



Dr.WEB
for UNIX Mail 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 Mail Servers

バージョン**11.1**

管理者マニュアル

2020/10/12

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 Mail Serversの構成	14
隔離に移動する	21
ファイルのパーミッションと権限	22
動作モード	23
システム要件と互換性	27
ライセンス	31
インストールとアンインストール	32
Dr.Web for UNIX Mail Serversをインストールする	33
ユニバーサルパッケージをインストールする	33
コマンドラインからインストールする	35
リポジトリからインストールする	35
Dr.Web for UNIX Mail Serversをアップグレードする	38
最新のアップデートを入手する	38
新しいバージョンにアップグレードする	39
Dr.Web for UNIX Mail Serversをアンインストールする	41
ユニバーサルパッケージをアンインストールする	42
コマンドラインからアンインストールする	42
リポジトリからインストールしたDr.Web for UNIX Mail Serversをアンインストールする	42
追加情報	45
Dr.Web for UNIX Mail Serversパッケージとファイル	45
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	48
セキュリティサブシステムを設定する	54
SELinux セキュリティポリシーを設定する	54
開始する	57
製品の登録と有効化	58
製品の動作確認	60
フィルターとしてのMTAとの統合	61
SMTPプロキシモードでDr.Web for UNIX Mail Serversを使用する	68
透過プロキシモードでDr.Web for UNIX Mail Serversを使用する	69



簡単な説明	73
Dr.Web for UNIX Mail Serversコンポーネント	77
Dr.Web ConfigD	77
動作原理	77
コマンドライン引数	78
設定パラメータ	79
Dr.Web Ctl	82
コマンドラインフォーマット	84
使用例	109
設定パラメータ	113
Dr.Web Web管理インターフェース	114
コンポーネントを管理する	116
脅威の管理	116
設定を管理する	118
集中管理モードの管理	122
ローカルファイルをスキャンする	123
メールアーカイブのパスワードを復元する	126
Dr.Web MailD	127
動作原理	128
コマンドライン引数	129
設定パラメータ	130
メールシステムとの統合	137
Luaでのメール処理	137
Dr.Web Anti-Spam	185
動作原理	185
コマンドライン引数	186
設定パラメータ	187
SpIDer Gate	190
動作原理	191
コマンドライン引数	192
設定パラメータ	192
Dr.Web Firewall for Linux	195
動作原理	195
コマンドライン引数	200
設定パラメータ	200
Luaでの接続処理	224



Dr.Web ClamD	233
動作原理	233
コマンドライン引数	233
設定パラメータ	234
外部アプリケーションとの統合	239
Dr.Web File Checker	242
動作原理	242
コマンドライン引数	243
設定パラメータ	243
Dr.Web Network Checker	246
動作原理	246
コマンドライン引数	248
設定パラメータ	249
スキャンクラスタを作成する	253
Dr.Web Scanning Engine	257
動作原理	257
コマンドライン引数	258
設定パラメータ	260
Dr.Web Updater	262
動作原理	262
コマンドライン引数	263
設定パラメータ	264
Dr.Web ES Agent	270
動作原理	270
コマンドライン引数	270
設定パラメータ	271
Dr.Web HTTPD	274
動作原理	274
コマンドライン引数	275
設定パラメータ	276
HTTP APIの説明	279
Dr.Web SNMPD	303
動作原理	303
コマンドライン引数	305
設定パラメータ	305
SNMPモニタリングシステムとの統合	309





Dr.Web SNMP MIB	317
Dr.Web MeshD	345
動作原理	345
コマンドライン引数	348
設定パラメータ	349
Dr.Web CloudD	353
動作原理	353
コマンドライン引数	354
設定パラメータ	354
Dr.Web LookupD	356
動作原理	356
コマンドライン引数	357
設定パラメータ	358
Dr.Web StatD	370
動作原理	370
コマンドライン引数	370
設定パラメータ	371
付録	373
付録 A. コンピューター脅威の種類	373
付録 B. コンピューター脅威の駆除	377
付録 C. テクニカルサポート	380
付録 D. Dr.Web for UNIX Mail Servers 設定ファイル	382
ファイル構造	382
パラメータタイプ	384
付録 E. SSL 証明書を生成する	387
付録 F. 既知のエラー	390
付録 G. 略語のリスト	440



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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail Serversは、UNIX(**GNU/Linux**、**FreeBSD**)で実行されているメールサーバーやプロキシを、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 Mail 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 Mail 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 Mail 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 Mail 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」デバイスの場合には、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には、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. メールメッセージのスキャン。Dr.Web for UNIX Mail Serversは、次のメールメッセージスキャンのモードをサポートしています。

- **メールサーバー (MTA) に接続された外部フィルターのモード。** Dr.Web for UNIX Mail Serversは、外部フィルター (*Milter*、*Spamd*、*Rspamd*) との接続用のインターフェースをサポートするメールサーバーに統合できます。フィルターモードでは、MTAが主導して、メールサーバーに届いたすべてのメールが有効化されたインターフェースを経由してDr.Web for UNIX Mail Serversに送信され、スキャンされます。インターフェースの機能に応じて、フィルターとして動作するDr.Web for UNIX Mail Serversは次のことが可能です。
 - **メールスキャンの結果をサーバーに通知します。** この場合、メールサーバーは受信した結果に従ってメールメッセージを個別に処理する必要があります（スキャン結果に脅威の存在に関する情報が含まれている場合は、配信を拒否する、ヘッダーを追加する、またはメールの内容を変更します）。
 - **メッセージを受信または拒否するコマンドをメールサーバーに送信します。**
 - **指定されたヘッダーを追加するか、検出された悪意のあるコンテンツや不要なコンテンツを削除して、メールメッセージを変更します。** 削除された悪意のあるコンテンツは、パスワードで保護されたアーカイブとしてメールメッセージに添付されます。メールメッセージの受信者は、保護されたアーカイブを解凍するためのパスワードをメールサーバー管理者に要求できます。推奨されませんが、必要に応じて、管理者はパスワードで保護されていないアーカイブの使用を設定できます。



メールサーバーへのコマンドの送信または変更されたメッセージの返信は、*Milter*インターフェースでのみサポートされます。*Spamd*と*Rspamd*では、Dr.Web for UNIX Mail Serversがサーバーにコマンドを送信し、変更されたメールメッセージを返すことはできません。「メールメッセージはスパムです」または「メールメッセージはスパムではありません」という2つの判定のうち1つがサーバーに返されます。このようなメッセージの処理に関するすべてのアクション（メールヘッダーの追加や変更、メッセージの拒否、受信者への送信など）は、*MTA側の設定*で定義する必要があります。

メールメッセージが拒否された理由、MTAがメールメッセージに適用する必要があるアクションをMTAに返すために、テキスト変数（*Spamd*には *report*、*Rspamd*には *action*）が使用されます。これはMTA設定で処理できる、LUAメッセージ処理手順によって返されます（たとえば、*Exim*ではACL）。

- **SMTPプロキシモード**は、1つまたは複数のMTAやMDAにさらに転送したSMTPトラフィックを迂回してスキャンします。実際には、このモードは前のモードと似ています。Dr.Web for UNIX Mail Serversが（*Milter*、*Spamd*、または*Rspamd*を使用して）MTA（たとえば**Postfix**）に接続され、このMTAは他のMTAにメールメッセージを送信するようにカスタマイズされています（たとえば、さまざまなドメイン宛てのメッセージルーティングの実行など）。
- **メールプロトコルの透過プロキシモード**。このモードでは、Dr.Web for UNIX Mail Serversは（SpIDer Gateコンポーネントを使用して）共有相手に対して透過的にMTAやMUAの間でデータを共有するためのチャンネルに埋め込まれたプロキシサーバーの機能と送信済みメッセージのスキャナの機能を実装します。製品は主なメールプロトコル（SMTP、POP3、IMAP）に透過的に組み込むことができます。このモードでは、組み込まれているプロトコルにもよりますが、Dr.Web for UNIX Mail Serversが受信者にメールメッセージを送信（未変更、またはヘッダーの追加やリパックされたメールメッセージの形式で変更した状態）する、あるいはその配信をブロックすることができます。これには送信者または受信者への適切なプロトコルエラーの返信も含まれます。



透過プロキシモードは、**GNU/Linux**でのみ使用できます。

Dr.Web for UNIX Mail Serversは単体で動作可能なメールサーバーではないため、プロキシモードで動作させるには、Dr.Web for UNIX Mail Serversが動作する同じホストにメールサーバー（MTA）をインストールする必要があります。

Dr.Web for UNIX Mail Serversはディストリビューションと設定に応じて、メールメッセージのスキャンを実行します。

- 脅威を含む**悪意のある添付ファイルの検出**。
- **悪意のあるWebサイトまたは望ましくないカテゴリーに属するWebサイトへのリンクの検索**。
- **フィッシングとスパムの兆候の検出**（DKIMテクノロジー、スパムフィルタリングの自動的に更新されたルールデータベース、DNSxLブラックリスト内の送信者のアドレスの存在をチェックするメカニズムを使用）。
- メールシステムの**管理者が独自に設定したセキュリティ基準への準拠**（正規表現を使用したメッセージ本文とヘッダーのスキャン）。

メールメッセージに含まれている望ましくないWebサイトへのリンクの確認には、自動的に更新されるWebリソースカテゴリーのデータベースを使用します。Dr.Web for UNIX Mail Serversと共に配信されます。また、メールメッセージに記載されているWebソースが他のDr.Web製品によって悪意のあるものとしてマークされている場合、Dr.Web Cloudは情報の入手可能性を確認するように要求されます。

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。

メールメッセージ内のDr.Web MailDコンポーネントによって検出された脅威は、サーバー上の検疫に移動され、変更されたメールメッセージ内でユーザー受信者に送信されます。それは、パスワードで保護されたアーカイブにまとめられています。ユーザーは、Dr.Web for UNIX Mail Serversの管理者から受け取ったパスワードを指示するだけで、アーカイブの内容にアクセスできます。

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、Webリソースカテゴリのデータベース、メールスパムフィルタリングのルールの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 Mail 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。



バージョン11.0以降のDr.Web for UNIX Mail Serversでは、メールメッセージに適用可能なアクションが大幅に削減されています。

バージョン11.0以降、Dr.Web for UNIX Mail Serversはメールメッセージに対して次の操作のみを実行します。

- 管理者が設定した基準に準拠していること、スパムの兆候をスキャンしていることを確認するためのメールメッセージチェック(DNSxLブラックリストをチェックする設定がされている場合、そのリストの送信者ドメインのチェックも実施)
- 悪意のあるWebサイトまたは望ましくないカテゴリーに属するWebサイトへのリンクを検索
- 悪意のある添付ファイルの検出

スキャン用のメールメッセージの受信に使用されたプロトコルとメールメッセージを送信した側(MTA/MDAまたはMUA)が転送済みメールメッセージの変更をサポートしている場合、Dr.Web for UNIX Mail Serversは標準的なアクション「無視」と「拒否」に加え、事前に定義されたりパックテンプレートの1つに基づいてメールメッセージをリパックできます(リパック中は、すべての脅威がメールに添付された保護アーカイブに移動され、脅威や望ましくない内容に関する通知がメールの本文に追加されます)。その上、メールのヘッダーを追加、修正する基本機能がサポートされています。

その他のすべてのアクション(管理者への通知の送信、添付ファイルの完全な削除、名前変更など)が必要な場合は、保護されたメールサーバー(MTA/MDA)を介して実装する必要があります。必要に応じて、サードパーティの開発者から対応する処理用に設計された一連の特定のフィルタープラグインを手し、接続することにより、保護されたメールサーバー経由でそれらを実装する必要があります。

ディストリビューションによっては、Dr.Web Anti-SpamコンポーネントがDr.Web for UNIX Mail Serversに含まれていない場合があります。この場合、スパムのメッセージスキャンは実行されません。メールアンチスパムコンポーネントDr.Web Anti-Spamによってメールメッセージが誤って検出された場合は、スパムフィルターの品質を分析および改善するために、それらを専用のアドレスに転送をお願いいたします。分析の対象となる各メッセージを個別の.emlファイルに保存してください。次に、保存したファイルをメールメッセージに添付して、専用のアドレスに送信してください。

- 誤ってスパムと判定されたメッセージは vrnonspam@drweb.com に送信してください。
- 検出されなかったスパムメッセージは vrspam@drweb.com に送信してください。

Dr.Web for UNIX Mail Serversの構成

Dr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail 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 Mail Serversのインターフェースを提供。

以下は、Dr.Web for UNIX Mail 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。ウイルスと悪意のあるプログラムを検出するアルゴリズムを実装します (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> <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>
Dr.Web Scanning Engine	<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。 <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で使われる外部 (Dr.Web for UNIX Mail 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</p> <p>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>
Webリソースカテゴリーのデータベース	<p>Web分類されたリソースのリストを含む、自動的に更新されるデータベース。不要なWebサイトを識別するために使用されます。</p> <p>SpIDer Gate、Dr.Web MailDなど、ユーザーとアプリケーションのネットワークアクティビティ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>
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。



コンポーネント	説明
	<ul style="list-style-type: none">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>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> <hr/> <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、ネットワーク経由で製品のコンポーネントによって送信されます (Dr.Web ClamD、SpIDer Gate、Dr.Web MailDなどのコンポーネント)。Dr.Web for UNIX Mail 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。 <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> <hr/> <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 Mail 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> <hr/> <p>実行ファイル: drweb-meshd</p>



コンポーネント	説明
	ログに表示される内部名: MeshD

2. 脅威検索コンポーネント

コンポーネント	説明
SpIDer Gate	<p>ネットワークトラフィックとURLを監視するためのコンポーネント。</p> <p>ネットワークからローカルホストにダウンロードされ、そこから外部ネットワークに送信されたデータの脅威をスキャンするように設計されています。また、コンポーネントは、Webリソースの不要なカテゴリーだけでなく、システム管理者が作成したブラックリストにも含まれるネットワークホストとの接続を阻止します。</p> <p>メールプロトコル (SMTP、POP3、IMAP) の透過プロキシのモードで、コンポーネント Dr.Web MailD によって使用されます。</p> <p>Dr.Web Network Checker を使用して、受信したデータをスキャンします。</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-gated ログに表示される内部名: GateD</p>
Dr.Web Firewall for Linux	<p>ネットワーク接続モニター。</p> <p>SpIDer Gate によって使用され、送信されたネットワークトラフィックをスキャンするためにサーバー上で動作するアプリケーションに接続ルーティングを提供します。</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-firewall ログファイルに出力される内部名: LinuxFirewall</p>
Dr.Web MailD	<p>電子メールメッセージスキャンコンポーネント。</p> <p>電子メールメッセージを分析し、脅威をスキャンする準備をします。次の2つのモードで動作できます。</p> <ol style="list-style-type: none">1) <i>Milter</i>、<i>Spamc</i> または <i>Rspamc</i> インターフェースを介して接続されたメールサーバー (Sendmail、Postfix など) のフィルター。2) メールプロトコル (SMTP、POP3、IMAP) のトランスパレントなプロキシサーバー。このモードでは、SpIDer Gate を使用します。 <p>Dr.Web Network Checker を使用して電子メールメッセージのデータをスキャンします。</p>



コンポーネント	説明
	実行コンポーネントファイル: drweb-maild ログに表示される内部名: MailD
Dr.Web Anti-Spam	スパムメールのスキャンを実行するコンポーネントです。 Dr.Web MailDによって使用されます。ディストリビューションパッケージによっては利用できない場合があります。利用できない場合、Dr.Web MailDによるスパムメールのスキャンは実行されません。 ARM64アーキテクチャの場合、このコンポーネントはサポートされていません。 実行ファイル: drweb-ase ログに表示される内部名: Antispam

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 Mail Servers設定デーモン。次の機能を実行します。 <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 Mail 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。 実行ファイル: drweb-configd ログファイルに出力される内部名: ConfigD
Dr.Web ES Agent	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。 <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 Mail 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。 実行ファイル: drweb-esagent ログに表示される内部名: ESAgent
Dr.Web Updater	更新コンポーネント ウイルスデータベース、Webリソースカテゴリーのデータベース、スキャンエンジン、スパムの兆候についてメールメッセージをスキャンするためのライブラリのDoctor Webサーバーアップデートからダウンロードします。



コンポーネント	説明
	<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 LookupD	<p>外部データソースからデータを取得するためのコンポーネント。</p> <p>外部データソース (ディレクトリサービス、ファイル、相対データベースなど) からデータを取得します。データはトラフィックモニタリングのルールで使用されます。</p> <p>実行ファイル: drweb-lookupd ログに表示される内部名: LookupD</p>
Dr.Web StatD	<p>Dr.Web for UNIX Mail 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 Mail Servers管理 Webサーバー。</p> <p>Dr.Web for UNIX Mail 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</p>



コンポーネント	説明
	ログに表示される内部名 : HTTPD
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 Mail 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 Mail 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</p> <p>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 Mail 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</p> <p>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 Mail Serversを透過的に使用できるようになります。</p> <p>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。</p> <p>実行ファイル: drweb-clamd</p> <p>ログに表示される内部名 : ClamD</p>

下の図は、Dr.Web for UNIX Mail 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。

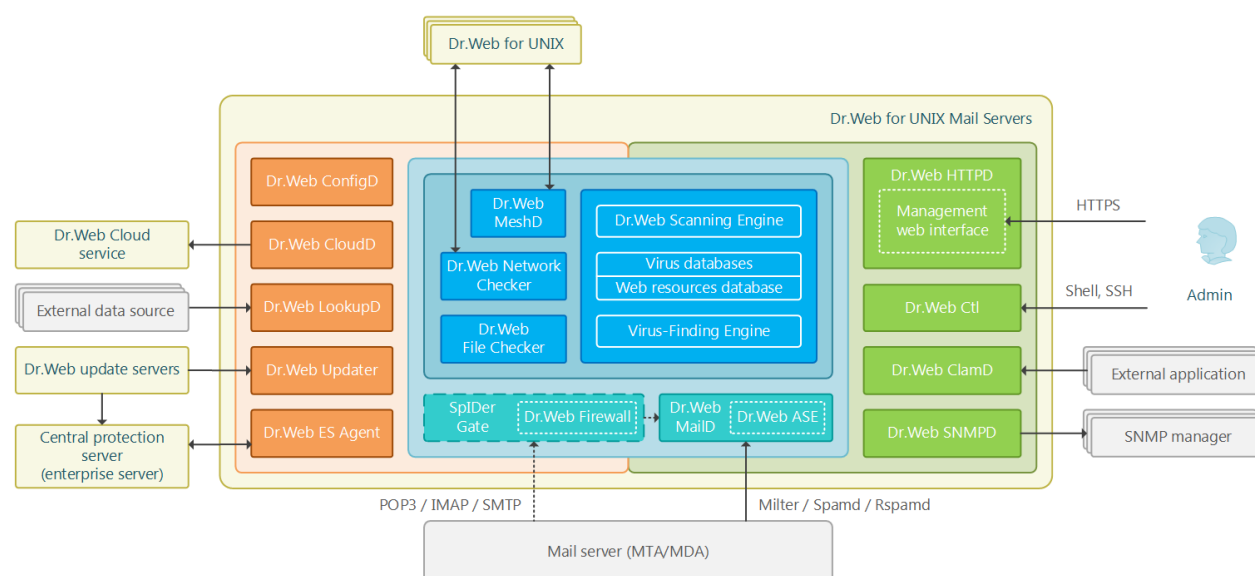


図1. Dr.Web for UNIX Mail Serversの構造

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 Mail 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 Mail 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 Mail 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 Mail 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 Mail Serversコンポーネントの詳細については、[Dr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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。



アクション	必要な権限
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。 <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、削除アクションの代わりにコンテナの隔離への移動が実行されます。</div>
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。 <div> 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。</div>
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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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。

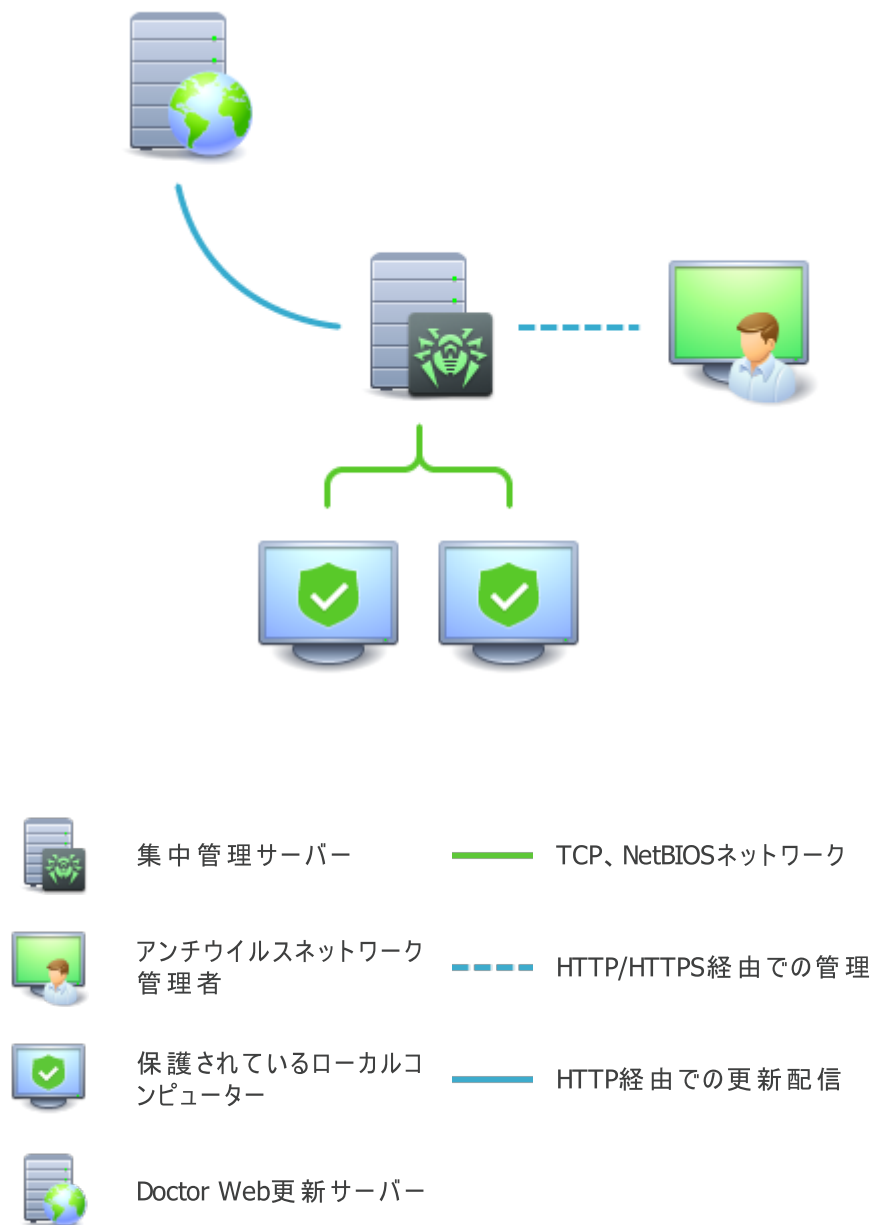


図2. アンチウイルスネットワークの理論的構造

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 Mail 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 Mail 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 Mail 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きます。



Dr.Web for UNIX Mail 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 Mail 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](#)
- [サポート対象のメールサーバー\(MTA\)](#)
- [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 Mail 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 (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 Mail 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><p>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。</p><hr/><p>コンポーネントDr.Web Firewall for Linuxが正しく動作するためには、以下のオプションを指定してOSカーネルが構築されている必要があります。</p><ul style="list-style-type: none">• <code>CONFIG_NETLINK_DIAG, CONFIG_INET_TCP_DIAG;</code>• <code>CONFIG_NF_CONNTRACK_IPV4, CONFIG_NF_CONNTRACK_IPV6, CONFIG_NF_CONNTRACK_EVENTS</code>• <code>CONFIG_NETFILTER_NETLINK_QUEUE, CONFIG_NETFILTER_NETLINK_QUEUE_CT, CONFIG_NETFILTER_XT_MARK.</code><p>必要なオプションの組み合わせは、使用するOSのディストリビューションキットによって異なります。</p></div>



コンポーネント	要件
	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。
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 Mail 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 Mail 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
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 Mail 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 Mail 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 Mail 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

- **CommuniGate Pro**メールサーバーと統合するための**python3**パッケージ。



[コマンドライン](#)でDr.Web for UNIX Mail 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

- SpIDer Gateは、OSにインストールされている他のファイアウォール（**SUSE Linux Enterprise Server** OSの**Shorewall**および**SuseFirewall2**、**Fedora** OS、**CentOS**、**RedHat Enterprise Linux**の**FirewallD**など）と競合する可能性があります。競合の兆候は、コードx109のSpIDer Gateのエラーに関するメッセージ、またはコードx102のDr.Web Firewall for Linuxのエラーに関するメッセージです。競合を解決する方法は、それぞれ「既知のエラー」セクションのエラー[x109](#)と[x102](#)で説明されています。
- 使用しているOSに1.4.15より前のバージョンの**NetFilter**が含まれている場合、SpIDer Gateは正しく動作しない可能性があります。この問題は、**NetFilter**の内部エラーに関連しており、SpIDer Gateを無効にすると、ネットワーク接続が切断され、再確立できなくなります。この問題が発生した場合は、バージョン1.4.15以降の**NetFilter**を含むOSにアップグレードすることをお勧めします。問題を解決する方法は、セクション「[既知のエラーの説明](#)」で説明されています。

サポート対象のメールサーバー（MTA）

Dr.Web for UNIX Mail Serversには、メールサーバー（MTA）がインストールされている必要があります。

- プラグインフィルターのモードでDr.Web for UNIX Mail ServersとMTAを[統合](#)するには、メールサーバーが外部のスパムおよびアンチウイルスフィルターと統合するためのインターフェース（*Miller*、*Spamd*、*Rspamd*）をサポート



ートしている必要があります。たとえば、以下のリストのMTAを使うことができます。**Sendmail**、**Postfix**、**Exim**、**CommuniGate Pro**。

- *Milter*、*Spamd*、*Rspamd*の統合インターフェースをサポートしていないMTAは、[Dr.Web ClamD](#)アンチウイルススキャンコンポーネントへの直接接続で、アンチウイルススキャン *Clamd*のインターフェースを介して Dr.Web for UNIX Mail Serversと統合できます (MTAをインストールして設定するには、追加の統合モジュールが必要になる可能性があります)。この統合モードでは[Dr.Web MailD](#)コンポーネントが使用されないため、メールメッセージでスパムがスキャンされず、脅威が検出された場合にメールメッセージをリパックすることはできません。感染したメールメッセージの処理を目的としたすべてのアクションは、メールサーバーに転送されます。メールサーバーは脅威に対するメールメッセージのスキャンの結果を取得します。



統合設定は複雑なため、メールサーバーQmailを操作するには、透過プロキシモードを使用することをお勧めします。

- [透過プロキシ](#)モードでは、MTAとMDA間、またはMDAとMUA間で透過的にメールメッセージのアンチウイルスおよびアンチスパムスキャンを行うDr.Web for UNIX Mail Serversを統合できます (プロトコルSMTP、POP3、IMAPを介したデータ交換チャネルへの統合が実行されます)。このモードでは、MTAとDr.Web for UNIX Mail Serversを同じホストにインストールする必要があります。



透過プロキシモードでは、Dr.Web for UNIX Mail ServersにSpIDer Gateが含まれている必要があります。SpIDer Gateは**GNU/Linux**でのみ実行されます。

- [SMTPプロキシ](#)モードは、MTAが受信メッセージのルーティングに設定されている (メールリレーのように機能する) プラグインフィルターのモード (**Postfix**など) で、Dr.Web for UNIX Mail ServersとMTAが統合する特殊なケースです。

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 Mail Serversは **SELinux** をサポートしていません。また、Dr.Web for UNIX Mail 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 Mail Serversのインストールが必要な場合、Dr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail Serversをインストールする。](#)
- [Dr.Web for UNIX Mail Serversをアップグレードする。](#)
- [Dr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail Serversをインストールする

Dr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail Serversユニバーサルパッケージは、drweb-*<version>*-av-mail-*<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 Mail 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-mail-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 Mail 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。

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ています(**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 Mail 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 Mail 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。インストールを終了するには、「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、インストールは終了します。
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 Mail 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、インストールが終了します。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 Mail 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 Mail 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 Mail 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-mail-servers
```

代替りのパッケージマネージャ (**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 Mail 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-mail-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 Mail 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-mail-servers
```

代替りのパッケージマネージャー(**rpmrake** 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も実行できます。

2. リポジトリから Dr.Web for UNIX Mail 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-mail-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-mail-servers
```

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



SUSE Linux (zypper)

1. リポジトリを追加するには、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 Mail 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-mail-servers
```

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

Dr.Web for UNIX Mail Serversをアップグレードする

Dr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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（たとえば、プロキシモードでのDr.Web for UNIX Mail Servers動作の場合、MTA（メールサーバー）が必要です）。

お使いのバージョンのDr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail Serversを更新できない場合は、現在のバージョンのDr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail 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。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 Mail 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 Mail 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 Mail 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 Mail Serversバージョンを削除する必要があり、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、ファイ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-mail-servers-gateways-doc
- drweb-maild-web
- drweb-maild

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 Mail 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 Mail Serversを別のマシンにインストールしてください。



Doctor Webのリポジトリからインストールされた現在のバージョンのDr.Web for UNIX Mail Serversをアップグレードするには、以下の手順を実行してください。

1. リポジトリからインストールされた現在のDr.Web for UNIX Mail Serversバージョンを[アンインストール](#)します。
2. 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）。
3. リポジトリから新しいバージョンのDr.Web for UNIX Mail Serversを[インストール](#)します。



[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。

キーファイルの転送

選択したDr.Web for UNIX Mail 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 Mail 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 Mail Serversをアンインストールする

Dr.Web for UNIX Mail 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。



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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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-mail-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-mail-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 Mail 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 Mail 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。

代替のマネージャー（**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 Mail 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 Mail 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-mail-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-mail-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-mail-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-mail-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 Mail 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 Mail 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。

代わりのマネージャー(**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 Mail 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-mail-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-mail-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 Mail 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 Mail Serversパッケージとファイル

パッケージ

Dr.Web for UNIX Mail 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-ase	Dr.Web Anti-Spam Engine (Dr.Web ASE) のコンポーネントファイル 一部のディストリビューションでは使用できません。
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 Mail Serversディレクトリの階層、製品設定とシステム環



パッケージ	コンテンツ
	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 Mail 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-dws	Webリソースカテゴリーのデータベースのファイル
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-mail-servers-doc	PDFドキュメント
drweb-mail-servers	Dr.Web for UNIX Mail Serversのルートメタパッケージ
drweb-gated	SpIDer Gateコンポーネントのファイル
drweb-firewall	Dr.Web Firewall for Linuxコンポーネントのファイル
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
drweb-libs	メインライブラリファイル
drweb-lookupd	Dr.Web LookupDコンポーネントのファイル
drweb-lua	ネットワーク接続監視用に設計されたDr.Web for UNIX Mail Serversコンポーネントによって使用されるLuaインタプリタのファイル
drweb-maild	Dr.Web MailDコンポーネントのファイル
drweb-netcheck	Dr.Web Network Checker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



パッケージ	コンテンツ
drweb-se	Dr.Web Scanning Engineコンポーネントのファイル
drweb-snmpd	Dr.Web SNMPDコンポーネントのファイル
drweb-update	Dr.Web Updaterコンポーネントのファイル
drweb-vaderetro	VadeSecure によって設計された VadeRetro アンチスパムライブラリのファイル。 一部のディストリビューションでは使用できません。

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 Mail 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 Mail 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。
certs/	– 使用中の証明書のファイル。
<opt_dir>/	Dr.Web for UNIX Mail 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）。



ディレクトリ	コンテンツ
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。またここには、Dr.Web for UNIX Mail Serversディストリビューションに含まれている場合、スパム VadeRetro (libvaderetro.so) に対しメールメッセージをスキャンするためのライブラリもあります。
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 Mail 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 Mail 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 Mail 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 Mail 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
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
<p>MTAに接続可能なフィルターとしてメールをスキャンするためのスイート</p> <p><i>注意: メールメッセージのアンチウイルススキャンが必要ない場合は、drweb-netcheckおよびdrweb-seパッケージをインストールする必要はありません。Dr.Web Network Checkerを介してスキャン用のデータを受信する別のサーバーでアンチウイルススキャンが実行される場合、drweb-seパッケージのインストールがスキップされる可能性があります。URLを望ましくないWebリソースのカテゴリに含める必要がない場合は、drweb-dwsパッケージのインストールをスキップできます。スパムのメールメッセージスキャンが必要ない場合は、drweb-antispamおよびdrweb-vaderetroパッケージのインストールをスキップできます。</i></p> <p><i>*マークは、drweb-seパッケージがインストールされていない場合にインストールされないコンポーネントを示しています。**マークは、drweb-dwsパッケージがインストールされていない場合にインストールされないコンポーネントを示しています。Dr.Web Updaterコンポーネント (***マークが付いています) は、ウイルスデータベースまたはWebリソースカテゴリのデータベースがインストールされている場合にのみ</i></p>	<p>drweb-maild drweb-dws *** drweb-antispam ** drweb-vaderetro ** drweb-netcheck * drweb-se *</p>	<ul style="list-style-type: none">• Dr.Web Ctl• Dr.Web ConfigD• Dr.Web MailD• Dr.Web ASE ****• VadeRetroスパムフィルター****• Dr.Web Network Checker• Dr.Web Scanning Engine *• Dr.Web Updater ***• ウイルスデータベース*• Webリソースカテゴリのデータベース**



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
<p>インストールされます。****マークは、スパムをスキャンするパッケージがインストールされていない場合にインストールされないコンポーネントを示しています。Dr.Web Updaterコンポーネント(***ラベルが付いています)は、ウイルスデータベース、Webリソースカテゴリーデータベース、Vaderetroスパムフィルターがインストールされている場合にのみインストールされます。</p>		
<p>SMTP、POP3、IMAPプロトコルの透過プロキシモードでメールをスキャンするためのスイート</p> <p>注意: メールメッセージのアンチウイルススキャンが必要ない場合は、drweb-netcheckおよびdrweb-seパッケージをインストールする必要はありません。Dr.Web Network Checkerを介してスキャン用のデータを受信する別のサーバーでアンチウイルススキャンが実行される場合、drweb-seパッケージのインストールがスキップされる可能性があります。URLを望ましくないWebリソースのカテゴリーに含める必要がない場合は、drweb-dwsパッケージのインストールをスキップできます。スパムのメールメッセージスキャンが必要ない場合は、drweb-antispamおよびdrweb-vaderetroパッケージのインストールをスキップできます。</p> <p>*マークは、drweb-seパッケージがインストールされていない場合にインストールされないコンポーネントを示しています。**マークは、drweb-dwsパッケージがインストールされていない場合にインストールされないコンポーネントを示しています。Dr.Web Updaterコンポーネント(***マークが付いています)は、ウイルスデータベースまたはWebリソースカテゴリーのデータベースがインストールされている場合にのみインストールされます。****マークは、スパムをスキャンするパッケージがインストールされていない場合にインストールされないコンポーネントを示しています。Dr.Web Updaterコンポーネント(***ラベルが付いています)は、ウイルスデータベース、Webリソースカテゴリー</p>	<p>drweb-gated drweb-firewall drweb-maild drweb-dws *** drweb-antispam ** drweb-vaderetro ** drweb-netcheck * drweb-se *</p>	<ul style="list-style-type: none">• Dr.Web Ctl• Dr.Web ConfigD• SpIDer Gate• Dr.Web Firewall for Linux• Dr.Web MailD• Dr.Web ASE ****• VadeRetroスパムフィルター****• Dr.Web Network Checker• Dr.Web Scanning Engine *• Dr.Web Updater ***• 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**



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
リーデータベース、 Vaderetro スパムフィルターがインストールされている場合にのみインストールされます。		

リポジトリからインストールされたDr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail Serversが対象としているプラットフォームです。Dr.Web for UNIX Mail 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 Mail 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 Mail 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-mail-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 Mail 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 Mail 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 Mail Serversとの動作に問題が生じます。この場合、Dr.Web for UNIX Mail 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 Mail Serversの設定を変更する必要があります。

この章では、**SELinux**セキュリティポリシーの**設定**の詳細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

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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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** デモンが使用されている場合、audit(監査)に関するログが /var/log/audit/audit.log ファイルに保存されます。それ以外の場合、ブロックされた動作に関するメッセージが一般的なログファイル(/var/log/messages または /var/log/syslog)に保存されます。

SELinuxにブロックされて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 Mail 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(**RedHat 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 Mail 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。



RedHat 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。



開始する

1. インストールされたDr.Web for UNIX Mail 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 Mail 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 Mail Serversを、*Milter*、*Spamd*、*Rspamd*を介して動作する外部フィルターとして接続し、使用するメールサーバーと**統合**します。
4. **SMTPプロキシ**モードでDr.Web for UNIX Mail Serversを使用する場合は、まず、トランジットMTA機能を実行するメールサーバーをインストールして設定します（インストールされていない場合）。
5. **GNU/Linux**ベースのシステムの場合、メールサーバーやMUAに対して透過型のプロキシモードを**設定**できます。このモードでは、Dr.Web for UNIX Mail Serversとメールサーバーとの実際の統合を実行する必要はありません。プロトコルSMTP、POP3、IMAPとの透過型の統合がサポートされています。
6. 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、**Dr.Web ClamD**、**Dr.Web SNMPPD**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 Mail 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 Mail Serversは、メールメッセージに対して次の操作のみを実行します。

- 管理者が設定した基準に準拠していること、スパムの兆候をスキャンしていることを確認するためのメールメッセージチェック(DNSxLブラックリストをチェックする設定がされている場合、そのリストの送信者ドメインのチェックも実施)
- 悪意のあるWebサイトまたは望ましくないカテゴリーからWebサイトへのリンクを検索
- 悪意のある添付ファイルの検出

スキャン用のメールメッセージの受信に使用されたプロトコルとメールメッセージを送信した側(MTA/MDAまたはMUA)が転送済みメールメッセージの変更をサポートしている場合、Dr.Web for UNIX Mail Serversは標準的なアクション「無視」と「拒否」に加え、事前に定義されたりパックテンプレートの1つに基づいてメールメッセージをリパックできます(リパック中は、すべての脅威がメールに添付された保護アーカイブに移動され、脅威や望ましくない内容に関する通知がメールの本文に追加されます)。その上、メールのヘッダーを追加、修正する基本機能がサポートされています。

その他のすべてのアクション(管理者への通知の送信、添付ファイルの完全な削除、名前変更など)が必要な場合は、保護されたメールサーバー(MTA/MDA)を介して実装する必要があります。必要に応じて、サードパーティの開発者から対応する処理用に設計された一連の特定のフィルタープラグインを入手し、接続することにより、保護されたメールサーバー経由でそれらを実装する必要があります。

スパムの兆候に対するメールメッセージのスキャン機能は、Dr.Web for UNIX Mail Serversのディストリビューションによっては利用できない可能性があります。



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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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せん。



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 Mail 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 Mail 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 Mail 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 Mail 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、登録時に指定したものと同一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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 X50 > 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 Mail 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。次にこのファイルをスキャンし、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。

フィルターとしてのMTAとの統合

この統合方法では、メールスキャン用の外部フィルターとしてDr.Web MailDをメールサーバーに直接接続することを想定しています。*Milter*、*Spamd*、*Rspamd*インターフェースを使用する全てのメールサーバー(**Exim**、**Sendmail**、**Postfix**など)に接続できます。

このセクションの内容：

- [Dr.Web MailDを設定する](#)
- [MTAを設定する](#)
- [一部のMTAの設定例](#)



1) Dr.Web MailDパラメータを設定する

Dr.Web MailDとメールサーバーを統合するには、設定ファイル内のDr.Web MailDの**設定**セクション（[MailD] セクション）で現在のパラメータ値を確認し、必要に応じて変更する必要があります。

1.1) メールメッセージスキャン時のDr.Web MailDの一般的な動作パラメータ

TemplateContacts、**ReportLanguages**パラメータを使用して、脅威やスパムを含むメールメッセージをリパックするときのメール生成のパラメータを指定します。**RepackPassword**パラメータ値として、リパック後にメールメッセージに追加される脅威を含む保護されたアーカイブのパスワード生成方法を指定します（デフォルトではNone値が指定され、パスワードによるアーカイブはパスワードで保護されていませんが、推奨しません）。

1.2) Dr.Web MailDとMTAの統合パラメータ

まず、使用する統合インターフェース（*Milter*、*Spamd*、*Rspamd*）を決定し、MTA接続のパラメータと、選択したインターフェースで受信するメールのスキャンパラメータを指定する必要があります。特定のインターフェースを介してMTAとの統合を制御するDr.Web MailDのすべてのパラメータには、次のように名前にそれぞれのプレフィックスが付いています。

- *Milter** - *Milter*インターフェースの場合。
- *Spamd** - *Spamd*インターフェースの場合。
- *Rspamd** - *Rspamd*インターフェースの場合。

次のパラメータの値を指定する必要があります（ここで、*<interface>*は、MTAインターフェースとの統合のために選択したインターフェースに対応するパラメータ名のプレフィックスです）。

1. *<interface>Socket*は、対応するインターフェースを介してMTAからスキャン済みメールメッセージを取得するためにDr.Web MailDによって使用されるソケットです。UNIXソケットまたはネットワークソケットを使用できます。
2. メールメッセージスキャンの長さとしリソース強度を制限するパラメータ（**ScanTimeout**、**HeuristicAnalysis**、**PackerMaxLevel**、**ArchiveMaxLevel**、**MailMaxLevel**、**ContainerMaxLevel**、**MaxCompressionRatio**）。きめ細かい設定が不要な場合は、パラメータデータの値をデフォルトの状態しておくことを推奨します。
3. メールのフィルタールールを（条件に応じて）より細かく設定するには、Luaでデフォルトのメールスキャン手順のテキストを編集します。

すべての設定を調整したら、Dr.Web for UNIX Mail 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）。



Dr.Web MailDとMTAとのインタラクションに *Spamd/Rspamd* インターフェースが使用されている場合、このインタラクションでは、Dr.Web MailDは、メールメッセージがクリーンかスパムとして分類されるかをMTAに通知するアクションしか実行できません。メールメッセージが管理者によって設定された制限に違反している場合、またはメールメッセージや不要なコンテンツに何らかの脅威がある場合、「メールメッセージはスパムです」の判定がMTAに送信されます。メールメッセージの処理を目的としたすべてのアクション（ヘッダーの追加、メールメッセージの拒否、受信者への配信など）は、*MTA側の設定*で定義する必要があります。

メールメッセージが拒否された理由、MTAがメールメッセージに適用する必要があるアクションをMTAに返すために、テキスト変数（*Spamd*には *report*、*Rspamd*には *action*）が使用されます。これはMTA設定で処理できる、LUAメッセージ処理手順によって返されます（たとえば、**Exim**ではACL）。

2) MTAのパラメータを設定する

MTAとDr.Web MailDの間のインタラクションを有効にするには、MTAによって処理されたメールをスキャンする外部フィルターとしてDr.Web for UNIX Mail Serversを使用できるようにメールサーバーの設定を編集します。

1. メールメッセージをスキャンするときにMTAとDr.Web MailDのインタラクションに使用されるインターフェース（*Milter*、*Spamd*、*Rspamd*）を指定します。
2. 選択したインターフェースを介してMTAをDr.Web MailDに接続するためのパラメータを指定します（使用するソケットは、Dr.Web MailDの設定で対応するインターフェースの `<interface>Socket` パラメータで指定されているものと一致する必要があります）。
3. インタラクションインターフェース経由でのメールスキャン結果の受信に対応するMTAの動作を設定します。

MTAの設定を変更したら、再起動します。

3) 一部のMTAの設定例

以下は、Dr.Web MailDをメールメッセージの外部フィルターとして *Milter*、*Spamd*、*Rspamd* インターフェース経由で **Postfix**、**Sendmail**、**Exim**、**CommuniGate Pro** に接続する場合のこれらのMTAの設定例です。



以下の例では、`<MailD socket>`、`<MailD IP address>`、`<MailD port>` の値は、Dr.Web MailDが待ち受け（リッスン）しているソケット（Dr.Web MailD設定の `<interface>Socket` パラメータで示されています。ここで、`<interface>` は、MTAと統合された、選択されたインターフェースに対応するパラメータの名前のプレフィックスです）に置き換える必要があります。

たとえば、Dr.Web MailDがネットワークソケットを使用して *Milter* インターフェース経由でMTAと統合され、MTAとDr.Web MailDの両方がローカルホスト上で動作し、Dr.Web MailDがポート12345で *Milter* 経由の接続を待ち受け（リッスン）する場合、この値は、Dr.Web for UNIX Mail Servers設定ファイルの [MailD] セクションで **MilterSocket** パラメータとして指定する必要があります。MTA設定では、`<MailD socket>` 変数の値に「127.0.0.1:12345」を、`<MailD IP address>` 変数のアドレスに「127.0.0.1」を、`<MailD port>` 変数の値に「12345」をそれぞれ指定する必要があります。

場合によっては、Dr.Web MailDとの接続のソケットアドレスに、プレフィックス `<type>` とMTA設定で使われるアドレスのタイプ（`inet`、`inet6`、`unix`）を追加する必要があります。



1. Postfix

- *Milter*:

MTA設定ファイル`main.cf`に以下の行を追加します。

```
smtpd_milters = <type>: <MailD socket>
milter_content_timeout = 300s
milter_default_action = tempfail
milter_protocol = 2
```

`smtpd_milters`および`milter_protocol`パラメータのみが必須であることに注意してください。それ以外のパラメータは省略できます。

2. Sendmail

- *Milter*:

MTAプロトタイプ設定ファイル`sendmail.mc`に以下の行を追加します。

```
INPUT_MAIL_FILTER(`drweb-milter', `S=<MailD socket>, F=T')
```

`sendmail.mc`ファイルを変更したら、必ず次のいずれかのコマンドを実行し、このファイルをアクティブな設定ファイル`sendmail.cf`に変更してください。

```
make -C /etc/mail
sendmailconfig
m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
```

上のコマンドはすべて、**Sendmail**の設定ファイルが`/etc/mail`ディレクトリにあることを前提としています。

3. Exim

- *Spamd*:

MTA設定ファイル`exim.conf`に以下の行を追加します。

```
spamd_address = <MailD socket>
acl_smtp_data = acl_check_data

acl_check_data:
  warn spam = nobody:true
  add_header = X-Spam_score: $spam_score\n\
  X-Spam_score_int: $spam_score_int\n\
  X-Spam_bar: $spam_bar\n\
  X-Spam_report: $spam_report

  deny message = This message scored $spam_score spam points.
  spam = nobody:true
  condition = ${if >{$spam_score_int}{10000}{true}{false}}

  accept message = This message scored $spam_score spam points.
  spam = nobody:true
  condition = ${if >{$spam_score_int}{1000}{true}{false}}
```



```
remove_header = Subject
add_header = Subject: [SPAM] $rh_Subject
```

- *Rspamd*:

MTA設定ファイルexim.confに以下の行を追加します。

```
spamd_address = <MailD socket> variant=rspond
acl_smtp_data = acl_check_data

acl_check_data:
  #ヘッダーフィールドを追加します
  warn spam = nobody:true
  add_header = X-Spam_score: $spam_score\n\
    X-Spam_score_int: $spam_score_int\n\
    X-Spam_bar: $spam_bar\n\
    X-Spam_report: $spam_report

  # Reject the message with proper description if Rspamd filter tells to
  do so
  deny spam = nobody:true
  message = ${extract{2}{:}}{$spam_action}}
  condition = ${if eq}${extract{1}{:}}{$spam_action}}{reject}}

  # Accept the message otherwise
  accept
```



上記の設定例では、オプションWITH_CONTENT_SCAN=yesでビルドされたバージョン4.6(またはそれ以降)のEximが使用されることを想定しています。Spamdの設定では、Dr.Web MailDがSPAMまたはTHREATという単語を含むメッセージ(report)を返すことを想定しています。そのため、Eximはwarnまたはdenyのアクションをメールメッセージに適用します。Rspamdの設定では、Dr.Web MailDがアクションADD_HEADERまたはアクションREJECT: <message>を返すことを想定しています。そのため、Eximはwarnまたはdenyアクションをメールメッセージに適用します。

4.CommuniGate Pro

- *Rspamd*:

1. CommuniGateProと連動するには特別なモジュールが必要です。これはDr.Webリポジトリに含まれており、標準のパッケージマネージャーを介してインストールできます。

Debian、Ubuntu、Mintの場合:

```
# apt-get install drweb-cgp-plugin
```

RedHatおよびCentOSの場合:

```
# yum install drweb-cgp-plugin
```

Fedoraの場合:

```
# dnf install drweb-cgp-plugin
```

2. モジュールは/opt/drweb.com/share/cgp/にインストールされます。このディレクトリに移動し、ファイルCgpDrweb_AS_AV.py を次のように実行可能にします。



```
# cd /opt/drweb.com/share/cgp/  
# chmod +x CgpDrweb_AS_AV.py
```

3. Webインターフェースを使用して **CommuniGate Pro**を設定します。

- **Settings** → **General** → **Helpers**に移動します。モジュールを**CommuniGate Pro**に接続します。**Content Filtering**セクションで、新しいフィルターを設定し、*Enabled*に切り替え、フィルター名を指定します(たとえば、*CgpDrweb_AS_AV*)。**Program Path**/パラメータで、スクリプトファイルへのパスを指定します
(**GNU/Linux**、*/opt/drweb.com/share/cgp/CgpDrweb_AS_AV.py*、スクリプトを起動するオプションなど。たとえば、*-r* - ソケットのアドレスとポート、*-u*または *--rspamd-unix-socket* - UNIXソケットへのパス、*--debug* - デバッグモードで起動)。**Helpers**を使用できるように、エキスパートまたはアドバンスビューモードを有効化します(CommuniGatePro設定の **環境設定** → **インターフェース**)。可能なすべてのオプションのリストを表示するには、次のコマンドを実行します。

```
# ./CgpDrweb_AS_AV.py --help
```

変更内容を保存します。

- **Settings** → **Mail** → **Rules**に移動します。新しいルール名(*CgpDrweb_AS_AV*など)を指定して、**Add Rule**をクリックします。*Highest*ルール設定を選択し、変更を保存して、ルール名の右側にある**Edit**をクリックします。**Data**ドロップダウンメニューで、*Message Size*を選択します。**Operation**フィールドで*less than*を選択し、**Parameter**フィールドで*40960000*を指定します。**Action**フィールドで、*ExternalFilter*を選択します。**Parameter**で、以前に作成したフィルターの名前(この場合は*CgpDrweb_AS_AV*)を選択します。変更内容を保存します。
- 脅威検出レスポンスルールを追加し、その名前(*Drweb_threats*など)を指定して、**Add Rule**をクリックします。ルールのプライオリティー*5*を指定し、変更を保存して、ルールの右側にある**Edit**をクリックします。ルールの条件を2回追加します。
 - **Data**ドロップダウンリストで*Header Field*を選択し、**Operation**フィールドで*is*を選択し、**Parameter**フィールドで*X-Spam-Action: reject*を指定します。
 - **Data**ドロップダウンリストで*Header Field*を選択し、**Operation**フィールドで*is*を選択し、**Parameter**フィールドで*X-Spam-Symbol-1: threat**を指定します。
- **Action**フィールドで、*Reject with*を選択します。**Parameter**で、テキストを指定します(たとえば、*The message contains threat(s)*)。変更内容を保存します。
- 脅威検出レスポンスルールを追加し、その名前(*Drweb_spam*など)を指定して、**Add Rule**をクリックします。ルールのプライオリティー*5*を指定し、変更を保存して、ルールの右側にある**Edit**をクリックします。ルールの条件を追加します。ドロップダウンメニュー**Data**で*Header Field*を選択します。フィールド**Operation**で*is*を選択し、フィールド**Parameter**で*X-Spam-Action: tag*を選択します。フィールド**Action**で*Tag Subject*を選択し、**Parameter**でヘッダープレフィックス(*[SPAM]*など)を指定します。変更内容を保存します。

4. 以下のファイルのコンテンツをコピーして、*hook.lua*として保存します。

```
--メッセージスキャン手順、  
--Rspamdプロトコルを使用して送信  
  
function rspamd_hook(ctx)  
  
--脅威を検出するためのメッセージスキャン  
if ctx.message.has_threat() then
```



```
return {
  score = 900,
  threshold = 100,
  action = "reject",
  symbols = {
    {
      name = "threat",
      score = 900
    }
  }
}
end
```

—スパムを検出するためのメッセージスキャン

```
if ctx.message.spam.score > 100 then
  return {
    score = ctx.message.spam.score,
    threshold = 100,
    action = "tag",
    symbols = {
      {
        name = "spam",
        score = ctx.message.spam.score
      }
    }
  }
end

return {
  score = ctx.message.spam.score,
  threshold = 100,
  action = "accept",
  symbols = {
    {
      name = "The message is clean",
      score = 0
    }
  }
}
end
```

5. 次のコマンドを実行します。

```
# drweb-ctl cfset MailD.RspamdHttpSocket <socket
address>:<port>
# drweb-ctl cfset MailD.RspamdHook <path to hook>
```

フックのコードを編集した場合は、変更後に次のようにDr.Web ConfigDを再起動する必要があります。

```
# service drweb-configd restart
```



SMTPプロキシモードでDr.Web for UNIX Mail Serversを使用する

この統合方法では、SMTP経由でメールメッセージを中継するメールサーバー（**Exim**、**Sendmail**、**Postfix**など）をインストールする（またはすでにインストールされているメールサーバーを使用する）こと、およびDr.Web MailDがメールスキャン用の外部フィルターとしてこのメールサーバーに接続することを前提としています。*Milter*、*Spamd*、*Rspamd*インターフェースを使用する任意のメールサーバーに接続できます。

このセクションの内容：

- [メールサーバーのスキャンパラメータを設定する。](#)
- [Dr.Web MailD設定を設定する。](#)
- [3\) PostfixのSMTPプロキシ設定例。](#)

1) メールサーバーのスキャンパラメータを設定する

SMTPプロキシを実現するには、メールサーバーがメールメッセージを受信し、*Milter*、*Spamd*、*Rspamd*インターフェースを介してメールスキャン用の外部フィルターとして接続されたDr.Web MailDでメールメッセージをスキャンし、指定されたルーティングルールに従ってメールメッセージの配信チェーンの最後または次の中間MTAにメールメッセージを送信するように設定する必要があります。

Milter、*Spamd*、または*Rspamd*インターフェースを介してDr.Web MailDをメールスキャン用の外部フィルターとして接続するために必要なMTAパラメータは、「フィルターとしてのMTAとの統合」のセクションに記載されています。

メールメッセージの送受信のルーティング設定は、インストールされているメールサーバーによって異なります。次の例は、**Postfix**メールサーバーのこのような設定を示しています。

2) Dr.Web MailD設定を設定する

Dr.Web MailDとメールサーバーを統合するには、設定ファイル内のDr.Web MailDの[設定](#)セクション（[MailD] セクション）にあるパラメータの値を確認し、必要に応じて変更する必要があります。このような設定の例は、「フィルターとしてのMTAとの統合」セクションにあります。

3) PostfixのSMTPプロキシ設定例

次の例では、**Postfix**がドメインexample1.orgおよびexample2.comからメールボックスに送信されたメールメッセージを受信すると想定しています（メールメッセージのルーティングテーブルは、/etc/postfix/transportファイルで指定されています）。ネストされた脅威およびスパムに関するメッセージのスキャンは、Dr.Web MailD.によって*Milter*インターフェースを介して実行されます。Dr.Web MailDは、ホスト10.20.30.40.でポート1234をリッスンします。

1. main.cf設定ファイルの内容：

```
#メールメッセージのスキャンと転送が実行されるドメイン
#メールメッセージ。
relay_domains = example1.org, example2.com

#実行する外部Milterフィルターに接続するための設定
#ウイルスとスパムのメッセージスキャン。
```



```
smtpd_milters = inet:10.20.30.40:1234
milter_protocol = 2

#Transport table (mail routing settings).
transport_maps = hash:/etc/postfix/transport
```

2. transportファイルの内容:

```
#文字列形式:
#<transfer domain> <connection type>:<MTA address>:<listening port
number>

#ドメイン「example1.org」のすべての送受信メール
#スキャンした後、MTAに転送されます。
#これは、ホスト「relay.example1.org」にあります(デフォルトでは
#SMTPプロトコルのポート)
example1.org      smtp:relay.example1.org

#ドメイン「example2.com」のすべての送受信メール
#スキャンした後、MTAに転送されます。
#これは、IPアドレス2. 2. 2からポート10025のホストにあります
example2.com      smtp:2.2.2.2:10025
```

透過プロキシモードでDr.Web for UNIX Mail Serversを使用する



このオプションは、**GNU/Linux OS**の製品ディストリビューションでのみ使用できます。

Milter、*Spamd*、または*Rspamd*を介して、または*ClamAV*プロトコルを使用して([Dr.Web ClamD](#)コンポーネントを直接使用して) Dr.Web for UNIX Mail Serversと通信することができないメールサーバーを使用する場合は、Dr.Web for UNIX Mail Serversがインストールされているインターネットゲートウェイ経由で受信した情報が[SpIDer Gate](#)ネットワーク接続モニター(透過プロキシモード)によってスキャンされるように[Dr.Web Firewall for Linux](#)コンポーネントを設定します。

このセクションの内容:

- [Dr.Web MailDパラメータを設定する](#)。
- [透過プロキシパラメータを設定する](#)。
- [スキャン設定](#)。

1) Dr.Web MailDパラメータを設定する

Dr.Web for UNIX Mail Serversを設定するには、まず設定ファイル内のDr.Web MailDの[設定](#)セクション([MailD]セクション)で現在のパラメータ値を確認し、必要に応じて変更する必要があります。

TemplateContacts、**ReportLanguages**の各パラメータを使用して、脅威やスパムを含むメールメッセージをリパックするときのメール生成のパラメータを決定します。**RepackPassword**パラメータの値として、電子メールメッセージに追加される、脅威を含む保護されたアーカイブのパスワードの生成方法を指定します(デフォ



ルトではパスワードは未設定となっており、パスワードによるアーカイブの保護はされていません。これは許容されますが、推奨されません。

2) 透過プロキシパラメータを設定する

透過プロキシモードを設定するには、Dr.Web Firewall for Linux (セクション [LinuxFirewall]) の **設定** のセクションで、設定ファイルの一部のパラメータ値を次のように変更します。

パラメータ	必要な値
InspectSmtplib>	<ul style="list-style-type: none">SMTP経由で転送されるデータを監視する必要がある場合は On (<i>MUAとMTA間またはMTAとMTA間のデータ転送</i>)SMTP経由で転送されるデータを監視する必要がない場合は Off
InspectPop3	<ul style="list-style-type: none">POP3経由で転送されるデータを監視する必要がある場合は On (<i>MUAとMDA間のデータ転送</i>)POP3経由で転送されるデータを監視する必要がない場合は Off
InspectImap	<ul style="list-style-type: none">IMAP経由で転送されるデータを監視する必要がある場合は On (<i>MUAとMDA間のデータ転送</i>)IMAP経由で転送されるデータを監視する必要がない場合は Off
AutoconfigureIptables	Yes
AutoconfigureRouting	Yes
LocalDeliveryMark	Auto
ClientPacketsMark	Auto
ServerPacketsMark	Auto
TproxyListenAddress	127.0.0.1:0 <i>Dr.Web Firewall for Linuxの操作に特別なIPアドレスまたはポートを使用する場合は、ここで指定します</i>
OutputDivertEnable	<ul style="list-style-type: none">送信接続 (現在のホストで開始された接続。MTAによって発信された接続など) を監視する必要がある場合は Yes送信接続を監視する必要がない場合は No
OutputDivertNfqueueNumber	Auto
OutputDivertConnectTransparently	No
InputDivertEnable	<ul style="list-style-type: none">受信接続 (リモートホストで開始される接続で、そのサーバー側は現在のホストで動作するMTAなどのアプリケーション) を監視する必要がある場合は Yes受信接続を監視する必要がない場合は No



パラメータ	必要な値
<code>InputDivertNfqueueNumber</code>	Auto
<code>InputDivertConnectTransparently</code>	Yes

Dr.Web Firewall for Linux>の設定を表示および変更するには、次の方法を使用します。

- [コマンドラインベースの管理ツール](#) - Dr.Web Ctl(**drweb-ctl** `cfshow`および**drweb-ctl** `cfset`コマンドを使用します)。
- Dr.Web for UNIX Mail Serversの管理[Webインターフェース](#)(デフォルトでは、Web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)。

次は、コマンドの例です。

```
# drweb-ctl cfset LinuxFirewall.InputDivertEnable Yes
```

Dr.Web Firewall for Linuxは次のように設定されます。受信接続を介して転送されたデータはSpIDer Gateによってチェックされ、それらのデータをチェックするために、メールスキャンコンポーネントDr.Web MailDにリダイレクトされます。`Inspect <protocol>`パラメーターの値がOnに設定されているメールプロトコル(SMTP、POP3、IMAP)が使用された場合にのみ、Dr.Web MailDにリダイレクトされます。

SSL/TLSの安全な接続を使用するメール配信チャネルにDr.Web for UNIX Mail Serversを統合するには、以下の追加アクションを実行する必要があります。

- 次のコマンドを実行して対応するパラメータの値を指定することで、SSL/TLS経由で送信されるトラフィックのスキャンを有効にします。

```
# drweb-ctl cfset LinuxFirewall.UnwrapSsl Yes
```

drweb-ctl ツールの`cfset`コマンドまたは管理Webインターフェースを使用することを推奨します。これらを使用した場合、スキャンルールが自動的に更新されるためです。スキャンルールはこのパラメータに依存します。

- 次のコマンドを実行して、Dr.Web for UNIX Mail Serversが保護されたSSL/TLSチャネルに統合するために使用する証明書をエクスポートします(証明書をPEM形式で保存するために使用されるファイルの名前を指定する必要があります)。

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

- 取得した証明書を信頼できる証明書のシステムリストに追加し、可能な場合には、それをメールクライアントおよびサーバー用の信頼できる証明書として書き込みます。詳細は、[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) スキャンパラメータを設定する

設定ファイルのDr.Web Firewall for Linuxの設定のセクション([LinuxFirewall] セクション)で次のパラメータを指定する必要があります。

1. メールメッセージスキャンの長さとしリソースの強度を制限する、メールメッセージとそこで検出された添付ファイルのスキャンパラメータ(`ScanTimeout`、`HeuristicAnalysis`、`PackerMaxLevel`、`ArchiveMaxLevel`、`MailMaxLevel`、`ContainerMaxLevel`、



MaxCompressionRatio)。きめ細かい設定が不要な場合は、パラメータデータの値をデフォルトの状態にしておくことを推奨します。

2. 対応するパラメータ**Block***を指定し、メールメッセージ内のリンクおよびファイルのスキャンパラメータを設定します。
3. 受信したメールメッセージのスキャンが不可能であること(設定限度を超える(前の項目を参照)、メールメッセージ構造の違反、スキャンエンジンのエラー、パスワードで保護されている添付アーカイブの可用性など)に対するDr.Web MailDの応答を定義する**BlockUnchecked**値のパラメータを指定します。このパラメータが**Yes**に設定されている場合、メールメッセージやその添付ファイルをスキャンできないときには、MTAはこのメールメッセージを拒否する設定を受け取ります。
4. メールメッセージのフィルタリングルールをよりきめ細かく(さまざまな条件に基づいて)設定するには、[Lua procedure](#)または**RuleSet**[ルール](#)を編集します。

すべての設定を調整したら、Dr.Web for UNIX Mail 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:

- メールサーバーの操作:
 - [Milter、Spamd、またはRspamdを介してDr.Web for UNIX Mail ServersをフィルターとしてMTAに接続する方法。](#)
 - [Dr.Web for UNIX Mail ServersをアンチウイルスフィルターClamdとしてMTAに接続する方法。](#)
 - [SMTPプロキシモード用に製品を設定する方法。](#)
 - [MTAのトランスペアレントプロキシモードを設定する方法。](#)
- Dr.Web for UNIX Mail Serversの一般的な動作:
 - [Dr.Web for UNIX Mail 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 Mail Serversを有効化する方法](#)
 - [Dr.Web for UNIX Mail Serversをアップグレードする方法](#)
 - [Dr.Web for UNIX Mail Serversコンポーネントを追加または削除する方法](#)
 - [Dr.Web for UNIX Mail 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](#)

Milter、Spamd、またはRspamdを介してDr.Web for UNIX Mail ServersをフィルターとしてMTAに接続する方法

[フィルターとしてのMTAとの統合](#)セクションの指示に従ってください。

Dr.Web for UNIX Mail ServersをアンチウイルスフィルターClamdとしてMTAに接続する方法

[外部アプリケーションとの統合](#)セクションの指示に従ってください。



この場合、メールスキャン(スパムの兆候のスキャンを含む)用に設計された特別なコンポーネント [Dr.Web MailD](#) は使用されません。MTAによって送信されたメールメッセージは、アンチウイルスによってのみスキャンされます。脅威が検出された場合、メッセージ処理はメールサーバーによって直接実行されます。

SMTPプロキシモード用にDr.Web for UNIX Mail Serversを設定する方法

[SMTPプロキシモードでDr.Web for UNIX Mail Serversを使用する](#)セクションの指示に従ってください。



MTAのトランスペアレントプロキシモードを設定する方法

[透過プロキシモードでDr.Web for UNIX Mail Serversを使用する](#)セクションの指示に従ってください。

Dr.Web for UNIX Mail Serversを再起動する方法

Dr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail Serversで提供される[Dr.Web Ctl](#)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 사용되는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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail Serversのアンチウイルス機能が**ブロック**されます。

Dr.Web for UNIX Mail 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。



Dr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail Serversコンポーネント

このセクションでは、Dr.Web for UNIX Mail 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設定デーモンは、Dr.Web for UNIX Mail Serversのコアコンポーネントです。すべてのDr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail Serversに通知します。

設定デーモンDr.Web ConfigDは常にroot権限で起動されます。他のDr.Web for UNIX Mail 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。設定デーモンは、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 Mail 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、設定デーモンにはDr.Web for UNIX Mail 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、設定管理デー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、デー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、デー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。デーモンは、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、起動時に設定デーモン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 Mail 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 Mail 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
--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
--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 Mail 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 Mail 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(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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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>	インターネットリソースカテゴリーの自動的に更新されるデータベースのファイルを含むディレクトリへのパス。 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 Mail 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 Mail 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 Mail Serversのインストール中に決定されます。
TrustedGroup <i>{group name / GID}</i>	信頼するユーザーのグループ。このパラメータはネットワークトラフィックモニターコンポーネント（SpIDer Gate）の動作に使用されます。これらのユーザーのネットワークトラフィックはスキャンされずにSpIDer Gateによってスキップされます。 ここには存在しないグループを指定することはできません。その場合、SpIDer Gateは起動に失敗します。 パラメータ値がない場合は、SpIDer Gate設定のOutputDivertパラメータにAuto値を指定することはできません。 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>	メールのスパムスキャンに使用される VadeRetro ライブラリのファイルへのパス(対応する機能が製品でサポートされている場合)。 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
AntispamDir <i>{path to directory}</i>	VadeRetro ライブラリのファイルを含むディレクトリへのパス。 デフォルト値: <var_dir>/antispam <ul style="list-style-type: none">• GNU/Linuxの場合: /var/opt/drweb.com/antispam• FreeBSDの場合: /var/drweb.com/antispam
VersionNotification <i>{Boolean}</i>	現在インストールされているDr.Web for UNIX Mail 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 Mail 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 Mail Servers設定のパラメータを確認・変更する
- Dr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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
<code>scan <path></code>	<p>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。</p> <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(<i>stdin</i>)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(<i>stdin</i>)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><p>--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)。</p></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>任意オプション、複数回設定できます。</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。



コマンド	説明
	<ul style="list-style-type: none">• JSON - JSON形式のシリアル化されたレポート。 デフォルト値 : <i>BRIEF</i> <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。 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>--PackerMaxLevel <number> - パックされたオブジェクトをスキャンする際のネスティングレベルの上限を指定します。 値に 0 が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。 デフォルト値 : 8</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。 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>--MailMaxLevel <number> - メールメッセージ(pst、tbbなど)をスキャンする際のネスティングレベルの上限を指定します。 値に 0 が指定された場合、ネストされたオブジェクトはスキャン中にスキップされます。 デフォルト値 : 8</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。 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>--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。 率は 2 以上にする必要があります。 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。 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。 使用可能な値 : REPORT、CURE、QUARANTINE、DELETE 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。 使用可能な値 : REPORT、QUARANTINE、DELETE 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>



コマンド	説明
	<p>使用可能な値: <i>REPORT</i>、<i>QUARANTINE</i>、<i>DELETE</i> 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> 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> 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>。 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> 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> デフォルト値: <i>REPORT</i></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 (<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。</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



コマンド	説明
	<ul style="list-style-type: none">• 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> <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>
proscan	<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><u>オプション:</u></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>




コマンド	説明
	<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>--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> <p>実行可能ファイルで脅威が検出された場合、Dr.Web for UNIX Mail 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。</p>
netscan [<path>]	<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 (scanコマンドと同様) を介してのみ行われます。</p>



コマンド	説明
	<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>この引数を省略すると、入力スレッド<code>stdin</code>を介して受信したデータがスキャンされます。</p> <p>オプション:</p> <p><code>--Report <type></code> - 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><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 2 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>--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>
flowscan <path>	<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</p> <div><p>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、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>--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 : On</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>




コマンド	説明
	<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>--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>-m [--Method] <i><SSH/Telnet></i> - 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>-l [--Login] <i><name></i> - 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>-i [--Identity] <i><path to file></i> - 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>-p [--Port] <i><number></i> - 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>--Password <i><password></i> - 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>--Exclude <i><path></i> - 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>--Report <i><type></i> - 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: BRIEF</p> <p>--ScanTimeout <i><number></i> - 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>--PackerMaxLevel <i><number></i> - 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>--ArchiveMaxLevel <i><number></i> - 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>--MailMaxLevel <i><number></i> - 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>
checkmail <path to file>	<p>目的 : (コンポーネント Dr.Web MailD を使用して) 脅威、スパムの兆候、悪意のあるリンク、またはメール処理ルールへの非適合などの理由でファイルに保存されているメールメッセージのスキャンを実行します。コンソール出力スレッド (<i>stdout</i>) は、メッセージスキャンの結果と、メールメッセージスキャンのために Dr.Web MailD コンポーネントによるスキャンの過程でこのメッセージに適用されたアクションを表示します。</p> <p>引数 :</p> <p><path to file> - スキャンが必要なメールメッセージのファイルへのパス。必須の引数です。</p> <p>オプション :</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>-r [--Rules] <list of rules> - メールメッセージのスキャン中に従うルールの一覧を指定します。</p> <p>ルールが指定されなかった場合、デフォルトで指定されている次のルールセットが適用されます。</p> <pre>threat_category in (KnownVirus, VirusModification, UnknownVirus, Adware, Dialer) : REJECT total_spam_score gt 0.80 : REJECT url_category in (InfectionSource, NotRecommended, CopyrightNotice) : REJECT</pre> <p><i>Dr.Web ASEがインストールされていない場合、スパムのスキャンルール(2番目のストリング)は自動的にセットから除外されます。</i></p> <p>-c [--Connect] <IP>:<port> - スキャンされるメッセージの送信者の接続用アドレスとして使用されるネットワークソケットを指定します。</p>



コマンド	説明
	<p>-e [--Hello] <name> - メッセージを送信したクライアントの識別子を指定します (IPアドレスまたはFQDNホスト、SMTPコマンドHELO/EHLO)。</p> <p>-f [--From] <email> - 送信者のメールアドレスを指定します (SMTPコマンドMAIL FROM)。</p> <p>アドレスが指定されていない場合、それぞれのメールのアドレスが使用されます。</p> <p>-t [--Rcpt] <email> - 受信者のメールアドレスを指定します (SMTPコマンドRCPT TO)。</p> <p>アドレスが指定されていない場合、それぞれのメールのアドレスが使用されます。</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 Mail 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 Mail 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。• <port> - 集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。



コマンド	説明
	<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 Mail 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 Mail 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 Mail 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><u>Dr.Web ClamD</u> 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 cfset ClamD.Endpoint.point1 -a</pre> <p>例：</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>
<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>.<parameter> = <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> = <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 <u>Dr.Web ConfigD</u> 設定デーモンに送信します。</p> <p>このシグナルを受信すると、Dr.Web ConfigD 設定デーモンは 設定 を再度読み込み、それに必要な変更を Dr.Web for UNIX Mail Servers コンポーネントに送信します。その後、設定デー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>



コマンド	説明
	オプション: None

3.4. 検出された脅威および隔離を管理するコマンド

検出された脅威および隔離を管理するコマンドには以下のものがあります。

コマンド	説明
threats [<action> <object>]	<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> <p><code>--Quarantine <threat list></code> - 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><code>--Delete <threat list></code> - 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><code>--Ignore <threat list></code> - 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>



コマンド	説明
	<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、<code><threat list></code> の代わりに <code>All</code> 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>
<code>quarantine</code> [<code><action></code> <code><object></code>]	<p>目的： <u>隔離</u> 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 <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、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><code>-a</code> [<code>--Autonomous</code>] - 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 <u>Dr.Web File Checker</u> 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><code>--Format</code> "<code><format string></code>" - 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 <u>以下</u> 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</code> [<code>--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>--Discovery</code> [<code><list of directories></code>,] - 指定されたディレクトリのリストから <u>隔離ディレクトリ</u> 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。<code><list of directories></code> 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> <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>



コマンド	説明
	<div><pre>quarantine --Autonomous --Discovery</pre></div> <p>--Delete <object> - 指定されたオブジェクトを隔離から削除します。 オブジェクトは隔離から永久に削除されることに注意してください。この操作は元に戻せません。</p> <p>--Cure <object> - 隔離内の指定されたオブジェクトの修復を試みます。 オブジェクトが修復された場合であっても、それは隔離内に残ります。修復されたオブジェクトを隔離から復元するには --Restore コマンドを使用します。</p> <p>--Restore <object> - 指定されたオブジェクトを隔離から元の場所に復元します。 このコマンドでは、drweb-ctlを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>--TargetPath <path> - オブジェクトを隔離から指定された場所に復元します。指定された名前を持つファイルとして復元するか (<path>がファイルへのパスであった場合)、またはただ単に指定されたディレクトリに復元します (<path>がディレクトリへのパスであった場合)。--Restore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><object> は隔離内のオブジェクトの識別子を指定します。隔離されたすべてのオブジェクトに対してコマンドを適用する場合は、<object>の代わりに All を指定してください。例：</p> <div><pre>\$ drweb-ctl quarantine --Restore All --TargetPath test</pre></div> <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testサブディレクトリに復元します。</p> <p>--Restore All では、追加のオプション --TargetPath (指定された場合)にはファイルへのパスではなくディレクトリへのパスを指定する必要があります。</p>

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
%{n}	新しい文字列
%{t}	集計



マーカー	説明
<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（「%Y-%b-%d %H:%M:%S」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
<code>%{htime}</code>	脅威に関連したイベントの日時
<code>%{app}</code>	脅威を処理したDr.Web for UNIX Mail ServersコンポーネントのID
<code>%{event}</code>	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。
<code>%{err}</code>	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
<code>%{qid}</code>	隔離されたオブジェクトのID
<code>%{qtime}</code>	オブジェクトを隔離に移動した日時



マーカー	説明
<code>%{curetime}</code>	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）
<code>%{cureres}</code>	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">• <code>cured</code> - 脅威は修復されています。• <code>not cured</code> - 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
<code>appinfo</code>	<p>目的: アクティブな Dr.Web for UNIX Mail 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">• 内部で使用される名前• プロセスIDGNU/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><code>-f [--Follow]</code> - 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>
<code>baseinfo</code>	<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>



コマンド	説明
	<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 Mail 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> <pre>\$ drweb-ctl certificate > <cert_name>.pem</pre> <p>引数：None</p> <p>オプション：None</p>
events	<p>機能：Dr.Web for UNIX Mail 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 <type> - 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] <date, time> - 指定されたタイムスタンプの前に発生したイベントを表示します（<date, time> は YYYY-MM-DD hh:mm:ss のフォーマットで指定します）。</p> <p>-u [--Until] <date, time> - 指定されたタイムスタンプの後に発生したイベントを表示します（<date, time> は YYYY-MM-DD hh:mm:ss のフォーマットで指定します）。</p> <p>-t [--Types] <type list> - 指定されたタイプのイベントのみを表示します（コンマで区切られます）。</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



コマンド	説明
	<p>・ UnexpectedAppTermination - コンポーネントの予期しないシャットダウン すべてのタイプのイベントを表示するには、All を使用します。</p> <p>--ShowSeen - 既読イベントも表示されます。</p> <p>--Show <list of events> - リストアップされたイベントを表示します (イベント識別子はコンマで区切られます)。</p> <p>--Delete <list of events> - リストアップされたイベントを削除します (イベント識別子はコンマで区切られます)。</p> <p>--MarkAsSeen <list of events> - リストアップされたイベントを既読としてマークします (イベント識別子はコンマで区切られます)。</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、<events list>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 Mail 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> <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 events コマンドの --Types オプションの説明を参照してください。この引数は必須です。</p> <p>オプション :</p> <p>-o [--Output] <path to file> - 指定したファイルにレポートを保存します。このオプションは必須です。</p> <p>-s [--Since] <date, time> - 指定されたタイムスタンプよりも後に発生したイベントのレポートを作成します (<date, time> は YYYY-MM-DD hh:mm:ss のフォーマットで指定します)。</p> <p>-u [--Until] <date, time> - 指定されたタイムスタンプよりも前に発生したイベントのレポートを作成します (<date, time> は YYYY-MM-DD hh:mm:ss のフォーマットで指定します)。</p> <p>--TemplateDir <path to directory> - HTMLレポートテンプレートを含むディレクトリへのパスです。</p> <p>-s、-u、--TemplateDirは必須のオプションではありません。</p> <pre>\$ drweb-ctl --report Mail -o report.html</pre> <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 report.html ファイルに保存します。</p>
idpass <identifier>	<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 MailID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</p>



コマンド	説明
	<p>ワードを表示します（つまり、RepackPassword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>-s [--Secret] <secret> - 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。<i>Dr.Web MailD設定</i>に示されます。また、RepackPassword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>
license	<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 <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<i>Doctor Web</i>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（stdout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>



コマンド	説明
	<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 Mail Serversの構成のセクションに記載されています。また、appinfo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: ファイルを処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> <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. *email.eml* ファイル内に保存されたメールメッセージを、デフォルトのルールセットを使用してスキャンする:

```
$ drweb-ctl checkmail email.eml
```

2. 設定の管理

1. 実行中のプロセスに関するものを含む、現在のDr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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
```

5. このメールメッセージに対して、パスワード生成のHMAC方法が使用されており、最新の秘密ワードがDr.Web MailDの設定で示されていることを条件に、ID 12345で保護されたアーカイブのパスワードをメールメッセージに生成します。

```
$ drweb-ctl idpass 12345
```



Dr.Web for UNIX Mail Serversにコンポーネントの1つとしてDr.Web MailDが含まれていない場合、コマンドの例5は機能しません。

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 Mail 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](#)
- [メールアーカイブのパスワードを復元する](#)

概要

Dr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail 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 Mail 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で、<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 Mail 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 Mail 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 Mail 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 Mail 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。
- **脅威を含んだ添付アーカイブのパスワード** - スパムの兆候がある不審なメールメッセージの添付ファイル、感染した添付ファイル、不審なURL付きのメールメッセージの一部を含むアーカイブの[パスワードを復元する](#)ためのパネルを表示します。
- **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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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。
- **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の名称の隣（右側）には、このカテゴリに分類される検出済みの脅威の数が表示されます。そのカテゴリに属する脅威が現在表示され、選択されているカテゴリは、暗い色のフォントで強調されています。必要なカテゴリの脅威を表示するには、メニューのカテゴリの名前をクリックしてください。



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（[SpIDer Gate](#)、[Dr.Web MailD](#)）、[Dr.Web ClamD](#)によって検出された脅威は、脅威ページには表示されません。これらのコンポーネントによって検出された脅威を追跡するために、SNMPを介して使用可能な脅威カウンターと追跡通知を制御できます（[Dr.Web SNMPD](#)はMIB Dr.Web[構造](#)に従って脅威カウンターと通知へのアクセスを与えます）。

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 Mail 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。
- 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



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 Mail 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 Mail 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 Mail 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 Mail 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ーを表示します。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 Mail 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 Gateの[設定パラメータ](#)。
- Dr.Web Firewall for Linuxの[設定パラメータ](#)。
- コンポーネントDr.Web MailD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 LookupD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 Mail 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 Mail 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 Settings) 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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。

メールアーカイブのパスワードを復元する

Webインターフェースでは、メールユーザーに受信された脅威を含んだ、保護されたアーカイブのパスワードを迅速に復元できます。このようなアーカイブは、[アクションPass](#)がメールメッセージに適用された場合に、スキャンされたメールメッセージの悪意のある不審な部分を保存するために、Dr.Web for UNIX Mail Serversによって使用されます。[設定パラメータ](#) `RepackPassword`の値に応じて、以下のようにアーカイブされます。

- パスワードで保護されていません (*None*)。
- パラメータに示されているのと同じパスワードで保護されています (*Plain*)。
- 秘密のワードと一意のメールメッセージ識別子に基づいて各アーカイブ用に生成された一意のパスワードで保護されています (*HMAC*)。

ユーザーが一意のメールメッセージ識別子を共有し、管理者がパスワード生成に使用される秘密のワードを知っている場合、パスワード復元のためのインターフェースでは、メールシステムの管理者は *HMAC* 方式で保護されたアーカイブのパスワードを(ユーザーのリクエストにより)復元できます(デフォルトでは、モード *HMAC* が設定されている場合、秘密のワードはパラメータ `RepackPassword` の値からの現在有効な秘密のワードとなります)。



パスワード生成方式が変更された場合、パスワード復号が正常に実行されるためには、脅威を含んだ保護されたアーカイブのメールメッセージのアンパックとパスワード生成の実行時に使用されていた秘密のワードが必要となります。

ユーザーのメールメッセージに一意の識別子がない場合、アーカイブのパスワード生成が *Plain* 方式を使用して実行されたことを意味し、パスワード復元インターフェースはパスワードを復元できません。

パスワードを復元する

脅威のある保護されたアーカイブのパスワードの復元は、Webインターフェースのメインメニューで**脅威を含んだ添付アーカイブのパスワード**項目を選択すると表示されるパネルを介して実行されます。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。パスワード復元パネルの外観は以下のようになります。



図12. メールアーカイブのパスワード復元パネル

HMAC方式で生成されたアーカイブのパスワードを復元するには、以下のように指示します。

- パスワードで保護されたアーカイブを含むメールメッセージの受信者によって提供された**メッセージID**を指定してください。
- メール処理時にDr.Web MailD設定で使用された**秘密のフレーズ**(デフォルトでは、パスワード生成のHMAC方式がDr.Web MailD設定で指示されている場合、このフィールドには現在有効な秘密のワードを入力します)。

アーカイブのパスワードを復元するには、**パスワードを取得**をクリックします。生成されたパスワードは、**アーカイブのパスワード**フィールドに表示されます。

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。

Dr.Web MailD

Dr.Web MailDは、メールの直接スキャン、悪意のあるコンテンツの検出(添付ファイルだけでなく望ましくないWebサイトへのリンクも含む)、およびメッセージにスパムの兆候があるかどうかに関する解析とメッセージがメールシステム管理者によって指定されたセキュリティ基準に準拠しているかどうかに関する解析(管理者によって指定された正規表現を使用したメールメッセージの本文とヘッダーのスキャン)を行えるように設計されています。

このコンポーネントは、標準のインターフェースである *Milter*、*Spamd*、*Rspamd*(これらのインターフェースは通常、**SpamAssassin**フィルターで使用されます)を介してメールサーバー(MTA)に統合したり、送信側と受信側(MTAとMTA、MDAとMUA)にとって透過的にメールプロトコル(SMTP、POP3、IMAP)に統合したりできます。2番目の方法は、**SpIDer Gate**コンポーネントのネットワークトラフィックのスキャン機能がDr.Web MailDコンポーネントによって使用されることを意味します。



[SpIDer Gate](#)モニターはGNU/Linux環境でのみ動作するため、透過的な統合方法（「プロキシ」モード）は、GNU/Linux環境で動作するメールサーバーでのみ使用できます。

メールメッセージのスキャンの負荷が高まると、[Dr.Web Network Checker](#)コンポーネントによって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 Mail Serversに使用可能なファイル記述子の数の[上限を増やす](#)必要があります。

動作原理

コンポーネントでメールを保護する方法には、次の2つがあります。

1. 外部のメールフィルタとしてのメールサーバー（**Sendmail**、**Postfix**、**Exim**など）への接続（次の拡張機能を使用：*Milter*、*Spamd*、*Rspamd*）。
2. SMTP、POP3、IMAP4のプロトコルを介してメールサーバーに対して透過的に転送されたメールのスキャンを実行するプロキシの設定。このスキャン方法の設定には、[SpIDer Gate](#)と[Dr.Web Firewall for Linux](#)が使用されます。これらのコンポーネントはGNU/Linuxでしか動作しないことから、この方法はGNU/LinuxファミリーのOSでのみ使用できます。

スキャンされたメールメッセージは、コンポーネント設定で設定されているルールに従って処理されます。メールサーバーとのインタラクションに使用されるインターフェースごとに、メールメッセージ処理のための独自のルールセットを指定できます。プロキシメカニズムを使用する場合（プロトコルSMTP、POP3、IMAPを介して直接受信したメールメッセージをスキャンする際など）、コンポーネントはDr.Web Firewall for Linuxの設定で決定された処理ルールを使用します。

メールメッセージのURLのスキャンには、SpIDer Gateコンポーネントと同じWebリソースカテゴリーのデータベースが使用されます。[Dr.Web CloudD](#)コンポーネントは、Dr.Web Cloudクラウドサービスを参照するために使用されます（クラウドサービスの使用はDr.Web for UNIX Mail Serversの[共通設定](#)で設定され、必要に応じて無効化できます）。送信されたデータを確認するために、Dr.Web MailDは[Dr.Web Network Checker](#)コンポーネントを使用します。後者では、[Dr.Web Scanning Engine](#)スキャンエンジンを介してスキャンが開始されます。

MTAから*Milter*、*Spamd*、*Rspamd*のインターフェースを介して（[フィルターモード](#)で）受信されたメールメッセージの処理は、Luaで記述された特別な処理手順（*hook*）を呼び出すことによって実装されます。この手順の間に、メッセージに関して利用可能なすべての情報（送信者、受信者、内部構造、ヘッダー値、スパムスコア）を分析した結果に従って、メッセージが拒否されるかスキップされるかが決定されます。*Milter*インターフェースの場合、MTAがメッセージに適用するアクション（「pass」、「reject」、「return an error to sender」など）が返されます。検証手順の一部が「pass」の場合、ヘッダーを追加/変更など、レターに変更が加えられる場合があります。メッセージの悪意のある部分はパスワードで保護されたアーカイブに保存（つまりリパック）されます。スキャン対象のメッセージの変更をサポートしていない*Spamd*や*Rspamd*のインターフェースの場合、判定は、その文字に割り当てられた「スパムレート」およびレターをスパムとして認識するためのしきい値の形でMTAに返されます（MTAからのレターを拒否するには、レートがしきい値を超過している必要があります）。レートに加えて、テキストによる判定（プロトコルによってreportまたはaction）がMTAに返されます。これはMTA設定で分析できます。

Luaの柔軟性と処理手順から得られる多数のメッセージ情報により、Dr.Web Anti-Spamから受け取ったスコアによる典型的なスパムチェックや、添付された脅威または悪質なURLの検索だけでなく、メールサーバーによるメールメッセージ処理に必要な判定と連携した、任意の条件のチェックも実装できます。検証手順の詳細と手順の例については、[Luaでのメール処理](#)のセクションを参照してください。



スパムの兆候の存在に関するメッセージ分析では、Dr.Web MailDは特別なコンポーネント[Dr.Web Anti-Spam](#)を使用します。



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

コマンドライン引数

Dr.Web MailD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-maild [<parameters>]
```

Dr.Web MailD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-maild --help
```

このコマンドはDr.Web MailD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 Mail Serversの他のコンポーネントからメールオブジェクトスキャンのリクエストを受信するときに、[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し、必要に応じてメールオブジェクトをスキャンするには、Dr.Web for UNIX Mail 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 MailDコンポーネントによる任意のメールメッセージの処理をスキャンするには、Dr.Web Ctlツールのcheckmailコマンドを使用します。これを行うには、スキャンしたメールメッセージをドライブに保存して（.eml形式など）、次のコマンドを使用します。

```
$ drweb-ctl checkmail <path to file .eml>
```



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-maild**

設定パラメータ

コンポーネントは、Dr.Web for UNIX Mail Serversの統合された[設定ファイル](#)の[MailD]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-maild <ul style="list-style-type: none">• GNU/Linuxの場合: /opt/drweb.com/bin/drweb-maild• FreeBSDの場合: /usr/local/libexec/drweb.com/bin/drweb-maild
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
FixedSocketPath <i>{path to file}</i>	固定コンポーネントコピーの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。 デフォルト値: (未設定)
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
TemplatesDir	メールがブロックされた場合にユーザーに返されるメールのテンプレートを含むディレクトリへのパス。



<code>{path to directory}</code>	<p>デフォルト値: <code><var_dir>/templates/maild</code></p> <ul style="list-style-type: none">• GNU/Linuxの場合 合: <code>/var/opt/drweb.com/templates/maild</code>• FreeBSDの場合: <code>/var/drweb.com/templates/maild</code>
TemplateContacts <code>{string}</code>	<p>脅威に関するメッセージに挿入されるDr.Web for UNIX Mail Serversの管理者の連絡先(メッセージテンプレートで使用されます)。</p> <p>連絡先情報は、最初のメッセージから脅威やその他の望ましくないオブジェクトが削除されている、パスワードで保護されたアーカイブを含む添付ファイルを取得した場合にのみ、リパックされたメッセージに追加されます。RepackPasswordパラメータの現在の値(以下参照)に従って添付アーカイブがパスワードで保護されていない場合、連絡先情報は変更されたメッセージに追加されません。</p> <p>デフォルト値: (未設定)</p>
ReportLanguages <code>{string}</code>	<p>サービスメールメッセージ(メールがブロックされた場合に送信者に返されるメールメッセージなど)の生成に使用される言語。各言語は2文字の表記(<i>en</i>, <i>ru</i>など)で識別されます。</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: 言語 <i>ru</i> および <i>de</i> をリストに追加します。</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<div><pre>[MailD] ReportLanguages = "ru", "de"</pre></div>• 2つの文字列(文字列ごとに1つの値)<div><pre>[MailD] ReportLanguages = ru ReportLanguages = de</pre></div>2. コマンド <code>drweb-ctl cfset</code> を使用して値を追加します。 <div><pre># drweb-ctl cfset MailD.ReportLanguages -a ru # drweb-ctl cfset MailD.ReportLanguages -a de</pre></div> <p>デフォルト値: <i>en</i></p>
RepackPassword <code>{None Plain(<password>) HMAC(<secret>)}</code>	<p>メッセージに添付され受信者に送信された悪意のあるオブジェクトのアーカイブのパスワードを生成する方法。以下の方法を使用できます。</p> <ul style="list-style-type: none">• なし - アーカイブはパスワードで保護されません(非推奨)。



	<ul style="list-style-type: none">• Plain (<password>) - すべてのアーカイブが同じパスワード<password>で保護されます。• HMAC (<secret>) - <secret>と<message identifier>のペアに基づいてアーカイブごとに一意のパスワードが生成されます。 <p>メッセージIDと既知のシークレットを使用してアーカイブを保護するパスワードを復元するには、drweb-ctl idpass コマンドを使用します。</p> <div> デフォルトでは、このパラメータには値Noneが設定されています。これはDr.Web for UNIX Mail Serversの設定中に変更することを推奨します。</div> <p>デフォルト値 : なし</p>
ScanTimeout <i>{time interval}</i>	<p>Dr.Web MailDによって開始された1つのメールメッセージのスキャンのタイムアウトを設定します。</p> <p>1秒から1時間の範囲の値を指定できます。</p> <p>デフォルト値 : 3m</p>
HeuristicAnalysis <i>{On / Off}</i>	<p>Dr.Web MailDによって開始されたメールメッセージの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。</p> <p>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>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>
PackerMaxLevel <i>{integer}</i>	<p>圧縮されたオブジェクトスキャン時の最大ネストレベルを設定します。Dr.Web MailDによって開始されたスキャン中に、より深い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>
ArchiveMaxLevel <i>{integer}</i>	<p>パックされたオブジェクトをスキャンする際の最大ネストレベルを指定します。Dr.Web MailDによって開始されたスキャン中に、より深い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>
MailMaxLevel <i>{integer}</i>	<p>メールメッセージとメールボックスのスキャン時の最大ネストレベルを指定します。Dr.Web MailDによって開始されたスキャン中に、より深い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>
ContainerMaxLevel <i>{integer}</i>	<p>他のコンテナ (HTMLページなど) のスキャン時の最大ネストレベルを指定します。Dr.Web MailDによって開始されたスキャン中に、より深い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>
MaxCompressionRatio <i>{integer}</i>	<p>圧縮/バ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Dr.Web MailDによって開始された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>
MilterSocket <i>{path to file / IP address:port}</i>	<p>メールの <i>Milter</i> フィルターとしてMTAに接続するためのソケット (Dr.Web MailDを対応するフィルターとして使用しているときに、MTAはこのソケットに接続します)。UNIXソケットまたはネットワークソケットを使用できます。</p> <p><i>Milter</i> 経由で送信されるメッセージの処理ルールは、MilterHook パラメータで指定します (以下を参照)。</p> <p>デフォルト値 : (未設定)</p>
MilterDebugIpc <i>{Boolean}</i>	<p><i>Milter</i> プロトコルメッセージをデバッグログに出力します (LogLevel = Debug)。</p> <p>デフォルト値 : No</p>
MilterTraceContent <i>{Boolean}</i>	<p><i>Milter</i> プロトコルインターフェースを介してスキャン用に受信したメールメッセージの本文をデバッグログに出力します (LogLevel = Debug)。</p> <p>デフォルト値 : No</p>
MilterHook <i>{path to file / Lua function}</i>	<p><i>Milter</i> インターフェース経由で受信したメールメッセージを処理する Lua スクリプト、またはスクリプトを含むファイルへのパス (Luaでのメール処理 セクションを参照)。</p> <p>使用できないファイルを指定すると、コンポーネントを読み込む際にエラーが表示されます。</p> <p>デフォルト値 :</p> <pre>local dw = require "drweb" local dwcfg = require "drweb.config" function milter_hook(ctx) -- Reject the message if it is likely spam if ctx.message.spam.score >= 100 then</pre>



	<pre>dw.notice("Spam score: " .. ctx.message.spam.score) return {action = "reject"} else -- Assign X-Drweb-Spam headers in accordance with spam report ctx.modifier.add_header_field("X-DrWeb- SpamScore", ctx.message.spam.score) ctx.modifier.add_header_field("X-DrWeb- SpamState", ctx.message.spam.type) ctx.modifier.add_header_field("X-DrWeb- SpamDetail", ctx.message.spam.reason) ctx.modifier.add_header_field("X-DrWeb- SpamVersion", ctx.message.spam.version) end -- Check if the message contains viruses, repack if so for threat, path in ctx.message.threats{category = {"known_virus", "virus_modification", "unknown_virus", "adware", "dialer"}} do ctx.modifier.repack() dw.notice(threat.name .. " found in " .. (ctx.message.part_at(path).name or path)) end -- Repack if unwanted URL has been found for url in ctx.message.urls{category = {"infection_source", "not_recommended", "owners_notice"}} do ctx.modifier.repack() dw.notice("URL found: " .. url .. "(" .. url.categories[1] .. ")") end -- Assign X-AntiVirus header ctx.modifier.add_header_field("X-AntiVirus", "Checked by Dr.Web [MailD version: " .. dwcfg.maild.version .. "]") -- Accept the message with all scheduled transformations applied return {action = 'accept'} end</pre>
SpamdSocket <i>{path to file / IP address:port}</i>	<p>メールメッセージの <i>Spamd</i> フィルターとして MTA に接続するためのソケット (Dr.Web MailD を対応するフィルターとして使用しているときに、MTA はこのソケットに接続します)。UNIX ソケットまたはネットワークソケットを使用できます。</p> <p><i>Spamd</i> 経由で送信されるメッセージの処理ルールは、SpamdReportHook パラメータで指定します (以下を参照)。</p> <p>デフォルト値: (未設定)</p>



SpamdDebugIpc <i>{Boolean}</i>	<i>Spamd</i> プロトコルメッセージをデバッグログに出力します (LogLevel = Debug)。 デフォルト値: No
SpamdReportHook <i>{path to file / Lua function}</i>	<i>Spamd</i> インターフェース経由で受信したメールメッセージを処理する Luaスクリプト、またはスクリプトを含むファイルへのパス (Luaでのメール処理 セクションを参照)。 使用できないファイルを指定すると、コンポーネントを読み込む際にエラーが表示されます。 デフォルト値: <pre>local dw = require "drweb" function spamd_report_hook(ctx) local score = 0 local report = "" -- Add 1000 to the score for each threat found in the message for threat, path in ctx.message.threats{category = {"known_virus", "virus_modification", "unknown_virus", "adware", "dialer"}} do score = score + 1000 report = report .. "Threat found: " .. threat.name .. "\n" dw.notice(threat.name .. " found in " .. (ctx.message.part_at(path).name or path)) end -- Add 100 to the score for each unwanted found URL in the message for url in ctx.message.urls{category = {"infection_source", "not_recommended", "owners_notice"}} do score = score + 100 report = report .. "Url found: " .. url .. "\n" dw.notice("URL found: " .. url .. "(" .. url.categories[1] .. ")") end -- Add the spam score score = score + ctx.message.spam.score report = report .. "Spam score: " .. ctx.message.spam.score .. "\n" if ctx.message.spam.score >= 100 then dw.notice("Spam score: " .. ctx.message.spam.score) end -- Return the check result return { score = score, threshold = 100,</pre>



	<pre>report = report } end</pre>
SpoolDir <i>{path to directory}</i>	スキャンされたメールメッセージの一時ストレージディレクトリ。 デフォルト値: /tmp/com.drweb.maild
RspamdHttpSocket <i>{path to file / IP address:port}</i>	メールの <i>Rspamd</i> フィルターとして MTA に接続するためのソケット (このソケットは、 <i>Rspamd</i> プロトコルの HTTP オプションで Dr.Web MailD を対応するフィルターとして使用している間、MTA によって使用されます)。UNIX ソケットまたはネットワークソケットを使用できます。 <i>Rspamd</i> を介して送信されるメッセージの処理ルールは、 RspamdHook パラメータで指定されます (以下を参照)。 デフォルト値: (未設定)
RspamdSocket <i>{path to file / IP address:port}</i>	メールの <i>Rspamd</i> フィルターとして MTA に接続するためのソケット (このソケットは、 <i>Rspamd</i> プロトコルの HTTP オプションで Dr.Web MailD を対応するフィルターとして使用している間、MTA によって使用されます)。UNIX ソケットまたはネットワークソケットを使用できます。 デフォルト値: (未設定)
RspamdDebugIpc <i>{Boolean}</i>	<i>Rspamd</i> プロトコルメッセージをデバッグログに出力します (LogLevel = Debug)。 デフォルト値: No
RspamdHook <i>{path to file / Lua function}</i>	<i>Rspamd</i> インターフェース経由で受信したメールメッセージを処理する Lua スクリプト、またはスクリプトを含むファイルへのパス (Lua でのメール処理 セクションを参照)。 使用できないファイルを指定すると、コンポーネントを読み込む際にエラーが表示されます。 デフォルト値: <pre>local dw = require "drweb" function rspamd_hook(ctx) local score = 0 local symbols = {} -- Add 1000 to the score for each threat found in the message for threat, path in ctx.message.threats{category = {"known_virus", "virus_modification", "unknown_virus", "adware", "dialer"}} do score = score + 1000 table.insert(symbols, {name = threat.name, score = 1000}) dw.notice(threat.name .. " found in " .. (ctx.message.part_at(path).name or path)) end</pre>



```
-- Add 100 to the score for each unwanted URL
found in the message
for url in ctx.message.urls{category =
{"infection_source", "not_recommended",
"owners_notice"}} do
    score = score + 100
    table.insert(symbols, {name = "URL " ..
url, score = 100})
    dw.notice("URL found: " .. url .. "(" ..
url.categories[1] .. ")")
end

-- Add the spam score
score = score + ctx.message.spam.score
table.insert(symbols, {name = "Spam score",
score = ctx.message.spam.score})
if ctx.message.spam.score >= 100 then
    dw.notice("Spam score: " ..
ctx.message.spam.score)
end

-- Return the check result
return {
    score = score,
    threshold = 100,
    symbols = symbols
}
end
```

メールシステムとの統合

Dr.Web MailDとメールシステムとの統合については、以下のセクションで説明します。

- [フィルターとしてのMTAとの統合](#) - Dr.Web MailDを、メールスキャン用の外部フィルターとして、メールサーバー（**Exim**、**Sendmail**、**Postfix**）に接続します。
- [SMTPプロキシモードでDr.Web for UNIX Mail Serversを使用する](#) - メールスキャンの外部フィルターとしてメールメッセージの転送を実行するメールサーバーへのDr.Web MailDの接続。
- [透過プロキシモードでDr.Web for UNIX Mail Serversを使用する](#) - Dr.Web MailDをメールプロトコル（SMTP、POP3、IMAP）に直接統合します。MTA/MDAおよびMUAに対して透過します。

それ以外にも、MTAを[コンポーネント](#) Dr.Web ClamDに直接[接続](#)して、スパムの兆候やその他の脅威に対してメールスキャンを実行できます。

Luaでのメール処理

このセクションの内容：

- [概要](#)
- [Milter用のスクリプト](#)
- [Spamd用のスクリプト](#)
- [Rspamd用のスクリプト](#)



- [メッセージ構造を説明する表](#)
- [メッセージ構造を説明するテーブル](#)

概要

Dr.Web MailDコンポーネントはLuaプログラムインタプリタを介したインタラクションをサポートします（バージョン5.3.4を使用。Dr.Web for UNIX Mail Serversに同梱）。Luaで記述されたスクリプトをコンポーネントで使用すると、メールメッセージの分析と処理を実行できます。

いずれかのインターフェース（*Milter*、*Spamd*、*Rspamd*）を介してスキャン用に受信したメールメッセージの解析は、対応する*Hookパラメータの指定したインターフェースのパラメータグループにあるDr.Web MailD設定で指定されるLuaのスクリプトを使用して実行されます（Luaプログラムテキスト、または必要な処理プログラムを含むファイルへのパスのいずれかを指定できます）。



その他のメール処理用 Luaスクリプトの例は、次の場所にあります。
<https://github.com/DoctorWebLtd/drweb-lua-examples/tree/master/maild>

Milterインターフェースのメッセージ処理のためのスクリプト

スクリプトの必要条件

ファイルには、メッセージスキャンモジュールのエントリポイントとなるグローバル関数が含まれている必要があります（Dr.Web MailDは、新しく受信したメッセージを処理する際にこの関数を呼び出します）。処理関数は、次の呼び出し規則を満たす必要があります。

1. 関数名は`milter_hook`です。
2. 引数は`MilterContext`テーブルのみです（関数から処理されたメールメッセージに関する情報へのアクセス権限を付与します）。
3. 返り値は`MilterResult`完了テーブルのみです。返り値は、スキャンされたメッセージについての判定（承認:"accept"、拒否:"reject"、変更:"change"、破棄:"discard"）の他、メッセージが承認された場合にメッセージに適用される（可能性がある）アクションを定義します。

*Milter*インターフェースを介してスキャンするために受信されたすべてのメッセージの*Accept*判定を無条件にDr.Web MailDに返すスクリプトの定義例（`ctx`引数は`MilterContext`テーブルのインスタンスになります）

```
function milter_hook(ctx)
    return {action = "accept"}
end
```

例

処理中に以下の変更を加える例：

- メールメッセージで検出された脅威の名前をヘッダー**X-Found**の値として追加する。
- スпамスコアが100ポイントを超える場合は、メールの件名（ヘッダー**Subject**の値）に" [SPAM] "プレフィックスを追加する。



```
function milter_hook (ctx)

-- 検出された脅威の名前をヘッダーに追加します
for threat in ctx.message.threats() do
    ctx.modifier.add_header_field("X-Found", threat.name)
end

-- メッセージのスパムスコアが100ポイントを超える場合は、
-- Subjectヘッダーの値を変更します
if ctx.message.spam.score > 100 then
    local old_value = ctx.message.header.value("Subject") or ""
    local new_value = "[SPAM] " .. old_value
    ctx.modifier.change_header_field("Subject", new_value)
end

-- 保留中の変更を適用して受信者にメッセージを送信します
return {
    action = "accept",
    modifications = ctx.modifier.modifications()
}

end
```

処理中にメッセージをリパックする例:

- 検出された脅威を保護されたアーカイブに移動する。
- スпамスコアが100ポイントを超える場合は、保護されたアーカイブにメールメッセージを移動する。

```
function milter_hook(ctx)

ctx.modifier.repack_password = "xxx"
ctx.modifier.repack_message = ""

-- すべての部分をパスワードで保護されたアーカイブに移動します
-- 脅威が見つかったメッセージ
for threat, path in ctx.message.threats() do
    ctx.modifier.repack(path)
    local msg = " Threat found: " .. threat.name
    ctx.modifier.repack_message = ctx.modifier.repack_message .. msg
end

-- スпамスコアが100ポイントを超えている場合、
-- メッセージ全体をリパックします
if ctx.message.spam.score > 100 then
    ctx.modifier.repack()
    local msg = " Spam score: " .. ctx.message.spam.score
    ctx.modifier.repack_message = ctx.modifier.repack_message .. msg
end

-- 保留中の変更を適用して受信者にメッセージを送信します
-- 変更テーブルが指定されていない場合は、
-- 自動的に返されます
return {action = "accept"}

end
```



メッセージから削除された不要な部分をすべて含むアーカイブは、新しく生成されたメッセージ(リパックされたメッセージ)の添付ファイルとして受信者に送信されます。アーカイブはパスワードで保護されます。この場合のパスワードは、文字列"xxx"が強制的に適用されます。

使用中のテーブル

テーブルMilterContext

milter_hook関数の入力引数として使用されます。処理されたメールメッセージに関する情報(フィールド、構造、ヘッダー、本文、送信者と受信者に関する情報、SMTPセッションに関する情報)へのアクセス権限を提供します。テーブルには以下のフィールドを含みます。

フィールド	説明	データタイプ
session_id	このクライアントからのメッセージが処理されている間のクライアントセッションの識別子。	文字列
sender	メールの送信者に関する情報。	テーブル MilterSender
helo	メールメッセージを送信したSMTPクライアントから受信したウェルカム文字列 HELO/EHLO、または文字列が見つからない/不明の場合 (MTAによって提供されない場合)はnil	文字列
from	山括弧なしの送信者のメールアドレス(例:user@domain.com)	文字列
to	山括弧なしの受信者のメールアドレス	テーブル RcptTo
message	メール(本文とすべてのヘッダーを含む)	テーブル MimeMessage
modifier	MilterModifier テーブルには、 MilterResult テーブルのスキャン結果に従って"accept"アクションが生成された場合にメッセージに行われるすべての変更が含まれます。	テーブル MilterModifier
無効になったメタメソッド: なし		

テーブルMilterSender

[MilterContext](#)テーブルのsenderフィールドとして使用されます。このテーブルには、メール送信者に関する情報が格納され、以下のフィールドが含まれます。

フィールド	説明	データタイプ
hostname	送信者のホスト名(FQDN)	文字列
family	文字列で示した接続タイプ <ul style="list-style-type: none">"U" - 不明なタイプ"L" - UNIXソケット経由の接続"4" - IPv4経由の接続"6" - IPv6経由の接続	文字列



フィールド	説明	データタイプ
port	ポート番号	整数
ip	送信者のホストのIPアドレス。IPアドレスがないか不明の場合（MTAから提供されない場合）はnil	テーブル IpAddress
無効になったメタメソッド: なし		

テーブルMilterResult

結果として使用されます。milter_hook関数によって返されます。以下のフィールドを含みます。

フィールド	説明	データタイプ
action	メッセージに適用するアクションの説明を含む文字列: <ul style="list-style-type: none">"accept" - 承認（MTAから受信者へのメッセージ送信を許可します）。"discard" - 送信者に通知せずにメッセージを破棄します"reject" - メッセージを拒否し、SMTP 5**コードを送信者に返します。"tempfail" - メッセージを拒否し、SMTP 4**コードを送信者に返します。"replycode" - codeフィールドで指定されたSMTP応答を送信者に送信します。 必須フィールド。	文字列
code	送信者に送信される3桁のSMTP応答コード（例: "541"）。 オプションのフィールドです。action = "replycode"の場合にのみ使用します。	文字列
text	送信者に送信される応答テキストを含む文字列（例: "User not local or invalid address - Relay denied"）。 オプションのフィールドです。action = "replycode"の場合にのみ使用します。	文字列
message	送信者に送信された応答テキストを含む文字列（例: "Message rejected as spam"）。 オプションのフィールドです。action = "reject"の場合にのみ使用します。	文字列
modifications	変更の説明を含むテーブル。受信者に送信する前にメールメッセージに適用されます。	テーブル MilterModifications



フィールド	説明	データタイプ
	オプションのフィールドです。 action = "accept"の場合にのみ使用します。	
added_recipients	追加のメッセージ受信者のメールアドレスのリスト。 オプションのフィールドです。 action = "accept"の場合にのみ使用します。	文字列の配列
deleted_recipients	メッセージ受信者のリストから除外する必要があるメールアドレスのリスト。 オプションのフィールドです。 action = "accept"の場合にのみ使用します。	文字列の配列
incident	Mailタイプの 登録済みイベント のインシデントの説明。 <ul style="list-style-type: none">このフィールドが文字列の場合、この文字列の内容がMailイベントの <i>incident_text</i> フィールドに送信され、イベントが登録されます。このフィールドがブール値で <code>false</code> に等しい場合、Mailイベントの <i>incident_text</i> フィールドは存在せず、イベントは登録されません。このフィールドがブール値で <code>true</code> に等しい場合、Mailイベントの <i>incident_text</i> フィールドは自動的に入力され、<i>incident_text</i> の値が空でない場合はイベントが登録されます。	文字列またはブール値
無効になったメタメソッド: なし		

テーブル *MilterModifications*

受信者への配信が決定された場合 (`accept` アクションが選択された場合) に、メールメッセージに対して行われる必要がある、すべての変更の説明に使用されます。次のフィールドが含まれます (すべてのフィールドはオプションです。対応するフィールド値がない場合、アクションはメッセージに適用されません)。

フィールド	説明	データタイプ
new_body	処理されたメッセージの本文を置き換えるために使用される新しいメッセージ本文 (ヘッダーなし)	文字列
added_fields	処理されたメッセージに追加されるヘッダー	MilterAddedField テーブルの配列
changed_fields	処理されたメッセージから変更または削除されるヘッダー	MilterChangedField テーブルの配列
無効になったメタメソッド: なし		

テーブル *MilterAddedField*

処理されたメッセージに追加されるヘッダーの説明に使用されます。以下のフィールドを含みます。



フィールド	説明	データタイプ
name	ヘッダー名	文字列
value	ヘッダー値	文字列
無効になったメタメソッド: なし		

テーブル *MilterChangedField*

処理されたメッセージ内で変更される(または削除される)ヘッダーの説明に使用されます。以下のフィールドを含みます。

フィールド	説明	データタイプ
name	ヘッダー名	文字列
index	変更するメッセージ内でnameの名前を持つヘッダーの序数(1からカウント)	番号
value	ヘッダーの新しい値(ヘッダーを削除する場合、値は空の文字列""になります)。	文字列
無効になったメタメソッド: なし		



処理後にメッセージに加えられる変更の説明については、[MilterModifications](#)テーブルに直接入力しないことをお勧めします。代わりに、コンテキストから受け取ることができる[MilterModifier](#)テーブルのメソッドを使用してください。

テーブル *MilterModifier*

処理後(および受信者に送信される場合)に、メッセージの変更のスケジュールを設定するためのインターフェースを提供するために使用されます。以下のフィールドを含みます。

フィールド	説明	データタイプ
add_header_field	メールメッセージに新しいヘッダーを追加するアクションのスケジュールを設定する関数。 次の2つの必須の引数を受け取ります。 <ul style="list-style-type: none">• nameはヘッダー名(文字列)です。• valueはヘッダー値(文字列)です。 値はRFC 2047に従ってエンコードされます。	機能
change_header_field	指定されたヘッダーを変更(または削除)するアクションのスケジュールを設定する関数。 次の2つの必須の引数を受け取ります。 <ul style="list-style-type: none">• nameはヘッダー名(文字列)です。	機能



フィールド	説明	データタイプ
	<ul style="list-style-type: none">• valueはヘッダー値（文字列）です。 <p>メッセージに指定された名前を持つ複数のヘッダーがある場合、この関数はその名前を持つ最初のヘッダーの値を変更します。同じヘッダーの値が複数回変更された場合は、最後の値だけが保持されます。valueが空の文字列""の場合、ヘッダーのnameはメッセージから削除されます。</p> <p>値はRFC 2047に従ってエンコードされます。</p>	
modifications	メールメッセージへの実行がスケジュール設定されている変更の全リストを含む MilterModifications テーブルを返す関数。引数はありません。	機能
repack	<p>指定したメッセージ部分（部分が指定されていないか指定された部分がない場合はメッセージ全体）のリパックのスケジュールを設定する関数。リパック中に、指定した部分がパスワード付きでアーカイブに追加されます。</p> <p>オプションの引数pathまたはiteratorを受け入れます。</p> <ul style="list-style-type: none">• pathは、アーカイブされるスキャンされたメールの添付ファイルへのパスです。パスが指定されていない場合や、指定されたパスが無効な場合は、メッセージ全体がアーカイブされます。• iteratorはメッセージ部分の反復子であり、関数によって、MimePartテーブルのthreats、urls、attachments、files、parts、leaf_parts、text_partsが返されます。この場合、反復子から返されたメッセージのすべての部分がリパックされるようにスケジュールされます。 <p>関数の引数が指定されていない場合、または指定されたパスが無効な場合は、メッセージ全体がアーカイブされます。</p> <p>例：</p>	機能



フィールド	説明	データタイプ
	<pre>-- パスワード付きアーカイブへのメッセージのリパッ クのスケジュールを設定します -- (メッセージ全体) ctx.modifier.repack() -- パスワード付きアーカイブへのメッセージのリパッ クのスケジュールを設定します -- 指定されたパスのメッセージ部分(または -- その部分がない場合メッセージ全体) ctx.modifier.repack('/1/2/3') -- パスワード付きアーカイブへのメッセージのリパッ クのスケジュールを設定します -- (実行ファイルを含むすべての部分) ctx.modifier.repack(ctx.message.fi les{name='*.exe'}) -- パスワード付きアーカイブへのメッセージのリパッ クのスケジュールを設定します -- (すべてのZIP添付ファイル) ctx.modifier.repack(ctx.message.at tachments{name='*.zip'})</pre>	
repack_archive_name	メッセージの悪意のあるアイテムまたは不要なアイテムを圧縮するためのアーカイブの名前。デフォルトでは、"quarantine.zip"。	文字列
repack_password	アーカイブ保護のためのパスワード。指定されていない場合は、構成ファイルに指定されたパスワードが使用されます(RepackPassword パラメータ)。	文字列
repack_message	メッセージ(またはその部分)のリパックの理由を表す任意のメッセージ。最終メッセージに追加されます(省略することもできます)。	文字列
templates_dir	リパックのためのテンプレートが保存されているディレクトリへのパス。パスは、設定ファイル(TemplatesDir パラメータ)に指定したパスを基準にした相対パスになります。デフォルト値は"milter"です(つまり、milterサブディレクトリのテンプレートが使用されます)。	文字列
無効になったメタメソッド: なし		

このテーブルにアクセスするには、[MilterContext](#)テーブルのmodifierフィールドを使用する必要があります。
例:



```
function milter_hook(ctx)

-- ヘッダーリストの末尾に新しいヘッダーを追加する
-- スケジュールを設定します
ctx.modifier.add_header_field("X-Name", "Value")

-- "Subject"フィールドの値を"New value"に変更するスケジュールを設定します
ctx.modifier.change_header_field("Subject", "New value")

-- パスワード付きアーカイブへのメッセージのリパックのスケジュールを設定します
ctx.modifier.repack()

-- メッセージ保留中のすべての変更を使用し、
-- milterプロトコルを介して判定を返します(テーブルMilterResult)
return { action = "accept" }
end
```

[MilterModifier](#)テーブルは使用せずに、[MilterModifier](#)テーブル(およびそのmodificationsフィールド、つまり[MilterModifications](#)テーブル)に直接入力する例。

```
-- "X-Checked: True"ヘッダーを追加し、
-- 受信者へのメッセージ送信を有効にします。
```

```
function milter_hook(ctx)
return {
  action = "accept",
  modifications = {
    added_fields = {
      {
        name = "X-Checked",
        value = "True"
      }
    }
  }
}
end
```

[MilterModifier](#)テーブルに加えられた変更を無視した、accept判定の返信例:

```
function milter_hook(ctx)

...

-- メッセージヘッダーを追加するスケジュールを設定します
ctx.modifier.add_header_field('X-Header', 'some value')

...

-- 空のMilterModificationsテーブルを強制的に返します
return {action = "accept", modifications = {}}
end
```



Spamdインターフェースのメッセージ処理のためのスクリプト

スクリプトの必要条件

ファイルには、メッセージスキャンモジュールのエントリポイントとなるグローバル関数が含まれている必要があります (Dr.Web MailDは、新しく受信したメッセージを処理する際にこの関数を呼び出します)。処理関数は、次の呼び出し規則を満たす必要があります。

1. 関数名はspamd_report_hookです。
2. 引数はSpamdContextテーブルのみです (関数から処理されたメールメッセージに関する情報へのアクセス権限を付与します)。
3. 返り値は入力済みのSpamdReportResultテーブルのみです。返り値はSpamdを介した応答を定義します。

Dr.Web MailDでメッセージをスパムとしてマークする必要があるという判定を無条件に返すスクリプトの適切な定義の例 (スパムポイント: 200、スパム認識しきい値: 100、メッセージ: メッセージはスパムとして認識されました。これ以降、ctx引数はSpamdContextテーブルのインスタンスになります) :

```
-- 簡単な実行例

function spamd_report_hook(ctx)
  return {
    score = 200,
    threshold = 100,
    report = "The message was recognized as spam"
  }
end
```

使用中のテーブル

テーブルSpamdContext

spamd_report_hook関数の入力引数として使用されます。処理されたメールメッセージに関する情報 (フィールド、構造、ヘッダー、本文、送信者と受信者に関する情報、SMTPセッションに関する情報) へのアクセス権限を提供します。テーブルには以下のフィールドを含みます。

フィールド	説明	データタイプ
session_id	このクライアントからのメッセージが処理されている間のクライアントセッションの識別子。	文字列
message	メールメッセージ。	テーブル MimeMessage
無効になったメタメソッド: なし		

テーブルSpamdReportResult

結果として使用されます。spamd_report_hook関数によって返されます。スパムのスキャン結果をDr.Web MailDに渡します。結果はMTAに返されます。以下のフィールドを含みます。



フィールド	説明	データタイプ
score	スキャン中にメールメッセージに割り当てられたスパムポイントの数 (MTAの場合、 Exim によって <code>\$spam_score</code> 変数と <code>\$spam_score_int</code> 変数が入力されます)	番号
threshold	メッセージがスパムと見なされるしきい値	番号
report	メッセージスキャンのテキスト結果 (MTAの場合、 Exim によって <code>\$spam_report</code> 変数が入力されます)	文字列
incident	Mailタイプの登録済みイベントのインシデントの説明。 <ul style="list-style-type: none">このフィールドが文字列の場合、この文字列の内容がMailイベントの<code>incident_text</code>フィールドに送信され、イベントが登録されます。このフィールドがブール値で<code>false</code>に等しい場合、Mailイベントの<code>incident_text</code>フィールドは存在せず、イベントは登録されません。このフィールドがブール値で<code>true</code>に等しい場合、Mailイベントの<code>incident_text</code>フィールドは自動的に入力され、<code>incident_text</code>の値が空でない場合はイベントが登録されます。	文字列またはブール値
無効になったメタメソッド: なし		

Rspamdインターフェースのメッセージ処理のためのスクリプト

スクリプトの必要条件

ファイルには、メッセージスキャンモジュールのエントリポイントとなるグローバル関数が含まれている必要があります (Dr.Web MailDは、新しく受信したメッセージを処理する際にこの関数を呼び出します)。処理関数は、次の呼び出し規則を満たす必要があります。

1. 関数名は`rspamd_hook`です。
2. 引数は`RspamdContext`テーブルのみです (関数から処理されたメールメッセージに関する情報へのアクセス権限を付与します。下のテーブルの説明を参照)。
3. 返り値は入力済みの`RspamdResult`テーブルのみです (下のテーブルの説明を参照)。返り値は`RspamD`を介した応答を定義します。

スクリプトの定義例 (`ctx`引数は`RspamdContext`テーブルのインスタンスになります) :

```
-- 簡単な実行例

function rspamd_hook(ctx)
  return {
    score = 200,
    threshold = 100
  }
end
```



例

MTAと、メールメッセージにスパムポイントを付与する理由を定義する[RspamdSymbol](#)テーブルに対して推奨されるアクションの応答例:

```
function rspamd_hook(ctx)
  return {
    score = 1080,
    threshold = 100,
    action = "REJECT:Malicious message"
    symbols = {
      {
        name = "Threat found",
        score = 1000
      },
      {
        name = "Spam score by VadeRetro",
        score = 80
      }
    }
  }
end
```

使用中のテーブル

テーブルRspamdContext

`rspamd_hook`関数の入力引数として使用されます。処理されたメールメッセージに関する情報へのアクセス権を提供します。テーブルには以下のフィールドを含みます。

フィールド	説明	データタイプ
<code>session_id</code>	このクライアントからのメッセージが処理されている間のクライアントセッションの識別子。	文字列
<code>sender</code>	メッセージ送信者に関する情報	テーブル RspamdSender
<code>helo</code>	SMTPクライアントから受信した文字列HELO/EHLO、または文字列が見つからない/不明の場合(MTAによって提供されない場合)は <code>nil</code>	文字列
<code>from</code>	送信者のメールアドレス(山括弧なし、例: <code>user@domain.com</code>)。アドレスが見つからない/不明な場合(MTAから提供されない場合)は <code>nil</code>	文字列
<code>to</code>	山括弧なしの受信者のメールアドレス	テーブル RcptTo
<code>message</code>	メールメッセージ	テーブル MimeMessage
無効になったメタメソッド: なし		

テーブルRspamdSender



メッセージ送信者に関する情報を記述します。以下のフィールドを含みます。

フィールド	説明	データタイプ
hostname	送信者のホストの名前 (FQDN)、または名前が見つからないか不明の場合 (MTAによって提供されない場合) は <code>nil</code>	文字列
ip	送信者のホストのIPアドレス。アドレスが見つからないか不明の場合 (MTAから提供されない場合) は <code>nil</code>	テーブル IpAddress
無効になったメタメソッド: なし		

テーブル *RspamdResult*

これは、`rspamd_hook`関数の結果として使用されます。次のフィールドとしてメッセージスキャンレポートが含まれます。

フィールド	説明	データタイプ
score	スキャン中にメールメッセージに割り当てられたスパムポイントの数 (MTAの場合、 Exim によって <code>\$spam_score</code> 変数と <code>\$spam_score_int</code> 変数が入力されます)	番号
threshold	メッセージがスパムと見なされるしきい値	番号
action	オプションのフィールドです。メッセージスキャンの結果としてMTAに推奨されるアクション (MTAの場合、 Exim により <code>\$spam_action</code> 変数が入力されます)	文字列
symbols	オプションのフィールドです。 <code>score</code> フィールドで指定されたスパムポイント数を割り当てる理由を特定するための RspamdSymbol テーブルの配列	RspamdSymbol テーブルの配列
incident	Mailタイプの 登録済みイベント のインシデントの説明。 <ul style="list-style-type: none">このフィールドが文字列の場合、この文字列の内容がMailイベントの<code>incident_text</code>フィールドに送信され、イベントが登録されます。このフィールドがブール値で<code>false</code>に等しい場合、Mailイベントの<code>incident_text</code>フィールドは存在せず、イベントは登録されません。このフィールドがブール値で<code>true</code>に等しい場合、Mailイベントの<code>incident_text</code>フィールドは自動的に入力され、<code>incident_text</code>の値が空でない場合はイベントが登録されます。	文字列またはブール値
無効になったメタメソッド: なし		

テーブル *RspamdSymbol*

記号の内容を表すテーブル。メッセージに割り当てられている特定数のスパムポイントに対してスキャン中に見つかったアイテム (脅威のあるファイル、不要なURLなど) を示します。テーブルには以下のフィールドを含みます。

フィールド	説明	データタイプ
name	検出されたアイテムの名前。	文字列



フィールド	説明	データタイプ
score	アイテム検出のためにメッセージに割り当てられるスパムポイントの数。	番号
description	オプションのフィールドです。検出されたアイテムの説明	文字列
無効になったメタメソッド: なし		

メッセージ構造を説明する表

テーブルRcptTo

SMTPプロトコルのRCPT TOコマンドで発生したメッセージ受信者(山括弧なし)のメールアドレスの配列を含むテーブル。さらに、次のフィールドが含まれています。

フィールド	説明	データタイプ
search	<p>アドレス配列内の指定されたテンプレートの少なくとも1つに対応する少なくとも1つのアドレスの存在を確認する関数。</p> <p>Perl構文(PCRE)の1つの必須patterns引数(検索パターン: 1つ(文字列)または複数(文字列の配列))の正規表現を受け入れます。</p> <p>ブール値を返します。</p> <ul style="list-style-type: none">• true - 少なくとも1つのテンプレートに完全に対応するアドレスが見つかった場合。• false - それ以外の場合。 <p>大文字と小文字を区別しません。</p>	機能
all_match	<p>すべてのアドレスがアドレス配列内の指定されたテンプレートの少なくとも1つに対応するかどうかをチェックする関数。</p> <p>Perl構文(PCRE)の1つの必須patterns引数(検索パターン: 1つ(文字列)または複数(文字列の配列))の正規表現を受け入れます。</p> <p>ブール値を返します。</p> <ul style="list-style-type: none">• true - すべてのアドレスが少なくとも1つのテンプレートに完全に対応する場合。• false - それ以外の場合。 <p>大文字と小文字を区別しません。</p>	機能
無効になったメタメソッド: なし		

テーブルMimeMessage

このテーブルは、スキャンされたメールメッセージの概要を示します(MimePartテーブルから継承され、そのすべてのフィールドを含みます)。テーブルには以下のフィールドを含みます。



フィールド	説明	データタイプ
dkim	メールメッセージのDKIM署名 (RFC 6376 を参照)	DKIM テーブル
raw	クライアントから受信したメッセージ	文字列
spam	スパムの兆候に対するメッセージスキャンの結果についてのレポート	テーブル Spam
from	メッセージにFromがない場合、メッセージヘッダーの値はFromまたはnil	テーブル From
to	メッセージにToがない場合、メッセージヘッダーの値はToまたはnil	テーブル To
date	メッセージにDateがない場合、メッセージヘッダーの値は、Dateまたはnil	文字列
message_id	メッセージにMessage-IDがない場合、メッセージヘッダー値はMessage-IDまたはnil	文字列
subject	メッセージにSubjectがない場合、メッセージヘッダーの値はSubjectまたはnil	文字列
user_agent	メッセージにUser-Agentがない場合、メッセージヘッダーの値はUser-Agentまたはnil	文字列
(MimePart テーブルから継承したフィールド)		
無効になったメタメソッド: なし		

テーブルMimePart

このテーブルは、メールメッセージの部分を説明したもので、次のフィールドが含まれます。

フィールド	説明	データタイプ
header	メールメッセージのヘッダー	テーブル MimeHeader
body	該当部分の本体。添付された部品がある場合はnil。	テーブル MimeBody
part	テーブルの配列として(現在のメッセージ部分に)添付された部分。添付された部品がない場合、配列は空になります。	MimePart テーブルの配列
content_disposition	このヘッダーが該当部分にない場合、Content-Dispositionヘッダーのコンテンツ、またはnil。	ContentDisposition テーブル
content_id	このヘッダーが該当部分にない場合、Content-IDヘッダーのコンテンツまたはnil。	文字列
content_type	このヘッダーが該当部分にない場合、Content-Typeヘッダーのコンテンツまたはnil。	ContentType テーブル



フィールド	説明	データタイプ
name	添付ファイル名。該当部分が添付ファイルでない場合はnil	文字列
part_at	<p>path引数(メッセージの子部分へのパス)を受け取る関数。指定されたパスにある添付されたメッセージ部分(テーブルMimePart)を返します。</p> <p>pathは"/ 1/2/3"のような文字列となります。これは、root_part.part [1]. part [2]. part [3]を意味します。数字のない""、"/"、"//"のようなパスはメッセージ部分に対応し、この関数の呼び出し元になります(例: root_part)。指定したパスに子部分がない場合や、パスが正しくない場合は、関数はnilを返します。</p>	機能
threats	<p>オプションの引数filterを1つ受け取る関数。この関数は単一の値、つまり反復子関数を返します。この反復子を使用すると、メッセージのこの部分と添付部分にある、指定されたfilter条件を満たすすべての脅威を調べることができます。反復子関数は引数を持たず、次の2つの値を返します。</p> <ul style="list-style-type: none">• Virusテーブル。• 検出された脅威を含むメッセージ部分への相対パス。 <p>filter引数として、次のものを使用できます。</p> <ul style="list-style-type: none">• ThreatFilterテーブル。• Virus引数のみを受け取り、次のブール値を返す任意の叙述関数:<ul style="list-style-type: none">◦ true - 引数が条件を満たしている(脅威である)場合。◦ false - それ以外の場合。	機能
urls	<p>オプションの引数filterを1つ受け取る関数。この関数は単一の値、つまり反復子関数を返します。この反復子を使用すると、メッセージのこの部分と添付部分にある、指定されたfilter条件を満たすすべてのURLを調べることができます。反復子関数は引数を持たず、次の2つの値を返します。</p> <ul style="list-style-type: none">• Urlテーブル。• 見つかったURLを含むメッセージ部分への相対パス。 <p>filter引数として、次のものを使用できます。</p> <ul style="list-style-type: none">• UrlFilterテーブル。• Url引数のみを受け取り、次のブール値を返す任意の叙述関数:<ul style="list-style-type: none">◦ true - 引数が条件を満たしている(不要である)場合。	機能



フィールド	説明	データタイプ
	<ul style="list-style-type: none">◦ false - それ以外の場合。	
attachments	<p>オプションの引数 <code>filter</code> を1つ受け取る関数。この関数は単一の値、つまり反復子関数を返します。この反復子を使用すると、メッセージのこの部分と添付部分にある、指定された <code>filter</code> 条件を満たすすべての添付ファイルを調べることができます。反復子関数は引数を持たず、次の2つの値を返します。</p> <ul style="list-style-type: none">• MimePart テーブル。• 見つかった添付ファイルを含むメッセージ部分への相対パス。 <p><code>filter</code> 引数として、次のものを使用できます。</p> <ul style="list-style-type: none">• PartFilter テーブル。• MimePart 引数のみを受け取り、次のブール値を返す任意の叙述関数<ul style="list-style-type: none">◦ true - 引数が条件を満たしている場合。◦ false - それ以外の場合。	機能
files	<p>オプションの引数 <code>filter</code> を1つ受け取る関数。この関数は単一の値、つまり反復子関数を返します。この反復子を使用すると、メッセージのこの部分と添付部分（アーカイブを含む）にある、指定された <code>filter</code> 条件を満たすすべてのファイルを調べることができます。反復子関数は引数を持たず、次の2つの値を返します。</p> <ul style="list-style-type: none">• 文字列で示したファイル名。• 見つかったファイルを含むメッセージ部分への相対パス。 <p><code>filter</code> 引数として、次のものを使用できます。</p> <ul style="list-style-type: none">• FileFilter テーブル。• ファイル名を文字列として受け取り、次のブール値を返す任意の叙述関数：<ul style="list-style-type: none">◦ true - 引数が条件を満たしている場合。◦ false - それ以外の場合。	機能
parts	<p>オプションの引数 <code>filter</code> を1つ受け取る関数。この関数は単一の値、つまり反復子関数を返します。この反復子を使用すると、メッセージのこの部分と添付部分にある、指定された <code>filter</code> 条件を満たすすべてのメッセージ部分を調べることができます。反復子関数は引数を持たず、次の2つの値を返します。</p> <ul style="list-style-type: none">• MimePart テーブル。• メッセージ部分への相対パス。 <p><code>filter</code> 引数として、次のものを使用できます。</p> <ul style="list-style-type: none">• PartFilter テーブル。	機能



フィールド	説明	データタイプ
	<ul style="list-style-type: none">• MimePartテーブルを受け取り、次のブール値を返す任意の叙述関数：<ul style="list-style-type: none">◦ true - 引数が条件を満たしている場合。◦ false - それ以外の場合。	
leaf_parts	<p>オプションの引数 <code>filter</code> を1つ受け取る関数。この関数は単一の値、つまり反復子関数を返します。この反復子を使用すると、メッセージのこの部分と添付部分にある、指定された <code>filter</code> 条件を満たすすべてのリーフ部分を調べることができます。反復子関数は引数を持たず、次の2つの値を返します。</p> <ul style="list-style-type: none">• MimePartテーブル。• メッセージ部分への相対パス。 <p><code>filter</code> 引数として、次のものを使用できます。</p> <ul style="list-style-type: none">• PartFilterテーブル。• MimePartテーブルを受け取り、次のブール値を返す任意の叙述関数：<ul style="list-style-type: none">◦ true - 引数が条件を満たしている場合。◦ false - それ以外の場合。	機能
text_parts	<p>オプションの引数 <code>filter</code> を1つ受け取る関数。この関数は単一の値、つまり反復子関数を返します。この反復子を使用すると、メッセージのこの部分と添付部分にある、指定された <code>filter</code> 条件を満たすすべてのテキスト部分を調べることができます。反復子関数は引数を持たず、次の2つの値を返します。</p> <ul style="list-style-type: none">• MimePartテーブル。• メッセージ部分への相対パス。 <p><code>filter</code> 引数として、次のものを使用できます。</p> <ul style="list-style-type: none">• PartFilterテーブル。• MimePartテーブルを受け取り、次のブール値を返す任意の叙述関数：<ul style="list-style-type: none">◦ true - 引数が条件を満たしている場合。◦ false - それ以外の場合。	機能
scan_reports	<p>オプションの <code>filter</code> を1つ受け取る関数。この関数は単一の値、つまり反復子関数を返します。この反復子を使用すると、指定された <code>filter</code> 条件を満たす、メールの該当部分およびその添付ファイルの部分をスキャンするレポートを処理できます。</p> <p>反復子関数には引数がなく、単一の値、つまり ScanReport テーブルを返します。</p> <p><code>filter</code> 引数として、次のものを使用できます。</p> <ul style="list-style-type: none">• ScanReportFilter テーブル。	機能



フィールド	説明	データタイプ
	<ul style="list-style-type: none">• ScanReportテーブルを受け取り、次のブール値を返す任意の叙述関数：<ul style="list-style-type: none">◦ <code>true</code> - 引数が条件を満たしている場合。◦ <code>false</code> - それ以外の場合。	
<code>has_url</code>	<p>オプション引数 <code>filter</code> を1つの受け取る関数（既述の <code>urls</code> 関数の説明を参照）。</p> <p>ブール値を返します。</p> <ul style="list-style-type: none">• <code>true</code> - メッセージの該当部分とその添付された部分に条件 <code>filter</code> を満たすURLが含まれる場合。• <code>false</code> - それ以外の場合。 <p>例：</p>	機能



フィールド	説明	データタイプ
	<pre>if ctx.message.has_url() then -- メールメッセージに少なくとも1つのURLが見つかりました end if ctx.message.has_url{category = "adult_content"} then -- adult_content のリンクが見つかりました end if ctx.message.has_url{category = {"adult_content", "social_networks"}} then -- 「adult_content」または「social_networks」リンクが見つかった場合 end if ctx.message.has_url{category = "black_list"} then -- ブラックリストリソースへのリンクが見つかった場合 end if ctx.message.has_url{host = "example.com"} then -- ホスト部分が「example.com」であるリンクが見つかりました end if ctx.message.has_url{host_not = "*example.com"} then -- ホスト部分が「*example.com」に該当しないリンクが見つかりました end if ctx.message.has_url(function(url) return port > 80 end) then -- ポート番号が80より大きいリンクが見つかりました end</pre>	
has_threat	<p>オプション引数 <code>filter</code> を1つの受け取る関数（既述の threats 関数の説明を参照）。</p> <p>ブール値を返します。</p> <ul style="list-style-type: none">• <code>true</code> - メッセージの該当部分と添付ファイル部分に条件 <code>filter</code> を満たす脅威が含まれる場合。• <code>false</code> - それ以外の場合。 <p>例：</p>	機能



フィールド	説明	データタイプ
	<pre>if ctx.message.has_threat() then -- メッセージに、いずれかのカテゴリーの脅威が1つ以上含まれています end if ctx.message.has_threat({category = "known_virus"}) then -- メッセージに、「known_virus」カテゴリーの脅威が1つ以上含まれている end if ctx.message.has_threat{category = "known_virus"} then -- 同上 end if ctx.message.has_threat({category = {"known_virus", "joke"}}) then -- メッセージに、「known_virus」カテゴリーまたは「joke」カテゴリーの脅威が1つ以上含まれている end if ctx.message.has_threat{category_not = "joke"} then -- メッセージに、「joke」以外のカテゴリーの脅威が含まれている end</pre>	
has_file	<p>オプション引数 <code>filter</code> を1つの受け取る関数（既述の <code>files</code> 関数の説明を参照）。</p> <p>ブール値を返します。</p> <ul style="list-style-type: none">• <code>true</code> - メッセージの該当部分とその添付ファイル部分に条件 <code>filter</code> を満たすファイルが含まれる場合（アーカイブのファイルを含む）。• <code>false</code> - それ以外の場合。 <p>例：</p> <pre>if ctx.message.has_file() then -- メールメッセージに少なくとも1つのファイルが見つかりました end if ctx.message.has_file{name = "*.exe"} then -- メールメッセージに少なくとも1つのexeファイルが見つかりました end</pre>	機能



フィールド	説明	データタイプ
has_part	オプション引数 <i>filter</i> を1つの受け取る関数（既述の parts 関数の説明を参照）。 ブール値を返します。 <ul style="list-style-type: none">• <code>true</code> - メッセージの該当部分とその添付ファイル部分に条件 <i>filter</i> を満たす部分が含まれる場合。• <code>false</code> - それ以外の場合。	機能
has_scan_report	オプション引数 <i>filter</i> を1つ受け取る関数（上記の scan_reports 関数の説明を参照）。 ブール値を返します。 <ul style="list-style-type: none">• <code>true</code> - メッセージの該当部分とその添付ファイル部分に条件 <i>filter</i> を満たすスキャンレポートが含まれる場合。• <code>false</code> - それ以外の場合。 使用例については、 ScanReportFilter テーブルの編集を参照してください。	機能
search	正規表現 (PCRE) を使用してこのメッセージセクション内のテキストを検索する関数。正規表現 (文字列) を受け取ります。引用符内で文字列を使用する場合は、スラッシュ文字をエスケープする必要があります。 ブール値を返します。 <ul style="list-style-type: none">• <code>true</code> - 指定した正規表現との一致がこのセクションまたは子部分で見つかった場合。• <code>false</code> - それ以外の場合。	機能
無効になったメタメソッド: なし		

テーブルFrom

Fromメールメッセージヘッダーを説明するテーブル。ヘッダー（文字列の配列）から抽出されたメールアドレスのリストが含まれます。さらに、次のフィールドが含まれます。

フィールド	説明	データタイプ
search	アドレス配列内の指定されたテンプレートの少なくとも1つに対応する少なくとも1つのアドレスの存在を確認する関数。 Perl構文 (PCRE) の1つの必須 <i>patterns</i> 引数（検索パターン: 1つ（文字列）または複数（文字列の配列））の正規表現を受け入れます。 ブール値を返します。 <ul style="list-style-type: none">• <code>true</code> - 少なくとも1つのテンプレートに完全に対応するアドレスが見つかった場合。	機能



フィールド	説明	データタイプ
	<ul style="list-style-type: none">• false - それ以外の場合。 大文字と小文字を区別しません。	
all_match	すべてのアドレスがアドレス配列内の指定されたテンプレートの少なくとも1つに対応するかどうかをチェックする関数。 Perl構文 (PCRE) の1つの必須 patterns 引数 (検索パターン: 1つ (文字列) または複数 (文字列の配列)) の正規表現を受け入れます。 ブール値を返します。 <ul style="list-style-type: none">• true - すべてのアドレスが少なくとも1つのテンプレートに完全に対応する場合。• false - それ以外の場合。 大文字と小文字を区別しません。	機能
無効になったメタメソッド: <ul style="list-style-type: none">• __tostringは、デコードされたヘッダー値を返す関数です。• __concatは、ヘッダーの復号化された値と文字列を結合する関数です。		

テーブルTo

Toメールメッセージヘッダーを説明するテーブル。Fromテーブルと同じフィールドとメソッドが含まれています。

ContentTypeテーブル

メッセージ部分のContent-Typeヘッダーを説明するテーブル。以下のフィールドを含みます。

フィールド	説明	データタイプ
type	メッセージ部分のMIMEタイプ	文字列
subtype	メッセージ部分のサブタイプ	文字列
param	次のフィールドを持つテーブル配列形式のヘッダーパラメータ: <ul style="list-style-type: none">• nameはパラメータ名 (文字列) です。• valueはパラメータ値 (文字列) です。	テーブル配列
無効になったメタメソッド: <ul style="list-style-type: none">• __tostringは、デコードされたヘッダー値を返す関数です。• __concatは、ヘッダーの復号化された値と文字列を結合する関数です。		

ContentDispositionテーブル

メッセージ部分のContent-Dispositionヘッダーを説明するテーブル。以下のフィールドを含みます。



フィールド	説明	データタイプ
type	メッセージ部分のビュータイプ	文字列
param	次のフィールドを持つテーブル配列形式のヘッダーパラメータ: <ul style="list-style-type: none">• nameはパラメータ名(文字列)です。• valueはパラメータ値(文字列)です。	テーブル配列
無効になったメタメソッド: <ul style="list-style-type: none">• __tostringは、デコードされたヘッダー値を返す関数です。• __concatは、ヘッダーの復号化された値と文字列を結合する関数です。		

テーブルSpam

スパムに対するメッセージスキャンについてのレポートを説明するテーブル。以下のフィールドを含みます。

フィールド	説明	データタイプ
type	メッセージのタイプ(スパムのステータス) 可能な値: <ul style="list-style-type: none">• "legit" - メッセージはスパムではありません。• "spam" - メッセージはスパムです。• "virus" - ヒューリスティックアナライザVadeRetroにより、メッセージ本文にウイルスが検出されました。• "bounce" - メッセージには、元のメッセージの送信者に送信されたネガティブ配信確認(DSN)に関するレポートが含まれています。• "suspicious" - 疑わしいメッセージ。• "pce" - 有効なサブスクリプションサービスによって送信される「プロフェッショナルな」商用(広告)メッセージ。• "mce" - 有効なサブスクリプションサービスでは送信されないが、サブスクリプションを解除する方法が含まれる商用(広告)メッセージ。• "dce" - サブスクリプションを解除する方法のない「ダークティーン」コマーシャル(広告)メッセージ。• "community" - ソーシャルネットワークからのメッセージ。• "transactional" - トランザクション関連のメッセージ(登録、サービスまたは商品の購入)。• "phishing" - 不正なメッセージ。• "scam" - 不正なメッセージ(詐欺メッセージ)。	文字列
score	メッセージごとに記録されたスパムポイント数。	番号
normalized_score	インターバル[0, 1]で正規化されたスパムスコア	番号
reason	メールメッセージがスパムであるとされた理由の説明を含む暗号化された文字列	文字列



フィールド	説明	データタイプ
version	VadeRetro ライブラリバージョン	文字列
無効になったメタメソッド: なし		

テーブルVirus

脅威を説明するテーブル。以下のフィールドを含みます。

フィールド	説明	データタイプ
type	脅威の種類 (Doctor Webの分類による)。可能な値: <ul style="list-style-type: none">"known_virus" - 既知の脅威 (ウイルスデータベースに説明がある脅威)。"virus_modification" - 既知の脅威の亜種。"unknown_virus" - 未知の脅威、疑わしいオブジェクト。"adware" - 広告プログラム。"dialer" - ダイアラープログラム。"joke" - ジョークプログラム。"riskware" - 潜在的に危険なプログラム。"hacktool" - ハッキングツール。	文字列
name	脅威の種類 (Doctor Webの分類による)	文字列
無効になったメタメソッド: なし		

テーブルUrl

URLを説明するテーブル。以下のフィールドを含みます。

フィールド	説明	データタイプ
scheme	スキーム (プロトコル) プレフィックス。例: "http"	文字列
host	ホスト名またはIPアドレス。例: "example.com"	文字列
port	ポート番号。例: 80。URLに含まれていない場合、値はnilになります。	番号
path	リソースへのパス。例: "index.html"。URLに含まれていない場合、値はnilになります。	文字列
categories	スキャンの結果としてURLに割り当てられたカテゴリー。可能な値: <ul style="list-style-type: none">"infection_source" - 感染源。"not_recommended" - 非推奨のWebサイト。"adult_content" - アダルトコンテンツ。"violence" - 暴力。	文字列のテーブル



フィールド	説明	データタイプ
	<ul style="list-style-type: none"> "weapons" - 武器。 "gambling" - ギャンブル。 "drugs" - 薬物。 "obscene_language" - 卑猥な表現。 "chats" - チャット。 "terrorism" - テロリズム。 "free_email" - 無料メール。 "social_networks" - ソーシャルネットワーク。 "owners_notice" - 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サイト。 "online_games" - オンラインゲーム。 "anonymizers" - アノマイザー。 "cryptocurrency_mining_pools" - 仮想通貨マイニングプール。 "jobs" - 求人検索サイト。 "black_list" - ブラックリスト(メールサーバー管理者によって非推奨と見なされるリソース)。 	
legal_url	URLがowners_noticeカテゴリーに属する場合、フィールドには所有者のWebサイトへのURLが含まれます。属さない場合は、nilになります。	文字列
<p>無効になったメタメソッド:</p> <ul style="list-style-type: none"> __toString - この関数は、URLコンテンツを文字列 (UTF-8) として返します。 __concat - この関数は、URL文字列値と別の文字列を連結します。 		

テーブルThreatFilter

脅威に対するフィルターを説明するテーブル。次のフィールドが含まれます(すべてのフィールドはオプションです)。

フィールド	説明	データタイプ
category	脅威が該当するカテゴリーのリスト(大文字と小文字は区別されません)。Virusテーブルのtypeフィールドの説明にあるカテゴリーのリストを参照してください。	文字列または文字列のテーブル
category_not	脅威が該当しないカテゴリーのリスト(大文字と小文字は区別されません)。	文字列または文字列のテーブル
無効になったメタメソッド: なし		

フィルターフィールドが指定されていない(値がnil)場合、脅威はフィルターと一致します。複数のフィルターフィールドが指定されている場合、条件は接続詞(論理積)によって結合されます。フィルターフィールドがテーブル(リスト)の場合、オブジェクトは少なくとも1つのテーブル(リスト)の項目と一致する必要があります。

使用例:



1.メッセージ内に見つかったすべての脅威名をログに出力するには、次の手順を実行します。

```
function milter_hook(ctx)

...

for virus in ctx.message.threats() do
  dw.notice("threat found: " .. virus.name)
end

...

end
```

2.カテゴリーフィルターに一致する脅威名と、脅威が検出されたメッセージ部分の名前をログに出力するには、次の手順を実行します。

```
function milter_hook(ctx)

...

for v, p in ctx.message.threats({category = "known_virus"}) do
  dw.notice("found " .. v.name .. " in " .. ctx.message.part_at(p).name(p))
end

...

end
```

3.叙述関数に一致する脅威名と、脅威が検出されたメッセージ部分の名前をログに出力するには、次の手順を実行します。

```
function milter_hook(ctx)

...

local function eicar_filter(v)
  return v.name == "EICAR Test File (NOT a Virus!)"
end

for v, p in ctx.message.threats(eicar_filter) do
  dw.notice("found " .. v.name .. " in " .. ctx.message.part_at(p).name(p))
end

...

end
```

テーブルUrFilter

URLのフィルターを説明するテーブル(既述のテーブル[ThreatFilter](#)と同様のもの)。次のフィールドが含まれます(すべてのフィールドはオプションです)。



フィールド	説明	データタイプ
category	URLが該当するカテゴリーのリスト（大文字と小文字は区別されません）。 Url テーブルのcategoriesフィールドの説明にあるカテゴリーのリストを参照してください。	文字列または文字列のテーブル
category_not	URLが該当しないカテゴリーのリスト（大文字と小文字は区別されません）。	文字列または文字列のテーブル
text	URLと一致しなければならないテキスト	文字列または文字列のテーブル
text_not	URLと一致できないテキスト	文字列または文字列のテーブル
host	URLに存在するホスト（ドメイン）	文字列または文字列のテーブル
host_not	URLにないホスト（ドメイン）	文字列または文字列のテーブル
無効になったメタメソッド: なし		

フィルターフィールドが指定されていない（値が`nil`）場合、脅威はフィルターと一致します。複数のフィルターフィールドが指定されている場合、条件は接続詞（論理積）によって結合されます。フィルターフィールドがテーブル（リスト）の場合、オブジェクトは少なくとも1つのテーブル（リスト）の項目と一致する必要があります。

使用例:

1. メッセージ内に見つかったすべてのURLをログに出力するには、次の手順を実行します。

```
function milter_hook(ctx)

...

for url in ctx.message.urls() do
  dw.notice("url found: " .. url)
end

...

end
```

2. カテゴリーに一致するURLと、URLが検出されたメッセージ部分の名前をログに出力するには、次の手順を実行します。



```
function milter_hook(ctx)

...

for u, p in ctx.message.urls{category = "adult_content"} do
  dw.notice("found " .. u.text .. " in " .. ctx.message.part_at(p).name(p))
end

...

end
```

テーブルFileFilter

ファイルのフィルターを説明するテーブル(既述のテーブルThreatFilterと同様のもの)。次のフィールドが含まれます(すべてのフィールドはオプションです)。

フィールド	説明	データタイプ
name	ファイルに必要な名前。例: "*.exe"、"eicar.txt"。 大文字と小文字を区別しません。	文字列または文字列のテーブル
name_re	ファイル名が一致しなければならない正規表現(PCRE)。 例: ".*\\.zip"、[".*\\.zip"]。 大文字と小文字を区別しません。引用符内で文字列を使用する場合は、スラッシュ文字をエスケープする必要があります。	文字列または文字列のテーブル
name_not	ファイルを持つことができない名前。 大文字と小文字を区別しません。	文字列または文字列のテーブル
name_re_not	ファイル名が一致できない正規表現(PCRE)。 大文字と小文字を区別しません。引用符内で文字列を使用する場合は、スラッシュ文字をエスケープする必要があります。	文字列または文字列のテーブル
無効になったメタメソッド: なし		

複数のフィルターフィールドが指定されている場合、条件は接続詞(論理積)によって結合されます。フィルターフィールドがテーブル(配列)の場合、オブジェクトは少なくとも1つのテーブル(配列)の項目と一致する必要があります。フィルターフィールドが指定されていない(値がnil)場合、ファイルはフィルターと一致します。

使用例:

拡張子として"exe"を持つファイルを含む部分の名前をログに出力する場合



```
function milter_hook(ctx)

...

for f, p in ctx.message.files{name = "*.exe"} do
  local where = ctx.message.part_at(p).name
  if not where or where == "" then where = p end
  dw.notice("EXE found in " .. where)
end

...

end
```

テーブルPartFilter

メッセージ部分のフィルターを説明するテーブル(既述のテーブル[FileFilter](#)と同様のもの)。次のフィールドが含まれます(すべてのフィールドはオプションです)。

フィールド	説明	データタイプ
name	その部分に必要な名前。 例: "*.exe"、"eicar.txt"。 大文字と小文字を区別しません。	文字列または文字列のテーブル
name_re	部分名が一致しなければならない正規表現(PCRE)。例: ".*\\.zip"、[".*\\.zip"]。 大文字と小文字を区別しません。引用符内で文字列を使用する場合は、スラッシュ文字をエスケープする必要があります。	文字列または文字列のテーブル
content_type	部品(添付ファイル)に必要なContent-Type値。例: "image/*"。 大文字と小文字を区別しません。	文字列または文字列のテーブル
content_disposition	該当部分(添付ファイル)が持っていなければならないContent-Disposition値。 例: "inline"、"attachment"。 大文字と小文字を区別しません。	文字列または文字列のテーブル
name_not	部分が持つことができない名前。 大文字と小文字を区別しません。	文字列または文字列のテーブル
name_re_not	メッセージ部分の名前が一致できない正規表現(PCRE)。 大文字と小文字を区別しません。引用符内で文字列を使用する場合は、スラッシュ文字をエスケープする必要があります。	文字列または文字列のテーブル



フィールド	説明	データタイプ
content_type_not	Content-Type部分で一致することができない値。 大文字と小文字を区別しません。	文字列または文字列のテーブル
content_disposition_not	Content-Disposition部分で一致することができない値。 大文字と小文字を区別しません。	文字列または文字列のテーブル
無効になったメタメソッド: なし		

フィルターフィールドが指定されていない(値が`nil`)場合、任意の部分(添付ファイル)がフィルターと一致します。複数のフィルターフィールドが指定されている場合、条件は接続詞(論理積)によって結合されます。フィルターフィールドがテーブル(配列)の場合、オブジェクトは少なくとも1つのテーブル(配列)の項目と一致する必要があります。

使用例:

1. すべての添付ファイルとそのMD5ハッシュをログに出力するには、次の手順を実行します。

```
function milter_hook(ctx)

...

for a, p in ctx.message.attachments() do
  -- Content-TypeとContent-Dispositionに指定されていない場合、
  -- 添付ファイル名は空文字列になります
  local name = a.name
  if name == "" then name = "at path " .. p end
  dw.notice("Attachment: " .. name .. "; md5=" .. a.body.md5)
end

...

end
```

2. `.exe`拡張子を持つすべての添付ファイルをログに出力するには、次の手順を実行します。

```
function milter_hook(ctx)

...

for a in ctx.message.attachments{name = "*.exe"} do
  dw.notice("EXE attachment: " .. a.name)
end

...

end
```

3. メールメッセージ内の画像を種類別にカウントするには、次の手順を実行します。



```
function milter_hook(ctx)

...

local images = {}
for part, path in ctx.message.parts{content_type = "image/*"} do
    local subtype = part.content_type.subtype
    images[subtype] = (images[subtype] or 0) + 1
end

for t, c in pairs(images) do
    dw.notice("Found " .. t .. " images: " .. c)
end

...

end
```

4. 添付ファイルにあるすべてのオーディオファイルをログに出力するには、次の手順を実行します。

```
function milter_hook(ctx)

...

for p, path in ctx.message.parts{
    content_type = "audio/*",
    content_disposition = {"inline", "attachment"}
} do
    local name = p.name
    if name == "" then name = "<unnamed>" end
    dw.notice("Audio file: " .. name)
end

...

end
```

テーブルScanReportFilter

脅威のメッセージ部分をスキャンするレポートのフィルターを説明するテーブル(上記の[FileFilter](#)と同様)。次のフィールドが含まれます(すべてのフィールドはオプションです)。

フィールド	説明	データタイプ
error	ScanReport に含める必要のあるエラー。たとえば、"password_protected"、"scan_timeout"。 大文字と小文字を区別しません。	文字列または文字列のテーブル
error_not	ScanReport に含めることができないエラー。たとえば、"password_protected"、"scan_timeout"。 大文字と小文字を区別しません。	文字列または文字列のテーブル
無効になったメタメソッド: なし		



複数のフィルターフィールドが指定されている場合、条件は接続詞（論理積）によって結合されます。フィルターフィールドがテーブル（配列）の場合、スキャンレポートは少なくとも1つのテーブル（配列）の項目と一致する必要があります。フィルターフィールドが指定されていない場合（値は`nil`）、スキャンレポートはすべてフィルターに一致します。

使用例：

1. パスワードで保護されたアーカイブのスキャンに失敗した場合は、メッセージを隔離します。

```
function milter_hook(ctx)

...

if ctx.message.has_scan_report{error = 'password_protected'} then
  return
  {
    action = 'accept', deleted_recipients = ctx.to,
    added_recipients = {'quarantine@mail.domain.com'}
  }
end

...

end
```

2. スキャン制限を超えている場合は、次のようにメッセージを隔離します。

```
function milter_hook(ctx)

...

local limit_errors = {
  'archive_level_limit', 'compression_limit',
  'container_level_limit', 'mail_level_limit',
  'packer_level_limit', 'report_size_limit'
}

if ctx.message.has_scan_report{error = limit_errors} then
  return
  {
    action = 'accept', deleted_recipients = ctx.to,
    added_recipients = {'quarantine@mail.domain.com'}
  }
end

...

end
```

3. スキャンエラーがある場合は、次のようにメッセージを拒否します。

```
function milter_hook(ctx)

...

end
```



```
if ctx.message.has_scan_report{error = '*'} then
  return {action = 'reject'}
end

...

end
```

テーブルMimeHeader

このテーブルは、メッセージ部分のヘッダーについて説明します。以下のフィールドを含みます。

フィールド	説明	データタイプ
field	ヘッダーとその値のリスト	HeaderField テーブルの配列
search	正規表現 (PCRE) を使用してヘッダーを検索する関数。正規表現 (文字列) を受け取ります。メッセージ部分のすべてのヘッダーが検索対象になります。引用符内で文字列を使用する場合は、スラッシュ文字をエスケープする必要があります。 ブール値を返します。 <ul style="list-style-type: none">• true - field.name .. ": " .. field.value.decoded文字列が、少なくとも1つのヘッダーに対して指定した正規表現と一致する場合。• false - それ以外の場合。	機能
value	指定したヘッダーの値を返す関数。ヘッダー名 (文字列) を受け取ります。 指定した名前を持つ最初に見つかったヘッダーに対応する HeaderFieldValue テーブルを返します。ヘッダーが見つからなかった場合は、nil を返します。	機能
無効になったメタメソッド: なし		

テーブルHeaderField

このテーブルは、メッセージ部分のヘッダーについて説明します。以下のフィールドを含みます。

フィールド	説明	データタイプ
name	ヘッダー名	文字列
value	ヘッダー値	テーブル HeaderFieldValue
url	ヘッダー値に含まれるURLのリスト (Subjectヘッダーのみ)。それ以外のヘッダーの場合は、nil	Url テーブルの配列
無効になったメタメソッド: なし		



テーブルHeaderFieldValue

このテーブルは、メールメッセージヘッダーの値を説明したもので、次のフィールドが含まれます。

フィールド	説明	データタイプ
raw	未加工の(デコードされていない)ヘッダー値	文字列
decoded	デコードされたヘッダー値	文字列
無効になったメタメソッド:		
<ul style="list-style-type: none">• <code>__toString</code> - この関数は、HeaderFieldValueの内容(<code>decoded</code>フィールドの値)を文字列として返します。• <code>__concat</code> - この関数は、HeaderFieldValue(<code>decoded</code>フィールドの値)と別の文字列を連結します。		

テーブルMimeBody

このテーブルは、メッセージ部分の本体について説明します。以下のフィールドを含みます。

フィールド	説明	データタイプ
raw	メッセージ部分の未加工の(デコードされていない)本文	文字列
decoded	メッセージ部分本体のデコードされた値(Content-Transfer-Encoding ヘッダーと Content-Type ヘッダーの値に応じたもの)	文字列
text	Content-Type ヘッダーの <code>charset</code> パラメータに従って、UTF-8でデコードされたメッセージ部分本体の値。 " Content-Type : text/*"を持つ部分または Content-Type が空の部分にのみ存在します。それ以外の場合は、 <code>nil</code> になります。	文字列
scan_report	脅威のスキャンについてのレポート	テーブル ScanReport
url	部分テキストに見つかったURL。 Url テーブルの配列。 <code>text</code> フィールドがない場合(<code>nil</code>)、フィールドは空になります。	Url テーブルの配列
search	正規表現(PCRE)を使用してこの本文内のテキストを検索する関数。正規表現(文字列)を受け取ります。引用符内で文字列を使用する場合は、スラッシュ文字をエスケープする必要があります。 ブール値を返します。 <ul style="list-style-type: none">• <code>true</code> - 本文がテキストであり、一致が見つかった場合。• <code>false</code> - それ以外の場合。	機能
md5	メールメッセージ本文のMD5ハッシュ。	文字列
sha1	メールメッセージ本文のSHA1ハッシュ。	文字列



フィールド	説明	データタイプ
sha256	メールメッセージ本文のSHA256ハッシュ。	文字列
無効になったメタメソッド: なし		

テーブルScanReport

脅威のスキャンについてのレポートを説明するテーブル。以下のフィールドを含みます。

フィールド	説明	データタイプ
object	スキャンされたオブジェクトの名前	文字列
archive	スキャンされたオブジェクトがコンテナの場合は、コンテナに関する情報。オブジェクトがコンテナではない場合、nil	Archive テーブル
virus	検出された脅威のリスト	Virus テーブルの配列
error	<p>エラーが発生した場合は、スキャンエラーの文字列が含まれます。発生していない場合は、nilになります。使用可能な値:</p> <ul style="list-style-type: none">• "path_not_absolute" - 指定されたパスは絶対パスではありません。• "file_not_found" - ファイルが見つかりませんでした。• "file_not_regular" - ファイルは通常のファイルではありません。• "file_not_block_device" - ブロックデバイスではありません。• "name_too_long" - 名前が長すぎます。• "no_access" - アクセスが拒否されました。• "read_error" - 読み取りエラーが発生しました。• "write_error" - 書き込みエラー。• "file_too_large" - ファイルが大きすぎます。• "file_busy" - ファイルは使用中です。• "unpacking_error" - アンパックエラー。• "password_protected" - アーカイブはパスワードで保護されています。• "arch_crc_error" - CRCアーカイブエラー。• "arch_invalid_header" - 無効なアーカイブヘッダー。• "arch_no_memory" - アーカイブを解凍するための十分なメモリがありません。• "arch_incomplete" - 不完全なアーカイブ。• "can_not_be_cured" - ファイルを修復できません。• "packer_level_limit" - パックされたオブジェクトのネストレベルの上限を超えました。• "archive_level_limit" - アーカイブのネストレベルの上限を超えました。	文字列



フィールド	説明	データタイプ
	<ul style="list-style-type: none">"mail_level_limit" - メールファイルのネストレベルの上限を超えました。"container_level_limit" - コンテナのネストレベルの上限を超えました。"compression_limit" - 圧縮率の上限を超えました。"report_size_limit" - レポートサイズの上限を超えました。"scan_timeout" - スキャンタイムアウトの上限を超えました。"engine_crash" - スキャンエンジンの障害。"engine_hangup" - スキャンエンジンのハングアップ。"engine_error" - スキャンエンジンエラー。"no_license" - アクティブなライセンスが見つかりません。"multiscan_too_late" - マルチスキャンエラー。"curing_limit_reached" - 修復試行の上限を超えました。"non_supported_disk" - ディスクタイプはサポートされていません。"unexpected_error" - 予期しないエラー。	
item	スキャンされたオブジェクトがコンテナ（アーカイブ、添付されたMIMEオブジェクトなど）の場合、添付されたアイテムのスキャンについて報告します。	ScanReport テーブルの配列
無効になったメタメソッド: なし		

Archiveテーブル

アーカイブを説明するテーブル。以下のフィールドを含みます。

フィールド	説明	データタイプ
type	アーカイブの種類: <ul style="list-style-type: none">"archive" - アーカイブ。"mail" - メールファイル。"container" - その他のコンテナ。	文字列
name	アーカイブ名。例: ZIP	文字列
無効になったメタメソッド: なし		

DKIMテーブル

メッセージ内のすべてのDKIM署名を説明するテーブル。以下のフィールドを含みます。

フィールド	説明	データタイプ
signature	メッセージに存在するDKIM署名のリスト	DKIMSignature テーブルの配列



フィールド	説明	データタイプ
has_valid_signature	<p>1つのオプションの引数 <code>filter</code> を受け取って返す関数</p> <ul style="list-style-type: none">• DKIMSignature テーブルの形式で "pass" に等しいスキャン結果を持つ最初に検出された DKIM 署名。• 検証で署名が検出されなかった場合、<code>nil</code> が表示されます。 <p><code>filter</code> 引数として、次のものを使用できます。</p> <ul style="list-style-type: none">• DKIMSignatureFilter テーブル。• DKIMSignature 引数のみを受け取り、ブール値を返す任意の叙述関数<ul style="list-style-type: none">◦ <code>true</code> - 引数が条件を満たしている場合。◦ <code>false</code> - それ以外の場合。	機能
無効になったメタメソッド: なし		

DKIMSignatureテーブル

メッセージの DKIM 署名を説明するテーブル。以下のフィールドを含みます。

フィールド	説明	データタイプ
auid	DKIM 署名の "i" タグから取得される エージェントまたはユーザー識別子 (AUID) の値は、デフォルト値を考慮します	文字列
data	DKIM 署名の "b" タグから抽出された署名のテキスト (base64) 値	文字列
result	DKIM 署名検証結果	DKIMResult テーブル
sdid	DKIM 署名の "d" タグから取得した署名ドメイン識別子 (SDID) の値	文字列
selector	DKIM 署名の "s" タグから取得したセレクター	文字列
無効になったメタメソッド: なし		

DKIMResultテーブル

メッセージの DKIM 署名を説明するテーブル。以下のフィールドを含みます。

フィールド	説明	データタイプ
type	<p>テキスト形式の DKIM 署名検証結果。次の値が含まれる場合があります。</p> <ul style="list-style-type: none">• <code>pass</code> は、署名の検証が成功したことを示します。• <code>fail</code> は、署名の検証が失敗したことを示します (つまり、メール本文のハッシュと一致しないか、署名を検証できませんでした)。• <code>neutral</code> は、DKIM 署名の構文エラーです。	文字列



フィールド	説明	データタイプ
	<ul style="list-style-type: none">temperrorは、ドメインキーの取得に失敗したことを示します (DNSエラー)。permerrorは、他のタイプのエラー (署名形式、キー形式、キーと署名の間の不整合など) を示します。	
comment	スキャン結果のコメント (Authentication-Resultsのコメントとして使用できます)	文字列
key_size	スキャン中に使用されるキーサイズはnilか、キーまたはスキャン結果の取得に失敗した場合はneutral	番号
無効になったメタメソッド: なし		

テーブルDKIMSignatureFilter

DKIMメッセージ署名のフィルターを説明するテーブル (上記のFileFilterテーブルと同様)。次のフィールドが含まれます (すべてのフィールドはオプションです)。

フィールド	説明	データタイプ
domain	DKIM署名のSDIDフィールドのドメインが対応するドメイン	文字列または文字列のテーブル
domain_not	DKIM署名のSDIDフィールドのドメインが対応すべきではないドメイン	文字列または文字列のテーブル
無効になったメタメソッド: なし		

フィルターフィールドが指定されていない場合 (つまり、nil値が含まれている場合)、このメッセージのDKIM署名はすべてフィルターと一致します。複数のフィルターフィールドが指定されている場合、条件は接続詞 (論理積) によって結合されます。フィルターフィールドタイプがテーブル (配列) の場合、フィルターされたオブジェクトは、テーブル (配列) 要素の少なくとも1つと一致する必要があります。

利用可能な補助モジュール

LuaのプログラムスペースでDr.Web for UNIX Mail Serversとやり取りするために、次の特定のモジュールをインポートできます。

モジュール名	機能
drweb	Luaプログラムを起動したDr.Web for UNIX Mail ServersコンポーネントとLuaプロシージャの非同期実行の手段のログに、Luaプログラムからのメッセージを記録する機能を提供するモジュール
drweb.lookup	Dr.Web LookupDMモジュールを呼び出して外部ソースからデータを要求するためのツールを提供するモジュール
drweb.dnsxl	ホストのアドレスがDNSxLブラックリストにあるかどうかを確認するためのツールを提供するモジュール



モジュール名	機能
drweb.regex	文字列と正規表現を一致させるためのインターフェースを提供するモジュール
drweb.subprocess	外部アプリケーション(プロセス)を実行するためのインターフェースを提供するモジュール
drweb.config	Dr.Web MailD設定パラメータ値を持つテーブルを提供するモジュール。

drwebモジュールの内容

1. 機能

このモジュールは次の機能を提供します。

1.1.LuaプログラムからのメッセージをDr.Web for UNIX Mail Serversコンポーネントログに保存するための機能:

- `log(<level>, <message>)` は<message>文字列をDr.Web for UNIX Mail Serversログに<level>レベル(必要なレベルは、「debug」、「info」、「notice」、「warning」、「error」を使用して定義します)で書き込みます。
- `debug(<message>)` は<message>文字列をDr.Web for UNIX Mail ServersログにDEBUGレベルで書き込みます。
- `info(<message>)` は<message>文字列をDr.Web for UNIX Mail ServersログにINFOレベルで書き込みます。
- `notice(<message>)` は<message>文字列をDr.Web for UNIX Mail ServersログにNOTICEレベルで書き込みます。
- `warning(<message>)` は<message>文字列をDr.Web for UNIX Mail ServersログにWARNINGレベルで書き込みます。
- `error(<message>)` は<message>文字列をDr.Web for UNIX Mail ServersログにERRORレベルで書き込みます。

1.2.Luaプロシジャの同期管理のための機能:

- `sleep(<sec.>)` はこのLuaプロシジャインスタンスの実行を指定された秒数で一時停止します。
- `async(<Lua function>[, <argument list>])` は、指定された関数の非同期開始を起動し、指定された引数リストに転送します。`async`関数呼び出しはすぐに完了し、戻り値(**Future**テーブル)を使用すると、<Lua function>の結果を取得できます(まだ実行が完了していない場合は、完了するまで待機している可能性があります)。

1.3.IPアドレスを[IpAddress](#)テーブルとして表示するための機能:

- `ip(<address>)` は、**IpAddress**テーブルの形式で<address>文字列として送信される、IPアドレスを指定します。IPv4またはIPv6アドレスのいずれかを使用できます。

1.4.テキストファイルから外部データをアップロードするには:

- `load_set(<file path>)` は、指定されたテキストファイルのコンテンツからtrue値を含むテーブルを生成し、ファイルから読み取られた文字列はキーとして使用されます。空の文字列と空白文字のみで構成される文字列は無視され、テーブルには含まれません。
- `load_array(<file path>)` は、指定されたテキストファイルのコンテンツから文字列の配列を生成します。



空の文字列と空白文字のみで構成される文字列は無視され、配列には含まれません。

2. テーブル

2.1. **Future**テーブルは、`async`関数を使用して関数を実行した後の保留中の結果を表します。テーブルには以下のフィールドを含みます。

フィールド	説明	データタイプ
<code>wait</code>	<code>async</code> 関数を使用して開始した関数の結果を返す関数。関数がまだ実行を完了していない場合は、完了を待って結果を返します。 <code>wait</code> が呼び出される前に関数が完了した場合、結果はすぐに返されます。開始された関数が失敗した場合、 <code>wait</code> 呼び出しは同じエラーを生成します。	機能
無効になったメタメソッド: なし		

2.2 **IpAddress**テーブルはIPアドレスを表します。以下のフィールドを含みます。

フィールド	説明	データタイプ
<code>belongs</code>	<p>指定したサブネット (IPアドレス範囲) のIpAddressテーブルに保存されているIPアドレスの所属を確認する関数。</p> <p>「<code><IP address></code>」または「<code><IP address>/ <mask></code>」のような文字列を唯一の引数として受け取ります。ここで、<code><IP address></code>はホストアドレスまたはネットワークアドレス(「127. 0. 0. 1」など)、<code><mask></code>はサブネットワークマスク(「255. 0. 0. 0」などのIPアドレスとして、または「8」などの数値形式で指定できます)です。</p> <p>ブール値を返します。</p> <ul style="list-style-type: none">• <code>true</code>は、アドレスが指定されたアドレスの少なくとも1つと等しいか、指定されたサブネット (IPアドレスの範囲) の少なくとも1つに属していることを示します。• <code>false</code> - それ以外の場合。	機能
<p>無効になったメタメソッド:</p> <ul style="list-style-type: none">• <code>__tostring</code>は、文字列内のIpAddressを変更する関数です。例:「127. 0. 0. 1」(IPv4)または「:: 1」(IPv6)• <code>__concat</code>は、IpAddressを文字列に結合する関数です。• <code>__eq</code>は、2つのIpAddressが等しいことを確認するための関数です。• <code>__band</code>は、マスクを適用するための関数 (例: <code>dw.ip('192.168.1.2') & dw.ip('255. 255. 254. 0')</code>) です。		

3. 例



3.1.非同期的に開始される手順によって生成される、ログへの出力メッセージ:

```
local dw = require "drweb"

-- この関数は2秒間待機して文字列を返します。
-- 引数として受信されます
function out_msg(message)
    dw.sleep(2)
    return message
end

-- 「メイン」関数
function intercept(ctx)
    -- NOTI CELレベルでDr. Web for UNIX Mail Serversログに文字列を出力します
    dw.notice("Intercept function started.")

    -- out_msg関数の2つのコピーを非同期で起動します
    local f1 = dw.async(out_msg, "Hello,")
    local f2 = dw.async(out_msg, " world!")

    -- out_msg関数のコピーの完了を待機中です
    -- out_msgとその結果をログに出力します
    -- Dr. Web for UNIX Mail Servers ログにデバッグレベルで出力します
    dw.log("debug", f1.wait() .. f2.wait())
end
```

3.2.指定されたスケジュールに従って定期的に開始する手順を作成する:

```
local dw = require "drweb"

-- Futureテーブルをfutureグローバル変数で保存し、
-- Luaのガベージコレクターにより
-- 計画されたタスクが破壊されないようにします
future = dw.async(function()
    while true do
        -- 毎日、次のメッセージがログに表示されます
        dw.sleep(60 * 60 * 24)
        dw.notice("A brand new day began")
    end
end)
```

3.3.文字列のIPアドレスを変更する:

```
local dw = require "drweb"

local ipv4 = dw.ip("127.0.0.1")
local ipv6 = dw.ip("::1")
local mapped = dw.ip("::ffff:127.0.0.1")
```

drweb.lookupモジュールの内容

1. 機能



このモジュールは次の機能を提供します。

- `lookup(<request>, <parameters>)` は Dr.Web LookupD モジュールから利用できる外部ストレージからデータを要求します。`<request>` パラメータは、Dr.Web LookupD 設定内のセクション (文字列 `<type>@<tag>`) に対応している必要があります。`<parameters>` 引数はオプションで、リクエストを生成するために使用される置換を表します。これらのパラメータはテーブルとして設定されます。このテーブルのキーと値は文字列でなければなりません。この関数は、リクエストの結果である文字列の配列を返します。
- `check(<checked string>, <request>, <parameters>)` は、Dr.Web LookupD モジュールを介して利用できる外部リポジトリで `<checked string>` が見つかった場合に `true` を返します。引数 `<request>` および `<parameters>` は、`lookup` 関数の引数と同じです (上記を参照)。`<checked string>` 引数は、文字列または `__tostring` メタメソッドを持つテーブル (つまり、文字列にフォーマットできる) であると想定されます。

2. 例

データソース `LookupD.LDAP.users` から取得されたユーザーリストのログへの出力:

```
local dw = require "drweb"
local dwl = require "drweb.lookup"

-- 「メイン」関数
function intercept(ctx)
  -- NOTI CELレベルでDr. Web for UNIX Mail Serversログに文字列を出力します
  dw.notice("Intercept function started.")

  -- リクエスト結果をDr. Web for UNIX Mail Serversログへ出力
  -- 'ldap@users' データソースへ
  for _, s in ipairs(dwl.lookup("ldap@users", {user="username"})) do
    dw.notice("Result for request to 'ldap@users': " .. s)
  end
end

end
```

drweb.dnsxlモジュールの内容

1. 機能

このモジュールは次の機能を提供します。

- `ip(<IP address>, <DNSxL server>)` は指定されたIPアドレス `<IP address>` に対応するDNSxLサーバー `<DNSxL server>` からAタイプのDNSレコードをリクエストします。
検査されているIPアドレスがDNSxLサーバーのリストに登録されている場合、結果は架空のIPアドレスのリストになります。さらに、返された架空のIPアドレスのそれぞれに、検査済みの `<IP address>` がこのサーバーのリストに表示されている理由が含まれていることがあります (通常、理由タイプは返された架空のIPアドレスの最後のオクテット値によって決まります)。DNSxLサーバーにIPアドレス `<IP address>` に対応するAタイプのDNSレコードが含まれていない場合、関数は `nil` を返します。
- `url(<URL>, <SURBL server>)` は `<URL>` ドメイン部分に対応する `<SURBL server>` サーバーにからAタイプのDNSレコードをリクエストします (HTTPリダイレクトは処理されません)。
`<URL>` から取得された、検査されているドメインがSURBLサーバーのサーバーリストに登録されている場合、結果は架空のIPアドレスのリストになります。さらに、返された架空のIPアドレスのそれぞれに、検査済みのドメインがこのサーバーのリストに表示されている理由が含まれていることがあります (通常、理由タイプは返された架空のIPアドレスの最後のオクテット値によって決まります)。SURBLサーバーに `<URL>` からのドメインに対応するAタイプのDNSレコードが含まれていない場合、この関数は `nil` を返します。



関数の引数は、文字列または文字列にキャストされるオブジェクトです（たとえば、<IP address>としては [IpAddress](#) テーブルを使用でき、<URL>としては [Uri](#) テーブルを使用できます）。IPアドレスは、[IpAddress](#) テーブルの配列として返されます。

2. テーブル

2.1. [IpAddress](#) テーブルはIPアドレスを表します。テーブルについては [上](#) で説明しています。

3. 例

DNSxLサーバーによるIPアドレスのスキャン結果のログへの出力：

```
local dw = require "drweb"
local dwxl = require "drweb.dnsxl"

-- 「メイン」関数
function intercept(ctx)
  -- NOTICEレベルでDr. Web for UNIX Mail Serversログに文字列を出力します
  dw.notice("Intercept function started.")

  -- スキャン結果をDr. Web for UNIX Mail Serversログに出力します
  -- IPアドレス10. 20. 30. 40はDNSxLサーバーのブラックリストに登録されています
  -- dnsxl.server1.org
  local records = dwxl.ip("10.20.30.40", "dnsxl.server1.org")
  if records then
    for _, ip in ipairs(records) do
      dw.notice("DNSxL A record for 10.20.30.40: " .. ip)
    end
  end
end
```

drweb.regexモジュールの内容

1. 機能

このモジュールは次の機能を提供します。

- `search(<template>, <text>[, <flags>])` - <text>文字列に<template>正規表現と一致するサブストリングが含まれている場合は`true`を返します。オプションの<flags>パラメータ(整数)は、関数の動作に影響を与える一連のフラグであり、論理和でつながられます。
- `match(<template>, <text>[, <flags>])` - <template>正規表現がそのサブストリングだけでなく<text>ストリング全体と一致しなければならない点を除いて`search`と同じです。

2. 利用可能なフラグ

- `ignore_case`はテキストの大文字と小文字を区別しません。

3. 例



```
local rx = require "drweb.regex"

rx.search("te.?t", "some Text") -- false
rx.search("te.?t", "some Text", rx.ignore_case) -- true

rx.match("some.+", "some Text") -- true
```

drweb.subprocessモジュールの内容

1. 機能

このモジュールは次の機能を提供します。

- `run(<parameters>)` は指定されたプロセス(アプリケーション)を同期モードで実行します(この関数はプロセスが終了した後にのみコントロールを戻します)。`<parameters>` 引数は、ファイルへの実行可能ファイルのパス、起動時にアプリケーションに渡されるすべての引数(配列 `argv`)、アプリケーションの入出力ストリーム(`stdin`、`stdout`、`stderr`)に関連付けられたオプションのパラメータを含むテーブルです。オプションのパラメータは、アプリケーションの(現在の)作業ディレクトリと環境変数を指定します。

関数の結果は、終了後のプロセス操作の結果(プロセスが終了した終了コードまたはシグナル番号)を含むテーブルになります。さらに、プロセス実行パラメータのテーブルで指定すると、返されるテーブルに、`stdout`および`stderr`出力ストリームから読み込まれるデータを含むフィールドを含めることができます。

2. テーブル

2.1. 入力実行パラメータのテーブル。以下のフィールドを含みます。

フィールド	説明	データタイプ
(名前なし)	ファイルパスとアプリケーション実行引数(配列 <code>argv</code>)。 必須フィールド。フィールドはコマンドライン引数の数だけ繰り返され、最初の値は <code>argv[0]</code> 、つまり実行可能パスに対応します。	文字列
<code>stdin</code>	実行後にアプリケーション(プロセス)が入力ストリーム(<code>stdin</code>)から受け取るテキスト。オプションのフィールド(指定しない場合、 <code>stdin</code> は何も受け取りません)。	文字列
<code>stdout</code>	返されるテーブルのフィールドの名前。このフィールドは、プロセスが <code>stdout</code> ストリームに出力するテキストを受け取ります。オプションのフィールド(指定しない場合、出力は <code>stdout</code> に保存されません)。	文字列
<code>stderr</code>	返されるテーブルのフィールドの名前。このフィールドは、プロセスが <code>stderr</code> ストリームに出力するテキストを受け取ります。オプションのフィールド(指定しない場合、出力は <code>stderr</code> に保存されません)。	文字列
<code>env</code>	プロセス環境に送信される環境変数をフィールドに持つテーブル。環境変数は、" <code><variable name>=<value></code> "のペアで指定されます。オプションのフィールド(指定しない場合、環境変数は設定されません)。	テーブル
<code>workdir</code>	実行中のプロセスの作業(現在の)ディレクトリ。オプションのフィールド(指定しない場合、作業ディレクトリは設定されません)。	文字列

2.2. 実行結果のテーブル(`run`関数の戻り値)以下のフィールドを含みます。



フィールド	説明	データタイプ
exit_status	プロセスが正常に終了したときの返りコード。発生していない場合は、nilになります。	番号
exit_signal	プロセスが終了したときのシグナル番号発生していない場合は、nilになります。	番号
(入カパラメータテーブルの stdoutフィールドの値)	終了したプロセスの <i>stdout</i> ストリームから読み込まれたデータ。フィールドは、入カパラメータのテーブルで <i>stdout</i> フィールドが指定されている場合にのみ使用可能です。	文字列
(入カパラメータテーブルの stderrフィールドの値)	終了したプロセスの <i>stderr</i> ストリームから読み込まれたデータ。フィールドは、入カパラメータのテーブルで <i>stderr</i> フィールドが指定されている場合にのみ使用可能です。	文字列

3.例

3.1.**cat**ユーティリティを引数なしで実行し、'some data'テキストをその入力ストリームに渡し、コマンド出力の結果を返されるテーブルの *stdout_field* フィールドに渡すには、次のように指定します。

```
local sp = require 'drweb.subprocess'

local cat_result = sp.run({
  '/bin/cat',
  stdin = 'some data',
  stdout = 'stdout_field',
})
```

cat_result 変数に格納される結果のテーブルには、以下のフィールドが含まれます。

フィールド	値
exit_status	0
exit_signal	nil
stdout_field	'some data'

3.2.**-c**と *env | grep TESTVAR 1>&2* のパラメータを指定して **sh** コマンド (インタプリタによりコマンド実行) を実行し、*VALUE* 値を持つ *TESTVAR* 変数を環境に追加し、コマンド *stderr* の出力結果を返されるテーブルの *stderr_field* フィールドに渡すには、次のように指定します。

```
local sp = require 'drweb.subprocess'

local env_result = sp.run({
  '/bin/sh', '-c', 'env | grep TESTVAR 1>&2',
  env = { TESTVAR = 'VALUE' },
  stderr = 'stderr_field'
})
```

env_result 変数に格納される結果のテーブルには、以下のフィールドが含まれます。



フィールド	値
exit_status	0
exit_signal	nil
stderr_field	'TESTVAR=VALUE\n'

3.3. **pwd**コマンドを実行して作業ディレクトリをシステムのルートディレクトリに設定し、コマンド`stdout`の出力結果を返されるテーブルの`stdout_field`フィールドに渡すには、次のように指定します。

```
local sp = require 'drweb.subprocess'

local pwd_result = sp.run{
  '/bin/pwd',
  workdir = '/',
  stdout = 'stdout_field'
}
```

`pwd_result`変数に格納される結果のテーブルには、以下のフィールドが含まれます。

フィールド	値
exit_status	0
exit_signal	nil
stdout_field	'/\n'

3.4. **kill**コマンドを`bash`で実行し、**SIGKILL**シグナルをインタプリタに渡すには、次のように指定します。

```
local sp = require 'drweb.subprocess'

local kill_result = sp.run{' /bin/bash', '-c', 'kill -9 $$'}
```

`kill_result`変数に格納される結果のテーブルには、以下のフィールドが含まれます。

フィールド	値
exit_status	nil
exit_signal	9

プロセスを非同期的に実行するには、`async`関数呼び出し内で`run`関数を実行します（上を参照）。

drweb.configモジュールの内容

1. 機能

このモジュールには関数はありません。

2. 利用可能なテーブル

このモジュールでは、次のフィールドで**MailDConfig**テーブルを提供します。



フィールド	説明	データタイプ
version	Dr.Web MailDバージョン。	文字列
無効になったメタメソッド: なし		

MailDConfigテーブルは、モジュールによってmaildフィールドとして提供されます。

3. 例

以下はDr.Web MailDコンポーネントの現在のバージョンをログに記録する出力です。

```
local dw = require 'drweb'
local cfg = require 'drweb.config'

-- 「メイン」関数
function milter_hook(ctx)

  -- NOTI CELレベルでDr. Web for UNIX Mail Serversログに文字列を出力します
  dw.notice(cfg.maild.version)

end
```

Dr.Web Anti-Spam

Dr.Web Anti-Spamは、メールメッセージをスキャンしてスパムを検出するためのコンポーネントです。このコンポーネントは、メールスキャンコンポーネントDr.Web MailDによって使用されます。パッケージによっては、Dr.Web for UNIX Mail ServersにDr.Web Anti-Spamがない場合があります（この場合、Dr.Web MailDはスパムスキャンを実行しません）。

動作原理

スパムの兆候についてDr.Web MailD（またはその他の外部アプリケーション）から受信したメッセージの解析は、**VadeSecure**によって開発された**VadeRetro**アンチスパムソリューションを使用して実行されます。メッセージの解析は、スパムに関する情報の外部ソースへの要求なしに、スタンドアロンモードで実行されます。このソリューションでは、メッセージのスパム分類のためのルールのデータベースが動的に更新されるため、メッセージの処理速度が速くなり、メッセージ解析品質が継続的に向上します（更新は**Dr.Web Updater**で自動的に行われます）。



ユーザーは、メールメッセージのアンチスパムスキャンにDr.Web Anti-Spam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 Anti-Spamには**Google Protobuf**に基づく特別なAPIが含まれています。Dr.Web Anti-Spam APIガイドとDr.Web Anti-Spamを使用したクライアントアプリケーションの例入手するには、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。



Dr.Web Anti-Spamコンポーネントは、ARM64アーキテクチャ向けDr.Web for UNIX Mail Serversのバージョンには含まれていません。



Dr.Web Anti-Spamは、アンチスパムライブラリ**VadeRetro**によってメールメッセージに付与されたポイントを、0から1までの数字（パーセンテージ評価）に変更することによって正規化します。Dr.Web Anti-Spamの**VadeRetro**ポイントと評価（パーセンテージ）のおおよその一致の表は以下のとおりです。

VadeRetroポイント	Dr.Web Anti-Spam/パーセンテージ
0以下	0.00
0-10	0.00-0.19
10-50	0.19-0.63
50-100	0.63-0.80
100-150	0.80-0.86
150-200	0.86-0.90
200-300	0.90-0.93
300-400	0.93-0.95
400-500	0.95-0.96
500以上	0.96-1.00



指定された**VadeRetro**ポイント d に対する、Dr.Web Anti-Spamのパーセンテージ p の正確な値を取得するには、次の式を使用します。 $p = 2 \cdot \arctg(0.030777 \cdot d) / \pi$ 。

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

- 誤ってスパムと判定されたメッセージは vrnonspam@drweb.com に送信してください。
- 検出されなかったスパムメッセージは vrspam@drweb.com に送信してください。

コマンドライン引数

OSのコマンドラインからDr.Web Anti-Spamを起動するには、次のコマンドを使用します。

```
$ <opt_dir>/bin/drweb-ase [<arguments>]
```

Dr.Web Anti-Spamでは、次のオプションを使用できます。

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-ase --help
```

このコマンドはDr.Web Anti-Spam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

スタンドアロンモードでコマンドラインからコンポーネントを直接起動するオプションは提供されていません。メールのスパムスキャン中にDr.Web Anti-Spamコンポーネントによって自動的に実行されます。さらに、コンポーネント構成でFixedSocketパラメータ値が定義されている場合、1つのコンポーネントコピーがDr.Web ConfigD設定デーモンによって常に行われ、このUNIXソケットを介してユーザーが使用できるようになります。コンポーネントパラメータとメールオブジェクトチェックを管理するには、コマンドラインからDr.Web for UNIX Mail Serversを管理するためのDr.Web Ctlユーティリティを使用します(コマンドdrweb-ctlによって実行されます)。

スパムのDr.Web Anti-Spamコンポーネント(Dr.Web MailDコンポーネント経由)による任意のメールメッセージをスキャンするには、ツールDr.Web Ctlのコマンド checkmailを使用します。これを行うには、スキャンしたメールメッセージをドライブに保存して(.eml形式など)、次のコマンドを使用します。

```
$ drweb-ctl checkmail <path to file .eml/>
```



このコンポーネントに関するマニュアルをコマンドラインから要求するには、`man 1 drweb-ase` コマンドを使用します。

設定パラメータ

コンポーネントは、Dr.Web for UNIX Mail Serversの統合された設定ファイルの[Antispam]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}	<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 <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-ase <ul style="list-style-type: none">• GNU/Linuxの場合: /opt/drweb.com/bin/drweb-ase• FreeBSDの場合: /usr/local/libexec/drweb.com/bin/drweb-ase
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
FixedSocket <i>{path to file}</i>	固定コンポーネントコピーのソケットファイルへのパス。 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。 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。 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）。 デフォルト値: 1h
FullCheck <i>{Boolean}</i>	メールのフルスキャンを実行してスパムの兆候がないか調べます。Noの場合、スパムスコアの数値が FastCheckStopThreshold で指定された値を超えるとすぐにスキャンが停止します。 デフォルト値: Yes
FastCheckStopThreshold <i>{integer}</i>	FullCheck パラメータの値がNoに設定されている場合、スパムスコアが上限に達すると、メッセージのスキャンが停止します。 デフォルト値: 300
AllowCyrillicText <i>{Boolean}</i>	キリル文字のテキストを含むメールを許可します。Noの場合、そのようなメールのスパムスコアが増加します。 デフォルト値: Yes
AllowCjkText	アジア（中国語、日本語、韓国語）言語のメールを含むメールを許可します。Noの場合、そのようなメールのスパムスコアが増加します。



<i>{Boolean}</i>	デフォルト値 : Yes
CheckCommercialEmails <i>{Boolean}</i>	広告メール(プロモーションメール、プロモーションやセールスの通知など)を識別します。Noの場合、そのようなメールはスパムと見なされません。 デフォルト値 : No
CheckSuspiciousEmails <i>{Boolean}</i>	疑わしいメール(懸賞金の提供を申し出るメールなど)を識別します。Noの場合、そのようなメールはスパムと見なされます。 デフォルト値 : No
CheckCommunityEmails <i>{Boolean}</i>	ソーシャルメディアメールを識別します。Noの場合、そのようなメールはスパムと見なされます。 デフォルト値 : No
CheckTransactionalEmails <i>{Boolean}</i>	トランザクション通知(登録、サービスや商品の購入など)を識別します。Noの場合、そのようなメールはスパムと見なされます。 デフォルト値 : No
DetectSpamType <i>{Boolean}</i>	スパムメールタイプ(不正行為、詐欺)を識別します。Noの場合、そのようなメールはスパムと見なされます。 デフォルト値 : No



SpIDer Gate



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。

ネットワークトラフィックとURLを監視するコンポーネントSpIDer Gateは、データ(ネットワークからローカルコンピューター、ローカルホストからネットワークにダウンロードされたデータ)の脅威を検査し、不要なカテゴリーに含まれるWebリソースや管理者によって定義されたブラックリストに含まれるネットワークホストとの接続を防止します。

コンポーネント設定では、スキャン対象のプロトコルの種類を指定することができます。コンポーネントには、検査済みの接続を介してデータを送信するために使用されるプロトコルタイプのアナライザが含まれています。プロトコルがメールプロトコルであると判定された場合、脅威の解析と検索には[Dr.Web MailD](#)メールメッセージコンポーネントを使用します。

コンポーネントは、URLがいずれかのカテゴリー(HTTP/HTTPSプロトコルを利用する接続のスキャンに使用される)に属しているかどうかを確認するために、Doctor Webの更新サーバーから定期的に更新されるWebリソースカテゴリーのデータベースを使用するだけでなく、Dr.Web Cloudサービスも参照します。Doctor Webは、以下のWebリソースカテゴリーを追跡します。

- *InfectionSource* - 悪意のあるソフトウェアを含むWebサイト(「感染源」)。
- *NotRecommended* - アクセスすることが推奨されない不正なWebサイト(「ソーシャルエンジニアリング」を使用しているもの)。
- *AdultContent* - ポルノまたはエロティックなコンテンツ、出会い系サイトなどを含むWebサイト。
- *Violence* - 暴力行為を助長するWebサイトや、さまざまな死亡事故などに関するコンテンツを含むWebサイト。
- *Weapons* - 武器および爆発物に関するWebサイトや、それらの製造に関する情報を提供しているWebサイト。
- *Gambling* - 勝負事、カジノ、オークション、オンラインゲームへのアクセスを提供するWebサイト(賭けサイトを含む)。
- *Drugs* - 麻薬の使用、製造または流通を促進するWebサイト。
- *ObsceneLanguage* - 卑猥な言葉を含む(タイトル、記事などに)Webサイト。
- *Chats* - テキストメッセージのリアルタイム送信を提供するWebサイト。
- *Terrorism* - 攻撃的なプロパガンダ、またはテロ攻撃に関する内容を含むWebサイト。
- *FreeEmail* - メール無料登録を提供するWebサイト。
- *SocialNetworks* - さまざまなソーシャルネットワークサービス: 一般、仕事、企業、興味、テーマ別出会い系サイト。
- *DueToCopyrightNotice* - 一部の著作物(映画、音楽など)の著作権者によって定義されるWebサイト。
- *OnlineGames* - インターネットへの常時接続を使用してゲームへのアクセスを提供するWebサイト。
- *Anonymizers* - ユーザーが個人情報を隠し、ブロックされたWebリソースにアクセスすることを可能にするWebサイト。
- *CryptocurrencyMiningPool* - 仮想通貨マイニングのための一般的なサービスへのアクセスを提供するWebサイト。
- *Jobs* - 求人検索Webサイト。



システム管理者は、ホストが属するカテゴリーに基づいて、望ましくないホストへのアクセスを設定できます。またユーザーは、特定のホストへのアクセスをブロックするために独自のブラックリストを設定したり、アクセスを許可したリするためにホワイトリストを設定することもできます。ホワイトリストのホストへのアクセスは、それらが望ましくないカテゴリーに属する場合でも許可されます。ローカルのブラックリストとWebリソースのカテゴリーのデータベースにURLに関する情報がない場合、コンポーネントはDr.Web Cloudサービスを参照して、他のDr.Web製品から受信するこうしたURLに悪意があるかどうかの情報をリアルタイムで検査できます。



同一のWebサイトは、複数のカテゴリーに同時に所属させることができます。そのようなWebサイトへのアクセスは、不要なカテゴリーのいずれに属する場合もブロックされます。

Webサイトがホワイトリストに含まれる場合でも、データ(Webサイトから送信およびダウンロードされたもの)に脅威が含まれているかどうかはスキャンされます。

HTTPプロトコルを介して転送されるファイルのスキャンの負荷が高まると、[Dr.Web Network Checker](#)コンポーネントによって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 Mail Serversに使用可能なファイル記述子の[上限を増やす](#)必要があります。

動作原理

SpIDer Gateコンポーネントは、ユーザーアプリケーションによって確立されたネットワーク接続を監視します。コンポーネントは、クライアントアプリケーションが接続しようとしているサーバーが、設定で不要と指定されているWebリソースカテゴリーのいずれかに属するかどうかを検査します。さらに、コンポーネントはDr.Web Cloudを参照してURLを検査できます。URLが不要なカテゴリー(Dr.Web Cloudのリクエストによって返されたものを含む)またはシステム管理者によって定義されたブラックリストのいずれかに属する場合、接続は中断され、アクセスが許可されていないというメッセージが含まれるHTMLページが表示されます(HTTP/HTTPS接続の場合)。HTMLページは、コンポーネントに付属するテンプレートに従ってSpIDer Gateによって生成されます。このページには、リクエストされたリソースにアクセスできないという通知とブロックに関する詳細が表示されます。SpIDer Gateがブロックする必要のある脅威を見つけた場合、同様のページが表示され、クライアントに返されます。接続にHTTP(S)とは異なるプロトコルが使用されている場合、コンポーネントはこのサーバーとの接続を確立するための許可のみをスキャンします。メールプロトコル(SMTP、POP3、またはIMAP)であると判断された場合、メールメッセージのスキャン用コンポーネント[Dr.Web MailD](#)がデータの解析と脅威の検索に使用されます。このコンポーネントは個別にメールメッセージを分類し、ファイルとURLに囲まれた本文から抽出します。それを前提に、コンポーネントはコンポーネントSpIDer Gateと共通のブロックパラメータを使用します。

補助コンポーネント[Dr.Web Firewall for Linux](#)は、クライアントアプリケーションによって確立されたりリモートサーバーとの接続をリダイレクトします。コンポーネントは、**GNU/Linux**システムコンポーネントの**NetFilter**ルールの動的管理を実行します。

[Dr.Web Updater](#)コンポーネントは、Doctor Web更新サーバーからWebリソースカテゴリーのデータベースを定期的かつ自動的に更新するために使用されます。同じコンポーネントは、[Dr.Web Scanning Engine](#)スキャンエンジン用のウイルスデータベースを更新するために使用されます。[Dr.Web CloudD](#)コンポーネントは、Dr.Web Cloudサービスを参照するために使用されます(クラウドサービスの使用は、Appendixes [共通設定](#)で設定され、必要に応じて無効にできます)。転送されたデータを検査するために、SpIDer Gateは[Dr.Web Network Checker](#)コンポーネントを使用します。後者では、[Dr.Web Scanning Engine](#)スキャンエンジンを介してスキャンが開始されます。



コマンドライン引数

SpIDer Gate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-gated [<parameters>]
```

SpIDer Gate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-gated --help
```

このコマンドはSpIDer Gate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 Mail 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-gated**

設定パラメータ

コンポーネントは、Dr.Web for UNIX Mail Serversの統合された[設定ファイル](#)の[GateD]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}	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-gated <ul style="list-style-type: none">• GNU/Linuxの場合: /opt/drweb.com/bin/drweb-gated• FreeBSDの場合: /usr/local/libexec/drweb.com/bin/drweb-gated
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
TemplatesDir <i>{path to directory}</i>	Webリソースをブロックしたときに送信されるHTML通知のテンプレートを含むディレクトリへのパス。 デフォルト値: <var_dir>/templates/gated <ul style="list-style-type: none">• GNU/Linuxの場合: /var/opt/drweb.com/templates/gated• FreeBSDの場合: /var/drweb.com/templates/gated
CaPath <i>{path}</i>	信頼できるルート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。 デフォルト値: 信頼できる証明書のリストへのパス。パスはお使いの GNU/Linux ディストリビューションに依存します。 <ul style="list-style-type: none">• Astra Linux, Debian, Linux Mint, SUSE Linux, Ubuntuの場合、通常は/etc/ssl/certs/です。• CentOSとFedoraの場合、/etc/pki/tls/certs/ca-bundle.crtです。• 他のディストリビューションでは、コマンドopenssl version -dの実行結果によってパスを定義できます。• コマンドが使用できない場合、またはOSディストリビューションを特定できない場合は、値/etc/ssl/certs/が使用されます。



接続スキャンの設定を変更しても、変更を加える前にアプリケーションによってすでに確立されている接続のスキャンには影響しません。



補助コンポーネントDr.Web Firewall for Linuxの[設定](#)で、トラフィックモニタリングのより具体的なパラメータを指定します。



Dr.Web Firewall for Linux



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。

コンポーネントを正しく動作させるため、以下のオプションを指定してOSカーネルが構築されている必要があります。

- `CONFIG_NETLINK_DIAG, CONFIG_INET_TCP_DIAG;`
- `CONFIG_NF_CONNTRACK_IPV4, CONFIG_NF_CONNTRACK_IPV6, CONFIG_NF_CONNTRACK_EVENTS`
- `CONFIG_NETFILTER_NETLINK_QUEUE, CONFIG_NETFILTER_NETLINK_QUEUE_CT, CONFIG_NETFILTER_XT_MARK.`

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

Dr.Web Firewall for Linuxは補助コンポーネントです。SpIDer Gateに対して接続マネージャー機能を実行します。Dr.Web Firewall for Linuxは、ホスト接続がSpIDer Gateを通過し、接続トラフィックが監視されるようにします。

動作原理

このセクションの内容:

- [概要](#)
- [接続監視のメカニズム](#)
- [接続監視の順序](#)

概要

Dr.Web Firewall for Linuxコンポーネントにより、SpIDer Gateが正しく動作するようにします。**NetFilter** (**GNU/Linux**OSコンポーネント) 用に調整されたルーティングルールを解析し、確立された接続が、クライアントアプリケーションとリモートサーバー間の中間の機能(プロキシ)を実行するSpIDer Gateにリダイレクトされるように修正します。

Dr.Web Firewall for Linuxは、トランジット接続だけでなく、送信と受信のリダイレクトのルールを別々に管理できます。迂回またはリダイレクトのルールを正確に設定するには、コンポーネントではLuaで書かれたスクリプトだけでなく設定に組み込まれたルールを使うことができます。

接続監視のメカニズム

接続を監視するために、Dr.Web Firewall for Linuxはルーティングポリシーのデータベース(**man ip: ip route**、**ip rule**参照)と**NetFilter**システムコンポーネントの**`nf_conntrack`**インターフェースで指定されたルーティングテーブルを使用します。監視された接続と転送されたパケットには、Dr.Web Firewall for Linuxが**NetFilter**のチェーンのさまざまな段階で接続をリダイレクトし、転送されたパケットを正しく処理できるようにするビットマークが付けられます(詳細は**man iptables**を参照)。



iptablesルールのアクション

Dr.Web Firewall for Linuxは、**iptables**ルールで次のアクションを使用します。

- **MARK**: このアクションにより、Dr.Web Firewall for Linuxは指定された数字マークをパケットに設定できます。
- **CONNMARK**: このアクションにより、Dr.Web Firewall for Linuxは指定された数字マークを接続に設定できます。
- **TProxy**: このアクションにより、Dr.Web Firewall for Linuxは、パケットのコンテンツを変更することなく、**PREROUTING NetFilter**チェーンから指定されたネットワークソケット (<IP address>: <port>) にパケットをリダイレクトできます。このアクションを使用すると、Dr.Web Firewall for Linuxは接続の最初の宛先アドレスを特定できます。
- **NFQUEUE**: このアクションにより、エンジンのネットワークスタックから、スキャンのためにカーネル空間外で動作するプロセスにパケットを送信できます。したがって、Dr.Web Firewall for Linuxは、特殊な *Netlink* ソケットを介して、指定した番号のキュー **NFQUEUE** に接続し、処理で判定するために必要なパケットを入手します (Dr.Web Firewall for Linuxは、**NetFilter** に、**DROP**: ドロップ、**ACCEPT**: 許可、**REPEAT**: 繰り返しのいずれかの判定を伝える必要があります)。

パケットと接続のマーク

パケットをマークするため、Dr.Web Firewall for Linuxは、パケットおよび接続マークで使用可能な32ビットのうち次の3つを使用します。

- **LDM**ビット (*Local Delivery Mark*)。マークにこのビットがあるパケットは、使用しているルーティングルールに基づいてローカルホストに送信されます。
- **CPM**ビット (*Client Packets Mark*)。クライアント (接続開始側) とプロキシ (Dr.Web Firewall for Linuxなど) 間の接続を示します。
- **SPM**ビット (*Server Packets Mark*)。プロキシ (Dr.Web Firewall for Linuxなど) とサーバー (接続受信側) 間の接続を示します。

LDP、**SDP**、**MCP**ビットは、ルーティング接続を実行する他のアプリケーションがパケットをマークするために使用していない任意のさまざまなビットにすることができます。デフォルトでは、Dr.Web Firewall for Linuxは適切な (他のアプリケーションでは使用されていない) ビットを自動的に選択します。

ルートとルーティングポリシー (**ip rule**、**ip route**)

Dr.Web Firewall for Linuxを (あらゆる接続スキャンモードで) 正しく動作させるには、100番のルーティングテーブルを使用する**ip rule**ルーティングポリシーをシステムに設定する必要があります。

```
from all fwmark <LDM>/<LDM> lookup 100
```

次のルートをテーブルに追加する必要があります。

```
local default dev lo scope host
```

このルーティングポリシーは、マークに**LDM**ビットが入っているパケットが常にローカルホストに送信されることを保証します。



それ以降、 XXX ビットの $\langle XXX \rangle$ 文字列は、 2^N (N はパケットマーク内の XXX ビットの序数)に等しい16進値になります。たとえば、最小(ゼロ)ビットがLDMビットとして選択されている場合は、 $\langle LDM \rangle = 2^0 = 0x1$ になります。

NetFilter (iptables) のルール

Dr.Web Firewall for Linuxを(あらゆる接続スキャンモードで)正しく動作させるには、次の6つのルール(**iptables-save**出力コマンド形式で表示)が**NetFilter**システムコンポーネントの該当するチェーンのnatテーブルとmangleテーブルに存在する必要があります。

```
*nat

-A POSTROUTING -o lo -m comment --comment drweb-firewall -m mark --mark
<LDM>/<LDM> -j ACCEPT

*mangle

-A PREROUTING -m comment --comment drweb-firewall -m mark --mark
0x0/<CPM+SPM> -m connmark --mark <SPM>/<CPM+SPM> -j MARK --set-xmark
<LDM>/<LDM>
-A PREROUTING -p tcp -m comment --comment drweb-firewall -m mark ! --mark
<CPM+SPM>/<CPM+SPM> -m connmark --mark <CPM>/<CPM+SPM> -j TPROXY --on-port
<port> --on-ip <IP-address> --tproxy-mark <LDM>/<LDM>
-A OUTPUT -m comment --comment drweb-firewall -m mark --mark
<CPM>/<CPM+SPM> -j CONNMARK --set-xmark <CPM>/0xffffffff
-A OUTPUT -m comment --comment drweb-firewall -m mark --mark
<SPM>/<CPM+SPM> -j CONNMARK --set-xmark <SPM>/0xffffffff
-A OUTPUT -m comment --comment drweb-firewall -m mark --mark 0x0/<CPM+SPM>
-m connmark ! --mark 0x0/<CPM+SPM> -j MARK --set-xmark <LDM>/<LDM>
```



以下の説明では、0~5の番号がこれらのルールに割り当てられています(文書に記載されている順序で)。式 $\langle X+Y \rangle$ は、それぞれの数 X と Y のビット数「OR」(合計)を意味します。

ルール番号2のパラメータ $\langle IP\ address \rangle$ と $\langle port \rangle$ は、Dr.Web Firewall for Linuxが監視された接続を管理するネットワークソケットを示します。

さらに、Dr.Web Firewall for Linux設定で監視接続モード(送信、受信、トランジット)を有効にする場合は、次の追加ルールが該当するチェーンのmangleテーブル(*OUTPUT*、*INPUT*、*FORWARD*)に存在する必要があります。

- 送信(*OUTPUT*) 接続を監視するには:

```
-A OUTPUT -p tcp -m comment --comment drweb-firewall -m tcp --tcp-flags
SYN,ACK SYN -m mark --mark 0x0/<CPM+SPM> -j NFQUEUE --queue-num <ONum> --
queue-bypass
```

- 受信(*INPUT*) 接続を監視するには:



```
-A INPUT -p tcp -m comment --comment drweb-firewall -m tcp --tcp-flags SYN,ACK SYN -m mark --mark 0x0/<CPM+SPM> -j NFQUEUE --queue-num <INum> --queue-bypass
```

- トランジット(*FORWARD*) 接続を監視するには:

```
-A FORWARD -p tcp -m comment --comment drweb-firewall -m tcp --tcp-flags SYN,ACK SYN -m mark --mark 0x0/<CPM+SPM> -j NFQUEUE --queue-num <FNum> --queue-bypass
```



以下の説明では、6、7、8の番号がこれらのルールに割り当てられています（文書に記載されている順序で）。

ここで、<ONum>、<INum>、<FNum>は、Dr.Web Firewall for Linuxが対応する接続のインストールを示すパケット（SYNフラグが設定されているがACKフラグは含まれていないパケット）を待機しているNFQUEUE内のキューの数です。

接続監視の順序

ルール6、7、8のいずれかに従って、対応する方向の新しいネットワーク接続を示すパケットは、CPMとSPMのどちらのビットでもマークされていない場合、**NetFilter**によって該当するNFQUEUEキューに入れます。ここでパケットは、*nf_conntrack*インターフェースを介してDr.Web Firewall for Linuxによって読み取られます。ルール3と4は、接続を監視済みとしてマークします。つまり、接続マークに接続方向が設定されていることを示すビットがあります。このビット番号は、パケットマークのビット番号と一致します。その結果、ルール1、2、5に従って、この接続を介して送信されたパケットはDr.Web Firewall for Linuxによって配信されます。ルール0がnatテーブルのPOSTROUTINGチェーンの最上部に追加されるため、NATが設定されている場合、マークされたパケットのアドレスは送信されません（Dr.Web Firewall for Linuxの監視および接続処理ロジックに干渉するため）。

パケットがいずれかのNFQUEUEキューに現れると、Dr.Web Firewall for Linuxは、**NetFilter**で誤ったルールが設定されている場合に備えて、パケットの基本的な処理を実行します。次に、Dr.Web Firewall for Linuxは、ルール4に従い、それ自体の名前と、PSCとマークされたソケットを使用してサーバーへの接続を試みます。ローカル配信のルール5は適用されません。パケットはSPMでマークされており、このルールは<CPM + SPM>でマークされたパケットにのみ適用できるためです。

- サーバーへの接続が失敗した場合、Dr.Web Firewall for Linuxは、RSTビットを含むクライアントパケットを生成し、<IP address>:<port>のペアをリクエストされたサーバーのネットワークソケットのアドレスに置き換えます。DROP判定もNFQUEUEに送信されます。RSTビットを含むパケットの送信に使用されるソケットは<CPM+SPM>としてマークされているため、上記のルールはどれも適用されず、パケットは通常のルーティングルールに従ってクライアントに配信されます。
- リモートサーバーへの接続が成功した場合、Dr.Web Firewall for Linuxは、監視したSYNパケットをコピーし、<LDM+CPM>とマークされたソケットから再送信して、パケットをローカルネットワークソケットにリダイレクトします。LDMビットが設定されているため、指定したルーティングルールに従って出カインターフェースを選択すると、パケットは*looback*インターフェースに追加されます。その後、**NetFilter** PREROUTINGチェーンに追加され、そこでルール2が適用されます。したがって、パケットは変更されることなくネットワークソケットDr.Web Firewall for Linuxにリダイレクトされます。この機能により、Dr.Web Firewall for Linuxは接続アドレスの4つの要素すべて（パケット送信者のIPアドレスとポート、パケット受信者のIPアドレスとポート）を保存できます。

Dr.Web Firewall for Linuxがルール2に従って監視した接続を受信するネットワークソケットの場合、IP_TRANSPARENTオプションと<LDM+CPM>マークが設定され、このソケットからDr.Web Firewall for



Linuxによって送信されたパケットが*NFQUEUE*キューに分類されないようにします。クライアントが接続すると、保存されている4要素のアドレス(パケット送信者のIPアドレスとポート、パケット受信者のIPアドレスとポート)を使用して、ペアのソケットが検索されます。クライアントとサーバーの接続が確立されると、Luaの手順とDr.Web Firewall for Linux設定で指定したスキャンルールに従ってスキャンされます。スキャンが成功し、接続が安定している場合は、クライアント側とサーバー側を接続する関連ソケットのペアが転送データの分析のためにSpIDer Gateコンポーネントに転送されます。次のクライアントとサーバー間の対話は、メディエーターSpIDer Gateを介して確立されます。Dr.Web Firewall for Linuxは、クライアント側とサーバー側に関連付けられたソケットペアに加えて、確立された接続をスキャンするためのパラメータとルールをSpIDer Gateに送信します。

Dr.Web Firewall for Linux動作の概略図を以下に示します。

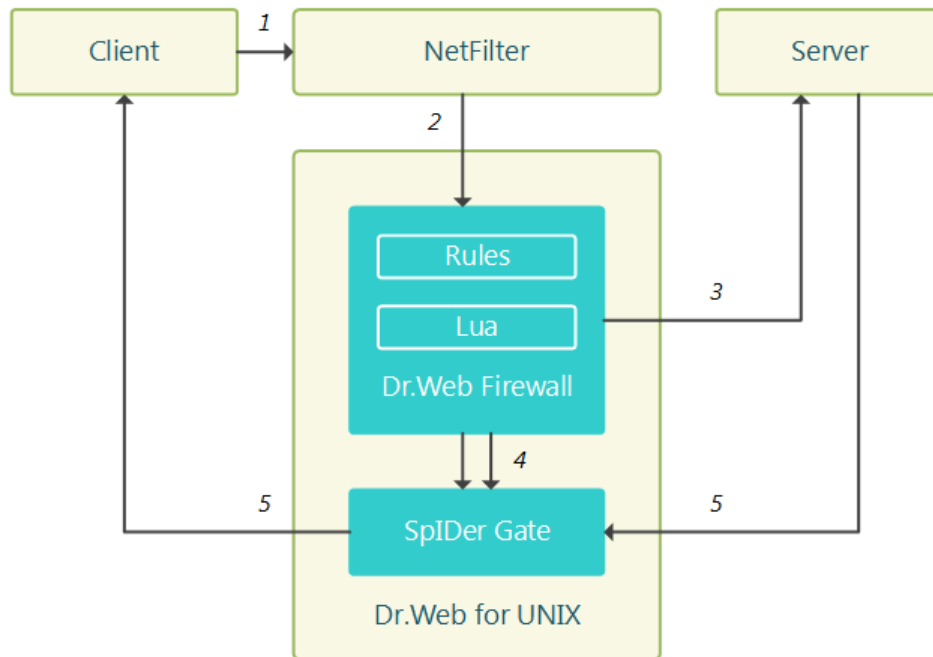


図13. コンポーネントの動作図

以下の接続処理のステップには番号が付いています。

1. クライアントがサーバーへの接続を試みます。
2. ルーティングルールに従って、**NetFilter**の接続をDr.Web Firewall for Linuxにリダイレクトします。
3. Dr.Web Firewall for Linuxは、クライアントの名前と接続スキャンを使用して、サーバーへの接続を試みます。
4. 接続のクライアント側とサーバー側、接続処理用のSpIDer Gate、およびスキャンの設定とルールに関連するソケットペアの送信。
5. メディエーターとしてSpIDer Gateを介したサーバーとクライアント間のデータ交換。



Dr.Web Firewall for Linuxを正しく動作させるためには、ルーティングテーブルに正しい数のビットマーク、*NFQUEUE*キュー、接続監視用のネットワークソケットアドレスを使用するこうしたルールが必要です。デフォルト設定では、コンポーネントは必要なルール設定を自動的に実行します。設定で接続の自動設定が無効になっている場合、コンポーネントを起動するときに必要なルールを手動で入力する必要があります。



コマンドライン引数

Dr.Web Firewall for Linux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-firewall [<options>]
```

Dr.Web Firewall for Linux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-firewall --help
```

このコマンドはDr.Web Firewall for Linux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 Mail 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(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-firewall**

設定パラメータ

コンポーネントは、Dr.Web for UNIX Mail Serversの統合された[設定ファイル](#)の[LinuxFirewall]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](#)。
- [トラフィックモニタリングとアクセスブロックのルール](#)。



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-firewall <ul style="list-style-type: none">• GNU/Linuxの場合 合: /opt/drweb.com/bin/drweb-firewall• FreeBSDの場合 合: /usr/local/libexec/drweb.com/bin/drweb-firewall
XtablesLockPath <i>{path to file}</i>	iptables (NetFilter) テーブルブロックファイルへのパス。パラメータ値が指定されていない場合は、/run/xtables.lock と/var/run/xtables.lockパスが検査されます。指定されたパスまたはデフォルトのパスにファイルが見つからない場合は、コンポーネントを起動したときにエラーが発生します。 デフォルト値: (指定なし)
InspectFtp <i>{On / Off}</i>	FTPプロトコルを介して転送されたデータをスキャンするかどうかを指示します。 実際のデータスキャンは、指定されたスキャンルールに従って実行されます (下記参照)。 デフォルト値: On
InspectHttp <i>{On / Off}</i>	HTTPプロトコルを介して転送されたデータをスキャンするかどうかを指示します。 実際のデータスキャンは、指定されたスキャンルールに従って実行されます (下記参照)。 デフォルト値: On
InspectSmtpt <i>{On / Off}</i>	SMTPプロトコルを介して転送されたデータをスキャンするかどうかを指示します (インストールされている場合は、 Dr.Web MailD が使用されます)。



	<p>実際のデータスキャンは、指定されたスキャンルールに従って実行されます(下記参照)。</p> <p>デフォルト値: On</p>
InspectPop3 {On / Off}	<p>POP3プロトコルを介して転送されたデータをスキャンするかどうかを指示します(インストールされている場合は、Dr.Web MailDが使用されます)。</p> <p>実際のデータスキャンは、指定されたスキャンルールに従って実行されます(下記参照)。</p> <p>デフォルト値: On</p>
InspectImap {On / Off}	<p>IMAPプロトコルを介して転送されたデータをスキャンするかどうかを指示します(インストールされている場合は、Dr.Web MailDが使用されます)。</p> <p>実際のデータスキャンは、指定されたスキャンルールに従って実行されます(下記参照)。</p> <p>デフォルト値: On</p>
AutoconfigureIptables {Yes / No}	<p>iptablesインターフェースを介してNetFilterシステムコンポーネントを設定するためのルール。</p> <p>使用可能な値:</p> <ul style="list-style-type: none">• Yes - コンポーネントを起動するときにNetFilterのルールを設定し、動作を自動的に終了するときにルールを削除します(推奨)。• No - ルールの自動設定を実行しません。必要なルールは、コンポーネントを起動する前に管理者が手動で追加し、動作が完了した後に削除する必要があります。 <div><p>iptablesのルールの自動設定が許可されていない場合は、iptablesに必要なルールがコンポーネント動作開始前に利用できるようになっている必要があります。</p></div> <p>デフォルト値: Yes</p>
AutoconfigureRouting {Yes / No}	<p>ip routeとip ruleのルーティングルールとポリシーの設定モード。</p> <p>使用可能な値:</p> <ul style="list-style-type: none">• Yes - コンポーネントを起動するときにip routeとip ruleのルーティングルールとポリシーを設定し、動作を自動的に終了するときにルールを削除します(推奨)。• No - ルールの自動設定を実行しません。必要なルールは、コンポーネントを起動する前に管理者が手動で追加し、動作が完了した後に削除する必要があります。






	<div><p>ルーティングルールとポリシーの自動設定が許可されていない場合は、ip routeとip ruleに必要なルールがコンポーネント動作開始前に利用できるようになっている必要があります。</p></div> <p>デフォルト値 : Yes</p>
LocalDeliveryMark {integer / Auto}	<p>接続を監視するためにDr.Web Firewall for Linuxネットワークソケット(TproxyListenAddressパラメータで指定、下記参照)にリダイレクトされるパケットの<LDM>マーク。</p> <p>使用可能な値 :</p> <ul style="list-style-type: none">• <integer> - パケットの<LDM>マーク。2^Nに等しく、Nがパケット内のLDMビット数の場合、0 ≤ N ≤ 31。• Auto - Dr.Web Firewall for Linuxはパケットマークの適切なビット数を自動的に選択できます(推奨)。 <div><p><LDM>番号を手動で割り当てるときは、(NetFilter経路を含む)ルート接続とパケットを管理する他のアプリケーションが、パケットマークで対応するビット数を使用していないことを確認してください。無効な値を指定した場合、コンポーネントの起動は失敗します。</p><p>AutoconfigureIptables = No、AutoconfigureRouting = Noの場合、指定された<LDM>番号を手動で追加する必要があるルーティングルールで使用してください。</p></div> <p>デフォルト値 : Auto</p>
ClientPacketsMark {integer / Auto}	<p>接続を開始するクライアントとDr.Web Firewall for Linuxの間で転送されるパケットの<CPM>マーク。</p> <p>使用可能な値 :</p> <ul style="list-style-type: none">• <integer> - パケットの<CPM>マーク。2^Nに等しく、Nがパケット内のCPMビット数の場合、0 ≤ N ≤ 31。• Auto - Dr.Web Firewall for Linuxはパケットマークの適切なビット数を自動的に選択できます(推奨)。



	<div><p><CPM>番号を手動で割り当てるときは、(NetFilter経由を含む)ルート接続とパケットを管理する他のアプリケーションが、パケットマークで、対応するビット数を使用していないことを確認してください。無効な値を指定した場合、コンポーネントの起動は失敗します。</p><p>AutoconfigureIptables = Noの場合、指定された<CPM>番号を手動で追加する必要があるルーティングルールで使用する必要があります。</p></div> <p>デフォルト値: Auto</p>
ServerPacketsMark {integer / Auto}	<p>Dr.Web Firewall for Linuxと接続を受信するサーバーの間で転送されるパケットの<SPM>マーク。</p> <p>使用可能な値:</p> <ul style="list-style-type: none">• <integer> - パケットの<SPM>マーク。2^Nに等しく、Nがパケット内のSPMビット数の場合、0 ≤ N ≤ 31。• Auto - Dr.Web Firewall for Linuxはパケットマークの適切なビット数を自動的に選択できます(推奨)。 <div><p><SPM>番号を手動で割り当てるときは、(NetFilter経由を含む)ルート接続とパケットを管理する他のアプリケーションが、パケットマークで対応するビット数を使用していないことを確認してください。無効な値を指定した場合、コンポーネントの起動は失敗します。</p><p>AutoconfigureIptables = No、AutoconfigureRouting = Noの場合、指定された<SPM>番号は手動で追加する必要があるルーティングルールで使用する必要があります。</p></div> <p>デフォルト値: Auto</p>
TproxyListenAddress {network socket}	<p>Dr.Web Firewall for Linuxが監視した接続を受信するネットワークソケット(<IP address>: <port>)。ポート0を指定すると、システムによって自動的に選択されます。</p>



	<div><p>該当するソケットが他のアプリケーションによって使用されていないことを確認する必要があります。無効な値を指定した場合、コンポーネントの起動は失敗します。</p><p>AutoconfigureIptables = Noの場合、指定されたIPアドレスとポートは手動で追加する必要があるルーティングルールで使用する必要があります。</p></div> <p>デフォルト値 : 127.0.0.1:0</p>
OutputDivertEnable {Yes / No}	<p>受信接続モード(つまりローカルホストに接続があるリモートのアプリケーションによって開始された接続)の監視。</p> <p>使用可能な値 :</p> <ul style="list-style-type: none">• Yes - 送信接続の監視と処理を行います。• No - 送信接続の監視と処理は行いません。 <div><p>この設定は、AutoconfigureIptables = Noの場合に手動で追加または削除されるルーティングルール番号5を追加または削除します。</p></div> <p>デフォルト値 : No</p>
OutputDivertNfqueueNumber {integer / Auto}	<p>Dr.Web Firewall for Linuxが送信接続を開始するSYNパッケージを取得するキュー番号 <i>NFQUEUE</i>。</p> <p>使用可能な値 :</p> <ul style="list-style-type: none">• <integer> - <i>NFQUEUE</i>で監視された送信接続のSYNパケットを監視するためのキュー番号 <ONum>。• Auto - Dr.Web Firewall for Linuxは適切なキュー番号を自動的に選択できます(推奨)。 <div><p><ONum>番号を手動で割り当てるときは、(NetFilterルール経由を含む)接続とパケットを管理する他のアプリケーションが、相応するキュー番号を使用していないことを確認してください。無効な値を指定した場合、コンポーネントの起動は失敗します。</p><p>AutoconfigureIptables = Noの場合、指定された<ONum>番号を手動で追加する必要があるルーティングルール番号5で使用する必要があります。</p></div>




	デフォルト値 : Auto
OutputDivertConnectTransparently <i>{Yes / No}</i>	<p>送信接続のために監視されたパケットの送信者(クライアント)のIPアドレスを使用して受信者(サーバー)に接続するためのエミュレーションモード。</p> <p>使用可能な値 :</p> <ul style="list-style-type: none">• Yes - 接続を監視するときに、自分の代わりに接続をリクエストしたクライアントのアドレスを使用してサーバーに接続します• No - Dr.Web Firewall for Linuxアドレスからサーバーに接続します。 <p>クライアントとDr.Web Firewall for Linuxアドレスは通常、送信接続監視モードでは同じであるため、デフォルト値はNoになります。</p> <p>デフォルト値 : No</p>
InputDivertEnable <i>{Yes / No}</i>	<p>受信接続モード(つまりローカルホストに接続があるリモートホストのアプリケーションによって開始された接続)の監視。</p> <p>使用可能な値 :</p> <ul style="list-style-type: none">• Yes - 受信接続の監視と処理を行います。• No - 受信接続の監視と処理を行いません。 <div><p>この設定は、AutoconfigureIptables = Noの場合に手動で追加または削除されるルーティングルール番号6を追加または削除します。無効な値を指定した場合、コンポーネントの起動は失敗します。</p></div> <p>デフォルト値 : No</p>
InputDivertNfqueueNumber <i>{integer / Auto}</i>	<p>Dr.Web Firewall for Linuxが受信接続を開始するSYNパケットを取得するキュー番号 <i>NFQUEUE</i>。</p> <p>使用可能な値 :</p> <ul style="list-style-type: none">• <integer> - <i>NFQUEUE</i>で監視された送信接続のSYNパケットを監視するためのキュー番号 <INum>。• Auto - Dr.Web Firewall for Linuxは適切なキュー番号を自動的に選択できます(推奨)。



	<div><p><INum>番号を手動で割り当てるときは、(NetFilterルール経由を含む)接続とパケットを管理する他のアプリケーションが、相応するキュー番号を使用していないことを確認してください。無効な値を指定した場合、コンポーネントの起動は失敗します。</p><p>AutoconfigureIptables = Noの場合、指定された<INum>番号を手動で追加する必要があるルーティングルール番号6で使用する必要があります。</p></div> <p>デフォルト値: Auto</p>
InputDivertConnectTransparently {Yes / No}	<p>受信接続のために監視されたパケットの送信者(クライアント)のIPアドレスを使用して受信者(サーバー)に接続するためのエミュレーションモード。</p> <p>使用可能な値:</p> <ul style="list-style-type: none">• Yes - 接続を監視するときに、自分の代わりに接続をリクエストしたクライアントのアドレスを使用してサーバーに接続します• No - Dr.Web Firewall for Linuxアドレスからサーバーに接続します。 <p>受信接続監視モードでは、すべてのトラフィックがDr.Web Firewall for Linuxを通過するため、不正なクライアントのアドレスを使用してサーバーに安全に接続する可能性があります。これがデフォルト値がYesである理由です。</p> <p>デフォルト値: Yes</p>
ForwardDivertEnable {Yes / No}	<p>トランジット接続モード(つまりその他のリモートホストに接続があるリモートホストのアプリケーションによって開始された接続)の監視。</p> <p>使用可能な値:</p> <ul style="list-style-type: none">• Yes - トランジット接続の監視と処理を行います。• No - トランジット接続の監視と処理は行いません。 <div><p>この設定は、AutoconfigureIptables = Noの場合に手動で追加または削除されるルーティングルール番号7を追加または削除します。</p></div> <p>デフォルト値: No</p>
ForwardDivertNfqueueNumber	<p>Dr.Web Firewall for Linuxがトランジット接続を開始するSYNパケットを取得するキュー番号 <i>NFQUEUE</i>。</p>



<p><i>{integer / Auto}</i></p>	<p>使用可能な値:</p> <ul style="list-style-type: none">• <code><integer></code> - <i>NFQUEUE</i>で監視されたトランジット接続のSYNパケットを監視するためのキュー番号 <code><FNum></code>。• <code>Auto</code> - Dr.Web Firewall for Linuxは適切なキュー番号を自動的に選択できます (推奨)。 <div data-bbox="828 454 1436 889"><p><code><FNum></code>番号を手動で割り当てるときは、(NetFilterルール経由を含む)接続とパケットを管理する他のアプリケーションが、相応するキュー番号を使用していないことを確認してください。無効な値を指定した場合、コンポーネントの起動は失敗します。</p><p>AutoconfigureIptables = <code>No</code>の場合、指定された <code><FNum></code>番号を手動で追加する必要があるルーティング <u>ルール</u>番号7で使用してください。</p></div> <p>デフォルト値: <code>Auto</code></p>
<p>ForwardDivertConnectTransparently</p> <p><i>{Yes / No}</i></p>	<p>トランジット接続のために監視されたパケットの送信者 (クライアント) のIPアドレスを使用して受信者 (サーバー) に接続するためのエミュレーションモード。</p> <p>使用可能な値:</p> <ul style="list-style-type: none">• <code>Yes</code> - 接続を監視するときに、自分の代わりに接続をリクエストしたクライアントのアドレスを使用してサーバーに接続します• <code>No</code> - Dr.Web Firewall for Linuxアドレスからサーバーに接続します。 <p>トランジット接続監視モードでは、すべてのトラフィックが <i>Dr.Web Firewall for Linux</i>がインストールされているのと同じホスト (ルーター) を通過するという保証はないため、正しい動作のデフォルト値は <code>No</code> になります。保護されたアプリケーションが同じルーターを使用することがネットワーク設定によって保証されている場合、このパラメータを <code>Yes</code> に設定できます。この場合は、<i>Dr.Web Firewall for Linux</i> がサーバーに接続するときは常にクライアントのアドレスへの接続を評価します。</p> <p>デフォルト値: <code>No</code></p>
<p>ExcludedProc</p> <p><i>{path to file}</i></p>	<p>プロセスのホワイトリストとして使用することができるプロセスのリスト、つまりネットワーク活動を監視してはならないプロセスのリスト。</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：プロセスのリストにwgetとcurl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>[LinuxFirewall] 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>[LinuxFirewall] ExcludedProc = /usr/bin/wget ExcludedProc = /usr/bin/curl</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 LinuxFirewall.ExcludedProc - a /usr/bin/wget # drweb-ctl cfset LinuxFirewall.ExcludedProc - a /usr/bin/curl</pre> <div><p>このパラメータで示されるプロセスリストの実際の使用方法は、Dr.Web Firewall for Linuxに定義されているスキャンルールでの使用方法によって決まります。</p><p>デフォルトルール（以下参照）は、リストからの全プロセスのトラフィックがスキャンせずに許可されることを保証します。</p></div> <p>デフォルト値：（未設定）</p>
UnwrapSsl <i>{Boolean}</i>	<p>SSL/TLS接続を介して転送された暗号化トラフィックをスキャンするように指示します。</p>



	<div><p>最近の実行例では、この変数の値は保護されたトラフィックの処理に影響しません。処理を管理するには、SET Unwrap_SSL = true/falseアクションを含むルールを作成する必要があります(以下参照)。</p><p>drweb-ctlユーティリティのcfsetコマンドまたはWebインターフェースを使用してこのパラメータの値を変更した場合、影響を受ける依存ルールが自動的に適用されます。</p></div> <p>デフォルト値 : No</p>
BlockInfectionSource <i>{Boolean}</i>	<p>悪意のあるソフトウェア (<i>InfectionSource</i>カテゴリーに含まれる)を含むWebサイトへの接続試行をブロックするように指示します。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります(下記の詳細を参照)。</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : Yes</p>
BlockNotRecommended <i>{Boolean}</i>	<p>非推奨サイト (<i>NotRecommended</i>カテゴリーに含まれる)への接続試行をブロックするように指示します。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります(下記の詳細を参照)。</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : Yes</p>
BlockAdultContent <i>{Boolean}</i>	<p>アダルトコンテンツ (<i>AdultContent</i>カテゴリーに含まれる)を含むWebサイトへの接続試行をブロックするように指示します。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります(下記の詳細を参照)。</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : No</p>



BlockViolence <i>{Boolean}</i>	<p>暴力的描写 (<i>Violence</i> カテゴリーに含まれる) を含む Web サイトへの接続試行をブロックするように指示します。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります(下記の詳細を参照)。</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : No</p>
BlockWeapons <i>{Boolean}</i>	<p>武器に関する Web サイト (<i>Weapons</i> カテゴリーに含まれる) への接続試行をブロックするように指示します。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります(下記の詳細を参照)。</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : No</p>
BlockGambling <i>{Boolean}</i>	<p>ギャンブルの Web サイト (<i>Gambling</i> カテゴリーに含まれる) への接続試行をブロックするように指示します。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります(下記の詳細を参照)。</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : No</p>
BlockDrugs <i>{Boolean}</i>	<p>麻薬に関する Web サイト (<i>Drugs</i> カテゴリーに含まれる) への接続試行をブロックするように指示します。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります(下記の詳細を参照)。</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : No</p>
BlockObsceneLanguage <i>{Boolean}</i>	<p>卑猥な表現 (<i>ObsceneLanguage</i> カテゴリーに含まれる) を含む Web サイトへの接続試行をブロックするように指示します。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります(下記の詳細を参照)。</p>



	<pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : No</p>
BlockChats <i>{Boolean}</i>	<p>チャットWebサイト (<i>Chats</i> カテゴリに含まれる) への接続試行をブロックするように指示します。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります(下記の詳細を参照)。</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : No</p>
BlockTerrorism <i>{Boolean}</i>	<p>テロリズムに関するWebサイト (<i>Terrorism</i> カテゴリに含まれる) への接続試行をブロックするように指示します。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります(下記の詳細を参照)。</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : No</p>
BlockFreeEmail <i>{Boolean}</i>	<p>無料メールサービスのWebサイト (<i>FreeEmail</i> カテゴリに含まれる) への接続試行をブロックするように指示します。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります(下記の詳細を参照)。</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : No</p>
BlockSocialNetworks <i>{Boolean}</i>	<p>ソーシャルネットワーキングサイト (<i>SocialNetworks</i> カテゴリに含まれる) への接続試行をブロックするように指示します。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります(下記の詳細を参照)。</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : No</p>



BlockDueToCopyrightNotice <i>{Boolean}</i>	<p>著作権者のリクエストに従って追加されたWebサイト (<i>DueToCopyrightNotice</i>カテゴリーに含まれる)への接続試行をブロックするように指示します。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります(下記の詳細を参照)。</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : Yes</p>
BlockOnlineGames <i>{Boolean}</i>	<p>オンラインゲームWebサイト (<i>OnlineGames</i>カテゴリーに含まれる)への接続試行をブロックするように指示します。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります(下記の詳細を参照)。</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : No</p>
BlockAnonymizers <i>{Boolean}</i>	<p>アノマイザーWebサイト (<i>Anonymizers</i>カテゴリーに含まれる)への接続試行をブロックするように指示します。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります(下記の詳細を参照)。</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : No</p>
BlockCryptocurrencyMiningPools <i>{Boolean}</i>	<p>仮想通貨マイニングのための一般的なサービスへのアクセスを提供するWebサイト (<i>CryptocurrencyMiningPool</i>カテゴリーに含まれる)への接続試行をブロックするように指示します。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります(下記の詳細を参照)。</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : No</p>
BlockJobs <i>{Boolean}</i>	<p>求人検索Webサイト (求人カテゴリーに含まれます)への接続試行をブロックするように指示します。</p>



	<p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります(下記の詳細を参照)。</p> <pre>url_category in "LinuxFirewall.BlockCategory" : Block as _match</pre> <p>デフォルト値 : No</p>
<p>Whitelist</p> <p><i>{domain list}</i></p>	<p>ホワイトリストとして使用できるドメインのリスト(つまり、これらのドメインがブロックされたカテゴリーに含まれている場合でも、ユーザーの接続が許可されているドメインのリスト。さらに、このリストに示されているドメインのすべてのサブドメインへユーザーがアクセスすることが許可されます)。</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 : ドメインexample.comとexample.netのリストに追加します。</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>[LinuxFirewall] Whitelist = "example.com", "example.net"</pre><ul style="list-style-type: none">2つの文字列(文字列ごとに1つの値)<pre>[LinuxFirewall] Whitelist = example.com Whitelist = example.net</pre>コマンド drweb-ctl cfsetを使用して値を追加します。 <pre># drweb-ctl cfset LinuxFirewall.Whitelist -a example.com # drweb-ctl cfset LinuxFirewall.Whitelist -a example.net</pre>



	<div><p>このパラメータで示されるドメインリストの実際の使用方法は、Dr.Web Firewall for Linuxに定義されているスキャンルールでの使用方法によって決まります。</p><p>デフォルトルールのリスト(下記参照)は、ブロックされるWebソースカテゴリーのリストのドメインがこのリストに含まれている場合でも、このリストのドメイン(およびそのサブドメイン)へのアクセスが提供されることを保証します(ただしHTTPプロトコルを経由したサーバーへのリクエストの場合のみ)。さらに、このデフォルトのルールセットは、ホワイトリストドメインからダウンロードしたデータが脅威に対してスキャンされることを保証します(データはレスポンスで返され、変数directionには値responseがあるため)。</p></div> <p>デフォルト値: (未設定)</p>
Blacklist <i>{domain list}</i>	<p>ブラックリストとして使用できるドメインのリスト(つまり、これらのドメインがブロックされたカテゴリーに含まれていない場合でも、ユーザーの接続が禁止されているドメインのリスト。さらに、このリストに示されているドメインのすべてのサブドメインへユーザーがアクセスすることが禁止されます)。</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: ドメインexample.comとexample.netのリストに追加します。</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<div><pre>[LinuxFirewall] Blacklist = "example.com", "example.net"</pre></div>2つの文字列(文字列ごとに1つの値)<div><pre>[LinuxFirewall] Blacklist = example.com Blacklist = example.net</pre></div>コマンドdrweb-ctl cfsetを使用して値を追加します。



	<pre># drweb-ctl cfset LinuxFirewall.Blacklist -a example.com # drweb-ctl cfset LinuxFirewall.Blacklist -a example.net</pre> <div><p>このパラメータで示されるドメインリストの実際の使用方法は、Dr.Web Firewall for Linuxに定義されているスキャンルールでの使用方法によって決まります。</p><p>デフォルトルールの一覧(以下参照)は、このリストのドメイン(およびそのサブドメイン)へのアクセスがHTTPプロトコル上で常に禁止されることを保証します。このドメインがホワイトリストとブラックリストに同時に追加される場合、デフォルトのルールにより、そのドメインへのユーザーアクセスは確実にブロックされます。</p></div> <p>デフォルト値: (未設定)</p>
ScanTimeout <i>{time interval}</i>	<p>SpIDer Gate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>
HeuristicAnalysis <i>{On / Off}</i>	<p>SpIDer Gate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。</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、BlockSuspicious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>
PackerMaxLevel <i>{integer}</i>	<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 Gate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>
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。SpIDer Gate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>
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。SpIDer Gate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>
ContainerMaxLevel <i>{integer}</i>	<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 Gate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>
MaxCompressionRatio <i>{integer}</i>	<p>圧縮/パックされた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)。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 Gateによって開始されたファイル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>
BlockKnownVirus <i>{Boolean}</i>	<p>データに既知の脅威が含まれる場合、そのデータの受信または送信をブロックするように指示します。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります (下記の詳細を参照)。</p> <div><pre>threat_category in "LinuxFirewall.BlockThreat" : Block as _match</pre></div> <p>デフォルト値 : Yes</p>
BlockSuspicious <i>{Boolean}</i>	<p>データに未知の脅威 (ヒューリスティックアナライザによって検出されたもの) が含まれる場合、そのデータの受信または送信をブロックするように指示します。</p>



	<p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります(下記の詳細を参照)。</p> <pre>threat_category in "LinuxFirewall.BlockThreat" : Block as _match</pre> <p>デフォルト値 : Yes</p>
BlockAdware <i>{Boolean}</i>	<p>データにアドウェアが含まれる場合、そのデータの受信または送信をブロックするように指示します。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります(下記の詳細を参照)。</p> <pre>threat_category in "LinuxFirewall.BlockThreat" : Block as _match</pre> <p>デフォルト値 : Yes</p>
BlockDialers <i>{Boolean}</i>	<p>データにダイヤラープログラムが含まれる場合、そのデータの受信または送信をブロックするように指示します。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります(下記の詳細を参照)。</p> <pre>threat_category in "LinuxFirewall.BlockThreat" : Block as _match</pre> <p>デフォルト値 : Yes</p>
BlockJokes <i>{Boolean}</i>	<p>データにジョークプログラムが含まれる場合、そのデータの受信または送信をブロックするように指示します。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります(下記の詳細を参照)。</p> <pre>threat_category in "LinuxFirewall.BlockThreat" : Block as _match</pre> <p>デフォルト値 : No</p>
BlockRiskware <i>{Boolean}</i>	<p>データにリスクウェアが含まれる場合、そのデータの受信または送信をブロックするように指示します。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります(下記の詳細を参照)。</p> <pre>threat_category in "LinuxFirewall.BlockThreat" : Block as _match</pre>



	デフォルト値 : No
BlockHacktools <i>{Boolean}</i>	<p>データにハッキングツールが含まれる場合、そのデータの受信または送信をブロックするように指示します。</p> <p>ブロックをアクティブにするには、次のルールを設定に追加する必要があります(下記の詳細を参照)。</p> <pre>threat_category in "LinuxFirewall.BlockThreat" : Block as _match</pre>
	デフォルト値 : No
BlockUnchecked <i>{Boolean}</i>	<p>データがスキャンできない場合、そのデータの受信または送信をブロックするように指示します。</p> <div><p>このパラメータ値は、エラーのためにtrueまたはfalseに評価することが不可能なルールの処理に影響します。Noを指定した場合、ルールは実行されていないルールとしてスキップされます。Yesを指定した場合、Block as BlackListアクションが実行されます。</p></div>
	デフォルト値 : No
InterceptHook <i>{path to file / Lua function}</i>	<p>Luaで接続を処理するためのスクリプトまたはそのスクリプトを含むファイルへのパス(Luaでの接続処理セクションを参照)。</p> <p>使用できないファイルを指定すると、コンポーネントを読み込む際にエラーが表示されます。</p> <p>デフォルト値 :</p> <pre>local dwl = require 'drweb.lookup' function intercept_hook(ctx) -- do not check if group == Root.TrustedGroup if ctx.divert == "output" and ctx.group == "drweb" then return "pass" end -- do not check connections from privileged ports -- except FTP active mode if ctx.src.port >= 0 and ctx.src.port <= 1024 and ctx.src.port ~= 20 then return "pass"</pre>



```
end

return "check"

end
```



接続スキャンの設定を変更しても、変更を加える前にアプリケーションによってすでに確立されている接続のスキャンには影響しません。それらをすでに実行中のアプリケーションに適用する必要がある場合は、アプリケーションを再起動するなどして、アプリケーションを強制的に切断してから再度接続する必要があります。

トラフィックモニタリングとアクセスブロックのルール

このセクションには、上のパラメータの他、11個のルールセット**RuleSet*** (**RuleSet0**、...、**RuleSet10**)も含まれます。これらは、トラフィックスキャン、Webリソースへのユーザーアクセスのブロック、インターネットからのコンテンツのダウンロードのブロックを直接管理します。条件の一部の値 (IPアドレス範囲、Webサイトカテゴリーのリスト、Webソースのブラックリストとホワイトリストなど) については、テキストファイルからロードされる値の置き換えがあり、LDAPを介して外部データソースから抽出されます ([Dr.Web LookupD](#)コンポーネントを使用)。接続を設定する際には、最終的な解決を含むルールが見つかるまで、すべてのルールが昇順で検査されます。ルールリストのギャップは無視されます。

ルールを表示して編集する

ルールリストを簡単に編集するためにブランクのものが残されています。つまり、ルールが指定されていない **RuleSet** <i> </i> があります (<i> - RuleSetルールセット番号)。RuleSet <i> </i> 以外の項目を追加することはできませんRuleSet <i> </i> の要素内のルールは追加および削除できます。ルールの表示と編集は、次のいずれかの方法で実行できます。

- (任意のテキストエディターで) [設定ファイル](#) 設定ファイルを表示、編集する (このファイルにはデフォルトと異なるパラメータのみが保存されます)。
- [Web管理インターフェース](#) 経由 (インストールされている場合)。
- コマンドラインベースのインターフェースを介して - [Dr.Web Ctl](#) (**drweb-ctl cfshow** および **drweb-ctl cfset** [コマンド](#))。



ルールを編集して設定ファイルを変更した場合は、これらの変更を適用するためにDr.Web for UNIX Mail Serversを再起動します。それには、**drweb-ctl reload** コマンドを使用します。

コマンド**drweb-ctl cfshow**を使用してルールを表示します。

ルールセット**LinuxFirewall.RuleSet1**のコンテンツを表示するには、このコマンドを使用します。

```
# drweb-ctl cfshow LinuxFirewall.RuleSet1
```

drweb-ctl cfset コマンドを使用してルールを編集します (以降、<i>rule</i> - ルールのテキスト)。

- **LinuxFirewall.RuleSet1** セットのすべてのルールを新しいルールで置き換えます。

```
# drweb-ctl cfset LinuxFirewall.RuleSet1 ' <i>rule</i> '
```



- **LinuxFirewall.RuleSet1**ルールセットに新しいルールを次のように追加します。

```
# drweb-ctl cfset -a LinuxFirewall.RuleSet1 '<rule>'
```

- **LinuxFirewall.RuleSet1**セットから特定のルールを次のように削除します。

```
# drweb-ctl cfset -e LinuxFirewall.RuleSet1 '<rule>'
```

- **LinuxFirewall.RuleSet1**ルールセットを次のようにデフォルトの状態にリセットします。

```
# drweb-ctl cfset -r LinuxFirewall.RuleSet1
```

drweb-ctlツールを使用してルールのリストを編集するときは、追加するルールのテキストを一重引用符または二重引用符で囲み、ルールのテキスト内にある二重引用符の前にはバックスラッシュ(「\」)をエスケープ文字として使用します(ルール自体のテキストに二重引用符が含まれている場合)。

設定の**RuleSet** <i>/>変数には、ルールの格納について次のような特徴があります。

- 無条件ルールを追加するときは、条件部分とコロンを省略できます。ただし、そのようなルールは常にルールのリストに文字列「 : <action>」として格納されます。
- 複数のアクションを含むルール(「 <condition> : <action 1>, <action 2>」など)を追加すると、そのようなルールは基本ルールのチェーン「 <condition> : <action 1>」と「 <condition> : <action 2>」に変更されます。
- ロギングまたはルールは、条件部分で条件の離接(論理和)を許可しないため、論理和を実装するには、各ルールに離接語条件がある条件で一連のルールを記録する必要があります。

接続をスキップするための無条件ルール(Passアクション)を**LinuxFirewallRuleSet1**セットに追加するには、次のコマンドのみを実行します。

```
# drweb-ctl cfset -a LinuxFirewall.RuleSet1 'Pass'
```

ただし、指定したルールセットからこのルールを削除するには、次のコマンドを実行する必要があります。

```
# drweb-ctl cfset -e LinuxFirewall.RuleSet1 ' : Pass'
```

LinuxFirewall.RuleSet1ルールを、接続用の標準テンプレートへのパスを未解決アドレスから変更してブロックを実行するルールセットに追加するには、次のコマンドを実行する必要があります。

```
# drweb-ctl cfset -a LinuxFirewall.RuleSet1 'src_ip not in  
file("/etc/trusted_ip") : set http_template_dir = "mytemplates", Block'
```

ただし、このコマンドでは指定したセットに2つのルールが追加されるため、ルールのセットからこれらのルールを削除するには、次の2つのコマンドを実行する必要があります。

```
# drweb-ctl cfset -e LinuxFirewall.RuleSet1 'src_ip not in  
file("/etc/trusted_ip") : set http_template_dir = "mytemplates"  
# drweb-ctl cfset -e LinuxFirewall.RuleSet1 'src_ip not in  
file("/etc/trusted_ip") : Block'
```



「悪意のあるオブジェクト*KnownVirus*やテロリズムカテゴリーからのURLが検出された場合はブロックする」などのルールをLinuxFirewall.RuleSet1ルールセットに追加するには、このルールセットに次の2つのルールを追加する必要があります。

```
# drweb-ctl cfset -a LinuxFirewall.RuleSet1 'threat_category in (KnownVirus)
: Block as _match'
# drweb-ctl cfset -a LinuxFirewall.RuleSet1 'url_category in (Terrorism) :
Block as _match'
```

ルールのセットからこれらのルールを削除する場合にも、2つのコマンドを実行する必要があります（上の例を参照）。

デフォルトのルールセット

デフォルトでは、次のブロックルールセットが指定されています。

```
RuleSet0 =
RuleSet1 = divert output : set HttpTemplatesDir = "output"
RuleSet1 = divert output : set MailTemplatesDir = "firewall"
RuleSet1 = divert input : set HttpTemplatesDir = "input"
RuleSet1 = divert input : set MailTemplatesDir = "server"
RuleSet1 = proc in "LinuxFirewall.ExcludedProc" : Pass
RuleSet1 = : set Unwrap_SSL = false
RuleSet2 =
RuleSet3 =
RuleSet4 =
RuleSet5 = protocol in (Http), direction request, url_host in
"LinuxFirewall.Blacklist" : Block as BlackList
RuleSet5 = protocol in (Http), direction request, url_host in
"LinuxFirewall.Whitelist" : Pass
RuleSet6 =
RuleSet7 = protocol in (Http), direction request, url_category in
"LinuxFirewall.BlockCategory" : Block as _match
RuleSet8 =
RuleSet9 = protocol in (Http), divert input, direction request,
threat_category in "LinuxFirewall.BlockThreat" : Block as _match
RuleSet9 = protocol in (Http), direction response, threat_category in
"LinuxFirewall.BlockThreat" : Block as _match
RuleSet9 = protocol in (Smtplib), threat_category in
"LinuxFirewall.BlockThreat" : REJECT
RuleSet9 = protocol in (Smtplib), url_category in "LinuxFirewall.BlockCategory"
: REJECT
RuleSet9 = protocol in (Smtplib), total_spam_score gt 0.80 : REJECT
RuleSet9 = protocol in (Pop3, Imap), threat_category in
"LinuxFirewall.BlockThreat" : REPACK as _match
RuleSet9 = protocol in (Pop3, Imap), url_category in
"LinuxFirewall.BlockCategory" : REPACK as _match
RuleSet9 = protocol in (Pop3, Imap), total_spam_score gt 0.80 : REPACK as
_match
RuleSet10 =
```

最初のルールは、**ExcludedProc**パラメータ（上を参照）で指定されたプロセスによって接続が確立された場合、他の条件を検査せずに接続をスキップすることを示します。次のルール（条件なしで実行されます）は保護された接続のラップ解除をブロックします。このルールとその下位にあるすべてのルールは、接続が除外されたプロ



セスで設定されていない場合にのみ考慮されます。また、後続のすべてのルールはプロトコルに依存するため、保護された接続のラップ解除が無効になっている場合は、条件がtrueと評価されるかどうかを定義できないため、ルールは実行されません。

次のルールは、デフォルトのルールセットにおけるHTTP接続に対する処理の内容です。

1. 接続が確立されたホストがブラックリストに含まれている場合、そのホストがブラックリストに含まれているため、接続はブロックされます。他のスキャンは実行されません。
2. ホストがホワイトリストに含まれている場合、接続はスキップされ、他のスキャンは実行されません。
3. クライアントからリクエストされたURLが、アクセスが望ましくないとマークされているWebリソースのカテゴリに含まれている場合は、脅威が検出されたために接続がブロックされます。他のスキャンは実行されません。
4. HTTP経由の脅威があるリモートホストから受信したレスポンスに、ブロックされたカテゴリに属する脅威が含まれる場合、その脅威が検出されたために接続がブロックされます。他のスキャンは実行されません。
5. ローカルホストからリモートホストに移行したデータに、ブロックされたカテゴリに属する脅威が含まれる場合、その脅威が検出されたために接続がブロックされます。他のスキャンは実行されません。

この5つのルールは、**InspectHttp**パラメータでオンが指定されている場合にのみ機能します。それ以外の場合、これらのルールはどれも機能しません。

RuleSet9で指定される次の6つのルールは、メールプロトコルを介して送受信されるデータのスキャンを管理します。これらのルールは、送信されたメール(SMTP、POP3、またはIMAPプロトコル経由)に、スパムとしてブロックまたは分類する必要があるカテゴリに属する添付ファイルまたはURLが含まれていることが検出された場合に有効になります(Dr.Web ASEパーセンテージは0.8以上)。メールがSMTPプロトコルを介して送信される場合、メールの伝送(つまり送信または受信)はブロックされますが、IMAPとPOP3プロトコルの場合は、メールはそのコンテンツから悪意のあるコンテンツを除去するために処理(「再パッケージング」)されます。



メールのスパムの兆候をスキャンするためのコンポーネントであるDr.Web Anti-Spamが使用できない場合、スパムの兆候をスキャンするためのメールスキャンは実行されません。この場合、スパムレベルのスキャン(値 `total_spam_score`)を含むルールは使用できません。

メール処理ルールは、相応する**Inspect <EmailProtocol>**パラメータに**On**が指定されている場合にのみ実行されることに注意してください。それ以外の場合、これらのルールはどれも実行されません。さらに、送信されたメールのマルウェアの添付ファイルを調べるためにメールスキャン用のDr.Web MailDコンポーネントをインストールする必要があります。コンポーネントがインストールされていない場合、「検査できません」というエラーのため、送信されたメールはブロックされます。検査できないメッセージの送信を許可するには、**BlockUnchecked = No**パラメータを設定します(上記を参照)。また、メールスキャンコンポーネントがインストールされていない場合は、**InspectSmtп**、**InspectPop3**、**InspectImap**パラメータに**No**を指定することをお勧めします。

トラフィックモニタリングとアクセスブロックのルールの例

1. IPアドレス範囲が10.10.0.0~10.10.0.254のユーザーにChats以外のすべてのカテゴリのWebサイトへのHTTPアクセスを許可する。

```
protocol in (HTTP), src_ip in (10.10.0.0/24), url_category not in (Chats)
: Pass
```

ルール

```
protocol in (HTTP), url_host in "LinuxFirewall.Blacklist" : Block as
BlackList
```




が、指定されたルールより上のルールリストに割り当てられている場合、IPアドレス範囲が10.10.0.0～10.10.0.254のユーザーは、ブラックリストのドメイン、つまりパラメータLinuxFirewall.Blacklistにリストされているドメインへのアクセスもブロックされます。また、このルールが下に割り当てられている場合、IPアドレス範囲が10.10.0.0～10.10.0.254のユーザーは、ブラックリストのWebサイトにもアクセスできます。

解決Passは最終的なものであるため、これ以上のルールはチェックされず、したがってダウンロードされたデータのウイルススキャンも実行されません。IPアドレス範囲が10.10.0.0～10.10.0.254のユーザーに、ブラックリストに含まれていないChats以外のすべてのカテゴリーのWebサイトへのアクセスを許可し、同時に脅威のダウンロードをブロックするには、次のルールを使用します。

```
protocol in (HTTP), url_category not in (Chats), url_host not in
"LinuxFirewall.Blacklist", threat_category not in
"LinuxFirewall.BlockCategory" : Pass
```

2. インターネットからダウンロードしたビデオファイルのコンテンツ(つまり、MIMEタイプが「video/*」のデータ(*はMIMEクラスvideoの任意のタイプ))のスキャンを実行しない。

```
direction response, content_type in ("video/*") : Pass
```

ローカルコンピューターから読み込んだファイル(MIMEタイプが「video/*」のファイルを含む)は、レスポンスではなくリクエストで送信されるため(つまり変数directionには値requestがあるため)にスキャンされません。

Luaでの接続処理

このセクションの内容:

- [概要](#)
- [接続処理のスクリプトにおける要件](#)
- [例](#)
- [使用中のテーブル](#)
- [利用可能な補助モジュール](#)

概要

Dr.Web Firewall for LinuxはLuaのプログラムインタプリタを介して対話をサポートします(バージョン5.3.4が使用され、Dr.Web for UNIX Mail Serversと一緒に提供されます)。Luaで書かれたスクリプトは、解析のためにSpIDer Gatelに送信される前に、事前接続スキャンのためにコンポーネントによって使用されます。

Dr.Web Firewall for Linux設定(InterceptHookパラメータ内)が次のパスで指定されている場合、Luaスクリプトを使用した接続解析が、接続スキャンのスクリプトを含む、Luaで書かれたファイルに実行されます。それ以外の場合は、コンポーネント設定で指定されているデフォルト設定と処理ルール(RuleSet*パラメータ)を使用して接続処理が実行されます。



接続処理用のLuaスクリプトのその他の例については、次のリンクからご確認ください。
<https://github.com/DoctorWebLtd/drweb-lua-examples/tree/master/firewall>。



接続処理のスクリプトにおける要件

このファイルには、接続スキャンモジュールのエントリポイントであるグローバル関数が含まれている必要があります（Dr.Web Firewall for Linuxは、新しく受信した接続を処理するためにこの関数を呼び出します）。処理関数は、次の呼び出し規則を満たす必要があります。

1. 関数名 - `intercept_hook`;
2. 引数は、Luaコンテキストテーブルのみです（処理された接続の関数からの情報へのアクセスを提供します。以下の表の説明を参照してください）。
3. 戻り値は、以下の表の文字列値のみです。

値	判定の説明
pass	SpIDer Gateによるスキャンを行わずに接続をスキップする
check	SpIDer Gateを使用して接続をスキャンする
drop	パケット損失で接続をブロックする
reject	接続を破棄する（接続を開始し、RSTフラグ付きのTCPパケットを受信するクライアント）

例

1. すべての接続について無条件にpass判定（スキップ）を返すLuaスクリプト。

```
-- Function of connection scanning written by the user
function intercept_hook(ctx)
    return "pass" -- do not scan the connection
end
```

2. Dr.Web Firewall for Linuxに対し、drwebグループのユーザー権限で実行されているアプリケーションからの送信ローカル接続、または（接続の所有者とその方向に関係なく）権限のあるポートから開始された接続、またはローカルネットワークからのIPアドレスから始まる接続を除く、確立された接続すべてをスキャンのために送信するように指示するスクリプト。



```
function intercept_hook(ctx)
  -- Do not scan connections, initiated from the local
  -- host (divert == "output") by application under the name of
  -- "drweb" (group == "[drweb]")
  if ctx.divert == "output" and ctx.group == "drweb" then
    return "pass"
  end

  -- Do not scan connections, initiated from
  -- privileged ports (range is from 0 to 1024)
  if ctx.src.port >= 0 and ctx.src.port <= 1024 then
    return "pass"
  end

  -- Do not scan connections from local network IP addresses
  -- (IP address range 127.0.0.1/8)
  if ctx.src.ip.belongs("127.0.0.0/8") then
    return "pass"
  end

  -- 接続はデフォルトでスキャンされます
  return "check"
end
```

使用中のテーブル

1. InterceptContextテーブル

このテーブルは、処理された接続のデータを`intercept_hook`関数に転送するために使用されます。データを使用して、接続をどうするかを決定できます（スキャンせずにスキップ、切断、またはSpIDer Gateによるスキャンのために送信）。Dr.Web Firewall for Linuxではテーブルにデータを入力します。テーブルのデータの中には、`intercept_hook`関数が実行される時点ですでに認識されているものがあります。他の情報（いわゆる「遅延」データ）は、テーブルの該当するフィールドのリクエストに応じて直接評価されます。テーブルには以下のフィールドを含みます。

フィールド	説明	データタイプ
src	接続を開始したクライアントのアドレスとポート 例： <pre>if ctx.src.port >= 0 and ctx.src.port <= 1024 then return "pass" end</pre>	TcpEndpoint テーブル
dst	クライアントによって接続が開始されたサーバーのアドレスとポート 例：	TcpEndpoint テーブル



フィールド	説明	データタイプ
	<pre>if ctx.dst.ip.belongs("10.20.30.41/8") then return "reject" end</pre>	
divert	<p>監視した接続のタイプ。以下のいずれかの値にできます。</p> <ul style="list-style-type: none">「output」 - 送信接続。「input」 - 受信接続。「forward」 - トランジット接続。 <p>例：</p> <pre>if ctx.divert == "forward" then return "check" end</pre>	文字列
iface_in	<p>接続元のインターフェース名。</p> <p>インターフェース名が定義されていない場合は、nil値になります。</p>	文字列
iface_out	<p>接続を初期化するパケットが送信されたインターフェース名。</p> <p>インターフェース名が定義されていない場合は、nil値になります。</p>	文字列
uid	<p>送信接続を開始したユーザーID。</p> <p>接続タイプ(divert)が「output」ではない場合、またはUIDを定義できない場合は、nil値になります。</p>	番号
gid	<p>送信接続を開始したグループID。</p> <p>接続タイプ(divert)が「output」ではない場合、またはGIDを定義できない場合は、nil値になります。</p>	番号
user	<p>送信接続を開始したユーザー名。</p> <p>接続タイプ(divert)が「output」ではない場合、またはユーザー名を定義できない場合は、nil値になります。</p>	文字列
group	<p>送信接続を開始したグループ名。</p> <p>接続タイプ(divert)が「output」ではない場合、またはユーザー名を定義できない場合は、nil値になります。</p>	文字列
pid	<p>送信接続を開始したプロセスID。</p> <p>接続タイプ(divert)が「output」ではない場合、またはPIDを定義できない場合は、nil値になります。</p>	番号
exe_path	<p>送信接続を開始したアプリケーションの実行可能ファイルへのパス。</p>	文字列



フィールド	説明	データタイプ
	接続タイプ(<code>divert</code>)が「 <code>output</code> 」ではない場合、または実行可能パスを定義できない場合は、 <code>nil</code> 値になります。	
無効になったメタメソッド: なし		

2. TcpEndpointテーブル

このテーブルは、接続ポイント(クライアントまたはサーバー)のアドレスを説明しています。以下のフィールドを含みます。

フィールド	説明	データタイプ
<code>ip</code>	IPアドレス	IpAddress テーブル
<code>port</code>	ポート番号	番号
無効になったメタメソッド:		
<ul style="list-style-type: none"><code>__tostring</code> - TcpEndpointを文字列に変換する関数。例: 「127. 0. 0. 1: 443」(IPv4)または「[: : 1]: 80」(IPv6)<code>__concat</code> - TcpEndpointを文字列に追加する関数		

利用可能な補助モジュール

LuaのプログラムスペースでDr.Web for UNIX Mail Serversとやり取りするために、次の特定のモジュールをインポートできます。

モジュール名	機能
drweb	Luaプログラムを起動したDr.Web for UNIX Mail ServersコンポーネントとLuaプロシージャの非同期実行の手段のログに、Luaプログラムからのメッセージを記録する機能を提供するモジュール
drweb.lookup	Dr.Web LookupDモジュールを呼び出して外部ソースからデータを要求するためのツールを提供するモジュール

drwebモジュールの内容

1. 機能

このモジュールは次の機能を提供します。

1.1. LuaプログラムからのメッセージをDr.Web for UNIX Mail Serversコンポーネントログに保存するための機能:

- `log(<level>, <message>)` は<message>文字列をDr.Web for UNIX Mail Serversログに<level>レベル(必要なレベルは、「`debug`」、「`info`」、「`notice`」、「`warning`」、「`error`」を使用して定義します)で書き込みます。
- `debug(<message>)` は<message>文字列をDr.Web for UNIX Mail Serversログに`DEBUG`レベルで書き込みます。



- `info(<message>)` は `<message>` 文字列をDr.Web for UNIX Mail Serversログに *INFO* レベルで書き込みます。
- `notice(<message>)` は `<message>` 文字列をDr.Web for UNIX Mail Serversログに *NOTICE* レベルで書き込みます。
- `warning(<message>)` は `<message>` 文字列をDr.Web for UNIX Mail Serversログに *WARNING* レベルで書き込みます。
- `error(<message>)` は `<message>` 文字列をDr.Web for UNIX Mail Serversログに *ERROR* レベルで書き込みます。

1.2. Luaプロシジャの同期管理のための機能:

- `sleep(<sec.>)` はこのLuaプロシジャインスタンスの実行を指定された秒数で一時停止します。
- `async(<Lua function>[, <argument list>])` は、指定された関数の非同期開始を起動し、指定された引数リストに転送します。`async`関数呼び出しはすぐに完了し、戻り値(**Future**テーブル)を使用すると、`<Lua function>`の結果を取得できます(まだ実行が完了していない場合は、完了するまで待機している可能性があります)。

1.3. IPアドレスを**IpAddress**テーブルとして表示するための機能:

- `ip(<address>)` は、**IpAddress**テーブルの形式で `<address>` 文字列として送信される、IPアドレスを指定します。IPv4またはIPv6アドレスのいずれかを使用できます。

1.4. テキストファイルから外部データをアップロードするには:

- `load_set(<file path>)` は、指定されたテキストファイルのコンテンツから `true` 値を含むテーブルを生成し、ファイルから読み取られた文字列はキーとして使用されます。空の文字列と空白文字のみで構成される文字列は無視され、テーブルには含まれません。
- `load_array(<file path>)` は、指定されたテキストファイルのコンテンツから文字列の配列を生成します。空の文字列と空白文字のみで構成される文字列は無視され、配列には含まれません。

2. テーブル

2.1. **Future**テーブルは、`async`関数を使用して関数を実行した後の保留中の結果を表します。テーブルには以下のフィールドを含みます。

フィールド	説明	データタイプ
<code>wait</code>	<code>async</code> 関数を使用して開始した関数の結果を返す関数。関数がまだ実行を完了していない場合は、完了を待つ結果を返します。 <code>wait</code> が呼び出される前に関数が完了した場合、結果はすぐに返されます。開始された関数が失敗した場合、 <code>wait</code> 呼び出しは同じエラーを生成します。	機能
無効になったメタメソッド: なし		

2.2 **IpAddress**テーブルはIPアドレスを表します。以下のフィールドを含みます。

フィールド	説明	データタイプ
<code>belongs</code>	指定したサブネット (IPアドレス範囲) の IpAddress テーブルに保存されているIPアドレスの所属を確認する関数。	機能



フィールド	説明	データタイプ
	<p>「<IP address>」または「<IP address>/<mask>」のような文字列を唯一の引数として受け取ります。ここで、<IP address>はホストアドレスまたはネットワークアドレス（「127. 0. 0. 1」など）、<mask>はサブネットワークマスク（「255. 0. 0. 0」などのIPアドレスとして、または「8」などの数値形式で指定できます）です。</p> <p>ブール値を返します。</p> <ul style="list-style-type: none">• trueは、アドレスが指定されたアドレスの少なくとも1つと等しいか、指定されたサブネット（IPアドレスの範囲）の少なくとも1つに属していることを示します。• false - それ以外の場合。	

無効になったメタメソッド:

- `__toString`は、文字列内の**IpAddress**を変更する関数です。例: 「127. 0. 0. 1」（IPv4）または「:: 1」（IPv6）
- `__concat`は、**IpAddress**を文字列に結合する関数です。
- `__eq`は、2つの**IpAddress**が等しいことを確認するための関数です。
- `__band`は、マスクを適用するための関数（例: `dw.ip('192.168.1.2') & dw.ip('255.255.254.0')`）です。

3. 例

3.1. 非同期的に開始される手順によって生成される、ログへの出力メッセージ:

```
local dw = require "drweb"

-- この関数は2秒間待機して文字列を返します。
-- 引数として受信されます
function out_msg(message)
    dw.sleep(2)
    return message
end

-- 「メイン」関数
function intercept(ctx)
    -- NOTICEレベルでDr. Web for UNIX Mail Serversログに文字列を出力します
    dw.notice("Intercept function started.")

    -- out_msg関数の2つのコピーを非同期で起動します
    local f1 = dw.async(out_msg, "Hello,")
    local f2 = dw.async(out_msg, " world!")

    -- out_msg関数のコピーの完了を待機中です
    -- out_msgとその結果をログに出力します
    -- Dr. Web for UNIX Mail Servers ログにデバッグレベルで出力します
    dw.log("debug", f1.wait() .. f2.wait())
end
```



3.2. 指定されたスケジュールに従って定期的に開始する手順を作成する:

```
local dw = require "drweb"

-- Futureテーブルをfutureグローバル変数で保存し、
-- Luaのガベージコレクターにより
-- 計画されたタスクが破壊されないようにします
future = dw.async(function()
    while true do
        -- 毎日、次のメッセージがログに表示されます
        dw.sleep(60 * 60 * 24)
        dw.notice("A brand new day began")
    end
end)
```

3.3. 文字列のIPアドレスを変更する:

```
local dw = require "drweb"

local ipv4 = dw.ip("127.0.0.1")
local ipv6 = dw.ip("::1")
local mapped = dw.ip("::ffff:127.0.0.1")
```

drweb.lookupモジュールの内容

1. 機能

このモジュールは次の機能を提供します。

- `lookup(<request>, <parameters>)` はDr.Web LookupDモジュールから利用できる外部ストレージからデータを要求します。<request>パラメータは、Dr.Web LookupD設定内のセクション(文字列<type>@<tag>)に対応している必要があります。<parameters>引数はオプションで、リクエストを生成するために使用される置換を表します。これらのパラメータはテーブルとして設定されます。このテーブルのキーと値は文字列でなければなりません。この関数は、リクエストの結果である文字列の配列を返します。
- `check(<checked string>, <request>, <parameters>)` は、Dr.Web LookupDモジュールを介して利用できる外部リポジトリで<checked string>が見つかった場合に`true`を返します。引数<request>および<parameters>は、`lookup`関数の引数と同じです(上記を参照)。<checked string>引数は、文字列または`__tostring`メタメソッドを持つテーブル(つまり、文字列にフォーマットできる)であると想定されます。

2. 例



データソースLookupD.LDAP.usersから取得されたユーザーリストのログへの出力:

```
local dw = require "drweb"
local dwl = require "drweb.lookup"

-- 「メイン」関数
function intercept(ctx)
  -- NOTICEレベルでDr. Web for UNIX Mail Serversログに文字列を出力します
  dw.notice("Intercept function started.")

  -- リクエスト結果をDr. Web for UNIX Mail Serversログへ出力
  -- 'ldap@users' データソースへ
  for _, s in ipairs(dwl.lookup("ldap@users", {user="username"})) do
    dw.notice("Result for request to 'ldap@users': " .. s)
  end
end

end
```




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 Mail 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 Mail 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、メールサーバー(**Postfix**や**Exim**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 Mail 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>	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-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 Mail 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 Mail 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>	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	コンポーネントの実行ファイルへのパス。



<code>{path to file}</code>	<p>デフォルト値 : <code><opt_dir>/bin/drweb-clamd</code></p> <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>
<p>Start</p> <p><code>{Boolean}</code></p>	<p>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。</p> <p>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。</p> <p>デフォルト値 : <code>No</code></p>
<p><code>Endpoint.<tag>.ClamdSocket</code></p> <p><code>{IP address / UNIX socket}</code></p>	<p><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。</p> <p>1つの <code><tag></code> ポイントに指定できるソケットは1つのみです。</p> <p>デフォルト値 : (未設定)</p>
<p><code>[Endpoint.<tag>.]DetectSuspicious</code></p> <p><code>{Boolean}</code></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疑わしいファイルについて通知します。</p> <p><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。</p> <p>デフォルト値 : <code>Yes</code></p>
<p><code>[Endpoint.<tag>.]DetectAdware</code></p> <p><code>{Boolean}</code></p>	<p>アドウェアを含むファイルについて通知します。</p> <p><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。</p> <p>デフォルト値 : <code>Yes</code></p>
<p><code>[Endpoint.<tag>.]DetectDialers</code></p> <p><code>{Boolean}</code></p>	<p>ダイヤラーを含むファイルについて通知します。</p> <p><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。</p> <p>デフォルト値 : <code>Yes</code></p>



<code>[Endpoint.<tag>.]DetectJokes</code> <code>{Boolean}</code>	<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>
<code>[Endpoint.<tag>.]DetectRiskware</code> <code>{Boolean}</code>	<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>
<code>[Endpoint.<tag>.]DetectHacktools</code> <code>{Boolean}</code>	<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>
<code>[Endpoint.<tag>.]ReadTimeout</code> <code>{time interval}</code>	<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>
<code>[Endpoint.<tag>.]StreamMaxLength</code> <code>{size}</code>	<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>
<p>[Endpoint.<tag>.]HeuristicAnalysis</p> <p>{On / Off}</p>	<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>
<p>[Endpoint.<tag>.]PackerMaxLevel</p> <p>{integer}</p>	<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>
<p>[Endpoint.<tag>.]ArchiveMaxLevel</p> <p>{integer}</p>	<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>
<p>[Endpoint.<tag>.]MailMaxLevel</p> <p>{integer}</p>	<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</p>



	<p>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>.]ContainerMaxLevel</code> <code>{integer}</code>	<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>
<code>[Endpoint.<tag>.]MaxCompressionRatio</code> <code>{integer}</code>	<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)。



ClamdSocket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**clamad**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**clamad**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
メールメッセージサービス	
メールサーバー Postfix	clamad の使い方: メールメッセージのウイルスや悪意のあるプログラムのスキャン。 統合要件: 中間コンポーネントの使用: clamsmtpd 、 clamav-milter 、 amavisd-new 。 ドキュメントへのリンク: Postfix のドキュメント: http://www.postfix.org/documentation.html amavisd-new の説明とソースコードファイル: http://www.amavis.org/
メールサーバー Exim	clamad の使い方: メールメッセージのウイルスや悪意のあるプログラムのスキャン。 統合要件: Exim 設定ファイルに次の設定を追加する



製品	統合
	<pre>av_scanner = clamd: <path_to_clamd_UNIX_socket></pre> <p><path_to_clamd_UNIX_socket>は、***Dr.Web ClamDで設定された接続ポイントのソケット(エンドポイント)に対応します。</p> <p>ドキュメントへのリンク:</p> <p>Eximのドキュメント: http://exim.org/docs.html</p>
メールサーバー CommuniGate Pro	<p>clamdの使い方:</p> <p>メールメッセージのウイルスや悪意のあるプログラムのスキャン。</p> <p>統合要件:</p> <p>中間コンポーネントとしてcgpavを使用する。</p> <p>ドキュメントへのリンク:</p> <p>CommuniGate Proのドキュメント: https://www.communigate.com/CommunigatePro/</p> <p>cgpavの説明とソースコードファイル: http://program.farit.ru/index.html</p>

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。

CommuniGate ProのDr.Web ClamDへの接続例:

1. **cgpav** (バージョン1.5) のダウンロードと構築:

```
$ wget http://program.farit.ru/antivir/cgpav-1.5.tar.gz
$ tar -xzf cgpav-1.5.tar.gz
$ cd cgpav-1.5/
$ ./configure
$ make && make install
```

設定段階で、「Choose Anti-Virus daemon」への応答を選択するときは *Clamav* を選択します。

2. Dr.Web ClamDの設定:

```
[ClamD]
Start = yes

[ClamD.Endpoint.mail]
ClamdSocket = /var/run/drweb.clamd
```

3. **CommuniGate Pro**の設定:

- 1) **CommuniGate Pro**設定ファイル(/var/CommuniGate/Settings/cgpav.conf)で、Dr.Web ClamDソケットへのパスを指定します。

```
clamd_socket = /var/run/drweb.clamd
```

- 2) **CommuniGate Pro**のWebインターフェースで以下を設定します。



- **Settings** → **General** → **Helpers**に移動します。**Content Filtering**で、新しいフィルターを設定します。これを *Enabled* に切り替え、フィルター名 (*drweb* など) を指定し、**Program Path**/パラメータで *cgpav* を指定します。変更内容を保存します。
- **Settings** → **Mail** → **Rules**に移動します。新しいルール名 (*drweb_scan* など) を指定して、**Add Rule** をクリックします。*Highest* ルール設定を選択し、変更を保存して、ルール名の右側にある **Edit** をクリックします。**Data** ドロップダウンメニューで *Message Size* を選択します。**Operation** フィールドで *greater than* を選択し、**Parameter** フィールドで *1* を指定します。**Action** フィールドで *ExternalFilter* を選択します。**Parameter** で、以前に作成したフィルター (この場合は *drweb*) の名前を選択します。変更内容を保存します。



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 Mail 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 Mail 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。
- 「*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、[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 Mail 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 Mail 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 Mail 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)。 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 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 Mail 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(Dr.Web MailD、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 Mail 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、(Dr.Web MailD、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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail Serversの組み込みや、外部 (Dr.Web for UNIX Mail 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ター。</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 Mail 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。

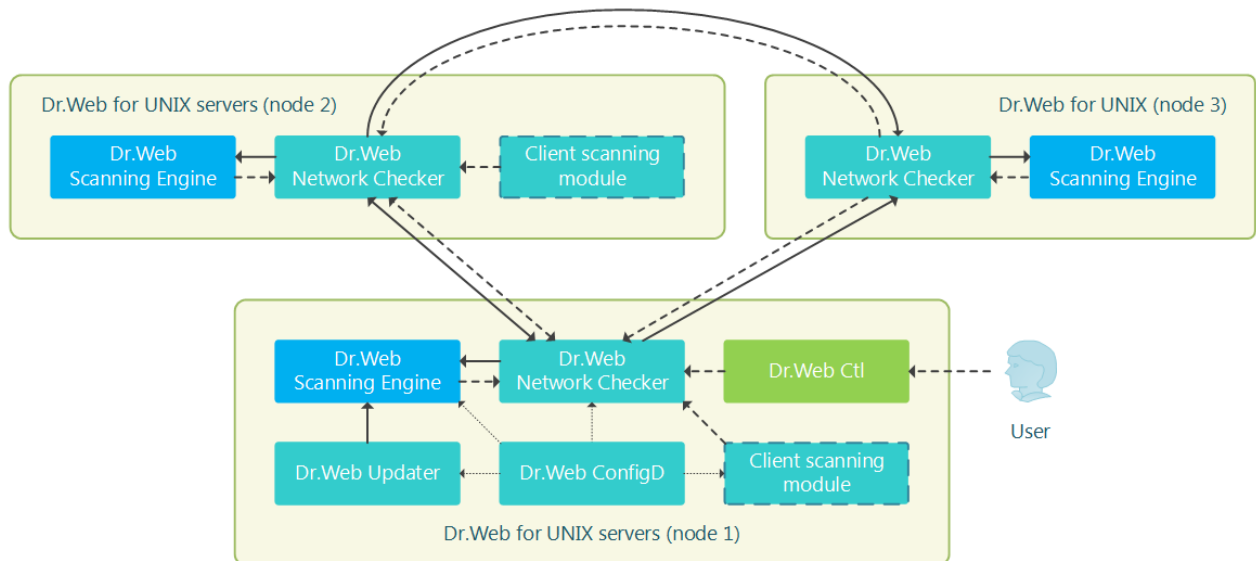


図14. スキャンングラスタの構造

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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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、Webリソースカテゴリーのデータベースとアンチスパムコンポーネント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 Mail 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 Mail 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リソースカテゴリーのデータベース)。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.dr1`) 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 Mail 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 Mail 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 Mail 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 Mail 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: <code><var_dir>/custom-drl/bases</code></p> <ul style="list-style-type: none">• GNU/Linuxの場合: <code>/var/opt/drweb.com/custom-drl/bases</code>• FreeBSDの場合: <code>/var/drweb.com/custom-drl/bases</code>
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ー。</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 Mail 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: <code><var_dir>/drl/version</code></p> <ul style="list-style-type: none">• GNU/Linuxの場合: <code>/var/opt/drweb.com/drl/version</code>• FreeBSDの場合: <code>/var/drweb.com/drl/version</code>
VersionUpdateEnabled <i>{Boolean}</i>	<p>Dr.Web for UNIX Mail 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ー。</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>特別な更新ゾーンのサーバーのリストを含む署名付きファイルへのパス。Webリソースカテゴリーのデータベースを更新するために使用されます。</p> <p>パラメータが空ではなく、指定されたファイルが存在する場合、更新にはサーバーのみが使用されます。リストのメインファイル(上を参照)は無視されます。パラメータによって認識されたファイルが空の場合、更新の試行は失敗します。</p> <p>デフォルト値: <code><var_dir>/drl/dws/custom.drl</code></p> <ul style="list-style-type: none">• For GNU/Linux: <code>/var/opt/drweb.com/drl/dws/custom.drl</code>• FreeBSDの場合: <code>/var/drweb.com/drl/dws/custom.drl</code>
DwsDrlDir <i>{path to directory}</i>	<p>標準的な更新ゾーンのサーバーに接続するためのファイルを含むディレクトリへのパスを定義します。Webリソースカテゴリーのデータベースを更新するために使用されます。</p> <p>デフォルト値: <code><var_dir>/drl/dws</code></p> <ul style="list-style-type: none">• GNU/Linuxの場合: <code>/var/opt/drweb.com/drl/dws</code>• FreeBSDの場合: <code>/var/drweb.com/drl/dws</code>



DwsCustomDrlDir <i>{path to directory}</i>	<p>特別な「カスタマイズされた」更新ゾーンのサーバーに接続するためのファイルを含むディレクトリへのパスを定義します。Webリソースカテゴリーのデータベース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(上を参照)はWebリソースカテゴリーのデータベースを更新するためには使用されません。</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 <i>{Boolean}</i>	<p>Webリソースカテゴリーのデータベース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>
AntispamDrlDir <i>{path to directory}</i>	<p>標準的な更新ゾーンのサーバーに接続するためのファイルを含むディレクトリへのパスを定義します。アンチスパムライブラリの更新に使用されます。</p> <p>デフォルト値: <var_dir>/drl/antispam</p> <ul style="list-style-type: none">• GNU/Linuxの場合: /var/opt/drweb.com/drl/antispam• FreeBSDの場合: /var/drweb.com/drl/antispam
AntispamCustomDrlDir <i>{path to directory}</i>	<p>特別な「カスタマイズされた」更新ゾーンのサーバーに接続するためのファイルを含むディレクトリへのパスを定義します。アンチスパムライブラリの更新に使用されます。</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(上を参照)はアンチスパムライブラリの更新には使用されません。</p> <p>デフォルト値: <var_dir>/custom-drl/antispam</p> <ul style="list-style-type: none">• GNU/Linuxの場合: /var/opt/drweb.com/custom-drl/antispam• FreeBSDの場合: /var/drweb.com/custom-drl/antispam
AntispamUpdateEnabled <i>{Boolean}</i>	<p>アンチスパムライブラリ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: No</p>
BackupDir <i>{path to directory}</i>	<p>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。</p>



	デフォルト値: /tmp/update-backup
MaxBackups <i>{integer}</i>	<p>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。</p> <p>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。</p> <p>デフォルト値: 0</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>最小値 - 10s.</p> <p>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 update [--local-cloud] 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 = Yes 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。</p> <p>デフォルト値: 30s</p>
UseLocalCloud <i>{Boolean}</i>	<p>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)。</p> <ul style="list-style-type: none">• No-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 update --local-cloudコマンドを使用して明示的に実行できます。• Yes - 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)。 <p>デフォルト値: Yes</p>



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 Mail 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 Mail 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 Mail 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](#)設定データモジュール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 Mail Serversを集中管理サーバーに接続するには、Dr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail Serversを管理するだけでなく、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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail Serversの管理WebインターフェースがDr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail 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（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 Mail 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 <i>{address, ...}</i>	<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 Mail Serversの管理](#)
- [概要](#)
- [ユーザー認証と承認](#)
- [Dr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail 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: (<i>SCS cookie</i>)</p> <p>正常に実行された結果: LexMapsオブジェクト、(<i>SCS-cookie</i>)</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: (<i>SCS cookie</i>)、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、(<i>SCS cookie</i>)</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: (<i>SCS cookie</i>)</p> <p>正常に実行された結果: StartUpdateオブジェクト、(<i>SCS-cookie</i>)</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: (<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>
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>
その他	
idpass	<p>アクション: 脅威 Dr.Web MailD を含むリパックされたアーカイブのパスワードを取得します。</p> <p>URI: /api/10.2/idpass</p> <p>HTTPメソッド: POST</p> <p>入力パラメータ: (<i>SCS cookie</i>)、IdpassRequestオブジェクト</p> <p>正常な結果: パスワードを含む文字列 (<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 Mail 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 Mail 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。

9) **IdpassRequest** オブジェクトには、パスワードで保護されたアーカイブに関するデータが含まれています

```
{
  "id": string,    //Identifier from the letter
  * "secret": string //Secret word (optional field)
}
```

secret フィールドが指定されておらず、パスワードタイプが `Plain` でない場合は、**MailD.RepackPassword** 設定パラメータの値が使用されます。パスワードタイプが `Plain` の場合は、エラー（[Error](#) オブジェクト）「`EC_INVALID_ARGUMENT`」が返されます。



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>
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/ <<i>endpoint</i>></p> <p>HTTPメソッド: POST</p> <p>入力パラメータ: (<i>SCS-cookie</i>)、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、(<i>SCS-cookie</i>)</p>
WebページカテゴリーデータベースのURLの確認	
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: (<i>SCS cookie</i>)、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、(<i>SCS-cookie</i>)</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: (<i>SCS cookie</i>)、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、(<i>SCS-cookie</i>)</p>



APIコマンド	説明
<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: (<i>SCS cookie</i>)、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、(<i>SCS-cookie</i>)</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> <p>入力パラメータ: (<i>SCS cookie</i>)、CheckFileRequestオブジェクト</p> <p>正常に実行された結果: FileResultオブジェクト、(<i>SCS-cookie</i>)</p>

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はダイア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>



APIコマンド	説明
	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>)、 FileThreat オブジェクト
<code>cure_threat</code>	アクション: 脅威のIDである <i><threat ID></i> で指定された脅威の修復を試みます。 URI: <code>/api/10.2/cure_threat/ <threat ID></code> 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
<code>delete_threat</code>	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含むファイルを削除します。 URI: <code>/api/10.2/delete_threat/ <threat ID></code> 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
<code>ignore_threat</code>	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: <code>/api/10.2/ignore_threat/ <threat ID></code> 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
<code>quarantine_threat</code>	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: <code>/api/10.2/quarantine_threat/ <threat ID></code> 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、**XA**tttr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
<code>quarantine</code>	<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: <code>/api/10.2/quarantine/</code></p> <p>HTTPメソッド: GET</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: (<i>SCS cookie</i>)、QuarantineIdオブジェクト(隔離内のオブジェクト)の配列</p>
<code>site_quarantine</code>	<p>アクション: <code><site ID></code>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: <code>/api/10.2/quarantine/ <site ID></code></p> <p>HTTPメソッド: GET</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: (<i>SCS cookie</i>)、QuarantineIdオブジェクト(隔離内のオブジェクト)の配列</p>
<code>qentry_info</code>	<p>アクション: 隔離オブジェクトのIDである <code><entry ID></code>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>



APIコマンド	説明
	URI: /api/10.2/qentry_info/ <entry ID> HTTPメソッド: GET 入力パラメータ: (SCS cookie) 正常に実行された結果: (SCS cookie)、QEntryオブジェクト
cure_qentry	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。 URI: /api/10.2/cure_qentry/ <entry ID> HTTPメソッド: POST 入力パラメータ: (SCS cookie) 正常に実行された結果: (SCS cookie)、空のオブジェクト
delete_qentry	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。 URI: /api/10.2/delete_qentry/ <entry ID> HTTPメソッド: POST 入力パラメータ: (SCS cookie) 正常に実行された結果: (SCS cookie)、空のオブジェクト
restore_qentry	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。 URI: /api/10.2/restore_qentry/ <entry ID> HTTPメソッド: POST 入力パラメータ: (SCS cookie) 正常に実行された結果: (SCS cookie)、空のオブジェクト

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ー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":"2F686F6D652F757365722F2E636F6D2E64727765622E71756172616E74696E65",
"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":"467CD4C6D423C55448B71CD5B8152776",
```



```
"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 Mail Serversを統合するよう設計されたSNMPエージェントです。この統合により、Dr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail Servers操作の統計。
3. Dr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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ません。</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ません。</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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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_perfddata_file=/usr/nagiosgraph/var/rrd/perfddata.log
service_perfddata_file_template=$LASTSERVICECHECK$||$HOSTNAME$||$SERVICEDE
SC$||$SERVICEOUTPUT$||$SERVICEPERFDATA$
service_perfddata_file_mode=a
service_perfddata_file_processing_interval=30
service_perfddata_file_processing_command=process-service-perfddata-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 Mail 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 Mail 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 Mail Serversの現在の状態に関する情報	
components	.3.1	Dr.Web for UNIX Mail 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接続のスキャン中に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	メッセージスキャンエラーの数（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キ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> を介したメールスキャンの統計
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	メッセージスキャンエラーの数（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キ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> を介したメールスキャンの統計
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(UNIX時間)
<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(UNIX時間)
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(UNIX時間)
<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(UNIX時間)



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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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。

```
...
[MeshD]
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。

```
...
[MeshD]
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 Mail 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(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 Mail 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。</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Dr.Web MeshD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、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。 <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Dr.Web MeshD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。</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Dr.Web MeshD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、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。 <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 Mail 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](#)スキャンエンジンとインターネットへのアクセスを監視するコンポーネントの誤検知の可能性が少なくなります。

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 Mail 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 Mail 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。

このコンポーネントは、Dr.Web CloudサービスにユーザーがリクエストしたURLのスキャンをリクエストする際に、ネットワークトラフィックのスキャンコンポーネント、[SpIDer Gate](#)。

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 Mail 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 Mail 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 Mail 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 LookupD

Dr.Web LookupDコンポーネントは、LDAPプロトコルを使用してデータを取得するために、外部ソース(テキストファイル、リレーショナルデータベース、ディレクトリサービス、LDAPプロトコルのインタラクションのサポート)を参照するように設計されています。受信したデータはルールで使用され、それによってネットワーク接続がスキャンされます(ユーザー認証のチェックなど)。このデータは、特定の条件が満たされた場合にURLへのアクセスをブロックするためにも使用されます。

コンポーネントの設定では、いくつかのデータソースに接続するためのパラメータを指定できます。Dr.Web LookupDは、Dr.Web for UNIX Mail Serversのいずれかのコンポーネントからデータ要求を受信した場合にのみ、必要なデータソースに接続します。

Dr.Web LookupDでは、次のデータソースへの参照がサポートされます。

- テキストファイル(*AllMatch*、*Mask*、*Regex*、*Cidr*モード)。
- リレーショナルデータベース(**MySQL**、**PostgreSQL**、**SQLite**)。
- **Redis**データストレージ。
- ディレクトリサービス(**Active Directory**や、LDAP経由のアクセスを提供するその他のサービス、たとえば**OpenLDAP**など)。

LDAPプロトコルによるデータの共有は、オープンチャネルまたは保護されたチャネル上でSSL/TLSを適用することで実行できます。安全な接続を使用するには、Dr.Web LookupDに適切なSSL証明書と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必要がある場合は、**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、[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。

動作原理

このコンポーネントは、テキストファイル、リレーショナルデータベース、ネットワークストレージ、LDAPプロトコルをサポートするディレクトリサービス(**Active Directory**など)にデータをリクエストするように設計されています。受信したデータ(ユーザーのIDや権限など)は、Dr.Web for UNIX Mail Serversのコンポーネントに転送され、さまざまなルールでスキャンに使用されます(ユーザーがリクエストしたURLなどにアクセスを許可するなど)。



このマニュアルではリレーショナルデータベース、**Redis**ストレージ、ディレクトリサービス、LDAPプロトコルの動作原理については説明しません。必要に応じて、対応する参考資料を参照してください。

Dr.Web LookupDコンポーネントは、必要に応じて(データのリクエストを受信するときに)[Dr.Web ConfigD](#)設定デーモンによって自動的に起動されます。

特定のコンポーネントからのデータ受信に関するリクエストが到着すると、[Dr.Web ConfigD](#)構成デーモンがDr.Web LookupDを起動します(起動されていない場合)。次に、コンポーネントはリクエストされたデータソースからリクエストを実行してレスポンスを返します。リクエストに応じて、応答は所定の検索条件に従ってデータソースから取得された、特定の検索条件を満たす文字列のリスト、または所定の条件に一致する文字列が検索結果に含まれているかどうかを示す論理値(trueまたはfalse)で構成されます。

Dr.Web LookupD設定では、指定可能なデータソースの数に制限はありません。クライアントコンポーネントは、データ取得リクエストを作成するときに、データソースを指定する必要があります。Dr.Web LookupDは、起



動後しばらくの間、新しいリクエストを待機します。それ以上リクエストがない場合は、待機期間が経過した後、Dr.Web LookupDは自動的にシャットダウンします。

Dr.Web for UNIX Mail Serversのその他のコンポーネントがDr.Web LookupDを使用する基本的な方法は、これらのコンポーネントの動作ルールで指定されているいくつかの条件の有効性を確認するために必要なデータを取得することです。ルールの適用性と条件の妥当性をチェックするときに、Dr.Web LookupDに対するデータリクエストが自動的に実行されます。

テキストファイル処理の特性

1. テキストファイルを処理するとき、文字列の先頭と末尾のスペースは破棄されます。空白行と最初の文字が「#」で始まる行は無視されます。
2. テキストファイルは不変のデータソースと見なされ、その内容はメモリ内に完全にキャッシュされます。さらに、検証のためのこれらのファイルに対するリクエストの結果もキャッシュされます。そのため、ソースファイルが変更されている場合は、**drweb-ctl**の`reload`コマンドなどを使用してDr.Web ConfigDコンポーネントにHUPシグナルを送信することで、Dr.Web LookupDに設定を再読み込みさせる必要があります。

MySQL接続の状況

MySQL接続の前に、**MySQL**ファイル設定の`[client]`セクションのパラメータがデフォルトで読み取られます（ファイル検索は、`/etc/my.cnf`、`/etc/mysql/my.cnf`、`/etc/alternatives/my.cnf`のパスで行われます）。

コマンドライン引数

Dr.Web LookupD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-lookupd [<parameters>]
```

Dr.Web LookupD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>	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-lookupd --help
```

このコマンドはDr.Web LookupD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 Mail 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-lookupd**

設定パラメータ

コンポーネントは、Dr.Web for UNIX Mail Serversの統合された[設定ファイル](#)の[LookupD]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](#)
- [データソースセクション](#)
- [新しいデータソース用のセクションを追加する](#)

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-lookupd <ul style="list-style-type: none">• GNU/Linuxの場合: /opt/drweb.com/bin/drweb-lookupd• FreeBSDの場合: /usr/local/libexec/drweb.com/bin/drweb-lookupd
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
DebugLibldap <i>{Boolean}</i>	libldapライブラリのデバッグメッセージも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（つまり、 LogLevel = DEBUG の場合）。 デフォルト値 : No
LdapCheckCertificate <i>{No / Allow / Try / Yes}</i>	SSL/TLS経由のLDAP接続の証明書検証モード。 使用可能な値 : <ul style="list-style-type: none">• No - サーバーの証明書を要求しない。• Allow - サーバーの証明書を要求する。証明書が提供されない場合、セッションは通常どおりに続行されます。サーバーの証明書が提供されたもののスキャンできない（対応するルート証明書が見つからない）場合、証明書は無視され、セッションは通常どおりに続行されます。• Try - サーバーの証明書を要求する。証明書が提供されない場合、セッションは通常どおりに続行されます。サーバーの証明書が提供されたものの確認できない（対応するルート証明書が見つからない）場合、セッションは終了します。• Yes - サーバーの証明書を要求する。証明書が提供されないか、スキャンできない場合（対応するルート証明書が見つからない場合）、セッションは終了します。 <p>LDAPデータソースの場合、この証明書検証モードは、ldaps://スキームまたはStartTLS拡張機能を使用されときのURLの処理方法に影響します。ADデータソースの場合は、対応するセクションでUseSSL=Yesが指定されている場合（以下参照）のサーバーへの接続に影響します。</p> デフォルト値 : Yes
LdapCertificatePath <i>{path to file}</i>	安全なSSL/TLS接続を介したLDAPサーバーへの接続（ Active Directory ）に使用されるSSL証明書へのパス。 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。 デフォルト値 : （未設定）
LdapKeyPath <i>{path to file}</i>	安全なSSL/TLS接続を介したLDAPサーバーへの接続（ Active Directory ）に使用されるプライベートキーへのパス。 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。 デフォルト値 : （未設定）
LdapCaPath <i>{path}</i>	SSL/TLSを介したLDAPプロトコルによるデータの共有に信頼して使用できる、信頼できるルート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>デフォルト値：信頼できる証明書のリストへのパス。パスはお使いのGNU/Linuxディストリビューションに依存します。</p> <ul style="list-style-type: none">• Astra Linux、Debian、Linux Mint、SUSE Linux、Ubuntuの場合、通常は/etc/ssl/certs/です。• CentOSとFedoraの場合、/etc/pki/tls/certs/ca-bundle.crtです。• 他のディストリビューションでは、コマンドopenssl version -dの実行結果によってパスを定義できます。• コマンドが使用できない場合、またはOSディストリビューションを特定できない場合は、値/etc/ssl/certs/が使用されます。
DbIdleTimeout <i>{time interval}</i>	<p>データベース(またはRedisストレージ)への確立された接続がアイドル状態になっている場合にその接続を切断するまでのタイムアウト期間。</p> <p>デフォルト値：5m</p>
MysqlDefaultConn <i>{URL}</i>	<p>MySQLデータベースに接続するためのパラメータをデフォルトで設定するURL。</p> <p>使用可能な値：</p> <ul style="list-style-type: none">• tcp://[<user>[:<password>]@][<host>][:<port>][/<database name>][?<parameter>=<value>[&...]]• unix://[<user>[:<password>]@]<path to socket>[:<database name>][?<parameter>=<value>[&...]] <p>URI要件に注意してください。</p> <p>デフォルト値：(未設定)</p>
PqDefaultConn <i>{URL}</i>	<p>PostgreSQLデータベースに接続するためのパラメータをデフォルトで設定するURL。</p> <p>使用可能な値：</p> <ul style="list-style-type: none">• tcp://[<user>[:<password>]@][<host>][:<port>][/<database name>][?<parameter>=<value>[&...]]• unix://[<user>[:<password>]@]<path to socket>[:<database name>][?<parameter>=<value>[&...]] <p>URI要件に注意してください。</p> <p>デフォルト値：(未設定)</p>
SqliteDefaultConn <i>{path to file}</i>	<p>デフォルトのSQLiteデータベースファイルへのパス(file:///スキームプレフィックスを指定)。</p> <p>デフォルト値：(未設定)</p>
RedisDefaultConn <i>{URL}</i>	<p>PostgreSQLデータベースの接続パラメータをデフォルトで設定するURL。</p> <p>使用可能な値：</p> <ul style="list-style-type: none">• tcp://[<password>@][<host>][:<port>][/<database index>]• unix://[<password>@]<socket path>[:<database index>] <p>URI要件に注意してください。</p>



デフォルト値：(未設定)

データベース接続のURI要件

1. tcp:およびunix:スキームプレフィックスのみを使用します(ローカルUNIXソケットの場合)。データベース固有のプレフィックス(postgresql:およびmysql:など)はサポートしていません。**SQLite**データベースファイルへのパスは、file://スキームプレフィックスで指定されます。
2. <host>フィールドがURIで指定されていないか、localhostホストが指定されている場合、ホストアドレス127.0.0.1が置き換えられます。この場合、**MySQL**および**PostgreSQL**データベースでは、ネットワーク接続が指定されているにもかかわらず、ローカルUNIXソケットを介してデフォルトで接続が確立されます。
3. URIフィールド(<user>、<password>、<database name>など)または接続パラメータ文字列に特殊文字(スペース、列など)が含まれている場合は、次のように16進コーディングを使用します。たとえば、
 - スペース - 「%20」
 - ':' - 「%3A」
 - '/' - 「%2F」
 - '@' - 「%40」
 - '%' - 「%25」
4. **MySQL**の場合、接続パラメータ文字列には次のパラメータのみを含めることができます。

パラメータ名	データベースドキュメントの文字・記号	タイプ	説明
init	<i>MYSQL_INIT_COMMAND</i>	文字列	データベースへの接続後に実行するSQLコマンド
compression	<i>MYSQL_OPT_COMPRESS</i>	論理	データ圧縮を使用する
connect-timeout	<i>MYSQL_OPT_CONNECT_TIMEOUT</i>	整数	未使用の接続を切断するためのタイムアウト(秒)
reconnect	<i>MYSQL_OPT_RECONNECT</i>	論理	自動再接続を許可または拒否する
read-timeout	<i>MYSQL_OPT_READ_TIMEOUT</i>	整数	サーバーからのパケット受信のタイムアウト(秒)
write-timeout	<i>MYSQL_OPT_WRITE_TIMEOUT</i>	整数	パケットをサーバーに送信するためのタイムアウト(秒)
charset	<i>MYSQL_SET_CHARSET_NAME</i>	文字列	デフォルトの接続に使用される文字エンコーディングの名前
plugin-dir	<i>MYSQL_PLUGIN_DIR</i>	文字列	プラグインを格納するサーバーのディレクトリへのパス



パラメータ名	データベースドキュメントの文字・記号	タイプ	説明
nonblock	<i>MYSQL_OPT_NONBLOCK</i>	整数	ブロック以外のI/O操作のスタックサイズ
ssl-key	<i>MYSQL_OPT_SSL_KEY</i>	文字列	安全な接続を確立するために使用されるプライベートキー（PEM形式）へのパス
ssl-cert	<i>MYSQL_OPT_SSL_CERT</i>	文字列	安全な接続を確立するために使用されるパブリックキー証明書（PEM形式）へのパス
ssl-ca	<i>MYSQL_OPT_SSL_CA</i>	文字列	信頼できるCA証明書を含むファイル（PEM形式）へのパス
ssl-capath	<i>MYSQL_OPT_SSL_CAPATH</i>	文字列	信頼できるCA証明書を含むディレクトリへのパス（PEM形式）
ssl-cipher	<i>MYSQL_OPT_SSL_CIPHER</i>	文字列	安全な接続でサポートされている暗号化アルゴリズムのリスト
ssl-crl	<i>MYSQL_OPT_SSL_CRL</i>	文字列	失効した証明書を含むファイル（PEM形式）へのパス
ssl-crlpath	<i>MYSQL_OPT_SSL_CRLPATH</i>	文字列	失効した証明書を含むディレクトリへのパス（PEM形式）
ssl-fp	<i>MARIADB_OPT_SSL_FP</i>	文字列	有効なサーバー証明書のSHA1ハッシュ
ssl-fp-list	<i>MARIADB_OPT_SSL_FP_LIST</i>	文字列	有効なサーバー証明書のSHA1ハッシュを含むファイルへのパス
tls-passphrase	<i>MARIADB_OPT_TLS_PASSPHRASE</i>	文字列	パスワードで保護されたクライアントプライベートキーのパスワード
tls-version	<i>MARIADB_OPT_TLS_VERSION</i>	文字列	サポートされるTLSバージョンのリスト
server-verify-cert	<i>MYSQL_OPT_SSL_VERIFY_SERVER_CERT</i>	論理	サーバー証明書の検証を許可または禁止する
server-public-key-path	<i>MYSQL_SERVER_PUBLIC_KEY</i>	文字列	RSAサーバーパブリックキーを含むファイル



パラメータ名	データベースドキュメントの文字・記号	タイプ	説明
			(PEM形式)へのパス

データベースのドキュメントのパラメータの詳細については、
https://mariadb.com/kb/en/library/mysql_optionsv/を参照してください。

5. **PostgreSQL**データベースについては、<https://www.postgresql.org/docs/current/libpq-connect.html#LIBPQ-PARAMKEYWORDS>も参照してください。

データソースセクション

設定ファイルには、一般的なセクションである[LookupD]の他、データソースへの接続を記述するセクション（各接続につき1つのセクション）もあります。これらのセクションには、[LookupD.<タイプ>.<名前>]というスキームを使用して名前が付けられます。ここで、


- <タイプ> - 接続の種類：
 - LDAP - **LDAP**を使用するディレクトリサービス用。
 - AD - **Active Directory**サービス。
 - AllMatch - *AllMatch*モードのテキストファイル用（フル認証）。
 - Mask - マスクモードのテキストファイル用（マスク認証）。
 - Regex - *Regex*モードのテキストファイル用（PCRE標準の正規表現に対する認証）。
 - Cidr - *Cidr*モードのテキストファイル用（IPアドレスまたはIPアドレス範囲認証）。
 - Pq - **PostgreSQL**データベース用。
 - Mysql - **Mysql**データベース用。
 - Sqlite - **Sqlite**データベース用。
 - Redis - **Redis**データベース用。
- <名前> - 接続の一意のID（タグ）。これを使用してルールから接続を参照できます。

例:[LookupD.LDAP.auth1]。データソースのセクション内に含まれるパラメータのセットは、接続の種類によって異なります。データソースセクションの数に制限はありません。

1.LDAPタイプのセクションで使用されるパラメータ

Url {string}	<p>使用されるLDAPサーバーと抽出されるデータを定義するURL。URLは、RFC 4516に従って次のスキームに基づいて構築されます。</p> <p><scheme>://<host>[:<port>]/<dn>[?<attrs>[?<scope>[?<filter>[?<extensions>]]]]</p> <p><scheme> - サーバーへの接続方法（許可されるスキーム:ldap、ldaps、ldapi）。</p> <p><host>[:<port>] - リクエストを受信するLDAPサーバーアドレス。</p> <p><dn> - オブジェクトの識別名。このオブジェクトに関する情報が送信されました。</p>
---------------------	--



	<p><attrs> - レコード属性の名前。この値はリクエスト内で受信する必要があります。</p> <p><scope> - 検索範囲 (base、one、sub)。</p> <p><filter> - 抽出された属性の値に対するフィルター条件。</p> <p><extensions> - リクエストで使用されるLDAP拡張子のリスト。</p> <p>機能：</p> <ul style="list-style-type: none">属性のリスト <attrs> では、「*」、「+」、「1.1」の任意の特殊文字を使用できます。以下の自動的に解決されるプレースホルダーは、URLの <dn> および <filter> 部分で使用できます。<ul style="list-style-type: none">\$u は、クライアントコンポーネントによって送信されたユーザー名に自動的に置き換えられます。\$d は、クライアントコンポーネントによって送信されたドメインに自動的に置き換えられます。\$D - dc= <subdomain>、dc= <domain> に変更される <subdomain>、<domain> チェーン。\$ - 「\$」文字。<filter> 条件で特殊文字（「*」、「（」、「）」、「\」、コードが0の文字など）を通常の文字として使用する必要がある場合、それらの文字は \XX と記述する必要があります。さらに、URL LDAP の特殊文字は、シーケンス %XX を使用してエンコードされます。たとえば、「/」文字の ldap:スキームに従って URL をローカル LDAP サーバースocket へのパスの一部として使用する場合、この文字は %2f としてエンコードされます。<extensions> で許可される拡張機能として、StartTLS と 1.3.6.1.4.1.1466.20037 のみがサポートされます。これらの拡張機能では、保護されたスキームである ldaps を使用することが明示されていない場合でも、TLS メカニズム（つまり、LDAP サーバとの保護された接続の確立）が使用されます。使用される拡張機能の名前の前に「!」文字がある場合は、TLS を使用する必要があります。つまり、安全な接続を確立できない場合には、リクエストは処理されません。それ以外の場合は、安全な接続が確立されていなくてもリクエストは処理されます。 <div> 指定された拡張機能は、保護された ldaps スキームでは使用できません。詳細については、RFC 4516 または man ldap_search_ext_s を参照してください。</div> <p>例：</p> <pre>"ldaps://ds.example.com:990/\$D?givenName,sn,cn?sub?(uid=\$u)" "ldap://ldap.local/o=org,dc=nodomain?ipNetworkNumber?sub?(objectClass=ipNetwork)?!StartTLS"</pre> <p>デフォルト値：（未設定）</p>
BindDn {string}	<p>ユーザーが認証を受けなければならないLDAPディレクトリ内のオブジェクト。</p> <p>例：「cn=admin,dc=nodomain」</p> <p>デフォルト値：（未設定）</p>



BindPassword <i>{string}</i>	LDAPサーバー上での認証に使用するユーザーのパスワード。 デフォルト値：(未設定)
ChaseReferrals <i>{Boolean}</i>	現在のLDAPサーバーがリクエストへの応答として他のLDAPサーバーへの参照を返す場合、その参照に従うようコンポーネントに指示します。 デフォルト値：No

2.ADタイプのセクションで使用されるパラメータ

Host <i>{string}</i>	接続する Active Directory サービスのサーバーが稼働しているホストのドメイン名 (FQDN) または IP アドレス。 例：「win2012.win.local」 デフォルト値：(未設定)
Port <i>{integer}</i>	Active Directory サービスのサーバーが待ち受け(リッスン)するホスト上のポート。 デフォルト値：389
Dn <i>{string}</i>	Active Directory 内のオブジェクトの <i>DN</i> 。これは LDAP URL の <i>dn</i> 部分に似ています。 例：「dc = win、dc = local」 デフォルト値：(未設定)
User <i>{string}</i>	識別に使用される、サーバー上のユーザー ID。 例：「Administrator@WIN.LOCAL」 デフォルト値：(未設定)
Password <i>{string}</i>	Active Directory サーバー上での認証に使用されるユーザーのパスワード。 デフォルト値：(未設定)
ChaseReferrals <i>{Boolean}</i>	現在の Active Directory サーバーがリクエストへの応答として他のLDAPサーバーへの参照を返す場合、その参照に従うようコンポーネントに指示します。 デフォルト値：No
UseSSL <i>{Boolean}</i>	Active Directory サーバーへの接続にSSL/TLSを使用するよう指示します。 デフォルト値：No

3.AllMatch、Mask、Regex、Cidrタイプのセクションパラメータ

File <i>{path}</i>	検索文字列を含むテキストファイルへのパス。 例：「/etc/file1」 デフォルト値：(未設定)
------------------------------	---



注意

- AllMatchタイプのセクションで指定したファイルの文字列は、大文字と小文字を区別しない完全に一致する文字列の検索に使用されます。
- Maskタイプのセクションで指定したファイルの文字列は、マスクワイルドカードと見なされます。マスクは、標準文字と特殊文字を含む正規表現の簡略版と見なすことができます。文字列とマスクの照合は、大文字と小文字を区別しないで行われます。マスクには、次の特殊文字と式を含めることができます。

* - 任意の文字シーケンス。

? - 任意の1つの記号。

[<character set>] - セットの文字(たとえば、[bac])

[<character set>] - セットのどの記号にも一致しない文字(たとえば、[!cab])

[[:<class>:]] - 文字(alnum、alpha、ascii、blank、cntrl、digit、graph、lower、print、punct、space、upper、xdigit)のPOSIXクラスの文字。

サブストリングと一致するマスクには、「*」記号で囲まれたサブストリングが含まれている必要があります。(例: *host*)。いずれかの特殊文字を指定する必要がある場合は、バックスラッシュを使用して文字をエスケープする必要があります(\\[, \\], *, \\?)。必要に応じて、バックスラッシュをエスケープすることもできます(\\)。他の文字をエスケープしても意味はありません。たとえば文字列\\a\\b\\c*\\d\\?\\は文字列abc*d?\\に変換されます。マスクの例:

```
#「name」文字列に完全に一致します
name

#3文字の文字列に一致します:
#最初の文字は「c」、2番目は任意、3番目は「t」
#例:「cat」、「cut」、「cct」
c?t

#「user」、「users」、「us3rr」、「ussr1」などの文字列に一致します
#([:alpha:] 文字クラスは任意のアルファベット
#文字、特殊文字「?」は任意の文字に一致します)
us[[:alpha:]]34]r?

#「.con」、「file.col」、「3...co!」などの文字列に一致します
#(「.co」の前の任意の文字シーケンス、その後ろは
#「m」と「?」以外の任意の文字)
*.co[!m\\?]

#「host」を含む任意の文字列に一致します。
#例:「host」、「localhost」、「hostel」、「ghosts」
*host*
```

- Regexタイプのセクションで指定したファイルの文字列は、PCRE(Perl互換正規表現)の通常の拡張機能として解釈されます。文字列と正規表現の照合は、大文字と小文字を区別しないで行われます。正規表現の例:

```
#IPv4
(\\d{1,3}\\.){3}\\d{1,3}

#.comドメインのメールアドレス
\\w+@\\w+\\.com
```



- *Cidr*タイプのセクションで指定したファイルの文字列は、IPアドレスまたはIPアドレス範囲として解釈されます。IPアドレスとIPアドレス範囲では、IPv4形式とIPv6形式が許可されます。サブネットマスクは、ビット（オクテット）形式とCIDR（*Classless Inter-Domain Routing*）表記で指定できます。例：

```
#IPv4
192.168.0.1
192.168.0.0/12
192.168.0.0/255.255.255.224

#IPv6
fe80::c7e8/32
fe80::c7e8/255.255.255.224
```

4.Pq、Mysql、Sqliteタイプのセクションで使用されるパラメータ

Conn <i>{string}</i>	<p>データベース接続文字列。</p> <p>使用可能な値：</p> <ul style="list-style-type: none">• Mysql（MySQL）、Pq（PostgreSQL）セクションの場合： <code>tcp://[<user>[:<password>]@]<host>[:<port>][/<database name>][?<parameter>=<value>[&...]]</code> <code>unix://[<user>[:<password>]@]<path to socket>[:<database name>][?<parameter>=<value>[&...]]</code> 例：「tcp://user:pwd@localhost:1234/userdb」、 「unix://user:pwd@tmp/pgsql.sock:userdb」 URI要件に注意してください。• Sqlite（SQLite）セクションの場合： データベースファイルへのパス（file://スキームプレフィックスを指定）。 例：「file:///home/user/users.db」 <p>デフォルト値：対応する*DefaultConnパラメータ値によって定義</p>
Request <i>{string}</i>	<p>データベースへのSQLクエリー文字列（SELECT）。ADおよびLDAPタイプのソースについては、以下の自動的に許可されるマーカーをクエリーで使用できます。</p> <ul style="list-style-type: none">• \$u、\$Uは、クライアントコンポーネントによって送信されたユーザー名に自動的に置き換えられます。• \$d、\$Dは、クライアントコンポーネントによって送信されたドメインに自動的に置き換えられます。• \$\$は、「\$」文字に置き換えられます。 <p>例："SELECT username FROM users INNER JOIN domains ON users.domain = domains.id WHERE domains.name = \$d AND users.name = \$u"</p> <p>デフォルト値：（未設定）</p>



注意

SQLクエリーとして、SELECTタイプのクエリーのみ指定できます。置換を実行した後、クエリーは「そのまま」データベースに送信されます。クエリー結果に複数のカラムが含まれる場合、最初のカラムを除くすべてのカラムが無視されます。

5.Redisタイプのセクションで使用されるパラメータ

Conn <i>{string}</i>	Redis データストレージとの接続文字列。 使用可能な値： <ul style="list-style-type: none">tcp://[<password>@] <host>[:<port>] [/<database index>]unix://[<password>@] <socket path>[:<database index>] URI要件 に注意してください。 例：「tcp://localhost:6379」 デフォルト値：RedisDefaultConn/パラメータ値によって定義
Request <i>{string}</i>	Redis ストレージのクエリー文字列。クエリーでは、以下の自動的に許可されるマーカーを使用できます。 <ul style="list-style-type: none">\$u、\$Uは、クライアントコンポーネントによって送信されたユーザー名に自動的に置き換えられます。\$d、\$Dは、クライアントコンポーネントによって送信されたドメインに自動的に置き換えられます。\$sは、「\$」文字に置き換えられます。 例："HVALS bad_users" デフォルト値：(未設定)

注意:クエリー結果に複数のカラムが含まれる場合、最初のカラムを除くすべてのカラムが無視されます。

新しいデータソース用のセクションを追加する

Dr.Web for UNIX Mail Servers用のコマンドラインベースの管理ツールである[Dr.Web Ctl](#)([drweb-ctl コマンド](#) 経由でアクセス)を使用し、<名前>タグを使って、サポートされるタイプの新しいデータソース用の新しいセクションを追加するには、次のコマンドを使用する必要があります。

```
# drweb-ctl cfset LookupD.<type> -a <name>
```

例:

```
# drweb-ctl cfset LookupD.AD -a WinAD1
# drweb-ctl cfset LookupD.AD.WinAD1.Host 192.168.0.20
```

最初のコマンドは[LookupD.AD.WinAD1]という名前のセクションを設定ファイルに追加し、2番目のコマンドはこのセクション内のホストパラメータの値を変更します。



あるいは、次のように新しいセクションを[設定ファイル](#)に直接書き込む（ファイルの末尾に追加するなど）こともできます。

```
[LookupD.AD.WinAD1]  
Host = 192.168.0.20
```



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）。



Dr.Web StatD

Dr.Web StatDコンポーネントは、Dr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail 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。
- クリックカーは、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/バッファ) で動作し、解析されたプログラムの実行は命令ごとにモデル化されます。ただし、これらの命令は実際にはCPUによって実行されるものではありません。エミュレーターがポリモーフィック型ウイルスに感染したファイルを受信すると、エミュレーションの結果は復号されたウイルスコードになります。これは、シグネチャチェックサムを検索することで簡単に判別できます。

ヒューリスティック解析

ヒューリスティックアナライザの検出手法は、ウイルスコードに典型的な、または非常にまれな特徴 (属性) に関する特定の情報に基づいています (ヒューリスティック)。各属性は、その深刻度および信頼度を定義する重み係数を持っています。属性が悪意のあるコードであることを示している場合には重み係数がプラスになり、コンピューター脅威の特徴を示していない場合はマイナスになります。ヒューリスティックアナライザはファイルの重み付け合計値に応じて、未知のウイルスに感染している可能性を計算します。それらの合計が一定のしきい値を超えて



いる場合、ヒューリスティックアナライザによって、オブジェクトは未知のウイルスに感染している可能性があると判定されます。

ヒューリスティックアナライザはファイル解凍の柔軟なアルゴリズムである FLY-CODE™テクノロジーも使用します。このテクノロジーは、Dr.Webにとって既知のパッカーのみでなく、これまでに発見されていない未知のパッカーによって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र्फ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。
- **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。

Dr.Web MailDがメールメッセージをスキャンすると、次のアクションがメールメッセージに適用されます。

- **Pass** (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。
- **Reject** (拒否) - メールメッセージを拒否し、受信者への配信を禁止するように指示します。
- **Tempfail** (Tempfail) - メールメッセージの配信の代わりに、送信者または受信者にエラーメッセージを返すように指示します。
- **Discard** (破棄) - メールメッセージを受け入れ、受信者には配信しません。
- **Repack** (リパック) - メールメッセージを受信者に配信する前に、脅威を隔離に移動することによってメッセージを修正するように指示します。メールメッセージにアーカイブを添付し、脅威検出に関する通知を追加します。
- **Add Header** (ヘッダーの追加) - 受信者への配信時にメールメッセージにヘッダーを追加します。
- **Change Header** (ヘッダーの変更) - 受信者への配信中に、指示されたヘッダーの値を変更します。



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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail Serversの設定パラメーター(`drweb.ini` の内容、ルール、ルールで使用する値のファイル、Luaプロシージャなどを含む)
- Dr.Web for UNIX Mail 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 Mail Servers設定ファイル

すべてのDr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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。
 - **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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail Serversをインストールする](#)および[Dr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail Serversを再インストールしてください。

Dr.Web for UNIX Mail 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 Mail Serversをインストールする](#)および[Dr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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: ネットワーク経由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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail Serversまたはコンポーネントの1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 Mail 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。
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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail Serversをインストールする](#)および[Dr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail Serversをインストールする](#)および[Dr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail Serversをインストールする](#)および[Dr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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. このエラーがDr.Web Firewall for Linuxによって発生している場合、他のファイアウォールと競合している可能性があります。たとえば、Dr.Web Firewall for Linuxが**Fedora**、**CentOS**、**Red Hat Enterprise Linux**の**Firewalld**と競合することが知られています（起動するたびに、**Firewalld**はDr.Web Firewall for Linuxにより追加されたトラフィックルーティングルールを破棄します）。このエラーを解決するには、以下のコマンドを実行してDr.Web for UNIX Mail Serversを再起動します

```
# service drweb-configd restart
```

または

```
# drweb-ctl reload
```



Firewalldの動作を許可すると、OSの再起動も含め、**Firewalld**の再起動ごとにDr.Web Firewall for Linuxのエラーが繰り返し発生する可能性があります。このエラーを解決するには、**Firewalld**を無効にします（お使いのOSのマニュアルに含まれている**Firewalld**のマニュアルを参照してください）。

3. 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）。
4. この手順で問題が解決しない場合は、Dr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail Serversをインストールする](#)および[Dr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail Serversをインストールする](#)および[Dr.Web for UNIX Mail 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 Mail 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: 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail 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 Mail Serversを再起動させます。

```
# service drweb-configd restart
```

4. Dr.Web for UNIX Mail 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 Mail 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 Mail Serversをインストールする](#)および[Dr.Web for UNIX Mail 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 Mail 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 Mail 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. このエラーがSpIDer Gateによって発生している場合、オペレーティングシステムに互換性のないソフトウェアがある可能性があります。このソフトウェアは、**NetFilter**システムファイアウォールのルールを生成します。これにより、SpIDer Gateが正しく動作しなくなります。おそらく、**Shorewall**または**SuseFirewall2**がシステムにインストールされているでしょう(**SUSE Linux OS**の場合)。**NetFilter**システムファイアウォールを設定するアプリケーションは、指定されたルールシステムの整合性をチェックして書き換えることがあります。これがSpIDer Gateがこのようなアプリケーションと競合する主な理由です。
SpIDer Gate操作に干渉しないように、互換性のないソフトウェアを再設定してください。それが不可能な場合は、オペレーティングシステムの起動時に読み込まれないようにソフトウェアを無効にします。以下の手順に従って、**SuseFirewall2** アプリケーション(**SUSE Linux OS**の場合)の設定を行ってください。
1) **SuseFirewall2**の設定ファイル(デフォルトでは/etc/sysconfig/SuSEfirewall2ファイルです)



を開きます。

2) 以下のテキストブロックを見つけます。

```
# Type: yesno
#
# Install NOTRACK target for interface lo in the raw table. Doing so
# speeds up packet processing on the loopback interface. This breaks
# certain firewall setups that need to e.g. redirect outgoing
# packets via custom rules on the local machine.
#
# Defaults to "yes" if not set
#
FW_LO_NOTRACK=""
```

3) パラメータ値に `No` を指定します。

```
FW_LO_NOTRACK="no"
```

4) **SuseFirewall2**を再起動します。そのために、以下のコマンドを使用します。

```
# rcSuSEfirewall12 restart
```



SuseFirewall2の設定内にFW_LO_NOTRACKがない場合、競合を解決するためにはアプリケーションを無効にし、それがシステム起動時に読み込まれないようにする必要があります(たとえば、**SUSE Linux Enterprise Server 11**にはこれが必要です)。

競合アプリケーションを再設定または無効にした後、SpIDer Gateを再起動してください。

2. 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、互換性のないソフトウェアを無効にするか再設定し、Dr.Web for UNIX Mail 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: 無効な *VadeRetro* ライブラリです。

エラーコード: x110

説明: **VadeRetro** アンチスパムライブラリのファイルが見つからないか、使用できないか、あるいは破損しています(メー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 Mail 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. **vaderetro.so** ライブラリファイルへのパスを確認してください。必要に応じてパスを変更します([設定ファイル](#)の[Root] [セクション](#)にある **VaderetroLibPath** 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.VaderetroLibPath
```

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.VaderetroLibPath <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.VaderetroLibPath -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-maildパッケージを再インストールしてください。

Dr.Web for UNIX Mail 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 Mail Serversをインストールする](#)および[Dr.Web for UNIX Mail 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: *Webリソースカテゴリーのデータベースがありません。*

エラーコード: x112

説明: Webリソースカテゴリーのデータベースがありません。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX Mail 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. Webリソースカテゴリーディレクトリのデータベースへのパスを確認してください。必要に応じてパスを変更します（[設定ファイル](#)の[Root] [セクション](#)にあるDwsDirパラメータ）。
 - パス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.DwsDir
```

新しいパラメータ値を設定するには、以下のコマンドを実行します。



```
# drweb-ctl cfset Root.DwsDir <new path>
```

パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset Root.DwsDir -r
```

2. Webリソースカテゴリーのデータベースを更新：

- 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：[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 Mail 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 Mail 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 Mail Serversをインストールする](#)および[Dr.Web for UNIX Mail 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: *SpIDer Gate*を使用することができません。

エラーコード: x117

説明: SpIDer Gateコンポーネントがありません(ネットワーク接続のスキャンに必要です)。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX Mail 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-gated**実行ファイルへのパスを確認してください。必要に応じてパスを変更します([設定ファイル](#)の[GateD][セクション](#)にあるExePathパラメータ)。

または、コマンドライン管理ツールの [コマンド](#) を使用することもできます。

現在のパラメータ値を確認するには、以下のコマンドを実行します。

```
$ drweb-ctl cfshow GateD.ExePath
```

新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset GateD.ExePath <new path>
```

パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset GateD.ExePath -r
```

2. 設定にSpIDer Gateコンポーネントの設定が含まれていない場合、または正しいパスを入力した後もエラーが継続する場合は、drweb-gatedパッケージをインストールまたは再インストールしてください。

Dr.Web for UNIX Mail 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 Mail Serversをインストールする](#)および[Dr.Web for UNIX Mail 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: *MailD*を使用することができません。

エラーコード: x118

説明: Dr.Web MailDコンポーネントが見つかりません(メール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 Mail 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-maild**実行ファイルへのパスを確認してください。必要に応じてパスを変更します([設定ファイル](#)の[MailD][セクション](#)にあるExePathパラメータ)。

または、コマンドライン管理ツールの [コマンド](#) を使用することもできます。

現在のパラメータ値を確認するには、以下のコマンドを実行します。



```
$ drweb-ctl cfshow MailD.ExePath
```

新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset MailD.ExePath <new path>
```

パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset MailD.ExePath -r
```

2. 設定にDr.Web MailDコンポーネントの設定が含まれていない場合、または正しいパスを入力した後もエラーが継続する場合は、drweb-maildパッケージをインストールまたは再インストールしてください。

Dr.Web for UNIX Mail 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 Mail Serversをインストールする](#)および[Dr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail 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 Mail Serversをインストールする](#)および[Dr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail Serversをインストールする](#)および[Dr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail Serversをインストールする](#)および[Dr.Web for UNIX Mail 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: *Firewall for Linux*を使用することができません。

エラーコード: x122

説明: Dr.Web Firewall for Linuxコンポーネントがありません(ネットワーク接続のスキャンに必要です)。

エラーの発生した場所と理由に関する詳細については、Dr.Web for UNIX Mail 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-firewall**実行ファイルへのパスを確認してください。必要に応じてパスを変更します([設定ファイル](#)の[LinuxFirewall][セクション](#)にあるExePathパラメータ)。

または、コマンドライン管理ツールの [コマンド](#)を使用することもできます。

現在のパラメータ値を確認するには、以下のコマンドを実行します。



```
$ drweb-ctl cfshow LinuxFirewall.ExePath
```

新しいパラメータ値を設定するには、以下のコマンドを実行します。

```
# drweb-ctl cfset LinuxFirewall.ExePath <new path>
```

パラメータ値をデフォルトに復元するには、以下のコマンドを実行します。

```
# drweb-ctl cfset LinuxFirewall.ExePath -r
```

2. 設定にDr.Web Firewall for Linuxコンポーネントの設定が含まれていない場合、または正しいパスを入力した後もエラーが継続する場合は、drweb-firewallパッケージをインストールまたは再インストールしてください。

Dr.Web for UNIX Mail 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 Mail Serversをインストールする](#)および[Dr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail Serversをインストールする](#)および[Dr.Web for UNIX Mail 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 Mail 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 Mail 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 Mail Serversをインストールする](#)および[Dr.Web for UNIX Mail 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 Mail 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 Mail 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：	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 Mail 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 Mail 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。

```
[Service]
LimitNOFILE=16384
```

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 Mail 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](#) までご連絡ください。

症状：	<p>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>を実行しようとすると、次のいずれかのエラーが発生します。</p> <pre>Error: connect: No such file or directory: "<path>/ .com.drweb.public"</pre> <p>または</p> <pre>Error: connect: Connection refused: "<path>/ .com.drweb.public".</pre>
説明：	設定デーモンDr.Web ConfigDが使用できないため、Dr.Web for UNIX Mail 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。

```
# service drweb-configd restart
```

Dr.Web ConfigDとDr.Web for UNIX Mail 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 Mail Serversは**PAM**がないと正しく動作できません)。

3. エラーが解決しない場合は、Dr.Web for UNIX Mail 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 Mail 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 Mail Serversをインストールする](#)および[Dr.Web for UNIX Mail 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。

症状：

1. SpIDer Gateを無効にした後、すべてのネットワーク接続が切断され(SSH/FTPプロトコル経由での送信、および場合によっては受信も)、再確立できなくなります。
2. 以下のコマンドを使用して、**NetFilter (iptables)**ルール全体を検索する。

```
# iptables-save | grep "comment --comment --comment"
```

を使用すると、空以外の結果が返ってくる。

説明：

このエラーは1.4.15より前のバージョンの不正な**NetFilter (iptables)**動作に関連しています。この内部エラーのため、SpIDer Gateが一意的ラベル(コメント)が付いたルールをルールのリストに追加すると、そのルールは誤って追加されます。その結果、SpIDer Gateはシャットダウン時に接続の迂回ルールを削除できません。

エラーの解決：

1. SpIDer Gateモニターを再度有効にしてください
2. SpIDer Gateを無効にする必要がある場合、以下のコマンドを使用して、**NetFilter (iptables)**の不正なルールを削除してください

```
# iptables-save | grep -v "comment --comment --comment" | iptables-restore
```

iptables-save および **iptables-restore** コマンドにはルート権限が必要です。権限を昇格するには**su** および **sudo** コマンドを使用することができます。また、このコマンドは正しくないコメントを持つすべてのルール(例：同じトラフィックのリダイレクトを実行する他のアプリケーションによって追加されたものなど)を削除するという点に注意してください。

追加情報：

- この問題の発生を防ぐため、お使いのOSをアップグレードすることが推奨されます(または、少なくとも**NetFilter**をバージョン1.4.15以降に)。



- また、**iptables**ユーティリティを使用して必要なルールを指定することで接続を手動でSpIDer Gateへリダイレクトさせる場合は、Dr.Web Firewallの設定で、SpIDer Gateへの接続のリダイレクトを手動モードに切り替えることができます（この方法は推奨されません）。
- 詳細はマニュアル**man: drweb-firewall(1)**、**drweb-gated(1)**、**iptables(8)**を参照してください。

引き続きエラーが発生する場合は、[テクニカルサポート](#)までご連絡ください。

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	モニターチャン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
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



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
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
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



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
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
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



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
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
110	EC_BAD_VADERETRO_LIB	無効な VadeRetro ライブラリです	エラーx110
112	EC_NO_DWS_BASES	Webリソースデータベースがありません	エラーx112
115	EC_NO_LOOKUPD	LookupDは使用できません	エラーx115
117	EC_NO_GATED	GateDは使用できません	エラーx117
118	EC_NO_MAILD	MailDを使用できません	エラーx118
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
122	EC_NO_FIREWALL	Firewallは使用できません	エラーx122
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
<i>AD</i>	Microsoft Active Directory
<i>DN</i>	(LDAP) Distinguished Name(識別名)
<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>IMAP</i>	Internet Message Access Protocol(メールプロトコル)
<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>MBR</i>	Master Boot Record(マスターブートレコード)
<i>MDA</i>	Mail Delivery Agent(メール配信エージェント)
<i>MTA</i>	Mail Transfer Agent(メールサーバー)
<i>MUA</i>	Mail User Agent(メールクライアント)
<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>POP</i>	Post Office Protocol(メールプロトコル)
<i>RPM</i>	Red Hat Package Manager(Red Hatパッケージマネージャー)
<i>RAA</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>SMTP</i>	Simple Mail Transfer Protocol(メールプロトコル)
<i>SNI</i>	Server Name Indication(サーバー名表示)



文字・記号	説明
<i>SNMP</i>	Simple Network Management Protocol(シンプルネットワークマネー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)
<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)

