴を有するウイルスもあることから形式的になる場合があり、また全てを網羅したものではありません。新しい種類のウイルスが次々と出現し続け、その分類は正確さを増していくためです。ウイルスの分類に関する詳細は Dr.Web公式サイト を参照してください。

ウイルスの完全な名称はピリオドで区切られた複数の要素から成り、プレフィックスおよびサフィックスの使用が一般的です。**Dr.Web** が使用するプレフィックスとサフィックスのグループ別リストを以下に掲載します。

プレフィックス

対象OS

以下のプレフィックスは特定のOSの実行ファイルを感染させるウイルスの名称に使用されます。

- Win – Windows 3.1の16ビットプログラム
- Win95 – Windows 95/98/Me の32ビットプログラム
- WinNT – Windows NT/2000/XP/Vista の32ビットプログラム
- Win32 – Windows 95/98/Me および NT/2000/XP/Vista の32ビットプログラム
- Win32.NET – Microsoft .NET Framework オペレーティング環境のプログラム
- OS2 – OS/2 プログラム
- Unix – 様々なUNIXシステムのプログラム
- Linux – Linux のプログラム
- FreeBSD – FreeBSD のプログラム
- SunOS – SunOS（Solaris）のプログラム
- Symbian – Symbian OS（モバイル OS）のプログラム

感染対象以外のシステム用プログラムであっても感染させることのできるウイルスも

ありますので注意してください。

マクロウイルス

以下のプレフィックスは、MS Officeのオブジェクトを感染させるマクロウイルスの名称に使用されます（そのようなウイルスに感染したマクロの言語が指定されます）。

- WM – Word Basic (MS Word 6.0-7.0)
- XM – VBA3 (MS Excel 5.0-7.0)
- W97M – VBA5 (MS Word 8.0)、VBA6 (MS Word 9.0)
- X97M – VBA5 (MS Excel 8.0)、VBA6 (MS Excel 9.0)
- A97M – MS Access'97/2000 のデータベース
- PP97M – MS PowerPoint のプレゼンテーションファイル
- O97M – VBA5 (MS Office'97)、VBA6 (MS Office 2000) このウイルスはMS Officeの複数のコンポーネントファイルに感染します。

開発言語

C、C++、Pascal、Basicなどの高級プログラミング言語で記述されたウイルスの名称には HLL グループが使用されます。

- HLLW – ワーム
- HLLM – メールワーム
- HLLO – 感染対象プログラムのコード書き換えウィルス
- HLLP – 寄生ウイルス
- HLLC – コンパニオンウイルス

以下のプレフィックスも開発言語に関するものです。

- Java – Java仮想マシンに対するウイルス

スクリプトウイルス

以下のプレフィックスは異なるスクリプト言語で記述されたウイルスに使用されます。

- VBS – Visual Basic Script
- JS – Java Script
- Wscript – Visual Basic Script および／または Java Script
- Perl – Perl

- PHP – PHP
- BAT – MS-DOS コマンドインタプリタ

トロイの木馬

- Trojan – トロイの木馬に対する総称。多くの場合、このグループのプレフィックスは Trojan プレフィックスと一緒に使用されます。
- PWS – パスワードを盗むトロイの木馬
- Backdoor – RAT機能のあるトロイの木馬（Remote Administration Tool – リモート管理ユーティリティー）
- IRC – Internet Relay Chat チャンネルを使用するトロイの木馬
- DownLoader – 様々な悪意のあるプログラムをインターネット経由で秘密裡にダウンロードするトロイの木馬
- MulDrop – ウイルスを含むファイルをインターネット経由で秘密裡にダウンロードするトロイの木馬
- Proxy – 第三者に対し、感染したコンピューターを通じてインターネット上で匿名で作業することを可能にするトロイの木馬
- StartPage（Seeker） – ブラウザのホームページ（スタートページ）のアドレスを許可なくすり替えるトロイの木馬
- Click – ユーザのブラウザを特定のサイト（または複数のサイト）にリダイレクトするトロイの木馬
- KeyLogger – キーストロークを追跡記録し、収集された情報を犯罪者に送信するスパイウェアトロイの木馬
- AVKill – アンチウイルスプログラムやファイアーウォールなどを終了させる、または削除します
- KillFiles、KillDisk、DiskEraser – 特定のファイル（ドライブ上の全てのファイル、特定のフォルダ内にあるファイルなど）を削除します
- DelWin – Windows OS の動作に必要なファイルを削除します
- FormatC – C ドライブをフォーマットします
- FormatAll – 全てのドライブをフォーマットします
- KillMBR – マスターブートレコード（MBR）を破壊または削除します
- KillCMOS – CMOS メモリを破壊または削除します

ネットワーク攻撃ツール

- Nuke – OSの既知の脆弱性を利用してシステムを異常終了させるためのツール
- DDoS – DDoS攻撃（Distributed Denial Of Service）を実行するためのエージェントプログラム

- FDoS（Flooder）– DDoS攻撃の手法を利用してインターネット上で悪意のある動作を実行するためのプログラム。1つのシステムに対して複数のエージェントから同時に攻撃を行うDDoSと異なり、FDoSプログラムは1つの独立したプログラムとして動作します。

悪意のあるプログラム

- Adware – 広告プログラム
- Dialer – ダイアラープログラム（モデムを登録された有料の番号、または有料のリソースにリダイレクトする）
- Joke – ジョークプログラム
- Program – 潜在的に危険なプログラム（リスクウェア）
- Tool – ハッキングに使用されるプログラム（侵入用ツール）

その他

- Exploit – OSやアプリケーションの脆弱性を悪用し、悪意のあるコードを埋め込んだり許可されていないアクションを実行するツール
- Generic – 環境や開発方法を示す他のプレフィックスの後に付けられるプレフィックスで、この種類のウイルスとして典型的なものであることを示します。特徴的な機能（文字列や特殊な動作など）を持たないウイルスに名前を付ける際に使用されます。
- Silly – 特徴を持たないウイルスに対し、異なる修飾子と共に過去において使用されていました。

サフィックス

サフィックスはいくつか特定のウイルスの名称に使用されます。

- Origin – *Origins Tracing* アルゴリズムを使用して検出されたオブジェクトに付けられるサフィックス
- generator – ウイルスではなくウイルスを作成するジェネレータ
- based – ウイルスジェネレータによって作成されたウィルス、または変更が加えられたウィルス。どちらの場合においてもこの種類の名称は全般的であり、数百、時には数千のウイルスを定義します。
- dropper – ウイルスではなくウイルスのインストーラー

付録 D. テクニカルサポート

Dr.Web 製品の有償版を購入されたカスタマーはサポートサービスをご利用いただけます。http://support.drweb.co.jp/ の **Doctor Web テクニカルサポート** をご覧ください。

製品のインストールまたは使用に関する問題が発生した場合、以下の **Doctor Web** サポートオプションをご利用ください。

- http://download.drweb.co.jp/ から最新のマニュアルおよびガイドをダウンロードして見る
- http://support.drweb.co.jp/ で、よくある質問を見る
- http://forum.drweb.com/ で、Dr.Web official forum（英語、ロシア語）を参照する

問題が解決しなかった場合、サポートサイト http://support.drweb.co.jp/ の該当するセクションでwebフォームに入力し、直接 **Doctor Web テクニカルサポート** にお問い合わせください。

企業情報については、**オフィシャル Doctor Web ウェブサイト** http://company.drweb.co.jp/contacts/japan/ をご覧ください。