



Dr.WEB
Agent for Windows

ユーザーマニュアル



© Doctor Web, 2022無断複写・転載を禁じます。

本マニュアルは特定のDr.Webソフトウェアの使用に関する情報を提供し、参照目的で用いられることを意図したものです。Dr.Webソフトウェアに特定の機能や技術仕様が備わっているかどうかを評価する際の根拠となるものではなく、また、Dr.Webソフトウェアが特定の要件や技術的タスク/パラメータ、サードパーティのマニュアルに合致するかどうかを判断するために使用するものではありません。

本マニュアルの著作権はDoctor Webが有します。本マニュアルのどの部分も、いかなる形式、方法、および購入者が個人で利用する以外のいかなる目的においても、無断で複写、出版、転載することを禁じます。

商標

Dr.Web、SpIDer Mail、SpIDer Guard、CureIt!、CureNet!、AV-Desk、KATANA、Dr.WEBロゴは、ロシアおよびその他の国におけるDoctor Webの商標および登録商標です。本マニュアルに記載されているその他の商標、登録商標、および会社名の著作権はそれぞれの所有者が有します。

免責事項

Doctor Webおよびそのリセラー、ディストリビューターは、過失または損失、このマニュアルによって直接、または間接的に引き起こされた、または引き起こされたと考えられるいかなる損害、および本マニュアルに含まれる情報の利用、または利用できないことに対する責任を負わないものとします。

Dr.Web Agent for Windows

バージョン**13.0**

ユーザーマニュアル

2022/07/28

Doctor Webロシア本社

2-12A, 3rd str. Yamskogo polya, Moscow, Russia, 125124

ウェブサイト: <https://www.drweb.com/>

電話番号: +7 (495) 789-45-87

支社および海外オフィスについては、Doctor Web公式サイトをご覧ください。

Doctor Web

Doctor Web は、悪意のあるソフトウェアやスパムからの効果的な保護を提供するDr.Web情報セキュリティソリューションの開発および販売を行っています。

Doctor Web のカスタマーは、世界中のホームユーザーから政府機関、小規模な会社、大企業にまで広がっています。

Dr.Web アンチウイルスソリューションは、マルウェア検出における継続的な卓越性と国際情報セキュリティ基準への遵守によって1992年よりその名を広く知られています。

Dr.Web ソリューションに与えられたロシア連邦による認定や数々の賞、そして世界中に広がるそのユーザーが、製品に対する並外れた信頼の何よりの証です。

Dr.Web 製品に対するサポートについて、すべてのカスタマーに対して厚く御礼申し上げます。



目次

1. はじめに	7
1.1. 表記規則	7
2. 製品について	9
2.1. 保護コンポーネントと管理モジュール	9
2.2. 検出手法	10
2.3. システム要件	14
2.4. アンチウイルスの動作検査	15
3. Dr.Web のインストール、アンインストール、変更	17
3.1. フルインストーラからのインストール	17
3.2. パーソナルインストールパッケージからのインストール	22
3.3. コンポーネントを設定する	29
3.4. 製品の削除と再インストール	31
4. プログラムメニュー	33
5. Security Center	36
6. 通知フィード	38
7. プログラム設定	40
7.1. 全般設定	40
7.1.1. プログラム設定のパスワード保護	41
7.1.2. インターフェースのカラーテーマを選択する	42
7.1.3. プログラム言語を選択する	44
7.1.4. Dr.Webの動作ログ	44
7.1.5. 隔離設定	47
7.1.6. 統計レコードの自動削除	48
7.2. 通知設定	49
7.3. Self-Protection	52
7.4. ファイルスキャンのオプション	54
7.5. Server	56
7.6. Server通知	61
8. ファイルとネットワーク	63
8.1. ファイルシステムのリアルタイム保護	64
8.2. Webトラフィックをチェックする	70
8.3. メールスキャン	73



8.3.1. メールスキャンを設定する	75
8.3.2. Anti-Spamの設定	79
8.4. Firewall	83
8.4.1. Firewallの設定	84
8.5. コンピューターのスキャン	101
8.5.1. スキャンの開始とスキャンモード	102
8.5.2. 検出された脅威を駆除する	104
8.5.3. 追加設定	106
8.6. Dr.Web for Microsoft Outlook	107
8.6.1. ウイルススキャン	108
8.6.2. スпам検査	110
8.6.3. イベントのロギング	112
8.6.4. 統計	113
9. 予防的保護 (Preventive Protection)	115
9.1. ランサムウェア保護 (Ransomware Protection)	116
9.2. 動作解析 (Behavior Analysis)	121
9.3. エクスプロイト防止 (Exploit Prevention)	128
10. デバイス	131
10.1. バスとデバイスクラスのブロック	134
10.2. 許可するデバイス	139
11. Office Control	142
11.1. インターネットリソースへのアクセス	145
11.2. コンピューターとインターネットの使用時間制限	150
11.3. ファイルとフォルダへのアクセス	151
12. 隔離マネージャー	153
13. 除外	155
13.1. Webサイト	156
13.2. ファイルとフォルダ	158
13.3. アプリケーション	160
13.4. Anti-Spam	164
14. コンポーネント動作に関する統計	166
15. Server通知	173
16. テクニカルサポート	176
16.1. 問題解決サポートオプション	176
16.2. プログラムについて	179



17. 付録A.追加のコマンドラインパラメータ	180
17.1. ScannerとConsole Scannerのパラメータ	180
17.2. インストールパッケージのパラメータ	185
17.3. リターンコード	187
18. 付録B.コンピューター脅威と駆除手法	189
18.1. コンピューターの脅威のタイプ	189
18.2. 脅威に対するアクション	192
19. 付録C.ウイルスの名称	193
20. 付録D.主な用語と概念	197



1. はじめに


このマニュアルには、Dr.Web Agent for Windows製品のインストール方法、使用方法、ウイルスの脅威によくある問題の解決方法に関する推奨事項が記載されています。マニュアルには主に、Dr.Webコンポーネントの標準動作モード(デフォルト設定)が記載されています。

付録には、Dr.Webの設定に関する上級ユーザー向けの一般的な情報と追加のパラメータについて記載されています。

1.1. 表記規則

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	説明
	重要な注釈、またはエラーを引き起こす可能性のある状況に関する警告
アンチウイルスネットワーク	新しい用語、または強調したい用語
<IP-address>	プレースホルダー
保存	ボタン、ウィンドウ、メニューアイテム、および他のプログラムインターフェース要素の名称
CTRL	キーボードのキー名称
C:\Windows\ \\	ファイルやフォルダの名前、コード例
付録 A	本書の他のページや外部 Web ページへのリンク

略語

以下の略語は本マニュアル内では次の意味でのみ使われます。

- Dr.Web - Dr.Web Agent for Windows
- FTP - File Transfer Protocol(ファイル転送プロトコル)
- HTTP - Hypertext Transfer Protocol(ハイパーテキスト転送プロトコル)
- IMAP - Internet Message Access Protocol(インターネットメッセージアクセスプロトコル)
- IMAPS - Internet Message Access Protocol Secure(インターネットメッセージアクセスプロトコルセキュア)
- MTU - Maximum Transmission Unit(最大転送ユニット)



- NNTP - Network News Transfer Protocol(ネットワークニュース転送プロトコル)
- OS - Operating system(オペレーティングシステム)
- POP3 - Post Office Protocol Version 3(ポストオフィスプロトコルバージョン3)
- POP3S - Post Office Protocol Version 3 Secure(ポストオフィスプロトコルバージョン3セキュア)
- SIP - Session Initiation Protocol(セッション確立プロトコル)
- SMTPS - Simple Mail Transfer Protocol Secure(シンプル メールトランスファープロトコル)
- SSL - Secure Sockets Layer(セキュアソケットレイヤー)
- TCP - Transmission Control Protocol(トランスミッションコントロールプロトコル)
- TLS - Transport Layer Security(トランスポートレイヤーセキュリティ)
- UAC - User Account Control(ユーザーアカウント制御)
- URL - Uniform Resource Locator(ユニフォームリソースロケータ)



2. 製品について

Dr.Web Agent for Windows は、あらゆる種類のウイルス、ルートキット、トロイの木馬、スパイウェア、アドウェア、ハッキングツール、および外部からの侵入を試みるその他様々な悪意のあるオブジェクトからWindows搭載コンピューターのRAM、ハードディスク、リムーバブルメディアを保護します。

Dr.Web Agent for Windows は、異なる機能を担う複数のモジュールで構成されています。スキャンエンジンとウイルスデータベースは、すべてのコンポーネントとプラットフォームに共通です。

製品のコンポーネントは常時更新されます。新しい脅威のシグネチャが、ウイルスデータベース、Webサイトカテゴリのデータベース、およびメールスパムのフィルタリングルールに定期的追加されていきます。定期的な更新により、ユーザーのデバイスやアプリケーション、データに対する最新の保護を提供します。さらに、スキャンエンジンに搭載されたヒューリスティック解析が、未知の悪意のあるソフトウェアからの保護を確実なものにします。

Dr.Web Agent for Windows は様々な望ましくないプログラム(アドウェア、ダイアラー、ジョークプログラム、リスクウェア、ハッキングツール)を検出し、お使いのコンピューター上から削除します。Dr.Webはデフォルトのコンポーネントの機能を使用して、望ましくないプログラムを検出し、それらを含むファイルに対してアクションを実行します。

サポート ページの [プログラムについて](#) セクションで、製品のバージョン、最新更新日、Dr.Web AgentのID番号に関する情報を確認できます。

2.1. 保護コンポーネントと管理モジュール

Dr.Web Agent for Windows には、以下の保護コンポーネントと管理モジュールが含まれています。

コンポーネント／モジュール	説明
SpIDer Guard	メモリに常駐するコンポーネント。SpIDer Guardはプロセスとファイルの起動と作成をスキャンし、悪意のあるアクティビティを検出します。
SpIDer Gate	HTTPトラフィックをスキャンするコンポーネント。デフォルトでは、SpIDer Gateインターネットモニターは受信したHTTPトラフィックを自動的にスキャンし、ウイルスや他の悪意のあるプログラムを含むオブジェクトの転送をブロックします。信頼性が低く悪意のあるWebサイトのURLフィルタリングもデフォルトで有効になっています。SpIDer Gateは、HTTP、XMPP (Jabber)、TLS (SSL) プロトコルでトラフィックをスキャンします。
SpIDer Mail	コンピューター上のメールクライアントとメールサーバー間のPOP3/SMTP/IMAP4/NNTPプロトコル (IMAP4はIMAPv4rev1の略です) を介したデータのやり取りを監視し、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。また、SpIDer Mail は Dr.Web Anti-Spam を使用してメールのスパムスキャンを行います。
Dr.Web Firewall	お使いのコンピューターを不正アクセスから保護し、重要なデータがネットワークを通じて漏洩するのを防ぐパーソナルファイアーウォールです。



コンポーネント／モジュール	説明
Office Control	Webサイト、ファイル、フォルダへのアクセス制限や、ユーザーがさまざまなWindowsアカウントでコンピューターとインターネットを使用する際のカスタム時間制限を設定できるコンポーネント。
Behavior Analysis	重要なシステムオブジェクトへのアプリケーションアクセスを制御し、実行中のアプリケーションのエクスプロイト防止と整合性を提供するコンポーネント。
Exploit Prevention	アプリケーションの脆弱性を利用する悪意のあるオブジェクトをブロックするコンポーネント。
Ransomware Protection	ランサムウェアに対する保護を提供するコンポーネント。
Scanner	オンデマンド起動し、コンピューターにウイルスや他の悪意のあるソフトウェアがないかをスキャンするグラフィカルインターフェースを備えたスキャナー。
コンソールDr.Web Scanner	Dr.Web Scannerのコマンドラインバージョン。
Dr.Web for Microsoft Outlook	Microsoft Outlookのメールボックスで脅威とスパムをスキャンするプラグイン。
SpIDer Agent	アンチウイルス製品の設定および管理モジュール。

2.2. 検出手法

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

シグネチャ解析

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署名と比較するシグネチャ解析で始まります。シグネチャはウイルスを特定する為に必要かつ十分な、連続するバイトの有限なシーケンスです。シグネチャ辞書のサイズを抑える為、Dr.Web アンチウイルスソリューションはシグネチャのシーケンス全体ではなくチェックサムを使用します。チェックサムはシグネチャを特定し、ウイルス検出および駆除の正確さを維持します。Dr.Web ウイルスデータベースは、いくつか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全体を検出できるよう設計されています。

Origins Tracing

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、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)のような悪質な脅威から保護されます。新種・亜種ウイルスの検出を可能にするほか、Origins Tracing はDr.Web ヒューリスティックアナライザによる誤検出を劇的に減らします。Origins Tracing アルゴリズムを使用して検出されたオブジェクトの名前には、.Origin拡張子が付きます。



実行のエミュレーション

プログラムコード実行のエミュレーション手法は、署名のチェックサム解析が効果的ではない場合、または著しく困難な場合（サンプルから信頼できる署名を抽出できないため）に、ポリモーフィック型ウイルスや暗号化ウイルスを検出するために使用されます。プロセッサおよびランタイム環境のプログラミングモデルである *エミュレータ* が、解析するサンプルコードの実行をエミュレートします。エミュレータは保護されたメモリスペース（*エミュレーションバッファ*）内で動作し、解析するプログラムの実行は命令ごとに順次行われます。ただし、これらの命令がCPUによって実際に実行されることはありません。ポリモーフィック型ウイルスに感染したファイルがエミュレータによって処理されると、ウイルスのボディが復号化され、署名のチェックサム解析によって簡単に識別されるようになります。

ヒューリスティック解析

ヒューリスティックアナライザの検出手法は、ウイルスコードに典型的な、または非常にまれな特徴（属性）に関する特定の情報に基づいています（*ヒューリスティック*）。各属性は、その深刻度および信頼度を定義する重み係数を持っています。属性が悪意のあるコードであることを示している場合には重み係数がプラスになり、コンピューター脅威の特徴を示していない場合はマイナスになります。ヒューリスティックアナライザ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。それらの合計が一定の閾値を超えている場合、ヒューリスティックアナライザによって、オブジェクトは未知のウイルスに感染している可能性があるとして判定されます。

ヒューリスティックアナライザはファイル解凍の柔軟なアルゴリズムである FLY-CODE テクノロジーも使用します。このテクノロジーは、Dr.Web にとって既知のパッカーのみでなく、これまでに発見されていない未知のパッカーによって圧縮されたファイル内に悪意のあるオブジェクトが存在する可能性をヒューリスティックに検出します。Dr.Web アンチウイルスソリューションはパックされたオブジェクトのスキャン中に構造エントロピー解析も使用します。このテクノロジーはコードの配置を解析することで脅威を検出します。そのため、1つの検体から、同じポリモーフィックパッカーによってパックされた他の多くの脅威を検出することが可能になります。

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もまたタイプ I またはタイプ II のエラーを侵す可能性があります（ウイルスを見逃す、または誤検知）。そのため、ヒューリスティックアナライザによって検出されたオブジェクトは「疑わしい」オブジェクトとして定義されます。

動作解析 (Behavior Analysis)

動作解析では、システム内のすべてのプロセスアクションのシーケンスを分析します。悪意のある動作が検出されると、そのプログラムのアクションはブロックされます。

Dr.Web Process Heuristic

動作解析テクノロジーである Dr.Web Process Heuristic により、従来のシグネチャベースの解析やヒューリスティック解析をくぐり抜ける危険な新しい悪意のあるプログラムからシステムを保護します。

Dr.Web Process Heuristic は動作中のプログラムの動作をリアルタイムで解析します。悪意のある動作に関する情報を使用して、プログラムが危険であるかどうかを判断し、脅威を駆除するために必要な処置を行います。Dr.Web Process Heuristic を使用して検出されたオブジェクトは、名前に DPH プレフィックスが付けられます。

このデータ保護テクノロジーによって、未知のマルウェアによる損害を最小限に抑えることができます。また、システムリソースの消費は非常に少なくなっています。

Dr.Web Process Heuristic はシステムを改変しようとするあらゆる試みをモニタリングします。



- ネットワーク経由でアクセス可能な共有ファイルやフォルダを含む、ユーザーのファイルを改変する悪意のあるプロセスを検出（暗号化ランサムウェアの動作など）
- 他のアプリケーションのプロセス内にマルウェアが自身のコードを挿入することを防ぐ
- マルウェアによる改変からクリティカルなシステム領域を保護
- 悪意のある、疑わしい、または信頼できないスクリプトやプロセスの実行を検出し、停止させる
- マルウェアによるブートセクターの改変を防ぎ、悪意のあるコードがコンピューター上で実行されないようにする
- Windowsレジストリ内の変更をブロックし、セーフモードが無効にならないようにする
- マルウェアによる起動許可の変更を防ぐ
- ユーザーの許可なしに、新たなまたは未知のドライバがダウンロードされることを防ぐ
- マルウェアや、アンチアンチウイルスなどのアプリケーションがWindowsレジストリ内に登録されることを防ぎ、自動実行されないようにする
- 仮想デバイスドライバに関する情報を含んだレジストリセクションをロックし、新しい仮想デバイスが作成されないようにする
- マルウェアによるシステムルーチン（スケジュールによるバックアップなど）の妨害を防ぐ

Dr.Web Process Dumper

Dr.Web Process Dumperは、バックされた脅威の包括的な分析により、新しいパッカーによって隠される前にDr.Webウイルスデータベースに追加された、「新しい」とされる悪意のあるプログラムの検出を大幅に向上させます。また、このタイプの分析では、ウイルスデータベースに新しいエントリを追加し続ける必要がなくなります。Dr.Webウイルスデータベースを小さく維持することで、システム要件を絶えず増やす必要がありません。更新サイズは従来どおり小さく、一方で検出ならびに修復の品質は高レベルに保たれます。Dr.Web Process Dumperを使用して検出されたオブジェクトは、名前に `DPD` プレフィックスが付けられます。

Dr.Web ShellGuard

Dr.Web ShellGuardはお使いのデバイスをエクスプロイトから保護します。*エクスプロイト*はソフトウェアの脆弱性を悪用する悪意のあるオブジェクトです。これらの脆弱性は、標的となるアプリケーションやOSのコントロールを獲得するために悪用されます。Dr.Web ShellGuardを使用して検出されたオブジェクトは、名前に `DPH:Trojan.Exploit` プレフィックスが付けられます。

Dr.Web ShellGuardは、ほぼすべてのWindows搭載コンピューター上にインストールされる一般的なアプリケーションを保護します。

- 一般的なWebブラウザ（Internet Explorer、Mozilla Firefox、Google Chromeなど）
- MS Officeアプリケーション
- システムアプリケーション
- Java、Flash、PDFを使用するアプリケーション
- メディアプレイヤー（ソフトウェア）

Injection Protection（インジェクション保護）

*インジェクション*は、デバイス上で実行されているプロセスに悪意のあるコードを挿入（インジェクト）する攻撃手法です。Dr.Webは、システム内のすべてのプロセスの動作を常時監視し、悪意があると判断されたコードが挿入されるのを防ぎます。Injection Protectionを使用して検出されたオブジェクトは、名前に `DPH:Trojan.Inject` プレフィックスが付けられます。



Dr.Webはプロセスを実行したアプリケーションをスキャンし、次の情報についてチェックします。

- アプリケーションが新しいものであるかどうか
- どのようにシステム内に入ったのか
- アプリケーションのある場所
- アプリケーションの名前
- アプリケーションが、信頼できるアプリケーションのリストに含まれているかどうか
- 信頼できる認証センターの有効なデジタル署名を持っているかどうか

Dr.Webは、実行されたプロセスの状態を監視します（プロセス空間にリモートスレッドが作成されたかどうか、アクティブなプロセスに外部コードが埋め込まれたかどうかをチェックします）。

Dr.Webアンチウイルスプログラムは、アプリケーションが行う変更を制御し、システムや特権を持つプロセスが変更されるのを防ぎます。そのほか、悪意のあるコードが一般的なブラウザのメモリを変更できないようにします（インターネットで買い物をしたり、ネットバンキングで送金したりする場合など）。

Ransomware Protection (ランサムウェア保護)

Ransomware Protection は、ユーザーのファイルを暗号化ウイルスから保護するBehavior Analysisの手法の1つです。暗号化ランサムウェアは、コンピューターに侵入するとユーザーのデータへのアクセスをブロックし、それらを復元するために金銭を要求します。Ransomware Protectionを使用して検出されたオブジェクトは、名前にDPH:Trojan.Encoder プレフィックスが付けられます。

このコンポーネントは、ファイルの検索や読み取り、変更を試みるプロセスに特に注意を払い、疑わしいプロセスの動作を分析します。

アプリケーションについて、次の情報もチェックされます。

- アプリケーションが新しいものであるかどうか
- どのようにシステム内に入ったのか
- アプリケーションのある場所
- アプリケーションの名前
- アプリケーションが信頼できるものであるかどうか
- 信頼できる認証センターの有効なデジタル署名を持っているかどうか

また、ファイルの変更方法もチェックされます。悪意のある動作が検出された場合は、そのプログラムのアクションをブロックし、ファイルを変更しようとする試みを阻止します。

マシンラーニング

マシンラーニングは、ウイルスデータベースに含まれていない悪意のあるオブジェクトを検出し、駆除するために使用されます。この手法の利点は、悪意のあるコードを実行することなくその機能のみによって判断し、検出することができるということです。

脅威の検出は、特定の機能による悪意のあるオブジェクトの分類に基づいています。サポートベクターマシン (SVM) は、分類に使用されるマシンラーニングテクノロジーの基礎となり、スクリプト言語で書かれたコード片をデータベースに追加します。検出されたオブジェクトは、悪質なコードの特徴を持っているかどうかに基づいて分析さ



れます。マシンラーニングテクノロジーは、これらの機能やウイルスデータベースを自動的に更新するプロセスを作成します。

マシンラーニング手法は、脅威を検出するためのコード実行を必要とせず、シグネチャ解析に使用されるウイルスデータベースの定期的な更新なしに分類子の動的マシンラーニングを実行できるため、オペレーティングシステムのリソースを大幅に節約します。

2.3. システム要件

Dr.Webは、以下の要件を満たすシステムで使用することができます。

パラメータ	要件
CPU	i686互換プロセッサ
オペレーティングシステム	32ビットプラットフォームの場合： <ul style="list-style-type: none">• Windows XP Service Pack 2以降• Windows Vista Service Pack 2以降• Windows 7 Service Pack 1以降• Windows 8• Windows 8.1• Windows 10 21H2以前• Windows Server 2003 Service Pack 1• Windows Server 2008 Service Pack 2以降 64ビットプラットフォームの場合： <ul style="list-style-type: none">• Windows Vista Service Pack 2以降• Windows 7 Service Pack 1以降• Windows 8• Windows 8.1• Windows 10 21H2以前• Windows 11• Windows Server 2008 Service Pack 2以降• Windows Server 2008 R2 Service Pack 1以降• Windows Server 2012• Windows Server 2012 R2• Windows Server 2016• Windows Server 2019• Windows Server 2022
RAM空き容量	512 MB以上
画面解像度	1024×768以上推奨
クラウドおよび仮想化環境のサポート	プログラムは以下の環境での動作が保証されています。 <ul style="list-style-type: none">• VMware



パラメータ	要件
	<ul style="list-style-type: none">• Hyper-V• Xen• KVM
その他	<p>Dr.WebウイルスデータベースおよびDr.Webコンポーネントを更新するために、集中管理サーバーへの接続、またはモバイルモードでのインターネットへの接続が必要です。</p> <p>Dr.Web for Microsoft Outlookプラグインには、Microsoft Officeパッケージの次のMicrosoft Outlookクライアントのうちいずれか一つが必要です。</p> <ul style="list-style-type: none">• Outlook 2000• Outlook 2002• Outlook 2003• Outlook 2007• Outlook 2010 Service Pack 2• Outlook 2013• Outlook 2016• Outlook 2019• Outlook 2021



MicrosoftによるSHA-1ハッシュアルゴリズムのサポートは終了しています。Windows Vista、Windows 7、Windows Server 2008 または Windows Server 2008 R2に Dr.Web Agent for Windows をインストールする前に、お使いのオペレーティングシステムがSHA-256ハッシュアルゴリズムをサポートしていることを確認してください。詳細については [Doctor Web公式サイト](#) をご覧ください。



バージョン13.0のDr.Web Agent for Windowsと互換性があるのはバージョン12.0のDr.Webプラグインのみです。

2.4. アンチウイルスの動作検査

EICARファイルを使用してアンチウイルスの動作を検査する

EICAR(European Institute for Computer Anti-Virus Research) の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、動作確認のために標準的な 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検出に対する動作を、コンピューターを危険にさらすことなくテストするために特別に開発されたものです。test.comプログラム自体は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できています。この「ウイルス」を検出すると Dr.Web は EICAR Test File (Not a Virus!) という表示を出します。他のアンチウイルスツールも同様の方法でユーザーに警告します。



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、コンソールに EICAR-STANDARD-ANTIVIRUS-TEST-FILE! というメッセージを表示します。

test.com のファイルは、次の文字列のみを含んでいます。

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

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



EICAR テストファイル はシステムに対して実際に脅威を与えるものではないため、SpIDer Guard が 最適モード で動作している場合、テストファイルを実行しても動作は中断されることなく、またテストファイルは悪意あるファイルとして判定されません。ただし、そのようなファイルのコピーまたは作成を行った場合は、SpIDer Guard によって検知され、デフォルトで 隔離 に移されます。



3. Dr.Web のインストール、アンインストール、変更

Dr.Web Agent for Windows のインストール前に [システム要件](#) をお読みください。また、以下の操作を行うことが推奨されます。

- お使いのコンピューターで使用されているOSバージョンの、Microsoftからリリースされた重要な更新プログラムを全てインストールします ([Windows](#) および [Windows Server](#) の更新に関する詳細情報をご確認ください)。お使いのOSのサポートが終了している場合は、新しいものにアップグレードしてください。
- システムユーティリティでファイルシステムを検査し、問題が発見された場合にはそれを取り除いてください。
- Dr.Webコンポーネントとの互換性問題を避けるため、コンピューターから他のアンチウイルスソフトウェアを削除します。
- Dr.Web Firewallをインストールする場合は、他のファイアーウォールを全てコンピューターから削除します。
- Windows Server 2016以降では、グループポリシーを使用して手動でWindows Defenderを無効にします。
- 動作中のアプリケーションを全て閉じてください。



Dr.Web をインストールするには管理者権限が必要です。

以下のいずれかの方法でDr.Webをインストール、アンインストールまたは変更することができます。

1. リモート - ネットワーク経由で集中管理サーバーからこのプロセスは、アンチウイルスネットワークの管理者によって実行されます。ユーザーの操作は必要ありません。
2. ローカルで - ユーザーのコンピューター上で直接。Dr.Webは、[フルインストーラ](#) または [パーソナルインストールパッケージ](#) を使用してインストールすることができます。

Dr.Webアンチウイルスソフトウェアのインストールには次の2つのモードがあります。

- コマンドラインモード
- ウィザードモード

3.1. フルインストーラからのインストール

フルインストーラ `drweb-13.0.0-xxxxxxx-esuite-agent-full-windows.exe` はDr.Web Agentとアンチウイルスパッケージのインストールを同時に実行します。サーバー接続パラメータおよびサーバーでの端末認証のパラメータはインストーラには付属していません。

ウィザードモードでのインストール

ウィザードがコンピューターへのファイルのコピーを開始する前であれば、途中で以下の操作を実行することができます。

- **戻る** をクリックすると前のステップに戻ります。
- **次へ** をクリックすると次のステップへ進みます。
- **終了** をクリックするとインストールを中止します。

Dr.Webをインストールする

1. 管理者から受け取ったインストールパッケージを実行します。Dr.Webインストールウィザードのウィンドウが表示されます。



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る場合、インストールウィザードはインストールを開始する前にその削除を試みます。失敗した場合には、そのアンチウイルスソフトウェアを手動で削除する必要があります。



図 1. インストールウィザード

2. **集中管理サーバー** フィールドで、Dr.Webのインストール元となるサーバーのネットワークアドレスを指定し、**パブリックキーまたは証明書** フィールドでコンピューター上にあるキーファイル(drwcsd.pub)または証明書(.pem)へのフルパスを指定します。
アクティブなサーバーを検索する場合や、検索パラメータを指定する場合は、**検索** ボタンをクリックします。
次へ をクリックします。
3. インストールウィザードが、インストールの準備ができたことを通知します。



図 2. インストール準備完了

インストール をクリックすると、デフォルトのパラメータでインストールを実行できます。

インストールするコンポーネントの選択やインストールパスの指定、その他の設定を行うには [インストールパラメータ](#) リンク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。

4. 前のステップで [インストール](#) を選択した場合、[手順8](#) 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 ウィンドウが開きます。



図 3. インストールパラメータ

コンポーネント タブには、Dr.Webコンポーネントが一覧表示されます。

インストールするコンポーネントにチェックを入れてください。デフォルトでは Dr.Web Firewall 以外の全てのコンポーネントが選択されています。

5. インストールパス タブで、**Dr.Web Agent for Windows** のインストールフォルダを指定できます。デフォルトのインストール先は、システムディスク上の Program Files フォルダ内にあるDr.Webフォルダになっています。変更するには [参照](#) をクリックし、フォルダを指定してください。
6. アドバンスオプション タブで、追加の設定を行うことができます。



図 4. インストールパラメータのアドバンスオプション

次のオプションがあります。

- システムの、インストールされたソフトウェア一覧に**Dr.Web Agent**を登録する - Windows標準ツールを使用した Dr.Web の [アンインストール](#) および [コンポーネントの設定](#) を可能にします。
- **ユーザーエミュレーションの禁止** - Dr.Webウィンドウ内で機能するマウスやキーボードをエミュレートするスクリプトの実行を含む、サードパーティ製ソフトウェアによるDr.Web設定の変更をすべて防ぎます (Dr.Web設定を変更するスクリプト、Dr.Webの動作を変更することを目的としたその他の操作など)。
- 集中管理サーバーでの手動認証を有効にするには、**認証** チェックボックスにチェックを入れ、ワークステーションの認証パラメータを指定します。
 - **端末 ID** - サーバー上のワークステーションの識別子
 - **パスワード** - サーバーにアクセスするためのパスワード

この場合、ワークステーションはサーバーにアクセスするために管理者の手動承認を必要としません。

圧縮 および **暗号化** ドロップダウンリストから、サーバーと Dr.Web との間のトラフィックに必要なモードを選択してください。

設定を保存するには **OK** をクリックします。次に **インストール** をクリックしてください。

7. Dr.Webのインストールが始まります。ユーザーの操作は必要ありません。
8. インストールの完了後、コンピューターを再起動するよう指示されます。すぐに**再起動** をクリックしてください。



コマンドラインからのインストール

コマンドラインを使用してDr.Webのインストールを開始するには、インストールファイルがあるフォルダに移動し、必要なコマンドラインオプションを使用して実行ファイル名 (drweb-13.0.0-xxxxxxx-esuite-agent-full-windows.exe) を入力してください。

コマンドラインパラメータの一覧は [付録 A](#) をご覧ください。

3.2. パーソナルインストールパッケージからのインストール

パーソナルインストールパッケージから製品をインストールする場合、インストールはネットワーク経由で実行されません。

パーソナルインストールパッケージにはDr.Web Agentインストーラと、接続するDr.Webサーバーおよびサーバー上での端末認証のための一連のパラメータが含まれています。

ウィザードモードでのインストール

ウィザードがコンピューターへのファイルのコピーを開始する前であれば、途中で以下の操作を実行することができます。

- **戻る** をクリックすると前のステップに戻ります。
- **次へ** をクリックすると次のステップへ進みます。
- **終了** をクリックするとインストールを中止します。

Dr.Webをインストールする

1. プロバイダ管理者から受け取ったインストールパッケージ
drweb_ess_windows_<Station_name>.exe を実行します。Dr.Webインストールウィザードのウィンドウが表示されます。



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る場合、インストールウィザードはインストールを開始する前にその削除を試みます。失敗した場合には、そのアンチウイルスソフトウェアを手動で削除する必要があります。



図 5. インストールウィザード

2. **次へ** をクリックします。
3. 次のステップで、コンピューター上にあるパブリックキー (`drwcsd.pub`) または証明書 (`.pem`) へのフルパスを指定します。

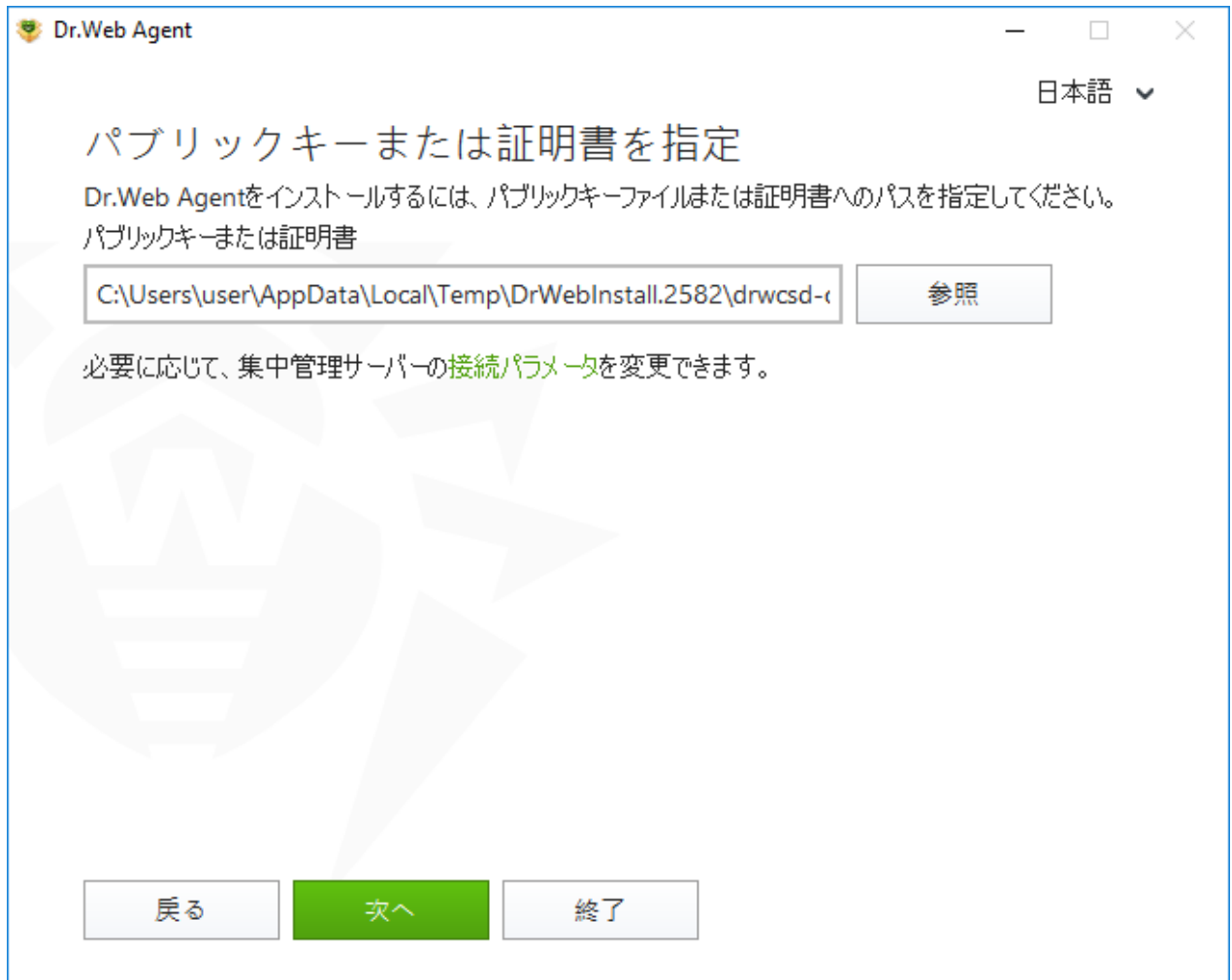


図 6.パブリックキーまたは証明書を指定

- 必要に応じて、集中管理サーバーへの接続パラメータを変更することができます。その場合は、該当するリンクをクリックしてください。接続パラメータ ウィンドウが開きます。パーソナルインストールパッケージからインストールする場合、必要なすべての接続パラメータはあらかじめ指定されています。



パラメータの変更はアンチウイルスネットワーク管理者の承諾を得た上で行うようにしてください。

Dr.Web Agent

日本語

接続パラメータ

集中管理サーバーへの接続パラメータに関してはシステム管理者までお問い合わせください。
集中管理サーバー

検索

Serverでの手動による承認

端末 ID

パスワード

圧縮

暗号化

OK キャンセル

図 7. 集中管理サーバーへの接続パラメータ



集中管理サーバーへの接続パラメータの詳細についてはアンチウイルスネットワーク管理者までお問い合わせください。

集中管理サーバー フィールドで、Dr.Webの接続先となるサーバーのネットワークアドレスを指定することができます。デフォルトでは、このフィールドにはインストールファイルが作成されたサーバーのパラメータが自動的に入力されます。アクティブなサーバを検索する場合や検索パラメータを指定する場合は **検索** ボタンをクリックします。

サーバ上で設定済みのID等のパラメータを使用して認証するには、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。その後、次の認証パラメータを指定してください:

- **端末 ID** - サーバー上のワークステーションの識別子
- **パスワード** - サーバーにアクセスするためのパスワード

この場合、ワークステーションはサーバーにアクセスするために管理者の手動承認を必要としません。



Dr.Web Control Center 内で作成されたインストールファイルを使用してDr.Webをインストールする際に、手動認証オプションが選択されている場合、**端末 ID** および **パスワード** のフィールドは自動的に入力されます。



圧縮 および 暗号化 ドロップダウンリストから、サーバーと Dr.Web との間のトラフィックに必要なモードを選択してください。

設定を保存するには **OK** をクリックします。次に **次へ** をクリックしてください。



接続の確立に失敗した場合は、表示されたリンクからネットワークパラメータを確認するか、該当するボタンをクリックしてサーバーに再度接続してください。

5. 接続が確立された後、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** をクリックしてください。



図 8. インストール準備完了

インストールするコンポーネントの選択やインストールパスの指定、その他の設定を行うには **インストールパラメータ** リンク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。

6. 前のステップで **インストール** を選択した場合、**手順9** 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** ウィンドウが開きます。



図 9. インストールパラメータ

コンポーネント タブには、Dr.Webコンポーネントが一覧表示されます。

インストールするコンポーネントにチェックを入れてください。デフォルトでは Dr.Web Firewall 以外の全てのコンポーネントが選択されています。

7. インストールパス タブで、**Dr.Web Agent for Windows** のインストールフォルダを指定できます。デフォルトのインストール先は、システムディスク上の Program Files フォルダ内にあるDr.Webフォルダになっています。変更するには [参照](#) をクリックし、フォルダを指定してください。
8. アドバンスオプション タブで、追加のインストール設定を行うことができます。



図 10. インストールパラメータのアドバンスオプション

必要に応じ、システムの、インストールされたソフトウェア一覧に**Dr.Web Agent**を登録する オプションを有効にしてください。このオプションによって、Windows標準ツールを使用した Dr.Web の [アンインストール](#) や [コンポーネントの設定](#) も可能になります。

ユーザーエミュレーションの禁止 オプションは、Dr.Webウインドウ内で機能するマウスやキーボードをエミュレートするスクリプトの実行を含む、サードパーティ製ソフトウェアによるDr.Web設定の変更をすべて防ぎます (Dr.Web設定を変更するスクリプト、Dr.Webの動作を変更することを目的としたその他の操作など)。

設定を保存するには **OK** をクリックします。次に **インストール** をクリックしてください。

9. Dr.Webのインストールが始まります。ユーザーの操作は必要ありません。

10. インストールの完了後、コンピューターを再起動するよう指示されます。すぐに**再起動** をクリックしてください。

コマンドラインからのインストール

コマンドラインを使用してDr.Webのインストールを開始するには、インストールファイルがあるフォルダに移動し、必要なコマンドラインオプションを使用して実行ファイル名 (drweb_ess_windows_<Station_name>.exe)を入力してください。

コマンドラインパラメータの一覧は [付録 A](#) をご覧ください。



Dr.Webインストール中のBFEサービスエラー

いくつかのDr.Webコンポーネントでは、BFE(ベースフィルタエンジンサービス)を実行する必要があります。このサービスが不在または破損している場合、Dr.Webはインストールできません。BFEサービスが損傷しているまたは存在しない場合は、コンピューター上のセキュリティ脅威が存在している可能性があります。

Dr.Webのインストールがエラーで終了した場合は、次の操作を行います。

1. Doctor WebのユーティリティCureNet!を使用してワークステーションのシステムをスキャンします。ユーティリティのデモバージョン(修復機能なしの診断のみ)については、<https://download.drweb.com/curenet/>をご確認ください。
CureNet!フルバージョンの利用規約と価格については <https://estore.drweb.com/utilities/> をご覧ください。
 2. BFEサービスを復元します。これには、Windowsファイアウォールリカバリ [ユーティリティ](#) (Windows 7以降用)を使用できます。Windows Serverオペレーティングシステムでは、BFEサービスを手動で有効にするか、または再起動します。BFEサービスを再起動できない場合、またはサービスの一覧に表示されない場合は、[Microsoftテクニカルサポート](#) までお問い合わせください。
 3. Dr.Webインストールウィザードを実行し、上記の手順に従ってインストールを実行します。
- 問題が引き続き発生する場合は、Doctor Webテクニカルサポートまでご連絡ください。

3.3. コンポーネントを設定する



コンポーネント設定の変更を行うことができるのは、アンチウイルスネットワーク管理者によって該当するオプションが有効化されている場合のみです。

コンポーネントの設定は、アンインストール／変更ウィザードで行うことができます。アンインストール／変更ウィザードは、次の2つの方法のいずれかで開くことができます。

- インストールファイルがある場合は、それを実行します。
- Windowsコントロールパネルから：
 1. Windowsコントロールパネルで[プログラム]をクリックし、
 2. インストールされているプログラムのリストで、**Dr.Web Agent** を選択します。
 3. **変更** をクリックします。

コンポーネントを削除または追加するには

1. アンインストール／変更ウィザードで **コンポーネントの変更** をクリックします。



図11. アンインストール／変更ウィザード

2. 開いたウィンドウ内で、追加したいコンポーネントのチェックボックスにチェックを入れ、削除したいコンポーネントのチェックを外してください。
3. **適用** をクリックします。

アンインストール／変更ウィザードウィンドウでは、以下のオプションを設定することもできます。

- **プログラムの復元** - コンピューター上のアンチウイルス保護を復元する必要がある場合。この機能は、Dr.Webコンポーネントの一部が壊れている場合に適用されます。
- **プログラムの削除** - インストールされたすべてのコンポーネントを **削除** します。



3.4. 製品の削除と再インストール



Dr.Web のローカルでのアンインストールを行うには、そのオプションが集中管理サーバー上で管理者によって許可されている必要があります。

Dr.Web をアンインストールした後は、コンピューターはウイルスやその他のマルウェアから保護されなくなります。

Dr.WebをWindowsコントロールパネルから削除する



この方法はインストール中にシステムの、インストールされたソフトウェア一覧に **Dr.Web Agent** を登録する オプションを有効にした場合のみ使用することができます。

Dr.Web をバックグラウンドモードでインストールした場合、Windows 標準ツールを使用したアンインストールは `-regagent` パラメータが指定されている場合のみ使用することができます。

インストールファイルがある場合は、手順 1~3 をスキップできます。インストールファイルを実行し、[手順 4](#) に進んでください。

Dr.Web Agent for Windows を削除するには Windows の削除コンポーネントを実行します。

1. リストで、プログラム名の行を選択します。
2. **Delete** をクリックします。
3. **保存するパラメータ** ウィンドウで、システムから削除しないコンポーネントのチェックボックスにチェックを入れます。保存されたオブジェクトや設定は、再度インストールする際に使用できます。デフォルトでは、全てのオプション（**隔離**、**Dr.Web Agent の設定**、**ファイルのコピー**）が選択されています。**次へ** をクリックします。
4. Dr.Web の削除を確認するには、次のウィンドウで **削除** をクリックします。
5. コンピューターが再起動されると変更が適用されます。**後で再起動する** をクリックすることで再起動を遅らせることができます。Dr.Web コンポーネントの削除または変更の手順を直ちに完了させるには **すぐに再起動** をクリックしてください。

コマンドラインを使用して削除する

コマンドラインを使用して Dr.Web をアンインストールするには、実行ファイル名 (`win-es-agent-setup.exe`) を入力し、必要なパラメータを指定してください。



`win-es-agent-setup.exe` ファイルは `C:\ProgramData\Doctor Web\Setup\` フォルダ内にあります。

例えば Dr.Web をアンインストールし、完了後にシステムを再起動させるには、次のコマンドを使用します。

```
win-es-agent-setup.exe /instMode remove /reboot yes
```





Dr.Webを再インストールする

1. アンチウイルスネットワーク管理者から最新版インストールパッケージを入手します。
2. [前述の方法](#)で、プログラムをアンインストールします。
3. コンピューターを再起動してください。
4. インストールパッケージを使用して、[プログラムを再インストール](#)します。インストール中に、キーファイルへのパスを指定してください。
5. コンピューターを再起動してください。




4. プログラムメニュー

Dr.Webがインストールされると、Windowsの通知領域に  アイコンが追加されます。このアイコンには、現在の [アプリケーションの状態](#) が反映されます。Dr.Webメニューを開くには、 をクリックしてください。アプリケーションが動作していない場合は、スタートメニューでアプリケーショングループ **Dr.Web** を展開し、**Security Center** を選択します。



アンチウイルスネットワーク管理者が集中管理サーバー上で該当する設定を有効にしている場合、Dr.Webアイコンは通知領域に表示されません。

Dr.Webメニュー  では、セキュリティステータスを表示したり、メインの管理ツールとプログラム設定にアクセスしたりできます。



コンポーネント設定の変更や無効化は、Dr.Webが接続されている集中管理サーバーの管理者によってブロックされている場合には行うことができません。

設定 ウィンドウ内で **Dr.Webの設定をパスワードで保護する** が有効になっている場合、コンポーネントの設定にアクセスする際にもパスワードの入力が必要になります。

製品設定のパスワードが分からなくなってしまった場合はシステム管理者までご連絡ください。



図 12. プログラムメニュー



メニュー項目

パソコンのセキュリティステータス - すべてのプログラムコンポーネントが有効になっている場合は、コンピューターは保護されています。ステータスが表示されます。1つ以上のコンポーネントが無効になっている場合、ステータスは「コンピューターは保護されていません」に変わります。

Security Center - メイン設定、保護コンポーネント設定 (Office Control 設定を含む)、除外設定にアクセスするためのウィンドウを開きます。

更新 (モバイルモード動作時のみ) - ウイルスデータベースの状態と最終更新日に関する情報。プログラムコンポーネントとウイルスデータベースの更新を開始します。

サポート - サポートのウィンドウを開きます。



制限時間 (インターネットまたはコンピューターの使用時間制限のオプションが Office Control コンポーネントで有効になっている場合) - 時間間隔が指定されている場合、インターネットまたはコンピューターの使用制限または中断時間に関する簡単な情報が表示されます。

Server通知 (新しいメッセージがあり、対応するオプションがサーバー上で有効になっている場合) - [サーバーメッセージ](#) のウィンドウを開きます。

Self-Protection (Self-Protectionが無効の場合) - スイッチを使用してSelf-Protectionを有効にすることができます。

サーバー接続ステータス - 端末がサーバーに接続できない場合にのみ表示されます。端末が正常に接続されている場合、ステータスは表示されません。


5つのステータスのうちいずれか1つが表示されます:

アイコン	ステータス
	<ul style="list-style-type: none">● 端末はサーバーでの承認を待っています● モバイルモード● 集中管理サーバーに接続しています
	<ul style="list-style-type: none">● サーバーに接続されていません● 接続エラー




通知フィード  - [通知フィード](#) のウィンドウを開きます。

アプリケーションの状態

Dr.Web アイコンは現在のアプリケーションの状態を表しています。

Dr.Webアイコン	説明
	必要なコンポーネントは全て動作中で、コンピューターは保護されています。また、集中管理サーバーとの接続は確立されています。



Dr.Webアイコン	説明
	Self-Protectionまたは重要なコンポーネントが無効になっているか、ウイルスデータベースが最新ではありません。これにより、アンチウイルスとコンピューターのセキュリティが低下します。またはサーバーとの接続が切れています。サーバーが接続を拒否したか、そのリソースへのアクセスを拒否した可能性があります。Self-Protectionまたは無効なコンポーネントを有効にしてください。またはサーバーとの接続が確立するまでお待ちください。接続が確立されない場合は、アンチウイルスネットワーク管理者まで連絡してください。
	コンポーネントはOSのスタートアッププロセスが完了した後に起動します。コンポーネントが起動するまでしばらくお待ちください。または、主要なDr.Webコンポーネントの起動時にエラーが発生しました。コンピューターがウイルスに感染する危険性があります。アイコンが変化しない場合はアンチウイルスネットワーク管理者まで連絡してください。
	Scannerが現在動作中です。



5. Security Center

Security Center ウィンドウから、全てのコンポーネント、ツール、統計情報、プログラム設定にアクセスできます。

Security Center ウィンドウを開くには

1. Dr.Web [メニュー](#)  を開きます。
2. **Security Center** を選択します。

スタートメニューから **Security Center** ウィンドウを開くには

1. スタートメニュー で、**Dr.Web** グループを開きます。
2. **Security Center** をクリックします。






図13. Security Center ウィンドウ

設定のグループ



メインウィンドウから設定の次のグループにアクセスできます。

- **Security Center**、メインタブ - 全てのセキュリティコンポーネントとツールにアクセスできます：
 - [ファイルとネットワーク](#)
 - [Preventive Protection](#)
 - [デバイス](#)
 - [Office Control](#)



- [隔離マネージャー](#)
- [除外](#)
- [統計](#) タブ - メインプログラムの動作イベントに関する統計情報を提供します。
- プログラムウィンドウ上部にある  ボタン - [プログラムの設定](#) にアクセスできます。
- プログラムウィンドウ上部にある  ボタン - [テクニカルサポートのレポート](#) を生成し、製品バージョンやコンポーネントとウイルスデータベースの最終更新日に関する情報を確認できる [サポート](#) ウィンドウにアクセスできます。
- プログラムウィンドウ上部にある  ボタン - プログラム動作イベントに関する重要な通知を確認できる [通知](#) ウィンドウにアクセスできます。

管理モード

全ての設定グループにアクセスするには、プログラムウィンドウの下部にあるロック  をクリックしてDr.Webを[管理モード](#)に切り替えます。Dr.Webが管理モードになると、ロックが開かれます .

どちらのモードでも、[隔離マネージャー](#)にフルアクセスできます。また、全てのセキュリティコンポーネントを有効にして、管理モードに切り替えることなくScannerを開始することもできます。セキュリティコンポーネントを無効にするには、コンポーネント設定とプログラム設定にアクセスし、管理モードに切り替える必要があります。



コンポーネント設定の変更や無効化は、Dr.Webが接続されている集中管理サーバーの管理者によってブロックされている場合には行うことができません。

保護ステータス

プログラムウィンドウの一番上に、システム保護のステータスが表示されます。




- **コンピューターは保護されています。** 全てのコンポーネントが有効になり、正しく動作しています。Self-Protectionが有効で、ライセンスが有効です。緑色で表示されます。
- **コンピューターは保護されていません。** 少なくとも1つのコンポーネントが無効になっている場合に表示されます。赤色で表示されます。無効にされたコンポーネントタイルも赤で強調表示されます。



6. 通知フィード

このウィンドウには、プログラム操作イベントに関する重要な通知が表示されます。このウィンドウの通知は、一部のデスクトップ通知と重複します。

プログラムメニューから通知フィードにアクセスするには

1. Dr.Web [メニュー](#)  を開きます。
2.  ボタンをクリックします。 アイコンの上に、保存された通知の数が表示されます。
3. イベント通知のウィンドウが開きます。

Security Centerから通知フィードウィンドウにアクセスするには

1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. プログラムウィンドウ上部にある  をクリックします。
3. イベント通知のウィンドウが開きます。

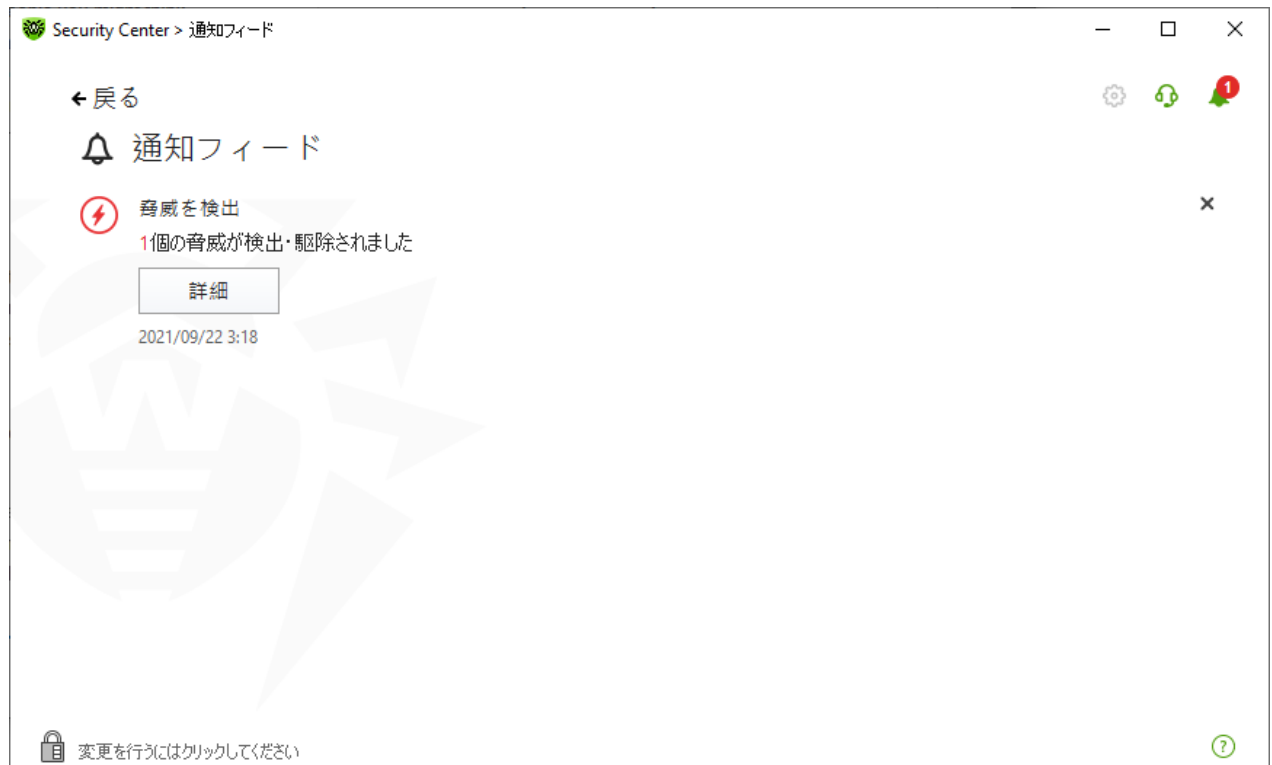


図 14. 通知フィードウィンドウ



通知保持期間

通知は2週間保存されます。問題が解決すると、通知は削除されます。

通知のタイプ

 重要な通知	
脅威	<ul style="list-style-type: none">脅威が検出されました。脅威を駆除するために再起動が必要です。ウイルスデータベースが古くなりました。
サーバーとの接続	<ul style="list-style-type: none">サーバーとの接続が禁止されています。サーバー接続エラー。
オブジェクトやデバイスへのアクセスがブロックされている旨の通知	<ul style="list-style-type: none">デバイスは設定によってブロックされています。
 主要な通知	
更新	<ul style="list-style-type: none">更新を完了するには、再起動が必要です。
 軽微な通知	
新しいバージョン	<ul style="list-style-type: none">新しいバージョンが入手可能です。
新しいメッセージ	<ul style="list-style-type: none">管理者が新しいメッセージを送信しました。





表示設定

フィード内の通知の表示設定は、デスクトップ通知の通知設定と重複しています。特定の通知がフィードに表示されないように表示設定を変更するには、**通知のパラメータ** ウィンドウの **デスクトップ** 列で該当するオプションのチェックを外します。[通知設定](#) セクションも参照してください。



7. プログラム設定

プログラム設定を開くには

1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. Dr.Webが [管理者モード](#) で動作していることを確認してください(プログラムウィンドウ下部にあるロックが開いています )。管理者モードではない場合は、ロックをクリックします 。
3. プログラムウィンドウ上部にある  をクリックします。
4. 設定ウィンドウが開きます。



設定の変更は、Dr.Webが接続されている集中管理サーバーの管理者によってこのオプションが有効にされている場合のみ行うことができます。

[全般設定](#) 内で **Dr.Web**の [設定をパスワードで保護する](#) が有効になっている場合、Dr.Webメイン設定にアクセスする際にパスワードを入力する必要があります。

このセクションでは以下の設定を行うことができます。





- [一般](#) - パスワードで設定を保護したり、言語やカラーテーマを選択したりすることができます。
- [通知](#) - ポップアップ通知の表示について設定することができます。
- [Self-Protection](#) - 追加のセキュリティパラメータを設定します。
- [ファイルスキャンのオプション](#) - Scannerのパラメータを設定します。
- [Server](#) - 集中管理サーバーへの接続パラメータを設定します。
- [Server通知](#) - サーバー通知を表示するためのパラメータを設定します。

7.1. 全般設定

全般設定には以下の機能があります。

- [プログラム設定のパスワード保護](#)
- [インターフェースのカラーテーマを選択する](#)
- [プログラム言語を選択する](#)
- [動作ログのロギング設定](#)
- [隔離設定](#)
- [統計レコードの自動削除設定](#)

全般設定にアクセスするには

1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. Dr.Webが [管理者モード](#) で動作していることを確認してください(プログラムウィンドウ下部にあるロックが開いています )。管理者モードではない場合は、ロックをクリックします 。
3. プログラムウィンドウ上部にある  をクリックします。



4. 製品のメイン設定ウィンドウが開きます。ウィンドウの左側にある **一般** を選択します。



図 15. 全般設定

7.1.1. プログラム設定のパスワード保護

パスワードを使用して、コンピューター上のDr.Web設定へのアクセスを制限することができます。Dr.Webの設定にアクセスするたびに、パスワードが必要になります。

パスワードを設定するには

1. 全般設定のウィンドウで、**スリット** スイッチを使用して **Dr.Webの設定をパスワードで保護する** オプションを有効にします。



図 16. 設定のパスワード保護

2. 開いたウィンドウで、パスワードを設定して確認します。
3. **OK** をクリックします。



製品設定のパスワードが分からなくなってしまった場合は、システム管理者までご連絡ください。

7.1.2. インターフェースのカラーテーマを選択する

必要に応じて、プログラムインターフェースのカラーテーマを切り替えることができます。インターフェースのカラーテーマ ドロップダウンリストから次のオプションのいずれかを選択してください。

- **ライト**: 明るい外観を使用します。
- **ダーク**: 暗い外観を使用します。
- **システム**: システムインターフェースの色を使用します。デフォルトではこのオプションが選択されています。



図 17. インターフェースのカラーテーマを選択する



ダークカラーテーマは、次のOSを搭載したコンピューターで使用できます : Windows 10(バージョン1909以降)、Windows 11、Windows Server 2019以降(バージョン1809以降)。それ以前のバージョンでは、インターフェースのカラーテーマ設定は非表示になっています。

インターフェースのダークカラーテーマが正しく機能するには、KB5011503以降のアップデートが必要です。



7.1.3. プログラム言語を選択する

必要に応じて、プログラムのインターフェース言語を切り替えることができます。言語リストは自動的に更新されます。したがって、現在Dr.Webのグラフィカルインターフェースで使用できる全てのローカリゼーション言語が含まれています。言語を切り替えるには、言語 グループのドロップダウンメニューから言語を選択します。



図18. プログラム言語を選択する

7.1.4. Dr.Webの動作ログ

1つまたは複数のDr.Webコンポーネントやサービスの詳細なロギングを有効にすることができます。

動作ログのロギング設定を変更するには

1. ログ セクションで 変更 をクリックします。



図 19. 全般設定、ログ

詳細なロギング設定のウィンドウが開きます：



図 20. 動作ログのロギング設定

2. 詳細なロギングを有効にするコンポーネントを選択します。デフォルトでは、すべてのDr.Webコンポーネントで標準モードでのロギングが有効になっています。ログには以下の情報が記録されます。



コンポーネント	情報
SpIDer Guard	<p>更新時刻、SpIDer Guardの起動時刻と停止時刻、ウイルスイベント、スキャンされたファイルのデータ、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、ファイルコンテナ)のコンテンツ。</p> <p>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、それらのオブジェクトを除外リストに追加することでコンピューターのパフォーマンスを向上させることができます。</p>
SpIDer Mail	<p>更新時間、メールアンチウイルスSpIDer Mailの起動時間と停止時間、ウイルスのイベント、接続のインターセプト設定、スキャンされたファイルのデータ、パッカー名、スキャンされたアーカイブのコンテンツ。</p> <p>メールの監視設定をテストする場合に、このモードの使用を推奨します。</p>
SpIDer Gate	<p>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。</p> <p>チェックされたオブジェクト、およびインターネットモニターの動作に関する詳細な情報を受け取る場合に、このモードの使用を推奨します。</p>
Scanner	<p>スキャンモジュールとウイルスデータベース情報の更新、Scanner の起動時間と停止時間、検出された脅威に関する情報、パッカー名、スキャンされたアーカイブのコンテンツ。</p>
Firewall	<p>サービスが受け取るリクエストに関する情報と決定、リクエストの理由を含む不明な接続に関する情報、エラーに関する情報。</p> <p>詳細なロギングを有効にすると、コンポーネントはネットワークパケットに関するデータを収集します (pcapログ)。</p>
Dr.Web Update	<p>更新されたDr.Webファイルのリストおよ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、Dr.Webコンポーネントの再起動に関する詳細。</p>
Dr.Web Service	<p>Dr.Webコンポーネント、Dr.Webコンポーネント設定の変更、コンポーネントの開始・停止、予防的保護イベント、集中管理サーバーへの接続に関する情報。</p>

メモリダンプの作成

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 オプションでは、複数のDr.Web コンポーネントの動作に関する有用な情報を保存することができます。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ちます。Doctor Web テクニカルサポートのスペシャリストから指示があった場合、またはスキャンや駆除エラーの発生時にこのオプションを有効にすることを推奨します。メモリダンプは%PROGRAMFILES%\Common Files\Doctor Web\Scanning Engine\ フォルダ内の .dmpファイルに保存されます。

詳細なログを有効にする



Dr.Web の動作に関する詳細なデータのロギングが有効になっている場合、最大限の情報が記録されます。そのため、ログファイルサイズの上限が無効になったり、システムおよび Dr.Web



の動作に影響が出る場合があります。このモードはコンポーネント動作のエラーの発生時またはアンチウイルスネットワーク管理者からの指示があった場合にのみ使用するようにしてください。

1. Dr.Web 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. 設定を保存するには **OK** をクリックします。



ロギング設定の変更は、Dr.Web が接続されている集中管理サーバー上で管理者によってブロックされている場合には行うことができません。

デフォルトでは、ログファイルのサイズ上限は10 MB(SpIDer Guard では100 MB)となっています。サイズが上限を超えた場合、ファイルのコンテンツは以下のように縮小されます。

- 今行ったスキャンのログファイルサイズが上限を超えていない場合、ファイルはそのまま保持されます。
- 今行ったスキャンのログファイルサイズが上限を超えた場合、現在のセッションのサイズに縮小されます。

7.1.5. 隔離設定

隔離内のオブジェクトの保存について設定することで(例: 保存期間を設定する、リムーバブルメディアに隔離フォルダを作成する)、ディスクの過剰な使用を防ぐことができます。

検出された脅威の保管設定を変更するには

1. 全般設定ウィンドウで、**アドバンス設定** リンクをクリックします。
2. **隔離** セクションで、 スイッチを使用して必要なオプションを有効または無効にします。

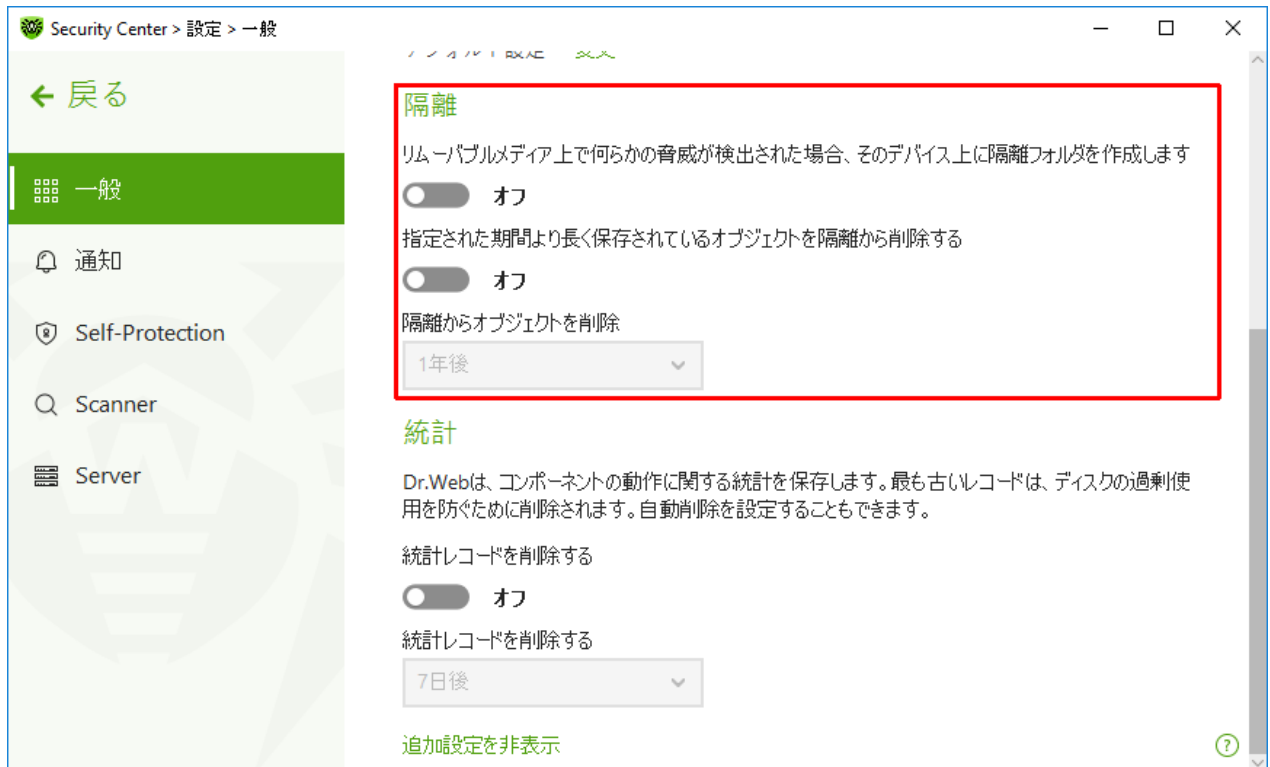


図21. 隔離設定

3. 隔離からオブジェクトを自動的に削除するには、ドロップダウンメニューで期間を選択します。保存期間が指定した期間を経過したオブジェクトは削除されます。

リムーバブルメディア上に隔離を作成する

リムーバブルメディア上で何らかの脅威が検出された場合、そのデバイス上に隔離フォルダを作成します。オプションを使用して、リムーバブルメディア上で検出された脅威について、そのリムーバブルメディア上に隔離フォルダを作成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、検出された脅威は暗号化されずに隔離フォルダへ移されます。リムーバブルメディア上に隔離フォルダが作成されるのは、それら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、リムーバブルメディア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。

このオプションを無効にすると、リムーバブルメディア上で検出された脅威はローカルディスク上の隔離フォルダに移動されます。

隔離からオブジェクトを自動削除する

ディスクの過剰な使用を防ぐには、隔離からのオブジェクトの自動削除を有効にします。

7.1.6. 統計レコードの自動削除

デフォルトでは、Dr.Webはディスクの過剰使用を防ぐために最適な数の **統計** レコードを保存します。また、指定した期間を超えて保存されている統計レコードの自動削除を有効にすることができます。



統計レコードの自動削除を有効／無効にするには

1. 全般設定ウィンドウで、アドバンス設定 リンクをクリックします。
2. 統計 セクションで、 スイッチを使用して統計レコードの自動削除を有効または無効にします。

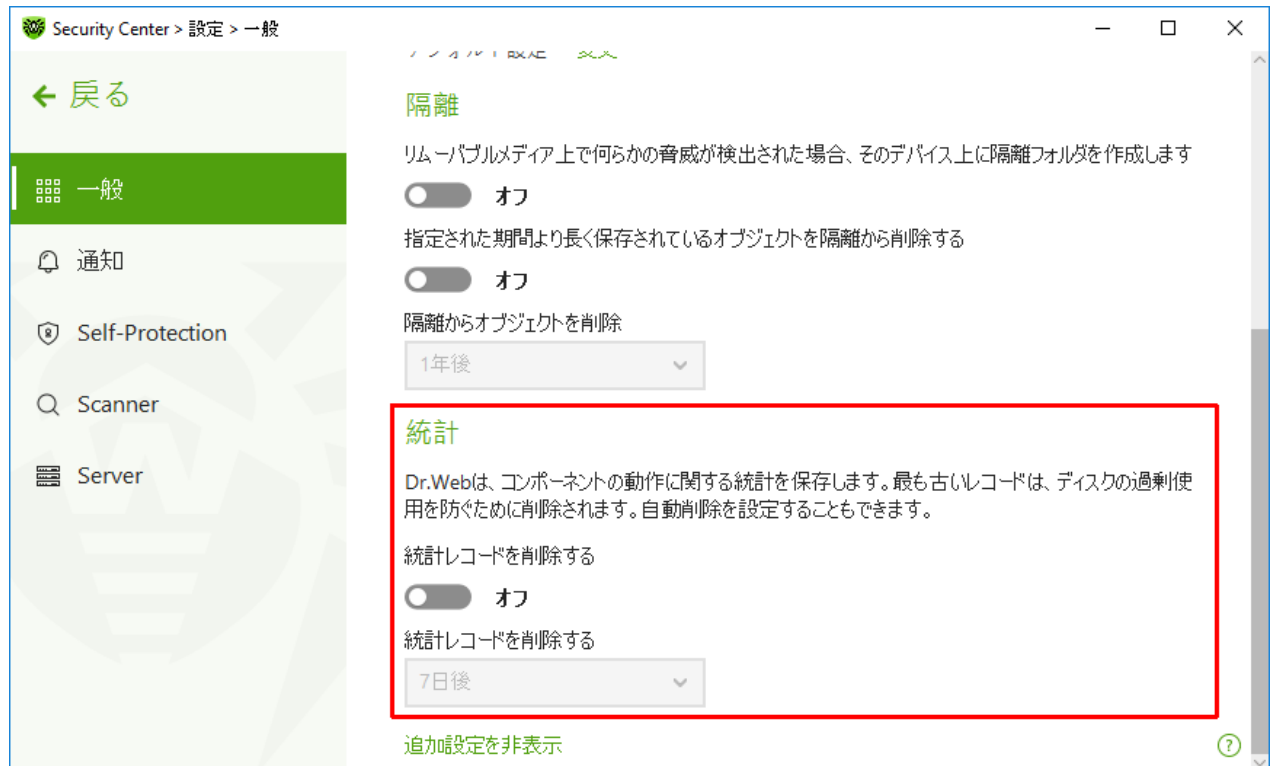


図22. 統計情報の設定

3. このオプションを有効にしたら、ドロップダウンメニューで期間を選択します。保存期間が指定した期間を経過したレコードは削除されます。

7.2. 通知設定





Dr.Web動作のクリティカルなイベントや重要なイベントに関する通知を受け取るためのパラメータを設定できます。

このセクションでは以下の設定を行うことができます。

• 通知パラメータの設定

必要に応じて、Dr.Web動作のクリティカルなイベントや重要なイベントに関する通知を受け取るためのパラメータを設定してください。

通知設定を開くには

1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. Dr.Webが [管理者モード](#) で動作していることを確認してください(プログラムウィンドウ下部にあるロックが開いています )。管理者モードではない場合は、ロックをクリックします 。
3. プログラムウィンドウ上部にある  をクリックします。



4. 製品のメイン設定ウィンドウが開きます。ウィンドウの左側にある **通知** を選択します。



図 23.通知設定

通知のパラメータを設定するには

1. **通知のパラメータ** をクリックします。
2. 受信する通知を選択します。ポップアップ通知を表示するには、必要な通知タイプの横にあるチェックボックスをオンにします。

通知を受信しない場合は、全てのチェックボックスをオフにします。

通知タイプ	説明
脅威が検出されました	SpIDer GuardとSpIDer Gateで検出された脅威についての通知。 この通知はデフォルトで有効になっています。
重要な通知	以下の重大な問題について通知： <ul style="list-style-type: none">• Firewall からの応答を待つ接続が検出されました。• お使いのログインとパスワードが、既に集中管理サーバーへの接続に使用されています。 この通知はデフォルトで有効になっています。
主要な通知	以下の問題についての重要な通知： <ul style="list-style-type: none">• コンピューターの利用可能時間が終了しました。• ウイルスデータベースが最新ではありません(モバイルモードで動作している場合)。• デバイスがブロックされました。



通知タイプ	説明
	<ul style="list-style-type: none">システム日時の変更がブロックされました。保護されたオブジェクトへのアクセスが、動作解析によってブロックされました。保護されたオブジェクトへのアクセスが、Exploit Preventionによってブロックされました。保護されたオブジェクトへのアクセスが、Ransomware Protection(ランサムウェア保護)によってブロックされました。プロセスの起動が管理者によってブロックされました。MSIパッケージのインストールが管理者によってブロックされました。スクリプトの起動が管理者によってブロックされました。プロセスによるオブジェクトの読み込みがブロックされました。プロセスによる実行可能ファイルの作成がブロックされました。プロセスによる実行可能ファイルの変更がブロックされました。 これらの通知はデフォルトで無効になっています。
軽微な通知	以下の問題についての軽微な通知： <ul style="list-style-type: none">URLが Office Control によってブロックされました。URL が SpIDer Gate によってブロックされました。インターネットでの作業時間が終了しました。保護されたオブジェクトへのアクセスが Office Control によってブロックされました。コンピューターのスキャンがアンチウイルスネットワーク管理者によって実行されています。コンピューターのスキャンがスケジュールに従って実行されています。スキャンが完了しました。更新が完了しました。更新エラーです。 これらの通知はデフォルトで無効になっています。

3. 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。

オプション	説明
通知をフルスクリーンモードで表示しない	コンピューター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)に通知を隠します。 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オフにしてください。
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	コンピューター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 Firewall の通知を別のデスクトップ上に表示させます。 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。



以下の内容に関する通知は上記いずれの分類にも含まれず、ユーザーに対して常に表示されます：

- 優先度の高い更新がインストールされ、再起動が必要です。
- 脅威の駆除を完了するためにコンピューターの再起動が必要です。
- 自動再起動
- プロセスがオブジェクトに変更を加える際の許可を求めるリクエスト。
- 集中管理サーバー管理者から送信されたメッセージ。
- サーバーとの接続に成功しました。
- 新しいキーボードが接続されました。

7.3. Self-Protection

アンチウイルスを標的とする悪意のあるプログラムによる不正な変更や誤った破損からDr.Web自体を保護するための設定を行うことができます。

このセクションでは以下の設定を行うことができます。

- [Self-Protectionを有効または無効にする](#)
- [システム日時に対する変更をブロックする](#)

Self-Protection設定を開くには





1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. Dr.Webが [管理者モード](#) で動作していることを確認してください(プログラムウィンドウ下部にあるロックが開いています )。管理者モードではない場合は、ロックをクリックします 。
3. プログラムウィンドウ上部にある  をクリックします。
4. 製品のメイン設定ウィンドウが開きます。ウィンドウの左側にある **Self-Protection** を選択します。



図 24. Dr.Web Self-Protection/パラメータ

Self-Protectionの設定

Self-Protectionを有効にする(推奨) オプションでは、Dr.Web のファイルやプロセスを不正なアクセスから保護します。Self-Protectionはデフォルトで有効になっています。Self-Protectionを無効にすることは推奨されません。



デフラグツールの動作中に何らかの問題が発生した場合には、一時的にSelf-Protectionを無効にしてください。

システムの復元ポイントにロールバックするには、Self-Protectionを一時的に無効にしてください。

ユーザーエミュレーションの禁止 オプションでは、Dr.Webウインドウ内で機能するマウスやキーボードをエミュレートするスクリプトの実行を含む、サードパーティ製ソフトウェアによるDr.Web設定の変更をすべて防ぐことができます(Dr.Web設定を変更するスクリプト、Dr.Webの動作を変更することを目的としたその他の操作など)。

スクリーンリーダーとの互換性を有効にする オプションを使用することで、Dr.Webのインターフェース要素の情報を読み上げるJAWSやNVDAなどのスクリーンリーダーを使用できます。このオプションは、障害のある方がDr.Webインターフェースにアクセスすることを可能にするものです。

日時

一部の悪意のあるプログラムは意図的にシステムのデータと時間を変更します。その結果、ウイルスデータベースはスケジュール通りに更新されず、ライセンスは期限切れとされ、保護コンポーネントは無効になります。







システム日時の変更をブロック オプションでは、システムのタイムゾーンや日時に対する手動または自動での変更をブロックすることができます。制限はすべてのシステムユーザーに対して設定されます。このオプションによって Office Control の [時間制限機能](#) を強化することができます。Office Control 内でインターネットやコンピューターの使用制限が設定されている場合、このオプションは自動的に有効になります。システム時間の変更が試行された場合に通知を受け取るようにするには、[通知パラメータ](#) で設定を行ってください。

7.4. ファイルスキャンのオプション

Scannerのパラメータを設定し、検出された脅威に対するデフォルトのアクションを変更できます。ほとんどの場合は、デフォルト設定が最適なものとなっています。必要がない限り変更しないようにしてください。

ファイルスキャンのオプションを開くには

1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. Dr.Webが [管理者モード](#) で動作していることを確認してください(プログラムウィンドウ下部にあるロックが開いています )。管理者モードではない場合は、ロックをクリックします 。
3. プログラムウィンドウ上部にある  をクリックします。
4. 製品のメイン設定ウィンドウが開きます。ウィンドウの左側にある **Scanner** を選択します。



コンポーネント設定の変更を行うことができるのは、Dr.Webが接続されている集中管理サーバー上で管理者によって該当するオプションが有効化されている場合のみです。



図 25. Scannerの設定



スキャンのオプション

このページでは Dr.Web Scanner 動作の全般的なパラメーターを設定することができます。

- **バッテリー駆動時にスキャンを一時停止する** - バッテリーモードに切り替えるときにスキャンを一時停止するには、このオプションを有効にします。このオプションはデフォルトで無効になっています。
- **警告音を有効にする** - Dr.Web Scannerが脅威を検出または駆除する全てのイベントに対して警告音を使用するには、このオプションを有効にします。このオプションはデフォルトで無効になっています。
- **コンピューターリソースの使用** - Dr.Web Scanner によって使用されるコンピューターリソースの上限を指定します。デフォルトの値は多くの場合に最適となっています。

アクション

この設定グループでは、感染したファイルや疑わしいファイル、マルウェアが検出された際のScannerの処理(アクション)を指定できます。

感染したオブジェクトのタイプごとに、それぞれのドロップダウンリストから個別にアクションを設定することができます。

- **感染した** - 既知の修復可能(と思われる)なウイルスに感染したオブジェクト
- **疑わしい** - 感染していると思われる、または悪意のあるオブジェクトを含んでいると思われるオブジェクト
- **潜在的に危険なオブジェクト(リスクウェア)**

デフォルトでは、Scannerは既知のウイルスや修復できる可能性のあるウイルスに感染したファイルについては、それらの修復を試みます。それ以外の危険なオブジェクトは **隔離** に移動します。Scannerのアクションは、検出された脅威のタイプごとに個別に変更できます。利用可能なアクションのセットは、脅威の種類によって異なります。デフォルトのアクションは最適なものとなっており、「推奨」と記載されています。

検出された脅威に対して、以下のアクションのうちいずれか1つを選択することができます。

アクション	説明
修復、修復不可能な場合は隔離	オブジェクトを感染前の状態に復元します。オブジェクトが修復不可能な場合や修復に失敗した場合は、隔離に移します。 このアクションは、トロイの木馬プログラムおよび 複合オブジェクト(アーカイブ、メールボックス、ファイルコンテナなど)に含まれる感染ファイルを除く、既知の修復可能なウイルスに感染したオブジェクトに対してのみ用いることができます。
修復、修復不可能な場合は削除	オブジェクトを感染前の状態に復元します。オブジェクトが修復不可能な場合や修復に失敗した場合は削除します。 このアクションは、トロイの木馬プログラムおよび 複合オブジェクト(アーカイブ、メールボックス、ファイルコンテナなど)に含まれる感染ファイルを除く、既知の修復可能なウイルスに感染したオブジェクトに対してのみ用いることができます。
削除	オブジェクトを削除します。 このアクションはブートセクターには使用できません。



アクション	説明
隔離	オブジェクトを 隔離 フォルダへ移します。 このアクションはブートセクターには使用できません。
無視	通知を表示せず、いずれのアクションも実行せずにオブジェクトをスキップします。 アドウェア、ダイアラー、ジョークプログラム、ハッキングツール、リスクウェアなどの潜在的に危険なファイルに対してのみ用いることができます。



複合オブジェクト（アーカイブ、メールの添付ファイル、ファイルコンテナ）内の脅威は個別に処理することができません。Dr.Web Scanner は、複合オブジェクト全体に対して選択されたアクションを適用します。

追加設定

詳細設定を開くには、**スキャンのオプション** ウィンドウで **アドバンス設定** リンクをクリックします（図 [Scannerの設定](#) 参照）。

インストールパッケージ、アーカイブ、メールファイルのスキャンを無効にすることができます。このオプションはデフォルトで有効になっています。

スキャン完了後にScannerが実行するアクションを、以下から1つ選択することができます。

- **アクションを適用しない** - Scanner は検出された脅威のリストを表示します。
- **検出された脅威を駆除** - Scanner は自動的に脅威を駆除します。
- **検出された脅威を駆除してコンピューターをシャットダウン** - Scanner は脅威を自動的に駆除し、コンピューターをシャットダウンします。

7.5. Server

Dr.WebとServer間の接続パラメータの確認や変更、Dr.Webのモバイルモードの設定を行うことができます。サーバー接続パラメータの変更はアンチウイルスネットワーク管理者によって制限されている場合があります。その場合、ボタンやチェックボックスは使用できなくなっています。

このセクションでは以下の設定を行うことができます。

- [接続パラメータ](#)
- [集中管理サーバーへの接続設定](#)
- [証明書](#)
- [端末接続パラメータ](#)
- [アドバンス設定](#)
- [モバイルモード](#)

端末とサーバー間のインタラクションパラメータに移動する

1. Dr.Web **メニュー** を開き、**Security Center** を選択します。
2. Dr.Webが **管理者モード** で動作していることを確認してください(プログラムウィンドウ下部にあるロックが開いています)。管理者モードではない場合は、ロックをクリックします 。
3. プログラムウィンドウ上部にある をクリックします。
4. 製品のメイン設定ウィンドウが開きます。ウィンドウの左側にある **Server** を選択します。



図26.端末接続設定

接続パラメータ

接続パラメータ グループには以下が表示されます。

- 接続のステータス - 端末と集中管理サーバーの接続状態
- **Server**アドレス - 端末が接続されている集中管理サーバーのアドレス
- **端末 ID** - 集中管理サーバーに接続するためのワークステーションID

ネットワーク管理者によって該当する権限が与えられている場合は、サーバーの接続設定を確認・管理することができます。



集中管理サーバーへの接続は、アンチウイルスネットワーク管理者と協力して行う場合のみ設定することが可能です。それ以外の場合、コンピューターはアンチウイルスネットワークから切断されます。



接続設定

現在の集中管理サーバーまたは新しいサーバーへの接続を設定するには、**設定を変更** をクリックします。接続設定 ウィンドウが開きます。



図27.サーバー接続設定

テーブルには、端末が接続できるすべてのサーバーのリストが表示されます。テーブルからサーバーを削除して新しいサーバーを追加することができます。

テーブル内のオブジェクトを操作するには、次の管理要素を使用できます。

- (+) ボタン - エントリを削除します。

証明書

端末を集中管理サーバーに接続させるには、有効な証明書(特定のサーバーごとの証明書、または複数のサーバーに対応する証明書)が必要です。複数のサーバーへの接続に使用する複数の証明書を追加できます。有効な証明書は、アンチウイルスネットワークの管理者によって提供されます。

デフォルトでは、管理者がサーバー上の暗号化キーを変更していない限り、インストール中に使用された証明書が指定されています。キーが変更された場合は、生成された証明書のリストから最新の証明書が表示されません。使用可能な証明書のリストを表示するか、または別の証明書を追加するには、**証明書のリスト** リンクをクリックします。

新しい証明書を追加するには、(+) をクリックします。開いたウィンドウで、必要なファイルを選択してください。

使用しない証明書を削除するには、(🗑️) をクリックします。



端末接続パラメータ

端末の接続パラメータを変更するには

1. 端末接続パラメータ ウィンドウで、サーバーとの接続に使用する端末IDとパスワードを指定します。端末IDとパスワードはサーバー管理者から提供されます。
2. **OK** をクリックして変更を保存してください。

接続パラメータをリセットし、新規端末として集中管理サーバーに接続するには

1. 端末接続パラメータ ウィンドウで パラメータをリセットして新規端末として接続 をクリックします。
2. 開いたウィンドウで、接続パラメータをリセットして新規端末として接続することを確認します。この操作は取り消すことができません。
3. 端末の登録が集中管理サーバーで確認されるとDr.Webは新しい端末IDとパスワードを受け取ります。この端末IDとパスワードがサーバー接続に使用されます。

仮想エージェントの接続パラメータ

サーバー側の設定に応じて、端末をDr.Web Scanning Serverに接続できます。その場合、端末はファイルとURLのスキャン要求をサーバーに送信する *仮想エージェント* と見なされます。ウイルスデータベースとフィルターのデータベースは端末上に保存されません

Dr.Web Scanning Serverを使用する場合、*仮想エージェントの接続パラメータ* 設定が次の情報とともに端末上に表示されます。

- 端末のDr.Web Scanning Server接続ステータス
- Dr.Web Scanning ServerのID



図 28. Dr.Web Scanning Serverとの接続



Dr.Web Scanning Serverとの接続がない場合、端末は保護されていません。アンチウイルスネットワーク管理者に連絡してください。

アドバンス設定

詳細設定を開くには、**Server** ウィンドウでアドバンス設定 リンクをクリックします(図 [端末接続設定](#) を参照)。アドバンス設定 グループで次のオプションを選択できます。

- **システム時間をServerの時間と同期させる** – コンピューターのシステム時刻を集中管理サーバーの時刻と同期させます。このモードでは、Dr.Webはサーバーの時刻に合わせてお使いのコンピューターの時刻を定期的に設定します。
- **Serverに接続できない場合にモバイルモードを使用する** – Serverに接続できない場合でもウイルスデータベースを最新の状態に保ちます。

モバイルモード

お使いのコンピューターが集中管理サーバーに接続できない状態が長期間継続する場合、Doctor Web 更新サーバーから更新を受け取るために Dr.Web をモバイルモードで動作させることを推奨します。モバイルモードを有効にするには **Serverに接続できない場合にモバイルモードを使用する** チェックボックスにチェックを入れてください。



Serverに接続できない場合にモバイルモードを使用する オプションは、集中管理サーバーの設定で、該当するワークステーションでのこのモードの使用が許可されている場合にのみ有効または無効にすることができます。



モバイルモードでは、Dr.Webは集中管理サーバーへの接続を試みます。接続に3回失敗した後、Doctor Webの更新サーバーからウイルスデータベースの更新を実行します。サーバーとの接続を確立しようとする試みは、約1分間隔で実行されます。

モバイルモードを設定するには

1. **設定** ボタンをクリックします。モバイルモード ウィンドウが開きます。
2. **更新を受け取る** ドロップダウンリストから、Doctor Webの更新サーバーでアップデートを確認する頻度を選択します。



更新を受け取る リストから **手動** を選択した場合、自動更新は実行されません。Dr.Webメニューで更新を有効にすることができます。

3. プロキシサーバーを使用するには、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。以下のフィールドがアクティブになります。

オプション	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
ログイン	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
認証の種類	プロキシサーバーへの接続に必要な認証の種類を選択

4. 編集が完了したら、**OK** をクリックして変更を保存します。変更を保存せずにウィンドウを閉じるには **キャンセル** をクリックします。



モバイルモードでは、ウイルスデータベースのみが更新されます。

集中管理サーバーとの接続が再確立される前に、サーバーに接続されていない状態で **Server** に接続できない場合にモバイルモードを使用する オプションを無効にした場合、ウイルスデータベースは更新を停止しますが、サーバーの検索は続行されます。

サーバー上でワークステーションの設定に対して行われたすべての変更は、モバイルモードが無効になり、Dr.Webと集中管理サーバー間の接続が再確立された後にのみ有効になります。






7.6. Server通知

ネットワーク管理者は、端末へのサーバー通知の送信を有効にすることができます。この機能は、集中管理サーバー上の通知を管理するのに便利です。端末に対してこの機能が有効になっている場合、一般 ウィンドウに **Server通知** セクションが表示されます。



図 29. Server通知の自動削除設定

Server通知の自動削除を有効／無効にするには

1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. Dr.Webが **管理者モード** で動作していることを確認してください(プログラムウィンドウ下部にあるロックが開いています )。管理者モードではない場合は、ロックをクリックします 。
3. プログラムウィンドウ上部にある  をクリックします。
4. 製品のメイン設定ウィンドウが開きます。ウィンドウの左側にある **Server通知** を選択します。
5. スイッチ  を使用して、**Server通知を自動的に削除** オプションを有効または無効にします。
6. このオプションを有効にした場合は、**Server通知の最大保存時間** ドロップダウンリストで必要な期間を選択してください。指定した期間を経過すると通知は削除されます。

8. ファイルとネットワーク

この設定のグループでは、主要な保護コンポーネントとScannerの設定にアクセスできます。

ファイルとネットワーク 設定グループを開くには

1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. 開いたウィンドウで、ファイルとネットワーク タイルをクリックします。





図30. ファイルとネットワーク ウィンドウ

保護コンポーネントを有効または無効にする

スイッチ  を使用して、必要なコンポーネントを有効または無効にします。

コンポーネントの設定を開くには

1. Dr.Webが [管理者モード](#) で動作していることを確認してください(プログラムウィンドウ下部にあるロックが開いています )。管理者モードではない場合は、ロックをクリックします 。
2. 必要なコンポーネントのタイルをクリックします。


このセクションでは以下の設定を行うことができます。

- [ファイルシステムモニターSpIDer Guard](#) は、開かれたファイルや起動したファイル、変更されたファイル、起動したプロセスをリアルタイムでスキャンするコンポーネントです。
- [インターネットモニターSpIDer Gate](#) は、HTTPトラフィックをスキャンするコンポーネントです。



- [メールアンチウイルスSpIDer Mail](#) は、メール内の悪意のあるオブジェクトの有無や、メールがスパムか否かをスキャンするコンポーネントです。
- [Firewall](#) は、インターネット経由での接続やデータのやり取りを制御し、疑わしい接続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コンポーネントです。
- [Scanner](#) は、ユーザーの要求やスケジュールに従ってオブジェクトをスキャンするコンポーネントです。
- [Dr.Web for Microsoft Outlook](#) は、Microsoft Outlook用のモジュールです。



コンポーネントを **無効** するには、Dr.Webを **管理者モード** で実行する必要があります。そのためには、プログラムウィンドウの下部にあるロック  をクリックします。

8.1. ファイルシステムのリアルタイム保護

ファイルシステムモニター SpIDer Guard は、コンピューターをリアルタイムで保護し、コンピューターが感染することを防ぎます。SpIDer Guard はWindowsの起動時に自動的に起動し、ファイルが開かれたり、実行されたり、編集されたりした場合にそのファイルをスキャンします。また、SpIDer Guard は起動したプロセスの動作も監視します。

ファイルシステムモニターを有効／無効にするには



1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. 開いたウィンドウで、**ファイルとネットワーク** タイルをクリックします。
3. スイッチ  を使用して、ファイルシステムモニター SpIDer Guard を有効または無効にします。



図 31. SpIDer Guard を有効／無効にする



このセクションでは以下の設定を行うことができます。

- [SpIDer Guardオペレーションの特性](#)
- [リムーバブルメディアのスキャン](#)
- [検出された脅威に対するアクション](#)
- [SpIDer Guardのスキャンモードを選択](#)
- [追加設定](#)

以下も参照してください。

- [ファイルやフォルダをスキャンから除外](#)
- [アプリケーションをスキャンから除外](#)

SpIDer Guard オペレーションの特性

デフォルトの設定では、SpIDer Guard は、ハードドライブで作成または変更されたファイルと、リムーバブルメディアで開いている全てのファイルに対してのオンアクセススキャンを実行します。さらに、SpIDer Guard は実行中のプロセスのウイルスのようなアクティビティを常に監視し、悪意のあるプロセスが検出された場合はそれをブロックします。



SpIDer Guard では、アーカイブ、メールアーカイブ、ファイルコンテナ内のファイルはスキャンされません。アーカイブまたはメールの添付ファイル内のファイルが感染している場合は、アーカイブ抽出時に脅威を検出し、コンピューターが感染しないようにします。

デフォルトでは、SpIDer Guard はWindowsの起動時に自動的に読み込まれ、現在のWindowsセッション中にはアンロードできません。





Dr.WebとMicrosoft Exchange Server の間に互換性がない場合があります。問題が発生した場合は、SpIDer Guard の [除外リスト](#) にMicrosoft Exchange Serverデータベースとトランザクションログを追加してください。

SpIDer Guard ファイルシステムモニターの設定

感染したオブジェクトが検出された場合、SpIDer Guard は指定された設定に従ってアクションを適用します。ほとんどの場合、デフォルト設定が最適です。必要がない限り変更しないでください。

SpIDer Guard 設定を開くには

1. Dr.Webが [管理者モード](#) で動作していることを確認してください(プログラムウィンドウ下部にあるロックが開いています )。管理者モードではない場合は、ロックをクリックします 。
2. **SpIDer Guard** タイルをクリックします。コンポーネントの設定ウィンドウが開きます。

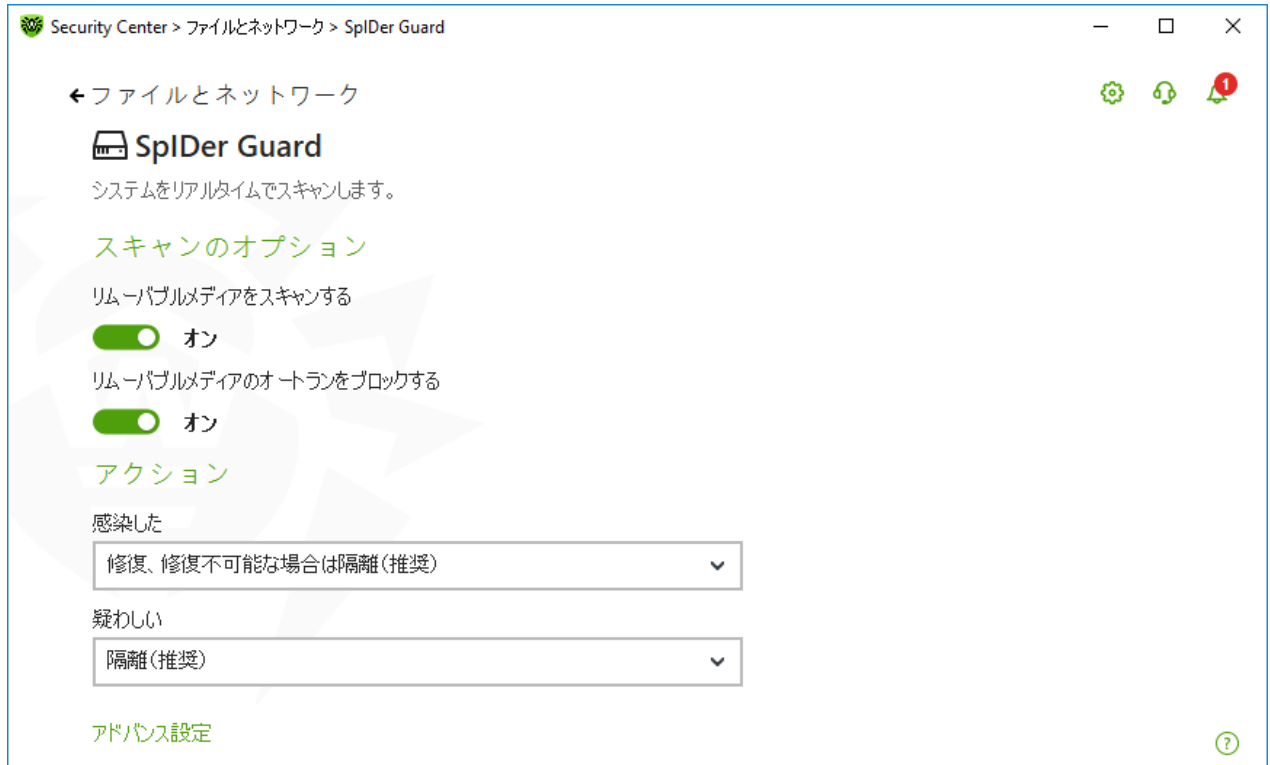



図 32. ファイルシステムモニターの設定

リムーバブルメディアのスキャン

デフォルトの設定では、SpiDer Guard は、ハードドライブで作成または変更されたファイルと、リムーバブルメディアで開かれている全てのファイルに対してのオンアクセススキャンを実行し、それらのアクティブコンテンツの自動起動をブロックします。SpiDer Guard がファイルシステムへのアクセスをリアルタイムモードで監視し、悪意のあるコードの実行をブロックするため、コンピュータがリムーバブルメディアを介して感染するのを防ぐことができます。



OSによっては、一部のリムーバブルメディアがハードドライブとして認識されることがあります（ポータブルUSBハードドライブなど）。その場合、Windowsの通知領域に「ハードウェアの安全な取り外し」や「メディアを取り出す」アイコンが表示されません。パラノイドスキャンモードでない限り、SpiDer Guard は、そのようなディスクからファイルを読み取る際にはスキャンを実行しません。そのようなデバイスは接続時にDr.Web Scannerでスキャンしてください。

スキャンのオプション 設定グループのスイッチ  を使用して、リムーバブルメディアをスキャンするとリムーバブルメディアのオートランをブロックする オプションを有効または無効にできます。



自動実行オプションで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のオートランをブロックする オプションを一時的に無効にすることをお勧めします。

検出された脅威に対するアクション

このグループでは、Dr.Webがファイルシステムモニター SpiDer Guard で検出された脅威に対するアクションを設定できます。

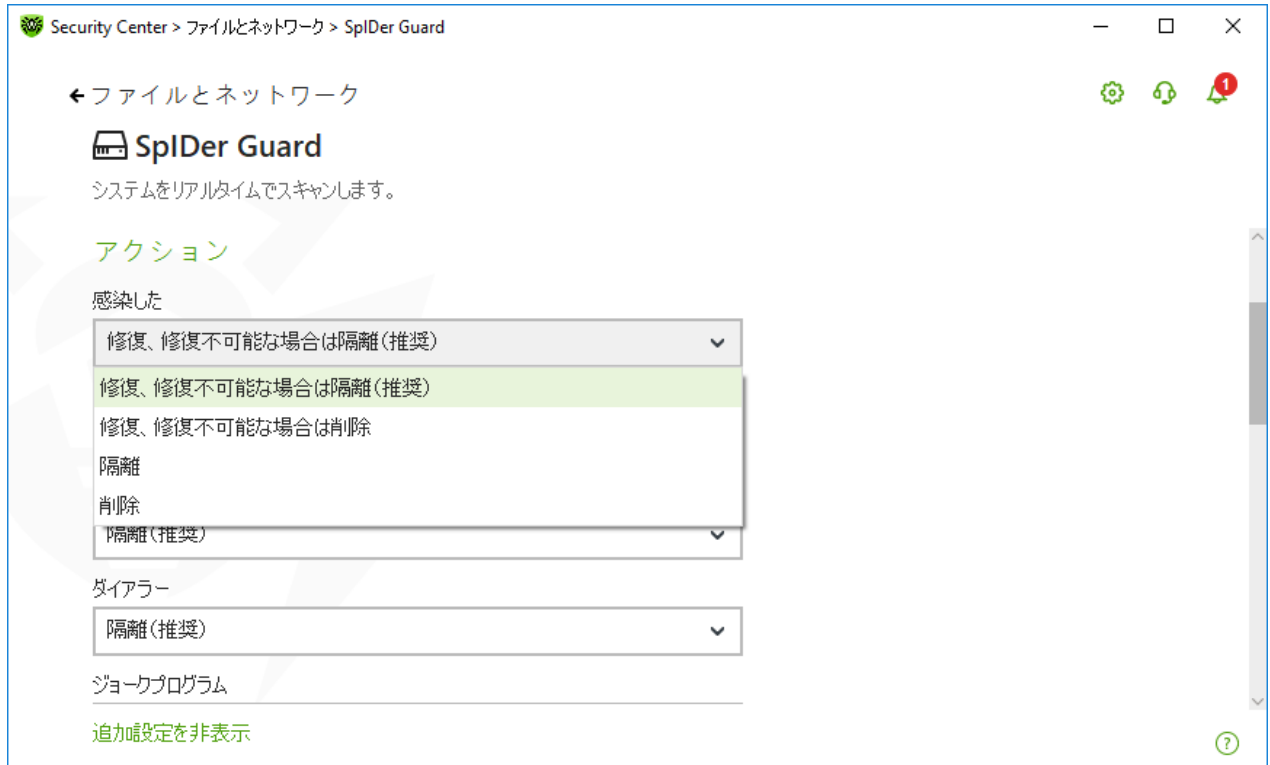


図 33. 脅威に対するアクションを設定する

アクションは、悪意のあるオブジェクトや疑わしいオブジェクトのタイプごとに個別に設定されます。これらのアクションは、オブジェクトのタイプによって異なります。オブジェクトのタイプごとに推奨されるアクションがデフォルトで設定されています。処理された全てのオブジェクトのコピーは、**隔離**に保存されます。

可能なアクション

以下のアクションを脅威に適用することができます。

アクション	説明
修復、修復不可能な場合は隔離	オブジェクトを感染前の状態に復元します。オブジェクトが修復不可能な場合や修復に失敗した場合は、隔離に移します。 このアクションは、トロイの木馬プログラムおよび複合オブジェクト（アーカイブ、メールボックス、ファイルコンテナなど）に含まれる感染ファイルを除く、既知の修復可能なウイルスに感染したオブジェクトに対してのみ用いることができます。
修復、修復不可能な場合は削除	オブジェクトを感染前の状態に復元します。オブジェクトが修復不可能な場合や修復に失敗した場合は削除します。 このアクションは、トロイの木馬プログラムおよび複合オブジェクト（アーカイブ、メールボックス、ファイルコンテナなど）に含まれる感染ファイルを除く、既知の修復可能なウイルスに感染したオブジェクトに対してのみ用いることができます。
削除	オブジェクトを削除します。 このアクションはブートセクターには使用できません。



アクション	説明
隔離	オブジェクトを 隔離 フォルダへ移します。 このアクションはブートセクターには使用できません。
無視	通知を表示せず、いずれのアクションも実行せずにオブジェクトをスキップします。 アドウェア、ダイアラー、ジョークプログラム、ハッキングツール、リスクウェアなどの潜在的に危険なファイルに対してのみ用いることができます。
レポート	通知を表示し、いずれのアクションも実行せずにオブジェクトをスキップします。 このアクションは疑わしいオブジェクトおよびマルウェアに対してのみ用いることができます。

SpIDer Guard スキャンモード

このセクションおよび次のセクションにアクセスするには、[アドバンス設定](#) リンクをクリックします。

この設定グループでは、SpIDer Guard のファイルスキャンモードを選択できます。

モード	説明
最適、デフォルトで使用	<p>このモードでは、SpIDer Guardは以下のいずれかのアクションが実行された場合のみオブジェクトをスキャンします。</p> <ul style="list-style-type: none">ハードドライブ上のオブジェクトに対し、ファイルの実行、新しいファイルの作成、既存のファイルまたはブートセクター内へのレコードの追加が試行された場合リムーバブルメディア上のオブジェクトに対し、ファイルまたはブートセクターへのあらゆるアクセス(書き込み、読み込み、実行)が試行された場合 <p>Dr.Web Scannerが全てのハードドライブを完全にスキャンした後、このモードを使用することをお勧めします。このモードを有効にすると、SpIDer Guardは、リムーバブルメディアを介して新しいウイルスやその他の悪意のあるオブジェクトがコンピューターに侵入する可能性を食い止め、過去のスキャンから「クリーン」であることが判明しているオブジェクトを除外することによってパフォーマンスも維持します。</p>
パラノイド	<p>このモードでは SpIDer Guard は、ハードドライブ・ネットワークドライブ・リムーバブルメディア上にある、ファイルおよびブートセクターに対するあらゆるアクセス(作成、書き込み、読み込み、実行)が試行された場合に、それらをスキャンします。</p> <p>このモードでは最大の保護が保証されますが、コンピューターのパフォーマンスは大幅に低下します。</p>



追加設定

このグループの設定では、オンザフライでオブジェクトをスキャンするためのパラメータを指定でき、選択した SpIDer Guard の動作モードに関係なく常に適用されます。以下を有効にできます。

- ヒューリスティック解析の使用
- ダウンロードするプログラムおよびモジュールのスキャン
- インストールパッケージのスキャン
- ネットワークドライブ上にあるファイルのスキャン(非推奨)
- コンピューターのルートキットスキャン(推奨)
- Windows Script HostおよびPowerShellで実行されたスクリプトのスキャン(Windows 10、Windows 11向け)

ヒューリスティック解析

デフォルトでは、SpIDer Guard は [ヒューリスティック解析](#) を用いてスキャンを実行します。このオプションが無効になっている場合、スキャンにはシグネチャ解析のみが用いられます。

ルートキットのバックグラウンドスキャン

Dr.Web 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、実行中のプロセスおよびモジュール、RAM、MBR/VBRディスク、コンピューターBIOSシステム、およ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(プロセッサ時間、RAMの空き容量など)およ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。



バックグラウンドルートキットスキャンの際には、[除外するファイル](#) 指定されたファイルおよびフォルダはスキャンされません。

ルートキットのバックグラウンドスキャンはデフォルトで有効になっています。



バックグラウンドスキャンが有効になっている場合、SpIDer Guard を無効にしてもそのスキャンは実行されます。SpIDer Guard が有効であるか無効であるかは、バックグラウンドスキャンの実行に関係しません。

8.2. Webトラフィックをチェックする

SpIDer GateはHTTPトラフィックをスキャンし、悪意のあるオブジェクトをブロックします。HTTPは、ブラウザ、ダウンロードマネージャー、インターネットで動作する他のアプリケーションによって使用されます。SpIDer Gateは、HTTPSなどの暗号化プロトコルで送信されたデータはチェックしません。

デフォルトでは、SpIDer Gateは非推奨サイトや感染源として知られるWebサイトをフィルタリングします。

SpIDer Gate はWindowsの起動と同時に自動的に起動し、メインメモリ内に常駐します。

トラフィックのスキャンと非推奨サイトのフィルターを有効／無効にするには

1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. 開いたウィンドウで、ファイルとネットワーク タイルをクリックします。
3. スイッチ  を使用して、SpIDer Gate を有効または無効にします。



図34. SpIDer Gate を有効／無効にする

このセクションでは以下の設定を行うことができます。

- [IMクライアントのトラフィックとURLをスキャン](#)
- [ブロックパラメータ](#)
- [プログラムをブロック](#)
- [チェックされていないオブジェクトや破損しているオブジェクトをブロック](#)
- [アーカイブとインストールパッケージを確認](#)
- [チェック時にシステムリソースを使用](#)
- [トラフィック方向](#)

以下も参照してください:

- [スキャンからWebサイトを除外](#)
- [アプリケーションをスキャンから除外](#)

トラフィックチェックのオプション

ほとんどの場合、デフォルトの SpIDer Gate 設定が最適です。必要がない限り変更しないでください。



コンポーネント設定の変更を行うことができるのは、Dr.Webが接続されている集中管理サーバー上で管理者によって該当するオプションが有効化されている場合のみです。

SpIDer Gate 設定を開くには

1. Dr.Webが **管理者モード** で動作していることを確認してください(プログラムウィンドウ下部にあるロックが開いています)。管理者モードではない場合は、ロックをクリックします 。
2. **SpIDer Gate** タイルをクリックします。コンポーネントの設定ウィンドウが開きます。



図35. HTTPトラフィックチェック設定

IMクライアントのトラフィックとURLをスキャン

スキャンのオプション グループで、Mail.ru Agent、ICQ、Jabberクライアントなどのインスタントメッセージクライアントによって送信されたURLやファイルのスキャンを有効にできます。チェックされるのは着信トラフィックのみです。デフォルトでは、このオプションが有効になっています。



検出された脅威には、次のアクションが適用されます。

ファイル名	アクション
URLスキャン	
感染源として知られるWebサイト	自動的にブロックされます。
著作権者からの申し立てによりリストに追加された非推奨サイトやURL	ブロックパラメータグループの設定に従ってブロックされます。
ファイルスキャン	
ウイルス	自動的にブロックされます。
マルウェア： • 疑わしい • リスクウェア • ダイアラー • ハッキングツール • アドウェア • ジョークプログラム	プログラムをブロックグループの設定に従ってブロックされます。

SpIDer Gate がメッセージ内のURLをスキャンする際は、スキャンから除外する[Webサイト](#)と[アプリケーション](#)が適用されます。

ブロックパラメータ

ブロックパラメータグループでは、該当するオプションを有効にすることで、著作権所有者からの申し立てにより一覧に追加されたURLと信頼できないWebサイトの自動ブロックを有効にできます。

必要なWebサイトへのアクセスを許可するには、**除外**グループで[除外を指定](#)します。



デフォルトでは、SpIDer Gate は [スキャンから除外するアプリケーションのリスト](#) を除いて、感染源またはマルウェアソースとして知られるWebサイトへのアクセスをブロックします。

プログラムをブロック

このセクションおよび次のセクションにアクセスするには、[アドバンス設定](#) リンクをクリックします。

SpIDer Gate では以下のマルウェアをブロックできます：

- 疑わしい
- リスクウェア
- ダイアラー
- ハッキングツール



- アドウェア
- ジョークプログラム

マルウェアのブロックを有効にするには、[アドバンス設定](#) リンクをクリックし、[プログラムをブロック](#) グループで対応するスイッチを有効にします。デフォルトでは、SpIDer Gateは疑わしいプログラム、アドウェア、ダイヤラーをブロックします。

オブジェクトをブロック

SpIDer Gate では、チェックされていないオブジェクトや破損したオブジェクトをブロックできます。デフォルトでは、これらの設定は無効になっています。設定を開くには、[アドバンス設定](#) リンクをクリックします。

詳細設定

[アーカイブをスキャン](#) と [インストールパッケージをスキャン](#) する。デフォルトでは、この設定は無効になっています。

システムリソース消費のレベル。 ファイルを読み込むときなどに、Dr.Webで最終的なファイルサイズを特定できないことがあります。その場合、ファイルは分割してスキャンに送信されます。これには、コンピューターリソースが使用されます。リソースの使用レベルを設定し、サイズが不明なファイルを送信する頻度を決定できます。高いリソース使用レベルを選択すると、ファイルがより頻繁に送信され、より高速にスキャンされます。ただし、頻繁にスキャンを行うとプロセッサの負荷が増えます。

トラフィックスキャンモード。 デフォルトでは、SpIDer Gate は受信トラフィックのみをスキャンします。必要に応じて、[HTTPトラフィックタイプ](#) をスキャンするよう選択できます。

トラフィックのチェック中は、SpIDer Gate 設定、[ホワイトリスト](#)、[スキャンから除外するアプリケーションのリスト](#) が適用されます。

8.3. メールスキャン

SpIDer Mailでメールをスキャンします。メールアンチウイルスSpIDer Mailはデフォルトでインストールされます。メモリに常駐し、OSの起動時に自動的に実行されます。SpIDer Mailは、Dr.Web Anti-spamを使用してスパム（迷惑メール）をスキャンすることもできます。SpIDer Mailは、暗号化されたメールトラフィックはスキャンできません。

メールスキャンを有効／無効にするには


1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. 開いたウィンドウで、[ファイルとネットワーク](#) タイルをクリックします。
3. スイッチ  を使用して、メールアンチウイルス SpIDer Mail を有効または無効にします。



図 36. SpIDer Mail を有効／無効にする

このセクションでは以下の設定を行うことができます。

- [メールの処理](#)
- [その他のコンポーネントによるメールスキャン](#)

以下も参照してください。

- [メールスキャンを設定](#)
- [Anti-Spamの設定](#)

メール処理

SpIDer Mail は受信するすべてのメールを監視し、メールクライアントが受け取る前にそれらをスキャンします。脅威が検出されなかった場合、メールは、あたかもサーバーから直に送られたかのようにメールクライアントに渡されます。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、感染した受信メールやスキャンされなかったメール(例えば、構造が複雑だったために)を検出した際に SpIDer Mail は以下のようなアクションを実行します。

メールの種類	アクション
感染したメール	メッセージから悪意のあるコンテンツを削除し、その後、通常通り配信します。このアクションはメールの 修復 と呼ばれます。
疑わしいオブジェクトを含んだメール	メッセージを個別のファイルとして 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ールの 隔離 です。隔離されたメールはすべて POP3、IMAP4メールサーバーからも削除されます。



メールの種類	アクション
安全なメールとスキャンされなかったメール	メッセージをメールクライアントに渡します(スキップ)。

送信されるメールが感染している、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。ユーザーはメールが送信されない旨の通知を受け取ります(そのようなメールは通常、メールクライアントによって保存されます)。

その他のコンポーネントによるメールスキャン

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できますが、SpIDer Mail には次のような利点があります。

- Dr.Web Scanner はポピュラーなメールボックスのフォーマットすべてをサポートしているわけではありません。SpIDer Mail を使用した場合は、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 はメール受信時ではなく、ユーザーの操作に応じ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る場合があります。

8.3.1. メールスキャンを設定する

デフォルトでは、SpIDer Mail は既知の修復可能な(と思われる)ウイルスに感染したメッセージの修復を試み、アドウェア、ダイアラー、修復不可能または疑わしいメッセージを **隔離** に移し、危険度の低いその他の脅威を無視します。それ以外のメッセージはそのままの状態です。SpIDer Mail によって配信されます(スキップ)。デフォルトのメールスキャン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。

このセクションでは以下の設定を行うことができます。

- [検出された脅威に対するアクション](#)
- [メールスキャンのパラメータを設定](#)
- [アーカイブをスキャン](#)

メールスキャンを設定

デフォルトの SpIDer Mail 設定は最近のユーザーに最適な内容になっており、最大限の保護が提供され、必要なユーザー操作は最小限に抑えられます。ただし、デフォルトではSpIDer Mailによってメールプログラムの一部の機能がブロックされることがあります(たとえば、複数のアドレスにメッセージを送信すると大量配信とみなされ、受信メールのスパムはスキャンされません)。自動削除された場合は、感染したメッセージのテキストの安全な部分からの有用な情報も利用できなくなります。





コンポーネント設定の変更を行うことができるのは、Dr.Webが接続されている集中管理サーバー上で管理者によって該当するオプションが有効化されている場合のみです。

メールスキャン設定の編集を開始するには

1. Dr.Web [メニュー](#) を開き、**Security Center** を選択します。



2. 開いたウィンドウで、**ファイルとネットワーク** タイルをクリックします。
3. Dr.Webが **管理者モード** で動作していることを確認してください(プログラムウィンドウ下部にあるロックが開いています )。管理者モードではない場合は、ロックをクリックします 。
4. **SpIDer Mail** タイルをクリックします。コンポーネントの設定ウィンドウが開きます。

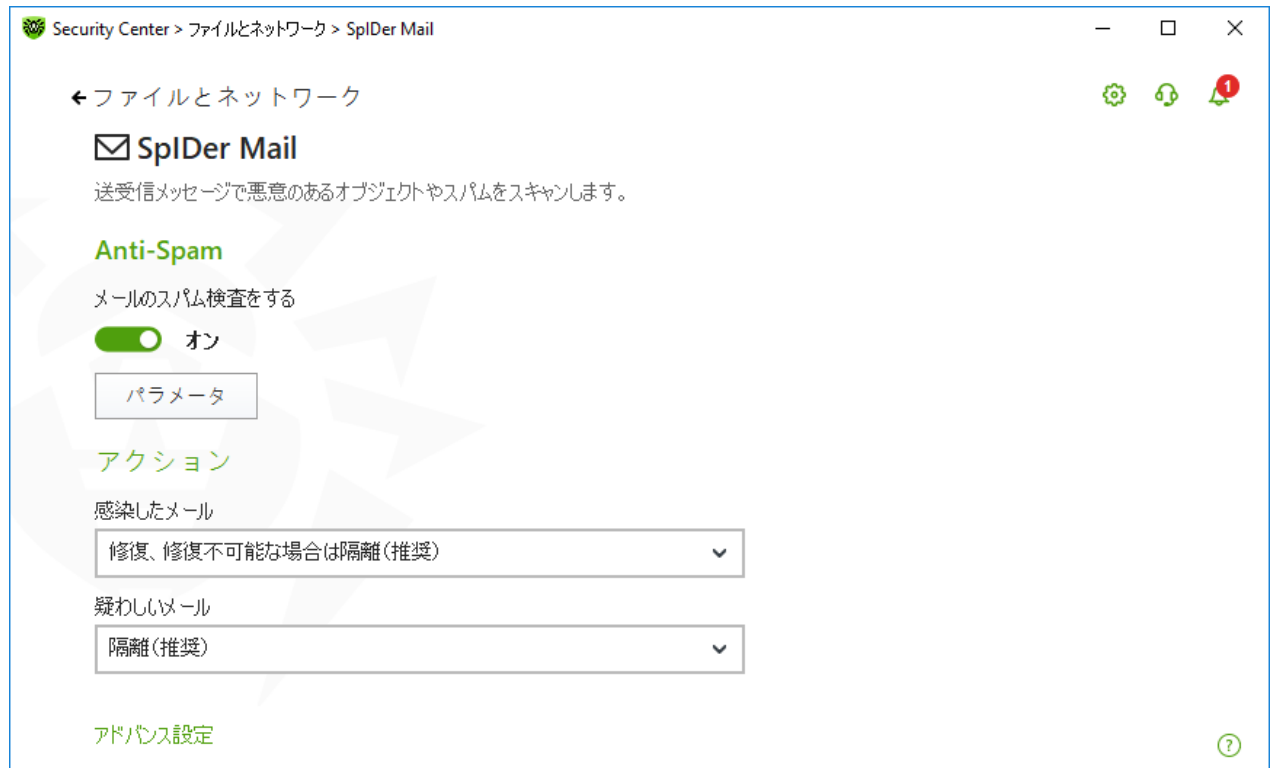


図37. メールスキャンの設定

検出された脅威に対するアクション

このグループでは、Dr.Webが脅威を検出した場合にメッセージに対して適用するアクションを設定できます。

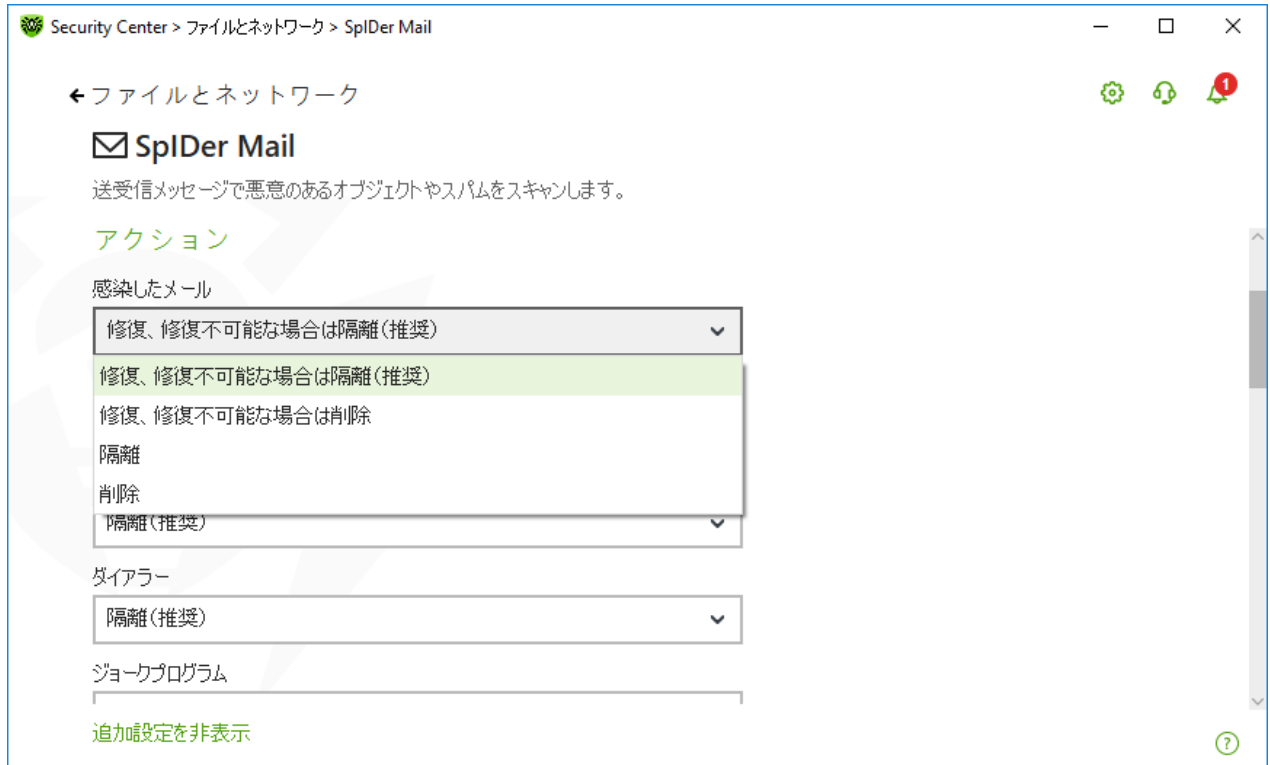


図 38. メッセージに対するアクションを設定する

可能なアクション

以下のアクションを脅威に適用することができます。

アクション	説明
修復、修復不可能な場合は隔離	メールを感染前の状態に復元しようとします。メールが修復不可能な場合や修復に失敗した場合は、隔離に移します。 検出と同時に削除されるトロイの木馬プログラムを除く感染したメールに対して用いることができます。アーカイブ内のファイルに対しては使用できません。 メッセージの送信に失敗します(送信メールの場合)。
修復、修復不可能な場合は削除	メールを感染前の状態に復元しようとします。メールが修復不可能な場合や修復に失敗した場合は、削除します。 メッセージの送信に失敗します(送信メールの場合)。
削除	メールを削除します。メールは受信者に配信されず、メールクライアントはその旨の通知を受け取ります。 メッセージの送信に失敗します(送信メールの場合)。
隔離	メールを 隔離 フォルダへ移します。メールは受信者に配信されず、メールクライアントはその旨の通知を受け取ります。 メッセージの送信に失敗します(送信メールの場合)。



アクション	説明
無視	メールを通常通りメールクライアントに渡します。すなわち、いかなるアクションも実行しません。

セキュリティのレベルをデフォルトの設定よりも高くしたい場合、**アドバンス設定** リンクをクリックし、**未スキャン** に対して **隔離** を選択してください。隔離に移したファイルは、後でDr.Web Scannerによってスキャンすることをお勧めします。



メールのスキャンを無効にしたい場合、SpIDer Guard が常時コンピューターを監視していることを確認してください。

メールスキャンのパラメータを設定

メッセージスキャンのパラメータにアクセスするには、**アドバンス設定** リンクをクリックします。

メールに対する追加動作

このグループでは、SpIDer Mail がメールを処理する際に適用される追加のアクションを設定することができます。

オプション	説明
'X-AntiVirus' ヘッダをメッセージに入れる	このオプションはデフォルトで有効になっています。 データフォーマットを編集することはできません。SpIDer Mail はスキャン結果および Dr.Web のバージョンに関する情報を、処理したメッセージのヘッダーに加えます。
サーバーの変更されたメールを削除する	SpIDer Mail によって 削除または 隔離 アクションが適用されたメッセージを削除します。メッセージは、メールクライアントの設定に関係なくメールサーバーから削除されます。

スキャンの最適化

このグループでは、あまりにも複雑なためスキャンに時間がかかり過ぎるメッセージを SpIDer Mail が未検査メッセージとして判定するための条件を設定することができます。**メッセージスキャンのタイムアウト** オプションを有効にし、スキャンにかかる最大時間を設定してください。その上限(デフォルトでは250秒)を超えると SpIDer Mail はスキャンを中止します。



アーカイブをスキャン

メールに添付されたアーカイブファイルを SpIDer Mail によってスキャンしたい場合は **アーカイブをスキャン** オプションを有効にします。必要に応じて、以下のオプションを有効にしてアーカイブのスキャンパラメータを設定してください。

- **展開するファイルのサイズ上限** – 解凍時のファイルサイズ上限です（デフォルトでは30,720 KB）。解凍するファイルのサイズが上限を超えた場合、SpIDer Mail はアーカイブを展開せず、スキャンも行いません。
- **アーカイブの最大ネストレベル** – ネスティングレベルが指定された値（デフォルト値は64）よりも大きい場合、SpIDer Mail はこの上限レベルまで解凍とスキャンを続行します。



パラメータ値を0に設定した場合、上限は無くなります。

追加設定

以下の設定では、追加のメールスキャンパラメータを設定できます。

- ヒューリスティック解析を使用する - このモードでは、**特別な手法** を使用して、未知のウイルスに感染している可能性の高いオブジェクトを検出します。ヒューリスティック解析を無効にするには **ヒューリスティック解析を使用する（推奨）** チェックボックスのチェックを外してください。
- インストールパッケージのスキャン - インストールパッケージをスキャンします。このオプションはデフォルトで無効になっています。

通知設定

指定されたアクションが実行された後、SpIDer Mail は通知領域内に通知を表示します。必要に応じて、デスクトップの通知を **設定** することができます。

8.3.2. Anti-Spamの設定

Anti-Spam設定を含むデフォルトのSpIDer Mail設定は、ほとんどの場合に最適なものとなっています。必要がない限り変更しないようにしてください。

スパムメールのスキャンを有効／無効にするには




1. Dr.Web **メニュー**  を開き、**Security Center** を選択します。
2. 開いたウィンドウで、**ファイルとネットワーク** タイルをクリックします。
3. Dr.Webが **管理者モード** で動作していることを確認してください（プログラムウィンドウ下部にあるロックが開いています ）。管理者モードではない場合は、ロックをクリックします 。
4. **SpIDer Mail** タイルをクリックします。コンポーネントの設定ウィンドウが開きます。



図39. メールスキャンの設定

5. **Anti-Spam** セクションで、対応するスイッチ を使用してスパムメールのスキャンを有効または無効にします。

Anti-Spamのパラメータを設定する

1. **Anti-Spam** グループで **パラメータ** をクリックします。

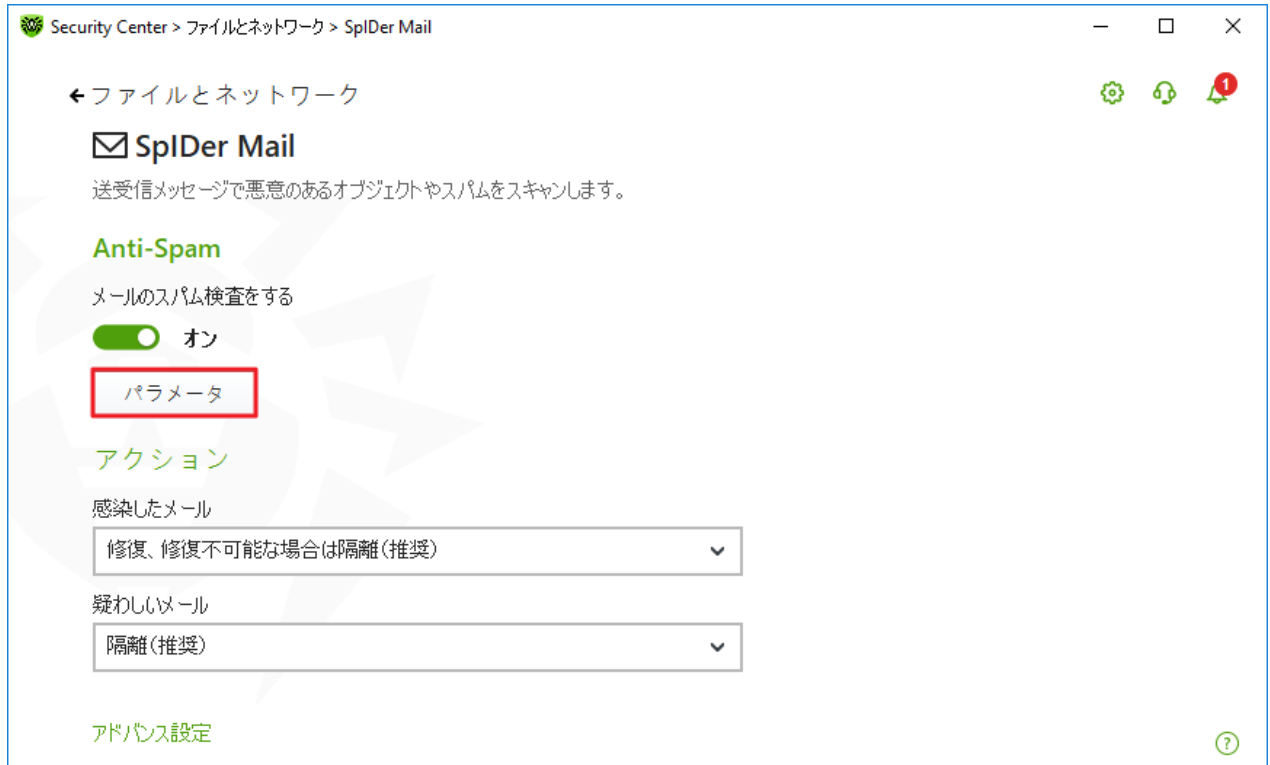


図 40. Anti-Spamのパラメータを変更する

2. 開いている **Anti-spam**パラメータ ウィンドウで、必要なオプションを有効または無効にします。

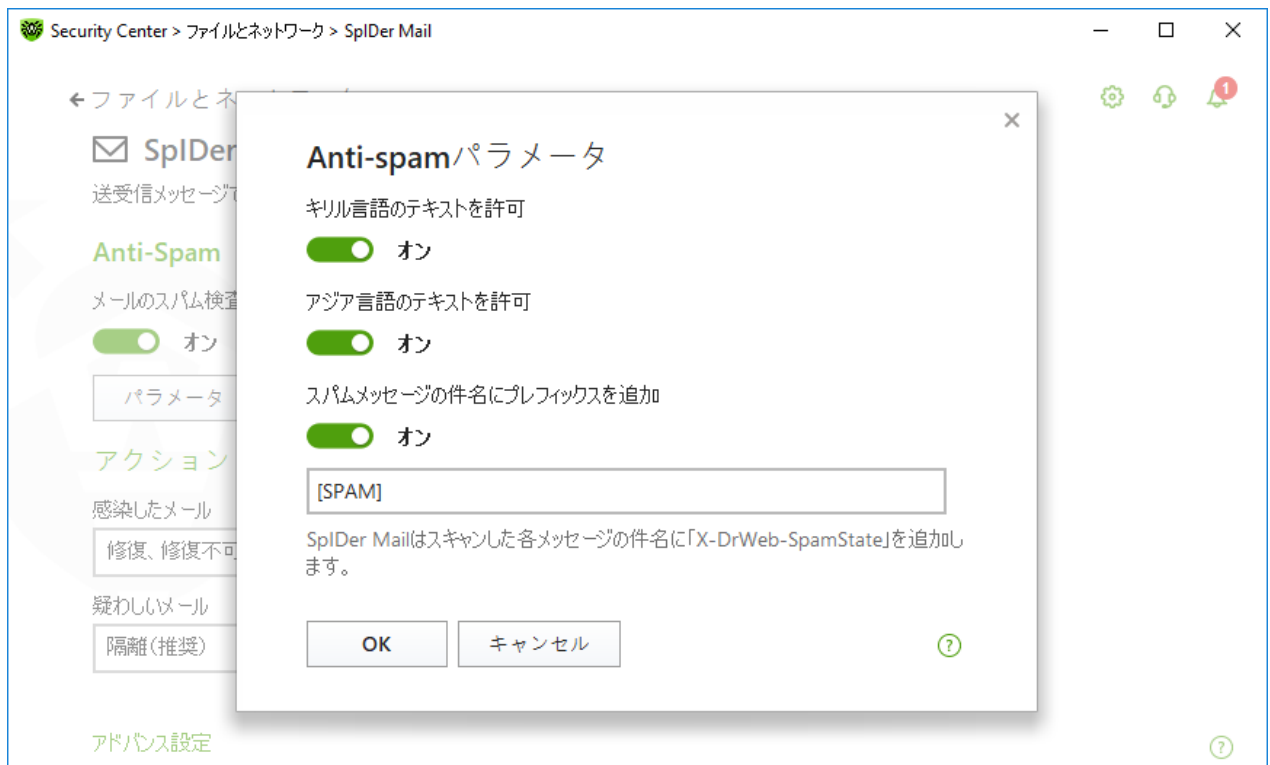


図41. Anti-Spamのパラメータ



使用可能なスキャン設定（デフォルトで有効です）

オプション	説明
キリル言語のテキストを許可	SpIDer Mail がキリル言語のメールを自動的にスパムと見なさないようにするにはこのチェックボックスにチェックを入れます。このオプションが無効な場合、キリル文字を含んだメッセージはスパムと見なされる可能性が高くなります。
アジア言語のテキストを許可	このチェックボックスを選択すると、SpIDer Mailでアジア言語のエンコードが使用されたメールを事前分析なしにスパムとしてマークしないようにします。これを選択しない場合、メールがスパムとしてマークされる可能性が高くなります。
スパムメッセージの件名にプレフィックスを追加	デフォルトでは、SpIDer Mail はすべてのスパムメールの件名欄に [SPAM] プレフィックスを加えます。 SpIDer Mail はスパムメッセージの件名に特別なプレフィックスを加えます。 プレフィックスを使用することで、ヘッダによるフィルタリングを行うことができないメールクライアント（例：Microsoft Outlook Express）内のスパムに対するフィルタリングルールを作成することが可能になります。

3. 設定を保存するには、**OK** をクリックします。

追加情報

Anti-Spamテクノロジー

Dr.Web Anti-Spamテクノロジーは、いくつかのグループに分けられるルールから成っています。

- **ヒューリスティック解析** - メールすべてのパート（ヘッダ、メッセージ本文、添付ファイル）を実証的に解析するテクノロジーです。
- **回避技術の検出** - アンチスパムフィルターをすり抜けるためにスパマーによって使用される回避技術を検出するテクノロジーです。
- **HTML署名解析** - HTMLコードを含むメッセージを、アンチスパムライブラリ内の既知のパターンリストと比較するテクノロジーです。スパマーが使用する典型的な画像サイズに関するデータと併せて用いられ、オンラインコンテンツにリンクしたHTMLコードを含むスパムメールからユーザーを保護します。
- **意味解析** - 特別な辞書を使用して、メッセージの単語と句（目に見えるもの、および隠されたもの）をスパムで使用されるものと比較するテクノロジーです。
- **アンチスキュム** - いわゆる「ナイジェリア」詐欺、ローン詐欺、宝くじおよびカジノ詐欺、銀行やクレジット会社からの偽のメールを含む、スキュムおよびファームングメッセージをフィルタリングするテクノロジーです。
- **テクニカルスパム** - メールサーバーからの配信に失敗した旨を伝えるメッセージであるバウンスを検出するテクノロジーです。そのようなメッセージはメールワームによっても送信されるため、バウンスは望まれないメッセージとして検出されます。



スパムフィルターによるメールの処理

SpIDer Mailは処理されたメッセージに以下のヘッダを加えます。

- X-DrWeb-SpamState: <value> - <value> は、メッセージがスパムである(Yes)またはスパムではない(No)とSpIDer Mailによって判断されたことを示します。
- X-DrWeb-SpamVersion: <version> - <version> は Dr.Web Anti-Spam のバージョンです。
- X-DrWeb-SpamReason: <spam rate> - <spam rate> には様々なスパム基準に基づいた評価の一覧が含まれています。

選択されている場合、これらのヘッダおよびプレフィックスを件名欄で使用し、メールクライアントでのメールフィルタリングを設定することができます。



IMAP/NNTPプロトコルを使用している場合、メールを完全な形で即座にメールサーバーからダウンロード(事前のヘッダ検査無しで)するようメールクライアントを設定してください。スパムフィルターが正常に動作するために必要です。

スパムフィルターはMIME RFC 822準拠のメールメッセージを処理します。

スパムフィルターのパフォーマンス向上のために、スパム検出におけるエラーを確認された際は、報告をお願いいたします。

スパム検出のエラー

スパムフィルターでエラーが見つかった場合は以下の手順を実行してください。

1. 新しいメールを作成し、誤って処理されたメッセージを添付します。メール本文に含まれるメッセージは分析されません。
2. メッセージをアンチウイルスネットワーク管理者 に送信してください。

8.4. 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、望まない接続や疑わしい接続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します。

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



Firewallを有効／無効にするには



1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. 開いたウィンドウで、**ファイルとネットワーク** タイルをクリックします。
3. スイッチ  を使用して、Firewall を有効または無効にします。



図 42. Firewallを有効／無効にする

このセクションでは以下の設定を行うことができます。

- [Firewallの設定](#)
- [アプリケーションのパラメータ](#)
- [アプリケーションルール](#)
- [アプリケーションルールのパラメータの設定](#)
- [ネットワークのパラメータ](#)
- [パケットフィルター](#)
- [パケットフィルタリングルールの設定](#)
- [フィルタリングルール](#)

8.4.1. Firewallの設定

Firewallの以下の設定を行うことができます。

- [動作モードを選択する](#)
- [許可されたアプリケーションを一覧表示する](#)
- [既知のネットワークのパラメータを設定する](#)



設定で **Dr.Web** の設定をパスワードで保護する オプションが有効になっている場合、Firewall の設定にアクセスする際にパスワードを入力する必要があります。

デフォルトでは、Firewall は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しません。イベントのロギングは動作モードに関係なく行われます。

ほとんどの場合、デフォルト設定が最適です。必要がない限り変更しないでください。

Firewall の設定を開いて動作モードを選択するには

1. Dr.Web が **管理者モード** で動作していることを確認してください (プログラムウィンドウ下部にあるロックが開いています)。管理者モードではない場合は、ロックをクリックします 。
2. **Firewall** タイルをクリックします。コンポーネントの設定ウィンドウが開きます。



図43. Firewallの設定

お使いのコンピューター上のアプリケーションが相互に接続すること、すなわちコンピューター上にあるアプリケーション間の無制限なローカル接続 (127.0.0.1 インターフェース [ローカルホスト] への送受信) を許可するには **ループバックインターフェースを許可** を有効にしてください。このオプションは、接続がルールに一致していることが確認された後に適用されます。ネットワーク経由で行われる接続、およびコンピューター内で行われる接続の両方に対してルールを適用したい場合はチェックを外してください。



動作モードを選択する

以下の動作モードの内いずれかを選択してください。

動作モード	説明
信頼できるアプリケーションへの接続を許可する	<p>デフォルトではこのモードが適用されます。</p> <p>このモードでは、すべての信頼できるアプリケーションに対し、インターネットなどのネットワークリソースへのアクセスが許可されます。信頼できるアプリケーションには、システムアプリケーション、Microsoft証明書を持ったアプリケーション、有効なデジタル署名を持ったアプリケーションなどがあります。そのようなアプリケーションに対するルールはルールリストに表示されません。他のアプリケーションに対しては、Firewall では未知の接続を手動で許可またはブロックし、新しいルールを作成 するようプロンプトを出します。</p> <p>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、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。</p>
未知の接続を許可	<p>このモードでは、未知のアプリケーションからの、インターネットも含めたネットワークリソースへの接続が全て許可されます。Firewall は接続試行の検出に関する通知を表示しません。</p>
インタラクティブモード	<p>このモードでは、未知の接続を検出した際の Firewall の動作をユーザーによって完全に管理します。</p> <p>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、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。</p>
未知の接続をブロック	<p>このモードでは、Firewall は未知のアプリケーションからの、インターネットも含めたネットワークリソースへの接続をすべてブロックします。</p> <p>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、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を表示せずにアプリケーションのネットワーク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、指定されているアクションに従って接続を処理します。</p>



アプリケーションのパラメータ

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や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。また、アプリケーションによる他のプロセスの実行を有効／無効にすることが可能です。ルールは、システムおよびユーザーアプリケーションの両方に対して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。新しいフィルタリングルールを作成できるほか、既存のルールを編集または削除することができます。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特定されます。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。

プロセスに対してブロックルールが作成されている、または 未知の接続をブロック モードが設定されている状態で、ルールを無効にした、または動作モードを変更した場合、プロセスは次の接続試行までブロックされます。

アプリケーションルール

アプリケーションルール ウィンドウを開くには




1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. 開いたウィンドウで、ファイルとネットワーク タイルをクリックします。
3. Dr.Webが [管理者モード](#) で動作していることを確認してください(プログラムウィンドウ下部にあるロックが開いています )。管理者モードではない場合は、ロックをクリックします 。
4. **Firewall** タイルをクリックします。コンポーネントの設定ウィンドウが開きます。
5. **アプリケーションルール** セクションで、**変更** をクリックします。アプリケーションのリストが表示されたウィンドウが開きます。これらのアプリケーションには、ルールが設定されています。



図44. アプリケーションルール

6. 新しいルールセットの作成または既存のルールセットの編集を開始するには、**(+)** をクリックするか、アプリケーションを選択して **(✎)** をクリックします。必要なルールを検索するには、**(🔍)** をクリックします。

アプリケーションがコンピューターから削除された場合でも、該当するルールは自動で削除されません。リストのショートカットメニュー内で **使用されていないルールを削除** をクリックし、手動で削除してください。

既存のルールセットの編集または新しいルールセットの作成

新しいアプリケーションルールセットを作成（またはルールセットの編集 <アプリケーション名>）ウィンドウで、ネットワークリソースへのアクセスを設定し、他のアプリケーションの起動を有効または無効にできます。

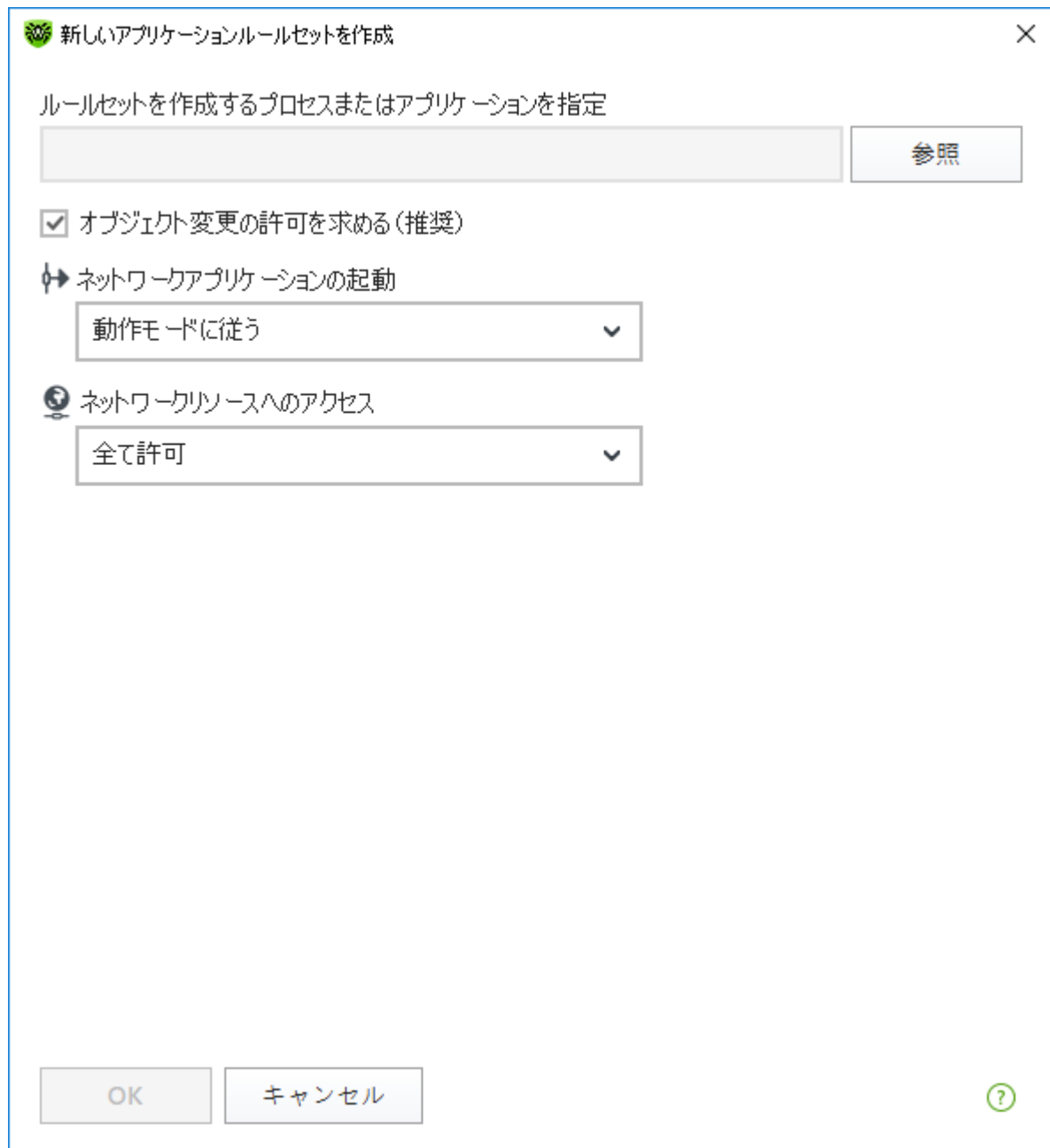


図 45. 新しいルールセットの作成

他のアプリケーションの起動

他のアプリケーションの起動を有効／無効にするには、**ネットワークアプリケーションの起動** ドロップダウンリスト内で次のうちいずれか1つを選択してください。

- **許可** - アプリケーションによる他のプロセスの起動を有効にします。
- **ブロック** - アプリケーションによる他のプロセスの起動を無効にします。
- **動作モードに従う** - Firewall の **動作モード** 内で指定された設定を使用します。



ネットワークリソースへのアクセス

1. ネットワークリソースにアクセスするためのモードを指定します。
 - 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。
 - 動作モードに従う - Firewall の **動作モード** 内で指定された設定を使用します。
 - ユーザー指定 - このモードでは、異なる接続ごとに許可／ブロックのルールセットを作成することができます。
2. ユーザー指定 モードを選択した場合、以下のアプリケーションルールセットの詳細が表に表示されます。

パラメータ	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 - 接続をブロックします。• パケットを許可 - 接続を許可します。
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 - 接続の方向に関係なくルールが適用されます。
説明	ルールの説明

3. 必要に応じ、既定のルールセットを編集、または新規のルールセットを作成してください。
4. 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** を行ってください。
5. 設定の調整が終わったら、**OK** をクリックして変更を保存するか、**キャンセル** をクリックして変更をキャンセルします。別のモードに移行すると、ルールセットで行われた全ての変更が保持されます。

アプリケーションが変更または更新されるたびにネットワークリソースへのアクセスを確認するには、**オブジェクト変更の許可を求める(推奨)** を有効にします。

Firewall通知ウィンドウからのアプリケーションルールの作成

Firewallがインタラクティブモードまたは 信頼できるアプリケーションへの接続を許可する 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。

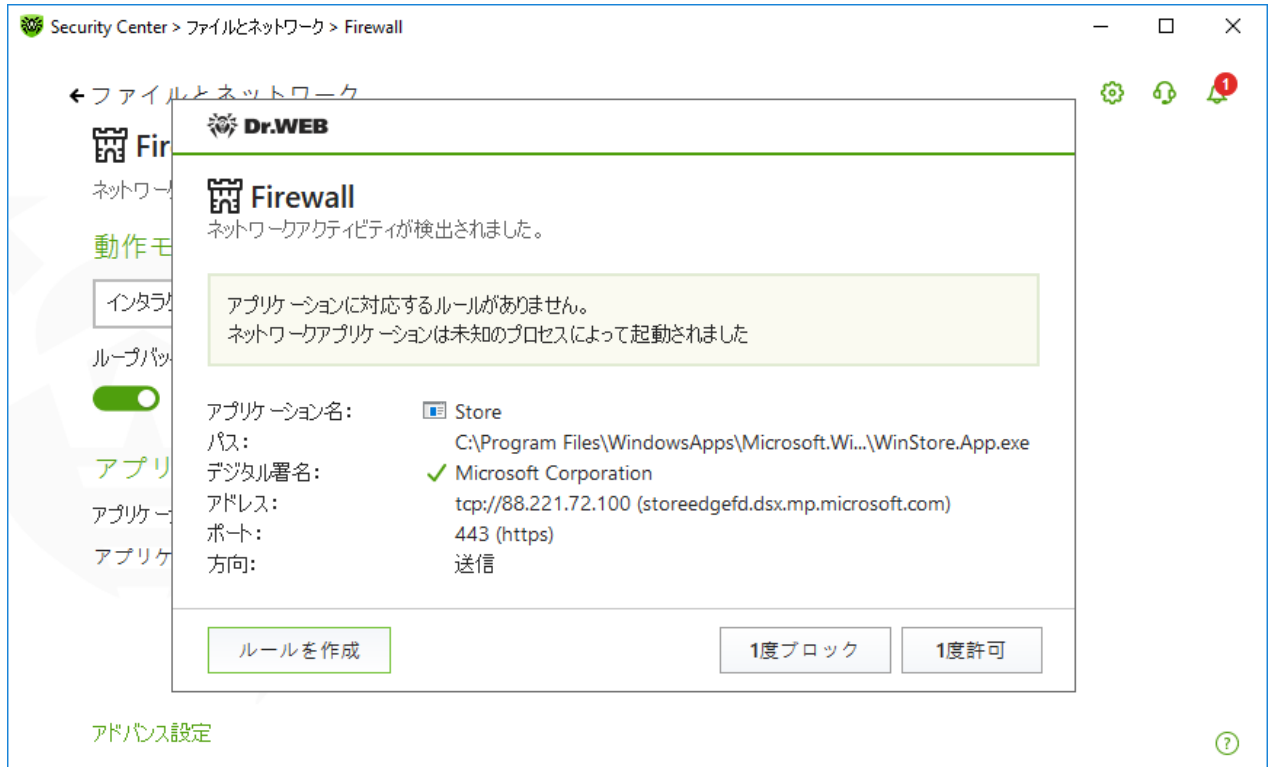


図46. ネットワーク接続試行の通知の例



制限付きユーザーアカウント(ゲスト)で動作している場合、Dr.Web Firewall はネットワークアクセスの試行に対する警告を表示しません。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、そのセッションに警告が表示されます。

アプリケーションの追加

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。

フィールド	説明
アプリケーション名	アプリケーション名。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ください。
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。

- このポートを使用したアプリケーションのアクセスを1回ブロックするには、**1度ブロック** を選択します。
- このポートを使用したアプリケーションのアクセスを1回許可するには、**1度許可** を選択します。



- 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 **ルールを作成** してください。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 **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** をクリックします。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。



Windowsオペレーティングシステムでは、システムプロセスとして機能するサービスを一意に識別することができない場合があります。システムプロセスによって接続試行が検出された場合は、接続に関する情報内に記載されたポートに注意してください。指定されたポートを使用してアクセスできるアプリケーションを使用している場合は、この接続を許可します。

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アプリケーション)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。
2. 実行するアクションを決定したら、次のうちいずれか一つを選択してください。
 - この接続を1回ブロックするには、**ブロック** を選択します。
 - この接続を許可するには、**許可** を選択します。
 - 親プロセスに対するルールを作成するには、**ルールを作成** をクリックし、開いたウィンドウ内で **必要な設定** を行ってください。
3. **OK** をクリックします。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。**ルールを作成** をクリックすると新しいウィンドウが開き、アプリケーションとその親プロセスに対して新しいルールを作成することができます。

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. ネットワークリソースへのアクセス セクションで **ユーザー指定** モードを選択します。
2. ルールセットの **編集** ウィンドウで、**(+)** ボタンを押して新しいルールを追加するか、リストからルールを選択し、**(P)** ボタンを押してルールを編集します。
3. 以下のパラメータを設定します：

パラメータ	説明
全般	
ルール名	作成／編集するルールの名前
説明	ルールの説明



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 - 接続をブロックします。• パケットを許可 - 接続を許可します。
ステータス	ルールのステータス： <ul style="list-style-type: none">• 有効 - 該当する全ての接続に対してルールが適用されます。• 無効 - ルールは適用されません。
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 - 接続の方向に関係なくルールが適用されます。
ログ	ロギングモード： <ul style="list-style-type: none">• 有効 - イベントのロギングを行います。• 無効 - ルールの情報をログに記録しません。
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プロトコルとトランスポートレベルプロトコルを指定します。 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 次のトランスポートレベル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• RAW
ローカル／リモートアドレス	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)に該当する複数の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と同じ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、全てを選択してください。
ローカルポート／リモートポート	接続に使用されるポート。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。



パラメータ	説明
	全てのポートに対してルールを適用するには、 全て を選択してください。

4. **OK** をクリックします。

ネットワークのパラメータ

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。Firewallは、コンピューター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。

そのためパケットフィルターでは、[アプリケーションフィルター](#) に比べてより包括的なネットワークへのアクセス管理を行うことができます。

パケットフィルター

ネットワーク ウィンドウでは、特定のインターフェースを介して送信されたパケットをフィルタリングするための一連のルールを作成できます。

ネットワーク ウィンドウを開くには




1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. 開いているウィンドウで、**ファイルとネットワーク セクション**を選択します。
3. Dr.Webが [管理者モード](#) で動作していることを確認してください(プログラムウィンドウ下部にあるロックが開いています )。管理者モードではない場合は、ロックをクリックします 。
4. **Firewall** タイルをクリックします。コンポーネントの設定ウィンドウが開きます。
5. **アドバンス設定** グループを展開します。
6. **アプリケーションルール** セクションで、**変更** をクリックします。ネットワークインターフェースの一覧が表示されたウィンドウが開きます。これらのネットワークインターフェースには、ルールが設定されています。




図47. ネットワークインターフェイスのルールセット

7. 必須インターフェイスには、適切なルールセットを選択します。適切なルールセットが存在しない場合は、[ルールを作成](#)できます。

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：

- デフォルトルール - このルールセットは、新しい [ネットワークインターフェイス](#) に対してデフォルトで使用されます。
- 全て許可 - 全てのパケットを通過させます。
- 全てブロック - 全てのパケットをブロックします。

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作成](#)することができます。

使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  をクリックし、全て表示 を選択します。開いたウィンドウ内で、常にリスト上に表示させるインターフェイスを指定することができます。アクティブなインターフェイスは自動的にリスト上に表示されます。

 をクリックすると、非アクティブなインターフェイスを削除できます。

インターフェイスパラメータにアクセスするには、インターフェイスの名前をクリックします。

パケットフィルターの設定

既存のルールセットを設定して新しいルールセットを追加するには、[ルールセット](#) ボタンをクリックして [パケットフィルターの設定](#) ウィンドウに移動します。



図48. パケットフィルターの設定

このページでは、以下の操作を行うことができます。

- 新しいルールを追加、既存のルールを変更、削除するなど、[フィルタリングのルールセット](#)を設定する。
- 高度な[フィルタリング設定](#)を行う。

ルールセットを設定する

次のいずれかを実行してください：

- ネットワークインターフェースの新しいルールセットを追加するには、 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、該当するルールセットをリスト上で選択し 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 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 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 ウィンドウでは、次のオプションを選択できます。

オプション	説明
動的パケットフィルタリングを有効にする	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 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



オプション	説明
	<p>(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ー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>
フラグメント化されたIPパケットを処理する	<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(フラグメント化)されたパケットのうちの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>

変更を保存するには **OK** をクリックします。変更を保存せずにウィンドウを閉じるには **キャンセル** をクリックします。

パケットフィルタリングのルールセット

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リング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。

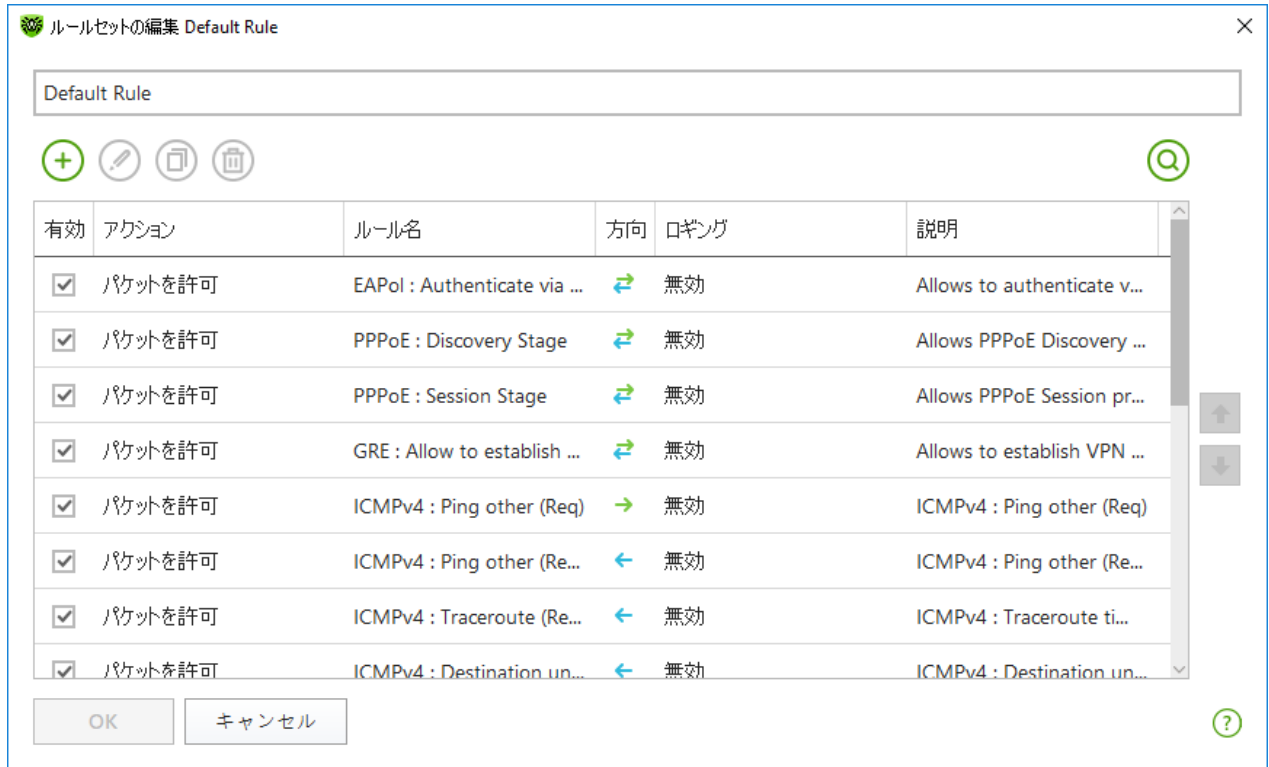







図 49. パケットフィルタリングのルールセット

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。

パラメータ	説明
有効	ルールのステータス
アクション	パケットの送受信を検出した際に 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 - パケットをブロックします。 ● パケットを許可 - パケットを許可します。
ルール名	ルールの名前
方向	接続の方向： <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ルールが適用されます。 ● ↔ - パケットの送信方向に関係なくルールが適用されます。
ロギング	ルールのロギングモード。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 - パケットの情報をログに記録しません。
説明	ルールの説明



ルールセットの編集と作成



1. 必要に応じ、ルールセット名を追加または編集してください。
2. フィルタリングルールを作成するには、次のオプションを使用します。
 - 新しいルールを追加するには、 をクリックします。新しいルールがリストの先頭に追加されます。
 - ルールを変更するには、ルールを選択して  をクリックします。
 - 選択したルールのコピーを追加するには、 をクリックします。選択したルールの前にコピーが追加されます。
 - 選択したルールを削除するには、 をクリックします。
 - 必要なルールを検索するには、 をクリックします。
3. ルールの作成または編集を選択した場合は、開いているウィンドウで **ルール設定を構成** します。
4. 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。
5. 編集が完了したら、**OK** をクリックして変更を保存します。変更をキャンセルするには **キャンセル** をクリックします。



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ー** 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。

フィルタリングルールの設定

ルールの追加と編集

1. パケットフィルタールールセットの作成または編集ウィンドウで  または  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:

説明:

アクション: ▼

方向: ▼

ログ: ▼

フィルタリング基準

フィルタリング基準をこのルールに追加することができます。

?

図 50. フィルタリングルールを追加する

2. 以下のパラメータを設定します：

パラメータ	説明
ルール名	作成／編集するルールの名前
説明	ルールの説明
アクション	パケットの送受信を検出した際に 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 - パケットをブロックします。● パケットを許可 - パケットを許可します。
方向	接続の方向： <ul style="list-style-type: none">● 受信 - 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 - コンピューター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。● 全て - 接続の方向に関係なくルールが適用されます。
ログ	ルールのロギングモード。Firewall のログに記録する情報を指定します。 <ul style="list-style-type: none">● パケット全体 - パケット全体をログに記録します。● ヘッダのみ - パケットのヘッダのみをログに記録します。● 無効 - パケットの情報をログに記録しません。

3. **基準を追加** をクリックすることで、必要に応じて、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のフィルタリング基準を追加することができます。**フィルタリング基準を追加** ウィンドウが開きます。

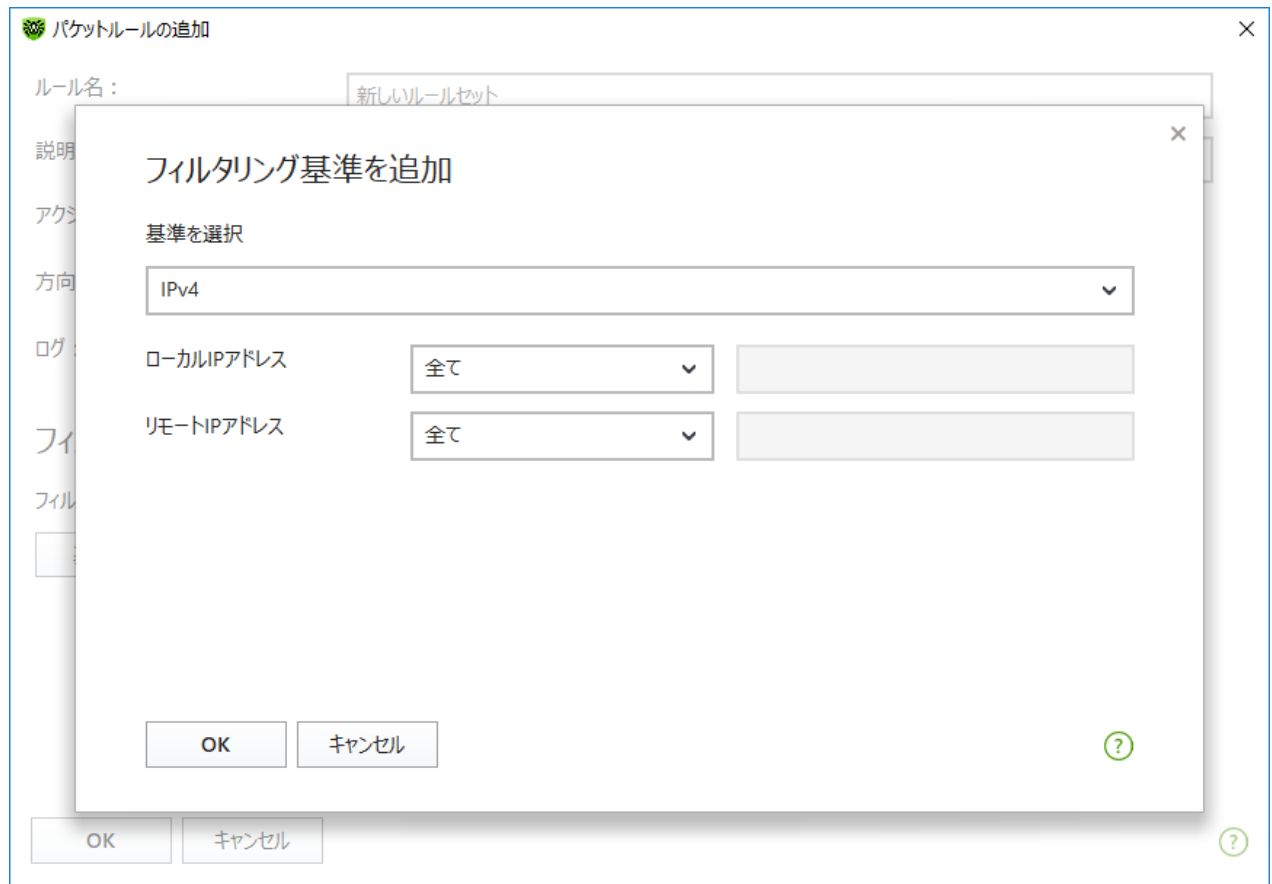


図 51. フィルタリング基準を追加

ドロップダウンリストから必要なフィルタリング基準を選択します。このウィンドウでは、選択した基準のパラメータを設定することもできます。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。ルールアクションがパケットに適用されるには、パケットがルールのすべての基準を満たしている必要があります。

また、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。追加されたすべての基準は、パケットルールの編集ウィンドウに表示され、変更することができます。

4. 編集が完了したら、**OK** をクリックして変更を保存します。変更を保存せずにウィンドウを閉じるには **キャンセル** をクリックします。



いずれの基準も指定しなかった場合、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。

ローカルIPアドレス および **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ーの物理アドレスから送信されたすべてのパケットに対してルールが適用されます。

8.5. コンピューターのスキャン

Scanner コンポーネントは、コンピューターのアンチウイルススキャンを実行します。Scanner は、ブートセクター、メモリー、複合オブジェクト(アーカイブ、コンテナ、メール)内にある個別のファイルやオブジェクトを検査します。デフォルトでは、Dr.Webはコンピューターのスキャン中にすべての **検出手法** を用います。



Scanner は悪意のあるオブジェクトを検出すると、ユーザーに対する通知のみを行います。すべての感染した、または疑わしいオブジェクトに関する情報はリストで表示され、そこで [必要なアクションを選択](#) することができます。検出されたすべての脅威に対してデフォルトのアクションを適用するか、または特定のオブジェクトに対して必要なアクションを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Scanner の [設定ウィンドウ](#) 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。検出された各脅威に対するカスタムのアクションはスキャンの完了後に設定することができますが、脅威の種類に応じた全般的なアクションはスキャン前に設定しておく必要があります。

以下も参照してください。

- [ファイルスキャンのオプション](#)
- [スキャンの開始とスキャンモード](#)
- [検出された脅威を駆除する](#)

8.5.1. スキャンの開始とスキャンモード

ファイルのスキャンを開始するには



Windows Vista、Windows Server 2003以降のOSを使用している場合、Scanner を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。それ以外の場合、管理者権限を持たないユーザーがアクセスすることのできないファイル（システムフォルダを含む）に対するスキャンは実行されません。

1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. 開いたウィンドウで、ファイルとネットワーク タイルをクリックし、次に **Scanner** タイルをクリックします。



スタート メニューからファイルスキャンを開始することもできます。そのためには、アプリケーショングループ **Dr.Web** を展開し、**Dr.Web Scanner** を選択します。

3. 必要なスキャンモードを選択します。
 - 重要なWindowsオブジェクトのみをスキャンするには **クイックスキャン** を選択します。
 - 論理ドライブおよびリムーバブルメディア上のファイルをスキャンするには **フルスキャン** を選択します。
 - 選択したオブジェクトのみをスキャンするには **カスタムスキャン** を選択します。Scannerウィンドウが開きません。



図 52. スキャンモードを選択する

現在のスキャン後にアクションを選択することもできます。その場合は、ウィンドウ下部にある該当するリンクをクリックしてください。このアクションは、[Scanner設定](#) で選択された動作に依存せず、一般設定にも影響しません。

4. スキャンが開始されます。スキャンを一時停止したい場合は **一時停止** を、停止したい場合は **中止** をクリックします。



一時停止 ボタンは、プロセスおよびRAMのスキャン中には使用できません。

スキャンが完了すると、Scanner は検出された脅威について通知し、脅威を **駆除** するよう勧めます。



特定のファイルまたはフォルダをスキャンするには

1. ファイルまたはフォルダのショートカットメニュー（デスクトップまたはWindowsエクスプローラで）を開きます。
2. **Dr.Web**でスキャン を選択します。ファイルまたはフォルダはデフォルト設定に従ってスキャンされます。

スキャンモード

スキャンモード	説明
クイックスキャン	このモードでは次のオブジェクトをスキャンします。 <ul style="list-style-type: none">• 全ディスク上のブートセクター• RAM• 起動ディスク上のルートディレクトリ



スキャンモード	説明
	<ul style="list-style-type: none">• Windowsシステムフォルダ• ユーザーのドキュメントフォルダ(マイドキュメント)• 一時ファイル• システム復元ポイント• ルートキット(スキャンが管理者権限で実行された場合) <div style="border: 1px solid #ccc; background-color: #e6f2e6; padding: 10px; margin-top: 10px;"> このモードでは、アーカイブおよびEメールファイルはスキャンされません。</div>
フルスキャン	このモードでは、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	このモードでは、任意のファイルやフォルダ、オブジェクト(フォルダおよびファイル、RAMブートセクターなどのオブジェクト)をスキャンすることができます。オブジェクトを選択するには  をクリックしてください。

8.5.2. 検出された脅威を駆除する

スキャンが完了すると、Scannerは検出された脅威について通知し、脅威を駆除するよう勧めます。



Dr.Web Scannerの [設定](#) ページの **スキャン後** の項目で **検出された脅威を駆除** または **検出された脅威を駆除してコンピューターをシャットダウン** を有効にした場合、脅威は自動的に駆除されます。



図 53. スキャン後のアクションを選択する

スキャン結果のリストには、次の情報が含まれています。

カラム	説明
ファイル名	このカラムには感染した、または疑わしいオブジェクトの名前が表示されます（ファイルが感染している場合はファイル名、ブートセクターが感染している場合は ブートセクター 、ハードドライブのMBRが感染している場合は マスターブートレコード ）。
脅威	Doctor Webの分類に応じた、ウイルスや ウイルスの亜種 の名前です。疑わしいオブジェクトに対しては、「感染の可能性がある」という示唆、およびヒューリスティックアナライザによる分類から推測されるウイルスの種類が表示されます。
アクション	Scannerの設定 に応じた、検出された脅威に対して推奨されるアクションです。選択した脅威にアクションを適用するには、ドロップダウンリストオプションを使用します。
パス	ファイルへのフルパス

リスト内のすべての脅威を駆除する

アクションは、**Scannerの設定** に従って脅威ごとに指定されます。リスト内で指定されているアクションを適用してすべての脅威を駆除するには、**駆除** をクリックします。

脅威のリストで指定されているアクションを変更するには

1. オブジェクトまたはオブジェクトのグループを選択します。
2. アクション 列 (カラム) でドロップダウンリストから必要なアクションを選択します。



3. **駆除** をクリックします。Scannerが表内の全ての脅威の駆除を開始します。

選択した脅威を駆除する

選択した脅威を個別に駆除することもできます。その場合は以下の手順を実行します。

1. オブジェクト、複数のオブジェクト (CTRLキーを押す) またはオブジェクトのグループを選択します。
2. ショートカットメニューを開き、必要なアクションを選択します。Scannerは選択した脅威の駆除を開始します。

脅威駆除の制限

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。
- アーカイブやインストールパッケージ内のファイル、メールに添付されたファイルに対してはいかなるアクションも行うことができません。アクションはファイル全体に適用されます。

Scannerレポート

Dr.Web Scanner の動作に関する詳細なログが %USERPROFILE%\Doctor Web フォルダ内にある `dwscanner.log` ファイルに保存されます。

8.5.3. 追加設定

このセクションでは、追加のScannerオプションについて説明します。

- [コマンドラインモードでのスキャン](#)
- [Console Scanner](#)

コマンドラインモードでのスキャン

Scannerはコマンドラインモードで実行できます。これにより、現在のスキャンセッションの設定とスキャン対象のオブジェクトのリストを追加のパラメータとして指定できます。

スキャンを実行するコマンドラインは次のようになります。

```
[ <path_to_program> ] dwscanner [ <switches> ] [ <objects> ]
```

スイッチは、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。スイッチ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。スイッチはスラッシュ (/) 記号で始まり、空白で区切られます。

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。オブジェクトへのパスが指定されなかった場合、Dr.Web インストールフォルダ内で検索されます。



以下は、スキャンの対象となるオブジェクトを指定する際に最もよく使用される例です。

- /FAST - システムの **クイックスキャン** を実行します。
- /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の基本的なスキャンを実行します。また、ルートキットスキャンを実行します。

Console Scanner

Dr.Web には、コマンドラインからのスキャンや、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(設定を行うことで、隔離に移すことが可能です)。

Console Scannerを起動するコマンドラインは次のようになります。

```
[ <path_to_program> ] dwscancl [ <switches> ] [ <objects> ]
```

パラメータはスラッシュ (/) 記号で始まり、複数のパラメータは空白で区切られます。スキャンするオブジェクトは空のまま、または空白で区切って複数指定することができます。

使用可能なConsole Scannerスイッチの一覧は [付録 A](#) 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。
- 12 - Scanning Engine(スキャニングエンジン)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。

8.6. Dr.Web for Microsoft Outlook

主な機能

Dr.Web for Microsoft Outlookプラグインは以下の機能を実行します。

- 受信するメール添付ファイルのアンチウイルス検査
- スпам検査
- マルウェアの検出と駆除
- 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



Dr.Web for Microsoft Outlook プラグインの設定

プラグイン動作のパラメータ設定、および統計情報の確認はMicrosoft Outlookのメールアプリケーション内で行うことができます。ツール → オプション → **Dr.Web Anti-virus** ページ(Microsoft Outlook 2010の場合はファイル → オプション → アドイン セクションの Dr.Web for Microsoft Outlook を選択して アドイン オプション ボタンをクリック)を選択してください。



Microsoft Outlook パラメータの **Dr.Web Anti-Virus** ページは、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 ページでは、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。
- **添付ファイルの検査** - メールスキャンの設定、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。
- **アンチスパムフィルター** - スпамに対するプログラムのアクションを指定し、メールアドレスのブラックリストとホワイトリストを作成することができます。
- **統計** - スキャン済み、および処理済みオブジェクトの数を確認することができます。

8.6.1. ウイルススキャン

Dr.Web for Microsoft 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、または残りのシステムから遮断するために **隔離** へ移すことができます)。

Dr.Web for Microsoft Outlook は、次の悪意のあるオブジェクトを検出します。

- 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
- ハッキングツール
- 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

アクション

Dr.Web for Microsoft Outlookでは、メールの添付ファイル内の感染したファイル、疑わしいファイルや悪意のあるオブジェクトの検出に対するプログラムの処理(アクション)を指定できます。



メールの添付ファイルのウイルススキャンを設定し、検出された有害なオブジェクトのプログラム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で、ツール→ オプション→ **Dr.Web**アンチウイルス ページ (Microsoft Outlook 2010の場合は ファイル→ オプション→ アドイン セクションでDr.Web for Microsoft Outlookを選択して アドインオプション ボタンを選択)に移動し、**添付ファイル検査** をクリックします。



添付ファイル検査 ウィンドウは管理者権限を持つユーザーのみ使用可能です。

Windows Vista以降のOSでは **添付ファイルの検査** 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。

添付ファイル検査 ウィンドウで、スキャンされたオブジェクトのタイプごとのアクションやスキャンが失敗した場合のアクションを指定します。アーカイブのスキャンを有効または無効にすることもできます。

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、既知の修復可能な(と思われる)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、次のタイプの不要なソフトウェアの検出に対する反応を設定します。
 - アドウェア
 - ダイアラー
 - ジョークプログラム
 - ハッキングツール
 - リスクウェア
- **検査エラーの時** ドロップダウンリストでは、添付ファイルをスキャンできない場合、つまり添付ファイルが破損しているかパスワードで保護されている場合のアクションを設定できます。
- **アーカイブを検査する(推奨)** チェックボックスを使用すると、添付されたアーカイブファイルのスキャンを有効または無効にすることができます。スキャンを有効にするには、このチェックボックスをオンにします。スキャンを無効にするには、このチェックボックスをオフにします。

異なる種類のオブジェクトに対して、アクションが個別に割り当てられます。

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。
- **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。
- **無視** - 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。

8.6.2. スпам検査

Dr.Web for Microsoft Outlook は Dr.Web Anti-spam を使用してメールのスパムチェックを行い、ユーザーが指定した [設定](#) に従ってメールのフィルタリングを実行します。

スパム検査の設定を行うには、[ツール](#) → [オプション](#) ® **Dr.Web Anti-virus** ページに行き、(Microsoft Outlook 2010の場合は [ファイル](#) → [オプション](#) → [アドイン](#) セクションで Dr.Web for Microsoft Outlook を選択して [アドインオプション](#) ボタンをクリック) [アンチスパムフィルター](#) をクリックしてください。[アンチスパムフィルター](#) ウィンドウが開きます。



アンチスパムフィルター 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 [アンチスパムフィルター](#) 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。

Anti-Spamフィルターの設定

アンチスパムフィルターのパラメータを設定する

1. アンチスパムフィルターを有効にするには [スパム検査をする](#) チェックボックスにチェックを入れます。
2. [メールヘッダーにプレフィックスを加える](#) チェックボックスにチェックを入れると、スパムメールのヘッダーにテキストを追加することができます。追加するプレフィックステキストはチェックボックス右のフィールドで指定します。デフォルトでは ***SPAM*** です。
3. [検査済みメッセージをメッセージオプション内で開封済みにすることができます](#)。メールを開封済みにするチェックボックスにチェックを入れてください(デフォルトでチェックが入っています)。
4. [ホワイトリストとブラックリスト](#) を設定することもできます。



スパムフィルターによってメッセージが誤って判定された場合、解析のためにそのメッセージをアンチウイルスネットワーク管理者に送信してください。

ブラックリストとホワイトリスト

ブラックリストとホワイトリストは、メールのフィルタリングに使用されます。

ホワイトリストとブラックリストを参照・編集するには、[アンチスパムフィルターウィンドウ](#) 内でそれぞれ [ホワイトリスト](#) または [ブラックリスト](#) をクリックします。

ホワイトリストまたはブラックリストにアドレスを追加するには

1. [追加](#) をクリックします。
2. 該当するフィールドにメールアドレスを入力します。
3. [リストを編集](#) 内で **OK** をクリックします。



リスト内のアドレスを変更するには

1. 変更したいアドレスを選択し、**変更** をクリックします。
2. 必要な変更を加えます。
3. リストを編集 内で **OK** をクリックします。

アドレスをリストから削除するには

1. リストからアドレスを選択します。
2. **削除** をクリックします。

ブラックリストとホワイトリスト ウィンドウ で、**OK** をクリックして変更を保存してください。

ホワイトリスト

送信者のアドレスがホワイトリスト上にある場合、そのメールに対するスパムスキャンは行われません。詳細

- 特定の送信者を追加するには、メールアドレス全体を入力します (例: mail@example.net)。この送信者からのメールはすべて配信されます。
- リストには1つの項目につき1つのアドレス、またはアドレスのマスクを入力してください。
- 送信者アドレスのグループを追加する場合は、それらの名前を定義するマスクを入力します。このマスクにより、オブジェクト定義用のテンプレートを定義します。メールアドレスに使用される通常の文字および特別な * 記号を含むことができます。この記号は、任意の(空白を含む)シーケンスの任意の文字と置き換えられます。例えば、次のようなアドレスを使用することができます。

- mailbox@domain.com
- *box@domain.com
- mailbox@dom*
- *box@dom*



アスタリスク(*)を置くことができるのは、アドレスの先頭または末尾のみです。

@ 記号は必須です。

- ドメイン内のメールアドレスから送信されたメールをすべて配信するには、アドレス内でユーザー名の代わりにアスタリスク(*)を使用します。例えば、*@example.net と入力すると、SpIDer Mail は example.net ドメイン内のすべての送信者からのメールをスキャンせずに配信します。
- あらゆるドメイン内の特定のユーザー名のメールアドレスから送信されたメールを配信するには、アドレス内でドメイン名ではなくアスタリスクメールアドレス(*)を使用します。例えば、name@* と入力すると、SpIDer Mail はメールボックス名が name であるすべての送信者からのメールをスキャンせずに配信します。

ブラックリスト

送信者のアドレスがブラックリスト上にある場合、メッセージは自動的にスパムと見なされます。詳細

- 特定の送信者を追加するには、メールアドレス全体を入力します (例: spam@spam.com)。このアドレスからのメールはすべて自動的にスパムと見なされます。



- リストには1つの項目につき1つのアドレス、またはアドレスのマスクを入力してください。
- 送信者アドレスのグループを追加する場合は、それらの名前を定義するマスクを入力します。このマスクにより、オブジェクト定義用のテンプレートを定義します。メールアドレスに使用される通常の文字および特別な * 記号を含むことができます。この記号は、任意の(空白を含む)シーケンスの任意の文字と置き換えられます。

例えば、次のようなアドレスを使用することができます。

- mailbox@domain.com
- *box@domain.com
- mailbox@dom*
- *box@dom*



アスタリスク(*)を置くことができるのは、アドレスの先頭または末尾のみです。

@ 記号は必須です。

- ドメイン内のメールアドレスから送信されたメールをすべてスパムとして処理するには、アドレス内でユーザー名の代わりにアスタリスク(*)を使用します。例えば、 *@spam.com と入力した場合、spam.com ドメイン内のすべての送信者からのメールをスパムとして処理します。
- あらゆるドメイン内の特定のユーザー名のメールアドレスから送信されたメールをスパムとして処理するには、アドレス内でドメイン名の代わりにアスタリスク(*)を使用します。例えば、name@* と入力すると、SpIDer Mail は、メールボックス名が name であるすべての送信者からのメールをスパムとして処理します。

8.6.3. イベントのロギング

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

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

イベントログ

Windows Event Logには以下の情報が記録されます。

- プログラムの起動と停止
- 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

イベントログを表示するには

1. OSの コントロールパネル を開きます。
2. 管理ツール→イベントビューア を選択してください。
3. 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ファイルに登録されたイベントの一覧が表示されます。Dr.Web for Microsoft Outlook メールソースは Dr.Web for Microsoft Outlook アプリケーションになっています。



デバッグテキストログ

デバッグログには以下の情報が記録されます。

- 脅威の検出に関する情報
- 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、ウイルスデータベース)
- コア障害

プログラムのロギングを設定するには

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. 最も詳細なレベルでロギングを行うには **詳細なロギング** にチェックを入れてください。デフォルトでは標準モードになっています。



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 Microsoft 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。

3. **OK** をクリックして変更を保存してください。



ログ 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 **ログ** 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。

テキストログを開くには

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. フォルダ内に**表示** をクリックします。ログを含んだフォルダが開きます。

8.6.4. 統計

Microsoft Outlookメールアプリケーション内で **ツール** → **オプション** → **Dr.Web Anti-virus** ページ (Microsoft Outlook 2010の場合は **ファイル** → **オプション** → **アドイン** セクションの **Dr.Web for Microsoft 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に関する統計情報を一覧で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に分類されます。

- **検査済** - 検査されたオブジェクトやメールの総数
- **感染** - 感染しているメール添付オブジェクトの総数
- **疑わしい** - ウイルスに感染していると思われる(ヒューリスティック解析によって)メールの数



- 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 - 感染していないオブジェクトやメールの数

以下のアクションが適用されたオブジェクトの数が表示されます。

- 隔離済 - 隔離へ移されたオブジェクトの数
- 削除済 - システムから削除されたオブジェクトの数
- 無視 - 変更せずにスキップされたオブジェクトの数
- スпамメール - スпамとして検出されたオブジェクトの数

デフォルトでは、統計情報は %USERPROFILE%\Doctor Web フォルダ内の drwebforoutlook.log ファイルに保存されます。



統計はセッション中に蓄積され、コンピューターまたは Dr.Web Agent for Windows が再起動された場合はゼロにリセットされます。

9. 予防的保護(Preventive Protection)

このグループでは、コンピューターのセキュリティを危険にさらす他のプログラムの動作に対するDr.Webのアクションを設定し、エクスプロイトに対する保護レベルを選択できます。

Preventive Protection 設定グループを開くには

1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. 開いたウィンドウで、**Preventive Protection** タイルをクリックします。





図54. Preventive Protection ウィンドウ

Preventive Protectionを有効または無効にする

スイッチ  を使用して、予防的保護を有効または無効にします。

コンポーネントの設定を開くには

1. Dr.Webが [管理者モード](#) で動作していることを確認してください(プログラムウィンドウ下部にあるロックが開いています )。管理者モードではない場合は、ロックをクリックします 。
2. 必要なコンポーネントのタイルをクリックします。




Preventive Protectionの有効化／無効化やコンポーネント設定の変更を行うことができるのは、Dr.Webが接続されている集中管理サーバー上で管理者によって該当するオプションが有効化されている場合のみです。



このセクションでは以下の設定を行うことができます。

- [Behavior Analysis](#) - システムオブジェクトへのアプリケーションアクセスを設定します。
- [Ransomware Protection](#) - ユーザーファイルの暗号化を防止します。
- [Exploit Prevention](#) - アプリケーションの脆弱性の悪用をブロックします。






Preventive Protectionを無効にするには、Dr.Webを管理者モードで実行する必要があります。そのためには、プログラムウィンドウの下部にあるロック  をクリックします。

9.1. ランサムウェア保護 (Ransomware Protection)

Ransomware Protectionにより、既知のアルゴリズムを使用してユーザーファイルを暗号化しようとするプロセスをセキュリティ上の脅威として検出することができます。ランサムウェアは、このようなプロセスの1つです。コンピューター上に侵入すると、このような悪意のあるプログラムはユーザーデータへのアクセスをブロックし、それを解除するための身代金を要求します。これらのプログラムは最も多く拡散されている悪意のあるプログラムの1つであると考えられ、企業と一般ユーザーの両方に大きな損害をもたらしています。主要な感染経路は、大量送信されるメールに含まれた悪意のあるファイルやマルウェアへのリンクです。

Doctor Webの統計では、暗号化ランサムウェアによって暗号化されたファイルを復元できる可能性はわずか10%となっています。そのため、ランサムウェアに対抗する最も効果的な方法は、感染を防ぐことであるといえます。ランサムウェアに感染するユーザーの数は減少傾向にありますが、Dr.Webのテクニカルサポートには毎月1000件にも及ぶ復号化のリクエストが寄せられています。

Ransomware Protection ウィンドウを開くには

1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. 開いたウィンドウで、**Preventive Protection** タイルをクリックします。
3. Dr.Webが [管理者モード](#) で動作していることを確認してください (プログラムウィンドウ下部にあるロックが開いています )。管理者モードではない場合は、ロックをクリックします 。
4. **Ransomware Protection** タイルをクリックします。



コンポーネント設定の変更を行うことができるのは、Dr.Webが接続されている集中管理サーバー上で管理者によって該当するオプションが有効化されている場合のみです。



図55. Ransomware Protection コンポーネントへのアクセス

このセクションでは以下の設定を行うことができます。

- [ファイルを暗号化しようとするアプリケーションの動作に対するアクションの設定](#)
- [特定のアプリケーションに対する個別のルール](#)

ファイルを暗号化しようとするアプリケーションに対するDr.Webのアクション

Ransomware Protection のパラメータを設定するには

1. Dr.Webが **管理者モード** で動作していることを確認してください(プログラムウィンドウ下部にあるロックが開いています)。管理者モードではない場合は、ロックをクリックします 。
2. **Ransomware Protection** タイルをクリックします。コンポーネントの設定ウィンドウが開きます。
3. ドロップダウンメニューで、全てのアプリケーションに適用するアクションを選択します。

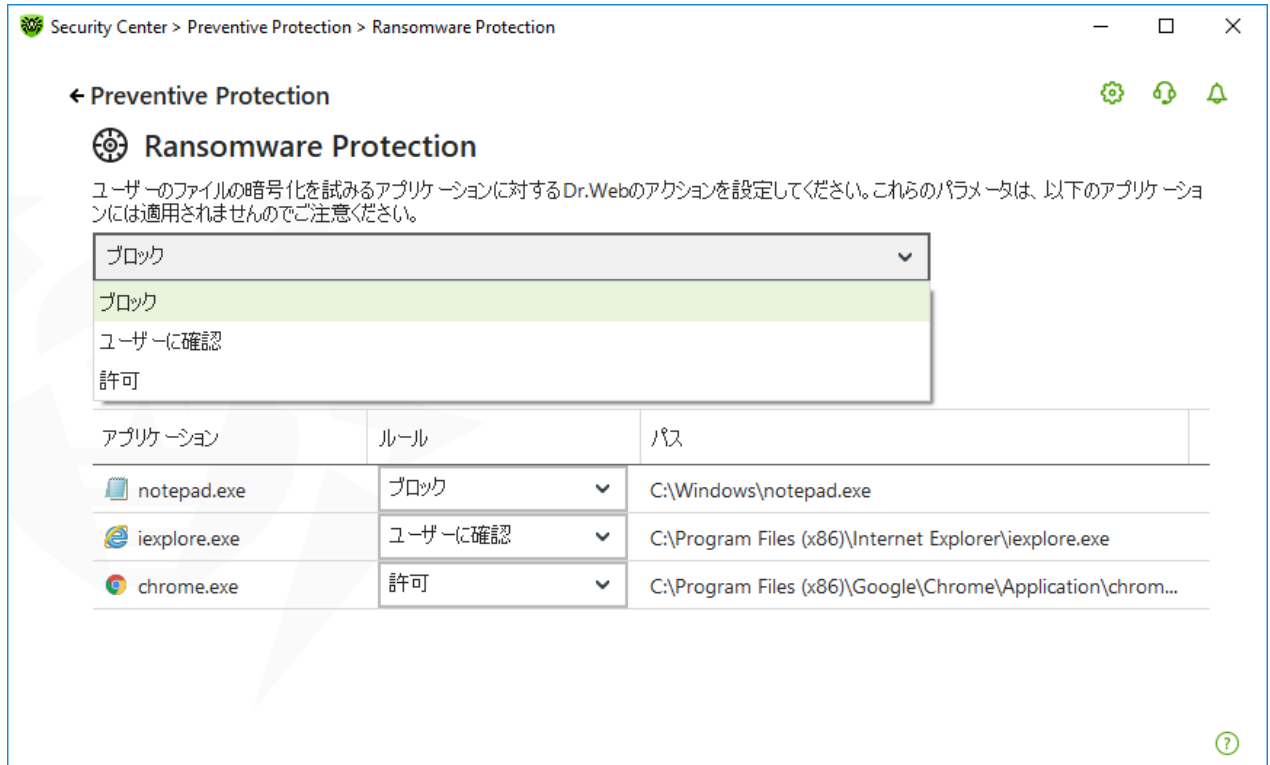


図56. Dr.Webのアクションを選択する

- 許可 - すべてのアプリケーションに対して、ユーザーのファイルを変更することを許可します。
- ブロック - 全てのアプリケーションに対して、ユーザーファイルを暗号化することを許可しません。このモードはデフォルトで有効になっています。アプリケーションがユーザーのファイルを暗号化しようとする時、以下の通知が表示されます。



図57. アプリケーションによるユーザーファイル変更の試みがブロックされた場合の通知の例

- ユーザーに確認 - アプリケーションがユーザーファイルを暗号化しようとした場合に通知が表示され、暗号化をブロックするか無視するかを選択することができます。



図58. アプリケーションがユーザーファイルを変更しようとした場合の通知例

- **修正** ボタンをクリックすると、プロセスはブロックされ、隔離されます。アプリケーションが隔離から復元された場合でも、コンピューターが再起動されるまでそのアプリケーションを起動することはできません。
- 通知ウィンドウを閉じた場合、アプリケーションは処理されません。

通知を受信する



必要に応じて、Ransomware Protectionのアクションに関する、デスクトップの通知を[設定](#)できます。

以下も参照してください。

- [通知](#)

特定のアプリケーションに対する個別のルール

特定のアプリケーションに対する Ransomware Protection のアクションを設定することができます。その場合、該当するアプリケーションをリストに追加し、コンポーネントのアクションを選択してください。リスト内のオブジェクトを操作するには、次の管理要素を使用できます。

-  ボタン - アプリケーションを個別のルールを持つアプリケーションのリストに追加します。
-  ボタン - アプリケーションを個別のルールを持つアプリケーションのリストから削除します。

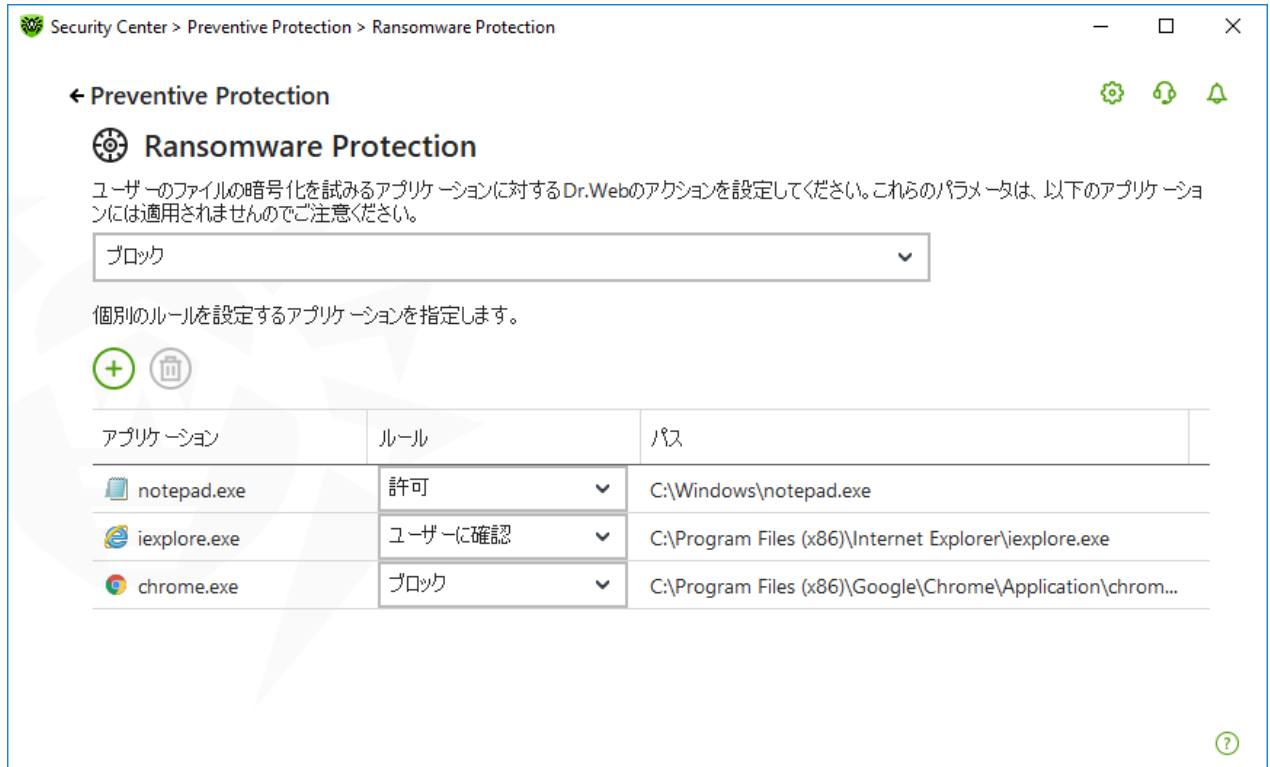


図59. コンポーネントの全般ルールに含まれないアプリケーション

アプリケーションをリストに追加するには

1. 。
2. 開いたウィンドウ内で **参照** をクリックし、アプリケーション実行ファイルへのパスを指定します。

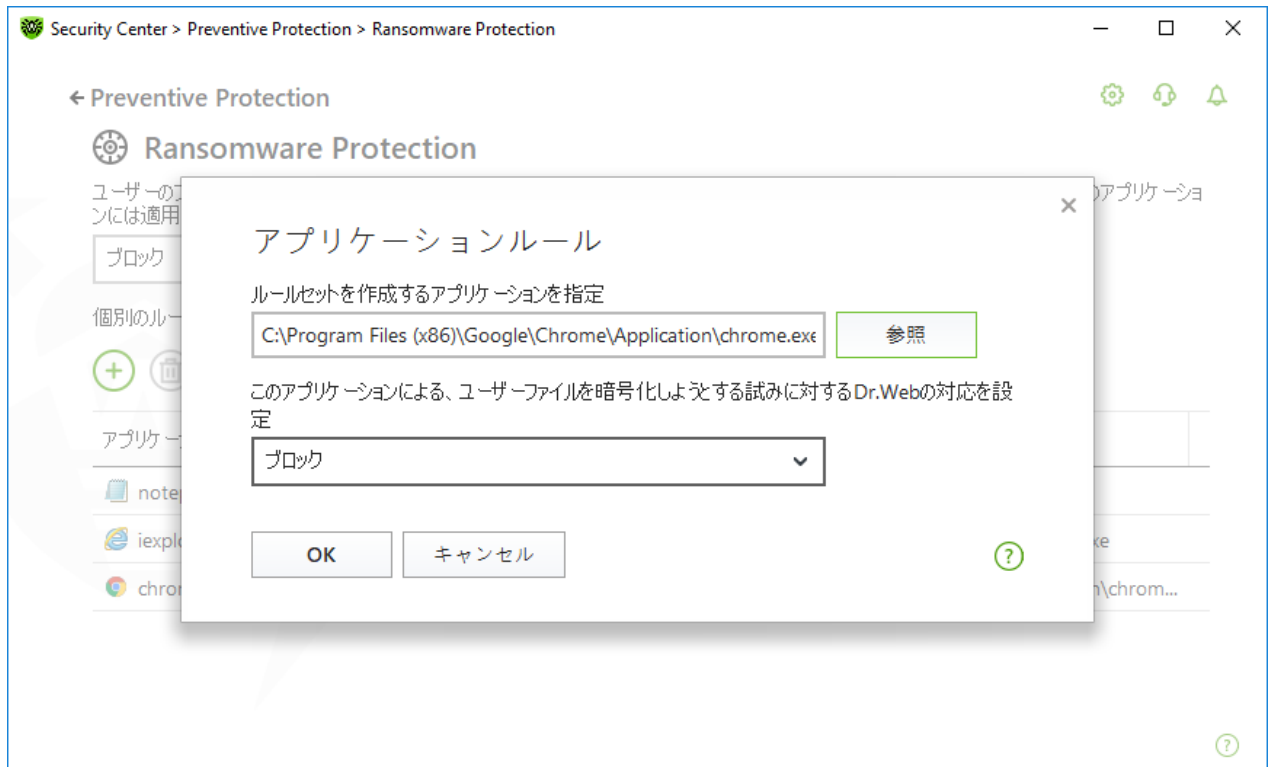


図60. 特定のアプリケーション用のルールを選択する



3. ドロップダウンリストから必要なコンポーネントのアクションを選択します。
4. **OK** をクリックします。

以前に選択したルールを変更することもできます。




ルールが設定されたアプリケーションに対するDr.Webのアクションを変更するには

1. Ransomware Protection コンポーネントの[メインウィンドウ](#)で、必要なアプリケーションを選択します。
2. ルール 列の該当する行で、ユーザーのファイルを暗号化しようとするアプリケーションに対するアクションをドロップダウンリストから選択します。

9.2. 動作解析 (Behavior Analysis)

Behavior Analysis を使用することで、お使いのコンピューターを感染させる可能性のあるサードパーティ製アプリケーションの動作 (HOSTSファイルや重要なシステムレジストリキーの変更など) に対するDr.Webの対応を設定することができます。Behavior Analysis が有効になっている場合、システムオブジェクトの自動変更がOSに対する悪意のある試みであることやOSに悪影響を与えるものであることが明らかであればDr.Webはそれらの変更をブロックします。Behavior Analysisは、従来のシグネチャベースの検出やヒューリスティック分析による検出を回避可能な、未知の悪意のあるプログラムからシステムを保護します。

Behavior Analysis ウィンドウにアクセスするには

1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. 開いたウィンドウで、**Preventive Protection** タイルをクリックします。
3. Dr.Webが [管理者モード](#) で動作していることを確認してください (プログラムウィンドウ下部にあるロックが開いています )。管理者モードではない場合は、ロックをクリックします 。
4. **Behavior Analysis** タイルをクリックします。



コンポーネント設定の変更を行うことができるのは、Dr.Webが接続されている集中管理サーバー上で管理者によって該当するオプションが有効化されている場合のみです。



図61. Behavior Analysis コンポーネントへのアクセス

このセクションでは以下の設定を行うことができます。

- [コンポーネントの動作モード](#)
- [必要なアプリケーションルールを作成、編集する](#)
- [保護されたオブジェクトの説明](#)

Behavior Analysisの設定

ほとんどの場合、デフォルト設定が最適です。必要がない限り変更しないでください。

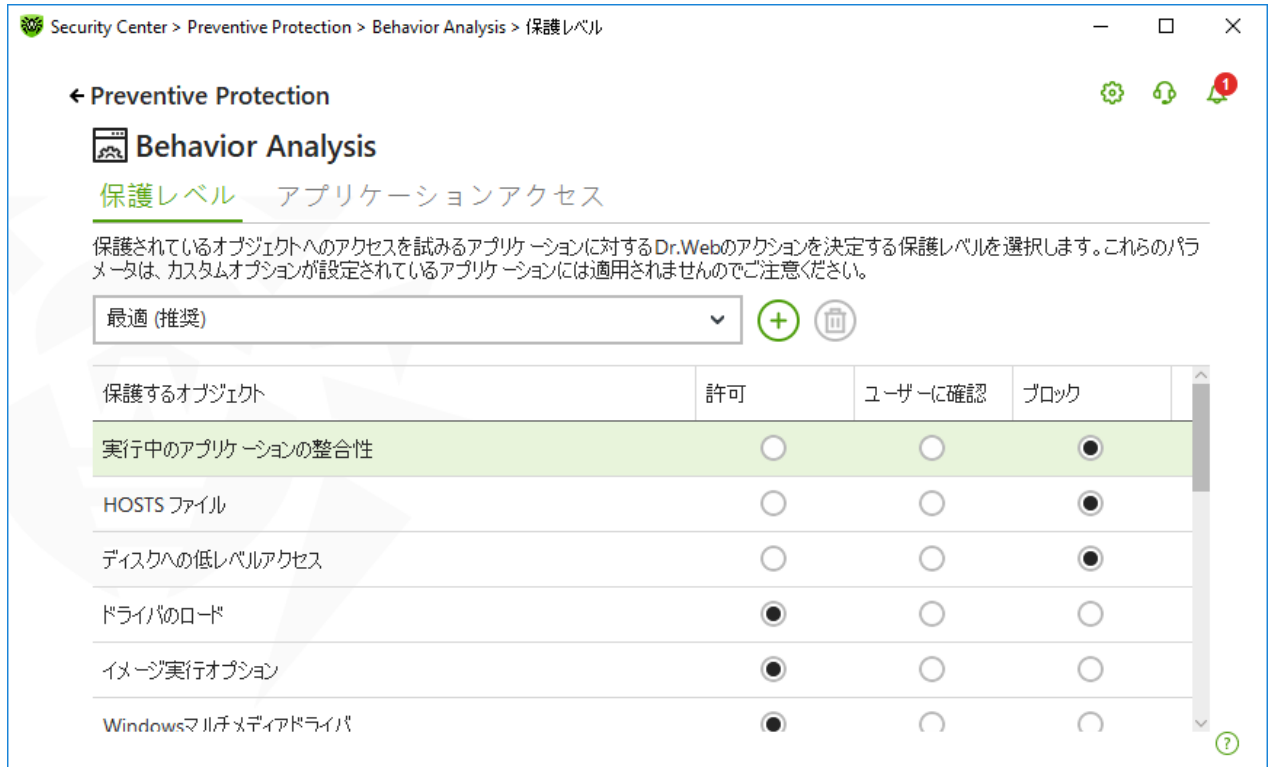


図62. Behavior Analysisの設定

特定のオブジェクトやプロセスに対して個別の保護レベルを設定したり、全てのプロセスに共通で適用される一般保護レベルを設定したりできます。一般保護レベルを設定するには、保護レベル タブのドロップダウンリストから選択します。

保護レベル

保護レベル	説明
最適 (推奨)	<p>オペレーティングシステムを破損させようという悪意のある意図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。オペレーティングシステムに悪影響を与える悪意のある試みであることが明らかであれば、ディスクへの低レベルのアプリケーションアクセスもブロックし、HOSTSファイルを変更から保護します。</p> <div style="border: 1px solid #ccc; padding: 5px; background-color: #e6f2e6;"> 信頼されていないアプリケーションによるアクションのみがブロックされます。 </div>
中	<p>コンピューターが感染する危険性が高い場合は、このモードを選択して保護を強化できます。このモードでは、悪意のあるソフトウェアによって使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がブロックされます。</p> <div style="border: 1px solid #ccc; padding: 5px; background-color: #e6f2e6;"> 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サードパーティ製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。 </div>

パラノイド	重要なWindowsオブジェクトへのアクセスを完全に制御する必要がある場合は、このモードを選択します。このモードでは、Dr.Webはドライバの読み込みとプログラムの自動実行をインタラクティブに制御します。
ユーザー指定	このモードでは、さまざまなオブジェクトにカスタム保護レベルを設定できます。

ユーザーモード

全ての変更はユーザーモードに保存されます。このウィンドウでは、必要な設定を保存するための新しい保護レベルを作成することもできます。保護されたオブジェクトは、全てのコンポーネント設定で読み取ることができます。

保護されたオブジェクトを変更するアプリケーションの試みに対するDr.Webのアクションを1つ選択できます。

- 許可 - 保護されたオブジェクトへのアクセスは、全てのアプリケーションで許可されます。
- ユーザーに確認 - アプリケーションが保護されたオブジェクトを変更しようとする時、通知が表示されます。




図63. 保護されたオブジェクトへのアクセス要求に関する通知の例

- ブロック - アプリケーションが保護されたオブジェクトを変更しようとする時、アクセスはブロックされます。この場合、通知が表示されます。



図64. 保護されたオブジェクトへのアクセスがブロックされた場合の通知の例


新しい保護レベルを作成するには

1. デフォルト設定を確認し、必要に応じて編集してください。
2.  ボタンをクリックします。



3. 開いたウィンドウ内で新しいプロファイルの名前を入力します。
4. **OK** をクリックします。

作成した保護レベルを削除するには

1. ドロップダウンメニューから、以前に作成された削除したいプロファイルを選択します。
2.  ボタンをクリックします。初期設定されているプロファイルは削除できません。
3. **OK** をクリックして削除を確定してください。

通知を受信する

必要に応じて、Behavior Analysisのアクションに関する、デスクトップの通知を**設定**できます。

以下も参照してください。

- [通知](#)

アプリケーションアクセス

特定のアプリケーションに対するカスタムアクセスパラメータを追加するには、**アプリケーションアクセス** タブに移動します。このタブでは、新しいアプリケーションルールを追加したり、既存のアプリケーションルールを編集または削除したりできます。

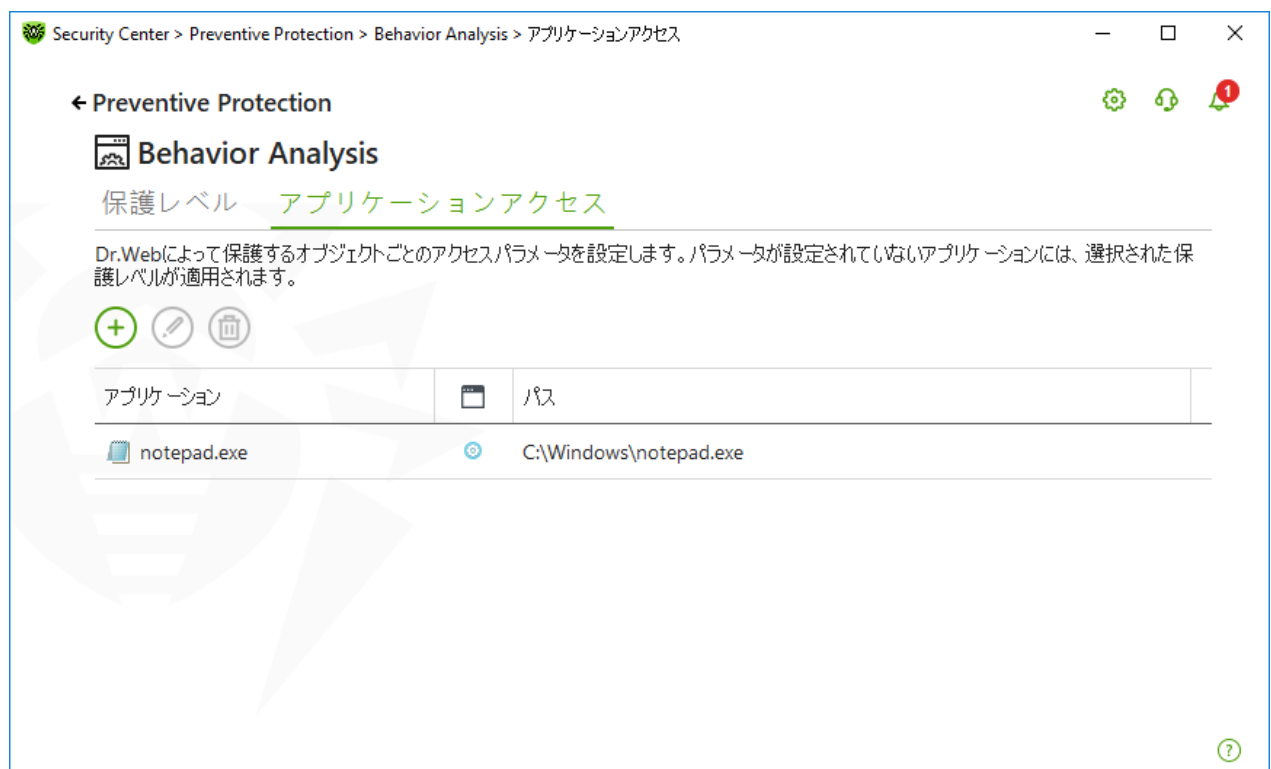


図65. アプリケーションアクセス設定

テーブル内のオブジェクトを操作するには、次の管理要素を使用できます。

-  ボタン - アプリケーションのルールセットを追加します。



- ボタン - 既存のルールセットを編集します。
- ボタン - ルールセットを削除します。

(ルールタイプ) 列には、3つのルールタイプが表示されます。

- - 全ての保護オブジェクトに対して全て許可ルールが設定されています。
- - 保護されたオブジェクトには異なるルールが設定されています。
- - 全ての保護オブジェクトに対して全てブロックが設定されています。

アプリケーションルールを追加するには

1. をクリックします。
2. 開いたウィンドウ内で **参照** をクリックし、アプリケーション実行ファイルへのパスを指定します。

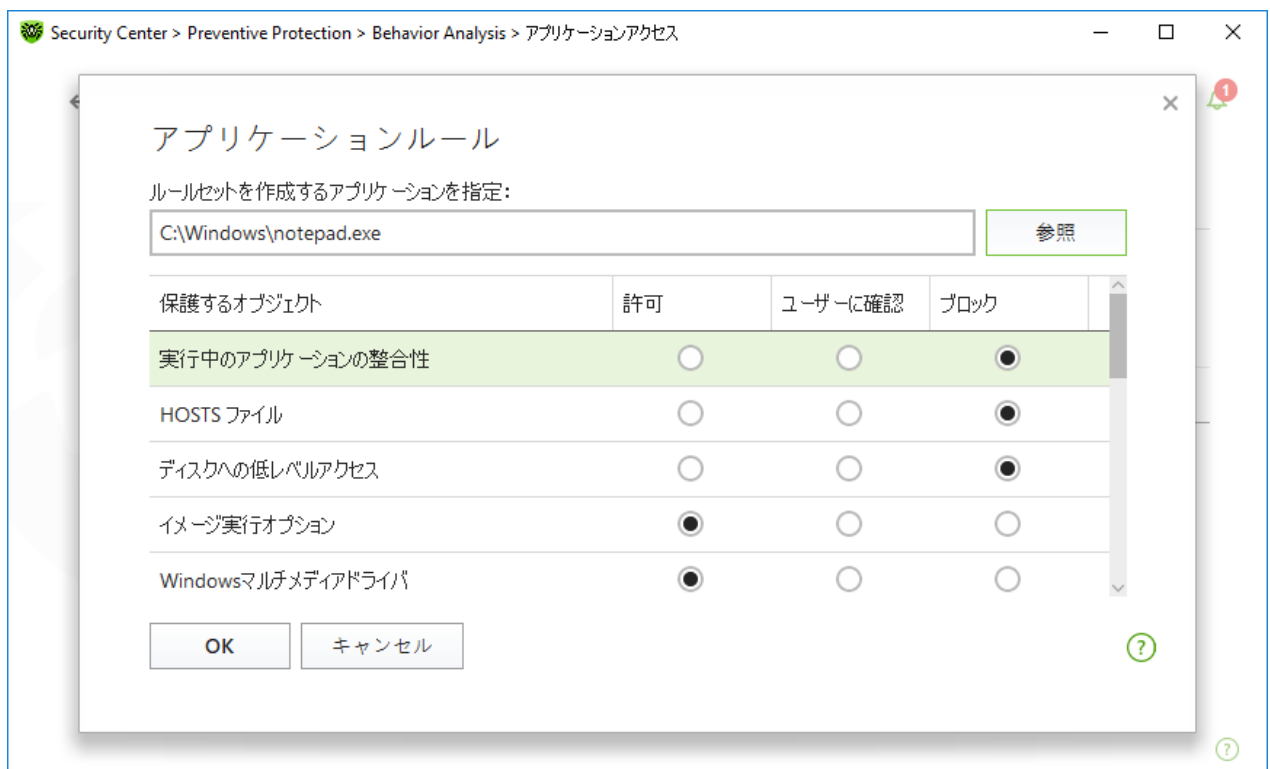


図66. アプリケーションのルールセットを追加する

3. デフォルト設定を確認し、必要に応じて編集してください。
4. **OK** をクリックします。

保護するオブジェクト

保護するオブジェクト	説明
実行中のアプリケーションの整合性	動作中のアプリケーションにコードを挿入するプロセスを検出します。このようなプロセスはコンピューターセキュリティを危険にさらす可能性があります。



保護するオブジェクト	説明
HOSTSファイル	OSはインターネットへの接続時にHOSTSファイルを使用します。このファイルに対する変更は、ウイルスに感染していることを示唆する場合があります。
ディスクへの低レベルアクセス	アプリケーションによるディスク上への、ファイルシステムを避けたセクタ単位の書き込みをブロックします。
ドライバーのロード	アプリケーションによる、新しいまたは未知のドライバのロードをブロックします。
重要なWindowsオブジェクト	<p>以下のレジストリブランチに対する変更をブロックします（全てのユーザープロファイルおよびシステムプロファイル内）。</p> <p>イメージ実行オプション</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options <p>Windowsマルチメディアドライバ :</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Drivers32• Software\Microsoft\Windows NT\CurrentVersion\Userinstallable.drivers <p>Winlogonの値 :</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL <p>Winlogonの通知 :</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify <p>Windowsシェルのオートラン :</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Windows, AppInit_DLLs, LoadAppInit_DLLs, Load, Run, IconServiceLib <p>実行ファイルの関連付け :</p> <ul style="list-style-type: none">• Software\Classes\.exe, .pif, .com, .bat, .cmd, .scr, .lnk (keys)• Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile (keys) <p>ソフトウェア制限ポリシー (SRP: Software Restriction Policies) :</p> <ul style="list-style-type: none">• Software\Policies\Microsoft\Windows\Safer <p>Internet Explorerのプラグイン (BHO) :</p> <ul style="list-style-type: none">• Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects <p>プログラムのオートラン :</p> <ul style="list-style-type: none">• Software\Microsoft\Windows\CurrentVersion\Run• Software\Microsoft\Windows\CurrentVersion\RunOnce• Software\Microsoft\Windows\CurrentVersion\RunOnceEx• Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup• Software\Microsoft\Windows\CurrentVersion\RunOnceEx\Setup• Software\Microsoft\Windows\CurrentVersion\RunServices



保護するオブジェクト	説明
	<ul style="list-style-type: none">• Software\Microsoft\Windows\CurrentVersion\RunServicesOnce ポリシーオートラン: <ul style="list-style-type: none">• Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run セーフモードの構成: <ul style="list-style-type: none">• SYSTEM\ControlSetXXX\Control\SafeBoot\Minimal• SYSTEM\ControlSetXXX\Control\SafeBoot\Network セッションマネージャーのパラメータ <ul style="list-style-type: none">• System\ControlSetXXX\Control\Session Manager\SubSystems, Windows システムサービス: <ul style="list-style-type: none">• System\CurrentControlSet\Services






Microsoft社による重要な更新のインストール、またはプログラム(デフラグツールを含む)のインストールや動作に問題が発生した場合は、Behavior Analysisを一時的に無効にします。

9.3. エクスプロイト防止(Exploit Prevention)

Exploit Prevention コンポーネントを使用すると、既知のアプリケーションの脆弱性を使用する悪意のあるプログラムをブロックできます。

Exploit Prevention 設定を開くには

1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. 開いたウィンドウで、**Preventive Protection** タイルをクリックします。
3. Dr.Webが [管理者モード](#) で動作していることを確認してください(プログラムウィンドウ下部にあるロックが開いています )。管理者モードではない場合は、ロックをクリックします 。
4. **Exploit Prevention** タイルをクリックします。コンポーネントの設定ウィンドウが開きます。



コンポーネント設定の変更を行うことができるのは、Dr.Webが接続されている集中管理サーバー上で管理者によって該当するオプションが有効化されている場合のみです。



図67. Exploit Prevention コンポーネントへのアクセス

コンポーネント設定ウィンドウの該当するドロップダウンリストで、エクスプロイトに対して必要な保護レベルを選択します。



図68. 保護レベルを選択する



保護レベル

保護レベル	説明
認証されていないコードの実行を防止	OSのクリティカルな領域にアクセスするために悪意のあるオブジェクトがソフトウェアの脆弱性を悪用しようとした場合に、それらを検知し、自動的にブロックします。
インタラクティブモード	OSのクリティカルな領域にアクセスするために悪意のあるオブジェクトがソフトウェアの脆弱性を悪用しようとした場合に、それらを検知し、該当するメッセージを表示させます。内容を確認後、適切なアクションを選択してください。
認証されていないコードの実行を許可	OSのクリティカルな領域にアクセスするために悪意のあるオブジェクトがソフトウェアの脆弱性を悪用しようとした場合に、それらを検知し、自動的に許可します。

通知を受信する

必要に応じて、Exploit Preventionのアクションに関する、デスクトップの通知を[設定](#)できます。

以下も参照してください。

- [通知](#)



10. デバイス

デバイス ウィンドウでは、特定のデバイスやバスへのアクセスを制限し、許可するデバイスリストを設定することができます。



デバイスのアクセス設定は、全てのWindowsアカウントに適用されます。

デバイス ウィンドウを開くには




1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. Dr.Webが [管理者モード](#) で動作していることを確認してください(プログラムウィンドウ下部にあるロックが開いています )。管理者モードではない場合は、ロックをクリックします 。
3. デバイス タイルをクリックします。



図 69. デバイス ウィンドウへのアクセス

このセクションでは以下の設定を行うことができます。

- [一般的なブロック設定](#)
- [デバイスクラスとバスのブロック](#)
- [許可するデバイスリストを設定](#)



一般的な設定

対応する設定を有効にすると、次のことができます。

- プリンタへのジョブの送信をブロックする。
- ローカルネットワークとインターネットを介したデータ転送をブロックする。

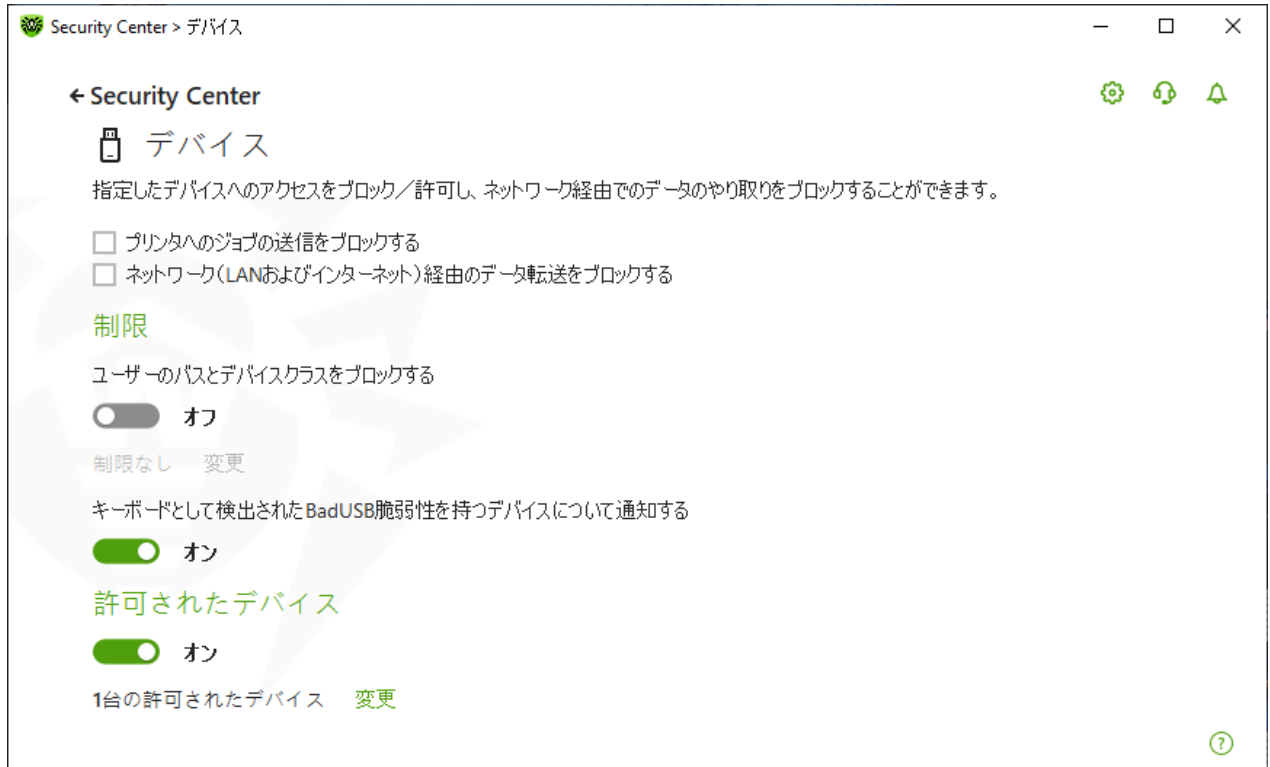


図 70. デバイスのブロック設定

全てのオプションは、デフォルトで無効になっています。




リムーバブルメディアをブロックする オプションは、2022年2月2日の製品コンポーネント更新前にこのオプションを有効にしていたユーザーのみが使用できます。このオプションを使用していなかった場合、または製品を初めてインストールする場合、リムーバブルメディア上のデータへのアクセスを防ぐには ユーザーのデバイスクラスとバスをブロック オプションを使用してください。

制限

デバイスのブロック設定

デバイスのブロック機能により、すべてのバス上の1つまたは複数のデバイスクラスをブロックし、1つまたは複数のバスに接続されているすべてのデバイスをブロックすることができます。デバイスクラスは、同じ機能を実行するすべてのデバイス群(たとえば、印刷デバイス)です。バスは、コンピューターの機能ユニット(たとえば、USB)間でデータを転送するための通信サブシステムです。

選択したデバイスクラスまたはバスへのアクセスをブロックするには

1. スイッチ  を使用して、ユーザーのデバイスクラスとバスをブロック オプションを有効にします。
2. **変更** リンクをクリックします。
3. 開いたウィンドウで、アクセスを制限する [デバイスクラスまたはバスを選択できます](#)。

BadUSBの脆弱なデバイスに関する通知

感染したUSBデバイスの中には、コンピューターがキーボードとして認識するものがあります。接続されたUSBデバイスがキーボードであるかどうかをDr.Webで確認するには、**キーボードとして検出されたBadUSB脆弱性を持つデバイスについて通知する** オプションを有効にします。このとき、キーボードが接続されている場合は、指定されたキーを押すように求められます。

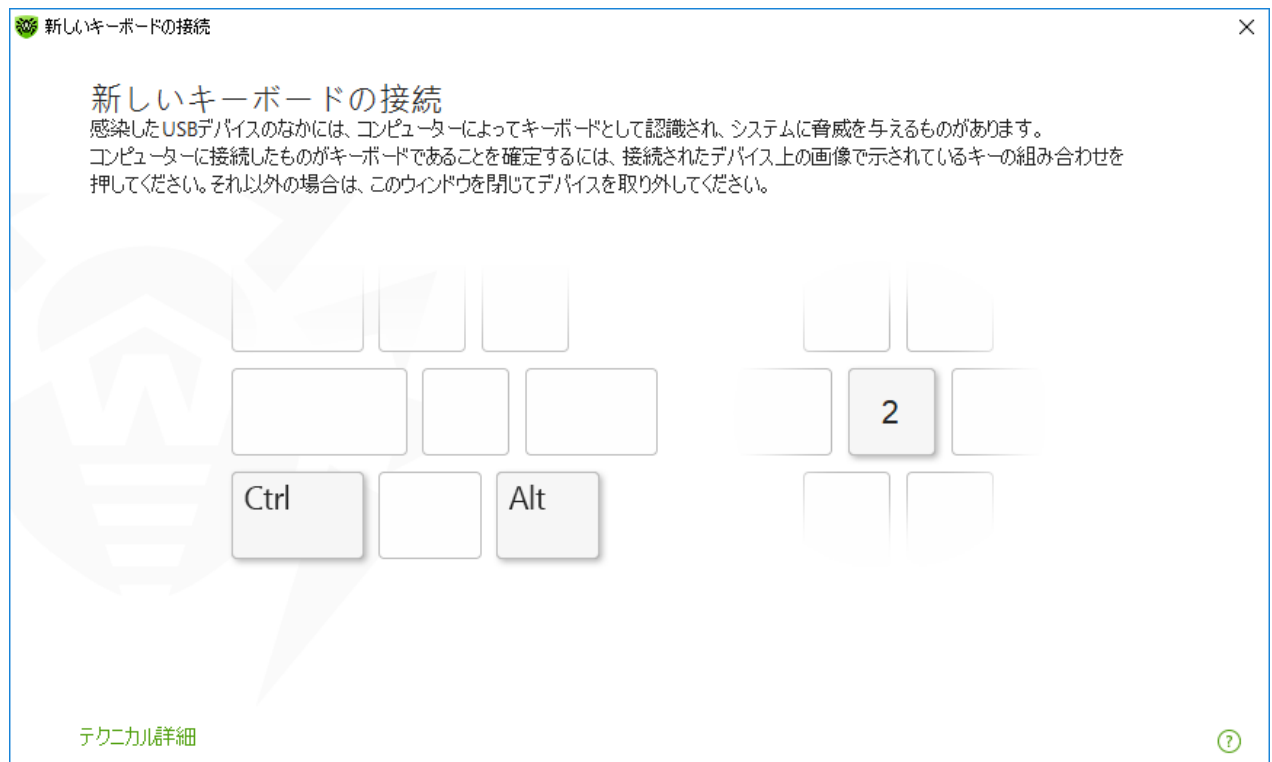



図 71. キーボードのブロック解除ウィンドウ

テクニカル詳細 リンクをクリックすると、デバイスに関する詳細情報のウィンドウが開きます。

許可するデバイス

バスまたはデバイスクラスへのアクセスをブロックした後、特定のデバイスを許可するデバイスリストに追加することで、そのデバイスへのアクセスを許可することができます。また、このリストにデバイスを追加することで、そのデバイスについてBadUSB脆弱性の有無をチェックすることもできます。

デバイスを許可するデバイスリストに追加する



1. スイッチ  を使用して、許可されたデバイス オプションを有効にします。
2. **変更** (このボタンは、いずれかの制限が設定されている場合に使用することができます) をクリックします。



3. 開いたウィンドウで、アクセス制限が適用されない [デバイスのリストを生成できます](#)。

10.1. バスとデバイスクラスのブロック

デバイスクラスとバス ウィンドウを開くには

1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. 開いたウィンドウで、**デバイス** タイルをクリックします。
3. **制限** 設定グループで、スイッチを使用して **ユーザーのデバイスクラスとバスをブロック** オプションを有効にします .
4. **変更** をクリックします。
5. 開いたウィンドウで、アクセスを制限するデバイスクラスまたはバスを選択できます。

このウィンドウには、ブロックされたバスやデバイスクラスに関する情報を含んだテーブルが表示されます。デフォルトでは、テーブルは空になっています。ブロックリストにバスまたはクラスを追加すると、それらがテーブルに表示されません。ブロックされたバスの行には、そのバス上のブロックされた全てのクラスが表示されます。





図72. ブロックされたクラス


ブロックされたクラス 列には、対応するバス上のブロックされたクラスの数が表示されます。複数のクラスがバス上でブロックされている場合は、ドロップダウンメニューとして表示されます。


全てのバスでブロックされたクラスはグレー表示されます。

テーブル内のオブジェクトを操作するには、次の管理要素を使用できます。


-  ボタン - ブロックリストにオブジェクトを追加します。
-  ボタン - テーブル内で選択したオブジェクトの設定を編集します。



-  ボタン - 選択したオブジェクトをブロックリストから削除します。

ブロックされたバスとブロックされたクラスに関する詳細情報を表示できます。これを行うには、必要な行を選択して  をクリックします。

バスのブロック

1. 特定のバス上の、バス全体または一部のデバイスをブロックするには、 をクリックします。
2. ドロップダウンメニューからブロックするオブジェクト(バス)を選択します。**次へ** をクリックします。

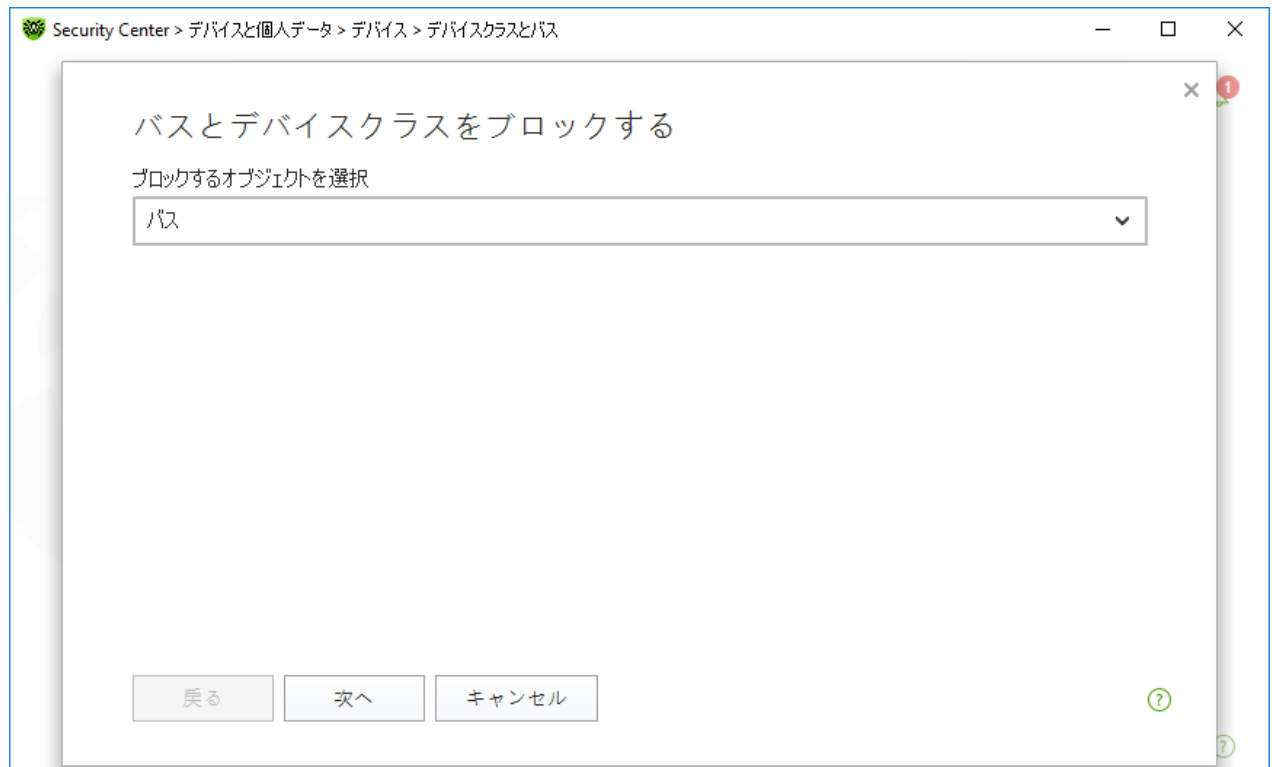


図73. ブロックするオブジェクトを選択する

3. バスのタイプを選択します。**次へ** をクリックします。

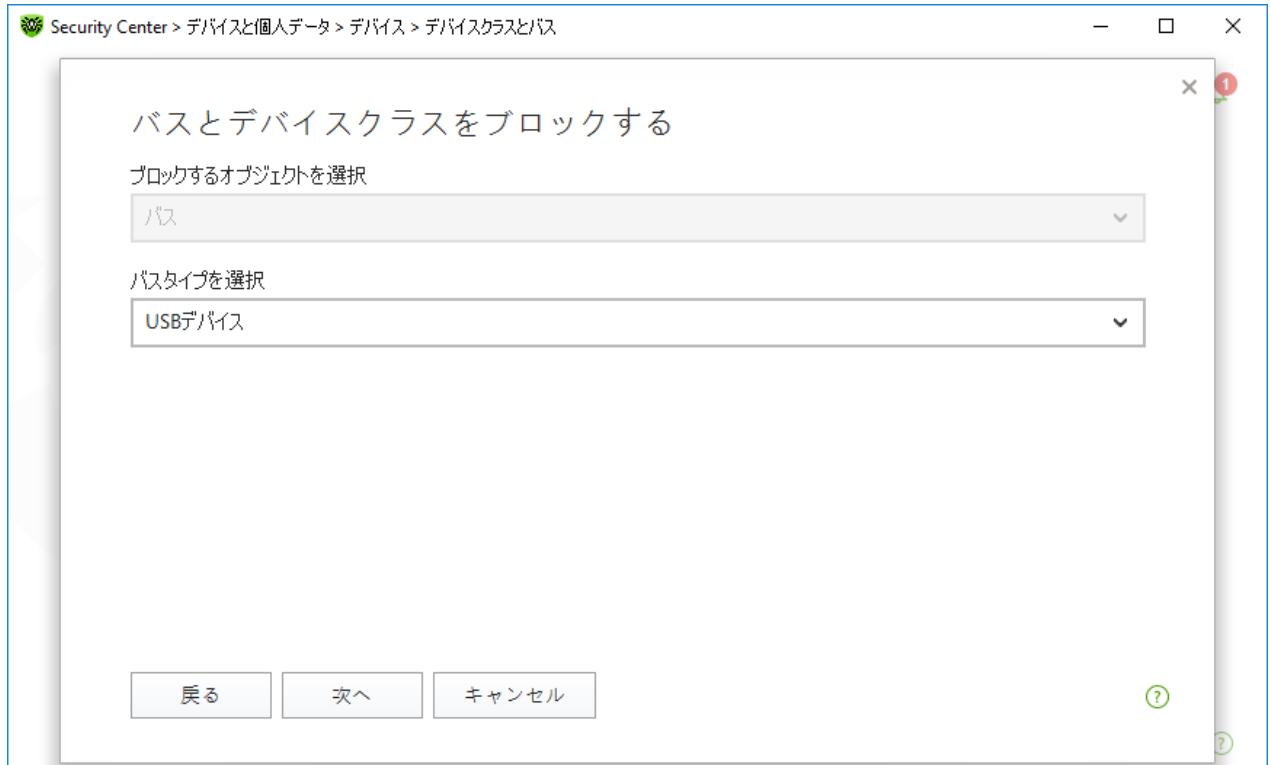


図74. バスのタイプを選択する

4. ブロックのタイプを選択し、**次へ** をクリックします。

- **全体** - 選択したバス上の全てのデバイスクラスをブロックします。
- **一部** - 選択したバスでブロックするデバイスクラスを選択できるウィンドウを開きます。

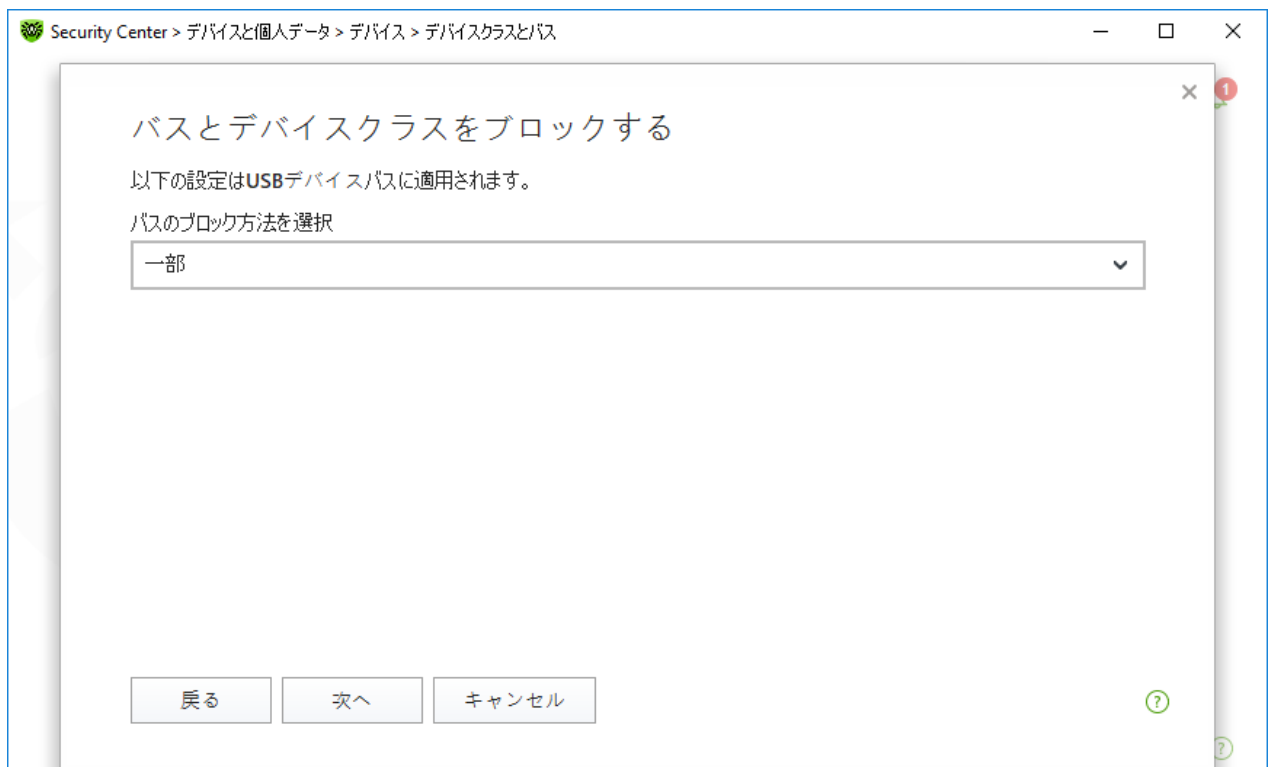


図75. バスのブロック方法を選択する



5. **一部** を選択した場合、開いたウィンドウのリスト上でブロックするクラスにチェックを入れます。**ブロック** をクリックします。

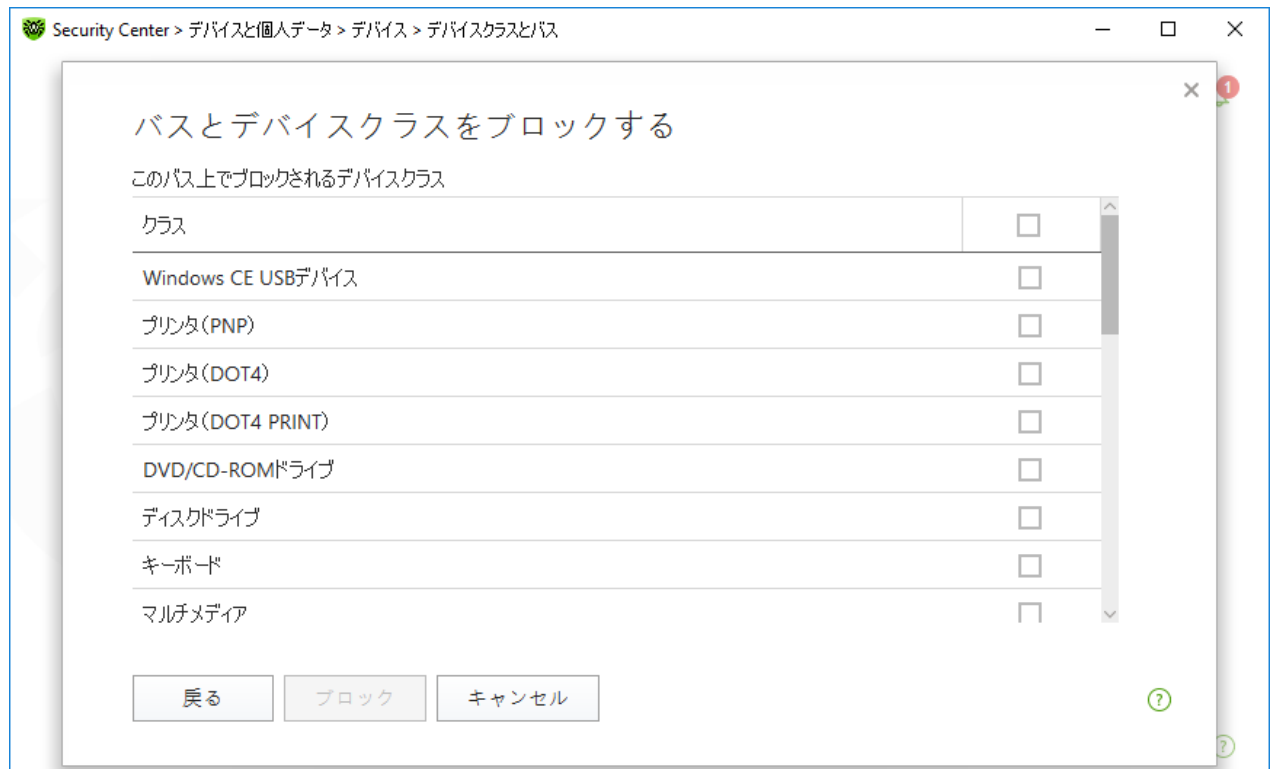


図76. バスのデバイスクラスを選択する

デバイスクラスのブロック

1. 1つまたは複数のクラスをブロックするには、**(+)** をクリックします。
2. ドロップダウンメニューで、ブロックするオブジェクト(クラス)を選択します。**次へ** をクリックします。

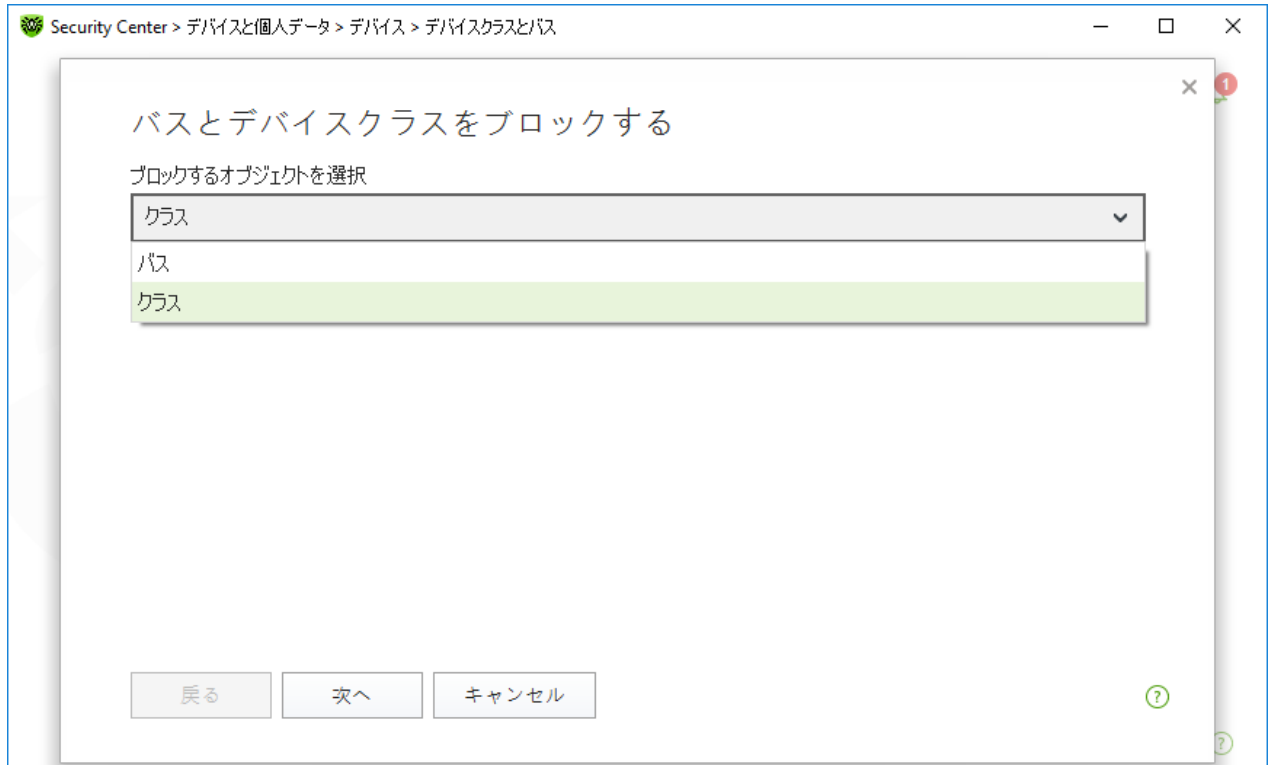


図77. ブロックするオブジェクトを選択する

3. リストの中から、ブロックするクラスをチェックします。ブロック をクリックします。



図78. デバイスクラスを選択する



機能を有効化する前に接続されたデバイスをブロックするには、デバイスを再接続するか、システムを再起動する必要があります。ブロック機能は、その有効化後に接続されたデバイスにのみ適



用されます。


USBバスをブロックすると、キーボードとマウスが除外に追加されます。

通知を受け取る

ブロックするデバイスでのポップアップ表示を[設定](#)できます。

10.2. 許可するデバイス

許可されたデバイス ウィンドウを開くには



1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. 開いたウィンドウで、**デバイス** タイルをクリックします。
3. 許可されたデバイス グループで、**変更** をクリックします。

許可されたデバイス ウィンドウには、許可するデバイスリストに追加されたすべてのデバイスに関する情報が含まれています。これらの情報はテーブルに表示されます。



図 79. 許可するデバイス

テーブル内のオブジェクトを操作するには、次の管理要素を使用できます。

-  ボタン - デバイスのルールセットを追加します。
-  ボタン - デバイスのルールセットを編集します。



- ボタン - デバイスのルールセットを削除します。

許可するデバイスリストに追加されたデバイスの詳細情報を表示できます。これを行うには、必要な行を選択して をクリックします。

⇨ (ルールタイプ) 列には、2つのルールタイプが表示されます。

- - 全て許可 ルールが設定されています。
- - 読み取り専用 ルールが設定されています。

デバイスを許可するデバイスリストに追加する

1. デバイスがコンピューターに接続されていることを確認してください。
2. をクリックします。開いたウィンドウ内で **参照** をクリックし、デバイスを選択してください。フィルターを使用することで、接続しているデバイスのみ、または接続されていないデバイスのみを表内に表示することができます。**OK** をクリックします。

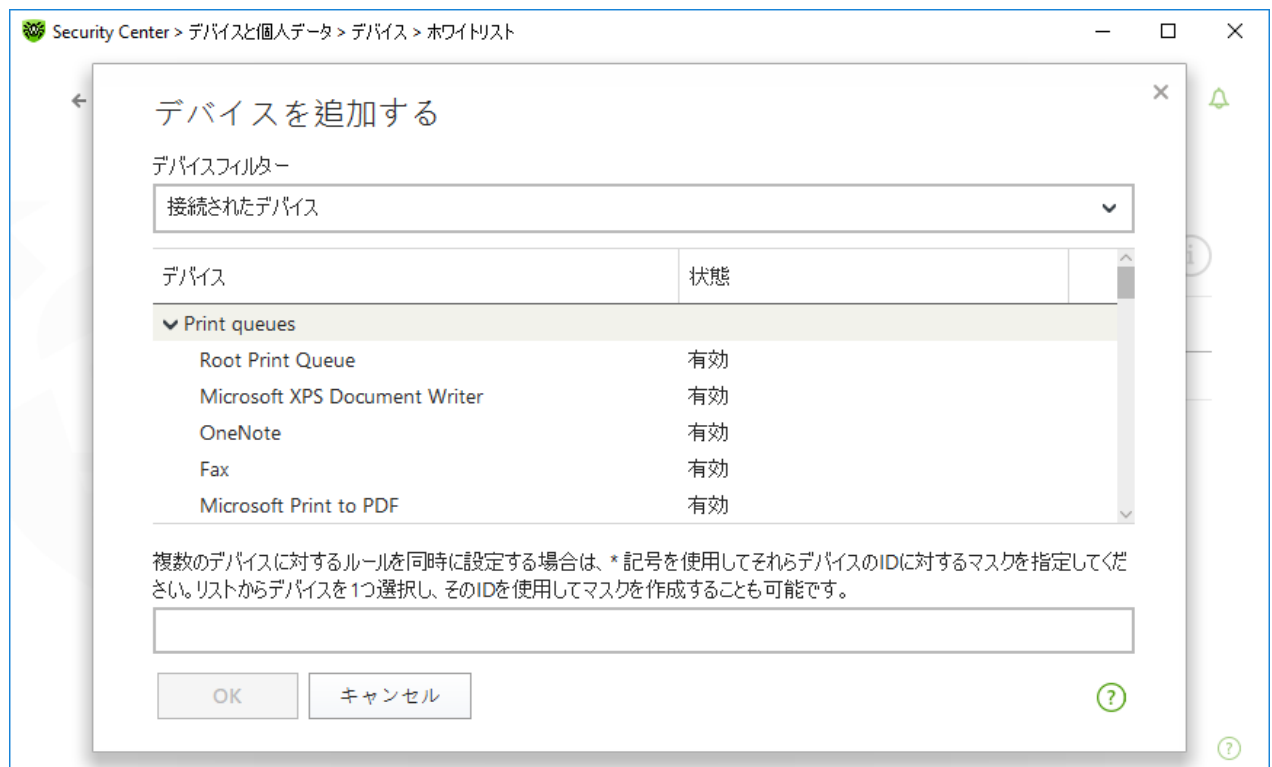


図 80. デバイスを許可するデバイスリストに追加する

3. ファイルシステムデバイスに対するアクセスのルールを作成することができます。ルール カラムで **全て許可** または **読み取り専用** モードのうちいずれか一つを選択してください。特定のユーザーに対して新しいルールを作成するには をクリックします。ルールを削除するには をクリックしてください。

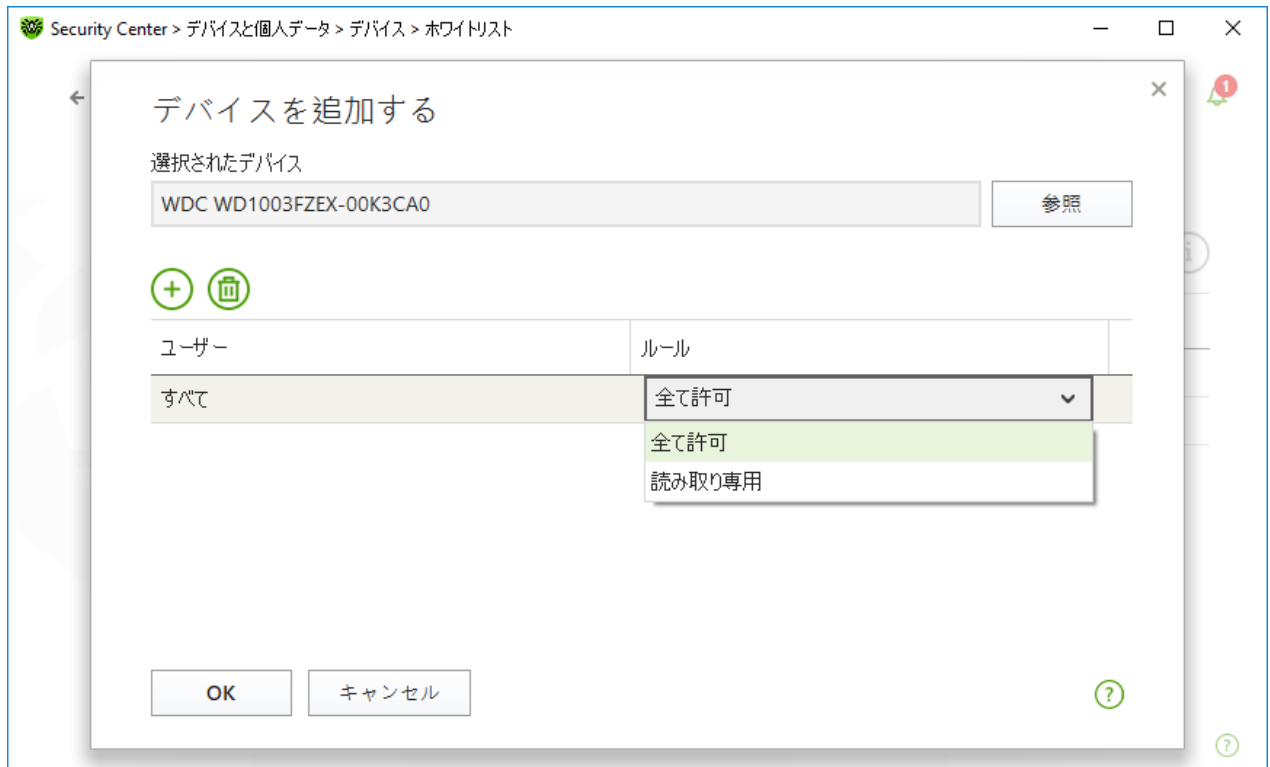


図81. 特定のユーザー用のルールを選択する

4. 変更を保存するには、**OK** をクリックします。変更を保存せずにウィンドウを閉じるには、**キャンセル** をクリックします。許可するデバイスリストに戻ります。

11. Office Control

Office Control コンポーネントによって、Webサイトやファイルおよびフォルダへのアクセスを管理することができます。また、インターネットとコンピューターの使用時間に制限を設けることもできます。

デフォルトでは、Office Controlは有効になっており、**制限なし** モードで動作します。

Office Controlを有効にするには





1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. 開いたウィンドウで、**Office Control** セクションを選択します。**Office Control** ウィンドウが開きます。



図 82. Office Control

3. Dr.Webが [管理者モード](#) で動作していることを確認してください(プログラムウィンドウ下部にあるロックが開いています )。管理者モードではない場合は、ロックをクリックします 。
4. 該当するスイッチ  を使用して、Office Controlを有効または無効にします。



新たに追加されたユーザーは、各アカウントの初回ログイン後にリストに表示されます。

特定のユーザーに対してOffice Controlを設定する

ユーザーに制限を設定する前に、そのユーザーが管理者権限を持っていないことを確認してください。管理者権限がある場合、ユーザーは Office Control コンポーネントの設定を変更し、アクセス制限を無効にすることができます。



コンポーネント設定の変更を行うことができるのは、Dr.Webが接続されている集中管理サーバー上で管理者によって該当するオプションが有効化されている場合のみです。

Office Control設定を開くには

1. Dr.Webが **管理者モード** で動作していることを確認してください(プログラムウィンドウ下部にあるロックが開いています)。管理者モードではない場合は、ロックをクリックします 。
2. Office Control ウィンドウ(図 [Office Control](#) を参照)で、Office Control を設定するユーザー名のタイトルをクリックします。選択したユーザーの Office Control 設定のウィンドウが開きます。



図 83. Office Controlを設定する

3. Office Controlを設定するための該当するタブを選択します。
 - **インターネット** - インターネットリソースへのアクセスを設定します。このタブでは、ユーザーが望ましくないWebサイト(暴力、ギャンブルなど)にアクセスすることを制限したり、特定のWebサイトへのアクセスのみを許可したりすることができます。[インターネットリソースへのアクセス](#) セクションを参照してください。
 - **時間** - コンピューターとインターネットへのアクセスを設定します。このタブでは、選択した時間帯や曜日にコンピューターとインターネットの使用時間制限を設定できます。[時間制限](#) セクションを参照してください。
 - **ファイルとフォルダ** - ファイルシステムへのアクセスを設定します。このタブでは、特定のファイルやフォルダ(ローカルドライブやリムーバブルメディア上の)へのアクセスを制限できます。[ファイルとフォルダへのアクセス](#) セクションを参照してください。



ユーザーのWindowsアカウントに管理者権限が付与されている場合は、その種類を「標準ユーザー」に変更する必要があります。



ユーザーアカウントの種類を変更する方法

Windows XP

1. スタートメニューで **コントロールパネル** をクリックし、**ユーザーアカウント** を選択します。
2. 変更するアカウントの種類を選択し、**アカウントの種類の変更** をクリックします。
3. ユーザーアカウントの種類に **制限付きのユーザーアカウント** を選択します。
4. **アカウントの種類の変更** をクリックして設定を保存します。

Windows VistaおよびWindows 7の場合

1. スタートメニューで **コントロールパネル** をクリックし、**ユーザーアカウント** を選択します。
2. アカウントの種類を変更するには、**別のアカウントの管理** をクリックします。
3. 変更するアカウントの種類を選択し、**アカウントの種類の変更** をクリックします。
4. ユーザーアカウントの種類に **標準ユーザー** を選択します。
5. **アカウントの種類の変更** をクリックして設定を保存します。

Windows 8の場合

1. **コントロールパネル** を開き、**ユーザーアカウントとファミリーセーフテ** を選択します。
2. **別のアカウントの管理** をクリックします。
3. 変更するアカウントの種類を選択し、**アカウントの種類の変更** をクリックします。
4. ユーザーアカウントの種類に **標準ユーザー** を選択します。
5. **アカウントの種類の変更** をクリックして設定を保存します。

Windows 8.1の場合

1. 画面の右下の角にマウスポインターを移動し、**設定** をクリックします。**PC設定の変更** をクリックします。
2. **アカウント** をクリックし、次に **その他のアカウント** をクリックします。
3. 変更するアカウントの種類を選択し、**アカウントの種類の変更** をクリックします。
4. ユーザーアカウントの種類に **標準ユーザー** を選択します。
5. **OK** をクリックします。

Windows 10の場合


1. **スタート** ボタンを選択し、**設定** をクリックします。
2. 開いたウィンドウで **アカウント** を選択します。
3. ウィンドウ左側で **家族とその他のユーザー** を選択します。
4. 種類を変更するアカウントのアイコンをクリックし、**アカウントの種類の変更** をクリックします。



5. ユーザーアカウントの種類に **標準ユーザー** を選択します。
6. **OK** をクリックします。

Windows 11の場合

1. スタート ボタンを選択し、**設定** をクリックします。
2. 開いたウィンドウで **アカウント** を選択します。
3. ウィンドウ中央で **家族とその他のユーザー** を選択します。
4. 種類を変更するアカウントのアイコンをクリックし、**アカウントの種類の変更** をクリックします。
5. ユーザーアカウントの種類に **標準ユーザー** を選択します。
6. **OK** をクリックします。

システムにアカウントが1つしかない場合は、その種類を標準ユーザーに変更することはできません。詳細については、[Microsoftテクニカルサポート](#)  サイトをご覧ください。

通知を受信する

必要に応じて、Office Control の動作に関する、デスクトップの通知を **設定** することができます。

11.1. インターネットリソースへのアクセス

インターネット タブでは、ユーザーが望ましくないWebサイト(暴力、ギャンブルなど)にアクセスすることを制限したり、特定のWebサイトのみアクセスを許可したりすることができます。デフォルトでは、すべてのユーザーに対して **制限なし** モードが設定されています。次のモードも使用できます。

- カテゴリー別にアクセスを制限する
- ホワイトリスト上の**Web**サイトに対するアクセスのみを許可

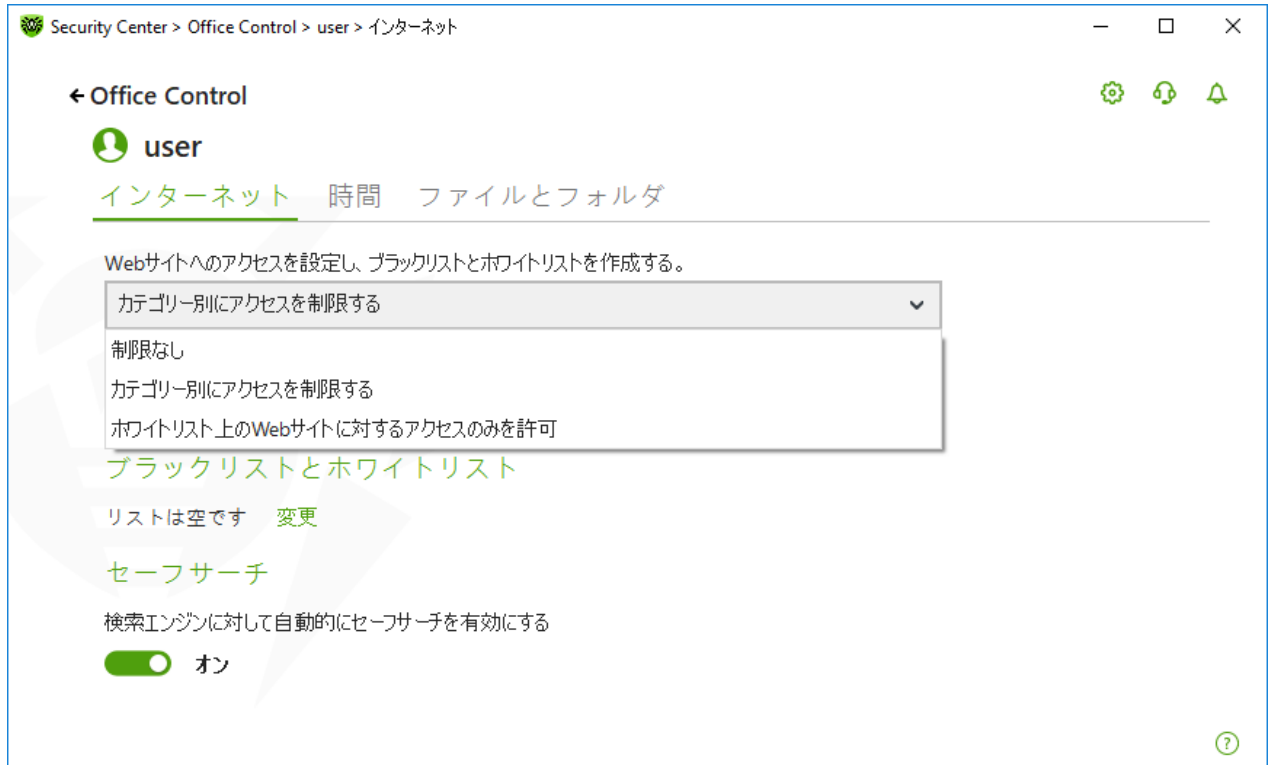


図 84. Office Controlのモードを選択する

カテゴリ別にアクセスを制限する モード

このモードでは、ブロックするWebサイトのカテゴリを指定できます。同じWebサイトを複数のカテゴリに割り当てることができます。この場合、Office Controlは、制限リストに含まれているカテゴリのうち少なくとも1つに属している場合に、サイトへのアクセスをブロックします。

このモードでは、他の制限に関係なくアクセスを許可／ブロックするサイトを追加することもできます。これには [ブラックリストとホワイトリスト](#) を使用します。

特定のカテゴリのWebサイトへのアクセスを許可またはブロックするには

1. **Web**サイトのカテゴリ グループで **変更** をクリックします。ブロックするカテゴリの設定ウィンドウが開きます。

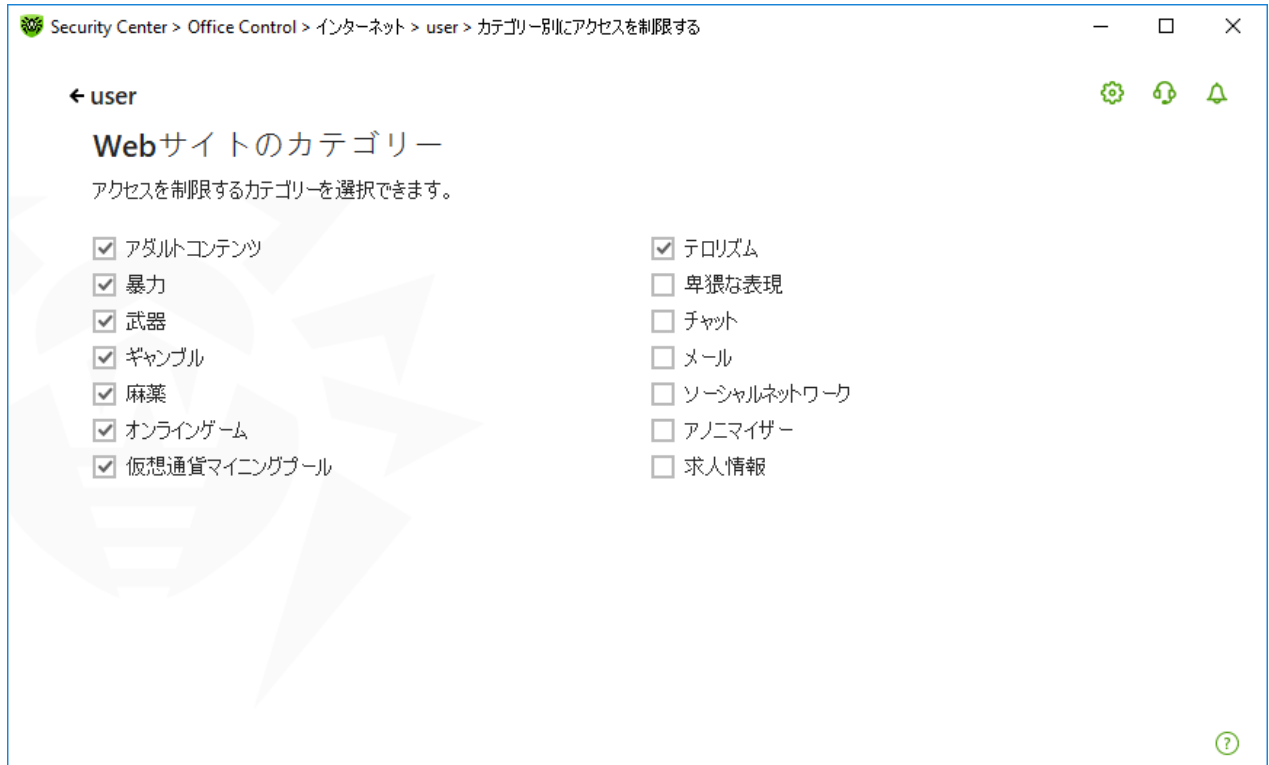


図 85. ブロックするWebサイトのカテゴリ

2. 特定のカテゴリのWebサイトへのアクセスを許可またはブロックするには、チェックボックスをオンまたはオフにします。

インターネットリソースのカテゴリ

カテゴリ	説明
アダルトコンテンツ	ポルノや性的なコンテンツ、出会い系サイトなどを含むWebサイト
暴力	暴力行為を助長するWebサイトや、様々な死亡事故などに関するコンテンツを含むWebサイト
武器	武器および爆発物に関するWebサイトや、それらの製造に関する情報を提供しているWebサイト
ギャンブル	ギャンブル、カジノ、オークションのオンラインゲームへのアクセスを提供するWebサイト(賭けサイトを含む)
麻薬	麻薬の使用、製造または流通を促進するWebサイト
オンラインゲーム	インターネットへの常時接続を使用してゲームへのアクセスを提供するWebサイト
テロリズム	攻撃的なプロパガンダ、またはテロ攻撃に関する内容を含むWebサイト
卑猥な表現など	猥褻な言葉を含む(タイトル、記事などに) Webサイト
チャット	テキストメッセージのリアルタイム送信を提供するWebサイト
メール	Webメールボックスの無料登録を提供するWebサイト



カテゴリー	説明
ソーシャルネットワーク	様々なソーシャルネットワーク: 一般、仕事、企業、興味、テーマ別 出会い系サイト
アノニマイザー	ユーザーが個人情報を隠し、ブロックされたWebリソースにアクセスすることを可能にするWebサイト
仮想通貨マイニングプール	仮想通貨マイニングのための一般的なサービスへのアクセスを提供するWebサイト
求人情報	求人情報の投稿や検索に使用されるWebサイト

ホワイトリスト上のWebサイトに対するアクセスのみを許可 モード

このモードでは、ホワイトリストに含まれているものを除いた、すべてのWebサイトへのアクセスがブロックされます。



ホワイトリスト上のWebサイトに対するアクセスのみを許可 モードを選択すると、ホワイトリストにあるWebサイトが正しく表示されない場合があります。外部リソースと統合されたバナーやその他のサイトエレメントは表示されません。

ブラックリストとホワイトリスト

他のOffice Control設定に関係なくアクセスを許可またはブロックしたいWebサイトのブラックリストとホワイトリストを設定することができます。



お使いのブラウザで以前に開かれたことのあるサイトを追加する場合は、ブラックリストまたはホワイトリストにサイトを追加する前にブラウザのキャッシュをクリアしてください。

Office Controlのブラックリストとホワイトリストを設定する

1. ブラックリストとホワイトリスト グループで **変更** をクリックします。ブラックリストとホワイトリストの設定ウィンドウが開きます。



図 86. Office Controlのブラックリストとホワイトリストを設定する

2. アクセスを許可するかブロックするかに応じて ホワイトリスト または ブラックリスト のフィールド内にサイトのドメイン名またはドメイン名の一部を入力してください。
 - 特定のサイトを追加する場合は、そのURLを入力します(例: `www.example.com`)。そのサイトにあるすべてのWebページへのアクセスが許可／禁止されます。
 - URLに特定のテキストを含むWebサイトへのアクセスを許可／禁止する場合、入力フィールドにそのテキストを入力してください。

例えば `example` と入力した場合、`example.com`、`example.test.com`、`test.com/example`、`test.example222.ru` などのアドレスへのアクセスが許可／禁止されます。
 - 特定のドメイン内にあるWebサイトへのアクセスを許可／禁止したい場合、入力するドメイン名にピリオド(.)記号を使用してください。そのWebサイト内にあるすべてのWebページへのアクセスが許可／禁止されます。ストリングがスラッシュ(/)記号も含んでいる場合、この記号の前にあるサブストリングはドメイン名と見なされ、後ろにあるサブストリングは、このドメイン内でアクセスを許可／禁止するWebサイトアドレスの一部と見なされます。

例えば `example.com/test` と入力した場合、`example.com/test11`、`template.example.com/test22` などのWebページへのアクセスが許可／禁止されます。
 - 特定のWebサイトを除外する場合は、それらの名前のマスクを入力してください。マスクは `mask://...` フォーマットで追加されます。

マスクはオブジェクト名の共通部分を定義します:

 - '*' は、任意のシーケンス(空のものを含む)の任意の記号と置き換えられます。
 - '?' は、任意の1つの記号(空を含む)と置き換えられます。



例:

 - `mask://*.com` または `.com-` ドメインが `.com` であるすべてのWebサイトを開くことを許可／禁止します。



- mask://mail - 名前に「mail」を含むあらゆるWebサイトを開くことを許可／禁止します。
- mask://???.com/ - 名前が三文字以下の文字から成る、ドメインが .com であるすべてのWebサイトを開くことを許可／禁止します。

入力したアドレスは一般的な形に変換される場合があります。例: http://www.example.com は www.example.com に変えられます。

3. Webサイトをリストに追加するには  をクリックします。
4. アドレスをリストから削除するには、該当するアイテムを選択して  をクリックします。
5. 他のアドレスを追加するには、手順2と3を繰り返します。

セーフサーチ

セーフサーチ オプションは、検索エンジンの結果に影響します。このオプションを使用することで、検索エンジンツールを使用した検索結果から望まないWebページを除外することができます。

セーフサーチ 機能を有効にするには、スイッチ  を オン 状態に設定します。

11.2. コンピューターとインターネットの使用時間制限

時間 タブでは、コンピューターとインターネットの使用時間に制限を設定できます。デフォルトでは、すべてのユーザーに対して **制限なし** モードが設定されています。

時間帯の表を使用して、時間制限を設定することができます。



コンピューターまたはインターネットの使用時間に制限を設定すると、メイン設定の [Self-Protection](#) ページ内にある **システム日時の変更をブロック** オプションが自動的に有効になります。

コンピューターとインターネットの使用時間制限の表

この表は、Office Controlの **制限なし** モードで使用できます。表が変更された場合、**制限なし** モードは **ユーザー指定** に自動的に切り替わります。

この表を使用して、ユーザーに対してコンピューターまたはインターネットの使用を許可する時間帯と曜日を指定できます。コンピューターへのアクセスが制限される時間になると、ユーザーは自動的にログオフされます。特定のユーザーのアカウントに対する制限が有効になっている間、該当するユーザーはログインすることができません。インターネットの使用制限が有効になっている場合、すべてのインターネットコンテンツのダウンロードが停止します。

制限時間 タイルをクリックすると、アクセス制限が有効になるまでの残り時間をDr.Web [メニュー](#) 内で確認することができます。

テーブルモードで時間制限を設定するには

1. ユーザーのインターネットアクセスを禁止したい曜日および時間を選択し、該当する時間帯を青くマーキングします:
 - 1つの時間帯を選択する場合、該当する時間帯を1回だけクリックします。

- 隣り合った複数の時間帯を選択したい場合は、最初の時間帯を1回クリックし、マウスのボタンを押したまま残りの時間帯を選択してください。
2. ユーザーのコンピューター使用を禁止したい曜日および時間を選択し、該当する時間帯を赤くマーキングします。
- 1つの時間帯を選択する場合、該当する時間帯を2回クリックします。
 - 隣り合った複数の時間帯を選択したい場合は、最初の時間帯を2回クリックし、マウスのボタンを押したまま残りの時間帯を選択してください。

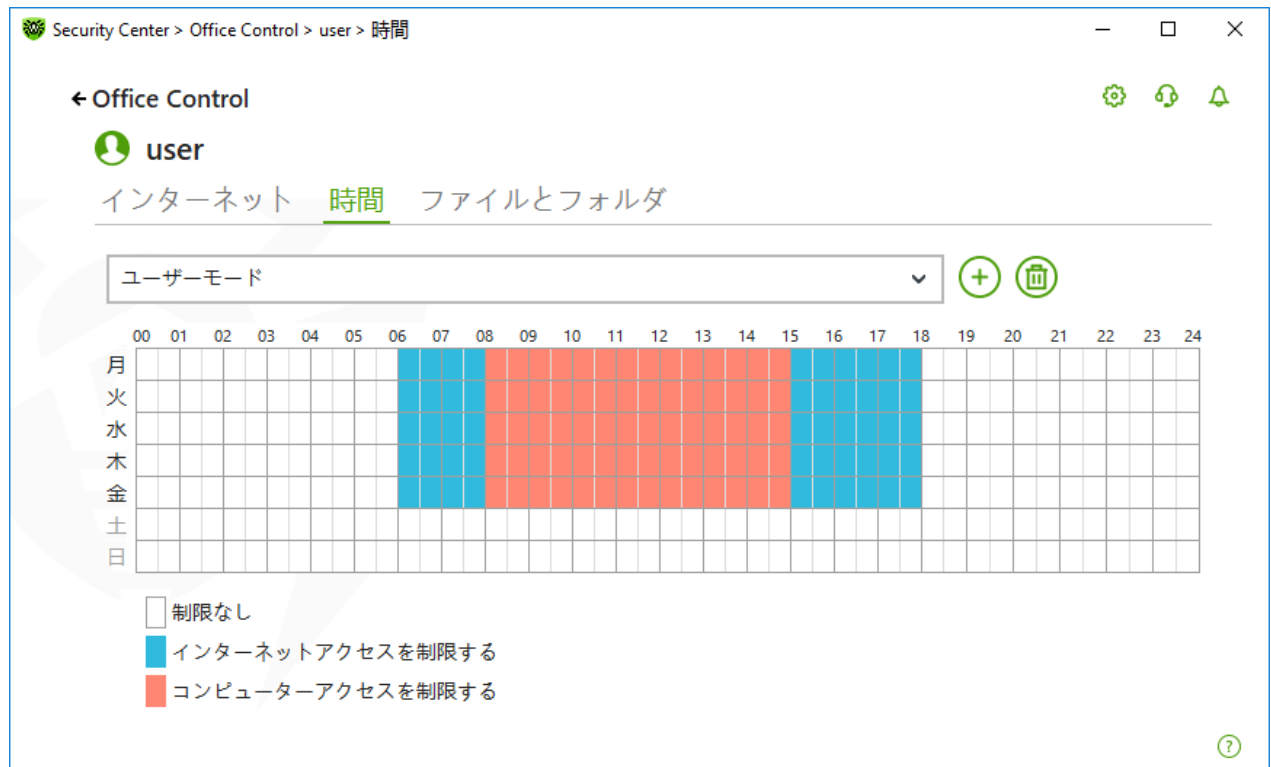


図 87. コンピューターおよびインターネット使用の表

1人のユーザーに対して異なる設定のプロファイルを作成することができます。このオプションによって、設定プロファイルを簡単に切り替えることが可能になります。

設定プロファイルの作成と削除

- 設定プロファイルを作成するには、**(+)** をクリックします。現在の表の設定が保存されます。設定を変更すると、設定は自動的にプロファイルに保存されます。
- 設定プロファイルを削除するには、**(🗑)** をクリックします。

11.3. ファイルとフォルダへのアクセス

ファイルとフォルダ タブでは、ファイルやフォルダへのアクセスを制限できます。デフォルトでは、制限は設定されていません。

ユーザーのファイルやフォルダへのアクセス制限を有効または無効にするには、スイッチ **🔘** を使用します。



図 88. ファイルやフォルダへのアクセスを管理する



コンピューターがリムーバブルメディアから起動された場合や、指定されたオブジェクトに対するアクセスがコンピューター上にインストールされている他のOSから行われた場合、アクセスの制限は保証されません。

ファイルとフォルダへのアクセスを制限するには

1. スイッチ を使用してファイルとフォルダへのアクセス制限を有効にします。
 2. オブジェクトをリストに追加するには をクリックし、ファイルまたはフォルダを選択します。
 3. 追加されたオブジェクトのアクセスモードを選択します。
 - **ブロック** - 選択したオブジェクトへのアクセスを完全にブロックします。
 - **読み取り専用** (デフォルトで選択されています) - オブジェクトの読み込みを許可します (ドキュメントや画像の表示、実行ファイルの開始など)。オブジェクトの削除、変更は許可されません。
- リストからオブジェクトを削除するには、該当するファイルを選択し をクリックします。

12. 隔離マネージャー

隔離マネージャーは、隔離されたファイルを管理するためのツールです。隔離には、悪意のあるオブジェクトが検出されたファイルが含まれています。また、隔離にはDr.Webによって処理されたファイルのバックアップコピーも格納されます。隔離マネージャーを使用して、隔離されたファイルを削除、再スキャン、復元することができます。

隔離マネージャー ウィンドウを開くには

1. Dr.Web [メニュー](#) を開き、**Security Center** を選択します。
2. **隔離マネージャー** タイルをクリックします。



図 89. 隔離内のオブジェクト

ウインドウ中央の表には、隔離されたオブジェクトに関する以下の情報が含まれています。

- **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 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フルパス



お使いのユーザーアカウントでアクセス可能なオブジェクトのみが表示されます。隠しオブジェクトを見るには管理者権限が必要です。

デフォルトでは隔離内のバックアップコピーは表示されません。それらを表示させるには をクリックし、ドロップダウンリストから **バックアップコピーを表示** を選択してください。





隔離されたオブジェクトに対する動作

管理者モードでは、以下のボタンを使用することができます。

-  (復元) ボタン - 1つまたは複数のオブジェクトを選択したフォルダに移動します。



このアクションはオブジェクトが安全であると分かっている場合のみ使用してください。

-  (再検査) - 隔離されているファイルを再度スキャンします。
-  (削除) ボタン - 1つまたは複数のオブジェクトを隔離およびシステムから削除します。

これらの設定は、1つまたは複数のオブジェクトを選択し、それらを右クリックすることでも開くことができます。

一度に全てのオブジェクトを隔離から削除するには、 をクリックし、ドロップダウンリストで **全て削除** を選択します。

アドバンス

隔離されたファイルの保存先や自動削除を設定するには、隔離マネージャーの設定 に移動します。

13. 除外

このグループでは、SpIDer Guard、SpIDer Gate、SpIDer Mail、Scanner によるスキャンからの除外を設定できるほか、スパムメッセージのスキャンを実行しない送信者のアドレスをブラックリストまたはホワイトリストに追加できます。

除外 設定グループを開くには

1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. 開いたウィンドウで、**除外** タイルをクリックします。

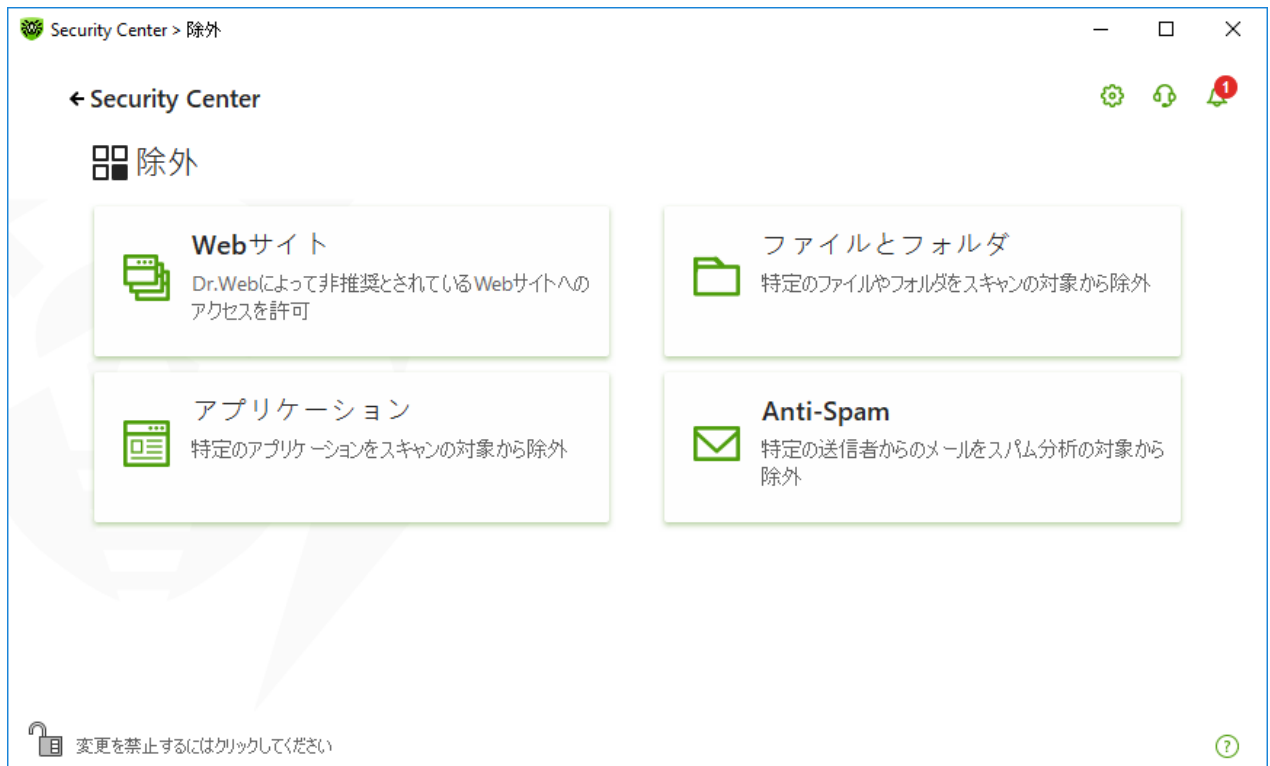




図90. 除外

除外設定を開くには

1. Dr.Webが [管理者モード](#) で動作していることを確認してください(プログラムウィンドウ下部にあるロックが開いています )。管理者モードではない場合は、ロックをクリックします 。
2. 該当するセクションのタイルをクリックします。



設定はアンチウイルスネットワーク管理者によってロックされる可能性があることに注意してください。

このセクションでは以下の設定を行うことができます。

- [Webサイト](#) - Doctor Webで推奨されていないWebサイトへのアクセスを設定します。
- [ファイルとフォルダ](#) - SpIDer GuardとScanner のスキャンから、特定のファイルとフォルダを除外します。




- [アプリケーション](#) - SpIDer Guard、SpIDer Gate、SpIDer Mail のスキャンから、特定のプロセスを除外します。
- [Anti-Spam](#) - スпам用のSpIDer Mailメッセージのスキャンを設定します。

13.1. Webサイト

SpIDer Gate HTTPトラフィックスキャンの設定に関係なくアクセスを許可するWebサイトのリストを設定できます。SpIDer Gate 設定で**非推奨サイトをブロックする** オプションが有効になっている場合、特定のWebサイトを除外リストに追加することで、それらサイトへのアクセスを許可することができます。リストに追加されているWebサイトへのアクセスは許可されますが、Webサイトのウイルススキャンは行われません。

アクセスを許可する**Webサイト**のリストを設定するには

1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. 開いたウィンドウで、**除外** タイルをクリックします。
3. **Webサイト** タイルをクリックします。

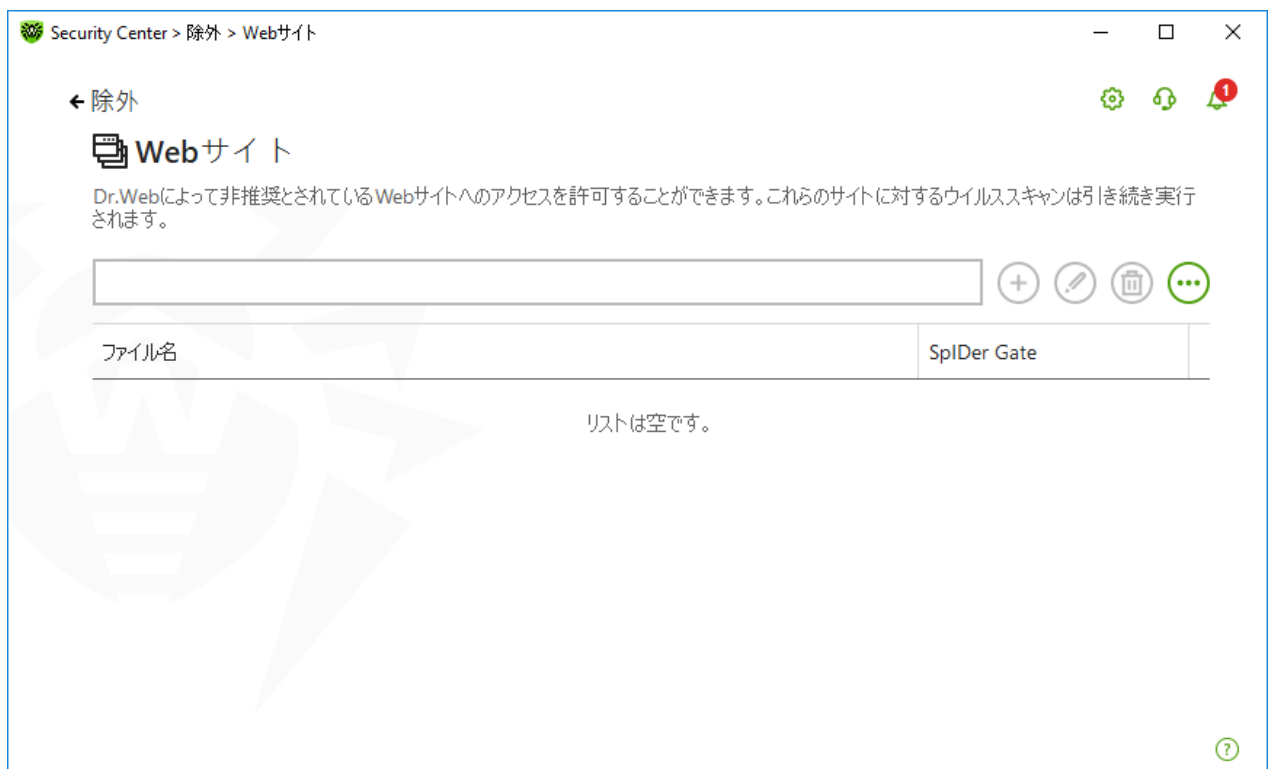


図91. 除外するWebサイトのリスト

デフォルトでは、このリストは空になっています。Webサイトを除外リストに追加すると、他の SpIDer Gate 設定に関係なく、ユーザーはそのWebサイトにアクセスできるようになります。Webサイトが Office Control のブラックリストと除外リストの両方に追加された場合、アクセスはブロックされます。

ドメイン名をリストに追加するには

1. 他の制限に関係なくアクセスするWebサイトのドメイン名またはドメイン名の一部を入力フィールドに入力します。



- 特定のサイトを追加する場合は、サイト名を入力します(例: `www.example.com`)。このサイトにあるすべてのWebページへのアクセスが許可されます。
- URLに特定のテキストを含むWebサイトへのアクセスを許可する場合、入力フィールドにそのテキストを入力してください。例えば `example` と入力した場合、`example.com`、`example.test.com`、`test.com/example`、`test.example222.ru` などのアドレスへのアクセスが許可されます。
- 特定のドメイン内にあるWebサイトへのアクセスを許可したい場合、入力するドメイン名にピリオド(.)記号を使用してください。そのWebサイト内にあるすべてのWebページへのアクセスが許可されます。ストリングがスラッシュ(/)記号も含んでいる場合、この記号の前にあるサブストリングはドメイン名と見なされ、後ろにあるサブストリングは、このドメイン内でアクセスを許可するWebサイトアドレスの一部と見なされます。例えば `example.com/test` と入力した場合、`example.com/test11`、`template.example.com/test22` などのWebページへのアクセスが許可されます。
- 特定のWebサイトを除外する場合は、それらの名前のマスクを入力してください。マスクは `mask://...フォーマット` で追加されます。


マスクはオブジェクト名の共通部分を定義します:

- '*' は、任意のシーケンス(空のものを含む)の任意の記号と置き換えられます。
- '?' は、任意の1つの記号(空を含む)と置き換えられます。

例:





- `mask://*.com/` - ドメインが `.com` であるすべてのWebサイトを開くことを許可します。
- `mask://mail` - 名前に「mail」を含むあらゆるWebサイトを開くことを許可します。
- `mask://????.com/` - 名前が三文字以下の文字から成る、ドメインが `.com` であるすべてのWebサイトを開くことを許可します。

入力したアドレスは一般的な形に変換される場合があります。例: `http://www.example.com` は `www.example.com` に変えられます。

2.  ボタンをクリックするか、キーボードの ENTER を押します。指定したアドレスがリストに表示されます。
3. 他のアドレスを追加するには、手順1と2を繰り返します。

リスト内容の管理

テーブル内のオブジェクトを操作するには、次の管理要素を使用できます。

-  ボタン - アドレスを除外リストに追加します。このボタンは、テキストフィールドに記号が含まれている場合に使用できます。
-  ボタン - 除外リスト内の選択したWebサイトのアドレスを編集します。
-  ボタン - 選択したWebサイトのアドレスを除外リストから削除します。
-  をクリックすると以下のオプションにアクセスすることができます。
 - エクスポート - 作成した除外リストを保存して、Dr.Webがインストールされている別のコンピューターで使用できるようにします。
 - インポート - 別のコンピューターで作成された除外リストを使用できるようにします。
 - 全てクリアする - 全てのオブジェクトを除外リストから削除します。

1つまたは複数のオブジェクトを選択して右クリックすると、オブジェクトを削除または編集できます。



13.2. ファイルとフォルダ

SpIDer Guard コンポーネントと Scanner コンポーネントによるシステムのアンチウイルススキャンから除外するファイルやフォルダのリストを管理できます。Dr.Webの隔離フォルダ、一部のプログラムの作業フォルダ、一時ファイル(ページングファイル)などを除外できます。

除外するファイルとフォルダのリストを設定するには



1. Dr.Web **メニュー**  を開き、**Security Center** を選択します。
2. 開いたウィンドウで、**除外** タイルをクリックします。
3. **ファイルとフォルダ** タイルをクリックします。



図92. ファイルとフォルダの除外リスト

デフォルトではリストは空です。特定のファイルやフォルダを除外に追加するか、マスクを使用して特定のファイルグループのスキャンを無効にします。追加されたオブジェクトは、両方のコンポーネントのスキャンまたは各コンポーネントのスキャンから個別に除外することができます。

ファイルとフォルダを除外リストに追加するには

1. 除外リストにファイルまたはフォルダを追加するには、次の内いずれか1つを実行してください。
 - 既存のファイルやフォルダを追加するには、 ボタンをクリックします。開いているウィンドウで、**参照** ボタンをクリックしてファイルまたはフォルダを選択します。ファイルまたはフォルダのフルパスを入力するか、フィールドのパスを編集してからリストに追加できます。例：
 - C:\folder\file.txt - C:\folder フォルダに保存されている file.txt ファイルを除外します。



- C:\folder\ - C:\folder フォルダと、そのサブフォルダ内のすべてのファイルをスキャン対象から除外します。
- 特定の名前のファイルを除外するには、名前と拡張子をパスなしで入力します。例：
 - file.txt - 全てのフォルダ内にある、file という名前と .txt 拡張子を持った全てのファイルをスキャン対象から除外します。
 - file - 全てのフォルダ内にある、file という名前を持った全てのファイルをその拡張子に関係なくスキャン対象から除外します。
- ファイルやフォルダのグループを除外するには、名前のマスクを入力します。

マスクはオブジェクト名の共通部分を定義します：

- アスタリスク記号 (*) は、任意のシーケンス(空のものを含む)の任意の文字と置き換えられます。
- 疑問符 (?) は、任意の文字(1つ)と置き換えられます。

例：





- Report*.doc は、"Report" という語で始まる名前を持つ全てのMicrosoft Wordドキュメントを定義します(例:ReportFebruary.doc、Report121209.doc など)。
- *.exe は、すべての実行ファイル、すなわちEXE拡張子を持ったファイルを定義します(例:setup.exe、iTunes.exe など)。
- photo????09.jpg は、"photo" で始まり、間にその他の文字を4つ含んで "09" で終わる名前を持った全てのJPGイメージを定義します(例:photo121209.jpg、photoJoe09.jpg、photo----09.jpg など)。
- file* - 全てのフォルダ内にある、file で始まる名前を持った全てのファイルをその拡張子に関係なくスキャン対象から除外します。
- file.* - 全てのフォルダ内にある、file という名前を持った全てのファイルをその拡張子に関係なくスキャン対象から除外します。
- C:\folder** - C:\folder フォルダに保存されている全てのサブフォルダとファイルを除外します。サブフォルダ内に保存されているファイルはスキャンされます。
- C:\folder* - C:\folder フォルダと、そのサブフォルダ内の全てのファイルを階層に関係なくスキャン対象から除外します。
- C:\folder*.txt - C:\folder フォルダ内の全ての *.txt ファイルをスキャン対象から除外します。サブフォルダ内の *.txt ファイルはスキャンされます。
- C:\folder**.txt - C:\folder フォルダの第一レベルサブフォルダ内の全ての *.txt ファイルをスキャン対象から除外します。
- C:\folder***.txt - C:\folder フォルダ内の全ての階層のサブフォルダ内の全ての *.txt ファイルをスキャン対象から除外します。C:\folder フォルダ直下にあるファイルに対しては、*.txt ファイルも含め、スキャンを行います。

2. ファイルやフォルダを追加するウィンドウで、選択したオブジェクトをスキャンしないコンポーネントを指定します。
3. **OK** をクリックすると、指定されたファイルまたはフォルダがリスト上に表示されます。
4. 他のファイルやフォルダを追加するには、手順1～3を繰り返します。



リスト内容の管理

テーブル内のオブジェクトを操作するには、次の管理要素を使用できます。

-  ボタン - オブジェクトを除外リストに追加します。
-  ボタン - 除外リスト内の選択したオブジェクトを編集します。
-  ボタン - 選択したオブジェクトを除外リストから削除します。
これらの設定は、1つまたは複数のオブジェクトを選択し、それらを右クリックすることでも開くことができます。
-  をクリックすると以下のオプションにアクセスすることができます。
 - エクスポート - 作成した除外リストを保存して、Dr.Webがインストールされている別のコンピューターで使用できるようにします。
 - インポート - 別のコンピューターで作成された除外リストを使用できるようにします。
 - 全てクリアする - 全てのオブジェクトを除外リストから削除します。

13.3. アプリケーション

ファイルモニターSpIDer Guard、インターネットモニターSpIDer Gate、メールアンチウイルスSpIDer Mail によるスキャンから除外するプログラムとプロセスのリストを指定できます。これらアプリケーションの動作の結果として変更されたオブジェクトは、スキャンの対象から除外されます。

除外するアプリケーションのリストを設定するには


1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. 開いたウィンドウで、**除外** タイルをクリックします。
3. **アプリケーション** タイルをクリックします。



図 93. 除外するアプリケーションのリスト

デフォルトではリストは空です。

アプリケーションをリストに追加するには

1. プログラムまたはプロセスを除外リストに追加するには **(+)** をクリックします。以下のうちいずれか1つを実行してください。

- 開いたウィンドウ内で **参照** をクリックし、アプリケーションを選択します。アプリケーションへのフルパスを手動で入力することも可能です。例：

`C:\Program Files\folder\example.exe`

- スキャンの対象から除外するアプリケーションの名前をフィールドに入力してください。アプリケーションへのフルパスは必要ありません。例：

`example.exe`

- アプリケーションをスキャンから除外するには、それらの名前を定義するマスクを入力します。

マスクはオブジェクト名の共通部分を定義します：

- '*' は、任意のシーケンス(空のものを含む)の任意の文字と置き換えられます。
- '?' は、任意の文字(1つ)と置き換えられます。

例：

- `C:\Program Files\folder*.exe` - `C:\Program Files\folder` フォルダ内のアプリケーションをスキャンの対象から除外します。サブフォルダ内のアプリケーションに対してはスキャンを行います。
- `C:\Program Files**.exe` - `C:\Program Files` フォルダの第一レベルサブフォルダ内のアプリケーションをスキャン対象から除外します。



- C:\Program Files***.exe - C:\Program Files フォルダ内の全ての階層にあるサブフォルダ内のアプリケーションをスキャン対象から除外します。C:\Program Files フォルダ直下にあるアプリケーションに対してはスキャンを行います。
 - C:\Program Files\folder\exam*.exe - C:\Program Files\folder フォルダ内の exam で始まる名前を持った全てのアプリケーションをスキャンの対象から除外します。サブフォルダ内のアプリケーションに対してはスキャンを行います。
 - example.exe - 全てのフォルダ内にある、example という名前と .exe 拡張子を持った全てのアプリケーションをスキャン対象から除外します。
 - example* - 全てのフォルダ内にある、example で始まる名前を持った全ての種類のアプリケーションをスキャン対象から除外します。
 - example.* - 全てのフォルダ内にある、example という名前を持った全てのアプリケーションをその拡張子に関係なくスキャン対象から除外します。
- この変数の名前と値がシステム変数の設定で指定されている場合は、変数の名前でスキャンからアプリケーションを除外できます。例：

%EXAMPLE_PATH%\example.exe - システム変数の名前によってアプリケーションを除外します。システム変数の名前と値はOS設定内で指定することができます。

Windows7以降: コントロールパネル → システム → システムの詳細設定 → 詳細設定 → 環境変数 → システム環境変数

例における変数の名前: EXAMPLE_PATH

例における変数の値: C:\Program Files\folder

2. 設定ウィンドウで、選択したアプリケーションをスキャンしないコンポーネントを指定します。

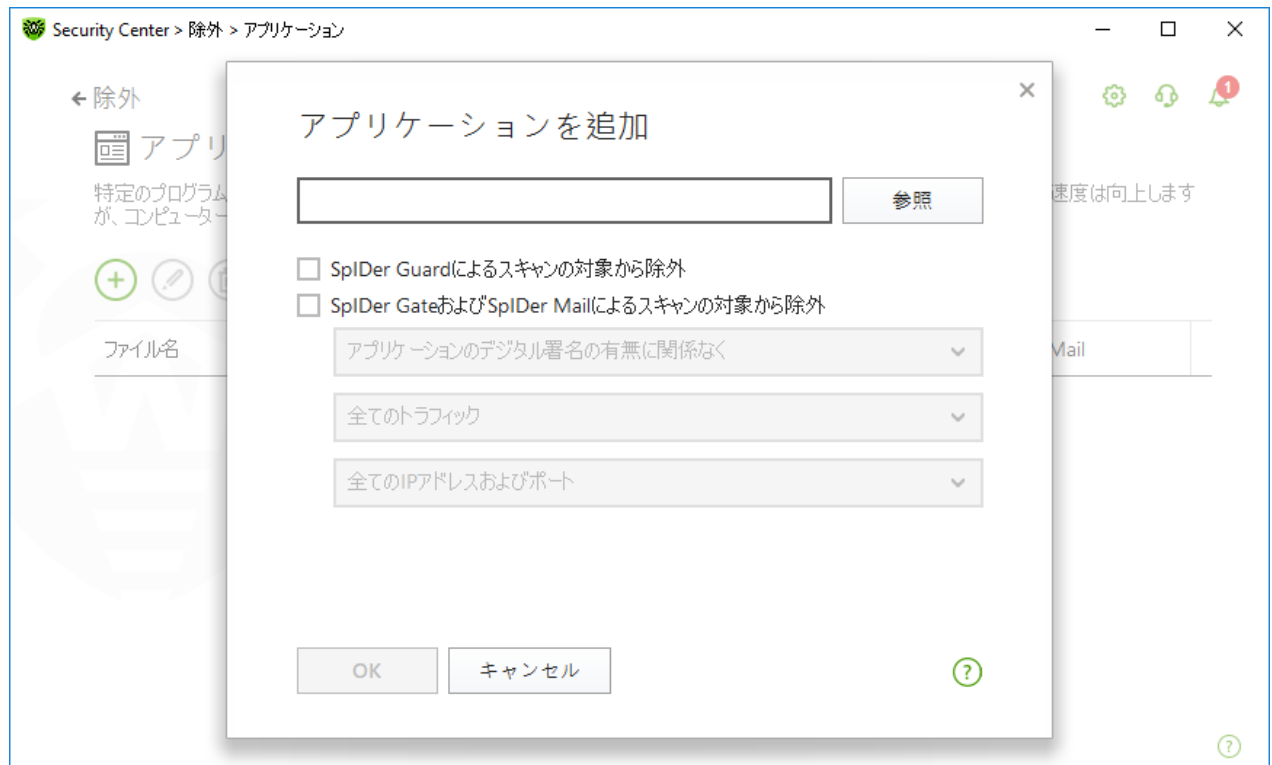


図94. アプリケーションを除外リストに追加する

3. SpIDer GateとSpIDer Mailでは、追加の条件を指定します。






パラメータ	説明
アプリケーションのデジタル署名の有無に関係なく	有効な電子署名の有無に関係なく、アプリケーションをスキャンから除外するには、このパラメータを選択します。
アプリケーションに有効なデジタル署名がある場合	有効なデジタル署名がある場合にのみ、アプリケーションをスキャンから除外するには、このパラメータを選択します。それ以外の場合、アプリケーションはコンポーネントによってスキャンされます。
全てのトラフィック	暗号化されたアプリケーションと暗号化されていないアプリケーションのトラフィックをスキャンから除外するには、このパラメータを選択します。
暗号化トラフィック	暗号化されたアプリケーショントラフィックのみをスキャンから除外するには、このパラメータを選択します。
全てのIPアドレスおよびポート	全てのIPアドレスとポート上のトラフィックをスキャンから除外するには、このパラメータを選択します。
特定のIPアドレスおよびポート	特定のIPアドレスとポートをスキャンから除外するには、このパラメータを選択します。他のIPアドレスとポートからのトラフィックはスキャンされます（特に指定しない限り）。
アドレスおよびポートを指定する	除外設定を行う手順は以下のとおりです： <ul style="list-style-type: none">● 特定のポートに対応する特定のドメインをスキャンから除外するには、たとえば「site.com:80」と入力します。● カスタムポート（例：1111）上のトラフィックをスキャンの対象から除外するには、たとえば「*:1111」と入力します。● すべてのポートでトラフィックのスキャンを除外するには、「site:*」と入力します。

4. **OK** をクリックすると、選択されたアプリケーションがリスト上に表示されます。


5. 追加したいプログラムが他にもある場合は、操作を繰り返します。

リスト内容の管理

テーブル内のオブジェクトを操作するには、次の管理要素を使用できます。

-  ボタン - オブジェクトを除外リストに追加します。
-  ボタン - 除外リスト内の選択したオブジェクトを編集します。
-  ボタン - 選択したオブジェクトを除外リストから削除します。

これらの設定は、1つまたは複数のオブジェクトを選択し、それらを右クリックすることでも開くことができます。


-  をクリックすると以下のオプションにアクセスすることができます。
 - エクスポート - 作成した除外リストを保存して、Dr.Webがインストールされている別のコンピューターで使用できるようにします。
 - インポート - 別のコンピューターで作成された除外リストを使用できるようにします。
 - 全てクリアする - 全てのオブジェクトを除外リストから削除します。



13.4. Anti-Spam

メッセージをスパムスキャンから除外する送信者のリストを設定することができます。

ホワイトリストとブラックリストを作成するには

1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. 開いたウィンドウで、**除外** タイルをクリックします。
3. **Anti-Spam** タイルをクリックします。

ブラックリストとホワイトリスト上の送信者からのメッセージに対する SpIDer Mail コンポーネントの動作：

- ホワイトリストにアドレスを追加すると、その送信者からのメッセージは安全であるとみなされ、スパムのスキャンは行われません。
- ブラックリストにアドレスを追加すると、この送信者からのメッセージは自動的にスパムとみなされます。




図95. ブラックリストとホワイトリスト

デフォルトでは、両方のリストは空です。

除外リストにメールアドレスを追加するには




1. 検査なしに自動的にメッセージを処理したい送信者のアドレス、または複数のアドレスに対するマスクを入力してください。詳細
 - 特定の送信者を追加する場合は、メールアドレス全体を入力します(例: name@mail.com)。この送信者からのメールはすべて検査なしに自動的に処理されます。



- 類似したユーザー名を持つ送信者を加える場合、アドレス内の異なる部分を'*'または'? '記号で置き換えてください。'*'は任意の記号のシーケンス、'? 'は任意の1つの記号の代わりに使用します。例えば name*@mail.com と入力した場合、SpIDer Mail は name@mail.com、name1@mail.com、name_of_name@mail.com、およびその他同じようなユーザー名を持つ送信者からのメッセージを自動的に処理します。
 - 特定のドメイン内のアドレスから送信されるメールをすべて自動的に処理したい場合、アドレス内でユーザー名の代わりにアスタリスク(*)記号を使用してください。例えばmail.comドメイン内の送信者からのメッセージを指定する場合は*@mail.com と入力します。
2. 入力したアドレスをリストに追加するには、 をクリックするか、キーボードの ENTER を押します。
 3. 他のアドレスを追加するには、手順1と2を繰り返します。

リスト内容の管理

テーブル内のオブジェクトを操作するには、次の管理要素を使用できます。

-  ボタン - メールアドレスをリストに追加します。このボタンは、テキストフィールドに記号が含まれている場合に使用できます。
-  ボタン - 選択したメールアドレスを除外リストから削除します。
-  をクリックすると以下のオプションにアクセスすることができます。
 - 変更 - リストで選択したメールアドレスを編集できます。
 - エクスポート - 作成した除外リストを保存して、Dr.Webがインストールされている別のコンピューターで使用できるようにします。
 - インポート - 別のコンピューターで作成された除外リストを使用できるようにします。
 - 全てクリアする - 全てのオブジェクトを除外リストから削除します。

1つまたは複数のオブジェクトを選択して右クリックすると、オブジェクトを削除または編集できます。



14. コンポーネント動作に関する統計

主要なDr.Webコンポーネントの動作に関する統計情報にアクセスできます。

保護コンポーネント動作の重要なイベントに関する統計を開くには


1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. 開いているウィンドウで、**統計** タブを選択します。
3. **統計** ページが開き、次のグループのレポートを見ることができます。
 - [詳細なレポート](#)
 - [Office Control](#)
 - [脅威](#)
 - [Firewall](#)



図96. コンポーネント操作に関する統計

4. レポートを見るグループを選択します。

詳細なレポート

このウィンドウでは、全てのプログラム操作イベントの詳細情報を確認できます。



日付	コンポーネント	イベント
16.10.2018 14:10	更新	更新が完了
16.10.2018 14:49	更新	更新が完了
16.10.2018 15:19	更新	更新が完了
16.10.2018 15:55	更新	更新が完了
16.10.2018 16:28	更新	更新が完了
16.10.2018 17:06	更新	更新が完了
16.10.2018 17:38	更新	更新が完了
16.10.2018 18:11	更新	更新が完了

図97. 詳細なレポートウィンドウ

レポートには以下の情報が記録されます：

- 日付 - イベントの日時。
- コンポーネント - イベントを報告したコンポーネントまたはモジュール。
- イベント - イベントの簡単な説明。

デフォルトでは、常に全てのイベントが表示されます。

管理要素 (🔍)、(i)、(☰) は、テーブル内のオブジェクトを操作するために使用されます。

追加のフィルターを使用して特定のイベントを選択できます。

Office Control

Office Control タイルでは、ユーザーアカウントごとにブロックされたURLに関する統計を見ることができます。



日付	ブロックされたリソース	ブロックの理由
6/6/2019 6:56 AM	reddit.com	アダルトコンテンツ
6/6/2019 6:56 AM	reddit.com	アダルトコンテンツ
6/6/2019 6:56 AM	reddit.com	アダルトコンテンツ
6/6/2019 6:56 AM	reddit.com	アダルトコンテンツ
6/6/2019 6:55 AM	facebook.com	ソーシャルネットワーク
6/6/2019 6:55 AM	facebook.com	ソーシャルネットワーク
6/6/2019 6:55 AM	facebook.com	ソーシャルネットワーク
6/6/2019 6:55 AM	facebook.com	ソーシャルネットワーク

図98. Office Controlの統計情報ウィンドウ

レポートには以下の情報が記録されます：

- 日付 - ブロックした日時。
- ブロックされたリソース - ブロックされたリソースへのリンク。
- ブロックの理由 - ブロックされたリソースが含まれているカテゴリまたは除外リスト。

デフォルトでは、常に全てのイベントが表示されます。

管理要素 (🔍)、(i)、(⋮) は、テーブル内のオブジェクトを操作するために使用されます。

追加のフィルターを使用して特定のイベントを選択できます。



統計には、埋め込みウィジェットなど、他のWebページと統合された外部リソースに関する情報も含まれています。統計にそのような要素があるということは、ユーザーが意図的にそれらのWebサイトにアクセスしようとしたということを意味するものではありません。

脅威

脅威 タイルには、一定の期間における脅威の合計数に関する情報が表示されます。



このタイルを開くと、事前定義されたすべての脅威に対するフィルターが適用された状態で、詳細なレポートウィンドウが開きます。

The screenshot shows a window titled 'Security Center > 統計 > 詳細なレポート'. It features a navigation bar with a back arrow and '統計', and a title bar with '詳細なレポート'. Below the title bar is a filter bar with a green bar containing the text '脅威をブロック, オブジェクトをブロック, 脅威を検出, 許可されていないコードの実行をブロック, Dr.Web for Microsoft Outlookが脅...' and icons for search, refresh, and help. The main content is a table with three columns: '日付', 'コンポーネント', and 'イベント'. The table contains six rows of data, all showing 'SplDer Gate' as the component and '脅威をブロック' as the event. The dates range from 18.10.2018 18:30 to 22.10.2018 13:09. There are also icons for management elements (Y, i, ...) and a help icon (?) at the bottom right.

日付	コンポーネント	イベント
22.10.2018 13:09	SplDer Gate	脅威をブロック
22.10.2018 13:09	SplDer Gate	脅威をブロック
18.10.2018 18:30	SplDer Gate	脅威をブロック
18.10.2018 18:30	SplDer Gate	脅威をブロック
18.10.2018 18:29	SplDer Gate	脅威をブロック
18.10.2018 18:29	SplDer Gate	脅威をブロック

図99. 脅威に関する統計ウィンドウ

レポートには以下の情報が記録されます：

- 日付 - 脅威を検出した日時。
- コンポーネント - 脅威を検出したコンポーネント。
- イベント - イベントの簡単な説明。

デフォルトでは、常に全てのイベントが表示されます。

管理要素 (Y)、(i)、(...) は、テーブル内のオブジェクトを操作するために使用されます。

追加のフィルターを使用して特定のイベントを選択できます。

ネットワークアクティビティ

コンピューター上に Dr.Web Firewall がインストールされている場合は、ネットワークアクティビティに関するレポートを見ることができます。

アクティブなアプリケーション、アプリケーションログ、パケットフィルターログに関する情報を見るには、ドロップダウンリストから必要なオブジェクトを選択してください。



名前	方向	プロトコル	ローカルアドレス	リモートアドレス	送信	受信
▼ svchost.e...	2の接続(接続の数)					
	リッスン(待...	TCPv6	:::49665	:::0	0 byte	0 byte
	リッスン(待...	TCPv4	0.0.0.0:49665	0.0.0.0:0	0 byte	0 byte
▶ svchost.e...	1の接続(接続の数)					
▶ svchost.e...	8の接続(接続の数)					
▶ svchost.e...	4の接続(接続の数)					
▶ svchost.e...	6の接続(接続の数)					
▶ svchost.e...	6の接続(接続の数)					

図100. Firewallウィンドウの統計

レポートにはアクティブな各アプリケーションに関する以下の情報が含まれています：

- 方向
- プロトコル
- ローカルアドレス
- リモートアドレス
- 送信されたデータパケットのサイズ
- 受信したデータパケットのサイズ

現在の接続の1つをブロックするか、以前にブロックされた接続を許可できます。これを行うには、必要な接続を選択して右クリックします。接続状態に応じて、使用できるオプションは1つだけです。

アプリケーションログには以下の情報が含まれています。

- アプリケーション起動時間
- アプリケーション名
- アプリケーションのプロセスルール名
- 方向
- アクション
- エンドポイント

アプリケーションログを有効にするには、**Firewall** ページに移動して、アプリケーションルールを追加または編集ウィンドウを開きます。詳細については、「[アプリケーションルールの設定](#)」のセクションを参照してください。




パケットフィルターログには以下の情報が含まれています：

- データパケット処理の開始時間
- 方向
- プロセスルール名
- インターフェース
- パケットデータ




パケットフィルターのログを有効にするには、**Firewall** ページに移動して、パケットフィルタールールを追加または編集 ウィンドウを開きます。詳細については、[パケットフィルタリングのルールセット](#) を参照してください。

列の1つをクリックすると、イベントは昇順または降順に並び替えられます。

フィルター

特定のパラメータに対応するイベントのみのリストを表示するには、フィルターを使用します。全てのレポートには、 をクリックして使用できるプリセットフィルターがあります。カスタムイベントフィルターを作成することもできます。

テーブル要素を管理するボタン：

-  をクリックすると以下のオプションにアクセスできます。
 - 設定された期間または更新イベントのフィルターに、事前定義されたフィルターを選択する。
 - 現在のカスタムフィルターを保存する。以前に保存したカスタムフィルターを削除することもできます。
 - 現在のフィルターを全て削除する。
-  をクリックすると以下のオプションにアクセスすることができます。
 - 選択された項目をコピー - 選択した項目をクリップボードにコピーできます。
 - 選択されたデバイスをエクスポート - 選択した項目を.csv形式で指定したフォルダにエクスポートできます。
 - 全てエクスポート - テーブルの全ての項目を.csv形式で指定したフォルダにエクスポートできます。
 - 選択した項目を削除する - 選択したイベントを削除できます。
 - 全て削除 - テーブルから全てのイベントを削除できます。
-  ボタンをクリックすると、イベントに関する詳細情報が表示されます。いずれかの項目が選択されている場合に使用できます。このボタンをもう一度クリックすると、イベントの詳細情報が非表示になります。

カスタムフィルターを設定するには

1. 特定のパラメータでフィルタリングするには、必要な列の見出しをクリックします。
 - 日付でフィルタリングする。ウィンドウの左部分にある予め指定された期間の1つを選択するか、ご自身で期間を指定することができます。必要な期間を設定するには、カレンダーで期間の開始日と終了日を選択するか、**期間** フィールドで日付を指定します。日付によるフィルタリングは、昇順または降順で並び替えることもできます。




The screenshot shows the 'Security Center > 統計 > 詳細なレポート' (Security Center > Statistics > Detailed Report) page. The page title is '統計 > 詳細なレポート' (Statistics > Detailed Report). Below the title, there are navigation icons and a search icon. The main content area is a table with columns for '日付' (Date), 'コンポーネント' (Component), and 'イベント' (Event). The table is currently empty. To the left of the table, there are filter options: '並び替え: 降順 昇順' (Sort by: Descending Ascending), '期間:' (Period:), and a date range selector showing '14/08/2019 17:00' to '16/10/2019 17:00'. Below the date range, there are three calendar views for August 2019, September 2019, and October 2019. The date '15' in August is highlighted. A green '適用' (Apply) button is at the bottom left of the filter section.

図101. データのソート

- コンポーネントごとにフィルタリングする。レポートに含まれる情報をコンポーネントで確認したり、昇順または降順に並び替えたりできます。
- イベントごとにフィルタリングする。レポートに表示するイベントを確認したり、昇順または降順に並び替えたりできます。

Office Controlの統計情報には、日付フィルターに加えて、次のオプションがあります。

- ブロックされたりリソースでフィルタリングする。項目を昇順または降順のみで並び替えることができます。
 - ブロックの理由でフィルタリングする。レポートに表示するブロックの理由を確認したり、昇順または降順に並び替えたりできます。
2. フィルターパラメータを選択したら、**適用** をクリックします。選択したアイテムがテーブルの上に表示されます。
 3. フィルターを保存するには、 をクリックして **フィルターを保存** を選択します。
 4. 開いたウィンドウ内で新しいフィルターの名前を入力します。**保存** をクリックします。

15. Server通知

ネットワーク管理者は、どの端末でもサーバー通知を有効にすることができます。この機能は、端末のうちの1台で操作を行う際に管理者にとって必要になる場合があります。

Server通知 ウィンドウを開くには


1. Dr.Web [メニュー](#)  を開きます。
2. **Server通知** を選択します。




図102. Server通知 ウィンドウ

受信した通知はすべてウィンドウの上部に表示されます。通知に関する情報を表示するには、それをクリックしてください。



フィルター

特定のパラメータに該当する通知のみのリストを表示するには、フィルターを使用します。 をクリックすると、デフォルトのフィルターのみを使用することができます。その設定はサーバーで設定されているものと同じです。カスタムイベントフィルターを作成することも可能です。

テーブル要素を管理するボタン:

-  をクリックすると以下のオプションにアクセスできます。
 - デフォルトのフィルターを選択するには
 - 現在のカスタムフィルターを保存する。以前に保存したカスタムフィルターを削除することもできます。



- 現在のフィルターを全て削除する。
-  をクリックすると以下のオプションにアクセスすることができます。
 - 選択された項目をコピー - 選択した項目をクリップボードにコピーできます。
 - 選択されたデバイスをエクスポート - 選択した項目を.csv形式で指定したフォルダにエクスポートできます。
 - 全てエクスポート - テーブルの全ての項目を.csv形式で指定したフォルダにエクスポートできます。
 - 選択した項目を削除する - 選択した通知を削除できます。
 - 既読にする - すべての通知を既読にすることができます。
 - 全て削除 - テーブルから全ての通知を削除できます。
- すべての通知を検索するには、 をクリックします。

カスタムフィルターを設定するには

1. 特定のパラメータでフィルタリングするには、必要な列の見出しをクリックします。
 - 端末でフィルタリングする。項目を昇順または降順のみで並べ替えることができます。
 - カテゴリーでフィルタリングする。レポートに含まれる情報をカテゴリーで確認したり、昇順または降順に並べ替えたりできます。以下のカテゴリーで通知をフィルタリングすることができます。
 - 管理者
 - 端末
 - ライセンス
 - 新規端末
 - リポジトリ
 - インストール
 - その他
 - サーバー通知でフィルタリングする。項目を昇順または降順のみで並べ替えることができます。
 - 日付でフィルタリングする。ウィンドウの左部分にある予め指定された期間の1つを選択するか、ご自身で期間を指定することができます。必要な期間を設定するには、カレンダーで期間の開始日と終了日を選択するか、期間 フィールドで日付を指定します。日付によるフィルタリングは、昇順または降順で並び替えることもできます。



Server通知

Server通知

並び替え: 降順 昇順

期間: 05/14/2019 5:00 PM — 07/16/2019 5:00 PM

今日

7日

30日

6か月


指定された期間

全ての期間

適用

端末	カテゴリ	Server通知	日付
testlab-imac.local			
testlab-imac.local			
testlab-imac.local			
testlab-imac.local			
testlab-imac.local			
testlab-imac.local			

図103. データのソート

2. フィルターパラメータを選択したら、**適用** をクリックします。選択したアイテムがテーブルの上に表示されます。
3. フィルターを保存するには、 をクリックして **フィルターを保存** を選択します。
4. 開いたウィンドウ内で新しいフィルターの名前を入力します。**保存** をクリックします。



16. テクニカルサポート

Dr.Web製品のインストールまたは使用中に問題が発生した場合、テクニカルサポートへのお問い合わせの前に以下のオプションをご利用ください:

- <https://download.drweb.com/doc/> から最新のマニュアルやガイドをダウンロードして読む。
- https://support.drweb.com/show_faq/ で「よくあるご質問」を読む。
- <https://forum.drweb.com/index.php> でDr.Webフォーラムを見る。

問題が解決しなかった場合、サポートサイト <https://support.drweb.com/> 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までお問い合わせください。

企業情報については、Doctor Web 公式サイト <https://company.drweb.com/contacts/offices/> をご覧ください。

16.1. 問題解決サポートオプション

アンチウイルスネットワーク管理者にお問い合わせの際は、お使いのオペレーティングシステムとDr.Webの操作に関するレポートの生成が必要な場合があります。

レポートウィザードを使用してレポートを生成するには

1. Dr.Web [メニュー](#)  を開き、**Security Center** を選択します。
2. 開いたウィンドウで、**レポートウィザードへ移動** をクリックします。

Security Center ウィンドウの右上にある  ボタンをクリックしてこのウィンドウにアクセスすることもできます。

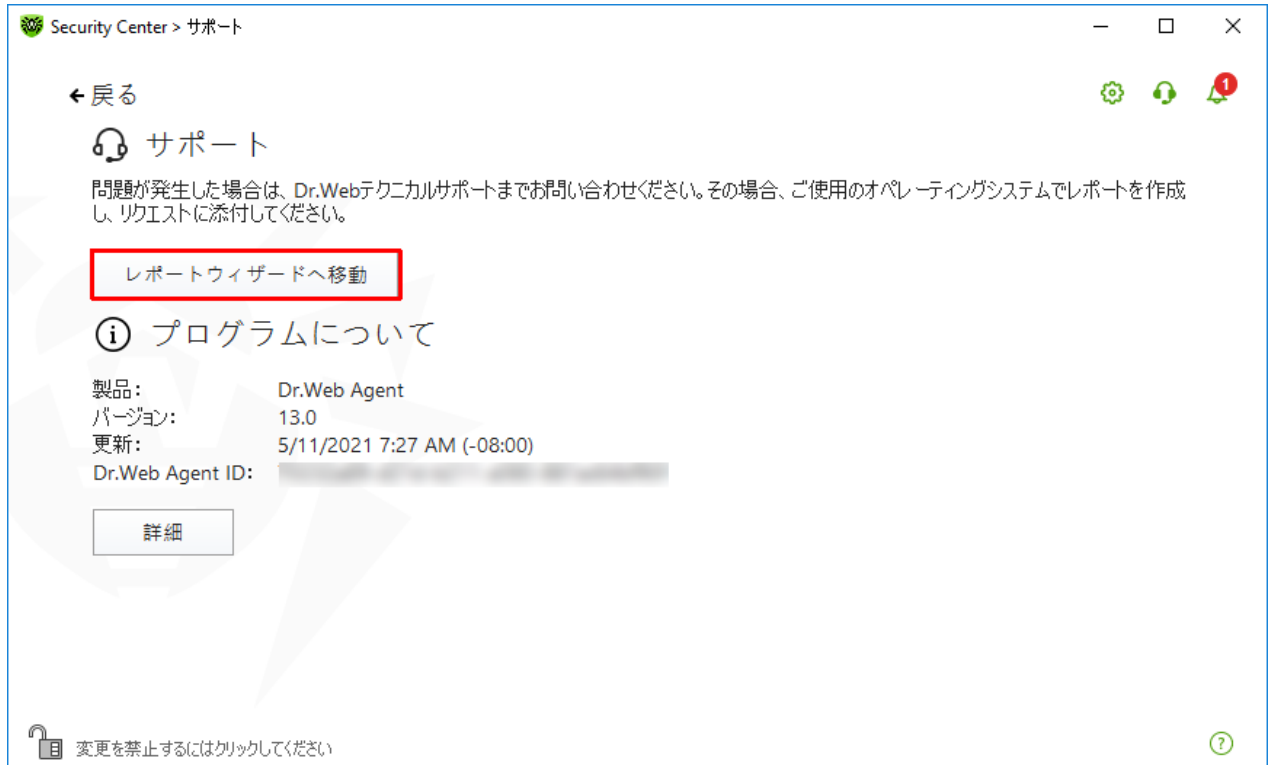


図104. サポート

3. 開いたウィンドウで、**レポートを作成する** をクリックします。

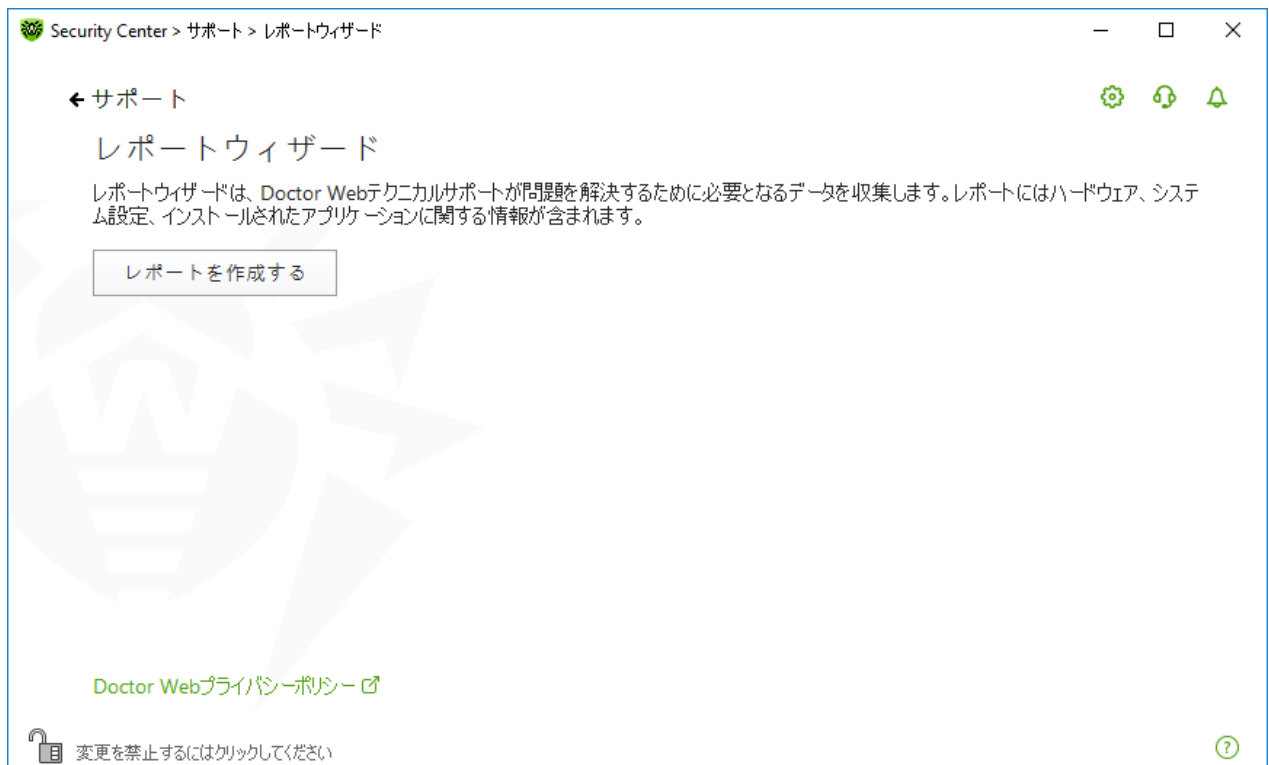


図105. テクニカルサポート用にレポートを生成する

4. レポートの生成が開始されます。



コマンドラインからのレポート作成

レポートを作成するには以下のコマンドを使用してください:

```
/auto 例: dwsysinfo.exe /auto
```

次のコマンドを使用することもできます:

```
/auto /report:[<full path to the archive>] 例:dwsysinfo.exe /auto /report:C:\report.zip
```

レポートは%USERPROFILE%フォルダのDoctor Webサブフォルダ内にアーカイブとして保存されます。アーカイブが作成された後、**フォルダを開く** ボタンをクリックすることでアーカイブにアクセスできます。

レポートに含まれる情報

レポートには以下の情報が含まれます。

1. OSに関する技術的情報

- お使いのコンピューターに関する概要
- 実行中のプロセスに関する情報
- スケジュールされたタスクに関する情報
- サービス、ドライバに関する情報
- デフォルトのブラウザに関する情報
- インストールされているアプリケーションに関する情報
- ポリシーに関する情報
- HOSTSファイルに関する情報
- DNSサーバーに関する情報
- システムイベントログ
- システムフォルダ一覧
- レジストリブランチ
- Winsock プロバイダ
- ネットワーク接続
- デバッガDr.Watsonのログ
- パフォーマンスインデックス

2. インストールされているDr.Web製品に関する情報:

- Dr.Web製品の種類とバージョン
- インストールされているコンポーネントとDr.Webモジュールに関する情報
- Dr.Web製品の設定と設定パラメータに関する情報
- ライセンス情報
- Dr.Webの動作ログ

Dr.Webに関する情報は、アプリケーションとサービスのログ→**Doctor Web**のイベントビューアにあります。

16.2. プログラムについて

プログラムについて セクションには、以下の情報が表示されます。

- 製品バージョン
- 最終更新日時
- Dr.Web Agent ID

Dr.Webについて ウィンドウには、インストールされているコンポーネントのバージョンとウイルスデータベースの更新日に関する情報が表示されます。

このウィンドウにアクセスするには

1. Dr.Web メニュー Dr.Web icon を開き、サポート を選択します。
2. 開いたウィンドウで、詳細 をクリックします。

Security Center ウィンドウの右上にある  ボタンをクリックしてこのウィンドウにアクセスすることもできます。

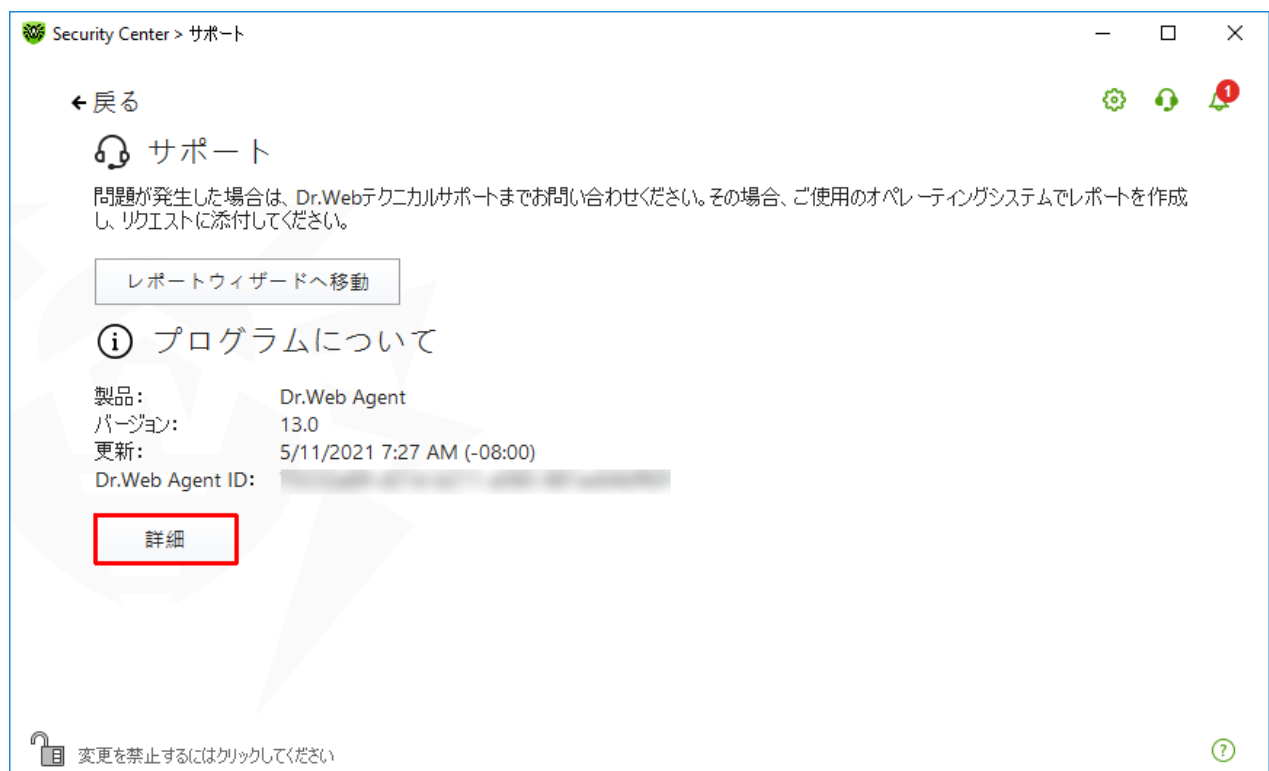


図106.Dr.Webについて ウィンドウへのアクセス



17. 付録A.追加の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(スイッチ)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。Dr.Web Scanner、Console Scanner で使用可能です。設定ファイルには無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も高いプライオリティを持ちます。

スイッチは (/) 記号で始まり、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。

17.1. ScannerとConsole Scannerのパラメータ

スイッチ	説明
/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)
/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。
/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。
/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(デフォルト:無制限)。
/ARL: <ネスティングレベル>	アーカイブの最大ネスティングレベル(デフォルト:無制限)
/ARS: <サイズ>	最大アーカイブサイズ(デフォルト:無制限、単位: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(デフォルト:無制限、単位:KB)
/ARX: <サイズ>	スキャンの対象となるアーカイブ内ファイルの最大サイズ(デフォルト:無制限、単位:KB)
/BI	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。
/CUSTOM	カスタムスキャンを実行します。追加のパラメータが指定されている場合(スキャンするオブジェクト、または /TM や /TBパラメータなど)、指定されたオブジェクトのみをスキャンします。(Scannerのみ)
/DCT	予測されるスキャン所要時間を表示しません。(Console Scannerのみ)
/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: <スレッド数>	指定されたスレッド数でスキャンを実行します。



スイッチ	説明
/FAST	システムの クイックスキャン を実行します。追加のパラメータが指定されている場合（スキャンするオブジェクト、または /TM や /TB パラメータなど）、指定されたオブジェクトもスキャンされます。（Scannerのみ）
/FL: <ファイル名>	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のフルスキャンを実行します（ブートセクタを含む）。追加のパラメータが指定されている場合（スキャンするオブジェクト、または /TM や /TB パラメータなど）、クイックスキャンが実行され、指定されたオブジェクトもスキャンされます。（Scannerのみ）
/FX: <マスク>	マスクに合致するファイルのスキャンの対象から除外します。（Console Scannerのみ）
/GO	ユーザーからの回答を必要とする質問をスキップするScannerの動作モードです。選択を必要とする場合の決定は自動的に行われます。このモードは、毎日または毎週の自動ファイルスキャンを行う場合に便利です。スキャンの対象となるオブジェクトをコマンドライン内で指定する必要があります。/GO パラメータと一緒に使用することができるのは /LITE、/FAST、/FULL パラメータです。このモードでは、バッテリー駆動に切り替わった際にスキャンを停止します。
/Hまたは/?	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。
/LITE	RAMおよび全てのディスクのブートセクタの基本的なスキャンを実行し、ルートキットスキャンも行います。（Scannerのみ）
/LN	シェルリンクを解決します。デフォルトで無効になっています。
/LS	LocalSystemアカウントの権限を使用してスキャンを行います。デフォルトで無効になっています。
/MA	メールファイルのスキャンします。デフォルトで有効になっています。
/MC: <試行回数>	修復の最大試行回数を設定します（デフォルト：無制限）。
/NB	修復された、また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を制限します。スキャンに必要なメモリ容量とスキャンプロセスのシステムのプライオリティを決定します（デフォルト：無制限、単位：%）。



スイッチ	説明
/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 <code>ok</code> 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です。以下を指定することができます。 0 - 最低 L - 低い N - 通常(デフォルト設定) H - 高い M - 最高
/PAL: <ネスティングレベル>	実行パッカーの最大ネスティングレベルです。この上限を超えた場合、Scannerはスキャンを指定されたレベルまで行います。デフォルト値は1,000です。
/QL	全てのディスク上の隔離されたファイル一覧を表示します。(Console Scannerのみ)
/QL: <論理ドライブ名_文字>	指定された論理ドライブ上の隔離されたファイル一覧を表示します。(Console Scannerのみ)
/QNA	パスを二重引用符で囲みます。
/QR[:[d][:p]]	保存されている期間が<p>(数字)日を超えた、<d>(論理ドライブ名_文字)ドライブ上の隔離ファイルを削除します。<d> および <p>を指定しなかった場合、全てのドライブ上にある隔離ファイルを削除します。(Console Scannerのみ)
/QUIT	/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 Scanner を終了します。(Scanner のみ)
/RA: <ファイル名>	指定されたファイルにプログラム動作のレポートを追加します。デフォルトではロギングは無効になっています(Scannerをコマンドラインモードで実行している場合)。
/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。
/RK	ルートキットスキャンを実行します。デフォルトで無効になっています。
/RP: <ファイル名>	指定されたファイルにプログラム動作のレポートを追加します。デフォルトではロギングは無効になっています(Scannerをコマンドラインモードで実行している場合)。
/RPC: <秒>	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)



スイッチ	説明
/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: <ターゲットアドレス>	指定された動的RPCエンドポイントを使用します。(Console Scannerのみ)
/RPCH: <ホスト名>	リモートコールに、指定したホスト名を使用します。(Console Scannerのみ)
/RPCP: <プロトコル>	指定したRPCプロトコルを使用します。使用可能なプロトコルは lpc、np、tcpです。(Console Scannerのみ)
/SCC	複合オブジェクトのコンテンツを表示します。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。
/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)
/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。
/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。
/ST	Scannerをバックグラウンドモードで開始します。/GO パラメータが指定されていない場合、脅威が検出された場合のみグラフィカルモードで表示されます。このモードでは、バッテリー駆動に切り替わった際にスキャンを停止します。
/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。
/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(デフォルト:無制限、単位:秒)
/WCL	drwebwcl 互換出力(Console Scannerのみ)
/X:S[:R]	スキャンの完了後にシステムに対して行うアクションを指定します: シャットダウン、再起動、一時停止、休止 (ShutDown/Reboot/Suspend/Hibernate)。



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) :

アクション	説明
/AAD:<action>	アドウェアに対するアクション(DQIR可)
/AAR:<action>	感染したアーカイブファイルに対するアクション(DQIR可)
/ACN:<action>	感染したインストールパッケージに対するアクション(DQIR可)
/ADL:<action>	ダイアラーに対するアクション(DQIR可)
/AES:<action>	悪用可能なソフトウェアに対するアクション(IR可)
/AHT:<action>	ハッキングツールに対するアクション(DQIR可)
/AIC:<action>	修復不可能ファイルに対するアクション(DQR可)
/AIN:<action>	感染ファイルに対するアクション(CDQR可)
/AJK:<action>	ジョークプログラムに対するアクション(DQIR可)
/AML:<action>	感染したメールファイルに対するアクション(QIR可)
/ARW:<action>	リスクウェアに対するアクション(DQIR可)
/ASU:<action>	疑わしいファイルに対するアクション(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もあります。例:

/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。

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

```
[<プログラムへのパス>]dwscancl /AR- /AIN:C /AIC:Q C:\
```




"C:"ドライブ上にある、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` を指定してください。

17.2. インストールパッケージのパラメータ

`/compression <mode>` - 集中管理サーバーとの間のトラフィックの圧縮モードです。<mode>には次の値を使用することができます。

- `yes` - 圧縮を使用します。
- `no` - 圧縮を使用しません。
- `possible` - 圧縮が可能です。Server側の設定に応じて、使用するか否かを決定します。

指定されなかった場合、デフォルトで`possible`が使用されます。

`/encryption <mode>` - 集中管理サーバーとの間のトラフィックの暗号化モードです。<mode>には次の値を使用することができます。

- `yes` - 暗号化を使用します。
- `no` - 暗号化を使用しません。
- `possible` - 暗号化が可能です。Server側の設定に応じて、使用するか否かを決定します。

指定されなかった場合、デフォルトで`possible`が使用されます。

`/excludeFeatures <components>` - インストールから除外するコンポーネントのリストです。複数のコンポーネントを指定する場合は","記号で区切ってください。以下のコンポーネントを指定することができます：

- `scanner` - Dr.Web Scanner
- `spider-mail` - SpIDer Mail
- `spider-g3` - SpIDer Guard
- `outlook-plugin` - Dr.Web for Microsoft Outlook
- `firewall` - Dr.Web Firewall
- `spider-gate` - SpIDer Gate
- `parental-control` - Office Control
- `antispam-outlook` - Dr.Web for Microsoft Outlook コンポーネント向け Dr.Web Anti-spam
- `antispam-spidermail` - SpIDer Mail コンポーネント向け Dr.Web Anti-spam

正しく指定されなかったコンポーネントにはデフォルトのインストールステータスが適用されます。

`/id <station_id>` - Dr.Web Agent がインストールされる端末のIDです。

Serverでの自動認証を行うには `/pwd` と共にパラメータを指定してください。認証パラメータが設定されなかった場合、認証の決定はServer側で行われます。

`/includeFeatures <components>` - インストールする必要があるコンポーネントのリストです。複数のコンポーネントを指定する場合は","記号で区切ってください。以下のコンポーネントを指定することができます：

- `scanner` - Dr.Web Scanner



- spider-mail - SpIDer Mail
- spider-g3 - SpIDer Guard
- outlook-plugin - Dr.Web for Microsoft Outlook
- firewall - Dr.Web Firewall
- spider-gate - SpIDer Gate
- parental-control - Office Control
- antisipam-outlook - Dr.Web for Microsoft Outlook コンポーネント向け Dr.Web Anti-spam
- antisipam-spidermail - SpIDer Mail コンポーネント向け Dr.Web Anti-spam

正しく指定されなかったコンポーネントにはデフォルトのインストールステータスが適用されます。

`/installdir <folder>` - インストールフォルダです。

指定されなかった場合、デフォルトでシステムドライブ上のProgram Files\DrWebフォルダにインストールされます。

`/instMode <mode>` - インストーラの起動モードです。<mode>には次の値を使用することができます。

- remove - インストールされたプロダクトを削除します。

指定されなかった場合、起動モードはデフォルトでインストーラが自動的に決定します。

`/lang <language_code>` - インストーラの言語です。言語コードはISO-639-1で指定します。

指定されなかった場合、デフォルトでシステム言語が使用されます。

`/pubkey <path>` - Server証明書またはパブリックキーファイルへのフルパスです。

証明書またはパブリックキーが指定されなかった場合、ローカルインストールの実行後、インストーラは自動で実行フォルダの証明書(.pem拡張子)またはパブリックキー(drwcsd.pub)を使用します。証明書またはパブリックキーファイルがインストール実行フォルダ以外の場所にある場合、そこへのフルパスを手動で指定する必要があります。

Control Center内で生成されたインストールパッケージを実行する場合、パブリックキーはインストールパッケージに含まれています。コマンドラインパラメータでパブリックキーを指定する必要はありません。

`/pwd <password>` - Dr.Web Agent がServerにアクセスするためのパスワードです。

Serverでの自動認証には/idと共にパラメータを指定してください。認証パラメータが設定されなかった場合、認証の決定はServer側で行われます。

`/regagent <mode>` - インストールされたプログラムのリスト内に Dr.Web Agent を登録するかどうかを指定します。<mode>には次の値を使用することができます。

- yes - リスト内に Dr.Web Agent を登録します。
- no - リスト内に Dr.Web Agent を登録しません。

指定されなかった場合、デフォルトでnoが使用されます。

`/retry <number>` - マルチキャストリクエストを送信してServerの検索を試行する回数の上限です。指定された回数内にServerから応答がなかった場合、Serverは見つからなかったと判断されます。



指定されなかった場合、Serverの検索試行は3回まで行われます。

`/server "[<protocol>/]<server_address>[:<port>]"` - Dr.Web Agent のインストールが開始される Serverであり、インストール後に Dr.Web Agent が接続されるServerのアドレスです。

指定されなかった場合、デフォルトでマルチキャストリクエストの送信によってServerを検索します。

`/silent <mode>` - インストーラをバックグラウンドモードで実行するかどうかを指定します。<mode>には次の値を使用することができます。

- `yes` - インストーラをバックグラウンドモードで実行します。
- `no` - インストーラをグラフィカルモードで実行します。

指定されなかった場合、Dr.Web Agent のインストールはデフォルトでグラフィカルモードで実行されます。

`/timeout <time>` - Server検索の際に応答を待つ時間の上限です(秒)。タイムアウトの時間内は応答メッセージの受信を続けます。

指定されなかった場合、デフォルトで3 秒になります。

17.3. リターンコード

リターンコードと、それに対応するイベントは以下のとおりです：

リターンコードの値	イベント
0	ウイルスは見つかりませんでした。
1	既知のウイルスが検出されました。
2	既知のウイルスの亜種が検出されました。
4	疑わしいオブジェクトが見つかりました。
8	ファイルアーカイブ、メールアーカイブ、またはコンテナ内で既知のウイルスが検出されました。
16	ファイルアーカイブ、メールアーカイブ、またはコンテナ内で既知のウイルスの亜種が検出されました。
32	ファイルアーカイブ、メールアーカイブ、またはコンテナ内で疑わしいオブジェクトが見つかりました。
64	少なくとも1つの感染したオブジェクトが修復されました。
128	少なくとも1つの感染した、または疑わしいファイルが削除／名前変更／隔離されました。

プログラムによって返される実際の値は、スキャン中に発生したイベントに対応するコードの合計値になります。合計値は各イベントコードに分解することができます。



例えば、リターンコード $9 = 1 + 8$ は、既知のウイルスが検出され、それらにはアーカイブ、メールアーカイブ、またはコンテナ内のウイルスが含まれ、修復などのアクションは実行されず、スキャン中にその他の「ウイルス」イベントは発生していないことを意味します。



18. 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)が益々広く拡散されるようになってきました。その発達はコンピューターサイエンスの誕生と同時に始まり、それらに対抗するための保護テクノロジーもまた並行する形で進化を遂げてきました。しかしながら、そのようなプログラムの進化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介して拡散されます。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よう設計され、完全に自動モードで動作することができるものもあります。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、最も一般的かつ広く拡散され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する保護を提供します。

18.1. コンピューターの脅威のタイプ

本マニュアルにおける「脅威」とは、コンピューターやネットワークに対して潜在的または直接的にダメージを与える、あるいはユーザーの情報や権利を危険にさらす可能性のある、あらゆるソフトウェア(すなわち悪意のある、またはその他の不審なプログラム)を意味します。ただし、一般的に「脅威」という言葉は、コンピューターやネットワークセキュリティに対するあらゆる潜在的な危険(すなわち、攻撃に悪用される可能性のある脆弱性)を指して使用される場合があります。

下記に記載するプログラムはすべて、ユーザーのデータや機密性を脅かす機能を持っています。自身の存在をユーザーから隠さないプログラム(スパムを送信するソフトウェアやトラフィックアナライザなど)は状況によっては脅威と成り得ますが、通常はコンピューター脅威としては見なされません。

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)ことができ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。

Doctor Web では、コンピューターウイルスは感染させるオブジェクトに応じて次のカテゴリーに分類されます。

- **ファイルウイルス** - OSファイルを感染させ(通常、実行ファイルとダイナミックライブラリ)、それらが実行されると同時に起動します。
- **マクロウイルス** - Microsoft Office、またはマクロコマンド(通常、Visual Basicで記述されている)に対応しているその他のプログラム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(マクロ)で、特定の状況下で起動されます(例えばMicrosoft Wordでは、ドキュメントを開く、閉じる、または保存すると自動的にマクロが開始されます)。
- **スクリプトウイルス** - スクリプト言語を使用して作成され、多くの場合、別のスクリプト(OSサービスファイルなど)を感染させます。Webアプリケーション内の脆弱なスクリプトを悪用することで、スクリプトの実行に対応しているその他の種類のファイルを感染させることもできます。



- **ブートウイルス** - ディスクのブートセクター、ハードディスクのパーティションやマスターブートレコードを感染させます。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、そのタスクを続けることができます。

多くのウイルスは自身を検出から保護するための特別なメカニズムを持ち、これらのメカニズム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す。使用する保護手法に応じて、ウイルスは次の2つのグループに分類することができます。

- **暗号化ウイルス** - 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。このウイルスのサンプルは全て、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** - コード暗号化の他に特別な復号化プロシージャを用います。このプロシージャは各コピーごとに異なっています。つまり、この種類のウイルスはバイトシグネチャを持ちません。
- **ステルスウイルス(インビジブルウイルス)** - 特定のアクションを実行して、感染したオブジェクトでの活動と存在を隠します。このようなウイルスは、オブジェクトを感染させる前にそのオブジェクトの特性を収集し、スキャナーが変更されたファイルを探し出す際に誤認させるための「ダミー」特性を作り出します。

ウイルスは、記述された言語(多くの場合はアセンブリで書かれていますが、高度なプログラミング言語やスクリプト言語などで書かれたウイルスもあります)や感染させるOSに応じて分類することもできます。

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も広く拡散されるようになってきています。ウイルス同様、自身を複製することができますが、他のオブジェクトを感染させることはありません。ネットワークからコンピューターに侵入し(通常、メールの添付ファイルとして)、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拡散します。拡散はユーザーのアクションに応じて、または自動的に開始されます。

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)内にロードされる、いわゆる感染部分(シェルコード)を持っています。その後、シェルコードによって、ワームのボディがネットワーク経由で実行ファイルとしてダウンロードされます。シェルコードがシステム内に存在するだけであれば、システムを再起動することで(RAMが削除されリセットされます)ワームを削除することができますが、ワームのボディがコンピューターに侵入してしまった場合はアンチウイルスプログラムでなければ対処できません。

ワームはその拡散速度によって、例えペイロードを持っていない(システムに直接的な被害を与えない)場合であっても、ネットワーク全体の機能を損なう能力を持っています。

Doctor Webでは、拡散手法に応じてワームを以下のように分類します。

- **ネットワークワーム** - 様々なネットワークおよびファイル共有プロトコル経由で拡散されます。
- **メールワーム** - メールプロトコル(POP3、SMTPなど)経由で拡散されます。
- **チャットワーム** - 広く使用されているメッセージャーがチャットプログラム(ICQ、IM、IRCなど)のプロトコルを使用します。

トロイの木馬

これらのプログラムは自己複製しません。トロイの木馬は頻繁に使用されるプログラムを置き換え、自身の機能を実行(またはその動作を模倣)します。一方で、システム内で悪意のある行為(データの破損または削除、秘密情報の送信など)を行ったり、ハッカーが許可なくコンピューターにアクセスできるようにしたりするなど、第三者のコンピューターに損害を与える可能性があります。



ウイルス同様、トロイの木馬もまた様々な悪意のある動作を実行し、ユーザーから自身の存在を隠すほか、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、多くのトロイの木馬は、ユーザーまたは特定のシステムプロセスによって起動される個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、リムーバブルストレージ、メール添付ファイルなどを介して)。

トロイの木馬はウイルスやワームによって拡散される場合があり、また、トロイの木馬の実行する悪意のある動作の多くが他の種類の脅威によっても実行されうることから、その分類が難しくなっています。以下のトロイの木馬は、Doctor Webでは個別のクラスとして分類されています。

- **バックドア** - 犯罪者が保護メカニズムをすり抜けてシステムにアクセスすることを可能にするトロイの木馬です。バックドアはファイルを感染させることはなく、レジストリキーを改変することで自身をレジストリ内に登録します。
- **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。また、その他のプログラムのプロセスやレジストリキー、フォルダ、ファイルを隠すことができます。個別のプログラムとして、または他の悪意のあるアプリケーションのコンポーネントとして拡散されます。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ブライ機能を妨害し、一方、KMRはシステムのカーネルレベルで機能を妨害し、その検出を困難にします。
- **キーロガー** - ユーザーがキーボードを使用して入力したデータを記録します。これらの悪意のあるプログラムは様々な機密情報(ネットワークパスワード、ログイン、バンクカードデータなど)を盗むことができます。
- **クリックカー** - Webサイトのトラフィックを増加させる、またはDos攻撃を実行するためにユーザーを特定のインターネットリソースへリダイレクトします。
- **プロキシサーバー型トロイの木馬** - サイバー犯罪者に対し、被害者のコンピューターを経由した匿名でのインターネットアクセスを提供します。

トロイの木馬は上記以外の悪意のある動作を実行することも可能です。例えば、ブラウザのホームページを変更したり、特定のファイルを削除することができます。ただし、それらの動作はその他の種類の脅威(ウイルスまたはワーム)によっても実行されることがあります。

ハッキングツール

ハッキングツールは、侵入者によるハッキングを可能にするプログラムです。最も一般的なものは、ファイアーウォールまたはコンピューター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はなく、管理者がネットワークのセキュリティを検査するためにも用いられます。ハッキングにも使用することのでき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ハッキングツールに分類されることがあります。

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。その目的はユーザを脅えさせたり、不快感を与えたりすることにあります。



ダイアラー

これらは、さまざまな電話番号をスキャンし、モデムが応答する番号を見つけるために設計された特別なプログラムです。これらの番号は、電話機能の価格をマークアップするため、または高価な電話サービスにユーザーを接続するために使用されます。

リスクウェア

コンピューター脅威として意図されたものではないプログラムです。しかし、その機能によってシステムセキュリティを脅かす可能性があるため軽微な脅威として分類されます。リスクウェアには、データを破損または削除してしまう危険性のあるプログラムのほか、ハッカーや悪意のあるアプリケーションによってシステムに害を与えるために利用される可能性のあるプログラムが含まれます。そのようなプログラムには、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。

疑わしいオブジェクト

ヒューリスティックアナライザによって検出される、潜在的なコンピューター脅威です。このようなオブジェクトには、あらゆる種類の脅威(情報セキュリティスペシャリストにとって未知のものでさえも)が含まれ、また、誤検出の際には安全なオブジェクトであることが判明する場合があります。疑わしいオブジェクトを含むファイルは隔離へ移動し、解析のために Doctor Web アンチウイルスラボへ送信することを強く推奨します。

18.2. 脅威に対するアクション

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

1. **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。
2. **隔離** - 悪意のあるオブジェクトを特別なフォルダに移し、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や、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ため Doctor Web のアンチウイルスラボに送信することを推奨します。
3. **削除** - コンピューター脅威を駆除する最も効果的なアクションで、あらゆる種類の悪意のあるオブジェクトに対して適用可能です。オブジェクトが悪意のあるコードのみで構成され有益な情報を持っていない場合(例えばコンピューターワームの修復は、そのコピーを全て削除することを意味します)、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このアクションが適用されることがあります。
4. **ブロック** - 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、またはファイルへのアクセスを全てブロックします。



19. 付録C.ウイルスの名称

Dr.Webコンポーネントによって脅威が検出されると、ユーザーインターフェースにはDoctor Webスペシャリストによって付けられた脅威の名前が表示されます。これらの名称はある特定の原則に基づいており、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せん。そのような原則を知ることは、保護するシステム上のソフトウェアや脆弱性を理解する上で有益であると考えられます。ウイルスの分類に関する最新の情報は <https://vms.drweb.com/classification/> を参照してください。

この分類方法は、同時に複数の特徴を有するウイルスもあることから形式的になる場合があり、また全てを網羅したものではありません。新しい種類のウイルスが次々と出現し続け、その分類は正確さを増していくためです。

ウイルスの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。

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 - 16ビットのWindows 3.1プログラム
- Win95 - 32ビットのWindows 95/98/Me プログラム
- WinNT - 32ビットのWindows NT/2000/XP/Vista/7/8/8.1/10プログラム
- Win32 - 32ビットのWindows 95/98/Me およびNT/2000/XP/Vista/7/8/8.1/10プログラム
- Win64 - 64ビットのWindows XP/Vista/7/8/8.1/10/11プログラム
- Win32.NET - Microsoft .NET Framework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できるウイルスもありますので注意してください。

マクロウイルス

以下のプレフィックスは、MS Officeのオブジェクトを感染させる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を感染させます)

開発言語

C、C++、Pascal、Basicなどの高級プログラミング言語で記述されたウイルスの名称には HLL グループが使用されます。関数アルゴリズムを指定するには、次の修飾子を使用できます。

- 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

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ー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

脆弱性を悪用するツール

- Exploit - OSやアプリケーションの既知の脆弱性を悪用し、システム内にマルウェアを侵入させたり許可されていないアクションを実行したりするためのツールです

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。

スクリプトウイルス

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

- VBS - Visual Basic Script
- JS - Java Script
- Wscript - Visual Basic Script または Java Script
- Perl - Perl
- PHP - PHP
- BAT - MS-DOS コマンドインタプリタ

悪意のあるプログラム

以下のプレフィックスは、ウイルスではない悪意のあるプログラムに使用されます。

- 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、または有料のリソース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 (ハッキングツール)

その他

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。

- `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なものであり、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



20. 付録D.主な用語と概念

あ

アンチウイルスネットワークは、1つのローカルネットワークに接続されている、Dr.Web製品（Dr.Web Anti-virus for Windows、Dr.Web Anti-virus for Windows Servers、Dr.Web Security Space）がインストールされたコンピューターの複合体です。

う

ウイルスの**亜種**は、検出はされるものの元のウイルスに対する修復アルゴリズムを適用することができない、既知のウイルスに対する改変の結果となるコードです。

え

エクスプロイトは、ソフトウェアの脆弱性を利用してシステムを攻撃するプログラム、コード片、または一連のコマンドです。

エミュレーションは、特別なコンピュータプログラムの使用中に機能が欠けたり結果が変わったりすることのない、別のシステムを使用したシステム動作の模倣です。

か

管理者モードは、ユーザーがすべてのセキュリティコンポーネント設定とプログラム設定にアクセスできるDr.Webのモードです。管理者モードに切り替えるには、ロック  をクリックします。

こ

更新ミラーは、ローカルネットワークの他のコンピューターの更新元として設定されたコンピューターです。

し

信頼できるアプリケーションは、drwbase.dbの信頼できる署名のリストにデジタル署名が追加されているアプリケーションです。信頼できるアプリケーションのリストには、Google Chrome、Firefox、Microsoftアプリケーションなどの一般的なソフトウェアが含まれています。

て

デジタル署名は、偽造からドキュメントを保護するために付加されるデジタルドキュメントの属性です。デジタル署名の秘密鍵によって情報を暗号化することによって生成されます。証明書に含まれる秘密鍵の所有者を識別し、送信されたデジタルドキュメントが改ざんされていないことを証明することができます。

デバイスクラスは、同じ機能を実行するデバイス（印刷デバイスなど）です。



は

バスは、コンピューターの機能的ユニット（USBなど）間でデータを転送するための通信サブシステムです。

ハッシュ値は一意のファイル識別子、すなわち、特定の長さの数字と文字による列です。ハッシュはデータの整合性を検証するために使用されます。

ひ

ヒューリスティックは、その統計的有意性が実験的に確認されている仮定です。

