



Dr.WEB®

Anti-virus
for Windows

管理者ガイド

Defend what you create

© Doctor Web, 2003-2013. All rights reserved.

このドキュメントにある材料は、「ドクターウェブ」の所有物であり、製品の購入者が個人的な目的で使用する場合にのみ使用することができます。ネットワークリソースに掲載されている、あるいは通信チャンネルとマスコミを通じて伝達されたこのドキュメントのいかなる部分もコピーされてはならず、または情報源へのリンクなしでの個人的な目的で利用される以外の方法で利用してはなりません。

商標

Dr.Web, SplDer Mail, SplDer Guard, CureIt!, CureNet!, AV-desk, Dr.WEBロゴは、ロシアと(または)他の国々において登録されたDoctor Webの商標です。このドキュメントで言及されたその他の登録された商標、ロゴタイプ、会社名は、各社の商標です。

責任の制限

Doctor Webとそのディストリビューターは、いかなる状況においてもこのドキュメントにある間違いと(または)見落とし、それに関連して発生する製品の購入者への損害・損失に対して如何なる責任も負うものではありません。

Dr.Web Anti-virus for Windows

バージョン8.0

管理者ガイド

30.04.2013

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 R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 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貢献に
心より感謝いたします。**



目次

1. はじめに	7
1.1. このマニュアルについて	9
1.2. 表記規則	10
1.3. システム要件	11
1.4. ライセンス交付	12
1.4.1. キーファイル	12
1.4.2. キーファイルの取得	13
1.4.3. ライセンスの更新	15
1.5. ウイルスの検出手法	16
1.6. アンチウイルスの動作検査	17
2. Dr.Web Anti-virus のインストール	18
2.1. インストール手順	19
2.2. Dr.Web Anti-virus の再インストールと削除	27
2.3. キーファイルの取得	29
3. 開始する	31
3.1. Spl Der Agent	34
3.2. 一般設定	37
通知	38
Updater	41
アンチウイルスネットワーク	44
保護レベル	45
Dr.Web Cloud	47
レポート	48



隔離	51
プロキシサーバ	52
言語	54
セルフプロテクション	54
復元	55
3.3. ライセンスマネージャ	56
3.4. 隔離マネージャ	59
3.5. アンチウイルスネットワーク	61
4. Dr.Web Scanner	62
4.1. Scanner の動作	64
4.2. ウイルス検出時のアクション	67
4.3. Scanner の設定	69
4.4. コマンドラインモードでのスキャン	73
4.5. Console Scanner	74
4.6. Scannerの自動起動	74
5. Spl Der Guard	76
5.1. Spl Der Guard の管理	77
5.2. Spl Der Guard の設定	78
6. Spl Der Mail	82
6.1. Spl Der Mail の管理	84
6.2. Spl Der Mail の設定	85
7. Dr.Web for Outlook	91
7.1. Dr.Web for Outlook の設定	91
7.2. 脅威の検出	92
7.2.1. 脅威の種類	93
7.2.2. アクションの設定	93



7.4. ログイン	96
7.4.1. イベントログ	96
7.4.2. デバッグテキストログ	97
7.5. 統計	98
8. Dr.Web Firewall	99
8.1. Dr.Web Firewall の学習	99
8.2. Dr.Web Firewall の管理	104
8.3. Firewall の設定	107
8.3.1. アプリケーション	108
8.3.2. 親プロセス	114
8.3.3. インターフェイス	115
8.3.4. アドバンス	123
8.4. イベントログ	126
8.4.1. アクティブなアプリケーション	127
8.4.2. アプリケーションログ	128
8.4.3. パケットフィルターのログ	130
9. 自動更新	132
9.1. Updater の起動	132
付録	135
付録 A. コマンドラインパラメータ	135
Scanner 及び Console Scanner パラメータ	135
Dr.Web Updater コマンドラインパラメータ	141
付録 B. コンピュータ脅威と駆除手法	145
付録 C. ウイルスの名称	153
付録 D. テクニカルサポート	158



1. はじめに

Dr.Web Anti-virus for Windows 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、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** のモジュールの構造にあり、また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BMR OS/2®、Novell® NetWare®、Macintosh®、Microsoft Windows Mobile®、Andorid®、Symbian R、Unix R系システム (Linux®, FreeBSD R など)向けアンチウイルスがあります。

Dr.Web Anti-virus 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 は様々な望ましくないプログラム (アドウェア、ダイヤラ 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、お使いのコンピューター上から削除します。望ましくないプログラムの検出およびそれらのプログラムに含まれているファイルに対するアクションの実行には、標準的なアンチウイルスコンポーネントが使用されます。

Dr.Web Anti-virus 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イ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ワークエラ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スキャンを行います。コマンドラインでの実行も可能です (**Dr.Web Console Scanner for Windows**)。
- **SpIDer Guard® for Windows** – メインメモリ内に常駐し、ファイルとメモリの検査を行うアンチウイルスガードです。ウイルスと思われる活動を検出します。
- **SpIDer Mail® for Windows (Mail Guard)** – 電子メールに対するアンチウイルスガードです。コンピューターのメールクライアントからメールサーバーへのPOP3/SMTP/IMAP4/NNTPプロトコル (IMAP4はMAPv4rev1です)によるアクセスを監視し、メールクライアントがサーバーからメールを受信する前、またはメールサーバーへメールを送信する前にメールウイルスを検出し駆除します。
- **Dr.Web for Outlook** – Microsoft Outlookのメールボックスでウイルスを検査するプラグインです。



- **Dr.Web Firewall** – 許可されていない外部アクセスからコンピューターを守り、重要なデータがネットワークを介して流出することを防ぎます。
- **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ファイルの更新を受け取り、自動インストールを行います。
- **SpIDer Agent – Dr.Web Anti-virus** のコンポーネントの設定と管理を行うユーティリティです。



1.1. このマニュアルについて

このユーザー マニュアルには **Dr.Web Anti-virus** のインストール及び効果的な利用方法に関する情報が記載されています。

グラフィックインターフェース (GUI) に関する詳細な説明は、あらゆるコンポーネントからアクセス可能な **Dr.Web Anti-virus** のヘルプ内にあります。

このユーザーマニュアルには、**Dr.Web Anti-virus** のインストール方法、プログラムの使用方法、ウイルス脅威によって引き起こされた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、プログラムコンポーネントの標準的な動作モード (デフォルト設定での) についての説明になります。

付録 には、上級者ユーザーの為の **Dr.Web Anti-virus** 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、本マニュアル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/> で常時ご確認いただけます。



1.2. 表記規則

本マニュアルでは、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イス (GUI) のボタン及びその他のエレメントの名称や、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	Dr.Web 製品またはエポポーネットの名称
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、アプリケーションの出力例
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。 また、定義としての用語を示す場合もあります。
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

本ユーザー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イス
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 をインストールする前に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、コンピュータから他のアンチウイルスパッケージを全てアンインストールして下さい
- **Dr.Web Firewall** をインストールする場合は、他のファイアウォールをコンピュータからアンインストールして下さい

項目	要件
OS	32-bit プラットフォーム： <ul style="list-style-type: none">• Windows® XP (SP2または3)• Windows Vista®• Microsoft® Windows® 7• Microsoft® Windows® 8 64-bit プラットフォーム： <ul style="list-style-type: none">• Windows Vista®• Microsoft® Windows® 7• Microsoft® Windows® 8 Microsoftのオフィシャルサイトからシステムコンポーネントをダウンロード・インストールする必要がある場合があります。その場合、必要なコンポーネント及びダウンロードURLがプログラムによって通知されます。
ハードディスクの空き領域	Dr.Web Anti-virus コンポーネントに330 MB インストールの際に作成されるファイルは上記とは別に容量が必要になります。
CPU	i686互換
RAM	512 MB以上
その他	ウイルスデータベースと Dr.Web Anti-virus コンポーネントの更新のためのインターネット接続



1.4. ライセンス交付

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

Dr.Web Anti-virus 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詳細は [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。

- ユーザーが使用を許可されているコンポーネントの一覧
- ライセンス有効期限
- その他の制限 (プログラムの使用が許可されているコンピューターの台数など)

キーファイルには以下の3つの種類があります。

- **ライセンスキーファイル**は **Dr.Web** ソフトウェアと一緒に購入され、ソフトウェアの使用およびテクニカルサポートの利用を可能にします。ライセンスキーファイルのパラメータは、ソフトウェアの使用許諾契約に従って規定されます。またこのファイルには、ユーザーと製品の販売会社に関する情報も含まれています。
- **デモキーファイル**は、**Dr.Web** 製品を試用するためのものです。ソフトウェアの全機能は無償で利用できますが、期間は30日に制限されています。



同一コンピューターに対するデモキーファイルの交付は4月に1回のみとなります。

- 一時キーファイルは、インストールの際にライセンスキーファイル、またはデモキーファイルが提示されない場合に使用されます。このキーファイルでも **Dr. Web Anti-virus** コンポーネントの全機能を使用できますが、ライセンスキーファイルまたはデモキーファイルをインストールするまで更新は利用出来ません。また [SpIDer Agent](#) [メニュー](#) の **My Dr.Web** および **Update** 項目にはアクセスできなくなります。



キーファイルは、次の条件が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** に必要な全てのアンチウイルスポイ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** 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

ライセンスキーファイルは以下のいずれかの方法で取得することができます。

- [製品のインストール中に](#)
- [Doctor Web公式サイト](#) での手動での [製品の登録](#) によって
- 製品のディストリビューションキットに同梱
- 販売店から個別のデータキャリアとして提供

製品の [インストール](#) またはディストリビューションキットによって取得したキーファイルは自動的にインストールされます。他の方法で取得したキーファイルは、[インストール](#) する必要があります。

手動での登録によるキーファイルの取得



キーファイルの登録およびダウンロードにはインターネット接続が必要です。

ライセンスキーファイルを取得するには、製品のシリアル番号が必要です。シリアル番号をお持ちでない場合、[インストール時](#) にデモキーファイルのみ受け取ることができます。

1. インターネットブラウザを起動し、製品付属の登録カードに記載されているサイトにアクセスします。
2. 登録フォームにお客様情報を入力して下さい。
3. 登録カードに記載されているシリアル番号を入力して下さい。
4. ライセンスキーファイルが、登録フォームで指定した電子メールのZIPアーカイブの形で送信されます。登録後に、登録ページからライセンスキーファイル



ルをダウンロードすることもできます。WindowsではZIPアーカイブから自動的にファイルが展開されます。追加のソフトウェアを購入または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。

インストール時にキーファイルを取得



キーファイルの登録およびダウンロードにはインターネット接続が必要です。インストールの前に、コンピュータ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。登録手順の過程でデモキーファイルを受け取ることが出来ます。

1. インストール手順を開始します (**インストール手順** 参照)。
2. **キーファイル** のステップで **インストール中にファイルを取得します** を選択して下さい。
3. インストラクションに従って残りのインストール手順を進めて下さい。インストールが完了すると、キーファイルを取得する **手順** が開始されます。その手順が完了すると **Dr.Web Anti-virus** が自動的にライセンスキーファイルをダウンロード・インストールします。

キーファイルは key 拡張子を持つファイルまたはそのようなファイルを含むアーカイブとして配信されます。ユーザーはインストール時または初回の更新時に **Dr.Web Updater** 経由でキーファイルを受け取ることが出来ます。このユーティリティは公式サイト上でプログラム登録を行い(シリアル番号提示後)、キーファイルを取得します。この方法は個々のワークステーションを保護する **Dr.Web** プログラムでのみ使用可能です。シリアル番号が無い場合、ユーザーが入手できるのはデモキーのみになります (**キーファイルの取得** 参照)。

キーファイルは有効期限が切れるまで保存しておくことを推奨します。製品を再インストール、または複数のコンピュータにインストールする場合には初回の登録時に取得したキーファイルを使用することができ、再度シリアル番号を登録する必要はありません。



デモキーファイルは、登録を行ったコンピュータ上でのみ使用可能です。



再登録

キーファイルを紛失した場合は、前回の登録時に入力したのと同じ個人情報を入力し、再登録を行う必要があります。メールアドレスは別のものを使用することができ、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。



デモキーファイルの再登録では、前回の登録時に交付されたのと同じキーファイルが交付されます。

キーファイル取得の回数には上限があります。同じシリアル番号での登録は25回までです。この回数を超えてリクエストされてもキーファイルは送信されません。その場合、詳しく状況およびシリアル番号登録時に入力した個人情報を添えて [テクニカルサポート](#) までご連絡ください。



有効なキーファイル（ライセンスまたはデモ）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. ライセンスの更新

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の更新が必要となる場合があります。製品と一緒に新しいライセンスを登録してください。Dr.Web Anti-virus は、製品の動作を停止する必要や再インストールの必要のない、ライセンスの「オンラインアクセス」更新をサポートしています。

ライセンス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更新するために **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もできます。[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** 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. 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した検査を実行し、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. スキャンはまず、ファイルコードセグメントを既知のウイルスシグネチャ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 ウィルスデータベース** 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** は既知の感染メカニズムを用いる新種・亜種ウイルスを検出するための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** ユーザーは 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 のエラーを犯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 ウィルスラボ** 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。



1.6. 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。

アンチウイルスソフトウェアベンダーの多くは、動作確認の為に標準的なtest.comプログラムを使用しています。このプログラムは、インストールされたアンチウイルスのウイルスを検出した際の動作を、お使いのコンピューターセキュリティを危険にさらすことなくテストするために特別に設計されたものです。test.comプログラム自体はウイルスではありませんが、多くのアンチウイルスプログラムによってウイルスとして処理されるようになっています。**Dr.Web Anti-virus** は、この「ウイルス」を検出するとEICAR Test File (Not a Virus!) という通知を表示します。他のアンチウイルスプログラムも同様の方法でユーザーに通知を行います。

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

test.comのファイルは、次の文字列のみで形成されています。

```
X50!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として保存することで、「ウイルス」と認識される上記のようなプログラムを作成することができます。



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。ただし、そのようなファイルをシステム内でコピーまたは作成した場合は**SpIDer Guard** に検出され、デフォルト設定では **隔離** フォルダに移されます。



2. Dr.Web Anti-virus のインストール

インストールの前には以下の操作を行うことを強く推奨します。

- 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全てインストールして下さい(同社のサイト <http://windowsupdate.microsoft.com> からダウンロード、インストールすることができます)。
- システムユーティリティ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。
- 動作中のアプリケーションを全て閉じて下さい。



Dr.Web Anti-virus 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。

ご使用のコンピュータへの **Dr.Web Anti-virus** のインストールを開始するには、以下のいずれかを実行して下さい。

- 1つの実行ファイルとして提供されているファイルがある場合は、そのファイルを実行して下さい。
- CD/DVDドライブにディスクを挿入します。自動実行機能が有効になっている場合は、インストールが自動的に開始されます。自動実行機能が無効になっている場合は、ディストリビューションキットの実行ファイルを手動で実行して下さい。

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. インストール手順



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

Dr.Web Anti-virus 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. 通常モード

コマンドラインパラメータを使用したインストール

コマンドラインパラメータを使用して **Dr.Web Anti-virus** をインストールするには、実行ファイル名と必要なパラメータ(これらのパラメータはバックグラウンドモードでのインストール、インストール言語、インストール後の再起動、**Dr.Web Firewall** のインストールに關与します)をコマンドライン内に入力してください。

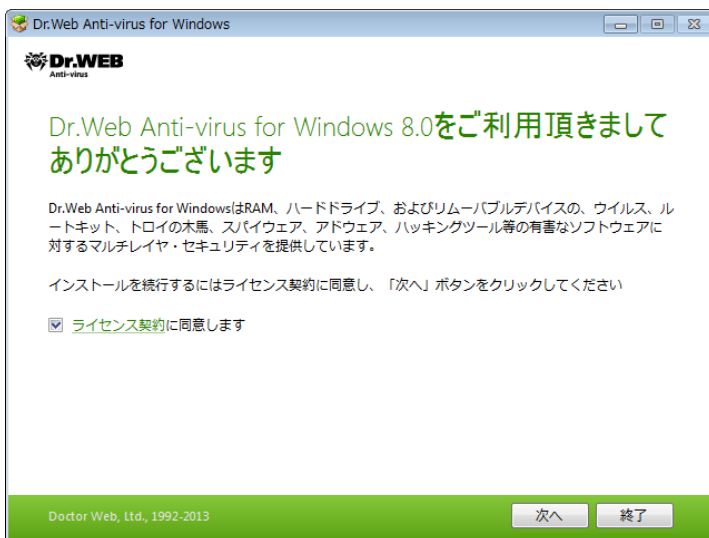
パラメータ	説明
reboot	インストール完了後にコンピューターを自動的に再起動
installFirewall	Dr.Web Firewall をインストール
lang	インストールに使用する言語。このパラメータの値は ISO 639-1 言語コードです。
silent	バックグラウンドモードでのインストール

例えば **Dr.Web Anti-virus** をバックグラウンドモードでインストールし、インストール後に再起動を行う場合は、次のコマンドを実行します。

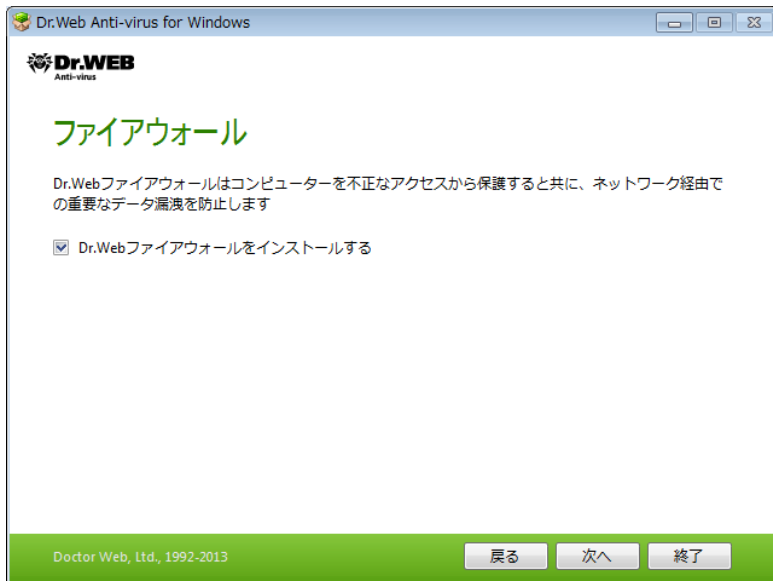
```
C:\Documents and Settings\drweb-800-win.exe /  
silent yes /reboot yes
```

通常インストール

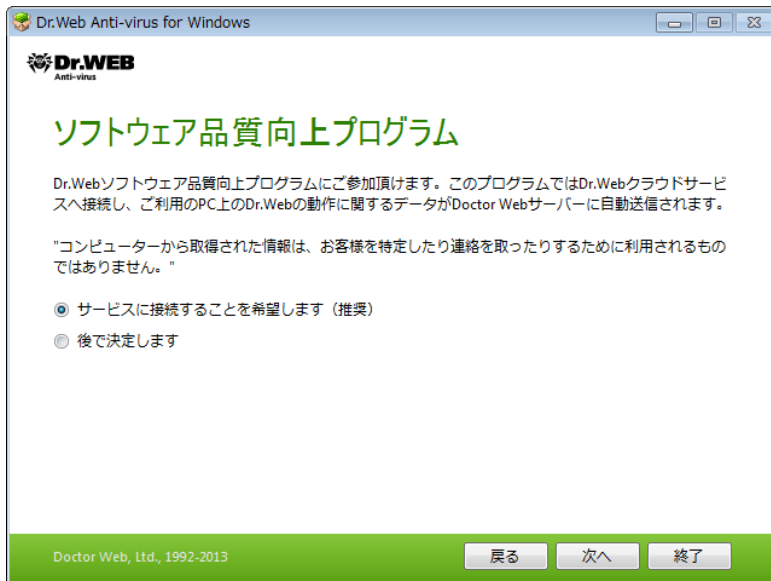
1. コンピューター上に他のアンチウイルスソフトウェアがインストールされていた場合、インストールウィザードは **Dr.Web Anti-virus** と他のアンチウイルス間の非互換性について警告し、その削除を勧めます。
2. 使用許諾契約書が表示されます。インストールを続行するには規約をお読みになり、同意して **次へ** をクリックしてください。



3. 次のウインドウで **Dr.Web Firewall** のインストールを勧められます。

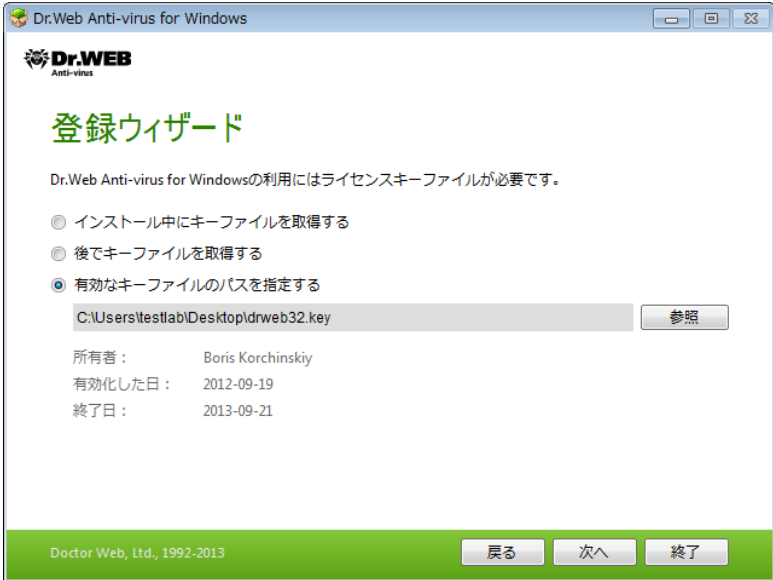


4. 次のステップでは、最新の情報を利用したWebサイトのチェックを可能にする **Dr.Web** クラウドサービスへの接続を勧められます。



5. **Dr.Web Anti-virus** の動作に必要なキーファイル (ライセンスまたはデモ)を要求するウィンドウが表示されます。以下の操作のうち、いずれか1つを実行してください。
- 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** をクリックしてキーファイルを選択してください。
 - インストールの間にキーファイルを取得する場合、**インストール中にキーファイルを取得する** を選択してください。
 - **一時キーファイル** を使用してインストールを続行する場合、**後でキーファイルを取得する** を選択してください。ライセンスまたはデモキーファイルをインストールするまで、更新は利用できません。

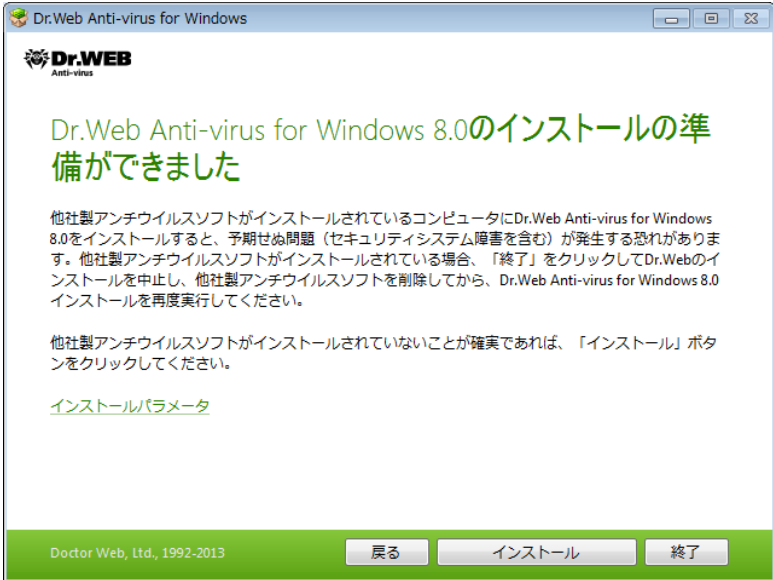
次へ をクリックします。



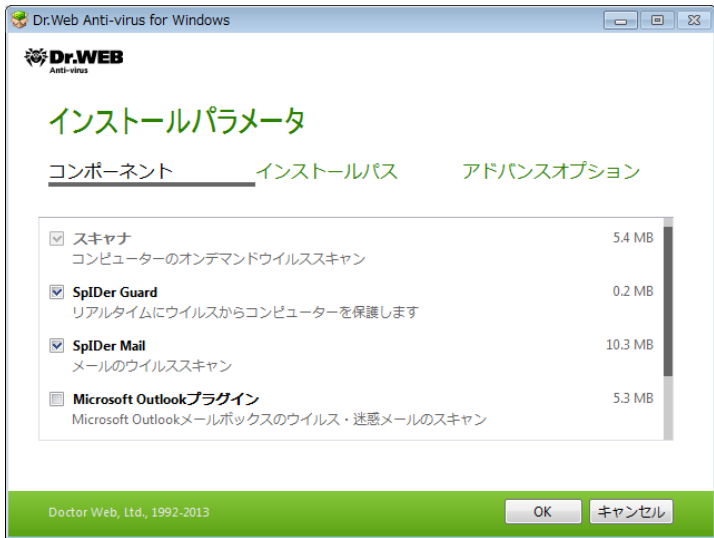
Dr.Web Anti-virus キーファイルのみを使用してください。このタイプのキーファイルは、**.key**拡張子を持っています。

6. プログラムのインストール準備が完了した旨の通知が表示されます。デフォルトのパラメータでインストールを開始するには **インストール** をクリックします。

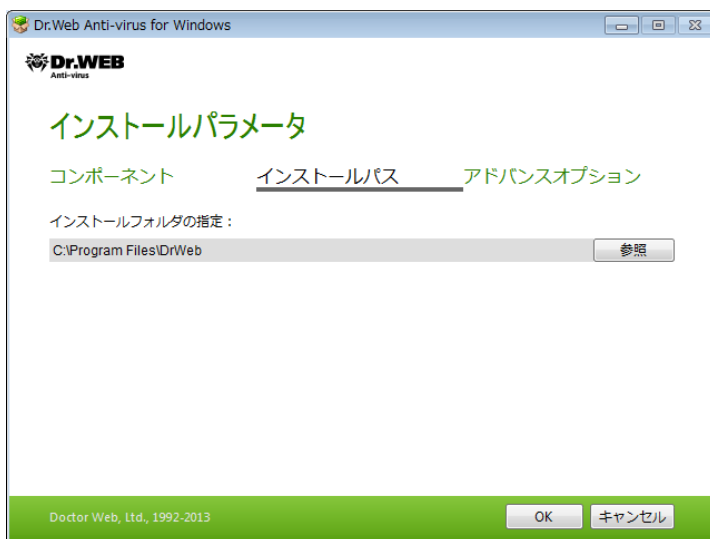
インストールするコンポーネントを選択するには、**インストールパス**及びその他の追加パラメータを指定して **インストールパラメータ** をクリックしてください。このオプションは上級者ユーザー向けです。



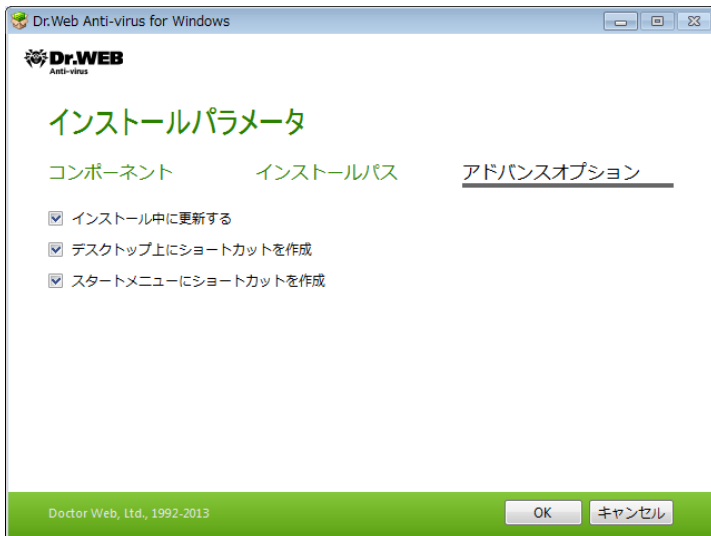
7. 先のステップで **インストール** をクリックした場合は、[step 10](#) に進んでください。それ以外の場合、**インストールパラメータ** ウィンドウが表示されます。1つ目のタブで、インストールするエポータントを指定します。



8. このタブではインストールパスを変更することができます。



- step 5 で有効なキーファイルを指定、または **インストール中にキーファイルを取得する** を選択した場合は、最後のタブで、ウイルスデータベース及びその他のプログラムコンポーネントに対する更新をダウンロードするための **インストール中に更新する** チェックボックスにチェックを入れることができます。また、このウィンドウでは **Dr.Web Anti-virus** へのショートカットを作成することも可能です。



インストールパラメータの調整が終了したら**OK** をクリックします。

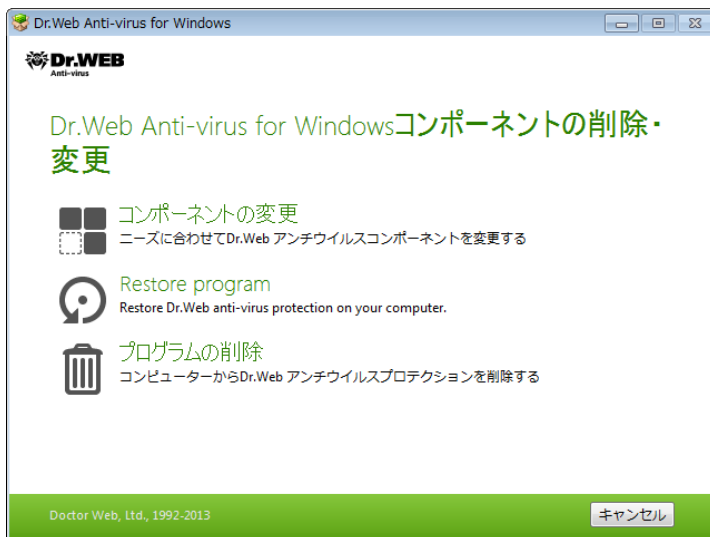
- step 5 で **後でキーファイルを取得する** を選択した場合、インターネット経由でキーファイルを取得する **手順** がここで開始されます。
- キーファイルを指定して、又はインストール中にキーファイルを受け取り step 9 で **インストール中に更新する** を選択した場合、及びデフォルトインストールの間には、ウィザードがウイルスデータベースおよび **Dr.Web Anti-virus** のコンポーネントを更新します。更新は自動的に開始され、ユーザーの操作は必要ありません。
- Dr.Web Firewall** のインストールを選択した場合、インストール完了後にコンピューターを再起動する必要があります。

2.2. Dr.Web Anti-virus の再インストールと削除

- Windowsの[プログラムと機能]でインストールウィザードを開始してください。
- 表示されたウィンドウで、インストールモードを選択してください。
 - インストールするコンポーネントを変更するには **コンポーネントの変更** を選択します。



- インストールされた全てのコンポーネントを削除するには **プログラムの削除** を選択します。



3. プログラム **Dr.Web Anti-virus** を削除する、またはインストールするコンポーネントを変更するには、ウインドウ内に表示される確認コードを入力する必要があります。
4. 削除またはコンポーネント変更の手順を完了するために、プログラムの指示に従ってコンピューターを再起動させてください。



2.3. キーファイルの取得

新しいキーファイルの登録手続きは、インストールの間に自動的に開始されるか、またはインストール完了後に **SpIDer Agent** メニューから行うことができます。この手続きによって **Doctor Web 公式サイト** に接続し、製品を登録することができます。

キーファイルを取得するには

1. 最初のステップで、取得する **キーファイルの種類** (ライセンスまたはデモ) を選択してください。

Dr.Web 製品購入の際に交付されたシリアル番号をお持ちの場合は **ライセンスキーファイル** を選択し、シリアル番号を入力して下さい。製品を試用目的でインストールした場合は **デモキーファイル** を選択し、step 2へ進んで下さい。



既に **Dr.Web Anti-virus for Windows** ユーザーである方は、新しいライセンスの期限を150日延長する特典を利用できる場合があります。登録したシリアル番号を入力するかライセンスキーファイルを提示してください。

次へをクリックします。登録情報を入力するウィンドウが開きます。

2. キーファイルの取得に必要な全てのフィールドを埋め、次へ をクリックしてください。

3. ライセンスキーを取得する手続きが開始されます。キーファイルが正常にダウンロードされると、ウィンドウにはメッセージとライセンスの有効期限が表示されます。ダウンロードに失敗した場合は、エラーメッセージが表示されます。



3. 開始する

インストールプログラムによって以下の **Dr.Web Anti-virus** コンポーネントをインストールすることができます。

- **Scanner** (GUIバージョン及びコンソールバージョン)
- **SpIDer Guard**
- **SpIDer Mail**
- **Dr.Web for Outlook**
- **ファイアーウォール**
- **自動更新ユーティリティ**
- **SpIDer Agent**

Dr.Web Anti-virus 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、統一された検出・駆除アルゴリズムを採用していますが、スキャン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。

例えば **Scanner for Windows** 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)をユーザーの指示またはスケジュールに応じてスキャンします。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スキャンされます。タスクの実行時をユーザーが選択するため、他の重要なプロセスに必要なリソースが足りなくなることを心配する必要がありません。

SpIDer Guard は、コンピュータのメインメモリ上に常駐し、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。このプログラムはハードドライブ上で実行・作成・変更されているファイル、またはムーバブルメディアおよびネットワークドライブ上で開かれた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スキャンレベルにより、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ほとんどありません。ただし、スキャン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。またウイルスの中には、その特殊な動作を基に **SpIDer Guard** のみが検出可能なものもあります。

SpIDer Mail も同様にメモリ内に常駐します。このプログラムは、メールクライアントからのPOP3/SMTTP/IMAP4/NNTPプロトコルによるメールサーバーへのアクセスを



全て監視し、メールクライアントがメールを受信(送信)する前にそれらをスキャンします。**SpIDer Mail** はコンピューターを経由するメールトラフィックをその時点で全て検査するように設計されているため、リソース消費を抑え、より効果的にメールボックスのスキャンを行うことが可能です。例えば、ユーザーのアドレス帳にあるアドレスに対する、ワーム自身のメールクライアントを使用して行われるメールワームコピーの大量送信をコントロールすることが可能です。また、**SpIDer Guard** によるメールファイルのスキャンを無効にすることもでき、コンピューターのリソース消費を大幅に削減することができます。

Dr.Web Firewall は不正アクセスからコンピューターを保護し、重要なデータがネットワークを介して漏えいすることを防ぎます。**Dr.Web Firewall** は接続の試行およびデータの送受信を監視し、望まない又は疑わしいアクセスをネットワークレベルおよびアプリケーションレベルの両方でブロックすることを可能にします。



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** 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スキャンレベル(最大)でスキャンする
- **SpIDer Guard** をデフォルト設定で使用する
- **SpIDer Mail** を使用してメールの完全なスキャンを実行する
- **Dr.Web Firewall** を使用して不明な接続を全てブロックする
- ウイルスデータベースの更新と同時に、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** が一時的に無効になっている状態で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更新が定期的に(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. Spl Der Agent

Dr.Web Anti-virus がインストールされると、タスクバーの通知領域に **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、動作中のエコーネット、最終更新日、ウイルスデータベース内のウイルスシグネチャ数に関するポップアップメッセージが表示されます。また設定 (下記参照) 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。

アイコンのコンテキストメニューで、**Dr.Web Anti-virus** エコーネッ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** のバージョンに関するウィンドウを開きます。

ライセンスを登録 の項目は、**Doctor Web** サーバーからキーファイルを取得するための **登録手続き** を開始します。

マイDr.Web の項目は、**Doctor Web 公式サイト** 上にあるユーザー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、シリアル番号など) の確認、ライセンスの更新、テクニカルサポート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** のヘルプを開きます。

SpIDer Guard、**SpIDer Mail**、**Updater** の項目は、該当するコンポーネントの管理、設定、統計

ウィンドウを開きます。

Scanner の項目は **Dr.Web Scanner** 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** ファイル、レジストリ、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。

デバッ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。
- 画像に表示されているテキストまたは **Dr.Web Anti-virus** のアクセスパスワードを入力します。

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](#)
- **Dr.Web Anti-virus** 及び特定のコンポーネントの [一般設定](#)
- [隔離マネージャ](#)
- [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、お使いのOS及び**Dr.Web Anti-virus**の動作に関する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。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**の切り替えが可能です。**ユーザーモード**ではコンポーネント設定にアクセスできず、また全てのコンポーネント及びセルフプロテクションを無効にすることもできません。**管理者モード**に切り替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、管理者権限のないユーザーとしてWindows XPS上にログインする場合や、Windows Vista、Microsoft Windows 7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。それ以外の場合、この項目は表示されず、**SpIDer Agent**のメニューから全ての機能にアクセスすることが出来ます。




3.2. 一般設定



Dr.Web Anti-virus 設定は ユーザー モードでは使用出来ません。

集中管理での設定調整によって、**Dr.Web Anti-virus** の一般設定、および **Scanner** を除くその全てのコンポーネントの設定を行うことが出来ます。

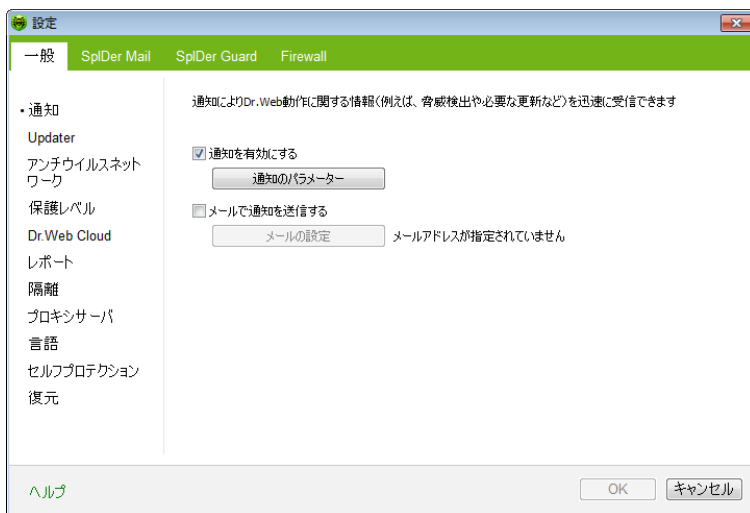
一般設定を行うには

1. Windows通知領域内で **SpIDer Agent** アイコン  をクリックしてください。
2. **ツール** を選択した後、**設定** を選択します。設定ウインドウが開き、一般タブに以下のページが含まれています。
 - **通知** - **Dr.Web Anti-virus** の通知設定
 - **Updater** - **Dr.Web Anti-virus** ウイルスデータベース及びコンポーネントの更新設定
 - **アンチウイルスネットワーク** - アンチウイルスネットワークの一部としての **Dr.Web Anti-virus** の動作を設定
 - **保護レベル** - バックグラウンドでのルートキットスキャンを有効にする。また、コンピュータのセキュリティを脅かす可能性のある動作に対する設定
 - **Dr.Web Cloud** - **Doctor Web** クラウドサービスへの接続
 - **レポート** - **Dr.Web Anti-virus** コンポーネントのイベントに関するロギングの設定
 - **隔離** - 感染した又は疑わしいファイルを隔離するための **隔離** の設定
 - **プロキシサーバ** - **Dr.Web Anti-virus** コンポーネントのインターネット接続パラメータを設定
 - **言語** - インターフェースで使用する言語を選択
 - **セルフプロテクション** - 追加のセキュリティ設定
 - **復元** - **Dr.Web Anti-virus** 設定のインポート及びエクスポート、デフォルト値への復元
3. 必要な設定を行います。セクション内の設定に関する情報は参照するには **ヘルプ** をクリックしてください。



通知

このページでは、タスクバーの通知領域内にある **SpIDer Agent** アイコン¹⁾ 上に表示されるポップアップ、及びメール通知のタイプを設定することができます。



通知の設定

1. 何らかの通知を受け取る場合は **通知を有効にする** チェックボックスにチェックを入れてください。
2. **通知のパラメーター** をクリックすると、受け取ることの出来る通知のリストが表示されます。



通知種別	デスクトップ	メール
SpIDer Guard		
脅威が検出されました	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SpIDer Gate		
URLがブロックされています	<input type="checkbox"/>	<input type="checkbox"/>
脅威が検出されました	<input checked="" type="checkbox"/>	<input type="checkbox"/>
ペアレンタルコントロール		
URLへのアクセスがブロックされています	<input type="checkbox"/>	<input type="checkbox"/>
オブジェクトへのアクセスがブロックされました	<input type="checkbox"/>	<input type="checkbox"/>
インターネット接続時間が切れました	<input type="checkbox"/>	<input type="checkbox"/>
コンピュータ使用時間が切れました	<input checked="" type="checkbox"/>	<input type="checkbox"/>
予防的保護		
セルフプロテクションの状態が変更されました	<input type="checkbox"/>	<input type="checkbox"/>
保護されるオブジェクトへのアクセスがプロ...	<input type="checkbox"/>	<input type="checkbox"/>
Firewall		

通知をフルスクリーンモードで表示しない
 フルスクリーンモードでファイアウォール通知を別の画面に表示する

ヘルプ OK キャンセル

- 受け取りたい通知のタイプのチェックボックスにチェックを入れてください。ポップアップ通知を表示させるには **デスクトップ** コラム内のチェックボックスを、メールでの通知を受け取るには **メール** コラム内のチェックボックスにチェックを入れます。
- 必要に応じて、次の追加的パラメータを設定してください。

チェックボックス	説明
通知をフルスクリーンモードで表示しない	コンピュータ上でアプリケーションがフルスクリーンモードで動作している場合 (ゲームや映画など) に通知を隠すには、このチェックボックスにチェックを入れてください。 モードに関係なく通知を表示させる場合はこのチェックボックスをクリアしてください。
フルスクリーンモードでファイアウォール通知を別の画面に表示する	コンピュータ上でアプリケーションがフルスクリーンモードで動作している場合 (ゲームや映画など) に ファイアウォール の通知を別のデスクトップ上に表示させるには、このチェックボックスにチェックを入れてください。



チェックボックス	説明
	アプリケーションがフルスクリーンモードで動作している同一デスクトップ上に通知を表示させる場合はこのチェックボックスをクリアしてください。

5. メール通知を選択した場合は、メール送信の**設定**を行ってください。
6. 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。

メール通知の設定

1. **通知を有効にする** チェックボックス、及び必要なメール通知が**通知のパラメーター** ウィンドウ内で選択されていることを確認してください。
2. **メールで通知を送信する** チェックボックスにチェックを入れます。
3. **メールの設定** をクリックすると、メールパラメータのウィンドウが開きます。



The image shows a dialog box titled "メールのパラメーター" (Email Parameters) with a close button in the top right corner. The dialog contains the following fields and options:

- メールアドレス** (Email Address): Input field containing "メールアドレス".
- SMTPサーバー** (SMTP Server): Input field.
- ポート** (Port): Input field containing "25".
- ログイン** (Login): Input field.
- パスワード** (Password): Input field with an eye icon for visibility toggle.
- セキュリティ** (Security): Dropdown menu set to "なし" (None).
- 認証** (Authentication): Dropdown menu set to "ベーシック" (Basic).
- テスト** (Test) button: Labeled "テストメッセージを送信する" (Send test message).
- Footer buttons: **ヘルプ** (Help), **OK**, and **キャンセル** (Cancel).



4. 以下のパラメータを指定してください。

オプション	説明
メールアドレス	通知の送信先アドレスを入力
SMTPサーバー	Dr.Web Anti-virus がメール通知送信に使用する送信 (SMTP)サーバーを入力
ポート	Dr.Web Anti-virus がメールサーバーへの接続に使用するポートを入力
ログイン	Dr.Web Anti-virus がメールサーバーへの接続に使用するログインを入力
パスワード	メールサーバーへの接続時に使用するログインパスワードを入力
セキュリティ	接続のセキュリティレベルを選択
認証	メールサーバーへの接続時に使用する認証方法を選択

- 設定したパラメータを使用してテストメッセージを送信するには **テスト** をクリックします。数分以内にメッセージを受信しなかった場合は接続設定を確認してください。
- 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。

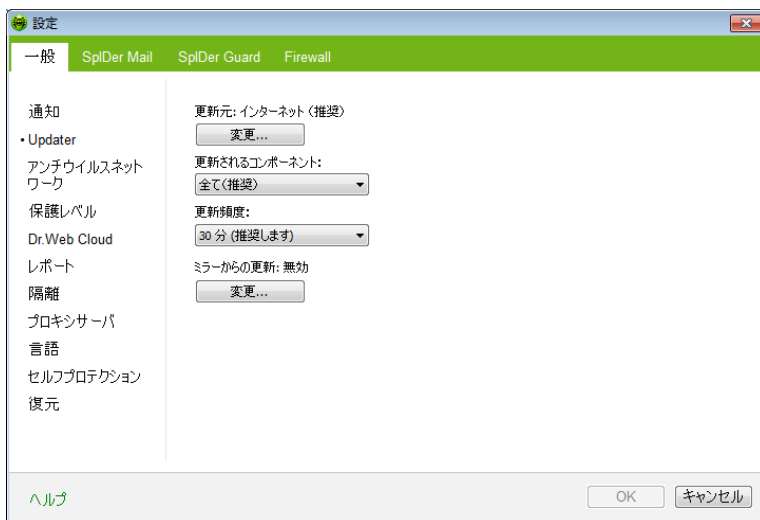
通知を一時的に無効にする

メール通知を無効にするには **メールで通知を送信する** チェックボックスをクリアしてください。

全てのタイプの通知を無効にするには **通知を有効にする** チェックボックスをクリアしてください。

Updater

このページでは、更新するコンポーネント、更新元、更新間隔、ミラーからの更新などの **Dr.Web Anti-virus** 更新パラメータを設定することができます。



オプション	説明
更新元	更新元を指定
更新されるコンポーネント	次の更新モードの内いずれか1つを選択 <ul style="list-style-type: none">• 全て(推奨) – Dr.Web Anti-virus ウイルスデータベース、エンジン、及びその他のコンポーネントを更新します。• データベースのみ – Dr.Web Anti-virus ウイルスデータベース、エンジンを更新します。その他のコンポーネントは更新されません。
更新頻度	更新の頻度を選択
ミラーからの更新	Dr.Web 製品がインストールされたローカルネットワークコンピュータが使用する更新ミラーを作成

更新元

更新元を選択するには **変更** をクリックします。開いたウィンドウ内で以下のいずれかの更新元を選択してください。

- **インターネット(推奨)** – 更新は **Doctor Web** サーバーからダウンロード



されます。デフォルトではこの更新元が使用されます。

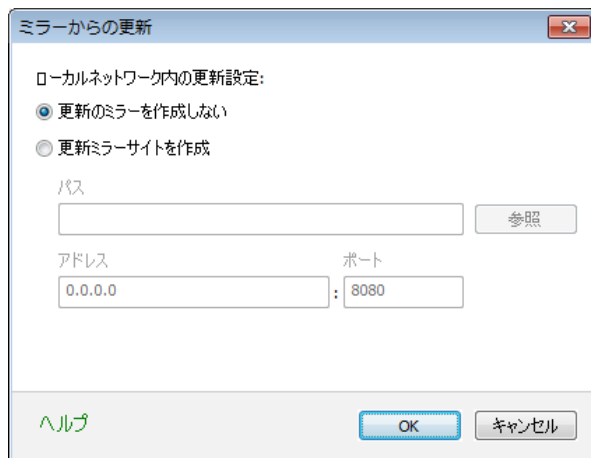
- **ローカル、またはネットワークフォルダ** - 更新は、それがコピーされたローカルまたはネットワークフォルダからダウンロードされます。フォルダへのパスを指定するには **参照** をクリックしてフォルダを選択するか、または手動でアドレスを入力してください。必要に応じ、ユーザー名とパスワードを入力してください。
- **アンチウイルスネットワーク - Dr.Web Anti-virus** 製品がインストールされているローカルネットワークコンピュータ上に更新ミラーが作成されている場合に、そのコンピュータから更新をダウンロードします。

ミラーからの更新

お使いのコンピュータが**Dr.Web** 製品のインストールされた他のローカルネットワークコンピュータによって更新元として使用されることを許可する場合は、**ミラーからの更新** 下の **変更** をクリックし、開いたウィンドウ内で **更新ミラーサイト** を作成を選択してください。次に、更新がコピーされるフォルダへのパスを指定します。お使



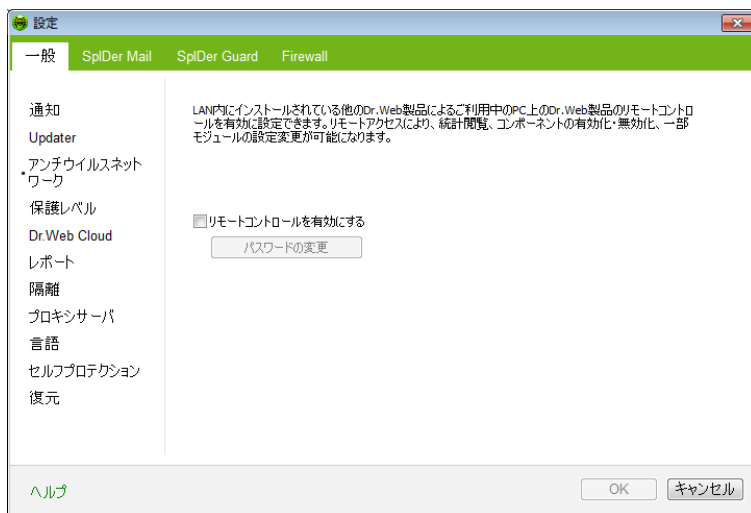
いのコンピュータが複数のネットワークに接続されている場合、いずれか1つのネットワーク内にあるコンピュータが使用可能なIPアドレスを指定することができます。HTTP通信のポートを指定することも可能です。



アンチウイルスネットワーク

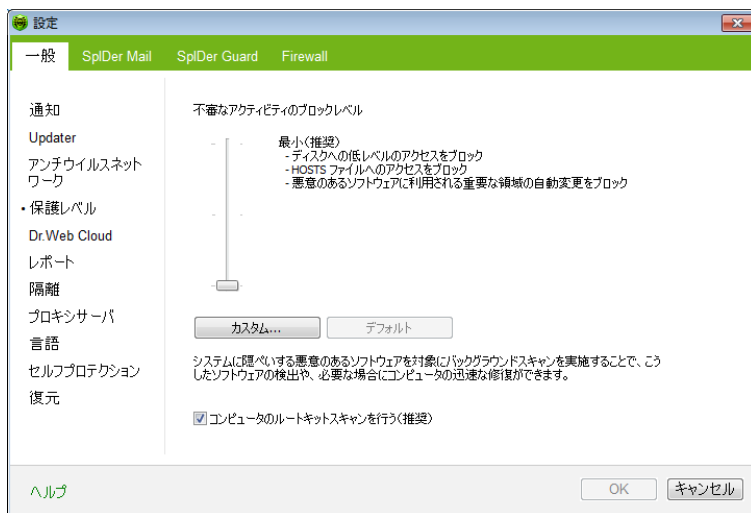
このページでは、[アンチウイルスネットワーク](#)によって、お使いのアンチウイルスを他のローカルネットワークコンピュータからリモート管理することが出来ます。お使いのコンピュータがアンチウイルスネットワークに接続されている場合、ローカル [更新ミラー](#) を作成し、アンチウイルス保護の状態やお使いのコンピュータをリモートで管理することが出来ます(統計を見る、[Dr.Web Anti-virus](#) コンポーネントを有効/無効にする又はそれらの設定を調整する)。

Dr.Web Anti-virus 設定への不正なアクセスを防ぐには、リモートコントロールのパスワードを設定してください。



保護レベル

このページでは、お使いのコンピュータのセキュリティを脅かすような他のプログラムの動作に対する **Dr.Web Anti-virus** の対応を設定することができます。また、ルートキット(特定のプロセスの実行、レジストリ変更、ファイル及びフォルダの改変などのOSIに対する変更を隠すために使用される悪意のあるプログラム)のバックグラウンドスキャンを有効にすることも出来ます。



保護レベル

デフォルトの **最小** モードでは、OSを破損させる悪意のある試みを明白に示唆するような、システムオブジェクトに対する自動変更を無効にします。また、ディスクへの低レベルアクセスをブロックし、HOSTSファイルを改変から保護します。

コンピューターが感染する危険性が高い場合、**中** モードを選択することで保護レベルを上げることが出来ます。このモードでは、悪意のあるソフトウェアに利用される可能性のある重要なオブジェクトへのアクセスをブロックします。



このモードを使用すると、保護されたレジストリブランチを使用する正規のソフトウェアとの互換性の問題が生じる場合があります。

重要なWindowsオブジェクトへのアクセスを全てコントロールした場合は **パラノイド** モードを選択することが出来ます。このモードでは、ドライバのロードやプログラムの自動実行に対するインタラクティブコントロールも可能です。

カスタムモード



このモードでは、コンピュータのセキュリティを脅かす可能性のある特定の動作に対する **Dr.Web Anti-virus** の柔軟な設定が可能です。



重要なMicrosoftの更新のインストール、又はプログラム（デフラグツールを含む）のインストールや動作中に問題が発生した場合、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。

ルートキットのバックグラウンドスキャン

Dr.Web Anti-virus に含まれているアンチルートキットコンポーネントによって、複雑な脅威に対するOSのバックグラウンドスキャンを行い、必要に応じて、検出されたアクティブな感染を修復することができます。

このオプションが有効になっている場合、**Dr.Web Anti-rootkit** はメモリ内に常駐します。**SpIDer Guard** によるファイルのオンザフライスキャンとは異なり、ルートキットスキャンではオートランオブジェクト、実行中のプロセス及びモジュール、RAM、MBR/VBRディスク、コンピュータBIOSシステム及びその他のシステムオブジェクトもスキャンされます。

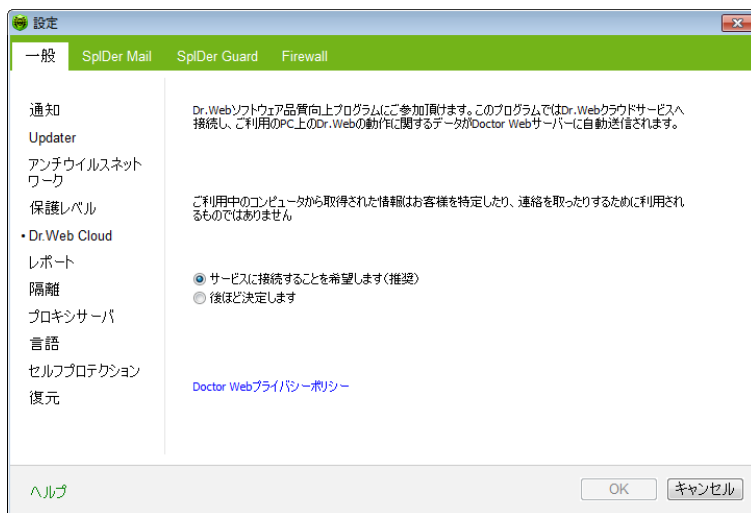
Dr.Web Anti-rootkit の主な特長の1つは、システムリソースの消費（プロセス時間、RAMの空き容量など）及びハードウェアキャパシティに対する優れたパフォーマンスです。

Dr.Web Anti-rootkit は脅威を検出するとユーザーに対して通知を行い、悪意のある活動を駆除します。

バックグラウンドスキャンを有効にするには、**コンピュータのルートキットスキャンを行う(推奨)** チェックボックスにチェックを入れてください。

Dr.Web Cloud

このページでは **Doctor Web** クラウドサービスに接続し、**Dr.Web** の品質向上プログラムに参加することができます。



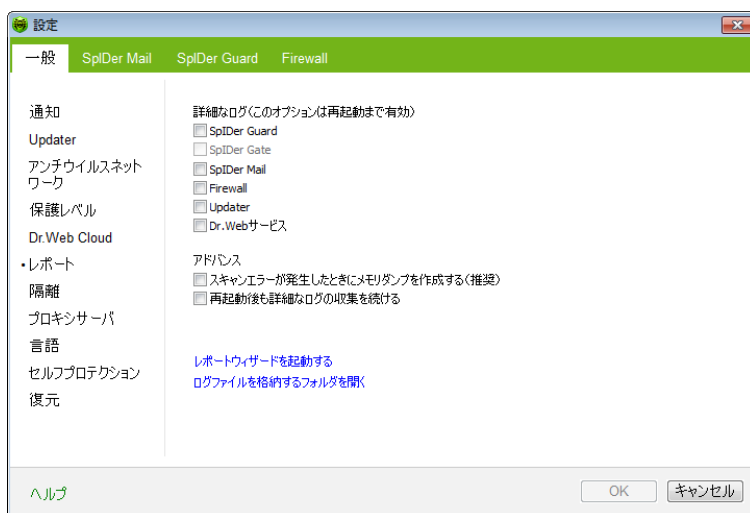
ソフトウェア品質向上プログラム

ソフトウェア品質向上プログラムにご参加いただける場合、お使いのコンピュータ上の **Dr.Web Anti-virus** の動作に関するデータ(個人を特定しないもの)が定期的にDr.Webのサーバーへ送信されます(**Dr.Web Firewall** に対して作成されたルールセットなど)。受け取った情報は、ユーザーを特定したり連絡を取ったりする目的で使用されることはありません。

Doctor Web 公式サイト 上のプライバシーポリシーをご覧ください。
Doctor Web プライバシーポリシー リンクをクリックしてください。

レポート

このページでは **Dr.Web Anti-virus** コンポーネントのログに関する設定を行うことができます。



デフォルトでは、標準モードで以下の情報が記録されます。

コンポーネント	情報
SpiDer Guard	更新時刻および SpIDer Guard の起動 停止時刻、ウイルスイベント、スキャンされたファイル名、パッカー名、スキャンされた複合オブジェクト(アーカイブ、メール添付ファイル、ファイルコンテンツ)のコンテンツ SpIDer Guard によって最も頻繁にスキャン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。必要に応じてそのようなオブジェクトをスキャン対象外リストに追加することで、コンピューターパフォーマンスを向上させることができます。
SpiDer Mail	更新時刻および SpIDer Mail の起動 停止時刻、ウイルスイベント、接続監視設定、スキャンされたファイル名、パッカー名、スキャンされたアーカイブのコンテンツ メールの監視設定をテストしたい場合にこのモードの使用を推奨します。
SpiDer Gate	更新時刻および SpIDer Gate の起動 停止時刻、ウイルスイベント、接続監視設定、スキャンされたファイル名、パッカー名、スキャンされたアーカイブのコンテンツ チェックされたオブジェクト及びHTTPモニターの動作に関する詳細な情報を受け取りたい場合にこのモードの使用を推奨します。



コンポーネント	情報
Firewall	Dr.Web Firewall は、標準モードでは動作に関するログを記録しません。詳細なロギングを有効にすると、 ファイアーウォール はネットワークケットに関するデータを収集します (pcap ログ)。
Updater	更新された Dr.Web Anti-virus ファイルのリスト及びそのダウンロード状況、補助スクリプト実行に関する詳細、更新日時、更新後に再起動した Dr.Web Anti-virus コンポーネントに関する詳細

ログファイルを見るには

ログファイルを見るには **ログファイルを格納するフォルダを開く** をクリックします。

詳細なログを有効にするには



Dr.Web Anti-virus の動作に関する詳細なデータのロギングは、ログの著しい増加やプロセス負荷の増大を引き起こす場合があります。このモードはエラーの発生時または **Doctor Web テクニカルサポート** からの指示があった場合のみ使用することを推奨します。

1. **Dr.Web Anti-virus** コンポーネントの詳細なログを有効にするには、該当するチェックボックスにチェックを入れてください。
2. デフォルトでは、詳細なロギングモードはOSの最初の再起動前に使用されます。再起動の前と後でコンポーネントの動作をロギングする必要がある場合、**再起動後も詳細なログの収集を続ける** チェックボックスにチェックを入れてください。
3. 変更を保存します。

アドバンス設定

スキャンエラーが発生したときにメモリダンプを作成する (推奨) オプションは、**Dr.Web Anti-virus** コンポーネントのエラーに関する有用な情報を最大限まで保存します。発生した問題に対する **Doctor Web テクニカルサポート** のスペシャリストによる詳細な分析および解決に役立つため、動作エラーの発生時にはこのオプションを有効にすることを推奨します。

またこのページでは、お使いのOS及び **Dr.Web Anti-virus** の動作に関するデータを収集して **Doctor Web テクニカルサポート** へ送信することも出来ます。レ

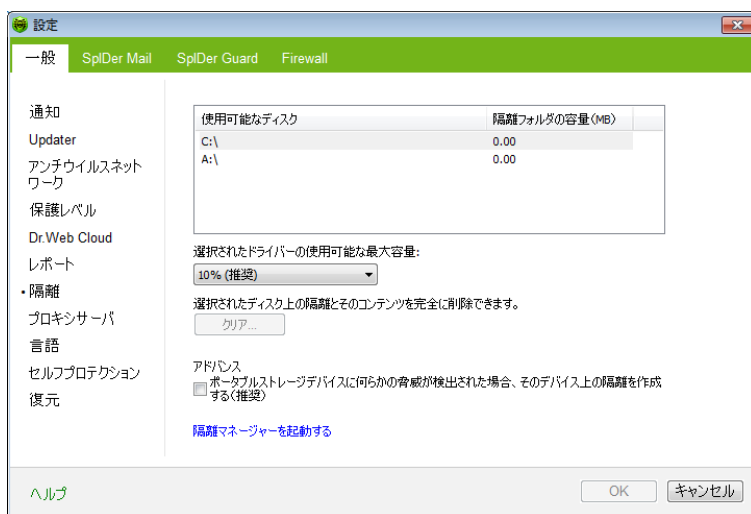


ポर्टワイガードを起動する をクリックしてください。

隔離

このページでは **Dr.Web Anti-virus 隔離** の設定、そのサイズの設定、隔離されたファイルの削除を行うことができます。

隔離 フォルダは、疑わしいファイルが検出された各論理ドライブ上に個別に作成されます。



隔離の最大サイズを設定する

1. **隔離** サイズの上限を設定したドライブをリストから選択してください。
2. **選択されたドライブの使用可能な最大容量** リストから必要な容量を選択します。

隔離 サイズの上限はディスク容量に対するパーセンテージで表されます (複数の論理ドライブが選択されている場合、このサイズは **隔離** フォルダを含んでいる全てのドライブに適用されます)。制限なしに設定すると **隔離** フォルダのサイズには上限がなくなります。



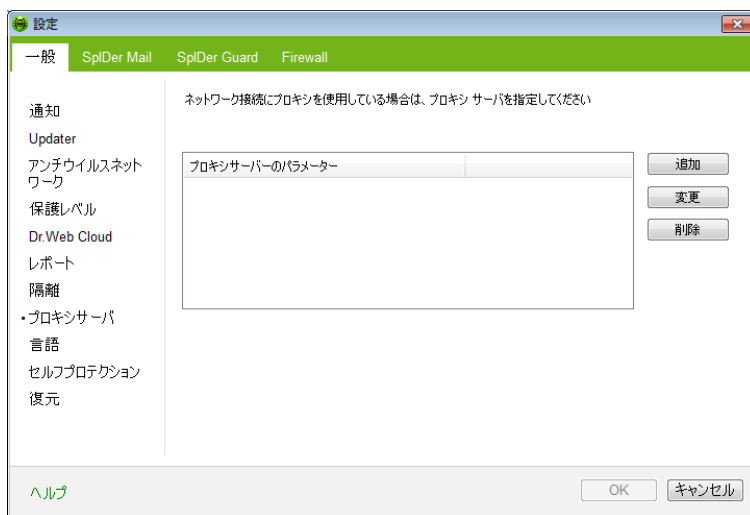
隔離を空にする

1. 隔離された全てのファイルを削除したいドライブをリストから選択してください。
2. クリアをクリックし、指示に従って削除を確定してください。

ポータブルストレージデバイス上で検出された感染したオブジェクトを隔離するには **アドバンス** 設定を使用します。デフォルトでは、検出された脅威は暗号化されずにこのデバイス上の **隔離** フォルダへ移されます。ポータブルストレージデバイス上に **隔離** フォルダが作成されるのは、それらのデバイスが書き込み可能である場合のみです。別々のフォルダを使用し、ポータブルストレージデバイス上で暗号化を行わないことで、データ損失の可能性を防ぎます。

プロキシサーバ

このページでは、コンポーネントの接続パラメータを指定することができます。



デフォルトでは、コンポーネントは全て直接接続モードを使用します。必要に応じて1つないし複数のプロキシサーバに対して接続パラメータを指定することが出来ます。



プロキシサーバーリストの作成

1. **Dr.Web Anti-virus 一般設定** 内で **プロキシサーバ** ページを選択します。
2. 新しいプロキシサーバーを追加するには **追加** をクリックしてください。接続設定のウィンドウが開きます。

プロキシサーバーのパラメーター

アドレス: ポート:

ユーザー:

パスワード:

許可の種類
なし

ヘルプ OK キャンセル

3. プロキシサーバーへの接続に以下のパラメータを指定してください。

パラメータ	説明
アドレス	プロキシサーバーのアドレスを指定
ポート	プロキシサーバーのポートを指定
ユーザー	プロキシサーバーへの接続時に使用するユーザー名を指定
パスワード	指定したユーザー名でプロキシサーバーに接続する際に使用するパスワードを指定
許可の種類	プロキシサーバーへの接続に必要な認証の種類を選択
Dr.Web Anti-virus コンポーネント	指定されたプロキシサーバーを使用してコンポーネントがインターネットに接続できるようにするには、コンポーネント名の横にある該当するチェックボックスにチェックを入れてください。

4. 他のプロキシサーバーを追加する場合は、step 2 とstep 3 を繰り返してください。プロキシサーバーへの接続設定を編集するには、リスト上で該当するプロキシを選択して **変更** をクリックします。リストからプロキシサー

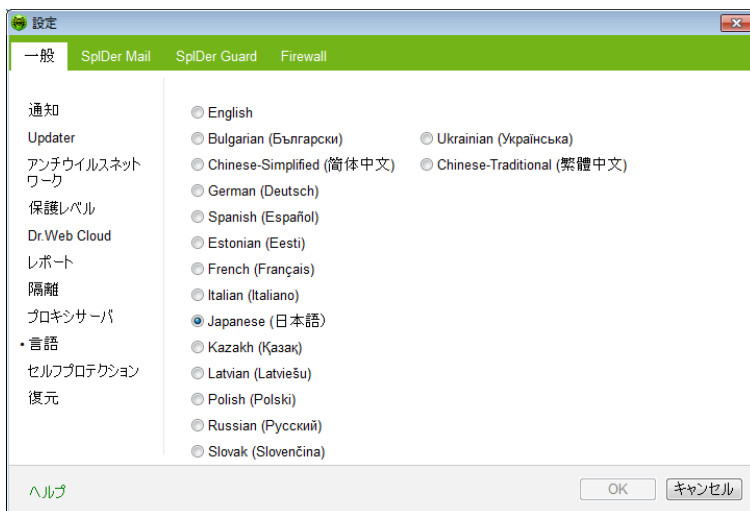


バーを削除するには、該当するプロキシを選択して **削除** をクリックします。

5. 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** をクリックします。

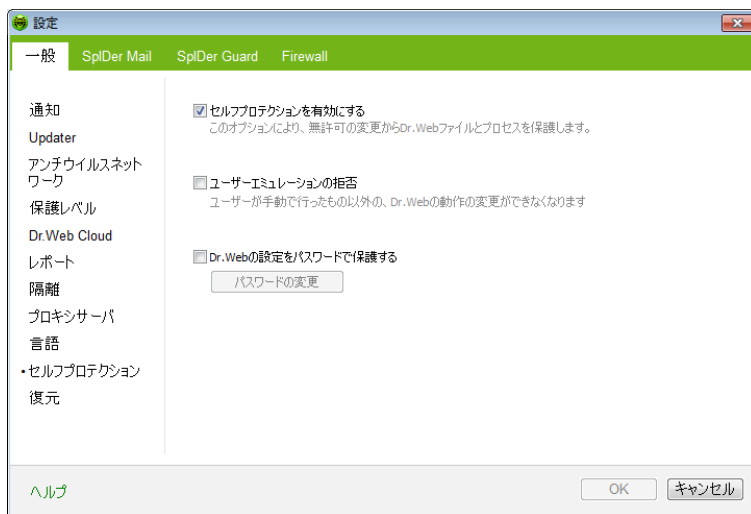
言語

このページでは、**Dr.Web Anti-virus** グラフィカルインターフェースで使用される言語を選択することができます。使用可能な全ての言語が自動的に表示されず。



セルフプロテクション

このページでは、アンチ・アンチウイルスプログラムによる不正な改変や誤った破損から**Dr.Web Anti-virus** 自体を保護するための設定を行うことができます。



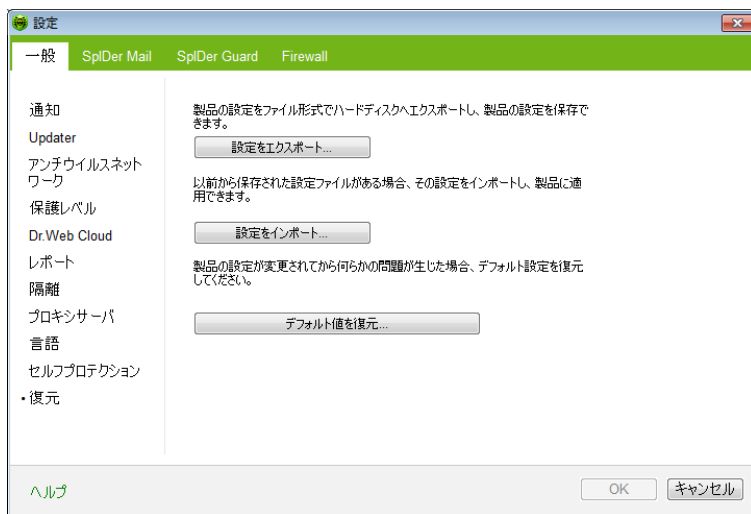
セルフプロテクションを有効にする オプションでは **Dr.Web Anti-virus** ファイル、レジストリキー、プロセスを破損や削除から保護します。セルフプロテクションを無効にすることは推奨できません。

ユーザーエミュレーションの拒否 オプションでは、ユーザーと **Dr.Web Anti-virus** のインタラクションをエミュレートした、またはユーザーによって起動されたスクリプトの実行を含む **Dr.Web Anti-virus** の動作に対する自動での変更を全て防ぎます。

Dr.Webの設定をパスワードで保護する オプションでは **Dr.Web Anti-virus** の設定にアクセスする際に必要となるパスワードを設定することができます。


復元

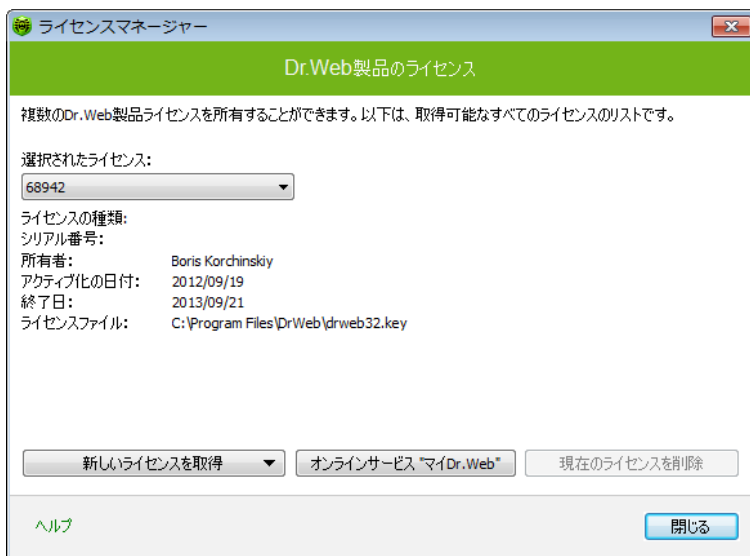
このページでは **Dr.Web Anti-virus** の全ての設定をデフォルト値に復元、また設定をエクスポート・インポートすることが出来ます。



3.3. ライセンスマネージャ

ライセンスマネージャ は **Dr.Web Anti-virus** 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 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** を選択した後、**ライセンスマネージャ** を選択します。



オンラインサービス"マイDr.Web" は **Dr.Web Anti-virus 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、ライセンスの更新、テクニカルサポートへの問い合わせなどを行うことができます。

Doctor Web サーバーからキーファイルを受け取るための登録手続きを開始するには **新しいライセンスを取得** をクリックし、ドロップダウンメニューで **インターネット** からを選択してください。 **キーファイルの取得手続き** が開始されます。

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** をクリックします。ドロップダウンメニューで **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** は自動的にキーファイルの使用を開始します。

インストール中にキーファイルを取得した場合、またはディストリビューションセットに含まれている場合はキーファイルのインストールは自動的に開始され、その他の操作は必要ありません。

キーファイルをリストから削除するには、該当するキーファイルを選択して **現在のラ**



ライセンスを削除 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** 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** 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 もしくはデモ キーファイルが見つからなかった場合、**Dr.Web Anti-virus** コンポーネントの動作はブロックされます。有効なキーファイルを取得するには、**SpIDer Agent** のコンテキストメニューで **ライセンスを登録** を選択してください。



3.4. 隔離マネージャー

Dr.Web Anti-virus 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。書き込み可能なポータブルストレージデバイス上で感染したオブジェクトが検出された場合はデバイス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、**ツール** を選択した後に **隔離マネージャー** を選択します。



ウインドウの中央に、隔離されたオブジェクトに関する以下の情報を含んだ表が表示されます。

- **オブジェクト** – 隔離されたオブジェクトの名称
- **脅威** – オブジェクトが隔離へ移された際の **Dr.Web Anti-virus** によるマルウェアの分類
- **移動日** – オブジェクトが **隔離** に移された日時
- **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パス



表示されるオブジェクトは、お使いのユーザーアカウントでアクセス可能なもののみです。

表示されていないオブジェクトを見るには、**Dr.Web Anti-virus** インストールフォルダを開いて `dwqrui.exe` ファイルを上位の権限を持つアカウントで実行するか、または **Dr.Web Anti-virus** を管理者アカウントで起動してください。

隔離されたオブジェクトを管理するには

1. 管理したいオブジェクト (1 つまたは複数) のチェックボックスにチェックを入れてください。
2. 次のボタンのいずれか1つをクリックして必要なアクションを適用します。

ボタン	説明
復元	選択したオブジェクトを隔離から削除し、元の場所 (隔離に移される前にオブジェクトが置かれていたフォルダ) に復元します。 このオプションは、そのオブジェクトが有害でないことが確実な場合にのみ使用してください。
指定場所に復元	選択したオブジェクトを隔離から削除し、指定した場所に復元します。 このオプションは、そのオブジェクトが有害でないことが確実な場合にのみ使用してください。
削除	選択したオブジェクトを隔離およびシステムから削除します。



3.5. アンチウイルスネットワーク

アンチウイルスネットワーク は **Dr.Web Anti-Virus** には含まれていませんが、お使いのコンピュータ上の **Dr.Web Anti-Virus** へのアクセスを許可することはできます。リモート接続を許可するには、**一般設定** の **アンチウイルスネットワーク** ページ内で **リモートコントロールを有効にする** にチェックを入れ、アクセスに必要なパスワードを入力してください。



Dr.Web Security Space のキーファイルを使用している場合、<http://download.drweb.co.jp/doc/> から該当するドキュメントをダウンロードし、**アンチウイルスネットワーク** に関する詳細を確認することができます。

Dr.Web Anti-Virus のリモートユーザーは以下の項目を使用することができます。

- **プログラムについて**
- [ライセンスを登録](#)
- **マイDr.Web**
- **ヘルプ**
- [SpIDer Guard](#)
- [SpIDer Mail](#)
- [Firewall](#)
- **ツール**
- **セルフプロテクションを無効にする / 有効にする**
- [Updater](#)
- [ライセンスマネージャ](#)
- [一般設定](#)
- **レポートウィザード**

リモートコントロールでは統計の表示、コンポーネントの有効 / 無効、設定の変更が可能です。**隔離** と **Scanner** は使用できません。**Firewall** の設定および統計も使用できませんが、**Firewall** を有効 / 無効にすることは可能です。



4. Dr.Web Scanner

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スキャンします。特別なパッカーによってバックされた実行ファイルは、スキャン時に解凍されます。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（IC、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に従ってなければなりません）のファイルもスキャンされます。

デフォルト設定の **Dr.Web Scanner** 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。感染した又は疑わしいオブジェクトは全て表内に表示され、必要なアクションを手動で選択することができます。

デフォルトの設定は多くの場合に最適なものとなっていますが、必要に応じ **Dr. Web Scanner** の **スキャナの設定ウインドウ** で、脅威を検出した際のアクションを変更することができます。スキャンの完了後に、検出された各脅威に対するカスタムのアクション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アクションを事前に設定しておく必要があります。





4.1. Scanner の動作

Dr.Web Scanner は通常のWindowsアプリケーションとしてインストールされ、ユーザーによって、又は自動的に起動されます ([Scanner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(システムフォルダを含む)に対するスキャンは実行されないため、Scanner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。

Scanner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 Scanner** アイコンをクリックする。
- タスクバー通知領域内にある **SpIDer Agent** アイコンのコンテキストメニュー内で **Scanner** をクリックする ([SpIDer Agent](#) 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 Scanner** 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スキャン](#) 参照)。

Scanner が起動すると、そのメインウィンドウが開きます。

スキャンには **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、スキャン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スキャンします。

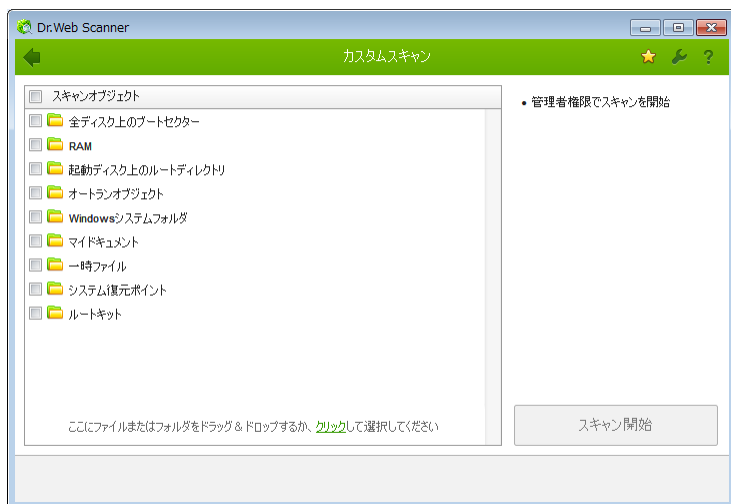
- RAM
- 全ディスク上のブートセクター
- オートランオブジェクト
- 起動ディスク上のルートディレクトリ
- Windowsインストールディスクのルートフォルダ
- Windowsシステムフォルダ
- マイドキュメントフォルダ
- システムの一時フォルダ
- ユーザーの一時フォルダ



スキャン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のルートキットスキャンも実行されます。

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)をスキャンします。またルートキットスキャンも実行されます。

カスタムスキャン モードでは、スキャンするオブジェクト(フォルダおよびファイル、RAM・オートランオブジェクト・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スキャンを開始するには **スキャン開始** をクリックします。



スキャンが開始されると **停止** 及び **中止** ボタンが有効になります。

- スキャンを一時停止した場合は **停止** ボタンを押して下さい。中断されたスキャンを再開した場合は **再開** ボタンを押します。
- スキャンを中止した場合は **中止** ボタンを押して下さい。



停止 ボタンは、プロセス及びRAMのスキャン中は使用できません。



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その他のコンピュータ脅威が検出された際に通知を行います。**駆除** をクリックすると、検出された全ての脅威を同時に駆除することができます。この場合 **Dr.Web Scanner** は、その設定および脅威の種類に応じて最も効果的なアクションを適用します。必要に応じ、特定の脅威に対して個別のアクションを適用、またはそのデフォルトアクションを変更することも可能です。

検出された脅威は、感染したオブジェクトを元の状態に復元するか（修復）、または修復が不可能な場合、それらをお使いのシステムから完全に削除する（削除）ことで駆除されます。



駆除 をクリックすると、表内で選択されたオブジェクトに対してアクションが適用されます。スキャンが完了すると **Dr.Web Anti-virus** はデフォルトで全てのオブジェクトを選択します。必要に応じ、オブジェクト名の隣にあるチェックボックス、またはテーブルヘッダー内 ドロップダウンメニューの脅威のカテゴリを使用することで選択をカスタマイズすることが可能です。

Dr.Web Scanner

スキャンが完了しました

Dr.Web Scanner は脅威を検出しました
検出された脅威の連や駆除を推奨します。Dr.Web Scannerは設定に応じてアクションを適用します。

検出された脅威: 3
駆除された脅威: 0
検査の時間: 00:00:00

駆除

ファイル名	脅威	アクション	パス
b349a38d59078...	Trojan.Winlock.7589	修復	...lb349a38d5907875e027ced05a1748c1
764ed5f9f86adb...	Trojan.Winlock.7589	修復	...764ed5f9f86adb36697804364df8ac39
c4ccdb2d892010...	Trojan.Winlock.7589	修復	...lc4ccdb2d892010e9039f10c10bd4bdc0f

追加情報を非表示にする



アクションの選択

1. 必要に応じ、**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** ウィンドウ内の任意の場所で右クリックし **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(ブートセクター)以外のオブジェクトの隔離、または削除はできません。
- アーカイブ内、インストールパッケージ内、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**も行いうことができません。

Dr.Web Scanner の動作に関する詳細なログは %USERPROFILE%*Doctor Web フォルダ内のdwwscanner.log ファイルに保存されます。





4.3. Scanner 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(システムフォルダを含む)に対するスキャンは実行されないため、**Scanner** 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多くのアプリケーションにとって最適なものとなっています。特に必要がない限り変更しないようにして下さい。

Scannerの設定

1. **Scanner** 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。複数のタブを含んだ **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 **Help**  ボタンを使用して下さい。
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下さい。

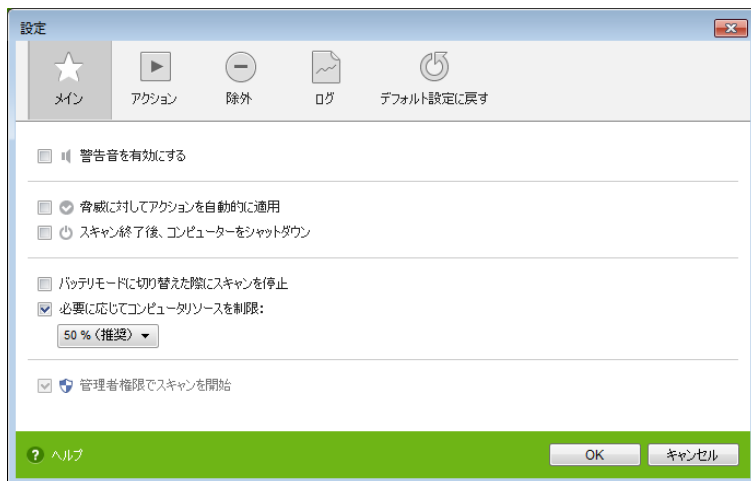


メイン

このタブでは **Scanner** 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 **Scanner** 間のインタラクションを設定することが可能です。

Scanner 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)はスキャンされません。 **Scanner** 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。

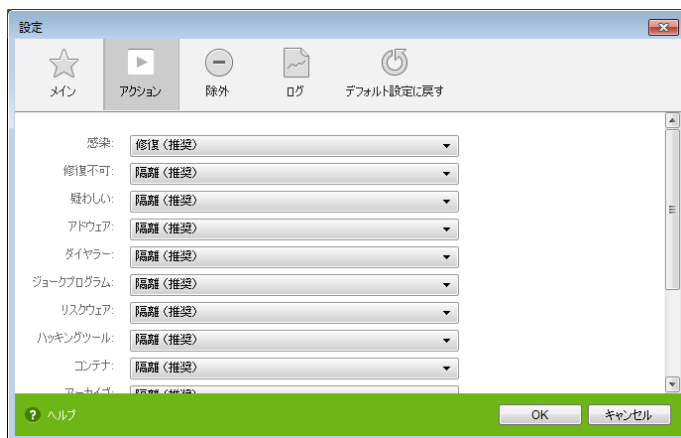




アクション

検出された脅威に対するアクションを設定する

1. **設定** ウィンドウ内で **アクション** タブを選択します。



2. **感染** ドロップダウンリストで、**感染**したオブジェクトの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。



ほとんどの場合、**修復** アクションが推奨となっています。

3. **修復不可能なオブジェクト**に対するアクションを **修復不可** ドロップダウンリストから選択してください。アクションの種類は**感染**したオブジェクトの場合と同様ですが、**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** 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ください(前項と同様です)。
5. **アドウェア**、**ダイヤラ** 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**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



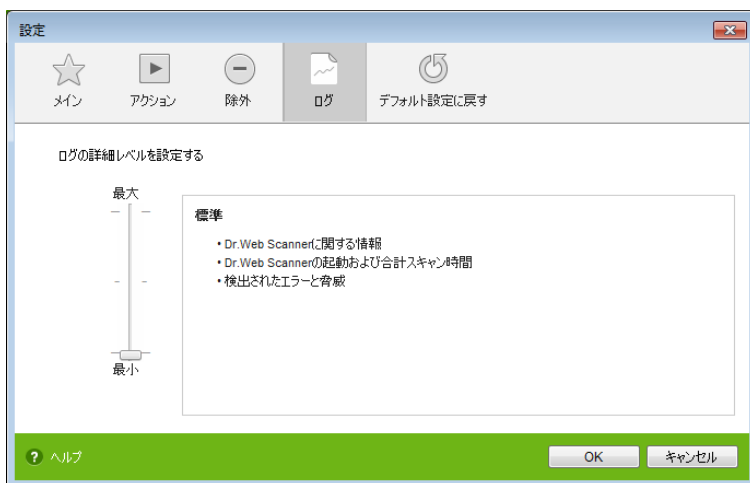
は疑わしいコードが検出された場合にそれらのオブジェクト全体に対して適用されるプログラムの自動アクションも、同様に設定します。

7. 感染したファイルの修復を完了する為にWindows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** - 保存されていないデータは失われる場合があります。
- **再起動を提案する**

ログ

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の多くはそのまま使用するようになっています。ログの詳細レベル(デフォルトでは、感染した又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、バックされたファイルおよびアーカイブのスキャンに関する情報、スキャン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スキャン

コマンドラインモードで **Scanner** 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、スキャン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。また、このモードでは **スケジュール** による **Scanner** の自動起動が可能です。

コマンドラインからスキャンを実行する

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>] [<オプションパラメータ>]
```

スキャンするオブジェクトは空のままか、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、スキャン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 [スキャンモード](#) 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スキャンを実行します。

オプションパラメータはプログラムの設定を指定するコマンドラインパラメータです。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 (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) でスキャンが実行されます。

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. Console Scanner

Dr.Web Anti-virus には、高度な設定が可能な **Console Scanner** も含まれています。



Console Scanner は疑わしいファイルを **隔離** には移しません。

Console Scannerの起動

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>]dwscancl [<オプション/パラメータ>] [<オブジェクト>]
```

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

オプションパラメータはプログラムの設定を指定するコマンドラインパラメータです。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](#) を参照してください。

リターンコード

- 0 - スキャン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 - スキャン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、**Console Scanner** に対するライセンスがありません。
- 12 - **Scanning Engine** が起動しませんでした。
- 255 - スキャンはユーザーによって中断されました。

4.6 Scannerの自動起動

Dr.Web Anti-virus のインストール中に、アンチウイルススキャンタスクが **タスクスケジューラ** 内に自動的に作成されます (タスクはデフォルトでは無効になっています)。



す。

作成されたタスクのパラメータを確認するには、**コントロールパネル** → **管理ツール** → **タスクスケジューラ**を開いてください。

タスクの一覧から**Dr.Web Daily scan**を選択します。このタスクの有効化、開始時間の調整、必要なパラメータの設定を行うことができます。

全般 タブで、表示したタスクの一般情報および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** タブでは、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を参照することができます。

また、ユーザー独自のアンチウイルススキャンタスクを作成することも可能です。システムスケジューラの操作に関する詳細については、ヘルプシステムやWindowsのドキュメントを参照してください。



インストールされたコンポーネントに **Dr.Web Firewall** が含まれていた場合、**Dr.Web Anti-virus** のインストールが終了した後の一度目のシステム再起動後、**タスクスケジューラ** は **Firewall** にブロックされます。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。



5. SpIDer Guard

SpIDer Guard はメインメモリ内に常駐するアンチウイルスモニターです。ファイル及びメモリをオンザフライでスキャンし、ウイルスと思われる活動を検出します。

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。



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スキャンを実行します。スキャン方法は **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どうかを常にモニターし、検出した場合にはそれらのプロセスをブロックします。

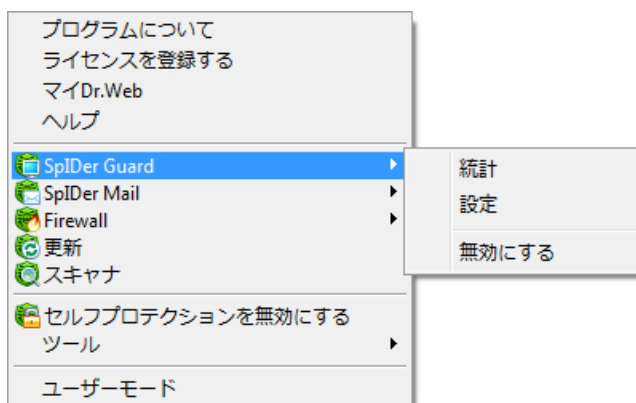
また **Dr.Web Anti-virus** に含まれている **SpIDer Guard** は感染したオブジェクトを検出すると、デフォルト設定では **アクションタブ** で指定されたアクションを実行します。

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** ウィ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。



5.1. SpliDer Guard の管理

SpliDer 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（スキャンされたオブジェクト数、感染した又は疑わしいオブジェクト数、ウイルスと思われる活動、実行されたアクションなど）を含む **統計** ウィンドウを開きます。

設定 は **SpIDer Guard** の設定ウィンドウを開きます（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）。



設定 および 無効にする/有効にする は **ユーザー** モードでは使用できません。

SpIDer Guard を無効にするには確認 コード またはパスワードを入力してください。 (**Dr.Web Anti-virus 一般設定** 内 **セルフプロテクション** ページで **Dr.Webの設定をパスワードで保護する** チェックボックスにチェックを入れた場合)

5.2. SpliDer Guard の設定

SpIDer Guard の調整可能な主なパラメータは **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、そのページへ移動しヘルプをクリックします。

パラメータの調整終了後、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。

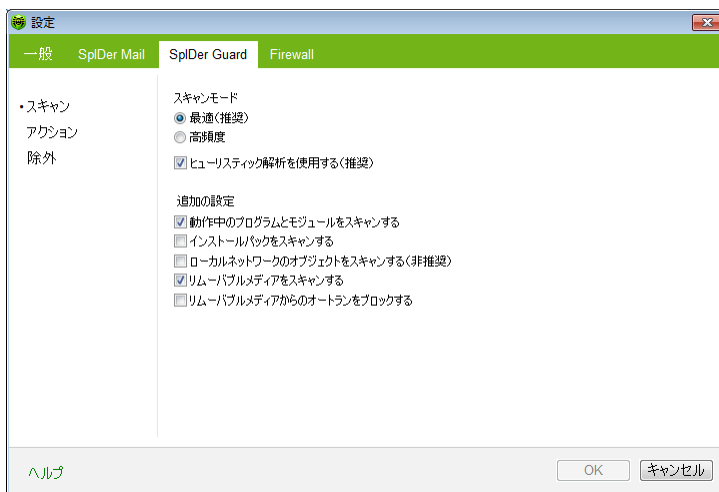
よ変更される設定は以下のとおりです。

スキャン

デフォルトでは **SpIDer Guard** のスキャンモードは **最適** に設定されています。ハードドライブ上で実行中 作成中 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スキャンされます。

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解析を使用する 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解析に基づいたウイルス検出手法)を有効にします。



外付け記憶装置 (USBインターフェースを持つモバイルドライブなど)の中には、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のあるものがあります。そのため、このようなデバイスには慎重に使用する必要があり、コンピューターへの接続時には **Scanner** によるウイルススキャンを実行するようにしてください。

アーカイブのスキャンを無効にすると、例えば **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でき、その検出は遅れます。感染したアーカイブの解凍時 (または感染したメッセージを開く時) 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試行され、**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スキャンするよう **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、いずれのスキャン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拡散す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 チェックボックスのチェックを外すことを推奨します。

アクション

このページでは、感染したオブジェクトに対する **SpliDer 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 **Scanner** 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. コンピュータ脅威と駆除手法](#) に記載されています。

SpliDer Guard のデフォルトアクションを変更する

1. **SpliDer 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. **アドウェアとダイアラ プログラム** のドロップダウンリストで、危険なファイル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んだ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. 変更を適用して **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。

除外

このページでは、スキャンの対象から除外するフォルダとファイルを指定します。

除外するファイルとフォルダのリスト フィールドで、スキャン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。

リストはデフォルトでは空になっています。ファイル、フォルダ、またはマスクをリストに加えるには、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場合や、リストに加える前にフィールド内でパスを編集する場合には **参照** をクリックし、オブジェクトを選択します。

ファイルまたはフォルダをリストから削除するには、それらをリスト内で選択し **削除** をクリックします。



6. SplIDer Mail

デフォルトでは **SplIDer Mail for Windows** はインストールされるコンポーネントのセットに含まれており、メモリ内に常駐し、Windowsのスタートアップ時に自動で起動します。自動起動モードは **SplIDer Agent 設定** で無効にすることができます。

また、デフォルトの設定では、コンピュータ上のあらゆるメールプログラムから110番ポートのPOP3サーバーへのアクセス、25番ポートのSMTPサーバーへのアクセス、143番ポートのMAP4サーバーへのアクセス、119番ポートのNNTPサーバーへのアクセスを全て自動的に監視します。

受信するメールは全て、メールクライアントが受け取る前に **SplIDer Mail** によって監視され、ウイルスがないかどうか最大レベルの詳細さでスキャンされます。ウイルスまたは疑わしいオブジェクトが検出されなかった場合、メッセージは、あたかもサーバーから直に送られたかのように "transparent" (透過) モードでメールプログラムに渡されます。送信されるメールに対しても、それらがサーバーに送られる前に同様の処理が行われます。

デフォルトでは、スキャンされなかったメッセージ (例えば、構造が複雑だったために)、および感染した受信メッセージを検出した際に **SplIDer Mail** は以下のようなアクションを実行します。

- ウィルスに感染したメールは配信されません。メールプログラムはメール削除の指示を受け取り、サーバーはこのメールが受信された旨の通知を受け取ります (このアクションはメッセージの削除です)。
- 感染が疑われるオブジェクトを含んだメッセージを別々のファイルとして隔離へ移動し、メールクライアントに通知を送信します (このアクションはメッセージの隔離です)。
- スキャンされなかったメッセージ、および感染していないメッセージを通過させます。
- 削除または移動された全てのメールは、POP3またはMAP4サーバー上に残ります。

送信されるメッセージが感染している、または感染が疑われる場合、それらはサーバーには送られません。ユーザーはメッセージが送信されない旨の通知を受け取ります (そのようなメッセージは通常、メールプログラムによって保存されます)。

メールを介して配信された未知のウイルスがコンピュータ上に存在する場合で



も、プログラムはそのようなウイルスの典型的な動作（例えば、大量送信の試行など）を検出することが可能です。このオプションはデフォルトで有効になっています。

プログラムのデフォルト設定は、最も高いレベルの保護を提供しユーザーの操作を最小限に抑える、初心者の方にも最適なものとなっています。ただし、メールプログラムのいくつかのオプションはブロックされる場合があります（例えば、複数のアドレスに対するメッセージの送信は大量送信と見なされる場合があります、受信するメールのスパムスキャンは実行されません）、自動削除が実行された場合には感染したメールの安全なテキストパートにある情報も失われます。上級者ユーザーは、メールスキャンのパラメータ及びウイルスイベントに対するプログラムのアクション設定を変更することが可能です。

POP3、SMTP、IMAP4、またはNNTPトラフィックを自動監視出来ない場合がありますが、そのような場合は接続の手動監視を設定することができます。

Dr.Web Scanner も様々なフォーマットのメールボックス内に存在するウイルスを検出することが出来ますが、**SpIDer Mail** にはいくつか優位な点があります。

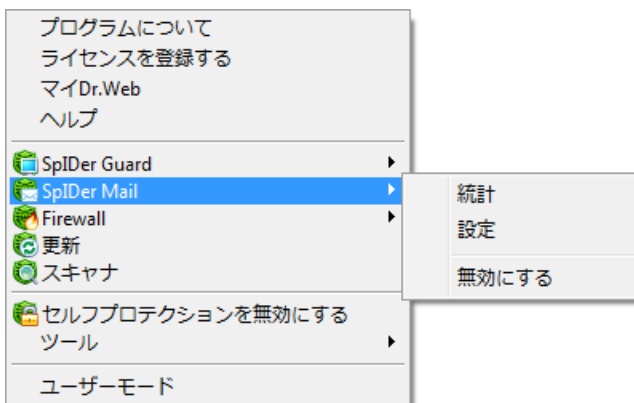
- **Dr.Web Scanner** は一般的なメールボックスのフォーマット全てをサポートしているわけではありませんが、**SpIDer Mail** を使用した場合、感染したメールはメールボックスに配信されることすらありません。
- **Scanner** はメールの受信時ではなくユーザーの要求に応じて又はスケジュールに従ってメールボックスをチェックします。さらに、このアクションはリソースを消費する上に時間がかかります。

したがって、デフォルト設定での全てのエンポイントの中で、メールを介して配信されるウイルスおよび疑わしいオブジェクトを最初に検出し、それらのエンポイントへの侵入を防ぐことが出来るのは **SpIDer Mail** になります。また、他のエンポイント無しにメールをスキャンするため、リソースを節約することが可能です。



6.1. SpliDer Mail の管理

SpliDer Mail の管理は **SpliDer Agent** アイコンのコンテキストメニュー内にある **SpliDer Mail** から行うことができます ([SpliDer Agent](#) 参照)。



設定 を選択すると **SpliDer Mail** の設定ウインドウが開きます ([SpliDer Mail の設定](#) 参照)。

統計 を選択するとセッションにおけるプログラムの動作に関する情報 (スキャンされたオブジェクト数、感染した又は疑わしいオブジェクト数、実行されたアクション) を表示するウインドウが開きます。

無効にする / 有効にする で **SpliDer Mail** を起動 / 停止することができます。



設定 および 無効にする / 有効にする は **ユーザー** モードでは使用できません。



6.2. Spl Der Mail の設定

SplDer Mail の設定を変更するには [SplDer Mail の管理](#) に記載されている手順で設定ウィンドウを開いてください。

設定を編集する際にはプログラムのヘルプシステムを使用してください。各ページのヘルプを見るには **ヘルプ** をクリックします。インターフェイスの特定の要素にはコンテキストプロンプトを持つものもあります。

編集終了後、**OK** をクリックします。

多く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。デフォルト以外で最もよく使用されるパラメータは以下のとおりです。

アクション	設定
感染したメール	修復(推奨)
修復不可能なメール	隔離(推奨)
疑わしいメール	隔離(推奨)
検査されていないメール	無視(推奨)
破損したメール	無視(推奨)
アドウェア	隔離(推奨)
ダイヤラープログラム	隔離(推奨)
ジョークプログラム	無視(推奨)
クラッキングツール	無視(推奨)
リスタウェア	無視(推奨)



デフォルトのアクションを変更する

1. **感染したメール** のドロップダウンリストで、感染したメール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)。
2. **修復不可能なメール** のドロップダウンリストで、修復できないメール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)。隔離されたファイルに対する他のアクションについては、[ウイルス検出時のアクション](#) を参照してください。
3. **疑わしいメール** のドロップダウンリストで、疑わしいメール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. **検査されていないメール** および **破損したメール** のドロップダウンリストで、検査されていないまたは破損したメールを検出した際のアクションを選択します (**無視** を推奨します)。
5. **アドウェア** および **ダイヤラープログラム** のドロップダウンリストで、アドウェアまたはダイヤラー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. 変更を適用してSpIDer Mail 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。

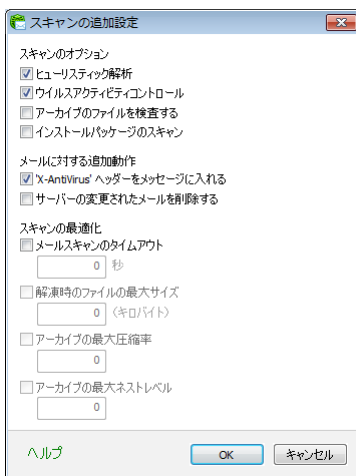


SpIDer Guard が常に起動している場合には、疑わしいメールに対する保護を無効にしても構いません。

検査されていないメール のドロップダウンリストで **隔離** を選択することにより、アンチウイルス保護の信頼性をデフォルトで設定されたレベルよりも高めることができます。この場合、移動されたメッセージファイルをScannerで検査するようにしてください。

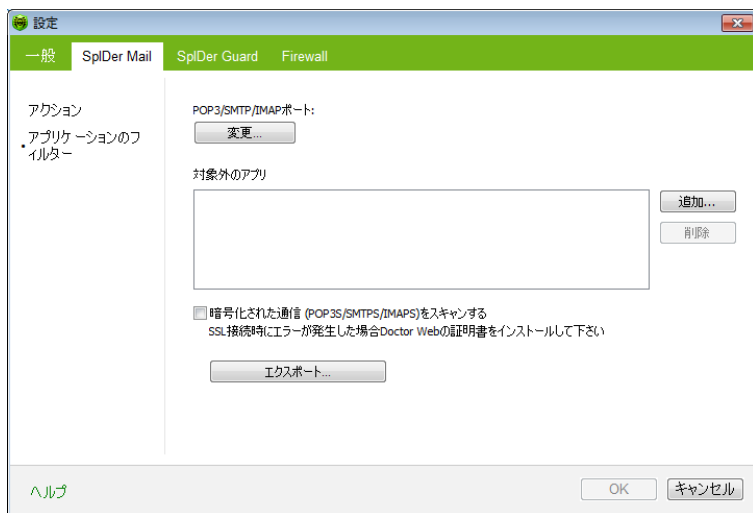
削除または隔離されたメッセージをPOP3/IMAP4サーバー上から即座に削除するモードを有効にすることができます。追加設定内の **サーバーの変更されたメールを削除する** チェックボックスにチェックを入れてください。

追加設定を開くには **アドバンス** をクリックします。



アプリケーションのフィルター

デフォルト設定では、SpIDer Mail はコンピュータ上で動作中の全てのアプリケーションのメールトラフィックを自動的に監視します。このページでメールクライアントとメールサーバー間の接続監視、及び SpIDer Mail による監視の対象から除外したいメールトラフィックを持つアプリケーションのリストを設定することができます。



ファイル、フォルダ、マスクをリストに追加するには、入力欄にそれらの名前を入力し、**追加** をクリックしてください。既存のファイル名やフォルダを入力するには、**追加** をクリックし、標準ウインドウからオブジェクトを選択してください。

ファイルやフォルダをリストから削除するには、削除したいオブジェクトをリスト上で選択し、**削除** をクリックしてください。

モードに対する監視オプションを設定するには、ポートのリスト下にある **変更** をクリックします。

デフォルトでは、以下の自動監視ルールのみがリストに含まれています。

- 143番ポート (標準IMAP4メールサーバー) 経由でアクセスされる全てのIPアドレス
- 119番ポート (標準NNTPメールサーバー) 経由でアクセスされる全てのIPアドレス
- 110番ポート (標準POP3メールサーバー) 経由でアクセスされる全てのIPアドレス
- 25番ポート (標準SMTPメールサーバー) 経由でアクセスされる全てのIPアドレス



デフォルトでは、リストには全てのIPアドレス（*記号で指定）及び143番ポート（標準のIMAP4ポート）、119番ポート（標準のNNTPポート）、110番ポート（標準のPOP3ポート）、25番ポート（標準のSMTPポート）経由でアクセスされるIPアドレス全てが含まれています。

SpIDer Mailポート	サーバーのアドレス	サーバーのポート

リスト上で選択し **削除** をクリックするとリストから削除することができます。

サーバーまたはサーバーグループをリストに追加するには **サーバーのアドレス** フィールドにアドレス（ドメイン名、またはIPアドレス）を、**サーバーのポート** フィールドに接続が行われるポートの番号を入力し、**追加** をクリックしてください。



*がある場合、**localhost** アドレスは監視されません。必要な場合はリスト内でこのアドレスを明確に指定してください。

監視の手動設定

1. **SpIDer Mail 設定** ウィンドウ内で **アプリケーションのフィルター** ページを選択し、ポートのリスト下にある **変更** をクリックします。
2. そこへの接続を監視するリソースのリスト（POP3/SMTP/IMAP4/NNTPサーバー）を作成します。7000から始めて番号を付けます。以後これらの番号を **SpIDer Mail ポート** と呼びます。
3. それぞれのリソースに対して、**SpIDer Mail ポート** 入力フィールドにメー



ルサーバーに割り当てた **SpIDer Mail ポート** を、サーバーのアドレスフィールドにサーバーのドメイン名またはIPアドレスを、サーバーのポートフィールドに接続が行われるポート番号を入力し、**追加** をクリックしてください。

4. 同様の操作を各リソースに対して行います。
5. **OK** をクリックしてください。



メールクライアントの設定では、POP3/SMTP/IMAP4/NNTPサーバーのポートとアドレスの代わりに、localhost:<ポート_SpIDer_Mail>のアドレスを指定して下さい。<ポート_SpIDer_Mail>は該当するPOP3/SMTP/IMAP4/NNTPサーバーに割り当てられたアドレスです。

安全な接続

POP3S、SMTPS、IMAPSなどの安全なプロトコル経由で配信されるデータのスキャンを有効にすることができます。そのようなデータをスキャンするには **暗号化された通信(POP3S/SMTPS/IMAPS)をスキャンする** チェックボックスにチェックを入れてください。安全な接続を使用するお使いのクライアントアプリケーション(メールクライアント)がデフォルトのWindowsシステム証明書ストレージを参照しない場合、**Doctor Web SSL 証明書** をエクスポートする必要があります。

Doctor Web 証明書

SSLプロトコルを使用してやり取りされたデータをスキャンする必要がある場合は、例えば **POP3S、SMTPS、IMAPS** 経由でメッセージを送受信するよう**SpIDer Mail** を設定することが出来ます。これらのプロトコルは暗号化されたSSL通信を使用します。**Dr.Web Anti-virus** がそのような暗号化された通信をスキャンし、Windowsシステム証明書ストレージを参照しないメールクライアントやいくつかのブラウザとの透過的な整合性を維持するためには **Doctor Web SSL 証明書** をアプリケーション証明書ストレージ内にインポートする必要が生じる場合があります。今後の使用のために証明書をシステムストレージから第三者アプリケーション内に保存する場合は **エクスポート** をクリックしフォルダを選択してください。



7. Dr.Web for Outlook

Dr.Web for Outlook プラグインは以下の機能を実行します。

- SMTP、POP3、およびHTTPプロトコル経由で送受信されたメール添付ファイルのアンチウイルス検査
- SSL暗号化接続を介して送受信されたメール添付ファイルのチェック
- 悪意のあるオブジェクトの検出および駆除
- マルウェア検出
- 未知のウイルスに対する追加保護としてのヒューリスティック解析

7.1. Dr.Web for Outlook の設定

[ツール] -> [オプション] -> [Dr.Web Anti-virus] タブ (Microsoft Outlook 2010の場合は [ファイル]-> [オプション] の **Dr.Web for Outlook** を選択して [アドイン オプション] ボタンをクリック)を選択すると、Microsoft Outlookのメールアプリケーションで **Dr.Web for Outlook** プラグインの設定および統計情報の参照が可能です。



Microsoft Outlook パラメータの **Dr.Web Anti-virus** タブは、ユーザーがそれらの設定を変更する権限を持っている場合のみアクティブになります。

Dr.Web Anti-Virus タブでは、現在の保護の状態が表示され (有効 / 無効) 以下のプログラム機能へのアクセスが可能です。

- **ログ** - プログラムのロギングを設定することができます。
- **添付の検査** - メール検査の設定、および検出された悪意のあるオブジェクトに対するプログラムのアクションを指定することができます。
- **統計** - 検査済み、および処理済みのオブジェクト数を確認することができます。



7.2. 脅威の検出

Dr.Web for Outlook は異なる様々な **検出手法** を使用します。**感染したオブジェクト** はユーザーが指定した **アクション** に応じて処理されます (感染したオブジェクトを修復、削除、または **隔離** へ移すことができます)。



7.2.1. 脅威の種類

Dr.Web for Outlook は、メール内の次の脅威を検出します。

- 感染したオブジェクト
- ファイルまたはアーカイブ内のボムウイルス
- アドウェア
- 侵入用ツール
- ダイアラー
- ジョークプログラム
- リスクウェア
- スパイウェア
- トロイの木馬
- コンピュータワームおよびウイルス

7.2.2. アクションの設定

Dr.Web for Outlook では、感染したファイル、疑わしいファイル、および悪意のあるオブジェクトをメール添付ファイルのスキャン中に検出した際のプログラムのアクションを指定することが出来ます。

メール添付ファイルのウイルススキャンを設定し、検出された悪意のあるオブジェクトに対するプログラムのアクションを指定するには、Microsoft Outlookメールアプリケーション内の **[ツール] -> [オプション] -> [Dr.Web Anti-virus]** タブ (Microsoft Outlook 2010の場合は **[ファイル]-> [オプション]** の **Dr.Web for Outlook** を選択して **[アドイン オプション]** ボタンをクリック) を選択し、**添付ファイルの検査** をクリックします。



添付の検査 ウィンドウでは、異なる種類の検査済みオブジェクトに対するアクション、および検査が失敗した際のアクションを指定します。アーカイブの検査を有効／無効にすることも出来ます。

ウイルス脅威を検出した際のアクションを設定するには以下のオプションを使用してください。

- **感染した** ドロップダウンリストでは、既知のウイルスに感染したファイルを検出した際のアクションを設定します。
- **修復されていない** ドロップダウンリストでは、既知の修復不可能なウイルスに感染したファイルを検出した際（またはファイルの修復に失敗した場合）のアクションを設定します。
- **疑わしい** ドロップダウンリストでは、ウイルスに感染している疑いのあるファイルを検出（ヒューリスティックアナライザーの対応によって）した際のアクションを設定します。
- **マルウェア** セクションでは、以下のような望ましくないソフトウェアを検出した



際のアクションを設定します。

- ダイアラ
- ジョークプログラム
- リスクウェア
- 侵入用ツール
- **検査エラーの時** ドロップダウンリストでは、添付ファイルを検査出来なかった場合（添付ファイルが破損していた、またはパスワード保護されていた場合など）のアクションを設定することができます。
- **アーカイブを検査する（推奨）** チェックボックスでは、添付されたアーカイブファイルの検査を有効 / 無効にすることができます。検査を有効にするにはチェックを入れ、無効にするにはチェックを外してください。

異なる種類のオブジェクトに対して、それぞれ個別にアクションが割り当てられます。

検出されたウイルス脅威に対して以下のアクションを設定することができます。

- **修復**（感染したオブジェクトに対してのみ）- オブジェクトの感染前の状態への復元を試みます。
- **修復不可能として対処**（感染したオブジェクトに対してのみ）- 修復不可能なオブジェクトに対して指定されたアクションが実行されます。
- **削除** - オブジェクトを削除します。
- **隔離** - オブジェクトを特別な **隔離** フォルダへ移動します。
- **スキップ** - いずれのアクションも実行せず、通知も表示せずにオブジェクトをスキップします。



7.4. ロギング

Dr.Web for Outlook では、次のログファイルにエラー及びアプリケーションイベントが記録されます。

- [Windowsのイベントログ](#)
- [Dr.Web デバッグテキストログ](#)

7.4.1. イベントログ

Dr.Web for Outlook は、Windows Event Logに以下の情報を記録します。

- プラグインの起動と停止
- ライセンスキーファイル/パラメータ:ライセンス認証、ライセンス期限 (情報はプログラムの起動時と動作中およびキーファイルの変更時に書き込まれます)
- ライセンスエラー:キーファイルが無い、キーファイル内でプログラムモジュールの使用が許可されていない、ライセンスがブロックされている、キーファイルが破損している (情報はプログラムの起動時および動作中に書き込まれます)
- プログラムモジュールのパラメータ:Scanner、エンジン、ウイルスデータベース (情報はプログラムの起動時およびモジュールの更新時に書き込まれます)
- 脅威の検出に関する情報
- ライセンス失効の通知 (失効の30日、15日、7日、3日、2日、および1日前にメールが記録されます)

イベントログを表示するには

1. **コントロールパネル**で、**管理ツール**→ **イベントビューア**を選択します。
2. ツリー表示で **アプリケーション** を選択します。ユーザーアプリケーションによってログに登録されたイベントの一覧が表示されます。**Dr.Web for Outlook** メールソースは **Dr.Web for Outlook アプリケーション** になっています。



7.4.2. デバッグテキストログ

Dr.Web for Outlook テキストログに以下の情報を記録することが出来ます。

- ライセンスの妥当性状況
- 検出された悪意のあるオブジェクトごとのマルウェア検出レポート
- 読み込み / 書き込みエラー、またはアーカイブやパスワード保護されたファイルのスキャン中に発生したエラー
- プログラムモジュールのパラメータ (**Scanner**、エンジン、**Dr.Web ウイルスデータベース**)
- 主要な障害
- ライセンス失効の通知 (失効の30日、15日、7日、3日、2日、および1日前にメールが記録されます)



ログファイルへのプログラムのロギングを有効にすると、サーバーパフォーマンスが低下します。そのため、**Dr.Web for Outlook** の動作中にエラーが発生した場合にのみロギングを有効にすることを推奨しています。

ロギングの設定

1. **Dr.Web Anti-virus** タブで、**ログ** をクリックします。ログ設定用のウィンドウが表示されます。
2. ログの詳細レベル (0 ~ 5) を指定します。
 - レベル 0 はロギングを無効にします。
 - レベル 5 は最も詳細なロギングのレベルです。デフォルトではロギングは無効になっています。
3. ログファイルサイズの上限を指定します (キロバイト)
4. **OK** をクリックして変更を保存してください。



Log ウィンドウは、管理者権限を持つユーザーのみが使用可能です。

Windows Vista 以降のOSでは **Log** をクリックした後、

- UACが有効な場合 : 管理者はプログラムの動作について確認を求められ、管理者権限のないユーザーはシステム管理者のアカウントを入力するよう要求されます。
- UACが無効な場合 : 管理者はプログラム設定を変更できますが、ユーザーは設定の変更にアクセスできません。



プログラムログを見る

テキストログを開くには、**ログを見る** をクリックします。

7.5. 統計

Microsoft Outlookメールアプリケーション内の[ツール] -> [オプション] -> [Dr. Web Anti-virus] タブ (Microsoft Outlook 2010の場合は [ファイル]-> [オプション] の **Dr.Web for Outlook** を選択して [アドイン オプション] ボタンをクリック)を選択すると、プログラムによって検査・処理されたオブジェクトの総数を統計情報として確認することができます。

スキャン済みオブジェクトは次のよう分類されます。

- **検査された** - 検査されたメールの総数
- **感染した** - ウイルスを保有しているメールの数
- **疑わしい** - ウイルスに感染していると思われるメールの数 (ヒューリスティックアナライザー対応時)
- **修復された** - プログラムによって修復されたオブジェクトの数
- **検査されていない** - 検査できない、またはスキャン中にエラーが発生したオブジェクトの数
- **感染していない** - 感染していないメッセージの数

アクションが適用されたオブジェクトの以下のカテゴリ別の数が指定されます。

- **隔離された** - **隔離** へ移されたオブジェクトの数
- **削除された** - システムから削除されたオブジェクトの数
- **スキップされた** - 変更せずにスキップされたオブジェクトの数

デフォルトでは、統計情報ファイルは %USERPROFILE%\DoctorWeb フォルダ (Windows 7ではC:\Users\ <ユーザー名> \ DoctorWeb)内の drwebforoutlook.stat ファイルです。統計情報を消去するには、このファイルを削除してください。



drwebforoutlook.stat 統計情報ファイルは、システムユーザーごとに個別に用意されます。



8. Dr.Web Firewall

Dr.Web® Firewall は不正アクセスからパソコンを守り、ネットワーク経由で重要なデータが漏洩するのを防ぎます。また、接続の試行やデータのやり取りをモニターし、望まぬ接続や疑わしい接続をネットワークレベル及びアプリケーションレベルの両方でブロックします。

主な機能

Dr.Web Firewall は以下の機能を備えています。

- 全ての送受信トラフィックの管理およびフィルタリング
- アプリケーションレベルでのアクセス制御
- ネットワークレベルでのパケットフィルタリング
- ルールセットの高速選択
- イベントのロギング

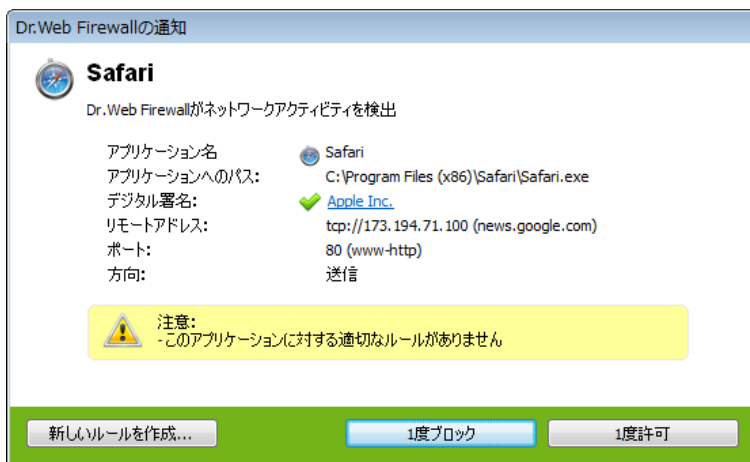
8.1. Dr.Web Firewall の学習

デフォルトでは、インストールが完了すると **Dr.Web Firewall** は全ての新しい（ファイアウォールにとって未知の）接続試行を傍受し、必要なアクションを選択するようユーザーにプロンプトを出すことでOSの通常の動作を学習していきます。

一時的なソリューションを選択するか、または **Dr.Web Firewall** が同様の接続を検出するたびに適用されるルールを作成します。



制限付きユーザーアカウント(ゲスト)を使用している場合、**Firewall** はネットワークアクセスの試行に対するプロンプトを表示しません。管理者権限でのセッションが同時にアクティブになっている場合、通知はそのセッションに転送されません。



接続試行に対するアクション

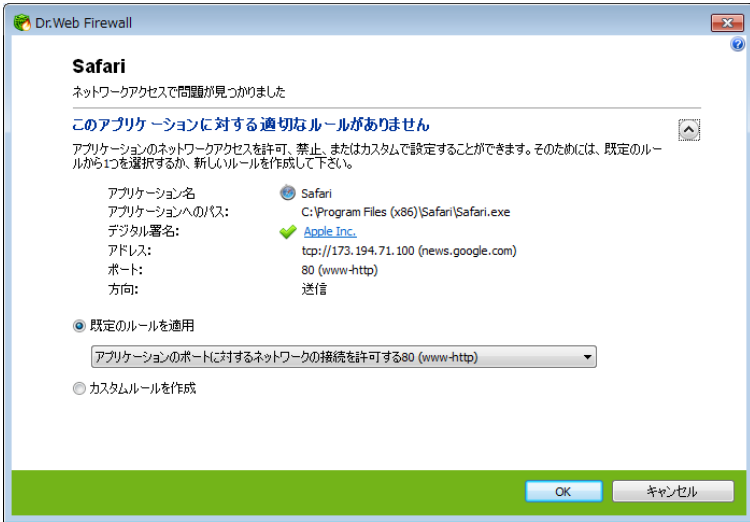
1. ルールを決定する際には、表示される以下の情報を確認してください。

情報	説明
アプリケーション名	アプリケーション名。アプリケーションへのパス フィールドに示されたパスがプログラムの正しい場所と一致していることを確認して下さい。
アプリケーションへのパス	アプリケーションの実行ファイルへのフルパスとファイル名
デジタル署名	アプリケーションのデジタル署名
アドレス	使用するプロトコルとアプリケーションが接続を試行しているネットワークアドレス
ポート	接続で使用されるポート番号
方向	接続の方向

2. 適切なアクションを選択してください。
 - この接続を1回ブロックするには、**1度ブロック**を選択します。
 - この接続を1回許可するには、**1度許可**を選択します。
 - 新しいアプリケーションのフィルタリングルールを作成するウィンドウを開くには、**新しいルールを作成**を選択して下さい。表示されたウィンドウ内で既定のルールを選択するか、または新しい **アプリケーション**

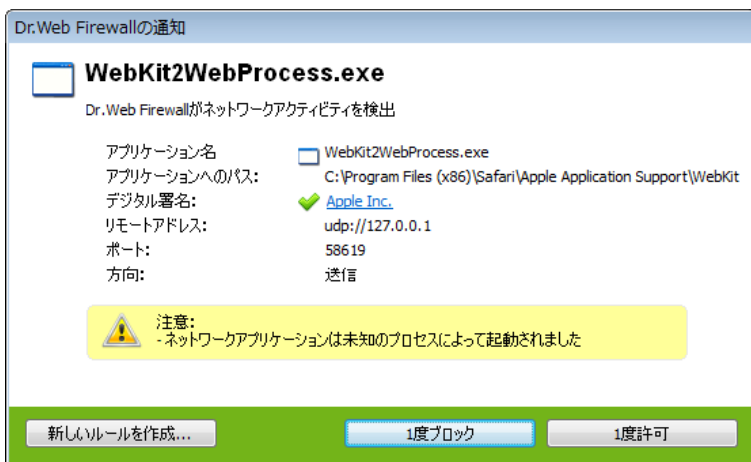


ルールを作成 してください



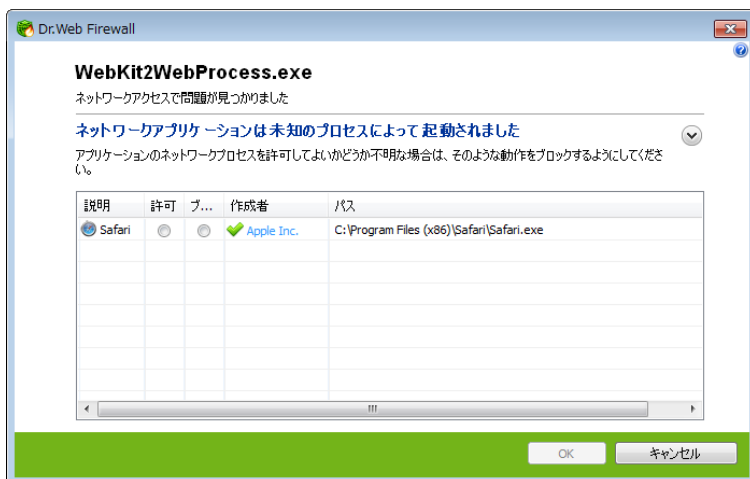
3. **OK** をクリックしてください。Dr.Web Firewall は、選択されたアクションを実行して通知ウィンドウを閉じます。

接続が信頼できるアプリケーション (ルールが既に設定されている) によって開始されているが、このアプリケーションが未知の親プロセスによって実行されている場合は該当する警告が表示されます。



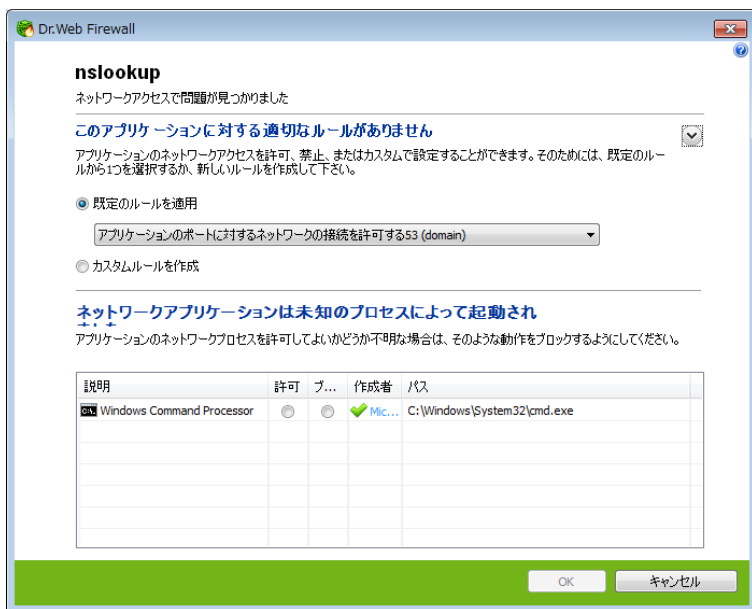
親プロセスルールの設定

1. 通知内に表示された親プロセスに関する情報を確認してください。
 - この接続を1回ブロックするには、**ブロック**をクリックします。
 - この接続を1回許可するには、**許可**をクリックします。
 - 新しいアプリケーションのフィルタリングルールを作成するウィンドウを開くには、**新しいルールを作成**を選択して下さい。表示されたウィンドウ内で既定のルールを選択するかまたは新しい**親プロセスルールを作成**して下さい。



2. **OK** をクリックしてください。 **Dr.Web Firewall** は、選択されたアクションを実行して通知ウィンドウを閉じます。

未知のプロセスが別の未知のプロセスによって実行された場合、該当する情報が表示されます。**新しいリールを作成** を選択した場合は新しいウィンドウが表示され、アプリケーションおよびその親プロセスの新しいリールを作成することができます。



ルールを作成するには管理者権限が必要です。

8.2. Dr.Web Firewall の管理

Dr.Web Firewall はネットワークコンポーネントとしてインストールされ、Windowsのスタートアップと同時に起動します。必要な場合、**Dr.Web Firewall** を一時停止、その統計を閲覧、設定を変更することができます。

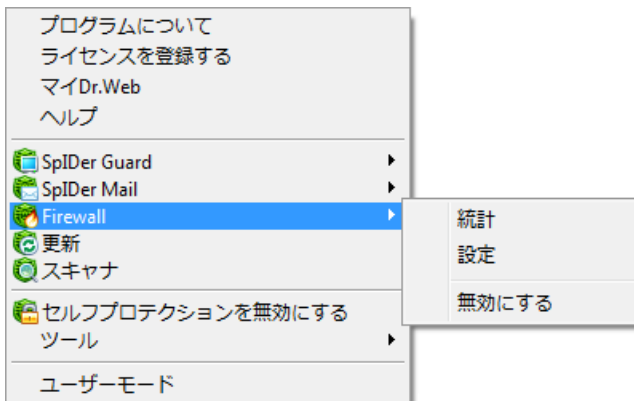


制限つきユーザーアカウント(ゲスト)でセッションが開始されると、**Firewall** はアクセスエラーメッセージを表示します。**SpIDer Agent** にはFirewallの状態は無効と表示されますが、実際は**Firewall** は有効で、デフォルトの設定または以前に管理者モードで設定された設定で動作します。

SpIDer Agent を使用して **Dr.Web Firewall** の主要な設定および管理を



行うことができます。**SpIDer Agent** アイコン  をクリックし **Firewall** を選択してください。



オプション	説明
統計	Dr.Web Firewall によって処理されたイベントに関する 情報 を表示します。
設定	Dr.Web Firewall 設定 を開きます。 Dr.Web Anti-virus 一般設定 の 復元 ページで、設定をデフォルト値に戻すことができます。
無効にする / 有効にする	Dr.Web Firewall の動作を停止または再開します。 有効にする は、動作が一時停止されている場合にのみ表示されます。



設定 および **無効にする / 有効にする** は、**ユーザー** モードでは使用することが出来ません。

一時的な停止

Dr.Web Firewall による、HTTP送受信トラフィックのアンチウイルス検査を一時的に停止することができます。



このオプションは ユーザー モードでは使用できません。

このオプションは十分に注意して使用してください。

Dr.Web Firewall を無効にするには

通知領域内で **SpIDer Agent** アイコン  をクリックし、**Firewall** を選択した後に **無効にする** を選択します。



Dr.Web Firewall を無効にするには、確認コードまたはパスワード(**Dr. Web Anti-virus 一般設定** 内の **セルフプロテクション** ページで **Dr.Web** の設定をパスワードで保護する チェックボックスにチェックを入れている場合)を入力してください。

Dr.Web Firewall を有効にするには

通知領域内で **SpIDer Agent** アイコン  をクリックし、**Firewall** を選択した後に **有効にする** を選択します。



8.3. Firewall の設定



Dr.Web Firewall の設定を行うには管理者権限が必要です。

Dr.Web Firewall の使用を開始するには、次の設定が必要です。

- プログラムの動作モードを **選択** する
- 許可するアプリケーションの **リストを設定** する


Dr.Web Firewall はWindowsのスタートアップと同時に起動し、イベントの **ロギング** を開始します。デフォルトでは **Dr.Web Firewall** は **学習** モードで動作します。



Internet Connection Sharing (インターネット接続共有) に問題が発生した場合 (ホストコンピュータに接続されているコンピュータからのインターネット接続がブロックされているなど)、ローカル設定に応じて、サブネットからの全てのパケットを許可する **パケットフィルタリングルール** をホストコンピュータ上で指定してください。

SpIDer Agent によって、**Dr.Web Firewall** の管理および設定を行うことができます。デフォルトの設定は多くの場合に最適なものとなっています。必要のない限り変更しないようにしてください。

Dr.Web Firewall の設定

1. 通知領域内で **SpIDer Agent** アイコン  をクリックし、**Firewall** を選択した後 **設定** を選択します。以下のページを含んだ設定ウインドウの **Firewall** タブが開きます。
 - **アプリケーション** ページ - アプリケーションに対するフィルタリングパラメータを設定することができます。
 - **親プロセス** ページ - 別のアプリケーションによって起動されたアプリケーションに対するルールを設定することができます。
 - **インターフェイス** ページ - ネットワークパケットレベルでのフィルタリングパラメータを設定することができます。
 - **アドバンス** ページ - **Dr.Web Firewall** の動作モードを選択することができます。
2. 必要なオプションを設定してください。ページ内のオプションに関する情報



を参照するには **ヘルプ** をクリックします。

3. 設定終了後、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** をクリックします。

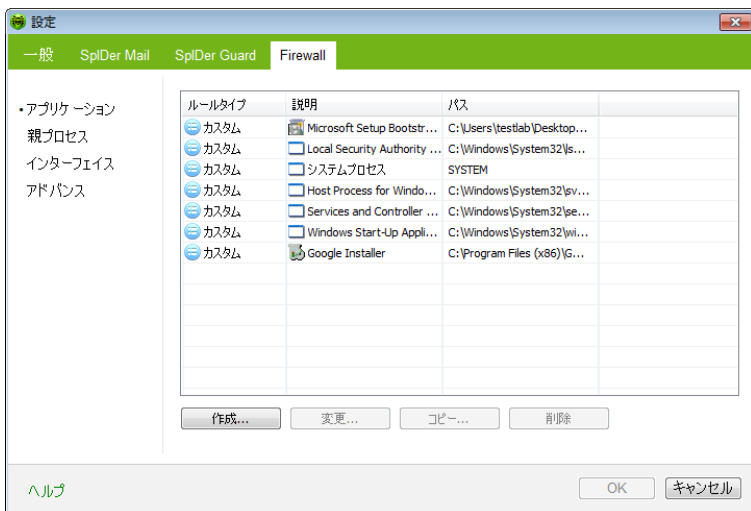
8.3.1. アプリケーション

アプリケーションレベルのフィルタリングにより、様々なアプリケーションおよびプロセスのネットワークリソースへのアクセスを管理することができます。システムとユーザーアプリケーションの双方に対してルールを作成することができます。

このページには **アプリケーションフィルターのルールが設定されている** 全てのアプリケーションとプロセスの一覧が表示されます。各アプリケーションはその実行ファイルへのパスによって明確に示されます。**Dr.Web Firewall** はオペレーティングシステムカーネル（一意の実行ファイルがないシステムプロセス）に適用するルールセットを示すためにSYSTEM名を使用します。



各アプリケーションに対して作成できるルールセットは1つのみです。





ルールセットの作成

Dr.Web Firewall の設定ウィンドウで **アプリケーション** ページを開き、次のいずれかを行ってください。

- 新しいルールセットを追加するには、**作成** をクリックしてください。
- 既存のルールセットを編集するには、リスト内で該当するルールセットを選択し **変更** をクリックしてください。
- 既存のルールセットのコピーを追加するには、リスト内で該当するルールを選択し **コピー** をクリックしてください。コピーしたルールは選択したルール(コピー元)の後に追加されます。
- アプリケーションに対する全てのルールセットを削除するには、リスト内で該当するルールセットを選択し **削除** をクリックしてください。



ルールが作成されたアプリケーションファイルが変更された場合(更新などによって)、**Dr.Web Firewall** はアプリケーションのネットワークへのアクセス許可について再度確認を行います。

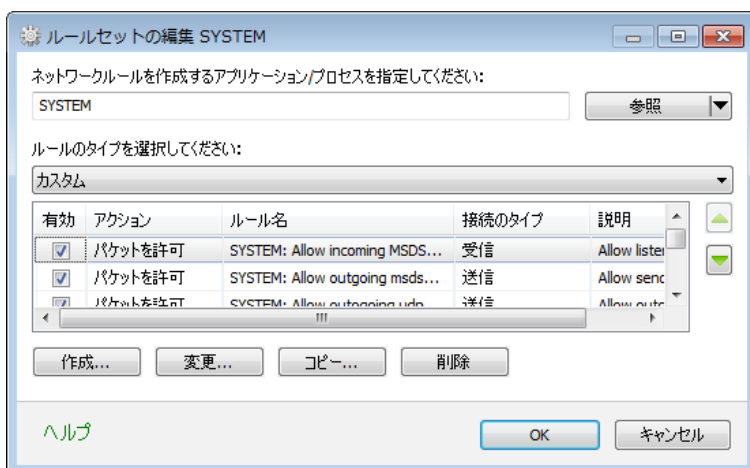
アプリケーションルール

新しいアプリケーションルールを作成(または **ルールセットの編集**)ウィンドウには、アプリケーションまたはプロセスに対するフィルタリングルールのタイプ及び、**カスタム** を選択した場合にはルールセットの一覧が表示されます。ルールのタイプは変更することができ、アプリケーション用の新しいルールを追加したり既存のルールとそれらの実行順序を変更することによってリストを編集することも可能です。ルールはセット内での順番に従って適用されます。

Dr.Web Firewall が **学習モード** で動作している場合、未知の接続が試行された際に表示される通知ウィンドウから直接新しいルールの作成を行うことができます。

新しいアプリケーションルール作成のウィンドウを開くには

Dr.Web Firewall **設定** ウィンドウ内で **アプリケーション** ページを選択します。ページ内で **作成** をクリックするか、アプリケーションを選択した後 **変更** をクリックします。



セット内の各ルールに対し次の情報が表示されます。

項目	説明
有効	ルールのステータス
アクション	インターネットへの接続試行を検出した際に Dr.Web Firewall が実行するアクション <ul style="list-style-type: none">• パケットをブロック• パケットを許可
ルール名	ルールの名前
接続のタイプ	接続の方向 <ul style="list-style-type: none">• 受信 - コンピューター上のアプリケーションに対してネットワークから接続が試行された場合にルールが適用されます• 送信 - コンピューター上のアプリケーションからネットワークへの接続が試行された場合にルールが適用されます• 全て - 接続の方向に関わらずルールが適用されます
説明	ルールの説明



ルールの作成

- 開いたウィンドウ内で、ルールセットを適用するアプリケーションを指定して下さい。
 - ユーザープログラムに対してルールセットを作成する場合、**参照** をクリックし、アプリケーション実行ファイルを選択します。
 - プロセスに対してルールセットを作成する場合、**参照** 上の矢印をクリックし、**動作中のアプリケーション** を選択してプロセスを選びます。
- ルールのタイプを指定します。
 - 全て許可** - 全ての接続が許可されます。
 - 全てブロック** - 全ての接続がブロックされます。
 - カスタム** - このモードでは、異なる接続を許可 / ブロックするルールのセットを作成できます。
- カスタム** タイプを選択した場合、次のオプションを使用してフィルタリングルールを作成して下さい。
 - 新しいルールを作成するには、**作成** をクリックして下さい。作成されたルールはリストの最後に追加されます。
 - ルールを編集するには、該当するルールを選択し **変更** をクリックして下さい。
 - ルールのコピーを作成するには、該当するルールを選択し **コピー** をクリックして下さい。コピーしたルールは、選択したルール (コピー元) の後ろに追加されます。
 - ルールを削除するには、該当するルールを選択し **削除** をクリックして下さい。
- 新しいルールの作成、または既存のルールの編集を選択した場合、開いたウィンドウ内で **ルールの設定** を行って下さい。
- ルールの順番を変更するにはリスト横にある矢印を使用します。ルールはセット内での順番に従って適用されます。
- 設定の編集後、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** をクリックして下さい。

ルールの設定

アプリケーションのフィルタリングルールは、特定のアプリケーションと特定のネットワークホスト間の通信を制御します。



ルールの追加と編集

1. 以下のパラメーターを設定します。

パラメータ	説明
全般	
ルール名	ルールの名前
説明	ルールの説明
ステータス	ルールのステータス <ul style="list-style-type: none">• 有効 - ルールが適用されます• 無効 - ルールはまだ適用されません
接続の種類	接続の方向 <ul style="list-style-type: none">• 受信 - コンピューター上のアプリケーションに対してネットワークから接続が試行された場合にルールが適用されます• 送信 - コンピューター上のアプリケーションからネットワークへの接続が試行された場合にルールが適用されます• 全て - 接続の方向に関わらずルールが適用されます



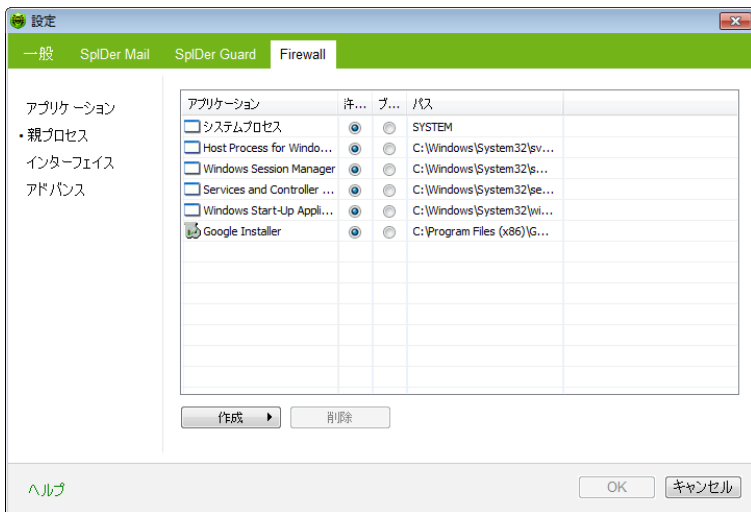
パラメータ	説明
アクション	インターネットへの接続試行を検出した際に Dr. Web Firewall が実行するアクション <ul style="list-style-type: none">• パケットをブロック• パケットを許可
ルールの設定	
プロトコル	接続で使用されるネットワークと通信レベルのプロトコルを指定します。 Dr. Web Firewall は次のネットワークプロトコルをサポートしています。 <ul style="list-style-type: none">• IPv4• IPv6• IP all – 全てのIPプロトコル Dr. Web Firewall は次の通信レベルのプロトコルをサポートしています。 <ul style="list-style-type: none">• TCP• UDP• TCP & UDP – TCPまたはUDPプロトコル
ローカルアドレス	リモートホストのIPアドレス、特定のアドレス(等しい)またはアドレスの範囲(範囲内)を使用した複数のIPアドレス、特定のサブネットマスク(マスク)、お使いのコンピューターがネットワークアドレスを持つ全てのサブネットマスク(MY_NETWORK)のいずれかを指定することができます。 全てのリモートホストに対してルールを作成するには、 全て を選択して下さい。
ローカルポート	接続が行われるポート、特定のポート番号(等しい)またはポートの範囲(範囲内)のいずれかを指定することができます。 全てのポートに対してルールを適用するには、 全て を選択して下さい。

2. 設定の終了後、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** をクリックして下さい。



8.3.2. 親プロセス

このページでは、アプリケーションやプロセスによる他のアプリケーションの実行を許可 / ブロックするためのルールを設定することができます。



親プロセスに対するルールを追加する

1. 親プロセスを選択してください。
 - アプリケーションに対する新しいルールを設定するには、**作成** をクリックしてプログラムの実行ファイルを選択して下さい。
 - 実行中のプロセスに対する新しいルールを追加するには、**作成** 上の矢印をクリックし、動作中のアプリケーションを選択してプロセスを選びます。
2. 必要なアクションを設定してください。
 - **ブロック** アプリケーションが他のプロセスを実行することを禁止します
 - **許可** アプリケーションが他のプロセスを実行することを許可します

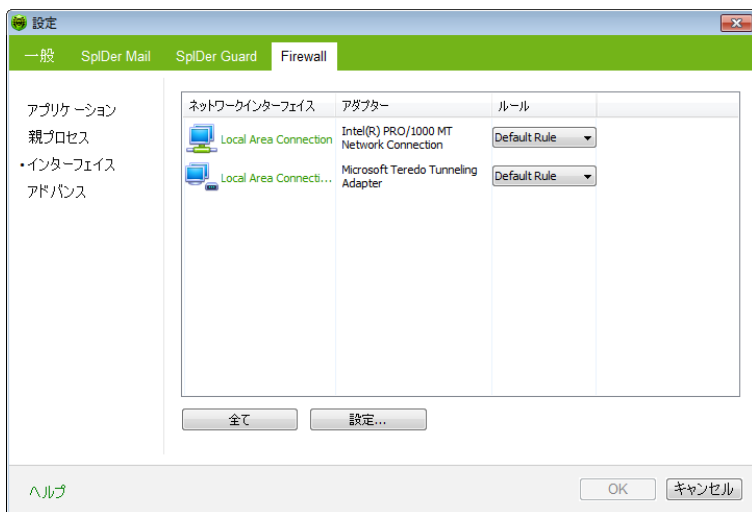
デフォルトでは、新しいプロセスはブロックされます。



ルールが設定されている親プロセスの実行ファイルが変更された場合（更新後など）**Firewall** はユーザーに対してプロンプトを出し、ルールを再度確定し、この親プロセスによる今後のアプリケーションの実行を許可するよう要求します。

8.3.3. インターフェイス

インターフェイス ページで、コンピューター上にインストールされた異なるネットワークインターフェイス経由でやり取りされるパケットをフィルタリングするためのルールセットを選択することができます。



ネットワークインターフェイスに対するルールセットの設定

1. **Dr.Web Firewall** 設定ウィンドウ内で **インターフェイス** を選択します。
2. 該当するインターフェイスに対して、適切なルールセットを選択してください。ルールセットが存在しない場合は新しいパケットフィルタリングルールを **作成** することができます。
3. 設定を保存するには **OK** を、保存せずにウィンドウを閉じるには **キャンセル** をクリックしてください。

利用可能な全てのインターフェイスをリストに加えるには **全て** をクリックします。リス



ト上に永続的に加えられるインターフェースを選択するためのウィンドウが開きます。アクティブなインターフェースは自動的にリスト上に表示されます。

インターフェースに対するルールを設定するには **設定** をクリックします。

パケットフィルター

パケットフィルタリングによって、どのプログラムからの接続であるかに関係なく、ネットワークへのアクセスを管理することができます。**Dr.Web Firewall** は、コンピュータの **ネットワークインターフェース** を経由してやり取りされるネットワークパケットに対してそれらのルールを適用します。

また、**アプリケーションフィルター** より低いレベルにあるネットワークへのアクセスを管理することができるため、より柔軟な選択が可能になります。

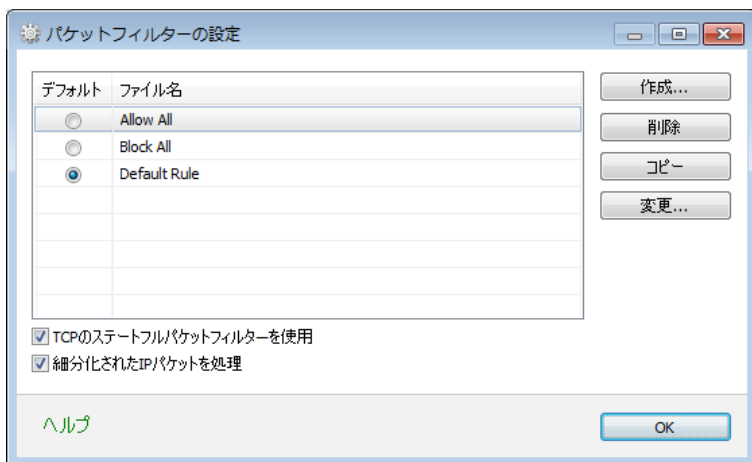
Dr.Web Firewall のデフォルトのフィルタリングルールセットは次のとおりです。

- **Allow All** – 全てのパケットを通過させます
- **Block All** – 全てのパケットをブロックします
- **Default Rule** – このセットには、最も標準的なシステム設定を記述したルールと一般的なネットワーク攻撃を防ぐルールが含まれています。このルールセットは、新しい **ネットワークインターフェース** に対してデフォルトで使用されます。

フィルタリングモード間の切り替えを簡単にするために、フィルタリングルールのカスタムセットを作成することができます。

ネットワークインターフェースに対するルールセットの設定

1. **Dr.Web Firewall** の設定ウィンドウ内で **パケットフィルター** ページを選択します。
2. 次のうちいずれかを実行します。
 - 新しいルールを追加、既存のルールを変更・削除、またはルール実行の順番を変更するなどフィルタリングのルールセットを **設定** する。
 - 一般的なフィルタリングの **設定** を行う(追加設定)。



フィルタリングルールセットの設定

次のいずれかを実行してください。

- 新しいルールを追加するには、**作成** をクリックしてください。作成されたルールはリストの先頭に追加されます。
- 既存のルールセットを編集するには、該当するルールセットをリスト上で選択し**変更** をクリックしてください。
- 既存のルールセットのコピーを追加するには、該当するルールセットを選択し **コピー** をクリックしてください。コピーされたルールは、選択されたルールセットの後ろに追加されます。
- 既存のルールセットを削除するには、該当するルールセットを選択し **削除** をクリックしてください。

追加設定

パケットフィルターの設定 内では、以下のオプションを選択することができます。



オプション	説明
TCPのステートフルパケットフィルタを使用	<p>既存のTCP接続の状態に応じてパケットをフィルタリングするにはこのチェックボックスにチェックを入れてください。TCPプロトコルの分類によるアクティブな接続に適合しないパケットは Dr.Web Firewall によってブロックされます。このオプションによってDoS攻撃（サービスの拒否）、リソースのスキャン、データの挿入、その他悪意のある操作からコンピュータを保護することができます。</p> <p>複雑なデータ伝達アルゴリズムを持つプロトコル（FTP、SIPなど）を使用する際にも、このチェックボックスにチェックを入れることを推奨します。</p> <p>TCP接続の状態に関係なくパケットをフィルタリングする場合は、チェックを外してください。</p>
細分化されたパケットを処理	<p>大容量のデータのやり取りを処理するには、このチェックボックスにチェックを入れてください。パケットの最大サイズ（MTU - Maximum Transmission Unit）はネットワークによって変動します。そのため、大きいIPパケットは通信の際にいくつかのパケットに分けられることがあります。このオプションを有効にすると、細分化されたパケットのうち最初のパケットに適用されたルールが、残りの全てのパケットにも適用されます。</p> <p>細分化されたパケットをそれぞれ個別に処理する場合は、チェックを外してください。</p>

パケットフィルタールールセット

パケットルールの追加（または **ルールセットの編集**）ウィンドウには、選択したルールセットに含まれるパケットフィルタールールのリストが表示されます。新しいルールセットを作成する、既存のルールセットを編集する、またルールを実行する順番を変更することができます。ルールはセット内での順番に従って適用されます。



セット内の各ルールに対して以下の情報が表示されます。

項目	説明
有効	ルールのステータス
アクション	インターネットへの接続試行を検出した際に Dr.Web Firewall が実行するアクション <ul style="list-style-type: none">• パケットをブロック• パケットを許可
ルール名	ルールの名前
方向	パケットの送信者 <ul style="list-style-type: none">• ← → - コンピュータがネットワークからパケットを受信する場合にルールが適用されます• → - コンピュータからネットワーク内にパケットが送信される場合にこのルールが適用されます• ↔ - パケットの送信方向に関わらずルールが適用されます
ログ	ルールのロギングモード。 Dr.Web Firewall のログに記録する情報を指定します。 <ul style="list-style-type: none">• ヘッダのみ - パケットのヘッダのみをログに記録します• パケット全体 - パケット全体をログに記録します



項目	説明
	<ul style="list-style-type: none">無効 - いずれの情報も記録しません
説明	ルールの説明

新しいルールセットを作成する、既存のルールセットを編集する、またルールを実行する順番を変更することができます。ルールはセット内での順番に従って適用されます。

ルールセットの設定

- パケットルールの追加** ページで、新しいルールの作成または既存のルールの編集を選択した場合、開いたウィンドウ内でルールセット名を指定して下さい。
- 次のオプションを使用してフィルタリングルールを作成して下さい。
 - 新しいルールを作成するには、**作成** をクリックして下さい。作成されたルールはリストの先頭に追加されます。
 - ルールを編集するには、該当するルールを選択し **変更** をクリックして下さい。
 - ルールのコピーを作成するには、該当するルールを選択し **コピー** をクリックして下さい。コピーされたルールは、選択されたルールの後ろに追加されます。
 - ルールを削除するには、該当するルールを選択し **削除** をクリックして下さい。
- 新しいルールの作成、または既存のルールの編集を選択した場合、開いたウィンドウ内で **ルールの設定** を行って下さい。
- ルールの順番を変更するにはリスト横にある矢印を使用します。ルールはリスト内での順番に従って適用されます。
- 設定の編集後、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** をクリックして下さい。



ルールセット内のルールが設定されていないパケットは、**アプリケーションフィルタ** - ルールによって許可されているものを除き、自動的にブロックされます。



パケットフィルタリングルール

ルールの追加と編集

1. パケットフィルタリングルールセットの作成または編集ウィンドウで **作成** または **変更** をクリックしてください。パケットフィルタリングルールの作成・編集ウィンドウが開きます。

パケットルールの追加

ルール名: 新しいルール

説明: ルールの説明

アクション: パケットを許可

方向: 受信

ログ: 無効

基準: ARP

追加

ヘルプ OK キャンセル

2. 次のパラメータを設定してください。

パラメータ	説明
ルール名	ルールの名前
説明	ルールの説明
アクション	インターネットへの接続試行を検出した際に Dr. Web Firewall が実行するアクション <ul style="list-style-type: none">• パケットをブロック• パケットを許可
方向	パケットの送信者 <ul style="list-style-type: none">• 受信 - コンピュータがネットワークからパケットを受信する場合にルールが適用されます• 送信 - コンピュータからネットワーク内にパケットが送信される場合にルールが適用されます



パラメータ	説明
	<ul style="list-style-type: none">• 全て - パケットの送信方向に関わらずルールが適用されます
ログ	ルールのロギングモード。Dr.Web Firewall のログに記録する情報を指定します。 <ul style="list-style-type: none">• ヘッダのみ - パケットのヘッダのみをログに記録します• パケット全体 - パケット全体をログに記録します• 無効 - いずれの情報も記録しません
基準	フィルタリングの基準 (トランスポートプロトコルやネットワークプロトコルなど)。フィルタリング基準を追加するには、リストから基準を選択し 追加 をクリックしてください。フィルタリング基準は任意の数だけ追加することができます。ヘッダの中には追加の基準を設定することが可能なものもあります。

3. 設定の編集後、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。



いずれの基準も指定しなかつた場合、**アクション** フィールドの設定に応じて全てのパケットを許可またはブロックします。

例：

サブネットワークからの全てのパケットを許可するパケットフィルターの追加は次のようになります。



パケットルールの追加

ルール名: 新しいルール

説明: ルールの説明

アクション: パケットを許可

方向: 受信

ログ: 無効

基準: DestOpt

追加

Authentication
設定できるパラメーターがありません

TCP

ローカルポート: 全て

リモートポート: 全て

ヘルプ

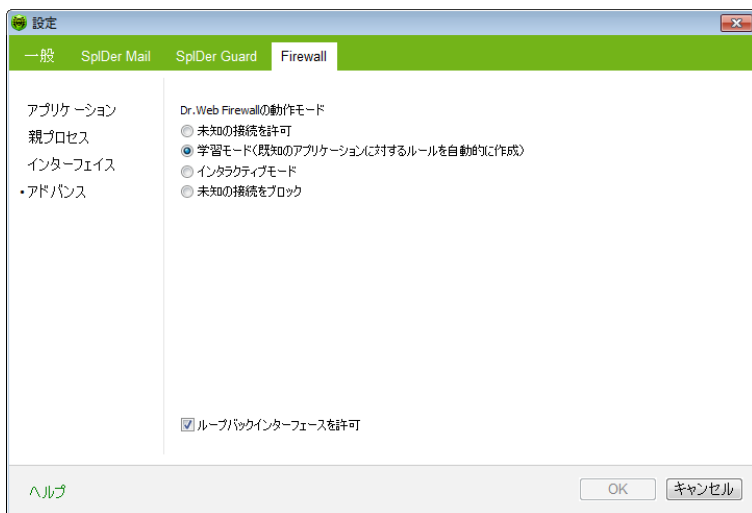
OK

キャンセル

ローカルIPアドレス 及び リモートIPアドレス で 全て を選択した場合、IPv4ヘッダを含みローカルコンピュータの物理アドレスから送信された全てのパケットに対してルールが適用されます。

8.3.4. アドバンス

アドバンス ページで、**Dr.Web Firewall** が新しいファイアーウォールにとって未知の接続の試行を検知した際に行うデフォルトの動作を選択し、アドバンス設定を行うことができます。これらのルールはアプリケーションレベルで適用されます。



動作モードの設定

1. **Dr.Web Firewall** 設定ウィンドウ内で **アドバンス** を選択します。
2. 以下の動作モードの内いずれかを選択してください。
 - **インタラクティブモード**
 - (デフォルト) **学習モード(既知のアプリケーションに対するルールを自動的に作成)** - 学習モード。既知のアプリケーションに対するルールが自動的に作成されます。
 - **未知の接続をブロック** - アクセスを制限するモード。 **Dr.Web Firewall** にとって未知の接続を全てブロックします。既知の接続に対しては適切なルールが適用されます。
 - **未知の接続を許可** - フリーアクセスモード。未知のアプリケーションからのネットワークへのアクセスを全て許可します。
3. 設定を保存するには **OK** を、保存せずにウィンドウを閉じるには **キャンセル** をクリックしてください。

インタラクティブモード

このモードでは、未知の接続を検出した際の **Dr.Web Firewall** の動作をユーザーによって完全に管理します。これにより、コンピューターで作業を行っている間に



プログラムの学習が行われます。

ユーザーアプリケーションまたはオペレーティングシステムからネットワークへの接続が試行された場合、**Dr.Web Firewall** はそれらのアプリケーションに対するフィルタリングルールセットが設定されているかどうかを確認します。ルールが設定されていない場合、一時的なソリューションを選択するか、または同様の接続を検出するたびに繰り返し適用されるルールを作成するようユーザーに提案します。

学習モード

このモードでは、既知のアプリケーションに対するルールが自動的に作成されます。その他のアプリケーションに対する**Dr.Web Firewall**の動作はユーザーによって管理されます。

ユーザーアプリケーションまたはオペレーティングシステムからネットワークへの接続が試行された場合、**Dr.Web Firewall** はそれらのアプリケーションに対するフィルタリングルールセットが設定されているかどうかを確認します。ルールが設定されていない場合、一時的なソリューションを選択するか、または同様の接続を検出するたびに繰り返し適用されるルールを作成するようユーザーに提案します。

デフォルトではこのモードが適用されます。

未知の接続をブロック

このモードでは、インターネットも含めたネットワークリソースへの未知の接続を全てブロックします。

ユーザーアプリケーションまたはオペレーティングシステムからネットワークへの接続が試行された場合、**Dr.Web Firewall** はそれらのアプリケーションに対するフィルタリングルールセットが設定されているかどうかを確認します。ルールが設定されていない場合、ユーザーに対する通知の表示なしに、ネットワークへのアクセスをブロックします。ルールが設定されている場合は、指定されたアクションに応じて接続を処理します。

未知の接続を許可



このモードでは、インターネットも含めたネットワークリソースへの未知の接続を全て許可します。接続試行の検出に関する通知は表示されません。

アドバンス設定

コンピューター上の全てのアプリケーション間の相互接続を許可する(コンピューター上にインストールされたアプリケーション間の接続を無制限に許可する)には **ループバックインターフェースを許可** チェックボックスにチェックを入れてください。このタイプの接続には、いずれのルールも適用されません。ネットワーク経由での接続およびコンピューター内での接続の両方に対してルールを適用する場合はチェックを外してください。

8.4. イベントログ

Dr.Web Firewall は、接続の試行およびネットワークパケットをログに記録します。統計ウィンドウで以下のログを確認することができます。

- **アプリケーションフィルターログ (アプリケーションログ)** - 様々なアプリケーションからのネットワークへの接続試行と、それらに対して適用されたルールに関する情報が保存されます。
- **パケットフィルターログ (パケットフィルターのログ)** - **Firewall** によって処理されたネットワークパケット、パケットの処理に適用されたルール、パケットのやり取りに使用されたネットワークインターフェースに関する情報が保存されます。詳細レベルは各パケットアプリケーションルールの設定に依存します。

アクティブなアプリケーション のページには、その時点でネットワークに接続されている **アプリケーション** のリストが表示されます。

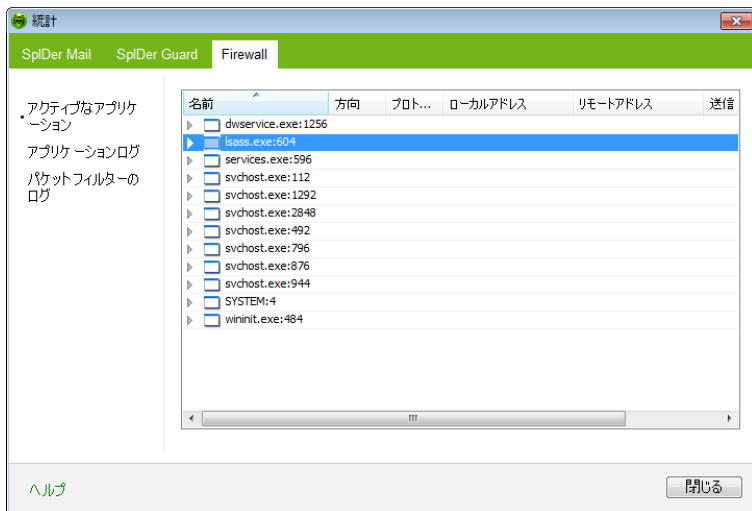
統計ウィンドウを開くには

通知領域内で **SpIDer Agent** アイコン  をクリックし、**Firewall** を選択した後 **統計** を選びます。



8.4.1. アクティブなアプリケーション

アクティブなアプリケーションのリストは、その時点でネットワークにアクセスしているアプリケーションに関する情報が表示されます。



各アプリケーションに関する以下の情報が表示されます。

項目	説明
名前	アプリケーションの名称
方向	接続の方向 <ul style="list-style-type: none">受信 - コンピューター上のアプリケーションに対してネットワークから接続が試行された場合にルールが適用されます送信 - コンピューター上のアプリケーションからネットワークへの接続が試行された場合にルールが適用されます受信待機 - コンピューター上のアプリケーションがネットワークからの接続を待っている状態である場合にルールが適用されます
プロトコル	データのやり取りに使用されるプロトコル



項目	説明
ローカルアドレス	接続を試行したプロトコルおよびホストアドレス
リモートアドレス	接続試行の対象であるプロトコルおよびホストアドレス
送信	この接続を介して送信されたデータの大きさ(バイト)
受信	この接続を介して受信されたデータの大きさ(バイト)

アクティブなアプリケーションのページ内では、リスト上にあるアクティブなプロセスを右クリックし **プロセスを終了** を選択することでそれらを停止させることができます。

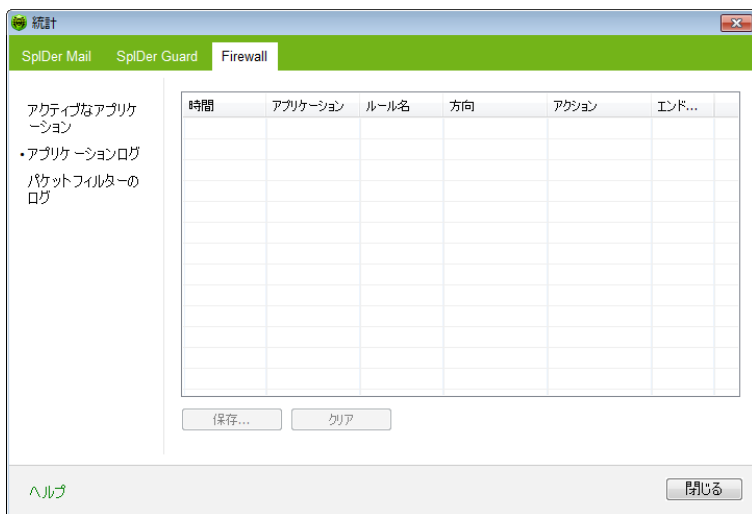


アクティブなプロセスを終了させるには管理者権限が必要です。それ以外の場合、中断できるのはお使いのアカウントで実行しているプロセスのみです。

アクティブな接続のブロック、またはアクティブでない接続のブロック解除はコンテキストメニューからも行うことができます。ブロックされた接続はリスト内で赤く表示されません。

8.4.2. アプリケーションログ

アプリケーションログには、コンピューターにインストールされたアプリケーションからネットワークへの接続試行に関する情報が保存されます。



項目	説明
時間	接続が試行された日時
アプリケーション	アプリケーション実行ファイルへのフルパス、そのアプリケーション名およびプロセスID番号 (PID)
ルール名	適用されたルールの名前
方向	接続の方向 <ul style="list-style-type: none">受信 - コンピューター上のアプリケーションに対してネットワークから接続が試行された場合にルールが適用されます送信 - コンピューター上のアプリケーションからネットワークへの接続が試行された場合にルールが適用されます全て - 接続の方向に関わらず適用されます
アクション	インターネットへの接続試行を検出した際に Dr.Web Firewall が実行する操作 <ul style="list-style-type: none">パケットをブロックパケットを許可
エンドポイント	接続に使用されるプロトコル、IPアドレス、ポート



このページ上で、ログをファイルに保存またはクリアすることができます。

アプリケーションフィルターログの保存

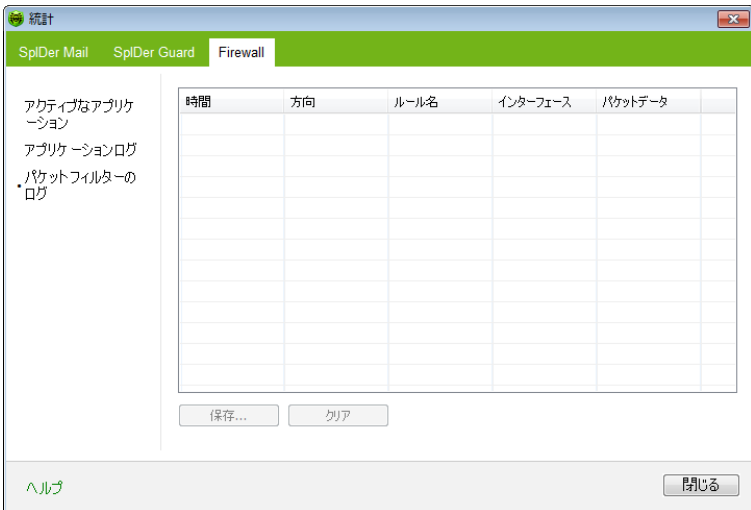
保存 をクリックし、ログの保存先となるファイルの名前を入力してください。

アプリケーションフィルターログのクリア

クリア をクリックします。全ての情報が削除されます。

8.4.3. パケットフィルターのログ

パケットに対して **ヘッダのみ** または **パケット全体** のロギングモードが指定されている場合、コンピューターにインストールされている全てのネットワークインターフェースを經由して送受信されたそれらパケットに関する情報がパケットフィルターログに保存されます。パケットに対してロギングの **無効** モードが設定されている場合、情報は保存されません。





項目	説明
時間	パケットが処理された日時
方向	パケットの送信者 <ul style="list-style-type: none">← - パケットはネットワークからコンピューターへ送信されました→ - パケットはコンピューターからネットワークへ送信されました← - ネットワークからコンピューターへ送信されたパケットはブロックされました→ - コンピューターからネットワークへ送信されたパケットはブロックされました
ルール名	適用されたルールの名前
インターフェース	パケットの送受信に使用されたネットワークインターフェース
パケットデータ	パケットのデータ量。保存されるデータの量は、ルールの ロギングモード設定 によって決まります。

このページ上で、ログをファイルに保存またはクリアすることができます。

パケットフィルターログの保存

保存 をクリックし、ログの保存先となるファイルの名前を入力してください。

パケットフィルターログのクリア

クリア をクリックします。全ての情報が削除されます。



9. 自動更新

Doctor Web のアンチウイルスソリューションは、コンピュータ脅威の検出に **Dr.Webウイルスデータベース** を使用します。それらのデータベースには、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署名が含まれています。しかし、現在のコンピュータ脅威はその進化と亜種登場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ます。感染のリスクを減らすため、**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** は、新しいウイルスを検出し、その拡散を防ぐために必要な情報を受け取ります。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。

9.1. Updater の起動

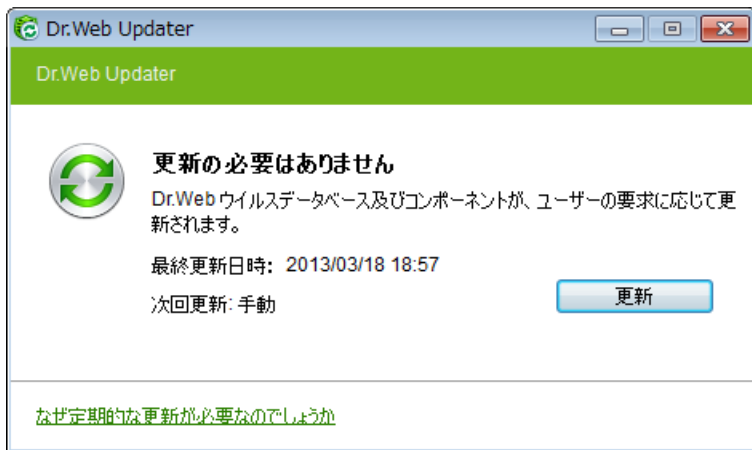
Updater は次のいずれかの方法で起動することができます。

- **Dr.Web Anti-virus** 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** メニュー内で **Updater** を選択

Updater が起動すると **Dr.Webウイルスデータベース** 及び **Dr.Web Anti-virus** 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。必要に応じ、更新プロセスを開始することが可能です。パラメータは **Dr.Web Anti-virus 一般設定** の **Updater** ページ上で設定することができます。



Dr.Web Updater 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の場合は%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 **Updater** は **キーファイル** (ライセンスまたはデモ)が登録されているかどうかの確認を行います。キーファイルが見つからない場合、ユーザー登録手続きの過程でインターネット上からキーファイルを取得するよう提案します。

キーファイルが見つからない場合は **Doctor Web** サーバー上でその有効性を確認します (ファイルが不法に配布されたものであると発覚した場合など、信用性に問題がある場合そのファイルはブロックされることがあります)。不正使用が原因でキーファイルがブロックされた場合、**Updater** は該当する警告を表示し、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、**Dr.Web Anti-virus** を購入したディーラーまでお問い合わせください。

キーファイルが正常に確認された後、**Updater** はお使いの **Dr.Web Anti-virus** 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



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** の新しいバージョンがリリースされた際にはそれらもダウンロード・インストールされます。

Dr.Web Anti-virus 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が必要な場合があります。その場合、**Updater** によって警告が表示されず。



Scanner、**SpIDer Guard**、**SpIDer Mail** 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ります。

Updater がコマンドラインモードで起動された場合、コマンドラインパラメータ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

追加のコマンドラインパラメータ(オプションパラメータ)は、実行ファイルを開くことで起動可能なプログラムのパラメータを設定するために使用されます。**Scanner**、**Console Scanner** および **Dr.Web Updater** で使用可能です。設定ファイルでは使用できないパラメータ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より高い優先順位を持ちます。

オプションパラメータは / 記号で始まり、他のコマンドラインパラメータ同様スペースによって分けられます。

Scanner 及び Console Scanner 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。**(Scanner のみ)**

/AR - アーカイブをスキャンします。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スキャンします。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> - アーカイブ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、Scannerはアーカイブの解凍もスキャンも行いません**(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、Scannerはアーカイブの解凍もスキャンも行いません**(無制限、KB)**。

/ART:<サイズ> - 圧縮率チェックが最初に行なわれるアーカイブ内にあるファイルの最小サイズ**(無制限、KB)**。



/ARX:<サイズ> - スキャンの対象となるアーカイブ内オブジェクトの最大サイズ(無制限, KB)。

/BI - **Dr.Webウイルスデータベース** に関する情報を表示します。デフォルトで有効になっています。

/DR - フォルダを再帰的にスキャンします(サブフォルダをスキャンします)。デフォルトで有効になっています。

/E:<エンジン> - 指定されたスロット数でスキャンを実行します。

/FAST - システムの **クイック** スキャンを実行します。(Scanner のみ)

/FL:<パス> - 指定したファイルに記載されているファイルのスキャンします。

/FM:<マスク> - 指定されたマスクに合致するファイルのスキャンします。デフォルトでは全てのファイルがスキャンされます。

/FR:<正規表現> - 指定された正規表現に合致するファイルのスキャンします。デフォルトでは全てのファイルがスキャンされます。

/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。(Scanner のみ)

/H 又は **/?** - 簡単なヘルプを表示します。(Console Scanner のみ)

/HA - 未知の脅威を検出するための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> - ライセンスキーファイルの指定。Scanner実行ファイルのある **Dr.Web** インストールフォルダ以外の場所にキーファイルが保存されている場合、このパラメータを指定する必要があります(デフォルトでは C:\Program Files\Dr.Web\ フォルダの drweb32.key 又はその他適切なファイルが使用されます)。

/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スキャンを実行します。Scanner によるルートキットスキャンも行われません。(Scanner のみ)

/LN - ショールINK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 – メールファイルをスキャンします。デフォルトで有効になっています。

/MC:<上限> – 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 – 修復された又は削除されたファイル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] – スキャン時におけるシステムリソースの使用とスキャンプロセスのプライオリティを制限します (無制限、%)。

/NOREBOOT – スキャン終了後にシステムの再起動またはシャットダウンを行いません。(Scanner のみ)

/NT – NTFS ストリームをスキャンします。デフォルトで有効になっています。

/OK – スキャンされた全てのオブジェクトの一覧を表示し、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> – 現在のスキャンタスクのプライオリティ:

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> – 指定されたファイルにスキャンのログを追加します。デフォルトではログは作成されません。

/RP:<file.log> – 指定されたファイルにスキャンのログを上書きします。デフォルトではログは作成されません。

/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。(Console Scanner のみ)



/RPCD – 動的RPC IDを使用します。(**Console Scanner** のみ)

/RPCE – 動的RPCエンドポイントを使用します。(**Console Scanner** のみ)

/RPCE:<名前> – 指定されたRPCエンドポイントを使用します。(**Console Scanner** のみ)

/RPCH:<名前> – IPアドレスで指定したホスト名を使用します。(**Console Scanner** 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ipc、np、tcpです。(**Console Scanner** のみ)

/QL – 全てのディスク上の隔離されたファイルを一覧にします。(**Console Scanner** のみ)

/QL:<論理ドライブ名> – 指定されたドライブ (文字) 上の隔離されたファイルを一覧にします。(**Console Scanner** のみ)

/QR[:[d][:p]] – 保存されている期間が<p> (数字)日を超えた、<d>(文字)ドライブ上の隔離ファイルを削除します。<d>を指定しなかった場合、全てのドライブ上の該当するファイルを削除します。<p> を指定しなかった場合、その古さに関係なく全ての隔離ファイルを削除します (<p> を0と見なします)。(**Console Scanner** のみ)

/QNA – ファイル名を二重引用符で囲みます。

/QUIT – 検出された脅威が駆除されたかどうかに関係なく、スキャンの完了後に **Dr.Web Scanner** を終了します。(**Scanner** のみ)

/REP – シンボリックリンク先をスキャンします。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。

/SILENTMODE – バックグラウンドスキャンを実行します。脅威が検出されると **Dr.Web Scanner** ウィンドウが開き、それら脅威の一覧が表示されます。脅威が検出されなかった場合はウィンドウは表示されません。(**Scanner** のみ)



/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 - ログを画面に表示します。デフォルトで有効になっています。(**Console Scanner** のみ)

/SPS - スキャンの進捗を画面に表示します。デフォルトで有効になっています。(**Console Scanner** のみ)

/SST - オブジェクトのスキャン時間を表示します。デフォルトで無効になっています。

/TB - ハードドライブのマスターブートレコード (MBR) を含むブートセクタをスキャンします。

/TM - Windowsシステムコントロールエリアを含むメモリ内のプロセスをスキャンします。

/TS - Autorunフォルダ内のオブジェクト、システムiniファイル、Windowsレジストリを含む、autorunオブジェクトをスキャンします。

/TR - システム復元ポイントをスキャンします。

/W:<秒> - 最大スキャン時間 (無制限、秒)。

/WCL - drwebwcl互換出力 (**Console Scanner** 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 **Console Scanner** のみで、デフォルトで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 – 疑わしいファイルに対するアクション (R、DQIR可)

指定されたオプションを無効 / 有効にする修飾子を持つことのできるパラメータがあります。

/AC- オプションは無効です。

/AC、/AC+ オプションは有効です。

これらの修飾子は、オプション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内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記載されているパスをスキャン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、無制限になります。

Console Scanner でのコマンドラインパラメータ使用例です。

[< 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スキャンし、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



Scanner 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 Updater コマンドラインパラメータ

共通オプション:

パラメータ	説明
<code>-h [--help]</code>	このメッセージを表示
<code>-v [--verbosity] arg</code>	ログの詳細レベル。次のうち1つを設定: error、info、debug
<code>-d [--data-dir] arg</code>	レポートと設定のあるディレクトリ
<code>--log-dir arg</code>	ログファイル保存ディレクトリ
<code>--log-file arg</code> (= <code>dwupdater.log</code>)	ログファイル名
<code>-r [--repo-dir] arg</code>	レポートディレクトリ(デフォルトでは <code><data_dir>/repo</code>)
<code>-t [--trace]</code>	traceを有効にする
<code>-c [--command] arg</code> (= <code>update</code>)	実行するコマンド: <code>getversions</code> 、 <code>getcomponents</code> 、 <code>getrevisions</code> 、 <code>init</code> 、 <code>update</code> 、 <code>uninstall</code> 、 <code>exec</code> 、 <code>keyupdate</code>
<code>-z [--zone] arg</code>	設定ファイルで指定されたゾーン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
<code>-s [--version] arg</code>	バージョン
<code>-p [--product] arg</code>	製品名



パラメータ	説明
-a [--path] arg	製品ディレクトリパス。このディレクトリが、製品に含まれる全てのコンポーネントの、デフォルトでのディレクトリになります。 Dr.Web Updater は、このディレクトリ内でキーファイルを検索します。
-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	プロキシサーバーのユーザー名
-k [--password] arg	プロキシサーバーのパスワード
-g [--proxy] arg	更新用 プロキシサーバー <アドレス>:<ポート>
-e [--exclude] arg	インストールの際に除外されるコンポーネントの名前

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、その製品のみが更新されます。指定しなかった場合は、全ての製品が更新されます。コンポーネントが指定された場合、それらのコンポーネントのみが更新されます。
-n [--component] arg	指定されたバージョンへ更新するコンポーネント <名前>, <バージョン>
-x [--selfrestart] arg (=yes)	Dr.Web Updater の更新後に再起動。デフォルトでyesに設定されています。noに設定した場合、再起動を要求する通知が表示されます。
--geo-update	更新前にupdate.drweb.comからIPアドレスのリストを取得
--type arg (=normal)	以下のうち1つ： <ul style="list-style-type: none">• reset-all – 全てのコンポーネントをリビジョンにリセット• reset-failed – 失敗したコンポーネントをリビジョンにリセット• 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の、又は指定したリビジョンに更新



パラメータ	説明
	<ul style="list-style-type: none">• update-revision – 最新のレジヨが存在する場合、全てのコンポーネントを現在のレジヨから最新に更新• normal – 全てのコンポーネントを更新
-g [--proxy] arg	更新用 プロキシサーバー <アドレス>:<ポート>
-u [--user] arg	プロキシサーバーのユーザー名
-k [--password] arg	プロキシサーバーのパスワード
--param arg	スクリプトへの追加パラメータ<名前>:<値>
-l [--progress-to-console]	ダウンロード及びスクリプト実行に関する情報をコンソールに表示

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	指定された場合、その機能をスクリプトで実行
-p [--param] arg	スクリプトへの追加パラメータ<名前>:<値>
-l [--progress-to-console]	スクリプト実行に関する情報をコンソールに表示

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
-p [--product] arg	製品に含まれるコンポーネントのリストを取得するために製品を指定。製品が指定されていない場合、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]	コマンド実行に関する情報をコンソールに表示
--param arg	スクリプトへの追加パラメータ <名前>: <値>
-e [--add-to- exclude]	削除するコンポーネント。このコンポーネントの更新は行われません。

keyupdate コマンドパラメータ

パラメータ	説明
-m [--md5] arg	以前のキーファイルのMD5ハッシュ値
-o [--output] arg	新しいキーを保存する出力ファイル名
-b [--backup]	古いキーファイルが存在する場合はそれをバックアップする



パラメータ	説明
-g [--proxy] arg	更新用 プロキシサーバー <アドレス>:<ポート>
-u [--user] arg	プロキシサーバーのユーザー名
-k [--password] arg	プロキシサーバーのパスワード
-l [--progress-to-console]	ダウンロードに関する情報をコンソールに表示

download コマンドパラメータ

パラメータ	説明
--zones arg	ゾーンの記述 ファイル
--key-dir arg	キーファイルが保存されているディレクトリ
-l [--progress-to-console]	コマンド実行に関する情報をコンソールに表示
-g [--proxy] arg	更新用 プロキシサーバー <アドレス>:<ポート>
-u [--user] arg	プロキシサーバーのユーザー名
-k [--password] arg	プロキシサーバーのパスワード
-s [--version] arg	バージョン
-p [--product] arg	製品名

付録 B. コンピューター脅威と駆除手法

コンピューターテクノロジーや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 び散られるようになってい ます。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続けていることから、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、リムーバブルメディアを經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。その他にはハッカーによって操作されるツールがあり、それらは最も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。

本章では、最も一般的かつ広範囲に拡散しているマルウェアのタイプ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

この種類の悪意のあるプログラムは、他のプログラム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は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）を感染させ、その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機能を持ったウイルスをメモリ常驻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進化していません。

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、その活動を偽るような動作を実行することで、感染したオブジェクト内における自身の存在を隠します。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、変更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(多くの場合アセンブラ、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悪意のあるプログラムより先広がり拡散されるようになってきています。ウイルス同様、自身を複製しそれらを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、電子メールの添付ファイル経由で)、ネットワーク内にある他のコンピューターに自身のコピーを配信します。ユーザー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する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は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(シボルコード)を持っています。シボ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えば場合はアンチウイルスプログラムのみが対処可能です。

ワームはその拡散速度によって、例えば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損なう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削除、機密情報を送信など）を実行したり、犯罪者が許可無しにコンピュータにアクセス（例えば第三者のコンピュータ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に類似しており、また、それ自体がウイルスのコンポーネントとなることも可能です。ただしほとんどのトロイの木馬は、ユーザー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拡散されます（ファイル交換サーバー、リモートストレージ、メール添付ファイルなどを介して）。

ルートキット

自身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、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も、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も拡散することが可能であり、基本的には、クラッカーがアクセス権限を得たシステム上にインストールするユーザーのセッションになります。

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。ユーザーモードで動作するユーザー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キット（KMR）です。UMRはユーザーモードドライバ機能を妨害し、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、ファイアウォール又はコンピュータ保護システムのその他のコンポーネントにおける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。ハッキングにも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、犯罪組織、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ィンドウを閲覧した際に、密かにシステム上にロードされ、ユーザーの許可なしに自身をインストールします。スパイウェアが存在することによって現れる一般的な副次的な症状は、不安定なブラウザの動作、およびシステムパフォーマンスの低下です。

アドウェア

アドウェアは通常、ユーザー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信されて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動作します。

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ム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。その目的はユーザーを脅えさ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、ユーザーのデータまたは機密情報を危険にさらすため、悪意があるものと見なされます。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キングアナライザーは、状況によっては脅威と化す可能性はありますが、通常は悪意のあるものと見なされません。

その他のプログラムの中には、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。

- **フラ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取得を繰り返し試す攻撃方法です。
- **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、攻撃対象とな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、大量のIPアドレスから同時に攻撃を行います。
- **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。パケットスニッフィ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。パケットスニッフィ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。
- **スプーフイング** - 接続を詐称して第三者になりすますことにより、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フォームを使って、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。被害者はこのメッセージによって、犯罪者の作成した偽サイトを訪れ、パスワードやPINコード、その他の個人情報を入力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

コンピュータ脅威を駆除する方法には様々なものがあります。**Doctor Web** 製品はコンピュータ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て、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合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 (オブジェクトの構造および動作を感染前の状態に戻す) します。悪意のあるプログラムの全てが修復可能なわけではありませんが、**Doctor Web** 製品は、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に **Doctor Web** の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また、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又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、ファイルが動作でき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・攻撃の対象となるオブジェクトの種類・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と、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す。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

攻撃の対象となる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のプログラム
- OS2 – OS/2 プログラム
- Unix – 様々なUNIX系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

意図された感染対象ではないシステムのプログラムであっても感染させることの出



来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のファイルに感染します)

開発言語

C、C++、Pascal、Basicなど的高级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
- HLL0 – 感染対象プログラムのコードを上書きするウイルス
- 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せん。

- VBS – Visual Basic Script
- JS – Java Script
- Wscript – Visual Basic Script 及び/ 又は 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 – 様々な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機能を持つトロイの木馬 (Remote Administration Tool – リモート管理ユーティリティ)
- 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密かにダウンロードするトロイの木馬
- MulDrop – そのボディに含まれる様々なウイルスを密かにダウンロードするトロイの木馬
- Proxy – 感染したコンピュータを通じてインターネット上で第三者が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アドレス (スタートページ) を許可なくすり替えるトロイの木馬
- Click – ユーザー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 – キーボード入力を記録し、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停止、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の既知の脆弱性を悪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 (Flooder Denial of Service) 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 (登録された有料の番号、または有料のリンクにモデムをリダイレクトする)
- 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既知の脆弱性を悪用し、悪意のあるコードを埋め込んだ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 – 特徴を持たない単純なウイルスに対し、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、または変更が加えられたウイルス。いずれの場合においても、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内でwebフォームに必要事項を入力し、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、公式 **Doctor Web** サイト <http://company.drweb.co.jp/contacts/japan/> をご覧ください。

