Dr.WEB®

Anti-virus + Anti-spam
for UNIX Mail Servers

管理者マニュアル

Defend what you create

Anti-virus Dr.Web for UNIX mail servers
バージョン **6.0.1**
管理者マニュアル
09.11.2011

ロシア本社
2-12A, 3rd str. Yamskogo polya
Moscow, Russia
125124

ウェブサイト www.drweb.com
電話 +7 (495) 789-45-87

地方支店、オフィスに関する情報は、弊社のオフィシャルサイトにあります。

Doctor Web

弊社はマルウェアおよび迷惑メールに対する効率的な保護を
提供する Dr.WebR 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。

個人ユーザから政府機関、また中小企業から国際的な企業まで、
世界中のあらゆる地域に弊社のお客様は広がっています。

Dr.Web アンチウイルスソリューションは 1992年以来、
卓越したマルウェアの検出能力と国際的な情報
セキュリティ基準への適合で良く知られています。
Dr.Web ソリューションには政府による認証や表彰が
何度も与えられていること、また弊社製品のユーザが
世界中に広がっていることは、弊社製品に対する
皆さまからの絶大な信頼の証しだと自負しています。

**弊社の全てのお客さまからの多大なるご支援と
ご貢献に心より感謝いたします。**

目次

はじめに

本マニュアルではUNIX®系システムにおけるメールプロセス及びフィルタリングに対する以下の**Dr.Web®**ソリューションについて説明します。

- **Anti-virus** + **anti-spam Dr.Web for UNIX mail servers**
- **Anti-spamDr.Web for UNIX mail servers**
- **Anti-virus Dr.Web for UNIX mail servers**
- **Anti-virus** + **anti-spam Dr.Web for UNIX mail gateways**
- **Anti-spam Dr.Web for UNIX mail gateways**
- **Anti-virus Dr.Web for UNIX mail gateways**

これらのソリューションは全て、インストールするモジュールとプラグインの組み合わせが異なるだけです。以後これらは全て**Dr.Web for UNIX mail servers**と記します。インストールするモジュールに応じて、異なるメールトランスファーシステムとの統合が確立され、ウイルスやスパムからメールを保護します。また、ソフトウェアはメールゲートウェイとしても動作可能です。
ソリューションにはそれぞれ主要なUNIX系OS（以後「UNIXシステム」であるLinux、FreeBSD、Solaris、x86向けの3つのバリエーションがあります。これらのバリエーションの違いはわずかで、以後は全て**Dr.Web for UNIX mail servers**と記します。重要な違いはそれぞれ別のチャプター及びパラグラフ内で説明します。

本マニュアルはアンチウイルス保護及びセキュリティの責任者（以後「*管理者*」）向けのものです。

UNIXシステム内の電子メール保護の特徴

- 全ての受信SMTPトラフィック内のウイルスとその診断及び駆除を検査します。
  ほとんどの場合、ウイルスは直接UNIXシステム向けに作られたものではありません。WordやExcel及びその他のオフィスアプリケーションを含む一般的なWindowsのウ　　イルスは電子メールを介して広がります。
- スパム及び望ましくない通信をフィルタリング

Dr.Web for UNIX mail servers ソリューションは上記どちらのタスクも実行します。

Dr.Web Daemonアンチウイルスパッケージは外部アンチウイルスフィルタープラグインとして、ほとんど全てのデータ処理スキーマで使用可能です。`Vaderetro`プラグインは外部スパムフィルターとして使われます。**Dr.WebMailD**パッケージはメールトラフィックの分析及び処理に使われ、その他全てのパッケージとSendmail、Postfix、

Courier、Qmail、CommuniGate Pro、ZMailer、 Exim メールトランスファーシステムとの統合を可能にします。**Dr.Web MailD**はまた、**Dr.Web Security Suite**によってコントロールされるアンチウイルスネットワークの一部としても操作可能です。

Dr.Web for UNIX mail serversソリューションによって解決できる問題の範囲は、インストールするモジュール（メッセージを直接処理する特別なライブラリの種類によって決まります。

また、2つのSDKを使用することが可能です。
- **Receiver/Sender**コンポーネントの機能を実行する新しいモジュールの開発ツール、及び新しいMTAに対するサポートを提供するSDK。
- メールを処理する新しいプラグインの開発ツールを提供するSDK。

本マニュアルでは、**Dr.Web for UNIX mail servers**ソリューションのフルコンフィギュレーション（例：広く使われているMTAと動作するためのモジュールや利用できる全てのプラグインとの）でのセットアップ、調整、及びスタートアップ手順の基本的なステップについて説明します。
- 製品に関する一般的な情報
- **Dr.Web for UNIX mail servers** ソリューションのインストール
- **Dr.Web for UNIX mail servers**ソリューションのスタートアップ
- **Dr.Web for UNIX mail servers**ソリューションの調整

また、本書の末尾にはテクニカルサポートサービスの連絡先が掲載されています。

Dr.Web製品は常に発展を続けています。ウイルスデータベースへのアドオンは毎日、または1日に数回もリリースされ、製品の新しいバージョンが登場しています。アンチウイルス保護の診断テクニックや手法、及びUNIXシステムのその他のアプリケーションとの統合が定期的に改良されています。**Dr.Web**と互換性のあるアプリケーションのリストは拡張を続け、そのため本マニュアル内で説明する設定や機能の一部は現在のプログラムのバージョンと若干異なる場合があります。最新のプログラム情報を得るにはデリバリーパッケージに含まれているドキュメンテーションファイルを参照してください。

表記規則

本書では、以下の文字・記号を使用しています。

文字・記号	意味
太字	グラフィカルユーザインターフェース(GUI)の要素の名称や本書のとおり正確に入力する必要のある入力例
緑色の太字	**Doctor Web** 製品またはコンポーネントの名称
緑色で下線付きの文字	本書の他のページや他のWebページへのリンク
固定幅フォント	コマンドラインの入力例、出力例
イタリック体	ユーザが提供しなければならない情報を表すプレースホルダ。コマンドラインの入力例がイタリック体の場合は、パラメータ値を示します。
大太字	キーボードのキー名称
プラス記号 ('+')	キーの同時押し(例: ALT+F1 は、ALTキーとF1キーを同時に押すことを意味します。)
感嘆符	重要な注釈、またはエラーなどを引き起こす可能性のある状況に関する警告

ソフトウェアのコンポーネントがインストールされるディレクトリを定義するために `%bin_dir`, `%etc_dir`, `%var_dir` の表記を使用しています。

使用するOSごとに、それぞれ以下のディレクトリを指します。

Linux, Solaris:

```
%bin_dir = /opt/drweb/
%etc_dir = /etc/drweb/
%var_dir = /var/drweb/
```

FreeBSD:

```
%bin_dir = /usr/local/drweb/
%etc_dir = /usr/local/etc/drweb/
%var_dir = /var/drweb/
```

システム要件

Dr.Web for UNIX mail serversは、以下の要件を満たすシステムで使用する

ことができます。

対応OS:

- Linux（カーネル2.4.x 以降）
- FreeBSD 6.x以降（Intel x86）
- Solaris 10（Intel x86）

32bit/64bit（x86_64）環境に対応していますが、64bit環境では32bitアプリケーションの動作をサポートする必要があります。

例:

32bitアプリケーションの動作を有効にするためには、Debian/Ubuntu Linux では`ia32-libs`ライブラリが、ALT Linux では`i586-glibc-core`ライブラリが必要です。

Dr.Web for UNIX mail servers ハードウェアの要件は、コマンドラインインターフェース（CLI）ハードウェアの要件と同じです。**Dr.Web for UNIX mail servers**ソリューションのインストールに必要なディスク空き容量は最大で165Mbです。

Dr.Web for UNIX mail serversのグラフィカルインストーラーが適切に動作するにはX Windowシステムが必要です。ポストインストールスクリプトのグラフィカルモードでの動作を効にするにはxtermまたはxvdターミナルエミュレータがインストールされている必要があります。

また、システムに以下のパッケージがインストールされていることが必要です。

- `libglade2`
- `libgtk2`
- `libstdc++6`
- `base64`
- `unzip`
- `crond`

ハードウェア要件は**Dr.Web for UNIX mail servers**ソリューションによって解決する問題の範囲、及び操作中のシステム負荷の合計によって大幅に異なります。

パッケージファイルロケーション

Dr.Web for UNIX mail serversソリューションはデフォルトで%bin_dir、%etc_dir、%var_dirディレクトリにインストールされます。これらのディレクトリ内にOSに依存しないディレクトリツリーが作成されます。

- %bin_dir – **Dr.Web for UNIX mail servers** ソリューションの実行可能モジュール、及びアップデートモジュール**Dr.Web Updater**（Perlスクリプト update.pl）。
- %bin_dir/lib/ – ローダブルライブラリとしてのアンチウイルスエンジン（drweb32.dll）。同じサブディレクトリ内に**Dr.Web for UNIX mail servers**ソリューションパッケージ向けの様々なサービスライブラリを置くことができます。
- %bin_dir/agent/ – **Dr.Web Agent**モジュールの追加設定ファイルです。
- %etc_dir/monitor/ – **Dr.Web Monitor**モジュールの追加設定ファイルです。
- %bin_dir/maild/scripts/ – プラグイン、及び様々なMTAに対する設定スクリプト、**Dr.Web for UNIX mail servers**ソリューションのコンフィギュレーションのバージョン4.44から5.0へのアップグレードを実行するマイグレーションスクリプト。
- %bin_dir/doc/ — ドキュメンテーション。全てのドキュメンテーションは英語及びロシア語のプレーンテキストファイル（KOI8-R 、UTF-8 エンコード）になっています。
- %var_dir/bases/*.vdb — 既に知られているウイルスのデータベースです。
- %etc_dir — **Dr.Web for UNIX mail servers**ソリューションの設定ファイルであるdrweb32.ini、 agent.conf、monitor.conf、plugin_NAME.conf、maild_MTA.conf、drwebd.enable、drweb-monitor.enableです（最後の2つはデーモンの動作の調整に使われます）。
- %bin_dir/lib/ru_scanner.dwl — **Dr.Web Scanner**及び**Dr.Web Daemon**パッケージの言語ファイルです。
- %etc_dir/maild/templates/ — メッセージ内で悪意のあるオブジェクトを検出した時や、**Daemon**またはプラグインの動作中にエラーが発生した後に、異なる種類の受信者に送信する通知のテンプレートです。
- %bin_dir/web/ — **Dr.Web for UNIX mail servers**のウェブイ

ンターフェースを持ったウェブミンパッケージです（drweb-maild-web.wbm.gz）。

- %var_dir/infected/ – 感染した、または感染が疑われるファイルを移動させる隔離ディレクトリです（**Dr.Web**ソフトウェアシステムコンポーネントの設定でそのような動作が指定されていた場合）。

設定ファイル

Dr.Web for UNIX mail serversシステムコンポーネントのセットアップには設定ファイルが使われます。設定ファイルは次の構造を持ったプレーンテキストファイルです（どのテキストエディターでも編集できるようになっています）。

```
--- beginning of the file ---
[Section 1 name]
Parameter1 = value1, ..., valueK
...
ParameterM = value1, ..., valueK
...
[Section X name]
Parameter1 = value1, ..., valueK
...
ParameterY = value1, ..., valueK
--- end of the file ---
```

";" または "#" で始まる行は、コメント行です。コメントアウトされた行は、設定ファイルのパラメータを読み込むときにスキップされます。コメント行、または値が指定されていないパラメータの場合は、ハードコード化されたデフォルト値が使用されます。

不正なパラメータが指定されている場合、**Dr.Web for UNIX mail servers**はエラーメッセージを出力して終了します。設定ファイルに未知のパラメータを見つけると、**Dr.Web for UNIX mail servers**はログファイルに警告を出力し続けます。

パラメータ値は引用符で囲むことが出来ます（空白文字を含む場合は引用符で囲まれていなくてはなりません）。パラメータの中には、複数の値を持つことが出来るものがあります。そのような値はカンマで区切ることが出来、またそれぞれの値を設

定ファイルの別々のストリング内で設定することが可能です。複数の値を持つかどうかは、パラメータ記述内に明記されています。

例:

カンマで区切られた複数の値:

Names = XXXXX, YYYYY

複数のストリング内に設定された複数の値

Names = XXXXX

Names = YYYYY

本書ではパラメータは全て次のように記述します。

ParameterName = {parameter type | possible values}

パラメータ記述。

{複数の値を持つ可能性}

デフォルト値:

ParameterName = {value | empty}

パラメータは、該当する設定ファイル内での順番通りに記述されます。

パラメータにはいくつかの種類があり、それぞれ以下の値を指定することができます。

- numerical value - 0以上の整数。
- time - 時間を示す0以上の整数。

  s 秒
  m 分
  h 時
  d 日

  例: 30s, 15m
- size - ファイルサイズなどを示す0以上の整数。

  b バイト

k　キロバイト
m　メガバイト
g　ギガバイト

例: 20b, 15k

大文字と小文字は区別しません。単位が省略された場合はバイトで値が設定されます。

- permissions – ファイルとディレクトリに与えられるアクセス権を示す数値。

  例: 755 (-rwxr-xr-x), 644 (-rw-r--r--)

- path to file/directory – ファイルまたは、ディレクトリへのパス。
- actions – 実行される動作、処理(パラメータごとに実行可能な動作が異なるため、それぞれのパラメータで説明があります)。必須、及び任意の2つのタイプのアクションがあります。**Dr.Web MailD** では必須のアクションを1つ、任意のアクションを3つまで指定することが出来ます。必須アクションは常にリストの最初にきます。**Dr.Web Scanner** に対して指定出来るアクションは1つだけです。

  使用出来る必須アクション:

  - Cure – 感染したオブジェクトの修復及びメッセージのリパック。
  - Remove – 感染したオブジェクトの削除及びメッセージのリパック。
  - Discard – 送信者にその旨の通知を出さずにメッセージを拒否。
  - Pass – メッセージを渡す。
  - Reject – 送信者にその旨の通知を出してメッセージを拒否。
  - Tempfail – メッセージが一時的に送信されない旨を送信者に通知。

  使用出来る任意のアクション:

  - Quarantine – メッセージを隔離に移動。
  - Redirect [(address[|address|...])] – 角括弧内に指定されたアドレスにメッセージを転送。アドレスが指定されていない場合、メッセージは [MailD]セクション内の**RedirectMail**パラメータ値で定義されたアドレスに送られます。"|" 記号で区切ることによって複数のアドレスを指定することが可能で

す。

- Notify – 検出した脅威に関するレポートを送信。メッセージの処理は続けられます。
- Add-header (HEADER) – メッセージにHEADER を追加。HEADERは [NAME:]BODYで指定され、 NAME はヘッダー名で(デフォルトではX-DrWeb-MailD)、BODY はヘッダーの値です。
- Score (SCORE) – メッセージスコアにSCOREを追加。SCOREの値はマイナスの場合があります。

Dr.Web Scannerで使用出来るアクション:

- Cure – 感染したオブジェクトの修復。
- Delete – 感染したオブジェクトの削除。
- Rename – 感染したオブジェクトのリネーム。
- Move – ファイルを隔離に移動。
- Ignore – ファイルをスキップ。
- Report – 情報のログへの出力のみ。

- address – **Dr.Web for UNIX mail servers** コンポーネントと外部パッケージのソケット。 これらのパラメータは TYPE:ADDRESSで指定されます。使用出来るアドレスタイプは次のとおりです。
  - inet – TCPソケットをPORT@HOST_NAMEの形式で指定します。HOST_NAMEは、ホスト名・IPアドレスのどちらでも指定できます。

    例:

    Address = inet:3003@127.0.0.1
  - local – ローカルのUNIXソケットをソケットファイルへのパスで指定します。

    例:

    Address = local:%var_dir/.daemon
  - PID – プロセスの実アドレスは、そのPIDファイルから読み込まれる必要があります。 指定可能な場合、個々のパラメータの説明で記載があります。
- text value – パラメータ値はテキスト文字列で、引用符で囲むことが出来ます(空白を含む場合は引用符で囲まれていなくてはなりません)。

- pool options – スレッドプールの設定。

  最初は、プール内のスレッド数は定義されています。

  - auto – プール内のスレッド数は現在のシステムロードに応じて自動的に検出されます。
  - N – 負ではない整数。プール内の少なくとも N 個のスレッドがアクティブになります。要求に応じて新しいスレッドが作成されます。
  - N-M – 正の整数で、M = N。プール内の少なくとも N 個のスレッドがアクティブになります。要求に応じて新しいスレッドがM個まで作成されます。

  さらに、以下の追加パラメータを指定することが出来ます。

  - timeout = {time} – 指定された時間内にスレッドがアクティブにならなかった場合、そのスレッドは閉じられます。このパラメータは最初のNスレッドには影響を与えず、それらは要求を待ち続けます。

    デフォルト値: 2m
  - stat = {yes|no} – プール内にあるスレッドの統計。SIGUSR1システムシグナルを受け取るたびに、[General]セクションからの**BaseDir**パラメータ値で指定されたディレクトリに保存されます。

    デフォルト値: no
  - log_level = {Quiet|Error|Alert|Info|Debug} – プール内にあるスレッドに対するログの詳細レベル。値が明確に指定されていない場合は[Logging]セクションからの**LogLevel**パラメータ値が使われます。
  - stop_timeout = {time} – 動作しているスレッドが停止するまでの時間の上限(プログラムが動作を終了、またはプール内のスレッド数を減らす必要がある場合など)。

  例:

  InPoolOptions = auto, timeout=1m, stat = yes

  スレッド数は自動的に検出されます。それを過ぎるとスレッドが動作していないと見なされるタイムアウトは1分に設定され、統計が収集されます。
- string – コンマによって区切られたテキスト値のセットです。パラメータ値がfile:/path_to_fileフォーマットで設定されている場合、テキ

スト値は path_to_fileファイルから取られます。このファイル内でテキスト値はそれぞれ別々のラインで指定されなくてはなりません。値をpath_to_fileファイルから読み込むことが出来ない場合、エラーに関する通知がログに出力され、プログラムは続けて実行されます。

- lookups – オブジェクト内の検索を実行、またそれらの値を受け取るための一般インターフェース。値はコンマによって区切られています。値の前に検索の種類を特定するプレフィックスを置くことが出来ます。[PREFIX1:]VALUE。1, [PREFIX2:]VALUE2, ... プレフィックスが指定されていない場合、値のみが使われます。使用出来るプレフィックスは以下のとおりです。
    - file – ファイルへのパス。ファイル内の値はそれぞれ新しいライン上になくてはなりません。 ファイル内でソート、及びバイナリサーチを使うことができるので、最も速く検索することが出来ます。
    - regex – 正規表現（Perlシンタックス）はサブストリングとして検索されます。完全に適合する必要ありません。
    - rfile – ファイルへのパス。ファイルには正規表現（Perlシンタックス）のセットが含まれ、それらはそれぞれ新しいライン上になくてはなりません。
    - ldap – LDAPサーバ上でパスを検索。
    - odbc, oracle – ODBCまたはOracleデータベースに対するSQL要求。
    - postgres – PostgreSQL データベースに対するSQL要求。
    - cdb – CDBデータベースに対する要求（例えばデータベースキーのテキスト名）。CDBデータベースはSQLシンタックスには対応していません。対応しているのは[text key]:[text value] 要求のみです。
    - berkeley – Berkeleyデータベースに対する要求。
    - firebird – Firebirdデータベースに対するSQL要求。
    - sqlite – SQLiteデータベースに対するSQL要求。
    - mysql – MySQLデータベースに対するSQL要求。
- LookupsLite – 1つの点を除いてlookupsと同じです。このタイプでは値そのものか、またはfileタイプの検索のみ使うことが出来ます。
- storage – データを保存するオブジェクト。プレフィックスの種類が異なり、また $sマクロを使用することが出来ないという点を除いてlookupsと

同じシンタックスです。

使用出来るプレフィックスは以下のとおりです。

- odbc – シンタックスはLDAPに対する要求と同じです。SQL要求では、値は：name<type> フォーマットで指定されます。 name は保存するオブジェクトの名前（パラメータごとにそれぞれ独自の、使用できる名前のリストが使われます）で、typeはデータベースに記録される時に使われるパラメータの種類です。
- oracle – シンタックスはODBCに対する要求と同じです。
- postgres, mysql, sqlite, firebird – シンタックスは1つの点を除いてODBCに対する要求と同じです。char(length) タイプには対応していません。ストリングデータにはvarchar_longタイプを使う必要があります。

例:

"odbc:insert into plugin_stat values (:plugin_name<varchar_long>, :size<int>, :num<int>)";

この要求ではカンマが使われているため、引用符が必要であることに注意してください。

- TLS Settings – TLS及びSSL暗号化通信設定。設定フォーマットは PARAMETER VALUEです。PARAMETER VALUEのペアはカンマで区切られています。VALUEがファイルへのパスである場合、大文字と小文字の区別をします。現在のバージョンでは以下の設定に対応しています。
  - **use_sslv2** {yes | no} – SSLv2プロトコル使用のトグル。このプロトコルは安全ではないので、デフォルトでは使用は無効になっています。
  - **use_sslv3** {yes | no} – SSLv3プロトコル使用のトグル。デフォルトでは有効です。
  - **use_tlsv1** {yes | no} – TLSv1プロトコル使用のトグル。デフォルトでは有効です。
  - **private_key_file** {path to the file} – プライベートキーファイルへの絶対パス。キーはPEMフォーマットでなくてはならず、また暗号化することが出来ます。サーバコンフィギュレー

ションにはパラメータが必要です。パラメータの値はデフォルトでは指定されていません。

- **private_key_password** {string} - **private_key_file**パラメータで指定されたキーに対するパスワード。パラメータ値はデフォルトでは指定されていません。
- **certificate** {path to the file} - 署名付きパブリックキーがある証明書のファイルへのパス。このパラメータの値は**private_key_file**パラメータの値と一緒に指定する必要があります。サーバコンフィギュレーションにはこのパラメータが必要です。パラメータの値はデフォルトでは指定されていません。
- **verify_mode** {none | peer | client_once | fail_if_no_peer_cert} - ピア証明書を検証するモードを設定。
  - ✓ none - ピア証明書の検証をスキップします。デフォルトではこの値が設定されています。
  - ✓ peer - ピア証明書を検証します。サーバが匿名暗号化に対する証明書を送信しない場合、クライアントモードではこのパラメータは無視されます。クライアント接続ではこれがデフォルト値です。
  - ✓ client_once - 初めて接続された時にのみサーバが証明書を要求するようにします。このパラメータのpeer値と一緒にのみ使用することが可能です。
  - ✓ fail_if_no_peer_cert - クライアント証明が無い場合にエラーとして扱うようサーバを設定します。値はこのパラメータのpeer値と一緒にのみ使用することが可能です。

例:

verify_mode peer, verify_mode client_once

verify_mode none

peer と none が同じブロック内にある場合、最後に指定された値が使われます。

- **verify_ca** {the path to a file | the path to a directory} – PEMフォーマットのCA証明書があるファイルまたはディレクトリへの絶対パス。これらの証明書はピアの証明書を検証するのに使われます。
- **cipher_list** {string} – 使用出来る暗号化アルゴリズムのリスト。リストのフォーマットに関する情報を得るにはman ciphersコマンドを使用します(OpenSSLがインストールされている必要があります)。

- value – パラメータの中には、上記以外のタイプを持つことが出来るものもあります。

Dr.Web MailDコンポーネントへのロギングは非常に詳細(Debug値が指定されている場合)、または完全に省略される(Quiet値が指定されていて、どの情報もロギングされない場合)ことがあります。ログの詳細レベルの設定にはQuiet、Error、Info、Alert、Notice、Warning、Verbose、Debugの値を使用します。

全ての**Dr.Web MailD**コンポーネントにQuiet、Error、Alert、Info、Debugのログの詳細レベルを使用します。

Dr.Web Daemon 及び **Dr.Web Scanner** コンポーネントは Error、Info、Notice、Warning、Alertのレベルで動作します。

Dr.Web Updaterコンポーネントには Quiet、Error、Alert、Info、Debug、Verboseのレベルを使用します。

インストールとアンインストール

本章では、**Dr.Web for UNIX mail servers**のインストールとアンインストールについて説明しています。記載されている手順は、root権限で実行する必要があります。

古いバージョンのパッケージ（rpmまたはdebフォーマットの）を全て、アンインストールする必要があります。

Dr.Web for UNIX mail serversのUNIXシステム向けディストリビューションパッケージは、ESP Package Manager（EPM）形式のパッケージを使用することができるEPMフォーマットです（インストール／アンインストールのスクリプト、及び標準GUIを含んだスクリプトベースのディストリビューションパッケージ）。これらのスクリプトは全て、**Dr.Web for UNIX mail servers**のコンポーネントではなくEPMパッケージ自体のものです。

Dr.Web for UNIX mail serversのインストールとアンインストール、及びアップグレードは以下の方法で行うことが出来ます。

- インストール／アンインストールGUI経由で
- インストール／アンインストール用コンソールスクリプト経由で

インストールの際には依存関係が判断されます。例えば、あるコンポーネントをインストールする場合、他のコンポーネントがいくつかインストールされている必要があり（例えば、`drweb-daemon`パッケージをインストールするには`drweb-common`及び`drweb-bases`がインストールされている必要があります）、それらは自動的にインストールされます。

EPMパッケージからの他の**Dr.Web**製品がいくつかインストールされているコンピューターに**Dr.Web for UNIX mail servers**をインストールする場合、アンインストールGUI経由でモジュールを削除しようとする度に、他の製品のものを含む全ての**Dr.Web**モジュールを削除するように要求されます。

必要なコンポーネントを誤って削除してしまわないよう、アンインストールの際に実行する動作と選択は慎重に行うようにしてください。

Distribution Package for UNIX systemsからのインストール

Dr.Web for UNIX mail serversは、自己抽出パッケージとして提供されます。

drweb-mail-[product-name]_[version number]~[OS name].run

パッケージには、以下のコンポーネントが含まれています。

- drweb-common: 設定ファイル(drweb32.ini)、ライブラリ、ドキュメント、ディレクトリ構造。インストールの際に、drwebユーザとdrwebグループが作成されます。
- drweb-bases: ウイルス検査エンジン、ウイルス定義ファイル。drweb-commonパッケージがインストールされている必要があります。
- drweb-libs: すべてのコンポーネントに必要な共通ライブラリ
- drweb-epm6.0.0-libs: GUIインストーラ・アンインストーラのライブラリ。drweb-libsパッケージがインストールされている必要があります。
- drweb-epm6.0.0-uninst: GUIアンインストーラに必要なファイル。drweb-epm6.0.0-libsパッケージがインストールされている必要があります。
- drweb-boost144: **Dr.Web Agent**と**Dr.Web Monitor**の共通ライブラリ。drweb-libsパッケージがインストールされている必要があります。
- drweb-updater: ウイルス検査エンジンとウイルス定義ファイルのアップデートユーティリティ。drweb-common、drweb-libsパッケージがインストールされている必要があります。
- drweb-agent:**Dr.Web Agent**の実行ファイル、ドキュメント。drweb-common、drweb-boost144パッケージがインストールされている必要があります。
- drweb-daemon: **Dr.Web Daemon**の実行ファイル、ドキュメント。drweb-bases、drweb-libsパッケージがインストールされている必要があります。
- drweb-scanner: **Dr.Web Scanner**の実行ファイル、ドキュメン

ト。drweb-bases、drweb-libsパッケージがインストールされている必要があります。

- drweb-monitor: **Dr.Web Monitor**の実行ファイル、ドキュメント。 drweb-common、drweb-boost144パッケージがインストールされている必要があります。
- drweb-maild: **Dr.Web MailD**の実行ファイル、ドキュメント。drweb-maild-commonパッケージがインストールされている必要があります。
- drweb-maild-common: **Dr.Web Agent**、**Dr.Web Monitor**、**Dr.Web MailD**のライブラリ。 drweb-common、drweb-gperftools0、 drweb-agent、drweb-monitor パッケージがインストールされている必要があります。
- drweb-maild-plugin-drweb: drwebプラグインとその設定ファイル、ドキュメント、コンフィギュレーションスクリプトのライブラリ。drweb-maild パッケージがインストールされている必要があります。
- drweb-maild-web: **Dr.Web for UNIX mail servers**のウェブインターフェース。
- drweb-maild-plugin-headersfilter: headersfilterプラグインとその設定ファイル、ドキュメント、コンフィギュレーションスクリプトのライブラリ。drweb-maild パッケージがインストールされている必要があります。
- drweb-maild-plugin-modifier: modifierプラグインとその設定ファイル、ドキュメント、コンフィギュレーションスクリプトのライブラリ。drweb-maild パッケージがインストールされている必要があります。
- drweb-maild-plugin-vaderetro: vaderetroプラグイン、ドキュメント、コンフィギュレーションスクリプトの設定ファイル。drweb-maild、drweb-libvaderetro パッケージがインストールされている必要があります。
- drweb-libvaderetro: vaderetroプラグインのライブラリ。
- drweb-maild-smtp: **Dr.Web for UNIX mail servers**がSMTP及びLMTPプロトコルのプロキシサーバとして動作出来るようにする**Sender**及び**Receiver**モジュールの実行ファイル、**Dr.Web Monitor**の該当する設定、ドキュメント、コンフィギュレーションスクリプトを含んだ**Dr.Web MailD** 設定ファイル。drweb-maild パッケージがインストールされている必要があります。
- drweb-maild-cgp: Communigate Pro MTA(mail transfer agent)とのインタラクションを可能にする**Sender**及び**Receiver**モジュー

ルの実行ファイル、特定のMTAに対する設定を含んだ**Dr.Web MailD**設定ファイル、ドキュメント、**Dr.Web MailD**とのインタラクションを調整する為のCommunigate Proコンフィギュレーションスクリプト。`drweb-maild` パッケージがインストールされている必要があります。

- `drweb-maild-courier`: Courier MTA(mail transfer agent)とのインタラクションを可能にする**Sender**及び**Receiver**モジュールの実行ファイル、特定のMTAに対する設定を含んだ**Dr.Web MailD**設定ファイル、 ドキュメント、**Dr.Web MailD**とのインタラクションを調整する為のCourierコンフィギュレーションスクリプト。`drweb-maild`パッケージがインストールされている必要があります。
- `drweb-maild-exim`: Exim MTA(mail transfer agent)とのインタラクションを可能にする**Sender**及び**Receiver**モジュールの実行ファイル、特定のMTAに対する設定を含んだ**Dr.Web MailD**設定ファイル、 ドキュメント、**Dr.Web MailD**とのインタラクションを調整する為のEximコンフィギュレーションスクリプト。`drweb-maild`パッケージがインストールされている必要があります。
- `drweb-maild-postfix`: Postfix MTA(mail transfer agent)とのインタラクションを可能にする**Sender**及び**Receiver**モジュールの実行ファイル、特定のMTAに対する設定を含んだ**Dr.Web MailD**設定ファイル、 ドキュメント、**Dr.Web MailD**とのインタラクションを調整する為のPostfixコンフィギュレーションスクリプト。`drweb-maild`パッケージがインストールされている必要があります。
- `drweb-maild-qmail`: Qmail MTA(mail transfer agent)とのインタラクションを可能にする**Sender**及び**Receiver**モジュールの実行ファイル、特定のMTAに対する設定を含んだ**Dr.Web MailD**設定ファイル、ドキュメント、**Dr.Web MailD**とのインタラクションを調整する為のQmailコンフィギュレーションスクリプト。`drweb-maild`パッケージがインストールされている必要があります。
- `drweb-maild-sendmail`: Sendmail MTA(mail transfer agent)とのインタラクションを可能にする**Sender**及び**Receiver**モジュールの実行ファイル、特定のMTAに対する設定を含んだ**Dr.Web MailD**設定ファイル、 ドキュメント、**Dr.Web MailD**とのインタラクションを調整する為のSendmailコンフィギュレーションスクリプト。`drweb-maild`パッケージがインストールされている必要があります。
- `drweb-maild-zmailer`:ZMailer MTA(mail transfer agent)とのインタラクションを可能にする**Sender**及び**Receiver**モジュールの実行ファイル、特定のMTAに対する設定を含んだ**Dr.Web MailD**設定ファイル、 ドキュメント、**Dr.Web MailD**とのインタラクションを調整する為のZMailerコンフィギュレーションスクリプト。`drweb-maild`パッケージがインストールされている必要があります。

- drweb-gperftools0: **Dr.Web MailD**が使用するGoogleパフォーマンスツールのライブラリ。drweb-libs パッケージがインストールされている必要があります。
- drweb-mail-servers-gateways-doc: 英語及びロシア語の管理者マニュアルです。

64bit版のパッケージにはdrweb-libs64が含まれています。

Dr.Web for UNIX mail serversのすべてのコンポーネントを自動的にインストールするためにコンソール(CLI)または、GUIベースのシェルを使用することができます。前者の場合、以下のようなコマンドでインストールパッケージに実行権を与えてください。

```
# chmod +x drweb-mail-[product-name]_[version number]~[OS name].run
```

パッケージを実行します。

```
# ./drweb-mail-[product-name]_[version number]~[OS name].run
```

drweb-mail-[product-name]_[version number]~[OS name] の形式でディレクトリが作成され、 GUIインストーラが起動します。root権限がない場合は、rootのパスワードを要求されます。

GUIインストーラが起動しない場合は、コンソール(CLI)のインストーラが起動します。

インストールを開始せずに、パッケージの抽出のみを行う場合は、以下のように --noexecパラメータを指定します。

```
# .drweb-mail-[product-name]_[version number]~[OS name].run --noexec
```

パッケージの抽出を行ったあとに以下のコマンドを実行して、GUIインストーラを起動することもできます。

```
# drweb-mail-[product-name]_[version number]~[OS name]/install.sh
```

コンソールインストーラを起動するには以下のコマンドを使用します。

```
# drweb-mail-[product-name]_[version
```

number]~[OS name]/setup.sh

インストールによって以下の処理が行われます。

- オリジナルの設定ファイルが[configuration_file_name].N.という名前で%etc_dir/software/conf/ディレクトリに保存されます。
- 設定ファイルのコピーがインストールソフトウェアの該当するディレクトリに配置されます。
- その他のファイルがインストールされます。既に同じ名前のディレクトリファイルが存在する場合（旧バージョンのアンインストールが適切に行われなかった場合など）は、新しいファイルで上書きし、古いファイルのコピー（[file_name].O）が保存されます。ディレクトリ内に[file_name].Oファイルが既に存在する場合は、それが新しいファイルに置き換えられます。
- グラフィカルインストーラの該当するウィンドウで**Run interactive postinstall script**チェックボックスを選択した場合、コンポーネントがインストールされた後、**Dr.Web for UNIX mail servers**の基本的な調整のためにポストインストールスクリプトが起動します。

GUIインストーラによるインストール

GUIを使ってインストールするには

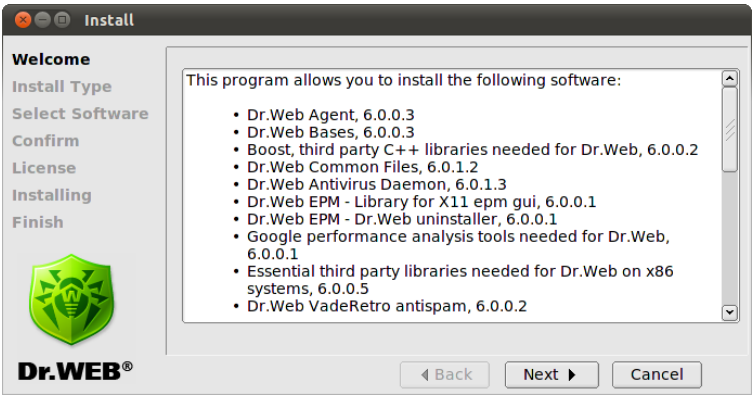
1. 以下のコマンドを実行します。

   ```
   # drweb-mail-[product-name]_[version number]~[OS name]/install.sh
   ```

   セットアッププログラムが起動します。**"Next"** をクリックして次に進みます。インストールを終了する場合は、**"Cancel"** をクリックします。

2. 起動画面で**"Next"** をクリックしてください。

図1. 起動画面



3. インストール種別の選択画面が表示されます。

図2. MTAのインストール種別画面

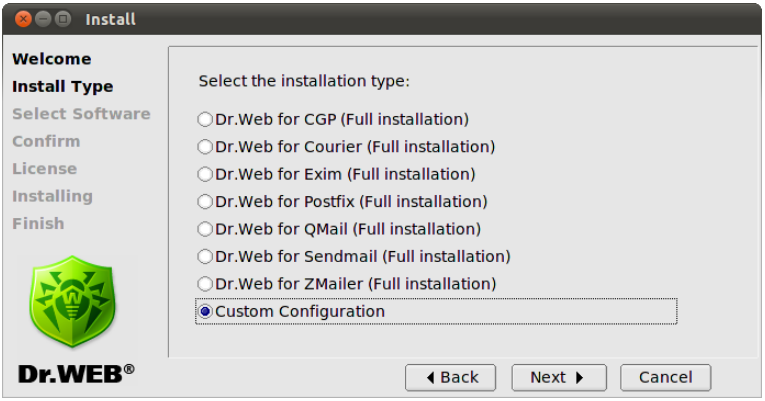
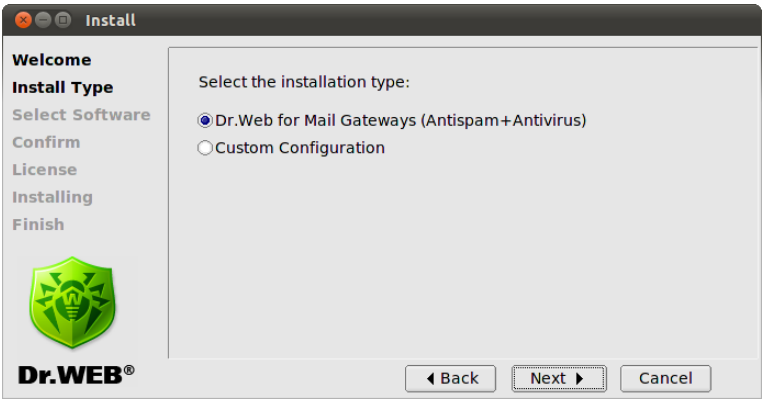
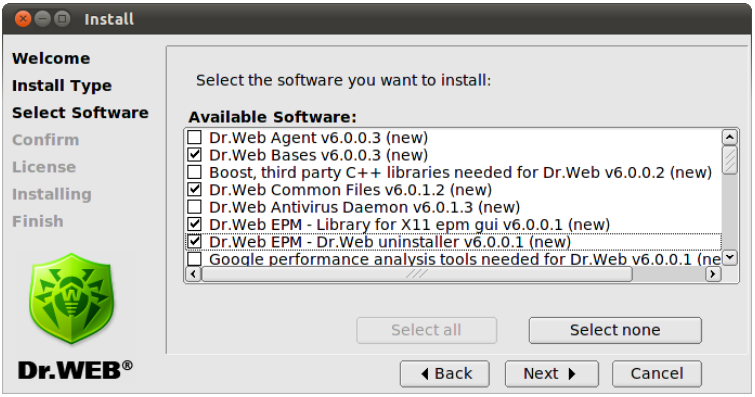


図3.Dr.Web for Mail Gatewaysのインストール種別画面



"Custom Configuration"を選択した場合、**Select Software**画面で必要なコンポーネントを選択してください。

図4. Select Software画面



インストールするソフトウェアの選択時に依存関係の確認が自動的に行われます。

例）**Dr.Web Antivirus Daemon** を選択すると、**Dr.Web Bases** と **Dr.Web Common Files** も一緒に選択されます。

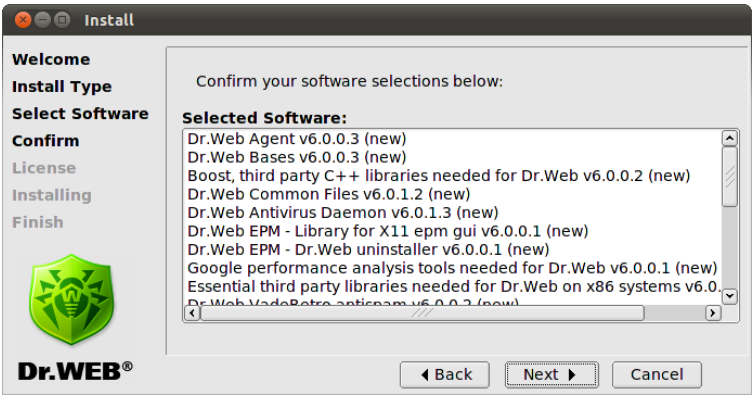
インストールの際に、異なるMTA向けのパッケージはお互いに競合する場合があります（drweb-maild-smtpと様々なdrweb-maild-MTA）。例えば、**Dr.Web Mail Daemon – Exim Connector** と **Dr.Web Mail Daemon – Postfix Connector**を同時にインストールしようとした場合、エラーメッセージを受け取りどれか1つを選択するように要求されます。

"Select None" をクリックすると、すべての選択が解除されます。

選択が終了したら **"Next"** をクリックしてください。

2. **Confirm**画面でインストールするコンポーネントを確認してください。

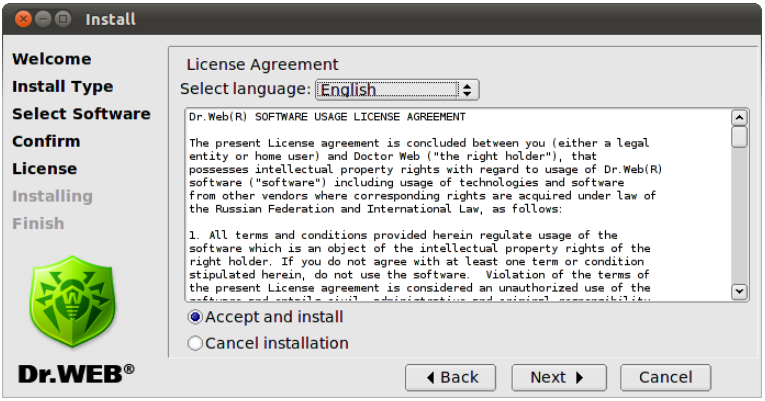
図5.Confirm画面



選択を確認して**"Next"**をクリックします。変更するには**"Back"**をクリックしてください。

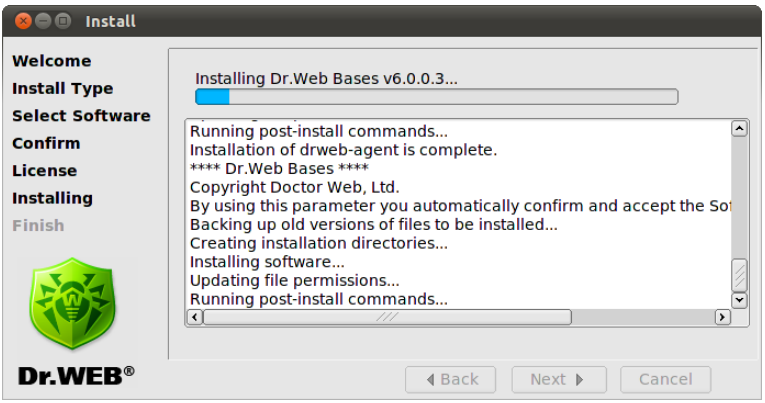
3. ソフトウェア使用許諾契約が表示されます。インストールを続けるには同意してください。必要に応じ、**Language**リストで言語を選択してください。

図6.ソフトウェア使用許諾契約



4. 上記3でソフトウェア使用許諾契約に同意した場合は、インストールが開始されます。 **Installing**画面でインストールのプロセスをリアルタイムで確認することが出来ます。

図7. Installing画面



インストール処理のログは、`drweb-mail-[product-name]_`

[version number]~[OS name]ディレクトリのinstall.logファイルに記録されます。**"Run interactive postinstall script"**を選択した場合、コンポーネントのインストールが完了すると、 **Dr.Web for UNIX mail servers**基本設定を行うポストインストールスクリプトが起動します。

図8. インタラクティブポストインストールスクリプト

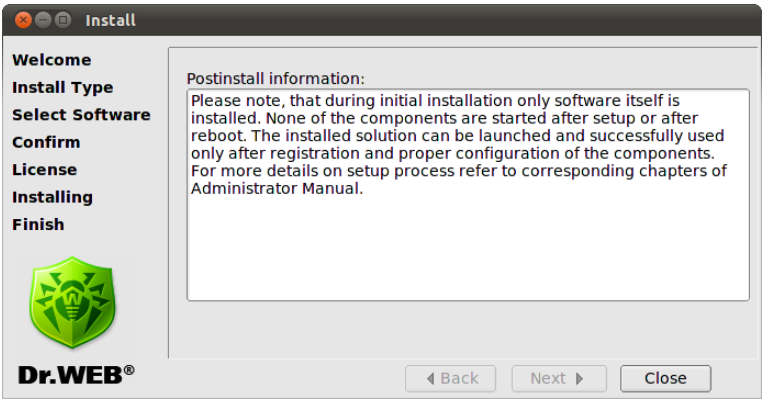
```
DrWeb
This installation script will help you to configure DrWeb for Mail server Antivirus+Antispam

Do you want to continue? (YES/no)
yes

Enter list of plugins to process message before placing it to queue/DB.
Possible values: (headersfilter|modifier). Values are delimited with commas.
 [default=]:modifier

Enter list of plugins to process message after placing it to queue/DB.
Possible values: (headersfilter). Values are delimited with commas.
 [default=]:headersfilter

Enter email address to send notifications to.
 [default=postmaster@localhost]:

Enter email address to send notifications from.
 [default=DrWEB-MAIL-DAEMON@localhost]:

Enter list of protected networks (e.g. 127.0.0.0/8). Values are delimited with commas.
 [default=127.0.0.0/8]:

Enter list of protected domains. Values are delimited with commas.
 [default=localhost]:

Enter language(s) to use in reports.
Possible values: (en|ja|ru). Values are delimited with commas.
 [default=en]:


==============
Configuration:

Plugins directory = /opt/drweb/maild/plugins
lng files directory = /etc/drweb/maild/lng
Before queue plugins = modifier
After queue plugins = headersfilter
Administrator email address = postmaster@localhost
Filter email address = DrWEB-MAIL-DAEMON@localhost
Protected networks = 127.0.0.0/8
Protected domains = localhost
Language(s) for reports = en

Press 1 to Save updated configuration,
2 to go Back to editing, 3 to Cancel or 5 to Redisplay [1]
```

キーファイルへのパスを指定し、**Dr.Web for UNIX mail servers**の正常な動作に必要なサービス(**Dr.Web Daemon**、**Dr.Web Agent**、**Dr.Web Monitor**など)を自動的に有効にするよう、このスクリプトに要求されます。

図9. MTAの設定、サービスを自動で起動

5. **Finish**画面で、**Dr.Web for UNIX mail servers**の正常な動作に必要なインストール後の設定に関する情報を確認します。

図10. 終了画面



"Close"をクリックしてセットアップを終了します。

コンソールインストーラによるインストール

GUIインストールが行えない場合、自動的にコンソールインストーラが開始されます。また、コンソールインストーラを起動できない場合（必要な権限が無い場合など）は以下のコマンドを使用して手動で開始することも可能です。

```
# drweb-mail-[product-name]_[version number]~[OS name]/setup.sh
```

コンソールからインストールするには

1. コンソールインストーラが起動すると、対話式ウィンドウが表示されます。

```
user@hostname: ~
Файл  Правка  Вид  Поиск  Терминал  Справка

This installation script will help you install DrWeb for Mail server Antivirus+Antispam

Do you want to continue? (YES/no)
```

2. **Dr.Web for UNIX mail servers**をインストールする場合、**Y** または **Yes** を入力します。インストールしない場合は、 **N** または **No** を入力します（大文字と小文字は区別しません）。ENTERキーを押してください。
3. インストールの種別を選択する画面が表示されます。

```
user@hostname: ~
Файл  Правка  Вид  Поиск  Терминал  Справка
Select the installation type:
        1       Dr.Web for CGP (Full installation)
        2       Dr.Web for Courier (Full installation)
        3       Dr.Web for Exim (Full installation)
        4       Dr.Web for Postfix (Full installation)
        5       Dr.Web for QMail (Full installation)
        6       Dr.Web for Sendmail (Full installation)
        7       Dr.Web for ZMailer (Full installation)
        8       Custom Configuration

Choose one configuration to install [1] :
```

実行したいインストール種別の番号を入力し、ENTERキーを押してください。

4. **"Custom Configuration"** を選択した場合、コンポーネントを選択する画面が表示されます。

```
user@hostname: ~
Файл  Правка  Вид  Поиск  Терминал  Справка
        [ ] 16 Dr.Web Mail Daemon - Dr.Web plugin v6.0.0.2 (new)
        [ ] 17 Dr.Web Mail Daemon - HeadersFilter plugin v6.0.0.2 (new)
        [ ] 18 Dr.Web Mail Daemon - Modifier plugin v6.0.0.2 (new)
        [ ] 19 Dr.Web Mail Daemon - VadeRetro plugin v6.0.0.2 (new)
        [ ] 20 Dr.Web Mail Daemon - Postfix connector v6.0.0.2 (new)
        [ ] 21 Dr.Web Mail Daemon - qmail connector v6.0.0.2 (new)
        [ ] 22 Dr.Web Mail Daemon - Sendmail connector v6.0.0.2 (new)
        [ ] 23 Dr.Web Maild Web Interface v6.0.0.2 (new)
        [ ] 24 Dr.Web Mail Daemon - ZMailer connector v6.0.0.2 (new)
        [ ] 25 Dr.Web Mail Daemon v6.0.0.2 (new)
        [ ] 26 Dr.Web Monitor v6.0.0.3 (new)
        [ ] 27 Dr.Web Antivirus Scanner v6.0.1.3 (new)
        [ ] 28 Dr.Web Updater v6.0.0.4 (new)

To select a package you want to install or deselect some previously
selected package - enter the corresponding package number and press Enter.

You may enter A or All to select all the packages, and N or None to deselect all of the
m.
Enter I or Install to install selected packages.
Enter 0, Q or Quit to quit the dialog.
All values are case insensitive.
Select:
```

インストールするコンポーネントの番号を入力し、ENTERキーを押してください。

5. ソフトウェア使用許諾が表示されます。スペースキーでソフトウェア使用許諾のページを進めることができます。

```
user@hostname: ~
Файл  Правка  Вид  Поиск  Терминал  Справка
Dr.Web(R) SOFTWARE USAGE LICENSE AGREEMENT

The present License agreement is concluded between you (either a legal
entity or home user) and Doctor Web ("the right holder"), that
possesses intellectual property rights with regard to usage of Dr.Web(R)
software ("software") including usage of technologies and software
from other vendors where corresponding rights are acquired under law of
the Russian Federation and International Law, as follows:

1. All terms and conditions provided herein regulate usage of the
software which is an object of the intellectual property rights of the
right holder. If you do not agree with at least one term or condition
stipulated herein, do not use the software.  Violation of the terms of
the present License agreement is considered an unauthorized use of the
software and entails civil, administrative and criminal responsibility.

2. If you are a legal owner of the Software's copy, you receive the
non-exclusive and non-transferable right to use the software in any part
of the world limited to installing the software , launching and loading it
into the memory of a computer. Your legally obtained sixteen-character
alphanumeric code (serial number) is used to register and acquire a
license key file required to maintain operation of the Software in
--More--(23%)
```

インストールを続けるにはソフトウェア使用許諾に同意し、 **Y** または **Yes** を入力してください。インストールが開始されます。

6. すぐにインストールが開始されます。コンソールでインストールのプロセスをリアルタイムで確認することが出来ます。

```
user@hostname: ~
Файл  Правка  Вид  Поиск  Терминал  Справка

This installation script will help you to configure DrWeb for Mail server Antivirus+Ant
ispam

Do you want to continue? (YES/no) yes
yes

Enter path to key file for Dr.Web MailD.
If you don't have the key yet you can leave this value unspecified,
but you must set LicenseFile parameter value in configuration file agent.conf,
and parameter Key in configuration file drweb32.ini before MailD is
launched or any plugin is installed.
 [default=]:

Enter list of plugins to process message before placing it to queue/DB.
Possible values: (vaderetro|headersfilter|drweb|modifier). Values are delimited with co
mmas.
 [default=headersfilter]:headersfilter

Enter list of plugins to process message after placing it to queue/DB.
Possible values: (vaderetro|drweb|modifier). Values are delimited with commas.
 [default=modifier]:
```

7. インストール完了後、**Dr.Web for UNIX mail servers**の基本設定を行うポストインストールスクリプトが自動的に起動します。キーファイルへのパスを指定し、**Dr.Web for UNIX mail servers**の正常な動作に必要なサービス(**Dr.Web Daemon**、**Dr.Web Agent**、**Dr.Web Monitor**など)を自動的に有効にするよう、このスクリプトにに要求されます。

Distribution Package for UNIX Systemsのアンインストール

GUIアンインストーラ経由で**Dr.Web for UNIX mail servers**の全てのコンポーネントを削除するには、以下のコマンドを実行します。

```
# drweb-mail-[product-name]_[version number]~[OS name]/remove.sh
```

root権限がない場合は、rootのパスワードを要求されます。

GUIアンインストーラが起動しない場合は、インタラクティブコンソールアンインストーラが起動します。

アンインストール後、drwebユーザとdrwebグループを削除することができます。

アンインストールによって以下の処理が行われます。

- オリジナルの設定ファイルを`%etc_dir/software/conf/`ディレクトリから削除します。
- ユーザーによって設定ファイルが編集されていた場合は、ファイルを残します。
- **Dr.Web**のその他のファイルが削除されます。インストール時に古いファイルのコピーが作成されていた場合（通常`[file_name].O`という名前）、インストール前の名前で復元されます。
- ライセンスキーとログファイルは対応するディレクトリに残されます。

GUIインストーラによるアンインストール

GUIを使ってアンインストールするには

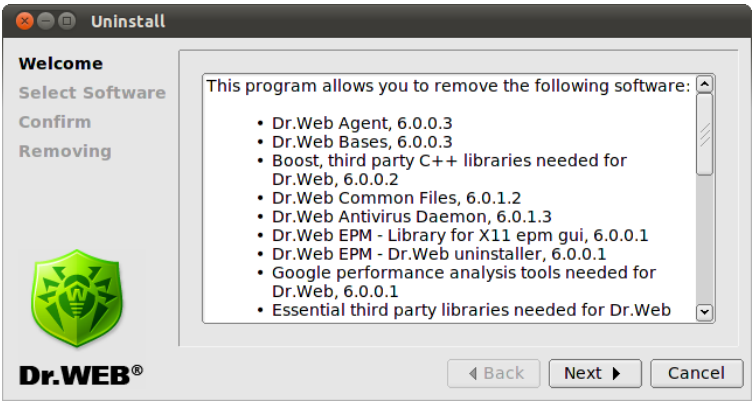
1. 以下のコマンドを実行します。

   ```
   # drweb-mail-[product-name]_[version number]~[OS name]/remove.sh
   ```

   セットアッププログラムが起動します。**"Next"** をクリックして次に進みます。インストールを終了する場合は、**"Cancel"** をクリックします。

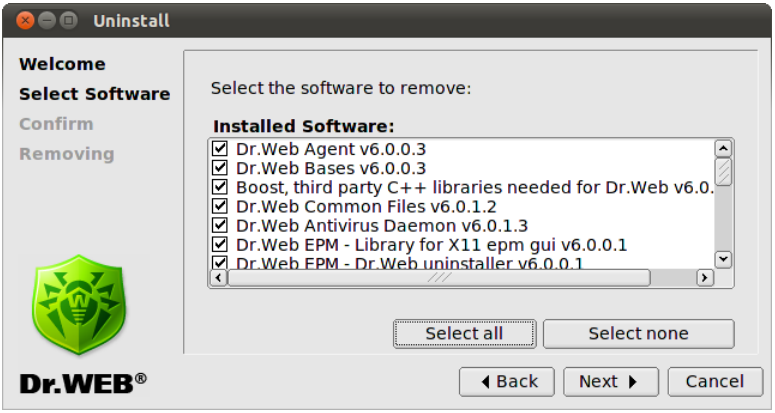
2. 起動画面で**"Next"** をクリックしてください。

図11.起動画面



3. **Select Software** 画面で、削除するコンポーネントを選択します。

図12. Select Software 画面



依存関係のあるコンポーネントは自動的に選択されます。

EPM-packagesによって既に他の**Dr.Web**製品がインストールされているコンピューターに**Dr.Web for UNIX mail servers**をインストールする場合、アンインストールGUI経由でモジュールを削除しようとする度に、他の製品のものを含む全ての**Dr.Web**モジュールを削除するように要求されます。

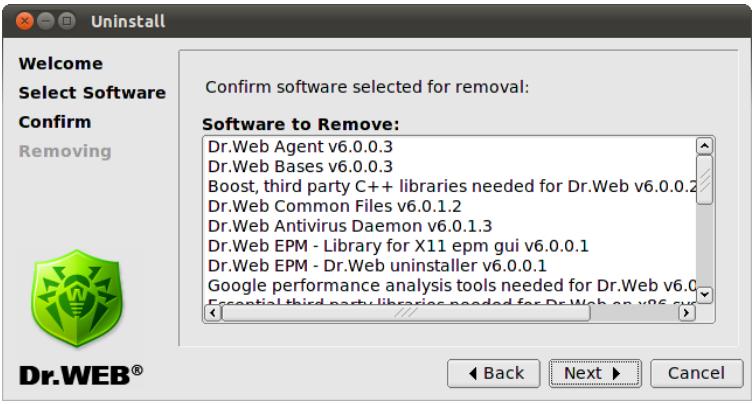
必要なコンポーネントを誤って削除してしまわないよう、アンインストールの際に実行する動作と選択は慎重に行うようにしてください。

"Select All" をクリックすると、全てのコンポーネントが選択され、**"Select None"** をクリックすると、全ての選択が解除されます。

選択が終了したら**Next**をクリックしてください。

3. **Confirm**画面でアンインストールするコンポーネントを確認してください。

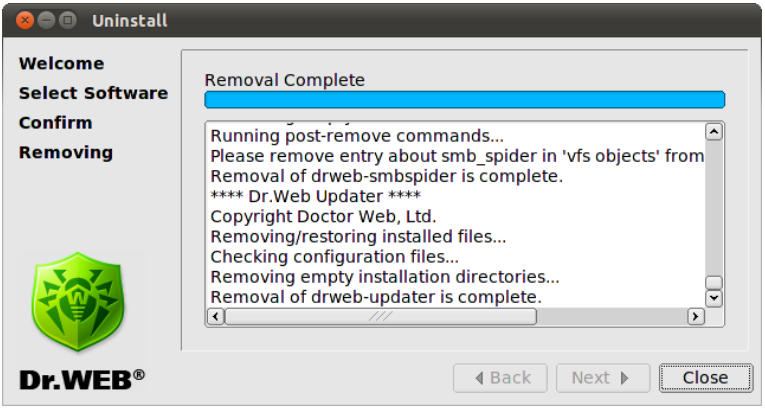
図13. 確認画面



選択を確認して**"Next"**をクリックします。変更するには**"Back"**をクリックしてください。

4. **Removal** 画面でアンインストールのプロセスをリアルタイムで確認することが出来ます。

図14. Removal 画面



5. **"Close"**をクリックしてセットアップを終了します。

コンソールアンインストーラによるアンインストール

GUIアンインストールを行えない場合、自動的にコンソールアンインストーラが開始します。

コンソールからアンインストールするには

1. コンソールアンインストーラが起動すると、対話式ウィンドウが表示されます。

```
user@hostname: ~
Файл  Правка  Вид  Поиск  Терминал  Справка

This script will help you remove Dr.Web packages

Do you wish to continue? (YES/no)
```

Dr.Web for UNIX mail serversをアンインストールする場合、**Y** または **Yes** を入力します。アンインストールしない場合は、**N** または **No** を入力します（大文字と小文字は区別しません）。ENTERキーを押してください。

2. アンインストールするコンポーネントの選択画面が表示されます。

```
user@hostname: ~
Файл  Правка  Вид  Поиск  Терминал  Справка
        [X] 10 Dr.Web VadeRetro antispam (6.0.0.2)
        [X] 11 Dr.Web Mail Daemon - CommuniGate Pro connector (6.0.0.2)
        [X] 12 Dr.Web Mail Daemon - common files (6.0.0.2)
        [X] 13 Dr.Web Mail Daemon - Dr.Web plugin (6.0.0.2)
        [X] 14 Dr.Web Mail Daemon - HeadersFilter plugin (6.0.0.2)
        [X] 15 Dr.Web Mail Daemon - Modifier plugin (6.0.0.2)
        [X] 16 Dr.Web Mail Daemon - VadeRetro plugin (6.0.0.2)
        [X] 17 Dr.Web Mail Daemon (6.0.0.2)
        [X] 18 Dr.Web Maild Web Interface (6.0.0.2)
        [X] 19 Dr.Web mail server and mail gateways documentation (6.0.0.2)
        [X] 20 Dr.Web Monitor (6.0.0.3)
        [X] 21 Dr.Web Antivirus Scanner (6.0.1.3)
        [X] 22 Dr.Web Updater (6.0.0.4)

To select a package you want to remove or deselect some previously
selected package - enter the corresponding package number and press Enter.

You may enter A or All to select all the packages, and N or None to deselect all of the
m.
Enter R or Remove to remove selected packages.
Enter 0, Q or Quit to quit the dialog.
All values are case insensitive.
Select:
```

3. プロンプトに従って削除するコンポーネントを選択してください。

4. 選択が終了したら、**Y** または **Yes** を入力してENTERキーを押してください（大文字と小文字は区別しません）。

```
user@hostname: ~
Файл  Правка  Вид  Поиск  Терминал  Справка
        drweb-agent
        drweb-bases
        drweb-boost144
        drweb-common
        drweb-daemon
        drweb-epm6.0.0-libs
        drweb-epm6.0.0-uninst
        drweb-gperftools0
        drweb-libs
        drweb-libvaderetro
        drweb-maild-cgp
        drweb-maild-common
        drweb-maild-plugin-drweb
        drweb-maild-plugin-headersfilter
        drweb-maild-plugin-modifier
        drweb-maild-plugin-vaderetro
        drweb-maild
        drweb-monitor
        drweb-scanner
        drweb-updater
Are you sure you want to remove the selected packages? (YES/no)
```

5. コンソールでアンインストールのプロセスをリアルタイムで確認することが出来ます。
6. アンインストールが完了したら、セットアップを終了してください。

ネイティブパッケージからのインストール

Dr.Web for UNIX mail servers は一般的なLinuxディストリビューション、Solaris、FreeBSDのネイティブパッケージからインストールすることが出来ます。

パッケージは全て**Dr.Web** の公式リポジトリ http://officeshield.drweb.com/drweb/に置かれています。お使いのシステムのパッケージマネージャにこのリポジトリを追加すると、リポジトリからのその他のプログラム同様、必要なパッケージをインストール・アップデート・アンインストール出来るようになります。依存関係は自動的に解決されます。

アップデートを反映させるには、リポジトリからアップデートした後に全てのDr.Webサービスを再起動する必要があります。

ソリューションによって、以下のパッケージのいずれかをインストールすることが出来ま

す。

- drweb-mail-gateways-as - **Dr.Web Antispam for UNIX Mail Gateways**
- drweb-mail-gateways-av - **Dr.Web Antivirus for UNIX Mail Gateways**
- drweb-mail-gateways-av-as - **Dr.Web Antivirus + Antispam for UNIX Mail Gateways**
- drweb-courier-as - **Dr.Web Antispam for Courier Mail Servers**
- drweb-courier-av - **Dr.Web Antivirus for Courier Mail Servers**
- drweb-courier-av-as - **Dr.Web Antivirus + Antispam for Courier Mail Servers**
- drweb-postfix-as - **Dr.Web Antispam for Postfix Mail Servers**
- drweb-postfix-av - **Dr.Web Antivirus for Postfix Mail Servers**
- drweb-postfix-av-as - **Dr.Web Antivirus + Antispam for Postfix Mail Servers**
- drweb-qmail-as - **Dr.Web Antispam for qmail Mail Servers**
- drweb-qmail-av - **Dr.Web Antivirus for qmail Mail Servers**
- drweb-qmail-av-as - **Dr.Web Antivirus + Antispam for qmail Mail Servers**
- drweb-sendmail-as - **Dr.Web Antispam for Sendmail Mail Servers**
- drweb-sendmail-av - **Dr.Web Antivirus for Sendmail Mail Servers**
- drweb-sendmail-av-as - **Dr.Web Antivirus + Antispam for Sendmail Mail Servers**
- drweb-cgp-as - **Dr.Web Antispam for CommuniGate Pro Mail Servers**
- drweb-cgp-av - **Dr.Web Antivirus for CommuniGate Pro Mail Servers**

- drweb-cgp-av-as - **Dr.Web Antivirus + Antispam for CommuniGate Pro Mail Servers**
- drweb-exim-as - **Dr.Web Antispam for Exim Mail Servers**
- drweb-exim-av - **Dr.Web Antivirus for Exim Mail Servers**
- drweb-exim-av-as - **Dr.Web Antivirus + Antispam for Exim Mail Servers**
- drweb-zmailer-as - **Dr.Web Antispam for ZMailer Mail Servers**
- drweb-zmailer-av - **Dr.Web Antivirus for ZMailer Mail Servers**
- drweb-zmailer-av-as - **Dr.Web Antivirus + Antispam for ZMailer Mail Servers**

Debian、Ubuntu (apt)

Debianリポジトリはライセンスキーによってデジタル署名されています。正常に動作する為に、キーを以下のコマンドでインポートする必要があります。

```
wget -O - http://officeshield.drweb.com/drweb/
drweb.key | apt-key add -
```

または

```
curl http://officeshield.drweb.com/drweb/drweb.
key | apt-key add -
```

お使いのシステムに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加えてください。

```
deb http://officeshield.drweb.com/drweb/debian stable
non-free
```

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います。

```
apt-get update

apt-get install <package name>
```

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使います。

```
apt-get remove <package name>
```

またはグラフィカルマネージャ(Synapticなど)を使ってパッケージをインストール、アンインストールすることも出来ます。

ALT Linux、PCLinuxOS (apt-rpm)

お使いのシステムに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加えてください。

32-bit版:

```
rpm http://officeshield.drweb.com/drweb/
altlinux stable/i386 drweb
```

64-bit版:

```
rpm http://officeshield.drweb.com/drweb/
altlinux stable/x86_64 drweb
```

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います。

```
apt-get update
```

```
apt-get install <package name>
```

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使います。

```
apt-get remove <package name>
```

またはグラフィカルマネージャ(Synapticなど)を使ってパッケージをインストール、アンインストールすることも出来ます。

Mandriva (urpmi)

正常に動作する為に、以下のコマンドでキーをインポートする必要があります。

```
rpm --import http://officeshield.drweb.com/
```

```
drweb/drweb.key
```

以下のファイルを開きます。

http://officeshield.drweb.com/drweb/drweb-i386.urpmi-media

または

http://officeshield.drweb.com/drweb/drweb-x86_64.urpmi-media

リポジトリをシステムに加えるよう促されます。

またはコンソールを使用して以下のコマンドでリポジトリを追加することも出来ます。

```
urpmi.addmedia drweb http://officeshield.drweb.
com/drweb/mandriva/stable/i386/
```

または

```
urpmi.addmedia drweb http://officeshield.drweb.
com/drweb/mandriva/stable/x86_64/
```

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います。

```
urpmi.update drweb
```

```
urpmi <package name>
```

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使います。

```
urpme <package name>
```

またはグラフィカルマネージャ(rpmdrakeなど)を使ってパッケージをインストール、アンインストールすることも出来ます。

Red Hat Enterprise Linux、Fedora、CentOS (yum)

以下のコンテンツのファイルを `/etc/yum.repos.d` ディレクトリに加えてください。

32-bit版:

```
[drweb]
name=DrWeb - stable
baseurl=http://officeshield.drweb.com/drweb/
el5/stable/i386/
gpgcheck=1
enable=1
gpgkey=http://officeshield.drweb.com/drweb/
drweb.key
```

64-bit版:

```
[drweb]
name=DrWeb - stable
baseurl=http://officeshield.drweb.com/drweb/
el5/stable/x86_64/
gpgcheck=1
enable=1
gpgkey=http://officeshield.drweb.com/drweb/
drweb.key
```

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います。

```
yum install <package name>
```

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使います。

```
yum remove <package name>
```

またはグラフィカルマネージャ(PackageKit、Yumexなど)を使ってパッケージをインストール、アンインストールすることも出来ます。

Zypper package manager (SUSE Linux)

リポジトリを追加するには以下のコマンドを実行してください。

```
zypper ar -t YUM http://officeshield.drweb.com/
```

```
drweb/el5/stable/i386/ drweb
```

または

```
zypper ar -t YUM http://officeshield.drweb.com/
drweb/el5/stable/x86_64/ drweb
```

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います。

```
zypper refresh
```

```
zypper install <package name>
```

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使います。

```
zypper remove <package name>
```

またはグラフィカルマネージャ(YaSTなど)を使ってパッケージをインストール、アンインストールすることも出来ます。

FreeBSD

FreeBSDのメタポートから**Dr.Web**製品をインストールすることが出来ます。http://officeshield.drweb.com/drweb/freebsd/ports/から必要なポートのアーカイブをダウンロードしてください。アーカイブを解凍し、`make install`を実行します。

Solaris

Solaris のネイティブパッケージはパブリックFTPサーバftp://ftp.drweb.com/pub/drweb/unix/release/Solaris/packages からダウンロードし、`pkgadd`ユーティリティーを使用してインストールすることが出来ます。

コンフィギュレーションスクリプト

コンポーネントが全てインストールされると、**Dr.Web MailD**の基本的な設定をするために`configure.pl`コンフィギュレーションスクリプトを使用することが出来ます。このスクリプトは`%bin_dir/maild/scripts/`ディレクトリにあります。スクリプトを起動すると、プラグインを使用したメール処理の方法(メッセージがデータベースに置かれる前に受信するのか、後に受信するのか等)、通知に使用する言語、送信先のアドレス、及び保護するネットワークとドメインのリストへのパス

を指定するように要求されます。**Dr.Web for UNIX mail servers**の使用を開始するにはこれらの情報で十分ですが、機能を全て実行するにはそれぞれのコンポーネント及びMTAの設定を手動で行う必要があります。

パラメータ、方法及び技術的なことに関する詳細は、本書の該当する章（調整とスタートアップ、プラグイン、MTAとの統合）を参照してください。

`%bin_dir/maild/scripts/` ディレクトリの`configure_`*<MTA>*`.sh` 及び `plugin_`*<name>*`_configure.pl` スクリプトは、プラグイン及びMTAがベストな動作をするために十分な機能のコンフィギュレーションを提供するものではありません。参照するソースとしてのみ使用してください。

設定ファイルの置き換え、移行によるアップグレード

Dr.Web for UNIX mail servers には、古い設定ファイルを置き換え、新しいフォーマットに合うように古いルールを変換するだけでバージョン4.44から6.0に移行することが出来るスクリプトが含まれています。これらのスクリプトは`%bin_dir/maild/scripts/`ディレクトリ内にあり、コンソールからのみ起動することが可能です。

Dr.Web for UNIX mail servers には以下のスクリプトが含まれています。

- 古い設定ファイルを置き換えるdwmigrate_to_new_conf.pl スクリプト。コンソールからこのスクリプトを実行する際に、製品の古いバージョンと新しいバージョンを指定してください。

  `# ./dwmigrate_to_new_conf.pl` *<古いバージョン> <新しいバージョン>*

  デフォルトでは"4.44" と "6.0"バージョンが使われます。このスクリプトは%etc_dirの設定ファイルを検索します。オリジナルの設定ファイルはCONF拡張子を持ち、新しい設定ファイルはCONF.NEW拡張子を持ちます。デフォルトのディレクトリにそのようなファイルが無かった場合は、それらの設定ファイルのあるディレクトリへの代わりのパスを求められます。必要な設定ファイルが全て見つかった後、dwmigrate_to_new_rules.plスクリプトが実行され、このスクリプトが古いルールを新しいフォーマットに変換します（詳細は下記）。次に.confファイルの設定が.conf.newファイルに移され、移行が成功すると.confファイルを.conf.newファイルで置き換えるよう促されま

す。

- `dwmigrate_to_new_rules.pl` スクリプトは古いルールを新しいフォーマットに変換します。コンソールからこのスクリプトを実行する際に、古い設定ファイル及び新しい設定ファイルへのパスを指定してください。

  `#  ./dwmigrate_to_new_rules.pl` *<古い設定ファイルへのパス> <新しい設定ファイルへのパス>*

  このスクリプトは古い設定ファイルからのルールを変更し、それらを新しい設定ファイルの該当するセクションからのルールと比較します。変更が無かった場合、(デフォルト値が残っている場合など)、スクリプトは通知を出してその動作を終了します。変更があった場合は、変更したルールを新しい設定ファイルに挿入するよう要求されます。

  スクリプトはif構文を使ったルール(例:notify.Virus=allow if rcpt:"foo\.com")を変更することは出来ません。そのようなルールは手動で変更してください。

  例:

  ```
  Sender:"lol@foo\.com"    notify.Skip=allow, notify.Virus=allow if rcpt:"foo\.com"
  ```

  は、以下のように変更します。

  ```
  Sender:"regex:lol@foo\.com"  && rcpt:"regex:foo\.com"  cont  notify.Virus=allow
  Sender:"lol@foo\.com"  cont  notify.Skip=allow
  ```

バージョン4.44から6.0への移行の際に**Dr.Web MailD**の2つの内部データベース、メッセージデータベースと統計データベースが削除されます。

drweb及びheadersfilterプラグインを含んだ**Dr.Web for UNIX mail servers**の機能は、**Dr.Web for UNIX Anti-virus solution**によるメールフィルターのそれを上回ります。 特別なスクリプトによって、古いバージョンのメールフィルターから新しいシステムのものに移行することが可能です。これらのスクリプトは `%bin_dir/maild/scripts/`ディレクトリ内にあり、コンソールからのみ起動することが出来ます。

メールフィルターからDr.Web for UNIX mail serversに設定を移行するには

1. `%etc_dir` ディレクトリの設定ファイルを除く、全てのインストールされているメールフィルター（それらと一緒に使われるMTAの設定ファイルを含む）を削除してください。
2. **Dr.Web for UNIX mail servers**と、必要な全てのプラグインをインストールします。drwebプラグインは必ずインストールしてください。メッセージをヘッダーでフィルタリングしたい場合はheadersfilterプラグインをインストールしてください。
3. `%bin_dir/maild/scripts/` ディレクトリの移行スクリプトを使用してメールフィルターの設定を**Dr.Web for UNIX mail servers** 設定ファイルの該当するセクションに移します。
   - `addresses_conf_to_rules.pl`スクリプトは`addresses.conf`設定ファイルの全ての設定を**Dr.Web MailD**設定ファイルの[Rules] セクションのルールにコピーします。
   - `users_conf_to_rules.pl`スクリプトは`users.conf`設定ファイルの全ての設定を**Dr.Web MailD**設定ファイルの[Rules] セクションのルールにコピーします。
   - `viruses_conf_to_rules.pl`スクリプトは`viruses.conf`設定ファイルの全ての設定を**Dr.Web MailD**設定ファイルの[Rules] セクションのルールにコピーします。
   - `filter_conf_to_maild.pl`スクリプトはメールフィルターの全ての設定を`drweb32.ini`設定ファイル及びフィルターの設定ファイルから**Dr.Web MailD**、drweb、headersfilterの設定ファイルにコピーします。

Dr.Web for UNIX mail serversの起動

Linux、Solarisの場合

Dr.Web for UNIX mail serversソリューションを起動するには以下の手順を実行してください。

1. ソフトウェアを登録します。
2. drweb32.key ファイルを**Dr.Web for UNIX mail servers** 実行ファイルのディレクトリ(UNIXシステムのデフォルトディレクトリは%bin_dirです)に置きます。他の場所にあるキーファイルを使用したい場合は、ファイルへのフルパスをdrweb32.ini設定ファイルの**Key**パラメータ値で指定する必要があります。Standaloneモードで動作する場合、このパスは**Dr.Web Agent**コンポーネントの設定ファイルagent.confの**LicenseFile**パラメータ値で指定してください。
3. 必要に応じて設定ファイルを編集し、ソフトウェアの設定を行ってください。設定についての詳細は本書の該当する章を参照してください。
4. %etc_dir ディレクトリのdrwebd.enableファイルにENABLE値として1を指定し、**Dr.Web Daemon**を有効にしてください。**Dr.Web Daemon**が必要無い場合(ネットワーク内にある他のコンピューター上に、設定が正しく行われ動作している**Daemon**がある)はENABLE値は0に指定してください(これはデフォルト値でもあります)。
5. %etc_dirディレクトリのdrweb-monitor.enableファイルにENABLE値として1を指定し、**Dr.Web Monitor**を有効にしてください。
6. コンソールまたはお使いのOSのファイルマネージャから**Dr.Web Daemon**及び**Dr.Web Monitor**の起動スクリプトを実行してください。起動後、**Dr.Web Monitor**が**Dr.Web for UNIX mail servers**ソリューションのその他全てのコンポーネント(**Sender**、**Receiver**、**Notifier**など)を起動させます。コンポーネントはそれぞれ個別に起動することも出来ますが、**Agent**経由で設定を受け取るため、**Dr.Web Agent**を最初に起動させる必要があります。

FreeBSDの場合

Dr.Web for UNIX mail serversソリューションを起動するには以下の手順を実行してください。

1. ソフトウェアを登録します。
2. drweb32.key ファイルを**Dr.Web for UNIX mail servers** 実行ファイルのディレクトリ(UNIXシステムのデフォルトディレクトリは%bin_dirです)に置きます。他の場所にあるキーファイルを使用したい場合は、ファイルへのフルパスをdrweb32.ini設定ファイルの**Key**パラメータ値で指定する必要があります。Standaloneモードで動作する場合、このパスは**Dr.Web Agent**コンポーネントの設定ファイルagent.confの**LicenseFile**パラメータ値で指定してください。
3. 必要に応じて設定ファイルを編集し、ソフトウェアの設定を行ってください。設定についての詳細は本書の該当する章を参照してください。
4. /etc/rc.conf ファイルに以下の記述を追加します。
   - drwebd_enable="YES" – **Dr.Web Daemon**を有効にします。**Dr.Web Daemon**が必要無い場合(ネットワーク内にある他のコンピューター上に、設定が正しく行われ動作している**Daemon**がある)は記述を追加しないでください。
   - drweb_monitor_enable="YES" – **Dr.Web Monitor**を有効にします。
5. コンソールまたはお使いのOSのファイルマネージャから**Dr.Web Daemon**及び**Dr.Web Monitor**の起動スクリプトを実行してください。起動後、**Dr.Web Monitor**が**Dr.Web for UNIX mail servers**ソリューションのその他全てのコンポーネント(**Sender**、**Receiver**、**Notifier**など)を起動させます。コンポーネントはそれぞれ個別に起動することも出来ますが、**Agent**経由で設定を受け取るため、**Dr.Web Agent**を最初に起動させる必要があります。

SELinuxの場合

SELinuxで保護されているOS上で**Dr.Web Scanner**と**Dr.Web Daemon**を稼動させる場合、drweb-scannerとdrweb-daemonモジュールの動作を可能とするためにポリシーをコンパイルする必要があります。

使用するテンプレートは、Linuxディストリビューションの種類やバージョン、SELinuxのポリシー及びユーザー設定によって大きく異なります。詳細は各種Linuxディストリビューションのドキュメントを参照してください。

必要なポリシーを作成するためにpolicygentoolコマンドを使用することが出来ます。このコマンドには、ポリシーモジュールの名前（モジュールとのインタラクションは調整する必要があります）及び対応する実行ファイルへのフルパスの2つのパラメータがあります。

例:

```
# policygentool drweb-scanner %bin_dir/drweb.real
```
- **Dr.Web Scanner**

```
# policygentool drweb-daemon %bin_dir/drwebd.real
```
- **Dr.Web Daemon**

次の3つのファイルが作成されます。

```
[module_name].te
[module_name].fc
[module_name].if
```

[module_name].te ファイルをコンパイルするために以下のコマンドを実行します。

```
checkmodule -M -m -o module-name [module_name].te
```

ポリシーのコンパイルを行うには、ご利用のシステムに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。

必要なポリシーのコンパイルを行うために以下のコマンドを実行します。

```
semodule_package -o [module_name].pp -m module-name
```

コンパイルしたポリシーモジュールをインストールするために以下のコマンドを実行します。

```
semodule -i [module_name].pp
```

ソフトウェア登録およびライセンスキーファイル

Dr.Web for UNIX mail serversソリューションの使用に関する権利は、ライセンスキーファイルによって制御されています。

ライセンスキーファイルには以下の情報が含まれています。

- 使用を許可された**Dr.Web for UNIX mail servers**のコンポーネント一覧
- ライセンスの有効期限
- 使用を許可されたプラグイン一覧（プラグインの中には登録が必要ないものもあります）
- その他の制限事項（保護するワークステーション数など）

ライセンスキーファイルは`*.key`拡張子を持ち、デフォルトでは**Dr.Web for UNIX mail servers** 実行ファイルのディレクトリに配置されます。

ライセンスキーファイルは、不正な改変を防ぐためにデジタル署名されており、変更されたライセンスキーファイルは無効になります。ライセンスキーファイルをテキストエディタで開くと破損する恐れがありますので注意してください。

認定パートナーから**Dr.Web for UNIX mail servers**ソリューションを購入したユーザはライセンスキーファイルを取得することが出来ます。キーファイルのパラメータは購入したライセンスに応じて指定されます。ライセンスキーファイルにはユーザ名（または企業名）及び販社の名前が含まれています。

ユーザはデモキーファイルを取得することもでき、**Dr.Web for UNIX mail servers**ソリューションの全ての機能をお試しいただけます。ただし、使用期間には期限があり、テクニカルサポートはご利用いただけません。

ライセンスキーファイルは`*.key`拡張子を持ったファイル、またはライセンスキーを含むzipファイルとして提供されます。

ライセンスキーファイルは以下のいずれかの方法で受け取ります。

- *.key拡張子を持ったライセンスキーファイルを含むzipファイルを電子メールで受信する(通常、Webサイトで登録した後)。アーカイブユーティリティーを使用してライセンスキーを解凍し、**Dr.Web for UNIX mail servers** 実行ファイルのディレクトリ(UNIXシステムのデフォルトディレクトリは%bin_dirです)にコピー/移動します。
- インストールパッケージに含まれている場合
- *.key拡張子のファイルとして別々のメディアに提供される場合。この場合、ライセンスキーファイルを手動で%bin_dirディレクトリにコピーする必要があります。

通常、ライセンスキーファイルはWebサイトでのシリアル登録後に電子メールで送られます(Webサイトのアドレスは製品に付属している登録カードに記載されています)。入力フォームに従い、シリアル番号(登録カードに記載されています)を登録してください。ライセンスがアクティベートされます。シリアル番号に対応したライセンスキーファイルが発行され、指定されたユーザのメールアドレスに送られます。

ライセンスキーファイルは期限が切れるまで保存しておき、**Dr.Web for UNIX mail servers**の再インストールまたは修復を行う場合に使用することを推奨します。ライセンスキーファイルが破損、または紛失している場合は、ライセンスのアクティベートと同じ手順でリカバリすることができます。この場合、シリアル番号などの情報は最初の登録時のものと同じにする必要があります。電子メールアドレスのみ変更可能です(変更した場合、ライセンスキーファイルは新たに登録した電子メールアドレス宛に送付されます)。シリアル番号が**Dr.Web for UNIX mail servers**データベースに登録された内容と一致すれば、対応するライセンスキーファイルが自動的に発行されます。

同じシリアル番号による登録は、25回まで行うことができます。25回を超えてライセンスキーファイルのリカバリを行う場合は、http://support.drweb.co.jp/register/ でライセンスキーファイルのリカバリを要求する必要があります。登録の際に入力した全ての情報、有効な電子メールアドレス、状況の詳しい説明を提供してください。**Dr.Web for UNIX mail servers**テクニカルサポートサービスエンジニアによって承認されると、自動サポートシステムまたは電子メールでライセンスキーファイルが発行されます。

コンポーネントのライセンスキーファイルへのパスは対応する設定ファイル(drweb32.ini)内の**Key**パラメータ値で指定されています。

例:

```
Key = %bin_dir/drweb32.key
```

ライセンスキーファイルの読み込みに失敗した(パスの誤り、アクセス権の拒否な

ど)、有効期限が切れている、ブロックされた、または無効な場合、各コンポーネントは終了します。

ライセンスの有効期限まで2週間になると、**Dr.Web Scanner**は起動時に警告メッセージを出力し、**Dr.Web Daemon**は起動、再起動、再読み込みの度に、電子メールでユーザに通知します。このオプションを有効にするには`drweb32.ini`設定ファイルの`[Daemon]`セクションで**`MailCommand`**パラメータをセットする必要があります。

他の場所にあるキーファイルを使う場合、ファイルへのフルパスを**Dr.Web Agent**設定ファイルの`[StandaloneMode]`の**`LicenseFile`**パラメータ値で指定する必要があります([StandaloneMode] セクションの説明を参照してください)。

Dr.Web for UNIX mail serversソリューションでは、複数のライセンスキーを同時に使用することが出来ます。使用を許可されたプラグインの一覧にはキーファイルの情報に含まれている全てのプラグインが載っています(または、少なくともその中の1つ)。1つのプラグインの操作に対する制限は、使用されている全てのキーファイルの情報に基づいて設定されています。

ソフトウェア全体の操作には、全てのプラグインが同じ制限を持っている必要があります。異なる制限を持ったプラグインを含むキーファイルがあった場合、**Dr.Web for UNIX mail servers**ソリューション全体の動作には、最も低い値が使われます。

例:

3つのライセンスキーを使用。1つ目では`drweb`プラグインに対する制限が1日につき10,000メール。2つ目ではvaderetroプラグインに対する制限が1日につき15,000メール、3つ目では再び`drweb`プラグインに対する制限が1日につき10,000メールであった場合、**Dr.Web for UNIX mail servers**ソリューションはキーファイルの情報に含まれている両方のプラグインと動作することが出来ます。しかし、`drweb`プラグインが実際には1日に20,000のメールを処理できるにも関わらず、プラグインの操作に対する全体の制限は1日につき15,000メール(vaderetroのもの)になります。

コマンドラインDr.Web Scanner

Dr.Web Scannerはローカルマシン上のウイルスを検出し、修復します。

コマンドラインパラメータ

Dr.Web Scanner は、以下のコマンドで実行します。

```
$ %bin_dir/drweb <path> [parameters]
```

<path>にはウイルス検査を実行するディレクトリへのパスを指定します。パラメータを指定せずに<path>引数のみで**Scanner**を実行した場合、デフォルトのパラメータ設定でスキャンを行います。

次の例では、ユーザーのホームディレクトリが検査されます。

```
$ %bin_dir/drweb ~
```

スキャンが完了すると、感染したファイル、または感染が疑われるファイルを以下のように表示します。

```
/path/file infected [virus] VIRUS_NAME
```

情報が表示された後、以下のような検査レポートが表示されます。

```
Report for "/opt/drweb/tmp":
Scanned        : 34/32    Cured      : 0
Infected       : 5/5      Removed    : 0
Modifications  : 0/0      Renamed    : 0
Suspicious     : 0/0      Moved      : 0
Scan time      : 00:00:02 Scan speed : 5233
KB/s
```

スラッシュ "/" で区切られた数字は、最初の数字がファイルの総数、2番目の数字がアーカイブ内のファイル数を意味します。

ウイルス検査のテストを行う場合は、製品パッケージに含まれている`readme.eicar`ファイルを使用することができます。このファイルをテキストエディタで開き、記載内容に従って`eicar.com`ファイルに変更してください。**Dr.Web Scanner**でこのファイルを検査すると以下のようなメッセージが出力されます。

```
%bin_dir/doc/eicar.com infected by Eicar Test File (Not a Virus!)
```

Eicar Test Fileはウイルスではなく、アンチウイルス製品のテストに使用されている無害な68バイトのコードです。

Scannerには多くのコマンドラインパラメータがあります。UNIX規約に従って、空白(スペース)によってパスと区切られ、ハイフン("-")で始まります。利用可能なパラメータの一覧は、-?、-h、-helpいずれかのパラメータで**Scanner**を実行することで確認できます。

コマンドラインパラメータの主な内容

- 検査対象の指定
- 検査内容の指定
- 検出時の動作の指定
- スキャナ、検査結果の出力に関する指定

検査対象の指定:

- `path` – ウイルス検査を実行するパスを指定します。複数のパスを指定することが可能です。
- `@[+]<file>` – ファイルに記載されたオブジェクトを検査します。プラス記号"+"は、スキャンが完了した後にオブジェクトのリストからファイルを削除しないようスキャナーに命令を出します。リストのファイルには、定期的にスキャンされるディレクトリへのパス、または1度だけ検査を実行するファイルのリストを含むことが出来ます。
- `sd` – カレントディレクトリから開始し、全てのサブディレクトリ内にあるファイルを再帰的にスキャンします。
- `fl` – シンボリックリンク先のファイル・ディレクトリを検査します。ループするリンクは無視されます。
- `mask` – ファイル名のマスクを無視します。

検査内容の指定:

- al – 全てのファイルを検査します。
- ar[d|m|r][n] – アーカイブファイルを検査します(ARJ、CAB、GZIP、RAR、TAR、ZIPなど)。感染したファイルを含むアーカイブをd – 削除、m – 隔離、r – 名前変更します。 n – アーカイブプログラム名を出力しません。アーカイブは*.tar 、または圧縮された*.tar.bz2、*.tbz形式が可能です。
- cn[d|m|r][n] – コンテナ内のファイルを検査します(HTML、RTF、PowerPointなど)。感染したオブジェクトを含むコンテナを d – 削除、 m – 隔離、r – 名前変更します。n – コンテナ名を出力しません。
- ml[d|m|r][n] – 電子メール書式ファイルを検査します。感染した電子メールファイルを d – 削除、m – 隔離、r – 名前変更します。n – 電子メールファイルの種類を出力しません。
- upn – LZEXE、DIET、PKLITE、EXEPACK で圧縮された実行ファイルを検査します。
- ex – 設定ファイルの**FilesTypes**パラメータで指定されている拡張子のファイルを検査します。
- ha – ヒューリスティック解析を有効にします。

検出時の動作の指定:

- cu[d|m|r] – 感染ファイルの修復、または d – 削除、m – 隔離、r – 名前変更。
- ic[d|m|r] – 修復不可能なファイルに対する動作: d – 削除、m – 隔離、r – 名前変更。
- sp[d|m|r] – 感染が疑われるファイルに対する動作:d – 削除、m – 隔離、r – 名前変更。
- adw[d|m|r|i] – アドウェアに対する動作: d – 削除、m – 隔離、r – 名前変更、i – 無視。
- dls[d|m|r|i] – ダイヤラーに対する動作: d – 削除、m – 隔離、r – 名前変更、i – 無視。
- jok[d|m|r|i] – ジョークプログラムに対する動作: d – 削除、m – 隔離、r – 名前変更、i – 無視。
- rsk[d|m|r|i] – リスクウェアに対する動作: d – 削除、m – 隔離、r – 名前変更、i – 無視。

- hck[d|m|r|i] – ハッキングプログラムに対する動作: d – 削除、m – 隔離、r – 名前変更、i – 無視。

スキャナ、検査結果の出力に関する指定:

- v, version – **Scanner**とアンチウイルスエンジンのバージョン情報を表示します。
- ki – ライセンスキーとその所有者に関する情報を表示します(UTF8のみ)。
- foreground[yes|no] – **Scanner**をフォアグラウンドで起動するか、バックグラウンドで起動するかを指定します。
- ot – 情報を標準出力に出力します。
- oq – 情報の出力を無効にします。
- ok – 感染していないクリーンなファイルを"Ok" で表示します。
- log=<path to file> – 指定ファイルにログを記録します。
- ini=<path to file> – 他の設定ファイルを使う場合の、ファイルへのパスの指定です。
- lng=<path to file> – 言語ファイルへのパスの指定です。
- -a=<Agent address> –**Scanner**を集中管理モードで開始します。
- --only-key – 開始時に**Scanner**が**Agent**からライセンスキーファイルのみを受信します。

以下のパラメータは、パラメータの後ろに"–"を付けることで無効にすることができます。

```
-ar -cu -ha -ic -fl -ml -ok -sd -sp
```

例:

以下のコマンドでは、ヒューリスティック解析が無効な状態で<path>ディレクトリをスキャンします(デフォルトでは有効)。

```
$ drweb <path> -ha-
```

Scanner のデフォルトのパラメータ設定は以下のとおりです。

```
-ar -ha -fl- -ml -sd
```

デフォルトのパラメータ設定は、完全なウイルス検査を実行するために最適な推奨設定となっています。前述の方法により、必要に応じて無効にするパラメータを指定することができます。

アーカイブファイル、及び圧縮されたファイルの検査を無効にした場合にはウイルス対策のレベルが低下する可能性があります。ウイルスはアーカイブ内（特に自己解凍ファイル）に侵入したり、メールの添付ファイル内に含まれていることが多々あり、マクロウイルスに感染しやすいオフィスドキュメント（Word、Excel）もまた、電子メールを介してアーカイブやコンテナ内に侵入するからです。

尚、デフォルトのパラメータ設定では、修復に関する動作、修復不可能または感染が疑われるファイルに対する動作は行いません。感染ファイルを修復するには検出時の動作を明示的に指定する必要があります。

推奨動作は以下のとおりです。

- `cu` – 修復（感染したファイルを削除、隔離、名前変更することなく）。
- `icd` – 修復不可能なファイルを削除します。
- `spm` – 感染が疑われるファイルを隔離します。
- `spr` – 感染が疑われるファイルを名前変更します。

cu（修復）を指定して**Scanner**を実行した場合、感染ファイルの修復を試みます。検出されたウイルスが既知のもので、修復のインストラクションがウイルスデータベースにある場合のみ修復可能です。ただし、その場合でも感染したファイルが著しく破損している場合、修復は失敗します。

アーカイブの中の感染ファイルを検出した場合には、修復や削除などの動作は行われません。別々のディレクトリにアーカイブファイルを展開し、動作を指定した上で**Scanner**を実行する必要があります。

d（削除）を指定して**Scanner**を実行した場合、ハードディスク上から感染ファイルを全て削除します。 このオプションは、修復不可能な感染ファイルに対する動作に適しています。

`r`（名前変更）を指定して**Scanner**を実行した場合、ファイルの拡張子を変更します。（デフォルトでは`*.#??`です。eicar.#omのように拡張子の最初の文字を"#"に変更します。）他のOSの感染が疑われるファイルに対する動作に適しており、ファイルが誤って実行されることを防ぎ、感染を防ぐことができます。

`m`（隔離）を指定して**Scanner**を実行した場合、感染ファイルまたは感染が疑わ

れるファイルを隔離ディレクトリ(デフォルトでは%var_dir/infected/)に隔離します。他のOSの感染ファイル、または感染が疑われるファイルはUNIXシステムを感染させることは無いので、このオプションはあまり使われません。UNIXシステムの、感染が疑われるファイルを隔離すると、システムの不具合を引き起こす場合があります。

デイリー検査コマンド(推奨):

```
$ drweb <path> -cu -icd -spm -ar -ha -fl--ml -sd
```

コマンドの内容をテキストファイルに保存し、以下のように実行可能にすることで、検査コマンドをシェルスクリプトで実行させることもできます。

```
# chmod a+x [file name]
```

また、**Scanner**のデフォルト設定は設定ファイルで変更することができます。

設定ファイル

Scannerはデフォルト設定で使うことも出来ますが、要件や状況に応じて変更することも可能です。**Scanner**の設定は、設定ファイルに保存されています(デフォルトでは%etc_dirディレクトリ内のdrweb32.ini)。他の設定ファイルを使う場合は、起動時に以下のようにファイルへのフルパスをコマンドラインパラメータで指定してください。

```
$ %bin_dir/drweb -ini=%bin_dir/etc/drweb.ini
```

設定ファイルの構造やパラメータの種類についての説明は、設定ファイルの章を参照してください。

[Scanner]

EnginePath = {path to file}	ウイルス検査エンジン(drweb32.dll)の指定です。このパラメータは **Updater**でも使われます。 デフォルト値: **EnginePath** = %bin_dir/lib/drweb32.dll

VirusBase = {list of paths to masks}	ウイルス定義ファイルの指定です。 ワイルドカード"*"の利用とカンマ","区切りによる複数指定が可能です。 デフォルト値: **VirusBase** = %var_dir/bases/*.vdb,%var_dir/bases/*.VDB
UpdatePath = {path to directory}	**Updater** (update.pl) の一時作業用ディレクトリの指定で、必須パラメータです。 デフォルト値: **UpdatePath** = %var_dir/updates/
TempPath = {path to directory}	ウイルス検査エンジンの一時作業用ディレクトリの指定です。システムのメモリが十分でない場合や特定の種類のアーカイブを展開する場合に使います。 デフォルト値: **TempPath** = /tmp/
LngFileName = {path to file}	言語ファイルの指定です。 デフォルト値: **LngFileName** = %bin_dir/lib/ru_scanner.dwl
Key = {path to file}	キーファイルの指定です(ライセンスまたはデモ)。 デフォルト値: **Key** = %bin_dir/drweb32.key
OutputMode = {Terminal | Quiet}	drwebプロセスの起動時のメッセージ出力の指定です。 Terminal - 標準出力 Quiet - 出力を抑制 デフォルト値:

	OutputMode = Terminal
HeuristicAnalysis = {Yes | No}	未知のウイルスを検出するためのヒューリスティック解析の有効・無効の指定です。 ヒューリスティック解析を使用することで、ウイルス情報データベースに登録されていない未知のウイルスの検出に効果を発揮します。一方で、ウイルスに似たコードを持つプログラムなどを誤検出する可能性があることに留意が必要です。 疑わしいファイルを解析の為にhttp://vms.drweb.com/sendvirus/からDr.Webに送ってください。送信する際はファイルをパスワードで保護されたアーカイブ内に置き、 メッセージ内にパスワードを記載し、Scannerのレポートを添付してください。 デフォルト値: **HeuristicAnalysis** = Yes
ScanPriority = {value}	Scannerのプロセスの優先度の指定です。 –20(最も高い優先度) ~ 19(Linux)または、20(Linux以外)の整数 デフォルト値: **ScanPriority** = 0
FilesTypes = {list of file extensions}	**ScanFiles**パラメータがByTypeの場合などに検査対象となる拡張子の指定です。 "*"と"?" によるワイルドカードの利用が可能です。 デフォルト値:

	FilesTypes = EXE, COM, SYS, OV?, BAT, BIN, DRV, PRG, BOO, SCR, CMD, VXD, 386, DLL, FON, DO?, XL?, WIZ, RTF, CL*, HT*, VB*, JS*, INF, AR?, ZIP, R??, PP?, OBJ, LIB, HLP, MD?, INI, MBR, IMG, CSC, CPL, MBP, SHS, SHB, PIF, SO, CHM, REG, XML, PRC, ASP, LSP, MSO, OBD, THE*, NWS, SWF, BMP, MPP, OCX, DVB, CPY, MSG, EML
FilesTypesWarnings = {Yes | No}	検査対象外ファイルに関する警告の指定です。 **ScanFiles**パラメータがByTypeの場合、検査対象外ファイルの検査要求に対して警告するかどうかの指定です。 デフォルト値: **FilesTypesWarnings** = Yes
ScanFiles = {All | ByType}	検査モードの指定です。 All を指定した場合は、全てのファイルを検査します。ByTypeを指定した場合は、**FileType**パラメータで指定された拡張子のファイルのみを検査します。 このパラメータはローカルスキャンモードでのみ使用することができます。メールボックス内のファイルは拡張子に関係なく常に検査されます。 デフォルト値: **ScanFiles** = All
ScanSubDirectories = {Yes | No}	サブディレクトリの検査に関する指定です。 検査対象ディレクトリ内のサブディレクトリを検査します。 デフォルト値: **ScanSubDirectories** = Yes

CheckArchives = {Yes | No}	アーカイブファイルの検査に関する指定です。 ZIP、RAR、ARJ、TAR、GZIP、CABその他のアーカイブファイルを検査します。 デフォルト値: **CheckArchives** = Yes
CheckEMailFiles = {Yes | No}	電子メール書式ファイルの検査に関する指定です。 デフォルト値: **CheckEMailFiles** = Yes
ExcludePaths = {list of path (masks)}	検査を除外するディレクトリの指定です。 デフォルト値: **ExcludePaths** = /proc,/sys,/dev
FollowLinks = {Yes | No}	シンボリックリンク先のファイル・ディレクトリの検査に関する指定です。 デフォルト値: **FollowLinks** = No
RenameFilesTo = {mask}	名前変更時の拡張子のマスクに関する指定です。 デフォルト値の"#??"の場合、"#"は拡張子の該当箇所を"#"で置き換えることを意味し、"??"は該当箇所を置き換えないことを意味します。eicar.comの検出で名前変更をした場合、eicar.#omとなります。拡張子がないファイルの場合は、".#"を付加します。 デフォルト値: **RenameFilesTo** = #??
MoveFilesTo = {path to directory}	隔離先のディレクトリの指定です。 デフォルト値:

	MoveFilesTo = %var_dir/infected/
EnableDeleteArchiveAction = {Yes | No}	感染ファイルを含むmultipartオブジェクト(アーカイブ、メールボックス、html)の削除に関する指定です。 このオプションを有効にした場合、感染ファイルを含むアーカイブやメールボックス(mbox形式の場合)ごと削除されますので注意してください。 デフォルト値: **EnableDeleteArchiveAction** = No
InfectedFiles = {Report | Cure | Delete | Move | Rename | Ignore}	感染ファイルに対する処理の指定です。 • Report - ログに記録 • Cure - 修復 • Delete - 削除 • Move - **MoveFilesTo**パラメータで指定された隔離ディレクトリに隔離 • Rename - **RenameFilesTo** パラメータで指定されたマスクを使用して名前変更 • Ignore - 無視 Delete、Move、Rename の処理は、感染ファイルを含むアーカイブ、コンテナ、メールボックスに指定された場合、ファイルごと削除、隔離、名前変更されますので注意してください。 デフォルト値: **InfectedFiles** = Report
SuspiciousFiles = {Report | Delete | Move | Rename | Ignore}	感染が疑われるファイルに対する処理の指定です。 • Report - ログに記録 • Delete - 削除 • Move - **MoveFilesTo**パラメータで指定された隔離ディレクトリに隔離

	• Rename – **RenameFilesTo** パラメータで指定されたマスクを使用して名前変更 • Ignore – 無視 デフォルト値: **SuspiciousFiles** = Report
IncurableFiles = {Report |Delete | Move | Rename | Ignore}	修復不可能なファイルに対する処理の指定です(**InfectedFiles** = Cureの場合のみ使用してください)。 • Report – ログに記録 • Delete – 削除 • Move – **MoveFilesTo**パラメータで指定された隔離ディレクトリに隔離 • Rename – **RenameFilesTo** パラメータで指定されたマスクを使用して名前変更 • Ignore – 無視 デフォルト値: **IncurableFiles** = Report
ActionAdware = {Report | Delete | Move | Rename | Ignore}	アドウェアに対する処理の指定です。 • Report – ログに記録 • Delete – 削除 • Move – **MoveFilesTo**パラメータで指定された隔離ディレクトリに隔離 • Rename – **RenameFilesTo** パラメータで指定されたマスクを使用して名前変更 • Ignore – 無視 デフォルト値: **ActionAdware** = Report

ActionDialers = {Report | Delete | Move | Rename | Ignore}	ダイヤラーに対する処理の指定です。 • Report – ログに記録 • Delete – 削除 • Move – **MoveFilesTo**パラメータで指定された隔離ディレクトリに隔離 • Rename – **RenameFilesTo** パラメータで指定されたマスクを使用して名前変更 • Ignore – 無視 デフォルト値: **ActionDialers** = Report
ActionJokes = {Report | Delete | Move | Rename | Ignore}	ジョークプログラムに対する処理の指定です。 • Report – ログに記録 • Delete – 削除 • Move – **MoveFilesTo**パラメータで指定された隔離ディレクトリに隔離 • Rename – **RenameFilesTo** パラメータで指定されたマスクを使用して名前変更 • Ignore – 無視 デフォルト値: **ActionJokes** = Report
ActionRiskware = {Report | Delete | Move | Rename | Ignore}	リスクウェアに対する処理の指定です。 • Report – ログに記録 • Delete – 削除 • Move – **MoveFilesTo**パラメータで指定された隔離ディレクトリに隔離 • Rename – **RenameFilesTo** パラメータで指定されたマスクを使用して名前変更 • Ignore – 無視 デフォルト値:

	ActionRiskware = Report
ActionHacktools = {Report | Delete | Move | Rename | Ignore}	ハッキングプログラムに対する処理の指定です。 • Report – ログに記録 • Delete – 削除 • Move – **MoveFilesTo**パラメータで指定された隔離ディレクトリに隔離 • Rename – **RenameFilesTo** パラメータで指定されたマスクを使用して名前変更 • Ignore – 無視 デフォルト値: **ActionHacktools** = Report
ActionInfectedMail = {Report | Delete | Move | Rename | Ignore}	感染ファイルを含むメールボックスに対する処理の指定です。 • Report – ログに記録 • Delete – 削除 • Move – **MoveFilesTo**パラメータで指定された隔離ディレクトリに隔離 • Rename – **RenameFilesTo** パラメータで指定されたマスクを使用して名前変更 • Ignore – 無視 デフォルト値: **ActionInfectedMail** = Report
ActionInfectedArchive = {Report | Delete | Move | Rename | Ignore}	感染ファイルを含むアーカイブに対する処理の指定です。 • Report – ログに記録 • Delete – 削除 • Move – **MoveFilesTo**パラメータで指定された隔離ディレクトリに隔離

	• Rename – **RenameFilesTo** パラメータで指定されたマスクを使用して名前変更 • Ignore – 無視 デフォルト値: **ActionInfectedArchive** = Report
ActionInfectedContainer = {Report | Delete | Move | Rename | Ignore}	感染ファイルを含むコンテナに対する処理の指定です。 • Report – ログに記録 • Delete – 削除 • Move – **MoveFilesTo**パラメータで指定された隔離ディレクトリに隔離 • Rename – **RenameFilesTo** パラメータで指定されたマスクを使用して名前変更 • Ignore – 無視 デフォルト値: **ActionInfectedContainer** = Report
LogFileName = {file name}	ログファイルの指定です。 syslogを指定することができます(**SyslogFacility**と**SyslogPriority**パラメータの指定が必要です)。 デフォルト値: **LogFileName** = syslog
SyslogFacility = {Daemon | Local0 .. Local7 | Kern | User | Mail}	syslogのファシリティの指定です。 デフォルト値: **SyslogFacility** = Daemon

SyslogPriority = {Alert | Warning | Notice | Info | Error}	syslogのプライオリティの指定です。 デフォルト値: **SyslogPriority** = Info
LimitLog = {Yes | No}	ログファイルのサイズ制限の指定です。**LogFileName** = syslogの場合は無視されます。 有効(yes)にするとScanner起動時にログファイルのサイズをチェックし、最大サイズを超えている場合にログファイルを削除します(直近のログファイルは、.bakの拡張子で残されます)。ログファイルの最大サイズは、**MaxLogSize**パラメータで指定します。 デフォルト値: **LimitLog** = No
MaxLogSize = {value in Kbytes}	ログファイルの最大サイズの指定です(**LimitLog** = Yes の場合)。 0以上の整数で、ログファイルのサイズ(キロバイト)を指定します。 起動時にログファイルが変更されるのを防ぎたい場合は、このパラメータ値を0に設定してください。 デフォルト値: **MaxLogSize** = 512
LogScanned = {Yes | No}	Yesの場合、検査した全てのファイルの情報をログに記録します。 デフォルト値: **LogScanned** = Yes
LogPacked = {Yes | No}	Yesの場合、DIET、PKLITEなどで圧縮されたファイルに関する情報をログに記録します。 デフォルト値: **LogPacked** = Yes

LogArchived = {Yes | No}	Yesの場合、アーカイバに関する情報をログに記録します。 デフォルト値: **LogArchived** = Yes
LogTime = {Yes | No}	Yesの場合、ログの各行に処理時間を記録します(**LogFileName** = syslogの場合は使用できません)。 デフォルト値: **LogTime** = Yes
LogStatistics = {Yes | No}	Yesの場合、検査の統計情報をログに記録します。 デフォルト値: **LogStatistics** = Yes
RecodeNonprintable = {Yes | No}	ログ中の表示できない文字の置換に関する指定です。 デフォルト値: **RecodeNonprintable** = Yes
RecodeMode = {Replace | QuotedPrintable}	表示できない文字の置換方法の指定です(**RecodeNonprintable** = Yesの場合)。 **Replace**の場合は、**RecodeChar**パラメータで指定する文字に置換します。 QuotedPrintableの場合は、quoted-printableエンコード文字列で置換します。 デフォルト値: **RecodeMode** = QuotedPrintable
RecodeChar = {"?" | "_" | ...}	表示できない文字を置換する文字列の指定です(**RecodeMode** = Replaceの場合)。 デフォルト値:

	RecodeChar = "?"

アーカイブファイルの検査時間を短縮するために次のパラメータを使用することができます（アーカイブ内のいくつかのオブジェクトは検査されません）。

MaxCompressionRatio = {value}	アーカイブファイルを展開して検査する際の圧縮比の上限値の指定です。 指定された圧縮比を超える場合には検査を行いません。 デフォルト値: **MaxCompressionRatio** = 5000
CompressionCheckThreshold = {value in Kbytes}	アーカイブファイルの圧縮比を確認するファイルサイズの下限値（キロバイト）の指定です。 デフォルト値: **CompressionCheckThreshold** = 1024
MaxFileSizeToExtract = {value in Kbytes}	アーカイブ中の最大ファイルサイズ（キロバイト）の指定です。 指定された値を超えたファイルは検査を行いません。 デフォルト値: **MaxFileSizeToExtract** = 500000
MaxArchiveLevel = {value}	アーカイブファイルを検査する際の最大ネストレベルの指定です。 最大ネストレベルを超えるアーカイブファイルは検査を行いません。 デフォルト値: **MaxArchiveLevel** = 8
MaximumMemoryAllocationSize = {value in Mbytes}	1個のファイルを検査する際に消費するメモリについて、最大値を制限するための指定です（メガバイト）。 "0"が指定された場合、制限はありません。

	デフォルト値: **MaximumMemoryAllocationSize** = 0
ScannerScanTimeout = {time in seconds}	1個のファイルを検査する際のタイムアウト値の指定です(秒)。 "0"が指定された場合、タイムアウトはしません。 デフォルト値: **ScannerScanTimeout** = 0
MaxBasesObsolescencePeriod = {time in hours}	ウイルス定義ファイルが古くなっていないかを示すための期間です(時間)。 最終更新から指定された期間を経過すると、ウイルス定義ファイルが古くなっていることを示す通知がコンソールに出力されます。"0"が指定された場合、チェックされません。 デフォルト値: **MaxBasesObsolescencePeriod** = 24
ControlAgent = {Agent socket address}	**Agent**のソケットをTYPE:ADDRESSの形で指定します。TYPEはソケットの種類です。 • inet - TCPソケット • localまたはunix - UNIXソケット 例: **ControlAgent** = inet:4040@127.0.0.1,local:%var_dir/ipc/.agent デフォルト値: **ControlAgent** = local:%var_dir/ipc/.agent

OnlyKey = {Yes | No}	Yesの場合、**Scanner**は**Agent**からライセンスキーファイルのみを受け取り、ローカルドライブ上の設定ファイルを使用します。 Noの場合、**Scanner**は**Agent**からライセンスキーファイルと設定情報を受け取ります。 デフォルト値: **OnlyKey** = No

Dr.Web Scannerの起動

Dr.Web Scannerは以下のコマンドで実行します。

```
$ %bin_dir/drweb
```

%bin_dir　ディレクトリがPATH環境変数に追加されている場合、どこからでも"drweb"とコマンド入力するだけで**Dr.Web Scanner**を実行することができます。ただし、セキュリティ上の理由から推奨はできません。

Dr.Web Scannerは、root権限でもユーザ権限でも実行することができます。ユーザ権限の場合は、ウイルス検査及び感染したファイルの修復はユーザが書き込み権限を持ったディレクトリ内でのみ行われます(通常はユーザホームディレクトリ$HOME)。また、感染したファイルの隔離や名前変更についても制限を受ける場合があります。

Scannerが実行されると、プログラムバージョンのほか、ウイルス定義ファイルやライセンスキーに関する情報などを出力します。

```
Dr.Web (R) Scanner for Linux, v6.0.1 (February 19, 2010)
Copyright (c) Igor Daniloff, 1992-2010
Support service: http://support.drweb.com/
To purchase: http://buy.drweb.com/
Program version: 6.0.0.10060 <API:2.2>
Engine version: 6.0.0.9170 <API:2.2>
Loading /var/drweb/bases/drwtoday.vdb - Ok, virus records: 1533
```

```
Loading  /var/drweb/bases/drw60012.vdb  -  Ok,
virus records: 3511
---------------------------------------------
Loading  /var/drweb/bases/drw60000.vdb  -  Ok,
virus records: 1194
Loading  /var/drweb/bases/dwn60001.vdb  -  Ok,
virus records: 840
Loading  /var/drweb/bases/drwebase.vdb  -  Ok,
virus records: 78674
Loading  /var/drweb/bases/drwrisky.vdb  -  Ok,
virus records: 1271
Loading  /var/drweb/bases/drwnasty.vdb  -  Ok,
virus records: 4867
Total virus records: 538681
Key file: /opt/drweb/drweb32.key
Key file number: XXXXXXXXXX
Key file activation date: XXXX-XX-XX
Key file expiration date: XXXX-XX-XX
```

このレポートが表示された後**Scanner**が終了します。ウイルス検出時の動作を指定する場合は、コマンドラインパラメータを追加します。

Dr.Web Daemon

Dr.Web Daemonは、他の**Dr.Web**コンポーネントからの検査要求に応じ、ウイルス検査を行うアンチウイルスモジュールです。ディスク上のファイルまたは、ソケット経由で転送されたデータの両方を検査することが可能です。検査要求は特別なプロトコルを使用してUNIXソケットまたはTCPソケッ経由で送られます。**Dr.Web Daemon**は**Scanner**と同じアンチウイルスエンジン及びウイルスデータベースを使用し、既知のウイルスを検出、修復することが出来ます。

Dr.Web Daemonは常時動作しており、検査要求を送るためにシンプルなプロトコルを使用しています。そのため、メールサーバーに対するアンチウイルスフィルターとしてのパーフェクトなソリューションとなっているのです。

コマンドラインパラメータ

Dr.Web Daemonは、コマンドラインパラメータの使用をサポートしています。パラメータは、ハイフン"-"で指定し、スペースで区切ります。パラメータのリストを表示する場合は、`-?`、`-h` 、または`-help`パラメータで`drwebd`を実行します。

Dr.Web Daemonでは、以下のコマンドラインパラメータを使用することができます。

- `-ini=<path to file>` – 設定ファイルへのパスの指定です(デフォルト以外を指定する場合)。
- `--foreground=<yes|no>` – **Daemon**の動作モードの指定です。"`Yes`"の場合、**Daemon**はフォアグラウンドモードで動作し、"`No`"の場合はバックグラウンド(デーモン)モードで動作します。
- `--check-only <command line parameters for checking>` – 設定ファイルと指定されたコマンドラインパラメータのチェックを行います。
- `-a=<Agent address>` – **Daemon**を集中管理モードで動作させます(設定ファイル、ライセンスキーファイルを**Agent**から受け取ります)。
- `--only-key` – **Agent**からライセンスキーファイルのみを受け取ります(ローカルの設定ファイルを使用します)。

設定

Dr.Web Daemonはデフォルト設定で使うことも出来ますが、要件や状況に応じて変更することも可能です。**Daemon**の設定は、%etc_dirディレクトリ内にある設定ファイル(デフォルトではdrweb32.ini)に保存されています。他の設定ファイルを使う場合は、起動時にファイルへのフルパスをコマンドラインパラメータで指定してください。

設定ファイルの構造やパラメータの種類についての説明は、設定ファイルの章を参照してください。

[Daemon] section

EnginePath = {path to file}	ウイルス検査エンジン(drweb32.dll)の指定です。 デフォルト値: **EnginePath** = %bin_dir/lib/drweb32.dll
VirusBase = {list of files or masks}	ウイルス定義ファイルの指定です。 ワイルドカード"*"の利用とカンマ","区切りによる複数指定が可能です。 Default value: **VirusBase** = %var_dir/bases/*.vdb,%var_dir/bases/*.VDB
UpdatePath = {path to directory}	**Updater** (update.pl) の一時作業用ディレクトリの指定で、必須パラメータです。 デフォルト値: **UpdatePath** = %var_dir/updates/
TempPath = {path to directory}	ウイルス検査エンジンの一時作業用ディレクトリの指定です。システムのメモリが十分でない場合や特定の種類のアーカイブを展開する場合に使います。

	TempPath = %var_dir/spool/
Key = {path to file}	キーファイルの指定です(ライセンスまたはデモ)。**Daemon**と**Scanner** は異なるライセンスキーファイルを持っているのでご注意ください。この場合、それに応じてこのパラメータの値を変更する必要があります。**Daemon**は複数のキーファイルを同時に使用することが出来ます。それぞれに対してdrweb32.iniファイルの[Daemon]セクション内で**Key**パラメータ値を指定する必要があります。この場合、**Daemon**は使用できる全てのキーファイルからライセンスパーミッションを集めようとします。 デフォルト値: **Key** = %bin_dir/drweb32.key
MailAddressesList = {path to file}	検査対象とするメールアドレス一覧ファイルへのパスの指定です。15または30アドレスライセンスの場合に有効となります。 デフォルト値: **MailAddressesList** = %etc_dir/email.ini
OutputMode = {Terminal | Quiet}	drwebプロセスの起動時のメッセージ出力の指定です。 Terminal - 標準出力 Quiet - 出力を抑制 デフォルト値: **OutputMode** = Terminal
RunForeground = {Yes | No}	Yesの場合、**Daemon**をフォアグラウンドで動作させます。 通常は、デフォルトのNo(デーモン)を使用します。特別なユーティリティ(**Dr.Web Monitor**など)を使用する場合の指定です。

	デフォルト値: **RunForeground** = No
User = {user name}	**Daemon**を起動するユーザ名の指定です。**Daemon**及びフィルターに使用される、別々の**drweb**ユーザアカウントを作成することを推奨します。セットアップにかかる時間は減りますが、**Daemon**をroot権限で実行することは推奨できません。SIGHUPを使用して設定をリロードする場合、このパラメータは変更されません。 デフォルト値: **User** = drweb
PidFile = {path to file}	**Daemon**のPIDファイルへのパスの指定です。 デフォルト値: **PidFile** = %var_dir/run/drwebd.pid
BusyFile = {path to file}	**Daemon**の子プロセスが検査中に作成するロックファイルへのパスの指定です。 ファイル名の末尾に子プロセスのPIDが付加されます(例:/var/run/drwebd.bsy.123456)。 デフォルト値: **BusyFile** = %var_dir/run/drwebd.bsy
ProcessesPool = {process pool settings}	子プロセスの生成に関する指定です。 まず、プール内のプロセス数を指定します。 • auto - システムの負荷状態により、自動的にプロセス数が生成されます。 • N - 1以上の整数を指定します。指定した数だけプロセスが生成され、必要に応じて追加プロセスが生成されます。

	• N-M – 1以上の整数を指定します。Nに指定した数だけプロセスが予め生成されますが、Mで指定された数を超えてプロセスは生成されません。 次に、任意の追加パラメータを指定することもできます。 • **timeout** = {time in seconds} – アクティブでないプロセスを終了するまでのタイムアウト値の指定です(前述のNで指定された数のプロセスは、このパラメータの影響を受けません)。 • **stop_timeout** = {time in seconds} – 稼働プロセスを停止させるまでの最大待ち時間の指定です。 デフォルト値: **ProcessesPool** = auto,**timeout**=120,**stop_timeout**=1
OnlyKey = {Yes | No}	Yesの場合、**Agent**からライセンスキーファイルのみを受け取ります。設定はローカルの設定ファイルに従います。 Noの場合、**Agent**からライセンスキーファイルと設定ファイルを受け取ります。 デフォルト値: **OnlyKey** = No
ControlAgent = {socket address}	**Agent**のソケットをTYPE:ADDRESSの形で指定します。TYPEはソケットの種類です。 • inet - TCPソケット • localまたはunix - UNIXソケット 例: **ControlAgent** = inet:4040@127.0.0.1,local:%var_dir/ipc/.agent デフォルト値:

	ControlAgent = local:%var_dir/ipc/.agent
MailCommand = {command}	Daemon及びUpdaterが通知メールを管理者に送信する際のコマンドの指定です。ライセンスの有効期限まで2週間になると、Daemonは起動、再起動、再読み込みの度に通知を送信します。 デフォルト値: **MailCommand** = "/usr/sbin/sendmail -i -bm -f drweb --root"
NotifyPeriod = {value}	ライセンスキーの期限切れを示す通知メールを何日前から送信するかの指定です。"0"を指定した場合、ライセンスの期限が切れた後に通知メールが送信されます。 デフォルト値: **NotifyPeriod** = 14
NotifyFile = {path to file}	ライセンスキーの期限切れを示す通知メールを送信した日時を記録するファイルの指定です。 デフォルト値: **NotifyFile** = %var_dir/.notify
NotifyType = {Ever | Everyday | Once}	ライセンスキーの期限切れを示す通知メールを送信する頻度の指定です。 Once - 1回限り Everyday - 毎日 Ever - Daemonの再起動時およびウイルス定義ファイルの更新時 デフォルト値: **NotifyType** = Ever

FileTimeout = {value in seconds}	1個のファイルを検査する最大時間(秒)の指定です。 デフォルト値: **FileTimeout** = 30
StopOnFirstInfected = {Yes | No}	ウイルスを1個検出した時点で検査を終了するかどうかの指定です。 デフォルト値: **StopOnFirstInfected** = No
ScanPriority = {value}	**Daemon**のプロセスの優先度の指定です。 –20(最も高い優先度) ~ 19(Linux)または、20(Linux以外)の整数 デフォルト値: **ScanPriority** = 0
FilesTypes = {list of file extensions}	**ScanFiles**パラメータがByTypeの場合に検査対象となる拡張子の指定です。 "*" と "?" によるワイルドカードの利用が可能です。 デフォルト値: **FilesTypes** = EXE, COM, SYS, OV?, BAT, BIN, DRV, PRG, BOO, SCR, CMD, VXD, 386, DLL, FON, DO?, XL?, WIZ, RTF, CL*, HT*, VB*, JS*, INF, AR?, ZIP, R??, PP?, OBJ, LIB, HLP, MD?, INI, MBR, IMG, CSC, CPL, MBP, SHS, SHB, PIF, SO, CHM, REG, XML, PRC, ASP, LSP, MSO, OBD, THE*, NWS, SWF, BMP, MPP, OCX, DVB, CPY, MSG, EML
FilesTypesWarnings = {Yes | No}	検査対象外ファイルに関する警告の指定です。 **ScanFiles**パラメータがByTypeの場合、検査対象外ファイルの検査要求に対して警告す

	るかどうかの指定です。 デフォルト値: **FilesTypesWarnings** = Yes
ScanFiles = {All | ByType}	検査モードの指定です。 All を指定した場合は、全てのファイルを検査します。ByTypeを指定した場合は、**FileType**パラメータで指定された拡張子のファイルのみを検査します。 このパラメータはローカルスキャンモードでのみ使用することができます。メールボックス内のファイルは拡張子に関係なく常に検査されます。 デフォルト値: **ScanFiles** = All
CheckArchives = {Yes | No}	アーカイブファイルの検査に関する指定です。 ZIP, RAR, ARJ, TAR, GZIP, CAB その他のアーカイブファイルを検査します。 デフォルト値: **CheckArchives** = Yes
CheckEMailFiles = {Yes | No}	電子メール書式ファイルの検査に関する指定です。 デフォルト値: **CheckEMailFiles** = Yes
ExcludePaths = {list of paths or masks}	検査を除外するディレクトリの指定です。 デフォルト値: **ExcludePaths** = /proc,/sys,/dev
FollowLinks = {Yes | No}	シンボリックリンク先のファイル・ディレクトリの検査に関する指定です。 デフォルト値:

	FollowLinks = No
RenameFilesTo = {mask}	名前変更時の拡張子のマスクに関する指定です。 デフォルト値の"#??"の場合、"#"は拡張子の該当箇所を"#"で置き換えることを意味し、"??"は該当箇所を置き換えないことを意味します。eicar.comの検出で名前変更をした場合、eicar.#omとなります。拡張子がないファイルの場合は、".#"を付加します。 デフォルト値: **RenameFilesTo** = #??
MoveFilesTo = {path to directory}	隔離先のディレクトリの指定です。 デフォルト値: **MoveFilesTo** = %var_dir/infected/
BackupFilesTo = {path to directory}	感染ファイルに対して修復(Cure)を指定している場合に、元のファイルをバックアップするディレクトリの指定です。 デフォルト値: **BackupFilesTo** = %var_dir/infected/
LogFileName = {file name}	ログファイルの指定です。 syslogを指定することができます(**SyslogFacility**と**SyslogPriority**パラメータの指定が必要です)。 デフォルト値: **LogFileName** = syslog
SyslogFacility = {Daemon | Local0 .. Local7 | Kern |	syslogのファシリティの指定です。 デフォルト値: **SyslogFacility** = Daemon

User | Mail}	
SyslogPriority = {Alert | Warning | Notice | Info | Error}	syslogのプライオリティの指定です。 デフォルト値: **SyslogPriority** = Info
LimitLog = {Yes | No}	ログファイルのサイズ制限の指定です。 デフォルト値: **LimitLog** = No
MaxLogSize = {value in Kbytes}	ログファイルの最大サイズの指定です(**LimitLog** = Yes の場合)。 0以上の整数で、ログファイルのサイズ(キロバイト)を指定します。 デフォルト値: **MaxLogSize** = 512
LogScanned = {Yes | No}	Yesの場合、検査した全てのファイルの情報をログに記録します。 デフォルト値: **LogScanned** = Yes
LogPacked = {Yes | No}	Yesの場合、DIET、PKLITEなどで圧縮されたファイルに関する情報をログに記録します。 デフォルト値: **LogPacked** = Yes
LogArchived = {Yes | No}	Yesの場合、アーカイバに関する情報をログに記録します。 デフォルト値: **LogArchived** = Yes

LogTime = {Yes | No}	Yesの場合、ログの各行に処理時間を記録します(**LogFileName** = syslogの場合は使用できません)。 デフォルト値: **LogTime** = Yes
LogProcessInfo = {Yes | No}	Yesの場合、検査を実施したプロセスのPIDと検査を要求したクライアントのIPアドレス(またはホスト名)が記録されます。 デフォルト値: **LogProcessInfo** = Yes
RecodeNonprintable = {Yes | No}	ログ中の表示できない文字の置換に関する指定です。 デフォルト値: **RecodeNonprintable** = Yes
RecodeMode = {Replace | QuotedPrintable}	表示できない文字の置換方法の指定です(**RecodeNonprintable** = Yesの場合)。 **Replace**の場合は、**RecodeChar**パラメータで指定する文字に置換します。QuotedPrintableの場合は、quoted-printableエンコード文字列で置換します。 デフォルト値: **RecodeMode** = QuotedPrintable
RecodeChar = {"?" | "_" | ...}	表示できない文字を置換する文字列の指定です(**RecodeMode** = Replaceの場合)。 デフォルト値: **RecodeChar** = "?"
Socket = {socket address}	**Daemon**が検査要求を待ちうけるソケットの指定です。

	ソケットを指定する方法はいくつかあります。 複数のソケットアドレスは1つのストリング内で指定する必要があります。TYPE:ADDRESSの形で指定し、TYPEはソケットの種類です。 • inet - TCPソケット • localまたはunix - UNIXソケット 例: Socket = inet:3000@127.0.0.1, local:%var_dir/.daemon またPORT [interfaces] | FILE [access] の形で指定することも出来ます。 TCPソケットには10進法でのポート番号(PORT)、要求を受けるインターフェース名のリストかIPアドレス(interfaces)を指定します。 例: **Socket** = 3000 127.0.0.1, 192.168.0.100 UNIXソケットにはソケット名(FILE)、8進法でのアクセスパーミッション(access)を指定します。 例: **Socket** = %var_dir/.daemon Socketパラメータの数に制限はありません。正しく指定されたすべての設定で**Daemon**が動作します。利用可能な全てのインターフェースで検査要求を受ける場合は、3000 0.0.0.0と指定してください。
	デフォルト値: **Socket** = %var_dir/run/.daemon

SocketTimeout = {value in seconds}	ソケット経由で送受信されるデータのタイムアウト値(秒)の指定です。ファイルの検査時間は含みません。

	デフォルト値: **SocketTimeout** = 10

アーカイブファイルの検査時間を短縮するために次のパラメータを使用することができます(アーカイブ内のいくつかのオブジェクトは検査されません)。除外されたアーカイブに対する動作は該当するモジュールのArchiveRestrictionパラメータで定義されます。

MaxCompressionRatio = {value}	アーカイブファイルを展開して検査する際の圧縮比の上限値の指定です。 指定された圧縮比を超える場合には検査を行いません。 デフォルト値: **MaxCompressionRatio** = 500
CompressionCheckThreshold = {value in Kbytes}	アーカイブファイルの圧縮比を確認するファイルサイズの下限値(キロバイト)の指定です(**MaxCompressionRatio**パラメータで指定されている場合)。 デフォルト値: **CompressionCheckThreshold** = 1024
MaxFileSizeToExtract = {value in Kbytes}	アーカイブ中の最大ファイルサイズ(キロバイト)の指定です。 指定された値を超えたファイルは検査を行いません。 デフォルト値: **MaxFileSizeToExtract** = 40960
MaxArchiveLevel = {value}	アーカイブファイルを検査する際の最大ネストレベルの指定です。 最大ネストレベルを超えるアーカイブファイルは検査を行いません。

	デフォルト値: **MaxArchiveLevel** = 8

Dr.Web Daemonの起動

Daemonをデフォルト設定で起動させると、以下の処理が実行されます。

- 設定ファイルを検索して読み込みます。設定ファイルが見つからない場合、プロセスは終了します。設定ファイルへのパスは、起動時にコマンドラインパラメータ-ini: {path/to/your/drweb32.ini}で指定するか、デフォルトの設定ファイル(%etc_dir/drweb32.ini)を使用します。
- ログファイルを作成します。**Daemon**が使用するユーザアカウントは、ログファイルディレクトリに対して適切な権限を持っている必要があります。ユーザ権限の場合、デフォルトのログディレクトリ(/var/log/)に対して書き込み権限がありません。**User**パラメータを指定した場合、**LogFileName**パラメータでログファイルを適切な場所に指定する必要があります。
- 設定ファイルで指定された場所からライセンスキーファイルを読み込みます。ライセンスキーファイルが見つからない場合、プロセスは終了します。
- **User**パラメータが指定された場合、**Daemon**はユーザアカウントを作成し(デフォルト値:drweb)、適切な権限を付与します。
- **Engine**(drweb32.dll)を読み込みます。**Engine**が見つからない場合、または異常な場合、プロセスは終了します。
- 設定ファイルで指定された場所から、ウイルス定義ファイルを任意の順番で読み込みます。ウイルス定義ファイルが破損している、または見つからない場合でもプロセスは続行されます。
- **Daemon**モードになり、ログファイルに情報を出力します。
- **Daemon**と他の**Dr.Web for UNIX mail servers**ソリューションモジュールが連携するためのソケットを作成します。TCPソケットを使用している場合、複数の接続が可能です(少なくとも1つの接続が確立されていれば読み込みは続行されます)。UNIXソケットを使用している場合、**Daemon**のユーザアカウントはこのソケットを含んだディレクトリの読み取り、及び書き込み権限を持っている必要があります。モジュールのユーザアカウントはディレクトリそのものに対する実行アクセス、及びソケットファイルに対する読み込

み、書き込み権限を持っている必要があります。ユーザ権限の場合、デフォルトのログディレクトリ(/var/log/)に対して書き込み権限がありません。**User**パラメータが指定された場合、**Socket**パラメータを再定義してソケットファイルへのパスを指定する必要があります。ソケットが作成できなかった場合、プロセスは終了します。

- **Daemon**のPIDファイルが作成されます。**Daemon**のユーザアカウントはPIDファイルを含んだディレクトリに対して適切な書き込み権限を持っている必要があります。ユーザ権限の場合、デフォルトのログディレクトリ(/var/log/)に対して書き込み権限がありません。**User**パラメータが指定された場合、**PidFile**パラメータを再定義してPIDファイルへのパスを指定する必要があります。PIDファイルが作成できなかった場合、プロセスは終了します。

シグナルの処理

Dr.Web Daemonは、以下のシグナルを受け取ることができます。

- SIGHUP – 設定ファイルの再読み込み
- SIGTERM – **Daemon**の終了要求
- SIGKILL – **Daemon**の強制終了(何か問題が発生した場合)

Dr.Web Daemonのテストと診断

Daemonの稼働状態を確認する場合、以下のようなコマンドを実行します。

```
$ netstat -a
```

必要なソケットが全て作成されているかどうかを確認してください。

TCP ソケット:

```
--- cut ---
Active Internet connections (servers and
established)
Proto  Recv-Q  Send-Q  Local Address  Foreign
Address  State
tcp  0  0  localhost:3000  *:*  LISTEN
```

```
raw  0  0 *:icmp  *:*  7
raw  0  0 *:tcp  *:*  7
Active UNIX domain sockets (servers and
established)
Proto  RefCnt  Flags  Type  State  I-Node  Path
unix  0  [ ACC ]  STREAM  LISTENING  384  /dev/
gpmctl
unix  0  [ ]  STREAM  CONNECTED  190  @0000001b
unix  1  [ ]  STREAM  CONNECTED  1091
@00000031
unix  0  [ ACC ]  STREAM  LISTENING  403 /tmp/.
font-unix/fs7100
unix  4  [ ]  DGRAM  293  /dev/log
unix  1  [ ]  STREAM  CONNECTED  1092  /dev/
gpmctl
unix  0  [ ]  DGRAM  450
unix  0  [ ]  DGRAM  433
unix  0  [ ]  DGRAM  416
unix  0  [ ]  DGRAM  308
--- cut ---
```

Unix ソケット:

```
--- cut ---
Active Internet connections (servers and
established)
Proto  Recv-Q  Send-Q  Local Address  Foreign
Address  State
raw  0  0 *:icmp  *:*  7
raw  0  0 *:tcp  *:*  7
Active UNIX domain sockets (servers and
established)
```

```
Proto  RefCnt  Flags  Type  State  I-Node  Path
unix  0  [ ACC ]  STREAM  LISTENING  384 /dev/
gpmctl
unix  0  [ ]  STREAM  CONNECTED  190 @0000001b
unix  1  [ ]  STREAM  CONNECTED  1091 @00000031
unix  0  [ ACC ]  STREAM  LISTENING  1127 %
var_dir/.daemon
unix  0  [ ACC ]  STREAM  LISTENING  403 /tmp/.
font-unix/fs7100
unix  4  [ ]  DGRAM  293  /dev/log
unix  1  [ ]  STREAM  CONNECTED  1092 /dev/
gpmctl
unix  0  [ ]  DGRAM  450
unix  0  [ ]  DGRAM  433
unix  0  [ ]  DGRAM  416
unix  0  [ ]  DGRAM  308
--- cut ---
```

コンソールに出力されている結果が上記と異なる場合や必要なソケットがリスト上に無い場合、**Daemon**の起動に失敗しています。

Daemonのコンソールクライアント(drwebdc)を使用してテストを実行し、サービス情報を確認してください。

TCP ソケット:

```
$ drwebdc -nHOSTNAME -pPORTNUM -sv -sb
```

Unix ソケット:

```
$ drwebdc -uSOCKETFILE -sv -sb
```

コンソールに以下のような情報が出力されます。

```
--- cut ---
- Version: DrWeb Daemon 6.00
- Loaded bases:
```

```
Base /var/drweb/bases/drwtoday.vdb
contains 5 records.
Base /var/drweb/bases/drw60003.vdb
contains 409 records.
Base /var/drweb/bases/drw60002.vdb
contains 543 records.
Base /var/drweb/bases/drwebase.vdb
contains 51982 records.
Base /var/drweb/bases/drw60001.vdb
contains 364 records.
Total 53303 virus-finding records.
--- cut ---
```

上記のような出力結果を得られない場合は、診断モードでdrwebdcを実行します。

TCPソケット:

```
$ drwebdc -nHOSTNAME -pPORTNUM -sv -sb -v
```

UNIXソケット:

```
$ drwebdc -uSOCKETFILE -sv -sb -v
```

詳細ログを元に問題箇所の特定を行うことができます。

```
dwlib: fd: connect() failed - Connection
refused
dwlib: tcp: connecting to 127.0.0.1:3300 -
failed
dwlib: cannot create connection with a DrWeb
daemon
ERROR: cannot retrieve daemon version
Error -12
```

Daemonのテストを行う場合は、製品パッケージに含まれているeicar.comプログラムを使用することができます。readme.eicarファイルをテキストエディタで開き、記載内容に従ってeicar.comファイルに変更してください。

50アドレス以上のメールサーバーに対するライセンスを使用する場合：

TCPソケット:

```
$ drwebdc -nHOSTNAME -pPORTNUM -f eicar.com
```

UNIXソケット:

```
$ drwebdc -uSOCKETFILE -f eicar.com
```

15～30アドレスのメールサーバーに対するライセンスを使用する場合：

TCPソケット:

```
$ drwebdc -nHOSTNAME -pPORTNUM -e -FEMAIL_ADDRESS -REMAIL_ADDRESS -f eicar.com
```

UNIXソケット:

```
$ drwebdc -uSOCKETFILE -e -FEMAIL_ADDRESS -REMAIL_ADDRESS -f eicar.com
```

EMAIL_ADDRESS はemail.iniの中のアドレスの1つです。

以下のような情報が出力されることを確認してください。

```
Results: daemon return code 0x20
(known virus is found)
```

上記のような出力結果を得られない場合、ファイルが検査されたかどうか**Daemon**ログファイルを確認してください。検査されていない場合は上記の方法で診断を実行してください。

上記の出力結果を得られた場合は、**Daemon**を稼働させることが出来ます。

検査モード

Dr.Web Daemonは、以下のモードでウイルス検査が可能です。

- ソケット経由で受信するデータの検査（リモート検査モード）
- ディスク上のファイル検査（ローカル検査モード）

リモート検査モードの場合、**Daemon**はソケットから検査データを受信します。**Daemon**はソケットから受信したあらゆるデータ、ファイルを検査することができます。このモードでは読み取り権限無しでファイルの検査を行うことができますが、ローカル検査モードに比べ効率は劣ります。

ローカル検査モードの場合、**Daemon**はディスク上の指定されたファイルの検査を行います。このモードではクライアントは、検査するファイルへのパスだけを**Daemon**に送るので、効率的で簡単に利用できるというメリットがあります。

ローカル検査モードではユーザ権限を正確に調整する必要があります。**Daemon**は、指定されたそれぞれのファイルに対して読み取り権限を持っている必要があります。

Daemonをメールサーバーと使用する場合は注意が必要です。通常メールフィルターはメールシステムの代わりとして動作し、その権限を使用するからです。ローカル検査モードでは、メールフィルターはメールシステムから受信したメッセージのファイルを作成し、そこへのパスを**Daemon**に提供します。この時点で、フィルターが適切なファイルを作成するディレクトリに対するアクセス権限を慎重に指定する必要があります。**Daemon**によって権限を使われているユーザをメールのサブシステムグループに含むか、または**Daemon**をメールシステムユーザの権限で起動するかどちらかを推奨します。

システムが正しく設定されていれば**Daemon**はルート権限を使う必要がありません。

Dr.Web Updater

Dr.Web Updaterは、**Dr.Web for UNIX mail servers**ソリューションのウイルス定義ファイルを自動更新するための、Perlで書かれたコンソールスクリプト update.plで、**Dr.Web for UNIX mail servers**の実行ファイルを含んだディレクトリ内にあります。

Dr.Web Updaterの設定は、%etc_dirディレクトリ内にあるdrweb32.ini設定ファイルの[Updater]セクションに定義されています。他の設定ファイルを使用する場合、起動時にそのファイルへのフルパスをコマンドラインパラメータで指定してください。

スクリプトを実行するには以下のコマンドを使用します。

```
$ %bin_dir/update.pl [parameters]
```

更新

Dr.Web for UNIX mail serversソリューションを最適な状態で使用するには、ウイルス定義ファイルを定期的に更新する必要があります。

ウイルス定義ファイルは、".vdb"の拡張子です。アップデートサーバでは、lzmaアーカイブで保存される場合もあります。新しいウイルスが発見されると、それらを記述したデータベースの小さなファイル(数KBしかない)がリリースされ、迅速で効果的な対処が可能です。

ウイルス定義ファイルの更新には、デイリーアップデート (drwtoday.vdb)とウィークリーアップデート(drwXXXYY.vdb)があります。 XXX は、ウイルス検査エンジンのバージョンを示しており、YYは00から始まる連番です(例えばバージョン6.0に対する最初の更新はdrw60000.vdb)。

デイリーアップデートは、新種のウイルスに対応するために毎日、あるいは1日に数回もリリースされています。新しいデイリーアップデートが適用された場合、drwtoday.vdbファイルは上書きされます。また、新しいウィークリーアップデートが適用された場合、drwtoday.vdbファイルの内容はdrwXXXYY.vdbファイルにコピーされ、新しい空のdrwtoday.vdbファイルが生成されます。

ウイルス定義ファイルを手動で更新したい場合、まず最初に、実行されなかった定期的な更新を全てインストールする必要があります。次に、drwtoday.vdbファイルを上書きします。

メインのウイルス定義ファイルに更新を追加するには、該当するファイルを**Dr.Web for UNIX mail servers**実行ファイルのディレクトリ(デフォルトでは/var/drweb/bases/)か、設定ファイルで指定されたディレクトリに配置してください。

drwrisky.vdb、drwnasty.vdbの2つ追加ファイルで、アドウェアやダイヤラ-、ハッキングプログラムなどの不正プログラムに対応する定義ファイルを提供します。拡張子や形式は、ウイルス定義ファイルと同様です。

アンチウイルス技術は発展を続けているため、新しいバージョンのアンチウイルスパッケージが適宜リリースされます。更新されたアルゴリズムが含まれ、ウイルス検査エンジン(**Engine**)に実装されます。それと同時に、リリースされた全ての更新が1つにまとめられ、既知のウイルス全てが記録されたウイルス定義ファイルによって新しいバージョンのパッケージは完全なものになります。通常、新しい定義ファイルは古い**Engine**に接続することも出来ます。ただし、その場合新しいウイルスの検出や修復は保証されません。そのためには**Engine**のアルゴリズムがアップグレードされている必要があるからです。

ウイルス、その他の不正プログラムに対応する定義ファイルには、以下のような種類があります。

- drwebase.vdb – 製品リリース時に同梱されるウイルス定義ファイル
- drwXXXYY.vdb – ウイルス定義ファイルのウィークリーアップデート(drwtoday.vdbの1週間分を集約したファイル)
- drwtoday.vdb – ウイルス定義ファイルのデイリーアップデート
- drwnasty.vdb – 製品リリース時に同梱されるマルウェア定義ファイル
- dwnXXXYY.vdb – マルウェア定義ファイルのウィークリーアップデート(dwntoday.vdbの1週間分を集約したファイル)
- dwntoday.vdb – マルウェア定義ファイルのデイリーアップデート
- drwrisky.vdb – 製品リリース時に同梱されるリスクウェア定義ファイル
- dwrXXXYY.vdb – リスクウェア定義ファイルのウィークリーアップデート(dwrtoday.vdbの1週間分を集約したファイル)
- dwrtoday.vdb – リスクウェア定義ファイルのデイリーアップデート

cronの設定

For Linux:ソフトウェアのインストール中に、ユーザ設定の特別なファイルが/etc/cron.d/ ディレクトリ内に作成されます。これによりcronと**Dr.Web Updater**間のインタラクションが有効になります。

For FreeBSD and Solaris: cronと**Dr.Web Updater**間のインタラクションを有効にするには、cronを手動で設定する必要があります。

例えば、FreeBDSを使用する場合は drwebユーザのcrontabに以下のストリングを加えることが出来ます。

```
*/30 * * * * /usr/local/drweb/update.pl
```

Solarisを使用する場合は以下のコマンドを使います。

```
# crontab -e drweb
# 0,30 * * * * /opt/drweb/update.pl
```

コマンドラインパラメータ

Dr.Web Updater のパラメータは、設定ファイルに定義する方法と以下のコマンドラインパラメータで指定する方法があります。

- --ini=path_to_configuration_file;
- --what=component_to_be_updated.

Component_to_be_updatedは、scannerまたは、daemonです。この値が指定されない場合、**Updater**は設定ファイルの情報を使用します。

また、コマンドラインパラメータとして --not-need-reloadパラメータを指定することができます。

- --not-need-reloadが指定されていない場合、update.plの処理が終了すると全てのdaemonが再起動されます(定義ファイルの追加や削除など、更新があった場合のみ再起動されます)。
- --not-need-reloadは 指定されているがそれに対する値が設定されていない場合、update.pl終了後どのdaemonも再起動されま

せん（定義ファイルの追加や削除など、更新があった場合でも再起動されません）。

daemonの名前を `--not-need-reload`パラメータの値として使用することが出来ます。空白を使わずにカンマで区切ることによって複数の名前を1つのストリング内で指定することが可能です。大文字小文字の区別はありません。名前がパラメータ値として指定されたdaemonは再起動されません。

例:

```
$ %bin_dir/update.pl --not-need-reload=drwebd
```

設定ファイル

Updaterの設定は、`%etc_dir`ディレクトリ内にある設定ファイル（デフォルトでは`drweb32.ini`）に保存されています。他の設定ファイルを使う場合は、起動時にファイルへのフルパスをコマンドラインパラメータで指定してください。

設定ファイルの構造やパラメータの種類についての説明は、設定ファイルの章を参照してください。

`[Updater] section`

UpdatePluginsOnly = {Yes | No}	Yesが指定された場合、プラグインのみが更新されます。**Daemon**および**Scanner** は更新されません。 デフォルト値: **UpdatePluginsOnly** = No
Section = {Daemon | Scanner}	**Daemon**と**Scanner** のどちらを更新対象とするかの指定です。 コマンドラインパラメータの `--what` で指定された場合、`--what`オプションが優先されます。 デフォルト値: **Section** = Daemon
ProgramPath = {path to file}	**Daemon**または**Scanner** へのパスです。**Dr. Web Updater**が製品バージョンやAPI情報を取得するために使用します。 デフォルト値:

	ProgramPath = %bin_dir/drwebd
SignedReader = {path to file}	電子署名されたファイルの検証用プログラムのパスの指定です。 デフォルト値: **SignedReader** = %bin_dir/read_signed
LzmaDecoderPath = {path to file}	lzmaアーカイブを展開するプログラムのパスの指定です。 デフォルト値: **LzmaDecoderPath** =
LockFile = {path to file}	**Dr.Web Updater**実行時のロック用ファイルのパスの指定です。 デフォルト値: **LockFile** = %var_dir/run/update.lock
CronSummary = {Yes | No}	Yesの場合、**Dr.Web Updater**の実行結果は標準出力に出力されます。**Updater**がcronによって実行されている場合、管理者にメールで通知するためにこのモードを使用することができます。 デフォルト値: **CronSummary** = Yes
DrlFile = {path to file}	ウイルス定義ファイルやウイルス検査エンジンなどを更新するための更新サーバのURLが定義されたリストの指定です。**Dr.Web Updater**は、リストからランダムにサーバを選択し、更新を行います。このリストは、**Dr.Web**によって電子署名されているため編集しないでください。更新は自動的に実行されます。 デフォルト値: **DrlFile** = %var_dir/bases/update.drl

CustomDrlFile = {path to file}	カスタムdrlファイル(*.drl)のパスの指定です。**Dr.Web** によって電子署名されているため編集しないでください。更新は自動的に実行されます。 デフォルト値: **CustomDrlFile** = %var_dir/bases/custom.drl
FallbackToDrl = {Yes | No}	どの*.drlファイルを最初に使用するかの指定です。Yesの場合、**Updater**は、**CustomDrlFile** で指定されたリストを使用します。失敗した場合、**DrlFile** で指定されたリストが使用されます。 デフォルト値: **FallbackToDrl** = Yes
DrlDir = {path to directory}	プラグインを更新するための更新サーバのURLが定義されたリストを含むディレクトリの指定です。リストは、**Dr.Web**によって電子署名されているため編集しないでください。 デフォルト値: **DrlDir** = %var_dir/drl/
Timeout = {numerical value in seconds}	更新時のダウンロードにおけるタイムアウト(秒)の指定です。 デフォルト値: **Timeout** = 90
Tries = {numerical value}	**Dr.Web Updater**が更新サーバに接続を試みる回数の指定です。 デフォルト値: **Tries** = 3

ProxyServer = {proxy server name or IP}	プロキシサーバの指定です。プロキシサーバを使用して更新する場合は、プロキシサーバのホスト名または、IPアドレスを指定してください。 デフォルト値: **ProxyServer** =
ProxyLogin = {proxy server user login}	プロキシサーバの認証に用いるユーザ名の指定です。 デフォルト値: **ProxyLogin** =
ProxyPassword = {proxy server user password}	プロキシサーバの認証に用いるユーザのパスワードの指定です。 デフォルト値: **ProxyPassword** =
LogFileName = {file name}	ログファイルの指定です。syslogを指定することができます(**SyslogFacility**と**SyslogPriority**パラメータの指定が必要です)。 デフォルト値: **LogFileName** = syslog
SyslogFacility = {Daemon | Local0 .. Local7 | Kern | User | Mail}	syslogのファシリティの指定です。 デフォルト値: **SyslogFacility** = Daemon
LogLevel = {Debug | Verbose | Info | Warning | Error | Quiet}	ログの詳細レベルの指定です。 デフォルト値: **LogLevel** = Verbose
LotusdPidFile = {path to file}	**Lotus Daemon** PID ファイルのパスの指定です。 デフォルト値:

	LotusdPidFile = %var_dir/run/drweblotusd.pid
MaildPidFile = {path to file}	drweb-maild PID ファイルのパスの指定です。 デフォルト値: **MaildPidFile** = %var_dir/run/drweb-maild.pid
IcapdPidFile = {path to file}	drweb-icapd PID ファイルのパスの指定です。 デフォルト値: **IcapdPidFile** = %var_dir/run/drweb_icapd.pid
BlacklistPath = {path to directory}	.dwsフィルが保存されるディレクトリの指定です。 デフォルト値: **BlacklistPath** = %var_dir/dws
AgentConfPath = {path to file}	**Agent**の設定ファイルのパスです。 デフォルト値: **AgentConfPath** = %var_dir/agent.conf
PathToVadeRetro = {path to file}	libvaderetro.so ライブラリのパスです。 デフォルト値: **PathToVadeRetro** = %var_dir/lib/libvaderetro.so
ExpiredTimeLimit = {number}	ライセンスキーの有効期限について、残り日数を知らせるための指定です。 デフォルト値: **ExpiredTimeLimit** = 14

ESLockfile = {path to file}	ロックファイルのパスです。ロックファイルが存在している場合、**Dr.Web Updater**はcronによる自動実行はされません。
	デフォルト値: **ESLockfile** = %var_dir/run/es_updater.lock

更新プロセス

更新プロセスは、以下の手順で行われます。

- **Dr.Web Updater**が設定ファイルを読み込みます。
- **Dr.Web Updater**は[Updater]セクションのパラメータだけでなく、**EnginePath**、**VirusBase**、**UpdatePath**、**PidFile**のパラメータも使用します。
- **Dr.Web Updater**は、更新サーバから利用可能なアップデートのリストを要求し、対応するlzmaアーカイブをダウンロードします。lzmaが見つからない場合は、*.vdb形式でダウンロードします[Updater]セクションの**LzmaDecoderPath**パラメータに指定されている解凍ユーティリティによって、lzmaアーカイブからファイルを抽出します。。
- ダウンロードされたアップデートはUpdatingに記載されているとおり、対応するディレクトリに配置されます。

Dr.Web Agent

Dr.Web Control Agentモジュール（以後**Agent**）は、メモリ常駐型モジュールです。**Dr.Web for UNIX mail servers**ソリューションのモジュールに対する様々な設定を行ったり、利用可能なライセンスに基づいてアンチウイルスポリシーを決定し、ウイルスの統計を収集するために使用します。**Dr.Web for UNIX mail servers**の別々のモジュールを開始したり、全体の設定が変更された場合、**Agent**がそれらのモジュールに、必要な全ての設定情報を送信します。制御シグナルを交換することによって、他のモジュールとのインタラクションが可能です。

Dr.Web for UNIX mail serversソリューションの全てのコンポーネント（**Monitor**を除く）は、設定を drweb-agentモジュール経由で受け取るので、このモジュールが他の全てのモジュールより先に（ただしdrweb-monitorモジュールの後で）起動している必要があります。

同じ名前を持つ複数のパラメータを設定ファイル内で指定する場合、**Agent**はそれらをカンマで区切って1つのストリング内にまとめます。1つの大きなルールを複数の小さなルールに分けることが出来るので、このオプションはルールを指定する際に役に立ちます。

例:

```
GlobalRules = select message, append_html "lookup:file:/maild-files/somehtml.html"
```

このルールは以下のように指定することも出来ます。

```
GlobalRules = select message
GlobalRules = append_html "lookup:file:/maild-files/somehtml.html"
```

設定ファイルでのルールの記述やパラメータ値にバックスラッシュ"\"を使用することも出来ます。この場合、**Agent**はバックスラッシュで分けられた全てのラインを1つにまとめます。バックスラッシュの後に空白は使えません。

例:

```
to:neko@neko cont \
```

```
modifier/LocalRules=select mime.headers "X-Spam-Level" "\\*\\*\\*", \
# 3 or more stars
if found,\
select mime.headers Subject ".*",\
replace "[SPAM] " "^",\
endif
```

動作モード

Dr.Web for UNIX mail serversを使用し、**Dr.Web Enterprise Security Suite**によって管理されたアンチウイルスネットワークに接続することが出来ます。そのような集中管理モードで動作するために、追加のソフトウェアをインストールしたり**Dr.Web for UNIX mail servers**をアンインストールする必要はありません。

そのために、**Agent**は以下の2つのモードのいずれかで動作することが出来ます。

- Standaloneモード。保護するコンピューターがアンチウイルスネットワークに含まれていない、又はリモート操作されていない場合。このモードでは、設定ファイルおよびキーファイルはローカルドライブ上にあり、**Agent**は保護するコンピューターから管理されます。
- Enterpriseモード(集中管理モード)。保護するコンピューターが集中管理サーバから管理されている場合。このモードでは、**Dr.Web for UNIX mail servers**のいくつかの機能や設定がセキュリティポリシーに従って変更、またはブロックされることがあります。ライセンスキーファイルは集中管理サーバから受け取るので、ローカルコンピューター上のキーファイルは使用されません。

Enterpriseモード(集中管理モード)を使用する場合

1. 集中管理サーバへの接続に必要となる情報(公開鍵や接続先の情報など)をウイルス対策の管理者に確認します。
2. **Agent**の設定ファイル(デフォルト:`%etc_dir/agent.conf`)の`[EnterpriseMode]`セクションで以下のパラメータを設定してください。

- 管理者に確認した公開鍵ファイルの場所を`PublicKeyFile`パラメータで指定してください（通常、`%var_dir/drwcsd.pub`）。このファイルは、**Dr.Web Enterprise Security Suite**へのアクセスで利用する暗号鍵を含んでいます。ウイルス対策の管理者の方は、**Dr.Web Enterprise Security Suite**サーバの対応するディレクトリで公開鍵ファイルの存在を確認することができます。
- **Dr.Web Enterprise Security Suite**のIPアドレスまたはホスト名に`ServerHost`パラメータを指定してください。
- **Dr.Web Enterprise Security Suite**のポート番号（通常2193）に`ServerPort`パラメータを指定してください。

3. 集中管理サーバに接続する為に、`UserEnterpriseMode`パラメータに**Yes**を指定してください。

   集中管理モードでは、**Dr.Web for UNIX mail servers**のいくつかの機能や設定がセキュリティポリシーに従って変更、またはブロックされることがあります。ライセンスキーファイルは集中管理サーバから受け取るので、ローカルコンピューター上のキーファイルは使用されません。

Dr.Web for UNIX mail servers が集中管理モードをフルサポートする為に、**Monitor**の動作もEnterpriseモードに設定する必要があります。詳細については **Dr.Web UNIX Monitor**の Operation Modeをご覧ください。

Standaloneモードを使用する場合

1. **Agent**の設定ファイル（デフォルト: `%etc_dir/agent.conf`）の`[StandaloneMode]`セクションですべてのパラメータが適切に指定されていることを確認します。
2. **Agent**設定ファイルの`[EnterpriseMode]`セクションで`UseEnterpriseMode`パラメータに**No**を指定してください。

   このモードに変更すると**Dr.Web for UNIX mail servers**の全ての設定はロック解除され、前回の、またはデフォルトの値に復元されます。再度**Dr.Web for UNIX mail servers**の全ての機能にアクセスし、設定を行うことが出来ます。

Dr.Web for UNIX mail serversがStandaloneモードで正常に動作するためには有効なライセンスキーファイルが必要です。このモードでは、集中管　理サーバから受け取ったキーファイルは使用できません。

コマンドラインパラメータ

Agentでは、以下のコマンドラインパラメータを使用することができます。

- `-h, --help` – コマンドラインパラメータのヘルプを表示します。
- `-v, --version` – 現在の**Agent** のバージョンに関する情報を表示します。
- `-u, --update-all` – すべてのモジュールを更新します。
- `-f, --update-failed` – 標準モードによる更新に失敗したモジュールを更新します。
- `-C, --check-only` – 設定のチェックのみを行います。**Agent**起動時にはこのコマンドラインパラメーターは使用できません。
- `-p, --newpwd` – **Dr.Web ESS**にアクセスするためのユーザ名とパスワードを変更します。
- `-d, --droppwd` – **Dr.Web ESS**にワークステーションを再登録するために、**Dr.Web ESS**に登録したユーザ名とパスワードを破棄します。
- `-c <path to file>, --conf <path to file>` – 設定ファイルへのパスの指定です（デフォルト以外を指定する場合）。
- `-s <path to file>, --socket <path to file>` – ソケットの指定です。
- `-P <path to file>, --pid-file <path to file>` – **Agent**のPIDファイルのパスの指定です。
- `-e <application name>, --export-config <application name>` – 引数で指定するアプリケーションの**Dr.Web ESS**サーバーへのエクスポート。**Agent**起動時にはこのコマンドラインパラメーターは使用できません。

設定ファイル

Dr.Web Agentの設定は、`%etc_dir/agent.conf` に定義されています。

[Logging]セクション

`[Logging]`セクションには、**Dr.Web Agent**のロギングに関する設定が定義されています。

`[Logging]`

Level = {Quiet | Error | Alert | Info | Debug}	**Agent**のログの詳細レベルの指定です。 デフォルト値: **Level** = Info
IPCLevel = {Quiet | Error | Alert | Info | Debug}	IPCライブラリのログの詳細レベルの指定です。 デフォルト値: **IPCLevel** = Error
SyslogFacility = {Daemon | Local0 .. Local7 | Kern | User | Mail}	syslogのファシリティの指定です。 デフォルト値: **SyslogFacility** = Daemon
FileName = {path}	ログファイルの指定です。 syslogを指定することができます。 デフォルト値: **FileName** = syslog

[Agent]セクション

[Agent]セクションには、**Dr.Web Agent**に関する設定が定義されています。

[Agent]

MetaConfigDir = {path to directory}	drweb-agentのメタ設定ファイル(meta-configuration files)があるディレクトリ名の指定です。**Agent**と**Dr.Web** 製品の他のモジュールが連携するために必要な設定が定義されています。**Dr.Web** によって提供されるため、編集の必要はありません。 デフォルト値: **MetaConfigDir** = %bin_dir/agent/
UseMonitor = {Yes | No}	Yesの場合、**Monitor** が **Dr.Web for UNIX mail servers**の一部として動作するようにdrweb-agentに通知します。 デフォルト値: **UseMonitor** = Yes
MonitorAddress = {address}	**Agent**と**Monitor**が連携するために使用するソケットの指定です。(**Monitor**の設定ファイルで定義されている**Address**パラメータの値と同じでなくてはなりません。) デフォルト値: **MonitorAddress** = local:%var_dir/ipc/.monitor
MonitorResponseTime = {time in seconds}	drweb-monitorモジュールからの応答を待つ最大時間(秒)の指定です。指定された時間内に**Monitor**からの応答がない場合、**Agent**は、drweb-monitorが起動していないと判断し、**Monitor**との接続確立を終了します。

	デフォルト値: **MonitorResponseTime** = 5
PidFile = {path to file}	**Agent**のPIDファイルのパスの指定です。 デフォルト値: **PidFile** = %var_dir/run/drweb-agent.pid

[Server]セクション

[Server]セクションには、**Dr.Web Agent**と**Dr.Web for UNIX mail servers**のその他のモジュールが連携するための設定が定義されています。

[Server]

Address = {socket address}	ソフトウェアモジュールと**Agent**が連携するために使用されるソケットの指定です。カンマ区切りで複数のソケットを指定することができます。 デフォルト値: **Address** = local:%var_dir/ipc/.agent, inet:4040@127.0.0.1
Threads = {numerical value}	drweb-agentのスレッド数の指定です。**Agent**にウイルス統計を通知するモジュールの最大同時接続数を制御します。このパラメータの値はSIGHUPシグナルを使って変更することは出来ません。 デフォルト値: **Threads** = 2
Timeout = {time in seconds}	**Agent**と他の**Dr.Web**モジュールが接続を確立する際のタイムアウト値。 デフォルト値: **Timeout** = 15

[EnterpriseMode]セクション

[EnterpriseMode]セクションには、**Agent**が**Enterprise**モードで動作するための設定が定義されています。

[EnterpriseMode]

UseEnterpriseMode = {Yes | No}	Yesの場合、drweb-agentはEnterpriseモードで動作し、Noの場合はStandaloneモードで動作します。 デフォルト値: **UseEnterpriseMode** = No
ComputerName = {text value}	**Dr.Web Enterprise Security Suite**ネットワークでのコンピュータ名の指定です。 デフォルト値: **ComputerName** =
VirusbaseDir = {path to directory}	ウイルス定義ファイルが配置されているディレクトリの指定です。 デフォルト値: **VirusbaseDir** = %var_dir/bases
PublicKeyFile = {path to file}	**Dr.Web Enterprise Security Suite**サーバへの接続に使用する公開鍵のパスの指定です。 デフォルト値: **PublicKeyFile** = %bin_dir/drwcsd.pub
ServerHost = {IP address}	**Dr.Web Enterprise Security Suite**サーバのIPアドレスの指定です。 デフォルト値: **ServerHost** = 127.0.0.1

ServerPort = {port number}	**Dr.Web Enterprise Security Suite**サーバのポート番号の指定です。 デフォルト値: **ServerPort** = 2193
CryptTraffic = {Yes | Possible | No}	**Dr.Web Enterprise Security Suite**サーバと**Agent**間のトラフィックの暗号化に関する指定です。 デフォルト値: **CryptTraffic** = possible
CompressTraffic = {Yes | Possible | No}	**Dr.Web Enterprise Security Suite**サーバと**Agent**間のトラフィックの圧縮に関する指定です。 デフォルト値: **CompressTraffic** = possible
CacheDir = {path to directory}	設定ファイルや**Dr.Web Enterprise Security Suite**サーバへの登録情報などが保存されるディレクトリの指定です。 デフォルト値: **CacheDir** = %var_dir/agent

[StandaloneMode]セクション

[StandaloneMode] セクションには、**Agent**が**Standalone**モードで動作するための設定が定義されています。

[StandaloneMode]

StatisticsServer = {server address}	ウイルス統計サーバのIPアドレスまたは、ホスト名の指定です。 デフォルト値: **StatisticsServer** = stat.drweb.com:80/update

StatisticsUpdatePeriod = {time in minutes}	統計情報の更新レートの指定です。このパラメータの値には5分以上を指定してください。 デフォルト値: **StatisticsUpdatePeriod** = 10
StatisticsProxy = {proxy server address}	ウイルス統計プロキシサーバのIPアドレスまたは、ホスト名の指定です。 例: StatisticsProxy = localhost:3128 デフォルト値: **StatisticsProxy** =
StatisticsProxyAuth = {text value}	プロキシサーバへのアクセスに利用するユーザ名とパスワードの指定です。 例: StatisticsProxyAuth = test:testpwd デフォルト値: **StatisticsProxyAuth** =
UUID = {identifier}	ウイルス統計サーバ http://stat.drweb.com/ で利用するユニークなユーザ識別子の指定です。UUIDは、統計の転送に必要です。機能を有効にする場合は、このパラメータ値に個人のUUIDを指定する必要があります(通常、ライセンスキーファイルのmd5 sumが使用されます)。 デフォルト値: **UUID** =
LicenseFile = {path to file}	Dr.Webのライセンスキーファイル、またはデモキーファイルの指定です。 デフォルト値:

	LicenseFile = %bin_dir/drweb32.key
ProtectedEmails = {lookups}	保護された電子メールアドレスのリストの指定です。これらは明示的に指定することが出来ます。またはアドレスを含むファイルへのパスを指定、lookupを使用することも可能です。 デフォルト値: **ProtectedEmails** = file:%etc_dir/email.ini

[Update]セクション

[Update] セクションには、**Dr.Web Enterprise Security Suite**から**Dr.Web for UNIX mail servers**のコンポーネントを更新するための定義が含まれています。

[Update]

CacheDir = {path to directory}	**Agent**がダウンロードした更新ファイルを一時保存するディレクトリの指定です。 デフォルト値: **CacheDir** = %var_dir/updates/cache
RegFile = {path to file}	インストール済みの更新情報に関するファイルの指定です。 デフォルト値: **RegFile** = %var_dir/agent.reg
Timeout = {time in seconds}	**Agent**がダウンロードした更新ファイルを処理する際のタイムアウト値(秒)の指定です。 デフォルト値: **Timeout** = 120
RootDir = {path to	ルートディレクトリの指定です。

directory}	デフォルト値: **RootDir** = /

詳細については、**Dr.Web Enterprise Security Suite**の*管理者用ガイド*を参照してください。

Dr.Web Unix Control Agentの起動

ポストインストールスクリプトで"Configuration Services"オプションを選択した場合は、**Dr.Web Agent**を含むすべてのサービスは自動的に起動します。

Agentがデフォルト設定で起動すると、以下の処理が実行されます。

1. 設定ファイルを読み込みます。設定ファイルが見つからない場合、**Agent**は終了します。
2. [EnterpriseMode] セクションのパラメータが正しく設定されており、**Dr.Web for UNIX mail servers**ソリューションがアンチウイルスネットワーク内で動作している場合、**Agent**はEnterpriseモードで起動します。それ以外の場合で、[Standalone]セクションのパラメータが正しく設定されている時は、**Agent**はStandaloneモードで起動します。[Standalone]セクションのパラメータが設定されていない場合、**Agent**は終了します。
3. **Agent**と他の**Dr.Web**モジュールが連携する為のソケットが作成されます。TCPソケットを使用する場合は複数の接続が可能です(少なくとも1つの接続が確立されていれば読み込みは続行されます)。UNIXソケットを使用する場合、drweb-agentを実行する権限を持つユーザがそのディレクトリに対する書き込み、および読み込み権限を持っている場合にのみソケットが作成されます。ソケットが作成されなかった場合、**Agent**は終了します。

現時点では**Dr.Web for UNIX mail servers** は**Dr.Web Enterprise Security Suite**との統合をサポートしていません。**Agent**はStandaloneモードでのみ動作可能です。

各動作モードごとの先の手順は以下のとおりです。

Enterpriseモードの場合

- **Agent**は、**Dr.Web Enterprise Security Suite**に接続します。**Dr.Web Enterprise Security Suite**に接続できなかった場合や認証プロセスが失敗した場合、**Agent**はStandaloneモードでの起動を試みます。接続が確立された場合は読み込みが続行されます。
- **Agent**がキーファイルと設定情報を**Dr.Web Enterprise Security Suite**から受け取ります。それらを全て受信した後で、**Agent**は動作可能な状態になります。

Standaloneモードの場合

- **Agent**と他の**Dr.Web**モジュールが連携する為のmeta-configurationファイルがロードされます。ファイルの場所は**Agent**設定ファイルの`[Agent]`セクション内の `MetaConfigDir`パラメータで設定されています。meta-configurationファイルの読み込みに成功すると**Agent**が動作可能な状態になります。

他のソフトウェアとの連携

他のソフトウェアとの連携は、**Agent**のmetaconfigurationファイル(amc-files)によって行われます。これらのファイルは、それぞれの**Dr.Web**モジュールが **Agent**から受け取る設定パラメータ値を定義します。

このモジュールの名前が付いた`Application`セクションで、それぞれのモジュールに関する設定が定義されています。セクションの終端では、`EndApplication`を指定する必要があります。

モジュールの設定には以下のパラメータが定義されている必要があります。

- **`id`**: **Dr.Web Enterprise Security Suite**内のモジュールのID。
- **`ConfFile`**: モジュールの設定ファイルへのパス。
- **`Components`**: コンポーネントの定義。セクションの終端では`EndComponents`を指定する必要があります。それぞれのコンポーネントに対して、名前、設定ファイル内のセクション一覧、およびそれらのセクション内の、コンポーネントの正常な動作に必要なパラメータが指定されます。セクションの一覧、およびパラメータはカンマで区切られます。個々のパラメータを正しく定義するためにフルパスを指定してください(例:`/Quarantine/DBISettings`)。セクションの定義には名前のみ指定してください(例:`General`)。セクションおよびパラメータの定義では

改行にバックスラッシュ（\）を使用します。

Dr.Web MailD for Linuxのamc-fileの例:

```
Application "MAILD"
 id       40
 ConfFile    "/etc/drweb/maild_smtp.conf"
 Components
 lookup_ldap  LDAP
 lookup_regex  REGEX
 drweb-maild  General, Logging, MailBase, Stat,
Maild, Filters,
            Quarantine, /_Rules=Rule*:Rules, /
Reports/Send,
          /Reports/SendTimes, /Reports/Names, /
Reports/MaxPoolSize,
           /Reports/MaxStoreInDbPeriod,Reports/
CheckForRemovePeriod,
               /Notifier/FilterMail, /Notifier/
NotifyLangs,
         /Notifier/LngBaseDir
 drweb-notifier General, Logging, Notifier, /
Sender/Method, /_Rules,
         Reports, /Filters/BeforeQueueFilters,
                 /Filters/AfterQueueFilters, /
Quarantine/AccessByEmail,
         /Quarantine/StoredTime
 drweb-sender  General, Logging, Sender
 drweb-receiver  General,  Logging,  /Maild/
ProtectedNetworks,
               /Maild/ProtectedDomains, /Maild/
IncludeSubdomains,
         SASL, Receiver
```

```
 EndComponents
EndApplication
```

ウイルス統計情報

Agentはウイルス統計情報をコントロールモジュールから受け取り、**Dr.Web**のウイルス統計サイト http://stat.drweb.com/ （インターネット接続が可能な場合）、または**Dr.Web Enterprise Security Suite**（**Agent**がEnterpriseモードで動作している場合）に送信します。**Agent**がこの統計サイトに接続するには、ユニークなユーザ識別子（UUID）が必要です。デフォルトでは、ライセンスキーファイルのMD5チェックサムがUUIDとして使用されます。**Dr.Web**テクニカルサポートサービスに依頼してUUIDを取得することも可能ですが、この場合は、**Agent**の設定ファイルで明示的にUUIDを指定する必要があります。

統計サイトでは、ある特定のサーバ、**Dr.Web Anti-virus for UNIX systems**によって、あるいはアンチウイルスプラグインを持った**Doctor Web**ソリューションによってサポートされた全てのサーバに対するウイルスの集計を見ることが出来ます。**Agent**は、連携する複数の異なる**Dr.Web**製品から同時に統計を処理することが出来ます。

統計処理結果には期間中に最も多く検出されたウイルスに関する情報（検出の数、全体の割合）が含まれています。

統計はHTMLとXML形式になっています。このデータを他のサイトに載せる場合、Webサイトのコンセプトやデザインに合わせて変化させることが可能な後者が便利です。

http://stat.drweb.com/にアクセスすることで、**Dr.Web**によって収集されたウイルス統計情報を参照することができます。サポートする全てのサーバについての、検出されたウイルスの数および全体の割合のリストを見ることが出来ます。

このWebページは、お使いのブラウザによって表示が異なる場合があります。

Start date: 11 May 2007, 00:00 Mail
End date: 11 May 2007, 11:00 Files
Top: 10 Query Plot graph

11.05.2007 00:00 - 11.05.2007 11:00		
1	Win32.HLLM.Beagle	17570 (29.94%)
2	Win32.HLLM.Netsky.35328	8585 (14.63%)
3	Win32.HLLM.MyDoom.based	5757 (9.81%)
4	Win32.HLLM.Netsky.based	5408 (9.21%)
5	Win32.HLLM.Perf	3873 (6.60%)
6	Win32.HLLM.Graz	3639 (6.20%)
7	Win32.HLLM.MyDoom.33808	3128 (5.33%)
8	Win32.HLLP.Sector	1294 (2.20%)
9	Win32.HLLM.Beagle.pswzip	1092 (1.86%)
10	Win32.HLLM.MyDoom.49	944 (1.61%)

Total scanned: 3638081
Total infected: 58688 (1.61%)

図 15. ウイルス統計情報

検索条件を変更して何度も検索するには:

1. **Mail**または**Files**フラグを指定して、電子メール内で検出されたウイルスの統計を表示するか、ファイル内で検出されたウイルスの統計を表示するかを選択します。
2. **Start date**と**End date**のドロップダウンリストで、検索対象とする期間を指定します。
3. **Top**フィールドに、統計テーブルで表示するウイルスの数を入力します（最も多く検出されたウイルスから表示されます）。
4. 統計をグラフィックでも表示したい場合は **Plot graph** チェックボックスにチェックを入れます。
5. **Query**ボタンをクリックします。 http://info.drweb.com/export/xml/top でウイルス統計情報のXMLフォームを確認することができます。

例:

```
<drwebvirustop period="24" top="5"
vdbaseurl="http://info.drweb.com/
virus_description/" updatedutc="2009-06-09
09:32:02">
    <item>
        <vname>Win32.HLLM.Netsky</vname>
        <dwvlid>62083</dwvlid>
        <place>1</place>
        <percents>34.201062139103</percents>
    </item>
    <item>
        <vname>Win32.HLLM.MyDoom</vname>
        <dwvlid>9353</dwvlid>
        <place>2</place>
        <percents>25.1303270912579</percents>
    </item>
    <item>
        <vname>Win32.HLLM.Beagle</vname>
        <dwvlid>26997</dwvlid>
        <place>3</place>
        <percents>13.4593034783378</percents>
    </item>
    <item>
        <vname>Trojan.Botnetlog.9</vname>
        <dwvlid>438003</dwvlid>
        <place>4</place>
        <percents>7.86446592583328</percents>
    </item>
```

```
    <item>
        <vname>Trojan.DownLoad.36339</vname>
        <dwvlid>435637</dwvlid>
        <place>5</place>
        <percents>7.31494163115527</percents>
    </item>
</drwebvirustop>
```

このファイルでは以下のXML属性が使用されています。

- period – 統計情報の収集期間(時間)
- top – 統計情報内での、多く検出されたウイルスの順位
- updatedutc – 統計情報の最終更新日時
- vname – ウイルス名
- place – 統計上のウイルスの場所
- percents – 検出の割合

periodパラメータの値とサンプルのサイズはユーザが変更することは出来ません。

パーソナライズされた統計情報を得るには:

以下のいずれかのWebページにアクセスしてください。

- HTMLでの統計情報を見るには http://stat.drweb.com/view/<UUID> にアクセスしてください。
- XMLフォームでの統計情報を見るには http://stat.drweb.com/xml/<UUID> にアクセスしてください。

どちらの場合も <UUID> はライセンスキーファイルのMD5チェックサムです(**Dr.Webテクニカルサポート**から受け取ったUUIDを持っていない限り)。

例:

```
<drwebvirustop period="24" top="2" user="<UID>"
lastdata="2005-04-12 07:00:00+04">
    <item>
```

```
        <caught>69</caught>
        <percents>24.1258741258741</percents>
        <place>1</place>
        <vname>Win32.HLLM.Netsky.35328</vname>
    </item>
    <item>
        <caught>57</caught>
        <percents>19.9300699300699</percents>
        <place>2</place>
        <vname>Win32.HLLM.MyDoom.54464</vname>
    </item>
</drwebvirustop>
```

このファイルでは以下のXML属性が使用されています。

- period – 統計情報の収集期間（時間）
- top – 統計情報内での、多く検出されたウイルスの順位
- user – ユーザ識別子
- lastdata – ユーザがサーバにデータを送信した最終日時
- vname – ウイルス名
- place – 統計上のウイルスの場所
- caught – ある特定のウイルスの検出数
- percents – 検出の割合

periodパラメータの値とサンプルのサイズはユーザが変更することは出来ません。

Dr.Web Monitor

Dr.Web Unix Monitor（以後**Monitor**）は、メモリ常駐型のモジュールです。

Dr.Web Unix Monitorは、**Dr.Web for UNIX mail servers**全体の耐障害性を向上する役割を担っています。ソフトウェアモジュールおよびコンポーネントの正常な起動と停止、異常発生時の再起動を確実に行います。**Monitor**はすべてのモジュールを起動し、必要に応じて付加コンポーネントの読み込みを行います。モジュールの起動に失敗すると、**Monitor**はその後何度も起動を試み、その回数および間隔は**Monitor**の設定で定義されています。

すべてのモジュールをロードすると**Monitor**はそれらのモジュールを永続的に制御し、モジュールまたはコンポーネントが異常動作した場合は、異常が生じたアプリケーションを再起動します。再起動を試みる回数の上限と間隔は、**Monitor**の設定ファイルに定義されています。モジュールが異常動作を始めると、**Monitor**がシステム管理者に通知します。**Monitor**は制御シグナルを送ることで**Dr.Web Control Agent**と連携することが出来ます。

動作モード

Dr.Web for UNIX mail serversを使用し、**Dr.Web Enterprise Security Suite**によって管理されたアンチウイルスネットワークに接続することが出来ます。そのような集中管理モードで動作するために、追加のソフトウェアをインストールしたり**Dr.Web for UNIX mail servers**をアンインストールする必要はありません。

そのために、**Agent**は以下の2つのモードのいずれかで動作することが出来ます。

- Standaloneモード。保護するコンピューターがアンチウイルスネットワークに含まれていない、又はリモート操作されていない場合。このモードでは、設定ファイルおよびキーファイルはローカルドライブ上にあり、**Agent**は保護するコンピューターから管理されます。 モジュールは**Monitor**設定ファイル内の設定で起動します。

- Enterpriseモード（集中管理モード）。保護するコンピューターが集中管理サーバから管理されている場合。このモードでは、**Dr.Web for UNIX mail servers**のいくつかの機能や設定がセキュリティポリシーに従って変更、またはブロックされることがあります。ライセンスキーファイルは集中管理サーバから受け取るので、ローカルコンピューター上のキーファイルは使用されません。

Enterpriseモード（集中管理モード）を使用する場合

1. 集中管理サーバへの接続に必要となる情報（公開鍵や接続先の情報など）をウイルス対策の管理者に確認します。
2. **Monitor**の設定ファイル（デフォルト: `%etc_dir/monitor.conf`）の `UseEnterpriseMode`のパラメータに**Yes**に指定してください。

   集中管理モードでは、**Dr.Web for UNIX mail servers**のいくつかの機能や設定がセキュリティポリシーに従って変更、またはブロックされることがあります。ライセンスキーファイルは集中管理サーバから受け取るので、ローカルコンピューター上のキーファイルは使用されません。

Dr.Web for UNIX mail servers が集中管理モードをフルサポートする為に、**Agent**の動作もEnterpriseモードに設定する必要があります。詳細については **Dr.Web UNIX Agent** の Operation Modeをご覧ください。

Standaloneモードを使用する場合

1. **Monitor**の設定ファイル（デフォルト: `%etc_dir/monitor.conf`）の`[Monitor]`セクションで`RunAppList`パラメータに、**Monitor**の起動に必要なすべてのパラメータが含まれていることを確認します。
2. **Monitor**設定ファイルの`[Monitor]`セクションで`UseEnterpriseMode`パラメータに`No`を設定します。

   このモードに変更すると**Dr.Web for UNIX mail servers**の全ての設定はロック解除され、前回の、またはデフォルトの値に復元されます。再度**Dr.Web for UNIX mail servers**の全ての機能にアクセスし、設定を行うことが出来ます。

Dr.Web for UNIX mail serversがStandaloneモードで正常に動作するためには有効なライセンスキーファイルが必要です。このモードでは、集中管　理サーバから受け取ったキーファイルは使用できません。

コマンドラインパラメータ

Dr.Web　Monitorでは、以下のコマンドラインパラメータを使用することができます。

- `-h, --help` - コマンドラインパラメータのヘルプを表示します。
- `-v, --version` - 現在の **Monitor**のバージョンに関する情報を表示します。
- `-u, --update` - 更新モード
- `-C, --check-only` - 設定のチェックのみを行います。
- `-A, --check-all` - すべてのモジュールの設定をチェックします。
- `-c <path to file>, --conf <path to file>` - 設定ファイルへのパスの指定です（デフォルト以外を指定する場合）。
- `-r, --run component1[,component2]`- コンポーネントを起動します（指定した順序で起動）。

  例:

  `-r AGENT, DAEMON`

設定ファイル

Dr.Web Monitorの設定は、`%etc_dir/monitor.conf` に定義されています。

[Logging]セクション

Dr.Web Monitorの設定には、設定ファイル（デフォルトでは`% etc_dir/monitor.conf.`）を使用します。設定ファイルの構造やパラメータの種類につ

いての説明は、本書の設定ファイルの章を参照してください。

[Logging]

Level = {Quiet | Error | Alert | Info | Debug}	**Monitor**のログの詳細レベルの指定です。 デフォルト値: **Level** = Info
IPCLevel = {Quiet | Error | Alert | Info | Debug}	IPCライブラリのログの詳細レベルの指定です。 デフォルト値: **IPCLevel** = Error
SyslogFacility = {Daemon | Local0 .. Local7 | Kern | User | Mail}	syslogのファシリティの指定です。 デフォルト値: **SyslogFacility** = Daemon
FileName = {syslog | path to file}	ログファイルの指定です。 syslogを指定することができます。 デフォルト値: **FileName** = syslog

[Monitor]セクション

[Monitor] セクションには、**Monitor**の主要な設定が全て定義されています。

[Monitor]

RunForeground = {Yes | No}	Yesの場合、**Monitor**はdaemonモードを使用できません。 通常は、デフォルトのNo(デーモン)を使用します。特別なユーティリティ(daemontoolsなど)を使用する場合にYesを指定します。 デフォルト値: **RunForeground** = No

User = {user name}	特定のユーザ権限で**Monitor**を実行するユーザ名の指定です。 デフォルト値: **User** = drweb
Group = {group name}	特定のユーザ権限で**Monitor**を実行するユーザのグループの指定です。 デフォルト値: **Group** = drweb
PidFileDir = {path to directory}	**Monitor**の起動時にそのPIDファイルが保存されるディレクトリの指定です。 デフォルト値: **PidFileDir** = %var_dir/run/
ChDir = {path to directory}	**Monitor**起動時に作業ディレクトリを変更する場合の指定です。指定した場合、**Monitor**は作業ディレクトリを指定されたディレクトリに変更します。 デフォルト値: **ChDir** = /
MetaConfigDir = {path to directory}	メタ設定ファイル(meta-configuration files)があるディレクトリ名の指定です。**Monitor**と**Dr.Web**製品の他のモジュールが連携するために必要な設定が定義されています。**Dr.Web**によって提供されるため、編集の必要はありません。 デフォルト値: **MetaConfigDir** = %etc_dir/monitor/
Address = {address}	**Monitor**が制御シグナルを受信するために使用するソケットの指定です。 デフォルト値:

	Address = local:%var_dir/ipc/.monitor
Timeout = {time in seconds}	Monitorと他のDr.Webモジュールが接続を確立する際のタイムアウト値の指定です。 デフォルト値: **Timeout** = 5
TmpFileFmt = {text}	一時ファイル名の指定です。 例:path_to_file.XXXXXX X - 一時利用する乱数 デフォルト値: **TmpFileFmt** = %var_dir/msgs/tmp/monitor.XXXXXX
RunAppList = {text}	Monitorによって起動するモジュールの指定です。カンマ区切りで複数指定が可能です。 システムからコンポーネントをアンインストールする場合には、**RunAppList**パラメータ値からそのコンポーネント名を削除する必要があります。それ以外の場合、Monitorがその他のコンポーネントを起動及び初期化することが出来なくなります。 デフォルト値: **RunAppList** = AGENT
UseEnterpriseMode = {Yes | No}	Enterpriseモードの指定です。 Yesの場合、Monitorによって起動するモジュールの一覧は、**RunAppList**パラメータからではなく、drweb-agent から受け取ります。 Noの場合、Standaloneモードで動作します。 デフォルト値: **UseEnterpriseMode** = No

RecoveryTimeList= {time in seconds}	モジュールを再起動する際のインターバル(秒)の指定です。 カンマ区切りで複数の値を指定することができます。1つ目のパラメータ値で指定されたインターバルの後、モジュールの再起動を試みます。2回目の試行は2つ目のパラメータ値で指定し、3回目以降も同じです。 デフォルト値: **RecoveryTimeList** = 0,30,60
InjectCmd = {string}	レポートを送信するコマンドの指定です。 root@localhost以外のアドレスにレポートを送信したい場合は、そのアドレスをコマンド内で指定する必要があります。 デフォルト値: **InjectCmd** = "/usr/sbin/sendmail -t"
AgentAddress = {socket address}	**Monitor**が**Agent**と連携するために使用するソケットの指定です。(**Dr.Web Agent**の設定ファイルの**Address** パラメータで指定されている値と同じである必要があります。) デフォルト値: **AgentAddress** = local:%var_dir/ipc/.agent
AgentResponseTime = {time in seconds}	drweb-agentモジュールからの応答を待つ最大時間(秒)の指定です。 指定時間の間に**Agent**から応答がない場合、**Monitor**はdrweb-agentエージェントが動作していないと判断し、**Agent**の再起動を試みます。 デフォルト値: **AgentResponseTime** = 5

Dr.Web Unix Monitorの起動

ポストインストールスクリプトで"Configuration Services"オプションを選択した場合は、**Dr.Web Agent**を含むすべてのサービスは自動的に起動します。

Monitorがデフォルト設定で起動すると、以下の処理が実行されます。

1. 設定ファイルを読み込みます。設定ファイルが見つからない場合、**Monitor**は終了します。
2. daemonモードになり、ログファイルに情報を出力します。
3. **Monitor**と他のモジュールが連携するためのソケットを作成します。TCPソケットを使用している場合、複数の接続が可能です(少なくとも1つの接続が確立されていれば読み込みは続行されます)。UNIXソケットを使用している場合、drweb-monitorを実行する権限を持つユーザがそのディレクトリに対する書き込み、および読み込み権限を持っている場合にのみ作成されます。ソケットが作成できなかった場合、プロセスは終了します。
4. Monitor PID情報を持ったPIDファイルが作成されます。作成されなかった場合、読み込みは終了します。
5. drweb-monitorモジュールが他のソフトウェアモジュールを起動します。モジュールの起動に失敗した場合、**Monitor**は再起動を試みます。全ての再試行に失敗した場合、**Monitor**は前回起動したモジュールを全てアンロードして終了します。モジュールの起動に関する問題は、利用できるいずれかの方法(ログファイルに出力、電子メールで通知、特定のプログラムを起動)で**Monitor**によってレポートされます。モジュールが使用する通知の方法は**Monitor**のmeta-configurationファイル内で設定されています。

自動モードでDr.Web Monitorを起動させるには:

- %etc_dir/drweb-monitor.enable ファイルのENABLE変数値が 1に 変更されている必要があります(LinuxとSolarisの場合)。
- または/etc/rc.conf ファイルにdrweb_monitor_enable="YES"の記述が追加されている必要があります(FreeBSDの場合)。

他のソフトウェアとの連携

他のソフトウェアとの連携は、*Monitor configuration files* (mmc-files) によって行われます。mmc-filesは、**Dr.Web Monitor**と連携できる製品パッケージに含まれています。これらのファイル内にはコンポーネントのコンテンツ、バイナリのロケーション、その起動する順番、及び起動パラメータが定義されています。

このモジュールの名前が付いたApplicationセクションで、それぞれのモジュールに関する設定が定義されています。セクションの終端では、EndApplicationを指定する必要があります。

以下のパラメータが定義されている必要があります。

- **FullName** - コンポーネントのフルネーム
- **Path** - バイナリファイルへのパス
- **Depends** - 先に起動している必要があるコンポーネントの名前。例えば、DAEMONを起動する場合には先にAGENTが起動している必要があり、**Dr.Web Daemon**のmmc-files内のDependsパラメータはAGENT値を持っています。依存関係がない場合は、このパラメータをスキップすることができます。
- **Components** - コンポーネントの起動時に起動するモジュール（このパラメータで指定された順番で）のバイナリファイル。それぞれのモジュールに対する、コマンドラインパラメータ（引用符で囲まれている場合があります）、起動及びシャットダウンのタイムアウト、通知の種類、及び起動の権限。

  Notification type - コンポーネントの不具合に関する通知をどこに送信するかを定義します。MAIL値が指定されている場合、通知はメールで送信され、LOG値 が指定されている場合は情報がログに出力されます。

  Startup privileges - どのグループまたはユーザの権限を使用してコンポーネントを起動するかを定義します。

Dr.Web Daemon for Linuxのmmc-fileの例:

```
Application "MAILD"
 FullName     "Dr.Web (R) MailD"
 Path       "/opt/drweb/"
```

```
 Depends     "AGENT"
 Components
  # name       args    MaxStartTime MaxStopTime
NotifyType User:Group
  drweb-notifier local:/var/drweb/ipc/.agent 30
30 MAIL drweb:drweb
  drweb-sender  local:/var/drweb/ipc/.agent 15
30 LOG  drweb:drweb
  drweb-maild   local:/var/drweb/ipc/.agent 120
30 MAIL drweb:drweb
  drweb-receiver local:/var/drweb/ipc/.agent 15
30 MAIL root:drweb
 EndComponents
EndApplication
```

Dr.Web for UNIX Mail Servers

Dr.Web for UNIX mail serversは、お互いに連携するソフトウェアモジュールのグループです。**Dr.Web for UNIX mail servers**モジュールはSMTP及びLMTPプロトコルのproxy-serverとして、または幅広いMTA（Sendmail、Postfix、Exim、CommuniGate Pro、Courier、Zmailer、Qmail）に対して、自身の設定、統計情報、レポート、及び隔離機能を持ったフィルタとして動作することが出来ます。

Dr.Web for UNIX mail serversのコンポーネントは以下のアルゴリズムに従い、連携してメールを処理します。

1. **Receiver**コンポーネントはメールシステムから直接、またはSMTP/LMTPプロトコル経由でメールを受信し、メールを検査する`drweb-maild`コンポーネントに転送します。

   インストールされているメールシステムや使用するプロトコルによって、このコンポーネントの機能は異なるモジュールで実行されます（`drweb-receiver`、`drweb-milter`、`drweb-cgp-receiver`など）。複数の**Receiver**モジュール間の同期オペレーションに対応し、複数のソースから同時にメールを受信、処理することが可能です。**Receiver**モジュールのいくつかは`drweb-maild`コンポーネントによるメール検査の結果を受け取るとすぐに、受信したメールを変更、送信することが出来ます。例えば`drweb-milter`モジュールはこの機能を持ち、SMTPセッションが閉じる前に検査結果をSendmailシステムに返すことが可能です。

2. `Drweb-maild`モジュールはメール処理システムの主要なコンポーネントです。メールのMIME処理を行い、プラグインにメールを転送します。また、データベースにメールを保存する役割も果たします。検査結果は**Receiver**コンポーネント（結果を待つ時間がタイムアウトしていない場合）か**Sender**コンポーネントのどちらかに送られます。
3. メールは`drweb-maild`モジュールに接続されたプラグインによって処理されます。ユーザは`drweb-maild`モジュールの動作を妨げることなく、いつでもプラグインを起動、またはその接続を切ることが出来ます。メールはユーザによって設定された順番で処理され、プラグインが作成したメールは全て**Sender**コンポーネント経由で送信されます。プラグインの中には、正常に動作するためにデータベースのサポートが必要なものがあります。
4. **Sender**コンポーネントは、メールを別々のメールシステムに直接、またはSMTP/LMTPプロトコル経由で送信します。インストールされているメールシステムや使用するプロトコルによって、このコンポーネントの機能は異なるモジュールで実行されます（`drweb-sender`、`drweb-cgp-sender`など）。**Sender**コンポーネントは`drweb-maild`、

drweb-notifier、drweb-monitorからメールの送信要求を受け取ることが出来ます。

5. drweb-notifierモジュールはソフトウェアシステムの動作中にレポートを作成、送信します。プラグイン、およびその他のシステムコンポーネントがレポートの作成を要求することが出来ます（例えば、ウイルスが検出された時など）。Drweb-maildモジュールは、接続された全てのプラグインの動作に関する統計情報の一般レポートの作成要求を送信することが出来ます。**Sender**コンポーネントは、メールの送信失敗についてのDSNレポートを要求することが出来ます。レポートは送信者、受信者、及びシステム管理者に送信されます。
6. drweb-agentモジュールによって、メール処理システムは**Dr.Web Enterprise Security Suite**と連携してStandaloneモード、及びEnterpriseモードで動作することが出来ます。Enterpriseモードでは、全てのシステムコンポーネント（drweb-monitor以外）がdrweb-agentモジュール経由で設定情報を受け取ります。そのため、drweb-agentモジュールは他のコンポーネントより先に起動している必要があります。drweb-agentはまた、ライセンスの有効性を検査し、システムコンポーネントの動作に関する統計情報（ブロックしたオブジェクト名、処理したファイルの合計サイズなど）を収集します。
7. drweb-monitorモジュールは、ユーザの設定した順番で他のシステムモジュールを起動、終了させます。また、それらの動作を監視し、異常な動作を始めたモジュールを再起動させ、システム管理者に通知します（設定でそのようなアクションが指定されていた場合）。

以下のプラグインを使用することが出来ます。

- drweb - **Dr.Web Daemon**モジュールを使用して、受信する全てのメールのウイルス検査を実行します。メールは分解されて**Daemon**に転送されるため、MIME処理は必要ありません。
- headersfilter - メールをヘッダでフィルタリングします。フィルタリングルールに正規表現（Perl）を使うことが出来ます。
- vaderetro - 独自の**VadeRetro**ライブラリを使用してスパムメールをフィルタリングします。このライブラリは動的にアップデートされています。**VadeRetro**はメール処理の速さに優れています。
- modifier - このプラグインによって、メールの内容やエンベロープに応じてメール全体、またはその一部を変更することが出来ます。検査したメールに英数字の署名を加えたり、スパムと判定されたメールから画像を削除することが出来ます。

コマンドラインパラメータ

全てのUNIXプログラム同様、**Dr.Web for UNIX mail servers**のソフトウェアモジュールはコマンドラインパラメータの使用をサポートしています。

コマンドラインは以下のようになります。

`module_name [parameters] agent_socket`

- `module_name` は、**Dr.Web for UNIX mail servers** モジュールの名前です（例: `drweb-maild`、または`drweb-notifier`）。
- `parameters` は、追加のコマンドラインパラメータです。
- `agent_socket` は、**Dr.Web for UNIX mail servers**モジュールが**Dr.Web Agent**から設定情報を受け取る際に経由するソケットです。

利用可能なパラメータの一覧は、`-h`、または`-help`パラメータでモジュールを実行することで確認できます。**Dr.Web for UNIX mail servers**モジュールの現在のバージョンでは以下のコマンドラインパラメータを使用できます。

- `-v, --version` – 現在のモジュールのバージョンです。
- `-l <level>, --level <level>` – **Dr.Web for UNIX mail servers**モジュールのログの詳細レベルです。デフォルト値は `info` です。
- `-t <value in seconds>, --timeout <value in seconds>` – 設定情報の受信を待つ最大時間です。
- `--component arg` – **Agent**に設定情報を要求する際に使用するコンポーネントの名前です。
- `--log-name arg` – ロギングに使用するコンポーネントの名前です。
- `--unique-id arg` – **Receiver**と**Sender**コンポーネントのユニークなIDです。このパラメータによって複数の**Receiver**と**Sender**が同時に動作することが可能になります。**Receiver**と**Sender**のそれぞれのコンポーネントは起動時にユニークなIDを受け取ります。メールの送信には同じIDを持った**Receiver**/**Sender**コンポーネントのペアが選択されます（適切なSenderが見つからない場合はデフォルトの**Sender**を使用します）。利用可能な**Sender**の一覧は`SIGHUP`を使用してリロードされます。
- `--check-only` – モジュールをこのパラメータで起動すると設定の検査が実行されます。正常に機能するためには**Dr.Web Agent**が動作

している必要があります。

検査が正常に終了すると、以下のメッセージがコンソールに出力されます。

```
Options OK
```

検査の間にエラーが発生した場合は、以下のメッセージがコンソールに出力されます。

```
Options ERROR
```

- `--check-all` - このパラメータで起動すると**Dr.Web Monitor**は自身の設定だけでなく、他のモジュールの設定も検査します。

例:

```
$ drweb-maild -t 30 local:%var_dir/ipc/.agent
```

`local:%var_dir/ipc/.agent`内の**Agent**のソケットを使用し、設定データの受信タイムアウト30秒で**Dr.Web MailD**を起動します。

シグナル

全てのプログラムモジュールは、以下のシグナルのメモリサポートプロセッシング内に常駐しています。

- `SIGHUP` - **Dr.Web Monitor**がこのシグナルを受信すると、動作中の全てのコンポーネントに設定を再読み込みさせます。
- `SIGINT`と`SIGTERM` - このシグナルのどちらかを受信すると、モジュールは動作を終了します。

以下のモジュールは追加のシグナルを処理することが出来ます。

- **Receiver**および**Sender**コンポーネントは`SIGALRM`シグナルを受信すると、内部ディレクトリ構造を検査して失われたメールを探します。そのようなメールが見つかった場合は送信を試みます。
- **Sender**コンポーネントは`SIGUSR2`シグナルを受信すると、内部キューにある全てのメッセージの送信を試みます。
- **Receiver**モジュールは`SIGUSR1`シグナルを受信すると、アドレス検査の統計情報を別々のファイルに保存します。

- 全てのコンポーネントはSIGUSR1シグナルを受信すると、動的スレッドプールの動作、及び持続的接続に関する統計情報のファイルをDr.Web MailD設定ファイル[General]セクションの**BaseDir**パラメータ内で指定されたディレクトリに保存します。

内部統計情報

スレッドプールの動作、およびそれらのプールに対する持続的接続に関する統計情報は、スレッドプールの設定内(Dr.Web MailD設定ファイルの**InPoolOptions**と**OutPoolOptions**パラメータ)で追加パラメータ**stat** = yesを指定することによって、その設定が明示的に有効になっている場合のみ収集されます。

例:

InPoolOptions = auto, **stat** = yes

SIGUSR1シグナル受信時に作成されるファイルの名前は以下のようになります。

- name_[callback_](cli|srv)[.unique-id].txt – 接続に関する統計情報
- name_[callback_](thr[N])[.unique-id].txt – プールに関する統計情報

  - name – "drweb-" の部分を除いたコンポーネントの名前。
  - callback – Receiver インターフェースのコールバック。
  - cli – クライアント 接続。
  - srv – server 接続。
  - unique-id – ユニークな識別子で起動するモジュール。
  - thr – スレッドプール。

このようなファイルが既に存在している場合、統計情報はこのファイルの最後に追加されます。

エントリの始まりは以下のようになります。

```
==================================
start:  Tue Oct  9 14:44:15 2008
curr:   Tue Oct  9 14:44:29 2008
period: 0d 0h 0m 14s
```

統計情報収集の開始日、現在の日付、および出力に必要な時間の上限が表示されます。

srv には作成された、または閉じられた接続の数、別々のキュー内でのエレメント数の上限が表示されます。

```
closed: 0 (0 num/sec)
total created = 0 (0 num/sec)
max rea = 0 est = 0 don = 0 act = 0
```

cliには要求に応じて作成された、またはタイムアウトで閉じられた接続の数、それらの平均数および現在の数が表示されます。

```
created on request = 0 (0 num/sec)
closed by timeout = 0 (0 num/sec)
avg number = 0
current = 2
```

thr の出力は以下のようになります。

```
min = 2 max = 2147483647 type = 0 freetime = 120
busy max = 0 avg = 0
requests for new threads = 0 (0 num/sec)
creating fails = 0
max processing time = 0 ms; avg = 0 ms
curr = 2 busy = 0
```

- 1番目のライン - 1つのプール内の最小、および最大のスレッド数、プールの種類、追加のスレッドが休止状態の場合にそれを閉じるまでの最大時間(秒)が表示されます。
- 2番目のライン - ビジースレッドの最大および平均数が表示されます。

- 3番目のライン - 追加のスレッド作成要求の数および頻度が表示されます。
- 4番目のライン - 追加のスレッド作成に失敗した回数が表示されます。
- 5番目のライン - これらの要求を処理するのにかかる最大、および平均の時間が表示されます。
- 6番目のライン - プール内にある現在のスレッド数、ビジースレッドの数が表示されます。

調整とスタートアップ

Dr.Web for UNIX mail servers はデフォルト設定で使うことも出来ますが、最適な動作の為に、特定の要件や状況に応じて調整することが出来ます。

Dr.Web for UNIX mail servers の全ての設定は、`%etc_dir`ディレクトリ内にある3つの設定ファイルに保存されています。**Dr.Web MailD**の一般設定は`maild_MTA.conf`ファイル内にあります。**Dr.Web Agent**および**Dr.Web Monitor**の設定は `agent.conf` と `monitor.conf`ファイル内にあります。

Dr.Web for UNIX mail servers の全てのファイルがデフォルトのディレクトリ内にある場合、一般セットアップを`configure.pl`スクリプト(デフォルトでは`%bin_dir/maild/scripts/`ディレクトリ内にあります)経由で実行することが出来ます。起動後、このスクリプトは必須パラメータの値をプロンプトし、それらを`maild_MTA.conf`設定ファイルに書き込みます。メールトランスファーシステムとの連携に必要なその他のパラメータは、**Dr.Web MailD**設定ファイルを編集することによって手動で設定する必要があります。

設定ファイル

Dr.Web MailDの設定は、`%etc_dir/maild_MTA.conf`に定義されています。設定ファイルの構造やパラメータの種類についての説明は、設定ファイルの章を参照してください。

[General]セクション

`[General]` セクションには、**Dr.Web MailD**の一般設定が定義されています。

BaseDir = {path to directory}	メインの動作ディレクトリ。ソケット、データベース、その他のファイルが含まれています。**Dr.Web MailD**の現在のバージョンでは、変更された値はSUGHUPシグナルを受信してシステムを再起動した場合には反映されません。 デフォルト値: **BaseDir** = %var_dir/
MaxTimeoutForThreadActivity = {time}	スレッドを閉じるまでの最大待機時間。このパラメータはシステムを再起動、またはシャットダウンする際に使用します。システムがサインオフするまでのトータルの時間は次のように算出されます:プールの数と**MaxTimeoutForThreadActivity**パラメータ値を掛け合わせ、その結果に特定の時定数を加えます。 デフォルト値: **MaxTimeoutForThreadActivity** = 30s
IpcTimeout = {time}	コンポーネント間の通信タイムアウトの指定です。 デフォルト値: **IpcTimeout** = 40s
Hostname = {string}	**Dr.Web for UNIX mail servers**が動作しているホストの名前です。 デフォルト値: **Hostname** =

[Logging]セクション

[Logging] セクションでは、ロギングに関する設定が定義されています。ロギングは**Dr.Web for UNIX mail servers**の全てのメインモジュール対して実行されます。

Level = {Quiet | Error | Alert | Info | Debug}	ログの詳細レベルの指定です。 デフォルト値: **Level** = Info
IPCLevel = {Quiet | Error | Alert | Info | Debug}	IPCライブラリのログの詳細レベルの指定です。 デフォルト値: **IPCLevel** = Alert
SyslogFacility = {Daemon | Local0 .. Local7 | Kern | User | Mail}	syslogのファシリティの指定です。 デフォルト値: **SyslogFacility** = Mail
FileName = {syslog | path to file}	ログファイルの指定です。 syslogを指定することができます。 デフォルト値: **FileName** = syslog

SyslogFacilityパラメータにDaemon値が指定されている場合、データをファイルかsyslogに出力することが出来ます。syslogdを使用する場合、ストリングは全て以下のようになります。

```
'['tid']' name[.sub] level [id(/mta-id)] text
```

- tid – ストリングの出力に使用するスレッドの識別子
- name – 出力を実行するコンポーネントの名前(例:プラグイン名)
- sub – 出力を実行するコンポーネントサービスの名前

重要なサービスは以下のとおりです。

- ipc – インタープロセス通信サービス。
- thrN – スレッドプールサポートサービス。
- report – レポートサポートサービス。
- ldap、odbc、oracle、sqlite、mysql、postgres、cdb、berkeley、firebird – ルックアップサポートサービス。

- control – インタラクティブ管理サービス。
- parser – テンプレートパーササービス。
- MRS – SMTP/LMTPサービス経由でメールを受信。
- smtp – SMTPサービス経由でメールを送信。
- lmtp – LMTPサービス経由でメールを送信。
- pipe – PIPEサービス経由でメールを送信。
- queue – 内部キューサービスの処理。
- level – ログの詳細レベル。次の値を使用することが出来ます：FATAL、ERROR、WARN、INFO、DEBUG
- id – ログのラインにあるメールの識別子。数字は16進法で指定してください。
- mta-id – MTA（このメッセージを受信するMTA）の中にあるメッセージの識別子。**Dr.Web MailD**がMTAと統合されていて、そのような情報の取得が許可されている場合のみ使用出来ます。
- text – ログメッセージのテキスト。

モジュールが起動するとログの詳細レベルはデフォルトでINFOに設定され、**Agent**から設定を受け取った後、それに応じて変更されます。DEBUGレベルでのモジュール起動ログを見るために（例：**Agent**から受け取ったパラメータに関する情報を取得するため） --levelコマンドラインパラメータを使うことが出来ます（値をdebugに設定することによって）。

[MySQL]セクション

[MySQL]セクションには、**Dr.Web MailD**とMySQLデータベース間の連携を確立、維持する為の設定が定義されています。

User = {string}	MySQLデータベースユーザ名です。 デフォルト値： **User** =
Password = {string}	MySQLデータベースパスワードです。 デフォルト値： **Password** =

DB = {string}	MySQLデータベースの名前です。 デフォルト値: **DB** =
Host = {hostname}	MySQLデータベースが使用するホストの名前です。 デフォルト値: **Host** = localhost
Port = {port address}	MySQLデータベースへの接続に使用するポートです。 例: TCPソケットを使用する場合 **Port** = tcp://1234 UNIXソケットを使用する場合 **Port** = unix:///path/to/socket デフォルト値: **Port** =
Connections = {integer}	MySQLデータベースへの同時接続数。パラメータ値が0に設定されている場合、接続は要求に応じてその度に確立されます(通常、余分な時間がかかります)。先に接続が開設されている場合は、再接続に時間をかけることなくデータベースリクエストを順番に処理することが出来ます。 デフォルト値: **Connections** = 4
SizeLimit = {integer}	データベースの1リクエストに対して受け取る処理結果の最大数です。パラメータ値が0に設定されている場合、制限はありません。このパラメータ値は個別の外部参照設定内で指定することも出来ます。

	デフォルト値: **SizeLimit** = 10
SkipDomains = {LookupsLite}	データベースを参照しないドメインリストの指定です。このパラメータによって全体のパフォーマンスが向上し、サーバ負荷が大幅に軽減されます。このパラメータ値は個別の外部参照設定内で指定することも出来ます。 デフォルト値: **SkipDomains** =
Lib = {path to file}	libmysqlclient.so ライブラリへのパスの指定です。 デフォルト値: **Lib** = /usr/lib/libmysqlclient_r.so

[PostgreSQL]セクション

[PostgreSQL]セクションには、**Dr.Web MailD**とPostgreSQLデータベース間の連携を確立、維持する為の設定が定義されています。

ConnectionsString = {string}	PostgreSQLデータベースの接続設定のストリングです。 デフォルトパラメータを使用する場合、ストリングを空にすることが出来ます。また、スペースで区切って複数のパラメータ設定を含むことも可能です。各パラメータはkeyword = valueの書式で記載します。イコール記号の前後のスペースは任意です。空の値、またはスペースを含む値を記述する場合はそれらを一重引用符で囲ってください。 詳細については http://postgresql.org/docs/8.3/static/libpq-connect.html をご覧ください。 例: **ConnectionString** =

	host=localhost port=5432 user=ai password=qwerty dbname=drweb **ConnectionString** = hostaddr=127.0.0.1:5432 dbname=mailddb user=mailddbuser password=Str0ngPaSSw0rd デフォルト値: **ConnectionsString** =
SizeLimit = {integer}	データベースの1リクエストに対して受け取る処理結果の最大数です。パラメータ値が0に設定されている場合、制限はありません。 デフォルト値: **SizeLimit** = 10
SkipDomains = {LookupsLite}	データベースを参照しないドメインリストの指定です。このパラメータによって全体のパフォーマンスが向上し、サーバ負荷が大幅に軽減されます。このパラメータ値は個別の外部参照設定内で指定することも出来ます。 デフォルト値: **SkipDomains** =
Lib = {path to file}	**libpq.so** ライブラリへのパスの指定です。 デフォルト値: **Lib** = /usr/lib/libpq.so

[Firebird]セクション

[Firebird]セクションには、**Dr.Web MailD**とFirebirdデータベース間の連携を確立、維持する為の設定が定義されています。

Host = {hostname}	Firebirdデータベースのホスト名です。

	デフォルト値: **Host** = localhost
Database = {string}	Firebirdデータベースの名前です。 デフォルト値: **Database** =
User = {string}	Firebirdデータベースのユーザ名です。 デフォルト値: **User** =
Password = {string}	Firebirdデータベースのパスワードです。 デフォルト値: **Password** =
Charset = {string}	Firebirdデータベース内で使用されているcharsetエンコーディングです。 デフォルト値: **Charset** = us-ascii
SizeLimit = {integer}	データベースの1リクエストに対して受け取る処理結果の最大数です。パラメータ値が0に設定されている場合、制限はありません。 デフォルト値: **SizeLimit** = 10
SkipDomains = {LookupsLite}	データベースを参照しないドメインリストの指定です。このパラメータによって全体のパフォーマンスが向上し、サーバ負荷が大幅に軽減されます。このパラメータ値は個別の外部参照設定内で指定することも出来ます。 デフォルト値: **SkipDomains** =

Lib = {path to file}	libFBclient.so ライブラリへのパスの指定です。 デフォルト値: **Lib** = /usr/lib/libFBclient.so

[CDB]セクション

[CDB]セクションには、**Dr.Web MailD**とCDBデータベース間の連携を確立、維持する為の設定が定義されています。

Sources = {path to file}	CDBデータベースへのパス一覧です。 デフォルト値: **Sources** =
SkipDomains = {LookupsLite}	データベースを参照しないドメインリストの指定です。このパラメータによって全体のパフォーマンスが向上し、サーバ負荷が大幅に軽減されます。このパラメータ値は個別の外部参照設定内で指定することも出来ます。 デフォルト値: **SkipDomains** =

[Berkeley]セクション

[Berkeley]セクションには、**Dr.Web MailD**とBerkeleyデータベース間の連携を確立、維持する為の設定が定義されています。

Databases = {path to file}	データベースへのパス一覧です。 デフォルト値: **Databases** =
Environment = {path to directory}	Berkeleyデータベースの一時ロックファイルが保存されるディレクトリへのパスの指定です。 デフォルト値: **Environment** =

SizeLimit = {integer}	データベースの1リクエストに対して受け取るバイトの上限です。値は1024～65536の間で指定してください。それ以外の値を指定しても、強制的にその範囲内に含まれます。 デフォルト値: **SizeLimit** = 1
SkipDomains = {LookupsLite}	データベースを参照しないドメインリストの指定です。このパラメータによって全体のパフォーマンスが向上し、サーバ負荷が大幅に軽減されます。このパラメータ値は個別の外部参照設定内で指定することも出来ます。 デフォルト値: **SkipDomains** =
Lib = {path to file}	libdb.so ライブラリへのパスの指定です。 デフォルト値: **Lib** = /usr/lib/libdb.so

[SQLite]セクション

[SQLite]セクションには、**Dr.Web MailD**とSQLiteデータベース間の連携を確立、維持する為の設定が定義されています。

Database = {path to file}	SQLiteデータベースファイルへのパスの指定です。 デフォルト値: **Database** =
SizeLimit = {integer}	データベースの1リクエストに対して受け取る処理結果の最大数です。パラメータ値が0に設定されている場合、制限はありません。 デフォルト値: **SizeLimit** = 1

SkipDomains = {LookupsLite}	データベースを参照しないドメインリストの指定です。このパラメータによって全体のパフォーマンスが向上し、サーバ負荷が大幅に軽減されます。このパラメータ値は個別の外部参照設定内で指定することも出来ます。 デフォルト値: **SkipDomains** =
Lib = {path to file}	libsqlite3.soライブラリへのパスの指定です。 デフォルト値: **Lib** = /usr/lib/libsqlite3.so
BusyTimeout = {time in milliseconds}	**Dr.Web MailD**がデータベースにエントリを追加する際のタイムアウト時間の指定です。 デフォルト値: **BusyTimeout** = 2000

[ODBC]セクション

[ODBC]セクションには、**Dr.Web MailD**とODBCデータベース間の連携を確立、維持する為の設定が定義されています。

Lib = {path to file}	ODBCバージョン3.0以降をサポートするライブラリへのパスの指定です。ライブラリはスレッドサポートで作成されている必要があり、UnixODBCを推奨します。ライブラリはdlopenシステムコールを使用して配置されます(該当のマニュアルを参照してください)。現在のバージョンでは、SIGHUPシグナルでは変更が反映されません。 デフォルト値: **Lib** = /usr/lib/libodbc.so
ConnectData = {string}	ODBCデータベースへの接続用パラメータの指定です。以下の2つの書式を使用することが出来ます。 • USER/PASSWORD/@DSN

	• DSN=value;UID=value; PWD=value ODBCとの動作を開始するには、少なくともDSN値が指定されている必要があります。このパラメータ値は個別の外部参照設定内で指定することも出来ます。 デフォルト値: **ConnectData** =
SizeLimit = {string}	データベースの1リクエストに対して受け取る処理結果の最大数です。パラメータ値が0に設定されている場合、制限はありません。このパラメータ値は個別の外部参照設定内で指定することも出来ます。 デフォルト値: **SizeLimit** = 0
SkipDomains = {LookupsLite}	データベースを参照しないドメインリストの指定です。このパラメータによって全体のパフォーマンスが向上し、サーバ負荷が大幅に軽減されます。このパラメータ値は個別の外部参照設定内で指定することも出来ます。 デフォルト値: **SkipDomains** =

[Oracle]セクション

[Oracle]セクションには、**Dr.Web MailD**とOracleデータベース間の連携を確立、維持する為の設定が定義されています。

Lib = {path to file}	Oracle OTLバージョン8以降をサポートするライブラリへのパスの指定です。ライブラリはスレッドサポートで作成されている必要があります。ライブラリはdlopenシステムコールを使用して配置されます(該当のマニュアルを参照してください)。現在のバージョンでは、SIGHUPシグナルでは変更が反映されません。 デフォルト値:

		Lib =
ConnectData {string}	=	Oracleデータベースへの接続用パラメータの指定です。以下の2つの書式を使用することが出来ます。 • USER/PASSWORD/@DSN • DSN=value;UID=value; PWD=value Oracleとの動作を開始するには、少なくともDSN値が指定されている必要があります。このパラメータ値は個別の外部参照設定内で指定することも出来ます。 デフォルト値: **ConnectData** =
SizeLimit {string}	=	データベースの1リクエストに対して受け取る処理結果の最大数です。パラメータ値が0に設定されている場合、制限はありません。このパラメータ値は個別の外部参照設定内で指定することも出来ます。 デフォルト値: **SizeLimit** = 0
SkipDomains {LookupsLite}	=	データベースを参照しないドメインリストの指定です。このパラメータによって全体のパフォーマンスが向上し、サーバ負荷が大幅に軽減されます。このパラメータ値は個別の外部参照設定内で指定することも出来ます。 デフォルト値: **SkipDomains** =

[LDAP]セクション

[LDAP]セクションには、**Dr.Web MailD**とLDAPサーバ間の連携を確立、維持する為の設定が定義されています。

Lib = {path to file}	OpenLDAPバージョン2.0以降をサポートするライブラリへのパスの指定です。ライブラリはスレッドサポートで作成されている必要があります(ファイル名に"_r"サフィックスが含まれている必要があります)。ライブラリはdlopenシステムコールを使用して配置されます(該当のマニュアルを参照してください)。現在のバージョンでは、SIGHUPシグナルでは変更が反映されません。 デフォルト値: **Lib** = /usr/lib/libldap_r.so
Hostname = {string}	LDAPサーバのホスト名の指定です。未設定の場合はlocalhostが使用されます。このパラメータ値は個別の外部参照設定内で指定することも出来ます。 デフォルト値: **Hostname** =
Port = {number}	LDAPサーバのポート番号を指定します。未設定の場合は389が使用されます。このパラメータ値は個別の外部参照設定内で指定することも出来ます。 デフォルト値: **Port** = 389
Timeout = {time}	LDAPサーバ処理のタイムアウト時間の指定です。このパラメータ値は個別の外部参照設定内で指定することも出来ます。 デフォルト値: **Timeout** = 10s
Version = {string}	使用するLDAPプロトコルのバージョン番号を指定します。TLS/SSLを使用する場合は3以上を指定してください。未設定の場合は3が使用されます。このパラメータ値は個別の外部参照設定内で指定することも出来ます。

	デフォルト値: **Version** = 3
Bind = {Yes | No}	LDAPサーバへの接続時にbindを有効にします。LDAPプロトコルがバージョン3以上であればbindは不要です。このパラメータ値は個別の外部参照設定内で指定することも出来ます。 デフォルト値: **Bind** = No
BindDn = {string}	bind用のDN(Distinguished Name)の指定です。このパラメータ値は個別の外部参照設定内で指定することも出来ます。 デフォルト値: **BindDn** =
BindPw = {string}	bind用のDNに対するパスワードの指定です。このパラメータ値は個別の外部参照設定内で指定することも出来ます。 デフォルト値: **BindPw** =
SearchBase = {string}	検索の基準となるDN の指定です(RFC2253)。 デフォルト値: **SearchBase** =
SizeLimit = {integer}	データベースの1リクエストに対して受け取る処理結果の最大数です。パラメータ値が0に設定されている場合、制限はありません。このパラメータ値は個別の外部参照設定内で指定することも出来ます。 デフォルト値: **SizeLimit** = 0
Dereference = {3 |	LDAP エイリアスの実名参照方法の指定です。

2 | 1 | 0}	• 0 – 実名参照しない。 • 1 – 検索で実名参照する。 • 2 – 検索のためのベースオブジェクトを探すときのみ実名参照する。 • 3 – 常に実名参照する。 このパラメータ値は個別の外部参照設定内で指定することも出来ます。 デフォルト値: **Dereference** = 0
ChaseReferrals = {integer}	LDAP_OPT_REFERRALS設定です。このパラメータを設定するにはLDAPプロトコルバージョンが3以上である必要があります。このパラメータ値は個別の外部参照設定内で指定することも出来ます。 デフォルト値: **ChaseReferrals** = 0
SkipDomains = {LookupsLite}	データベースを参照しないドメインリストの指定です。このパラメータによって全体のパフォーマンスが向上し、サーバ負荷が大幅に軽減されます。このパラメータ値は個別の外部参照設定内で指定することも出来ます。 デフォルト値: **SkipDomains** =
CheckPeriod = {time}	不要なLDAPサーバへの接続を切断する為の無通信時間の指定です。LDAPサーバへの接続状況の確認もこの指定時間ごとに実行されます。 デフォルト値: **CheckPeriod** = 2m

[MailBase]セクション

[MailBase]セクションには、**Dr.Web MailD**データベースに関する設定が定義されています。

MaxStoredMessages = {integer}	メールデータベースに保存するメールの最大数の指定です。パラメータ値が0に設定されている場合、制限はありません。データベース内のメール数がこのパラメータ値を上回る場合は、指定された数になるまで古いメールから削除されていきます。送信済みメッセージはすぐに削除され、未送信メールは送信された後で削除されます。 デフォルト値: **MaxStoredMessages** = 100000
MaxStorageSize = {size in bytes}	メールデータベースの最大サイズの指定です(バイト)。パラメータ値が0に設定されている場合、サイズの制限はありません。データベースサイズがこのパラメータで設定された上限を超えた場合、指定されたサイズになるまで古いメッセージから削除されていきます。 デフォルト値: **MaxStorageSize** = 0
MaxPoolSize = {integer}	メールデータベースプールの最大サイズの指定です。パラメータ値が0に設定されている場合、プールサイズは物理メモリの利用可能量に応じて自動的に設定されます。現在のバージョンでは、SIGHUPシグナルでは変更が反映されません。 デフォルト値: **MaxPoolSize** = 0

SendTimeout {time}	=	プラグインがメッセージを非同期に検査する際のタイムアウトを指定します。指定された時間を超えた場合、メッセージ検査において何らかのエラーが発生したとみなされます。そのような場合のアクションは[Maild]セクションの**ProcessingErrors**パラメータで定義されます。 デフォルト値: **SendTimeout** = 30s
FrozenTimeout {time}	=	メッセージの追加処理時間の指定です。**SendTimeout**パラメータで指定された時間内にプラグインがメッセージを処理できなかった場合、**FrozenTimeout**パラメータで指定された時間まで延長することができます。現在のバージョンでは、このパラメータはアンチスパムプラグインでのみ有効で、明示的に指定する必要があります。 デフォルト値: **FrozenTimeout** = 2h
DeleteTimeout {time}	=	メッセージをメールデータベースに保存しておく時間の指定です。このパラメータ値は**FrozenTimeout**パラメータ値よりも大きくなくてはなりません。 デフォルト値: **DeleteTimeout** = 48h
BackupPeriod {time}	=	データベースをバックアップする間隔の指定です。パラメータ値に0を指定した場合、バックアップは行われません。 デフォルト値: **BackupPeriod** = 0

BackupName = {filename}	データベースのバックアップファイル名です。指定されたファイル名が?記号で終わっている場合、バックアップはその都度新しいファイルに保存され、ファイル名の?記号はバックアップ時間の値に置き換えられます。 デフォルト値: **BackupName** = %var_dir/msgs/db/.maildb.backup
MaxBodySizeInDB = {size}	データベースに保存されるメッセージの最大サイズの指定です。このサイズを超えたメッセージは個別の外部ファイルに保存されます。 デフォルト値: **MaxBodySizeInDB** = 1k
SyncMode = {Yes | No}	内部データベースに使用する同期モードの指定です。 yesの場合、各トランザクションごとにfsyncが呼び出されます。その結果、ディスク上に保存されているデータベースは常に最新の状態になりますが、システムパフォーマンスは低下します。 noの場合、データベースの同期にOSのバッファリングが使用されます。その結果、drweb-maildがクラッシュした場合には最後のトランザクションからデータの一部が失われる可能性がありますが、DBは破損せず、システムパフォーマンスは向上します。システムの信頼性のために特に要求されていなければ、このパラメータはnoのままで構いません。 デフォルト値: **SyncMode** = no

[Filters]セクション

[Filters]セクションでは、**Dr.Web MailD**プラグインの一般設定が定義されています。

LibDir = {path to directory}	プラグインを保存するディレクトリの指定です。 デフォルト値: **LibDir** = %bin_dir/maild/plugins/
Settings = {list of plug-in settings}	プラグインのスタートアップ設定です。以下の書式で指定してください。 **Settings** = [plugin_settings], [plugin_settings]... [plugin_settings]は plugin_name: [PARAM1]|...|[PARAMN]で、[PARAMN]は **setting_name** = setting_valueです。 例: **Settings** = vaderetro: **max_size** = 400k|**log_level**=debug, drweb: **max_size** = 10m Vaderetroプラグインに対して、検査するメッセージの最大サイズ400キロバイト、ログの詳細レベルdebugに設定。drwebプラグインに対して、検査するメッセージの最大サイズ10メガバイトに設定。 値は全て、大文字小文字の区別はありません(ファイルへのパス以外)。 デフォルト値: **Settings** =

現在のバージョンでは、プラグインに対して以下のパラメータのみ指定することが出来ます。

section = {text value}	プラグインパラメータを保存する設定ファイル内のセクションの名前です。

max_size = {size}	検査するメッセージの最大サイズの指定です。パラメータ値が0に設定されている場合、制限はありません。デフォルト値はプラグインが置かれているキューに応じて、**MaxSizeBeforeQueueFilters**、**MaxSizeAfterQueueFilters**パラメータ値によって定義されます。このパラメータは plugin_name/**max_size** = valueの形でも指定することが出来ます。 **max_size** を使用したクライアントのルールは以下のようになります。 [Rule:client1] ... plugin_name/**max_size** = {size} [Rules] **md-client**:client1 cont rule=client1 例: [Rule:Client1] **AdminMail** = root@client1.drweb.ru **SenderAddress** = inet:25@10.0.0.0 **ProtectedDomains** = client1.drweb.ru, client1 **ProtectedEmails** = regex:.*@client1.drweb.ru, regex:.*@client1 **ProtectedNetworks** = 10.0.0.0/32 drweb/**max_size** = 100k [Rules] ... **md-client**:client1 cont **rule**=client1

log_level = {Quiet | Error | Alert | Info | Debug}	ログの詳細レベルの指定です。デフォルト値は[Logging]セクションの**Level**パラメータ値と同じです。
log_ipc_level = {Quiet | Error | Alert | Info | Debug}	IPCライブラリのログの詳細レベルの指定です。デフォルト値は[Logging]セクションの**IpcLevel**パラメータ値と同じです。
syslog_facility = {Daemon | Mail | Local0 .. Local7}	syslogのファシリティの指定です。デフォルト値は[Logging]セクションの**SyslogFacility**パラメータ値と同じです。
log_filename = {syslog | path to file}	ログファイルへのパスの指定です。syslogをログファイル名として指定することが出来、その場合ロギングはsyslogdシステムサービスによって実行されます。
path_to_lib = {path to file}	プラグインライブラリへのパスの指定で、絶対パスと相対パスを使用することが出来ます。相対パスで指定された場合、[Filters]セクションの**LibDir**パラメータ値がルートになります。 デフォルト値は次のアルゴリズムによって定義されます:**LibDir**パラメータ値として指定されたパスに"/lib+plug-in name.so"ストリングを加えます。例えば、デフォルト設定を使用してLinux環境でvaderetroプラグインを**Dr.Web MailD**に接続する場合、次のパスを使用します:%bin_dir/maild/plugins/libvaderetro.so **Settings**パラメータ経由で、第三者プラグインを**Dr.Web MailD**に接続することが出来ます。この場合のパラメータ値の指定方法も上記と同様です: **Settings** = NewUserPlugin: **log_level**=info|**max_size**=200k

BeforeQueueFilters = {list of plug-ins}	メッセージがキュー、またはデータベースに置かれる前にそれを処理するプラグインのリストです。 デフォルト値: **BeforeQueueFilters** =
MaxSizeBeforeQueueFilters = {size}	**BeforeQueueFilters**パラメータ値で指定されたプラグインが処理するメッセージの最大サイズの指定です。プラグインに対して**max_size**パラメータ値が明示的に指定されていない場合のみ使用されます。パラメータ値が0に設定されている場合、サイズの制限はありません。 デフォルト値: **MaxSizeBeforeQueueFilters** =
AfterQueueFilters = {list of plug-ins}	メッセージがキュー、またはデータベースに置かれた後にそれを処理するプラグインのリストです。 デフォルト値: **AfterQueueFilters** =
MaxSizeAfterQueueFilters = {size}	**AfterQueueFilters**パラメータ値で指定されたプラグインが処理するメッセージの最大サイズの指定です。プラグインに対して**max_size**パラメータ値が明示的に指定されていない場合のみ使用されます。パラメータ値が0に設定されている場合、サイズの制限はありません。 デフォルト値: **MaxSizeAfterQueueFilters** = 0
PluginsBaseDir = {path to directory}	プラグインの実行時に使用する作業用ディレクトリへのパスの指定です。 デフォルト値: **PluginsBaseDir** = %var_dir/plugins/

[Stat]セクション

[Stat] セクションでは、**Dr.Web MailD**内に集められる統計情報に関する設定が定義されています。

Detail = {value}	以下のログの詳細レベルがあります。 • off – 統計情報の収集を無効にします。これにより、ソフトウェアのパフォーマンスを向上させることが出来ます。統計情報はエクスポートされず、レポートも送信されません。 • low – ソフトウェア全体の動作に関する統計情報の収集を有効にします。統計情報をエクスポートし、レポートを送信することができます。 • medium – 設定内でこの機能が無効になっていないグループに関する統計情報を収集します。グループの統計情報へはコントロールソケットかWebインターフェース経由でアクセスすることが出来ます。 • high – この機能が無効になっていない内部データベース内の一覧に含まれている全てのユーザに関する統計情報を収集します。ユーザ統計情報へはコントロールソケットかWebインターフェース経由でアクセスすることが出来ます。 lowレベルで収集された統計情報はレポートにも含まれます(この機能が有効になっている場合)。 このパラメータは、各クライアントのルール内でそれぞれ個別に指定することが可能です(**StatDetail**という名称になります)。
	デフォルト値: **Detail** = low

Send = {Yes | No}	統計情報サーバ、または**Dr.Web Security Suite**サーバ（**Dr.Web MailD**がアンチウイルスネットワークの一部として動作している場合）へのレポート送信の指定です。 デフォルト値: **Send** = Yes
SendPeriod = {time}	統計情報のサーバへの送信間隔の指定です。 デフォルト値: **SendPeriod** = 10m
Timeout = {time}	統計情報の送信タイムアウトの指定です。 デフォルト値: **Timeout** = 30s

Dr.Web MailDを使用し、storageタイプ経由で統計情報をエクスポートすることが出来ます。

storageタイプ経由での統計情報のエクスポートを有効にする方法は以下のとおりです。

1. [Stat]セクションの**ExportStat**パラメータ値にYesを指定します。
2. [Stat]セクションの、以下のいずれかのパラメータ値に統計情報エクスポートコマンドを指定します。

ExportStat = {Yes | No}	該当するパラメータで定義されたストレージへの統計情報のエクスポートの指定です（下記参照）。 このパラメータの値は全てのクライアントがデフォルトとして使用し、各クライアントに対して個別に指定することが出来ます。 デフォルト値: **ExportStat** = No

ExportBlockObjectsStorage = {query string}	ブロックされたメッセージに関する統計情報の、外部ストレージへの保存方法の指定です。メッセージがブロックされた直後にエクスポートが実行されます。以下は要求に使用する値の一覧です。 • :number<int> – ユニークなメッセージ識別子 • :q_name<varchar_long> – メッセージが保存された隔離ファイルへのパス(隔離内に保存された場合) • :virus_name<varchar_long> – メッセージ内で見つかったブロックされたオブジェクトの名前 • :virus_code<int> – メッセージ内で見つかったブロックされたオブジェクトのコード コードの一覧 ○ 1 – 感染している ○ 2 – ウイルスによる改変 ○ 3 – 感染が疑われる ○ 4 – 修復された ○ 5 – 削除された ○ 6 – フィルタリングされた ○ 7 – スキップされた ○ 8 – アーカイブ制限 ○ 9 – エラー ○ 10 – 読み込みエラー ○ 11 – 書き込みエラー ○ 12 – アドウェア ○ 13 – ダイヤラ- ○ 14 – ジョークプログラム ○ 15 – リスクウェア ○ 16 – ハッキングプログラム

	• : plugin_name<varchar_long> – メッセージをブロックしたプラグインの名前 • :sender<varchar_long> – 山括弧内の送信者のアドレス • :client_ip<varchar_long> – メールデータベースにメッセージをロードしたクライアントのIPアドレス(分かる場合) • :date<timestamp> – メールデータベースへのメッセージのロードのタイムスタンプ • :client_id<varchar_long> – メールデータベースへの保存が実行されるユーザのユニークな識別子 例: ExportBlockObjectsStorage = "odbc:insert into viruses values (:number<int>, :q_name<varchar_long>, :virus_name<varchar_long>, :virus_code<int>, :plugin_name<varchar_long>, :sender<varchar_long>, :client_ip<varchar_long>, :date<timestamp>, :client_id<varchar_long>)" このパラメータの値は全てのクライアントがデフォルトとして使用し、各クライアントに対して個別に指定することが出来ます。
	デフォルト値: **ExportBlockObjectsStorage** =
ExportStatStorage = {query string}	処理したメッセージの数に関する統計情報のエクスポートの指定です。エクスポートは以下のタイミングで実行されます。 • シャットダウン時

	• [Stat]セクションの **SendPeriod**パラメータ値で指定された時間が経過した後 統計情報が空の場合（処理されたメッセージが無い）、何もエクスポートされません。 以下は要求に使用する値の一覧です。 • :size<int> – 検査したメッセージの合計サイズ（バイト） • :num<int> – 検査したメッセージの総数 • :q_num<int> – 隔離に保存されたメッセージの総数 • :r_num<int> – 転送されたメッセージの総数 • :n_num<int> – 通知メッセージの総数 • :pass_num<int> – 検査を通過したメッセージの総数 • :reject_num<int> – 拒否されたメッセージの総数 • :discard_num<int> – 削除されたメッセージの総数 • :tempfail_num<int> – 一時的に拒否されたメッセージの総数 • :date<timestamp> – メールデータベースのタイムスタンプ • :q_size<int> – 隔離に保存されたメッセージの合計サイズ • :r_size<int> – 転送されたメッセージの合計サイズ • :n_size<int> – 通知メッセージの合計サイズ • :pass_size<int> – 検査を通過したメッセージの合計サイズ

	• :reject_size<int> - 拒否されたメッセージの総数 • :discard_size<int> - 削除されたメッセージの合計サイズ • :tempfail_size<int> - 一時的に拒否されたメッセージの合計サイズ • :work_time<int> - プラグインが動作する最大時間(ミリ秒) 例: **ExportStatStorage** = "odbc:insert into g_stat values(:size<int>, :num<int>, :q_num<int>, :r_num<int>, :n_num<int>, :pass_num<int>, :reject_num<int>, :discard_num<int>, :tempfail_num<int>, :date<timestamp>)" デフォルト値: **ExportStatStorage** =
ExportPluginStatStorage = {query string}	[Reports]セクションの**Names**パラメータ値で指定されたプラグイン(パラメータ値が指定されていない場合は動作している全てのプラグイン)に関する統計情報のエクスポートの指定です。エクスポートは以下のタイミングで実行されます。 • シャットダウン時 • SIGHUP シグナル受信時 • 管理者にレポートが送信された時 • レポートがあまり頻繁に送信されない場合は、指定された間隔時間が経過した後 統計情報が空の場合(処理されたメッセージが無い)、何もエクスポートされません。 以下は要求に使用する値の一覧です。

	• **ExportStatStorage** パラメータの場合と同じです • : plugin_name<varchar_long> - 統計情報をエクスポートするプラグインの名前 例: **ExportPluginStatStorage = "** odbc:insert into plugin_stat values(: plugin_name<varchar_long>, : size<int>, :num<int>, : q_num<int>, :r_num<int>, : n_num<int>, :pass_num<int>, : reject_num<int>, : discard_num<int>, : tempfail_num<int>, : date<timestamp>)"
	デフォルト値: **ExportPluginStatStorage** =

エクスポートに使用出来るストレージについての詳細は統計情報のエクスポートの章を参照してください。

[Reports]セクション

[Reports]セクションでは、プラグインの動作に関するレポートの作成および送信についての設定が定義されています。

Send = {Yes | No}	レポートを送信するかどうかの指定です。このパラメータの値は全てのクライアントがデフォルトとして使用し、各クライアントに対して個別に指定することが出来ます(**ReportsSend**という名称になります)。
	デフォルト値: **Send** = Yes

SendTimes = {time}	レポートのスケジュール指定です。 シンタックスは以下のようになります。 • hour:minute:second[-period] - 毎日指定された時間にレポートを送信 • Nw/hour:minute:second[-period] - 毎週N番目の曜日(0 -日曜日、1 -月曜日、2 -火曜日など)の指定された時間にレポートを送信 • Nm/hour:minute:second[-period] - 毎月N番目の日の指定された時間にレポートを送信 期間が指定されていた場合({time}書式)、その期間がレポートの対象となります。特に指定が無い場合は24時間になります。 例: **SendTimes** = 00:00:00-24h, 1w/00:00:00-7d, 2M/21:23:32-31d この場合、日々のレポートは深夜0時に、週次のレポートは毎週月曜日の深夜0時に、月次のレポートは毎月2日の21:23:32にそれぞれ配信されます。 このパラメータの値は全てのクライアントがデフォルトとして使用し、各クライアントに対して個別に指定することが出来ます(**ReportsSendTimes**という名称になります)。 デフォルト値: **SendTimes** = 24h
Mail = {e-mail address}	レポートメールを送信する宛先の指定です。指定されていない場合、[Notifier]セクションの**AdminMail**パラメータ値で指定されたメールアドレスが使用されます。カンマで区切って、複数のパラメータを指定することが出来ます。

	このパラメータの値は全てのクライアントがデフォルトとして使用し、各クライアントに対して個別に指定することが出来ます(**ReportsMail**という名称になります)。 **ReportsMail**パラメータ値が設定されている場合、レポートは**AdminMail**パラメータで指定されているアドレスには送信されませんのでご注意ください。 **Mail** =
Names = {list of plug-ins}	レポートに処理結果を含めるプラグインの一覧です。書式:plug-in_name1, plug-in_name2, ... パラメータ値が設定されていない場合、[Filters]セクションの**BeforeQueueFilter**および**AfterQueueFilter**パラメータ値で指定されたプラグインが対象となります。 このパラメータの値は全てのクライアントがデフォルトとして使用し、各クライアントに対して個別に指定することが出来ます(**ReportsNames**という名称になります)。 **Names** =
TopListSize = {integer}	検出されたオブジェクトとそれらを送信したアドレスの上位件数の指定です。パラメータ値は各リスト上の掲載数を指定します。0を指定した場合はトップリストが作成されず、-1を指定した場合はリストの件数が無制限になります。 このパラメータの値は全てのクライアントがデフォルトとして使用し、各クライアントに対して個別に指定することが出来ます(**ReportsTopListSize**という名称になります)。 **TopListSize** = 20

MaxStoreInDbPeriod = {time}	レポート用データベースに統計情報を保存しておく最大の期間の指定です。0を指定した場合、データは削除されません。 **MaxStoreInDbPeriod** = 31d

CheckForRemovePeriod = {time}	レポート用データベースから古いデータを削除するためのチェック間隔の指定です。 **CheckForRemovePeriod** = 5m

Dr.Web MailD設定ファイルには、プラグインの動作に関するレポートの作成、および**Super-Administrator**への送信についての追加パラメータが含まれています。

GeneralSend = {Yes | No}	Super-Administratorへの一般レポートの送信の指定です。レポート内には全てのクライアントに関する統計情報、および全てのプラグインに関する一般統計情報がデフォルトで表示されています。 一般レポートの設定には全て**General**プレフィックスが付きます。 **GeneralSend** = Yes

GeneralSendTimes = {time}	Super-Administratorへ一般レポートを送信するタイムテーブルの指定です。シンタックスは以下の通りです。 • hour:minute:second[-period] - 毎日指定された時間にレポートを送信 • Nw/hour:minute:second[-period] - 毎週N番目の曜日(0 -日曜日、1 -月曜日、2 -火曜日など)の指定された時間にレポートを送信 • Nm/hour:minute:second[-period] - 毎月N番目の日の指定された時間にレポートを送信 期間が指定されていた場合、その期間がレポートの対象となります。特に指定が無い場合は24時間になります。 デフォルト値: **GeneralSendTimes** = 00:00:00

GeneralClientFilter = {regular expression}	レポートを準備する際のクライアントのフィルタリングに関する指定です。空でないパラメータ値は正規表現です。この値がクライアントの識別子と比べられ、一致した場合、そのクライアントに関する情報はレポートに含まれます。一般統計情報には全てのクライアントに関する情報が含まれます。 **GeneralClientFilter** =
GeneralTotalStat = {Yes | No}	一般レポートに含まれている各プラグインに関する情報の指定です。 **GeneralTotalStat** = Yes
GeneralMail = {e-mail address}	Super-Administratorへのレポート送信に使用するアドレスの指定です。 **GeneralMail** =
GeneralNames = {list of plug-in modules}	Super-Administratorへのレポートに処理結果を含めるプラグインの一覧です。書式:plug-in_name1, plug-in_name2, ... パラメータ値が設定されていない場合、[Filters]セクションの**BeforeQueueFilter**および**AfterQueueFilter**パラメータ値で指定されたプラグインが対象となります。 **GeneralNames** = drweb1, drweb2
GeneralTopListSize = {number}	検出されたオブジェクトの数とSuper-Administratorへのレポート内に表示されるアドレスの指定です。 **GeneralTopListSize** = 20

[Quarantine]セクション

[Quarantine]セクションでは、**Quarantine**が正常に動作するための設定が定義されています。

Path = {path to directory}	隔離ディレクトリへのパスの指定です。 デフォルト値: **Path** = %var_dir/infected/
FilesMode = {numeric value}	隔離処理時のファイルのパーミッションの指定です。この値は**QuarantineFilesMode**パラメータ内で指定することも出来ます。 デフォルト値: **FilesMode** = 0660
FilenamesMode = {Std | Tai | Rand48}	隔離処理時のファイル名書式の指定です。 • Std - mkstemp コマンドを使用して、隔離されたファイルをリネーム %FilenamesPrefix.XXXXXXテンプレートを使用します。 %FilenamesPrefixは**FilenamesPrefix**パラメータ値で指定されたプレフィックスで、 XXXXXXはランダムな文字と数字です。 • Tai - TAI(International Atomic Time／国際原子時)によって、隔離されたファイルをリネーム %sec.%usec.%FilenamesPrefix.XXXXXXテンプレートを使用します。 • Rand48 -lrand48コマンドを使用して、隔離されたファイルをリネーム %FilenamesPrefix.XXXXXXXXテンプレートを使用します。 デフォルト値: **FilenamesMode** = Std

FilenamesPrefix = {text value}	隔離されたファイルのリネームに使用されるプレフィックスの指定です。"%" と "_"をパラメータ値に含むことは出来ません。この値は **QuarantineFilenamesPrefix**パラメータ内でも指定することが出来ます。 デフォルト値: **FilenamesPrefix** = maild
AccessByEmail = {Yes | No}	隔離処理されたメッセージを取得する為の制御メール機能を有効にする。特別なメッセージは**FilterMail**パラメータ値内(またはルール内)で指定された、特別なSubjectヘッダを持つメールアドレスに送信されます。 q:relative_path_to_file relative_path_to_file は、隔離ディレクトリに保存されたファイルへの相対パスです(例: /drweb/drweb.quarantine.puYtWx)。リクエストに対する返信メッセージは、受信者または送信者のうちの1人が制御メール送信者と一致する場合にのみ送信されます。そのような制御メールは、受信したレポート内の該当するリンクをクリックすると、MUAによって自動的に作成されます。 デフォルト値: **AccessByEmail** = Yes
StoredTime = {time}	隔離保存したメールの保存期間の指定です。パラメータ値が0に設定されている場合、期間に制限はありません。 デフォルト値: **StoredTime** = 24h
MaxSize = {size in Kbytes}	隔離内に保存できるメールの最大サイズです。 値が0に設定されている場合、サイズに制限はありません。

	このサイズは各メールのボディのみのサイズで、ディスク上の実際のサイズではありません。 このパラメータは内部データベースのサイズにのみ反映され、DBIストレージには反映されません(もし接続されている場合)。 このパラメータの値は全てのクライアントがデフォルトとして使用し、各クライアントに対して個別に指定することが出来ます。 デフォルト値: **MaxSize** = 0
MaxNumber = {numerical value}	隔離内に保存できるメールの最大数です。 値が0に設定されている場合、数に制限はありません。 このパラメータは内部データベース内のメール数にのみ反映され、DBIストレージには反映されません(もし接続されている場合)。 このパラメータの値は全てのクライアントがデフォルトとして使用し、各クライアントに対して個別に指定することが出来ます。 デフォルト値: **MaxNumber** = 0
MoveToDBI = {Yes | No}	隔離処理したメッセージの、ファイルストレージからDBIストレージへの移動の指定です。この機能にはPerlモジュールのFile::Temp、およびDBIがインストールされている必要があります。 デフォルト値: **MoveToDBI** = No
DBISettings = {string}	DBIストレージ接続パラメータの指定です。 例: "dbi:Pg:dbname=emails_db"

	データベースはSQL-ASCIIキャラクタセットを使用して作成する必要があります。 デフォルト値: **DBISettings** =
DBIUsername = {text value}	DBIストレージに接続するためのユーザ名の指定です。 デフォルト値: **DBIUsername** =
DBIPassword = {text value}	DBIストレージに接続するためのユーザパスワードの指定です。 デフォルト値: **DBIPassword** =
SQLInsertCommand = {string}	DBIストレージにメッセージを追加するコマンドの指定です。エレメントのセット、タイプ、順番は決まっています。 1. number - メッセージの番号 2. string - メッセージが含まれているファイルへの相対パス 書式: client/plug-in/id.prefixー clientはクライアントの識別子、または "def"ワード(どのクライアントにも属していないメッセージがある場合)です。plug-inはプラグインの名前で、idは16進法でのメッセージ番号(出力には8つのキャラクタが使用されます)、prefixは**FilenamesMode**または**FilenamesPrefix**パラメータ値によって定義されたプレフィックスです。 3. timestamp - データベースにメッセージを追加した時間 4. string - エンベロープのFromヘッダ(山括弧内) 5. string -エンベロープの受信者一覧。値は山括弧で囲まれ、カンマで区切られます。

	6. string - メッセージのボディ リクエスト内のエレメントは"?"記号で置き換えます。 例: **SQLInsertCommand** = "INSERT INTO mail_export values (?,?,?,?,?,?)" デフォルト値: **SQLInsertCommand** =
SQLRemoveCommand = {string}	DBIストレージに保存されているメッセージを削除するコマンドの指定です。データベース内のメールの保存期間が指定されている場合に使用します。リクエスト内で指定するパラメータはtimeのみで、この時間よりも古いメッセージは全て削除されます。リクエスト内のエレメントは"?"記号で置き換えます。 例: **SQLRemoveCommand** = "DELETE FROM mail_export WHERE put_time<=?" デフォルト値: **SQLRemoveCommand** =
SQLSelectCommand = {string}	DBIストレージ内のメッセージにアクセスするためのコマンドの指定です(制御文字を使用して隔離からメッセージをリクエストするなど、必要な場合)。リクエスト内で使用されるパラメータは隔離内の相対ファイル名のみです。リクエスト内のエレメントは"?"記号で置き換えます。エレメントのセット、タイプ、順番は決まっています。 1. number - メッセージ番号 2. timestamp - データベースにメッセージを追加した時間 3. string - メッセージのボディ 4. string - エンベロープのFromヘッダ(山括弧内)

	5. string - エンベロープの受信者一覧。値は山括弧で囲まれ、カンマで区切られます。 6. <relative path to file> オブジェクトのあるファイルへの相対パス。詳細については上記**SQLInsertCommand**パラメータの説明を参照してください。 例: **SQLSelectCommand** = "SELECT id, put_time,body,sender,rcpts, filename FROM mail_export WHERE filename LIKE ?" デフォルト値: **SQLSelectCommand** =
PulseTime = {time}	古いメッセージを削除、およびメッセージをファイルストレージからDBIストレージに移動する時間間隔の指定です。パラメータ値が0に設定されている場合、**PathToDrwebQp**パラメータ値内で指定されたプログラムは起動しません。 デフォルト値: **PulseTime** = 5m
PathToDrwebQp = {path to file}	drweb-qpプログラムへのパスの指定です。 デフォルト値: **PathToDrwebQp** = %bin_dir/drweb-qp
MoveAll = {Yes | No}	受信した全てのメッセージを、アーカイブするために直接/Path_parameter_value/def/backup/ディレクトリに移す指定です。パラメータは**MoveToDBI** = yesと一緒に使用する必要があります。そうでない場合、受信するメッセージですぐにディレクトリが一杯になってしまいます。 デフォルト値:

	MoveAll = No

[Maild]セクション

[Maild] セクションでは、**Dr.Web MailD**が正常に動作する為の一般設定が定義されています。

ProtectedNetworks = {lookups}	保護するネットワークのリストを指定します。値はCIDR形式で指定します。 例: **ProtectedNetworks** = 10.0.0.0/24, 127.0.0.0/8, 192.168.0.68 デフォルト値: **ProtectedNetworks** = 127.0.0.0/8
ProtectedDomains = {lookups}	保護するドメインのリストを指定します。 例: **ProtectedDomains** = example.ru, example.com デフォルト値: **ProtectedDomains** =
IncludeSubdomains = {Yes | No}	保護するドメインリスト内のサブドメインも保護対象にする指定です。 デフォルト値: **IncludeSubdomains** = yes
InPoolOptions = {pool settings}	メッセージ受信、内部キュー構成用のスレッドプールの指定です。 デフォルト値: **InPoolOptions** = auto

OutPoolOptions = {pool settings}	メッセージ送信用のスレッドプールの指定です。 デフォルト値: **OutPoolOptions** = auto
RedirectMail = {e-mail address}	Redirectアクションが適用された際にメッセージを転送するアドレスを指定します。 デフォルト値: **RedirectMail** = root@localhost
OnlyTrustedControlMails = {Yes | No}	制御メール(例えば、隔離からメッセージを受け取るために)を、保護されたネットワークからのみ送信する指定です。**Receiver**コンポーネントからクライアントのIPアドレスに関する情報を取得できなかった場合、**Dr.Web for UNIX mail servers**にメッセージを渡す前にMTAが正しいReceivedヘッダを追加するように、**GetIpFromReceivedHeader** = Yesを使用する必要があります。制御メールを機能させるには、クライアントの送信メールトラフィックを**Dr.Web**によって検査する必要があります。 デフォルト値: **OnlyTrustedControlMails** = Yes
MaxScore = {numerical value}	メッセージの最大スコアの指定です。メッセージのスコアがこのパラメータ値を上回っている場合、**MaxScoreAction**パラメータ内で指定されたアクションが適用され、メッセージの検査は中止されます。このパラメータはメッセージがプラグインに渡される前にチェックされ、各プラグインによる検査の後に対応されます。 デフォルト値: **MaxScore** = 10000

MaxScoreAction = {actions}	メッセージのスコアが**MaxScore**パラメータ内で指定された閾値を超えている場合に適用するアクションの指定です。rejectアクションが指定され、 **UseCustomReply**パラメータ値にyesが指定されている場合、SMTPの返信は**ReplyMaxScore**パラメータで指定されたものが使用されます。アクションが全て適用されると、メッセージの検査は完了したと見なされます。 必ず指定しなくてはならない必須アクションはpass、discard、reject、tempfailです。 追加のアクションは quarantine、redirect、add-header、scoreです。 このパラメータでは複数のアクションを指定することが出来ます。 デフォルト値: **MaxScoreAction** = reject
MaxMimeParts = {numerical value}	メッセージ内のMIMEパートの最大数を指定します。値が0に設定されている場合、検査は実行されません。メッセージ内のMIMEパート数がこの閾値を超えた場合、メッセージの処理は中断され、**ProcessingError**パラメータで指定されたアクションが適用されます。 デフォルト値: **MaxMimeParts** = 1000
MaxNestedMimeParts = {numerical value}	メッセージ内にネストされたMIMEパートの最大数を指定します。値が0に設定されている場合、検査は実行されません。メッセージ内のネストされたMIME数がこの閾値を超えた場合、メッセージの処理は中断され、**ProcessingError**パラメータで指定されたアクションが適用されます。 デフォルト値: **MaxNestedMimeParts** = 100

LicenseLimit = {actions}	ライセンス制限が原因で検査されなかったメッセージに適用するアクションの指定です。 必ず指定しなくてはならない必須アクションはpass、discard、reject、tempfailです。 追加のアクションはquarantine、redirect、notify、add-header、scoreです。 このパラメータでは複数のアクションを指定することが出来ます。 デフォルト値: **LicenseLimit** = pass
EmptyFrom = {actions}	エンベロープのFromヘッダがブランクなメッセージに適用するアクションの指定です。メール通知を使用している場合に起こりうる状況で、スパマーもこのヘッダを無視します。 必ず指定しなくてはならない必須アクションはcontinue、discard、rejectです。 追加のアクションはquarantine、redirect、add-header、scoreです。 このパラメータでは複数のアクションを指定することが出来ます。 デフォルト値: **EmptyFrom** = continue
ProcessingErrors = {actions}	検査中にエラーを引き起こすメッセージに適応されるアクションの指定です。 必ず指定しなくてはならない必須アクションはpass、discard、reject、tempfailです。 追加のアクションはquarantine、redirect、notify、add-header、scoreです。 このパラメータでは複数のアクションを指定することが出来ます。

	デフォルト値: **ProcessingErrors** = pass
RulesLogLevel = {Quiet | Error | Alert | Info | Debug}	ルール処理に関するログの詳細レベルを指定します。 デフォルト値: **RulesLogLevel** = Alert
PidFile = {path to file}	drweb-maild 処理の PIDファイルへのパスの指定です。 デフォルト値: **PidFile** = %var_dir/run/drweb-maild.pid

以下のパラメータはブロックされたメールに対してSMTPが返すメッセージを定義します。

Dr.Web for UNIX mail serversのコンポーネントによってメッセージがブロックされると、SMTPはエラーコード 550 5.7.0および特定のテキストメッセージを返します。メッセージのテキストは以下のパラメータ値内で指定することが出来、引用符で囲まれている必要があります。

UseCustomReply = {Yes | No}	SMTPセッション中のカスタムメッセージの使用を有効にする指定です。受信するメッセージが拒否された場合にSMTPが返すメッセージとして送信されます。 デフォルト値: **UseCustomReply** = No
ReplyEmptyFrom = {string}	**EmptyFrom** = rejectが適用され、**UseCustomReply** = Yesの場合に返されるメッセージの指定です。テキストのパートのみ指定することが出来ます:"550 5.7.0 Text"(空白を含むテキストは引用符で囲まれている必要があります) デフォルト値: **ReplyEmptyFrom** = "DrWEB maild:

	Messages from <> are blocked by administrator."
ReplyProcessingError = {string}	**ProcessingError** = rejectが適用され、**UseCustomReply** = Yesの場合に返されるメッセージの指定です。テキストのパートのみ指定することが出来ます："550 5.7.0 Text"（空白を含むテキストは引用符で囲まれている必要があります） デフォルト値： **ReplyProcessingError** = "DrWEB maild: Message is rejected due to software error."
ReplyMaxScore = {string}	**MaxScoreAction** = rejectが適用され、**UseCustomReply** = yesの場合に返されるメッセージの指定です。テキストのパートのみ指定することが出来ます："550 5.7.0 Text"（空白を含むテキストは引用符で囲まれている必要があります） デフォルト値： **ReplyMaxScore** = "Dr.Web MailD: Message is rejected due to score limit exceed."
GetIpFromReceivedHeader = {Yes | No}	**Receiver**コンポーネントからクライアントの IPアドレス情報を取得できなかった場合、Receivedヘッダの値をそのアドレスとして使用する指定です。 デフォルト値： **GetIpFromReceivedHeader** = Yes
Control = {Yes | No}	drweb-maildの対話型インターフェースを有効にします。 デフォルト値： **Control** = No

ControlAddress = {socket address}	drweb-maildの対話型インターフェースが使用するソケットのアドレスの指定です。 デフォルト値: **ControlAddress** = inet:3009@127.0.0.1
ControlPoolOption = {pool settings}	drweb-maild.のコントロールソケットに対するスレッドプールの設定を指定します。 デフォルト値: **ControlPoolOption** = auto
SkipDSNOnBlock = {Yes | No}	RejectまたはTempfailアクションを実行したにも関わらず**Receiver**コンポーネントに戻り値を正常に受け渡せなかった場合にDSNの送信をスキップする指定です。 デフォルト値: **SkipDSNOnBlock** = No

[Receiver]セクション

[Receiver]セクションでは**Receiver**コンポーネントの設定が定義されています。このコンポーネントはEximおよびPostfixメールシステム向け**Dr.Web for UNIX mail servers**、および**Dr.Web for UNIX mail gateways**で使用します。

Address = {socket address}	**Receiver**コンポーネントがメッセージを受け取る際に使用するアドレスの指定です。このパラメータの値としてソケットのアドレスが指定されます(TCPソケットをinet:port@hostname形式で、またはUNIXソケットをlocal:path_to_socket_file形式で)。 デフォルト値: **Address** = inet:25@0.0.0.0
PoolOptions = {pool settings}	スレッドプールの設定を指定します。 デフォルト値:

	PoolOptions = auto
RealClients = {Yes | No}	クライアントまたはMTAからの直接接続の許可を指定します。 デフォルト値: **RealClients** = Yes
ProcessingErrors = {actions}	メッセージ受信中にエラーが発生した際に適用するアクションの指定です。必須アクションはtempfail、discard、rejectで、指定可能なアクションはいずれか1つです。 デフォルト値: **ProcessingErrors** = reject
StalledProcessingInterval = {time}	処理が完了しなかったメッセージの再処理間隔の指定です。プラグインが受信し、**Checker**コンポーネントに送るための処理が時間内に完了しなかったメッセージで、ネットワークまたは電源に問題がある場合に発生する可能性があります。 デフォルト値: **StalledProcessingInterval** = 10m
OneCommandTimeout = {time}	1つのコマンドを実行する際の最大許容時間の指定です。 デフォルト値: **OneCommandTimeout** = 5m
OneMessageTimeout = {time}	1通のメッセージを受信する際の最大許容時間の指定です。 デフォルト値: **OneMessageTimeout** = 10m

AddReceivedHeader = {Yes | No}	受信したメッセージ全てにReceived ヘッダを追加する指定です。 デフォルト値: **AddReceivedHeader** = Yes
ReturnReject = {Yes | No}	Rejectアクションが発生した場合の**Receiver**コンポーネントポリシーの指定です。Yesが指定された場合、5** errorを返します。Noが指定された場合は2** errorを返し、DSNレポートがメッセージの送信者に送付されます。 Exim MTAを使用し、**BeforeQueueFilters**リストにいくつかプラグインがある場合、メッセージが Eximキュー内でフリーズするのを防ぐため**ReturnReject** = Noにすることを推奨します。 デフォルト値: **ReturnReject** = Yes
GreetingString = {string}	新しいクライアントが接続された際にグリーティングメッセージを出力する指定です。"%host%"マクロが [General]セクションの**Hostname**パラメータ値に置き換えられ、"%ver%"マクロがdrweb-receiverモジュールの現在のバージョンに置き換えられます。 デフォルト値: **GreetingString** = "%host% Dr.Web SMTP receiver v%ver% ready"
MaxRecipients = {integer}	最大受信者数の指定です。パラメータ値が0に設定されている場合、受信者数に制限はありません。 接続を開始したIPアドレスがtrustedに設定されている場合、この制限は検査されません。 デフォルト値: **MaxRecipients** = 100

MaxConcurrentConnection = {integer}	1つのIPアドレスからのSMTP接続の最大数を指定します。パラメータ値が0に設定されている場合、制限はありません。 デフォルト値: **MaxConcurrentConnection** = 5
MaxMailsPerSession = {integer}	1セッションごとのメッセージの最大数を指定します。パラメータ値が0に設定されている場合、制限はありません。 デフォルト値: **MaxMailsPerSession** = 20
MaxReceivedHeaders = {integer}	Receivedヘッダの最大数の指定です。パラメータ値が0に設定されている場合、制限はありません。 デフォルト値: **MaxReceivedHeaders** = 100
MaxErrorsPerSession = {integer}	1セッションごとのエラーの許容最大数の指定です。パラメータ値が0に設定されている場合、制限はありません。 デフォルト値: **MaxErrorsPerSession** = 10
MaxMsgSize = {size}	メッセージの最大サイズの指定です。この制限は、接続を開始したIPアドレスがtrustedに設定されている場合でも、常に**Receiver**コンポーネントによって検査されます。 デフォルト値: **MaxMsgSize** = 10m
MaxJunkCommands = {integer}	セッションごとのRSET、NOOP、NTFYコマンドの最大数を指定します。 指定された値を超えた場合、エラーカウンタがアクティブになります。

	エラーカウンタの値は、メッセージがdrweb-maildモジュールによって正常に処理される度に0に設定されます。パラメータ値が0に設定されている場合、この制限は無視されます。 デフォルト値: **MaxJunkCommands** = 100
MaxHELOCommands = {integer}	セッションごとのHELO、EHLO、LHLOコマンドの最大数を指定します。 指定された値を超えた場合、エラーカウンタがアクティブになります。 パラメータ値が0に設定されている場合、この制限は無視されます。 デフォルト値: **MaxHELOCommands** = 20
RelayDomains = {lookups}	メッセージの中継を許可するドメインのリストの指定です。 デフォルト値: **RelayDomains** =

以下のパラメータは、trustedに設定されていない接続IPアドレスをSMTPセッションの様々なステージで検証するアクションを指定します。

デフォルトではlocalhostおよびUNIXソケットからの接続のみがtrustedと見なされます。

接続のIPアドレスに適用される検証アクションは、対応するパラメータ値内でカンマで区切って連続的に指定されます。アクションは指定された順番で適用されます。

SessionRestrictions = {string}	接続が開始されるとすぐに実行される検査

	• trust_protected_network [SCORE] - [SCORE] - 接続IPアドレスが**ProtectedNetworks**パラメータで指定されたリストに含まれている場合、そのアドレスはtrustedになります。SCOREが指定されている場合、その値は現在のセッション内で転送される各メッセージのスコア、および送信者のIPアドレスのスコアに加えられます。 • trust_protected_domains [SCORE] - 接続IPアドレスが**ProtectedDomains**パラメータで指定されたリストに含まれているかどうかの検査で、二重のDNSリクエストを使用して実行されます。受信したホスト名が**ProtectedDomains**リスト内にあるかどうかを検査する為にPTRリクエストが送信されます。リストに含まれていた場合、受信したアドレスのリスト内に接続IPアドレスがあるかどうかを検査するためにAリクエストが送信され、これもあった場合に、アドレスはtrustedなIPアドレスになります。SCOREが指定されている場合、その値は現在のセッション内で転送される各メッセージのスコア、および送信者のIPアドレスのスコアに加えられます。 • trust_white_networks [SCORE] - 接続IPアドレスが**WhiteNetworks**パラメータで指定されたホワイトリストに含まれている場合、そのアドレスはtrustedになります。SCOREが指定されている場合、その値は現在のセッション内で転送される各メッセージのスコア、および送信者のIPアドレスのスコアに加えられます。

	• trust_white_domains [SCORE] - 接続IPアドレスが**WhiteDomains**パラメータで指定されたホワイトリストに含まれているかどうかの検査で、PTRリクエストが送信されます。リスト内にあった場合はtrustedなIPアドレスになります。SCOREが指定されている場合、その値は現在のセッション内で転送される各メッセージのスコア、および送信者のIPアドレスのスコアに加えられます。 • reject_dnsbl [SCORE] - 接続IPアドレスが**DNSBLList**パラメータで指定されたRBL/DNSBLブラックリストに含まれているかどうかの検査で、PTRリクエストが送信されます。リスト内にあった場合、セッションは中断されエラーコードが返されます。SCOREが指定されている場合、その値は現在のセッション内で転送される各メッセージのスコア、および送信者のIPアドレスのスコアに加えられます。 • reject_black_networks [SCORE] - 接続IPアドレスが**BlackNetworks**パラメータで指定されたブラックリストに含まれている場合、セッションが中断されます。SCOREが指定されている場合、エラーがログに出力され、スコアの値は現在のセッション内で転送される各メッセージのスコア、および送信者のIPアドレスのスコアに加えられます。

	• reject_black_domains [SCORE] - 接続IPアドレスが**BlackNetworks**パラメータで指定されたブラックリストに含まれているかどうかの検査で、PTRリクエストが送信されます。リスト内にあった場合、セッションは中断されエラーコードが返されます。SCOREが指定されている場合、エラーがログに出力され、スコアの値は現在のセッション内で転送される各メッセージのスコア、および送信者のIPアドレスのスコアに加えられます。 デフォルト値: **SessionRestrictions** = trust_protected_network, trust_sasl_authenticated
HeloRestrictions = {string}	HELO/EHLO ステージで実行される検査 • reject_unknown_hostname [SCORE] - ホスト名がDNS AレコードおよびDNS MXレコードのどちらも持っていない場合、そのアドレスからのメールはブロックされます。SCOREが指定されている場合、エラーがログに出力され、スコアの値は現在のセッション内で転送される各メッセージのスコア、および送信者のIPアドレスのスコアに加えられます。Aリクエストが送信され、またMXリクエストが送信される場合もあります。 • reject_diff_ip [SCORE] - **Receiver**のIPアドレスが接続を開始したIPアドレスと異なる場合、そのアドレスからのメールはブロックされます。SCOREが指定されている場合、エラーがログに出力され、スコアの値は現在のセッション内で転送される各メッセージのスコア、および送信者のIPアドレスのスコアに加えられます。 デフォルト値:

	HeloRestrictions =
SenderRestrictions = {string}	FROMステージで実行される検査 • reject_unknown_domain [SCORE] – 送信者のホスト名がDNS AレコードおよびDNS MXレコードのどちらも持っていない場合、そのアドレスからのメールはブロックされます。SCOREが指定されている場合、エラーがログに出力され、スコアの値は現在のセッション内で転送される各メッセージのスコア、および送信者のIPアドレスのスコアに加えられます。Aリクエストが送信され、またMXリクエストが送信される場合もあります。 • trust_sasl_authenticated [SCORE] – SASL認証に成功した場合、アドレスはtrustedなIPアドレスになります。SCOREが指定されている場合、その値がメッセージスコアに加えられます。 デフォルト値: **SenderRestrictions** = trust_sasl_authenticated
RecipientRestrictions = {string}	RCPTステージで実行される検査。全ての受信者が順番に検査されます。 • reject_unknown_domain [SCORE] – 送信者のホスト名がDNS AレコードおよびDNS MXレコードのどちらも持っていない場合、そのアドレスからのメールはブロックされます。SCOREが指定されている場合、エラーがログに出力され、スコアの値は現在のセッション内で転送される各メッセージのスコア、および送信者のIPアドレスのスコアに加えられます。Aリクエストが送信され、またMXリクエストが送信される場合もあります。

	• reject_unauth_destination [SCORE] – 送信先のドメインが **RelayDomains**リストおよび **ProtectedDomains**リストのどちらにも含まれていない場合、このアドレスへのメールはブロックされます。SCORE が指定されている場合、エラーがログに出力され、スコアの値がメッセージスコアに加えられます。 • reject_unknown_rcpts [SCORE] – 送信先が **ProtectedEmails**リスト内で指定されているかどうかを検査します。宛先のアドレスがリストに含まれていない場合、このアドレスへのメールはブロックされます。SCOREが指定されている場合、エラーがログに出力され、スコアの値がメッセージスコアに加えられます。**anti_dha** **Reputation IP Filter**と一緒に使用することを推奨します。 デフォルト値: **RecipientRestrictions** = reject_unauth_destination
DataRestrictions = {string}	RCPT ステージで実行される検査。全ての受信者が順番に検査されます。 • reject_spam_trap [SCORE] – スパムトラップの検査です。宛先のアドレスが<USER@HOST>形式を持っている必要があります。**ProtectedDomains**パラメータで指定されたリストにホスト名が含まれていて(リストが空でなければ)、**SpamTrap**パラメータで指定されたリストにユーザ名が含まれている場合、メッセージはブロックされます。SCOREが指定されている場合、エラーがログに出力され、スコアの値がメッセージスコアに加えられます。フルメールアドレスは**SpamTrap**リスト内で指定することも出来ます。

	• reject_multi_recipient_bounce [SCORE] - FROMヘッダが空で複数の宛先をもつメールをブロックします。SCOREが指定されている場合、エラーがログに出力され、スコアの値がメッセージスコアに加えられます。 デフォルト値: **DataRestrictions** =
RestrictionStat = {Yes | No}	制限のある動作に関する統計情報です。統計情報を得るにはdrweb-receiver処理にSIGUSER1シグナルを送信してください。統計情報は[General]セクションの**BaseDir**パラメータ内で指定されたディレクトリにあるrestrictions.txtファイルに保存されています。 デフォルト値: **RestrictionStat** = No
DelayRejectToRcpt = {Yes | No}	RCPTステージまでメールのブロックを行わない指定です。このパラメータを設定すると最新でないメールクライアントと一緒に動作することができ、ブロックされた送信先アドレスのリストをログファイルに出力することが出来ます。 デフォルト値: **DelayRejectToRcpt** = Yes
BlackNetworks = {lookups} **WhiteNetworks** = {lookups}	ネットワークのブラックリストとホワイトリストの指定です。これらのリストはtrust_white_networksおよびreject_black_networksアクションで使用します。詳細については**ProtectedNetworks**パラメータを参照してください。 デフォルト値: **BlackNetworks** = **WhiteNetworks** =

DNSBLList = {lookups}	DNSBLサーバのリストの指定です。このリストはreject_dnsblアクションで使用します。サーバはパラメータ値内で指定された順番で、メッセージがブロックされるまで、またはリストの最後まで検査されます。 デフォルト値: **DNSBLList** =
PositiveDNSBLCacheTimeout = {time}	DNSBLサーバから返ってきた陽性の返答をキャッシュするタイムアウトの指定です。 デフォルト値: **PositiveDNSBLCacheTimeout** = 24h
NegativeDNSBLCacheTimeout = {time}	DNSBLサーバから返ってきた陰性の返答をキャッシュするタイムアウトの指定です。 デフォルト値: **NegativeDNSBLCacheTimeout** = 10m
NegativeDNSCacheTimeout = {time}	DNSサーバから返ってきた陰性の返答をキャッシュするタイムアウトの指定です。パラメータ値はDNSBL以外の全てのDNSの返答に対して有効です。 デフォルト値: **NegativeDNSCacheTimeout** = 10m
BlackDomains = {lookups} **WhiteDomains** = {lookups}	ドメインのブラックリストとホワイトリストの指定です。これらのリストはtrust_white_domainsおよびreject_black_domainsアクションで使用されます。詳細については**ProtectedDomains**パラメータを参照してください。 デフォルト値: **BlackDomains** = **WhiteDomains** =

SpamTrap = {lookups}	スパムトラップアドレスのリストの指定です。このリストはreject_spam_trapアクションで使用されます。 デフォルト値: **SpamTrap** =
ReputationIPFilter = {list of filters}	**Reputation IP filter**によって、接続に関して収集された統計情報に応じてスコアをIPアドレスに割り当てることができ、スコアの合計が閾値を超えていた場合にはそのIPアドレスを一時的にブロックすることが出来ます。 使用可能なフィルタは次のとおりです: **anti_dha**、**errors_filter**、**score_filter** フィルタはカンマで区切って記載され、指定された順番で検査されます。 デフォルト値: **ReputationIPFilter** =
ProtectedEmails = {lookups}	保護するアドレスのリストの指定です。reject_unknown_rcpts制限内で使用されます。 無効な宛先を持つメールを破棄し、DHA攻撃を防ぐことが出来ます(**Reputation IP Filter**内の**anti_dha**フィルタと一緒に使用されている場合)。 このパラメータとreject_unknown_rcpts制限を一緒に指定し、**anti_dha**フィルタと一緒に使用することを推奨します。 デフォルト値: **ProtectedEmails** =
MaxSessionScore = {integer}	各セッションの一般スコアに対する閾値の指定です。このスコアが閾値を超えている場合、該当する接続は一時的なエラーを返して閉じられます。この値が0に設定されている場合、このパラメータは無視されます。

	デフォルト値: **MaxSessionScore** = 10000

制限によって、メッセージが検査の為にdrweb-maildへ渡される前にSMTPセッションのステージでdrweb-receiverモジュール内の望まないメールをフィルタアウトすることが出来ます。リソースの消費を抑えることが出来、スパム検出能力を向上させる高いレベルのスパムフィルタリングが加わります。

制限はSMTPセッションの以下のステージで適用されます。

- 新しいクライアントの接続(**SessionRestrictions**パラメータ)
- HELO/EHLOコマンドの受信(**HeloRestrictions**パラメータ)
- FROMコマンドの受信 - クライアントが新しいメッセージの送信者を指定した場合(**SenderRestrictions**パラメータ)
- RCPTコマンドの受信 - クライアントが現在のメッセージに新しい宛先を追加した時(**RecipientRestrictions**パラメータ)
- DATAコマンドの受信 - クライアントが全ての宛先の転送を完了し、メッセージのボディを送信する準備が出来ている時(**DataRestrictions**パラメータ)

制限は、***Restrictions**パラメータ値としてカンマで区切って設定され、その順番で左から右へ検査されます。制限が検査されるのは、他の検査が全て実行された後になります(コマンドの優先順位、それらのパラメータの有効性など)。

各接続ごとにTrusted IPフラグが検査されます。設定されている場合、制限は検査されません。Trusted IPフラグはUNIXソケットを使用して確立された接続に対しては常に設定され、また、いくつかの制限に対しても設定することが出来ます。

ブロックされたメールの数やその効率を明らかにするために、それぞれの制限に関する統計情報を収集することが出来ます。収集されたデータを取得するには、シグナルの章に記載されている方法でdrweb-receiver処理に特別なシグナルを送ってください。統計情報の収集を有効/無効にするには**RestrictionStat**パラメータを使用してください。

ブロックの効果は、SMTPセッションのどのステージで実行されるかによって異なります。ブロックが**SessionRestrictions**パラメータの制限に応じて実行されている場合、セッション全体がブロックされているようになります。すなわち、ユーザか

らの以降の全コマンドに対してエラーが返されます。その他の全てのステージでのブロックは特定のコマンドにのみ効果があります。

各制限は任意のパラメータースコア値 [SCORE] を取ることが出来ます(スコア値が唯一の必須パラメータである**set_score**および**add_score**制限を除く)。スコアは、制限の種類によって異なる方法で処理されます。

- メッセージの現在のスコアがパラメータ内で指定された値よりも小さい場合に制限が適用されます。
- メッセージの現在のスコアがパラメータ内で指定された値よりも大きい場合に制限が適用されます。
- 制限がアクティブになった場合、該当するパラメータの値がメッセージスコアに加えられます。

制限はSMTPセッションのステージによって、現在のセッション内における各メッセージのスコアと一緒に実行される(**SessionRestrictions**と**HeloRestrictions**ステージ)か、または処理された各メッセージの個別のスコアと一緒に実行されます(その他のステージ)。

制限を検査するほとんど全てのステージで使用できる制限に加え、各ステージごとの特定の制限もあります。前者には以下が適用されます。

- mark_trust [SCORE] - Trusted IP フラグをセットします。このパラメータ以降の制限は全てスキップされます。 SCOREが指定されている場合、現在のメッセージスコアが指定されたスコアよりも小さい場合にのみTrusted IP フラグがセットされます。
- sleep SEC [SCORE] - スリープする時間をSECに秒で指定します。 スパマーの大半は、サーバからの返答をほんの数秒でさえも待たないので、それらをブロックするのに便利です。SCOREが指定されている場合、現在のスコアが指定されたスコアよりも大きいメッセージにのみ制限が適用されます。
- tempfail [SCORE] - SMTPの一時的なエラー(コード4*)を返します。いくつかの検査を通らなかったが、後で通過する可能性のあるクライアントを一時的に拒否する必要がある場合に便利です。SCOREが指定されている場合、現在のスコアが指定されたスコアよりも大きいメッセージにのみエラーが返されます。
- reject [SCORE] - SMTPの恒久的なエラー(コード5*)を返します。クライアントが検査を通らず、また今後も通過できない場合に便利です。SCOREが指定されている場合、現在のスコアが指定されたスコアよりも大きいメッセージにのみエラーが返されます。

- pass_sasl_authenticated [SCORE]- クライアントがSASL認証を通過した場合に、SMTPのこのステージ上での他の検査を全てスキップします。認証はHELO/EHLOコマンドを受け取った後にのみ通過することが出来るので、この制限は**SenderRestrictions**、**RecipientRestrictions**および**DataRestrictions**ステージでのみ便利です。SCOREが指定されている場合、現在のスコアがそのスコアよりも小さいメッセージに対する検査のみスキップされます。スキップされるのは、SMTPセッションのこのステージのみに対して指定された検査だけであるという点にご注意ください(例: pass_sasl_authenticatedの後)。他のステージでの検査はスキップされません。
- set_score SCORE - 現在のメッセージスコアをSCORE値へ変更します。**SessionRestrictions**または**HeloRestrictions**ステージで使用された場合、セッション内の全てのメッセージの値に効果があります。他のステージでは現在処理されているメッセージのスコアに効果があります。
- add_score SCORE - SCORE値を現在のメッセージスコアに加えます。**SessionRestrictions**または**HeloRestrictions**ステージで使用された場合、セッション内の処理された全てのメッセージのスコアに効果があります。他のステージでは現在処理されているメッセージのスコアに効果があります。

例:

SenderRestrictions = trust_protected_networks, reject

- **ProtectedNetworks**内で指定されたIPアドレスからのメールのみ受信を許可します。他のIPアドレスはブロックされます。

SenderRestrictions = trust_protected_networks, trust_protected_domains, sleep 5, add_score 10

- **ProtectedNetworks**内で指定されたIPアドレスからのメール、および**ProtectedDomains**内で指定されたドメインからのメールのみ受信を許可します。その他のメールについては、継続前に5秒停止し、メッセージスコアを10ポイント追加します。

[SASL]セクション

[SASL]セクションでは、**Dr.Web for UNIX mail gateways**(SMTPプロトコ

ルのプロキシサーバとして動作する）内のSASL認証に関する設定が定義されています。

Use = {Yes | No}	SASL認証を有効にする指定です。 デフォルト値: **Use** = No
Driver = {cyrus}	SASL認証ドライバの指定です。現在のバージョンではcyrusドライバのみ使用可能です。インストールし、cyrus-sasl2ライブラリをセットアップしてください。 デフォルト値: **Driver** = cyrus
BrokenAuthClients = {Yes | No}	標準的でないAUTHプロトコルシンタックス使用する、古いSMTPクライアントに対するサポートの指定です。 デフォルト値: **BrokenAuthClients** = Yes
AuthenticatedHeader = {Yes | No}	登録されているユーザの名前をReceivedヘッダに加えます。値がYesに設定されている場合、その名前は全ての人に対して表示されます。 デフォルト値: **AuthenticatedHeader** = No

[Cyrus-SASL]セクション

[Cyrus-SASL] セクションでは、cyrus-saslドライバが正常に動作する為の設定が定義されています。

Lib = {path to file}	cyrus-sasl2 ライブラリへの絶対パスの指定です。 デフォルト値:

	Lib = /usr/lib/libsasl2.so.2
Path = {string}	設定ファイルの名前(.conf拡張子が自動的に付きます)の指定です。cyrus-sasl2ライブラリはこのファイルからその設定を受け取ります。 デフォルト値: **Path** = maild
ServerHostname = {string}	ホスト名の指定です。パラメータ値が設定されていない場合、[General]セクションの**Hostname**パラメータ値が使用されます。**Hostname**値も指定されていない場合はgethostnameメソッドから返された値が使用されます。 デフォルト値: **ServerHostname** =
ServerRealm = {string}	サーバが所属するSASLレルムの指定です。 デフォルト値: **ServerRealm** =
SecurityOptions = {string}	セキュリティ設定のリストです。カンマで区切られます。 以下のセキュリティ設定が可能です。 • noplaintext - 単純な受動的攻撃(例:PLAIN、LOGIN)を受けやすい機構を禁止します。 • noactive - 認証交換の際の、能動的攻撃(辞書攻撃以外)からの保護の指定です。 • nodictionary - 受動的な辞書攻撃を受けやすい認証機構を禁止します。 • noanonymous - 匿名のログインに対する認証機構を禁止します。

	• mutual_auth - 相互認証の要求の指定です。 デフォルト値: **SecurityOptions** = noanonymous

[Sender]セクション

[Sender]セクションでは、**Sender**コンポーネント(メッセージを送信する)の設定が定義されています。このセクションはCommunigate Proメールトランスファーシステムとの動作向け**Dr.Web**ソフトウェアディストリビューションには含まれていません。

UseSecureHash = {Yes | No}	送信するメッセージ全てに**SecureHash**ヘッダを加えます。**UseSecureHash**および**SecureHash**パラメータは、CourierとEximメールトランスファーシステム向けのソリューション、および**Dr.Web for UNIX mail gateways**では使用されません。 SendmailおよびQmaiMTA向け**Dr.Web for UNIX mail servers**では、メッセージの送信と受信に同じMTAを使う場合、**UseSecureHash**パラメータにYesを指定する必要があります。それにより、メッセージループを回避し、システムオペレーションを最適化することが出来ます。 メッセージの送信と受信に異なるMTAを使う場合は、**SecureHash**ヘッダがシステム上限値を超えないようにNoを指定する必要があります。 デフォルト値: **UseSecureHash** = Yes

	Zmailer MTA向け**Dr.Web for UNIX mail servers**では、ルーティング段階でdrweb-zmailerを使用する場合(process.cfから起動される場合)のみ、Yesを指定する必要があります。この場合、drweb-senderによって作成されたメッセージは全てdrweb-zmailerによって処理されます。メッセージループおよび二重チェックの可能性を避けるため、**SecureHash**ヘッダが追加されます。 デフォルト値: **UseSecureHash** = No
	Postfix MTA向け**Dr.Web for UNIX mail servers**では、Posxfixとの対話が milterプロトコル経由で実行される場合のみ(drweb-milterモジュールを使用)、Yesを指定する必要があります。この場合、drweb-senderによって作成されたメッセージは全てdrweb-milterによって処理されます。メッセージループおよび二重チェックの可能性を避けるため、**SecureHash**ヘッダが追加されます。 デフォルト値: **UseSecureHash** = No
SecureHash = {string}	**SecureHash**ヘッダの内容の指定です。このパラメータ値には任意の記号のストリング(記号は10個以上)を使用することが出来ます。セキュリティ強化の為に、パラメータのデフォルト値は変更しておくことを強く推奨します。 Zmailer MTA向け**Dr.Web for UNIX mail servers**では、このパラメータ値はZmailerがルーティング段階で使用されている場合にdrweb-zmailerのスタートアップに使用する--hashパラメータ値と同じである必要があります。
	デフォルト値: **SecureHash** = !!!---------___EDIT_THIS___!!!

StalledProcessingInterval = {time}	プラグインが受信したものの、時間内に**Checker**コンポーネントへの送信が完了しなかったメッセージの再処理間隔の指定です。このような状況はネットワークか電源に問題が発生した場合に起こる可能性があります。 デフォルト値: **StalledProcessingInterval** = 10m
SendingIntervals = {time}	メッセージの送信処理の間隔を指定します。 デフォルト値: **SendingIntervals** = 0s, 30s, 60s, 10m, 30m, 2h, 8h, 1d, 1d
Method = {SMTP | LMTP | PIPE}	**Sender**コンポーネントがメッセージを送信する方法の指定です。 • SMTP - SMTPプロトコル経由でメッセージを送信 • LMTP - LMTPプロトコル経由でメッセージを送信 • PIPE - PIPE経由で外部メールプログラムへメッセージを送信 デフォルト値: **Method** =
MailerName = {SMTP | Sendmail | Postfix | CommuniGate | Qmail | Exim | Zmailer | Courier}	**Dr.Web for UNIX mail servers**と一緒に動作するMTAの指定で、**Method** = pipeの場合に使用します。現在のバージョンでは、SIGHUPシグナルでは変更が反映されません。 デフォルト値: このパラメータのデフォルト値は、使用するMTAによって異なります。

Address = {address}	**Sender**コンポーネントがメッセージを送信する際に使用するアドレスの指定です。**Method** = pipeの場合、メッセージの受信に使用するMTAへのフルパスを指定する必要があります。指定しなかった場合は、メッセージの送信に使用するソケットのアドレスがこのパラメータの値として指定されます。**Dr.Web for UNIX mail gateways**では標準タイプのアドレスに加え、mx:HOSTNAMEタイプも使用することが出来ます(HOSTNAMEはホスト名です)。このタイプを使用した場合、ホスト名を使用するMXレコードを全て受信し、それらに応じてメッセージを送信します。 デフォルト値: このパラメータのデフォルト値は、使用するMTAによって異なります。
Options = {string}	**Method** = pipeの場合に起動される外部メールプログラムのオプションを指定します。 デフォルト値: **Options** =
InPoolOptions = {pool settings}	メッセージ受信、内部キュー構成用のスレッドプールのオプションを指定します。 デフォルト値: **InPoolOptions** = auto
OutPoolOptions = {pool settings}	メッセージ送信用のスレッドプールのオプションを指定します。 デフォルト値: **OutPoolOptions** = auto

以下のパラメータはEximおよびPostfix MTA向けソリューション、**Dr.Web for UNIX mail gateways**でのみ指定されます。

HeloCmdTimeout = {time}	HELO/EHLOコマンド実行のタイムアウト時間の指定です。

	デフォルト値: **HeloCmdTimeout** = 5m
MailFromCmdTimeout = {time}	MAILコマンド実行のタイムアウト時間の指定です。 デフォルト値: **MailFromCmdTimeout** = 5m
RcptToCmdTimeout = {time}	RCPTコマンド実行のタイムアウト時間の指定です。 デフォルト値: **RcptToCmdTimeout** = 5m
DataCmdTimeout = {time}	DATA/BDATコマンド実行のタイムアウト時間の指定です。 デフォルト値: **DataCmdTimeout** = 2m
DataBlockTimeout = {time}	メッセージ送信のタイムアウト時間の指定です。 デフォルト値: **DataBlockTimeout** = 3m
EndOfDataTimeout = {time}	SMTP/LMTP経由でメッセージを送信する際のデータ終了コマンド(.)のタイムアウト時間の指定です。 デフォルト値: **EndOfDataTimeout** = 10m
OtherCmdsTimeout = {time}	SMTP/LMTP経由でメッセージを送信する際の上記以外のコマンドのタイムアウト時間を指定します。 デフォルト値: **OtherCmdsTimeout** = 2m

PipeTimeout = {time}	PIPEを使用して返答を受け取る際のタイムアウト時間の指定です。 デフォルト値: **PipeTimeout** = 2m
SendDSN = {Yes | No}	DSN レポート送信の指定です。 デフォルト値: **SendDSN** = No
Router = {string}	送信先に応じたメッセージのルーティングルールを指定します。異なる送信先へのメッセージを別々のメールアドレスから送信することが出来ます。送信先を複数持つメッセージを異なるメールアドレスから送信しなければならない場合、宛先のリストはグループ分けされている必要があります(各グループが個々のメールアドレスからメッセージのコピーを受け取れるように)。 パラメータ値はDOMAIN ADDRESSの書式で指定します。 • DOMAIN は送信先のエンベロープをチェックするストリングです。エンベロープは<user@host>書式です。検索では大文字小文字を区別しません。 例えば"@localhost"ストリングを検索した場合、<test@localhost>と <yy@localhost.localdomain> エンベロープがマッチし、<@localhost>ストリングを検索した場合は<test@localhost>エンベロープのみがマッチします。

	• ADDRESS は、エンベロープ内にDOMAINストリングがある場合のメッセージ送信先のアドレスです。ADDRESSの書式はこの設定ファイル内の**Address**パラメータの書式と同じです。 "|"記号で区切って複数のアドレスを指定することが出来、その場合メッセージは最初に接続可能となったアドレスに送られます。 例: **Router** = @main.server.com> mx:main.server.com| inet:25@backup.server.com この場合、main.server.comドメインからの受信者宛メッセージは、main.server.comのMXレコード内で示されたアドレスに送信されます。送信に失敗した場合、システムはポート25上の backup.server.comへメッセージの送信を試みます。
	デフォルト値: **Router** =

[Milter]セクション

[Milter]セクションでは、drweb-milterモジュールの動作を管理する設定が定義されています。drweb-milterモジュールは、milterプロトコル経由での**Dr.Web for UNIX mail servers**とPostfixおよびSendmail MTA間の連携に使用します。このセクションはPostfixおよびSendmailメールトランスファーシステムとの動作向けパッケージの**Dr.Web MailD**設定ファイルに含まれています。

Address = {socket address}	milterプロトコル経由で接続を確立する為のソケットアドレスを指定します。メールシステムの設定内(Sendmail MTAのsendmail.cf設定ファイル内、Postfix MTAのmain.cf設定ファイル内)で指定した定義に従う必要があります。このパラメータ値には PIDファイルへのパスは使用できません。

	例: **Address** = local:%var_dir/ipc/drweb-milter.skt デフォルト値: **Address** = inet:3001@127.0.0.1
Timeout = {time}	drweb-milterがSendmailまたはPostfix MTAに接続するタイムアウト時間の指定です。メールシステムの設定ファイル内のどの**Timeout**パラメータ値よりも大きい値を指定してください。 デフォルト値: **Timeout** = 2h
PendedConnections = {numeric value}	接続保留キューの長さの指定です(drweb-milterはMTAがメッセージを処理するのを待ちます)。 デフォルト値: **PendedConnections** = 64
CanChangeBody = {Yes | No}	MTAがメッセージ本文の変更機能をサポートしているかどうかの指定です。バージョン2.4以降のPostfix MTAはこの機能をサポートしています。現在のバージョンでは、SIGHUPシグナルでは変更が反映されません。 デフォルト値: **CanChangeBody** = Yes
ProcessingTimeout = {time}	drweb-milterモジュールのメッセージ検査のタイムアウト時間を指定します。[MailBase]セクションの**SendTimeout**パラメータ値よりも大きい値を設定することを強く推奨します。 デフォルト値: **ProcessingTimeout** = 40s

ProcessingErrors = {actions}	メッセージ検査中にエラーが発生した際の処理を指定します。tempfail、discard、pass、 rejectのアクションのうち、いずれか1つを指定してください。 デフォルト値: **ProcessingErrors** = reject
MinPersistConnection = {numeric value}	drweb-milterモジュールとの最小接続数の指定です。 デフォルト値: **MinPersistConnection** = 2
UseStat = {Yes | No}	drweb-milterモジュールとの接続に関する統計情報の指定です。統計情報は、drweb-milterモジュールがSIGUSR1を受信するとファイルに出力されます。 デフォルト値: **UseStat** = No
MaxFreetime = {time}	drweb-milterモジュールとの全ての接続を閉じるまでのタイムアウト時間を指定します。 デフォルト値: **MaxFreetime** = 2m
ReplyPoolOptions = {pool settings}	drweb-milterモジュールからの応答を処理するためのスレッドプールのオプションを指定します。 デフォルト値: **ReplyPoolOptions** = auto

[CgpReceiver]セクション

[CgpReceiver]セクションでは、**Receiver**コンポーネントとCommuniGate Proメールトランスファーシステム間の連携を可能にする設定が定義されています。このセクションは上記MTAとの動作向けパッケージの**Dr.Web MailD**設定ファイルに含まれています。

ProcessingTimeout = {time}	**Receiver**コンポーネントのメール検査のタイムアウト時間を指定します。[MailBase]セクションの**SendTimeout**パラメータ値よりも大きい値を指定することを強く推奨します。 デフォルト値: **ProcessingTimeout** = 40s
PoolOptions = {pool settings}	スレッドプールの設定を指定します。 デフォルト値: **PoolOptions** = auto
ProcessingErrors = {actions}	メッセージ検査中にエラーが発生した際の処理を指定します。tempfail、discard、pass、 rejectのアクションのうち、いずれか1つを指定してください。 デフォルト値: **ProcessingErrors** = reject
ChownToUser = {string}	CommuniGate Pro MTAから受け取ったメッセージファイルに対する所有者を指定します。drweb-cgp-receiverモジュールは管理者権限(root)で実行されているので、このパラメータ値を空のままにして**Dr.Web for UNIX mail servers** システム全体を管理者権限で起動するか、または**Dr.Web for UNIX mail servers**の実行に使用した特定のユーザ名をこのパラメータ値として設定することが出来ます(デフォルトではdrweb)。 デフォルト値: **ChownToUser** = drweb

[CgpSender]セクション

[CgpSender]セクションでは、**Sender**コンポーネントとCommuniGate Proメールトランスファーシステム間の連携を可能にするための設定が定義されています。このセクションは上記MTAとの動作向けパッケージの**Dr.Web MailD**設定ファイルに含まれています。

UseSecureHash = {Yes | No}	送信するメッセージ全てに**SecureHash**ヘッダを追加する指定です。Noが指定されている場合、drweb-cgp-receiverモジュールはPIPEを使用して送信されたメッセージは検査しません。Yesが指定されている場合、**SecureHash**ヘッダを持ったメッセージは検査せずに通過させます。メッセージの送信と受信に異なるMTAを使う場合は、**SecureHash**ヘッダがシステム上限値を超えないようにNoを指定する必要があります。 デフォルト値: **UseSecureHash** = No
SecureHash = {string}	**SecureHash**ヘッダの内容の指定です。このパラメータ値には任意の記号のストリング(記号は10個以上)を使用することが出来ます。セキュリティ強化の為に、パラメータのデフォルト値は変更しておくことを強く推奨します。 デフォルト値: **SecureHash** = !!!---------___EDIT_THIS___!!!
PoolOptions = {pool settings}	スレッドプールの設定を指定します。 デフォルト値: **PoolOptions** = auto
SubmitDir = {path to directory}	CommuniGate Pro MTAが送信するためのッセージをdrweb-cgp-senderモジュールが配置するディレクトリの指定です。 デフォルト値: **SubmitDir** = /var/CommuniGate/Submitted
SubmitFilesMode = {permissions}	作成された通知、または修復されたメッセージに対するパーミッションの指定です。 デフォルト値:

	SubmitFilesMode = 0600
SubmitFilenamesPrefix = {string}	配置されたメッセージのファイル名に対するプレフィックスの指定です。ファイル名の書式は以下の通りです。 %{SubmitDir}/%{SubmitFilenamesPrefix}XXXXXX CommuniGate Pro MTAによって、またはファイル名に基づいてメッセージに与えられたメッセージ識別子と置き換えられる "%s"マクロを使用することが出来ます。このマクロを使用することによってログファイルの解析を簡易化することが出来ます。 デフォルト値: **SubmitFilenamesPrefix** = drweb_submit_%s_
SubmitFilenamesMode = {std | tai | rand48}	配置されたメッセージのファイル名に対する命名規則の指定です。 • Std - mkstempコマンドを使用してファイルをリネーム drweb_submit_XXXXXX テンプレートを使用します。 • Tai - TAI(国際原子時)によってファイルをリネーム %sec.%usec.drweb_submit_XXXXXX テンプレートを使用します。 • Rand48 -lrand48コマンドを使用してファイルをリネーム drweb_submit_XXXXXXXX テンプレートを使用します。 デフォルト値: **SubmitFilenamesMode** = std

[Courier]セクション

[Courier]セクションでは、**Dr.Web MailD**とCourierメールトランスファーシステム間の連携を可能にする為の設定が定義されています。このセクションは上記MTAとの動作向けパッケージの**Dr.Web MailD**設定ファイルに含まれています。

ProcessingTimeout = {time}	drweb-courier モジュールがメッセージ検査を待つ最大処理時間の指定です。[MailBase]セクションの **SendTimeout**パラメータ値よりも大きい値を設定してください。 デフォルト値: **ProcessingTimeout** = 40s
ProcessingErrors = {actions}	メッセージ検査中にエラーが発生した際の処理を指定します。tempfail、discard、pass、rejectのアクションのうち、いずれか1つを指定してください。 デフォルト値: **ProcessingErrors** = reject
MainPoolOptions = {pool settings}	メッセージ処理用スレッドプールのオプションの指定です。 デフォルト値: **MainPoolOptions** = auto
ReplyPoolOptions = {pool settings}	drweb-maild モジュールからの応答を処理するスレッドプールのオプションの指定です。 デフォルト値: **ReplyPoolOptions** = auto
BaseDir = {path to directory}	Courier MTAのインストールディレクトリの指定です。 デフォルト値: **BaseDir** = /usr/lib/courier

SocketDirs = {path to directory}	Courier MTAとの通信に使用するUNIXソケットを作成するディレクトリのリストを指定します。UNIXソケットはリスト上の最初のディレクトリ内に作成されます。その他のディレクトリをチェックしてdrweb-courierモジュールと同じ名前のUNIXソケットを検索し、見つかった場合はそのソケットを削除します。現在のバージョンでは、SIGHUPシグナルでは変更が反映されません。 デフォルト値: **SocketDirs** = /usr/lib/courier/var/allfilters, /usr/lib/courier/var/filters
SocketAccess = {permissions}	**Dr.Web MailD** とCourier MTAの連携に使用するUNIXソケットに対するパーミッションの指定です。現在のバージョンでは、SIGHUPシグナルでは変更が反映されません。 デフォルト値: **SocketAccess** = 0660

[Qmail]セクション

[Qmail]セクションでは、**Dr.Web MailD**とQmailメールトランスファーシステム間の連携を可能にする設定が定義されています。このセクションは上記MTAとの動作向けパッケージの**Dr.Web MailD**設定ファイルに含まれています。

ProcessingTimeout = {time}	drweb-qmail モジュールがメッセージ検査を待つ最大処理時間の指定です。[MailBase]セクションの **SendTimeout**パラメータ値よりも大きい値を設定してください。 デフォルト値: **ProcessingTimeout** = 40s
ReadingTimeout = {time}	qmail-queue モジュールからエンベロープ、およびメッセージ本文を受け取る最大処理時間の指定です。 デフォルト値:

	ReadingTimeout = 20m
ProcessingErrors = {actions}	メッセージ検査中にエラーが発生した際の処理を指定します。tempfail、discard、pass、rejectのアクションのうち、いずれか1つを指定してください。 デフォルト値: **ProcessingErrors** = reject
MainPoolOptions = {pool settings}	メッセージ処理用スレッドプールのオプションの指定です。 デフォルト値: **MainPoolOptions** = auto
ReplyPoolOptions = {pool settings}	drweb-maild モジュールからの応答を処理するスレッドプールのオプションの指定です。 デフォルト値: **ReplyPoolOptions** = auto
ListenUnixSockets = {socket address}	drweb-qmailモジュールがqmail-queueモジュールからの検査要求を待ち受けるUNIXソケットのリストを指定します。このリスト内のソケットはqmail-queueモジュールによってモニターされるファイルのリストにも含まれている必要があります。qmail-queue --helpコマンドを使用してリストを見ることが出来ます。 デフォルト値: **ListenUnixSockets** = local:%var_dir/ipc/.qmail
QmailQueue = {path to file}	qmail標準のqmail-queueの指定です。 デフォルト値: **QmailQueue** = /var/qmail/bin/qmail-queue.original

[Notifier]セクション

[Notifier]セクションでは、drweb-notifierモジュールに関する設定が定義されています。drweb-notifierはDr.Web for UNIX mail serversのコンポーネント動作に関するレポートを作成、送信します。

PoolOptions = {pool settings}	スレッドプールのオプションを指定します。 初めに、プール内のスレッド数を指定します。 • auto – プール内のスレッド数は、システム負荷に応じて自動的に検出されます。 • N – 負でない整数です。プール内にある少なくともN個のスレッドがアクティブになり、要求に応じて新しいスレッドが作成されます。 • N-M – 正の整数で、M ≥ Nです。プール内にある少なくともN個のスレッドがアクティブになり、要求に応じて M 個までの新しいスレッドが作成されます。 以下の追加パラメータを指定できます。 • **timeout** = {time} – 指定された時間内にスレッドがアクティブにならなかった場合に、そのスレッドを閉じます。このパラメータは先頭のN個のスレッドには適用されず、それらは永久にリクエストを待ち続けます。デフォルト値: 2m • **stat** = {yes|no} – プール内にあるスレッドの統計情報に関する指定です。SIGUSR1シグナルを受信する度に[General]セクションの**BaseDir**パラメータ値で指定されたディレクトリに保存されます。デフォルト値: no • **log_level** = {Quiet|Error|Alert|Info|Debug} – プール内にあるスレッドのログの詳細レベルを指定します。値が明示的に指定されていない場合、[Logging]セクションの**LogLevel**パラメータ値が使用されます。

	• **stop_timeout** = {time} - 実行中のスレッドが停止するまでの最大時間の指定です(プログラムが動作を終了した時やプール内のスレッド数を減らす必要があるときなど)。 デフォルト値: **PoolOptions** = auto
TemplatesBaseDir = {path to directory}	レポートテンプレートファイルの保存ディレクトリを指定します。 デフォルト値: **TemplatesBaseDir** = %etc_dir/maild/templates
LngBaseDir = {path to directory}	レポート言語リソースファイルの保存ディレクトリの指定です。言語ファイルは.lng拡張子を持っています。ターゲット言語(ロシア語にru、英語にenなど)は、言語ファイル内で最初にアンコメントされたラインで指定します。指定された値はレポート作成に使用する言語を定義する為に**NotifyLangs**パラメータ内で使用されます。 デフォルト値: **LngBaseDir** = %etc_dir/maild/lng
AdminMail = {e-mail address}	システム管理者のメールアドレスの指定です。複数のアドレスを指定することが出来ます。その場合、作成されたレポートはそれらのアドレス全てに送信され、メッセージ本文には指定された全てのアドレスが含まれます。このパラメータを指定しない場合はレポートが送信されないので、指定することを推奨します。 デフォルト値: **AdminMail** = root@localhost
FilterMail = {e-mail address}	レポートを含んだメッセージのFromヘッダ内で指定されるメールアドレスの指定です。

	デフォルト値: **FilterMail** = root@localhost
NotifyLangs = {string}	レポート作成のプロセスで使用する言語の指定です。 デフォルト値: **NotifyLangs** = en
TemplatesParserLogLevel = {quiet | error | alert | info | debug}	レポートを作成するサブシステムの、テンプレート処理に関するログの詳細レベルを指定します。 デフォルト値: **TemplatesParserLogLevel** = info
RulesLogLevel = {quiet | error | alert | info | debug}	ルール処理に関するログの詳細レベルの指定です。 デフォルト値: **RulesLogLevel** = info
MsgIdMap = {string}	**Receiver**コンポーネントと**Sender**コンポーネントを対応付けるためのメッセージ識別子のマッピングを指定します。指定されていない場合、デフォルトの**Sender**コンポーネンによって処理されます(識別子の無い)。 例: MsgIdMap = id[12] sender_notifications この場合、id1またはid2識別子を持つ**Receiver**コンポーネントによって作成されたレポートメッセージはsender_notifications識別子を持つ**Sender**コンポーネンによって処理されます。 デフォルト値: **MsgIdMap** =

QuarantinePrefix = {string}	隔離領域に保存されたファイルパスの出力に加えるプレフィックスの指定です。このパラメータによって、オフサイトのサーバを使用して隔離内のファイルにアクセスすることが出来ます。 例えば、**Dr.Web for UNIX mail servers**が動作している同じホスト上にHTTPサーバをインストールし**QuarantinePrefix** = http://mailhost/quarantine/を使用してセットアップした場合、レポート内のリンクは http://mailhost/quarantine/headersfilter/drweb.quarantine.2kqtvIなどのようになります。 デフォルト値: **QuarantinePrefix** =

Dr.Web MailDがメッセージを処理する際に、どのプラグインもあらゆるイベント(ウイルスの検出、プロセスエラー、メッセージのブロックなど)に関する通知レポートの送信を要請することができます。それらのレポートは**Dr.Web Notifier**(drweb-notifierモジュール)によって作成され、**Sender**コンポーネント経由で送信されます。

レポートは全て.msg拡張子を持ったテンプレートファイルとして提出されます。**Dr.Web Notifier**は、**TemplatesBaseDir**パラメータ内で指定されたパスが示すディレクトリ内を検索してそのレポートを探します。テンプレートはマクロ、条件、サイクリックパス、及び外部ファイルの埋め込み(これらのファイルのシンタックスはnotify.*ファイル内に記述されています)をサポートしているので、簡単に変更することができます。

以下の3つのタイプのレポートを使用することが出来ます。

- 特定のメッセージに関する情報を持ったレポート
- **Dr.Web MailD**ソフトウェアの一般的な動作に関する情報を持った定期的なレポート
- メッセージ送受信の失敗に関するDSNレポート

全てのケースにおいて、コンポーネントがdrweb-notifierモジュールにレポートの名前を送信します。DSNテンプレート以外の全てのテンプレートはhtmlおよびプレーンテキスト形式です。ルールの該当するセクションでの html設定に応じて、適切な形式が選択されます。

1つ目のタイプのレポートの場合、以下の各宛先にレポートを送信する必要があるかどうか、ルールを使用して**Dr.Web Notifier**がチェックします（詳細については[Rules] セクションをご覧ください）。

- 送信者へ
- 受信者へ（それぞれの受信者に対するレポートの設定が異なる場合、全ての受信者が正しい形式で確実にレポートを受け取るように更にレポートを送信します）
- 管理者へ

レポートの名前は.msg拡張子を持った外部モジュールの名前に sender_、rcpts、およびadmin_プレフィックスを加えて作成します。そのようなファイルが見つからない場合、エラーがレポートされます。

2つ目のタイプのレポートの場合、**Dr.Web Notifier**はソフトウェアの動作に関する一般的統計のレポート1つのみを管理者に送信します。このレポートのテンプレートは report.msgファイル内にあります。

3つ目のタイプのレポートは、配信失敗に関するDSNレポートです。このレポートのテンプレートはdsn.msgファイル内にあります。

Dr.Web Notifierは、次の正規表現に従ったテンプレートを持つ全てのファイルをアップロードします： (admin|rcpts|sender|report|dsn)_?(.*?)\.msg.

テンプレートファイルを変更する事も可能です。**NotificationNamesMap**パラメータによって、**Dr.Web Notifier**に転送されたレポートの名前を新しい名前（これを使用して新しいテンプレートファイルの名前が作成されます）にマップすることが出来ます。マッピングは**Dr.Web Notifier**に知られている名前に対してのみ実行されます。そうでない場合、必要なファイルを見つけることが出来なくなるからです。

[ProxyClient]セクション

[ProxyClient]セクションではdrweb-proxy-clientモジュールに関する設定が定義されています。

ProxyServersAddresses = {list of	drweb-proxy-server コンポーネントが使用するソケットアドレスのリストを指定します。

sockets}	アドレスは次のように指定します: ADDRESS1 [WEIGHT1], ADDRESS2 [WEIGHT2] .. ADDRESSは基本的なアドレスタイプです。WEIGHTは0から100までのオプションの数値で、このアドレスの「重さ」を定義します。このWEIGHTはネットワーク内の1つのホスト上での相対負荷を定義します。値が大きいほどサーバ上の負荷は大きくなります。 drweb-proxy-clientと同じホスト上で動作している**Receiver**コンポーネントから受け取ったメールは、これらのソケットを使用して該当するソフトウェアに渡され、スキャンされます。これらのアドレスの中には少なくとも1つ有効なサーバアドレスが含まれている必要があります。アドレスはUsing Proxyに記載されたアルゴリズムに応じて使用されます。 デフォルト値: **ProxyServersAddresses** = inet:8088@SERVER-IP
Address = {list of sockets}	drweb-proxy-serverコンポーネントからメール送信のリクエストを受け取る為に **Sender**コンポーネントが使用するソケットアドレスのリストを指定します。 drweb-proxy-server コンポーネントはProxyServer] セクションの**ProxyClientsAddresses**パラメータに設定された値に応じて、これらのアドレスにメールを送信します。 デフォルト値: **Address** = inet:8066@0.0.0.0
MailPoolOptions = {pool settings}	**Receiver**コンポーネントからのリクエストを処理するスレッドプールの設定を指定します。

	スレッドプールは**Receiver**コンポーネントからのリクエストを処理し、チェックの為にメッセージをリモートdrweb-proxy-serverコンポーネントに送信します。チェックの後、メッセージは**Receiver**コンポーネントに返されるか、または**Sender**コンポーネント経由で送信されます。 デフォルト値: **MailPoolOptions** = auto
SenderPoolOptions = {pool settings}	drweb-proxy-serverコンポーネントからの**Sender**コンポーネント経由でのメール送信リクエストを処理するスレッドプールの設定を指定します。 メッセージが**Sender**コンポーネントに送信される前に一時ディレクトリが作成され、そこにメッセージが保存されます。**Sender**の動作結果はdwreb-proxy-serverに返されます。 デフォルト値: **SenderPoolOptions** = auto

[ProxyServer]セクション

[ProxyServer]セクションではdrweb-proxy-serverモジュールに関する設定が定義されています。

Address = {list of sockets}	drweb-proxy-clientコンポーネントからのリクエストを受け取るためにdrweb-proxy-serverコンポーネントが使用するソケットアドレスのリストを指定します。 drweb-proxy-client は[ProxyClient]セクションの**ProxyServersAddresses**パラメータに設定された値に応じて、チェックのためにメッセージをdrweb-proxy-serverコンポーネントに渡します。 デフォルト値: **Address** = inet:8088@0.0.0.0

ProxyClientsAddresses = {list of sockets}	メッセージ送信に関するリクエストを受け取る為にdrweb-proxy-clientコンポーネントが使用するソケットアドレスのリストを指定します。 アドレスは次のように指定します: ADDRESS1 [WEIGHT1], ADDRESS2 [WEIGHT2] .. ADDRESSは基本的なアドレスタイプです。WEIGHTは0から100までのオプションの数値で、このアドレスの「重さ」を定義します。このWEIGHTはネットワーク内の1つのホスト上での相対負荷を定義します。値が大きいほどサーバ上の負荷は大きくなります。 このパラメータ値で指定するソケットアドレスはProxyClient]セクションの**Address**パラメータ値のソケットアドレスと一致させてください。 デフォルト値: **ProxyClientsAddresses** = inet:8066@CLIENT-IP
ReceiverPoolOptions = {pool settings}	メッセージをチェックの為にdrweb-maildに渡す役割を持つスレッドプールの設定を指定します。 プール内のスレッドはメッセージをチェックするリクエストをdrweb-proxy-clientから受け取り、このメッセージにユニークなIDを作成してチェックの為にdrweb-maildに渡します。チェックが完了した後、drweb-proxy-clientはオリジナルの、または変更されたメッセージを受け取ります。 デフォルト値: **ReceiverPoolOptions** = auto
SenderPoolOptions = {pool settings}	**Sender**コンポーネント経由で送信する為にメッセージをdrweb-proxy-clientに渡す役割を持つスレッドプールの設定を指定します。

	プール内のスレッドはメッセージ送信のリクエストを様々なコンポーネントから受け取り、それらを処理する為にdrweb-proxy-clientに渡します。 処理結果はメッセージ送信のリクエストをしたコンポーネントに返されます。 デフォルト値: **SenderPoolSettings** = auto

[POP3]セクション

Dr.Web MailD はプロトコルフィルタプログラム経由でPOP3サーバと動作することが可能です。POP3フィルタプログラムはPOP3サーバのdrweb-maildに接続されたプロキシサーバで、POP3サーバによってユーザに送信された電子メールをフィルタします。POP3サーバはローカル、またはリモートコンピュータ上で動作することができます。

[POP3]セクションではdrweb-pop3モジュールに関する設定が定義されています。

ServerAddress = {socket address}	POP3サーバに接続する為にPOP3フィルタが使用するアドレスの指定です。 デフォルト値: **ServerAddress** = inet:pop3@localhost

ListenAddress = {socket address}	クライアントからのリクエストを受け取る為に使用するソケットアドレスのリストです。 次の種類のアドレスを指定することが出来ます: inet:.. or inet-ssl:..（TLS/SSLを使用する場合） 後者の場合、POP3フィルタが使用するPOP3Sプロトコルが必要です。 デフォルト値: **ListenAddress** = inet:5110@localhost

ServerTLSSettings = {TLS/SSL settings}	POP3でのサーバ接続に対するTLS/SSL 設定を指定します。 設定はカンマで区切られます。認証および非公開キー(private_keyファイル)が指定され、inet-sslソケットが使用されている場合のみサーバが使用されます。使用可能なパラメータについての詳細は一般設定ファイルの説明をご覧ください。 例: **ServerTLSSettings** = use_sslv2 no, private_key_file /path/to/pkey, certificate /path/to/certificate POP3フィルタによって権限を使用されるユーザ(通常drwebユーザ)は認証のあるファイルに対する読み取り権限を持っている必要があります。 デフォルト値: **ServerTLSSettings** =
ClientTLSSettings = {TLS/SSL settings}	POP3でのクライアント通信に対するTLS/SSL設定の指定です。 設定はカンマで区切られます。使用可能なパラメータについての詳細は一般設定ファイルの説明をご覧ください。 例: **ClientTLSSettings** = use_sslv2 no, private_key_file /path/to/pkey, certificate /path/to/certificate POP3フィルタによって権限を使用されるユーザ(通常drwebユーザ)は認証のあるファイルに対する読み取り権限を持っている必要があります。 デフォルト値: **ClientTLSSettings** =

IoTimeout = {time}	動作が進行中の場合の、クライアントソケットとの全ての入力／出力動作に対するタイムアウトの指定です。 デフォルト値: **IoTimeout** = 60s
ProcessingTimeout = {time}	drweb-maild がメッセージを処理するタイムアウトの指定です。 デフォルト値: **ProcessingTimeout** = 60s
MinFilterToMaildConnections = {numerical value}	POP3フィルタとdrweb-maild 間の接続数の下限を指定します。 デフォルト値: **MinFilterToMaildConnections** = 2
MaxFilterToMaildConnections = {numerical value}	POP3フィルタとdrweb-maild 間の接続数の上限を指定します。値が0に設定されている場合、接続数に制限はありません。 デフォルト値: **MaxFilterToMaildConnections** = 0
FilterToMaildKeepAliveTime = {time}	POP3フィルタとdrweb-maild 間の非活動接続を保持する時間の上限を指定します。 drweb-maildとインタラクトする為にPOP3フィルタはdrweb-maildとの接続を複数維持し、各接続はそれぞれ1つの動作を行います。使用可能な接続が残っていない場合、**MaxFilterToMaildConnection**パラメータ値で指定された閾値の数に達するまで新しい接続が作成されます。**FilterToMaildKeepAliveTime**パラメータ値で指定された時間を超えて接続が非活動であった場合、それらの接続は閉じられます。開かれた接続の合計は**MinFilterToMaildConnections**パラ

	メータ値よりも少なくなることはありません。 デフォルト値: **FilterToMaildKeepAliveTime** = 30s
ThreadInactivityTimeout = {time}	スレッド非活動のタイムアウトを指定します。この時間を経過すると、非活動スレッドは削除されます。 デフォルト値: **ThreadInactivityTimeout** = 30s
PoolOptions = {pool settings}	メインスレッドプールの設定を指定します。このスレッドはクライアントからの接続を処理します。 各接続にはそれぞれ新しいスレッドが必要です。それが無い場合、クライアントのいくつかはフリースレッドを待って接続が切れたままになります。 デフォルト値: **PoolOptions** = auto
CallbackPoolOptions = {pool settings}	補助スレッドプール設定の指定です。スレッドはdrweb-maildからの、完了したメッセージ処理に関するシグナルを処理します。 デフォルト値: **CallbackPoolOptions** = auto
MaxConnections = {numerical value}	受信する接続数の上限を指定します。値が0に設定されている場合、制限はありません。 デフォルト値: **MaxConnections** = 0
DoS_Blackhole = {Yes | No}	1つのIPアドレスからの同時接続が多すぎた場合に、クライアントに対してエラーメッセージを送信せずにそれらをすぐにドロップする指定です。

	デフォルト値: **DoS_Blackhole** = no
DisablePlainText = {Yes | No}	クライアントがログインおよびパスワードをプレーンテキストで送信することを許可しない指定です。前もって設定するにはOpenSSLが必要です。 デフォルト値: **DisablePlainText** = no
MaxConnectionsPerIp = {numerical value}	1つのIPアドレスからの同時接続数の上限を指定します。値が0に設定されている場合、制限はありません。 デフォルト値: **MaxConnectionsPerIp** = 0
MaxCommandLength = {size}	POP3プロトコルに対するコマンドの最大サイズを指定します。各コマンドは、クライアントからサーバに送信されるストリングです。現在のRFCによると、このコマンドの可能な最大サイズは約1000バイトです。 このパラメータ値が小さい(10バイト以下)、または0に設定されている場合、クライアントのコマンドは処理されないので注意してください。 デフォルト値: **MaxCommandLength** = 1000b
OnFilterErrors = {actions}	メッセージがdrweb-maildモジュールに渡される前にエラーが発生した場合にメッセージに適用されるアクションの指定です。可能な値はrejectおよびpassです。 デフォルト値: **OnFilterErrors** = reject

セッションが開始されるとフィルタがPOP3コマンド**USER username**からユーザの名前を抜き取り、セッションの間中それを保存しておきます。POP3サーバ上での認証に成功すると、フィルタはメッセージをサーバからクライアントに渡します。

RETRコマンドへのサーバ応答以外の全てのコマンドおよびデータは変更されて渡されます。

RETRコマンドへのサーバ応答はdrweb-maildに渡され、処理されます。ユーザに渡されるのはその後になります。

POP3フィルタがプラグインの設定によってメッセージをブロックし、そのメッセージにredirectアクションを適用する場合、転送は実行されないので注意してください。**Dr.Web for UNIX mail servers**の現在のバージョンでは、POP3フィルタは**Sender**コンポーネントにメッセージを送ることが出来ないため、作成されたメッセージはいずれも送信されません。

POP3フィルタとお使いのMTAとのインタラクションを設定するにはmaild_MTA.mmcファイル内の以下のラインをアンコメントしてください。

```
drweb-pop3  local:/var/drweb/ipc/.agent  15  30
  MAIL  drweb:drweb
```

[IMAP]セクション

Dr.Web MailD はプロトコルフィルタプログラム経由でIMAPサーバと動作することが可能です(キャッシングはサポートされています)。IMAPフィルタプログラムはIMAPサーバのdrweb-maildと接続されたプロキシサーバで、サーバによってユーザに送信された電子メールをフィルタします。IMAPサーバはローカル、またはリモートコンピュータ上で動作することができます。

[IMAP]セクションではdrweb-imapモジュールに関する設定が定義されています。

ServerAddress = {socket address}	フィルタがIMAPサーバへの接続に使用するアドレスの指定です。 デフォルト値: **ServerAddress** = inet:imap@127.0.0.1
ListenAddress = {socket address}	クライアントからのリクエストを受け取る際に使用するソケットアドレスのリストを指定します。

	次の種類のアドレスを指定することが出来ます: `inet:..` or `inet-ssl:..` (TLS/SSLを使用する場合) 後者の場合、IMAPフィルタが使用するIMAPSプロトコルが必要です。
	デフォルト値: **ListenAddress** = `inet:5200@0.0.0.0`
ServerTLSSettings = `{TLS/SSL settings}`	IMAPでのサーバ接続に対するTLS/SSL設定を指定します。 設定はカンマで区切られます。認証および非公開キー(`private_key`ファイル)が指定され、`inet-ssl`ソケットが使用されている場合のみサーバが使用されます。使用可能なパラメータについての詳細は一般設定ファイルの説明をご覧ください。 例: **ServerTLSSettings** = `use_sslv2 no, private_key_file /path/to/pkey, certificate /path/to/certificate` IMAPフィルタによって権限を使用されるユーザ(通常`drweb`ユーザ)は認証のあるファイルに対する読み取り権限を持っている必要があります。 プログラムの現在のバージョンではSSLセッションのキャッシュは出来ません。
	デフォルト値: **ServerTLSSettings** =
ClientTLSSettings = `{TLS/SSL settings}`	IMAPでのクライアント通信に対するTLS/SSL設定の指定です。. 設定はカンマで区切られます。使用可能なパラメータについての詳細は一般設定ファイルの説明をご覧ください。 例:

	ClientTLSSettings = use_sslv2 no, private_key_file /path/to/pkey, certificate /path/to/certificate IMAPフィルタによって権限を使用されるユーザ(通常drwebユーザ)は認証のあるファイルに対する読み取り権限を持っている必要があります。 プログラムの現在のバージョンではSSLセッションのキャッシュは出来ません。 デフォルト値: **ClientTLSSettings** =
IoTimeout = {time}	動作が進行中の場合の、クライアントソケットとの全ての入力/出力動作に対するタイムアウトの指定です。 デフォルト値: **IoTimeout** = 60s
ProcessingTimeout = {time}	drweb-maild がメッセージを処理するタイムアウトの指定です。 デフォルト値: **ProcessingTimeout** = 60s
MinFilterToMaildConnections = {numerical value}	IMAPフィルタとdrweb-maild 間の接続数の下限を指定します。 デフォルト値: **MinFilterToMaildConnections** = 2
MaxFilterToMaildConnections = {numerical value}	IMAPフィルタとdrweb-maild間の接続数の上限を指定します。値が0に設定されている場合、接続数に制限はありません。 デフォルト値: **MaxFilterToMaildConnections** =

	0
FilterToMaildKeepAliveTime = {time}	IMAPフィルタとdrweb-maild間の非活動接続を保持する時間の上限を指定します。 drweb-maildとインタラクトする為にIMAPフィルタはdrweb-maildとの接続を複数維持し、各接続はそれぞれ1つの動作を行います。使用可能な接続が残っていない場合、**MaxFilterToMaildConnection**パラメータ値で指定された閾値の数に達するまで新しい接続が作成されます。**FilterToMaildKeepAliveTime**パラメータ値で指定された時間を超えて接続が非活動であった場合、それらの接続は閉じられます。開かれた接続の合計は**MinFilterToMaildConnections**パラメータ値よりも少なくなることはありません。
	デフォルト値: **FilterToMaildKeepAliveTime** = 60s
CallbackPoolOptions = {pool settings}	補助スレッドプール設定の指定です。スレッドはdrweb-maildからの、完了したメッセージ処理に関するシグナルを処理します。
	デフォルト値: **CallbackPoolOptions** = auto
ThreadInactivityTimeout = {time}	スレッド非活動のタイムアウトを指定します。この時間を経過すると、非活動スレッドは削除されます。
	デフォルト値: **ThreadInactivityTimeout** = 30s

PoolOptions = {pool settings}	メインスレッドプールの設定を指定します。このスレッドはクライアントからの接続を処理します。各接続にはそれぞれ新しいスレッドが必要です。それが無い場合、クライアントのいくつかはフリースレッドを待って接続が切れたままになります。 デフォルト値: **PoolOptions** = auto
MaxConnections = {numerical value}	受信する接続数の上限を指定します。値が0に設定されている場合、制限はありません。 デフォルト値: **MaxConnections** = 0
MaxConnectionsPerIp = {numerical value}	1つのIPアドレスからの同時接続数の上限を指定します。値が0に設定されている場合、制限はありません。 デフォルト値: **MaxConnectionsPerIp** = 0
DisablePlainText = {Yes | No}	クライアントがログインおよびパスワードをプレーンテキストで送信することを許可しない指定です。前もって設定するにはOpenSSLが必要です。 デフォルト値: **DisablePlainText** = no
DoS_Blackhole = {Yes | No}	1つのIPアドレスからの同時接続が多すぎた場合に、クライアントに対してエラーメッセージを送信せずにそれらをすぐにドロップする指定です。 デフォルト値: **DoS_Blackhole** = no
MaxCommandLength = {size}	IMAPプロトコルに対するコマンドの最大サイズを指定します。各コマンドは、クライアントからサーバに送信されるストリングです。現在のRFCによると、このコマンドの可能な最大サイズは約1000バ

	イトです。 このパラメータ値が小さい(10バイト以下)、または0に設定されている場合、クライアントのコマンドは処理されないので注意してください。 デフォルト値: **MaxCommandLength** = 1000b
MaxCachedHeadersPerMail = {size}	よく使われるヘッダを保存する為に割り当てられるメモリサイズの上限を指定します。IMAPフィルタは、メインメッセージヘッダへのアクセスを迅速化するためにそれらをランダムにキャッシュします。 値が0に設定されている場合、制限はありません。 デフォルト値: **MaxCachedHeadersPerMail** = 64k
MaxLettersPerUser = {numerical value}	1つのセッション中にキャッシュされるメッセージの最大数を指定します。IMAPプロトコルによってクライアントは1つのメッセージに対する部分的リクエストを大量に実行することが出来る為、IMAPフィルタは、チェックされたメッセージのキャッシュを保持します。 多くの場合リクエストは順次実行されますが、ユーザが複数のレコードを要求した場合はメッセージを2つ以上キャッシュする必要があります。 値が0に設定されている場合(推奨出来ません)、キャッシュされるメッセージ数に上限は無いとみなされます。 デフォルト値: **MaxLettersPerUser** = 6
MaxDiskPerUSer = {size}	キャッシュされたメッセージが占めるディスク容量の上限を指定します。 デフォルト値: **MaxDiskPerUSer** = 10m

OnFilterErrors {actions}	=	メッセージがdrweb-maildモジュールに渡される前にエラーが発生した場合にメッセージに適用されるアクションの指定です。可能な値はrejectおよびpassです。 デフォルト値: **OnFilterErrors** = reject

IMAPフィルタは、メインメッセージヘッダへのアクセスを迅速化するためにそれらをRAMメモリ内にキャッシュします。 理論上、使用可能なメモリを全て消費し、ヘッダを多く含む大量のメッセージによってIMAPフィルタの動作を遅くさせることが可能です。

IMAPフィルタは、キャッシュするヘッダの合計サイズをコントロールする特別なanti-floodingパラメータである**MaxCachedHeadersPerMail**を持っています。このパラメータの値が小さすぎると、MIME attachmentの名前とタイプを表示するのが難しくなる場合があるので注意してください。

IMAPフィルタとお使いのMTAとのインタラクションを設定するにはmaild_MTA.mmcファイル内の以下のラインをアンコメントしてください。

```
drweb-imap  local:/var/drweb/ipc/.agent  15  30
  MAIL  drweb:drweb
```

[Rules]セクション

[Rules]セクションでは、メッセージ処理に関するルールが定義されています。ルールによって、ユーザの必要に応じて**Dr.Web MailD**動作のパラメータを柔軟に変更することが出来ます。特定のエレメントのセットを持つメッセージに対するプログラムの動作を指定し、それらに応じてメッセージ処理の手順を変更することが出来ます。そのようなエレメントには送信者および受信者のアドレス、検出された悪意のあるオブジェクト、その他追加的な特徴(送信者のIPアドレスやメッセージのサイズなど)があります。ルールは指定された順番に適用されます。

ルールはそれぞれ2つのパートから成っています。

```
CONDITION stop|cont [SETTINGS]
```

CONDITIONは、SETTINGSパートi内で指定されたアプリケーションの設定を有効にするためにtrueである必要があります。ルール内でSETTINGSが指定されていない場合、CONDITIONを使用して外部ソース(ldap、mysql)から

SETTINGSをダウンロードすることも可能です。

正規表現はそれぞれ2つのパートから成っています。
[prefix_name:][value]

prefix_nameはパラメータ名で、value はパラメータ値です。

以下のパラメータ名を使用することが出来ます。

- **any** - 送信者または受信者。パラメータ値 - lookup。
- **from (sender)** - 送信者。パラメータ値 - lookup。
- **to (rcpt)** - 受信者。パラメータ値 - lookup。
- **block** - オブジェクト(ウイルスまたはその他悪意のあるオブジェクト)をブロック。パラメータ値 - lookup。
- **client-ip** - 送信者のIPアドレス(**Receiver**コンポーネントが送信者のIPアドレスに関する情報を促すように調整されている場合)。パラメータ値 - 保護するネットワークのリスト。
- **client-port** - 送信者のポート番号(**Receiver**コンポーネントが送信者のポート番号に関する情報を促すように調整されている場合)。パラメータ値 - ポート番号。
- **server-unix-socket** - 接続を受け取るためのUNIXソケットへの絶対パス(**Receiver**コンポーネントがソケットアドレスに関する情報を促すように調整されている場合)。パラメータ値 - UNIXソケットへのパス。
- **server-ip** - メールを受け取るために**Receiver**が使用するインターフェースのIPアドレス(**Receiver**コンポーネントがインターフェースIPアドレスに関する情報を促すように調整されている場合)。パラメータ値 - 保護するネットワークのリスト。
- **server-port** - 接続を受け取るためのサーバのポート番号(**Receiver**コンポーネントがサーバポート番号に関する情報を促すように調整されている場合)。パラメータ値 - ポート番号。
- **id** - 特定のメールを受け取る**Receiver**のユニークなID(**Receiver**コンポーネントがIDに関する情報を促すように調整されている場合)。パラメータ値 - **Receiver**IDを含んだストリング。
- **auth** - 送信者の認証成功に関する情報(**Receiver**コンポーネントが送信者認証に関する情報を促すように調整されている場合)。パラメータ値 - 指定されていません。
- **size** - メッセージのサイズ。サイズの値の前に比較記号{!= | == | < | > | <= | >=}を指定することが出来ます。比較記号が指定されてい

ない場合、デフォルトで≤（小さいか等しい）が使用されます。いくつかのサービスキャラクタ（"!" と "="）は比較記号シンタックス内で使用されるので、比較記号を使用する場合は該当する値を引用符で囲んでください。

例:

```
"size:>=10m" cont scan=no
```

10 MBよりも大きなメッセージは全てスキャンの対象から除外されます。この場合、引用符の使用は必須です。

- **md-client** – ルールからその設定を受け取るクライアントのユニークなIDです。起動前に、**Dr.Web MailD**は全てのアクティブなクライアントに対する設定をルール内から探します。

  例:

  ```
  "md-client:client1"
  ```

  メッセージがclient1クライアントに対して受信される場合、このコンディションはtrueになります。

- **score** – メッセージスコアです。スコア値の前に比較記号{!= | == | < | > | <= | >=}を指定することが出来ます。比較記号が指定されていない場合、比較記号≤のデフォルトグループが使用されます。いくつかのサービスキャラクタ（"!" と "="）は比較記号シンタックス内で使用されるので、比較記号を使用する場合は該当する値を引用符で囲んでください。

パラメータ名が指定されていない場合、デフォルトで**any**が使用されます。パラメータ値に空白、または "|&)(!="記号が含まれている場合は引用符で囲まれている必要があります。引用符内で個別の引用符号（""）を指定する場合はバックスラッシュ（"\"）を前に置いてください。

また[prefix_name:][value]の代わりに、それぞれ常に正の値、負の値を持つ特別なキーワードtrueとfalseが使われる場合もあります。

例:

```
true cont some_settings
```

この設定は常に適用されます（このルールが検査の間に処理された場合）。

別々のコンディションは括弧や論理演算子AND （&&）、OR （||）、NOT （!）に

よって結合することが出来ます（括弧内で代わりのシンタックスが指定されます）。

例:

```
sender:test && "size:>=10k"
```

このCONDITIONは、メッセージの送信者が "test"でメッセージサイズが10キロバイトよりも大きい場合にtrueになります。

```
!("rcpt:ldap:///??sub?(mail=$s)" OR auth:)
```

このCONDITIONは、ldapの"mail"フィールド内に少なくとも1人の受信者が見つからず、送信者が認証されていない場合にtrueになります。

メッセージがプラグインによって処理される場合、プラグインは**Dr.Web MailD**に特定のパラメータ値を要求することが出来ます。この場合**Dr.Web MailD**はルール内で指定されたコンディションに従ってメッセージを検査します。以下のアルゴリズムが使用されます。

1. まず、データベース内に受信者が存在するかどうかチェックされます。存在した場合、データベース内に保存されている設定内で、この受信者および受信者の全てのグループに対するパラメータ値の検索が実行されます。
2. データベース内に一致するものが見つからなかった場合、パラメータ値の検索は設定ファイル内で指定されたルール内で実行されます。ルールは指定された順番で上から下へ検査されます。まずCONDITIONが検査され、一致した場合、ルールのSETTINGSパート内で該当するパラメータ値が検索されます。
3. 必要なパラメータ値が見つからず、CONDITIONの後に"stop"が続いている場合、検索は**Dr.Web MailD**のデフォルトパラメータ値のあるセクション内で実行されます。必要なパラメータ値が見つからず、CONDITIONの後に"cont"が続いている場合、他のコンディションに従って更なる検査が実行されます。

必要なパラメータ値と一致するものが他のコンディション内に無いと分かっている場合、Stop によって検索する時間を削減することが出来ます。

例:

```
rcpt (sender, any): [address or regular expression] stop|cont [settings]
```

このルールによって、特定のユーザに対する設定をいくつか指定することが出来ます。

SETTINGS は、特定の値を持った**Dr.Web MailD**パラメータのセットです。

[plug-in_name/]**param1** = value1, [plug-in_name/]**param2** = value2 ...

paramNはパラメータ名で、valueNはパラメータ値です。パラメータがプラグインによって使用される場合、スラッシュを挟んでパラメータ名の前にプラグイン名を指定する必要があります。

SETTINGSは特定のパラメータ値が必要な場合のみ処理されます。そのためパラメータ値内のエラーは、プログラムが起動され使用された場合にのみ検出されることがあります。起動前にエラーを検出するにはcheck-onlyモード(コマンドラインパラメータ--check-onlyで)を使用します。パラメータ値がデータベースに保存される際にその有効性が即座に検査され、無効なパラメータを持つルールはブロックされます。

例:

sender:a@drweb.com cont headersfilter/**Action** = pass, vaderetro/**max_size** = 100k

この場合、送信者a@drweb.comに対して、headersfilterプラグインに**Action** = passが指定され、vaderetroプラグインのメッセージサイズの上限(**max_size**)が100キロバイトに設定されています。

valueN内でカンマを使用する場合、その前にバックスラッシュ"\"を指定する必要があります。

例:

to:a@drweb.com cont drweb/**ProcessingErrors** = pass\, redirect(err@drweb.com)

この場合、pass, redirect(err@drweb.com)値を引用符内に置くことは出来ません。パーサがストリングのその部分をそれぞれ1つの値に分けてサブストリングの解析を行わず、**ProcessingErrors**にしてしまうからです。

SETTINGSセクション内のパラメータを指定しない場合、それらはCONDITIONセクション内のlookupコマンドでサーバから直接要求されます。

LDAPを使用している場合に便利です。

```
to:regex:.*@drweb.com  &&  "ldap:///-drwebRules-sub-(mail=$s)" cont
```

この例では、メッセージ受信者のドメインがdrweb.comで、送信者または全ての受信者がldapのコンディション"mail=$s"に従っている場合、drwebRulesフィールドのパラメータが使用されます。パラメータは新しいメッセージごとにアップロードされ、キャッシュに保存されます。これにより、ユーザはサーバを再起動させることなく設定を変更することが出来ます。LDAPのルックアップは括弧があるので引用符で囲まれています。

ルールのストリングがラインよりも長くなる場合、ラインの終端にバックスラッシュ"\"を置いてルールを次のラインに続かせます。

ルールは常に上から下へ、左から右へ処理されます。そのため新しいパラメータは古いパラメータをブロックします。例えば、**html**=yes,**html**=noと指定した場合、最後の値(**html**=no)が設定されます。

このアルゴリズムは、いくつかの異なる動作をするものを除いてルール内のほとんど全てのパラメータに使用されます。ルールが処理されると、例外グループのパラメータの新しい値がそれぞれ前回見つかった値に加えられ、データベースおよび設定ファイル内の全てのルールで検索が続行されます。検索の最後に、見つかった全ての値が結合されます。

例外のパラメータには以下のものがあります。

- **LocalRules** (Dr.Web Modifier プラグイン内)
- **AcceptCondition** (headersfilter プラグイン内)
- **RejectCondition** (headersfilter プラグイン内)
- **AcceptPartCondition** (headersfilter プラグイン内)
- **RejectPartCondition** (headersfilter プラグイン内)
- **MissingHeader** (headersfilter プラグイン内)
- **WhiteList** (VadeRetro プラグイン内)
- **BlackList** (VadeRetro プラグイン内)
- **RegexsForCheckedFilename** (drweb プラグイン内)

動作の違いは全て、パラメータの記述内で明示的に指定されます。

address-、user-　、domain-指定パラメータが全てデータベース内に保存される場合、それらは1つのライン内で指定するようにしてください。

例:

アドレス	ルール
test1@drweb.com	VadeRetro/SubjectPrefix = \"spam\", modifier/localrules=select message\, append_text "Some Text"
test2@drweb.com	headersfilter/MissingHeader = Date, headersfilter/MissingHeader =From, headersfilter/MissingHeader = To

これらのパラメータに対する**stop**指示は通常通り処理されます。この指示は検索を中止し、パラメータの累積値を返します。

例:

例えばODBC経由でデータベースをセットアップする場合、以下のようになります。

アドレス	ルール
test@drweb.com	modifier/LocalRules = select message\, append_text "Scanned 3333!

設定ファイル内に以下のルールも設定されます。

```
true cont modifier/LocalRules = select message\, append_text "Scanned 44444 - global rules!", modifier/LocalRules = quarantine
```

データベース内で、特定のユーザに対し以下のようなルールのセットが設定されます。

```
> email-info test@drweb.com
  test@drweb.com A=1 S=1
name:
  aliases: alias_test@drweb.com
  groups: divine good evil
```

```
rules:
1: true cont modifier/LocalRules = select message\, append_text "Scanned!", modifier/LocalRules = quarantine
2: true cont modifier/LocalRules = select message\, append_text "Scanned 2222!"
3: "rcpt:odbc:select rules from maild where a='$s'" cont
custom:
```

Dr.Web Modifierプラグインが処理するtest@drweb.comへのメッセージに対しては、**LocalRules**パラメータの以下の値が使用されます。

```
select message, append_text "Scanned!", quarantine, select message, append_text "Scanned 2222!", select message, append_text "Scanned 3333!", select message, append_text "Scanned 44444 - global rules!", quarantine
```

これらの値の特定の順番を考慮してください。まずデータベースから値が取られ、次に設定ファイルから取られます。

メッセージに対してさらに他の受信者が指定され、それらに対してデータベース内でmodifier/**LocalRules**パラメータの他の値が指定されている(または全く指定されていない)場合、データベースからのそれらの値は全て無視され、以下のグローバル変数が適用されます。

```
select message, append_text "Scanned 44444 - global rules!", quarantine
```

ルールストリング内にエラーがあった場合(ルックアップの処理を除く全ての場合において)、それらはログファイルに出力され、ルール自体は無視されます。ルールの全てのパートが同時に処理されるわけではないということに注意してください。ルックアップ値およびいくつかの変数の値は使用される直前に処理されるため、それらの値内でのエラーは全てメールメッセージを処理する瞬間に出る可能性があります。起こりうる全てのエラーに対する設定をチェックするにはdrweb-maildコンポーネントを --check-onlyコマンドラインパラメータで動作させてください。

使用可能なパラメータの種類は以下のとおりです。

- ルール内でのみ指定されたパラメータ

- 他のモジュールの設定ファイル内で指定されたパラメータ
- クライアントによってのみ使用され、1つの必須コンディション－クライアントのユニークなID(md-client)でのみ指定されたパラメータ

各パラメータがルール内で使用可能であるかどうかは他のモジュールの設定ファイル内で指定され、ドキュメンテーション内のパラメータ記述に記載される必要があります。

[rules] 内では以下のパラメータを設定することが出来ます。

html = {Yes | No}	Yesの場合、html書式で通知を作成するよう**Dr.Web MailD**に命令します。それ以外の場合はプレーンテキスト書式で作成されます。 デフォルト値: **html** = Yes
quarantine = {Yes | No}	Yes の場合、メッセージを隔離に移動するよう命令します。 デフォルト値: **quarantine** = Yes
scan = {list of plug-ins}	メッセージ検査にどの**Dr.Web MailD**プラグインを使用するかを指定します。プラグイン名はコロンで区切られます。パラメータ値がAllに設定されている場合、全てのプラグインがメッセージを検査します。Noが設定されている場合、どのプラグインも使用されません。 プラグイン名を区切るにはコロン":"を使用します。リストからプラグインを除外するには、そのプラグインの前にマイナス記号"-"を指定します。"-"記号とプラグイン名の間には空白を入れません。"-"記号の無いプラグイン名はAll値の後には指定できません。 例: **scan** = all – 全てのプラグインによって検査されます。 **scan** = no –どのプラグインも使用されません。

	scan = all:-foo – foo以外の全てのプラグインによって検査されます。 **scan** = Foo:Bar – fooおよびbarプラグインによってのみ検査されます。 **scan** = all:foo – 間違ったパラメータフォーマットです。Allパラメータ値の後に"-"記号の無いプラグイン名を指定することは出来ません。 **scan** = -foo:all – 間違ったパラメータフォーマットです。Allパラメータ値はストリングの頭に設定する必要があります。 **scan** = -foo – 間違ったパラメータフォーマットです。Allパラメータ値が無い場合に"-"記号の付いたプラグイン名を指定することは出来ません。 デフォルト値: **scan** = All
notify[.{notification type}] ={allow|block}[({address types})][condition]	通知メールの種別、送付先、生成の可否などを指定します。allowは生成を許可し、blockは禁止します。種別が指定されていない場合、このパラメータ値は全ての通知に適用されます。 使用可能な通知の種別はdrweb-notifierモジュールがサポートしているものに限ります。追加のプラグインはそれぞれが持つ種別を追加することが出来ます。デフォルトでは以下の通知の種別がサポートされています。 • **notify.Virus** - ウイルス検出通知 • **notify.Cured** - メッセージ修復通知 • **notify.Skip** - ファイル検査不可(スキップ)通知 • **notify.Archive** - アーカイブ検査制限抵触通知 • **notify.Error** - メッセージ検査中のエラー発生通知

- **notify.Rule** - ルール制限抵触通知
- **notify.License** - ライセンス制限抵触通知
- **notify.Malware** - マルウェア検出通知

パラメータ値の後にqualifierを括弧で囲んで指定することが出来ます。これは、適用されるパラメータに対するアドレスの種類を指定します。コロンで区切って複数の種類を指定することが出来ます。使用可能なqualifierは以下のとおりです。

- sender - メール送信者への通知
- rcpt - メール受信者への通知
- admin - メール管理者への通知
- any（またはqualifier無し）- 全ての種類のアドレスへの通知

例:

Notify=block or notify=block (any) - 全ての通知メールを禁止

notify.Virus = block (sender: admin) - 送信者・管理者宛のウイルス検出通知メールを禁止

ある種別の通知に対するルールが見つからず、また一般ルールも見つからなかった場合（種別指定の無い）、該当する通知は無効とみなされます。

Notifyパラメータの複数の値は、**Dr.Web Modifier**プラグイン内の**LocalRules**パラメータに使用されるものと同じルールに応じて結合されます。

例:

true cont **notify.virus** = allow (sender)

true cont **notify.virus** = allow (admin), **notify** = block

	これらのルールは以下のルールと同じになります。 `true cont` **`notify.virus`** `= allow (sender:admin),` **`notify`** `= block` ウイルスに関する通知のみが管理者および送信者宛に送られ、それ以外の通知は全てブロックされます。
	デフォルト値: デフォルトの通知パラメータは以下のとおりです。 • **`notify`** `= block(any)` • **`notify.Virus`** `= allow(any)` • **`notify.Cured`** `= allow(admin:sender)` • **`notify.Skip`** `= allow(sender)` • **`notify.Archive`** `= allow(admin:sender)` • **`notify.Error`** `= allow(admin:sender)` • **`notify.Rule`** `= allow(admin)` • **`notify.License`** `= allow(admin)` • **`notify.Malware`** `= allow(any)`
`plugin_name/max_size` `= {size}`	それぞれのプラグインが検査するメッセージの最大サイズを指定します。
`plugin_name/use` `= {Yes | No}`	Yesの場合、プラグインにメッセージをスキャンする指示を出します。Noの場合、プラグインにメッセージ検査をスキップする指示を出します。
`NotificationNamesMap` `= notify_name1`	それぞれのプラグインモジュールに対して、検査するメッセージの最大サイズを設定することが出来ます。

file_name1, notify_name2 file_name2 ...	**NotificationNamesMap** = name1 file_name1, name2 file_name2 ... レポート名を新しいものにマッピングすることが出来ます。例えば、エンベロープに応じて他のレポートを割り当てる際に使用することが可能です。 パラメータ • nameN - 新しいファイルが作成される通知の名前です。名前のリストは **notify**パラメータの記述内にあります。また、一般レポートに対して report名を、DSNに対してdsnを指定することも出来ます。 • file_nameN - 通知に対する新しいレポートファイル名です。ファイル名の頭にsender_、rcpts_、admin_、report_、dsn_のプレフィックスのいずれかを付け、ファイル拡張子を.msgに変更します。その結果、[Notifier]セクションの **TemplatesBaseDir**パラメータで指定されたディレクトリ内で検索されるファイルの名前は sender_file_nameN.msgになります。 例: **NotificationNamesMap** = virus my-virus, archive my-arch
SenderAddress = {address1|address2|...}	メッセージを送信するために**Sender**コンポーネントに渡されるアドレスの指定です。"|"記号で区切って複数のアドレスを指定することが出来ます。以下のようなルール内で **SenderAddress**パラメータを使用した場合、 "to:mysql:select * from adr" cont SenderAddress = address1|address2|address3

	"to:mysql:select * from adr" の基準を満たしたメッセージが、リスト上にある使用可能な最初のアドレスに送信されます(例えばaddress1が使用可能でなかった場合、address2への送信が試行され、address2も使用出来なかった場合address3が使用されます)。 **Sender**がそのパラメータをサポートしている場合、メッセージを指定されたアドレスに直接送信します。現時点では**SenderAddress**パラメータをサポートしているのはSMTP/LMTPメソッドを使用したdrweb-senderモジュールのみです。
rule = {section name}	よく使用するパラメータのグループを1つの**User**パラメータセクション内にまとめることが出来ます。**rule**指示を用いることで追加パラメータを使用することが可能です。 各セクションはユニークな名前を持っている必要があります。それぞれのセクションは、初めて使用される前に指定されていなくてはなりません。**Dr.Web MailD**の現在のバージョンでは1つのルールに対して1つの**rule**パラメータのみサポートしています。
	ユーザセクションヘッダの書式は以下のとおりです。 [Rule: name], nameは、英数字および空白を含むユニークなセクション名です。各パラメータは一行ごとに記述します。ユーザセクションの終わりは次のセクションの始まりか、設定ファイルの終わりによって示すことが出来ます。 設定ファイルはuserパラメータの特別なセクション(デフォルトパラメータのセクション)を含んでいます。これにはdefaultという名前が付き、セクションのヘッダ内のRuleキーワードはスキップすることが出来ます。
	全てのレポートをブロックし隔離への移動を無効にする、ユーザパラメータを持ったセクションの例です。

	[Rule:MySection] **quarantine** = no **notify** = block ユーザセクションのルール内で**MySection**を使用した例です。 [Rules] **Rcpt**:regex:example\.com cont rule=mysection **Sender**:lol@foo.com && **block**:vir1 cont **notify.Skip**=allow, **notify.Virus**=allow, **rule**=MySection
	これらのルールが実行されると、レポートはブロックされ、受信者がexample.comドメインに属するメッセージの隔離への移動が無効になります。メッセージがlol@foo.comから送信され、ブロックするオブジェクトvir1が見つかった場合、検出されたウイルスに関するレポートのみが送信されファイルの隔離への移動は無効になります。

メッセージ内に複数の受信者が存在する場合について考えてみましょう。以下のパラメータ、

plugin_name/max_size

NotifyLangs

AdminMail

html

scan

plugin_name/use

およびクライアントの設定に適用される第三の全てのパラメータは、それぞれの受信者に対して別々に処理されます。例えば、あるパラメータに対する2人の受信者に異なる値が指定されていた場合、適用可能な他の設定を持ったメッセージのコピーがそれぞれの受信者に対して作成されます。

他のパラメータについては、CONDITIONが全ての受信者に対して実行される場合にパラメータ値がこのルールから使用されます。それ以外の場合はデフォルト値が使用されます。

コマンドラインパラメータ経由でのdrweb-maildモジュール内のルールの有効性は、特別なインターフェース経由でチェックすることが出来ます。これらのパラメータを使用して、仮想メッセージの様々な属性を指定することが可能です。モジュールは、このメッセージに適用可能なルールの設定を全てコンソールに出力します。使用可能な属性は以下のとおりです。

- -s [--sender] arg - メッセージ送信者（エンベロープから）
- -r [--rcpt] arg - メッセージ受信者（エンベロープから）
- -b [--block] arg - ブロックするオブジェクト（例：ウイルス名）
- --client-ip arg - 送信者のIPアドレス
- --server-ip arg - 受信者のサーバーのIPアドレス
- --client-port arg - 送信者のポート番号
- --server-port arg - 受信者のサーバーのポート番号
- --server-us arg - 受信者のサーバーのUNIXソケット
- --id arg - 受信者のユニークなID
- --auth -メッセージを、認証されたユーザから受信
- --size arg - メッセージサイズ（この値は{size}の型を持っています）
- --score arg - メッセージスコア
- --md-client arg – クライアントのユニークなID

例:

```
$ ./drweb-maild --auth
Thu May 29 16:03:44 2009 [3081324208] maild.rules DEBUG notify* :
Thu May 29 16:03:44 2009 [3081324208] maild.rules DEBUG all : block
Thu May 29 16:03:44 2009 [3081324208] maild.rules DEBUG archive : from=allow; admin=allow;
Thu May 29 16:03:44 2009 [3081324208] maild.rules DEBUG
```

```
Thu May 29 16:03:44 2009 [3081324208] maild.rules DEBUG cured : from=allow;
Thu May 29 16:03:44 2009 [3081324208] maild.rules DEBUG
Thu May 29 16:03:44 2009 [3081324208] maild.rules DEBUG error : from=allow; admin=allow;
Thu May 29 16:03:44 2009 [3081324208] maild.rules DEBUG
Thu May 29 16:03:44 2009 [3081324208] maild.rules DEBUG license : admin=allow;
Thu May 29 16:03:44 2009 [3081324208] maild.rules DEBUG
Thu May 29 16:03:44 2009 [3081324208] maild.rules DEBUG malware : from=allow; to=allow; admin=allow;
Thu May 29 16:03:44 2009 [3081324208] maild.rules DEBUG
Thu May 29 16:03:44 2009 [3081324208] maild.rules DEBUG rule : admin=allow;
Thu May 29 16:03:44 2009 [3081324208] maild.rules DEBUG
Thu May 29 16:03:44 2009 [3081324208] maild.rules DEBUG skip : from=allow;
Thu May 29 16:03:44 2009 [3081324208] maild.rules DEBUG
Thu May 29 16:03:44 2009 [3081324208] maild.rules DEBUG virus : from=allow; to=allow; admin=allow;
Thu May 29 16:03:44 2009 [3081324208] maild.rules DEBUG scan : all
Thu May 29 16:03:44 2009 [3081324208] maild.rules DEBUG html : 1
```

Lookup（外部参照）

Lookupは、外部ソースにあるオブジェクトおよびその値を参照するためのコモンインターフェースです。値はカンマで区切られます。lookupの種類を定義する特別なプレフィックスを値の前に置くことが出来ます。

```
[prefix1:]value1, [prefix2:]value2, ...
```

プレフィックスが指定されていない場合、値はそのまま使用されます。使用可能なプレフィックスは以下のとおりです。

- `value` – 参照される値自体がこのプレフィックスの後に指定されます。値に記号などが含まれている場合に便利です。
- `file` - ファイルへのパスです。ファイル内の値は一行に1つずつ指定します。それにより、二分探索が用いられ高速な検索が実行されます。
- `regex` - この値はPerl互換の正規表現です。検査の間にサブストリングが参照され、完全な一致は必要ありません。
- `rfile` - ファイルへのパスです。ファイルにはPerl互換の正規表現が含まれ、一行に1つずつ指定します。検査の間にサブストリングが参照され、完全な一致は必要ありません。
- `ldap` - LDAPサーバへのパスで、以下の書式で指定します。

  [**param1**=val1|**param2**=val2|...|] ldap_url

  ldap_urlはLDAPクエリのURLで、**param1**、**param2**などは、そのlookupに対する**Dr.Web MailD**設定ファイル[LDAP]セクションからのローカルパラメータです。このセクションからは、使用可能であると明示的に述べられているパラメータのみ指定することが可能です。

  LDAP URL は以下のようになります。

  ```
  ldap://hostport/dn[?attrs[?scope[?filter[?
  exts]]]]
  ```

  - `hostport` – ホスト名および追加のポート番号（hostname[:port]）
  - `dn` – 検索データベース
  - `attrs` – カンマで区切って列挙する、要求する属性のリスト

- scope – base、one、subの3つのストリングのうちいずれか
- filter – フィルタ名
- exts – LDAPおよび／またはAPI拡張オプション

例:

```
ldap://ldap.example.net/dc=example,dc=net?
cn,sn?sub?(cn=*)
```

フィルタ名には特別な記号のセットを指定することが出来ます。この値はクエリがLDAPサーバへ送られる前に、必要なエレメントに変更されます。

- $s – 要求されたエレメントに変更されます。例えば、あるアドレスを検索した場合、$sはこのアドレス全体に変更され（山括弧無しで）、あるドメインを検索した場合、$sはドメイン名に置き換えられます。
- $d – あるアドレスを検索した場合、$dはそのアドレスのドメイン部分に置き換えられます。それ以外の場合、要求全体が挿入されます。
- $u – あるアドレスを検索した場合、$uはそのアドレスのユーザ名に置き換えられます。ドメイン名を検索した場合、空のストリングが挿入されます。
- $$ – $1つに置き換えられます。

LDAPを使用する場合、OpenLDAP v. 2.0以降のライブラリが必要です。

- odbc, oracle - ODBC、Oracleデータベースに対するSQLクエリで、以下の書式で指定します。

  [**param1**=val1|**param2**=val2|...|] sql_request

  param1、**param2** などは、ODBC lookupおよびOracle lookupに対する**Dr.Web MailD**設定ファイルのそれぞれ[ODBC]、[Oracle] セクションからのローカルパラメータです。このセクションからは、使用可能であると明示的に述べられているパラメータのみ指定することが可能です。ldap lookupと同じ特別な記号を使用することが出来ます。

  新しいDSN設定が適用されるのはソフトウェアを再起動した後になります（SIGHUPシグナルの送出では既存の接続が再初期化されないことに注意してください）。

ODBCを使用する場合、ODBC version 3.0以降をサポートするODBCライブラリが必要です。このライブラリはスレッド対応でコンパイルされていなければなりません。UnixODBC 2.0以降の使用を推奨します。

Oracleを使用する場合、OTLv8以降をサポートするOracleクライアント付属のlibclntshが必要です。

Oracleに接続する際にユーザ名、パスワード、および**ConnectionString**パラメータの値としての接続名（**ConnectionString** = user/password@connectionname）を指定しなくてはならない場合があります。

接続名の設定には2つの方法があります。

1. Dr.Web MailDとOracleが同じコンピューターにインストールされている場合、Oracleドキュメンテーションに応じて、最初に環境変数ORACLE_HOMEを**Dr.Web MailD**に対して設定する必要があります。次に$ORACLE_HOME/network/admin/tnsnames.oraファイル内でTNS名の1つを接続名として指定します。
2. $ORACLE_HOME/network/admin/tnsnames.oraから直接セットアップ記述（改行無しで）をコピーすることも可能です。

例:

tnsnames.ora ファイル:

```
CONNECTIONNAME =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = localhost)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = CONNECTIONNAME)
    )
  )
```

そこで、

```
user/password@ CONNECTIONNAME
```

または

```
user/pasword@(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = localhost)(PORT = 1521))(CONNECT_DATA = (SERVER = DEDICATED)(SERVICE_NAME = CONNECTIONNAME)))
```

を接続ストリングとして指定することが出来ます。

- `postgres` - PostgreSQLデータベースに対するSQLクエリで、シンタックスはODBCに対する要求と同じです。
- `cdb` - データベース内に保存されているキーの英数字名です。CDB自体は`[alphanumerical key]:[alphanumerical value]`のペアが保存されている読み取り専用のデータベースです。データベースファイルは`tinycdb`パッケージを使用して作成することが出来ます。このlookupを使用するにはCDBデータベースのファイルリストを指定してください。ファイルは1つのテーブルのように取り扱うことができ、テーブル名はパスを取り除いたファイル名と同じになります(`file: /path/to/table.cdb --> table.cdb`へのフルパスを指定しない)。

  テーブルからのエントリを読むには以下のコマンドを使用します。

  ```
  select * from table.cdb where key='123'
  select * from table.cdb where key='$'
  ```

  CDBデータベースはSQLクエリ入力言語をサポートしていないため、 ドライバはlookupと動作する為にシングルコマンドをSQLにエミュレートします。

  ```
  select * from @tablename where key='@string'
  ```

  `@tablename`は**Dr.Web MailD**設定ファイルの`[CDB]`セクション内でソースアイテムとして指定されたいずれかのファイル名に変更してください。`cdb` lookupでは`ldap` lookupと同じ特別な記号を使用することが出来ます。

  例:

```
cdb:skipdomains=regex:^inbox|select *
from my_file where key='$s'
```

- berkeley - Berkeley DBとのインタラクションを可能にします。クエリの書式はcdbプレフィックスの書式と同じです。セットアップの際にシンボリックリンク/usr/lib/libdb.soが作成され、現在のライブラリを示します。シンボリックリンクが作成されなかった場合、正しいライブラリのバージョンを指定する必要があります(例:/usr/lib/libdb-4.5.so)。このlookupと動作することが出来るのはライブラリv. 4.3～4.6のみです。ldap lookupと同じ特別な記号を使用することが出来ます。
- firebird - Firebirdデータベースに対するSQLクエリで、シンタックスはODBCに対する要求と同じです。データベースに接続するにはHostフィールドでデータベースサーバのアドレスを指定してください。

```
Host=somehost            #somehost:3050
Host=somehost/1234       #somehost:1234
```

- sqlite - SQLiteデータベースに対するSQLクエリで、シンタックスはODBCに対する要求と同じです。このlookupを使用できるのはSQLiteデータベースv. 3.xのみです。

  SQLiteは、プログラムが書き込みをする間ファイルがロックされる仕様になっています。そのため、複数のプログラムで1つのSQLiteデータベースを使用している場合、データベースへの排他的なアクセスが出来ない時間(**Dr.Web MailD**設定ファイル[SQLite]セクションの**BusyTimeout**パラメータで指定された時間)が生じる可能性があります。その場合、エラーメッセージ"Database is locked"を出して書き込み処理は中断されます。

  GUIを持つツールは予備のデータベースをロックすることがあるため、そのようなツールは使用しないようにしてください。第三者プロセスがデータベースを長時間ロックした場合、または**Dr.Web MailD**そのものが1つのファイルに対して異なるタイプの統計情報を短いタイムアウト時間で出力するようにセットアップされている場合、統計情報のエクスポート中にエラーが発生することがあります。

  sqlite lookupではldap lookupと同じ特別な記号を使用することが出来ます。

  いくつかのパラメータに対する値が保存されたSQLiteデータベースが一定の時間使用できなかったが、その後接続が復元された場合、SQLiteとの接続を再初期化するためにHUPシグナルがdrweb-maildモジュールに

送信される必要があります。

- mysql - MySQLデータベースに対するSQLクエリで、シンタックスはODBCに対する要求と同じです。

プレフィックスの後に、それぞれのlookupに対して任意のローカルパラメータのリストを以下の書式で指定することが出来ます。

NAME1 = VALUE1 | NAME2 = VALUE2 | ... |

- NAMEM – パラメータ名（大文字小文字は区別されません）
- VALUEN – パラメータ値

使用可能なローカルパラメータは以下のとおりです。

- **SkipDomains** – lookup要求からスキップすることが出来るドメインのリストです。このパラメータについての詳細は設定ファイルのlookup設定内をご覧ください。
- **OnError** = {ignore|exception} – lookupのエラー処理手順を設定します。

  デフォルトでは"ignore" が使用され、エラーは無視され情報がログに出力されます。

  "exception" 値は、共通のエラーとして処理される（例えば**ProcessingError**パラメータを使用して）例外を作るよう指示します。企業が対応するセーフティポリシーを取り入れている場合に使用され、それぞれのメッセージはその他のコンポーネント内（lookupが使用しているデータベース内など）で起こりうる全てのエラーに関係なく処理される必要があります。

OnErrorパラメータは全てのlookupセクション（LDAP、ODBC、...）内で指定することができ、それらのlookupの処理中に生じたエラーに対して該当するアクションが適用されます。

OnErrorパラメータを使用したこのエラー処理は、パラメータ値の検索が実行されたときのみ使用することができ、**Dr.Web MailD**が起動された時には使用できません。そのためスタートアップ時に正常に処理されなかったlookupがあった場合、それらのlookupに対する**OnError**パラメータ値に関係なく、そのようなエラーは致命的とみなされます。

Lookup使用例

このクエリでは、ODBCストレージ内maildテーブルのdomainカラムにあるドメインからの全てのメッセージが、保護されたドメインに属するものとされます。

ProtectedDomains = "odbc:select domain from maild where domain='\$s'"

このクエリでは、%etc_dir/email.iniからの全てのアドレス、ローカルホストアドレス、およびLDAPクエリldaps:///??sub?(mail=$s)の後に見つかった全てのアドレス(fake.com:が付いたものを除く)が保護されているものとされます。

ProtectedEmails = file:%etc_dir/email.ini, localhost, ldap:skipdomains=regex:.*fake.com$|ldaps:///--sub-(mail=$s)

このクエリでは、あるアドレスがMySQLデータベース内maildテーブルのemailカラムにリストアップされているかどうかのチェックが実行されます。アドレスが見つかった場合、メッセージはrouterinfoカラム内で見つかったアドレスに送信されます。それ以外の場合は、アドレス内にfooを含む全ての受信者に送信されます。

Router = mysql:select routerinfo from maild where email='\$s', foo inet:234@foo.ru

Lookupをルール内で使用することが出来ます。

このクエリによって、受信者アドレスを含んだ全てのmailLDAPフィールドがrulesフィールドを受信することが出来ます。rulesフィールドにはこの受信者に適用される設定が含まれています。特別な記号が使用されているので(丸括弧など)、CONDITIONsは全て引用符で囲まれている必要があります。

"rcpt:ldap:///-rules-sub-(mail=$s)" cont

例えば、

rcpt:"ldap:///-rules-sub-(mail=$s)" cont,

と記述した場合、コンパイルエラーが発生します。

Mon Jun 29 18:53:01 2009 [3081262768] maild.rules ERROR '(' can not follow' "ldap:///-rules-sub-'

Mon Jun 29 18:53:01 2009 [3081262768]

```
maild.rules ERROR error in parse condition:
'rcpt:"ldap:///-rules-sub-(mail=$s)" cont'
```

このクエリによってアドレスをチェックすることが出来ます。SQLiteデータベース内domainテーブルのskipaddrフィールドに送信者か受信者のアドレスが含まれている場合、それらに対してdrwebプラグインは使用されません。

```
"any:sqlite:select skipaddr from domain
where skipaddr = '$s'" cont scan=all:-drweb
```

Lookup使用の制限

パラメータの中にはlookupsではなくLookupsLiteのみ使用可能なものがあります。

LookupsLiteはlookups同様に外部データの参照機能ですが、参照できる外部データの種別がfileのみであるという点が異なります。LookupsLiteは

- lookupの設定（各lookupに対する**SkipDomains**パラメータなど）
- プラグインの設定

で使用されます。

使用出来ないlookupを指定しようとした場合、以下のメッセージがログに出力されます。

```
Wed Jun 10 14:02:20 2009 [4160149200] Modifier
ERROR Error in init lookup [cdb:select * from /
root/mail/base_file_for_CDB.txt where
key='domain']: can't use this lookup here
```

Lookupの検証

lookupの有効性は、特別なdrweb-lookupユーティリティを用いて検証することが出来ます。以下のコマンドによって有効性を要求します。

```
$ %bin_dir/drweb-lookup [parameters]
query
```

queryは検索が実行される様々なタイプのlookupで、parametersはコマンドラインパラメータです。

以下のパラメータを使用することが出来ます。

- -h [--help] - コマンドラインパラメータのヘルプを表示します。
- -v [--version] - 現在のバージョンを表示します。
- -l [--level] arg - ログの詳細レベルの指定です。
- --syslogfacility arg - syslogのファシリティを指定します。
- -i [--ipc-level] arg - IPCログの詳細レベルを指定します。
- --log-filename arg - ログファイル名の指定です。
- -a [--agent] arg - lookupの追加設定を受け取る**Agent**へのパスを指定します。
- -t [--timeout] arg - **Agent**から設定を受け取るタイムアウトの指定です。
- -q [--query] arg - 検索される値を持ったクエリのストリングです。"-"が指定された場合、標準入力を使用する必要があります。
- -e [--exist] - lookup内にエレメントがあるかどうかのみがチェックされ、その値は受け取りません。

例:

```
$ ./drweb-lookup -q q -e e,w
q NOT FOUND

$ ./drweb-lookup -q q -e q,q
FOUND q

$ ./drweb-lookup -q test@drweb.com -e
'ldap:///-displayName-sub-(mail=$s)'
FOUND test@drweb.com

$ ./drweb-lookup -q test@drweb.com
'ldap:///-displayName-sub-(mail=$s)'notify.
```

```
virus=block, notify.virus=allow(rcpt), drweb/
ProcessingErrors = pass
```

```
$ ./drweb-lookup -q test@drweb.com "odbc:
select rules from maild where a='\$s'" scan =
all:-drweb
```

統計情報

Dr.Web MailDの動作中に一般統計、およびブロックしたメッセージに関する統計の2つのタイプの統計情報を収集することが出来ます。

一般統計情報には**Dr.Web**ソフトウェアの一般的動作に関する情報（検査されたメッセージの数とサイズ、スパムメッセージの数など）が含まれています。ブロックしたメッセージに関する統計情報には、ブロックした特定のメッセージおよび悪意のあるその内容が含まれています。

全ての統計情報は内部データベースに保存されます。一般統計情報は内部キャッシュに収集され、5分ごとにDBに保存されます。`drweb-maild`モジュールに障害が発生した場合、統計情報の一部が失われる場合があります。ブロックしたメッセージに関する統計情報は直接DBに保存され、必要に応じてエクスポートすることが出来ます。コントロールソケットの特別なコマンドを使用して統計情報に関する詳細を受信することが出来ます。

[Stat] セクションの**Detail**パラメータ、および各クライアントに対するルール内で指定する**StatDetail**パラメータ経由で設定することが出来るログの詳細レベルがあります。

- `Stat off` は統計情報の収集を無効にし、**Dr.Web for UNIX mail servers**の動作性能を向上させます。その結果、統計情報のエクスポートおよびレポートの送信は行いません。
- `Stat low` はソフトウェア全体の動作に関する統計情報の収集、クライアントの動作に関する統計情報の収集を有効にします。その結果、統計情報をエクスポート、およびレポートを送信することが出来ます。
- `Stat medium` は、設定内でこの機能が無効にされていないグループに関する統計情報の収集を可能にします。グループ統計情報へのアクセスはコントロールソケット経由かウェブインターフェース経由で行うことが出来ます。

- `Stat high` は、設定内でこの機能が無効にされていない内部データベース内にリストアップされた全てのユーザに関する統計情報の収集を可能にします。ユーザ統計情報へのアクセスはコントロールソケット経由かウェブインターフェース経由で行うことが出来ます。

統計情報のエクスポート

統計情報のエクスポートは**Agent**経由のみではなく、**Dr.Web MailD**を使用してストレージタイプ経由でも実行することが出来ます。これら2つのオプションは同時に有効にすることが可能です。

Agent経由での統計情報のエクスポートはデフォルトでは無効になっており、全てのクライアントに関する一般統計情報にのみ使用することが出来るという点に注意してください。ストレージタイプ経由でのエクスポートは各クライアントごと、およびスーパー管理者に対して個別に調整する必要があります。

前者の場合、統計情報は全て**Agent**に送られ、そこから**Dr.Web**統計サーバ(**Agent**設定ファイル`%etc_dir/agent.conf`の`[StandaloneMode]`セクション内**StatisticServerHost**、**StatisticServerPort**、**UUID**パラメータ)か集中管理サーバ(対応する設定は**Agent**設定ファイル`%etc_dir/agent.conf`の`[EnterpriseMode]`セクション内にあります)に送られます。

後者の場合、統計情報は**Dr.Web MailD**を使用してストレージタイプのオブジェクトに送られます。ストレージシンタックスは、プレフィックスの違いと"`$s`"記号が使われないという点を除いてlookupのものと同じです。以下のプレフィックスを使用することが出来ます。

- `odbc` – シンタックスはLDAPへのリクエストと同じです。

  保存する値はSQLリクエスト内で`name<type>`書式で指定することが出来ます。

  - `name` - 保存するオブジェクトの名前です(各パラメータごとにそれぞれの使用可能な名前のリストが使用されます)
  - `type` - データベースに記録を保存する際に使用されるパラメータの種類です。各オブジェクトごとにそのデフォルトタイプが使用され、変更することは推奨できません。

  デフォルトタイプ:

  - varchar_long - ODBC内のSQL_LONGVARCHARと同じです。
  - timestamp - ODBC内のTIMESTAMP_STRUCTと同じです。
  - int - 32ビットのデジタル整数。
  - char(length) - 0で終わるストリング。
- oracle – シンタックスはODBCへのリクエストと同じです。
- postgresmysql、sqlite、firebird – char(length)タイプをサポートしていない、およびvarchar_longタイプはラインデータに使用しなくてはならないという違いを除いて、シンタックスはODBCへのリクエストと同じです。

例:

ExportStatStorage = "odbc:insert into plugin_stat values(:plugin_name<varchar_long>,:size<int>,:num<int>)"

この要求内ではカンマが用いられているので引用符が必要であるという点に注意してください。

全てのクライアントに対して、storageタイプを持つ統計情報のエクスポートを有効にするには、まず最初に[Stat] セクション内の**ExportStat**パラメータ値にYesを設定し、[Stat]セクション内で以下のパラメータのうち少なくとも1つの値を設定して統計情報エクスポートに対するコマンドを設定してください。

- **ExportBlockObjectsStorage** – ブロックしたメッセージに関する統計情報をエクスポートするオブジェクトのリスト
- **ExportStatStorage** – **Dr.Web for UNIX mail servers** によって処理された全てのメッセージに関する統計情報のエクスポート
- **ExportPluginStatStorage** – 各プラグインによって処理されたメッセージに関する統計情報のエクスポート

上記で指定したパラメータの詳細については[Stat] セクションをご覧ください。

統計情報のエクスポートを各クライアントごとに有効にするには、[Stat]セクション内のパラメータ設定と同様、ルール内で**ExportStat**、**ExportBlockObjectsStorage**、**ExportStatStorage**、**ExportPluginStatStorage**パラメータをそれぞれのクライアントに対して個別に設定してください。

例:

```
[Rule:client1]
...
ExportStat = yes
      ExportBlockObjectsStorage = "odbc:insert into client1_viruses values
       (:number<int>, :q_name<varchar_long>, :virus_name<varchar_long>, \
                        :virus_code<int>, :plugin_name<varchar_long>, :sender<varchar_long>,\
                 :client_ip<varchar_long>, :date<timestamp>)"
...
```

隔離

メールメッセージはプラグインまたはdrweb-maildモジュール自体からの要求に応じて隔離に移動され、/quarantine/path/def/name/ディレクトリ内に保存されます。nameは要求を行ったモジュールの名前です。

メッセージが隔離に置かれると、ファイルが2つ作成されます。1つはメッセージ本文（その名前は**FilenamesMode**または**FilenamesPrefix**パラメータ内の設定に応じて作成され、"_"は全て"."に置き換えられます）、もう1つはエンベロープ用のものです。

エンベロープは以下の書式で保存されます。

- int4_t – 送信者アドレスの長さ
- sN – 送信者アドレス
- int4_t – 受信者の数
- int4_t sN – 各受信者に対して。int4_tはネットワークバイトオーダー内の4バイト整数です。

MoveAllパラメータの値にYesが設定されている場合、**Dr.Web MailD**によっ

て処理された全てのメールが/path/def/backup/ディレクトリに保存されます。

メッセージ本文が隔離ディレクトリに保存されるだけでなく、メッセージ自体が内部データベースに登録され、メッセージエンベロープ、保存した時間、隔離に移動した理由などの情報がそこに保存されます。

隔離はコントロールソケット経由で効率的に管理することが出来ます。コンロトールソケットに対するコマンドを使用して隔離内のメッセージを送信、リダイレクト、削除、検索することが可能です。

隔離にメッセージを保存しておく時間の上限は**StoredTime**パラメータで設定することが出来ます。また、隔離のサイズの上限(**MaxSize**パラメータ)とその中にあるメッセージ数の上限(**MaxNumber**パラメータ)も指定することが出来ます。

一度に複数の制限を指定した場合、それら全てが同時に適用されます。**MaxSize**と**MaxNumber**の制限は新しいメッセージが隔離に保存される度に検査されます。**StoredTime**制限は定期的に検査され、その周期は**PulseTime**パラメータで指定されます。

drweb-qpユーティリティは古いメッセージを隔離から削除し、外部DBIデータベースに移します。Perlバージョン5.0以降で動作します。drweb-qpへのパスを**PathToDrwebQp**パラメータ内で指定する必要があります。drweb-qpの初期化は**PulseTime**パラメータによって実行されます。**PulseTime**パラメータに0が設定されている場合、**StoredTime**制限およびdrweb-qpユーティリティは使用されません。

DBIの使用

隔離メッセージはファイルシステム内だけでなく、DBIストレージに保存することも出来ます。この機能を使用するにはPerlバージョン5.0以降、インストールされたDBIとFile::Tempモジュール、設定済みのDBIストレージが必要です(データベースと動作するためのDBIモジュールの設定と調整についての詳細はDBIに関するドキュメントをご覧ください)。メッセージをデータベースに送るには、データベースがSQL-ASCII文字コードセットで作成されている必要があります。

DBIとのインタラクションはdrweb-qpユーティリティ経由でのみ可能で、そこへのパスは**PathToDrwebQp**パラメータで指定されます。

DBIを使用するには以下のことを実行してください。

- **MoveToDBI**パラメータの値にYesを設定し、それに合わせて**DBISettings**、**DBIUsername**、**DBIPassword**パラメータを調整してDBIストレージへのアクセスを有効にしてください。この3つのパラメータは**DBI->connect**に属するものです。シンタックスについての詳細は、全てのDBIモジュールに関するドキュメントに記載されています(man DBD::mysqlや man DBD::Pgなど)。
- 以下のSQLコマンドを設定してください。
  - **SQLInsertCommand** - メールメッセージをDBIストレージに加えます。
  - **SQLRemoveCommand** - メールメッセージをDBIストレージから削除します。隔離内のメッセージに対して保存期限が設定されている場合に使用します。
  - **SQLSelectCommand** - DBIストレージに保存されているメッセージへのアクセスを可能にします。隔離内のメッセージが検索される(例:制御メッセージ経由)際に使用します。

起こりうるエラー:

以下のようなエラーが発生した場合、

```
maild ERROR Error in system call for [/opt/drweb/drweb-qp --Level debug --SyslogFacility Daemon --BaseDir /var/drweb/ --ProcessMail 1 --MoveToDBI 0 --StoredTime 86400 --SQLInsertCommand "" --MDClient "def" >/dev/null 2>&1 &]
```

drweb-maild処理に使用出来るメモリの上限の増加を試行してください(例:ulimit -mコマンドなど)。

制御メールの使用

隔離へのアクセスは特別な制御メール経由でも可能です。Subjectフィールド内のそれらのメールにはdrweb-maildによって実行されるコマンドが含まれています。メールはDr.Web MailD設定ファイル内[Notifier]セクションの**FilterMail**パラメータ内で、またはこのメールに対するローカルルール内で指定されたアドレスに送信される必要があります。制御メールに対するACLのセット

アップはDr.Web MailD設定ファイル内[Maild]セクションの**OnlyTrustedControlMails**パラメータのセットアップ値によって実行されます。

制御メールはDr.Web MailD設定ファイル内[Quarantine]セクションの**AccessByEmail**パラメータにYesが設定されている場合に有効となります。

隔離からメールを受け取るには制御メールのSubjectフィールド内でq: relative_path_to_fileを指定してください。relative_path_to_fileは隔離内にあるファイルへの相対パスです(例:/def/drweb/F/00014F8F.DW_SHOT_PRODUCT.QqFpdH)。

隔離メッセージの要求は、その送信者、または受信者の内の1人が制御メールの送信者と同一である場合のみ可能です。

メッセージが隔離された際にDr.Web MailD通知サービスによって送信されるレポート内の該当するリンクをクリックすると、MUAによって自動的に制御メールを作成することができます。

drweb-qcontrolの使用

隔離の管理および隔離内の検索にはdrweb-qcontrolユーティリティを使用します。このユーティリティのインターフェースはDBIストレージ内、またはディスク上のファイル内どちらに保存されているメッセージにも使用することが出来ます。

使用可能なコマンドラインパラメータは以下のとおりです。

- -h [--help] - ヘルプを使用します。
- --version - プログラムのバージョンに関する情報を見ます。
- -v [--verbose] - 実行された全てのアクション、および受け取った結果に関する情報をコンソールに出力します。
- -l [--level] arg (=error) - スタートアッププロセスのロギングに対するログの詳細レベルです。可能な値はquiet、error、alert、info、debugです。
- --syslogfacility arg (=mail) - ロギングにsyslogdシステムユーティリティを使用した場合のログの種別です。可能な値はdaemon、mail、local0...local7です。

- -i [--ipc-level] arg (=error) – IPCログの詳細レベルです。可能な値はquiet、error、alert、info、debugです。
- --log-filename arg (=syslog) – ロギングがsyslogdシステムユーティリティによって実行された場合のログファイルの名前、またはsyslog値です。
- --sendmail arg (=/opt/drweb/drweb-inject) – drweb-inject ユーティリティへのパスです。
- -s [--socket] arg (=local:/var/drweb/ipc/.ctl) – **Dr.Web MailD**コントロールソケットへのパスです。
- --agent arg (=local:/var/drweb/ipc/.agent) – 設定の受け取りに**Dr.Web Control Agent**のアドレスを使用します。
- --timeout arg (=60) – **Dr.Web Control Agent**から設定情報を受け取る際の待ち受け最大時間です。

アクションを適用するメッセージのリストを入手するにはユニークな識別子、すなわち隔離内に保存されたファイルへの相対パスを使用します。識別子内では特別な記号("%"は0以上の任意の記号、"_"は1つの任意の記号です。)が用いられます。識別子を設定する際にはdef/を頭に指定してください。

例:

def/%00014F7F% -00014F7Fが付いた隔離されたメッセージ全てを選択します。

def/drweb/% - drwebプラグインによって隔離されたメッセージ全てを選択します。

選択される識別子のファイルは検索条件、またはコマンドラインから受け取ります。標準入力ストリームを使用することも出来ます(検索基準が指定されておらず、コマンドライン経由で設定された識別子が無い場合)。

可能なアクションは以下のとおりです。

- --view – ある特定の識別子を持ったメッセージを全て、PAGER環境変数内で指定されたプログラム経由で表示する指定です。PAGER変数内で値が指定されていない場合、catプログラムが使用されます。
- --send – ある特定の識別子を持ったメッセージを全て元の受信者に送信します。配信にはdrweb-injectユーティリティが用いられます。

- --redirect [list_of_rcpts] - ある特定の識別子を持ったメッセージを全てアドレスのリストに転送します。配信にはdrweb-injectユーティリティが用いられます。
- --remove - ある特定の識別子を持ったメッセージを全て隔離から削除します。
- --stat - ある特定の識別子を持ったメッセージに関する統計情報を出力します。

例:

```
drweb-qcontrol --stat def/%
1. def/backup/B/00014F8B.DW_SHOT_PRODUCT.U0dshM
   from: a@1; to: a@fff; time: 2008-08-14
12:10:57
2. def/drweb/F/00014F8F.DW_SHOT_PRODUCT.QqFpdH
   from: a@4; to: a@fff; time: 2008-08-14
13:00:50
3. def/backup/C/00014F8C.DW_SHOT_PRODUCT.A39xp7
   from: a@2; to: a@fff; time: 2008-08-14
13:00:50
4. def/backup/F/00014F8F.DW_SHOT_PRODUCT.tMi6W2
   from: a@4; to: a@fff; time: 2008-08-14
13:00:50
5. def/drweb/3/00014F93.DW_SHOT_PRODUCT.n9xPjU
   from: a@3; to: a@fff; time: 2008-08-14
13:30:49
6. def/backup/3/00014F93.DW_SHOT_PRODUCT.ewYFVA
   from: a@3; to: a@fff; time: 2008-08-14
13:30:49
7. def/backup/4/00014F94.DW_SHOT_PRODUCT.JQ3sLH
   from: a@3; to: a@fff; time: 2008-08-14
13:30:49
```

アクションは指定された順番で実行されます(1つのコマンド内で複数のアクションを指定することが可能です)。

例:

```
drweb-qcontrol --send --remove def/backup/F/00014F7F.DW_SHOT_PRODUCT.yv4ro9
```

このコマンドは`def/backup/F/00014F7F.DW_SHOT_PRODUCT.yv4ro9`識別子を持つメッセージを元の受信者に送信し、次にそのメッセージを隔離から削除します。

隔離されたメッセージをDBIストレージに保存するように**Dr.Web MailD**を設定してある場合、コマンドライン内で追加のSQLコマンドを指定する必要があります。

- `--sql-remove-command` - このファイル識別子を使用する隔離ディレクトリからメッセージを削除することが出来ます。

  例:

  ```
  --sql-remove-command "DELETE FROM mail_export WHERE filename LIKE ?"
  ```

`drweb-qcontrol`ユーティリティは、保存されたメッセージ内で検索を実行する為のシンプルなインターフェースも持っています。

使用可能な検索条件は以下のとおりです。

- `--search-from {address}` - エンベロープ内の送信者アドレスを検索します。
- `--search-to {address}` - エンベロープ内の受信者アドレスを検索します。
- `--search-headers {header_name[:value]}` - ヘッダを検索します。`header_name`は検索対象となるヘッダの名前です。`value`が指定されていない場合、ヘッダ名のみが使用されます。`value`が指定されている場合はそれがヘッダの記述内でサブストリングとして検索されます。ヘッダ名およびその値の大文字小文字は区別されません。
- `--search-inbody {list of strings}` - メッセージ本文内のサブストリングを検索します。メッセージ本文はシングルユニットとして扱われ、MIME-decodingは行いません。大文字小文字は区別されません。

特別な記号`*`、`^`、`$`を**`--search-headers`**および**`--search-inbody`**パラメータの引数として使用した場合、検索コマンドを正しく処理する為にバックスラッシュ(`\`)をそれらの前に置いてください。

例:

```
--search-inbody \* --stat
```

検索条件はそれぞれ個別にチェックされます。

例:

```
--search-to addr1 --search-to addr2
```

エンベロープに受信者アドレスaddr1またはaddr2を含むメッセージを検索します(論理和ORを使用して結合します)。

例:

```
--search-from from@drweb.com --search-to to@drweb.com -search-headers "Subject: [SPAM]" --search-inbody "spam"
```

from@drweb.comから送信された、to@drweb.comに送信された、Subject内に[SPAM]という語を含む、メッセージ本文にスパムという語を含む、の内いずれかに該当する、隔離内のメッセージ全てを検索します。

ファイルのリストを持つコマンドライン内で指定された検索条件がある場合、検索はそれらのファイル内でのみ実行されます。

例:

```
drweb-qcontrol --stat --search-from a@5 def/backup/%
```

a@5によって送信され、アーカイブされた全てのメッセージに関する情報をコンソールに出力します。

```
1. def/backup/5/00014F95.DW_SHOT_PRODUCT.1LXzg1 from: a@5; to: a@drweb.com time: 2008-8-14 15:1:46
```

隔離を新しいバージョンに移行

Dr.Web MailDのバージョン6.0以降から隔離の構造が変わりました。メッセージ本文は以前と変わらずファイルシステム内に保存されますが、メッセージエンベロープおよびサービス情報は内部データベースに保存されるようになりました。

%bin_dir/maild/scripts/ディレクトリにある quarantine_migration.plスクリプトは隔離を新しいバージョンに移行するためのものです。起動されると必要なデフォルト設定を全て検出し、新しいバージョンの隔離のへの移行を勧めます。移行は自動的に実行され、保存されていたデータの期間、処理されたまたはスキップされたメッセージの数、およびエラーの数を含んだレポートが出力されます。

対話式インターフェースによる管理

Dr.Web MailDの動作の際に対話式インターフェースを介してコマンドを実行することが可能です。対話はdrweb-maildモジュールのコントロールソケット経由で行われます(drweb-maild自体が動作していてコントロールソケットが有効になっていることが必要です)。

対話式インターフェースによる管理を実行するには以下の手順を実行してください。

1. **Dr.Web MailD**設定ファイルの[Maild]セクションにある**Control**パラメータにYesを設定します。
2. **Dr.Web MailD**設定ファイルの同じセクションにある**ControlAddress**パラメータで指定されたアドレスに接続し、対話モードでコマンドを入力してください。確立可能な対話式接続は1つだけなので注意してください。

対話は行ごとに実行され、ユーザがストリングをいくつか入力すると、それに対してdrweb-maildがストリングをいくつか出力します。そのため複数行のコマンドを使用することは出来ず、複雑なルールは1行ずつ入力する必要があります。

drweb-maildから出力される情報の終わりは空の行で示します。

複数の対話式接続を同時に確立することが出来ます。IPv4およびIPv6プロトコルのどちらもサポートしています。**Control**パラメータの値に関係なく、**Dr.Web MailD**は常に/directory_specified_as_a_value_of_BaseDir_parameter/ipc/.ctlの接続待ちソケットを開いています。

使用可能なコマンドは以下のとおりです。

- **help** [section|command] - 全てのセクションのコマンド一覧を出力します。このコマンドの後にセクション名を指定し、そのセクションの全てのコマンドに関する情報を受け取ることが出来ます。また、情報を得たいコマンドの名前を指定することも出来ます。**help all**コマンドを使用して全てのコマンドの一覧を見ることが可能です。
- **option** [regex] - drweb-maildおよびプラグインによって使用されるパラメータとその値の一覧を出力します。パラメータ名を**option**コマンドに対する正規表現として指定すると、それに一致するパラメータの一覧のみが出力されます。正規表現が指定されていない場合、全てのパラメータが出力されます。
- **db-state** - 内部データベースの状態を以下の書式で出力します。

  Number: NC/NM

  Size: SC/SM

  NCおよびNMはデータベース内の現在のメッセージ数と上限で、SCおよびSMはバイト単位での現在のデータベースサイズと上限です。NMまたはSMが0の場合、制限はありません。

- **queue-state** - 内部キューにあるメッセージの状態を出力します。メッセージの総数、およびそれぞれのメッセージに関する情報が出力されます。総数が大きい場合、drweb-maildの2番目のプールのスレッドが不足している可能性があります(**OutPoolOptions**パラメータで調整)。
- **send-stat** - 統計情報を強制的に送信/エクスポートします(**Dr.Web MailD**設定ファイルの[Stat]セクションにある**SendPeriod**パラメータによって設定されたタイムアウトに対するアクションと似ています)。このコマンドは**Dr.Web MailD**設定ファイルの[Stat]セクションにある**Send**パラメータがYesに設定されている場合に使用することが出来ます。
- **send-report** [period] - プラグインの動作に関するレポートメールを強制的に送信します(**Dr.Web MailD**設定ファイルの[Reports]セクションにある**SendTimes**パラメータによって設定されたタイムアウトに対するアクションと似ています)。このコマンドは**Dr.Web MailD**設定ファイルの[Stat]セクションにある**Send**パラメータがYesに設定されている場合に使用することが出来ます。periodはレポート対象の期間を定義し、設定されていない場合は24時間が対象となります。
- **backup** - 内部データベースのバックアップを作成します。
- **quarantine-pulse** - 隔離処理のためのdrweb-qpユーティリティを強制的に初期化します(**Dr.Web MailD**設定ファイルの[Quarantine]セクションにある**PulseTime**パラメータによって設定

されたタイムアウトに対するアクションと似ています)。

- **dump-cache-stat** - キャッシュされた統計情報を全てオペレーティングメモリから内部データベースに移します。
- **get** [(id1|-|id1-[id2]) [(plugin_name|-)]] - 内部データベースに保存されているメッセージに関する情報を出力します。idNは要求されたメッセージの数で、id1-id2のような場合はこの範囲のメッセージを、id1のように指定するとid1で始まる番号(番号は16進法で指定します)を持つ全てのメッセージをそれぞれ指定することが出来ます。plugin_nameはメッセージを隔離データベースに移動したプラグインの名前です。"-"はパラメータが指定されていないことを意味し、その場合データベースの全てのメッセージに関する情報が出力されます。

  例:

  get - drweb - drwebプラグインによって隔離されたメッセージに関する情報を出力します。

  get - outputs - データベースに保存された全てのメッセージに関する情報を出力します。
- **send** [(id1|-|id1-[id2]) [(plugin_name|-)] [force]] - メッセージをそのエンベロープの受信者宛てに送信します。コマンド**get**の出力で**send**=noとなっているメッセージのみ送信することが出来ます。パラメータの記述は**get**コマンドと同じです。新しいパラメータ**force**を指定すると**send**=yesのメッセージも送信することが可能です。
- **export** [(id1|-|id1-[id2]) [(plugin_name|-)] [(dir_name|-)] [env] - 指定したメッセージをデータベースから別々のファイルにエクスポートします。パラメータの記述は**get**コマンドと同じですが、以下の2つのパラメータを追加することも出来ます。
  - **dir_name** - ファイルを保存するディレクトリへのパスです。パスが指定されていない場合、**Dr.Web MailD**設定ファイルの[General]セクションにある**BaseDir**パラメータの値が使用されます。
  - **env** - この値が指定されている場合、エンベロープもファイルにエクスポートされます。1行目に送信者アドレスが、2行目に受信者アドレスが出力され、複数の場合はカンマで区切って列挙されます。

  メッセージの保存ファイル名は"識別子.eml"に、エンベロープ情報の保存ファイル名は"識別子.envelope"になります。

例:

```
export 00002D94 vaderetro /t env
Success export body to /t/00002D94.eml
and envelope to /t/00002D94.envelope
```

- **remove** [(id1|-|id1-[id2]) [(plugin_name|-)] - 指定されたメッセージをデータベースから削除します。パラメータの記述は**get**コマンドと同じです。

  例:

  ```
  remove 00002D93
  Success remove record 00002D93
  ```

- **send_and_remove** [(id1|-|id1-[id2]) [(plugin_name|-)] [force_send] [ignore_send_error] - 指定されたメッセージをデータベースから送信、削除します。**force_send**パラメータの値は**send**コマンドの**force**パラメータの値と同じです。メッセージが**send_and_remove**コマンドによって無事に送信された場合やメッセージの配信が必要でない場合(前に送信されている)、メッセージは削除されます。**ignore_send_error**パラメータが指定されている場合、配信がうまくいったかどうかに関わらずメッセージは削除されます。
- **notify** - 通知の作成をチェックします。コマンドはドキュメンテーションのあるディレクトリ内の`notify.*`ファイルに記載されています。
- **version** - 製品のバージョンを出力します。
- **stop** - 製品を停止します。
- **reload** - `drweb-maild`に`SIGHUP`シグナルを送信します。

ユーザ、グループ、エイリアスの管理

Rules内でクライアントごとに特定の設定をしたり、それらを柔軟に調整することが出来ます。また、複数のユーザをグループにまとめ、そのグループに対して設定をすることも可能です(グループ設定は該当するグループ内の全てのユーザに適用されます)。

ユーザの数が多い場合、ルール内でそれぞれに対して設定をするのは効率的ではありません。設定するルールが多ければ多いほどユーザに対する設定の検索が遅

くなるからです。検索の速度を速めメモリを効率的に使用するために、各ユーザに対するルールはローカルデータベースに保存することを推奨します。

ルールに加え、ユーザに関するその他の情報もいくつかデータベースに保存されます。特定のユーザに関する情報を見るにはコントロールソケットに**email-info**コマンドを送信してください。情報は以下の書式で出力されます。

```
[client-id1/]email1 A=active1 S=stat1
name: name1
aliases: alias1 alias2 ..
groups: group1 group2
rules:
1: rule11
2: rule12
...
 custom:
tag1: info1..
tag2: info2..
...
```

- client-id1 – ユーザが属するクライアントのIDです。
- A=active1 – このユーザがアクティブかどうかの指定です。アクティブでない場合、ユーザ設定を持つルールは全て無視されます。
- S=stat1 – このユーザに関する別々の統計情報を収集するかどうかの指定です。各ユーザごとに統計情報の収集を有効にするには、一般統計情報に対してhigh ログの詳細レベルを設定してください。
- name: name1 – ユーザ名です。
- aliases:, groups:, rules:, custom: – エイリアス、グループ、グループおよび個人の設定などに関する情報です。

ユーザはグループにまとめることが出来ます。グループはユーザと同じ設定（クライアントID、グループ名、アクティビティステータス、別々の統計情報を入手可能かどうか、グループメンバーのリスト、および追加のサービス情報）を持っています。特定のグループに関する情報を見るにはコントロールソケットに**groups-info**コマンドを送信してください。情報は以下の書式で出力されます。

```
[client-id1/]group1 A=active1 S=stat1
```

```
emails:
email1
email2
...
custom:
tag1: info1..
tag2: info2..
...
```

ユーザが複数のアドレスを持っている場合、それらを次の方法でまとめることが出来ます。1つのアドレスをプライマリメールアドレスにし、その他のアドレスをエイリアスとします。その結果それらのアドレスは全て1つのものとして扱われ、同じ設定が適用され、統合された統計情報が収集されます。

パラメータの値は以下のアルゴリズムで選択されます。

- ユーザに対するルール内でパラメータ値を検索します。
- ユーザのルール内にそのようなパラメータが無い（またはパラメータ値が指定されていない）場合、このユーザが属するグループに対するルール内で検索が行われます（一覧の最後にあるグループから最初のグループまで）。
- グループの設定内にそのようなパラメータが無い（またはパラメータ値が指定されていない）場合、設定ファイル内で指定されたクライアントのルールで検索されます。
- それでもパラメータが見つからない場合、設定ファイル内で指定されたグローバルルールで検索が実行されます。
- 設定ファイル内に無い場合はデフォルトのハードコードされた値が使用されます。

値は最初に見つかったものが適用されるため、ユーザに対するリスト内で指定するグループの順番は非常に重要です。

メッセージ内で複数の受信者が指定され、それらの受信者に対して同じパラメータの異なる値が見つかった場合、以下の2つの解決方法があります。

1. いくつかのパラメータに対して（[Rules]　セクションに記載）メッセージが複製され（各受信者に対してメッセージのコピーを作成）、異なるコピーに対してそれぞれ異なる設定を適用。
2. それに対してメッセージを複製出来ないようなパラメータを無視し、クライアントの設定を適用、またはグローバル設定かハードコードされたデフォルト値を使用。

設定をチェックする際にユーザルールとグループルールは結合され、1つのリストとして処理されるので注意してください(ユーザのルールが最初にきます)。そのため、それらのリストを処理する際にはリスト内の「ユーザ」部分の設定が「グループ」部分の設定と一致し、上記のアルゴリズムが実行されます。

ユーザ、グループ、およびエイリアスの管理はコントロールソケット経由、またはウェブインターフェース経由で行うことが出来ます。

ユーザ、グループ、エイリアスの管理には特別なコマンドを使用します。

- **client** – **Dr.Web for UNIX mail servers**の管理者です。空の識別子が割り当てられます。
- **email** – ユーザのメールアドレスです(RFC5322準拠)。山括弧(<>)や引用符('')で囲むことが出来ます。長さは1024バイト以下にしてください。
- **client-email** – 2つの値[client-id/]emailで、**Dr.Web MailD**ではclient-id は常に空です。
- **emails-list** – client-email の一覧で、空白で区切って列挙します。
- **group** – グループ名で、一重引用符で囲みます。対応するサブストリングに空白が含まれていない場合、引用符は省略できます。引用符を使用する場合、テキスト内にある一重引用符の前に追加の一重引用符を置く必要があります。グループ名の長さは1024バイト以下にしてください。
- **client-group** – 2つの値[client-id/]groupで、**Dr.Web MailD**ではclient-id は常に空です。
- **ext-client-group** = [client-id/]group | client-id/ - client-groupと同じです。
- **group-list** – client-group の一覧で、空白で区切って列挙します。
- **ext-group-list** – ext-client-group の一覧で、空白で区切って列挙します。
- **RULE** – **Dr.Web MailD**ルールの一覧にあるルールです。ストリングにカンマが含まれ、それらが引用符で囲まれていない場合、それぞれのカンマの前にバックスラッシュ\を1つ置く(可能な値が1つのパラメータ)かまたは複数\\\置く(可能な値が複数あるパラメータ)必要があります。

  例:

  true cont headersfilter/RejectCondition = FileName = \"\.e\\\,e\"\, FileName = \"\.

com\", headersfilter/RejectPartCondition = FileName = \"\.e\\\,e\"\, FileName = \"\.com\"

true cont vaderetro/action = discard\, quarantine

- **tag** – ユーザ、またはグループに関する情報の検索タグとして使用される任意の記号のストリング[a-zA-Z0-9_-]です。ウェブインターフェースに対するこのパラメータの値はwebに設定されています。
- **info** – 改行までのライン全体です。従って改行、ヌル文字を含むことが出来ません。
- **settings** – ユーザまたはグループに対するいくつかの設定で、parameter_name=valueのペアで指定できます。パラメータは空白で区切ります。以下のパラメータを使用することが出来ます。
  - A (active) - 0(アクティベートされていない)または1(アクティベートされている)のいずれかの値をとることが出来ます。オブジェクトがアクティベートされていない場合、そのオブジェクトと接続されている全てのルールは使用されません。デフォルトではどのオブジェクトもアクティブと見なされます(このパラメータ値が指定されていない場合)。
  - S (stat) - オブジェクトに対する統計情報の収集を設定します。0(アクティベートされていない)または1(アクティベートされている)のいずれかの値をとることが出来ます。このパラメータの無効化(0)は、統計情報収集のプロセスにのみ影響し、結果には影響しません(既に収集されている統計情報はそのままです)。デフォルトでは、統計情報の収集は無効です。
  - N (name) - ユーザの名前で(グループに対してはこのパラメータは無視されます)、グループの場合と同様に一重引用符で囲むことが出来ます。このパラメータが指定されていない場合、ユーザ名は空のままになります。長さは1000バイトまでです。

    例:

    S=1 A=0 N='Some user'

    S=0

あるclient-emailに対するグループの優先順位づけをそのまま維持する為に、それぞれのclient-emailに対してグループのセットは管理されますが、グループに対してclient-emailのセットは管理されないので注意してください。

コントロールソケットを操作する際には、*user*がシステムに入力される全てのメールアドレスです。アドレスのコントロールには以下のコマンドを使用します。

- **email-set** client-email [settings] - クライアントに対するemailアドレスの作成またはアップデートで、client-email内で設定されます。アドレスが無い場合は作成され、settings内に指定されていない設定があった場合、それらの設定にはデフォルト値が設定されます。
- **email-remove** client-email - クライアントに対するemailアドレスの削除で、client-email内で設定されます。ユーザは全てのグループからも削除されます。アドレスが存在しない場合や、エイリアスであった場合はエラーが出力されます。
- **email-rename** client-email email - 1つ目のパラメータで設定されたメインユーザアドレスを、2つ目のパラメータで設定されたアドレスに変更します。1つ目のパラメータ内にアドレスが存在しない、アドレスがエイリアスである、または新しいアドレスが既に存在する場合、エラーが出力されリネームは実行されません。
- **email-set-groups** client-email [list-of-groups] - client-emailアドレスを含むグループのリストを設定します。グループの順番は重要です（リストの最後にあるグループ設定の優先度が高くなります）。

  list-of-groupsが空の場合、client-emailアドレスに対するリスト内のグループが全て削除されます。list-of-groupsリスト内では複数のグループは空白で区切って列挙します。client-emailまたはあるグループがリスト内に存在しない場合、エラーが出力され、アクションは実行されません。リスト内に同じグループが2つ存在する場合もエラーが出力されます。client-emailがエイリアスの場合、元の受信者がアップデートされます。list-of-groupsリストにclient-idが指定されている場合、それがclient-emailアドレスのclient-idと一致する必要があります。一致しない場合はエラーが出力されます。list-of-groupsのエイリアス内でclient-idが指定されていない場合、client-emailのclient-idと同じ値が取られます。

- **email-get-groups** emails-list - emails-listリストにあるアドレス全てのグループリストを受け取ります。あるアドレスがリスト内に存在しない場合エラーが出力されますが、コマンドの処理は続行されます。client-emailがエイリアスの場合、元の受信者に対する情報が出力されます。

出力書式:

```
client-id/email1: group1 group2 group3 ...
client-id/email2: group21 group22 group23
...
```

グループ名に空白が含まれている場合、groupNを一重引用符で囲むことが出来ます。

- **email-get-rules** emails-list - emails-listリストのアドレス全てに対する設定、またはルールを受け取ります。あるアドレスがリスト内に存在しない場合エラーが出力されますが、コマンドの処理は続行されます。エイリアスが送信される場合は、元の受信者に対する設定が出力されます。エラーは存在しないアドレス全てに対して出力されます。

  出力書式:

```
[client-id1/]email1
1: rule1
2: rule2
...
[client-id2/]email2
1: rule21
2: rule22
...
```

- **email-insert-rule** client-email index RULE - emailアドレス、およびclient-email内のクライアントに対するシーケンス番号インデックスを持った新しいルールの挿入です。emailまたはクライアントが存在しない場合、エラーが出力されます。数字(index)は1から始まります。indexの値が、指定されたemailに対するルールの最大値よりも大きい場合、ルールのリストの最後に新しいルールRULEが追加されます。インデックスindexが命令によって新しいルールに割り当てられます。

  例: emailに対して既にルールが2つ指定されている場合、index(=10)を持った新しいルールを追加すると、リストの最後にindex(=3)を持ったルールとして追加されます。index ≤ 0の場合、およびRULEが空(ルールが指定されていないなど)の場合はエラーが出力されます。

  変更が完了すると、現在のグループに対するルールが**email-get-rules**の出力書式で出力されます。

- **email-remove-rule** client-email index - emailアドレスおよびclient-email内のクライアントに対する、シーケンス番号indexを持ったルールを削除します。数字(index)は1から始まります。client-emailが存在しない場合、エラーが出力されます。indexの値が、指定されたemailiに対するルールの最大値よりも大きい、またはindex ≤ 0の場合もエラーが出力されます。エイリアスが送信される場合、元のアドレスに対する設定がアップデートされます。

  変更が完了すると、ルールは**email-get-rules**に対する出力書式で出力されます。

- **email-get-custom** -tag emails-list - emails-list内の各ユーザと接続された、tagの付いた情報を受け取ります。あるアドレスがリスト内に存在しない場合エラーが出力されますが、コマンドの処理は続行されます。tagの付いた情報が存在しない場合、空のストリングが出力されます。情報は1つのアドレスにつき1行ずつです。tagの代わりに"-"記号が指定されている場合、全てのタグに関する情報が出力されます。

  <u>出力書式</u>:

  ```
  [client-id1/]email1
  tag: info..
  [client-id2/]email2
  tag2: info2..
  ```

- **email-set-custom** tag client-email [info] - client-emailのユーザに対するtagと接続されたinfoテキストの設定です。ユーザが見つからない場合、エラーが出力されます。infoが指定されていない場合、ユーザに関する全ての情報を持ったタグが削除されます。
- **email-info** emails-list - emails-listの全てのアドレスに関する完全な情報を受け取ります。あるアドレスがリスト内に存在しない場合エラーが出力されますが、コマンドの処理は続行されます。アドレスルールは全てのグループおよびアドレス設定に対してコンパイルされた表示で出力されます。エイリアスの場合、グループおよび設定に関する情報は元のアドレスのものになります。ルールの設定は最初にユーザ設定、次にグループの動作と逆の順番でグループ設定、という順番で出力されます。ルールをコンパイルする際にグループおよびユーザのアクティビティコントロールが考慮されます。

  <u>出力書式</u>:

  ```
  [client-id1/]email1 A=active1 S=stat1
  ```

```
name: name1
aliases: alias1 alias2 ..
groups: group1 group2
rules:
1: rule11
2: rule12
...
 custom:
tag1: info1..
tag2: info2..
...
[client-id2/]email2 A=active2 S=stat2
name: name2
aliases: alias12 alias22 .. | alias for email2
groups: group3
rules:
1: rule21
2: rule22
...
custom:
tag21: info21..
tag22: info22..
...
```

グループ名に空白が含まれている場合、groupNを一重引用符で囲むことが出来ます。

<u>エイリアスの出力書式</u>:

```
[client-id1/]email1
aliases: alias for email
```

- **email-search** [range:START/NUMBER] [email: part-of-email] [name:'part-of-name']

[ignore:alias|nonalias] – アドレスまたはアドレスの一部を検索します。START(0で始まる数字)から始めて、NUMBERの数のアドレスを出力します。STARTおよびNUMBERが指定されていない場合、見つかったアドレス全てが出力されます。STARTおよびNUMBERが負の場合、エラーが出力されます。STARTおよびNUMBERの値が見つかったアドレスの数を上回っていた場合、その値に制限はありません(従って、制限のないSTARTに対してはアドレスがリストの最初から出力され、制限のないNUMBERに対してはリスト内の全てのアドレスが出力されます)。

- part-of-email – 検索されるメールアドレスのサブストリングかエイリアスです。指定されていない場合、既知のアドレスおよびエイリアスが全て出力されます。出力書式は**email-info**の出力と同じです。part-of-email内のユーザのユニークなIDは省略せずに指定してください。
- part-of-name – ユーザ名のサブストリングです(名前に一重引用符'が含まれている場合、その前に別の'を置く必要があります。サブストリングに空白が無い場合、囲む引用符は省略できます)。指定されたサブストリングを名前に含むユーザのみが出力されます。
- ignore – 無視するレコードの種別を定義します。ーalias(通常のアドレス内を検索)、nonaliasー通常のアドレス(エイリアス内のみ検索)

emailとnameが同時に指定されている場合、どちらの制限も満たすようなユーザのみが出力されます。ユーザ名がエイリアスに対して保存されていないので、エイリアスとユーザ名のサブストリングを同時に検索に使用することはおかしなことです。

- **email-count** [range:START/NUMBER] [email:part-of-email] [name:'part-of-name'] [ignore:alias|nonalias] –プロセスは**email-search**と同じですが、見つかったアドレスの数が出力されます。

エイリアスの管理には以下のコマンドを使用します。

- **aliases-get** emails-list – emails-listリストの全てのアドレスに対するエイリアスの出力リストです。存在しないアドレスまたは他のエイリアスがemails-listに含まれていた場合エラーが出力されますが、コマンドの処理は続行されます。同じアドレスが2つ見つかった場合もエラーが出力されます。

  <u>出力書式</u>:

[client-id1/]email1: alias1 alias2 alias3 ...
[client-id2/]email2: alias21 alias22 alias23 ...

- **aliases-set** client-email [emails-list] - client-emailで設定された、emailおよびクライアントのアドレスに対してエイリアスのリストを設定します。client-emailが存在しないか、エイリアスだと思われる場合、エラーが出力されます。emails-listが指定されていない場合、client-emailにリンクされている全てのエイリアスが削除されます。少なくとも1つのアドレスを含んでいて、それが登録されているか、または異なるアドレスのエイリアスである場合エラーが出力され、コマンドの実行はキャンセルされます。emails-list内のアドレスに対してclient-idが指定されている場合、それがclient-emailアドレスのclient-idと一致する必要があります。一致しない場合はエラーが出力されます。client-idがエイリアス内のemails-listで指定されていない場合、client-email内で設定されたclient-idと同じ値が設定されます。

グループの管理には以下のコマンドを使用します。

- **groups-set** client-group [settings] - groupという名前を持つグループの作成またはアップデートで、クライアントに対してclient-group内で設定されます。グループが存在しない場合は作成されます。settings内に指定されていない設定があった場合、それらの設定にはデフォルト値が設定されます。
- **groups-remove** client-group - groupという名前を持つグループの削除で、クライアントに対してclient-group内で設定されます。セットされたグループが存在しない場合はエラーが出力されます。削除可能なグループ内の各ユーザに対して、そのユーザが含まれているグループがグループリストから削除されます。
- **groups-rename** client-group group - 1番目のパラメータで設定されたグループの名前を、2番目のパラメータで設定された名前にリネームします。指定されたグループが存在しない、または指定した名前が既に使われている場合エラーが出力され、アクションは実行されません。
- **groups-get-rules** [group-list] - group-listリスト内の全てのグループに対するルールまたは設定を受け取ります。group-list内のあるグループが存在しない場合エラーが出力されますが、コマンドの処理は続行されます。

出力書式:

```
[client-id1/]group1
1: rule1
2: rule2
...
[client-id2/]group2
1: rule21
2: rule22
...
```

- **groups-insert-rule** client-group index RULE - groupという名前を持つグループおよびクライアントに対するシーケンス番号indexを持つルールの前への新しいルールの挿入で、client-group内で設定されます。設定された名前のグループが存在しない場合、エラーが出力されます。数字(index)は1から始まります。indexの値が、指定されたグループに対するルールの最大値よりも大きい場合、ルールのリストの最後に新しいルールRULEが追加され、indexが割り当てられます。

  例:

  グループに対してルールが2つだけ設定されていた場合、index = 10の新しいルールを追加しようとすると、ルールはリストの最後にindex = 3で追加されます。

  index ≤ 0の場合、およびRULEが空(ルールが指定されていないなど)の場合はエラーが出力されます。変更が完了すると、このグループに対するルールが**groups-get-rules**の出力書式で出力されます。

- **groups-remove-rule** client-group index - client-group内で設定され、groupグループおよびclientに対するシーケンス番号indexを持ったルールを削除します。数字(index)は1から始まります。groupまたはClientが存在しない場合、エラーが出力されます。indexの値が、指定されたグループiに対するルールの最大値よりも大きい、またはindex ≤ 0が空(ルールが指定されていないなど)の場合はエラーが出力されます。

- **groups-info** [ext-group-list] - ext-group-listリスト内のグループを構成する全てのユーザ、およびアクティビティに関する情報とランダムな情報を出力します。ext-group-list内のあるグループが存在しない場合エラーが出力されますが、コマンドの処理は

続行されます。ext-group-listが指定されていない場合、全てのClientsに対して存在するグループ全てに関する情報が出力されます。クライアントIDのみの場合、情報は全てのグループに関して出力されます。アドレスリスト内のエイリアスは出力されません。

出力書式:

```
[client-id1/]group1 A=active1 S=stat1
emails:
email1
email2
...
custom:
tag1: info1..
tag2: info2..
...
[client-id2/]group2 A=active2 S=stat2
emails:
email21
email22
...
custom:
tag21: info21..
tag22: info22..
...
```

- **groups-count** [ext-group-list] - コマンドは**groups-info**と同様に実行されますが、見つかったグループの数のみ出力します。
- **groups-get-custom** -|tag group-list - group-list内の各グループと接続されたタグtagの付いた情報を受け取ります。group-list内のあるグループが存在しない場合、エラーが出力されますが、コマンドの処理は続行されます。tagの付いた情報が存在しない場合は空のストリングが出力されます。情報は1つのグループにつき1行ずつです。tagの代わりに"-"記号が指定されている場合、全てのタグに関する情報が出力されます。

出力書式:

```
[client-id1/]group1
tag: info..
[client-id2/]group2
tag2: info2..
```

- **groups-set-custom** tag client-group [info] – client-groupグループに対するtagタグに接続されたテキストinfoの設定です。グループが見つからない場合、エラーが出力されます。infoが設定されていない場合、リンクされた全ての情報を持つタグが削除されます。

コントロールソケット経由での隔離管理

コントロールソケット経由で隔離を使用するには以下のコマンドを使用します。

- **Client** – **Dr.Web for UNIX mail servers**の管理者。空のIDが割り当てられます。
- **id** – [Quarantine]セクション内の**Path**パラメータで設定されるディレクトリから相対的な、テキスト本文のあるファイルへのパスです。 例えば[Quarantine]セクション内の**Path**パラメータが/var/drweb/infected(デフォルト値)の場合、ID def/drweb/E/00020EBE.maild.xeAX4uは、本文がファイル/var/drweb/infected/def/drweb/E/00020EBE.maild.xeAX4u内に置かれているメッセージにリンクします。
  - def – "def"という語です。
  - drweb – メッセージをブロックしたプラグインの名前です。メッセージがdrweb-maildコンポーネントによってブロックされた場合、値はmaildに設定されます。メッセージがアーカイブに移された場合、値はbackupに設定されます。
- **id-like** – **id**と同じですが、次の特別な記号を使用することが出来ます。"%"は0以上の任意の記号で、"_"は1つの任意の記号です。

  例:

  def/%00014F7F% – 00014F7Fが付いた隔離されたメッセージ全てです。

  def/drweb/% – drwebプラグインによって隔離されたメッセージ全てを選択します。

メッセージ本文はデコードされた形（UTF8暗号化で）でデータベースに保存され、タブ以外の全ての制御文字（ASCII　0..21と127）は空白に置き換えられます。

各コマンドの実行結果は最後に空のストリングを付けて出力されます。

隔離の管理には以下のコマンドを使用します。

- **quarantine-search** [range:START/NUMBER] [sort:SORT_TYPE] [sender:EMAIL_SUBSTR] [rcpt:EMAIL_SUBSTR]* [period:DATE1[/DATE2]] [size:SIZE] [subject:'SUBJECT_SUBSTR'] [id:id-like] [order:ascent|descent] – 指定した条件で隔離内のメッセージを検索します。メッセージはSTART（0で始まる数字）から始まり、NUMBERの数だけ出力されます。STARTおよびNUMBERが指定されていない場合、その他の条件を満たす、見つかったメッセージが全て出力されます。NUMBER 0値は全てのエレメントの出力を意味します。

  以下は使用されているパラメータの説明です。

  - SORT_TYPE – ソートの種類です。使用可能な値は以下のとおりです。
    - ✓ date（デフォルト） – メッセージが隔離に移された日付でソートします。
    - ✓ size – メッセージサイズでソートします。
    - ✓ sender – 送信者アドレスでソートします。
    - ✓ subject – メッセージの件名でソートします。
  - EMAIL_SUBSTR – rcptまたはsenderフィールド内で検索するサブストリング。
  - period – メッセージが出力される期間です。指定されていない場合、メッセージは全期間に渡って出力されます。
  - DATE1 – 指定された時間（その時間を含む）の後に隔離へ移されたメッセージを出力します。
  - DATE2 – 指定された時間（その時間を含む）よりも前に隔離へ移されたメッセージを出力します。DATEの書式

はISO書式YYYYMMDDTHHMMSS(Tは時間と日付の区切りです)を使用します。時間は動作中の**Dr.Web MailD**を持つホストに対するローカルタイムとして設定、出力されます。

- SIZE - 指定された値(バイト)を超えるサイズのメッセージのみを返します。値が0に設定されている場合、サイズの制限はありません。
- SUBJECT_SUBSTR – メッセージの元の件名(コンポーネントによってメッセージが変更される前の)内にある、引用符で囲まれたサブストリングです。サブストリングに空白が含まれていない場合、引用符は省略することが出来ます。名前に引用符が含まれている場合、名前の前に' 記号をもう1つ置く必要があります。
- order – 結果を返す順番です(ascent - 昇順、descent 降順)。デフォルト値はdescentです。

パラメータの中に間違いがあると、**quarantine-search**コマンドは実行されません。受信者のテンプレートが複数指定されている場合、全てのテンプレートを含んだメッセージのみが出力されます(論理演算ANDと同様)。rcpt以外の全てのパラメータでは、コマンドラインの最後に指定された値が使用され、rcptでは新しい値が入力される度に受信者の数が増えます。

出力書式:

```
N. id SENDER RCTPS
SIZE DATE SUBJECT
BLOCK_OBJECT1
BLOCK_OBJECT2
...
```

- N – 見つかったメッセージのシーケンス番号
- SENDER – エンベロープ内のメッセージ送信者
- RCPTS – エンベロープ内のメッセージ受信者
- SUBJECT – メッセージの件名(UTF8出力)
- SIZE – バイトでのメッセージサイズ
- DATE – メッセージを隔離に移動した日付
- BLOCK_OBJECTN – このメッセージをブロックしたオブジェクト

例:

```
# quarantine-search
```

最も新しいものから始めて、隔離内の全てのメッセージのリストを返します。

```
# quarantine-search range:45/15 id:def/drweb/%
```

隔離内にある、drwebプラグインに対する最初の45個を抜かした最新15メッセージを返します。

```
# quarantine-search rcpt:vasya@pupkin.com
```

隔離内にある、受信者がvasya@pupkin.comである全てのメッセージを最新のものから返します。

```
# quarantine-search sort:size sender:period:20090101T100001/20090102T100000 size:5242880 id:def/vaderetro/%
```

2009年1月1日の午前10時から翌日の午前10時にvaderetroプラグインに対して受信し、サイズが5メガバイトよりも大きいメッセージを降順で出力します。

出力例:

```
quarantine-search
0. def/drweb/9/00021569.maild.BMED3y <ai@drweb.com> <alias_ai81@drweb.com>
829 20091117T102126 [EICAR] test2
EICAR Test File (NOT a Virus!)
1. def/backup/9/00021569.maild.3PLb8e <ai@drweb.com> <alias_ai81@drweb.com>
828 20091117T100213 [EICAR] test
```

- **quarantine-count** [range:START/NUMBER] [sort:SORT_TYPE] [sender:EMAIL_SUBSTR] [rcpt:EMAIL_SUBSTR]* [period:DATE1[/DATE2]] [size:SIZE] [subject:'SUBJECT_SUBSTR'] [id:id-like] [order:ascent|descent] - **quarantine-search** コマンドと同様ですが、メッセージではなく見つかったメッセージの総数が出力されます。

  出力例:

  ```
  quarantine-count
  ```

234

- **quarantine-remove** id-like [part-of-email1, part-of-email2, ..] – 指定された受信者(サブストリングとして検索された)part-of-email1, part-of-email2, ... を、IDがid-likeと一致する(指定された受信者は全てエンベロープ内に存在する必要があります)メッセージのエンベロープから削除します。メッセージに受信者が残っていないか、削除するリストが指定されていない場合、メッセージが完全に隔離から削除されます。

  例:

  ```
  # quarantine-remove %/backup/% drweb.com>
  ```

  drweb.comで終わるアドレスを持つ全てのメッセージを、隔離およびバックアップから削除します。

  ```
  # quarantine-remove % <foo@dwreb.com> <foo2@dwreb.com>
  ```

  受信者が同時にfoo@dwreb.comおよびfoo2@dwreb.comである全てのメッセージを、隔離およびバックアップから削除します。

  ```
  # quarantine-remove client2/drweb/E/00020EFE.maild.Q5FRbO
  ```

  指定されたIDを持つメッセージが削除されます。

- **quarantine-limits** – 隔離に設定された現在の制限を出力します。

  出力書式:

  ```
  client-id1: NUMBER/MAX-NUMBER SIZE/MAX-SIZE
  ...
  total: NUMBER/MAX-NUMBER SIZE/MAX-SIZE
  ```

  where:

  - NUMBER/MAX-NUMBER – メッセージの現在の数、および数の上限です。上限が設定されていない場合0が出力されます。
  - SIZE/MAX-SIZE – 隔離内のメッセージの現在のサイズ、およびサイズの上限です(バイト)。上限が設定されていない場合0が出力されます。
  - client-id1 – クライアントのIDで、それに対して情報を出力します。

  - total – 全てのデータベースに関する情報です。

- **quarantine-send** id-like [email1 email2 ...] – 指定された受信者(email1 email2 ...)に隔離からメッセージを送信します。受信者が指定されていない場合、メッセージはエンベロープの元の受信者に送信されます。出力書式は全てのメッセージの送信結果によって定義されます。
  RES in sending (to RCPTS_LIST): id

  - RCPTS_LIST – メッセージ受信者の実際のリスト
  - RES – 送信結果に応じてOKまたはERROR
  - id – メッセージ本文のファイルパス

  出力書式:
  OK in sending (to <ai@drweb.com> <as@sd>): def/backup/6/00004DD6.maild.VQ80Ro

  OK in sending (to <ai@drweb.com> <as@sd>): def/backup/6/00004DC6.maild.PWfqe3

- **quarantine-add** id from rcpt1 rcpt2... – 指定されたファイルを隔離に加えます。fromはメッセージ送信者で、rcptNは受信者です。アドレスは山括弧<>で囲むことが出来ます。指定されたidを持つファイルが存在しない場合、エラーが出力されます。

コントロールソケット経由で統計情報を受け取る

クライアント、ユーザ、およびグループに対する**Dr.Web for UNIX mail servers**の動作に関する統計情報は、コントロールソケットのコマンドインターフェース経由で受け取ることが出来ます。以下のコマンドを使用します。

- **client** – **Dr.Web for UNIX mail servers**の管理者です。空のIDが割り当てられます。
- **email** – ユーザのメールアドレスです(RFC5322に準拠)。山括弧(<>)または引用符('')で囲むことが出来ます。
- **client-email** – [client-id/]emailで、client-idはclientのユニークなIDです。clientに対してはデフォルトで空にすることが可能です。client-idは大文字小文字の区別はしません。
- **group** – 引用符('')で囲んだグループ名です。サブストリングに空白が含まれていない場合、引用符は省略することが出来ます。引用符を使用する場合は名前の前にもう1つ ' を置いてください。

- **client-group** = [client-id/]group - client-id はclientのユニークなIDです。 クライアントに対してはデフォルトで空にすることが可能です。client-idは大文字小文字の区別はしません。

統計情報を扱う際には、検査されたメッセージに関する一般統計情報は、クライアントに対するものとユーザーおよびグループに対するものとで収集される方法が異なるという点に注意してください。

- クライアントに関する統計情報は内部キャッシュに収集され、5分ごとに内部データベースにフラッシュされます（保存はdump-cache-statコマンドを実行、HUPシグナルを受信、**Dr.Web for UNIX mail servers**をシャットダウンした際に行われます）。
- ユーザおよびグループに関する統計情報は内部データベースの対応するレコードに直接保存されます。情報を保存しようとした際に、レコードがデータベース内に5分以上あった場合、新しいレコードが作成され以降の変更はそこに保存されます。

コマンドが内部データベースと動作すると、ユーザおよびグループに関する最後のレコードにはその作成時から現在までの統計情報が全て含まれます。クライアントに関する統計情報は適宜保存されるので、一般統計情報の表示に5分までの遅れが生じることがあります。

統計情報のコマンドには複数の一般パラメータがあります。

- **period** = period:DATE1[/DATE2] – 選択された期間の統計情報を出力します。
  where:
  - DATE1 – 統計情報を出力する期間の下限です。出力書式および時間書式は下記をご覧ください。
  - DATE2 – 統計情報を出力する期間の上限です。パラメータが設定されていない場合、現在の時間になります。書式は下記をご覧ください。

  期間が設定されていない場合、全ての統計情報が出力されます。
- **ignore** = ignore:total|block – 出力する統計情報のフィルタリングです。
- **total** – 検査されたメッセージに関する一般統計情報を出力しません。
- **block** – ブロックされたメッセージに関する一般統計情報を出力しません。このパラメータが設定されていない場合、全ての種類の統計情報が出力されます。

- **plugin** = plugin:name - 指定されたプラグインに関する情報を出力します。nameは統計情報を出力するプラグインの名前です。**plugin**が設定されていない場合、情報は全てのプラグインに関して出力されます。存在しないプラグインが設定された場合、エラーが出力されコマンドはキャンセルされます。*が指定された場合、一般統計情報が出力されます。

同じようなパラメータが複数指定された場合、最後に指定されたパラメータに関する統計が出力されます。

使用可能なコマンドは以下のとおりです。

- **stat-client** client-id|*|- [period] [ignore] [plugin] - 設定されたクライアントclient-idに関する統計情報の作成です。client-idで指定されたクライアントが存在しない場合、エラーが出力されコマンドの実行はキャンセルされます。client-idの代わりに"*"が指定された場合、全てのクライアントに関する統計情報が出力され、"-"が指定された場合(引用符無しで)は、デフォルトのクライアントに関する統計情報が出力されます(空のIDで)。オプションのパラメータはランダムな順番で指定することが出来ます。
- **stat-group** client-group [period] [ignore] [plugin] - client-groupのグループに関する統計情報の作成です。グループが存在しない場合はエラーが出力され、コマンドの実行はキャンセルされます。オプションのパラメータはランダムな順番で指定することが出来ます。
- **stat-email** client-email [period] [ignore] [plugin] - 現在のユーザclient-emailに関する統計情報の作成です。指定されたアドレスに関する統計情報が存在しない場合(例えば、アドレスが正しくないなど)、空のストリングが出力されます。アドレスがエイリアスの場合、メインアドレスに関する統計情報が出力されます。オプションのパラメータはランダムな順番で指定することが出来ます。
- **stat-remove-client** client-id|*|- [period] [ignore] [plugin] - 設定されたクライアントclient-idに関する統計情報を削除します。client-idで指定されたクライアントが存在しない場合、エラーが出力されコマンドの実行はキャンセルされます。client-idの代わりに"*"が指定された場合、全てのクライアントに関する統計情報が出力され、"-"が指定された場合(引用符無しで)は、デフォルトのクライアントに関する統計情報が出力されます(空のIDで)。結果として、削除されたレコードの数が表示されます。
- **stat-remove-group** client-group [period]

[ignore] [plugin] - client-groupのグループに関する統計情報を削除します。結果として、削除されたレコードの数が表示されます。

- **stat-remove-email** client-email [period] [ignore] [plugin] - 特定のユーザclient-emailに関する統計情報を削除します。結果として、削除されたレコードの数が表示されます。
- **remove-old-stat** [time] - 全てのクライアント、グループおよびユーザに関する全ての統計情報(time(タイプ (time))内で設定された時間よりも古い場合)を削除します。値が設定されていない場合、24時間よりも古い統計情報が全て削除されます。
- **dump-cache-stat** - クライアントに関する一般統計情報の内部キャッシュを内部データベースにフラッシュします。この機能は製品自体によって適宜呼び出され、また、HUPシグナルの受信やシャットダウンによっても呼び出されます。

各プラグインモジュールの動作に関する統計情報は2つのパートから成る書式で出力されます。

1. 検査されたメッセージに関する一般統計情報

   PLUGIN DATE [P] [R] [D] [T] [Q] [RE] [N] [C] [S] [U] [F] [I] [DI] [DM] [DSV] [DC] [DD] [DSK] [DAR] [DE] [DTA] [DTD] [DTJ] [DTR] [DTH] [PS] [RS] [DS][TS] [QS] [RES] [NS] [CS] [SS] [US] [FS] [IS] [WT] ...
2. ブロックされたメッセージに関する統計情報

   PLUGIN DATE FROM|- IP|- 'BLOCK1' TYPE1 'BLOCK2' TYPE2 ...

- PLUGIN - 統計情報の出力を指定するプラグイン名です。*が指定されると、全体の一般統計情報が出力されます(プラグイン経由で出力設定されていないメッセージも含まれます)。
- DATE - レコードが作成された時間です。検査されたメッセージに関する一般統計情報では、統計情報を保存する期間の始めを意味します。期間の終わりは新しいレコードの始めになります。続くレコードが存在しない場合、期間の始めに5分が追加されます。書式はISO書式YYYYMMDDTHHMMSS(Tは時間と日付の区切りです)を使用します。時間は**Dr.Web for UNIX mail servers**を持つホストに対するローカルタイムとして設定、出力されます。

WTまでの(WTを含む)下記の値が以下の書式で出力されます。

NAME=VAL – **NAME**は値の名前(P, PS...)で、VALは数値です。値のいくつかが指定されていない場合、それらは0になります。

可能な値:

- P/PS – アクションpassが実行されたメッセージの数/サイズ(バイト)
- R/RS – アクションrejectが実行されたメッセージの数/サイズ(バイト)
- D/DS – アクションdiscardが実行されたメッセージの数/サイズ(バイト)
- T/TS – アクションtempfailが実行されたメッセージの数/サイズ(バイト)
- Q/QS – アクションtempfailが実行されたメッセージの数/サイズ(バイト)
- RE/RES – アクションredirectが実行されたメッセージの数/サイズ(バイト)
- N/NS – アクションnotifiyが実行されたメッセージの数/サイズ(バイト)
- C/CS – クリーンなメッセージの数/サイズ(バイト)
- S/SS – スパムと判断されたメッセージの数/サイズ(バイト)
- U/US – 疑いなくスパムと判断されたメッセージの数/サイズ(バイト)
- F/FS – フィルタによってブロックされたメッセージの数/サイズ(バイト)
- I/IS – ウイルスを含んだメッセージの数/サイズ(バイト)
- DI – 感染した添付ファイルの数
- DM – 既知のウイルスの亜種に感染した添付ファイルの数
- DSV – 未知のウイルスに感染した添付ファイルの数
- DC – 修復された添付ファイルの数
- DD – 削除された添付ファイルの数
- DSK – 様々な理由により、アンチウイルス検査無しで通過した添付ファイルの数
- DAR – アーカイブの制限が原因で、アンチウイルス検査無しで通過した添付ファイルの数
- DE – 処理中のエラーを持った添付ファイルの数

- DTA – アドウェアを含んだ添付ファイルの数
- DTD – ダイアラーを含んだ添付ファイルの数
- DTJ – ジョークプログラムを含んだ添付ファイルの数
- DTR – リスクウェアを含んだ添付ファイルの数
- DTH – ハッキングプログラムを含んだ添付ファイルの数
- WT – プラグインがメッセージの処理にかけた時間(ミリ秒)

ブロックされたメッセージに対するリストには以下のフィールドが含まれています。

- BLOCK[12..] – ブロックしたオブジェクトの名前(ウイルスなど)です。グループの場合と同様、一重引用符で囲みます(上記参照)。
- TYPE[12..] – ブロックしたオブジェクトの種類です。名前は**NAME**のものが使用されます(上記参照)。可能な値はDI-DTH、F、S、Uです。
- FROM – エンベロープのメッセージ送信者です。
- IP – メッセージ送信者のIPアドレスです。

drweb-inject ユーティリティの使用

ローカル**Sender**コンポーネント経由でメールを送受信するにはdrweb-injectユーティリティを使用します。このユーティリティはメッセージ本文を標準入力ストリーム経由で受け取り、成功時には0を、失敗時にはnon-zeroをレスポンスコードとして返します。

使用可能なコマンドラインパラメータは以下のとおりです。

- --help - コマンドラインパラメータ上にヘルプを表示します。
- --version - 現在のバージョンを表示します。
- --agent arg - 設定を受け取るための**Agent**へのパスです(またはデフォルトパラメータに対する空のストリングで、その場合**Agent**への要求はされません)。
- --timeout arg - **Agent**から設定を受け取るタイムアウトの指定です。
- --id arg - メッセージが配信される**Sender**コンポーネントのユニークなIDです。
- -f [--env-from] arg - エンベロープのFromフィールドに送信者のアドレスを挿入します。

- -F [--from] arg - 配信されたメッセージにFromフィールドが無かった場合、この引数からのFull Nameが使用されます。
- -i [--ignore-dot] - "."記号を含んだストリングを、メッセージ本文入力の完了シグナルとして解釈しません。
- -t [--extract-recipients] - "**To:**"メッセージヘッダからの全ての受信者をエンベロープに追加します。

drweb-injectユーティリティがデフォルトディレクトリ内に無い場合、そこへのパスはdrweb-qcontrolの起動時に**--**sendmailコマンドラインパラメータによって指定することが出来ます。**-v**を使用して詳細な情報を受け取ることも可能です。

送信者が指定されていない場合、プログラムの動作に権限を使用しているユーザの名前が使われます。そのような名前が見つからない場合、プログラムの動作はエラーコードnon-zeroを出して中断されます。

複数のReceiver/Senderコンポーネントの同時使用

複数の**Receiver**および／または**Sender**コンポーネントを同時にdrweb-maildに接続することが可能です。

この機能は以下の目的で使用されます。

- 複数のMTAまたはSMTPプロキシとの同時インタラクションを可能にする為
- 各**Receiver**／**Sender**コンポーネントに対して別々の設定を可能にする為（それにより、モニターされるインターフェースに対して異なる設定の使用が可能になります）
- 1つのMTAから別のMTAへのメッセージのリダイレクトを可能にする為（ルーティングの為）

このような同時使用を可能にする方法は以下のとおりです。

1. **Receiver**グループおよび**Sender**グループの各コンポーネントにユニークなIDを割り当てます（**Receiver**のいくつかのIDは**Sender**のいくつかのIDと同じ場合がありますが、同じIDを持つ**Receiver**のペアは存在しません）。
2. 設定情報をどのように受信するか、それぞれのコンポーネントに知らせます。
3. **Receiver**によって送信された各メッセージにコンポーネントのユニークなIDをタグとして割り当てます。
4. メッセージを処理した後、drweb-maildは**Receiver**のIDと同じIDを

持つ利用可能な**Sender**を検索します。そのような**Sender**が見つからない場合、常に利用可能であるデフォルトの**Sender**(ユニークなIDが指定されていない)にメッセージを送信することが出来ます。

5. 利用可能な**Sender**のリストは起動時に作成され、`SIGHUP`シグナルを受信するとリフレッシュされます。
6. `drweb-notifier`によって作成されたメッセージのルーティングは**Dr.Web MailD**設定ファイル[`Notifier`]セクションの**`MsgIdMap`**パラメータによって管理されます。このパラメータによって、**Receiver**からのメッセージに対する**Sender**レポートをどこに送信するかを定義することが出来ます。

Receiver/**Sender**のユニークなIDは`--unique-id`コマンドラインパラメータ経由で設定されます。コンポーネントがこのパラメータで起動されると、`%var_dir/msgs/{in|out}`ディレクトリ内にメッセージキューのためのサブディレクトリをいくつか作成し、ディレクトリ内には**Sender**に対する特別なUNIXソケットが作成されます。

コンポーネントの2番目のコピー(例:`drweb-receiver`)が起動されると、追加的な調整を実行する必要があります。つまり、このコピーが設定情報をどのように受け取るかを指定する必要があります。

コンポーネントが設定情報を得るには2つの方法があります。

- `*.conf`ファイルの新しいコピーを作成する
- 現存する`*.conf`ファイルのコピーを変更する(こちらの方が簡単ですが、柔軟性は劣ります)

現存する*.confファイルを変更する方法は以下のとおりです。

- **Dr.Web MailD** `*.amc`ファイルに、コンポーネントの新しいコピーに関する情報を加えます。

  例:

  ```
  drweb-receiver2 General, Logging, /
  MailDesk/Clients, /_Rules, /Maild/
  ProtectedNetworks, /Maild/
  ProtectedDomains, /Maild/
  IncludeSubdomains, SASL, Receiver2
  ```

drweb-receiver2は**Dr.Web Agent**とのインタラクションに使用するコンポーネントの新しい名前で、Receiver2は設定ファイル内の対応するセクションの新しい名前です。

その他のパラメータはオリジナルコンポーネントの設定セクションからコピーする必要があります。*.amcファイルのシンタックスに関する詳細は、前出の**Dr.Web Agent**の章をご覧ください。

- コンポーネント設定のメインセクションを*.confファイルにコピーします。このセクションをリネームし（前のステージで設定した名前を指定してください）、2番目のコンポーネントの新しいセクション内にある他の設定全てを変更します。
- 新しい設定情報を受け取る為に**Dr.Web Agent**を起動または再起動してください。
- 以下のコマンドラインパラメータを指定して新しいコンポーネントを起動します。
  - --unique-id id - idはコンポーネントのユニークなIDです。
  - --component name - nameは**Dr.Web Agent**と連携するために新しいコンポーネントが使用する名前です（上の例ではdrweb-receiver2）。
  - --section - コンポーネントのメインセクションの新しい名前です（上の例ではReceiver2）。

例:

```
DEFAULT_BIN_PATH/drweb-receiver --unique-id id1
--component drweb-receiver2 --section Receiver2

DEFAULT_BIN_PATH/drweb-sender --unique-id id1
--component drweb-sender2 --section Sender2
```

*.confファイルの新しいコピーを作成するのはもっと難しくなりますが、設定ファイルのコンポーネントのメインセクションにあるパラメータだけでなく全てのパラメータを調整することが出来ます。

*.confファイルのコピーを作成する方法は以下のとおりです。

- *.confファイルのコピーを作成し、適宜パラメータをセットアップします(セクションのリネームは必要ありません)。
- 新しい*.amcファイルを作成し、新しいコンポーネントに関する情報のみを入れてください。前のステージで作成した新しい*.conf設定ファイルへのパスも指定する必要があります。
- 新しい設定情報を受け取る為に**Dr.Web Agent**を起動または再起動してください。
- 以下のコマンドラインパラメータを指定して新しいコンポーネントを起動します。
  - --unique-id id - idはコンポーネントのユニークなIDです。
  - --component name - nameは**Dr.Web Agent**と連携するために新しいコンポーネントが使用する名前です(上の例ではdrweb-receiver2)。

例:

```
DEFAULT_BIN_PATH/drweb-receiver --unique-id id2
--component drweb-receiver2
DEFAULT_BIN_PATH/drweb-sender --unique-id id2
--component drweb-sender2
```

どちらの方法でも、新しいコンポーネントを使用するために**Dr.Web Monitor**をセットアップすることが出来ます。そのためには**Dr.Web MailD**の*.mmcファイルに、対応するライン(新しいコンポーネントの起動に関する)を加えてください。*.mmcファイルのシンタックスに関する詳細は上記**Dr.Web Monitor**の章をご覧ください。

Unified Score

Unified Scoreは、各メッセージに割り当てられた合算されたスコアによってスパムを検出するテクノロジーです。メッセージスコアは符号付き整数で、大きければ大きいほどメッセージがスパムである可能性が高くなります。メッセージが正常であると判定されるデフォルトの閾値は99で、100-999の間のスコアはスパムと判定され、1000以上のスコアは疑いなくスパムと判定されます。

メッセージスコアはいくつかの方法で変更することが出来ます。

- **Action**タイプの変数内でオプションのscore (SCORE)アクションを使用することが出来ます。SCOREは整数で、現在のメッセージスコアに加えることが出来ます。
- Vaderetro アンチスパムプラグインがメッセージにスコアを割り当て、そのスコアがメッセージスコアの合計に加算されます(その後スパム閾値と比較されます)。
- add_scoreまたはset_score制限を使用してメッセージスコアを変更することも可能です(他の制限のパラメータにもこの操作が可能なものがあります)。
- Reputation IP Filterを使用して、現在のセッションからの全てのメッセージスコアを変更することが出来ます。

メッセージスコアは以下の方法で用いることが出来ます。

- Vaderetroプラグイン内で、スパム閾値と比較されます。
- ルールのコンディション内でもメッセージスコアを使用することが出来ます(スコアプレフィックス)。詳細については[Rules] セクションをご覧ください。
- **Modifier**プラグインパラメータのコンディション内でメッセージスコアを使用および変更することが可能です。詳細についてはDr.Web Modifier プラグインの章をご覧ください。
- メッセージスコアが**Dr.Web MailD**設定ファイル[MailD]セクションの**MaxScore**パラメータの値よりも大きい場合、**MaxScoreAction**パラメータの値として指定されたアクションがメッセージに適用されます。
- いくつかの制限内では現在のスコアに応じて異なるアクションをメッセージに適用することが出来ます。
- メッセージスコアの合計が[Receiver] セクションの**MaxSessionScore**パラメータの値よりも大きくなった場合、セッション全体がdrweb-receiver内でブロックされます。
- Reputation IP Filterのscore_filterを使用して、合計スコアが大きいアドレスをフィルタリングすることが出来ます。

Reputation IP Filter

Reputation IP Filterは、**Dr.Web for UNIX mail servers**に接続された各IPアドレスに関する統計情報の収集を可能にするテクノロジーで、収集されたデータに応じて、IPアドレスに対するアクションを実行します(例えば、そのIPを一時的にブロックなど)。このテクノロジーはスパマーの検出を可能にし、DHA攻撃も防ぎます。

Reputation IP Filterモジュールは**ReputationIPFilter**パラメータでフィルタが1つだけ指定されている場合、または**MaxConcurrentConnection**パラメータの値が0に設定されている場合に有効になります。

デフォルトでは**ReputationIPFilter**パラメータの値はscore_filterに設定され、IPフィルタは有効になり、IPアドレスからの全てのメッセージおよびセッションに割り当てられた平均スコアに応じて、それらのアドレスがフィルタリングされます。

IPアドレスに関する全ての情報はRAMメモリ内に置かれ、定期的にファイルに保存されます。情報はdrweb-receiverプロセスがSIGALRMシグナルを受信する度に(**StalledProcessingInterval**パラメータ設定に応じて自身でこのシグナルを作成します)、またはdrweb-receiver処理が停止した際にファイルに保存されます。ファイルはdrweb-receiverが起動した時のみ読み込まれます。

ファイルは、**ReputationIPFilter**パラメータでフィルタが1つ指定されてさえいれば、保存およびロードされます。IP接続が無い場合、情報は収集されず保存されません。IP接続に関する情報は[General]セクションの**BaseDir**パラメータで指定されたディレクトリにあるipv4.binおよびipv6.binファイルに(それぞれIPv4およびIPv6アドレスに対して)保存されます。ファイル保存中および読み込み中にエラーが発生した場合、この情報はログに出力されます。これらのファイルに保存されたデータはバイナリでOS依存なので、他のシステム上での使用は推奨できません。

このIPが**Trusted IP**とされていない場合、**Reputation IP Filter**モジュール内のIPチェックが**SessionRestrictions**ステージの直後に実行されます(***Restrictions**および**Trusted IP**についての詳細は[Receiver] セクションを参照してください)。

Reputation IP FilterにブロックされたくないIPアドレスがある場合、**SessionRestrictions**パラメータ内でそれらを**Trusted IP**にする必要があります。**Reputation IP Filter**によって誤ってブロックされてしまったIPアドレスをブロック解除する場合も、それらを**SessionRestrictions**パラメータ内で**Trusted IP**にしてください。その後のこのIPからの接続は全て**Reputation IP Filter**に無視されます。

Reputation IP filter によって、収集された統計情報に応じてスコアをIPアドレスに割り当てることができ、またIPアドレスの合計スコアが閾値よりも大きい場合

にこのIPアドレスを一時的にブロックすることも出来ます。

使用可能なフィルタはanti_dha、errors_filter、score_filterです。

Reputation IP filter はIPアドレスが**SessionRestriction**の検査を通過するとすぐにそれを検査します(trustedになっていない場合。**SessionRestrictions**パラメータ内で**Trusted IP**とされた場合は**Reputation IP filter**には検査されません)。

フィルタはカンマで区切って列挙され、指定された順番で検査されます。各フィルタに対して最初に名前が指定され、次にそのパラメータが空白で区切って指定されます(パラメータは全てオプションです)。

パラメータは**NAME**=VALのペアとして設定されます(値と等号の間に空白は置かないでください)。

フィルタの一般パラメータには以下のものがあります(Uは正の整数で、Iは整数、Dは浮動小数点数です)。

- **min_msgs**=U – drweb-maildがフィルタをアクティベートする為に必要な、検査を通過するメッセージの最小限の数の指定です。 値が0に設定されている場合、このパラメータは無視されます。
- **min_errors**=U – フィルタをアクティベートする為に必要な、SMTPセッションのステージに登録されるエラーの最小限の数の指定です。値が0に設定されている場合、このパラメータは無視されます。
- **min_wrong_rcpts**=U – フィルタをアクティベートする為に必要な、SMTPクライアントによって転送される無効な受信者(RCPT TOコマンドの後に拒否された)の最小限の数の指定です。値が0に設定されている場合、このパラメータは無視されます。
- **min_conn**=U – フィルタをアクティベートする為に必要な、IPアドレスからの接続の最小限の数を指定します。値が0に設定されている場合、このパラメータは無視されます。
- **block_period**=T – フィルタの制限内でIPアドレスが通過しない場合にブロックする期間の指定です。T は {time} で記述します。値が0に設定されている場合、このフィルタの制限内でIPが通過しない場合でもブロックは実行されません。
- **score**=I – 現在のセッション内の全てのメッセージに割り当てられるスコアの指定で、このスコアはIPアドレスの一般スコアにも追加されます。スコ

ア値が0でない場合、block_periodの代わりにこのパラメータ値が適用され、ブロックする代わりにスコアがIPアドレスに割り当てられます。

各フィルタに対してユニークなパラメータのセット、および一般パラメータに対する固有のデフォルト値のセットがあります。

- anti_dha – DHA(Directory Harvest Attack)攻撃を防ぎます。このフィルタを使用するには、保護するアドレスを**ProtectedEmails**パラメータの値として省略せずに指定する必要があります。

  固有のパラメータ:

  - **wrong_per_valid_rcpts**=D – 無効なメッセージ受信者の数(RCPT TOコマンドの後に拒否された)と有効な受信者数の間の比率で、フィルタの動作を定義するメインのパラメータです。有効な受信者が存在しない場合、この値は1と見なされます。値が0に設定されていた場合、フィルタは無視されます。

    デフォルト値: 10.0

  一般パラメータのデフォルト値:

  - **min_msgs**=0
  - **min_errors**=0
  - **min_wrong_rcpts**=20
  - **min_conn**=0
  - **block_period**=2h
  - **score**=0

- errors_filter – 特定のIPアドレスから確立されたSMTPセッションの間に発生したエラーの数に応じてIPアドレスをフィルタリング出来るようにします。

  固有のパラメータ:

  - **errors_per_msg**=D – SMTPセッションの間に生じたエラーの数とdrweb-maildに渡されたメッセージの数の比率です。drweb-maildに渡されたメッセージが無い場合、その数は1とみなされます。パラメータ値が0に設定されている場合、この検査は無視されます。

    デフォルト値: 0

  - **errors_per_conn**=D – SMTPセッションの間に生じたエラーの数と、このIPアドレスからの接続数の比率です。フィルタは、パラメータ値が0以外で、このIPアドレスから

の接続が少なくとも1つある場合にのみ適用されます。

デフォルト値: 2.0

これらのパラメータが両方指定されている場合、**errors_per_msg**パラメータが先に検査され、その後**errors_per_conn**パラメータが検査されます。どちらのパラメータ値も0に設定されている場合、フィルタは無視されます。

一般パラメータのデフォルト値:

- **min_msgs**=0
- **min_errors**=100
- **min_wrong_rcpts**=0
- **min_conn**=50
- **block_period**=2h
- **score**=0

- score_filter – 全てのメッセージ、およびこのIPアドレスからのセッションに割り当てられた平均スコアに応じてIPアドレスをフィルタリング出来るようにします。一般Unified Scoreシステムに含まれ、例えば、確立するSMTP接続ステージ上でスパマーをブロックすることが出来ます。

  固有のパラメータ:

  - **score_per_msg**=D – 特定のIPアドレスに対する一般スコア(そのIPから送信されたメッセージの全てのスコアとそのIPによって開始された全てのセッションのスコアの合計)とdrweb-maildに渡されたメッセージ数の比率です。drweb-maildに渡されたメッセージが無い場合、その数は1とみなされます。パラメータ値が0に設定されている場合、この検査は無視されます。

    デフォルト値: 0

  - **score_per_conn**=D – 特定のIPアドレスに対する一般スコアとそのIPアドレスからの接続数の比率です。フィルタは、パラメータ値が0以外で、このIPアドレスからの接続が少なくとも1つある場合にのみ適用されます。

    デフォルト値: 100.0

  これらのパラメータが両方指定されている場合、**score_per_msg**パラメータが先に検査され、その後**score_per_conn**パラメータが検査されます。どちらのパラメータ値も0に設定されている場合、フィルタは無視されます。

  一般パラメータのデフォルト値:

- **min_msgs**=0
- **min_errors**=0
- **min_wrong_rcpts**=0
- **min_conn**=100
- **block_period**=2h
- **score**=0

例:

ReputationIPFilter = errors_filter score=20, score_filter

最初のフィルタは、SMTPセッションの間にあまりに多くのエラーを発生したIPアドレスによって確立されたセッション内の全てのメッセージにスコア20を設定します。2番目のフィルタは、そこからの接続数に対して平均スコアが大きすぎるIPアドレスを全てブロックします。

プラグイン

現時点では**Dr.Web for UNIX mail servers**の以下のプラグインを使用することが出来ます。

- drweb アンチウイルスプラグイン
- vaderetro アンチスパムプラグイン
- headersfilter プラグイン(ヘッダによってメールをフィルタリング)
- modifier プラグイン(メッセージの部分を変更できる)

drwebアンチウイルスプラグイン

drwebは**Dr.Web for UNIX mail servers**のアンチウイルスプラグインで、電子メールのアンチウイルス検査を実行します。

drwebプラグインが正しく動作するには、アンチウイルス検査を直接実行する**Dr.Web Anti-virus Engine**とdrwebdモジュール(**Dr.Web Daemon**)が必要です。drwebdモジュールおよびアンチウイルス**Engine**は**Dr.Web for UNIX mail servers**の一般ディストリビューションパッケージに含まれており、

drwebプラグインよりも先にインストールされている必要があります。

検査のためにdrwebdモジュールに送られるメッセージはセグメントに分けられてるので、**Engine**およびdrwebdモジュールによってサポートされているmime処理は必要ありません。メッセージの解析が終わるとプラグインがその結果をモジュールに送信し、**AddXHeaders**パラメータ値にYesが指定されている場合は以下のヘッダを追加します。

- X-Anti-virus: Name - Name はアンチウイルスソフトウェアの名前とバージョンです。
- X-Anti-virus-Code - Codeはdrwebdモジュールの戻り値です。

drwebプラグインの設定はplugin_drweb.conf設定ファイル内にあります。

drwebプラグインのインストール

drwebプラグインを **Dr.Web for UNIX mail servers**に接続するには、**Dr.Web MailD**設定ファイル内でメッセージ処理の為のプラグインリストにdrwebを加える必要があります。メッセージがデータベースに移される前にdrwebプラグインによってそれを処理したい場合は、このプラグインを**Dr.Web MailD**設定ファイル[Filter]セクションの**BeforeQueueFilters**パラメータ値のリストに加えてください。

例:

```
BeforeQueueFilters = drweb, vaderetro
```

メッセージがデータベースに移された後にdrwebプラグインによってそれを処理したい場合は、このプラグインを**Dr.Web MailD**設定ファイル[Filter]セクションの**AfterQueueFilters**パラメータ値のリストに加えてください。

例:

```
AfterQueueFilters = drweb
```

drweb plug-inのセットアップ

プラグインの動作に関する主要なパラメータは全て%etc_dir/

plugin_drweb.conf設定ファイル内で設定します。設定ファイルの構造やパラメータの種別についての説明は設定ファイルを参照してください。パラメータは設定ファイル内での順番のとおりに説明します。

[anti-virus]セクションではdrwebプラグインの一般設定が定義されています。

[Antivirus] セクション

Address = {socket address}	アンチウイルスプラグインとdrwebd間の連携の為のソケットの指定です。異なるサーバ上にある**Daemons**との連携に複数のソケットを指定することが可能です。リストの先頭にあるアドレスが主要なアドレスと見なされ、残りは予備となります。このパラメータは、標準アドレスタイプの他にPIDにも対応しています。これを使用する場合、daemonの本当のアドレスはそのPIDファイルから取られます。 **例:** PIDファイルへのパスを指定する場合。 **Address** = pid:%var_dir/run/drwebd.pid 複数のアドレスを指定する場合。 **Address** = pid:%var_dir/run/drwebd.pid, inet:3000@srv2.example.com デフォルト値: **Address** = pid:%var_dir/run/drwebd.pid
Timeout = {time value}	drwebdがコマンドを実行する際のタイムアウトの指定です。値が0に設定されている場合、時間の制限はありません。 デフォルト値: **Timeout** = 30s

HeuristicAnalysis = {Yes | No}	ヒューリスティック解析によってdrwebdが未知のウイルスを検出できるようにする設定です。ヒューリスティック解析が無効になっている場合、よく知られたウイルス(ウイルスデータベースに情報があるウイルス)のみが検出されます。ヒューリスティック解析を有効にした場合、正式なプログラムの動作とウイルスの動作の類似性によって誤検出が発生する可能性があり、また検査にかかる時間が少し長くなる場合があります。 デフォルト値: **HeuristicAnalysis** = Yes
TCP_NODELAY = {Yes | No}	Yes は、**TCP_NODELAY** オプションが有効なソケットを使用します。 ネットワークに問題が無い限り、デフォルトのNoを変更しないでください。 デフォルト値: **TCP_NODELAY** = No
ReportMaxSize = {size}	drwebdログファイルの最大サイズの指定です。**ReportMaxSize** = 0の場合、サイズに制限はありません。マルウェアやメール爆弾を検出した際にログファイルのサイズが数メガバイトを超えてしまう可能性があるので、パラメータ値をnullに設定することは推奨できません。 デフォルト値: **ReportMaxSize** = 50k
AddXHeaders = {Yes | No}	Yesが指定された場合、検査するメッセージにヘッダのX-Anti-VirusとX-Anti-Virus-Codeを追加します。 デフォルト値: **AddXHeaders** = Yes

Paranoid = {Yes | No}	Yesが指定された場合、メッセージをパラノイドモードで検査します。このモードではメッセージをセグメント単位で**Daemon**に送信するため、ウイルス検出率は向上しますが検査にかかる時間は長くなります。 passが適用されたオブジェクトがメッセージに含まれている場合、このオブジェクトに関する統計情報の重複が起こる可能性があるので注意してください(添付ファイル、およびメッセージそのものが処理された際にウイルスが検出された場合)。また、いくつかの追加アクション(notify、redirect)も2回適用される場合があります。 デフォルト値: **Paranoid** = No
RegexsForCheckedFilename = {list of regular expressions}	メッセージ検査後にdrwebdによって提供されたレポート内のファイル名を検査する為に、アンチウイルスプラグインが使用する正規表現のリストです。アーカイブされたファイルの名前は">"記号で始まります(">"記号の数はアーカイブのネストレベルによって決まります)。ファイル名のいずれかの部分がリスト内の正規表現にマッチした場合、**BlockByFilename**パラメータで指定されたアクションが適用されます。この検査は、ウイルスが検出されなかったファイルに対してのみ実行されます。 例: **RegexsForCheckedFilename** = "^>.*?\\s{5\\,}" **BlockByFilename**パラメータで指定されたアクションが、名前に5つ以上空白のあるアーカイブまたはファイルを含んだ全てのメッセージに対して適用されます。 デフォルト値: **RegexsForCheckedFilename** =

LicenseLimit {actions}	=	ライセンス制限によって検査が行われなかった際に適用するアクションの指定です。基本処理はpass、tempfail、discard、rejectで、追加処理はquarantine、redirect、notifyです。 同時に複数の値を指定することが出来ます。 デフォルト値: **LicenseLimit** = pass
Infected {actions}	=	既知のウイルスに感染したメッセージに対するアクションを指定します。基本処理はcure、remove、discard、rejectで、追加処理はquarantine、redirect、notifyです。 同時に複数の値を指定することが出来ます。 デフォルト値: **Infected** = cure, quarantine
Suspicious {actions}	=	未知のウイルスに感染した疑いのあるメッセージに対するアクションを指定します。基本処理はpass、remove、discard、rejectで、追加処理はquarantine、redirect、notifyです。 同時に複数の値を指定することが出来ます。 デフォルト値: **Suspicious** = reject, quarantine, notify
Incurable {actions}	=	修復不可能なメッセージに対するアクションを指定します。基本処理はremove、discard、rejectで、追加処理はquarantine、redirect、notifyです。 同時に複数の値を指定することが出来ます。 デフォルト値: **Incurable** = reject,

	quarantine, notify
Adware = {actions}	アドウェア感染メッセージに対するアクションを指定します。基本処理はpass、remove、discard、rejectで、追加処理はquarantine、redirect、notifyです。 同時に複数の値を指定することが出来ます。 デフォルト値: **Adware** = reject, quarantine, notify
Dialers = {actions}	ダイアラー感染メッセージに対するアクションを指定します。基本処理はpass、remove、discard、rejectで、追加処理はquarantine、redirect、notifyです。 同時に複数の値を指定することが出来ます。 デフォルト値: **Dialers** = reject, quarantine, notify
Jokes = {actions}	ジョークソフト感染メッセージに対するアクションを指定します。基本処理はpass、remove、discard、rejectで、追加処理はquarantine、redirect、notifyです。 同時に複数の値を指定することが出来ます。 デフォルト値: **Jokes** = reject, quarantine, notify
Riskware = {actions}	リスクウェア感染メッセージに対するアクションを指定します。基本処理はpass、remove、discard、rejectで、追加処理はquarantine、redirect、notifyです。 同時に複数の値を指定することが出来ます。 デフォルト値:

	Riskware = reject, quarantine, notify
Hacktools = {actions}	侵入用ツール感染メッセージに対するアクションを指定します。基本処理はpass、remove、discard、rejectで、追加処理はquarantine、redirect、notifyです。 同時に複数の値を指定することが出来ます。 デフォルト値: **Hacktools** = reject, quarantine, notify
SkipObject = {actions}	以下の理由により、デーモンが検査出来ないオブジェクトを含んだメッセージに対するアクションを指定します。 • パスワード保護されているかアーカイブが壊れている。シンボリックリンク、または通常ファイルではないファイルがメッセージに添付されている。 • タイムアウトで検査が中断された(詳細はメイン設定ファイルdrweb32.ini内の**SocketTimeout**および**FileTimeout**パラメータに関する記述を参照してください)。 基本処理はpass、remove、discard、rejectで、追加処理はquarantine、redirect、notifyです。 同時に複数の値を指定することが出来ます。 デフォルト値: **SkipObject** = pass
ArchiveRestriction = {actions}	メイン設定ファイルdrweb32.iniで設定されたアーカイブ検査制限に抵触したため、daemonによって検査出来ないアーカイブを含んだメッセージに対するアクションを指定します。

	• アーカイブ圧縮率が設定ファイルdrweb32.ini内の**MaxCompressionRatio**パラメータの値を超えている。 • パックされたオブジェクトのサイズが設定ファイルdrweb32.ini内の**MaxFileSizeToExtract**パラメータの値を超えている。 アーカイブのネストレベルが設定ファイルdrweb32.ini内の**MaxArchiveLevel**パラメータの値を超えている。 基本処理はpass、remove、discard、rejectで、追加処理はquarantine、redirect、notifyです。 同時に複数の値を指定することが出来ます。
	デフォルト値: **ArchiveRestriction** = reject, quarantine, notify

ScanningErrors = {actions}	検査中にdrwebdにエラーを生じさせたメッセージに対するアクションを指定します(例えば**Daemon**が、メモリが足りない状態で動作していた、または先の処理へ進むために必要な権限を持っていなかったなど)。基本処理はpass、remove、reject、tempfailで、追加処理はquarantine、redirect、notifyです。同時に複数の値を指定することが出来ます。
	デフォルト値: **ScanningErrors** = reject, quarantine

ProcessingErrors {actions}	=	検査中にプラグインにエラーを生じさせたメッセージに対するアクションを指定します（例えばアンチウイルスプラグインが、メモリが足りない状態で動作していた、またはdaemonに接続できなかったなど）。基本処理はpass、discard、reject、tempfailで、追加処理はquarantine、redirect、notifyです。同時に複数の値を指定することが出来ます。 デフォルト値: **ProcessingErrors** = reject
BlockByFilename {actions}	=	**RegexsForCheckedFilename**パラメータで指定した正規表現にマッチするファイルをアーカイブ内に検出した際に適用するアクションを指定する。基本処理はpass、discard、reject、tempfailで、追加処理はquarantine、redirect、notifyです。同時に複数の値を指定することが出来ます。 drwebdとの通信がTCPソケット経由で実行された場合、異なるファイル名のフォーマットが使用されるので注意してください。 例: 127.0.0.1 [17078] >/var/drweb/msgs/db/6/00007976/.msg/1.part - Ok ここでは">"記号で始まらず、IPアドレスと検査プロセスの数で始まります。そのため**RegexsForCheckedFilename**パラメータ値の正規表現は、その違いを考慮して作成する必要があります。 デフォルト値: **BlockByFilename** = reject, quarantine, notify

メッセージがアンチウイルスプラグインによってブロックされると、**Dr.Web MailD**からのSMTP応答はエラーコード550 5.7.0、および以下に記載するパラメータの値によって定義されるテキストメッセージになります。これらのパラメータの値は引用符で囲む必要があります。

UseCustomReply {Yes | No}	=	メッセージを拒否した際にSMTPが返すカスタムエラーメッセージの設定です。 デフォルト値: **UseCustomReply** = No
ReplyInfected {text value}	=	**Infected** = rejectまたは**Incurable** = rejectアクションが適用され、**UseCustomReply** = yesの場合にSMTPが返すメッセージの指定です。指定することが出来るのは文字列内のテキストの部分のみで、空白を含む場合は引用符で囲む必要があります。 例: 550 5.7.0 "Text part of reply" デフォルト値: **ReplyInfected** = "DrWEB anti-virus: Message is rejected because it contains a virus."
ReplyMalware {text value}	=	**Adware**、**Dialers**、**Jokes**、**Riskware**、**Hacktools** = rejectアクションが適用され、**UseCustomReply** = yesの場合にSMTPが返すメッセージの指定です。指定することが出来るのは文字列内のテキストの部分のみで、空白を含む場合は引用符で囲む必要があります。 例: 550 5.7.0 "Text part of reply" デフォルト値: **ReplyMalware** = "DrWEB anti-virus: Message is rejected because it contains a malware."
ReplySuspicious {text value}	=	**Suspicious** = rejectアクションが適用され、**UseCustomReply** = yesの場合にSMTPが返すメッセージの指定です。指定することが出来るのは文字列内のテキストの部分のみで、空白を含む場合は引用符で囲む必要があ

	ります。 例: 550 5.7.0 "Text part of reply" デフォルト値: **ReplySuspicious** = "DrWEB anti-virus: Message is rejected because it contains suspicious content."
ReplySkipObject = {text value}	**SkipObject** = rejectアクションが適用され、**UseCustomReply** = yesの場合にSMTPが返すメッセージの指定です。指定することが出来るのは文字列内のテキストの部分のみで、空白を含む場合は引用符で囲む必要があります。 例: 550 5.7.0 "Text part of reply" デフォルト値: **ReplySkipObject** = "DrWEB anti-virus: Message is rejected because it cannot be checked."
ReplyArchiveRestriction = {text value}	**ArchiveRestriction** = rejectアクションが適用され、**UseCustomReply** = yesの場合にSMTPが返すメッセージの指定です。指定することが出来るのは文字列内のテキストの部分のみで、空白を含む場合は引用符で囲む必要があります。 例: 550 5.7.0 "Text part of reply" デフォルト値: **ReplyArchiveRestriction** = "DrWEB anti-virus: Message is rejected because it contains archive which violates restrictions."

ReplyError = {text value}	**ScanningErrors**、**ProcessingErrors** アクションが適用され、**UseCustomReply** = yesの場合にSMTPが返すメッセージの指定です。指定することが出来るのは文字列内のテキストの部分のみで、空白を含む場合は引用符で囲む必要があります。 例: 550 5.7.0 "Text part of reply" デフォルト値: **ReplyError** = "DrWEB anti-virus: Message is rejected due to software error."

ReplyBlockByFilename = {text value}	**BlockByFilename** = reject アクションが適用され、**UseCustomReply** = yesの場合にSMTPが返すメッセージの指定です。指定することが出来るのは文字列内のテキストの部分のみで、空白を含む場合は引用符で囲む必要があります。 例: 550 5.7.0 "Text part of reply" デフォルト値: **ReplyBlockByFilename** = "DrWEB MailD: Message is rejected due to filename pattern"

headersfilter プラグイン

Headersfilterプラグインは、ヘッダに応じてメッセージをフィルタリングします。フィルタリングのルールを設定する際には正規表現(Perlシンタックス)を使用することが出来ます。

headersfilterプラグインのインストール

headersfilterプラグインを**Dr.Web for UNIX mail servers**に接続するには、**Dr.Web MailD**設定ファイル内で、メッセージを処理するプラグインのリストにheadersfilterを加えてください。メッセージがデータベースに移される前にそれ

をheadersfilterプラグインによって処理したい場合は、このプラグインの名前をDr.Web MailD設定ファイル[Filter]セクションの**BeforeQueueFilters**パラメータの値のリストに加える必要があります。

例:

BeforeQueueFilters = drweb, headersfilter

メッセージがデータベースに移された後にそれをheadersfilterプラグインによって処理したい場合は、このプラグインの名前をDr.Web MailD設定ファイル[Filter]セクションの**AfterQueueFilters**パラメータの値のリストに加えてください。

例:

AfterQueueFilters = headersfilter

headersfilterプラグインのセットアップ

プラグインの動作に関する主要なパラメータは全て%etc_dir/plugin_headersfilter.conf設定ファイル内で設定します。設定ファイルの構造やパラメータの種別についての説明は設定ファイルを参照してください。パラメータは設定ファイル内での順番のとおりに説明します。

[Headersfilter]セクションではheadersfilterプラグインの一般設定が定義されています。

フィルタリングのパラメータは下記に記載するルールによって定義されます。ルールは記述されている順番に評価され(リスト内で最初に設定されたルールが最初に評価されます)、適切なルールが見つかり、そのルールに設定されたアクションをプラグインが実行するまで続けられます。

Reject*ルールがメッセージに適用された場合、そのメッセージに対する処理はそれ以上行われません。**Accept***ルールがメッセージに適用された場合、その他のルールは無視され、メッセージはDr.Web MailDの他のプラグインによって処理されます。

[headersfilter] セクション

ScanEncodedHeaders = {Yes | No}	ヘッダの値をデコード前に検査する指定です。例えば、このパラメータの値がYesでコンディションが**RejectCondition** Subject = "iso-8859-5"の場合、Subjectフィールドがiso-8859-5によってエンコードされたメッセージをフィルタリングすることが出来ます。Yesを指定すると、エンコードされたヘッダはデコードの前後で計2回検査されます。 デフォルト値: **ScanEncodedHeaders** = Yes
RejectCondition = {set of conditions}	メッセージ拒否ルールの指定です。メッセージのヘッダが指定された条件のいずれかにマッチした場合、そのメッセージは拒否されます。拒否されたメッセージに対するアクションはこのセクションの**Action**パラメータで指定することが出来ます。条件はどのヘッダに対しても指定することが可能で、通常、ヘッダ名と正規表現から成っています。 HEADER = regular_expression 角括弧、または論理演算子のORやANDを使用して複数の条件を結合することが出来ます。また"!="演算子を使用することも可能です。空白を含む表現は引用符で囲む必要があります。 例: **RejectCondition** Subject = "money" AND Content-Type = "text/html" さらにあと2つフィルタリングの種類があります。 • No HEADER - ある特定のヘッダを持たないメッセージに適した条件です。 例: **RejectCondition** No From - Fromフィールドの無い全てのメッセージを拒否します。

	• HEADER = "8bit" - 8ビット文字をヘッダに含む全てのメッセージを拒否します。 デフォルト値: **RejectCondition =**
AcceptCondition = {set of conditions}	メッセージ許可ルールの指定です。メッセージのヘッダが指定された条件のいずれかにマッチした場合、検査が中断され、メッセージは即座に他のプラグインに送られて処理されます。条件はどのヘッダに対しても指定することが可能です。**AcceptCondition**パラメータの記述に関する詳細は上記**RejectCondition**パラメータの記述を参照してください。 デフォルト値: **AcceptCondition =**
FilterParts = {Yes | No}	**RejectPartCondition**および**AcceptPartCondition**パラメータのルールを有効にします。 デフォルト値: **FilterParts** = Yes
RejectPartCondition = {set of conditions} **AcceptPartCondition =** {set of conditions}	ルールは**RejectCondition**および**AcceptCondition**パラメータのものと同じですが、添付ファイルのヘッダにのみ適用されます。また、**FileName** = maskという条件を使用することも出来ます。maskはPOSIX 1003.2に準拠した正規表現です。 これらのルールによるフィルタリングは、**FilterParts**パラメータにYesが指定されている場合のみ可能です。 デフォルト値: **RejectPartCondition =** **AcceptPartCondition =**

MissingHeader = {text value}	指定したヘッダが無いメッセージを拒否します。 例: **MissingHeader** = "To", "From" デフォルト値: **MissingHeader** =
Action = {actions}	拒否したメッセージに対するアクションの指定です。基本処理はpass、tempfail、discard、rejectで、追加処理はquarantine、redirect、notify、add-headerです。カンマで区切って1つの文字列内で複数の値を指定することが出来ます。 デフォルト値: **Action** = reject, notify

メッセージがプラグインによってブロックされると、**Dr.Web MailD**からのSMTP応答はエラーコード550 5.7.0、および以下に記載するパラメータの値によって定義されるテキストメッセージになります。これらのパラメータの値は引用符で囲む必要があります。

UseCustomReply = {Yes | No}	メッセージを拒否した際にSMTPが返すカスタムエラーメッセージの設定です。 デフォルト値: **UseCustomReply** = No
ReplyRuleFilter = {text value}	**Action** = rejectアクションが適用され、**UseCustomReply** = yesの場合にSMTPが返すメッセージの指定です。指定することが出来るのは文字列内のテキストの部分のみで、空白を含む場合は引用符で囲む必要があります。 例: 550 5.7.0 "Text part of reply" デフォルト値: **ReplyRuleFilter** = "DrWEB

	HeadersFilter plugin: Message is rejected by headers rule filter."

vaderetro anti-spamプラグイン

Vaderetroは**Dr.Web for UNIX mail servers**で使用されるプラグインで、フランスの企業Goto Softwareによってデザインされた**VadeRetro**ライブラリを使用してスパムをフィルタリングします。

VadeRetro ライブラリは、迷惑メールに関する外部情報ソースを参照せず、スタンドアロンでメール解析を行います。さらに、動的にアップデートされるライブラリコードが、素早い処理速度と常に向上し続けるメッセージ解析のレベルを確実なものにします。

解析の結果に応じて、ライブラリによって処理されたメッセージはそれぞれスコア(-10000～+10000の整数)を受け取ります。値が小さいほど、そのメッセージがスパムではない可能性が高くなります。閾値は`vaderetro`設定ファイルの**`SpamThreshold`**パラメータによって定義されます。メッセージのスコアが**`SpamThreshold`**パラメータの値以上の場合、そのメッセージはスパムに分類されます。

解析の最後の段階で、**VadeRetro**ライブラリは以下のヘッダをメッセージに加えることが出来ます。

- `X-Drweb-SpamScore: n`－ `n` はVadeRetroがメッセージに割り当てるスコアです。
- `X-Drweb-SpamState: b`－スパムおよび感染メッセージの場合`b`は**Yes**で、スパムではないメッセージおよび配送失敗通知メール(バウンスメール)の場合は**No**です。
- `X-Drweb-SpamState-Num: s`－`s`はメッセージ分類結果で、0、1、2、3の以下の値をとります。
  - `s = 0` – 正常メール
  - `s = 1` – スパム
  - `s = 2` – ウイルスメール
  - `s = 3` – バウンスメール(配送失敗通知など)

  このヘッダは`vaderetro`設定ファイルの

AddXDrwebSpamStateNumHeaderパラメータの値に**Yes**が指定されている場合にのみ追加されます。

- X-Drweb-SpamVersion: version－versionは**VadeRetro**ライブラリのバージョンです。このヘッダはvaderetro設定ファイルの**AddVersionHeader**パラメータの値に**Yes**が指定されている場合にのみ追加されます。
- X-Spam-Level: z－zは"*" のセットです（各"*"はスコア10に相当します）。 このヘッダはvaderetro設定ファイルの**AddXSpamLevel**パラメータの値に**Yes**が指定されている場合にのみ追加されます。
- X-DrWeb-SpamReason: some_text－some_textはアンチスパムモジュールのエンコードされた診断メッセージで、スパム検出のクオリティを高める為に必要です。このパラメータはメッセージに対する**AddXHeaders**パラメータにyesが指定されている場合にのみ追加されます。

さらに、vaderetroプラグインは**VadeRetro**ライブラリによって感染メッセージまたはスパムと分類されたメッセージの件名にvaderetro設定ファイルの**SubjectPrefix**パラメータの値を追加することが出来ます。これは**SubjectPrefix**パラメータに何か値が指定されている場合にのみ使うことが出来ます。通知に対しては**Subject**フィールドの始めに**NotifySubjectPrefix**パラメータの値を追加することが出来、**UnconditionalSpamThreshold**パラメータを使用して疑いなくスパムと判定されたメッセージに対しては**Subject**フィールドの始めに**UnconditionalSubjectPrefix**の値を追加することが出来ます。

誤ってスパムと判定されたメッセージはvrnonspam@drweb.comに、スパムフィルタを通過してしまったスパムはvrspam@drweb.comに送信してください。

vaderetroプラグインのインストール

vaderetroプラグインを**Dr.Web for UNIX mail servers**に接続するには、**Dr.Web MailD**設定ファイル内でメッセージを処理するプラグインのリストにvaderetroを追加する必要があります。メッセージがデータベースに移される前にそれをvaderetroプラグインによって処理したい場合、このプラグインの名前を**Dr.Web MailD**設定ファイル[Filter]セクションの**BeforeQueueFilters**パラメータの値のリストに加えてください。

例：

```
BeforeQueueFilters = drweb, vaderetro
```

メッセージがデータベースに移された後にそれをvaderetroプラグインによって処理したい場合は、このプラグインの名前をDr.Web MailD設定ファイル[Filter]セクションの**AfterQueueFilters**パラメータの値のリストに加えてください。

例:

```
AfterQueueFilters = vaderetro
```

vaderetroプラグインのセットアップ

プラグインの動作に関する主要なパラメータは全て%etc_dir/plugin_vaderetro.conf 設定ファイル内で設定します。設定ファイルの構造やパラメータの種別についての説明は設定ファイルを参照してください。パラメータは設定ファイル内での順番のとおりに説明します。

[VadeRetro]セクションではvaderetroプラグインの一般設定が定義されています。

[Vaderetro] セクション

FullCheck = {Yes | No}	実装されている全てのスパム検出ロジックを実行します。この検査を通過した各メッセージは-10000～ +10000の間のスコアを受け取ります。スコアが小さいほど、メッセージがスパムである可能性は低くなります。スコアがプラグイン設定ファイル内の**SpamThreshold**パラメータで指定された閾値以上の場合、そのメッセージは疑いなくスパムと判定されます。この完全検査は全体の動作を遅くしてしまう可能性があるので注意してください。
	デフォルト値: **FullCheck** = Yes

NoHamFrom = {Yes | No}	このパラメータの値にYesが指定されている場合、あらかじめ定義されている**Dr.Web MailD**のアドレス(例:nospam@domain.ru)に送信されたメッセージの検査は実行されません。 デフォルト値: **NoHamFrom** = Yes
AddXHeaders = {Yes | No}	X-Drweb-SpamStateおよびX-Drweb-SpamScoreヘッダをメッセージに追加する指定です。前者にはメッセージがスパムかどうかの情報が含まれ、後者には完全検査に応じたスコアの総合計が含まれています。 デフォルト値: **AddXHeaders** = Yes
AddVersionHeader = {Yes | No}	VadeRetroのバージョン情報を表すX-Drweb-SpamVersion ヘッダをメッセージに追加する指定です。 デフォルト値: **AddVersionHeader** = No
AddXDrwebSpamStateNumHeader = {Yes | No}	X-Drweb-SpamState-Numヘッダをメッセージに追加する指定です。**VadeRetro**ライブラリが分類に応じて割り当てる数値が含まれます。 • 0 - 正常メール • 1 - スパム • 2 - ウイルスメール • 3 - バウンスメール デフォルト値: **AddXDrwebSpamStateNumHeader** = No

AddXSpamLevel = {Yes | No}	X-Spam-Levelヘッダをメッセージに追加する指定です。この値はスコア10に相当する* 記号を持っています（例えば110のスコアを持つメッセージには X-Spam-Level: **********ヘッダが追加されます）。 デフォルト値: **AddXSpamLevel** = No
CheckForViruses = {Yes | No}	スパムウイルスに対するヒューリスティック検査の指定です。 デフォルト値: **CheckForViruses** = Yes
CheckDelivery = {Yes | No}	SMTP配送失敗通知メッセージ検査の指定です。 デフォルト値: **CheckDelivery** = No
AllowRussian = {Yes | No}	ロシア語を含むメールの許可を指定します。 デフォルト値: **AllowRussian** = Yes
AllowCJK = {Yes | No}	中国語、日本語、韓国語を含むメールの許可を指定します。 デフォルト値: **AllowCJK** = Yes
WhiteList = {lookups}	ホワイトリストを含むファイルの指定です。許可するアドレスをファイル内で1行につき1つずつ指定します。*@mycompany.comのようにワイルドカード記号（*）を使用することでドメインを指定することが出来ます。 **例:** hello@myneighbourhood.co.uk

	*@mycompany.com デフォルト値: **WhiteList** =
BlackList = {lookups}	ブラックリストを含むファイルの指定です。拒否するアドレスをファイル内で1行につき1つずつ指定します。*@mycompany.comのようにワイルドカード記号(*)を使用することでドメインを指定することが出来ます。 デフォルト値: **BlackList** =
SubjectPrefix = {text value}	スパムと判定されたメッセージの**件名**の前に追加するプレフィックスの指定です。メッセージスコアが**SpamThreshold**の値よりも大きく、スパムと判定された場合に追加されます。 デフォルト値: **SubjectPrefix** =
UnconditionalSubjectPrefix = {text value}	疑いなくスパムと判定されたメッセージの**件名**の前に追加するプレフィックスの指定です。メッセージスコアが**UnconditionalSpamThreshold**の値よりも大きく、疑いなくスパムと判定された場合に追加されます。 デフォルト値: **UnconditionalSubjectPrefix** =
NotifySubjectPrefix = {text value}	バウンスメールと判定された(**VadeRetro**ライブラリによって"3"と評価された)メッセージの**件名**の前に追加するプレフィックスの指定です。 デフォルト値: **NotifySubjectPrefix** =
PathToVadeRetro = {path to file}	**VadeRetro**アンチスパムライブラリへのパスの指定です。update.plスクリプト経由で動的アッ

	プデートが可能で、新しいバージョンがダウンロードされて古いライブラリと置き換えられ、drweb-maildにSIGHUPシグナルが送られます。 デフォルト値: **PathToVadeRetro** = %var_dir/lib/libvaderetro.so
UnconditionalSpamThreshold = {numerical value}	メッセージスコアがこのパラメータ値以上の場合、疑いなくスパムと判定され、**UnconditionalAction**パラメータで指定されたアクションがメッセージに適用されます。**SpamThreshold**パラメータの値以上の数値を指定してください。 デフォルト値: **UnconditionalSpamThreshold** = 1000
SpamThreshold = {numerical value}	メッセージスコアがこのパラメータ値以上の場合、スパムと判定され、**Action**パラメータで指定されたアクションがメッセージに適用されます。この検査はメッセージスコアが**UnconditionalSpamThreshold**パラメータの値よりも小さい場合のみ実行されます。**UnconditionalSpamThreshold**パラメータの値以下の数値を指定してください。 デフォルト値: **SpamThreshold** = 100
UnconditionalAction = {actions}	疑いなくスパムと判定されたメッセージに適用するアクションの指定です。基本処理はpass、remove、discard、rejectで、追加処理はquarantine、redirectです。 デフォルト値: **UnconditionalAction** = pass

Action = {actions}	スパムと判定されたメッセージに適用するアクションの指定です。基本処理はpass、reject、discard、tempfailで、追加処理はquarantine、redirectです。 デフォルト値: **Action** = pass
NotifyAction = {actions}	バウンスメールと判定されたメッセージに適用するアクションの指定です。基本処理はpass、reject、discard、tempfailで、追加処理はquarantine、redirectです。 デフォルト値: **NotifyAction** = pass
UseCustomReply = {Yes | No}	メッセージを拒否した際にSMTPが返すカスタムエラーメッセージの設定です。 デフォルト値: **UseCustomReply** = No
SpamCustomReply = {text value}	**Action**、**UnconditionalAction**、**NotifyAction** = rejectアクションが適用され、**UseCustomReply** = yesの場合にSMTPが返すメッセージの指定です。指定することが出来るのは文字列内のテキストの部分のみで、空白を含む場合は引用符で囲む必要があります。 **例:** 550 5.7.0 "Text part of reply" デフォルト値: **SpamCustomReply** = "Dr.Web vaderetro plugin: this is spam!"

FromProtectedNetworkScoreAdd = {numerical value}	メッセージ送信者のアドレスが **ProtectedNetwork**リスト内にある場合に、メッセージのスコアに特定の値を加える指定です。負の値を使用出来ます。この機能を無効にしたい場合、このパラメータに0を指定してください。 デフォルト値: **FromProtectedNetworkScoreAdd** =
UseReplyCache = {Yes | No}	**ProtectedNetworkReplyCacheLifeTime**および **ReplyToProtectedNetworkScoreAdd** パラメータを有効／無効にします。このパラメータが無効になっている場合、reply_cacheストレージは使用されません。 デフォルト値: **UseReplyCache** =
ProtectedNetworkReplyCacheLifeTime = {time}	reply_cacheへのエントリを保存する期間の指定です。メッセージ送信者のアドレスが **ProtectedNetwork**のリスト内にある場合、そのメッセージの全ての受信者のアドレスが、このパラメータで指定された期間の間、特別なストレージreply_cacheに追加されます。受信者のアドレスが既にストレージにある場合はエントリが更新されます。送信者がreply_cache内にある応答メッセージのスコアは **ReplyToProtectedNetworkScoreAdd** パラメータを使用して変更することが出来ます。 デフォルト値: **ProtectedNetworkReplyCacheLifeTime** =
ReplyToProtectedNetworkScoreAdd = {numerical value}	送信者がreply_cache内にあるメッセージのスコアに追加する値の指定です。 デフォルト値: **ReplyToProtectedNetworkScoreAdd** =

Modifierプラグイン

Modifierプラグインはメッセージの各パーツを変更します（テキストをメッセージ本文に追加する、疑わしい添付ファイルをリネームするなど）。**Dr.Web Modifier**は基本正規表現、拡張正規表現、およびPerl互換正規表現に対応しています。

Modifierプラグインの設定ファイル内で指定できるルールには4つの種類があります。

1つ目はメッセージ全体に適用されるルールです。

- pass、accept - メッセージを許可します。グローバルルールで処理された場合、メッセージ変更プラグインに関する以後の処理を一切行わずにメールデーモンにメッセージを許可することを通知し、プラグインとしての処理を終了します。ローカルルールで処理された場合、以後のローカルルールの処理は行わずにグローバルルールの処理を開始します。
- reject - メッセージを拒否して送信者に通知します。
- discard - 通知せずにメッセージを拒否します。
- notify - 管理者に通知します。このコマンドの後、通知の作成に使用するレポートテンプレートの名前を指定してください。そうでない場合、メッセージ処理の間にエラーメッセージが表示されます。テンプレートはディレクトリ内にあり、そこへのパスは**Dr.Web MailD**設定ファイルの**TemplatesBaseDir**パラメータの値で指定されます。

  例:

  ```
  GlobalRules = select message, notify rule
  ```

  プレフィックスadmin_および.msg拡張子が**Dr.Web Notifier**によって自動的に挿入されます。
- tempfail - 一時的なサーバーの失敗を送信者に報告します。
- redirect - メッセージを指定したアドレスに転送します。
- quarantine - メッセージを隔離に送ります。

stopコマンドはルールの処理を中断します。アクションは既に処理されているルール（pass、accept、rejectなど）、また最後に実行されたコマンドに応じて適用されます。

acceptはpass + stopとほとんど同じです。ただしacceptはローカルルールでは処理を中断し、グローバルルールではpassと同じになります。

passはdiscardおよびtempfailよりも優先されます。ただしrejectは最優先され、メッセージの処理を中止し、以後の全てのアクションは実行されません(notifyを除く)。

これらのコマンドは、通知に挿入する追加のテキストフィールドで補完する必要があります。

各メールメッセージは、MIMEオブジェクト、そのヘッダと内容、マルチパートメッセージ内に添付されたMIMEオブジェクトから成っています。それぞれのパートに対して、削除、署名追加、テキストの置き換えや変更などの異なるアクションを実行することが出来ます。他の種類の全てのルールが別々のエレメント、またはエレメントのセットに適用されます。

各コマンドの前にselect、or、and、nand、norのインストラクションの内の1つを指定する必要があります。各コマンドの後には選択のパラメータを指定します。

2つ目は別々のエレメントに適用されるルールです。

- select message

  メッセージのルートMIMEエレメントを選択します。

- select mime(headers), select mime.headers

  select mime(prologue), select mime.prologue

  select mime(body), select mime.body

  select mime(epilogue), select mime.epilogue

  これらのコマンドで様々なMIMEオブジェクトを選択します。括弧のあるコマンドは指定されたエレメントを含んだMIMEオブジェクトを選択しますが、ドットのあるコマンドはエレメントそのものを選択します。

  例:

  select mime(headers) Content-type "x-video"

`remove`

このコマンドはメッセージから全てのvideoエレメントを削除します。

`select mime.headers Content-type "x-video"`

`remove`

このコマンドは全てのvideoエレメントからデータタイプに関する情報を削除します。複合MIMEパートを選択できるのは、それがメッセージそのものである場合のみです。

- `select mime(headers)` *header_name regular_expression_to_match_header_body*

  `select mime(prologue)` *regular_expression*

  `select mime(body)` *regular_expression*

  `select mime(epilogue)` *regular_expression*

  これらのコマンドは、指定したテンプレートに一致するテキストを持ったエレメントを選択します。

- `select sender` <*regular_expression*>

  `select recipient` <*regular_expression*>

  これらのコマンドは、受信者と送信者に関する情報を持ったエントリを選択します。この情報はエンベロープからとられます。必要な記号のシーケンスが見つかった場合、`select sender`および`select receiver`コマンドが`select message`コマンドとして処理されます。

  例:

  以下のコマンドを使用して、管理者に対するメッセージの最後にグリーティングを追加することが出来ます。

  `select recipient "root@localhost", append_text "hello, root"`

複数の条件によってエレメントを選択する必要がある場合、該当する論理演算子を使用してルールを組み合わせることが出来ます。

- `and` - 指定されたルールに一致するアイテムのみを選択内に残します。
- `nand` - 指定されたルールに一致しないアイテムのみを選択内に

残します。

- or - 指定されたルールに一致するアイテムのみを選択に追加します。
- nor - 指定されたルールに一致しないアイテムのみを選択に追加します。

これらの演算子はマルチパートMIMEのオブジェクトの選択にのみ使用することができ、そのようなオブジェクトの別々のパートには使用できないので注意してください。

html中に"<script"という文字列があるMIMEパートを選択:

```
select mime(headers) Content-type html
and mime(body) "\<script"
```

2つの別々のルールが順番に適用されます。1つ目でContent-typeヘッダ内の全てのhtmlエレメントを選択し、2つ目でそのエレメントの中から"<script"記号のセットを持つものが選択されます(大文字小文字は無視されます)。

"<"記号の前のバックスラッシュは"<script"を算術値ではなくストリングとして扱うことを意味するものです。

例:

```
select mime(headers) Content-type html
nand mime(body) "\<script"
```

最初の条件によってContent-typeヘッダ内の全てのhtmlエレメントが選択されます。2つ目の条件によって"<script"という文字列を持つエレメントがそこから除外されます。

例:

```
select mime(headers) Content-type html
or mime(body) "\<script"
```

最初の条件によってContent-typeヘッダ内の全てのhtmlエレメントが選択されます。2つ目の条件によって"<script"という文字列を持つエレメントが選択に加えられます。

例:

```
select mime(headers) Content-type html
nor mime(body) "\<script"
```

最初の条件によってContent-typeヘッダ内の全てのhtmlエレメントが選択されます。2つ目の条件によって"<script"という文字列を持たないエレメントが選択に加えられます。

後続のルールの前にselectを指定すると、前回の選択が解除されます。

例:

```
select mime(headers) Content-type html
select mime(body) "\<script"
```

最初の条件によってContent-typeヘッダ内の全てのhtmlエレメントが選択されます。2つ目の条件によって最初の選択が解除され、"<script"という文字列を含むエレメントのみが選択されます。

演算子が指定されていない場合、後続のルールは全て無視され選択には変更が加わりません。

例:

```
select mime(headers) Content-type html
mime(body) "\<script"
```

選択は最初の条件でのみ行われ、Content-typeヘッダ内のhtmlエレメントのみが選択されます。

Modifierプラグインとvaderetroプラグインに互換性を持たせるには、メッセージヘッダ内の検索に比較命令">n"および"<n"を使用してください。ヘッダが整数を含み(例:X-Drweb-SpamScore "30")、あるルールに一致する(例:select mime(headers) X-Drweb-SpamScore "<50")場合、そのヘッダにModifierルールを適用することが出来ます。

この場合は、select mime(headers) X-Drweb-SpamScore "\<50"ルールでもX-Drweb-SpamScore "<50"ヘッダのエレメントが選択されるので、"<"記号の前にバックスラッシュは必要ありません。

select_mimesコマンドを使用して、MIMEオブジェクトをそのヘッダによって選択することが出来ます。ヘッダとオブジェクトを同じ条件で選択する必要がある場

合に、これによってプラグインの動作を早めることが出来ます。オブジェクト全体を選択したい場合は、そのオブジェクトからエレメントを1つだけ選択してください。

3つ目は選択したエレメントを変更するためのルールです。

このルールはMIMEオブジェクトの内容にのみ適用されます。

- `replace` *expression_for_replacement regular_expression_to_be_replaced*
  `replace_all` *new_text*

  これらのコマンドは、テキストを他のテキストと置き換えます。

  例:

  添付されているファイルの拡張子をリネームします。

```
select mime.headers Content-disposition "filename=.*\\.exe",\
or mime.headers Content-type "name=.*\\.exe",\
replace "\\.ex_" "\\.exe",\
pass
```

  これらのコマンドはマルチパートメッセージのパートには使えません。つまり、2つのサブオブジェクトを持ったマルチパートMIMEオブジェクトから成るメッセージに対しては

```
select message
replace_all «text»
```

  というコマンドは有効ではありません。マルチパートオブジェクト自体は他のオブジェクトのコンテナであり、データを含まないからです。

  `replace`および`replace_all`コマンドに対しては、関数呼び出しを*expression_for_replacement*および*new_text*として使用することが可能です。それらは`${func_name}`として指定することが出来ます。関数の引数は現在の*regular_expression_to_be_replaced*です。

  以下の関数に対応しています。

- lc - 小文字に切り換えます。
- uc - 大文字に切り換えます。
- urlencode - 引数をURLとして使用できる文字列にエンコードします。
- self - 正規表現を変更せずに返します。

例:

```
select mime.headers "Subject" "^.*$", replace_all "old:${self} new:${lc}"
```

指定されたパターンに一致するメッセージのSubjectヘッダ(例:"This is Subj")を"old:This is Subj new:this is subj"で置き換えます。

例:

```
select mime.body ".*", replace "Upper:${uc}" "http://\\S+"
```

指定されたパターンに一致する、メッセージ本文からのいくつかのテキスト(例:"Text1 http://vasya.pup.kin Text2")を"Text1 Upper:HTTP://VASYA.PUP.KIN Text2"で置き換えます。

例:

```
select mime.body ".*", replace "http://check-url.com?url=${urlencode}" "http://\\S+"
```

指定されたパターンに一致する、メッセージ本文からのいくつかのテキスト(例:"Visit http://vasya.com?id=3")を"Visit http://check-url.com?url=http%3A%2F%2Fvasya%2Ecom%3Fid%3D3"で置き換えます。

- remove

このコマンドは、ルートMIMEオブジェクト以外の全ての種類の選択されたオ

ブジェクトを削除します。

例:

removeコマンドは以下のようなルール内では使用できません。

```
GlobalRules = select mime(body) "text", remove, pass
GlobalRules = select mime(body) "script", remove, pass
```

- prepend_text
  append_text
  prepend_html
  append_html

  これらのコマンドは、選択したMIMEオブジェクトにプレーンテキストかhtmlを加えます。

例:

```
select message
append_html "<h1>checked by anti-spam</h1>" [[7b:]encoding]
```

これらのコマンドは、オプションのパラメータencodingによってセットされたエンコーディング、およびプレフィックス"7b:"によってセットされた7-bit context transferエンコーディングでメッセージに署名を付けます。

ある特定のエンコーディングにテキストを挿入する必要がある場合、言語ファイル(.lng拡張子)をソースとして使用することが出来ます。.lngファイルから必要な文字列を選択するには$1, $2 ... $nパラメータを使用してください。nは.lngファイル内の文字列の番号です。

例:

.lng ファイルが以下のような場合、

```
1 = string1
```

```
2 = some other string
...
```

append_text $2 はappend_text "some other string" コマンドと同じになります。

値そのものか「ファイル」タイプのルックアップのみ使用できるLookupsLiteタイプの値を介してルックアップを使用することも可能です。

例:

```
append_text "lookup:file:path_to_file"
```

以下のコマンドでヘッダをメッセージに追加することが出来ます。

```
select message, addheader "foo:bar"
```

このコマンドは、fooという名前でbarという値のヘッダを、選択したメッセージエレメントに追加します。ヘッダの名前と値はコロンで区切って列挙します。

4つ目はif/else構造を作成するためのルールです。

- goto - 無条件に転送
- goto(y) - エレメントが少なくとも1つ選択されている場合、無条件に転送
- goto(n) - エレメントが選択されていない場合、無条件に転送

パラメータ値に正の整数を使用することができ、一度にいくつのルールをスキップする必要があるかを指定します。

例:

実行ファイルが添付されたメッセージを全て拒否したい場合、以下のコマンドを使用してください。

```
mime(header) Content-type "executable"
goto(n) 1
reject
```

上記のコードは以下のように実行されます。

```
selection=find(mimes with content type "*executable*")
if(selection){
    reject mail;
}
```

`if [not] found .... else .... endif`コマンドを使用することも可能です。

例:

```
select mime.headers "X-DrWeb-SpamState" "yes",\
if found,\
select mime(headers) Content-type "image",\
remove,\
endif,\
```

上記のコマンドによって、**Vaderetro**プラグインがスパムと判定したメッセージから全ての画像を削除することが出来ます。

正規表現内で引用符を使用する場合、複数の"\"記号でそれらをエスケープする必要があります。現在のバージョンでは、引用符のエスケープに"\"記号が6個必要です。

例:

```
GlobalRules = select mime.headers Subject ".*\\\\\\\"", if found, reject, endif
```

また、各メッセージのスコアをチェックすることも出来ます。処理の始めにメッセージに割り当てられる最初のスコアは0になります。if score、add_score、set_scoreコマンドを使用して、プラグインが処理の間にこのスコアをチェック、変更することが出来ます。"if score"は"if found"コマンドと同じ働きをしますが、チェックするのはメッセージスコアのみです(それより前の"select"コマンドの結果は無視します)。

例:

```
....
if found,\
   set_score 10,\
```

```
endif,\
```

メッセージに新しいスコア10を設定します（それが条件に抵触しない場合）。

例:

```
....
add_score 11,\
```

メッセージのスコアに11加えます。

例:

```
....
if score >100,\
   reject,\
else,\
   add_score -5,\
endif
```

メッセージスコアが100よりも大きい場合、このメッセージは拒否されます。それ以外の場合、スコアから5を引きます。

`if score` 引数は空白無しの1つの文字列として指定し（例えば`< 100`ではなく`<100`）、比較演算子および整数の引数を含んでいる必要があります。

以下の比較演算子を使用することが出来ます。

- `if score <2` - スコアが2より小さい場合
- `if score >5` - スコアが5より大きい場合
- `if score =8` - スコアが8の場合

整数の引数は、-20億～+20億の間の32bit整数です。メッセージの処理中にスコアがオーバーフローする場合があり、それにより他のモジュールが正しく動作しなくなることがあります。そのため、ルール内で無意味に大きいスコア値を使用することは推奨できません（例えば`add_score`パラメータに2000000000を指定するなど）。

選択したMIMEオブジェクトにテキストを加えた後、選択は破棄されます。

	remove	replace	replace all	append text	prepend text	append html	prepend html	add header	add score	set score	accept	discard	reject	tempfail	notify	redirect	quarantine
mime.header	+	+	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-
mime.prologue	+	+	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-
mime.epilogue	+	+	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-
mime.body	+	+	+	-	-	-	-	-	-	-	-	-	-	-	-	-	-
mime(headers)	+	*	*	-	-	-	-	+	-	-	-	-	-	-	-	-	-
mime(prologue)	+	*	*	-	-	-	-	+	-	-	-	-	-	-	-	-	-
mime(epilogue)	+	*	*	-	-	-	-	+	-	-	-	-	-	-	-	-	-
mime(body)	+	*	*	-	-	-	-	+	-	-	-	-	-	-	-	-	-
sender	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
recipient	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
message	-	-	-	-	-	-	-	-	+	+	+	+	+	+	+	+	+

表1.オブジェクト選択肢と実行可能な処理（コマンド）

- ***** mime.bodyの場合と同じ
- **+** 利用可能
- **-** 利用不可

例:

- 複数の条件によってエレメントを選択する

```
GlobalRules = select mime(headers) Content-type
"text", and mime(body) "typical spam",\
```

- そのようなエレメントが見つかったら、メッセージを破棄する

```
goto(n) 1,\
discard,\
```

- それ以外の場合、実行ファイルを全て選択しそれらを削除する

```
select mime(headers) Content-disposition ".
exe",\
remove,\
```

- メッセージ本文に署名を追加する

```
select message, append_text "checked!"
```

goto(n) 1,\およびdiscard,\の後ろに空白を置くと、ルールが実行されないので注意してください。

メッセージに**html**ファイルを追加する

```
GlobalRules = select message, append_html "lookup:file:/maild-files/somehtml.html"
```

選択したユーザからのメッセージを削除する

```
GlobalRules = select mime(headers) From "weirdohacker@server.net", if found, reject, endif
```

メッセージを転送する

```
GlobalRules = select mime.headers To "someaddress@my-net.com", replace_all "anotheraddress@my-net.com"
```

この例では、元のメッセージはsomeaddress@my-net.comに送信され、そのコピーがanotheraddress@my-net.comに送信されます。

メッセージを元の受信者に送信したくない場合は以下のルールを使用してください。

- 特定の条件によってメッセージを選択する

```
GlobalRules = select mime.headers Subject "Help",\
if found,\
select mime.headers To "someaddress@my-net.com",\
if found,\
```

- 選択したメッセージを特定のアドレスに転送する

```
redirect "anotheraddress@my-net.com",\
```

- *選択したメッセージが誤って元の受信者に送信されないよう、そのメッセージを削除する*

```
discard,\
endif,\
stop,\
endif,\
```

メッセージを件名に応じて転送する

```
GlobalRules = \
```

- *サポート部門へのメッセージをチェックする*

```
select mime.headers Subject "support|bugreport
[s]|help",\
if found,\
```

- *テンプレートが見つからない場合、以下のコマンドが渡されます*

```
select mime.headers To "@company.com", \
if found,\
redirect "support@company.com",\
endif,\
pass, \
endif,\
```

- *クライアントがオーダーを望んだ場合、以下のコマンドが実行されます*

```
select mime.headers Subject "price|buy|order",\
if found,\
select mime.headers To "@company.com", \
if found,\
redirect "sell@company.com",\
endif,\
pass, \
endif,\
```

- その他のトピック

```
select mime.headers To "@company.com", \
redirect "inbox@company.com",\
pass
```

添付された実行ファイルを検索してそれらをリネームする

```
select mime.headers Content-disposition "filename=.*\\.exe", or mime.headers Content-type "name=.*\\.exe",\
replace "\\.ex_" "\\.exe",\
pass
```

Modifierプラグインのインストール

Modifierプラグインを**Dr.Web for UNIX mail servers**に接続するには、**Dr.Web MailD**設定ファイル内でメッセージを処理するプラグインのリストに**Modifier**を追加する必要があります。メッセージがデータベースに移される前にそれを**Modifier**プラグインによって処理したい場合、このプラグインの名前を**Dr.Web MailD**設定ファイル[Filter]セクションの**BeforeQueueFilters**パラメータの値のリストに加えてください。

例:

```
BeforeQueueFilters = modifier
```

メッセージがデータベースに移された後にそれを**Modifier**プラグインによって処理したい場合は、このプラグインの名前を**Dr.Web MailD**設定ファイル[Filter]セクションの**AfterQueueFilters**パラメータの値のリストに加えてください。

例:

```
AfterQueueFilters = modifier
```

Modifierプラグインのセットアップ

プラグインの動作に関する主要なパラメータは全て%etc_dir/plugin_modifier.conf 設定ファイル内で設定します。設定ファイルの構造やパラメータの種別についての説明は設定ファイルを参照してください。パラメータは設定ファイル内での順番のとおりに説明します。

[Modifier]セクションでは**Modifier**プラグインの一般設定が定義されています。

[Modifier] セクション

GlobalRules = {list of rules}	メッセージ処理のグローバルルールを設定します。詳細および例はreadmeファイルをご覧下さい。ルールは**GlobalRules**パラメータ内でカンマで区切って指定します。4つのグループのルールがあります。
	• メールメッセージ全体に適用されるコマンド
	  ○ pass - それ以上の検査を実行せずにメッセージを通過させます。
	  ○ reject - メールを拒否して送信者に通知します。
	  ○ discard - メールを拒否して通知しません。
	  ○ notify - 通知を送信します。
	  ○ tempfail - 一時的なサーバの失敗を送信者にレポートします。
	• メッセージの選択したパートに適用されるコマンド
	• 選択したエレメントを変更するためのコマンド
	• if/else条件を作成するコマンド
	
	例:
	以下のルールはメッセージにhtmlファイルを追加します。
	GlobalRules = select message, append_html "lookup:file:/maild-files/somehtml.html"
	以下のルールは指定したユーザからのメッセージを削除します。
	GlobalRules = select mime

	(headers) From "weirdohacker@server.net", if found, reject, endif デフォルト値: **GlobalRules** = rule1, rule2, ...
Encoding = {text value}	ルールから直接append_textおよびprepend_textコマンドで挿入するテキストの、プラグインによって指定するエンコードです。 デフォルト値: **Encoding** = koi8-r

MTAとの統合

この章では**Dr.Web for UNIX mail servers**と様々なメールトランスファーシステムとの統合について説明します。統合のプロセスを簡易化するため、ディストリビューションパッケージには各MTA向けの設定用スクリプトが含まれています。

configure_MTA.shスクリプトは、**Dr.Web for UNIX mail servers**とお使いのメールシステムとの統合をセットアップします。スタートアップ後、必要なメールシステムがインストールされているかどうかをこのスクリプトがチェックし、インストールされていないようであれば、スクリプトは操作を終了します。インストールされている場合は、基本的なセットアップに必要ないくつかの設定についての質問をスクリプトがユーザに投げかけます。セットアップは手動でも行うことができます（詳細については本マニュアルの該当する章をご覧ください）。

SMTPプロキシモードとの統合

Dr.Web MailDはメールプロトコルのプロキシサーバとして働き、それによって多くのメールシステムと一緒に使うことができます。このモードでは drweb-receiverモジュールはSMTP/LMTPサーバとして働き、drweb-senderモジュールはSMTP/LMTPクライアントとして働きます。さらに、drweb-senderモジュールはメッセージを直接ローカルメールシステムに送ることができます。

drweb-receiverには、最新のマルチプレクサ(epoll、kevent、/dev/pollなど)を使って導入された高パフォーマンスのSMTPサーバが含まれています。このSMTPサーバはマルチスレッドで、それぞれのスレッド、IPv6プロトコル、SMTP拡張子の番号ごとに複数のコネクションに対応しています。

- PIPELINING (RFC2920)
- 8BITMIME (RFC1652)
- ENHANCEDSTATUSCODES (RFC3463)
- SIZE (RFC1870)
- AUTH (RFC4954)

メールをインターネットから直接受け取る場合、新しくdrweb-receiverに導入されたいくつかのテクノロジーがメールのフィルタリングをより簡単に、効率的にします。制限およびReputation IP FilterによってSMTPセッションの段階でメールをフィルタリングすることが出来ます(そして、例えばDHA攻撃を防ぐことが出来ます)。

drweb-receiver、drweb-senderモジュールに対する全ての設定は、**Dr.Web MailD**設定ファイルの[Receiver]および[Sender]セクションで定義され、本マニュアルのReceiverおよびSenderに記述しています。

CommuniGate Proとの統合

CommuniGate Proの設定

CommuniGate Pro(以後CGP)で**Dr.Web MailD**からメッセージを送信および受信するには以下の手順を実行してください。

1. リモート管理のためのWebAdminプログラムを使用してCGPに接続します。
2. 設定 -> 全般 -> ヘルパー メニューへ。
3. 以下のパラメータで新しい外部コンテンツフィルタを追加します。

   Use Filter: DrWeb Maild

   Log: Problems

   Path: %bin_dir/drweb-cgp-receiver

   Time-Out: 2 minutes

Auto-Restart: 15 seconds

4. CGPの実行に使用した権限がdrweb-cgp-receiverのスタートアップに適切であるかどうかをチェックします。
5. 設定 -> Queue -> ルール メニューへ。
6. "check messages of less than N bytes"のような新しいルールを作成します。

新しいルールを作成するには以下の手順を実行してください。

1. ルールの名前を選択し(例えばdrweb-filter)、**Create New**ボタンをクリックします。
2. **Edit**ボタンをクリックし、**Action**フィールドでExternal Filter値を指定します。
3. **Parameters**フィールド内で設定 -> 全般 -> ヘルパーメニューの**Filter**フィールドと同じ値を入力します。

GROUP、LIST、RULES(http://www.communigate.com/CommuniGatePro/Transfer.html)から受信したメッセージの重複チェックを防ぐには、以下の設定をルールに追加して下さい。

Submit Address not in GROUP*,LIST*,RULES*

メッセージがPIPE経由でアップロードされた場合、認証されたことを示すフラグが失われる場合があります。さらに、**AfterQueueFilters**リスト内にプラグインがいくつかあった場合、ルールに以下のラインを追加する必要があります。

Any Recipient not in alldomains@main.domain, all@*

main.domain はCGPサーバのメインのドメインです。

高度な設定(各ユーザごとのフィルタリングを有効/無効にする設定など)についての情報はCGPと一緒に配布されているドキュメントを参照してください。

Dr.Web MailDの設定

CGPとの統合で、**Dr.Web MailD**のdrweb-cgp-senderモジュールは**Sender**コンポーネントとして動作します。このモジュールはmailグループの権限で起動され、それによってcgpディレクトリに書き込むことが可能です。一方**Dr.Web MailD**のdrweb-cgp-receiverモジュールは**Receiver**コンポーネントとして動作します。このモジュールはCGPメールシステム自体によってroot権

限で起動されます。

このような設定でDr.Web MailDを正しく動作させるために、他のDr.Web MailDモジュールをどのユーザの権限で起動させるかを明示的に指定する必要があります。ユーザの名前はDr.Web MailD設定ファイル[CgpReceiver]設定セクションの**ChownToUser**パラメータで設定するか、このパラメータの値を指定せずにプログラム全体 をroot権限で実行してください。

drweb-cgp-senderはPIPEドライバ経由で新しいメッセージをCGPに転送するので、メッセージがループするのを防ぐために特別なヘッダを追加する必要があります。このヘッダはDr.Web MailD設定ファイル[CgpSender]セクションの**UseSecureHash**パラメータまたは**SecureHash**パラメータで設定します。

この場合drweb-cgp-receiverモジュールは、このヘッダを持つメッセージを検査せずに通過させます。Dr.Web MailD設定ファイル[CgpSender]セクションの**UseSecureHash**パラメータの値にNoを指定することでこのヘッダの使用を無効にすることが出来ます。それによってモジュールはPIPEドライバから受信した全てのメッセージを検査せずに通過させます。

Dr.Web MailDがCGPと正常に動作するための全ての設定はDr.Web MailD設定ファイルの[CgpReceiver]および[CgpSender]セクションで定義され、本マニュアルのCgpReceiverおよびCgpSenderの章に記述しています。

既知の障害

Linuxでは、コマンドラインをHelpers設定経由で変更またはアップデートした後、前回のフィルタのプロセスはCGPを再起動するまでゾンビプロセスとして残ります。

詳細:

drweb-cgp-receiverを起動すると以下のメッセージが表示される。

```
/usr/libexec/ld-elf.so.1: Shared object "libstdc++.so.6" not found, required by "libboost_thread.so"
```

ソリューション:

システムは、%bin_dir/lib/ディレクトリ内にある必要なライブラリを見つけることが出来ません。libstdc++.so.6ライブラリとlibgcc_s.so.1ライ

ブラリを、%bin_dir/lib/からライブラリのあるシステムディレクトリにコピーする必要があります（またはそれらのライブラリへのシンボリックリンクを作成してください）。

Sendmail MTAとの統合

SendmailとDr.Web MailDの統合にはMilter APIが必要です。お使いのSendmailがMilter APIライブラリに対応していない場合、対応ライブラリにそれを追加するようSendMailをリビルドする必要があります。詳細についてはSendmailのドキュメントを参照してください。

Dr.Web MailD設定ファイル[Sender]セクションの**SecureHash**パラメータの値が指定されていることを確認してください（値には任意の記号の文字列を設定することができます。記号は10個以上使用することを推奨します）。また、同セクション内の**UseSecureHash**パラメータの値にはYesを指定してください。

Sendmail MTAとDr.Web MailDの統合はMilter API経由で（drweb-milterモジュールはReceiverコンポーネントとして使用されます）以下のように実行されます。

- Sendmailはdrweb-milter転送アドレス__ADDRESS__によって定義された転送接続を介して、Milter APIまたはメッセージ自体から内部コマンドを受け取ります。メッセージはメールセッションのステージ（helo、mail from:、rcpt to:など）に応じセグメントに分けられて転送されるため、drweb-milterモジュールによって一時ファイルに保存されます。drweb-milterは、メッセージに関する命令をMilter API経由でSendmailに送信します。

  Milter APIはマルチスレッドライブラリで、同時に複数のメールセッションを処理することができます。上記に記載した統合スキーマにおいて、Sendmailはクライアント、drweb-milterはサーバとなります。従って、sendmail.cf設定ファイル内でアドレスを指定する必要があり、接続に適したクライアントアドレスがSendmailによって選択されます。

- drweb-milterモジュールは、他のトランスポート接続経由でdrweb-maildモジュールにコマンドを送り、応答を待ちます。

上記に記載したスキーマにおいて、drweb-milterモジュールはSendmailインターフェースとdrweb-maildモジュール間のエージェントとして動作します。Sendmailとdrweb-milterモジュールはSendmailと別々のコンピューター上で動作する

ことが可能ですが、drweb-milterモジュールとdrweb-maildモジュールは同じコンピューター上で動作する必要があります。

Sendmailの設定

SendmailとDr.Web MailD間の統合をセットアップするにはsendmail.mc設定ファイルおよびsendmail.cf設定ファイルの編集が必要な場合があります。

sendmail.cf設定ファイルを再コンパイルしたくない場合は、以下のラインを挿入または追加することも可能です（該当する定義が既にファイル内に存在する場合）。

バージョン8.14.0以降:

```
-------------------- cut ------------------
############################
# Input mail filters
############################
O InputMailFilters=drweb-filter
O Milter.LogLevel=6
############################
#       Xfilters
############################
Xdrweb-filter,  S=__ADDRESS__,
F=T, T=C:1m;S:5m;R:5m;E:1h
------------------- cut ---------------------
```

ローカルで送信されたメッセージ（mailまたはsendmailシステムコールによって）をチェックするには、sendmail.cf設定ファイルに加えられた全ての変更をsubmit.cfファイルおよびsubmit.mcファイルにコピーする必要があります。

submit.cfファイルおよびsubmit.mcファイルはデフォルトで読み取り専用になっているので、編集する前にアクセス権限を変更（書き込み権限を与えます）するようにしてください。また、**PrivacyOptions**パラメータにnobodyreturn値を追加する必要もあります。

例:

```
-------------------- cut ------------------
# privacy flags
O PrivacyOptions=goaway,noetrn,nobodyreturn
-------------------- cut ------------------
```

Or in {sendmail_src}/cf/cf/feature/msp.m4:

```
-------------------- cut ------------------
define('confPRIVACY_FLAGS'
'goaway,noetrn,nobodyreturn,restrictqrun')
-------------------- cut ------------------
```

フィルタを使用できない場合、以下のフラグ(F=)を有効にしてください。

- R – 送信失敗
- T – 送信遅延

F=RおよびF=Tのどちらも指定されていない場合、メッセージは検査されずに通過します。

sendmail.mcに以下のラインを追加することも出来ます。

バージョン8.14.0以降:

```
-------------------- cut ---------------------
INPUT_MAIL_FILTER('drweb-filter',
'S=__ADDRESS__,
F=T, T=C:1m;S:5m;R:5m;E:1h')
define('confMILTER_LOG_LEVEL','6')
-------------------- cut ---------------------
```

タイムアウトはSendmailに対して設定されたタイムアウトの値に応じて設定してください。

```
O Timeout.datablock=XX
```

デフォルト値は1時間です(XX=>1h)。

sendmail.cf設定ファイルを変更した後は、再コンパイルしてください。

__ADDRESS__ストリングは、drweb-milterへの接続に使用するトランスポートアドレスを指定します。書式と値はDr.Web MailD設定ファイル[Milter]セクションの**Address**パラメータのものと同じです。

TCPソケットに対しては以下の書式でアドレスを指定してください。

inet:__PORT__@__HOST__

__PORT__ and __HOST__ は確定値を持っている必要があります(例:inet:3001@localhost)。

UNIXソケットに対しては以下の書式でアドレスを指定してください。

local:__SOCKPATH__

__SOCKPATH__ストリングで、フィルタを起動した権限によってアクセスが可能なパスを指定してください(例:local:/var/run/drweb-milter.sock)。

フィルタの設定に関する詳細はSendmailのドキュメントを参照してください。必要なパラメータ全てに値を指定した後、Sendmailを再起動する必要があります。

drweb-maildモジュール内にあるSendmailメッセージID(sendmail's message ID)のロギング、および認証成功に関する情報のdrweb-maildへの送信を有効にするには、以下のラインをsendmail.cfに含めてください。

```
------------------- cut ---------------------
O Milter.macros.envfrom=i,{auth_type}, ...
------------------- cut ---------------------
```

(省略記号は他のパラメータを表しています)

Dr.Web MailDが送信者のIPアドレスおよびホスト名を定義するため、また受信者のインターフェースアドレスをdrweb-maildモジュールに送信するためには以下のラインをsendmail.cf設定ファイル内に含めてください。

```
------------------- cut ---------------------
O Milter.macros.connect=_,{if_addr}, ...
```

```
------------------- cut ---------------------
```

（省略記号は他のパラメータを表しています）

syslogへの以下のメッセージの出力を無効にするには、

```
------------------- cut ---------------------
X-Authentication-Warning:      some.domain.com:
drweb set sender to DrWeb-DAEMON@some.domain.
com using -f
------------------- cut ---------------------
```

drweb-milterを操作している権限を持ったユーザ(デフォルトではdrwebユーザ)をsubmit.cf内のtrusted-usersリストに加える必要があります。submit.cf設定ファイルおよびsendmail.cf設定ファイル内でユーザを直接リストに加えてください。

```
------------------- cut ---------------------
#####################
#   Trusted users   #
#####################
Tdrweb
------------------- cut ---------------------
```

またはsubmit.mcファイルに以下のラインを加えてください。

```
------------------- cut ---------------------
define('confTRUSTED_USERS', 'drweb')
------------------- cut ---------------------
```

Dr.Web MailDの設定

Senderコンポーネントとのdrweb-milterの正常な動作に必要な設定は全て**Dr.Web MailD**設定ファイル内の[Sender]および[Milter]セクションで定義され、本マニュアルのSenderおよびMilterの章に記載されています。

既知の障害

詳細:

フィルタとSendmail間の通信にUNIXソケットを使用した場合に、`Milter API` ライブラリ(Sendmailと一緒に配布された)がソケットに使用されるファイルを削除しなかった(バージョン8.12.2よりも前)。

ソリューション:

バージョン8.12.xに対しては、`listener-8.12.0-1.patch`を使用することが可能です。バージョン8.11.xではこのファイルは手動で削除するか、フィルタをコントロールするスクリプト経由で削除する必要があります。この問題はSendmailバージョン8.12.2で修正されました。

詳細:

デモキーをローカルスキャンモードで使用すると、次のサーバへ送られるメッセージの`size`値がフィルタ通過時に2倍になる(メッセージ自体は変更されないか、またはバナーメッセージが追加される)。

ソリューション:

この問題はSendmailバージョン8.12.3以降で修正されました。

詳細:

フィルタが、高負荷状態のコンピューター上でアクティブになっている場合にログ内に以下のエントリがある。

`"... Milter (drweb-filter): select(read): interrupted system call"`

ソリューション:

この問題はSendmailバージョン8.12.3以降で修正されました。

詳細:

フィルタが、高負荷状態のコンピューター上でアクティブになっている場合にログ内に以下のエントリがある。

```
"... Milter (drweb-filter): select(read): timeout before data write"
"... Milter (drweb-filter): to error state"
```

ソリューション:

問題は、指定されたタイムアウト内にSendmailがフィルタとの接続を確立出来ないことにあります。バージョン8.11以降ではタイムアウトは5秒に設定され、変更することが出来ませんが、バージョン8.12以降ではフィルタの記述内で変更することが出来ます(Cの値)。

```
Xdrweb-filter, S=__ADDRESS__, F=T, T=C:1m;S:5m;R:5m;E:1h
```

Mail Postfixとの統合

主要動作原理

Dr.Web MailDとPostfixは以下に示すいずれかの方法で統合することが出来ます。

- after-queueモード(http://www.postfix.org/FILTER_README.html#advanced_filter)
- before-queueモード(http://www.postfix.org/SMTPD_PROXY_README.html)
- milterプロトコル(http://www.postfix.org/MILTER_README.html)

after-queueモードでは、**Dr.Web MailD**は以下の方法でPostfixと連携します。

SMTP/LMTPサーバとして動作するdrweb-receiverがPostfix SMTPモジュールから新しいメッセージを受信し、解析の為にdrweb-maildモジュールへ転送します。解析結果に応じてメッセージはメールシステムに送られるか(おそらく変更されたコピーとして)、ブロックされます(この場合、メールシステムに追加レポートを送信することが出来ます)。Postfixへのメールの転送は、メッセージをsmptdデーモンに配信するSMTP/LMTPクライアントとして動作するdrweb-sender経由で実行されます。

Postfixのフィルタ設定に関する詳細は、http://www.postfix.org/FILTER_README.htmlなどにあるPostfixのドキュメントを参照してください。

Dr.Web MailDはbefore-queueモードでPostfixと連携することも出来ます(システム負荷が大きい場合は推奨できません)。before-queueモードでの動作の設定に関する詳細は、http://www.postfix.org/SMTPD_PROXY_README.htmlを参照してください。

milterプロトコル経由によるPostfixとの連携は以下の方法で行います。

- drweb-milter(**Receiver**コンポーネントとして動作する)のトランスポートアドレスによって定義されたトランスポート接続経由で、PostfixがMilter APIから内部コマンドとメッセージを受け取ります。メッセージはメールセッションのステージ(helo、mail from:、rcpt to:など)に応じて、セグメントに分けられて送信され、drweb-milterモジュールによって一時ディレクトリに保存されます。drweb-milterは、メッセージに適用するアクションに関する命令をMilter API経由でPostfixに送ります。

  Milter APIはマルチスレッドライブラリで、同時に複数のメールセッションを処理することができます。上記に記載した統合スキーマにおいて、Postfixはクライアント、drweb-milterはサーバとなります。従って、Postfixのmail.cf設定ファイル内でdrweb-milterモジュールのアドレスを指定する必要があり、この接続に適したクライアントアドレスがPostfixによって選択されます。

- drweb-milterモジュールは、他のトランスポート接続経由でdrweb-maildモジュールにコマンドを送り、応答を待ちます。

上記に記載したスキーマにおいて、drweb-milterモジュールはPostfixインターフェースとdrweb-maildモジュール間のエージェントとして動作します。Postfixとdrweb-milterモジュールは別々のコンピューター上で動作することが可能ですが、drweb-milterモジュールとdrweb-maildモジュールは

同じコンピューター上で動作する必要があります。

Mail Postfix の設定

Dr.Web MailDとPostfixの連携を`after-queue`モードで設定するには、Postfixの`main.cf`設定ファイルに以下のラインを追加してください。

```
  content_filter = scan:_ADDR_REC_
  receive_override_options =
no_address_mappings
```

`_ADDR_REC_`は、例えば`127.0.0.1:8025`などの、リッスンしている`drweb-receiver`モジュールのアドレスです（**Dr.Web MailD**設定ファイル[`Receiver`]セクションの**`Address`**パラメータ）。

Postfixの`master.cf`設定ファイル内で以下のラインを追加する必要があります。

```
scan unix  -  - n - NN smtp
  -o smtp_send_xforward_command = yes
_ADDR_SEN_ inet n - n - NN smtpd
  -o content_filter =
  -o receive_override_options =
      no_unknown_recipient_checks,
      no_header_body_checks
  -o smtpd_helo_restrictions =
  -o smtpd_client_restrictions =
  -o smtpd_sender_restrictions =
  -o smtpd_recipient_restrictions =
      permit_mynetworks, reject
  -o mynetworks = 127.0.0.0/8
  -o smtpd_authorized_xforward_hosts =
      127.0.0.0/8
```

_ADDR_SEN_は、例えば127.0.0.1:8026などの、メッセージを送信する為にdrweb-senderモジュールが接続するアドレスです(**Dr.Web MailD**設定ファイル[Sender]セクションの**Address**パラメータ)。

NNの数(Postfixサーバによって実行される処理の最大数)は、drweb-receiverおよびdrweb-senderモジュールのプール内にあるスレッドの数(**Dr.Web MailD**設定ファイル[Receiver]セクションの**PoolOptions**パラメータ、および[Sender]セクションの**OutPoolOptions**パラメータ)と同じにすることを推奨します。この制限を削除するにはNNの部分に"-"(マイナス記号)を指定してください。

Dr.Web for UNIX mail serversをインストールする際に、Postfix設定ファイルに対する上記全ての変更が、configure_MTA.shスクリプトによって自動的に実行されます。従って、**Dr.Web for UNIX mail servers**とPostfixはデフォルトで、after-queueモードで動作するように設定されます。

設定ファイルに変更を適用した後、Postfixを再起動してください。

このモードでの動作には、Postfixのバージョン2.3.3以降が必要になります。

Dr.Web for UNIX mail serversとPostfixはデフォルトでafter-queueモードで連携するように設定されています。milterプロトコルを使用するには、Postfix設定ファイルを再度編集する必要があります。**content_filter**パラメータを**smtpd_milters**パラメータに変更し、master.cfファイルに加えられた全ての変更を削除してください。必要な制限はPostfix設定ファイル内で直接指定することが出来ます。

Postfixがそれを経由してdrweb-milterモジュールと連携するトランスポートアドレスはTCPソケット、またはUNIXソケットとして指定することが出来ます。

アドレスはPostfix設定ファイルmain.cfの**smtpd_milters**パラメータ内で指定します。接続をTCPソケット経由で確立する場合、パラメータ値はinet:host@port(例:**smtpd_milters**=inet:127.0.0.1:3001)の書式で設定し、UNIXソケット経由の場合はunix:pathname(pathnameはUNIXソケットへの絶対パスです)の書式で設定します。

UNIXソケットを使用する場合、Postfixがソケット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。

Postfixとdrweb-milterモジュール間のトランスポート接続アドレスも、**Dr.Web MailD**設定ファイル[Milter]セクションの**Address**パラメータ内で指定する必要があります。このパラメータの書式と値はmain.cfファイルのsmtpd_millersパラメータのものと同一にしてください。

トランスポートアドレスの他に、以下のパラメータをmain.cf設定ファイル内で指定してください。

- **milter_content_timeout** = 300s - Postfixのこのタイムアウトは非常に重要で、**Dr.Web MailD**が**BeforeQueueFilters**モードでメッセージを検査する際にかかる時間の上限を定義します。このパラメータの値は**Dr.Web MailD**設定ファイル[Milter]セクションの**ProcessingTimeout**パラメータの値よりも大きくしておくことを推奨します。
- **milter_default_action** = tempfail - このパラメータは、drweb-milterモジュールとの連携中にエラーが生じた場合にPostfixがとるアクションを定義します。
- **milter_protocol** = 6 - milterプロトコルの、必要とされるバージョン
- **milter_mail_macros** = _ - このパラメータによって、**Dr.Web MailD**が送信者のIPアドレスおよびホスト名を取り出すことが出来ます。
- **milter_end_of_data_macros** = i auth_type - このパラメータによって、メッセージに関する情報をdrweb-milterログに追加する認証に関する情報、およびメッセージIDを取り出すことが出来ます。

Dr.Web MailDの設定

Dr.Web MailDの動作もまた、設定する必要があります。**Dr. Web Monitor**を使用して**Dr.Web**を起動した場合、drweb-milterモジュールは**Receiver**コンポーネントとして起動されなくてはなりません。そのためには、drweb-milterモジュールを起動するためのラインを%etc_dir/monitor/maild_postfix.mmcからアンコメントしてください。また、drweb-receiverモジュールを起動するためのラインをコメントアウトすることも推奨します。その結果、drweb_postfix.mmcには同じラインが含まれる事になります。

```
# drweb-receiver local:%var_dir/ipc/.agent 15 30 MAIL drweb:drweb
drweb-milter local:%var_dir/ipc/.agent 15 30 MAIL drweb:drweb
```

drweb-senderモジュールの動作も設定してください。**Dr.Web MailD**設定ファイル[Sender]セクションで以下のパラメータを指定してください。

```
Address = /usr/local/sbin/sendmail
Method = pipe
MailerName = postfix
```

Addressパラメータでは、Postfixパッケージからsendmailプログラムへのパスを設定します。

Dr.Web MailD設定ファイル[Sender]セクションの**SecureHash**パラメータの値も指定する必要があります(任意の記号からなるストリングをこのパラメータの値として設定することができ、記号は10個以上が推奨されます)。また、このセクション内の**UseSecureHash**パラメータにはYes値を指定してください。

必要なパラメータを全て指定した後は**Dr.Web MailD**を、次にPostfixを(再)起動してください。

drweb-milterと**Sender**および**Receiver**コンポーネントとの正常な動作に必要な設定は全て、**Dr.Web MailD**設定ファイルの[Receiver]、[Sender]、および[Milter]セクションで定義され、本マニュアルのReceiver、Sender、Milterの章に記載されています。

Exim MTAとの統合

Dr.Web MailDがEximメールシステムと連携する場合、drweb-receiverモジュールは**Receiver**コンポーネントとして動作し、drweb-senderモジュールは**Sender**コンポーネントとして動作します。Eximを**Dr.Web MailD**と接続するには2つの方法があります。

- special transportによる接続

  長所: Eximを再コンパイルする必要が無く、システムが、比較的古いバージョンのEximとも動作することが出来る。

短所: システムパフォーマンスの低下。

- Eximの`local_scan`による接続。この場合**Receiver**は、他のコンポーネントとは異なり、**Dr.Web Agent**からではなくEximメールシステムの設定ファイルから設定データを受け取ります。

  長所: システムパフォーマンスの向上。

  短所: Eximを再コンパイルする必要があり、Eximはバージョン4.50以降でなくてはならない。

Exim MTAの設定

初期設定は、どちらの接続方法の場合でも同じです。

まず最初に、Exim設定ファイルの`MAIN CONFIGURATION SETTINGS`セクション内で、信頼できるユーザのリストに`drweb`ユーザを加える必要があります。

```
------------------ cut -----------------------
##############################################
#           MAIN CONFIGURATION SETTINGS       #
##############################################

trusted_users = drweb
------------------ cut -----------------------
```

Eximが、`drweb-sender`からメッセージを受け取った直後にメールの配信を実行し、その過程で重大な遅延が生じた場合(例:SMTPを使用している際に)、`[Sender]`セクションの**PipeTimeout**パラメータで指定されたタイムアウトが適用されることがあるので注意してください。Eximは配信が完了するまで受信成功のコードを`drweb-sender`に返さないからです。この問題を回避するために、最初に全てのメッセージをキューに送信し、その後で配信を実行するようにEximを設定することが出来ます。

Exim設定ファイルに新しい`acl`を追加します。

```
acl_check_drweb_scanned:
warn
```

```
condition = ${if and {{def:received_protocol}
{eq {${received_protocol}}\
{drweb-scanned}}} {yes}{no}}
control = queue_only
accept
```

その後、それを有効にしてください。

```
acl_not_smtp = acl_check_drweb_scanned
```

以下の記述はExim4.xxに対してのみ有効です。それ以前のバージョン(3.xx)の設定を調整する方法は、該当するドキュメント(http://www.exim.org/index.htmlなど)を参照してください。

Exim設定内でspecial transportまたはルーターを追加する必要があります。メールシステムの設定ファイル内でRouters Configurationセクションを探してください。以下のヘッダで始まっています。

```
------------------ cut -----------------------
##############################################
#        ROUTERS CONFIGURATION               #
# Specifies how remote addresses are handled #
##############################################
#          ORDER DOES MATTER                 #
#   A remote address is passed to each in    #
#       turn until it is accepted.           #
##############################################

begin routers
```

というラインの直後に、以下の記述を追加してください。

```
drweb_router:
  driver = accept
   condition = "${if eq {$received_protocol}
{drweb-scanned}{0}{1}}"
# check_local_user
```

```
  retry_use_local_part
  transport = drweb_transport
```

受信者のチェックが必要な場合、check_local_userパラメータをアンコメントしてください。

Exim設定ファイル内で、トランスポートが記述されているセクションを探してください。以下のヘッダで始まっています。

```
------------------ cut -----------------------
##############################################
#     TRANSPORTS CONFIGURATION               #
##############################################
#        ORDER DOES NOT MATTER               #
#  Only one appropriate transport is called  #
#          for each delivery.                #
##############################################
------------------ cut -----------------------
```

このセクションに、必要なトランスポートの記述を追加してください。

```
drweb_transport:
  driver = lmtp
  socket = __ADDRESS__
  batch_max = 100
  timeout = 5m
  user = drweb
# headers_add = "X-Maild-Checked: DrWEB for Exim"
```

_ADDRESS_は、UNIXソケット%var_dir/ipc/.drweb_maildなどの、drweb-receiverのリッスンモジュールのアドレス(**Dr.Web MailD**設定ファイル内[Receiver]セクションの**Address**パラメータ)です。

次に、**Dr.Web MailD**設定ファイル内[Sender]セクションの**Address**パラメータ内でEximへのパスを指定し(例:/usr/exim/bin/exim/)、同じく[

Sender] セクションの**MailerName**パラメータの値にEximを指定してください。

変更が全て終了した後、**Dr.Web MailD**とEximを再起動してください。

このモードで**Dr.Web MailD**と連携するには、Eximのバージョンが4.50以降である必要があります。

まず最初に、 local_scan機能に対応したEximを再コンパイルしてください。
First, you must recompile Exim with support of local_scan function:

- %bin_dir/doc/maild/local_scan/local_scan.c を exim*/Local/ ディレクトリにコピーします。
- %bin_dir/doc/maild/local_scan/Makefile.sample内で指定されたパラメータを、exim*/Local/ディレクトリ内にあるEximのMakefileに加えます。該当するパラメータが既にMakefile内で指定されている場合は、それらをアンコメントして編集することが出来ます。
- EximのMakefile内では、Eximの起動に権限を使用したユーザの名前も指定する必要があります(**Dr.Web MailD**に指定された名前と同じにしてください)。ユーザ名は**EXIM_USER**パラメータによって定義され、デフォルトでは**EXIM_USER** = drwebです。
- Eximをコンパイルし、インストールします。makeまたはmake installコマンドの実行が、以下のようなメッセージを出して中断された場合、
  /libexec/ld-elf.so.1: Shared object "libgcc_s.so.1" not found, required by "libboost_thread.so"

  修正する方法は2つあります。

  - ライブラリlibstdc++.so.6およびlibgcc_s.so.1を、%bin_dir/lib/からシステムのライブラリがあるディレクトリにコピー(またはそれらへのリンクを作成)することが出来ます。
  - 以下のコマンドをコンソールから実行することが出来ます。

    ```
    $ export LD_LIBRARY_PATH=%bin_dir/lib/:$LD_LIBRARY_PATH
    ```

Eximを再度コンソールからコンパイルし、インストールしてください。

次に、Eximシステムを設定してください。クイック設定には%bin_dir/doc/maild/local_scan/configure.sampleファイルのパラメータの値を使用することが出来ます。必要なラインをExim設定ファイルのlocal_scanセクションにコピーするだけです。

コンポーネントの設定に関する情報を検索するには、以下のコマンドをコンソールから実行してください。

```
$ PATH_TO_BIN_DIR/exim -bP local_scan
```

PATH_TO_BIN_DIRはEximバイナリへのパスです。

Dr.Web MailDの設定

Eximとの連携の為に**Dr.Web MailD**を設定するには**Dr.Web MailD**設定ファイル[Sender]セクションの**Address**パラメータ内でEximメールシステムへのパスを指定(例:/usr/exim/bin/exim/)し、同セクションの**MailerName**パラメータの値にEximを設定してください。

local_scan機能を介して動作が実行されている場合、**Receiver**モジュールはEximに組み込まれているので、drweb-receiverモジュールを別々に起動する必要はありません。**Dr.Web Monitor**を使用して**Dr.Web MailD**を起動した場合、drweb-receiverを起動するライン%etc_dir/monitor/maild_exim.mmcをコメントアウトしてください。

```
#drweb-receiver local:%var_dir/ipc/.agent 15 30 MAIL drweb:drweb
```

変更が全て終了した後、**Dr.Web MailD**とEximを再起動してください。

Dr.Web MailDとEximとの正常な動作に必要な設定は全て、**Dr.Web MailD**設定ファイル[Receiver]および[Sender]セクションで定義され、本マニュアルのReceiverおよびSenderの章に記載されています。

既知の障害

Eximの再起動時に以下のようなエラーが表示された場合、

transport drweb_transport: cannot find transport driver "lmtp"

LMTPトランスポートサポート無しで設定されたことを意味します。LMTPトランスポートに変更するか(詳細についてはhttp://www.exim.org/などの、Exim MTAに関するドキュメントを参照してください)、EximをLMTPトランスポートサポートと一緒に再コンパイルしてください。後者の場合、Eximシステムの/Local/Makefileファイル内で **TRANSPORT_LMTP** = yesのラインを追加するかアンコメントする必要があります。

qmail MTAとの統合

qmailの動作の原理は、メールシステムをオーバーライドするということに基づいています(proxying)。qmail-queueモジュールのインターフェースセット経由で、フィルタがメッセージを受信して検査を行い、感染していなければそれをqmail-queueに移します。

このモードでの動作には次の制限があります。drweb-qmailが検査要求をリッスンするUNIXソケット(**Dr.Web MailD**設定ファイル[Qmail]セクションの**ListenUNIXSockets**パラメータ内で設定します)が、一定のパスの範囲内に置かれていなくてはなりません。パスのリストを表示するには、qmail-queueを--helpコマンドラインパラメータで実行してください。

Dr.Web MailDとの連携にはqmailのバージョン1.03以降が必要です。受信するメールが失われるのを防ぐため、フィルタをインストールするのはqmailが停止している時のみにしてください。

qmailの設定

Dr.Web MailDをqmailに接続するには、以下の手順を実行してください。

- オリジナルのqmail-queueファイルを保存します。後ほど必要になるので、保存場所を覚えておいてください。
- qmail-queueを%bin_dirディレクトリから/qmail/bin/にコピーします。新しいqmail-queue(**Dr.Web MailD**のフィルタ)、およびコピーしたqmail-queue.originalに適切な権限を設定するのを忘れないようにしてください。

drwebユーザの権限で**Dr.Web MailD**およびqmail-queueが動作している設定を使用することを推奨します。この設定の正常な動作を確実なものにした

い場合、qmail-queueに以下の権限を設定してください。

```
-rws--x--x X drweb qmail SIZE DATE qmail-queue
-rws--x--x X qmailq qmail SIZE DATE qmail-queue.original
```

以下のコマンドを使用します。

```
$ chown drweb:qmail qmail-queue
$ chmod 4711 qmail-queue
$ chown qmailq:qmail qmail-queue.original
$ chmod 4711 qmail-queue.original
```

Dr.Web MailDの設定

Dr.Web MailDとqmailとの正常な動作に必要な設定は全て、**Dr.Web MailD**設定ファイル[Sender]および[Qmail]セクションで定義され、本マニュアルのSenderおよびQmailの章に記載されています。

既知の障害

詳細:

起動時に、qmailが以下のエラーのうちいずれかを返す。

1. terminate called after throwing an instance of 'St9bad_alloc'
   what(): St9bad_alloc
2. bash: xmalloc: cannot allocate 2 bytes (0 bytes allocated)
3. qmail-queue.real: error while loading shared libraries: libc.so.6: failed to map segment from shared object: Cannot allocate memory
4. /var/qmail/bin/qmail-smtpd:
   error while loading shared libraries:

```
libc.so.6: failed to map segment from shared object:
Cannot allocate memory
```

ソリューション:

この問題は、起動スクリプトで使用されるメモリの上限が高すぎるのが原因です。Dave Sillスクリプトを使用する場合を例に挙げると、命令softlimit -m 2000000内の値は、例えば0を、右に足すことによって増やして(20000000に)ください。

詳細:

SMTPプロトコル経由で受信した全てのメッセージに対する応答として、qmailが以下のようなストリングを返す。

```
451 qq trouble making network connection (#4.3.0)
```

ソリューション:

qmail-queueが、drweb-qmail(**Dr.Web MailD**の**Receiver**コンポーネントとして動作する)によって作成されたUNIXソケットに接続する為の十分な権限を持っていないか、qmail-queueにデフォルトで指定されたパスがこのソケットへのパスではない可能性があります。権限を確認し、**Dr.Web MailD**設定ファイル[Qmail]セクションの**ListenUNIXSocket**パラメータの値がデフォルトのパス(パスのリストはqmail-queueを--helpコマンドラインパラメータで実行することで入手できます)と一致するようにしてください。

詳細:

SMTPプロトコル経由で受信したそれぞれのメッセージに対して、メッセージ本文を受信した際にqmailがコンソールに以下のようなストリングを返す。

```
qmail-inject: fatal: qq temporary problem (#4.3.0)
/usr/libexec/ld-elf.so.1: Shared object "libstdc++.so.6" not found,
```

```
required by "libboost_program_options.so"
```

ソリューション:

システムは、%bin_dir/lib/ディレクトリ内にある必要なライブラリを見つけることが出来ません。libstdc++.so.6ライブラリとlibgcc_s.so.1ライブラリを、%bin_dir/lib/からライブラリのあるシステムディレクトリにコピーする必要があります(またはそれらのライブラリへのシンボリックリンクを作成してください)。

ZMailer MTAとの統合

drweb-zmailerモジュールは、ZMailer v. 2.99.55以降とのみ互換性があります。**Dr.Web MailD**は以下の2つのモードでZMailerと連携することが出来ます。

- SMTP接続段階でコンテキストフィルタとして

  長所: SMTP接続段階でメッセージをブロックすることができる。

  短所: SMTP接続のみが検査されシステム負荷が高い場合、パフォーマンスが低下。

- ルーティング段階でコンテキストフィルタとして

  長所: ZMailerを介して受信する全てのメール(ローカルメール、およびUUCPプロトコル経由で転送されたメールを含む)を検査し、システム負荷が高い場合にも安定したパフォーマンス。

  短所: メッセージを受信時にブロック出来ない(rejectおよびtempfailアクションはdiscardと同じです)。パフォーマンスを向上させ、メッセージループを防ぐために**SecureHash**の使用が必要。

ZMailerとの連携ではdrweb-zmailer モジュールは**Dr.Web MailD**の**Receiver**コンポーネントとして使用されます。

drweb-zmailerとフィルタの正常な動作を確実なものにしたい場合は、パッチをインストールすることを推奨します(可能な場合)。

パッチをインストールする方法は以下のとおりです。

- $(ZMAILER_SRCHOME)/smtpserver(ZMAILER_SRCHOMEはZMailerバイナリのあるディレクトリへのパスです)ディレクトリを開きます。
- 以下のコマンドを実行してください。

```
$ patch < smtpdata.c.XXX.patch
```

XXXは、パッチを適用するZmailerのバージョンです。

SMTP接続段階でのコンテキストフィルタモード

SMTP接続段階で**Dr.Web MailD**とZMailerを統合する方法は以下のとおりです。

- drweb-zmailer.shを$MAILBINディレクトリにコピー(またはシンボリックリンクを作成)します(ファイルへのパスはzmailer.conf内で指定します)。
- smtpserver.confファイルにPARAM contentfilter $MAILBIN/drweb-zmailer.shのラインを加えて編集してください。

コマンドラインパラメータはcontentfilter内で指定することが出来ないので、drweb-zmailer.shスクリプト内で定義する必要があります。

ルーティン段階でのコンテキストフィルタモード

メールサーバによって処理されるメッセージは全て、ルーティング段階を通過します。そのため、ルーティング段階の最後はフィルターを接続するのに最も適しています。接続を可能にするには、$MAILBIN/cf/process.cfを以下のように編集します。

以下のラインを探してください。

```
LOGMSG=()     # This is a LIST of files where to log..
#|    The LOGMSG variable is used by the intercept facility (in crossbar.cf)
#|    to make sure only a single copy of a
```

```
message is saved when required.
#|   Each sender - recipient address pair can
cause an intercept which can
#|   specify a file to save the message to.
 This variable is appended to
#|  elsewhere, and processed at the end of this
function.
```

その下に以下の内容を追加します。

```
###-> Dr.Web MailD support
ch='"DEFAULT_BIN_PATH/drweb-zmailer.sh"  --hash
__EDIT_THIS__ --file $POSTOFFICE/router/$file'
      case  "$ch" in
            -1*) #reject or disacrd
                  /bin/rm -f "$file"
                  return
                  ;;
            1*) #tempfail
                  /bin/rm -f "$file"
                  return
                  ;;
            *);;
      esac
###-> end of Dr.Web MailD support
```

_EDIT_THIS__(--hashパラメータの値)には、**Dr.Web MailD**設定ファイル[Sender]セクションの**SecureHash**パラメータと同じ値を設定し、同セクションの**UseSecureHash**パラメータの値にYesを指定します。

追加設定

送信者のSMTPエンベロープが空であるメッセージ(通常、エラーメッセージや、配送に失敗したことを通知するメッセージが空のSMTPエンベロープで送信されます。また、スパマーからもそのようなメッセージが送信されます)の受信を無効にする簡

単な方法はpolicytest.c.XXX.patchをインストールすることです。インストール手順はsmtpdata.c.XXX.patchの場合と同じです。

ZMailerがdrweb-zmailerモジュールを起動する度に新しいメッセージが処理されます。システムパフォーマンスを最適化するために、drweb-zmailerの全ての設定をコマンドライン内で指定する必要があります（例えばdrweb-zmailer.shスクリプト内で定義することが出来ます）。

drweb-zmailerのコマンドライン内では以下のパラメータを指定することが出来ます。

- -h [--help] - ヘルプを表示して終了します。
- -v [--version] - バージョンを表示して終了します。
- -u [--user] arg (=drweb) - drweb-maildの起動に権限を使用したユーザの名前です。

  ZMailerはデフォルトで、root権限でdrweb-zmailerを起動するので、**Dr.Web MailD**全体をroot権限で起動する（さらに、このパラメータの値に空のラインを設定します-u ""）か、またはこのパラメータに必要な値を指定する必要があります。

- -l [--level] arg (=info) - ログの詳細レベルです。可能な値はQuiet、Error、Alert、Info、Debugです。
- -i [--ipclevel] arg (=info) - IPCログの取得レベルです。 可能な値はQuiet、Error、Alert、Info、Debugです。
- -f [--facility] arg (=mail) - ロギングにsyslogdを使用する場合のログの種類です（syslogのファシリティ）。可能な値はDaemon、Mail、Local0-7です。
- -b [--basedir] arg (=%var_dir) - **Dr.Web MailD**のメインの動作ディレクトリです。このパラメータの値は**Dr.Web MailD**設定ファイル[General]セクションの**BaseDir**パラメータの値と同じです。
- -t [--timeout] arg (=30) - 1つのメッセージを処理する時間の上限。
- --file arg - 処理するファイルへのパスです。コンテキストフィルタモードでのルーティング段階でのみ指定してください。
- --hash arg - **Dr.Web MailD**設定ファイル[Sender]セクショ

ンの**SecureHash**パラメータの値です。コンテキストフィルタモードでのルーティング段階でのみ指定してください。

- `--interface arg (=1)` - smtpserverのバージョンです。コンテキストフィルタモードでのSMTP接続段階でのみ指定してください。0はバージョン2.99.55以前、1はバージョン2.99.56以降です。
- `-e [ --error-action ] arg (=reject)` - フィルタの動作中に内部エラーが生じた際に、メッセージに適用するアクションの指定です。可能な値は`pass`、`reject`、`discard`、`tempfail`です。

Courierとの統合

Courierの設定

Dr.Web MailDとCourierを統合する方法は以下の通りです。

1. 以下のコマンドを実行して`drweb-courier`モジュールに対する権限を設定してください。

```
$ chown COURIER_USER:drweb "DEFAULT_BIN_PATH/drweb-courier"
$ chmod 6771 "DEFAULT_BIN_PATH/drweb-courier"
```

   `COURIER_USER`は、Courierの起動に権限を使用したユーザです。また、全てのディレクトリ、および`drweb`グループの`%var_dir`ディレクトリ内にある全てのサブディレクトリに対して書き込み、読み取り、実行のパーミッションが設定されているようにしてください。

2. `drweb-courier`モジュールをCourierフィルタディレクトリ(デフォルトでは`/usr/local/libexec/filters/`です)にコピー(またはsymlinkを作成)します。
3. drweb-courierモジュールをCourierにグローバルとして登録します。

```
$ /usr/local/sbin/filterctl start drweb-courier
```

   後でフィルタを無効にする場合は、以下のコマンドを実行してください。

```
$ /usr/lib/courier/sbin/filterctl stop
```

drweb-courier

4. 検査を実行するサービスを設定する為にenablefilteringファイルを作成、または編集します(esmtpまたはuucp、複数指定する場合は空白で区切って列挙します)。
5. **Dr.Web MailD**設定ファイル[Courier]セクションの**BaseDir**パラメータおよび**SocketDirs**パラメータが、お使いのCourierメールシステムの設定と一致していることを確認してください。詳細については、man courierfilterコマンドを実行してください。
6. Courierのフィルタリングを有効にします。

```
$ /usr/lib/courier/sbin/courierfilter start
```

Dr.Web Daemonの動作に権限を使用しているdrwebユーザは、Courierによってスプール内に作成されたファイルに対する読み取り権限を得るために、courierグループに含まれている必要があります。

Dr.Web MailDの設定

Dr.Web MailDとCourierとの正常な動作に必要な設定は全て、**Dr.Web MailD**設定ファイル[Sender]および[Courier]セクションで定義され、本マニュアルのSenderおよびCourierの章に記載されています。

Proxyの使用

Dr.Web for UNIX mail serversに含まれているプロキシによって、コンピュータリソースの管理に関する目的を達成することが可能です。

1. メールの処理や検査の操作を異なるホスト上で実行出来るように**Receiver**モジュールと**Sender**モジュールがdrweb-maildモジュールと別々に動作しているため、**Dr.Web for UNIX mail servers**の効率を大幅に向上させることが出来ます。
2. ロードバランシングスキーマN:M(Nはメールトラフィックを処理するホストの数、Mはメールにウイルスやスパムが無いかをチェックするホストの数です)を使用することで、ネットワーク内のコンピューティングリソースを柔軟に管理できます。

drweb-maildコンポーネントはクラスタの導入には対応しておらず、相互間で内部データ(統計、隔離、データベース設定など)を共有出来ないので注意してください。その結果、各drweb-maildコンポーネントはそれぞれ独自の統計、隔離、および設定を持つことになります。

プロキシはdrweb-proxy-clientとdrweb-proxy-serverのコンポーネントで構成されています。

- drweb-proxy-client - **Receiver**および**Sender**コンポーネントが動作しているコンピュータ上で動作します。drweb-maildの代わりに起動し、他のコンポーネントとの連携においてdrweb-maildと同じ役割を果たします。
- drweb-proxy-server - drweb-maildモジュールが動作しているコンピューター上で動作し、、**Receiver**および**Sender**コンポーネントと同じ役割を果たします。

drweb-proxy-clientと drweb-proxy-serverコンポーネントはお互いに連携し、オリジナルのメールメッセージ及びそれらの変更されたものを、以降のプロセスの為に、異なるホスト上にある**Dr.Web for UNIX mail servers**の他のコンポーネントに送ることが出来ます。

drweb-notifier、drweb-monitor、およびdrweb-agentコンポーネントはそれぞれのホスト上で動作しています。

proxyを使った一般的な操作スキーマは次のようになります。

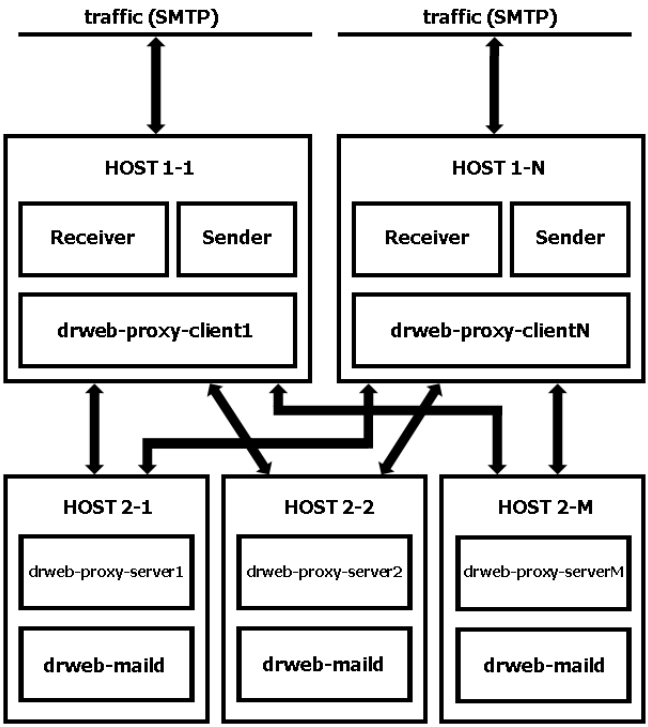


図16.proxy経由での操作図解

スキーマから分かる通り`drweb-proxy-client`と`drweb-proxy-server`はどちらも、異なるホスト上にある任意の数の補助コンポーネントと連携することが出来ます。これは特別なバランスシステムを使用することによって実行されます。

`ProxyServersAddresses`または**`ProxyClientsAddresses`**パラメータ(それぞれ`[ProxyClient]`、`[ProxyServer]`セクション)の値で指定されたソケットアドレスにはそれぞれ重量が割り当てられます。したがって、アドレスは次の書式で指定されます。

```
ADDRESS1 [WEIGHT1], ADDRESS2 [WEIGHT2] ..
```

ADDRESSにはベーシックなアドレスが入ります。WEIGHTは0から100までのオプション数値で、このアドレスの重量を定義します。このWEIGHTはネットワーク内にある特定のホスト上の相対的ワークロードを定義します。値が大きいほどそのサーバーのロードが大きいことを意味します。

[ProxyClient]セクションの**ProxyServersAddresses**パラメータは、drweb-proxy-server*コンポーネントがリクエストを受け取るのに使用するHOST2-*のアドレス(上記のスキーマ参照)を指定します。

[ProxyClient]セクションの**ProxyClientsAddresses**パラメータは、drweb-proxy-client*コンポーネントがリクエストを受け取るのに使用するHOST1-*のアドレス(上記のスキーマ参照)を指定します。

例:

ProxyServersAddresses = inet:8066@10.3.0.73 10, inet:8066@10.3.0.72 5

この場合、10.3.0.73ホストは10.3.0.72ホストの2倍のメールメッセージを受け取ります。WEIGHTが指定されていない場合は、デフォルトで1と見なされます。複数のアドレスが同じWEIGHTを持っている場合、それらは同等と見なされ同じ数のリクエストを受け取ります。

WEIGHTが0に設定されている場合、そのようなアドレスはバックアップアドレスと見なされます。1またはそれよりも大きいWEIGHTを持つ利用可能なアドレスが残っていない場合のみ、それらのアドレスにリクエストが送られます。一般的なアドレス選択アルゴリズムは以下のようになります。

1. 最も大きなWEIGHT値を持つアドレスへのメッセージ送信が試行されます。エラーが生じた場合、それよりも少ないWEIGHTを持つ次のアドレスが選ばれます(このWEIGHTは1またはそれよりも大きい必要があります)。利用可能なWEIGHT ≥ 1のアドレスが残っていない場合は、バックアップアドレスが使われます(手順のp.3)。
2. 選択したアドレスへのメッセージ送信が試行されます。エラーが生じた場合、このアドレスは利用できないものと見なされ、手順が初めから繰り返されます(手順のp.1)。
3. WEIGHTが0より大きいアドレスが全て利用できないと分かった場合、バックアップアドレスへのメッセージ送信が試行されます。バックアップアドレスはリストに載っている順番にチェックされます。バックアップアドレスも利用不可能だった場合は、エラーが返ってきます。

WEIGHT値は、それぞれのサーバー上の利用可能なリソースに応じて選択し、 割り当ててください。

メッセージは検査の為にdrweb-maildモジュールに送られ、**BeforeQueue**のプラグインによって処理された後、全て送信元のクライアントに返されます。

メッセージが**AfterQueue**のプラグインによって処理された場合、その処理済みメールを受け取るクライアントのアドレスは、**ProxyClientsAddresses**内のクライアントアドレスの重量に応じて選択されます。

重複するメッセージ(Rulesの記述参照)およびdrweb-maildによって作成されたメッセージ(レポート、通知)もまた、プラグインがあるキューに関係なく、**ProxyClientsAddresses**のリストから選択されたクライアントに送られます。

ProxyClientsAddressesリストから選択されたクライアントに送信されるメッセージには、Rules内で指定された設定(もしあれば)が適用されます(例えば**SenderAddress**パラメータの値)。

proxyがMilter、Qmail、またはCourierMTA(したがってdrweb-milterモジュールと)と連携する際には、プラグインを**AfterQueue**に置かない方がいいという点に注意してください。現時点ではproxyは**Receiver**コンポーネントへのバックドアコネクションに対応していません。そのため、drweb-maildからの応答がすぐに**Receiver**に返って来なかった場合(例えばプラグインが**AfterQueue**内にある場合)、drweb-milterは**ProcessingTimeout**の期限が切れた後にのみSMTPセッションを終了します。

M=N=1に対する最適な(ただし、可能なものはこれだけではありません)接続手順を下記に記します。これによって、セットアップおよび調整の際に起こりうる失敗の大半を防ぐことが出来ます。

M=N=1の場合は以下の手順でproxyをセットアップしてください(方法は他にもありますが、設定の際に生じるエラーを防ぐ為にこの方法を推奨します)。

1. HOST1-1上(つまり、メールトラフィックの処理に使用し、drweb-proxy-clientコンポーネントがあるホスト上)の**Dr.Web MailD**をセットアップ、調整します。以下のコマンドで設定の妥当性をチェックして下さい。

- /etc/init.d/drweb-monitor check - LinuxおよびSolaris
- /usr/local/etc/rc.d/00.drweb-monitor.sh check - FreeBSD

2. HOST1-1上の**Dr.Web MailD**を実行し、メールが正常に処理されているかチェックして下さい。
3. HOST2-1上（つまり、メールメッセージのチェックに使用し、drweb-proxy-serverコンポーネントがあるホスト上）の**Dr.Web MailD**をセットアップします。**Receiver**および**Sender**コンポーネントはこのホスト上では必要ないので、セットアップの際にその調整をスキップすることができます。
4. HOST1-1と同様にHOST2-1上の設定を調整してください。
5. HOST2-1上にある%etc_dir/monitorディレクトリのmmcファイルから該当するラインをコメントアウトして**Receiver**および**Sender**コンポーネントのスタートアップを無効にしてください。drweb-proxy-serverコンポーネントのスタートアップは有効にする必要があります。

同じホスト上でdrweb-proxy-server と **Receiver**/**Sender**コンポーネントを同時にスタートさせようとした場合、**Dr.Web Monitor**は動作を終了し、どのコンポーネントも起動されないので注意してください。このエラーに関する情報はログに出力されます。

6. HOST2-1上にある**Dr.Web MailD**設定ファイル[ProxyServer]セクションの**ProxyClientsAddresses**パラメータの値としてHOST1-1のIPアドレスを指定します。このアドレスは[ProxyClient]セクションの**Address**パラメータの値と同一にしてください。メールはそこに送信されます。
7. HOST2-1上の設定の妥当性を以下のコマンドでチェックして下さい。
   - /etc/init.d/drweb-monitor check - LinuxおよびSolaris
   - /usr/local/etc/rc.d/00.drweb-monitor.sh check - FreeBSD

全て正しく設定されていれば、HOST2-1上で**Dr.Web MailD**を起動することが出来ます。

8. HOST1-1上にある**Dr.Web MailD**設定ファイル内[ProxyClient]セクションの**ProxyServersAddresses**パラメータの値としてHOST2-1のIPアドレスを指定します。このアドレスは[ProxyServer]セクションの**Address**パラメータの値と同一にして

ください。メッセージ検査のリクエストはそこに送信されます。

9. HOST1-1上にある%etc_dir/monitorディレクトリのmmcファイルから該当するラインをコメントアウトしてdrweb-maildコンポーネントのスタートアップを無効にしてください。drweb-proxy-clientコンポーネントのスタートアップは有効にする必要があります。

同じホスト上でdrweb-proxy-client とdrweb-maildコンポーネントを同時にスタートさせようとした場合、**Dr.Web Monitor**は動作を終了し、どのコンポーネントも起動されないので注意してください。このエラーに関する情報はログに出力されます。

10. HOST1-1上の設定の妥当性を以下のコマンドでチェックして下さい。
    - /etc/init.d/drweb-monitor check - LinuxおよびSolaris
    - /usr/local/etc/rc.d/00.drweb-monitor.sh check - FreeBSD

全て正しく設定されていれば、**Dr.Web MailD**を再起動することが出来ます。今後は全てのメールが検査の為にHOST2-1に転送されます。

11. HOST1-1上の**Dr.Web Daemon**および**Dr.Web Updater**はもう必要ないので無効にしても構いません（システム上にそれ以上**Dr.Web**製品が無い場合）。

Mおよび／またはNが1よりも大きい場合も、このアルゴリズムを適用することが出来ます。上記の通りに追加のホストを接続し、それらのホスト上にある設定ファイル内の該当するパラメータの値（[ProxyServer]セクションの**ProxyClientsAddresses**および[ProxyClient]セクションの**ProxyServersAddresses**）を編集してください。

WEIGHT値は、それぞれのホスト上の利用可能なリソースの量に応じて設定する必要があります。

Dr.Web console for UNIX mail servers

Dr.Web for UNIX mail servers は **Dr.Web console for UNIX mail servers** を使用することでWebインターフェースによる設定が行えます。WebインターフェースはWebminのプラグインとして実装されます。

Webminの詳細については、Webminのサイトを参照してください。 (http://www.webmin.com/).

Dr.Web console for UNIX mail servers は、以下のPerlモジュールを必要とします:

- `XML::Parser` - XML文書の構文解析用モジュール
- `JSON::XS` - JSON(JavaScript Object Notation)を用いたデータ変換モジュール
- `XML::XPath` - XPath式の解析・評価用モジュール
- `Text::Iconv` - `iconv()`のPerlインターフェース用モジュール
- `perl-devel` 、もしくは `libperl-dev` (利用しているUnix環境によって異なります) - `Text::Iconv`をビルドするパッケージ
- `Date::Parse` - 日付のUNIXフォーマット変換用モジュール
- `CGI` - CGIモジュール
- `CGI::Carp` - HTTPDエラーレポート作成用モジュール
- `MIME::Words` - RFC 2047エンコード用モジュール
- `MIME::Base64` - Base64エンコード用モジュール
- `MIME::QuotedPrint` - quoted-printableエンコード処理用モジュール
- `MIME::Entity` - MIMEメッセージのデコードと処理用モジュール
- `MIME::Parser` - MIME解析処理用モジュール
- `MIME::Head` - MIMEメッセージのヘッダ処理用モジュール
- Storable - データ構造体の永続化用モジュール
- `POSIX` - POSIXシステムコマンドへのアクセス用モジュール
- `Digest::MD5` - MD5暗号化アルゴリズム用モジュール
- `Encode` - エンコード用モジュール
- `Encode::Byte` - シングルバイト文字エンコード用モジュール

- `Encode::JP` - 日本語エンコード用モジュール
- `File::Stat` - 組み込み関数 stat()用インターフェースモジュール
- `File::Find` - ディレクトリツリーサーチ用インターフェースモジュール
- `Encode::CN` - 中国語エンコード用モジュール
- `Encode::HanExtr` - 中国語エンコードの予備セットモジュール

モジュールがない場合は、コンソールからのインストールをお勧めします。モジュール名が異なる場合もありますが、ほとんどの以下のパッケージに含まれています:

`perl-Convert-BinHex, perl-IO-stringy, perl-MIME-tools, perl-XML-Parser, perl-XML-XPath`

rpm でインストールを行う場合は、`noarch.rpm`パッケージの使用をお勧めします。

以下のコマンドによってモジュールのインストールが可能です (利用しているOSによって異なります)。

Debian/Ubuntu:

```
apt-get install libjson-perl libjson-xs-perl
libxml-parser-perl libxml-xpath-perl
libtimedate-perl libmime-tools-perl
```

root権限が必要です。

Red Hat/Fedora/CentOS 5:

```
yum install perl-JSON perl-JSON-XS perl-XML-
Parser perl-XML-XPath perl-TimeDate perl-MIME-
tools
```

root権限が必要です。

その他のOS:

```
cpan JSON JSON::XS XML::Parser XML::XPath
Date::Parse MIME::Words MIME::Entity MIME::
Parser MIME::Head
```

root権限が必要です。

Webminのバージョンと使用しているWebブラウザによってWebインターフェースのレイアウトが異なることがあります。本書では、以下の環境で取得したスクリーンショットを使用しています。

Webmin 1.480

Firefox 3.0.7 (Mozilla/5.0 (Windows; U; Windows NT 5.1; ru; rv:1.9.0.7) Gecko/2009021910 Firefox/3.0.7) デフォルト設定

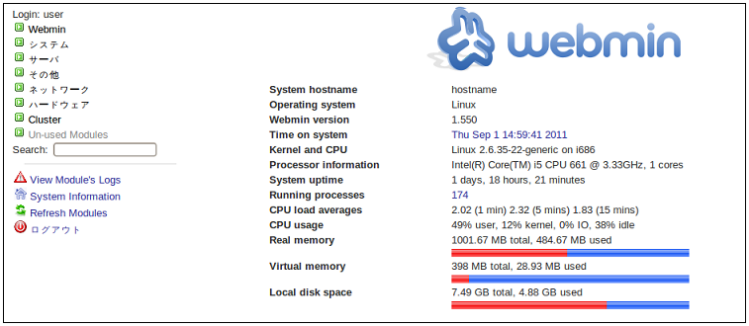
インストール

Dr.Web console for UNIX Mail Servers のインストールは以下の手順で行います。

- Webmin のインストール
- Webminのプラグインモジュール **Dr.Web console for UNIX Mail Servers** のインストール(`%bin_dir/web/`)

Webminの設定、モジュールのインストールは、WebminのWebインターフェースで行います。

図 17. Webmin メインページ



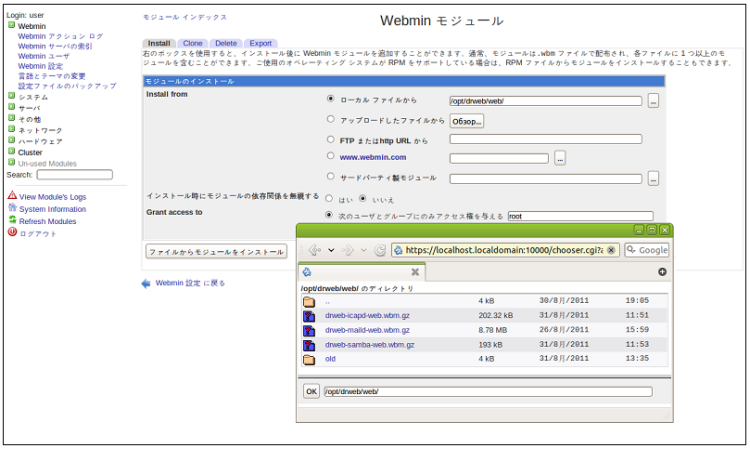
新しいモジュールのインストールは、**Webmin 設定**ページの **Webmin モジュール** で行います。

図 18. Webmin 設定

以下の手順でモジュールのインストールを行います。

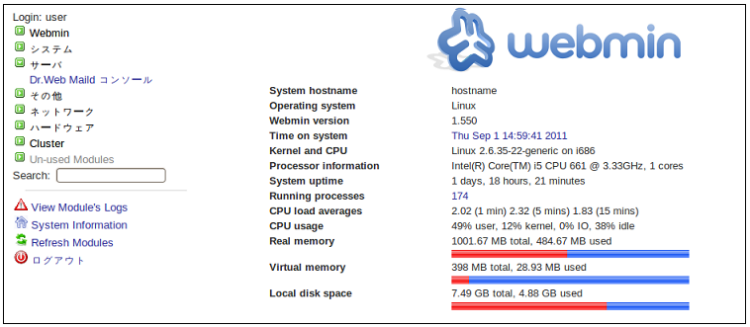
1. **Webmin** モジュールページで、ローカル ファイルからテキストフィールドの右にある **Browse** ボタンを押します。開いたウィンドウに、フォルダ・ファイルを入力します。
2. インストールパッケージを選択します。(`%bin_dir/web/`にある **Dr.Web console for UNIX Mail Servers** のパッケージを選択します。)

図 19. Webmin モジュール



3. ファイルクリックでウィンドウ下のフィールドにアイテムが選択された後、OKボタンを押します。
4. インストールパッケージを選択後、ファイルからモジュールをインストール ボタンを押してインストールを開始します。
5. インストールが成功すると、 サーバセクションのメニューに **Dr.Web console for UNIX Mail Servers** が表示されます。

図 20. Dr.Web console for UNIX Mail Servers



基本設定

Dr.Web console for UNIX Mail Servers ページのトップに **モジュール設定** リンクがあります。 **隔離** セクションに設定ファイルのパス、initスクリプト、ブラックリスト・ホワイトリストのディレクトリパスなどを指定できます。

図 21. Module configuration

ユーザインターフェース

Dr.Web console for UNIX Mail Servers では、ブラウザの **Back**（戻る）ボタンを使用しないでください。**Back** ボタン、もしくはそれに相当するキーを使用した場合、メインメニューに戻ります。

図 22. Dr.Web console for UNIX Mail Servers

画面右上に **Dr.Web MailD** と **Dr.Web for UNIX mail servers** の現在のバージョンが表示されます。

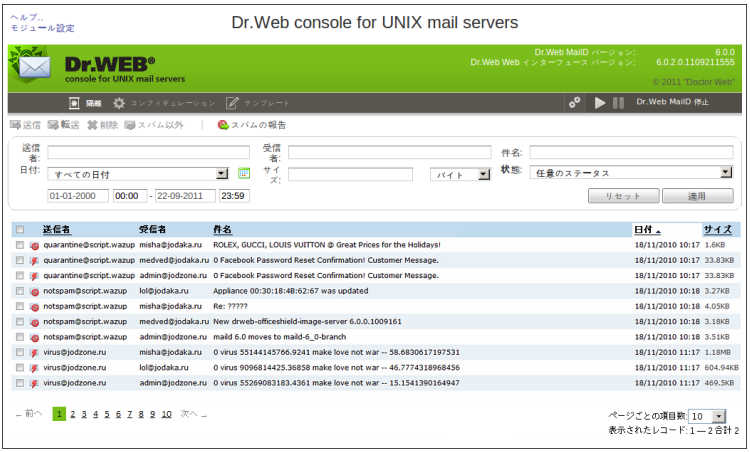
画面上には **隔離**, **コンフィギュレーション**, **テンプレート** の3セクションが配置されています。デフォルトでは、**隔離** セクションが開きます。

このセクションの右には **Start Dr.Web MailD** と **Stop Dr.Web MailD** のボタンが配置され、ステータスが表示されています。

隔離

Dr.Web for UNIX mail servers のアンチウィルス・アンチスパムでフィルタされたメッセージは、設定によって隔離された場合、隔離(Quarantine)タブ内で管理することができます。

図 23. "Quarantine（隔離）"タブ



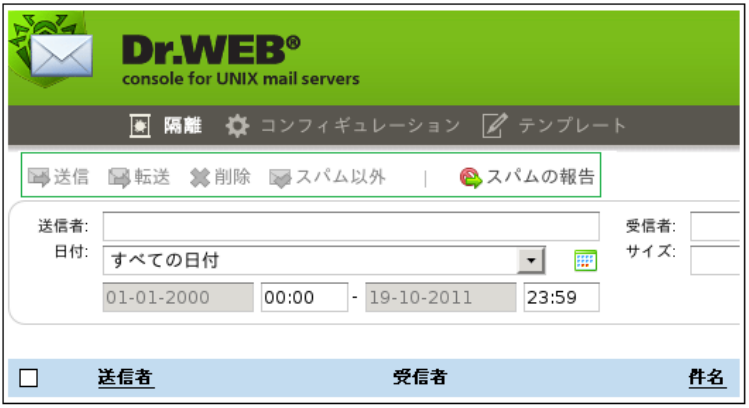
隔離（**Quarantine**）タブには下記の項目があります。

- ツールバー
- フィルター機能
- 隔離されたメッセージリスト
- ナビゲーション と1ページ内での表示数を変更するドロップダウンメニュー

ツールバー

ツールバーボタン（ **Report spam** ボタン以外）はリストからメッセージが選択された時点でアクティブになります。

図 24. ツールバー



ツールバーによって以下のことを実行できます。

- 隔離されたメッセージを元の受信者に送信。 該当するメッセージを選択し、 **Send**（**送信**）ボタンを押す。
- 隔離されたメッセージを転送。 該当するメッセージを選択し、 **Forward**（**転送**）ボタンを押す。 オープンしたウィンドウに必要事項を記入：受信者（受信者e-mail アドレス），件名（Subject），メッセージ（転送されるメールに対するメッセージテキスト），添付（Attachments）（メールを添付として転送）
- 隔離されたメッセージを削除。該当するメッセージを選択し、 **Delete**（**削除**）ボタンを押すか、キーボードのDEL キーを押す。
- 間違った"スパム" 該当するスパムステータスのメッセージを選択し、 **Not Spam** ボタンを押す。メッセージは自動的に受信者に送信され、隔離フォルダから削除される。
- スパムのレポート。

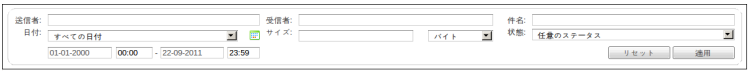
スパムのレポートはメッセージリストからは操作できません。スパムと思われるメッセージはファイルシステムに保存し、その後、**Dr. Web for UNIX mail servers**によって提供されたインターフェースを使用して**Dr. Web**ラボに送信してください。

Report spam ボタンを押すと、ウィンドウがオープンし、疑わしいメッセージを含むファイルをアップロードすることができます。

フィルタ

隔離されたメッセージをフィルタによって操作しやすいよう表示させます。

図25. フィルタ



フィルタによって以下のクライテリアで表示させることができます。

- **Sender**（送信者）- 送信者のe-mail アドレス。アドレスの全て、もしくは一部を入力。
- **Recepient**（受信者）- 受信者のe-mail アドレス。 アドレスの全て、もしくは一部を入力。
- **Subject**（件名）- 件名中の任意の文字列
- **Date**（日付）- メッセージが隔離された日付。 ドロップダウンリストから期間を選択、もしくは ボタンでカレンダーから入力。以下のオプションが選択可能：
  - ✓ **all dates** - 隔離フォルダの全てのメッセージを選択
  - ✓ **today** - 当日12:00 a.m. から現在までのメッセージを選択
  - ✓ **yesterday** - 前日12:00 a.m. から当日12:00 a.m. までのメッセージを選択
  - ✓ **this week** - 週始めから現在までのメッセージを選択
  - ✓ **this month** - 月始めから現在までのメッセージを選択
  - ✓ **custom period** - カレンダーによって任意の期間のメッセージを選択

図26. カレンダー

ドロップダウンから **custom period** を選択するか、 ボタンを押すことでカレンダーウィンドウが開きます。 期間を指定し、**OK** ボタンを押すと、カレンダーウィンドウが閉じ、フィールド

に値が入力されます。直接値を入力して指定することもできます。

期間指定した場合、その日時を含む期間に隔離されたメッセージのみが表示されます。特定の時間を指定したい場合には、その時間を入力することで、該当のメッセージが表示されます。

- **Size**(サイズ) - 指定サイズ以上のメッセージを選択(デフォルトbyte、ドロップダウンメニューで変更可能)。0 を設定するとサイズは考慮しない。
- **Status**(ステータス) - 隔離の理由。
  - ✓ **virus** - アンチウィルスモジュールによってウィルスと認識された
  - ✓ **spam** - アンチスパムモジュールによってスパムと認識された
  - ✓ **rule** - 内部ルールによって隔離された
  - ✓ **processing error** - メッセージ処理中にエラーとなり隔離された

クライテリア設定後、 **Apply** ボタンを押してください。 **Reset** ボタンでデフォルトに戻ります。

メッセージリスト

隔離フォルダにメッセージがある場合、隔離(**Quarantine**)タブに表形式でメッセージが表示されます。

図27. メッセージリスト

送信者	受信者	件名	日付	サイズ
quarantine@script.wazup	misha@jodaka.ru	ROLEX, GUCCI, LOUIS VUITTON @ Great Prices for the Holidays!	18/11/2010 10:17	1.6KB
quarantine@script.wazup	medved@jodaka.ru	0 Facebook Password Reset Confirmation! Customer Message.	18/11/2010 10:17	33.83KB
quarantine@script.wazup	admin@jodzone.ru	0 Facebook Password Reset Confirmation! Customer Message.	18/11/2010 10:17	33.83KB
notspam@script.wazup	lol@jodaka.ru	Appliance 00:30:18:4B:62:67 was updated	18/11/2010 10:18	3.27KB
notspam@script.wazup	misha@jodaka.ru	Re: ?????	18/11/2010 10:18	4.05KB
notspam@script.wazup	medved@jodaka.ru	New drweb-officeshield-image-server 6.0.0.1009161	18/11/2010 10:18	3.18KB
notspam@script.wazup	admin@jodzone.ru	maild 6.0 moves to maild-6_0-branch	18/11/2010 10:18	3.51KB
virus@jodzone.ru	misha@jodaka.ru	0 virus 55144145766.9241 make love not war -- 58.6830617197531	18/11/2010 11:17	1.18MB
virus@jodzone.ru	lol@jodaka.ru	0 virus 9096814425.36858 make love not war -- 46.7774318968456	18/11/2010 11:17	604.94KB
virus@jodzone.ru	admin@jodzone.ru	0 virus 55269083183.4361 make love not war -- 15.1541390164947	18/11/2010 11:17	469.5KB

管理者は全ての隔離されたメッセージにアクセスすることができます。

表のデータは以下の項目でまとめられています。

- **Status** 列 - メッセージのステータス(隔離の理由)です。それぞれのステータス

でアイコンが異なります: - ウィルスを含んでいます, - スパムと判定されています, - 内部フィルタリングルールによって隔離されています, - 処理中にエラーが発生しました。マウスポインタをアイコンの上に置くと、隔離された理由の詳細が確認できます。

- **Sender** 列 - 送信者メールアドレスです。
- **Recipient** 列 - 受信者のメールアドレスです。
- **Subject** 列 - 件名です。件名はソートして表示順を変更できます。
- **Date** 列 - 隔離された日時です。過去24時間以内に隔離されたメッセージは時間のみが表示されます。日時はソートして表示順を変更できます。
- **Size** 列 - メッセージサイズです。サイズはソートして表示順を変更できます。

メッセージの選択には、チェックボックスにチェックを入れてください。全てのメッセージを選択する場合には、表左上のヘッダのチェックボックスにチェックを入れてください。

受信者（Recipient）, 件名（Subject）, 日付（Date） フィールドはメッセージにリンクされています: クリックすると下記のようなメッセージスクリーンが表示されます。

図28. 隔離メッセージ

メッセージの内容、ソース(**ソースの表示**リンク)、ヘッダ(**ヘッダー**リンク)、添付が確認できます。

隔離領域に戻る ボタンを押すと隔離(Quarantine)のメイン画面に戻ります。

ナビゲーション

図29. ナビゲーション

ナビゲーションでは以下のことが実行できます。

- 表の前・次のページにジャンプします。(CTRL+矢印キーでも同様にジャンプします)
- ページ番号によって各ページを表示します。
- メッセージのトータル数と現在表示しているリストの位置を表示します。

隔離(Quarantine)セクションの1ページの表示数を変更したい場合は、画面右下のドロップダウンメニューで変更できます。10, 20, 50, 100 に変更可能です。 メニュー選択後、自動的に画面が切り替わります。

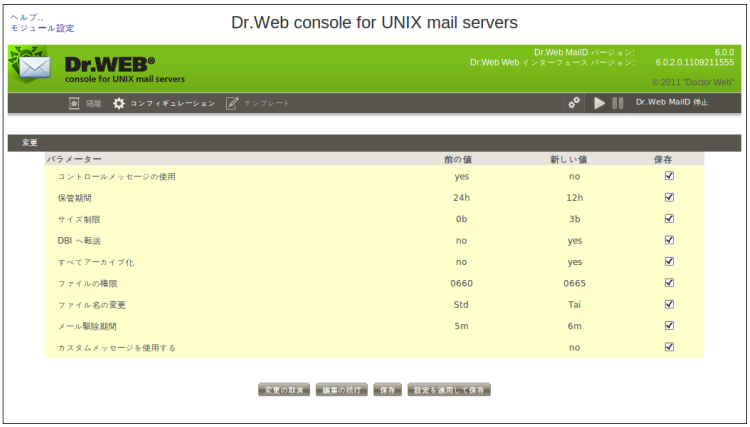
表が再表示されるかソートされると、それまでの選択は解除されます。

設定

ボタンを押してテキストフィールドに指定することで、ドロップダウンリストからパラメータ値を選択することができます。 **詳細** リンクで詳細を表示できます。パラメータ変更後に値を戻したい場合は アイコンをクリックすることで値を戻せます。また、 アイコンでデフォルト値に戻ります。

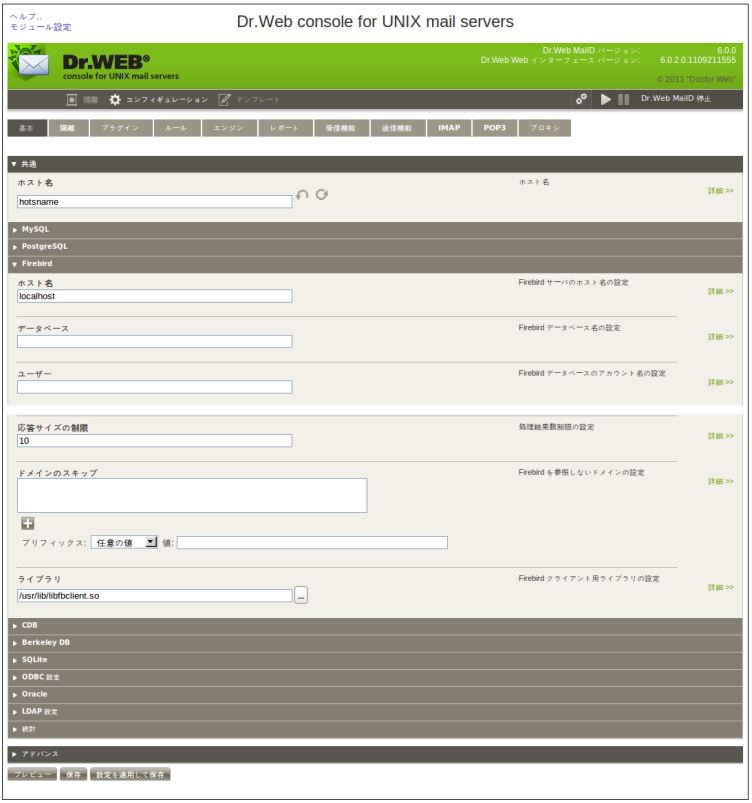
変更確認には**プレビュー(Preview)**をクリックしてください。 プレビューページでは全ての変更を保存するか一部の変更を保存するかどうか、選択できます。更に変更を加えたい場合には、**Continue Editing** をクリックし、プレビューページに戻ってください。変更を実行しない場合は、 **Cancel** クリックしてください。保存する場合は、**Save** か **Apply and Save** をクリックしてください。

図30. プレビュー


ヘルプ
モジュール設定
Dr.Web console for UNIX mail servers
Dr.WEB®
console for UNIX mail servers
Dr.Web MailID バージョン: 6.0.0
Dr.Web Web インターフェース バージョン: 6.0.2.0.1109211555
© 2011 "Doctor Web"
隔離
コンフィギュレーション
テンプレート
Dr.Web MailID 停止
変更
パラメーター
前の値
新しい値
保存
コントロールメッセージの使用 yes no
保管期間 24h 12h
サイズ制限 0b 3b
DBI へ転送 no yes
すべてアーカイブ化 no yes
ファイルの権限 0660 0665
ファイル名の変更 Std Tai
メール駆除期間 5m 6m
カスタムメッセージを使用する no
変更の取消
操作の続行
保存
設定を適用して保存

"基本"タブ

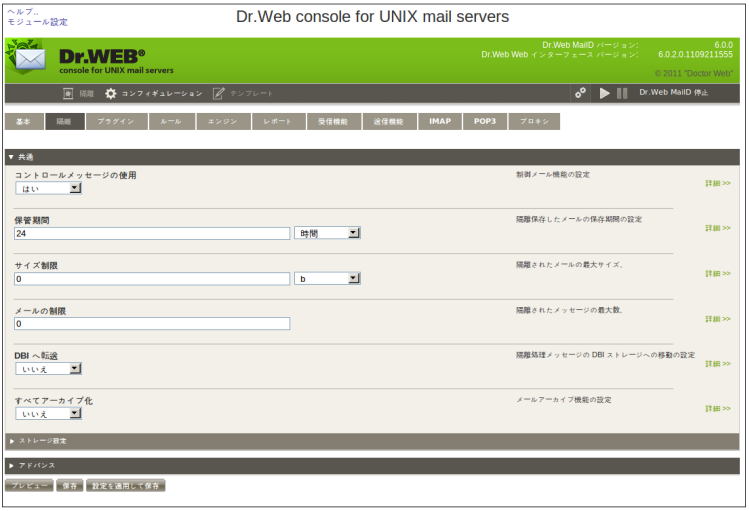
図31. 基本設定



このタブでは、統計情報のエクスポートと、 **Dr.Web MailD** とデータベースの設定について設定します。パラメータはドロップダウンから選択するか、テキスト欄に記入します。

"隔離" タブ

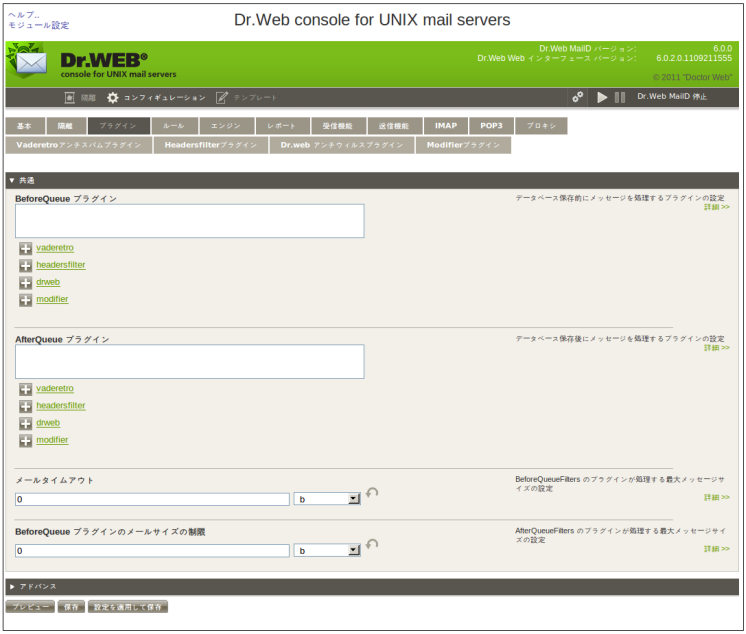
図32. 隔離設定



このタブでは隔離（**Quarantine**）セクションに関して設定します： メッセージを隔離する期間、隔離されたメッセージのアクセス権、名前変更オプション、DBIストレージの設定

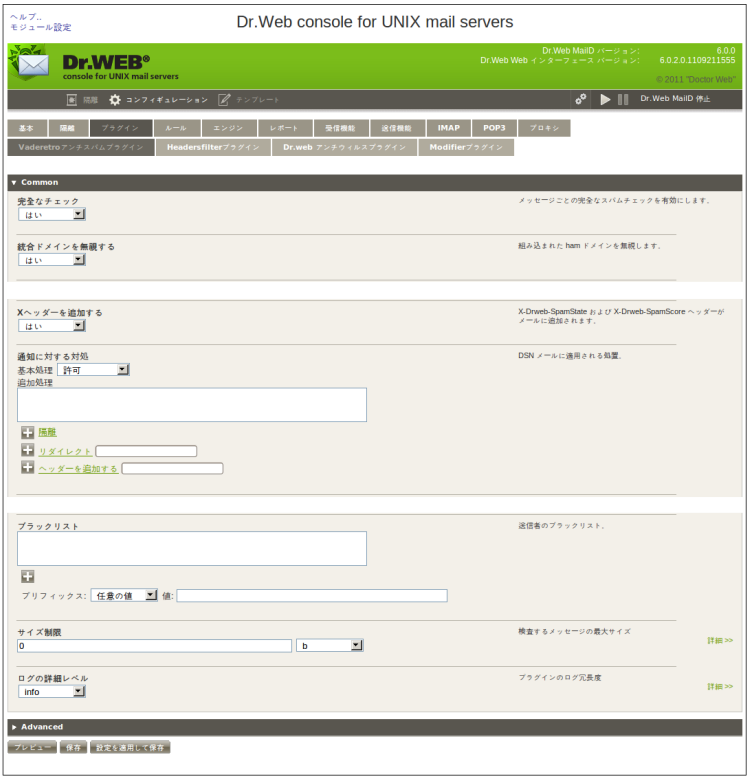
"プラグイン" タブ

図33. プラグイン設定



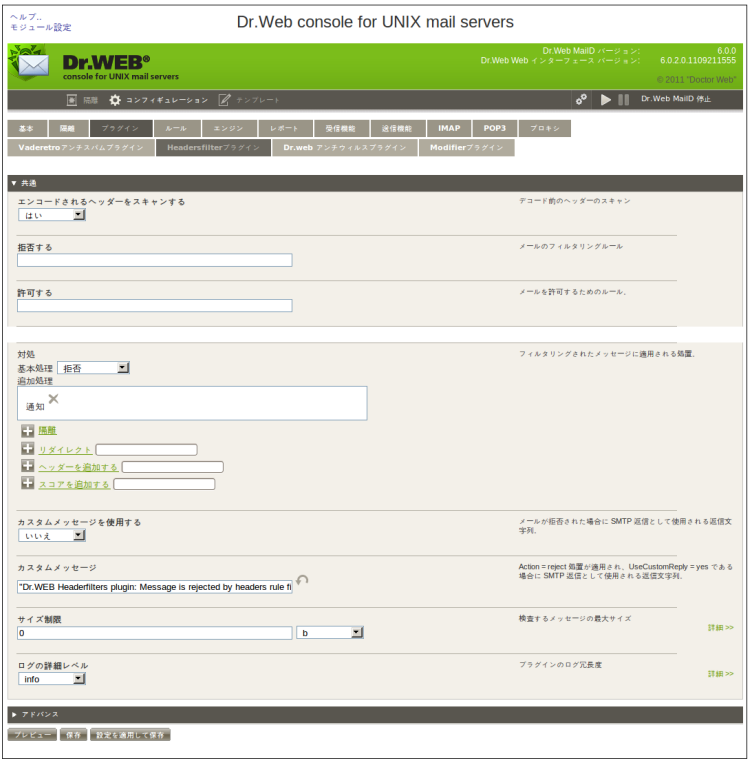
このタブでは全てのメールフィルタリングプラグインに関しての一般的な設定します。各プラグインの個別設定に関しては、それぞれのタブで設定します。

図34. Anti-spam 設定



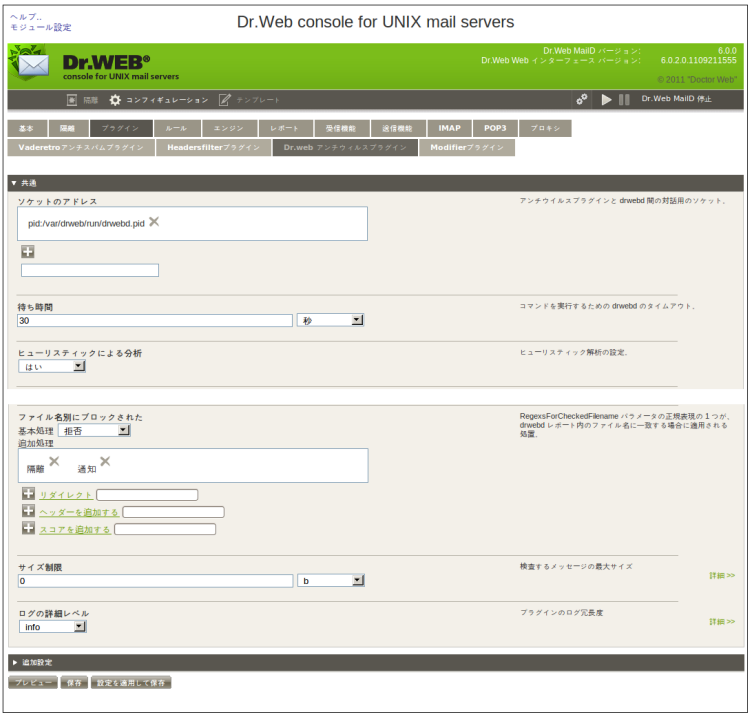
このタブでは VadeRetro アンチスパムプラグインの設定をします。

図35. Headers Filter 設定



このタブでは、ヘッダによってメッセージをフィルタリングするheadersfilterプラグインの設定をします。"HEADER = regular_expression" を全ての **~Condition**欄の "value" フィールドに設定します。Actionパラメータのredirect横のテキスト欄にはフィルタしたメッセージをリダイレクトする先のメールアドレスを設定します。

図36. アンチウィルス 設定



このタブでは Dr.Web アンチウィルスプラグインの基本設定を行います。

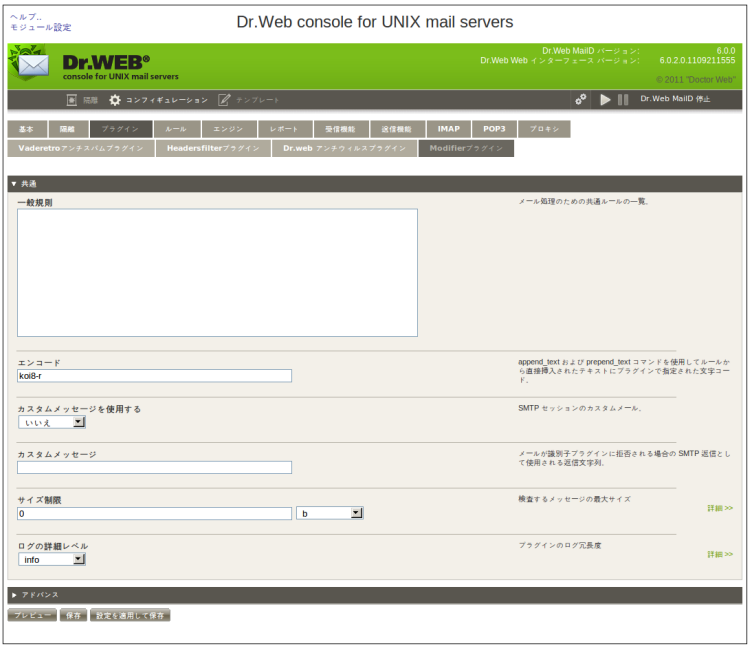
それぞれのパラメータの actions の redirect には、フィルタしたメッセージをリダイレクトする先のメールアドレスを設定します。（デフォルトでは **Engine** タブの **`RedirectMail`** パラメータが使用されます）

アドバンス設定で、ブロックされたメッセージのカスタムリプライを設定します。

図37. アンチウィルスアドバンス設定

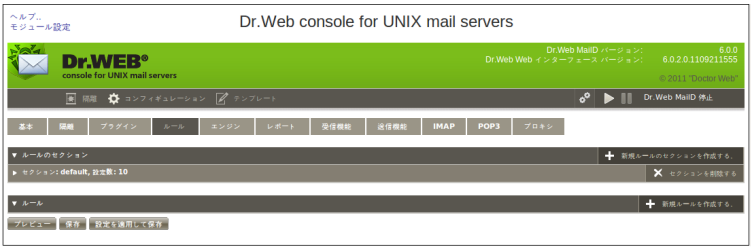
このタブでは Modifier プラグインの基本設定を行います。

図38. Modifier 設定



"ルール" タブ

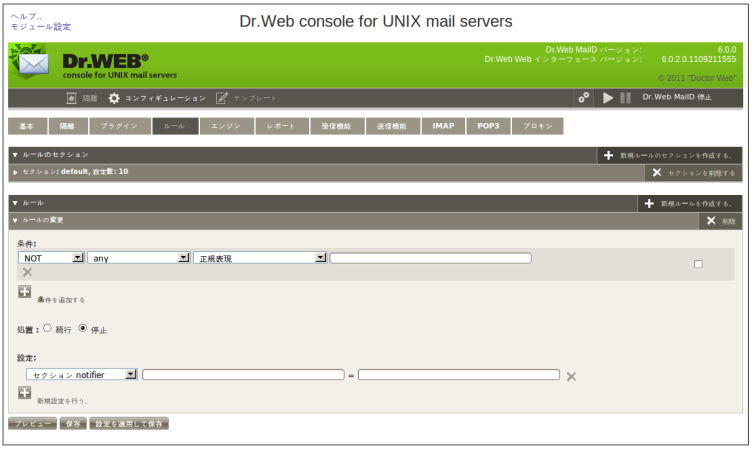
図39. ルール



このタブでは **Dr.Web MailD** の設定ファイル の [Rules]セクションの設定で

す。**Create new rule** ボタンによって異なるルールを設定することもできます。

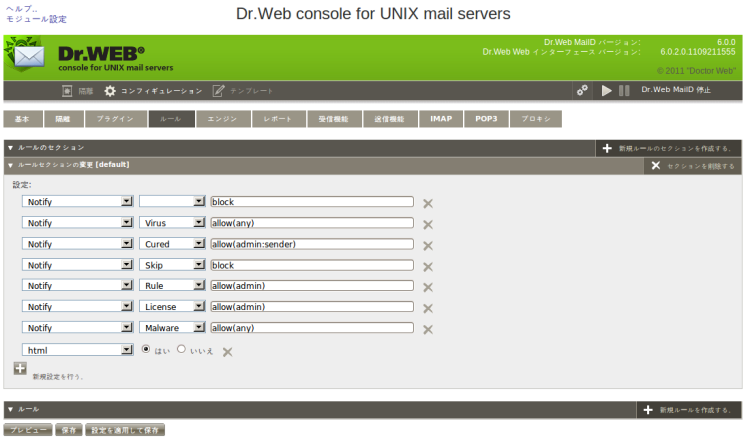
図40. ルール編集



ルール編集(Rule editing)メニューでは、**条件**(**Conditions**)、アクション(**Actions**)、**設定**(**Settings**) を設定します。条件は論理演算とグループによって設定します。 グループ化するには、チェックボックスにチェックを入れ、 ボタン近くの **group** ボタンを押します。グループ解除は、チェックボックスにチェックを入れ、 **ungroup** ボタンを押します。

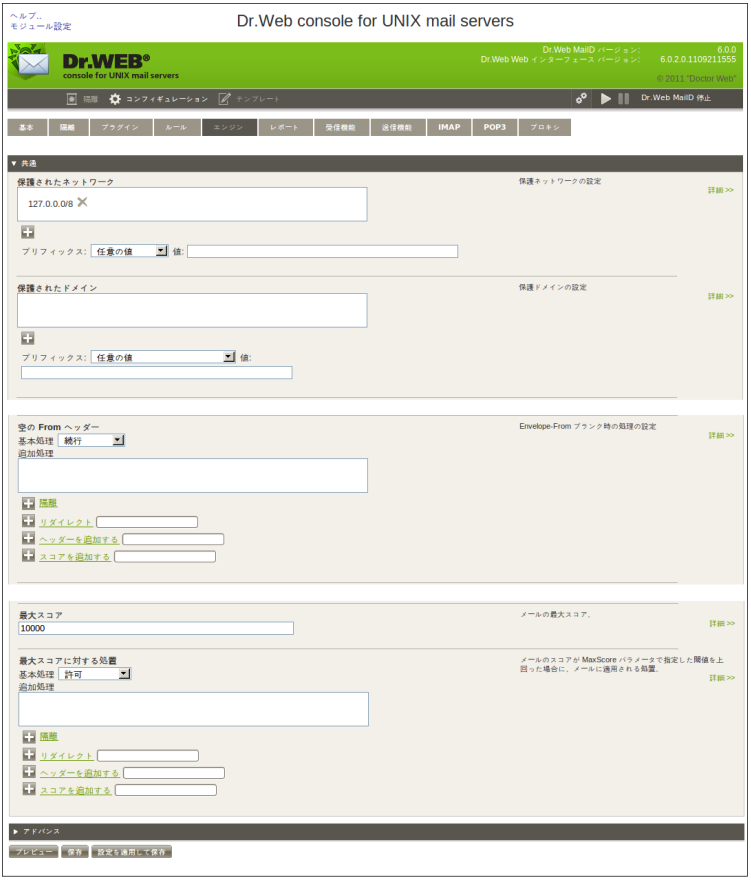
Create new rules section ボタンを押すと異なる設定を増やせます。

図41. ルールセクション編集



"エンジン" タブ

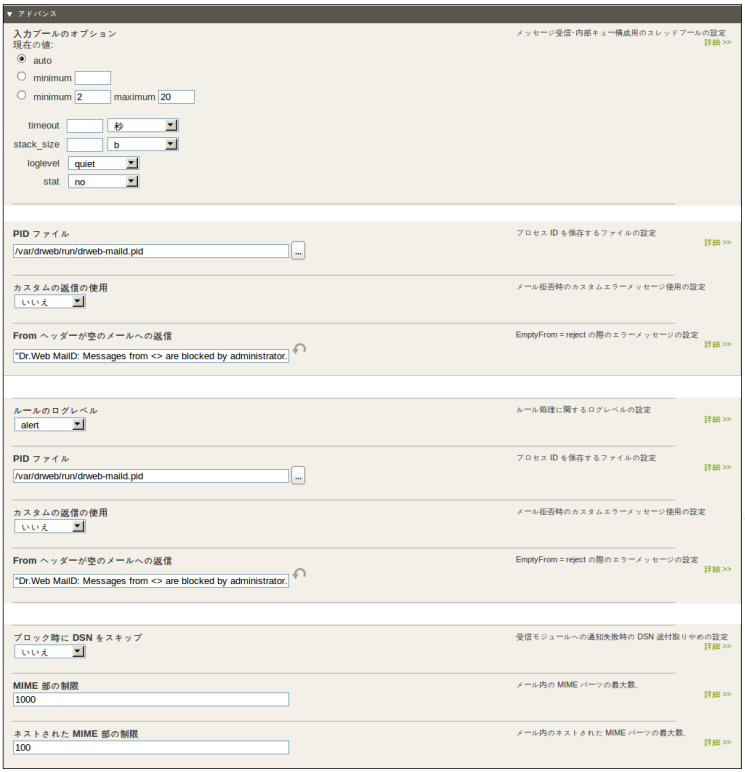
図42. エンジン一般設定



このタブでは、リダイレクトアクションに使用されるデフォルトメールアドレスを指定し、drweb-maild の制御を行います。

Pool オプションとカスタムリプライの設定も行います。

図43. アドバンスエンジン設定

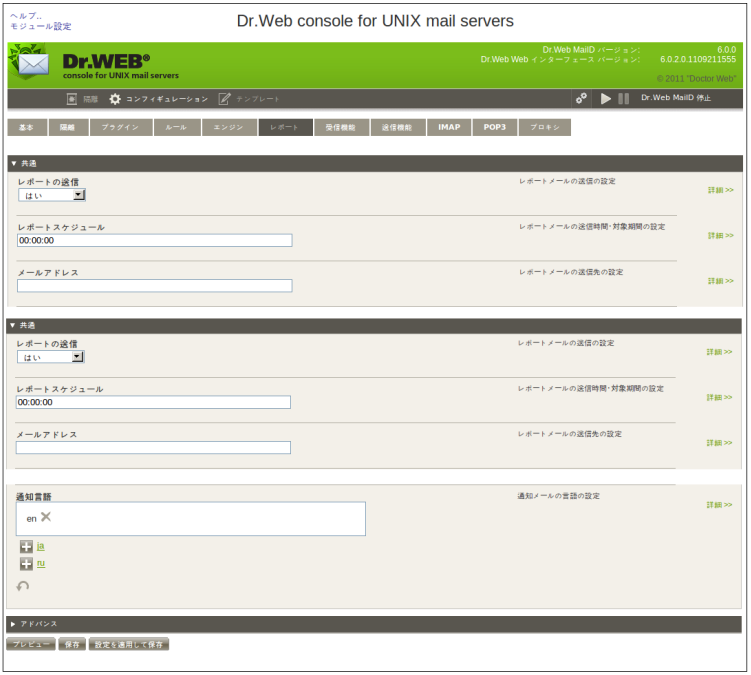


MailBase セクションでは、メールデータベースの設定を行います。

図44. MailBase 設定

"レポート " タブ

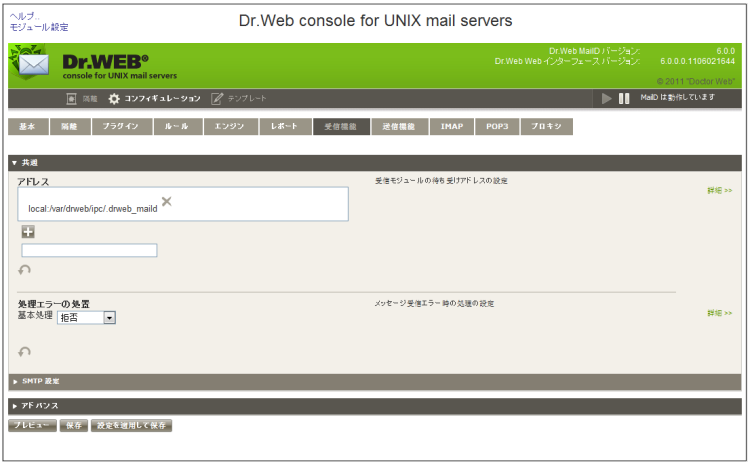
図45. レポート設定



このタブでは、管理者への統計レポート送信とデータベースへの保存に関するオプション設定を行います。

"受信機能" タブ

図46. メール受信一般設定



このタブでは、SMTP/LMTPリクエストのメールを受信する1つ、もしくは複数のアドレスと、エラー時のアクションを指定します。

アドバンスメール受信設定では、**Dr.Web MailD** とMTAとの相互設定を行います。

図47. アドバンスメール受信設定

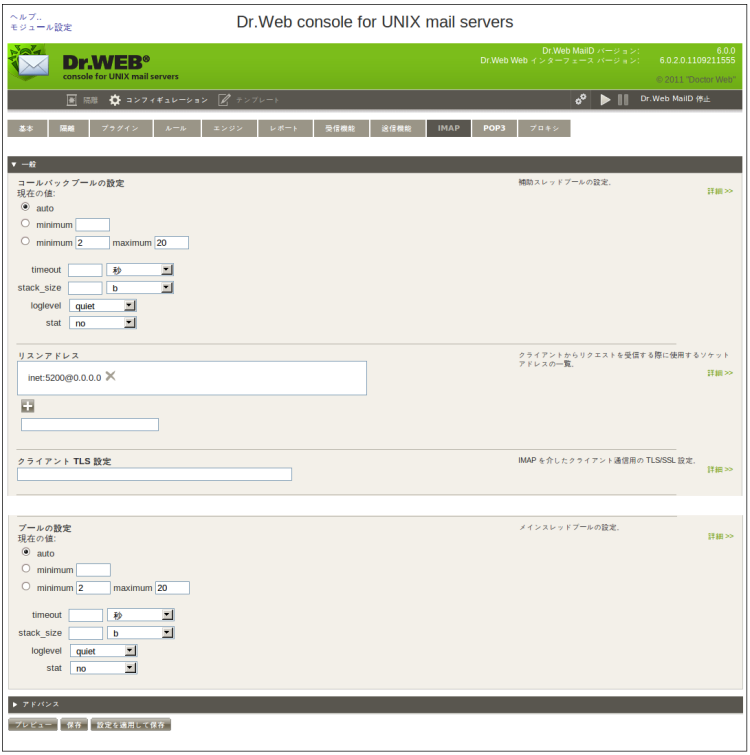
"送信機能" タブ

図48. メール送信設定

このタブでは、送信メッセージに対するアクションと、コマンド実行時のタイムアウト、**Daemon** やプラグイン実行時のメッセージを設定します。

"IMAP" タブ

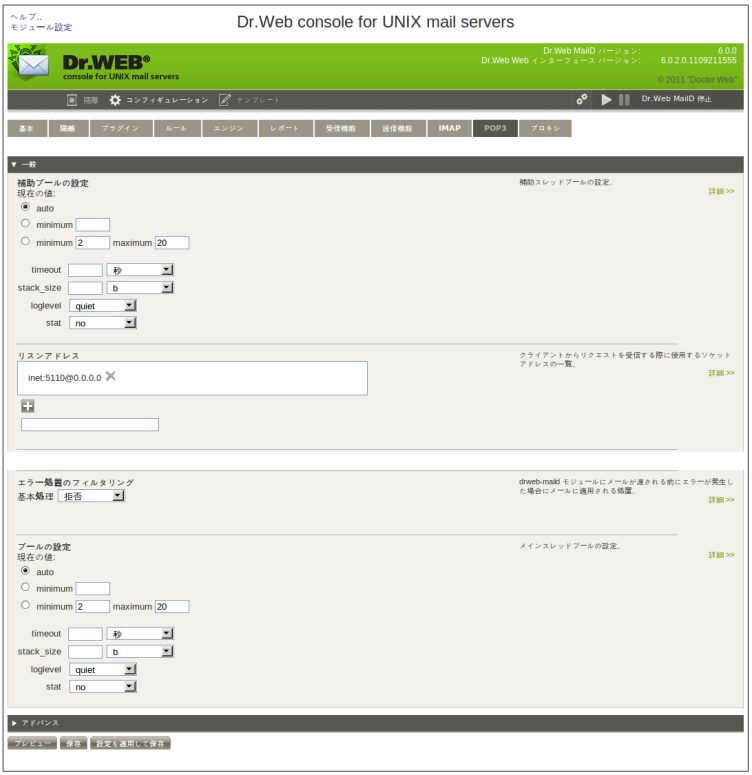
図49. IMAP 設定



このタブでは、IMAP フィルタの設定を行います。

"POP3"タブ

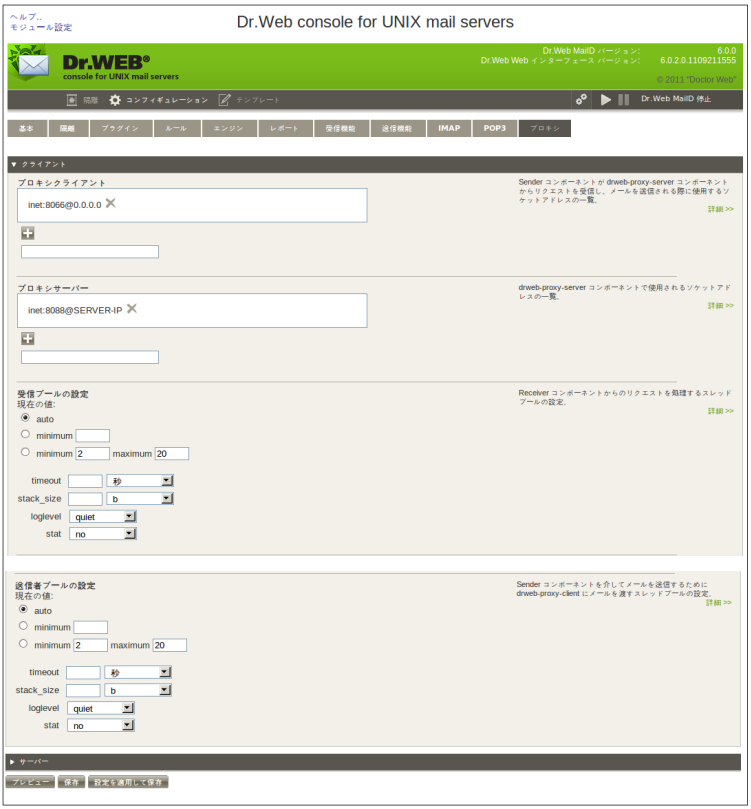
図50. POP3 設定



このタブでは、POP3 フィルタの設定を行います。

"プロキシ"タブ

図51. プロキシ設定



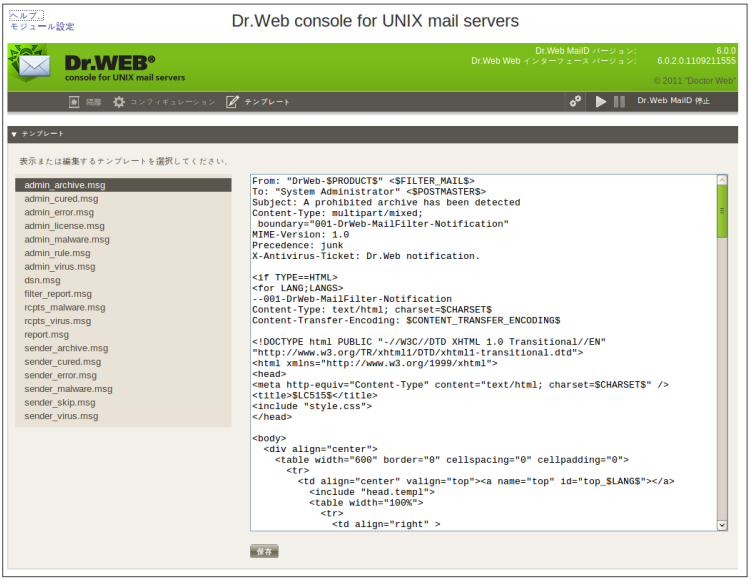
このタブでは、異なるホスト上にある **Dr.Web for UNIX mail servers** コンポーネントとの稼働を実現する、プロキシの設定を行います。

テンプレート

このセクションでは、ウィルス検出時や **Daemon**、プラグインのエラー時のメッセー

ジのテンプレートを設定します。

図52. テンプレート



ADMIN_ARCHIVE.msg – drweb32.ini設定ファイルで設定されたアーカイブに対する設定値を超えたために **Daemon** がスキャンできなかった場合のレポートテンプレートです。管理者に送信されます。

ADMIN_CURED.msg – 感染メッセージを修復したレポートテンプレートです。管理者に送信されます。

ADMIN_ERROR.msg – **Daemon** かプラグインエラーの場合のレポートテンプレートです。管理者に送信されます。

ADMIN_LICENSE.msg – ライセンス制限の為にチェックされなかった場合のレポートテンプレートです。管理者に送信されます。

ADMIN_MALWARE.msg – メッセージ内にマルウェアが検知された場合のレポートテンプレートです。管理者に送信されます。

ADMIN_RULE.msg – ルールによってメッセージが拒否された場合のレポートテンプレートです。管理者に送信されます。

ADMIN_VIRUS.msg – メッセージ内にウィルスが検知された場合のレポートテンプレートです。管理者に送信されます。

DSN.msg – ステータス通知のテンプレート

RCPTS_MALWARE.msg – メッセージ内にマルウェアが検知された場合のレポートテンプレートです。受信者に送信されます。

RCPTS_VIRUS.msg – メッセージ内にウィルスが検知された場合のレポートテンプレートです。受信者に送信されます。

REPORT.msg – 通常の **Daemon** レポートテンプレートです。

SENDER_ARCHIVE.msg – drweb32.ini設定ファイルで設定されたアーカイブに対する設定値を超えたために **Daemon** がスキャンできなかった場合のレポートテンプレートです。最初の送信者に送信されます。

SENDER_CURED.msg – 感染メッセージを修復したレポートテンプレートです。最初の送信者に送信されます。

SENDER_ERROR.msg – **Daemon** かプラグインエラーの場合のレポートテンプレートです。最初の送信者に送信されます。

SENDER_MALWARE.msg – メッセージ内にマルウェアが検知された場合のレポートテンプレートです。最初の送信者に送信されます。

SENDER_SKIP.msg – スキャン失敗時のレポートテンプレートです。パスワード保護されたファイルや壊れたアーカイブ、一般的でないファイルなどが添付されているような場合や、スキャンタイムアウトするような場合にスキャンが中断されます。レポートは最初の送信者に送信されます。

SENDER_VIRUS.msg – メッセージ内にウィルスが検知された場合のレポートテンプレートです。最初の送信者に送信されます。

お問い合わせ

Dr.Web for UNIX mail servers は常に改良され続けています。ご利用頂けるアップデートについての最新のニュースおよび情報は、以下のwebサイト上でご覧いただけます。

http://www.drweb.com/

セールス部門:

http://buy.drweb.com/

テクニカルサポート:

http://support.drweb.com/

問題が発生した場合にお送りいただくレポートには次の事柄を記載してください。

- お使いのOSの名称およびバージョン
- **Dr.Web for UNIX mail servers**モジュールのバージョン
- 全てのモジュールの設定ファイル
- 全てのモジュールのログファイル