Dr.WEB
Security Space

ユーザーマニュアル

Dr.Web Security Space
バージョン12.0
ユーザーマニュアル
2024/02/02

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。

世界中の個人ユーザーから政府機関、中小企業、大企業まで幅広いカスタマーに支持されています。

Dr.Webアンチウイルスソリューションは、マルウェア検出と国際情報セキュリティ基準への準拠における持続的な卓越性によって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数々の認定や賞、そして世界中に広がるユーザーが、製品の持つ並外れた信頼性を示す何よりの証です。

Dr.Web製品をご利用いただき誠にありがとうございます。

目次

1. はじめに

このマニュアルには、Dr.Web Security Space製品のインストール方法、使用方法、ウイルスの脅威による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
	エラーの可能性や特に注意を必要とする重要な注意事項に関する警告
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エレメントの名称
CTRL	キーボードのキーの名称
`C:\Windows\`	ファイルやフォルダの名前、コード例
付録 A	マニュアル内の別の章への相互参照や外部Webページへのハイパーリンク

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 Security Space
- 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）
- UNC - Uniform Naming Convention（汎用名前付け規則）
- 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 Security Space 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 Security Space 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サイトカテゴリーのデータベース、およびメールスパムのフィルタリングルールに定期的に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 Security Space 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 Security Space 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。
Parental 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

コンポーネント／モジュール	説明
	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	オンデマンドでまたはスケジュールに従って起動し、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。
Dr.Web Updater	登録ユーザーがウイルスデータベースとDr.Webモジュールの更新を受信して自動的にインストールできるようにするモジュール。
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。常時更新されていくDr.Web Cloudサービスと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、パ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）

Dr.Web ShellGuard は悪意のある動作を検出するために、ローカルで保存されていく情報のほか、Dr.Web Cloudサービスの以下のデータも使用します。

- 悪意のあるプログラムのアルゴリズムに関する情報
- 既知のクリーンなファイルに関する情報

- よく知られたソフトウェアデベロッパーの悪用されたデジタル署名に関する情報
- アドウェアおよびリスクウェアによって使用されるデジタル署名に関する情報
- 閲覧が望ましくないWebサイトに関する情報
- 特定のアプリケーションによって使用される保護アルゴリズム

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 Cloudサービスのブラックリストまたはホワイトリストに含まれているかどうか

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
- Dr.Web Cloudサービスにある、アプリケーションのブラックリストまたはホワイトリストに含まれているかどうか

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。クラウドサービスへの接続により、大量のデータがより速く処理され、システムの継続的なトレーニングにより、最新の脅威からの予防的保護が提供されます。このテクノロジーは、クラウドへの常時接続がなくても機能することができます。

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。

クラウドベースの脅威検出テクノロジー

クラウドベースの検出方法では、あらゆるオブジェクト（ファイル、アプリケーション、ブラウザ拡張機能など）をハッシュ値によってスキャンします。ハッシュは、特定の長さの数字と文字からなる一意のシーケンスです。ハッシュ値による分析では、オブジェクトは既存のデータベースを使用してスキャンされ、カテゴリー別に分類されます（クリーン、疑わしい、悪意のある、など）。クラウドベースのテクノロジーを使用して検出されたオブジェクトは、名前に `CLOUD` プレフィックスが付けられます。

このテクノロジーにより、ファイルスキャンの時間を最適化し、デバイスリソースを節約することができます。分析されるのはオブジェクトではなく、その固有のハッシュ値であるため、オブジェクトが悪意のあるものであるかどうかの決定はほとんど瞬時に行われます。Dr.Webのサーバーに接続されていない場合、ファイルはローカルでスキャンされ、接続が復元されるとクラウドスキャンが再開されます。

Doctor Webクラウドサービスは多くのユーザーから情報を収集し、これまで未知であった脅威に関するデータを迅速に更新します。これにより、デバイス保護の効果を高めます。

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

パラメータ	要件
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： • 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 22H2以前 64ビットプラットフォームの場合： • Windows Vista Service Pack 2以降 • Windows 7 Service Pack 1以降 • Windows 8 • Windows 8.1 • Windows 10 22H2以前 • Windows 11 22H2以前
RAM空き容量	512 MB以上
画面解像度	1024x768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。 • VMware • Hyper-V • Xen • KVM
その他	Microsoft Outlook用のDr.Webプラグインには、Microsoft Officeスイートの以下のMicrosoft Outlookクライアントのうちいずれか一つが必要です。 • 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またはWindows 7に Dr.Web Security Space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。

Dr.Webが正常に動作するために、以下のポートが開いている必要があります。

目的	方向	ポート番号
ライセンスの有効化と更新のため	送信	443
更新を受け取るため（httpsを使用して更新するオプションが有効になっている場合）	送信	443
更新を受け取るため	送信	80
メール通知を送信するため		25または465（またはメール通知の設定による）
Dr.Web Cloudに接続するため	送信	443（TCP） 2075（UDPを含む） 3010（TCP） 3020（TCP） 3030（TCP） 3040（TCP）

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、テストファイルの実行を終了させることはなく、またテストファイルは悪意あるファイルとして処理されません。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。

CloudCarファイルを使用してアンチウイルスの動作を検査する

Dr.Web Cloud サービスを確認するには、AMTSO（Anti-Malware Testing Standards Organization）のCloudCarテストファイルを使用します。このファイルは、クラウドサービスの動作を確認するために特別に作成されています。これはウイルスではありません。

Dr.Web Cloud の動作を確認するには

1. SpIDer Gate コンポーネントがインストールされている場合は、一時的に無効にします。Dr.Web Cloud サービスの使用が有効になっていることを確認します。
2. テストファイルをダウンロードします。ダウンロードするには、http://kettle.dev.drweb.com/public/cloudcar.exe（EXE、7 KB）にアクセスします。
3. SpIDer Guard がインストールされ有効になっている場合、ファイルがコンピューターに保存された後、Dr.Webはファイルを自動的に隔離に移動します。SpIDer Guard コンポーネントがインストールされていないか無効になっている場合は、ダウンロードしたファイルをスキャンしてください。これを行うには、ファイル名を右クリックし、コンテキストメニューの **Dr.Webでスキャン** オプションを選択します。
4. テストファイルがDr.Webによって `CLOUD:AMTSO.Test.Virus` として処理されていることを確認してください。脅威名の接頭辞 `CLOUD` は、Dr.Web Cloud が正しく動作していることを示しています。
5. SpIDer Gate コンポーネントが無効になっている場合は、手順1に従って有効にします。

3. Dr.Webのインストール、アンインストール、変更

Dr.Web Security Space 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すべてインストールします（Windows 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、ファイアーウォールをすべてコンピューターから削除します。
- 動作中のアプリケーションをすべて閉じてください。

> ⚠ Dr.Webをインストールするには管理者権限が必要です。
>
> Dr.Webは、サードパーティのプロアクティブなセキュリティ製品と互換性がありません。

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. 製品をインストールする

> ⚠ Dr.Webをインストールするには管理者権限が必要です。

ウィザードモードでのインストール

通常インストールを開始するには、以下のうちいずれかを実行してください。

- 実行ファイル（`drweb-12.0-ss-win.exe`）がある場合は、それを実行します。
- インストールパッケージが含まれている元のディスクがある場合は、そのディスクをCD／DVDドライブに挿入します。自動実行が有効になっている場合は、インストールが自動的に開始します。自動実行が無効になっている場合は、インストールキットの `autorun.exe` ファイルを手動で実行します。ウィンドウが開き、自動実行メニューが表示されます。**インストール** をクリックします。

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。
- **キャンセル** をクリックするとインストールを中止します。

プログラムをインストールするには

1. コンピューター上に他のアンチウイルスソフトウェアがインストールされていた場合、インストールウィザードはDr.Webと他のアンチウイルス間の非互換性について警告し、その削除を勧めます。

   ウィザードはインストールを開始する前に、インストールファイルが最新のものであるかどうかを確認します。より新しいインストールファイルが存在した場合、そちらをダウンロードするようユーザーに対して提案します。

2. インストール手順の最初のステップで、脅威に関する最新の情報（情報はリアルタイムに更新されます）を使用したスキャンを可能にする Dr.Webクラウドサービス に接続するように求められます。このオプションは、デフォルトで有効になっています。Dr.Web Firewall をインストールするかどうかを指定することもできます。

図 1. インストールウィザード

3. デフォルトのインストール設定を使用する場合は、手順4に進みます。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** をクリックしてください。

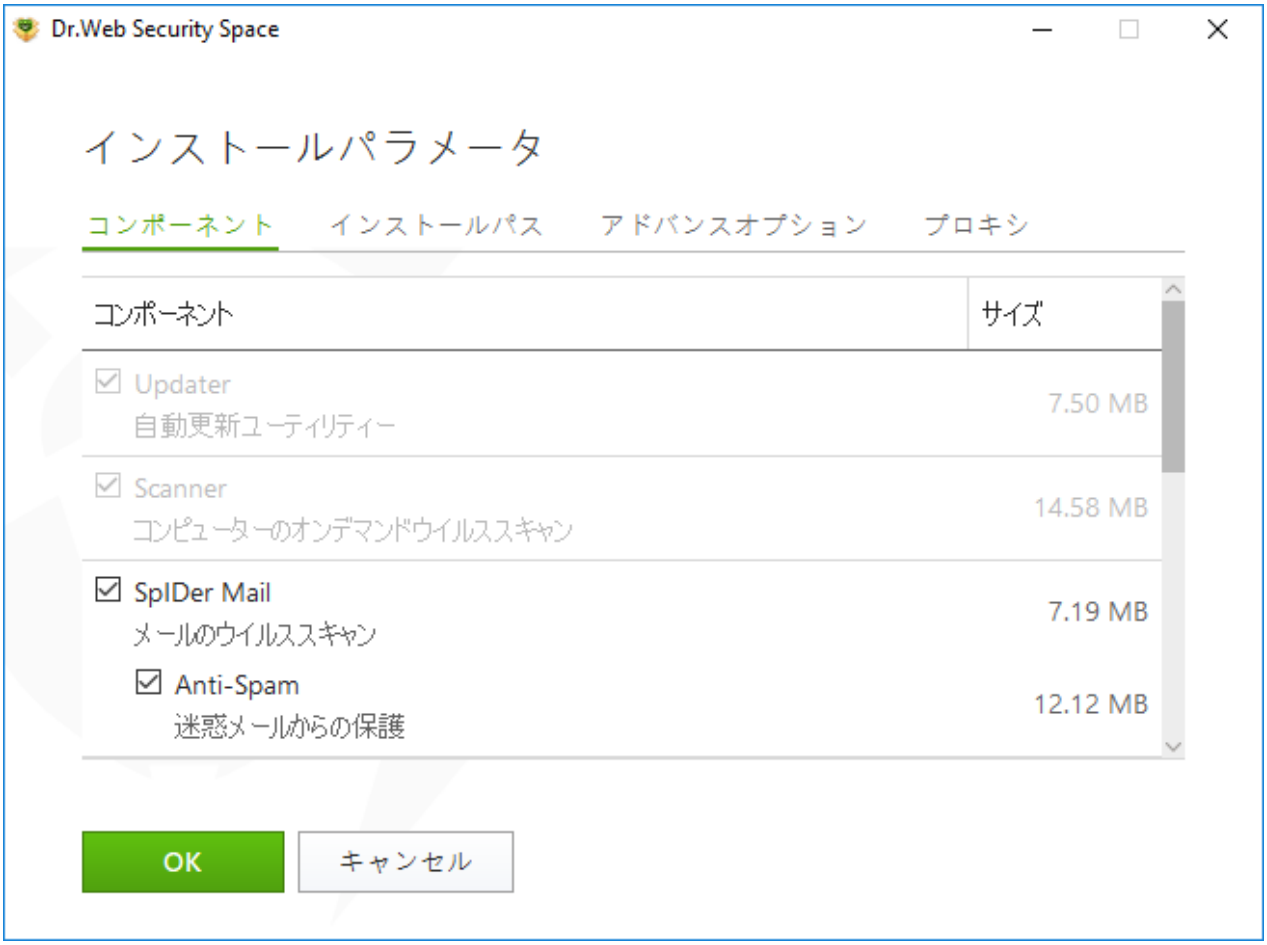

図 2. インストールパラメータ

このオプションは上級ユーザー向けです。

- 1つ目のタブで、インストールするコンポーネントを指定することができます。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。
- 2つ目のタブで、インストールパスを変更できます。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 `DrWeb` 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。
- 3つ目のタブで、ウイルスデータベースやその他のプログラムコンポーネントの更新をダウンロードするための **インストール中に更新する** オプションを有効にできます。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するには **スクリーンリーダーとの互換性を有効にする** オプションを有効にします。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。このタブでは、Dr.Webへのショートカットを作成するように求められます。
- 必要に応じ、プロキシサーバーのパラメータを設定してください。

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場合は **キャンセル** をクリックします。

4. **次へ** をクリックします。次へをクリックすることで、使用許諾契約書に同意したものとみなされますのでご注意ください。
5. **登録ウィザード** ウィンドウで次のうちいずれか1つを選択してください。
   - キーファイル がハードドライブまたはリムーバブルメディアに存在する場合は、**有効なキーファイルのパスを指定する** を選択します。**参照** をクリックしてダイアログボックスでキーファイルを選択します。詳細については、キーファイルを使用したアクティベーション セクションを参照してください。

- ライセンス無し でインストールを続行する場合、**後でライセンスを取得する** を選択してください。キーファイルを指定または取得するまで更新は利用できません。

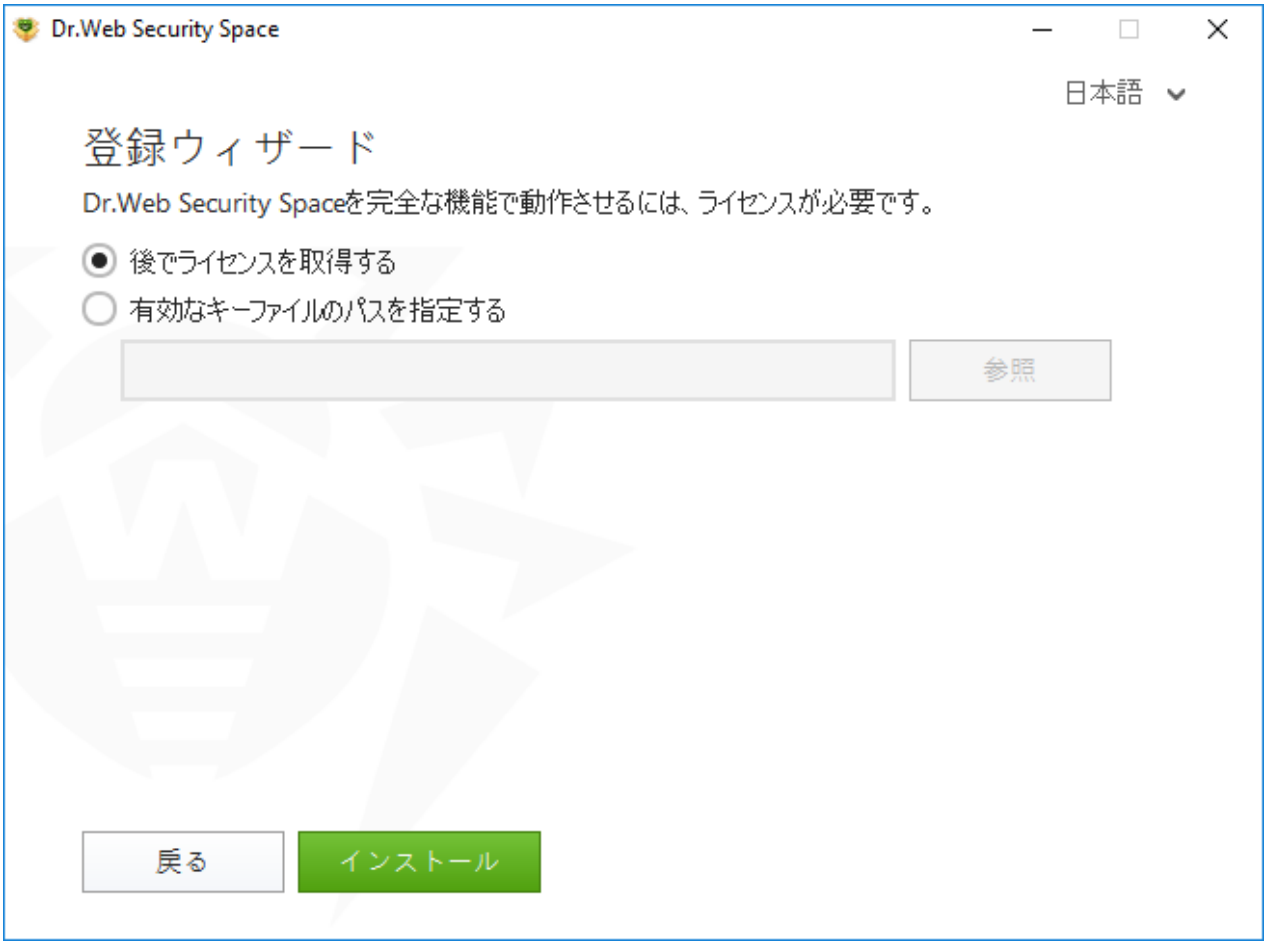

図 3. 登録ウィザード

インストール

6. インストール中にキーファイルを指定し、**インストール中に更新する** チェックボックスのチェックを外さなかった場合、ウィザードがウイルスデータベースおよび他のDr.Webコンポーネントを更新します。更新は自動的に開始され、ユーザーの操作は必要ありません。
7. インストールを完了するには、コンピューターを再起動してください。

コマンドラインからのインストール

バックグラウンドモードでDr.Webのインストールを開始するには、実行ファイル名を入力してコマンドラインで必要なパラメータを指定してください。

パラメータ	値
`installFirewall`	Dr.Web Firewallをインストールします。
`lang`	インストールに使用される言語。このパラメータの値は、ISO 639-1形式で指定します（例：`/lang en`）。

パラメータ	値
reboot	インストールが完了したら、コンピューターを自動的に再起動します。yes または no の値を使用できます。
silent	バックグラウンドモードでのインストール。yes または no の値を使用できます。
blockEmulateUserActions	インストール中に **ユーザーエミュレーションの禁止** オプションを有効にします。yes または no の値を使用できます。
allowUiAccessibility	インストール中にスクリーンリーダーとの互換性オプションを有効にします。yes または no の値を使用できます。
importSettings	ファイルから設定をインポートします（最大ファイルサイズは20 MBです）。ファイルへのパスを指定する必要があります。
enableDebugLogs	デバッグログを有効にします。yes または no の値を使用できます。デバッグログは、SpIDer Guard、SpIDer Mail、SpIDer Gate、Scanner、Dr.Web Updater、Dr.Web Serviceで有効になっています。インストール完了後にコンピューターを再起動すると、ログは無効になります。

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

```
drweb-12.0-ss-win.exe /silent yes /reboot yes
```

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（ベースフィルターエンジンサービス）を実行する必要があります。このサービスが存在しない場合や破損している場合、Dr.Webはインストールできません。BFEサービスの破損や不在は、コンピューター上にセキュリティ脅威が存在していることを示唆する場合があります。

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CureIt!を使用してシステムをスキャンします。CureIt!はDoctor Webの公式サイト https://free.drweb.com/download+cureit+free/ からダウンロードすることができます。
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。
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。

3.2. コンポーネントを設定する

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. 以下を選択します(コンピュータにインストールされているオペレーティングシステムによって異なります)。

OS	アクション			
Windows XP	スタートメニュー	スタート → コントロールパネル → プログラムの追加と削除		
	クラシックスタートメニュー	スタート → 設定 → コントロールパネル → プログラムの追加と削除		
Windows Vista	スタートメニュー	スタート → コントロールパネル	クラシックビュー	プログラムと機能
			ホームページ	プログラム → プログラムと機能
	クラシックのスタートメニュー	スタート → 設定 → コントロールパネル → プログラムの追加と削除		
Windows 7	スタート → コントロールパネル	小さい／大きいアイコン: プログラムとコンポーネント		
		カテゴリ: プログラム → プログラムのアンインストール		
Windows 8 Windows 8.1 Windows 10 Windows 11	コントロールパネル	小さい／大きいアイコン: プログラムと機能		
		カテゴリ: プログラム → プログラムのアンインストール		

  2. インストールされているプログラムのリストで、**Dr.Web Security Space** 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4. 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。
4. **Self-Protectionを無効にする** ウィンドウが開きます。表示された確認コードを入力してください。
5. **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破損し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。

3.3. 製品の削除と再インストール

Dr.Webを削除する

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。

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。

1. Windowsコントロールパネルから Dr.Web Security Space プログラムを削除するには、以下を選択してください（OSに応じて）：

OS	アクション			
Windows XP	スタートメニュー	スタート → コントロールパネル → プログラムの追加と削除		
	クラシックのスタートメニュー	スタート → 設定 → コントロールパネル → プログラムの追加と削除		
Windows Vista	スタートメニュー	スタート → コントロールパネル	クラシックビュー	プログラムと機能
			ホームページ	プログラム → プログラムと機能
	クラシックのスタートメニュー	スタート → 設定 → コントロールパネル → プログラムの追加と削除		
Windows 7	スタート → コントロールパネル	小さい／大きいアイコン：プログラムとコンポーネント		
		カテゴリ：プログラム → プログラムのアンインストール		
Windows 8 Windows 8.1 Windows 10 Windows 11	コントロールパネル	小さい／大きいアイコン：プログラムと機能		
		カテゴリ：プログラム → プログラムの		

OS	アクション			
		アンインストール		

2. リストで、プログラム名の行を選択します。
3. **削除** をクリックします。
4. **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、すべてのオプション（**隔離**Dr.Web Agent**Dr.Web Security Space** ）が選択されています。**次へ** をクリックします。
5. **Self-Protectionを無効にする** ウィンドウが開きます。表示された確認コードを入力し、**プログラムの削除** をクリックします。
6. 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。

Dr.Webを再インストールする

1. Dr.Webの公式サイト で、該当するフィールドに有効なシリアル番号を入力して、プログラムの最新版インストールパッケージをダウンロードします。
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. ダウンロードした実行ファイル（`drweb-12.0-ss-win.exe`）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. ライセンス

ユーザーの権利は、Doctor Webの公式サイトまたは認定パートナーから購入したライセンスによって定められています。ライセンスを取得することで、その有効期間を通して製品のすべての機能を使用することが可能になります。ユーザーの権利は、プログラムのインストール中にユーザーが同意する 使用許諾契約 に基づいて規定されます。

固有の *シリアル番号* は各ライセンスに対応し、ライセンスパラメータに従ってDr.Webの動作を規定する特別なファイルはローカルコンピューターに保存されます。このファイルは *キーファイル* と呼ばれます。キーファイルの詳細については、キーファイル セクションを参照してください。

購入前に製品の試用を希望する場合は、デモバージョンを有効化することができます。*試用期間* 中は製品のすべての機能とコンポーネントを利用することが可能です。同一コンピューター上でデモバージョンを有効化することができるのは1年に1回のみです。有効化中に特別なキーファイルが生成されます。

デモバージョンはWindows XPでは使用できません。

ライセンス有効化の方法

ライセンスは、次のいずれかの方法で有効化できます。

- インストール中にインストールウィザードから
- インストール後の任意のタイミングで、ライセンスマネージャーから
- Doctor Webの公式サイト https://products.drweb.com/register/ で

登録ウィザードでは、キーファイルを使用したライセンスの有効化のみ可能です。ライセンスマネージャーでは、シリアル番号またはキーファイルを使用してライセンスを有効化できます。

ライセンス有効化の詳細については、シリアル番号を使用した有効化 および キーファイルを使用した有効化 セクションを参照してください。

トライアルライセンス

Dr.Webユーザーの方は1カ月のトライアルライセンスを使用することができます。トライアルライセンスはライセンスマネージャーウィンドウまたはライセンス有効化ウィンドウ内で取得することができます。個人データの入力は必要ありません。

トライアルライセンスはWindows XPでは使用できません。

ライセンスについてご不明な点がある場合は、Doctor Web公式サイトの FAQ セクションをご確認ください。

ようこそ画面

Dr.Webを初めて起動すると、ようこそ画面が表示されます。

インストール中に有効なキーファイルを指定しなかった場合は、ようこそ画面を使用して次の操作を行うことができます。

- Doctor Web公式サイトで **購入する** をクリックしてライセンスを購入する
- **有効化** をクリックし、シリアル番号またはキーファイルを使用して ライセンスを有効化 する
- **トライアル版を取得** をクリックしてデモバージョンを使用する

デモバージョンはWindows XPでは使用できません。Windows XPユーザーはオンラインでシリアル番号を登録してキーファイルを取得できます（**シリアル番号を登録** をクリックして）。

ようこそ画面が表示されるのは、プログラムインストール後の1回だけです。

よくある質問

ライセンスを別のコンピューターに移行するにはどうすればよいですか？

ユーザーは、キーファイルまたはシリアル番号を使用して商用ライセンスを移行する権利を有しています。
Windows XP搭載コンピューターにライセンスを移行する場合は、キーファイルを使用する方法のみ可能です。

ライセンスを別のコンピューターに移行するには

- シリアル番号を使用する:
  1. ライセンス元のコンピューターでシリアル番号をコピーします。
  2. ライセンス元のコンピューターからDr.Webを削除するか、そのコンピューターで別のライセンスを有効化します。
  3. 移行先となるコンピューター上で現在のライセンスを有効化します。これを行うには、インストール後にライセンスマネージャーを使用します（シリアル番号を使用した有効化 参照）。
- キーファイルを使用する:
  1. 元のコンピューターからキーファイルをコピーします。デフォルトでは、キーファイル はDr.Webインストールフォルダに置かれ、`.key` 拡張子を持っています。
  2. ライセンス元のコンピューターからDr.Webを削除するか、そのコンピューターで別のライセンスを有効化します。
  3. 移行先となるコンピューター上で現在のライセンスを有効化します。これを行うには、製品のインストール中に登録ウィザードを使用するか、インストール後にライセンスマネージャーを使用します（シリアル番号を使用した有効化 参照）。

トライアルライセンス（デモバージョン）を別のコンピューターに移行することはできません。

登録時のメールアドレスを忘れてしまいました。復元するにはどうすればよいですか？

登録時に指定したメールアドレスを忘れてしまった場合は、Dr.Webテクニカルサポート（https://support.drweb.com）までお問い合わせください。

ライセンス登録時と異なるメールアドレスからリクエストを行った場合、テクニカルサポート担当者より、ライセンス証明書の写真またはスキャンのコピー、支払い領収書、オンラインストアのメール、およびライセンスの所有権を証明するその他の書類の提示を求められる場合があります。

登録時のメールアドレスを変更するにはどうすればよいですか？

登録時に指定したメールアドレスを変更する必要がある場合は、メールアドレス変更サービス（https://products.drweb.com/register/change_email）を使用してください。

製品に一部のコンポーネントが含まれていないのはなぜですか？

- ライセンスに含まれるすべてのコンポーネントがインストールされたわけではありません。

  不足しているコンポーネントを有効化するには

  1. Windowsコントロールパネルで[プログラム]をクリックします。
  2. インストールされているプログラムのリストで、プログラム名の行を選択します。
  3. **変更** ボタンをクリックします。アンインストール／変更ウィザードが起動します。
  4. **コンポーネントの変更** を選択します。
  5. コンポーネントのリストから有効にするコンポーネントを選択し、**適用** をクリックします。

  また、インストールファイル`drweb-12.0-ss-win.exe` を実行するという方法もあります。開いたウィンドウで **コンポーネントの変更** オプションを選択し、手順5に進みます。

- サポートされるコンポーネントの数がこの製品よりも少ない別の製品用のライセンスは、この製品で有効化されます。

  製品でどのライセンスが指定されているかを確認するには

  1. メインメニュー を開きます。
  2. **ライセンス** を選択します。**ライセンスマネージャー** ウィンドウが開きます。
  3. **選択されたライセンス** セクションでDr.Web Security Spaceが指定されているかどうかを確認してください。

  別の製品のライセンスが指定されていた場合：

1. Dr.Webが 管理モード 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）。管理モードではない場合は、ロックをクリックします。
2. **詳細** をクリックして、ライセンス情報ウィンドウを開きます。
3. ドロップダウンリストから別のライセンスを選択します。選択したライセンスがインストールされた製品と一致していることを確認してください。

インストールされた製品に関する情報を確認するには

1. メインメニュー を開きます。
2. **サポート** を選択します。**プログラムについて** セクションに、インストールされた製品が表示されます。

- インストールされた製品が、取得したライセンスと一致していません。

有効化されたライセンスと一致する別のDr.Web製品をインストールするには

1. 公式サイトからDr.Webの最新バージョンをダウンロードします：https://download.drweb.com/。
2. 製品のシリアル番号と登録用メールアドレスを指定して、**ダウンロード** をクリックします。
3. 必要な製品バージョンを選択して、インストールパッケージをダウンロードします。
4. 以前にインストールした製品を削除します。手順については、製品の削除と再インストール セクション を参照してください。
5. ダウンロードしたインストールファイルを使用して製品をインストールします。

4.1. ライセンスの有効化

すべての製品機能とコンポーネントにアクセスするには、ライセンスを有効化してください。次のいずれかを使用してライセンスを有効化できます。

- シリアル番号
- キーファイル

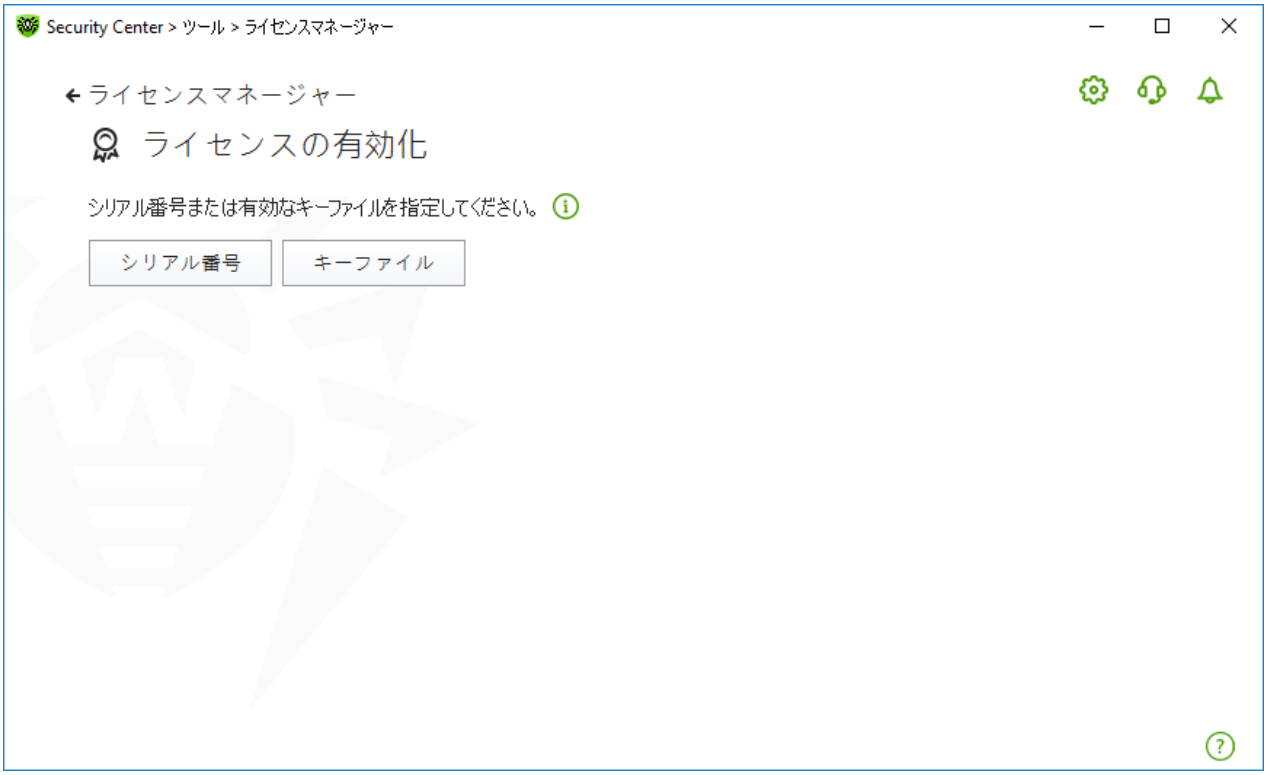

図 5. ライセンスの有効化

Windows XPユーザーは、キーファイルを使用した ライセンスの有効化 のみ可能です。

すでにDr.Webユーザーの方は、新しいライセンスの有効期間を延長することができます。

Dr.Web Anti-Virus for Windowsのライセンスを指定してDr.Web Security Spaceを有効化することができます。Dr.Web Anti-Virus for Windowsの提供する機能はDr.Web Security Spaceのものよりも少ないため、次のコンポーネントとツールは無効になります。

- SpIDer Gate
- Anti-Spam
- Webカメラやマイクへのアクセスのブロック
- デバイスのブロック
- データ損失防止
- Parental Control
- アンチウイルスネットワーク

Windows XPでのライセンスの有効化

Windows XPのユーザーは、キーファイルを使用したライセンスの有効化のみ可能です。キーファイルはなく、シリアル番号のみをお持ちの場合は、Doctor Web公式サイト 上でそれを登録する必要があります。登録が完了すると、キーファイルをダウンロードするためのリンクが利用可能になります。このキーファイルを使用して、インストール中またはインストール後に、ライセンスマネージャーに含まれる登録ウィザードでライセンスを有効化します:

1. Dr.Web メニュー で **ライセンス** を選択します。ライセンスマネージャーが開きます。**有効化** 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、キーファイルへのパスを指定します。
3. **OK** をクリックしてウィンドウを閉じ、ライセンスマネージャーに移動します。

> デモバージョンはWindows XPでは使用できません。

ライセンスの再有効化

キーファイルを紛失してしまった場合、ライセンスの再有効化が必要になる場合があります。

> ライセンス またはトライアルライセンス（デモバージョン）を再有効化した場合は、前回の登録時と同じキーファイルを受け取ります（有効期限が切れていない場合）。

製品を再インストール、または複数のコンピューター上にインストール（ライセンスで許可されている場合のみ）する場合、キーファイルの再有効化は必要ありません。

ライセンスマネージャーまたはライセンス管理用コマンドを使用してライセンスキーファイルを取得できる回数には上限があります。その上限回数を超えた場合は、https://products.drweb.com/register/ にてシリアル番号の登録を確認すると、メールにてキーファイルを受け取ることができます。キーファイルは、確認したシリアル番号に登録されたメールアドレスに送信されます。

4.1.1. シリアル番号を使用した有効化

シリアル番号をお持ちの場合は、次の操作を実行できます。

- ライセンスマネージャーを使用してライセンスを有効化する：
  1. Dr.Web メニュー で **ライセンス** を選択します。ライセンスマネージャーが開きます。**有効化** をクリックします。
  2. ライセンス有効化ウィンドウが開きます。**シリアル番号** をクリックします。

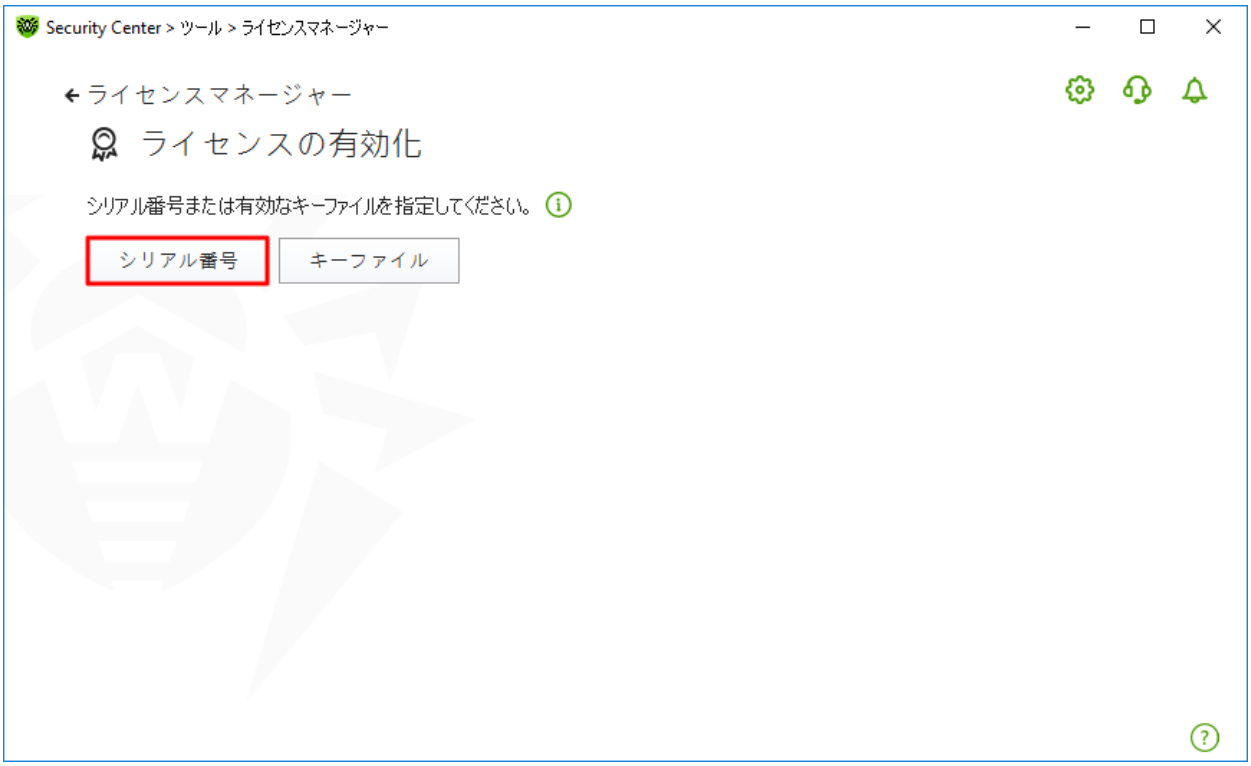

図 6. シリアル番号指定ウィンドウへのアクセス

3. 追加のウィンドウでシリアル番号を入力し、**有効化** をクリックします。

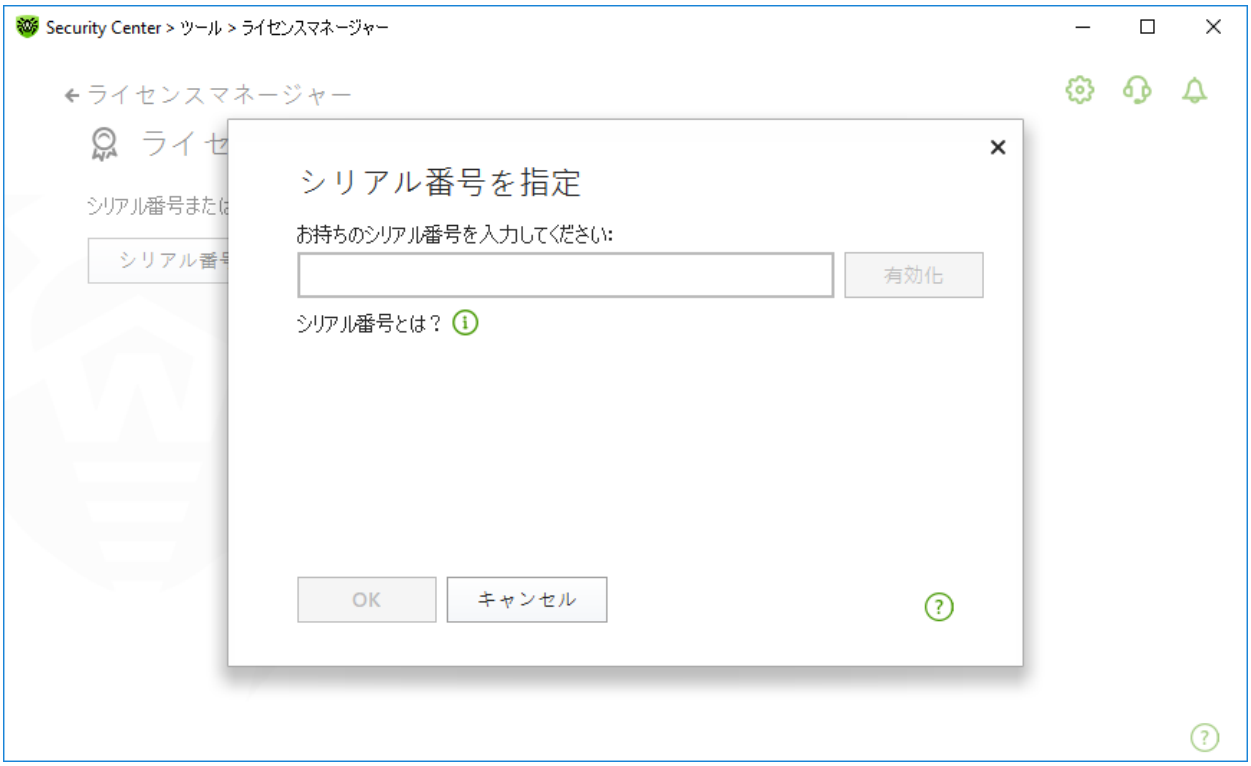

図 7. シリアル番号を使用した有効化

4. Doctor Webの公式サイトが開きます。登録データを入力し、ウェブサイトの指示に従って登録を完了してください。

長時間操作のない状態が続くとウィンドウが自動的に閉じ、エラーメッセージが表示されます。

シリアル番号の登録が完了するまで有効化ウィンドウを閉じないでください。ウィンドウが閉じている場合、キーファイルを使用したライセンスの有効化のみが可能です。

5. シリアル番号を登録するためのリンクが、指定したメールアドレスに送信されます。リンクに従ってライセンスの有効化を完了します。
6. 有効化に成功すると、プログラムウィンドウにライセンスに関する詳細情報が表示されます。**OK** をクリックしてウィンドウを閉じ、ライセンスマネージャーに移動します。

有効化に失敗した場合は、エラーメッセージが表示されます。インターネット接続パラメータを確認し、**再試行** をクリックしてください。

- Doctor Webの公式サイト でシリアル番号を登録し、ライセンス有効化のためのキーファイルを取得してください。

4.1.2. キーファイルを使用した有効化

キーファイルをお持ちの場合、次の方法でライセンスの有効化を行うことができます。

- インストール中に登録ウィザードを使用して:
  1. 製品のインストールを実行します。インストールの 手順5 で**有効なキーファイルのパスを指定する** を選択します。**インストール** をクリックします。

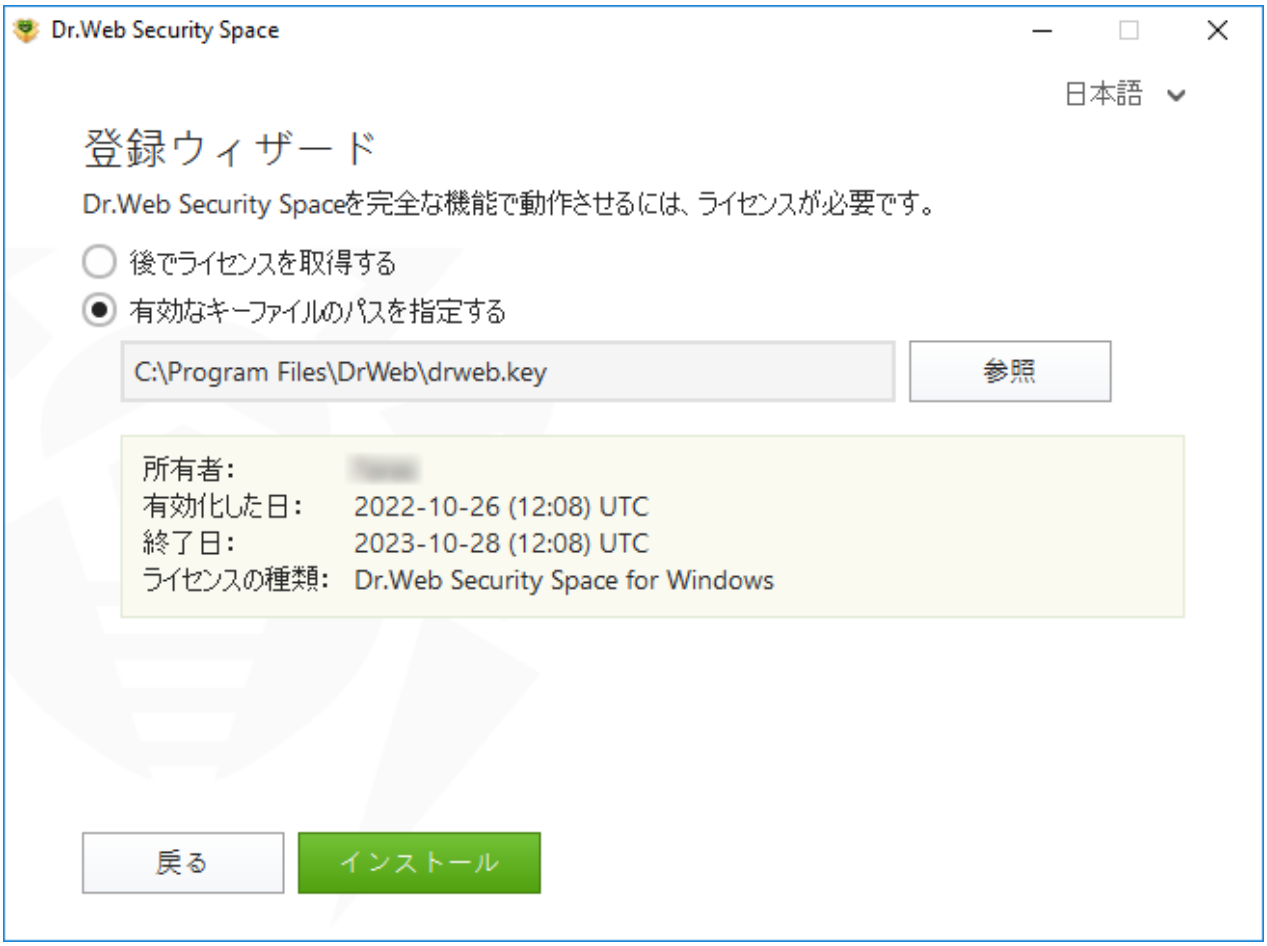

図 8. インストール、登録ウィザード

2. インストールウィザードの指示に従って製品のインストールを続行します。

- インストール後の任意のタイミングで、ライセンスマネージャーを使用して:

1. Dr.Web メニュー で **ライセンス** を選択します。ライセンスマネージャーが開きます。**有効化** をクリックします。
2. ライセンス有効化ウィンドウが開きます。**キーファイル** をクリックします。

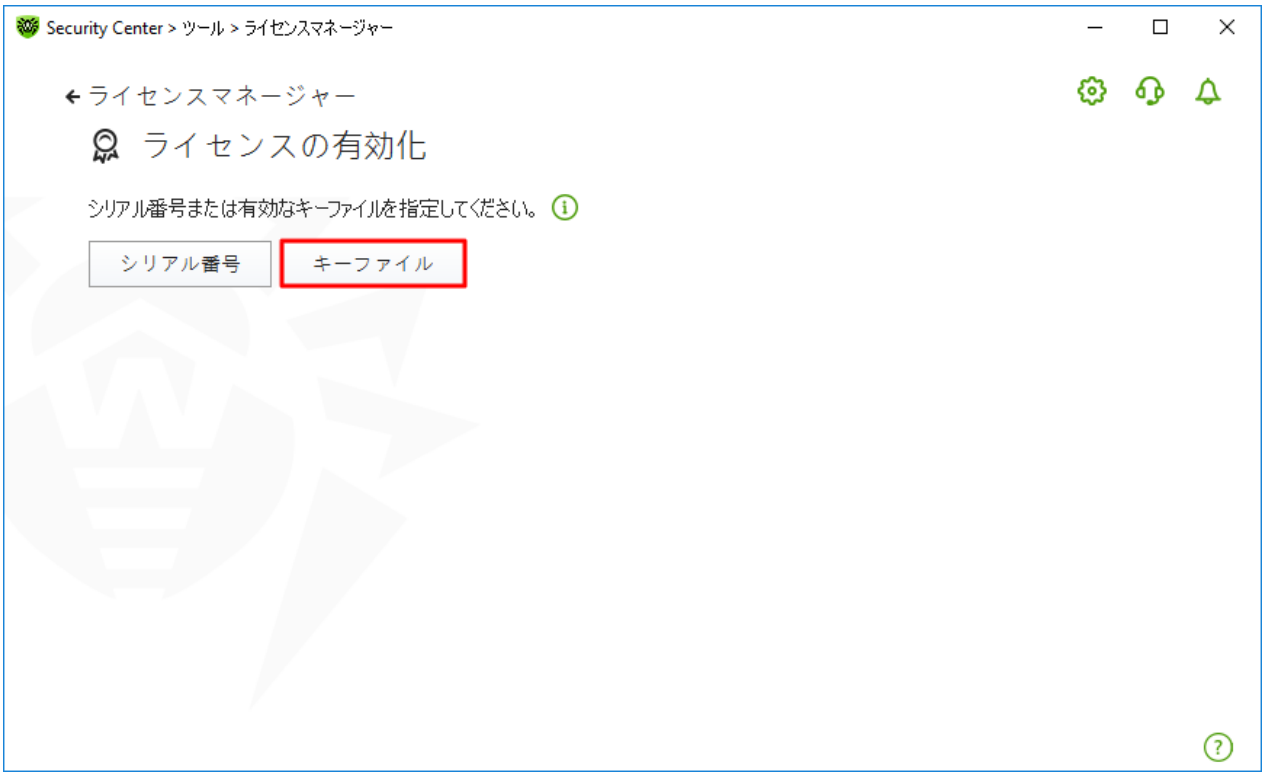

図 9. キーファイル指定ウィンドウへのアクセス

3. 開いたウィンドウ内で **参照** をクリックし、キーファイルへのパスを指定します。

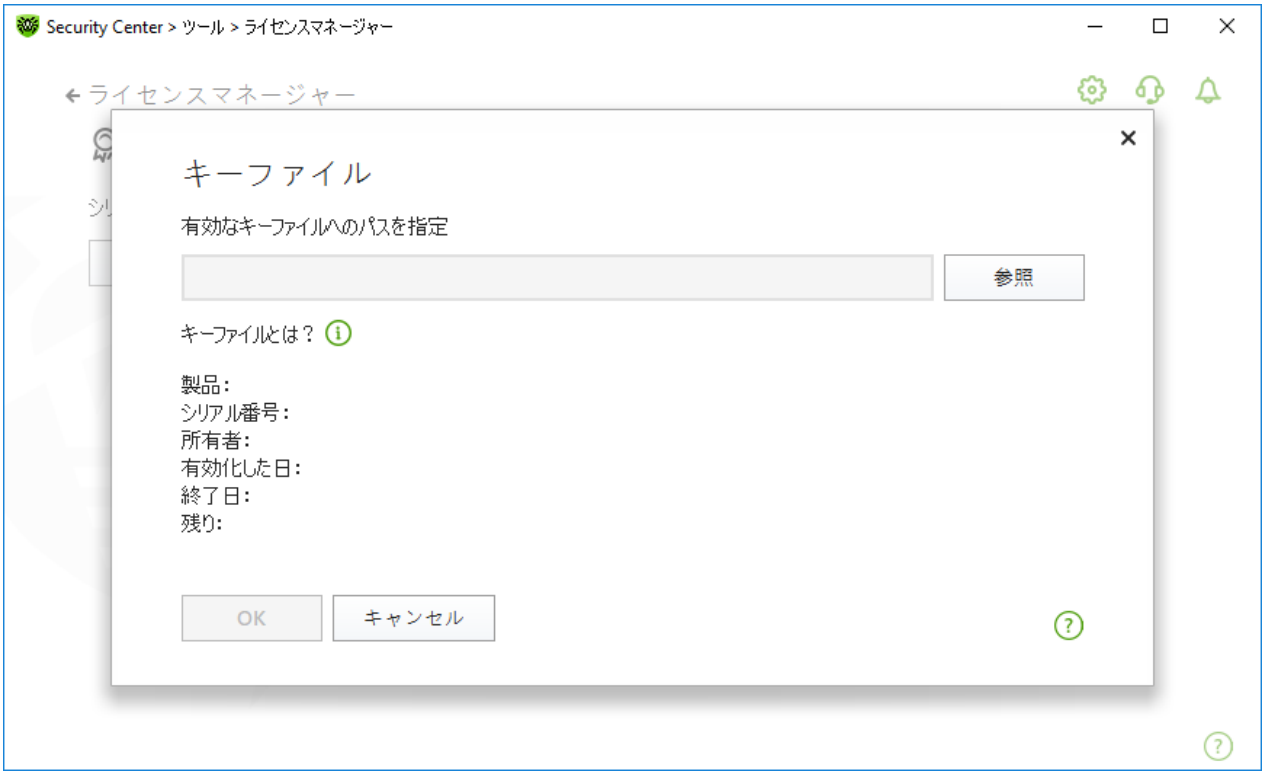

図 10. キーファイルを使用した有効化

4. **OK** をクリックしてウィンドウを閉じ、ライセンスマネージャーに移動します。

4.2. ライセンス更新

ライセンスマネージャーを使用して、Doctor Web公式サイト で現在のライセンスを更新することができます。

ライセンスマネージャーを使用して現在のライセンスを更新するには

1. Dr.Web メニュー を開き、**ライセンス** を選択します。
2. ライセンスマネージャーのウィンドウで、**購入する** をクリックします。ライセンスを割引価格で更新できるDoctor Webサイトのページが開きます。

Dr.Webはライセンスのオンザフライ更新をサポートしています。そのため、Dr.Web製品の動作を停止したり再インストールしたりする必要がありません。ライセンスを更新するには、新しいライセンスを有効化する必要があります。

> ⚠ 長時間操作のない状態が続くとウィンドウが自動的に閉じ、エラーメッセージが表示されます。
>
> 更新プロセスが完了するまで有効化ウィンドウを閉じないでください。ウィンドウが閉じている場合、キーファイル を使用したライセンスの有効化のみが可能です。

有効化に失敗した場合は、エラーメッセージが表示されます。インターネット接続パラメータを確認し、**再試行** をクリックしてください。

ライセンスを有効化するには

1. Dr.Web メニュー で **ライセンス** を選択してライセンスマネージャーを開きます。**有効化** をクリックします。
2. 開いたウィンドウで、**シリアル番号** をクリックして製品のシリアル番号を入力するか、または **キーファイル** をクリックしてキーファイルへのパスを指定してください。Windows XPユーザーは、キーファイルを使用した ライセンスの有効化 のみ可能です。

ライセンス有効化の詳細については、シリアル番号を使用した有効化 および キーファイルを使用した有効化 セクションを参照してください。

更新するライセンスの有効期間が終了すると、Dr.Webは新しいライセンスの使用を開始します。

更新するライセンスが有効な場合は、残りの日数が自動的に新しいライセンスに追加されます。 同時に、古いライセンスはブロックされ、登録時に指定したメールアドレスに通知が届きます。ライセンスマネージャー を使用して 古いライセンスを削除 することをお勧めします。

ライセンス更新についてご不明な点がある場合は、Doctor WebサイトのFAQ セクションをご確認ください。

よくある質問

ライセンスの更新後、30日以内にキーファイルがブロックされるというメールを受け取りました

更新したライセンスの有効期限がまだ満了していない場合は、残りの日数が新しいライセンスに自動的に追加され、同時に、更新を行ったライセンスがブロックされます。ブロックされたライセンスを使用すると、Dr.Webコンポ

ーネントは機能せず、ソフトウェアは更新されません。

以前のライセンスを削除することをお勧めします。ライセンスを削除するには、次の手順を実行します。

1. 管理モード で、Dr.Web メニュー で **ライセンス** を選択します。ライセンスマネージャーが開きます。
2. **詳細** をクリックして、ライセンス情報ウィンドウを開きます。
3. ドロップダウンメニューで更新を行ったライセンスを選択し、 をクリックします。

4.3. キーファイル

Dr.Webの使用権限は *キーファイル* 内で規定されています。製品ディストリビューションキットに含まれていたキーファイルは自動的にインストールされます。

キーファイルは `.key` 拡張子を持ち、以下の情報を含んでいます。

- 利用可能な（ライセンスされている）アンチウイルスコンポーネントの一覧
- 製品のライセンス有効期限
- テクニカルサポートの利用が可能であるかどうか
- その他の制限（ウイルススキャンを同時に実行することが可能なリモートコンピューターの台数など）

デフォルトでは、キーファイルはDr.Weのインストールフォルダに置かれます。Dr.Webは定期的にキーファイルを検証します。ライセンスの有効性を保つため、ファイルの編集または変更を行わないようにしてください。

有効なキーファイルが見つからない場合、すべてのDr.Webコンポーネントがブロックされます。

Dr.Webキーファイルは次の条件が満たされている場合に有効です。

- ライセンスの有効期限内であること
- キーファイルの整合性が損なわれていないこと

上記いずれかの条件が満たされていない場合、キーファイルは無効となり、Dr.Webはファイル、メモリ、メール内のマルウェア検出および駆除を停止します。

Dr.Webのインストール中にパスを指定しなかった場合は、一時キーファイルが使用されます。このキーファイルによって、Dr.Webの全機能が提供されます。ただし、Dr.Web メニュー の **更新** 項目は、ライセンスまたはトライアル版を有効にするか、ライセンスマネージャーを介して有効なキーファイルへのパスを指定するまで利用できません。

キーファイルはライセンス有効期限またはトライアルライセンスが満了するまで保管しておくことを推奨します。

トライアルライセンス（デモバージョン）を有効化するためのキーファイルは、登録手続きを行ったコンピューター上でのみ使用することができます。

5. 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。

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。

設定 ウィンドウ内で **Dr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およびパーソナルページ My Dr.Web を開く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テクニカルサポートまでご連絡ください。

図 11. プログラムメニュー

メニュー項目

My Dr.Web – Doctor Web 公式サイト上にあるユーザーのパーソナルページを開きます。このページでライセンスに関する情報（有効期限、シリアル番号）の確認、ライセンスの更新、テクニカルサポートへの問い合わせなどを行うことができます。

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（Parental 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。

ライセンス - ライセンスの有効期限が切れるまでの残り日数に関する情報。ライセンスマネージャー を開きます。

更新 - 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 Parental 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。

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。

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。
	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。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。
	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。有効なキーファイルをお持ちかどうかを確認し、必要な場合は インストール してください。
	Scannerが現在動作中です。

6. Security Center

Security Center ウィンドウから、すべ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12. 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 - すべ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
  - デバイスと個人データ
  - Parental Control

    - ツール
    - 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、**ツール** 設定グループ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。

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**。すべ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色で強調表示されます。
- **ライセンス期限が切れます**。ライセンスの有効期限が切れる7日前から表示されます。黄色で表示されます。ライセンスを更新するには、ライセンスマネージャー にアクセスします。

7. ウイルスデータベースとプログラムコンポーネントを更新する

悪意のあるオブジェクトを検出するために、Dr.Web製品は既知のすべての悪意のあるプログラムに関する情報が含まれたウイルスデータベースを使用します。データベースを定期的に更新することで、それまで未知であったウイルスを検出し、それらの拡散をブロックすることができます。また、以前は修復不可能であった感染したファイルを修復することが可能になる場合もあります。ウイルスデータベースの他に、Dr.Webソフトウェアコンポーネントとヘルプドキュメントも更新されます。

Dr.Webを更新するには、インターネットか更新ミラー（ローカルフォルダまたはネットワークフォルダ）、または更新ミラーが設定されているコンピューターが1台以上あるアンチウイルスネットワークに接続する必要があります。更新元設定のカスタマイズは、**一般** → **更新** で行うことができます。Dr.Web更新パラメータのカスタマイズの詳細は、更新 セクションを参照してください。

更新が必要かどうか確認する

ウイルスデータベースとプログラムコンポーネントが最新であるかどうかを確認するには、Dr.Web メニュー を開きます。更新が必要ない場合、**更新** 項目が緑色で表示されます。

図 13. Dr.Webメニュー

更新が必要な場合、**更新が必要です** が赤色で表示されます。

図 14. 更新が必要な場合

更新を開始する

更新の実行中に、お使いのバージョンのDr.Web向けの更新ファイルがすべてダウンロードされ、最新のバージョンがリリースされた場合にはDr.Webのアップグレードが行われます。

実行可能ファイル、ドライバ、またはライブラリの更新後、再起動が必要な場合があります。この場合、警告が表示されます。再起動する時間を設定したり、次のリマインダーの時間を選択できます。

Dr.Webメニュー から更新を実行するには

1. Dr.Web メニュー を開き、**更新** を選択します。このメニュー項目の色は、ウイルスデータベースとプログラムコンポーネントの更新状況によって異なる場合があります。
2. Dr.Webウイルスデータベースとコンポーネントが最新であるかどうかに関する情報や、それらの最終更新日を表示するウィンドウが開きます。**更新** をクリックして更新を開始します。

コマンドラインから更新を開始するには

1. Dr.Web インストールフォルダ(`%PROGRAMFILES%\Common Files\Doctor Web\Updater`)を開きます。
2. `drwupsrv.exe` ファイルを実行してください。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。

アップデートと統計ログ

統計 タブで更新履歴を確認するには

1. Dr.Web メニュー を開きます。
2. **Security Center** を選択します。
3. **統計** タブを開きます。

4. **詳細なレポート** タイルをクリックします。

Dr.Webの更新ログは、`%allusersprofile%\Doctor Web\Logs\` フォルダにある `dwupdater.log` ファイルに保存されています。

インターネットアクセスなしでのデータベースとコンポーネントの更新を設定する方法

コンピューターがローカルネットワークに接続されている場合、Dr.Web製品（Security Space、Anti-virus for Windows、Anti-virus for Windows Servers）がインストールされている別のコンピュータ上に作成された更新ミラーを使用してウイルスデータベースとコンポーネントを更新することができます。更新ミラーが作成されているコンピューターにインターネット接続が必要です。また、製品のバージョンが同じである必要があります。

更新ミラーの作成方法に関する詳細

更新ミラーからの更新を設定するには、2つの方法があります。

コンピューターがアンチウイルスネットワークに接続されている場合の更新を設定するには

1. 設定ウィンドウの アンチウイルスネットワーク セクションでDr.Web製品のリモートコントロールを有効にします。

図 15. リモートアクセスを有効にする

2. **設定** → **更新** ウィンドウに移動します。
3. **更新元** セクションで **変更** をクリックし、ドロップダウンリストから **アンチウイルスネットワーク** を選択します。

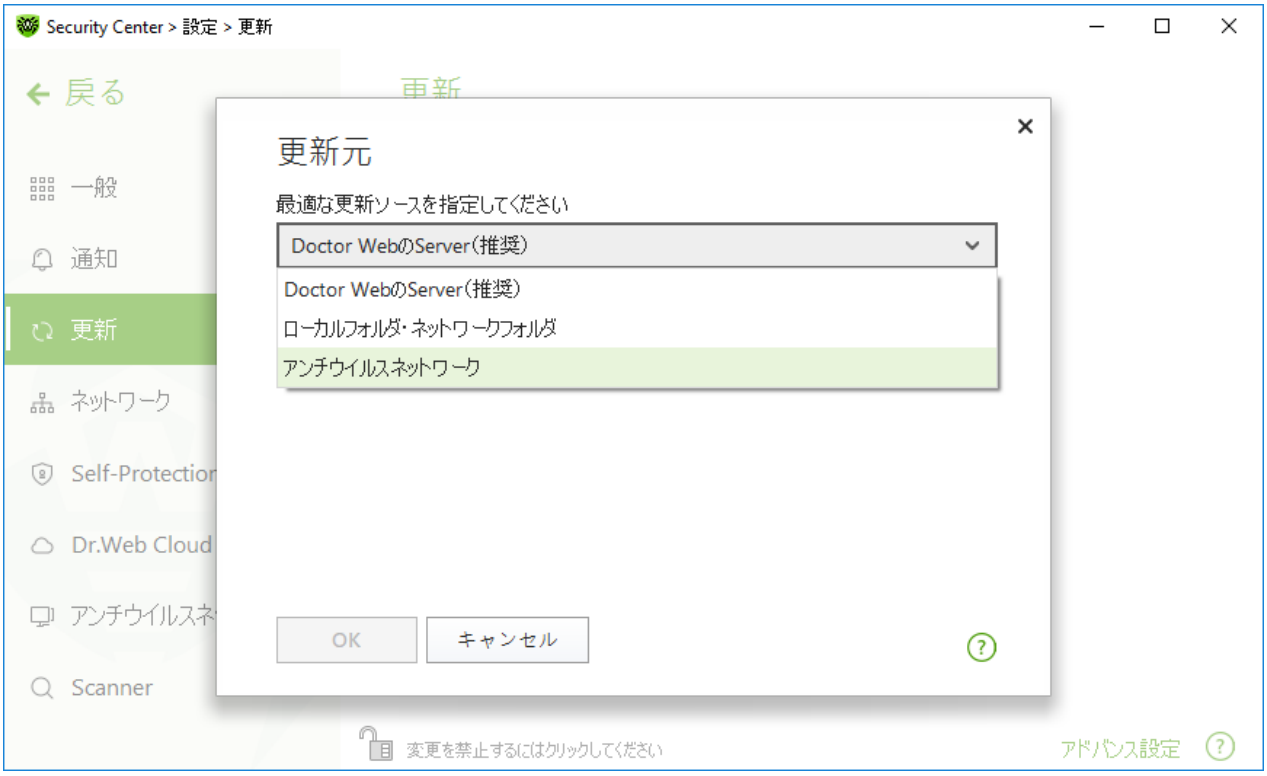

図 16. 更新元を選択する

4. ウイルスデータベースとコンポーネントの更新に使用するコンピューターを選択します。
5. **OK** をクリックします。

ローカルまたはネットワークフォルダからの更新を設定するには

1. **設定** → **更新** ウィンドウに移動します。
2. **更新元** セクションで **変更** をクリックし、ドロップダウンリストから **アンチウイルスネットワーク** を選択します。

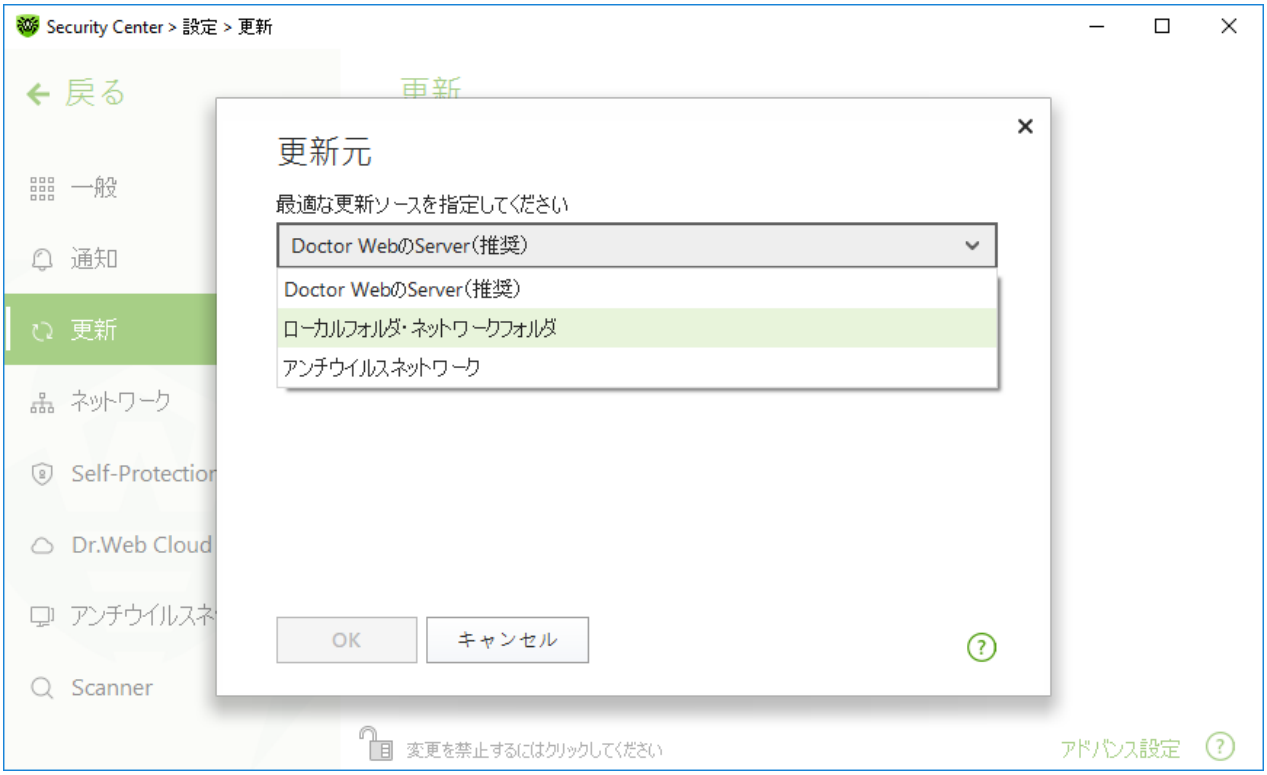

図 17. 更新元を選択する

3. **更新ミラーへのパス** フィールドで、**参照** ボタンをクリックしてフォルダを選択するか、UNCを使用して手動でパスを入力して、作成された更新ミラーのファイルを含むフォルダを指定します。
4. 必要に応じて、接続しようとしているフォルダに **ログイン** と **パスワード** を入力します。**ログイン** は、ネットワークフォルダのあるコンピューターのアカウントのユーザー名です。ログインには、ローカルネットワーク内のコンピューター名とフォルダへのフルパスが必要です。**パスワード** はアカウントのパスワードです。
5. **OK** をクリックします。

8. 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。

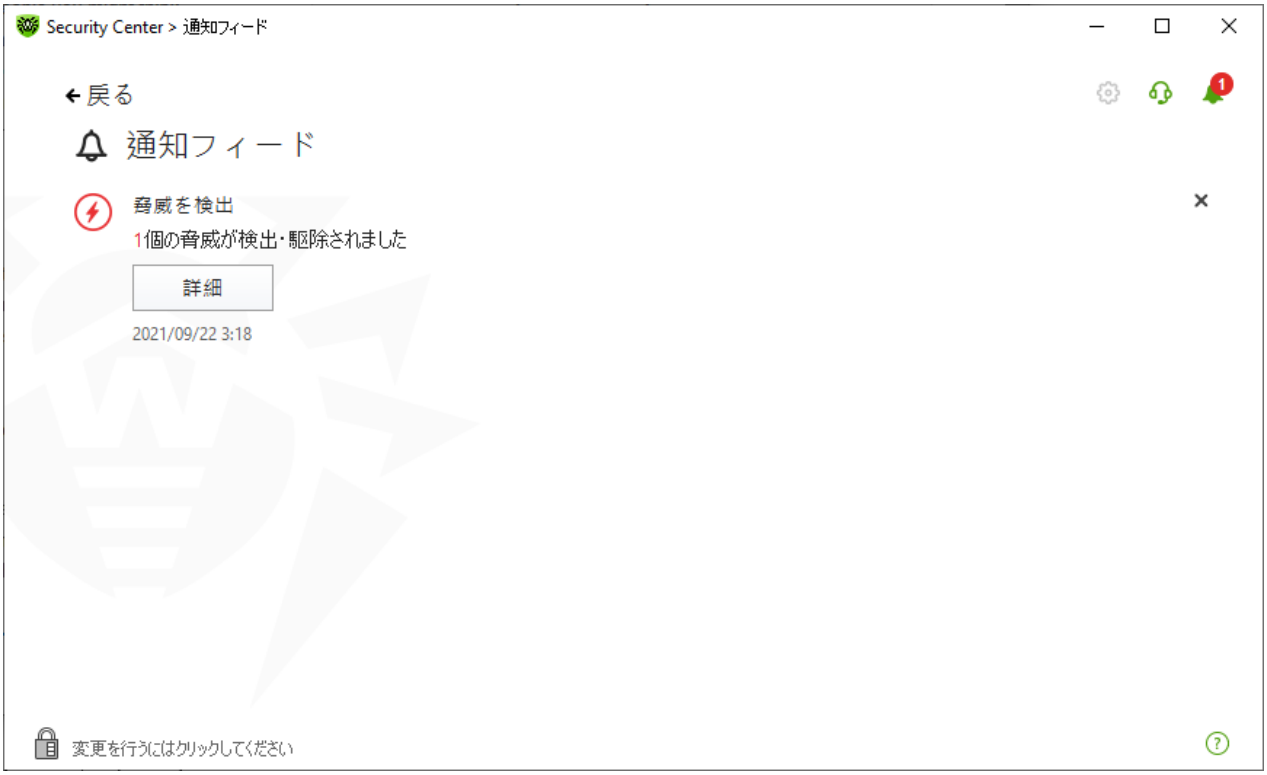

図 18. 通知フィードウィンドウ

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	
ライセンス	• 有効なライセンスが見つかりませんでした。 • 現在のライセンスがブロックされている旨の通知
脅威	• 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。
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	• 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	
ライセンス	• ライセンス有効期限切れについて。 • 現在のライセンスがブロックされている旨の通知
更新	• 更新を完了するには、再起動が必要です。
コンポーネント	• データ損失防止の方法の変更。
軽微な通知	
新しいバージョン	• 新しいバージョンが入手可能です。

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。

9. 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。

> 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、設定をインポートまたはエクスポート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およびメールによる通知の受信について設定することができます。
- 更新 - 更新のソースまたは頻度を変更し、更新ミラーを作成します。
- ネットワーク - プロキシサーバー接続や安全なプロトコル経由でやり取りされるデータのスキャンを設定します。
- Self-Protection - 追加のセキュリティパラメータを設定します。
- Dr.Web Cloud - Doctor Webクラウドサービスへのアクセスを設定します。
- アンチウイルスネットワーク - コンピューターにインストールされているDr.Webへのリモートアクセスを設定します。
- 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。

9.1. 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
- プログラム設定を管理する（設定のインポートやエクスポートまたはデフォルトの復元）
- 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。

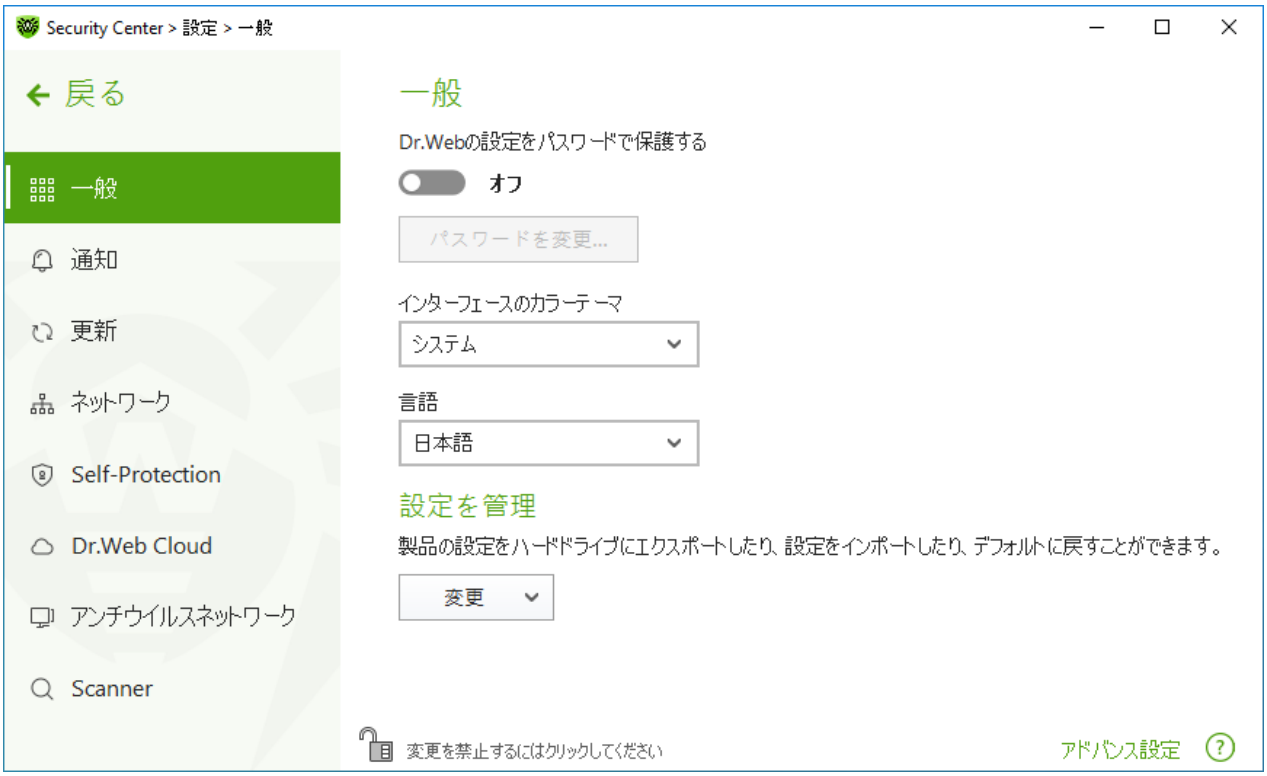

図 19. 全般設定

9.1.1. 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。パスワードは任意の長さにすることができ、文字、数字、特殊文字のあらゆる組み合わせを使用できます。保護を強化するため、10文字以上の異なる文字で構成されるパスワードを設定してください。Dr.Web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。

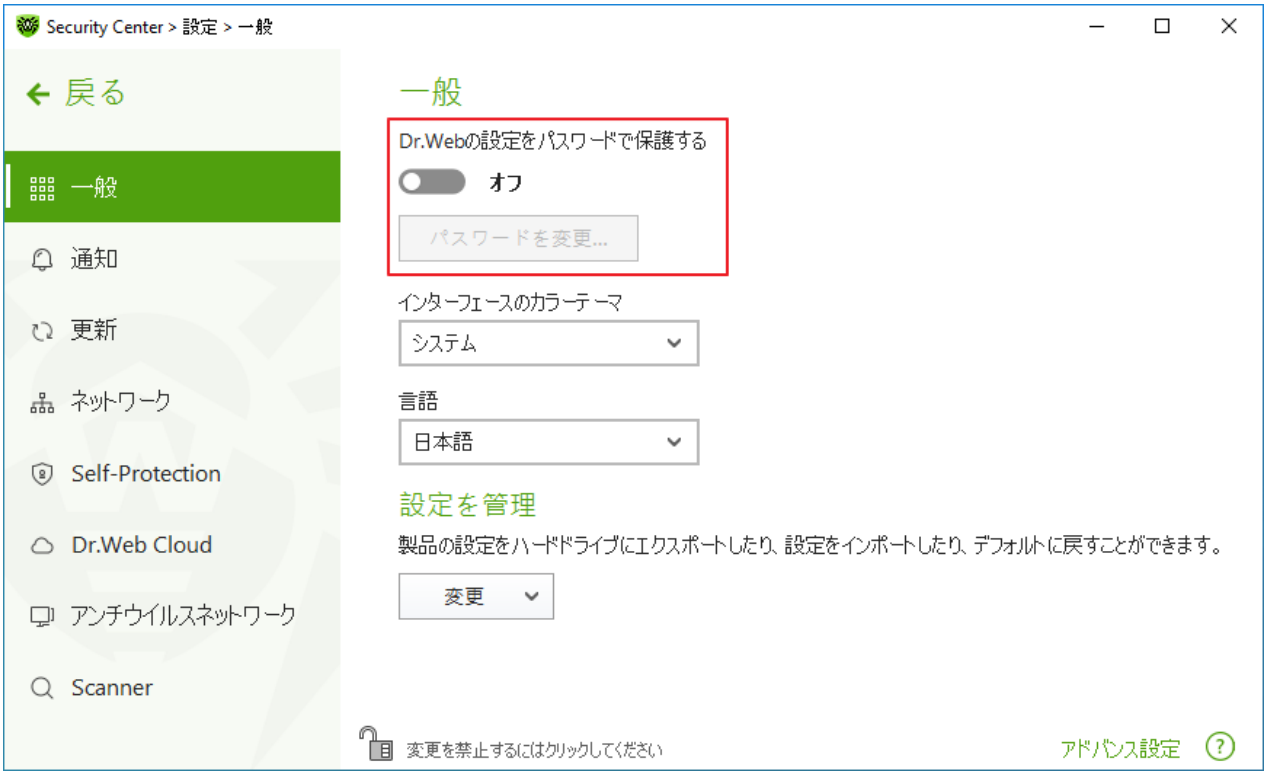

図 20. 設定のパスワード保護

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、現在の設定を保存せずにDr.Webプログラムを再インストールしてください。

9.1.2. 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。

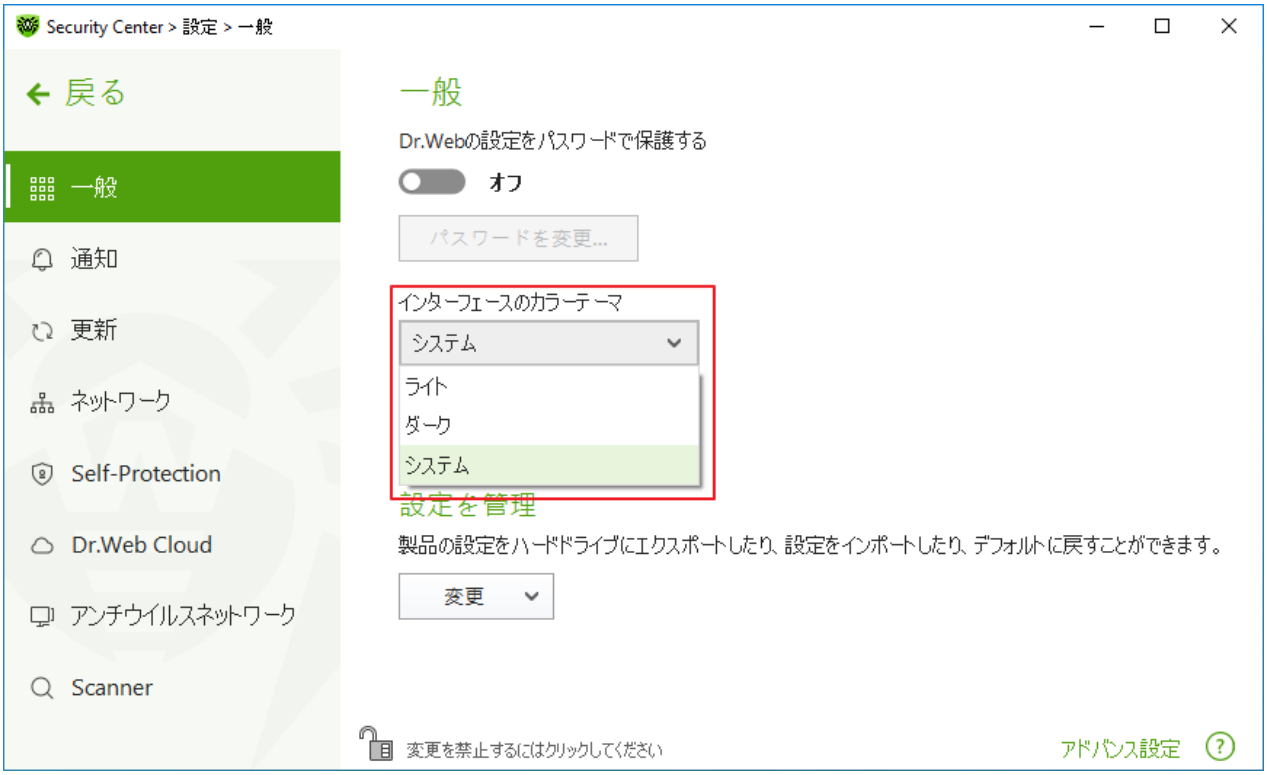

図 21. インターフェースのカラーテーマを選択する

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）およびWindows 11。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。

9.1.3. 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。

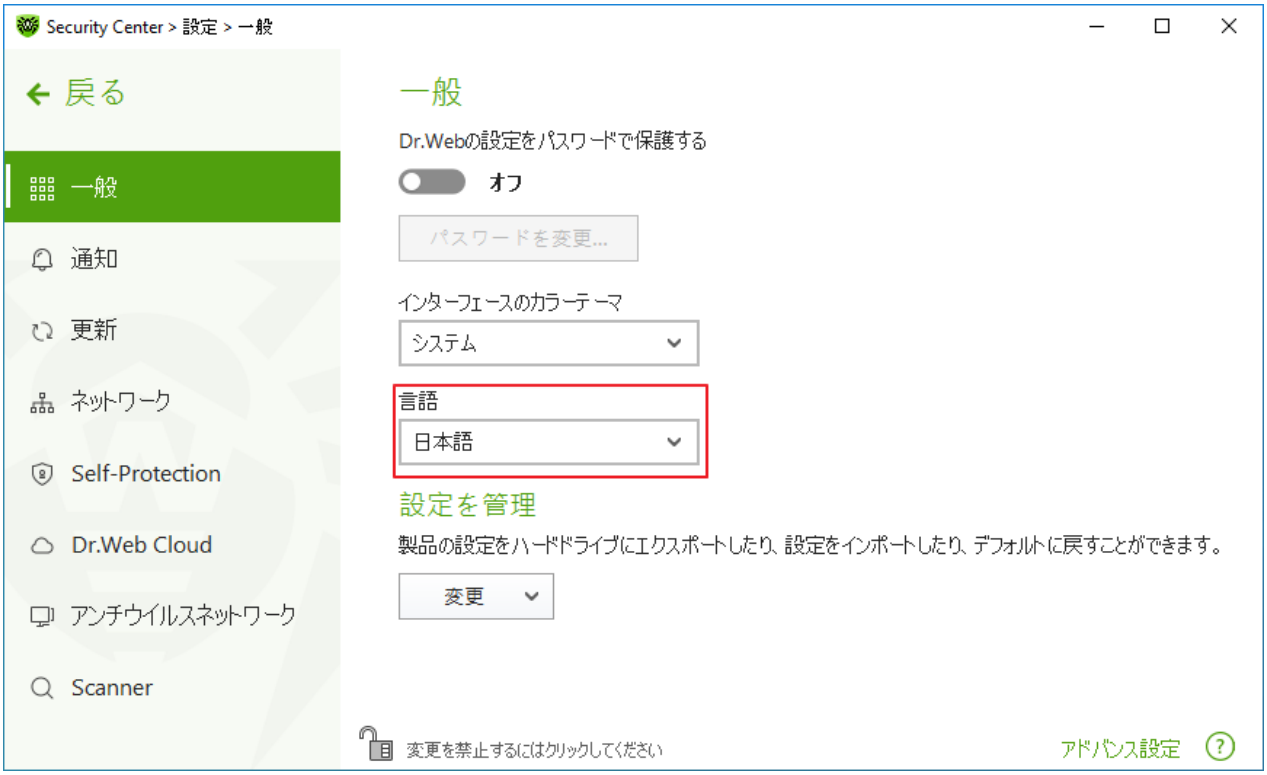

図22. プログラム言語を選択する

9.1.4. Dr.Web設定を管理する

設定を管理するには、**設定を管理** 設定グループのドロップダウンメニューで、次のいずれかのアクションを選択します。

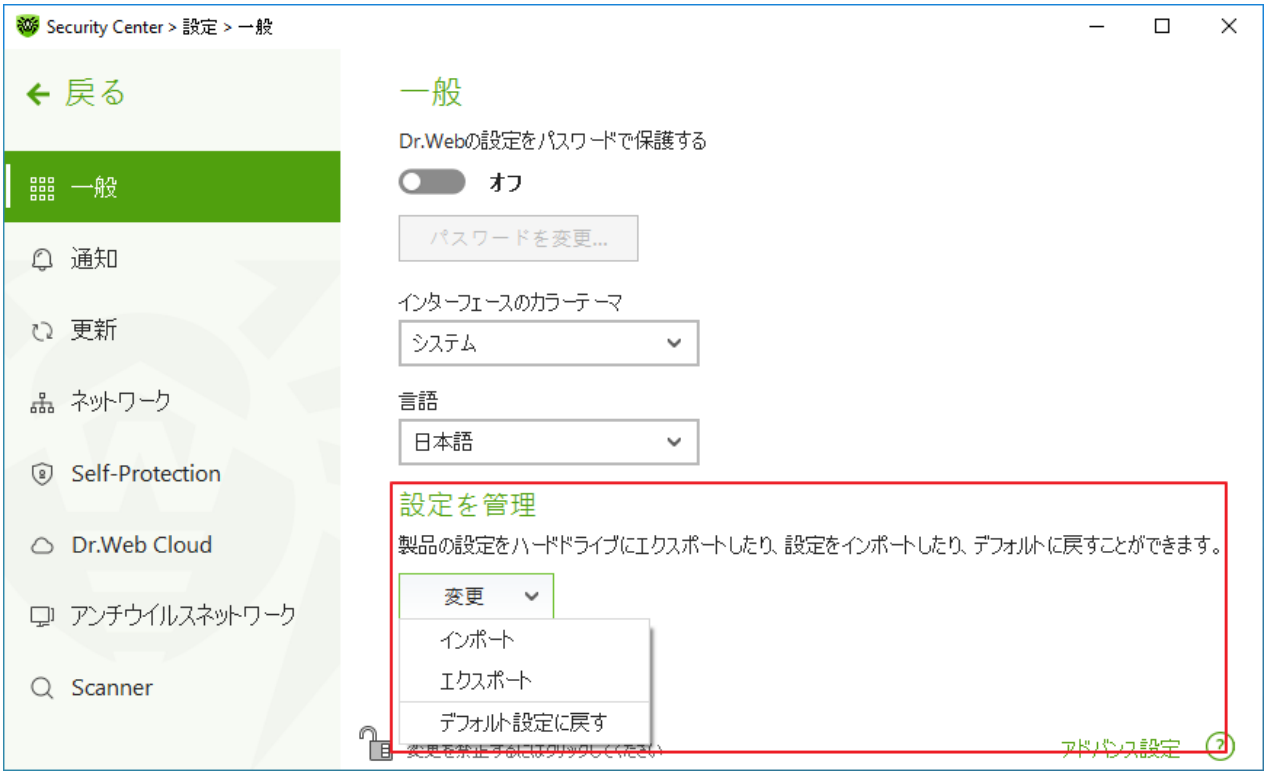

図 23. 設定を管理する

- デフォルト設定にリセットするには、**デフォルト設定に戻す** を選択してください。
- 別のコンピューター上で既に設定されているDr.Webの設定を使用したい場合は、**インポート** を選択します。
- 別のコンピュータで今の設定を使用する場合は、**エクスポート** を選択します。次に、別のコンピューターでインポート機能を使用します。

9.1.5. 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. **アドバンス設定** リンクをクリックします。
2. **ログ** セクションで **変更** をクリックします。

図 24. 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：

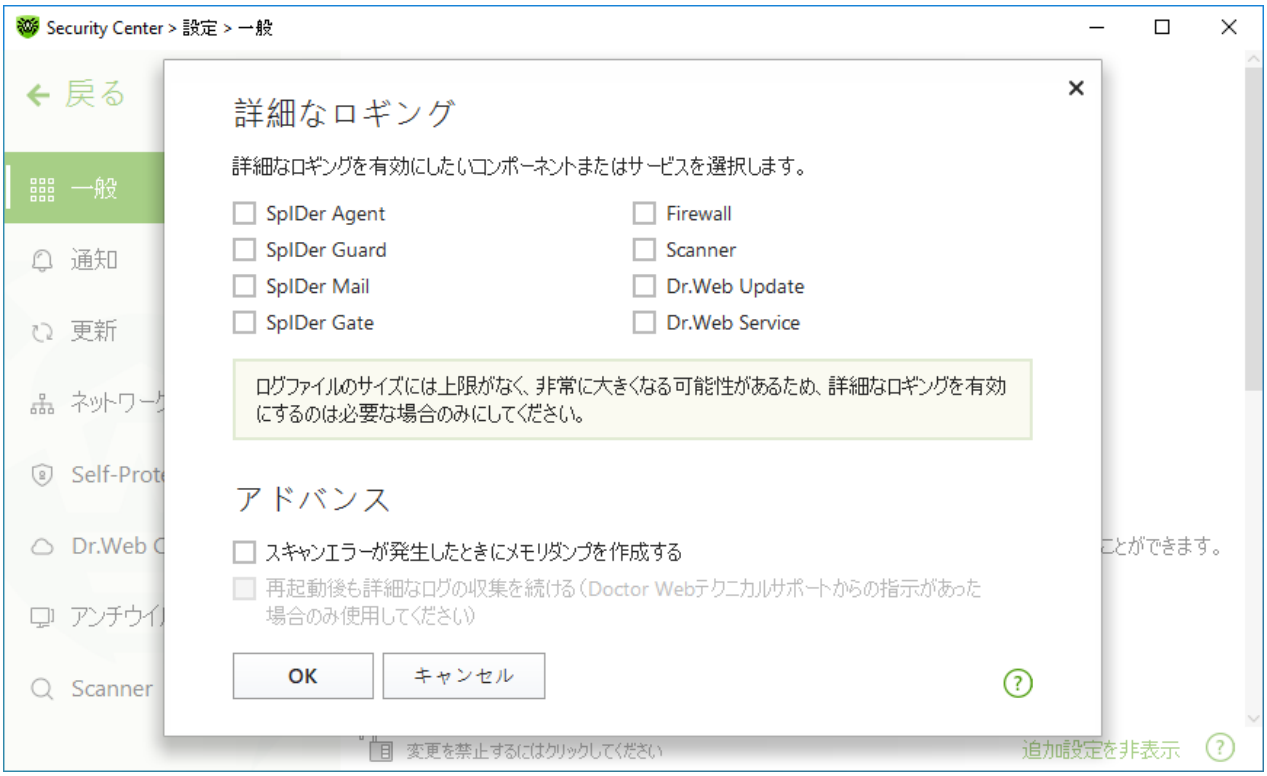

図 25. 動作ログのロギング設定

3. 詳細なロギングを有効にするコンポーネント、モジュール、またはサービスを選択します。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おり、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 Agent	更新時刻、SpIDer Agentの起動時刻と停止時刻、ウイルスイベント、アンチウイルスネットワークへの接続、ライセンスイベント、Dr.Webコンポーネントのステータス、設定管理（インポート、エクスポート）、エラー通知、システムの再起動通知。 プログラム動作におけるエラーの原因に関する詳細情報を取得するには、このモードを使用することをお勧めします。
SpIDer Guard	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。 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特定したい場合、このモードを使用することをお勧めします。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。
SpIDer Mail	更新時刻、SpIDer Mailの起動時刻と停止時刻、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。 メールの監視設定をテストする場合、このモードを使用することをお勧めします。
SpIDer Gate	更新時刻、SpIDer Gateの起動時刻と停止時刻、ウイルスイベント、接続監視設定、スキャンされたファイル名、パッカー名、スキャンされたアーカイブのコンテンツ。 チェックされたオブジェクト、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、このモードを使用することをお勧めします。
Scanner	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の起動時刻と停止時刻、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。
Firewall	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。 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）。
Dr.Web Update	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、更新日時、補助スクリプトの実行とDr.Webコンポーネントの再起動に関する詳細。
Dr.Web Service	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、アンチウイルスネットワークへの接続に関する情報。

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、システムやDr.Webのパフォーマンス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にエラーが発生した場合やDoctor Webテクニカルサポート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. デフォルトでは、詳細なロギングモードはOSの最初の再起動前まで有効になっています。再起動の前と後でコンポーネントの動作をロギングする必要がある場合、**再起動後も詳細なログの収集を続ける（Doctor Webテクニカルサポートからの指示があった場合のみ使用してください）** チェックボックスにチェックを入れてください。
3. 設定を保存するには **OK** をクリックします。

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。

- 現在のセッション情報が上限を超えていない場合、指定されたサイズに
- セッション情報が上限を超えた場合、現在のセッションのサイズに

9.1.6. 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。

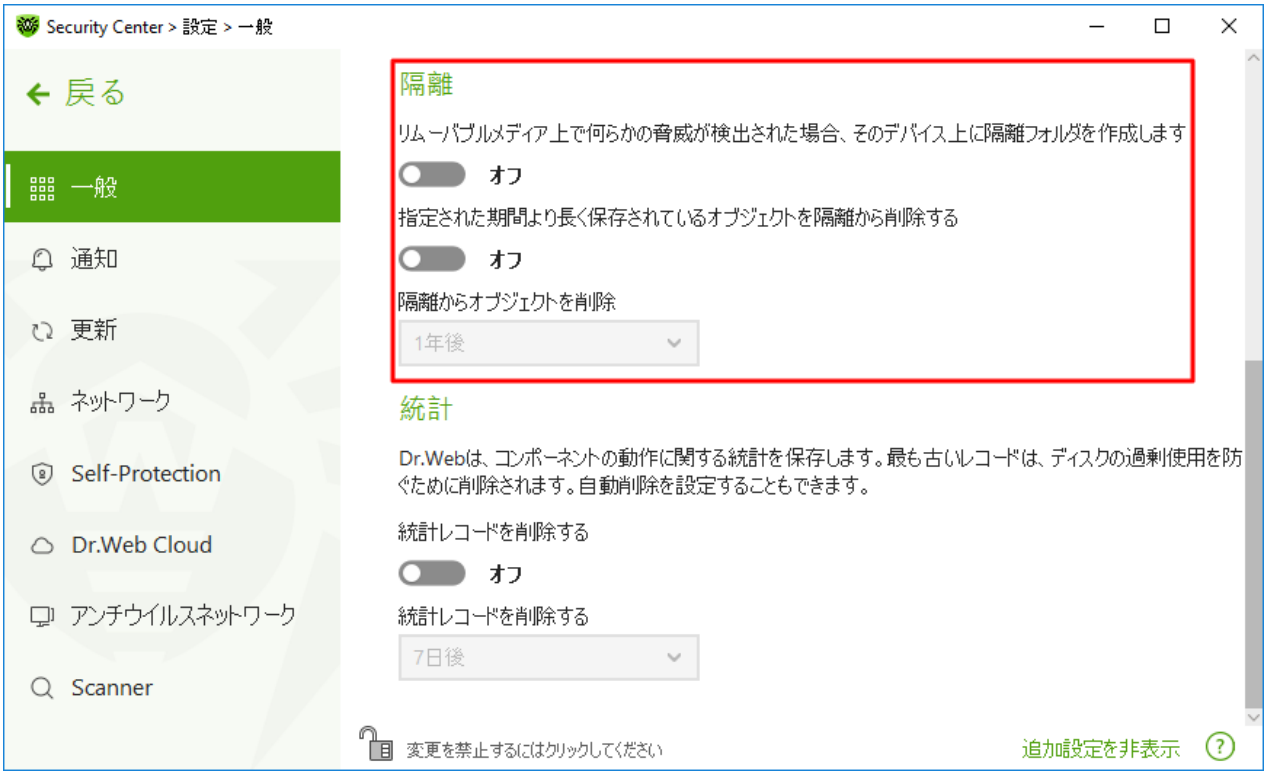

図26. 隔離設定

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。

9.1.7. 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。

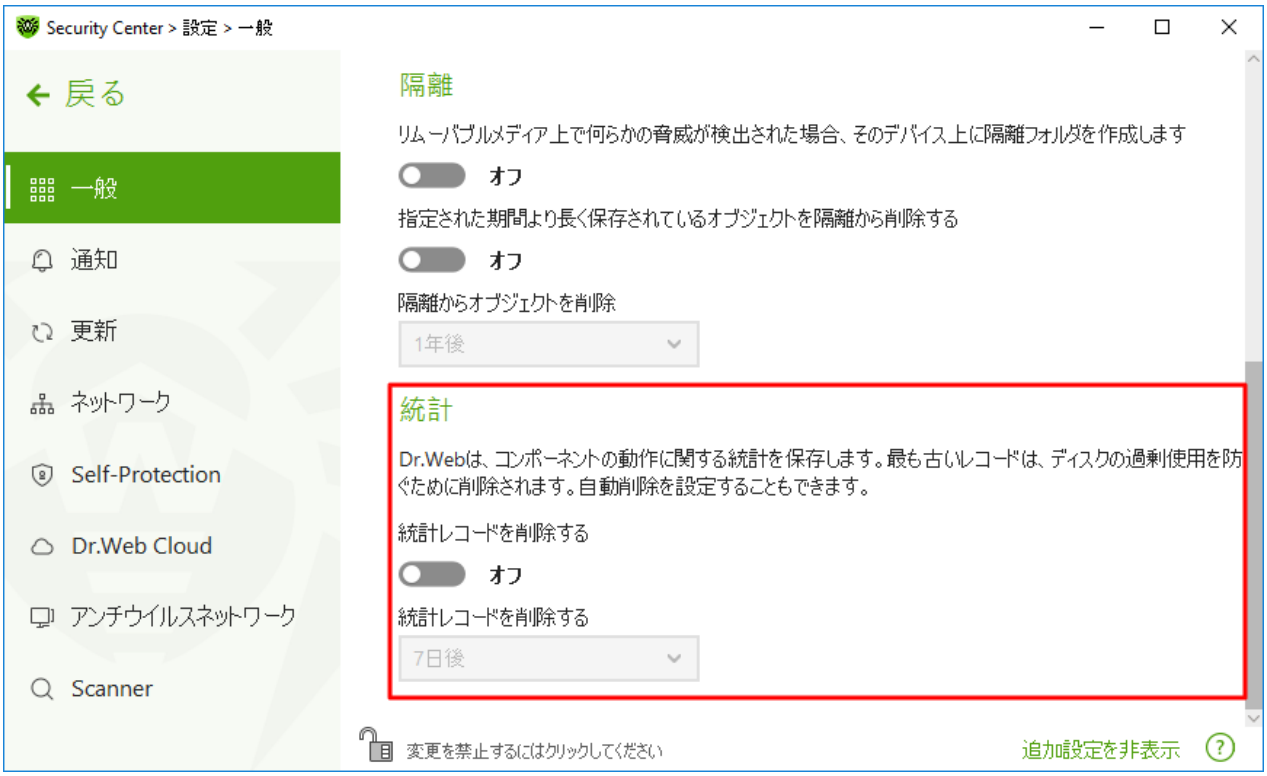

図27. 統計情報の設定

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。

9.2. 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
- デスクトップ上に通知を表示するための設定
- メール通知の設定

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 28.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。
   - デスクトップ上にポップアップ通知を表示するには、**デスクトップ** 列の該当するオプションを選択します。
   - メール通知を受信するには、**メール** 列の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： • Firewallからの応答を待つ接続が検出されました。 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：

通知タイプ	説明
	• 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。 • Webカメラやマイクへのアクセスがブロックされました。 • デバイスがブロックされました。 • 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。 • 製品のアップデートとサポートに関する情報
軽微な通知	以下の問題についての軽微な通知： • URLが Parental 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 Parental Control によってブロックされました。 • 更新が完了しました。 • 更新エラーです。 • プロセスによるフォルダ内容の変更がブロックされています。 これらの通知はデフォルトで無効になっています。ただし、プロセスによるフォルダ内容の変更試行のブロックに関する通知を除きます。
ライセンス	以下の問題についての通知： • ライセンスの有効期限が満了します。 • 有効なライセンスが見つかりませんでした。 • 現在のライセンスがブロックされています。

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。

4. メールでの通知を選択した場合は、コンピューターから メールを送信する 設定を行ってください。

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。
- アンチウイルスネットワーク内のリモートコンピューターへの接続に成功しました。
- トライアルライセンスが有効化されました。ライセンスの購入をお薦めします。
- 新しいキーボードが接続されました。

ポップアップ通知

通知設定ウィンドウで、Windows通知領域内にあるDr.Webアイコン 上の該当するオプションを有効にします。

メール通知

イベントに関するメール通知を受け取るには

1. 通知設定ウィンドウで、**通知をEメールで送信** オプションを有効にします。
2. 開いたウィンドウ内で、通知の受け取りに使用するメールアドレスを指定してください。手順7で、このメールアドレスを確定する必要があります。

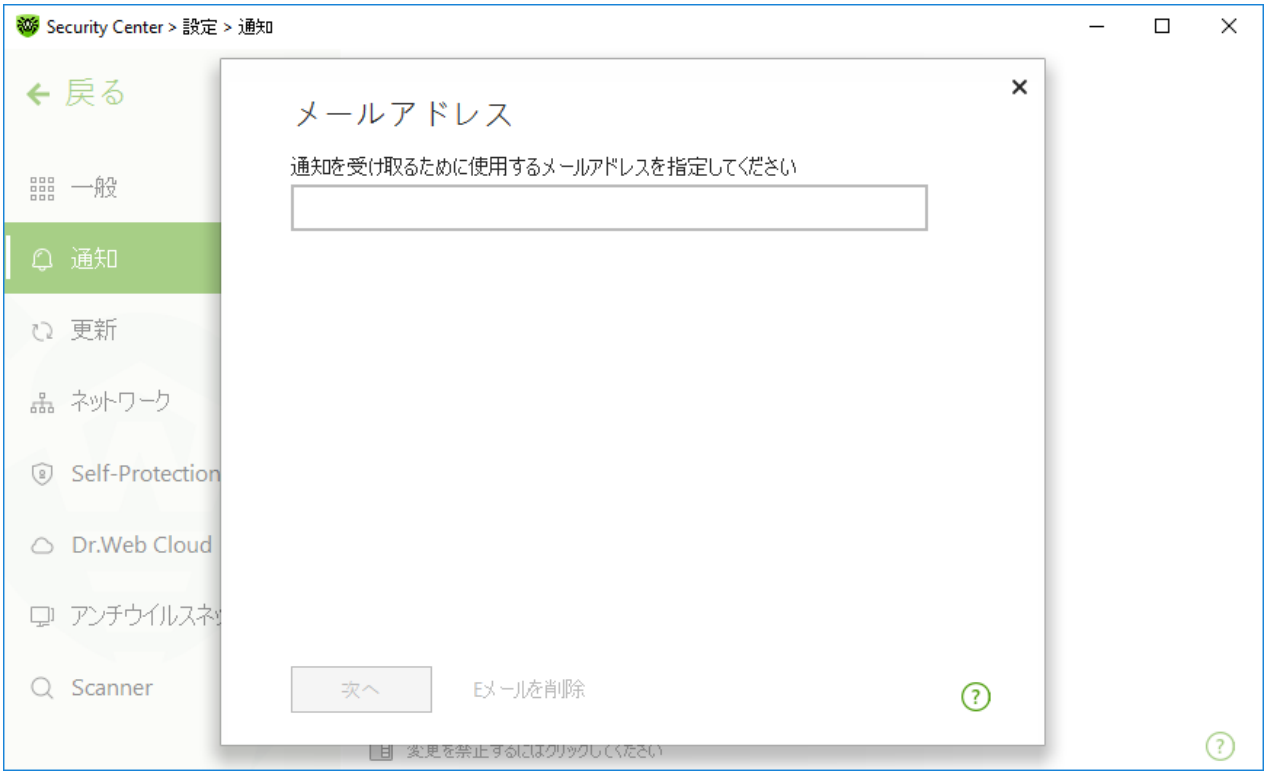

図 29. メール通知のアドレスの指定

3. **次へ** をクリックします。
4. 開いたウィンドウで、メール通知の送信に使用するアカウントの詳細を指定します。
   - リストからメールサーバーを選択し、使用するアカウントのログインとパスワードを入力してください。
   - 必要なメールサーバーがリストにない場合は、**手動で設定** を選択します。開いているウィンドウで、次のフィールドに入力します。

オプション	説明
SMTPサーバー	Dr.Webがメール通知送信に使用する送信（SMTP）サーバーを入力
ポート	Dr.Webがメールサーバーへの接続に使用するポートを入力
ログイン	Dr.Web がメールサーバーへの接続に使用するログインを入力
パスワード	メールサーバーへの接続時に使用するログインパスワードを入力
SSL/TLSを使用	メッセージ送信時にSSL/TLS暗号化を使用する場合は、このチェックボックスにチェックを入れます。
NTLM認証	メールサーバーへの接続時にNTLM認証を使用する場合は、このチェックボックスにチェックを入れます。

5. 設定したパラメータが正しいかどうかを確認するためにテストメッセージを送信するには **テストメッセージを送信** リンクをクリックします。通知の送信に使用されるメールアドレス（手順4で指定したもの）宛てにテストメッセージが送信されます。
6. **次へ** をクリックします。

7. 手順2で指定したメールアドレス宛てに送信された確認コードを入力します。10分以内にメッセージを受信しなかった場合は **コードを再度送信** をクリックしてください。コードが入力されなかった場合、このメールアドレスに対して通知は送信されません。

メールアドレスやその他のパラメータを変更する場合は、通知設定ウィンドウ（図 通知設定 参照）で **変更** をクリックし、手順2以降の操作を再度行ってください。

9.3. 更新設定

ウイルスデータベースおよびコンポーネントの更新を受信する期間と更新元を設定します。更新ミラーを作成して、別のコンピューターで更新を受信することもできます。

このページでは、以下のDr.Web更新パラメータを設定できます。

- 更新頻度
- 更新元
- 更新されるコンポーネント
- 更新ミラー

更新設定を開くには

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 **更新** を選択します。

図 30. 更新設定

更新頻度

デフォルト値(30分)は、脅威に関する情報を最新の状態に保つために最適な値となっています。更新頻度を指定するには、ドロップダウンリストから必要な値を選択します。

自動更新はバックグラウンドモードで実行されます。また、ドロップダウンメニューから **手動** オプションを選択することもできます。この場合、Dr.Webの更新を 手動で実行する 必要があります。

更新元を設定する

デフォルトの更新元は **Doctor WebのServer(推奨)** です。

更新元を選択するには

1. **更新元** グループの更新設定ウィンドウ(図更新設定を参照)で、**変更** リンクをクリックします。更新元の設定ウィンドウが開きます。

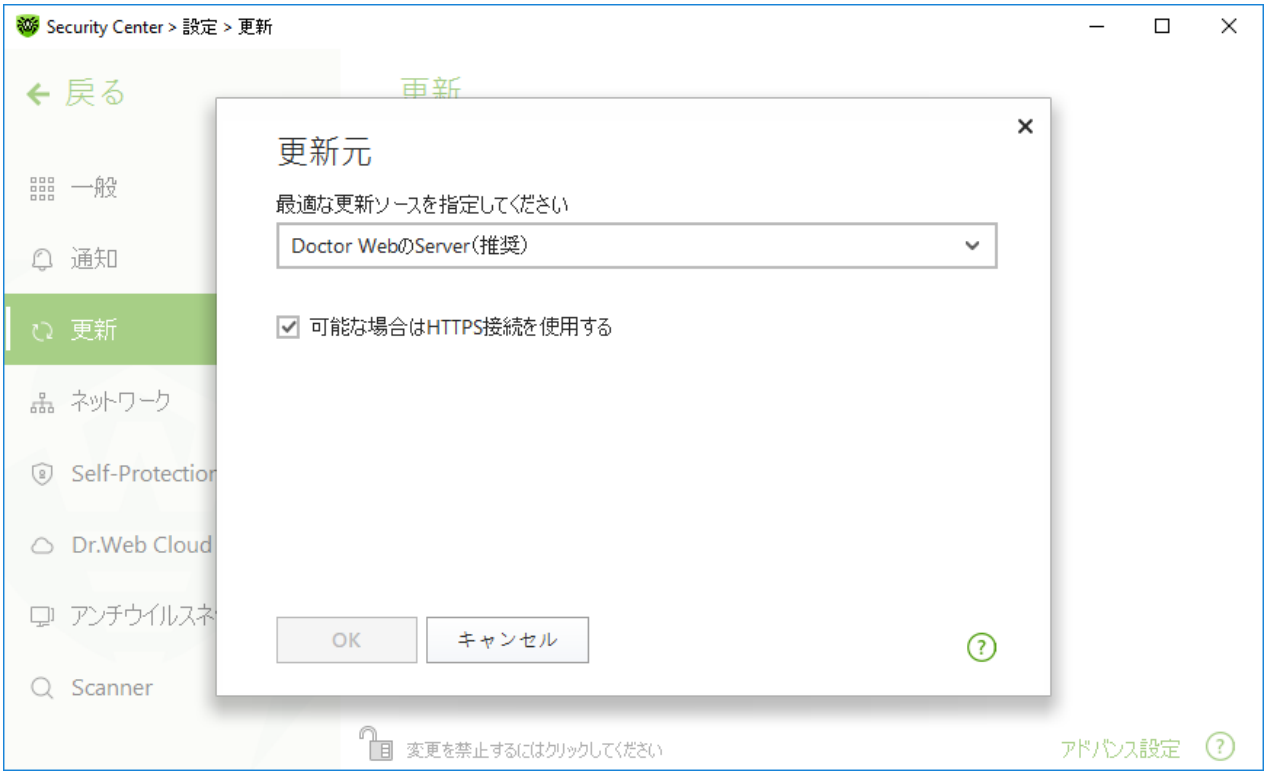

図 31. 更新元を設定する

2. ドロップダウンリストから更新元を選択します。
   - **Doctor WebのServer（推奨）** - インターネットを介したDoctor Webサーバーからの更新です。可能な場合に安全なプロトコル経由で更新をダウンロードする場合は **可能な場合はHTTPS接続を使用する** チェックボックスにチェックを入れてください。
   - **ローカルフォルダ・ネットワークフォルダ** - 更新がコピーされたローカルまたはネットワークフォルダからの更新です。フォルダへのパスを指定し（**参照** ボタンをクリックするか、またはUNCを使用して手動でパスを入力）、必要に応じてユーザー名とパスワードを入力してください。
   - **アンチウイルスネットワーク** - Dr.Web製品がインストールされ、更新ミラーが作成されたコンピューターを使用してローカルネットワークから更新します。更新元として使用するコンピューターを選択してください。
3. 設定を保存するには **OK** をクリックします。

Dr.Web製品のバージョン 12.0 が既にコンピューターにインストールされている場合、異なるDr.Web製品バージョンがインストールされているコンピューターを更新元として選択することはできません。重大な動作上の問題が発生する可能性があります。

詳細設定

詳細設定を開くには、**更新** 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 更新設定 参照）。

更新するコンポーネントを設定する

Dr.Web コンポーネントの更新をダウンロードするには、次のうちいずれかの方法を選択することができます。

- **全て（推奨）** - Dr.Webウイルスデータベース、スキャンエンジン、およびその他のDr.Webコンポーネントの更新をダウンロードします。
- **データベースのみ** - Dr.Webウイルスデータベース、スキャンエンジンの更新のみをダウンロードします。その他のDr.Webコンポーネントは更新されません。

更新ミラーの作成

更新ミラー は、更新ファイルがコピーされるフォルダです。ローカルネットワーク内にあるインターネットに接続されていない他のコンピューターのDr.Web更新元として使用することができます。

お使いのコンピューターを更新ミラーとして設定するには

1. 更新設定ウィンドウ（図 更新設定 参照）で **アドバンス設定** リンクをクリックし、スイッチ を使用して更新ミラーを有効にします。更新ミラー設定ウィンドウが開きます。

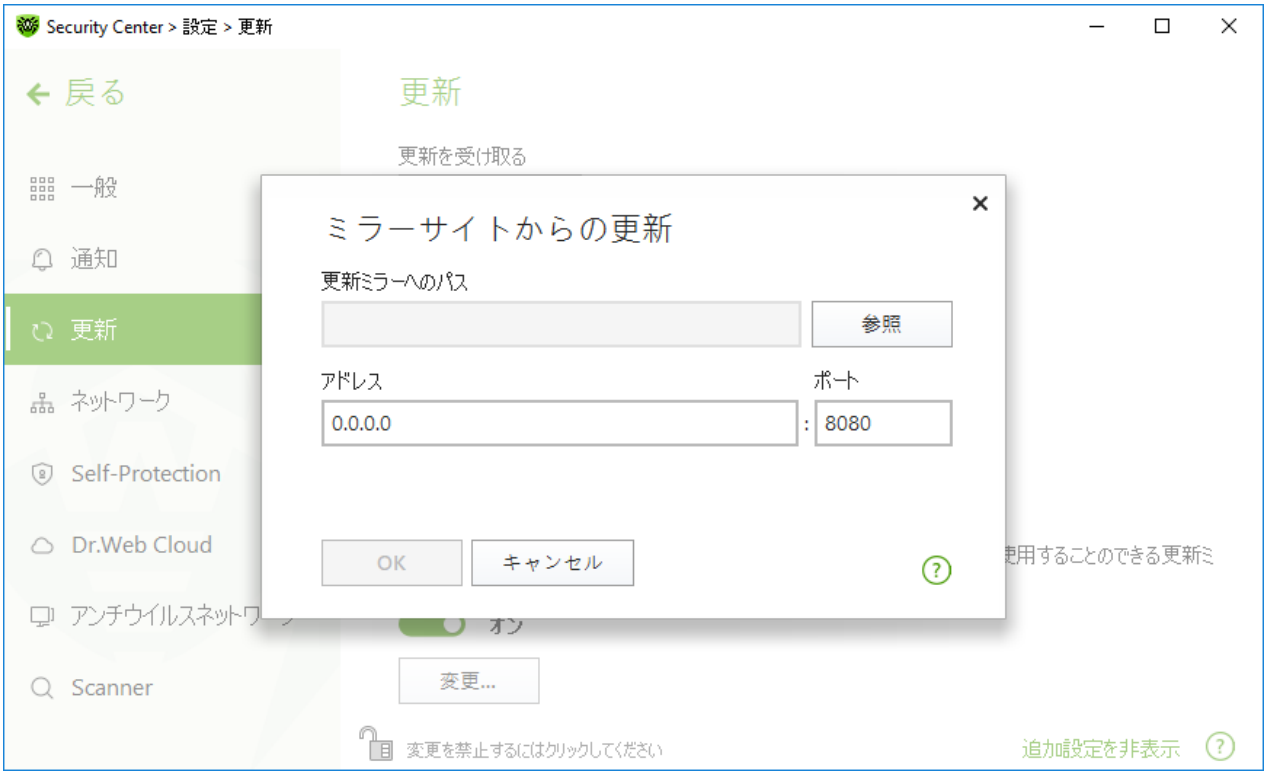

図 32. 更新ミラーを設定する

2. **参照** をクリックし、更新をコピーするフォルダを選択します。既存の空のフォルダを選択するか、新しいフォルダを作成してください。選択したフォルダが空でない場合、そのフォルダの内容がすべて削除されます。UNC形式でフォルダへのパスを指定することもできます。
3. お使いのコンピューターが複数のネットワークに接続されている場合、1つのサブネットのみのコンピューターで使用可能なIPアドレスを指定することができます。また、HTTPサーバーが接続要求を受信するためのポートを指定することもできます。
   - **アドレス** フィールドで、ホスト名またはIPアドレスを、Ipv4またはIpv6形式で指定します。

- ポート フィールドで、空いているポートを指定します。

4. 設定を保存するには **OK** をクリックします。

ミラーの更新頻度**更新を受け取る** で選択された値に応じたものになります。

9.4. ネットワーク

プロキシサーバーへの接続パラメータの設定、暗号化プロトコルを介して送信されたデータに対するスキャンの有効化、他のプログラムへのインポート用にDoctor Web証明書のエクスポートができます。

このセクションでは以下の設定を行うことができます。

- プロキシサーバーの接続設定
- 暗号化されたプロトコル経由でやり取りされたデータをスキャンする
- Dr.Web証明書をエクスポートする

ネットワーク設定を開くには：

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 ネットワーク を選択します。

図 33. プロキシサーバーへの接続および暗号化されたトラフィックの検査

プロキシサーバーの使用

デフォルトでは、すべてのコンポーネントが直接接続モードを使用します。必要に応じてプロキシサーバーの使用を有効にし、その接続設定を行うことができます。方法は以下のとおりです。

1. スイッチ を使用して、**プロキシサーバを使用する** オプションを有効にします。
2. **変更** をクリックし、次のプロキシサーバーのパラメータを設定してください。

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

安全な接続

Dr.Webによって、SSL、TLS、STARTTLSプロトコルでやり取りされるデータをチェックしたい場合は **暗号化されたトラフィックをスキャンする** オプションを有効にしてください。SpIDer Mail はPOP3S、SMTPS、IMAPS経由でやり取りされるメッセージ、ならびに SpIDer Gate はHTTPS経由でやり取りされるメッセージをチェックします。

安全な接続を使用するお使いのクライアントアプリケーション（メールクライアント）がデフォルトのWindowsシステム証明書ストレージを参照していない場合、Doctor Webセキュリティ証明書をエクスポートし、すべてのアプリケーションに手動でインポートする必要があります。

セキュリティ証明書の有効期間は1年です。必要に応じて、毎年証明書を再度インポートする必要があります。

セキュリティ証明書とは？

セキュリティ証明書は、プログラムが認証センターの1つで検査された認定プログラムであることを証明するための電子文書です。SSLプロトコル（Secure Socket Layer）が使用されているため、セキュリティ証明書はSSL証明書とも呼ばれています。ユーザーとWebサーバー間など、インターネット上のホスト間での暗号化された通信を提供します。

Webサイトのインターネットセキュリティ証明書を使用して動作するプログラムをインストール（インポート）すると、通信は認証チェック付きのセキュアモードで実行されます。これにより、犯罪者がデータを傍受することが困難になります。

次のアプリケーションでは、Dr.Web証明書のインポートが必要な場合があります。

- Operaブラウザ

- Firefoxブラウザ
- Mozilla Thunderbirdメールクライアント
- The Bat!メールクライアントなど

Dr.Web証明書をエクスポート／インポートするには

1. エクスポート ボタンが有効になっていない場合は、スイッチ を使用して 暗号化されたトラフィックをスキャンする オプションを有効にします。これにより、Dr.Webセキュリティ証明書が生成されます。
2. エクスポート をクリックします。
3. 証明書を保存するフォルダを選択します。**OK** をクリックします。
4. 証明書を対象のアプリケーションにインポートします。証明書のインポートの詳細については、対象アプリケーションのユーザーマニュアルを参照してください。

> 暗号化されたトラフィックをスキャンする が有効になっている場合、クラウドストレージクライアント（Googleドライブ、Dropbox、Yandex.Diskなど）を正しく動作させるには、これらのアプリケーションを SpIDer Gate によるスキャンの対象から除外してください。

9.5. 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改変や誤った破損から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 34. 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ぐことができます（Dr.Web設定を変更するスクリプト、ライセンスの削除、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 Parental Control の 時間制限機能 を強化することができます。Parental 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。

9.6. Dr.Web Cloud

Doctor Webクラウドサービスに接続し、Dr.Web品質向上プログラムに参加することができます。クラウドサービスは、ユーザーの端末上で検出された脅威に関する最新の情報を収集し、ウイルスデータベースが定期的に更新され、最新の脅威が効果的に駆除されるようにします。さらに、クラウドサービスではローカルコンピューター上と比べてより高速にデータが処理されます。

このセクションでは以下の設定を行うことができます。

- クラウドサービス
- ソフトウェア品質向上プログラム

Dr.Web Cloud 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 **Dr.Web Cloud** を選択します。
5. スイッチ を使用して、Dr.Web Cloud を有効または無効にします。

図 35. Dr.Web Cloudに接続する

クラウドサービス

Dr.Web Cloud は、Doctor Webのサーバー上でリアルタイムに更新される最新の脅威情報を使用したアンチウイルス保護を提供します。

更新設定によっては、アンチウイルス保護コンポーネントによって使用される脅威に関する情報が古くなる場合があります。クラウドサービスを使用すると、望ましくないコンテンツや感染したファイルが含まれているWebサイトからコンピューターのユーザーを保護できます。

ソフトウェア品質向上プログラム

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

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

9.7. Dr.Webへのリモートアクセス

アンチウイルスネットワーク コンポーネントを使用して、ローカルネットワークの他のコンピューターからのアンチウイルスのリモートコントロールを有効にすることができます。アンチウイルスネットワークを使用すると、セキュリティ状態（統計の表示、コンポーネントの有効化または無効化、それらの設定の変更）をリモートで制御し、ローカルネットワーク経由で更新を受け取ることができます。Dr.Webがインストールされている他のアンチウイルスネットワーク

コンピューターの更新元としてコンピューターを使用するには、そのコンピューター上で ミラーサイトからの更新 を設定します。

Dr.Webのリモートコントロールを有効／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 **アンチウイルスネットワーク** を選択します。
5. スイッチ を使用して、リモートコントロールを有効または無効にします。

図 36. アンチウイルスネットワーク

お使いのコンピューター上のDr.Web設定へリモートでアクセスするにはコードが必要です。オプションを有効にした際に自動的に生成されたコードを使用するか、または新しく設定することができます。

リモートコントロールを使用すると、統計情報を表示したり、コンポーネントを有効または無効にしたり、それらの設定を変更したりできます。隔離、Scanner、データ損失防止、アンチウイルスネットワーク は利用できません。

9.8. 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。

図 37. 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)内のファイルを除く、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)内のファイルを除く、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。
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。

10. 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38. 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* 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。

10.1. 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、感染を防ぎます。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、起動したプロセスの動作も監視します。

SpIDer Guard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 39. 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動作の特性
- 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 動作の特性

デフォルトの設定では、SpIDer Guard はハードドライブ上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上で開かれているすべてのファイルに対してオンアクセススキャンを実行します。さらに、ウイルスのようなアクティビティがないかどうか実行中のプロセスを常時監視し、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 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しません。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ロードされ、現在のWindowsセッション中にはアンロードできません。

SpIDer Guard 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 40. SpIDer Guardの設定

リムーバブルメディアのスキャン

デフォルトでは、SpIDer Guard はハードドライブ上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上で開かれているすべてのファイルに対して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、コンピューター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、ファイルシステムモニター SpIDer Guard によって検出された脅威に対するDr.Webのアクションを設定できます。

図 41. 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。処理されたすべ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)内のファイルを除く、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)内のファイルを除く、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。

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	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にのみオブジェクトをスキャンします。 • 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 Dr.Web Scannerがすべてのハードドライブを徹底的にスキャン した後で、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「クリーン」であることが判明しているオブジェクトをスキャン対象から除外することによってパフォーマンスを維持しつつ、新しいウイルスやその他の悪意のあるオブジェクトがリムーバブルメディアを介してコンピューターに侵入することを防ぎます。
パラノイド	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、または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。 このモードでは最大限の保護が提供されますが、コンピューターのパフォーマンスは大幅に低下します。

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ます。これらの設定は、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。

> ルートキットのバックグラウンドスキャン中には、除外するファイル ページで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。

10.2. 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をチェックできます。これを行うには、ネットワーク セクションの **暗号化されたトラフィックをスキャンする** オプションを有効にします。

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。そのようなWebサイトに関する情報は、Dr.Webクラウドサービスに保存されているリアルタイムデータからも取得されます。

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42. 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。

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43. 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 のリストが適用されます。

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ーの負荷が増えます。

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。

10.3. 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、POP3S、SMTPS、IMAPS経由で転送された暗号化メールトラフィックをスキャンできます。これを行うは、ネットワーク セクションで**暗号化されたトラフィックをスキャンする** オプションを有効にします。

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 44. 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、またはスケジュールに従ってメールボックスをチェックします。さらに、このアクションはリソースを消費する上に時間がかかる場合があります。

10.3.1. 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 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
- 暗号化されたプロトコル経由でやり取りされたメールをスキャン

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。

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45. 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。

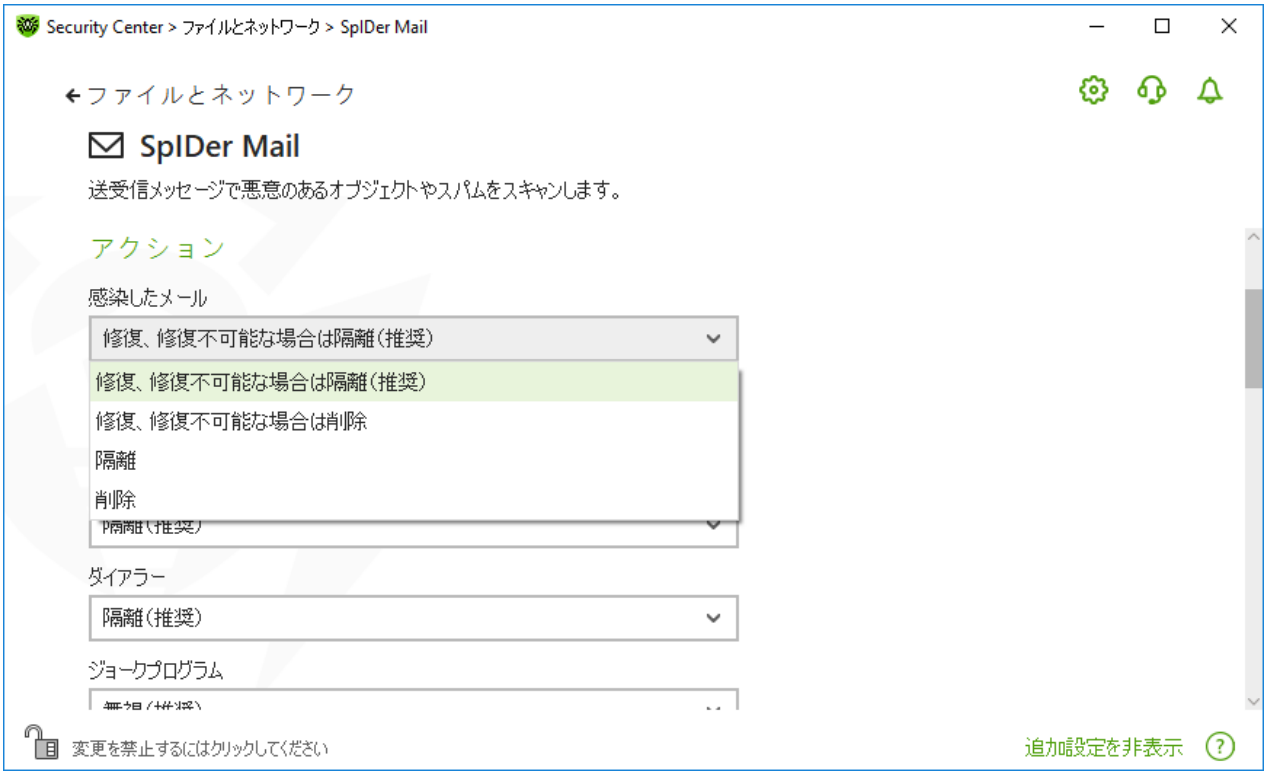

図 46. メッセージに対するアクションを設定する

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。

セキュリティー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 およびメールの通知を 設定 することができます。

POP3S、SMTPS、IMAPS経由で送受信されたメッセージのスキャン

SpIDer Mail によって、暗号化プロトコル経由で送受信されるデータをスキャンする場合は、ネットワーク ウィンドウ内で **暗号化されたトラフィックをスキャンする** オプションを有効にします。

10.3.2. 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47. 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。

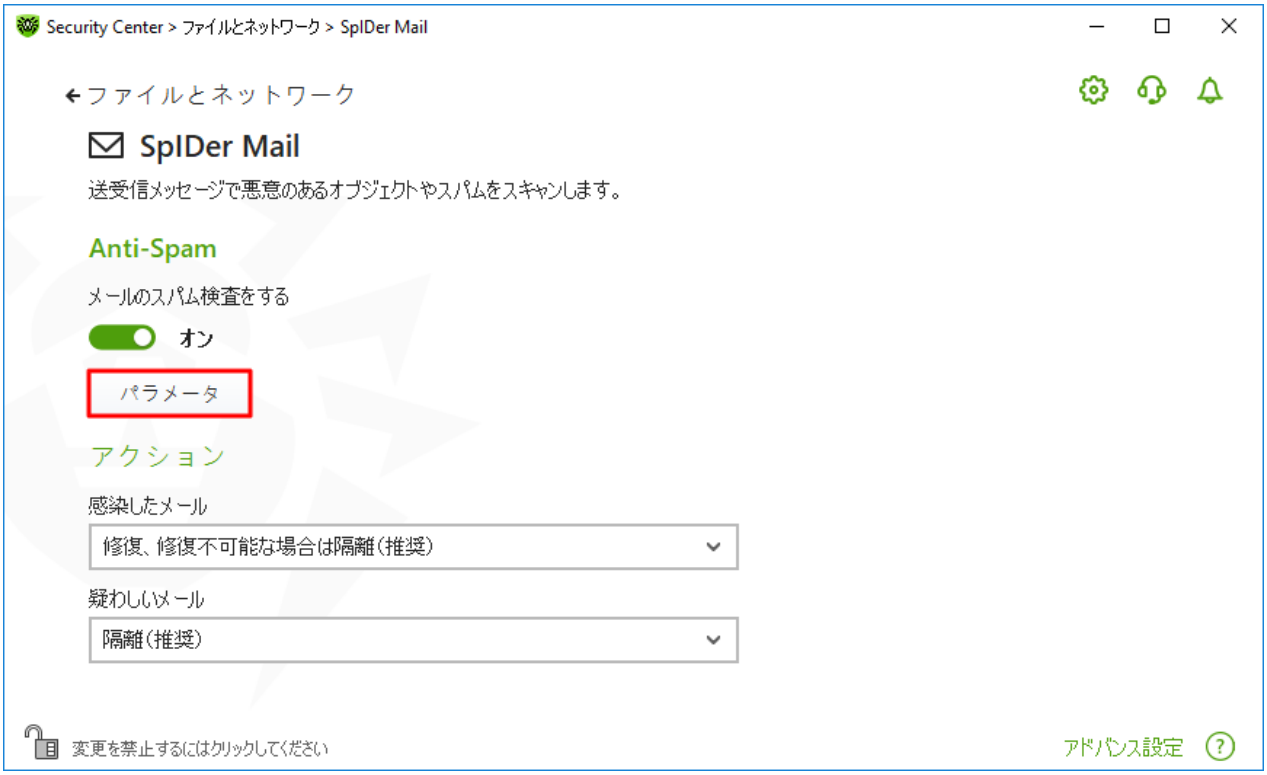

図 48. Anti-Spamのパラメータを変更する

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。

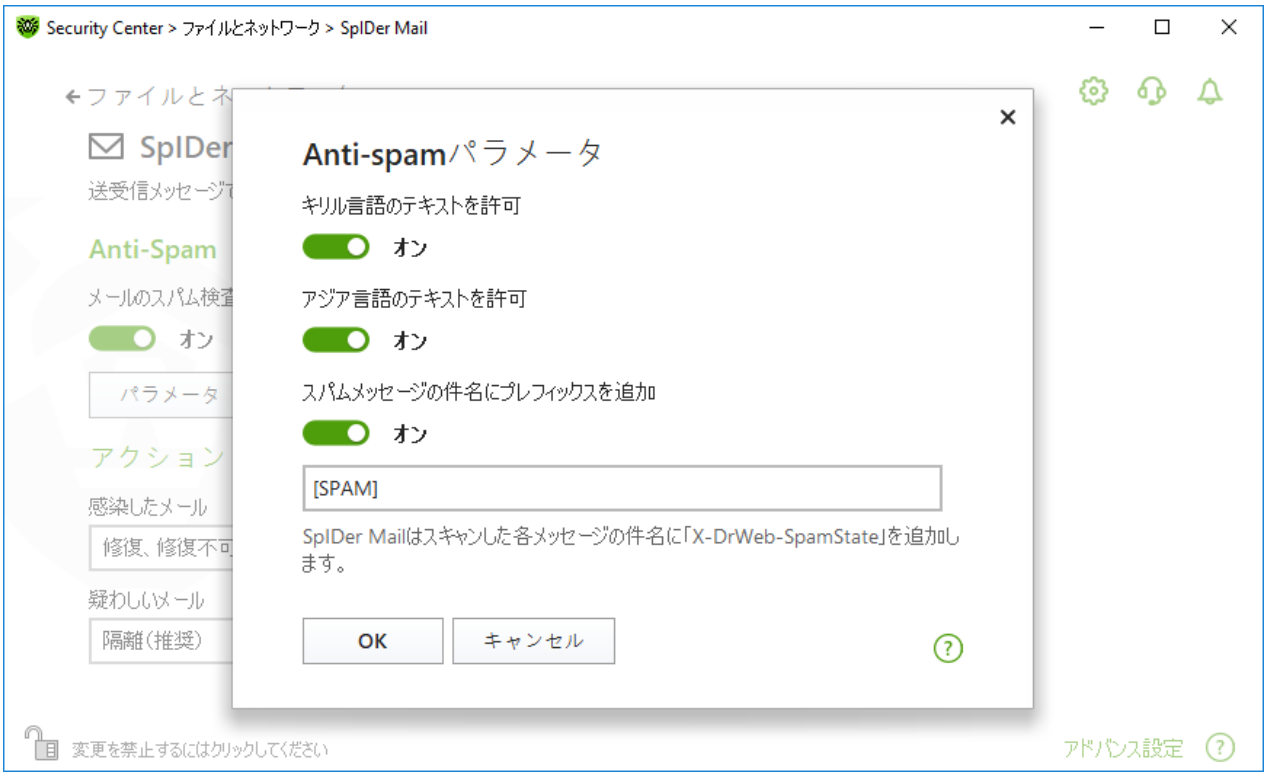

図49. Anti-Spamのパラメータ

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ール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	SpIDer Mailがアジア言語のエンコードが使用された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、そのようなメールはスパムと見な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** - メールのすべてのパート（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** - Anti-Spam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、Anti-Spam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。
- **アンチスキャム** - 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、スキャムおよびファーミ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>* にはさまざま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. 添付ファイル付きのメッセージを以下のアドレスのいずれかに送信してください。
   - 誤ってスパムと判定されたメッセージは nonspam@drweb.com へ送信してください。
   - 検出されなかったスパムメッセージは spam@drweb.com に送信してください。

10.4. 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 50. 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

10.4.1. 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51. 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	デフォルトではこのモードが適用されます。 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。 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。
未知の接続を許可	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。
インタラクティブモード	このモードでは、未知の接続を検出した際のFirewallの動作をユーザーによって完全に管理します。 ユーザーアプリケーションまたはオペレーティングシステムからネットワークへの接続が試行された場合、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。
未知の接続をブロック	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。 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。

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。

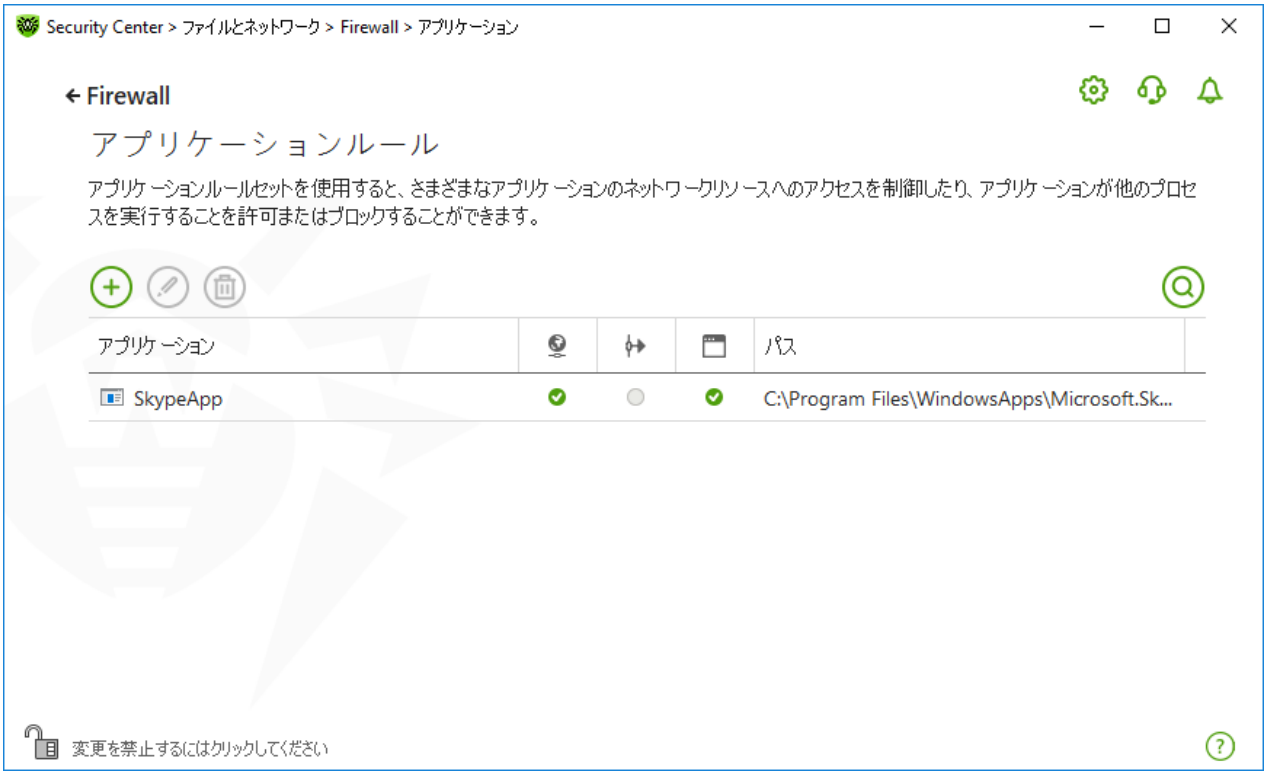

図52. アプリケーションルール

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。

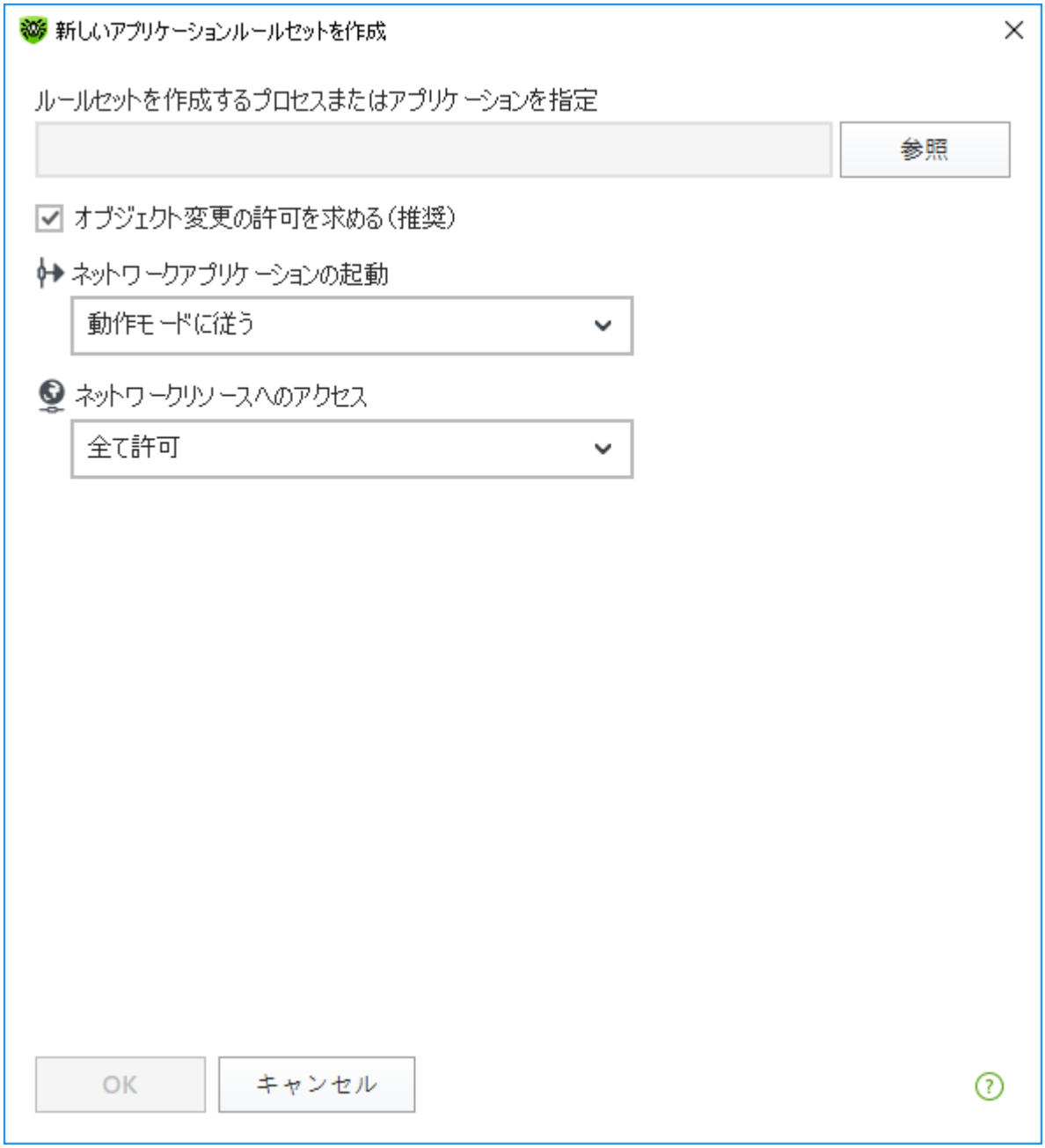

図 53. 新しいルールセットの作成

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: • **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: • **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ようにするには、**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。

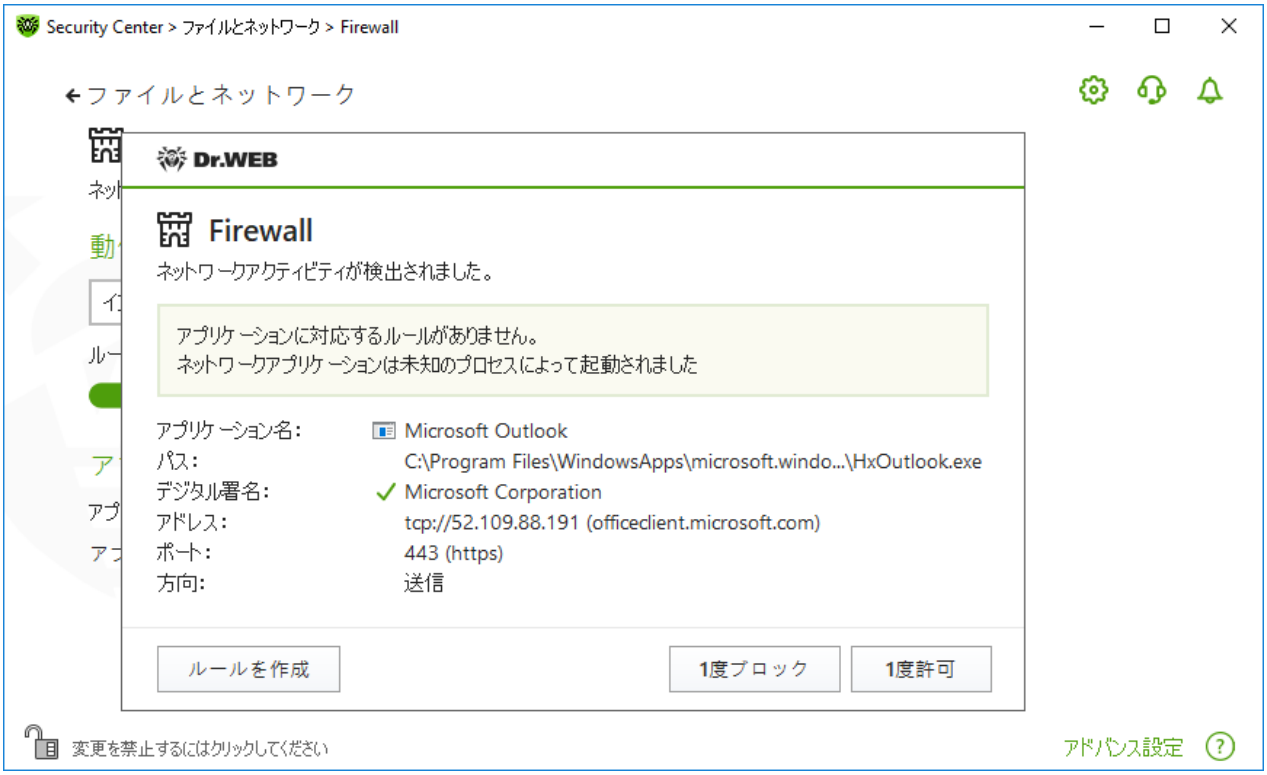

図54. ネットワーク接続試行の通知の例

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、✎ 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: • **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: • **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: • **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: • **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。 • 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。 • 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55. ネットワークインターフェースのルールセット

7. 必須インターフェースには、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ース 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を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ー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ー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ー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ースを削除できます。

インターフェースパラメータにアクセスするには、インターフェー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。

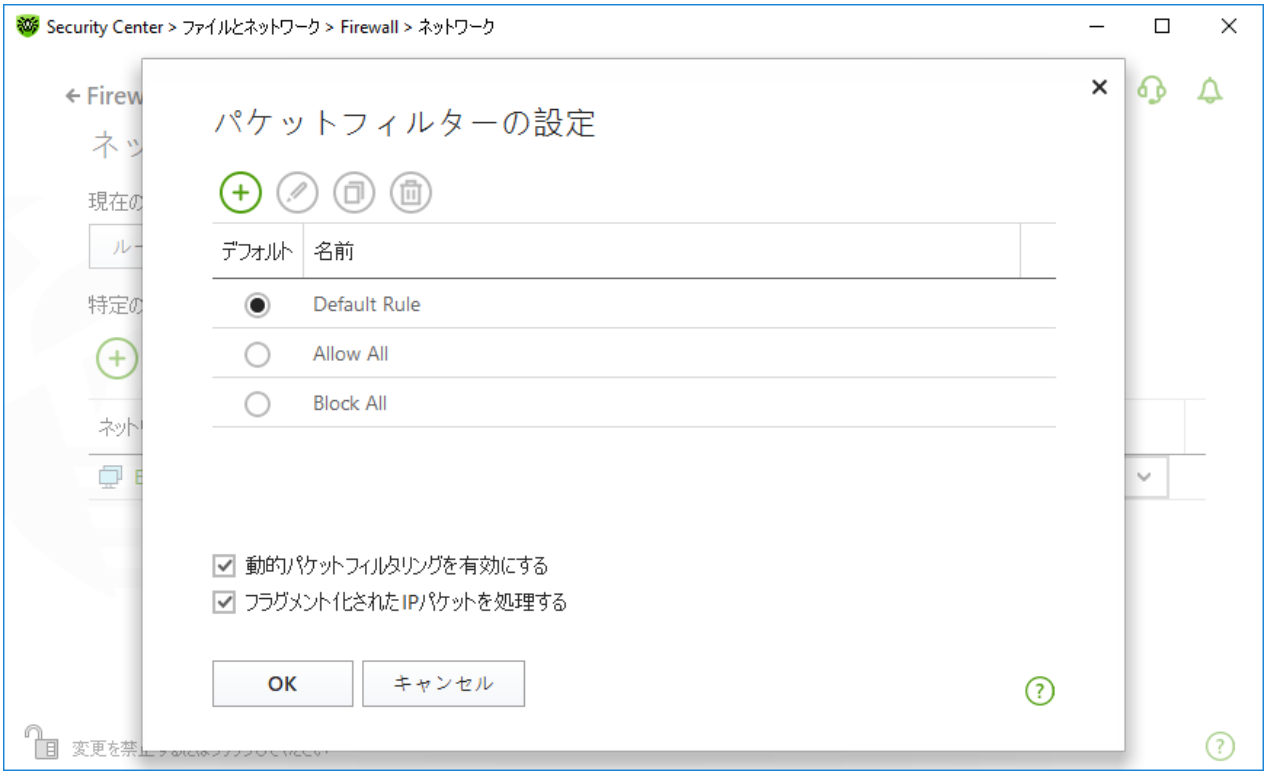

図56. パケットフィルターの設定

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
	（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。 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。 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。
フラグメント化されたIPパケットを処理する	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。 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。

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。

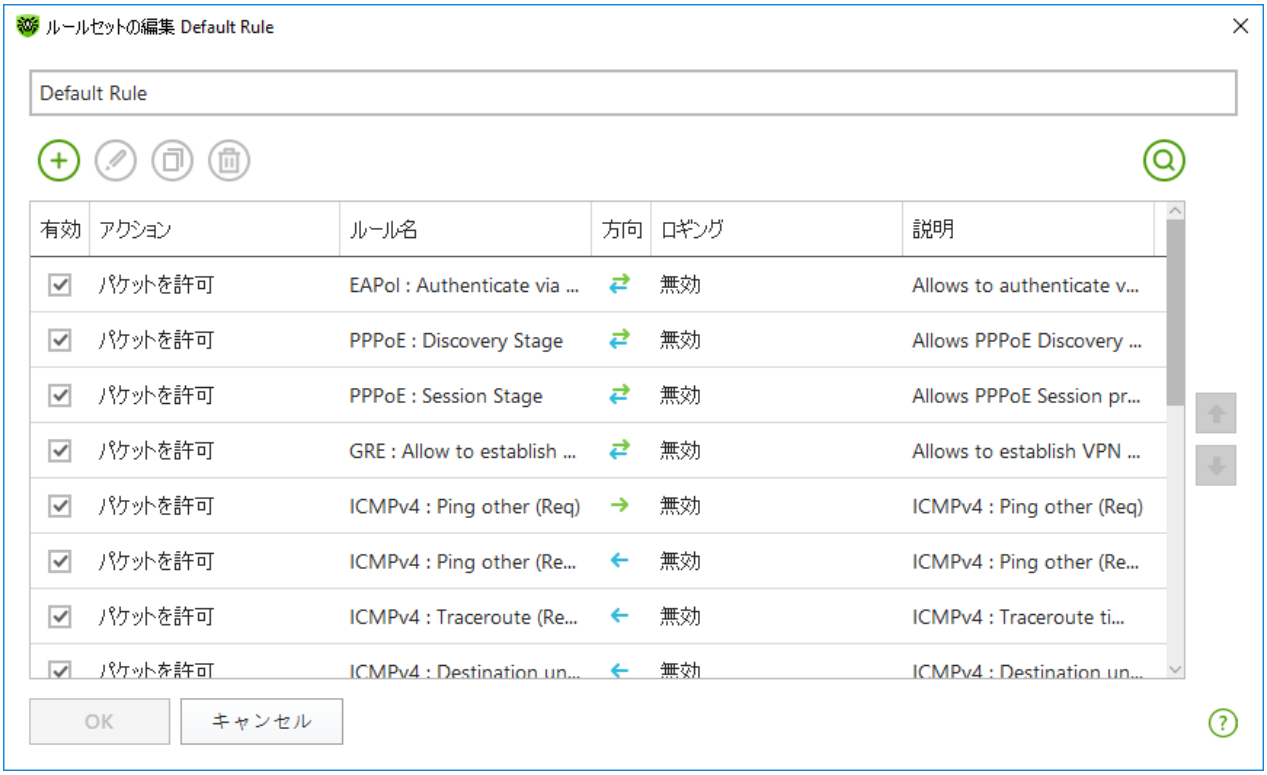

図 57. パケットフィルタリングのルールセット

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: • **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: • ← - 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。 • ⇄ - 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。 • **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。

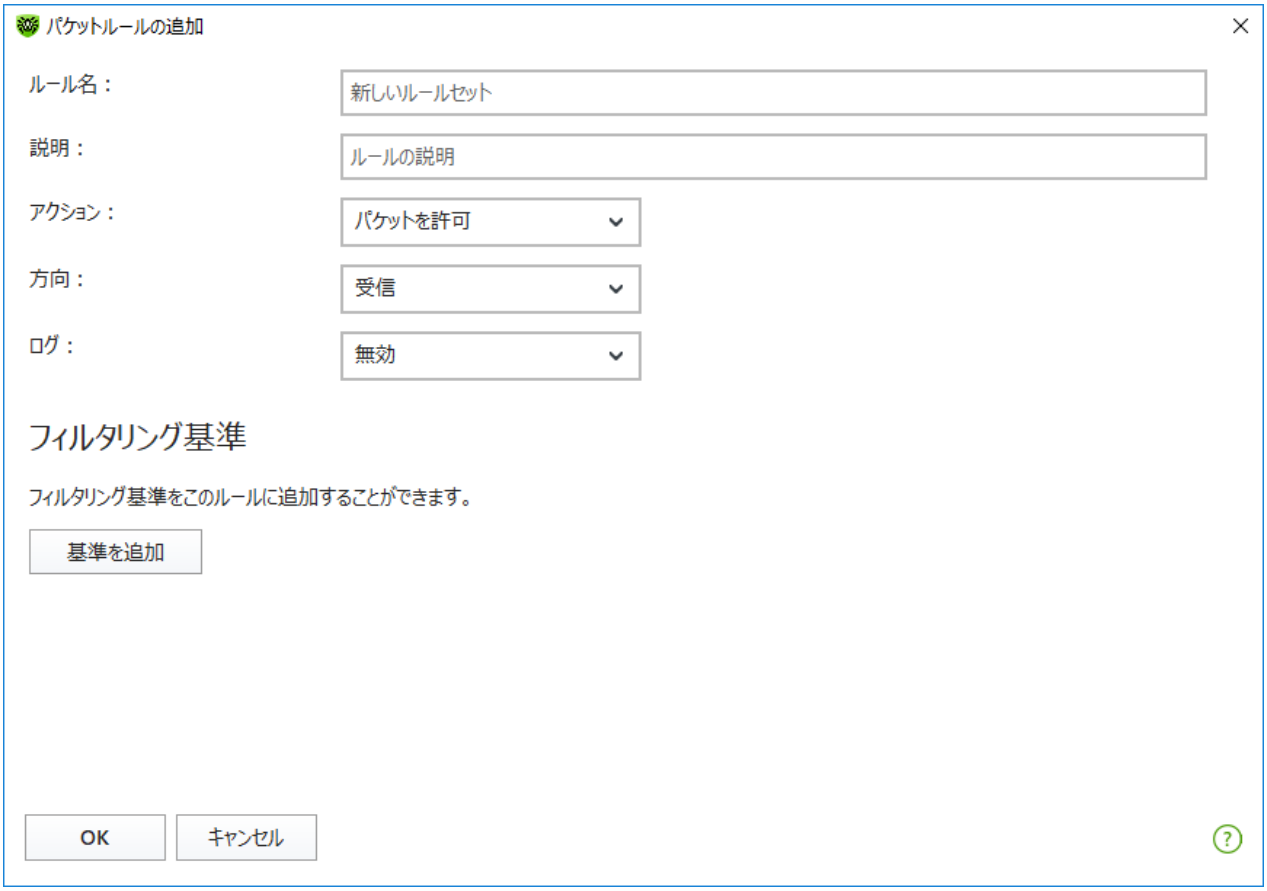

図 58. フィルタリングルールを追加する

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： • **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： • **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。 • **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。

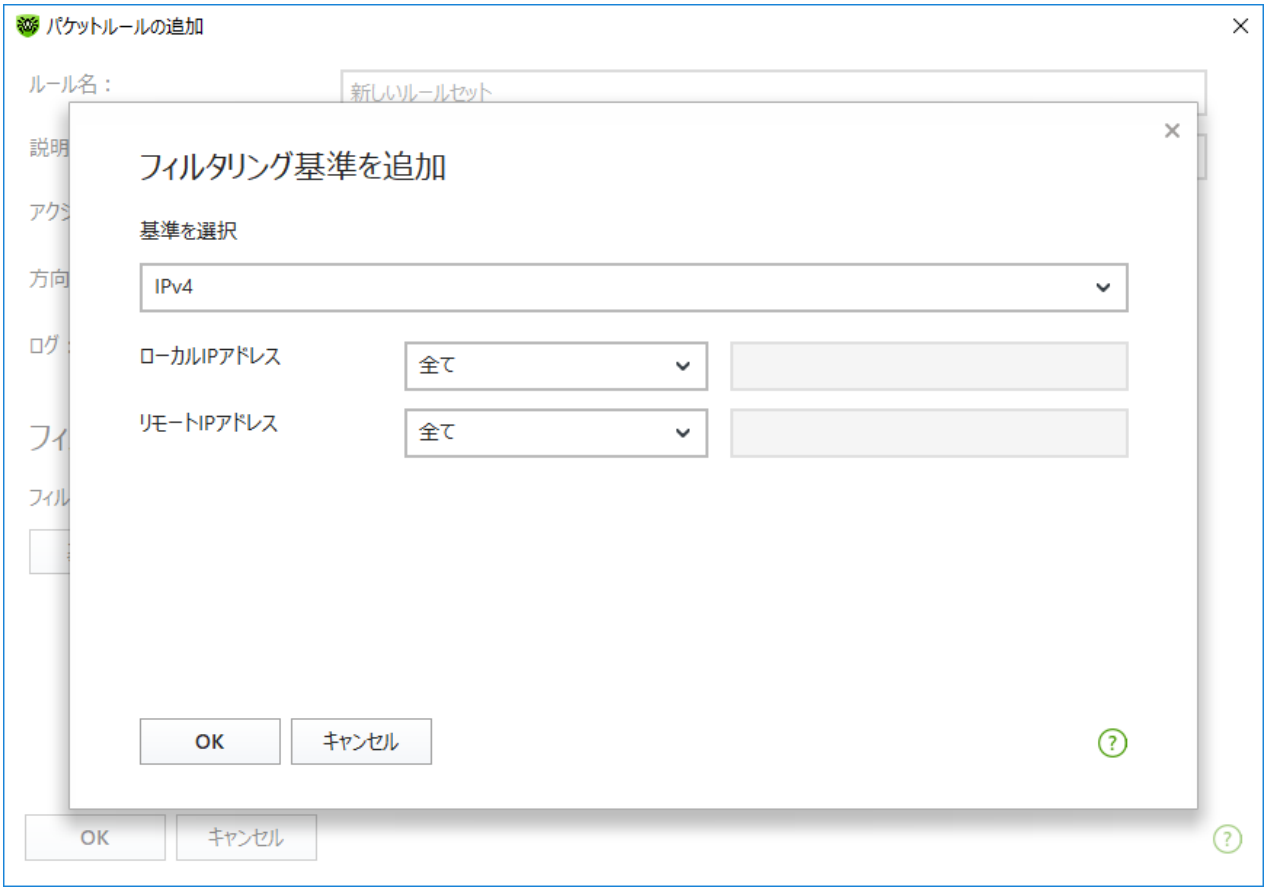

図 59. フィルタリング基準を追加

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すべ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。

10.5. 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

10.5.1. 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す。

図 60. 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。 • 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
	• 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） ⚠ 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。
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。

10.5.2. 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 61. 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。

10.5.3. 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
- スキャンの自動実行

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。スケジュールによるScannerの自動起動は、このモードで実行されます。

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。

11 - キーファイルが見つからないか、Console Scannerをサポートしていません。

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。

タスクスケジューラを介してシステムをスキャンする

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

タスク設定を確認するには、**コントロールパネル** （拡張ビュー）→ **管理ツール** →**タスクスケジューラ** を開いてください。

タスクの一覧から、スキャンタスクを選択します。タスクの有効化、開始時間の調整、必要なパラメータの設定を行うことができます。

全般 タブで、特定のタスクに関する全般情報およびセキュリティオプションを確認することができます。**トリガー** と **条件** ページでは、タスクを起動するための様々な条件を設定することができます。**ログ** ページではイベントログを参照することができます。

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

インストールされたコンポーネントに Firewall が含まれていた場合、Dr.Web のインストールが完了した後の一度目のシステム再起動後、タスクスケジューラは Firewall にブロックされます。スケジュールされたタスクは、新しいルールが作成された二度目の再起動の後に実行されます。

10.6. 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
- SSL暗号化接続を介して送受信されたメール添付ファイルのチェック
- スパム検査
- 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 - スパム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。

10.6.1. 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。

10.6.2. スパム検査

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

Anti-spamフィルターのパラメータを設定する

1. Anti-Spam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、解析とフィルタリング精度向上のためにそのメッセージを以下のアドレスに送信することができます。

- 誤ってスパムと判定されたメッセージは nonspam@drweb.com へ送信してください。
- ブロックされなかったスパムメッセージは spam@drweb.com へ送信してください。

メッセージは添付ファイルとして送信し、メッセージ本文には入れないようにしてください。

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、Anti-spam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。

10.6.3. 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す。

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

イベントログを表示するには

1. 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 メールのソースは 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。

- ライセンスの妥当性
- 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
- ライセンス失効の通知（失効の30日、15日、7日、3日、2日、および1日前にメールが記録されます）

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。

10.6.4. 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
- **スパムメール** - スパム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 Security Space が再起動された場合はゼロにリセットされます。

11. 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62. Preventive Protection 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。

- Ransomware Protection - ユーザーファイルの暗号化を防止します。
- 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。
- 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。

コンポーネントを *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。

11.1. 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 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、**Preventive Protection** タイルをクリックします。
3. スイッチ を使用して、Ransomware Protection を有効または無効にします。

図63. Ransomware Protection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。

- 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
- スキャン対象からの除外

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、すべ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。

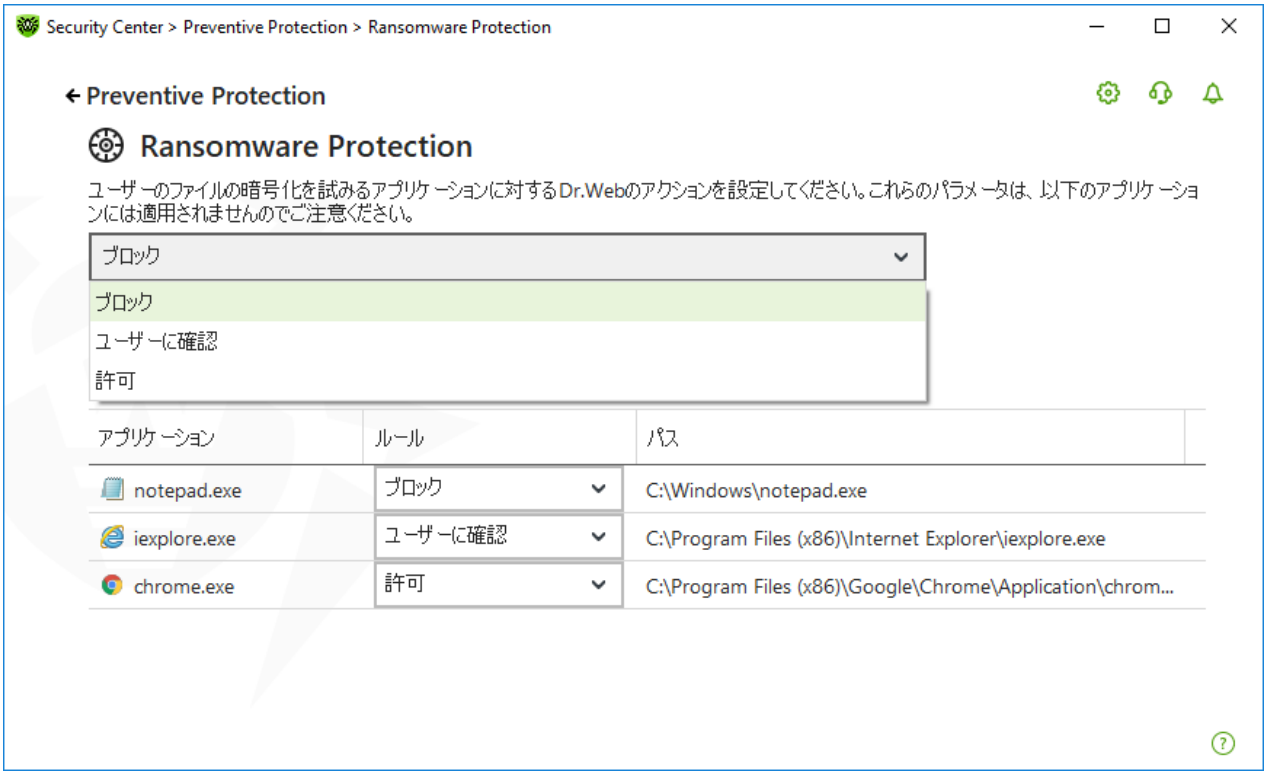

図64. Dr.Webのアクションを選択する

- **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** - すべ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と、以下の通知が表示されます。

図65. 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。

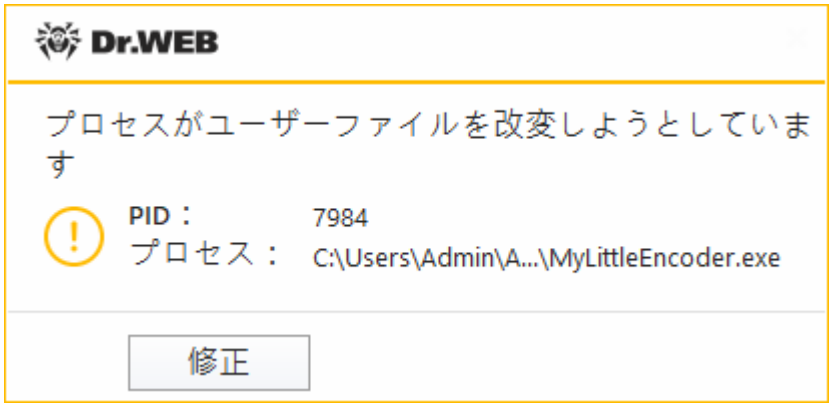

図66. アプリケーションがユーザーファイルを変更しようとした場合の通知例

  - **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、デスクトップとメールの通知を 設定 できます。

以下も参照してください。

- 通知

スキャンから除外するアプリケーションのリスト

Ransomware Protectionスキャンから除外するアプリケーションのリストを作成できます。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除外リストに追加します。
- 🗑 ボタン - アプリケーションを除外リストから削除します。

図67. ランサムウェア保護スキャンから除外する

アプリケーションをリストに追加するには

1. ⊕ をクリックし、開いたウィンドウで必要なアプリケーションを選択します。
2. **OK** をクリックします。

不正な変更からデータを保護するために、保護するファイルのリストにファイルを追加 することもできます。

11.2. 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信頼されていない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。アプリケーションが悪意のあるものであるかどうかを判断するために、コンポーネントはDr.Webクラウドサービスからのリアルタイムデータを使用します。

Behavior Analysis 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、**Preventive Protection** タイルをクリックします。
3. スイッチ を使用して、Behavior Analysis コンポーネントを有効または無効にします。

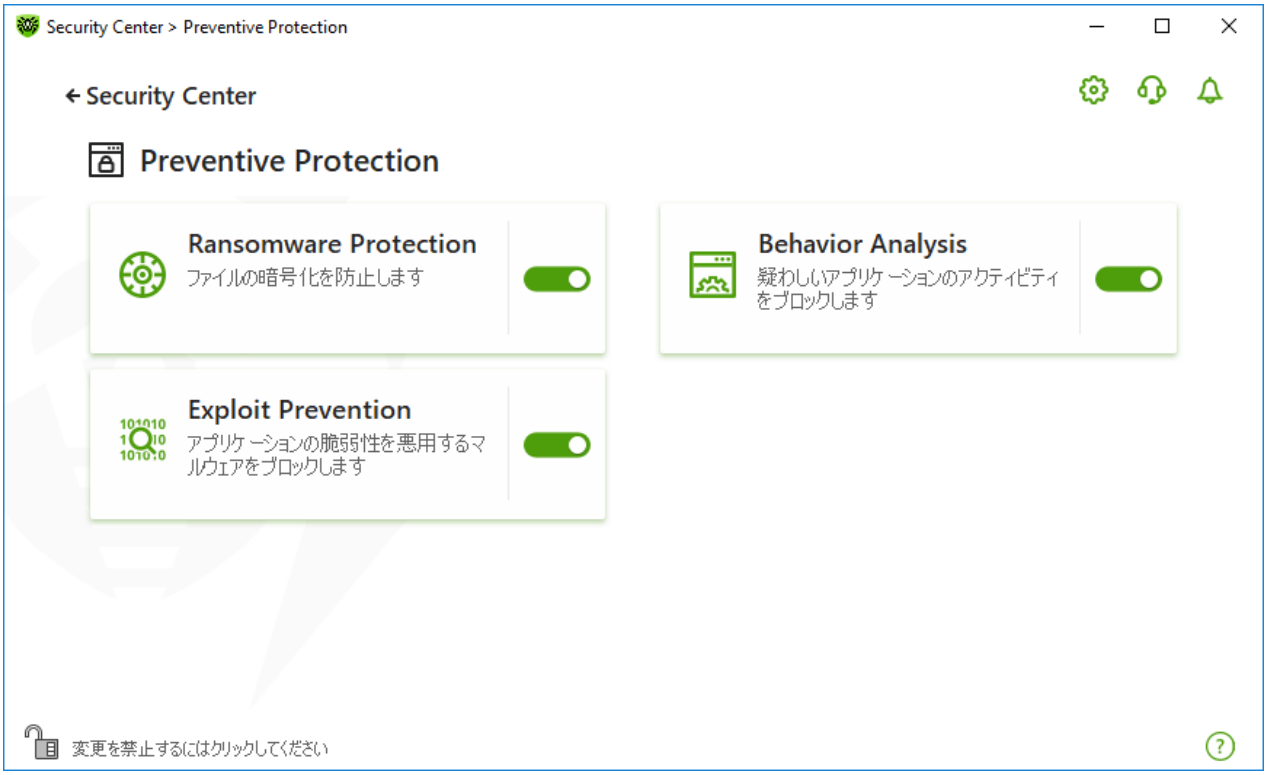

図68. Behavior Analysis コンポーネントを有効／無効にする

このセクションでは以下の設定を行うことができます。

- 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。

Behavior Analysis 設定を開くには

1. Dr.Webが 管理モード 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）。管理モードではない場合は、ロックをクリックします。
2. **Behavior Analysis** 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。

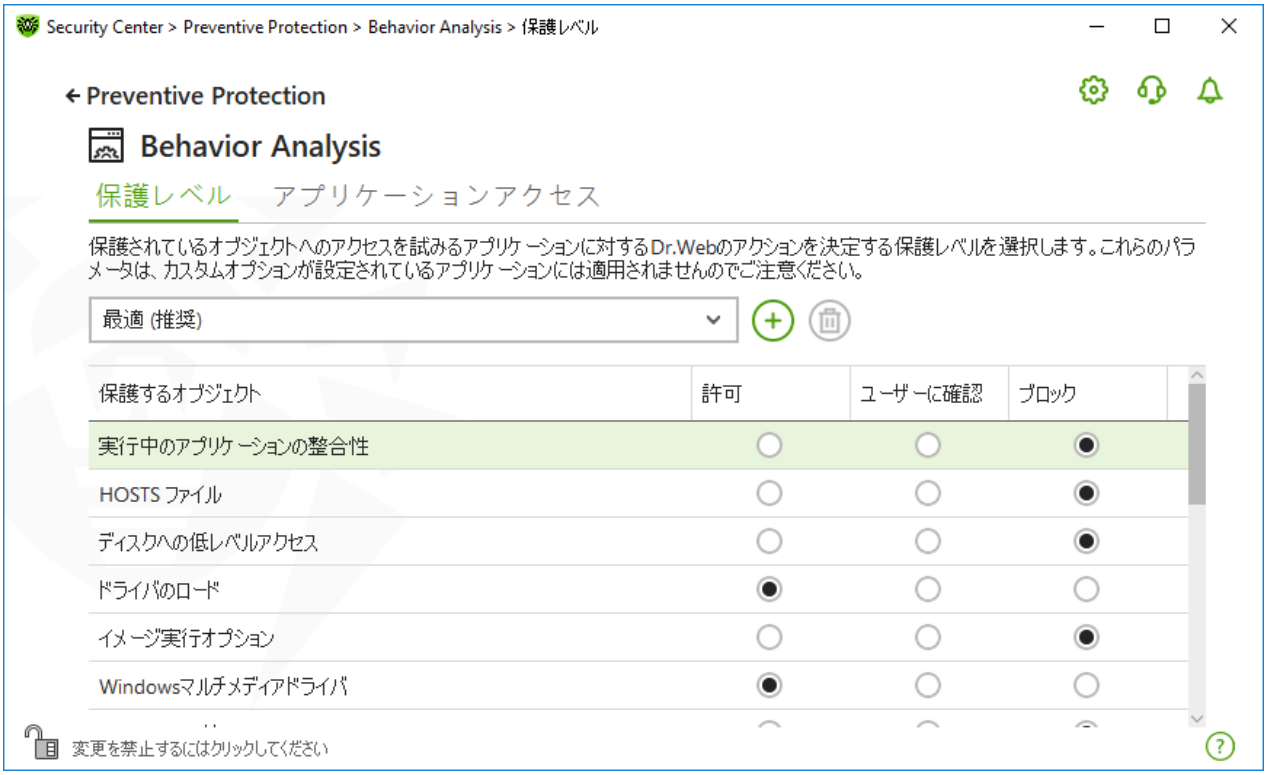

図69. Behavior Analysisの設定

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、すべ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）	このモードはデフォルトで設定されています。オペレーティングシステムに害を及ぼそうとする悪意のある意図を持った、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害を与える悪意のある試みであることが明らかな場合、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。 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。
中	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。 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。

保護レベル	説明
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、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することもできます。
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

すべての変更はユーザーモードで保存されます。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。保護するオブジェクトは、すべてのコンポーネント設定で確認できます。

保護されたオブジェクトを変更しようと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、すべ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と、通知が表示されます。

図70. 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と、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71. 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、デスクトップとメールの通知を設定 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。

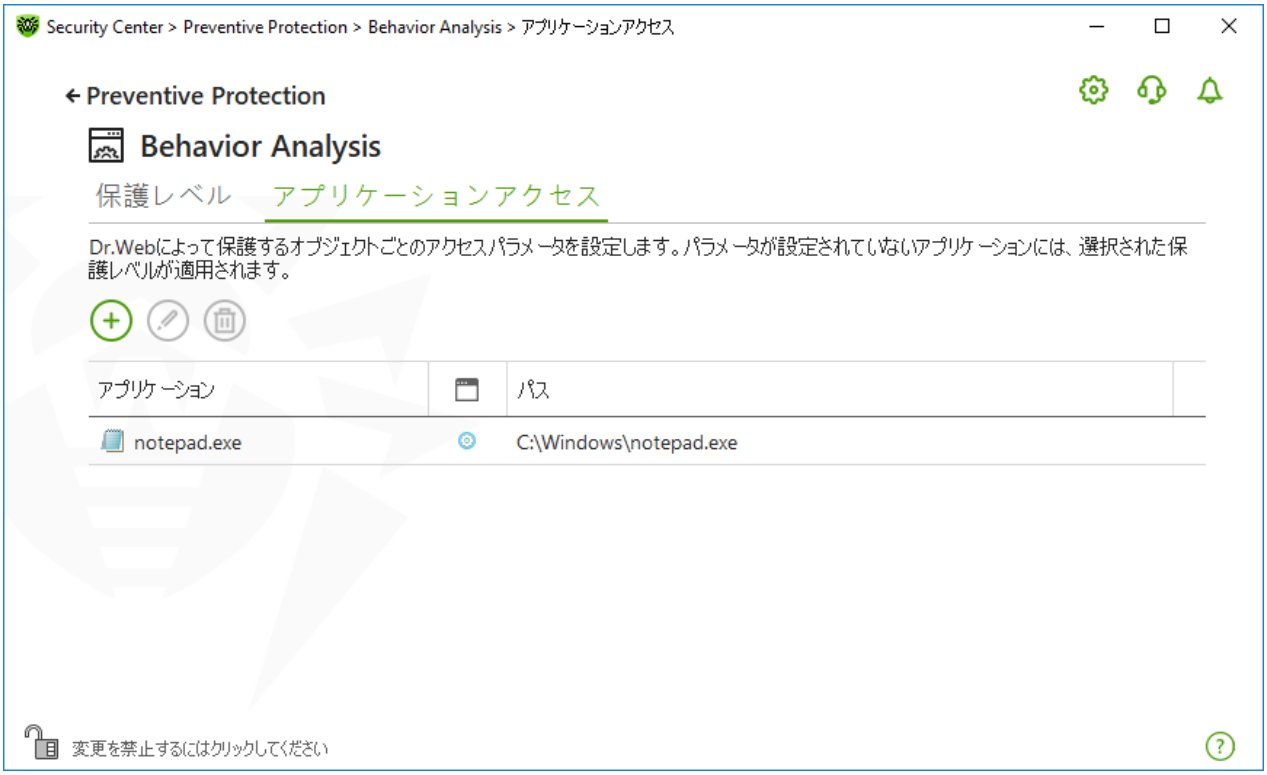

図72. アプリケーションアクセス設定

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。

- - すべての保護する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。
- - 保護するオブジェクトには異なるルールが設定されています。
- - すべての保護する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。

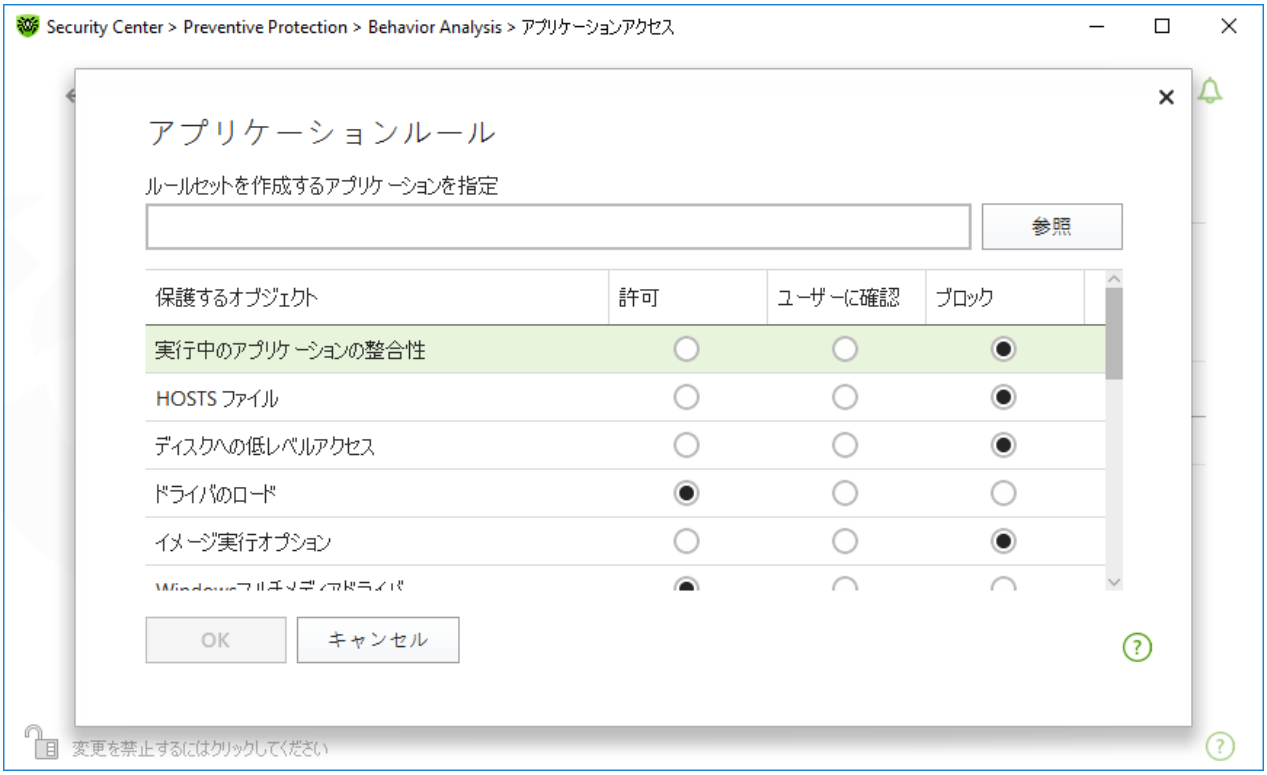

図73. アプリケーションのルールセットを追加する

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。
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す場合があります。
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	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（すべ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）。 イメージファイル実行オプション • Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options Windowsマルチメディアドライバ: • Software\Microsoft\Windows NT\CurrentVersion\Drivers32

保護するオブジェクト	説明
	• Software\Microsoft\Windows NT\CurrentVersion\Userinstallable.drivers Winlogonの値： • Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL Winlogonの通知： • Software\Microsoft¥Windows NT\CurrentVersion¥Winlogon¥Notify Windowsシェルのオートラン： • Software\Microsoft\Windows NT\CurrentVersion\Windows, AppInit_DLLs, LoadAppInit_DLLs, Load, Run, IconServiceLib 実行ファイルの関連付け： • Software\Classes\.exe, .pif, .com, .bat, .cmd, .scr, .lnk (keys) • Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile (keys) ソフトウェア制限ポリシー（SRP:Software Restriction Policies）： • Software\Policies\Microsoft\Windows\Safer Internet Explorerのプラグイン（BHO）： • Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects プログラムのオートラン： • 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 • Software\Microsoft\Windows\CurrentVersion\RunServicesOnce ポリシーオートラン： • Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run セーフモードの構成： • 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 • System\ControlSetXXX\Control\Session Manager\SubSystems, Windows システムサービス： • System\CurrentControlXXX\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てください。

11.3. 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。オブジェクトが悪意のあるものであるかどうかを判断するために、コンポーネントはDr.Webクラウドサービスからのデータも使用します。

Exploit Prevention 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、**Preventive Protection** タイルをクリックします。
3. スイッチ を使用して、Exploit Prevention コンポーネントを有効または無効にします。

図74. Exploit Prevention コンポーネントを有効／無効にする

Exploit Prevention 設定を開くには

1. Dr.Webが 管理モード 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 ）。管理モードではない場合は、ロックをクリックします 。
2. **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。

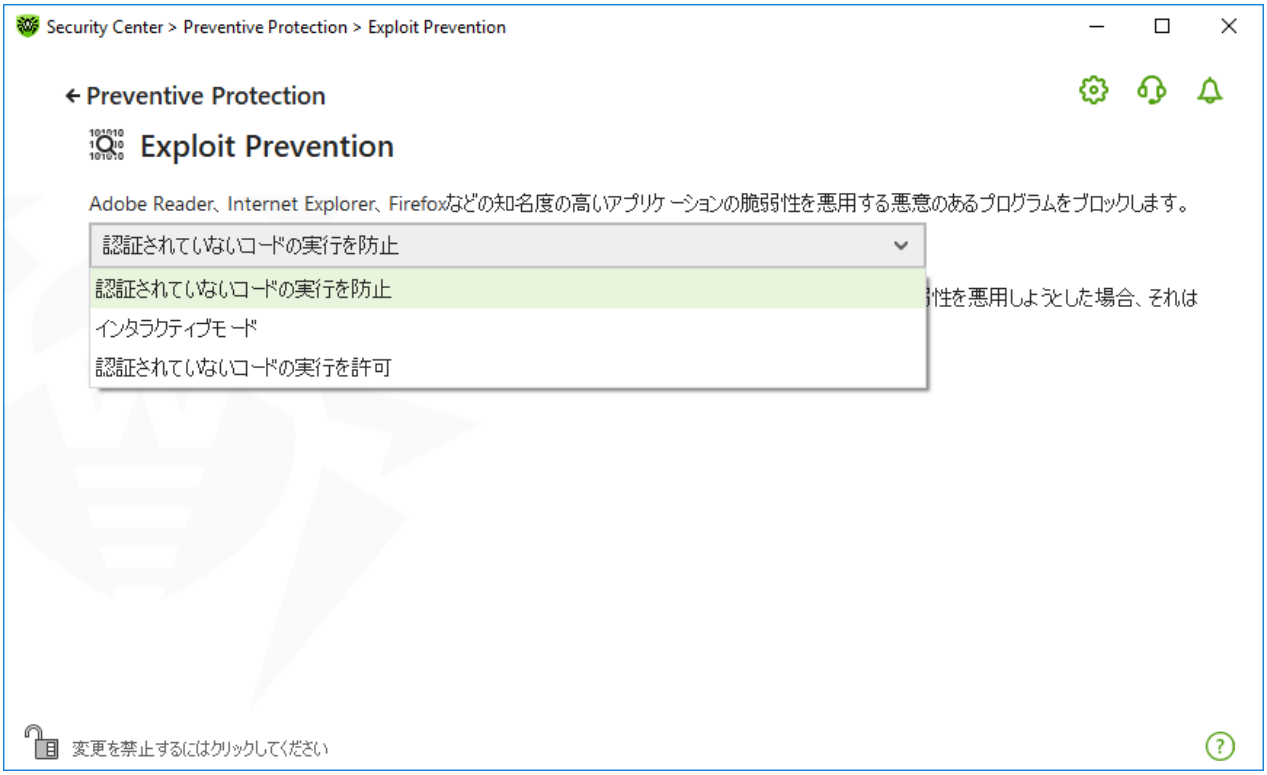

図75. 保護レベルを選択する

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、デスクトップとメールの通知を 設定 できます。

以下も参照してください。

- 通知

12. デバイスと個人データ

この設定グループでは、コンピューターに接続されたWebカメラやマイクへのアプリケーションアクセスを設定したり、重要なフォルダを保護したり、特定のバスやデバイスクラスへのアクセスをブロックしたりできます。

デバイスと個人データ 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、**デバイスと個人データ** タイルをクリックします。

図76。デバイスと個人データ ウィンドウ

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。

このウィンドウでは以下の設定を行うことができます：

- Webカメラ - Webカメラへのアプリケーションのアクセス制御
- マイク - マイクへのアプリケーションのアクセス制御
- データ損失防止 - 重要なファイルとフォルダに対する追加の保護
- デバイス - デバイスのブロックの管理

12.1. Webカメラへのアクセスを設定する

Dr.Webは、コンピューターに接続されたWebカメラへのアプリケーションアクセスを制御することによって、プライバシーを保護します。

Webカメラ 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、**デバイスと個人データ** 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. **Webカメラ** タイルをクリックします。設定ウィンドウが開きます。

図77. Webカメラ 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。

- Webカメラへのアプリケーションアクセスに対するDr.Webの動作
- 特定のアプリケーションのアクセス

Webカメラへのアプリケーションアクセスに対するDr.Webの動作

ドロップダウンウィンドウで、すべてのアプリケーションに適用する操作モードを選択します。

- **許可** - アプリケーションはWebカメラにアクセスできます。このオプションはデフォルトで選択されています。
- **ブロック** - アプリケーションはWebカメラにアクセスできません。

- **ユーザーに確認** - Webカメラにアクセスしようとするすべてのアプリケーションについて、そのアプリケーションに対するアクション（Webカメラへのアクセスを許可またはブロック）を選択するように求められます。

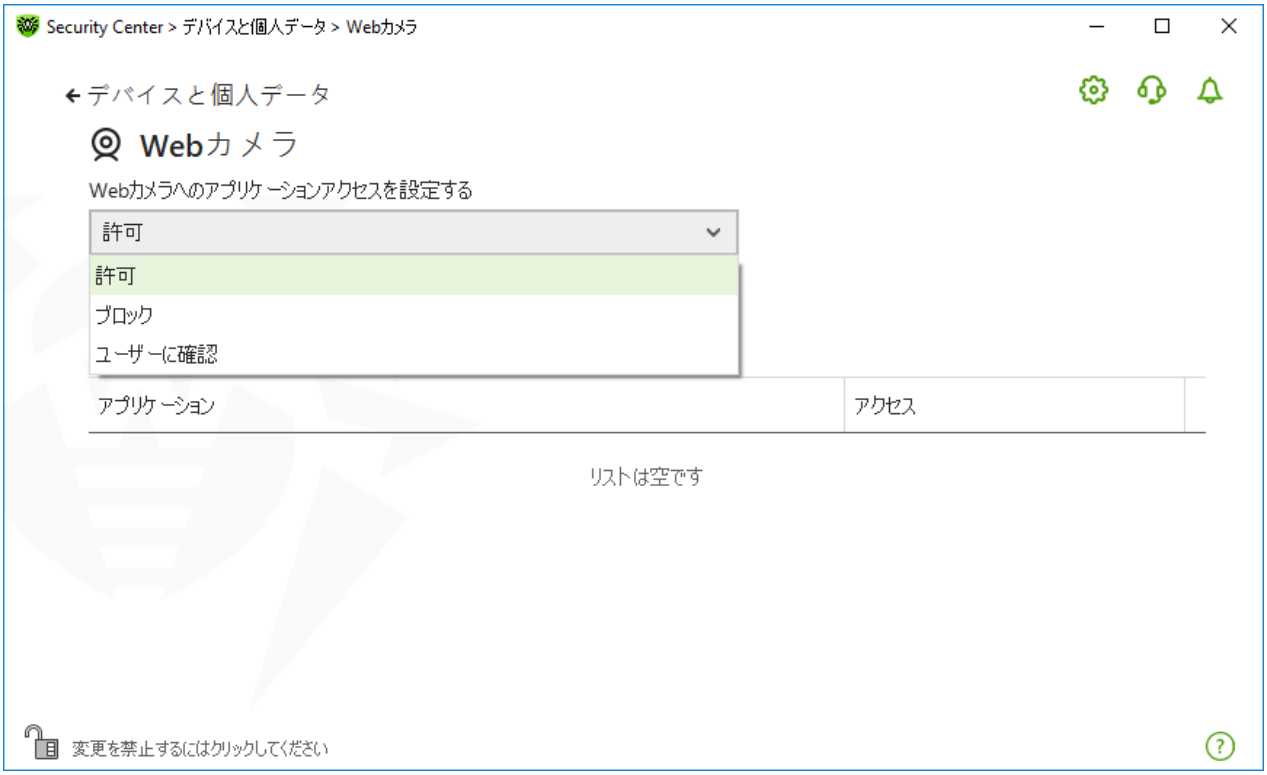

図 78. アプリケーションのアクセスモードを選択する

特定のアプリケーションのアクセス

特定のアプリケーションのアクセスルールを設定するには

1. ⊕ ボタンをクリックします。
2. 開いたウィンドウで、**参照** ボタンをクリックし、ルールを作成するアプリケーションを選択します。
3. ドロップダウンリストでWebカメラへのアクセスモードを選択します。

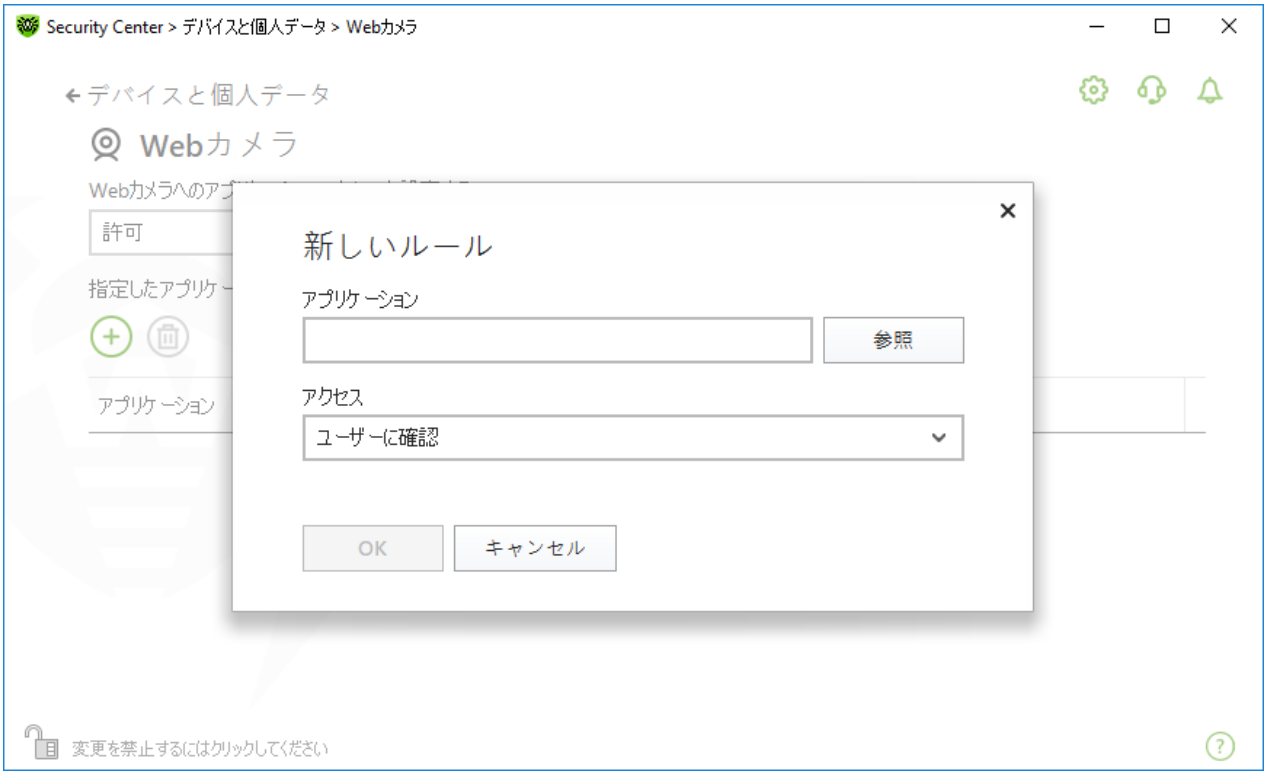

図79. アプリケーションのアクセスルールを作成する

4. **OK** をクリックします。

アプリケーションリスト

アプリケーションのアクセスルールを編集できます。

- 特定のアプリケーションのアプリケーションルールを編集するには、該当するアプリケーションのドロップダウンメニューで新しい値を選択します。
- ルールを削除するには、リストからアプリケーションを選択して をクリックします。**OK** をクリックして、削除を確定します。

通知を受信する

プロセスのWebカメラへのアクセスがブロックされると、通知が表示されます。必要に応じて、デスクトップおよびメールの通知を 設定 することができます。

12.2. マイクへのアクセスを設定する

Dr.Webは、コンピューターに接続されたマイクへのアプリケーションアクセスを制御することによって、プライバシーを保護します。

マイク 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、**デバイスと個人データ** 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. マイク タイルをクリックします。設定ウィンドウが開きます。

図80. マイク 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。

- マイクへのアプリケーションアクセスに対するDr.Webの動作
- 特定のアプリケーションのアクセス

マイクへのアプリケーションアクセスに対するDr.Webの動作

ドロップダウンウィンドウで、すべてのアプリケーションに適用する操作モードを選択します。

- **許可** - アプリケーションはマイクにアクセスできます。このオプションはデフォルトで選択されています。
- **ブロック** - アプリケーションはマイクにアクセスできません。
- **ユーザーに確認** - マイクにアクセスしようとするすべてのアプリケーションについて、そのアプリケーションに対するアクション（マイクへのアクセスを許可またはブロック）を選択するように求められます。

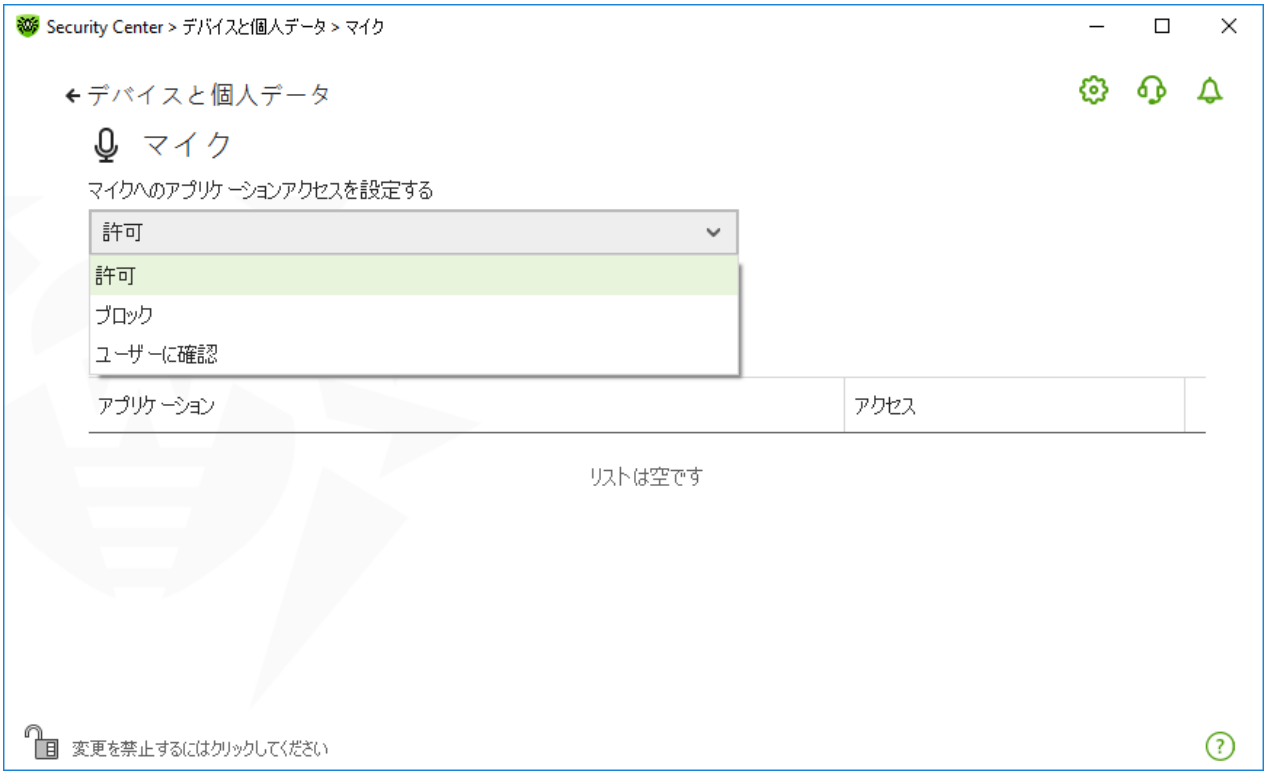

図 81. アプリケーションのアクセスモードを選択する

特定のアプリケーションのアクセス

特定のアプリケーションのアクセスルールを設定するには

1. ⊕ ボタンをクリックします。
2. 開いたウィンドウで、**参照** ボタンをクリックし、ルールを作成するアプリケーションを選択します。
3. ドロップダウンリストでマイクへのアクセスモードを選択します。

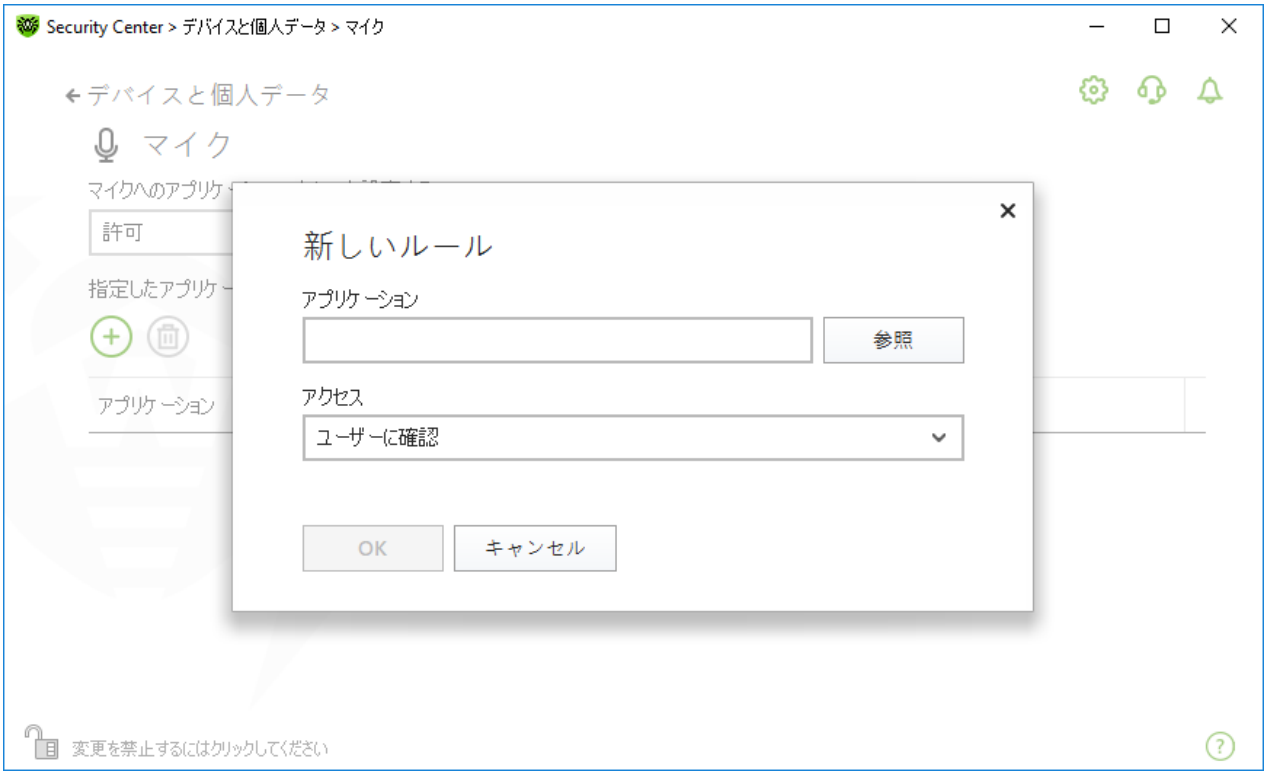

図82. アプリケーションのアクセスルールを作成する

アプリケーションリスト

アプリケーションのアクセスルールを編集できます。

- 特定のアプリケーションのアプリケーションルールを編集するには、該当するアプリケーションのドロップダウンメニューで新しい値を選択します。
- ルールを削除するには、リストからアプリケーションを選択して をクリックします。**OK** をクリックして、削除を確定します。

通知を受信する

プロセスのマイクへのアクセスがブロックされると、通知が表示されます。必要に応じて、デスクトップおよびメールの通知を 設定 することができます。

以下も参照してください。

- 通知

12.3. データ損失防止

データ損失防止 機能を使用することで、悪意のあるソフトウェアによって重要なフォルダの内容が変更されてしまうことを防ぎます。この機能を有効にすると、保護されたフォルダにファイルを追加したりファイルを表示したりすることはできますが、そのフォルダにあるファイルの修正や削除はブロックされます。アプリケーションのフォルダへのアクセスを許可するには、該当するアプリケーションを除外リストに追加します。以前に保存したコピーを復元することもできます。

データ損失防止 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、**デバイスと個人データ** タイルをクリックします。
3. Dr.Webが 管理モード 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）。管理モードではない場合は、ロックをクリックします。
4. **データ損失防止** タイルをクリックします。

図83. データ損失防止 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。

- 以前保存したファイルコピーを使用したDr.Web動作
- 保護されたフォルダを管理する
- 除外
- 保存したコピーの復元と削除

以前に保存したファイルのコピーを使用したDr.Web動作

バージョン12.0以降では、ファイルのコピーを保存するオプションはありません。代わりに、フォルダを保護するための新機能が追加されています。

動作原理が変更されたため、フォルダの保護を再度設定する必要があります。以前のバージョンのプログラムで保護されていたフォルダは、フォルダのコピーが保存されているかどうかに関係なく、保護するフォルダのリストに追加されます。バージョン12.0に更新した後の最初のプログラム起動時に、ファイルバックアップ機能を保護するフォルダ機能に切り替えることについての通知が表示されます。

図84. コンポーネントの動作原理の変更に関する通知

この通知では、保護が有効になっている検出されたすべてのフォルダとファイルのリストも表示されます。保護するフォルダのリストに追加できない場合は、リスト上でそのフォルダに が表示されます。システムフォルダ、Parental Control によってアクセスがブロックされているフォルダ、個別のファイルは保護することができません。

デフォルトでは、以前のバージョンから移されたフォルダの保護は無効になっています。それらを保護するには、**データ損失防止** ウィンドウに移動し、**保護を有効にする** 列で必要なフォルダにチェックを入れます。

以前のバージョンで保存したファイルのコピーを 復元 することもできます。

通知

プログラムをバージョン12.0にアップグレードした後、データ損失防止の動作原理の変更について通知が表示されます。

- コンピューターの再起動後、画面の中央にコンポーネントの動作原理の変更に関する通知が表示されます（図 84 参照）。
- 通知フィード内の、フォルダ保護方法の変更に関する通知で、フォルダ保護の新しい設定にアクセスするには、**保護を設定する** ボタンをクリックします。その後、通知は削除されます。

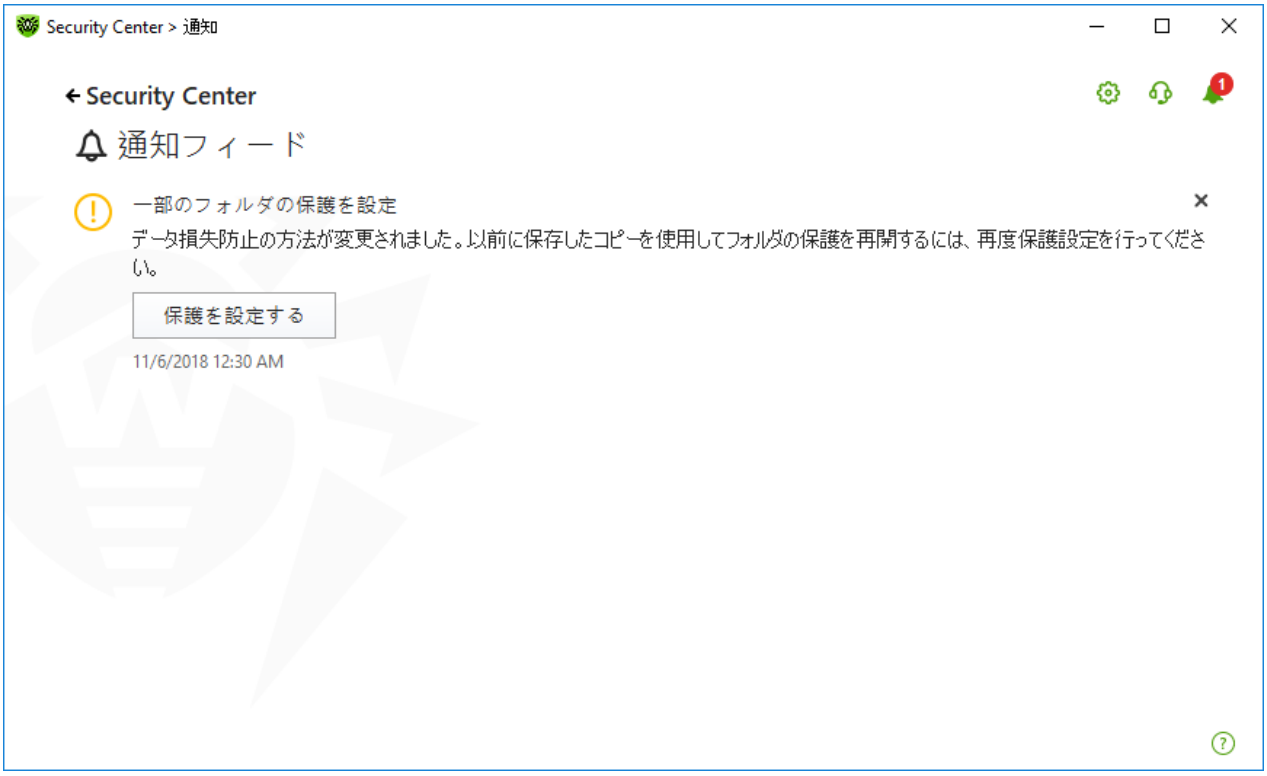

図85. フィード内の通知

- プログラムのアップデート後に **データ損失防止** ウィンドウを初めて開いた際には、保護することのできないフォルダとファイルのリストを含んだ通知が表示されます。

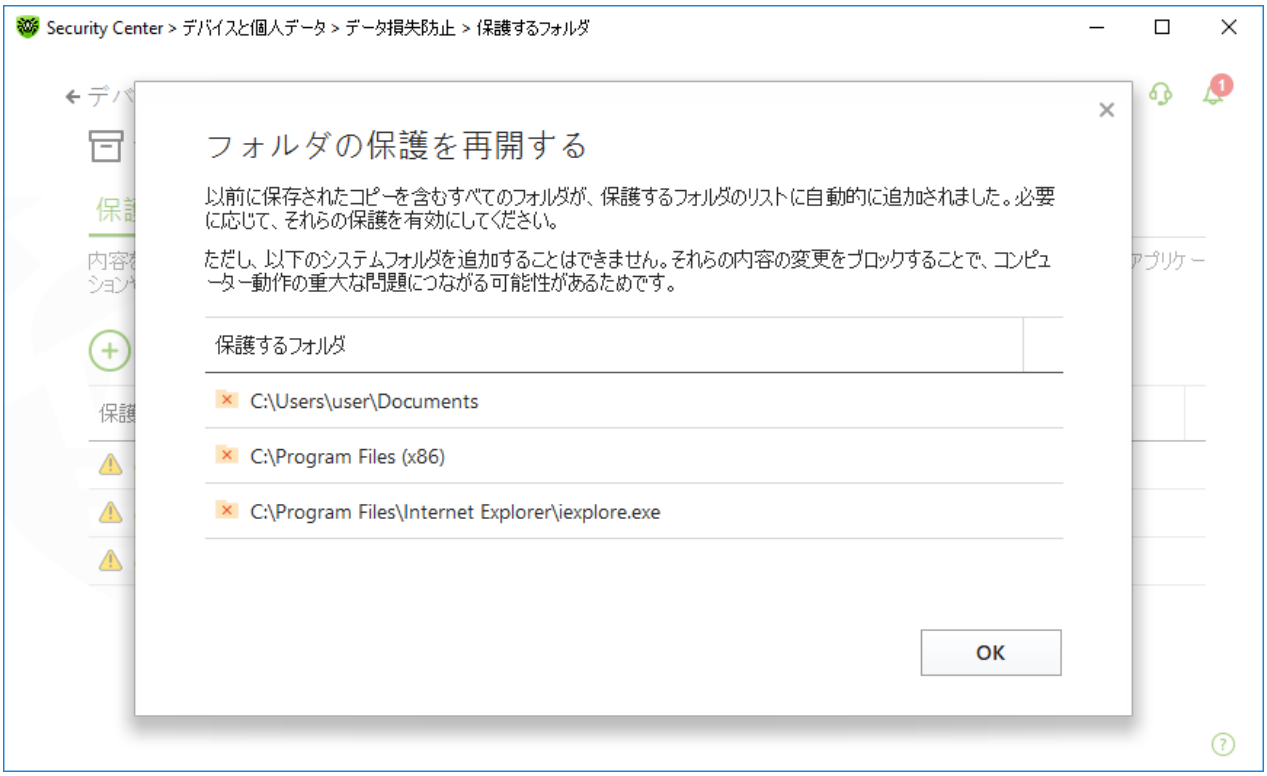

図 86. データ損失防止 ウィンドウを初めて開いたときに表示される通知

保護されたフォルダ

フォルダごとに、アプリケーションアクセスパラメータを設定できます。保護されたフォルダを表示したりコピーしたりすることができます。また、フォルダに新しい要素を作成することもできます。新しい要素を作成するプロセスが完了するまでの間は、そのプロセスによって要素を変更することができます。アプリケーションがフォルダにアクセスしようとした場合は、アクセスブロックに関する通知が表示されます。

保護されたフォルダ内のファイルで脅威が検出された場合、Dr.Webのみがそれらを削除したり変更したりできます。

保護されたフォルダのリストにフォルダを追加すると、そのフォルダにはデフォルトのルールが適用されます。すなわち、信頼するアプリケーションのリストに含まれるアプリケーション以外のすべてのアプリケーションに対して、フォルダの内容の変更や削除が制限されます。このリストを表示するには、Webサイト https://products.drweb.com/services/data_protection/ にアクセスしてください。このリストには、MicrosoftやAdobeのアプリケーションなど、最も一般的なアプリケーションが含まれています。`explorer.exe` などのシステムプロセスは、悪意のあるオブジェクトがシステムを攻撃するために使用される場合があるため、信頼できるアプリケーションのリストには含まれません。

保護されたフォルダのリストへのシステムフォルダの追加は制限されています。重大なシステム動作エラーにつながる可能性があります。

データ損失防止は、保護が設定されているオペレーティングシステム内のローカルファイルとフォルダ（物理的にデバイス上にある）に対してのみ適用されます。同じコンピューターに複数のオペレーティングシステムが入っている場合は、システムごとに個別にデータ損失防止を設定する必要があります。ネットワークファイルとフォルダを保護することはできません。

図87. 保護されたフォルダ

この表には、以下に関する情報が記載されています。

- 保護するオブジェクト
- 一般規則からの除外
- 保護ステータス

保護を有効にするには、必要なオブジェクトの **保護を有効にする** チェックボックスをオンにします。このチェックボックスをオフにするとフォルダは保護されなくなり、⚠ アイコン付きで表示されます。

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 - 保護するオブジェクトのリストにオブジェクトを追加します。
- ✎ ボタン - 表の要素を編集します。
- 🗑 ボタン - 保護するオブジェクトのリストからオブジェクトを削除します。

保護するフォルダのリストにフォルダを追加するには

1. ⊕ ボタンをクリックします。開いたウィンドウで、**参照** ボタンをクリックして必要なオブジェクトを選択します。
2. 必要に応じて、信頼するアプリケーションのフォルダへのアクセスを有効または無効にします。このオプションはデフォルトで有効になっています。
3. 一般設定に関係なく、オブジェクトへのフルアクセス権を持つ<u>アプリケーションを指定</u> することもできます。

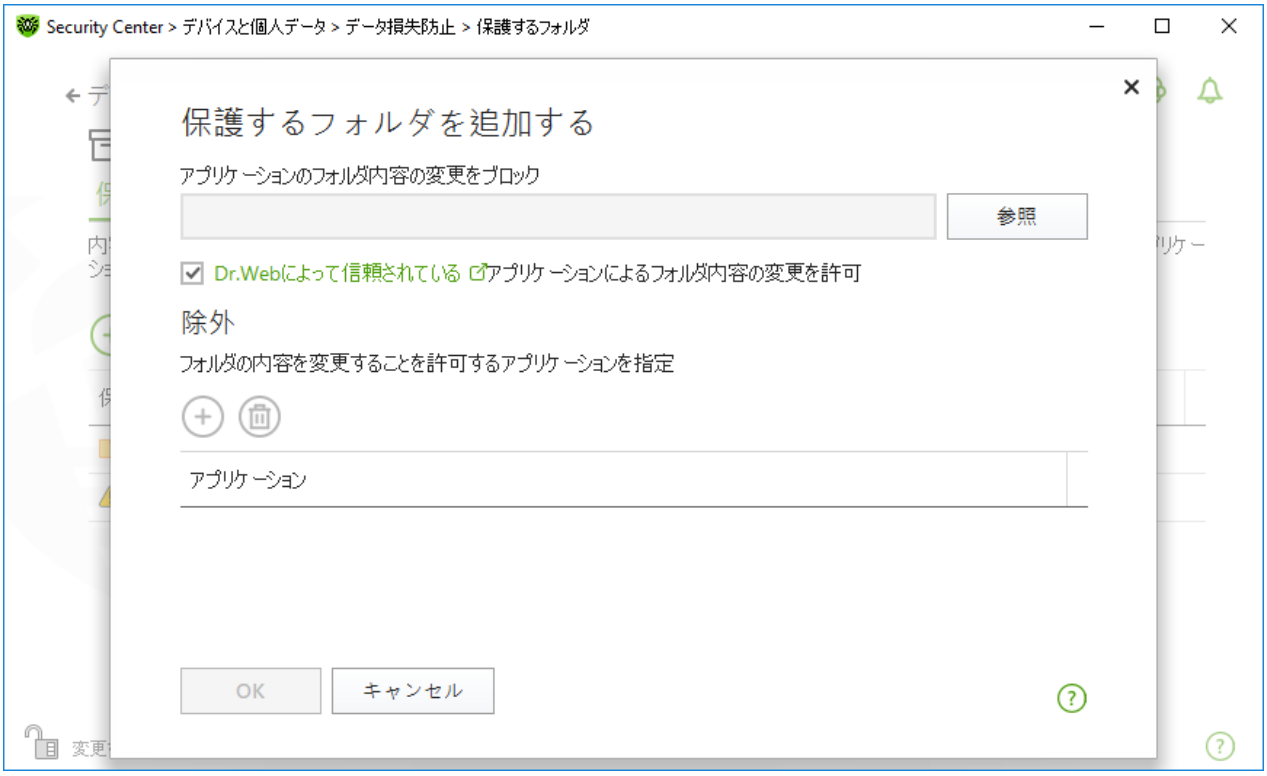

図88. 保護するフォルダを追加する

除外

保護されたフォルダへのフルアクセス権を持つアプリケーションの数は、データ損失防止のメインウィンドウの **ユーザーによる除外** 列に表示されます。

アプリケーションを除外リストに追加するには

1. データ損失防止 ウィンドウで ⊕ をクリックして保護されたフォルダのリストに新しいフォルダを追加します。
2. 開いたウィンドウ内で ⊕ をクリックします。保護されたフォルダ内のオブジェクトへのフルアクセス権を持つアプリケーションを選択します。
3. **OK** をクリックします。

保護するフォルダの除外リストを編集するには

1. リストからフォルダを選択し、✎ をクリックします。
2. 表の開いているウィンドウの一番下には、選択したフォルダへのフルアクセス権を持つすべてのアプリケーションが表示されます。
   - 新しいアプリケーションを追加するには、⊕ をクリックします。
   - アプリケーションを除外リストから削除するには、🗑 をクリックします。
3. **OK** をクリックします。

保存されたコピー

このタブは、以前のバージョンのプログラムで保存されたファイルのコピーがある場合にのみ使用できます。この機能を使用すると、保存したコピーを復元、削除できます。ただし、新たにコピーを保存することはできません。

図89. 保存されたコピーのリスト

作成されたコピーの削除

また、既存のコピーを削除してディスク領域を解放することもできます（コピーを削除しても元のファイルには影響しません）。これを行うには、必要なコピーを選択して ボタンをクリックします。

ファイルの復元

脅威によってファイルが破損してしまった場合に、作成されたそれらのコピーのうち特定の日付のものから復元できます。これを行うには、以下を実行します。

1. 必要なコピー（コピーが作成された日付が左側の列に表示されます）を選択し、 ボタンをクリックします。
2. 開いたウィンドウで、ファイルを復元するフォルダのパスを指定します。

12.4. デバイスのブロック

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. 開いたウィンドウで、**デバイスと個人データ** タイルをクリックします。
3. Dr.Webが 管理モード 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）。管理モードではない場合は、ロックをクリックします。
4. **デバイス** タイルをクリックします。

図 90.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。

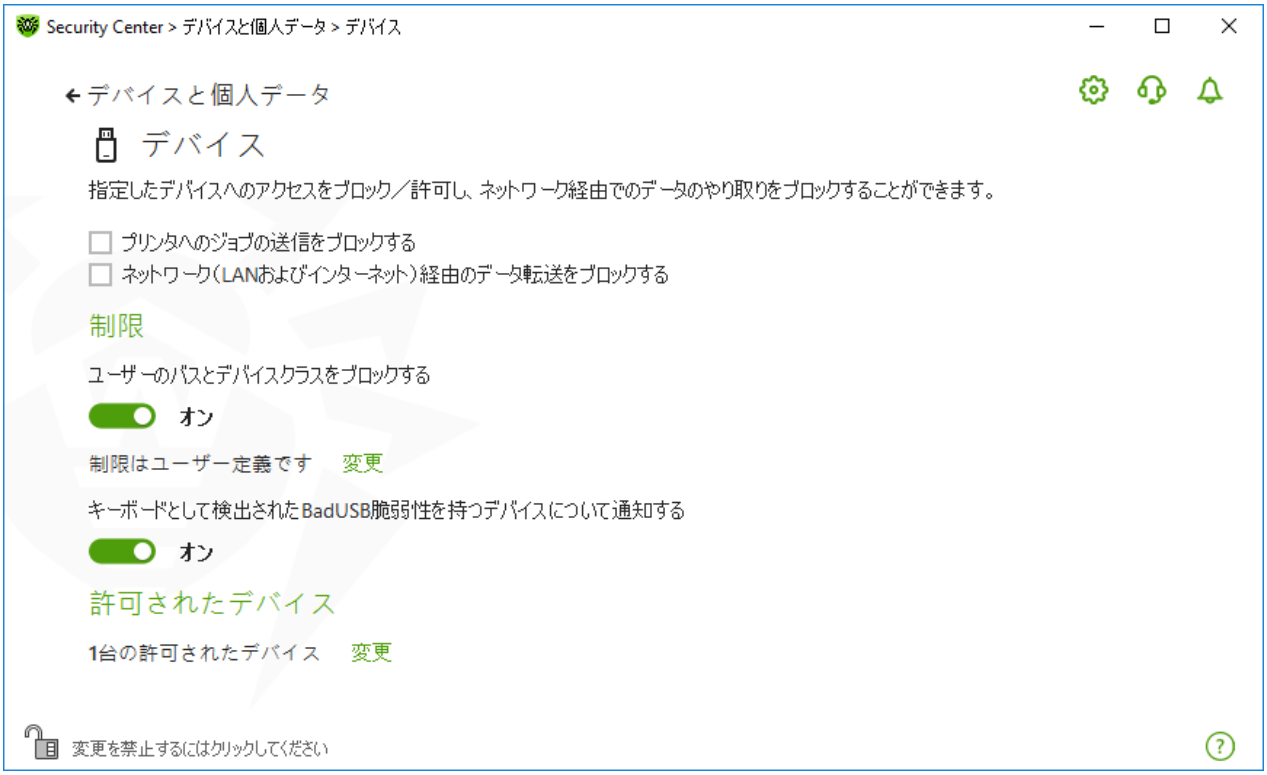

図 91.デバイスのブロック設定

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。

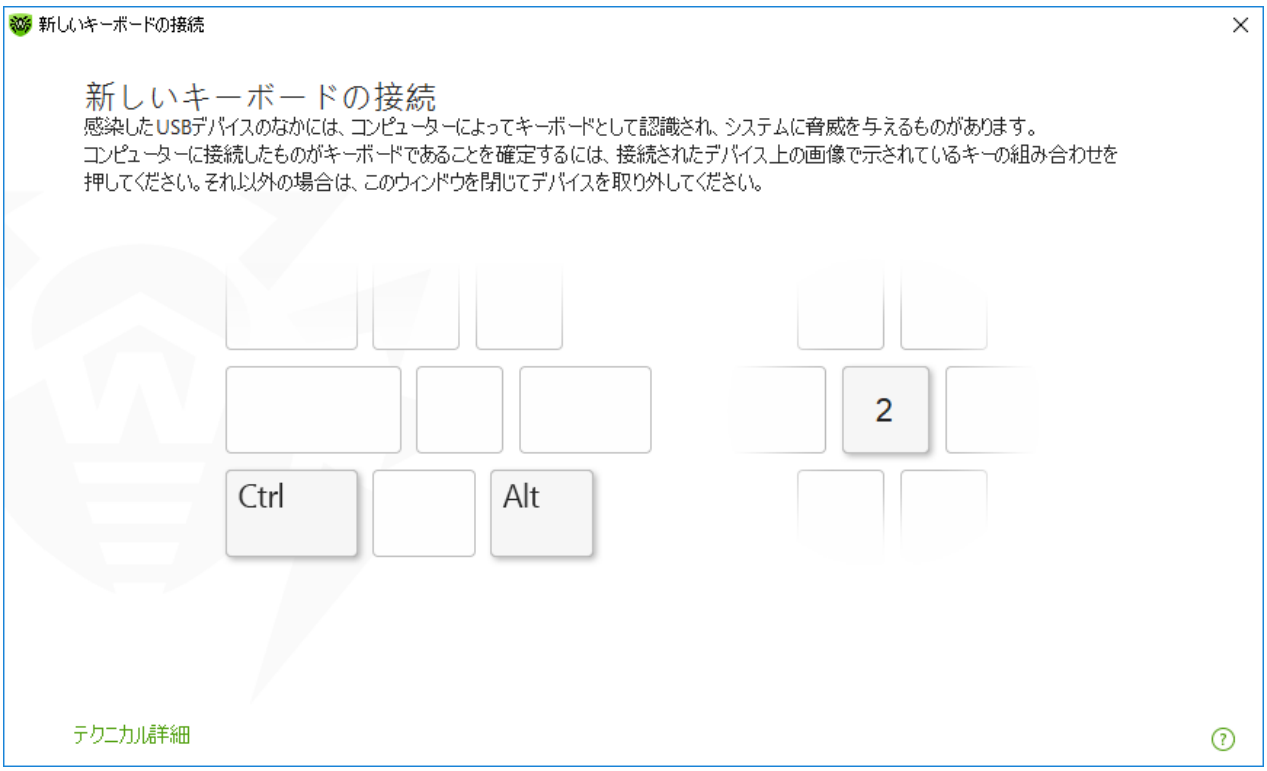

図 92.キーボードのブロック解除ウィンドウ

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。

許可するデバイスリストにデバイスを追加するには、**許可されたデバイス** オプションで **変更** をクリックします（このボタンは、制限が設定されている場合に使用できます）。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 。

12.4.1. 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、**デバイスと個人データ** タイルをクリックします。

3. 開いたウィンドウで、**デバイス** タイルをクリックします。
4. **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。
5. **変更** をクリックします。
6. 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す。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93. ブロックされたバスとクラス

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。

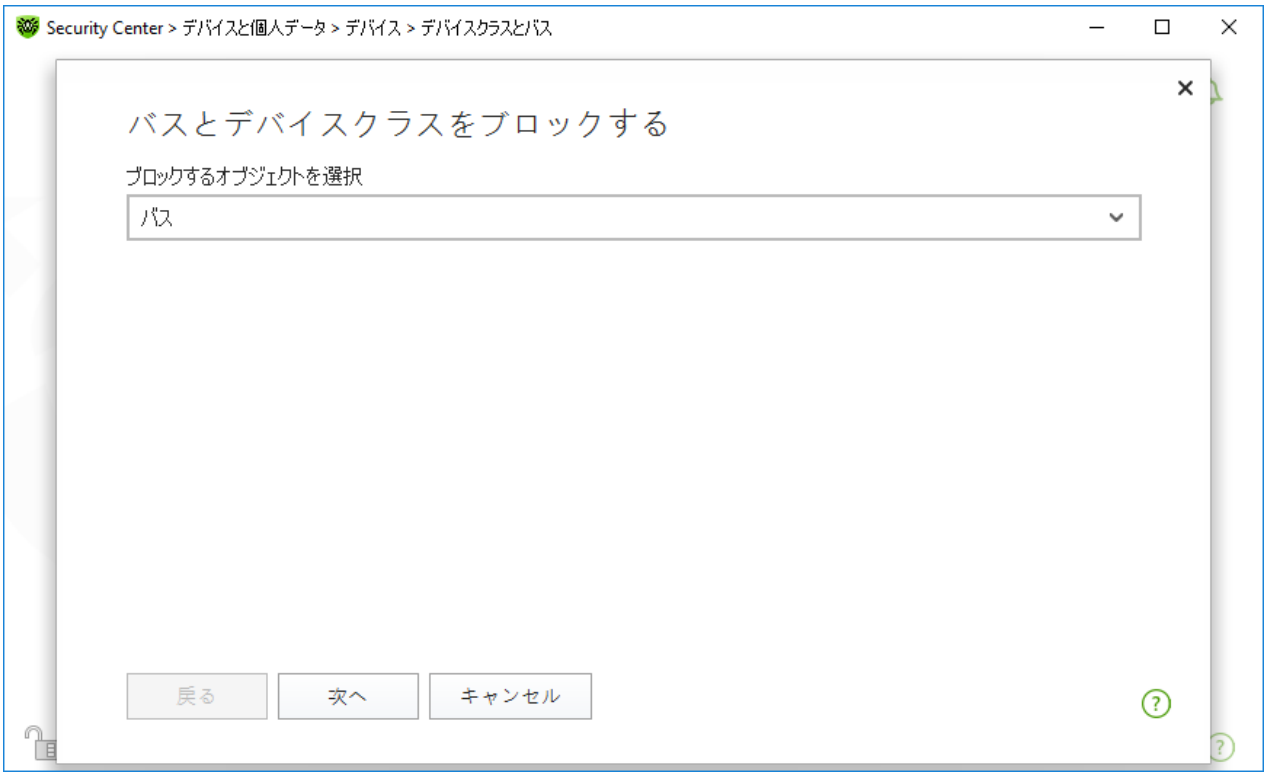

図94. ブロックするオブジェクトを選択する

3. バスのタイプを選択します。**次へ** をクリックします。

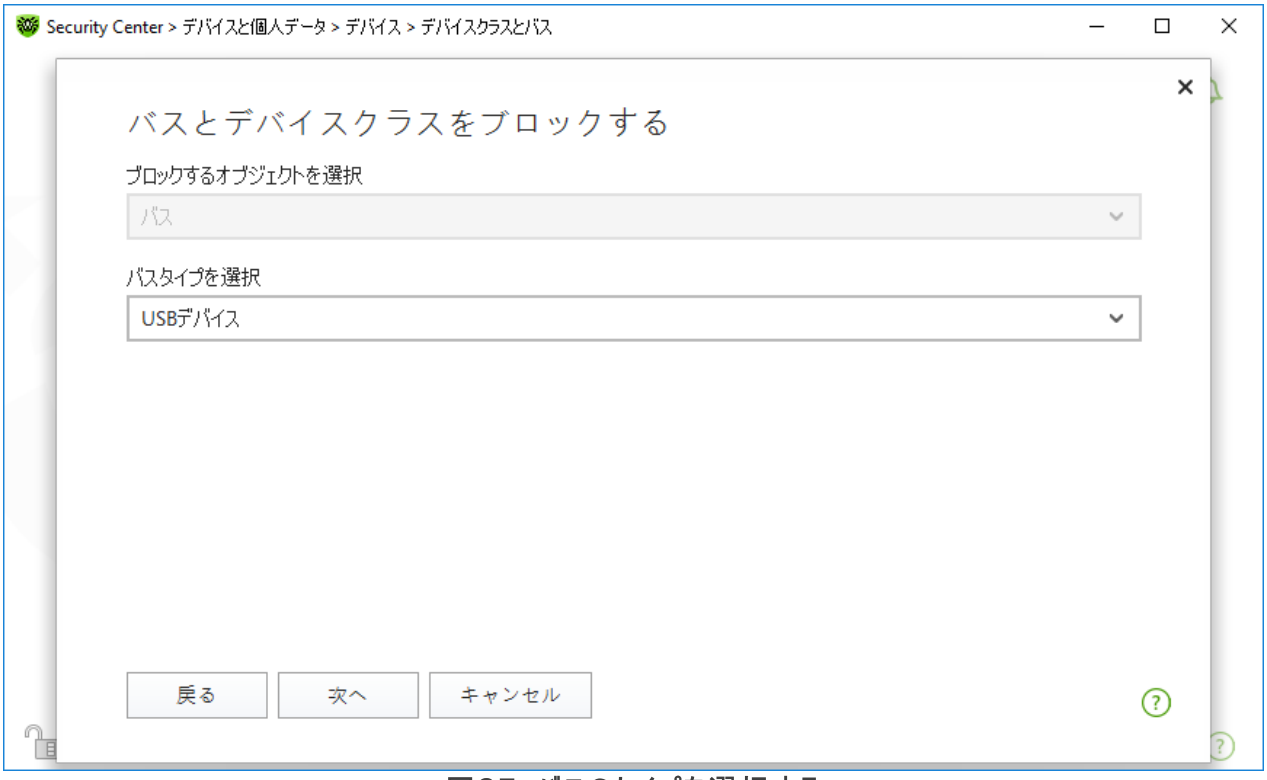

図95. バスのタイプを選択する

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。

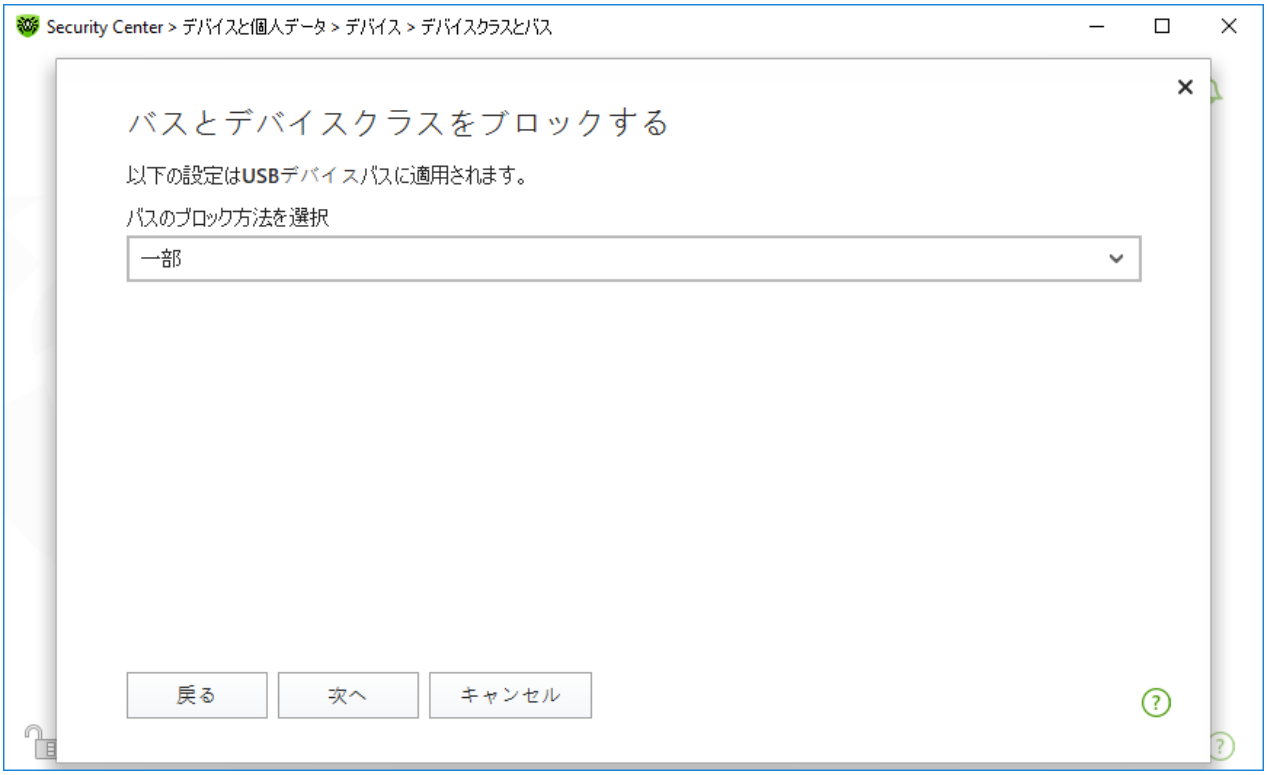

図96. バスのブロック方法を選択する

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。

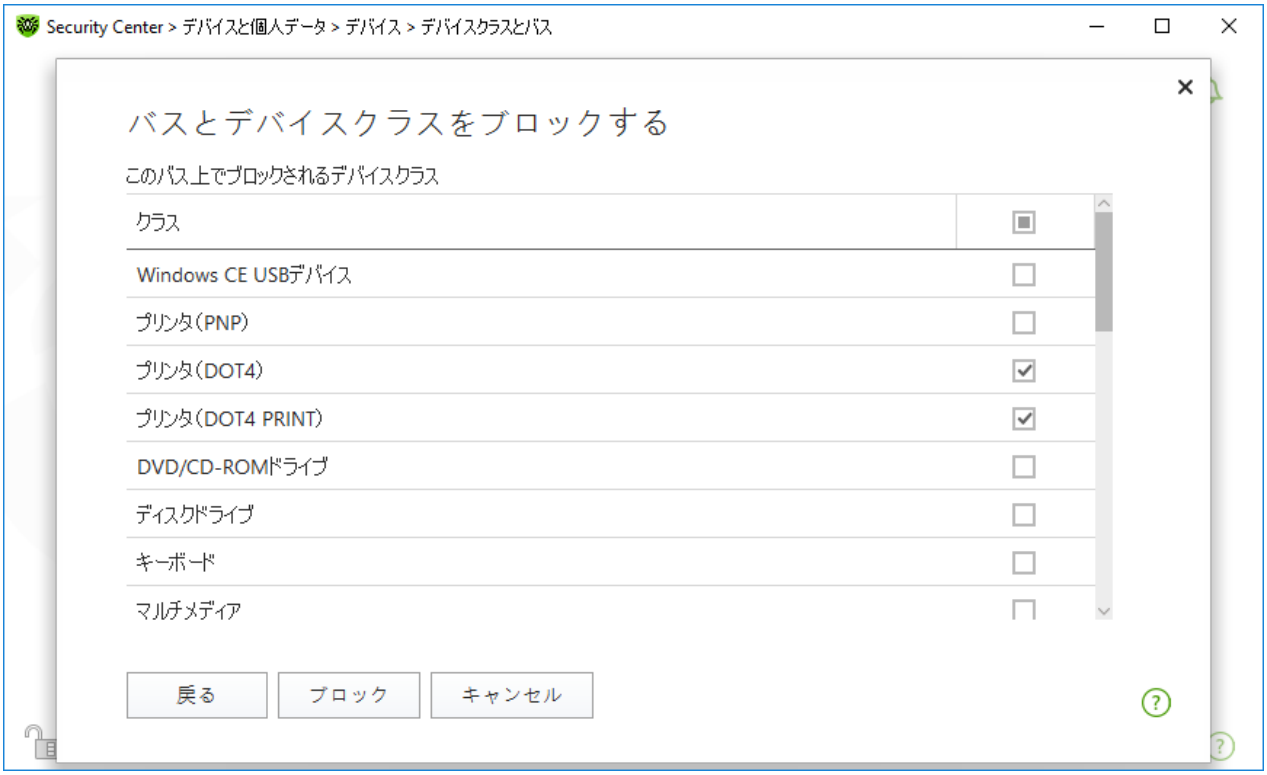

図97. バスのデバイスクラスを選択する

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。

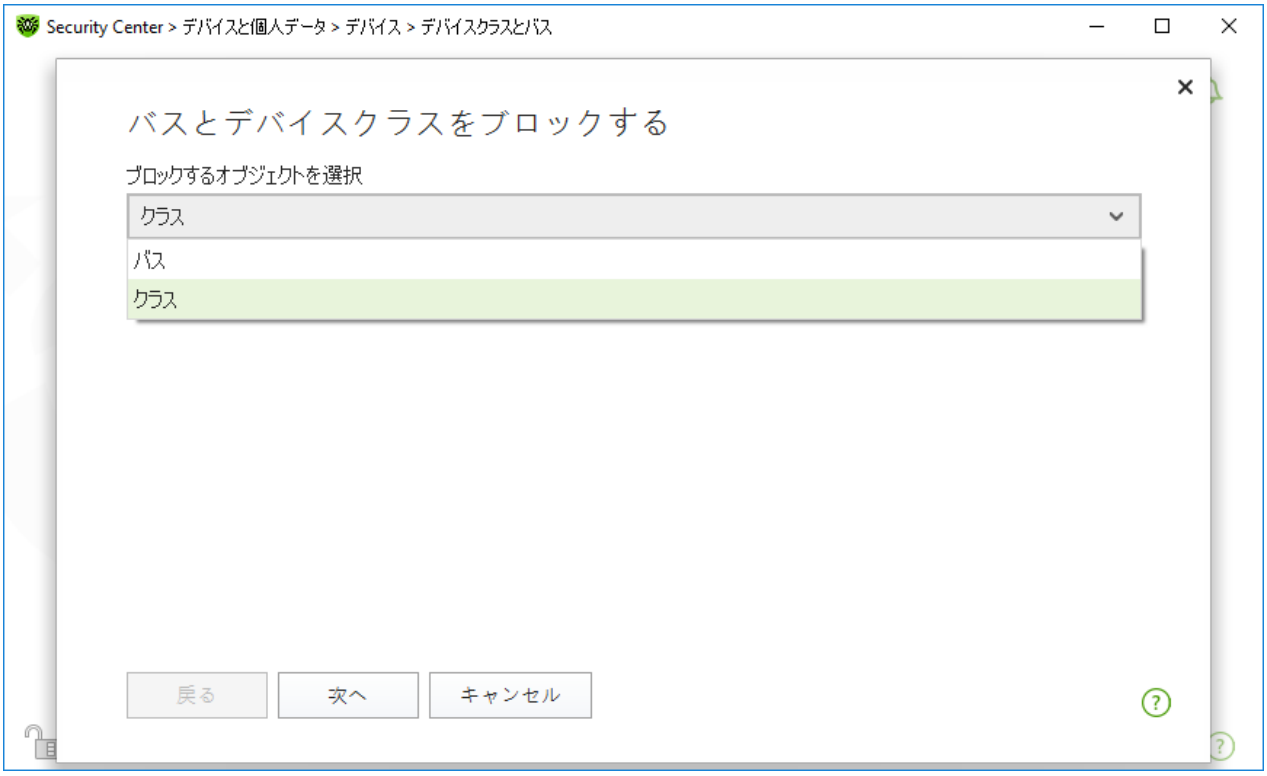

図98. ブロックするオブジェクトを選択する

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。

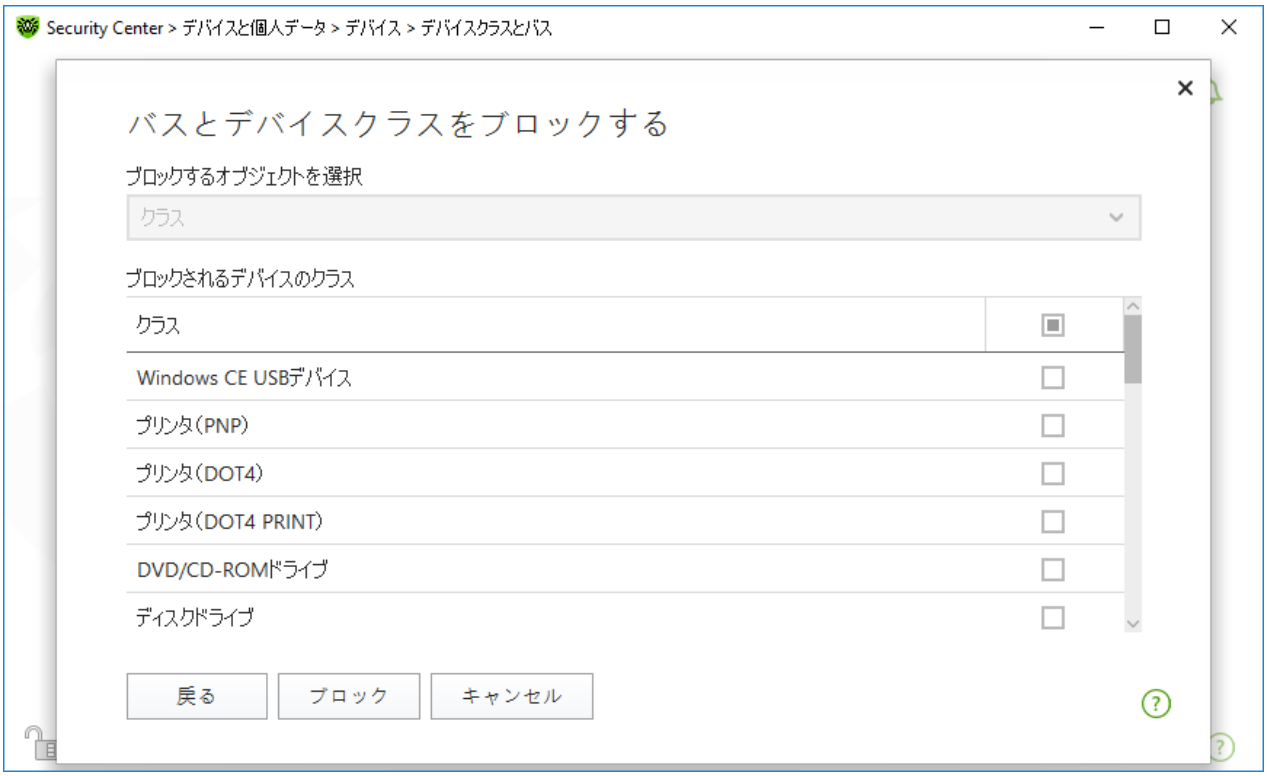

図99. デバイスクラスを選択する

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や、メールによる通知の受信を設定できます。

12.4.2. 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、**デバイスと個人データ** タイルをクリックします。
3. 開いたウィンドウで、**デバイス** タイルをクリックします。
4. **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。

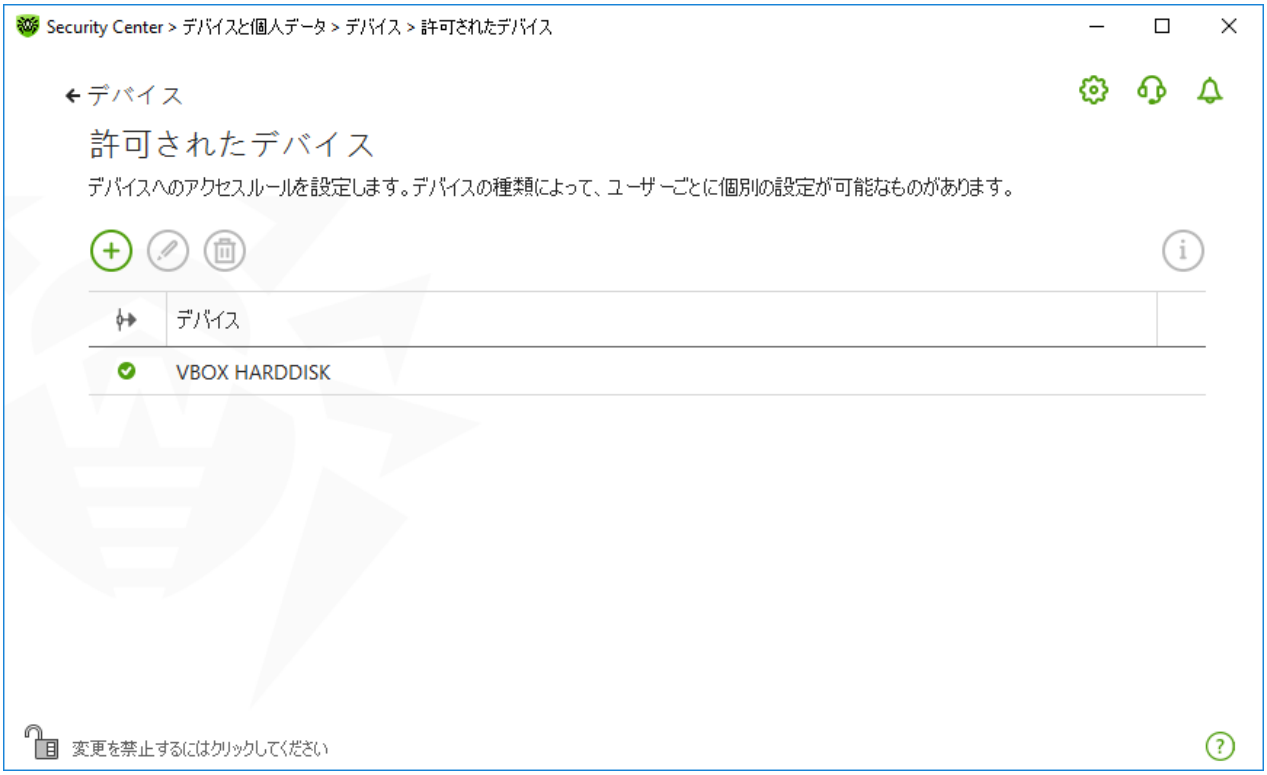

図 100. 許可するデバイス

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。

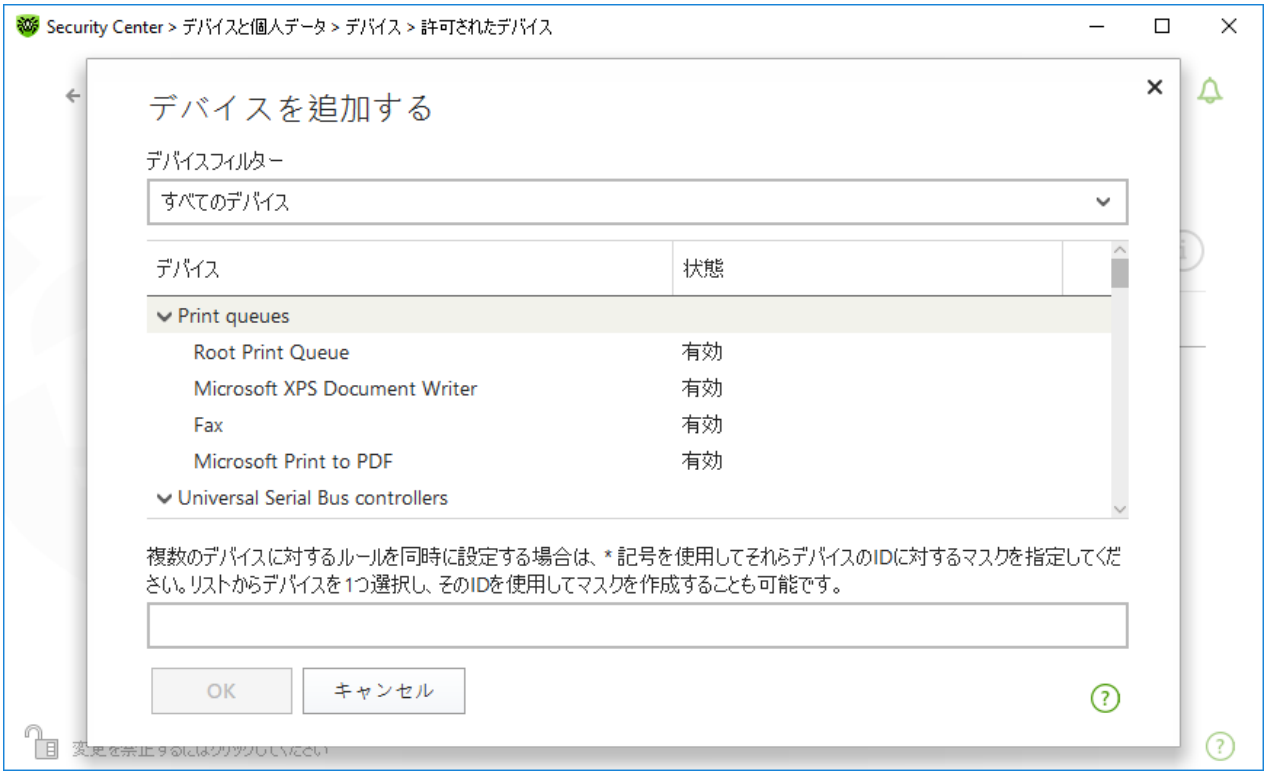

図 101. デバイスを許可するデバイスリストに追加する

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。

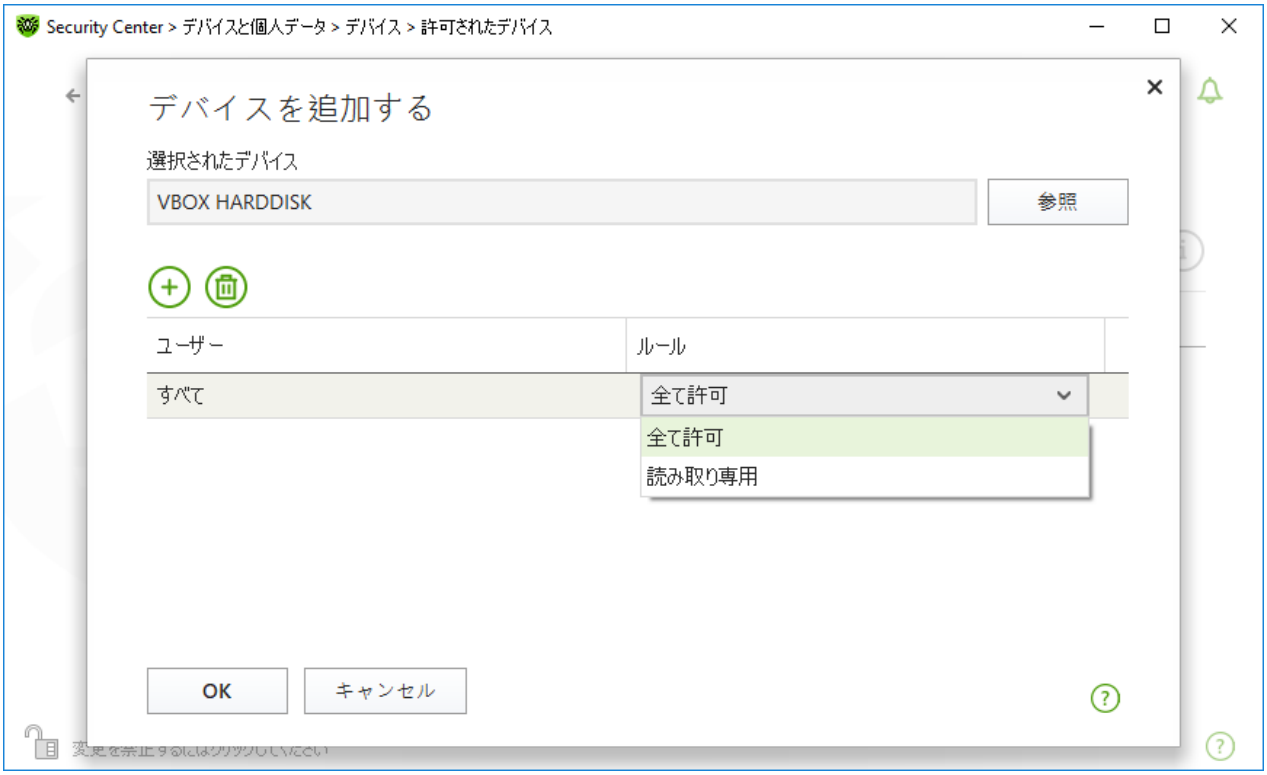

図102. 特定のユーザー用のルールを選択する

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。

13. Parental Control

Parental Control コンポーネントによって、Webサイト、ファイル、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、Parental Controlは各アカウントで有効になっており、**制限なし** モードで動作します。

Parental Control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、**Parental Control** セクションを選択します。**Parental Control** ウィンドウが開きます。

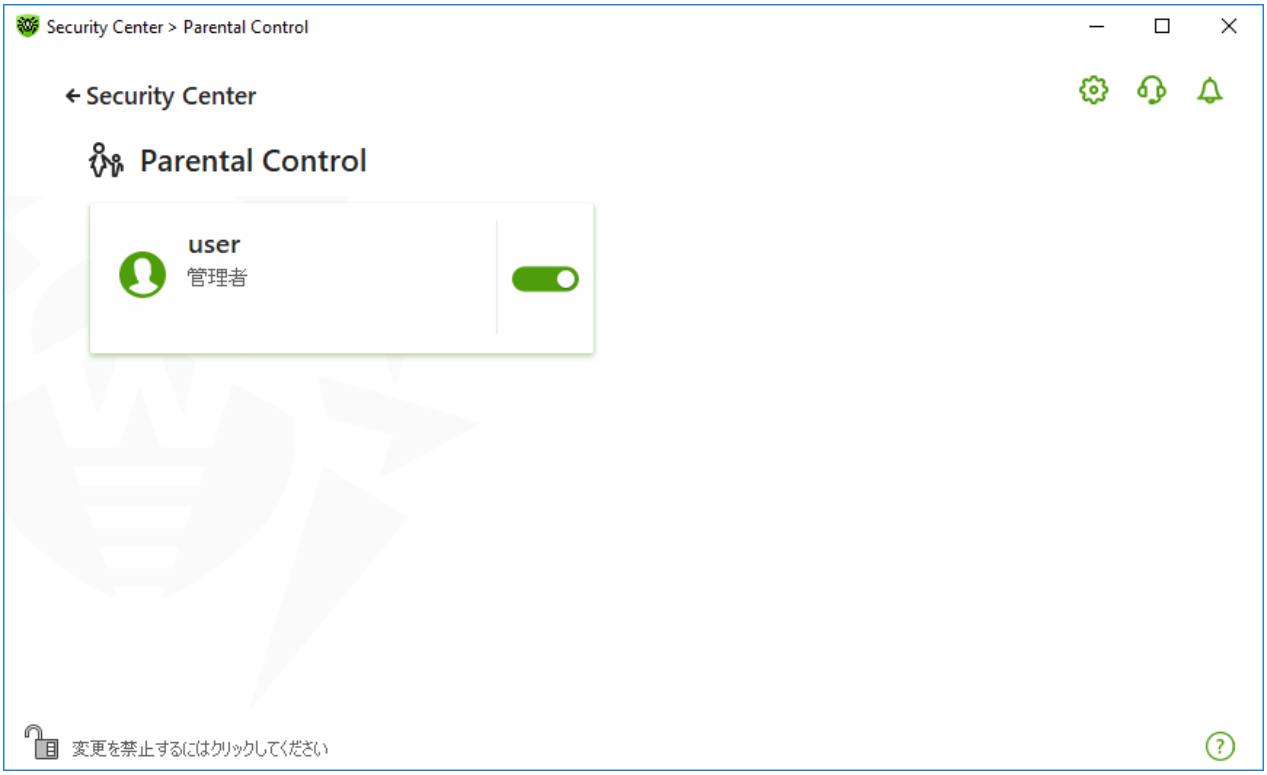

図 103. Parental Control

3. Dr.Webが 管理モード 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、必要なユーザーに対してParental 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Parental 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 Parental 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。

Parental Control設定を開くには

1. Dr.Webが 管理モード 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）。管理モードではない場合は、ロックをクリックします。
2. Parental Control ウィンドウ（図 Parental Control を参照）で、Parental Control を設定するユーザー名のタイルをクリックします。選択したユーザーの Parental Control 設定のウィンドウが開きます。

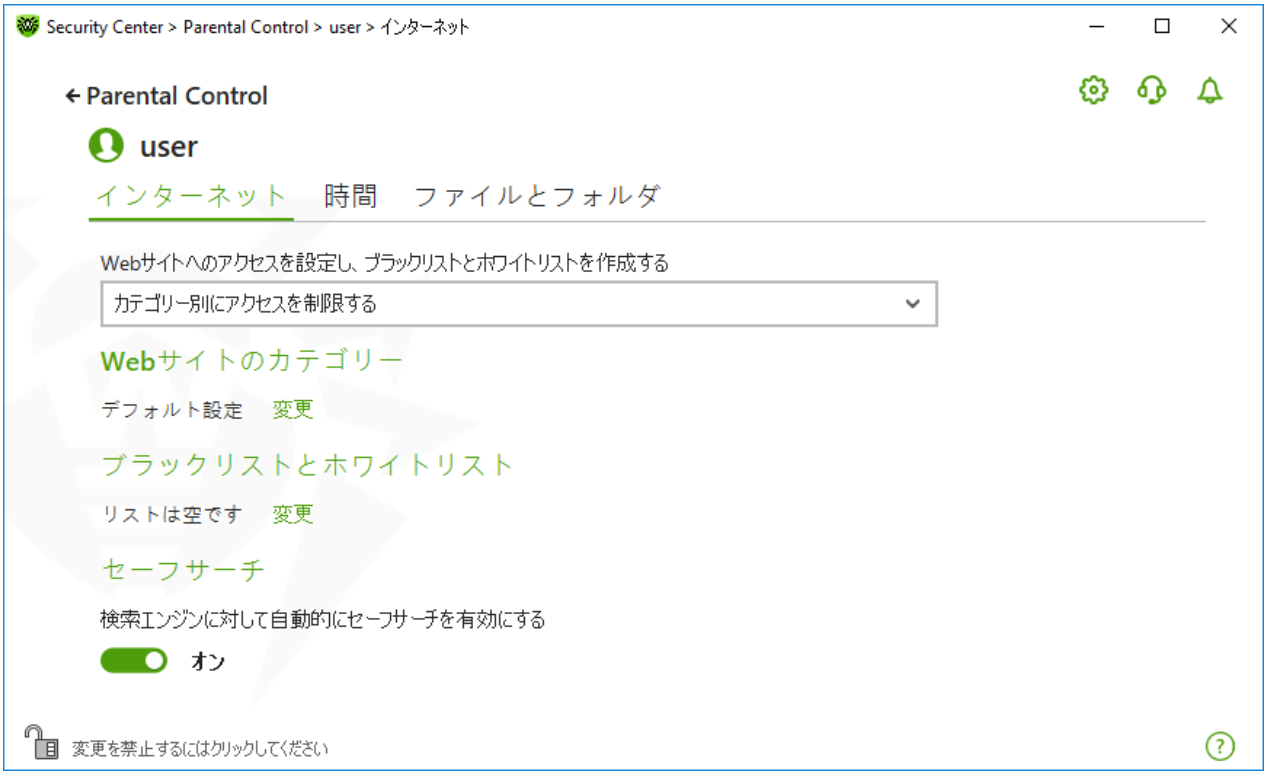

図 104. Parental Controlを設定する

3. Parental 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、Parental Control の動作に関する、デスクトップおよびメールの通知を 設定 することができます。

13.1. 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サイトのみに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**

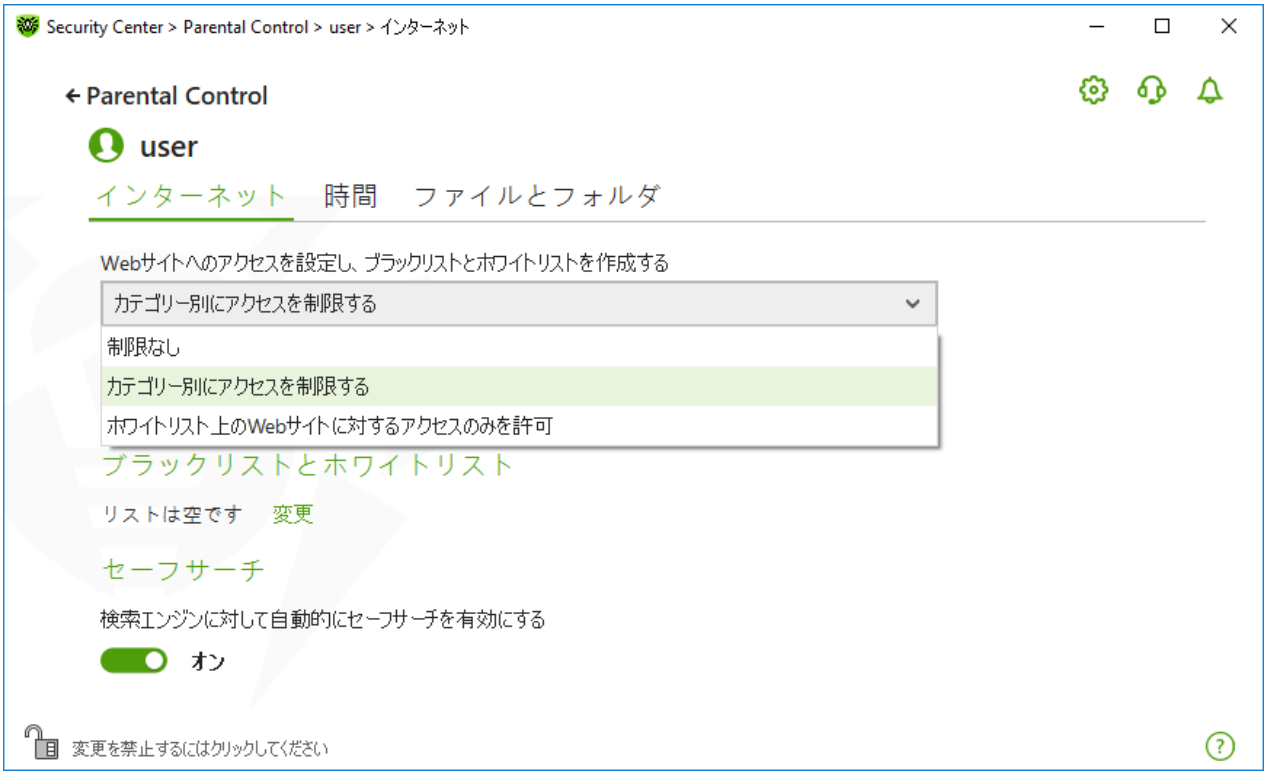

図 105. Parental Controlのモードを選択する

カテゴリー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サイトのカテゴリーを指定できます。同じWebサイトを複数のカテゴリーに割り当てることができます。この場合、Parental Controlは、制限リストに含まれているカテゴリーのうち少なくとも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。Webサイトの分類には、Dr.Webクラウドサービスからのデータも使用されます。

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。

カテゴリーへのアクセスを制限する前に、ブラウザのキャッシュをクリアしてください。

プログラム設定の ネットワーク セクションで 暗号化されたトラフィックをスキャンする オプションが無効になっている場合、暗号化を使用するWebサイトのトラフィック（例：HTTPSプロトコル）は分析されません。

特定のカテゴリーの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サイトのカテゴリー** 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ーの設定ウィンドウが開きます。

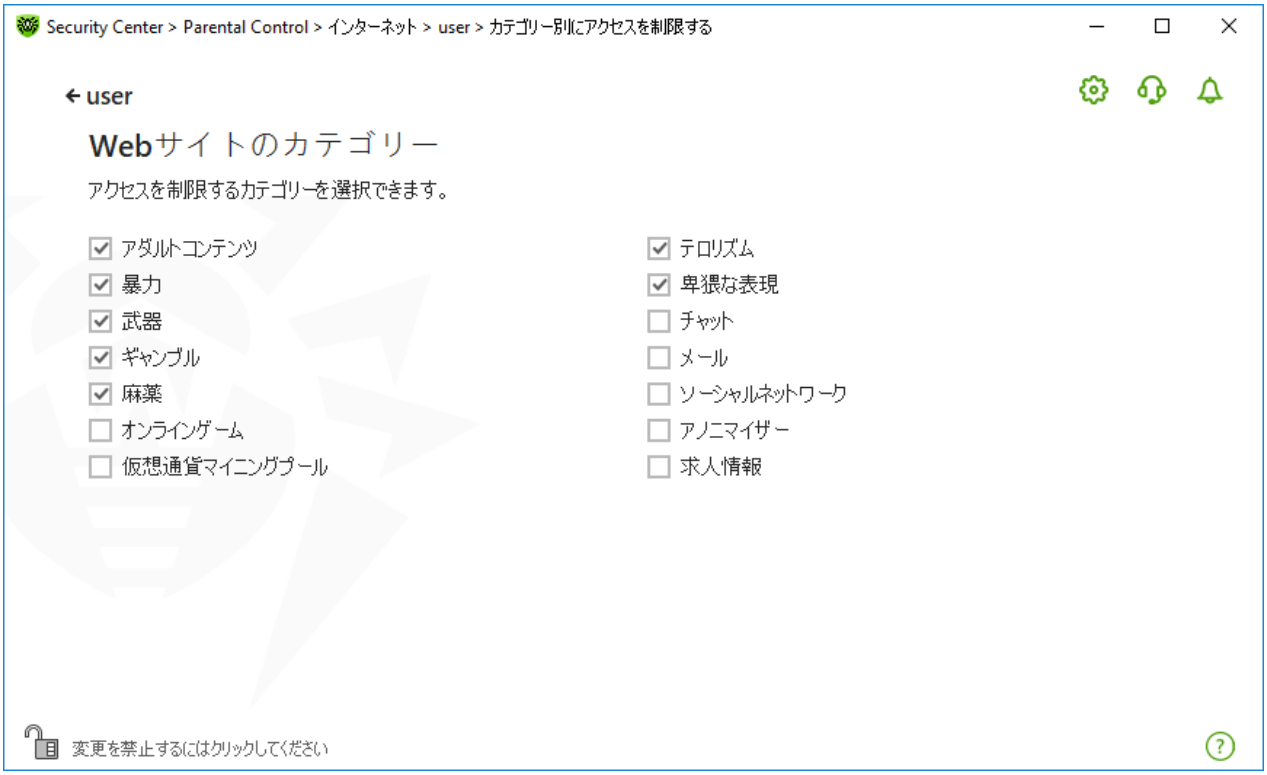

図 106. ブロックするWebサイトのカテゴリー

2. 特定のカテゴリーの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ー

カテゴリー	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Parental 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。

Parental 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 107. Parental 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サイトを **ホワイトリスト** フィールドに追加し、アクセスをブロックするサイトを **ブラックリスト** フィールドに追加します。リストにはマスク、ドメイン、またはURLアドレスを入力できます:

   - 特定のWebサイトをリストに追加するには、その名前のマスクを入力します。文字、数字、コロン(:)、スラッシュ(/)、ハイフン(-)、疑問符(?)、アスタリスク(*)を使用できます。マスクは `mask://...` の形式で追加されます。

     マスクはオブジェクト名の共通部分を定義します:

     - アスタリスク記号(*) は、任意の一連の文字列(空白も含む)を表します。
     - 疑問符(?)は、任意の1文字(空白も含む)を表します。

     例:

     - `mask://*.com/` - ドメインが `.com` であるすべてのWebサイトへのアクセスを許可／ブロックします。
     - `mask://mail` - 名前に「mail」を含むあらゆるWebサイトへのアクセスを許可／ブロックします。
     - `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サイトへのアクセスを許可／ブロックします。

   - 特定のドメイン内のWebサイトをリストに追加するには、アドレスの末尾にドット(.)を付けて、または付けずにドメイン名を入力します。文字、数字、スラッシュ(/)を使用できます。

     例:

     - `example.com` - `example.com` とそのサブドメイン `*example.com` へのアクセスを許可／ブロックします。
     - `example.` - サブドメイン `*example.com` へのアクセスは許可／ブロックしますが、`example.com` へのアクセスは許可／ブロックしません。

- .com - ドメイン .com のすべてのサブドメイン(example.com や www.test.com など)へのアクセスを許可／ブロックします。

- URLに特定のテキストを含むWebサイトをリストに追加するには、入力フィールドにそのテキストを入力します。文字、数字、スラッシュ(/)、ハイフン(-)を使用できます。

  例:

  - example.com/test - example.com/test11、template.example.com/test22 などのWebページへのアクセスを許可／ブロックします。
  - example - example.com、example.test.com、test.com/example、test.example222.com などのWebページへのアクセスを許可／ブロックします。

入力したアドレスは統一される場合があります。例:https://www.example.com は example.com に変換されます。

マスク、ドメイン、アドレスでは大文字と小文字が区別されません。例:example.com と ExAMple.COM は同じものとして扱われます。

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Webサイトを追加するには、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。

13.2. 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、または間隔を指定することで、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、Parental 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。

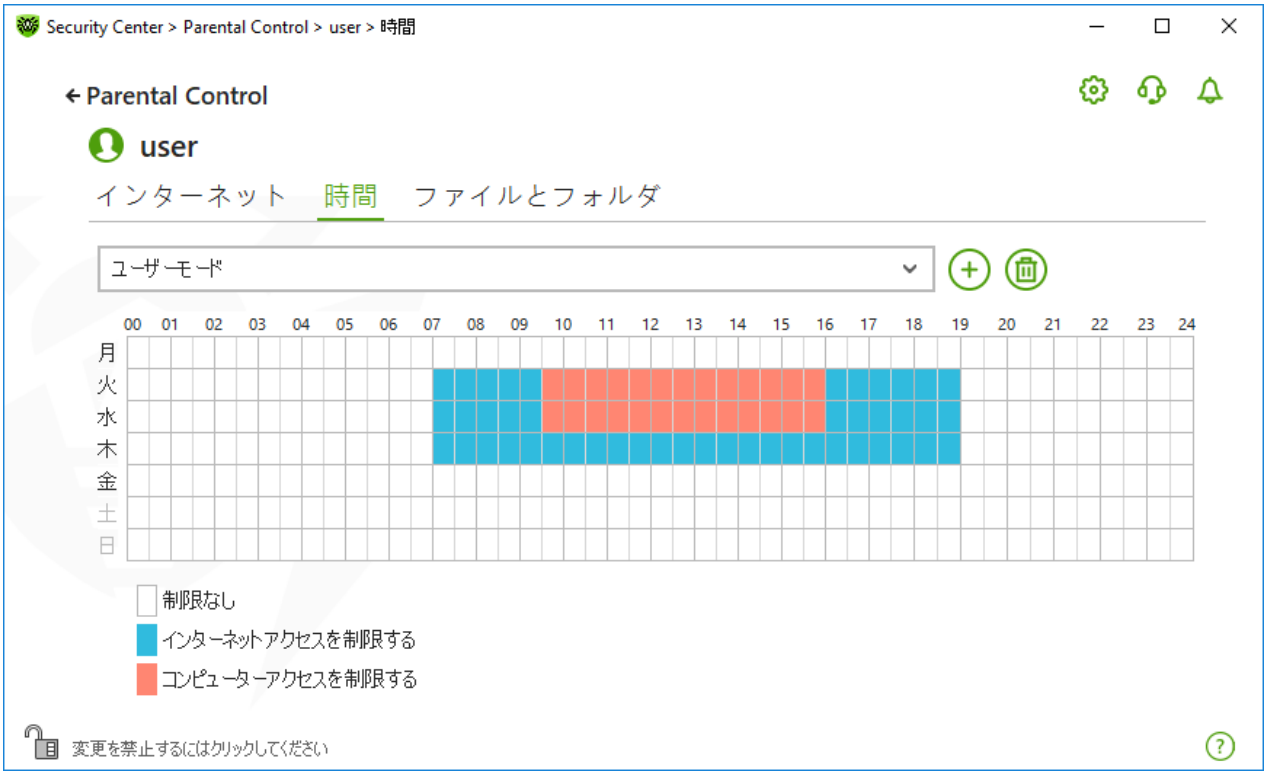

図 108. コンピューターおよびインターネット使用の表

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（例えば、学期中と休暇中で異なる制限時間を設定することができます）。

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。

コンピューター使用時間の上限

ユーザーが1日にコンピューターを使用することのできる時間を指定するには、**スキャン間隔の上限** モードを選択します。このモードでは、1日の使用時間をユーザーが自分で管理することができます。このモードではインターネットの使用に時間制限を設定することはできません。制限を設定するには、テーブルモードを使用します。

図 109. 使用時間の上限を設定する

以下の期間におけるコンピューターの使用時間を制限することができます。

- 月曜日から金曜日まで
- 土曜日と日曜日

ブロック グループでは、中断しないコンピューターの使用時間と使用を制限する時間（中断時間）を設定できます。

アドバンス設定 リンクをクリックすると、**夜間** 設定グループが使用可能になり、アクセスが許可されている合計時間に関係なく、夜間のコンピューターへのアクセスを制限できます。

13.3. 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 110. 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。

14. ツール

このウィンドウでは、Dr.Web製品を制御するための高度なツールにアクセスできます。

ツール 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、ツール タイルをクリックします。

図111. ツール

必要なツールウィンドウを開くには、対応するタイルをタップします。

このセクションでは以下の設定を行うことができます。

- 隔離マネージャー - 隔離されたファイルのリストと復元
- アンチウイルスネットワーク - ネットワーク内の他のコンピューターにインストールされているDr.Web製品へのリモートアクセス
- ライセンスマネージャー - 新しいライセンスを受け取るライセンス情報

14.1. 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. 開いたウィンドウで、**ツール** タイルをクリックします。
3. **隔離マネージャー** タイルをクリックします。

図 112. 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。

14.2. アンチウイルスネットワーク

このツールは、ネットワーク内にある他のコンピューター上の同一製品バージョン内のDr.Web Anti-virus for Windows、Dr.Web Anti-virus for Windows Servers、Dr.Web Security Spaceをユーザーが管理することを可能にします。

アンチウイルスネットワーク 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. 開いたウィンドウで、**ツール** タイルをクリックします。
3. **アンチウイルスネットワーク** タイルをクリックします。

図 113. アンチウイルスネットワークのノード

コンピューターにインストールされたDr.Web製品がリモート接続を許可している場合は、コンピューターがリスト表示されます。Dr.Webへの接続許可は、アンチウイルスネットワーク設定ページ で設定できます。

目的のコンピューターがリスト上にない場合は、手動で追加してください。⊕ をクリックし、IPv4またはIPv6の形式でIPアドレスを入力します。

⚠ 端末でコンポーネントが無効になっている場合は、感嘆符が表示されます。

アンチウイルスネットワーク動作のパラメータ

アンチウイルスネットワークの動作には、次のパラメータのマルチキャストおよびUDP要求が使用されます。

マルチキャスト要求のパラメータ:

- IPアドレス: IPv4の場合239.194.75.48、IPv6の場合ff08::28
- ポート: 55566
- ポーリング間隔: 2000ミリ秒

UDP要求のパラメータ:

- ポート: 55566
- ポーリング間隔: 2000ミリ秒

リモート**Dr.Web**に接続するには

1. リストから必要なコンピューターを選択します。展開された行には、端末上のコンポーネントのステータスと最後の更新についての詳細情報が表示されます。
2. **接続** をクリックします。
3. リモートアンチウイルスの設定内で 指定した コードを入力してください。リモート SpIDer Agent のアイコン がWindows通知領域内に表示され、接続成功についての通知が表示されます。

> リモートDr.Web製品との間に確立できる接続は1つのみです。既に接続が1つ確立されている場合、**接続** ボタンは無効になります。

統計を表示したり、コンポーネントを有効または無効にしたり、設定を変更したりできます。アンチウイルスネットワーク、隔離、Scanner、データ損失防止 は利用できません。

切断する オプションにもアクセスできます。このオプションを選択すると、リモートアンチウイルスへの現在の接続が無効になります。

14.3. ライセンスマネージャー

ライセンスマネージャーを使用して、お使いのコンピューター用のすべてのDr.Web ライセンス を確認することができます。また、使用するライセンスの変更、ライセンスの更新、新しいライセンスの購入とその有効化を行うこともできます。

Security Centerから ライセンスマネージャー 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. 開いたウィンドウで、ツール タイルをクリックします。
3. ライセンスマネージャー タイルをクリックします。

プログラムメニューから ライセンスマネージャー ウィンドウを開くには

1. Dr.Web メニュー を開きます。
2. ライセンス を選択します。

図 114. ライセンスマネージャー

現在のライセンスに関する詳細情報を見るには、**詳細** をクリックします。

現在使用されていないライセンスに関する情報を見るには

1. **詳細** をクリックして、ライセンス情報ウィンドウを開きます。
2. ドロップダウンリストから該当するライセンスを選択します。

ライセンスが複数の製品を対象としている場合は、リンク **他の対象製品** をクリックすると、対象となるすべての製品のリストがドロップダウンリストに表示されます。

同時に複数のライセンスを有効化している場合、ライセンスごとに有効期限が切れます。これを防ぐには、新しいライセンスを有効化する際に、以前に有効化したライセンスのシリアル番号を指定してください。これにより、すべてのライセンスの有効期間が統合されます。

ライセンスを削除するには

1. Dr.Webが 管理モード 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）。管理モードではない場合は、ロックをクリックします。
2. **詳細** をクリックして、ライセンス情報ウィンドウを開きます。
3. ドロップダウンリストから削除するライセンスを選択して、をクリックします。有効なライセンスが1つしかない場合、そのライセンスを削除することはできません。

ライセンスを現在のライセンスとして設定するには

1. Dr.Webが 管理モード 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）。管理モードではない場合は、ロックをクリックします。
2. **詳細** をクリックして、ライセンス情報ウィンドウを開きます。
3. 現在のライセンスとして設定するライセンスをドロップダウンリストから選択して、をクリックします。

購入する ボタンをクリックするとDoctor Web公式サイト上のページが開き、そこで新しいライセンスを購入するか、または現在のライセンスを更新できます。

- 有効化されたライセンスがない場合、新しいライセンスを購入できるページが開きます。サイト上の指示に従って、新しいライセンスを購入して有効化してください。
- すでに有効化されたライセンスをお持ちの場合、ライセンスの更新ページが開き、そこに現在のライセンスのすべてのパラメータが送信されます。サイト上の指示に従って、ライセンスを更新して有効化してください。ライセンス更新の詳細については、ライセンス更新 セクションを参照してください。

有効化 をクリックすると、新しいライセンスを有効化 するためのウィンドウが開きます。

アドバンス

ライセンス契約 をクリックすると、Doctor Web公式サイト上の使用許諾契約書が開きます。

15. 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115. 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。

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 - スパム用のSpIDer Mailメッセージのスキャンを設定します。

15.1. 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す。

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。

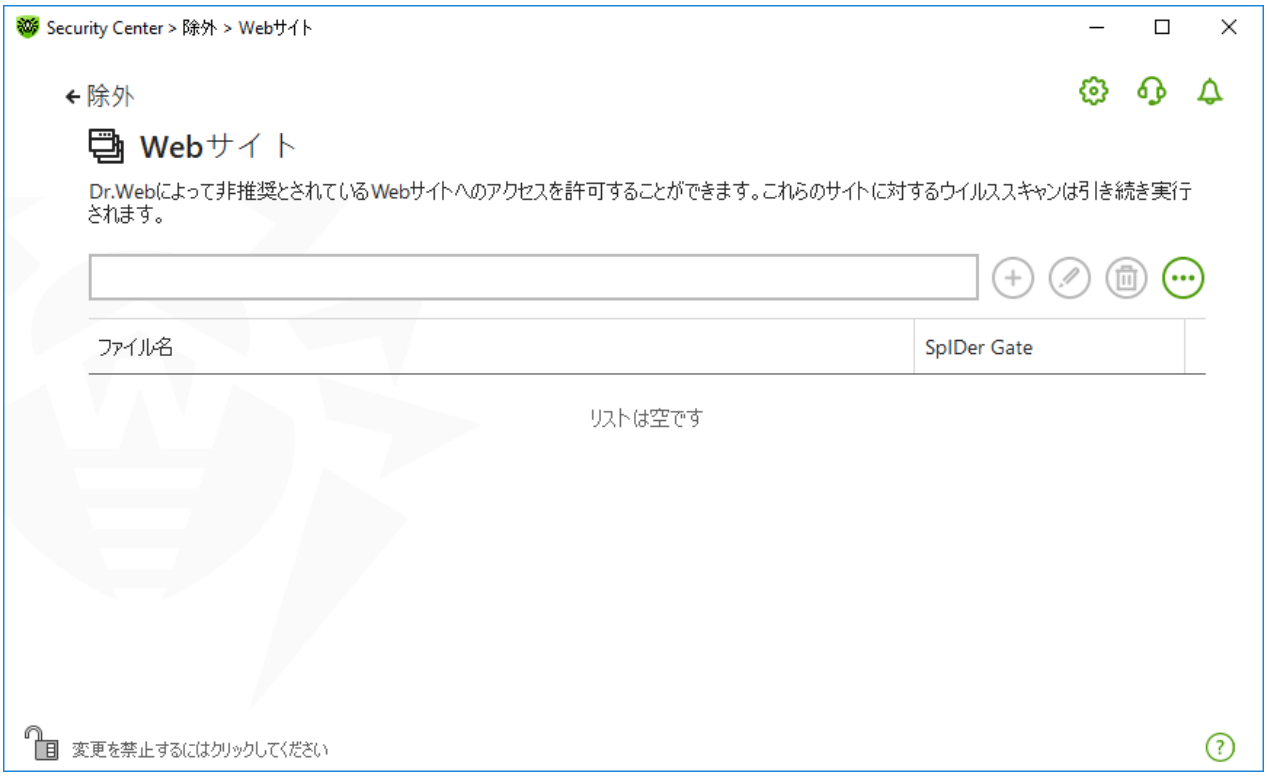

図116. 除外するWebサイトのリスト

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サイトにアクセスすることができるようになります。Webサイトが Parental 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。

15.2. 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117. 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。

15.3. 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 118. 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。

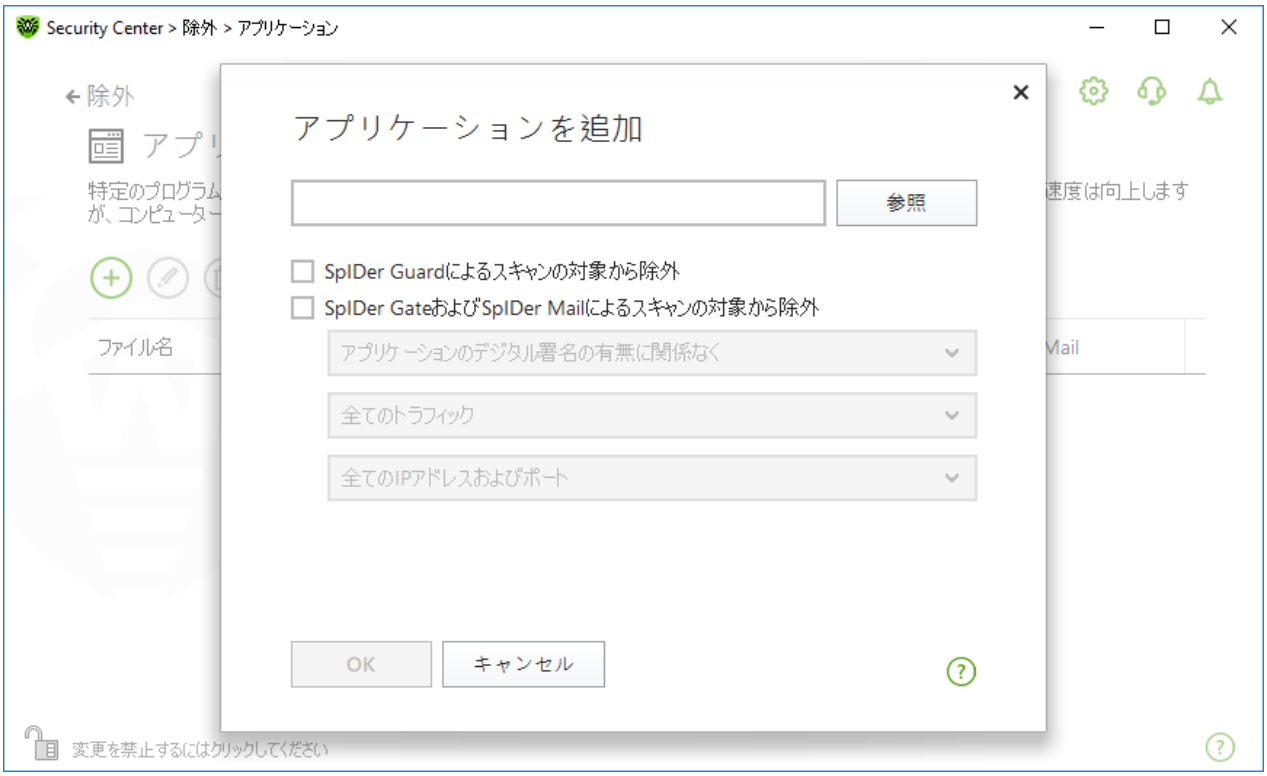

図119. アプリケーションを除外リストに追加する

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： • 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。

15.4. 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120. 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。

16. 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
   - Parental Control
   - 脅威
   - Firewall

図121. 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。

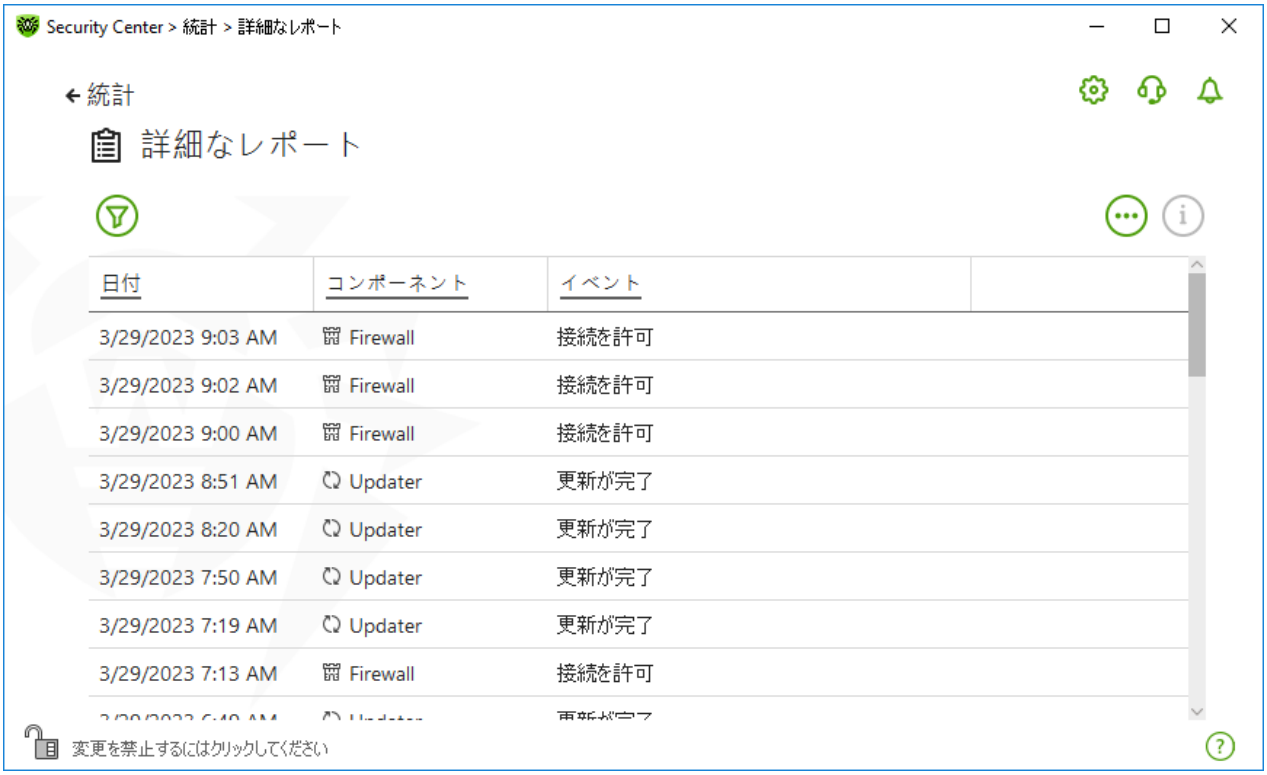

図122. 詳細なレポートウィンドウ

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 、、 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。

Parental Control

Parental 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。

図123. Parental 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ーまたは除外リスト。

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 、、 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。

図124. 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 、、 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。

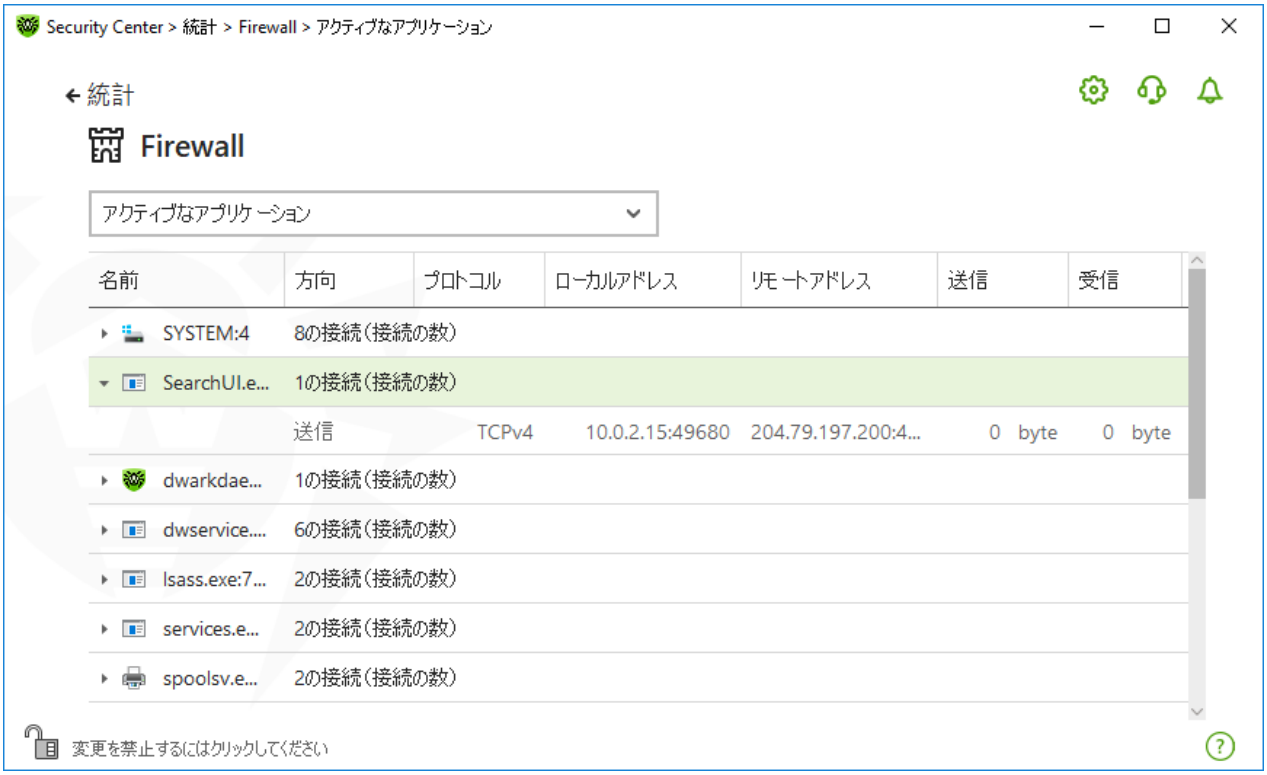

図125. Firewallウィンドウの統計

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べ替えられます。

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。

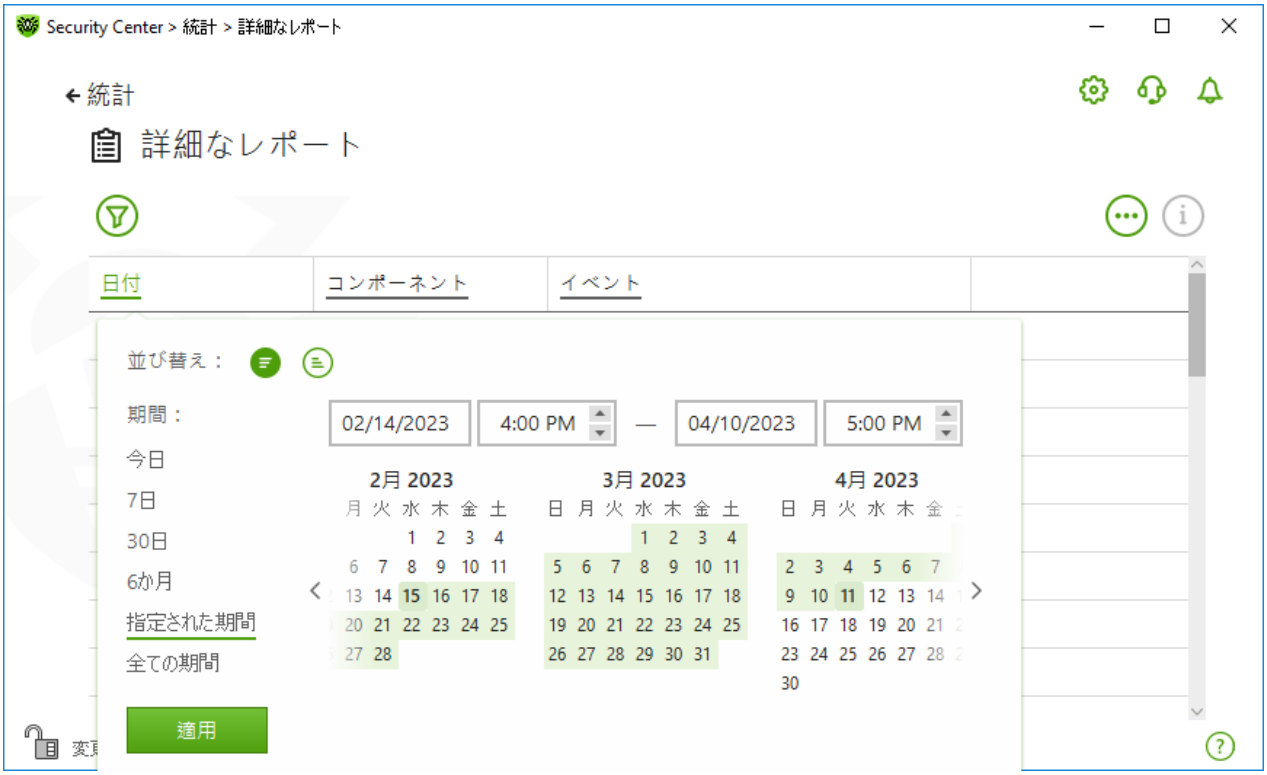

図126. データのソート

- 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べ替えたりできます。
- 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べ替えたりできます。

Parental 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べ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べ替えたりできます。

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。

17. 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/ 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。

17.1. 問題解決サポートオプション

Doctor Webテクニカルサポート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の動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。

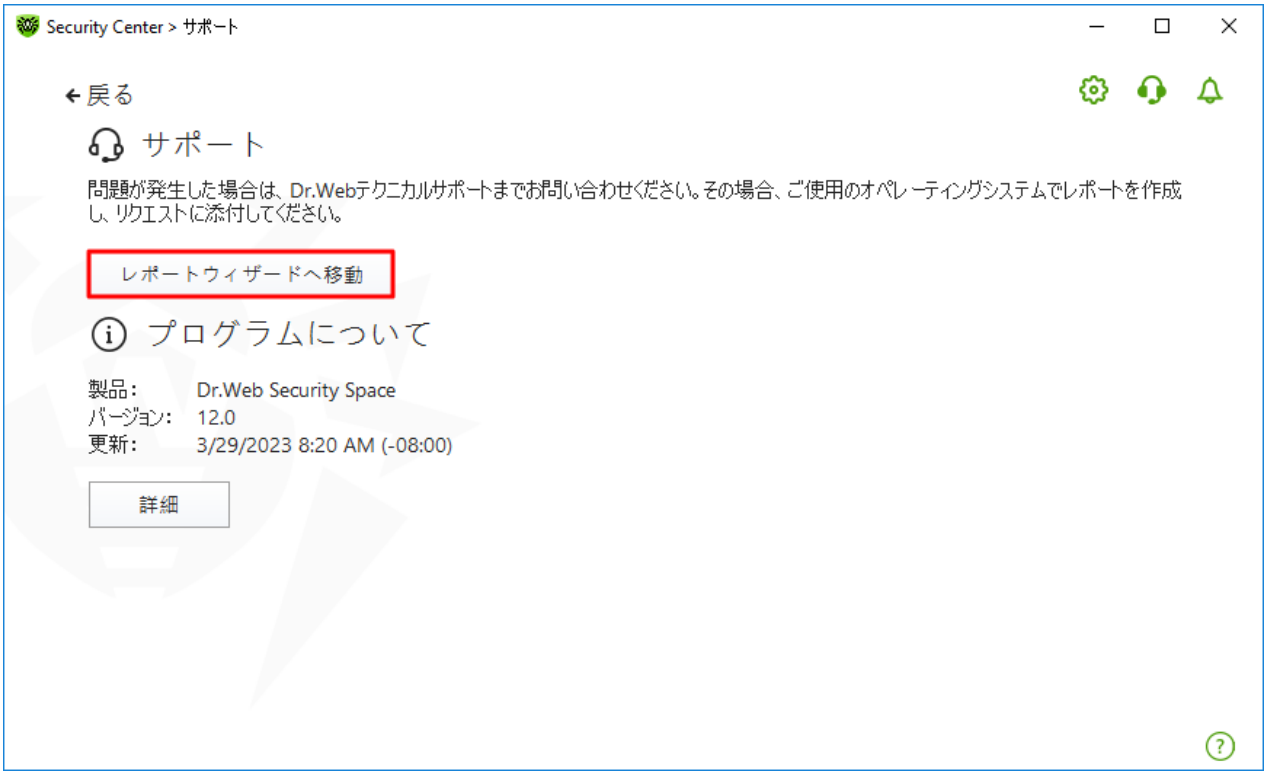

図127. サポート

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。

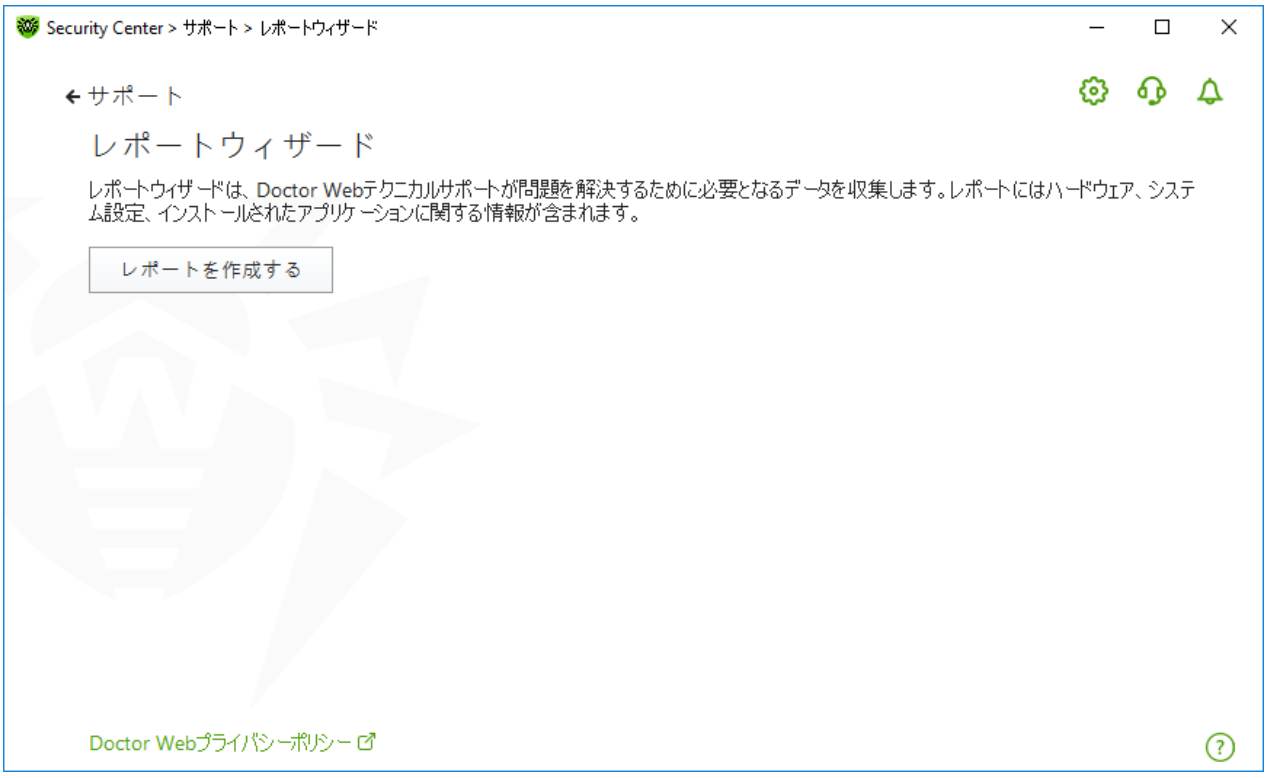

図128. テクニカルサポート用にレポートを生成する

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
   - システムフォルダー一覧
   - 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。

17.2. 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アイコンを開き、**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129.Dr.Webについて ウィンドウへのアクセス

18. 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、Dr.Web Updater で使用可能です。

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。

18.1. 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:*<commpression_ratio>*	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:*<nesting_level>*	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:*<size>*	最大アーカイブサイズ(デフォルト:無制限、単位:KB)。
/ART:*<size>*	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:*<size>*	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)
/CL	クラウドチェックを使用します。デフォルトで有効になっています。(Console 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。

スイッチ	説明
/E: *<number_of_threads>*	指定されたスレッド数でスキャンを実行します。
/FAST	システムの クイックスキャン を実行します。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: *<file_name>*	指定したファイルにリストされているパスをスキャンします。
/FM: *<mask>*	指定されたマスクに合致するファイルをスキャンします。デフォルトではすべてのファイルがスキャンされます。
/FR: *<regexpr>*	指定された正規表現に合致するファイルをスキャンします。デフォルトではすべてのファイルがスキャンされます。
/FULL	すべ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: *<mask>*	指定されたマスクに合致するファイルを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。
/KEY: *<key_file>*	キーファイルへのパスを指定します。Scanner実行ファイルのあるインストールフォルダ以外の場所にキーファイルが保存されている場合、このパラメータを指定する必要があります（デフォルトでは C:\Program Files\DrWeb\ フォルダの drweb32.key またはその他適切なファイルが使用されます）。
/LITE	RAMおよびすべ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	メールファイルをスキャンします。デフォルトで有効になっています。

スイッチ	説明
/MC:*<number_of_attempts>*	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：%）。
/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	スキャンされたすべてのオブジェクトの一覧を表示し、感染していないファイルに Ok を表示します。デフォルトで無効になっています。
/P:*<priority>*	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:*<nesting_level>*	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	すべ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:*<logical_drive_letter>*	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、すべ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	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:*<file_name>*	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）。

スイッチ	説明
/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:*<file_name>*	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:*<sec>*	Scanning Engineの接続タイムアウト。デフォルトでは30秒です。（Console Scannerのみ）
/RPCD	動的RPC IDを使用します。（Console Scannerのみ）
/RPCE	動的RPCエンドポイントを使用します。（Console Scannerのみ）
/RPCE:*<target_address>*	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:*<host_name>*	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:*<protocol>*	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。

スイッチ	説明
/TR	システム復元ポイントをスキャンします。
/W:*<sec>*	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して次のアクションを指定できます（C - 修復、Q - 隔離、D - 削除、I - 無視、R - 通知。R はConsole Scannerでのみ使用可能で、デフォルトですべ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:

[*<path_to_program>*]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すべ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。

18.2. Dr.Web Updaterコマンドラインパラメータ

共通オプション

パラメータ	説明
-h [--help]	プログラムの使用方法に関する簡単なヘルプメッセージを表示します。
-v [--verbosity] arg	ログの詳細レベル。次のうち1つを設定: error(標準)、info(詳細)、debug(デバッグ)
-d [--data-dir] arg	レポジトリと設定のあるフォルダ。
--log-dir arg	ログファイル保存フォルダ。
-r [--repo-dir] arg	レポジトリフォルダ(デフォルトでは *<data_dir>*/repo)。
-t [--trace]	トレースを有効にします。
-c [--command] arg (=update)	実行するコマンド: getversions、getcomponents、update、uninstall、exec、keyupdate、download
-z [--zone] arg	設定ファイルで指定されたゾーンの代わりに使用するゾーンのリスト

init コマンドパラメータ

パラメータ	説明
-s [--version] arg	バージョン番号。
-p [--product] arg	製品名。

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

updateコマンドパラメータ

パラメータ	説明
-p [--product] arg	製品名。指定した場合、その製品のみが更新されます。指定しなかった場合は、すべての製品が更新されます。コンポーネントが指定された場合、それらのコンポーネントのみが更新されます。
-n [--component] arg	指定されたバージョンへ更新するコンポーネント。 *<name>, <target revision>*
-x [--selfrestart] arg (=yes)	Dr.Web Updaterの更新後に再起動します。デフォルトで `yes` に設定されています。`no` に設定した場合、再起動を要求する通知が表示されます。
--geo-update	更新前に `update.drweb.com` からIPアドレスリストを取得します。
--type arg (=normal)	以下の内の1つ: • `reset-all` - すべてのコンポーネントの強制更新 • `reset-failed` - 破損したコンポーネントのリビジョンをリセット • `normal-failed` - 破損したものを含むすべてのコンポーネントを、現在のリビジョンから最新リビジョンまたは指定されたリビジョンに更新しようとします • `update-revision` - 現在のリビジョンのすべてのコンポーネントを最新リビジョン(ある場合)に更新しようとします • `normal` - すべてのコンポーネントを更新
-g [--proxy] arg	更新用のプロキシサーバー。*<address>:<port>*
-u [--user] arg	プロキシサーバーのユーザー名。
-k [--password] arg	プロキシサーバーのパスワード。
--param arg	追加のパラメータをスクリプトに渡します。 *<name>: <value>*

パラメータ	説明
-l [--progress-to-console]	ダウンロードとスクリプト実行に関する情報をコンソールに出力します。

getcomponentsコマンドパラメータ

パラメータ	説明
-s [--version] arg	バージョン番号。
-p [--product] arg	お使いの製品に含まれるコンポーネントのリストを取得するために製品を指定します。製品が指定されていない場合、そのバージョンのすべてのコンポーネントがリストアップされます。

getrevisionsコマンドパラメータ

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

uninstallコマンドパラメータ

パラメータ	説明
-n [--component] arg	アンインストールするコンポーネント名。
-l [--progress-to-console]	コマンド実行に関する情報をコンソールに出力します。
--param arg	追加のパラメータをスクリプトに渡します。 *<name>: <value>*
-e [--add-to-exclude]	削除するコンポーネント。このコンポーネントの更新は行われません。

keyupdateコマンドパラメータ

パラメータ	説明
-m [--md5] arg	以前のキーファイルのMD5ハッシュ値。
-o [--output] arg	新しいキーを保存するためのファイル名を出力します。
-b [--backup]	古いキーファイルが存在する場合は、そのバックアップ。
-g [--proxy] arg	更新用のプロキシサーバー。*<address>:<port>*

パラメータ	説明
-u [--user] arg	プロキシサーバーのユーザー名。
-k [--password] arg	プロキシサーバーのパスワード。
-l [--progress-to-console]	キーファイルのダウンロードに関する情報をコンソールに出力します。

downloadコマンドパラメータ

パラメータ	説明
--zones arg	ゾーンの記述ファイル。
--key-dir arg	キーファイルが保存されているフォルダ。
-l [--progress-to-console]	コマンド実行に関する情報をコンソールに出力します。
-g [--proxy] arg	更新用のプロキシサーバー。*<address>:<port>*
-u [--user] arg	プロキシサーバーのユーザー名。
-k [--password] arg	プロキシサーバーのパスワード。
-s [--version] arg	バージョン。
-p [--product] arg	ダウンロードする製品の名前。

18.3. 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。

リターンコードの値	イベント
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。

19. 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います。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。

19.1. 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一致するとは限りません。ほとんどのウイルスは、システム内のデータを破損させる、または破壊する目的を持っています。

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、そのタスクを続行することができます。

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ン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はユーザーモードライブラリ機能を妨害し、一方、KMRはシステムのカーネルレベルで機能を妨害し、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もあります。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。

19.2. 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。

20. 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す。そのような原則を知ることは、保護するシステム上のソフトウェアや脆弱性を理解する上で有益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
- HLLO - 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ー）
- IRC - Internet Relay Chat チャンネルを使用するトロイの木馬
- DownLoader - 様々な悪意のあるプログラムをインターネット経由で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）にリダレクトするトロイの木馬
- KeyLogger - キーボード入力を記録し、収集された情報を犯罪者に送信するスパイウェアトロイの木馬
- AVKill - アンチウイルスプログラムやファイアーウォールなどを停止、または削除します
- KillFiles、KillDisk、DiskEraser - 特定のファイル（ドライブ上の全てのファイル、特定のフォルダ内にあるファイルなど）を削除します
- DelWin - Windows OS の動作に必要なファイルを削除します

- FormatC - C ドライブをフォーマットします（FormatAll - 全てのドライブをフォーマットします）
- KillMBR - マスターブートレコード（MBR）を破壊または削除します
- KillCMOS - CMOS メモリを破壊または削除します

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

21. 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。