Dr.WEB
for Linux

ユーザーマニュアル

Dr.Web for Linux
バージョン11.1
ユーザーマニュアル
2024/01/10

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

はじめに

Dr.Web for Linuxをご購入いただきありがとうございます。本製品は最先端のウイルス 検出 ・駆除テクノロジーにより、様々なタイプの コンピューター脅威 からの信頼できる保護を提供します。

本マニュアルには、GNU/Linux系OS（以下UNIX とします）でのDr.Web for Linuxバージョン11.1のインストールと 使用に関する説明が記載されています。

コンピューター上に以前のバージョンのDr.Web for Linuxがすでにインストールされていて、それをバージョン11.1にアップグレードする場合は 新しいバージョンにアップグレードする に記載された手順に従ってください。

表記規則と略語

本マニュアルでは、以下の文字・記号を使用しています。

文字・記号	説明
	重要な事項や指示
	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
`/home/user`	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

本マニュアルでは、(端末または端末エミュレーターで)キーボードから入力されるコマンドラインのコマンドには、コマンドプロンプト記号 `$` または `#` が付いています。この記号は、該当するコマンドの実行に必要な権限を表しています(UNIX系システムの標準的規則に従って)。

`$` - コマンドはユーザー権限で実行できることを示します。

`#` - スーパーユーザー(通常は *root*)権限でコマンドを実行できることを示します。権限を昇格するには、`su` と `sudo` コマンドを使用してください。

略語のリストは、セクション 付録F. 略語のリスト にあります。

この製品について

このセクションには製品に関する以下の情報が含まれています。

機能

Dr.Web for Linuxはウイルスやその他のマルウェアから GNU/Linux コンピューターを保護するためのアンチウイルスソリューションです。

プログラムのメインコンポーネント（スキャンエンジン、ウイルスデータベース）は極めて効率的かつ省リソースなだけでなく、クロスプラットフォームでもあります。そのため、Doctor Webのスペシャリスト達は、さまざまなプラットフォームを標的とする脅威からポピュラーなOSのコンピューターやモバイルデバイスを保護する信頼性の高いアンチウイルスソリューションを作成することが可能です。現時点で、Doctor WebではDr.Web for Linuxのほかに、UNIX系システム（FreeBSD）、IBM OS/2、Novell NetWare、macOS、Windows 向けのアンチウイルスソリューションを提供しています。また、Android、Symbian、BlackBerry搭載デバイスに対する保護も提供しています。

最先端の保護を確実なものにするため、Dr.Web for Linuxのコンポーネントは定期的に更新され、Dr.Webウイルスデータベースには新しい署名が追加されています。未知のウイルスからの追加の保護を提供するため、スキャンエンジンにはヒューリスティック解析機能が実装されています。また、脅威に関する最新の情報を収集するDr.Web Cloudに接続することで、ユーザーが望ましくないWebサイトを訪問してしまうことを防ぎ、感染したファイルからOSを保護できます。

メイン機能

Dr.Web for Linuxのメイン機能

1. 悪意のあるプログラム（メールファイルやブートレコードを感染させるものを含むウイルス、トロイの木馬、メールワームなど）や望ましくないソフトウェア（アドウェア、ジョークプログラム、ダイアラーなど）の **検出と駆除** を行います。脅威を駆除する方法については、付録A. コンピューター脅威の種類 を参照してください。

   この製品は複数のマルウェア検出手法を同時に使用します。

   - *シグネチャ解析* - ウイルスデータベースに追加されている既知の脅威の検出を可能にします。
   - *ヒューリスティック解析* - ウイルスデータベースに含まれていない脅威の検出を可能にします。
   - *クラウドベースの脅威検出テクノロジー* - Dr.Web Cloudサービスを使用して、新しい脅威に関する最新の情報を収集し、それらをDr.Web製品に送信します。

   ヒューリスティック解析では誤検知が生じる可能性もあります。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、脅威を含むオブジェクトは「疑わしい」と見なされます。そのようなファイルは隔離に移し、解析

のためにDoctor Webアンチウイルスラボに送信することが推奨されます。脅威を駆除する方法については、付録B. コンピューター脅威の駆除 を参照してください。

ファイルシステムのスキャンは、オンデマンドまたはスケジュールによる自動で開始できます。スキャンにはフルスキャン（すべてのファイルシステムオブジェクトをスキャン）とカスタムスキャン（選択されたディレクトリやファイルなどのオブジェクトをスキャン）の2つのモードがあります。また、ユーザーはボリュームブートレコードのスキャンと現在アクティブなプロセスを実行する実行ファイルのスキャンを個別に開始できます。後者の場合、検出された悪意のあるファイルは駆除され、そのファイルによって実行されるすべてのプロセスが強制終了されます。

グラフィカルデスクトップ環境を備えたオペレーティングシステムでは、タスクバーまたはグラフィックファイルマネージャを使用したファイルスキャンの 統合 が可能です。さまざまなアクセスレベルでの強制アクセス制御を実装しているシステムでは、現在のレベルでは利用できないファイルを オフラインコピー としてスキャンできます。

ファイルシステムで検出された脅威を含むすべてのオブジェクトは、自律コピーモードで検出された脅威を除いて、永久保存される脅威のレジストリに登録されます。

Dr.Web for Linuxに含まれている コマンドラインツール を使用することで、SSHまたはTelnet経由でのリモート端末アクセスを提供するリモートネットワークホストのファイルシステムをスキャンし、脅威を検出することができます。

リモートスキャンは、リモートホスト上の悪意のあるファイルや疑わしいファイルを検出するためにのみ使用できます。リモートホスト上で検出された脅威を駆除するには、このホストが直接提供する管理ツールを使用する必要があります。たとえば、ルータや他のスマートデバイスの場合、ファームウェアを更新します。コンピューティングマシンの場合、それらに接続し（リモート端末モードをオプションの1つとして使用して）、ファイルシステムで必要な操作（ファイルの削除または移動など）を実行するか、マシン上にインストールされているアンチウイルスソフトウェアを実行します。

2. **ファイルへのアクセス監視** - このモードは、データファイルへのアクセスと実行ファイルを実行しようとする試みを追跡します。これにより、コンピューターを感染させようとするマルウェアを検出して駆除することができます。標準監視モードのほか、スキャンが完了するまでファイルへのアクセスをブロックする 強化（パラノイド）モードを使用することができます（脅威を含むファイルへのアクセスを防ぐのに役立ちますが、スキャン結果はアプリケーションがファイルにアクセスすることができた後でのみ明らかになります）。パラノイドモードではセキュリティが向上しますが、検証されていないファイルへのアプリケーションのアクセスは遅くなります。
3. **ネットワーク接続の監視** - HTTPおよびFTPプロトコルを使用してインターネットサーバー（Webサーバー、ファイルサーバー）にアクセスしようとする試みをすべて監視します。望ましくないカテゴリのWebサイトまたはホストへのアクセスや、悪意のあるファイルのダウンロードをブロックします。
4. **メールメッセージのスキャン** - 感染ファイルや望ましくないリンクを含むメール、スパムとして分類されたメールの送受信をブロックします。

   メールおよびダウンロードされるファイルに対する、ウイルスやその他Web上の脅威についてのスキャンは即座に実行されます。ディストリビューションによっては、Dr.Web for LinuxでDr.Web Anti-Spamを利用できない場合があります。そのような場合、メールメッセージのスパムスキャンは実行されません。

   望ましくないWebサイトへのアクセスを制限するために、Dr.Web for Linuxは自動的に更新されるWebリソースカテゴリーのデータベースと、ユーザーが編集するブラック／ホワイトリストをサポートしています。要求されたWebリソースがDr.Webの他のアンチウイルス製品によって悪意のあるものと判断されたものでないかどうかをチェックするために、Dr.Web Cloudサービスも使用されます。

アンチスパムコンポーネントDr.Web Anti-Spamによって誤って検出されたメールメッセージがある場合は、分析のため、また、スパムフィルタの品質向上のためにそれらを特別なアドレスに転送していただけますようお願いいたします。これを行うには、各メッセージを別々の `.eml` ファイルに保存します。次に、ファイルをメールメッセージに添付して、専用のアドレスに転送してください。

- *誤ってスパムと判定された* メッセージは nonspam@drweb.com に送信してください。
- *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。

5. **感染したオブジェクトや疑わしいオブジェクトの確実な隔離** - システムに害を及ぼすことを防ぐため、このようなオブジェクトは特別なストレージ(隔離)に移されます。隔離に移されたオブジェクトは特別な規則に従って名前を変更され、必要に応じて元の場所に復元できます(要求に応じてのみ)。
6. Dr.Webウイルスデータベースとスキャンエンジンの **自動更新** が、マルウェアに対するレベルの高い保護をサポートします。
7. ウイルスイベントに関する **統計の収集**、脅威検出イベントのロギング(コマンドラインツールからのみ利用可能)、およびウイルスインシデントに関する統計情報のDr.Web Cloudサービスへの送信。
8. **集中管理モードでの動作** (Dr.Web Enterprise Server、またはDr.Web AV-Deskサービスの一部としての集中管理サーバーに接続している場合) - このモードでは、保護されたネットワーク内のコンピューターに、統合されたセキュリティポリシーを導入することができます。ネットワークには、企業ネットワーク、プライベートネットワーク(VPN)、またはサービスプロバイダーのネットワーク(インターネットサービスプロバイダーなど)などが該当します。

Dr.Web Cloudサービスに保存されている情報を使用するには、ユーザーアクティビティ(訪問したWebサイトのアドレスなど)に関するデータの転送が必要です。そのため、Dr.Web Cloudは、ユーザーからの該当する同意を得た後でのみ使用することが可能になります。必要に応じて、いつでもプログラム設定内でDr.Web Cloudの使用を無効にすることができます。

Dr.Web for Linuxの構成

Dr.Web for Linuxは以下のコンポーネントで構成されています。

コンポーネント	説明
Scanner	ユーザーのリクエストに応じて、またはスケジュールに従ってファイルシステムオブジェクト(ファイル、ディレクトリ、ブートレコード)のスキャンを実行し、脅威を検出するコンポーネントです。ユーザーは グラフィカル モード、または コマンドライン からスキャンを開始できます。
SpIDer Guard	ファイル操作(作成、開く、閉じる、起動など)を追跡する常駐モードのコンポーネントです。プログラムの起動時に、実行ファイルのほか、新規ファイルや変更されたファイルの内容をスキャンするようScannerに要求を送信します。fanotifyシステムメカニズムまたはDoctor Webによって開発された特別なカーネルモジュール(*LKM [Linux Kernel Module]*)を使用してOSファイルシステムで動作します。fanotifyシステムメカニズムを使用する場合、モニターは強化モードで動作し、スキャンが完了するまで、まだチェックされていないファイル(すべての種類または実行ファイルのみ)へのアクセスをブロックします。デフォルトでは、強化モニタリングモードは 無効 になっています。
SpIDer Gate	常駐モードで動作し、すべてのネットワーク接続を監視するコンポーネントです。

コンポーネント	説明
	• リクエストされたURLがWebリソースの望ましくないカテゴリー（データベース）やユーザーのブラックリストに含まれていないかどうかを確認し、含まれていた場合は、それらリソースへのアクセスをブロックします 。 • 悪意のあるオブジェクトや望ましくないリンクが含まれたメールの送信をブロックします。 • また、このコンポーネントは、インターネットから（アクセスが制限されていないサーバーから）ダウンロードされるファイルをスキャンするScannerタスクを送信し、脅威が含まれている場合はダウンロードをブロックします。 そのほか、ユーザーが許可した場合は、スキャンのためにURLをDr.Web Cloudサービスへ送信します。
Scanning Engine	アンチウイルスソリューションのコアコンポーネントです。ウイルスや悪意のあるプログラム を 検出 するため、また、疑わしい動作を分析するためにScannerによって使用されます。
Dr.Web Anti-Spam	スパムメールのスキャンを実行するコンポーネントです。このコンポーネントは、ARM64およびE2Kアーキテクチャ向けのバージョンには含まれていません。
ウイルスデータベース	既知の脅威に関する情報が含まれた、自動的に更新されるデータベースです。脅威を検出して修復するためにスキャンエンジンによって使用されます。
Webリソースカテゴリーのデータベース	カテゴリーに分類されたWebリソースのリストが含まれる、自動的に更新されるデータベースです。望ましくないWebサイトへのアクセスをブロックするためにSpIDer Gateによって使用されます。
更新コンポーネント	ウイルスデータベース、Webリソースカテゴリーのデータベース、スキャンエンジンの更新をDoctor Webサーバーから自動的に（スケジュールに従って、またはオンデマンドで）ダウンロードするコンポーネントです。
グラフィカル管理インターフェース	Dr.Web for Linuxを管理するためのウィンドウグラフィカルインターフェースを提供するコンポーネントです。このコンポーネントは、ユーザーがグラフィカルモードでファイルシステムオブジェクトのスキャンを実行、SpIDer GuardおよびSpIDer Gateの動作を管理、隔離されたオブジェクトを確認、更新の受信を開始、Dr.Web for Linux動作を設定することを可能にします。
通知エージェント	バックグラウンドモードで動作するコンポーネントです。イベントのポップアップ通知ならびにDr.Web for Linuxインジケータを通知領域に表示し、スケジュールスキャンを実行します。デフォルトでは、デスクトップ環境でユーザーのセッションが開始された際に起動されます。
ライセンスマネージャー	グラフィカルモードでの ライセンス 管理を簡易化するコンポーネントです。ライセンスまたは試用期間の有効化、現在のライセンスに関する情報の表示、ライセンスの更新、ライセンスキーファイルのインストールまたは削除を行うことができます。

上記のコンポーネントとは別に、Dr.Web for Linuxにはユーザーの操作を必要とせずバックグラウンドで実行される追加のサービスコンポーネントも含まれています。

ファイルシステムモニターSpIDer Guardは、次のいずれかのモードで動作することができます。

- *FANOTIFY* - fanotifyモニタリングインターフェースを使用します（すべてのGNU/Linux系OSがこのモードをサポートしているわけではありません）。
- *LKM* - Doctor Webによって開発されたUNIXローダブルカーネルモジュールを使用します（カーネル2.6.x以降のあらゆるGNU/Linux系OSと互換性があります）。LKMの使用は、ARM64およびE2Kアーキテクチャではサポートされていません。

デフォルトでは、ファイルシステムモニターは環境に応じて自動的に適切な動作モードを選択します。SpIDer Guardを起動できない場合は、配布されたソースコードからローダブルカーネルモジュールを ビルドしてインストール してください。

隔離に移動する

隔離ディレクトリは、システムセキュリティにとって脅威となるファイルを直ちに修復できない場合に、それらを隔離するためのものです。そのような脅威はDr.Web for Linuxにとって未知のもの（すなわち、ヒューリスティックアナライザによって検出されたが、ウイルス署名と修復方法がデータベースに存在しないウイルス）か、スキャン中にエラーを引き起こしたものを指します。また、ユーザーが検出された脅威のリストで該当する アクション を選択した場合、またはScannerやSpIDer Guard設定内でその脅威の 種類 に対して該当するアクションを指定した場合、ファイルをオンデマンドで隔離することも可能です。

隔離されたファイルの名前は特別なルールに従って変更されます。隔離されたファイルの名前を変更することで、ユーザーやアプリケーションによって特定されることを防ぎ、Dr.Web for Linuxに備わった隔離管理ツールを回避してそれらにアクセスしようとする試みを困難にします。また、ファイルが隔離に移されると、それらを起動させる試みを防ぐために実行ビットがリセットされます。

隔離ディレクトリは以下の場所にあります。

- *ユーザーのホームディレクトリ*（コンピューター上に複数のユーザーアカウントが存在する場合、各ユーザーに個別の隔離ディレクトリが作成される可能性があります）
- ファイルシステムにマウントされた *各論理ボリュームのルートディレクトリ*

Dr.Web for Linux隔離ディレクトリの名前には常に `.com.drweb.quarantine` が付き、*「隔離」* アクション が適用されてから作成されます。その際、オブジェクトを隔離するために必要なディレクトリのみが作成されます。ディレクトリを選択する際はファイル所有者の名前を使用します。検索は悪意のあるオブジェクトのある場所から上の階層に向かって行われ、所有者のホームディレクトリに到達した場合、このディレクトリに作成された隔離フォルダが選択されます。そうでない場合、ファイルはボリュームのルートディレクトリ内に作成された隔離内に移されます（これはファイルシステムのルートディレクトリと同じではない場合があります）。したがって、隔離に移された感染したファイルは常にボリューム上にあり、これより、システム内の異なる場所に複数のリムーバブルデータストレージや他のボリュームがマウントされている場合に隔離の正常な動作を可能にします。

ユーザーは隔離内のオブジェクトを グラフィカル モードで、または コマンドライン から管理できます。すべてのアクションが、統合された隔離に対して適用されます。すなわち、加えられた変更はその時点で使用可能なすべての隔離ディレクトリに対して適用されます。ユーザーにとって、ユーザーのホームディレクトリ内にある隔離ディレクトリは *ユーザー隔離* となり、それ以外の隔離ディレクトリは *システム隔離* となります。

隔離されたオブジェクトに対する操作は 有効なライセンス が見つからない場合でも行うことができます。ただし、この場合、隔離されたオブジェクトを修復することはできません。

ファイルのパーミッションと権限

ファイルシステムのオブジェクトをスキャンし、脅威を駆除するために、Dr.Web for Linux（を動作させるユーザー）は以下のパーミッションを必要とします。

アクション	必要な権限
検出されたすべての脅威を一覧にする	制限されていません。特別なパーミッションは必要ありません。
コンテナ（アーカイブ、メールファイルなど）のコンテンツを出力する （破損した、または悪意のあるエレメントのみを表示する）	制限されていません。特別なパーミッションは必要ありません。
隔離へ移動する	制限されていません。その読み込みまたは書き込み権限に関係なく、ユーザーは感染したすべてのファイルを隔離できます。
脅威を削除する	ユーザーは削除するファイルに対する書き込み権限を持っている必要があります。 コンテナ（アーカイブ、メール添付ファイルなど）内のファイルで脅威が検出された場合は、削除アクションの代わりにコンテナの隔離への移動が実行されます。
修復する	制限されていません。アクセス権限と修復されたファイルの所有者は修復後も変わりません。 検出された脅威を削除することによって修復が可能である場合、ファイルを削除できます。
隔離からファイルを復元する	ユーザーはファイルの読み込み権限と復元先ディレクトリへの書き込み権限を持っている必要があります。
隔離からファイルを削除する	ユーザーは隔離されたファイルへの書き込み権限を持っている必要があります。

Dr.Web for Linuxの権限を一時的に昇格させるには、グラフィカルモードで実行し、Dr.Web for Linuxウィンドウ内の 該当するボタン を使用します（操作を正しく完了させるために権限の昇格が必要な場合のみ使用することができるようになります）。Dr.Web for Linuxを グラフィカルモード で起動、またはコマンドライン管理 ツール をスーパーユーザー権限で起動させるには、ユーザーの変更を可能にする `su` コマンドか、別のユーザーとしてコマンドを実行することを可能にする `sudo` を使用できます。

Scannerは4 GBを超えるサイズのファイルをスキャンすることができません（そのようなファイルをスキャンしようとするとファイルサイズが大きすぎることを示すエラーメッセージ *"File is too large"* が表示されます）。

動作モード

Dr.Web for Linuxはスタンドアローンモード、または *集中管理サーバー* によって管理される *アンチウイルスネットワーク* の一部として動作できます。*集中管理モード* で動作させるために、追加のソフトウェアをインストールする必要も、Dr.Web for Linuxを再インストール／アンインストールする必要もありません。

- *スタンドアローンモード* では、保護されるコンピューターはアンチウイルスネットワークに接続されず、その動作はローカルで管理されます。このモードでは、設定およびライセンスキーファイルはローカルディスク上に置かれ、Dr.Web for Linuxのコントロールはすべて保護されるコンピューターで行われます。Doctor Web更新サーバーからウイルスデータベースの更新を受け取ります。
- *集中管理モード* では、コンピューターの保護は集中管理サーバーによって管理されます。このモードでは、Dr.Web for Linuxの一部の機能や設定が、アンチウイルスネットワークに対して適用される一般的な（企業の）アンチウイルス保護ポリシーに応じて変更される場合があります。集中管理モードでの動作に使用するライセンス キーファイル は集中管理サーバーから受け取ります。ローカルコンピューター上に保存されたキーファイルがある場合、それらは使用できません。ウイルスイベントに関する統計はDr.Web for Linuxの動作に関する情報と一緒に集中管理サーバーに送信されます。ウイルスデータベースの更新もまた、集中管理サーバーから受け取ります。
- *モバイルモード* では、Dr.Web for LinuxはDoctor Web更新サーバーから更新を受け取りますが、製品の動作はローカル設定で管理されます。使用されるキーファイルは集中管理サーバーから受け取ります。

Dr.Web for Linuxが集中管理モードまたはモバイルモードで動作している場合、次のオプションはブロックされます。

1. ライセンスマネージャー内でのライセンスキーファイルの削除
2. 手動での更新プロセスの開始と更新設定の変更
3. ファイルシステムスキャンのパラメータ設定

Dr.Web for Linuxが集中管理下で実行されている場合、SpIDer Guard設定とSpIDer Guardによる検査を有効／無効にするオプションは、サーバーで指定されたパーミッションに応じて許可されます。

集中管理モードでは、設定されたスケジュール によるファイルのスキャンを使用することはできません。

ユーザーによるオンデマンドでのスキャンの実行が集中管理サーバーで禁止されている場合、Dr.Web for Linuxウィンドウの スキャン開始ページ および **Scanner** ボタンは無効になります。

集中管理のコンセプト

Doctor Webの集中管理ソリューションはクライアント–サーバーモデルを使用します（下図参照）。

ワークステーションとサーバーは *ローカルにインストールされたアンチウイルスコンポーネント*（以下「Dr.Web for Linux」）によって保護されます。これらコンポーネントはリモートコンピューターのアンチウイルス保護を提供し、ワークステーションと集中管理サーバーとの接続を可能にします。

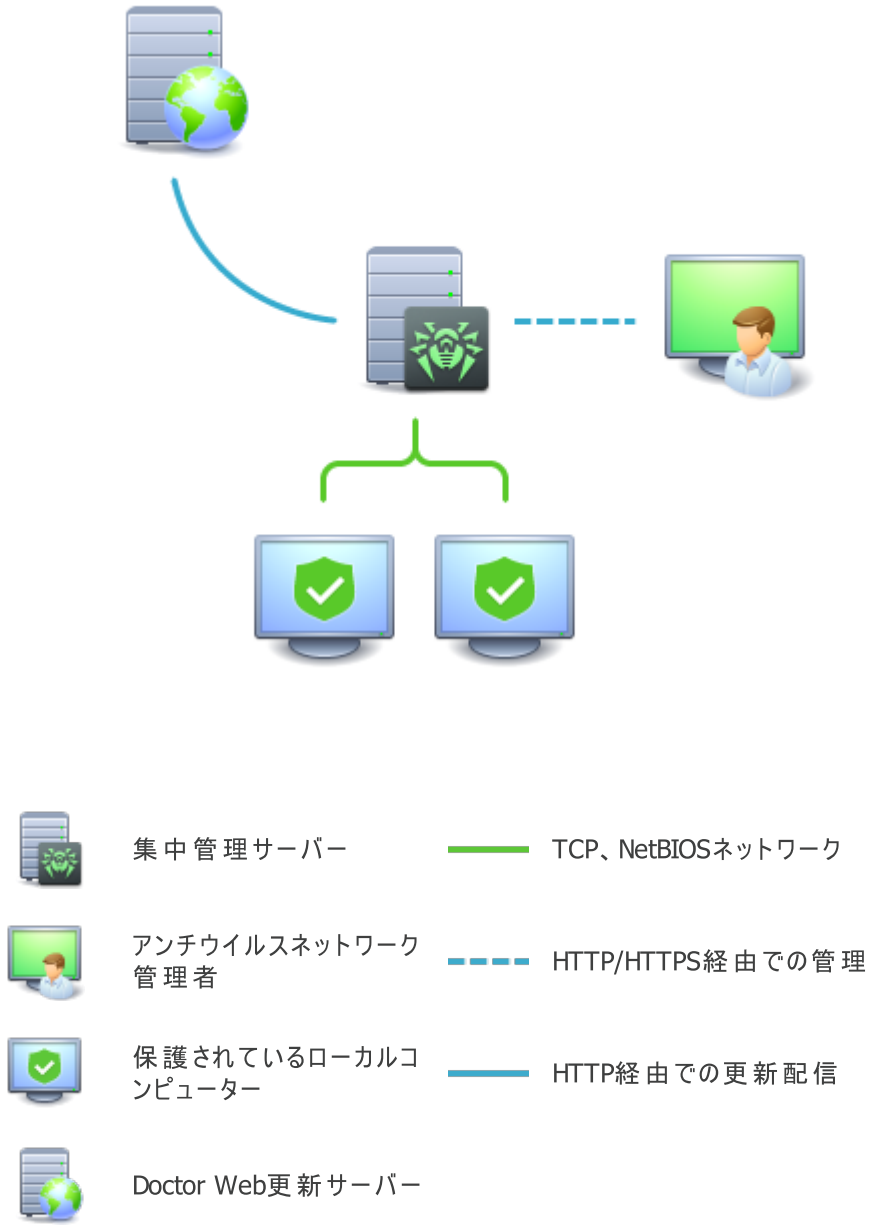

図 1. アンチウイルスネットワークの論理的構造

ローカルコンピューターの更新と設定は *集中管理サーバー* から行われます。アンチウイルスネットワーク内の一連の指示やデータ、統計も集中管理サーバーを経由します。保護するコンピューターと集中管理サーバー間のトラフィック量はかなり大きくなる場合があります。そこで、トラフィックを圧縮するオプションを提供しています。機密データの漏洩やコンピューター上にダウンロードされたソフトウェアの置き換えを防ぐため、暗号化もサポートされています。

必要なすべての更新がDoctor Web更新サーバーから集中管理サーバーにダウンロードされます。

ローカルアンチウイルスコンポーネントは、アンチウイルスネットワーク管理者より受け取ったコマンドに応じて集中管理サーバーから設定・管理されます。管理者は集中管理サーバーとアンチウイルスネットワークのトポロジーを管理し（リモートコンピューターから集中管理サーバーへの接続を検証するなど）、必要に応じてローカルアンチウイルスコンポーネントの動作を設定します。

ローカルアンチウイルスコンポーネントは、他社のアンチウイルス製品、または集中管理モードでの動作をサポートしていない他のDr.Webアンチウイルスソリューション（Dr.Web for Linux バージョン5.0など）と互換性がありません。同一コンピューター上に2つのアンチウイルスプログラムをインストールすると、システムクラッシュや重要なデータの紛失を引き起こす場合があります。

集中管理モードでは、集中管理サーバーを使用してDr.Web for Linuxの動作レポートをエクスポート、保存することができます（HTML、CSV、PDF、XML形式で）。

アンチウイルスネットワークに接続する

Dr.Web for Linuxは、以下のいずれかの方法でアンチウイルスネットワークに接続できます。

- Dr.Web for Linuxグラフィカルインターフェース内 設定ウィンドウ の**Mode** タブ で
- コマンドライン管理ツール（`drweb-ctl`）の `esconnect` コマンド を使用して

製品をアンチウイルスネットワークから切断する

Dr.Web for Linuxは、以下のいずれかの方法でアンチウイルスネットワークから切断できます。

- Dr.Web for Linuxグラフィカルインターフェース内 設定ウィンドウ の**Mode** タブ で
- コマンドライン管理ツール（`drweb-ctl`）の `esdisconnect` コマンド を使用して

システム要件と互換性

このセクションの内容：

システム要件

Dr.Web for Linuxは、以下の要件を満たすコンピューターで使用できます。

コンポーネント	要件
プラットホーム	次のアーキテクチャとコマンドシステムのプロセッサがサポートされています。 • Intel/AMD: 32-bit (*IA-32, x86*); 64-bit (*x86-64, x64, amd64*) • ARM64 • E2K *(Elbrus)* • IBM POWER (*ppc64el*)
RAM空き容量	500 MB以上（1 GB以上を推奨）
ハードディスク空き容量	Dr.Web for Linuxディレクトリが保存されるボリュームに少なくとも2 GB
オペレーティングシステム	PAMおよび `glibc` ライブラリバージョン2.13以降、`systemd` 初期化システムバージョン209以降を使用するカーネルバージョン2.6.37以降のGNU/Linux サポートされているGNU/Linuxディストリビューションのリストは以下をご確認ください。
その他	次の有効なネットワーク接続： • 更新をダウンロードし、Dr.Web Cloudサービスにリクエストを送信（ユーザーが手動で承認した場合のみ）するためのインターネット接続 • 集中管理 モードで動作している場合は、ローカルネットワーク上の集中管理サーバーへの接続

SpIDer Gateを正しく動作させるため、以下のオプションを組み込んでOSカーネルを構築する必要があります。

- *CONFIG_NETLINK_DIAG*、*CONFIG_INET_TCP_DIAG*
- *CONFIG_NF_CONNTRACK_IPV4*、*CONFIG_NF_CONNTRACK_IPV6*
  CONFIG_NF_CONNTRACK_EVENTS
- *CONFIG_NETFILTER_NETLINK_QUEUE*
  CONFIG_NETFILTER_NETLINK_QUEUE_CT、*CONFIG_NETFILTER_XT_MARK*

必要なオプションの組み合わせは、使用するGNU/Linuxのディストリビューションキットによって異なります。

Dr.Web for Linuxを正しく動作させるために、以下のポートを開いてください。

目的	方向	ポート番号
更新を受け取るため	送信	80
Dr.Web Cloudサービスに接続するため	送信	2075（TCP、UDP） 3010（TCP） 3020（TCP） 3030（TCP） 3040（TCP）

Dr.Web for Linuxには、他のアンチウイルスソフトウェアプログラムとの互換性がありません。1台のコンピューター上に2つのアンチウイルスをインストールする際に発生する可能性のあるシステムエラーやデータ損失を回避するため、Dr.Web for Linuxをインストールする前に他のすべてのアンチウイルスプログラムをコンピューターからアンインストールしてください。

サポートされているOSディストリビューションのリスト

Dr.Web for Linuxは次のUNIXディストリビューションに対応しています。

プラットホーム	サポートされているGNU/Linuxのバージョン
x86_64	• ALT 8 SP • ALT Server 9、10 • ALT Workstation 9、10 • Astra Linux Common Edition（Orel）2.12 • Astra Linux Special Edition 1.5（累積パッチ20201201SE15）、1.6（累積パッチ20200722SE16）、1.7 • CentOS 7、8 • Debian 9、10、11、12 • Fedora 37、38 • GosLinux IC6 • Red Hat Enterprise Linux 7、8 • RED OS 7.2 MUROM、RED OS 7.3 MUROM

プラットホーム	サポートされているGNU/Linuxのバージョン
	• SUSE Linux Enterprise Server 12 SP3 • Ubuntu 18.04、20.04、22.04
x86	• ALT 8 SP • ALT Workstation 9、10 • CentOS 7 • Debian 10
ARM64	• ALT 8 SP • ALT Server 9、10 • ALT Workstation 9、10 • Astra Linux Special Edition (Novorossiysk) 4.7 • CentOS 7、8 • Debian 11、12 • Ubuntu 18.04
E2K	• ALT 8 SP • Astra Linux Special Edition（Leningrad）8.1（累積パッチ 20201201SE15） • Elbrus-D MCST 1.4 • GS CS Elbrus 8.32 TVGI.00311-28
ppc64el	• CentOS 8 • Ubuntu 20.04

ALT 8 SPおよびGosLinux 7.1では、強制アクセス制御はサポートされていません。

これらの要件を満たすその他のUNIXディストリビューションであっても、Dr.Web for Linuxとの完全な互換性は保証されていません。互換性の問題が発生した場合は、テクニカルサポート にお問い合わせください。

必要な追加のコンポーネントとパッケージ

- グラフィカルモードでのDr.Web for Linuxの動作を有効にし、インストールとアンインストールのためのプログラムをグラフィカルモードで起動するには、X Window Systemグラフィックシェルといずれかのウィンドウマネージャーが必要です。また、Ubuntu Unityデスクトップ環境で インジケータ を正しく動作させるために、追加のライブラリが必要となる場合があります（デフォルトでは、`libappindicator1` という名前のライブラリが必要です）。
- コマンドライン用に設計されたインストーラまたはアンインストーラをグラフィカルモードで起動するには、端末エミュレータ（xterm、xvtなど）が必要です。
- インストールまたはアンインストール中の権限昇格を有効にするには、次のいずれかのユーティリティが必要です：`su`、`sudo`、`gksu`、`gksudo`、`kdesu`、`kdesudo`。Dr.Web for Linuxを正しく動作させるには、OSでPAMが使用されている必要があります。

コマンドライン でDr.Web for Linuxを便利に操作するために、使用しているコマンドシェルでコマンドオートコンプリートの調整機能を有効にできます（無効になっている場合）。

追加のパッケージやコンポーネントのインストールに問題が発生した場合は、お使いのOSディストリビューションのマニュアルを参照してください。

OSのコンポーネントとの互換性

- デフォルトではSpIDer Guardはfanotifyシステムメカニズムを使用しますが、fanotifyが実装されていないOSや他の理由で使用できないOSでは、製品内にあらかじめ組み込まれた形で提供される特別な *LKMモジュール* を使用します。製品ディストリビューションには、上のすべてのGNU/Linuxシステム用のカーネルモジュールが含まれています。必要に応じて、バージョン2.6.x以降のGNU/Linuxカーネルを使用するOS向けに配布されるソースコードとは独立して カーネルモジュールをビルドする ことができます。
ARM64およびE2Kアーキテクチャでは、LKMでの動作はサポートされていません。

  GNU/Linux（LKMモジュール）経由でのSpIDer Guardの操作は、Xen ハイパーバイザー環境で起動されたオペレーティングシステムではサポートしていません。Xen環境でのOS操作中に、SpIDer Guardが使用しているLKMモジュールをロードしようとすると、OSカーネルの 致命的なエラー（いわゆる「*カーネルパニック*」エラー）が発生する可能性があります。

  SpIDer Guardは強化（パラノイド）モードで動作することができます。このモードでは、fanotifyを介してのみ、また、OSカーネルが有効な `CONFIG_FANOTIFY_ACCESS_PERMISSIONS` オプションで構築されている場合にのみ、まだスキャンされていないファイルへのアクセスをブロックします。

- SpIDer Gateはシステムにインストールされている他のファイアーウォールと競合する可能性があります。
  - ShorewallおよびSuseFirewall2との競合（SUSE Linux Enterprise Serverの場合）。これらのファイアーウォールとの競合が発生した場合は、コード `x109` が付いたSpIDer Gateのエラーメッセージが表示されます。この競合を解決する方法は、付録「既知のエラー」に 記載されて います。
  - FirewallD（Fedora、CentOS、Red Hat Enterprise Linux）との競合。これらのファイアーウォールとの競合が発生した場合は、コード `x102` が付いたSpIDer Gateのエラーメッセージが表示されます。この競合を解決する方法は、付録「既知のエラー」に 記載されて います。
- 使用しているOSに含まれるNetFilterのバージョンが *1.4.15以前* の場合、SpIDer Gateが正しく動作しない可能性があります。この問題は、NetFilterの内部エラーに関連しており、SpIDer Gateを無効にするとネットワーク接続が切断され、再確立できなくなります。この問題が発生した場合は、バージョン1.4.15以降のNetFilterを含むOSにアップグレードすることをおすすめします。問題を解決する方法は、セクション「既知のエラーの説明」に 記載されています。
- 通常の動作では、SpIDer Gateは、Webブラウザやメールクライアントを含む、ネットワークを使用するすべてのユーザーアプリケーションと互換性があります。安全な接続を正しくスキャンする には、安全な接続を使用するアプリケーション（Webブラウザやメールクライアントなど）の信頼できる証明書のリストにDr.Web for Linux の証明書を追加する必要があります。
- SpIDer Gateの動作を 変更（前回無効にしたモニターを有効にする、安全な接続のスキャンモードを変更する）した後は、IMAPプロトコルを使用してメールサーバーからメールを受信する *メールクライアントを再起動させる* 必要があります。

セキュリティサブシステムとの互換性

デフォルトでは、Dr.Web for LinuxはSELinuxをサポートしていません。また、Dr.Web for Linuxは、強制アクセスモデルを使用するGNU/Linuxシステム（たとえば、ユーザーとファイルに異なる特権レベルを付与するPARSEC強制アクセスサブシステムの備わったシステムなど）では機能が制限されたモードで動作します。

SELinuxを持つシステム（およびその他の強制アクセスモデルを使用するシステム）にDr.Web for Linuxをインストールする場合、Dr.Web for Linuxの全機能が動作するように、セキュリティサブシステムを設定する必要がある場合があります。詳細については、セキュリティサブシステムを設定する のセクションを参照してください。

ライセンス

Dr.Web for Linuxを使用する権限は、Doctor Webまたはそのパートナーから購入したライセンスによって付与されます。ユーザー権限を規定するライセンスパラメータは、製品のインストール時にユーザーが同意する使用許諾契約（https://license.drweb.com/agreement/ 参照）に従って設定されます。ライセンスには、ユーザーとベンダーに関する情報のほか、以下のような購入した製品の使用パラメータも含まれています。

- ユーザーに対してライセンスされたコンポーネントのリスト
- Dr.Web for Linuxライセンスの有効期間
- その他の制限（購入したDr.Web for Linuxを使用することのできるコンピューターの台数など）

製品をお試しになりたいユーザーは *試用期間* を有効にできます。試用期間を正しく有効化した場合、ユーザーには有効期間を通してDr.Web for Linuxの全機能を使用する権利が与えられます。

各Doctor Web製品ライセンスは、コンピューター上に保存される特別なファイルに関連したユニークなシリアル番号を持っています。このファイルは *ライセンスキーファイル* と呼ばれ、ライセンスのパラメータに従ってDr.Web for Linuxコンポーネントの動作を規定します。試用期間を有効にすると、*デモ* キーファイルと呼ばれる特別なキーファイルが自動的に生成されます。

コンピューター上でライセンスまたは試用期間が有効化されていない場合（試用期間のために購入したライセンスの有効期限が切れている場合を含む）、Dr.Web for Linuxのアンチウイルス機能はブロックされます。また、Dr.Webウイルスデータベースおよびコンポーネントの更新をDoctor Web更新サーバーからダウンロードすることはできません。ただし、企業またはインターネットサービスプロバイダーによって管理される アンチウイルスネットワーク の一部として集中管理サーバーに接続することで Dr.Web for Linuxを有効にできます。この場合、製品の動作と更新は集中管理サーバーによって管理されます。

インストールとアンインストール

このセクションでは、Dr.Web for Linuxバージョン11.1をインストールおよびアンインストールする方法について説明します。また、最新の更新を入手する方法や、Dr.Web for Linuxの以前のバージョンがすでにコンピューターにインストールされている場合に新しいバージョンにアップグレードする手順も記載されています。

さらに、Dr.Web for Linuxコンポーネントのカスタムインストールとアンインストール手順（Dr.Web for Linuxの動作中に生じたエラーの解決方法や、機能セットを限定してインストールする方法など）、Dr.Web for Linuxのインストールと動作に必要になる可能性がある高度なセキュリティサブシステムの設定（SELinuxなど）についてもご確認いただけます。

- Dr.Web for Linuxをインストールする
- Dr.Web for Linuxをアップグレードする
- Dr.Web for Linuxをアンインストールする
- セキュリティサブシステムを設定する
- 追加情報：
  - Dr.Web for Linuxファイルの場所
  - コンポーネントのカスタムインストールとアンインストール

これらの手順を実行するには、スーパーユーザー権限（*root* ユーザーの権限）が必要です。権限を昇格するには、`su` コマンド（カレントユーザーを変更する）または `sudo` コマンド（指定されたコマンドを別のユーザーの権限で実行する）を使用します。

Dr.Web for Linuxと、他社のアンチウイルス製品との互換性は *保証されていません*。1台のシステム上に2つのアンチウイルスがインストールされることで、*OSのエラーを引き起こし*、*重要なデータが失われる可能性があります*。Dr.Web for Linuxをインストールする前に、他社アンチウイルス製品をコンピューターから削除することが *強く推奨されます*。

コンピューター上に他のDr.Webアンチウイルス製品が ユニバーサルパッケージ（`.run`）から *すでにインストールされ* ていて、さらに別のDr.Webアンチウイルス製品（たとえば、ユニバーサルパッケージからDr.Web for UNIX File Serversをインストールしていて、そこに Dr.Web for Linuxをインストールするなど）をインストールする場合、インストールされている製品のバージョンがインストールする製品のバージョンと *同じ* であることを確認します。新しくインストールする製品のバージョンがインストールされている製品のものよりも新しい場合、インストール *前* に、インストールされている製品を新しくインストールする製品のバージョンまで 更新 する必要があります。

Dr.Web for Linuxをインストールする

Dr.Web for Linuxをインストールするには、以下の手順のいずれか1つを行います。

1. Doctor Webの公式サイトから、UNIXシステム向け ユニバーサルパッケージ が含まれたインストールファイルをダウンロードします。パッケージは、環境に応じて開始されるインストーラ(グラフィカルとコンソール)と共に提供されます。
2. Doctor Webの該当するパッケージリポジトリから ネイティブパッケージ をダウンロードします。

古いバージョンのパッケージマネージャー使用しているディストリビューション(ALT 8 SPなど)では、ユニバーサルパッケージ をインストールすることを推奨します。

Dr.Web for Linuxのインストールは指定された方法のいずれかを使用して実行します。ライセンスを有効にするか、キーファイルをインストールする必要があります。または、Dr.Web for Linuxを集中管理サーバーに接続することもできます。そのいずれかを行うまで、アンチウイルス保護は*無効の状態です*。

メッセージの受信にIMAPを使用しているメールクライアント(Mozilla Thunderbirdなど)がシステムで実行されている場合は、受信メッセージをスキャンできるようにするため、アンチウイルスのインストール後に再起動します。

上のいずれかの方法でDr.Web for Linuxをインストールした後、そのコンポーネントに対する修正や製品の新しいバージョンがリリースされた場合には、製品を アンインストール または 更新 できます。また、必要に応じ、インストールしたDr.Web for Linuxを正常に動作させるため、UNIX の セキュリティサブシステムを設定 することもできます。個々のコンポーネントの動作について問題が生じた場合は、インストールした Dr.Web for Linux をアンインストールすることなく、それらコンポーネントのカスタムインストールとアンインストール を実行できます。

ユニバーサルパッケージをインストールする

Dr.Web for Linuxは `drweb-<version>-av-linux-<platform>.run` という名前のインストールファイルとして提供されます。*<platfrom>* は製品が対象としているプラットフォーム(32ビットプラットフォームは`x86`、64ビットプラットフォームは`amd64`、`arm64`、`e2s`)です。例:

```
drweb-11.1-av-linux-amd64.run
```

インストールファイルの名前が *<file_name>*`.run` の形式で指定されます。

Dr.Web for Linuxのコンポーネントをインストールするには以下の手順を行ってください。

1. Doctor Web公式サイトからインストールファイルをダウンロードします。
2. それをコンピューターのハードディスクドライブの、任意のディレクトリに保存します(例:`/home/`*<username>*、*<username>* はカレントユーザーの名前)。
3. ファイルを保存したディレクトリに移動し、実行権限をコマンドで許可します。コマンドの例:

```
# chmod +x <file_name>.run
```

4. 以下のコマンドを使用してアーカイブを実行します。

```
# ./<file_name>.run
```

ファイルプロパティ（パーミッション）の変更とファイルの実行は、グラフィカルシェルの標準的なファイルマネージャーを使用することも可能です。

CSE モードで動作するバージョン1.6および1.7のAstra Linux SEにDr.Web for Linuxをインストールする場合、Doctor Webのパブリックキーが信頼できるキーのリストに含まれていないことが原因でインストーラが起動しない場合があります。この場合は、CSEモードを設定して（CSEモードでの起動を設定する（Astra Linux SE 1.6および1.7）を参照）、インストーラを再起動してください。

まず、これによりアーカイブの整合性チェックが実行され、その後、アーカイブファイルが一時ディレクトリに展開されてインストールプログラムが開始されます。ユーザーがroot権限を持っていない場合、インストールプログラムはルートパスワード（sudo が使用されます）を要求することで権限の昇格を試みます。失敗した場合、インストールプロセスは中止されます。

ファイルシステム内の一時ディレクトリへのパスに、展開されたファイルのための十分な空き容量がない場合、インストールプロセスは中止され、該当するメッセージが表示されます。この場合、TMPDIR システム環境変数の値を変更して、十分な空き容量のあるディレクトリを示すようにしてください。その後、再度インストールを実行します。または、--target オプションを使用することもできます（詳細は コンポーネントのカスタムインストールとアンインストール セクションを参照）。

ディストリビューションパッケージが起動される環境によって、以下のインストールプログラムのうちいずれか1つが実行されます。

- グラフィカルモード 用のインストールウィザード
- コマンドラインモード 用のインストーラ

グラフィカルモード用のインストールウィザードの実行に失敗した場合、コマンドラインモード用のインストーラが自動的に実行されます。

5. インストーラの指示に従ってください。

次のコマンドを実行することで、インストールプログラムをサイレントモードで実行することもできます。

```
# ./<file_name>.run -- --non-interactive
```

この場合、インストールプログラムはサイレントモードで起動され、ユーザーインターフェイスなしで動作します（コマンドラインモードで表示されるダイアログも表示されません）。

注意事項

- このオプションを使用することで、Dr.Web使用許諾契約に *同意* したものとみなされます。使用許諾契約 /opt/drweb.com/share/doc/LICENSE ファイルに置かれています。ファイルの拡張子は使用許諾契約に使用されている言語を示しています。LICENSE ファイルが拡張子を持っていない場合、Dr.Web使用許諾契約は英語で書かれています。使用許諾契約に *同意しない* 場合、インストール後にDr.Web for Linuxを アンインストール する必要があります。
- インストールプログラムをサイレントモードで実行するには管理者（root）権限が必要です。権限を昇格するには、su または sudo コマンドを使用できます。

お使いのUNIXディストリビューションにSELinuxセキュリティサブシステムが備わっている場合、それによってインストールプロセスが妨げられる可能性があります。そのような状況が発生した場合は、以下のコマンドを入力することで、SELinuxを一時的に *Permissive* モードに設定します。

```
# setenforce 0
```

次に、インストーラを再起動させます。インストールが完了した後、製品コンポーネントの正常な動作を可能にするようSELinux セキュリティポリシー を設定します。

インストールプロセスが完了すると、展開されたインストールファイルがすべて削除されます。

ダウンロードした *<file_name>*.run ファイル（そこからインストールが行われたファイル）を保存しておくことが推奨されます。これにより、Dr.Web for Linuxやコンポーネントの再インストールを行う際にそれらのバージョンを更新する必要がなくなります。

インストールの完了後、デスクトップグラフィックシェルの **アプリケーション** メニュー上に **Dr.Web** アイテムが表示されます。このアイテムには以下の2つのアイテムが含まれています。

- **Dr.Web for Linux** - Dr.Web for Linuxを グラフィカルモード で開始します。
- **Remove Dr.Web components** - コンポーネントを アンインストール します。

ユーザーが再度ログインした後、通知領域内にプログラム インジケータ が自動的に表示されます。

Dr.Web for Linuxを正しく動作させるために、システム要件と互換性 セクションで指定されているインストールパッケージをインストールする必要がある場合があります（たとえば、64ビットプラットフォーム上にインストールされた32ビットアプリケーションのサポートを可能にするライブラリ、通知領域内にプログラム インジケータ を正常に表示させるためのライブラリ libappindicator1 など）。

グラフィカルモードでインストールする

インストールプログラムは起動時に、Dr.Web for Linuxの動作にエラーを発生させる、または動作を不可能にするような問題がないかどうかをチェックします。そのような問題が発見された場合、該当するメッセージが画面上に表示され、問題がリストアップされます。**Exit** をクリックすることでインストールをキャンセルし、問題を解決してください。この場合、後ほどインストールプログラムを 再起動 させる必要があります（必要なライブラリ がインストールされた後で、またはSELinuxを一時的に 無効にした 後で、など）。ただし、Dr.Web for Linuxのインストールをキャンセルしないことを選択することもできます。その場合は、**Continue** をクリックします。このボタンをクリックした後、プロセスが開始され、インストールウィザードのウィンドウが表示されます。この場合、インストールが完了した後で、またDr.Web for Linuxの動作に エラー が発生した場合には、問題を解決する必要があります。

グラフィカルモード用のインストールプログラムが起動した後、インストールウィザードのウィンドウが表示されます。

図 2. インストールウィザードのウェルカムページ

コンピューターにDr.Web for Linuxをインストールするには、以下の手順を行います。

1. Doctor Webの使用許諾契約をお読みになるには、インストールマスターの開始ページ上にある該当するリンクをクリックします。インストールされるコンポーネントの使用許諾契約と、著作権情報が記載されたページが開きます。

   必要に応じ、使用許諾契約と著作権情報を印刷できます（システムにプリンターがインストールされ、設定されている場合）。その場合は、使用許諾契約のページの該当するタブを開き、**Print** ボタンをクリックします。

   ページを閉じるには **OK** をクリックします。

2. セットアップがファイルのコピーを開始する前に、インストール後に Dr.Web for Linuxを自動的にDr.Web Cloudに接続するように設定できます。その場合は、該当するオプションを有効にしてください（ウィザードを開始すると、オプションはデフォルトで有効になります）。Dr.Web for LinuxがDr.Web Cloudを使用しないようにする場合は、チェックボックスのチェックを外してください。必要に応じ、プログラムの 設定 内で、いつでもDr.Web for LinuxをDr.Web Cloudに接続できます。

3. インストールを続けるには、**Install** をクリックします。それにより、Doctor Webの使用許諾契約に同意したものとみなされます。Dr.Web for Linuxをインストールしない場合は、**Cancel** をクリックます。このボタンをクリックすると、インストールウィザードが終了します。

4. インストール開始後、プログレスバーを表示するページが開きます。インストール中のログを見るには **Details** をクリックします。

5. プログラムファイルがコピーされ、システム設定の必要な調整が行われた後、インストール結果を表示する最後のページが開きます。

6. インストールウィザードを終了するには **OK** をクリックします。お使いのデスクトップ環境がこの機能の使用をサポートしている場合、インストールの最後のステップで、Dr.Web for Linuxを グラフィカルモード で起動するよう促されます。インストール後に製品を起動させるには、**Run Dr.Web for Linux now** にチェックを入れ、**OK** をクリックします。

インストールがエラーによって失敗した場合、インストールウィザードの最後のページに該当するメッセージが表示されます。この場合、**OK** をクリックしてインストールウィザードを終了してください。その後、エラーの原因を取り除き、インストール手順を再度開始します。

コマンドラインからインストールする

コマンドライン用のインストールプログラムが起動したら、画面上にコマンドプロンプトが表示されます。

1. インストールを開始するには、「Do you want to continue?（続けますか？）」に対して *Yes* または *Y* を入力してください。インストーラを終了するには *No* または *N* を入力します。この場合、インストールはキャンセルされます。
2. その後、画面上に表示されるDoctor Webの使用許諾契約をお読みください。テキストを1行進めるには ENTER キーを、次の画面へ進むには スペース キーを押します。テキストを1行戻る、または前のページに戻るオプションはありません。
3. 使用許諾契約をお読みになった後、規約に同意するよう促すプロンプトが表示されます。同意するには *Yes* または *Y* を、同意しない場合は *No* または *N* を入力します。後者の場合、インストーラは自動的に終了します。
4. 使用許諾契約に同意した後、Dr.Web for Linuxコンポーネントのインストールが自動的に開始されます。インストールの実行中には、インストールされたコンポーネントのリストを含む、インストールプロセス（インストールログ）に関する情報が画面に表示されます。
5. インストールが正常に完了すると、インストーラは自動的に終了します。エラーが発生した場合は、エラーに関する詳細が含まれたメッセージが表示され、インストーラは終了します。
6. インストールしたDr.Web for Linuxの使用を開始するには、製品を いずれかの方法 で起動してください。

インストールがエラーによって失敗した場合、エラーの原因となった問題を解決し、インストール手順を再度開始してください。

リポジトリからインストールする

Dr.Web for Linuxのネイティブパッケージは、https://repo.drweb.com のDr.Web公式リポジトリにあります。OSのパッケージマネージャーが使用するリストにDr.Webリポジトリを追加すると、OSのリポジトリから他のさまざまな製品をインストールするのと同様に、ネイティブパッケージから製品をインストールすることができるようになります。必要な依存関係は自動的に解決されます。また、この場合、OSパッケージマネージャーによる、接続されたリポジトリからインストールされたすべてのDr.Webコンポーネントの検出がサポートされています。検出されたすべての更新のインストールの提案もサポートされています。

Dr.Webリポジトリにアクセスするには、インターネットアクセスが必要です。

以下に記載するすべてのコマンド（リポジトリ追加、電子署名キーのインポート、パッケージのインストールとアンインストールに使用されるコマンド）は管理者権限で実行する必要があります（*root* ユーザーによって）。権限を昇格するには、`su` コマンド（カレントユーザーを変更する）または `sudo` コマンド（指定されたコマンドを別のユーザーの権限で実行する）を使用します。

以下のOS（パッケージマネージャ）の手順を参照してください。

- Debian、Mint、Ubuntu（apt）
- ALT Linux、PCLinuxOS（apt-rpm）
- Mageia、OpenMandriva Lx（urpmi）
- Red Hat Enterprise Linux、Fedora、CentOS（yum、dnf）
- SUSE Linux（zypper）

Debian、Mint、Ubuntu（apt）

1. これらOS用のリポジトリはDoctor Webによって電子署名されています。リポジトリにアクセスするには、以下のコマンドを実行することで、デジタル署名キーをインポートし、パッケージマネージャーストレージに追加します。

```
# apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys
8C42FC58D8752769
```

2.リポジトリを追加するには、`/etc/apt/sources.list` ファイルに以下のラインを追加します。

```
deb https://repo.drweb.com/drweb/debian 11.1 non-free
```

1および2の手順は、特別なDEBパッケージをリポジトリからダウンロード、インストールすることでも実行できます。
パッケージは次のリンクからダウンロードします：https://repo.drweb.com/drweb/drweb-repo11.1.deb

3. リポジトリから Dr.Web for Linuxをインストールするには、以下のコマンドを使用します。

```
#apt-get update
# apt-get install drweb-workstations
```

代わりのパッケージマネージャー（Synapticまたはaptitudeなどを使用して製品をインストールすることもできます。パッケージの競合が発生した場合は、それを解決するためにaptitudeなどの代わりのマネージャーを使用することが推奨されます。

ALT Linux、PCLinuxOS（apt-rpm）

1.リポジトリを追加するには、`/etc/apt/sources.list` ファイルに以下のラインを追加します。

```
rpm https://repo.drweb.com/drweb/altlinux 11.1/<arch> drweb
```

<arch> には、パケットアーキテクチャを指定します：

- 32-bitバージョンの場合：`i386`
- AMD64アーキテクチャの場合：`x86_64`
- ARM64アーキテクチャの場合：`aarch64`
- E2Kアーキテクチャの場合：`e2s`

2. リポジトリからDr.Web for Linuxをインストールするには、以下のコマンドを使用します。

```
#apt-get update
# apt-get install drweb-workstations
```

代わりのパッケージマネージャー（Synapticまたはaptitudeなどを使用して製品をインストールすることもできます。

Mageia、OpenMandriva Lx（urpmi）

1.以下のコマンドを使用してリポジトリを接続します。

```
# urpmi.addmedia drweb https://repo.drweb.com/drweb/linux/11.1/<arch>/
```

<arch> には、パケットアーキテクチャを指定します：

- 32-bitバージョンの場合：`i386`
- 64-bitバージョンの場合： `x86_64`

2. リポジトリからDr.Web for Linuxをインストールするには、以下のコマンドを使用します。

```
# urpmi drweb-workstations
```

代わりのパッケージマネージャー（rpmdrake など）を使用して製品をインストールすることもできます。

Red Hat Enterprise Linux、Fedora、CentOS（yum、dnf）

1. 以下のコンテンツが含まれた `drweb.repo` ファイルを `/etc/yum.repos.d` ディレクトリに追加します。

```
[drweb]
name=DrWeb - 11.1
baseurl=https://repo.drweb.com/drweb/linux/11.1/$basearch/
gpgcheck=1
enabled=1
gpgkey=https://repo.drweb.com/drweb/drweb.key
```

`echo` などのコマンドを使用して上のコンテンツをファイルにロギングし、出力をリダイレクトする場合は、`$` 記号をエスケープする必要があります（`\$`）。

1の手順は、特別なRPMパッケージをリポジトリからダウンロード、インストールすることでも実行できます。
パッケージは次のリンクからダウンロードします：https://repo.drweb.com/drweb/drweb-repo11.1.rpm

2. リポジトリからDr.Web for Linuxをインストールするには、以下のコマンドを使用します。

```
# yum install drweb-workstations
```

Fedora のバージョン22以降では、マネージャー `yum` の代わりに `dnf` を使用することが推奨されます。例：

```
# dnf install drweb-workstations
```

代わりのパッケージマネージャー（PackageKit または Yumex など）を使用して製品をインストールすることもできます。

SUSE Linux（zypper）

1. リポジトを追加するには、以下のコマンドを使用します。

```
# zypper ar https://repo.drweb.com/drweb/linux/11.1/\$basearch/ drweb
```

2. リポジトリからDr.Web for Linuxをインストールするには、以下のコマンドを使用します。

```
# zypper refresh
# zypper install drweb-workstations
```

代わりのパッケージマネージャー（YaSTなど）を使用して製品をインストールすることもできます。

Dr.Web for Linuxをアップグレードする

Dr.Web for Linuxには2つの更新モードがあります。

1. 現在の製品バージョンに対してリリースされたパッケージやコンポーネントの更新を入手する。通常、このような更新ではエラー修正やコンポーネント機能の軽微な改良が行われています。
2. 新しいバージョンにアップグレードする。このアップグレードオプションは、お使いのDr.Web for Linuxの新しいバージョンをDoctor Webがリリースした場合に使用します。この場合、新しい機能が追加されています。

最新のアップデートを入手する

このセクションの内容:

オンラインでアップデートする

該当するセクション に記載されている方法を使用してDr.Web for Linuxをインストールすると、パッケージマネージャーは自動的にDr.Webパッケージリポジトリに接続します。

- インストールが ユニバーサルパッケージ（ファイル `.run`）から実行され、システムでDEBパッケージが使用されている場合（たとえば、Debian、Mint、UbuntuなどのOS）、Dr.Web パッケージの動作には、それぞれのバージョンのパッケージマネージャー `zypper` が使用されます。これはDr.Web for Linuxのインストール時に自動的にインストールされます。

  このマネージャーが含まれる更新されたDr.Webパッケージを入手してインストールするには、*<opt_dir>*`/bin` ディレクトリ（GNU/Linux - `/opt/drweb.com/bin`）へ行き、次のコマンドを実行します。

  ```
  # ./zypper refresh
  # ./zypper update
  ```

- それ以外の場合は、お使いのOSで使用されているパッケージマネージャーの更新コマンドを使用します。例:
  - Red Hat Enterprise Linux とCentOSでは、`yum` コマンドを使用します。
  - Fedora では、`yum` または `dnf` コマンドを使用します。
  - SUSE Linux では、`zypper` コマンドを使用します。
  - Mageia と OpenMandriva Lx では、`urpmi` コマンドを使用します。
  - Alt Linux、PCLinuxOS、Debian、Mint、Ubuntu では、`apt-get` コマンドを使用します。

また、お使いのOS用に開発された別のパッケージマネージャーを使用することもできます。必要に応じて、使用しているパッケージマネージャーのマニュアルを参照してください。

新しいDr.Web for Linuxバージョンがリリースされた場合、コンポーネントが含まれたパッケージは、Dr.Webリポジトリの新しい製品バージョンに該当するセクションに置かれます。この場合、更新の際にパッケージマネージャーを新しいDr.Webリポジトリセクションに切り替える必要があります（新しいバージョンにアップグレードする 参照）。

オフラインでアップデートする

インターネット接続がブロックまたは制限されている安全性の高い環境では、オフラインでウイルスデータベースを更新することが可能です。インターネットに接続されているコンピューターに更新をダウンロードし、USBドライブまたはローカルネットワーク共有にコピーしてから、別のコンピューター（インターネットに接続されていない）にインストールする必要があります。

更新手順は、コマンドラインから実行する必要があります。

更新を取得するには

1. インターネットに接続されているコンピューターで次のコマンドを実行します。

```
$ drweb-ctl update --Path <a path to a directory to store updates>
```

2. ダウンロードした更新をUSBドライブまたはローカルネットワーク共有にコピーします。

3. 更新するコンピューターにリムーバブルドライブまたはローカルネットワーク共有をマウントします。USBドライブを使用した場合は、次のコマンドを実行します。

```
# mkdir /mnt/usb
# mount <a path to the device> /mnt/usb
```

4. 次のコマンドで更新を適用します。

```
$ drweb-ctl update --From /mnt/usb
```

新しいバージョンにアップグレードする

注意事項

以前のバージョンのDr.Web for Linuxをバージョン11.1にアップグレードする手順がサポートされています。お使いのDr.Web for Linuxのバージョンは、インストール時に使用したものと同じ方法でアップグレードする必要があります。

- 現在のバージョンがリポジトリからインストールされている場合、アップグレードではリポジトリからプログラムパッケージを更新する必要があります。
- 現在のバージョンがユニバーサルパッケージからインストールされている場合、製品をアップグレードするには、新しいバージョンのDr.Web for Linuxを含んでいる別のユニバーサルパッケージをインストールする必要があります。

お使いのバージョンの製品がどのようにインストールされているかを確認するには、Dr.Web for Linux実行可能ディレクトリにプログラムアンインストールスクリプト `remove.sh` が含まれているかどうかを確認します。含まれている場合、現在のバージョンはユニバーサルパッケージからインストールされています。それ以外の場合は、リポジトリからインストールされています。

インストールした方法で製品を更新できない場合は、現在のバージョンのDr.Web for Linuxをアンインストールし、いずれかの方法で新しいバージョンをインストールしてください。以前のバージョンのDr.Web for Linuxのインストールとアンインストールの手順は、バージョン11.1の現行のマニュアルに記載されている インストール と アンインストール の手順と同じです。詳細については、現在のバージョンのDr.Web for Linuxのユーザーマニュアルを参照してください。

Dr.Web for Linuxのバージョン6.0.2からバージョン11.1へのアップグレードは、古いDr.Web for Linuxをアンインストールしてバージョン11.1を インストール することで *のみ* 実行できます。

現在のバージョンのDr.Web for Linuxが 集中管理 モードで動作している場合は、集中管理サーバーのアドレスを記録することをお勧めします。たとえば、バージョン6.0.2以降のDr.Web for Linuxのアドレスを確認するには、次のコマンドを使用できます。

```
$ drweb-ctl appinfo
```

このコマンドの結果、次のような行が出力されます。

```
ESAgent; <PID>; RUNNING 1; Connected <address>, on-line
```

<address> の部分を保存します（`tcp://` *<IP address>* `:` *<port>* のようになっています。例：`tcp://10.20.30.40:1234`）。さらに、サーバー証明書ファイルを保存することをお勧めします。

現在使用している接続パラメータを調べる際に問題が発生した場合は、お使いの製品バージョンの管理者マニュアルをご確認いただくか、アンチウイルスネットワーク管理者までお問い合わせください。

バージョン11.1にアップグレードする

アップグレードのためにユニバーサルパッケージをインストールする

インストールファイル からDr.Web for Linux 11.1をインストールします。インストール中に、ディストリビューションからインストールされている古いバージョンを自動的にアンインストールするように求められます。

リポジトリからアップグレードする

Doctor Webのリポジトリからインストールされた現在のバージョンのDr.Web for Linuxをアップグレードするには、必要なパッケージのタイプに応じて、次のいずれかの操作を行います。

- **RPMパッケージ（yum）を使用する場合**：
  1. リポジトリを変更します（現在のバージョンのパッケージリポジトリから11.1パッケージリポジトリへ）。

リポジトリの名前は リポジトリからインストールする セクションにあります。詳しいリポジトリの変更方法については、お使いのOSディストリビューションのヘルプガイドを参照してください。

  2. 以下のコマンドを使用して新しいバージョンをインストールします。

```
# yum update
```

または、マネージャー `dnf` を使用している場合（バージョン22以前の Fedora など）は、以下のコマンドを使用します。

```
# dnf update
```

パッケージの更新中にエラーが発生した場合は、Dr.Web for Linuxをアンインストールし、再度インストールします。必要に応じて、リポジトリからインストールしたDr.Web for Linuxをアンインストールする および リポジトリからインストールする（使用しているOSとパッケージマネージャーの項目）を参照してください。

- **DEBパッケージ（apt-get）を使用する場合**：
  1. リポジトリを変更します（現在のバージョンのパッケージリポジトリから11.1パッケージリポジトリへ）。
  2. 以下のコマンドを入力し、Dr.Web for Linuxパッケージをアップグレードします。

```
#apt-get update
# apt-get dist-upgrade
```

Ubuntu 14.04（64ビット版）OSの場合、`apt-get dist-upgrade` コマンドが失敗する場合がありますので注意してください。この場合は、aptitudeパッケージマネージャーを使用してください（製品をアップグレードするには、aptitude `dist-upgrade` コマンドを実行します）。

キーファイルの転送

選択したDr.Web for Linuxのアップグレード方法に関係なく、ライセンス キーファイル は自動的にデフォルトの場所にインストールされます。

キーファイルの自動インストール中に問題が発生した場合は、手動でインストールする ことができます。Dr.Web for Linuxバージョン9.0以前のライセンスキーファイルは、`/etc/opt/drweb.com` ディレクトリにあります。有効なライセンスキーファイルを失くしてしまった場合は、Doctor Web テクニカルサポート までご連絡ください。

集中管理サーバーとの接続を復元する

アップグレードされたバージョンが集中管理サーバーに接続されている場合、可能であれば、Dr.Web for Linuxをアップグレードした後に接続が自動的に再確立されます。そうでない場合は、次のいずれかの方法を使用して（保存されたアドレスとサーバーのパブリックキーファイルを指定する必要があります）、アップグレードされたバージョンをアンチウイルスネットワークに接続できます。

- Dr.Web for Linux 設定ウィンドウ の **Mode** タブ でチェックボックスにチェックを入れます。
- 次の コマンド を使用してください。

```
$ drweb-ctl esconnect <address> --Certificate <path to the server certificate file>
```

接続処理に問題が発生した場合は、アンチウイルスネットワークの管理者までお問い合わせください。

アップグレード手順における注意点

- リポジトリから製品をアップグレードする際に現在のバージョンのDr.Web for Linuxがアクティブである場合、古いバージョンのプロセスは、アップグレード完了後にユーザーがシステムからログオフするまで実行されたままになります。Dr.Web for Linuxがグラフィカルモードで動作している場合は、通知領域に古いバージョンの アイコン が表示されることがあります。
- Dr.Web for Linuxをアップグレードした後、SpIDer Gateの 設定 がデフォルトにリセットされることがあります。
- メッセージの受信にIMAPを使用しているメールクライアント（Mozilla Thunderbird など）がシステムで実行されている場合は、 受信メッセージをスキャンできるようにするため、アンチウイルスのインストール後に再起動してください。

バージョン6.0.2以前をアップグレードする

バージョン6.0.2以前のDr.Web for Linuxからバージョン11.1へのアップグレードは、古いDr.Web for Linuxをアンインストールしてバージョン11.1をインストールすることでのみ実行できます。古いバージョンをアンインストールする方法の詳細については、Dr.Web for Linuxのインストールされているバージョンのユーザーマニュアルを参照してください。

キーファイルの転送

Dr.Web for Linuxをアップグレードした後、ライセンス キーファイル は自動ではデフォルトの場所にインストールされませんが、手動で インストールできます。Dr.Web for Linuxバージョン6.0.2以前のライセンスキーファイルは、`/home/<user>/.drweb` ディレクトリにあります（隠しディレクトリです）。有効なライセンスキーファイルを失くしてしまった場合は、Doctor Web テクニカルサポート までご連絡ください。

Dr.Web for Linux 11.1はバージョン9.0以前のDr.Web for Linuxをサポートしていません。古いバージョンの隔離にファイルが残っている場合は、これらのファイルを手動で取り出すか、削除できます。Dr.Web for Linux 6.0.2（およびそれ以前のバージョン）では、次のディレクトリが隔離として使用されます。

- `/var/drweb/infected` - システム隔離
- `/home/<user>/.drweb/quarantine` - ユーザー隔離（*<user>* はユーザー名）

隔離されたファイルの処理を簡易化するために、アップグレードを開始する前に古いバージョンのDr.Web for Linuxを使用して隔離を修正することをお勧めします。

Dr.Web for Linuxをアンインストールする

Dr.Web for Linux をインストールした方法に応じて、次のいずれかの方法で製品をアンインストールできます。

1. アンインストーラーを起動 して、(環境に応じてグラフィカルモードまたはコマンドラインモードで) ユニバーサルパッケージをアンインストールする。
2. パッケージシステムマネージャー経由でDoctor Webリポジトリからインストールした パッケージをアンインストール する。

ユニバーサルパッケージをアンインストールする

UNIXシステム向けの ユニバーサルパッケージ からインストールしたDr.Web for Linuxは、デスクトップ環境のアプリケーションメニューまたはコマンドラインからアンインストールできます。

アンインストールツールはDr.Web for Linuxだけでなく、コンピューターにインストールされている *他のすべての* Dr.Web製品をアンインストールすることに注意してください。

Dr.Web for Linux以外の他のDr.Web製品がコンピューターにインストールされている状況で Dr.Web for Linuxのみをアンインストールするには、自動削除ツールを実行する代わりに コンポーネントのカスタムインストールとアンインストール の手順を使用します。

アプリケーションメニューからDr.Web for Linuxをアンインストールする

アプリケーションメニューで **Dr.Web** をクリックし、**Remove Dr.Web components** を選択します。アンインストールツールが起動します。

コマンドラインからDr.Web for Linuxをアンインストールする

Dr.Web for Linuxをアンインストールするには、次のコマンドを使用して、`/opt/drweb.com/bin` ディレクトリにある `remove.sh` スクリプトを実行します。

```
# /opt/drweb.com/bin/remove.sh
```

アンインストールツールが(環境に応じて、グラフィカルモードまたはコマンドラインモードのいずれかで) 実行されます。

アンインストールツールをコマンドラインから直接実行するには、次のコマンドを使用します。

```
# /opt/drweb.com/bin/uninst.sh
```

Dr.Web for Linuxのアンインストールについては、以下のセクションに記載されています。

- グラフィカルモードで製品をアンインストールする
- コマンドラインからアンインストールする

次のコマンドを実行することで、アンインストールツールをサイレントモードで起動することもできます。

```
# /opt/drweb.com/bin/remove.sh --non-interactive
```

この場合、アンインストールツールはサイレントモードで実行され、ユーザーインターフェースなしで動作します（コマンドラインモードのプログラムダイアログを含む）。アンインストールツールをサイレントモードで実行するにはroot権限が必要です。権限を昇格するには、`su` または `sudo` コマンドを使用できます。

ALT 8 SPでは、ユニバーサルパッケージのアンインストール時に次のようなメッセージが表示されることがあります。

```
/etc/init.d/drweb-configd: No such or directory
```

これらのメッセージは、システムの機能に影響を与えるものではありません。アンインストールは正しく行われています。

グラフィカルモードで製品をアンインストールする

アンインストールウィザードがグラフィカルモードで起動すると、ウェルカムページが開きます。

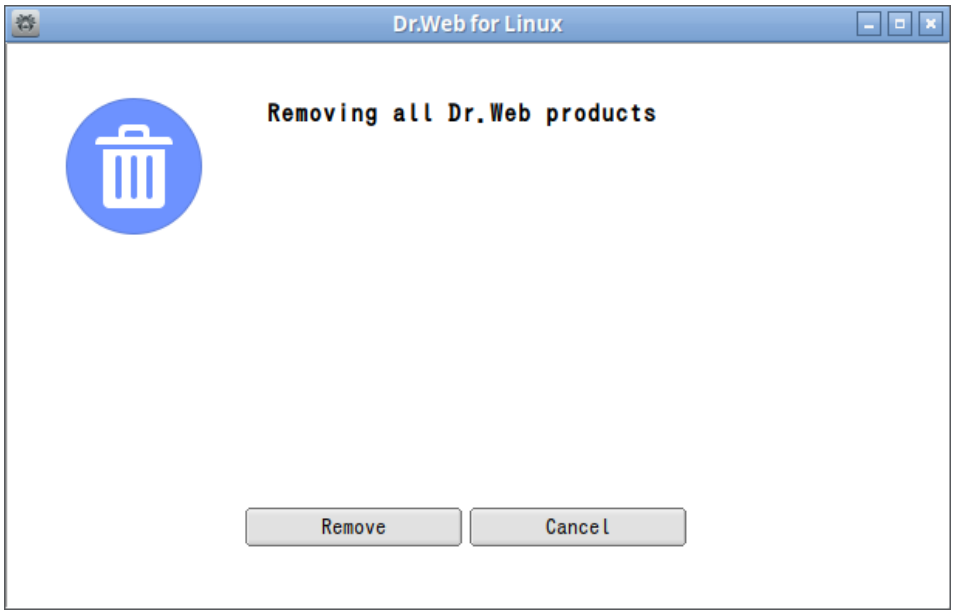

図 3. ウェルカムページ

1. Dr.Web製品をアンインストールするには、**削除** をクリックしてください。アンインストールウィザードを閉じて、Dr.Web製品のアンインストールを中止するには、**Cancel** をクリックします。
2. アンインストール開始後、プログレスバーを表示するページが開きます。ログを見るには **Details** をクリックします。
3. Dr.Web for Linuxファイルが正常にアンインストールされ、必要なすべての変更がシステム設定に加えられた後、アンインストールウィザードは操作が正常に完了したことを通知する最後のページを表示します。
4. アンインストールウィザードを閉じるには **OK** をクリックします。

コマンドラインからアンインストールする

コマンドラインベースの削除プログラムが起動すると、製品をアンインストールするメッセージがコマンドラインに表示されます。

1. アンインストールを開始するには、「Do you want to continue?（続けますか？）」に対して *Yes* または *Y* を入力してください。アンインストーラを終了するには *No* または *N* を入力します。この場合、Dr.Web製品のアンインストールはキャンセルされます。

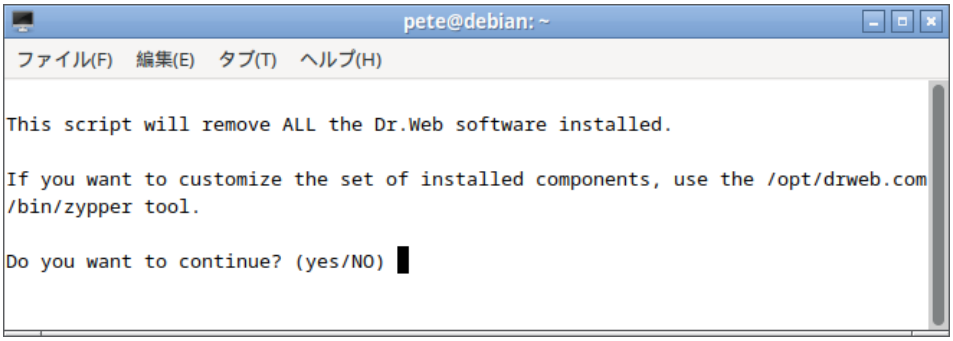

図4.製品のアンインストールの確認

2. アンインストールを確定すると、インストールされているすべてのDr.Web製品の自動アンインストールが開始されます。この手順の間、アンインストールのプロセスに関する情報が画面に表示され、アンインストールログに記録されます。
3. プロセスが完了すると、アンインストールプログラムは自動的に終了します。

リポジトリからインストールしたDr.Web for Linuxをアンインストールする

以下に記載される、パッケージのアンインストールに使用されるコマンドはスーパーユーザー（root）権限で実行する必要があります。権限を昇格するには、`su` コマンド（カレントユーザーを変更する）または `sudo` コマンド（指定されたコマンドを別のユーザーの権限で実行する）を使用します。

以下のOS（パッケージマネージャ）の手順を参照してください。

- Debian、Mint、Ubuntu（apt）
- ALT Linux、PCLinuxOS（apt-rpm）
- Mageia、OpenMandriva Lx（urpmi）
- Red Hat Enterprise Linux、Fedora、CentOS（yum、dnf）
- SUSE Linux（zypper）

Debian、Mint、Ubuntu（apt）

Dr.Web for Linuxのルートメタパッケージをアンインストールするには、以下のコマンドを入力します。

```
# apt-get remove drweb-workstations
```

ルートのメタパッケージをすべての依存ファイルと一緒にアンインストールする場合は、以下のコマンドを実行します。

```
# apt-get remove drweb-workstations --autoremove
```

不要になったすべてのパッケージを自動的にアンインストールするには、以下のコマンドを入力します。

```
# apt-get autoremove
```

`apt-get` コマンドを使用したアンインストールには以下の特徴がありますので注意してください。

1. 最初のコマンドは `drweb-workstations` パッケージのみをアンインストールします。依存関係を解決するために自動的にインストールできる他のすべてのパッケージはシステムに残ります。
2. 2番目のコマンドは、名前が「`drweb`」（Dr.Web製品名の標準的接頭辞）で始まるすべてのパッケージをアンインストールします。このコマンドは、Dr.Web for Linuxのパッケージだけでなく、この接頭辞を持つパッケージをすべてアンインストールします。
3. 3番目のコマンドは、他のパッケージの依存関係を解決するために自動的にインストールされた、不要になった（削除などにより）パッケージをすべてアンインストールします。このコマンドは、Dr.Web for Linuxのパッケージだけでなく、使用されていないすべてのパッケージをアンインストールします。

代わりのパッケージマネージャー（Synaptic または aptitude など）を使用してDr.Web for Linuxパッケージをアンインストールすることもできます。

ALT Linux、PCLinuxOS（apt-rpm）

この場合、Dr.Web for Linuxのアンインストールは、DebianおよびUbuntu上でのアンインストールと同じです（上記 参照）。

代わりのパッケージマネージャー（Synaptic または aptitude など）を使用してDr.Web for Linuxパッケージをアンインストールすることもできます。

ALT 8 SPでは、ユニバーサルパッケージのアンインストール時に次のようなメッセージが表示されることがあります。

```
/etc/init.d/drweb-configd: No such or directory
```

これらのメッセージは、システムの機能に影響を与えるものではありません。アンインストールは正しく行われています。

Mageia、OpenMandriva Lx（urpme）

Dr.Web for Linuxをアンインストールするには、以下のコマンドを入力します。

```
# urpme drweb-workstations
```

不要になったすべてのパッケージを自動的にアンインストールするには、以下のコマンドを入力します。

```
# urpme --auto-orphans drweb-workstations
```

`urpme` コマンドを使用したアンインストールには以下の特徴がありますので注意してください。

1. 最初のコマンドは `drweb-workstations` パッケージのみをアンインストールします。依存関係を解決するために自動的にインストールできる他のすべてのパッケージはシステムに残ります。
2. 2番目のコマンドは、ルートメタパッケージ `drweb-workstations` 、および他のパッケージの依存関係を解決するために自動的にインストールされた、不要になった（アンインストールなどにより）パッケージをすべてアンインストールします。このコマンドは、Dr.Web for Linuxのパッケージだけでなく、使用されていないすべてのパッケージをアンインストールします。

代わりのパッケージマネージャー（rpmdrake など）を使用してDr.Web for Linuxパッケージをアンインストールすることもできます。

Red Hat Enterprise Linux、Fedora、CentOS（yum、dnf）

インストールされているすべてのDr.Webパッケージをアンインストールするには、以下のコマンドを入力します（一部のOSでは、「*」記号をエスケープする必要があります：「*」）。

```
# yum remove drweb*
```

Fedora のバージョン22以降では、マネージャー `yum` の代わりに `dnf` を使用することが推奨されます。例:

```
# dnf remove drweb*
```

`yum`（`dnf`）コマンドを使用したアンインストールには以下の特徴がありますので注意してください。

このコマンドは、名前が「`drweb`」（Dr.Web製品名の標準的接頭辞）で始まるすべてのパッケージをアンインストールします。このコマンドは、Dr.Web for Linuxのパッケージだけでなく、この接頭辞を持つパッケージをすべて削除します。

代わりのパッケージマネージャー（PackageKit または Yumex など）を使用してDr.Web for Linuxパッケージをアンインストールすることもできます。

SUSE Linux（zypper）

Dr.Web for Linuxをアンインストールするには、以下のコマンドを入力します。

```
# zypper remove drweb-workstations
```

インストールされているすべてのDr.Webパッケージをアンインストールするには、以下のコマンドを入力します（一部のOSでは、「`*`」記号をエスケープする必要があります:「`\*`」）。

```
# zypper remove drweb*
```

`zypper` コマンドを使用したアンインストールには以下の特徴がありますので注意してください。

1. 最初のコマンドは `drweb-workstations` パッケージのみをアンインストールします。依存関係を解決するために自動的にインストールできる他のすべてのパッケージはシステムに残ります。
2. 2番目のコマンドは、名前が「`drweb`」（Dr.Web製品名の標準的接頭辞）で始まるすべてのパッケージをアンインストールします。このコマンドは、Dr.Web for Linuxのパッケージだけでなく、この接頭辞を持つパッケージをすべてアンインストールします。

代わりのパッケージマネージャー（YaST など）を使用してDr.Web for Linuxパッケージをアンインストールすることもできます。

追加情報

Dr.Web for Linuxファイルの場所

Dr.Web for Linuxのインストール後、その構成ファイルはファイルシステムの `/opt`、`/etc`、`/var` ディレクトリに置かれます。

ディレクトリの構造

ディレクトリ	コンテンツ
`/opt/drweb.com`	コンポーネントの実行ファイルとDr.Web for Linuxの動作に必要な主なライブラリ
`/etc/opt/drweb.com`	コンポーネント設定ファイル（デフォルト）とスタンドアローン モード でのDr.Web for Linuxの動作用ライセンスキーファイル
`/var/opt/drweb.com`	ウイルスデータベース、スキャンエンジン、一時ファイル、Dr.Web for Linuxの動作に必要な追加のライブラリ

コンポーネントのカスタムインストールとアンインストール

必要に応じ、該当するそれぞれの パッケージ をインストール／アンインストールすることで、特定のコンポーネントのみをインストール／アンインストールできます。コンポーネントのカスタムインストールとアンインストールは、製品をインストールした際と同じ方法で実行する必要があります。

コンポーネントを再インストールするには、まず初めにそのコンポーネントをアンインストールし、その後再度インストールしてください。

Dr.Web for Linuxコンポーネントのインストールとアンインストール:

- リポジトリからインストールする
- ユニバーサルパッケージからインストールする

1. リポジトリからインストールされたDr.Web for Linuxコンポーネントのインストールとアンインストール

Dr.Web for Linuxをリポジトリからインストールした場合、コンポーネントのカスタムインストール／アンインストールには、お使いのOSで使用されているパッケージマネージャーのコマンドを使用します。以下はその例です:

1. CentOS上にインストールされているDr.Web for LinuxからSpIDer Gate（`drweb-gated` パッケージ）をアンインストールするには、次のコマンドを使用します。

```
# yum remove drweb-gated
```

2. Ubuntu上にインストールされているDr.Web for LinuxにSpIDer Gate（`drweb-gated` パッケージ）を追加でインストールするには、以下のコマンドを使用します。

```
# apt-get install drweb-gated
```

必要に応じて、お使いのOSで使用されているパッケージマネージャーのヘルプを参照してください。

2.ユニバーサルパッケージからインストールされたDr.Web for Linuxコンポーネントのインストールとアンインストール

Dr.Web for Linuxがユニバーサルパッケージからインストールされていて、コンポーネントのパッケージを追加でインストールまたは再インストールする場合、Dr.Web for Linuxのインストール元のインストールファイル（`.run` 拡張子の付いたファイル）が必要です。このファイルを保存していない場合は、Doctor Webの公式サイトからダウンロードしてください。

インストールファイルを展開する

.runファイルを実行する際は、以下のコマンドラインパラメータを指定することもできます。

`--noexec` - インストールプロセスを開始せずに、Dr.Web for Linuxのインストールファイルを展開します。ファイルは `TMPDIR` 環境変数で指定されたディレクトリに置かれます（通常は `/tmp`）。

`--keep` - インストール完了後にDr.Web for Linuxのインストールファイルとインストールログを自動的に削除しません。

`--target` *<directory>* - Dr.Web for Linuxのインストールファイルを、指定されたディレクトリ *<directory>* に展開します。

インストールファイルについて指定することのできるコマンドラインパラメータの全リストを見るには、以下のコマンドを入力してください。

```
$ ./<file_name>.run --help
```

Dr.Web for Linuxコンポーネントのカスタムインストールでは、展開されたDr.Web for Linuxインストールファイルを使用する必要があります。それらのファイルを含んだディレクトリがない場合は、以下のコマンドを入力します。

```
$ ./<file_name>.run --noexec --target <directory>
```

コマンドが実行された後、展開されたDr.Web for Linuxファイルを含む *<directory>* ディレクトリ内に、*<file_name>* という名前のネストされたディレクトリが現れます。

コンポーネントのカスタムインストール

RUNインストールファイルには、Dr.Web for Linuxのすべてのコンポーネントのパッケージ（RPMフォーマットで）とサポートファイルが含まれています。各コンポーネントのパッケージファイルは以下の構造を持っています。

```
<component_name>_<version>~linux_<platform>.rpm
```

<version> は製品リリースのバージョンと時間が含まれたストリングで、*<platfrom>* はDr.Web for Linuxが対象としているプラットフォームです。Dr.Web for Linuxのコンポーネントが含まれているパッケージの名前はすべて「drweb」プレフィックスで始まります。

`zypper` パッケージマネージャーはインストールキットでのパッケージのインストール時に有効になります。カスタムインストールでは、サービススクリプト `installpkg.sh` を使用します。その際、まずインストールパッケージのコンテンツをディレクトリに展開する必要があります。

パッケージをインストールするには、スーパーユーザー権限（*root* ユーザーの権限）が必要です。権限を昇格するには、`su` コマンド（カレントユーザーを変更する）または `sudo` コマンド（指定されたコマンドを別のユーザーの権限で実行する）を使用します。

コンポーネントパッケージのインストールまたは再インストールを開始するには、展開されたインストールキットのあるディレクトリに行き、コンソール経由で以下のコマンドを実行します（または、グラフィカルモードのターミナルエミュレーター経由）。

```
# ./scripts/installpkg.sh <package_name>
```

例:

```
# ./scripts/installpkg.sh drweb-gated
```

Dr.Web for Linux全体のインストールを開始する必要がある場合は、以下のコマンドを使用して自動インストールスクリプトを実行してください。

```
$ ./install.sh
```

その他、製品のルートメタパッケージを実行することで、すべてのDr.Web for Linuxパッケージをインストールできます（不足しているか、誤って削除してしまったコンポーネントをインストールするため）。

```
# ./scripts/installpkg.sh drweb-workstations
```

コンポーネントのカスタムアンインストール

お使いのOSがRPMフォーマットのパッケージを使用している場合、コンポーネントのカスタムアンインストールでは、OSのパッケージマネージャーの該当するアンインストールコマンドを使用します。

- Red Hat Enterprise LinuxとCentOSでは、`yum remove` *<package_name>* コマンドを使用します。
- Fedoraでは、`yum remove` *<package_name>* または `dnf remove` *<package_name>* コマンドを使用します。
- SUSE Linuxでは、`zypper remove` *<package_name>* コマンドを使用します。
- Mageiaと OpenMandriva Lxでは、`urpme` *<package_name>* コマンドを使用します。
- Alt LinuxとPCLinuxOSでは、`apt-get remove` *<package_name>* コマンドを使用します。

例（Red Hat Enterprise Linuxの場合）：

```
# yum remove drweb-gated
```

お使いのOSがDEBパッケージを使用している場合、カスタムアンインストールでは、Dr.Web for Linuxのインストール中に自動的にインストールされるパッケージマネージャー `zypper` を使用する必要があります。`/opt/drweb.com/bin` ディレクトリに行き、以下のコマンドを実行します。

```
# ./zypper rm <package_name>
```

例：

```
# ./zypper rm drweb-gated
```

Dr.Web for Linuxをアンインストールする必要がある場合は、以下のコマンドを入力して 自動削除 スクリプトを実行します。

```
# ./uninst.sh
```

コンポーネントを再インストールするには、まずそのコンポーネントをアンインストールし、その後、インストールキットからのカスタムインストールまたはフルインストールを実行することで再度インストールします。

セキュリティサブシステムを設定する

OSに強化セキュリティサブシステムSELinuxが実装されている場合や、PARSECなどの強制アクセス制御システム（UNIXで使用されていた従来の任意モデルではなく）が使用されている場合は、それらがデフォルト設定になっているとDr.Web for Linuxとの動作に問題が生じます。この場合、Dr.Web for Linuxが確実に正常に動作するよう、セキュリティサブシステムやDr.Web for Linuxの設定を変更する必要があります。

このセクションでは、Dr.Web for Linux正しく動作させるための次の設定について説明します。

- SELinuxセキュリティポリシーを設定する
- PARSEC強制アクセス制御システム（Astra Linux SE OS）の パーミッションを設定する
- CSEモードでの起動を設定する（クローズドソフトウェア環境）（OS Astra Linux SE 1.6および1.7）

> Dr.Web for Linuxに対するPARSEC強制アクセス制御システムの権限を設定することで、Dr.Web for Linuxのコンポーネントが、設定されたセキュリティポリシーの制限を回避し、異なる権限レベルを持ったファイルにアクセスすることが可能になります。

Dr.Web for Linux コンポーネントに対する PARSEC強制アクセス制御システムの権限を設定していない場合でも、Dr.Web for Linux の グラフィカル管理インターフェース を 自律的コピー モードを実行することでファイルのスキャンを開始できます。その場合、`drweb-gui` コマンド を `--Autonomous` パラメータで実行してください。また、コマンドライン からディレクトリのスキャンを開始することもできます。その場合は、コマンド呼び出し内で同じパラメータ（`--Autonomous`）を指定して `drweb-ctl` コマンド を実行します。この場合、スキャンセッションを開始したユーザーのものよりも低い特権レベルを必要とするファイルをスキャンすることが可能になります。このモードには以下の機能があります。

- Dr.Web for Linuxグラフィカルユーザーインターフェイスを自律コピーとして実行するには、有効な キーファイル が必要です。 集中管理 モードでの操作はサポートされていません（集中管理サーバーからエクスポートされた キーファイル をインストールするオプションを使用することができます）。この場合、Dr.Web for Linuxが集中管理サーバーに接続されている場合であっても、自律コピーモードで検出された脅威について集中管理サーバーには *通知されません*。
- 自律コピーの動作をサポートする全ての追加コンポーネントは、現在のユーザー下で起動され、そのセッション用に個別に生成された設定ファイルで動作します。
- 使用されるすべての一時ファイルとUNIXソケットは、自律的コピーの起動時に作成される固有の名前を持つディレクトリ内にのみ作成されます。一時ファイルのために、システムディレクトリ内に固有の一時ディレクトリが作成されます（このディレクトリへのパスは `TMPDIR` 環境変数内で取得できます）。
- グラフィカル管理インターフェースの自律コピーではSpIDer GuardとSpIDer Gateを *起動* することはできません。Scannerでサポートされている ファイルスキャン と隔離管理 の機能のみ利用することができます。
- 必要なすべてのパス（ウイルスデータベース、スキャンエンジン、サービスコンポーネントの実行ファイルへのパス）はデフォルトで指定されているか、特別な環境変数から取得できます。
- 同時に動作する自律コピーの数に制限はありません。
- 自律コピーがシャットダウンされると、一連のサービスコンポーネントも終了します。

SELinuxセキュリティポリシーを設定する

UNIXディストリビューションにSELinuxが搭載されている場合（*Security-Enhanced UNIX*）、Dr.Web for Linuxコンポーネントのインストール後にそれらを正常に動作させるには（スキャンエンジンの動作など）、SELinuxセキュリティポリシーを設定する必要がある場合があります。

1.ユニバーサルパッケージを使用したインストールの問題

SELinuxが有効になっている場合、Dr.Web for Linuxコンポーネントを動作させる *drweb* ユーザーの作成がブロックされることがあり、インストールファイル（`.run`）からのインストールは失敗する場合があります。

drweb ユーザーを作成できなかったためにファイル（`.run`）からのDr.Web for Linuxのインストールに失敗した場合は、getenforce コマンドで `SELinux` の動作モードをチェックしてください。コマンドは現在のスキャンモードを出力します。

- *Permissive* - 保護は有効ですが、許可方式が使用されています。セキュリティポリシーに違反する動作は拒否されませんが、動作に関する情報はログに記録されます。
- *Enforced* - 保護は有効で、制御方式が使用されています。セキュリティポリシーに違反する動作は拒否され、動作に関する情報はログに記録されます。
- *Disabled* - SELinuxはインストールされていますが、有効になっていません。

SELinuxが *Enforced* モードで動作している場合は *Permissive* モードに変更してください。その際、以下のコマンドを使用します。

```
# setenforce 0
```

このコマンドはSELinuxの *Permissive* モードを一時的に（次の再起動まで）有効にします。

> `setenforce` コマンドで有効にした動作モードに関係なく、OSの再起動後、SELinuxは設定内で指定された動作モードに戻りますので注意してください（SELinuxの設定ファイルは通常、`/etc/selinux` ディレクトリにあります）。

Dr.Web for Linuxが正常にインストールされた後、製品を起動させる前に *Enforced* モードを再度有効にしてください。その際、以下のコマンドを使用します。

```
# setenforce 1
```

2. Dr.Web for Linuxの動作に関する問題

SELinuxが有効になっている場合に、特定のDr.Web for Linuxコンポーネント（ScannerやSpIDer Guardによって使用される `drweb-se` や `drweb-filecheck` など）を起動できないことがあります。その場合、オブジェクトのスキャンとファイルシステムのモニタリングを使用できません。補助モジュールが起動しない場合、Dr.Web for Linuxのメインウィンドウにエラー *119* および *120* のメッセージが表示され、それらエラーに関する情報が `syslog` によって記録されます（通常、ログは `/var/log/` ディレクトリに置かれています）。

SELinuxセキュリティシステムによってアクセスが拒否された場合、そのようなイベントのログが記録されます。一般的に、システムで audit デーモンが使用されている場合、audit（監査）に関するログ

が /var/log/audit/audit.log ファイルに保存されます。それ以外の場合、ブロックされた動作に関するメッセージが一般的なログファイル(/var/log/messages または /var/log/syslog)に保存されます。

SELinuxにブロックされて補助モジュールが動作しない場合は、それらに対して特別なセキュリティポリシーを設定します。

一部のUNIXディストリビューションには以下のユーティリティが備わっていませんのでご注意ください。その場合、ユーティリティの追加パッケージをインストールする必要がある場合があります。

SELinuxセキュリティポリシーを設定する

1. SELinuxのポリシーソースコードの新しいファイルを作成します(.te ファイル)。このファイルは記載されているポリシーモジュールに関連した制限を規定するものです。このポリシーソースコードは以下のいずれかの方法で作成できます。
   1) audit2allow ユーティリティを使用して - 最もシンプルな方法です。ユーティリティはシステムログファイル内のアクセス拒否に関するメッセージからpermissiveルールを生成します。自動でメッセージを検索するよう設定するか、手動でログファイルへのパスを指定できます。

      この方法は、Dr.Web for Linuxのコンポーネントが SELinuxセキュリティポリシーに違反していて、それらのイベントが監査ログファイルに記録されている場合のみ使用できます。そうでない場合、そのようなイベントが起こるのを待つか、policygentool ユーティリティを使用して強制的にpermissiveポリシーを作成(下記参照)してください。

      

      audit2allow ユーティリティは policycoreutils-python パッケージ、policycoreutils-devel パッケージ(バージョンによってRedHat Enterprise Linux、CentOS、Fedora)、または python-sepolgen パッケージ(Debian、Ubuntu)のいずれかにあります。

      audit2allow の使用例:

      ```
      # grep drweb-se.real /var/log/audit/audit.log | audit2allow -M drweb-se
      ```

      この例では、drweb-se モジュールに対するアクセス拒否メッセージを見つけるために audit2allow ユーティリティが audit.log ファイル内で検索を実行します。

      ポリシーソースファイル drweb-se.te と、インストール可能な drweb-se.pp ポリシーモジュールの2つのファイルが作成されます。

      システム監査ログ内でセキュリティ違反イベントが見つからなかった場合、ユーティリティはエラーメッセージを返します。

      ほとんどの場合、audit2allow ユーティリティによって作成されたポリシーファイルを変更する必要はありません。したがって、手順4 の drweb-se.pp ポリシーモジュールのインストールに進むことを推奨します。audit2allow ユーティリティは semodule コマンドの呼び出しを出力します。出力をコマンドラインにコピーして実行すると、手順4 が完了します。Dr.Web for Linuxコンポーネント用に自動的に生成されたセキュリティポリシーを変更する場合のみ、手順2 に進みます。
   2) policygentool ユーティリティを使用する - この場合、設定するモジュール動作の名前と、実行ファイルへのフルパスを指定してください。

Red Hat Enterprise LinuxとCentOS向けの `selinux-policy` パッケージに含まれている `policygentool` ユーティリティは正常に機能しない場合があります。その場合は `audit2allow` ユーティリティを使用してください。

`policygentool` を使用したポリシー作成の例:

- `drweb-se`:

```
# policygentool drweb-se /opt/drweb.com/bin/drweb-se.real
```

- `drweb-filecheck`:

```
# policygentool drweb-filecheck /opt/drweb.com/bin/drweb-filecheck.real
```

いくつかの共通ドメイン特性を指定するよう促すプロンプトが表示されます。その後、ポリシーを決定する3つのファイル(*<module_name>.te*、*<module_name>.fc*、*<module_name>.if*)が各モジュールについて作成されます。

2. 必要に応じ、生成されたポリシーソースファイル *<module_name>.te* を編集し、その後、`checkmodule` ユーティリティを使用して、ローカルポリシーのこのソースファイルをバイナリ形式に変換(`.mod` ファイル)します。

コマンドを正常に実行するには、システムに `checkpolicy` パッケージがインストールされている必要があります。

使用例:

```
# checkmodule -M -m -o drweb-se.mod drweb-se.te
```

3. `semodule_package` ユーティリティを使用して、インストール用のポリシーモジュールを作成します(`.pp` ファイル)。

例:

```
# semodule_package -o drweb-se.pp -m drweb-se.mod
```

4. 作成されたポリシーモジュールをインストールするには、`semodule` ユーティリティを使用します。

例:

```
# semodule -i drweb-se.pp
```

SELinuxの動作と設定に関する詳細は、お使いのUNIXディストリビューションのマニュアルを参照してください。

PARSEC権限を設定する

PARSECセキュリティサブシステム(強制アクセス制御システム)の備わったOSでは、アプリケーションによるファイルへのアクセスはそれらが持つ権限のレベルによって異なります。そのため、SpIDer Guardは付与されている権限レベルで許可されるファイルアクセスイベントのみを監視することができます。

また、ユーザーが0以外の権限レベルで操作している場合、Dr.Web for Linux のグラフィカルインターフェースはSpIDer Guardならびにアンチウイルスサービスコンポーネントと連携できません（これらが異なる権限レベルで動作している場合）。統合された 隔離 へもアクセスできない場合があります。

OSでPARSEC が使用され、0以外の権限レベルで操作を実行しているユーザーアカウントが存在する場合は、コンポーネントが異なる権限レベルで実行されるようにDr.Web for Linuxをカスタマイズする必要があります。

このセクションでは、Dr.Web for Linux正しく動作させるためのPARSECの設定について説明します。

- 異なる複数の権限レベルで実行されるコンポーネントの連携を カスタマイズする
- ユーザー権限を使用し、Dr.Web for Linuxコンポーネントの 自動起動をカスタマイズする
- ファイルアクセスイベントを監視するよう SpIDer Guardを設定する

これらの手順を実行するには、スーパーユーザー権限（*root*ユーザーの権限）が必要です。権限を昇格するには、`su` コマンド（カレントユーザーを変更する）または `sudo` コマンド（指定されたコマンドを別のユーザーの権限で実行する）を使用します。

異なる複数の特権レベルで実行されるコンポーネントの連携をカスタマイズする

バージョン1.6のAstra Linux SEの場合：

システムファイル `/etc/parsec/privsock.conf` を修正し、Dr.Web for Linux設定デーモン（`drweb-configd`）が *privsock* メカニズムを使用することを承認します。`drweb-configd` は、すべてのアンチウイルスコンポーネント間の連携を担うDr.Web for Linuxのサービスコンポーネントです。*privsock* メカニズムは、必須コンテキストを使用して情報を処理するのではなく、アクセスサブジェクトの必須コンテキストで動作するプロセスと連携してシステムネットワークサービスを操作するためのものです。

1. いずれかのテキストエディターで `/etc/parsec/privsock.conf` ファイルを開きます。次の行を追加します。

```
/opt/drweb.com/bin/drweb-configd
/opt/drweb.com/bin/drweb-configd.real
```

2. ファイルを保存し、OSを再起動します。

バージョン1.5以前のAstra Linux SEの場合：

Dr.Web for Linux（`drweb-configd`）設定デーモン起動スクリプトを変更します。これを行うには、以下の手順に従ってください。

1. 権限レベル0を使用してシステムにログインします。
2. いずれかのテキストエディターで、`/etc/init.d/drweb-configd` スクリプトファイルを開きます。
3. このファイル内で `start_daemon()` の機能の定義を見つけ、以下のラインを置き換えます。

```
"$DAEMON" -d -p "$PIDFILE" >/dev/null 2>&1
```

次のラインと置き換えます。

```
execaps -c 0x100 -- "$DAEMON" -d -p "$PIDFILE" >/dev/null 2>&1
```

4. 一部のOS（Astra Linux SE 1.3など）では、PARSECサブシステムからのコンポーネントの起動依存の追加表示が必要になる場合があります。この場合は、ファイル内の文字列も変更する必要があります。

```
# Required-Start: $local_fs $network
```

この文字列を次のように変更します。

```
# Required-Start: $local_fs $network parsec
```

5. ファイルを保存し、OSを再起動します。

ユーザー権限でコンポーネントの自動起動をカスタマイズする

ユーザーが対話するDr.Web for Linuxコンポーネントをユーザー環境で使用できるようにするには（ユーザーが0以外の権限レベルで操作を実行している場合）、PAM設定を含むファイルを変更して、必要なDr.Web for Linuxコンポーネントがユーザーセッションの開始時に自動的に起動し、セッションの終了時に終了するようにする必要があります。このモジュール（Doctor Webによって設計された特別な `pam_drweb_session.so` PAMモジュール）は、`drweb-session` メディエーションコンポーネントを起動します。これは、ユーザー環境で実行されるコンポーネントのローカルコピーと、0レベルの権限で動作しOSの起動時に自動実行されるコンポーネントを接続します。

PAM設定を変更するには、Dr.Web for Linuxに含まれている `drweb-configure` 設定ユーティリティを使用することをお勧めします。または、必要な設定ファイルに手動で変更を加えることも可能です。

1.drweb-configureユーティリティを使用する

`drweb-configure` は、Dr.Web for Linuxの複雑なパラメータの設定を簡易化するために開発された特別な補助ユーティリティです。

1. 必要なDr.Web for Linuxコンポーネントが0以外の権限レベルで実行されている場合に、ユーザーの環境でそれらコンポーネントの自動起動を有効または無効にするには、次のコマンドを使用します。

```
$ sudo drweb-configure session <mode>
```

<mode> には次のいずれかの値を指定することができます。

- `enable` - ユーザーセッション中の、必要なコンポーネントの適切な権限での自動起動を有効にします。
- `disable` - ユーザーセッション中の、必要なコンポーネントの適切な権限での自動起動を無効にします（これにより、Dr.Web for Linux の一部の機能が使用できなくなります）。

2. システムを再起動させてください。

`drweb-configure` を使用したPAM設定の方法についてヘルプを参照するには、次のコマンドを使用します。

```
$ drweb-configure --help session
```

2.PAM設定を手動で変更する

pam_parsec_mac.so PAMを使用するAstra Linuxおよびその他のディストリビューションの場合

1. PAM設定を変更するには、pam_parsec_mac.so PAMモジュールを起動する /etc/pam.d ディレクトリ内のすべての設定ファイルを変更する必要があります。そのようなファイルのリストを取得するには、次のコマンドを実行します。

   ```
   # grep -R pam_parsec_mac.so /etc/pam.d
   ```

   リストにあるすべてのファイルに、次の *セッションタイプの* レコードを追加します。

   - *セッション* タイプの最初のレコードの前に:

   ```
   session optional pam_drweb_session.so type=close
   ```

   - *セッション* タイプの最後のレコードの後に:

   ```
   session optional pam_drweb_session.so type=open
   ```

2. 変更したファイルを保存します。
3. PAMモジュールを含むシステムディレクトリから pam_drweb_session.so ファイルへのシンボリックリンクを作成します。pam_drweb_session.so ファイルは、Dr.Web for Linuxライブラリディレクトリ(/opt/drweb.com/lib/)にあります。たとえば、64ビットオペレーティングシステムではモジュールへのパスは /opt/drweb.com/lib/x86_64-linux-gnu/pam/ です。
4. OSを再起動します。

pam_namespace.so PAMモジュールを使用するALT 8 SPおよびその他のディストリビューションの場合

1. PAM設定を変更するには、pam_namespace.so PAMモジュールを起動する /etc/pam.d ディレクトリ内のすべての設定ファイルを変更する必要があります。そのようなファイルのリストを取得するには、次のコマンドを実行します。

   ```
   # grep -R pam_namespace.so /etc/pam.d
   ```

2. 2. pam_parsec_mac.so PAMモジュールを使用するディストリビューションのレコードと同じ *セッション* タイプのレコード(上記参照)を各ファイルに追加します。

ファイルアクセスイベントを監視するようSpIDer Guardを設定する

SpIDer Guardファイルモニターが、あらゆるレベルのアクセス権限を持つファイルへのアクセス試行を検出することができるようにするには、SpIDer Guardの動作モードを *Fanotify* に切り替える必要があります。

SpIDer Guardを *Fanotify* 動作モードに切り替えるには、以下の コマンド を実行します。

```
# drweb-ctl cfset LinuxSpider.Mode Fanotify
```

追加の情報を取得するには、次のコマンドを使用します。

```
$ man drweb-spider
```

CSEモードでの起動を設定する（Astra Linux SE 1.6および1.7）

Astra Linux SEでは、特別な *クローズドソフトウェア環境*（CSE）モードをサポートしています。このモードでは、実行ファイルに開発者のデジタル署名がある場合のみアプリケーションを起動できます。OSの信頼済みキーのリストに開発者のパブリックキーを追加する必要があります。

デフォルトでは、Astra Linux SE用に提供されているDr.Web for LinuxコンポーネントはDoctor Webデジタル署名で署名されており、署名のパブリックキーはアプリケーションのインストール中に信頼済みキーのリストに自動的に追加されるため、Astra Linux SE 1.5以前のバージョンでCSEモードを有効にしていればDr.Web for Linuxは正常に起動します。

ただし、Astra Linux SE 1.6では署名メカニズムが変更されているため、Astra Linux SE 1.6および1.7のCSEモードでDr.Web for Linuxを起動するには、OSの設定が必要です。

Astra Linux SE 1.6および1.7でCSEモードでのDr.Web for Linuxの起動を設定する

1. `astra-digsig-oldkeys` パッケージがインストールされていない場合は、OSのインストールディスクを使用してインストールします。
2. Doctor Webのパブリックキーを、`/etc/digsig/keys/legacy/keys` のディレクトリに追加します（ディレクトリがない場合は作成します）。

   ```
   #
   cp /opt/drweb.com/share/doc/digsig.gost.gpg /etc/digsig/keys/legacy/keys
   ```

3. 次のコマンドを実行します。

   ```
   # update-initramfs -k all -u
   ```

4. OSを再起動します。

開始する

1. Dr.Web for Linuxを起動する
2. Dr.Web for Linuxを正しく動作させる
3. ファイル監視モードを設定する
4. 必要に応じて除外を設定する

製品の登録と有効化

このセクションの内容：

ライセンスを購入・登録する

ライセンス購入後、製品コンポーネントとウイルスデータベースの更新が Doctor Web 更新サーバーから定期的にダウンロードされます。また、購入した製品のインストール中や使用中に問題が発生した場合、Doctor Webまたはそのパートナーによって提供されるテクニカルサポートサービスをご利用いただけます。

Dr.Web製品の購入や製品のシリアル番号の入手は、パートナー（パートナーのリストは https://partners.drweb.com/ を参照）から、またはオンラインストア（https://estore.drweb.com/）で行うことができます。ライセンスのオプションに関する詳細については、Doctor Webの公式サイト（https://license.drweb.com/）を参照してください。

Dr.Web for Linuxの正規ユーザーであることを証明し、ウイルスデータベースの更新を含むDr.Web for Linuxの機能を有効化するためにライセンス登録が必要です。インストールが完了したら、製品を登録してライセンスの有効化を行うことをお勧めします。購入したライセンスは、以下のいずれかの方法で有効にできます。

Dr.Web for Linuxの有効化

ライセンスは以下のいずれかの方法で有効化することができます。

- ライセンスマネージャーに含まれた 登録ウィザード 経由で
- Doctor Web 公式サイト https://products.drweb.com/register/ で

ライセンスを有効化または更新するには、シリアル番号を入力する必要があります。シリアル番号はDr.Web for Linuxと一緒に提供されるか、オンラインでライセンスを購入または更新した際にメールで提供されます。

ライセンスを更新するには、登録したシリアル番号を入力するか、前回のライセンスキーファイルを提示してください。そうでない場合、新しいライセンスの期限が150日短縮されます。

複数のコンピューター上でDr.Web for Linuxを使用するための有効化されていない複数のライセンスを所有しており、Dr.Web for Linuxを1台のコンピューターでのみ使用したい場合は、そのように指定することができます。その場合、すべてのライセンスが統合され、ライセンス有効期限が自動的に延長されます。

試用期間

Dr.Webユーザーの方は1か月の試用期間を取得することができます。試用期間はライセンスマネージャーの登録ウィザードウィンドウ内で取得できます。個人データを入力する必要はありません。

ライセンスマネージャーの登録ウィザードは、初回のDr.Web for Linux起動時に開きます（通常、Dr.Web for Linuxのインストールが完了すると登録ウィザードが起動します）。現在のライセンスに関する情報が表示されたページで **新しいライセンスを取得** をクリックすることで、いつでもライセンスマネージャーから試用期間の登録または取得を開始できます。

シリアル番号を使用してライセンスを有効化する、またはデモライセンスをリクエストするには、有効なインターネット接続が必要です。

ライセンスマネージャー経由で試用期間またはライセンスを有効化した場合、キーファイル（ライセンスまたはデモ）はローカルコンピューター上の目的のディレクトリ内に自動的に生成されます。Webサイト上で登録を行った場合、キーファイルはメールで送信されます。このキーファイルを手動で インストール する必要があります。

登録ウィザードが使用できない場合（オペレーティングシステムにGUIがない場合など）、コマンドラインインタフェース `drweb-ctl` のライセンス管理用 コマンド を使用できます。これにより、登録されたライセンスのシリアル番号（メールで入手した試用期間のシリアル番号を含む）に対応するデモキーファイルまたはライセンスキーファイルを取得できます。`drweb-ctl` ユーティリティに関する詳細はユーザーマニュアルを参照してください。

Dr.Web for Linuxのユーザーマニュアルフルバージョンは以下の方法で入手可能です。

- Doctor Web 公式サイト https://download.drweb.com/doc/ で（インターネット接続が必要です）
- `/opt/drweb.com/share/doc` フォルダ内のPDFファイルとして（ファイル名のサフィックスは、マニュアルの言語を示しています）

キーファイルのインストール

製品の有効なライセンスに対応するキーファイルをお持ちの場合（キーファイルをメールで受け取った場合、またはDr.Web for Linuxを別のコンピューター上で使用する場合など）、そのキーファイルへのパスを指定することでDr.Web for Linuxを有効にできます。キーファイルへのパスを指定するには以下の方法があります。

- 登録手順の最初のステップで、ライセンスマネージャー 内で **その他の有効化の種類** をクリックし、キーファイルまたはキーが含まれたzipアーカイブへのパスを指定する。

- 手動で。この場合、以下の手順を行ってください。
  1. アーカイブの場合はキーファイルを展開します。
  2. キーファイルを `/etc/opt/drweb.com` ディレクトリにコピーし、必要に応じてファイル名を `drweb32.key` に変更します。
  3. 次の コマンド を実行します。

     ```
     # drweb-ctl reload
     ```

     すべての変更が適用されます。

また、次の コマンド を使用することもできます。

```
# drweb-ctl cfset Root.KeyPath <path to the key file>
```

この場合、キーファイルは `/etc/opt/drweb.com` ディレクトリにコピーされず、元の場所に残ります。

キーファイルが `/etc/opt/drweb.com` ディレクトリにコピーされない場合、ユーザーはファイルが破損や削除から確実に保護されているようにする必要があります。キーファイルが誤ってシステムから削除されてしまう可能性があるため（キーファイルのあるディレクトリが定期的にクリーンアップされる、など）、このインストール方法は推奨されません。キーファイルが失われた場合、新しいキーファイルをサポートに要請することができます。ただし、その回数には上限があります。

集中管理サーバーとの接続

インターネットサービスプロバイダーまたはネットワーク管理者によって、集中管理サーバーとの 接続設定ファイル が提供される場合、ファイルへのパスを指定することでDr.Web for Linuxを有効にできます。以下の手順を行ってください。

- 設定ウィンドウ内 で **Mode**タブ へ行き、**集中管理モードを有効にする** チェックボックスにチェックを入れます。表示されたメニューで *ファイルから読み込む* を選択し、接続設定ファイルへのパスを指定して **接続** をクリックします。

2回目以降の登録

キーファイルを紛失し、現在のライセンス期限が切れていない場合は、再度登録する必要があります。前回の登録時と同じ個人データを入力してください。メールアドレスは別のものを使用できます。その場合、キーファイルは新しく指定されたアドレスに送信されます。

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。

キーファイル

キーファイルは、Dr.Web for Linux の購入した ライセンス または有効化した試用期間に対応する、ローカルコンピューター上に保存される特別なファイルです。このファイルには提供されたライセンスまたは試用期間に関する情報が含まれ、また、このファイルに応じて使用権が規定されます。

キーファイルは `.key` 拡張子を持ち、以下の条件を満たす場合に有効です。

- ライセンス有効期間または試用期間が満了していない。
- 試用期間またはライセンスが、製品に必要なすべてのアンチウイルスコンポーネントに対応している。
- キーファイルの整合性が損なわれていないこと。

いずれかの条件が満たされていない場合、ライセンスキーファイルは無効になります。

Dr.Web for Linuxの動作中、キーファイルはデフォルトの `/etc/opt/drweb.com` ディレクトリ内に `drweb32.key` という名前で置かれている必要があります。

Dr.Web for Linuxのコンポーネントは、キーファイルが使用可能かつ有効であるかどうかを定期的に確認します。編集されることを防ぐため、キーファイルはデジタル署名されています。キーファイルを編集すると無効になります。誤って無効にしてしまうことを防ぐため、キーファイルをテキストエディタで開かないようにすることが推奨されます。

有効なキーファイル（ライセンスまたはデモ）が見つからない場合、またはライセンスの有効期限が切れている場合、有効なキーファイルがインストールされるまでアンチウイルスコンポーネントの動作はブロックされます。

ライセンスキーファイルは、有効期限が切れるまで保存しておくことが推奨されます。Dr.Web for Linuxを再インストールしたり別のコンピューターにインストールしたりする場合にライセンスキーファイルを使用できます。この場合、登録時に提供したものと同じ製品シリアル番号とお客様データを使用する必要があります。

通常、Dr.WebのキーファイルはZIPアーカイブでメールによって送信されます。キーファイルが含まれたアーカイブの名前は `drweb32.zip` または `agent.zip` になります（メールに *複数* のアーカイブが添付されている場合は `agent.zip` のみを使用してください）。アーカイブを展開せずに、登録ウィザード内でそこへのパスを指定できます。キーファイルをインストールする前に、適切なツールを使用してアーカイブを展開し、キーファイルをいずれかのディレクトリ（ホームディレクトリやUSBフラッシュドライブなど）に抽出します。

接続設定ファイル

接続設定ファイルはDr.Web for Linuxと 集中管理 サーバーとの接続を設定するパラメータが保存されている特別なファイルです。このファイルはアンチウイルスネットワークの管理者またはインターネットサービスプロバイダー（インターネットサービスプロバイダーが集中管理アンチウイルス保護サービスに対するサポートを提供している場合）によって提供されます。

Dr.Web for Linuxを集中管理サーバーに接続する際に、このファイルを使用して Dr.Web for Linuxを有効にできます（この場合、追加の ライセンス を購入せずにDr.Web for Linuxをスタンドアローンモードで使用することはできません）。

製品の動作確認

EICAR（*European Institute for Computer Anti-Virus Research*）テストによって、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確認できます。このテストは、インストールされたアンチウイルスツールのウイルス検出の動作を、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設計されています。

EICAR, テストは実際に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じようにユーザーに警告します。EICARテストファイルは、MS DOS/MS Windows向けの68バイトのCOMファイルです。実行されると、ターミナル画面またはコンソールエミュレータに次のラインを出力します。

```
EICAR-STANDARD-ANTIVIRUS-TEST-FILE!
```

EICAR テストファイルは、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*
```

上の文字列でファイルを作成すると、「ウイルス」として認識されるテストファイルができあがります。

Dr.Web for Linuxが正常に動作していれば、テストファイルはスキャンの種類に関係なくファイルシステムのスキャン中に検出され、検出された脅威についてユーザーに対して通知が行われます：EICAR Test File (NOT a Virus!)

EICARテストを使用したDr.Web for Linux動作の確認を、コマンドラインから実行する場合のコマンドの例：

```
$ tail /opt/drweb.com/share/doc/drweb-se/readme.eicar | grep X5O > testfile
&& drweb-ctl scan testfile && rm testfile
```

このコマンドは `/opt/drweb.com/share/doc/drweb-se/readme.eicar` ファイル（製品と一緒に提供）からEICARテストファイルの本体を表す文字列を抽出し、それをカレントディレクトリ内に作成された `testfile` という名前のファイルに書き込みます。そのファイルをスキャンし、その後ファイルを削除します。

上記のテストを行うには、カレントディレクトリへの書き込みアクセスが必要です。また、ディレクトリに `testfile` という名前のファイルが含まれていないことを確認してください（必要に応じ、コマンド内でファイル名を変更してください）。

テストウイルスが検出されると、以下のメッセージが表示されます。

```
<path to the current directory>/testfile - infected with EICAR Test File (NOT a
Virus!)
```

テスト中にエラーが発生した場合は、既知のエラー を参照してください。

SpIDer Guardが有効になっている場合、悪意のあるファイルはただちに削除または隔離できます（コンポーネントの設定によって異なります）。この場合、コマンド `rm` はファイルが見つからないことを通知します。これはモニターが通常モードで動作していることを意味します。

ファイル監視モード

概要

ファイルへのアクセスを制御するファイルシステムモニターSpIDer Guardでは、3つの監視モードを使用することができます。

- *通常*（デフォルトで設定されています）- SpIDer Guardはファイルアクセス（作成、開始、終了、実行）を監視し、ファイルスキャンを要求します。スキャン時に脅威が検出された場合は、脅威を駆除するためのアクションが適用されます。ファイルスキャンが終了するまで、アプリはファイルにアクセスすることができます。
- *実行ファイルの強化された制御* - SpIDer Guardは実行不可能と見なされるファイルを通常モードの場合と同様に監視します。実行可能と見なされるファイルへのアクセスは、ファイルスキャンが終了するまで試行時にブロックされます。

> 実行ファイルはPEフォーマットやELFフォーマットのバイナリファイルと、"#!"プリアンブルを含むテキストスクリプトファイルです。

- *「パラノイド」モード* - SpIDer Guardはファイルのスキャンが終了するまで、ファイルへのアクセスをそれらの試行時にブロックします。

Scannerはファイルスキャンの結果を特定の期間キャッシュに保存します。そのため、同じファイルに再度アクセスすると、キャッシュに情報がある場合ファイルは再スキャンされず、スキャン結果の代わりにキャッシュにあるデータが表示されます。パラノイド監視モードを使用するとファイルへのアクセス速度が大幅に低下します。

ファイル監視モードの切り替え

> SpIDer Guardが `FANOTIFY` モードで動作し、OSカーネルが `CONFIG_FANOTIFY_ACCESS_PERMISSIONS` オプションを有効にして構築されている場合にのみ、強化されたファイルの監視と事前ブロックを利用することができます。
>
> ---
>
> SpIDer Guardの監視モードの切り替えは、`drweb-ctl` ユーティリティの `cfset` コマンドを使用して実行されます。
>
> ---
>
> SpIDer Guardの監視モードを切り替えるには、管理者（root）特権が必要です。権限を取得するには、`su` コマンドを使用して別のユーザーに切り替えるか、`sudo` コマンドを使用して別のユーザーとして操作を実行します。

- SpIDer Guardを `FANOTIFY` モードに切り替えるには、以下のコマンドを実行します。

```
$ sudo drweb-ctl cfset LinuxSpider.Mode FANOTIFY
```

- 監視モードを切り替えるには、次のコマンドを使用してください。

```
$ sudo drweb-ctl cfset LinuxSpider.BlockBeforeScan <mode>
```

<mode> はブロックモードです。

- `Off` - アクセスはブロックされません。SpIDer Guardは通常の（ブロックしていない）監視モードで動作します。
- `Executables` - 実行ファイルへのアクセスがブロックされます。SpIDer Guardは実行ファイルの監視を強化します。
- `All` - すべてのファイルへのアクセスがブロックされます。SpIDer Guardはファイルを「パラノイド」モードで監視します。

- キャッシュ内に保存されるファイルスキャン結果の有効期限を変更するには、次のコマンドを使用します。

```
$ sudo drweb-ctl cfset FileCheck.RescanInterval <period>
```

<period> パラメータは、キャッシュに保存されているスキャン結果の有効期限を決定します。`0s` から `1m` までの値を指定することができます。1秒未満の値を指定した場合、遅延は発生せず、ファイルは要求時にスキャンされます。

Dr.Web for Linuxを開始する

ユーザーによるDr.Web for Linuxの操作は、管理用グラフィカルインターフェースを提供するコンポーネントを使用したグラフィカルモード、またはコマンドラインから行うことができます（グラフィカルモード用の端末エミュレータを使用した操作を含む）。

- Dr.Web for Linuxの管理用グラフィカルインターフェースを開始するには、アプリケーション で **Dr.Web for Linuxを選択するか、OSのコマンドラインに以下のコマンドを入力します。**

```
$ drweb-gui
```

この場合、デスクトップ環境を使用することができれば、Dr.Web for Linuxの管理用グラフィカルインターフェースが起動します。グラフィカルインターフェースの起動時にファイルのスキャンを実行する場合やインターフェースの 自律コピー を開始する場合は、パラメータ と共にこのコマンドを使用できます。

- Dr.Web for Linux動作の管理に関する詳細については コマンドラインからの操作 を参照してください。
- グラフィカルデスクトップ環境では、Dr.Web for Linuxによるスキャンをタスクバー（Ubuntu の **Unity Launcher** など）やグラフィックファイルマネージャー（Nautilus など）から開始できます。また、デスクトップの通知領域内にアプリケーションのステータスインジケータが表示され、そこからポップアップ通知が表示されるほか、アプリケーションメニューにアクセスできます。その他すべてのサービスコンポーネント同様、インジケータは自動的に起動し、その動作にはユーザーの操作を必要としません。詳細については、デスクトップ環境との統合 を参照してください。
- SpIDer Guardによる強化されたファイルモニタリングを有効にする方法については、SpIDer Guard を参照してください。

いずれの方法でDr.Web for Linuxをインストールした場合でも、すでに取得されている場合はインストール完了後にライセンスを有効にするかキーファイルをインストールする、またはDr.Web for Linuxを集中管理サーバーに接続する必要があります（製品の登録と有効化 参照）。そのいずれかを行うまで、*アンチウイルス保護は無効の状態です。*

メールクライアント（Mozilla Thunderbirdなど）がメールサーバーからメールを受信する際に使用されるIMAPメールプロトコルはセッションで動作します。したがって、SpIDer Gate モニター の動作を変更（前回無効にしたモニターを有効にする、安全な接続のスキャン モード を変更する）した後は、メールクライアントを再起動させる必要があります。これにより、SpIDer Gateは動作モードを変更した後も受信メールのスキャンを行うことが可能になります。

グラフィカルモードでの動作

このセクションの内容:

概要

デスクトップ環境でのDr.Web for Linuxの動作には、2つのコンポーネントが関与しています。

- 通知エージェント - デスクトップ環境でユーザーのセッションが開始されると自動的に起動されるコンポーネントです。このコンポーネントは、Dr.Web for Linuxの動作のイベントに関するポップアップ通知を表示します。また、システム通知領域にDr.Web for Linuxのステータスインジケータを表示するほか、通知エージェントを操作するためのメインメニューも表示します。
- グラフィカル管理インタフェース - グラフィカルデスクトップ環境で動作し、Dr.Web for Linuxの動作を管理するためのウィンドウインターフェースを提供するコンポーネントです。

通知エージェント

Dr.Web for Linuxの通知エージェントは、次のように設計されています。

1. Dr.Web for Linuxの ステータスインジケータ を表示させる
2. モニターと更新を管理し、グラフィカル管理インターフェースを起動させる
3. イベントに関するポップアップ通知を表示させる
4. 指定されたスケジュールに従ってスキャンを実行する

グラフィカル管理インターフェース

Dr.Web for Linuxグラフィカル管理インターフェースによって、以下のタスクを実行することができます。

1. ウイルスデータベースの状態(最新であるかどうか)とライセンスの有効期間を含む、Dr.Web for Linuxの動作に関するステータスを表示する
2. ファイルシステムモニターSpIDer Guardを 有効／無効 にする
3. ネットワーク接続モニターSpIDer Gateを 有効／無効 にする
4. オンデマンドでの ファイルのスキャン を開始する:
   - *クイックスキャン* は、システムファイルとクリティカルなシステムオブジェクトを検査します。
   - *フルスキャン* は、すべてのシステムファイルを検査します。
   - *カスタムスキャン* は、指定されたファイルとディレクトリ、または特殊なオブジェクト(ブートレコード、アクティブなプロセス)のみを検査します。

   スキャンするファイルを選択するには、スキャンを実行する前に対象となるディレクトリとファイルを指定するか、それらをファイルマネージャーのウィンドウからメインページ(以下参照)またはDr.Web for Linuxウィンドウの **Scanner** ページにマウスでドラッグ&ドロップしてください。

5. 駆除またはスキップされた脅威、および隔離されたオブジェクトを含む、現在の操作中にDr.Web for Linuxによって検出された すべての脅威を表示する
6. 削除や復元が可能な、隔離に移されたオブジェクトを表示する
7. Dr.Web for Linuxコンポーネントの動作パラメータの設定 。次のオプションがあります。
   - 検出された脅威に対してScannerおよびSpIDer Guardが適用するアクション（その種類に応じて）
   - Scannerによるスキャンおよびspider Guardによる管理の対象から除外するディレクトリとファイルのリスト
   - SpIDer Gateによって使用されるWebサイトのブラックリストとホワイトリスト、およびインターネットからダウンロードされた、またはメールで受け取ったファイルのスキャンパラメータ
   - 頻度、スキャンの種類、カスタムスキャンの対象となるオブジェクトのリストを含む、スケジュールによるファイルシステムスキャンの設定
   - 動作モード（集中管理サーバーに接続、または集中管理サーバーとの接続を切断）
   - ネットワークアクティビティ モニタリングパラメータ（暗号化トラフィックの検査を有効／無効にする）
   - Dr.Web Cloudサービス使用の 許可
8. ライセンスの管理（ライセンスマネージャー を使用して実行）
9. 集中管理サーバーから送信されたアンチウイルスネットワークの状態に関する メッセージの表示（Dr.Web for Linuxがアンチウイルスネットワーク内で動作していて、アンチウイルスネットワーク管理者が集中管理サーバーで該当する設定を行っている場合のみ）

Dr.Web for Linuxを正しく動作させるには、動作前にサービスコンポーネントを開始する必要があります。そうでない場合、起動直後に該当する警告メッセージを表示して終了します。標準モードでは、必要なすべてのサービスコンポーネントが自動的に起動され、ユーザーの操作は必要ありません。

グラフィカル管理インターフェースの外観

以下の画像はDr.Web for Linuxグラフィカル管理インターフェースのメインウィンドウの外観です。

図 5. Dr.Web for Linuxグラフィカル管理インターフェース

ナビゲーションパネルは、ウィンドウの左側にあります。ナビゲーションパネルのボタンを使用して、次の操作を実行できます。

ボタン	説明
1.常に表示	
	以下の操作を行うことのできるメインページを開きます。 • ファイルシステムモニターSpIDer Guardを有効／無効にする。 • ネットワーク接続モニターSpIDer Gateを有効／無効にする。 • ファイルシステムオブジェクト（ファイル、ブートレコード）と実行中のプロセスのスキャンを開始する。 • ウイルスデータベースが最新であるかどうかを確認し、必要に応じて更新する。 • ライセンスマネージャーを起動して現在のライセンスのステータスを確認し、必要に応じて新しいライセンスを登録する。
	隔離に移されたファイルを確認し、必要に応じてそれらを削除・復元することのできる 隔離ページ を開く。
	Dr.Web for Linux 設定ウィンドウ を開く。主な設定項目は次のとおりです： • Scanner • ファイルシステムモニターSpIDer Guard • ネットワーク接続モニターSpIDer Gate • スケジュールスキャン また、集中管理モードの設定を行うこともできます。
	参照資料 やDoctor Webによるサポートリソースを提供する： • 製品情報

ボタン	説明
	• ユーザーマニュアル • Dr.Web Forum • テクニカルサポート • ユーザー専用ページ **My Dr.Web** リンクはすべて、お使いのシステムにインストールされているブラウザで開きます。
2.状況に応じて表示	
	スキャンタスクのリストが表示されるページを開く。このページでは、未完了（実行中）のスキャンタスクを見つけることができます。 *スキャンが実行されている場合にのみ、ナビゲーションパネルに表示されます。*
	完了したスキャンのリストが表示されるページを開く。スキャン結果に応じて、ボタンの色が変わります。 1. 緑 - すべてのスキャンが正常に完了しました。検出されたすべての脅威が駆除されました。 2. 赤 - 検出された脅威の中に駆除されていないものがあります。 3. 黄 - 少なくとも1つのスキャンタスクが失敗しました。 *少なくとも1つのスキャンが開始された場合にのみ、ナビゲーションペインに表示されます。*
	Scannerまた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関するページを開く。 *少なくとも1つの脅威が検出された場合にのみ、ナビゲーションペインに表示されます。*
	スキャン開始ページが開いていてアクティブな場合にのみ、ナビゲーションペインに表示されます。 *メインウィンドウの他のページに移動するかスキャンセッションが開始されると、更新管理ページが自動的に閉じられ、ボタンがナビゲーションペインから削除されます。*
	SpIDer Guard管理ページが開いていてアクティブな場合にのみ、ナビゲーションペインに表示されます。 *メインウィンドウの他のページに移動すると、SpIDer Guard管理ページが自動的に閉じられ、ボタンがナビゲーションペインから削除されます。*
	SpIDer Gate管理ページが開いていてアクティブな場合にのみ、ナビゲーションペインに表示されます。 *メインウィンドウの他のページに移動すると、SpIDer Gate管理ページが自動的に閉じられ、ボタンがナビゲーションペインから削除されます。*
	更新管理ページが開いていてアクティブな場合にのみ、ナビゲーションペインに表示されます。 *メインウィンドウの他のページに移動すると、更新管理ページが自動的に閉じられ、ボタンがナビゲーションペインから削除されます。*
	ライセンスマネージャー管理ページが開いていてアクティブな場合にのみ、ナビゲーションペインに表示されます。

ボタン	説明
	メインウィンドウの他のページに移動すると、ライセンスマネージャー管理ページが自動的に閉じられ、ボタンがナビゲーションペインから削除されます。
	集中管理サーバーからの メッセージを表示する ページを開く。 *Dr.Web for Linuxが集中管理 モード で動作していて、アンチウイルスネットワーク管理者がワークステーションへのメッセージ送信を有効にしている場合にのみ、ナビゲーションペインに表示されます。*

メインページ

Dr.Web for Linuxグラフィカル管理インターフェースのメインページには、スキャンするファイルとディレクトリをドラッグ＆ドロップできるターゲットペインが表示されます。ペインには**ここにファイルをドラッグするか、またはクリックして選択してください** と表示されています。オブジェクトをファイルマネージャーから Dr.Web for Linux メインページにドラッグ＆ドロップした後、それらの カスタムスキャン が開始されます（Scannerがすでに他のオブジェクトをスキャンしている場合、新しいスキャンタスクは キューに入ります）。

メインページには、次のボタンも表示されます。

- **SpIDer Guard** - ファイルシステムモニターSpIDer Guardの現在の状態を表示します。ボタンをクリックすると、SpIDer Guardを開始または停止し、その動作に関する統計を確認することのできる 管理ページ を開くことができます。
- **SpIDer Gate** - ネットワーク接続モニターSpIDer Gateの現在の状態を表示します。 ボタンをクリックすると、SpIDer Gateを開始または停止し、その動作に関する統計を確認することのできる 管理ページ を開くことができます。
- **Scanner** - ファイルシステムのファイルやディレクトリ、その他のオブジェクト（ブートレコードなど）の スキャンを開始 することのできるページを開くことができます。
- **最終更新** - ウイルスデータベースの現在の状態を表示します。ボタンをクリックすると、更新プロセスを開始（必要な場合）することのできる 更新管理ページ を開くことができます。
- **ライセンス** - 現在のライセンスのステータスを表示します。このボタンをクリックすると、ライセンスマネージャー ページが開きます。このページでは、ライセンスに関する詳細情報を確認することができ、また、必要に応じて新しいライセンスを購入して登録することもできます。

デスクトップ環境との統合

Dr.Web for Linuxでは、グラフィカルデスクトップ環境との統合について、次の4つの方法がサポートされています。

- デスクトップ通知領域に アプリケーションステータスインジケータ を表示します（使用しているグラフィカル環境でサポートされている場合）。インジケータを使用することで、アプリケーションのコンテキストメニューを表示し、ポップアップ通知を表示できます。
- メインスキャンコマンドを含む コンテキストメニュー を表示します。ユーザーがマウスを使用してタスクバーのアプリケーションアイコンを右クリックすると、コンテキストメニューが表示されます。
- グラフィカルファイルマネージャー のコンテキストメニューのコマンドによって、選択したファイルやディレクトリのスキャンを開始します。

- ユーザーがDr.Web for Linuxのメインウィンドウにファイルやディレクトリを ドラッグ&ドロップ すると、それらのスキャンを開始します。

通知領域のステータスインジケータ

ユーザーがログオンすると、通知エージェントがデスクトップ通知領域（使用しているグラフィカル環境でサポートされている場合）に、Dr.Web for Linuxアイコンに似たインジケータを表示させます。インジケータはアプリケーションの状態を表示し、Dr.Web for Linuxメニューへのアクセスを提供します。何らかの問題が発生した場合（ウイルスデータベースが古い、ライセンスの有効期限が近づいているなど）、インジケータに感嘆符  が表示されます。

ステータスインジケータに加え、通知エージェントはDr.Web for Linux動作に関する次のような重要なイベントをユーザーに対して知らせる、ポップアップ通知も表示します。

- 検出された脅威（SpIDer GuardおよびSpIDer Gateによって検出されたものを含む）
- ライセンスの有効期間が近づいている

このアイコンをクリックすると、Dr.Web for Linuxコンテキストメニューが開きます。

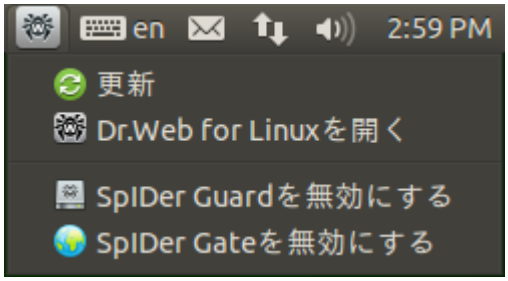

図 6. Dr.Web for Linuxインジケータコンテキストメニュー

Dr.Web for Linuxを開く を選択すると、画面に管理用のDr.Web for Linuxグラフィカルインターフェースの ウィンドウ が表示されます。つまり、Dr.Web for Linuxの 動作 が開始されます。**SpIDer Gateを有効にする／SpIDer Gateを無効にする** または **SpIDer Guardを有効にする／SpIDer Guardを無効にする** を選択すると、該当するモニターの動作が開始または停止されます。いずれのモニターについても、その動作を無効にするには、管理者特権を持つユーザーとして認証を行う必要があるということに注意してください（アプリケーションの権限管理 参照）。**更新** を選択すると、更新処理が開始されます。

インジケータがDr.Web for Linux動作の問題について通知すると、問題の原因となったコンポーネントのアイコンにも感嘆符が表示されます。例： 

ステータスインジケータのエラー

1. インジケータにクリティカルなエラーマーク  が表示され、ドロップダウンメニューに **読み込んでいます** と表示される場合は、一部のコアコンポーネントが使用できないためにDr.Web for Linuxを開始できないということを意味しています。この状態が続く場合は、このエラーを手動で 解決 するか、テクニカルサポート までご連絡ください。
2. ユーザーがログインした後に、通知領域内にインジケータが表示されない場合は、このエラーを手動で 解決 するか、テクニカルサポート までご連絡ください（使用しているグラフィカル環境で本機能がサポートされている場合に限る）。

デスクトップ環境によっては、インジケータの外観と動作が上のものと異なる場合があります。たとえば、アイコンがドロップダウンメニューに表示されないことがあります。

タスクバーアイコンのコンテキストメニュー

デスクトップ環境にタスクバーが含まれている場合（UbuntuのUnity Launcherなど）、Dr.Web for Linuxを起動すると、タスクバーにアプリケーションアイコンの付いたボタンが表示されます。**アプリケーション** デスクトップのメニューの **Dr.Web for Linux** 項目からアプリケーションを起動することをお勧めします。タスクボタンを右クリックすると、アプリケーションメニューが表示されます。メニューは次のようになります（UbuntuのUnity Launcherの例）。

図 7. タスクバーのコンテキストメニュー

- クイックスキャン、フルスキャン、カスタムスキャン を選択すると、それぞれ対応する スキャンタスク を開始することができます（カスタムスキャン の場合、スキャンするオブジェクトを選択できるページが開きます）。
- **Dr.Web for Linux** を選択するとグラフィカルインターフェースが 起動 し（起動していない場合）、**終了** を選択するとグラフィカルインタフェースが 終了 します（起動している場合）。
- **Launcherに登録** を選択すると、グラフィカルインターフェースや全般的なスキャンタスクにすばやくアクセスできるように、タスクバーのアプリケーションアイコンをロックできます。

タスクキュー にファイルシステムスキャン実行されたタスクがある場合は、実行されたアクティブなスキャンタスクの合計を表わすインジケータがタスクバーのアプリケーションアイコンの上に表示されます。

デスクトップ環境によっては、タスクバー、コンテキストメニュー、メニュー項目の動作（クイックスキャン、フルスキャン、カスタムスキャン を除く）は上と異なる場合があります。

タスクバーアイコンのエラー

タスクバーにアプリケーションアイコンが表示されているのにコンテキストメニューにスキャンタスクを開始する項目がない場合は、アプリケーション メニューの **Dr.Web for Linux** からアプリケーションを起動してください（ターミナルエミュレータの **Dr.Web GUI for Linux** コマンド、または通知領域内 ステータスインジケータ のコンテキストメニューで **Dr.Web for Linuxを開く** からアプリケーションを起動するのではなく）。

ファイルマネージャーからスキャンを開始する

Dr.Web for Linuxでは、グラフィックファイルマネージャー（Nautilusなど）のウィンドウから直接ファイルやディレクトリをスキャンできます。ファイルやディレクトリをスキャンする方法は次のとおりです。

1. ファイルマネージャーのウィンドウでファイルやディレクトリを選択し、マウスで右クリックします。
2. 表示されたコンテキストメニューで、**別のアプリケーションで開く** を選択します。
3. インストールされているアプリケーションの一覧で、**Dr.Web for Linux** を見つけて選択します。

通常、ファイルを開くために初めてDr.Web for Linuxの使用を選択した後、この関連付けがファイルマネージャーによって保存され、以後はコンテキストメニューに **Dr.Web for Linuxで開く** の項目が含まれるようになります。

グラフィカルファイルマネージャーによっては、選択されたファイルを処理するためのアプリケーションを選択する方法とコンテキストメニューの項目は、上のものと異なる場合があります。

ファイルマネージャーのコンテキストメニューの使用中に発生する問題

GNU/Linuxの一部のグラフィカル環境では、ファイルやディレクトリと、ファイルマネージャー内で **別のアプリケーションで開く**（他のアプリケーションで開く）を選択することによって選択された **Dr.Web for Linux** との関連付けを自動的に設定できます（MIMEタイプに基づいて）。したがって、それらのファイルまたはディレクトリをダブルクリックすると、**Dr.Web for Linux** が実行されます。この問題を解決するには、ファイルと **Dr.Web for Linux** との間に 設定された関連付けをキャンセル してください。

グラフィカル管理インターフェースのウィンドウにファイルとディレクトリをドラッグ&ドロップする

Dr.Web for Linuxでは、ファイルマネージャーのウィンドウやグラフィカルファイルマネージャーのディレクトリからDr.Web for Linux管理用グラフィカルインターフェースを実行するウィンドウにマウスポインタでファイルやディレクトリをドラッグ&ドロップすることによって、それらのスキャンを開始できます。ドラッグ&ドロップしてスキャンを開始するには、インターフェースウィンドウで メインページ または スキャンの種類 を表示するページが開いている必要があります。ページに **ここにファイルをドラッグするか、またはクリックして選択してください**（Dr.Web for Linux管理用インターフェースウィンドウにオブジェクトをドラッグ&ドロップすることができるということを示します）と記載された領域が含まれている場合、ドロップされたファイルオブジェクトがスキャンされます。

グラフィカルインターフェースの開始とシャットダウン

Dr.Web for Linuxグラフィカル管理インターフェースの起動

Dr.Web for Linuxグラフィカル管理インターフェースを起動するには、次の手順を実行します。

- アプリケーション で **Dr.Web for Linux** を選択します。

または

- 通知領域内の Dr.Web for Linux ステータスインジケータ アイコンを右クリックし、**Dr.Web for Linuxを開く** を選択します。

コマンド `drweb-gui` を入力することで、コマンドライン からもDr.Web for Linuxグラフィカル管理インターフェースを開始できます。この方法はグラフィカル環境がコマンドラインモードでアクセス可能な場合（端末エミュレータウィンドウ内で操作している場合など）のみ使用できます。

Dr.Web for Linuxグラフィカル管理インターフェースの終了

Dr.Web for Linuxグラフィカル管理インターフェースをシャットダウンするには、タイトルバーにあるクローズボタンを使用してウィンドウを閉じます。

注意：通知エージェント、SpIDer Guard、SpIDer Gateを含むサービスコンポーネントは、Dr.Web for Linuxグラフィカルインターフェースを閉じた後も動作を続けます（ユーザーによって無効にされない限り）。

通常動作時には、必要なすべてのサービスコンポーネントの動作にユーザーの操作は必要ありません。

脅威の検出と駆除

脅威の検索と駆除は、Scannerによって（ユーザー によるオンデマンドで、または スケジュールに従って）、またはファイルシステムモニターSpIDer Guardやネットワーク接続モニターSpIDer Gateによって開始できます。

- SpIDer Guard とSpIDer Gateを有効または無効にするには、通知領域内の コンテキストメニュー を使用するか、モニター設定の該当するページを開きます（ファイルシステムモニタリング および ネットワーク接続のモニタリング 参照）。
- Scannerの現在のタスクを見る、またはそれらを管理するには、タスク管理 のページを開きます。
- Scannerによって検出された、またはSpIDer Guardによるチェック中に検出された脅威を見るには、脅威リストのページ を開きます。
- 隔離された脅威を管理するには、隔離を見る ページを開きます。
- 検出された脅威に対するDr.Web for Linuxのアクションを設定するには、設定ウィンドウ を開きます。このウィンドウで、スキャンを開始するための スケジュール の設定や、暗号化された接続のモニタリングを 設定 することもできます。

Dr.Web for Linuxが 集中管理モード で動作していて、ユーザーによるオンデマンドでのスキャンの実行が集中管理サーバーで禁止されている場合、Dr.Web for Linuxウィンドウの **Scanner** ページ は無効になります。また、この場合、たとえスケジュールで設定されている場合であっても、通知エージェントと管理用グラフィカルインターフェースはスキャンを実行しません。

オンデマンドスキャン

このセクションの内容：

- スキャンの種類
- スキャンを開始する
- カスタムスキャンオブジェクトのリストを編集する
- リスト上のオブジェクトのカスタムスキャンを開始する

スキャンの種類

ユーザーによるオンデマンドで、以下のうちいずれかのモードでのスキャンを開始できます。

- *クイックスキャン* - 感染のリスクが高いクリティカルなシステムオブジェクト（ブートレコード、システムファイルなど）をスキャンします。
- *フルスキャン* - Dr.Web for Linuxを起動したユーザーが使用できるすべてのファイルシステムオブジェクトをスキャンします。
- *カスタムスキャン* - ユーザーが指定したファイルシステムオブジェクトまたはその他の特別なオブジェクトをスキャンします。

Dr.Web for Linuxが 集中管理 モードで動作していて、オンデマンドスキャンの実行が集中管理サーバー上で禁止されている場合、このページは無効になります。

スキャンの間はプロセスロードが増大し、バッテリーの減りが早くなる場合があります。スキャンを実行する際はコンピューターをコンセントに接続することを推奨します。

スキャンを開始する

スキャンを開始するには、メイン ページで **Scanner** ボタンをクリックします。

スキャンの種類のページが開きます。*クイックスキャン* または *フルスキャン* を開始するには、該当するボタンをクリックします。これらのボタンがクリックされると、スキャンプロセスが自動的に開始されます。

図 8. スキャンの種類を選択するページ

スキャンは現在のアプリケーションの権限で実行されます。権限が現在アクティブとなっているユーザーがスーパーユーザー権限を有していない場合、そのユーザーがアクセスできないフィールドやディレクトリはいずれもスキャンできません。権限を持っていないファイルをスキャンするには、スキャン開始前にアプリケーションの権限を昇格させてください。詳細については アプリケーションの権限管理 を参照してください。

特定のファイルやディレクトリの *カスタムスキャン* スキャンを開始するには、以下のうちいずれか1つを行います。

- **必要なオブジェクトをドラッグ & ドロップする**

  必要なファイルやディレクトリをシステムのファイルマネージャーウィンドウから **ここにファイルをドラッグするか、またはクリックして選択してください** でマークされたエリアにドラッグ & ドロップします。メイン ページにオブジェクトをドラッグ & ドロップすることもできます。

  ページ上にオブジェクトをドラッグすると、ウィンドウが **ファイルをここにドロップ** ラベルで指定されたペインに変わります。スキャンを開始するには、マウスボタンを離すことで、ドラッグしたオブジェクトをターゲットエリアにドロップしてください。

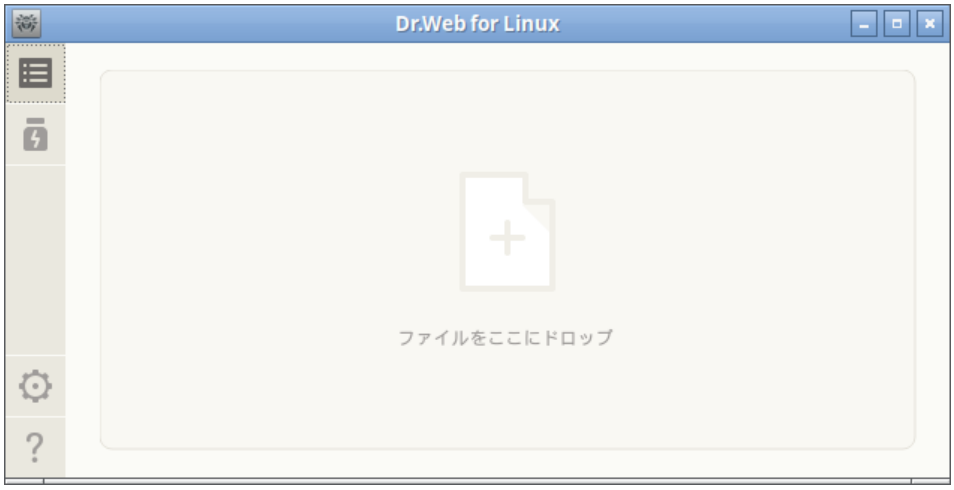

図 9. スキャンするオブジェクトをドロップするターゲットエリア

- **スキャンするオブジェクトのリスト**

  スキャンするオブジェクトを選択するには、ターゲットエリアをクリックします。カスタムスキャン用にシステムオブジェクトを選択するためのウィンドウが開きます。

図 10. スキャンするオブジェクトのリスト

カスタムスキャンの対象となるオブジェクトのリストには、あらかじめ4つのアイテムが含まれています。

- *すべてのディスクのブートレコード* - このアイテムを有効にした場合、使用可能なすべてのディスクのすべてのブートレコードがスキャンの対象として選択されます。
- *システムのバイナリとライブラリ* - このアイテムを有効にした場合、システムライブラリのあるすべてのディレクトリ(`/bin`、`/sbin` など)がスキャンの対象として選択されます。

- *ユーザーファイルのあるディレクトリ* - このアイテムを有効にした場合、ユーザーファイルと現在のセッションのファイルがあるすべてのディレクトリ(`/home/<username>`[~]、`/tmp`、`/var/mail`、`/var/tmp`)がスキャンの対象として選択されます。
- *実行中のプロセス* - このアイテムを有効にした場合、現在実行中のプロセスのコードが含まれたバイナリ実行ファイルがスキャンの対象として選択されます。この場合、脅威が検出されると悪意のあるオブジェクトが駆除されるだけでなく、アクティブなプロセスが終了されます。

カスタムスキャンオブジェクトのリストを編集する

必要に応じ、スキャンの対象となるオブジェクトのリストにカスタムのパスを追加できます。必要なオブジェクトをドラッグ＆ドロップするか(オブジェクトへのパスが自動的にリストに追加されます)、またはリスト下の + ボタンをクリックします。この場合、標準的なダイアログウィンドウが開き、そこで必要なオブジェクト(ファイルまたはディレクトリ)を選択できます。オブジェクトを選択した後、**開く** をクリックします。

デフォルトでは、隠しファイルや隠しディレクトリは選択用ウィンドウに表示されません。そのようなオブジェクトを見えるようにするには、ウィンドウ内で ✱ ボタンをクリックします。

選択したすべてのパスをリストから削除するには、− ボタンをクリックします。パスを含むリストアイテムが選択されている場合、パスは削除の対象として選択されています。複数のパスを選択するには、SHIFT キーまたは CTRL キーを押したままリスト内でアイテムを選択します。リスト内の最初の4つのアイテムはあらかじめ設定されているもので、削除することはできません。

リスト上のオブジェクトのカスタムスキャンを開始する

リスト上のオブジェクトのカスタムスキャンを開始するには、必要なすべてのファイルやディレクトリのチェックボックスにチェックを入れ、**スキャン** をクリックします。ボタンがクリックされると、選択したオブジェクトのスキャンが開始されます。

スキャンの開始後、現在のセッションのすべてのスキャンタスク(完了したタスク、進行中のタスク、保留中のタスク)が含まれたキューにタスクが追加されます。スキャンタスクの管理 ページでタスクのリストを確認し、それらを管理できます。

オブジェクトのスケジュールスキャン

Dr.Web for Linuxでは、特定のファイルシステムオブジェクトに対するスケジュールスキャンを 指定されたスケジュール に従って自動的に実行することができます。

Dr.Web for Linuxが 集中管理 モードで動作していて、オンデマンドスキャンの実行が集中管理サーバー上で禁止されている場合、このオプションは無効になります。

スキャンの種類

スケジュールに従って、以下の種類のスキャンを実行することができます。

- *クイックスキャン* - 感染のリスクが高いクリティカルなシステムオブジェクト(ブートレコード、システムファイルなど)をスキャンします。

- *フルスキャン* - Dr.Web for Linuxを起動したユーザーが使用できるすべてのファイルシステムオブジェクトをスキャンします。
- *カスタムスキャン* - ユーザーが指定したファイルシステムオブジェクトまたはその他の特別なオブジェクトをスキャンします。

スキャンを開始する

設定したスケジュールに従って自動的にスキャンが開始されます。スキャンの開始は次のように行われます。

1. スキャン開始時にグラフィカルインターフェースが実行されている場合は、グラフィカルインターフェースによって
2. スキャン開始時にグラフィカルインターフェースを使用できない場合は、通知エージェントによって

スケジュールスキャンの開始後、管理用グラフィカルインターフェースが自動的に起動され（まだ起動していない場合）、作成されたタスクは現在のセッションのすべてのスキャンタスク（完了したタスク、進行中のタスク、保留中のタスク）が含まれたキューに追加されます。スキャンタスクの管理 ページでタスクのリストを確認し、それらを管理できます。

スキャンタスクを管理する

特別なDr.Web for Linuxページで、作成されたタスクと進行中のタスクのリストを見ることができます。少なくとも1つのタスクがキュー内にある場合、タスクリストのページを開くボタンが ナビゲーションペイン 内に表示されます。キュー内のタスクのステータスに応じて、ボタンには以下のうちいずれか1つのアイコンが付きます。

	少なくとも1つのタスクが完了していません（アイコンがアニメーション）。
	リスト上のすべてのスキャンタスクが完了しているか、ユーザーによって停止されました。脅威が検出されなかったか、検出されたすべての脅威が駆除されました。
	リスト上のすべてのスキャンタスクが完了しているか、ユーザーによって停止されました。検出された脅威の一部が駆除されていません。
	リスト上のすべてのスキャンタスクが完了しているか、ユーザーによって停止されました。一部のタスクが失敗しました。

タスクは作成時刻でソートされます（最新のタスクから順に表示）。

図 11. タスク管理ページ

リスト上の各タスクについて以下の情報が表示されます。

- スキャンタイプ（このリストには *クイックスキャン*、*フルスキャン*、*カスタムスキャン* だけでなく、追加のスキャンの種類も含まれています。下を参照してください）。
- スキャンを開始したユーザーの名前（名前が分からない場合はシステムの識別子 *UID* が表示されます）
- タスクの作成日および完了日（完了した場合）
- 検出された脅威の数、駆除された脅威の数、スキップされたファイルの数、スキャンされたオブジェクトの合計数

リスト上のタスクに付けられたカラーマークはタスクのステータスを示しています。以下の色が使用されます。

	スキャンは完了していないか、保留中です。
	スキャンは完了しているか、ユーザーによって停止されました。脅威が検出されなかったか、検出されたすべての脅威が駆除されました。
	スキャンはエラーによって停止しました。
	スキャンは完了しているか、ユーザーによって停止されました。検出された脅威のうち少なくとも1つが駆除されていません。

リストには、Dr.Web for Linuxウィンドウ内で ユーザーによって直接作成され、Scannerによって実行されたスキャンタスクだけでなく、設定されたスケジュールに従って自動的に実行されたスキャンタスクも含まれるということに注意してください。

タスクの説明エリアでは、以下のうち1つのボタンを使用できます。

- **キャンセル** - 保留中のタスクをキャンセルします。このボタンはタスクが保留中の場合に使用可能です。ボタンをクリックすると、タスクが完了します。タスクに関する情報はリスト上に残ります。
- **停止** - 進行中のタスクを停止します。ボタンをクリックした後は、停止したタスクを再開することはできません。このボタンはタスクが進行中の場合に使用可能です。停止したタスクに関する情報はリスト上に残ります。

- **閉じる** - 完了したタスクに関する情報を閉じ、タスクをリストから削除します。このボタンは、タスクが完了していない場合と検出されたすべての脅威が駆除された場合に使用可能です。
- **駆除** - 脅威を駆除します。このボタンはタスクが完了していて、検出された一部の脅威が駆除されていない場合に使用可能です。
- **詳細** - 検出された脅威のリストを開き、それらを駆除します。このボタンはタスクが完了していて、検出された一部の脅威が駆除されていない場合に使用可能です。

タスクに関する詳細と検出された脅威のリスト（検出された場合）を含む、スキャン結果に関する情報を表示するには **レポート** をクリックします。

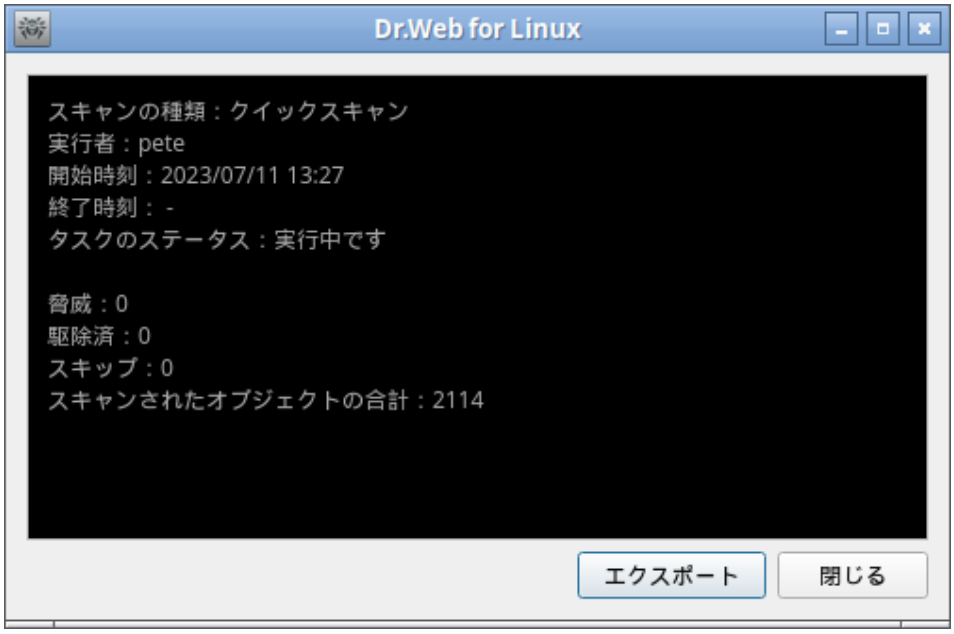

図 12. スキャン結果に関する詳細

GNU/LinuxなどのUNIX系OSのファイルシステムは、名前付きファイルとして表示されるがデータが含まれた実際のファイルではない特殊なオブジェクトを含むことができます（シンボリックリンク、ソケット、名前付きパイプ、デバイスファイルなど）。これらは *通常* ファイルに対して *特殊* ファイルと呼ばれます。Dr.Web for Linuxによるスキャンでは、特殊ファイルは *常に* スキップされます。

検出された脅威名をクリックすると、その説明がシステムにインストールされているブラウザで開きます（Doctor Web 公式サイトのページが開きます。インターネット接続が必要です）。

スキャンレポートをテキストファイルに保存する場合は **エクスポート** をクリックします。スキャンに関する詳細が含まれたウィンドウを閉じるには **閉じる** をクリックします。

グラフィカルモードで開始されたスキャン（スケジュールによるスキャンを含む）中に検出された脅威に対しては、**Scanner** タブ 上の設定内で指定された アクション が適用されます。

Scanner タブ上で指定された脅威駆除の設定は *集中管理* スキャンおよび *コンソール* スキャンでは使用されませんので注意してください。

検出されたすべての脅威を見るには、検出された脅威のリストページ を開きます。

ファイルシステムモニタリング

このセクションの内容:

概要

ファイルシステムオブジェクトの継続的なモニタリングは、ファイルシステムモニターSpIDer Guardによって行われます。

Dr.Web for Linuxグラフィカル管理インタフェースでSpIDer Guard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を有効／無効にする
- コンポーネントの統計と検出された脅威のリストを見る
- ファイルシステムモニターの次のパラメータを設定する:
  - 検出された脅威に対するアクション
  - スキャンの対象から除外するオブジェクトのリスト

ファイルシステムモニターSpIDer Guardの動作を管理する

Dr.Web for Linux の管理ページで、ファイルシステムモニターSpIDer Guardを有効／無効にしたり、その動作に関する統計を確認したりできます。このページにアクセスするには、メインページ で **SpIDer Guard** をクリックします。

図 13. SpIDer Guard管理ページ

SpIDer Guardの管理ページには、以下の情報が表示されます。

- ファイルシステムモニターSpIDer Guardの状態（有効／無効）およびコンポーネントの動作中にエラーが発生した場合はその詳細
- SpIDer Guardの統計:

- ファイルの平均スキャン速度
- 検出・駆除された脅威の数

SpIDer Guardを有効にするには、**有効** をクリックします。SpIDer Guardを無効にするには、**無効** をクリックします。

> ファイルシステムモニターSpIDer Guardを無効にするには、アプリケーションが昇格した権限で動作している必要があります。アプリケーションの権限管理 を参照してください。
>
> ---
>
> Dr.Web for Linux が 集中管理 サーバー によって動作している場合、SpIDer Guardを有効／無効にするオプションは、それがサーバーで無効になっている場合はブロックされます。

SpIDer Guardの状態（有効／無効）は次のように表示されます。

	ファイルシステムモニターSpIDer Guardは有効になっていて、ファイルシステムを保護しています。
	コンポーネントがユーザーによって無効にされているか、エラーが発生したため、ファイルシステムモニターSpIDer Guardはファイルシステムを保護していません。

ページを閉じるには、ペイン内のボタンを使用して別のページに移動してください。

Dr.Web for Linuxの現在のセッションでSpIDer Guardによって検出された脅威のリストは 検出された脅威 ページ（少なくとも1つの脅威が検出された場合に見ることができます）に表示されます。

ファイルシステムモニターSpIDer Guardを設定する

ファイルシステムモニターSpIDer Guardの動作は 設定ウィンドウ 内で設定できます。

- **SpIDer Guard** タブ で、検出された脅威に対するアクションを設定します。
- **除外** タブ で、モニタリングの対象から除外するオブジェクトを指定します。

> SpIDer Guardによる強化されたファイルモニタリングについては、ファイル監視モード を参照してください。

SpIDer Guardの動作に関する問題

SpIDer Guardの動作中にエラーが発生した場合、管理ページにエラーメッセージが表示されます。問題を解決するには、付録D に記載された既知のエラーに関する説明を参照してください。

ネットワーク接続をモニタリングする

このセクションの内容：

- 概要
- ネットワーク接続モニターSpIDer Gateの動作を管理する
- SpIDer Gateを設定する

- SpIDer Gateの動作に関する問題

概要

確立されたネットワーク接続の継続的な制御はSpIDer Gateによって行われます。ユーザーのブラックリストに追加されたWebサイトや訪問が望ましくないと見なされるWebサイトへのアクセスを制限します。そのほか、SpIDer Gateは以下のスキャンを行います:

- 送受信メールのスキャン
- インターネットからダウンロードされるファイルのスキャン

スキャンしたオブジェクトで脅威が検出されたた場合、SpIDer Gateは受信または送信をブロックします。

Dr.Web for Linuxグラフィカル管理インタフェースで SpIDer Gateの動作を設定することができます。

- ネットワーク接続モニターSpIDer Gateを有効／無効にする
- スキャンされたオブジェクトとブロックされたオブジェクトの数、ならびにWebサイトへのアクセス試行回数を見る
- ネットワーク接続モニタリングの次のパラメータを設定する:
  - スキャンするトラフィックの種類（Webトラフィック、FTPトラフィック）を選択する
  - アクセスを制限するWebサイトとホストのリスト
  - Webサイトとホストのパーソナルブラックリストとホワイトリスト
  - インターネットからダウンロードされるファイルをスキャンするパラメータ

メールに含まれている脅威は、メールクライアントによってローカルファイルシステムに保存される時点で、有効になっているファイルシステムモニターSpIDer Guardによって検出されます。

ネットワーク接続モニターSpIDer Gateの動作を管理する

Dr.Web for Linuxの管理ページで、ネットワーク接続モニターSpIDer Gateを有効／無効にしたり、その動作に関する統計を確認したりできます。このページにアクセスするには、メインページ で **SpIDer Gate** をクリックします。

図 14. SpIDer Gate管理ページ

SpIDer Gateの管理ページには、以下の情報が表示されます。

- ネットワーク接続モニターSpIDer Gateの状態（有効／無効）およびコンポーネントの動作中にエラーが発生した場合はその詳細
- SpIDer Gateの統計：
  - メールおよびインターネットからダウンロードされるファイルの平均スキャン速度
  - スキャンされたオブジェクト（メールメッセージ、インターネットからダウンロードされるファイル、URL）の数
  - ブロックされた、Webサイトへのアクセス試行と悪意のあるオブジェクトの数

SpIDer Gateを有効にするには、**有効** をクリックします。SpIDer Gateを無効にするには、**無効** をクリックします。

ネットワーク接続モニターSpIDer Gateを無効にするには、アプリケーションが昇格した権限で動作している必要があります。アプリケーションの権限管理 を参照してください。

Dr.Web for Linuxが 集中管理 サーバー によって動作している場合、SpIDer Gateを有効／無効にするオプションは、それがサーバーで無効になっている場合はブロックされます。

ネットワーク接続モニターSpIDer Gateの状態（有効／無効）は次のように表示されます。

	SpIDer Gateが有効になっていて、ネットワーク接続（およびメールとインターネットアクセス）を制御しています。
	コンポーネントがユーザーによって無効にされているか、エラーが発生したため、SpIDer Gateはネットワーク接続を制御していません（Webサイトへのアクセスは制限されず、メールおよびダウンロードされるファイルはスキャンされません）。

メッセージの受信にIMAPを使用しているメールクライアント（Mozilla Thunderbirdなど）がシステムで実行されている場合は、受信メッセージをスキャンできるようにするため、アンチウイルスのインストール後に再起動します。

ページを閉じるには、ペイン内のボタンを使用して別のページに移動してください。

SpIDer Gateを設定する

ネットワーク接続モニターSpIDer Gateの動作設定は 設定ウィンドウ 内で行います。

- **SpIDer Gate** タブ で、ブロックするWebサイトカテゴリーと検出された脅威に対するアクションのリストを設定できます。
- **除外** タブ で、Webサイトのブラックリストとホワイトリストを設定し、アプリケーションのネットワークアクティビティをモニタリングの対象から除外できます。
- **ネットワーク** タブ で、保護された接続（SSL/TLS）のスキャンを管理できます。

SpIDer Gateの動作に関する問題

ネットワーク接続モニターSpIDer Gateの動作中にエラーが発生した場合、管理ページにエラーメッセージが表示されます。問題を解決するには、付録D. 既知のエラー セクションに記載された既知のエラーに関する説明を参照してください。

ディストリビューションによっては、Dr.Web for LinuxでDr.Web Anti-Spamを利用できない場合があります。そのような場合、メールメッセージのスパムスキャンは実行されません。

アンチスパムコンポーネントDr.Web Anti-Spamによって誤って検出されたメールメッセージがある場合は、分析のため、また、スパムフィルタの品質向上のためにそれらを特別なアドレスに転送していただけますようお願いいたします。これを行うには、各メッセージを別々の `.eml` ファイルに保存します。次に、ファイルをメールメッセージに添付して、専用のアドレスに転送してください。

- *誤ってスパムと判定された* メッセージは nonspam@drweb.com に送信してください。
- *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。

検出された脅威を見る

このセクションの内容:

概要

Dr.Web for Linuxの現在のセッションでScannerやSpIDer Guardによって検出された脅威のリストは 専用のページに表示されます(少なくとも1つの脅威が検出された場合に見ることができます)。

脅威が検出された場合、ナビゲーションペイン内の  をクリックすることで、このページを開くことができます。

図 15. 脅威のリストページ

リストでは、検出されたそれぞれの脅威について以下の情報が表示されます。

- 悪意のあるオブジェクトの名前
- 脅威 の名前（Doctor Webの分類による）
- 脅威に対して適用された（または適用される）アクション
- 悪意のあるオブジェクトへのパス

駆除された脅威はリスト内にグレーで表示されます。

検出された脅威を駆除する

リスト内の脅威に駆除されなかったものがある場合、リスト上部の **駆除** ボタンが使用可能になります。ボタンをクリックすると、該当する **アクション** フィールドで指定されたアクションが脅威に対して適用されます。脅威の駆除に失敗した場合、リスト上の脅威が赤色で表示され、**アクション** フィールド内にエラーメッセージが表示されます。

デフォルトでは、脅威に適用されるアクションは脅威を検出したコンポーネントの設定に応じて選択されます。特定の種類の脅威に対して適用するアクションをScannerとSpIDer Guardのそれぞれに設定できます。設定ウィンドウ 上の該当するタブを開き、設定を編集してください。

特定の種類の脅威に対して アクション *報告* を実行するように Scanner または SpIDer Guard を設定した場合、脅威のリスト内では該当する種類の脅威に対するアクションとして 何もしない が表示されます。そのような脅威を駆除するには、**アクション** フィールドで、それぞれの脅威に対するアクションを指定してください。

設定で指定されたものと異なるアクションを適用する必要がある場合は、**アクション** フィールドをクリックし、メニューから該当するアクションを選択してください。

コンテナ（アーカイブ、メール添付ファイルなど）内のファイルで脅威が検出された場合は、削除アクションの代わりにコンテナの隔離への移動が実行されます。

脅威のリストでは、一度に複数のアイテムを選択できます。その場合、CTRL キーまたは SHIFT キーを押したままマウスボタンでアイテムを選択します。

- 離れた複数の脅威を選択する場合は CTRL キーを押します。
- 連続する複数の脅威を選択する場合は SHIFT キーを押します。

脅威を選択した後、選択領域内で右クリックし、表示されたメニューで該当するアイテムをクリックすることで、必要なアクションを適用できます。メニューから選択されたアクションが、選択されたすべての脅威に対して適用されます。

注意事項

- 複合オブジェクト（アーカイブ、メールなど）内で脅威が検出された場合、選択されたアクションは複合オブジェクト全体に適用されます（感染したオブジェクトのみでなく）。
- *修復* アクションは、特定の種類の脅威には適用することができません。。

必要に応じ、脅威を駆除するために アプリケーション権限 を昇格させてください。

無視 アクションが指定された脅威は、グラフィカルユーザーインターフェースが再起動されるまでリストに表示されます。

脅威に関する情報を見る

検出された脅威に関する詳細を見るには、該当する行で右クリックし、表示されたコンテキストメニューで **詳細** を選択します。脅威および感染したオブジェクトの情報が含まれたウィンドウが開きます。複数の脅威に関する詳細を見る場合は、CTRL キーを押しながらマウスの左ボタンを使用してそれらのオブジェクトを選択します。

図 16. 脅威に関する情報

このウィンドウには以下の情報が表示されます。

- 脅威 の名前（Doctor Webの分類による）
- 脅威を検出したDr.Web for Linuxコンポーネントの名前

- 脅威が検出された日時
- 脅威が検出されたファイルシステムオブジェクトに関する情報：オブジェクト名、所有者、最終変更日、ファイルシステム内のオブジェクトへのパス
- 脅威に対して最期に適用されたアクションとその結果（そのコンポーネントで、脅威に対して自動的にアクションを適用するオプションが有効になっていた場合。たとえば、アプリケーション設定の 該当するタブ 内で設定することができます）

脅威名をクリックすると、その説明がシステムにインストールされているブラウザで開きます（Doctor Web公式サイトのページが開きます。インターネット接続が必要です）。

表示された情報をテキストファイルに保存する場合は **エクスポート** をクリックします（ボタンをクリックすると、ファイル参照ウィンドウが開きます）。脅威とオブジェクトの説明ウィンドウを閉じるには **閉じる** をクリックします。

隔離の管理

このセクションの内容：

- 概要
- 隔離された脅威にアクションを適用する
- 隔離されたオブジェクトの詳細を見る

概要

Dr.Web for Linuxによって隔離されたオブジェクトのリストは専用のページに表示されます。ページを開くには、ナビゲーションペイン で  をクリックします。

図 17. 隔離管理ページ

隔離されたファイルが存在する場合、すべての脅威について以下の情報がリストに表示されます。

- 悪意のあるオブジェクトの名前
- 隔離内のオブジェクトに対して適用する アクション
- 脅威 の名前（Doctor Webの分類による）

隔離された脅威にアクションを適用する

隔離内にあるオブジェクトにアクションを適用するには、該当する脅威に関する情報が含まれた行内の任意の場所で右クリックし、表示されたショートカットメニューから必要なアクションを選択します。複数のオブジェクトに対して1つのアクションを適用する場合、該当する行を選択し、任意のエリアで右クリックします。複数の行を選択するには、CTRL キーまたは SHIFT キーを押したまま選択します。

- CTRL キーを押すと、複数の行を一度に選択できます。
- SHIFT キーを押すと、連続する複数の行を選択できます。

メニューには以下のアクションが含まれています。

- **復元**- 選択されたオブジェクトを元の場所に復元します。
- **次の場所に復元** - 選択されたオブジェクトをファイルシステム内の指定された場所に復元します（復元先の場所を選択するウィンドウが表示されます）。
- **削除** - 選択されたオブジェクトを永久に削除します。
- **再スキャン** - 選択されたオブジェクトを再スキャンし、可能であれば修復します。

選択されたアクションがオブジェクトに対して問題なく適用されると、該当する行が表内から自動的に削除されます。アクションの適用に失敗した場合、該当する行はアクティブな状態のままで赤くなり、**アクション** フィールドにエラーの詳細が表示されます。

隔離されたオブジェクトに対してアクションを適用する際、アプリケーションの権限を昇格する必要が生じる場合があります。いずれかのユーザーによって隔離に移されたオブジェクトに対してアクションを適用する場合などです。

隔離されたオブジェクトの詳細を見る

隔離されたオブジェクトに関する詳細を見るには、該当する行で右クリックし、表示されたメニューで **詳細** を選択します。オブジェクトの情報が含まれたウィンドウが開きます。複数のオブジェクトに関する詳細を見る場合は、コンテキストメニューを開く前にそれらのオブジェクトを選択してください。

図 18. 隔離されたオブジェクトの詳細

このウィンドウには以下の情報が表示されます。

- 脅威 の名前（Doctor Webの分類による）
- オブジェクトが隔離に移された日時
- オブジェクトが移された隔離の 種類
- 最後に適用されたアクションとその結果
- 隔離されたファイルシステムオブジェクトに関する詳細：名前、所有者、最終変更日、ファイルシステム内のオブジェクトのパス

脅威名をクリックすると、その説明がシステムにインストールされているブラウザで開きます（Doctor Web公式サイトのページが開きます。インターネット接続が必要です）。

表示された情報をテキストファイルに保存する場合は **エクスポート** をクリックします（ボタンをクリックすると、ファイル参照ウィンドウが開きます）。脅威とオブジェクトの説明ウィンドウを閉じるには **閉じる** をクリックします。

アンチウイルス保護を更新する

このセクションの内容：

- 概要
- 更新を設定する
- Updaterの動作に関する問題

概要

ウイルスデータベース、Webカテゴリーデータベースおよびアンチウイルスエンジンの定期的な更新はUpdaterによって自動的にダウンロード・インストールされます。必要に応じ、ウィンドウの専用ページでデータベースの状態を確認し、強制的に更新を行うことができます。このページを開くには、メインページ で **最終更新** をクリックします。

図 19. 更新管理ページ

このページには以下の情報が表示されます。

- ウイルスデータベース、Webリソースカテゴリーのデータベース、スキャンエンジンの状態
- 前回の更新に関する情報と、スケジュールされている次回の自動更新の時間

強制的に更新するには、**更新** をクリックします。更新管理ページを閉じるには、ナビゲーションペイン内の該当するボタンをクリックすることで別のメインウィンドウページを選択してください。

Dr.Web for Linuxが 集中管理 モードで動作している場合、更新管理ページはブロックされることがあります。

更新を設定する

Dr.Web for Linuxの更新設定は、設定ウィンドウ の **メイン**タブ で行うことができます。

Updaterの動作に関する問題

Updaterの不具合が検出された場合、更新管理ページにエラー情報が表示されます。問題を解決するには、付録D に記載された既知のエラーに関する詳細を参照してください。

ライセンスマネージャー

このセクションの内容：

概要

ライセンスマネージャーでは、Dr.Web for Linuxユーザーに対して発行された現在のライセンスに関する情報を表示できます。ライセンスに関するデータは、ユーザーのコンピューター上でのDr.Web for Linuxの動作を提供するライセンスキーファイルに含まれています。コンピューター上にライセンスキーファイルもデモキーファイルも見つからない場合、Dr.Web for Linuxのすべての機能（ファイルのスキャン、ファイルシステムモニタリング、ウイルスデータベース更新を含む）がブロックされます。

ライセンスマネージャー

ライセンスマネージャーページは、Dr.Web for Linuxグラフィカルインターフェースで使用できます。ページを開くには、メインページ で **ライセンス** をクリックします。

Dr.Web for Linuxのデモキーファイルまたはライセンスキーファイルがインストールされている場合、ライセンスマネージャーの開始ページには、ライセンス番号、ライセンス所有者、有効期間などのライセンス情報が表示されます。この情報は対応するキーファイルから取得されます。

ライセンスマネージャーページの外観は以下のようになります。

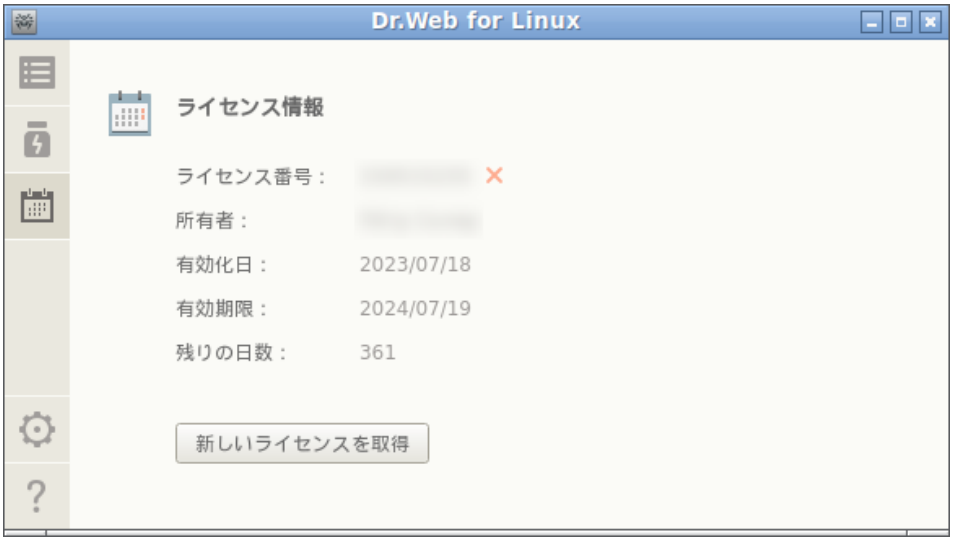

図 20. ライセンス情報ページ

ライセンスキーファイルを 削除 するには、ライセンス番号の横にある ✕ をクリックします。

ライセンスマネージャーページを閉じるには、ナビゲーションペイン内の該当するボタンをクリックすることで別のメインウィンドウページを選択します。

ライセンスの有効化

ライセンスマネージャーを使用してライセンスを有効にし、Dr.Web for Linuxの機能を提供する対応するキーファイルを取得（新しいライセンスの購入または現在のライセンスの更新によって）、またはデモライセンスを取得するには、**新しいライセンスを取得** をクリックします。その後、登録ウィザードが開きます。登録ウィザードは、Dr.Web for Linuxのインストール後の初回起動時にも自動的に開きます。

最初のステップで、有効化の種類を選択する必要があります。次の3つの種類があります。

1. シリアル番号を使用してライセンスまたは試用期間を 有効化 する
2. 試用期間を 取得 する
3. 先に取得したキーファイルを インストール する

シリアル番号を登録、または試用期間を取得するには、インターネット接続が必要です。

1. シリアル番号を使用してライセンスまたは試用期間を有効にする

シリアル番号を使用してライセンスまたは試用期間を有効にするには、テキストフィールドにその番号を入力し、**有効化** をクリックします。

図 21. シリアル番号を使用した登録

シリアル番号または有効なキーファイルをお持ちでない場合は、Doctor Webの公式サイトでライセンスを購入できます。オンラインストアのページを開くには、**ライセンスを購入** をクリックします。

Dr.Web製品のライセンスを購入するその他の方法については、製品の登録と有効化 を参照してください。

有効化 ボタンをクリックすると、Doctor Web 登録サーバーとの接続が確立されます。

指定されたシリアル番号が2台のコンピューター用のライセンスに対応する場合は、Dr.Web for Linuxを使用するコンピューターの台数を選択する必要があります。**2台のコンピューター(On two computers)** を選択した場合、別のコンピューターで2つ目のシリアル番号を有効にし、別のライセンスキーファイルを受け取ることができます。登録されたライセンスの有効期間は同じです(例:1年間)。**1台のコンピューター(On one computer** を選択した場合は、購入したキットから2つ目のシリアル番号を指定する必要があります。この場合、後でこのシリアル番号を別のコンピューター上で登録することはできません(シリアル番号は順次有効化されるため、ライセンスキーファイルのコピーを使用することもできません)が、現在のライセンス有効期間は2倍になります(たとえば、ライセンス有効期間が1年の場合は2年間)。

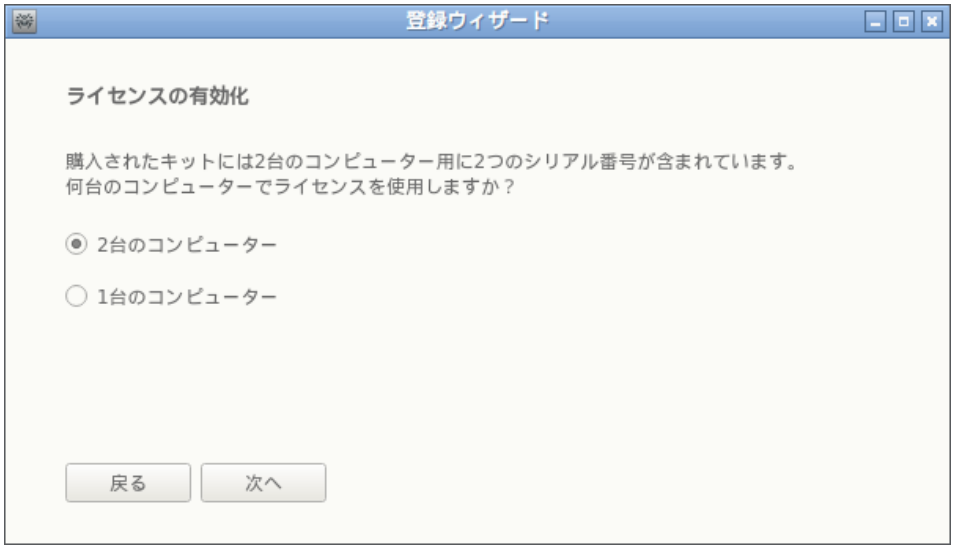

図 22. コンピューターの台数を選択する

ライセンスを有効化するコンピューターの台数を選択した後で **次へ** をクリックします。**1台のコンピューター** を選択した場合は、ウィザードの次のステップで 2つ目のシリアル番号を入力して **次へ** をクリックします。

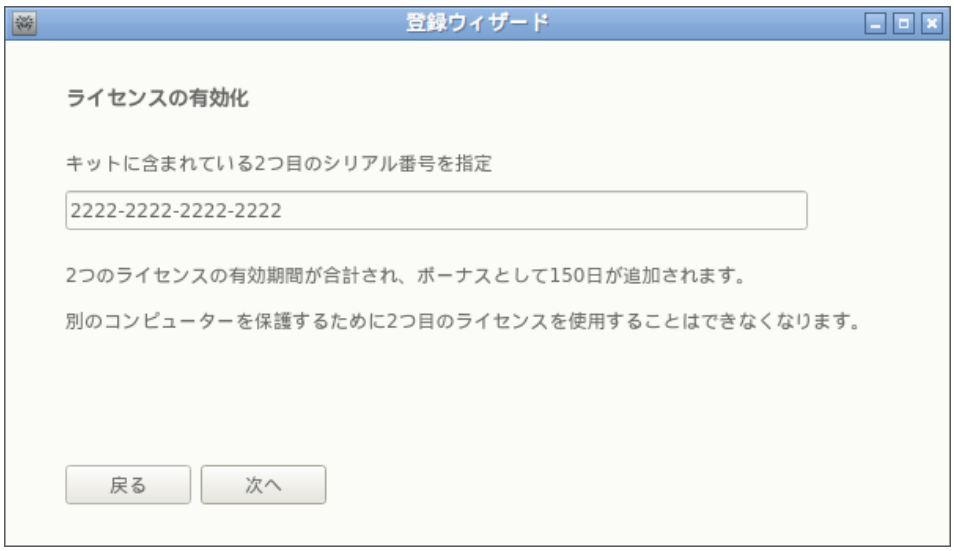

図 23. キットに含まれている2つ目のシリアル番号を指定

次のステップでは、ボーナスを受け取り、ライセンス期間を150日間延長するよう求められます。ボーナスを受け取るには、**前回のライセンスを指定** を選択します。ボーナスを受け取らない場合や、前回のライセンスを持っていない場合は、**前回のライセンスを持っていません** を選択してください。次に **次へ** をクリックします。

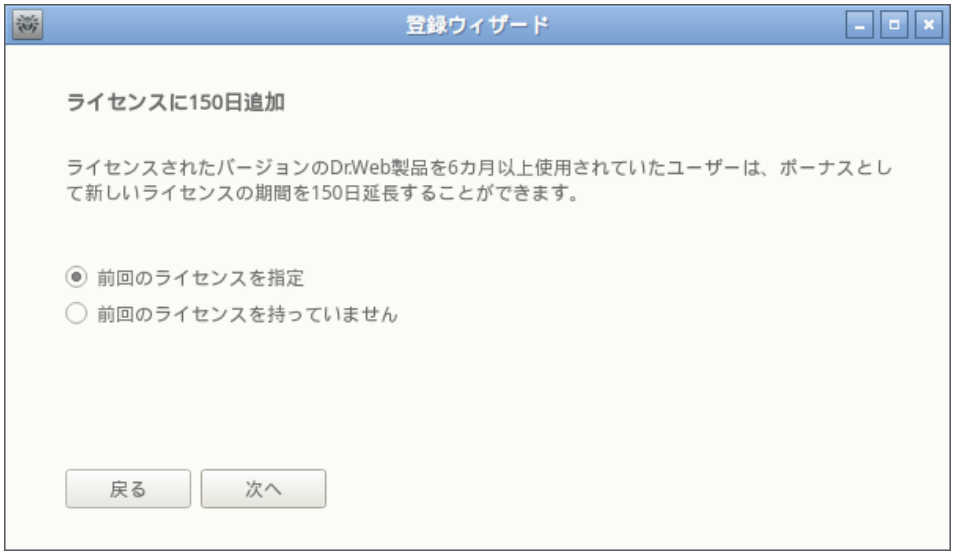

図 24. ボーナスのプロンプト

最初のステップで特別な *更新* シリアル番号を指定した場合、このステップでボーナスプロンプトは表示されません。代わりに、更新ライセンスの有効期間が150日短くなることのないよう、前回のライセンスを指定するように指示されます。このステップで **前回のライセンスを持っていません** を選択すると、新しいライセンスの有効期間が150日短くなります。

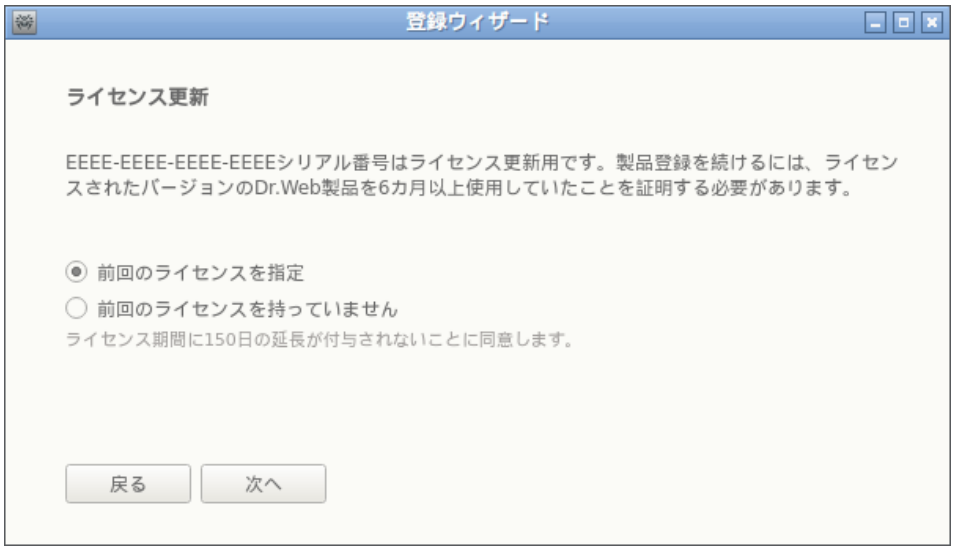

図 25. ライセンス更新

前回のライセンスを指定 を選択した場合、開いたウィンドウで、前回のライセンスのシリアル番号またはキーファイルを指定します。

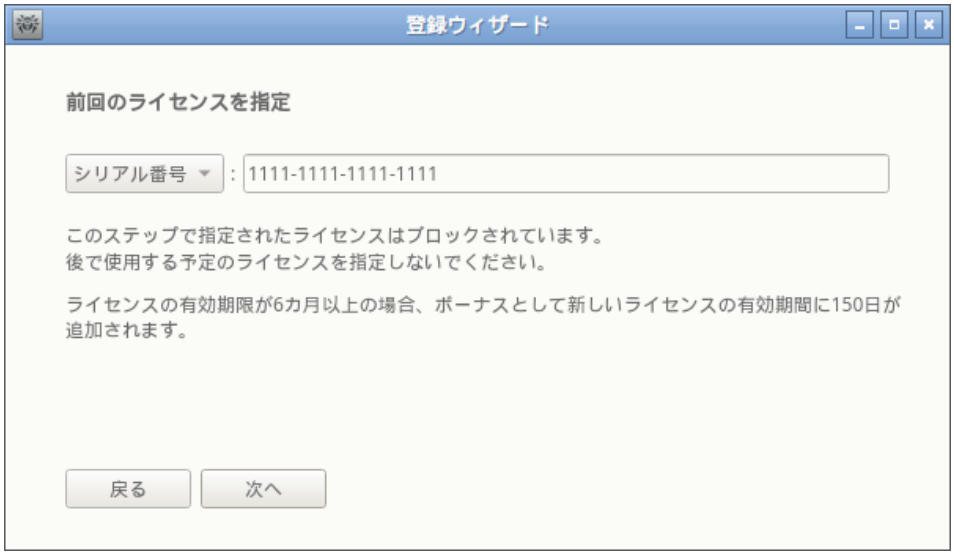

図 26. 前回のライセンスを指定する

期限の切れていないライセンスを指定した場合、新しいライセンスの有効期間に前回のライセンスの残りの期間が追加されます。2つのシリアル番号でライセンスを有効にした場合、使用可能なボーナスは前のステップで指定したオプションによって異なるものになります。

- **2台のコンピューター** を選択し、*このコンピューターが1台目* の場合。1台目のコンピューターに対して150日間のボーナスを有効にするには、このコンピューターに対して発行された前回のライセンスを指定します（ある場合）。*ここで2つ目のシリアル番号を指定しないでください。*
- **2台のコンピューター** を選択し、*このコンピューターが2台目* の場合。2台目のコンピューターに対して150日間のボーナスを有効にするには、このコンピューターに対して発行された前回のライセンスを指定します（ある場合）。*ここで1つ目のシリアル番号を指定しないでください。*
- **1台のコンピューター** を選択した場合。この場合、購入したライセンスの期間が2倍になるだけでなく、ライセンス期間も150日間延長されます。また、2台目のコンピューターに対して発行された前回のライセンスを指定した場合、新しいライセンスの2倍になった期間にさらに150日間が追加されます（前回のライセンスの残りの期間も追加されます）。

前回のライセンスを指定するには、該当するボックスにシリアル番号を入力するか、キーファイルを指定します。方法は、編集ボックスの左側にあるドロップダウンリストで該当するオプションを選択します。キーファイルを指定するには、次のいずれかの操作を行います。

- 入力フィールドでファイルへのパスを指定する
- **参照** をクリックして、ファイルを指定する
- ファイルをファイルマネージャーのウィンドウから登録ウィザードのウィンドウにドラッグ&ドロップする

キーファイルを展開せずに、キーファイルが含まれたzipアーカイブをそのまま指定できます。

登録を続けるには、**次へ** をクリックします。

次のステップで、以下を含む登録データを指定します。

- 登録名
- お住まいの地域（国）（リストから選択）
- 有効なメールアドレス

登録フォームのすべてのフィールドが必須です。

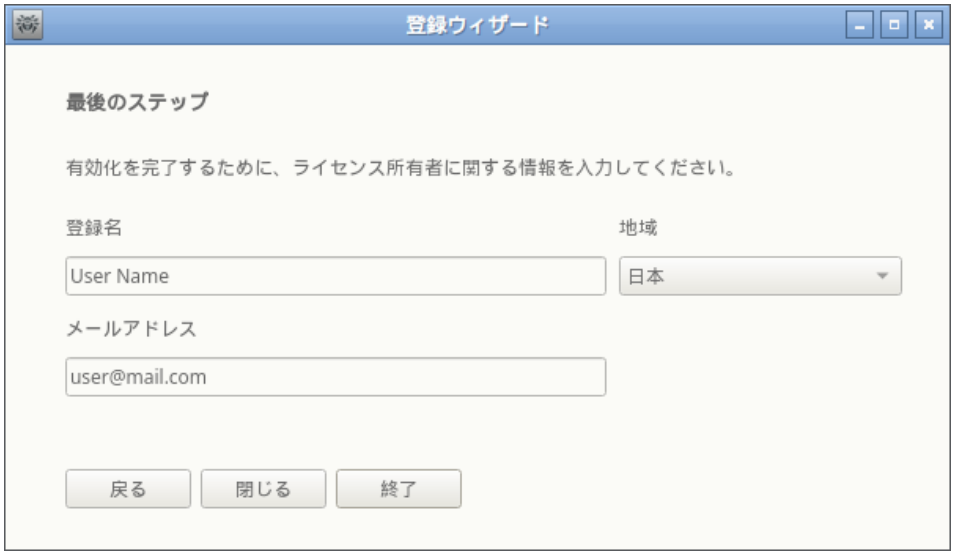

図 27. ユーザー情報ページ

すべてのフィールドが正しく入力されたら、**終了** をクリックしてサーバーとの接続を確立し、ライセンスキーファイルを取得します。必要に応じて、ライセンスキーファイルをこのコンピューターから 削除 した後に別のコンピューターで使用できます。

2. 試用期間を取得する

Dr.Web for Linuxコンポーネントのすべての機能を30日間お試しいただける試用期間を有効にする場合は、有効化の最初のステップでリンク**30日間の試用期間を有効化** をクリックします。

ライセンスマネージャーで1か月の試用期間を有効にする場合、個人データを提供する必要はありません。

3. 先に取得したキーファイルをインストールする

有効なライセンスと、関連するキーファイル（たとえば、Doctor WebまたはDoctor Webのパートナーからメールで入手したもの）を使用している場合は、そのキーファイルをインストールして、Dr.Web for Linuxを有効にできます。そのためには、最初のステップで **その他の有効化の種類** をクリックし、表示されたボックスにキーファイルへのパスを指定します。

図 28. キーファイルによる有効化

キーファイルを指定するには、次の操作を行います。

- 入力フィールドでファイルへのパスを指定する
- **参照** をクリックして、ファイルを指定する
- ファイルをファイルマネージャーのウィンドウから登録ウィザードのウィンドウにドラッグ&ドロップする

キーファイルを展開せずに、キーファイルが含まれたzipアーカイブをそのまま指定できます。

キーファイルへのパス（またはキーファイルを含むアーカイブへのパス）を指定したら、**終了** をクリックしてキーファイルを自動的にインストールします。必要に応じて、キーファイルが自動的に解凍され、Dr.Web for Linux ファイルのあるディレクトリにコピーされます。インターネットに接続する必要はありません。

有効化の手順が完了すると（選択した有効化の種類に関係なく）、該当するメッセージを含むウィザードの最終ページが表示されます。**OK** をクリックしてウィザードを終了し、Dr.Web for Linux の メインページ を開きます。

図 29. 有効化が成功したという通知

いずれかのステップでエラーが発生した場合、該当するメッセージとエラーに関する短い説明を含むページが表示されます。下図はそのようなページの例です。

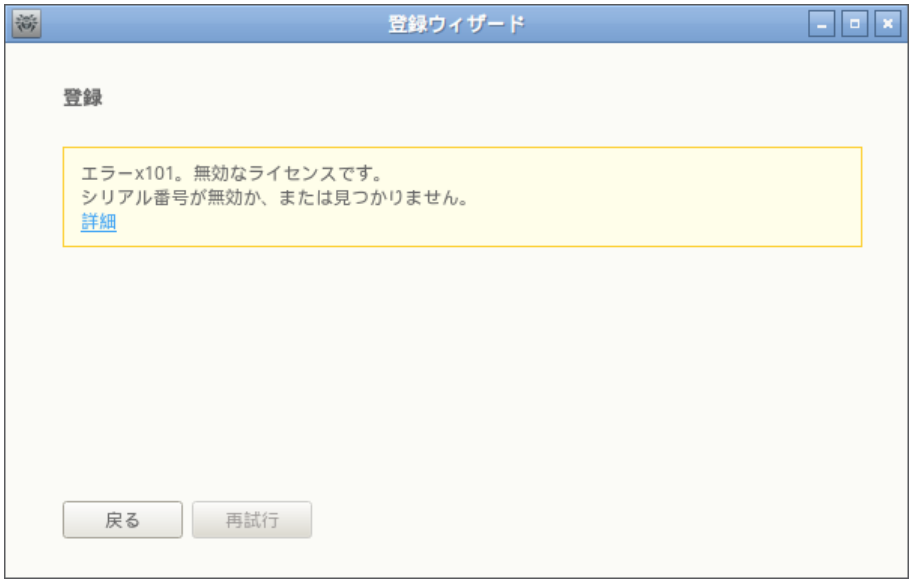

図 30. エラーメッセージ

エラーが発生した場合は、前のステップに戻って修正することたできます（たとえば、シリアル番号を修正する、正しいファイルパスを指定するなど）。前のステップに戻るには、**戻る** をクリックします。

一時的な問題（一時的なネットワーク障害など）が原因でエラーが発生した場合は、**再試行** をクリックすることで操作を再試行できます。必要であれば、**閉じる** をクリックして登録をキャンセルし、ウィザードを終了できます。この場合、後で登録手続きを再度実行する必要があります。シリアル番号を確認するためにウィザードがDoctor Web登録サーバーへの接続を確立できない場合は、以下のページが表示されます。

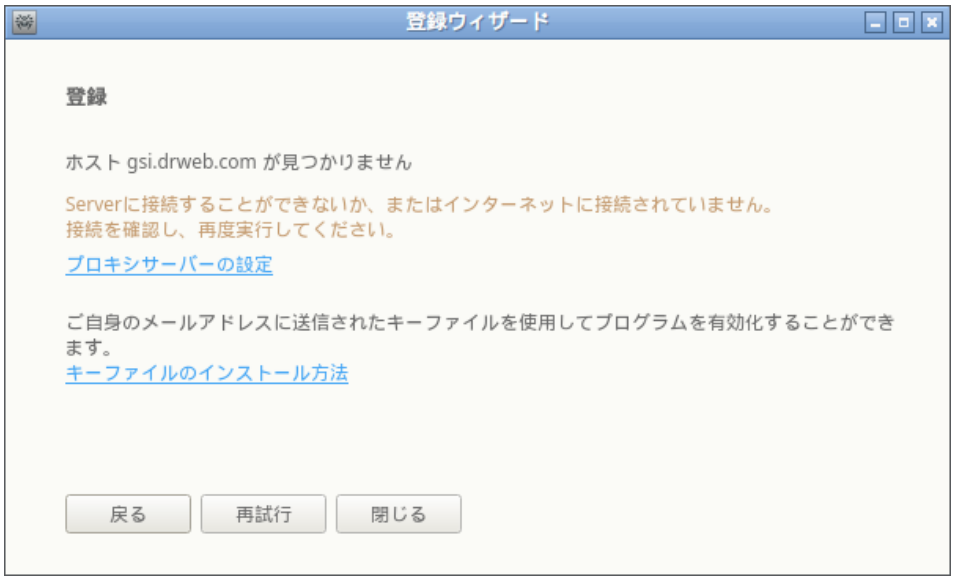

図 31. 登録サーバー接続エラー

コンピューターがインターネットへの直接接続を使用できないことが原因でエラーが発生し、プロキシサーバーを使用してインターネットにアクセスする場合は、**プロキシサーバーの設定** のリンクをクリックして、プロキシサーバー設定ウィンドウを開きます。

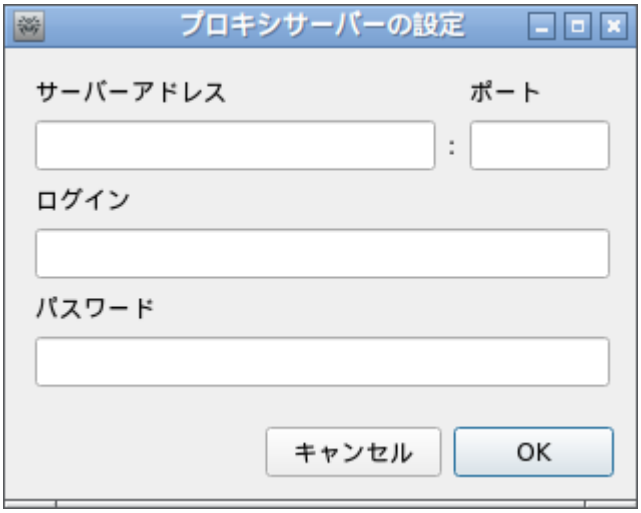

図 32. プロキシサーバーの設定

プロキシサーバーの設定を指定し、**OK** をクリックします。その後、**再試行** をクリックしてDoctor Web登録サーバーとの接続を再試行してください。

新しいライセンスを有効にして新しい キーファイル を生成すると、Dr.Web for Linuxで使用されていた前回のキーファイルが自動的にバックアップコピーとして `/etc/opt/drweb.com` ディレクトリに保存されます。必要に応じて、キーファイルを インストール することで再度使用できます。

ライセンスキーファイルを削除する

必要に応じて（Dr.Web for Linuxを別のコンピューターで使用する場合など）、Dr.Web for Linuxの動作を管理するインストールされたライセンスキーファイルを削除できます。そのためには、ライセンス情報 のページ（ライセンスマネージャーの開始ページ）を開き、現在のライセンス番号の横にある ✕ をクリックします。

その後、表示されたウィンドウで **はい** をクリックしてライセンスキーファイルの削除を確定してください。削除をキャンセルするには、**No** をクリックします。

図 33. ライセンスキーファイルを削除する前の確認ダイアログ

ライセンスキーファイルを削除するには、アプリケーションをスーパーユーザー権限で起動する必要があります。アプリケーションに昇格された権限がない場合、キーファイルを削除しようとしてもはいボタンを使用できません。必要に応じて 権限を昇格 してください。昇格に成功するとはいボタンが使用可能になります。

ライセンスキーファイルを削除しても、ライセンスの有効期間には影響しません。ライセンスの有効期限が切れていない場合は、残りの期間、このライセンスの新しいキーファイルを取得できます。

ライセンスキーファイルが削除されると、新しいライセンスまたは試用期間が有効になるまで、Dr.Web for Linuxのすべてのアンチウイルス機能(ファイルのスキャン、ウイルスデータベース、スキャンエンジン、Webリソースカテゴリデータベースの 更新、ファイルシステムの モニタリング)がブロックされます。

集中管理サーバーからのメッセージを見る

このセクションの内容:

- 概要
- メッセージに対してアクションを適用する
- メッセージをフィルタリングする

概要

Dr.Web for Linuxが集中管理サーバーに 接続されている 場合は、集中管理サーバーからワークステーションに送信されたアンチウイルスネットワークの状態に関するメッセージを見ることができます。アンチウイルスネットワーク管理者はツールを使用して、ネットワークの状態と集中管理サーバーの重要なイベントを監視できます。

ネットワークの状態とネットワークイベントに関するメッセージは、Dr.Web for Linuxが接続されている集中管理サーバーでアンチウイルスネットワーク管理者が該当する設定を行っている場合にのみワークステーションに送信されます。そうでない場合、メッセージを見ることはできず、Dr.Web for Linuxメインウィンドウには該当するページは表示されません。

サーバーからのメッセージを見るためのインターフェースは個別のページに表示されます。ページを開くには、ナビゲーションペイン で  をクリックします。

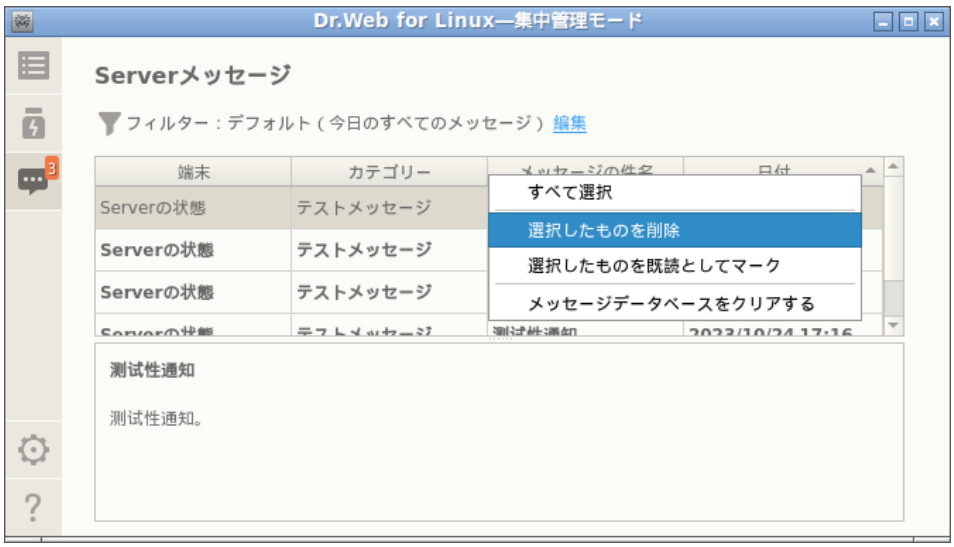

図 34. 集中管理サーバーメッセージのページ

リストでは、それぞれのメッセージについて以下の情報が表示されます。

- メッセージに示されているワークステーションの名前（アドレス）
- メッセージのカテゴリー
- メッセージのタイトル（件名）
- メッセージがサーバーによって送信された日時

メッセージを見るには、リストから該当するメッセージを選択してください。選択されたメッセージの本文が、メッセージリストの下のペインに表示されます。未読メッセージは太字で表示されます。

アンチウイルスネットワークの状態とイベントに関するメッセージは、集中管理サーバーの設定で指定されている言語で表示されます。

メッセージに対してアクションを適用する

メッセージにアクションを適用するには、該当するメッセージに関する情報が含まれた行内の任意の場所で右クリックし、表示されたドロップダウンメニューから必要なアクションを選択します。複数のメッセージに対して1つのアクションを適用する場合、該当する行を選択し、任意のエリアで右クリックします。複数の行を選択するには、CTRL キーまたは SHIFT キーを押したまま選択します。

- 離れた複数のメッセージを選択する場合は CTRL キーを押します。
- 連続する複数のメッセージを選択する場合は SHIFT キーを押します。

すべてのメッセージを選択する場合は CTRL+A キーを押します。

メニューには以下のアクションが含まれています。

- リスト内のフィルタリングされたメッセージをすべて選択する
- 選択したメッセージを削除する
- 選択したメッセージを既読にする
- メッセージデータベースをクリーンアップする

データベースをクリーンアップすると、受信したメッセージがすべて削除されます（未読メッセージも含む）。

集中管理サーバーから受信したメッセージは、設定 で指定されている最大保存期間が終了すると自動的に削除されますのでご注意ください。

メッセージをフィルタリングする

サーバーからは大量のメッセージが送信される場合があるため、送信元サーバーアドレス、アンチウイルスネットワークワークステーション名、メッセージカテゴリー、受信期間でそれらをフィルタリングすることができるようになっています。デフォルトで有効になっているフィルターでは、当日中にすべてのサーバーから受信したすべてのカテゴリーのメッセージが表示されます。

必要に応じて、フィルターを編集することができます。編集するには、リンク **編集** をクリックしてください。フィルターペインが上部に開きます。

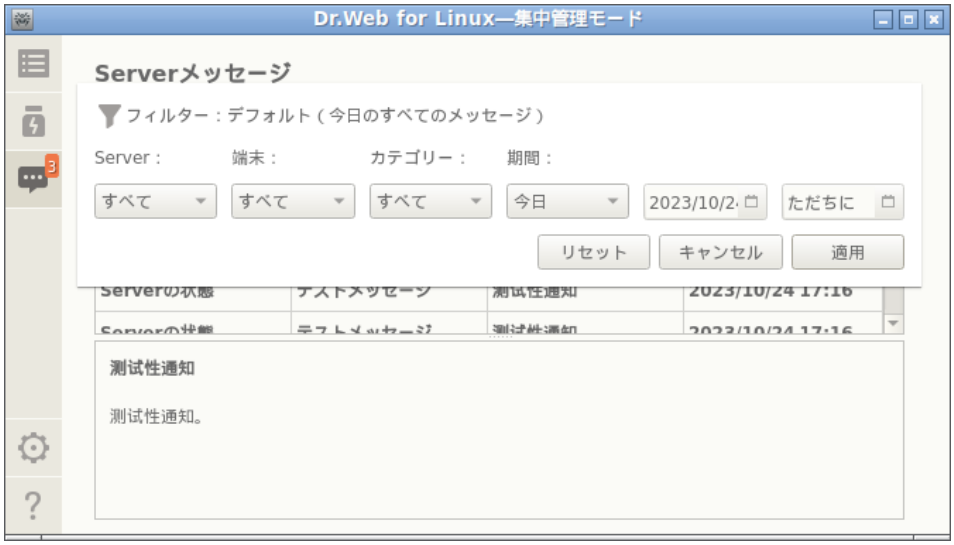

図 35. メッセージのフィルターペイン

フィルターペインでは、次のパラメータを指定できます。

- **Servers** - 表示するメッセージの送信元サーバーのリスト
- **端末** - 表示するメッセージが関連するワークステーションのリスト（そのワークステーションに関するメッセージを表示します）
- **カテゴリー** - 表示するメッセージのカテゴリー
- **期間** - 表示するメッセージの生成期間のリスト。リストから標準期間を選択することも、開始時と終了時を指定することもできます。

変更を保存するには、**適用** をクリックします。フィルターペインを閉じて変更内容を破棄するには、**キャンセル** をクリックします。フィルターをデフォルト値にリセットするには、**リセット** をクリックします。

アプリケーションの権限管理

Dr.Web for Linuxの一部の動作は、アプリケーションが *スーパーユーザー* 権限（*root* ユーザー）に相当する昇格した権限（*管理者権限*）を持っている場合のみグラフィカルモードで実行できます。そのような動作には以下のものがあります。

1. システムの隔離に移された（ユーザーディレクトリではなく隔離 ディレクトリ に）オブジェクトの管理
2. 他のユーザー（特にrootユーザー）の ファイルとディレクトリをスキャン
3. ファイルシステムモニターSpIDer Guardを 無効 にする
4. ネットワーク接続モニターSpIDer Gateを 無効 にする
5. ライセンスキーファイルの 削除、集中管理サーバーへの 接続とその接続の切断

> アプリケーションがrootユーザー（たとえば `su` または `sudo` コマンドを使用して）によって起動されていて場合であっても、デフォルトではアプリケーションは昇格した権限を付与されて *いません*。

昇格した権限を必要とするアクションのために開かれるすべてページに、ロックアイコンのついた特別なボタンが表示されます。アイコンはアプリケーションがスーパーユーザー権限を有しているかどうかを表しています。

	アプリケーションは昇格した権限を持っていません。権限をroot権限に昇格するにはアイコンをクリックします。
	アプリケーションはroot権限を持っています。権限を降格する（管理者権限からユーザー権限に）にはアイコンをクリックします。

権限を昇格するためにアイコンをクリックすると、ユーザー認証ウィンドウが開きます。

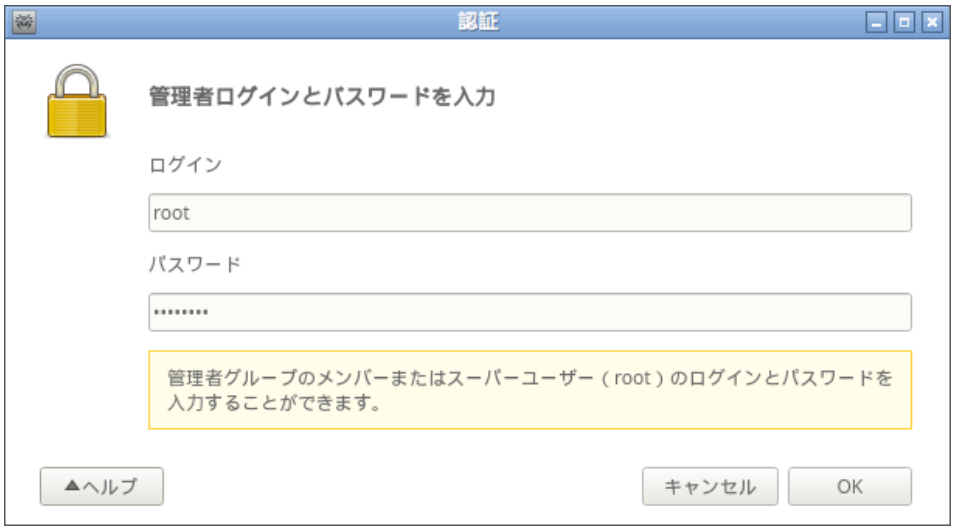

図 36.認証ウィンドウ

アプリケーションに管理者権限を付与するには、Dr.Web for Linuxの *管理者グループ* に含まれているユーザー、またはスーパーユーザー（システムアカウント *root*）の認証情報を指定し、**OK** をクリックします。権限の昇格をキャンセルするには **キャンセル** をクリックしてウィンドウを閉じます。**ヘルプ** ボタンをクリックすると、認証方法について説明する簡単なヘルプを表示したり非表示にしたりすることができます。

Dr.Web for Linuxのインストール中に、権限をスーパーユーザー権限に昇格することができるユーザーのグループ（たとえば *sudo* グループ）が管理者グループとして選択されます。そのようなグループを探す試みに失敗した場合は、認証ウィンドウでスーパーユーザーのログインとパスワード（*root*）を入力することで、アプリケーションの権限を昇格できます。

管理者権限からユーザー権限への切り替えには認証は必要ありません。

ヘルプと参照情報

ヘルプファイルにアクセスするには、Dr.Web for Linuxの ナビゲーションペイン で  を押します。

次のドロップダウンメニューが表示されます。

- **ヘルプ** - Dr.Web for Linux ユーザーマニュアルを開きます。
- **フォーラム** - Doctor WebフォーラムのWebページを開きます（有効なインターネット接続が必要です）。
- **テクニカルサポート** - Doctor WebテクニカルサポートのWebページを開きます（有効なインターネット接続が必要です）。
- **My Dr.Web** - Doctor Web公式サイト上のユーザー専用ページを開きます（有効なインターネット接続が必要です）。
- **詳細** - お使いのDr.Web for Linuxのバージョンに関する情報が含まれたウィンドウを開きます。

そのほか、Dr.Web for Linuxメインウィンドウのいずれかのページでエラーメッセージが表示された場合、**詳細** リンクをたどることで、エラーに関する情報と問題を解決するための手順を確認できます。

さらに、パラメータ値のリストに新しい値を追加するには、オプション-aを使用する必要があります（以下参照）。

動作設定

次のようなアプリケーションパラメータの設定

- 更新頻度
- Scannerによる リクエストに応じたスキャン 中に検出された脅威、また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 for Linuxのアクション
- ScannerおよびSpIDer Guardによるスキャンの対象から除外するオブジェクトのリスト
- ネットワーク接続モニタリングのパラメータ
- Scannerによって実行されるスキャンのスケジュール
- 保護モード（スタンドアローン、集中管理）
- Dr.Web Cloudサービスのクライアントを使用する

Dr.Web for Linux設定ウィンドウ内で行います。

このウィンドウを開くには、ナビゲーションバー で  をクリックします。

設定ウィンドウ内で以下のページを使用できます。

- メイン - 通知、または自動更新頻度の有効化と設定を行うことができます。
- Scanner - スケジュールまたはリクエストに応じたScannerによるスキャンで検出された脅威に対するDr.Web for Linuxのアクションを設定できます。
- SpIDer Guard - 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 for Linuxのアクションを設定することができます。
- SpIDer Gate - SpIDer Gateがどのようにネットワーク接続をコントロールするかを設定できます。
- 除外 - リクエストまたはスケジュールに応じたScannerによるスキャン、SpIDer Guardによる検査、SpIDer Gateによるモニタリングの対象から除外するオブジェクトのリストを設定できます。
- スケジューラ - 指定されたスケジュールに応じた定期的なスキャンを設定できます。
- ネットワーク - SpIDer Gateによる保護された接続（HTTPSなどのSSL/TLSによる接続）の検査を有効／無効にする、保護された接続を傍受するために使用されるDr.Web証明書をファイルに保存することができます。
- モード - Dr.Web for Linux動作の 保護モード（スタンドアローン、集中管理）を選択できます。
- Dr.Web Cloud - Dr.Web for LinuxがDr.Web Cloudサービスを使用することを有効または無効にできます。

ヘルプファイルを開くには、設定ウィンドウ内の該当するページ上で ? をクリックします。

これらのページ上で行われた設定の変更はすべて、直ちに適用されます。

Dr.Web for Linuxが エンタープライズモード で動作している場合、一部の設定はブロックされ、変更できない場合があります。

メイン設定

このセクションの内容：

- 概要
- 更新用のプロキシサーバーの設定

概要

メイン タブで、アプリケーションのメイン設定を行うことができます。

図 37. メインタブ

オプション	アクション
警告音を有効にする	次のような特定のイベントについて音声による通知を使用するにはチェックボックスにチェックを入れます。 • 脅威の検出（ScannerおよびSpIDer Guardによる） • オブジェクトのスキャンエラー • その他
ポップアップ通知を表示する	次のような特定のイベントについてポップアップ通知を使用するにはチェックボックスにチェックを入れます。 • 検出された脅威 • スキャンエラー • その他
通知ステータスを使用する	コンポーネントの状態を変更した際にポップアップ通知を表示するようにするにはチェックボックスにチェックを入れます。
更新をダウンロード	ウイルスデータベース、Webリソースカテゴリーデータベース、Dr.Web for Linuxスキャンエンジンの利用可能な更新をUpdaterによってチェックする頻度を選択します。
プロキシサーバー	更新を受け取るためのプロキシサーバー設定を行う場合にクリックします（外部サーバーへの接続がネットワークセキュリティポリシーによって禁止されている場合、Updaterはプロキシサーバーを使用します）。
デフォルト設定を復元	デフォルト設定を復元する場合にクリックします。

更新設定を管理し、デフォルト設定を復元するには、アプリケーションがroot権限を持っている必要があります。詳細については アプリケーションの権限管理 を参照してください。

更新用のプロキシサーバーの設定

Updaterが使用するプロキシサーバーを設定するウィンドウ内で以下を行うことができます。

- 更新を受け取る際のプロキシサーバーの使用を有効または無効にする
- 更新の受け取りに使用するプロキシサーバーのアドレスを指定する
- プロキシサーバーに接続するためのポートを指定する
- プロキシサーバーでの認証に使用するユーザー名とパスワードを指定する

図 38. プロキシサーバーの設定

サーバーアドレスには、IPアドレスのほか、私用するプロキシサーバーが動作するホストのFQDNを指定できます。サーバーアドレスとポートは必須パラメータです。更新にはHTTPプロトコルが使用されるため、HTTPプロキシサーバーを使用する必要があります。プロキシサーバーがインターネットアクセスに認証を必要とする場合のみ、ログインとパスワードを指定します。

変更を保存してウィンドウを閉じるには **OK** をクリックします。変更をキャンセルしてウィンドウを閉じるには **キャンセル** をクリックします。

ファイルスキャン設定

このセクションの内容:

概要

Scanner タブで、Scannerによる、ユーザーの リクエスト に応じた、またはスケジュールに応じた スキャンで検出された脅威に対するDr.Web for Linuxのアクションを設定できます。

図 39. Scanner設定タブ

ドロップダウンメニューで、該当する カテゴリー の脅威を検出した際にDr.Web for Linuxがオブジェクトに対して適用するアクション を選択します。

コンテナ（アーカイブ、メール添付ファイルなど）内のファイルで脅威が検出された場合は、削除アクションの代わりにコンテナの隔離への移動が実行されます。

脅威に対してアクションを自動的に適用 チェックボックスにチェックを入れることで、リクエストまたはスケジュールに応じたスキャン中にScannerによって検出された脅威に対して指定されたアクションを適用するよう Dr.Web for Linuxを設定できます（ユーザーは脅威の駆除について通知を受け、脅威に関する詳細が 脅威リスト に表示されます）。チェックボックスにチェックが入っていない場合、Scannerによって検出された脅威は「検出された脅威のリスト」に追加され、ユーザーは適用するアクションを手動で選択する必要があります。

ファイルスキャンのアドバンス設定ウィンドウを開くには、**アドバンス** をクリックします。

注意：

- **除外**タブ で、Scannerによるスキャンからファイルやフォルダを除外できます。
- Scannerについて設定された脅威検出時のアクションは（自動での適用を含む）、SpIDer Guardの動作には影響しません。SpIDer Guardの脅威検出時のアクションは 該当する タブで設定します。

脅威に対するScannerのアクションを変更し、アドバンス設定にアクセスするには、アプリケーションが昇格した権限で動作している必要があります。アプリケーションの権限管理を参照してください。

Dr.Web for Linuxが集中管理サーバーによって動作している場合、Scannerを設定するオプションは、それがサーバーで無効になっている場合はブロックされます。

Scannerのアドバンス設定

スキャンのアドバンス設定ウィンドウでは、Scannerの以下のパラメータを設定できます。

- コンテナのスキャンを有効／無効にする:
  - アーカイブ
  - メールファイル
- 1つのファイルのスキャンにかかる時間の上限を設定する

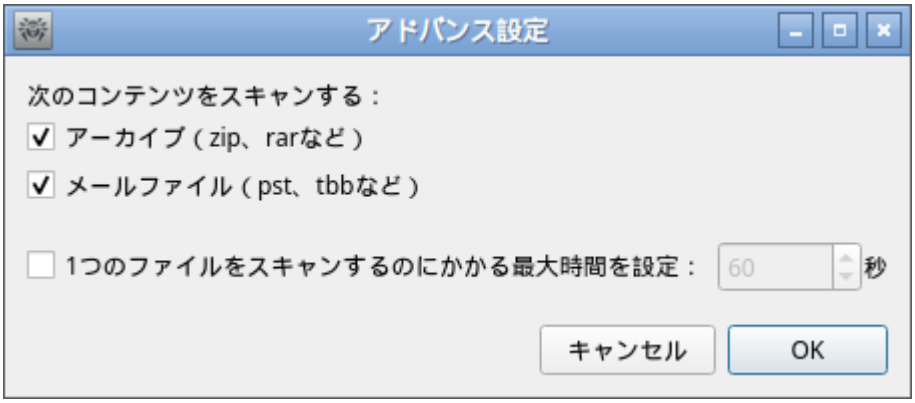

図 40. Scannerのアドバンス設定

コンテナのスキャンを有効にするチェックボックスにチェックが入っていない場合、コンテナファイル構造はScannerによってスキャンされますが、中に含まれているファイルはスキャンの対象から除外されます。

変更を保存してウィンドウを閉じるには **OK** をクリックします。変更をキャンセルしてウィンドウを閉じるには キャンセル をクリックします。

ファイルシステムモニタリングの設定

SpIDer Guard タブでは、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 for Linuxのアクションを設定できます。

図 41. ファイルシステムモニタリングの設定ページ

アドバンス設定を含むこのページは、Scanner設定（**Scanner** タブ）のページと同じです。

コンテナ（アーカイブ、メール添付ファイルなど）内のファイルで脅威が検出された場合は、削除アクションの代わりにコンテナの隔離への移動が実行されます。

注意：

- **除外**タブ で、SpIDer Guardによるモニタリングからファイルを除外できます。
- SpIDer Guardによる強化されたファイルモニタリングについては、ファイル監視モード を参照してください。
- SpIDer Guardについて設定された脅威検出時のアクションは、Scannerの動作には影響しません。Scannerの脅威検出時のアクションは 該当する ページで設定します。

ファイルシステムモニターSpIDer Guardの設定を変更するには、アプリケーションが昇格した権限で動作している必要があります。アプリケーションの権限管理 を参照してください。

Dr.Web for Linuxが 集中管理 サーバー によって動作している場合、SpIDer Guardを設定するオプションは、それがサーバーで無効になっている場合はブロックされます。

ネットワーク接続のモニタリング設定

このセクションの内容：

- 概要
- Webサイトのカテゴリーを選択する
- ファイルのスキャンパラメータを管理する

概要

SpIDer Gate タブでは、インターネットへのアクセス試行時にSpIDer Gateによって使用されるセキュリティポリシーを設定できます。

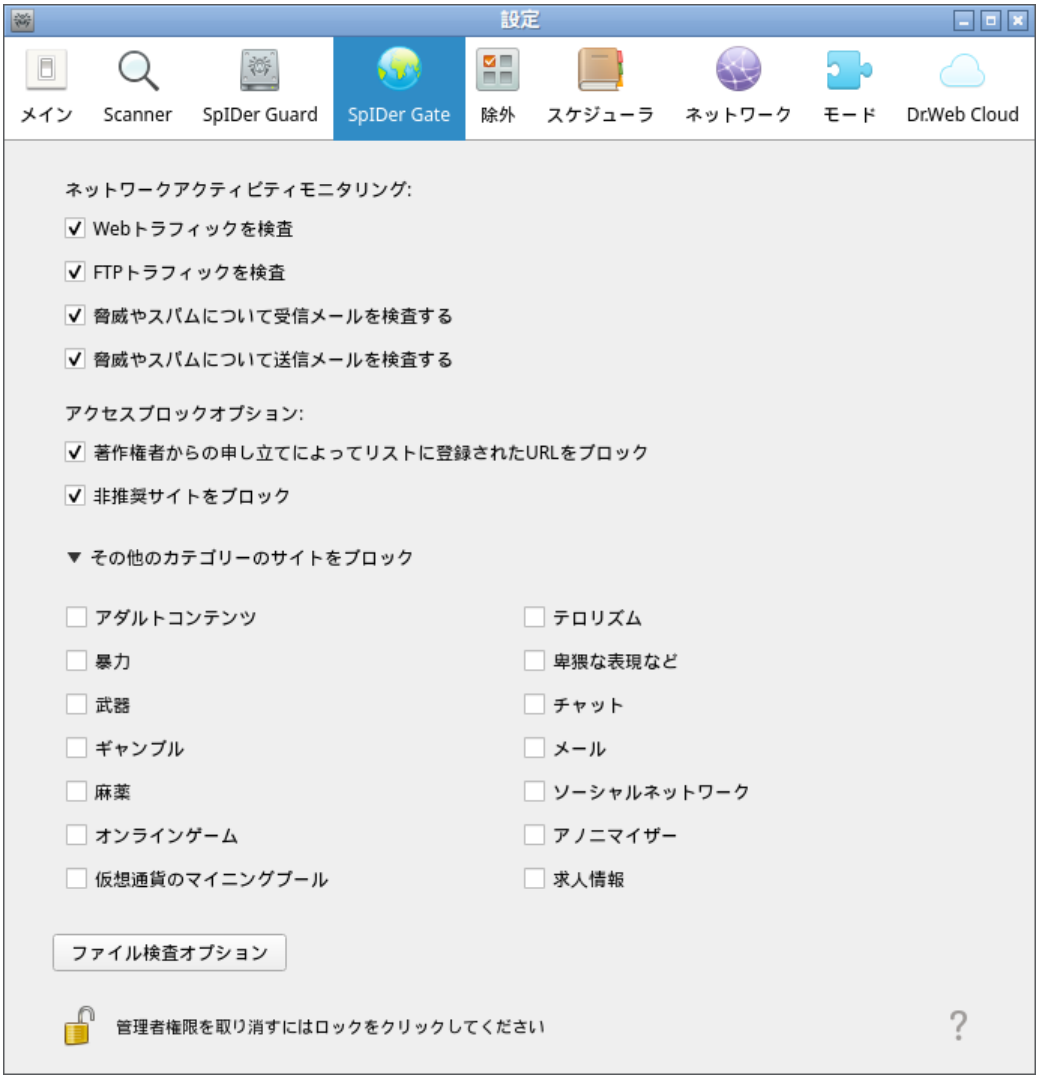

図 42. ネットワーク接続のモニタリング設定

ネットワークアクティビティモニタリング セクションのスイッチを選択／選択解除することで、モニターが制御するネットワークアクティビティの種類を指定できます（制御が 有効 になっている場合）

Webサイトのカテゴリーを選択する

モニタリングオプション セクションのスイッチはアクセスを制限するWebサイトとホストのカテゴリーを指定します（そのようなサイトへのブラウザからのアクセス試行のみでなく、FTPサーバーへのアクセス試行にも適用されます）。該当するスイッチャーを有効／無効にすることで、それぞれ以下のカテゴリーのWebサイトやホストへのアクセスを許可／禁止できます。

カテゴリー	説明
著作権者からの申し立てによってリストに登録されたURL	著作権を侵害するコンテンツが含まれたWebサイト（著作権所有者による）。そのようなWebサイトには、海賊版サイト、ファイルリファレンスディレクトリ、ファイルホスティングサービスなどが含まれます。
非推奨サイト	信頼性に欠けるコンテンツが含まれたWebサイト（フィッシング、パスワード盗難などが疑われる）です。
アダルトコンテンツ	アダルトコンテンツが含まれたWebサイトです。
暴力	暴力的な内容（戦争やテロリズムなど）が含まれたWebサイトです。
武器	武器や爆発物に関する情報が含まれたWebサイトです。
ギャンブル	インターネットカジノやギャンブル、賭け事のWebサイトです。
麻薬	麻薬の製造や販売、使用に関する情報が含まれたWebサイトです。
卑猥な表現	卑猥な言葉が含まれたWebサイトです。
チャット	チャットのWebサイトです。
テロリズム	テロリズムに関する情報が含まれたWebサイトです。
メール	無料のメール登録を提供するWebサイトです。
ソーシャルネットワーク	ソーシャルネットワーキングサイトです。
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サイトです。
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サイトです。
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サイトです。
求人情報	求人検索Webサイト。

Webリソースカテゴリーのデータベースは Dr.Web for Linuxと一緒に提供され、ウイルスデータベースの更新時に自動的に更新されます。ユーザーはデータベースを編集することはできません。

1つのWebリソースが複数のカテゴリーに含まれる場合があります。少なくとも1つの選択されたカテゴリーにURLが含まれている場合、SpIDer Gateはそこへのアクセスをブロックします。選択可能なカテゴリーのリストを簡易版または詳細版で表示するには **その他のカテゴリーのサイトをブロック** ラベルをクリックします。

いずれのカテゴリーにも該当しないWebサイトまたはホストへのアクセスをブロックする場合、それらをユーザーのブラックリストに追加します。上のカテゴリーのいずれかに含まれており、望ましくないとされているWebサイトやホストへのアクセスを許可する場合は、それらをユーザーのホワイトリストに追加します。必要に応じ、SpIDer Gateによってネットワーク接続を監視しないアプリケーションのリストを設定することもできます。

SpIDer Gateによるモニタリングについての、Webサイトやアプリケーションのブラックリストとホワイトリストは **除外** タブ で設定できます。

感染源として知られているWebサイト のカテゴリーに属するWebサイトやホストについては、それらがホワイトリストに追加されている場合であっても、そこへのアクセスは常に無効になります。

ファイルのスキャンパラメータを管理する

SpIDer Gateがインターネットからダウンロードされるファイルをスキャンする際のパラメータを設定するには、**ファイル検査オプション** をクリックします。

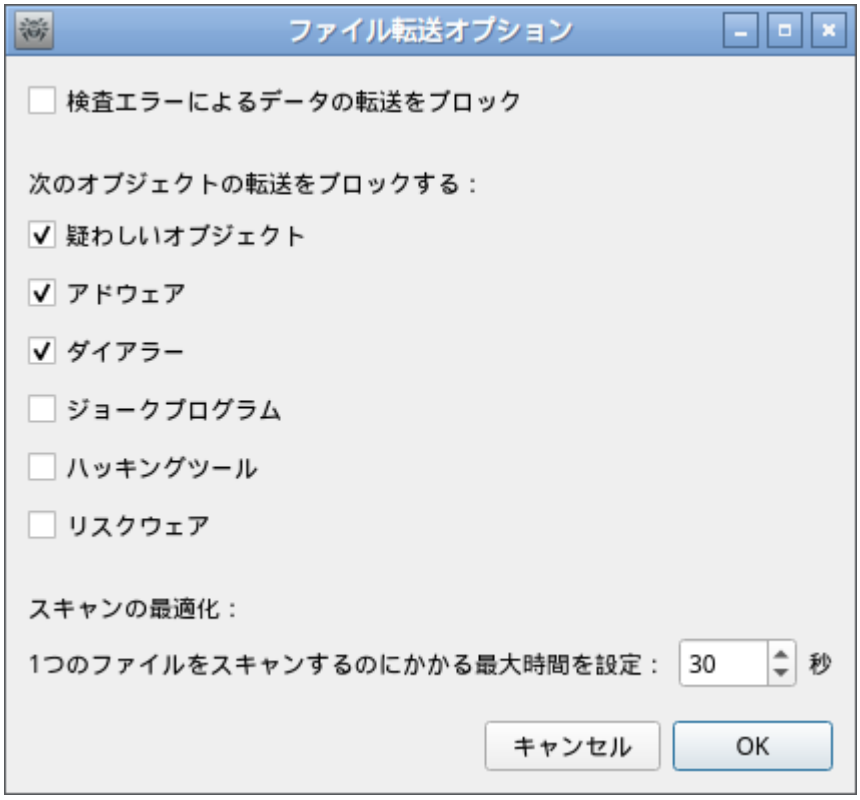

図 43. ファイルのスキャン設定ウィンドウ

表示されたウィンドウ内で、それらの送信が試みられた際にブロックする悪意のあるオブジェクトのカテゴリーを指定できます。チェックボックスにチェックが入っている場合、そのカテゴリーに当てはまるファイルは、ダウンロード時にブロックされます。チェックボックスにチェックが入っていない場合、そのカテゴリーに当てはまるファイルはダウンロードできます。また、ダウンロードするファイルのスキャンにかかる時間の上限を設定することもできます。**検査エラーによるデータの転送をブロック** チェックボックスが選択されている場合、エラーによってスキャンできなかったファイルはブロックされ、ダウンロードできません。そのようなファイルのダウンロードを許可するには、チェックボックスのチェックを外します（推奨されません）。

ダウンロードするファイルのスキャンが、指定された時間の上限を超えたために失敗した場合、そのようなファイルは **検査エラーによるデータの転送をブロック** チェックボックスにチェックが入っている場合であっても未検査として *扱われず*、ブロックされません。

変更を保存してウィンドウを閉じるには **OK** をクリックします。変更をキャンセルしてウィンドウを閉じるには キャンセル をクリックします。

SpIDer Gateの設定を変更するには、アプリケーションが昇格した権限で動作している必要があります。アプリケーションの権限管理 を参照してください。

除外設定

除外 ページには、除外設定用の以下のボタンがあります。

- ファイルとディレクトリ - ScannerおよびSpIDer Guardによるスキャンの対象から除外するファイルシステムオブジェクトへの パスを指定 するためのウィンドウを開きます。
- **Web**サイト - SpIDer Gateによって適用される ポリシー に関係なくアクセスを制限するWebサイトの ブラックリストとホワイトリスト を管理するウィンドウを開きます。
- アプリケーション - ネットワーク接続をSpIDer Gateによってコントロールしない アプリケーションを指定 するためのウィンドウを開きます。

図 44. 除外設定ページ

除外リストにオブジェクトを追加、または除外リストからオブジェクトを削除するには、アプリケーションが昇格した権限で動作している必要があります。アプリケーションの権限管理 を参照してください。

ファイルとディレクトリの除外

このセクションの内容:

概要

ファイルとディレクトリ ウィンドウ内で、スキャンの対象から除外するファイルとフォルダのリストを管理できます。ウィンドウを開くには、**除外** タブ にある **ファイルとディレクトリ** をクリックします。

このウィンドウで、ユーザーの リクエスト や スケジュール に応じたScannerによるスキャン、ならびにSpIDer Guardによる モニタリング の対象から除外するオブジェクトへのパスをリストアップできます。

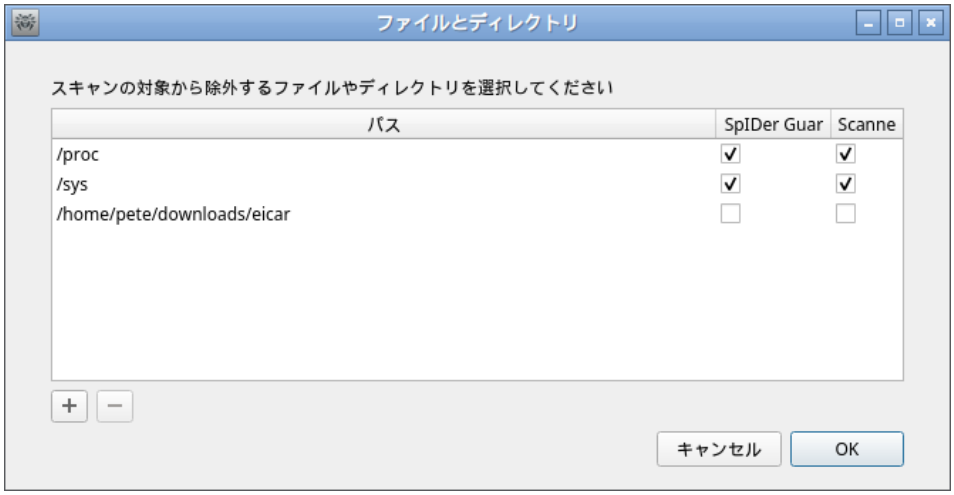

図 45. ファイルとフォルダの除外設定

Scannerによるスキャン（リクエストまたはスケジュールに応じた）とファイルシステムモニターSpIDer Guardによるモニタリングから、同一のオブジェクトを除外できます。該当するカラム内のチェックボックスで、そのオブジェクトがどの除外グループに追加されているかが分かります。

除外リストにオブジェクトを追加する、または除外リストからオブジェクトを削除する

- オブジェクトをScannerまたはSpIDer Guardの除外グループに追加するには、オブジェクトの行内にある該当するチェックボックスを選択してください。オブジェクトをリストから削除するには、該当するチェックボックスのチェックを外します。
- リストにオブジェクトを追加するには、リスト下にある ＋ ボタンをクリックし、表示されたウィンドウ内でオブジェクトを選択してください。ファイルマネージャーウィンドウからオブジェクトをドラッグすることでリストに追加することもできます。
- リストからオブジェクトを削除するには、テキスト内で該当する行を選択し、リスト下の − ボタンをクリックします。

変更を保存してウィンドウを閉じるには **OK** をクリックします。変更をキャンセルしてウィンドウを閉じるには **キャンセル** をクリックします。

アプリケーションの除外

このセクションの内容：

概要

ネットワーク接続モニターSpIDer Gateによるモニタリングの対象から、アプリケーションのネットワーク接続を除外できます。**除外** タブ にある **アプリケーション** ボタンをクリックすることで **アプリケーション** ウィンドウを開いてください。

このウィンドウで、ネットワーク接続をSpIDer Gateによって コントロール しないアプリケーションの実行ファイルへのパスをリストアップできます。

図 46. ネットワークアプリケーションの除外設定

除外リストにアプリケーションを追加する、または除外リストからアプリケーションを削除する

- リストにアプリケーションを追加するには、リスト下にある ＋ ボタンをクリックし、表示されたウィンドウ内でアプリケーション実行ファイルを選択してください。ファイルマネージャーウィンドウから実行ファイルをドラッグすることでアプリケーションをリストに追加することもできます。
- リストからアプリケーションを削除するには、テキスト内で該当する行を選択し、リスト下の − ボタンをクリックします。

変更を保存してウィンドウを閉じるには **OK** をクリックします。変更をキャンセルしてウィンドウを閉じるには **キャンセル** をクリックします。

Webサイトのブラックリストとホワイトリスト

このセクションの内容：

概要

リスト管理 ウィンドウ内で、Webサイトのブラックリストとホワイトリストを管理できます。ウィンドウを開くには、**除外** タブ にある **Webサイト** をクリックします。

このウィンドウで、アクセスをネットワーク接続モニターSpIDer Gateによって常に無効にする、または常に有効にするWebサイトをリストアップできます。

図 47. ブラックリストとホワイトリストの管理ウィンドウ

感染源として知られているWebサイト のカテゴリーに属するWebサイトについては、それらがホワイトリストに追加されている場合であっても、そこへのアクセスは常に無効になります。

Webサイトをブラックリストとホワイトリストに追加する、またはブラックリストとホワイトリストから削除する

- Webサイトをブラックリストまたはホワイトリストに追加するには、編集ボックスにそのドメインを入力し、それぞれのボタンをクリックします。
  - **許可** ボタンをクリックすると、アドレスが *ホワイト* リストに追加されます。
  - **ブロック** ボタンをクリックすると、アドレスが *ブラック* リストに追加されます。
- ドメインアドレスをホワイトリスト／ブラックリストに追加することで、ドメイン内のすべてのリソースへのアクセスが、それぞれ許可／禁止されます。
- Webサイトをブラックリストまたはホワイトリストから削除するには、リスト上で該当するサイトを選択し、**削除** ボタンをクリックします。

変更を保存してウィンドウを閉じるには **OK** をクリックします。変更をキャンセルしてウィンドウを閉じるには **キャンセル** をクリックします。

スケジューラの設定

このセクションの内容：

概要

スケジューラ タブでは、オブジェクトをスケジュールに応じて自動的にスキャンするオプションを有効にできるほか、そのスケジュールを設定し、スキャンの種類を選択できます。

図 48. スケジュール設定ページ

スケジュールによる自動スキャンを有効にするには、**スケジュールされたスキャンを実行** チェックボックスにチェックを入れます。この場合、Dr.Web for Linuxは定期的に特定の種類のスキャンを開始するスケジューラのタスクを作成します。

スケジュールスキャンは、通知エージェントによって、またはスキャン開始時に起動している場合は管理用グラフィカルインターフェイスによって直接、指定された間隔で開始されます。Dr.Web for Linuxが 集中管理 サーバーによるコントロール下で動作している場合、または有効な ライセンス が見つからない場合、スケジュールによるスキャンは実行されません。

スケジュールによるスキャンおよび オンデマンド でのスキャンは、**Scanner**タブ で指定された内容で設定されます。

スケジューラの設定

スケジュールによるスキャンが有効になっている場合、以下のパラメータを設定できます。

- スキャンを開始する曜日を選択する（該当するチェックボックスにチェックを入れます）
- スキャンを開始する時間（時と分）を設定する
- スキャンの種類（*クイックスキャン*、*フルスキャン*、*カスタムスキャン*）を選択します。
- *カスタムスキャン* を選択する場合、スキャンするオブジェクトのリストも設定します。それを行うには、**スキャンするオブジェクト** ボタンをクリックします（スキャンするオブジェクトの数が括弧内に表示されます）。

  その後、オンデマンドでのカスタムスキャンの ファイル選択ダイアログ と同様のウィンドウ内で必要なオブジェクトを選択してください。リストにオブジェクトを追加するには、＋ ボタンをクリックするか、ファイルマネージャーウィンドウからオブジェクトをドラッグ&ドロップします。

スケジュールによるスキャンを無効にするには、**スケジュールされたスキャンを実行** チェックボックスのチェックを外します。通知エージェントの該当するタスクが自動的に削除されます。

ネットワークを介して拡散される脅威に対する保護

このセクションの内容:

概要

ネットワーク タブで、SSLおよびTLSベースのプロトコルを使用する安全な接続を介したトラフィックに対する、ネットワーク接続モニターSpIDer Gateによるスキャンを有効にできます。

図 49. 安全な接続の検査設定タブ

保護された接続のスキャンを設定する

SSLおよびTSLプロトコルを使用して保護されたトラフィックから送信されたトラフィックをSpIDer Gateでスキャンすることを許可するには、**安全なSSL/TLS通信のトラフィックを検査する** チェックボックスを選択します。保護されたトラフィックのスキャンを無効にするには、チェックボックスのチェックを外します。

保護されたトラフィックのスキャンを管理するには、アプリケーションが昇格した権限で動作している必要があります。アプリケーションの権限管理 を参照してください。

メッセージの受信にIMAPを使用しているメールクライアント（Mozilla Thunderbirdなど）がシステムで実行されている場合は、**安全なSSL/TLS通信のトラフィックを検査する** モードを有効にしてから再起動します。

保護されたネットワーク接続を介して転送されるトラフィックのスキャンが正しく行われるようにするため、特別なDr.Web証明書をファイルにエクスポートし、保護された接続を使用する信頼するアプリケーションの証明書のリストに手動で追加してください。そのようなアプリケーションは主にWebブラウザとメールクライアントになります。Dr.Web証明書が信頼するリストに追加されていない場合、HTTPS経由でアクセス可能なWebサイトから受け取ったデータは正常に表示されません（たとえば、オンラインバンキングサイト、メールサーバーのWebインターフェースなど）。Dr.Web証明書がメールクライアントの信頼する証明書のリストに追加されていない場合、データ転送に保護されたプロトコルを使用する（SMTPSなど）メールサーバーでの認証は失敗します。

Dr.Web証明書をファイルにエクスポートするには、**Dr.Web証明書を保存** ボタンをクリックし、開いたウィンドウでファイルの保存先を指定してください。デフォルトのファイル名は `SpIDer Gate Trusted Root Certificate.pem` ですが、必要に応じて変更できます。

次に、保存したDr.Web証明書のファイルを、保護された接続の確立を試みる際に失敗するアプリケーションの信頼する証明書のリストに手動で追加します。1つのアプリケーションに対して証明書を追加する必要があるのは1回のみです。**ネットワーク** 設定で **安全なSSL/TLS通信のトラフィックを検査する** チェックボックスをオフにして再度チェックを入れる場合、改めてDr.Web証明書を保存して信頼する証明書のリストに追加する必要はありません。

Dr.Web証明書を信頼する証明書のリストに追加する

Mozilla Firefoxブラウザ

1) メインメニューで **設定** を選択し、表示された設定ページで **アドバンス** を選択します。また別のページが開きます。そこで、**証明書** を選択してください。
2) **証明書を表示** ボタンをクリックします。表示されたウィンドウで **認証局証明書** タブを開き、**インポート** をクリックします。
3) 開いたウィンドウ内でDr.Web証明書（デフォルトのファイル名は `SpIDer Gate Trusted Root Certificate.pem`）へのパスを指定し、**開く** をクリックします。
4) 開いたウィンドウ内で、チェックボックスを使用して、必要な証明書の信頼レベルを指定してください。3つのチェックボックスすべてにチェックを入れることが推奨されます（Webサイトの識別、メールユーザーの識別、ソフトウェアの識別）。その後、**OK** をクリックします。
5) 信頼する証明書のリスト内に、新しいセクション *DrWeb* が表示されます。このセクションには、追加された証明書が含まれています（デフォルトでは*SpIDer Gate Trusted Root Certificate*）。
6) **OK** をクリックして証明書のリストがあるウィンドウを閉じ、ブラウザ設定のページを閉じてください（ブラウザタブバーの該当するタブを閉じることで）。

Mozilla Thunderbirdメールクライアント

1) メインメニューで **設定** を選択し、表示された設定ページで **アドバンス** をクリックします。また別のページが開きます。そこで、**証明書** を選択してください。
2) **証明書を表示** ボタンをクリックします。表示されたウィンドウで **認証局証明書** タブを開き、**インポート** をクリックします。
3) 開いたウィンドウ内でDr.Web証明書（デフォルトのファイル名は `SpIDer Gate Trusted Root Certificate.pem`）へのパスを指定し、**開く** をクリックします。
4) 開いたウィンドウ内で、チェックボックスを使用して、必要な証明書の信頼レベルを指定してください。3つのチェックボックスすべてにチェックを入れることが推奨されます（Webサイトの識別、メールユーザーの識別、ソフトウェアの識別）。その後、**OK** をクリックします。
5) 信頼する証明書のリスト内に、新しいセクション *DrWeb* が表示されます。このセクションには、追加された証明書が含まれています（デフォルトでは*SpIDer Gate Trusted Root Certificate*）。
6) **OK** をクリックして証明書のリストがあるウィンドウを閉じ、**閉じる** をクリックしてメールクライアントの設定ページを閉じてください。
7) メールクライアントを再起動させてください。

コマンドライン経由でDr.Web証明書を信頼する証明書のリストに追加する

グラフィカルユーザーインターフェイスのほかに、コマンドラインを使用してDr.Web証明書を追加することもできます。証明書を生成するには、次のコマンドを実行します（PEM形式の証明書を保存する名前を指定する必要があります）：

```
$ drweb-ctl certificate > <cert_name>.pem
```

次に、証明書をシステムストレージに追加します。この操作には、Linuxディストリビューションに応じて異なるコマンドを使用します。Ubuntu、Debian、Mintの場合：

```
# cp <cert_name>.pem /etc/ssl/certs/
# c_rehash
```

CentOS、Fedoraの場合：

```
# cp <cert_name>.pem /etc/pki/ca-trust/source/anchors/
# update-ca-trust extract
```

モード設定

このセクションの内容：

概要

モード タブで、Dr.Web for Linuxを集中管理サーバーに接続したり（集中管理 モード を有効化）、集中管理サーバーとの接続を切断したり（Dr.Web for Linuxはスタンドアローンモードで動作）できます。

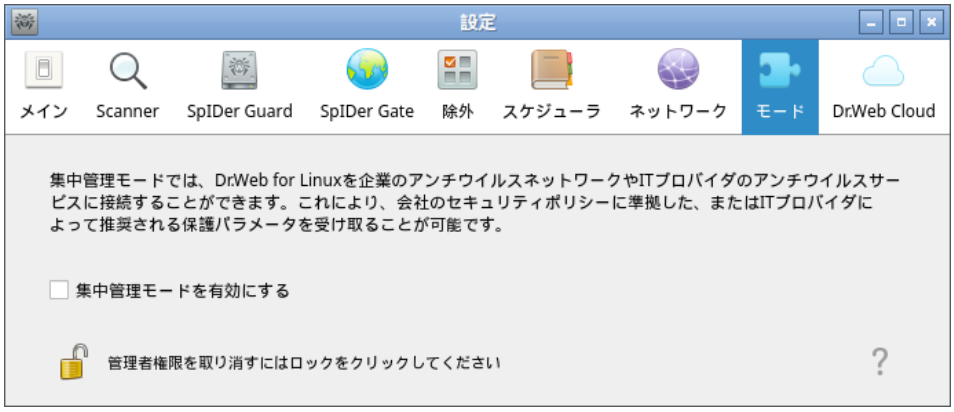

図 50. モードタブ

Dr.Web for Linuxを集中管理サーバーに接続、または集中管理サーバーとの接続を切断するには、該当するチェックボックスを使用します。

Dr.Web for Linuxを集中管理サーバーに接続、または集中管理サーバーとの接続を切断するには、アプリケーションが昇格した権限を持っている必要があります。アプリケーションの権限管理 を参照してください。

集中管理サーバーとの接続

集中管理サーバーとの接続を試行するための、接続パラメータのウィンドウが表示されます。

図 51. 集中管理サーバーに接続する

ウィンドウ上部のドロップダウンリストから、集中管理サーバーとの接続方法を1つ選択します。3つの方法があります。

- *ファイルから読み込む*
- *手動で設定*
- *自動で検出*

ファイルから読み込む を選択した場合、該当するボックス内で接続設定ファイルへのパスを指定します。*手動で設定* を選択した場合、集中管理サーバーのアドレスとポートを指定します。*手動で設定* または *自動で検出* では、証明書ファイル（ネットワーク管理者またはインターネットサービスプロバイダーから提供された）へのパスを指定する必要があります。

また、**認証** セクションで集中管理サーバーでの認証用のログイン（ワークステーション識別子）とパスワードを指定することもできます（分かっている場合）。これらが入力されている場合、集中管理サーバーへの接続は、正し

い識別子／パスワードが入力された場合のみ成功します。これらのフィールドが空の場合、集中管理サーバーへの接続は、それが集中管理サーバーによって許可された場合のみ確立されます（サーバーの設定に応じて、自動で、またはアンチウイルスネットワーク管理者によって）。

さらに、ワークステーションを「**新規端末**」として接続 オプションを使用できます（新規ユーザーとして接続するため）。集中管理サーバー上でこのオプションが許可されている場合、接続が許可された後、サーバーはユニークな識別子／パスワードの組み合わせを自動的に生成します。これらは、お使いのコンピューターをサーバーに接続する際に使用します。このモードでは、ホストがサーバー上ですでにアカウントを作成している場合であっても、集中管理サーバーはホストに対して新しいアカウントを生成するという点に注意してください。

アンチウイルスネットワーク管理者またはサービスプロバイダーによって提供された指示に厳密に従って接続パラメータを指定してください。

サーバーに接続するには、すべてのパラメータを指定し、**接続** をクリックして接続が確立されるのを待ちます。接続を確立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。

Dr.Web for Linuxを集中管理サーバーに接続した後、動作モードがスタンドアローンに切り替えられるまで、プログラムはサーバーによって管理されます。集中管理モードでは、OSが起動する度にサーバーとの接続が自動的に確立されます。詳細については 動作モード を参照してください。

ユーザーによるオンデマンドでのスキャンの実行が集中管理サーバーで禁止されている場合、Dr.Web for Linuxウィンドウの スキャン開始ページ および **Scanner** ボタンは無効になります。また、この場合、Scannerはスケジュールで設定されているスキャンを実行しません。

アドバンス設定

サーバーメッセージの最大保存時間 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の状態やワークステーションが集中管理サーバーから受信したイベントに関する メッセージ の最大保存期間を選択できます。メッセージが未読の場合でも、保存期間が過ぎるとそれらは自動的に削除されます。

アンチウイルスネットワークの状態とイベントに関するメッセージは、Dr.Web for Linuxが接続されている集中管理サーバーでアンチウイルスネットワーク管理者がワークステーションに対するメッセージの送信を設定している場合にのみ受信されます。それ以外の場合、メッセージを表示することはできず、保護モードの設定ページに **サーバーメッセージの最大保存時間** ドロップダウンリストは表示されません。

Dr.Web Cloudの設定

Dr.Web Cloud タブで、Dr.Web for LinuxがDr.Web Cloudサービスを使用することを有効または無効にできます。

Dr.Web Cloudは、Doctor Web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、アンチウイルスコンポーネントの使用する情報は最新のものではなくなっている場合があります。Cloud Serviceは、ユーザーが望ましくないWebサイトを開くことを確実に防ぎ、感染したファイルからお使いのシステムを保護します。

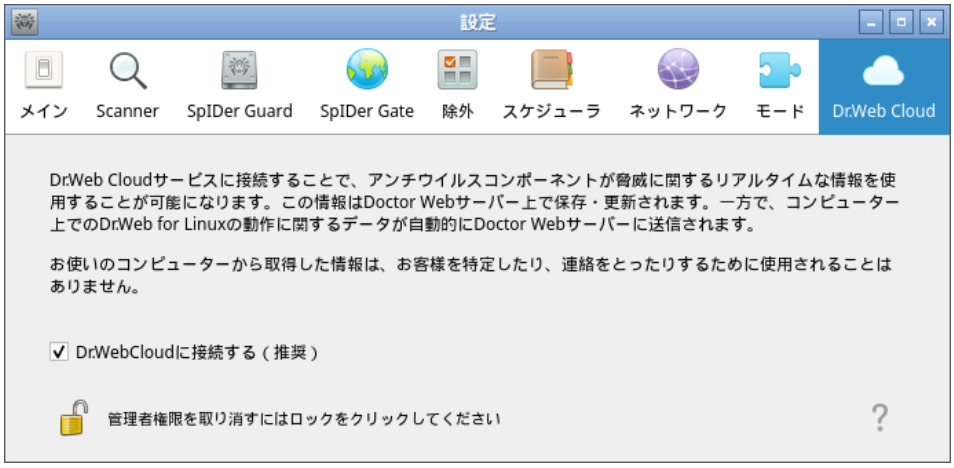

図 52. Dr.Web Cloudタブ

Dr.Web for LinuxがDr.Web Cloudサービスを使用することを有効または無効にするには、該当するチェックボックスを選択またはクリアします。

Dr.Web Cloudサービスとのインタラクションには、アクティブなインターネット接続が必要です。

Dr.Web for LinuxがDr.Web Cloudサービスを使用することを有効または無効にするには、アプリケーションが昇格した権限を持っている必要があります。アプリケーションの権限管理を参照してください。

追加情報

コマンドライン引数

オペレーティングシステムのコマンドラインからDr.Web for Linux GUI を起動するには、次のコマンドを使用します。

```
$ drweb-gui [<path>[ <path> …] | <parameters>]
```

<path> はスキャンの対象となるパスです。空白で区切って複数のパスを指定できます。

また、次のパラメータを指定することもできます（*<parameters>*）：

- `--help (-h)` - サポートされているコマンドラインパラメータに関する情報を表示し、GUIの動作を終了します。
- `--version (-v)` - GUIのバージョンに関する情報を表示します。
- `--Autonomous (-a)` - Dr.Web for Linux GUIの自律コピーを実行します。
- `--FullScan` - Dr.Web for Linux GUIの起動時にフルスキャンを開始します。
- `--ExpressScan` - Dr.Web for Linux GUIの起動時にクイックスキャンを開始します。
- `--CustomScan` - Dr.Web for Linux GUIの起動時にカスタムスキャンを開始します（スキャンするオブジェクトを選択するページが開きます）。

例:

```
$ drweb-gui /home/user/
```

Dr.Web for Linux GUIを起動し、指定されたディレクトリ内のファイルのScannerによるスキャンを開始します（該当するタスクが 現在のスキャンリスト に表示されます）。

自律コピーを起動する

Dr.Web for Linuxは、特別なモードである、*自律コピーとしての実行をサポートしています。*

Dr.Web for Linuxグラフィカル管理インターフェースが自律コピーとして 実行 されている場合は、一連のサービスコンポーネント（*Dr.Web for Linuxのバックグラウンド動作設定デーモン* `drweb-configd`、Scanner、スキャンエンジン）と連携して動作し、ソフトウェアの実行中のインスタンスをサポートするために実行されます。

自律コピーとして動作するDr.Web for Linuxグラフィカル管理インターフェースの特徴:

- Dr.Web for Linuxグラフィカルユーザーインターフェイスを自律コピーとして実行するには、有効なキーファイルが必要です。 集中管理 モードでの操作はサポートされていません（集中管理サーバーからエクスポートされた キーファイル をインストールすることができます）。この場合、Dr.Web for Linuxが集中管理サーバーに接続されている場合であっても、自律コピーモードで検出された脅威について集中管理サーバーには *通知されません* 。
- グラフィカル管理インターフェースの自律コピーとしての動作をサポートする全ての追加コンポーネントは、現在のユーザー下で起動され、そのセッション用に個別に生成された設定ファイルで動作します。
- 使用されるすべての一時ファイルとUNIXソケットは、自律的コピーの起動時に作成される固有の名前を持つディレクトリ内にのみ作成されます。一時ファイルのために、システムディレクトリ内に固有の一時ディレクトリが作成されます（このディレクトリへのパスは `TMPDIR` 環境変数内で取得できます）。
- グラフィカル管理インターフェースの自律コピーではSpIDer GuardとSpIDer Gateを *起動* することはできません。Scannerでサポートされている ファイルスキャン と 隔離管理 の機能のみ利用することができます。
- 必要なすべてのパス（ウイルスデータベース、スキャンエンジン、サービスコンポーネントの実行ファイルへのパス）はデフォルトで指定されているか、特別な環境変数から取得できます。
- 同時に実行することのできるグラフィカル管理インターフェースの自律コピーの数に制限はありません。
- グラフィカル管理インターフェースの自律コピーがシャットダウンされると、一連のサービスコンポーネントも終了します。

コマンドラインからの操作

このセクションの内容:

概要

特別なDr.Web Ctユーティリティ（`drweb-ctl`）を使用することで、OSのコマンドラインからDr.Web for Linuxスキャンサーバーの動作を管理できます。このユーティリティを使用して次の動作を実行できます。

- ブートレコードを含む、ファイルシステムオブジェクトのスキャンを開始する
- リモートネットワークホストでファイルのスキャンを開始する（下記 の注を参照）
- アンチウイルスコンポーネント（ディストリビューションに応じてウイルスデータベース、スキャンエンジンなど）の更新を開始する
- Dr.Web for Linux設定のパラメータを確認・変更する
- Dr.Web for Linuxコンポーネントのステータスや検出された脅威に関する統計を確認する
- 隔離されたオブジェクトを確認・管理する
- 集中管理サーバーに接続する、または集中管理サーバーとの接続を切断する

Dr.Web for Linuxを管理するユーザー コマンド はDr.Web for Linuxサービスコンポーネントが動作中の場合のみ適用されます（デフォルトでは、コンポーネントはシステム起動時に自動的に起動します）。

一部のコントロールコマンドはスーパーユーザー権限を必要とします。

権限を昇格させるには `su` コマンド（カレントユーザーを変更する）または `sudo` コマンド（指定したコマンドを他のユーザーの権限で実行する）を使用します。

`drweb-ctl` ツールはDr.Web for Linuxの動作を管理するコマンドのオートコンプリートをサポートしています（コマンドシェル内で該当するオプションが有効になっている場合）。コマンドシェルがオートコンプリートを許可していない場合、このオプションの設定を行うことができます。方法については、お使いのOSディストリビューションのマニュアルを参照してください。

シャットダウンする際、ツールはPOSIX準拠システムの規則に従って終了コードを返します。操作が正常に完了した場合は0（ゼロ）、それ以外の場合は0以外（ゼロ以外）です。

ツールが0以外（non-null）の終了コードを返すのは、内部エラーの場合のみであるという点に注意してください（例：ツールがコンポーネントに接続できなかった、リクエストされた操作を実行できなかった）。ツールが脅威を検出（そして駆除）した場合は、リクエストされた操作（例：スキャン）が正常に実行されたため、0（null）終了コードを返します。検出された脅威と適用されたアクションのリストを明らかにする必要がある場合、コンソールに表示されたメッセージを分析してください。

すべてのエラーのコードについては、付録D. 既知のエラー セクションのリストをご確認ください。

リモートホストスキャン

Dr.Web for Linuxを使用して、リモートネットワークホストにあるファイルの脅威に対するスキャンを実行できます。このようなホストには、フルコンピューティングマシン（ワークステーションやサーバーなど）だけでなく、ルーター、セットトップボックス、いわゆる「モノのインターネット（IoT）」と呼ばれるその他の「スマート」デバイスも含まれます。リモートスキャンを実行するには、リモートホストが *SSH*（*セキュアシェル*）または *Telnet* を介したリモート端末アクセスを提供する必要があります。デバイスにアクセスするには、リモートホストのIPアドレスとドメイン名、*SSH* または *Telnet* を介してリモートでシステムにアクセスするユーザーの認証情報を知っている必要があります。このユーザーは、スキャン済みファイルへのアクセス権限（少なくとも読み取り権限）を持っている必要があります。

この機能は、リモートホスト上の悪質なファイルや疑わしいファイルの検出にのみ使用できます。リモートスキャンを用いた脅威の排除（すなわち、悪意のあるオブジェクトの隔離への移動、削除および修復）はできません。リモートホスト上で検出された脅威を排除するには、このホストが直接提供する管理ツールを使用する必要があり

ます。たとえば、ルーターおよび他の「スマート」デバイスの場合、ファームウェア更新のためのメカニズムを使用できます。コンピューティングマシンの場合、それらへの接続（たとえば、リモートターミナルモードを使用）、ファイルシステム内のそれぞれの操作（ファイルの削除または移動など）、またはそれらにインストールされたアンチウイルスソフトウェアの実行により行うことができます。

リモートスキャンはコマンドラインツール `drweb-ctl` からのみ実行できます（コマンド コマンド `remotescan` を使用します）。

呼び出しフォーマット

1.製品を管理するためのコマンドラインユーティリティのコマンドフォーマット

Dr.Web for Linux の動作を管理するコマンドラインツールのフォーマットは以下のとおりです。

```
$ drweb-ctl [<general options> | <command> [<argument>] [<command options>]]
```

各パラメータは次のとおりです：

- *<general options>* - コマンドが指定されていない場合に起動時に適用できる、またはあらゆるコマンドにおいて適用できるオプションです。起動時に必須ではありません。
- *<command>* - Dr.Web for Linuxによって実行されるコマンドです（スキャンの開始、隔離されたオブジェクトのリストを出力、その他のコマンドなど）。
- *<argument>* - コマンド引数です。指定されたコマンドに依存します。コマンドによってはない場合もあります。
- *<command options>* - 指定されたコマンドの動作を管理するためのオプションです。一部のコマンドでは省略できます。

2. 全般的なオプション（general options）

以下の全般的なオプションを使用できます。

オプション	説明
`-h, --help`	全般的なヘルプ情報を表示して終了します。いずれかのコマンドに関するヘルプ情報を表示させるには、以下の呼び出しを使用ます。 `$ drweb-ctl <command> -h`
`-v, --version`	モジュールバージョンに関する情報を表示して終了します。
`-d, --debug`	指定されたコマンドの実行時にデバッグ情報を表示するよう指示します。コマンドが指定されていない場合は実行できません。以下の呼び出しを使用します。 `$ drweb-ctl <command> -d`

3. コマンド

Dr.Web for Linuxを管理するコマンドは以下のグループに分けることができます。

- アンチウイルススキャン のコマンド
- 更新および集中管理モードでの動作を管理する コマンド
- 設定を管理する コマンド
- 検出された脅威および隔離を管理する コマンド
- 情報に関する コマンド

コマンドラインから製品のこのコンポーネントに関するヘルプを要求するには、次のコマンドを使用します：`man 1 drweb-ctl`

3.1. アンチウイルススキャンのコマンド

アンチウイルススキャンを管理するコマンドには以下のものがあります。

コマンド	説明
`scan` *<path>*	機能：Scannerによる、指定されたファイルやディレクトリのスキャンを開始します。 引数： <*path*> - スキャンするファイルまたはディレクトリへのパスです（パスは相対パスでも可）。 *`--stdin` または `--stdin0` オプションを使用する場合、この引数は省略できます。特定の条件を満たす複数のファイルを指定するには、`find` ユーティリティ（使用例 参照）および `--stdin` または `--stdin0` オプションを使用します。* オプション： `-a [--Autonomous]` は、指定されたスキャンを実行し、完了後にそれらを終了させるために スキャンエンジンとScannerの自律コピーを実行します。自律コピーによるスキャン中に検出された脅威は、`threats` コマンドによって表示される検出された脅威のリストに追加されず（下記 参照）、それらの脅威に関する情報は集中管理サーバーには送信されません（スキャンサーバーDr.Web for Linuxが集中管理サーバーで管理されている場合）。 `--stdin` - スキャンのためのパスのリストを標準的な入力文字列（*stdin*）から取得します。リスト内のパスは改行文字（`\n`）で区切られている必要があります。 `--stdin0` - スキャンのためのパスのリストを標準的な入力文字列（*stdin*）から取得します。リスト内のパスはヌル文字（`\0`）で区切られている必要があります。

コマンド	説明
	 `--stdin` および `--stdin0` オプションを使用する場合、リストのパスに検索のパターンまたは正規表現を含めることはできません。`--stdin` および `--stdin0` オプションを使用して、外部ユーティリティ(`scan` コマンドの `find` など)によって生成されるパスリストを処理することをお勧めします(使用例 を参照)。 `--Exclude` *<path>* - 除外するパスです。パスは相対パスにすることができ、ファイルマスクを含むことができます(ワイルドカード「`?`」と「`*`」、シンボルクラス「`[ ]`」、「`[! ]`」、「`[^ ]`」を使用することができます)。 *任意オプション、複数回設定できます。* `--Report` *<type>* - スキャンレポートのタイプを指定します。 使用可能な値: • `BRIEF` - 短いレポート • `DEBUG` - 詳細なレポート • `JSON` - JSON形式のシリアル化されたレポート デフォルト値: *BRIEF* `--ScanTimeout` *<number>* - 1つのファイルをスキャンする際のタイムアウトをミリ秒で指定します。 値に *0* が指定された場合、スキャンにかかる時間は制限されません。 デフォルト値: *0* `--PackerMaxLevel` *<number>* - パックされたオブジェクトをスキャンする際のネスティングレベルの上限を指定します。 値に *0* が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。 デフォルト値: *8* `--ArchiveMaxLevel` *<number>* - アーカイブ(zip、rarなど)をスキャンする際のネスティングレベルの上限を指定します。 値に *0* が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。 デフォルト値: *8* `--MailMaxLevel` *<number>* - メールメッセージ(pst、tbbなど)をスキャンする際のネスティングレベルの上限を指定します。 値に *0* が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。 デフォルト値: *8* `--ContainerMaxLevel` *<number>* - その他のコンテナ(HTMLなど)をスキャンする際のネスティングレベルの上限を指定します。 値に *0* が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。 デフォルト値: *8* `--MaxCompressionRatio` *<ratio>* - スキャンされるオブジェクトの最大圧縮率を指定します。

コマンド	説明
	値は *2* 以上にする必要があります。 デフォルト値：*3000* `--MaxSizeToExtract` *<size>* - アーカイブに含まれるファイルの最大サイズを指定します。このパラメータの値よりサイズが大きいファイルは、スキャン時にスキップされます。デフォルトでは、アーカイブ内のファイルのサイズ制限はありません。サイズは、サフィックス（b、kb、mb、gb）を付けた数値で指定します。サフィックスが指定されていない場合、値はバイト単位のサイズとして扱われます。 `--HeuristicAnalysis` *<On|Off>* - スキャン中のヒューリスティック解析を有効または無効にします。 デフォルト値：*On* `--OnKnownVirus` *<action>* - シグネチャベースの解析を使用して検出された既知の脅威に対して適用されるアクションです。 *可能なアクション：Report、Cure、Quarantine、Delete* デフォルト値：*Report* `--OnIncurable` *<action>* - 修復不可能な脅威が検出された場合、または修復アクション（`Cure`）が失敗した場合に適用されるアクションです。 可能なアクション：*Report、Quarantine、Delete* デフォルト値：*Report* `--OnSuspicious` *<action>* - ヒューリスティック解析によって検出された疑わしいオブジェクトに対して適用されるアクションです。 可能なアクション：*Report、Quarantine、Delete* デフォルト値：*Report* `--OnAdware` *<action>* - 検出されたアドウェアに対して適用されるアクションです。 可能なアクション：*Report、Quarantine、Delete* デフォルト値：*Report* `--OnDialers` *<action>* - 検出されたダイアラーに対して適用されるアクションです。 可能なアクション：*Report、Quarantine、Delete* デフォルト値：*Report* `--OnJokes` *<action>* - 検出されたジョークプログラムに対して適用されるアクションです。 可能なアクション：*Report、Quarantine、Delete* デフォルト値：*Report* `--OnRiskware` *<action>* - 検出されたリスクウェアに対して適用されるアクションです。 可能なアクション：*Report、Quarantine、Delete* デフォルト値：*Report* `--OnHacktools` *<action>* - 検出されたハッキングツールに対して適用されるアクションです。 可能なアクション：*Report、Quarantine、Delete* デフォルト値：*Report*

コマンド	説明
	 コンテナ（アーカイブ、メール添付ファイルなど）内のファイルで脅威が検出された場合は、削除アクション（*Delete*）の代わりにコンテナの隔離への移動（*Quarantine*）が実行されます。 `--FollowSymlinks` - シンボリックリンクを自動的に解決します。
`bootscan` *<disk drive>* | `ALL`	機能：Scannerによる、指定されたディスク上のブートレコードのスキャンを実行します。MBRとVBRの両方がスキャンされます。 引数： *<disk drive>* - ブートレコードをスキャンするディスクデバイスのブロックファイルへのパス。スペースで区切って複数のディスクデバイスを指定できます。引数は必須です。デバイスファイルの代わりに `ALL` を指定した場合は、使用可能な全てのディスクデバイスにある全てのブートレコードが確認されます。 オプション： `-a [--Autonomous]` は、指定されたスキャンを実行し、完了後にそれらを終了させるために、スキャンエンジンとScannerの自律コピーを実行します。自律コピーによるスキャン中に検出された脅威は、`threats` コマンドによって表示される検出された脅威のリストに追加されず（以下 参照）、それらの脅威に関する情報は集中管理サーバーには送信されません（スキャンサーバーDr.Web for Linuxが集中管理サーバーで管理されている場合）。 `--Report` *<type>* - スキャンレポートのタイプを指定します。 使用可能な値： • `BRIEF` - 短いレポート • `DEBUG` - 詳細なレポート • `JSON` - JSON形式のシリアル化されたレポート デフォルト値：*BRIEF* `--ScanTimeout` *<number>* - 1つのファイルをスキャンする際のタイムアウトをミリ秒で指定します。 値に *0* が指定された場合、スキャンにかかる時間は制限されません。 デフォルト値：*0* `--HeuristicAnalysis` *<On|Off>* - スキャン中のヒューリスティック解析を有効または無効にします。 デフォルト値：*On* `--Cure` *<Yes|No>* - 脅威が検出された際に修復を試みる動作を有効または無効にします。 値に *No* が指定された場合、検出された脅威に関する通知のみが表示されます。 デフォルト値：*No* `--ShellTrace` - ブートレコードをスキャンする際の、追加のデバッグ情報の表示を有効にします。
`procscan`	機能：Scannerによる、現在実行中のシステムプロセスのコードを含んだ実行ファイルのスキャンを開始します。悪意のある実行ファイルが検出された場

コマンド	説明
	合、それらは駆除され、それらの実行ファイルによって実行されたすべてのプロセスを強制的に終了します。 引数：None オプション： `-a [--Autonomous]` は、指定されたスキャンを実行し、完了後にそれらを終了させるために、スキャンエンジンとScannerの自律コピーを実行します。自律コピーによるスキャン中に検出された脅威は、`threats` コマンドによって表示される検出された脅威のリストに追加されず（以下 参照）、それらの脅威に関する情報は集中管理サーバーには送信されません（スキャンサーバーDr.Web for Linuxが集中管理サーバーで管理されている場合）。 `--Report` *<type>* - スキャンレポートのタイプを指定します。 使用可能な値： • `BRIEF` - 短いレポート • `DEBUG` - 詳細なレポート • `JSON` - JSON形式のシリアル化されたレポート デフォルト値：*BRIEF* `--ScanTimeout` *<number>* - 1つのファイルをスキャンする際のタイムアウトをミリ秒で指定します。 値に *0* が指定された場合、スキャンにかかる時間は制限されません。 デフォルト値：*0* `--HeuristicAnalysis` *<On|Off>* - スキャン中のヒューリスティック解析を有効または無効にします。 デフォルト値：*On* `--PackerMaxLevel` *<number>* - パックされたオブジェクトをスキャンする際のネスティングレベルの上限を指定します。 値に *0* が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。 デフォルト値：*8* `--OnKnownVirus` *<action>* - シグネチャベースの解析を使用して検出された既知の脅威に対して適用されるアクションです。 可能なアクション：*Report*、*Cure*、*Quarantine*、*Delete* デフォルト値：*Report* `--OnIncurable` *<action>* - 修復不可能な脅威が検出された場合、または修復アクション（`Cure`）が失敗した場合に適用されるアクションです。 可能なアクション：*Report*、*Quarantine*、*Delete* デフォルト値：*Report* `--OnSuspicious` *<action>* - ヒューリスティック解析によって検出された疑わしいオブジェクトに対して適用されるアクションです。 可能なアクション：*Report*、*Quarantine*、*Delete* デフォルト値：*Report* `--OnAdware` *<action>* - 検出されたアドウェアに対して適用されるアクションです。

コマンド	説明
	可能なアクション：*Report*、*Quarantine*、*Delete* デフォルト値：*Report* `--OnDialers` <action> - 検出されたダイアラーに対して適用されるアクションです。 可能なアクション：*Report*、*Quarantine*、*Delete* デフォルト値：*Report* `--OnJokes` *<action>* - 検出されたジョークプログラムに対して適用されるアクションです。 可能なアクション：*Report*、*Quarantine*、*Delete* デフォルト値：*Report* `--OnRiskware` *<action>* - 検出されたリスクウェアに対して適用されるアクションです。 可能なアクション：*Report*、*Quarantine*、*Delete* デフォルト値：*Report* `--OnHacktools` *<action>* - 検出されたハッキングツールに対して適用されるアクションです。 可能なアクション：*Report*、*Quarantine*、*Delete* デフォルト値：*Report* 実行ファイルで脅威が検出された場合、Dr.Web for Linuxは、そのファイルによって開始されたすべてのプロセスを終了するという点に注意してください。
`remotescan` *<host> <path>*	機能：*SSH*または *Telnet*を使用して接続することにより、指定されたリモートホスト上の指定されたファイルまたはディレクトリのスキャンを開始します。 リモートスキャンで検出された脅威は駆除されず、`threats`コマンドで表示される脅威のリストには含まれないということに注意してください（下記 参照）。 この機能はリモートホストの悪意のあるファイルや疑わしいファイルの検出にのみ使用できます。リモートホストで検出された脅威を排除するには、このホストから直接提供される管理ツールを使用する必要があります。コンピューティングマシンの場合、それらのマシン（オプションとして、リモートターミナルモードを使用）およびそれらのファイルシステムのそれぞれの操作（ファイルの削除または移動など）に接続するか、それらにインストールされたアンチウイルスソフトウェアを実行して行うことができます。 引数： *<host>* - リモートホストのIPアドレスまたはドメイン名です。 *<path>* - スキャンするファイルまたはディレクトリへのパスです（パスは絶対パスでなければなりません）。

コマンド	説明
	オプション: `-m [--Method]` *<SSH|Telnet>* - リモートホスト接続方法(プロトコル)です。 *方法が指定されていない場合は、SSHが使用されます。* `-l [--Login]` *<name>* - 選択されたプロトコル経由でリモートホストでの認証に使用されるログインID(ユーザー名)です。 *ユーザー名が指定されていない場合、コマンドを起動したユーザー名を用いてリモートホストに接続しようとします。* `-i [--Identity]` *<path to file>* - 選択されたプロトコル経由で指定されたユーザーの認証に使用されるプライベートキーが含まれるファイルへのパスです。 `-p [--Port]` *<number>* - 選択されたプロトコル経由で接続するリモートホストのポート番号です。 デフォルト値: *選択したプロトコル用のデフォルトポートです(SSHは22、Telnetは23)* `--ForceInteractive` - SSHインタラクティブセッションを使用します(*SSH*接続の場合のみ)。 *オプション機能です。* `--TransferListenAddress` *<address>* - リモートデバイスからスキャン用に送信されるファイルを受信するためにリッスンされるアドレスです。 *オプション機能です。指定されなかった場合、任意のアドレスが使用されます。* `--TransferListenPort` *<port>* - リモートデバイスからスキャン用に送信されるファイルを受信するためにリッスンされるポートです。 *オプション機能です。指定されなかった場合、任意のポートが使用されます。* `--TransferExternalAddress` *<address>* - スキャン用にファイルを送信するためにリモートデバイスに指定されるアドレスです。 *オプション機能です。指定されなかった場合、"`--TransferListenAddress`" の値、またはすでに確立されているセッションの送信アドレスが使用されます。* `--TransferExternalPort` *<port>* - スキャン用にファイルを送信するためにリモートデバイスに指定されるポートです。 *オプション機能です。指定されなかった場合、自動で決定されたポートが使用されます。* `--Password` *<password>* - 選択されたプロトコルを介してユーザー認証に使用されるパスワードです。 *パスワードはプレーンテキストとして転送されることに注意してください。* `--Exclude` *<path>* - スキャンの対象から除外するパスです。パスにはファイルマスクを含むことができます(ワイルドカード「`?`」と「`*`」、シンボルクラス「`[ ]`」、「`[! ]`」、「`[^ ]`」を使用することができます)。パス(ファイルマスクを含むパスを含む)は絶対パスである必要があります。 *任意オプション、複数回設定できます。* `--Report` *<type>* - スキャンレポートのタイプを指定します。 使用可能な値:

コマンド	説明
	• BRIEF - 短いレポート • DEBUG - 詳細なレポート • JSON - JSON形式のシリアル化されたレポート デフォルト値：*BRIEF* --ScanTimeout *<number>* - 1つのファイルをスキャンする際のタイムアウトをミリ秒で指定します。 値に *0* が指定された場合、スキャンにかかる時間は制限されません。 デフォルト値：*0* --PackerMaxLevel *<number>* - パックされたオブジェクトをスキャンする際のネスティングレベルの上限を指定します。 値に *0* が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。 デフォルト値：*8* --ArchiveMaxLevel *<number>* - アーカイブ（zip、rarなど）をスキャンする際のネスティングレベルの上限を指定します。 値に *0* が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。 デフォルト値：*8* --MailMaxLevel *<number>* - メールメッセージ（pst、tbbなど）をスキャンする際のネスティングレベルの上限を指定します。 値に *0* が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。 デフォルト値：*8* --ContainerMaxLevel *<number>* - その他のコンテナ（HTMLなど）をスキャンする際のネスティングレベルの上限を指定します。 値に *0* が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。 デフォルト値：*8* --MaxCompressionRatio *<ratio>* - スキャンされるオブジェクトの最大圧縮率を指定します。 値は *2* 以上にする必要があります。 --MaxSizeToExtract *<size>* - アーカイブに含まれるファイルの最大サイズを指定します。このパラメータの値よりサイズが大きいファイルは、スキャン時にスキップされます。デフォルトでは、アーカイブ内のファイルのサイズ制限はありません。サイズは、サフィックス（b、kb、mb、gb）を付けた数値で指定します。サフィックスが指定されていない場合、値はバイト単位のサイズとして扱われます。 デフォルト値：*3000* --HeuristicAnalysis *<On/Off>* - スキャン中のヒューリスティック解析を有効または無効にします。 デフォルト値：On
checkmail *<path to file>*	機能：脅威、スパムの兆候、悪意のあるリンク、メール処理ルールへの不適合を検出するために、ファイルに保存されたメールメッセージのスキャンを実行します（メール処理コンポーネントを使用して）。コンソールの出力スレッド（*stdout*）

コマンド	説明
	には、スキャンの結果と、メール処理コンポーネントによるスキャン中にメッセージに対して適用されたアクションが表示されます。 引数: *<path to file>* - スキャンが必要なメールメッセージのファイルへのパスです。必須の引数です。 オプション: `--Report` *<type>* - スキャンレポートのタイプを指定します。 使用可能な値: • *BRIEF* - 短いレポート • *DEBUG* - 詳細なレポート • *JSON* - JSON形式のシリアル化されたレポート デフォルト値: *BRIEF* `-r [--Rules]` *<list of rules>* - メールメッセージのスキャン中に従うルールのリストを指定します。 *ルールが指定されなかった場合、デフォルトで指定されている以下のルールセットが適用されます。* `threat_category in (KnownVirus, VirusModification, UnknownVirus, Adware, Dialer) : REJECT` `total_spam_score gt 0.80 : REJECT` `url_category in (InfectionSource, NotRecommended, CopyrightNotice) : REJECT` *Dr.Web Anti-Spamがインストールされていない場合、スパムのスキャンルール(2番目の文字列)はセットから自動的に除外されます。* `-c [--Connect]` *<IP>:<port>* - スキャンされるメッセージの送信者の接続用アドレスとして使用されるネットワークソケットを指定します。 `-e [--Helo]` *<name>* - メッセージを送信したクライアントの識別子を指定します(IPアドレスまたはFQDNホスト、SMTPコマンドHELO/EHLO)。 `-f [--From]` *<email>* - 送信者のメールアドレスを指定します(SMTPコマンドMAIL FROM)。 *アドレスが指定されていない場合、それぞれのメールのアドレスが使用されます。* `-t [--Rcpt]` *<email>* - 受信者のメールアドレスを指定します(SMTPコマンドRCPT TO)。 *アドレスが指定されていない場合、それぞれのメールのアドレスが使用されます。* メール処理コンポーネントがインストールされていない場合、このコマンドを呼び出すとエラーが返されます。

上のコマンド以外に、`drweb-ctl` ツールは追加のスキャンパラメータをサポートしています。詳細については `man 1 drweb-ctl` を参照してください。

3.2.更新および集中管理モードでの動作を管理するコマンド

更新および集中管理モードでの動作を管理するコマンドには以下のものがあります。

コマンド	説明
`update`	機能：Doctor Webの更新サーバーまたはDr.Web MeshDを経由したローカルクラウドから、アンチウイルスコンポーネント（ディストリビューションによって、ウイルスデータベース、スキャンエンジンなど）の更新を開始し、更新プロセスがすでに実行されている場合はそれを終了するか、またはファイルの最新の更新を以前のバージョンへロールバックします。 Dr.Web for Linuxが集中管理サーバーに接続されている場合、このコマンドは効力を持ちません。 引数：None オプション： `-l [--local-cloud]` - Dr.Web for Linuxに接続されたローカルクラウドを使用して更新をダウンロードします。このオプションが指定されていない場合、更新は Doctor Web 更新サーバー からダウンロードされます（デフォルトの動作）。 `--From <path>` - 指定したディレクトリからオフラインで更新を適用します。 `--Path <path>` - オフラインで更新するためのファイルを指定されたディレクトリに保存します。そのディレクトリにすでにファイルがある場合は、それらが更新されます。 `--Rollback` - 最後の更新をロールバックし、更新されたファイルの以前のバージョンを復元します。 `--Stop` - 実行中の更新プロセスを終了します。
`esconnect <server>[:<port>]`	機能：Dr.Web for Linuxを指定された集中管理サーバー（Dr.Web Enterprise Serverなど）に接続します。動作モードの詳細については、動作モード を参照してください。 引数： • *<server>* - 集中管理サーバーが動作しているホストのIPアドレスまたはホスト名です。この項目は必須です。 • *<port>* - 集中管理サーバーによって使用されるポート番号です。引数はオプションであり、集中管理サーバーが標準以外のポートを使用する場合にのみ指定する必要があります。 オプション： `--Certificate <path>` - 接続する集中管理サーバーの証明書ファイルへのパスです。

コマンド	説明
	`--Login` *<ID>* - 集中管理サーバーへの接続に使用されるログインID(ワークステーションID)です。 `--Password` *<password>* - 集中管理サーバーへの接続用パスワードです。 `--Group` *<ID>* - ワークステーションが接続時に追加されるグループのIDです。 `--Rate` *<ID>* - ワークステーションが集中管理サーバーグループの1つに含まれている場合に、そのワークステーションに適用されるタリフグループのIDです(`--Group` オプションと一緒にのみ指定できます)。 `--Compress` *<On|Off>* - データの圧縮を有効(*On*)または無効(*Off*)にします。指定しない場合、圧縮の使用はサーバーによって決定されます。 `--Encrypt` *<On|Off>* - データの暗号化を有効(*On*)または無効(*Off*)にします。指定しない場合、暗号化の使用はサーバーによって決定されます。 `--Newbie` - "新規端末(newbie)"として接続します(サーバーで新しいアカウントを取得します)。 このコマンドは、`drweb-ctl` を *ルート* 権限で実行する必要があります。必要に応じて、`su` または `sudo` コマンドを使用してください。
`esdisconnect`	機能:Dr.Web for Linuxを集中管理サーバーから切断し、その動作をスタンドアロンモードに切り替えます。 Dr.Web for Linuxがすでにスタンドアロンモードで動作している場合、このコマンドは効力を持ちません。 引数:None オプション:None このコマンドは、`drweb-ctl` を *ルート* 権限で実行する必要があります。必要に応じて、`su` または `sudo` コマンドを使用してください。

3.3. 設定を管理するコマンド

設定を管理するコマンドには以下のものがあります。

コマンド	説明
`cfset` *<section>*. *<parameter>* *<value>*	機能:Dr.Web for Linuxの現在の設定で、指定されたパラメータのアクティブな値を変更します。 引数:

コマンド	説明
	• *<section>* - パラメータのある設定ファイルのセクション名です。この引数は必須です。 • *<parameter>* - パラメータの名前です。この引数は必須です。 • *<value>* - 新しいパラメータ値です。この引数は必須です。 パラメータ値を指定するには、*<section>.<parameter> <value>*という形式を使用します。代入記号「=」はここでは使用しません。 複数のパラメータ値を指定する場合は、追加するパラメータ値の数だけコマンド `cfset` の呼び出しを繰り返す必要があります。パラメータ値のリストに新しい値を追加するには、`-a` オプションを使用します（以下を参照）。文字列「*<value 1>, <value 2>*」が *<parameter>* の1つの値と見なされてしまうため、文字列 *<parameter> <value 1>, <value 2>* を引数として指定することはできません。 設定ファイルに関する詳細は、`man 5 drweb.ini` で表示されるドキュメントページを参照してください。 **オプション：** `-a [--Add]` - 現在のパラメータ値を置き換えず、指定された値をリストに追加します（リストとして指定された複数の値を持つことのできるパラメータに対してのみ使用可能）。このオプションは、タグを付けたパラメータの新しいグループを追加する場合にも使用してください。 `-e [--Erase]` - 現在のパラメータ値を置き換えず、指定された値をリストから削除します（リストとして指定された複数の値を持つことのできるパラメータに対してのみ使用可能）。 `-r [--Reset]`—パラメータ値をデフォルトにリセットします。その際、コマンド内で *<value>* は必要なく、指定された場合は無視されます。 オプションは必須ではありません。指定されなかった場合は、現在のパラメータ値（パラメータに複数の値がある場合は値の全リスト）が指定された値に置き換えられます。 このコマンドは、`drweb-ctl` をルート権限で実行する必要があります。必要に応じて、`su` または `sudo` コマンドを使用してください。
`cfshow [<section>[.<parameter>]]`	**機能：** Dr.Web for Linuxの現在の設定のパラメータを表示します。 パラメータを表示するコマンドは *<section>.<parameter> = <value>* のように指定します。インストールされていないコンポーネントのセクションとパラメータは表示されません。 **引数：** • *<section>* - 表示するパラメータのある設定セクションの名前です。この引数は任意です。指定されなかった場合、すべての設定セクションのパラメータが表示されます。

コマンド	説明
	• *<parameter>* - 表示するパラメータの名前です。この引数は任意です。指定されなかった場合、セクションのすべてのパラメータが表示されます。それ以外の場合は、このパラメータのみが表示されます。セクション名なしにパラメータが指定された場合、すべての設定ファイルセクションにある、その名前を持つすべてのパラメータが表示されます。 オプション: `--Uncut`—すべての設定パラメータを出力します(現在インストールされているコンポーネントのセットによって使用されているもの以外も含む)。このオプションが指定されていない場合、インストールされたコンポーネントの設定に使用されているパラメータのみが出力されます。 `--Changed` - デフォルトの値と異なる値を持つパラメータのみを表示します。 `--Ini` - パラメータ値をINIファイルフォーマットで表示します。まず角括弧内でセクション名が指定され、次に *<parameter>* = *<value>* ペアでセクションパラメータが表示されます(1行につき1ペア)。 `--Value` - 指定されたパラメータの値のみを表示します(この場合、*<parameter>*引数は必須です)。
`reload`	機能: Dr.Web for Linux サービスコンポーネントを再起動させます。その際、ログが再度開かれ、設定ファイルを再読み込みし、異常終了したコンポーネントの再起動が試みられます。 引数: None オプション: None

3.4. 検出された脅威および隔離を管理するコマンド

検出された脅威および隔離を管理するコマンドには以下のものがあります。

コマンド	説明
`threats` [*<action>* *<object>*]	機能: 指定されたアクションを、検出された脅威に適用します。アクションの種類はコマンドオプションによって指定します。 アクションが指定されていない場合、検出されたが駆除されていない脅威に関する情報を表示します。脅威に関する情報は、オプションの `--Format` 引数で指定されたフォーマットに従って表示されます。`--Format` 引数が指定されていない場合は、各脅威に関する次の情報が表示されます。 • 脅威に対して割り当てられた識別子(順序数) • 感染したファイルへのフルパス • 脅威に関する情報(脅威の名前、Doctor Webの分類による脅威の種類) • ファイルに関する情報(サイズ、ファイル所有者のユーザー名、最後に変更された時間) • 脅威に対して適用された操作の履歴(検出、アクションの適用など) 引数: None オプション:

コマンド	説明
	`--Format` "*<format string>*" - 脅威に関する情報を指定されたフォーマットで表示します。フォーマット文字列の説明は 以下 のとおりです。 *このオプションがアクションオプションと一緒に指定されている場合は無視されます。* `-f [--Follow]` - 新しい脅威に関する新しいメッセージを待ち、それらを受け取り次第、表示します（CTRL+C で待機を中断します）。 *このオプションがアクションオプションと一緒に指定されている場合は無視されます。* `--Directory` *<list of directories>* - *<list of directories>* で指定したディレクトリ内のファイルで検出された脅威のみを表示します。 *このオプションが以下のオプションと一緒に適用された場合は無視されます。* `--Cure` *<threat list>* - 指定された脅威を修復しようと試みます（脅威の識別子をコンマで区切りで指定）。 `--Quarantine` *<threat list>* - 指定された脅威を 隔離 に移します（脅威の識別子をコンマで区切りで指定）。 `--Delete` *<threat list>* - 指定された脅威を削除します（脅威の識別子をコンマで区切りで指定）。 `--Ignore` *<threat list>* - 指定された脅威を無視します（脅威の識別子をコンマで区切りで指定）。 検出されたすべての脅威に対してアクションを適用する必要がある場合は、*<threat list>* の代わりに `All` を指定します。例： `$ drweb-ctl threats --Quarantine All` この例では、検出された悪意のあるオブジェクトすべてを隔離に移します。
`quarantine` [*<action>* *<object>*]	機能：隔離 内の指定されたオブジェクトに対してアクションを適用します。 アクションが指定されなかった場合、隔離されたオブジェクトに関する情報とそのIDが、隔離に移された元のファイルに関する簡単な情報と一緒に表示されます。隔離されたオブジェクトに関する情報は、オプションの `--Format` 引数で指定されたフォーマットに従って表示されます。`--Format` 引数が指定されていない場合は、隔離された各オブジェクトについて次の情報が表示されます。 • 隔離されたオブジェクトに対して割り当てられた識別子（順序数） • 隔離に移される前の、元のファイルへのパス • ファイルが隔離に移された日付 • ファイルに関する情報（サイズ、ファイル所有者のユーザー名、最後に変更された時間） • 脅威に関する情報（脅威の名前、Doctor Webの分類による脅威の種類） 引数：None オプション： `-a [--Autonomous]` - 指定された隔離コマンドを実行するためにScannerの個別のインスタンスを開始し、完了後にそれを終了します。 *このオプションは下のオプションと一緒に適用できます。*

コマンド	説明
	`--Format` "*<format string>*" - 隔離されたオブジェクトに関する情報を指定されたフォーマットで表示します。フォーマット文字列の説明は 以下 のとおりです。 *このオプションがアクションオプションと一緒に指定されている場合は無視されます。* `-f [--Follow]` - 新しい脅威に関する新しいメッセージを待ち、それらを受け取り次第、表示します（CTRL+C で待機を中断します）。 *このオプションがアクションオプションと一緒に指定されている場合は無視されます。* `--Discovery [`*<list of directories>*`,]` - 指定されたディレクトリのリストで隔離ディレクトリを検索し、脅威を検出すると統合された隔離に追加します。*<list of directories>* が指定されていない場合は、ファイルシステムの共通の場所（ボリュームマウントポイントとユーザーホームディレクトリ）にある隔離ディレクトリを検索します。 *このオプションは* `-a`*（*`--Autonomous`*）オプション（上を参照）だけでなく、下に一覧で示されている任意のオプションおよびアクションとともに指定できます。さらに、自律コピーとして* `quarantine` *コマンドを起動すると（*`-a`*（*`--Autonomous`*）オプションを指定して、*`--Discovery` *オプションは指定しない場合）、次の呼び出しと同じになります。* `quarantine --Autonomous --Discovery` `--Delete` *<object>* - 指定されたオブジェクトを隔離から削除します。 *オブジェクトは隔離から永久に削除されることに注意してください。この操作は元に戻せません。* `--Cure` *<object>* - 隔離内の指定されたオブジェクトの修復を試みます。 *オブジェクトが修復された場合であっても、それは隔離内に残ります。修復されたオブジェクトを隔離から復元するには* `--Restore` *オプションを使用します。* `--Restore` *<object>* - 指定されたオブジェクトを隔離から元の場所に復元します。 *このコマンドでは、*`drweb-ctl` *をroot権限で起動する必要がある場合があります。感染していても隔離からファイルを復元できます。* `--TargetPath` *<path>* -オブジェクトを隔離から指定された場所に復元します。指定された名前を持つファイルとして復元するか（*<path>* がファイルへのパスであった場合）、またはただ単に指定されたディレクトリに復元します（*<path>* がディレクトリへのパスであった場合）。パスは絶対パスでも相対パスでも構いません（現在のディレクトリを参照）。 *このオプションは* `--Restore` *との組み合わせでのみ使用できます。* *<object>* は隔離内のオブジェクトの識別子を指定します。隔離されたすべてのオブジェクトに対してアクションを適用する場合は、*<object>* の代わりに `All` を指定してください。例： `$ drweb-ctl quarantine --Restore All --TargetPath test` 全ての隔離されたオブジェクトを、`drweb-ctl` コマンドが起動された現在のディレクトリにある `test` サブディレクトリに復元します。

コマンド	説明
	`--Restore All` では、追加のオプション `--TargetPath`（指定された場合）にはファイルへのパスではなくディレクトリへのパスを指定する必要があります。

脅威および隔離コマンド用のフォーマット出力

出力フォーマットは、オプション引数 `--Format` として指定されたフォーマット文字列を使用して定義されます。フォーマット文字列は引用符で囲んで指定する必要があります。フォーマット文字列には、特定の情報として表示される特殊なマーカーだけでなく、一般的な記号（「そのまま」で表示されるもの）を含めることができます。以下のマーカーを使用することができます。

1. `threats` と `quarantine` コマンドに共通：

マーカー	説明
`%{n}`	新しい文字列
`%{t}`	集計
`%{threat_name}`	Doctor Webの分類に従って検出された脅威（ウイルス）の名前
`%{threat_type}`	Doctor Webの分類に従った脅威のタイプ（「既知のウイルス」など）
`%{size}`	元のファイルサイズ
`%{origin}`	パスを含む元のファイルのフルネーム
`%{path}`	`%{origin}` の同義語
`%{ctime}`	元のファイルが変更された日時（*「%Y-%b-%d %H:%M:%S」* フォーマット、例：`2018-Jul-20 15:58:01`）
`%{timestamp}`	`%{ctime}` と似ているが、*UNIXのタイムスタンプ* フォーマット
`%{owner}`	元のファイル所有者のユーザー名
`%{rowner}`	元のファイルのリモートユーザー所有者（該当しない場合や値が不明な場合は ? と置き換えられます）

2. `threats` コマンドに固有：

マーカー	説明
`%{hid}`	脅威に関連付けられているイベントの履歴にある脅威レコードのID
`%{tid}`	脅威のID
`%{htime}`	脅威に関連したイベントの日時
`%{app}`	脅威を処理したDr.Web for Linuxコンポーネントの ID
`%{event}`	脅威に関連する最新イベント：

マーカー	説明
	• FOUND - 脅威が検出されました。 • Cure - 脅威は修復されました。 • Quarantine - 脅威のあるファイルが隔離されました。 • Delete - 脅威のあるファイルが削除されました。 • Ignore - 脅威は無視されました。 • RECAPTURED - 他のコンポーネントによって脅威が再度検出されました。
%{err}	エラーメッセージテキスト（エラーが空の文字列に置き換えられない場合）

3. quarantine コマンドに固有：

マーカー	説明
%{qid}	隔離されたオブジェクトのID
%{qtime}	オブジェクトを隔離に移動した日時
%{curetime}	隔離に移されたオブジェクトの修復を試みた日時（該当しない場合または値が不明の場合は ? に置き換えられます）
%{cureres}	隔離されたオブジェクトの修復を試みた結果： • cured - 脅威は修復されています。 • not cured - 脅威は修復されていないか、修復が試みられていません。

例

```
$ drweb-ctl quarantine --Format "{%{n} %{origin}: %{threat_name} - %{qtime}%{n}}"
```

このコマンドは、次のタイプのレコードとして隔離内容を表示します。

```
{
  <path to file>:  <threat name>  -  <date of moving to quarantine>
}
...
```

3.5.情報に関するコマンド

情報に関するコマンドには以下のものがあります。

コマンド	説明
appinfo	機能：アクティブなDr.Web for Linuxコンポーネントに関する情報を出力します。 現在実行中の各コンポーネントに関する以下の情報が表示されます。 • 内部で使用される名前 • プロセス識別子 GNU/Linux（PID）

コマンド	説明
	• 状態（実行中、停止など） • コンポーネントの動作がエラーによって終了した場合、エラーコード • 追加情報（任意） 設定デーモン（drweb-configd）については、以下の追加情報が表示されます。 • インストールされたコンポーネントのリスト - *Installed* • 設定デーモンによって起動する必要のあるコンポーネントのリスト - *Should run* 引数：None オプション： -f [--Follow] - モジュールのステータス変更に関する新しい情報を待ち、それらを受け取り次第メッセージを表示します（CTRL+C で待機を中断します）。
baseinfo	機能：スキャンエンジンの現在のバージョン、およびウイルスデータベースのステータスに関する情報を表示します。 以下の情報が表示されます。 • スキャンエンジンのバージョン • 現在使用されているウイルスデータベースがリリースされた日時 • 使用可能なウイルスレコードの数（ウイルスデータベース内の） • ウイルスデータベースおよびスキャンエンジンが最後に更新された時間 • スケジュールされている次回の自動更新の時間 引数：None オプション： -l [--List] - ダウンロードされたウイルスデータベースのファイルと各ファイルのウイルスレコード数の全リストを表示します。
certificate	機能：保護された接続をスキャンするためにDr.Web for Linux によって使用される、信頼できるDr.Web証明書のコンテンツを表示します（設定 ページ内でこのオプションが有効になっている場合）。証明書を *<cert_name>*.pem ファイルに保存するには、以下のコマンドを使用してください： `$ drweb-ctl certificate > <cert_name>.pem` 引数：None オプション：None
events	機能：Dr.Web for Linuxイベントを表示します。そのほか、このコマンドを使用してイベントを管理（既読としてマーク、削除）することができます。 引数：None オプション： --Report *<type>* - イベントレポートのタイプを指定します。

コマンド	説明
	使用可能な値： • BRIEF - 短いレポート • DEBUG - 詳細なレポート • JSON - JSON形式のシリアル化されたレポート -f [--Follow] - 新しいイベントを待ち、発生時にそれらを表示します（CTRL + Cはスタンバイを中断します）。 -s [--Since] *<date, time>* - 指定されたタイムスタンプの前に発生したイベントを表示します（*<date, time>* は YYYY-MM-DD hh:mm:ss のフォーマットで指定します）。 -u [--Until] *<date, time>* - 指定されたタイムスタンプの後に発生したイベントを表示します（*<date, time>* は YYYY-MM-DD hh:mm:ss のフォーマットで指定します）。 -t [--Types] *<type list>* - 指定されたタイプのイベントのみを表示します（コンマで区切られます）。 次のイベントタイプを使用できます。 • Mail - メール内で脅威を検出 • UnexpectedAppTermination - コンポーネントの予期しないシャットダウン すべてのタイプのイベントを表示するには、All を使用します。 --ShowSeen - 既読イベントも表示されます。 --Show *<list of events>* - リストアップされたイベントを表示します（イベント識別子はコンマで区切られます）。 --Delete *<list of events>* - リストアップされたイベントを削除します（イベント識別子はコンマで区切られます）。 --MarkAsSeen *<list of events>* - リストアップされたイベントを既読としてマークします（イベント識別子はコンマで区切られます）。 すべてのイベントを「既読」としてマークする場合や削除する場合は、*<events list>* ではなく All を指定します。例： `$ drweb-ctl events --MarkAsSeen All` このコマンドはすべてのイベントを「既読」としてマークします。
report *<type>*	機能：Dr.Web for Linuxイベントに関するレポートをHTML形式で作成します（ページ本文は指定したファイルに出力されます）。 引数： *<type>* - レポートを作成するイベントのタイプです（タイプを1つ指定します）。可能な値については、上記 events コマンドの --Types オプションの説明を参照してください。この引数は必須です。 オプション： -o [--Output] *<path to file>* - 指定したファイルにレポートを保存します。このオプションは必須です。

コマンド	説明
	`-s [--Since]` *<date, time>* - 指定されたタイムスタンプよりも後に発生したイベントのレポートを作成します（*<date, time>* は `YYYY-MM-DD hh:mm:ss` のフォーマットで指定します）。 `-u [--Until]` *<date, time>* - 指定されたタイムスタンプよりも前に発生したイベントのレポートを作成します（*<date, time>* は `YYYY-MM-DD hh:mm:ss` のフォーマットで指定します）。 `--TemplateDir` *<path to directory>* - HTMLレポートテンプレートを含むディレクトリへのパスです。 `-s`、`-u`、`--TemplateDir` は必須のオプションではありません。 `$ drweb-ctl report Mail -o report.html` たとえば、上記のコマンドは、メールメッセージでのすべての脅威検出イベントに関するレポートをデフォルトのテンプレートで生成し、結果をカレントディレクトリの `report.html` ファイルに保存します。
`license`	機能：現在有効化されているライセンスに関する情報を表示、デモバージョンのライセンスを取得、またはすでに登録されているライセンス（すでにWebサイト上で登録されているものなど）のキーファイルを取得します。 オプションが指定されていない場合は以下の情報が表示されます（スタンドアロンモードのライセンスを使用している場合）： • ライセンス番号 • ライセンスの有効期間が満了する日時 集中管理サーバーから受け取ったライセンスを使用している場合（集中管理モードまたはモバイルモードで製品を使用するため）、該当するメッセージが表示されます。 引数：None オプション： `--GetDemo` - 1か月間有効なデモキーをリクエストします。試用期間の提供に関する条件を満たしている場合はそのキーを受け取ることができます。 `--GetRegistered` *<serial number>* - 新しいキーファイルの提供に関する条件に違反（ライセンスが集中管理サーバーによって管理される場合に製品を集中管理モードで使用していないなど）していない場合、指定されたシリアル番号に対するライセンスキーファイルを取得します。 `--Proxy http://`*<username>*`:`*<password>*`@`*<server address>*`:`*<port>* - プロキシサーバー経由でライセンスキーを取得します。前述のオプションのいずれか1つ（`--GetDemo` または `--GetRegistered`）のみと共に使用されます。 *シリアル番号が試用期間用のものではない場合、まずDoctor WebのWebサイトでそれを登録する必要があります。* Dr.Web製品のライセンスに関する詳細については、ライセンス のセクションを参照してください。

コマンド	説明
	シリアル番号を登録、または試用期間を取得するには、インターネット接続が必要です。
`log`	機能：Dr.Web for Linuxの最新のログレコードをコンソール画面（*stdout* スレッドで）に表示します（`tail` コマンドと同様）。 引数：None オプション： `-s [--Size]` *<number>* - 画面に表示される最後のログレコードの数。 `-c [--Components]` *<components list>* - そのレコードを表示する必要があるコンポーネントのIDのリストです。IDはコンマで区切って指定します。引数が指定されていない場合、あらゆるコンポーネントによってログに記録されたすべてのレコードが表示されます。 *インストールされているコンポーネントの実際のID（ログに表示される内部コンポーネント名など）は、`appinfo` コマンドを使用して指定できます（上記を参照）。* `-f [--Follow]` - ログ内の新しいメッセージを待ち、それらを受け取り次第メッセージを表示します（Ctrl + Cキーを押して待機を中断します）。

使用例

このセクションでは、Dr.Web Ctl（`drweb-ctl`）ユーティリティの使用例を示します。

- オブジェクトのスキャン：
  - シンプルなスキャンのコマンド
  - 条件によって選択されたファイルのスキャン
  - 追加のオブジェクトのスキャン
- 設定の管理
- 脅威の管理
- 自律コピーモードでの動作例

1. オブジェクトのスキャン

1.1. シンプルなスキャンのコマンド

1. デフォルトのパラメータで `/home` ディレクトリのスキャンを実行する：

```
$ drweb-ctl scan /home
```

2. `daily_scan` ファイルに含まれているパスをスキャンする（1行につき1つのパス）：

```
$ drweb-ctl scan --stdin < daily_scan
```

3. *sda* ドライブ上のブートレコードのスキャンを実行する：

```
$ drweb-ctl bootscan /dev/sda
```

4. 実行中のプロセスのスキャンを実行する:

```
$ drweb-ctl procscan
```

1.2. 条件によって選択されたファイルのスキャン

以下は、スキャンの対象となるファイルの選択と、ユーティリティ `find` の動作結果の使用例です。取得したファイルのリストは、パラメータ `--stdin` または `--stdin0` を指定して `drweb-ctl scan` コマンドに送信されます。

1. `find` ユーティリティによって返されたリストに含まれ、NUL(`\0`)記号で区切られたファイルをスキャンする:

```
$ find -print0 | drweb-ctl scan --stdin0
```

2. ファイルシステムの1つのパーティション上の、ルートディレクトリから始まり、すべてのディレクトリ内にあるすべてのファイルをスキャンする:

```
$ find / -xdev -type f | drweb-ctl scan --stdin
```

3. `/var/log/messages` および `/var/log/syslog` ファイルを除いて、ルートディレクトリから始まり、すべてのディレクトリ内にあるすべてのファイルをスキャンする:

```
$ find / -type f ! -path /var/log/messages ! -path /var/log/syslog |
drweb-ctl scan --stdin
```

4. ルートディレクトリから始まり、すべてのディレクトリ内にある *root* ユーザーのすべてのファイルをスキャンする:

```
$ find / -type f -user root | drweb-ctl scan --stdin
```

5. ルートディレクトリから始まり、すべてのディレクトリ内にある *root* および *admin* ユーザーのすべてのファイルをスキャンする:

```
$ find / -type f \( -user root -o -user admin \) | drweb-ctl scan --stdin
```

6. ルートディレクトリから始まり、すべてのディレクトリ内にある、UIDが1000～1005の範囲内にあるユーザーのファイルをスキャンする:

```
$ find / -type f -uid +999 -uid -1006 | drweb-ctl scan --stdin
```

7. ルートディレクトリから始まり、ネスティングレベルが5以下のすべてのディレクトリ内にあるファイルをスキャンする:

```
$ find / -maxdepth 5 -type f | drweb-ctl scan --stdin
```

8. サブディレクトリ内のファイルを無視して、ルートディレクトリ内にあるファイルをスキャンする:

```
$ find / -maxdepth 1 -type f | drweb-ctl scan --stdin
```

9. ルートディレクトリから始まり、すべてのディレクトリ内にあるファイルとすべてのシンボリックリンクをスキャンする:

```
$ find -L / -type f | drweb-ctl scan --stdin
```

10. ルートディレクトリから始まり、すべてのディレクトリ内にあるファイルをシンボリックリンクをたどらずにスキャンする:

```
$ find -P / -type f | drweb-ctl scan --stdin
```

11. ルートディレクトリから始まり、すべてのディレクトリ内にある2017年5月1日以前に作成されたファイルをスキャンする:

```
$ find / -type f -newermt 2017-05-01 | drweb-ctl scan --stdin
```

1.3. 追加のオブジェクトのスキャン

1. リモートホスト *192.168.0.1* 上の `/tmp` ディレクトリ内にあるオブジェクトを、*user* ユーザーとしてパスワード *passw* を使用してSSH経由でそれらに接続することでスキャンする:

```
$ drweb-ctl remotescan 192.168.0.1 /tmp --Login user --Password passw
```

2. `email.eml` ファイル内に保存されたメールメッセージを、デフォルトのルールセットを使用してスキャンする:

```
$ drweb-ctl checkmail email.eml
```

2. 設定の管理

1. 実行中のコンポーネントに関するものを含む、現在のDr.Web for Linuxパッケージに関する情報を表示する:

```
$ drweb-ctl appinfo
```

2. アクティブな設定の `[Root]` セクションからすべてのパラメータを出力する:

```
$ drweb-ctl cfshow Root
```

3. アクティブな設定の `[LinuxSpider]` セクション内で `Start` パラメータに `No` を設定する(これによりファイルシステムモニターSpIDer Guardが無効になります):

```
# drweb-ctl cfset LinuxSpider.Start No
```

このアクションを実行するにはスーパーユーザー権限が必要です。権限を昇格させるには、以下の例のように `sudo` コマンドを使用できます。

```
$ sudo drweb-ctl cfset LinuxSpider.Start No
```

4. Dr.Web for Linuxのアンチウイルスコンポーネントを強制的にアップデートする:

```
$ drweb-ctl update
```

5. Dr.Web for Linuxのコンポーネント設定を再起動する:

```
# drweb-ctl reload
```

このアクションを実行するにはスーパーユーザー権限が必要です。権限を昇格させるには、以下の例のように sudo コマンドを使用できます。

```
$ sudo drweb-ctl reload
```

6. サーバー証明書が /home/user/cscert.pem ファイルである場合に、Dr.Web for Linuxをホスト *192.168.0.1*で動作している集中管理 サーバーに接続する:

```
$ drweb-ctl esconnect 192.168.0.1 --Certificate /home/user/cscert.pem
```

7. settings.cfg 設定ファイルを使用して、Dr.Web for Linuxを集中管理 サーバーに接続する:

```
$ drweb-ctl esconnect --cfg <path to the settings.cfg file>
```

8. Dr.Web for Linuxを集中管理サーバーから切断する:

```
# drweb-ctl esdisconnect
```

このアクションを実行するにはスーパーユーザー権限が必要です。権限を昇格させるには、以下の例のように sudo コマンドを使用できます。

```
$ sudo drweb-ctl esdisconnect
```

9. drweb-update と drweb-configd によってDr.Web for Linuxログ内に作成された最後のログレコードを表示する:

```
# drweb-ctl log -c Update,ConfigD
```

3.脅威の管理

1. 検出された脅威に関する情報を表示する:

```
$ drweb-ctl threats
```

2. 隔離されていない脅威を含むファイルをすべて隔離へ移動する:

```
$ drweb-ctl threats --Quarantine All
```

3. 隔離されたファイルのリストを表示する:

```
$ drweb-ctl quarantine
```

4. 隔離からすべてのファイルを復元する:

```
$ drweb-ctl quarantine --Restore All
```

4. 自律コピーモードでの動作例

1. 自律コピーモードでファイルとプロセスをスキャンし、隔離する:

```
$ drweb-ctl scan /home/user -a --OnKnownVirus=Quarantine
$ drweb-ctl quarantine -a --Delete All
```

最初のコマンドは自律コピーモードで `/home/user` ディレクトリにあるファイルをスキャンします。既知のウイルスが含まれるファイルは隔離に移動されます。2番目のコマンドは隔離コンテンツを（自律コピーモードでも）処理し、すべてのオブジェクトを削除します。

付録

付録A. コンピューター脅威の種類

本マニュアルでは、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な損害を与え、ユーザーの情報や権限を侵害するあらゆる種類のソフトウェアを*「脅威」*と定義します（悪意のあるソフトウェアやその他の不要なソフトウェア）。広義では、コンピューターまたはネットワークのセキュリティに対するあらゆる種類の潜在的な危険（すなわちハッカー攻撃につながる脆弱性）を指して「脅威」とする場合があります。

以下に記載するすべての種類のプログラムは、ユーザーのデータまたは機密情報を危険にさらすものです。姿を隠さないプログラム（スパム配信ソフトウェアや様々なトラフィックアナライザなど）は、状況によっては脅威と化す可能性はありますが、通常はコンピューター脅威とみなされません。

コンピューターウイルス

この種類のコンピューター脅威は、他のオブジェクト内にそのコードを埋め込む（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、また埋め込ま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の分類では、ウイルスは感染させるオブジェクトの種類に応じて分けられます。

- *ファイルウイルス* - OSのファイル（通常、実行ファイルおよびダイナミックライブラリ）を感染させ、そのファイルの起動と同時にアクティブになります。
- *マクロウイルス* は、Microsoft®Officeやマクロコマンドをサポートする他のアプリケーション（Visual Basicで書かれたものなど）が使用す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、完全に機能するプログラミング言語で書かれた一種の実装プログラム（マクロ）です。たとえば、Microsoft® Wordでは、文書を開く（閉じる、保存するなど）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、他のスクリプト（OSのサービスファイルなど）を感染させます。また、スクリプトの実行が可能な他のファイルフォーマットも感染させることができ、Webアプリケーションにおけるスクリプトの脆弱性を悪用します。
- *ブートウイルス* - ディスクのブートレコード、ハードディスクドライブのパーティションまたはマスターブートレコードを感染させます。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、そのタスクを続行できる状態を保ちます。

多くのウイルスは検出に対抗する何らかの手段を持ち、その手法は常時改良され続けています。すべてのウイルスは、その使用する手法に応じて分類できます。

- *暗号化ウイルス* - ファイル、ブートセクター、またはメモリ内で検出されるのを防ぐため、感染の度に自身のコードを暗号化します。このウイルスのコピーはすべて、ウイルスのシグネチャとして使用される共通のコードフラグメント（復号プロシージャ）のみを含んでいます。
- *ポリモーフィック型ウイルス* - 同様に自身のコードを暗号化しますが、コピーごとに異なる特別な復号プロシージャの生成も行います。つまり、この種類のウイルスはシグネチャバイトを持ちません。
- *ステルスウイルス* - その活動を偽り、感染したオブジェクト内に潜むための動作を実行します。この種類のウイルスは、感染させる前のオブジェクトの情報を「ダミー」として表示させ、改変したファイルが検出されないようにします。

ウイルスは、書かれているプログラミング言語（ほとんどの場合アセンブラ、高級プログラミング言語、スクリプト言語など）、または感染させるOSに応じて分類することもできます。

コンピューターワーム

「コンピューターワーム」型の悪意のあるプログラムは、ウイルスやその他のマルウェアよりも多く見られるようになってきています。ウイルス同様、自身を複製し拡散できますが、他のオブジェクトを感染させることはありません。ネットワークを通じて（通常、メールの添付ファイルとして）侵入し、ネットワーク内にある他のコンピューターにコピーを拡散します。ユーザーの操作に応じて、または攻撃するコンピューターを選択する自動モードで拡散を開始します。

ワームは1つのファイル（ワームの本体）のみで構成されているとは限りません。多くのワームが、メインメモリ（RAM）内に読み込んだ後にワームの本体を実行ファイルとしてネットワーク経由でダウンロードする感染部分（シェルコード）を持っています。シェルコードがシステム内に存在するだけであれば、システムを再起動することで（RAMが削除されリセットされます）ワームを削除できますが、ワームの本体がコンピューターに侵入してしまった場合はアンチウイルスプログラムのみが対処可能です。

ワームはその驚異的な拡散速度によって、ペイロードを持っていない（直接的な被害を与えない）場合であっても、ネットワーク全体の機能を破壊する能力を持っています。

Doctor Webの分類では、ワームはその拡散方法によって以下のように分けられます。

- *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自身のコピーを拡散します。
- *メールワーム* - メールプロトコル（POP3、SMTPなど）を使用して拡散します。
- *チャットワーム* - 広く使用されているメッセンジャーおよび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。

トロイの木馬プログラム

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

トロイの木馬の悪意のある特徴はウイルスのものと類似しており、またトロイの木馬がウイルスのコンポーネントであるという場合もあります。しかし、ほとんどのトロイの木馬は、ユーザーまたはシステムタスクによって起動される個別の実行ファイルとして配布されます（ファイル交換サーバー、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）。

トロイの木馬はしばしばウイルスやワームによって配布されることや、他の種類の脅威によっても実行されうる悪意のある動作の多くがトロイの木馬にも起因することから、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では個別の種類として分類されています。

- *バックドア* - 既存のアクセスおよびセキュリティシステムをすり抜けて侵入者がシステム内にログイン、または権限を必要とする機能を使用することを可能にしてしまうトロイの木馬です。バックドアはファイルを感染させませんが、自身をレジストリ内に書き込んでレジストリキーを改変します。
- *ルートキット* - その存在を隠す目的で、OSのシステム機能を妨害するように設計された悪意のあるプログラムです。さらに、他のプログラム（他の脅威など）のプロセスや異なるレジストリキー、フォルダ、ファイルを隠ぺいすることもできます。ルートキットは独立したプログラムとして、または他の悪意のあるプログラムに含まれるコンポーネントとして拡散されます。また、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、自身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で入力した情報を記録します。その目的は個人情報（ネットワークパスワード、ログイン、クレジットカードデータなど）を盗むことです。
- *クリッカー* - Webサイトのトラフィックを増加させる目的で、またはDDoS攻撃を実行するためにハイパーリンクを別のアドレスにリダレクトします。
- *プロキシ型トロイの木馬* - 被害者のコンピューターを介して匿名でインターネットにアクセスすることを可能にします。

トロイの木馬は、Webブラウザのスタートページを変更したり特定のファイルを削除したりするなど、これら以外の悪意のある動作も実行することがあります。ただしそのような動作もまた、他の種類の脅威（ウイルスやワーム）によって実行される場合があります。

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その他のコンピューター保護システムコンポーネントの脆弱性を検出するポートスキャナです。それらのツールはハッカーだけではなく、管理者がネットワークのセキュリティを検査するためにも用いられます。ハッキングに使用することの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含まれることがあります。

アドウェア

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布されてWebブラウザ上に広告を表示させる場合もあります。アドウェアプログラムの多くは、スパイウェアによって収集されたデータを用いています。

ジョークプログラム

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

ダイアラー

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

リスクウェア

これらのソフトウェアアプリケーションは悪意のある目的のために作成されたものではありませんが、コンピューターセキュリティに対する脅威となりうる特徴を持っているため、危険度の低い脅威として分類されます。リスクウェアプログラムはデータを破損または削除してしまう可能性があるのみならず、クラッカー（悪意のあるハッカー）や悪意のあるプログラムによって、システムに被害を与える目的で使用されることがあります。そのようなプログラムの中には、さまざまなリモートチャットおよび管理ツール、FTPサーバーなどがあります。

疑わしいオブジェクト

これらは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。そのようなオブジェクトはいかなる脅威（未知のものを含む）でもありえ、また誤検出の場合には安全なオブジェクトである可能性もあります。疑わしいオブジェクトを含むファイルは隔離に移すことが推奨されます。また、疑わしいオブジェクトは解析のために Doctor Webウイルスラボに送信してください。

付録B. コンピューター脅威の駆除

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

- 検出方法
- 脅威に関連したアクション

検出方法

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ために必要かつ十分な、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ため、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ユーザーはランサムウェアであ る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他、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

プログラムコードエミュレーションの技術は、チェックサムによる検索が直接適用できない場合、または実行するのが非常に困難な場合（安全な署名を構築することが不可能なため）に、ポリモーフィック型ウイルスと暗号化ウイルスの検出に使用されます。この方法は、*エミュレーター*、つまりプロセッサーとランタイム環境のプログラミングモデルによる解析コード実行のシミュレーションを意味します。エミュレーターは保護されたメモリ領域（エミュレーションバッファ）で動作し、解析されたプログラムの実行は命令ごとにモデル化されます。ただし、これらの命令は実際にはCPUによって実行されるものではありません。エミュレーターがポリモーフィック型ウイルスに感染したファイルを受信すると、エミュレーションの結果は復号されたウイルスコードになります。これは、シグネチャチェックサムを検索することで簡単に判別できます。

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しきい値を超

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パック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のエラーを生じさせる可能性があります（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。

上の検出手法に加え、Dr.Webアンチウイルスソリューションは既知の悪意のあるソフトウェアに関する最も新しい情報も使用します。Doctor Webアンチウイルスラボ のエキスパートによって新しい脅威が発見されると、そのウイルスシグネチャ、振る舞い特性、属性を追加した更新が即座に配信されます。更新は1時間に数回行われる場合もあり、たとえ新種のウイルスがDr.Web常駐保護を通過してシステムに侵入した場合でも、更新後には検出され駆除されます。

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）。

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 Cloud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。

Dr.Web Cloud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。

アクション

コンピューター脅威を回避するために、Dr.Webアンチウイルス製品は悪意のあるオブジェクトに対して様々なアクションを適用します。ユーザーはデフォルト設定を使用、自動的に適用するアクションを設定、あるいは検出の度に手動でアクションを選択できます。使用可能なアクションは以下のとおりです。

- **Ignore** *(無視)* - いずれのアクションも実行せず、検出された脅威をスキップします。
- **Report** *(報告)* - アクションを適用せず、検出された脅威について通知します。
- **Cure** *(修復)* - 感染したオブジェクトから悪意のあるコンテンツのみを削除し、修復します。ただし、すべての種類の脅威に対して適用できるわけではありません。
- **Quarantine** *(隔離)* - 検出された脅威を特別なフォルダに移し、残りのシステムから隔離します。
- **Delete** *(削除)* - 感染したオブジェクトを永久に削除します。

コンテナ（アーカイブ、メール添付ファイルなど）内のファイルで脅威が検出された場合は、削除アクションの代わりにコンテナの隔離への移動が実行されます。

付録C. 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。

問題に対する円滑な対応を可能にするため、テクニカルサポートにご連絡いただく前に、インストールされた製品とその設定、およびシステム環境に関するデータセットを生成することをお勧めします。これは、Dr.Web for Linuxディストリビューションに含まれている特別なユーティリティを使用して行うことができます。

テクニカルサポートに提出するデータを収集するには、次のコマンドを使用します。

```
# /opt/drweb.com/bin/support-report.sh
```

テクニカルサポートに提出するデータを収集する際は、ユーティリティをスーパーユーザー権限（*root*ユーザーの権限）で起動することをお勧めします。権限を昇格するには、`su` コマンド（カレントユーザーを変更する）または `sudo` コマンド（指定されたコマンドを別のユーザーの権限で実行する）を使用します。

ユーティリティは次の情報を収集してアーカイブします。

- OSに関するデータ（名前、アーキテクチャ、`uname -a` コマンドの結果）
- Doctor Webパッケージを含む、システムにインストールされているパッケージのリスト
- ログの内容
  - Dr.Web for Linuxのログ（コンポーネントごとに設定されている場合）
  - `syslog` システムデーモンのログ（`/var/log/syslog`、`/var/log/messages`）
  - システムパッケージマネージャーのログ（`apt`、`yum` など）
  - `dmesg` のログ
- 5.次のコマンドを実行します：`df`, `ip a` (`ifconfig -a`), `ldconfig -p`, `iptables-save`, `nft export xml`
- Dr.Web for Linuxの設定と構成に関する情報：
  - ダウンロードされたウイルスデータベースのリスト（`drweb-ctl baseinfo -l`）

- Dr.Web for Linuxディレクトリにあるファイルのリストとそれらファイルの MD5ハッシュ値
- スキャンエンジンDr.Web Virus-Finding EngineのバージョンとMD5ハッシュ値
- Dr.Web for Linuxの設定パラメーター（`drweb.ini` の内容、ルール、ルールで使用される値のファイル、Luaプロシージャなどを含む）
- Dr.Web for Linuxがスタンドアロンモードで動作している場合、キーファイルから取得したユーザーの情報と権限

製品とそのシステム環境に関する情報を含むアーカイブは、ユーティリティを起動したユーザーのホームディレクトリに保存されます。ファイルの名前は次のようになります。

```
drweb.report.<timestamp>.tgz
```

<timestamp> は、レポート作成のタイムスタンプ（ミリ秒単位）です（例：`20190618151718.23625`）。

付録D. 既知のエラー

このセクションの内容:

本セクション内に記載されていないエラーが発生した場合は、テクニカルサポートまでご連絡ください。その際、エラーコードと、問題を再現するための手順をお伝えください。

エラーを特定するための推奨事項

- エラーの考えられる原因や背景を特定するには、Dr.Web for Linuxのログを参照してください(デフォルトでは、OSによって `/var/log/syslog` ファイルまたは `/var/log/messages` ファイルにあります)。また、コマンド `drweb-ctl log` を使用することもできます。
- エラーを特定するために、個別のファイルにログを記録するよう設定し、ログへの広範な情報の出力を有効にすることが推奨されます。そのために、以下のコマンドを実行してください。

```
# drweb-ctl cfset Root.Log <path to log file>
# drweb-ctl cfset Root.DefaultLogLevel DEBUG
```

- デフォルトのロギング方法とログの詳細レベルに戻すには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.Log -r
# drweb-ctl cfset Root.DefaultLogLevel -r
```

エラーコード

エラーメッセージ	*モニターチャネルに関するエラー*
エラーコード	x1
説明	コンポーネントの1つが設定デーモンDr.Web ConfigDと接続できません。

エラーの解決:

1. 以下のコマンドを実行することで設定デーモンを再起動させてください。

```
# service drweb-configd restart
```

2. PAMの認証メカニズムがインストール、設定されていて、正常に動作していることを確認します。そうでない場合は、インストール・設定します(詳細についてはお使いのOSディストリビューション向けの管理者ガイドとマニュアルを参照してください)。
3. PAMが正常に設定されていて、設定デーモンを再起動しても問題が解決しない場合は、Dr.Web for Linux設定をデフォルトに復元してください。

そのために、たとえば以下のコマンドを実行するなどして、*<etc_dir>*/drweb.ini ファイルのコンテンツを削除します（設定ファイルのバックアップを作成することが推奨されます）：

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

設定ファイルのコンテンツを削除した後に設定デーモンを再起動させます。

4. 設定デーモンを起動することができない場合は、drweb-configd パッケージを再インストールしてください。

   Dr.Web for LinuxまたはDr.Web for Linuxコンポーネントのインストールとアンインストールの方法については、Dr.Web for Linuxをインストールする および Dr.Web for Linuxをアンインストールする のセクションを参照してください。

引き続きエラーが発生する場合は テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*操作はすでに実行中です*
エラーコード	x2
説明	ユーザーによって要求された操作はすでに実行中です。
エラーの解決： 1. 操作が完了するまでお待ちください。必要に応じ、しばらく時間をおいて再度アクションを実行します。	
引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*操作は保留中です*
エラーコード	x3
説明	ユーザーによって要求された操作は保留の状態です（ネットワーク接続を確立中、またはDr.Web for Linuxコンポーネントの1つがローディング中や初期化中で時間を要するなどの理由）。
エラーの解決： 1. 操作が開始されるまでお待ちください。必要に応じ、しばらく時間をおいて再度アクションを実行します。	
引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*ユーザーによって中断されました*
エラーコード	x4
説明	アクションはユーザーによって終了されました（時間がかかるなどの理由）。
エラーの解決： 1. しばらく時間をおいて再度アクションを実行します。	
引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*操作がキャンセルされました*
エラーコード	x5
説明	アクションがキャンセルされました（アクションの実行がタイムアウトした可能性があります）。
エラーの解決：	
1. 再度アクションを実行します。	
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*IPC接続が切断されました*
エラーコード	x6
説明	コンポーネントの1つのプロセス間通信（IPC）が切断されました（多くの場合、ユーザーのコマンドによって、またはアイドル状態であるためにコンポーネントがシャットダウンしたことによって）。
エラーの解決：	
1. 操作が完了していない場合は、再度開始してください。そうでない場合、シャットダウンはエラーではありません。	
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*無効なIPCメッセージサイズです*
エラーコード	x7
説明	コンポーネントのプロセス間通信（IPC）中に無効なサイズのメッセージを受信しました。
エラーの解決：	
1. 以下のコマンドを入力し、Dr.Web for Linuxをアンインストールします。 `# service drweb-configd restart`	
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*無効なIPCメッセージフォーマットです*
エラーコード	x8
説明	コンポーネントのプロセス間通信（IPC）中に無効なフォーマットのメッセージを受信しました。
エラーの解決：	
1. 以下のコマンドを入力し、Dr.Web for Linuxをアンインストールします。	

```
# service drweb-configd restart
```

引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*準備が完了していません*
エラーコード	x9
説明	必要なコンポーネントまたはデバイスがまだ初期化されていないため、要求されたアクションを実行できません。

エラーの解決：

1. しばらく時間をおいて再度アクションを実行します。

引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*コンポーネントがインストールされていません*
エラーコード	x10
説明	必要なコンポーネントがまだインストールされていないため、必要な操作を実行できません。

エラーの解決：

1. 必要なコンポーネントが含まれたパッケージをインストールまたは再インストールします。
   - Scannerがインストールされていない場合：`drweb-filecheck`
   - SpIDer Guardがインストールされていない場合：`drweb-spider`
   - SpIDer Gateがインストールされていない場合：`drweb-gated`
   - Updaterがインストールされていない場合：`drweb-update`
2. 引き続きエラーが発生する場合や、どのコンポーネントがインストールされていないのか特定できない場合は、Dr.Web for Linuxをアンインストールし、再度システムにインストールします。

   Dr.Web for LinuxまたはDr.Web for Linuxコンポーネントのインストールとアンインストールの方法については、Dr.Web for Linuxをインストールする および Dr.Web for Linuxをアンインストールする のセクションを参照してください。

引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*予期せぬIPCメッセージです*
エラーコード	x11
説明	コンポーネントのプロセス間通信（IPC）中に予期せぬメッセージを受信しました。

エラーの解決：

1. 以下のコマンドを入力し、Dr.Web for Linuxをアンインストールします。

```
# service drweb-configd restart
```

引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*IPCプロトコル違反です*
エラーコード	x12
説明	コンポーネントのプロセス間通信（IPC）中にプロトコル違反が発生しました。

エラーの解決：

1. 以下のコマンドを入力し、Dr.Web for Linuxをアンインストールします。

```
# service drweb-configd restart
```

引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*サブシステムの状態が未知です*
エラーコード	x13
説明	要求された操作を実行するために必要なサブシステムの現在の状態が不明です。

エラーの解決：

1. 操作を繰り返します。
2. 引き続きエラーが発生する場合は、以下のコマンドを実行することでDr.Web for Linuxを再起動させてください。

```
# service drweb-configd restart
```

その後、操作を繰り返します。

引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*パスは絶対パスでなければなりません*
エラーコード	x20
説明	ファイルまたはディレクトリへの絶対パスが必要ですが、相対パスが指定されています。

エラーの解決：

1. 絶対パスになるよう、ファイルまたはディレクトリへのパスを変更します。

引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*十分なメモリがありません*
エラーコード	x21
説明	要求された操作（サイズの大きなファイルを開く、など）を完了するために必要な、十分なメモリがありません。
エラーの解決：	
1. Dr.Web for Linuxプロセスが使用可能なメモリのサイズを増やし（`ulimit` コマンドで上限を変更するなどして）、プログラムを再起動して操作を繰り返します。	
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*IOエラー*
エラーコード	x22
説明	入出力（I/O）エラーが発生しました（ドライブがまだ初期化されていない、またはファイルシステムのパーティションをもはや使用できない、など）。
エラーの解決：	
1. 必要なI/Oデバイスまたはファイルシステムのパーティションが使用可能であるかどうかを確認します。必要に応じ、それをマウントして操作を繰り返します。	
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*そのようなファイルまたはディレクトリがありません*
エラーコード	x23
説明	指定された、ファイルシステムのオブジェクト（ファイルまたはディレクトリ）がありません。削除された可能性があります。
エラーの解決：	
1. パスを確認します。必要に応じ、それを変更して操作を繰り返します。	
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*パーミッションが拒否されました*
エラーコード	x24
説明	指定された、ファイルシステムのオブジェクト（ファイルまたはディレクトリ）にアクセスする十分な権限がありません。
エラーの解決：	
1. パスが正しいかどうか、また、コンポーネントが要求される権限を持っているかどうかを確認します。オブジェクトにアクセスする必要がある場合、アクセス権限を変更するか、コンポーネントの権限を昇格させます。操作を繰り返します。	

引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*ディレクトリではありません*
エラーコード	x25
説明	ファイルシステムの、指定されたオブジェクトがディレクトリではありません。ディレクトリへのパスを入力します。
エラーの解決：	
1. パスを確認します。それを変更し、操作を繰り返します。	
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*データファイルが破損しています*
エラーコード	x26
説明	要求されたデータが破損しています。
エラーの解決：	
1. 操作を繰り返します。 2. 引き続きエラーが発生する場合は、以下のコマンドを実行することでDr.Web for Linuxを再起動させてください。 `# service drweb-configd restart` その後、操作を繰り返します。	
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*ファイルはすでに存在しています*
エラーコード	x27
説明	ファイルの作成を試みる際に、同じ名前を持つ別のファイルが検出されました。
エラーの解決：	
1. パスを確認します。それを変更し、操作を繰り返します。	
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*読み取り専用ファイルシステム*
エラーコード	x28
説明	要求しようとしているファイルシステムは読み取り専用です。

エラーの解決： 1. パスを確認します。ファイルシステムの書き込み可能なパーティションを指すようにパスを変更し、操作を繰り返します。
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*ネットワークエラー*
エラーコード	x29
説明	ネットワークエラーが発生しました（リモートホストが予期せず応答を停止したか、必要な接続に失敗した可能性があります）。
エラーの解決： 1. ネットワークが使用可能であること、ネットワーク設定が正しいことを確認します。必要に応じ、ネットワーク設定を変更し、操作を繰り返します。	
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*ドライブではありません*
エラーコード	x30
説明	アクセスしようとしている入出力（I/O）がドライブではありません。
エラーの解決： 1. ドライブ名を確認します。ドライブを指すようにパスを変更し、操作を繰り返します。	
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*予期せぬEOFがあります*
エラーコード	x31
説明	データの読み込み中に、予期せずファイルの末尾に達しました。
エラーの解決： 1. ファイル名を確認します。必要に応じ、正しいファイルを指すようにパスを変更し、操作を繰り返します。	
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*ファイルが変更されています*
エラーコード	x32
説明	スキャン中にファイルの変更が検出されました。
エラーの解決：	

1. 再スキャンしてください。
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*通常ファイルではありません*
エラーコード	x33
説明	アクセスしようとしているオブジェクトは通常ファイルではありません。ディレクトリ、ソケット、またはファイルシステム内のその他のオブジェクトである可能性があります。
エラーの解決：	
1. ファイル名を確認します。必要に応じ、通常のファイルを指すようにパスを変更し、操作を繰り返します。	
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*名前はすでに使用されています*
エラーコード	x34
説明	ファイルシステムのオブジェクト（ディレクトリ、ファイル、ソケット）の作成を試みた際に、同じ名前を持つ別のオブジェクトが検出されました。
エラーの解決：	
1. パスを確認します。それを変更し、操作を繰り返します。	
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*ホストがオフラインです*
エラーコード	x35
説明	ネットワーク経由でリモートホストを使用できません。
エラーの解決：	
1. 必要なホストが使用可能であるかどうかを確認します。必要に応じ、ホストアドレスを変更して操作を繰り返します。	
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*リソースの上限に達しています*
エラーコード	x36
説明	特定のリソースの使用について設定された上限に達しています。
エラーの解決：	

1. 必要なリソースの使用可能状況を確認します。必要に応じ、このリソースの使用に関する上限を引き上げて、操作を繰り返します。
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*異なるマウントポイントです*
エラーコード	x37
説明	ファイルを復元する試みが、2つの異なるマウントポイント間での移動を意味しています。
エラーの解決：	
1. ファイルを復元する別のパスを選択し、操作を繰り返します。	
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*アンパックエラー*
エラーコード	x38
説明	アーカイブの解凍に失敗しました（ファイルがパスワードで保護されているか、破損している可能性があります）。
エラーの解決：	
1. ファイルが破損していないことを確認します。アーカイブがパスワード保護されている場合、正しいパスワードを入力することで保護を解除し、操作を繰り返します。	
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*ウイルスデータベースが破損しています*
エラーコード	x40
説明	ウイルスデータベースが破損しています。
エラーの解決：	

1. ウイルスデータベースディレクトリへのパスを確認してください。必要に応じてパスを変更します（設定ファイルの `[Root]` セクションにある `VirusBaseDir` パラメータ）。

   パスの確認・修正には、コマンドライン管理ツールの コマンド を使用します。

   - 現在のパラメータ値を確認するには、以下のコマンドを実行します。

     ```
     $ drweb-ctl cfshow Root.VirusBaseDir
     ```

   - 新しいパラメータ値を設定するには、以下のコマンドを実行します。

     ```
     # drweb-ctl cfset Root.VirusBaseDir <new path>
     ```

   - パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.VirusBaseDir -r
```

2. 以下のいずれかの方法でウイルスデータベースを更新します。
   - アプリケーションの メインウィンドウ 内にある更新管理ページ で 更新 をクリックします。
   - 通知領域にあるステータスインジケータの コンテキストメニュー で 更新 をクリックします。
   - コマンド を実行します。

```
$ drweb-ctl update
```

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*サポートされていないバージョンのウイルスデータベースです*
エラーコード	x41
説明	現在のウイルスデータベースは、以前のバージョンのプログラム用に設計されています。

エラーの解決：

1. ウイルスデータベースディレクトリへのパスを確認してください。必要に応じてパスを変更します（設定ファイルの [Root] セクションにある VirusBaseDir パラメータ）。

   パスの確認・修正には、コマンドライン管理ツールの コマンド を使用します。
   - 現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow Root.VirusBaseDir
```

   - 新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.VirusBaseDir <new path>
```

   - パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.VirusBaseDir -r
```

2. 以下のいずれかの方法でウイルスデータベースを更新します。
   - アプリケーションの メインウィンドウ 内にある更新管理ページ で 更新 をクリックします。
   - 通知領域にあるステータスインジケータの コンテキストメニュー で 更新 をクリックします。
   - コマンド を実行します。

```
$ drweb-ctl update
```

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*ウイルスデータベースが空です*
エラーコード	x42

説明	ウイルスデータベースが空です。

エラーの解決：

1. ウイルスデータベースディレクトリへのパスを確認してください。必要に応じてパスを変更します（設定ファイルの `[Root]` セクションにある `VirusBaseDir` パラメータ）。

   パスの確認・修正には、コマンドライン管理ツールの コマンド を使用します。

   - 現在のパラメータ値を確認するには、以下のコマンドを実行します。

     ```
     $ drweb-ctl cfshow Root.VirusBaseDir
     ```

   - 新しいパラメータ値を設定するには、以下のコマンドを実行します。

     ```
     # drweb-ctl cfset Root.VirusBaseDir <new path>
     ```

   - パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

     ```
     # drweb-ctl cfset Root.VirusBaseDir -r
     ```

2. 以下のいずれかの方法でウイルスデータベースを更新します。
   - アプリケーションの メインウィンドウ 内にある更新管理ページ で **更新** をクリックします。
   - 通知領域にあるステータスインジケータの コンテキストメニュー で **更新** をクリックします。
   - コマンド を実行します。

     ```
     $ drweb-ctl update
     ```

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*オブジェクトを修復できません*
エラーコード	x43
説明	脅威の駆除中に、修復不可能なオブジェクトに対して修復アクションを適用する試みが行われました。

エラーの解決：

1. オブジェクトに対して適用可能なアクションを選択し、操作を繰り返します。

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*サポートされていないウイルスデータベースの組み合わせです*
エラーコード	x44
説明	現在のウイルスデータベースの組み合わせはサポートされていません。

エラーの解決：

1. ウイルスデータベースディレクトリへのパスを確認してください。必要に応じてパスを変更します（設定ファイルの `[Root]` セクションにある `VirusBaseDir` パラメータ）。

パスの確認・修正には、コマンドライン管理ツールの コマンド を使用します。

- 現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow Root.VirusBaseDir
```

- 新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.VirusBaseDir <new path>
```

- パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.VirusBaseDir -r
```

2. 以下のいずれかの方法でウイルスデータベースを更新します。
   - アプリケーションの メインウィンドウ 内にある更新管理ページ で **更新** をクリックします。
   - 通知領域にあるステータスインジケータの コンテキストメニュー で **更新** をクリックします。
   - コマンド を実行します。

```
$ drweb-ctl update
```

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*スキャンの上限に達しています*
エラーコード	x45
説明	オブジェクトのスキャン中に、指定された上限に達しました(アンパックされたファイルのサイズ上限、ネスティングレベルの上限など)。

エラーの解決:

1. 以下のいずれかの方法で、スキャンにおける上限を変更します(コンポーネント設定内で)。
   - アプリケーションの 設定 ウィンドウ内、コンポーネント設定のページで
   - `drweb-ctl cfshow` および `drweb-ctl cfset` コマンド を使用して
2. 設定の変更後、試みた操作を繰り返します。

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*認証に失敗しました*
エラーコード	x47
説明	認証に、無効なユーザー認証情報が使用されました。

エラーの解決:

1. 必要な権限を持ったユーザーの有効な認証情報を入力して、再度、認証を実行してください。

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*認証に失敗しました*
エラーコード	x48
説明	カレントユーザーには、要求された操作を実行するための十分な権限がありません。
エラーの解決：	
1. 必要な権限を持ったユーザーの有効な認証情報を入力して、再度、認証を実行してください。	
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*無効なアクセストークンです*
エラーコード	x49
説明	Dr.Web for Linuxコンポーネントの1つが、昇格された権限を必要とする操作へのアクセスを試みる際に無効な認証トークンを提示しました。
エラーの解決：	
1. 必要な権限を持ったユーザーの有効な認証情報を入力して、再度、認証を実行してください。	
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*無効な引数です*
エラーコード	x60
説明	コマンドを実行しようとした際に無効な引数が使用されました。
エラーの解決：	
1. 有効な引数を使用して、再度アクションを実行します。	
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*無効な操作です*
エラーコード	x61
説明	無効なコマンドを実行しようとする試みが検出されました。
エラーの解決：	
1. 有効なコマンドを使用して、再度アクションを実行します。	
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*root権限が必要です*

エラーコード	x62
説明	このアクションを実行することができるのは、root権限を持ったユーザーのみです。
エラーの解決： 1. 権限をルート権限に昇格させ、再度アクションを実行します。権限を昇格させるには、su および sudo コマンドを使用します。	
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*集中管理モードでは許可されていません*
エラーコード	x63
説明	要求されたアクションは、Dr.Web for Linuxがスタンドアロンモードで動作している場合のみ実行できます。
エラーの解決： 1. Dr.Web for Linuxの動作モードをスタンドアロンモードに変更し、操作を繰り返します。 2. 動作モードをスタンドアロンモードに変更するには、 • モード設定ページで Enable the central protection mode チェックボックスのチェックを外します。 • または、コマンドを実行します。 `# drweb-ctl esdisconnect`	
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*サポートされていないOSです*
エラーコード	x64
説明	Dr.Web for Linuxは、ホスト上にインストールされているOSをサポートしていません。
エラーの解決： 1. システム要件のリスト内に記載されているOSをインストールします。	
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*実装されていない機能です*
エラーコード	x65
説明	コンポーネントの1つの、必要な機能がプログラムの現在のバージョンには備わっていません。

エラーの解決：

1. 設定ファイル `/etc/opt/drweb.com/drweb.ini` のコンテンツをクリアすることで、Dr.Web for Linuxのデフォルト設定を復元してください。この手順を実行する前にファイルのバックアップを作成することが推奨されます。例：

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

2. 設定ファイルのコンテンツを削除した後に、次のコマンドを実行することでDr.Web for Linuxを再起動させます。

```
# service drweb-configd restart
```

引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*未知のオプションです*
エラーコード	x66
説明	設定ファイルに、未知のパラメータまたはDr.Web for Linuxの現在のバージョンでサポートされていないパラメータが含まれています。

エラーの解決：

1. いずれかのテキストエディタで `/etc/opt/drweb.com/drweb.ini` ファイルを開き、無効なパラメータを含む行を削除します。ファイルを保存し、次のコマンドを実行することでDr.Web for Linuxを再起動します。

```
# service drweb-configd restart
```

2. 問題が解決しない場合は、Dr.Web for Linux設定をデフォルトに戻してしてください。

   設定をデフォルトに戻すには、次のコマンドを実行するなどによって、設定ファイル `/etc/opt/drweb.com/drweb.ini` のコンテンツをクリアします（設定ファイルのバックアップを作成することが推奨されます）。

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

   設定ファイルのコンテンツを削除した後に、Dr.Web for Linuxを再起動させます。

引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*未知のセクションです*
エラーコード	x67
説明	設定ファイルに、未知のセクションまたはDr.Web for Linuxの現在のバージョンでサポートされていないセクションが含まれています。

エラーの解決：

1. いずれかのテキストエディタで /etc/opt/drweb.com/drweb.ini ファイルを開き、未知のセクションを削除してください。ファイルを保存し、次のコマンドを実行することでDr.Web for Linuxを再起動します。

```
# service drweb-configd restart
```

2. 問題が解決しない場合は、Dr.Web for Linux設定をデフォルトに戻してしてください。

   設定をデフォルトに戻すには、次のコマンドを実行するなどによって、設定ファイル /etc/opt/drweb.com/drweb.ini のコンテンツをクリアします（設定ファイルのバックアップを作成することが推奨されます）。

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

   設定ファイルのコンテンツを削除した後に、Dr.Web for Linuxを再起動させます。

引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*無効なオプション値です*
エラーコード	x68
説明	設定ファイル内の1つまたは複数のパラメータ値が無効です。

エラーの解決：

1. 以下のいずれかの方法で、有効なパラメータ値を設定します。
   - アプリケーションの 設定 ウィンドウ内、コンポーネント設定のページで
   - drweb-ctl cfshow および drweb-ctl cfset コマンドを使用して

   当該パラメータの有効な値が分からない場合は、そのパラメータを使用するコンポーネントのヘルプファイルを参照してください。パラメータ値をデフォルト値に戻すこともできます。
2. または、設定ファイル /etc/opt/drweb.com/drweb.ini を直接編集することも可能です。その場合は、いずれかのテキストディタで設定ファイルを開き、無効なパラメータ値を含む行を見つけ、有効な値を設定します。その後、ファイルを保存し、以下のコマンドを実行することでDr.Web for Linuxを再起動させます。

```
# service drweb-configd restart
```

3. この手順で問題が解決しない場合は、Dr.Web for Linux設定をデフォルトに戻してください。

   設定をデフォルトに戻すには、次のコマンドを実行するなどによって、設定ファイル /etc/opt/drweb.com/drweb.ini のコンテンツをクリアします（設定ファイルのバックアップを作成することが推奨されます）。

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

   設定ファイルのコンテンツを削除した後に、Dr.Web for Linuxを再起動させます。

引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*無効な状態です*

エラーコード	x69
説明	Dr.Web for Linux、またはコンポーネントの1つが、要求された操作を完了させることのできない状態にあります。

エラーの解決：

1. しばらく時間をおいて再度アクションを実行します。
2. 引き続きエラーが発生する場合は、以下のコマンドを実行することでDr.Web for Linuxを再起動させてください。

```
# service drweb-configd restart
```

引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*使用可能な値は1つのみです*
エラーコード	x70
説明	設定ファイルでは、値のリストは単一値パラメータから成ります。

エラーの解決：

1. 以下のいずれかの方法で、有効なパラメータ値を設定します。
   - アプリケーションの 設定 ウィンドウ内、コンポーネント設定のページで
   - `drweb-ctl cfshow` および `drweb-ctl cfset` コマンドを使用して

   当該パラメータの有効な値が分からない場合は、そのパラメータを使用するコンポーネントのヘルプファイルを参照してください。パラメータ値をデフォルト値に戻すこともできます。
2. または、設定ファイル `/etc/opt/drweb.com/drweb.ini` を直接編集することも可能です。その場合は、いずれかのテキストディタで設定ファイルを開き、無効なパラメータ値を含む行を見つけ、有効な値を設定します。その後、ファイルを保存し、以下のコマンドを実行することでDr.Web for Linuxを再起動させます。

```
# service drweb-configd restart
```

3. この手順で問題が解決しない場合は、Dr.Web for Linux設定をデフォルトに戻してください。

   設定をデフォルトに戻すには、次のコマンドを実行するなどによって、設定ファイル `/etc/opt/drweb.com/drweb.ini` のコンテンツをクリアします（設定ファイルのバックアップを作成することが推奨されます）。

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

   設定ファイルのコンテンツを削除した後に、Dr.Web for Linuxを再起動させます。

引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*レコードが見つかりません*
エラーコード	x80

説明	脅威のレコードがありません（他のDr.Web for Linuxコンポーネントによって処理された可能性があります）。
エラーの解決： 1. しばらくしてから脅威のリストを更新してください。	
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*レコードは現在処理中です*
エラーコード	x81
説明	脅威のレコードは、他のDr.Web for Linuxコンポーネントによって処理されています。
エラーの解決： 1. しばらくしてから脅威のリストを更新してください。	
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*ファイルはすでに隔離済みです*
エラーコード	x82
説明	ファイルはすでに隔離されています（脅威が別のDr.Web for Linuxコンポーネントによって処理された可能性があります）。
エラーの解決： 1. しばらくしてから脅威のリストを更新してください。	
引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。	

エラーメッセージ	*更新前にバックアップを行うことができません*
エラーコード	x89
説明	更新サーバーから更新をダウンロードする前に対象となるファイルのバックアップコピーを作成しようとする試みが失敗しました。

エラーの解決：

1. 更新されたファイルのバックアップコピーを保存するディレクトリへのパスを確認します。必要に応じてパスを変更します（設定ファイルの `[Update]` セクションにある `BackupDir` パラメータ）。

   パスの確認・修正には、コマンドライン管理ツールの コマンド を使用できます。

   - 現在のパラメータ値を確認するには、以下のコマンドを実行します。

     ```
     $ drweb-ctl cfshow Update.BackupDir
     ```

   - 新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Update.BackupDir <new path>
```

- パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Update.BackupDir -r
```

2. 以下のいずれかの方法でウイルスデータベースを更新します。
   - アプリケーションの メインウィンドウ 内にある更新管理ページで 更新 をクリックします。
   - 通知領域にあるステータスインジケータの コンテキストメニュー で 更新 をクリックします。
   - コマンド を実行します。

```
$ drweb-ctl update
```

3. 引き続きエラーが発生する場合は、更新コンポーネントを実行しているユーザーアカウントが BackupDir で指定されているディレクトリへの書き込み権限を持っているかどうかを確認します。このユーザーの名前は RunAsUser パラメータ内で指定されます。必要に応じ、RunAsUser パラメータ内で指定されたユーザー名を変更するか、足りない権限をディレクトリのプロパティ内で与えます。
4. それでもエラーが続く場合は、drweb-update パッケージを再インストールします。

   Dr.Web for LinuxまたはDr.Web for Linuxコンポーネントのインストールとアンインストールの方法については、Dr.Web for Linuxをインストールする および Dr.Web for Linuxをアンインストールする のセクションを参照してください。

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*無効なDRLファイルです*
エラーコード	x90
説明	更新サーバーのリストが含まれている1つまたは複数のファイルの整合性が侵害されました。

エラーの解決：

1. 必要に応じ、サーバーのリストを含むファイルのパスを確認します（設定ファイルの [Update] セクション内 *DrlDir の名前を持つパラメータ）。その場合 、コマンドライン管理ツールのコマンド を使用します。
   - 現在のパラメータ値を表示するには、コマンドを使用します（*<*DrlDirPath>* は、指定されたパラメータ名に置き換える必要があります。パラメータ名が不明な場合は、セクション内のパラメータ値を参照します。角括弧内のコマンド部分は省略します。

```
$ drweb-ctl cfshow Update[.<*DrlDir>]
```

   - 新しいパラメータ値を設定するには、コマンドを実行します（*<*DrlDir>* は、指定されたパラメータ名に置き換える必要があります。

```
# drweb-ctl cfset Update.<*DrlDir> <new path>
```

   - パラメータ値をデフォルトに戻すには、コマンドを実行します（*<*DrlDir>* は、指定されたパラメータ名に置き換える必要があります。

```
# drweb-ctl cfset Update.<*DrlDir> -r
```

2. 以下のいずれかの方法でウイルスデータベースを更新します。
   - アプリケーションの メインウィンドウ 内にある更新管理ページ で 更新 をクリックします。
   - 通知領域にあるステータスインジケータの コンテキストメニュー で 更新 をクリックします。
   - コマンド を実行します。

   ```
   $ drweb-ctl update
   ```
3. エラーが続く場合は、drweb-bases および drweb-dws コンポーネント(パッケージ)を別々にインストールし、更新を開始してください。
4. それでもエラーが解決されない場合は、Dr.Web for Linuxをアンインストールし、再度システムにインストールします。

   Dr.Web for LinuxまたはDr.Web for Linuxコンポーネントのインストールとアンインストールの方法については、Dr.Web for Linuxをインストールする および Dr.Web for Linuxをアンインストールする のセクションを参照してください。

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*無効なLSTファイルです*
エラーコード	x91
説明	更新されたウイルスデータベースのリストが含まれているファイルの整合性が侵害されました。

エラーの解決:

1. 以下のいずれかの方法でウイルスデータベースを更新します。
   - アプリケーションの メインウィンドウ 内にある更新管理ページ で 更新 をクリックします。
   - 通知領域にあるステータスインジケータの コンテキストメニュー で 更新 をクリックします。
   - コマンド を実行します。

   ```
   $ drweb-ctl update
   ```
2. それでもエラーが続く場合は、drweb-update パッケージを再インストールします。
3. それでもエラーが解決されない場合は、Dr.Web for Linuxをアンインストールし、再度システムにインストールします。

   Dr.Web for LinuxまたはDr.Web for Linuxコンポーネントのインストールとアンインストールの方法については、Dr.Web for Linuxをインストールする および Dr.Web for Linuxをアンインストールする のセクションを参照してください。

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*無効な圧縮ファイルです*
エラーコード	x92
説明	ダウンロードした更新を含むファイルの整合性が侵害されました。

エラーの解決:

1. 以下のいずれかの方法でウイルスデータベースを更新します。
   - アプリケーションの メインウィンドウ 内にある更新管理ページ で 更新 をクリックします。
   - 通知領域にあるステータスインジケータの コンテキストメニュー で 更新 をクリックします。
   - コマンド を実行します。

   ```
   $ drweb-ctl update
   ```

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*プロキシ認証エラーです*
エラーコード	x93
説明	プログラムは、設定内で指定されたプロキシサーバーを使用して更新サーバーに接続できませんでした。

エラーの解決：

1. プロキシサーバーへの接続に使用されたパラメータを確認します（設定ファイルの `[Update]` セクション内 `Proxy` パラメータで設定されています）。必要に応じ、プロキシサーバーを変更するか、接続にプロキシを使用しないようにしてください。

   接続パラメータの確認・設定は メイン設定 ページで行います。

   または、コマンドライン管理ツールの コマンド を使用することもできます。

   - 現在のパラメータ値を確認するには、以下のコマンドを実行します。

     ```
     $ drweb-ctl cfshow Update.Proxy
     ```

   - 新しいパラメータ値を設定するには、以下のコマンドを実行します。

     ```
     # drweb-ctl cfset Update.Proxy <new parameters>
     ```

   - パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

     ```
     # drweb-ctl cfset Update.Proxy -r
     ```

2. 以下のいずれかの方法でウイルスデータベースを更新します。
   - アプリケーションの メインウィンドウ 内にある更新管理ページ で 更新 をクリックします。
   - 通知領域にあるステータスインジケータの コンテキストメニュー で 更新 をクリックします。
   - コマンド を実行します。

     ```
     $ drweb-ctl update
     ```

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*使用可能な更新サーバーがありません*
エラーコード	x94

説明	プログラムは、いずれの更新サーバーにも接続できませんでした。

エラーの解決：

1. ネットワークが使用可能であるかどうかを確認します。必要に応じ、ネットワーク設定を変更します。
2. ネットワークアクセスがプロキシサーバー経由でのみ使用可能である場合、プロキシサーバーへの接続パラメータを指定します（設定ファイルの `[Update]` セクション内 `Proxy` パラメータで設定します）。必要に応じ、プロキシサーバーを変更するか、接続にプロキシを使用しないようにしてください。

   接続パラメータの確認・設定は メイン設定 ページで行います。

   または、コマンドライン管理ツールの コマンド を使用することもできます。

   - 現在のパラメータ値を確認するには、以下のコマンドを実行します。

   ```
   $ drweb-ctl cfshow Update.Proxy
   ```

   - 新しいパラメータ値を設定するには、以下のコマンドを実行します。

   ```
   # drweb-ctl cfset Update.Proxy <new parameters>
   ```

   - パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

   ```
   # drweb-ctl cfset Update.Proxy -r
   ```

3. ネットワーク接続パラメータ（プロキシサーバーのパラメータを含む）が正しくてもエラーが発生する場合は、利用可能な更新サーバーのリストを使用していることを確認してください。使用されている更新サーバーのリストは、設定ファイルの `[Update]` セクションのパラメータ `*DrlDir` で表示されます。`*CustomDrlDir` パラメータが既存の正しいサーバーリストのファイルを示す場合、標準的な更新ゾーンのサーバーではなく、リスト内で指定されたサーバーが使用されます（対応する`*DrlDir` パラメータで指定されている値は無視されます）。

   接続設定を確認したり、設定を行うには、コマンドライン管理ツールの コマンド を使用できます。

   現在のパラメータ値を表示するには、コマンドを使用します（*<*DrlDirPath>* は、指定されたパラメータ名に置き換える必要があります。パラメータ名が不明な場合は、セクション内のパラメータ値を参照します。角括弧内のコマンド部分は省略します。

   ```
   $ drweb-ctl cfshow Update[.<*DrlDir>]
   ```

   新しいパラメータ値を設定するには、コマンドを実行します（*<*DrlDir>* は、指定されたパラメータ名に置き換える必要があります。

   ```
   # drweb-ctl cfset Update.<*DrlDir> <new path>
   ```

   パラメータ値をデフォルトに戻すには、コマンドを実行します（*<*DrlDir>* は、指定されたパラメータ名に置き換える必要があります。

   ```
   # drweb-ctl cfset Update.<*DrlDir> -r
   ```

4. 以下のいずれかの方法でウイルスデータベースを更新します。
   - アプリケーションの メインウィンドウ 内にある更新管理ページ で **更新** をクリックします。
   - 通知領域にあるステータスインジケータの コンテキストメニュー で **更新** をクリックします。
   - コマンド を実行します。

   ```
   $ drweb-ctl update
   ```

引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*キーファイルのフォーマットが無効です*
エラーコード	x95
説明	キーファイルのフォーマットがサポートされていません

エラーの解決：

1. キーファイルを持っているかどうか、また、キーファイルへのパスを確認します。キーファイルへのパスは、設定ファイルの [Root] セクションの KeyPath パラメータで指定できます。

   ライセンスのパラメータの確認と、キーファイルへのパスの設定は、アプリケーションの メインページ 内 ライセンスマネージャー ページで行います。

   または、コマンドライン管理ツールの コマンド を使用することもできます。

   - 現在のパラメータ値を確認するには、以下のコマンドを実行します。

     ```
     $ drweb-ctl cfshow Root.KeyPath
     ```

   - 新しいパラメータ値を設定するには、以下のコマンドを実行します。

     ```
     # drweb-ctl cfset Root.KeyPath <path to file>
     ```

   - パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

     ```
     # drweb-ctl cfset Root.KeyPath -r
     ```

2. キーファイルをお持ちでない場合や、お使いのキーファイルが破損している場合は、キーファイルを購入してインストールしてください。キーファイル、購入、インストールに関する詳細については ライセンス のセクションを参照してください。
3. キーファイルのインストールには、ライセンスマネージャー を使用できます。
4. また、https://support.drweb.com/get+cabinet+link/ のユーザーのWebページ **My Dr.Web** 内で、現在のライセンスオプションを確認できます。

引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*ライセンスの有効期限が切れています*
エラーコード	x96
説明	ライセンスの有効期限が切れています。

エラーの解決：

1. 新しいライセンスを購入し、受け取るキーファイルをインストールしてください。ライセンスの購入とキーファイルのインストールに関する詳細については ライセンス のセクションを参照してください。
2. 購入したキーファイルのインストールには、ライセンスマネージャー を使用できます。
3. また、https://support.drweb.com/get+cabinet+link/ のユーザーのWebページ **My Dr.Web** 内で、現在のライセンスオプションを確認できます。

引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*ネットワークオペレーションのタイムアウト*
エラーコード	x97
説明	ネットワークオペレーションがタイムアウトしました（リモートホストが予期せず応答を停止したか、必要な接続に失敗した可能性があります）。

エラーの解決：

1. ネットワークが使用可能であること、ネットワーク設定が正しいことを確認します。必要に応じ、ネットワーク設定を変更し、操作を繰り返します。
2. 更新中にエラーの発生が続く場合は、プロキシサーバーの使用に関するパラメータも確認し、必要に応じて、使用しているプロキシサーバーを変更するか、プロキシサーバーを使用しないようにしてください。

引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*無効なチェックサムです*
エラーコード	x98
説明	ダウンロードした更新を含むファイルのチェックサムが破損しています。

エラーの解決：

1. 以下のいずれかの方法で、しばらくしてから更新を再開します。
   - アプリケーションのメインウィンドウ内にある更新管理ページで **更新** をクリックします。
   - 通知領域にあるステータスインジケータのコンテキストメニューで **更新** をクリックします。
   - コマンドを実行します。

   ```
   $ drweb-ctl update
   ```

引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*無効なデモキーファイルです*
エラーコード	x99
説明	デモキーファイルが無効です（別のコンピューターから受け取ったものであるなど）。

エラーの解決：

1. 該当するコンピューターの新しい試用期間のリクエストを送信するか、新しいライセンスを購入して、受け取るキーファイルをインストールしてください。ライセンスの購入とキーファイルのインストールに関する詳細については ライセンス のセクションを参照してください。
2. 購入したキーファイルのインストールには、ライセンスマネージャーを使用できます。
3. また、https://support.drweb.com/get+cabinet+link/ のユーザーのWebページ **My Dr.Web** 内で、現在のライセンスオプションを確認できます。

引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*ライセンスキーファイルがブロックされています*
エラーコード	x100
説明	ライセンスはブロックされています（Dr.Web for Linuxの使用に関する使用許諾契約の条件に違反している可能性があります）。

エラーの解決：

1. 新しいライセンスを購入し、受け取るキーファイルをインストールしてください。ライセンスの購入とキーファイルのインストールに関する詳細については ライセンス のセクションを参照してください。
2. 購入したキーファイルのインストールには、ライセンスマネージャー を使用できます。
3. また、https://support.drweb.com/get+cabinet+link/ のユーザーのWebページ **My Dr.Web** 内で、現在のライセンスオプションを確認できます。

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*無効なライセンスです*
エラーコード	x101
説明	現在のライセンスが別のDr.Web製品のものであるか、インストールされているDr.Web for Linuxコンポーネントの動作がライセンスで許可されていません。

エラーの解決：

1. 新しいライセンスを購入し、受け取るキーファイルをインストールしてください。ライセンスの購入とキーファイルのインストールに関する詳細については ライセンス のセクションを参照してください。
2. 購入したキーファイルのインストールには、ライセンスマネージャー を使用できます。
3. また、https://support.drweb.com/get+cabinet+link/ のユーザーのWebページ **My Dr.Web** 内で、現在のライセンスオプションを確認できます。

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*無効な設定です*
エラーコード	x102
説明	Dr.Web for Linuxコンポーネントの1つが、誤った設定のために動作できません。

エラーの解決：

1. どのコンポーネントが原因でエラーが発生しているのか分からない場合は、ログファイルを確認して特定してください。
2. エラーがSpIDer Guardコンポーネントによって発生している場合、コンポーネントのモードにOSによってサポートされていないものが選択されている可能性があります。選択されているモードを確認し、必要に応じて `AUTO` 値（設定ファイルの `[LinuxSpider]` セクション内 `Mode` パラメータ）を設定することで、それを変更してください。

   モードの確認・修正には、コマンドライン管理ツールの コマンド を使用できます。

   - `AUTO` の値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset LinuxSpider.Mode AUTO
```

- パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset LinuxSpider.Mode -r
```

引き続きエラーが発生する場合は、SpIDer Guard用のローダブルカーネルモジュールを手動で作成してインストール

SpIDer Guardの動作とローダブルカーネルモジュールの動作は、サポートされているUNIXディストリビューション上でのみ保証されています（システム要件参照）。

3. エラーがSpIDer Gateによって発生している場合、別のファイアーウォールとの間に競合が起こっている可能性があります。例えば、SpIDer GateはFedora、CentOS、Red Hat Enterprise Linux の FirewallDと競合することが分かっています（FirewallDは起動の度に、SpIDer Gateによって指定されたトラフィックルーチンのルールを損なわせます）。このエラーを解決するには、以下のコマンドを実行することでDr.Web for Linuxを再起動させてください。

```
# service drweb-configd restart
```

または

```
# drweb-ctl reload
```

FirewallDの動作を許可する場合、SpIDer GateのエラーはFirewallDが再起動（OSの再起動を含む）する度に繰り返し発生する可能性があります。FirewallDを無効にすることで、このエラーを解決することができます（お使いのOSに付属している FirewallD のマニュアルを参照してください）。

4. エラーが別のコンポーネントで発生している場合は、以下のいずれかの方法によって、そのコンポーネントの設定をデフォルトに復元します。
   - `drweb-ctl cfshow` および `drweb-ctl cfset` コマンドを使用して
   - コンポーネントセクションからすべてのパラメータを削除することで、手動で設定ファイを編集する
5. この手順で問題が解決しない場合は、Dr.Web for Linux設定をデフォルトに戻してください。

   設定をデフォルトに戻すには、次のコマンドを実行するなどによって、設定ファイル `/etc/opt/drweb.com/drweb.ini` のコンテンツをクリアします（設定ファイルのバックアップを作成することが推奨されます）。

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

設定ファイルのコンテンツを削除した後に、次のコマンドを実行することでDr.Web for Linuxを再起動させます。

```
# service drweb-configd restart
```

引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*無効な実行ファイルです*

エラーコード	`x104`
説明	パスが誤っているか、実行ファイルのコンテンツが破損していることが原因で、Dr.Web for Linuxコンポーネントの1つを実行できません。

エラーの解決：

1. エラーが発生しているコンポーネントの名前が分からない場合は、ログファイルを確認して特定してください。
2. 以下のコマンドを実行することで（*<component section>*を、設定ファイルの該当するセクション名に変更します）、Dr.Web for Linux設定ファイル内でコンポーネントの実行ファイルへのパスを確認します（コンポーネントセクションの `ExePath` パラメータ）：

   ```
   $ drweb-ctl cfshow <component section>.ExePath
   ```

3. 以下のコマンドを実行することで（*<component section>*を、設定ファイルの該当するセクション名に変更します）、パスをデフォルトに復元します。

   ```
   # drweb-ctl cfset <component section>.ExePath -r
   ```

4. この手順で問題が解決しない場合は、該当するコンポーネントのパッケージを再インストールしてください。
   - Scannerの実行ファイルが破損している場合：`drweb-filecheck`
   - SpIDer Guardの実行ファイルが破損している場合：`drweb-spider`
   - SpIDer Gateの実行ファイルが破損している場合：`drweb-gated`
   - Updaterの実行ファイルが破損している場合：`drweb-update`
5. 引き続きエラーが発生する場合や、どの実行ファイルが無効であるのか特定できない場合は、Dr.Web for Linuxをアンインストールし、再度システムにインストールします。

   Dr.Web for LinuxまたはDr.Web for Linuxコンポーネントのインストールとアンインストールの方法については、Dr.Web for Linuxをインストールする および Dr.Web for Linuxをアンインストールする のセクションを参照してください。

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*Virus-Finding Engineを使用できません*
エラーコード	`x105`
説明	スキャンエンジンDr.Web Virus-Finding Engineのファイルがないか、使用できません（脅威の検出に必要です）。

エラーの解決：

1. `drweb32.dll` スキャンエンジンファイルへのパスを確認します。必要に応じてパスを変更します（設定ファイルの［`Root`］セクションにある `CoreEnginePath` パラメータ）。

   パスの確認・修正には、コマンドライン管理ツールの コマンド を使用できます。

   - 現在のパラメータ値を確認するには、以下のコマンドを実行します。

     ```
     $ drweb-ctl cfshow Root.CoreEnginePath
     ```

   - 新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.CoreEnginePath <new path>
```

- パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.CoreEnginePath -r
```

2. 以下のいずれかの方法でウイルスデータベースを更新します。
   - アプリケーションの メインウィンドウ 内にある更新管理ページ で **更新** をクリックします。
   - 通知領域にあるステータスインジケータの コンテキストメニュー で **更新** をクリックします。
   - コマンド を実行します。

```
$ drweb-ctl update
```

3. パスが正しく、ウイルスデータベースを更新した後もエラーが続く場合は、`drweb-bases` パッケージを再インストールしてください。
4. それでもエラーが解決されない場合は、Dr.Web for Linuxをアンインストールし、再度システムにインストールします。

   Dr.Web for LinuxまたはDr.Web for Linuxコンポーネントのインストールとアンインストールの方法については、Dr.Web for Linuxをインストールする および Dr.Web for Linuxをアンインストールする のセクションを参照してください。

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*ウイルスデータベースがありません*
エラーコード	`x106`
説明	ウイルスデータベースが見つかりません。

エラーの解決：

1. ウイルスデータベースディレクトリへのパスを確認してください。必要に応じてパスを変更します（設定ファイルの `[Root]` セクションにある `VirusBaseDir` パラメータ）。

   パスの確認・修正には、コマンドライン管理ツールの コマンド を使用できます。
   - 現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow Root.VirusBaseDir
```

   - 新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.VirusBaseDir <new path>
```

   - パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.VirusBaseDir -r
```

2. 以下のいずれかの方法でウイルスデータベースを更新します。
   - アプリケーションの メインウィンドウ 内にある更新管理ページ で **更新** をクリックします。
   - 通知領域にあるステータスインジケータの コンテキストメニュー で **更新** をクリックします。
   - コマンド を実行します。

```
$ drweb-ctl update
```

3. エラーが続く場合は、ウイルスデータベースとスキャンエンジン実行ファイルを含む `drweb-bases` パッケージを再インストールしてください。
4. それでもエラーが解決されない場合は、Dr.Web for Linuxをアンインストールし、再度システムにインストールします。

   Dr.Web for LinuxまたはDr.Web for Linuxコンポーネントのインストールとアンインストールの方法については、Dr.Web for Linuxをインストールする および Dr.Web for Linuxをアンインストールする のセクションを参照してください。

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*プロセスはシグナルによって中断されました*
エラーコード	x107
説明	コンポーネントがシャットダウンしました（ユーザーコマンドによって、またはアイドル状態であるためである可能性があります）

エラーの解決：

1. 操作が完了していない場合は、再度開始してください。そうでない場合、シャットダウンはエラーではありません。
2. コンポーネントが度々シャットダウンする場合は、以下のいずれかの方法によって、そのコンポーネントの設定をデフォルトに復元します。
   - `drweb-ctl cfshow` および `drweb-ctl cfset` コマンド を使用して
   - 手動で設定ファイを編集する（コンポーネントセクションからすべてのパラメータを削除することで）
3. 問題が解決しない場合は、Dr.Web for Linux設定をデフォルトに戻してしてください。

   設定をデフォルトに戻すには、次のコマンドを実行するなどによって、設定ファイル `/etc/opt/drweb.com/drweb.ini` のコンテンツをクリアします（設定ファイルのバックアップを作成することが推奨されます）。

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   設定ファイルのコンテンツを削除した後に、次のコマンドを実行することでDr.Web for Linuxを再起動させます。

   ```
   # service drweb-configd restart
   ```

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*予期せぬプロセスの中断です*
エラーコード	x108
説明	不具合によって予期せずコンポーネントがシャットダウンしました。

エラーの解決：

1. 中断された操作を繰り返します。
2. コンポーネントが度々異常にシャットダウンする場合は、以下のいずれかの方法によって、そのコンポーネントの設定をデフォルトに復元します。
   - `drweb-ctl cfshow` および `drweb-ctl cfset` コマンドを使用して
   - 手動で設定ファイを編集する(コンポーネントセクションからすべてのパラメータを削除することで)
3. 問題が解決しない場合は、Dr.Web for Linux設定をデフォルトに戻してしてください。

   設定をデフォルトに戻すには、次のコマンドを実行するなどによって、設定ファイル `/etc/opt/drweb.com/drweb.ini` のコンテンツをクリアします(設定ファイルのバックアップを作成することが推奨されます)。

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   設定ファイルのコンテンツを削除した後に、次のコマンドを実行することでDr.Web for Linuxを再起動させます。

   ```
   # service drweb-configd restart
   ```
4. Dr.Web for Linux設定を復元した後もエラーが続く場合は、コンポーネントパッケージを再インストールしてください。
5. それでもエラーが解決されない場合は、Dr.Web for Linuxをアンインストールし、再度システムにインストールします。

   Dr.Web for LinuxまたはDr.Web for Linuxコンポーネントのインストールとアンインストールの方法については、Dr.Web for Linuxをインストールする および Dr.Web for Linuxをアンインストールする のセクションを参照してください。

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*互換性のないソフトウェアが検出されました*
エラーコード	x109
説明	互換性のないソフトウェアが検出されたため、Dr.Web for Linuxコンポーネントは動作できません。このソフトウェアは、コンポーネントの正常な動作を妨げます。

エラーの解決:

1. このエラーがSpIDer Gateで発生している場合、オペレーティングシステムに互換性のないソフトウェアがある可能性があります。そのようなソフトウェアはNetFilterシステムファイアウォールのルールを生成し、それによりSpIDer Gateが正しく動作しなくなります。ShorewallまたはSuseFirewall2がシステムにインストールされている可能性があります(SUSE Linux OSの場合)。NetFilterシステムファイアウォールを設定するアプリケーションは、指定されたルールシステムの整合性をチェックして書き換えることがあります。これが、SpIDer GateがこのようなアプリケーションとSuseFirewall2アプリケーション(SUSE Linux OSの場合)の設定を行ってください。

   SpIDer Gateの動作に干渉しないように、互換性のないソフトウェアを再設定してください。それが不可能な場合は、オペレーティングシステムの起動時に読み込まれないようにソフトウェアを無効にします。以下の手順に従って、SuseFirewall2アプリケーション(SUSE Linux OSの場合)の設定を行ってください。

   1) SuseFirewall2 の設定ファイル(デフォルトでは `/etc/sysconfig/SuSEfirewall2` ファイルです)を開きます。
   2) 以下のテキストブロックを見つけます。

```
# Type: yesno
#
# Install NOTRACK target for interface lo in the raw table. Doing so
# speeds up packet processing on the loopback interface. This breaks
# certain firewall setups that need to e.g. redirect outgoing
# packets via custom rules on the local machine.
#
# Defaults to "yes" if not set
#
FW_LO_NOTRACK=""
```

3) パラメータ値に "no" を指定します:

```
FW_LO_NOTRACK="no"
```

4) 以下のコマンドを実行して SuseFirewall2を再起動させます。

```
# rcSuSEfirewall2 restart
```

SuseFirewall2の設定内に FW_LO_NOTRACK がない場合、競合を解決するためにはアプリケーションを無効にし、それがシステム起動時に読み込まれないようにする必要があるという点に注意してください(たとえば、SUSE Linux Enterprise Server 11にはこれが必要です)。

5) 競合するアプリケーションを再設定または無効にした後に、SpIDer Gateを再起動させます(該当するページで無効にした後、再度有効にします)。

2. エラーが別のコンポーネントで発生している場合、互換性のないソフトウェアを無効にするか、再設定し、それがDr.Web for Linuxの動作を妨げないようにしてください。

引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*無効なライブラリです*
エラーコード	x110
説明	アンチスパムライブラリのファイルがないか、使用できないか、破損しています(メールのスキャンに必要です)。

エラーの解決:

1. ライブラリファイルへのパスを確認してください。必要に応じてパスを変更します(設定ファイルの [Root] セクションにある AntispamCorePath パラメータ)。

   パスの確認・修正には、コマンドライン管理ツールの コマンド を使用できます。

   - 現在のパラメータ値を確認するには、以下のコマンドを実行します。

   ```
   $ drweb-ctl cfshow Root.AntispamCorePath
   ```

   - 新しいパラメータ値を設定するには、以下のコマンドを実行します。

   ```
   # drweb-ctl cfset Root.AntispamCorePath <new path>
   ```

- パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.AntispamCorePath -r
```

2. 以下のいずれかの方法でウイルスデータベースを更新します。
   - アプリケーションの メインウィンドウ 内にある更新管理ページ で 更新 をクリックします。
   - 通知領域にあるステータスインジケータの コンテキストメニュー で 更新 をクリックします。
   - コマンド を実行します。

```
$ drweb-ctl update
```

3. パスが正しく、ウイルスデータベースを更新した後もエラーが続く場合は、`drweb-maild` パッケージを再インストールしてください。
4. それでもエラーが解決されない場合は、Dr.Web for Linuxをアンインストールし、再度システムにインストールします。

   Dr.Web for LinuxまたはDr.Web for Linuxコンポーネントのインストールとアンインストールの方法については、Dr.Web for Linuxをインストールする および Dr.Web for Linuxをアンインストールする のセクションを参照してください。

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*Webリソースカテゴリーのデータベース*
エラーコード	x112
説明	Webリソースカテゴリーのデータベースがありません。

エラーの解決:

1. Webリソースカテゴリーディレクトリのデータベースへのパスを確認してください。必要に応じてパスを変更します（設定ファイルの [Root] セクションにある `DwsDir` パラメータ）。
   - パスの確認・修正には、コマンドライン管理ツールの コマンド を使用できます。

   現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow Root.DwsDir
```

   新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.DwsDir <new path>
```

   パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.DwsDir -r
```

2. 以下のいずれかの方法でウイルスデータベースを更新します。
   - アプリケーションの メインウィンドウ 内にある更新管理ページ で 更新 をクリックします。
   - 通知領域にあるステータスインジケータの コンテキストメニュー で 更新 をクリックします。
   - コマンド を実行します。

```
$ drweb-ctl update
```

3. エラーが継続する場合は、`drweb-dws` パッケージを個別にインストールしてください。このパッケージにはWebリソースカテゴリーのデータベースが含まれています。
4. それでもエラーが解決されない場合は、Dr.Web for Linuxをアンインストールし、再度システムにインストールします。

   Dr.Web for LinuxまたはDr.Web for Linuxコンポーネントのインストールとアンインストールの方法については、Dr.Web for Linuxをインストールする および Dr.Web for Linuxをアンインストールする のセクションを参照してください。

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*SpIDer Guard用のLinuxカーネルモジュールを使用することができません*
エラーコード	`x113`
説明	SpIDer Guardに必要なLinuxカーネルモジュールが見つかりません。

エラーの解決：

1. コンポーネントにいずれの動作モードが選択されているかを確認し、必要に応じて `AUTO` の値（設定ファイルの `[LinuxSpider]` セクション内の `Mode` パラメータ）を設定し、変更してください。

   モードの確認・修正には、コマンドライン管理ツールの コマンド を使用できます。

   - `AUTO` の値を設定するには、以下のコマンドを実行します。

     ```
     # drweb-ctl cfset LinuxSpider.Mode AUTO
     ```

   - パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

     ```
     # drweb-ctl cfset LinuxSpider.Mode -r
     ```

2. 引き続きエラーが発生する場合は、SpIDer Guar用のローダブルカーネルモジュールを手動で作成・インストール してください

   > ⚠ SpIDer Guardの動作とローダブルカーネルモジュールの動作は、サポートされているUNIXディストリビューション上でのみ保証されています（システム要件参照）。

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*SpIDer Gateを使用することができません*
エラーコード	`x117`
説明	SpIDer Gateコンポーネントがありません（ネットワーク接続のスキャンに必要です）。

エラーの解決：

1. `drweb-gated` 実行ファイルへのパスを確認してください。必要に応じてパスを変更します（設定ファイルの `[GateD]` セクションにある `ExePath` パラメータ）。

   または、コマンドライン管理ツールの コマンド を使用することもできます。

   - 現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow GateD.ExePath
```

- 新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset GateD.ExePath <new path>
```

- パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset GateD.ExePath -r
```

2. 設定にSpIDer Gateコンポーネントの設定が含まれていない場合、または正しいパスを入力した後もエラーが継続する場合は、`drweb-gated` パッケージをインストールまたは再インストールしてください。
3. それでもエラーが解決されない場合は、Dr.Web for Linuxをアンインストールし、再度システムにインストールします。

   Dr.Web for LinuxまたはDr.Web for Linuxコンポーネントのインストールとアンインストールの方法については、Dr.Web for Linuxをインストールする および Dr.Web for Linuxをアンインストールする のセクションを参照してください。

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*MailDを使用できません*
エラーコード	x118
説明	Dr.Web MailDコンポーネントがありません（メールのスキャンに必要です）。

エラーの解決：

1. `drweb-maild` 実行ファイルへのパスを確認してください。必要に応じてパスを変更します（設定ファイルの `[MailD]` セクションにある `ExePath` パラメータ）。

   または、コマンドライン管理ツールの コマンド を使用することもできます。

   - 現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow MailD.ExePath
```

   - 新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset MailD.ExePath <new path>
```

   - パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset MailD.ExePath -r
```

2. 設定にDr.Web MailDコンポーネントの設定が含まれていない場合、または正しいパスを入力した後もエラーが継続する場合は、`drweb-maild` パッケージをインストールまたは再インストールしてください。
3. それでもエラーが解決されない場合は、Dr.Web for Linuxをアンインストールし、再度システムにインストールします。

   Dr.Web for LinuxまたはDr.Web for Linuxコンポーネントのインストールとアンインストールの方法については、Dr.Web for Linuxをインストールする および Dr.Web for Linuxをアンインストールする のセクションを参照してください。

引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*Scanning Engineを使用できません*
エラーコード	x119
説明	Dr.Web Scanning Engineコンポーネント(drweb-se)が見つからないか、起動しないため、ファイルをスキャンできません。このモジュールは悪意のあるオブジェクトを探すために使用されます。 Scanner、SpIDer Guard、SpIDer Gateの起動に失敗しました(部分的に)。

エラーの解決:

1. drweb-se 実行ファイルへのパスを確認してください。必要に応じてパスを変更します(設定ファイルの [ScanEngine] セクションにある ExePath パラメータ)。

   または、コマンドライン管理ツールの コマンド を使用することもできます。

   - 現在のパラメータ値を確認するには、以下のコマンドを実行します。

     ```
     $ drweb-ctl cfshow ScanEngine.ExePath
     ```

   - 新しいパラメータ値を設定するには、以下のコマンドを実行します。

     ```
     # drweb-ctl cfset ScanEngine.ExePath <new path>
     ```

   - パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

     ```
     # drweb-ctl cfset ScanEngine.ExePath -r
     ```

2. 正しいパスを入力した後もエラーが継続する場合は

   - 次のコマンドを実行します。

     ```
     $ drweb-ctl rawscan /
     ```

     エラー: 無効なライセンスです が出力された場合は有効なキーファイルがありません。Dr.Web for Linuxを登録してライセンスを受け取ってください。ライセンス取得後に、キーファイル が使用可能であるかどうかを確認し、必要に応じてそれをインストールしてください。

   - お使いのOSにてSELinuxを有効化している場合、drweb-se モジュールに対するセキュリティポリシーを設定します(管理者マニュアルの SELinuxセキュリティポリシーを設定する を参照してください)。

3. 設定にコンポーネントの設定が含まれていない場合、またはこれまでの手順で問題が解決しない場合は、drweb-se パッケージをインストールまたは再インストールしてください。
4. それでもエラーが解決されない場合は、Dr.Web for Linuxをアンインストールし、再度システムにインストールします。

   Dr.Web for LinuxまたはDr.Web for Linuxコンポーネントのインストールとアンインストールの方法については、Dr.Web for Linuxをインストールする および Dr.Web for Linuxをアンインストールする のセクションを参照してください。

引き続きエラーが発生する場合は、テクニカルサポートまでご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*Scannerを使用できません*

エラーコード	`x120`
説明	`drweb-filecheck` がありません。

エラーの解決：

1. `drweb-filecheck` 実行ファイルへのパスを確認してください。必要に応じてパスを変更します（設定ファイルの `[FileCheck]` セクションにある `ExePath` パラメータ）。

   または、コマンドライン管理ツールの コマンド を使用することもできます。

   現在のパラメータ値を確認するには、以下のコマンドを実行します。

   ```
   $ drweb-ctl cfshow FileCheck.ExePath
   ```

   新しいパラメータ値を設定するには、以下のコマンドを実行します。

   ```
   # drweb-ctl cfset FileCheck.ExePath <new path>
   ```

   パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

   ```
   # drweb-ctl cfset FileCheck.ExePath -r
   ```

2. 正しいパスを入力した後もエラーが継続する場合は
   - お使いのOSにてSELinuxを有効化している場合、`drweb-se` モジュールに対するセキュリティポリシーを設定します（管理者マニュアルの SELinuxセキュリティポリシーを設定する を参照してください）。
3. 設定にコンポーネントの設定が含まれていない場合、またはこれまでの手順で問題が解決しない場合は、`drweb-filecheck` パッケージをインストールまたは再インストールしてください。
4. それでもエラーが解決されない場合は、Dr.Web for Linuxをアンインストールし、再度システムにインストールします。

   Dr.Web for LinuxまたはDr.Web for Linuxコンポーネントのインストールとアンインストールの方法については、Dr.Web for Linuxをインストールする および Dr.Web for Linuxをアンインストールする のセクションを参照してください。

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*ES Agentを使用できません*
エラーコード	`x121`
説明	Dr.Web ES Agentコンポーネントがありません（集中管理サーバーへの接続に必要です）。

エラーの解決：

1. `drweb-esagent` 実行ファイルへのパスを確認してください。必要に応じてパスを変更します（設定ファイルの `[ESAgent]` セクションにある `ExePath` パラメータ）。

   または、コマンドライン管理ツールの コマンド を使用することもできます。

   - 現在のパラメータ値を確認するには、以下のコマンドを実行します。

     ```
     $ drweb-ctl cfshow ESAgent.ExePath
     ```

- 新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset ESAgent.ExePath <new path>
```

- パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset ESAgent.ExePath -r
```

2. 設定にコンポーネントの設定が含まれていない場合、または正しいパスを入力した後もエラーが継続する場合は、`drweb-esagent` パッケージをインストールまたは再インストールしてください。
3. それでもエラーが解決されない場合は、Dr.Web for Linuxをアンインストールし、再度システムにインストールします。

   Dr.Web for LinuxまたはDr.Web for Linuxコンポーネントのインストールとアンインストールの方法については、Dr.Web for Linuxをインストールする および Dr.Web for Linuxをアンインストールする のセクションを参照してください。

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*Firewall for Linuxを使用できません*
エラーコード	`x122`
説明	`drweb-firewall` が見つからないか、起動に失敗しました。

エラーの解決：

1. `drweb-firewall` 実行ファイルへのパスを確認してください。必要に応じてパスを変更します（設定ファイルの `[LinuxFirewall]` セクションにある `ExePath` パラメータ）。

   または、コマンドライン管理ツールの コマンド を使用することもできます。

   - 現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow LinuxFirewall.ExePath
```

   - 新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset LinuxFirewall.ExePath <new path>
```

   - パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset LinuxFirewall.ExePath -r
```

2. 設定にDr.Web Firewall for Linuxコンポーネントの設定が含まれていない場合、または正しいパスを入力した後もエラーが継続する場合は、`drweb-firewall` パッケージをインストールまたは再インストールしてください。
3. それでもエラーが解決されない場合は、Dr.Web for Linuxをアンインストールし、再度システムにインストールします。

   Dr.Web for LinuxまたはDr.Web for Linuxコンポーネントのインストールとアンインストールの方法については、Dr.Web for Linuxをインストールする および Dr.Web for Linuxをアンインストールする のセクションを参照してください。

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*Network Checkerを使用できません*
エラーコード	x123
説明	drweb-netcheck がないか、起動しないため、ネットワーク接続を制御できません。このモジュールはダウンロードされたファイルをスキャンするために使用されます。 SpIDer Gateの起動に失敗しました(部分的に)。

エラーの解決:

1. drweb-netcheck 実行ファイルへのパスを確認してください。必要に応じてパスを変更します(設定ファイルの [NetCheck] セクションにある ExePath パラメータ)。

   または、コマンドライン管理ツールの コマンド を使用することもできます。

   - 現在のパラメータ値を確認するには、以下のコマンドを実行します。

     ```
     $ drweb-ctl cfshow NetCheck.ExePath
     ```

   - 新しいパラメータ値を設定するには、以下のコマンドを実行します。

     ```
     # drweb-ctl cfset NetCheck.ExePath <new path>
     ```

   - パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

     ```
     # drweb-ctl cfset NetCheck.ExePath -r
     ```

2. 設定にコンポーネントの設定が含まれていない場合、または正しいパスを入力した後もエラーが継続する場合は、drweb-netcheck パッケージをインストールまたは再インストールしてください。
3. それでもエラーが解決されない場合は、Dr.Web for Linuxをアンインストールし、再度システムにインストールします。

   Dr.Web for LinuxまたはDr.Web for Linuxコンポーネントのインストールとアンインストールの方法については、Dr.Web for Linuxをインストールする および Dr.Web for Linuxをアンインストールする のセクションを参照してください。

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*CloudDを使用できません*
エラーコード	x124
説明	Dr.Web CloudDが見つかりません(Dr.Web Cloudサービスへの要求に必要です)。

エラーの解決:

1. drweb-cloudd 実行ファイルへのパスを確認してください。必要に応じてパスを変更します(設定ファイルの [CloudD] セクションにある ExePath パラメータ)。

   または、コマンドライン管理ツールの コマンド を使用することもできます。

   - 現在のパラメータ値を確認するには、以下のコマンドを実行します。

     ```
     $ drweb-ctl cfshow CloudD.ExePath
     ```

- 新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset CloudD.ExePath <new path>
```

- パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset CloudD.ExePath -r
```

2. 設定にコンポーネントの設定が含まれていない場合、または正しいパスを入力した後もエラーが継続する場合は、`drweb-cloudd` パッケージをインストールまたは再インストールしてください。
3. それでもエラーが解決されない場合は、Dr.Web for Linuxをアンインストールし、再度システムにインストールします。

   Dr.Web for LinuxまたはDr.Web for Linuxコンポーネントのインストールとアンインストールの方法については、Dr.Web for Linuxをインストールする および Dr.Web for Linuxをアンインストールする のセクションを参照してください。

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

エラーメッセージ	*予期せぬエラーです*
エラーコード	x125
説明	いずれかのコンポーネントの動作に、予期せぬエラーが発生しました。

エラーの解決：

1. 以下のコマンドを入力し、Dr.Web for Linuxを再起動します。

```
# service drweb-configd restart
```

引き続きエラーが発生する場合は、テクニカルサポート までご連絡のうえ、エラーコードをお伝えください。

コードのないエラー

症状：SpIDer Guardのカーネルモジュール のインストール後、オペレーティングシステムがカーネルエラー "*Kernel panic*" で異常終了する。

説明：SpIDer Guardカーネルモジュールは、OSのカーネル環境では動作できません（たとえば、OSがXenハイパーバイザー環境で動作している場合）。

エラーの解決

1. 次の文字列をgrubローダーに追加して、SpIDer Guardカーネルモジュール（カーネルモジュール名は `drweb`）の読み込みをキャンセルします。

```
drweb.blacklist=yes
```

   オペレーティングシステムカーネルの読み込み設定文字列に追加します。
2. OSがロードされたら、追加のカーネルモジュールの `/lib/`uname-r`/extra` ディレクトリから `drweb.ko` カーネルモジュールをアンインストールします。

3. 以下のコマンドを実行して、SpIDer Guardの動作モードを *AUTO* に設定します。

```
# drweb-ctl cfset LinuxSpider.Mode AUTO
# drweb-ctl reload
```

4. 使用しているOSがfanotifyをサポートしていない場合、またはこのモードでSpIDer Guardによるファイルシステムの完全な管理が許可されておらずファイルシステム管理に *LKM* モードを使用する必要がある場合は、Xenハイパーバイザーを使用しないでください。

引き続きエラーが発生する場合は、テクニカルサポートまでご連絡ください。

症状：Dr.Web for Linux のメインウィンドウが無効になり、デスクトップの通知領域にある ステータスインジケータ にクリティカルなエラーのマークが表示され、ドロップダウンメニューには無効になっている1つのアイテム **読み込んでいます** のみが含まれている。

説明：コアコンポーネント `drweb-configd` を使用できないため、Dr.Web for Linuxは起動できません。

エラーの解決

1. 以下のコマンドを入力し、Dr.Web for Linuxをアンインストール します。

```
# service drweb-configd restart
```

2. このコマンドがエラーメッセージを返した場合、または効果がない場合は、`drweb-configd` コンポーネント（パッケージ）を個別にインストールしてください。

   また、これはシステム内でPAM認証が使用されていないということを意味している場合もあります。その場合は、PAMインストールして設定してください。

3. それでもエラーが解決されない場合は、Dr.Web for Linuxをアンインストールし、再度システムにインストールします。

   Dr.Web for LinuxまたはDr.Web for Linuxコンポーネントのインストールとアンインストールの方法については、Dr.Web for Linuxをインストールする および Dr.Web for Linuxをアンインストールする のセクションを参照してください。

引き続きエラーが発生する場合は、テクニカルサポートまでご連絡ください。

症状

1. ユーザーがログインした後に、通知領域内に ステータスインジケータ が表示されない。
2. コマンド

```
$ drweb-gui
```

   を実行しようとすると、Dr.Web for Linux メインウィンドウ が開く。

説明：お使いのシステムに、必要な追加ライブラリである `libappindicator1` がインストールされていない可能性があります。

エラーの解決

1. 次のコマンドを使用して、お使いのシステムにパッケージ `libappindicator1` がインストールされていることを確認します。

```
# dpkg -l | grep libappindicator1
```

2. このコマンドが画面に結果を出力しない場合、使用可能ないずれかのシステムパッケージマネージャーを用いてパッケージをインストールする必要があります。その後、ログアウトし、再度ログインしてください(*ログイン*)。

   また、これはシステム内でPAM認証が使用されていないということを意味している場合もあります。その場合は、PAMインストールして設定してください。
3. それでもエラーが解決されない場合は、Dr.Web for Linuxをアンインストールし、再度システムにインストールします。

   Dr.Web for LinuxまたはDr.Web for Linuxコンポーネントのインストールとアンインストールの方法については、Dr.Web for Linuxをインストールする および Dr.Web for Linuxをアンインストールする のセクションを参照してください。

引き続きエラーが発生する場合は、テクニカルサポート までご連絡ください。

症状

1. SpIDer Gateを無効にした後、すべてのネットワーク接続が切断され(SSH／FTPプロトコル経由での送信、および場合によっては受信も)、再確立することができない。
2. 以下のコマンドを使用して、NetFilter(`iptables`)ルール全体を検索すると、空以外の結果が返ってくる。

   ```
   # iptables-save | grep "comment --comment --comment"
   ```

   説明

このエラーは1.4.15より前のバージョンのNetFilter(`iptables`)の誤った動作に関連しています。この内部エラーのため、SpIDer Gateが一意のラベル(コメント)が付いたルールをルールのリストに追加すると、そのルールは正しく追加されません。その結果、SpIDer Gateはシャットダウン時に接続の迂回ルールを削除できません。

エラーの解決

1. SpIDer Gateモニターを再度有効にしてください
2. SpIDer Gateを無効にする必要がある場合、以下のコマンドを使用して、NetFilter(`iptables`)の正しくないルールを削除してください。

   ```
   # iptables-save | grep -v "comment --comment --comment" | iptables-
   restore
   ```

   `iptables-save` および `iptables-restore` コマンドにはroot権限が必要です。権限を昇格するには `su` または `sudo` コマンドを使用することができます。また、このコマンドは正しくないコメントを持つすべてのルール(例:同じくトラフィックのリダイレクトを実行する他のアプリケーションによって追加されたものなど)を削除するという点に注意してください。

追加情報:

- この問題の発生を防ぐため、お使いのOSをアップグレードすることが推奨されます(または、少なくともNetFilterをバージョン1.4.15以降に)。
- また、`iptables` ユーティリティを使用して必要なルールを指定することで接続を手動でSpIDer Gateへリダイレクトさせる場合は、Dr.Web Firewallの設定で、SpIDer Gateへの接続のリダイレクトを手動モードに切り替えることができます(この方法は推奨されません)。

- 詳細はマニュアル man: drweb-firewall(1)、drweb-gated(1)、iptables(8) を参照してください。

引き続きエラーが発生する場合は、テクニカルサポートまでご連絡ください。

症状：ファイルまたはディレクトリのアイコンをダブルクリックするとDr.Web for Linuxのスキャンが実行される。

説明：**Dr.Web for Linuxで開く** アクションと特定の種類またはディレクトリのファイルが、GUIによって自動的に関連付けられています。

エラーの解決

1. 1つの種類のファイルとDr.Web for Linuxとの関連付けをキャンセルしてください。関連付けは mimeapps.list ファイル、またはdefaults.list ファイル内に登録されています。ユーザープロファイル内で変更されたローカル設定のあるファイルは ~/.local/share/applications/ または ~/.config/ ディレクトリ内に保存されています（これらのディレクトリには通常「隠し」属性が付与されています）。
2. mimeapps.list または defaults.list ファイルをいずれかのテキストエディタで開きます（ファイルを編集するには、root権限が必要です。必要に応じ、su または sudo コマンドを使用します）。
3. ファイル内で [Default Applications] セクションと、*<MIME-type>*=drweb-gui.desktop となっている関連付けストリングを探します。例：

   ```
   [Default Applications]
   inode/directory=drweb-gui.desktop
   text/plain=drweb-gui.desktop;gedit.desktop
   ```

4. 関連付けストリングの（=の）右側の部分に drweb-gui.desktop 以外の他のアプリケーションへのリンクが含まれてた場合、drweb-gui（drweb-gui.desktop）リンクのみをストリングから削除してください。関連付けに drweb-gui アプリケーションへのリンクのみが含まれていた場合、関連付けストリング全体を削除します。
5. 変更したファイルを保存します。

追加情報：

- 現在の関連付けについて確認するには、xdg-mime、xdg-open、xdg-settings ユーティリティ（xdg-utils パッケージ内に含まれています）を使用してください。
- xdg ユーティリティの詳細については、man: xdg-mime(1)、xdg-open(1)、xdg-settings(1) を確認してください。

引き続きエラーが発生する場合は、テクニカルサポートまでご連絡ください。

さらに、パラメータ値のリストに新しい値を追加するには、オプション-aを使用する必要があります（以下参照）。

付録E. SpIDer Guard用カーネルモジュールの作成

このセクションの内容:

概要

OSが fanotifyモニタリングインターフェースをサポートしていない場合、SpIDer Guardはカーネル空間内で動作する特別なローダブルモジュール(Linuxカーネルモジュール、LKMモジュール)を使用します。

デフォルトでは、SpIDer Guardはfanotifyサービスをサポートしていないos用の完成したローダブルカーネルモジュールと一緒に提供されます。ローダブルカーネルモジュールは、`tar.bz2` アーカイブ内で提供されるソースコードを使用して作成することも可能です。

SpIDer Guardの使用するLKMモジュールは、GNU/Linuxカーネル2.6以降との動作を意図しています。

E2KおよびARM64アーキテクチャの場合、LKMでの動作はサポートされていません。

ソースコードのあるアーカイブはDr.Web for Linuxベースディレクトリの `share/drweb-spider-kmod/src` サブディレクトリ内にあります(デフォルトでは `/opt/drweb.com`)。アーカイブ名は `drweb-spider-kmod-<version>-<date>.tar.bz2` になります。`drweb-spider-kmod` ディレクトリには `check-kmod-install.sh` テストスクリプトも含まれています。お使いのOSが製品に含まれているカーネルモジュールをサポートしているかどうかを確認するにはスクリプトを実行してください。サポートしていない場合は手動でモジュールを作成するよう指示するメッセージが画面に表示されます。

指定したディレクトリ `drweb-spider-kmod` がない場合、`drweb-spider-kmod` パッケージを インストール します。

ソースコードからLKMモジュールを手動で構築するには、管理者(root)特権が必要です。その場合、`su` コマンドを使用して別のユーザーに切り替えるか、`sudo` コマンドを使用して別のユーザーとしてモジュールを構築できます。

カーネルモジュールを作成する

1. ソースコードが含まれているアーカイブをいずれかのディレクトリに展開します。たとえば、次のコマンドは作成されたディレクトリにソースコードを展開します。

```
# tar -xf drweb-spider-kmod-<version>-<date>.tar.bz2
```

ディレクトリはアーカイブと同じ場所に作成され、その名前はアーカイブと同じ名前になります。

2. 作成されたディレクトリで、以下のコマンドを実行します。

```
# make
```

make コマンドの実行中にエラーが発生した場合は問題を解決し（下記 参照）、再度コンパイルを開始してください。

3. *make* コマンドの実行に成功したら、以下のコマンドを入力してください。

```
# make install
# depmod
```

4. カーネルモジュールのコンパイルとシステムへの登録が完了したら、SpIDer Guardの追加設定を行います。次のコマンドを実行して、カーネルモジュールと連携するようにコンポーネントを設定します。

```
# drweb-ctl cfset LinuxSpider.Mode LKM
```

`LKM` の代わりに `AUTO` を指定することもできます。前者の場合、SpIDer Guardはカーネルモジュールとモニタリングインターフェースfanotifyを使用します。詳細については `man: drweb-spider(1)` を参照してください。

作成中に起こりうるエラー

make コマンドの実行中にエラーが発生する場合があります。その際は以下を確認してください。

- モジュールを作成するためには、Perl および GCC が必要です。これらがシステム上にない場合はインストールします。
- 一部のOSでは、手順を開始する前に `kernel-devel` パッケージをインストールする必要があります。
- 一部のOSでは、ソースコードのあるディレクトリへのパスが誤って指定されていることが原因で、作成に失敗する場合があります。その場合、`KDIR=`*<path to kernel source codes>* パラメータを使用して `make` コマンドを指定します。通常、ソースコードは `/usr/src/kernels/`*<kernel version>* ディレクトリにあります。

> `uname -r` コマンドによって返されるカーネルバージョンは、ディレクトリ名の *<kernel version>* と異なる場合があるという点に注意してください。

付録F. 略語のリスト

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。

文字・記号	説明
FQDN	Fully Qualified Domain Name（完全修飾ドメイン名）
GNU	GNUプロジェクト（GNU is Not Unix）
HTML	HyperText Markup Language（ハイパーテキストマークアップ言語）
HTTP	HyperText Transfer Protocol（ハイパーテキスト転送プロトコル）
HTTPS	HyperText Transfer Protocol Secure (over SSL/TLS)（ハイパーテキスト転送プロトコル（SSL/TLS経由））
ID	ID（識別子）
IMAP	Internet Message Access Protocol（メールプロトコル）
IP	Internet Protocol（インターネットプロトコル）
MBR	Master Boot Record（マスターブートレコード）
NSS	Novell Storage Services（Novellストレージサービス）
PID	Process ID（システムプロセスID）
PAM	Pluggable Authentication Modules（プラガブル認証モジュール）
POP	Post Office Protocol（メールプロトコル）
RPM	Red Hat Package Manager（Red Hatパッケージマネージャー）
SMTP	Simple Mail Transfer Protocol（メールプロトコル）
SP	Service Pack（サービスパック）
SSH	Secure Shell（セキュアシェル）
SSL	Secure Sockets Layer（セキュアソケットレイヤー）
TCP	Transmission Control Protocol（伝送制御プロトコル）
TLS	Transport Layer Security（トランスポート層セキュリティ）
UID	User ID（システムユーザーID）
URL	Uniform Resource Locator（ユニフォームリソースロケータ）
VBR	Volume Boot Record（ボリュームブートレコード）

文字・記号	説明
OS	オペレーティングシステム