



Dr.WEB
for UNIX File Servers

管理者マニュアル



© Doctor Web, 2020無断複写・転載を禁じます。

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

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

商標

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

免責事項

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

Dr.Web for UNIX File Servers

バージョン**11.1**

管理者マニュアル

2020/10/13

Doctor Webロシア本社

2-12A, 3rd str. Yamskogo polya, Moscow, Russia, 125040

ウェブサイト: <https://www.drweb.com/>

電話番号: +7 (495) 789-45-87

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

Doctor Web

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

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

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

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

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



目次

表記規則と略語	8
はじめに	9
この製品について	10
メイン機能	10
Dr.Web for UNIX File Servers の構成	12
隔離に移動する	19
ファイルのパーミッションと権限	20
動作モード	21
システム要件と互換性	24
ライセンス	28
インストールとアンインストール	29
Dr.Web for UNIX File Servers をインストールする	30
ユニバーサルパッケージをインストールする	30
コマンドラインからインストールする	32
リポジトリからインストールする	32
Dr.Web for UNIX File Servers をアップグレードする	35
最新のアップデートを入手する	36
新しいバージョンにアップグレードする	36
Dr.Web for UNIX File Servers をアンインストールする	39
ユニバーサルパッケージをアンインストールする	40
コマンドラインからアンインストールする	40
リポジトリからインストールした Dr.Web for UNIX File Servers をアンインストールする	41
追加情報	44
Dr.Web for UNIX File Servers パッケージとファイル	44
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	46
セキュリティサブシステムを設定する	51
SELinux セキュリティポリシーを設定する	51
PARSEC(Astra Linux SE) パーミッションの設定	54
CSEモードでの起動を設定する(Astra Linux SE 1.6)	56
開始する	58
製品の登録と有効化	58
製品の動作確認	61
ファイルシステムモニタリングの設定	62



Sambaファイルサーバーとの統合	64
NSSボリュームとの統合	67
簡単な説明	68
Dr.Web for UNIX File Serversコンポーネント	73
Dr.Web ConfigD	73
動作原理	73
コマンドライン引数	74
設定パラメータ	75
Dr.Web Ctl	78
コマンドラインフォーマット	79
使用例	105
設定パラメータ	108
Dr.Web Web管理インターフェース	109
コンポーネントを管理する	110
脅威の管理	111
設定を管理する	113
集中管理モードの管理	117
ローカルファイルをスキャンする	118
SpIDer Guard	122
動作原理	122
コマンドライン引数	125
設定パラメータ	125
ファイルシステムモニタリングの設定	132
SpIDer Guardにカーネルモジュールを使用する	132
SpIDer Guard for SMB	135
動作原理	135
コマンドライン引数	137
設定パラメータ	137
Sambaファイルサーバーとの統合	144
VFS SMBモジュールを構築する	144
SpIDer Guard for NSS	147
動作原理	147
コマンドライン引数	148
設定パラメータ	149
NSSボリュームとの統合	154
Dr.Web ClamD	155



動作原理	155
コマンドライン引数	155
設定パラメータ	156
外部アプリケーションとの統合	161
Dr.Web File Checker	163
動作原理	163
コマンドライン引数	164
設定パラメータ	164
Dr.Web Network Checker	167
動作原理	167
コマンドライン引数	169
設定パラメータ	170
スキャンクラスタを作成する	174
Dr.Web Scanning Engine	178
動作原理	178
コマンドライン引数	179
設定パラメータ	181
Dr.Web Updater	183
動作原理	183
コマンドライン引数	184
設定パラメータ	185
Dr.Web ES Agent	190
動作原理	190
コマンドライン引数	190
設定パラメータ	191
Dr.Web HTTPD	194
動作原理	194
コマンドライン引数	195
設定パラメータ	196
HTTP APIの説明	199
Dr.Web SNMPD	223
動作原理	223
コマンドライン引数	225
設定パラメータ	225
SNMPモニタリングシステムとの統合	229
Dr.Web SNMP MIB	237





Dr.Web MeshD	265
動作原理	265
コマンドライン引数	268
設定パラメータ	269
Dr.Web CloudD	273
動作原理	273
コマンドライン引数	274
設定パラメータ	274
Dr.Web StatD	276
動作原理	276
コマンドライン引数	276
設定パラメータ	277
付録	279
付録 A. コンピューター脅威の種類	279
付録 B. コンピューター脅威の駆除	283
付録 C. テクニカルサポート	286
付録D. Dr.Web for UNIX File Servers設定ファイル	288
ファイル構造	288
パラメータタイプ	290
付録E. SSL証明書を生成する	293
付録F. 既知のエラー	296
付録G. 略語のリスト	342



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



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 G. 略語のリスト](#) にあります。



はじめに

Dr.Web for UNIX File Serversをお買い上げ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および駆除テクノロジーを活用して、さまざまなタイプのコンピューター脅威からサーバーとユーザーを確実に保護します。

このマニュアルの目的は、**GNU/Linux**ファミリーのOSや、**FreeBSD**などの他のUNIX系OSを実行しているサーバーの管理者が、Dr.Web for UNIX File Serversバージョン11.1をインストールしてご使用いただけるように支援することです。

ファイルパスの表記法

Dr.Web for UNIX File Serversは、さまざまな**UNIX**ベースのOSで動作します。ファイルとコンポーネントへの実際のパスは、OSによって異なります。本書では、次の表記法を使用しています。

- `<opt_dir>` - 主な製品ファイルがあるディレクトリ(実行ファイルとライブラリを含む)。
- `<etc_dir>` - 設定ファイルとキーファイルがあるディレクトリ。
- `<var_dir>` - サポートと製品の一時ファイルが配置されているディレクトリ。

さまざまなOSの規則に対応する実際のパスは、以下の表に示されています。

OSの種類	文字・記号	実際のパス
GNU/Linux	<code><opt_dir></code>	<code>/opt/drweb.com</code>
	<code><etc_dir></code>	<code>/etc/opt/drweb.com</code>
	<code><var_dir></code>	<code>/var/opt/drweb.com</code>
FreeBSD	<code><opt_dir></code>	<code>/usr/local/libexec/drweb.com</code>
	<code><etc_dir></code>	<code>/usr/local/etc/drweb.com</code>
	<code><var_dir></code>	<code>/var/drweb.com</code>

スペースを考慮して、例では**GNU/Linux** OSのパスを使用しています。本書では、可能な場合においてすべてのOSの実際のパスが例に使用されています。



この製品について

このセクションには、Dr.Web for UNIX File Serversに関する次の情報が含まれています。

- [機能](#)。
- [メイン機能](#)。
- [Dr.Web for UNIX File Serversの構成](#)。
- [隔離に移動する](#)。
- [ファイルのパーミッションと権限](#)。
- [動作モード](#)。

機能

Dr.Web for UNIX File Serversは、UNIX(**GNU/Linux**、**FreeBSD**)で実行されているファイルサーバーを、ウイルスや他のタイプの悪意のあるソフトウェアから保護し、さまざまなプラットフォーム向けに作成された脅威の拡散を防ぐためのものです。

主なコンポーネント(スキャンエンジンとウイルスデータベース)は、非常に効果的でリソースを節約するだけでなく、クロスプラットフォームでもあるため、Doctor Webスペシャリストはさまざまなプラットフォームをターゲットとした脅威から一般的なOSのコンピューターやモバイルデバイスを守る、信頼性の高いアンチウイルスソリューションを作成できます。現在、Doctor WebではDr.Web for UNIX File Serversとともに、**UNIX**ベースのOS(**GNU/Linux**、**FreeBSD**)と**IBM OS/2**、**Novell NetWare**、**macOS**と**Windows**の両方のアンチウイルスソリューションを提供しています。さらに、**Android**、**Symbian**、**BlackBerry**、Windows Mobileを実行するデバイスを保護するための、他のアンチウイルス製品が開発されています。

Dr.Web for UNIX File Serversのコンポーネントは常に更新され、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、メールメッセージのスパムフィルタリングのルールデータベースには定期的に新しいシグネチャが追加されるため、サーバー、ワークステーション、モバイルユーザーとそのプログラムやデータに最新の保護を提供します。未知のウイルスに対する追加の保護を提供するため、スキャンエンジンとDr.Web Cloudサービスにはヒューリスティック解析が実装されており、シグネチャがデータベースにない最新の脅威に関する情報を保存します(この機能は一部の製品でのみ利用できます)。

メイン機能

Dr.Web for UNIX File Servers のメイン機能

1. **脅威の検出と駆除**。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に感染するものを含むウイルス、トロイの木馬、メールワームなど)や不要なソフトウェア(アドウェア、ジョークプログラム、ダイアラーなど)を検索します。コンピューターの脅威の種類に関する詳細については、[付録 A. コンピューター脅威の種類](#)を参照してください。

脅威の検出方法:

- **シグネチャ解析**。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、最近の脅威に関する最新情報を収集し、Dr.Web製品に送信します。



ヒューリスティックアナライザは誤検知を引き起こす可能性があることに注意してください。したがって、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。このようなファイルを隔離し、解析のためにDoctor Webアンチウイルスラボに送信することをお勧めします。脅威を駆除する方法の詳細は、[付録 B. コンピューター脅威の駆除](#)を参照してください。

ユーザーの要求に応じてファイルシステムをスキャンする場合、ユーザーが利用できるすべてのファイルシステムオブジェクトのフルスキャン、または指定されたオブジェクトのみ（指定された基準を満たす個別のディレクトリまたはファイル）のカスタムスキャンが可能です。さらに、システム内で現在アクティブなプロセスをサポートするボリュームと実行ファイルのブートレコードを別々にチェックすることもできます。後者の場合、脅威が検出されると、悪意のある実行ファイルを駆除するだけでなく、選択的スキャンにより実行されているすべてのプロセスが強制的に終了されます。一連の異なるアクセスレベルを持つファイルへのアクセスの必須モデルを実装するシステムでは、現在のアクセスレベルでは利用できないファイルのスキャンは特別な[自律コピー](#)モードで行うことができます。

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、永久保存された脅威レジストリに登録されます。

Dr.Web for UNIX File Serversに含まれている[Dr.Web Ctl](#)コマンドラインを使うと、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脅威ファイルシステムをスキャンできます。



リモートスキャンは、リモートホスト上の悪意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、このホストによって直接提供される管理ツールを使用する必要があります。たとえば、ルーターやその他の「スマート」デバイスの場合は、ファームウェア更新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は、コンピューティングマシンへの接続（任意でリモート端末モードを使用）と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）、またはコンピューティングマシン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の実行を介して実行できます。

2. ファイルへのアクセスの監視:

- **OS内のファイルシステムファイルイベント**を監視し、実行可能ファイルの実行を試みます。この機能により、サーバーのファイルシステムを感染させようとするマルウェアを検出して駆除できます。標準のモニタリングモードに加え、スキャンが完了するまでモニターがファイルへのアクセスをブロックする拡張（パラノイド）モードを有効にできます（これにより、感染したファイルへのアクセスを防止できます。ただし、アプリでファイルにアクセスすると、スキャン結果を入手できます。拡張モードでは、セキュリティレベルは向上しますが、まだスキャンされていないファイルへのアクセスが遅くなります。

ボリュームモニタリング機能は、**GNU/Linux** ファミリーのオペレーティングシステムでのみ利用可能です。他の[サポート対象の](#)オペレーティングシステムの場合、この機能を提供するコンポーネントはパッケージに含まれていません。

- **Samba共有ディレクトリ**。ファイルサーバーのローカルユーザーとリモートユーザーの読み取りおよび書き込み操作が監視されます。この機能により、悪意のあるプログラムのファイルストレージへの保存が試行された際に、マルウェアを検出、駆除できます。これにより、ネットワーク全体への拡散を防ぐことができます。
- **NSS (Novell Storage Services) ボリューム**。NSSファイルストレージユーザーの書き込み操作を監視します。この機能により、悪意のあるプログラムのNSSストレージへの保存を試行し、マルウェアを検出、駆除できます。これにより、ネットワーク全体へ広がることを防ぐことができます。

Novell Storage Servicesのボリューム監視機能は、**Novell Open Enterprise Server SP2 SUSE Linux Enterprise Server**オペレーティングシステム10 SP3以降でのみ使用可能です。他の[サポート対象の](#)オペレーティングシステムの場合、この機能を提供するコンポーネントはパッケージに含まれていません。

3. **感染したオブジェクトや疑わしいオブジェクトを確実に隔離**します。サーバーのファイルシステムで検出されたそのようなオブジェクトは、システムへの害を防ぐ特別なフォルダに移動され、隔離されます。隔離へ移動



されたオブジェクトは、特別なルールに従って名前が変更され、必要に応じて、オンデマンドでのみ元の場所に復元できます。

4. マルウェアに対する高度な保護を維持するための、スキャンエンジン、ウイルスデータベースの自動更新。
5. 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。SNMPを介して検出された脅威に関する通知を外部のモニタリングシステムと集中管理サーバーに(Dr.Web for UNIX File Serversが集中管理モードで動作している場合はDr.Web Cloudにも)送信。
6. 集中管理モードでの動作(Dr.Web Enterprise Serverなどの集中管理サーバーに接続されている場合、またはDr.Web AV-Deskサービスの一部として)。このモードによって、保護されたネットワーク内のコンピュータに統一されたセキュリティポリシーを実装することができます。企業のネットワーク、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)のいずれかです。

Dr.Web for UNIX File Serversの構成

Dr.Web for UNIX File Serversは複数のコンポーネントで構成され、各コンポーネントには独自の機能のセットがあります。コンポーネントの目的に応じて、次のカテゴリーに分類されます。

- **基本アンチウイルスコンポーネント**: Dr.Web for UNIX File Serversコアを形成。このカテゴリーのコンポーネントがない場合、製品はファイル(およびその他のデータ)をスキャンできず、ウイルスやその他の脅威を検出できません。
- **脅威検索コンポーネント**: これらのコンポーネントは、Dr.Web for UNIX File Serversの基本的なタスクを解決するために使用されます。これらのコンポーネントは、動作時に基本アンチウイルスコンポーネントを使用します。
- **サービスコンポーネント**: 補助的アンチウイルス保護の問題を解決(アンチウイルスデータベースの更新、集中管理サーバー接続、一般的なDr.Web for UNIX File Servers動作管理など)。
- **インターフェースコンポーネント**: (ユーザーまたはサードパーティのアプリケーション)にDr.Web for UNIX File Serversのインターフェースを提供。

以下は、Dr.Web for UNIX File Serversコンポーネントのリストです。

1. 基本アンチウイルスコンポーネント

コンポーネント	説明
Dr.Web Virus-Finding Engine	<p>スキャンエンジン。<u>ウイルスと悪意のあるプログラム</u>を検出する<u>アルゴリズム</u>を実装します(シグネチャ解析とヒューリスティック解析を使用)。</p> <p>スキャンエンジンはDr.Web Scanning Engine管理によって動作しています。</p> <hr/> <p>実行ファイル: drweb32.dll</p> <p>ログファイルに出力される内部名: CoreEngine</p>
<u>Dr.Web Scanning Engine</u>	<p>スキャンエンジン。このコンポーネントは、Dr.Web Virus-Finding Engineスキャンエンジンとアンチウイルスデータベースをロードします。</p> <ul style="list-style-type: none">● スキャンのためにファイルの内容とブートレコードをスキャンエンジンに送信します。● スキャンを待機しているファイルをキューに入れます。● このアクションが適用可能な脅威を修復します。



コンポーネント	説明
	<p>Dr.Web ConfigDによって動作するか、自律的に動作できます。</p> <p>Dr.Web File CheckerおよびDr.Web Network Checkerコンポーネントで使用されます。また、Dr.Web MeshDコンポーネント（特定のモード）、およびDr.Web Scanning Engine APIで使 用される外部（Dr.Web for UNIX File Serversに対して）アプリケーションで使用できます。</p> <p>実行ファイル：drweb-se ログに表示される内部名：ScanEngine</p>
ウイルスデータベース	<p>ウイルスデータベース。ウイルスのシグネチャやその他の脅威のデータベースと悪質なソフトウェアの検出と駆除のアルゴリズムは自動で更新されます。</p> <p>スキャンエンジンDr.Web Virus-Finding Engineで使 用され、一緒に提供されます。</p>
Dr.Web File Checker	<p>ファイルシステムコンポーネントと隔離マネージャーをスキャンするためのコンポーネント。</p> <ul style="list-style-type: none">ローカル（Dr.Web Scanning Engineに対して）ファイルシステムのファイルをスキャンするときに、脅威スキャンコンポーネントからタスクを受け取ります。タスクに従ってファイルシステムディレクトリをサーフし、スキャンするファイルをDr.Web Scanning Engineエンジンに送信し、スキャンの進行状況をクライアントコンポーネントに通知します。感染したファイルの削除、隔離への移動、隔離からの復元、隔離ディレクトリの管理を行います。キャッシュを構築し、最新の状態に保ちます。キャッシュには、以前にスキャンされたファイルに関する情報が含まれており、ファイルを再スキャンする周期を減らします。 <p>SpIDer Guard、SpIDer Guard for SMB、SpIDer Guard for NSSなどファイルシステムオブジェクトをスキャンするコンポーネントによって使 用されます。</p> <p>実行ファイル：drweb-filecheck ログに表示される内部名：FileCheck</p>
Dr.Web Network Checker	<p>ネットワークデータスキャンエージェント。</p> <ul style="list-style-type: none">実際にスキャンを実行する際、スキャンエンジンにデータを送信するのに使 用されます。データは、ネットワーク経路で製品のコンポーネントによって送信されます（Dr.Web ClamDなどのコンポーネント）。Dr.Web for UNIX File Serversが、リモートホストからまたはリモートホストへのスキャンにファイルを送受信するファイルの分散スキャンを手配することが可能になります。そのためには、リモートホストにはUNIXオペレーティングシステム用にインストールされ実行されているDr.Webを備えている必要があります。分散スキャンモードでは、多数のスキャンタスクのあるホスト（メールサーバー、ファイルサーバー、インターネットゲートウェイなど）の負荷を減らすことで、リモートホスト間でスキャン負荷を自動的に分散できます。



コンポーネント	説明
	<p>スキャン用のデータを受信できるネットワーク内のパートナーホストが存在する場合、スキャンにDr.Web Network Checkerを使用するコンポーネントはローカルのDr.Web Scanning Engineエンジンを使用しない場合があります。したがって、Dr.Web Scanning Engine、Dr.Web Virus-Finding Engine、およびアンチウイルスデータベースがない可能性があります。</p> <p>セキュリティ上の理由から、ファイルはSSLで転送されます。</p> <p>実行ファイル: drweb-netcheck ログに表示される内部名: NetCheck</p>
Dr.Web MeshD	<p>Dr.Web for UNIX File Serversをローカルクラウドに接続するコンポーネント。Dr.Web for UNIX製品が更新およびファイルスキャンの結果を交換し、スキャンのためにファイルを相互に送信し、スキャンエンジンサービスを直接提供できるようにします。</p> <p>このコンポーネントが製品に含まれている他、コンポーネントが接続されているローカルクラウドとスキャンエンジンサービスを提供するホストが存在する場合、Dr.Web Scanning Engine、Dr.Web Virus-Finding Engine、およびアンチウイルスデータベースがない可能性があります。</p> <p>実行ファイル: drweb-meshd ログに表示される内部名: MeshD</p>

2. 脅威検索コンポーネント

コンポーネント	説明
SpIDer Guard	<p>Linuxファイルシステムモニター。</p> <p>バックグラウンドモードで動作し、GNU/Linuxファイルシステム内のファイル操作（作成、開く、閉じる、実行など）を制御します。各操作が実行される場合、Dr.Web File Checkerコンポーネント要求を送り、プログラムの実行可能ファイルと同様に新規ファイルまたは変更されたファイルをスキャンします。</p> <p>そのオプションに応じて、OSはfanotifyメカニズム（OSによって用意されているAPI）またはDr.Webによって開発された特別なカーネルモジュールを使用します（LKMモジュールはSpIDer Guardと共に別のパッケージで用意されます）。システムメカニズムfanotifyを介して作業している場合、モニターは拡張モードで動作し、スキャンが完了するまでまだスキャン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できます。デフォルトでは、拡張モードは無効になっています。</p> <div> GNU/LinuxOS用ディストリビューションにのみ含まれています。</div> <p>実行ファイル: drweb-spider ログに表示される内部名: LinuxSpider</p>



コンポーネント	説明
SpIDer Guard用の GNU/Linux カーネルモジュール	<p>GNU/Linuxカーネルモジュール(LKMモジュール)は、一部のオペレーティングシステムでファイルシステムイベントにアクセスする際にSpIDer Guardが使用しています。これらのオペレーティングシステムでは、API fanotify が使用できないか、機能が制限されて実装されています。</p> <p>コンポーネントはコンパイル済み(fanotifyが実装されていない、または利用できないオペレーティングシステム用)のものと、手動でオペレーティングシステムカーネルモジュールを構築、インストールするためのソースコードとして含まれています(手順については、SpIDer Guard用のカーネルモジュールを構築するセクションを参照してください)。</p> <div> GNU/LinuxOS用ディストリビューションにのみ含まれています。</div> <p>実行ファイル: drweb.ko</p>
SpIDer Guard for SMB	<p>Samba共有ディレクトリモニター。</p> <p>Sambaサーバーのファイルストレージとして選択されたディレクトリで、バックグラウンドモードで動作し、ファイルシステムの操作(作成、開く、閉じる、読み取り、書き込み操作など)を監視します。新規または変更されたファイルの内容をスキャン用にDr.Web File Checkerコンポーネントに送ります。</p> <p>ファイルサーバーとの統合には、Sambaサーバー側で動作するVFS Sambaモジュールを使用します。</p> <p>実行ファイル: drweb-smbspider-daemon ログに表示される内部名: SMBSpider</p>
SpIDer Guard for NSS	<p>NSS(Novell Storage Services)ボリューム監視。</p> <p>バックグラウンドモードで動作し、ファイルシステムにマウントされたNSSボリューム上のファイルシステム操作(作成、開く、閉じる、書き込み操作など)を監視します。新規または変更されたファイルの内容をスキャン用にDr.Web File Checkerコンポーネントに送ります。</p> <div> GNU/LinuxOS用ディストリビューションにのみ含まれています。このコンポーネントは、SUSE Linux Enterprise Server 10 SP3以降をベースにしたNovell Open Enterprise Server SP2上でのみ動作できます。</div> <p>実行ファイル: drweb-nss ログに表示される内部名: NSS</p>

3. サービスコンポーネント

コンポーネント	説明
Dr.Web ConfigD	Dr.Web for UNIX File Servers設定デーモン。次の機能を実行します。



コンポーネント	説明
	<ul style="list-style-type: none">• 設定に応じて、製品のコンポーネントを起動／停止します。• 動作に障害が発生した場合、コンポーネントを自動的に再起動します。他のコンポーネントのリクエストに応じてコンポーネントを起動します。別のコンポーネントが起動またはシャットダウンしたときにアクティブなコンポーネントに通知します。• 現在のライセンスキーと設定に関する情報を保存し、このデータをすべてのコンポーネントに提供します。それらの情報を提供すると予測されるDr.Web for UNIX File Serversのコンポーネントから設定とライセンスキーを受け取ります。ライセンスキーと設定の変更について他のコンポーネントに通知します。 <p>実行ファイル: drweb-configd ログファイルに出力される内部名: ConfigD</p>
Dr.Web ES Agent	<p>集中管理エージェント集中管理モードとモバイルモードでの製品動作の組み合わせを確実なものにします。</p> <ul style="list-style-type: none">• 製品と集中管理サーバー間の接続、ライセンスキーファイル、ウイルスデータベースとコンポーネントの更新。• Dr.Web for UNIX File Serversに含まれるコンポーネントとその状態、ウイルスイベントの統計に関する情報をサーバーに送信します。 <p>実行ファイル: drweb-esagent ログに表示される内部名: ESAgent</p>
Dr.Web Updater	<p>更新コンポーネント</p> <p>ウイルスデータベース、スキャンエンジン。</p> <p>アップデートはスケジュールに従い、またユーザーの要求に応じて (Dr.Web Ctlまたは管理Webインターフェース経由で) 自動的にダウンロードできます。</p> <p>実行ファイル: drweb-update ログに表示される内部名: Update</p>
Dr.Web CloudD	<p>Dr.Web Cloudインタラクションコンポーネント。</p> <p>Dr.Web Cloudサービスに、閲覧したURLとスキャンしたファイルに関する情報を送信するコンポーネントです。これらの情報は、ウイルスデータベースにまだ記載されていない脅威をチェックします。</p> <p>実行ファイル: drweb-cloudd ログに表示される内部名: CloudD</p>
Dr.Web StatD	<p>Dr.Web for UNIX File Serversコンポーネントの動作イベントを格納するためのコンポーネント。</p> <p>プログラムの複雑なイベント (異常終了、脅威の検出など) のストレージを受け取り、管理します。</p> <p>実行ファイル: drweb-statd ログファイルに出力される内部名: StatD</p>



4. インターフェースコンポーネント

コンポーネント	説明
Dr.Web HTTPD	<p>Dr.Web for UNIX File Servers管理 Webサーバー。</p> <p>Dr.Web for UNIX File Serversコンポーネントを管理するためのカスタム HTTP APIを提供します。</p> <p>指定されたAPIは、管理 Webインターフェース（個別にインストールする必要があります）。</p> <p>セキュリティ上の理由から、WebインターフェースはHTTPS経由でユーザーと対話します。</p> <p>Dr.Web Network Checkerを使用して、スキャン用のデータをDr.Web Scanning Engineに送信します。</p> <p>実行ファイル: drweb-httpd ログに表示される内部名: HTTPD</p>
Dr.Web Web管理インターフェース	<p>管理 Webインターフェース</p> <p>ローカルホストまたはリモートホスト上の任意のブラウザからインターフェースにアクセスできます。Webインターフェースにより、製品はサードパーティの Webサーバー（Apache HTTP Serverなど）も Webminなどのリモート管理ツールも使用できません。</p> <p>コンポーネントの機能は、Dr.Web HTTPDコンポーネントによって提供されます。</p>
Dr.Web Ctl	<p>コマンドラインからDr.Web for UNIX File Serversを管理するためのツール。</p> <p>ユーザーがファイルスキャンを開始し、隔離されたオブジェクトを表示し、ウイルスデータベースの更新手順を開始し、Dr.Web for UNIX File Serversを集中管理サーバーに接続または切断し、パラメータを表示、設定できるようにします。</p> <p>実行ファイル: drweb-ctl ログに表示される内部名: Ctl</p>
Dr.Web SNMPD	<p>SNMPエージェント。</p> <p>Dr.Web for UNIX File ServersとSNMP経由の外部監視システムとの統合用に設計されています。このような統合により、製品のコンポーネントの状態を監視したり、脅威の検出と駆除に関する統計を収集したりできます。</p> <p>SNMP v2cとv3をサポートします。</p> <p>実行ファイル: drweb-snmpd ログに表示される内部名: SNMPD</p>
Dr.Web ClamD	<p>アンチウイルスデーモンである clamd（ClamAV® アンチウイルスのコンポーネント）のインターフェースをエミュレートするコンポーネント。</p> <p>ClamAV®をサポートするすべてのアプリケーションが、アンチウイルススキャンにDr.Web for UNIX File Serversを透過的に使用できるようになります。</p>



コンポーネント	説明
	モードに応じて、Dr.Web Network CheckerまたはDr.Web File Checkerを使用して、スキャン用のデータをDr.Web Scanning Engineに送信します。
	実行ファイル: drweb-clamd ログに表示される内部名: ClamD

下の図は、Dr.Web for UNIX File Serversの構造とその外部アプリケーションとの動作を示しています。

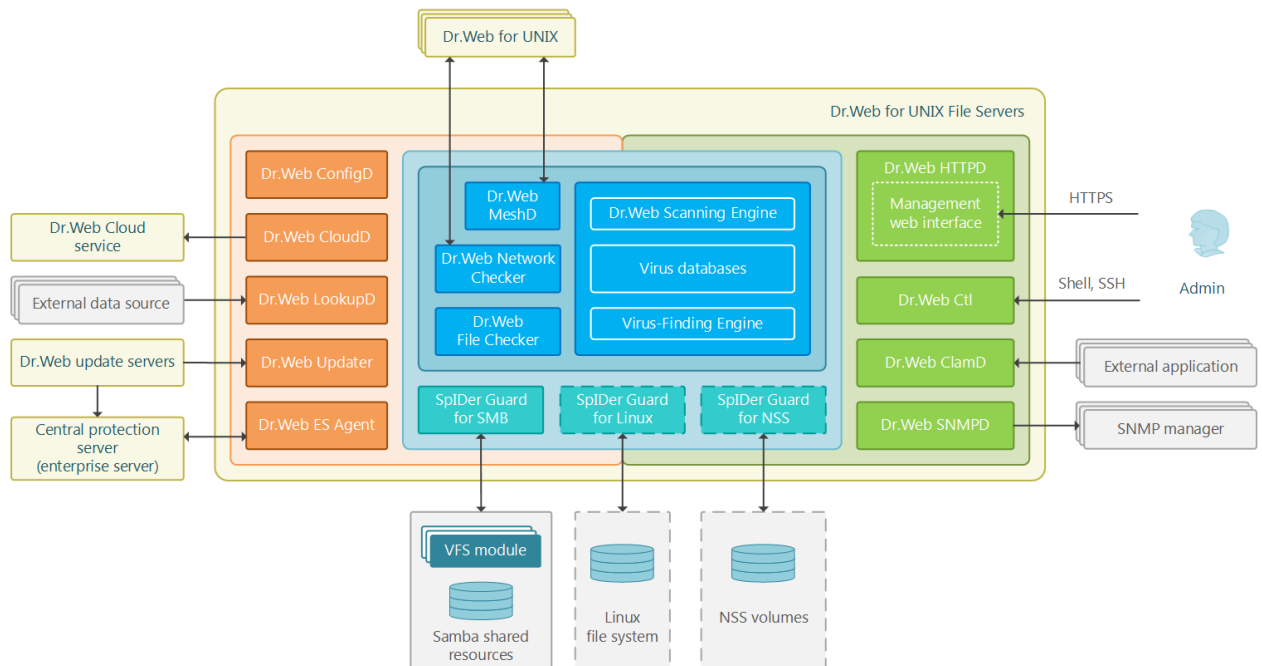


図1. Dr.Web for UNIX File Serversの構造

このスキームでは、次の表記法が使用されています。

	- Dr.Web for UNIX File Serversのコンポーネントおよびソリューションに含まれないDr.WebのシステムやDr.Webのアプリケーション。
	- Dr.Web for UNIX Mail Serversと連携する外部プログラムや製品。
	- 特定のアンチウイルス保護タスク(アンチウイルスデータベースの更新、集中管理サーバーへの接続、一般的な動作管理など)を実行するサービスコンポーネント。
	- (ユーザーまたはサードパーティ製アプリケーションに) Dr.Web for UNIX File Serversのインターフェースを提供するコンポーネント。
	- アンチウイルススキャンに使用されるコンポーネント。
	- Dr.Web for UNIX File Serversコアを形成する基本的なアンチウイルスコンポーネント。データとファイルのスキャンを実行するコンポーネントによって使用されます。

Dr.Web for UNIX File Serversのディストリビューションと使用状況によっては、破線でマークされたコンポーネントが含まれない場合があります。



Dr.Web for UNIX File Serversコンポーネントの詳細については、[Dr.Web for UNIX File Serversコンポーネント](#)を参照してください。

隔離に移動する

Dr.Web for UNIX File Servers 11.1の隔離ディレクトリは、システムセキュリティに脅威を与え、現在修復できないファイルを分離するのに役立ちます。このような脅威は、Dr.Web for UNIX File Serversにとって未知のもの（つまり、ヒューリスティックアナライザによってウイルスが検出されたが、ウイルスのシグネチャおよび修復方法がデータベースにないもの）または修復中にエラーを引き起こしたものになります。さらに、ユーザーが検出された脅威のリストで[アクション](#)として隔離を選択した場合や、脅威の[タイプ](#)ごとにアクションとして隔離を設定で指定した場合は、ユーザーの要求に応じてファイルを隔離できます。

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 UNIX File Servers 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隔離ディレクトリの名前は常に`.com.drweb.quarantine`となり、「隔離」[アクション](#)が適用されるまで作成されません。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、隔離に移動された感染ファイルは常にボリューム上に配置されるため、複数のリムーバブルデータストレージやその他のボリュームがシステム内の異なる場所にマウントされた場合でも、隔離は正しく動作します。

ユーザーは、ユーティリティ[Dr.Web Ctl](#)を使用してコマンドラインから隔離コンテンツを管理できる他、[管理用 Webインターフェース](#)（インストールされている場合）上からも管理できます。すべてのアクションは隔離全体に適用されます。つまり、変更はその時点で利用可能なすべての隔離ディレクトリに影響します。



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。

Dr.Web for UNIX File Serversのすべてのアンチウイルスコンポーネントが脅威の分離に隔離を使用できるわけではありません。たとえば、Dr.Web ClamD、Dr.Web ICAPD、Dr.Web MailDのコンポーネントでは使用されません（製品に含まれていない場合があります）。



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 UNIX File Servers(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。
アーカイブのコンテンツを一覧表示する (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。

スーパーユーザー(*root*) 権限でコマンドライン管理 [Dr.Web Ctl](#) ツールの動作を有効にするには、**su** コマンドを使用してユーザーを変更するか、**sudo** コマンドを使用して、他のユーザーとしてコマンドを実行できます。



Dr.Web Scanning Engine スキャンエンジンは、4 GB を超えるサイズのファイルをスキャンできません(このようなファイルをスキャンしようとすると、エラーメッセージ「ファイルサイズが大きすぎます」が表示されます)。



動作モード

Dr.Web for UNIX File Serversは、スタンドアロンモードでも、**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も動作できます。**集中管理**モードでの操作には、追加のソフトウェアのインストールやDr.Web for UNIX File Serversの再インストールまたは削除は必要ありません。

- **スタンドアロンモード**では、保護す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、その操作はローカルで管理されます。このモードでは、設定ファイルとライセンスキーファイルはローカルディスクにあり、Dr.Web for UNIX File Serversは保護するコンピューターから完全に制御されます。ウイルスデータベースの更新はDoctor Web更新サーバーから受信します。
- **集中管理モード**(エンタープライズモード)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 UNIX File Serversの一部の機能と設定は、アンチウイルスネットワークに実装されている一般的な(企業の)アンチウイルス保護ポリシーに従って調整できます。集中管理モードでの動作に使用されるライセンスキーファイルは、集中管理サーバーから受信されます。ローカルコンピューターに保存されているデモキーファイルがあっても、そのファイルは使用されません。Dr.Web for UNIX File Serversの操作に関する情報とともにウイルスイベントの統計が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への更新も集中管理サーバーから受信されます。
- **モバイルモード**では、Dr.Web for UNIX File ServersはDoctor Web更新サーバーから更新を受信しますが、製品の操作はローカル設定と集中管理サーバーから受信したライセンスキーファイルで管理されます。モバイルモードに切り替えることができるのは、集中管理サーバー設定で許可されている場合のみです。

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 UNIX File Servers」)によって脅威から保護されます。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。

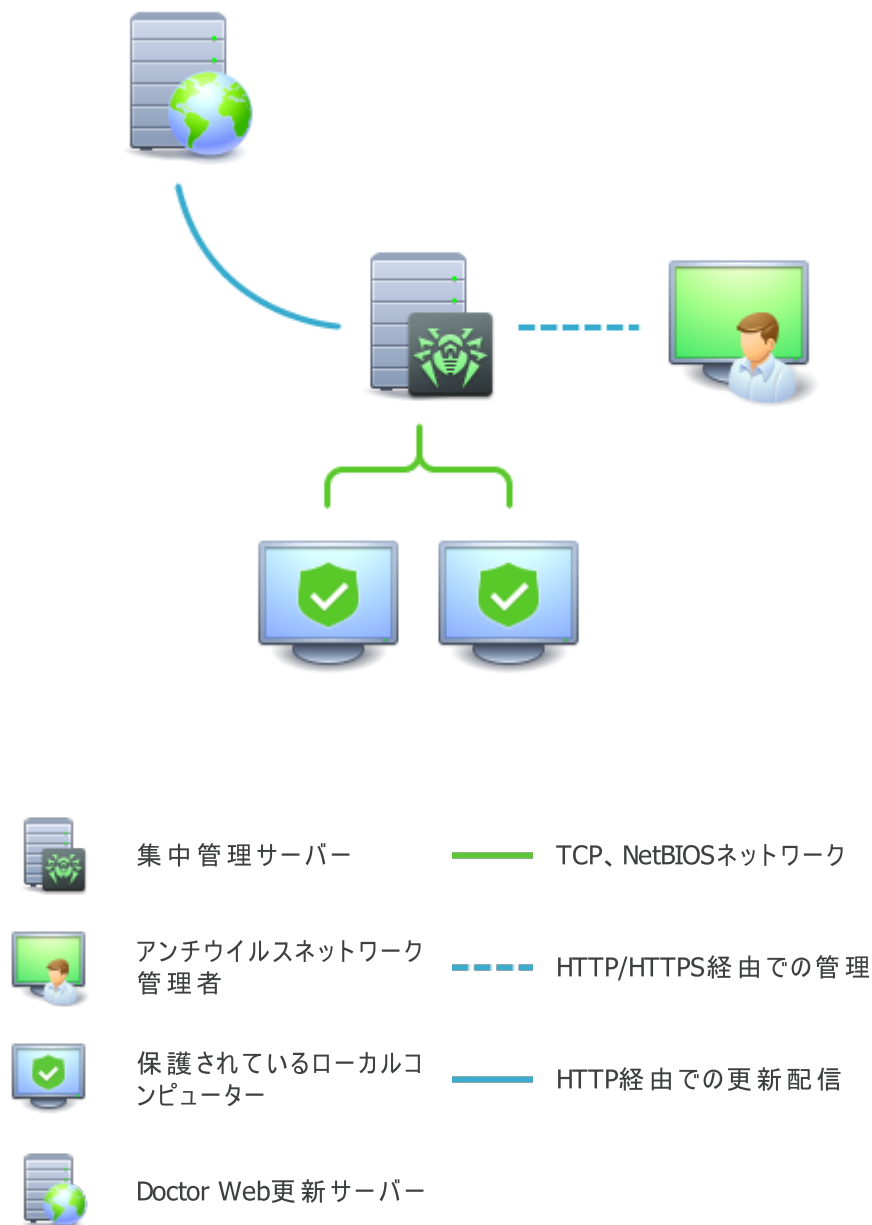


図2. アンチウイルスネットワークの理論的構造

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から受け取ったコマンドに従って、集中管理サーバーから設定および管理されます。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を管理し(たとえば、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)、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、第三者製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 Anti-virus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、集中管理センターを使用して操作レポートをエクスポートおよび保存できます。レポートは、HTML、CSV、PDF、XML形式でエクスポートおよび保存できます。

集中管理サーバーとの接続

Dr.Web for UNIX File Serversは、[Dr.Web Ctl](#)コマンドラインベース管理ツールの[esconnect](#)コマンドを使用して、アンチウイルスネットワークの集中管理サーバーに接続できます。



集中管理サーバーを検証するには、サーバーが使用する一意のパブリック暗号化キーに対応する証明書を使用します。デフォルトでは、[Dr.Web ES Agent](#)集中管理エージェントは、接続しているサーバーの証明書ファイルを指定しない限り、サーバーへの接続を許可しません。証明書ファイルは、最初に、Dr.Web for UNIX File Serversを接続するサーバーが提供するアンチウイルスネットワークの管理者から取得する必要があります。

Dr.Web for UNIX File Serversが集中管理サーバーに接続されている場合は、製品をモバイルモードに切り替えたり、集中管理モードに戻したりできます。モバイルモードのオン/オフの切り替えは、[Dr.Web ES Agent](#)コンポーネントの[MobileMode](#)設定パラメータのヘルプを使用しています。



Dr.Web for UNIX File Serversは、集中管理サーバーの設定で許可されている場合にのみ、モバイルモードに切り替えることができます。

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 UNIX File Serversは、[Dr.Web Ctl](#)コマンドラインベース管理ツールの[esdisconnect](#)コマンドを使用して、アンチウイルスネットワークの集中管理サーバーから切断できます。




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](#)
- [テスト済みOSディストリビューションのリスト](#)
- [追加のパッケージとコンポーネント](#)
- [免責事項](#)
- [サポート対象のファイルサーバー](#)
- [セキュリティサブシステムとの互換性](#)。

システム要件

Dr.Web for UNIX File Servers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
プラットフォーム	以下のアーキテクチャおよび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。 <ul style="list-style-type: none">• Intel/AMD: 32ビット (IA-32, x86)、64ビット (x86_64, x64, amd64)• ARM64
ランダムアクセスメモリー (RAM)	少なくとも500MbのRAM空き容量 (1Gb以上を推奨)。
ハードディスク容量	Dr.Web for UNIX File Servers ディレクトリのあるボリュームに1GB以上の空きディスク容量。
オペレーティングシステム	GNU/Linux (カーネルバージョン2.6.37以降、 glibc ライブラリ2.13以降を使用)、 FreeBSD (バージョン10.3以降)。 <div> オペレーションシステムはPAM認証メカニズムをサポートする必要があります。</div> <p>テスト済みのオペレーティングシステムのディストリビューションは以下のとおりです。</p>
その他	以下の有効なネットワーク接続が必要です。 <ul style="list-style-type: none">• ウイルスデータベースとDr.Web for UNIX File Serversコンポーネントの更新を可能にする有効な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サーバーへの接続で十分です。インターネットへの接続は必要ありません。

Dr.Web for UNIX File Servers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。

機能	方向	ポート番号
更新を受け取るため	送信	80



機 能	方 向	ポ ー ト 番 号
Dr.Web Cloudサービスに接続するため	送 信	2075 (UDPのポート番号を含む)

テスト済みオペレーティングシステムのディストリビューション

Dr.Web for UNIX File Serversは以下のディストリビューションでの動作が確認されています。

• GNU/Linux:

GNU/Linuxディストリビューション名	バージョン	プラットフォーム
Astra Linux Special Edition (Smolensk)	1.5、1.6	x86_64
ALT Linuxサーバー	9	ARM64
ALT Linuxワークステーション	9	ARM64
Debian	7.11、8.10、9.3	x86_64
Fedora	27～29	x86、x86_64
Red Hat Enterprise Linux	7.4	x86_64
CentOS	6.9、7.7、8	x86、x86_64、ARM64
SUSE Linux Enterprise Server	11 SP4、12 SP3	x86_64
Ubuntu	14.04、16.04、18.04	x86_64、ARM64

上記の要件を満たすその他の**GNU/Linux**ディストリビューションについては、Dr.Web for UNIX File Serversとの互換性テストは行われていませんが、対応している場合があります。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。

ARM64アーキテクチャの場合、次の**GNU/Linux**ディストリビューションの互換性がテストされています。Ubuntu 18.04、CentOS 7.7、ALT Linux Workstation 9、ALT Linux Server 9。他のディストリビューションはまだテストされていませんが、サポートされる可能性があります。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。

• FreeBSD:

バージョン	プラットフォーム
11.2、12	x86、x86_64



FreeBSD OS の場合、Dr.Web for UNIX File Serversは [ユニバーサルパッケージ](#)からのみインストールできます。

追加のパッケージとコンポーネント

Dr.Web for UNIX File Serversでは、追加のパッケージやOSコンポーネントをインストールする必要はありません（保護されたサーバーソフトウェアを除く。以下を参照）。



[コマンドライン](#) でDr.Web for UNIX File Servers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自動補完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。

免責事項

- オペレーティングシステムのカーネルモード（LKMモジュール）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 *サポート対象ではありません*。**Xen**環境でのOS操作中にSpIDer Guardカーネ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。
- オペレーティングシステムのカーネルモード（LKMモジュール）でのSpIDer Guardの動作は、ARM64アーキテクチャでは *サポートされていません*。
- SpIDer Guardは、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する拡張（パラノイド）[モード](#)で動作できますが、それは、**fanotify**を介し、OSカーネルがアクティブな `CONFIG_FANOTIFY_ACCESS_PERMISSIONS` オプションで構築されている場合に *限ります*。

サポート対象のファイルサーバー

1. Sambaファイルサービス

Samba ファイルサービスと[統合](#)するには、インストールおよび設定されたファイルサーバー **Samba** が必要です（サポート対象のSambaバージョン: 3.6.0、4.0.0 - 4.10.0）



Dr.Web for UNIX File ServersのSpIDer Guard for SMBモジュールは、**Samba**サーバーとの統合に特別なVFS SMBモジュールを使用します。SpIDer Guard for SMBコンポーネントでは、このモジュールのいくつかのバージョンが提供されています。それらは**Samba**のさまざまなバージョン向けに構築されています。ただし、提供されているVFS SMBモジュールのバージョンが、サーバーにインストールされている**Samba**のバージョンと互換性がない場合があります。たとえば、**Samba**サーバーがCLUSTER_SUPPORTオプションを使用している場合に発生することがあります。

VFS SMBモジュールが**Samba**サーバーと互換性がない場合は、Dr.Web for UNIX File Serversの[インストール](#)中に**対応する**メッセージが表示されます。この場合、**Samba**サーバー用のVFS SMBモジュールを手動で構築します（必要に応じてCLUSTER_SUPPORTオプションとの互換性も含めます）。

提供されているソースコードファイルからVFS SMBモジュールを構築する手順は、[VFS SMBモジュールを構築する](#)セクションで説明されています。

2. NSSファイルサービス

NSSファイルサービスとの[統合](#)には、オペレーティングシステム**SUSE Linux Enterprise Server 10 SP3**以降に基づいてインストールおよび設定された**Novell Open Enterprise Server SP2**（11 SP1、SP2）が必要です。

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 UNIX File Serversは**SELinux**をサポートしていません。また、Dr.Web for UNIX File Servers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 UNIX File Serversのインストールが必要な場合、Dr.Web for UNIX File Serversの全機能が動作するように、セキュリティサブシステムの追加設定を実行する必要があります。詳細は、[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 UNIX File Serversを使用する権限は、Doctor Web社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。ユーザー権限を特定するライセンスパラメータは、Dr.Web for UNIX File Serversのインストール中にユーザーが同意するライセンス契約 (<https://license.drweb.com/agreement/>を参照) 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他、以下を含む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 UNIX File Serversライセンスの有効期間
- その他の制限 (購入した製品を使用できるコンピューターの台数など)。

評価目的のために、ユーザーは *試用期間* を有効化することもできます。有効化が成功すると、ユーザーは、有効化した試用期間全体にわたってDr.Web for UNIX File Serversの全機能を使用できます。

各Doctor Web製品ライセンスには、ユーザーのコンピューターに保存されている特別なファイルに関連付けられた一意のシリアル番号があります。このファイルは、ライセンスパラメータに従ってコンポーネントの動作を制限し、*ライセンスキーファイル*と呼ばれます。試用期間が有効になると、*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。

コンピューターでライセンスまたは試用期間が有効になっていない場合、Dr.Web for UNIX File Serversコンポーネントはブロックされます。さらに、ウイルスデータベースとコンポーネントの更新プログラムをDoctor Web更新サーバーからダウンロードすることもできません。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](#) の一部として製品を集中管理サーバーに接続することで、Dr.Web for UNIX File Serversを有効化することができます。この場合、アンチウイルス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 UNIX File Servers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 UNIX File Servers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 UNIX File Servers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 UNIX File Servers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 UNIX File Serversのインストールと動作に必要な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 UNIX File Serversをインストールする。](#)
- [Dr.Web for UNIX File Serversをアップグレードする。](#)
- [Dr.Web for UNIX File Servers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 UNIX File Serversパッケージとファイル。](#)
 - [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 UNIX File Serversと他社のアンチウイルス製品との互換性は *保証されません*。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 UNIX File Servers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。

お使いのコンピューターに他の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をインストールする場合（たとえば、ユニバーサルパッケージからDr.Web for Linuxをインストールしていて、さらににDr.Web for UNIX File Serversをインストールする場合など）、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Dr.Web for UNIX File Serversのバージョンと[同じ](#)であることを確認してください。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Dr.Web for UNIX File Serversを新しくインストールする製品のバージョンに[アップグレード](#)する必要があります。

FreeBSD OSの場合、Dr.Web for UNIX File Serversは[ユニバーサルパッケージ](#)からのみインストールできます。



Dr.Web for UNIX File Serversをインストールする

Dr.Web for UNIX File Servers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Webサイトから、UNIXシステム用の[ユニバーサルパッケージ](#)を含むインストールファイルをダウンロードします。パッケージには、1つのインストーラが含まれています（インストールプログラムはコマンドラインモード用に開発されているため、グラフィカルデスクトップモードで使用するには、使用可能なターミナルエミュレーターが必要です）。
2. Doctor Webの対応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。



FreeBSD OSの場合、Dr.Web for UNIX File Serversは[ユニバーサルパッケージ](#)からのみインストールできます。

インストール中（ユニバーサル.runパッケージまたはパッケージマネージャーを使用してネイティブパッケージから）、インストール結果を含むメッセージがroot@localhostに送信されます。

上記のいずれかの方法でDr.Web for UNIX File Serversをインストールした後、そのコンポーネントに利用可能な修正があるか、新しいDr.Web for UNIX File Serversバージョンがリリースされている場合は、[アンインストール](#)または[更新](#)できます。必要に応じて、Dr.Web for UNIX File Serversを正しく動作させるために、**GNU/Linux**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機能に問題がある場合は、Dr.Web for UNIX File Serversをアンインストールせずに、該当するコンポーネントの[カスタムインストールおよびアンインストール](#)を実行できます。

選択したDr.Web for UNIX File Serversのインストール方法に関係なく、インストールが完了したら、ライセンスを有効化して、受け取ったキーファイルをインストールする必要があります。さらに、Dr.Web for UNIX File Serversを集中保管サーバーに[接続](#)することもできます。詳細は、[ライセンス](#)を参照してください。これを行わない場合、アンチウイルス保護機能が無効になります。さらに、場合によっては、[開始する](#)セクションで説明されているように、インストールしたDr.Web for UNIX File Serversの基本機能をカスタマイズする必要があります。

ユニバーサルパッケージをインストールする

Dr.Web for UNIX File Serversユニバーサルパッケージは、drweb-*<version>*-av-srv-*<OS>*-*<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。ここで、*<OS>*は**UNIX**ベースのオペレーティングシステムのタイプ、*<Platform>*はDr.Web for UNIX File Servers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）です。例：

```
drweb-11.1-av-srv-linux-x86.run
```

上のフォーマットに該当するインストールファイルの名前は、このセクション以降では*<file_name>*.runと表記します。

Dr.Web for UNIX File Servers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. ユニバーサルパッケージを含むインストールファイルがない場合は、Doctor Webの公式Webサイト（<https://download.drweb.com/>）からダウンロードしてください。
2. インストールファイルをコンピューターのハードディスクドライブに保存します。
3. 次のコマンド（例）を使用してアーカイブを実行できるようにします。



```
# 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。



*Enclosed Software Environment*モードで動作する**Astra Linux SE**バージョン1.6のOSにインストールする場合は、Doctor Webのパブリックキーが信頼できるキーのリストにないため、インストールプログラムの起動に失敗することがあります。この場合は、*Enclosed Software Environment*モード([CSEモードでの起動を設定する\(Astra Linux SE 1.6\)](#)を参照)を事前に設定してから、インストールプログラムを再起動する必要があります。

これにより、アーカイブの整合性チェックが実行され、その後にアーカイブファイルが一時ディレクトリに展開され、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そのユーザーにrootパスワードを要求して権限を昇格させようとし(**sudo** が使用されます)。この試みが失敗した場合、インストールプロセスは停止します。



ファイルシステム内の一時ディレクトリへのパスに、展開されるファイル用の十分な空き容量がない場合、インストールプロセスが停止し、対応するメッセージが表示されます。この場合は、`TMPDIR`システム環境変数の値を、十分な空き容量があるディレクトリを指すように変更し、インストールをやり直してください。 -- `target` オプションを使用することもできます。

その後、[コマンドラインモード](#)用のインストーラが自動的に起動されます(グラフィカルデスクトップ環境で実行するには、ターミナルエミュレーターが必要です)。

5. インストーラの指示に従ってください。
6. 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ー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と、Dr.Webライセンス契約の規定に同意することになります。ライセンス契約のテキストは、`/opt/drweb.com/share/doc/LICENSE`ファイルにあります。ファイル拡張子は、ライセンス契約の言語を示しています。ライセンスファイルに拡張子がない場合、Dr.Webライセンス契約は英語で記述されています。ライセンス契約の条件に同意しない場合は、インストール後にDr.Web for UNIX File Serversを[アンインストール](#)してください。
- アン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** および **sudo** コマンドを使用できます。



使用しているGNU/LinuxディストリビューションがSELinuxを備えている場合、インストールプロセスがセキュリティサブシステムによって中断される可能性があります。このような場合は、SELinuxをPermissiveモードに設定してください。これを行うには、次のコマンドを入力します。

```
# 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。

<opt_dir>、<etc_dir>、<var_dir>の表記規則の詳細は、はじめにを参照してください。

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。



<file_name>.runファイル（インストール元のファイル）を保存しておくことを推奨します。これにより、バージョンの更新を必要とせずにDr.Web for UNIX File Serversやそのコンポーネントを再インストールすることが可能になります。

コマンドラインからインストールする

コマンドラインベースのインストールプログラムを起動すると、製品をインストールするように促すメッセージが表示されます。

1. インストールを開始するには、「Do you want to continue?」に対して「Yes」または「Y」を入力します。インストーラを終了するには、「No」または「N」と入力します。この場合、インストールはキャンセルされます。
2. その後、画面に表示されているDr.Webライセンス契約の規約を確認する必要があります。Enterキーを押してテキストを1行ずつ下にスクロールするか、またはSpaceキーを押してテキストを1画面ずつ下にスクロールします。ライセンス契約を上スクロールするオプションはありません。
3. ライセンス契約のテキストを読んだ後、規約に同意するように求められます。ライセンス契約に同意する場合は、YesまたはYを入力します。同意しない場合は、NoまたはNを入力します。後者の場合、インストーラは終了します。
4. ライセンス契約の規約に同意すると、インストールが自動的に開始されます。手順の実行中、インストールされるDr.Webコンポーネントの一覧を含むインストールプロセス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、Dr.Web for UNIX File Serversの動作を管理する方法を通知するメッセージが表示されます。

エラーが発生した場合は、エラーについて説明するメッセージが画面に表示された後、インストーラが終了します。インストールがエラーによって失敗した場合、エラーの原因を取り除き、インストール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 UNIX File Serversのネイティブパッケージは<https://repo.drweb.com/>にあるDr.Webの公式リポジトリに保存されています。お使いのOSのパッケージマネージャーが使用するリポジトリのリストにDr.Webリポジトリを追加すると、OSのリポジトリから他のプログラムをインストールするのと同じようにネイティブパッケージから製品をインストールできます。必要な依存関係は自動的に解決されます。



以下で説明するコマンド(リポジトリの追加、デジタル署名キーのインポート、パッケージのインストールと削除に使用するコマンド)はすべて、スーパーユーザー(**root**)管理者権限で実行する必要があります。管理者権限を昇格するには、(現在のユーザーを変更する)**su**コマンド、または(他のユーザーの管理者権限で指定したコマンドを実行する)**sudo**コマンドを使用します。

FreeBSD OS の場合、Dr.Web for UNIX File Serversは ユニバーサルパッケージ からのみインストールできます。

以下のOS(パッケージマネージャー)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 http://repo.drweb.com/drweb/debian 11.1 non-free
```



1および2の項目は、リポジトリから特別なDEBパッケージ (<https://repo.drweb.com/drweb/drweb-repo11.1.deb>) をダウンロードしてインストールすることでも実行できます。

3. リポジトリから Dr.Web for UNIX File Servers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-file-servers
```

代替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** などの代替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 http://repo.drweb.com/drweb/altlinux 11.1/ <arch> drweb
```

<arch>は、使用されるパッケージ構造を表します。

- **32-bit**バージョン:i386
- **64-bit**バージョン:x86_64
- **ARM64**アーキテクチャの場合:aarch64

2. リポジトリから Dr.Web for UNIX File Servers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-file-servers
```

代替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>は、使用されるパッケージ構造を表します。

- **32-bit**バージョン:i386
- **64-bit**バージョン:x86_64

2. リポジトリから Dr.Web for UNIX File Servers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-file-servers
```

代替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 (`\$`)。

項目 1 は、リポジトリから特別な RPM パッケージ (<https://repo.drweb.com/drweb/drweb-repo11.1.rpm>) をダウンロードしてインストールすることでも実行できます。

2. リポジトリから Dr.Web for UNIX File Servers 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-file-servers
```

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-file-servers
```

代替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. リポジトリを追加するには、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 UNIX File Servers 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-file-servers
```

代替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 UNIX File Servers をアップグレードする

Dr.Web for UNIX File Servers 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. Dr.Web for UNIX File Servers の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 UNIX File Servers の新しいバージョンを Doctor Web がリリースし、それに新しい機能が備わっている場合に使用されます。



最新のアップデートを入手する

[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 UNIX File Servers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て（たとえば、**Debian**、**Mint**、**Ubuntu**などのOS）、OS（**FreeBSD**）にパッケージマネージャーがない場合、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 UNIX File Servers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
```



FreeBSD OS v.11.x for amd64では、更新に**zypper**マネージャーを使用すると、リポジトリアップデートエラーが発生する場合があります。この場合、compat10x-amd64サポートパッケージをインストールして、再試行してください。

パッケージをインストールするには、次のコマンドを使用します。

```
# pkg install compat10x-amd64
```

- 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を更新する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 UNIX File Serversバージョンがリリースされると、そのコンポーネントを含むパッケージは、新しいバージョンに対応するDr.Webリポジトリのセクションに配置されます。この場合、更新には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](#)を参照）。

新しいバージョンにアップグレードする

このセクションの内容：

- [注意事項](#)
- [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](#)
- [リポジトリからアップグレードする](#)



- [キーファイルの転送](#)
- [集中管理サーバーとの接続を復元する](#)

注意事項



新しいバージョンにアップグレードする前に、サーバーが新しいバージョンの[システム要件](#)を満たしていることを確認してください。これには、必要なプログラムがインストールされていることを含みます。

お使いのバージョンのDr.Web for UNIX File Serversは、製品のインストール時と同じ方法でアップグレードする必要があります。

- Dr.Web for UNIX File Serversの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のプログラムパッケージを更新する必要があります。
- Dr.Web for UNIX File Serversの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、Dr.Web for UNIX File Serversをアップグレードするには、新しいバージョンの製品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。



製品バージョンのインストール方法を特定するには、Dr.Web for UNIX File Serversの実行可能ディレクトリに`uninst.sh`のアンインストールスクリプトが含まれているかどうかを確認します。その場合、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。

FreeBSD OSの場合、Dr.Web for UNIX File Serversは[ユニバーサルパッケージ](#)からのみインストールできます。

インストールに使用した方法でDr.Web for UNIX File Serversを更新できない場合は、現在のバージョンのDr.Web for UNIX File Serversをアンインストールしてから、何ら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 UNIX File Serversのインストールおよびアンインストール手順は、バージョン11.1向けの本マニュアルにある[インストール](#)および[アンインストール](#)と同じです。追加情報については、最新バージョンのDr.Web for UNIX File Serversのユーザーマニュアルを参照してください。

現在のバージョンのDr.Web for UNIX File Serversが[集中管理](#)モードで動作している場合は、使用されている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 UNIX File Servers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`)。また、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、お使いのバージョンのDr.Web for UNIX File Servers用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。



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

[ユニバーサルパッケージ](#)からDr.Web for UNIX File Servers 11.1をインストールします。自動更新が不可能な場合は、新しいバージョンのインストール中に、コンピューターにインストールされているDr.Web for UNIX File Serversの古いバージョンのコンポーネントを自動的に削除するメッセージが表示されます。



更新中に、インストールされたDr.Web for UNIX File Serversバージョンを削除する必要があります。Dr.Webの複数のサーバー製品（ファイルサーバー用、メールサーバー用、インターネットゲートウェイ用などの製品）がお使いのサーバーに一緒にインストールされている場合、アップグレードされない他のサーバー製品を完全に機能させるために（すなわち、メールサーバー用およびインターネットゲートウェイ用の製品を維持するために）、削除対象として以下のパッケージのみを選択する必要があります。

- drweb-file-servers-doc
- drweb-samba-web
- drweb-smbspider

リポジトリからアップグレードする



Dr.Webバージョン6.0.2の複数のサーバー製品がお使いのサーバーに一緒にインストールされている場合（ファイルサーバー用製品、メールサーバー用製品、インターネットゲートウェイ用製品がインストールされている場合など）、Dr.Web for UNIX File Servers 6.0.2をリポジトリからバージョン11.1にアップグレードすることはできません。この場合は、新しいバージョンのDr.Web for UNIX File Serversを別のマシンにインストールしてください。

Doctor Web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 UNIX File Servers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、dnf)。

1. 使用する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）。



[リポジトリからインストールする](#)セクションで、11.1パッケージが保存されているリポジトリの名前を確認できます。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 UNIX File Serversをアンインストールして、再度インストールしてください。必要に応じて、[セクションリポジトリからインストールしたDr.Web for UNIX File Servers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および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**)。

1. 使用する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 UNIX File Servers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 UNIX File Serversのアップグレード方法に関係なく、すでにあるライセンス[キーファイル](#)（お持ちの場合）は自動的に転送され、新しいバージョンで必要な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](#)できます。

有効なライセンスキーファイルを紛失した場合は、[テクニカルサポート](#)に連絡してください。

集中管理サーバーとの接続を復元する

可能であれば、アップグレード後に集中管理サーバーへの接続が自動的に復元されます（アップグレード前に製品が集中管理サーバーに接続されていた場合）。接続が自動的に復元されなかった場合は、アップグレードしたDr.Web for UNIX File Serversのアンチウイルスネットワークへの接続を再度確立するために、次の[コマンド](#)を実行します。

```
$ drweb-ctl esconnect <アドレス> --Certificate <証明書ファイルへのパス>
```

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。

Dr.Web for UNIX File Serversをアンインストールする

Dr.Web for UNIX File Servers 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. [アンインストーラを起動](#)して、ユニバーサルパッケージをアンインストールします。



2. システムのパッケージマネージャーを使用して、Doctor Webの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](#)します。



Dr.Web for UNIX File Serversをアンインストールした後、SambaサーバーのディレクトリからDr.Webの**VFS**モジュールへのシンボリックリンクを手動で削除し、共有ディレクトリを記述する各セクションから次の行を削除して**Samba**(`smb.conf`)の設定ファイルを編集します。
`vfs objects = smb_spider(smb_spiderはDr.WebのVFS SMBEジュールへのシンボリックリンクの名前です)。`

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](#)からインストールされたDr.Web for UNIX File Serversは、コマンドラインからアンインストールできます(このオプションでは、グラフィカルデスクトップ環境を使用している場合、端末エミュレーターが必要です)。



アンインストールツールはDr.Web for UNIX File Servers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 UNIX File Servers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態でDr.Web for UNIX File Serversのみを削除するには、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。

コマンドラインからDr.Web for UNIX File Serversをアンインストールする

アンインストールツールは、`<opt_dir>/bin`ディレクトリ(**GNU/Linux**では`/opt/drweb.com/bin`)にある`uninst.sh`スクリプトによって起動されます。Dr.Web for UNIX File Serversのアンインストール手順については、セクション[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。

```
# env DRWEB_NON_INTERACTIVE=yes /opt/drweb.com/bin/uninst.sh
```

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** および **sudo** コマンドを使用できます。

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. 削除を開始するには、「Do you want to continue?」に対して「Yes」または「Y」を入力します。アンインストールを終了するには、「No」または「N」と入力します。この場合、Dr.Web製品の削除はキャンセルされます。



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 UNIX File Serversをアンインストールする

以下のOS(パッケージマネージャー)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 \(zypper\)](#)



パッケージのアンインストールにおいて、以下に記載されているすべてのコマンドは、スーパーユーザー(**root**)管理者権限を必要とします。管理者権限を昇格するには、(現在のユーザーを変更する)**su**コマンド、または(他のユーザーの管理者権限で指定したコマンドを実行する)**sudo**コマンドを使用します。

Debian、Mint、Ubuntu (apt)

Dr.Web for UNIX File Servers 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-file-servers
```

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:「*」)。

```
# apt-get remove drweb*
```

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. 最初のコマンドのケースでは、`drweb-file-servers`パッケージのみをアンインストールします。このパッケージの依存関係を解決するのに自動的にインストールされた可能性のある他のパッケージはシステムに残ります。
2. 2番目のコマンドのケースでは、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 UNIX File Servers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番目のコマンドのケースでは、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、依存パッケージのアンインストールなどにより不要になった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 UNIX File Servers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。

代わりのマネージャー(**Synaptic** または **aptitude** など)を使用して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 UNIX File Servers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](#)を参照)。

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

Mageia、OpenMandriva Lx(**urpme**)

Dr.Web for UNIX File Servers 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-file-servers
```

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-file-servers
```



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. 最初のコマンドのケースでは、`drweb-file-servers`パッケージのみをアンインストールします。このパッケージの依存関係を解決するのに自動的にインストールされた可能性のある他のパッケージはシステムに残ります。
2. 2番目のコマンドのケースでは、`drweb-file-servers`パッケージと、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、依存パッケージのアンインストールなどにより不要になった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 UNIX File Servers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。

代わりのマネージャー(**rpmdrake**など)を使用して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。

このコマンドのケースでは、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 UNIX File Servers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。

代替のマネージャー(**PackageKit** または **Yumex** など)を使用して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 UNIX File Servers 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-file-servers
```

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. 最初のコマンドのケースでは、drweb-file-serversパッケージのみをアンインストールします。このパッケージの依存関係を解決するのに自動的にインストールされた可能性のある他のパッケージはシステムに残ります。
2. 2番目のコマンドのケースでは、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 UNIX File Servers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。

代替のマネージャー(**YaST** など)を使用して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 UNIX File Serversパッケージとファイル

パッケージ

Dr.Web for UNIX File Serversは以下のパッケージで構成されています。

パッケージ	コンテンツ
drweb-bases	ウイルスデータベースファイル
drweb-boost	ブーストライブラリ
drweb-clamd	Dr.Web ClamDコンポーネントのファイル
drweb-cloudd	Dr.Web CloudDコンポーネントのファイル
drweb-common	メインの設定ファイル - drweb.ini、メインライブラリ、ドキュメント、Dr.Web for UNIX File Serversディレクトリの階層、製品設定とシステム環境に関する情報を収集するためのユーティリティ。 このパッケージのインストール中に、drwebという名前のユーザーとdrwebという名前のグループが作成されます。
drweb-configd	Dr.Web ConfigDファイル
drweb-configure	Dr.Web for UNIX File Servers設定用の補助ツールのファイル
drweb-ctl	Dr.Web Ctlファイル
drweb-documentation	HTMLフォーマットのDr.Web for UNIX製品ドキュメントファイル
drweb-engine	Dr.Web Virus-Finding Engineスキャンエンジンファイル
drweb-esagent	Dr.Web ES Agentコンポーネントのファイル
drweb-filecheck	Dr.Web File Checkerコンポーネントのファイル
drweb-file-servers-doc	PDFドキュメント
drweb-file-servers	Dr.Web for UNIX File Serversのルートメタパッケージ
drweb-httpd	Dr.Web HTTPDコンポーネントと管理Webインターフェース(メタパッケージ)のファイル
drweb-httpd-bin	Dr.Web HTTPDコンポーネントのファイル
drweb-httpd-webconsole	管理Webインターフェースのファイル
drweb-icu	Unicodeサポートとインターナショナルライゼーションのためのライブラリ



パッケージ	コンテンツ
drweb-libs	メインライブラリファイル
drweb-netcheck	Dr.Web Network Checkerコンポーネントのファイル
drweb-nss	SpIDer Guard for NSSコンポーネントのファイル
drweb-openssl	OpenSSL ライブラリ
drweb-protobuf	Google Protobuf ライブラリ
drweb-se	Dr.Web Scanning Engineコンポーネントのファイル
drweb-smbspider-daemon	SpIDer Guard for SMBコンポーネントのファイル (SMBモニタリングデーモン)
drweb-smbspider	SpIDer Guard for SMBコンポーネントのファイル
drweb-smbspider-modules	SpIDer Guard for SMBコンポーネントのファイル (VFS SMBモジュール)
drweb-smbspider-modules-src	SpIDer Guard for SMBコンポーネントのファイル (VFS SMBモジュールのソースコード)
drweb-snmpd	Dr.Web SNMPDコンポーネントのファイル
drweb-spider	SpIDer Guardコンポーネントのファイル
drweb-spider-kmod	<i>Linux</i> モードでSpIDer Guardを動作するための GNU/Linux カーネルモジュールのファイル
drweb-update	Dr.Web Updaterコンポーネントのファイル

セクション[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](#)には、Dr.Web for UNIX File Serversの典型的なタスクに対する解決策を提供するカスタムインストール用の典型的なコンポーネントセットがあります。

ファイル

Dr.Web for UNIX File Servers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。

使用されるディレクトリの構造

ディレクトリ	コンテンツ
<ul style="list-style-type: none">• GNU/Linuxの場合： /etc/init.d/• FreeBSDの場合： /usr/local/etc/rc.d/	Dr.Web ConfigDデーモン用のdrweb-configdスクリプト。
<etc_dir>	drweb.ini設定ファイルとdrweb32.keyキーファイル。また、次が含まれます。



ディレクトリ	コンテンツ
certs/	– 使用中の証明書のファイル。
<opt_dir>/	Dr.Web for UNIX File Serversのメインディレクトリ。次が含まれます。
bin/	– 全製品のコンポーネントの実行ファイル (Dr.Web Virus-Finding Engineを除く)。
include/	– 使用中のライブラリのヘッダーファイル。
lib/	– 使用中のライブラリ。
man/	– システムヘルプファイル: man 。
share/	– 次を含む補助製品ファイル。
doc/	▫ 製品ドキュメント (readmeファイル、ライセンス契約)、パッケージがすでにインストールされている場合は管理者ガイド)。
drweb-bases/	▫ Dr.Webのウイルスデータベースのファイル (インストール中に提供されたソースファイル)。
drweb-spider-kmod/	▫ SpIDer Guard (手動作成のソースコード) を動作するためのカーネルモジュールのファイル。
scripts/	▫ 補助スクリプトファイル。
<var_dir>/	以下を含む補助ファイルと一時ファイル:
bases/	– Dr.Webウイルスデータベースのファイル (更新バージョン)。
cache/	– 更新のキャッシュ。
drl/	– 使用中の更新サーバーのリスト。
dws/	– Webリソースカテゴリーのデータベースのファイル。
lib/	– ダイナミックリンクライブラリとしてのDr.Web Virus-Finding Engineスキャンエンジン (drweb32.dll) と、集中管理モードで作業するための設定。
update/	– ダウンロード中に更新を一時的に保存するためのディレクトリ。

ディレクトリで使用される文字・記号の詳細については、[はじめに](#)を参照してください。

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Dr.Web for UNIX File Servers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。カスタムコンポーネントのインストールまたはアンインストールは、製品のインストールと同じ方法で実行します。

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。

- [カスタムインストール用の一般的なコンポーネントキット](#)。



- Dr.Web for UNIX File Servers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](#)

カスタムインストール用の一般的なコンポーネントキット

[リポジトリ](#)または[ユニバーサルパッケージ](#)からルートメタパッケージをインストールする代わりに、機能を制限してDr.Web for UNIX File Serversをインストールする必要がある場合は、必要な機能を提供するコンポーネントパッケージのみをインストールできます。依存関係を解決するために必要なパッケージは自動的にインストールされます。以下の表は、一般的なDr.Web for UNIX File Serversタスクを解決するために設計されたコンポーネントセットを示しています。インストールするパッケージ列には、特定のコンポーネントスイートを取得するためにインストールする必要があるパッケージのリストがあります。

カスタムコンポーネントキット	インストールするパッケージ	インストールされるコンポーネント
コンソールスキャンのための最小キット	drweb-filecheck	<ul style="list-style-type: none">• Dr.Web Ctl• Dr.Web ConfigD• Dr.Web Scanning Engine• Dr.Web File Checker• Dr.Web Updater• ウイルスデータベース
GNU/Linux のファイルシステムをモニタリングするためのスイート	drweb-spider	<ul style="list-style-type: none">• Dr.Web Ctl• Dr.Web ConfigD• Dr.Web Scanning Engine• Dr.Web File Checker• Dr.Web Updater• SpIDer Guard• ウイルスデータベース
Samba 共有ディレクトリをモニタリングするためのスイート	drweb-smbspider	<ul style="list-style-type: none">• Dr.Web Ctl• Dr.Web ConfigD• Dr.Web Scanning Engine• Dr.Web File Checker• Dr.Web Updater• SpIDer Guard for SMB• ウイルスデータベース
NSS ボリュームをモニタリングするためのスイート	drweb-nss	<ul style="list-style-type: none">• Dr.Web Ctl• Dr.Web ConfigD• Dr.Web Scanning Engine• Dr.Web File Checker• Dr.Web Updater• SpIDer Guard for NSS• ウイルスデータベース



カスタムコンポーネントキット	インストールするパッケージ	インストールされるコンポーネント
ClamAV のエミュレーションのためのスイート (clamd)	drweb-clamd	<ul style="list-style-type: none">• Dr.Web Ctl• Dr.Web ConfigD• Dr.Web Scanning Engine• Dr.Web File Checker• Dr.Web Network Checker• Dr.Web Updater• Dr.Web ClamD• ウイルスデータベース

リポジトリからインストールされたDr.Web for UNIX File Servers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 UNIX File Servers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 UNIX File ServersからDr.Web ClamD(drweb-clamd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-clamd
```

2. **Ubuntu**にインストールされているDr.Web for UNIX File ServersにDr.Web ClamD(drweb-clamd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-clamd
```

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。

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 UNIX File Servers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 UNIX File Servers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 UNIX File Servers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Web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 UNIX File Servers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 UNIX File Servers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 UNIX File Servers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。

.runファイルの起動時に指定できるコマンドラインパラメータの一覧を表示するには、以下のコマンドを入力します。

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

カスタムインストールでは、展開されたインストールファイルを使う必要があります。それらのファイルが含まれたディレクトリがない場合、初めに展開します。その際、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、ディレクトリ `<directory>` 内に、ネストされたディレクトリの名前 `<file_name>` 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 UNIX File Servers 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、`<platform>` はDr.Web for UNIX File Serversが対象としているプラットフォームです。Dr.Web for UNIX File Servers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。

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` を使用する必要があります。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 **su** 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-clamd
```



Dr.Web for UNIX File Servers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 UNIX File Serversパッケージをインストールできます（欠けているか、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-file-servers
```

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-clamd
```

お使いのOSがDEBパッケージを使用している場合（**MSVS 3.0** OSを使用している場合も）、またはOSにパッケージマネージャーがない場合（**FreeBSD**）、カスタムアンインストールでは、Dr.Web for UNIX File Servers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。これを行うには、<opt_dir>/bin（**GNU/Linux**の場合は/opt/drweb.com/bin）ディレクトリに移動して、以下のコマンドを実行します。

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

例：

```
# ./zypper remove drweb-clamd
```

Dr.Web for UNIX File Servers 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 UNIX File Serversとの動作に問題が生じます。この場合、Dr.Web for UNIX File Servers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 UNIX File Servers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 UNIX File Serversを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**）



Dr.Web for UNIX File Servers に対する **PARSEC** 強制アクセス制御システムのパーミッションを設定することで、Dr.Web for UNIX File Servers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 UNIX File Serversの**PARSEC**強制アクセス制御システムのパーミッションをまだ設定していない場合は、引き続き**コマンドライン**から直接ファイルのスキャンを起動できます。これを行うには、コマンドの呼び出しで**--Autonomous**オプションを指定して、自律モードで**drweb-ctl****コマンド**を使用します。この方法でスキャンを開始すると、スキャンを開始したユーザーの権限を越えない権限でアクセスできるファイルだけをスキャンできます。このモードにはいくつかの機能があります。

- 自律コピーを実行するには、有効な**キーファイル**が必要です。**集中管理**モードでの作業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**することはできます）。この場合、Dr.Web for UNIX File Serversが集中管理サーバーに接続されていても、自律コピーは、自律コピーモードで検出された脅威を集中管理サーバーに通知しません。
- 自律コピーの機能をサポートするすべ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、特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）。
- 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、スキャン中に使用される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、または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は制限されません。
- 自律コピーが終了すると、一連のサポート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

GNU/Linuxディストリビューションに**SELinux**（*Security-Enhanced Linux*）が含まれている場合は、インストール後にDr.Web for UNIX File Serversのサービスコンポーネント（**スキャンエンジン**など）を正常に動作させるために、**SELinux**のセキュリティポリシーを設定することが必要になる場合があります。



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 UNIX File Servers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いためにファイルからのDr.Web for UNIX File Serversのインストールが失敗する場合は、**getenforce**コマンドを使用して**SELinux**の動作モードを確認してください。このコマンドは、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 UNIX File Servers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 UNIX File Serversの動作に関する問題

SELinuxの実行中にいくつかのDr.Web for UNIX File Serversコンポーネント(**drweb-se**や**drweb-filecheck**など)が起動できないことがあります。これにより、オブジェクトのスキャンやファイルシステムのモニタリングが不可能になります。これらのコンポーネントが起動できない場合は、**syslog**サービスによって管理されるシステムログ(通常このログは `/var/log` ディレクトリにあります)に *119*および *120*エラーメッセージが表示されます。

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`)に保存されません。

SELinuxにブロックされているために製品のスキャンコンポーネントが機能しない場合は、コンポーネント用の特別な**セキュリティポリシー**を設定する必要があります。



一部の **GNU/Linux** ディストリビューションには、下記のユーティリティがありません。その場合は、これらのユーティリティを備えた追加パッケージのインストールが必要になる場合があります。

SELinux セキュリティポリシーを設定するには以下の手順を行ってください。

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 UNIX File Servers のコンポーネントが **SELinux** の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 (**Red Hat Enterprise Linux**、**CentOS**、**Fedora**、バージョンによる)、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** コンポーネント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 `/var/log/audit/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 UNIX File Servers 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。そのためには、異なる方法で処理するコンポーネントの名前とその実行ファイルへのフルパスを指定します。



Red Hat Enterprise Linux と **CentOS Linux** 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** コンポーネントの場合:



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

• **drweb-filecheck**コンポーネントの場合:

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

ドメインを作成するための一般的なプロパティをいくつか指定するように求められます。その後、ポリシーを決定する以下の3つのファイルが(コンポーネントごとに)作成されます。

<module_name>.te、<module_name>.fc、<module_name>.if。

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**Linux**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(Astra Linux SE)パーミッションの設定

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)を備えたOSでは、アクセスするために必要な権限レベルがファイルによって異なるため、SpIDer Guardは、デフォルトでは、SpIDer Guardが実行されている権限レベルよりも高い権限レベルを持つファイルへのアクセスに関するイベントを監視できません。さらに、ユーザーが0番目以外の権限レベルで作業している場合、Dr.Web for UNIX File Serversのグラフィカルインターフェースは、SpIDer Guardや、異なる権限レベルで動作しているアンチウイルスサービスコンポーネントとやり取りできません。統合された**隔離**にもアクセスできない可能性があります。

PARSECがOSで使用されており、0番目以外の権限レベルで作業しているユーザーアカウントが存在する場合は、Dr.Web for UNIX File Serversをカスタマイズし、その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する必要があります。



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

- ユーザー権限を使用し、Dr.Web for UNIX File Servers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できるように[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。

ユーザー権限を使用し、Dr.Web for UNIX File Serversコンポーネントの自動起動をカスタマイズする

ユーザーがやり取りするDr.Web for UNIX File Serversコンポーネントをユーザー環境で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作業している場合)、必要なDr.Web for UNIX File Serversコンポーネントがユーザーセッションの開始時に自動起動し、セッションの終了時に終了するように、PAM設定を含むファイルを変更する必要があります。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** 仲介コンポーネントを起動します。このコンポーネントは、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番目の権限レベルで動作していて、OSのロード時に自動的に実行されるコンポーネントを結び付けます。

PAM設定を変更するには、Dr.Web for UNIX File Servers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 UNIX File Servers 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 UNIX File Serversコンポーネントが0以外の特権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 UNIX File Servers 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。

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



2. PAM設定ファイルを手動で変更する

1. **pam_parsec_mac.so** PAMモジュールを起動するPAM設定ファイル(/etc/pam.dディレクトリ内)に、以下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 UNIX File Servers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。

ファイルアクセスイベントを監視できるように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)

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**に提供されているDr.Web for UNIX File Servers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 UNIX File Servers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のCSEモードでDr.Web for UNIX File Serversを起動するには、OSの設定が必要です。



Dr.Web for UNIX File ServersをCSEモードで起動するようAstra Linux SE 1.6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）。
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. インストールされたDr.Web for UNIX File Serversの使用を開始するために、[キーファイル](#)を入手してインストールした上で[有効化](#)する必要があります。
2. Dr.Web for UNIX File Serversの[操作性](#)をさらにスキャンすることをお勧めします。
3. Dr.Web for UNIX File Serversを、必要なファイルサービスと統合します([Samba](#)または[NSS](#)のマニュアルをご覧ください)。
4. 必要に応じて、NSSボリューム外およびSamba共有ディレクトリ外のGNU/Linuxファイルシステムオブジェクトの[監視パラメータを設定します](#)。
5. サーバーの保護に必要な場合には、どのコンポーネントが実行されているかを確認し、追加のコンポーネントを有効にします(ディストリビューションに依存しますが、[SpIDer Guard](#)、[Dr.Web ClamD](#)、[Dr.Web SNMPD](#)等)。追加コンポーネントを有効にすること以外に、他のアクションを実行する必要がある場合があります。たとえば、デフォルトの設定を調整する必要があります。インストール済みおよび実行中のコンポーネントとその設定の一覧を表示するには、次のいずれかを使用します。
 - [コマンドラインベースの管理ツール](#)-Dr.Web Ctl(`drweb-ctl appinfo`、`drweb-ctl cfshow`、`drweb-ctl cfset`コマンドを使用します)。
 - Dr.Web for UNIX File Serversの管理用[ウェブインターフェース](#)(初期設定では、ウェブブラウザから<https://127.0.0.1:4443/>にアクセスすると利用できます)。

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](#)
- [デモライセンスを取得する](#)
- [キーファイルのインストール](#)
- [2回目以降の登録](#)

ライセンスを購入・登録する

ライセンスを購入すると、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。さらに、購入した製品をインストールまたは使用するとき問題が発生した場合は、Doctor Webまたはそのパートナーが提供するテクニカルサポートサービスを利用できます。

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](#)または[オンラインストア](#)から可能です。ライセンスオプションの詳細については、Doctor Web公式Webサイト(<https://license.drweb.com/>)にアクセスしてください。

ライセンス登録は、ユーザーがDr.Web for UNIX File Servers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定期的な更新を含むアンチウイルスの機能を有効にするために必要です。インストールが完了したら、製品を登録してライセンスを有効化することを推奨します。購入したライセンスは、Doctor Webの公式Webサイト(<https://products.drweb.com/register/>)で有効化できます。

有効化の際には、購入したライセンスの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 UNIX File Servers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。



これまでに製品を使用したことがある場合は、新しいライセンスに対して150日間の延長ボーナスを利用できます。このボーナスを有効にするには、登録済みのシリアル番号を入力するか、ライセンスキーファイルを提供します。

複数のサーバー上で Dr.Web for UNIX File Servers を使用するための複数のライセンスがあり、製品を1台のサーバーでのみ使用することを選択した場合、それを指定することができ、ライセンス有効期限は自動的に延長されます。

デモライセンスを取得する

ご利用のDr.Web for UNIX File Serversの試用期間は、Doctor Webの公式Webサイト (<https://download.drweb.com/demoreq/biz/>) で確認できます。製品を選択して登録フォームに記入すると、Dr.Web for UNIX File Serversを有効化するためのシリアル番号またはキーファイルが記載されたメールが届きます。



同じコンピューターでの2回目以降の試用期間は、一定の期間が経過した後に利用できます。

Dr.Web Ctl (drweb-ctl) コマンドラインツールのライセンスコマンドを使用すると、登録されたライセンスのシリアル番号のデモキーファイルまたはライセンスキーファイルを自動的に取得できます。

キーファイルのインストール

キーファイルは、Dr.Web for UNIX File Servers 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。



Dr.Web for UNIX File Serversの動作中、キーファイルはデフォルトの `<etc_dir>` (**GNU/Linux**の場合は `/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 UNIX File Servers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。改竄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ー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(正規またはデモライセンス)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管しておき、Dr.Web for UNIX File Serversの再インストールや、別のコンピューターへのインストールにはそのキーを使用することを推奨します。この場合、登録時に指定したのと同じ製品シリアル番号と顧客データを使用する必要があります。



メールメッセージでは、Dr.Webキーファイルは通常、zipアーカイブに圧縮されて転送されます。Dr.Web for UNIX File Serversアクティベーション用のキーファイルを含むアーカイブは、通常は `agent.zip` という名前です（メッセージに複数のアーカイブが含まれている場合は、`agent.zip` アーカイブを使用する必要があります）。キーファイルをインストールする前に、アーカイブを適宜解凍し、そこからキーファイルを抽出して、使用可能な任意のディレクトリ（たとえば、ホームディレクトリやUSBフラッシュドライブ）に保存してください。

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 UNIX File Serversを別のサーバ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 UNIX File Serversを有効化できます。その場合は、次の操作を行います。

1. アーカイブの場合はキーファイルを展開します。
2. 次のいずれかを実行してください：
 - キーファイルを `<etc_dir>` 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。
 - Dr.Web for UNIX File Servers [設定ファイル](#) で、`KeyPath` パラメータ値にキーファイルパスを指定します。
3. 次の [コマンド](#) を入力して、Dr.Web for UNIX File Serversの設定をリロードします。

```
# 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、Dr.Web for UNIX File Serversの再起動は不要です。キーファイルは `<etc_dir>` ディレクトリにコピーされず、元の場所に残ります。



`<opt_dir>`、`<etc_dir>`、`<var_dir>` の表記規則の詳細は、[はじめに](#) を参照してください。

キーファイルが `<etc_dir>` ディレクトリにコピーされない場合は、ユーザーはファイルが破損や削除から保護されていることを確認する必要があります。キーファイルがシステムから誤って削除される可能性があるため、この方法は推奨されません（たとえば、キーファイルが存在するディレクトリが定期的にクリーンアップされる場合）。キーファイルを紛失した場合は、サポートを要求して新しいファイルを取得できますが、要求できる回数には制限があります。

2回目以降の登録

キーファイルを紛失したが、既存のライセンスの有効期限が切れていない場合は、前回の登録時に指定した個人データを入力して、再度登録する必要があります。別のメールアドレスを使用できます。この場合、ライセンス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。

キーファイルをリクエストできる回数は制限されています。1つのシリアル番号は **最大25回** まで登録できます。その数を超えてリクエストが送信された場合、キーファイルは配信されません。紛失したキーファイルを入手するには、



Doctor Web [テクニカルサポート](#)に連絡して問題の詳細を説明し、シリアル番号の登録時に入力した個人データを伝えてください。ライセンスキーファイルはメールで送信されます。

キーファイルがメールで送信されたら、手動で[インストール](#)する必要があります。

製品の動作確認

EICAR (European Institute for Computer Anti-Virus Research) テストは、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、大多数のアンチウイルスによってウイルスのように扱われます。この「ウイルス」を検出すると、Dr.Web アンチウイルス製品は **EICAR Test File (NOT a Virus!)** を報告します。他のアンチウイルスツールも同様にユーザーに警告します。**EICAR** テストファイルは、実行時に端末画面またはコンソールエミュレーターに次の行を出力する **MS DOS/MS Windows** 用の 68 バイトの COM ファイルです。

```
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 UNIX File Servers 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!)**

コマンドラインから **EICAR** テストを使用して Dr.Web for UNIX File Servers の動作を確認するコマンドの例:

```
$ tail <opt_dir>/share/doc/drweb-se/readme.eicar | grep X5O > testfile &&  
drweb-ctl rawscan testfile && rm testfile
```

このコマンドは、`<opt_dir>/share/doc/drweb-se/readme.eicar` ファイル (Dr.Web for UNIX File Servers に付属) から **EICAR** テストファイルの本文を表す文字列を抽出し、それを現在のディレクトリに作成された `testfile` という名前のファイルに書き込みます。次にこのファイルのスキャンし、その後で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)。

`<opt_dir>`、`<etc_dir>`、`<var_dir>` の表記規則の詳細は、[はじめに](#) を参照してください。

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([付録F. 既知のエラー](#)を参照)。



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せん(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。

ファイルシステムモニタリングの設定

SpIDer Guardモニターを使用する**GNU/Linux**ファイルシステムモニタリングを設定するには、設定ファイルの[LinuxSpider] [設定](#)セクションにあるパラメータに値を指定します。

このセクションの内容:

- [メインファイルモニタリング設定](#)
- [ファイルモニタリングモードの切り替え](#)

メインファイルモニタリング設定

- モニターを有効にするには、**Start**値をYesに設定します。
- ファイルシステムモニターによる操作モードを**Mode**パラメータに指定します(Auto値を使用することをお勧めします)。
- 必要に応じて、**ExcludedProc**パラメータに、許可されたアプリケーション、つまりファイルへのアクセスがモニターによって制御され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します。
- 必要に応じて、**ExcludedFilesystem**パラメータに、モニターによってファイルが制御されないファイルシステムの名前(cifsなど)をリストします。
- 一連の保護スペースを指定してモニタリング範囲を指定します(保護スペースごとに別々のセクション[LinuxSpider.Space.<site name>]に指定します)。スペースごとに**Path**パラメータでモニタリングディレクトリへのパスを指定し、**Enable**値をYesに設定して、スペースをモニタリング範囲に追加します。
- **ExcludedPath**パラメータで(統合されたすべてのファイルシステムに対して、または各保護スペースに対して個別に)、除外範囲(モニタリング対象のオブジェクトおよびモニタリング対象から除外されるオブジェクトへのパスの一覧)を指定します。たとえば、一部のパスがファイルサーバー**Samba**によって制御される場合や**NSS**ボリュームである場合は、さまざまなモニターによるスキャン中に競合が発生しないように、これらのパスを除外範囲に追加する必要があります。
- ファイルスキャンのパラメータと、さまざまな種類の脅威が検出されたときのモニターによるアクションを指定します(必要に応じて、モニタリング範囲内のすべての保護スペースに個別に指定します)。



ファイルモニタリングモードの変更



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、予備ブロックを含む拡張ファイルモニタリングモードを使用できます。

SpIDer Guardモードを切り替えるには、管理者（ルート）権限が必要です。そのためには、**su**コマンドを使用してユーザーを切り替えるか、**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。
- Dr.Web File Checkerがキャッシュに保存するスキャン結果を最新のものとして定義する期間を変更するには、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。

すべての設定を調整したら、Dr.Web for UNIX File Serversを再起動します（**コマンド** `drweb-ctl reload` を使用します）。設定デーモンDr.Web ConfigDを再起動することもできます（**service** `drweb-configd restart` コマンドを使用します）。



Sambaファイルサーバーとの統合



SpIDer Guard for SMBモジュールは、**Samba**サーバーとの統合に特別なVFS SMBモジュールを使用します。SpIDer Guard for SMBでは、このモジュールのいくつかのバージョンが提供されています。それらは**Samba**のさまざまなバージョン向けに構築されています。ただし、提供されているVFS SMBモジュールのバージョンが、ファイルサーバーにインストールされている**Samba**のバージョンと互換性を持たない場合があります。たとえば、**Samba**サーバーがCLUSTER_SUPPORTオプションを使用している場合に発生することがあります。

VFS SMBモジュールが**Samba**サーバーと互換性がない場合は、Dr.Web for UNIX File Serversのインストール中に**対応するメッセージ**が表示されます。この場合、**Samba**サーバー用のVFS SMBモジュールを手動で構築します（必要に応じてCLUSTER_SUPPORTオプションとの互換性も含めます）。

提供されているソースコードファイルからVFS SMBモジュールを構築する手順は、[VFS SMBモジュールを構築する](#)セクションで説明されています。

このセクションの内容：

- [Sambaとの統合のためのステップ](#)
- [統合サポートのシナリオ](#)
- [設定ツール](#)

Sambaとの統合のためのステップ

SpIDer Guard for SMBを**Samba**ファイルサーバーと統合するには、以下の手順に従います。

1. **Samba**が読み込むVFS SMBモジュールが置かれたディレクトリ（**GNU/Linux**のデフォルトディレクトリは`/usr/lib/samba/vfs`）に、使用しているバージョンの**Samba**に対応するDr.Web提供のVFS SMBモジュールを指すシンボリックリンク`smb_spider.so`を作成します。

Dr.Webが提供するVFS SMBモジュールは、以下のライブラリを含むディレクトリに保存されます。

- `<opt_dir>/lib/samba` - 32ビットプラットフォーム用。
- `<opt_dir>/lib64/samba` - 64ビットプラットフォーム用。

モジュールのファイル名は、`libsmb_spider.so.<ver>`のようになります。ここで、`<ver>`はモジュールの対象となる**Samba**サーバーのバージョンです。

たとえば、`/opt/drweb.com/lib/samba/libsmb_spider.so.3.6.0`であれば、**GNU/Linux**環境の32ビットプラットフォーム上で動作する**Samba**サーバーバージョン3.6.0用のVFS SMBモジュールになります。

このアクションは`update-links.sh`統合シナリオを使用して実行できます（[後述のセクションを参照](#)）。

2. **Samba**サーバー設定ファイル`smb.conf`（**GNU/Linux**のデフォルトの場所は`/etc/samba`）に、共有ディレクトリ用のセクションを作成します。次のようなセクションになります。



```
[ <share name>]
comment = <any comment>
path = <path to the protected directory>
vfs objects = smb_spider
writeable = yes
browseable = yes
guest ok = yes
public = yes
```

ここで、**<share name>**は共有リソースの任意の名前、**<any comment>**はコメントを含む任意の行になります（オプション）。**vfs**オブジェクトで指定するオブジェクトの名前はシンボリックリンクに類したものにします（ここでは**smb_spider**）。

そうすると、**path**パラメータで指定されたこのディレクトリは、SpIDer Guard for SMBによってモニタリングされます。SpIDer Guard for SMBとVFS SMBモジュールとのインタラクションは、UNIXソケット **/ <samba chroot path>/var/run/.com.drweb.smb_spider_vfs**を介して実行されます。デフォルトでは、このUNIXソケットへのパスはSpIDer Guard for SMB設定およびVFS SMBモジュール設定で指定されます。

drweb-configure 設定ツールを使用しSpIDer Guard for SMBを**Samba** サーバー設定ファイルでカスタマイズされた場所に接続できます（[後述のセクション](#)を参照）。

3. ソケットへのパスを変更する場合は、SpIDer Guard for SMBの**設定**（**SmbSocketPath**パラメータ）と**Samba**の設定ファイル**smb.conf**の両方で新しいパスを指定します。その場合、**[<share name>]**セクションに次の行を追加します。

```
smb_spider:socket = <path to socket>
```

ここで、**<path to socket>**は、UNIXソケットへの絶対パス、つまり**chroot**（**<samba chroot path>**）を使用して**Samba**サーバー用に設定されたルートディレクトリからの相対パスで指定します。

4. 必要に応じて、**ExcludedPath**および**IncludedPath**パラメータを使用して、保護された共有ディレクトリにあるオブジェクトへのパスを除外したり、SpIDer Guard for SMBによるチェックに含めたりできます。ディレクトリへのパスまたはファイルへのパスを指定できます。ディレクトリを指定した場合、そのディレクトリのコンテンツはすべてスキップまたはスキャンされます。**IncludedPath**パラメータは**ExcludedPath**パラメータよりも優先されます。つまり、同じオブジェクト（ファイルまたはディレクトリ）が両方のパラメータ値に含まれる場合、このオブジェクトは検査されます。
5. この共有ディレクトリに個人用のスキャン設定（すべての共有ディレクトリに使用されるデフォルト設定とは異なるもの）を指定する場合、このディレクトリを制御するVFS SMBモジュール用のタグIDを作成します。

```
smb_spider:tag = <share name>
```

次に、SpIDer Guard for SMB設定で、この共有ディレクトリを保護するための個人設定を**個別のセクション** **[SMBSpider.Share. <share name>]**として指定します。

<share name>タグで識別される新しいセクションを、Dr.Web Ctコマンドラインツールを使用して追加するには、たとえば次のようなコマンド**drweb-ctl cfset**

SmbSpider.Share. <share name>. <parameter> <value>を使用する必要があります。

```
# drweb-ctl cfset SmbSpider.Share.UserFiles.OnAdware Quarantine
```

このコマンドは、**[SMBSpider.Share.BuhFiles]**セクションを設定ファイルに追加します。この追加されたセクションには、この共有ディレクトリのスキャンを調整するために使用可能なすべてのパラメータが含まれ



ます。つまり、コマンドで指定される **OnAdware** パラメータを除くすべてのパラメータの値が、一般 [SMBSpider] [セクション](#)のパラメータ値と一致します。

6. **Start**パラメータを**Yes**に設定して、SpIDer Guard for SMBを有効にします。

すべての設定を調整したら、Dr.Web for UNIX File Serversと**Samba**サーバーの両方を再起動します([コマンドdrweb-ctl reload](#)を使用します)。設定デーモンDr.Web ConfigDを再起動することもできます(**service drweb-configd restart**コマンドを使用します)。



Sambaの共有ディレクトリにあるファイルをスキャンする際にSpIDer GuardとSpIDer Guard for SMBの間の競合を避けるために、次のいずれかの操作を実行して、SpIDer Guardの追加設定を行うことをお勧めします。

- **Samba**共有ディレクトリを除外パスに追加します(共有ディレクトリを**ExcludedPath**パラメータで指定)。
- **Samba**プロセス(**smbd**)を除外プロセスのリストに追加します(**ExcludedProc**パラメータに**smbd**を指定します)。

統合サポートのシナリオ

SpIDer Guard for SMBを**Samba**ファイルサーバーと簡単に統合するために、Dr.Web for UNIX File Serversには統合設定用の特別なシェルスクリプトが用意されています。それらは `<opt_dir>/share/drweb-smbspider-modules`にあります。

スクリプトファイル	機能
update-links.sh	Samba ディレクトリのDr.Web VFS SMBE ジュールへのリンクを作成/更新するスクリプト
vfs-versions.sh	Dr.Web VFS SMBE ジュールのバージョンを確認する補助スクリプト。update-links.shスクリプトによって使用されます。

update-links.shシェルスクリプトは、Dr.Web for UNIX File Serversのインストール中に自動的に起動されます。必要に応じて、後で、手動で起動することもできます。

設定ツール

SpIDer Guard for SMBをファイルサーバー設定ファイルでカスタマイズされた**Samba**共有ディレクトリとの統合(ディレクトリの接続と切断)を簡単に実行できるように、特別なツール**drweb-configure**が設計されました。SpIDer Guard for SMBと共有ディレクトリとの接続を設定するには、次のコマンドを使用します。

```
$ drweb-configure samba [<parameters>]
```

次のパラメータを指定できます。

- + *<Samba resource>* - SpIDer Guard for SMBの保護に追加する**Samba**共有リソースの名前(`smb.conf`設定ファイルで指定されているもの)。



- - <*Samba resource*> - SpIDer Guard for SMBの保護から除外する**Samba**共有リソースの名前 (`smb.conf`設定ファイルで指定されているもの)。
- +/all - SpIDer Guard for SMBの保護に、`smb.conf`設定ファイルで指定されたすべての共有**Samba**リソースを追加します。
- -/all - SpIDer Guard for SMBの保護から、`smb.conf`設定ファイルで指定されたすべての共有**Samba**リソースを除外します。
- <*configuration file*> - 処理する必要がある**Samba**サーバー設定ファイル(`smb.conf`)へのパス。この引数を省略すると、**drweb-configure**ツールは実際の`smb.conf`ファイルを探します。



SpIDer Guard for SMBと**Samba**共有ディレクトリとの統合に関するヘルプドキュメントにアクセスするには、次のコマンドを使用します。

```
$ drweb-configure --help samba
```

NSSボリュームとの統合

Dr.Web for UNIX File Serversを**Novell Storage Services**ボリュームと統合するには、設定ファイルの[NSS] [セクション](#)にある次のパラメータに値を指定します。

- **ProtectedVolumes**パラメータで、**NSS**マウントポイントにあり、保護の対象となるファイルシステムボリュームの名前を指定します。パラメータが空の場合、**NSS**マウントポイントのすべてのボリュームが保護されます。
- 必要に応じて、**ExcludedPath**および**IncludedPath**パラメータを使用して、保護されたボリュームにあるオブジェクトへのパスを除外したり、SpIDer Guard for NSSによるチェックに含めたりできます。ディレクトリへのパスまたはファイルへのパスを指定できます。ディレクトリを指定した場合、そのディレクトリのコンテンツはすべてスキップまたはスキャンされます。**IncludedPath**パラメータは**ExcludedPath**パラメータよりも優先されます。つまり、同じオブジェクト(ファイルまたはディレクトリ)が両方のパラメータ値に含まれる場合、このオブジェクトは検査されます。パラメータ**IncludedPath**と**ExcludedPath**では、ファイルマスク(ワイルドカード)を使用できます。これらのパラメータで指定するパスの大文字と小文字を区別するかどうかは、**NSS**設定によって定義されます。
- **Start**パラメータをYesに設定して、SpIDer Guard for NSSを有効にします。

すべての設定を調整したら、Dr.Web for UNIX File Serversを再起動します([コマンドdrweb-ctl reload](#)を使用します)。設定デーモンDr.Web ConfigDを再起動することもできます(**service** `drweb-configd restart`コマンドを使用します)。



簡単な説明

このセクションの内容:

- ファイルリポジトリの操作:
 - [GNU/Linuxファイルシステムモニタリングを設定する方法](#)
 - [Dr.Web for UNIX File ServersをSambaサーバーに接続する方法](#)
 - [新しいSMB共有ディレクトリを追加する方法](#)
 - [Dr.Web for UNIX File ServersをNovell Storage Servicesに接続する方法](#)
 - [保護された新しいNSSボリュームを追加する方法。](#)
- Dr.Web for UNIX File Serversの一般的な動作:
 - [Dr.Web for UNIX File Serversを再起動する方法。](#)
 - [集中管理サーバーに接続する方法](#)
 - [集中管理サーバーから切断する方法](#)
 - [Dr.Web for UNIX File Serversを有効化する方法](#)
 - [Dr.Web for UNIX File Serversをアップグレードする方法](#)
 - [Dr.Web for UNIX File Serversコンポーネントを追加または削除する方法](#)
 - [Dr.Web for UNIX File Serversコンポーネントの動作を管理する方法](#)
 - [製品のログを表示する方法](#)

Dr.Web for UNIX File ServersをSambaサーバーに接続する方法

[Sambaファイルサーバーとの統合](#)セクションの指示に従ってください。

Dr.Web for UNIX File ServersをNovell Storage Servicesに接続する方法

[NSSボリュームとの統合](#)セクションの指示に従ってください。

GNU/Linuxファイルシステムモニタリングを設定する方法

[ファイルシステムモニタリングの設定](#)セクションの指示に従ってください。



Dr.Web for UNIX File Serversを再起動する方法

Dr.Web for UNIX File Serversがすでに実行されているときに再起動するには、Dr.Web ConfigD設定デーモンを管理するスクリプトを使用することもできます。デーモンの起動、停止、または再起動は、それぞれDr.Web for UNIX File Serversの起動、停止、または再起動を引き起こします。

Dr.Web ConfigDの動作を制御するシェルスクリプトは、標準のOSディレクトリ(**GNU/Linux**の場合は`/etc/init.d/`、**FreeBSD**の場合は`/usr/local/etc/rc.d/`)にあります。スクリプトの名前は`drweb-configd`です。次のパラメータがあります。

パラメータ	説明
<code>start</code>	実行していない場合は、Dr.Web ConfigDを起動するように指示します。Dr.Web ConfigDが起動すると、Dr.Web ConfigDはDr.Web for UNIX File Serversに必要なすべてのコンポーネントを起動します。
<code>stop</code>	Dr.Web ConfigDが実行中の場合はシャットダウンするように指示します。Dr.Web ConfigDがシャットダウンすると、Dr.Web ConfigDはDr.Web for UNIX File Serversのすべてのコンポーネントもシャットダウンします。
<code>restart</code>	Dr.Web ConfigDを再起動(シャットダウンしてから起動)するように指示します。Dr.Web ConfigDはシャットダウンしてからDr.Web for UNIX File Serversのすべてのコンポーネントを起動します。Dr.Web ConfigDが開始されていない場合、パラメータは開始と同じ効果があります。
<code>condrestart</code>	Dr.Web ConfigDが実行している場合のみ、再起動するように指示します。
<code>reload</code>	コンポーネントが実行している場合は、HUPシグナルをDr.Web ConfigDに送信するように指示します。Dr.Web ConfigDは、このシグナルをDr.Web for UNIX File Serversのすべてのコンポーネントに転送します。このパラメータは、すべてのコンポーネントに設定を再度読み込ませるために使用されます。
<code>status</code>	現在のDr.Web ConfigDの状態をコンソールに出力するように指示します。

たとえば、**GNU/Linux** OSでDr.Web for UNIX File Serversを再起動(または実行されていない場合は起動)するには、次のコマンドを使用します。

```
# /etc/init.d/drweb-configd restart
```

集中管理サーバーに接続する方法

1. 集中管理サーバーのアドレスとその証明書のファイルをアンチウイルスネットワーク管理者から入手します。またワークステーションのIDとパスワードやメイングループと課金プラングループのIDなどの追加パラメータが必要になる場合があります。
2. Dr.Web for UNIX File Serversで提供される**Dr.Web Ct**コマンドラインツールの**`esconnect`**コマンドを使用します。

接続するには、サーバーの証明書ファイルへのパスを指定して、`--Certificate`オプションを使用する必要があります。`--Login`と`--Password`パラメータを使用して、ホストのID(集中管理サーバーで使用する用語を使用する場合は「ワークステーション」ID)と集中管理サーバーの認証用パスワードも入力できます。この場合、サーバーへの接続は、正しいIDとパスワードのペアを指定した場合にのみ確立されます。パラ



メータが指定されない場合、サーバーへの接続は、(サーバーの設定に応じて、自動的またはアンチウイルスネットワークの管理者によって)サーバーで承認されている場合にのみ確立されます。

さらに、`--Newbie`オプション(新しいユーザーとして接続する)を使用することもできます。このモードがサーバーで許可されている場合、この接続が承認されると、サーバーは自動的に一意の識別子とパスワードのペアを生成します。これは、このエージェントがサーバーに接続する際に使用されます。このモードでは、このホスト用にすでに別のアカウントが存在している場合でも、集中管理サーバーはそのホストの新しいアカウントを生成します。

集中管理サーバーに接続する際に、Dr.Web for UNIX File Serversで実行するコマンドの例:

```
# drweb-ctl esconnect <server address> --Certificate <証明書ファイルへのパス>
```

集中管理サーバーへの接続を確立すると、サーバーに設定されている権限とDr.Web ES Agentコンポーネントの**設定パラメータ** `MobileMode`の値に応じて、Dr.Web for UNIX File Serversは集中管理モードまたはモバイルモードで動作します。無条件にモバイルモードを使用できるようにするには、パラメータの値をOnに設定します。集中管理モードで動作させるには、パラメータの値をOffに設定します。

集中管理サーバーに接続されているDr.Web for UNIX File Serversにモバイルモードへの切り替えを指示するコマンドの標準的な例は次のとおりです。

```
# drweb-ctl cfset ESAgent.MobileMode On
```



使用する集中管理サーバーがモバイルモードをサポートしていない、または許可していない場合、`MobileMode`パラメータを調整してもDr.Web for UNIX File Serversの動作をモバイルモードに切り替えることはできません。

集中管理サーバーから切断する方法

Dr.Web for UNIX File Serversを集中管理サーバーから切断してその動作をスタンドアロンモードに切り替えるには、Dr.Web for UNIX File Serversにある**Dr.Web Ctl**コマンドラインツールの**`esdisconnect`**コマンドを使用します。

```
# drweb-ctl esdisconnect
```

Dr.Web for UNIX File Serversをスタンドアロンモードで使用するには、有効なライセンス**キーファイル**が必要です。それ以外の場合は、動作がスタンドアロンモードに切り替えられた後、Dr.Web for UNIX File Serversのアンチウイルス機能が**ブロック**されます。

Dr.Web for UNIX File Serversを有効化する方法

1. Doctor WebのWebサイト <https://products.drweb.com/register/> から登録を実施します。
2. 登録時に指定したメールアドレスに、有効なライセンスキーファイルを含むアーカイブが送信されます(登録後にこのアーカイブをWebサイトから直接ダウンロードすることもできます)。
3. キーファイルの**インストール手順**を実行します。



新しいSMB共有ディレクトリを追加する方法

1. 共有ディレクトリを記述するセクションを追加して、**Samba**サーバーの設定ファイル(`smb.conf`)を編集します。共有ディレクトリを記述するセクションは、次のようになります。

```
[ <リソース名> ]
comment = <any comment>
path = <path to the protected directory>
vfs objects = smb_spider
writeable = yes
browseable = yes
guest ok = yes
public = yes
```

<share_name>は共有リソースの任意の名前、<any comment>はコメントを含む任意の行になります(オプション)。

2. 追加した共有ディレクトリのスキャン設定を指定する必要があり、これらの設定がデフォルトのSpIDer Guard for SMB設定と異なる場合は、[Sambaファイルサーバーとの統合](#)セクションに記載されている手順3と4を実行します。
3. **Samba**サーバーとDr.Web for UNIX File Serversを再起動します。

保護された新しいNSSボリュームを追加する方法

1. **ProtectedVolumes**パラメータ(設定ファイルの[NSS] [セクション](#))に、保護するボリュームの名前を指定します。このパラメータに値が割り当てられていない場合は、NSSボリュームのマウント用ディレクトリのすべてのボリュームが保護されます。
2. Dr.Web for UNIX File Servers Dr.Web for UNIX File Serversを再起動します。

Dr.Web for UNIX File Serversをアップグレードする方法

コンポーネントのバージョンを[更新](#)するか、[新しいバージョンにアップグレード](#)してください。

アップグレード中に、現在のDr.Web for UNIX File Serversバージョンを削除するように求められることがあります。

Dr.Web for UNIX File Serversコンポーネントを追加または削除する方法

[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](#)の手順に従います。

コンポーネントをインストール/アンインストールする場合、依存関係を解消するために他のDr.Web for UNIX File Serversコンポーネントを追加でインストールまたはアンインストールすることがあります。

コンポーネント動作を管理する方法

Dr.Web for UNIX File Serversコンポーネントのステータスを表示したり、それらの設定を管理したりするには、次のものを使用できます。



- [コマンドラインベースの管理ツール](#)Dr.Web Ctl(**drweb-ctl** appinfo、**drweb-ctl** cfshowおよび**drweb-ctl** cfsetコマンドを使用します。使用可能なコマンドの一覧を表示するには、**drweb-ctl --help**コマンドを使用します)。
- Dr.Web for UNIX File Serversの管理用[ウェブインターフェース](#)(初期設定では、ウェブブラウザから<https://127.0.0.1:4443/>にアクセスすると利用できます)。

Dr.Web for UNIX File Serversのログを表示する方法

デフォルト設定に従って、すべてのDr.Web for UNIX File Serversコンポーネントの一般ログは**syslog**ファイルに表示されます(システムコンポーネント**syslog**によってメッセージを記録するファイルはシステムに依存し、ディレクトリ/var/logにあります)。一般ログ設定は、[設定ファイル](#)の[Root] [セクション](#)(LogパラメータとDefaultLogLevelパラメータ)で定義されます。設定セクションの各[コンポーネント](#)には、LogパラメータとLogLevelパラメータがあります。ログの保存場所と、コンポーネントがログに出力するメッセージのログレベルを設定します。

また、**drweb-ctl log**[コマンド](#)を使用することもできます。

ログ設定を変更するには、コマンドライン管理ツールDr.Web CtlとDr.Web for UNIX File Servers管理Webインターフェース(インストールされている場合)を使用してください。

- エラーを特定するために、すべてのコンポーネントのログの出力先を別のファイルに設定し、デバッグ情報がログに出力されるようにすることを推奨します。そのためには、以下のコマンドを実行します。

```
# 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レベルに戻すには、次のコマンドを実行します。

```
# drweb-ctl cfset Root.Log -r
# drweb-ctl cfset Root.DefaultLogLevel -r
```




Dr.Web for UNIX File Serversコンポーネント

このセクションでは、Dr.Web for UNIX File Serversのコンポーネントについて説明します。各コンポーネントの機能、動作原理、[設定ファイル](#)に保存されているパラメータに関する情報を確認できます。

Dr.Web ConfigD

Dr.Web ConfigD設定デモンは、Dr.Web for UNIX File Serversのコアコンポーネントです。すべてのDr.Web for UNIX File Serversコンポーネント用に設定情報の中央ストレージを提供し、すべてのコンポーネントの動作を管理し、コンポーネント間の信頼できるデータの交換を整理します。

動作原理

メイン機能

1. 設定に応じてDr.Web for UNIX File Serversコンポーネントを起動／停止します。動作に障害が発生した場合、コンポーネントを自動的に再起動します。他のコンポーネントのリクエストに応じてコンポーネントを起動します。別のコンポーネントが起動またはシャットダウンしたときに、アクティブなDr.Web for UNIX File Serversコンポーネントに通知します。
2. 構成設定へのすべてのコンポーネントの集中アクセスを提供します。設定パラメータを集中管理するためのインターフェースを持つ特別なコンポーネントを提供します。設定の変更についてすべての必須コンポーネントに通知します。
3. 使用されているライセンスキーファイルからの情報をコンポーネントに提供します。特別なコンポーネントから新しいライセンス情報を受け取ります。ライセンスデータまたは構成パラメータの変更について、コンポーネントを実行しているDr.Web for UNIX File Serversに通知します。

設定デモンDr.Web ConfigDは常にroot権限で起動されます。他のDr.Web for UNIX File Serversコンポーネントを起動し、事前に開いているソケットを介してそれらと通信します。設定デモンは、情報ソケット（公に利用可能）と管理ソケット（スーパーユーザー権限を持つコンポーネントのみ利用可能）を介して他のDr.Web for UNIX File Serversコンポーネントから接続を受け取ります。設定パラメータとライセンスデータをファイルから読み込む、または[Dr.Web ES Agent](#)を介して使用されている集中管理サーバーから配信し、設定パラメータをデフォルトの正しい値に置き換えます。そのため、いずれかのコンポーネントが起動したとき、またはSIGHUPシグナルが送信されたとき、設定デモンにはDr.Web for UNIX File Serversの完全な一貫したパラメータのセットが設定されます。

SIGHUPシグナルを受信すると、設定管理デモンは設定パラメータとライセンスデータを再度読み込みます。必要に応じて、デモンはすべてのコンポーネント通知を送信して、設定を再度読み込むように指示します。SIGTERMシグナルを受信すると、デモンはすべてのコンポーネントをシャットダウンしてから、自身の操作を終了します。デモンは、シャットダウン後にコンポーネントの一時ファイルもすべて削除します。

通信の原理

1. すべてのコンポーネントは、起動時に設定デモンDr.Web ConfigDから受信した設定パラメータとライセンスデータのみを使用します。



2. デーモンは、管理されているすべてのコンポーネントから統合ログにメッセージを収集します。コンポーネントからエラーストリーム*stderr*に出力されたすべての情報はデーモンによって収集され、どのコンポーネントがこれを出したかを示すマークとともにDr.Web for UNIX File Serversの統合ログに書き込まれます。
3. シャットダウンすると、管理されているコンポーネントは終了コードを返します。コードが101、102、または103ではない場合、設定デーモンはこのコンポーネントを再起動します。そのため、コンポーネントが異常終了すると再起動され、*stderr*からのエラーメッセージがDr.Web for UNIX File Serversのログに登録されます。
 - コンポーネントがコード101で終了した場合、コンポーネントはライセンスパラメータが変更された後にのみ再起動されます。そのため、ライセンスの制限のためにコンポーネントが操作できない場合、コンポーネントはその操作を終了してコード101を*stderr*に出力します。
 - コンポーネントがコード102で終了した場合、そのコンポーネントは設定パラメータが変更された後にのみ再起動されます。そのため、設定が原因でコンポーネントが操作できない場合、コンポーネントはその操作を終了してコード102を*stderr*に出力します。設定デーモンは、パラメータが変更された後にのみコンポーネントの再起動を試みます。
 - リクエストに応じて設定デーモンによって開始されたコンポーネントは、アイドル状態になったときにその動作を終了し、コード103を出力することがあります。たとえば、[Dr.Web Scanning Engine](#)、[Dr.Web File Checker](#)などのコンポーネントです。
 - 設定デーモンからコンポーネントが受信した新しいパラメータ値を「オンザフライ」で適用できない場合、つまり再起動が必要な場合、コンポーネントはコード0で終了します。その場合、Dr.Web ConfigDはコンポーネントを再起動します。
 - コンポーネントが設定デーモンに接続できない、または通信プロトコルエラーが発生した場合、コンポーネントは*stderr*に適切なメッセージを出力してコード1で終了します。
4. シグナル交換：
 - 設定デーモンは、コンポーネントにSIGHUPシグナルを送信して設定パラメータを変更するよう指示します。
 - 設定デーモンは、コンポーネントにSIGTERMシグナルを送信して30秒以内に操作を終了するよう指示します。
 - SIGKILLシグナルは設定デーモンから送信され、SIGTERMシグナルの受信後30秒以内にシャットダウンしなかったコンポーネントを強制的に停止させます。

コマンドライン引数

設定デーモンDr.Web ConfigDを実行するには、コマンドラインに次のコマンドを入力します。

```
$ <opt_dir>/bin/drweb-configd [ <parameters> ]
```

設定デーモンDr.Web ConfigDは、以下のオプションを処理できます。

パラメータ	説明
<code>--help</code>	<p>機能：コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了するように指示します。</p> <p>短縮形： <code>-h</code></p> <p>引数： None</p>
<code>--version</code>	<p>機能：このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了するように指示します。</p> <p>短縮形： <code>-v</code></p>



	引数: None
--config	説明: 指定した設定ファイルを今後の操作に使用するように指示します。 短縮形: -c 引数: <path to the file> - 使用する設定ファイルへのパス。
--daemonize	説明: コンポーネントをデーモンとして実行するように指示します。つまり、端末にはアクセスできません。 短縮形: -d 引数: None
--pid-file	説明: 指定されたPIDファイルを今後の操作に使用するように指示します。 短縮形: -p 引数: <path to the file> - プロセスID(PID)の保存先ファイルへのパス。

例:

```
$ /opt/drweb.com/bin/drweb-configd -d -c /etc/opt/drweb.com/drweb.ini
```

このコマンドはDr.Web ConfigDを/etc/opt/drweb.com/drweb.iniの設定ファイルを使用するデーモンとして実行します。

スタートアップノート

Dr.Web for UNIX File Serversの操作を有効にするには、Dr.Web ConfigDがデーモンとして実行されている必要があります。標準起動中、Dr.Web ConfigDはOSの起動時に自動的に起動されます。そのため、Dr.Web ConfigDは、標準のOSディレクトリ(**GNU/Linux**の場合は/etc/init.d/、**FreeBSD**の場合は/usr/local/etc/rc.d/)にある標準管理スクリプトdrweb-configdと一緒に保存されます。コンポーネントの動作を管理するには、Dr.Web for UNIX File Servers用の[Dr.Web Ctl](#)コマンドラインベースの管理ツールを使用できます(これは[drweb-ctl](#)コマンドを使用して呼び出されます)。



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ドキュメントを要求するには、次のコマンドを使用します。**man 1 drweb-configd**

設定パラメータ

デーモンのDr.Web ConfigDは、Dr.Web for UNIX File Serversの統合された[設定ファイル](#)の[Root]セクションにあるコンフィギュレーションパラメータを使用します。

セクションには以下のパラメータが含まれています。

DefaultLogLevel {logging level}	すべてのDr.Web for UNIX File Serversコンポーネントのイベントログのデフォルトの ロギングレベル を定義します。 このパラメータの値は、設定で独自のログレベルが設定されていない製品内のすべてのコンポーネントに使用されます。 デフォルト値: Notice
---	---



LogLevel <i>{logging level}</i>	Dr.Web ConfigDのイベントログの ロギングレベル 。 デフォルト値: Notice
Log <i>{log type}</i>	設定デーモンの ロギング方式 と、このパラメータに別の値が指定されていないコンポーネントのロギング方式。 設定ファイルが読み込まれる前の初回起動時に、設定デーモンは次のパラメータ値を使用します。 <ul style="list-style-type: none">デーモンとして (-dオプションを付けて実行した場合) - SYSLOG:Daemonその他の場合 - Stderr コンポーネントがバックグラウンドモードで動作している(コマンドラインから -dオプションを使用して起動した)場合は、Stderrの値をこのパラメータに使用することはできません。 デフォルト値: Syslog:Daemon
PublicSocketPath <i>{path to file}</i>	すべてのDr.Web for UNIX File Serversコンポーネント間のやり取りに使用されるソケットへのパス。 デフォルト値: /var/run/.com.drweb.public
AdminSocketPath <i>{path to file}</i>	昇格された(管理者)権限を持つDr.Web for UNIX File Serversコンポーネント間のやり取りに使用されるソケットへのパス。 デフォルト値: /var/run/.com.drweb.admin
CoreEnginePath <i>{path to file}</i>	Dr.Web Virus-Finding Engineスキャンエンジンの動的ライブラリへのパス。 デフォルト値: <var_dir>/lib/drweb32.dll <ul style="list-style-type: none">GNU/Linuxの場合: /var/opt/drweb.com/lib/drweb32.dllFreeBSDの場合: /var/drweb.com/lib/drweb32.dll
VirusBaseDir <i>{path to directory}</i>	ウイルスデータベースファイルがあるディレクトリへのパス。 デフォルト値: <var_dir>/bases <ul style="list-style-type: none">GNU/Linuxの場合: /var/opt/drweb.com/basesFreeBSDの場合: /var/drweb.com/bases
KeyPath <i>{path to file}</i>	キーファイルへのパス(正規またはデモライセンス)。 デフォルト値: <etc_dir>/drweb32.key <ul style="list-style-type: none">GNU/Linuxの場合: /etc/opt/drweb.com/drweb32.keyFreeBSDの場合: /usr/local/etc/drweb.com/drweb32.key
CacheDir <i>{path to directory}</i>	キャッシュディレクトリへのパス(更新されたキャッシュとスキャンされたファイルに関する情報のキャッシュを保持するために使用されます)。 デフォルト値: <var_dir>/cache <ul style="list-style-type: none">GNU/Linuxの場合: /var/opt/drweb.com/cacheFreeBSDの場合: /var/drweb.com/cache
TempDir	一時ファイルがあるディレクトリへのパス。



<i>{path to directory}</i>	デフォルト値：システム環境変数TMPDIR、TMP、TEMPまたはTMPDIRからコピーされたパス（環境変数はこの順序で検索されます）。これらの環境変数がない場合は、/tmp。
RunDir <i>{path to directory}</i>	実行中のコンポーネントが有するすべてのPIDファイルと、Dr.Web for UNIX File Serversコンポーネント間のやり取りに使用されるソケットを含むディレクトリへのパス。 デフォルト値：/var/run
VarLibDir <i>{path to directory}</i>	Dr.Web for UNIX File Serversコンポーネントによって使用されるライブラリを含むディレクトリへのパス。 デフォルト値：<var_dir>/lib <ul style="list-style-type: none">• GNU/Linuxの場合：/var/opt/drweb.com/lib• FreeBSDの場合：/var/drweb.com/lib
VersionDir <i>{path to directory}</i>	Dr.Web for UNIX File Serversコンポーネントの現在のバージョンに関する情報が格納されているディレクトリへのパス。 デフォルト値：<var_dir>/version <ul style="list-style-type: none">• GNU/Linuxの場合：/var/opt/drweb.com/version• FreeBSDの場合：/var/drweb.com/version
DwsDir <i>{path to directory}</i>	このパラメータは使用されません。 デフォルト値：<var_dir>/dws <ul style="list-style-type: none">• GNU/Linuxの場合：/var/opt/drweb.com/dws• FreeBSDの場合：/var/drweb.com/dws
AdminGroup <i>{group name / GID}</i>	Dr.Web for UNIX File Servers管理用の管理者権限を持つユーザーのグループ。rootスーパーユーザーに加えて、これらのユーザーはDr.Web for UNIX File Serversコンポーネントの権限をスーパーユーザー権限に昇格させることができます。 デフォルト値：Dr.Web for UNIX File Serversのインストール中に決定されます。
TrustedGroup <i>{group name / GID}</i>	このパラメータは使用されません。 デフォルト値：drweb
DebugIpc <i>{Boolean}</i>	詳細なIPCメッセージをデバッグレベルでログファイルに含めるかどうかを示します（LogLevel = DEBUGの場合など）。IPCメッセージは、設定デーモンと他のコンポーネントとの間のやり取りを示します。 デフォルト値：No
UseCloud <i>{Boolean}</i>	Dr.Web Cloudサービスを参照して悪意のあるファイルやURLに関する情報を受け取るかどうかを指定します デフォルト値：No
AntispamCorePath <i>{path to file}</i>	このパラメータは使用されません。 デフォルト値：<var_dir>/lib/vaderetro.so <ul style="list-style-type: none">• GNU/Linuxの場合：/var/opt/drweb.com/lib/vaderetro.so



	• FreeBSD の場合: /var/drweb.com/lib/vaderetro.so
VersionNotification <i>{Boolean}</i>	現在インストールされているDr.Web for UNIX File Serversバージョンのアップデートが利用可能であることをユーザーに通知します。 デフォルト値: Yes

Dr.Web Ctl

このセクションの内容:

- [概要](#)
- [リモートホストスキャン](#)

概要

特別なDr.Web Ctl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 UNIX File Servers 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 UNIX File Servers設定のパラメータを確認・変更する
- Dr.Web for UNIX File Servers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
- 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
- 隔離されたオブジェクトを確認・管理する(Dr.Web File Checker[コンポーネント](#)を介して)
- 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

Dr.Web for UNIX File Serversを管理するためのユーザー[コマンド](#)は [Dr.Web ConfigD](#) 設定デーモンが動作中の場合のみ適用されます(デフォルトでは、この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 UNIX File Serversの動作を管理するコマンドの自動補完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)。コマンドシェルが自動補完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F. 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 UNIX File Servers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。リモートスキャンの手段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](#) `remotescan` を使用します）。

コマンドラインフォーマット

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 UNIX File Servers 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> ] ]
```

- **<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 UNIX File Servers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

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します。 <pre>\$ drweb-ctl <command> -h</pre>
-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。 <pre>\$ drweb-ctl <command> -d</pre>

3. コマンド

Dr.Web for UNIX File Servers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ドキュメントを要求するには、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>	目的 : Dr.Web File Checker コンポーネントを介して、指定されたファイルまたはディレクトリのチェックを開始します。




コマンド	説明
	<p>引数:</p> <p><path>—スキャンの対象として選択されたファイルやディレクトリへのパスです。</p> <p>--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。</p> <p>オプション:</p> <p>-a [--Autonomous] - Dr.Web Scanning EngineとDr.Web File Checkerの自律コピーを実行して指定したチェックを実行し、チェックが完了した後に終了します。自律スキャン中に検出された脅威は、threatsコマンド(以下参照)で表示される検出された脅威の共通リストに追加されません。またそれぞれの管理下で製品が実行されている場合、そうした脅威に関する情報は集中管理サーバーに配信されません。</p> <p>--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。</p> <p>--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。</p> <div> --stdin および --stdin0 を使用する際、リスト内のパスには検索のためのパターンまたは正規表現が含まれていないようにする必要があります。--stdin および --stdin0 オプションの推奨される使用法は、scan コマンド内でパスのリスト(find などの外部ユーティリティによって生成された)を処理するというものです(使用例 参照)。</div> <p>--Exclude <path> - チェックから除外するパス(マスク記号*と?は使用できません)。</p> <p><i>任意オプション、複数回設定できます。</i></p> <p>--Report <type> - スキャンレポートのタイプを指定します。</p> <p>使用可能な値:</p> <ul style="list-style-type: none">• 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。 <p>デフォルト値: BRIEF</p> <p>--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。</p> <p>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。</p> <p>デフォルト値: 0</p> <p>--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。</p> <p>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。</p> <p>デフォルト値: 8</p>



コマンド	説明
	<p>--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。</p> <p>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。</p> <p>デフォルト値 : 8</p> <p>--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。</p> <p>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。</p> <p>デフォルト値 : 8</p> <p>--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。</p> <p>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。</p> <p>デフォルト値 : 8</p> <p>--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。</p> <p>率は 2 以上にする必要があります。</p> <p>デフォルト値 : 3000</p> <p>--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。</p> <p>デフォルト値 : On</p> <p>--OnKnownVirus <action> - シグネチャ解析を用いて検出された脅威に適用される アクション です。</p> <p>使用可能な値 : REPORT、CURE、QUARANTINE、DELETE</p> <p>デフォルト値 : REPORT</p> <p>--OnIncurable <action> - 検出された脅威の修復に失敗した場合に適用される、または修復不可能な脅威に対して適用されるアクションです。</p> <p>使用可能な値 : REPORT、QUARANTINE、DELETE</p> <p>デフォルト値 : REPORT</p> <p>--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。</p> <p>使用可能な値 : REPORT、QUARANTINE、DELETE</p> <p>デフォルト値 : REPORT</p> <p>--OnAdware <action> - 検出されたアドウェアプログラムに対して適用されるアクションです。</p> <p>使用可能な値 : REPORT、QUARANTINE、DELETE</p> <p>デフォルト値 : REPORT</p> <p>--OnDialers <action> - ダイアラーに対して適用されるアクションです。</p> <p>使用可能な値 : REPORT、QUARANTINE、DELETE</p> <p>デフォルト値 : REPORT</p> <p>--OnJokes <action> - 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。</p> <p>使用可能な値 : REPORT、QUARANTINE、DELETE。</p>



コマンド	説明
	<p>デフォルト値: <i>REPORT</i></p> <p>--OnRiskware <action> - 潜在的に危険なプログラム(リスクウェア)に対して適用されるアクションです。</p> <p>使用可能な値: <i>REPORT</i>、<i>QUARANTINE</i>、<i>DELETE</i></p> <p>デフォルト値: <i>REPORT</i></p> <p>--OnHacktools <action> - ハッキングツールに対して適用されるアクションです。</p> <p>使用可能な値: <i>REPORT</i>、<i>QUARANTINE</i>、<i>DELETE</i></p> <p>デフォルト値: <i>REPORT</i></p> <div><p>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(<i>DELETE</i>)アクションの代わりにコンテナの隔離への移動(<i>QUARANTINE</i>)が実行されます。</p></div>
bootscan <disk drive> ALL	<p>目的: Dr.Web File Checkerコンポーネントを介して、指定されたディスクのブートレコードのチェックを開始します。MBRとVBRの両方のレコードがスキャンされます。</p> <p>引数:</p> <p><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。</p> <p>オプション:</p> <p>-a [--Autonomous] - Dr.Web Scanning EngineとDr.Web File Checkerの自律コピーを実行して指定したチェックを実行し、チェックが完了した後に終了します。自律スキャン中に検出された脅威は、threatsコマンド(以下参照)で表示される検出された脅威の共通リストに追加されません。またそれぞれの管理下で製品が実行されている場合、そうした脅威に関する情報は集中管理サーバーに配信されません。</p> <p>--Report <type> - レポートのタイプを指定します。</p> <p>使用可能な値:</p> <ul style="list-style-type: none">• 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。 <p>デフォルト値: <i>BRIEF</i></p> <p>--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。</p> <p>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。</p> <p>デフォルト値: 0</p> <p>--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。</p> <p>デフォルト値: <i>On</i></p> <p>--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。</p>



コマンド	説明
	<p>値に <i>No</i> 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。</p> <p>デフォルト値 : <i>No</i></p> <p>--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。</p>
procscan	<p>目的 : Dr.Web File Checkerを使用して、現在実行中のプロセスのコードを含む実行可能ファイルのチェックを開始します。悪意のある実行可能ファイルが検出されると、そのファイルは無効化され、このファイルによって実行される全てのプロセスは強制的に終了されます。</p> <p>引数 : None</p> <p>オプション :</p> <p>-a [--Autonomous] - Dr.Web Scanning EngineとDr.Web File Checkerの自律コピーを実行して指定したチェックを実行し、チェックが完了した後に終了します。自律スキャン中に検出された脅威は、threatsコマンド(以下参照)で表示される検出された脅威の共通リストに追加されません。またそれぞれの管理下で製品が実行されている場合、そうした脅威に関する情報は集中管理サーバーに配信されません。</p> <p>--Report <type> - レポートのタイプを指定します。</p> <p>使用可能な値 :</p> <ul style="list-style-type: none">• 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。 <p>デフォルト値 : <i>BRIEF</i></p> <p>--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。</p> <p>値に <i>0</i> 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。</p> <p>デフォルト値 : <i>0</i></p> <p>--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。</p> <p>デフォルト値 : <i>On</i></p> <p>--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イングレベルの上限を指定します。</p> <p>値に <i>0</i> 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。</p> <p>デフォルト値 : <i>8</i></p> <p>--OnKnownVirus <action> - シグネチャ解析を用いて検出された脅威に適用される アクション です。</p> <p>使用可能な値 : <i>REPORT</i>、<i>CURE</i>、<i>QUARANTINE</i>、<i>DELETE</i></p> <p>デフォルト値 : <i>REPORT</i></p> <p>--OnIncurable <action> - 検出された脅威の修復に失敗した場合に適用される、または修復不可能な脅威に対して適用されるアクションです。</p> <p>使用可能な値 : <i>REPORT</i>、<i>QUARANTINE</i>、<i>DELETE</i></p>



コマンド	説明
	<p>デフォルト値: <i>REPORT</i></p> <p>--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。</p> <p>使用可能な値: <i>REPORT</i>、<i>QUARANTINE</i>、<i>DELETE</i></p> <p>デフォルト値: <i>REPORT</i></p> <p>--OnAdware <action> - 検出されたアドウェアプログラムに対して適用されるアクションです。</p> <p>使用可能な値: <i>REPORT</i>、<i>QUARANTINE</i>、<i>DELETE</i></p> <p>デフォルト値: <i>REPORT</i></p> <p>--OnDialers <action> - ダイアラーに対して適用されるアクションです。</p> <p>使用可能な値: <i>REPORT</i>、<i>QUARANTINE</i>、<i>DELETE</i></p> <p>デフォルト値: <i>REPORT</i></p> <p>--OnJokes <action> - 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。</p> <p>使用可能な値: <i>REPORT</i>、<i>QUARANTINE</i>、<i>DELETE</i>。</p> <p>デフォルト値: <i>REPORT</i></p> <p>--OnRiskware <action> - 潜在的に危険なプログラム(リスクウェア)に対して適用されるアクションです。</p> <p>使用可能な値: <i>REPORT</i>、<i>QUARANTINE</i>、<i>DELETE</i></p> <p>デフォルト値: <i>REPORT</i></p> <p>--OnHacktools <action> - ハッキングツールに対して適用されるアクションです。</p> <p>使用可能な値: <i>REPORT</i>、<i>QUARANTINE</i>、<i>DELETE</i></p> <p>デフォルト値: <i>REPORT</i></p> <div> 実行可能ファイルで脅威が検出された場合、Dr.Web for UNIX File Serversはそのファイルから起動した全てのプロセスを終了させます。</div>
netscan [<i><path></i>]	<p>目的: ネットワークデータスキャン用にDr.Web Network Checkerエージェントを介して、指定されたファイルまたはディレクトリの分散スキャンを開始します。Dr.Web for UNIXを実行している他のホストへの接続が設定されていない場合、スキャンはローカルで利用可能なScanning Engine(<i>scan</i>コマンドと同様)を介してのみ行われます。</p> <p>引数:</p> <p><i><path></i> - スキャンの対象として選択されたファイルやディレクトリへのパスです。</p> <p>この引数を省略すると、入カスレッド<i>stdin</i>を介して受信したデータがスキャンされます。</p>




コマンド	説明
	<p>オプション:</p> <p>--Report <type> - スキャンレポートのタイプを指定します。</p> <p>使用可能な値:</p> <ul style="list-style-type: none">• 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。 <p>デフォルト値: <i>BRIEF</i></p> <p>--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。</p> <p>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。</p> <p>デフォルト値: 0</p> <p>--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。</p> <p>デフォルト値: <i>On</i></p> <p>--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。</p> <p>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。</p> <p>デフォルト値: 8</p> <p>--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。</p> <p>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。</p> <p>デフォルト値: 8</p> <p>--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。</p> <p>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。</p> <p>デフォルト値: 8</p> <p>--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。</p> <p>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。</p> <p>デフォルト値: 8</p> <p>--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。</p> <p>率は 2 以上にする必要があります。</p> <p>デフォルト値: 3000</p> <p>--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。</p> <p>値に <i>No</i> 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。</p>




コマンド	説明
	デフォルト値 : <i>No</i>
<code>flowscan <path></code>	<p>目的 : Dr.Web File Checkerを使用して"flow"メソッドを用いて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（通常、この方法はSpIDer Guardに含まれる場合はSpIDer Guardによって内部的に使用されます）</p> <div> ファイルとディレクトリのオンデマンドスキャンの場合は、<code>scan</code>コマンドを使用することを推奨します。</div> <p>引数 :</p> <p><code><path></code> - スキャンの対象として選択されたファイルやディレクトリへのパスです。</p> <p>オプション :</p> <p><code>--ScanTimeout <number></code> - 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。</p> <p>値に <i>0</i>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。</p> <p>デフォルト値 : <i>0</i></p> <p><code>--HeuristicAnalysis <On/Off></code> - 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。</p> <p>デフォルト値 : <i>On</i></p> <p><code>--PackerMaxLevel <number></code> - 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。</p> <p>値に <i>0</i>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。</p> <p>デフォルト値 : <i>8</i></p> <p><code>--ArchiveMaxLevel <number></code> - 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。</p> <p>値に <i>0</i>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。</p> <p>デフォルト値 : <i>8</i></p> <p><code>--MailMaxLevel <number></code> - 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。</p> <p>値に <i>0</i>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。</p> <p>デフォルト値 : <i>8</i></p> <p><code>--ContainerMaxLevel <number></code> - 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。</p> <p>値に <i>0</i>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。</p> <p>デフォルト値 : <i>8</i></p> <p><code>--MaxCompressionRatio <ratio></code> - 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。</p> <p>率は <i>2</i>以上にする必要があります。</p>




コマンド	説明
	<p>デフォルト値 : 3000</p> <p>--OnKnownVirus <action>—シグネチャ解析を用いて検出された脅威に適用される アクション です。</p> <p>使用可能な値 : REPORT、CURE、QUARANTINE、DELETE</p> <p>デフォルト値 : REPORT</p> <p>--OnIncurable <action> - 検出された脅威の修復に失敗した場合に適用される、または修復不可能な脅威に対して適用されるアクションです。</p> <p>使用可能な値 : REPORT、QUARANTINE、DELETE</p> <p>デフォルト値 : REPORT</p> <p>--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。</p> <p>使用可能な値 : REPORT、QUARANTINE、DELETE</p> <p>デフォルト値 : REPORT</p> <p>--OnAdware <action> - 検出されたアドウェアプログラムに対して適用されるアクションです。</p> <p>使用可能な値 : REPORT、QUARANTINE、DELETE</p> <p>デフォルト値 : REPORT</p> <p>--OnDialers <action> - ダイアラーに対して適用されるアクションです。</p> <p>使用可能な値 : REPORT、QUARANTINE、DELETE</p> <p>デフォルト値 : REPORT</p> <p>--OnJokes <action> - 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。</p> <p>使用可能な値 : REPORT、QUARANTINE、DELETE。</p> <p>デフォルト値 : REPORT</p> <p>--OnRiskware <action> - 潜在的に危険なプログラム(リスクウェア)に対して適用されるアクションです。</p> <p>使用可能な値 : REPORT、QUARANTINE、DELETE</p> <p>デフォルト値 : REPORT</p> <p>--OnHacktools <action> - ハッキングツールに対して適用されるアクションです。</p> <p>使用可能な値 : REPORT、QUARANTINE、DELETE</p> <p>デフォルト値 : REPORT</p> <div> 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。</div>
rawscan <path>	<p>目的 : Dr.Web File Checkerを使用せず、Dr.Web Scanning Engineに指定されたファイルまたはディレクトリに対して"raw"スキャンを直接実行します。</p>



コマンド	説明
	<div><p>"raw"スキャンで検出された脅威は、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(以下参照)。</p></div> <div><p>このコマンドは、Dr.Web Scanning Engineの機能をデバッグするためにのみ使用することを推奨します。ファイルで検出された脅威のうち少なくとも1つの脅威が駆除されている場合、コマンドは「修復済」ステータスを出力します(全ての脅威が駆除されているわけではありません)。したがって、徹底したファイルスキャンが必要な場合は、このコマンドを使用することは推奨しません。後者の場合は、scanコマンドを使用することを推奨します。</p></div> <p>引数:</p> <p><path> - スキャンの対象として選択されたファイルやディレクトリへのパスです。</p> <p>オプション:</p> <p>--ScanEngine <path> Dr.Web Scanning EngineのUNIXソケットへのパスです。-指定しない場合、Scanning Engineの自律インスタンスが起動されます(スキャンが完了するとシャットダウンします)。</p> <p>--Report <type> - レポートのタイプを指定します。</p> <p>使用可能な値:</p> <ul style="list-style-type: none">• 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。 <p>デフォルト値: BRIEF</p> <p>--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。</p> <p>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。</p> <p>デフォルト値: 0</p> <p>--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。</p> <p>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。</p> <p>デフォルト値: 8</p> <p>--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。</p> <p>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。</p> <p>デフォルト値: 8</p> <p>--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。</p> <p>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。</p>



コマンド	説明
	<p>デフォルト値 : 8</p> <p>--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。</p> <p>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。</p> <p>デフォルト値 : 8</p> <p>--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。</p> <p>率は 2 以上にする必要があります。</p> <p>デフォルト値 : 3000</p> <p>--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。</p> <p>デフォルト値 : On</p> <p>--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。</p> <p>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。</p> <p>デフォルト値 : No</p> <p>--ListCleanItem - スキャンされたコンテナで見つかったクリーン (感染していない) なファイルのリストを出力できるようにします。</p> <p>--ShellTrace - ファイル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。</p>
remotescan <host> <path>	<p>目的 : 指定されたリモートホストに接続し、SSHを使用して、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。</p> <div><p>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)。</p></div> <p>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、このホストによって直接提供される管理ツールを使用する必要があります。たとえば、ルーターやその他の「スマート」デバイスの場合は、ファームウェア更新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は、コンピューティングマシンへの接続 (任意でリモート端末モードを使用) と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)、またはコンピューティングマシン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の実行を介して実行できます。</p> <p>引数 :</p> <p><host> - リモートホストの IP アドレスまたはドメイン名。</p> <p><path> - スキャンの対象として選択されたファイルやディレクトリへのパスです。</p>



コマンド	説明
	<p>オプション:</p> <p><code>-m [--Method] <SSH/Telnet></code> - リモートホスト接続方法(プロトコル)。 方法が指定されていない場合は、SSHが使用されます。</p> <p><code>-l [--Login] <name></code> - 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)。 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。</p> <p><code>-i [--Identity] <path to file></code> - 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。</p> <p><code>-p [--Port] <number></code> - 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。 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 (SSHは22、Telnetは23)</p> <p><code>--Password <password></code> - 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。 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。</p> <p><code>--Exclude <path></code> - チェックから除外するパス(マスク記号*と?は使用できません)。 任意オプション、複数回設定できます。</p> <p><code>--Report <type></code> - スキャンレポートのタイプを指定します。 使用可能な値:</p> <ul style="list-style-type: none">• 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。 <p>デフォルト値: <i>BRIEF</i></p> <p><code>--ScanTimeout <number></code> - 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</p> <p><code>--PackerMaxLevel <number></code> - 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</p> <p><code>--ArchiveMaxLevel <number></code> - 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</p> <p><code>--MailMaxLevel <number></code> - 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。</p>



コマンド	説明
	<p>デフォルト値 : 8</p> <p>--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。</p> <p>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。</p> <p>デフォルト値 : 8</p> <p>--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。</p> <p>率は 2 以上にする必要があります。</p> <p>デフォルト値 : 3000</p> <p>--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。</p> <p>デフォルト値 : On</p>

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。

コマンド	説明
update	<p>目的 : 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はウイルスデータベース、アンチウイルスエンジンなど) の更新プロセスを開始するように指示し、既に実行されている更新プロセスを終了するか、最後の更新を以前に更新したファイルのバージョンにロールバックします。</p> <div> <i>Dr.Web for UNIX File Serversが集中管理サーバーに接続されている場合、このコマンドは無効です。</i></div> <p>引数 : None</p> <p>オプション :</p> <p>-l [--local-cloud] - Dr.Web MeshDに接続されている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。オプションが指定されていない場合、更新はDr.Web更新サーバーからダウンロードされます (デフォルト)。</p> <p>--Rollback - 最終更新をロールバックし、最終更新時に更新された前のバージョンのファイルを復元します。</p> <p>--Stop - 実行中の更新プロセスを終了します。</p>
esconnect <server>[:<port>]	<p>目的 : Dr.Web for UNIX File Servers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。詳細は、動作モードを参照してください。</p> <p>引数 :</p> <ul style="list-style-type: none"><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。この項目は必須です。



コマンド	説明
	<ul style="list-style-type: none">• <port> - 中管理サーバーによって使用されるポート番号。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。 <p>オプション:</p> <p>--Certificate <path>—接続先の集中管理サーバーの証明書へのファイルパス。</p> <p>--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)。</p> <p>--Password <password> - 集中管理サーバーへの接続用パスワード。</p> <p>--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。</p> <p>--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(--Groupオプションと一緒にのみ指定できます)。</p> <p>--Compress <On/Off>—データの圧縮を有効(<i>On</i>)または無効(<i>Off</i>)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。</p> <p>--Encrypt <On/Off>—データの暗号化を有効(<i>On</i>)または無効(<i>Off</i>)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。</p> <p>--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)。</p> <div> このコマンドでは、drweb-ctlをルート権限で起動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。</div>
esdisconnect	<p>目的 : Dr.Web for UNIX File Servers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ーンモードに切り替えます。</p> <div> <i>Dr.Web for UNIX File Serversがスタンドアローンモードで既に動作している場合、このコマンドは無効になります。</i></div> <p>引数 : None</p> <p>オプション : None</p> <div> このコマンドでは、drweb-ctlをルート権限で起動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。</div>



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
<code>cfset</code> <code><section>. <parameter></code> <code><value></code>	<p>目的: 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。</p> <p>"="(等号)はできないことに注意してください。</p> <p>引数:</p> <ul style="list-style-type: none">• <code><section></code> - 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。• <code><parameter></code> - パラメータの名前です。この引数は必須です。• <code><value></code> - パラメータに割り当てられる新しい値です。この引数は必須です。 <div> パラメータ値の設定には <code><section>. <parameter> <value></code> のフォーマットを常に使用します。</div> <p>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<code>cfset</code>の呼び出しを繰り返す必要があります。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<code>-a</code>を使用する必要があります(以下参照)。文字列<code>value1</code>、<code>value2</code>は単一のパラメータ値と見なされるため、コマンドオプション<code><parameter> value1</code>、<code>value2</code>は使用できません。</p> <p>設定ファイルの説明については、付録D. Dr.Web for UNIX File Servers設定ファイルセクション、または<code>man 5 drweb.ini</code>で表示されるドキュメントページを参照してください。</p> <p>オプション:</p> <p><code>-a</code> [<code>--Add</code>] - 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。</p> <p><code>-e</code> [<code>--Erase</code>] - 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)。このオプションを使用して、タグ付きのパラメータのグループ全体を削除することもできます。</p> <p><code>-r</code> [<code>--Reset</code>] - 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 <code><value></code> は必要なく、指定された場合は無視されます。</p> <p>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。</p>



コマンド	説明
	<p>Dr.Web ClamDコンポーネントへのさまざまな接続ポイントで個別パラメータ設定を含むセクション、またはSpIDer Guard for SMBモニターでは、個別のパラメータ設定がされているセクションに<code>-r</code>オプションを使用すると、そのパラメータ値は、このコンポーネントの一般設定セクションにある同じ名前の「親」パラメータの値に変更されます。</p> <p>Dr.Web ClamD用に新しい接続ポイント <code><point></code> を追加する必要がある場合は、以下のコマンドを使用します。<code><tag></code> を使用して Dr.Web ClamD または Samba 共有ディレクトリのパラメータを含むセクションに新しい接続ポイントを追加する必要がある場合は、以下のコマンドを使用します。</p> <pre>cfset ClamD.Endpoint.<point> -a 例： cfset ClamD.Endpoint.point1 -a cfset SmbSpider.Share.<tag> -a 例： cfset SmbSpider.Share.BuhFiles -a</pre> <div> このコマンドでは、drweb-ctl をルート権限で起動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。</div>
<code>cfshow</code> [<code><section></code>] [. <code><parameter></code>]	<p>目的： 現在の設定のパラメータ値を表示します。パラメータは <code><section></code>、<code><parameter></code> = <code><value></code> のように画面に出力されます。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。</p> <p>引数：</p> <ul style="list-style-type: none"><code><section></code> - 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。<code><parameter></code> - 表示するパラメータの名前です。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。 <p>オプション：</p> <p><code>--Uncut</code> - 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。</p> <p><code>--Changed</code> - デフォルト値とは異なる値を持つパラメータのみを出力します。</p> <p><code>--Ini</code> - パラメータ値をINIファイルフォーマットで表示します。まず鍵括弧内でセクション名が指定され、次に <code><parameter></code> = <code><value></code> 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）。</p> <p><code>--Value</code> - 指定されたパラメータの値のみを出力します（この場合、<code><parameter></code> 引数は必須です）。</p>
<code>reload</code>	<p>目的： SIGHUP シグナルを Dr.Web ConfigD 設定デーモンに送信します。</p>



コマンド	説明
	<p>このシグナルを受信すると、Dr.Web ConfigD設定デモンは設定を再度読み込み、それに必要な変更をDr.Web for UNIX File Serversコンポーネントに送信します。その後、設定デモンはプログラムログを再度開き、ウイルスデータベースを使用するコンポーネント（アンチウイルスエンジンを含む）を再起動し、異常終了したコンポーネントの再起動を試みます。</p> <p>引数：None</p> <p>オプション：None</p>

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
<code>threats</code> [<i><action></i> <i><object></i>]	<p>目的：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のオプションによって指定します。</p> <p>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<code>--Format</code>引数で指定されたフォーマットに従って表示されます。<code>--Format</code>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。</p> <ul style="list-style-type: none">• 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の使用する分類による脅威のタイプ）• 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） <p>引数：None</p> <p>オプション：</p> <p><code>--Format " <format string> "</code> - 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。</p> <p>このオプションを下のオプションと一緒に適用すると無視されます。</p> <p><code>-f [--Follow]</code> - 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）。</p> <p>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。</p> <p><code>--Directory <list of directories> - <list of directories></code>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。</p> <p>このオプションを下のオプションと一緒に適用すると無視されます。</p> <p><code>--Cure <threat list></code> - リストアップ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ってリストアップ）。</p>



コマンド	説明
	<p>--Quarantine <threat list> - リストアップされた脅威を隔離に移します（脅威のIDをコンマで区切ってリストアップ）。</p> <p>--Delete <threat list> - リストアップされた脅威を削除します（脅威の識別子をコンマで区切ってリストアップ）。</p> <p>--Ignore <threat list> - リストアップされた脅威を無視します（脅威の識別子をコンマで区切ってリストアップ）。</p> <p>検出されたすべての脅威に対してコマンド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：</p> <pre>\$ drweb-ctl threats --Quarantine All</pre> <p>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。</p>
quarantine [<action> <object>]	<p>目的：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。</p> <p>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次の情報が表示されます。</p> <ul style="list-style-type: none">• 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の使用する分類による脅威のタイプ） <p>引数：None</p> <p>オプション：</p> <p>-a [--Autonomous] - 指定された隔離コマンドを実行するファイルをチェックするためにDr.Web File Checkerコンポーネントの別のインスタンスを起動し、コマンド完了後にシャットダウンします。</p> <p>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。</p> <p>--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。</p> <p>このオプションを下のオプションと一緒に適用すると無視されます。</p> <p>-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）。</p> <p>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。</p> <p>--Discovery [<list of directories>] - 指定されたディレクトリのリストから隔離ディレクトリを検索し、脅威が検出された場合は統合された隔離ディレクトリに追加します。<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（ボリュームのマウントポイントとユーザーのホームディレクトリ）で隔離ディレクトリを検索します。</p>



コマンド	説明
	<p>このオプションは <code>-a</code> (<code>--Autonomous</code>) 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 <code>quarantine</code> コマンドを起動すると (<code>-a</code> (<code>--Autonomous</code>) オプションを指定して、<code>--Discovery</code> 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。</p> <pre>quarantine --Autonomous --Discovery</pre> <p><code>--Delete <object></code> - 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。</p> <p><code>--Cure <object></code> - 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 <code>--Restore</code> コマンドを使用します。</p> <p><code>--Restore <object></code> - 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 をスーパーユーザー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。</p> <p><code>--TargetPath <path></code> - 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 (<code><path></code> 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 (<code><path></code> がディレクトリへのパスであった場合)。<code>--Restore</code> コマンドとの組み合わせでのみ使用できます。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)。</p> <p><code><object></code> 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コマンドを適用する場合は、<code><object></code> の代わりに <code>All</code> を指定してください。例：</p> <pre>\$ drweb-ctl quarantine --Restore All --TargetPath test</pre> <p>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 <code>test</code> サブディレクトリに復元します。</p> <p><code>--Restore All</code> では、追加のオプション <code>--TargetPath</code> (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。</p>



隔離アクションが、*SpIDer Guard for NSS*の**設定**で、ある脅威のタイプに指定される場合、このタイプの脅威を含むオブジェクトは、`quarantine`コマンドでこのオブジェクトを隔離からNSSボリュームへの復元を試みる際に、再び隔離に配置されます。たとえば、次のデフォルト設定があります。

```
NSS.OnKnownVirus = Cure
NSS.OnIncurable = Quarantine
```

修復不可能なオブジェクトは全て隔離に移動します。これが、`quarantine`コマンドによって修復不可能なオブジェクトが隔離からNSSボリュームに復元されると、自動的に隔離に戻される理由です。

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、出力中に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、共通の記号（「そのまま」で表示されるもの）を含めることができます。以下のマーカーが利用可能です。

1. `threats`と`quarantine`コマンドに共通:

マーカー	説明
<code>%{n}</code>	新しい文字列
<code>%{t}</code>	集計
<code>%{threat_name}</code>	Doctor Webの分類に従って検出された脅威（ウイルス）の名前
<code>%{threat_type}</code>	Doctor Webの分類に従った脅威のタイプ（「既知のウイルス」など）
<code>%{size}</code>	元のファイルサイズ
<code>%{origin}</code>	パスを含む元のファイルのフルネーム
<code>%{path}</code>	<code>%{origin}</code> の同義語
<code>%{ctime}</code>	元のファイルが変更された日時（「 <code>%Y-%b-%d %H:%M:%S</code> 」フォーマット、例：2018-Jul-20 15:58:01）
<code>%{timestamp}</code>	<code>%{ctime}</code> と似ているが、UNIXのタイムスタンプフォーマット
<code>%{owner}</code>	元のファイル所有者のユーザー名
<code>%{rowner}</code>	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
<code>%{hid}</code>	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
<code>%{tid}</code>	脅威のID



マーカー	説明
%{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 UNIX File ServersコンポーネントのID
%{event}	脅威に関連する最新イベント: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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	<p>目的: アクティブな Dr.Web for UNIX File Serversコンポーネントに関する情報を出力します。</p> <p>現在実行中の各コンポーネントについて、次の情報が表示されます。</p> <ul style="list-style-type: none">• 内部で使用する名前• プロセスID GNU/Linux (PID)• 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) <p>設定デーモン (Dr.Web ConfigD) については、以下の追加情報が表示されます。</p> <ul style="list-style-type: none">• インストールされたコンポーネントのリスト — <i>Installed</i>• 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 — <i>Should run</i> <p>引数: None</p> <p>オプション:</p> <p>-f [--Follow] - コンポーネントのステータス変更に関する新しいメッセージを待ち、それらを受け取り次 第メッセージを出力します (Ctrl + Cキーを押して待機を中断します)。</p>
baseinfo	<p>目的: Virus-Finding Engine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。</p> <p>以下の情報が表示されます。</p> <ul style="list-style-type: none">• アンチウイルス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アンチウイルス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の自動更新の時間 <p>引数: None</p> <p>オプション:</p> <p>-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。</p>
certificate	<p>目的: Dr.Web for UNIX File Serversによって使用される Dr.Webの信頼できる証明書の内容を表示します。証明書を <cert_name>.pemファイルに保存するには、次のコマンドを使用できます。</p> <div><pre>\$ drweb-ctl certificate > <cert_name>.pem</pre></div> <p>引数: None</p>



コマンド	説明
	オプション: None
events	<p>機能: Dr.Web for UNIX File Servers 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。</p> <p>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。</p> <p>オプション:</p> <p>--Report <i><type></i> - イベントレポートのタイプを指定します。</p> <p>使用可能な値:</p> <ul style="list-style-type: none">• 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 <p>-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)。</p> <p>-s [--Since] <i><date, time></i> - 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 (<i><date, time></i> は YYYY-MM-DD hh:mm:ss のフォーマットで指定します)。</p> <p>-u [--Until] <i><date, time></i> - 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 (<i><date, time></i> は YYYY-MM-DD hh:mm:ss のフォーマットで指定します)。</p> <p>-t [--Types] <i><type list></i> - 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)。</p> <p>次のイベントタイプを使用できます。</p> <ul style="list-style-type: none">• 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 <p>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。</p> <p>--ShowSeen - 既読イベントも表示されます。</p> <p>--Show <i><list of events></i> - 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)。</p> <p>--Delete <i><list of events></i> - 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)。</p> <p>--MarkAsSeen <i><list of events></i> - 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)。</p> <p>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、<i><events list></i> ではなく All を指定します。例:</p> <pre>\$ drweb-ctl --MarkAsSeen --All</pre>
report	<p>機能: Dr.Web for UNIX File Servers 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)。</p> <p>引数:</p>



コマンド	説明
	<p><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 <code>events</code> コマンドの <code>--Types</code> 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。</p> <p>オプション:</p> <p><code>-o [--Output] <path to file></code> - 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。</p> <p><code>-s [--Since] <date, time></code> - 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)。</p> <p><code>-u [--Until] <date, time></code> - 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)。</p> <p><code>--TemplateDir <path to directory></code> - 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。</p> <p><code>-s</code>、<code>-u</code>、<code>--TemplateDir</code>は必須のオプションではありません。</p> <div><pre>\$ drweb-ctl --report Mail -o report.html</pre></div> <p>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 <code>report.html</code> ファイルに保存します。</p>
<code>idpass <identifier></code>	<p>目的: 指定されたIDを持つメールメッセージに対する、Dr.Web MailDによって生成され、メールメッセージから削除された脅威を含むアーカイブの保護に使用された、パスワードを表示します(つまり、<code>RepackPassword</code>パラメータが" HMAC (<secret>)"に設定されている場合のユニークなパスワード)。</p> <p>引数:</p> <ul style="list-style-type: none">• <identifier> - メールメッセージのID。 <p>オプション:</p> <p><code>-s [--Secret] <secret></code> - アーカイブパスワードの生成に使用される秘密のワード。</p> <p>コマンド呼び出し時に秘密のワードが示されていない場合は、現在の秘密のワード<secret>が使用されます。Dr.Web MailD設定に示されます。また、<code>RepackPassword</code>パラメータが利用できない場合、またはHMAC(<secret>) と異なる値に設定されている場合、コマンドはエラーを返します。</p>
<code>license</code>	<p>目的: 現在有効化されているライセンスに関する情報を表示、あるいはデモバージョンのライセンスを取得、あるい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。</p> <p>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(スタンドアローンモードのライセンスを使用している場合):</p> <ul style="list-style-type: none">• ライセンス番号• ライセンスの有効期限が切れる日時



コマンド	説明
	<p>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）、以下の情報が表示されます。</p> <p>引数：None</p> <p>オプション：</p> <p>--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。</p> <p>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。</p> <p>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セクションをご確認ください。</p> <div> シリアル番号を取得するには、インターネット接続が必要です。</div>
log	<p>目的：最後のプログラム複合ログレコードを（<code>stdout</code>ストリームで）コンソール画面に表示します（tailコマンドと同様）。</p> <p>引数：None</p> <p>オプション：</p> <p>-s [--Size] <number> - 表示される最後のログレコードの数。定義値が0の場合、全てのレコードが表示されます。引数が定義されていない場合は、最後の10件のレコードが表示されます。</p> <p>-c [--Components] <components list> - 表示する必要があるレコードのコンポーネントID。IDはコンマ区切りで定義されます。引数が定義されていない場合、全てのコンポーネントによって作成された使用可能なレコードが全て表示されます。</p> <p>現在のID（ログに表示される内部コンポーネント名など）は、のDr.Web for UNIX File Serversの構成のセクションに記載されています。また、<code>appinfo</code>コマンドを使ってそれらを取得できます（上を参照）。</p> <p>-f [--Follow] - ログで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）。</p>
stat	<p>目的：ファイル进行处理するコンポーネントの操作（CTRL + CまたはQを押すと統計表示が中断されます）、またはネットワークデータスキャンエージェントDr.Web Network Checkerの操作に関する統計を出力します。</p> <p>出力される統計情報には次が含まれます。</p> <ul style="list-style-type: none">スキャンを開始したコンポーネントの名前コンポーネントのPID最後の1分/5分/15分間に処理された1秒あたりのファイルの平均数スキャンしたファイルのキャッシュの使用率。1秒あたりの平均スキャンエラー数。 <p>分散されたスキャンエージェントの場合、次の情報が出力されます。</p>



コマンド	説明
	<ul style="list-style-type: none">• スキャンを開始したローカルコンポーネントのリスト• スキャン用のファイルを受信したリモートホストのリスト• スキャン用のファイルを送信したリモートホストのリスト <p>分散されたスキャンエージェントのローカルクライアントの場合、そのPIDと名前が指定されます。リモートクライアントの場合は、ホストのアドレスとポートが指定されます。</p> <p>ローカルとリモートの両方のクライアントに対して、次の情報が出力されます。</p> <ul style="list-style-type: none">• 1秒間にスキャンされたファイルの平均数• 1秒あたりの平均送受信バイト数• 1秒あたりの平均エラー数 <p>引数: None</p> <p>オプション:</p> <p>-n [--netcheck] - ネットワークデータスキャンエージェントの動作に関する統計情報。</p>

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 procsan
```

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**の操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見捨て、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. 設定の管理

1. 実行中のプロセスに関するものを含む、現在のDr.Web for UNIX File Servers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、以下の例に示すように、**sudo**コマンドを使用できます。

```
$ sudo drweb-ctl cfset LinuxSpider.Start No
```

4. Dr.Web for UNIX File Servers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 UNIX File Servers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、以下の例に示すように、**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 UNIX File Servers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. Dr.Web for UNIX File Servers 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、以下の例に示すように、**sudo**コマンドを使用できます。

```
$ sudo drweb-ctl esdisconnect
```

8. **drweb-update**と**drweb-configd**によってDr.Web for UNIX File Servers 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します。

```
$ 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します。

```
$ drweb-ctl threats --Quarantine All
```

3. 隔離されたファイルのリストを表示します。

```
$ drweb-ctl quarantine
```

4. 隔離からすべてのファイルを復元します。

```
$ 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、隔離します。

```
$ 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。

設定パラメータ

コマンドラインから製品を管理するためのDr.Web Ctlツールには、Dr.Web for UNIX File Serversの統合[設定ファイル](#)にパラメータを含む独自のセクションはありません。設定ファイルの[Root] [セクション](#)に指定されているパラメータを使用します



Dr.Web Web管理インターフェース

このセクションの内容:

- [概要](#)
- [コンポーネントを管理する](#)
- [脅威の管理](#)
- [設定を管理する](#)
- [ローカルファイルをスキャンする](#)

概要

Dr.Web for UNIX File ServersのWebインターフェースでは、以下の操作が可能です。

1. Dr.Web for UNIX File Serversコンポーネントの現在の状態を表示し、一部のコンポーネントを起動または停止します。
2. 更新のステータスを表示し、必要に応じて手動で更新プロセスを開始します。
3. 製品ライセンスのステータスを表示し、必要に応じてライセンスキーをロードします。
4. 検出された脅威のリストを表示し、隔離されたオブジェクトを管理します ([Dr.Web File Checker](#)コンポーネントを使用してローカルファイルシステムで検出された脅威のみが表示されます)。
5. Dr.Web for UNIX File Serversに含まれるコンポーネントの設定を編集します。
6. Dr.Web for UNIX File Serversを集中管理サーバーに接続するか、スタンドアロンモードに切り替えます。
7. ローカルファイルのオンデマンドスキャンを開始します (ブラウザで開いたページにファイルをドラッグ&ドロップして実行する機能も含まれます)。

Webインターフェースのシステム要件

以下のWebブラウザでは、Webインターフェースが正常に動作することが保証されています。

- **Microsoft Internet Explorer**-バージョン11以降。
- **Mozilla Firefox**-バージョン25以降。
- **Google Chrome**-バージョン30以降。

Webインターフェースにアクセスする

Webインターフェースにアクセスするには、ブラウザのアドレスバーに次のようなアドレスを入力します。

```
https:// <host_with_drweb>: <port>/
```

ここで、<host_with_drweb>は、Dr.Web for UNIX File ServersがDr.Web HTTPD Webインターフェースサーバーで動作するホストのIPアドレスまたは名前、<port>は、Dr.Web HTTPDがリッスンしている(このホスト上の)ポートです。ローカルホスト上で動作するDr.Web for UNIX File Serversコンポーネントにアクセスするには、IPアドレス127.0.0.1または名前localhostを使用します。[デフォルト](#)では、<port>は4443です。



したがって、デフォルトではローカルホストのWebインターフェースにアクセスするために、ブラウザのアドレスバーに次のURLを入力します。

```
https://127.0.0.1:4443/
```

管理サーバーとの接続が確立すると、スタートアップページが開き、認証フォームが表示されます。管理機能にアクセスするには、Dr.Web for UNIX File Serversが動作しているホスト上で管理権限を持つユーザーのログインとパスワードを指定して、認証フォームに入力します。

必要に応じて、個人ユーザー証明書を使用してWebインターフェースで認証を提供できます。その手順は下記です：

1. 認証局証明書で署名された個人証明書を作成します。
2. 管理用のWebインターフェースに接続するために使用されるブラウザで、署名済み証明書をユーザー認証証明書としてインポートします。
3. Dr.Web HTTPD [設定](#) (パラメータ `AdminSslCA`) で、個人証明書に署名する認証局証明書へのパスを指定します。

Webインターフェースでの許可に個人ユーザー証明書を使用する場合、許可フォームは表示されず、ユーザーは `root` として許可されます。

必要に応じて、[の付録E. SSL証明書を生成する](#)セクションを参照してください。

メインメニュー

認証に成功すると表示されるWebインターフェースの左ペインにメインメニューがあります。そのメニューアイテムでは以下の操作を実行できます。

- **メイン** - Dr.Web for UNIX File Serversのインストール済みコンポーネントとそのステータスの全リストを表示する [メインページ](#)を開きます。
- **脅威** - サーバー上で検出された [すべての脅威を表示する](#) ページを開きます。このセクションでは、これらの検出された脅威を管理できます（感染したオブジェクトの隔離、検出された悪意のあるオブジェクトの再スキャン、修復、削除など）。
- **設定** - サーバーにインストールされているDr.Web for UNIX File Serversの [コンポーネント設定](#) のページを開きます。
- **情報** - このWebインターフェースのバージョンとウイルスデータベースの状態に関する簡単な情報を表示するページを開きます。
- **ヘルプ** - Dr.Web for UNIX製品のヘルプ情報を含む新しいブラウザタブを開きます。
- **ファイルをスキャン** - [ファイルをすばやくスキャンする](#) ためのパネルを表示します。このパネルは、閉じられるまでWebインターフェースの開いているページの上部に表示されます。
- **ログアウト** - 現在のWebインターフェースセッションを終了します（ユーザーの個人証明書による認証には使用できません）。




コンポーネントを管理する


メインページでは、Dr.Web for UNIX File Serversに含まれるコンポーネントのリストを表示したり、それらの動作を管理したりすることができます。



リスト上にあるDr.Web for UNIX File Serversのコンポーネントは、脅威を監視するメインコンポーネントと、Dr.Web for UNIX File Serversが正常に動作するよう全体的に管理するサービスコンポーネントの2つのグループに分けられます。メインコンポーネントのリストは、ページ上部に表形式で表示されます（コンポーネントのリストは、ディストリビューション範囲によって異なります）。コンポーネントごとに、以下の情報が表示されます。

1. **名前**。名前をクリックすると、このコンポーネントの設定を含む[設定ページ](#)が開きます。
2. **状態**。コンポーネントの状態は、スイッチアイコンとコンポーネントの現在の状態に関するメモによって示されます。スイッチをクリックするだけで、コンポーネントを開始または中断できます。スイッチの状態には次のようなものがあります。

	- コンポーネントが無効になっているため、使用されていません。
	- コンポーネントが有効になっており、正しく動作しています。
	- コンポーネントは有効になっていますが、エラーにより動作していません。

コンポーネントの動作中にエラーが発生した場合は、コンポーネントの状態に関するメモではなく、エラーメッセージが表示されます。 アイコンをクリックすると、発生したエラーに関する詳細情報とエラーを解決するための推奨事項がウィンドウに表示されます。

3. **読み込み**。過去1分間、5分間、15分間に、コンポーネントによって1秒間に処理されたファイルの平均数がそれぞれ表示されます（3つの数字がスラッシュ「/」で区切られて表示されます）。
4. **エラー**。過去1分間、5分間、15分間にコンポーネントで1秒間に検出されたエラーの平均数がそれぞれ表示されます（3つの数字がスラッシュ「/」で区切られて表示されます）。

ツールチップを表示するには、 アイコンの上にカーソルを置きます。

メインコンポーネントに関する情報を提供する表の下に、サービスDr.Web for UNIX File Serversコンポーネント（[スキャンエンジン](#)、[ファイルスキャンコンポーネント](#)など）がタイル表示されます。サービスコンポーネントごとに、その状態と動作統計も表示されます。これらのコンポーネントの設定ページを開くには、必要なコンポーネントの名前をクリックします。通常、これらのコンポーネントは必要に応じて自動的に開始または停止されます。ユーザーによって手動で開始および停止される可能性があるサービスコンポーネントについては、名前および動作統計の他に、コンポーネントを開始および停止するためのスイッチもタイルに表示されます。

ページの下部には、ウイルスデータベースが最新かどうかという情報と、[ライセンス](#)情報が表示されます。ウイルスデータベースの強制アップデートを実行するには、[更新](#)をクリックします。[更新ボタン](#)（またはライセンスの現在の状態によっては[ライセンスをアクティブ化ボタン](#)）をクリックすると、Dr.Web for UNIX File Serversに対して有効なキーファイルをライセンスサーバーにアップロードしてライセンスを更新または有効化できます。

脅威の管理

脅威ページで、検出された脅威の一覧を表示し、それらに対する対応を管理できます。

このページには、ファイルシステムを監視およびスキャンするDr.Web for UNIX File Serversのコンポーネント（ネットワークトラフィックをスキャンするコンポーネントは除く）によって検出された脅威のすべてのリストが含まれています。ページ上部には、カテゴリー別に脅威にフィルターを適用できるメニューがあります。

- **ライセンスを有効化** - 検出されたすべての脅威（アクティブな脅威と隔離された脅威の両方を含む）を表示します。
- **アクティブ** - アクティブな（検出されたがまだ駆除されていない）脅威のみを表示します。



- **ブロック済** - ブロックされているすべての脅威、つまり中和されていないが、それを含む感染オブジェクトがブロックされている脅威をすべて表示します (SpIDer Guard for SMBIによって監視されているファイルストレージのみ)。
- **隔離済** - 隔離に移された脅威を表示します。
- **エラー** - エラーのために処理されなかった脅威を示します。

上部メニューの脅威カテゴリーの名称の隣 (右側) には、このカテゴリーに分類される検出済みの脅威の数が表示されます。そのカテゴリーに属する脅威が現在表示され、選択されているカテゴリーは、暗い色のフォントで強調されています。必要なカテゴリーの脅威を表示するには、メニューのカテゴリーの名前をクリックしてください。

脅威ごとに次の情報が一覧表示されています。




- **ファイル** - 悪意のあるオブジェクトを含むファイルの名前 (ファイルパスは指定されていません)。
- **所有者** - 感染ファイルを所有するユーザーの名前。
- **コンポーネント** - 脅威を検出したDr.Web for UNIX File Serversのコンポーネントの名前。
- **脅威** - (Doctor Web社の使用する分類に従い) ファイルで検出された脅威の名前。

リストで選択されているオブジェクトについては、以下の情報が表示されます。

- 脅威の名前 (Dr.Webウイルス情報ライブラリのページを開くと、その脅威の説明が表示されます)。
- ファイルのサイズ、Byte単位。
- 脅威を検出したコンポーネントの名前。
- 脅威が検出された日時。
- 脅威が最後に変更された日時。
- 感染ファイルを所有しているユーザーの名前。
- ファイルの所有者を含むグループの名前。
- ファイルをファイルサーバーにアップロードしたユーザーの名前 (SpIDer Guard for SMBIによって監視されているファイルストレージの場合のみ)。
- 脅威を含む隔離ファイルに割り当てられた識別子 (ファイルが隔離された場合)。
- ファイルの元の場所 (脅威の検出時にファイルが存在していた場所) を指すフルパス。

リスト内の任意のオブジェクトをクリックして選択できます。複数のオブジェクトを選択するには、対応するオブジェクトのチェックボックスを選択します。すべてのオブジェクトを選択するか選択をキャンセルするには、脅威リストのヘッダーのファイルフィールドのチェックボックスをオンにします。

リストで選択したオブジェクトにアクションを適用するには、脅威リストの真上にあるツールバーの対応するボタンをクリックします。ツールバーには、次のボタンがあります (選択した脅威の種類によっては、使用できないボタンがあります)。

	- 選択されたファイルを削除する (すなわち、永久に削除する) ように指示します。
	- 選択したファイルを隔離領域から元の場所に復元するように指示します。
	- 選択したファイルに追加のアクションを適用するように指示します (使用可能な操作はドロップダウンリストで指定します)。 <ul style="list-style-type: none">• 隔離 - 脅威を含む選択したファイルを隔離するように指示します



- 修復 - 脅威を修復しようとします
- 無視 - 選択したファイルで検出された脅威を無視し、リストから脅威を削除するように指示します



NSSボリュームで検出された脅威を管理するには、SpIDer Guard for NSSをインストールして起動する必要があります。

NSSボリュームを監視するSpIDer Guard for NSSの設定で、ある脅威の種類に対して自動的に適用されるべきアクションとしてQuarantineが指定されている場合、この種類の脅威を含むオブジェクトは、隔離からNSSボリュームへの復元が試行される際に、再び隔離に配置されます。たとえば、このモニターのデフォルト設定では、すべての修復不可能なオブジェクトが隔離されます。これが、修復不可能なオブジェクトが隔離からNSSボリュームに復元されると、自動的に隔離に戻る理由です。

検索クエリーに基づいて表示された脅威にフィルターを適用することもできます。フィルターを適用して不要な脅威を除外してクエリーに対応するものだけを表示するには、検索ボックスを使用します。検索ボックスはツールバーの右側に 🔍 マークと一緒に表示されています。脅威リストにフィルターを適用するには、検索ボックスに単語を入力します。名前や説明に入力した単語が含まれていない脅威はすべて非表示になります（このフィルターの適用では大文字と小文字が区別されません）。検索結果を消去してフィルターを適用していないリストを表示するには、検索ボックスの ✕ をクリックするか、単語を消去します。

設定を管理する

Dr.Web for UNIX File Serversに含まれ、[メインページ](#)に一覧表示されているコンポーネントの現在の[設定パラメータ](#)を表示、変更できます。そのためには、[設定ページ](#)を開きます。このページでは、Dr.Web for UNIX File Serversを[集中管理モード](#)または[スタンドアロンモード](#)に切り替えることもできます（これらのモードの詳細については、管理者マニュアルの[動作モード](#)を参照してください）。

ページの左側に表示されるメニューには、設定を表示、調整できるすべてのDr.Web for UNIX File Serversのコンポーネント名が含まれています。任意のコンポーネントの設定を表示、調整するには、まずこのメニューで該当するコンポーネント名をクリックします。現在、設定の表示および編集を行っているコンポーネントの名前は左側のメニューに強調表示されます。

- メニューの[集中管理](#)の項目を選択すると、集中管理モードを[管理するページ](#)に移動します。
- メニューの[全般設定](#)の項目は、Dr.Web ConfigDコンポーネントの[設定](#)に対応しています。これは、Dr.Web for UNIX File Serversの全体的な機能を担っています。

コンポーネントにメイン設定のセクションとは別の追加設定のセクションがある場合（たとえば、そのようなセクションはDr.Web ClamDコンポーネントで使用可能で、**ClamAV®** アンチウイルスのインターフェースをエミュレートしてこれらの追加セクションを使用し、異なる接続アドレスを使用するクライアントごとに個別のスキャンパラメータを保持します）、追加のセクションを展開したり折りたたんだりできることを示すアイコンがコンポーネント名の左側に表示されます。アイコンが ▶ の場合、追加のセクションは非表示になります。アイコンが ▼ の場合は、追加のセクションが1行に1つずつメニューに表示されます。追加セクションのリストを展開したり折りたたんだりするには、必要なコンポーネントの名前の横にある展開・折りたたみアイコンをクリックします。



- 設定を含む追加のセクションは、インデントラインとして表示されます。追加セクションのパラメータを表示または編集するには、その名前をクリックします。



- コンポーネントの設定を含む下位セクションの追加が許可されている場合、コンポーネント名の右側にある \oplus をクリックして追加します。次に、新しいサブセクションに一意の名前(タグ)を指定して、**OK**をクリックします。サブセクションを作成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。
- コンポーネントのサブセクションを削除するには、コンポーネント名にカーソルを合わせると表示されるサブセクション名(タグ)の右側の \times をクリックします。次に、サブセクションを削除することを確認してはいをクリックするか、いいえをクリックしてサブセクションを削除せずにウィンドウを閉じます。

設定ページの上部には、表示モードを変更できるメニューがあります。以下のモードが利用可能です。

- **ライセンスを有効化** - 表示および調整可能なすべてのコンポーネントの設定パラメータを含むテーブルを表示します。
- **変更** - デフォルトとは異なる値を持つコンポーネントの設定パラメータを含むテーブルを表示します。
- **Ini エディタ** - デフォルト設定とは異なる値を持つこのコンポーネントの設定パラメータを使用してテキストエディタを表示します。表示されるテキストは、[設定ファイル](#)と同じ形式です(パラメータ= 値のペアを含みます)。

検索クエリーに基づいて表示されたパラメータにフィルターを適用することもできます。フィルターを適用して不要なパラメータを除外し、クエリーに対応するものだけを表示するには、検索ボックスを使用します。検索ボックスは表示モードメニューの右側に  マークと一緒に表示されています。パラメータリストにフィルターを適用するには、検索ボックスに任意の単語を入力します。説明に入力した単語が含まれていないパラメータはすべて非表示になります(このフィルターの適用では大文字と小文字が区別されません)。検索結果を消去してフィルターを適用していないリストを表示するには、検索ボックスの  をクリックするか、その中の単語を消去します。

パラメータが表形式で表示されている場合(つまり、**ライセンスを有効化**表示モードと**変更**表示モード)にのみ、フィルターを適用してパラメータを除外できます。

表形式でコンポーネント設定を表示、編集する

表形式でパラメータを表示する場合(**ライセンスを有効化**表示モードと**変更**表示モード)、各表の行にはパラメータの名前と説明(左側)およびその現在値(右側)が含まれます。Boolean値パラメータ(使用可能な値が2つのみの場合、「はい」と「いいえ」)では、値の代わりにチェックボックスが表示されます(チェックを入れると「はい」を、チェックしないと「いいえ」を意味します)。



(変更されたものだけでなく)すべてのパラメータを表示するように選択した場合、変更された(デフォルト以外の)値は太字で示されます。

完全なパラメータリストはグループに分割されます(全般、アドバンスなど)。グループを折りたたむまたは展開するには、その見出し(名前)をクリックします。グループが折りたたまれていて、そのパラメータが表に表示されていない場合は、グループ名の左側に \triangleright のアイコンが表示されます。グループが展開されてテーブルにパラメータが表示されると、 \blacktriangledown のアイコンがグループ名の左側に表示されます。

パラメータを調整するには、表内の現在の値をクリックします(Boolean値パラメータの場合は、対応するチェックボックスのチェックマークを設定または削除します)。パラメータに一連の定義済みの値がある場合は、現在の値をクリックした後にすべてドロップダウンリストとして表示されます。パラメータに数値がある場合は、現在の値をクリックした後に編集ボックスが表示されます。必要な値を指定して、ENTERを押してください。以下の図は、パラメータ値を変更する方法の例を示しています(図に示されているコンポーネントのセットは、提供されているものとは異なる可能性があることに注意してください)。パラメータ値に対するすべての変更は、対応するコンポーネントの設定にすぐに適用されます。



図3. 表形式のコンポーネント設定

パラメータがその値として文字列を要求しているか、任意の値のリストを受け付ける場合は、パラメータの現在の値をクリックして編集すると、ポップアップウィンドウが表示されます。パラメータが値のリストを受け付ける場合は、次の図に示すように複数行の編集ボックスに表示されます（1行に1つの値）。一覧表示されている値を編集するには、編集ボックスで必要な行を変更、削除、または追加する必要があります。

図4. 値リストの編集

パラメータの値を編集したら、**保存**をクリックして変更内容を適用し、ウィンドウを閉じます。変更を適用せずにウィンドウを閉じるには、**キャンセル**をクリックするか、ポップアップウィンドウの右上隅にある **×** のアイコンをクリックします。

テキストエディターでコンポーネントの設定を表示、編集する

Ini エディタモードで**パラメータ**を表示すると、それらは製品の**設定ファイル**と同じ形式で表示されます（パラメータ＝値のペア）。ここでのパラメータは、設定ファイル（対応するコンポーネントの設定セクション）に直接書き込まれるパラメータの名前です。このモードでは、デフォルト値とは異なる値のパラメータのみが表示されます（つまり、ラ



イセンスを有効化表示モードで値が太字で強調されているパラメータ)。下の図は、このシンプルビューのテキストエディターでパラメータがどのように表示されるかを示しています。

Scanning Engine [ScanEngine]

全て 変更 Ini エディタ

このフィールドには、デフォルトと異なる値が設定されたコンポーネントのパラメータが表示されます。ここでは、設定ファイル内に保存されている形で(<parameter>=<value>ストリングとして)設定パラメータを指定することができます。パラメータをデフォルト値に復元するには、該当する値をエディタから削除してください。各コンポーネントで使用可能な設定パラメータとパラメータのセットに関する詳細はヘルプをご確認ください。

MaxForks=3

行われた変更はまだ保存されていません 保存 リセット

図5. 簡単なテキスト設定エディター

必要な変更を加えるには、設定ファイルの編集について説明したのと同じ規則に従って、このテキストエディターでテキストを編集します(これにより、左側で強調表示されているコンポーネントの設定を含むセクションのみが変更されます)。必要に応じて、コンポーネントで使用可能な任意のパラメータに新しい値を指定できます。この場合、このパラメータの値はデフォルト設定からエディターに入力した値に変わります。パラメータをデフォルト値にリセットする場合は、このテキストエディターでこのパラメータを含む行を消去してください。変更した場合は、変更を保存するとパラメータはデフォルト値に戻ります。

パラメータ値の編集が終了したら、**保存**をクリックして変更を適用するか、**キャンセル**をクリックして変更を破棄します。



保存をクリックすると、テキストが検証されます。プログラムは、すべてのパラメータが存在し、それらの設定値が有効であるかどうかを確認します。エラーが発生した場合は、適切なメッセージが表示されます。

パラメータ値を指定するために重要な設定ファイル、構造、機能の詳細については、[「付録D. Dr.Web for UNIX File Servers設定ファイル」](#)のセクションを参照してください。

追加情報

- Dr.Web ConfigDの[設定パラメータ](#)(共通設定)。
- SpIDer Guardの[設定パラメータ](#)。
- SpIDer Guard for NSSの[設定パラメータ](#)。
- SpIDer Guard for SMBの[設定パラメータ](#)。
- Dr.Web ES Agentの[設定パラメータ](#)。
- Dr.Web Updaterの[設定パラメータ](#)。
- Dr.Web ClamDの[設定パラメータ](#)。



- Dr.Web File Checkerの[設定パラメータ](#)。
- Dr.Web Scanning Engineの[設定パラメータ](#)。
- Dr.Web Network Checkerの[設定パラメータ](#)。
- Dr.Web SNMPDの[設定パラメータ](#)。
- Dr.Web CloudDの[設定パラメータ](#)。
- Dr.Web StatDの[設定パラメータ](#)。
- [集中管理モードの管理](#)。

集中管理モードの管理

Dr.Web for UNIX File Serversを集中管理サーバーに接続したり、スタンドアロンモードに戻して、製品を集中管理サーバーから切断したりすることができます。集中管理を管理できるページを開くには、**設定**ページの**設定メニュー**から**集中管理**という項目を選択します。

Dr.Web for UNIX File Serversを集中管理サーバーに接続したり、集中管理サーバーとの接続を切断したりするには、このページの該当するチェックボックスを使用します。

集中管理サーバーとの接続

集中管理サーバーに接続を試みたときに画面に表示されるポップアップウィンドウでは、集中管理サーバーに接続するためのパラメータを指定する必要があります。

The screenshot shows a dialog box titled "手動で設定" (Manual Setup) with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- A label "サーバーのアドレスとポート:" (Server address and port:) followed by a text input field.
- A label "サーバー証明書ファイル:" (Server certificate file:) followed by a text input field and a "参照" (Browse) button.
- A section header "▼ 認証(任意)" (Authentication (optional)).
- A label "ワークステーションID:" (Workstation ID:) followed by a text input field.
- A label "パスワード:" (Password:) followed by a text input field.
- A checkbox labeled "ワークステーションを「新規端末」として接続" (Connect workstation as "New terminal").
- At the bottom, there are two buttons: "接続" (Connect) and "キャンセル" (Cancel).

図6. 集中管理サーバーとの接続

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オプションを選択した場合は、このウィンドウの該当するフィールドで、接続設定を含むファイルへのパスも指定する必要があります。このファイルはアンチウイルスネットワーク管理者によって提供されます。手動で設定オプションを選択した場合は、集中管理サーバーのアドレスとポートを指定する必要があります。手動で設定または自動で検出オプションでは、サーバーのパブリックキー（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によって提供された）を含むファイルへのパスを指定することもできます。

また、集中管理サーバーでの認証用のワークステーション識別子（ID）とパスワードを知っている場合は、認証（任意）セクションでそれらを指定できます。これらのフィールドに入力すると、集中管理サーバーへの接続は、正しいIDとパスワードのペアが入力された場合にのみ成功します。これらのフィールドを空白のままにすると、集中管理サーバーへの接続は、集中管理サーバーで承認された場合（自動的またはアンチウイルスネットワーク管理者による承認）にのみ確立します。

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することもできます（新規ユーザーとして接続する場合）。この場合、ワークステーションからの接続に対して集中管理サーバーで新規端末モードが許可されていると、集中管理サーバーはこの接続を承認した後、自動的に一意のIDとパスワードのペアを生成します。今後コンピューターをサーバーに接続する際はこれを使用します。このモードでは、すでにサーバー上にワークステーションの別のアカウントがある場合でも、集中管理サーバーはワークステーション用に新しいアカウントを生成します。



接続パラメータは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指定してください。

集中管理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、接続が確立されるまで待ちます。サーバー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 UNIX File Serversを集中管理サーバーに接続すると、スタンドアロンモードに戻すまで、その動作は集中管理サーバーによって管理されます。Dr.Web for UNIX File Serversが開始されるたびに、集中管理サーバーへの接続が自動的に確立されます。

ローカルファイルをスキャンする

Webインターフェースには、ローカルコンピューター（現在Webインターフェースにアクセスしているコンピューター）に保存されているファイルをスキャンして、ファイルに悪意のあるコンテンツが含まれているかどうか確認する機能があります。スキャンにはDr.Web for UNIX File Serversに含まれているスキャンエンジンが使用されます。スキャン対象として選択されたファイルはDr.Web for UNIX File Serversが動作しているサーバーに（HTTPプロトコル経由で）アップロードされますが、脅威が見つかった場合でも、スキャン後にファイルがサーバーに保存されることも、隔離されることもありません。スキャンするファイルを送信したユーザーには、スキャンの結果についてのみ通知されます。



この機能は、Dr.Web for UNIX File ServersディストリビューションにDr.Web Network Checkerコンポーネントが含まれている場合にのみ使用できます。

ローカルファイルをスキャンするパネルを開いて、スキャン用のパラメータを設定する

Webインターフェースのメインメニューでファイルをスキャン項目を選択したときに表示されるローカルファイルのスキャンパネルを使用して、スキャンするファイルを選択してアップロードできます。起動したパネルは、Webインターフェースの右下隅に表示されます。ローカルファイルのスキャンパネルは以下のようになります。



図7. ローカルファイルのスキャンパネル


このパネルを閉じるには、パネルの右上隅にある **X** をクリックします。 アイコンをクリックすると、ローカルファイルのスキャン設定を表示できます。これには、ファイルをスキャンする最大時間（ローカルコンピュータからサーバーにファイルをアップロードするのにかかる時間は含まれません）、ヒューリスティック解析の使用、圧縮されたオブジェクトの最大圧縮率、コンテナ（アーカイブなど）に圧縮されたオブジェクトの最大ネストレベルなどが含まれます。



図8. ローカルファイルをスキャンするためのパラメータを設定する

変更した設定を適用して、スキャンするファイルを選択できるファイル選択モードに戻るには、**適用** ボタンを押します。設定に変更を適用せずにファイル選択に戻るには、**キャンセル** ボタンを押します。

ローカルファイルのスキャンを開始する

スキャンするファイルを選択してスキャンを開始するには、スキャンするファイルをここにドラッグするか、またはクリックして選択してくださいと表示されているターゲット領域を左クリックします。そこをクリックすると、各OSのファイルマネージャーの標準的なファイル選択ウィンドウが開きます。スキャン対象として一度に複数のファイルを選択できます。スキャン対象としてディレクトリを選択することはできませんのでご注意ください。ファイルマネージャ



ーウィンドウで選択したファイルをマウスで直接ファイルスキャンパネルのターゲットエリアにドラッグすることもできます。スキャンするファイルを指定すると、Dr.Web for UNIX File Serversがインストールされているサーバーへのアップロードが開始されます。ファイルがアップロードされると、スキャンが開始されます。ファイルのアップロードおよびスキャン中に、ファイルスキャンパネルにスキャン手順の全体的な進捗状況が表示されます。



図9. ローカルファイルのスキャンの進捗状況

必要に応じて、**停止**ボタンを押してスキャンを中止できます。スキャンが完了すると、アップロードされたファイルのスキャンに関するレポートがファイルスキャンパネルに表示されます。

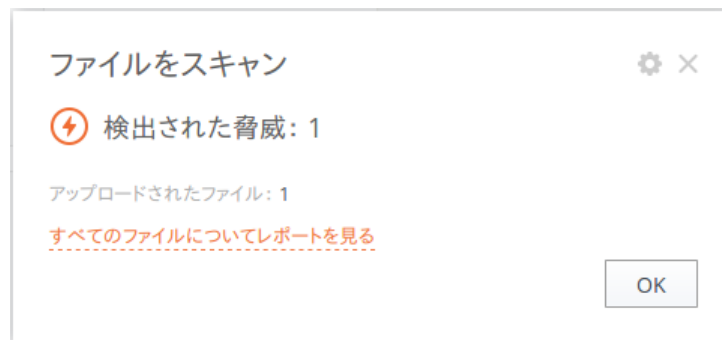


図10. スキャンしたローカルファイルの結果

複数のファイルがアップロードされると、スキャンに関する詳細なレポートが利用可能になります。拡張レポートを表示するには、**すべてのファイルについてレポートを見る**というリンクをクリックします。



図11. スキャンしたローカルファイルに関する詳細レポート



レポートを閉じて、パネルでスキャン対象の新しいファイルを選択できる状態に戻るには、**OK**を押します。



ファイルスキャンパネルを閉じているときでも、（スキャンの現在の設定を使用して）ローカルファイルのスキャンを開始することができます。ローカルファイルのアップロードとスキャンを開始するには、ファイルマネージャーウィンドウからブラウザで開いているWebインターフェースのページにドラッグアンドドロップします。



SpIDer Guard



このコンポーネントは **GNU/ Linux** OS のディストリビューションにのみ含まれています。

Linux ファイルシステムモニター SpIDer Guard では、**GNU/ Linux** ファイルシステムボリュームのファイルアクティビティをモニタリングできます。このコンポーネントは常駐モニターとして動作し、変更（ファイルの作成、開始、終了）に関連するメインファイルシステムのイベントを制御します。このようなイベントが検出されると、モニターはファイルが変更されたかどうかを確認し、変更されている場合は、[Dr.Web File Checker](#) ファイルスキャンコンポーネントのタスクを生成して、変更されたファイルを [Dr.Web Scanning Engine](#) スキャンエンジンでスキャンします。

さらに、ファイルシステムモニター SpIDer Guard は、その実行ファイルからプログラムを実行しようとする試みを検出します。実行ファイル内のプログラムがスキャン中に悪意のあるものとして検出された場合、この実行ファイルから起動されたすべてのプロセスは強制的に終了されます。

動作原理

このセクションの内容：

- [概要](#)
- [監視するファイルシステムの領域を定義する](#)
- [拡張ファイルモニタリングモード](#)

概要

ファイルシステムモニター SpIDer Guard は、**fanotify** メカニズムまたは Doctor Web によって開発された特別な Linux カーネルモジュール (*LKM - Linux kernel module*) のいずれかを使用してユーザーモードで動作します。すべての **Linux** カーネルバージョンがモニターで使用される **fanotify** をサポートしているわけではないため、起動時にコンポーネントの最適な動作モードを定義できる **自動モード (Auto)** を使用することをお勧めします。コンポーネントが指定された統合モードをサポートできない場合、コンポーネントは起動後に終了します。自動モード (Auto) が選択されている場合、コンポーネントは **fanotify** モード、**LKM** モードの順に使用を試みます。これら2つのモードのどちらも使用できない場合、コンポーネントは終了します。



一部のオペレーティングシステムでは、コンパイル済みのカーネルモジュールが SpIDer Guard とともに提供されます。SpIDer Guard を使用するオペレーティングシステム用にカーネルモジュールがコンパイルされていない場合は、Doctor Web が提供するソースコードファイルを使用してカーネルモジュールを手動で構築してインストールします（手順については、[SpIDer Guard 用のカーネルモジュールを構築する](#) セクションを参照）。

PARSEC マンデートアクセスサブシステムを使用する **Astra Linux SE** OS では、異なるマンデートレベルでのユーザー操作中にファイルアクセス監視の SpIDer Guard コンポーネントが正しく機能するために、**PARSEC**

新しいファイルまたは変更されたファイルが検出されると、モニターは [Dr.Web File Checker](#) ファイルチェッカーコンポーネントにこれらのファイルをスキャンするタスクを送信します。その後、コンポーネントは [Dr.Web Scanning Engine](#) スキャンエンジンによるスキャンを開始します。動作スキームは以下ようになります。**fanotify** システムメ



カニズム経由で操作している場合、モニターはスキャンされないファイルへのアクセス(すべての種類のファイルまたは実行ファイル(PE、ELF、プリアンブル#!付きのスクリプト)のみ)を、ファイルが完全に処理されるまでブロックできます(後述のセクションを参照)。



ファイルシステムモニターSpIDer Guardは、新しいファイルシステムボリュームのマウントとマウント解除(USBフラッシュドライブ、CD/DVD、RAIDアレイなど)を自動的に検出し、必要に応じてモニタリング対象オブジェクトのリストを調整します。

監視するファイルシステムの領域を定義

ファイルシステムのチェックを最適化するために、SpIDer Guardは、設定で指定されたファイルシステムの範囲内にあるファイルに対する要求のみを制御します。それぞれの範囲は、ファイルシステムツリーのディレクトリへのパスとして定義され、**保護スペース**と呼ばれます。すべての保護スペースが集まって、モニターによって制御される単一の**モニタリング範囲**を形成します。また、コンポーネントの設定(**除外範囲**)では、モニタリングから除外するディレクトリの集合を指定できます。コンポーネント設定で保護スペースを指定していない場合は、モニタリング範囲によってすべてのファイルシステムツリーが制御されます。つまり、ファイルがモニタリング範囲に属し、除外範囲に属していない場合、それらのファイルはモニタリングの対象になります。

除外の指定は、あるファイルが頻繁に変更され、その結果これらのファイルが繰り返しスキャンされ、システムの負荷が増大する場合に便利です。ディレクトリ内のファイルの頻繁な変更が悪意のあるプログラムによるものではなく信頼できるプログラムの操作によるものであることが確実に分かっている場合は、このディレクトリまたはこれらのファイルへのパスを除外リストに追加できます。この場合、ファイルシステムモニターSpIDer Guardは、モニタリング範囲内であっても、これらのオブジェクトの変更への応答を停止します。さらに、信頼できるプログラムのリストにプログラムを追加することもできます(**ExcludedProc**構成パラメータ)。この場合、変更されたファイルまたは作成されたファイルがモニタリングの対象になっていても、このプログラムによるファイル操作によってスキャンが実行されることはありません。同様に、必要に応じて、ローカルファイルシステムにマウントされている他のファイルシステム(CIFS経由でマウントされた外部ファイルサーバーディレクトリなど)にあるファイルのモニタリングとスキャンを無効にすることもできます。スキャン対象ではないファイルを持つファイルシステムを指定するには、**ExcludedFilesystem**パラメータを使用します。

指定されたスキャンパラメータを持つモニタリング範囲の一部である保護スペースは、コンポーネント設定の名前付きセクションとして設定され、その名前には保護スペースに割り当てられた一意の識別子が含まれます。保護スペースを記述する各セクションには、スペースのディレクトリを格納するファイルシステムへのパスを定義する**Path**パラメータ(つまり、このスペース内でモニターされるファイルシステムツリーフラグメント)と、保護スペース内のローカル(**Path**が基準)の除外範囲を定義する**ExcludedPath**パラメータが含まれます。

ExcludedPathパラメータには標準のファイルマスク(「*」と「?」の文字)を含めることができます。さらに、保護スペースを記述するセクションの外側に指定した**ExcludedPath**パラメータを使用すれば、グローバル除外範囲を指定することもできます。保護スペースのディレクトリを含む、この範囲に属するすべてのカタログがモニターから除外されます。各保護スペースには、グローバルおよび独自の除外範囲のみを追加できます。あるスペースが別のスペースにネストされている場合、スペースで囲って指定する除外設定はネストされたスペースには適用されません。さらに、各保護範囲設定には、ファイルモニタリングを有効にするかどうかを指定する論理パラメータ**Enable**があります。このパラメータがNoに設定されているか、**Path**パラメータの値が空になっている場合、スペースの内容はモニタリングされません。



モニター設定で指定したすべての保護スペースがモニタリングされない場合や、パスが指定されていない場合、システムのファイルツリーのファイルはモニタリングされないため、SpIDer Guardはアイドル状態で実行されます。ファイルシステムを単一の保護スペースとしてモニターする場合は、設定から名前付きスペースのセクションを削除します。



モニタリング範囲と除外範囲の設定例を考えます。コンポーネント設定で次のパラメータが設定されているとします。

```
[LinuxSpider]
  ExcludedPath = /directory1/tmp
  ...

[LinuxSpider.Space.space1]
  Path = /directory1
  ExcludedPath = "*.tmp"
  ...

[LinuxSpider.Space.space2]
  Path = /directory1/directory2
  ...

[LinuxSpider.Space.space3]
  Path = /directory3
  Enable = No
  ...
```

この設定は、/directory1/tmpフォルダを除く、/directory1ディレクトリとそのサブディレクトリにあるファイルがモニタリングされることになります。フルネームがマスク/directory1/*.tmpと一致するファイルもモニタリング対象になりません（範囲が保護スペース`space1`にネストされている場合でも、このマスクが適用されないネストされた範囲/directory1/directory2を除く）。/directory3ディレクトリ内のファイルはモニタリングされません。

拡張ファイルモニタリングモード

SpIDer Guardは3つのモニタリングモードを使用できます。

- **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。

Dr.Web File Checkerは、指定された期間、スキャン結果をキャッシュで保存するため、スキャン結果がキャッシュにあるファイルにアプリがアクセスした場合、ファイルは再スキャンされず、代わりにキャッシュされたスキャン結果が使用されます。それにもかかわらず、「パラノイド」モードでは、ファイルへのアクセスが大幅に遅くなります。

モニタリングモードを構成するには、コンポーネント**設定**のBlockBeforeScanパラメータ値を変更します。



コマンドライン引数

SpIDer Guardを実行するには、コマンドラインに次のコマンドを入力します。

```
$ <opt_dir>/bin/drweb-spider [<parameters>]
```

SpIDer Guardは次のオプションを処理できます。

パラメータ	説明
--help	機能：コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了するように指示します。 短縮形： -h 引数： None
--version	機能：このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了するように指示します。 短縮形： -v 引数： None

例：

```
$ /opt/drweb.com/bin/drweb-spider --help
```

このコマンドはSpIDer Guardに関する簡単なヘルプ情報を出力します。

スタートアップノート

コンポーネントは、自律モードで（他のコンポーネントから自律的に）OSのコマンドラインから直接起動することはできません。[Dr.Web ConfigD](#)設定デーモンによって自動的に起動します（OSの起動時）。コンポーネントの動作を管理するには、Dr.Web for UNIX File Servers用の[Dr.Web Ctl](#)コマンドラインベースの管理ツールを使用できます（これは**drweb-ctl**コマンドを使用して呼び出されます）。



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ドキュメントを要求するには、次のコマンドを使用します。**man 1 drweb-spider**

設定パラメータ

コンポーネントは、Dr.Web for UNIX File Serversの統合された[設定ファイル](#)の[LinuxSpider]セクションで指定されている設定パラメータを使用します。

- [コンポーネントパラメータ](#)
- [保護スペースのモニタリング設定をカスタマイズする](#)



コンポーネントパラメータ

セクションには以下のパラメータが含まれています。

LogLevel <i>{logging level}</i>	コンポーネントの ログの詳細レベル パラメータ値が指定されていない場合は、[Root] セクション の DefaultLogLevel パラメータの値が使用されます。 デフォルト値: Notice
Log <i>{log type}</i>	コンポーネントの ロギング方式 。 デフォルト値: Auto
ExePath <i>{path to file}</i>	コンポーネントの実行ファイルへのパス。 デフォルト値: <opt_dir>/bin/drweb-spider • GNU/ Linux の場合: /opt/drweb.com/bin/drweb-spider
Start <i>{Boolean}</i>	コンポーネントは Dr.Web ConfigD 設定デモンによって起動される必要があります。 このパラメータにYes値を指定すると、設定デモンはただちにコンポーネントを開始するように指示されます。また、No値を指定すると、設定デモンはただちにコンポーネントを終了するように指示されます。 デフォルト値: 提供されたDr.Webコンポーネントが動作する製品によって異なります。
Mode <i>{LKM / FANOTIFY / AUTO}</i>	ファイルシステムモニターSpIDer Guardの動作モード。 使用可能な値: <ul style="list-style-type: none">• LKM - オペレーティングシステムのカーネルにインストールされているDr.Web LKMモジュールを使用します (LKM - Linuxカーネルモジュール)。• FANOTIFY - fanotifyモニタリングインターフェースを使用します。• AUTO - 最適モードの自動選択。



	<div><p>さまざまなGNU/Linux OSカーネルは両方の動作モードを異なる方法でサポートしているため、このパラメータ値の変更は細心の注意を払って行う必要があります。ファイルシステムマネージャーとの統合に最適なモードが起動時に選択されることから、このパラメータ値をAUTOに設定することを強くお勧めします。この場合、コンポーネントはFANOTIFYモードの有効化を試み、失敗したらLKMを有効にしようとします。どのモードも設定できない場合、コンポーネントは終了します。</p><p>必要に応じて、SpIDer Guard用のカーネルモジュールを構築するセクションの指示に従って、ソースコードからDr.Web LKMモジュールを構築してインストールすることができます。</p></div> <p>デフォルト値: AUTO</p>
DebugAccess <i>{Boolean}</i>	<p>ファイルへのアクセスに関する詳細なメッセージをデバッグレベルでログファイルに含めるかどうかを示します (LogLevel = DEBUGの場合など)。</p> <p>デフォルト値: NO</p>
ExcludedProc <i>{path to file}</i>	<p>モニタリングから除外されるプロセスのリスト。ここで指定されているいずれかのプロセスによってファイル操作が開始された場合、変更または作成されたファイルはスキャンされません。</p> <p>リストをパラメータ値として指定できます。リストの値は、コンマ(引用符内の各値)で区切る必要があります。パラメータはセクションで複数回指定できます(この場合、そのすべての値が1つのリストにまとめられます)。</p> <p>例: プロセスのリストにwgetとcurlを追加します。</p> <ol style="list-style-type: none">設定ファイルに値を追加します。<ul style="list-style-type: none">1つの文字列に2つの値<pre>[LinuxSpider] ExcludedProc = "/usr/bin/wget", "/usr/bin/curl"</pre><ul style="list-style-type: none">2つの文字列(文字列ごとに1つの値)<pre>[LinuxSpider] ExcludedProc = /usr/bin/wget ExcludedProc = /usr/bin/curl</pre>コマンドdrweb-ctl cfsetを使用して値を追加します。 <pre># drweb-ctl cfset LinuxSpider.ExcludedProc - a /usr/bin/wget # drweb-ctl cfset LinuxSpider.ExcludedProc - a /usr/bin/curl</pre> <p>デフォルト値: (未設定)</p>



<p>ExcludedFilesystem</p> <p><i>{FS name}</i></p>	<p>指定されたファイルシステムにあるファイルへのアクセスを制御しません。</p> <p>この機能は、モニターがFANOTIFYモードで動作している場合にのみ利用可能です。</p> <p>リストをパラメータ値として指定できます。リストの値は、コンマ(引用符内の各値)で区切る必要があります。パラメータはセクションで複数回指定できます(この場合、そのすべての値が1つのリストにまとめられます)。</p> <p>例: リストにcifsファイルシステムとnfsファイルシステムを追加します。</p> <p>1. 設定ファイルに値を追加します。</p> <ul style="list-style-type: none">1つの文字列に2つの値 <pre>[LinuxSpider] ExcludedFilesystem = "cifs", "nfs"</pre> <ul style="list-style-type: none">2つの文字列(文字列ごとに1つの値) <pre>[LinuxSpider] ExcludedFilesystem = cifs ExcludedFilesystem = nfs</pre> <p>2. コマンドdrweb-ctl cfsetを使用して値を追加します。</p> <pre># drweb-ctl cfset LinuxSpider.ExcludedFilesystem -a cifs # drweb-ctl cfset LinuxSpider.ExcludedFilesystem -a nfs</pre> <p>デフォルト値: cifs</p>
<p>BlockBeforeScan</p> <p><i>{Off / Executables / All}</i></p>	<p>モニターによってスキャンされるまで、ファイルはアクセスの際にブロックされます(拡張または「パラノイド」モニタリングモードの使用)。</p> <p>使用可能な値:</p> <ul style="list-style-type: none">Off - スキャン対象でない場合でも、ファイルへのアクセスをブロックしません。Executables - モニターによってスキャンされない実行ファイル(PEファイル、ELFファイル、プリアンブル#!付きのスクリプト)へのアクセスをブロックします。All - モニターでチェックされないファイルへのアクセスをブロックします。 <p>モニターがFANOTIFYモードで動作している場合にのみ実行されるファイルのブロック。</p> <p>デフォルト値: Off</p>
<p>[*] ExcludedPath</p> <p><i>{path to file or directory}</i></p>	<p>モニタリングから除外する必要があるオブジェクトへのパス。ディレクトリまたはファイルパスを指定できます。ディレクトリを指定すると、ディレクトリのすべてのコンテンツが除外されます。ファイルマスク(「?」と「*」、および記号クラス「[]」、「[!]」、「[^]」を含む)が許可されます。</p>



	<p>リストをパラメータ値として指定できます。リストの値は、コンマ(引用符内の各値)で区切る必要があります。パラメータはセクションで複数回指定できます(この場合、そのすべての値が1つのリストにまとめられます)。</p> <p>例: リストにファイル/etc/file1とディレクトリ/usr/binを追加します。</p> <p>1. 設定ファイルに値を追加します。</p> <ul style="list-style-type: none">1つの文字列に2つの値 <pre>[LinuxSpider] ExcludedPath = "/etc/file1", "/usr/bin"</pre> <ul style="list-style-type: none">2つの文字列(文字列ごとに1つの値) <pre>[LinuxSpider] ExcludedPath = /etc/file1 ExcludedPath = /usr/bin</pre> <p>2. コマンドdrweb-ctl cfsetを使用して値を追加します。</p> <pre># drweb-ctl cfset LinuxSpider.ExcludedPath - a /etc/file1 # drweb-ctl cfset LinuxSpider.ExcludedPath - a /usr/bin</pre> <p>スキャン時にはファイルへの直接パスのみが解析されるため、ここではシンボリックリンクによる影響はありません。</p> <p>デフォルト値: /proc、/sys</p>
<p>[*] OnKnownVirus</p> <p>{action}</p>	<p>SpIDer Guardによるスキャン中にシグネチャ解析を使用して検出された既知の脅威(ウイルスなど)に対してDr.Web for UNIX File Serversによって適用されるアクション。</p> <p>可能なアクション: <i>Cure</i>、<i>Quarantine</i>、<i>Delete</i></p> <p>デフォルト値: <i>Cure</i></p>
<p>[*] OnIncurable</p> <p>{action}</p>	<p>SpIDer Guardによるスキャン中に検出された修復不可の脅威(<i>Cure</i>の適用に失敗したもの)に対してDr.Web for UNIX File Serversによって適用されるアクション。</p> <p>可能なアクション: <i>Quarantine</i>、<i>Delete</i></p> <p>デフォルト値: <i>Quarantine</i></p>
<p>[*] OnSuspicious</p> <p>{action}</p>	<p>SpIDer Guardによるスキャン中にヒューリスティック解析を使用して検出された未知の脅威(または疑わしいオブジェクト)に対してDr.Web for UNIX File Serversによって適用されるアクション。</p> <p>可能なアクション: <i>Report</i>、<i>Quarantine</i>、<i>Delete</i></p> <p>デフォルト値: <i>Quarantine</i></p>



[*] OnAdware <i>{action}</i>	SpIDer Guardによるスキャン中に検出されたアドウェアに対してDr.Web for UNIX File Serversによって適用されるアクション。 可能なアクション: <i>Report, Quarantine, Delete</i> デフォルト値: <i>Quarantine</i>
[*] OnDialers <i>{action}</i>	SpIDer Guardによるスキャン中に検出されたダイヤラーに対してDr.Web for UNIX File Serversによって適用されるアクション。 可能なアクション: <i>Report, Quarantine, Delete</i> デフォルト値: <i>Quarantine</i>
[*] OnJokes <i>{action}</i>	SpIDer Guardによるスキャン中に検出されたジョークに対してDr.Web for UNIX File Serversによって適用されるアクション。 可能なアクション: <i>Report, Quarantine, Delete</i> デフォルト値: <i>Report</i>
[*] OnRiskware <i>{action}</i>	SpIDer Guardによるスキャン中に検出されたリスクウェアに対してDr.Web for UNIX File Serversによって適用されるアクション。 可能なアクション: <i>Report, Quarantine, Delete</i> デフォルト値: <i>Report</i>
[*] OnHacktools <i>{action}</i>	SpIDer Guardによるスキャン中に検出されたハッキングツール(リモート管理用のツール、トロイの木馬など)に対してDr.Web for UNIX File Serversによって適用されるアクション。 可能なアクション: <i>Report, Quarantine, Delete</i> デフォルト値: <i>Report</i>
[*] ScanTimeout <i>{time interval}</i>	SpIDer Guardによって開始された1つのファイルに対するスキャンのタイムアウト。 <i>1秒から1時間の範囲の値を指定できます</i> デフォルト値: <i>30s</i>
[*] HeuristicAnalysis <i>{On / Off}</i>	SpIDer Guardによって開始されたファイルのスキャン中に脅威を検出するためにヒューリスティック解析を使用するかどうかを指定します。ヒューリスティック解析における検出の信頼性は高いのですが、ウイルススキャンに時間がかかります。 <i>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に適用されるアクションは、OnSuspiciousパラメータ値として指定します。</i> 使用可能な値: <ul style="list-style-type: none">On - スキャン時にヒューリスティック解析を使用するように指示します。Off - ヒューリスティック解析を使用しないように指示します。 デフォルト値: <i>On</i>
[*] PackerMaxLevel	圧縮されたオブジェクトスキャン時の最大ネスティングレベル。SpIDer Guardによるファイルスキャン時に、下位のネストレベルにあるすべてのオブ



<code>{integer}</code>	<p>ジェクトがスキップされます。</p> <p>0から60までの範囲の値を指定できます。値を0に設定すると、ネストしたオブジェクトはスキャンされません。</p> <p>デフォルト値：8</p>
<p>[*] ArchiveMaxLevel</p> <p><code>{integer}</code></p>	<p>アーカイブスキャン時の最大ネスティングレベル。SpIDer Guardによるファイルスキャン時に、下位のネストレベルにあるすべてのオブジェクトがスキップされます。</p> <p>0から60までの範囲の値を指定できます。値を0に設定すると、ネストしたオブジェクトはスキャンされません。</p> <p>デフォルト値：0</p>
<p>[*] MailMaxLevel</p> <p><code>{integer}</code></p>	<p>メールメッセージとメールボックスをスキャンするときの最大ネストレベル。SpIDer Guardによるファイルスキャン時に、下位のネストレベルにあるすべてのオブジェクトがスキップされます。</p> <p>0から60までの範囲の値を指定できます。値を0に設定すると、ネストしたオブジェクトはスキャンされません。</p> <p>デフォルト値：0</p>
<p>[*] ContainerMaxLevel</p> <p><code>{integer}</code></p>	<p>コンテナ（HTMLページなど）をスキャンするときの最大ネストレベル。SpIDer Guardによるファイルスキャン時に、下位のネストレベルにあるすべてのオブジェクトがスキップされます。</p> <p>0から60までの範囲の値を指定できます。値を0に設定すると、ネストしたオブジェクトはスキャンされません。</p> <p>デフォルト値：8</p>
<p>[*] MaxCompressionRatio</p> <p><code>{integer}</code></p>	<p>スキャンされるオブジェクトの最大圧縮率（非圧縮サイズと圧縮サイズの比率）。このオブジェクトの比率が制限を超えると、そのオブジェクトはSpIDer Guardによるスキャン中にスキップされます。</p> <p>圧縮率には2よりも小さい値は指定できません。</p> <p>デフォルト値：500</p>

保護スペースのモニタリング設定をカスタマイズする

ファイルシステムの保護スペースごとに、すべてのモニタリングパラメータを格納する[LinuxSpider]セクションとともに、設定ファイル内にモニタリング対象ファイルシステム領域（サイト）へのパスとモニタリングパラメータを含む個別のセクションを指定します。各セクションには、[LinuxSpider.Space.<space name>]の形式で名前を付ける必要があります。ここで、<space name>は保護スペースの一意的識別子になります。

このセクションには、[LinuxSpider]セクションにないパラメータを含める必要があります。

<p>Enable</p> <p><code>{Boolean}</code></p>	<p>Path（下を参照）で指定したディレクトリにある保護スペースのコンテンツがモニタリングされます。</p> <p>この保護スペースのコンテンツのモニタリングを停止するには、パラメータをNoに設定します。</p>
--	---



	デフォルト値: Yes
Path <i>{path to directory}</i>	モニタリングが必要なファイル(ネストされたディレクトリを含む)を格納するシステムディレクトリへのパスを指定します。 デフォルトでは、このパラメータには空の値が設定されています。そのため、モニタリング範囲に保護スペースを追加するときには値を指定する必要があります。 デフォルト値: (指定なし)



モニター設定で指定したすべての保護スペースがモニタリングされない場合や、パスが指定されていない場合、システムのファイルツリーのファイルはモニタリングされないため、SpIDer Guardはアイドル状態で実行されます。ファイルシステムを単一の保護スペースとしてモニターする場合は、設定から名前付きスペースのセクションを削除します。

上述の場合を除き、保護スペースの個別のセクションには、上の表で「[*]」の文字が付いているコンポーネント設定の共通セクションのパラメータのリストを含めることができます(脅威が検出されたときのアクション、最大アーカイブチェックレベルなど)。保護スペースにパラメータが指定されていない場合、このスペースのモニタリング手順は、対応するパラメータを使用して実行され、パラメータの値は[LinuxSpider]セクションから取得されます。

Dr.Web for UNIX File Servers管理用のDr.Web Ctlコマンドラインツール(**drweb-ctl**コマンドによって実行)を使用してタグ *<space name>*が付いた保護スペースのパラメータに新しいセクションを追加するには、次のコマンドを使用します。

```
# drweb-ctl cfset LinuxSpider.Space -a <space name>
```

例:

```
# drweb-ctl cfset LinuxSpider.Space -a Space1  
# drweb-ctl cfset LinuxSpider.Space.Space1.Path /home/user1
```

最初のコマンドは、[LinuxSpider.Space.Space1]セクションを設定ファイルに追加します。2番目のパラメータはセクションのPathパラメータの値を設定し、ファイルシステムのモニタリング領域へのパスを指定します。このセクションのその他のパラメータは[LinuxSpider]セクションのものと同じです。

ファイルシステムモニタリングの設定

ファイルシステムモニタリングの設定方法については、[ファイルシステムモニタリングの設定](#)を参照してください。

SpIDer Guardにカーネルモジュールを使用する

このセクションの内容:

- [概要](#)
- [カーネルモジュールを作成する](#)
- [作成中に起こりうるエラー](#)



概要

ファイルシステムオブジェクトに対するアクションをモニタリングするためにSpIDer Guardが使用する**fanotify**メカニズムをオペレーティングシステムがサポートしていない場合は、カーネル空間で特別なローダブルカーネルモジュールを使用できます（さらに、実装されている**fanotify**メカニズムのファイルシステムへのアクセスが制限されている場合も、カーネルモジュールを使用できます）。

デフォルトでは、SpIDer Guardには、[システム要件と互換性](#)の「システム要件」セクションに記載されているすべてのオペレーティングシステムで利用できる完全に構築されたローダブルカーネルモジュールが付属しています。さらに、SpIDer Guardで提供されているtar.bz2アーカイブのソースコードを使用して、ローダブルカーネルモジュールを手動で構築することもできます。



SpIDer Guardの使用するローダブルカーネルモジュールは、**GNU/Linux**カーネル2.6.*以降との動作に適したものとなっています。

ARM64アーキテクチャ向けDr.Web for UNIX File Serversのバージョンではサポートされていません。

ソースコードを含むアーカイブは、Dr.Web for UNIX File Serversのベースディレクトリ<opt_dir>のshare/drweb-spider-kmod/src/サブディレクトリにあります（**GNU/Linux**の場合：/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、Dr.Web for UNIX File Servers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。

指定したパスにdrweb-spider-kmodディレクトリがない場合は、drweb-spider-kmodパッケージをインストールします（Dr.Web for UNIX File Serversのインストール[方法](#)に応じて、[リポジトリ](#)から、またはユニバーサルパッケージからの[カスタムインストール](#)を使用）。



ソースコードファイルからローダブルカーネルモジュールを手動で構築するには、管理者（root）権限が必要です。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の追加設定を実行します。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を指定することも可能です。この場合、SpIDer Guardは自動的にカーネルモジュールまたは**fanotify**モニタリングインターフェースのいずれかを使用しようとしています。詳細については、次のコマンドを入力します。

```
$ man 1 drweb-spider
```

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。
- 特定のオペレーティングシステムでは、ソースコードを含むディレクトリへのパスが正しく定義されていないため、手順が失敗することがあります。その場合は、`KDIR=<path to kernel source codes>`パラメータを指定して**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>` と異なる場合があります。



SpIDer Guard for SMB

SpIDer Guard for SMBは、SMBファイルサーバー**Samba**によって使用される共有ファイルシステムディレクトリのモニターです。このコンポーネントでは、**Samba**共有ディレクトリ内のファイルに適用されたアクションをモニタリングできます。常駐モニターとして機能し、保護対象のファイルシステム内の基本的なアクション（作成、開く、閉じる、読み取り、書き込みの操作）を制御します。コンポーネントがそのような操作を検出すると、ファイルが変更されたかどうかを確認し、変更されている場合は、ファイルをスキャンするタスクが作成されて[Dr.Web File Checker](#)に送信されます。ファイルのスキャンが必要な場合、Dr.Web File Checkerは[Dr.Web Scanning Engine](#)によるスキャンを開始します。ファイルに脅威が含まれている場合、脅威が駆除されるまで、設定で指定された期間アクセスがブロックされます。また、コンポーネントの設定によって、スキャンエラーの場合にファイルをブロックするよう指示できます（有効なライセンスがない場合も含む）。



Sambaの共有ディレクトリにあるファイルをスキャンするプロセスで発生する可能性がある、SpIDer Guard for SMBの間

の競合を避けるために、次のいずれかの操作を実行して、SpIDer Guardの追加[設定](#)を行うことをお勧めします。

- **Samba**共有ディレクトリを除外範囲に追加します（これらのディレクトリを**ExcludedPath**パラメータで指定します）。
- **Samba**プロセス（**smbd**）を除外プロセスのリストに追加します（**ExcludedProc**パラメータに**smbd**を指定します）。



SpIDer Guard for SMBモニターは、**Samba**サーバーとの統合に特別なVFS SMBモジュールを使用します。SpIDer Guard for SMBでは、このモジュールのいくつかのバージョンが提供されています。それらは**Samba**のさまざまなバージョン向けに構築されています。ただし、提供されているVFS SMBモジュールのバージョンが、ファイルサーバーにインストールされている**Samba**のバージョンと互換性を持たない場合があります。たとえば、**Samba**サーバーが**CLUSTER_SUPPORT**オプションを使用している場合に発生することがあります。

VFS SMBモジュールが**Samba**サーバーと互換性がない場合は、提供されているソースコードから**Samba**サーバー用のVFS SMBモジュールを手動で構築します（必要に応じて**CLUSTER_SUPPORT**オプションとの互換性を含む）。提供されているソースコードファイルからVFS SMBモジュールを構築する手順は、[VFS SMBモジュールを構築する](#)セクションで説明されています。

動作原理

このセクションの内容：

- [概要](#)
- [監視するファイルシステムの領域を定義する](#)

概要

SpIDer Guard for SMBモニターはデーモンモードで動作します（通常、システム起動時に[Dr.Web ConfigD](#)の設定デーモンによって起動されます）。起動後、コンポーネントは**Samba**サーバー側で動作する特別なプラグイン



ンが接続されたサーバーとして動作し(VFS SMBモジュール)、共有ディレクトリでのユーザーのアクティビティをモニタリングします。新しいファイルまたは変更されたファイルがボリューム上に見つかったら、モニターは[Dr.Web File Checker](#)ファイルチェッカーにそのファイルをスキャンするように指示します。

モニターの要求によりスキャンされたファイルが、修復できない脅威または「ブロック」(*Block*)アクションが指定された脅威に感染している場合、モニターは対応する共有ディレクトリを制御するVFS SMBモジュールにこのファイルをブロックするよう指示します(つまり、ユーザーによるファイルの読み取り、編集、実行を禁止します)。この設定が無効になっていない場合は、ブロックされたオブジェクトと同じディレクトリにテキストファイルも作成されます。作成されたテキストファイルには、オブジェクトがブロックされた理由が記載されます。[アクション](#)「削除」(*Delete*)または「隔離」(*Quarantine*)が適用されたファイルの「予期しない消失」を回避する必要があります。したがって、ユーザーが移動または削除されたファイルを何度も再作成しようとするのを防ぎます。さらに、このテキストファイルは、コンピューターが悪意のあるプログラムに感染した可能性があることをユーザーに通知します。通知があれば、ユーザーはコンピューターのアンチウイルススキャンを開始し、ローカルで検出された脅威を駆除できます。さらに、SpIDer Guard for SMBの操作を提供する有効なライセンスがない場合を含め、スキャンエラーが発生した際にファイルを(対応する設定パラメータの値に応じて)ブロックできます。

監視するファイルシステムの領域を定義

Sambaサーバーの管理対象の共有ディレクトリに格納されている特定のファイルとディレクトリのモニタリングを無効にできます。たとえば、あるファイルが頻繁に変更され、その結果これらのファイルが繰り返しスキャンされ、システムの負荷が増大する場合に便利です。ファイルサーバーのストレージにあるこれらのファイルが一般的に頻繁に変更されるということが確実に分かっている場合は、それらを除外リストに追加することをお勧めします。この場合、モニターはこれらのオブジェクトの変更への応答を停止するため、スキャンは開始されません。

モニタリング対象のディレクトリと除外対象とを区別するために、**Samba**のファイルストレージモニターSpIDer Guard for SMBでは、次の2つの設定パラメータを使用します。

- **IncludedPath** - モニタリング対象のパス(モニタリング範囲)。
- **ExcludedPath** - モニタリングから除外するパス(除外範囲)。

通常、モニターのモニタリング範囲には、共有ディレクトリ全体が使用されます。複数のモニタリング範囲と除外範囲を指定した場合、パスが**ExcludedPath**パラメータで指定されていない共有ディレクトリか、**IncludedPath**パラメータで指定された共有ディレクトリのファイルのみがモニタリングされます。パスが両方のパラメータで指定されている場合、**IncludedPath**パラメータが他のパラメータよりも優先されます。つまり、指定されたパス内のオブジェクトは、Samba共有ディレクトリモニターであるAppendixesSpIDer Guard for SMBによってモニタリングされます。したがって、除外範囲内にあるファイルやディレクトリをモニタリング対象に追加するには、**IncludedPath**パラメータを使用します。

SpIDer Guard for SMBによってモニタリングされる**Samba**共有ディレクトリごとに、別々のモニタリング範囲と除外範囲、検出された脅威に対するアクションなど、さまざまな保護パラメータを指定できます。その場合、SpIDer Guard for SMBの設定セクションで、共有ディレクトリを制御するVFS SMBモジュールの設定を個別に指定します。



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SpIDer Guard for SMBを起動するには、次のコマンドを使用します。

```
$ <opt_dir>/bin/drweb-smbspider-daemon [<parameters>]
```

SpIDer Guard for SMBは次のオプションを処理できます。

パラメータ	説明
--help	機能：コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了するように指示します。 短縮形： -h 引数： None
--version	機能：このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了するように指示します。 短縮形： -v 引数： None

例：

```
$ /opt/drweb.com/bin/drweb-smbspider-daemon --help
```

このコマンドはSpIDer Guard for SMBに関する簡単なヘルプ情報を出力します。

スタートアップノート

コンポーネントは、自律モードで（他のコンポーネントから自律的に）OSのコマンドラインから直接起動することはできません。[Dr.Web ConfigD](#)設定デーモンによって自動的に起動します（OSの起動時）。コンポーネントの動作を管理するには、Dr.Web for UNIX File Servers用の[Dr.Web Ctl](#)コマンドラインベースの管理ツールを使用できます（これは[drweb-ctl](#)コマンドを使用して呼び出されます）。



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ドキュメントを要求するには、次のコマンドを使用します。**man 1 drweb-smbspider-daemon**

設定パラメータ

コンポーネントは、Dr.Web for UNIX File Serversの統合された[付録D. Dr.Web for UNIX File Servers設定ファイル](#)の[SMBSpider]セクションで指定されている設定パラメータを使用します。

- [コンポーネントパラメータ](#)
- [モニタリング設定をカスタマイズする](#)



コンポーネントパラメータ

セクションには以下のパラメータが含まれています。

LogLevel <i>{logging level}</i>	コンポーネントの ログの詳細レベル パラメータ値が指定されていない場合は、[Root] セクション の DefaultLogLevel パラメータの値が使用されます。 デフォルト値: Notice
Log <i>{log type}</i>	コンポーネントの ロギング方式 。 デフォルト値: Auto
ExePath <i>{path to file}</i>	コンポーネントの実行ファイルへのパス。 デフォルト値: <opt_dir>/bin/drweb-smbspider-daemon <ul style="list-style-type: none">• GNU/Linuxの場合: /opt/drweb.com/bin/drweb-smbspider-daemon• FreeBSDの場合: /usr/local/libexec/drweb.com/bin/drweb-smbspider-daemon
Start <i>{Boolean}</i>	コンポーネントは Dr.Web ConfigD 設定デーモンによって起動される必要があります。 このパラメータに Yes 値を指定すると、設定デーモンはただちにコンポーネントを開始するように指示されます。また、 No 値を指定すると、設定デーモンはただちにコンポーネントを終了するように指示されます。 デフォルト値: No
SambaChrootDir <i>{path to directory}</i>	SMBファイルストレージのルートディレクトリへのパスを定義します (chroot 制限を使用してファイルサーバーで再定義できます)。 ファイルサーバーのストレージにあるファイルおよびディレクトリへの全パスの先頭に挿入されるプレフィックスとして使用され、ローカルファイルシステムのルートに対する相対パスを記述します。 指定しない場合は、ファイルシステムのルートへのパス/が使用されます。 デフォルト値: (指定なし)
SmbSocketPath <i>{path to file}</i>	SpIDer Guard for SMBとVFS SMBEジュール間のインタラクションを可能にするソケットファイルへのパス。 パスは常に相対パスであり、 SambaChrootDir パラメータ値で指定したパスの補足となります (SambaChrootDir パラメータが空の場合は、ファイルシステムルートへのパス/で補足されます)。 デフォルト値: var/run/.com.drweb.smb_spider_vfs
ActionDelay <i>{time interval}</i>	脅威が検出されてから、SpIDer Guard for SMBがその脅威タイプに指定されたアクションを適用するまでの保留時間。この間、ファイルはブロックされます。



	デフォルト値 : 24h
MaxCacheSize {size}	<p>モニタリング対象のSMBディレクトリ内のスキャン済みファイルに関するデータを格納するためにVFS SMBモジュールによって使用されるキャッシュのサイズ。</p> <p>0を指定した場合、データはキャッシュされません。</p> <p>デフォルト値 : 10mb</p>
[*] ExcludedPath {path to file or directory}	<p>スキャン中にスキップする必要がある共有ディレクトリオブジェクトへのパス。ディレクトリまたはファイルパスを指定できます。ファイルマスク(文字「?」および「*」の他、文字クラス「[]」、「[!]」、「[^]」を含む)を使用することもできます。</p> <p>リストをパラメータ値として指定できます。リストの値は、コンマ(引用符内の各値)で区切る必要があります。パラメータはセクションで複数回指定できます(この場合、そのすべての値が1つのリストにまとめられます)。</p> <p>例 : リストにファイル/etc/file1とディレクトリ/usr/binを追加します。</p> <p>1. 設定ファイルに値を追加します。</p> <ul style="list-style-type: none">1つの文字列に2つの値 <pre>[SMBSpider] ExcludedPath = "/etc/file1", "/usr/bin"</pre> <ul style="list-style-type: none">2つの文字列(文字列ごとに1つの値) <pre>[SMBSpider] ExcludedPath = /etc/file1 ExcludedPath = /usr/bin</pre> <p>2. コマンドdrweb-ctl cfsetを使用して値を追加します。</p> <pre># drweb-ctl cfset SMBSpider.ExcludedPath - a /etc/file1 # drweb-ctl cfset SMBSpider.ExcludedPath - a /usr/bin</pre> <p>ディレクトリを指定すると、ディレクトリのすべてのコンテンツがスキップされます。</p> <p>デフォルト値 : (指定なし)</p>
[*] IncludedPath {path to file or directory}	<p>スキャンする必要がある共有ディレクトリオブジェクトへのパス。ディレクトリまたはファイルパスを指定できます。ファイルマスク(文字「?」および「*」の他、文字クラス「[]」、「[!]」、「[^]」を含む)を使用することもできます。</p> <p>リストをパラメータ値として指定できます。リストの値は、コンマ(引用符内の各値)で区切る必要があります。パラメータはセクションで複数回指定できます(この場合、そのすべての値が1つのリストにまとめられます)。</p> <p>例 : リストにファイル/etc/file1とディレクトリ/usr/binを追加します。</p>



	<p>1. 設定ファイルに値を追加します。</p> <ul style="list-style-type: none">• 1つの文字列に2つの値 <pre>[SMBSpider] IncludedPath = "/etc/file1", "/usr/bin"</pre> <ul style="list-style-type: none">• 2つの文字列 (文字列ごとに1つの値) <pre>[SMBSpider] IncludedPath = /etc/file1 IncludedPath = /usr/bin</pre> <p>2. コマンド drweb-ctl cfset を使用して値を追加します。</p> <pre># drweb-ctl cfset SMBSpider.IncludedPath - a /etc/file1 # drweb-ctl cfset SMBSpider.IncludedPath - a /usr/bin</pre> <p>ディレクトリを指定すると、ディレクトリのすべてのコンテンツがスキャンされます。</p> <p>このパラメータは ExcludedPath パラメータよりも優先されます (上の説明を参照)。つまり、同じオブジェクト (ファイルまたはディレクトリ) が両方のパラメータ値で指定されている場合、このオブジェクトはスキャンされます。</p> <p>デフォルト値: (未設定)</p>
<p>[*] AlertFiles</p> <p>{Boolean}</p>	<p>SMBディレクトリモニターによって悪意のあるものとしてブロックされたオブジェクトと同じディレクトリにテキストファイルを作成するかどうかを指定します。作成されたテキストファイルには、オブジェクトがブロックされた理由が記載されます。作成されたファイルは、<name of the blocked file>.drweb.alert.txt という名前になります。</p> <p>使用可能な値:</p> <ul style="list-style-type: none">• Yes - オブジェクトがブロックされた理由を説明するファイルを作成します。• No - ファイルを作成しません。 <p>デフォルト値: Yes</p>
<p>[*] OnKnownVirus</p> <p>{action}</p>	<p>SpIDer Guard for SMBによるスキャン中にシグネチャ解析を使用して検出された既知の脅威 (ウイルスなど) に対して Dr.Web for UNIX File Servers によって適用されるアクション。</p> <p>可能なアクション: <i>Block</i>、<i>Cure</i>、<i>Quarantine</i>、<i>Delete</i></p> <p>デフォルト値: <i>Cure</i></p>
<p>[*] OnIncurable</p> <p>{action}</p>	<p>SpIDer Guard for SMBによるスキャン中に検出された修復不可の脅威 (Cureの適用に失敗したもの) に対して Dr.Web for UNIX File Servers によって適用されるアクション。</p>



	<p>可能なアクション: <i>Block</i>、<i>Quarantine</i>、<i>Delete</i></p> <p>デフォルト値: <i>Quarantine</i></p>
<p>[*] OnSuspicious</p> <p>{action}</p>	<p>SpIDer Guard for SMBによるスキャン中にヒューリスティック解析を使用して検出された未知の脅威（または疑わしいオブジェクト）に対してDr.Web for UNIX File Serversによって適用されるアクション。</p> <p>可能なアクション: <i>Pass</i>、<i>Block</i>、<i>Quarantine</i>、<i>Delete</i></p> <p>デフォルト値: <i>Quarantine</i></p>
<p>[*] OnAdware</p> <p>{action}</p>	<p>SpIDer Guard for SMBによるスキャン中に検出されたアドウェアに対してDr.Web for UNIX File Serversによって適用されるアクション。</p> <p>可能なアクション: <i>Pass</i>、<i>Block</i>、<i>Quarantine</i>、<i>Delete</i></p> <p>デフォルト値: <i>Pass</i></p>
<p>[*] OnDialers</p> <p>{action}</p>	<p>SpIDer Guard for SMBによるスキャン中に検出されたダイヤラーに対してDr.Web for UNIX File Serversによって適用されるアクション。</p> <p>可能なアクション: <i>Pass</i>、<i>Block</i>、<i>Quarantine</i>、<i>Delete</i></p> <p>デフォルト値: <i>Pass</i></p>
<p>[*] OnJokes</p> <p>{action}</p>	<p>SpIDer Guard for SMBによるスキャン中に検出されたジョークに対してDr.Web for UNIX File Serversによって適用されるアクション。</p> <p>可能なアクション: <i>Pass</i>、<i>Block</i>、<i>Quarantine</i>、<i>Delete</i></p> <p>デフォルト値: <i>Pass</i></p>
<p>[*] OnRiskware</p> <p>{action}</p>	<p>SpIDer Guard for SMBによるスキャン中に検出されたリスクウェアに対してDr.Web for UNIX File Serversによって適用されるアクション。</p> <p>可能なアクション: <i>Pass</i>、<i>Block</i>、<i>Quarantine</i>、<i>Delete</i></p> <p>デフォルト値: <i>Pass</i></p>
<p>[*] OnHacktools</p> <p>{action}</p>	<p>SpIDer Guard for SMBによるスキャン中に検出されたハッキングツール（リモート管理用のツール、トロイの木馬など）に対してDr.Web for UNIX File Serversによって適用されるアクション。</p> <p>可能なアクション: <i>Pass</i>、<i>Block</i>、<i>Quarantine</i>、<i>Delete</i></p> <p>デフォルト値: <i>Pass</i></p>
<p>[*] BlockOnError</p> <p>{Boolean}</p>	<p>修復を試みたときにエラーが発生した場合や、SpIDer Guard for SMBモニターにファイルのスキャンを許可する有効なライセンスがない場合に、SpIDer Guard for SMBがファイルへのアクセスをブロックするかどうかを指定します。</p> <div><p>有効なライセンスがない場合、このパラメータがYesに設定されていると、SpIDer Guard for SMBは保護対象の共有ディレクトリに移動されたすべてのファイルをブロックします。</p></div>



	<p>使用可能な値：</p> <ul style="list-style-type: none">• Yes-ファイルへのアクセスをブロックします。• No - ファイルへのアクセスはブロックされません。 <p>デフォルト値：Yes</p>
<p>[*] ScanTimeout</p> <p>{time interval}</p>	<p>SpIDer Guard for SMBによって開始された1つのファイルに対するスキャンのタイムアウト。</p> <p>1秒から1時間の範囲の値を指定できます</p> <p>デフォルト値：30s</p>
<p>[*] HeuristicAnalysis</p> <p>{On / Off}</p>	<p>SpIDer Guard for SMBによるスキャン中に未知の脅威を検出するためにヒューリスティック解析を使用するかどうかを指定します。ヒューリスティック解析における検出の信頼性は高いのですが、ウイルススキャンに時間がかかります。</p> <p>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に適用されるアクションは、OnSuspiciousパラメータ値として指定します。</p> <p>使用可能な値：</p> <ul style="list-style-type: none">• On - スキャン時にヒューリスティック解析を使用するように指示します。• Off - ヒューリスティック解析を使用しないように指示します。 <p>デフォルト値：On</p>
<p>[*] PackerMaxLevel</p> <p>{integer}</p>	<p>圧縮されたオブジェクトスキャン時の最大ネスティングレベル。SpIDer Guard for SMBによるスキャン時に、下位のネストレベルにあるすべてのオブジェクトがスキップされます。</p> <p>0から60までの範囲の値を指定できます。値を0に設定すると、ネストしたオブジェクトはスキャンされません。</p> <p>デフォルト値：8</p>
<p>[*] ArchiveMaxLevel</p> <p>{integer}</p>	<p>アーカイブスキャン時の最大ネスティングレベル。SpIDer Guard for SMBによるスキャン時に、下位のネストレベルにあるすべてのオブジェクトがスキップされます。</p> <p>0から60までの範囲の値を指定できます。値を0に設定すると、ネストしたオブジェクトはスキャンされません。</p> <p>デフォルト値：0</p>
<p>[*] MailMaxLevel</p> <p>{integer}</p>	<p>メールメッセージとメールボックスをスキャンするときの最大ネストレベル。SpIDer Guard for SMBによるスキャン時に、下位のネストレベルにあるすべてのオブジェクトがスキップされます。</p> <p>0から60までの範囲の値を指定できます。値を0に設定すると、ネストしたオブジェクトはスキャンされません。</p> <p>デフォルト値：8</p>
<p>[*] ContainerMaxLevel</p> <p>{integer}</p>	<p>コンテナ（HTMLページなど）をスキャンするときの最大ネストレベル。SpIDer Guard for SMBによるスキャン時に、下位のネストレベルにあるすべてのオブジェクトがスキップされます。</p>



	<p>0から60までの範囲の値を指定できます。値を0に設定すると、ネストしたオブジェクトはスキャンされません。</p> <p>デフォルト値：8</p>
<p>[*] MaxCompressionRatio <i>{integer}</i></p>	<p>スキャンされるオブジェクトの最大圧縮率（圧縮サイズと非圧縮サイズの比率）。オブジェクトの比率が制限を超えると、そのオブジェクトはSpIDer Guard for SMBによるスキャン中にスキップされます。</p> <p>圧縮率には2よりも小さい値は指定できません。</p> <p>デフォルト値：500</p>

モニタリング設定をカスタマイズする

各共有ディレクトリ（ファイルストレージ）をモニタリングするVFS SMBモジュールごとに異なるタグを指定できます。指定は、SMBサーバー**Samba**の設定ファイル（通常はsmb.confファイル）で行います。smb.confファイル内のVFS SMBモジュールの一意のタグは、次のように指定します。

```
smb_spider:tag = <share name>
```

ここで、<share name>は、**Samba**サーバーによってVFS SMBモジュールに割り当てられる一意のタグであり、一部の共有ディレクトリを制御します。

VFS SMBモジュールに一意のタグ<share name>がある場合は、Dr.Web for UNIX File Serversの設定ファイルに[SMBSpider]の他に別のセクションを作成できます。作成したセクションには、このVFS SMBモジュールによって保護されている特定のファイルストレージをスキャンするためのすべての設定パラメータが保存されます。このセクションの名前は、[SMBSpider.Share.<share name>]のようになります。

VFS SMBモジュール用に作成されたセクションには、上のテーブルにアスタリスク「[*]」で指定したパラメータを含めることができます。SMBディレクトリモニターSpIDer Guard for SMBで動作するすべてのVFS SMBモジュールの動作はパラメータ値によって設定されるため、このような個別のセクションに他のパラメータを指定することはできません。

これらのパラメータが、このモジュール用に作成された個別のセクション[SMBSpider]に指定されていない場合、VFS SMBモジュールは一般セクション[SMBSpider.Share.<share name>]のパラメータ値を使用します。したがって、タグで示される個別のセクションが作成されていない場合、すべてのVFS SMBモジュールが共有ディレクトリのモニタリングに同じパラメータを使用します。[SMBSpider.Share.<share name>]セクションからパラメータを削除すると、このセクション（および<share name>を持つ対応する共有ディレクトリ）のパラメータ値は、一般[SMBSpider]セクションの同名の「親」パラメータから取得されます。この場合、デフォルトのパラメータ値は使用されません。

Dr.Web for UNIX File Servers管理用に**Dr.Web Ct**コマンドラインツールを使用して、共有**Samba**ディレクトリにタグ<share name>を持つ新しいセクションを追加するには（コマンドラインDr.Web Ctからソリューションを管理するために、drweb-ctlコマンドラインツールによって実行されます。**drweb-ctl**コマンドで実行します）、次のコマンドを使用します。

```
# drweb-ctl cfset SmbSpider.Share -a <share name>
```



例:

```
# drweb-ctl cfset SmbSpider.Share -a BuhFiles
# drweb-ctl cfset SmbSpider.Share.BuhFiles.OnAdware Quarantine
```

最初のコマンドは、設定ファイルに[SMBSpider.Share.BuhFiles]セクションを追加します。2つ目は、追加したセクションに上のテーブルの「[*]」記号が付いたすべてのパラメータが含まれるようにOnAdwareパラメータ値を変更します。OnAdwareを除き、[SMBSpider]セクションのパラメータ値と同じとなります。

Sambaファイルサーバーとの統合

Sambaサーバーとの統合方法については、[Sambaファイルサーバーとの統合](#)セクションを参照してください。

VFS SMBモジュールを構築する

このセクションの内容:

- [概要](#)
- [VFS SMBモジュールを構築する](#)

概要

Dr.Web for UNIX File Serversのインストール中に、ファイルサーバーで使用されている**Samba**のバージョンが、SpIDer Guard for SMBで提供されているVFS SMBモジュールと互換性がないことが検出された場合は、提供されているソースコードを使用して、VFS SMBモジュールを手動で構築する必要があります。

SpIDer Guard for SMB用のVFS SMBモジュールのソースコードは、drweb-smbspider-modules-srcという追加パッケージで提供され、tar.gzアーカイブに圧縮されています。drweb-smbspider-modules-srcパッケージには、drweb-smbspider-11.1.src.tar.gzアーカイブがソースコードとともに含まれています。このアーカイブは/usr/src/ディレクトリにあります。アーカイブがこのディレクトリにない場合は、ソースコードを使用してパッケージを手動でインストールします(Dr.Web for UNIX File Serversのインストール[方法](#)に応じて、[リポジトリ](#)から、またはユニバーサルパッケージの[カスタムインストールを使用](#))。

SpIDer Guard for SMBで使用するVFS SMBモジュールのソースコードの他に、ファイルサーバーにインストールされている**Samba**バージョンのソースコードも必要です。ソースコードがない場合は、開発者のソースからダウンロードしてください(例: <https://www.samba.org/samba/download/>)。ファイルサーバーにインストールされている**Samba**のバージョンを確認するには、次のコマンドを使用します。

```
$ smbld -V
```



SpIDer Guard for SMB用のVFS SMBモジュールを構築するには、サーバーに現在インストールされている**Samba**のバージョンのソースコードを使用する必要があります。それ以外のバージョンを使用した場合、SpIDer Guard for SMBの正しい動作は保証されません。

ソースコードから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。

VFS SMBモジュールを構築する

1. VFS SMBモジュールのソースコードを含むアーカイブを任意のディレクトリに解凍します。たとえば、次のようなコマンドです。

```
# tar -xf drweb-smbspider-11.1.src.tar.gz
```

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. サーバーにインストールされている**Samba**のバージョンを確認し、必要に応じてそのソースコードをダウンロードします。
3. サーバーにインストールされている**Samba**のバージョンが**CLUSTER_SUPPORT**オプションを使用しているかどうかを確認します。これを行うには、以下のコマンドを使用します。

```
$ smbld -b | grep CLUSTER_SUPPORT
```

出力されたものに**CLUSTER_SUPPORT**文字列が含まれている場合は、サーバーにインストールされている**Samba**バージョンのは**CLUSTER_SUPPORT**オプションを使用しています。

4. **Samba**のソースコードがあるディレクトリに移動し、設定(`./configure`)を実行してからサーバーの構築(`make`)を行います。設定時には、**CLUSTER_SUPPORT**に関わるオプションに正しい値を定義します。**Samba**の設定と構築方法については、開発者の公式マニュアル(<https://www.samba.org/samba/docs/>など)を参照してください。



ソースコードファイルからの**Samba**の構築は、次のステップでSpIDer Guard for SMBが使用するVFS SMBモジュールを正しく構築するためにのみ必要になります。サーバーにインストール済みの**Samba**をソースコードから構築された新しいバイナリに置き換える必要はありません。

5. **Samba**を正しく構築したら、VFS SMBモジュールのソースコードがあるディレクトリに移動して、次のコマンドを実行します。

```
# ./configure --with-samba-source=<path to dir with Samba src> && make
```

この場合、`<path to dir with Samba src>`は、前の手順で**Samba**を構築したディレクトリへのパスになります。

6. VFS SMBモジュールが正常に構築されたら、`libsmb_spider.so`バイナリファイルを`.libs`サブディレクトリ(構築中に作成)からインストール済みの**Samba**のVFSモジュールのディレクトリ(**GNU/Linux**の場合、デフォルトでは`/usr/lib/samba/vfs`)にコピーし、名前を`smb_spider.so`に変更します。これを行うには、以下のコマンドを使用します。

```
# cp ../libs/libsmb_spider.so /usr/lib/samba/vfs/smb_spider.so
```



7. 構築したVFS SMBモジュールをコピーしたら、VFS SMBモジュールと**Samba**サーバーを構築したディレクトリを削除できます。

その後、Dr.Web for UNIX File Serversと**Samba**サーバー間の統合を完了させる必要があります。その方法については、管理者マニュアルの[対応する](#)セクションに説明があります。この場合、統合の最初のステップで、インストール済みの**Samba**サーバーのVFSモジュールのディレクトリにsmb_spider.soシンボリックリンクを作成する必要はありません。



SpIDer Guard for NSS



このコンポーネントは、**GNU/Linux** OS用に設計されたディストリビューションにのみ含まれています。このコンポーネントは、**SUSE Linux Enterprise Server 10 SP3以降**をベースにした**Novell Open Enterprise Server SP2**上でのみ動作できます。

NSSボリュームモニターSpIDer Guard for NSSでは、NSS(**Novell Storage Services**)ファイルシステムボリューム上のファイルアクティビティを監視できます。このコンポーネントはデーモンモードで動作し、変更(作成、開始、終了)に関連するメインファイルシステムのイベントを制御します。このようなイベントが検出されると、モニターはファイルのコンテンツが変更されたかどうかを確認し、変更されている場合は、[Dr.Web File Checker](#)のタスクを生成して変更されたコンテンツをスキャンします。

動作原理

このセクションの内容:

- [概要](#)
- [スキャンオブジェクトへのパスを指定する](#)

概要

SpIDer Guard for NSSモニターはデーモンとして動作します(通常、OSの起動時に[Dr.Web ConfigD](#)設定デーモンによって起動されます)。このモニターは、その[設定](#)(**ProtectedVolumes**パラメータ)で指定されたこれらのNSSボリュームのみを監視し、制御します。NSSボリュームがマウントされるファイルシステムポイントは自動的に検出されます。新しいNSSファイルシステムボリュームがマウントまたはマウント解除されても、モニターは自動的に検出しません。NSSボリュームで新しいファイルまたは変更されたファイルが見つかったら、モニターは[Dr.Web File Checker](#)コンポーネントに、それをスキャンするように指示します。



NSSボリュームモニターには次のような機能があります。ファイルのコピー(保護されたボリュームへのコピーまたはNSSボリューム内のファイルのコピー)中に脅威が検出された場合に、SpIDer Guard for NSSは感染ファイルのコピーのみをマークします。元のファイルの脅威は検出されません。このファイルは、この(元の)ファイルへのアクセスを試みるまで、またはNSSボリューム上にあるこのファイルが変更されるまで安全と見なされます。

QuarantineアクションがNSSボリュームモニターの設定で、ある脅威のタイプに指定されている場合、このタイプの脅威を含むオブジェクトは、このオブジェクトを隔離からNSSボリュームに復元しようとした際に再び隔離に配置されます。たとえば、次のデフォルト[設定](#)があります。

```
NSS.OnKnownVirus = Cure  
NSS.OnIncurable = Quarantine
```

修復不可能なオブジェクトはすべて隔離に移動します。修復不可能なオブジェクトが隔離からNSSボリュームに復元されたときに自動的に隔離に戻されるのはこのためです。



スキャンオブジェクトへのパスを指定する

NSSボリュームのモニターSpIDer Guard for NSSは、保護されたボリューム(**ProtectedVolumes**パラメータ)にあるオブジェクトと、指定されたパス(**ExcludedPath**パラメータで指定されたものと一致しないもの、または**IncludedPath**パラメータで指定したパスと一致するもの)のみをチェックします。このパラメータはパラメータ**ExcludedPath**よりも優先されます。オブジェクトへのパスが両方のパラメータで指定されている場合、このオブジェクトはスキャンされます。たとえば、あるディレクトリ内のファイルが頻繁に変更され、その結果これらのファイルが繰り返しスキャンされ、システムの負荷が増大する場合に便利です。ディレクトリ内のファイルの頻繁な変更がウイルスによるものではなく信頼できるプログラムの操作によるものであることが確実に分かっている場合は、このディレクトリまたはこれらのファイルへのパスを除外リストに追加できます。この場合、NSSボリュームモニターSpIDer Guard for NSSはこれらのオブジェクトの変更に対する応答を停止します。**ExcludedPath**パラメータで指定したパスの内側にあるいくつかのオブジェクトのスキャンを許可する場合は、**IncludedPath**パラメータを使用するほうが適しています。

ボリュームvol1、vol2、vol3を持つシステムにおけるモニター設定の例を考えます。

```
ProtectedVolumes =  
ExcludedPath = vol1/path1, vol1/path2, vol2/sys  
IncludedPath = vol1/path1, vol1/path2/incl, vol2/doc
```

指定されたパラメータに従って、モニターはボリュームvol13内のすべてのファイル(スキャン制限なし)、ボリュームvol2内のすべてのファイル(/sysディレクトリとそのすべてのサブディレクトリ内のファイルを除く)をチェックします。ボリュームvol1では、/path2ディレクトリ内のファイルはチェックされません。ただし、このボリュームvol1の他のディレクトリにあるファイルは、/path2/inclディレクトリのコンテンツと同様にチェックされます。両方のリストで同じパス(この場合はvol1/path)を指定しても意味がありません。パススキャンに制限がなくなるためです。また、**IncludedPath**パラメータでパスvol2/docを指定しても意味がありません。このディレクトリはボリュームvol2に設定された除外対象には含まれず、/sysディレクトリのみが対象となるためです。

パラメータ**IncludedPath**と**ExcludedPath**では、ファイルマスク(ワイルドカード)を使用できます。たとえば、次のような設定です。

```
ExcludedPath = vol1/*.txt
```

この場合、ボリュームvol1(NSSボリュームのマウントポイントのディレクトリvol1にマウントされたボリューム)のスキャンから、「*.txt」マスクに一致するすべてのファイルが除外されます。パラメータ**IncludedPath**および**ExcludedPath**で指定されるパスの大文字と小文字を区別するかどうかは、NSS設定によって定義されます。

コマンドライン引数

SpIDer Guard for NSSを実行するには、コマンドラインに次のコマンドを入力します。

```
$ <opt_dir>/bin/drweb-nss [<parameters>]
```

SpIDer Guard for NSSは次のオプションを処理できます。

パラメータ	説明
-------	----



<code>--help</code>	<p>機能：コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了するように指示します。</p> <p>短縮形： <code>-h</code></p> <p>引数： None</p>
<code>--version</code>	<p>機能：このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了するように指示します。</p> <p>短縮形： <code>-v</code></p> <p>引数： None</p>

例：

```
$ /opt/drweb.com/bin/drweb-nss --help
```

このコマンドはSpIDer Guard for NSSに関する簡単なヘルプ情報を出力します。

スタートアップノート

コンポーネントは、自律モードで（他のコンポーネントから自律的に）OSのコマンドラインから直接起動することはできません。[Dr.Web ConfigD](#)設定デーモンによって自動的に起動します（OSの起動時）。コンポーネントの動作を管理するには、Dr.Web for UNIX File Servers用の[Dr.Web Ctl](#)コマンドラインベースの管理ツールを使用できます（これは**`drweb-ctl`**コマンドを使用して呼び出されます）。



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ドキュメントを要求するには、次のコマンドを使用します。**`man 1 drweb-nss`**

設定パラメータ

コンポーネントは、Dr.Web for UNIX File Serversの統合された[設定ファイル](#)の[NSS]セクションで指定されている設定パラメータを使用します。

セクションには以下のパラメータが含まれています。

LogLevel <i>{logging level}</i>	コンポーネントの ログの詳細レベル パラメータ値が指定されていない場合は、[Root] セクション の DefaultLogLevel パラメータの値が使用されます。 デフォルト値：Notice
Log <i>{log type}</i>	コンポーネントの ロギング方式 。 デフォルト値：Auto
LogProtocol <i>{Boolean}</i>	プロトコルメッセージがNSSボリュームモニターSpIDer Guard for NSSのログファイルに登録されているかどうかを示します。 使用可能な値： <ul style="list-style-type: none">• Yes - メッセージが登録されています。



	<ul style="list-style-type: none">• No - メッセージが登録されません。 デフォルト値 : No
ExePath <i>{path to file}</i>	コンポーネントの実行ファイルへのパス。 デフォルト値 : <opt_dir>/bin/drweb-nss <ul style="list-style-type: none">• GNU/Linuxの場合 : /opt/drweb.com/bin/drweb-nss
Start <i>{Boolean}</i>	コンポーネントは Dr.Web ConfigD 設定デーモンによって起動される必要があります。 このパラメータにYes値を指定すると、設定デーモンはただちにコンポーネントを開始するように指示されます。また、No値を指定すると、設定デーモンはただちにコンポーネントを終了するように指示されます。 デフォルト値 : No
ProtectedVolumes <i>{volume name}</i>	NSSボリュームにマウントされ、スイートによって保護されているNSSファイルシステムボリュームの名前。値を指定しない場合、NSSボリュームマウントポイントにあるすべてのボリュームを保護する必要があります。 リストをパラメータ値として指定できます。リストの値は、コンマ(引用符内の各値)で区切る必要があります。パラメータはセクションで複数回指定できます(この場合、そのすべての値が1つのリストにまとめられます)。 例 : ボリュームvol1とvol2のリストに追加します。 1. 設定ファイルに値を追加します。 <ul style="list-style-type: none">• 1つの文字列に2つの値 <div><pre>[NSS] ProtectedVolumes = "vol1", "vol2"</pre></div> <ul style="list-style-type: none">• 2つの文字列(文字列ごとに1つの値) <div><pre>[NSS] ProtectedVolumes = vol1 ProtectedVolumes = vol2</pre></div> 2. コマンドdrweb-ctl cfsetを使用して値を追加します。 <div><pre># drweb-ctl cfset NSS.ProtectedVolumes -a vol1 # drweb-ctl cfset NSS.ProtectedVolumes -a vol2</pre></div> デフォルト値 : (未設定)
ExcludedPath <i>{path to file or directory}</i>	スキャン中にスキップする必要があるオブジェクトへのパス。ディレクトリまたはファイルパスを指定できます。ディレクトリを指定すると、サブディレクトリを含むディレクトリのすべてのコンテンツがスキップされます。例外は、パラメータIncludedPathで指定されるオブジェクトパスです。このようなオブジェクトはスキャン対象になります。 リストをパラメータ値として指定できます。リストの値は、コンマ(引用符内の各値)で区切る必要があります。パラメータはセクションで複数回指定できます(この場合、そのすべての値が1つのリストにまとめられます)。



	<p>例：リストにファイル/etc/file1とディレクトリ/usr/binを追加します。</p> <ol style="list-style-type: none">1. 設定ファイルに値を追加します。<ul style="list-style-type: none">● 1つの文字列に2つの値<pre>[NSS] ExcludedPath = "/etc/file1", "/usr/bin"</pre><ul style="list-style-type: none">● 2つの文字列（文字列ごとに1つの値）<pre>[NSS] ExcludedPath = /etc/file1 ExcludedPath = /usr/bin</pre>2. <u>コマンド</u> drweb-ctl cfsetを使用して値を追加します。 <pre># drweb-ctl cfset NSS.ExcludedPath - a /etc/file1 # drweb-ctl cfset NSS.ExcludedPath -a /usr/bin</pre> <p>このパラメータを使用すると、ファイルマスク（ワイルドカード）を使用できます。指定したパスの大文字と小文字の区別は、NSS設定によって定義されます。</p> <p>リスト内のパスは、NSSボリュームマウントポイントに示されているパスからの相対パスにする必要があります。</p> <p>デフォルト値：（未設定）</p>
<p>IncludedPath</p> <p><i>{path to file or directory}</i></p>	<p>スキャンする必要があるオブジェクトへのパス。ディレクトリまたはファイルパスを指定できます。ディレクトリを指定すると、ディレクトリのすべてのコンテンツがスキャンされます。</p> <p>このパラメータは、ExcludedPathパラメータで指定されているオブジェクト（ファイルとサブディレクトリ）のパスのスキャンを個別に許可する場合にのみ使用できます。また、このパラメータはパラメータExcludedPathよりも優先されます。オブジェクトへのパスが両方のパラメータで指定されている場合、このオブジェクトはスキャンされます。</p> <p>リストをパラメータ値として指定できます。リストの値は、コンマ（引用符内の各値）で区切る必要があります。パラメータはセクションで複数回指定できます（この場合、そのすべての値が1つのリストにまとめられます）。</p> <p>例：リストにファイル/etc/file1とディレクトリ/usr/binを追加します。</p> <ol style="list-style-type: none">1. 設定ファイルに値を追加します。<ul style="list-style-type: none">● 1つの文字列に2つの値<pre>[NSS] IncludedPath = "/etc/file1", "/usr/bin"</pre><ul style="list-style-type: none">● 2つの文字列（文字列ごとに1つの値）



	<div>[NSS] IncludedPath = /etc/file1 IncludedPath = /usr/bin</div> <p>2. コマンド <code>drweb-ctl cfset</code> を使用して値を追加します。</p> <div># drweb-ctl cfset NSS.IncludedPath - a /etc/file1 # drweb-ctl cfset NSS.IncludedPath -a /usr/bin</div> <p>このパラメータを使用すると、ファイルマスク (ワイルドカード) を使用できません。指定したパスの大文字と小文字の区別は、NSS設定によって定義されます。</p> <p>リスト内のパスは、NSSボリュームマウントポイントに示されているパスからの相対パスにする必要があります。</p> <p>デフォルト値: (未設定)</p>
OnKnownVirus {action}	<p>NSSボリュームモニターによるスキャン中にシグネチャ解析で検出された既知の脅威 (ウイルスなど) に対して Dr.Web for UNIX File Serversによって適用されるアクション。</p> <p>可能なアクション: <i>Cure</i>、<i>Quarantine</i>、<i>Delete</i></p> <p>デフォルト値: <i>Cure</i></p>
OnIncurable {action}	<p>NSSボリュームモニターで開始されたスキャン中に検出された修復不可能な脅威 (つまり、<i>Cure</i> の適用に失敗したもの) に対して Dr.Web for UNIX File Serversに適用されたアクション。</p> <p>可能なアクション: <i>Quarantine</i>、<i>Delete</i></p> <p>デフォルト値: <i>Quarantine</i></p>
OnSuspicious {action}	<p>NSSボリュームモニターによるスキャン中にヒューリスティック解析を使用して検出された未知の脅威 (または疑わしいオブジェクト) に対して Dr.Web for UNIX File Serversによって適用されるアクション。</p> <p>可能なアクション: <i>Report</i>、<i>Quarantine</i>、<i>Delete</i></p> <p>デフォルト値: <i>Quarantine</i></p>
OnAdware {action}	<p>NSSボリュームモニターによるスキャン中に検出されたアドウェアに対して Dr.Web for UNIX File Serversによって適用されるアクション。</p> <p>可能なアクション: <i>Report</i>、<i>Quarantine</i>、<i>Delete</i></p> <p>デフォルト値: <i>Report</i></p>
OnDialers {action}	<p>NSSボリュームモニターによるスキャン中に検出されたダイアラーに対して Dr.Web for UNIX File Serversによって適用されるアクション。</p> <p>可能なアクション: <i>Report</i>、<i>Quarantine</i>、<i>Delete</i></p> <p>デフォルト値: <i>Report</i></p>



OnJokes <i>{action}</i>	NSSボリュームモニターによるスキャン中に検出されたジョークプログラムに対してDr.Web for UNIX File Serversによって適用されるアクション。 可能なアクション: <i>Report</i> 、 <i>Quarantine</i> 、 <i>Delete</i> デフォルト値: <i>Report</i>
OnRiskware <i>{action}</i>	NSSボリュームモニターによるスキャン中に検出されたリスクウェアに対してDr.Web for UNIX File Serversによって適用されるアクション。 可能なアクション: <i>Report</i> 、 <i>Quarantine</i> 、 <i>Delete</i> デフォルト値: <i>Report</i>
OnHacktools <i>{action}</i>	NSSボリュームモニターによるスキャン中に検出されたハッキングツール(リモート管理用のツール、トロイの木馬など)に対してDr.Web for UNIX File Serversによって適用されるアクション。 可能なアクション: <i>Report</i> 、 <i>Quarantine</i> 、 <i>Delete</i> デフォルト値: <i>Report</i>
OnError <i>{action}</i>	NSSボリュームモニターによるスキャン中にエラーの原因となったファイルに対してDr.Web for UNIX File Serversによって適用されるアクション。 可能なアクション: <i>Report</i> 、 <i>Quarantine</i> 、 <i>Delete</i> デフォルト値: <i>Report</i>
ScanTimeout <i>{time interval}</i>	NSSボリュームモニターによる1つのファイルに対するスキャンのタイムアウト。 <i>1秒から1時間の範囲の値を指定できます</i> デフォルト値: <i>30s</i>
HeuristicAnalysis <i>{On / Off}</i>	NSSボリュームモニターによるスキャン中に未知の脅威を検出するためにヒューリスティック解析を使用するかどうかを指定します。ヒューリスティック解析における検出の信頼性は高いのですが、ウイルススキャンに時間がかかります。 <i>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に適用されるアクションは、OnSuspiciousパラメータ値として指定します。</i> 使用可能な値: <ul style="list-style-type: none">• <i>On</i> - スキャン時にヒューリスティック解析を使用するように指示します。• <i>Off</i> - ヒューリスティック解析を使用しないように指示します。 デフォルト値: <i>On</i>
PackerMaxLevel <i>{integer}</i>	圧縮されたオブジェクトスキャン時の最大ネスティングレベル。NSSボリュームモニターによるスキャン中に、より深いネストレベルのすべてのオブジェクトがスキップされます。 <i>0から60までの範囲の値を指定できます。値を0に設定すると、ネストしたオブジェクトはスキャンされません。</i> デフォルト値: <i>8</i>



ArchiveMaxLevel <i>{integer}</i>	<p>アーカイブスキャン時の最大ネスティングレベル。NSSボリュームモニターによるスキャン中に、より深いネストレベルのすべてのオブジェクトがスキップされます。</p> <p>0から60までの範囲の値を指定できます。値を0に設定すると、ネストしたオブジェクトはスキャンされません。</p> <p>デフォルト値：0</p>
MailMaxLevel <i>{integer}</i>	<p>メールメッセージとメールボックスをスキャンするときの最大ネストレベル。NSSボリュームモニターによるスキャン中に、より深いネストレベルのすべてのオブジェクトがスキップされます。</p> <p>0から60までの範囲の値を指定できます。値を0に設定すると、ネストしたオブジェクトはスキャンされません。</p> <p>デフォルト値：8</p>
ContainerMaxLevel <i>{integer}</i>	<p>コンテナをスキャンする際の最大ネストレベル。NSSボリュームモニターによるスキャン中に、より深いネストレベルのすべてのオブジェクトがスキップされます。</p> <p>0から60までの範囲の値を指定できます。値を0に設定すると、ネストしたオブジェクトはスキャンされません。</p> <p>デフォルト値：8</p>
MaxCompressionRatio <i>{integer}</i>	<p>スキャンされるオブジェクトの最大圧縮率（圧縮サイズと非圧縮サイズの比率）。オブジェクトの比率が制限を超えると、そのオブジェクトはNSSボリュームモニターによるスキャン中にスキップされます。</p> <p>圧縮率には2よりも小さい値は指定できません。</p> <p>デフォルト値：500</p>



QuarantineアクションがNSSボリュームモニターの設定で、ある脅威のタイプに指定されている場合、このタイプの脅威を含むオブジェクトは、このオブジェクトを隔離からNSSボリュームに復元しようとした際に再び隔離に配置されます。たとえば、次のデフォルト設定があります。

NSS.OnKnownVirus = Cure
NSS.OnIncurable = Quarantine

修復不可能なオブジェクトはすべて隔離に移動します。修復不可能なオブジェクトが隔離からNSSボリュームに復元されたときに自動的に隔離に戻るのとはこのためです。

NSSボリュームとの統合

NSSボリュームとの統合方法については、[NSSボリュームとの統合](#)セクションを参照してください。



Dr.Web ClamD

Dr.Web ClamDコンポーネントは、Sourcefire, Inc.のアンチウイルス製品**Clam AntiVirus (ClamAV®)**のコアコンポーネントである**clamd**アンチウイルスデーモンのインターフェースを使用してエミュレーションを実行します。このインターフェースにより、**ClamAV®**とやり取りできる外部アプリケーションは、アンチウイルススキャンにDr.Web for UNIX File Serversを使用できます。

動作原理

このコンポーネントは、ローカルファイルシステムのファイルの内容と、ソケットを介して外部アプリケーションによって送信されたデータのストリームの両方をチェックします。このようなチェックは、外部アプリケーションのリクエストに応じてコンポーネントによって実行されます。さらに、コンポーネントは外部アプリケーションがソケットを介してオープンファイル記述子(ディスクリプタ)を渡したファイルの内容をチェックできます。



渡されたファイル記述子に基づくファイルスキャンは、記述子がローカルのUNIXソケットを介して渡された場合にのみ実行できます。

外部アプリケーションからローカルファイルシステム内のファイルへのパスが提供された場合、コンポーネントはスキャンタスクを[Dr.Web File Checker](#)ファイルチェッカーコンポーネントに送信します。それ以外の場合、コンポーネントは、ソケット経由で受信したデータを[Dr.Web Network Checker](#)に送信します。

デフォルトでは、コンポーネントはDr.Web for UNIX File Serversの起動時に自動的に起動されません。コンポーネントの起動を有効にするには、開始パラメータにYesの値を[設定](#)し、クライアントアプリケーション用に少なくとも1つの接続ポイントを定義する必要があります。その後、コンポーネントは外部アプリケーションからのファイルまたはデータストリームのスキャンリクエストの待機を開始します。コンポーネントの設定では、外部アプリケーション用に複数の接続ポイントを設定し、必要に応じて各ポイントに異なるスキャン設定を調整できます。

外部アプリケーションは、**clamd**との統合モジュールを装備している場合には、ファイルサービスサーバー(**Samba**や**ProFTPd**など)として表すことができます。詳細は、[外部アプリケーションとの統合](#)のセクションを参照してください。



検出された脅威はDr.Web for UNIX File Serversで駆除することはできません。外部アプリケーションにはスキャンの結果のみが通知されます。そのため、検出された脅威はすべて外部アプリケーションで駆除する必要があります。

コマンドライン引数

Dr.Web ClamDを実行するには、コマンドラインに次のコマンドを入力します。

```
$ <opt_dir>/bin/drweb-clamd [<parameters>]
```

Dr.Web ClamDは次のパラメータを処理できます。

パラメータ	説明
-------	----



<code>--help</code>	<p>機能：コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了するように指示します。</p> <p>短縮形： <code>-h</code></p> <p>引数： None</p>
<code>--version</code>	<p>機能：このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了するように指示します。</p> <p>短縮形： <code>-v</code></p> <p>引数： None</p>

例：

```
$ /opt/drweb.com/bin/drweb-clamd --help
```

このコマンドはDr.Web ClamDに関する簡単なヘルプ情報を出力します。

スタートアップノート

コンポーネントは、自律モードで（他のコンポーネントから自律的に）OSのコマンドラインから直接起動することはできません。必要に応じてDr.Web ConfigD設定デーモンによって自動的に起動されます（原則として、OSの起動時）。コンポーネントの動作を管理するには、Dr.Web for UNIX File Servers用のDr.Web Ctlコマンドラインベースの管理ツールを使用できます（これは**drweb-ctl**コマンドを使用して呼び出されます）。



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ドキュメントを要求するには、次のコマンドを使用します。**man 1 drweb-clamd**

設定パラメータ

コンポーネントは、Dr.Web for UNIX File Serversの統合された**設定ファイル**の[ClamD]セクションで指定されている設定パラメータを使用します。

- [コンポーネントパラメータ](#)。
- [コンポーネント構成の特別な側面](#)。

コンポーネントパラメータ

セクションには以下のパラメータが含まれています。

LogLevel <i>{logging level}</i>	<p>コンポーネントのログの詳細レベル</p> <p>パラメータ値が指定されていない場合は、[Root]セクションのDefaultLogLevelパラメータの値が使用されます。</p> <p>デフォルト値：Notice</p>
Log	<p>コンポーネントのロギング方式。</p> <p>デフォルト値：Auto</p>



<i>{log type}</i>	
ExePath <i>{path to file}</i>	コンポーネントの実行ファイルへのパス。 デフォルト値: <code><opt_dir>/bin/drweb-clamd</code> <ul style="list-style-type: none">• GNU/Linuxの場合 合: <code>/opt/drweb.com/bin/drweb-clamd</code>• FreeBSDの場合 合: <code>/usr/local/libexec/drweb.com/bin/drweb-clamd</code>
Start <i>{Boolean}</i>	コンポーネントは Dr.Web ConfigD 設定デーモンによって起動する必要があります。 このパラメータに <code>Yes</code> 値を指定すると、設定デーモンはただちにコンポーネントを開始するように指示されます。また、 <code>No</code> 値を指定すると、設定デーモンはただちにコンポーネントを終了するように指示されます。 デフォルト値: <code>No</code>
<code>Endpoint.<tag>.ClamdSocket</code> <i>{IP address / UNIX socket}</i>	<code><tag></code> という名前の新しい接続ポイントを定義し、ファイルの脅威をスキャンする必要があるクライアントにソケット (IPv4 アドレスまたは UNIX ソケットのアドレス) を割り当てます。 <i>1つの<tag>ポイントに指定できるソケットは1つのみです。</i> デフォルト値: (未設定)
<code>[Endpoint.<tag>.]DetectSuspicious</code> <i>{Boolean}</i>	ヒューリスティックアナライザによって検出された疑わしいファイルについて通知します。 <code>Endpoint.<tag></code> のプレフィックスが指定されている場合は、パラメータの値が <code><tag></code> 接続ポイントにのみ設定されることを意味します。それ以外の場合は、このパラメータに別の値が指定されていないすべてのポイントに設定されます。 デフォルト値: <code>Yes</code>
<code>[Endpoint.<tag>.]DetectAdware</code> <i>{Boolean}</i>	アドウェアを含むファイルについて通知します。 <code>Endpoint.<tag></code> のプレフィックスが指定されている場合は、パラメータの値が <code><tag></code> 接続ポイントにのみ設定されることを意味します。それ以外の場合は、このパラメータに別の値が指定されていないすべてのポイントに設定されます。 デフォルト値: <code>Yes</code>
<code>[Endpoint.<tag>.]DetectDialers</code> <i>{Boolean}</i>	ダイヤラーを含むファイルについて通知します。 <code>Endpoint.<tag></code> のプレフィックスが指定されている場合は、パラメータの値が <code><tag></code> 接続ポイントにのみ設定されることを意味します。それ以外の場合は、こ



	<p>のパラメータに別の値が指定されていないすべてのポイントに設定されます。</p> <p>デフォルト値: Yes</p>
<p>[Endpoint.<tag>.]DetectJokes</p> <p>{Boolean}</p>	<p>ジョークプログラムを含むファイルについて通知します。</p> <p>Endpoint.<tag>のプレフィックスが指定されている場合は、パラメータの値が<tag>接続ポイントにのみ設定されることを意味します。それ以外の場合は、このパラメータに別の値が指定されていないすべてのポイントに設定されます。</p> <p>デフォルト値: No</p>
<p>[Endpoint.<tag>.]DetectRiskware</p> <p>{Boolean}</p>	<p>リスクウェアを含むファイルについて通知します。</p> <p>Endpoint.<tag>のプレフィックスが指定されている場合は、パラメータの値が<tag>接続ポイントにのみ設定されることを意味します。それ以外の場合は、このパラメータに別の値が指定されていないすべてのポイントに設定されます。</p> <p>デフォルト値: No</p>
<p>[Endpoint.<tag>.]DetectHacktools</p> <p>{Boolean}</p>	<p>ハッキングツールを含むファイルについて通知します。</p> <p>Endpoint.<tag>のプレフィックスが指定されている場合は、パラメータの値が<tag>接続ポイントにのみ設定されることを意味します。それ以外の場合は、このパラメータに別の値が指定されていないすべてのポイントに設定されます。</p> <p>デフォルト値: No</p>
<p>[Endpoint.<tag>.]ReadTimeout</p> <p>{time interval}</p>	<p>クライアントからのデータを待つ最大タイムアウトを設定します。</p> <p>Endpoint.<tag>のプレフィックスが指定されている場合は、パラメータの値が<tag>接続ポイントにのみ設定されることを意味します。それ以外の場合は、このパラメータに別の値が指定されていないすべてのポイントに設定されます。</p> <p>デフォルト値: 5s</p>
<p>[Endpoint.<tag>.]StreamMaxLength</p> <p>{size}</p>	<p>クライアントから受信できるデータの最大サイズを設定します (スキャンするデータをバイトのストリームとして送信するため)。</p> <p>Endpoint.<tag>のプレフィックスが指定されている場合は、パラメータの値が<tag>接続ポイントにのみ設定されることを意味します。それ以外の場合は、このパラメータに別の値が指定されていないすべてのポイントに設定されます。</p> <p>デフォルト値: 25mb</p>



<code>[Endpoint.<tag>.] ScanTimeout</code> <code>{time interval}</code>	<p>クライアントから受信した1つのファイル（またはデータの一部）をスキャンする最大時間を設定します。</p> <p>1秒から1時間の範囲の値を指定できます。</p> <p>Endpoint.<tag>のプレフィックスが指定されている場合は、パラメータの値が<tag>接続ポイントにのみ設定されることを意味します。それ以外の場合は、このパラメータに別の値が指定されていないすべてのポイントに設定されます。</p> <p>デフォルト値：3m</p>
<code>[Endpoint.<tag>.] HeuristicAnalysis</code> <code>{On / Off}</code>	<p>スキャンにヒューリスティック解析を使用するかどうかを示します。</p> <p>Endpoint.<tag>のプレフィックスが指定されている場合は、パラメータの値が<tag>接続ポイントにのみ設定されることを意味します。それ以外の場合は、このパラメータに別の値が指定されていないすべてのポイントに設定されます。</p> <p>デフォルト値：On</p>
<code>[Endpoint.<tag>.] PackerMaxLevel</code> <code>{integer}</code>	<p>スキャンできるパックオブジェクトの最大ネストレベルを設定します。</p> <p>0から60までの範囲の値を指定できます。値を0に設定すると、ネストしたオブジェクトはスキャンされません。</p> <p>Endpoint.<tag>のプレフィックスが指定されている場合は、パラメータの値が<tag>接続ポイントにのみ設定されることを意味します。それ以外の場合は、このパラメータに別の値が指定されていないすべてのポイントに設定されます。</p> <p>デフォルト値：8</p>
<code>[Endpoint.<tag>.] ArchiveMaxLevel</code> <code>{integer}</code>	<p>スキャンできるアーカイブの最大ネストレベルを設定します。</p> <p>0から60までの範囲の値を指定できます。値を0に設定すると、ネストしたオブジェクトはスキャンされません。</p> <p>Endpoint.<tag>のプレフィックスが指定されている場合は、パラメータの値が<tag>接続ポイントにのみ設定されることを意味します。それ以外の場合は、このパラメータに別の値が指定されていないすべてのポイントに設定されます。</p> <p>デフォルト値：8</p>
<code>[Endpoint.<tag>.] MailMaxLevel</code> <code>{integer}</code>	<p>スキャンできるメールファイルの最大ネストレベルを設定します。</p>



	<p>0から60までの範囲の値を指定できます。値を0に設定すると、ネストしたオブジェクトはスキャンされません。</p> <p>Endpoint.<tag>のプレフィックスが指定されている場合は、パラメータの値が<tag>接続ポイントにのみ設定されることを意味します。それ以外の場合は、このパラメータに別の値が指定されていないすべてのポイントに設定されます。</p> <p>デフォルト値：8</p>
<p>[Endpoint.<tag>.]ContainerMaxLevel</p> <p>{integer}</p>	<p>スキャンできるコンテナ内のオブジェクトの最大ネストレベルを設定します。</p> <p>0から60までの範囲の値を指定できます。値を0に設定すると、ネストしたオブジェクトはスキャンされません。</p> <p>Endpoint.<tag>のプレフィックスが指定されている場合は、パラメータの値が<tag>接続ポイントにのみ設定されることを意味します。それ以外の場合は、このパラメータに別の値が指定されていないすべてのポイントに設定されます。</p> <p>デフォルト値：8</p>
<p>[Endpoint.<tag>.]MaxCompressionRatio</p> <p>{integer}</p>	<p>圧縮/パックされたオブジェクトの最大許容圧縮率（非圧縮サイズと圧縮サイズの比率）を設定します。オブジェクトの比率が制限を超えると、そのオブジェクトはスキャン中にスキップされます。</p> <p>圧縮率には2よりも小さい値は指定できません。</p> <p>デフォルト値：500</p>

コンポーネント構成の特別な側面

オプションのEndpoint.<tag>プレフィックスが付いているパラメータはグループ化できます。各グループは、クライアントがコンポーネントへの接続に使用する固有の接続ポイント(エンドポイント)を定義し、固有の<tag>IDが割り当てられています。同じグループに属するすべてのスキャンパラメータは、対応する接続ポイントに接続されているクライアントに対してデータがスキャンされる場合にのみ適用可能な設定を定義します。パラメータがEndpoint.<tag>のプレフィックスなしで指定されている場合は、すべての接続ポイントの値が設定されます。接続ポイントからパラメータを削除した場合は、このパラメータをプログラムのハードコードされたデフォルト値に戻す代わりに、同じ名前の対応する「親」パラメータの現在の値を使用します(Endpoint.<tag>プレフィックスなしで設定)。



ClandSocketパラメータは、リスニングソケットとこのソケットが対応するグループ(接続ポイント)の両方を定義するため、必ずEndpoint.<tag>プレフィックスを付けて指定する必要があります。



例:

外部アプリケーション(サーバー)の2つのグループに対して2つの接続ポイントを設定する必要があるとします。グループをそれぞれ *servers1* と *servers2* と呼びます。また、*servers1* グループのサーバーはUNIXソケットを介して接続できますが、*servers2* グループのサーバーはネットワーク接続を介して接続できます。さらに、ヒューリスティック解析はデフォルトで無効にする必要がありますが、*servers2* グループのサーバーには使用する必要があるとします。次の例は、これを設定する方法を示しています。

1) **設定ファイル**で以下のように設定します。

```
[ClamD]
HeuristicAnalysis = Off

[ClamD.Endpoint.servers1]
ClamSocket = /tmp/srv1.socket

[ClamD.Endpoint.servers2]
ClamSocket = 127.0.0.1:1234
HeuristicAnalysis = On
```

2) コマンドラインベースの管理ツール **Dr.Web Ctl** の場合:

```
# drweb-ctl cfset ClamD.HeuristicAnalysis Off
# drweb-ctl cfset ClamD.Endpoint -a servers1
# drweb-ctl cfset ClamD.Endpoint -a servers2
# drweb-ctl cfset ClamD.Endpoint.servers1.ClamSocket /tmp/srv1.socket
# drweb-ctl cfset ClamD.Endpoint.servers2.ClamSocket 127.0.0.1:1234
# drweb-ctl cfset ClamD.Endpoint.servers2.HeuristicAnalysis On
```



どちらの方法でも効果は同じですが、設定ファイルを編集する場合は、**drweb-configd** コンポーネントに **SIGHUP** 信号を送信して変更した設定を適用する必要があります(これを行うには **drweb-ctl** の **reload** コマンドを発行します)。

外部アプリケーションとの統合

clamad アンチウイルスデーモン(**ClamAV**に含まれています)の1つをエミュレートするこのインターフェースによって、Dr.Web ClamDは**clamd** アンチウイルスデーモンに接続できる外部アプリケーションと通信できます。

以下の表は、アンチウイルススキャンに**clamd**を使用できるアプリケーションの例を示しています。

製品	統合
ファイルサービス	
FTPサーバー ProFTPd	clamd の使い方: FTP経由でサーバーにアップロードされたファイルのスキャン。 統合要件: 追加モジュールの <code>mod_clamav</code> を使用して ProFTPd を構築します。 ドキュメントへのリンク:



製品	統合
	ProFTPd のドキュメント: http://www.proftpd.org/docs/ mod_clamavの説明とソースコードファイル: https://github.com/jbenden/mod_clamav

clamd アンチウイルスデーモンと同様に、Dr.Web ClamDと直接通信する外部ソフトウェアコンポーネントの設定で、**clamd**に接続するためのアドレスをUNIXソケットまたは設定された接続ポイント(エンドポイント)の1つでDr.Web ClamDにリッスンされるTCPソケットへのパスとして指定します。

ProFTPdのDr.Web ClamDへの接続例:

1. Dr.Web ClamDの設定:

```
[ClamD]
Start = yes

[ClamD.Endpoint.ftps]
ClamdSocket = 127.0.0.1:3310
```

2. **ProFTPd**の設定:

```
ClamAV on
ClamServer 127.0.0.1
ClamPort 3310
```



Dr.Web File Checker

ファイルスキャンコンポーネントDr.Web File Checkerは、ファイルシステムのファイルとディレクトリをスキャンするように設計されています。ファイルシステムオブジェクトをスキャンするためにDr.Web for UNIX File Serversの他のコンポーネントによって使用されます。さらに、このコンポーネントは隔離されたファイルを保存しているディレクトリの内容を管理するため、隔離マネージャーとしても機能します。

動作原理

このコンポーネントは、すべての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）へのアクセスに使用されます。スーパーユーザー（*root*）権限で起動します。

スキャン済みのすべてのファイルとディレクトリにインデックスを付け、特別なキャッシュで確認されたオブジェクトに関するすべてのデータを保存し、すでにスキャン済みのオブジェクトやそれ以来変更されていないオブジェクトを繰り返しスキャンしないようにします（この場合は、そうしたオブジェクトのスキャンリクエストを受信する際に、キャッシュから取得した以前のスキャン結果が返されます）。

ファイルシステムオブジェクトを確認するリクエストがDr.Web for UNIX File Serversのコンポーネントから受信されると、このオブジェクトにスキャンが必要かどうかを確認します。必要な場合は、[Dr.Web Scanning Engine](#)に対してスキャンタスクが生成されます。スキャンされたオブジェクトに脅威が含まれている場合、Dr.Web File Checkerはその脅威を検出された脅威レジストリに入れ、駆除（修復、削除、または隔離）します（脅威への対応としてスキャンを開始したクライアントコンポーネントによってこのアクションが指定されている場合）。スキャンは、製品のさまざまなコンポーネント（[SpIDer Guard for SMB](#)モニターなど）によって開始できます。

スキャン中、ファイルチェックコンポーネントでは、スキャン結果と適用されたアクションがあればそれを詳述するレポートを生成してクライアントコンポーネントに送信します。

標準のスキャン方法とは別に、内部使用には以下の特別な方法があります。

- 「*flow*」スキャン方法。このスキャン方法を使用するクライアントコンポーネントは、検出と駆除のパラメータを一度だけ初期化します。これらのパラメータは、このクライアントコンポーネントからのファイルをスキャンするための今後のすべてのリクエストに適用されます。この方法は[SpIDer Guardモニター](#)によって使用されます。
- 「*プロキシ*」スキャン方法。この方法を使用する場合、ファイルチェックコンポーネントは、検出された脅威にアクションを適用せずに、また今後のアクションを許可するために検出された脅威に関するレコードを保存せずに、ファイルをスキャンします。スキャン処理を開始したコンポーネントによって必要なアクションが適用される必要があります。この方法は、[SpIDer Guard for SMB](#)モニター、[Dr.Web ClamD](#)コンポーネントによって使用されます。

Dr.Web Ctlユーティリティのを使用し、[Dr.Web Ctl](#)ユーティリティの`flowscan`コマンド（`drweb-ctl`コマンドで起動）を使用し、「*フロー*」スキャン方法でファイルをスキャンできます。ただし、通常のオンデマンドスキャンでは、`scan`コマンドを使用することを推奨します。

作業中、ファイルスキャンコンポーネントは脅威のレジストリを保持して隔離を管理するだけでなく、ファイルスキャン全体の統計情報も収集し、最後の1分間、5分間、15分間の、1秒間に確認された平均ファイル数を計算します。



コマンドライン引数

Dr.Web Network Checkerを起動するには、コマンドラインに次のコマンドを入力します。

```
$ <opt_dir>/bin/drweb-filecheck [<parameters>]
```

Dr.Web File Checkerは次のパラメータを処理できます。

パラメータ	説明
--help	機能：コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了するように指示します。 短縮形： -h 引数： None
--version	機能：このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了するように指示します。 短縮形： -v 引数： None

例：

```
$ /opt/drweb.com/bin/drweb-filecheck --help
```

このコマンドはDr.Web File Checkerに関する簡単なヘルプ情報を出力します。

スタートアップノート

コンポーネントは、自律モードで（他のコンポーネントから自律的に）OSのラインから直接起動することはできません。Dr.Web for UNIX File Serversの他のコンポーネントからファイルシステムスキャンのリクエストを受信するときに、[Dr.Web ConfigD](#)設定デモンによって自動的に起動されます。コンポーネントの動作を管理し、必要に応じてファイルをスキャンするには、Dr.Web for UNIX File Servers用の[Dr.Web Ctl](#)コマンドラインベースの管理ツールを使用できます（**drweb-ctl**[コマンド](#)を使用して起動されます）。

Dr.Web File Checkerを使用して任意のファイルまたはディレクトリをスキャンするには、Dr.Web Ctlのscanコマンドを使用します。

```
$ drweb-ctl scan <path to file or directory>
```



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ドキュメントを要求するには、次のコマンドを使用します。**man 1 drweb-filecheck**

設定パラメータ

コンポーネントは、Dr.Web for UNIX File Serversの統合された[設定ファイル](#)の[FileCheck]セクションで指定されている設定パラメータを使用します。



このセクションは以下のパラメータを保存します。

LogLevel <i>{logging level}</i>	コンポーネントの ログの詳細レベル パラメータ値が指定されていない場合は、[Root] セクション の DefaultLogLevel パラメータの値が使用されます。 デフォルト値: Notice
Log <i>{log type}</i>	コンポーネントの ロギング方式 。 デフォルト値: Auto
ExePath <i>{path to file}</i>	コンポーネントの実行ファイルへのパス。 デフォルト値: <opt_dir>/bin/drweb-filecheck <ul style="list-style-type: none">• GNU/Linuxの場合: /opt/drweb.com/bin/drweb-filecheck• FreeBSDの場合: /usr/local/libexec/drweb.com/bin/drweb-filecheck
DebugClientIpc <i>{Boolean}</i>	詳細なIPCメッセージをデバッグレベルでログファイルに含めるかどうかを示します (LogLevel = DEBUGの場合など)。 デフォルト値: No
DebugScan <i>{Boolean}</i>	ファイルスキャン中に受信した詳細メッセージをデバッグレベルでログファイルに含めるかどうかを示します (LogLevel = DEBUGの場合など)。 デフォルト値: No
DebugFlowScan <i>{Boolean}</i>	「フロー」メソッドによるファイルスキャンに関する詳細メッセージをデバッグレベルでログファイルに含めるかどうかを示します (LogLevel = DEBUGの場合など)。通常、このスキャン方法は SpIDer Guard モニターによって使用されます。 デフォルト値: No
DebugProxyScan <i>{Boolean}</i>	「プロキシ」メソッドによるファイルスキャンに関する詳細メッセージをデバッグレベルでログファイルに含めるかどうかを示します (LogLevel = DEBUGの場合など)。通常、このスキャン方法は、 SpIDer Guard for SMB モニター、 Dr.Web ClamD コンポーネントによって使用されます。 デフォルト値: No
DebugCache <i>{Boolean}</i>	スキャンのキャッシュされた結果に関する詳細メッセージをデバッグレベルでログファイルに含めるかどうかを示します (LogLevel = DEBUGの場合など)。 デフォルト値: No
MaxCacheSize <i>{size}</i>	スキャンしたファイルに関するデータを保存するためのキャッシュの最大許容サイズ。 0を指定した場合、キャッシュは無効になります。 デフォルト値: 50mb
RescanInterval <i>{time interval}</i>	前回のスキャンの結果がキャッシュ内にある場合にファイルが再スキャンされない期間 (保存された情報が最新のものと見なされる期間)。



	<p>パラメータは0秒 から1分 までの値を指定できます。設定された間隔が1秒 未満の場合は遅延がないため、ファイルは任意のリクエストに応じてスキャンされます。</p> <p>デフォルト値 : 1s</p>
IdleTimeLimit <i>{time interval}</i>	<p>コンポーネントの最大アイドル時間。指定された時間が経過すると、コンポーネントはシャットダウンします。</p> <p>指定する値は、10秒 から30日 までの範囲内でなければなりません。</p> <p>デフォルト値 : 30s</p>



Dr.Web Network Checker

ネットワークチェッカーエージェントDr.Web Network Checkerでは、ネットワーク経由で受信したデータをスキャンエンジンでスキャンできる他、分散ファイルでの脅威のスキャンを実行できます。このコンポーネントを使用すると、ネットワークホストを介してデータ(ファイルの内容など)を送受信できるようDr.Web for UNIX File Serversがインストールされているネットワークホスト間の接続を調整し、スキャンを実行できます。このコンポーネントは、設定されているすべての利用可能なネットワークホストへのスキャンタスクの自動分配を調整します(ネットワークを介して送受信)。このコンポーネントは、スキャンタスクによって生じる負荷をホスト間に分散させます。リモートホストとの接続が設定されていない場合、コンポーネントはすべてのデータをローカルのDr.Web Scanning Engineにのみ送信します。

このコンポーネントは、ネットワーク接続を介して受信したデータのスキャンに常に使用されます。したがって、コンポーネントが見つからないか使用できない場合、スキャン用にネットワーク接続を介してデータを送信するコンポーネントのパフォーマンスは不正確になります(SpIDer Gate、Dr.Web ClamD)。



このコンポーネントは、Dr.Web File Checkerコンポーネントを置き換えることができないため、ローカルファイルシステムにあるファイルの分散スキャンを整理するようには作られていません。ローカルファイルの分散スキャンを整理するには、[Dr.Web MeshD](#)コンポーネントを使用します。

ネットワークを介して転送されるデータのスキャンの負荷が高まると、利用可能なファイル記述子(ファイルディスクリプタ)が枯渇し、スキャンに問題が生じる場合があります。この場合、Dr.Web for UNIX File Serversに利用できるファイル記述子の[制限数を増やす](#)必要があります。

スキャン時には、SSL/TLSを適用することにより、オープンチャネル経由または保護されたチャネル経由のいずれかでデータを共有できます。安全なHTTPS接続を使用するには、ファイルを共有するホストに適切なSSLサーバー証明書とプライベートキーを提供する必要があります。SSLキーと証明書を生成するには、**openssl**ユーティリティを使用できます。**openssl**ユーティリティを使用して証明書とプライベートキーを生成する方法の例については、のセクション[付録E. SSL証明書を生成する](#)を参照してください。

動作原理

このコンポーネントにより、スキャンでローカルファイルシステムのファイルとして表されていないデータを[Dr.Web Scanning Engine](#)エンジン(ローカルまたはリモートホストにある)に送信できます。このデータは、(SpIDer Gate、Dr.Web ClamD)接続を介してスキャンのデータを送信するコンポーネントによって処理されます。これらのコンポーネントは、ローカルホストにある場合でも、Dr.Web Scanning Engineエンジンへのファイル転送に常にDr.Web Network Checkerを使用することに注意してください。そのため、Dr.Web Network Checkerが利用できない場合、これらのコンポーネントは正しく機能しません。

また、Dr.Web Network Checkerは、Dr.Web for UNIX File Serversがインストールされているネットワーク(またはその他のDr.Web for UNIXソリューション10.1以降)の特定のノードセットとDr.Web for UNIX File Serversを接続することで、ローカルファイルシステムでファイルとして表示されない分散されたチェックデータの有無をまとめて確認できます。これにより、このコンポーネントは、検証でデータを交換する一連のネットワークノードであるスキャンクラスタを構築および設定できます(各インスタンスには、Dr.Web Network Checker分散検証エージェントの独自のインスタンスが必要です)。スキャンクラスタに含まれるネットワークの各ノードで、Dr.Web Network Checkerはスキャンデータのタスクの自動分散を実行し、ネットワークを介して、接続が設定されているすべての使用可能なノードに転送します。同時に、リモートノードで使用可能なリソースの量に応じて、データ検証によって発生するノードの負荷分散が実行されます(ロードで使用可能なリソース量の指標として、このノ



ードの核となるDr.Web Scanning Engineのスキャンによって生成される子のスキャンプロセス数が使用されます)。使用されている各ノードでのチェックを待機しているファイルキューの長さも推定されます。

この場合、スキャンクラスタに含まれる任意のネットワークノードは、リモートスキャンにデータを送信するスキャンクライアントの他、検証のために指定されたネットワークノードからデータを受信するスキャンサーバーとして機能します。必要に応じて、ノードがスキャンサーバーまたはスキャンクライアントとしてのみ機能するように分散スキャンエージェントを設定できます。

スキャン用にネットワーク経由で受信したデータは、一時ファイルとしてローカルファイルシステムに保存され、[Dr.Web Scanning Engine](#)エンジンに送信されるか、利用できない場合は、スキャンクラスタの他のノードに送信されます。

[設定](#)にある**InternalOnly**パラメータを使用すると、Dr.Web Network Checkerの動作モードを管理できます。これは、Dr.Web Network CheckerがDr.Web for UNIX File Serversをスキャンクラスタに含めるために使用されるのか、Dr.Web for UNIX File Serversローカルコンポーネントのみの内部目的のために使用されるのかを特定します。



ファイルのチェックにDr.Web Network Checkerを使用する独自のコンポーネント（外部アプリケーション）を作成できます（スキャンクラスタのノードに対するスキャンジョブの分配を含む）。そのために、Dr.Web Network Checkerコンポーネントは**Google Protobuf**テクノロジーに基づくカスタムAPIを提供しています。Dr.Web Network Checker APIの他、Dr.Web Network Checkerを使用するクライアントアプリケーションのサンプルコードが、`drweb-netcheck`パッケージの一部として提供されています。

スキャンクラスタの作成例は、[スキャンクラスタを作成する](#)セクションにあります。



コマンドライン引数

Dr.Web Network Checkerを実行するには、コマンドラインに次のコマンドを入力します。

```
$ <opt_dir>/bin/drweb-netcheck [<parameters>]
```

Dr.Web Network Checkerは次のオプションを処理できます。

パラメータ	説明
--help	機能：コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了するように指示します。 短縮形： -h 引数： None
--version	機能：このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了するように指示します。 短縮形： -v 引数： None

例：

```
$ /opt/drweb.com/bin/drweb-netcheck --help
```

このコマンドはDr.Web Network Checkerに関する簡単なヘルプ情報を出力します。

スタートアップノート

コンポーネントは、自律モードで（他のコンポーネントから自律的に）OSのコマンドラインから直接実行することはできません。必要に応じて、[Dr.Web ConfigD](#)構成デーモンによって自動的に実行されます（通常はOSの起動時）。コンポーネント[設定](#)で、**FixedSocket**パラメータの値が指定されており、**InternalOnly**パラメータがNoに設定されている場合、エージェントは常に実行されており、指定されたUNIXソケットを介してクライアントに使用可能です。ネットワーク経由でスキャンを開始するには、Dr.Web for UNIX File Servers管理用の[Dr.Web Ctl](#)コマンドラインツールを使用できます（[コマンドdrweb-ctl](#)で始まるもの）。リモートホストへの接続が設定されていない場合は、ローカルスキャンが開始されます。

Dr.Web Network Checkerを使用して任意のファイルまたはディレクトリをスキャンするには、Dr.Web Ctlツールのnetscanコマンドを使用します。

```
$ drweb-ctl netscan <path to file or directory>
```



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ドキュメントを要求するには、次のコマンドを使用します。**man 1 drweb-netcheck**



設定パラメータ

コンポーネントは、Dr.Web for UNIX File Serversの統合された[設定ファイル](#)の[NetCheck]セクションで指定されている設定パラメータを使用します。

セクションには以下のパラメータが含まれています。

LogLevel <i>{logging level}</i>	コンポーネントの ログの詳細レベル パラメータ値が指定されていない場合は、[Root] セクション のDefaultLogLevelパラメータの値が使用されます。 デフォルト値: Notice
Log <i>{log type}</i>	コンポーネントの ロギング方式 。 デフォルト値: Auto
ExePath <i>{path to file}</i>	コンポーネントの実行ファイルへのパス。 デフォルト値: <opt_dir>/bin/drweb-netcheck <ul style="list-style-type: none">• GNU/Linuxの場合: /opt/drweb.com/bin/drweb-netcheck• FreeBSDの場合: /usr/local/libexec/drweb.com/bin/drweb-netcheck
FixedSocket <i>{path to file / address}</i>	固定されたDr.Web Network Checkerエージェントインスタンスのソケット。 このパラメータが指定されている場合、 Dr.Web ConfigD 設定デモンは、このソケットを介してクライアントが使用可能な分散スキャンエージェントの実行中のコンポーネントのコピーが常に存在することを確認します。 使用可能な値: <ul style="list-style-type: none">• <path to file>は、ローカルのUNIXソケットへのパスです。• <address>は、ペア <IP address>: <port>で示されるネットワークソケットです。 デフォルト値: (未設定)
InternalOnly <i>{Boolean}</i>	コンポーネントの動作モードの管理。 値がYesに設定されている場合、LoadBalance*設定やFixedSocketパラメータの値に関係なく、コンポーネントはDr.Web for UNIX File Serversコンポーネントの内部目的にのみ使用され、スキャンクラスタへのDr.Web for UNIX File Serversの組み込みや、外部(Dr.Web for UNIX File Serversに対して)クライアントアプリケーションの処理には使用されません。 デフォルト値: No
RunAsUser	このパラメータは、コンポーネントを実行するユーザー名を決定します。ユーザー名は、ユーザーのUIDまたはユーザーのログインとして指



<code>{UID / user name}</code>	<p>定できます。ユーザー名が数字で構成されている場合（UIDに似ている場合）は、「name:」というプレフィックスを付けて指定します。次に例を示します。RunAsUser = name:123456。</p> <p>ユーザー名が指定されていない場合、コンポーネント操作は開始後にエラーが発生して終了します。</p> <p>デフォルト値: drweb</p>
IdleTimeLimit <code>{time interval}</code>	<p>コンポーネントがアイドル状態を維持できる最大時間。指定された値を超えると、コンポーネントはシャットダウンします。</p> <p>最小値 - 10s。</p> <p>LoadBalanceAllowFromパラメータまたはFixedSocketパラメータが設定されている場合、この設定は無視されます（時間間隔が経過しても、コンポーネントが動作を終了しません）。</p> <p>デフォルト値: 30s</p>
LoadBalanceUseSsl <code>{Boolean}</code>	<p>安全なSSL/TLS接続を他のホストへの接続に使用するかどうかを決定するインジケータ。</p> <p>使用可能な値:</p> <ul style="list-style-type: none">• Yes - SSL/TLSを使用するように指示します。• No - SSL/TLSを使用しないように指示します。 <p>このパラメータがYesに設定されている場合、証明書と対応するプライベートキーを、このホストとこのホストがやり取りするホストに対して指定する必要があります（パラメータLoadBalanceSslCertificateおよびLoadBalanceSslKey）。</p> <p>デフォルト値: No</p>
LoadBalanceSslCertificate <code>{path to file}</code>	<p>安全なSSL/TLS接続を介して他のホストと通信するためにDr.Web Network Checkerによって使用されるSSL証明書へのパス。</p> <p>証明書ファイルとプライベートキーファイル（後述のパラメータで指定されます）は、一致するペアを形成する必要があります。</p> <p>デフォルト値: (未設定)</p>
LoadBalanceSslKey <code>{path to file}</code>	<p>安全なSSL/TLS接続を介して他のホストと通信するためにDr.Web Network Checkerによって使用されるプライベートキーへのパス。</p> <p>証明書ファイルとプライベートキーファイル（上のパラメータで指定されます）は、一致するペアを形成する必要があります。</p> <p>デフォルト値: (未設定)</p>
LoadBalanceSslCa <code>{path}</code>	<p>信頼済みのルート証明書のリストを含むディレクトリまたはファイルへのパス。これらの証明書には、SSL/TLSプロトコルを介してデータを交換するときにスキャンクラス内のエージェントが使用する、証明書の信頼性を証明する証明書が必要です。</p> <p>パラメータ値が空の場合、このホストで作業しているDr.Web Network Checkerはやり取りをするエージェントの証明書を認証しま</p>



	<p>せん。ただし、設定によっては、ホスト上で動作しているエージェントが使用する証明書をこれらのエージェントが認証できます。</p> <p>デフォルト値：(未設定)</p>
LoadBalanceSslCrl <i>{path}</i>	<p>失効した証明書のシステムリストを含むディレクトリまたはファイルへのパス。</p> <p>パラメータ値が指定されていない場合、このホストで実行されているDr.Web Network Checkerは、やり取りするエージェントの証明書の有効性をチェックしませんが、設定によっては、このホストで実行されているエージェントが使用する証明書の有効性をチェックする場合があります。</p> <p>デフォルト値：(未設定)</p>
LoadBalanceServerSocket <i>{address}</i>	<p>リモートホストからスキャン用に送信されたファイルを受信するためにDr.Web Network Checkerがこのホスト上で待機しているネットワークソケット(IPアドレスとポート)(スキャンサーバーとして動作できる場合)。</p> <p>デフォルト値：(未設定)</p>
LoadBalanceAllowFrom <i>{IP address}</i>	<p>Dr.Web Network Checkerがスキャン用のファイルを受信できるリモートネットワークホストのIPアドレス(スキャンサーバーとして)。</p> <p>リストをパラメータ値として指定できます。リストの値は、コンマ(引用符内の各値)で区切る必要があります。パラメータはセクションで複数回指定できます(この場合、そのすべての値が1つのリストにまとめられます)。</p> <p>例：ホストアドレス192.168.0.1と10.20.30.45のリストに追加します。</p> <p>1. 設定ファイルに値を追加します。</p> <ul style="list-style-type: none">1つの文字列に2つの値 <pre>[NetCheck] LoadBalanceAllowFrom = "192.168.0.1", "10.20.30.45"</pre> <ul style="list-style-type: none">2つの文字列(文字列ごとに1つの値) <pre>[NetCheck] LoadBalanceAllowFrom = 192.168.0.1 LoadBalanceAllowFrom = 10.20.30.45</pre> <p>2. コマンドdrweb-ctl cfsetを使用して値を追加します。</p> <pre># drweb-ctl cfset NetCheck.LoadBalanceAllowFrom -a 192.168.0.1 # drweb-ctl cfset NetCheck.LoadBalanceAllowFrom -a 10.20.30.45</pre>



	<p>このパラメータが空の場合、削除されたファイルをスキャンのために受信することはできません（ホストはスキャンサーバーとして動作しません）。</p> <p>デフォルト値：（未設定）</p>
LoadBalanceSourceAddress <i>{IP address}</i>	<p>リモートスキャン用にファイルを転送するためにホスト上のDr.Web Network Checkerによって使用されるネットワークインターフェースのIPアドレス（ホストがスキャンサーバーとして動作し、複数のネットワークインターフェースを持つ場合）。</p> <p>空の値を指定すると、OSカーネルによって自動的に選択されたネットワークインターフェースが使用されます。</p> <p>デフォルト値：（未設定）</p>
LoadBalanceTo <i>{address}</i>	<p>ホスト上のDr.Web Network Checkerが（ネットワークスキャンクライアントとして）リモートスキャン用のファイルを送信できるリモートホストのソケット（IPアドレスまたはポート）。</p> <p>リストをパラメータ値として指定できます。リストの値は、コンマ（引用符内の各値）で区切る必要があります。パラメータはセクションで複数回指定できます（この場合、そのすべての値が1つのリストにまとめられます）。</p> <p>例：ソケット192.168.0.1:1234および10.20.30.45:5678をリストに追加します。</p> <p>1. 設定ファイルに値を追加します。</p> <ul style="list-style-type: none">1つの文字列に2つの値 <pre>[NetCheck] LoadBalanceTo = "192.168.0.1:1234", "10.20.30.45:5678"</pre> <ul style="list-style-type: none">2つの文字列（文字列ごとに1つの値） <pre>[NetCheck] LoadBalanceTo = 192.168.0.1:1234 LoadBalanceTo = 10.20.30.45:5678</pre> <p>2. コマンドdrweb-ctl cfsetを使用して値を追加します。</p> <pre># drweb-ctl cfset NetCheck.LoadBalanceTo -a 192.168.0.1:1234 # drweb-ctl cfset NetCheck.LoadBalanceTo -a 10.20.30.45:5678</pre> <p>パラメータ値が空の場合、ローカルファイルをリモートスキャン用に転送できません（ホストはネットワークスキャンクライアントとして動作しません）。</p> <p>デフォルト値：（未設定）</p>
LoadBalanceStatusInterval	<p>ワークロードに関する情報を含む次のメッセージをすべてのスキャンクライアントに送信する際にホストによって考慮されるタイムインターバ</p>



<code>{time interval}</code>	ル (<code>LoadBalanceAllowFrom</code> パラメータで指定)。 デフォルト値: 1s
<code>SpoolDir</code> <code>{path to directory}</code>	スキャン用にネットワーク経由で送信され、Dr.Web Network Checkerによって受信されたファイルを保存するために使用されるローカルファイルシステムディレクトリ。 デフォルト値: /tmp/netcheck
<code>LocalScanPreference</code> <code>{fractional number}</code>	ファイル (ローカルファイルまたはネットワーク経由で受信したファイル) をスキャンするスキャンサーバーが選択されたときに考慮される、このホストの相対的な重み (プライオリティ)。ローカルステーションの相対的な重みが、スキャンサーバーとして利用可能なすべてのホストの重みよりも大きい場合、ファイルはローカルでスキャンされます。 最小値 - 1。 デフォルト値: 1

スキャンクラスタを作成する

このセクションの内容:

- [注意事項](#)
- [スキャンングクラスタの作成例](#)
- [クラスタノードを設定する](#)
- [クラスタの動作を確認する](#)

注意事項

ファイルや他のオブジェクトのスキャン中に分散チェックを実行できるスキャンクラスタを作成するには、各ノードに Dr.Web Network Checkerコンポーネントがインストールされた一連のネットワークノードが必要です。クラスタノードにスキャン対象のデータの送受信以外の機能を持たせるには、ノードにスキャンエンジン Dr.Web Scanning Engine もインストールする必要があります。そのため、スキャンクラスタのノードを作成するには、次のコンポーネントの最小セット (最低限のもの) をサーバーにインストールする必要があります (ここにリストされているコンポーネントの機能を保証するために自動的にインストールされる Dr.Web for UNIX File Servers の他のコンポーネントは、スキップされます)。

1. Dr.Web Network Checker (`drweb-netcheck` パッケージ) は、ノード間のネットワークを提供するコンポーネントです。
2. [Dr.Web Scanning Engine](#) (`drweb-se` パッケージ) は、ネットワーク経由で受信したデータをスキャンするために必要なスキャンエンジンです。場合によっては、このコンポーネントが存在しません。その場合、ノードは他のスキャンクラスタノードに対してチェック対象のデータの送信のみを行います。

ピアツーピアネットワークのスキャンングクラスタを構成するノード、つまり各ノードは、このノードの Dr.Web Network Checkerコンポーネントで定義されている [設定](#) に応じて、スキャンクライアント (他のノードにスキャン用にデータを送信) またはスキャンサーバー (他のノードからスキャン用にデータを受信) として機能できます。適切に設定すれば、クラスタノードは同時にスキャンクライアントとスキャンサーバーの両方として機能します。

スキャンングクラスタ設定に関連する Dr.Web Network Checker パラメータは、`LoadBalance` で始まる名前を持ちます。

スキャンングラスタの作成例

下の図に表示されているスキャンングラスタの構成例を確認してください。

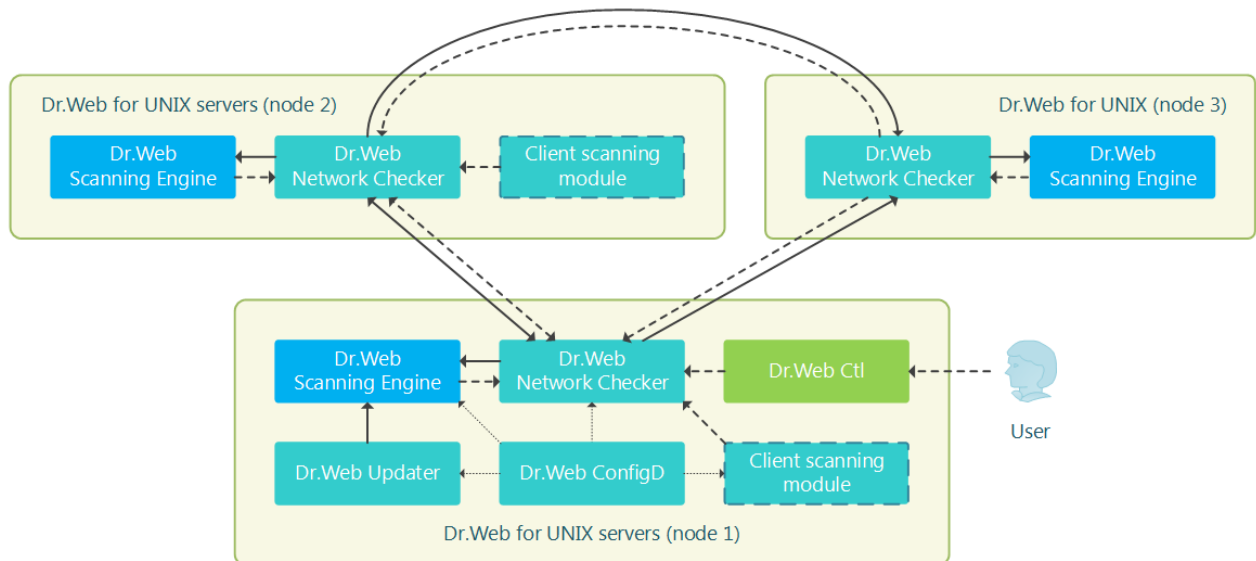


図12. スキャンングラスタの構造

ここでは、クラスタは3つのノード（図ではノード1、ノード2、ノード3として表示）で構成されると想定します。この場合、ノード1とノード2は、UNIXサーバー用のDr.Webの上位製品がインストールされているサーバーです（Dr.Web for UNIXファイルサーバーまたはDr.Web for UNIXインターネットゲートウェイなど。製品タイプは不問）。ノード3は、ノード1とノード2から転送されたファイルのスキャンをサポートするためにのみ使用されます。したがって、必要最小限のコンポーネントセット（Dr.Web Network CheckerおよびDr.Web Scanning Engine）のみがインストールされます。ノードの操作性を確保するために自動的にインストールされる他のコンポーネント（Dr.Web ConfigDなど）は図に記載されていません。ノード1と2は、相互間でサーバーおよびスキャンの両方のクライアントとして機能し（スキャンに関連する負荷の相互分散を実行）、ノード3はサーバーとしてのみ機能し、ノード1と2からタスクを受信します。

これらのコンポーネントは、ローカルにインストールされたスキャンエンジンDr.Web Scanning Engineとクラスタパートナーノードの間で分散され、負荷分散に応じてスキャンサーバーとして機能します。



ローカルファイルシステムでファイルとして表されていないデータをスキャンするコンポーネントのみが、検証のクライアントモジュールとして機能することに注意してください。これは、SpIDer GuardファイルシステムモニターおよびDr.Web File Checkerコンポーネントによるファイルの分散スキャンに使用できるスキャンクラスタを指します。

クラスタノードを設定する

指定したクラスタ構成をカスタマイズするには、すべてのクラスタノードでDr.Web Network Checker設定を変更する必要があります。以下の設定はすべて、.iniファイルで指定されます（設定ファイルの[フォーマットの説明](#)を参照）。



ノード1

```
[NetCheck]
InternalOnly=No
LoadBalanceUseSsl = No
LoadBalanceServerSocket = <Node 1 IP address>: <Node 1 port>
LoadBalanceAllowFrom = <Node 2 IP address>
LoadBalanceSourceAddress = <Node 1 IP address>
LoadBalanceTo = <Node 2 IP address>: <Node 2 port>
LoadBalanceTo = <Node 3 IP address>: <Node 3 port>
```

ノード2

```
[NetCheck]
InternalOnly=No
LoadBalanceUseSsl = No
LoadBalanceServerSocket = <Node 2 IP address>: <Node 2 port>
LoadBalanceAllowFrom = <Node 1 IP address>
LoadBalanceSourceAddress = <Node 2 IP address>
LoadBalanceTo = <Node 1 IP address>: <Node 1 port>
LoadBalanceTo = <Node 3 IP address>: <Node 3 port>
```

ノード3

```
[NetCheck]
InternalOnly=No
LoadBalanceUseSsl = No
LoadBalanceServerSocket = <Node 3 IP address>: <Node 3 port>
LoadBalanceAllowFrom = <Node 1 IP address>
LoadBalanceAllowFrom = <Node 2 IP address>
```

注意

- 他の(ここに記載されていない)Dr.Web Network Checkerパラメータは変更されません。
- IPアドレスとポート番号は実際のものに変更する必要があります。
- この例では、ノード間のデータ交換におけるSSLの使用は無効になっています。SSLを使用する必要がある場合は、**LoadBalanceUseSsl**パラメータに値**Yes**を設定するとともに、パラメータ**LoadBalanceSslCertificate**、**LoadBalanceSslKey**、**LoadBalanceSslCa**に必要な値を設定する必要があります。

クラスタの動作を確認する

データディストリビューションモードでのクラスタの動作を確認するには、ノード1とノード2で次のコマンドを使用します。

```
$ drweb-ctl netscan <path to file or directory>
```

指定されたコマンドを実行するときは、指定されたディレクトリのファイルをDr.Web Network Checkerでチェックする必要があります。これにより、カスタマイズされたクラスタノードにチェックが分散されます。スキャン前に各ノード



のネットワークチェックの統計を表示するには、次のコマンドを使用してDr.Web Network Checkerの統計の表示を実行します（統計の表示を中断するにはCTRL+Cを押します）。

```
$ drweb-ctl stat -n
```




Dr.Web Scanning Engine

スキャンエンジンDr.Web Scanning Engineではディスクデバイスのファイルやブートレコード (*MBR* - マスターブートレコード、*VBR* - ボリュームブートレコード) 内のウイルスやその他の悪意のあるオブジェクトを検索できます。コンポーネントによってスキャンエンジンDr.Web Virus-Finding Engineがメモリに読み込まれて起動される他、エンジンによる脅威の検出に使用するDr.Webウイルスデータベースが読み込まれます。

スキャンエンジンは、他のDr.Web for UNIX File Serversコンポーネント (これらはDr.Web File CheckerとDr.Web Network Checker、部分的にはDr.Web MeshD) からスキャンリクエストを受信するサービスとして、デーモンモードで動作します。*Dr.Web Scanning Engine*と*Dr.Web Virus-Finding Engine*がないか使用できない場合、このノードではアンチウイルススキャンは実行されません (*Dr.Web MeshD*コンポーネントを含む*Dr.Web for UNIX File Servers*を除く、このコンポーネントではスキャンエンジンサービスを提供するローカルクラウドノードへの接続が設定されます)。

動作原理

このコンポーネントは、埋め込まれた脅威のDr.Web for UNIX File Serversコンポーネントからファイルシステムオブジェクト (ファイルおよびブートディスクレコード) をスキャンするリクエストを受信するサービスとして動作します。また、スキャンタスクをキューに入れ、Dr.Web Virus-Finding Engineスキャンエンジンを使用してリクエストされたオブジェクトをスキャンします。脅威が検出され、スキャンタスクによって脅威を修復するように指示があった場合、このアクションをスキャンされたオブジェクトに適用できるのであれば、スキャンエンジンは修復を試みます。

スキャンエンジン、Dr.Web Virus-Finding Engineスキャンエンジン、ウイルスデータベースは1つの単位を構成しており、分離することはできません。スキャンエンジンはウイルスデータベースをダウンロードし、クロスプラットフォームのスキャンエンジンDr.Web Virus-Finding Engineの動作環境を提供します。ウイルスデータベースとスキャンエンジンは、Dr.Web for UNIX File Serversに含まれている[Dr.Web Updater](#)更新コンポーネントによって更新されますが、このコンポーネントはスキャンエンジンの一部ではありません。対応するコマンドがユーザーから送信された場合、更新コンポーネントは[Dr.Web ConfigD](#)設定デーモンによって定期的または強制的に実行されます。さらに、Dr.Web for UNIX File Serversが集中管理モードで動作している場合、ウイルスデータベースとスキャンエンジンの更新は、[Dr.Web ES Agent](#)によって実行されます。Dr.Web ES Agentは集中管理サーバーから更新を受け取ります。

Dr.Web Scanning Engineは、設定デーモンDr.Web ConfigDの管理下でも、自律モードでも動作できます。前者の場合、デーモンはエンジンを実行し、アンチウイルスデータベースが最新であることを確認します。後者の場合、エンジンの起動とウイルスデータベースの更新は、エンジンを使用する外部アプリケーションによって実行されます。ファイルのスキャンを要求するスキャンエンジンにリクエストを発行するDr.Web for UNIX File Serversコンポーネントは、他の外部アプリケーションと同じインターフェースを使用します。



ユーザーは、ファイルチェックにDr.Web Scanning Engineを使用して独自のコンポーネント (外部アプリケーション) を作成できます。このため、Dr.Web Scanning Engineには **Google Protobuf** に基づく特別なAPIが含まれています。Dr.Web Scanning Engine APIガイドとDr.Web Scanning Engineを使用したクライアントアプリケーションの例を入手するには、Doctor Webパートナーケア部門 (<https://partners.drweb.com/>) にお問い合わせください。

受信したタスクは、優先度 (高い、通常、低い) ごとのキューに自動的に分配されます。キューの選択は、タスクを作成したコンポーネントによって異なります。たとえば、ファイルシステムモニターによって作成されたタスクは、応答時間がモニターにとって重要であるため、優先順位が高くなります。スキャンエンジンは、スキャン用に受信したすべてのタスクの数やキューの長さなど、操作に関わる統計を計算します。平均負荷率として、スキャンエンジン



は1秒あたりのキューの平均長を使用します。このレートは、直近1分間、直近5分間、直近15分間の平均です。

Dr.Web Virus-Finding Engineスキャンエンジンは、機械語の命令やその他の実行可能コードの属性に基づいて潜在的に危険なオブジェクトを検出するために設計された、シグネチャ解析(シグネチャベースの脅威の検出)やその他のヒューリスティック解析および動作解析方法をサポートします。



ヒューリスティック解析は信頼性の高い結果を保証できず、次のようなエラーが発生する可能性があります。

- **最初のタイプのエラー。**これらのエラーは、安全なオブジェクトが悪意のあるものとして検出された場合に発生します(誤検知)。
- **2番目のタイプのエラー。**これらのエラーは、悪意のあるオブジェクトが安全であると検出されたときに発生します。

したがって、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ものとして扱われます。

疑わしいオブジェクトは隔離に移動することをお勧めします。ウイルスデータベースを更新した後、そのようなファイルはシグネチャ解析を使用してスキャンできます。2番目のタイプのエラーを避けるには、ウイルスデータベースを最新の状態に保ってください。

Dr.Web Virus-Finding Engineスキャンエンジンを使用すると、異なるコンテナ内のファイルや圧縮されたオブジェクトまたはオブジェクト(アーカイブ、メールメッセージなど)の両方をスキャンして修復できます。

コマンドライン引数

スキャンエンジンDr.Web Scanning Engineをコマンドラインから実行するには、次のコマンドを入力します。

```
$ <opt_dir>/bin/drweb-se <socket> [<parameters>]
```

必須の<socket>引数は、クライアントコンポーネントの要求を処理するためにDr.Web Scanning Engineによって使用されるソケットのアドレスを示します。ファイルパス(UNIXソケット)としてのみ設定できます。

Dr.Web Scanning Engineは次のオプションを処理できます。

パラメータ	説明
--help	機能: コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了するように指示します。 短縮形: -h 引数: None
--version	機能: このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了するように指示します。 短縮形: -v 引数: None
追加の起動パラメータ(設定ファイルのパラメータと同じものであり、必要に応じて置き換えます)。	



--EnginePath	<p>機能 : Dr.Web Virus-Finding Engineスキャンエンジンのライブラリへのパスを指定します。</p> <p>短縮形 : なし</p> <p>引数 : <i><path to the file></i> - 使用するライブラリへのフルパス。</p>
--VirusBaseDir	<p>機能 : ウイルスデータベースファイルがあるディレクトリへのパスを指定します。</p> <p>短縮形 : なし</p> <p>引数 : <i><path to the directory></i> - ウイルスデータベースディレクトリへのパス。</p>
--TempDir	<p>機能 : 一時ファイルがあるディレクトリへのパスを指定します。</p> <p>短縮形 : なし</p> <p>引数 : <i><path to the directory></i> - 一時ファイルを含むディレクトリへのフルパス。</p>
--Key	<p>機能 : キーファイルへのパスを指定します。</p> <p>短縮形 : なし</p> <p>引数 : <i><path to the file></i> - 使用するキーファイルへのフルパス。</p>
--MaxForks	<p>機能 : スキャン中にDr.Web Scanning Engineによって起動できる子プロセスの最大許容数を指定します。</p> <p>短縮形 : なし</p> <p>引数 : <i><number></i> - 子プロセスの最大許容数。</p>
--WatchdogInterval	<p>説明 : Dr.Web Scanning Engineが子プロセスが動作可能かどうかをチェックし、応答を停止したプロセスを停止する頻度を指定します。</p> <p>短縮形 : なし</p> <p>引数 : <i><time interval></i> - 子プロセスをチェックする頻度。</p>
--Shelltrace	<p>機能 : シェルトレースをオンにします (Dr.Web Virus-Finding Engineによって実行されたファイルスキャンの詳細情報をログに記録します)。</p> <p>短縮形 : なし</p> <p>引数 : None</p>
--LogLevel	<p>説明 : 操作中にDr.Web Scanning Engineによって実行されるロギングのレベルを設定します。</p> <p>短縮形 : なし</p> <p>引数 : <i><logging level></i>。可能な値は次のとおり。</p> <ul style="list-style-type: none">• DEBUG - 最も詳細なログレベル。すべてのメッセージとデバッグ情報が登録されます。• INFO - すべてのメッセージが登録されます。• NOTICE - すべてのエラーメッセージ、警告、通知が登録されます。• WARNING - すべてのエラーメッセージと警告が登録されます。• ERROR - エラーメッセージのみが登録されます。
--Log	<p>説明 : コンポーネントメッセージのロギングの方法を指定します。</p> <p>短縮形 : なし</p> <p>引数 : <i><log type></i>。可能な値は次のとおり。</p> <ul style="list-style-type: none">• Stderr[:ShowTimestamp] - メッセージは標準エラーストリームの<i>stderr</i>に出力されます。 追加オプションShowTimestampは、すべてのメッセージにタイムスタンプを追加するように指示します。• Syslog[:<facility>] - メッセージはシステムロギングサービスsyslogに送信されます。



追加オプション *<facility>* は、**syslog** のメッセージ登録レベルを指定するために使用します。次の値を使用できます。

- DAEMON - デーモンのメッセージ。
- USER - ユーザープロセスのメッセージ。
- MAIL - メールプログラムのメッセージ。
- LOCAL0 - ローカルプロセス0のメッセージ。

...

- LOCAL7 - ローカルプロセス7のメッセージ。

- *<path>* - すべてのメッセージが登録されているファイルへのパス。

例：

```
--Log /var/opt/drweb.com/log/se.log
--Log Stderr:ShowTimestamp
--Log Syslog:DAEMON
```

例：

```
$ /opt/drweb.com/bin/drweb-se /tmp/drweb.ipc/.se --MaxForks=5
```

このコマンドはDr.Web Scanning Engineスキャンエンジンのインスタンスを起動し、そのインスタンスに対してクライアントコンポーネントとのインタラクション用の `/tmp/drweb.ipc/.se` UNIXソケットを作成し、ファイルのスキャン中に開始する子スキャンプロセスを5つ以下にするように指示します。

スタートアップノート

必要に応じて、Dr.Web Scanning Engineスキャンエンジンの任意の数のインスタンスを起動できます。インスタンスは、(Dr.Web for UNIX File Serversコンポーネントだけでなく) クライアントアプリケーションにスキャンサービスを提供します。その場合、コンポーネントの**設定**で **FixedSocketPath** パラメータの値が指定されていると、スキャンエンジンの1つのインスタンスが **Dr.Web ConfigD** 設定デーモンによって常に実行され、このUNIXソケットを介してクライアントから利用可能になります。コマンドラインから直接起動したスキャンエンジンのインスタンスは、設定デーモンが実行中であっても、設定デーモンへの接続を確立せずに自律モードで動作します。コンポーネントの動作を管理し、必要に応じてファイルをスキャンするには、Dr.Web for UNIX File Serversの **Dr.Web Ctl** コマンドラインベースの管理ツールを使用できます (**drweb-ctl** コマンドを使用して起動されます)。

Dr.Web Scanning Engineを使用して任意のファイルまたはディレクトリをスキャンするには、Dr.Web Ctlツールの `rawscan` コマンドを使用します。

```
$ drweb-ctl rawscan <path to file or directory>
```



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ドキュメントを要求するには、次のコマンドを使用します。 **man 1 drweb-se**

設定パラメータ

コンポーネントは、Dr.Web for UNIX File Serversの統合された**設定ファイル**



このセクションは以下のパラメータを保存します。

LogLevel <i>{logging level}</i>	コンポーネントの ログの詳細レベル パラメータ値が指定されていない場合は、[Root] セクション の DefaultLogLevel パラメータの値が使用されます。 デフォルト値: Notice
Log <i>{log type}</i>	コンポーネントの ロギング方式 。 デフォルト値: Auto
ExePath <i>{path to file}</i>	コンポーネントの実行ファイルへのパス。 デフォルト値: <opt_dir>/bin/drweb-se <ul style="list-style-type: none">• GNU/Linuxの場合: /opt/drweb.com/bin/drweb-se• FreeBSDの場合: /usr/local/libexec/drweb.com/bin/drweb-se
FixedSocketPath <i>{path to file}</i>	Dr.Web Scanning Engineスキャンエンジンの固定インスタンスのUNIXソケットへのパス。 このパラメータが指定されている場合、 Dr.Web ConfigD 設定デーモンは、このソケットを介してクライアントが使用可能なスキャンエンジンのコンポーネントのコピーが常に実行されていることを確認します。 デフォルト値: (未設定)
IdleTimeLimit <i>{time interval}</i>	コンポーネントの最大アイドル時間。指定された時間が経過すると、コンポーネントはシャットダウンします。 最小値 - 10s. FixedSocketPath パラメータが設定されている場合、この設定は無視されません(時間間隔が経過しても、コンポーネントが動作を終了しません)。 デフォルト値: 30s
MaxForks <i>{integer}</i>	同時に実行できる、Dr.Web Scanning Engineによって実行される子プロセスの最大許容数。 Default value: 使用可能なCPUコアの数の2倍が自動的に使用されます。算出された数が4未満の場合は4になります。
BufferedIo <i>{On / Off}</i>	ファイルをスキャンするときは、バッファ付き入出力(I/O)を使用します。 FreeBSDおよびGNU/Linux OS でバッファ付きI/Oを使用すると、低速ディスクでのファイルスキャン速度を上げることができます。 デフォルト値: Off
WatchdogInterval <i>{time interval}</i>	応答を停止したプロセス(「watchdog」)を検出するために、子プロセスが動作可能かどうかをDr.Web Scanning Engineがチェックする頻度です。 デフォルト値: 1.5秒



Dr.Web Updater

更新コンポーネントDr.Web Updaterは、Doctor Web更新サーバーからウイルスデータベースおよびDr.Web Virus-Finding Engineスキャンエンジンの利用可能な更新をすべて受信し、更新をDr.Web for UNIX製品コンポーネントのローカルクラウドと同期 ([Dr.Web MeshD](#)が製品に含まれている場合はそれを経由) させることを目的に設計されています。

Dr.Web for UNIX File Serversが[集中管理モード](#)で動作している場合、更新は集中管理サーバー (Dr.Web Enterprise Serverなど) から受信されます。その場合、すべての更新は[Dr.Web ES Agent](#)経由でサーバーから受信され、Dr.Web Updaterは更新のダウンロードには使用されません (Dr.Web for UNIX製品のローカルクラウドと更新が同期されることはありません)。

動作原理

このコンポーネントは、Doctor Web更新サーバーへの接続を確立して、ウイルスデータベースとDr.Web Virus-Finding Engineスキャンエンジンの更新と、の更新を確認することを目的に設計されています。利用可能な更新ゾーンを構成するサーバーのリストは、特別なファイルに保存されます (ファイルは改変を防ぐために署名されています)。Doctor Web更新サーバーへの接続では、基本認証とダイジェスト認証のみがサポートされています。

Dr.Web for UNIX File Serversが集中管理サーバーに接続されていない場合、またはモバイルモードでサーバーに接続されている場合、Dr.Web UpdaterはDr.Web ConfigD設定デモンによって自動的に起動されます。起動は、[設定](#)で指定された周期で実行されます。適切な[コマンド](#)をユーザーから受け取った場合、コンポーネントは設定デモンによって起動することもできます (スケジュールされていない更新)。

サーバー上で利用可能になった更新は、`<var_dir>/cache`ディレクトリ (**GNU/Linux**の場合は `var/opt/drweb.com/cache`) にダウンロードされ、その後Dr.Web for UNIX File Serversの作業ディレクトリに移されます。

デフォルトでは、更新はすべてDr.Webの全製品に共通の更新ゾーンから実行されます。更新ゾーンに含まれる、デフォルトで使用されるサーバーのリストは、`*Dr1Dir`パラメータで定義されたディレクトリにあるファイルで指定され、更新タイプ別にグループ化されています (ウイルスデータベースおよびスキャンエンジンと、Webリソースカテゴリのデータベース)。これらのファイルは、更新されたコンポーネント (ウイルスデータベース、スキャンエンジン、アンチスパムコンポーネント) によってグループ化されています。ユーザーのリクエストに応じて (更新タイプごとに) 特別な更新ゾーンを作成できます。これが、`*CustomDr1Dir`パラメータで指定されたディレクトリにある、別のファイル (デフォルト名は `custom.drl`) で指定されているサーバーリストです。この場合、更新コンポーネントは、デフォルトゾーンのサーバーを使用せずに、これらのサーバーからのみ更新を受信します。

特別な更新ゾーンを使用しない場合は、コンポーネント設定で該当するパラメータの `*CustomDr1Dir` 値を削除します。



サーバーリストを含むファイルの中身は署名されているため、ファイルを変更することはできません。更新サーバーの特別なリストを作成する必要がある場合は、[テクニカルサポート](#)にお問い合わせください。

コンポーネントは、ユーザーのリクエストに応じて、更新のロールバックに備えて、更新したファイルをバックアップで保存します。バックアップしたファイルの場所と詳細レベルを設定で指定できます。更新をロールバックするには、



Dr.Web Ctl[Dr.Web Ctl](#)コマンドラインからソリューションを管理するためのDr.Web for UNIX File Serversのコマンドラインツールを使用します(**drweb-ctl**コマンドで実行されます)。

Dr.Web for UNIX File ServersがDr.Web for UNIX製品のローカルクラウドに接続されていて、集中管理サーバーに接続されていない場合、Dr.Web Updaterコンポーネントはクラウドホストによって受信された更新の同期にも使用されます。つまり、更新サーバーが受信した更新をクラウドに送信し、クラウドから更新を受信することになるため、Dr.Web更新サーバーの総負荷を軽減できます。このオプションはコンポーネント [設定](#) で有効または無効にできます。

コマンドライン引数

Dr.Web Updaterを実行するには、コマンドラインに次のコマンドを入力します。

```
$ <opt_dir>/bin/drweb-update [<parameters>]
```

Dr.Web Updaterは次のオプションを処理できます。

パラメータ	説明
--help	機能：コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了するように指示します。 短縮形： -h 引数： None
--version	機能：このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了するように指示します。 短縮形： -v 引数： None

例：

```
$ /opt/drweb.com/bin/drweb-update --help
```

このコマンドはDr.Web Updaterに関する簡単なヘルプ情報を出力します。

スタートアップノート

コンポーネントは、自律モードで(他のコンポーネントから自律的に)OSのコマンドラインから直接起動することはできません。必要に応じて、[Dr.Web ConfigD](#)設定デモンによって自動的に起動されます。コンポーネントの動作を管理し、ウイルスデータベースとスキャンエンジンを更新するには、Dr.Web for UNIX File Servers用の[Dr.Web Ctl](#)コマンドラインベースの管理ツールを使用できます(**drweb-ctl**[コマンド](#)を使用して呼び出されます)。



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ドキュメントを要求するには、次のコマンドを使用します。**man 1 drweb-update**



設定パラメータ

コンポーネントは、Dr.Web for UNIX File Serversの統合された[設定ファイル](#)の[Update]セクションで指定されている設定パラメータを使用します。

セクションには以下のパラメータが含まれています。

LogLevel <i>{logging level}</i>	コンポーネントの ログの詳細レベル パラメータ値が指定されていない場合は、[Root] セクション のDefaultLogLevelパラメータの値が使用されます。 デフォルト値: Notice
Log <i>{log type}</i>	コンポーネントの ロギング方式 。 デフォルト値: Auto
ExePath <i>{path to file}</i>	コンポーネントの実行ファイルへのパス。 デフォルト値: <opt_dir>/bin/drweb-update <ul style="list-style-type: none">• GNU/Linuxの場合: /opt/drweb.com/bin/drweb-update• FreeBSDの場合: /usr/local/libexec/drweb.com/bin/drweb-update
RunAsUser <i>{UID / user name}</i>	このパラメータは、コンポーネントを実行するユーザー名を決定します。ユーザー名は、ユーザーのUIDまたはユーザーのログインとして指定できます。ユーザー名が数字で構成されている場合（UIDに似ている場合）は、「name:」というプレフィックスを付けて指定します。次に例を示します。 RunAsUser = name:123456。 ユーザー名が指定されていない場合、コンポーネント操作は開始後にエラーが発生して終了します。 デフォルト値: drweb
UpdateInterval <i>{time interval}</i>	Dr.Web更新サーバーで更新を確認する頻度。これは、（自動または手動で開始した）更新サーバーへの接続が成功してから次に更新の実行を試みるまでの時間間隔です。 デフォルト値: 30m
RetryInterval <i>{time interval}</i>	前回の試行が失敗した場合に、更新サーバーを使用して更新の実行を再試行する頻度。 パラメータには、1mから30mまでの値を指定できます。 デフォルト値: 3m
MaxRetries <i>{integer}</i>	前回の試行が失敗した場合に、更新サーバーを使用して（RetryIntervalで指定された頻度で）更新の実行を繰り返し試みる回数。 値が0に設定されている場合、試行は繰り返されません（次の更新はUpdateIntervalで指定された時間間隔の後に実行されます）。 デフォルト値: 3

**Proxy***{connection string}*

Dr.Web更新サーバーへの接続時にUpdaterコンポーネント(Dr.Web Updater)が使用するプロキシサーバーに接続するためのパラメータを保存します(外部サーバーへの直接接続がネットワークのセキュリティポリシーによって禁止されている場合など)。

パラメータ値が指定されていない場合、プロキシサーバーは使用されません。

使用可能な値:

<connection string>は、プロキシサーバーの接続文字列です。文字列のフォーマット(URL)は以下のとおりです。

[<protocol>: //] [<user>: <password>@] <host>: <port>

各パラメータは次のとおりです。

- <protocol>は、使用されるプロトコルタイプです(現在のバージョンでは、httpのみが使用可能です)。
- <user>は、プロキシサーバーに接続するためのユーザー名です。
- <password>は、プロキシサーバーに接続するためのパスワードです。
- <host>は、プロキシのホストアドレスです(IPアドレスまたはドメイン名、つまりFQDN)。
- <port>は使用するポートです。

URLの <protocol>および <user>: <password>の部分がありません。プロキシサーバーのアドレス <host>: <port>は必須です。

ユーザー名またはパスワードに「@」、「%」、「:」の文字が含まれている場合、これらの文字はそれぞれ「%40」、「%25」、「%3A」の16進コードに変更する必要があります。

例:**1. 設定ファイルでの設定。**

- ポート123を使用したproxyhost.company.orgでホストされているプロキシサーバーへの接続:

Proxy = proxyhost.company.org:123

- ポート3336を使用し、パスワードが「passw」のユーザー「legaluser」としてHTTPプロトコルを経由した10.26.127.0でホストされているプロキシサーバーへの接続:

Proxy = http:// legaluser:passw@10.26.127.0:3336

- ポート3336、ユーザー名「user@company.com」、パスワード「passw%123:」を使用した10.26.127.0でホストされているプロキシサーバーへの接続:

Proxy = user%40company.com:passw%25123%3A@10.26.127.0:3336

2. コマンドdrweb-ctl cfsetを使用して同じ値を設定する場合:

```
# drweb-ctl cfset Update.Proxy  
proxyhost.company.org:123  
# drweb-ctl cfset Update.Proxy  
http://legaluser:passw@10.26.127.0:3336  
# drweb-ctl cfset Update.Proxy user%  
40company.com:passw%25123%3A@10.26.127.0:3336
```



	デフォルト値：(未設定)
ExcludedFiles <i>{file name}</i>	<p>Dr.Web Updaterコンポーネントによって更新されないファイルの名前を定義します。</p> <p>リストをパラメータ値として指定できます。リストの値は、コンマ(引用符内の各値)で区切る必要があります。パラメータはセクションで複数回指定できます(この場合、そのすべての値が1つのリストにまとめられます)。</p> <p>例：以下のファイルをリストに追加します。123.vdbおよび456.dws。</p> <ol style="list-style-type: none">設定ファイルに値を追加します。<ul style="list-style-type: none">1つの文字列に2つの値<pre>[Update] ExcludedFiles = "123.vdb", "456.dws"</pre>2つの文字列(文字列ごとに1つの値)<pre>[Update] ExcludedFiles = 123.vdb ExcludedFiles = 456.dws</pre>コマンド <code>drweb-ctl cfset</code> を使用して値を追加します。<pre># drweb-ctl cfset Update.ExcludedFiles -a 123.vdb # drweb-ctl cfset Update.ExcludedFiles -a 456.dws</pre> <p>デフォルト値：drweb32.lst</p>
NetworkTimeout <i>{time interval}</i>	<p>更新プロセス中にUpdaterコンポーネントのネットワーク関連の動作に課されるタイムアウト時間。</p> <p>このパラメータは、接続が一時的に切断されたときに使用されます。タイムアウトが切れる前に接続が再度確立された場合、中断された更新プロセスが継続されます。</p> <p>75sを超えるタイムアウト値を指定した場合は、TCPタイムアウトによって接続が閉じられるため効力を持ちません。許容される最小値は5sです。</p> <p>デフォルト値：60s</p>
BaseDrlDir <i>{path to directory}</i>	<p>標準的な更新ゾーンの更新サーバーへの接続に使用されるファイルを含むディレクトリへのパスを定義します。更新コンポーネントがウイルスデータベースおよびスキャンエンジンを更新するために使用されます。</p> <p>デフォルト値：<var_dir>/drl/bases</p> <ul style="list-style-type: none">GNU/Linuxの場合：/var/opt/drweb.com/drl/basesFreeBSDの場合：/var/drweb.com/drl/bases
BaseCustomDrlDir <i>{path to directory}</i>	<p>特別な「カスタマイズされた」更新ゾーンへの接続に使用されるファイルを含むディレクトリへのパスを定義します。ウイルスデータベースとスキャンエンジンを更新するために使用されます。</p>



	<p>パラメータで定義されたディレクトリ内に、空でない署名付きサーバーリストファイル(.drlファイル)がある場合、更新はこれらのサーバーからのみ実行され、主要なゾーンサーバー(上記参照)はウイルスデータベースおよびスキャンエンジンの更新には使用されません。</p> <p>デフォルト値: <var_dir>/custom-drl/bases</p> <ul style="list-style-type: none">• GNU/Linuxの場合: /var/opt/drweb.com/custom-drl/bases• FreeBSDの場合: /var/drweb.com/custom-drl/bases
BaseUpdateEnabled <i>{Boolean}</i>	<p>ウイルスデータベースとスキャンエンジンの更新が許可されているかどうかを示すインジケータ。</p> <p>使用可能な値:</p> <ul style="list-style-type: none">• Yes - 更新は許可されており、実行されます。• No - 更新は許可されていないため実行されません。 <p>デフォルト値: Yes</p>
VersionDir <i>{path to directory}</i>	<p>サーバーへの接続に使用されるファイルを含むディレクトリへのパスを定義します。Dr.Web for UNIX File Serversのバージョンの更新に使用されます。</p> <p>デフォルト値: <var_dir>/drl/version</p> <ul style="list-style-type: none">• GNU/Linuxの場合: /var/opt/drweb.com/drl/version• FreeBSDの場合: /var/drweb.com/drl/version
VersionUpdateEnabled <i>{Boolean}</i>	<p>Dr.Web for UNIX File Serversコンポーネントのバージョンの更新が許可されているかどうかを示すインジケータ。</p> <p>使用可能な値:</p> <ul style="list-style-type: none">• Yes - 更新は許可されており、実行されます。• No - 更新は許可されていないため実行されません。 <p>デフォルト値: Yes</p>
DwsCustomDrlPath <i>{path to file}</i>	<p>パラメータは使用されません。</p> <p>デフォルト値: <var_dir>/drl/dws/custom.drl</p> <ul style="list-style-type: none">• For GNU/Linux: /var/opt/drweb.com/drl/dws/custom.drl• FreeBSDの場合: /var/drweb.com/drl/dws/custom.drl
DwsDrlDir <i>{path to directory}</i>	<p>パラメータは使用されません。</p> <p>デフォルト値: <var_dir>/drl/dws</p> <ul style="list-style-type: none">• GNU/Linuxの場合: /var/opt/drweb.com/drl/dws• FreeBSDの場合: /var/drweb.com/drl/dws
DwsCustomDrlDir <i>{path to directory}</i>	<p>パラメータは使用されません。</p> <p>デフォルト値: <var_dir>/custom-drl/dws</p> <ul style="list-style-type: none">• GNU/Linuxの場合: /var/opt/drweb.com/custom-drl/dws• FreeBSDの場合: /var/drweb.com/custom-drl/dws
DwsUpdateEnabled	<p>パラメータは使用されません。</p> <p>デフォルト値: Yes</p>



<i>{Boolean}</i>	
AntispamDrlDir <i>{path to directory}</i>	パラメータは使用されません。 デフォルト値: <code><var_dir>/drl/antispam</code> <ul style="list-style-type: none">• GNU/Linuxの場合: <code>/var/opt/drweb.com/drl/antispam</code>• FreeBSDの場合: <code>/var/drweb.com/drl/antispam</code>
AntispamCustomDrlDir <i>{path to directory}</i>	パラメータは使用されません。 デフォルト値: <code><var_dir>/custom-drl/antispam</code> <ul style="list-style-type: none">• GNU/Linuxの場合: <code>/var/opt/drweb.com/custom-drl/antispam</code>• FreeBSDの場合: <code>/var/drweb.com/custom-drl/antispam</code>
AntispamUpdateEnabled <i>{Boolean}</i>	パラメータは使用されません。 デフォルト値: <code>No</code>
BackupDir <i>{path to directory}</i>	ロールバックに備えて、更新済みファイルの旧バージョンが保存されているディレクトリへのパス。更新するたびに、更新したファイルのみがバックアップされます。 デフォルト値: <code>/tmp/update-backup</code>
MaxBackups <i>{integer}</i>	更新済みファイルの以前のバージョンの最大保存数。この数を超えると、最も古いコピーが次の更新時に削除されます。 パラメータ値がゼロの場合、以前のバージョンのファイルは保存されません。 デフォルト値: <code>0</code>
IdleTimeLimit <i>{time interval}</i>	コンポーネントの最大アイドル時間。指定された時間が経過すると、コンポーネントはシャットダウンします。 最小値 - 10s。 コンポーネントは、スケジュールによる次の更新時または明示的なコマンド drweb-ctl <code>update</code> <code>--local-cloud</code> で起動されます。更新が完了すると、指定された時間間隔の間、待機します。新しいリクエストがない場合 (UseLocalCloud = <code>Yes</code> の場合のクラウドとのインタラクションを含む) は、次の更新を試行するまでシャットダウンします。 デフォルト値: <code>30s</code>
UseLocalCloud <i>{Boolean}</i>	Dr.Web更新サーバーに加えて、 Dr.Web MeshD コンポーネント経由で Dr.Web for UNIX製品のローカルクラウドと連携して、更新を同期します (クラウドに更新を送信し、クラウドから更新を取得します)。 <ul style="list-style-type: none">• <code>No</code> - 更新には Dr.Web更新サーバーのみ使用します。クラウドとの更新の同期は無効ですが、drweb-ctl <code>update</code> <code>--local-cloud</code> コマンドを使用して明示的に実行できます。• <code>Yes</code> - ホスト上の更新をローカルクラウドと同期します (利用可能な更新がある場合はクラウドから更新を取得し、ホスト上の更新のほうが新しい場合はクラウドに更新を送信します)。 デフォルト値: <code>Yes</code>



Dr.Web ES Agent

アンチウイルス集中管理エージェントDr.Web ES Agentは、Dr.Web for UNIX File Serversを[集中管理サーバー](#)（Dr.Web Enterprise Serverなど）に接続するように設計されています。

Dr.Web for UNIX File Serversが集中管理サーバーDr.Web ES Agentに接続されている場合、とライセンス[キーファイル](#)は、集中管理サーバーに保存されているキーファイルに従って同期されます。さらに、Dr.Web ES Agentウイルスイベントに関する統計、実行中のコンポーネントのリストとステータスを集中管理サーバーに送信します。

またDr.Web ES Agentは、更新コンポーネント[Dr.Web Updater](#)を経由せずに、接続されている集中管理サーバーから直接Dr.Web for UNIX File Serversのウイルスデータベースを更新します。

動作原理

Dr.Web ES Agentは、集中管理サーバー（Dr.Web Enterprise Serverなど）への接続を確立します。これにより、ネットワーク管理者はネットワーク内で共通のセキュリティポリシーを実装し、特にすべてのネットワークステーションとサーバーに対して同じスキャン設定と脅威検出への対応を設定できます。さらに、集中管理サーバーは最新のウイルスデータベース、の最新バージョンのリポジトリを保存するため、ネットワークの内部更新サーバーの役割も果たします（この場合、更新はDr.Web ES Agentで実行され、[Dr.Web Updater](#)は使用されません）。

Dr.Web ES Agentを集中管理サーバーに接続する際、エージェントはプログラムコンポーネントとライセンスキーファイルの最新の設定を確実に受信し、管理対象コンポーネントに適用するために[Dr.Web ConfigD](#)設定データに送信されるようにします。さらに、コンポーネントはステーションのファイルシステムオブジェクトをスキャンするタスク（スケジュールされたタスクを含む）も受信します。

Dr.Web ES Agentは、検出された脅威と適用されたアクションに関するサーバー統計を収集して送信します。

Dr.Web ES Agentを集中管理サーバーに接続するには、ホスト（集中管理サーバーでは「ステーション」）のパスワードとID、認証のためにサーバーによって使用されるパブリック暗号化キーファイルが必要です。ステーションIDの代わりに、ステーションが含まれるメインおよび課金プラングループのIDを指定できます。必要なIDとパブリックキーファイルについては、アンチウイルスネットワークの管理者に問い合わせてください。

さらに、このオプションが集中管理サーバーで許可されている場合は、ホストを保護されたサーバー（「ワークステーション」）に「新規端末」として接続できます。この場合、管理者が接続リクエストを確認した後に、集中管理サーバーでは自動的にIDとパスワードを生成し、今後の接続のためにそれをエージェントに送信します。

コマンドライン引数

Dr.Web ES Agentを実行するには、コマンドラインに次のコマンドを入力します。

```
$ <opt_dir>/bin/drweb-esagent [<parameters>]
```

Dr.Web ES Agentは次のオプションを処理できます。

パラメータ	説明
-------	----



<code>--help</code>	<p>機能：コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了するように指示します。</p> <p>短縮形： <code>-h</code></p> <p>引数： None</p>
<code>--version</code>	<p>機能：このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了するように指示します。</p> <p>短縮形： <code>-v</code></p> <p>引数： None</p>

例：

```
$ /opt/drweb.com/bin/drweb-esagent --help
```

このコマンドはDr.Web ES Agentに関する簡単なヘルプ情報を出力します。

スタートアップノート

コンポーネントは、自律モードで（他のコンポーネントから自律的に）OSのコマンドラインから直接起動することはできません。[Dr.Web ConfigD](#)設定デーモンによって自動的に起動します（OSの起動時）。コンポーネントの動作を管理し、Dr.Web for UNIX File Serversを集中管理サーバーに接続するには、Dr.Web for UNIX File Servers用の[Dr.Web Ctl](#)コマンドラインベースの管理ツールを使用できます（これは[drweb-ctl](#)コマンドを使用して呼び出されます）。



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ドキュメントを要求するには、次のコマンドを使用します。**man 1 drweb-esagent**

設定パラメータ

コンポーネントは、Dr.Web for UNIX File Serversの統合された[設定ファイル](#)の[ESAgent]セクションで指定されている設定パラメータを使用します。

セクションには以下のパラメータが含まれています。

LogLevel <i>{logging level}</i>	コンポーネントの ログの詳細レベル パラメータ値が指定されていない場合は、[Root] セクション のDefaultLogLevelパラメータの値が使用されます。 デフォルト値：Notice
Log <i>{log type}</i>	コンポーネントの ロギング方式 。 デフォルト値：Auto
ExePath <i>{path to file}</i>	コンポーネントの実行ファイルへのパス。 デフォルト値：<opt_dir>/bin/drweb-esagent • GNU/Linuxの場合：/opt/drweb.com/bin/drweb-esagent



	<ul style="list-style-type: none">● FreeBSDの場合: /usr/local/libexec/drweb.com/bin/drweb-esagent
DebugIpc <i>{Boolean}</i>	<p>詳細なIPCメッセージがデバッグレベルでログに含まれるかどうかを示します (LogLevel = DEBUGの場合) (Dr.Web ES AgentとDr.Web ConfigD設定デモンのインタラクション)。</p> <p>デフォルト値: No</p>
MobileMode <i>{On / Off / Auto}</i>	<p>集中管理サーバーに接続したときにモバイルモードで動作するDr.Web for UNIX File Serversの機能を決定します。</p> <p>使用可能な値:</p> <ul style="list-style-type: none">● On - 集中管理サーバーで許可される場合はモバイルモードを使用するように指示します (つまり、Dr.Web Updaterを介してDoctor Webの更新サーバーから更新を実行します)。● Off - モバイルモードを使用せずに集中管理モードで動作を継続するように指示します (更新は常に集中管理サーバーから受信されます)。● Auto - 集中管理サーバーで許可される場合はモバイルモードを使用し、どの接続が利用でき、品質が高いかに応じて、Dr.Web Updaterを介したDoctor Webの更新サーバーと集中管理サーバーの両方から更新を実行します。 <p>このパラメータの動作はサーバーの権限に依存することに注意してください。モバイルモードが使用するサーバーで許可されていない場合、このパラメータは無効です。</p> <p>デフォルト値: Auto</p>
Discovery <i>{On / Off}</i>	<p>エージェントが、集中管理サーバーに組み込まれているネットワークインスペクターからのdiscoveryリクエストを受信できるかどうかを示します (discoveryリクエストは、アンチウイルスネットワークの構造と状態を確認するためにインスペクターによって使用されます)。</p> <p>使用可能な値:</p> <ul style="list-style-type: none">● On - エージェントはdiscoveryリクエストを受信して処理できます。● Off - エージェントはdiscoveryリクエストを受信して処理できません。 <p>このパラメータは、集中管理サーバーの設定よりも優先順位が高いことに注意してください。パラメータ値がOffに設定されている場合、このオプションがサーバーで有効になっていてもエージェントはdiscoveryリクエストを受信しません。</p> <p>デフォルト値: On</p>
UpdatePlatform <i>{platform name}</i>	<p>エージェントが集中管理サーバーからスキャンエンジンの更新を受信するように指示します。スキャンエンジンは指定されたプラットフォーム向けに開発されました。プラットフォーム名はプラットフォーム名を含む文字列です。</p> <p>使用可能な値:</p> <ul style="list-style-type: none">● GNU/Linux: unix-linux-32、unix-linux-64、unix-linux-mips● FreeBSD: unix-freebsd-32、unix-freebsd-64● Darwin: unix-darwin-32、unix-darwin-64



パラメータ値は確実に変更が必要な場合のみ変更することを強くお勧めします。

デフォルト値：現在使用されているプラットフォームに依存



Dr.Web HTTPD

Dr.Web HTTPDは、HTTP経由で(たとえばWebブラウザ経由で) Dr.Web for UNIX File Serversとローカルおよびリモートで対話するためのインフラストラクチャを提供します。コンポーネントには、Dr.Web for UNIX File Serversを管理するためのインターフェース(Dr.Web HTTPDのインストールに加えて、Webブラウザ経由で製品を管理するためのWebインターフェースのファイルを含む個別のパッケージもインストールする必要があります)と、**Mozilla Firefox**ブラウザと**Google Chrome**ブラウザの拡張機能であるDr.Web Link Checkerコンポーネント(お使いのブラウザで使用可能な場合には個別にインストールされます)によって使用されるサービスインターフェースの2つがあります。

Dr.WebのWebインターフェースを介してDr.Web for UNIX File Serversを管理だけでなく、Dr.Web HTTPDのコマンドインターフェース(HTTP API)を直接使用し、HTTPSを介してDr.Web for UNIX File Serversのコンポーネントと対話することもできます。この機能により、Dr.Web for UNIX File Serversを管理するための独自のインターフェースを作成できます。

Dr.Web HTTPDが提供するHTTP APIの詳細については、[該当箇所](#)を参照してください。

安全なHTTPS接続を使用するには、Dr.Web HTTPDに適切なSSLサーバー証明書とプライベートキーを提供する必要があります。デフォルトでは、インストール中にDr.Web HTTPDのSSLサーバー証明書とSSLプライベートキーが自動的に生成されますが、必要に応じて独自の証明書とキーを生成することもできます。また、Dr.Web HTTPDによって信頼されている認証局証明書で署名されたユーザーの個人用認証証明書を、Dr.Web HTTPDに接続するときの自動クライアント認証に使用することもできます。

SSLキーと証明書を生成するには、**openssl**ユーティリティを使用できます。**openssl**ユーティリティを使用して証明書とプライベートキーを生成する方法の例については、のセクション[付録E. SSL証明書を生成する](#)を参照してください。

動作原理

Dr.Web HTTPDは、Dr.Web for UNIX File Serversの動作を管理するためのWebサーバーです。Dr.Web HTTPDがあれば、外部Webサーバー(**Apache HTTP Server**や**Nginx**など)や**Webmin**などの管理サービスを使用せずに済みます。さらに、コンポーネントは、同じホスト上にあるそのようなサーバーやサービスと同時に機能することができ、それらの動作を妨げることはありません。

Dr.Web HTTPDサーバーは、HTTPおよびHTTPSプロトコルを介して設定で指定されたソケットで受信したリクエストを処理します。このため、このサーバーは、Webサーバーと同じホスト上で動作しているときに、それらのサーバーと競合することはありません。セキュアHTTPSプロトコルはDr.Web for UNIX File Serversの管理に使用され、HTTPプロトコルはDr.Web Link Checkerブラウザ拡張リクエスト処理(ブラウザに個別にインストールされます)に使用されます。



Dr.Web管理WebインターフェースとDr.Web Link Checkerプラグインをインストールすることは、Dr.Web for UNIX File Serversを正しく機能させるための必須事項ではありません。これらはない場合もあります。対応するブロックが破線で囲まれているのはこのためです。

Dr.Web HTTPDコンポーネントは、Dr.Web for UNIX File Servers [Dr.Web ConfigD](#)設定デーモン、ファイルスキャン用の[Dr.Web File Checker](#)コンポーネント、およびその他のコンポーネントにコマンドを送信します。これらのコマンドは、提供されるHTTP APIを介して受信されたコマンド(管理Webインターフェース経由で作成されたコマンドやDr.Web Link Checkerブラウザプラグインからのリクエストとして作成されたコマンドを含む)に基づいています。



Dr.Web HTTPDを使用するDr.Web for UNIX File Serversの管理WebインターフェースがDr.Web for UNIX File Serversに含まれている場合は、[セクション](#)にその説明が記載されています。

Dr.Web管理WebインターフェースがDr.Web for UNIX File Serversに含まれていない場合は、Dr.Web HTTPDによるHTTP APIを対話に使用する任意の外部管理インターフェースを接続できます（[セクションHTTP APIの説明](#)で説明しています）。

コマンドライン引数

Dr.Web HTTPDを実行するには、コマンドラインに次のコマンドを入力します。

```
$ <opt_dir>/bin/drweb-httpd [<options>]
```

Dr.Web HTTPDは次のオプションを処理できます。

パラメータ	説明
--help	機能：コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了するように指示します。 短縮形： -h 引数： None
--version	機能：このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了するように指示します。 短縮形： -v 引数： None

例：

```
$ /opt/drweb.com/bin/drweb-httpd --help
```

このコマンドはDr.Web HTTPDに関する簡単なヘルプ情報を出力します。

スタートアップノート

コンポーネントは、自律モードで（他のコンポーネントから自律的に）OSのコマンドラインから直接起動することはできません。必要に応じて[Dr.Web ConfigD](#)構成デーモンによって自動的に起動されます（通常はOSの起動時）。コンポーネントが実行されていてWebインターフェースがインストールされている場合は、標準のWebブラウザを使用して、Webインターフェースが提供されているアドレスにHTTPS経由でアクセスするだけで、Dr.Web for UNIX File Serversのコンポーネントを管理できます。コンポーネントの動作を管理するには、Dr.Web for UNIX File Servers用の[Dr.Web Ctl](#)コマンドラインベースの管理ツールを使用できます（これは[drweb-ctl](#)コマンドを使用して呼び出されます）。



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ドキュメントを要求するには、次のコマンドを使用します。**man 1 drweb-httpd**



設定パラメータ

コンポーネントは、Dr.Web for UNIX File Serversの統合された[設定ファイル](#)の[HTTPD]セクションで指定されている設定パラメータを使用します。

セクションには以下のパラメータが含まれています。

LogLevel <i>{logging level}</i>	コンポーネントの ログの詳細レベル パラメータ値が指定されていない場合は、[Root] セクション のDefaultLogLevelパラメータの値が使用されます。 デフォルト値: Notice
Log <i>{log type}</i>	コンポーネントの ロギング方式 。 デフォルト値: Auto
ExePath <i>{path to file}</i>	コンポーネントの実行ファイルへのパス。 デフォルト値: <opt_dir>/bin/drweb-httpd <ul style="list-style-type: none">• GNU/ Linuxの場合: /opt/drweb.com/bin/drweb-httpd• FreeBSDの場合: /usr/local/libexec/drweb.com/bin/drweb-httpd
Start <i>{Boolean}</i>	コンポーネントは Dr.Web ConfigD 設定デーモンによって起動される必要があります。 このパラメータにYes値を指定すると、設定デーモンはただちにコンポーネントを開始するように指示されます。また、No値を指定すると、設定デーモンはただちにコンポーネントを終了するように指示されます。 デフォルト値: 製品管理インターフェースがインストールされているかどうかによって異なります。
AdminListen <i>{address, ...}</i>	Dr.Web HTTPDが、管理者権限を持つクライアントからの(HTTP経由での)接続をリッスン(待ち受け)しているネットワークソケット(すべてのネットワークソケットは <IPアドレス>:<ポート>で構成されます)のリスト。これらのソケットは、管理 Webインターフェース (Webインターフェースがインストールされている場合)への接続とHTTP APIへのアクセスの両方に使用されます。 リストの値は、コンマ(引用符内の各値)で区切る必要があります。パラメータはセクションで複数回指定できます(この場合、そのすべての値が1つのリストにまとめられます)。 例: ソケット192.168.0.1:1234および10.20.30.45:5678をリストに追加します。 1. 設定ファイルに値を追加します。 <ul style="list-style-type: none">• 1つの文字列に2つの値 <div><pre>[HTTPD] AdminListen = "192.168.0.1:1234", "10.20.30.45:5678"</pre></div>



	<ul style="list-style-type: none">• 2つの文字列（文字列ごとに1つの値） <div><pre>[HTTPD] AdminListen = 192.168.0.1:1234 AdminListen = 10.20.30.45:5678</pre></div> <p>2. コマンド <code>drweb-ctl cfset</code> を使用して値を追加します。</p> <div><pre># drweb-ctl cfset HTTPD.AdminListen -a 192.168.0.1:1234 # drweb-ctl cfset HTTPD.AdminListen -a 10.20.30.45:5678</pre></div> <p>値が指定されていない場合、HTTP APIとWebインターフェース（インストールされている場合）を使用することはできません。</p> <p>デフォルト値：127.0.0.1:4443</p>
PublicListen {address, ...}	<p>Dr.Web HTTPDが、権限が制限されているクライアント、たとえばブラウザにロードされたWebページに悪意のあるオブジェクトがないかスキャンするDr.Web Link Checkerブラウザプラグイン（このプラグインがインストールされている場合）などからの（HTTP経由での）接続をリッスン（待ち受け）しているネットワークソケット（すべてのネットワークソケットは <IPアドレス>:<ポート>で構成されます）のリスト。</p> <p>リストの値は、コンマ（引用符内の各値）で区切る必要があります。パラメータはセクションで複数回指定できます（この場合、そのすべての値が1つのリストにまとめられます）。</p> <p>例：ソケット192.168.0.1:1234および10.20.30.45:5678をリストに追加します。</p> <p>1. 設定ファイルに値を追加します。</p> <ul style="list-style-type: none">• 1つの文字列に2つの値 <div><pre>[HTTPD] PublicListen = "192.168.0.1:1234", "10.20.30.45:5678"</pre></div> <ul style="list-style-type: none">• 2つの文字列（文字列ごとに1つの値） <div><pre>[HTTPD] PublicListen = 192.168.0.1:1234 PublicListen = 10.20.30.45:5678</pre></div> <p>2. コマンド <code>drweb-ctl cfset</code> を使用して値を追加します。</p> <div><pre># drweb-ctl cfset HTTPD.PublicListen -a 192.168.0.1:1234 # drweb-ctl cfset HTTPD.PublicListen -a 10.20.30.45:5678</pre></div> <p>値が指定されていない場合、Dr.Web Link Checkerブラウザプラグインを使用することはできません。</p>



	<p>これらのアドレス(ソケット)では、HTTP APIのすべてのコマンドにアクセスしたり、管理Webインターフェースにアクセスしたりすることはできません。</p> <p>デフォルト値：(未設定)</p>
AdminSslCertificate <i>{path to file}</i>	<p>Webインターフェースサーバーが管理ソケットへの接続を確立するクライアントとHTTPS経由で通信するために使用するサーバー証明書ファイルへのパス。</p> <p>このファイルは、コンポーネントのインストール中に自動的に生成されます。</p> <p>証明書ファイルとプライベートキーファイル(後述のパラメータで指定されます)は、一致するペアを形成する必要があります。</p> <p>デフォルト値：<etc_dir>/certs/serv.crt</p> <ul style="list-style-type: none">• GNU/Linuxの場合：/etc/opt/drweb.com/certs/serv.crt• FreeBSDの場合：/usr/local/etc/drweb.com/certs/serv.crt
AdminSslKey <i>{path to file}</i>	<p>Webインターフェースサーバーが管理ソケットへの接続を確立するクライアントとHTTPS経由で通信するために使用するプライベートキーファイルへのパス。</p> <p>このファイルは、コンポーネントのインストール中に自動的に生成されます。</p> <p>証明書ファイル(前述のパラメータで指定されます)とプライベートキーファイルは、一致するペアを形成する必要があります。</p> <p>デフォルト値：<etc_dir>/certs/serv.key</p> <ul style="list-style-type: none">• GNU/Linuxの場合：/etc/opt/drweb.com/certs/serv.key• FreeBSDの場合：/usr/local/etc/drweb.com/certs/serv.key
AdminSslCA <i>{path to file}</i>	<p>HTTPS経由で管理ソケットに接続しているクライアントから提供された証明書をチェックするための信頼できるCA証明書として機能する証明書ファイルへのパス。</p> <p>クライアントの証明書がこのパラメータで設定された証明書で署名されている場合、このクライアントは認証のためにログイン/パスワードのペアを入力する必要はありません。また、このパラメータで設定された証明書で署名されているクライアント証明書を使用するクライアントでは、ログイン/パスワードによる認証は禁止されます。</p> <p>この証明書ベースの認証に成功したクライアントは、常にスーパーユーザー(ルート)として扱われます。</p> <p>デフォルト値：(未設定)</p>
WebconsoleRoot <i>{path to directory}</i>	<p>管理Webインターフェースがインストールされている場合にその管理Webインターフェースによって使用されるファイルを格納するディレクトリ(Apache HTTPサーバーのhtdocsディレクトリ相当)へのパス。</p> <p>デフォルト値：<opt_dir>/share/drweb-httpd/webconsole</p> <ul style="list-style-type: none">• GNU/Linuxの場合：/opt/drweb.com/share/drweb-httpd/webconsole



	<ul style="list-style-type: none">• FreeBSDの場合 合: /usr/local/libexec/drweb.com/bin/drweb-httpd/webconsole
LinkcheckerRoot <i>{path to directory}</i>	<p>Dr.Web Link Checker Webブラウザプラグインによって使用されるファイルを格納するディレクトリへのパス。</p> <p>デフォルト値: <opt_dir>/share/drweb-httpd/linkchecker</p> <ul style="list-style-type: none">• GNU/Linuxの場合: /opt/drweb.com/share/drweb-httpd/linkchecker• FreeBSDの場合 合: /usr/local/libexec/drweb.com/share/drweb-httpd/linkchecker
AccessLogPath <i>{path to file}</i>	<p>クライアントからWebインターフェースサーバーへのすべてのHTTP/HTTPSリクエストが登録されるファイルへのパス。</p> <p>指定しない場合、HTTP/HTTPSリクエストはファイルに記録されません。</p> <p>デフォルト値: (未設定)</p>

HTTP APIの説明

このセクションの内容:

- [Dr.Web for UNIX File Serversの管理](#)
- [概要](#)
- [ユーザー認証と承認](#)
- [Dr.Web for UNIX File Serversの管理](#)
- [脅威のリストの管理](#)
- [隔離の管理](#)
- [HTTP APIの使用例](#)。

1.概要

HTTP APIは、HTTPプロトコルを介してDr.Web for UNIX File Serversを制御および管理する手段として提供されます（セキュリティを確保するために、HTTPSプロトコルが使用されます）。

APIは、HTTPプロトコルの標準メソッドであるGETとPOSTを使用します。APIは、HTTPプロトコルのバージョン1.0を使用します。HTTP APIのコマンドのパラメータまたはそのようなコマンドの実行結果を表すデータは、HTTPリクエストの本文でJSONオブジェクトとしてテキスト形式で送信されます（コマンドの説明で特に明記されていない場合）。HTTP POSTリクエストの本文でJSONオブジェクトを送信する場合は、このようなリクエストのヘッダーのContent-Type:フィールドでapplication/jsonをその値として指定する必要があります。

HTTPリクエストに対するHTTPレスポンスのフォーマット

- HTTP APIコマンドを処理した結果、後で個別に説明するいくつかの特別な例を除き、レスポンスでJSONオブジェクト（行われたリクエストに固有のJSONオブジェクトか、このAPI呼び出しの処理中に例外が発生した場合は[Error](#) JSONオブジェクト）が返されます。



- レスポンスとして送信されたJSONオブジェクトにArrayタイプのフィールドがあり、この配列に要素が1つも含まれていない場合、このフィールドはサーバーからのレスポンスから省略されます。
- サーバーレスポンスのContent-Type: ヘッダーフィールドは、個別に説明するいくつかの例を除き application/json に設定されます。
- クライアントがHTTP APIにないコマンドを呼び出した場合、[EC_UNEXPECTED_MESSAGE](#)を値として保持するcodeという名前のフィールドを持つError JSONオブジェクトを含むレスポンスが返されます。
- SCSが使用される場合 ([下記](#)を参照)、レスポンスにはSCS cookieが含まれます。

JSONオブジェクト内の文字列のエンコード

- 文字列は、UTF-8エンコーディング(BOMなし)で送信されます。ASCII表の一部ではない記号は、送信JSON文字列内で\uXXXXのようなシーケンスでエスケープされませんが、UTF-8エンコードで送信されます。
- 受信JSONオブジェクトの文字列には、UTF-8でエンコードされた記号と\uXXXXのようなエスケープシーケンスの両方を含めることができます。

データ転送に関する一般的な制限

- 本文内のJSONオブジェクトを待つリクエスト(POSTメソッドによるリクエスト)では、[RFC 7159](#)の観点から正しいシンボルであれば、どんなシンボルでも許可されます。
- RESTアーキテクチャスタイルの要件に従って情報を送信するGETメソッドによるリクエストの場合は、[RFC 1945](#)に抵触しないシンボルであれば、どんなシンボルでもURIに含めることができます。
- [RFC 1945](#)に抵触しないシンボルは、リクエストの他の場所(ヘッダー、本文)に含めることもできます。

2. ユーザー認証と承認

クライアントがHTTPコマンドにアクセスするには、サーバーによってこのようなアクセスが許可されている必要があります。次の2つの認証／承認方法が用意されています。

1. [RFC 6896](#)に準拠したSCS(Secure Cookie Sessions for HTTP)を使用する。
2. Dr.Web HTTPDが信頼できるCAの証明書と見なす特別な証明書で署名されたクライアントのSSL証明書を[使用する](#)。この場合、クライアントは、認証を受けるためにrootの認証情報を正しく入力したかのように扱われます(X.509クライアント証明書が使用されます)

Secure Cookie Sessionが使用される場合、クライアントがAPIの使用を許可されていることを確認するCookie(以下では単にSCS cookieと呼びます)が従来の方法、つまりHTTPリクエスト／レスポンスのヘッダー(Cookie: はクライアントからサーバーに送信されるCookieを指定し、Set-Cookie: はサーバーからクライアントに送信されるCookieを指定します)で送信されます。クライアントの証明書に基づく認証が使用される場合は、SCS-cookieがクライアントから送信されても無視されます。

Secure Cookie Sessionを使用する場合、クライアントとDr.Web HTTPD間の対話は、クライアントがAPIのloginコマンドを送信し、APIをさらに使用するための認証を受けることから始まる必要があります。この場合、クライアントは認証に成功すると、クライアントが認証されたことを確認するSCS cookieを受け取ります。クライアント証明書に基づく認証が使用される場合は、loginコマンドを送信する必要はありません。また、このコマンドを使用して認証を受けようとすると、認証が拒否されレスポンスでエラー(Error JSONオブジェクト)が返されます。



2.1.ログインとパスワードを指定する(SCS)

認証コマンドのloginおよびlogoutは、SCSによる認証方法が使用される場合にのみ使用されます。そうでない場合は、これら2つのコマンドを呼び出そうとすると、呼び出しが拒否され、エラーが返されます(より正確には、エラーコードを含むErrorオブジェクトが返されます)。

ユーザー認証および承認コマンド:

APIコマンド	説明
login	<p>アクション: 指定されたユーザー名とパスワードに基づいてクライアントを認証し、HTTP APIのコマンドを使用することをクライアントに許可します。認証が成功すると、SCS-cookieが返されます。</p> <p>URI: /api/10.2/login</p> <p>HTTPメソッド: POST</p> <p>入力パラメータ: AuthOptionsオブジェクト</p> <p>正常に実行された結果: 空のオブジェクト、SCS cookie</p>
logout	<p>アクション: 提供されたSCS cookieを取り消します。その後、取り消されたSCS cookieを含むHTTP API呼び出しへのレスポンスとして、「EC_NOT_AUTHORIZED」エラーコードを含むErrorオブジェクトが返されます。</p> <p>URI: /api/10.2/logout</p> <p>HTTPメソッド: GET</p> <p>入力パラメータ: SCS cookie</p> <p>正常に実行された結果: 空のオブジェクト</p>
whoami	<p>アクション: 認証されたユーザーの名前を調べます。</p> <p>URI: /api/10.2/whoami</p> <p>HTTPメソッド: GET</p> <p>入力パラメータ: (SCS cookie)*</p> <p>正常に実行された結果: whoamiオブジェクト、(SCS cookie)</p>

*) SCS cookieは、SCSによる認証が使用される場合にのみ送受信する必要があるため、これ以降は括弧に入れて表記します。

使用中のオブジェクトの説明:

1) AuthOptions - 完全なHTTP APIを使用するために認証および承認される必要があるユーザーのログインデータを含むオブジェクト:

```
{
  "user": string, //User name
```



```
"password": string //User's password
}
```

2) **whoami** - HTTP APIを使用することを許可されたユーザーの名前を含むオブジェクト:

```
{
  "whoami" :
  {
    "user": string //User name
  }
}
```

3) **Error** - 発生したエラーに関する情報を含むオブジェクト:

```
{
  "error" :
  {
    "code" : string, //A string specifying an error code that looks like
    EC_XXX
    * "what": string //Description of the error
  }
}
```



リクエストの処理中にエラーが発生した場合にHTTP APIコマンドへのレスポンスとして返される **Error** JSONオブジェクトには、数値のエラーコードではなく、Dr.Web for UNIX File Serversのコンポーネントによって使用される内部文字列型コードを含む *code* フィールドがあります。このコードは、*EC_XXX* のような文字列です。対応する数値コードを見つけてエラーに関する詳細情報を入手するには、「[エラーの内部カタログ](#)」を参照してください。

2.2. 個人証明書を使用する認証

個人証明書を使用して認証する場合、`login` および `logout` コマンドは使用されません。代わりに、HTTPS 接続を確立するときに個人認証証明書が使用されます。個人証明書は、Dr.Web HTTPD 設定で信頼できるものとして指定された認証局証明書で署名されます。このメカニズムを使用すると、受信したリクエストは *root* ユーザーの代わりに実行されるリクエストと見なされます。

個人証明書を使用する認証の場合:

1. 認証局証明書で署名された個人証明書を作成します。
2. Dr.Web HTTPD [設定](#) (パラメータ `AdminSslCA`) で、個人証明書に署名する認証局証明書へのパスを指定します。
3. Dr.Web HTTPD に接続するたびに、署名付き証明書を使用します。

必要に応じて、の [付録E. SSL証明書を生成する](#) セクションを参照してください。



3.Dr.Web for UNIX File Serversを管理する

設定パラメータの現在の値を取得し、設定を変更するためのAPIコマンド:

APIコマンド	説明
設定を管理するコマンド	
get_lexmap	<p>アクション: 現在の設定 (ここではパラメータの語彙マップと呼ばれます) のパラメータ値を取得します。</p> <p>URI: /api/10.2/get_lexmap</p> <p>HTTPメソッド: GET</p> <p>入力パラメータ: (SCS cookie)</p> <p>正常に実行された結果: LexMapsオブジェクト、(SCS-cookie)</p>
set_lexmap	<p>アクション: 現在の設定の指定されたパラメータを設定または(デフォルトに)リセットします (パラメータの「語彙マップ」として送信されます)。</p> <p>URI: /api/10.2/set_lexmap</p> <p>HTTPメソッド: POST</p> <p>入力パラメータ: (SCS cookie)、LexMapオブジェクト</p> <p>正常に実行された結果: SetOptionResultオブジェクト、(SCS cookie)</p>
コマンドの更新	
start_update	<p>アクション: 更新を起動します。</p> <p>URI: /api/10.2/start_update</p> <p>HTTPメソッド: POST</p> <p>入力パラメータ: (SCS cookie)</p> <p>正常に実行された結果: StartUpdateオブジェクト、(SCS-cookie)</p>
stop_update	<p>アクション: アクティブな更新プロセスを停止します。</p> <p>URI: /api/10.2/stop_update</p> <p>HTTPメソッド: POST</p> <p>入力パラメータ: (SCS cookie)</p> <p>正常に実行された結果: 空のオブジェクト、(SCS cookie)</p>
ライセンス管理コマンド	



APIコマンド	説明
install_license	<p>アクション: 指定されたキーファイルをインストールします。</p> <p>URI: /api/10.2/install_license</p> <p>HTTPメソッド: POST</p> <p>入力パラメータ: (<i>SCS-cookie</i>)、キーファイル本体 (またはキーファイルを含むアーカイブ)</p> <p>正常に実行された結果: 空のオブジェクト、(<i>SCS cookie</i>)</p>
集中管理サーバーに接続するためのコマンド	
esconnect	<p>アクション: 集中管理モードを有効にします。</p> <p>URI: /api/10.2/esconnect</p> <p>HTTPメソッド: POST</p> <p>入力パラメータ: (<i>SCS cookie</i>)、ESConnectionオブジェクト</p> <p>正常に実行された結果: 空のオブジェクト、(<i>SCS cookie</i>)</p>
esdisconnect	<p>アクション: 集中管理モードをオフにします。</p> <p>URI: /api/10.2/esdisconnect</p> <p>HTTPメソッド: POST</p> <p>入力パラメータ: (<i>SCS cookie</i>)</p> <p>正常に実行された結果: 空のオブジェクト、(<i>SCS cookie</i>)</p>

製品のコンポーネントの設定が返され、いわゆる語彙マップ、つまり一連のパラメータと値のペアとして設定されます。[LexMaps](#)オブジェクトには、3つの語彙マップである以下の3つのフィールドが常に含まれます (つまり、3つの[LexMaps](#)オブジェクトが含まれます)。

- *active* - 設定パラメータのアクティブ値、つまり現在有効な値のマップ。
- *hardcoded* - 値が欠落しているか許可されていない場合に設定パラメータに割り当てられるデフォルト値のマップ。
- *master* - クライアントによって設定された設定パラメータの値のマップ。



`get_lexmap`コマンドは、実際にインストールされて実行されているコンポーネントだけでなく、Dr.Web for UNIX File Serversに含めることができるすべてのコンポーネントについて、常に3つすべての設定パラメータ値を返します。

使用されるJSONオブジェクトの説明:

- 1) **LexMaps** - パラメータ値のアクティブ、デフォルト、およびユーザー設定の語彙マップを含むオブジェクト



```
{
  "active":LexMap, //Active (current) values of configuration parameters
  "hardcoded":LexMap, //Default values of configuration parameters
  "master":LexMap //Configuration parameter values set
  //by the user
}
```

これらの各フィールドは、次に[LexOption](#)オブジェクトの配列が格納される[LexMap](#)オブジェクトです。

2) [LexMap](#) - パラメータの語彙マップを含むオブジェクト

```
{
  "option":LexOption[] //Array of configuration options
}
```

3) [LexOption](#) - 単一のパラメータまたは設定のセクション(パラメータのグループ)を含むオブジェクト

```
{
  "key": string, //Name of the option (configuration parameter/section)
  *"value":LexValue, //If this option is a single parameter
  *"map":LexMap //If this option is a section
}
```

[LexOption](#)オブジェクトは、Dr.Web for UNIX File Serversの設定のセクションまたは単一のパラメータを表します。このオブジェクトには、常にセクションの名前または単一のパラメータの名前に対応する`key`フィールドがあります。これに加えて、このオブジェクトが表すもの(単一のパラメータまたはセクション)に応じて、`value`フィールド(単一のパラメータを表す場合)または`map`フィールド(セクションを表す場合)もあります。セクションもまた、[LexMap](#)タイプのオブジェクトです。一方、単一のパラメータの値は、パラメータの値を文字列形式で指定する`item`フィールドを含む[LexValue](#)タイプのオブジェクトです。

4) [LexValue](#) - パラメータに割り当てられた値の配列を含むオブジェクト

```
{
  "item": string[] //Array of parameter values
}
```

`set_lexmap`コマンドは、その入力として[LexMap](#)オブジェクトを受け取ります。これには、値を新しい値に変更するか、デフォルトにリセットするすべてのパラメータを含める必要があります。デフォルト値にリセットするパラメータには、`value`フィールドを含めないでください。ユーザーが`set_lexmap`コマンドで指定した語彙マップに記載されていないパラメータは変更されません。`set_lexmap`コマンドは、その実行の結果として、コマンドで指定されたすべてのパラメータの変更結果を含む[SetOptionResult](#)オブジェクトを返します。

5) [SetOptionResult](#) - `item`フィールドにパラメータの変更結果の配列を含むオブジェクト

```
{
  "item":SetOptionResultItem[] //Array of results
}
```

このオブジェクトには、コマンドで指定されたすべてのパラメータの変更結果を表す[SetOptionResultItem](#)オブジェクトの配列が含まれています。

6) [SetOptionResultItem](#) - あるパラメータの値を変更することに関する情報を含むオブジェクト。

```
{
  "option": string, //Name of the parameter
}
```




```
"result": string, //Result of changing the value (error code)
*"lower_limit": string, //The lowest permitted value
*"upper_limit": string //The highest permitted value
}
```

*option*フィールドには、アクションが適用されたパラメータの名前が含まれており、*result*フィールドには、このパラメータの値を変更しようとした結果が含まれています。このフィールドは、指定された値を割り当てようとしたときに発生したエラーに関する文字列タイプのコードです。新しい値がパラメータに正常に割り当てられた場合、このフィールドにはEC_OKが含まれます。エラーの場合（このフィールドがEC_OKに等しくない場合）、このオブジェクトには、このパラメータの最大許容値と最小許容値を保持する*lower_limit*フィールドと*upper_limit*フィールドをオプションで含めることができます。

7) **StartUpdate**オブジェクトには、開始された更新プロセスに関するデータが含まれています

```
{
  "start_update":
  {
    "attempt_id" : number //Identifier of a launched updating process
  }
}
```

8) **ESConnection**オブジェクトには、開始された更新プロセスに関するデータが含まれています

```
{
  *"server": string,    //<Host address>:<port>
  "public_key": string, //Base64 server key
  *"newbie": boolean,   //False by default
  *"login": string,     //User name
  *"password": string   //Password
}
```

パラメータ*login*と*password*は、*newbie* = *true*の場合にのみ指定されます。

4. オブジェクトのスキャン

オブジェクトをスキャンするためのAPIコマンド:

APIコマンド	説明
ファイルスキャン (Dr.Web Network Checkerコンポーネント呼び出しを使用)	
scan_request	<p>アクション: 必要なパラメータを使用してファイルをスキャンする接続 (<i>endpoint</i>) の順序。</p> <p>URI: /api/10.2/scan_request</p> <p>HTTPメソッド: POST</p> <p>入力パラメータ: (<i>SCS cookie</i>)、ScanOptionsオブジェクト</p> <p>正常に実行された結果: ScanEndpointオブジェクト、(<i>SCS-cookie</i>)</p>



APIコマンド	説明
scan_endpoint	<p>アクション: 作成された <i>endpoint</i> 接続でのデータスキャン(ファイル本体など)の起動。</p> <p>URI: /api/10.2/scan_endpoint/<endpoint></p> <p>HTTPメソッド: POST</p> <p>入力パラメータ: (SCS-cookie)、検証可能なデータ</p> <p>正常に実行された結果: ScanReportオブジェクト、(SCS-cookie)</p>
<i>WebページカテゴリーデータベースのURLの確認</i>	
categorize_address	<p>アクション: サーバーアドレスがWebページカテゴリーデータベースにリストされているかどうかを確認します。</p> <p>URI: /api/10.2/categorize_address</p> <p>HTTPメソッド: POST</p> <p>入力パラメータ: (SCS cookie)、CategorizeAddressオブジェクト</p> <p>正常に実行された結果: CategorizedResourceオブジェクト、(SCS-cookie)</p>
categorize_url	<p>アクション: URLがWebページカテゴリーデータベースにリストされているかどうかを確認します。</p> <p>URI: /api/10.2/categorize_url</p> <p>HTTPメソッド: POST</p> <p>入力パラメータ: (SCS cookie)、CategorizeURLオブジェクト</p> <p>正常に実行された結果: CategorizedResourceオブジェクト、(SCS-cookie)</p>
<i>Dr.Web CloudクラウドのURLとファイルのスキャン</i>	
cloud_check_url	<p>アクション: Dr.Web Cloudで、WebページカテゴリーデータベースにリストされているURLに関するデータを確認します。</p> <p>URI: /api/10.2/cloud_check_url</p> <p>HTTPメソッド: POST</p> <p>入力パラメータ: (SCS cookie)、CheckUrlRequestオブジェクト</p> <p>正常に実行された結果: UrlResultオブジェクト、(SCS-cookie)</p>
cloud_check_file	<p>アクション: Dr.Web Cloudで、ファイルの悪質性に関するデータを確認します。</p> <p>URI: /api/10.2/cloud_check_file</p> <p>HTTPメソッド: POST</p>



APIコマンド	説明
	入力パラメータ: (<i>SCS cookie</i>)、 CheckFileRequest オブジェクト 正常に実行された結果: FileResult オブジェクト、(<i>SCS-cookie</i>)

使用されるJSONオブジェクトの説明:

1) **ScanOptions**は、ファイルスキャン用のエンドポイントを作成するために使用されるパラメータを含むオブジェクトです。

```
{
  "scan_timeout_ms": number, //A time-out to scan one file, in ms
  "cure": boolean, //Apply cure to infected file
  "heuristic_analysis": boolean, //Use heuristic analysis
  "packer_max_level": number, //Max packed object nesting level
  "archive_max_level": number, //Max archive nesting level
  "mail_max_level": number, //Max email object nesting level
  "container_max_level": number, //Max container nesting level
  "max_compression_ratio": number //Max archive compression value
}
```

2) **ScanEndpoint**は、ファイルスキャン用に作成されたエンドポイントに関するデータを含むオブジェクトです。

```
{
  "endpoint": string //Unique identifier of the created endpoint
}
```

オブジェクト本体で返される`endpoint`文字列は、`scan_endpoint`コマンド (URIの一部) でファイルスキャンを開始するために使用されます。

3) **ScanReport**は、脅威が検出されたファイルに関する情報を含むオブジェクト。

```
{
  "scan_endpoint": string, //File system object that contains the threat
  "size": number, //Size (in bytes) of the file that contains the threat
  "virus": VirusInfo[], //List of details about the found
  //threats
  "error": string, //An error message
  "heuristic_analysis": bool //Flag that shows whether heuristic
  //analysis was used
}
```

* `virus`フィールドと`error`フィールドは、スキャン中に脅威が検出されず、エラーが発生しなかった場合には、存在しない可能性があります。`scan_endpoint`を呼び出すため、`scan_endpoint`フィールドでは、Dr.Web Network Checkerコンポーネントによってローカルサーバーファイルシステムに作成され、スキャンに関するデータを含み、`scan_endpoint`リクエストの本文で送信される一時ファイルを必ず指定します。

4) **VirusInfo**は、検出された脅威に関する情報を含むオブジェクトです。

```
{
  "type": string, //Type of the detected threat
  "name": string //Name of the threat
}
```



5) **CategorizeAddress**は、検証されるURLに関するデータを含むオブジェクトです。

```
{
  "address" : string //IP address for verification
}
```

6) **CategorizeURL**は、検証されるURLに関するデータを含むオブジェクトです。

```
{
  "url" : string //URL for verification
}
```

7) **CategorizedResource**は、Webページの検証結果（ページがWebページカテゴリーデータベースにリストされているかどうかなど）を含むオブジェクトです。

```
{
  *"category": string,      //The main category
  "categories": string[], //List of all categories the resource falls
under
  *"legal_url": string      //URL of the copyright owner
}
```

*legal_url*フィールドは、リソースカテゴリーが「UC_OWNERS_NOTICE」の場合にのみ存在します。*category*フィールドは存在しない場合があります。リソースカテゴリーは文字列「UC_XXX」です。

- UC_INFECTION_SOURCE - 脅威のソース。
- UC_NOT_RECOMMENDED - アクセスが推奨されないWebページ。
- UC_ADULT_CONTENT - アダルトコンテンツ。
- UC_VIOLENCE - 暴力。
- UC_WEAPONS - 武器。
- UC_GAMBLING - ギャンブル。
- UC_DRUGS - 薬物。
- UC_OBSCENE_LANGUAGE - 卑猥な表現。
- UC_CHATS - チャット。
- UC_TERRORISM - テロリズム。
- UC_FREE_EMAIL - 無料メールサービス。
- UC_SOCIAL_NETWORKS - ソーシャルネットワーク。
- UC_ONLINE_GAMES - オンラインゲーム。
- UC_ANONYMIZERS - アノニマイザー。
- UC_CRYPTOCURRENCY_MINING_POOL - 仮想通貨マイニングプール。
- UC_JOBS - 求人検索リソース。
- UC_OWNERS_NOTICEは、著作権者からの申し立てによってリストに登録されたWebページ。

8) **CheckUrlRequest**は、Dr.Web Cloudによる検証の対象となるURLに関するデータを含むオブジェクトです。



```
{
  "url": string //URL to be verified
}
```

9) **UrlResult**は、Dr.Web CloudによるURL検証の結果に関するデータを含むオブジェクトです。

```
{
  "result": string,          //Error code EC_XXX
  "categories": string[] //List of all categories the resource falls under
                             (see above)
}
```

リソースが正常に検証されると、エラーコード「EC_OK」が返されます。リソースが既知のどのカテゴリーにも属していない場合、*categories*配列は空になります。

10) **CheckFileRequest**は、Dr.Web Cloudによって検証されるURLに関するデータを含むオブジェクトです。

```
{
  "sha1": string,          //SHA1 checksum of the scanned file, a hexadecimal
                             number
  "path": string,          //Path to a file
  "size": number,          //File size, in bytes
  *"source_url": string //URL of the file source (optional field)
}
```

11) **FileResult**は、Dr.Web CloudによるURL検証の結果に関するデータを含むオブジェクトです。

```
{
  "result": string, //Error code EC_XXX
  *"virus":VirusInfo //Information on a threat
}
```

ファイルが正常に検証されると、エラーコード「EC_OK」が返されます。脅威が検出されない場合、*virus*フィールドはありません。

12) **VirusInfo**は、検出された脅威に関する情報を含むオブジェクトです。

```
{
  "type": string, //Type of the detected threat
  "name": string //Name of the threat
}
```

*type*フィールド(脅威タイプ)は文字列「SE_XXX」です。

- SE_KNOWN_VIRUSは既知のウイルスです。
- SE_VIRUS_MODIFICATIONは既知のマルウェアの亜種です。
- SE_UNKNOWN_VIRUSは未知のウイルス(疑わしいオブジェクト)です。
- SE_ADWAREはアドウェアです。
- SE_DIALERはダイヤラープログラムです。
- SE_JOKEはジョークプログラムです。
- SE_RISKWAREは潜在的に危険なプログラムです。



- SE_HACKTOOLはハッキングツールです。

5. 脅威のリストの管理

スキャン中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のリストを管理できるように、HTTP APIには次のコマンドが用意されています。

APIコマンド	説明
threats	<p>アクション: 検出されたすべての脅威のIDを一覧表示します。</p> <p>URI: /api/10.2/threats/</p> <p>HTTPメソッド: GET</p> <p>入力パラメータ: (SCS cookie)</p> <p>正常に実行された結果: 脅威IDの配列</p>
site_threats	<p>アクション: <site ID>というIDを持つ、Webサイトによって占有されているディレクトリで見つかったすべての脅威の脅威IDのリストを取得します。</p> <p>URI: /api/10.2/threats/ <site ID></p> <p>HTTPメソッド: GET</p> <p>入力パラメータ: (SCS cookie)</p> <p>正常に実行された結果: 脅威IDの配列</p>
threat_info	<p>アクション: 脅威に関する情報を脅威のIDである <threat ID>で取得します。</p> <p>URI: /api/10.2/threat_info/ <threat ID></p> <p>HTTPメソッド: GET</p> <p>入力パラメータ: (SCS cookie)</p> <p>正常に実行された結果: (SCS-cookie)、FileThreatオブジェクト</p>
cure_threat	<p>アクション: 脅威のIDである <threat ID>で指定された脅威の修復を試みます。</p> <p>URI: /api/10.2/cure_threat/ <threat ID></p> <p>HTTPメソッド: POST</p> <p>入力パラメータ: (SCS cookie)</p> <p>正常に実行された結果: (SCS cookie)、空のオブジェクト</p>
delete_threat	<p>アクション: 脅威のIDである <threat ID>で指定された脅威を含むファイルを削除します。</p> <p>URI: /api/10.2/delete_threat/ <threat ID></p>



APIコマンド	説明
	HTTPメソッド : POST 入力パラメータ : (<i>SCS cookie</i>) 正常に実行された結果 : (<i>SCS cookie</i>)、空のオブジェクト
ignore_threat	アクション : 脅威のIDである <i><threat ID></i> で指定された脅威を無視します。 URI : /api/10.2/ignore_threat/ <i><threat ID></i> HTTPメソッド : POST 入力パラメータ : (<i>SCS cookie</i>) 正常に実行された結果 : (<i>SCS cookie</i>)、空のオブジェクト
quarantine_threat	アクション : 脅威のIDである <i><threat ID></i> で指定された脅威を隔離します。 URI : /api/10.2/quarantine_threat/ <i><threat ID></i> HTTPメソッド : POST 入力パラメータ : (<i>SCS cookie</i>) 正常に実行された結果 : (<i>SCS cookie</i>)、空のオブジェクト

検出された脅威のリストを要求するコマンド内のURIの *<site ID>* 部分は、保護されたWebサイトを含むディレクトリへのパスに置き換える必要があります。このようなディレクトリは、SpIDer Guardの設定 (**LinuxSpider.Space. <ID>.Path** パラメータ) でも指定されます。パスは、URLエンコードの規則に従って指定する必要があります。脅威ID *<threat ID>* は、指定されたアプリケーションで見つかった脅威のID (非負の整数) です。threat_info、cure_threat、delete_threat、ignore_threat、quarantine_threat コマンドでは、threats コマンドと site_threats コマンドによって返される配列に含まれている脅威IDのみを使用できます。

アクション履歴を含む脅威に関するすべての情報は、threat_info リクエストを使用して取得できます。情報は **FileThreat** オブジェクトとして返されます。

1) **FileThreat** は、次のデータを含むオブジェクトです。

```
{
  "threat_id": number, //Threat identifier
  "detection_time": UNIXTime, //Time when the threat was detected
  "report": ScanReport, //Report about scanning the file
  "stat": FileStat, //Information about the file
  "origin": string, //Name of the component that detected the threat
  "origin_pid": number, //PID of the component that detected the threat
  "task_id": number, //Identifier of the scanning task
  //in the scan engine
  "history": ActionResult[] //History of actions applied to the threat (an array)
}
```




*report*フィールドには[ScanReport](#)オブジェクトが含まれます。*stat*フィールドには[FileStat](#)オブジェクトが含まれ、*history*フィールドには[ActionResult](#)オブジェクト（ファイルに適用されたアクションの履歴）の配列が含まれます。

2) ScanReport - 脅威が検出されたファイルに関する情報を含むオブジェクト。

```
{
  "object": string, //File system object that contains the threat
  "size": number, //Size (in bytes) of the file that contains the threat
  "virus":VirusInfo[], //List of details about the found
  //threats
  *"error": string, //An error message
  "heuristic_analysis": bool //Flag that shows whether heuristic
  //analysis was used
}
```

*virus*フィールドは、検出されたすべての脅威に関する情報を含む[VirusInfo](#)オブジェクトの配列です。*error*フィールドは、エラーが発生した場合にのみ表示されます。

3) FileStatは、ファイル統計を含むオブジェクトです。

```
{
  "dev": number, //Device containing the file
  "ino": number, //The file inode number
  *"size": number, //Size of the file
  *"uid":User, //User ID of the file's owner
  *"gid":Group, //Group ID of the owning group
  *"mode": number, //The mode of access to the file
  *"mtime":UNIXTime, //Date/time when the file was last modified
  *"ctime":UNIXTime //Date/time when the file was created
  *"rsrc_size": number, //
  *"finder_info": string, //
  *"ext_finder_info": string, //
  *"uchg": string, //
  *"volume_name": string, //Volume name
  *"volume_root": string, //Root (mount point) of the volume
  *"xattr":XAttr[] //Extended information about the file
}
```

*xattr*フィールドには、**XAttr**オブジェクトの配列が含まれています。このオブジェクトには、*name*および*value*の2つの文字列タイプのフィールドがあります。*uid*フィールドと*gid*フィールドにはそれぞれユーザーオブジェクトとグループオブジェクトが含まれており、これらのオブジェクトにはそれぞれファイルの所有者とファイルを所有しているグループに関する情報が含まれています。これらのオブジェクトにはそれぞれ次の2つのフィールドがあります。

- *uid(gid)* - ユーザー（グループ）のID（数値）。
- *username(groupname)* - ユーザー（グループ）の名前（文字列）。

4) ActionResultは、ファイルに適用されたアクションとその結果に関する情報を含むオブジェクトです。

```
{
  "action": string, //The action applied
  "action_time":UNIXTime, //Date/time when the action was applied
  "result": string, //Result of applying the action
  "cure_report":ScanReport //Report about applying the action
}
```



cure_threat、delete_threat、ignore_threat、quarantine_threatコマンドは、正常に実行された場合は空のオブジェクトを返します。脅威に対して要求されたアクションがエラーのために失敗した場合（たとえば、脅威が駆除されなかった場合）、空のオブジェクトの代わりに[Error](#)オブジェクトが返されます。

6. 隔離の管理

隔離されている脅威を管理するため、HTTP APIには次のコマンドが用意されています。

APIコマンド	説明
quarantine	<p>アクション：隔離されたオブジェクトのIDの一覧を表示します。</p> <p>URI: /api/10.2/quarantine/</p> <p>HTTPメソッド: GET</p> <p>入力パラメータ: (SCS cookie)</p> <p>正常に実行された結果: (SCS cookie)、QuarantineIdオブジェクト(隔離内のオブジェクト)の配列</p>
site_quarantine	<p>アクション: <site ID>というIDを持つWebサイトのディレクトリで検出された後に隔離に移動されたすべての脅威について、隔離オブジェクトのIDの一覧を取得します。</p> <p>URI: /api/10.2/quarantine/ <site ID></p> <p>HTTPメソッド: GET</p> <p>入力パラメータ: (SCS cookie)</p> <p>正常に実行された結果: (SCS cookie)、QuarantineIdオブジェクト(隔離内のオブジェクト)の配列</p>
qentry_info	<p>アクション: 隔離オブジェクトのIDである <entry ID>で指定された隔離オブジェクトに関する情報を取得します。</p> <p>URI: /api/10.2/qentry_info/ <entry ID></p> <p>HTTPメソッド: GET</p> <p>入力パラメータ: (SCS cookie)</p> <p>正常に実行された結果: (SCS cookie)、QEntryオブジェクト</p>
cure_qentry	<p>アクション: 隔離オブジェクトのIDである <entry ID>で指定された隔離オブジェクトの修復を試みます。</p> <p>URI: /api/10.2/cure_qentry/ <entry ID></p> <p>HTTPメソッド: POST</p> <p>入力パラメータ: (SCS cookie)</p> <p>正常に実行された結果: (SCS cookie)、空のオブジェクト</p>



APIコマンド	説明
delete_qentry	<p>アクション: 隔離オブジェクトのIDである <entry ID>で指定された隔離オブジェクトを削除します。</p> <p>URI: /api/10.2/delete_qentry/<entry ID></p> <p>HTTPメソッド: POST</p> <p>入力パラメータ: (SCS cookie)</p> <p>正常に実行された結果: (SCS cookie)、空のオブジェクト</p>
restore_qentry	<p>アクション: 隔離オブジェクトのIDである <entry ID>で指定された隔離オブジェクトを元の場所に復元します。</p> <p>URI: /api/10.2/restore_qentry/<entry ID></p> <p>HTTPメソッド: POST</p> <p>入力パラメータ: (SCS cookie)</p> <p>正常に実行された結果: (SCS cookie)、空のオブジェクト</p>

quarantineコマンドとsite_quarantineコマンドは、[QuarantineId](#)型のオブジェクトの配列を返します。各オブジェクトには、隔離オブジェクトのIDが含まれています。IDは、*chunk_id*と*entry_id*の2つの部分で構成されています。

1) [QuarantineId](#)は、隔離オブジェクトの2つの部分からなるIDの両方の部分を含むオブジェクトです。

```
{
  "chunk_id": string,
  "entry_id": string
}
```

これら2つのフィールドが一体となって隔離オブジェクトの一般的なIDを構成します。qentry_info、cure_qentry、delete_qentry、またはrestore_qentryコマンドを使用して隔離オブジェクトにアクションを適用するには、隔離オブジェクトの一般的なIDである<entry ID>を<entry_id>@<chunk_id>の形式で指定する必要があります。qentry_infoコマンドを使用すると、隔離オブジェクトのIDで指定された隔離オブジェクトに関する詳細情報を取得できます。このコマンドは[QEntry](#)タイプのオブジェクトを返します。

2) [QEntry](#) - 隔離オブジェクトに関する情報を含むオブジェクト

```
{
  "entry_id": string, //Parts of the identifier of
  *"chunk_id": string, //this quarantined object
  *"quarantine_dir": string, //Quarantine directory
  "restore_path": string, //path where the quarantined
  //object will be restored
  "creation_time": number, //Date/time of moving to quarantine
  //(in UNIX time)
  "report": ScanReport, //Report about scanning the object
  //(see ScanReport described above)
```



```
"stat":FileStat, //Statistical information about the file
//(see FileStat described above)
*"history":QEntryOperation[], //History of operations performed on the
object
*"who":RemoteUser, //The remote owner of the file (if
//the file was quarantined from a file server
//storage)
*"detection_time": number, //Date/time of detecting the threat
*"origin": string, //Component that detected the threat
}
```

*report*フィールドには[ScanReport](#)オブジェクトが含まれます。*stat*フィールドには[FileStat](#)オブジェクトが含まれ、*history*フィールドには隔離オブジェクトに適用されたアクションの履歴が含まれます。各アクションエントリは、[QEntryOperation](#)オブジェクトによって記述されます。オプションの「who」フィールドには、削除されたユーザーに関する情報が[RemoteUser](#)オブジェクトの形式で含まれます。

3) [QEntryOperation](#)は、隔離オブジェクトに適用された操作に関するデータを含むオブジェクトです

```
{
  "action": string, //Operation performed on the object
  //(see the possible values below)
  "action_time": number, //Date/time when the operation was performed
  (UNIX Time)
  "result": string, //Error when trying to perform the operation (a code
  //EC_XXX)
  *"restore_path": string, //path for restoring the quarantined object
  //(if action = "QENTRY_ACTION_RESTORE")
  *"rescan_report":ScanReport //Report about rescanning (if
  //action = "QENTRY_ACTION_RESCAN")
}
```

*action*フィールドには、以下の値を指定できます。

- [QENTRY_ACTION_DELETE](#)は、隔離オブジェクトの削除を試みます。
- [QENTRY_ACTION_RESTORE](#)は、隔離オブジェクトの復元を試みます。
- [QENTRY_ACTION_RESCAN](#)は、隔離オブジェクトの再スキャンを試みます。
- [QENTRY_ACTION_CURE](#)は、隔離オブジェクトの修復を試みます。

4) [RemoteUser](#)は、ファイルを所有するリモートユーザーに関する情報を含むオブジェクトです（ファイルがファイルサーバストレージから隔離に再配置された場合）。

```
{
  *"ip": string, //IP-address of the user
  *"user": string, //User name
  *"domain": string //Domain of the user
}
```

[cure_gentry](#)、[delete_gentry](#)、[restore_gentry](#)コマンドの実行が成功すると、空のオブジェクトが返されます。隔離オブジェクトに対して要求された操作がエラーで終了した場合（たとえば、ファイルを復元できなかった場合）、空のオブジェクトの代わりに[Error](#)オブジェクトが返されます。



7.HTTP APIの使用例

HTTP APIの動作をテストするには、**curl**ユーティリティを使用します。API呼び出しの一般的なフォーマットは以下のとおりです。

```
$ curl https://<HTTPD.AdminListen>/<HTTP API URI> -k -X <HTTP method name>
[-H 'Content-Type: application/json' --data-binary '@<file of the JSON object>']
[-c <cookie file> [-b <cookie file>]] [> <file of the result>]
```

ここで、**-k**コマンドラインパラメータは、使用されるSSL証明書が有効であるかどうかを**curl**がチェックしないことを許可するために使用され、**-X**パラメータは、使用するHTTPメソッド(GETまたはPOST)を指定するために使用されます。JSONオブジェクトがこのHTTPリクエストの本文で渡される場合は、**-H**パラメータを使用してリクエストのヘッダーセクションにContent-Type: application/jsonヘッダーフィールドを追加できます。また、**--data-binary**パラメータを使用すると、JSONオブジェクト自体をリクエストの本文に追加し、テキストファイルからJSONオブジェクトを取得できます。SCSを使用して認証を受ける場合は、送受信されるSCS cookieを格納するファイルをそれぞれ**-b**パラメータと**-c**パラメータで指定する必要があります。このユーティリティとその引数に関する詳細な説明を表示するには、**curl --help**コマンドと**man curl**コマンドを使用してください。

1. ユーザー名とパスワード(SCS用)を指定して、クライアントを認証および承認する。

JSON形式のAuthOptionsオブジェクトがあらかじめuser.jsonというファイルに書き込まれている必要があります。例:

```
{"user": "<ユーザー名>", "password": "<パスワード>"}
```

```
$ curl https://127.0.0.1:4443/api/10.2/login -k -X POST -H 'Content-Type: application/json' --data-binary '@user.json' -c cookie.file
```

レスポンス:

```
HTTP/1.0 200 OK
Content-Type: application/json
Content-Length:2
Set-
Cookie:DWToken=6QXy4wn_JGov9A1GohWP_kvMK3dN6ccKegjNgKcmHpb_AqSrHg9cNX_yFJ
hxPDgr|MTQ2Mjg3Mzg4NQ==|cWd4Ow==|GywBUVOhU4w2LF_BKT5frg==|
kR_rip5nrpxWjJ2dfZ7Xfmvi3rE=; Secure; HttpOnly; Max-Age:900; Path=/
Pragma: no-cache

{}
```

Set-Cookieヘッダーフィールドには、HTTP APIに次のコマンドを送信するために使用する必要があるSCS-cookieが含まれています。認証と承認が成功した場合、レスポンスの本文には空のオブジェクトが含まれています。ユーザーが承認されなかった場合は、次のようなErrorオブジェクトが返されます。

```
HTTP/1.0 403 Forbidden
Content-Type: application/json
Content-Length:35
Pragma: no-cache

{"error":{"code":"EC_AUTH_FAILED"}}
```

2. Webサイトのディレクトリで検出された脅威のリストを取得する(ここではサイトのルートディレクトリとして/sites/site1ディレクトリが指定されています):



```
$ curl https://127.0.0.1:4443/api/10.2/threats/%2Fsites%2Fsite1 -k -X GET  
-c cookie.file -b cookie.file
```

レスポンス:

```
HTTP/1.0 200 OK  
Content-Type: application/json  
Content-Length:80  
Set-Cookie:DWToken=<...>; Secure; HttpOnly; Max-Age:900; Path=/  
Pragma: no-cache  
  
["1", "2", "3", "4"]
```

3. IDが1である脅威に関する情報を取得する:

```
$ curl https://127.0.0.1:4443/api/10.2/threat_info/1 -k -X GET -c  
cookie.file -b cookie.file
```

レスポンス:

```
HTTP/1.0 200 OK  
Content-Type: application/json  
Content-Length:574  
Set-Cookie:DWToken=<...>;  
Secure; HttpOnly; Max-Age:900; Path=/  
Pragma: no-cache  
  
{  
  "threat_id":1,"detection_time":1462881660,  
  "report":{"object":"/sites/site1/eicar.com.txt","size":68,"packer":[],  
    "virus":[{"type":"SE_KNOWN_VIRUS","name":"EICAR Test File (NOT a  
    Virus!)"}]},  
  "heuristic_analysis":true,"core_fingerprint":"0D2DD5A869DAB7AE354153A4D5F  
70F45",  
  "item":[],"log":[],"user_time":0,"system_time":0,"stat":  
    {"dev":2049,"ino":898,  
      "size":68,"uid":{"uid":1000,"username":"user"},"gid":  
        {"gid":1000,"groupname":"user"},  
      "mode":33204,"mtime":1441028214,"ctime":1460738554,"xattr":[]},  
  "origin":"APP_COMMAND_LINE_TOOL","origin_pid":2726,"task_id":1,"history":  
    []}
```

4. IDが1である脅威を隔離に移動する:

```
$ curl -v -c cookie.jar -b cookie.jar -k -X POST -H 'Content-  
Type:application/json'  
https://127.0.0.1:4443/api/10.2/quarantine_threat/1
```

レスポンス:

```
HTTP/1.0 200 OK  
Content-Type: application/json  
Content-Length:2  
Set-Cookie:DWToken=<...>; Secure; HttpOnly; Max-Age:900; Path=/  
Pragma: no-cache
```



```
{}
```

5. 指定されたWebサイトの隔離のコンテンツを表示する:

```
$ curl -v -k -X GET -c cookie.jar -b cookie.jar  
https://127.0.0.1:4443/api/10.2/quarantine/%2Fsites%2Fsite1
```

レスポンス:

```
HTTP/1.0 200 OK  
Content-Type: application/json  
Content-Length:76  
Set-Cookie:DWToken=<...>; Secure; HttpOnly; Max-Age:900; Path=/  
Pragma: no-cache  
  
[{"entry_id":"3070d3ce-7b6e-4143-9d9f-  
89ba3473a781","chunk_id":"801:2108d"}]
```

6. 隔離(分離)オブジェクトに関する情報を表示する:

```
$ curl -v -k -X GET -c cookie.jar -b cookie.jar  
https://127.0.0.1:4443/api/10.2/qentry_info/3070d3ce-7b6e-4143-9d9f-  
89ba3473a781@801:2108d
```

レスポンス:

```
HTTP/1.0 200 OK  
Content-Type: application/json  
Content-Length:781  
Set-Cookie:DWToken=<...>; Secure; HttpOnly; Max-Age:900; Path=/  
Pragma: no-cache  
  
{  
  "entry_id":"3070d3ce-7b6e-4143-9d9f-  
89ba3473a781","chunk_id":"3830313A3231303864",  
  "quarantine_dir":"2F686F6D652F757365722F2E636F6D2E64727765622E71756172616  
E74696E65",  
  "restore_path":"2E2E2F7473742F65696361722E636F6D2E747874","creation_time"  
:1462888884,  
  "report":{"object":"/home/user/tst/eicar.com.txt","size":68,"packer":[],  
  "virus":[{"type":"SE_KNOWN_VIRUS","name":"EICAR Test File (NOT a  
Virus!)"}]},  
  "heuristic_analysis":true,"core_fingerprint":"467CD4C6D423C55448B71CD5B81  
52776",  
  "item":[],"log":[],"user_time":0,"system_time":0},"stat":  
{  
  "dev":2049,"ino":898,  
  "size":68,"uid":{"uid":1000,"username":"user"},"gid":  
{  
    "gid":1000,"groupname":"user"},  
  "mode":33204,"mtime":1441028214,"ctime":1462888421,"xattr":[],"history":  
[],  
  "detection_time":1462888667,"origin":"APP_COMMAND_LINE_TOOL"}  
}
```

7. 設定の変更: SpIDer Guardをオフにする。

JSON形式のLexMapオブジェクトがあらかじめlexmap_ls_off.jsonというファイルに書き込まれている必要があります。



```
{"option":[{"key":"LinuxSpider","map":{"option":[{"key":"Start","value":{"item":["no"]}}]}]}
```

```
$ curl -v -k -c cookie.jar -b cookie.jar -X POST -H 'Content-Type: application/json' --data-binary '@lexmap_ls_off.json' https://127.0.0.1:4443/api/10.2/set_lexmap
```

レスポンス:

```
HTTP/1.0 200 OK
Content-Type: application/json
Content-Length:58
Set-Cookie:DWToken=<...>; Secure; HttpOnly; Max-Age:900; Path=/
Pragma: no-cache

{"item":[{"option":"LinuxSpider.Start","result":"EC_OK"}]}
```

8. 設定の変更: SpIDer Guardをオンにする。

JSON形式のLexMapオブジェクトがあらかじめ[lexmap_ls_on.json](#)というファイルに書き込まれている必要があります。

```
{"option":[{"key":"LinuxSpider","map":{"option":[{"key":"Start","value":{"item":["yes"]}}]}]}
```

```
$ curl -v -k -c cookie.jar -b cookie.jar -X POST -H 'Content-Type: application/json' --data-binary '@lexmap_ls_on.json' https://127.0.0.1:4443/api/10.2/set_lexmap
```

レスポンス:

```
HTTP/1.0 200 OK
Content-Type: application/json
Content-Length:58
Set-Cookie:DWToken=<...>; Secure; HttpOnly; Max-Age:900; Path=/
Pragma: no-cache

{"item":[{"option":"LinuxSpider.Start","result":"EC_OK"}]}
```

9. 設定の変更: ホストされているWebサイトをSpIDer Guardの保護下に置く。

このアクションは2つのステップで実行されます。まず、個別のサイト(SpIDer Guardでは「保護スペース」)のセクションを追加する必要があります。次に、サイトを保護するためのパラメータを指定する必要があります(少なくとも、サイトのファイルを格納するディレクトリへのパスを指定する必要があります)。

1) Webサイトを追加する。JSON形式のLexMapオブジェクトがあらかじめ[lexmap_site.json](#)というファイルに書き込まれている必要があります。

```
{"option":[{"key":"LinuxSpider","map":{"option":[{"key":"Space","map":{"option":[{"key":"<SITE_ID>","map":{"option":[]}}]}]}]}]}
```

ここで、<SITE_ID>は目的のWebサイトのIDです。

```
$ curl -v -k -c cookie.jar -b cookie.jar -X POST -H 'Content-Type: application/json' --data-binary '@lexmap_site.json' https://127.0.0.1:4443/api/10.2/set_lexmap
```

レスポンス:



```
HTTP/1.0 200 OK
Content-Type: application/json
Content-Length:11
Set-Cookie:DWToken=<...>; Secure; HttpOnly; Max-Age:900; Path=/
Pragma: no-cache

{"item":[]}
```

設定ファイルに新しく作成されたセクションにはまだパラメータが設定されていないため、このリクエストに対するレスポンスでは空のオブジェクトが返されます。

2) Webサイトのディレクトリへのパスを設定する。JSON形式のLexMapオブジェクトがあらかじめ [lexmap_site_path.json](#) というファイルに書き込まれている必要があります。

```
{"option":[{"key":"LinuxSpider","map":{"option":
[{"key":"Space","map":{"option":[{"key":"<SITE_ID>","map":
{"option":[{"key":"Path","value":{"item":["<PATH>"]}}]}]}]}],
ここで、<SITE_ID>は保護するWebサイトのID、<PATH>はこのサイトを格納しているディレクトリへのフルパスです。
```

```
$ curl -v -k -c cookie.jar -b cookie.jar -X POST -H 'Content-Type:
application/json' --data-binary '@lexmap_site_path.json'
https://127.0.0.1:4443/api/10.2/set_lexmap
```

レスポンス:

```
HTTP/1.0 200 OK
Content-Type: application/json
Content-Length:65
Set-Cookie:DWToken=<...>; Secure; HttpOnly; Max-Age:900; Path=/
Pragma: no-cache

{"item":[{"option":"LinuxSpider.Space.s2.Path","result":"EC_OK"}]}
```

この例では、s2は、SpIDer Guardによって保護されるディレクトリへのパスを指定したWebサイトのIDです。

10. 設定の変更: Webサイトの保護をオフにする。

JSON形式のLexMapオブジェクトがあらかじめ [lexmap_site_off.json](#) というファイルに書き込まれている必要があります。

```
{"option":[{"key":"LinuxSpider","map":{"option":
[{"key":"Space","map":{"option":[{"key":"<SITE_ID>","map":{"option":
[{"key":"Enable","value":{"item":["No"]}}]}]}]}],
ここで、<SITE_ID>は目的のWebサイトのIDです。
```

```
$ curl -v -k -c cookie.jar -b cookie.jar -X POST -H 'Content-Type:
application/json' --data-binary '@lexmap_site_off.json'
https://127.0.0.1:4443/api/10.2/set_lexmap
```

レスポンス:

```
HTTP/1.0 200 OK
Content-Type: application/json
Content-Length:67
```



```
Set-Cookie:DWToken=<...>; Secure; HttpOnly; Max-Age:900; Path=/  
Pragma: no-cache  
  
{"item":[{"option":"LinuxSpider.Space.s2.Enable","result":"EC_OK"}]}
```

この例では、*s2*は保護が無効になっている目的のWebサイトのIDです。



Dr.Web SNMPD

Dr.Web SNMPDは、SNMPプロトコルを実行するモニタリングシステムにDr.Web for UNIX File Serversを統合するように設計されたSNMPエージェントです。この統合により、Dr.Web for UNIX File Serversコンポーネントのステータスを追跡したり、脅威の検出と無効化に関する統計を収集したりできます。エージェントは、モニタリングシステムまたはSNMPマネージャーに以下の情報を提供するサポートをします。

- 任意のDr.Web for UNIX File Serversコンポーネントのステータス。
- 検出されたさまざまなタイプの脅威の数 (Dr.Web分類に対応)。

さらに、エージェントは、脅威を検出したときと検出された脅威の駆除が失敗したときにSNMPトラップを送信します。エージェントはSNMPプロトコルバージョン2cおよび3をサポートします。

エージェントが送信できる情報の説明は、Doctor Webによって作成されたMIB (管理情報ベース) の特別なセクションに格納されています。UNIX系オペレーティングシステム用にDr.Webが定義したMIBセクションには、以下の情報が指定されています。

1. 脅威の検出と駆除、Dr.Web for UNIX File Serversコンポーネントに関連するエラーに関するSNMPトラップ通知のフォーマット。
2. Dr.Web for UNIX File Servers操作の統計。
3. Dr.Web for UNIX File Serversコンポーネントのステータス。

SNMPプロトコルを介して取得できる情報の詳細については、対応する[セクション](#)を参照してください。

動作原理

このセクションの内容:

- [機能](#)
- [システムSNMPエージェントとの統合](#)

概要

デフォルトでは、コンポーネントはDr.Web for UNIX File Serversの起動時に自動的に実行されます。実行されると、コンポーネントはMIB Dr.Webで記述されている構造に従ってデータを構造化し、外部SNMPマネージャーからのデータ受信要求を待機します。コンポーネントは、[Dr.Web ConfigD](#)設定デーモンから、Dr.Web for UNIX File Serversコンポーネントのステータスに関する情報と検出された脅威に関する通知を直接受信します。

脅威は、Dr.Web for UNIX File Serversコンポーネントによるスキャン中にスキャンエンジンによって検出されます。何らかの脅威が検出されると、(この脅威の種類に) 該当するカウントが1つ増え、通知を受信できるすべてのSNMPマネージャーは、検出された脅威について通知するSNMPトラップを受け取ります。



カウンターの収集値 (たとえば、検出された脅威のカウンター) は、Dr.Web SNMPDの起動の間は保存されません。したがって、Dr.Web SNMPDが何らかの理由 (Dr.Web for UNIX File Serversの一般的な再起動を含む) で再起動されると、収集されたカウンターの値は0にリセットされます。



システムSNMPエージェントとの統合

メインシステムのSNMPエージェント**snmpd**(**net-snmp**)がすでにサーバー上で動作している場合にDr.Web SNMPエージェントが正しく動作するようにするには、Dr.Web MIBブランチを介した**snmpd**からDr.Web SNMPDへのSNMPリクエスト送信を設定します。そのためには、次の行を追加して**snmpd**設定ファイル(**GNU/Linux**の場合は、通常/etc/snmp/snmpd.conf)を編集します。

```
proxy -v <version> -c <community> <address>:<port> <MIB branch>
```

- <version> - 使用中のSNMPバージョン(2c、3)。
- <community> - Dr.Web SNMPDによって使用される「コミュニティストリング」。
- <address>:<port> - Dr.Web SNMPDによって待ち受け(リッスン)されるネットワークソケット。
- <MIB branch> - Dr.Webが使用する変数とSNMPトラップの[説明](#)を含むMIBブランチのOID(OIDは.1.3.6.1.4.1.29690)。

Dr.Web SNMPエージェントをデフォルト設定で使用している場合、追加する行は以下のようになります。

```
proxy -v 2c -c public localhost:50000 .1.3.6.1.4.1.29690
```

この場合、ポート161はシステムの標準**snmpd**によって使用されるため、ListenAddress[パラメータ](#)にDr.Web SNMPDに別のポートを指定する必要があります(この例では、50000)。



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 SNMPDを起動するには、次のコマンドを使用します。

```
$ <opt_dir>/bin/drweb-snmpd [<parameters>]
```

Dr.Web SNMPDは次のオプションを処理できます。

パラメータ	説明
--help	機能：コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了するように指示します。 短縮形： -h 引数： None
--version	機能：このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了するように指示します。 短縮形： -v 引数： None

例：

```
$ /opt/drweb.com/bin/drweb-snmpd --help
```

このコマンドはDr.Web SNMPDに関する簡単なヘルプ情報を出力します。

スタートアップノート

コンポーネントは、自律モードで（他のコンポーネントから自律的に）OSのコマンドラインから直接起動することはできません。必要に応じてDr.Web ConfigD設定デーモンによって自動的に起動されます（原則として、OSの起動時）。コンポーネントの動作を管理するには、Dr.Web for UNIX File Servers用のDr.Web Ctlコマンドラインベースの管理ツールを使用できます（これは**drweb-ctl**コマンドを使用して呼び出されます）。



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ドキュメントを要求するには、次のコマンドを使用します。**man 1 drweb-snmpd**

設定パラメータ

コンポーネントは、Dr.Web for UNIX File Serversの統合された設定ファイルの[SNMPD]セクションで指定されている設定パラメータを使用します。

セクションには以下のパラメータが含まれています。

LogLevel {logging level}	コンポーネントのログの詳細レベル パラメータ値が指定されていない場合は、[Root]セクションのDefaultLogLevelパラメータの値が使用されます。
--	---



	デフォルト値: Notice
Log <i>{log type}</i>	コンポーネントの ロギング方式 。 デフォルト値: Auto
ExePath <i>{path to file}</i>	コンポーネントの実行ファイルへのパス。 デフォルト値: <opt_dir>/bin/drweb-snmpd <ul style="list-style-type: none">• GNU/Linuxの場合: /opt/drweb.com/bin/drweb-snmpd• FreeBSDの場合: /usr/local/libexec/drweb.com/bin/drweb-snmpd
Start <i>{Boolean}</i>	コンポーネントは Dr.Web ConfigD 設定デーモンによって起動される必要があります。 このパラメータにYes値を指定すると、設定デーモンはただちにコンポーネントを開始するように指示されます。また、No値を指定すると、設定デーモンはただちにコンポーネントを終了するように指示されます。 デフォルト値: No
RunAsUser <i>{UID / user name}</i>	このパラメータは、コンポーネントを実行するユーザー名を決定します。ユーザー名は、ユーザーのUIDまたはユーザーのログインとして指定できます。ユーザー名が数字で構成されている場合（UIDに似ている場合）は、「name:」というプレフィックスを付けて指定します。次に例を示します。 RunAsUser = name:123456。 ユーザー名が指定されていない場合、コンポーネント操作は開始後にエラーが発生して終了します。 デフォルト値: drweb
ListenAddress <i>{address}</i>	クライアント接続（SNMPマネージャー）を待機するDr.Web SNMPDが待ち受け（リッスン）するアドレス（IPアドレスとポート）。 snmpd とのインタラクションには、標準ポート（161）とは異なるポートの指定と、 snmpd にプロキシ用の 設定を行う 必要があります。 デフォルト値: 127.0.0.1:161
SnmpVersion <i>{V2c / V3}</i>	使用されるSNMPプロトコルのバージョン（ <i>SNMPv2c</i> または <i>SNMPv3</i> ）。 デフォルト値: V2c
V3EngineId <i>{string}</i>	<i>SNMPv3</i> のエンジンIDの識別子（文字列）（ RFC 3411 に準拠）。 デフォルト値: 800073FA044452574542
TrapReceiver	Dr.Web for UNIX File Serversコンポーネントが脅威を検出した後にDr.Web SNMPDによって <i>SNMP</i> トラップが送信されるアド



<code>{address list}</code>	<p>レスのリスト（IPアドレスとポート）。</p> <p>リストをパラメータ値として指定できます。リストの値は、コンマ（引用符内の各値）で区切る必要があります。パラメータはセクションで複数回指定できます（この場合、そのすべての値が1つのリストにまとめられます）。</p> <p>例：ソケット192.168.0.1:1234および10.20.30.45:5678をリストに追加します。</p> <p>1. 設定ファイルに値を追加します。</p> <ul style="list-style-type: none">1つの文字列に2つの値 <div><pre>セクション[SNMPD] TrapReceiver = "192.168.0.1:1234", "10.20.30.45:5678"</pre></div> <ul style="list-style-type: none">2つの文字列（文字列ごとに1つの値） <div><pre>[SNMPD] TrapReceiver = 192.168.0.1:1234 TrapReceiver = 10.20.30.45:5678</pre></div> <p>2. コマンド<code>drweb-ctl cfset</code>を使用して値を追加します。</p> <div><pre># drweb-ctl cfset SNMPD.TrapReceiver - a 192.168.0.1:1234 # drweb-ctl cfset SNMPD.TrapReceiver - a 10.20.30.45:5678</pre></div> <p>デフォルト値：（未設定）</p>
V2cCommunity <code>{string}</code>	<p>Dr.Web MIB変数 が読み取りアクセスされたときに、SNMPマネージャ（<i>SNMPv2c</i>プロトコル）を認証する文字列「SNMP read community」。</p> <p>SnmVersion = <i>V2c</i>の場合、このパラメータが使用されず。</p> <p>デフォルト値：<code>public</code></p>
V3UserName <code>{string}</code>	<p>Dr.Web MIB変数 が読み取りアクセスされたときに、SNMPマネージャ（<i>SNMPv3</i>プロトコル）を認証するユーザー名。</p> <p>SnmVersion = <i>V3</i>の場合、このパラメータが使用されず。</p> <p>デフォルト値：<code>noAuthUser</code></p>
V3Auth <code>{SHA(<pwd>) / MD5(<pwd>) / None}</code>	<p>Dr.Web MIB変数 が読み取りアクセスされたときに、SNMPマネージャ（<i>SNMPv2c</i>プロトコル）を認証する方法。</p> <p>使用可能な値：</p> <ul style="list-style-type: none">SHA（<PWD>）-パスワードのSHAハッシュが使用されます（<PWD>文字列）。



	<ul style="list-style-type: none">• MD5 (<PWD>) -パスワードのMD5ハッシュが使用されます (<PWD>文字列)。• None-認証は無効になります。 <p>ここで、<PWD>はプレーンテキストのパスワードです。</p> <p>コマンドラインからパラメータ値を指定する場合、シェルによってはスラッシュ記号\を使用した角括弧のエスケープを必要とする場合があります。</p> <p>例：</p> <ol style="list-style-type: none">1. 設定ファイル内のパラメータ値： V3Auth = MD5(123456)2. コマンドdrweb-ctlcfsetを使用して、コマンドラインから同じパラメータ値を指定する場合： drweb-ctl cfset SNMPD.V3Auth MD5\ (123456\) <p>SnmVersion = V3の場合、このパラメータが使用されません。</p> <p>デフォルト値：なし</p>
V3Privacy {DES(<secret>) / AES128(<secret>) / None}	<p>SNMPメッセージを暗号化する方法 (SNMPv3プロトコル)。</p> <p>使用可能な値：</p> <ul style="list-style-type: none">• DES (<secret>) -DES暗号化アルゴリズムが使用されます。• AES128 (<secret>) - AES128暗号化アルゴリズムが使用されます。• None-SNMPメッセージは暗号化されません。 <p>ここで、<secret>は、マネージャーとエージェントが共有するシークレットキーです (プレーンテキスト)。</p> <p>コマンドラインからパラメータ値を指定する場合、シェルによってはスラッシュ記号\を使用した角括弧のエスケープを必要とする場合があります。</p> <p>例：</p> <ol style="list-style-type: none">1. 設定ファイル内のパラメータ値： V3Privacy = AES128(supersecret)2. コマンドdrweb-ctlcfsetを使用して、コマンドラインから同じパラメータ値を指定する場合： drweb-ctl cfset SNMPD.V3Privacy AES128\ (supersecret\) <p>SnmVersion = V3の場合、このパラメータが使用されません。</p> <p>デフォルト値：なし</p>



SNMPモニタリングシステムとの統合

Dr.Web SNMPエージェントは、SNMPプロトコル、バージョン2cまたは3を使用するモニタリングシステムのデータプロバイダーとして機能します。制御に使用できるデータのリストとデータ構造は、Dr.Web for UNIX File Serversに付属のDr.Web MIB記述ファイルDRWEB-SNMPD-MIB.txtに記述されています。このファイルは、ディレクトリ<opt_dir>/share/drweb-snmpd/mibsにあります。

簡単に設定できるように、このコンポーネントには一般的なモニタリングシステム用の設定テンプレートが付属しています。

- [Munin](#)
- [Nagios](#)
- [Zabbix](#)

モニタリングシステム用のカスタマイズテンプレートは、<opt_dir>/share/drweb-snmpd/connectorsディレクトリにあります。

Muninモニタリングシステムとの統合

Muninモニタリングシステムには、モニタリング対象ホストにローカルに存在するクライアント**munin-node**から統計を収集する中央サーバー（マスター）**munin**が含まれています。サーバーの要求に応じて、各モニタリングクライアントは、サーバーに転送されたデータを提供するプラグイン（プラグイン）を起動することによって、モニタリング対象ホストの動作に関するデータを収集します。

Dr.Web SNMPDと**Munin**モニタリングシステム間の接続を可能にするために、すぐに利用可能な**munin-node**用プラグインが提供されています。プラグインは、<opt_dir>/share/drweb-snmpd/connectors/munin/pluginsディレクトリにあります。このプラグインは、下の2つのグラフの作成に必要なデータを収集します。

- 検出された脅威の数
- ファイルのスキャン統計情報
- メールメッセージのスキャン統計情報

これらのプラグインは、SNMPプロトコルバージョン1、2c、3をサポートしています。これらのテンプレートプラグインに基づいて他のプラグインを作成すれば、Dr.Web SNMPD経由でDr.Web for UNIX File Serversコンポーネントのステータスをポーリングすることができます。

<opt_dir>/share/drweb-snmpd/connectors/muninディレクトリには、下のファイルがあります。

ファイル	説明
plugins/snmp__drweb_malware	ホスト上の Dr.Web for UNIX File Serversによって検出された脅威の数を収集するために、SNMP経由で Dr.Web SNMPDをポーリングするための munin-node プラグイン。
plugins/snmp__drweb_filecheck	ホスト上の Dr.Web for UNIX File Serversによってスキャンされたファイルの統計を収集するために、SNMP経由で Dr.Web SNMPDをポーリングするための munin-node プラグイン。



ファイル	説明
plugins/snmp__drweb_maild_multi	ホスト上のDr.Web for UNIX File Serversによってスキャンされたメールメッセージの統計を収集するために、SNMP経由でのDr.Web SNMPDのポーリングに使用される munin-node プラグイン。 このプラグインは、 Munin バージョン1.4以上で利用可能な機能 <i>multigraph</i> を使用します。
plugin-conf.d/drweb.cfg	Dr.Webプラグインの munin-node 設定の例（環境変数用）。

Muninにホストを接続する

この説明では、**Munin**モニタリングシステムがモニタリングサーバーにすでにデプロイされており、モニタリング対象ホストにはDr.Web SNMPDがインストール済みで**munin-node**と共に機能していると想定しています（コンポーネントは**snmpd**と共に**プロキシ**モードで機能することができます）。

1. モニタリング対象ホストの設定

- `snmp__drweb_*`ファイルを、プラグインライブラリ**munin-node**があるディレクトリにコピーします（ディレクトリはOSによって異なります）。たとえば、**Debian/Ubuntu**オペレーティングシステムであれば、パスは `/usr/share/munin/plugins` となります。
- 提供されているDr.Webプラグインを接続して、**munin-node**を設定します。これを行うには、**munin-node**と一緒に配布される**munin-node-configure**ユーティリティを使用します。

たとえば、次のようなコマンドです。

```
$ munin-node-configure --shell --snmp localhost
```

端末画面に、プラグインに必要なシンボリックリンクを作成するためのコマンドのリストを表示します。コピーして、コマンドラインで実行します。指定されたコマンドでは、次のことを前提としています。

- 1) **munin-node**は、Dr.Web SNMPDがインストールされているのと同じホストにインストールされる。インストール先が異なる場合は、`localhost`値ではなく、モニタリング対象ホストの適切なFQDNまたはIPアドレスを指定してください。
 - 2) Dr.Web SNMPDはSNMPバージョン2cを使用する。他のバージョンの場合は、**munin-node-configure**コマンドで適切なSNMPバージョンを指定してください。このコマンドには、プラグインを柔軟に設定するための引数がいくつかあります。たとえば、SNMPプロトコルのバージョン、モニタリング対象ホストでSNMPエージェントが待機しているポート、*コミュニティ*ストリングの実際の値などを指定できます。必要に応じて、**munin-node-configure**コマンドのマニュアルを参照してください。
- 必要であれば、**munin-node**用にインストールしたDr.Webプラグインを実行する環境のパラメータ値を定義（または再定義）します。環境パラメータとして、値*コミュニティ*ストリングが使用されます。これは、SNMPエージェントなどが使用するポートです。これらのパラメータは、ファイル `/etc/munin/plugin-conf.d/drweb` に定義する必要があります（必要に応じて作成します）。このファイルの例として、提供されているファイル `drweb.cfg` を使用します。
 - **munin-node**設定ファイル (`munin-node.conf`) で、モニタリング対象のパラメータの値を受け取るために**munin**サーバー（マスター）を**munin-node**に接続できるホストのすべてのIPアドレスを含めるための正規表現を指定します。たとえば、次のようになります。



```
allow ^10\.20\.30\.40$
```

この場合、IPアドレス10.20.30.40のみがホストパラメータを受信できます。

- たとえば、次のコマンドを使用して**munin-node**を再起動します。

```
# service munin-node restart
```

2. Muninサーバー(マスター)の設定

モニタリング対象ホストのアドレスと識別子を**Munin**設定ファイル**munin.conf**に追加します。このファイルは、デフォルトでは/etcディレクトリにあります(**Debian/Ubuntu**オペレーティングシステムでは/etc/munin/munin.confになります)。

```
[ <ID>; <hostname>. <domain> ]
address <host IP address>
use_node_name yes
```

ここで、<ID>は表示されるホストの識別子、<hostname>はホストの名前、<domain>はドメインの名前、<host IP address>はホストのIPアドレスです。

Muninモニタリングシステムの設定に関する公式マニュアルについては<http://munin.readthedocs.io>を参照してください。

Zabbixモニタリングシステムとの統合

Dr.Web SNMPDと**Zabbix**モニタリングシステム間の接続を確立するために必要なファイルテンプレートは、<opt_dir>/share/drweb-snmpd/connectors/zabbixディレクトリにあります。

ファイル	説明
zbx_drweb.xml	Dr.Web for UNIX File Serversがインストールされているモニタリング対象ホストを説明するためのテンプレート。
snmptt.drweb.zabbix.conf	SNMPトラップハンドラーである snmptt ユーティリティの設定

モニタリング対象ホストの機能を説明するためのテンプレート。

- カウンター(**Zabbix**の用語では「アイテム」)の説明。デフォルトでは、テンプレートはSNMP v2で使用されるように設定されています。
- 既存のグラフのセット: スキャンされたファイルの数と検出された脅威のタイプ別の分布。



Zabbixにホストを接続する

この説明では、**Zabbix**モニタリングシステムがモニタリングサーバーにすでにデプロイされており、モニタリング対象ホストにはDr.Web SNMPDがインストール済みで機能していると想定しています（コンポーネントは**snmpd**と共に**プロキシ**モードで機能することができます）。さらに、モニタリング対象ホストから**SNMP**トラップ（保護対象サーバーでDr.Web for UNIX File Serversによって検出された脅威に関する通知を含む）を受信する場合は、モニタリングサーバーに**net-snmp**パッケージをインストールします（標準ツールの**snmptt**および**snmptrapd**が使用されます）。

1. **Zabbix** Webインターフェースの**Configuration -> Templates**タブで、
`<opt_dir>/share/drweb-snmpd/connectors/zabbix/zbx_drweb.xml`ファイルからモニタリング対象ホストのテンプレートをインポートします。
2. モニタリング対象ホストを適切なリストに追加します（**Hosts -> Create host**）。ホストの適切なパラメータとSNMPインターフェースの設定を指定します（ホストの**drweb-snmpd**と**snmpd**の設定と一致する必要があります）。

- **Host**タブ:

Host name: *drweb-host*

Visible name: *DRWEB_HOST*

Groups: *Linux servers*を選択します

Snmp interfaces: **Add**をクリックして、Dr.Web SNMPDによって使用されるIPアドレスとポート（Dr.Web SNMPDはローカルホストで動作すると見なされるため、デフォルトではアドレス**127.0.0.1**とポート**161**が指定されています）を指定します。

- **Templates**タブ:

Addを押し、*DRWEB*を確認し、**Select**を押しします。

- **Macros**タブ:

Macro: *{ \$SNMP_COMMUNITY }*

Value: SNMP V2cに「read community」を指定します（デフォルトでは、*public*）。

Saveをクリックします。

注意: *{ \$SNMP_COMMUNITY }*マクロは、ホストテンプレートで直接指定できます。



デフォルトでは、インポートされた *DRWEB* テンプレートはSNMP v2用に設定されています。他のバージョンのSNMPを使用する場合は、該当するページでテンプレートに必要な編集を行います。

3. テンプレートがモニタリング対象ホストにバインドされた後、SNMP設定が正しく指定されていれば、**Zabbix**モニタリングシステムはテンプレートのカウンター（*アイテム*）のデータ収集を開始します。収集されたデータは、**Monitoring -> Latest Data**と**Monitoring -> Graphs**に表示されます。
4. Dr.Web SNMPDから**SNMP**トラップ通知を収集するために特別な *アイテムdrweb-traps*が使用されます。受信した**SNMP**トラップ通知のログは、**Monitoring -> Latest Data -> drweb-traps -> history**ページで利用できます。**Zabbix**は、通知を収集するために、**net-snmp**パッケージの標準ツール**snmptt**と**snmptrapd**を使います。Dr.Web SNMPDから**SNMP**トラップ通知を受信するためのツールの設定方法については、以下を参照してください。
5. 必要に応じて、Dr.Web SNMPDからの**SNMP**トラップ通知の受信時に状態を変更するトリガーを設定できます。状態の変更は、適切な通知を生成するためのイベントソースとして使用できます。下の例は、トリガーの設定式を示します。この式は**trigger expression**フィールドで指定されます。



- **Zabbixバージョン2.xの場合:**

```
{({TRIGGER.VALUE}=0 &
{DRWEB:snmptrap[.*\1\3\6\1\4\1\29690\...*].nodata(60)}=1 ) |
({TRIGGER.VALUE}=1 &
{DRWEB:snmptrap[.*\1\3\6\1\4\1\29690\...*].nodata(60)}=0)}
```

- **Zabbixバージョン3.xの場合:**

```
((TRIGGER.VALUE)=0 and {drweb-host:snmptrap[".29690."].nodata(60)}=1 ) or
({TRIGGER.VALUE}=1 and {drweb-host:snmptrap[".29690."].nodata(60)}=0 )
```

Dr.Web SNMPDからのSNMPトラップのログが1分以内に更新された場合、イベントがトリガー（値を1に設定）されます。ログが次の1分以内に更新されなかった場合、トリガーの値は再び0に設定されます。

Severityでは、このトリガーの通知タイプを *Not classified* とは異なるものにすることをお勧めします（例：*Warning*）。

ZabbixのSNMPトラップ通知の受信を設定する

1. モニタリング対象ホストのDr.Web SNMPD設定 (**TrapReceiver**パラメータ) で、**Zabbix**が動作しているホストで**snmptrapd**が待ち受け(リッスン)するアドレスを指定する必要があります。次に例を示します。

```
SNMPD.TrapReceiver = 10.20.30.40:162
```

2. **snmptrapd**の設定ファイル(**snmptrapd.conf**)に、同じアドレスと、受信したSNMPトラップ通知を処理するアプリケーションを指定します（この例では**snmpthandler**、**snmptt**コンポーネント）。

```
snmpTrapdAddr 10.20.30.40:162
traphandle default /usr/sbin/snmptthandler
```

Dr.Web SNMPDによって送信されたSNMPトラップを**snmptt**が不明なものとして破棄しないように、ファイルに次の文字列を追加します。

```
outputOption n
```

3. **snmptthandler**コンポーネントは、**Zabbix**のホストテンプレートに設定されている正規表現 (*アイテム drweb-traps* エレメント) に対応する指定された形式に従って、受信したSNMPトラップ通知をディスクのファイルに保存します。保存された通知のSNMPトラップフォーマットは、`<opt_dir>/share/drweb-snmppd/connectors/zabbix/snmptt.drweb.zabbix.conf` ファイルで指定します。ファイルは、`/etc/snmp` にコピーする必要があります。
4. さらに、フォーマットファイルへのパスを**snmptt.ini**に指定する必要があります。

```
[TrapFiles]
# snmptt.conf ファイルのリスト（これはsnmptrapd.conf ファイルではありません）。
# 完全なパスとファイル名。例: '/etc/snmp/snmptt.conf'
snmptt_conf_files = <<END
/etc/snmp/snmptt.conf
/etc/snmp/snmptt.drweb.zabbix.conf
END
```

その後、デーモンモードで起動している場合は**snmptt**を再起動します。



5. **Zabbix**サーバーの設定ファイル(`zabbix-server.conf`)で、次の設定を指定します(または、すでに指定されているかどうかを確認します)。

```
SNMPTrapperFile=/var/log/snmpd/snmpd.log
StartSNMPTrapper=1
```

ここで、`/var/log/snmpd/snmpd.log`は、受信したSNMPトラップに関する情報を登録するために**snmpd**が使用するログファイルです。

Zabbixの公式マニュアルについては、<https://www.zabbix.com/documentation/>を参照してください。

Nagiosモニタリングシステムとの統合

Dr.Web SNMPDと**Nagios**モニタリングシステム間の接続を確立するために必要なファイルと**Nagios**設定例は、`<opt_dir>/share/drweb-snmpd/connectors/nagios`ディレクトリにあります。

ファイル	説明
<code>nagiosgraph/rrdopts.conf-sample</code>	RRD設定ファイルの例
<code>objects/drweb.cfg</code>	<i>drweb</i> オブジェクトを記述する設定ファイル
<code>objects/nagiosgraph.cfg</code>	Nagios が使用する Nagiosgraph によって使用されるグラフ描画のためのコンポーネントの設定ファイル
<code>plugins/check_drweb</code>	Dr.Web for UNIX File Serversがインストールされているホストからデータを収集するためのスクリプト
<code>plugins/eventhandlers/submit_check_result</code>	<i>SNMP</i> トラップ通知を処理するためのスクリプト
<code>snmp/snmpd.drweb.nagios.conf</code>	<i>SNMP</i> トラップハンドラーである snmpd ユーティリティの設定

Nagiosにホストを接続する

この説明では、Webサーバーとグラフィックツール**Nagiosgraph**の設定を含む**Nagios**モニタリングシステムがモニタリングサーバーにすでにデプロイされており、モニタリング対象ホストにはDr.Web SNMPDがインストール済みで機能していると想定しています(コンポーネントは**snmpd**と共に**プロキシ**モードで機能することができます)。さらに、モニタリング対象ホストから*SNMP*トラップ(保護対象サーバーでDr.Web for UNIX File Serversによって検出された脅威に関する通知を含む)を受信する場合は、モニタリングサーバーに**net-snmp**パッケージをインストールします(標準ツールの**snmpd**および**snmptrapd**が使用されます)。

現在のマニュアルでは、次のようなパスの規則が使用されています(実際のパスはオペレーティングシステムと**Nagios**のインストールによって異なります)。

- `<NAGIOS_PLUGINS_DIR>` - **Nagios**プラグインを含むディレクトリ
(例: `/usr/lib64/nagios/plugins`)。
- `<NAGIOS_ETC_DIR>` - **Nagios**設定を含むディレクトリ(例: `/etc/nagios`)。
- `<NAGIOS_OBJECTS_DIR>` - **Nagios**オブジェクトを含むディレクトリ
(例: `/etc/nagios/objects`)。



- `<NAGIOSGRAPH_DIR>` - **Nagiosgraph**ディレクトリ(例: `/usr/local/nagiosgraph`)。
- `<NAGIOS_PERFDATA_LOG>` - **Nagios**がサービスチェックの結果を記録するファイル
(`<NAGIOSGRAPH_DIR>/etc/nagiosgraph.conf`の`perflog`ファイルと同じでなければなりません)。このファイルのレコードは`<NAGIOSGRAPH_DIR>/bin/insert.pl`スクリプトによって読み取られ、対応するRRAアーカイブ**RRD**ツールに記録されます。

Nagiosを設定する:

1. `check_drweb`ファイルを`<NAGIOS_PLUGINS_DIR>`ディレクトリに、`drweb.cfg`ファイルを`<NAGIOS_OBJECTS_DIR>`ディレクトリにコピーします。
2. 監視対象のDr.Web for UNIX File Serversがあるホストを`drweb`グループに追加します。ホストではDr.Web SNMPDが実行されている必要があります。デフォルトでは、このグループには`localhost`のみが追加されます。
3. 必要に応じて、**snmpwalk**ツールを介して`drweb`ホストのDr.Web SNMPDに接続するように指示する`check_drweb`コマンドを編集します。

```
snmpwalk -c public -v 2c $HOSTADDRESS$:161
```

SNMPプロトコルの適切なバージョンとパラメータ(「コミュニティストリング」や認証パラメータなど)の他、ポートを指定します。`$HOSTADDRESS$`変数をコマンドに含める必要があります(この変数は後でコマンドが呼び出されたときに、**Nagios**によって正しいホストアドレスに自動的に置き換えられるためです)。このコマンドではOIDは必要ありません。また、実行ファイルへのフルパス(通常は`/usr/local/bin/snmpwalk`)を使用してコマンドを指定することをお勧めします。

4. 次の文字列をファイルに追加して、`<NAGIOS_ETC_DIR>/nagios.cfg`設定ファイルの**DrWeb**オブジェクトを接続します。

```
cfg_file= <NAGIOS_OBJECTS_DIR>/drweb.cfg
```

5. **DrWeb**グラフィック用の**RRD**ツール設定を`rrdopts.conf-sample`ファイルから`<NAGIOSGRAPH_DIR>/etc/rrdopts.conf`ファイルに追加します。
6. **Nagiosgraph**がまだ設定されていない場合は、その設定に対して次の手順を実行します。
 - `nagiosgraph.cfg`ファイルを`<NAGIOS_OBJECTS_DIR>`ディレクトリにコピーし、**process-service-perfdata-for-nagiosgraph**コマンドで`insert.pl`スクリプトへのパスを編集します。たとえば、次のようになります。

```
$ awk '$1 == "command_line" { $2 = "<NAGIOSGRAPH_DIR>/bin/insert.pl" }  
{ print }' ./objects/nagiosgraph.cfg >  
<NAGIOS_OBJECTS_DIR>/nagiosgraph.cfg
```

- 次の行を追加して、`<NAGIOS_ETC_DIR>/nagios.cfg`設定ファイルにこのファイルを接続します。

```
cfg_file=<NAGIOS_OBJECTS_DIR>/nagiosgraph.cfg
```

7. `<NAGIOS_ETC_DIR>/nagios.cfg`設定ファイルの**Nagios**パラメータの値を確認します。



```
check_external_commands=1
execute_host_checks=1
accept_passive_host_checks=1
enable_notifications=1
enable_event_handlers=1

process_performance_data=1
service_perfdata_file=/usr/nagiosgraph/var/rrd/perfdata.log
service_perfdata_file_template=$LASTSERVICECHECK$||$HOSTNAME$||$SERVICEDE
SC$||$SERVICEOUTPUT$||$SERVICEPERFDATA$
service_perfdata_file_mode=a
service_perfdata_file_processing_interval=30
service_perfdata_file_processing_command=process-service-perfdata-for-
nagiosgraph

check_service_freshness=1
enable_flap_detection=1
enable_embedded_perl=1
enable_environment_macros=1
```

NagiosのSNMPトラップ通知の受信を設定する

1. モニタリング対象ホストのDr.Web SNMPD設定 (**TrapReceiver**パラメータ) で、**Nagios**が動作しているホストで**snmptrapd**が待ち受け(リッスン)するアドレスを指定します。次に例を示します。

```
SNMPD.TrapReceiver = 10.20.30.40:162
```

2. **SNMPトラップ**を受信したときに呼び出される
<**NAGIOS_PLUGINS_DIR**>/eventhandlers/submit_check_resultスクリプトがあるかどうかを確認します。スクリプトが見つからない場合は、<**opt_dir**>/share/drweb-snmppd/connectors/nagios/plugins/eventhandlers/ディレクトリのsubmit_check_resultファイルをこの場所にコピーします。このファイルで、CommandFileパラメータに指定されているパスを変更します。これは、<**NAGIOS_ETC_DIR**>/nagios.cfgファイルのcommand_fileパラメータと同じ値である必要があります。
3. snmptt.drweb.nagios.confファイルを/etc/snmp/snmptt.drweb.nagios.confにコピーします。このファイルで、パスをsubmit_check_resultに変更します。たとえば、次のようなコマンドを使用します。

```
$ awk '$1 == "EXEC" { $2 =  
<NAGIOS_PLUGINS_DIR>/eventhandlers/submit_check_result }{ print }'  
./snmp/snmptt.drweb.nagios.conf > /etc/snmp/snmptt.drweb.nagios.conf
```

4. 「/etc/snmp/snmptt.drweb.nagios.conf」文字列を/etc/snmp/snmptt.iniファイルに追加します。その後、デーモンモードで起動している場合は**snmptt**を再起動します。

Nagiosに必要な設定ファイルをすべて追加して編集したら、次のコマンドを使用して**Nagios**をデバッグモードで実行します。

```
# nagios -v <NAGIOS_ETC_DIR>/nagios.cfg
```

このコマンドを受け取ると、**Nagios**は設定エラーをチェックします。エラーがなかった場合は、**Nagios**を通常どおりに再起動できます (たとえば、**service nagios restart**コマンドを使用して)。



Nagiosの公式マニュアルについては、<http://www.nagios.org/documentation/>を参照してください。

Dr.Web SNMP MIB

SNMPプロトコルを介して外部モニタリングシステムから取得できるDr.Web for UNIX File Serversの動作パラメータの一覧を以下の表に示します。

パラメータ名	パラメータのOID	パラメータのタイプと説明
すべての名前に共通のプレフィックス: .iso.org.dod.internet.private.enterprises.drweb.drwebSnmpd すべてのOIDに共通のプレフィックス: .1.3.6.1.4.1.29690.2		
alert	イベントに関する非同期通知 (SNMPトラップ)	
threatAlert	.1.1	脅威の検出に関する通知
threatAlertFile	.1.1.1	感染ファイル名 (文字列)
threatAlertType	.1.1.2	脅威の種類 (整数*)
threatAlertName	.1.1.3	脅威名 (文字列)
threatAlertOrigin	.1.1.4	脅威を検出したコンポーネントの識別子 (整数***)
threatAlertRemoteIp	.1.1.5	ファイルへのアクセスに使用されたりモートホストのIPアドレス (文字列)
threatAlertRemoteUser	.1.1.6	ファイルにアクセスしたりモートユーザーの名前 (文字列)
threatAlertRemoteDomain	.1.1.7	ファイルへのアクセスに使用されたりモートホストの名前 (文字列)
threatActionErrorAlert	.1.2	脅威を駆除しようとしたときに発生したエラーに関する通知
threatActionErrorAlertFile	.1.2.1	感染ファイル名 (文字列)
threatActionErrorAlertType	.1.2.2	脅威の種類 (整数*)
threatActionErrorAlertName	.1.2.3	脅威名 (文字列)
threatActionErrorAlertOrigin	.1.2.4	脅威を検出したコンポーネントの識別子 (整数***)
threatActionErrorAlertError	.1.2.5	エラーの説明 (文字列)
threatActionErrorAlertErrorCode	.1.2.6	エラーコード (エラーカタログのコードに対応する整数)



パラメータ名	パラメータのOID	パラメータのタイプと説明
<i>threatActionErrorAlertAction</i>	.1.2.7	失敗したアクション(1 - 修復、2 - 隔離、3 - 削除、4 - 報告、5 - 無視)
<i>componentFailureAlert</i>	.1.3	コンポーネント障害に関する通知
<i>componentFailureAlertName</i>	.1.3.1	コンポーネント識別子(整数***)
<i>componentFailureAlertExitCodeDescription</i>	.1.3.2	コンポーネント終了コードの説明(文字列)
<i>componentFailureAlertExitCode</i>	.1.3.3	エラーコード(エラーカタログのコードに対応する整数)
<i>infectedUrlAlert</i>	.1.4	悪質なURLのブロックに関する通知(HTTP/HTTPS接続)
<i>infectedUrlAlertUrl</i>	.1.4.1	ブロックされたURL(文字列)
<i>infectedUrlAlertDirection</i>	.1.4.2	HTTPメッセージの方向(整数: 1 - 要求、2 - 応答)
<i>infectedUrlAlertType</i>	.1.4.3	脅威の種類(整数*)
<i>infectedUrlAlertName</i>	.1.4.4	脅威名(文字列)
<i>infectedUrlAlertOrigin</i>	.1.4.5	脅威を検出したコンポーネントの識別子(整数***)
<i>infectedUrlAlertSrcIp</i>	.1.4.6	接続元のIPアドレス(文字列)
<i>infectedUrlAlertSrcPort</i>	.1.4.7	接続元のポート(整数)
<i>infectedUrlAlertDstIp</i>	.1.4.8	接続先のIPアドレス(文字列)
<i>infectedUrlAlertDstPort</i>	.1.4.9	接続先のポート(整数)
<i>infectedUrlAlertSniHost</i>	.1.4.10	接続先のSNI(SSL接続)(文字列)
<i>infectedUrlAlertExePath</i>	.1.4.11	接続を確立したプログラムの実行可能パス(文字列)
<i>infectedUrlAlertUserName</i>	.1.4.12	接続を確立するプログラムを実行する権限を持つユーザーの名前(文字列)
<i>infectedAttachmentAlert</i>	.1.5	感染したメールの添付ファイルの検出に関する通知
<i>infectedAttachmentAlertType</i>	.1.5.1	脅威の種類(整数*)
<i>infectedAttachmentAlertName</i>	.1.5.2	脅威名(文字列)



パラメータ名	パラメータのOID	パラメータのタイプと説明
<i>infectedAttachmentAlertOrigin</i>	.1.5.3	脅威を検出したコンポーネントの識別子(整数***)
<i>infectedEmailAttachmentAlertSocket</i>	.1.5.4	メールメッセージの送信元のIPアドレス(文字列)
<i>infectedEmailAttachmentAlertMailFrom</i>	.1.5.5	メールメッセージの送信者(文字列)
<i>infectedEmailAttachmentAlertRcptTo</i>	.1.5.6	メールメッセージの受信者(文字列)
<i>infectedEmailAttachmentAlertMessageId</i>	.1.5.7	メールメッセージのMessage-IDヘッダーの値(文字列)
<i>infectedEmailAttachmentAlertAction</i>	.1.5.8	メールメッセージ全体または感染した添付ファイルに適用されたアクション(整数:1-リパック、2-拒否、3-破棄、4-修復、5-隔離、6-削除)
<i>infectedEmailAttachmentAlertDivert</i>	.1.5.9	メールメッセージの方向(整数:1-受信、2-送信)
<i>infectedEmailAttachmentAlertSrcIp</i>	.1.5.10	接続元のIPアドレス(文字列)
<i>infectedEmailAttachmentAlertSrcPort</i>	.1.5.11	接続元のポート(整数)
<i>infectedEmailAttachmentAlertDstIp</i>	.1.5.12	接続先のIPアドレス(文字列)
<i>infectedEmailAttachmentAlertDstPort</i>	.1.5.13	接続先のポート(整数)
<i>infectedEmailAttachmentAlertSniHost</i>	.1.5.14	接続先のSNI(SSL接続)(文字列)
<i>infectedEmailAttachmentAlertProtocol</i>	.1.5.15	プロトコルの種類(整数:1-SMTP、2-POP3、3-IMAP、4-HTTP)
<i>infectedEmailAttachmentAlertExePath</i>	.1.5.16	接続を確立したプログラムの実行可能パス(文字列)
<i>infectedEmailAttachmentAlertUserName</i>	.1.5.17	接続を確立するプログラムを実行する権限を持つユーザーの名前(文字列)
<i>categoryUrlAlert</i>	.1.6	不要なカテゴリーに属するURLのブロックに関する通知
<i>categoryUrlAlertUrl</i>	.1.6.1	ブロックされたURL(文字列)
<i>categoryUrlAlertCategory</i>	.1.6.2	URLが属するWebリソースカテゴリー(整数**)



パラメータ名	パラメータのOID	パラメータのタイプと説明
<i>categoryUrlAlertOrigin</i>	.1.6.3	脅威を検出したコンポーネントの識別子(整数***)
<i>categoryUrlAlertSrcIp</i>	.1.6.4	接続元のIPアドレス(文字列)
<i>categoryUrlAlertSrcPort</i>	.1.6.5	接続元のポート(整数)
<i>categoryUrlAlertDstIp</i>	.1.6.6	接続先のIPアドレス(文字列)
<i>categoryUrlAlertDstPort</i>	.1.6.7	接続先のポート(整数)
<i>categoryUrlAlertSniHost</i>	.1.6.8	接続先のSNI(SSL接続)(文字列)
<i>categoryUrlAlertExePath</i>	.1.6.9	接続を確立したプログラムの実行可能パス(文字列)
<i>categoryUrlAlertUserName</i>	.1.6.10	接続を確立するプログラムを実行する権限を持つユーザーの名前(文字列)
<i>categoryUrlEmailAttachmentAlert</i>	.1.7	メールメッセージ内の不要なURLの検出に関する通知
<i>categoryUrlEmailAttachmentAlertType</i>	.1.7.1	URLが属するWebリソースカテゴリー(整数**)
<i>categoryUrlEmailAttachmentAlertOrigin</i>	.1.7.2	脅威を検出したコンポーネントの識別子(整数***)
<i>categoryUrlEmailAttachmentAlertSocket</i>	.1.7.3	メールメッセージの送信元のIPアドレス(文字列)
<i>categoryUrlEmailAttachmentAlertMailFrom</i>	.1.7.4	メールメッセージの送信者(文字列)
<i>categoryUrlEmailAttachmentAlertRcptTo</i>	.1.7.5	メールメッセージの受信者(文字列)
<i>categoryUrlEmailAttachmentAlertMessageId</i>	.1.7.6	メールメッセージのMessage-IDヘッダーの値(文字列)
<i>categoryUrlEmailAttachmentAlertAction</i>	.1.7.7	メールメッセージ全体または添付ファイルに適用されたアクション(整数:1-リパック、2-拒否、3-破棄、4-修復、5-隔離、6-削除)
<i>categoryUrlEmailAttachmentAlertDivert</i>	.1.7.8	メールメッセージの方向(整数:1-受信、2-送信)
<i>categoryUrlEmailAttachmentAlertSrcIp</i>	.1.7.9	接続元のIPアドレス(文字列)



パラメータ名	パラメータのOID	パラメータのタイプと説明
<i>categoryUrlEmailAttachmentAlertSrcPort</i>	.1.7.10	接続元のポート(整数)
<i>categoryUrlEmailAttachmentAlertDstIp</i>	.1.7.11	接続先のIPアドレス(文字列)
<i>categoryUrlEmailAttachmentAlertDstPort</i>	.1.7.12	接続先のポート(整数)
<i>categoryUrlEmailAttachmentAlertSniHost</i>	.1.7.13	接続先のSNI(SSL接続)(文字列)
<i>categoryUrlEmailAttachmentAlertProtocol</i>	.1.7.14	プロトコルの種類(整数: 1 - SMTP、2 - POP3、3 - IMAP、4 - HTTP)
<i>categoryUrlEmailAttachmentAlertExePath</i>	.1.7.15	接続を確立したプログラムの実行可能パス(文字列)
<i>categoryUrlEmailAttachmentAlertUserName</i>	.1.7.16	接続を確立するプログラムを実行する権限を持つユーザーの名前(文字列)
<i>spamEmailAlert</i>	.1.8	メールメッセージのスパム認識に関する通知
<i>spamEmailAlertOrigin</i>	.1.8.1	脅威を検出したコンポーネントの識別子(整数 ***)
<i>spamEmailAlertSocket</i>	.1.8.2	メールメッセージの送信元のIPアドレス(文字列)
<i>spamEmailAlertMailFrom</i>	.1.8.3	メールメッセージの送信者(文字列)
<i>spamEmailAlertRcptTo</i>	.1.8.4	メールメッセージの受信者(文字列)
<i>spamEmailAlertMessageId</i>	.1.8.5	メールメッセージのMessage-IDヘッダーの値(文字列)
<i>spamEmailAlertAction</i>	.1.8.6	メールメッセージ全体または添付ファイルに適用されたアクション(整数: 1 - リパック、2 - 拒否、3 - 破棄、4 - 修復、5 - 隔離、6 - 削除)
<i>spamEmailAlertDivert</i>	.1.8.7	メールメッセージの方向(整数: 1 - 受信、2 - 送信)
<i>spamEmailAlertSrcIp</i>	.1.8.8	接続元のIPアドレス(文字列)
<i>spamEmailAlertSrcPort</i>	.1.8.9	接続元のポート(整数)
<i>spamEmailAlertDstIp</i>	.1.8.10	接続先のIPアドレス(文字列)



パラメータ名	パラメータのOID	パラメータのタイプと説明
<i>spamEmailAlertDstPort</i>	.1.8.11	接続先のポート(整数)
<i>spamEmailAlertSniHost</i>	.1.8.12	接続先のSNI(SSL接続)(文字列)
<i>spamEmailAlertProtocol</i>	.1.8.13	プロトコルの種類(整数: 1 - SMTP、2 - POP3、3 - IMAP、4 - HTTP)
<i>spamEmailAlertExePath</i>	.1.8.14	接続を確立したプログラムの実行可能パス(文字列)
<i>spamEmailAlertUserName</i>	.1.8.15	接続を確立するプログラムを実行する権限を持つユーザーの名前(文字列)
<i>blockedConnectionAlert</i>	.1.9	ネットワーク接続のブロックに関する通知
<i>blockedConnectionAlertOrigin</i>	.1.9.1	脅威を検出したコンポーネントの識別子(整数***)
<i>blockedConnectionAlertDivert</i>	.1.9.2	接続の方向(整数: 1 - 受信、2 - 送信)
<i>blockedConnectionAlertSrcIp</i>	.1.9.3	接続元のIPアドレス(文字列)
<i>blockedConnectionAlertSrcPort</i>	.1.9.4	接続元のポート(整数)
<i>blockedConnectionAlertDstIp</i>	.1.9.5	接続先のIPアドレス(文字列)
<i>blockedConnectionAlertDstPort</i>	.1.9.6	接続先のポート(整数)
<i>blockedConnectionAlertSniHost</i>	.1.9.7	接続先のSNI(SSL接続)(文字列)
<i>blockedConnectionAlertProtocol</i>	.1.9.8	プロトコルの種類(整数: 1 - SMTP、2 - POP3、3 - IMAP、4 - HTTP)
<i>blockedConnectionAlertExePath</i>	.1.9.9	接続を確立したプログラムの実行可能パス(文字列)
<i>blockedConnectionAlertUserName</i>	.1.9.10	接続を確立するプログラムを実行する権限を持つユーザーの名前(文字列)
stat	Dr.Web for UNIX File Serversの動作に関する統計	
<i>threatCounters</i>	.2.1	検出された脅威のカウンター
<i>knownVirus</i>	.2.1.1	検出された既知のウイルスの数(カウンター、整数)



パラメータ名	パラメータのOID	パラメータのタイプと説明
<i>suspicious</i>	.2.1.2	検出された疑わしいオブジェクトの数(カウンター、整数)
<i>adware</i>	.2.1.3	検出されたアドウェアの数(カウンター、整数)
<i>dialers</i>	.2.1.4	検出されたダイアラーの数(カウンター、整数)
<i>joke</i>	.2.1.5	検出されたジョークプログラムの数(カウンター、整数)
<i>riskware</i>	.2.1.6	検出されたリスクウェアの数(カウンター、整数)
<i>hacktool</i>	.2.1.7	検出されたハッキングツールの数(カウンター、整数)
scanErrors	.2.2	ファイルのスキャン中に発生したエラーのカウンター
<i>sePathNotAbsolute</i>	.2.2.1	「パスが絶対パスではありません」エラーの発生回数(カウンター、整数)
<i>seFileNotFound</i>	.2.2.2	「ファイルが見つかりません」エラーの発生回数(カウンター、整数)
<i>seFileNotRegular</i>	.2.2.3	「ファイルは通常のファイルではありません」エラーの発生回数(カウンター、整数)
<i>seFileNotBlockDevice</i>	.2.2.4	「ファイルはブロックデバイスではありません」エラーの発生回数(カウンター、整数)
<i>seNameTooLong</i>	.2.2.5	「パスまたはファイル名が長すぎます」エラーの発生回数(カウンター、整数)
<i>seNoAccess</i>	.2.2.6	「パーミッションが拒否されました」エラーの発生回数(カウンター、整数)
<i>seReadError</i>	.2.2.7	「読み取りエラー」の発生回数(カウンター、整数)
<i>seWriteError</i>	.2.2.8	「書き込みエラー」の発生回数(カウンター、整数)
<i>seFileTooLarge</i>	.2.2.9	「ファイルサイズが大きすぎます」エラーの発生回数(カウンター、整数)



パラメータ名	パラメータのOID	パラメータのタイプと説明
<i>seFileBusy</i>	.2.2.10	「ファイルがビジーです」エラーの発生回数(カウンター、整数)
<i>seUnpackingError</i>	.2.2.20	「アンパックエラー」の発生回数(カウンター、整数)
<i>sePasswordProtectd</i>	.2.2.21	「パスワード保護」エラーの発生回数(カウンター、整数)
<i>seArchCrcError</i>	.2.2.22	「アーカイブのCRCエラー」の発生回数(カウンター、整数)
<i>seArchInvalidHeader</i>	.2.2.23	「無効なアーカイブヘッダーです」エラーの発生回数(カウンター、整数)
<i>seArchNoMemory</i>	.2.2.24	「アーカイブを処理するのに十分なメモリがありません」エラーの発生回数(カウンター、整数)
<i>seArchIncomplete</i>	.2.2.25	「不完全なアーカイブ」エラーの発生回数(カウンター、整数)
<i>seCanNotBeCured</i>	.2.2.26	「オブジェクトを修復できません」エラーの発生回数(カウンター、整数)
<i>sePackerLevelLimit</i>	.2.2.30	「パックされたオブジェクトが最大ネストレベルを超えました」エラーの発生回数(カウンター、整数)
<i>seArchiveLevelLimit</i>	.2.2.31	「アーカイブが最大ネストレベルを超えました」エラーの発生回数(カウンター、整数)
<i>seMailLevelLimit</i>	.2.2.32	「メールファイルが最大ネストレベルを超えました」エラーの発生回数(カウンター、整数)
<i>seContainerLevelLimit</i>	.2.2.33	「コンテナが最大ネストレベルを超えました」エラーの発生回数(カウンター、整数)
<i>seCompressionLimit</i>	.2.2.34	「アーカイブの最大圧縮率を超えました」エラーの発生回数(カウンター、整数)
<i>seReportSizeLimit</i>	.2.2.35	「スキャン結果レポートの最大サイズを超えました」エラーの発生回数(カウンター、整数)
<i>seScanTimeout</i>	.2.2.40	「スキャンタイムアウトに達しました」エラーの発生回数(カウンター、整数)



パラメータ名	パラメータのOID	パラメータのタイプと説明
		数)
<i>seEngineCrash</i>	.2.2.41	「Scan Engineのクラッシュが検出されました」エラーの発生回数(カウンター、整数)
<i>seEngineHangup</i>	.2.2.42	「Scan Engineが応答を停止しました」エラーの発生回数(カウンター、整数)
<i>seEngineError</i>	.2.2.44	「Scan Engineの内部エラー」の発生回数(カウンター、整数)
<i>seNoLicense</i>	.2.2.45	「有効なライセンスが見つかりません」エラーの発生回数(カウンター、整数)
<i>seCuringLimitReached</i>	.2.2.47	「修復試行限界に達しました」エラーの発生数(カウンター、整数)
<i>seNonSupportedDisk</i>	.2.2.50	「サポートされていないディスクです」エラーの発生回数(カウンター、整数)
<i>seUnexpectedError</i>	.2.2.100	「予期せぬエラーです」の発生数(カウンター、整数)
<i>scanLoadAverage</i>	.2.3	ファイルスキャン負荷の指標
<i>filesScannedTable</i>	.2.3.1	他のコンポーネントの要求によりスキャンされたファイルの平均数
<i>filesScannedEntry</i>	.2.3.1.1	製品のコンポーネント(テーブル行全体、レコード)
<i>filesScannedIndex</i>	.2.3.1.1.1	コンポーネントのインデックス(識別子、整数***)
<i>filesScannedOrigin</i>	.2.3.1.1.2	コンポーネントの名前
<i>filesScanned1min</i>	.2.3.1.1.3	1秒間にチェックされたファイルの平均(1分間の平均)数(文字列)
<i>filesScanned5min</i>	.2.3.1.1.4	1秒間にチェックされたファイルの平均(5分間の平均)数(文字列)
<i>filesScanned15min</i>	.2.3.1.1.5	1秒間にチェックされたファイルの平均(15分間の平均)数(文字列)
<i>bytesScannedTable</i>	.2.3.2	他のコンポーネントの要求により実行されたスキャンの平均速度(1秒あたりのバイト数)



パラメータ名	パラメータのOID	パラメータのタイプと説明
bytesScannedEntry	.2.3.2.1	製品のコンポーネント(テーブル行全体、レコード)
bytesScannedIndex	.2.3.2.1.1	コンポーネントのインデックス(識別子、整数***)
bytesScannedOrigin	.2.3.2.1.2	コンポーネントの名前
bytesScanned1min	.2.3.2.1.3	1秒間にスキャンされた平均バイト数(1分間の平均)(文字列)
bytesScanned5min	.2.3.2.1.4	1秒間にスキャンされた平均バイト数(5分間の平均)(文字列)
bytesScanned15min	.2.3.2.1.5	1秒間にスキャンされた平均バイト数(15分間の平均)(文字列)
<i>cacheHitFilesTable</i>	.2.3.3	コンポーネントの要求によりキャッシュから取得されたスキャンレポートの平均数
cacheHitFilesEntry	.2.3.3.1	製品のコンポーネント(テーブル行全体、レコード)
cacheHitFilesIndex	.2.3.3.1.1	コンポーネントのインデックス(識別子、整数***)
cacheHitFilesOrigin	.2.3.3.1.2	コンポーネントの名前
cacheHitFiles1min	.2.3.3.1.3	1秒間にキャッシュから取得されたレポートの平均(1分間の平均)数(文字列)
cacheHitFiles5min	.2.3.3.1.4	1秒間にキャッシュから取得されたレポートの平均(5分間の平均)数(文字列)
cacheHitFiles15min	.2.3.3.1.5	1秒間にキャッシュから取得されたレポートの平均(15分間の平均)数(文字列)
<i>errorsTable</i>	.2.3.4	コンポーネントの要求により実行されたスキャン中の平均エラー数
errorsEntry	.2.3.4.1	製品のコンポーネント(テーブル行全体、レコード)
errorsIndex	.2.3.4.1.1	コンポーネントのインデックス(識別子、整数***)
errorsOrigin	.2.3.4.1.2	コンポーネントの名前



パラメータ名	パラメータのOID	パラメータのタイプと説明
errors1min	.2.3.4.1.3	1秒間のスキャンエラーの平均（1分間の平均）数（文字列）
errors5min	.2.3.4.1.4	1秒間のスキャンエラーの平均（5分間の平均）数（文字列）
errors15min	.2.3.4.1.5	1秒間のスキャンエラーの平均（15分間の平均）数（文字列）
net	.2.4	ネットワークアクティビティの統計
markedAsSpam	.2.4.1	スパムとしてマークされたメールメッセージの数（カウンター、整数）
blockedInfectionSource	.2.4.101	「感染源」カテゴリーに属するブロックされたURLの数（カウンター、整数）
blockedNotRecommended	.2.4.102	「非推奨」カテゴリーに属するブロックされたURLの数（カウンター、整数）
blockedAdultContent	.2.4.103	「アダルトコンテンツ」カテゴリーに属するブロックされたURLの数（カウンター、整数）
blockedViolence	.2.4.104	「暴力」カテゴリーに属するブロックされたURLの数（カウンター、整数）
blockedWeapons	.2.4.105	「武器」カテゴリーに属するブロックされたURLの数（カウンター、整数）
blockedGambling	.2.4.106	「ギャンブル」カテゴリーに属するブロックされたURLの数（カウンター、整数）
blockedDrugs	.2.4.107	「麻薬」カテゴリーに属するブロックされたURLの数（カウンター、整数）
blockedObsceneLanguage	.2.4.108	「卑猥な表現」カテゴリーに属するブロックされたURLの数（カウンター、整数）
blockedChats	.2.4.109	「チャット」カテゴリーに属するブロックされたURLの数（カウンター、整数）
blockedTerrorism	.2.4.110	「テロリズム」カテゴリーに属するブロックされたURLの数（カウンター、整数）
blockedFreeEmail	.2.4.111	「無料メールサービス」カテゴリーに属するブロックされたURLの数（カウ



パラメータ名	パラメータのOID	パラメータのタイプと説明
		ンター、整数)
<i>blockedSocialNetworks</i>	.2.4.112	「ソーシャルネットワーク」カテゴリーに属するブロックされたURLの数(カウンター、整数)
<i>blockedOwnersNotice</i>	.2.4.113	「著作権者の申し立て」カテゴリーに属するブロックされたURLの数(カウンター、整数)
<i>blockedOnlineGames</i>	.2.4.114	「オンラインゲーム」カテゴリーに属するブロックされたURLの数(カウンター、整数)
<i>blockedAnonymizers</i>	.2.4.115	「アノニマイザー」カテゴリーに属するブロックされたURLの数(カウンター、整数)
<i>blockedCryptocurrencyMiningPools</i>	.2.4.116	「仮想通貨マイニングプール」カテゴリーに属するブロックされたURLの数(カウンター、整数)
<i>blockedJobs</i>	.2.4.117	「求人検索サイト」カテゴリーに属するブロックされたURLの数(カウンター、整数)
<i>blockedBlackList</i>	.2.4.120	ユーザーのブラックリストからブロックされたURLの数(カウンター、整数)
info	Dr.Web for UNIX File Serversの現在の状態に関する情報	
components	.3.1	Dr.Web for UNIX File Serversコンポーネントのステータス
<i>configd</i>	.3.1.1	drweb-configd コンポーネントデータ
configdState	.3.1.1.1	コンポーネントの現在の状態(整数****)
configdExitCode	.3.1.1.2	前回の終了コード(エラーカタログのコードに対応する整数)
configdExitTime	.3.1.1.3	前回の終了時刻(<i>UNIX時間</i>)
configdInstalledApps	.3.1.1.101	インストールされたコンポーネントのリスト
configdAppEntry	.3.1.1.101.1	インストールされているコンポーネントに関する情報(テーブル行全体、レコード)



パラメータ名	パラメータのOID	パラメータのタイプと説明
configdAppIndex	.3.1.1.101.1.1	インストールされているコンポーネントのインデックス(序数)(整数)
configdAppName	.3.1.1.101.1.2	インストールされているコンポーネントの名前(文字列)
configdAppExePath	.3.1.1.101.1.3	コンポーネントの実行ファイルへのパス(文字列)
configdAppInstallTime	.3.1.1.101.1.4	コンポーネントがインストールされた時刻(<i>UNIX時間</i>)
configdAppIniSection	.3.1.1.101.1.5	設定ファイルにあるコンポーネントのパラメータを含むセクションの名前
<i>scanEngine</i>	.3.1.2	drweb-se コンポーネントデータ
scanEngineState	.3.1.2.1	コンポーネントの現在の状態(整数****)
scanEngineExitCode	.3.1.2.2	前回の終了コード(エラーカタログのコードに対応する整数)
scanEngineExitTime	.3.1.2.3	前回の終了時刻(<i>UNIX時間</i>)
scanEngineStatus	.3.1.2.101	Dr.Web Virus-Finding Engineの現在の状態(整数)
scanEngineVersion	.3.1.2.102	Dr.Web Virus-Finding Engineのバージョン(文字列)
scanEngineVirusRecords	.3.1.2.103	ウイルスレコードの数(整数)
scanEngineMaxForks	.3.1.2.104	スキャン対象の子プロセスの最大数(整数)
scanEngineQueues	.3.1.2.105	スキャンタスクのキュー
scanEngineQueuesLow	.3.1.2.105.1	優先度の低いタスクのキュー
scanEngineQueueLowOut	.3.1.2.105.1.1	キューから出て処理に転送された優先度の低いタスクの数(カウンター、整数)
scanEngineQueueLowSize	.3.1.2.105.1.2	キュー内で処理待ちになっている優先度の低いタスクの数(カウンター、整数)
scanEngineQueuesMedium	.3.1.2.105.2	通常優先度のタスクのキュー
scanEngineQueueMediumOut	.3.1.2.105.2.1	キューから出て処理に転送された通常優先度のタスクの数(カウンター、整数))



パラメータ名	パラメータのOID	パラメータのタイプと説明
scanEngineQueueMediumSize	.3.1.2.105.2.2	キュー内で処理待ちになっている通常優先度のタスクの数(カウンター、整数)
scanEngineQueuesHigh	.3.1.2.105.3	優先度の高いタスクのキュー
scanEngineQueueHighOut	.3.1.2.105.3.1	キューから出て処理に転送された優先度の高いタスクの数(カウンター、整数)
scanEngineQueueHighSize	.3.1.2.105.3.2	キュー内で処理待ちになっている優先度の高いタスクの数(カウンター、整数)
scanEngineVirusBasesTable	.3.1.2.106	ウイルスデータベースのリスト。
scanEngineVirusBasesEntry	.3.1.2.106.1	ウイルスデータベースに関する情報(テーブル行全体、レコード)
scanEngineVirusBaseIndex	.3.1.2.106.1.1	ウイルスデータベースのインデックス(整数)
scanEngineVirusBasePath	.3.1.2.106.1.2	ウイルスデータベースディレクトリへのパス(文字列)
scanEngineVirusBaseRecords	.3.1.2.106.1.3	ウイルスデータベース内のレコード数(整数)
scanEngineVirusBaseVersion	.3.1.2.106.1.4	ウイルスデータベースのバージョン(整数)
scanEngineVirusBaseTimestamp	.3.1.2.106.1.5	ウイルスデータベースのタイムスタンプ(<i>UNIX時間</i>)
scanEngineVirusBaseMD5	.3.1.2.106.1.6	MD5チェックサム(文字列)
scanEngineVirusBaseLoadResult	.3.1.2.106.1.7	このウイルスデータベースのダウンロード結果(文字列)
scanEngineQueuesTab	.3.1.2.107	スキャンタスクキューのリスト
scanEngineQueueEntry	.3.1.2.107.1	キューに関する情報(テーブル行全体、レコード)
scanEngineQueueIndex	.3.1.2.107.1.1	キューのインデックス(序数)(整数)
scanEngineQueueName	.3.1.2.107.1.2	キューの名前(文字列)
scanEngineQueueOut	.3.1.2.107.1.3	キューから出て処理に転送されたタスクの数(カウンター、整数)



パラメータ名	パラメータのOID	パラメータのタイプと説明
scanEngineQueueSize	.3.1.2.107.1.4	キュー内で処理待ちになっているタスクの数(カウンター、整数)
<i>fileCheck</i>	.3.1.3	drweb-filecheck コンポーネントデータ
fileCheckState	.3.1.3.1	コンポーネントの現在の状態(整数****)
fileCheckExitCode	.3.1.3.2	前回の終了コード(エラーカタログのコードに対応する整数)
fileCheckExitTime	.3.1.3.3	前回の終了時刻(<i>UNIX時間</i>)
fileCheckScannedFiles	.3.1.3.101	スキャン済みファイル数(カウンター、整数)
fileCheckScannedBytes	.3.1.3.102	スキャン済みバイト数(カウンター、整数)
fileCheckCacheHitFiles	.3.1.3.103	キャッシュから取得したスキャンレポートの数(カウンター、整数)
fileCheckScanErrors	.3.1.3.104	Scan Engineでのエラーの発生回数(カウンター、整数)
fileCheckScanStat	.3.1.3.105	クライアントのリスト
fileCheckClientEntry	.3.1.3.105.1	クライアントに関する情報(テーブル行全体、レコード)
fileCheckClientIndex	.3.1.3.105.1.1	クライアントのインデックス(序数)(整数)
fileCheckClientName	.3.1.3.105.1.2	クライアントコンポーネントの名前(文字列)
fileCheckClientScannedFiles	.3.1.3.105.1.3	このクライアントでスキャンされたファイル数(カウンター、整数)
fileCheckClientScannedBytes	.3.1.3.105.1.4	このクライアントでスキャンされたバイト数(カウンター、整数)
fileCheckClientCacheHitFiles	.3.1.3.105.1.5	このクライアントのキャッシュから取得したスキャンレポートの数(カウンター、整数)
fileCheckClientScanErrors	.3.1.3.105.1.6	このクライアントで動作しているときにScan Engineで発生したエラーの数(カウンター、整数)
<i>update</i>	.3.1.4	drweb-update コンポーネントデータ



パラメータ名	パラメータのOID	パラメータのタイプと説明
updateState	.3.1.4.1	コンポーネントの現在の状態(整数****)
updateExitCode	.3.1.4.2	前回の終了コード(エラーカタログのコードに対応する整数)
updateExitTime	.3.1.4.3	前回の終了時刻(UNIX時間)
updateBytesSent	.3.1.4.101	送信したバイト数(カウンター、整数)
updateBytesReceived	.3.1.4.102	受信したバイト数(カウンター、整数)
<i>esagent</i>	.3.1.5	drweb-esagent コンポーネントデータ
esagentState	.3.1.5.1	コンポーネントの現在の状態(整数****)
esagentExitCode	.3.1.5.2	前回の終了コード(エラーカタログのコードに対応する整数)
esagentExitTime	.3.1.5.3	前回の終了時刻(UNIX時間)
esagentWorkStatus	.3.1.5.101	コンポーネントの現在の動作モード(整数: 1 - スタンドアロンモード、2 - 接続中、3 - 接続待ち、4 - 接続承認済み)
esagentIsConnected	.3.1.5.102	サーバーに接続されているかどうか(整数、0 - いいえ、1 - はい)
esagentServer	.3.1.5.103	使用されている集中管理サーバーのアドレス(文字列)
<i>netcheck</i>	.3.1.6	drweb-netcheck コンポーネントデータ
netcheckState	.3.1.6.1	コンポーネントの現在の状態(整数****)
netcheckExitCode	.3.1.6.2	前回の終了コード(エラーカタログのコードに対応する整数)
netcheckExitTime	.3.1.6.3	前回の終了時刻(UNIX時間)
netcheckLocalSeForks	.3.1.6.101	ローカルで利用可能なScan Engineプロセスの数(整数)
netcheckRemoteSeForks	.3.1.6.102	リモートで利用可能なScan Engineプロセスの数(整数)



パラメータ名	パラメータのOID	パラメータのタイプと説明
netcheckLocalFilesScanned	.3.1.6.103	ローカルでスキャンされたファイルの数(カウンター、整数)
netcheckNetworkFilesScanned	.3.1.6.104	リモートスキャンでスキャンされたファイルの数(カウンター、整数)
netcheckLocalBytesScanned	.3.1.6.105	ローカルでスキャンされたバイト数(カウンター、整数)
netcheckNetworkBytesScanned	.3.1.6.106	リモートスキャンでスキャンされたバイト数(カウンター、整数)
netcheckLocalBytesIn	.3.1.6.107	ローカルクライアントから受信したバイト数(カウンター、整数)
netcheckLocalBytesOut	.3.1.6.108	ローカルクライアントに送信したバイト数(カウンター、整数)
netcheckNetworkBytesIn	.3.1.6.109	リモートホストから受信したバイト数(カウンター、整数)
netcheckNetworkBytesOut	.3.1.6.110	リモートホストに送信したバイト数(カウンター、整数)
netcheckLocalScanErrors	.3.1.6.111	ローカルのScan Engineプロセスでのエラーの発生回数(カウンター、整数)
netcheckNetworkScanErrors	.3.1.6.112	リモートのScan Engineプロセスでのエラーの発生回数(カウンター、整数)
<i>httpd</i>	.3.1.7	drweb-httpd コンポーネントデータ
httpdState	.3.1.7.1	コンポーネントの現在の状態(整数****)
httpdExitCode	.3.1.7.2	前回の終了コード(エラーカタログのコードに対応する整数)
httpdExitTime	.3.1.7.3	前回の終了時刻(<i>UNIX時間</i>)
<i>snmpd</i>	.3.1.8	drweb-snmpd コンポーネントデータ
snmpdState	.3.1.8.1	コンポーネントの現在の状態(整数****)
snmpdExitCode	.3.1.8.2	前回の終了コード(エラーカタログのコードに対応する整数)
snmpdExitTime	.3.1.8.3	前回の終了時刻(<i>UNIX時間</i>)



パラメータ名	パラメータのOID	パラメータのタイプと説明
<i>clamd</i>	.3.1.20	drweb-clamd コンポーネントデータ
clamdState	.3.1.20.1	コンポーネントの現在の状態(整数****)
clamdExitCode	.3.1.20.2	前回の終了コード(エラーカタログのコードに対応する整数)
clamdExitTime	.3.1.20.3	前回の終了時刻(<i>UNIX時間</i>)
<i>icapd</i>	.3.1.21	drweb-icapd コンポーネントデータ
icapdState	.3.1.21.1	コンポーネントの現在の状態(整数****)
icapdExitCode	.3.1.21.2	前回の終了コード(エラーカタログのコードに対応する整数)
icapdExitTime	.3.1.21.3	前回の終了時刻(<i>UNIX時間</i>)
icapdConnectionsIn	.3.1.21.101	承認された受信接続の数(カウンター、整数)
icapdConnectionsCount	.3.1.21.102	現在開いている接続の数(カウンター、整数)
icapdOptions	.3.1.21.103	<i>OPTIONS</i> 要求の数(カウンター、整数)
icapdReqmod	.3.1.21.104	<i>REQMOD</i> 要求の数(カウンター、整数)
icapdRespmo	.3.1.21.105	<i>RESPMOD</i> 要求の数(カウンター、整数)
icapdBad	.3.1.21.106	無効なリクエストの数(カウンター、整数)
<i>smbspider</i>	.3.1.40	drweb-smbspider-daemon コンポーネントデータ
smbspiderState	.3.1.40.1	コンポーネントの現在の状態(整数****)
smbspiderExitCode	.3.1.40.2	前回の終了コード(エラーカタログのコードに対応する整数)
smbspiderExitTime	.3.1.40.3	前回の終了時刻(<i>UNIX時間</i>)
smbspiderConnectionsIn	.3.1.40.101	開かれた接続の合計数(カウンター、整数)



パラメータ名	パラメータのOID	パラメータのタイプと説明
smbspiderConnectionsCount	.3.1.40.102	現在開いている接続の数(カウンター、整数)
smbspiderShareTable	.3.1.40.103	保護された Samba 共有リソースに関する統計
smbspiderShareEntry	.3.1.40.103.1	保護されている Samba 共有リソースに関する情報(テーブル行全体、レコード)
smbspiderShareIndex	.3.1.40.103.1.1	保護された Samba 共有リソースのインデックス(序数)(整数)
smbspiderSharePath	.3.1.40.103.1.2	保護された Samba 共有リソースへのパス(文字列)
smbspiderShareConnectionsIn	.3.1.40.103.1.3	開かれた接続の合計数(カウンター、整数)
smbspiderShareConnectionsCount	.3.1.40.103.1.4	現在開いている接続の数(カウンター、整数)
<i>gated</i>	.3.1.41	drweb-gated コンポーネントデータ
gatedState	.3.1.41.1	コンポーネントの現在の状態(整数****)
gatedExitCode	.3.1.41.2	前回の終了コード(エラーカタログのコードに対応する整数)
gatedExitTime	.3.1.41.3	前回の終了時刻(<i>UNIX時間</i>)
gatedInterceptedIn	.3.1.41.101	モニタリングした接続の数(カウンター、整数)
gatedInterceptedCount	.3.1.41.102	現在モニタリングされている接続の数(カウンター、整数)
<i>maild</i>	.3.1.42	drweb-maild コンポーネントデータ
maildState	.3.1.42.1	コンポーネントの現在の状態(整数****)
maildExitCode	.3.1.42.2	前回の終了コード(エラーカタログのコードに対応する整数)
maildExitTime	.3.1.42.3	前回の終了時刻(<i>UNIX時間</i>)
maildStat	.3.1.42.4	drweb-maild コンポーネントによる処理の統計
maildStatNative	.3.1.42.4.1	コンポーネントの内部インターフェース drweb-maild を介したメールス



パラメータ名	パラメータのOID	パラメータのタイプと説明
		キャンの統計（傍受したSMTP、POP3、IMAP接続のスクャン中にSpIDer Gateが受信したメッセージ）
maildStatNativePassed	.3.1.42.4.1.1	受信できなかったメッセージの数（カウンター、整数）
maildStatNativeRepacked	.3.1.42.4.1.2	再パッケージ化されたメッセージの数（カウンター、整数）
maildStatNativeRejected	.3.1.42.4.1.3	拒否されたメッセージの数（カウンター、整数）
maildStatNativeFailed	.3.1.42.4.1.4	メッセージスクャンエラーの数（カウンター、整数）
maildStatNativeQueueSize	.3.1.42.4.1.5	キューライン、つまりインターフェースを介してのスクャンを待機しているファイルの数（整数）
maildStatMilter	.3.1.42.4.2	drweb-maild コンポーネントのコンポーネントインターフェース <i>Milter</i> を介したメールスクャンの統計
maildStatMilterPassed	.3.1.42.4.2.1	受信できなかったメッセージの数（カウンター、整数）
maildStatMilterRepacked	.3.1.42.4.2.2	再パッケージ化されたメッセージの数（カウンター、整数）
maildStatMilterRejected	.3.1.42.4.2.3	拒否されたメッセージの数（カウンター、整数）
maildStatMilterFailed	.3.1.42.4.2.4	メッセージスクャンエラーの数（カウンター、整数）
maildStatMilterQueueSize	.3.1.42.4.2.5	キューライン、つまりインターフェースを介してのスクャンを待機しているファイルの数（整数）
maildStatSpamc	.3.1.42.4.3	drweb-maild コンポーネントのコンポーネントインターフェース <i>Spamc</i> を介したメールスクャンの統計
maildStatSpamcPassed	.3.1.42.4.3.1	受信できなかったメッセージの数（カウンター、整数）
maildStatSpamcRepacked	.3.1.42.4.3.2	再パッケージ化されたメッセージの数（カウンター、整数）
maildStatSpamcRejected	.3.1.42.4.3.3	拒否されたメッセージの数（カウンター、整数）



パラメータ名	パラメータのOID	パラメータのタイプと説明
maildStatSpamcFailed	.3.1.42.4.3.4	メッセージスキャンエラーの数(カウンター、整数)
maildStatSpamcQueueSize	.3.1.42.4.3.5	キューライン、つまりインターフェースを介してのスキャンを待機しているファイルの数(整数)
maildStatRspamc	.3.1.42.4.4	drweb-maild コンポーネントのコンポーネントインターフェース <i>Rspamd</i> を介したメールスキャンの統計
maildStatRspamcPassed	.3.1.42.4.4.1	受信できなかったメッセージの数(カウンター、整数)
maildStatRspamcRepacked	.3.1.42.4.4.2	再パッケージ化されたメッセージの数(カウンター、整数)
maildStatRspamcRejected	.3.1.42.4.4.3	拒否されたメッセージの数(カウンター、整数)
maildStatRspamcFailed	.3.1.42.4.4.4	メッセージスキャンエラーの数(カウンター、整数)
maildStatRspamcQueueSize	.3.1.42.4.4.5	キューライン、つまりインターフェースを介してのスキャンを待機しているファイルの数(整数)
<i>lookupd</i>	.3.1.43	drweb-lookupd コンポーネントデータ
lookupdState	.3.1.43.1	コンポーネントの現在の状態(整数****)
lookupdExitCode	.3.1.43.2	前回の終了コード(エラーカタログのコードに対応する整数)
lookupdExitTime	.3.1.43.3	前回の終了時刻(<i>UNIX時間</i>)
<i>antispam</i>	.3.1.44	drweb-ase コンポーネントに関するデータ
antispamState	.3.1.44.1	コンポーネントの現在の状態(整数****)
antispamExitCode	.3.1.44.2	前回の終了コード(エラーカタログのコードに対応する整数)
antispamExitTime	.3.1.44.3	前回の終了時刻(<i>UNIX時間</i>)
<i>cloudd</i>	.3.1.50	drweb-cloudd コンポーネントデータ



パラメータ名	パラメータのOID	パラメータのタイプと説明
clouddState	.3.1.50.1	コンポーネントの現在の状態(整数****)
clouddExitCode	.3.1.50.2	前回の終了コード(エラーカタログのコードに対応する整数)
clouddExitTime	.3.1.50.3	前回の終了時刻(<i>UNIX時間</i>)
<i>vpnd</i>	.3.1.51	drweb-vpnd コンポーネントデータ
vpndState	.3.1.51.1	コンポーネントの現在の状態(整数****)
vpndExitCode	.3.1.51.2	前回の終了コード(エラーカタログのコードに対応する整数)
vpndExitTime	.3.1.51.3	前回の終了時刻(<i>UNIX時間</i>)
vpndWorkStatus	.3.1.51.101	コンポーネントの現在の動作モード(整数:0 - オフ、1 - サーバー、2 - クライアント)
vpndConnectionState	.3.1.51.102	確立された接続のステータス(整数:0 - ステータス未設定、1 - 接続中、2 - 接続済み、3 - エラー、4 - NATの設定中、5 - 保護トンネルの作成中)
vpndNetworkName	.3.1.51.103	作成したパーソナルネットワークの名前(文字列)
<i>meshd</i>	.3.1.52	drweb-meshd コンポーネントデータ
meshdState	.3.1.52.1	コンポーネントの現在の状態(整数****)
meshdExitCode	.3.1.52.2	前回の終了コード(エラーカタログのコードに対応する整数)
meshdExitTime	.3.1.52.3	前回の終了時刻(<i>UNIX時間</i>)
<i>lotus</i>	.3.1.60	drweb-lotus コンポーネントデータ
lotusState	.3.1.60.1	コンポーネントの現在の状態(整数****)
lotusExitCode	.3.1.60.2	前回の終了コード(エラーカタログのコードに対応する整数)
lotusExitTime	.3.1.60.3	前回の終了時刻(<i>UNIX時間</i>)



パラメータ名	パラメータのOID	パラメータのタイプと説明
<i>macgui</i>	.3.1.100	drweb-gui (macOS 用)コンポーネントデータ
macguiState	.3.1.100.1	コンポーネントの現在の状態(整数****)
macguiExitCode	.3.1.100.2	前回の終了コード(エラーカタログのコードに対応する整数)
macguiExitTime	.3.1.100.3	前回の終了時刻(<i>UNIX時間</i>)
<i>macspider</i>	.3.1.102	drweb-spider (macOS 用)コンポーネントデータ
macspiderState	.3.1.102.1	コンポーネントの現在の状態(整数****)
macspiderExitCode	.3.1.102.2	前回の終了コード(エラーカタログのコードに対応する整数)
macspiderExitTime	.3.1.102.3	前回の終了時刻(<i>UNIX時間</i>)
macspiderWorkStatus	.3.1.102.101	コンポーネントの現在の動作モード(整数:0 - 未設定、1 - 読み込み中、2 - 実行中)
<i>macfirewall</i>	.3.1.103	drweb-firewall (macOS 用)コンポーネントデータ
macfirewallState	.3.1.103.1	コンポーネントの現在の状態(整数****)
macfirewallExitCode	.3.1.103.2	前回の終了コード(エラーカタログのコードに対応する整数)
macfirewallExitTime	.3.1.103.3	前回の終了時刻(<i>UNIX時間</i>)
<i>linuxgui</i>	.3.1.200	drweb-gui (GNU/ Linux の場合)コンポーネントデータ
linuxguiState	.3.1.200.1	コンポーネントの現在の状態(整数****)
linuxguiExitCode	.3.1.200.2	前回の終了コード(エラーカタログのコードに対応する整数)
linuxguiExitTime	.3.1.200.3	前回の終了時刻(<i>UNIX時間</i>)
<i>linuxspider</i>	.3.1.201	drweb-spider (GNU/ Linux の場合)コンポーネントデータ
linuxspiderState	.3.1.201.1	コンポーネントの現在の状態(整数****)



パラメータ名	パラメータのOID	パラメータのタイプと説明
linuxspiderExitCode	.3.1.201.2	前回の終了コード(エラーカタログのコードに対応する整数)
linuxspiderExitTime	.3.1.201.3	前回の終了時刻(<i>UNIX時間</i>)
linuxspiderWorkStatus	.3.1.201.101	コンポーネントの現在の動作モード(整数:0 - 未設定、1 - 読み込み中、2 - fanotify 経由で実行中、3 - LKM経由で実行中)
<i>linuxnss</i>	.3.1.202	drweb-nss (GNU/Linux の場合)コンポーネントデータ
linuxnssState	.3.1.202.1	コンポーネントの現在の状態(整数****)
linuxnssExitCode	.3.1.202.2	前回の終了コード(エラーカタログのコードに対応する整数)
linuxnssExitTime	.3.1.202.3	前回の終了時刻(<i>UNIX時間</i>)
linuxnssScannedFiles	.3.1.202.101	スキャン済みファイル数(カウンター、整数)
linuxnssScannedBytes	.3.1.202.102	スキャン済みバイト数(カウンター、整数)
linuxnssScanErrors	.3.1.202.103	スキャンエラーの発生回数(カウンター、整数)
<i>linuxfirewall</i>	.3.1.203	drweb-firewall (GNU/Linux の場合)コンポーネントデータ
linuxfirewallState	.3.1.203.1	コンポーネントの現在の状態(整数****)
linuxfirewallExitCode	.3.1.203.2	前回の終了コード(エラーカタログのコードに対応する整数)
linuxfirewallExitTime	.3.1.203.3	前回の終了時刻(<i>UNIX時間</i>)
<i>ctl</i>	.3.1.300	drweb-ctl コンポーネントデータ
ctlState	.3.1.300.1	コンポーネントの現在の状態(整数****)
ctlExitCode	.3.1.300.2	前回の終了コード(エラーカタログのコードに対応する整数)
ctlExitTime	.3.1.300.3	前回の終了時刻(<i>UNIX時間</i>)
license	.3.2	ライセンスのステータス



パラメータ名	パラメータのOID	パラメータのタイプと説明
<i>licenseEsMode</i>	.3.2.1	ライセンスは集中管理サーバーによって許可されました(整数:0 - いいえ、1 - はい)
<i>licenseNumber</i>	.3.2.2	ライセンス番号(整数)
<i>licenseOwner</i>	.3.2.3	ライセンスの所有者(文字列)
<i>licenseActivated</i>	.3.2.4	ライセンスを有効化した日(<i>UNIX時間</i>)
<i>licenseExpires</i>	.3.2.5	ライセンス有効期限(<i>UNIX時間</i>)

*) 脅威のタイプ:

コード	脅威の種類
1	既知のウイルス(<i>known virus</i>)
2	疑わしいオブジェクト(<i>suspicious</i>)
3	アドウェア(<i>adware</i>)
4	ダイヤラー(<i>dialer</i>)
5	ジョークプログラム(<i>joke program</i>)
6	リスクウェア(<i>riskware</i>)
7	ハッキングツール(<i>hacktool</i>)

**) URLのカテゴリ:

コード	脅威の種類
1	感染源(<i>infectionSource</i>)
2	非推奨(<i>notRecommended</i>)
3	アダルトコンテンツ(<i>adultContent</i>)
4	暴力(<i>violence</i>)
5	武器(<i>weapons</i>)
6	ギャンブル(<i>gambling</i>)
7	麻薬(<i>drugs</i>)



コード	脅威の種類
8	卑猥な表現など (<i>obsceneLanguage</i>)
9	チャット (<i>chats</i>)
10	テロリズム (<i>terrorism</i>)
11	無料メール (<i>freeEmail</i>)
12	ソーシャルネットワーク (<i>socialNetworks</i>)
13	著作権者からの申し立てによって登録されたURL (<i>ownerNotice</i>)
14	オンラインゲーム (<i>onlineGames</i>)
15	アノマイザー (<i>anonymizers</i>)
16	暗号通貨マイニングプール (<i>cryptocurrencyMiningPools</i>)
17	求人検索サイト (<i>Jobs</i>)
20	ブラックリストに追加済み (<i>blackList</i>)

***) Dr.Webコンポーネントのコード:

コード	コンポーネント
1	Dr.Web ConfigD (drweb-configd)
2	Dr.Web Scanning Engine (drweb-se)
3	Dr.Web File Checker (drweb-filecheck)
4	Dr.Web Updater (drweb-update)
5	Dr.Web ES Agent (drweb-esagent)
6	Dr.Web Network Checker (drweb-netcheck)
7	Dr.Web HTTPD (drweb-httpd)
8	Dr.Web SNMPD (drweb-snmpd)
20	Dr.Web ClamD (drweb-clamd)
21	Dr.Web ICAPD (drweb-icapd)
40	SpIDer Guard for SMB (drweb-smbspider-daemon)
41	SpIDer Gate (drweb-gated)



コード	コンポーネント
42	Dr.Web MailD (drweb-maild)
43	Dr.Web LookupD (drweb-lookupd)
50	Dr.Web CloudD (drweb-cloudd)
51	Dr.Web VPND (drweb-vpnd)
52	Dr.Web MeshD (drweb-meshd)
60	Dr.Web for Lotus
100	drweb-gui for macOS
102	SpIDer Guard for macOS for macOS
103	Dr.Web Firewall for macOS for macOS
200	drweb-gui for GNU/Linux
201	SpIDer Guard (drweb-spider)
202	SpIDer Guard for NSS (drweb-nss)
203	Dr.Web Firewall for Linux(drweb-firewall) for GNU/Linux
300	Dr.Web Ctl (drweb-ctl)
400	Enterprise scanner (Dr.Web for UNIX File Serversのコンポーネントではありません)

****) コンポーネントの状態:

コード	ステータス
0	インストールされていません
1	インストールされているが開始されていない
2	起動中
3	実行中
4	終了中

変数の値を直接取得するには、**snmpwalk**ユーティリティを使用します。

```
$ snmpwalk -Os -c <community> -v <SNMP version> <host address> <OID>
```



たとえば、ローカルホストで検出された脅威に関する統計を取得するには、次のコマンドを使用します (Dr.Web SNMPDの設定がデフォルト値に設定されている場合)。

```
$ snmpwalk -Os -c public -v 2c 127.0.0.1 .1.3.6.1.4.1.29690.2.2.1
```



Dr.Web MeshD

Dr.Web MeshDは、「ローカルクラウド」にインストールされたDr.Web for UNIX File Serversを持つホストを含むエージェントです。この製品は、ホストをインストール済みのDr.Web for UNIX製品に接続します。このクラウドを利用すると、次のタスクを解決できます。

- 複数のクラウドホストによる他のファイルスキャンサービスの提供（スキャンコアサービス）。
- ウイルスデータベースの更新をクラウドホスト間で配布する。

ホストをインストール済みのDr.Web for UNIX製品に接続するには、Dr.Web MeshDコンポーネントをすべてのホストにインストールする必要があります。コンポーネントによってクラウドのホストが組み込まれます。クラウド内のホストの権限とホストが使用するクラウド機能は、Dr.Web MeshD設定で簡単に設定できます。

データは、保護されたSSHチャンネルを介して他のクラウドホストと共有されます。

動作原理

Dr.Web MeshDは、Dr.Web for UNIX File Serversがインストールされているホストと他のクラウドホスト間のインタラクションを調整します。

- [接続タイプ](#)
- [動作モード](#)
- [サービス](#)

接続タイプ

Dr.Web MeshDでは、次の接続タイプを使用します。

- **クライアント（サービス）** - Dr.Web MeshDが他のクラウドホストに接続するために使用されます。これらのホストは、指定したホストによって提供されるサービスのクライアントです。



ホスト上で動作し、同じホスト上で動作するDr.Web MeshDを介してクラウド提供のサービスにアクセスするDr.Web for UNIX File Serversのコンポーネントは、ローカルのUNIXソケットを介してクライアントに接続します。その場合、クライアント接続は使用されません。

- **パートナー（ピアツーピア）** - ピア（サービス内）パートナークラウドホストとのインタラクションのためにDr.Web MeshDによって使用されます。通常、このような接続は、クラウドとやり取りするときの負荷の拡張と分散の他、クラウドホストの同期に使用されます。
- **アップリンク** - このホスト（クライアント）をクラウドホスト（サービスプロバイダー）に接続する際にDr.Web MeshDによって使用されます（スキャンのためのファイル転送など）。

使用する3つの種類の接続はすべて、それぞれのクラウドサービスに対して個別に設定されます。さらに同じホストを、サービス内でクライアントの要求（最新の更新を提供するなど）を処理するサーバーとして、および別のサービス内（リモートファイルスキャンなど）のクライアントとして設定できます。

クラウド内では、ホストは安全なSSHプロトコルを介して承認済みのインタラクションを実行します。つまり、ホスト間通信のすべての側面が常に相互認証されます。認証には、[RFC 4251](#)に従ってホストキーが使用されます。ローカルコンポーネントからのクライアント接続は常に信頼済みと見なされます。



動作モード

Dr.Web MeshDは、デーモンモードで動作し、ローカルホストにある他のDr.Web for UNIX File Serversコンポーネントからの要求で実行できます。Dr.Web MeshDがクライアント接続を提供するように設定されており(つまり、**ListenAddress**パラメータが空でない場合)、少なくとも1つのサービスがアクティブ化されている場合、Dr.Web MeshDはデーモンとして起動し、クライアントからの接続を待機します。また、Dr.Web MeshDは、リクエストに応じて、たとえば次の**コマンド**を実行するときに、ローカルホストで有効化できます。

```
$ drweb-ctl update --local-cloud
```

Dr.Web MeshDがクライアント接続を処理するように設定されておらず(**ListenAddress**パラメータが空の場合)、**IdleTimeLimit**パラメータで指定された期間中にDr.Web MeshDへのリクエストがない場合、コンポーネントは自動的に終了します。

サービス

更新を交換する(更新)

このサービスを使用すると、ホストはウイルスやその他のデータベースの更新をサブスクライブし、更新に関する通知を送信し、クラウドホスト間で更新ファイルをアップロードして共有できます。サービス設定は、**Update***パラメータを使用して設定できます。

標準のサービス使用法では、Dr.Web MeshDがインストールされ、会社のローカルネットワーク内の複数のマシン(サービスのクライアント)で更新を取得する機能が有効になっていると想定しています。一般的なクライアント**設定**は次のとおりです。

```
...
[MeshD]
UpdateChannel = On
UpdateUplink = <server address>
ListenAddress =
...
[Update]
UseLocalCloud = Yes
...
```

更新を配布するローカルサーバーでは、次の設定が指定されています。

```
UpdateChannel = On
UpdateUplink =
ListenAddress = <address>: <port>
```

ここで、クライアントのアップリンク接続の<server address>は、サーバーホストがクライアント接続を管理するために使用する<address>および<port>を参照する必要があります。

ホストの1つが更新サーバー(ローカルクラウドの外部: Dr.Web GUS更新サーバーまたは集中管理サーバー)から更新されている場合、ホストは必要なすべてのクライアントに通知を送信し(ホストが更新交換サーバーとして設定されている場合)、サーバーホストに、ホストから配布可能なファイルの新しいリストを送信します。通知を受信すると、クライアントホストはサーバーからの更新のダウンロードをリクエストできます。次に、クライアントから



ファイルをリクエストしてローカルに保存するか、サーバーからファイルをリクエストした他のクライアントに送信できません。

このシナリオでは、クライアントが異なるタイミングでDr.Web GUSにリクエストを送信するため、更新の遅延が短縮します。そのため、最初に更新されたクライアントは、必要なすべてのクラウドホストに最新の更新ファイルをすぐに配信します。また、トラフィック量とDr.Web GUSの負荷も軽減されます。



ローカルクラウドを更新の配布に使用する場合、Dr.Web MeshDIに加えて、ホストにはDr.Web Updaterコンポーネントが含まれている必要があることに注意してください。

リモートファイルスキャン(エンジン)

このサービスでは、Dr.Web Scanning Engineを使用してリモートファイルをスキャンできます。クライアントホストはスキャン用のファイルをサーバーホストに送信し、サーバーホストはファイルスキャン用のサービスを提供します。一般的なクライアント[設定](#)は次のとおりです。

```
...
[MeshDI]
EngineChannel = On
EngineUplink = <server address>
ListenAddress =
...
```

ローカルスキャンサーバーでは、次の設定が指定されています。

```
EngineChannel = On
EngineUplink =
ListenAddress = <address>: <port>
```

ここで、クライアントのアップリンク接続の<server address>は、サーバーホストがクライアント接続を管理するために使用する<address>および<port>を参照する必要があります。

スキャンするファイルを送信する(ファイル)

この機能は使用されません(リモートスキャンはEngineサービス内で提供されます)。

URLチェック

このサービスでは、サーバーホストを使用して、潜在的に危険で推奨されないカテゴリーに属するURLをチェックできます。クライアントホストは、チェックするURLをサーバーホストに送信します。一般的なクライアント[設定](#)は次のとおりです。

```
...
[MeshDI]
UrlChannel = On
UrlUplink = <server address>
ListenAddress =
...
```



URLチェックに使用されるローカルサーバーでは、次の設定が指定されています。

```
UrlChannel = On
UrlUplink =
ListenAddress = <address>: <port>
```

ここで、クライアントのアップリンク接続の *<server address>* は、サーバーホストがクライアント接続を管理するために使用する *<address>* および *<port>* を参照する必要があります。

コマンドライン引数

Dr.Web MeshDを実行するには、コマンドラインに次のコマンドを入力します。

```
$ <opt_dir>/bin/drweb-meshd [<parameters>]
```

Dr.Web MeshDは次のオプションを処理できます。

パラメータ	説明
--help	機能：コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了するように指示します。 短縮形： -h 引数： None
--version	機能：このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了するように指示します。 短縮形： -v 引数： None

例：

```
$ /opt/drweb.com/bin/drweb-meshd --help
```

このコマンドはDr.Web MeshDに関する簡単なヘルプ情報を出力します。

スタートアップノート

コンポーネントは、自律モードで（他のコンポーネントから自律的に）OSのコマンドラインから直接起動することはできません。[Dr.Web ConfigD](#)設定デモンによって必要になる場合は、自動的に起動されます。コンポーネントの動作を管理するには、Dr.Web for UNIX File Servers用の[Dr.Web Ctl](#)コマンドラインベースの管理ツールを使用できます（これは**drweb-ctl**コマンドを使用して呼び出されます）。



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ドキュメントを要求するには、次のコマンドを使用します。**man 1 drweb-meshd**



設定パラメータ

コンポーネントは、Dr.Web for UNIX File Serversの統合された[設定ファイル](#)の [MeshD] セクションで指定されている設定パラメータを使用します。

セクションには以下のパラメータが含まれています。

LogLevel <i>{logging level}</i>	コンポーネントの ログの詳細レベル パラメータ値が指定されていない場合は、[Root] セクション の DefaultLogLevel パラメータの値が使用されます。 デフォルト値 : Notice
Log <i>{log type}</i>	コンポーネントの ロギング方式 。 デフォルト値 : Auto
ExePath <i>{path to file}</i>	コンポーネントの実行ファイルへのパス。 デフォルト値 : <opt_dir>/bin/drweb-meshd <ul style="list-style-type: none">• GNU/Linuxの場合 : /opt/drweb.com/bin/drweb-meshd• FreeBSDの場合 : /usr/local/libexec/drweb.com/bin/drweb-meshd
DebugSsh <i>{Boolean}</i>	ロギングレベルが LogLevel = Debugの場合、ホスト上で動作している Dr.Web MeshDが送受信したSSHプロトコルメッセージ(メッセージとデータの転送に使用)のロギングを実行。 デフォルト値 : No
IdleTimeLimit <i>{time interval}</i>	コンポーネントの最大アイドル時間。指定された時間が経過すると、コンポーネントはシャットダウンします。 最小値 - 10s. デフォルト値 : 30s
DnsResolverConfPath <i>{path to file}</i>	DNSリゾルバ設定ファイルへのパス。 デフォルト値 : /etc/resolv.conf
ListenAddress <i><IP address>:<port></i>	コンポーネントがクラウドホストからの接続の受信を待機しているクライアント接続のネットワークソケット(アドレスとポート)。これらのホストは、このクラウドホストによって提供されるサービスのクライアントです。 値が指定されていない場合、コンポーネントはクライアントからの要求を受け取りません。 デフォルト値 : (未設定)
UpdateChannel <i>{On / Off}</i>	このホスト上で動作するDr.Web MeshDコンポーネントを有効または無効にし、クラウドのホスト間でウイルスデータベースの更新を交換します(たとえば、他のクラウドホストからウイルスデータベースの更新を取得し、新しい更新をクラウドに送信します)。



	<p>このパラメータがオンに設定されている場合、コンポーネント<i>Dr.Web MeshD</i>は<i>Dr.Web ConfigD</i>設定デーモンによって自動的に起動されます。</p> <p>デフォルト値: On</p>
UpdateUplink <i>{address}</i>	<p>このホストに更新を提供するサーバーとして機能する<i>Dr.Web MeshD</i>の上位ホストのアドレス。</p> <p>使用可能な値:</p> <ul style="list-style-type: none">• 値が指定されていない - サーバーがサービスに設定されておらず、<i>Dr.Web MeshD</i>はどこにも接続されていません。• <i><IP address>:<port></i> - <i>Dr.Web MeshD</i>は指定されたアドレスとポートでサーバーに接続します。• <i>dns:<service name>[:<domain>]</i> - サーバーのアドレスとポートは、<i><domain></i> DNSドメインのSRVレコードを検索することで指定されます。<i><domain></i>が指定されていない場合、DNSリゾルバ設定ファイルのドメインが使用されます(パスは<i>ResolverConfPath</i>で指定されます)。ドメインは、最後に検出されたドメインに応じて、<i>search</i>または<i>domain</i>フィールドから取得されます。 <p>デフォルト値: (指定なし)</p>
UpdateDebugIpc <i>{Boolean}</i>	<p>ロギングレベルがLogLevel = Debugの場合は、更新の交換サービスのログにデバッグ情報を出力します。</p> <p>デフォルト値: No</p>
UpdateTraceContent <i>{Boolean}</i>	<p>ロギングレベルがLogLevel = Debugの場合は、更新の交換サービスのログに送信済みデータを出力します。</p> <p>デフォルト値: No</p>
FileChannel <i>{On / Off}</i>	<p>このホスト上で動作する<i>Dr.Web MeshD</i>コンポーネントのファイル交換への参加を許可するオプションを有効または無効にします。</p> <p>このパラメータがオンに設定されている場合、コンポーネント<i>Dr.Web MeshD</i>は<i>Dr.Web ConfigD</i>設定デーモンによって自動的に起動されます。</p> <p>デフォルト値: On</p>
FileUplink <i>{address}</i>	<p>このホストのファイルをスキャンするサーバーとして機能する<i>Dr.Web MeshD</i>の上位ホストのアドレス。</p> <p>使用可能な値:</p> <ul style="list-style-type: none">• 値が指定されていない - サーバーがサービスに設定されておらず、<i>Dr.Web MeshD</i>はどこにも接続されていません。• <i><IP address>:<port></i> - <i>Dr.Web MeshD</i>は指定されたアドレスとポートでサーバーに接続します。• <i>dns:<service name>[:<domain>]</i> - サーバーのアドレスとポートは、<i><domain></i> DNSドメインのSRVレコードを検索することで指定されます。<i><domain></i>が指定されていない場合、DNSリゾルバ設定ファイルのドメインが使用されます(パスは<i>ResolverConfPath</i>で指定されます)。ドメインは、最後に検出されたドメインに応じて、<i>search</i>または<i>domain</i>フィールドから取得されます。 <p>デフォルト値: (指定なし)</p>



FileDebugIpc <i>{Boolean}</i>	ロギングレベルが LogLevel = Debug の場合は、ファイル交換サービスのログにデバッグ情報を出します。 デフォルト値: No
EngineChannel <i>{On / Off}</i>	このホストで動作するDr.Web MeshDコンポーネントがスキャンエンジンサービスの提供に参加できるようにするオプションを有効または無効にします。 <i>このパラメータがオンに設定されている場合、コンポーネントDr.Web MeshDはDr.Web ConfigD設定デーモンによって自動的に起動されます。</i> デフォルト値: On
EngineUplink <i>{address}</i>	このホストにスキャンエンジンサービスを提供するスキャンサーバーとして機能するDr.Web MeshDの上位ホストのアドレス。 使用可能な値: <ul style="list-style-type: none">• 値が指定されていない - サーバーがサービスに設定されておらず、Dr.Web MeshDはどこにも接続されていません。• <IP address>:<port> - Dr.Web MeshDは指定されたアドレスとポートでサーバーに接続します。• dns:<service name>[:<domain>] - サーバーのアドレスとポートは、<domain> DNSドメインのSRVレコードを検索することで指定されます。<domain>が指定されていない場合、DNSリゾルバ設定ファイルのドメインが使用されます(パスはResolverConfPathで指定されます)。ドメインは、最後に検出されたドメインに応じて、searchまたはdomainフィールドから取得されます。 デフォルト値: (指定なし)
EngineDebugIpc <i>{Boolean}</i>	ロギングレベルが LogLevel = Debug の場合は、スキャンサービスのログにデバッグ情報を出します。 デフォルト値: No
UrlChannel <i>{On / Off}</i>	このホストで動作するDr.Web MeshDコンポーネントがURLチェックサービスの提供に参加できるようにするオプションを有効または無効にします。
UrlUplink <i>{address}</i>	このホストにURLチェックサービスを提供するサーバーとして機能するDr.Web MeshDの上位ホストのアドレス。 使用可能な値: <ul style="list-style-type: none">• 値が指定されていない - サーバーがサービスに設定されておらず、Dr.Web MeshDはどこにも接続されていません。• <IP address>:<port> - Dr.Web MeshDは指定されたアドレスとポートでサーバーに接続します。• dns:<service name>[:<domain>] - サーバーのアドレスとポートは、<domain> DNSドメインのSRVレコードを検索することで指定されます。<domain>が指定されていない場合、DNSリゾルバ設定ファイルのドメインが使用されます(パスはResolverConfPathで指定されます)。ドメインは、最後に検出されたドメインに応じて、searchまたはdomainフィールドから取得されます。 デフォルト値: (指定なし)

**UrlDebugIpc***{Boolean}*

ロギングレベルが**LogLevel** = `Debug`の場合、デバッグ情報をURLチェックサービスのログに出力します。

デフォルト値 : `No`



Dr.Web for UNIX File Serversの現在のバージョンでは、*File*ファイル送信サービスは使用されません。代わりに、*Engine*スキャンエンジンサービスを使用します。



Dr.Web CloudD

Dr.Web CloudDコンポーネントはDr.Web Cloud (Doctor Webのクラウドサービス)を参照します。Dr.Web Cloudサービスは、検出された脅威に関する最新情報をすべてのDr.Webアンチウイルスソリューションから収集し、ユーザーが望ましくないWebサイトにアクセスするのを防ぎ、Dr.Webウイルスデータベースに記述のない新しい脅威を含んだ感染ファイルからOSを保護します。さらに、Dr.Web Cloudサービスを使用すると、[Dr.Web Scanning Engine](#)。

動作原理

このコンポーネントは、指定ファイルのコンテンツにローカルの[Dr.Web Scanning Engine](#)が把握していない脅威がないかスキャンし、指定URLがDoctor WebのWebリソースの定義済みカテゴリーに属するかどうかを確認するようDoctor Web Dr.Web Cloudサービスに指示します。また、コンポーネントは感染ファイルの検出に関する統計情報と、Dr.Web for UNIX File Serversを実行しているOSに関する情報を定期的にDr.Web Cloudに送信します。

Dr.Web CloudDは設定デーモンによって自動的に実行されます。コンポーネントは、ユーザーまたはDr.Web for UNIX File Serversコンポーネントの1つからコマンドを受信したときに実行されます。

コンポーネントによって使用されます。このコンポーネントを介したDr.Web Cloudサービスへの (URLとファイルのスキャンの実行) リクエストは、Dr.Web for UNIX File Serversのさまざまなコンポーネント (製品ソリューションによって異なります) から送信されます。

さらに、コンポーネントはコマンドライン[Dr.Web Ctl](#) (**drweb-ctl** コマンドによって起動) からのDr.Web for UNIX File Servers管理ユーティリティのコマンドによるファイルのスキャン中に使用されます。脅威が検出されたら、[Dr.Web Scanning Engine](#) スキャンエンジンがファイルに関するレポートをDr.Web Cloudに送信します。



コマンドライン引数

Dr.Web CloudDを実行するには、コマンドラインに次のコマンドを入力します。

```
$ <opt_dir>/bin/drweb-cloudd [<parameters>]
```

Dr.Web CloudDは次のオプションを処理できます。

パラメータ	説明
--help	機能: コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了するように指示します。 短縮形: -h 引数: None
--version	機能: このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了するように指示します。 短縮形: -v 引数: None

例:

```
$ /opt/drweb.com/bin/drweb-cloudd --help
```

このコマンドはDr.Web CloudDに関する簡単なヘルプ情報を出力します。

スタートアップノート

コンポーネントは、自律モードで(他のコンポーネントから自律的に)OSのコマンドラインから直接起動することはできません。必要に応じて、[Dr.Web ConfigD](#)設定デモンによって自動的に起動されます。コンポーネントの動作を管理し、からの情報を使用してファイルやURLをスキャンするには、Dr.Web for UNIX File Servers用の[Dr.Web Ct](#)コマンドラインベースの管理ツールを使用できます(**drweb-ctl**[コマンド](#)を使用して呼び出されます)。



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ドキュメントを要求するには、次のコマンドを使用します。**man 1 drweb-cloudd**

設定パラメータ

コンポーネントは、Dr.Web for UNIX File Serversの統合された[設定ファイル](#)の[CloudD]セクションで指定されている設定パラメータを使用します。

セクションには以下のパラメータが含まれています。

LogLevel	コンポーネントの ログの詳細レベル
{logging level}	



	<p>パラメータ値が指定されていない場合は、[Root] セクションの DefaultLogLevelパラメータの値が使用されます。</p> <p>デフォルト値: Notice</p>
Log <i>{log type}</i>	<p>コンポーネントの ロギング方式。</p> <p>デフォルト値: Auto</p>
ExePath <i>{path to file}</i>	<p>コンポーネントの実行ファイルへのパス。</p> <p>デフォルト値: <opt_dir>/bin/drweb-cloudd</p> <ul style="list-style-type: none">• GNU/Linuxの場合: /opt/drweb.com/bin/drweb-cloudd• FreeBSDの場合: /usr/local/libexec/drweb.com/bin/drweb-cloudd
RunAsUser <i>{UID / user name}</i>	<p>このパラメータは、コンポーネントを実行するユーザー名を決定します。ユーザー名は、ユーザーのUIDまたはユーザーのログインとして指定できます。ユーザー名が数字で構成されている場合 (UIDに似ている場合) は、「name:」というプレフィックスを付けて指定します。次に例を示します。</p> <p>RunAsUser = name:123456。</p> <p>ユーザー名が指定されていない場合、コンポーネント操作は開始後にエラーが発生して終了します。</p> <p>デフォルト値: drweb</p>
IdleTimeLimit <i>{time interval}</i>	<p>コンポーネントの最大アイドル時間。指定された時間が経過すると、コンポーネントはシャットダウンします。</p> <p>デフォルト値: 30s</p>
PersistentCache <i>{On / Off}</i>	<p>Dr.Web Cloud応答のキャッシュをディスクへ保存することを有効または無効にします。</p> <p>デフォルト値: Off</p>
DebugSdk <i>{Boolean}</i>	<p>詳細な Dr.Web Cloudメッセージをデバッグレベルでログファイルに含めるかどうかを示します (LogLevel = DEBUG)。</p> <p>デフォルト値: No</p>



Dr.Web StatD

Dr.Web StatDコンポーネントは、Dr.Web for UNIX File Serversコンポーネントの操作中に発生するイベントの統計を蓄積するために設計されています。イベントは無期限のリポジトリに保存され、リクエストに応じて取得できます。

動作原理

このコンポーネントは、Dr.Web for UNIX File Serversコンポーネントの操作中に取得されたイベントの蓄積と無期限の保存を確保します。次のタイプのイベントがログに記録されます。

- コンポーネントの緊急シャットダウン。
- 脅威の検出（特に電子メールメッセージ）

Dr.Web StatDはデーモンモードで動作し、設定制御デーモンによって自動的に起動されます。イベントの表示と管理は、[Dr.Web Ctl](#)ユーティリティの`command`イベントによって徹底されます。

コマンドライン引数

Dr.Web StatDを実行するには、コマンドラインに次のコマンドを入力します。

```
$ <opt_dir>/bin/drweb-statd [<parameters>]
```

Dr.Web StatDは次のオプションを処理できます。

パラメータ	説明
<code>--help</code>	機能：コマンドラインパラメータに関する簡単なヘルプ情報をコンソールまたはターミナルエミュレーターに出力し、完了時に終了するように指示します。 短縮形： <code>-h</code> 引数： None
<code>--version</code>	機能：このコンポーネントのバージョンに関する情報をコンソールまたはターミナルエミュレーターに出力し、完了後に終了するように指示します。 短縮形： <code>-v</code> 引数： None

例：

```
$ /opt/drweb.com/bin/drweb-statd --help
```

このコマンドはDr.Web StatDに関する簡単なヘルプ情報を出力します。

スタートアップノート

コンポーネントは、自律モードで（他のコンポーネントから自律的に）OSのコマンドラインから直接起動することはできません。必要に応じて、[Dr.Web ConfigD](#)設定デーモンによって自動的に起動されます。コンポーネントの



動作を管理するには、Dr.Web for UNIX File Servers用の[Dr.Web Ctl](#)コマンドラインベースの管理ツールを使用できます（これは[drweb-ctl](#)コマンドを使用して呼び出されます）。



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ドキュメントを要求するには、次のコマンドを使用します。**man 1 drweb-statd**

設定パラメータ

コンポーネントは、Dr.Web for UNIX File Serversの統合された[設定ファイル](#)の[StatD]セクションで指定されている設定パラメータを使用します。

セクションには以下のパラメータが含まれています。

LogLevel <i>{logging level}</i>	コンポーネントの ログの詳細レベル パラメータ値が指定されていない場合は、[Root] セクション の DefaultLogLevel パラメータの値が使用されます。 デフォルト値: Notice
Log <i>{log type}</i>	コンポーネントの ロギング方式 。 デフォルト値: Auto
ExePath <i>{path to file}</i>	コンポーネントの実行ファイルへのパス。 デフォルト値: <opt_dir>/bin/drweb-statd <ul style="list-style-type: none">• GNU/Linuxの場合: /opt/drweb.com/bin/drweb-statd• FreeBSDの場合: /usr/local/libexec/drweb.com/bin/drweb-statd
RunAsUser <i>{UID / user name}</i>	このパラメータは、コンポーネントを実行するユーザー名を決定します。ユーザー名は、ユーザーのUIDまたはユーザーのログインとして指定できます。ユーザー名が数字で構成されている場合（UIDに似ている場合）は、「name:」というプレフィックスを付けて指定します。次に例を示します。 RunAsUser = name:123456。 ユーザー名が指定されていない場合、コンポーネント操作は開始後にエラーが発生して終了します。 デフォルト値: drweb
IdleTimeLimit <i>{time interval}</i>	コンポーネントの最大アイドル時間。指定された時間が経過すると、コンポーネントはシャットダウンします。 最小値 - 10s。 デフォルト値: 30s
MaxEventStoreSize <i>{size}</i>	イベントデータベースの最大許容サイズ。mbで定義されます。例: MaxEventStoreSize = 100mb。 最小値 - 50mb。



デフォルト値 : 1GB



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さまざま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見なされません。

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に感染するウイルスです。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、文書を開くか、閉じるか、保存すると、マクロが自動的に開始されることがあります。
- **スクリプトウイルス**は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）に感染します。これらはスクリプトを実行できる他のファイル形式に感染することができるため、Webアプリケーションのスクリプトの脆弱性を利用します。
- **ブートウイルス**は、ディスクやパーティションのブートレコード、またはハードドライブのマスターブートレコードに感染します。多くのメモリを必要とせず、システムのロールアウト、再起動、またはシャットダウンが実行されるまでタスクを実行し続けられます。

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**は、感染するたびにコードを暗号化して、ファイル、ブートセクター、またはメモリ内での検出を妨げます。このようなウイルスのすべてのコピーには、ウイルスのシグネチャとして使用される可能性がある小さな共通コードの一部（復号手順）しか含まれていません。
- **ポリモーフィック型ウイルス**も同様に自身のコードを暗号化しますが、コピーごとに異なる特別な復号プロセスの生成も行います。つまり、この種のウイルスにはシグネチャバイトがありません。
- **ステルスウイルス**は、特定のアクションを実行して、感染したオブジェクトでの活動と存在を隠します。このようなウイルスは、オブジェクトを感染させる前にそのオブジェクトの特性を収集し、Scannerが変更されたファイルを探し出す際に誤認させるための「ダミー」特性を作り出します。



ウイルスは、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は、さまざまなネットワークと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。
- メールワームは、メールプロトコル（POP3、SMTPなど）を使用して拡散します。
- チャットワームは、広く使用されているメッセージャーや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）したりすることを可能にします。

トロイの木馬のマスクングと悪意のある機能は、ウイルスのそれに似ています。トロイの木馬は、ウイルスのコンポーネントである場合もあります。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）。

トロイの木馬はよくウイルスやワームによって拡散されることや、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では個別のクラスとして分類されています。

- バックドアは、侵入者がシステムにログオンしたり、既存のアクセスやセキュリティ対策を回避する特権機能を取得したりすることを可能にするトロイの木馬です。バックドアはファイルに感染しませんが、レジストリキーを変更して自身をレジストリに書き込みます。
- ルートキットは、自身を隠すためにOSのシステム機能を監視する際に使用されます。さらに、ルートキットは、他のプログラム（他の脅威）、レジストリキー、フォルダ、ファイルのプロセスを隠すことができます。ルートキットは独立したプログラムとして、または別の悪意のあるプログラムのコンポーネントとして拡散されます。動作モードに応じて2種類のルートキットがあります。ユーザーモードで動作（ユーザーモードライブラリの機能を監視）する



ユーザーモードのルートキット(UMR)とカーネルモードで動作する(システムのカーネルレベルで機能を監視して、悪意のあるプログラムを検出しにくくする)カーネルモードのルートキット(KMR)。

- キーロガーは、ユーザーがキーボードを使って入力したデータを記録するために使用されます。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。
- クリッカーは、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(ときに有害な)アドレスにリダイレクトします。
- 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さまざま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

ヒューリスティックアナライザによって検出される潜在的なコンピューター脅威です。これらのオブジェクトは、あらゆるタイプの脅威（ITセキュリティの専門家も把握していないもの）である可能性があり、または誤検出の場合もあります。疑わしいオブジェクトを含むファイルを隔離に移動するよう選択することをお勧めします。解析のために Doctor Web アンチウイルスラボにも送信する必要があります。



付録 B. コンピューター脅威の駆除

Doctor Webアンチウイルスソリューションは、悪意のあるソフトウェア検出に複数の手法を同時に使用します。それにより、感染が疑われるファイルに対する徹底的なスキャンを実行し、ソフトウェアの動作を管理できます。

- [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ンプ) 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圧縮されたファイル内に悪意のあるオブジェクトが存在する可能性をヒューリスティックに検出します。Dr.Webアンチウイルスソリューションはパックされたオブジェクトのスキャン中に構造エントロピー解析も使用します。このテクノロジーはコードの配置を解析することで脅威を検出します。そのため、1つの検体から、同じポリモーフニ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。

上のスキャン手法に加え、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製品は悪意のあるオブジェクトに対してさまざま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、あるいは検出のたび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するように指示します。
- **Report (報告する)** - 他のすべてのアクションを実行せずに、検出された脅威について通知します。
- **Block (ブロック)** - 感染したファイルにアクセスしようとする試みをすべてブロックするように指示します（このアクションを使用できないコンポーネントがある場合があります）。
- **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 UNIX File Servers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_dir>/bin/support-report.sh
```

<opt_dir> は、実行可能ファイルとライブラリを含むDr.Web for UNIX File Serversファイルのディレクトリです (**GNU/Linux** の場合はデフォルトで /opt/drweb.com)。ディレクトリに使用される規則については、[はじめに](#) を参照してください。



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 UNIX File Servers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
- 次のコマンドの出力: **df**, **ip a** (**ifconfig -a**)、**ldconfig -p**、**iptables-save**、**nft export xml**
- Dr.Web for UNIX File Servers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 UNIX File Servers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
- Dr.Web Virus-Finding EngineスキャンエンジンのバージョンとMD5ハッシュ値
- Dr.Web for UNIX File Servers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 UNIX File Servers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、レポート作成の完全なタイムスタンプ(ミリ秒単位)です(例: 20190618151718.23625)。



付録D. Dr.Web for UNIX File Servers設定ファイル

すべてのDr.Web for UNIX File Serversコンポーネントの設定パラメータは、特別な調整デーモンDr.Web ConfigDによって管理されます。これらのパラメータはdrweb.iniファイルに格納されています。デフォルトディレクトリは<etc_dir>です(**GNU/Linux**の場合は/etc/opt/drweb.com)。



設定ファイルには、デフォルト値と異なるパラメータのみが格納されています。パラメータが設定ファイルにない場合は、そのデフォルト値が使用されます。

<opt_dir>、<etc_dir>、<var_dir>の表記規則の詳細は、[はじめに](#)を参照してください。

次のコマンドを使用して、設定ファイルにないパラメータとデフォルト値を持つパラメータを含む、すべての設定のリストを表示できます。

```
$ drweb-ctl cfshow
```

パラメータ値は次のいずれかの方法で変更できます。

1. 設定ファイルでパラメータを指定(任意のテキストエディターでファイルを編集)し、変更を適用するためのSIGHUPシグナルを設定デーモン(**drweb-configd**コンポーネント)に送信します(これを行うには**drweb-ctl reload**コマンドを発行します)。
2. このコマンドをコマンドラインに入力します。

```
# drweb-ctl cfset <section>.<parameter> <new value>
```



このコマンドは、管理ツールDr.Web Ctlがスーパーユーザー権限で実行されている場合にのみ実行できます。スーパーユーザー権限を取得するには、**su**コマンドか**sudo**コマンドを使用します。

コマンドライン管理ツールDr.Web Ctl(**drweb-ctl**モジュール)のcfshowとcfsetのコマンド構文の詳細については、[Dr.Web Ctl](#)のセクションを参照してください。

ファイル構造

設定ファイルの構造は以下のとおりです。

- ファイルの内容は名前が付けられたセクションに分割されます。こうしたセクションで利用可能な名前は厳密に事前定義されており、変更できません。セクション名は角括弧で指定され、セクションパラメータを使用するDr.Web for UNIX File Serversコンポーネント名と似ています(設定デーモンDr.Web ConfigDのすべてのパラメータを保存する[Root][セクション](#)は除く)。
- 設定ファイル内の「;」または「#」文字は、コメントの始まりを示します。文字に続くすべてのテキストは、設定パラメータの読み取り中にDr.Web for UNIX File Serversコンポーネントによってスキップされます。
- ファイルの1行には、パラメータ値を1つだけ含めることができます。値を指定する一般的な形式は次のとおりです(「=」文字の前後の空白は無視されます)。



```
<Parameter name> = <Value>
```

- すべてのパラメータ名は厳密に事前定義されており、変更はできません。
- セクション名とパラメータ名はすべて大文字と小文字が区別されません。パラメータ値は、パスに含まれるディレクトリやファイルの名前を除くと、(UNIXのようなOSの場合でも)大文字と小文字が区別されません。
- ファイルで指定されるセクションの順序とセクションで指定されるパラメータの順序は重要ではありません。
- 設定ファイルのパラメータ値は引用符で囲むことができ、空白がある場合は引用符で囲む必要があります。
- 一部パラメータは値のリストを持つことができます。その場合、値はコンマで区切るか、設定ファイルの異なる行に複数指定します。前者の場合、コンマの前後の空白は無視されます。空白文字がパラメータ値の一部である場合は、その文字を引用符で囲む必要があります。

1つのパラメータに複数の値を指定する方法の例:

1) コンマ区切りリストとして:

```
Parameter = Value1, Value2, "Value 3"
```

2) 設定ファイルの複数行で:

```
Parameter = Value2  
Parameter = Value1  
Parameter = "Value 3"
```

パラメータ値を指定する順序は重要ではありません。



パラメータ値がパスである場合、コンマを使用したコンポーネントのリストが使用されている場合は、一覧表示された各パラメータ値を引用符で囲む必要があります。たとえば、パラメータ **ExcludedPaths** に2つのパス `/etc/file1` と `/etc/file2` が必要な場合、このパラメータは1つの文字列として以下のように設定ファイルに書き込むか

```
ExcludedPaths = "/etc/file1", "/etc/file2"
```

または2つの文字列として書き込みます

```
ExcludedPaths = /etc/file1  
ExcludedPaths = /etc/file2
```

上記以外の場合、このパラメータを使用するコンポーネントは、文字列「`/etc/file1`、`/etc/file2`」を1つのパスとして解釈します。

- パラメータに複数の値を指定できる場合は、明確に指定されます。そのため、現在のマニュアルや設定ファイルのコメント内で明確に指定されていない場合、パラメータに指定できる値は1つのみです。

設定ファイルのセクションの説明については、Dr.Web for UNIX File Serversコンポーネントの説明を参照してください。



パラメータタイプ

設定パラメータは以下のいずれかのタイプになります。

- **address** - `<IP address>:<port>`の値ペアとして指定したネットワーク接続アドレス。場合によっては、ポート値を省略できます（省略した場合は、パラメータの説明で指定されます）。
- **ブール値** - インジケータとして使用されるフラグ。このようなパラメータは、値がYesまたはNoになります。
- **整数** - パラメータ値は、非負の整数になります。
- **小数** - パラメータ値は、小数部分のある非負の整数になります。
- **時間間隔** - パラメータ値は、非負の整数と時間単位を示すサフィックス（文字）で構成される時間間隔になります。以下のサフィックスを使用できます。

- w - 週 (1w = 7d)
- d - 日 (1d = 24h)
- h - 時間 (1h = 60m)
- m - 分 (1m = 60s)
- s - 秒

サフィックスを省略した場合、間隔は秒単位と見なされます。秒単位で表される時間間隔では、小数点の後にミリ秒を指定できます（区切り文字の後に3桁以内、0.5秒～500ミリ秒など）。異なる時間単位で複数の時間間隔を指定できます。この場合、間隔の合計が計算されます（実際には、値が設定に書き込まれる前に時間間隔は常にミリ秒に変換されます）。

基本的には、すべての時間間隔は次の形式で表現されます。 $N_1wN_2dN_3hN_4mN_5[.N_6]s$ 。 N_1, \dots, N_6 はこの間隔に含まれる時間単位の数です。たとえば、1年（365日）は次のように表すことができます（すべてのレコードは同じ365日を表しています）：365d、52w1d、52w24h、51w7d24h、51w7d23h60m、8760h、525600m、31536000s。

以下の例では、30分、2秒、500ミリ秒の間隔を指定する方法を示しています。

1. 設定ファイルでの設定。

```
UpdateInterval = 30m2.5s
```

2. コマンド `drweb-ctl cfset` を使用：

```
# drweb-ctl cfset Update.UpdateInterval 1802.5s
```

3. コマンドラインパラメータ経由（例：コマンドライン引数の場合）。

```
$ drweb-se --WatchdogInterval 1802.5
```

- **サイズ** - パラメータ値は、オブジェクト（ファイル、バッファ、キャッシュなど）のサイズで表すことができ、非負の整数と単位を表すサフィックスで構成します。以下のサフィックスを使用できます。
 - mb - メガバイト (1mb = 1024kb)。
 - kb - キロバイト (1kb = 1024b)。
 - b - バイト。

サフィックスを省略した場合、サイズはバイト単位と見なされます。異なる単位で複数のサイズを指定できます。この場合、サイズの合計が計算されます（実際には、サイズ値は常にバイトに変換されます）。



- **ディレクトリ(ファイル)へのパス** - パラメータ値は、ディレクトリ(ファイル)へのパスである文字列になります。ファイルパスはファイル名で終わる必要があります。



UNIX系システムでは、ディレクトリとファイルの名前は、大文字と小文字が区別されます。パラメータ記述で明示的に指定されていない場合、パスに特殊文字(?,*)を含むマスクを含めることはできません。

- **ロギングレベル** - Dr.Web for UNIX File Serversコンポーネントのイベントを記録するレベル。このタイプのパラメータでは、以下の値を使用できます。
 - **DEBUG** - 最も詳細なログレベル。すべてのメッセージとデバッグ情報が登録されます。
 - **INFO** - すべてのメッセージが登録されます。
 - **NOTICE** - すべてのエラーメッセージ、警告、通知が登録されます。
 - **WARNING** - すべてのエラーメッセージと警告が登録されます。
 - **ERROR** - エラーメッセージのみが登録されます。
- **ログタイプ** - パラメータ値でDr.Web for UNIX File Serversコンポーネントによるログの実行方法(ロギング方式)を定義します。このタイプのパラメータでは、以下の値を使用できます。
 - **Stderr[:ShowTimestamp]** - メッセージは**stderr**(標準エラーストリーム)に表示されます。この値は設定デーモンの設定でのみ使用できます。バックグラウンドモードで動作する(「デーモン化される」)場合、つまりパラメータ**d**を指定して起動した場合、バックグラウンドモードで動作するコンポーネントは端末のI/Oストリームにアクセスできないため、この値は**使用できません**。追加パラメータ**ShowTimestamp**は、すべてのメッセージにタイムスタンプを追加するように指示します。
 - **Auto** - ログ対象のメッセージは設定デーモンDr.Web ConfigDに送られ、設定に基づいて一か所([Root]セクションのログパラメータ)に保存されます。この値は、**設定デーモンを除くすべてのコンポーネント**に指定され、デフォルト値として使用されます。
 - **Syslog[:<facility>]** - メッセージはシステムロギングサービス**syslog**に送信されます。
 - 追加オプション**<facility>**は、**syslog**のメッセージ登録レベルを指定するために使用します。次の値を使用できます。
 - **DAEMON** - デーモンのメッセージ。
 - **USER** - ユーザープロセスのメッセージ。
 - **MAIL** - メールプログラムのメッセージ。
 - **LOCAL0** - ローカルプロセス0のメッセージ。
 - ...
 - **LOCAL7** - ローカルプロセス7のメッセージ。
 - **<path>** - メッセージは指定されたログに直接保存されます。

パラメータ値の指定方法の例。

1. 設定ファイルでの設定。

```
Log = Stderr:ShowTimestamp
```

2. コマンドdrweb-ctl cfsetを使用:

```
# drweb-ctl cfset Root.Log /var/opt/drweb.com/log/general.log
```

3. コマンドラインパラメータ経由(例: コマンドライン引数の場合)。



```
$ drweb-se --Log Syslog:DAEMON
```

- **アクション** - 特定の脅威または別のイベントが検出されたときにDr.Web for UNIX File Serversコンポーネントによって実行されるアクション。次の値を使用できます。
 - **Report** - アクションは適用せず、検出された脅威についての通知のみをするよう指示します。
 - **Block** - 感染したファイルにアクセスしようとする試みを変更せずにすべてブロックするよう指示します（一部のコンポーネントではこのアクションを使用できない場合があります）。
 - **Cure** - 脅威の駆除を試みる（悪意のあるコンテンツのみを削除する）よう指示します。
 - **Quarantine**（隔離） - 感染したファイルを隔離に移動するよう指示します。
 - **Delete** - 感染したファイルを削除するよう指示します。



一部のアクションは特定のイベントにのみ適用できます（たとえば「スキャンエラー」イベントではCureアクションをトリガーできません）。許可されたアクションは、常にアクションタイプのパラメータに記述されます。

他のパラメータタイプと可能な値は、パラメータの説明で指定されています。



付録E. SSL証明書を生成する

安全なSSL/TLSデータチャネルとHTTPS、LDAPs、SMTPSなどのアプリケーションプロトコルを使用するDr.Web for UNIX File Serversコンポーネントの場合は、プライベートSSLキーと対応する証明書を提供する必要があります。一部のコンポーネントのキーと証明書は自動的に生成されます。それ以外の場合はDr.Web for UNIX File Serversユーザーが作成する必要があります。すべてのコンポーネントがPEN形式の証明書を使用します。

認証局(CA)の検証証明書や署名付き証明書など、SSL / TLSを介した接続に使用されるプライベートキーと証明書を生成するには、コマンドラインユーティリティ**openssl** (**OpenSSL**暗号化パッケージに含まれる)を使用できます。

プライベートキーとそれに対応するSSL証明書を、CA検証証明書によって署名されたSSL証明書と共に生成するために必要な一連のアクションを検討します。

プライベートSSLキーと証明書を生成する

生成手順は2つのステップで構成されています。

1. プライベートキー(RSAアルゴリズム、キーの長さは2048ビット)を生成します。

```
$ openssl genrsa -out keyfile.key 2048
```

キーをパスワードで保護する場合は、`-des3`オプションを使用します。生成されたキーは、現在のディレクトリの`keyfile.key`ファイルにあります。キーを表示するには、次のコマンドを使用します。

```
$ openssl rsa -noout -text -in keyfile.key
```

2. 既存のプライベートキーに基づいて指定された期間の証明書を生成します(この場合は365日)

```
$ openssl req -new -x509 -days 365 -key keyfile.key -out certificate.crt
```

このコマンドは、認証オブジェクトを識別するためのデータ(名前、組織など)を要求します。生成された証明書は、`certificate.crt`ファイルに置かれます。

生成された証明書の内容をスキャンするには、次のコマンドを使用します。

```
$ openssl x509 -noout -text -in certificate.crt
```

証明書を信頼済みCA証明書として登録する

信頼済みCA証明書のシステムリストに証明書を登録する場合(前の手順で証明書が生成される場合など)は、次の手順を実行します。

1. 証明書ファイルをシステムの信頼済み証明書ディレクトリ(**Debian/Ubuntu**の`/etc/ssl/certs/`)に移動またはコピーします。
2. 信頼済み証明書ディレクトリに、証明書へのシンボリックリンクを作成します。リンクの名前は証明書のハッシュ値です。
3. 証明書を含むシステムのディレクトリの内容にインデックスを付け直します。



以下の例では、これら3つすべてのアクションを実行します。ここでは、現在の証明書ディレクトリが信頼済み証明書ディレクトリ/etc/ssl/certs/であり、信頼済み証明書として登録されている証明書が/home/user/ca.crtファイルにあると想定しています。

```
# cp /home/user/ca.crt ./
# ln -s ca.crt `openssl x509 -hash -noout -in ca.crt`.0
# c_rehash /etc/ssl/certs/
```

署名付き証明書を作成する

署名付き証明書を作成するには、次の手順に従います。

1. 既存のプライベートキーに基づいて証明書に署名するためのリクエスト (*Certificate Signing Request (CSR)*) を生成します。キーが存在しない場合は、生成します。署名リクエストは次のコマンドで作成されます。

```
$ openssl req -new -key keyfile.key -out request.csr
```

このコマンドは、証明書を作成するコマンドと同様に、認証済みオブジェクトを識別するためのデータを要求します。このkeyfile.keyは、プライベートキーの既存のファイルです。受信したリクエストはrequest.csrファイルに保存されます。

リクエストの作成結果を確認するには、次のコマンドを使用します。

```
$ openssl req -noout -text -in request.csr
```

2. 次のコマンドを使用して、リクエストと既存のCA証明書に基づいて署名付き証明書を作成します。

```
$ openssl x509 -req -days 365 -CA ca.crt -CAkey ca.key -set_serial 01 -in request.csr -out sigcert.crt
```

署名付き証明書を作成するには、ルート証明書ca.crtとそのプライベートキーca.key(ca.crtとca.keyの代わりにcertificate.crt証明書とkeyfile.keyキーを使用することもできます。その場合、取得した証明書は自己署名されます)、署名リクエストのrequest.csrの3つのファイルが必要です。作成された署名付き証明書はsigcert.crtファイルに保存されます。

結果を確認するには、次のコマンドを使用します。

```
$ openssl x509 -noout -text -in sigcert.crt
```

作成する必要がある一意の証明書の数と同じだけこの手順を繰り返します。たとえば、スキャンクラスタ内の分散ファイルスキャンDr.Web Network Checkerのすべてのエージェントには、独自のキーと証明書が必要です。

署名付き証明書を変更する

一部のブラウザまたはメールクライアントでは、認証に使用される署名済み証明書をPKCS12形式に変更する必要があります。次のコマンドを使用して証明書を変更できます。

```
# openssl pkcs12 -export -in sigcert.crt -out sigcert.pfx -inkey keyfile.key
```



Sigcert.crtは署名済み証明書の既存ファイルです。keyfile.keyは対応するプライベートキーのファイルです。変更した証明書はsigcert.pfxに保存されます。



付録F. 既知のエラー

このセクションには次が含まれます。

- [エラーを特定するための推奨事項](#)。
- [エラーコードで検出されたエラー](#)の説明。
- [症状によって検出された](#)、コードのないエラーの説明。
- エラーコード、エラーメッセージ、それらの内部指定をリンクする[カタログ](#)。



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](#)に連絡することをお勧めします。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

- エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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
```

コードによるエラー

テキスト形式のエラーメッセージや数値のエラーコードを受け取る代わりに、EC_XXXのような内部エラーコード（たとえば、EC_APP_TERMINATED）を受信した場合は、[エラーの内部カタログ](#)の表を使用して数値のエラーコードと、このセクションに記載されているエラーの説明を見つけることができます。

エラーメッセージ: モニターチャン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[Dr.Web ConfigD](#)設定デーモンと接続できません。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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 UNIX File Servers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 UNIX File Serversまたはその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 UNIX File Serversをインストールする](#)および[Dr.Web for UNIX File Servers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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

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）。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

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)。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog](#)を使用することもできます。

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。

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(時間がかかるなどの理由によって)。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog](#)を使用することもできます。

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: Dr.Web for UNIX File Servers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)。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog](#)を使用することもできます。

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。

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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください (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-ctllog](#)を使用することもできます。

エラーの解決:

1. 以下のコマンドを入力し、Dr.Web for UNIX File Serversをリロードします。

```
# 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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください (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-ctllog](#)を使用することもできます。

エラーの解決:

1. 以下のコマンドを入力し、Dr.Web for UNIX File Serversをリロードします。

```
# 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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください (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-ctllog](#)を使用することもできます。

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。

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: 機能の実行に必要なコンポーネントがインストールされていません。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

エラーの解決:

1. 必要なコンポーネントをインストールまたは再インストールしてください。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. 必要なコンポーネントをインストールまたは再インストールしても解決しない場合は、Dr.Web for UNIX File Serversを再インストールしてください。

Dr.Web for UNIX File Serversまたはその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 UNIX File ServersをインストールするおよびDr.Web for UNIX File Servers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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

エラーの解決:

1. 以下のコマンドを入力し、Dr.Web for UNIX File Serversをリロードします。

```
# 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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

エラーの解決:

1. 以下のコマンドを入力し、Dr.Web for UNIX File Serversをリロードします。



```
# 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: このソフトウェアの一部であり、要求された操作を実行するために必要な特定のサブシステムについて、その現在の状態が未知であるということが明らかになりました。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

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 UNIX File Servers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（ファイルシステムのルートディレクトリから始まる）。現在使用されているのは相対パスです。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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）。



す)。また、[コマンドdrweb-ctllog](#)を使用することもできます。

エラーの解決：

1. Dr.Web for UNIX File Servers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)、Dr.Web for UNIX File Serversを再起動して操作を繰り返してください。

場合によっては、システムサービス**systemd**は指定した上限の変更を無視できます。この場合、ファイル/etc/systemd/system/drweb-configd.service.d/limits.confを編集し(ない場合は作成して)、変更後の制限値を指定します。たとえば、次のようになります。

```
[Service]
LimitDATA = 32767
```

systemdの利用可能な上限のリストはドキュメント**man systemd.exec**で確認できます。

次のコマンドを入力して、Dr.Web for UNIX File Servers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。

エラーメッセージ: I/O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う一度使用できない、など)。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog](#)を使用することもできます。

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: 指定された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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog](#)を使用することもできます。

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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog](#)を使用することもできます。

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てください。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog](#)を使用することもできます。

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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog](#)を使用することもできます。

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 UNIX File Servers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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

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: 読み取り専用ファイルシステム

エラーコード: x28

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）を作成または変更しようと試みた際に、ファイルシステムが読み取り専用であることが明らかになりました。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

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）。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

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: アクセスした入出力(I/O)がドライブではありません。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog](#)を使用することもできます。

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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog](#)を使用することもできます。

エラーの解決:

1. ファイル名を確認します。必要に応じ、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: ファイルのスキャン中に、ファイルが変更されていることが明らかになりました。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog](#)を使用することもできます。

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: ファイルシステムのオブジェクトへのアクセス中に、それが通常ファイルではないということが明らかになりました(つまり、ディレクトリ、ソケット、またはファイルシステムのその他のオブジェクトである)。



エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

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: ホストがオフラインです。

エラーコード: x35

説明: ネットワーク経路でリモートホストを利用できません。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

**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：異なるマウントポイントに属するファイルシステムディレクトリ間の移動を必要とするファイル復元の試みです。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

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：アーカイブのアンパックに失敗しました（パスワード保護されているか、破損している可能性があります）。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

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](#)



ルの[Root]セクションにあるVirusBaseDirVirusBaseDirパラメータ)。

パスを表示および変更するには、[Webインターフェース](#)の全般設定ページに移動します(インストールされている場合)。

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.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. ウイルスデータベースを更新します。

- Webインターフェースがインストールされている場合は、[Webインターフェース](#)のメインページで更新をクリックします。
- または、[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プログラムの古いバージョン向けのものです。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog](#)を使用することもできます。

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VirusBaseDirVirusBaseDirパラメータ)。

パスを表示および変更するには、[Webインターフェース](#)の全般設定ページに移動します(インストールされている場合)。

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.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. ウイルスデータベースを更新します。

- Webインターフェースがインストールされている場合は、[Webインターフェース](#)のメインページで更新をクリックします。
- または、[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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

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VirusBaseDirVirusBaseDirパラメータ）。
 - パスを表示および変更するには、[Webインターフェース](#)の全般設定ページに移動します（インストールされている場合）。
 - 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.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. ウイルスデータベースを更新します。

- Webインターフェースがインストールされている場合は、[Webインターフェース](#)のメインページで更新をクリックします。
- または、[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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

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VirusBaseDirVirusBaseDirパラメータ）。
 - パスを表示および変更するには、[Webインターフェース](#)の全般設定ページに移動します（インストールされている場合）。
 - 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.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. ウイルスデータベースを更新します。

- Webインターフェースがインストールされている場合は、[Webインターフェース](#)のメインページで更新をクリックします。
- または、[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)。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog`を使用することもできます。

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)。
 - [Webインターフェース](#)のコンポーネント設定のあるページ(インストールされている場合)。
 - `drweb-ctlcfshow`および`drweb-ctlcfset`[コマンド](#)を使用します。
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ています。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog`を使用することもできます。

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ください。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: 認証に使用された認証情報を持つユーザーが十分な権限を有していません。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog`を使用することもできます。

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ください。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 UNIX File Servers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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog](#)を使用することもできます。

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ください。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: コマンドの実行を試みる際に、無効な引数が使用されました。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog](#)を使用することもできます。

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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog](#)を使用することもできます。

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: スーパーユーザー権限が必要です。

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、スーパーユーザー権限を持ったユーザーのみです。



エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

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 UNIX File Servers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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

エラーの解決：

1. Dr.Web for UNIX File Servers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. Dr.Web for UNIX File Serversをスタンドアロンモードに切り替えるには
 - Webインターフェースがインストールされている場合は、[Webインターフェース](#)の集中管理の集中管理モードを有効にするチェックボックスをオフにします。
 - 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 UNIX File Servers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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください (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-ctllog](#)を使用することもできます。

エラーの解決:

1. Dr.Web for UNIX File Serversの設定をデフォルトに復元します。

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、次のコマンドを実行することでDr.Web for UNIX File Servers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 UNIX File Servers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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください (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-ctllog](#)を使用することもできます。

エラーの解決:

1. いずれかのテキストエディターで <etc_dir>/drweb.iniファイルを開き、無効なパラメータが含まれる行を削除します。ファイルを保存し、次のコマンドを実行することで[Dr.Web ConfigD](#)設定デーモンを再起動させます。

```
# service drweb-configd restart
```

2. 問題が解決しない場合は、Dr.Web for UNIX File Servers設定をデフォルトに戻してしてください。

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。



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 UNIX File Servers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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

エラーの解決:

1. いずれかのテキストエディターで <etc_dir>/drweb.iniファイルを開き、未知の（サポートされていない）セクションを削除します。ファイルを保存し、次のコマンドを実行することで[Dr.Web ConfigD](#)設定デモンを再起動させます。

```
# service drweb-configd restart
```

2. 問題が解決しない場合は、Dr.Web for UNIX File Servers設定をデフォルトに戻してしてください。

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モンを再起動させます。

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](#)内のパラメータの1つに、無効な値が含まれています。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

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。
 - [Webインターフェース](#)のコンポーネント設定のあるページ（インストールされている場合）。
 - **drweb-ctlcfshow**および**drweb-ctlcfset**[コマンド](#)を使用します。

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. 設定ファイル <etc_dir>/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エディター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、有効な値を設定してください。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 ConfigD](#)設定デモンを再起動させます。



```
# service drweb-configd restart
```

3. この手順で問題が解決しない場合は、Dr.Web for UNIX File Servers設定をデフォルトに戻してください。

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。

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 UNIX File Serversまたはコンポーネントの1つが無効な状態であるため、必要な操作を完了できません。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

エラーの解決:

- 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、以下のコマンドを実行することでDr.Web for UNIX File Servers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](#)内のパラメータの1つに、値のリストが含まれています。含むことができるのは1つの値のみです。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

エラーの解決:

- 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。
 - [Webインターフェース](#)のコンポーネント設定のあるページ（インストールされている場合）。
 - [drweb-ctlcfshow](#)および[drweb-ctlcfset](#)[コマンド](#)を使用します。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. 設定ファイル `<etc_dir>/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エディター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、有効な値を設定してください。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 ConfigD](#) 設定デーモンを再起動させます。

```
# service drweb-configd restart
```

3. この手順で問題が解決しない場合は、Dr.Web for UNIX File Servers 設定をデフォルトに戻してください。

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。

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：無効なタグ値です。

エラーコード：x71

説明：ユニークなタグ識別子を含んだ名前を持つ [設定ファイル](#) 内のセクションの1つに、無効なタグ識別子があります。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Servers ログをご確認ください（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](#) ログを使用することもできます。

エラーの解決：

1. [Webインターフェース](#) 内にセクションを作成しようとした際、または [コマンド](#) の使用中にエラーが発生した場合

```
# drweb-ctl cfset <section>.<parameter> <new value>
```

タグに有効な値を設定し、セクションを再度保存します。

2. セクションが設定ファイル `<etc_dir>/drweb.ini` に直接保存されている場合は、ファイルを編集します。これを行うには、いずれかのテキストエディターで設定ファイルを開き、無効なタグ値を含むセクション名を見つけて、タグに有効な値を設定します。ファイルを保存し、次のコマンドを実行することで [Dr.Web ConfigD](#) 設定デーモンを再起動させます。

```
# service drweb-configd restart
```

3. この手順で問題が解決しない場合は、Dr.Web for UNIX File Servers 設定をデフォルトに戻してください。

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。

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: 脅威のレコードにアクセスしようとした際に、レコードがないことが明らかになりました(脅威を処理したのが別のDr.Web for UNIX File Serversコンポーネントであった可能性があります)。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog](#)を使用することもできます。

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: 脅威のレコードにアクセスしようとした際に、レコードが別のコンポーネントによって処理中であることが明らかになりました。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog](#)を使用することもできます。

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: 検出された脅威を含むファイルを隔離に移動しようとした際に、ファイルがすでに隔離されていることが明らかになりました(脅威が別のコンポーネントによって処理された可能性があります)。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog](#)を使用することもできます。

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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください (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-ctllog](#)を使用することもできます。

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)。
 - パスを表示および変更するには、[Webインターフェース](#)の **Updater** ページに移動します (インストールされている場合)。
 - 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.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. ウイルスデータベースを更新します。
 - Webインターフェースがインストールされている場合は、[Webインターフェース](#)のメインページで更新をクリックします。
 - または、[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、Dr.Web Updaterコンポーネントを実行しているアカウントのユーザーが、BackupDirで指定された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てください。このユーザーの名前は、RunAsUserパラメータで指定されます。必要に応じて、RunAsUserパラメータで指定されているユーザーを変更するか、ディレクトリのプロパティで足りない権限を付与します。
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 UNIX File Serversまたはその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 UNIX File ServersをインストールするおよびDr.Web for UNIX File Servers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ファイルの1つで、整合性違反が検出されました。



エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

エラーの解決：

1. サーバーのリストを含むファイルへのパスを確認し、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 *Dr1Dirを持つパラメータ）。
 - パスを表示および変更するには、[Webインターフェース](#)の **Updater** ページに移動します（インストールされている場合）。
 - 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表示するには、コマンドを使用します（<*Dr1DirPath>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[.<*Dr1Dir>]
```

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（<*Dr1Dir>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.<*Dr1Dir> <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（<*Dr1Dir>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.<*Dr1Dir> -r
```

2. ウイルスデータベースを更新します。
 - Webインターフェースがインストールされている場合は、[Webインターフェース](#)のメインページで更新をクリックします。
 - または、[コマンド](#)を実行します。

```
$ drweb-ctl update
```

3. 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 UNIX File Serversまたはその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 UNIX File Serversをインストールする](#)および[Dr.Web for UNIX File Servers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で、整合性違反が検出されました。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

**エラーの解決：**

- しばらく時間をおいて再度ウイルスデータベースを更新します。

- Webインターフェースがインストールされている場合は、[Webインターフェース](#)のメインページで更新をクリックします。
- または、[コマンド](#)を実行します。

```
$ drweb-ctl update
```

- 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 UNIX File Serversまたはその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 UNIX File Serversをインストールする](#)および[Dr.Web for UNIX File Servers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：更新が含まれているダウンロードされたファイルで、整合性違反が検出されました。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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。

エラーの解決：

- しばらく時間をおいて再度ウイルスデータベースを更新します。

- Webインターフェースがインストールされている場合は、[Webインターフェース](#)のメインページで更新をクリックします。
- または、[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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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。

エラーの解決：

- プロキシサーバーへの接続に使用されているパラメータを確認します（[設定ファイル](#)の [Update] [セクション](#)のProxyパラメータで設定されています）。



- 接続パラメータを表示および設定するには、[Webインターフェース](#)の **Updater** ページに移動します（インストールされている場合）。
 - 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. ウイルスデータベースを更新します。

- Webインターフェースがインストールされている場合は、[Webインターフェース](#)のメインページで更新をクリックします。
- または、[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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

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. プロキシサーバーのみを使用してネットワークにアクセスできる場合は、プロキシサーバーに接続するためのパラメータを設定します（[設定ファイル](#)の [Update] [セクション](#)の **Proxy**パラメータで設定できます）。
- 接続パラメータを表示および設定するには、[Webインターフェース](#)の **Updater** ページに移動します（インストールされている場合）。
 - 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*Dr1Dirで表示されます。
*CustomDr1Dir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*Dr1Dirパラメータで指定されている値は無視されます)。

- 接続パラメータを表示および設定するには、[Webインターフェース](#)の **Updater** ページに移動します(インストールされている場合)。
- 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表示するには、コマンドを使用します(<*Dr1DirPath>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[.<*Dr1Dir>]
```

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(<*Dr1Dir>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.<*Dr1Dir> <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(<*Dr1Dir>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.<*Dr1Dir> -r
```

4. ウイルスデータベースを更新します。

- Webインターフェースがインストールされている場合は、[Webインターフェース](#)のメインページで更新をクリックします。
- または、[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

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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。
 - キーファイルへのパスを表示および設定するには、[Webインターフェース](#)の全般設定ページに移動します(インストールされている場合)。



- 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、または使用している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](#)を参照してください。
3. キーファイルをインストールするには、[Webインターフェース](#)のメインページの下部にあるライセンス有効化フォームを使用できます（インストールされている場合）。
4. また、<https://support.drweb.com/get+cabinet+link/>のユーザーのWebページ**My Dr.Web**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: ライセンスは有効期限が切れています。

エラーコード: x96

説明: 使用しているライセンスは有効期限が切れています。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

エラーの解決:

1. 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ます。ライセンスの購入方法とキーファイルのインストールの詳細については、管理者マニュアルの[ライセンス](#)を参照してください。
2. 購入したキーファイルをインストールするには、[Webインターフェース](#)のメインページの下部にあるライセンス有効化フォームを使用できます（インストールされている場合）。
3. また、<https://support.drweb.com/get+cabinet+link/>のユーザーのWebページ**My Dr.Web**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想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）。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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）。



す)。また、[コマンドdrweb-ctllog](#)を使用することもできます。

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：無効なチェックサムです。

エラーコード：x98

説明：更新が含まれているダウンロードされたファイルのチェックサムが検出されました。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

エラーの解決：

1. しばらく時間をおいて再度ウイルスデータベースを更新します。
 - Webインターフェースがインストールされている場合は、[Webインターフェース](#)のメインページで更新をクリックします。
 - または、[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：使用されている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）。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

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。ライセンスの購入方法とキーファイルのインストールの詳細については、管理者マニュアルの[ライセンス](#)を参照してください。
2. 購入したキーファイルをインストールするには、[Webインターフェース](#)のメインページの下部にあるライセンス有効化フォームを使用できます（インストールされている場合）。
3. また、<https://support.drweb.com/get+cabinet+link/>のユーザーのWebページMy Dr.Web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: 使用されているライセンスはブロックされています (Dr.Web for UNIX File Serversの使用に関するライセンス使用許諾契約の条件に違反している可能性があります)。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください (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-ctllog](#)を使用することもできます。

エラーの解決:

1. 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ます。ライセンスの購入方法とキーファイルのインストールの詳細については、管理者マニュアルの[ライセンス](#)を参照してください。
2. 受領したキーファイルをインストールするには、[Webインターフェース](#)のメインページの下部にあるライセンス有効化フォームを使用できます (インストールされている場合)。
3. また、<https://support.drweb.com/get+cabinet+link/>のユーザーのWebページMy Dr.Web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: 使用されているライセンスが別の製品のものであるか、Dr.Web for UNIX File Servers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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください (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-ctllog](#)を使用することもできます。

エラーの解決:

1. 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ます。ライセンスの購入方法とキーファイルのインストールの詳細については、管理者マニュアルの[ライセンス](#)を参照してください。
2. 受領したキーファイルをインストールするには、[Webインターフェース](#)のメインページの下部にあるライセンス有効化フォームを使用できます (インストールされている場合)。
3. また、<https://support.drweb.com/get+cabinet+link/>のユーザーのWebページMy Dr.Web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 UNIX File Servers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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください (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-ctllog](#)を使用することもできます。



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. 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、コンポーネント操作に選択されたモードがOSによってサポートされていない可能性があります。選択したモードを確認し、必要に応じて変更してください。自動の値(設定ファイルの[LinuxSpider]セクションにあるモードパラメータ)を設定することができます。

- モードを表示、変更するには、[Webインターフェース](#)のSpIDer Guardページに移動します(インストールされている場合)。
- 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。

AUTOの値を設定するには、以下のコマンドを実行します。

```
# Dr.Web 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。

```
# Dr.Web 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[手動で構築してインストール](#)します。



SpIDer Guardおよびローダブルカーネルモジュールの動作は、テスト済みのUNIXディストリビューションでのみ保証されています(管理者マニュアルの「[システム要件と互換性](#)」のセクションを参照してください)。

エラーが別のコンポーネントによって発生している場合、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てください。

- [Webインターフェース](#)のコンポーネント設定のあるページ(インストールされている場合)。
 - `drweb-ctlcfshow`および`drweb-ctlcfset`[コマンド](#)を使用します。
 - 手動で[設定ファイル](#)を編集してください(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してください)。
3. この手順で問題が解決しない場合は、Dr.Web for UNIX File Servers設定をデフォルトに戻してください。

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、次のコマンドを実行することでDr.Web for UNIX File Servers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、または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 UNIX File Serversコンポーネントの1つを実行できません。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

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 UNIX File Servers設定ファイル内でコンポーネントの実行可能パスを確認してください（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。

Dr.Web for UNIX File Serversまたはその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 UNIX File Serversをインストールする](#)および[Dr.Web for UNIX File Servers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を使用することができません

エラーコード：x105

説明：Dr.Web Virus-Finding Engineのファイルが見つからないか使用できません（脅威の検出に必要です）。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

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）。
 - パスを表示および変更するには、[Webインターフェースの全般設定ページ](#)に移動します（インストールされている場合）。
 - 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.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. ウイルスデータベースを更新します。

- Webインターフェースがインストールされている場合は、[Webインターフェース](#)のメインページで更新をクリックします。
- または、[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。

Dr.Web for UNIX File Serversまたはその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 UNIX File Serversをインストールする](#)および[Dr.Web for UNIX File Servers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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

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VirusBaseDirVirusBaseDirパラメータ）。
 - パスを表示および変更するには、[Webインターフェース](#)の全般設定ページに移動します（インストールされている場合）。
 - 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.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. ウイルスデータベースを更新します。

- Webインターフェースがインストールされている場合は、[Webインターフェース](#)のメインページで更新をクリックします。



リックします。

- または、[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)

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog](#)を使用することもできます。

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。
 - [Webインターフェース](#)のコンポーネント設定のあるページ(インストールされている場合)。
 - `drweb-ctlcfshow`および`drweb-ctlcfset`[コマンド](#)を使用します。
 - 手で[設定ファイル](#)を編集してください(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してください)。
3. 問題が解決しない場合は、Dr.Web for UNIX File Servers設定をデフォルトに戻してしてください。

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、次のコマンドを実行することでDr.Web for UNIX File Servers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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog](#)を使用することもできます。

**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。
 - [Webインターフェース](#)のコンポーネント設定のあるページ(インストールされている場合)。
 - **drweb-ctlcfshow**および**drweb-ctlcfset**[コマンド](#)を使用します。
 - 手動で[設定ファイル](#)を編集してください(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してください)。
3. 問題が解決しない場合は、Dr.Web for UNIX File Servers設定をデフォルトに戻してしてください。
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、次のコマンドを実行することでDr.Web for UNIX File Serversを再起動させます。

```
# service drweb-configd restart
```

4. Dr.Web for UNIX File Servers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。
Dr.Web for UNIX File Serversまたはその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 UNIX File Serversをインストールする](#)および[Dr.Web for UNIX File Servers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 UNIX File Serversコンポーネントは動作していません。このソフトウェアはコンポーネントの正しい動作を中断します。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog](#)を使用することもできます。

エラーの解決：

1. 無効にするか再設定し、Dr.Web for UNIX File Servers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： *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。



エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

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 自動 の値（[設定ファイル](#)の[LinuxSpider][セクション](#)内の モード パラメータ）を設定し、変更してください。
 - モードを表示、変更するには、[Webインターフェース](#)のSpIDer Guardページに移動します（インストールされている場合）。
 - 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。

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 Guard用のロードブルカーネルモジュールを[手動で構築してインストールします](#)。



SpIDer Guardおよびロードブルカーネルモジュールの動作は、テスト済みのUNIXディストリビューションでのみ保証されています（管理者マニュアルの「[システム要件と互換性](#)」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: *LookupDを使用することができません。*

エラーコード: x115

説明: Dr.Web LookupDコンポーネントが見つかりません（外部ソースからデータを選択する必要があります）

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください（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-ctllog](#)を使用することもできます。

エラーの解決：

1. **drweb-lookupd**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[LookupD][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 LookupD.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 LookupD.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 LookupD.ExePath -r
```

2. 設定にDr.Web LookupD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-lookupd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。

Dr.Web for UNIX File Serversまたはその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 UNIX File ServersをインストールするおよびDr.Web for UNIX File Servers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を使用することができません。*

エラーコード: x119

説明: Dr.Web Scanning Engineコンポーネントが見つからないか、起動に失敗しました(脅威の検出に必要です)。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog](#)を使用することもできます。

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 /
```

行「エラー: 有効なライセンスが指定されていません」が出力された場合、有効なキーファイルがありません。Dr.Web for UNIX File Serversを登録してライセンスを取得します。ライセンスを取得したら、[キーファイル](#)が使用可能かどうかを確認し、必要に応じてインストールします。

- お使いのOSがSELinuxを使用している場合、**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Dr.Web Scanning Engine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。

Dr.Web for UNIX File Serversまたはその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 UNIX File Serversをインストールする](#)および[Dr.Web for UNIX File Servers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: *File Checkerを使用することができません。*

エラーコード: x120

説明: Dr.Web File Checkerコンポーネントが見つからないか、起動に失敗しました(脅威の検出に必要です)。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog](#)を使用することもできます。

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がSELinuxを使用している場合、**drweb-filecheck**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Dr.Web File Checker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。

Dr.Web for UNIX File Serversまたはその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 UNIX File Serversをインストールする](#)および[Dr.Web for UNIX File Servers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を使用することができません。*

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)。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog](#)を使用することもできます。

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Dr.Web ES Agent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。

Dr.Web for UNIX File Serversまたはその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 UNIX File Serversをインストールする](#)および[Dr.Web for UNIX File Servers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*を使用することができません。

エラーコード: x123

説明: Dr.Web Network Checkerコンポーネントがありません(ダウンロードしたファイルのスキャンに必要です)。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog](#)を使用することもできます。

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Dr.Web Network Checker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。

Dr.Web for UNIX File Serversまたはその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 UNIX File ServersをインストールするおよびDr.Web for UNIX File Servers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を使用することができません。*

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)。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください(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-ctllog](#)を使用することもできます。

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Dr.Web CloudD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。

Dr.Web for UNIX File Serversまたはその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 UNIX File ServersをインストールするおよびDr.Web for UNIX File Servers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。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX File Serversログをご確認ください (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-ctllog](#)を使用することもできます。

エラーの解決:

1. 以下のコマンドを入力し、Dr.Web for UNIX File Servers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	カーネルモジュールSpIDer Guardのインストール後、OSがカーネルエラー「 <i>Kernel panic</i> 」で異常終了します。
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。	
<pre>drweb.blacklist=yes</pre>	
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、追加のモジュールの /lib/' <code>uname-r</code> '/extraディレクトリからdrweb.koモジュールを削除します。	
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。	
<pre># drweb-ctl cfset LinuxSpider.Mode AUTO # drweb-ctl reload</pre>	
4. 使用しているOSが fanotify をサポートしていないか、このモードでファイルシステムを完全に管理するSpIDer Guardの使用が許可されていない場合 (実際は Astra Linux SE などの必須アクセスモデルの GNU/Linux ファミリー)、ファイルシステム管理には LKM モードを使用する必要があります。 Xen ハイパーバイザーでは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 MailD、SpIDer Gate、Dr.Web ICAPD(表示されるコンポーネントのリストはインストールされている製品によって異なります)はメッセージをスキャンしません。Dr.Web for UNIX File Serversログにメッセージ「開いているファイルが多すぎます」が表示されます。
説明：	データスキャンの負荷が大きいため、Dr.Web Network Checkerは利用可能なファイル記述子(ディスクリプタ)数の上限に達しました。
エラーの解決：	
1. ulimit -n コマンドを使用してアプリケーションで使用可能なオープンファイルの記述子数上限を引き上げます(Dr.Web for UNIX File Serversの記述子数のデフォルト上限は16384です)。 場合によっては、システムサービス systemd は指定した上限の変更を無視できます。この場合、ファイル/etc/systemd/system/drweb-configd.service.d/limits.confを編集し(ない場合は作成して)、変更後の上限値を指定します。 <pre>[Service] LimitNOFILE=16384</pre> systemd の利用可能な上限のリストはドキュメント man systemd.exec で確認できます。	
2. 上限を変更したら、次のコマンドを実行してDr.Web for UNIX File Serversを再起動します。 <pre># service drweb-configd restart</pre>	
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：	WebブラウザはDr.Web管理Webインターフェースへの接続を確立できません。Dr.Webアンチウイルスソリューションのコンポーネントは実行中のプロセスのリスト(ps ax grep drweb)に含まれていません。 drweb-ctl rawscan 以外の drweb-ctl<command> を実行しようすると、次のいずれかのエラーが発生します。 Error: connect: No such file or directory: "<path>/ .com.drweb.public" または Error: connect: Connection refused: "<path>/com.drweb.public".
説明：	設定デーモンDr.Web ConfigDが使用できないため、Dr.Web for UNIX File Serversを起動できません。
エラーの解決：	
1. 次のコマンドを実行します。 <pre># service drweb-configd restart</pre> Dr.Web ConfigDとDr.Web for UNIX File Serversを再起動します。	
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。	



これは**PAM**認証がシステムで使用されていないことを意味する場合があることにも注意してください。その場合は、PAMをインストールして設定します（Dr.Web for UNIX File Serversは**PAM**がないと正しく動作できません）。

- エラーが解決しない場合は、Dr.Web for UNIX File Serversを削除してから再度インストールしてください。

Dr.Web for UNIX File Serversまたはその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 UNIX File Serversをインストールする](#)および[Dr.Web for UNIX File Servers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。

エラーの内部カタログ

エラーコード	シンボリック文字・記号	エラーについての内部メッセージ	説明
0	EC_OK	成功	これはエラーではありません
1	EC_MONITOR_IPC_ERROR	モニターチャネルに関するエラー	エラーx1
2	EC_ALREADY_IN_PROGRESS	操作はすでに実行中です	エラーx2
3	EC_IN_PENDING_STATE	操作は保留中です	エラーx3
4	EC_INTERRUPTED_BY_USER	ユーザーによって中断されました	エラーx4
5	EC_CANCELED	操作がキャンセルされました	エラーx5
6	EC_LINK_DISCONNECTED	リンクが切断されました	エラーx6
7	EC_BAD_MESSAGE_SIZE	無効なIPCメッセージサイズです	エラーx7
8	EC_BAD_MESSAGE_FORMAT	無効なIPCメッセージフォーマットです	エラーx8
9	EC_NOT_READY	準備が完了していません	エラーx9
10	EC_NOT_INSTALLED	コンポーネントがインストールされていません	エラーx10
11	EC_UNEXPECTED_MESSAGE	予期せぬIPCメッセージです	エラーx11
12	EC_PROTOCOL_VIOLATION	プロトコル違反です	エラーx12
13	EC_UNKNOWN_STATE	サブシステムの状態が未知です	エラーx13
20	EC_NOT_ABSOLUTE_PATH	パスは絶対パスでなければなりません	エラーx20
21	EC_NO_MEMORY	十分なメモリがありません	エラーx21
22	EC_IO_ERROR	IOエラー	エラーx22



エラーコード	シンボリック文字・記号	エラーについての内部メッセージ	説明
23	EC_NO_SUCH_ENTRY	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x23
24	EC_PERMISSION_DENIED	パーミッションが拒否されました	エラーx24
25	EC_NOT_A_DIRECTORY	ディレクトリではありません	エラーx25
26	EC_DATA_CORRUPTED	データファイルが破損しています	エラーx26
27	EC_FILE_EXISTS	ファイルはすでに存在しています	エラーx27
28	EC_READ_ONLY_FS	読み取り専用ファイルシステム	エラーx28
29	EC_NETWORK_ERROR	ネットワークエラー	エラーx29
30	EC_NOT_A_DRIVE	ドライブではありません	エラーx30
31	EC_UNEXPECTED_EOF	予期せぬEOFがあります	エラーx31
32	EC_FILE_WAS_CHANGED	ファイルが変更されています	エラーx32
33	EC_NOT_A_REGULAR_FILE	通常ファイルではありません	エラーx33
34	EC_NAME_ALREADY_IN_USE	名前はすでに使用されています	エラーx34
35	EC_HOST_OFFLINE	ホストがオフラインです	エラーx35
36	EC_LIMIT_REACHED	リソースの上限に達しています	エラーx36
37	EC_CROSS_DEVICE_LINK	マウントポイントが異なります	エラーx37
38	EC_UNPACKING_ERROR	アンパックエラー	エラーx38
40	EC_BASE_CORRUPTED	ウイルスデータベースが破損しています	エラーx40
41	EC_OLD_BASE_VERSION	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x41
42	EC_EMPTY_BASE	ウイルスデータベースが空です	エラーx42
43	EC_CAN_NOT_BE_CURED	オブジェクトを修復できません	エラーx43
44	EC_INVALID_BASE_SET	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x44
45	EC_SCAN_LIMIT_REACHED	スキャンの上限に達しています	エラーx45
47	EC_AUTH_FAILED	認証に失敗しました	エラーx47
48	EC_NOT_AUTHORIZED	認証に失敗しました	エラーx48



エラーコード	シンボリック文字・記号	エラーについての内部メッセージ	説明
49	EC_INVALID_TOKEN	無効なアクセストークンです	エラーx49
60	EC_INVALID_ARGUMENT	無効な引数です	エラーx60
61	EC_INVALID_OPERATION	無効な操作です	エラーx61
62	EC_ROOT_ONLY	スーパーユーザー権限が必要です	エラーx62
63	EC_STANDALONE_MODE_ONLY	集中管理モードでは許可されていません。	エラーx63
64	EC_NON_SUPPORTED_OS	サポートされていないOSです	エラーx64
65	EC_NOT_IMPLEMENTED	実装されていない機能です	エラーx65
66	EC_UNKNOWN_OPTION	未知のオプションです	エラーx66
67	EC_UNKNOWN_SECTION	未知のセクションです	エラーx67
68	EC_INVALID_OPTION_VALUE	無効なオプション値です	エラーx68
69	EC_INVALID_STATE	無効な状態です	エラーx69
70	EC_NOT_LIST_OPTION	使用可能な値は1つのみです	エラーx70
71	EC_INVALID_TAG	無効なタグ値です	エラーx71
80	EC_RECORD_NOT_FOUND	レコードが見つかりません	エラーx80
81	EC_RECORD_BUSY	レコードは現在処理中です	エラーx81
82	EC_QUARANTINED_FILE	ファイルはすでに隔離済みです	エラーx82
89	EC_BACKUP_FAILED	更新前にバックアップを行うことができません	エラーx89
90	EC_BAD_DRL_FILE	無効なDRLファイルです	エラーx90
91	EC_BAD_LST_FILE	無効なLSTファイルです	エラーx91
92	EC_BAD_LZMA_FILE	無効な圧縮ファイルです	エラーx92
93	EC_PROXY_AUTH_ERROR	プロキシ認証エラーです	エラーx93
94	EC_NO_UPDATE_SERVERS	使用可能な更新サーバーがありません	エラーx94
95	EC_BAD_KEY_FORMAT	キーファイルのフォーマットが無効です	エラーx95
96	EC_EXPIRED_KEY	ライセンスは有効期限が切れています	エラーx96
97	EC_NETWORK_TIMEOUT	ネットワークオペレーションのタイムアウト	エラーx97



エラーコード	シンボリック文字・記号	エラーについての内部メッセージ	説明
98	EC_BAD_CHECKSUM	無効なチェックサムです	エラーx98
99	EC_BAD_TRIAL_KEY	無効なトライアルライセンス	エラーx99
100	EC_BLOCKED_LICENSE	ブロックされているライセンスキーです	エラーx100
101	EC_BAD_LICENSE	無効なライセンスです	エラーx101
102	EC_BAD_CONFIG	無効な設定です	エラーx102
104	EC_BAD_EXECUTABLE	無効な実行ファイルです	エラーx104
105	EC_NO_CORE_ENGINE	コアエンジンは使用できません	エラーx105
106	EC_NO_VIRUS_BASES	ウイルスデータベースがありません	エラーx106
107	EC_APP_TERMINATED	プロセスはシグナルによって中断されました	エラーx107
108	EC_APP_CRASHED	予期せぬプロセスの中断です	エラーx108
109	EC_INCOMPATIBLE	互換性のないソフトウェアが検出されました	エラーx109
113	EC_NO_KERNEL_MODULE	カーネルモジュールは使用できません	エラーx113
115	EC_NO_LOOKUPD	LookupDは使用できません	エラーx115
119	EC_NO_SCAN_ENGINE	ScanEngineは使用できません	エラーx119
120	EC_NO_FILE_CHECK	FileCheckは使用できません	エラーx120
121	EC_NO_ESAGENT	ESAgentは使用できません	エラーx121
123	EC_NO_NET_CHECK	NetCheckは使用できません	エラーx123
124	EC_NO_CLOUDD	CloudDを使用できません	エラーx124
125	EC_UNEXPECTED_ERROR	予期せぬエラーです	エラーx125

付録G. 略語のリスト

このマニュアルでは、以下の用語は説明なしに使用されます。

文字・記号	説明
AD	Microsoft Active Directory
DN	(LDAP) Distinguished Name (識別名)



文字・記号	説明
<i>EPM</i>	ESP Package Manager (ESPパッケージマネージャー)
<i>FQDN</i>	Fully Qualified Domain Name (完全修飾ドメイン名)
<i>GID</i>	Group ID (システムユーザーグループID)
<i>GNU</i>	GNUプロジェクト (GNU is Not Unix)
<i>HTML</i>	HyperText Markup Language (ハイパーテキストマークアップ言語)
<i>HTTP</i>	HyperText Transfer Protocol (ハイパーテキスト転送プロトコル)
<i>HTTPS</i>	HyperText Transfer Protocol Secure (SSL/TLS経由)
<i>ID</i>	ID (識別子)
<i>IP</i>	Internet Protocol (インターネットプロトコル)
<i>LDAP</i>	Lightweight Directory Access Protocol (ライトウェイトディレクトリ アクセスプロトコル)
<i>LKM</i>	Linux Kernel Module (Linuxカーネルモジュール)
<i>MBR</i>	Master Boot Record (マスターブートレコード)
<i>NSS</i>	Novell Storage Services (Novellストレージサービス)
<i>OID</i>	(SNMP) Object ID (オブジェクトID)
<i>PID</i>	Process ID (システムプロセスID)
<i>PAM</i>	Pluggable Authentication Modules (プラグブル認証モジュール)
<i>RPM</i>	Red Hat Package Manager (Red Hatパッケージマネージャー)
<i>RRA</i>	Round-Robin Archive (ラウンドロビンアーカイブ)
<i>RRD</i>	Round-Robin Database (ラウンドロビンデータベース)
<i>SMB</i>	Server Message Block (ファイルアクセスプロトコル)
<i>SNMP</i>	Simple Network Management Protocol (シンプルネットワークマネジメントプロトコル)
<i>SP</i>	Service Pack (サービスパック)
<i>SSH</i>	Secure Shell (セキュアシェル)
<i>SSL</i>	Secure Sockets Layer (セキュアソケットレイヤー)
<i>TCP</i>	Transmission Control Protocol (伝送制御プロトコル)



文字・記号	説明
<i>TLS</i>	Transport Layer Security(トランスポート層セキュリティ)
<i>UID</i>	User ID(システムユーザーID)
<i>URI</i>	Uniform Resource Identifier(ユニフォームリソースアイデンティファイア)
<i>URL</i>	Uniform Resource Locator(ユニフォームリソースロケータ)
<i>VBR</i>	Volume Boot Record(ボリュームブートレコード)
<i>OS</i>	Operating System(オペレーティングシステム)
<i>FS</i>	File System(ファイルシステム)

